



Remote Monitoring for Business



Wireless Control **USER GUIDE**

Table of Contents

I. ABOUT THE WIRELESS CONTROL UNIT	1
FEATURES	1
QUICK START GUIDE	1
II. ORDER OF OPERATIONS	2
III. PORTAL AND DEVICE SETUP	2
ADD DEVICE	2
SETUP	3
VALIDATION	3
ACTIONS	4
IV. USING THE WIRELESS CONTROL	4
LED INDICATORS	4
CONNECTING THE RELAYS	4
V. DEVICE OVERVIEW IN IMONNIT	5
MENU SYSTEM	5
DETAILS VIEW	5
CONTROL VIEW	6
READINGS VIEW	6
ACTIONS VIEW	8
SETTINGS VIEW	12
VI. DEVICE SPECIFICATIONS	13
VII. SECURITY	14
VIII. SUPPORT	16
IX. WARRANTY INFORMATION	16
X. CERTIFICATIONS	18
XI. SAFETY RECOMMENDATIONS	20

I. ABOUT THE WIRELESS CONTROL UNIT

The ALTA® Wireless Control Unit has two separate relays that react in response to either the iMonnit®.com web portal or a wireless sensor on the network. The relays are capable of automatically controlling motors, equipment or electrical devices. Monnit control is currently available in 10-amp or 30-amp versions (10-amp unit has two 10-amp relays and 30-amp unit has two 30-amp relays).

Four LED indicators let the user know if the device is powered on, communicating with the online system and the status of each relay.

The user can also manually turn a relay on or off through the iMonnit software. Manual changes can also be temporary based on a set duration (ex. activate the relay for 10 minutes then return to the default state).

Example Use: If a water sensor detects water at a certain level in a sump pit, the relay will switch ON, activating the pump. When water is no longer detected, the relay will switch OFF, deactivating the pump motor.

WIRELESS CONTROL UNIT FEATURES

- Allows for automated control.
- 10-amp or 30-amp units available.
- Two separate relays per unit.
- Can be triggered manually through online monitoring interface.
- AC powered, always on for immediate response from the Monnit wireless sensor network.

Note: The Wireless Control requires an ALTA Gateway to receive commands from wireless sensors as all commands are processed through the iMonnit online software.

WIRELESS CONTROL QUICK START

- Create an iMonnit user account and assign a wireless gateway and sensors.
- Assign the wireless control device to the sensor network.
- Connect control relay's to devices you wish to control.
- Plug the control device's power supply into a power outlet.
- Pair the control relays with wireless sensor's on the same sensor network.
- Set sensor conditions that will activate the relays.

IMPORTANT!

Disconnect all power to the control unit and the device to be controlled, before connecting the control relay wires.



II. ORDER OF OPERATIONS

It is important to understand the order of operations for activating your sensor. If performed out of sequence, your sensor may have trouble communicating with iMonnit. Please perform the steps below in the order indicated to make sure you are performing the setup correctly.

1. **Create an iMonnit account (If a new user).**
2. **Register all sensors and gateways to a network in iMonnit.**
Sensors can only communicate with gateways on the same iMonnit network.
3. **Connect/power on the gateway and wait until it checks into iMonnit.**
4. **Power on the sensor and verify it checks into iMonnit.**
We recommend powering the sensor on near the gateway then moving to the installation location, checking signal strength along the way.
5. **Configure the sensor for use. (This can be done at any point after step 2.)**
6. **Install the sensor in the final location.**

Note: For information on setting up iMonnit and the gateway refer to the [iMonnit user guide](#) and the [gateways user guide](#).

Note: Device specific setup is covered in more detail in the following [user guide sections](#).

III. PORTAL AND DEVICE SETUP

If this is your first time using iMonnit, you will need to create a new account. If you have already created an account, start by logging into iMonnit. For instructions on how to register and set up your iMonnit account, please consult the [iMonnit user guide](#).

STEP 1: ADD DEVICE

1. Add the sensor in iMonnit.

Add the sensor to your account iiby choosing [Sensors](#) in the main menu. Navigate to the [Add Sensor](#) button.

A blue rounded rectangular button with a white plus sign icon on the left and the text "Add Sensor" in white on the right.

