ALTA by MONNIT

Remote Monitoring for Business

iMonnit
USER GUIDE

Table of Contents

I. ABOUT iMONNIT **1**

iMONNIT BASIC 1

iMONNIT PREMIERE 1

DOWNLOADING THE iMONNIT APP 3

iMONNIT SECURITY 4

II. REGISTRATION **5**

LOGGING INTO THE ONLINE SYSTEM 6

REGISTERING A DEVICE 6

III. THE HOMEPAGE **7**

MAIN NAVIGATION MENU 7

IV. SENSOR OVERVIEW **8**

MENU OVERVIEW 8

V. GATEWAY OVERVIEW **14**

HOW GATEWAYS WORK 14

GATEWAY SETTINGS 15

VI. ACTIONS OVERVIEW **22**

CREATING AN ACTION 22

VII. SENSOR MAPS OVERVIEW **25**

CREATING A SENSOR MAP 25

VIII. REPORTS OVERVIEW **26**

ADDING A REPORT 26

IX. USER OVERVIEW **28**

ADDING NEW USERS 28

X. NETWORKS OVERVIEW **29**

ADDING A NEW NETWORK 29

EDITING A NETWORK 29

XI. CREDITS OVERVIEW **30**

XII. SETTINGS OVERVIEW **31**

GENERATING A TOKEN 31

RENEWING A SUBSCRIPTION 32

XIII. WALLET OVERVIEW 34

ADDING A CARD 34

SUPPORT 35

WARRANTY INFORMATION 35

I. ABOUT iMONNIT

iMonnit® is a cloud based mobile Internet platform and central hub for managing Monnit® and ALTA® products. All data is secured on dedicated servers operating Microsoft SQL Server. This online user interface is where all your device settings can be arranged, supervised, and modified to reflect your unique environment. You can access iMonnit on any Internet browser simply by typing www.imonnit.com into the address bar. In addition, you can also download the iMonnit App from to your smartphone or tablet. Start with the basic version or upgrade to iMonnit Premiere to enjoy the full features your Monnit experience can offer.

iMONNIT BASIC

iMonnit Basic is included for free with all wireless sensors, providing basic features for you to configure and monitor your sensors online. These basic features only support one network and one registered user on an account. More advanced settings, permissions, and actions are available with an upgrade to iMonnit Premiere.

iMONNIT PREMIERE

iMonnit Premiere allows for enhanced functionality of your wireless sensors and includes an advanced software feature set at a low annual cost. All of iMonnit's advanced features are available for configuration. You can have more sensors on your account, support multiple users, and view floor plans for all your sensors.

System Requirements

- Ethernet gateways require existing Internet connection
- Wireless Sensor Adapter or USB Pro Gateways require Windows PC or 3rd party IoT gateway

BASIC	PREMIERE		EXPRESS	ENTERPRISE
ALWAYS FREE	STARTING @ $39	PRICE	STARTING @ $79	CALL FOR PRICING
	✓	BASIC CONFIGURATIONS	✓	✓
✓	✓	ADVANCED CONFIGURATIONS	✓	✓
✓	✓	HISTORY REPORTS	✓	✓
✓	✓	VISUAL CHARTS		✓
✓	✓	DATA EXPORT		✓
✓	✓	CALIBRATION	✓	✓
✓	✓	USB GATEWAY	✓	✓
✓	✓	ETHERNET GATEWAY	✓	✓
✓	✓	CELLULAR GATEWAY	*	✓
✓	✓	WiFi SENSORS		✓
✓	✓	INTERNET ACCESSIBLE	*	✓
		OFF-LINE ACCESS	✓	✓
✓	✓	ALERT HISTORY		✓
	✓	>1 ALERT RECIPIENTS		✓
✓	✓	GROUP CONFIGURATIONS	✓	✓
	✓	ACCESS CONTROL	✓	✓
✓	✓	EMAIL ALERTS		✓
✓	✓	SMS ALERTS		
✓	✓	VOICE CALLS		
	✓	SENSOR MAPPING		✓
	✓	AUTOMATED REPORTING		✓
2 hours	10 minutes	HEARTBEAT MINUTES	1 second	1 second
	Available	SUB-ACCOUNTS		Unlimited
1	20	# OF NETWORKS	1	20
500 per Network	500 per Network	# OF SENSORS	Up to 100	500 Per Network
1	Unlimited	# OF USERS	Multiple	Unlimited
45 Days	1 Year	SAVED HISTORY	5,000 records	Self-Managed
Online Only	Online Only	SUPPORT	Online Only	Online, Phone

* Depends on your personal firewall & server set-up.

Figure 1

DOWNLOADING THE iMONNIT APP

The iMonnit app is available on both Google Play and the Apple App Store. Use your smartphone to take a picture of the following QR code to be taken to a page to download the mobile app to your device.

Figure 2

Alternatively, you can go to the iMonnit site and select one of the direct links in the bottom of the login box.

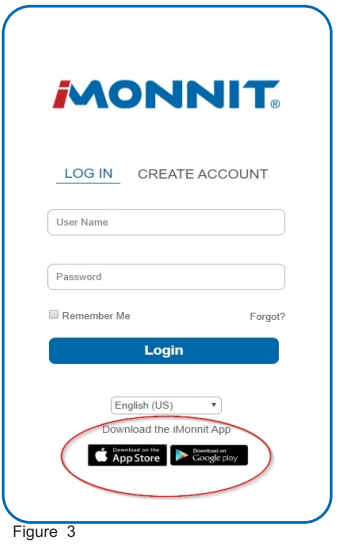


Figure 3

Android

Select the link to go to the Google Play store and download the “iMonnit: Mobile Software.” Choose the Install button and the app will begin to download to your smartphone or tablet.

Note: The app requires Android 4.0 and up.

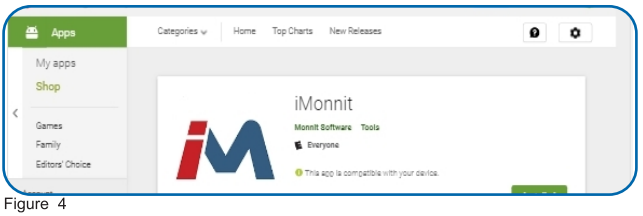


Figure 4

Apple (iOS)

Choose the link for the Apple (iOS) app to be taken to the App Store for Mac Devices. The app works with iPhone, iPad, and iPod Touch and free to download. Select the app labeled “iMonnit: Mobile Software.” Download the app and start registering your devices.

Note: The app is only available on the App Store for iOS devices and requires iOS 11.0 or later.

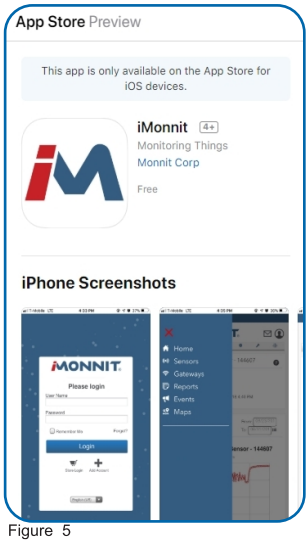


Figure 5

iMONNIT SECURITY

Security is paramount for the iMonnit when it comes to managing your environment and equipment. Great care and attention to detail has been taken to keep the exchange of data secure on a gateway and in device communications.

iMonnit 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, or an Application Programming Interface (API) safeguarded by 256-bit Transport Layer Security (TLS 1.2) encryption. TLS is blanket of protection to encrypt all data exchanged between iMonnit and you. The same encryption is available to you whether you are a Basic user of Premiere user of iMonnit. You can rest assured that your data is safe with iMonnit.

II. REGISTRATION

If this is your first time using the iMonnit online portal, you will need to create a new account. If you have already created an account, you can skip to the “Logging into the Online System” section. The following instructions will guide you through creating the account.

1. Open iMonnit in your mobile app or web browser.

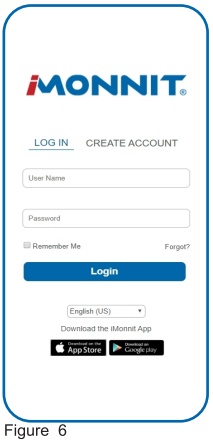


Figure 6

2. Navigate your cursor to the “Create Account” link located off to the right.

3. Next you will be asked to enter your account information in the following fields:

Note: If this is a Free Trial, you may not have received a subscription code yet. Leave the box blank and proceed.

