MAXIMO MONITOR
HANDS-ON LAB

In this Exercise, you will learn how to setup Monitor to receive data from a Node-Red simulator to devices in Monitor.

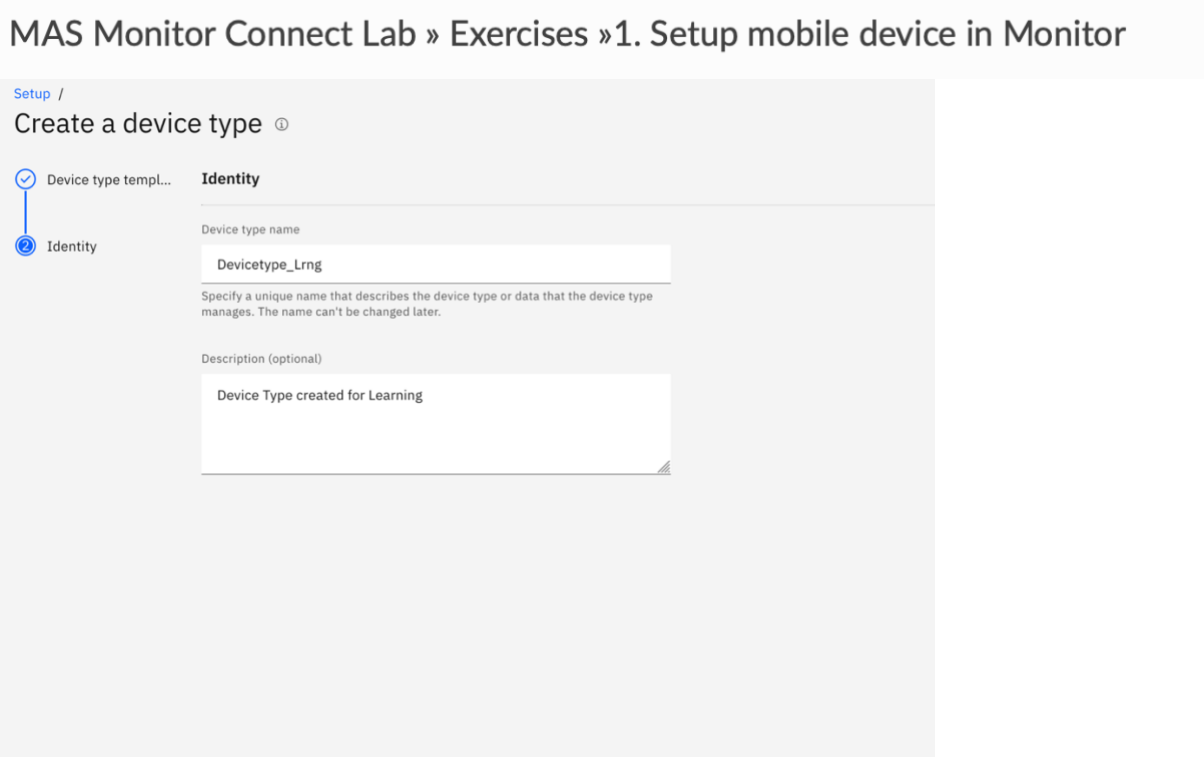
Step 1: Create a device type and setup metrics in Monitor

Step 2: Create a device in Monitor to send event data from Node-Red simulator

Note : Add your initials in Device type name and Device name e.g. (XX_Devicetype_Lrng) replace XX with your initials.

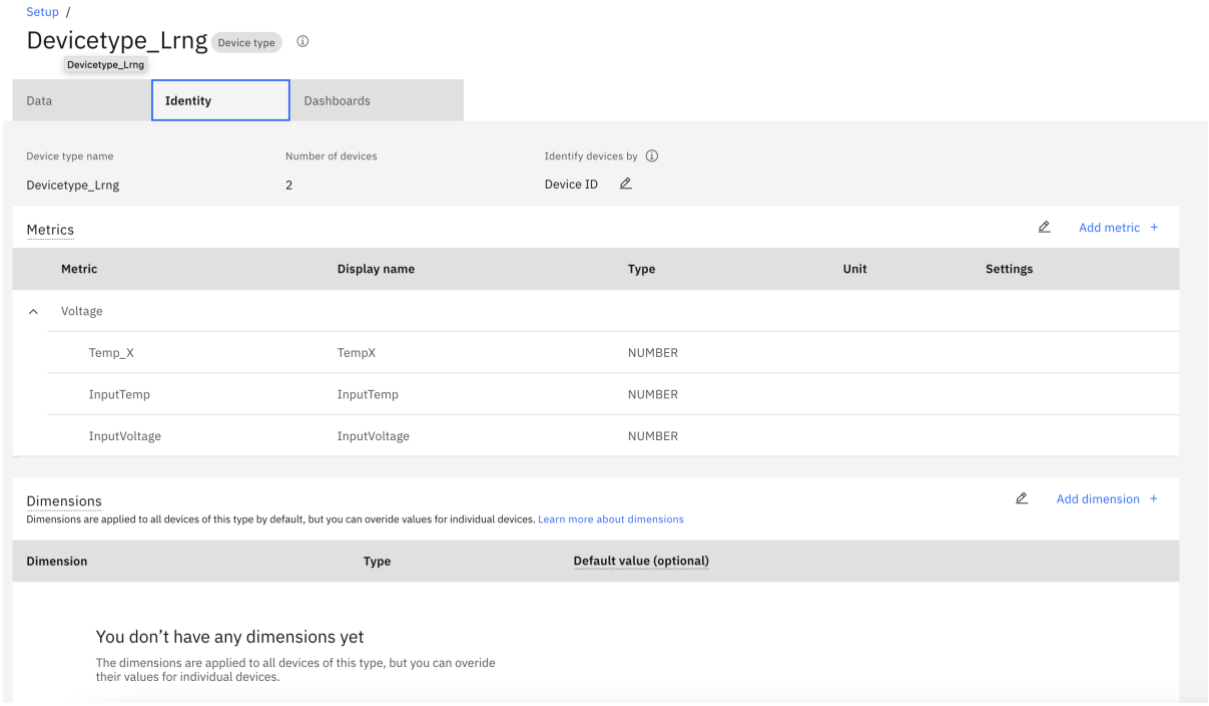
Create a device type

1. Go to Setup in Monitor
2. Go to Devices tab
3. Click on + button to create a device type
4. Choose Basic template
5. Next
6. Enter a Device type name, e.g. Devicetype_Lrng
   Take note of the name you give as you will need this in the Node-RED flow config
7. Create.



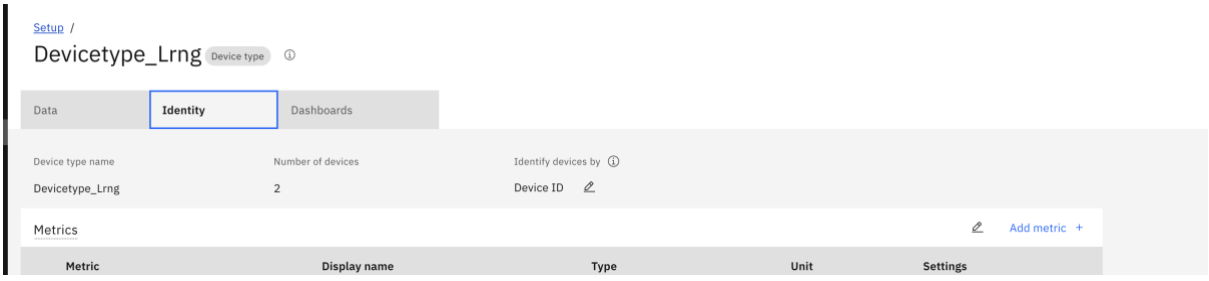
Create Metrics in the device type

1. Under Metrics section click Add metric
2. Click Add metric
   a. Enter InputTemp for Metric
   b. Enter InputTemp for Display name
   c. Enter Voltage for Event
   d. Choose NUMBER for Type
   e. Optionall you can enter Unit
3. Similar way we can add two more metrics as shown below.
4. Click Save



