IoT Device Creation

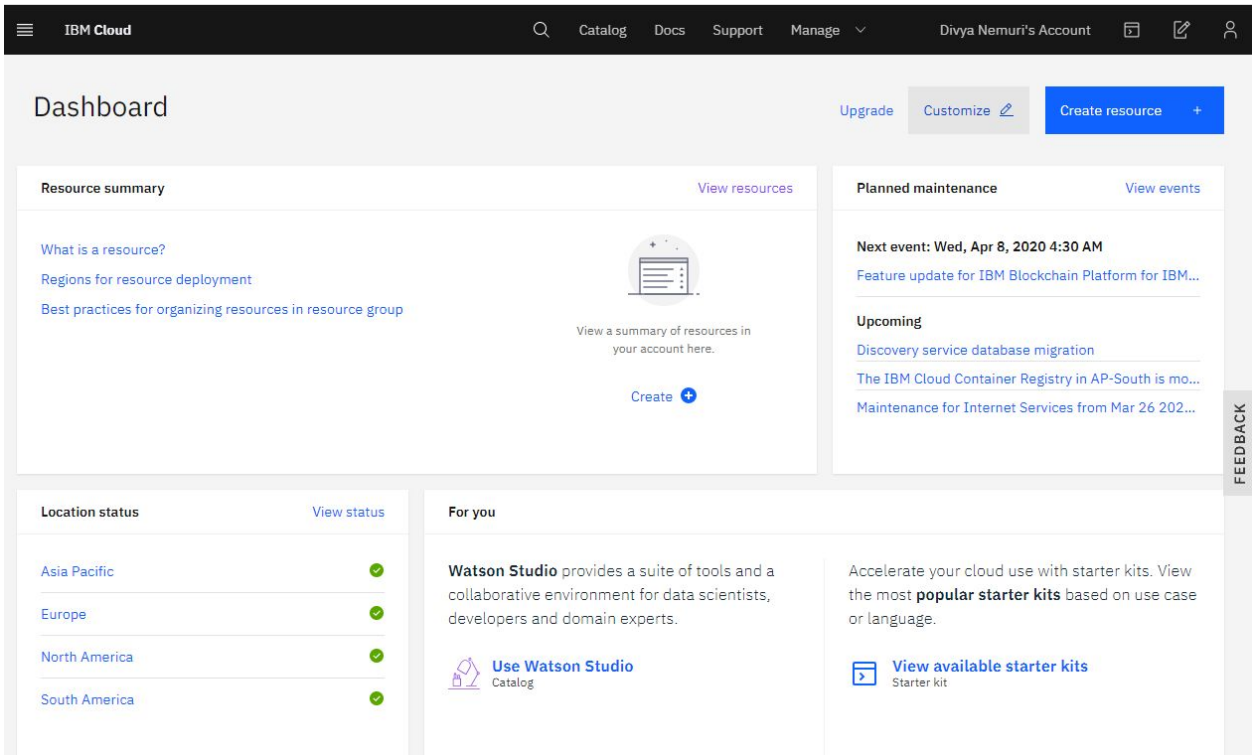
Brief: This tutorial will guide you in creating a device in the IBM IoT platform

Outcome:
In this tutorial, you will learn the following activities and tasks.

- Launching the IBM IoT platform
- Creating a device in the IBM IoT platform
- Generating the API keys for communicating/integrating with different applications
- Making a device secure with rules

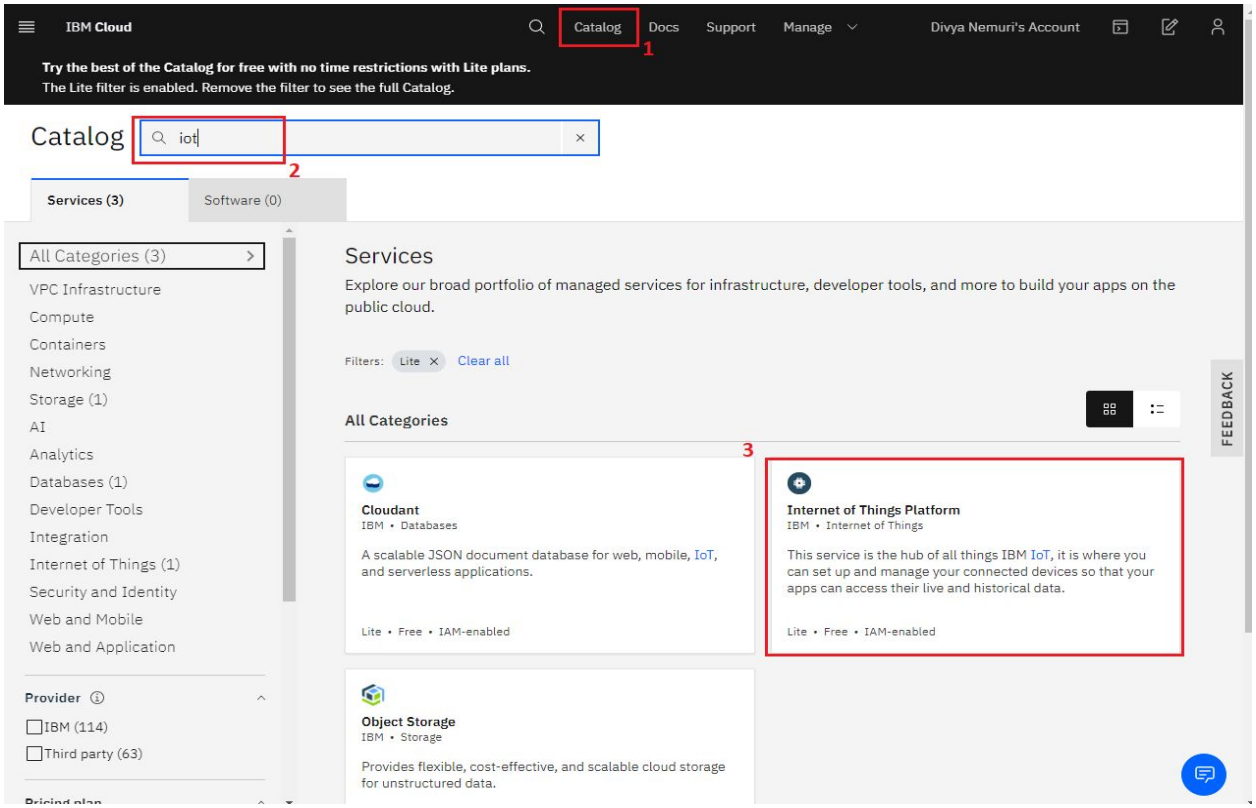
Activity:

Log in to Your IBM account using https://cloud.ibm.com/. Upon successful login to the cloud, you will be on the dashboard page. If you are a new user you won't have any resources listed. For a returning user, you will have your previous resources listed.