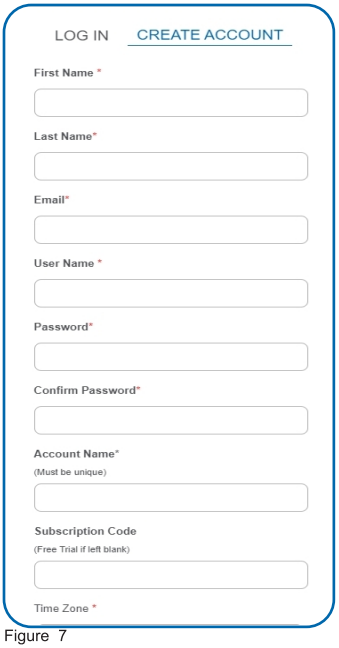


Figure 7

4. When completed, select the “Next” button.

5. This step will complete the user registration process and lead you onto registering your device. For steps on how to register your device, see the Registering a Device section below.

LOGGING INTO THE ONLINE SYSTEM

1. Open iMonnit in your mobile app or web browser.

2. Enter your user name and password.

Figure 8

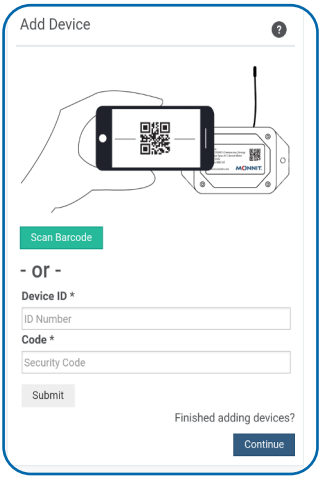
3. Select the “Login” button.

REGISTERING A DEVICE

You will need to enter the Device ID and the Security Code from your devices in the corresponding text boxes. Select the **Scan Barcode** button to use the camera on your smartphone to scan the QR code on your sensor and gateway. 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 Security Code manually.

- The Device ID is a unique number located on each device label.
- Next you’ll be asked to enter the Security Code (SC) on your device. A security code will be a set of six capital letters.

Figure 9



When completed, select the **Finish Adding** button.

III. THE HOMEPAGE

From the iMonnit homepage you can view how many active and/or alerting sensors and gateways, along with a complete list of networks on your account. Check this page regularly to make sure that your system is functioning properly.

Figure 10

MAIN NAVIGATION MENU

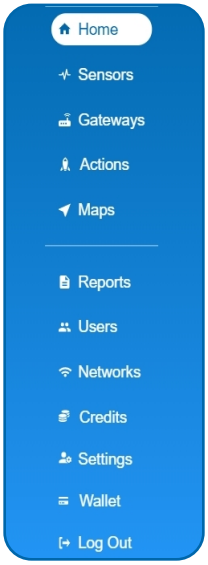


Figure 11

The main navigation menu is the primary resource you will refer to for information regarding your devices and settings. This is broken down into two sections: **Overview** and **Account**.

OVERVIEW

- **Home** - This will take you back to the homepage.
- **Sensors** - View and modify sensors on your account.
- **Gateways** - Adjust settings for your gateways.
- **Actions** - Create and edit actions for your sensors.
- **Maps** - Upload floorplans and position sensors where they are located in your environment. (Available only for Premiere Members.)

ACCOUNT

- **Reports** - Assemble detailed summaries for your system.
- **Users** - Modify all permissions and settings for users on your account. (Unlimited users only available for Premiere Members)
- **Networks** - Review and edit all networks on your account. (Mulitple networks only available for Premiere members)
- **Credits -** Add notification credits on your account.
- **Settings** - Subscribe to iMonnit Premiere and adjust account preferences.
- **Wallet -** Review and modify payment info for your account.

Each of these options are covered in their own user guide sections. Read on for more information on these various pages.

IV. SENSOR OVERVIEW

Select **Sensors** from the main navigation menu to access the sensor overview page and begin making adjustments to your sensors.

MENU SYSTEM

Details - Displays a graph of recent sensor data.

Readings - List of all past heartbeats and readings.

Actions - List of all actions attached to this sensor.

Settings - Editable levels for your sensor.

Calibrate - Reset readings for select sensors (Not available for all sensor types).

Scale - Change the scale of readings for your sensor (Not available for all sensor types).

Directly under the tab bar is an overview of your sensor. This allows you to see the signal strength and the battery level of the selected sensor.

- **Green** indicates the sensor is checking in and 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 out of date, due to perhaps a missed heartbeat check-in.

Details View

The Details View will be the first page you see upon selecting which sensor you would like to modify.

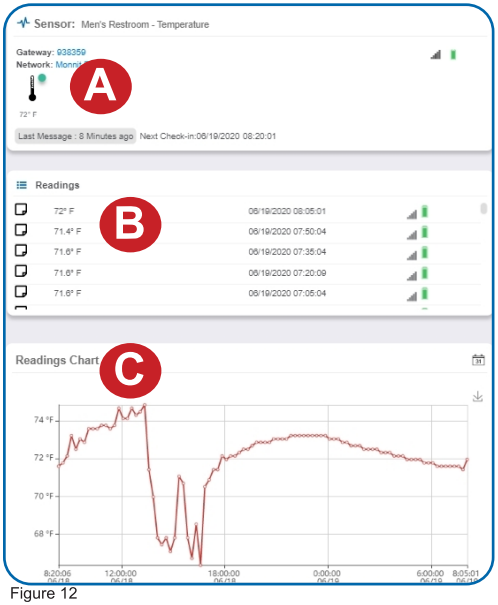


Figure 12

A. The sensor overview section will be above every page. This will consistently display the present reading, signal strength, battery level, and status.

B. The Recent Readings section below the chart shows your most recent data received by the sensor.

C. This graph charts how the sensor fluctuates 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 from and/or to date.

Readings View

Selecting the “Readings” tab within the tab bar allows you to view the sensor’s data history as time stamped data.

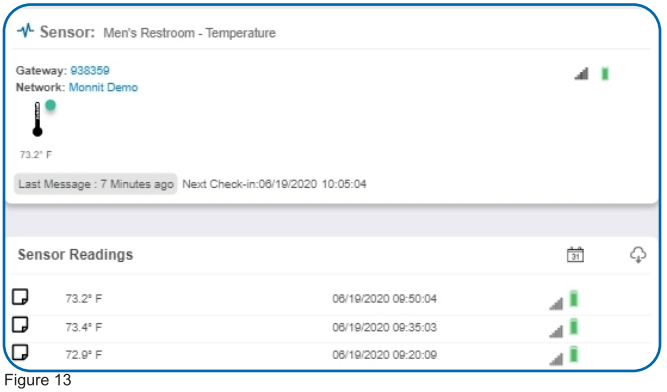


Figure 13

On the far right of the sensor history data is a cloud icon. Selecting this icon will export an excel file for your sensor into your download 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 most recent week 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 our database.

Sensor ID: If multiple sensors are exported you can distinguish which reading was from which using this number even if the names for some reason are the same.

Sensor Name: The name you have given 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.

Battery: Estimated life remaining of the battery.

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

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

Gateway ID: The Identifier of the gateway that relayed the data from the sensor.

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

Signal Strength: Strength of communication signal between the sensor and the gateway, shown as percentage value.

Voltage: Actual voltage measured at the sensor battery used to calculate battery percentage, similar to Received Signal you can use one or the other or both if they help you.

State

The integer presented here is generated from a single byte of stored data. A byte consists of 8 bits of data that we read as Boolean (True (1)/False (0)) fields.

Using a temperature sensor as an example.

If the sensor is using factory calibrations the Calibrate Active field is set True (1) so the bit values are 00010000 and it is represented as 16.

If the sensor is outside the Min or Max threshold, the Aware State is set True (1) so the bit values are 00000010 and it is represented as 2.

If the customer has calibrated the sensor this field the Calibrate Active field is set False (0) AND the sensor is operating inside the Min and Max Thresholds, the bits look like 00000000 this is represented as 0.

If the sensor is using factory calibrations and it is outside the threshold the bit values are 00010010 and it is represented as 18 (16 + 2 because both the bit in the 16 value is set and the bit in the 2 value is set).

Note: These two are the only bits that typically observed outside of our testing procedures.

Settings View

To edit the operational settings for a sensor, choose the "**Sensor**" option in the main navigation menu then select the "**Settings**" tab to access the configuration page. The example below is for a Temperature Sensor.

