ALTA by MONNIT

Remote Monitoring for Business

ALTA Advanced Edge Gateway

USER GUIDE

Table of Contents

I. INTRODUCTION

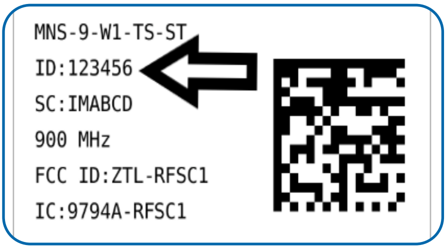
The ALTA Advanced Edge Gateway is to deliver sensor data from Monnit sensors to cloud providers, or to your own MQTT(S) broker or other application serving so. The gateway is designed to present an informed set up process, and providing reliable operation.

This guide is specifically directed to a new user of the gateway. Monnit provides several helpful resources to answer your questions and get your Edge Gateway set up:

1. **The Gateway:** The gateway includes reference materials accessible through a browser interface. The gateway has an automatic software updater, which will update the included reference materials at the same time. Thus, these should always be the most current.
2. **The User Guide:** Although you might have an out-of-date copy, the answers you need are still likely present here.
3. **Monnit Technical Support and Your Sales Representative:** After consulting the gateway browser interface and this user guide, if you cannot find the information you need, feel free to reach out using the telephone number at the end of this document.

By the end of this guide, you should have sensor data arriving in your cloud account or consuming application over MQTT.

GATEWAY ID



MNS-9-W1-TS-ST
ID:123456
SC:IMABCD
900 MHz
FCC ID:ZTL-RFSC1
IC:9794A-RFSC1

Figure 1

The Device ID is a unique six digit number located on the bottom label of your gateway.

You will require this ID several times as you work through this user guide, so please take note.

Below this is the six letter Security Code, which will be necessary for registering your device.

II. BASIC OPERATION OF THE GATEWAY

The ordinary system with an Advanced Edge Gateway includes some number of wireless sensors, a local area network with a router, and one or more cloud providers connected through the Internet, as depicted below:

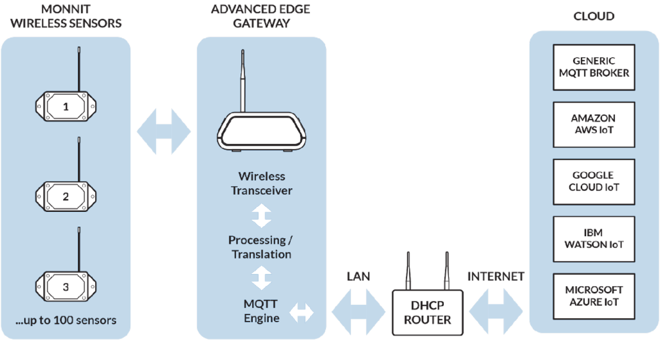


Figure 2

This gateway is implemented onto an Ubuntu Linux single-board computer platform, with Monnit proprietary software installed. Included with the gateway are an internal radio transceiver, an antenna, three indicator lights and a utility button:

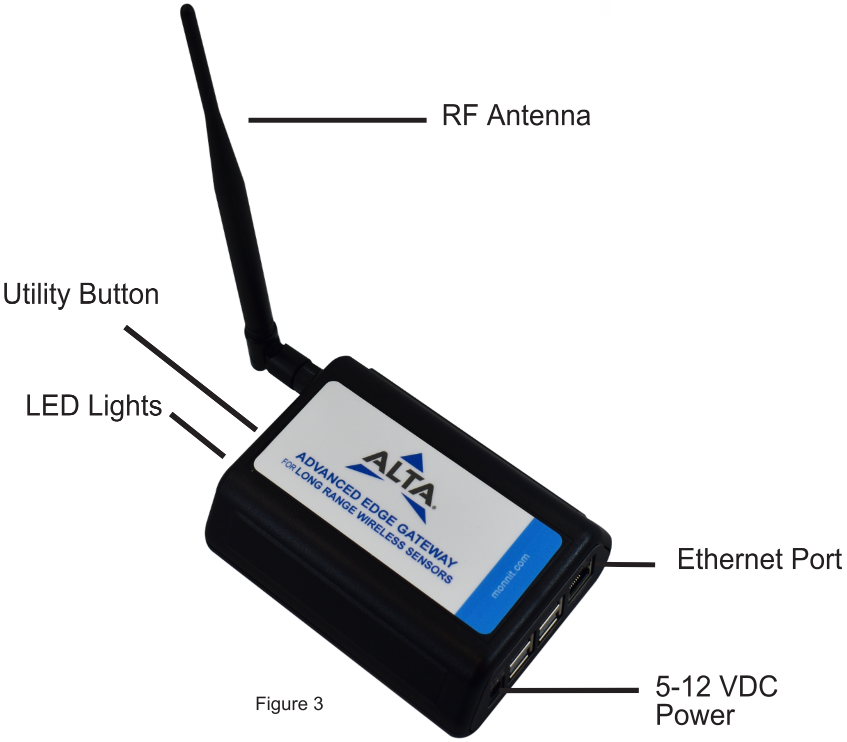


Figure 3

III. STARTING THE GATEWAY

POWERING THE GATEWAY

Power up the Advanced Edge Gateway by first plugging in the unit to an outlet and connecting the Ethernet Cable. It may take up to two minutes for the indicator LEDs to start flashing.

1. Connect your antenna to the gateway as seen in Figure 4.

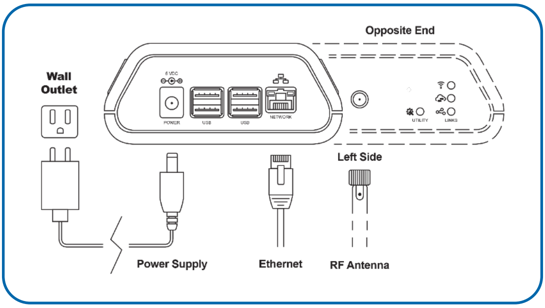


Figure 4

2. Plug in your power supply cord and Ethernet cable. The gateway connects to the Internet through a router providing the DHCP protocol. (A static IP address can be set later through the user interface.)

Control and monitoring of the gateway is provided to you in three ways. The first is a group of three LEDs and a utility button on the gateway's exterior. The second is an HTTPS interface accessible to browsers on the same local-area network. Lastly, is through the delivery of gateway and sensor reports at the cloud. These are further described below.

UNDERSTANDING THE GATEWAY LEDS

The gateway has three indicator LEDs that show the general status of the gateway (See Figure 5):

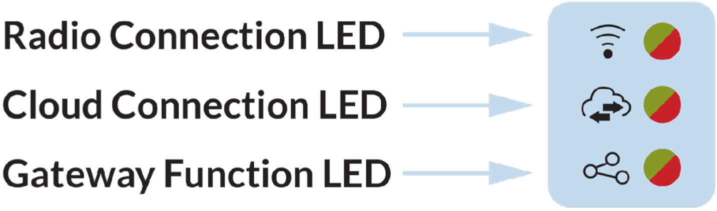


Figure 5

The top **Radio Connection LED** shows the state of the wireless transceiver, the middle **Cloud Connection LED** denotes the state of producer connections to the cloud, and the bottom **Gateway Function LED** shows power and whether the gateway software is running.