Desktop



Mobile

2. Find the device ID. See Figure 1.

The Device ID (ID) and Security Code (SC) are necessary to add a sensor. These can both be located on the label on the side of your device.



Figure 1



3. Adding your device. See Figure 2.

You will need to enter the Device ID and the SC from the temperature sensor in the corresponding text boxes. Use the camera on your smartphone to scan the QR code on your device. If you do not have a camera on your phone, or the system is not accepting the QR code, you may enter the Device ID and SC manually.

- The Device ID is a unique number located on each device label.
- Next, you'll be asked to enter the SC from your device. An SC consists of letters and must be entered in upper case (no numbers). It can also be found on the barcode label of your device.



Figure 2

When completed, select the **Add Device** button

Power cycle your gateway to ensure that the gateway will recognize the control unit. Once the control unit has been added to your network and before connecting the relay wires to any equipment, power on the control unit. Check that the bottom two LED indicators are illuminated green.

STEP 2: SETUP

Select your use case. See Figure 3.

To get up and running fast, your temperature sensor comes with preset use cases. Choose from the list or create your own custom settings. You can see your readings displayed in Fahrenheit or Celsius, the heartbeat interval, and aware state settings (see page 9 for definitions).

Select the **Skip** button when completed.

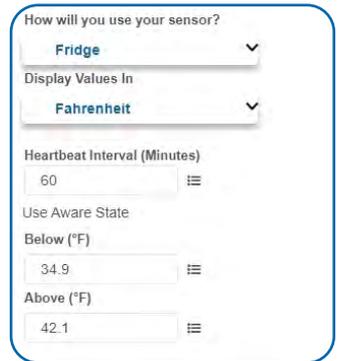


Figure 3

STEP 3: VALIDATION

Check your signal. See Figure 4.

The validation checklist will help ensure your sensor is communicating with the gateway properly and you have a strong signal.

Checkpoint 4 will only complete when your sensor achieves a solid connection to the gateway. Once you insert the batteries (or flip the switch on an industrial sensor) the sensor will communicate with the gateway every 30 seconds for the first few minutes.

Select the **Save** button when completed.

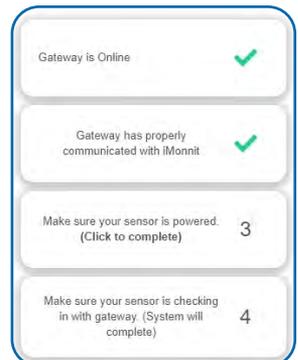


Figure 4



STEP 4: ACTIONS

Choose your Actions. See Figure 5.

Actions are the alerts that will be sent to your phone or email in the event of an emergency. Low battery life and device inactivity are two of the most common actions to have enabled on your device. See page 13 for how to set Actions for your sensor.

Select the **Done** button when completed.

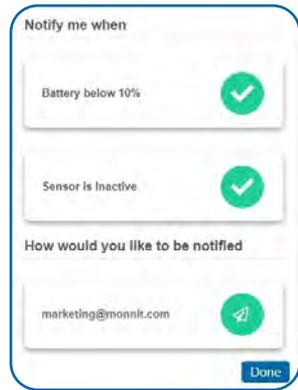


Figure 5

IV. USING THE WIRELESS CONTROL UNIT

WIRELESS CONTROL LED INDICATORS

The LED indicator lights on the Wireless Control Unit are the quickest way to see if your unit is functioning properly.

Relay 1 and 2

- A solid green light indicates the relay is “on” (closed.)
- No light is a signal that the relay is “off” (open.)

Radio

- Solid green indicates that the radio is active.
- A flashing light signals radio communication with a wireless gateway or sensor. This light will flash on every poll, corresponding to the set poll rate saved to the control unit in your iMonnit settings.

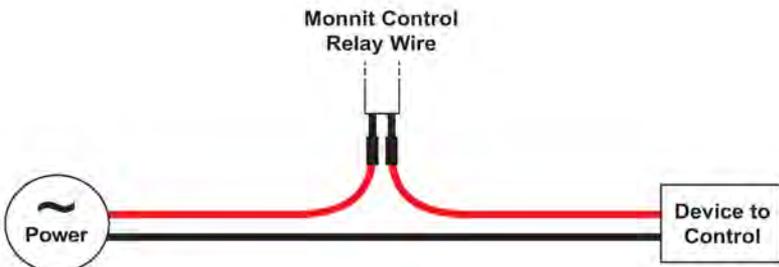
Power

A solid green light indicates the unit is receiving power.

