



Remote Monitoring for Business

iMONNIT™ ENTERPRISE

iMonnit Enterprise Admin USER GUIDE

Version 4.0.1.0

TABLE OF CONTENTS

I. ABOUT IMONNIT ENTERPRISE	1
IMONNIT ENTERPRISE FEATURES	1
MINIMUM SYSTEM REQUIREMENTS	1
INSTALLATION RECOMMENDATIONS	1
II. PREREQUISITES	2
WEB SERVER	2
SQL SERVER	2
ACTIVATION KEY	3
III. INSTALLATION	4
DOWNLOAD	4
ENTERPRISE SETUP UTILITY	4
IV. ADMINISTRATIVE OVERVIEW	10
FIRST LOGIN	10
ENTERING ADMINISTRATION MODE	10
PROXY MODE	11
CREATE SUB-ACCOUNT	11
DEVICE LOOKUP	11
V. HOMEPAGE OVERVIEW	12
THE HOMEPAGE	12
VI. SENSOR OVERVIEW	13
ADDING A DEVICE	13
SENSOR DETAILS	13
VII. GATEWAY OVERVIEW	17
GATEWAY HISTORY OVERVIEW	18
GATEWAY ACTION VIEW	19
GATEWAY SETTINGS VIEW	19
VIII. ACTIONS OVERVIEW	25
CREATING AN ACTION	25
IX. SENSOR MAPS OVERVIEW	28
X. CHARTS OVERVIEW	29
XI. REPORTS OVERVIEW	30
EDIT REPORT SECTION	30

REPORT SPECIFIC PARAMETERS	31
XII. USERS OVERVIEW	32
XIII. NETWORKS OVERVIEW	33
EDITING A NETWORK	33
XIV. SETTINGS OVERVIEW	34
GENERATING AN ACCESS TOKEN	34
SUPPORT	35
WARRANTY INFORMATION	35

I. ABOUT iMONNIT ENTERPRISE

[iMonnit Enterprise](#) is available for large organizations with specific data/usage requirements. It provides the same feature set as the iMonnit Premiere online software but allows the organization to host and maintain their own sensor data.

Note: In order for gateways to be programmed for communication with your iMonnit Enterprise installation location, the gateways will need to be unlocked. You can purchase unlock codes for your gateway(s) on [Monnit.com](#).

iMONNIT ENTERPRISE FEATURES

- Installed on your company's computer servers
- Includes notification via SMS text and email (requires SMTP server)
- Export sensor data to CSV format
- A maintenance fee of 20% can be paid annually for new updates

MINIMUM SYSTEM REQUIREMENTS

- Windows Server 2012 or newer, 2 GB RAM, 2.0GHz Processor, ASP.NET Framework v4.5
- Web Server, IIS 7, ASP.Net MVC Framework v4.0
- SQL Server 2012 or Newer (Database Server)

No time to setup your own server environment?

Monnit has you covered with the [iMonnit Enterprise Appliance](#).

The iMonnit Enterprise Appliance is a ready-to-use Internet of things software and database solution that comes pre-installed and pre-configured on an optimized PC. Specifically designed for companies that want the added features and benefits of running an on-premises, dedicated version of the iMonnit Internet of Things software platform, without requiring an existing server environment or the hassle of configuring an existing server to work as an IoT optimized system. Contact Monnit Sales for more information at 801-561-5555 or email sales@monnit.com.

INSTALLATION RECOMMENDATIONS

We recommend that you have a resource familiar with Microsoft stack server deployments. This resource should understand IIS website configuration, SQL Server Management, and Windows Services. This could be a System Administrator, Developer, DBA or someone with similar experience.

If you do not have access to a resource, Monnit provides the following installation support options;

- Complete Enterprise Installation

Note: To utilize this service we will need temporary administrative remote access to the server.

- Enterprise Installation Support

II. PREREQUISITES

Before launching the installation process for iMonnit Enterprise, be sure that your web server and SQL Server are properly configured. You will also need an Activation Key.

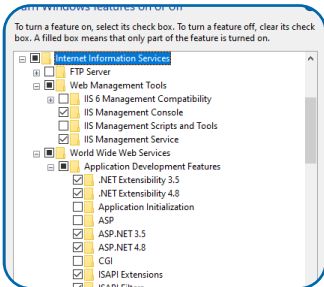


Figure 1

WEB SERVER

- Install or enable IIS 7
- Server OS (ex: server 2012) - Look inside Server Manager, Add Roll Web Server (IIS).
- When adding this role, make sure to add ASP.NET
- Example Steps: Desktop OS (ex: Windows 10)
- Open the **Control Panel** on your PC
- Select **Programs and Features**
- Look for **Turn Windows features on or off**. On

a Windows 10 OS, this is located in the bar off to the left.

- Open **Internet Information Services**.
- Check the boxes for **Web Management Tools** and **World Wide Web Services**.
- Choose **World Wide Web Services** and check all boxes under the application features. See Figure 1.
- When you click **OK**, it will start to reconfigure the PC and must reboot. You may also get an error message saying "Not all changes were made." If this occurs, the changes will be applied after rebooting.
- Install ASP.NET MVC4 from the Web Platform Installer. Download from here: <https://docs.microsoft.com/en-us/aspnet/mvc/mvc4>.
- Install an instance of Microsoft .Net framework 4.5. Download from here: <https://www.microsoft.com/en-us/download/details.aspx?id=30653>.

Note: Follow these steps in order to ensure the smoothest installation possible.

SQL SERVER

- Install an instance of SQL Server (2012 or later)
 - For small implementations (single or few networks) Express is sufficient: <https://www.microsoft.com/en-us/download/details.aspx?id=29062>
 - Download and install Service Pack as needed.
- During installation, make sure that you use mixed authentication mode.
- Create login credentials that can be used by the application to access the database.
 - SQL Express default server is (the computer name)\SQLEXPRESS
 - During setup, you must select either SQL Authentication or Mixed Mode Authentication (Windows Authentication and SQL Authentication).
 - You can use the default administrative account "sa" or create a secondary user and assign permissions to that user.