First Connection

When power is first applied to the gateway, only the Gateway Function LED will be lit green. When the gateway operating system has booted, and as the gateway software starts, all the lights will briefly flash red and green. Then the Radio Connection LED and Cloud Connection LED will blink green. The first time you power up the gateway, the Cloud Connection LED will flash red, indicating to you that sensor data is not being sent to the Cloud. That will be because the a connection hasn't yet been configured, see section (Insert) on how to resolve this issue.

Normal Operation

Most of the time the gateway software will boot automatically. Generally, green indicates normal condition, red shows a fault is present.

The Gateway Function LED will blink once per second, showing you the software is running. The Radio Connection LED and Cloud Connection LED will usually remain solid green, blinking when sensor data is received. If the gateway is able to make a connection to all cloud providers configured, then the Cloud Connection LED will likewise show solid green, blinking when messages are sent.

The other pattern you might occasionally see is from the software updater. The updater checks an Internet server on startup once per day. If a new software package is successfully downloaded and validated, it will be installed. The installer will display a bouncing up-down green on the LEDs for a few seconds as it begins and finishes an update, along with some additional patterns specific to the software that are beyond the scope of this guide. When the updater finishes, it will return control to the gateway software, and the usual operation will resume.

ANTENNA ORIENTATION

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

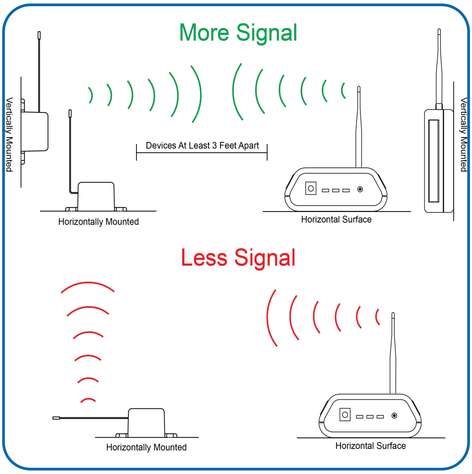
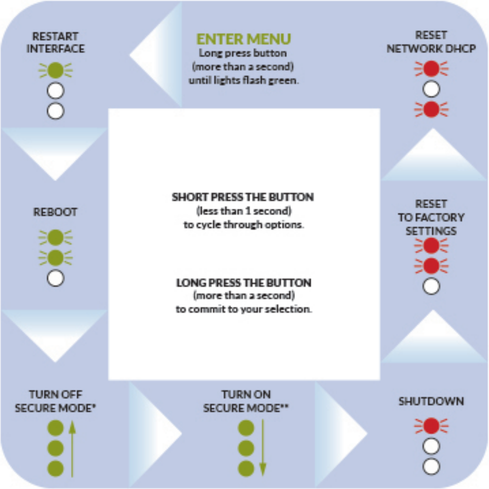


Figure 6

IV. THE UTILITY BUTTON AND MENU

Beside the indicator lights is a utility button through which commands can be issued to the gateway using the "Button Menu". Most of these functions can be commanded from the browser interface, but in case you can't get to it, they are available here. Please refer to the flowchart below for the Button Menu navigation and functions:



* ENABLES REMOTE ACCESS AND AUTO UPDATES
** DASABLES REMOTE ACCESS AND AUTO UPDATES

Figure 7

There are two principal methods of accessing the gateway. The first is through the utility button menu. Through this, you can perform some basic functions:

Restart interfaces: Choosing this button closes down and brings back up all connections to the cloud, Express Core, other connections, and restarts the HTTP user interface. This is most useful for diagnosing and mitigating connection errors.

Reboot: Reboots the Gateway's operating system, bringing everything up from a fresh start. This may take several minutes, so it is usually best to command the interfaces to restart first.

Turn off secure mode: Enables remote and local shell access to the Gateway, and enables the software autoupdater. Remote access is helpful for a technical support person in providing support.

Turn on secure mode: Disables remote and local shell access to the Gateway, and disables the software autoupdater. This is to lock down the gateway after it has been configured and is working, preventing unauthorized actions that could potentially disrupt operations. Note that the browser interface remains up, protected by a password.

Shutdown the gateway: Stops all processes running on the Gateway, and brings it into a condition where power may safely be removed.

Reset to factory settings: Clears the sensor list, the MQTT producers, and other configuration. Network settings are retained.

Reset network to DHCP: Used to back out of an erroneous static IP address or network configuration.

To operate these button menu items, it is of course necessary to be physically present at the Gateway. The HTTP or browser interface permits access at remote locations, and is generally preferred for most tasks.

The second method is to open the browser interface. See section **V. Accessing the Gateway** for instructions.

SHUTDOWN PROCEDURE ON THE UTILITY BUTTON MENU

Because this gateway includes an operating system, it is best to follow the shutdown procedure as much as possible. Please don't remove power from the gateway without performing the shutdown procedure.

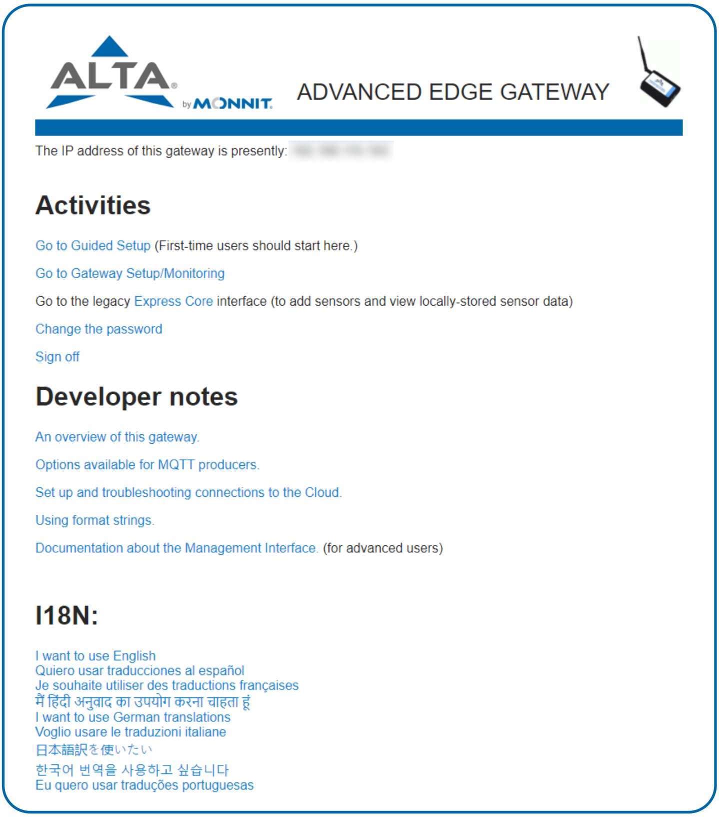
As described above, a shutdown can be commanded from the menu by long-pressing the utility button (for more than one second), short-pressing the button four times (until one blinking red light shows at the top), then long-pressing the button one more time to commit.

Monnit suggests waiting an additional two minutes before pulling the power cord.

V. THE BROWSER INTERFACE

The browser interface is a simpler way to manage your device. You can reach the browser interface by typing **https://aegw-{Device-ID}.local** into your address bar.

Note that the gateway will not be reachable in this way unless it is located on the same local-area network. If you see a warning about the certificate, please click on "go ahead" or it's equivalent. You will then reach the front index page seen in Figure 8 below:



The IP address of this gateway is presently: [redacted]

Activities

Go to Guided Setup (First-time users should start here.)

Go to Gateway Setup/Monitoring

Go to the legacy Express Core interface (to add sensors and view locally-stored sensor data)

Change the password

Sign off

Developer notes

An overview of this gateway.

Options available for MQTT producers.