Create a device in Monitor

1. Click the blue Setup link in the top left which will take you to the device types list



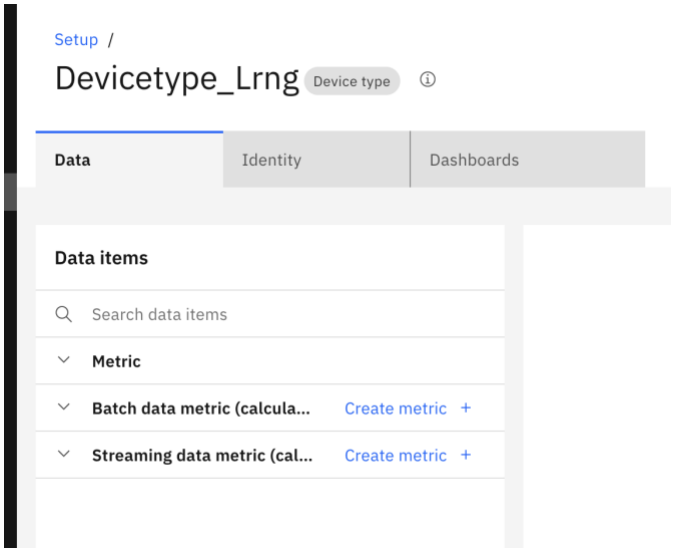
2. The device type you created should be selected
3. Click on `Add device +`

4. Enter Lrng_Device1 for name
5. Choose Custom token
6. Enter Pasword1!
7. Click Add and Close

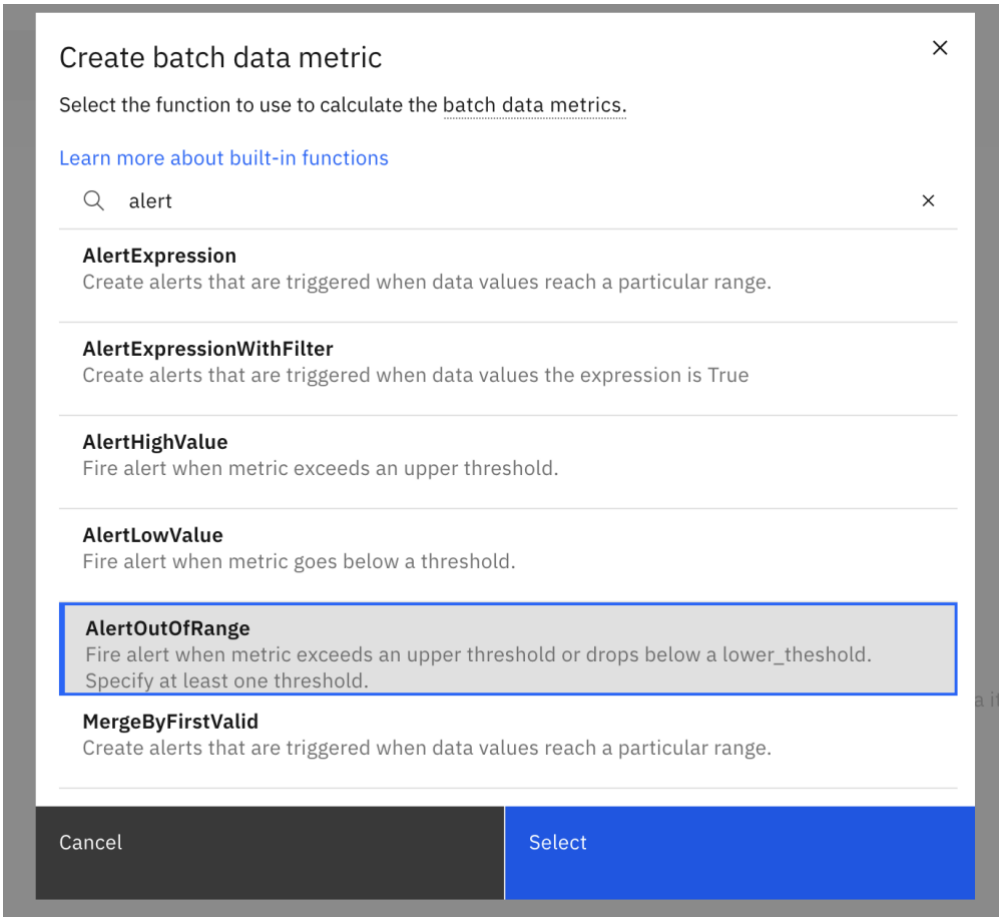
Add Calculations & Alerts

The "Alerts" function allows you to be notified when anomalies are detected.

1. Click setup menu. Search on DeviceType_Lrng
2. Click on Setup Device type button
3. Click on the + icon under Batch Data metric section to create new metric