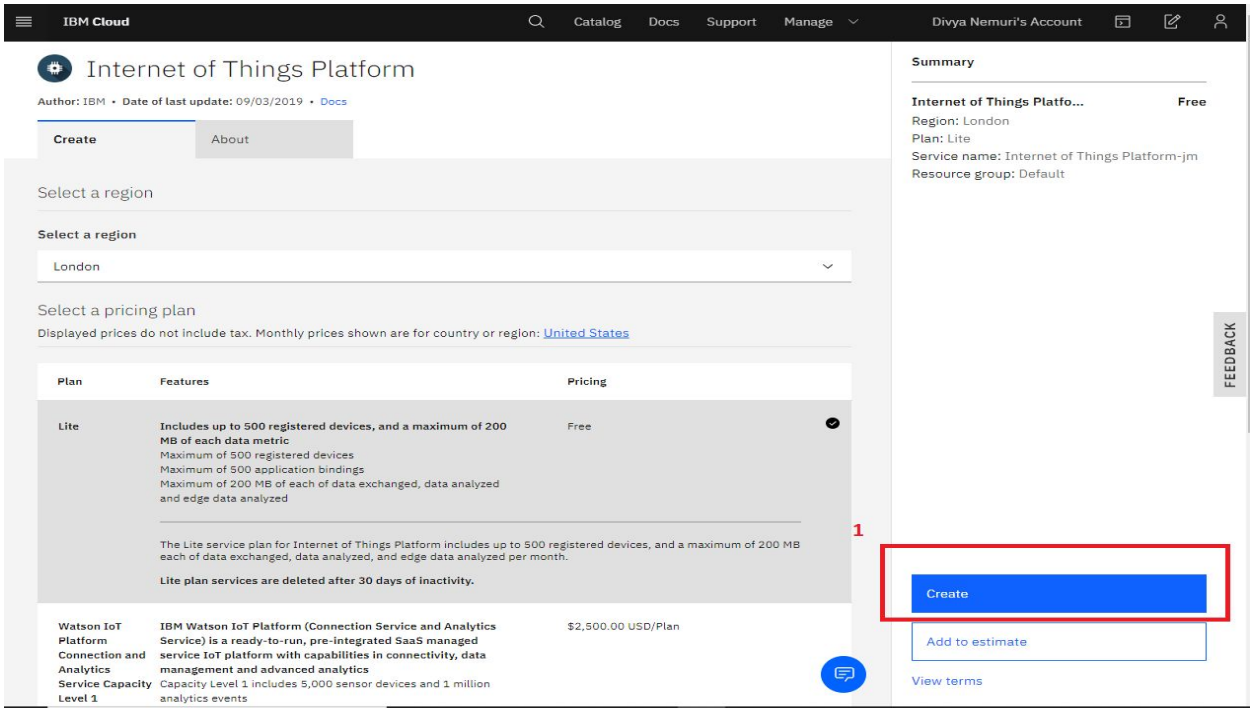


Task-1: Launch the IBM Watson IoT platform

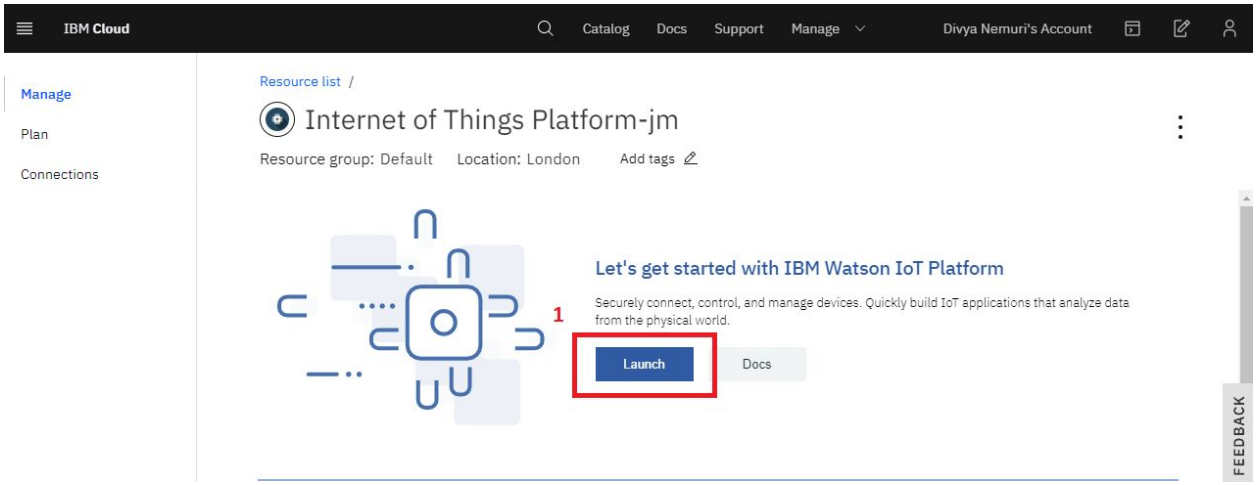
- Click on the catalog on the dashboard.
- Search for iot in the search bar provided.
- Click on the Internet of Things Platform to launch the IoT platform.



- Click on create to create an IoT platform for your project. Leave the default region provided.

