Mobiliya

Asset Tracking

Admin Guide - Version 1.0.0

September2017

Table of Contents

1. About this Guide

This guide is a user guide for Asset Tracking solution provided by Mobiliya. This will walk the user through the setup instructions & usage instructions required for using the solution.

2. About Mobiliya's Asset Monitoring Solution

Mobiliya's asset monitoring and tracking solution is a complete smart inventory management tool. The solution provides a web dashboard & a mobile application to Monitor, Locate and Report all the remote assets so that they are completely visible 24x7.

3. Intended Audience

This guide is intended for facility managers who want to use the system.

4. Pre-requisites

a. Assuming that the deployment is completed, admin must have a minimum of 1 gateway.

b. 2 sensors which will send data to gateway.

c. Mobile Application, can be downloaded from here.

d. Web application Login URL: https://<Front-end web app name>.azurewebsites.net

e. Rest API URL for Mobile app & Gateway: https://<Back-end web app name>.azurewebistes.net

f. Gateway download package location: https://<>

g. Each asset should have an asset barcode.

h. Setup

5. Setup

a. Software Setup

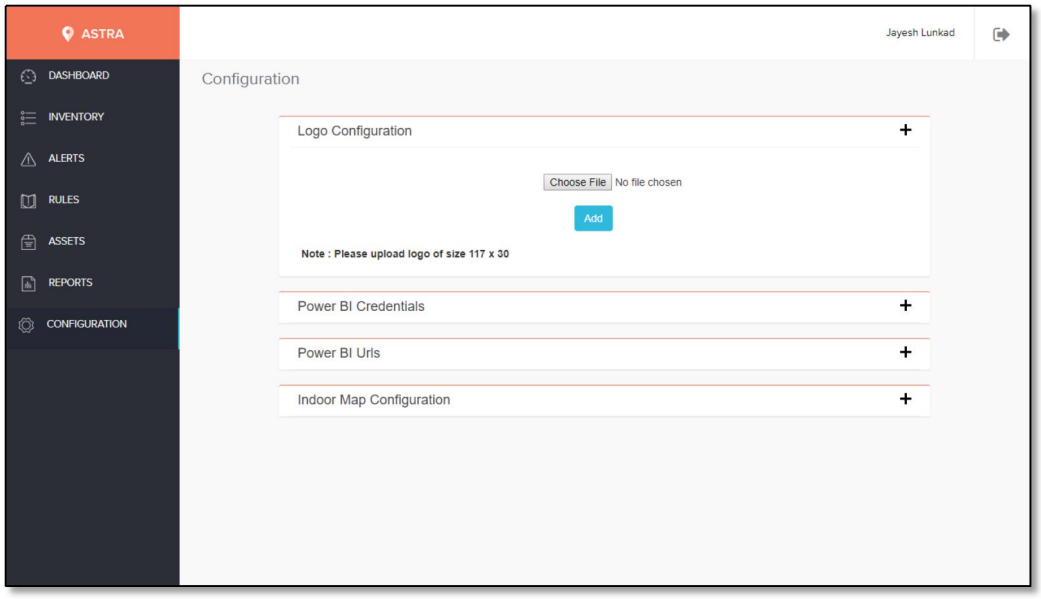
i. Configuration

a. ***Logo Configuration***

Admin can configure organization logo from this section:

1. Click on **Choose File** and choose an image file of respective organization logo.

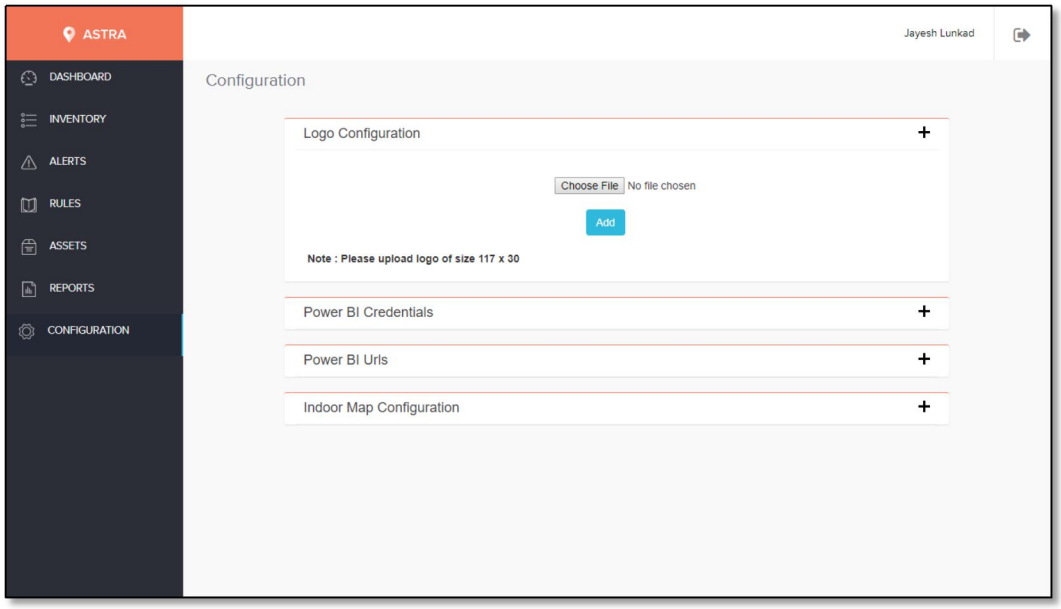
2. Click on **Add** button to update. Once the file is uploaded, the system will prompt a success notification.



b. Power BI Credential

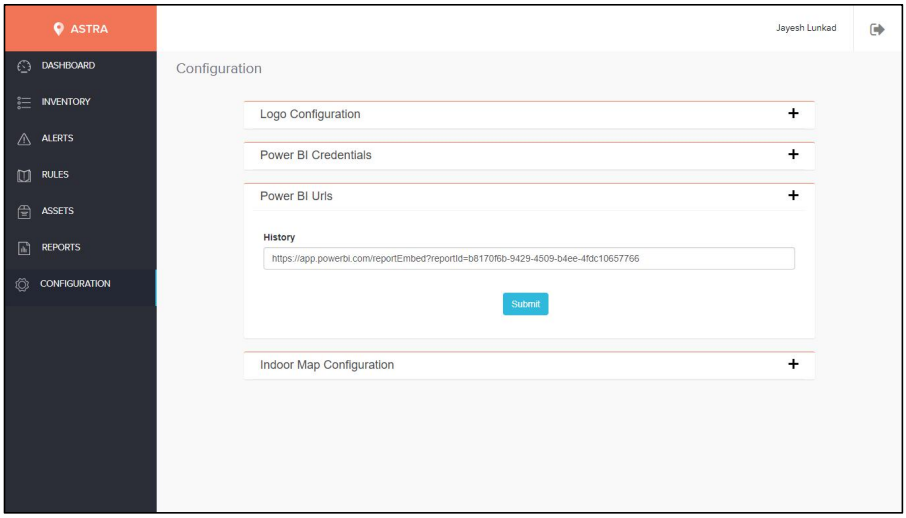
Admin must enter the following credentials to configure Power BI:

1. Client ID
2. Client Secret
3. Username
4. Password



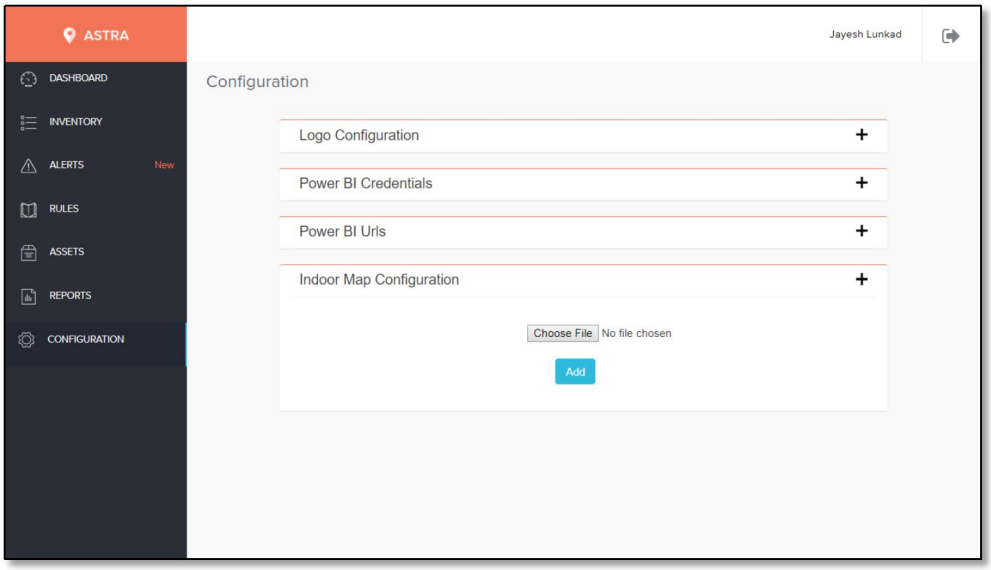
c. Power BI URLs

History report URL must be entered here which was published during the setup of the system.