- Make sure you use a strong password, (i.e. at least 8 characters, letters, numbers, and special characters.).
- You can use SQL Server Management Studio to check and manage user permissions.

Note: SQL Server Management Studio 2012 requires Microsoft .net 3.5 service pack 1. In Server 2012, you need to go to server manager --> Features --> click add Feature and add .net 3.5.1.

If you are unfamiliar with managing SQL Server you may need to contract the aid of a database administrator to assist with the setup and configuration of the database and application.

ACTIVATION KEY

Before installation, you will need an activation key. You can purchase an activation key through the Monnit web store (www.monnit.com) or by contacting your sales representative. During the installation the activation is done online automatically. This does require temporary internet access for the computer where the installation is being done.

After you receive your activation key, keep it in a safe location. The key will only allow for activation of a single computer. However, if you ever need to re-install the software, you can use the same key on the same computer.

III. INSTALLATION

DOWNLOAD

Start by downloading iMonnit Enterprise installation files, available for download here: <https://www.monnit.com/support/downloads>.

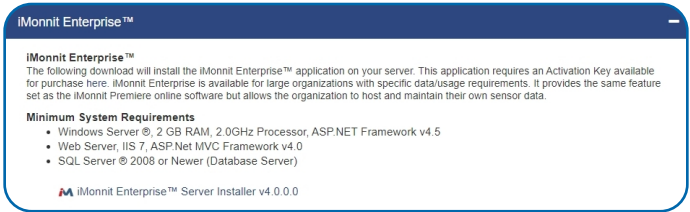


Figure 2

Run the installer by double-clicking the downloaded file. The installer will add the needed files to your hard drive. Multiple applications will be installed to enable the iMonnit Enterprise system to run properly. There is a step by step configuration wizard which will guide you through configuring each of the applications.

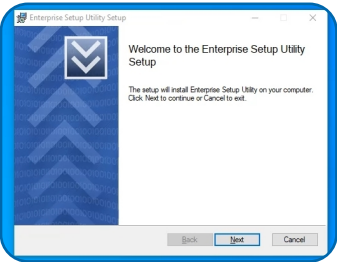


Figure 3

When the installer is finished, you will have a new icon on your desktop to launch the Enterprise Setup Utility.

ENTERPRISE SETUP UTILITY

Select the icon on your desktop to launch the Enterprise Setup Utility. You will be greeted with the welcome screen. Before choosing the **Begin Installation** button, navigate your cursor to the **Test Credentials** button. A successful test will look like the example in Figure 4. With your database connection verified, choose the **Begin Installation** button.



Figure 4

Activation

After you begin the installation, you'll be taken to the page to enter your Activation Key for authentication. Copy and paste your Activation Key in the text box and choose the **Activate** button. If your server is not connected to the Internet, you will need to use the manual activation process.



Figure 5

Manual Offline Activation

Follow these steps to complete your activation if the computer you are installing on cannot be given temporary access to the Internet for automatic activation.

After entering your Activation Key, if the configuration software is not able to communicate to the Internet, it will display the required form values for you to use to complete activation manually.

Using a web browser on an Internet connected device, navigate to:

<https://www.monnit.com/order/productActivation>

Enter the Manual Token into the form and press OK. Enter the Manual Key that is generated into the Enterprise Setup Utility to complete the manual activation.

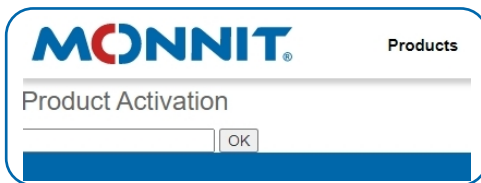
A screenshot of a web form titled "MONNIT Products" with a subtitle "Product Activation". Below the title is a text input field for a token, followed by an "OK" button. The form has a blue header bar and a blue footer bar.

Figure 6

Create Gateway Service

This is the server application that Monnit enabled gateways communicate with. When you click the **Create Service** button, you will see a command window come up and disappear. When this finishes, you can then select the **Next** button to continue.

A screenshot of a dialog box titled "Create Gateway Service". It contains two buttons: "Create Service" (disabled) and "Next" (active). Below the buttons, it says "Enterprise Wireless Gateway Service created successfully".

Figure 7

Internet Information Services (IIS) Website Configuration Setup

The website is the user portal you will use to view and configure Monnit sensors. This website will run in Microsoft Internet Information Services (IIS). IIS should have already been enabled as a prerequisite to installation.

Enter the information for IIS to be able to create your personal website experience. This step creates the website folder, application bindings, and the hosting site.

A. Physical Path - This field is where you will be storing the website folder. This field also configures IIS to where the folder is located.

B. IP Address - This field is the first of three binding fields. By default, this field is set to use all unassigned IP addresses, which means all requests to that server will land at that site. If you are using the same server for multiple websites, you may need to configure different IP Addresses.

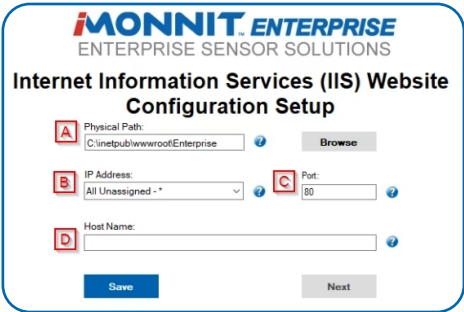


Figure 8

C. Port - This field is the second of three binding fields. By default, this field is set to use port 80, which means all requests to port 80 on the server's IP address will bring up the site.