Set up and troubleshooting connections to the Cloud.

Using format strings.

Documentation about the Management Interface. (for advanced users)

I18N:

I want to use English
Quiero usar traducciones al español
Je souhaite utiliser des traductions françaises
मैं हिंदी अनुवाद का उपयोग करना चाहता हूं
I want to use German translations
Voglio usare le traduzioni italiane
日本語訳を使いたい
한국어 번역을 사용하고 싶습니다
Eu quero usar traduções portuguesas

Figure 8

The page is organized in three categories:

Activities, or things you can do or configure,

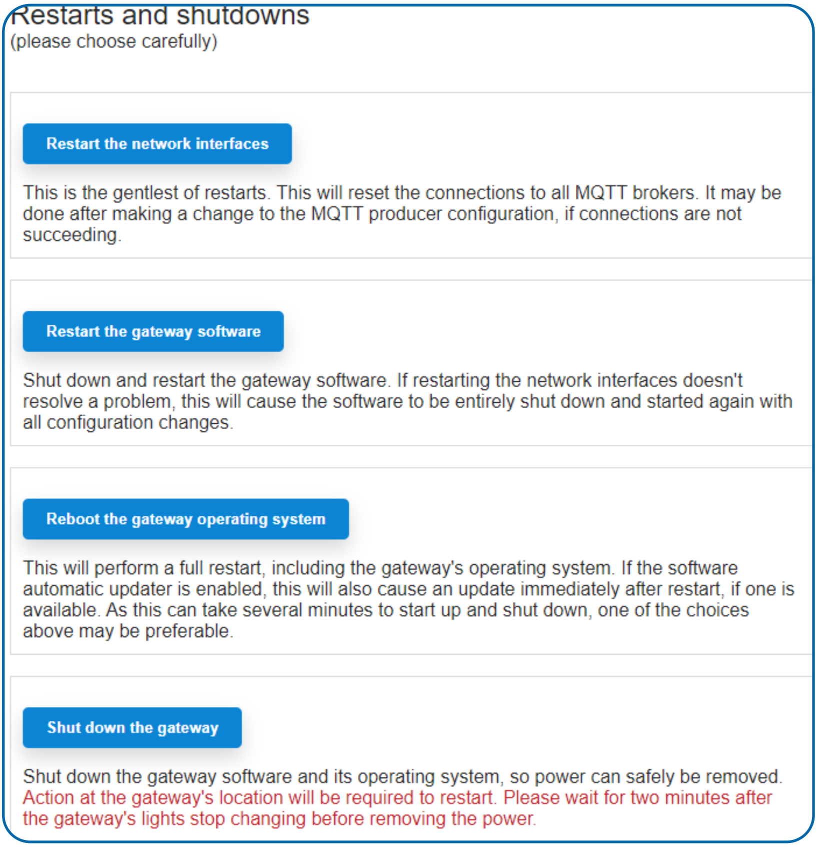
Developer notes, which is the main location for documentation, and

I18N: to change the language setting of this interface.

The Developer Notes are worth looking over when you have time or need. This guide will focus on **Activities**, mainly in the role of setting up the gateway for the first time. In the recommended procedure for setup, you should work your way down the activities on this page, starting with the Guided Setup described in the next section.

SHUTDOWN PROCEDURE ON THE BROWSER INTERFACE

Select the **Go to Gateway Setup/Monitoring** link. Then choose **Command a restart or a shutdown**. You'll then see a page that looks like Figure 9:



Restarts and shutdowns

(please choose carefully)

This is the gentlest of restarts. This will reset the connections to all MQTT brokers. It may be done after making a change to the MQTT producer configuration, if connections are not succeeding.

Shut down and restart the gateway software. If restarting the network interfaces doesn't resolve a problem, this will cause the software to be entirely shut down and started again with all configuration changes.

This will perform a full restart, including the gateway's operating system. If the software automatic updater is enabled, this will also cause an update immediately after restart, if one is available. As this can take several minutes to start up and shut down, one of the choices above may be preferable.

Shut down the gateway software and its operating system, so power can safely be removed. Action at the gateway's location will be required to restart. Please wait for two minutes after the gateway's lights stop changing before removing the power.

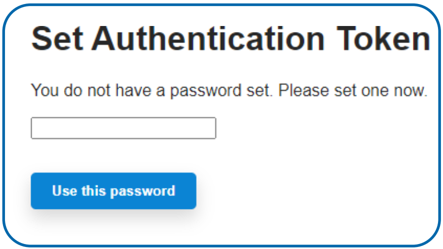
Figure 9

Selecting the "Shut down the gateway" button will bring the gateway into a condition for a safe shutdown. Please wait for two minutes after the gateway's lights stop changing before removing power.

VI. USING THE GUIDED SETUP FEATURE

The most significant benefit to the browser interface is the guided setup process. Start by first typing in **https://aegw-{Device-ID}.local** in your address bar. Bypass the warning about the certificate. At the index page, choose the **Go to Guided Setup** link, directly under the Activities section.

The first time you enter the Guided Setup or the Gateway Setup/Monitoring pages, you will see a screen like this:



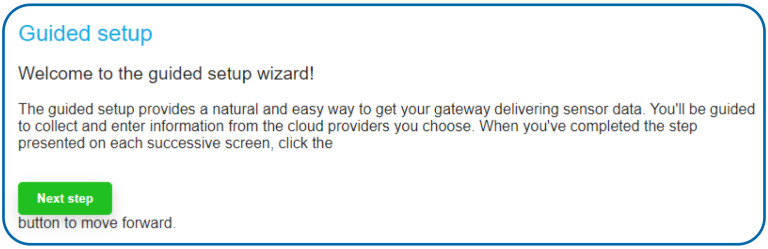
Set Authentication Token

You do not have a password set. Please set one now.

Figure 10

Go ahead and enter a password. You can change it later if needed. Please use a password with sufficient length and characters to give you the protection you need against unauthorized access, but keep in mind you'll have to remember it to avoid having to do a factory reset and re-configuring the Gateway entirely.

The Guided Setup begins with a page that looks like this:



Guided setup

Welcome to the guided setup wizard!

The guided setup provides a natural and easy way to get your gateway delivering sensor data. You'll be guided to collect and enter information from the cloud providers you choose. When you've completed the step presented on each successive screen, click the

button to move forward.

Figure 11

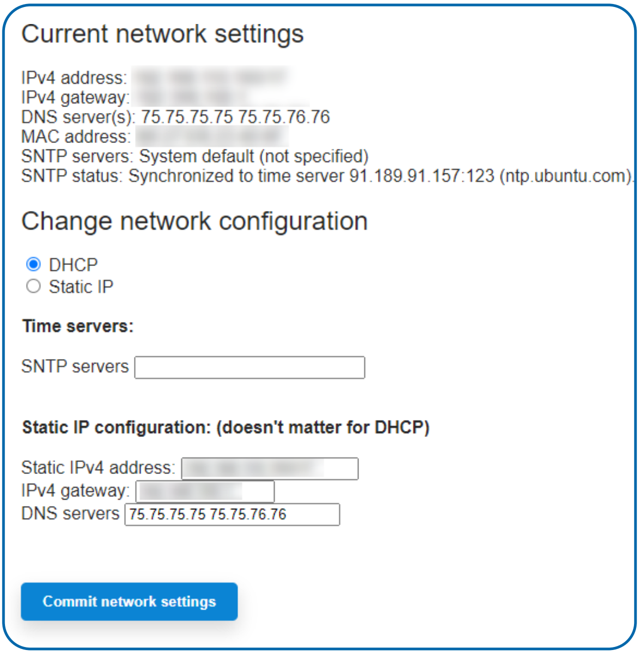
All the pages in the Guided Setup are available later, most through the gateway Setup/Monitoring page, as needed. The Guided Setup walks you through various items of configuration, step-by-step, giving you explanations and avoiding having anything missed.