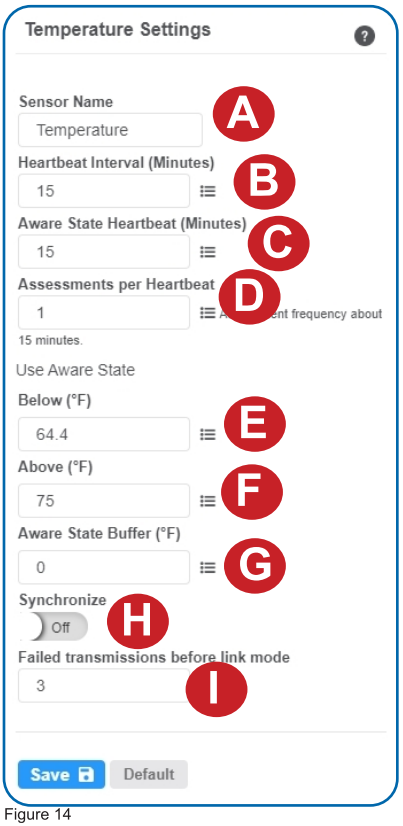


Figure 14

A. 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. Aware State Heartbeat is how often the sensor communicates with the gateway while in an Aware State.

D. Assessments per Heartbeat is how many times between heartbeats a sensor will check its measurements against its thresholds to determine whether it will enter an Aware State.

E. Below is the minimum reading the sensor should record before entering an Aware State.

F. Above is the maximum reading the sensor should record before entering an Aware State.

G. The **Aware State Buffer** is a buffer to prevent the sensor from bouncing between Standard Operation and Aware State when the assessments are very close to a threshold. For example, if a Maximum Threshold is set to 90° and the buffer is 1°, then once the sensor takes an assessment of 90.1° it will remain in an Aware State until dropping to 89.0°.

H. In small sensor networks the sensors can be set to **synchronize** their communications. The default setting off allows the sensors to randomize their communications therefore maximizing communication robustness. Setting this will synchronize the communication of the sensors.

I. Failed transmissions before link mode is the number of transmissions the sensor sends without response from a gateway before it goes to battery saving link mode. In link mode, the sensor will scan for a new gateway and if not found will enter battery saving sleep mode for up to 60 minutes before trying to scan again. A lower number will allow sensors to find new gateways with fewer missed readings. Higher numbers will enable the sensor to remain with its current gateway in a noisy RF environment better. (Zero will cause the sensor to never join another gateway, to find a new gateway the battery will have to be cycled out of the sensor.)

The default heartbeat interval is 120 minutes or two hours. It is recommended that you do not lower your heartbeat level too much because it will drain the battery.

Finish by selecting the **Save** button.

Note: Be sure to select the "Save" button anytime you make a change to any of the sensor parameters. All changes made to the sensor settings will be downloaded to the sensor on the next sensor heartbeat (check-in). Once a change has been made and saved, you will not be able to edit that sensor's configuration again until it has downloaded the new setting.

Calibrate View

If a sensor type has readings that need to be reset, the "Calibrate" tab will be available for selection in the sensor tab bar.

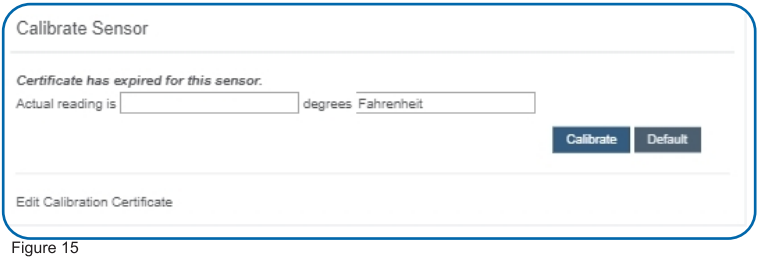


Figure 15

To calibrate a sensor, you will want to ensure that the environment of the sensor and other calibration device is stable. Note the "Expected Next Check-in" time for the sensor you are calibrating and take a reading from your calibration device a few minutes prior to the sensors next check-in.

Enter the actual (accurate) reading from the calibration device into the text field. If you need to change the unit of measurement you can do that here.

Press **Calibrate**.

To ensure that the calibration command is received prior to the sensors next check-in, press the control button on the back of the gateway, once, to force communication (Cellular and Ethernet gateways).

After pressing the **Calibrate** button and choosing the gateway button, the server will send the command to calibrate the specified sensor to the gateway. When the sensor checks-in, it will send the pre-calibration reading to the gateway, then receive the calibration command and update it's configuration. When the process is completed, it will send a "Calibration Successful" message. The server will display the sensor's last pre-calibrated reading for this check-in, then all future readings from the sensor will be based on the new calibration setting.

It is important to note that after calibrating the sensor, the sensor reading returned to the server is based on pre-calibration settings. The new calibration settings will take effect on the next sensor heartbeat.

Note: If you would like to send the changes to the sensor right away, please remove the battery(s) for a full 60 seconds, then re-insert the battery(s). This forces the communication from the sensor to the gateway and this the message to make a change from the gateway back to the sensor. (If the sensors are industrial sensors, turn the sensor off for a full minute, rather than removing the battery).

Creating a Calibration Certificate

Creating a sensor calibration certificate will mask the calibration tab from those who should not have permissions to adjust these settings. Permissions for self-certifying a calibration must be enabled in user permissions.

Directly below the calibrate button is the selection to **Create Calibration Certificate**.

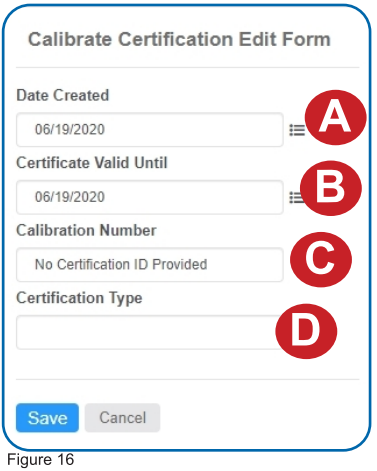


Figure 16

A. The **Date Created** will be filled with the current date by default.

B. The **Certificate Valid Until** field must be set one day in the future after the date contained in the "Date Certified" field.

C. **Calibration Number** is a unique number for your calibration certificate.

D. Calibration Type is unique to

Choose the **Save** button before moving on.

When the new certificate is accepted, the Calibration tab will change to a Certificate tab.

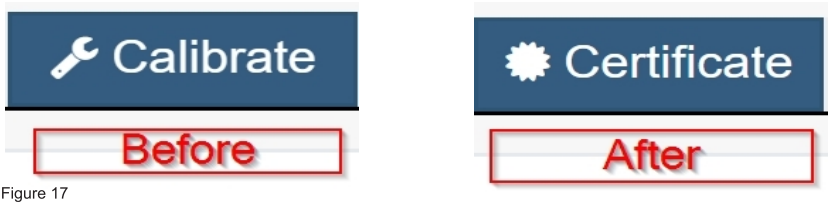


Figure 17

You will still be able to edit the certificate by choosing the Certificate Tab and navigating down to **Edit Calibration Certificate**.

The tab will revert back to "Calibrate" after the period for the certificate ends.

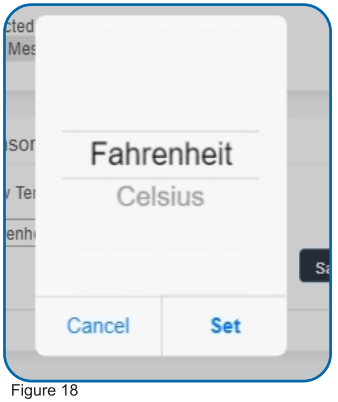


Figure 18

Scale View

If the sensor settings are influenced by temperature, the scale option will be available in the tab bar. To change the temperature unit of measurement from Fahrenheit to Celsius or vice versa, select the Scale tab.

Choose the text box to trigger a pop-up window allowing you to change the scale. Select the scale you prefer and push “Set.”

Press the **Save** button to complete your adjustment.

V. GATEWAY OVERVIEW

HOW GATEWAYS WORK

A **gateway** is the device that manages communication between your sensors and servers. On startup, the gateway will periodically transmit a heartbeat, checking in with the servers to make sure it is still receiving an active signal. Sensors also have heartbeats and will relay information to the gateway, which then forwards the data to the server. There are four different types of gateways:

Cellular, International Cellular, Ethernet, USB, and Serial Modbus Gateway. All gateways require an active iMonnit® account in order to be operational. Gateway settings can be accessed on iMonnit or in the offline local interface.