d. Indoor Map Configuration

Admin must upload Indoor Map in this section which will enable in position the gateways on the uploaded map later.



b. Hardware Setup

Device	Product Link
Dell 5000 Gateway	https://www.dell.com/en-us/work/shop/gateways-embedded-computing/edge-gateway-5000/spd/dell-edge-gateway-5000/xctoi5000us
BT Dongle	
Sensortag 2650	https://store.ti.com/cc2650stk.aspx
Mobile Device	IOS: Above 8.0 Android: 5.x (Lollipop) to 7.x (Nougat)

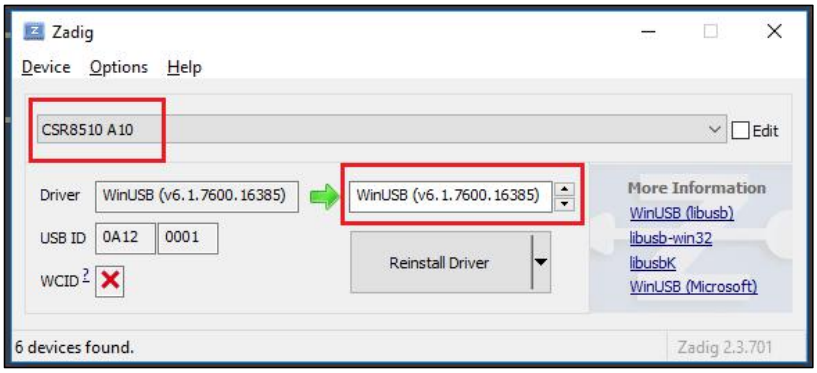
1. Connectivity

1. Ensure that the gateway has internet connection
2. Turn on Bluetooth of the gateway

2. Add Gateway

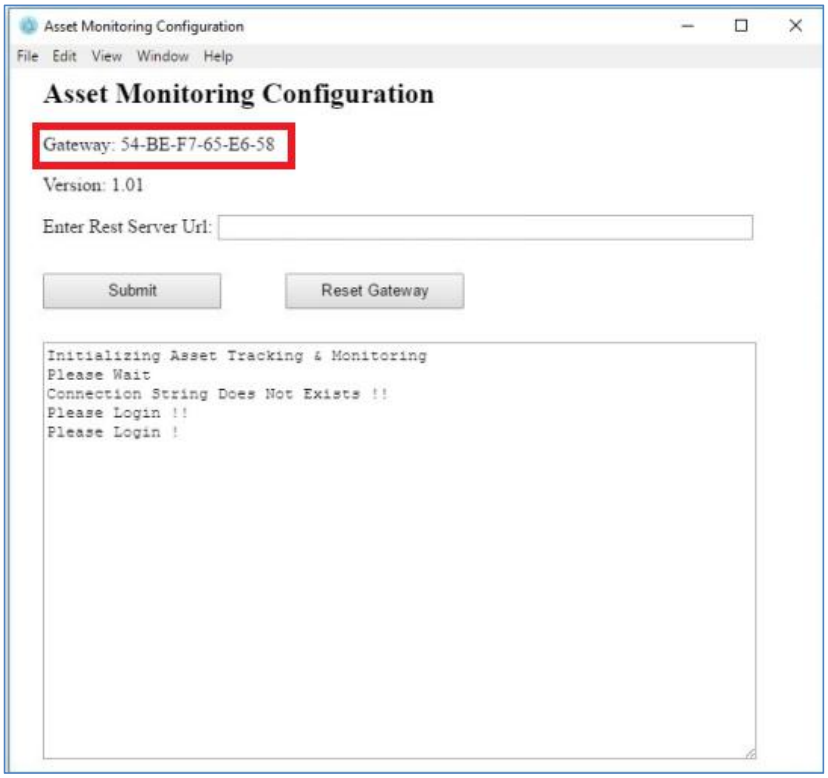
Admin must register on the web portal before proceeding as mentioned in this section. To add a gateway:

1. Download gateway Package by following below steps:
    i. Turn on the **Gateway**.
    ii. Download electron package from <URL>
    iii. Extract zip file and open *gateway-middleware-win32-x64* folder.
    iv. Follow the step to Install **WinUSB** driver
        1. Download **Zedit** from http://zadig.akeo.ie/
        2. Install and run downloaded **exe file**.
        3. Select **USB** device and **Driver**. Click **Reinstall**.

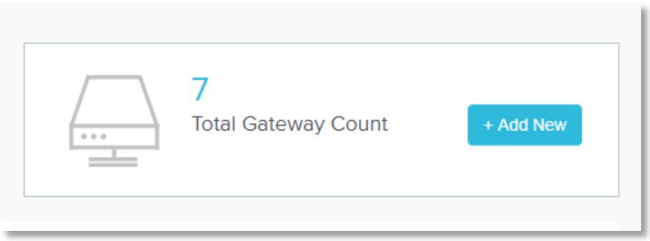


v. Double click on ***gateway-middleware.exe*** file

vi. Gateway window will open. Note the Gateway Key.



2. Now, from the web portal, choose Inventory section. Click on **+Add New** in Total Gateway count section.

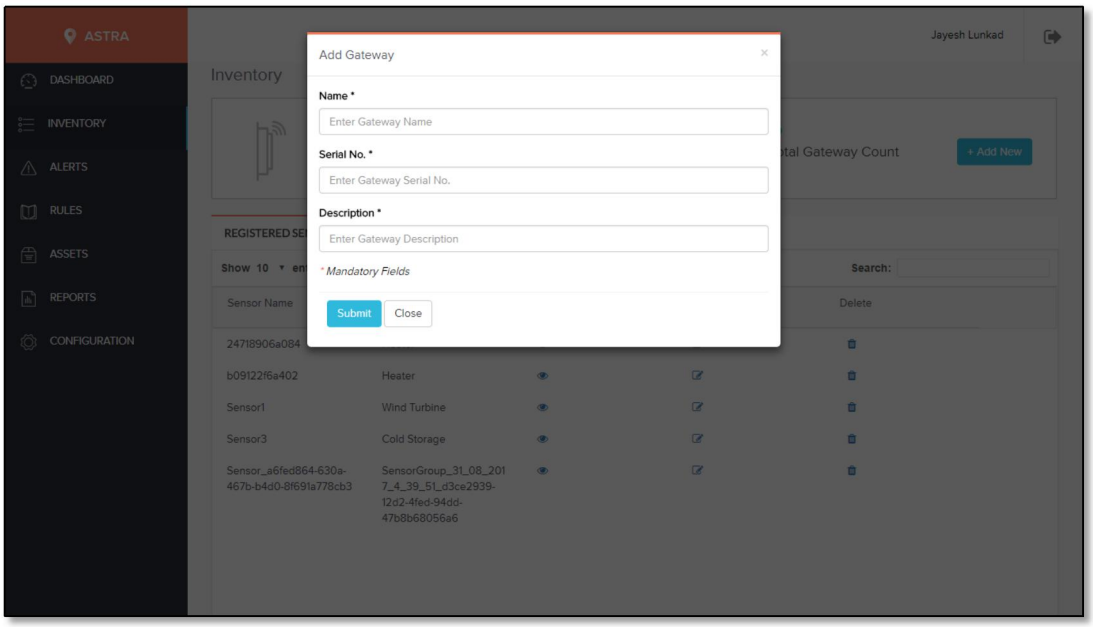


3. Enter **Gateway Name**, **Serial Number** and **Gateway Description**. Click on Submit to finish.

Gateway Name: Any meaningful name for the gateway. Ex: Floor 1 Gateway etc.

Serial Number: Enter the Gateway key as noted down in previous step.