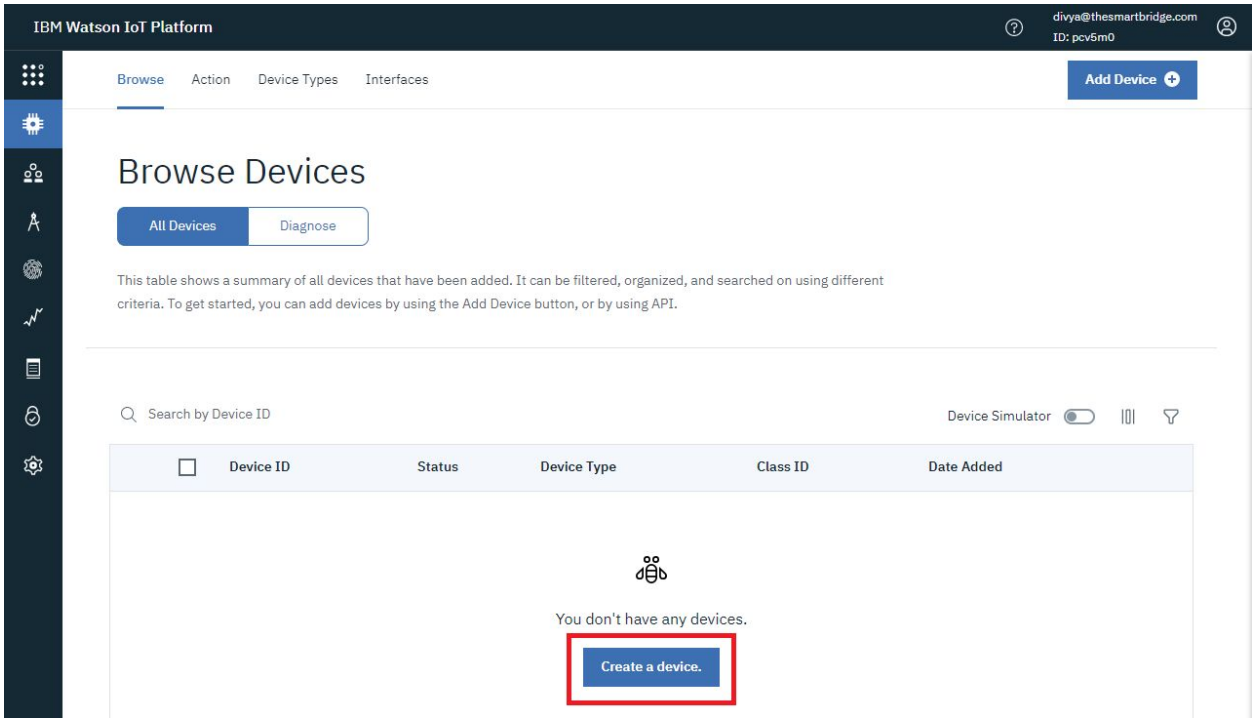


- After creating the IoT platform you are redirected to the IBM Watson IoT platform launch page. Click on the launch button to launch your IoT platform



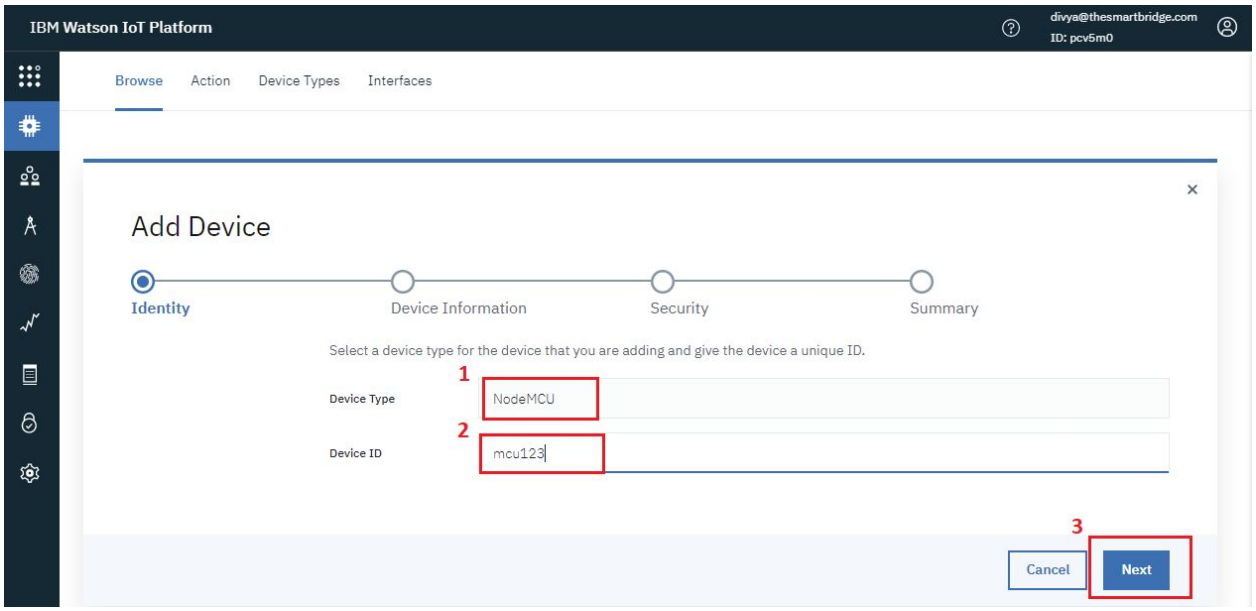
Task-2: IoT device creation

- After launching the platform you are in the IoT platform dashboard to create a device. Click on create to create a new device