- **Cellular Gateways**: Uses cell towers to facilitate communication between gateways and the monitoring system.
- **Ethernet Gateways**: Requires an Ethernet cable to establish a connection between your gateway and Monnit Servers using an IEEE 802.3 network.
- **USB Gateways**: Uses an existing internet connection on a PC to facilitate communication with the Monnit servers.
- **Serial Modbus Gateway**: Acts as a data concentric for Monnit wireless sensor networks.

Cellular, International Cellular, Ethernet, USB, and Serial Modbus Gateway. All gateways require an active iMonnit® account in order to be operational. Gateway settings can be accessed on iMonnit or in the offline local interface.

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

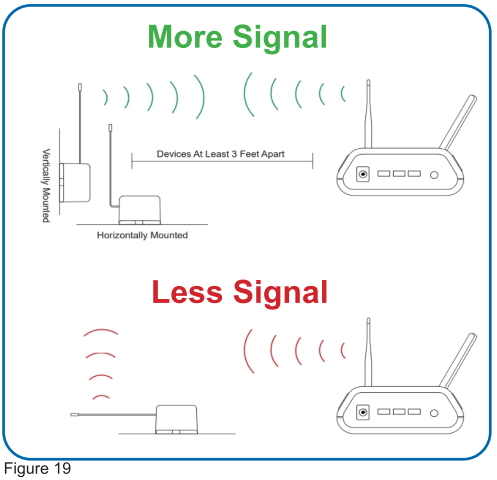


Figure 19

GATEWAY SETTINGS

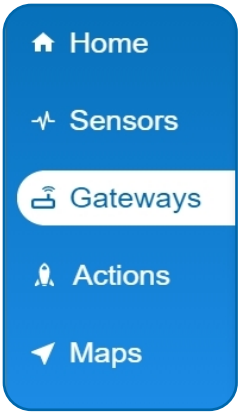


Figure 20

On iMonnit, find Gateways in the main navigation menu to start modifying your gateway settings.

A list of all the gateways registered to your account will display. There should be at least one gateway registered to your account in order for your sensors to be active.

Select one of your gateways from the list. There will be a series of tabs allowing you to view the status of your gateway and make changes.

Figure 21

A. History – This will be the first page to display. With a list of data received from previous heartbeats. If there have been any alert states in the past, they will show up here.

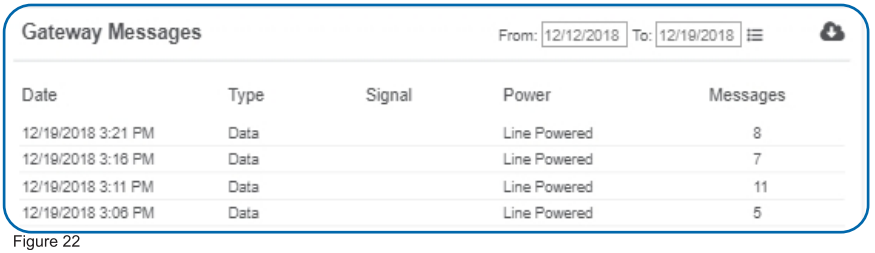
B. Events – This will display a list of all the events you have under this gateway. If you have not assigned any events to this gateway, the page will be blank. For tips on how to set an event, see Getting Started – Events for more information.

C. Settings – If you would like to make changes to your gateway network connection, you can do so here under the Settings section.

D. Sensor List – Here you will see a list of sensors registered to the gateway. If there aren't sensors registered to the gateway, the list will be blank.

Gateway History View

The first tab to display when entering your gateway will be the History tab, allowing you to view gateway messages as time stamped data.



Date	Type	Signal	Power	Messages
12/19/2018 3:21 PM	Data		Line Powered	8
12/19/2018 3:16 PM	Data		Line Powered	7
12/19/2018 3:11 PM	Data		Line Powered	11
12/19/2018 3:06 PM	Data		Line Powered	5

Figure 22

- On the far right of the gateway history data is a cloud icon. Selecting this icon will export an excel file for your sensor into your download 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 most recent week by default. Only the first 2,500 entries in the selected date range will be exported.

Gateway Action View

All actions assigned to the gateway can be found by selecting the Actions tab. If there are no active actions, none will be listed for the gateway. From here you have the option of selecting an action to edit, pausing notifications, or delaying alerts for one hour. For more on creating and editing action notifications, see the Action section of this guide.

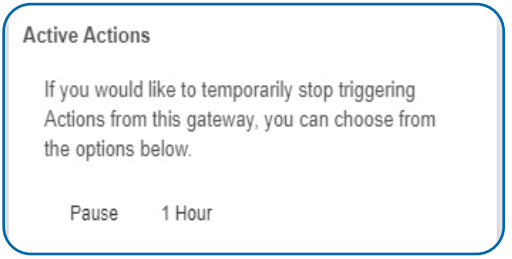


Figure 22

Gateway Settings View

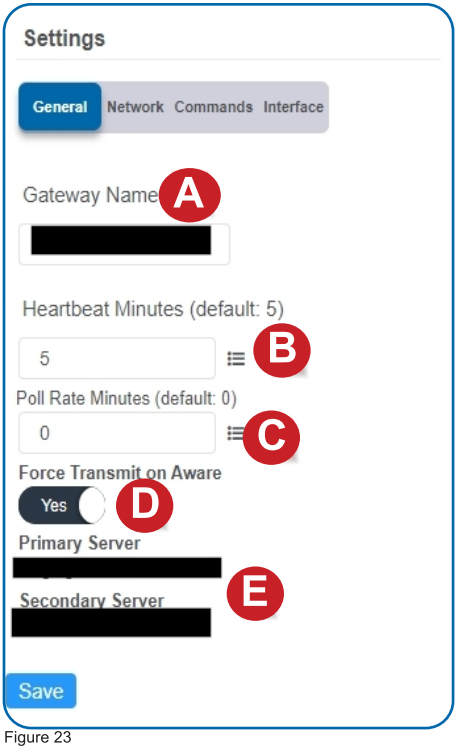


Figure 23

Select the **Settings** tab to enter gateway settings. Depending on the gateway model, there may be a different collection of general settings available for modification.

Ethernet Gateway General Settings

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

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

C. The **Poll Rate Minute** setting only applies if you are using Monnit Control or Monnit Local Alert. Here's how it works: to conserve cellular data, your gateway has a set heartbeat (meaning it only exchanges data with the iMonnit server once every five minutes by default). If you are using Monnit Control or Monnit Local Alert, you may want to control equipment or receive local alerts more frequently. If you were to increase your gateway heartbeat, you would increase your data usage substantially.

Setting a poll rate allows your gateway to check for priority incoming messages more frequently — while using a fraction of the data of a regular message exchange. Your gateway asks the iMonnit server if there are any priority incoming messages, and if there are, they are exchanged immediately. If not, no messages are exchanged until your gateway has its next regular heartbeat.

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

Setting a poll rate allows your gateway to check for priority incoming messages more frequently — while using a fraction of the data of a regular message exchange. Your gateway asks the iMonnit server if there are any priority incoming messages, and if there are, they are exchanged immediately. If not, no messages are exchanged until your gateway has its next regular heartbeat.

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

E. The **Primary Server** is the main server your gateway is programmed to communicate with. The **Secondary Server** is the next server the gateway will issue communication through if it cannot contact the Primary Server.

Cellular Gateway General Settings

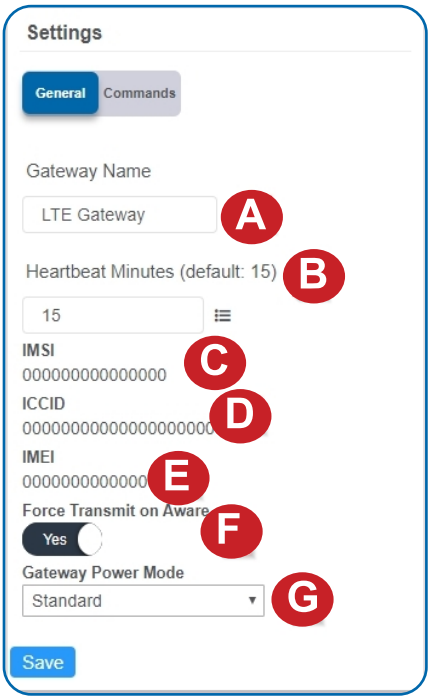


Figure 24

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

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

C. The **IMSI** (International Mobile Subscriber Identity) number as the mode to identify the country, mobile network, and subscriber. It is formatted as MCC-MNC-MSIN. MCC is the Mobile country Code. MNC is the Mobile Network Code attached to the cellular network. MSIN is a sequential serial number making the IMSI unique to a subscriber.