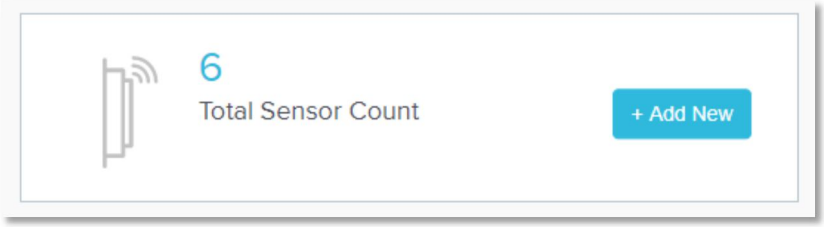
Description: Any description about gateway.



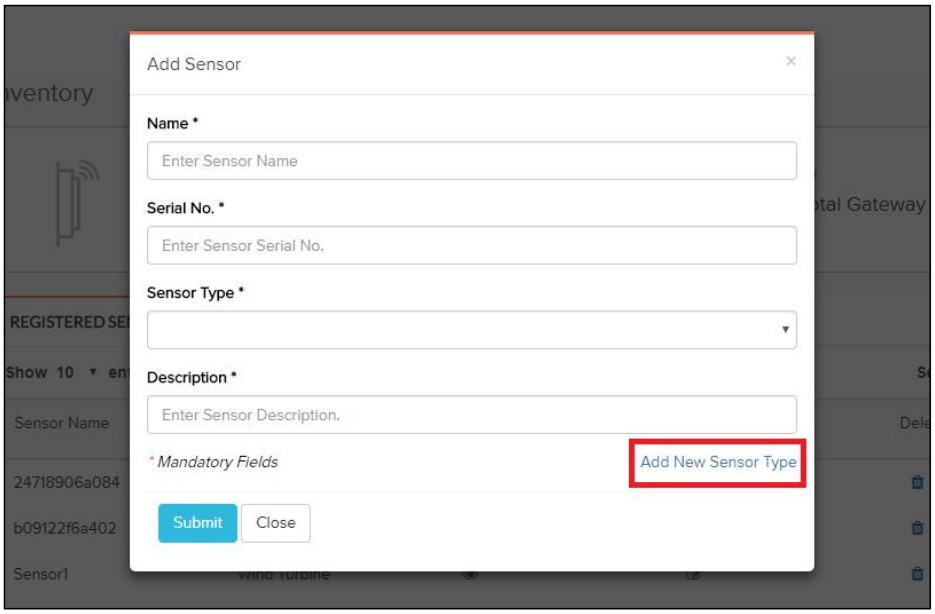
4. Follow steps mentioned in this section for each new gateway in order to on-board the gateway.

3. Add Sensor Type

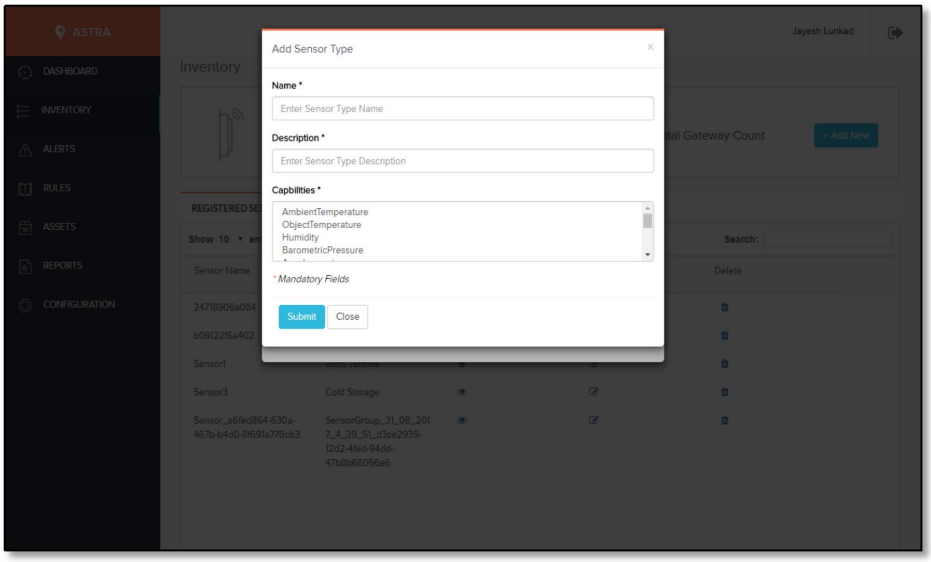
1. Click on Inventory. Click on **+Add New** in Total Sensor Count section.



2. Click on **Add New Sensor Type**



3. Enter **Name**, **Description** and choose multiple capabilities which are supported by the sensor.

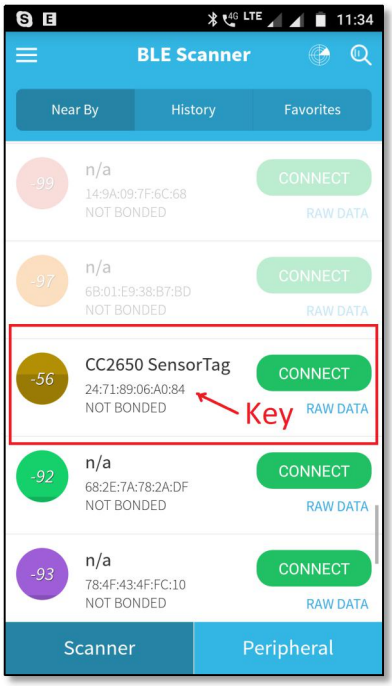


4. Add Sensor

User must provide sensor details to on board a sensor:
Name: Enter a sensor name. E.g.: Room 1 Temperature Sensor
Serial No: Enter the sensor key in this field. Admin must keep note of the sensor key as it will be used later in the flow. Follow the steps given below to find it:

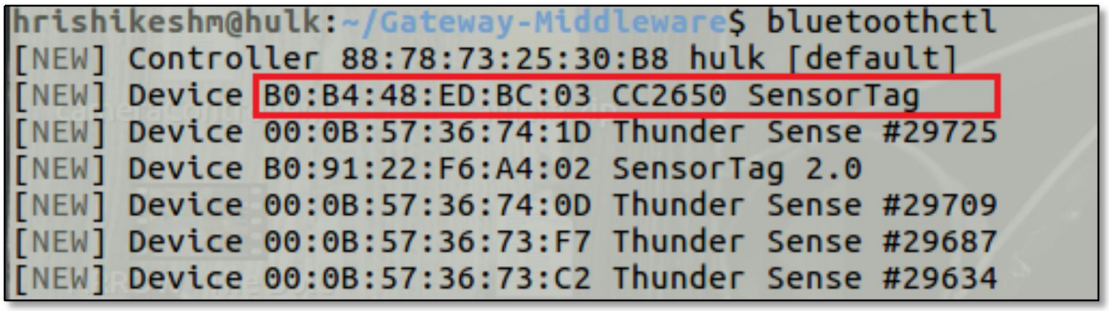
a) Using BLE Scanner App

1. Use any **BLE Scanner App** and scan for BLE devices.
2. Find the name of your Sensor type and note the Sensor Key.



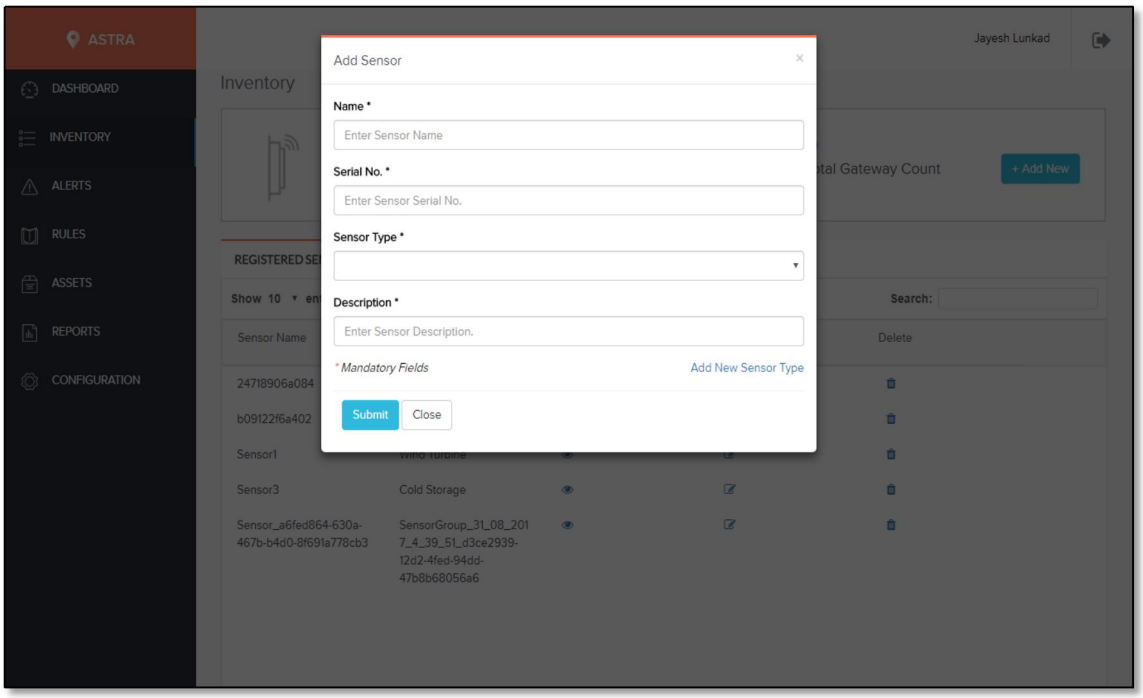
b) Using Ubuntu Or Linux System

1. Open Terminal and run **$ bluetoothctl**
2. Note the Sensor Key (MAC Address) of your sensor



Note: *Ignore ':'while adding sensor key*
E.g.: B0B448EDBC03

Sensor Type: Select a relevant sensor type from the drop down list.
Description: Enter a description for the sensor.