CONNECTING THE RELAYS

The relay acts as a switch on the line for your power source. The relays are by default NORMALLY OPEN, so there is no connection (lights for the relays will be off to indicate this). See the edit page in iMonnit and adjust your relay settings if you wish for the default state to be NORMALLY CLOSED.

The relay is just allowing the current to pass through, so it will be installed inline on the power wire. It is not connected to power and ground.



V. DEVICE OVERVIEW IN iMONNIT

Select **Sensors** from the main navigation menu in iMonnit to access the **Sensor Overview** page and begin to configure the settings of the Temperature Sensor.

MENU SYSTEM



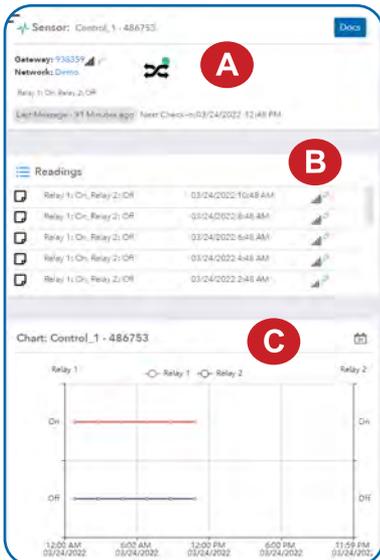
- A. Sensors** - List of all sensors on the network
- B. Control** - List of relay commands for the control unit to send.
- C. Details** - Displays a graph of recent sensor data
- D. Readings** - List of all past heartbeats and readings
- E. Actions** - List of all actions attached to the control unit
- F. Settings** - Editable levels for your control unit

Directly under the top horizontal tabbed menu bar is an overview of your device. You can see the signal strength of the selected device. A colored dot in the icon denotes its status.

- Green** indicates the sensor is checking in and is within user-defined safe parameters.
- Red** indicates the sensor has met or exceeded a user-defined threshold or triggered event.
- Gray** indicates that no sensor readings are being recorded, rendering the sensor inactive.
- Yellow** indicates that the sensor reading is outdated, due to perhaps a missed heartbeat check-in.

Details View

The Details View will be the first page you see upon selecting the control unit.



A. The **Sensor Overview** section is at the top of every page. This will consistently display the present reading, signal strength, battery level, and status.

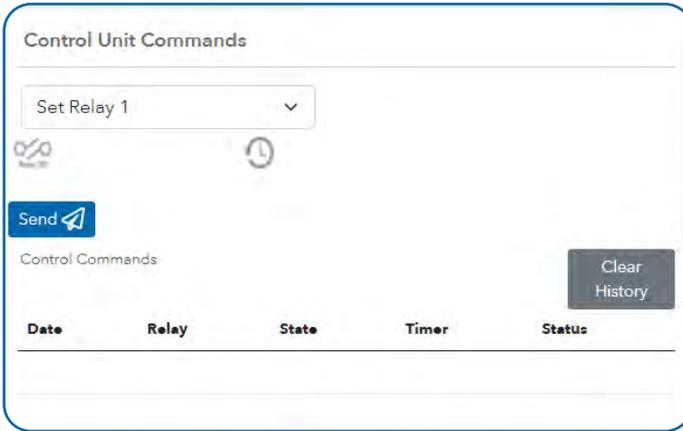
B. The **Readings** section shows the most recent data received by the sensor.

C. This graph charts any changes throughout a set date range. To change the date range displayed in the graph, navigate up to the top of the **Readings Chart** section on the right-hand corner to change the date range.



Control View

Control devices have two relays per device that are controlled separately. You can turn a relay on, off, or toggle the state. You can also set a duration by clicking on the timer icon. This will perform the selected toggle (on/off/toggle) for a set duration, then change back. To test the functionality of the relays when connected to equipment, go into the iMonnit portal, navigate to the "Control" tab:



Use the drop down to pick Relay 1 or 2 and select the relay icon to the right to toggle a state:

Turn the relay ON, (close it). The icon will turn **green**.