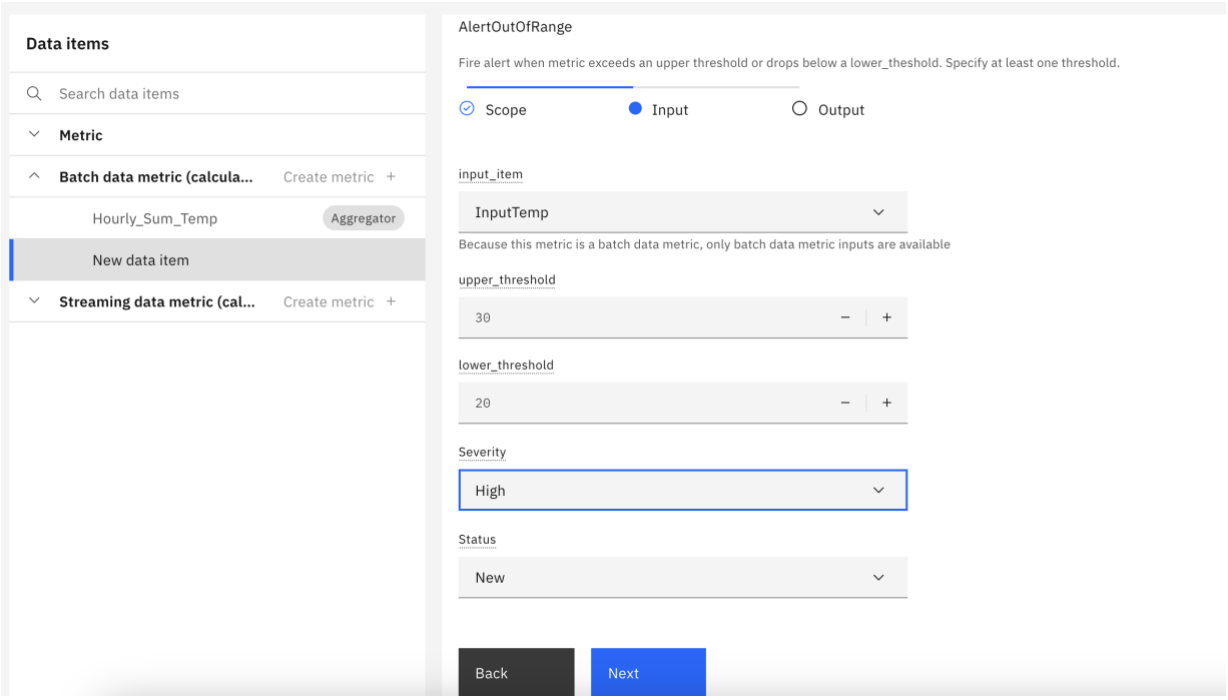


4. Select AlertOutOfRange

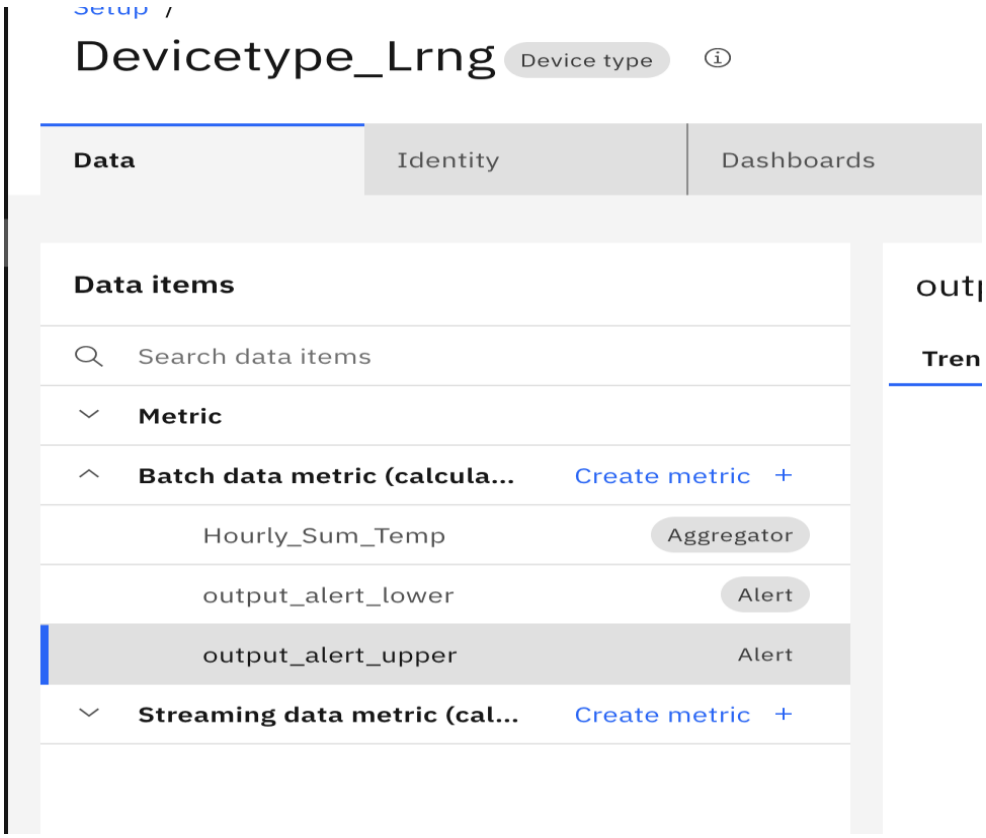


5. Select the Scope All Device of this type.
6. Select fields as below

    a. Input Item : InputTemp
    b. Upper_threshold : 30
    c. Lower_threshold : 20
    d. Severity : High
    e. Status : New