5. Generate QR Code for Sensor

1. Enter https://www.barcodesinc.com/generator/qr/
2. Paste the sensor key noted from the previous section

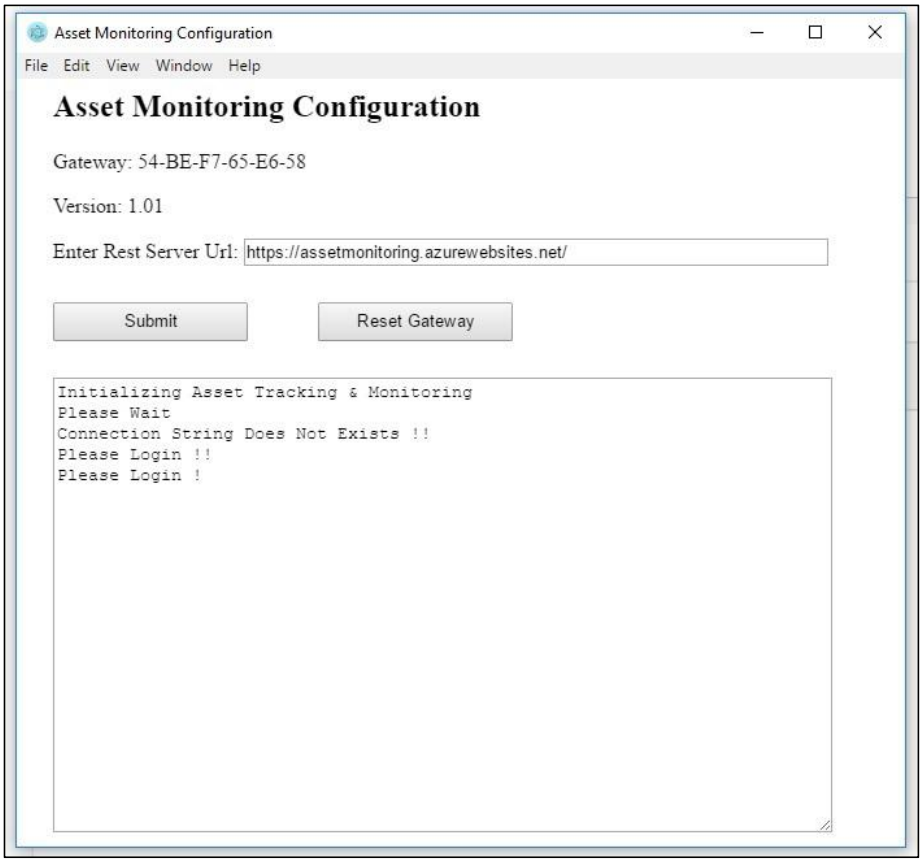
3. Click on Create QR Code.
4. Download this QR code as it will be required for scanning later.

6. Gateway Login

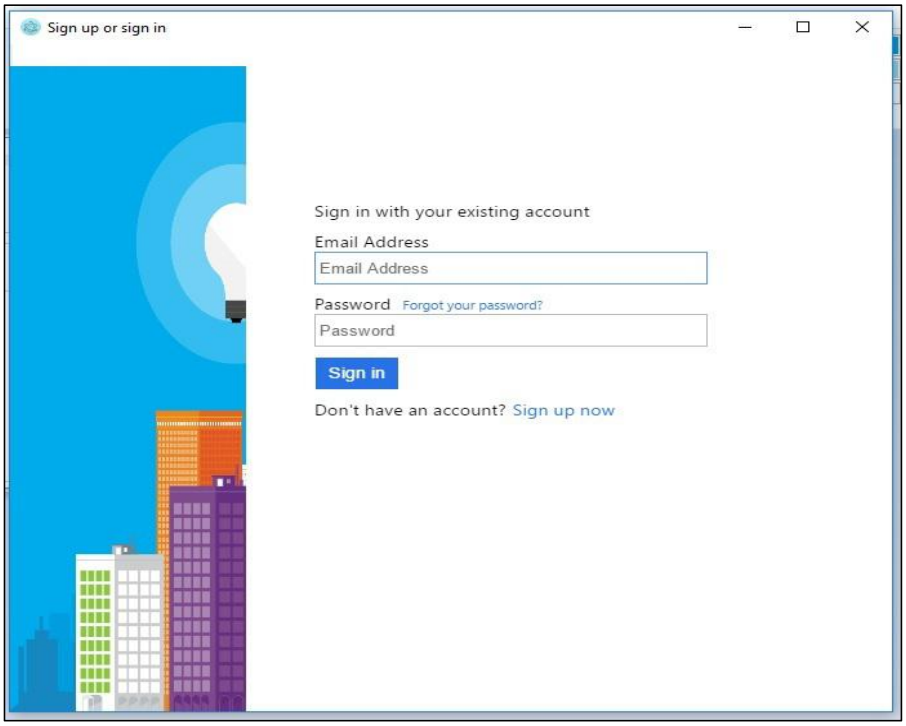
a) **Login**

i. Enter gateway application.

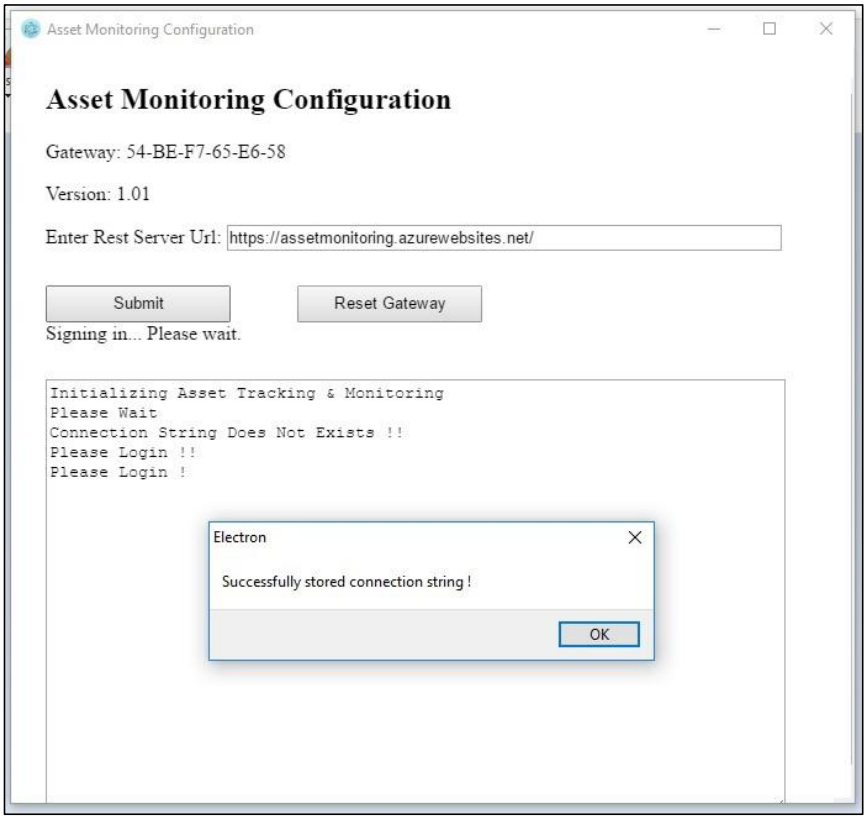
ii. Enter Rest Server URL and click on **Submit**.