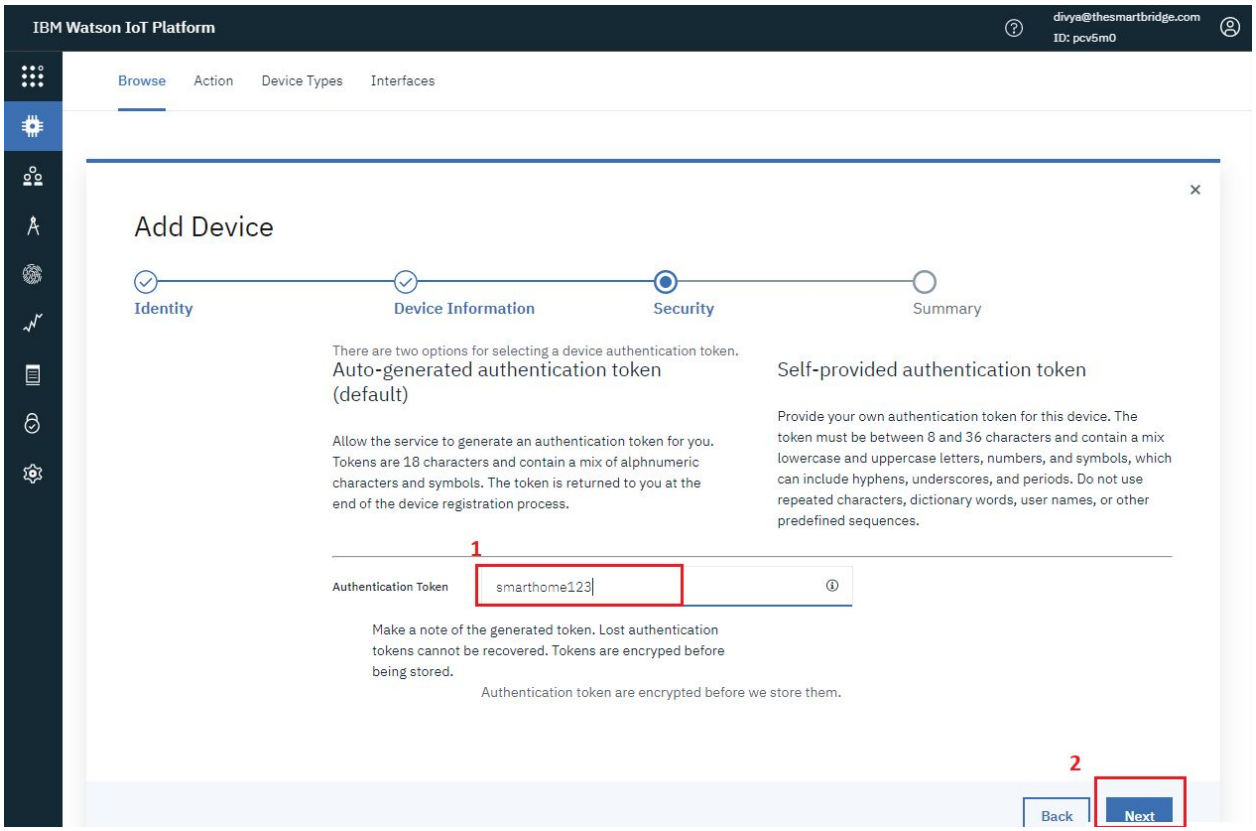


- Give a proper device type and device name related to your project or maybe related yo the microcontroller using for ease of access in the future. Click on next and you will be in the Device Information page where you can enter your device metadata like

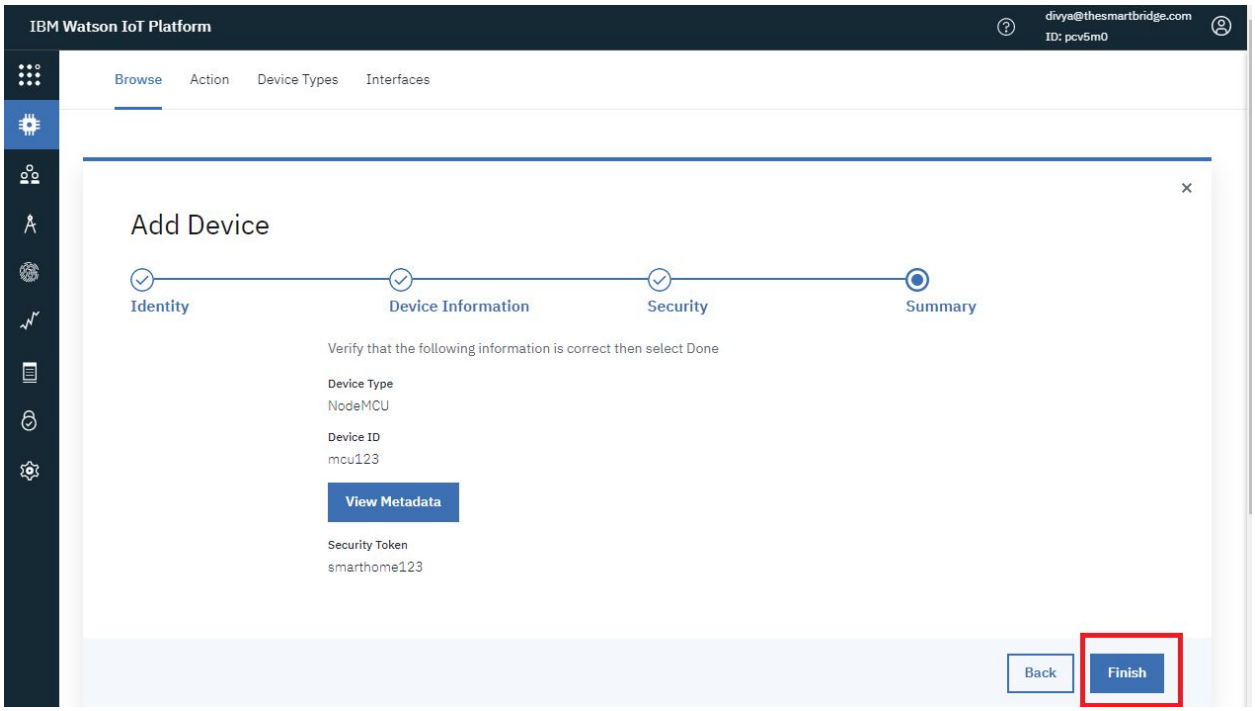
manufacturing number, model, description. It is not mandatory to fill those fields click on Next.



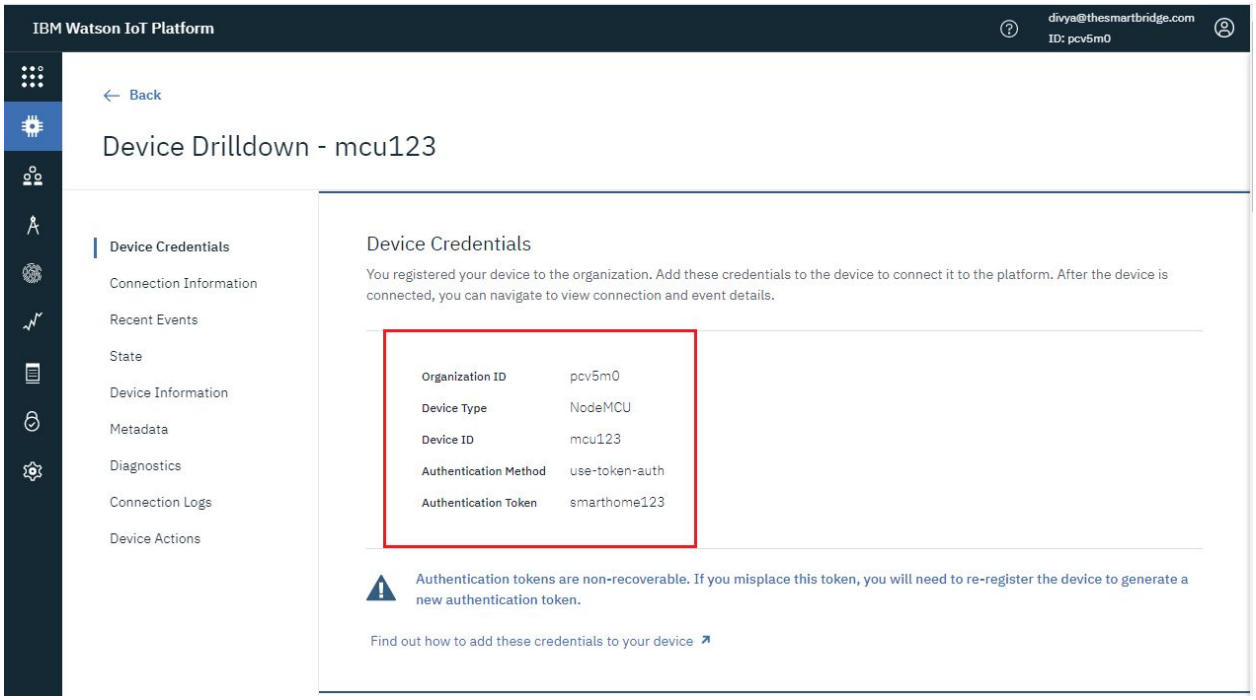
- In the security field, you should provide the authentication token to connect the device to the cloud. You can generate your own token or else the token can also be automatically generated. Click on next.