D. Host Name - This field is the last of the three binding fields. By default, this field is set to be blank. If left blank, IIS will route all traffic to the configured IP Address and port to this website. Optionally, you can configure the host name so that only requests with this host are routed to the iMonnit Enterprise web application. This option allows IIS to host multiple sites on a single IP Address.

Database Connection and Testing

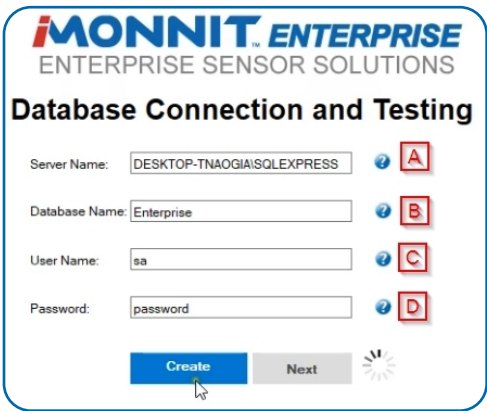


Figure 9

Enter the information to communicate with your SQL Server Instance. Before leaving this step, you will have tested communication with the database to ensure credentials are properly configured.

A. Server Name - This field is the server where your database is located. If you are using an instance name (default with SQL Server Express) the instance name will be included here also. Server can be either a DNS Resolvable host or an IP Address of the computer.

B. Database Name - This will be the name of the database. If you are upgrading and have an existing database make sure this name matches. If you are installing for the first time, the name entered here will be the name of the database that is created.

C. User Name - User authenticated to the database server for selected database.

*In order to ensure that the Enterprise database interprets values consistently, the default language must be set to English (US) for the database login that the application will be using.

Here is a sample script to update an existing login. Replace {LoginName} with the username of the Login to update:

```
ALTER LOGIN {LoginName} WITH DEFAULT_LANGUAGE = English
```

Or if you prefer to create a login. Replace {variables} as needed:

```
USE [{YourDatabaseName}]
```

```
CREATE LOGIN {PreferredLoginName} WITH PASSWORD=N'{password}',  
DEFAULT_DATABASE=[{YourDatabaseName}], DEFAULT_LANGUAGE=[{English}],  
CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
```

```
GO
```

```
USE [{YourDatabaseName}]
```

```
CREATE USER {PreferredLoginName} FOR LOGIN {PreferredLoginName}; EXEC  
sp_addrolemember N'db_owner', N'{PreferredLoginName}' EXEC sp_addrolemember  
N'db_datareader', N'{PreferredLoginName}' EXEC sp_addrolemember N'db_datawriter',  
N'{PreferredLoginName}'
```

```
GO
```

D. Password – Password for user to gain access to database.

SMTP MAIL SERVER SETUP

This step creates a connection to your SMTP server, so that the application can send notifications. This information can point to an email server, a SMTP forwarder, or a transactional email service.

A. SMTP Host - This field is the address of your SMTP server i.e. www.smtphost.com.

B. Port - This field is the port that your SMTP server uses.

C. User - This field is the admin email account that will be used to send notifications i.e. username@hostname.com.



The screenshot shows the 'MONNIT ENTERPRISE ENTERPRISE SENSOR SOLUTIONS' logo at the top. Below it is the title 'SMTP Mail Server Setup'. The form contains several input fields with corresponding labels: 'SMTP Host' (with a placeholder 'smtp.yourhostname.com'), 'Port' (with '25'), 'User' (with 'username@hostname.com'), 'Password' (with 'password'), 'Use SSL' (a dropdown menu set to 'True'), 'From Email Address' (with 'username@hostname.com'), 'From Name' (with 'Name of Company Sending Email'), and 'Return Path' (with 'username@hostname.com'). To the right of each input field is a blue circular icon with a question mark. On the far right, there is a vertical column of eight red square buttons labeled 'A' through 'H'. At the bottom of the form are two buttons: 'Test Email' (highlighted in blue) and 'Next' (with a mouse cursor icon pointing to it).

Figure 10

D. Password - This field is for the password to the email account which will be used to send notifications.

- E. Use SSL** - This field determines if your SMTP server uses SSL or not.
- F. From Email Address** - This field is the email address that will be sending out the notifications. This field can be different from the User field.
- G. From Name** - This field is used as the name of the company or the name of the person sending the notification.
- H. Return Path** - This field is typically the same as the user to negate spam issues with other SMTP servers.

Emails and Gateway Server Behavior

This step determines the type of Notifications which will be sent, what port the Gateway Service should be using, and if any inbound packets from all gateways or a specific gateway should be logged in the database.

Figure 11

for gateways to send information. Default is Any: 3000 or 192.168.0.2:3000

- E. Inbound Packet Retention** - This field determines if any gateway messages are stored in the database for troubleshooting.

Firewall Rules

This step creates an inbound firewall rule in Windows Firewall for both TCP and UDP. If you have additional firewalls you will need to also create rules for traffic coming from the gateways to the server.

- Inbound Port** - This field needs to be the same port used for “Address to Listen On”.

Figure 12

Wireless Gateway Server Test

This step tests if gateways will be able to speak to the database using the gateway service. Because this is run from the same computer as the service is running, it will bypass any firewalls.

Host Address - This field, by default, uses the specific servers NIC Card's IP Address if the test is successful the installation is complete.

iMONNIT™ ENTERPRISE
ENTERPRISE SENSOR SOLUTIONS

Wireless Gateway Server Test

Host Address: ?

Test Service

Finish

Service is Running
Attempting 192.168.110.210:3000
DNS Resolve: 192.168.110.210
TCP Connect Success
Message sent.
Message Received

Figure 13

IV. ADMINISTRATIVE OVERVIEW

The interface was created such that the administrative accounts can access the sub-accounts for administrative purposes. From your Administrative account, you will have access to an Administrative menu option from which you will be able to manage the sub-accounts, troubleshoot problems, find devices, check statuses, manage subscriptions, create new accounts, proxy into sub-accounts, and more. As a user of an administration account, all permissions can be managed from the green permissions link. In fact, when you are visiting the sub-accounts, you can do everything that the user of that sub-account can do, without limitations.