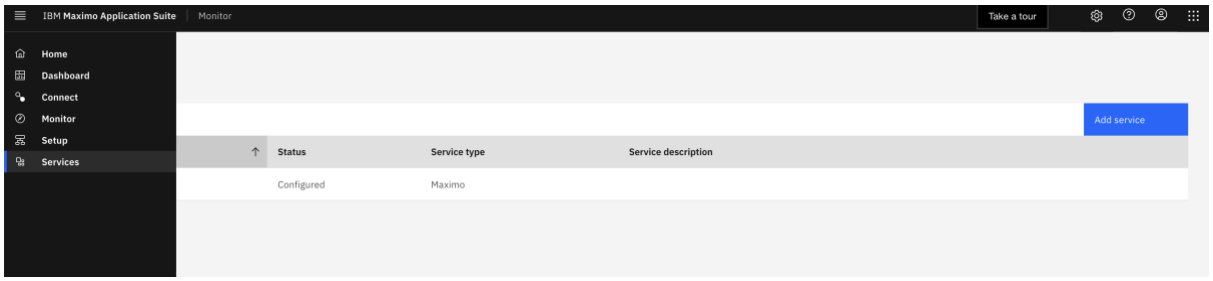


7. Click Next
8. Click on Create

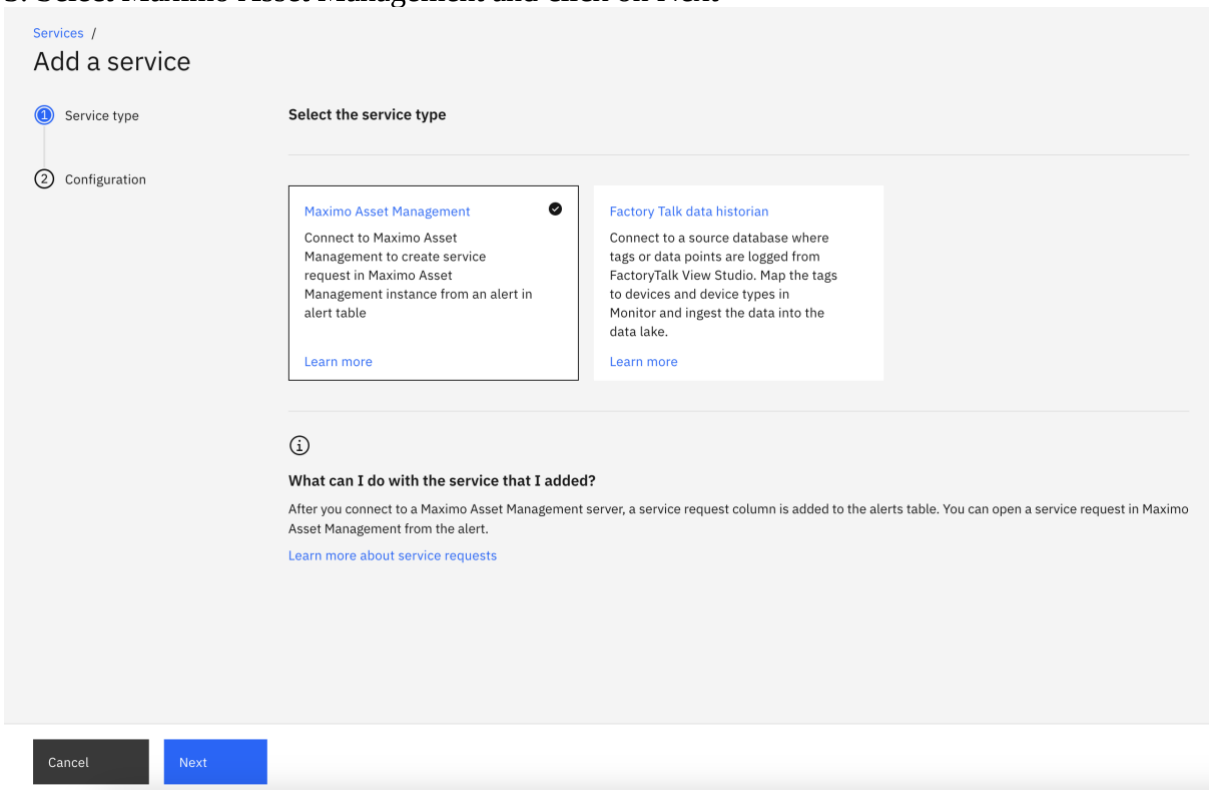


Connect to Maximo Manage to raise Service Request

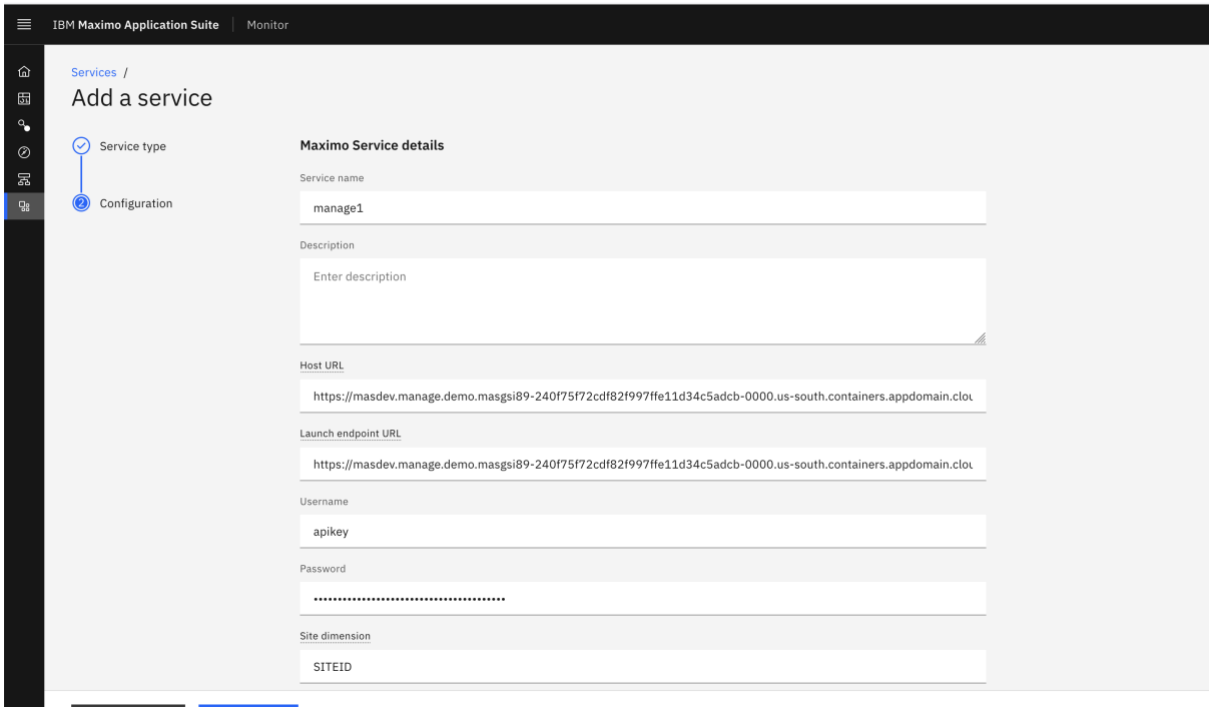
1. Click on Services tab



2. Click on Add Services
3. Select Maximo Asset Management and click on Next



4. Enter Service name : manage
5. Host URL : `https://<workspace_id>.manage.<mas_domain>`
6. Launch endpoint URL : `https://<workspace_id>.manage.<mas_domain>`
7. Username : apikey
8. Password : API token from API Key application
9. Click on Test connection and Finish



Install Node-RED locally

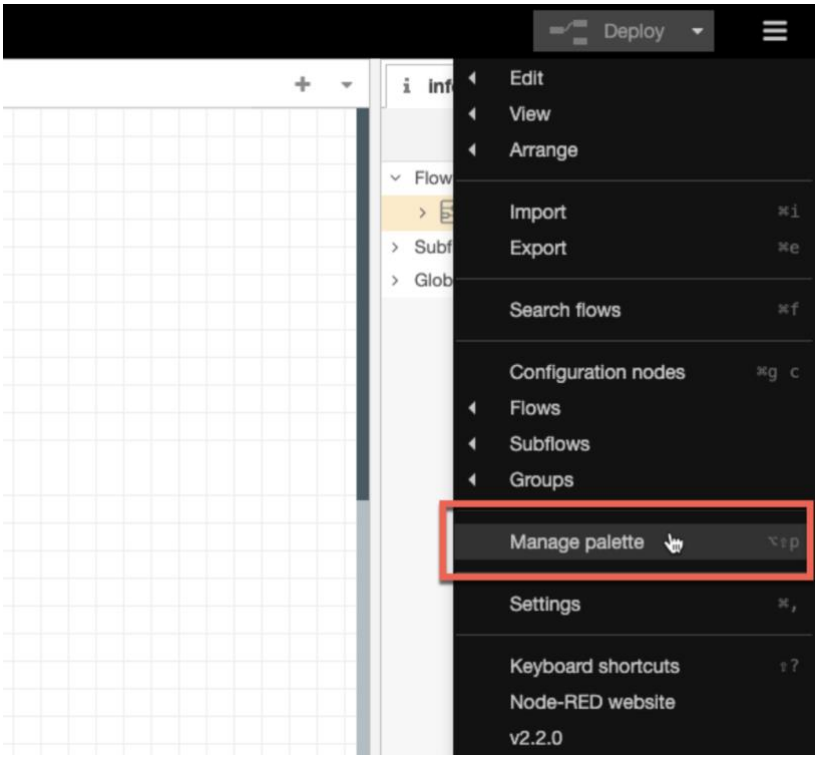
This is a fairly easy step, as you just have to follow this guide: [Running Node-RED locally]

Once installed and started open the browser and start the Node-Red editor.

Add required additional nodes

Before loading the Node-RED script you need to add the required additional node libraries.
Node-RED library dependencies:
- node-red-dashboard
- node-red-contrib-ui-upload
- node-red-contrib-chunks-to-lines

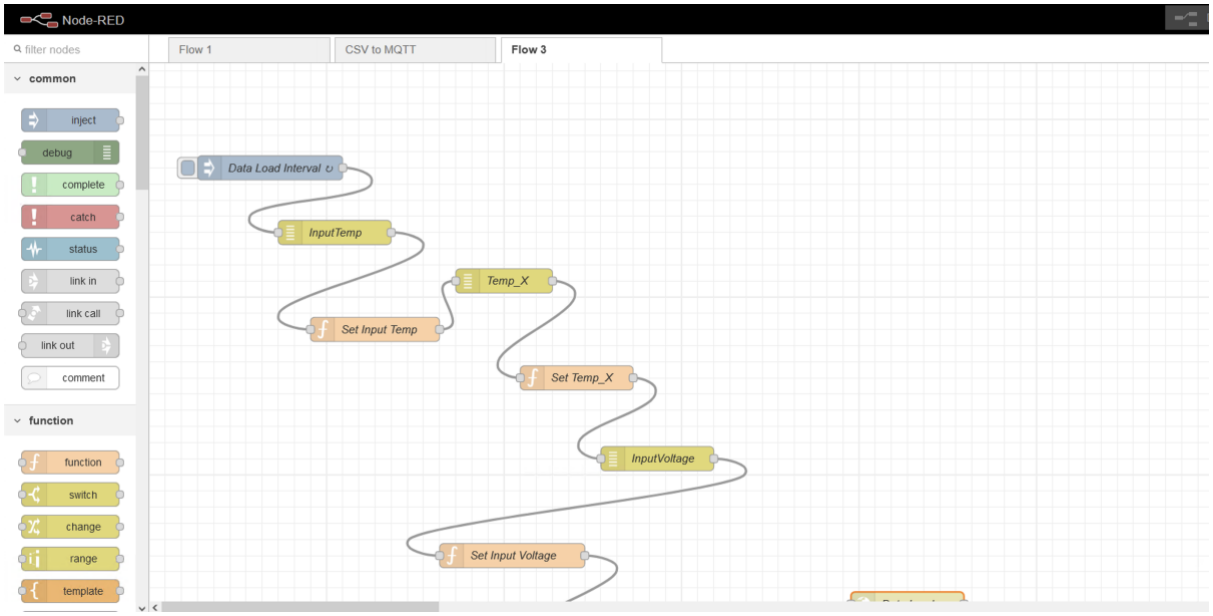
1. Click on the burger menu in upper right hand corner and select Manage Palette



2. Click on Install and write node-red-dashboard in the search field and click on Install.
3. Click on Install again.
4. Repeat the above step for other libraries.