- In the summary page click on finish to complete the IoT device creation.

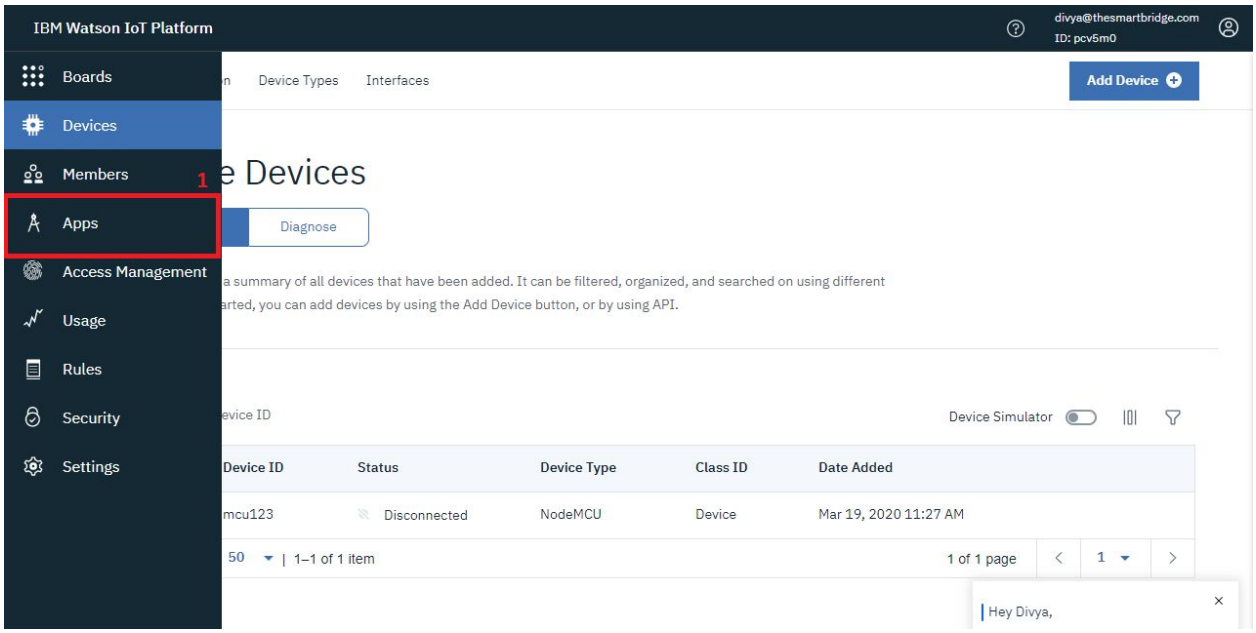


- Copy the device credentials you have created for your device. The credentials once lost can't be recovered as they are encrypted before saving in the cloud. So be cautious and copy them into a text file.