Turn the relay OFF (open it). The icon will turn **gray**. This is the default setting.

Choose the clock to set a duration time for the selected action to affect the relay, after which it will switch back. Note that time can be set in minutes but will display in the below table in seconds. If you want to simply switch the relay without a set time to switch back, leave the field empty. Press the "Send Control" button when finished.

Once the Send Control command is sent, it will take the combined time of the gateway poll interval OR heartbeat, if poll interval is not set plus the poll interval on the control unit to affect the relay. To speed up the process, force the gateway to communicate with the server and/or lower the poll rates.

Readings View

Select the **Readings** tab within the top horizontal menu bar to view the sensor's data history as time-stamped data.

- On the far right of the **Sensor History Data** is a cloud icon . Selecting this icon will export an Excel file of your sensor data into your downloads folder.

Note: Make sure you have the date range for the data you need input in the "From" and "To" text boxes. This will be the previous day by default. Only the first 2,500 entries in the selected date range will be exported.



The data file will have the following fields:

Message ID: Unique identifier of the message in the database.

Sensor ID: If multiple sensors are exported, you can distinguish between the sensors using this number — even if the names are the same.

Sensor Name: The name you gave the sensor.

Date: The date the message was transmitted from the sensor.

Value: Data presented with transformations applied, but without additional labels.

Formatted Value: Data transformed and presented as it is shown in the monitoring portal.

Raw Data: Raw data as it is stored from the sensor.

Sensor State: Binary field represented as an integer containing information about the state of the sensor when the message was transmitted. (See “*Sensor State*” explained below.)

Alert Sent: Boolean indicating if this reading triggered a notification sent from the system.

Sensor State

The value presented here is generated from a single byte of stored data. A byte consists of eight bits of data that we read as Boolean (True (1) / False (0)) fields.

When broken into individual bits, the State byte contains the following information:

aaaabcde

STS: This value is specific to the sensor profile and is often used to indicate error states and other sensor conditions.

UNUSED: This sensor does not use these bits.

AWARE: Sensors become aware when critical sensor-specific conditions are met. Going aware can cause the sensor to trigger and report before the heartbeat and cause the gateway to forward the data to the server immediately, resulting in near immediate transmission of the data.

TEST: This bit is active when the sensor is first powered on or reset and remains active for the first nine messages when using default configurations.

STS Specific Codes:

0 = No problems, sensor is functioning normally.

1 = Open circuit detected in lead.

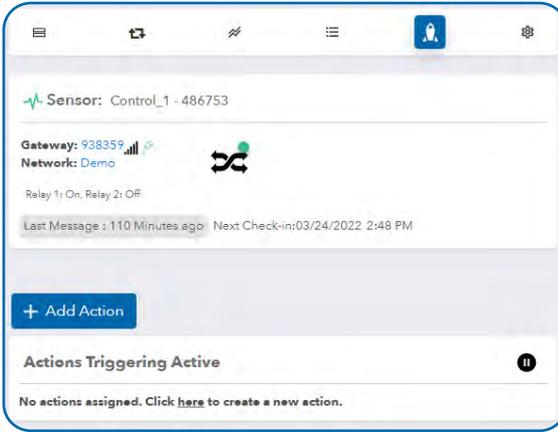
2 = Short circuit detected in lead.

3 = Range error. Temperature reads outside of -40° F and 257° F (-40° C and 125° C).



Actions View

From the **Actions** tab, you can Pause or Delay current triggers for the Wireless Control Unit.



A. Pause events by selecting this button. The chosen event will be paused indefinitely. It can be ended by picking the “Unpause” button.

B. Put events on a one-hour time delay by choosing the “1 Hour” button. It can be ended by selecting the “Unpause” button.

C. Alternatively, you can toggle an event off and on by dragging the switch left to right.

Creating an Action

Actions are triggers or alarms set to let you know when a sensor reading identifies that immediate attention is needed. Types of events include sensor readings, battery level, device inactivity, and scheduled data. Any one of these can be set to send a notification or trigger an action in the system. This guide will walk you through creating two types of events. First a sensor reading notification for a temperature sensor, then an inactivity notification configured for all sensors.