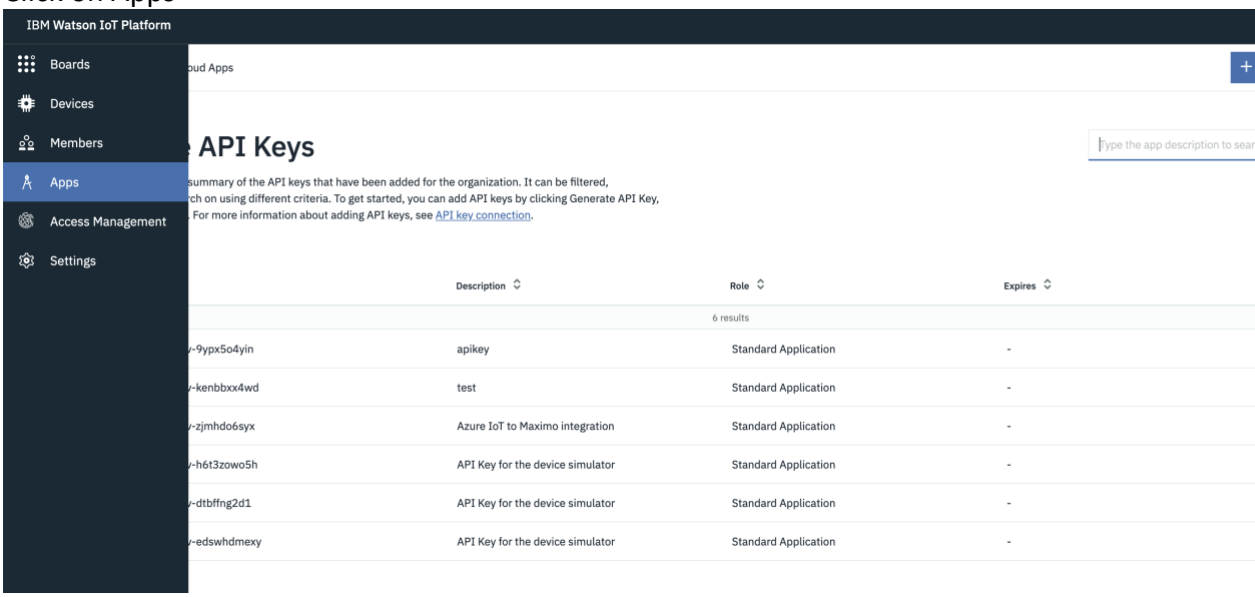
Import Node-RED flow

1. Download the flow from git-hub
2. Launch Node-RED
3. Click on the burger menu and choose Import
4. Click on select a file to import
5. Choose the file downloaded in step 1.
6. Click Import

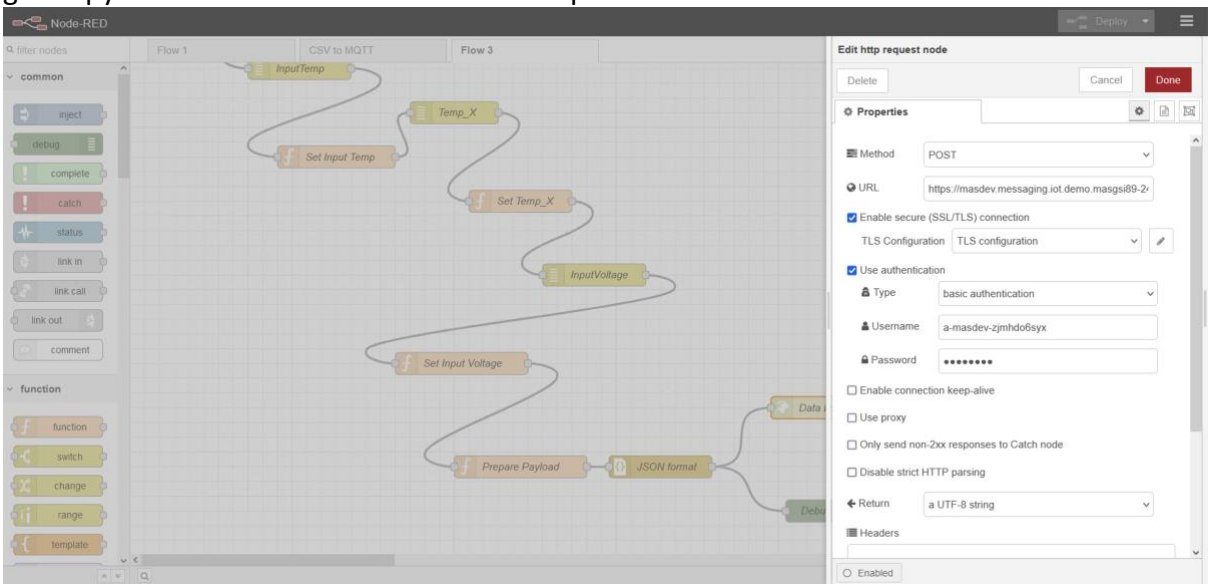


Modify Node-Red flow to ingest data in Monitor

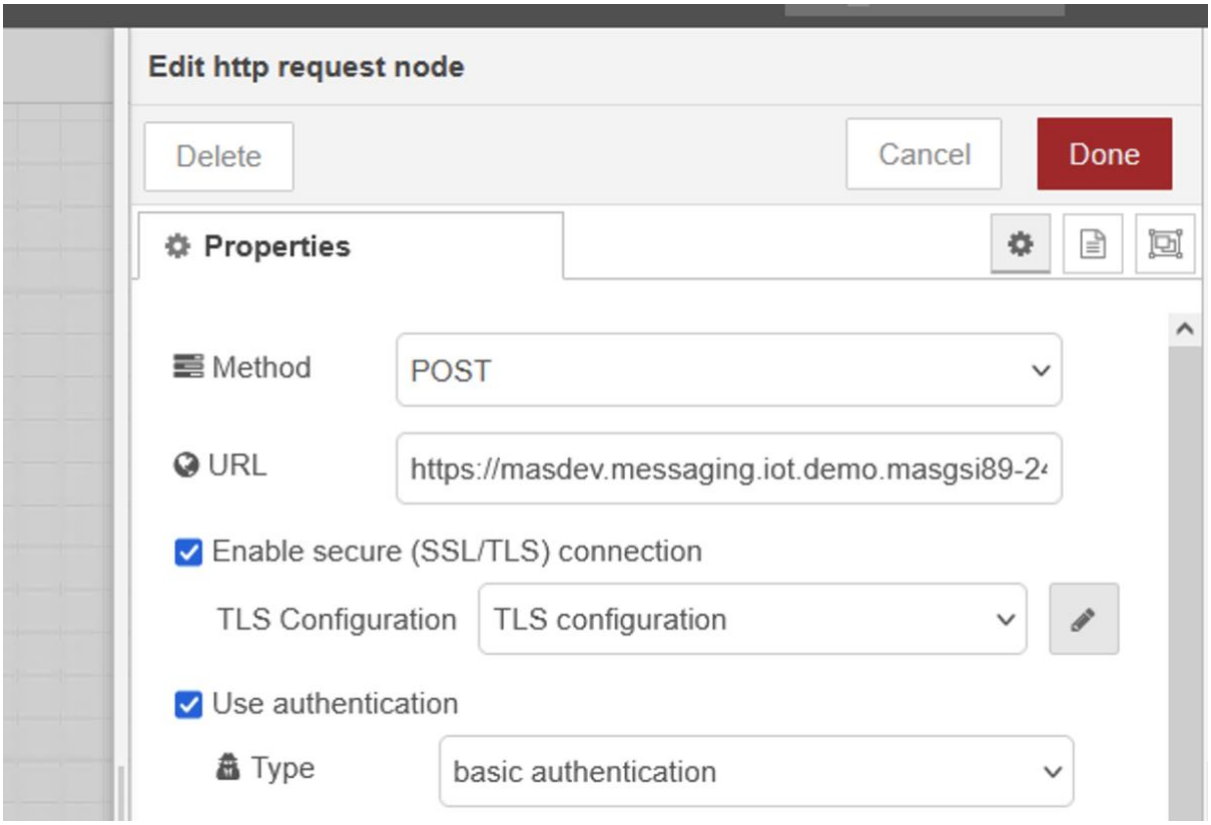
1. Click on Data Load node to configure it
2. Update the URL e.g. https://masdev.messaging.iot.demo.masgsi89-240f75f72cdf82f997ffe11d34c5adcb-0000.us-south.containers.appdomain.cloud/api/v0002/application/types/Devicetype_Lrng/devices/Lrng_Device1/events/Voltage
3. Open IoT application for Username & password
   a. Click on Apps