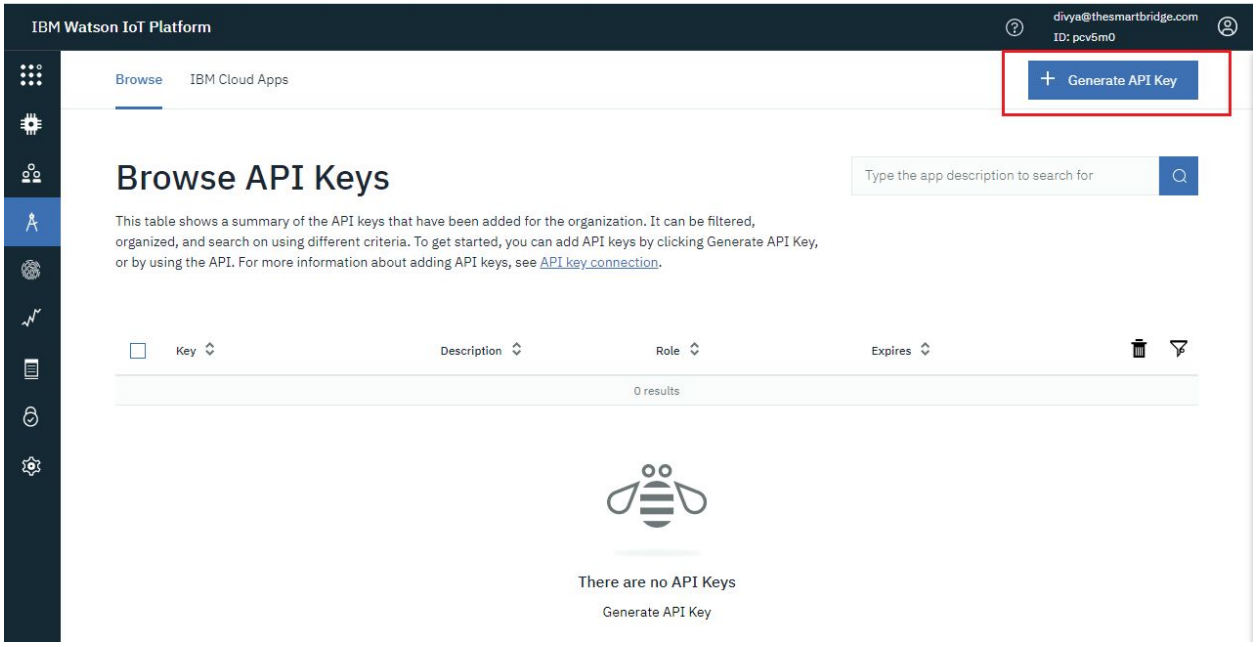


Task-3: API creation for Node-red application

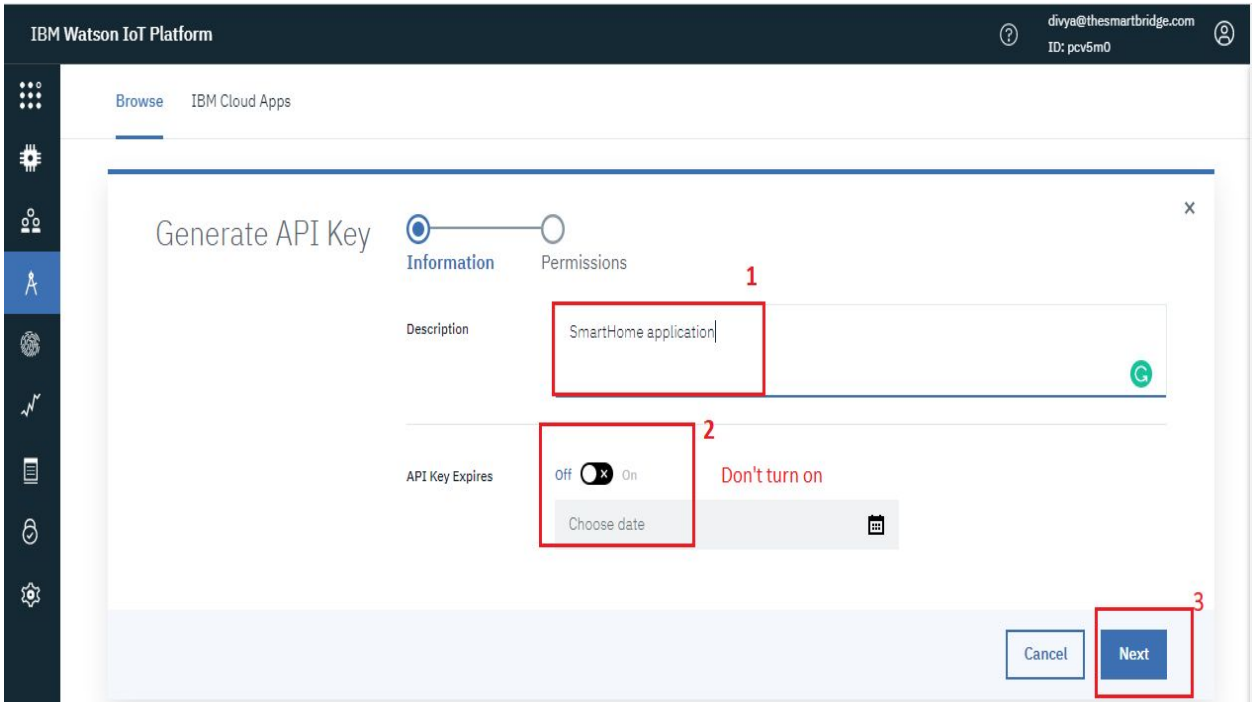
- Hover your mouse towards the device icon there you will be displayed with different sections in the IoT platform. Click on Apps for creating an API.



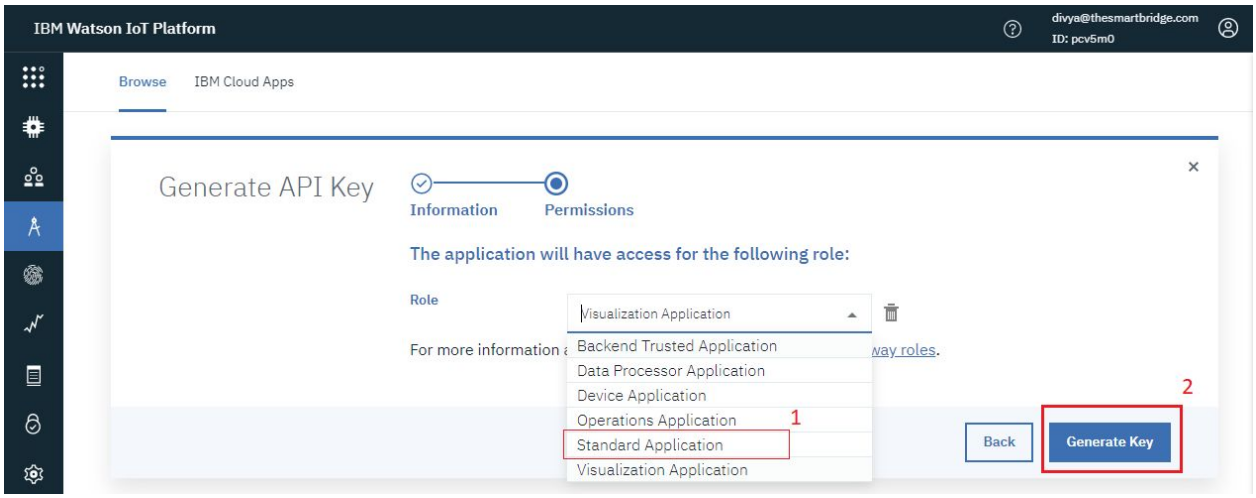
- After clicking on Apps you will be redirected to the Browse API keys page. For a new user or returning user click on the Generate API key button.



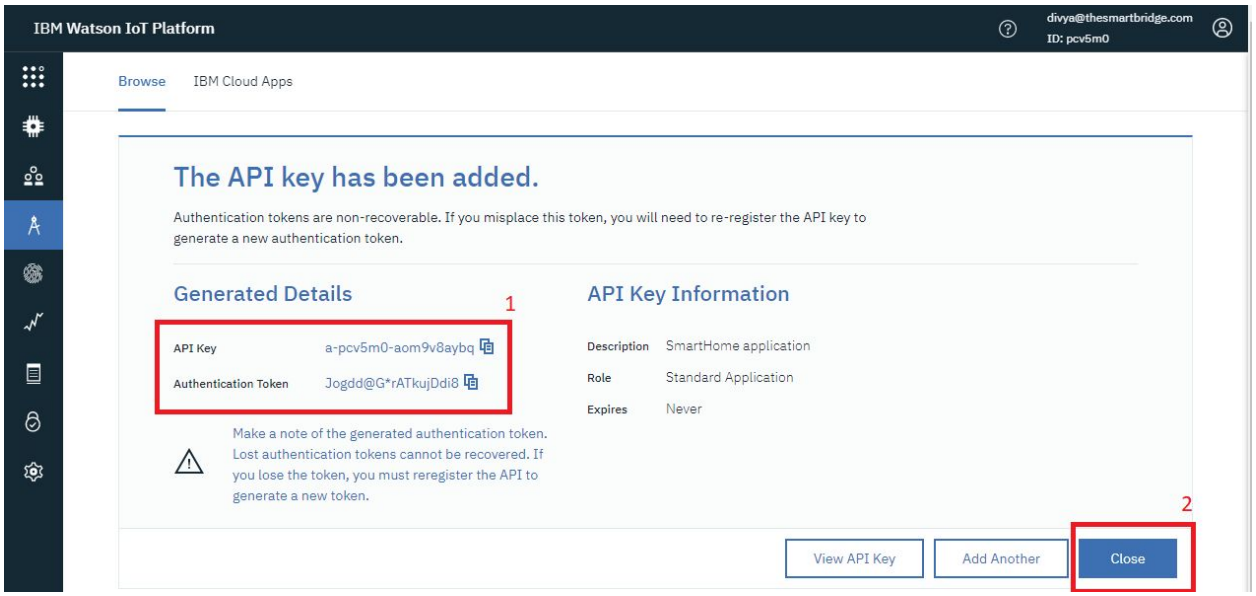
- In the information tab, provide the description of the API key you are generating for. The description may be about the project you are developing. Though it is not mandatory it is a good practice to identify the API key we have generated out of multiple.
- Don’t turn on the API expires unless you are aware of it. This will lead to expire your API key generated after the time period mentioned.
- Click on next for selecting the role of your API key



- In the roles tab, select the role as a standard application. Click on the generate key button to complete the API key generation.