FIRST LOGIN

Navigate in your browser to the web application you created in IIS. Type "localhost" into the address bar to be guided to the Enterprise login screen. The credentials that are set when you first install the database are:

Administrative Account

Username: Admin

Password: password

*The Administrative account will be used for adding Accounts/Subaccount, adding Users, handling permissions, and making changes at the Account level. You will not want to add your Networks, Sensors, and Gateways to this Account.

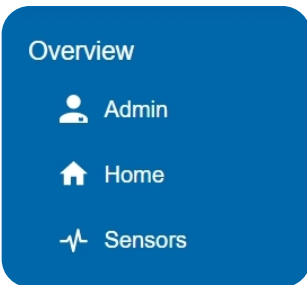


Figure 13

ENTERING ADMINISTRATION MODE

After logging in as a user of the administration account, an "Administration" link will appear on the main navigation menu.

Clicking this link will take you to the Account Search Screen.

You can easily search for accounts by typing part of their Account Number, Company Name, or name of the primary contact assigned to their account.

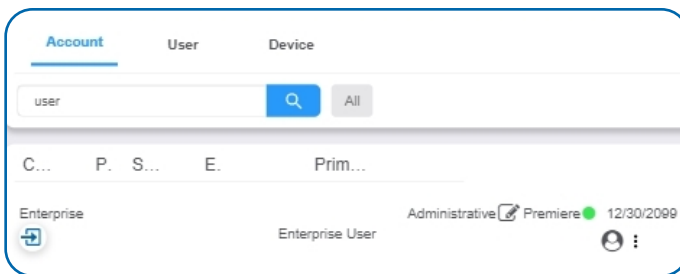


Figure 14

From this screen you can:

- Search for a specific account
- Manage the networks and devices on the account.
- View the detailed account information and user list.
- View details of the primary contact.
- Enter Proxy mode to view the account logged in as the primary contact.
- Create new Accounts so you can manage different clients logically.
- Clear items temporarily cached by the website so you don't have to wait for the cache to reset on its own.

Other pages you can see as an Administrator are "Portal," "Devices," and "Server."

PROXY MODE

Arrive here by clicking one of these icons on any user name in your search.



While in Proxy Mode you will have access to the account as if you used their credentials to log into the site. When you click the silhouette icon you'll see which account you are viewing at the top of the dropdown menu.

Using Proxy allows you to see the interface just as that user would. You will have the same privileges as the person you are logged in as and will be able to see and edit only the networks and accounts they can access.

CREATE SUB-ACCOUNT

Create a sub-account by first choosing "Portal" from the main navigation menu. Then select "Create Sub-Account" from the secondary menu. This will open the page to create a new account.

You will be asked to enter your account information in the following fields.

LOG IN

CREATE ACCOUNT

First Name *

Last Name *

Email *

User Name *

Password *

Confirm Password *

Account Name *

(Must be unique)

Subscription Code

(Free Trial if left blank)

Time Zone *

Figure 15

When completed, select the "Next" button. This step will complete the sub-account creation process and lead you onto registering your device. For steps on registering a device see the "Sensor Overview" section of this guide.

DEVICE LOOKUP

You can look up a device by choosing the "Device" tab on the Administration account home page. The Device Lookup report will help you identify where a sensor or a gateway belongs and a small snapshot of its status. For instance, if you have a sensor in your inventory but don't know where it is assigned, you can enter the Sensor ID and this report will identify which account and network the sensor is assigned to along with the sensor's name and the current status/last check in date.

V. HOMEPAGE OVERVIEW

THE HOMEPAGE

From the iMonnit Enterprise 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.

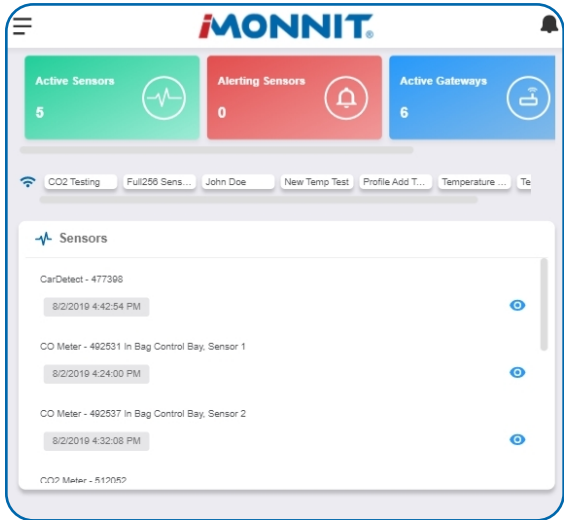


Figure 16

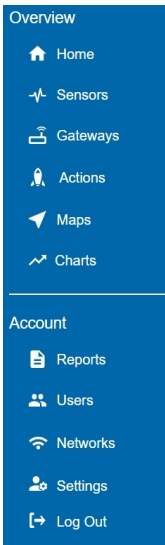


Figure 17

Main Navigation Menu

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 floor-plans and position sensors where they are located in your environment.
- **Charts** - Compare multiple charts for all your sensors.

ACCOUNT

- **Reports** - Assemble detailed summaries for your system.
- **Users** - Modify all permissions and settings for users on your account.
- **Networks** - Review and edit all networks on your account.
- **Settings** - Adjust account preferences.
- **Log out** - Log out of Enterprise.

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

VI. SENSOR OVERVIEW

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

ADDING A DEVICE

Gateways and sensors are added the same way.