1. Choose **Actions** in the main navigation menu.



2. A list of previously created Actions will display on the screen. From here, you have the ability to filter, refresh, and add new Actions to the list.

Note: If this is your first time adding an Action, the screen will be blank.



3. From the **Actions** page, tap **Add Action** in the lower right-hand corner.



4. Select your trigger

The drop-down menu will have the following options for Action Types

- **Sensor Reading:** Set Actions based on activity or reading.
- **Device Inactivity:** Actions when the device doesn't communicate for an extended period of time.
- **Battery Level:** This is where you can set to be notified when the battery level drops below a percentage. 15% is the default setting.
- **Advanced:** Actions based on advanced rules, such as comparing past data points with current ones.
- **Scheduled:** These Actions are performed at a set time basis.

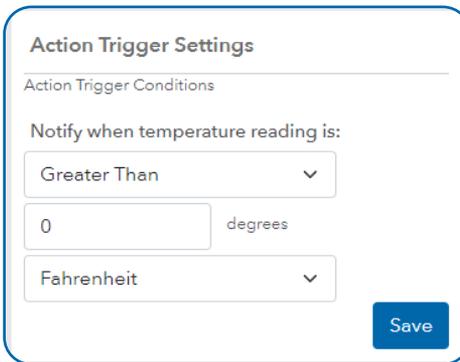


5. Select **Sensor Reading** from the drop-down menu.

6. A second drop-down menu will appear. From here, you will be able to see a list of the different type of sensors registered to your account. Choose **Temperature** in the drop-down menu.

7. Next, you will be asked to input the trigger settings. You have the option of setting this trigger for greater than or less than a temperature reading

8. Press the "Save" button.



Note: If you don't have a temperature sensor, the option in this example won't be available, select any variable output sensor and follow along.

Variable output sensors can have multiple event triggers created.

Example: A temperature sensor used in a freezer. You may want to be notified if the temperature goes below 0° or above 30° Fahrenheit. You would create two events.

- Event 1- Trigger Set for temperatures LESS THAN 0°F.
- Event 2 - Trigger set for temperatures GREATER THAN 30° F.



8. On the next screen select **Use Control Unit**.

9. Choose which relay you would like to use by clicking the icon on the left.

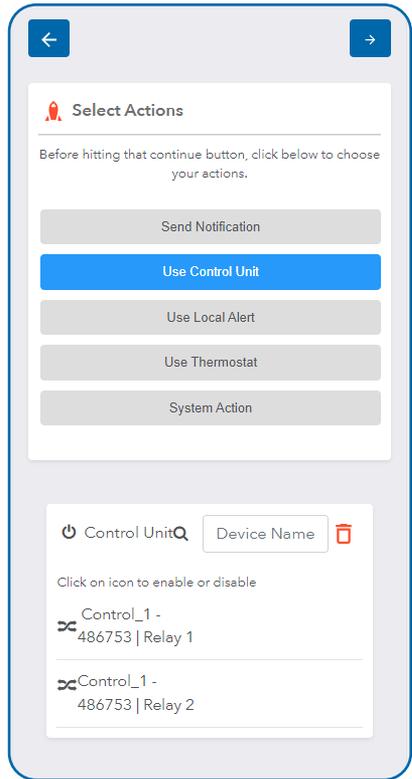


Relay off



Relay on

10. Select the right blue arrow to continue.

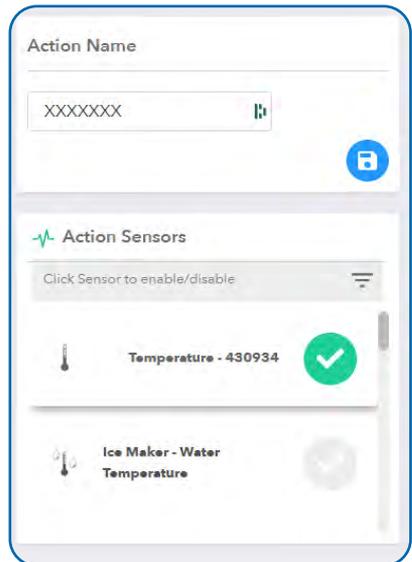


11. Name your action.

12. By default, the sensor(s) will not be assigned to the Action conditions you've just set. To assign a sensor, find the device(s) you want to designate for this Action and select. Selected sensor boxes will turn green when activated. Choose the sensor box again to unassign the sensor from the Action.