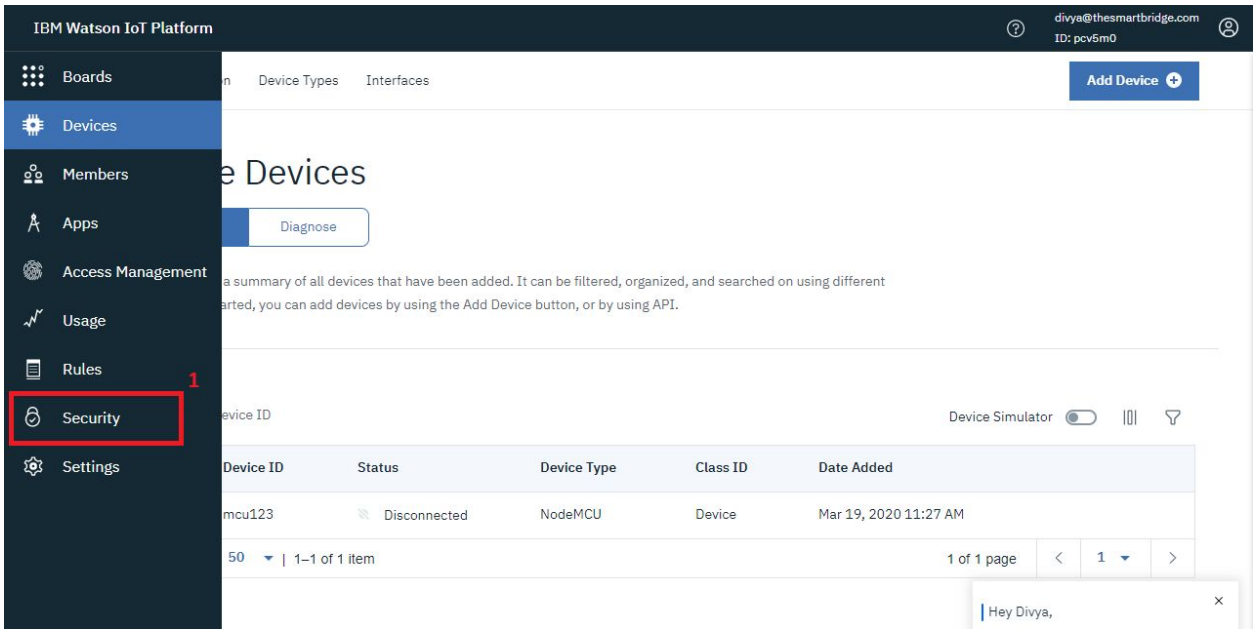


- Copy the generated API credentials into the text file you have created previously for the device credentials. Click on close.