- Start by choosing the **Add Sensor** button.
- If you have multiple networks, you can select which network you wish to add the device to from the dropdown menu. You have the option of adding one device or multiple.
 - Multiple devices uploads require .csv file with the device id and security code for each sensor. **Do not include the device name or any other information in the .csv file.** Upload the file on the multiple devices page and your new sensors will be added to Enterprise.
- The Device ID and Security Code are included on your sensor label.
 - The Device ID is a set of six numbers.
 - The Security Code is a set of six capital letters.
- If you are adding one device, enter the Device ID and Security Code in the corresponding text boxes. Then choose the **Add Device** button.

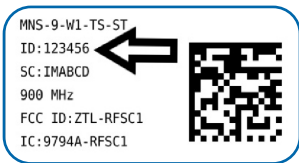



Figure 18

Choose the **Continue** button after adding your device. Review your sensors on the next screen.

Add Device

 Switch Network

Network: Network

Device ID

Code

Add Device

SENSOR DETAILS

With your sensor(s) now added and reporting to a gateway, a list of all your sensors will appear on the Sensor List page. Choosing any sensor will bring up the following information.

A tab bar across the top of the page is as follows:

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 Page

The Sensor Details Page will be the first page you see when choosing a sensor from the list.

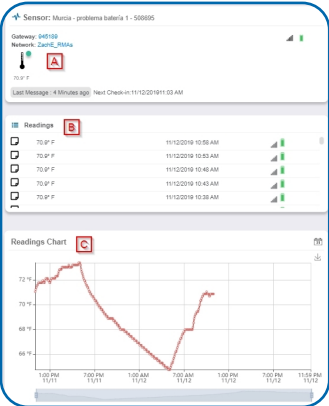


Figure 19

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.

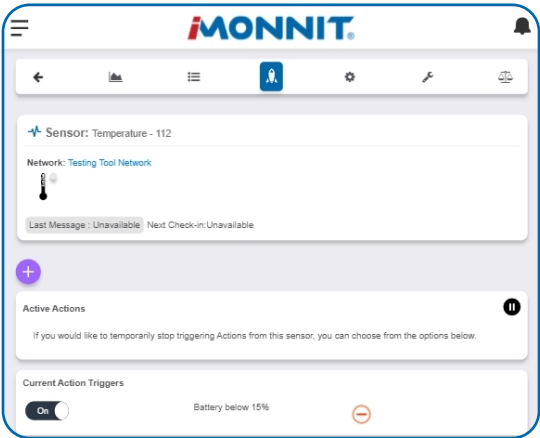



Figure 20

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 field:

MessageID: Unique identifier of the message in our database.

SensorID: 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 are 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.

The screenshot shows the 'Temperature Settings' page. It includes fields for 'Sensor Name' (set to 'Temperature 1'), 'Heartbeat Interval' (120), 'Aware State Heartbeat' (120), 'Sensor is on' (All Day), 'Assessments per Heartbeat' (1), 'Use Aware State' (Below and Above thresholds), 'Below' (-40), 'Above' (257), 'Aware State Buffer' (0), 'Synchronize' (Off), and 'Failed transmissions before link mode' (2). Red boxes labeled A through I are placed over the following elements: A (Sensor Name field), B (Heartbeat Interval field), C (Aware State Heartbeat field), D (Assessments per Heartbeat field), E (Below threshold field), F (Above threshold field), G (Aware State Buffer field), H (Synchronize toggle), and I (Failed transmissions before link mode field).

Figure 21

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°. Similarly at the Minimum Threshold the temperature will have to rise a degree above the threshold to return to Standard Operation.

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.)

VII. GATEWAY OVERVIEW

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 concentrator 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.

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).

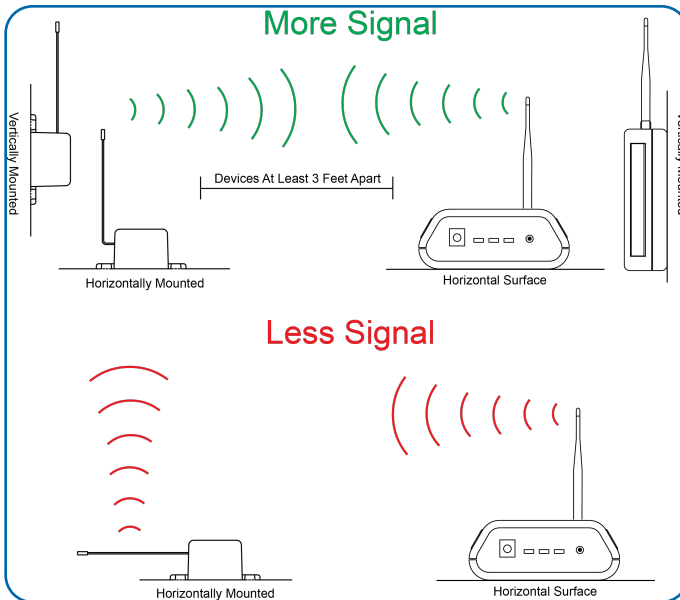


Figure 22

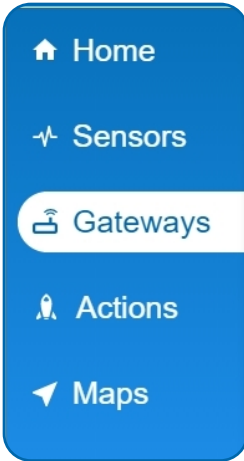


Figure 23

On iMonnit Enterprise, 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 24

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. Actions – This will display a list of all the actions you have under this gateway. If you have not assigned any actions to this gateway, the page will be blank.

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


D. Sensors – 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
06/10/2020 08:27:31	Data		Line Powered	3
06/10/2020 08:27:17	Data		Line Powered	24
06/10/2020 08:27:16	Data		Line Powered	42
06/10/2020 08:12:29	Data		Line Powered	24
06/10/2020 08:08:33	Data		Line Powered	10
06/10/2020 08:08:48	Data		Line Powered	43

Figure 25

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.