D. The **ICCID** is the nineteen digit unique identification number corresponding to the cellular SIM card. It is possible to change the information contained on a SIM (including the IMSI), but the identity of the SIM itself remains the same.

E. IMEI (International Mobile Equipment Identity) is a number exclusive to a Cellular Gateway to identify the gateway to the cell tower.

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

G. Gateway Power Mode is a dropdown menu to select how much power your gateway uses. Choose between Standard, Force High Power, or Force Low Power.

Network

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

Multiple interfaces can be active, but they each need a static IP address on the Gateway. Internet Service Providers (ISPs) assign IP (Internet Protocol) addresses to a computer so users can access the Internet. An IP address is a unique number typically formatted as 000.000.000.0.

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

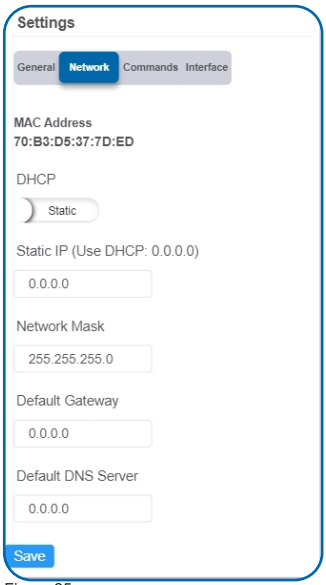


Figure 25

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

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

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

Default DNS Server - DNS Servers take alphanumerical data (like a url address) and dial the number for the server containing the information you're looking for.

Commands

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

Figure 26

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

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

If there are updates available for your gateway firmware, the **Update Gateway Firmware** button will appear, giving you the option to select it and install the latest firmware.

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

Interface

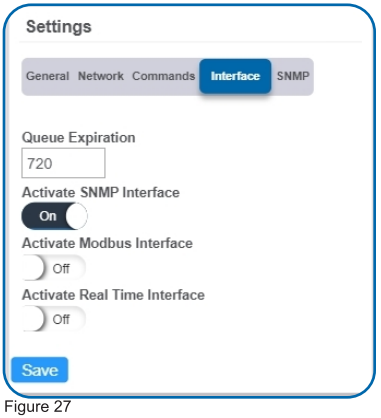


Figure 27

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

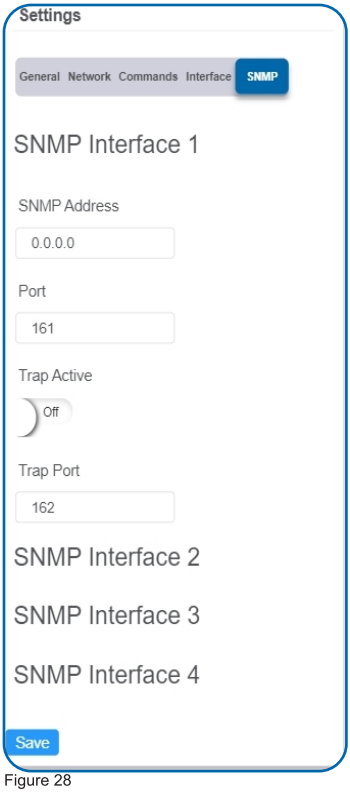


Figure 28

SNMP Interface – SNMP (Simple Network Management Protocol) compiles information from a variety of clients. This is especially helpful if you have multiple gateways for devices that need to communicate with the gateway. Monnit gateways can manage up to four clients. For more on the SNMP Interface visit the article SNMP Interface Configuration. Monnit gateways can manage up to four clients. The SNMP settings for a gateway can be adjusted on iMonnit and the offline local interface. You can continue to use SNMP without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received by the gateway.

- **SNMP Address** – This is the IP address for the SNMP Client you wish to communicate with the device. The Enterprise Gateway has sensor information @ 40101 - 40116 (100 – 115 raw address), and every 16 after in the same pattern; 40117 – 40132.

(116- 131 raw) is the next set of 16. Addresses of 0-15, 16-31, 32-47 refer to sensor slots 1, 2 and 3. This is the same as the Register Address of 40001-40016, 40017-40032, and 40033-40048.

- **Port** - The number for where the server data from the gateway is received. Ports 80 and 443 are reserved for https traffic. Web browsers use these ports to send requests to web servers.
- **Trap Active** – A “Trap” for an SNMP is an alert state sent from your connected device to the gateway which is then relayed to the server. By default, this option is off, but you can turn it on by toggling the switch over into the on position.
- **Trap Port** – The server port where the trap alert state is sent when active.

Modbus Interface – Modbus TCP (Transmission Control Protocol) is the Modbus RTU protocol with a TCP interface that runs on Ethernet. This allows blocks of binary data to be exchanged between computers. TCP is responsible for making sure all data is correctly received. IP (Internet Protocol) is responsible for making sure data is correctly addressed and routed. Monnit provides the Modbus TCP interface for you to pull gateway and sensor data. You can continue to use Modbus without the server interface active. The data will not be sent to a server, but you can continue to poll for the data as it is received by the gateway.

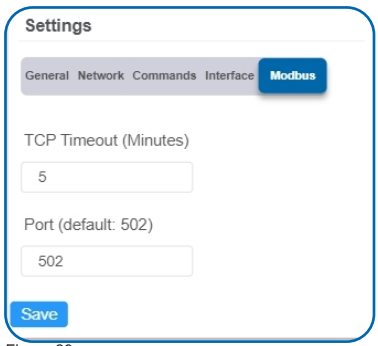


Figure 29

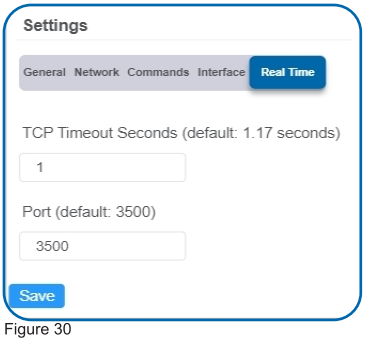


Figure 30

Real-time TCP - Real Time TCP (Transmission Control Protocol) guarantees response within a specific deadline. TCP is responsible for making sure all data is correctly received by the IP address. A static IP must be set on the gateway.

- **TCP Timeout Seconds** – The amount of time the gateway waits for a request to be received by the server before the session times out and the connection is refused.
- **Port** – The number for where the server data from the gateway is received. Ports 80 and 443 are reserved for https traffic. Web browsers use these ports to send requests to web servers.

Sensor List View

Choose the Sensor List tab to view a complete count of all sensors reporting to the selected gateway. This is only a list of the sensors. They cannot be edited from this page.

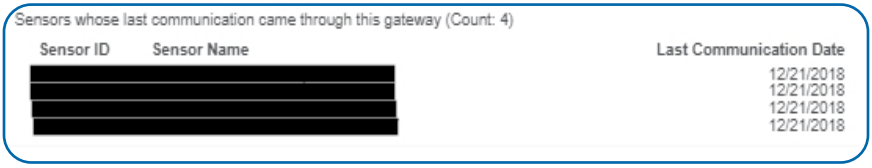


Figure 31

VI. ACTIONS OVERVIEW

Notifications for a single sensor or gateway can be created, deleted, and edited by selecting the “Actions” tab in the sensor tab bar.

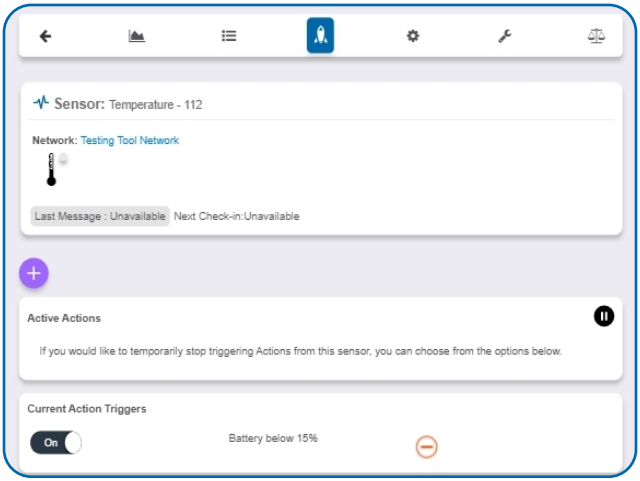


Figure 32

You can toggle the Action Trigger on or off by selecting the switch under Current Action Triggers.

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 actions 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.

- Select “Actions” in the main navigation menu.

Figure 33

- 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 event, the screen will be blank.

- From the Actions page, tap “Add Action” in the left hand corner.