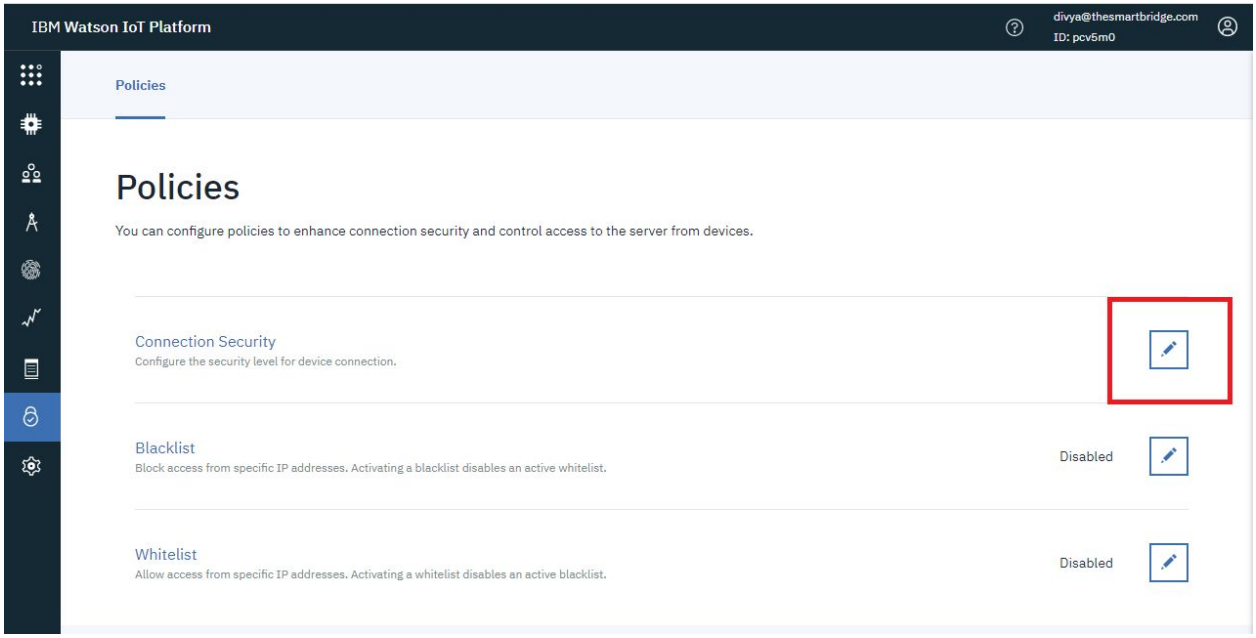


Task-4: Configuring the connection Security for the device created

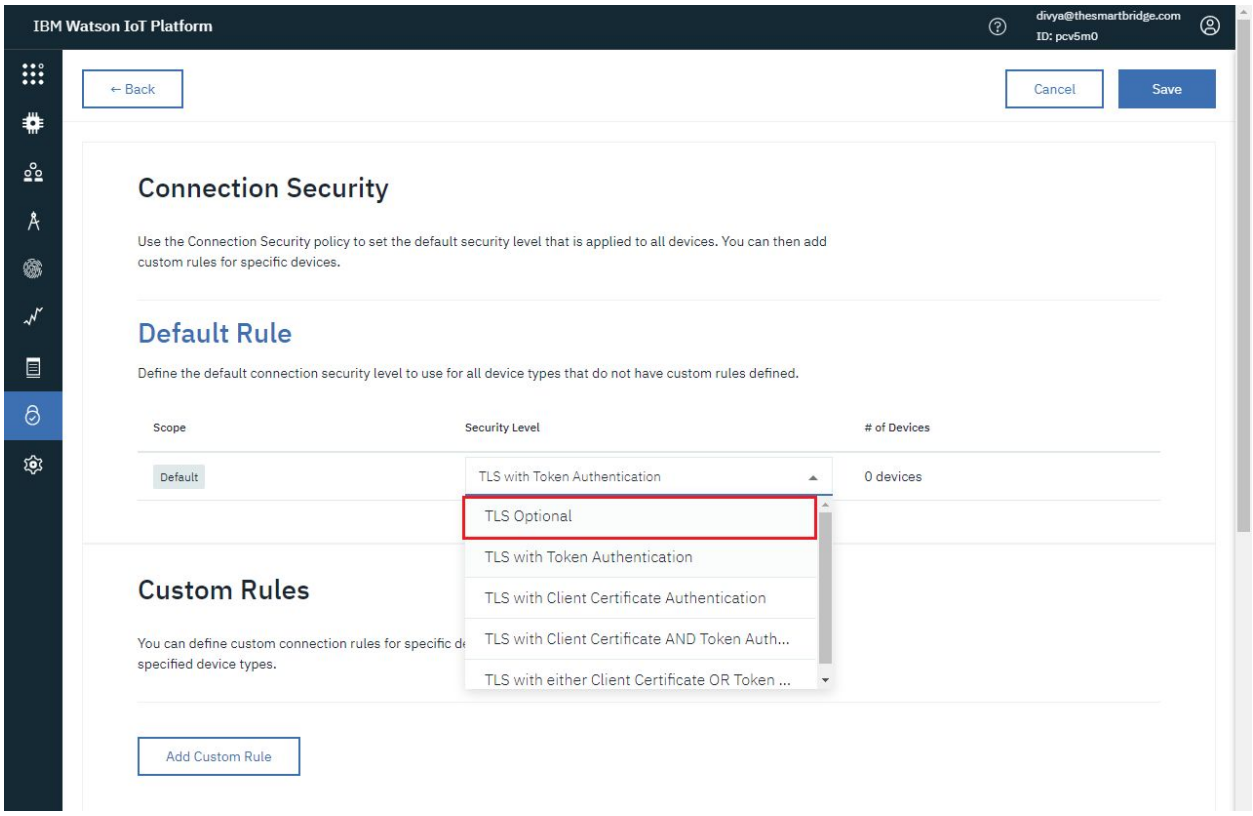
- Hover your mouse towards the navigation pane and click on Security for configuring the connection security.



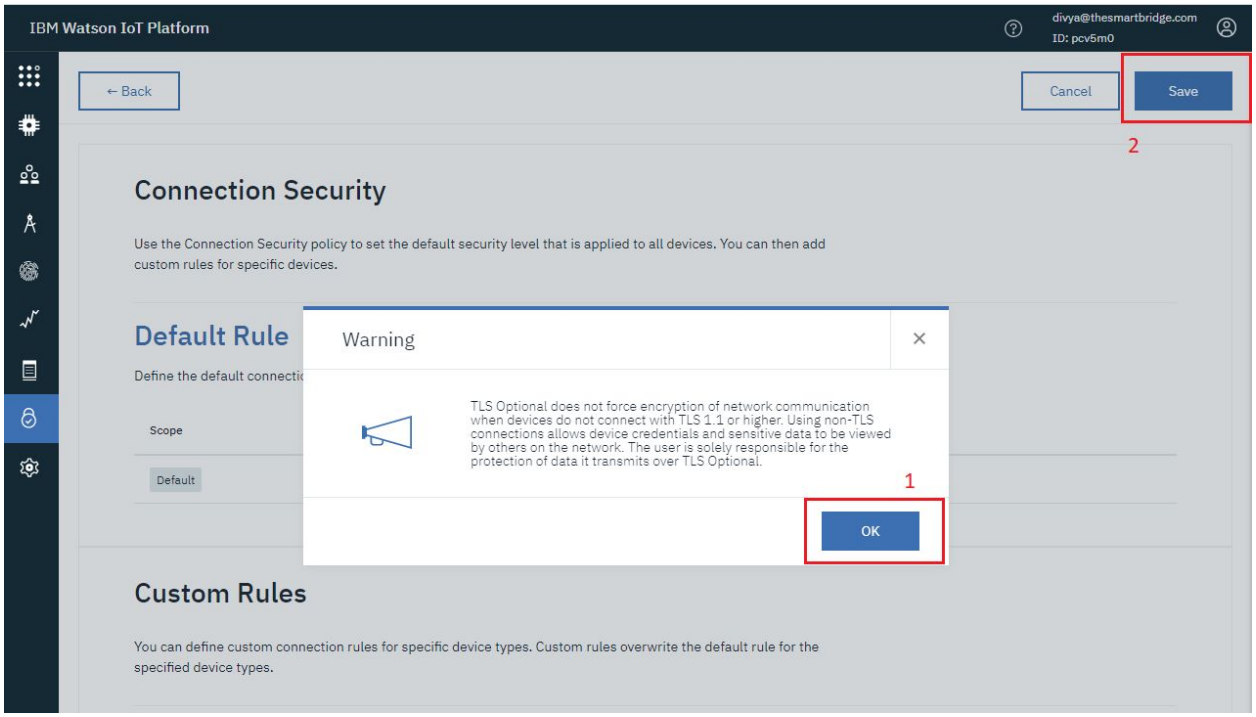
- In the Security tab, click on the edit icon for connection security



- In the connection security tab, select the default rule as TLS Optional



- After selecting the TLS optional rule you are prompted with a warning. Click on OK and then click on save for saving the rule created. If you don't save it, you have you to repeat the procedure of connection security again.


IBM Watson IoT Platform
divya@thesmartbridge.com
ID: pcv5m0
← Back
Cancel
Save
2
Connection Security
Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices.
Default Rule
Define the default connecti
Scope
Default
Warning
TLS Optional does not force encryption of network communication when devices do not connect with TLS 1.1 or higher. Using non-TLS connections allows device credentials and sensitive data to be viewed by others on the network. The user is solely responsible for the protection of data it transmits over TLS Optional.
1
OK
Custom Rules
You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types.