Continue toggling the sensor(s) corresponding to this new Action until you are satisfied with your selection. These can be adjusted later by returning to this page.

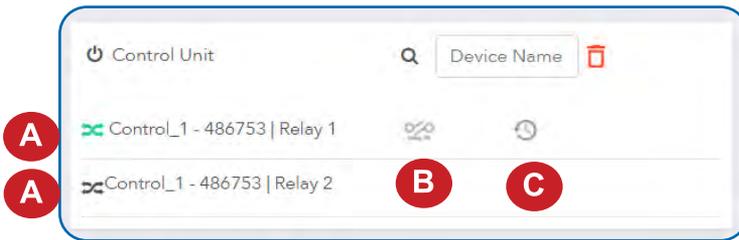
Press the **Save Icon** button to complete the process.



13. The **Action** Information page has a series of tabs across the top.



- A. Sensors:** A table of all past alert notifications for this specific event.
- B. History:** A table of all past alert notifications for this specific event.
- C. Trigger:** This is where you can review your trigger settings.
- D. Actions:** Where you set the action you want to happen when an alert state is triggered.
- E. Schedule:** Here you can schedule the event only to be active at certain times or certain days.



14. On the action information page you can toggle the on/off state of each relay (A) (B) is where you set the beginning state of each relay. **ON, OFF, OR TOGGLE.** (C) allows you to set a timer in minutes and seconds



Settings View

To edit the operational settings for the Wireless Control Unit, choose the “**Settings**” tab to access the configuration page.

The screenshot shows the 'Control_1 Settings' page. It contains the following fields and callouts:

- Sensor Name:** A text input field containing 'Control_1 - 486753'. Callout **A** points to this field.
- Heartbeat Interval (Minutes):** A text input field containing '120'. Callout **B** points to this field.
- Poll Interval:** A text input field containing '1'. Callout **C** points to this field.
- Failed transmissions before link mode:** A text input field containing '3'. Callout **D** points to this field.
- Relay 1:**
 - Relay 1 Title:** A text input field containing 'Relay 1'. Callout **E** points to this field.
 - Default State:** A toggle switch currently set to 'Off'. Callout **F** points to this toggle.
- Relay 2:**
 - Relay 2 Visible:** A toggle switch currently set to 'Show'. Callout **G** points to this toggle.
 - Relay 2 Title:** A text input field containing 'Relay 2'. Callout **H** points to this field.
 - Default State:** A toggle switch currently set to 'Off'. Callout **I** points to this toggle.

A. The **Sensor Name** is a unique name you give the sensor to easily identify it in a list and in any notifications.

B. The **Heartbeat Interval** is how often the sensor communicates with the gateway if no activity is recorded.

C. The **Poll Interval** allows a Monnit Control to check-in with the gateway for incoming control messages more frequently than the configurable heartbeat. This allows more timely action without generating multiple repeated data messages as a faster heartbeat would. Your gateway has a similar configuration to facilitate retrieving timely control messages from the server.

D. **Failed Transmissions Before Link Mode** this is the number of times unsuccessful communication between the Wireless Control Unit and the gateway can be attempted before the unit enters link mode. Link Mode is when the control unit starts going channel by channel trying to send a message to the gateway. This scan-cycle takes about 30 seconds. If all available channels have been tried and there is still no connection, no data will be sent for two hours.

E. **Relay Title** is where you can assign a name to the relay, just like the Sensor Name field above. The default name will be Relay 1 or Relay 2.

F. **Default State** is where you assign the open or closed state as the default setting for the relay so it can be adjusted in the Control tab. **“Off” is open. “On” is closed.** The control device will listen for messages from the iMonnit software via a Monnit wireless gateway, if a sensor reading meets the “Aware” state conditions, the control relay will automatically switch to the non-default state. When the sensor reports a reading outside of the “Aware” state conditions, the relay will switch back to its default state.

G. The **Show** switch toggles whether Relay 2 is shown as an option in the Control View or not. The same fields are available here as in Relay 1 to pair Relay 2 with a sensor.