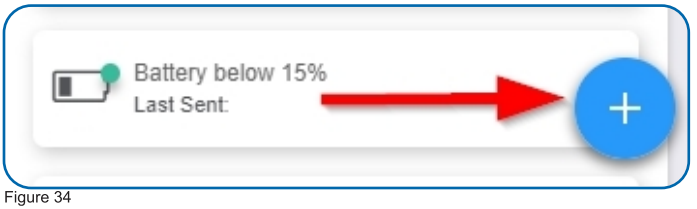


Figure 34

Step 1: What triggers your action?

- The dropdown menu will have the following options for Action Types:

Sensor Reading: Set actions based on sensor activity or reading.

Battery Level: This is where you can set to be notified when the battery level drops below a percentage. 15% is the default setting.

Device Inactivity: Actions when the device doesn’t communicate for an extended period of time.

Advanced: Actions based on advanced rules, such as comparing past data points with current ones.

Scheduled: These are actions that fire at a time set basis.

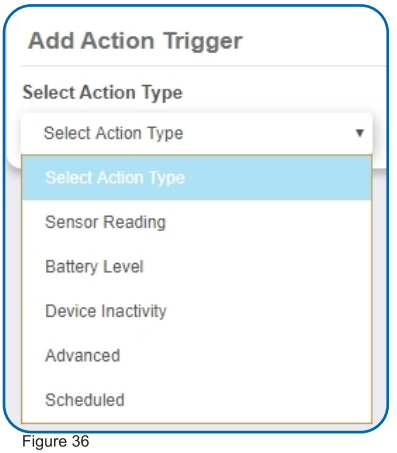


Figure 36

- Select **Sensor Reading** from the dropdown menu.
- A second dropdown 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 dropdown menu.
- 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.
- Press the “Save” button.

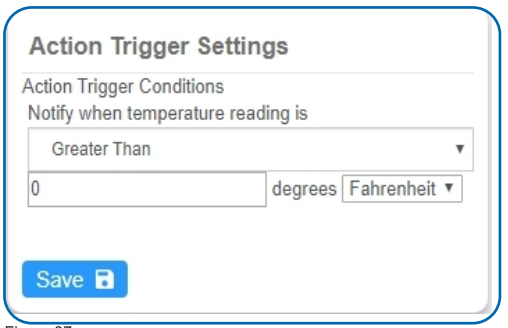


Figure 37

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.

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

Step 2: Actions

- Press the Add Action button under the Event Information header and available action types are presented in a select list.
  - **Notification Action:** Specify account users to receive notifications when this event triggers.
  - **System Action:** Assign actions for the system to process when this event triggers.

- Choose **Notification Action** from the notification list.

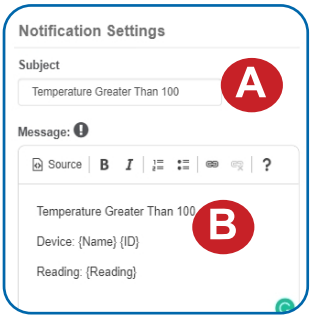


Figure 38

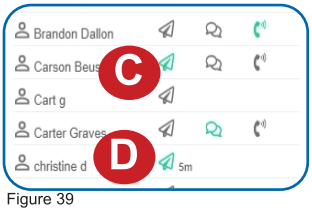


Figure 39

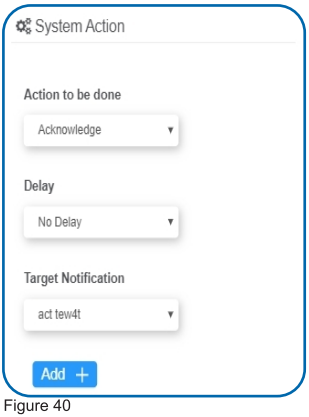


Figure 40

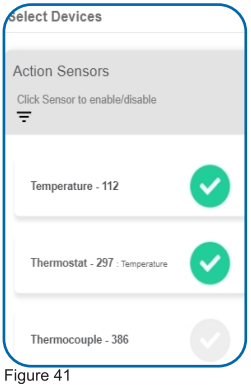


Figure 41

A. Configure the subject for the notification.

B. Customize the message body for the notification

C. Save button commits any changes to message content fields.

D. Recipient list identifies who will receive the notification.

- Select the icon next to a user to configure how they will be notified
- Choose if you want notifications sent immediately when triggered or if you want a delay before it is sent and press **Set.**
- A **green** icon indicates the users that will not receive the notifications.
- If a delay has been selected, the delay time will display beside the icon.
- Select System Action from the Add Action list.
- Scroll down to the System Action section.
- The Action to be Done select list has the following options.
  - **Acknowledge:** Automatically signal that you have been notified of an action. When an action has been triggered, alerts will continue processing until the action returns to a value that no longer triggers an action.
  - **Full Reset:** Reset your trigger so it is armed for the next reading.
  - **Activate:** Enable an action trigger.
  - **Deactivate:** Disable an action trigger.

Step 3: Action Name and Devices

- 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 "Checkmark button" to complete the process.

VII. SENSOR MAPS OVERVIEW

The Maps feature gives you the option of uploading your floorplan or other image to iMonnit® and allows you to virtually position sensors where you have physically placed sensors in the location. This is useful if you have multiple sensors and want to know see them in context of where they are placed. This guide will walk you through uploading a floorplan and positioning sensors.

CREATING A SENSOR MAP

1. Find the main navigation menu. and select “Maps.”

2. All previously created sensor maps will display.

3. To create a new sensor map, locate **Create Sensor Map** button.

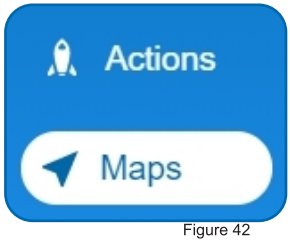


Figure 42

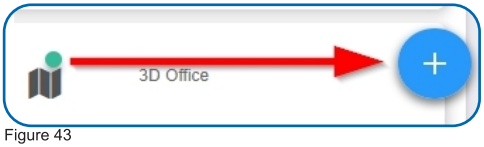


Figure 43

- The following page will ask you to enter a title for your new sensor map.
- Next you will upload a picture of your floorplan. Acceptable image formats are: bmp, gif, jpg, png, tiff.
- The following screen will be the Edit Map page. Choose the sensor you want to add to the map. The checkmark will turn green and the sensor icon will appear on the map.
- You can then drag it to the designated location on the map. Once your sensors are in you the desired locations, proceed to view the map.
- Select the **Save** button.

VIII. REPORTS OVERVIEW

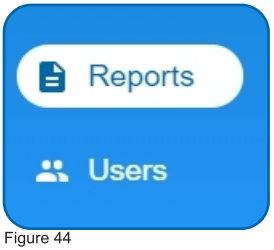


Figure 44

Reports are delivered regularly via email, updating you on sensor activity. The interval of these reports is easy to set and can even be submitted as one-time non-recurring updates. Regular reports help you stay up to date on your sensor activity. This guide will walk you through setting up a battery health report. You can use the same steps to set up other reports as needed. Some parameters will differ slightly depending on the type of report you select.

ADDING A REPORT

- To create a new report, select **Create Report** button.

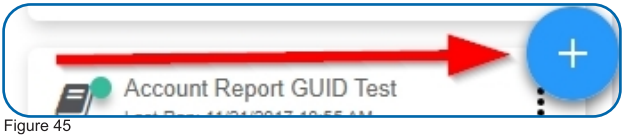


Figure 45

- Choose a Report Template.