Each step in the Guided Setup has two simple elements. The first element is the content of the step, as it appears elsewhere in the standard pageworks, enclosed in a box. The second element is the green "next" button to go to the next step. Setup of a Gateway is better accomplished by finishing each step before moving to the next.

The content of the pages displayed in the Guided Setup is substantially the same as if reached through the non-guided links, which will be described further below.

CURRENT NETWORK SETTINGS

It is critical that the Gateway has proper network settings. Otherwise, the gateway may fail to connect to the cloud or to synchronize the time. The network settings page on the browser interface appears like this:



Current network settings

IPv4 address: [redacted]
IPv4 gateway: [redacted]
DNS server(s): 75.75.75.75 75.75.76.76
MAC address: [redacted]
SNTP servers: System default (not specified)
SNTP status: Synchronized to time server 91.189.91.157:123 (ntp.ubuntu.com).

Change network configuration

● DHCP
○ Static IP

Time servers:

SNTP servers

Static IP configuration: (doesn't matter for DHCP)

Static IPv4 address: [redacted]
IPv4 gateway: [redacted]
DNS servers 75.75.75.75 75.75.76.76

Figure 12

It is usually most convenient to use DHCP. In this way the Gateway will acquire a valid IP address, DNS servers and other network settings from a DHCP router. The current settings are displayed on this page.

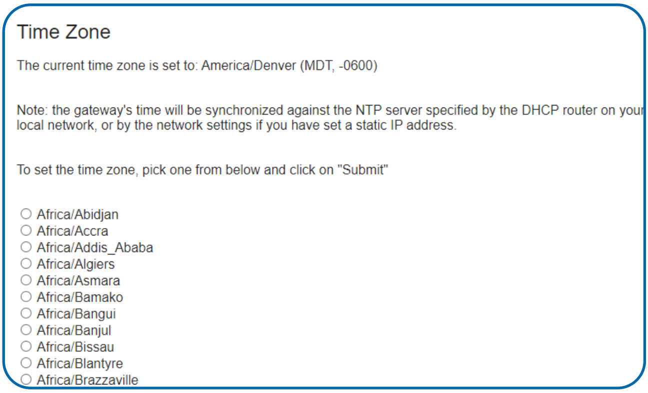
For those who wish the Gateway to have a set static IP address, entry fields are provided. After selecting "Static IP", entering the address, the LAN gateway, the DNS and SNTP servers and clicking the "Commit network settings" button, the gateway will change to those settings. After clicking the button, your browser may send HTTP requests to the previous IP address, and complain that the server is unavailable. The solution is to wait about a minute, then navigate back to the head address at http://aegw-{Device-ID}.local as described above. The Gateway will have announced itself at the new IP address over mDNS, and you will likely connect fine. (Restarting your browser may help as well.)

As explained in the next section, it is very important for the Gateway to have good time. There must be SNTP servers that can be reached.

TIME AND SETTING THE TIME ZONE

Because reports from sensors are indexed by time, it is very important for the Gateway to have current time. The Gateway does not have a real-time hardware clock, so in operation the Gateway synchronizes its clock to the SNTP server(s) specified in the Network Settings when it boots. When the gateway's clock is current, the clocks on the sensors are then synchronized as they open wireless sessions with the gateway. The gateway will not communicate with sensors until it has synchronized with at least one time server. (This will not generally result in data loss, because the sensors continue to maintain their internal clocks. The sensors will deliver logged reports when contact is resumed with the Gateway.)

In usual fashion, the clock of the gateway is kept synchronized to UTC. You may wish to have reports delivered with time referenced in a zone of your choosing. That is easy to set on the Time Zone page pictured in Figure 13:



Time Zone

The current time zone is set to: America/Denver (MDT, -0600)

Note: the gateway's time will be synchronized against the NTP server specified by the DHCP router on your local network, or by the network settings if you have set a static IP address.

To set the time zone, pick one from below and click on "Submit"

○ Africa/Abidjan
○ Africa/Accra
○ Africa/Addis_Ababa
○ Africa/Algiers
○ Africa/Asmara
○ Africa/Bamako
○ Africa/Bangui
○ Africa/Banjul
○ Africa/Bissau
○ Africa/Blantyre
○ Africa/Brazzaville

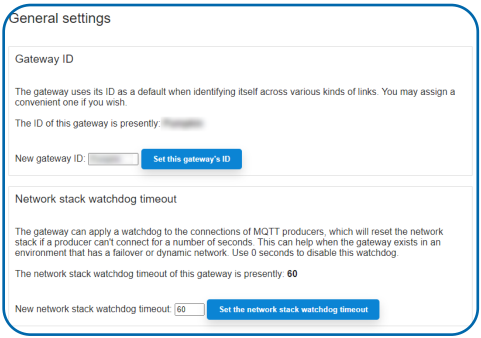
Figure 13

The selection of time zone takes effect immediately.

GENERAL SETTINGS

There are two settings to discuss on this page. They are the Gateway ID and the Network Stack Watchdog Timeout.

You may assign any string to be the ID of the gateway, as reported in the outgoing traffic to the cloud when the $G macro is used. If an ID is not set, the gateway will use "unassigned". In this way a consumer can correlate sensor data and the gateway through which it passed.



General settings

Gateway ID

The gateway uses its ID as a default when identifying itself across various kinds of links. You may assign a convenient one if you wish.

The ID of this gateway is presently: [redacted]

New gateway ID: [redacted]

Network stack watchdog timeout

The gateway can apply a watchdog to the connections of MQTT producers, which will reset the network stack if a producer can't connect for a number of seconds. This can help when the gateway exists in an environment that has a failover or dynamic network. Use 0 seconds to disable this watchdog.

The network stack watchdog timeout of this gateway is presently: **60**

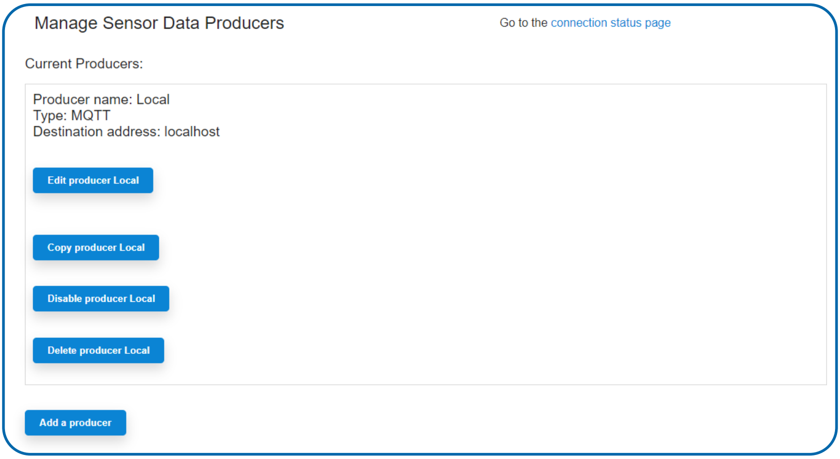
New network stack watchdog timeout: 60

Figure 14

The Network Stack Watchdog Timeout setting is provided for customers having gateways installed on unstable networks, e.g. those served by more than one DHCP server. Setting this value to 0 will turn it off. Otherwise, to use it, specify a number of seconds before the network stack is to be reset after a prolonged loss-of-contact with the cloud. When the network stack is reset, the gateway will seek the acquisition of a new DHCP lease, containing proper settings for DNS, SNTP and gateway IP address. The firing of this timer will cause minor interruption network connectivity (most likely less than a few seconds), so it is recommended generally to leave it set somewhere between 60 to 600 seconds (one to ten minutes).