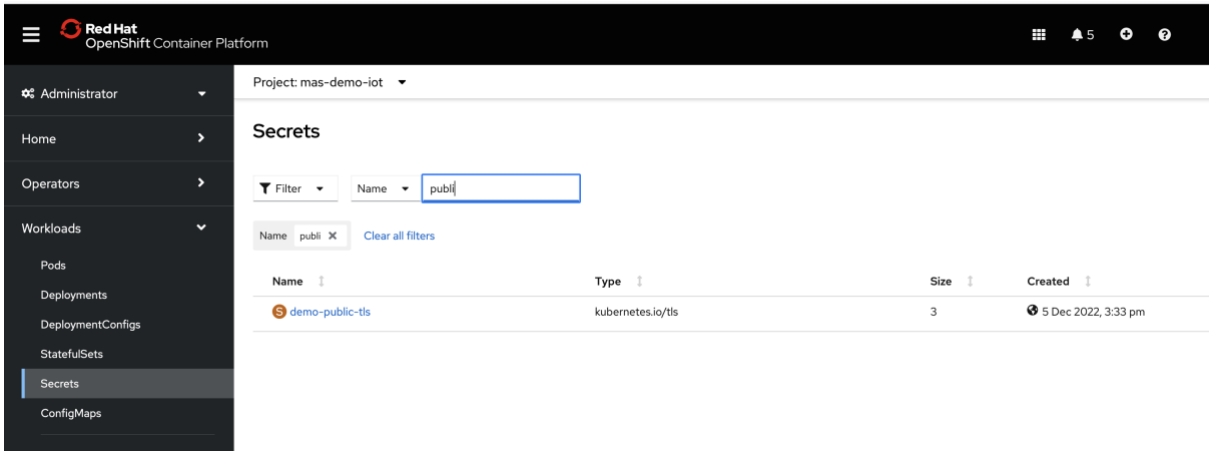
   b. Click on Generate API Key
   c. Provide Description and click Next
   d. Select role Standard Application
   e. Click on Generate Key.
   f. Copy API key to Node-red Username field
   g. Copy Authentication token to Node-red password field



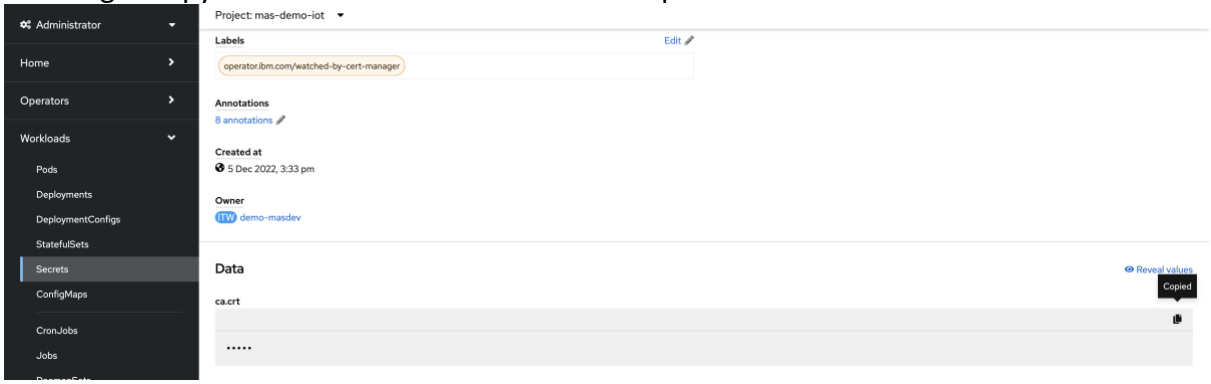
4. To configure TLS configuration
   a. Click on pencil icon beside TLS configuration field

b. 

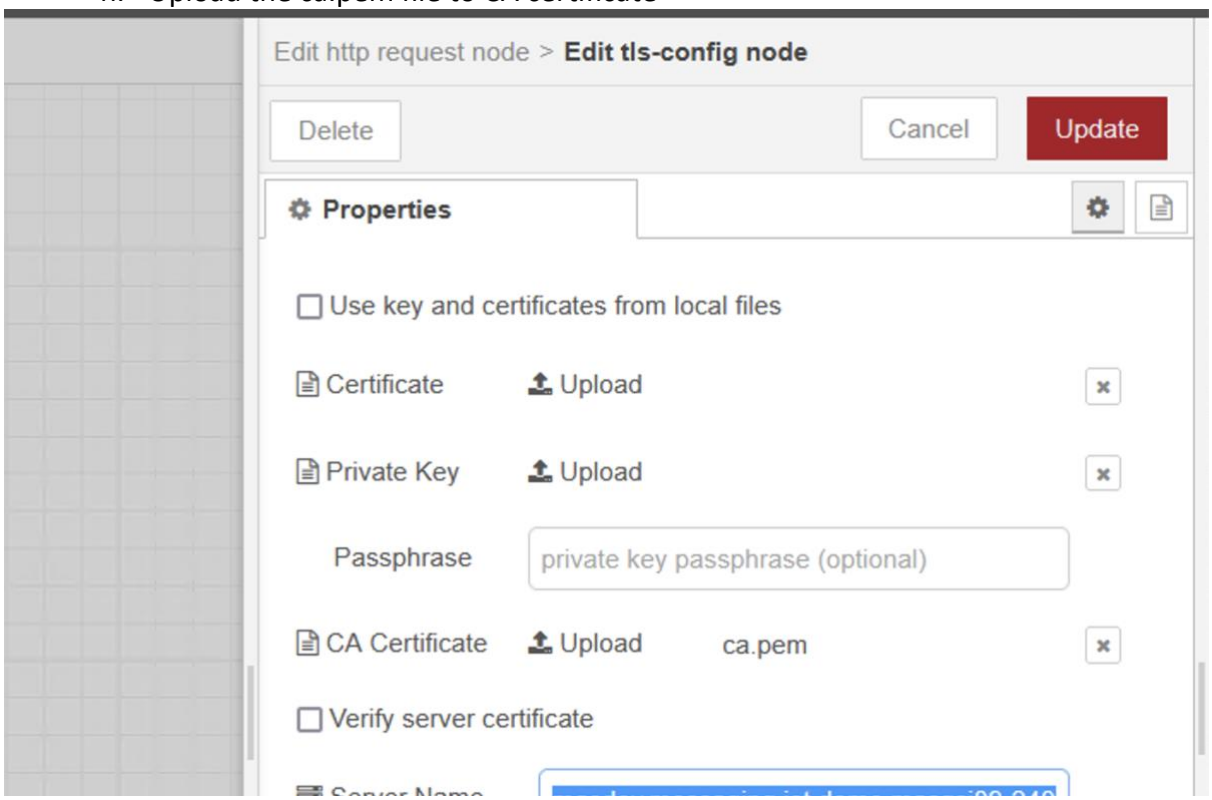
c. For CA certificate login to OCP console
d. Select Workload -> Secrets and choose IoT project e.g mas-demo-IoT
e. Search with Public-tls word