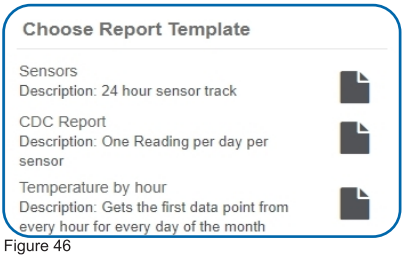


Figure 46

The following will use a “Network Data Export” option as an example:

Edit Report Section

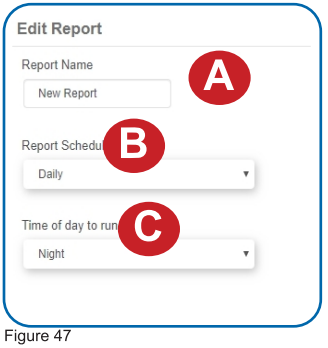


Figure 47

A. The Report Name is the primary identifier for the report.

B. Schedule your report for daily or once a week.

C. Set the time of day delivery for morning, mid-day, evening, or night.

Report Specific Parameters Section

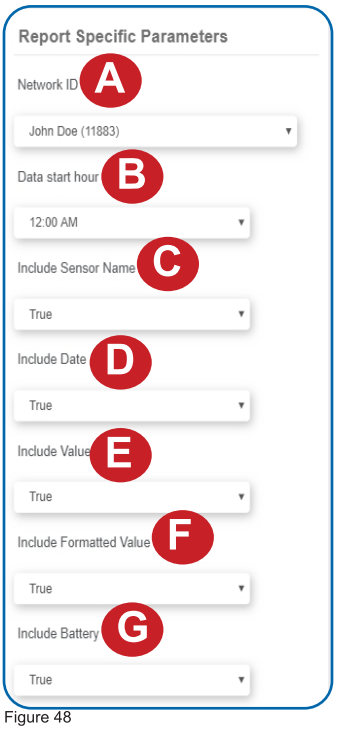


Figure 48

A. The Network ID assigns the network to the report.

B. Data start hour sets the time that the data will begin collecting.

C. Sensor Name adds the name of sensors to the report.

D. Date adds the calendar date to the report.

E. Include Value adds a value to the report.

F. Include Formatted Value adds a formatted value to the report.

G. Include Battery adds the battery percentage to the report.

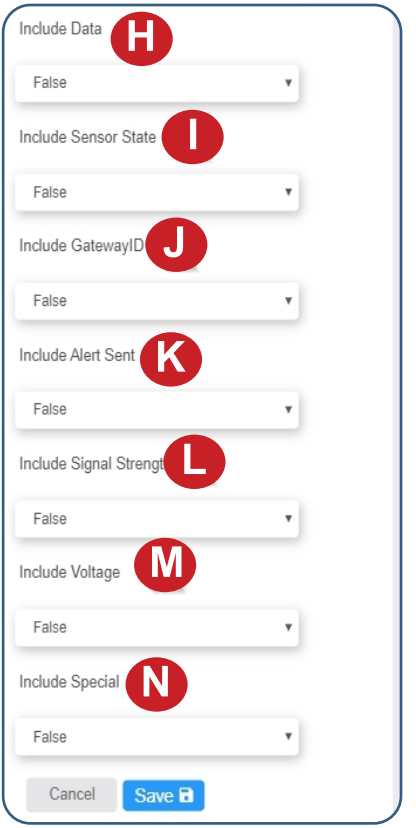


Figure 49

H. Include Data adds data entries to the report.

I. Include Sensor State adds the sensor state to the report.

J. Include GatewayID adds the gateway ID to the report.

K. Include Alert Sent adds the type of alert to the report.

L. Include Signal Strength adds the value for signal strength to the report.

M. Include Voltage adds the voltage data to the report.

N. Include Special adds additional data into extra columns.

Select the **Save** button.

IX. USERS OVERVIEW

Figure 50

The user list page can be accessed through the main menu. The user list will display all users who have access to your account. Basic iMonnit subscriptions may only have one primary user for the account.

The ability to add users to an account is an exclusive feature of iMonnit Premiere. Having additional users on an account gives you the chance to act as an administrator and control what each person is allowed to see and do on the account. This can be extremely helpful for a large company and several people need access to Monnit sensors in the event of an emergency.

ADDING NEW USERS

1. Select the **Add User** button.

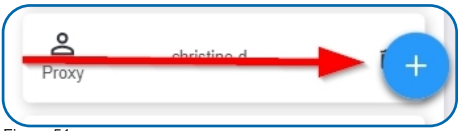


Figure 51

2. The Add User page will appear. Fill out all the text fields. The user name will autopopulate with the email address. The password must be at least eight characters.

Checking the box for "Is Administrator" gives the new user the ability to add new users to the account. By default, the box is not checked. Leave this box unchecked if you do not want them to have this ability.

After you have entered all the account information, select the **Submit** button.

Figure 52

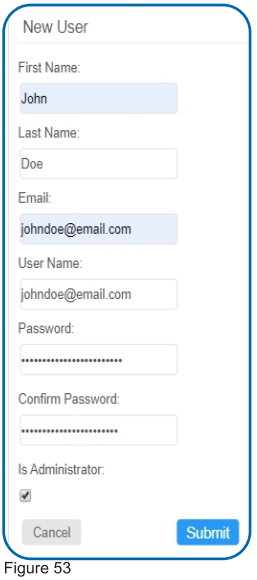


Figure 53

After submitting the new user information, the following tabs will guide you through editing their settings.

A. User Details lists new user's account information. This is where the password can be changed and reset. This information can be downloaded to your computer by clicking the cloud icon in the upper right corner.

B. User Permissions gives the administrator(s) the option of blocking users from having full access to the site.

Options include: Acknowledge Notifications, Edit Gateway Configuration, Password Unlock, and more.

C. User Preferences has a small list of custom settings for iMonnit.

D. Edit Notification Details is where you can adjust settings for how you want to be alerted about errors in sensors and gateways.

You can receive these alerts over email, text (SMS) messaging, or voicemail. By default, notifications will be off, if not adjusted. Activation can be accomplished by triggering the "Turn On Notifications" switch.

X. NETWORKS OVERVIEW

Figure 54

The following network list page allows you to edit details, create new sensor networks, and manage wireless gateways and sensors.

To have multiple, unlimited, networks is a feature available only for iMonnit Premiere members. Basic members will only be able to have one network and one account.

ADD A NEW NETWORK

1. Select the **New Network** button.

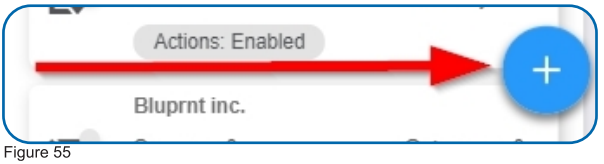


Figure 55

2. Enter the network name on the next screen. Select the **Save** button.

3. The next screen will have fields to customize the network:

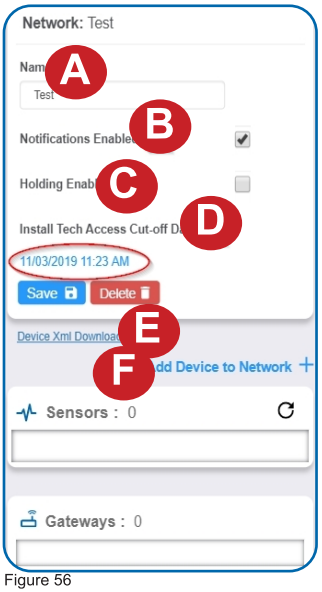


Figure 56

A. Name: This is the identifier the new network will be known by.

B. Notifications Enabled: Checking this box sets notifications to be sent from the network.

C. Holding Enabled: Checking this box sets this as a holding network. Sensor limits are not enforced and a gateway will not download the sensor to the network sensor list.

D. Install Tech Access Cut off Date: Presents the option to make changes to a device on the network during an install period. The date is set one day in the past by default.

E. Device Xml Download: Download an Xml file to a computer or mobile device.

F. Add Device to Network: Add devices to this new network. See page 6 of this guide for instructions. Remember that gateways must be added to the network before sensors.

EDITING A NETWORK

Choose any network from the list to edit the network. The network settings screen will be the same as above. Below that is a list of sensors and gateways that can be added or deleted.

The network edit page will display the option of changing the name of your network, enable notifications, enable holding, and review the Install Tech Access Cut-off Date. Remember to press the **Save** button after making any changes in this section.

Note: A sensor or gateway cannot be recovered once it has been deleted from the network. It is recommended that you export a sensor's data history before clearing it from the list.

XI. CREDITS OVERVIEW

Selecting “Credits” from the main menu opens a page to record notification credits for an account.

There are no credits required for E-mail notifications. There are also no credits required for External Provider SMS text (Short Message Service), which is not available in all areas.

Credits are required for Direct SMS and Voice Messaging based on the recipients country.