MANAGING SENSOR DATA PROCEDURES

Sensor data is transmitted to the cloud by way of one or more producers that you specify. Each producer defines an MQTT client that connects and sends data to one destination using an individual format, topics and other potential settings. This part of the user interface is more complex than a simple form, due to the differences between the cloud providers, so a questionaire format is used. The image below is representative of the Manage Sensor Data Producers page.



Manage Sensor Data Producers

Go to the connection status page

Current Producers:

Producer name: Local
Type: MQTT
Destination address: localhost

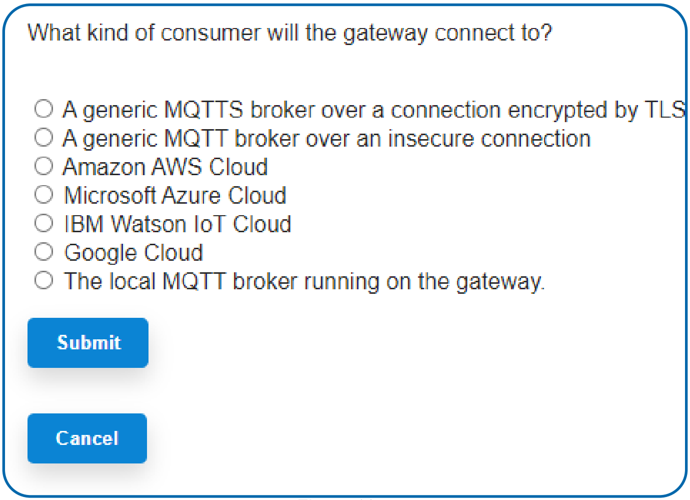
Figure 15

Here is a list of configured producers on the Gateway. Each producer has a button to edit, disable, enable, copy or delete it.

Producers can be enabled and disabled. Disabled producers are inactive, and don't connect. When a producer is first created it will be disabled. When its settings look correct, enable it to try it out with its particular cloud or MQTT broker.

Copying a producer can be very helpful, in a case where you have difficulty getting or keeping a connection up. You can start with one you know that works (for example to the local MQTT broker on the gateway), making incremental changes toward a working setup on another connection. It is also useful when you're changing message formats, creating a revisioned configuration (disabling the ones not current).

After clicking on the "Add a producer" button, you will see a page that looks like Figure 16:

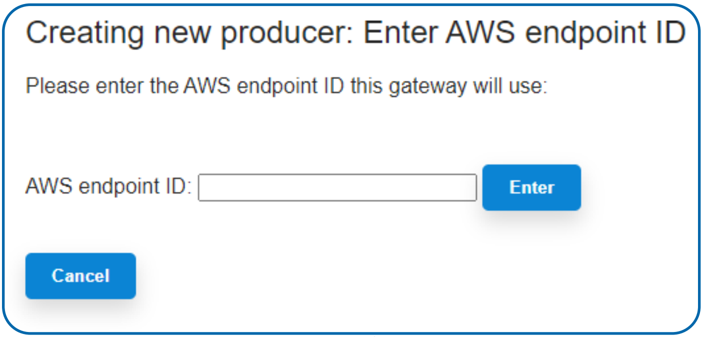


What kind of consumer will the gateway connect to?

○ A generic MQTTS broker over a connection encrypted by TLS
○ A generic MQTT broker over an insecure connection
○ Amazon AWS Cloud
○ Microsoft Azure Cloud
○ IBM Watson IoT Cloud
○ Google Cloud
○ The local MQTT broker running on the gateway.

Figure 16

The gateway provides successive dialogs in the questionaire, depending upon which kind of connection is to be made. For example, if you were to select Amazon AWS Cloud and click on "Submit", the next page would be:



Creating new producer: Enter AWS endpoint ID

Please enter the AWS endpoint ID this gateway will use:

AWS endpoint ID:

Figure 17

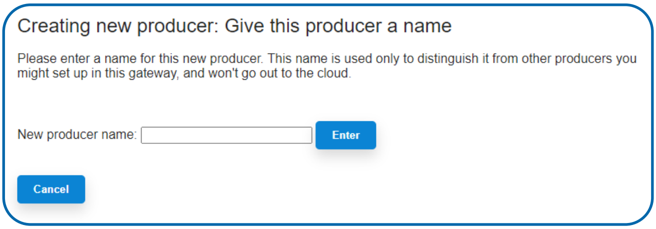
Successive pages would ask for the remaining information needed to set up a connection to your account in the AWS Cloud.

It isn't necessary to describe all the items in the dialogs and questionaires here. When you have entered the needed information, you will see a page with all resulting settings. Clicking on "Save this producer" commits it to the list, but disabled so you have a chance to make final edits without it connecting or sending erroneous messages. When it looks right, go to the list and enable the producer.

VII. EXAMPLE: MAKING AND TESTING A PRODUCER TO THE GATEWAY'S LOCAL MQTT BROKER

One of the quickest ways of testing a producer configuration and to get a feel for how the producers operate, is to create a test producer that publishes messages on the gateway's MQTT broker. This section will teach how to do that, and how to monitor the health of the connection.

The first steps are to click on the "Add a producer button", then select "The local MQTT broker running on the gateway". This is the following page:



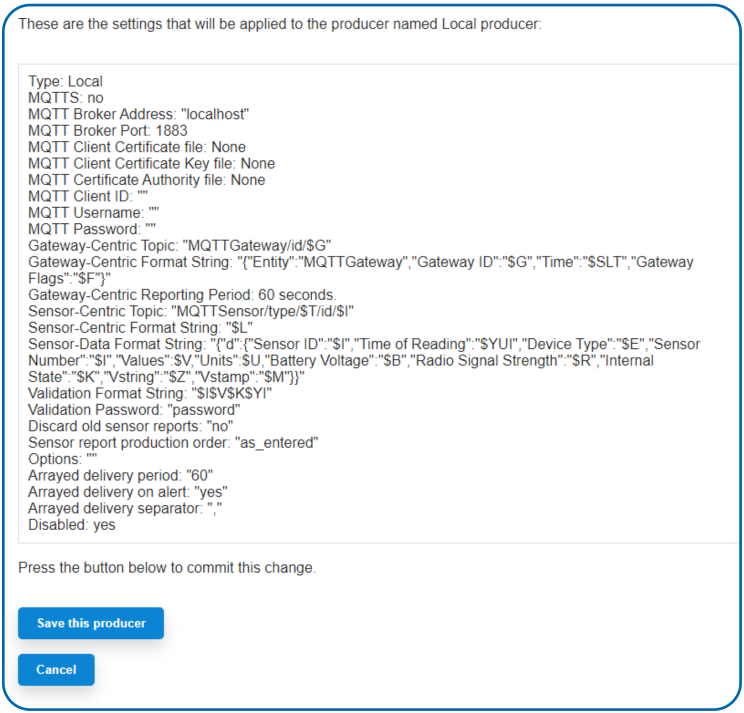
Creating new producer: Give this producer a name

Please enter a name for this new producer. This name is used only to distinguish it from other producers you might set up in this gateway, and won't go out to the cloud.