f. Open the secret
g. Copy the text of ca.crt and save it as ca.pem file



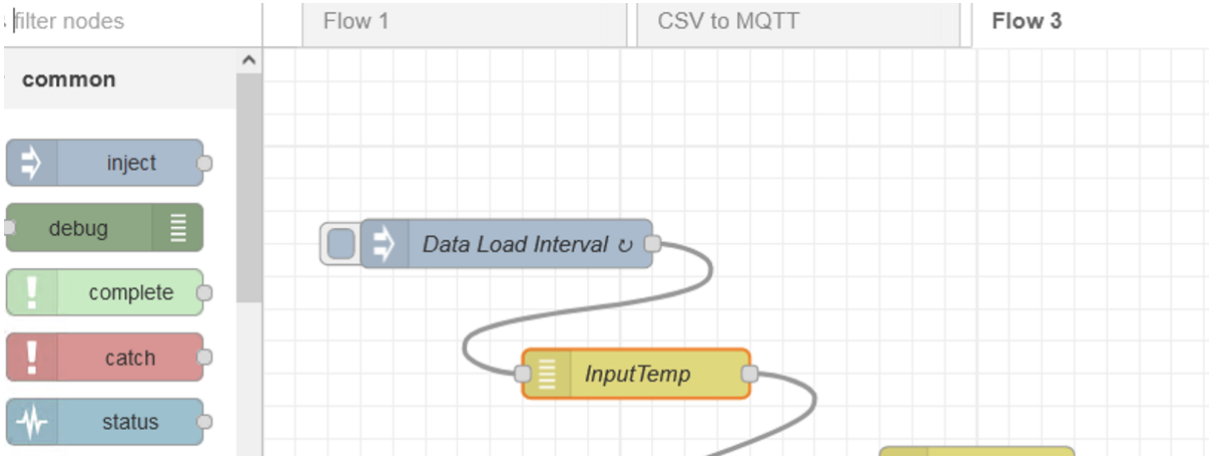
h. Upload the ca.pem file to CA certificate



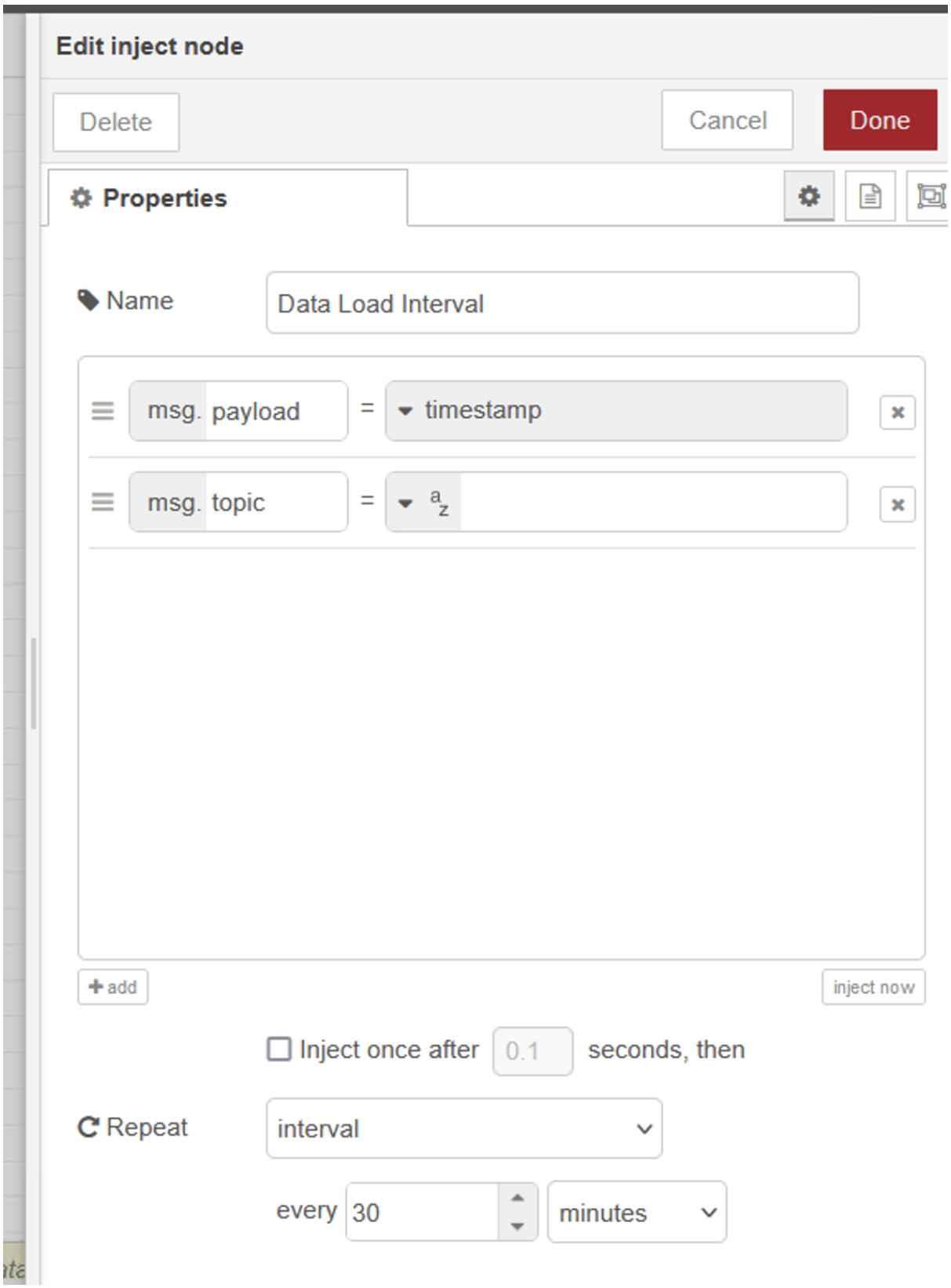
5. Provide server name e.g masdev.messaging.iot.demo.masgsi89-240f75f72cdf82f997ffe11d34c5adcb-0000.us-south.containers.appdomain.cloud
6. Click on Update
7. Click on Done
8. Click on Deploy