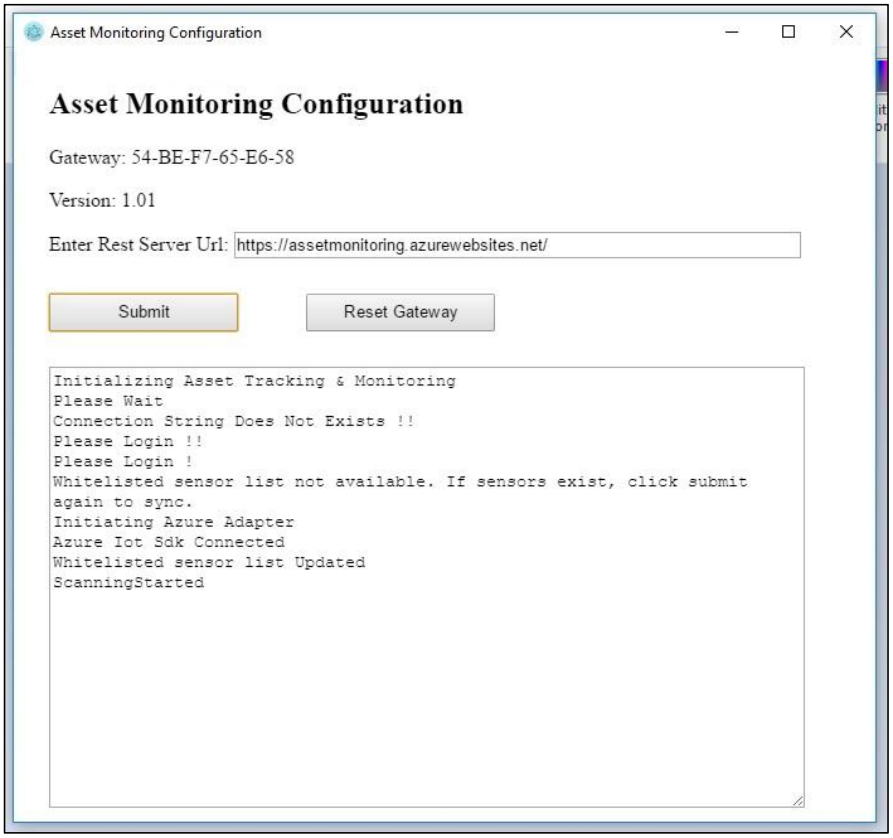
iii. User will be redirected to the Login page.



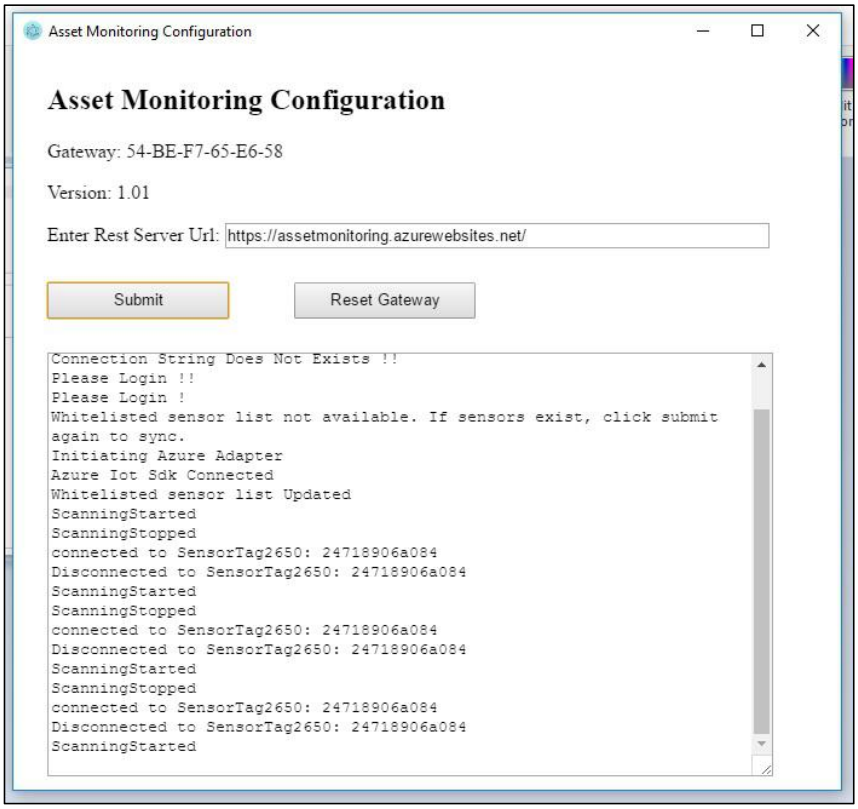
iv. Login into the account. Once Logged in, click on **OK**.



v. Scanning will start after Login. Observe logs for **'Scanning Started'** message.



vi. Turn the Sensor "**On"** to connect with Gateway. Observe the logs Connected/Disconnected for added sensors. Once connected, sensor will start sending data to IoT Hub.



6. User Instructions

a. Login

i. Open the browser and enter the **URL** of the web application

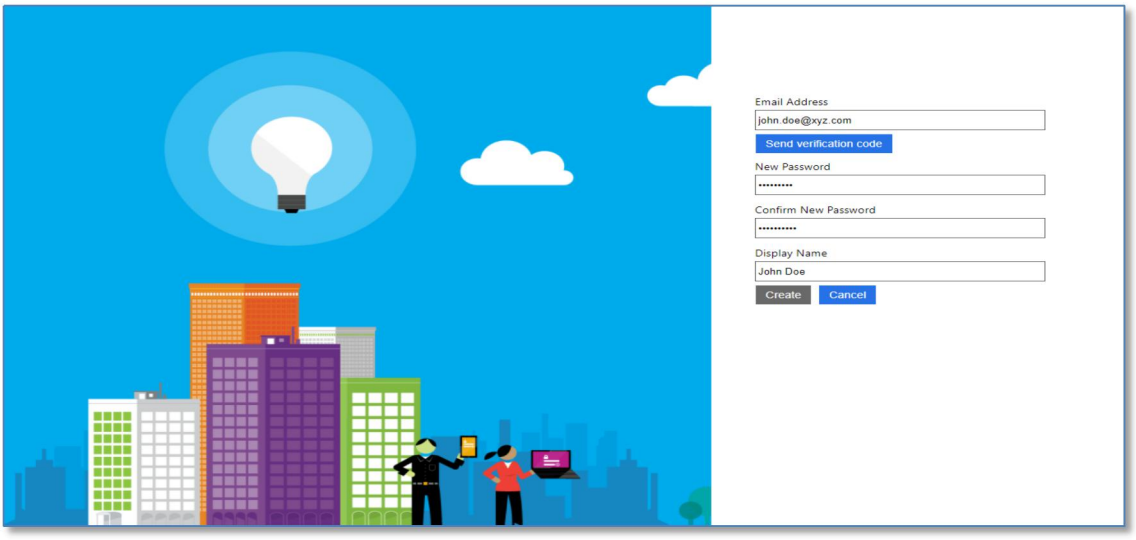
ii. The portal is best viewed in **Google Chrome**.

iii. Click on **Sign In** button.

b. Sign Up

To get started, users must first register on the portal. To register:

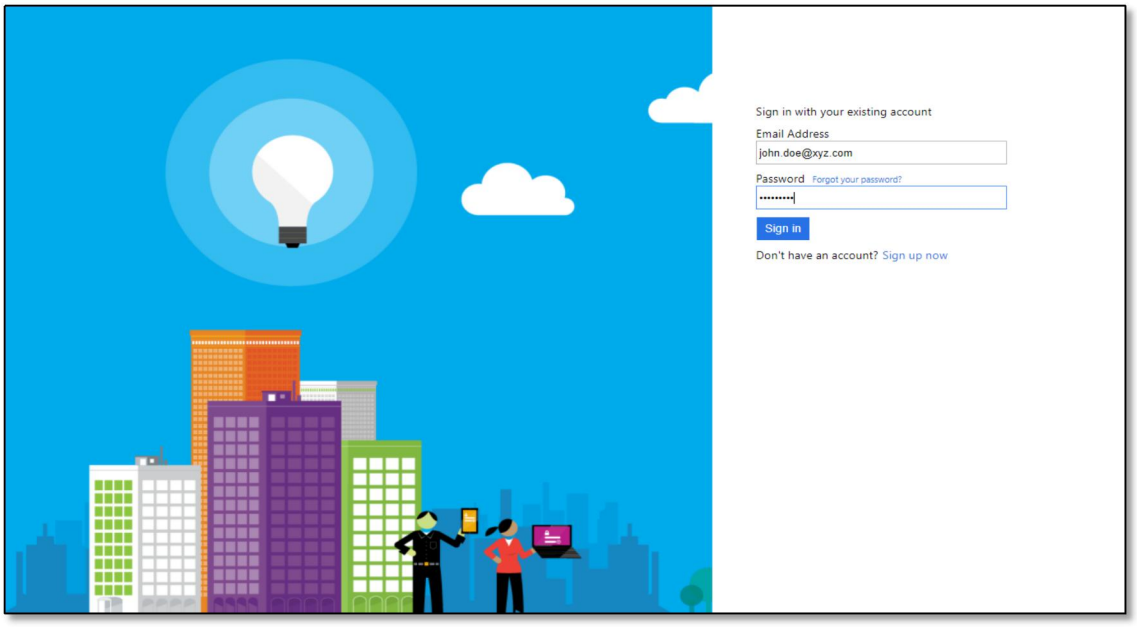
1. Enter a valid email address. Email addresses which are already registered cannot be used again.
2. Click on **'Send Verification Code'**. A verification code will be sent to the email address entered.
3. Enter the verification code to complete the sign up process.
4. After successful sign up the credentials will be registered on Azure Active Directory (AAD) and user will be redirected to the Dashboard.



c. Sign In

1. Use the sign up credentials to log in and start viewing the portal.

2. Contact administrator to change the password.



a) Dashboard

a) After logging in, user can see the dashboard , which comprises of the following metrics:

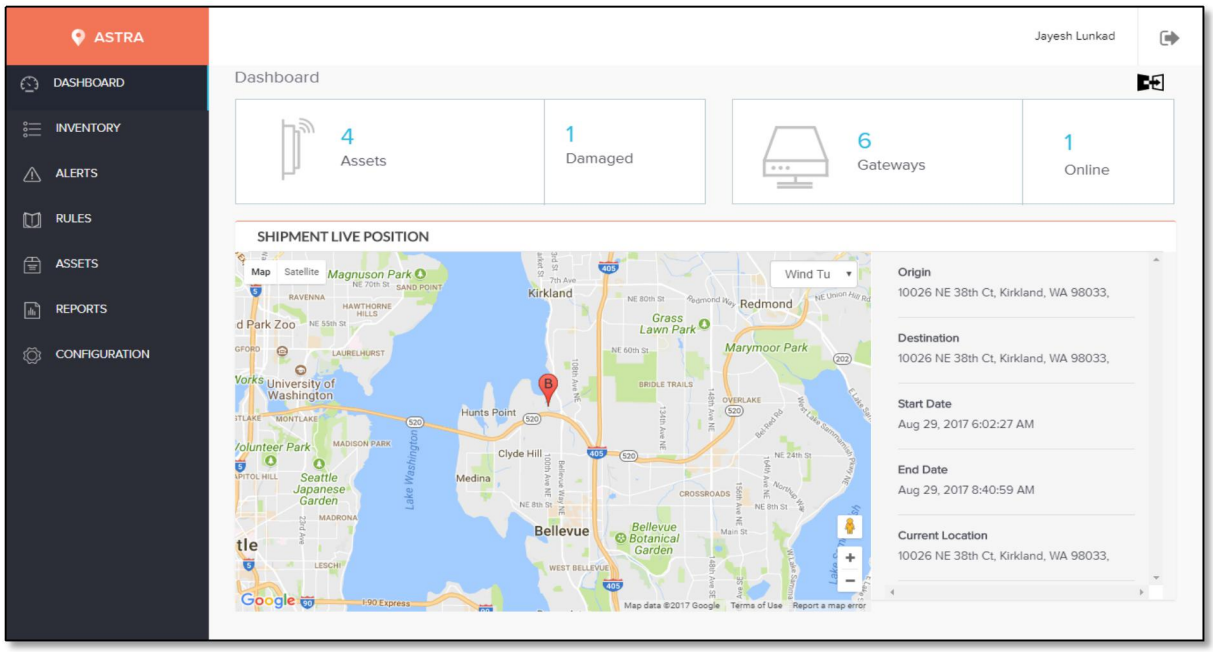
i. **Assets:** Shows the count of assets which are currently tagged to sensors.

ii. **Damaged:** Shows the count of assets which are in damaged state. Assets go in damaged state when rule applied on them breaks.

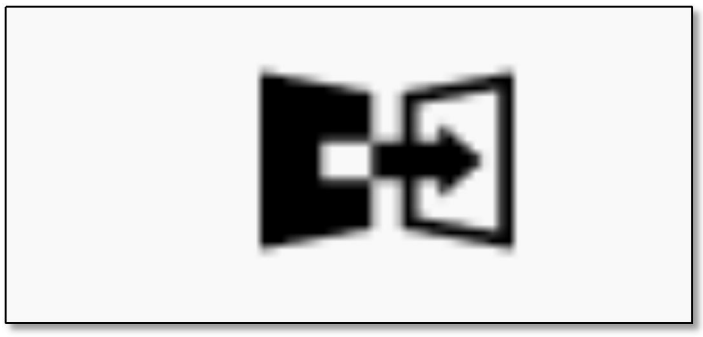
iii. **Gateways:** Number of gateways that are on-boarded.

iv. **Online:** Number of Active gateways currently sending out data.

v. **Shipment Live Position**: One can select a group and check the position of the shipment.



b) Click on the **Flip** icon (as shown below) to see indoor view of the premise where the user wants to monitor the assets.



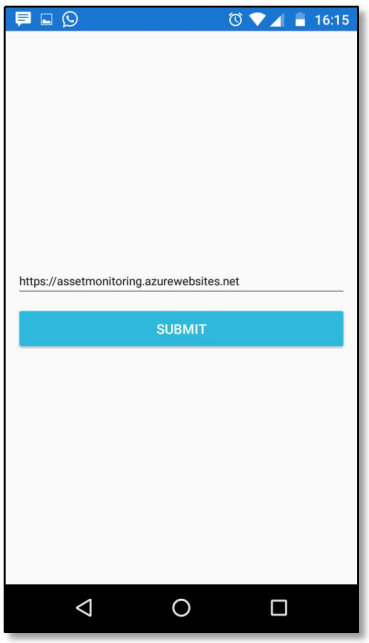
b) ASTRA Flow

1. Generate QR Code for Sensor

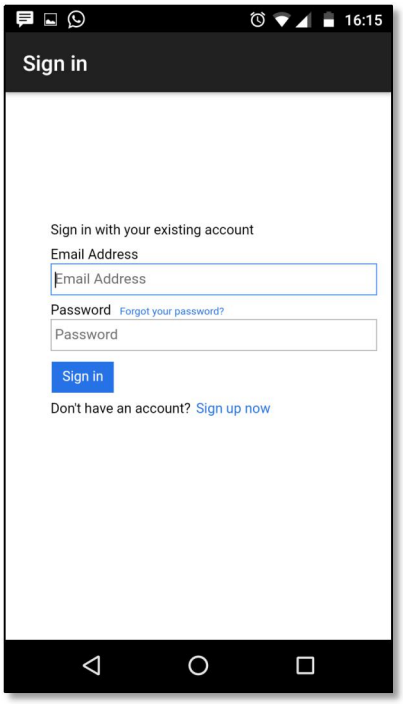
1. Log in to the web portal. Under the Inventory section note down the **Sensor Key** that needs to be tagged to an asset.
2. Log in to https://www.barcodesinc.com/generator/qr/ to generate QR code.
3. Paste the **Sensor Key**.
4. Click on **Create QR Code**.
5. **Download/Save** this QR code as it will be required for scanning subsequently.

2. Tagging Asset to a Sensor

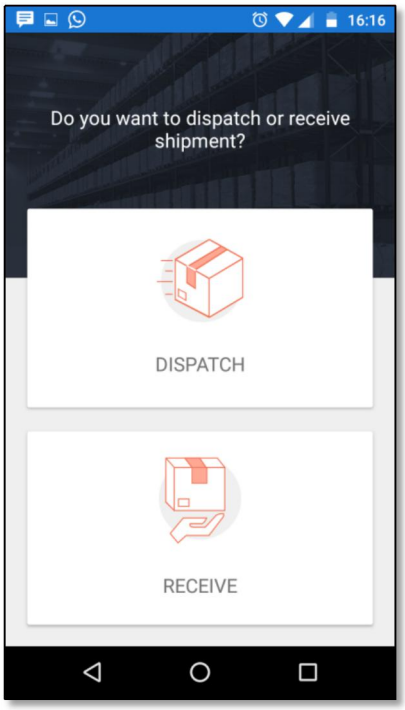
1. Log in to **ASTRA** mobile app
2. Enter **Domain Name** which is the REST server URL.