New producer name:

Figure 18

You can use virtually any name you wish. For the purposes of this example, we'll enter "Local producer" in this field and then click "Enter". That results in the gateway populating the configuration of an MQTT producer with some defaults, and showing it to you like so:



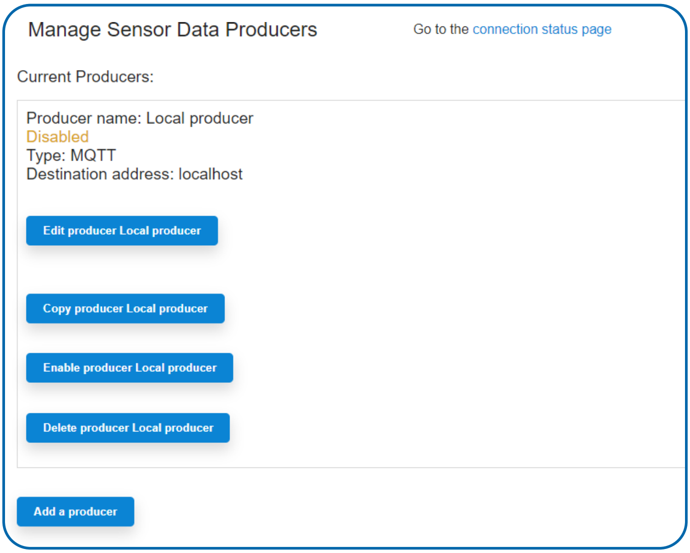
These are the settings that will be applied to the producer named Local producer:

```
Type: Local
MQTTS: no
MQTT Broker Address: "localhost"
MQTT Broker Port: 1883
MQTT Client Certificate file: None
MQTT Client Certificate Key file: None
MQTT Certificate Authority file: None
MQTT Client ID: ""
MQTT Username: ""
MQTT Password: ""
Gateway-Centric Topic: "MQTTGateway/id/$G"
Gateway-Centric Format String: "{"Entity":"MQTTGateway","Gateway ID":"$G","Time":"$SLT","Gateway
Flags":"$F"}"
Gateway-Centric Reporting Period: 60 seconds.
Sensor-Centric Topic: "MQTTSensor/type/$T/id/$I"
Sensor-Centric Format String: "$L"
Sensor-Data Format String: "{"d":{"Sensor ID":"$I","Time of Reading":"$YUI","Device Type":"$E","Sensor
Number":"$I","Values":$V,"Units":$U,"Battery Voltage":"$B","Radio Signal Strength":"$R","Internal
State":"$K","Vstring":"$Z","Vstamp":"$M"}}"
Validation Format String: "$I$V$K$YI"
Validation Password: "password"
Discard old sensor reports: "no"
Sensor report production order: "as_entered"
Options: ""
Arrayed delivery period: "60"
Arrayed delivery on alert: "yes"
Arrayed delivery separator: ","
Disabled: yes
```

Press the button below to commit this change.

Figure 19

As you can see, there are many fields that are empty. These configuration settings are described under "Options available for MQTT producers" under "Developer notes" on the index page, and will not be further described here. Just click on "Save this producer", and the example producer will be populated in the list:



Manage Sensor Data Producers

Go to the connection status page

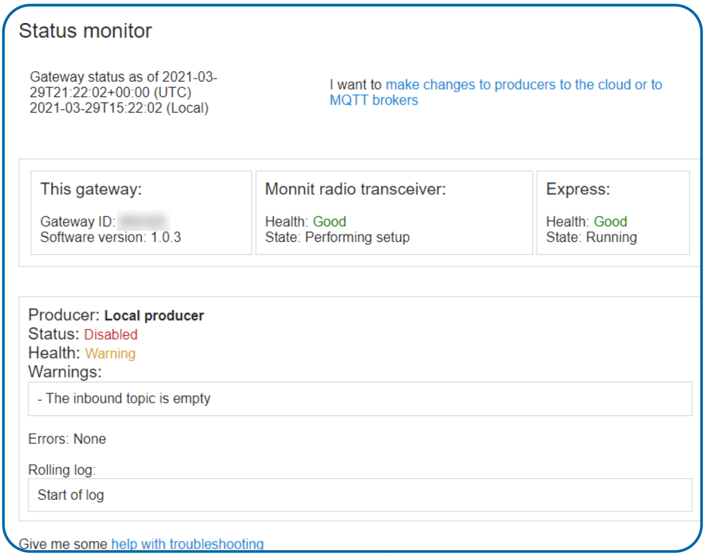
Current Producers:

Producer name: Local producer
Disabled
Type: MQTT
Destination address: localhost

Edit producer Local producer
Copy producer Local producer
Enable producer Local producer
Delete producer Local producer
Add a producer

Figure 20

Now, click on the "Go to the connection status page" at the top. You should be met with a page showing the status of all the existing producers. See Figure 21:



Status monitor

Gateway status as of 2021-03-29T21:22:02+00:00 (UTC)
2021-03-29T15:22:02 (Local)

I want to make changes to producers to the cloud or to MQTT brokers

This gateway:
Gateway ID: [redacted]
Software version: 1.0.3

Monnit radio transceiver:
Health: Good
State: Performing setup

Express:
Health: Good
State: Running

Producer: **Local producer**
Status: Disabled
Health: Warning
Warnings:
- The inbound topic is empty

Errors: None

Rolling log:

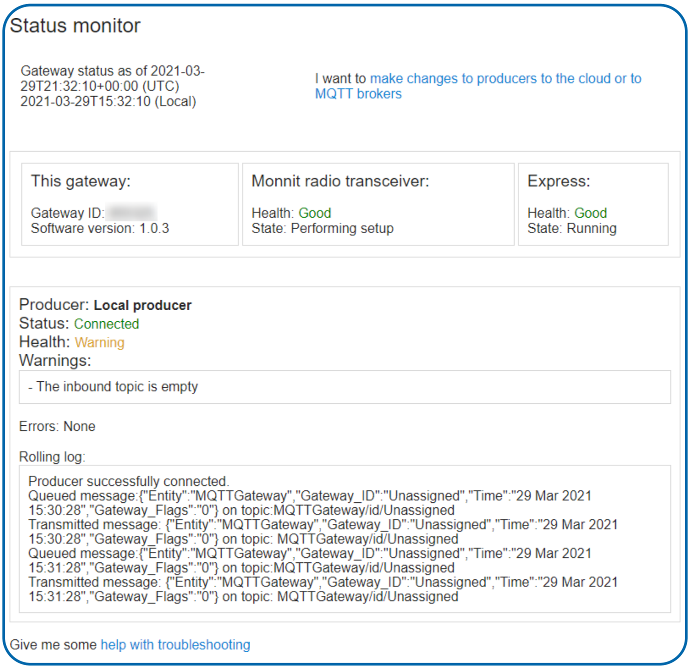
Start of log

Give me some help with troubleshooting

Figure 21

This page shows the status of several things, including the link to the radio transceiver, the link to Express Core, and the status of your new producer, which is "disabled". A disabled producer doesn't connect, and doesn't send any messages. Let's enable it so we can see something happening. Click on "I want to make changes to producers to the cloud or to MQTT brokers". You'll see the list of producers again. This time, in the box with the "Producer name: Local Producer", click "Enable producer Local producer". On the next screen click "Confirm enable". Then click on "Return to Manage delivery to the cloud or to MQTT brokers".