ALTA Wireless Control Unit Specifications		
Control Unit Relays	10-Amp Units	30-Amp Units
Initial Contact Resistance	Max. 100 mΩ	Max. 50 mΩ
Max Switching Power (resistive load)	2500VA 150W (NO) 1662VA 150W (NC)	8310VA (30A 277VAC)
Max Switching Voltage	250 VAC, 100 VDC (0.5A)	277 VAC
Max Switching Current	10A (AC), 5A (DC)	30A
Nominal Operating Power	360 mW	Approx 800 mW
Operate Time (at nominal voltage / 20°C)	Max 10 ms	Max 20 ms
Release Time (at nominal voltage / 20°C)	Max 10 ms	Max 10 ms
Max Operating Speed	20 times/min (at nominal switching capacity)	20 times/min (at nominal switching capacity)
Number of Relays	2 (individually controlled)	
Control Activation	- Automatic based on paired sensor - Manual through iMonnit online software	
Paired Sensor Relationship	1 sensor per relay (total: 2 sensors / device)	
Power		
Input Power	5.5 VDC @ 900 mA	
Mechanical		
Antenna	Connector: SMA Gain (dBi): 5.0	
Indicator Lights	Four LED indicators - Power - Radio (RF) communication - Relay 1 status (On/Off) - Relay 2 status (On/Off)	
Enclosure	ABS Plastic UL94V-0 flame rating	
Dimensions	5.5 x 3.355 x 1.25 in. (139.7 x 85.217 x 31.75 mm)	
Weight	8 ounces	
Environmental		
Operating Temperature	-40° to +85° C (-40° to +185° F)	
Certifications:	900 MHz product; FCC ID: ZTL- RFSC1 and IC: 9794A-RFSC1. 868 and 433 MHz product tested and found to comply with: CISPR 22:2008-09 / EN 55022:2010 - Class B and ETSI EN 300 220-2 V2.4.1 (2012-05).	



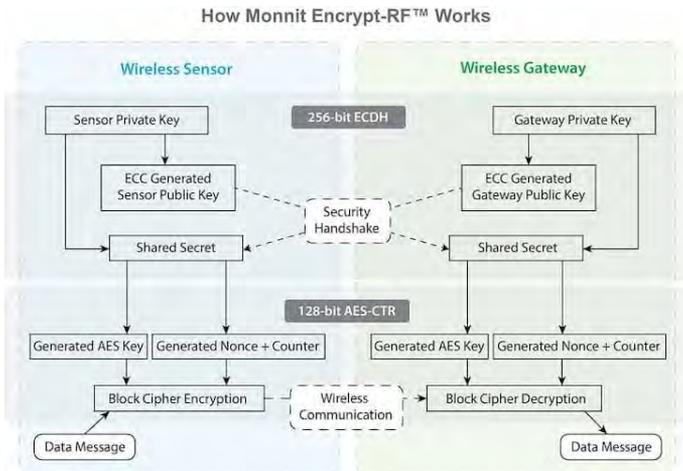
VII. SECURITY

Monnit ALTA Wireless, PoE•X (Power over Ethernet), and MoWi (Wi-Fi) sensors have been designed and built to securely manage data. Monnit works to ensure your data security is handled with the utmost care. The same methods utilized by financial institutions to transmit data are also used in Monnit's security infrastructure. Security features from sensors to gateways include tamper-proof network interfaces, data encryption, and bank-grade security.

Monnit's proprietary sensor protocol uses low 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 data traffic isn't altered between sensors and gateways. Paired with a best-in-class range and power consumption protocol, all data is transmitted securely from your devices, ensuring a smooth, worry-free experience.

SENSOR COMMUNICATION SECURITY

Monnit's sensor-to-gateway, secure wireless tunnel, **Encrypt-RF™**, 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 better battery life. Thanks to this combination, Monnit proudly offers robust bank-grade security at every level.