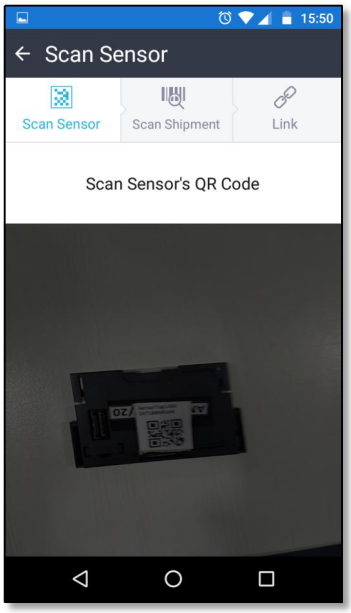
3. Log in into the app using the credentials acquired during set up stage of the web application.

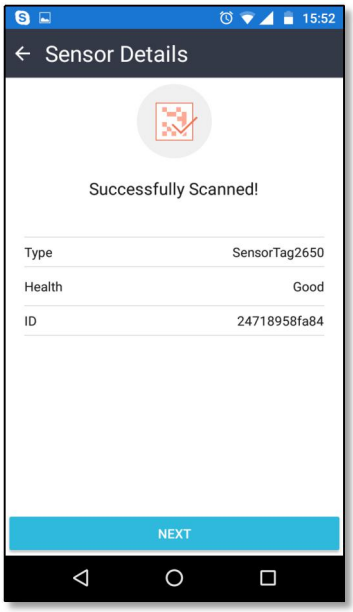


4. Click on **Dispatch** button.

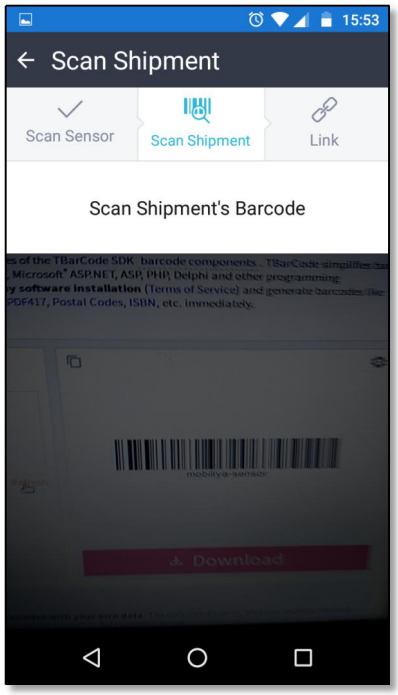


5. Scan the sensor QR Code downloaded from the QR code generator. After the code has been scanned successfully, click on **Next**.

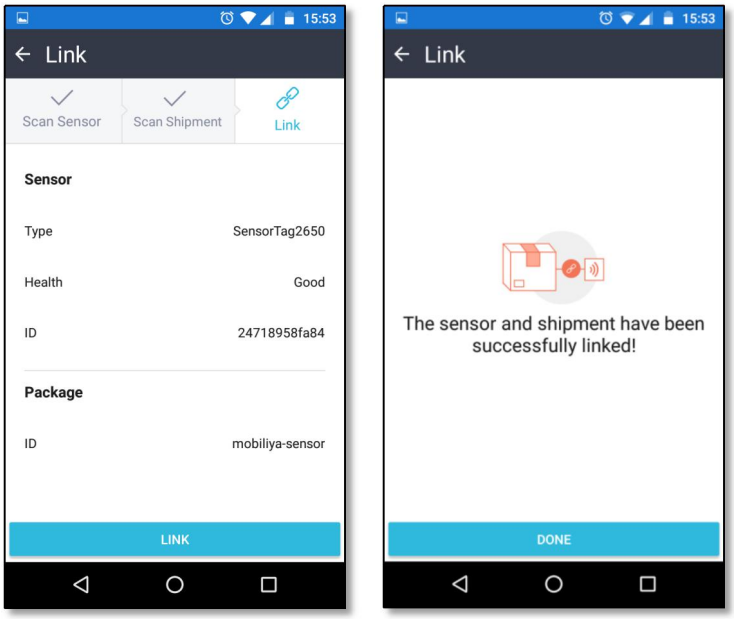




6. Scan the **asset barcode** which would be printed on the asset. If it is not printed, then generate a barcode for the text/id from this website. After the bar code is successfully scanned, click on **Next**.



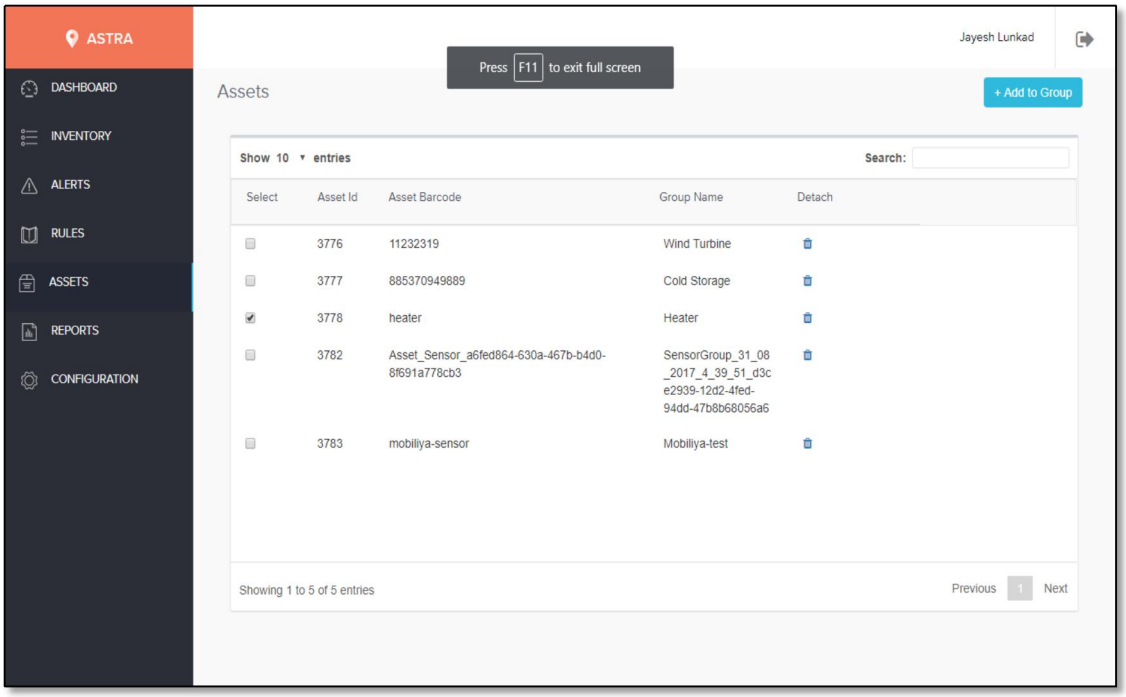
7. Link asset and sensor. After the asset is successfully linked, click on **Done**.



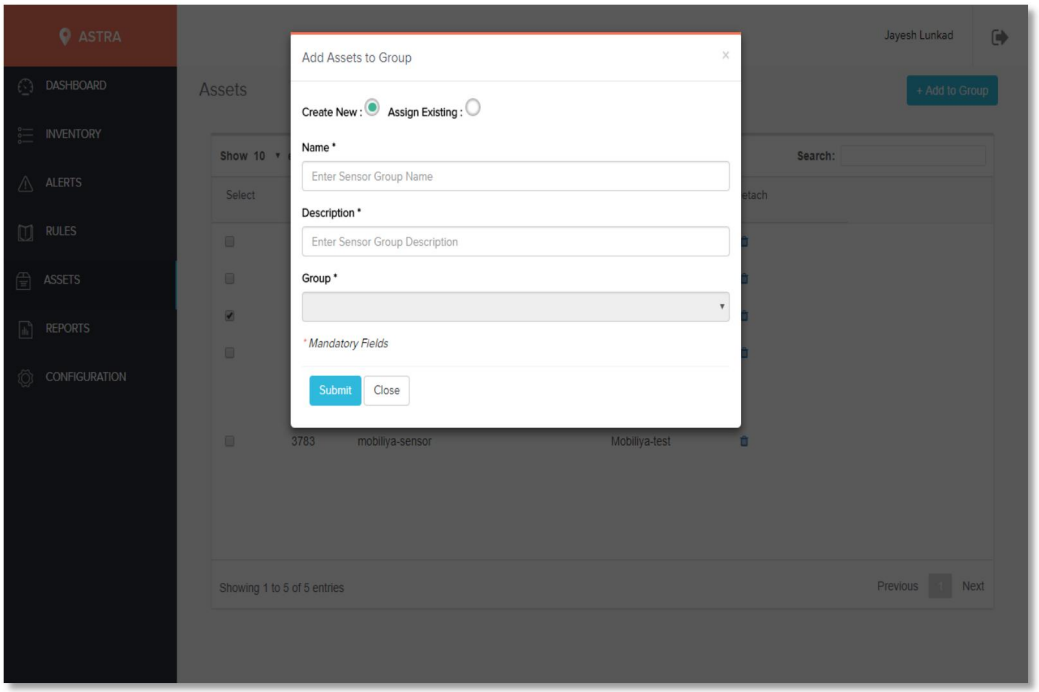
3. Add Asset to a Group

1. Click on the **Assets** section. Select the assets that need to be added to a group

2. Once the assets are selected, the "**Add to Group**" button will be automatically enabled.



3. Assets can be added to a new group or an already existing group. If it is a new group, enter a group name and description.