And there is the list of producers again, but with the "enable" button replaced with "disable" for the Local producer. Now click on "Go to the connection status page" again. You will then see something like Figure 22:



Status monitor

Gateway status as of 2021-03-29T21:32:10+00:00 (UTC)
2021-03-29T15:32:10 (Local)

I want to make changes to producers to the cloud or to MQTT brokers

This gateway:

Gateway ID: [redacted]
Software version: 1.0.3

Monnit radio transceiver:

Health: Good
State: Performing setup

Express:

Health: Good
State: Running

Producer: **Local producer**
Status: Connected
Health: Warning
Warnings:

- The inbound topic is empty

Errors: None

Rolling log:

```
Producer successfully connected.
Queued message:{"Entity":"MQTTGateway","Gateway_ID":"Unassigned","Time":"29 Mar 2021
15:30:28","Gateway_Flags":"0"} on topic:MQTTGateway/id/Unassigned
Transmitted message: {"Entity":"MQTTGateway","Gateway_ID":"Unassigned","Time":"29 Mar 2021
15:30:28","Gateway_Flags":"0"} on topic: MQTTGateway/id/Unassigned
Queued message:{"Entity":"MQTTGateway","Gateway_ID":"Unassigned","Time":"29 Mar 2021
15:31:28","Gateway_Flags":"0"} on topic:MQTTGateway/id/Unassigned
Transmitted message: {"Entity":"MQTTGateway","Gateway_ID":"Unassigned","Time":"29 Mar 2021
15:31:28","Gateway_Flags":"0"} on topic: MQTTGateway/id/Unassigned
```

Give me some help with troubleshooting

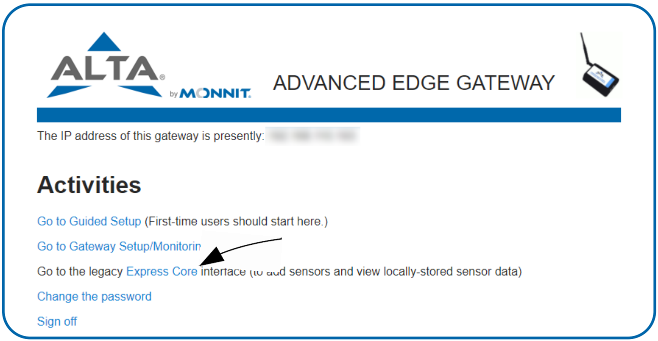
Figure 22

Now the status is "Connected". Further, in the producer's Rolling Log you can see that the producer successfully connected, and is queuing and transmitting messages to the broker. These messages are gateway-centric messages, sent out periodically, containing only information about the gateway and not about sensors. These messages provide a convenient way to monitor the state of the connection. Here we can tell the connection is very healthy: each queued message is immediately transmitted to the broker. When messages are queued but not transmitted, it means the gateway is trying to transmit them, but has not yet done so successfully.

Seeing that message are flowing, now is a good time to add sensors so we can see what sensor reports look like.

VIII. ADDING AND CONFIGURING SENSORS

Return to the index page of the browser interface, located at **https://aegw-{Device-ID).local.** Choose "Express Core" in the third Activity.



The IP address of this gateway is presently: [redacted]

Activities

Go to Guided Setup (First-time users should start here.)

Go to Gateway Setup/Monitorin

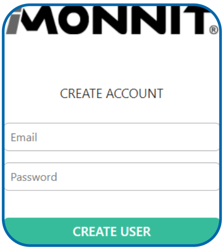
Go to the legacy Express Core interface (to add sensors and view locally-stored sensor data)

Change the password

Sign off

Figure 23

That will deliver you to the create account page for Express Core:



CREATE ACCOUNT

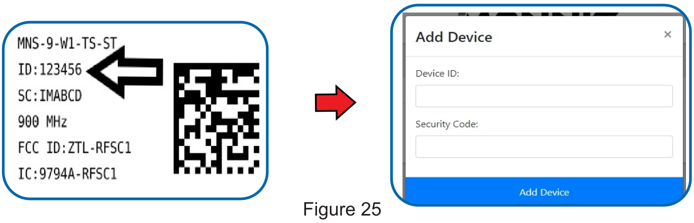
Email

Password

Figure 24

Enter an email and a password for the account, then click the **Create** button. The page will refresh and prompt you to log in with the email and password combination for the first time. You will need to accept the gateway’s SSL certificate to access the interface.

Sensors can be added by first opening the sensor page by selecting “Sensors” from the main navigation menu, then clicking the **Add Sensor** button. A box will pop-up prompting the entry of the Device ID and Security Code. These can be found on the label of your device. On sensors, this label is typically located on the side of the device. The **Device ID** consists of numbers. The **Security Code** is a set of six capital letters.



MNS-9-W1-TS-ST
ID:123456
SC:IMABCD
900 MHz
FCC ID:ZTL-RFSC1
IC:9794A-RFSC1

Add Device

Device ID:

Security Code:

Figure 25

After clicking on the "Add Device" button, the sensor will appear on the list appearing on the Sensors Page. Selecting a sensor from the list will open a page with the current readings of the sensor. You may then adjust the settings for a sensor by clicking the "Sensor Edit" button:

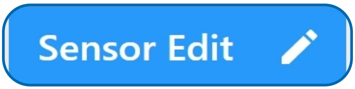


Figure 26

A page to modify the operational settings for the sensor will load. Be sure to choose the **Save** button after making any changes. Consult the user guides or video tutorials for that sensor type to understand the available settings.

Changes to the sensor list take effect within 30 seconds at the gateway. Changes to sensor configuration can take much longer, depending upon when a sensor opens a new session on its heartbeat with the gateway. To force a new session and cause sensor configuration to take immediately, you can cycle the power on that sensor, after 30 seconds have passed after clicking the Save button.

Once the sensor list has been updated and the sensor is transmitting data to the gateway, sensor-centric messages will be sent as directed by these settings, specific to each individual producer:

1. The sensor-centric format string
2. The sensor data format string, and
3. The sensor-centric topic.

A description of the operation of these is found at:
https://aegw-{Device-ID}.local/using_format_strings.