Ingest data from Node-Red to Monitor device

1. Double Click on Data load Interval node



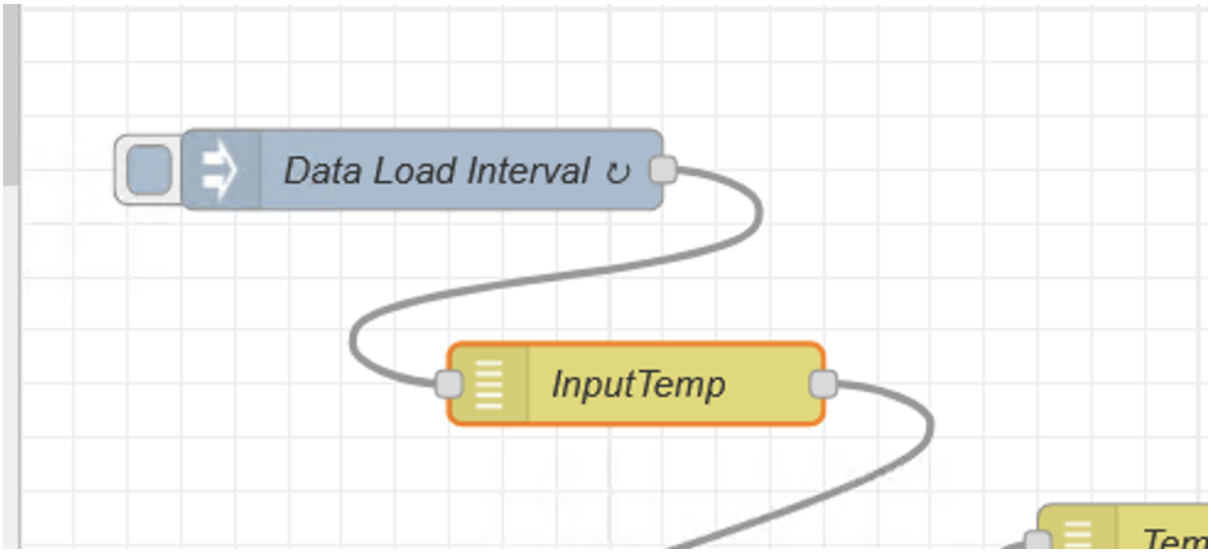
2. Set the Repeat property as below



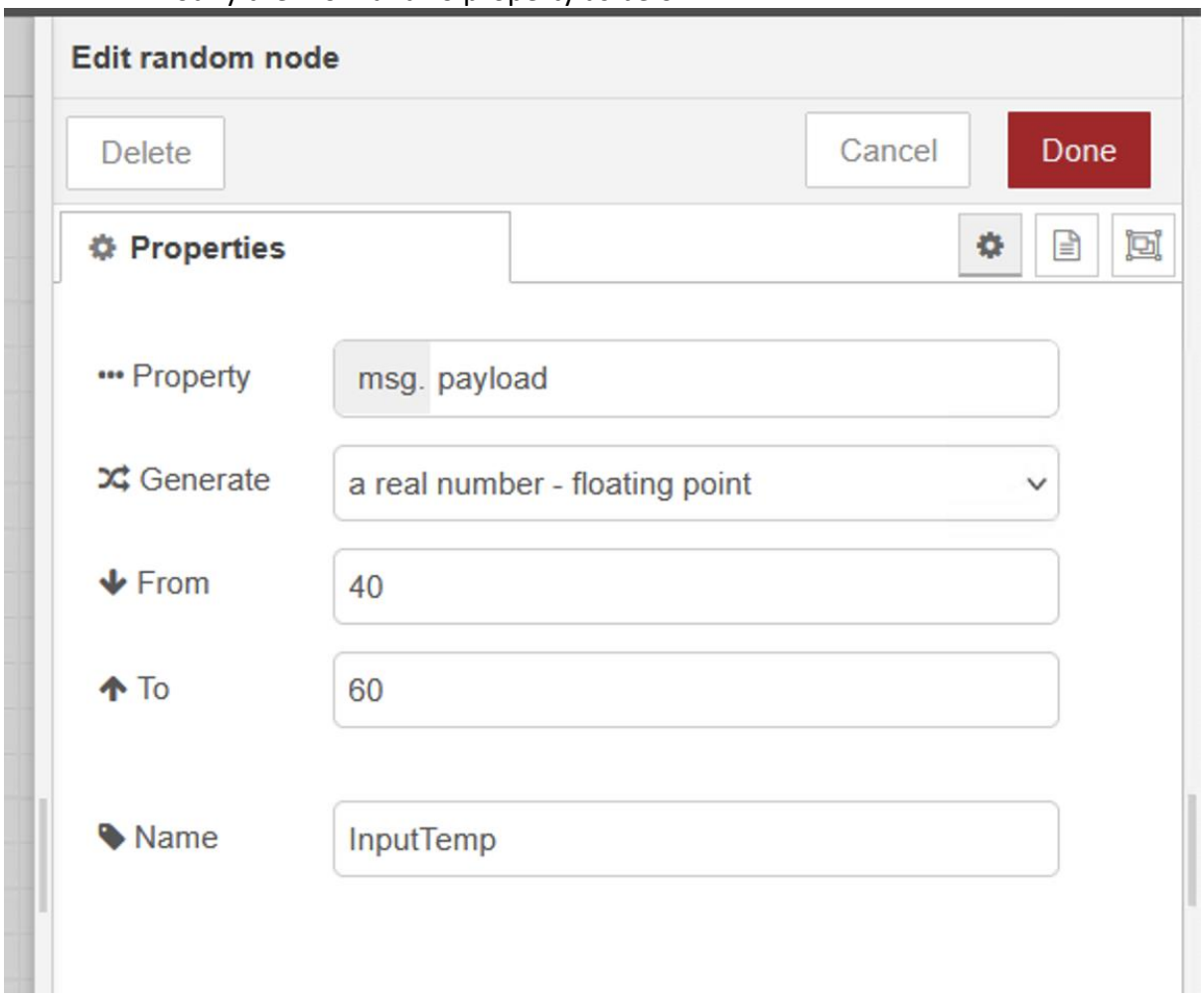
3. Click on Done
4. Click on Deploy

Send Anomaly data to monitor

1. Double click on Input temp flow

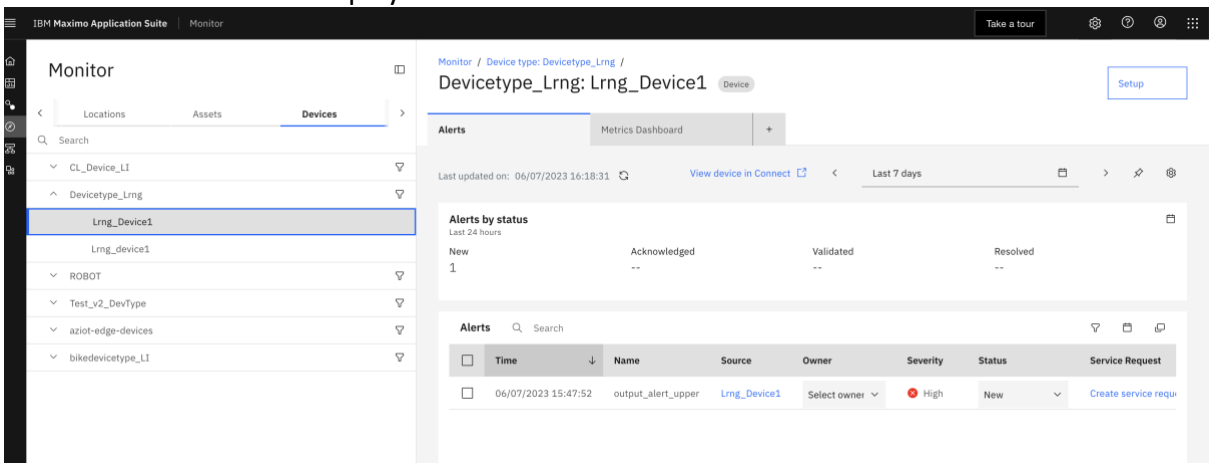


2. Modify the From and To property as below



3. Click on Done and Deploy the flow
4. Click on blue button on Data Load Interval node to ingest one record manually.

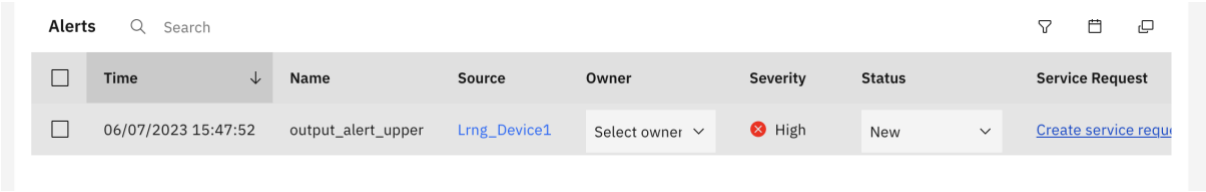
5. Go back to Monitor application and select Monitor tab
6. Click on Devices tab
7. Select the Device type and device name
8. Alert will be displayed on Alert table as shown below



Raise Service Request from Alert Table

Note: Create an asset in Manage application with the same name as device in monitor before creating service request.

1. Click on Create service request link



2. Enter the Reported by field
3. Click on create button