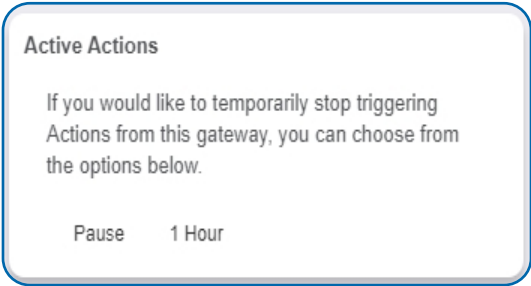


Figure 25

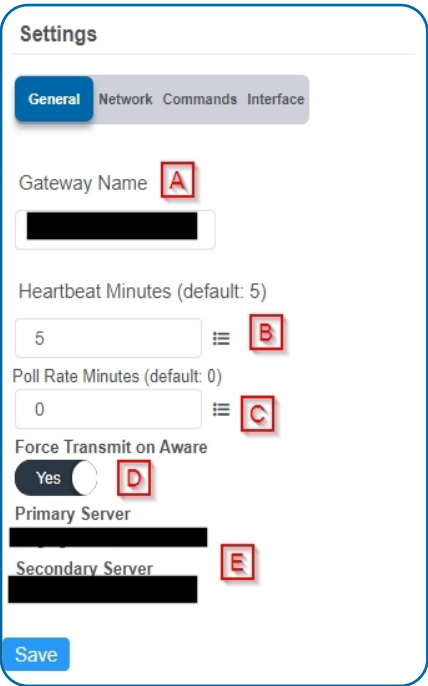


Figure 26
Setting a poll rate allows your gateway to check for priority incoming messages more frequently —while using a fraction of the data of a regular message exchange. Your gateway asks the server if there are any priority incoming messages, and if there are, they are exchanged immediately. If not, no messages are exchanged until your gateway has its next regular heartbeat.

GATEWAY SETTINGS VIEW

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

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

Settings

General Commands

Gateway Name

LTE Gateway

Heartbeat Minutes (default: 15)

15

IMSI

0000000000000000

ICCID

00000000000000000000

IMEI

0000000000000000

Force Transmit on Aware

Yes

Gateway Power Mode

Standard

Save

Figure 27

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 the gateway to identify it 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.

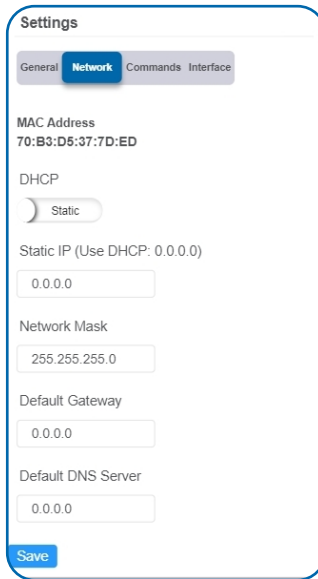
G. Gateway Power Mode is a dropdown menu to select how much power your gateway uses. Choose between Standard, Force High Power, or Force Low Power.

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**.



The screenshot shows a 'Settings' window with a 'Network' tab selected. The 'MAC Address' is '70:B3:D5:37:7D:ED'. The 'DHCP' toggle is set to 'Static'. Below it, the 'Static IP (Use DHCP: 0.0.0.0)' field is '0.0.0.0'. The 'Network Mask' field is '255.255.255.0'. The 'Default Gateway' field is '0.0.0.0'. The 'Default DNS Server' field is '0.0.0.0'. A 'Save' button is at the bottom left.

Figure 28

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 alphanumeric 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.

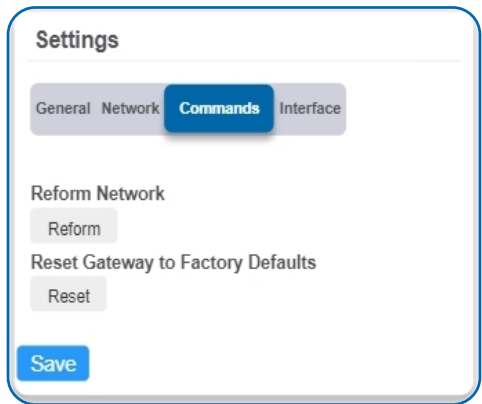


Figure 29

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

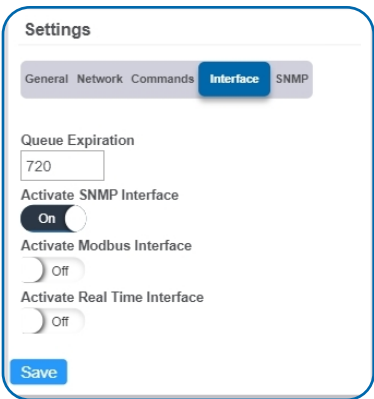


Figure 30

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.

Settings

General Network Commands Interface **SNMP**

SNMP Interface 1

SNMP Address
0.0.0.0

Port
161

Trap Active
☐ Off

Trap Port
162

SNMP Interface 2

SNMP Interface 3

SNMP Interface 4

Save

Figure 31

- **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 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.

Settings

General Network Commands Interface **Modbus**

TCP Timeout (Minutes)
5

Port (default: 502)
502

Save

Figure 32

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 Enterprise 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.
- **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.

Settings

General Network Commands Interface **Real Time**

TCP Timeout Seconds (default: 1.17 seconds)

1

Port (default: 3500)

3500

Save

Figure 33

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.