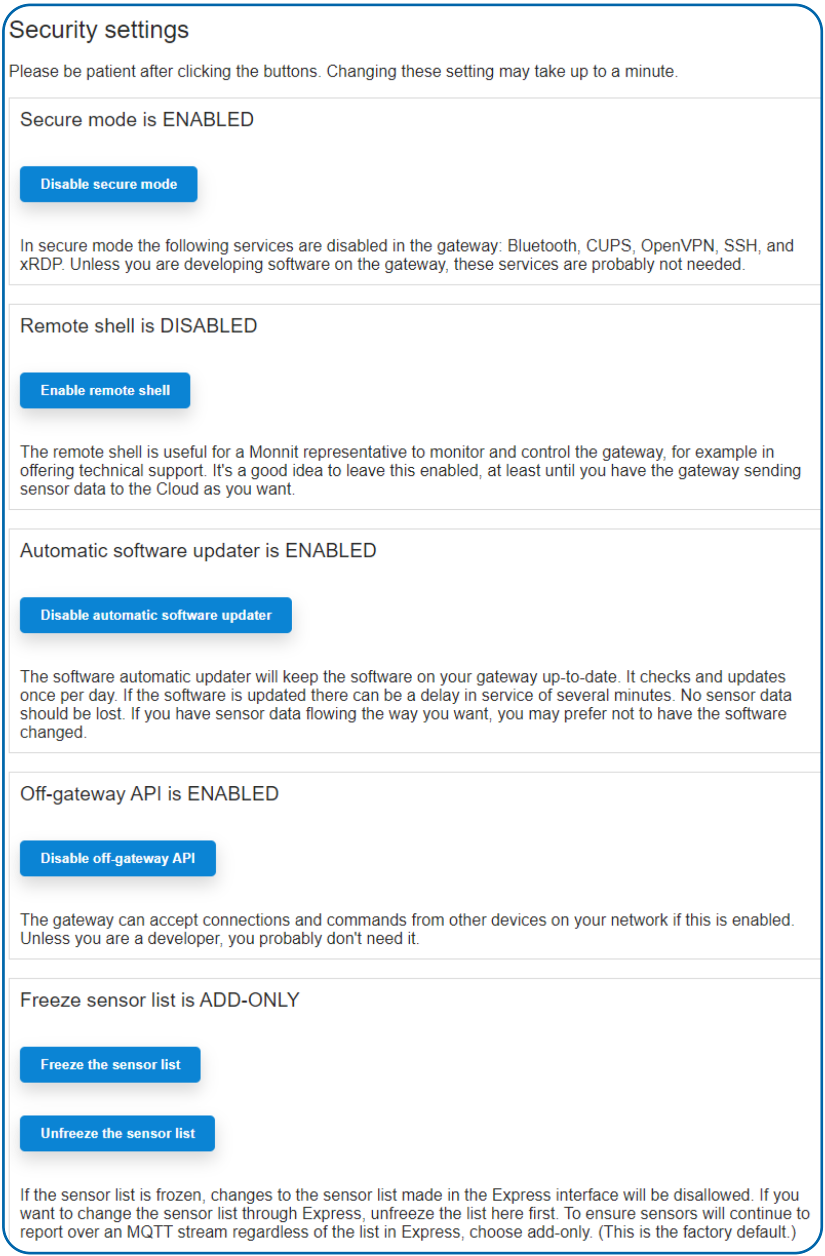
SENSOR SECURITY

The ALTA Advanced Edge Gateway has been designed and built to securely manage data from sensors monitoring your environment and equipment. 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.

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.

IX. GATEWAY SECURITY

The settings for security on the Gateway are traveled to by clicking on "Settings for security and control" on the index screen. This is what you will see, if the gateway is in its factory-reset state:



Security settings

Please be patient after clicking the buttons. Changing these setting may take up to a minute.

Secure mode is ENABLED

In secure mode the following services are disabled in the gateway: Bluetooth, CUPS, OpenVPN, SSH, and xRDP. Unless you are developing software on the gateway, these services are probably not needed.

Remote shell is DISABLED

The remote shell is useful for a Monnit representative to monitor and control the gateway, for example in offering technical support. It's a good idea to leave this enabled, at least until you have the gateway sending sensor data to the Cloud as you want.

Automatic software updater is ENABLED

The software automatic updater will keep the software on your gateway up-to-date. It checks and updates once per day. If the software is updated there can be a delay in service of several minutes. No sensor data should be lost. If you have sensor data flowing the way you want, you may prefer not to have the software changed.

Off-gateway API is ENABLED

The gateway can accept connections and commands from other devices on your network if this is enabled. Unless you are a developer, you probably don't need it.

Freeze sensor list is ADD-ONLY

If the sensor list is frozen, changes to the sensor list made in the Express interface will be disallowed. If you want to change the sensor list through Express, unfreeze the list here first. To ensure sensors will continue to report over an MQTT stream regardless of the list in Express, choose add-only. (This is the factory default.)

Figure 27

These settings on the Security Settings page are described there, with these brief additional comments:

For secure mode, the remote shell, and the automatic software updater:

When you get the gateway delivering data to the cloud the way that you want, you may wish to adjust these to lock down your gateway against potential intrusions and changes that could be made.

Likewise for the off-gateway API: if you're not using it, it's safe to turn it off. (If you don't know what it is, you're not using it.)

The factory-condition of the freeze sensor list setting is "add-only", meaning that from Express Core or a Monnit Server, you can only add to the gateway's sensor list. You can also freeze this list allowing no changes. Setting this to "not frozen" will allow both additions and deletions.

X. FURTHER ON-GATEWAY DOCUMENTATION

This User Guide provides information sufficient for an average user of the Edge Gateway to make connections and sent sensor data to the cloud, or an MQTT(S) broker, mainly using default settings. More instructional material is available in the browser interface, at the index page under "Developer notes". Subjects covered there include the specification of format strings to customize messages into the cloud, and controlling the order of delivery of logged sensor data after a network interruption.

Please also note that there are step-by-step guides there for connections to the major cloud providers. Look under "Set up and troubleshoot connections to the cloud", at the bottom. If you are having trouble making a connection to the cloud, these are very helpful.

ALTA Advanced Edge Gateway Specifications

Models	
Ethernet	MNG2-9-EDG-CCE
Processor	
CPU	Cortex-A53
RAM	1 GB LPDDR2 SDRAM
Disk	16 GB
Operating System	Ubuntu Linux
Power	
Input Power	5.0 VDC @ 2.5 A
Max Rated Input Power	5.5 VDC
Mechanical	
LEDs	Connectivity, Power, Cloud Services, Network Status
Enclosure	ABS
Dimensions	5.004 x 3.8 x 1.51 in.
Weight	7 ounces
Environmental	
Operating Temperature	0 to +50°C (32 to 122°F)
ALTA Wireless	
Transmit Power (EIRP)	50 mW (900 MHz), 25 mW (868 MHz), 10 mW (433 MHz)
Antenna Type	Connector: RPSMA Gain: 3.0 dBi
Wireless Range	1,200+ ft. non-line-of-sight *
Security	Encrypt-RF® (256-bit key exchange and AES-128 CBC)
Certifications Industry Canada	(Certifications Pending) RF: 900 MHz product includes model FCC ID: ZTL-G2SC1 / IC: 9794A-G2SC1 868 MHz product includes Module G2SC1 (IEC 300 220-1, -2); 433 MHz product includes Module G2SC2 (IEC 300 220-1,-2)

SUPPORT

For technical support and troubleshooting tips, please visit our support knowledge base 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 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 20 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)*

Monnit EGW4 cellular gateway models starting with MNG2-9-EGW-CCE and MNG2-9-EGW-CCE-POE also contain module: FCC ID: XPY2AGQN4NNN

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

- *3.67 dBi in 700 MHz, i.e. LTE FDD-12 band*
- *10 dBi in 850 MHz, i.e. LTE FDD-5 band*
- *6.74 dBi in 1700 MHz, i.e. LTE FDD-4 band*
- *7.12 dBi in 1900 MHz, i.e. LTE FDD-2 band*

Canada (IC)

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

The radio transmitters (IC: 9794A-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 licence-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 Èquivalente (P.I.R.È) 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: 8595A2AGQN4NNN) 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, méme 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: 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 commercialisation of Monnit and ALTA 868MHz and 433MHz wireless products in all the countries of the European Union.

⚠ **WARNING**: ISM and WCDMA/HSPA/GSM/GPRS/EDGE antennas are considered integral to the Monnit International Cellular Gateway and should remain fixed with 3 meters of the device during 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 European Community provides some Directives for the electronic equipment 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 telecommunication equipment is available, while the applicable Directives (Low Voltage and EMC) are available at: http://ec.europa.eu/enterprise/sectors/electrical

Additional Information and Support

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

MONNIT®

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

Change Log

Date	Change	Reason	Modified By
4/9/21	Change Log Created	Manager Request	Dillon F