DATA SECURITY ON THE GATEWAY

ALTA Gateways are designed to prevent prying eyes from accessing the data that is stored on the sensors. Gateways do not run on an off-the-shelf, multi-function operating system. Instead, they run on a purpose-specific, real-time, and embedded state machine that cannot be hacked to run malicious processes. There are also no active interface listeners that can be used to gain access to the device over the network. The fortified gateway secures your data from attackers and secures the gateway from becoming a relay for malicious programs.



iMONNIT SECURITY

The iMonnit system is the online software and central hub for configuring your device settings. All data is secured on dedicated servers operating Microsoft SQL Server. Access is granted through the iMonnit user interface that requires Two-Factor Authentication, or an Application Programming Interface (API) safeguarded by 256-bit Transport Layer Security (TLS 1.2) encryption. TLS is a blanket of protection to encrypt all data exchanged between iMonnit and you. The same encryption is available to you whether you are a Basic or Premiere user of iMonnit. You can rest assured that your data is safe with iMonnit.

iMONNIT ENTERPRISE

If your organization does not allow for external data communication due to sensitive information or regulations, such as national laboratories, where information systems need to remain behind advanced security protocols and firewalls, Monnit offers an on-premise version of iMonnit. iMonnit Enterprise provides the same feature set as the iMonnit Premiere online software but allows your organization to host and maintain its own sensor data.

OPTIONAL DATA AUTHENTICATION



SensorPrints is the industry's only end-to-end Internet of Things data authentication platform for low-power wireless sensors. SensorPrints authenticates data by issuing a unique fingerprint for each device within the IoT. Data is secured from the point of generation to the point of consumption. Easy to install and use, SensorPrints is the definitive IoT security solution for any enterprise.

SensorPrints authenticates data at both the point of generation and consumption, creating trust between the sensor and server levels. Implementing 256-bit SHA 3 authentication, SensorPrints creates a "fingerprint" for a Monnit Wireless Sensor that contains an authenticated sensor message. When data is transmitted from the sensor, it is accompanied by a generated authentication token. Upon receipt by the application, the token is evaluated via cryptographic hash function against a unique per sensor secret key. This step provides an unprecedented level of full-coverage security for any Monnit user wishing to secure their IoT devices and data. More information can be found at <https://www.monnit.com/products/software/sensorprints-data-authentication/>.



VIII. SUPPORT

For technical support and troubleshooting tips, please visit our support library 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. A support representative will call you within one business day.

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

IX. WARRANTY INFORMATION

(a) Monnit warrants that Monnit-branded products (Products) will be free from defects in materials and workmanship for a period of one (1) year from the date the Products arrive at the Customer's shipping address 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. Monnit shall provide the fix or patch after Monnit receives from the Customer (i) notice of such non-conformance, and (ii) sufficient information regarding such non-conformance so as to permit Monnit to create such bug fix or software patch. If any hardware component of any Product fails to conform to the Warranty in this Section, Monnit shall, at its option, refund the purchase price less any discounts, or repair or replace nonconforming Products with conforming Products or Products having substantially identical form, fit, and function. Monnit will then deliver the repaired or replacement Product to a carrier for land shipment to the Customer within a reasonable period after Monnit receives from the Customer (i) notice of such non-conformance, and (ii) the non-conforming Product provided; however, if, in its opinion, Monnit cannot repair or replace on commercially reasonable terms, it may choose to refund the purchase price. Repair parts and replacement Products may be reconditioned or new. All replacement Products and parts become the property of Monnit. Repaired or replacement Products shall be subject to the Warranty, if any remains, originally applicable to the Product repaired or replaced. The Customer must obtain from Monnit a Return Material Authorization (RMA) number prior to returning any Products to Monnit. Products returned under this Warranty must be unmodified.

The Customer may return all Products for repair or replacement due to defects in original materials and workmanship, if Monnit is notified within one year of the Customer's receipt of the Product. Monnit reserves the right to repair or replace Products at its own and complete discretion. 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. The Customer acknowledges that replacement Products may be repaired, refurbished or tested, and found to be complying. The 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, shall bear the risk of loss and such costs of shipment of repaired Products or replacements, and shall credit a Customer's reasonable costs of shipping such returned Products against future purchases.



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

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 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 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 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: 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, même si le brouillage est susceptible d'en compromettre le fonctionnement.



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 gas stations, oil refineries, etc.

It is the responsibility of the user to enforce the country regulations and the specific environmental regulations.

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

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

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

The European Community provides some Directives for the electronic equipment introduced to the market. All of the relevant information is available on the European Community website: <http://ec.europa.eu/enterprise/sectors/rtte/documents/>.

Additional Information and Support

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



Monnit Corporation

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