4. Reports

c) Live Report

This section of the portal shows live data of sensors which are currently sending data to the gateway. User needs to choose a sensor group and a

particular sensor from it to start viewing the data. User will see only those capabilities which the sensor supports.

d) **History Report**

This report maintains archives of the data sent by sensors for each capability. Users can go to a specific date back in time and check the trend of their sensors.

Also, this report shows when a rule was breached and provides trend of pre and post events of a breached event.

History Data Page:

This page shows the time line of events generated by the sensor in the past for each capability supported by the sensor.

Rule Trigger Page:

This page shows trend for those sensors that are included in the group that is being monitored by a rule. Any instances of rules being breached are marked in **Red**.

Note: Once a group is deleted from the web portal, the History data for that group is also deleted.

5. Rule Creation

1. Click on the **Rules** section and then on "**Add New**" button.

2. Select a group and create a rule for the required capability. Click on **Done**.

3. User will get an instant notification informing that the process of rule creation has started.

4. Once user receives a notification of successful rule creation, user can check live reports to see the implemented rule.

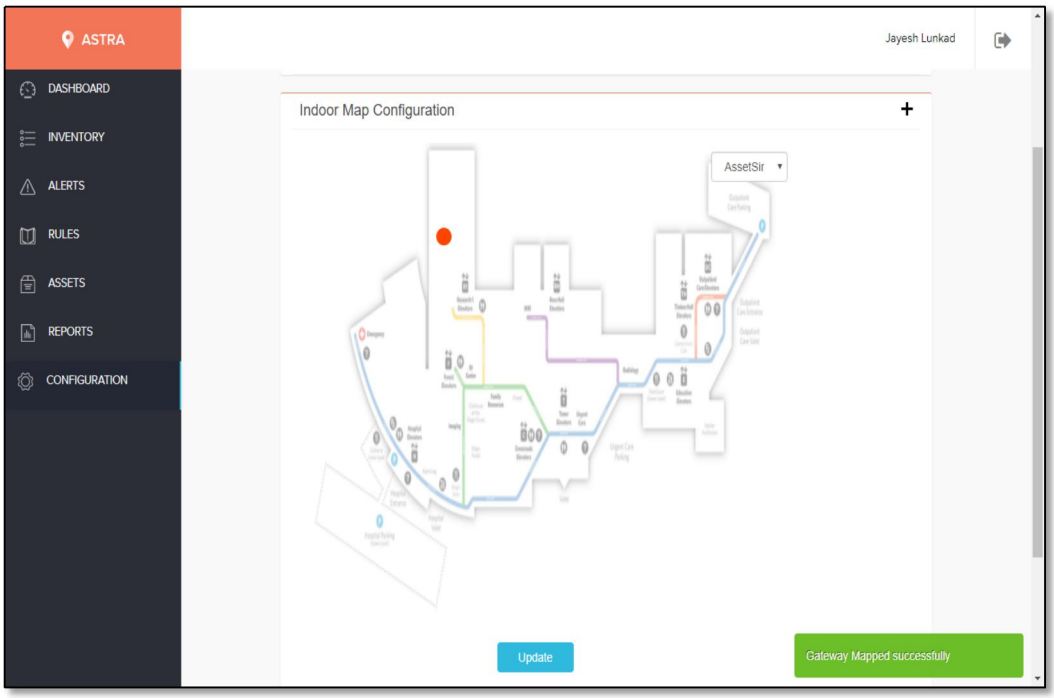
a) Indoor specific rules

1. Create Gateway Rules

Click on the **Rules** tab. Add a new gateway rule for a group.

2. Positioning gateway on the layout

1. Click on the **Configuration** tab.
2. Click on **Indoor Map Configuration** tab.
3. Select a **Gateway**. A Gateway icon [ ] will be displayed.
4. Drag the gateway icon on the layout where it needs to be positioned. Click on Update to finish.



3. Indoor Alert Notifications

User can view complete asset data and notifications by following a few simple steps:

1. Click on **Dashboard**.

2. Click on **Flip** icon below the Logout button.

3. A **Mapped Gateway** will be displayed with asset in the range circle.

4. Click on one asset. User can now see the live data coming from sensors on the right side of the screen.

5. On the same screen, alert notifications for assets are also displayed.

6. Alerts

1. This section displays all the alerts which have been received for a particular group, asset and capability. Select a particular feature from the drop down menu. Click on **Apply** to view.

2. Choosing an asset and capability are optional.

7. Asset Status

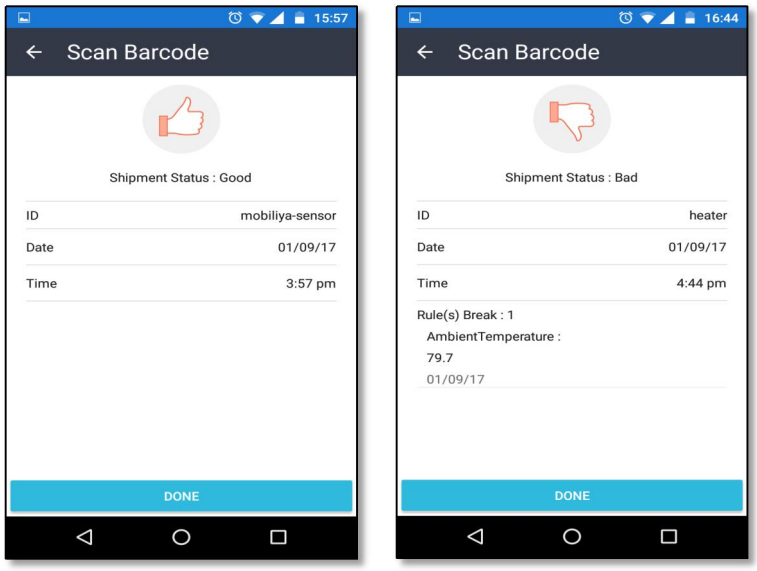
User can view the status of every asset in the following way:

1. Open mobile application using first 3 steps of this section.

2. Click on **Receive** button.

3. Scan asset barcode. It will show the status of the asset whether it is good or bad.

4. If the status is bad, it means that a rule(s) has been breached.



Frequently Asked Questions

Q1: What is an Asset?

An asset is an object whose condition needs to be tracked over a period of time. Example: Any product during transit of a shipment.

Q2: What is a Sensor?

Sensors are tagged to an asset to send environmental data such as humidity, temperature etc.

Q3: What is a capability?

A capability is a type of environmental information which a sensor provides. Different types of sensors provide different type of capabilities. Example: SensorTag provides capabilities like temperature and humidity.

Q4: What are groups in ASTRA?

Groups are a collection of sensors. A group can have sensors that provide multiple capabilities. In ASTRA, all rules are applied at the group level.

Q5: Power BI reports are not displayed.

This may be because the Power BI configuration has not been enabled. Users must contact their administrator to get it enabled.

Q6: Sensor data not visible in History report.

The History report refreshes every 3 hours. Users must ensure that they wait for the stipulated 3 hours before checking data for the newly added sensor in the History report.

Q7: App is asking for Domain URL on start up.

Mobile app requires Rest API URL for configuration. Users must contact administrator and update the URL. It will ask the URL only once.

Q8: Why are sensors not visible on the Reports page?

Users must ensure that the sensor that they are looking for has been linked to an asset.