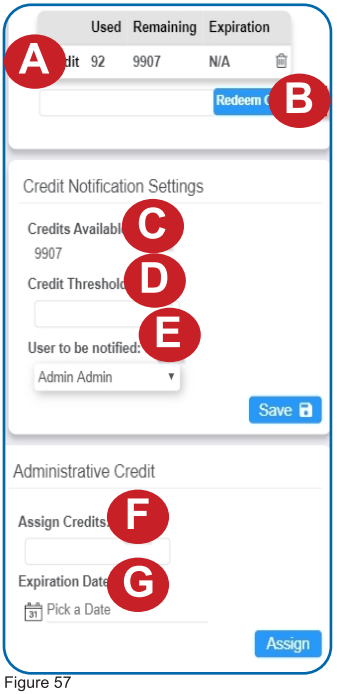


Figure 57

A. This is a running count of how many notification credits are on the account.

B. To redeem new notification credits, enter the code in this box and select the button for Redeem Code.

C. This box displays the number of credits available to be used.

D. This box displays the threshold for credit or limit they are allowed to reach.

E. Select the dropdown menu to choose a user to be notified.

F. This box enables the ability to assign Administrative Credits.

G. This box sets an expiration date for the Administrative Credits.

XII. SETTINGS OVERVIEW

Figure 58

Select the **Settings** tab to modify incorrect personal account information.

Account Number: This is a unique number for your account. If there is no account number, this entry will be the same as your name.

Company Name: This is an optional field for the Company Name. If there is no Company Name present this field will be the same as your name.

Primary Contact: This field displays your name along with your email. This a mandatory field as there must be a primary contact for the account to remain active so notifications can be sent.

Time Zone: There are a number of settings in iMonnit that are dependent on time. Set the time zone for your account here by first selecting a region and then a zone from the drop-down list.

Address, City, State, Postal Code, Country: These next few fields apply to your physical street address.

Recovery Email: An optional field for a secondary email address if your primary email cannot be reached.

Reseller: Check this box if you are a verified reseller.

Max Failed Logins: The maximum number of failed login attempts you wish to allow in order to protect your account from being hacked.

Remember to press the **Save** button after making any changes.

GENERATING A TOKEN

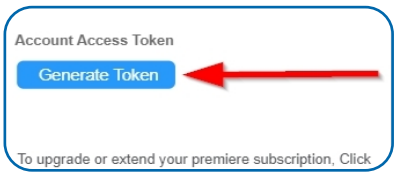


Figure 59

If you ever have to call into Monnit Technical Support, you may be asked to provide an Account Access Token. An Access Token is an alphanumerical code valid for 24 hours so Monnit support can assist with issues on the account. It can be extended or revoked if the problem is solved no longer wish to grant access.

- Scroll down to the Subscription section and select the **Generate Token** button
- Choose the button to receive the unique access code.

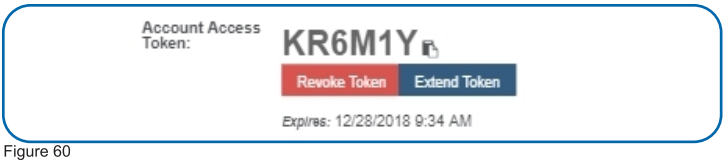


Figure 60

The code will automatically expire in 24 hours. Selecting the Extend button will grant a onetime week-long extension period before mandatory expiration. Choose the Revoke Token button to end access prior to the expiration date.

RENEWING A SUBSCRIPTION

Monnit Premiere Subscriptions are given out on a yearly basis. When it is time to renew, an email notification will be sent to let you know the subscription is about to expire.

You will need to verify that you have permission to create a certification before launching into the process. Do this by navigating to Users in the main menu.

Locate your account in the list. If you have a basic account, your name as the primary account holder will be the only one on the list. The availability of multiple users registered to one account is a feature only available on iMonnit Premiere.

Once in your account page, choose the **User Permissions** tab.

Verify that the checkbox for “Can Access Billing Pages” is checked. If the box is empty, check it and be sure to select the “Save” button before moving on.

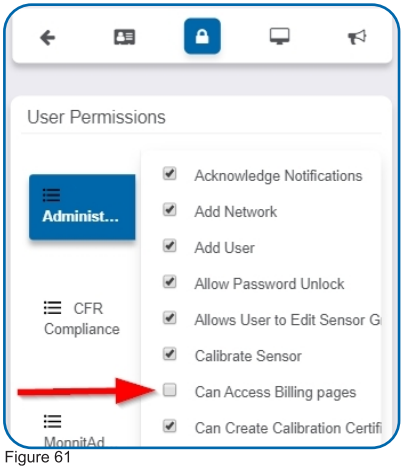


Figure 61

You must have a Monnit Store Account to renew your subscription. If you already have a login for the Monnit Store you may proceed on to the next section.

Return to the Account Settings’ Details page. Find the “Purchase Premiere” button located beneath the Subscription Key text box.

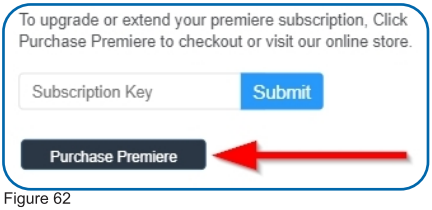


Figure 62

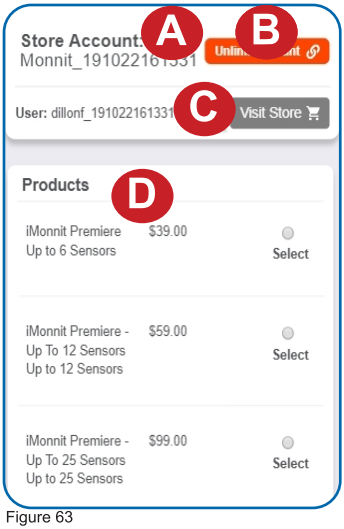


Figure 63

A. The new store name will be a combination between your iMonnit user name and the twelve-digit time stamp for when you created the account.

B. Unlinking your account will take you back to the login page.

C. Select this link to visit the online store and see what sort of options are out there to buy.

D. After you enter your card holder information, you can now move on to purchase a subscription to your account.

In the products section, you will see a list of iMonnit Premiere software. You must purchase a premiere account greater than the number of sensors registered to your account. If you have seven sensors, you cannot purchase “iMonnit Premiere for Up to 6 Sensors.” You need to select “iMonnit Premiere for Up to 12 Sensors” to support all your devices.

- Choose a radio button for the subscription you wish to purchase.
- Select the “Checkout” button.

You’ll be brought to the purchase screen.

The purchase screen will give you one last chance to review your shopping cart. Sales tax is automatically placed into the calculation of the price. This is software, so there is no added shipping cost. If everything meets your expectations, select the “**Purchase”** button.

The new subscription will be added to the list of Active Subscriptions on the Account Details tab.

XIII. WALLET OVERVIEW

Figure 64

Choosing the Wallet option in the main menu opens the page to input payment information. This will primarily be used to store card information used in renewing an iMonnit Premiere subscription.

ADDING A CARD

New cards can always be added in the “Add Card to Wallet” section. Fill out the typical credit card information including the Card Holder name, card number, expiration date and address. Then select the **Save** button.

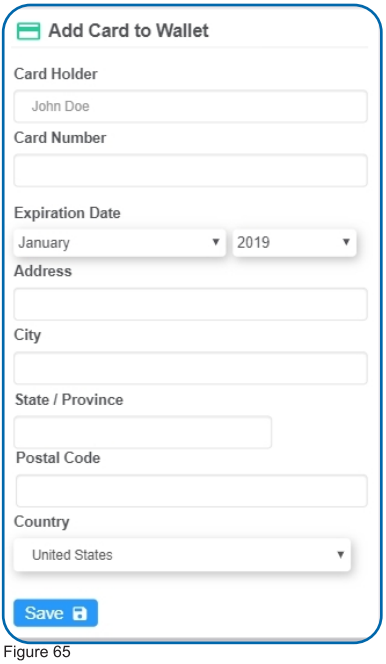


Figure 65

SUPPORT

For technical support and troubleshooting tips please visit our support library online at monnit.com/support/. If you are unable to solve your issue using our online support, email Monnit support at support@monnit.com with your contact information and a description of the problem, and a support representative will call you within 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 (Products) will be free from defects in materials and workmanship for a period of one (1) year from the date of delivery with respect to hardware and will materially conform to their published specifications for a period of one (1) year with respect to software. Monnit may resell sensors manufactured by other entities and are subject to their individual warranties; Monnit will not enhance or extend those warranties. Monnit does not warrant that the software or any portion thereof is error free. Monnit will have no warranty obligation with respect to Products subjected to abuse, misuse, negligence or accident. If any software or firmware incorporated in any Product fails to conform to the warranty set forth in this Section, Monnit shall provide a bug fix or software patch correcting such non-conformance within a reasonable period 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, shall bear the risk of loss and such costs of shipment of repaired Products or replacements, and shall credit 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 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.

MONNIT

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

Monnit, iMonnit and all other trademarks are property of Monnit, Corp. © 2020 Monnit Corp. All Rights Reserved.