Sensors whose last communication came through this gateway (Count: 4)

Sensor ID	Sensor Name	Last Communication Date
		12/21/2018
		12/21/2018
		12/21/2018
		12/21/2018

Figure 34

VIII. 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.

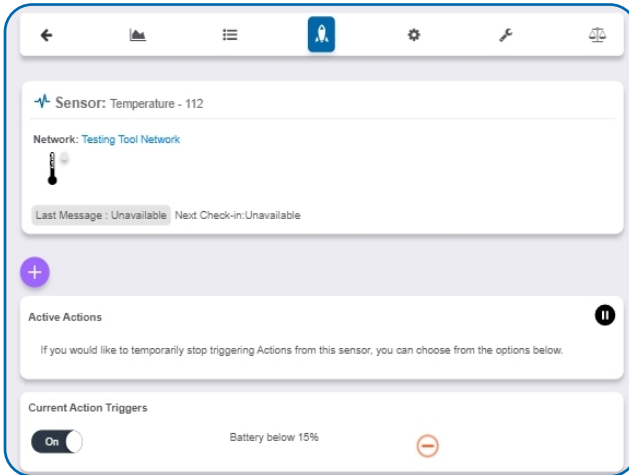


Figure 35

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.

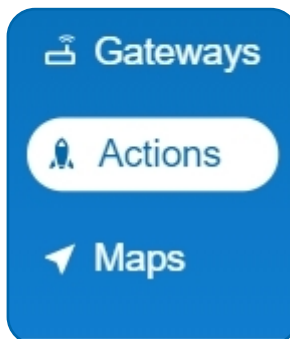


Figure 36

- 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.

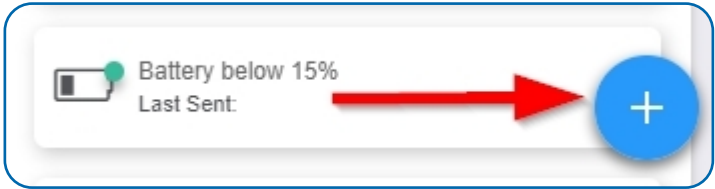


Figure 37

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.

- 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.

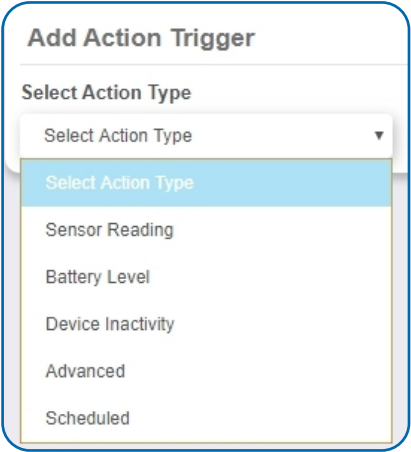


Figure 38



Figure 39

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.

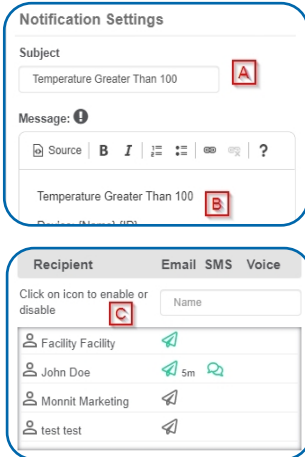


Figure 40

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.

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

- A. Configure the subject for the notification.
- B. Customize the message body for the notification
- C. The recipient list identifies who will receive the notification.

- Select the icon next to a user to configure how they will be notified.
- Decide 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.

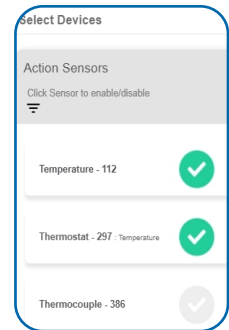


Figure 41

IX. SENSOR MAPS OVERVIEW

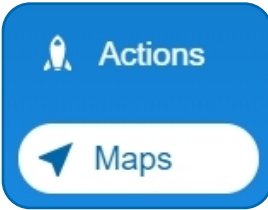


Figure 42

The Maps feature gives you the option of uploading your floorplan or other image to Enterprise 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.

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.

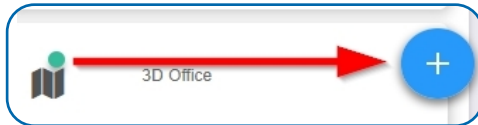


Figure 43

- 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.

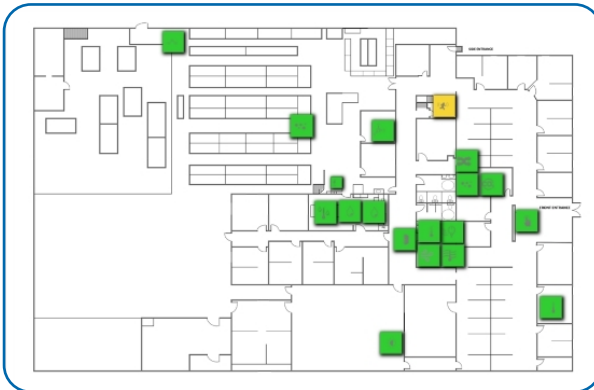


Figure 44

X.CHARTS OVERVIEW

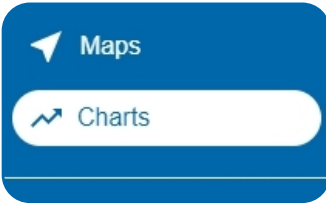


Figure 45

A. Calendar - This is where you can select which period you wish to compare sensor data from. By default, charts pull information from the past seven days.

B. Name - Search for a specific sensor in your list by typing it into the name field.

C. Network - If you have more than one sensor network, you can choose it here. If you only have the one, there will be no dropdown menu.

D. Sensors Selected - Totals the number of sensors you've selected to chart.

E. List - All sensors are listed alphabetically for you to make your selections.

When you're ready, choose the **Chart Sensors** button to view the graphs.

Sensor readings are charted on graphs located on the Sensor Details page, but you can also compare multiple charts through a selected date set through the "Charts" option on the main menu.

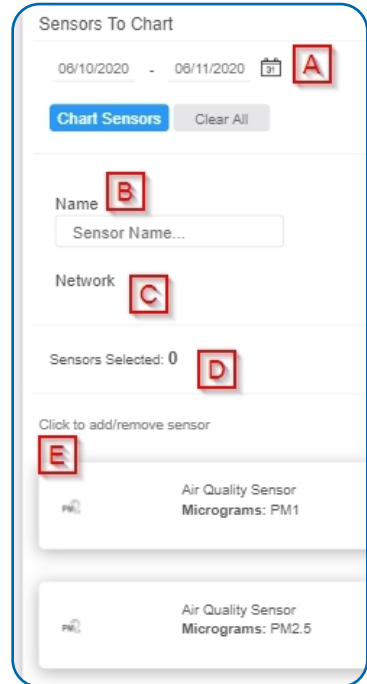


Figure 46

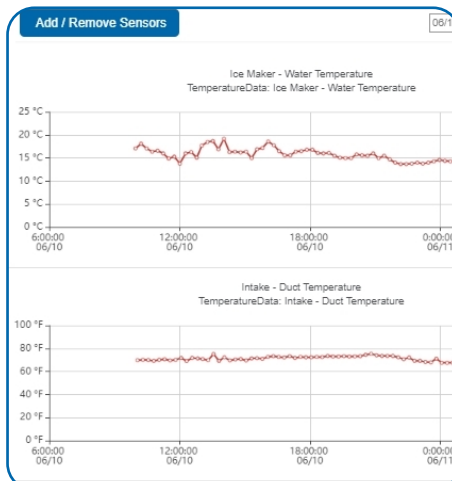


Figure 47

XI. REPORTS OVERVIEW

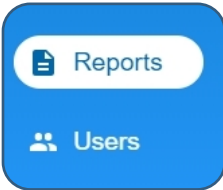


Figure 48

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.

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



Figure 49

- Choose a Report Template.

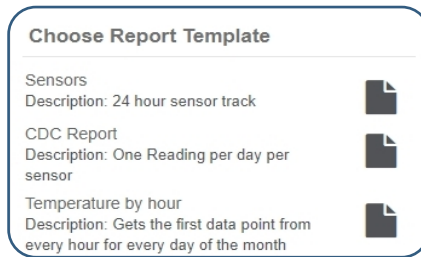


Figure 50

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

EDIT REPORT SECTION

Figure 51

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

- 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.

Report Specific Parameters

Network ID A

John Doe (11883) ▾

Data start hour B

12:00 AM ▾

Include Sensor Name C

True ▾

Include Date D

True ▾

Include Value E

True ▾

Include Formatted Value F

True ▾

Include Battery G

True ▾

Figure 52

- 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.

Include Data H

False ▾

Include Sensor State I

False ▾

Include GatewayID J

False ▾

Include Alert Sent K

False ▾

Include Signal Strength L

False ▾

Include Voltage M

False ▾

Include Special N

False ▾

Cancel


Save 

Figure 53

XII. USERS OVERVIEW

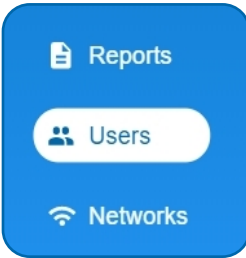


Figure 54

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.

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



Figure 55

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.

A 'New User' form with the following fields: 'First Name:' with a text input containing 'John'; 'Last Name:' with a text input containing 'Doe'; 'Email:' with a text input containing 'johndoe@email.com'; 'User Name:' with a text input containing 'johndoe@email.com'; 'Password:' with a password input field; 'Confirm Password:' with a password input field; and 'Is Administrator:' with a checked checkbox. At the bottom are 'Cancel' and 'Submit' buttons.

Figure 57

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.

XIII. NETWORKS OVERVIEW

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.

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

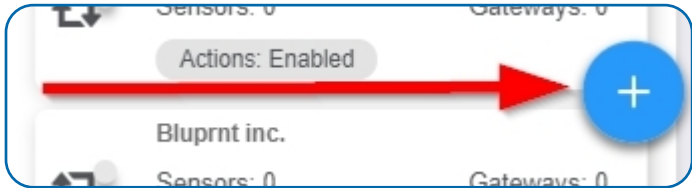


Figure 58

2. Enter the network name on the next screen. Select the **Save** button.
3. The next screen will have fields to customize the network:

A screenshot of the 'Network: Test' customization screen. It contains several fields and buttons: 'Name' (labeled A) with a text input containing 'Test'; 'Notifications Enabled' (labeled B) with a checked checkbox; 'Holding Enabled' (labeled C) with an unchecked checkbox; 'Install Tech Access Cut-off Date' (labeled D) with a date picker showing '11/03/2019 11:23 AM'; 'Save' (labeled E) and 'Delete' buttons; 'Device Xml Download' (labeled E); 'Add Device to Network' (labeled F) with a plus icon; and sections for 'Sensors : 0' and 'Gateways : 0' with empty input fields.

Figure 59

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.

XIV. SETTINGS OVERVIEW

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 Enterprise 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 AN ACCESS TOKEN

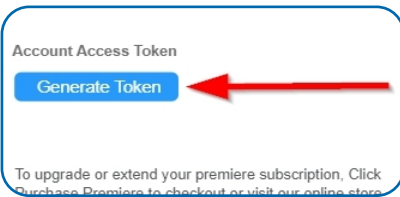


Figure 60

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

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 alphanumeric 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.

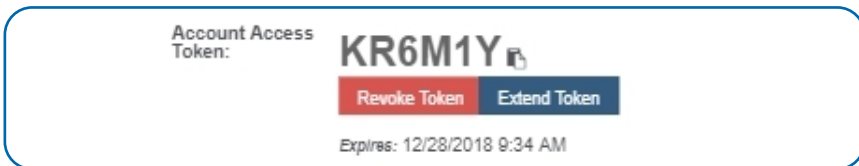


Figure 61

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.

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



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.