

IoT Device Creation

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

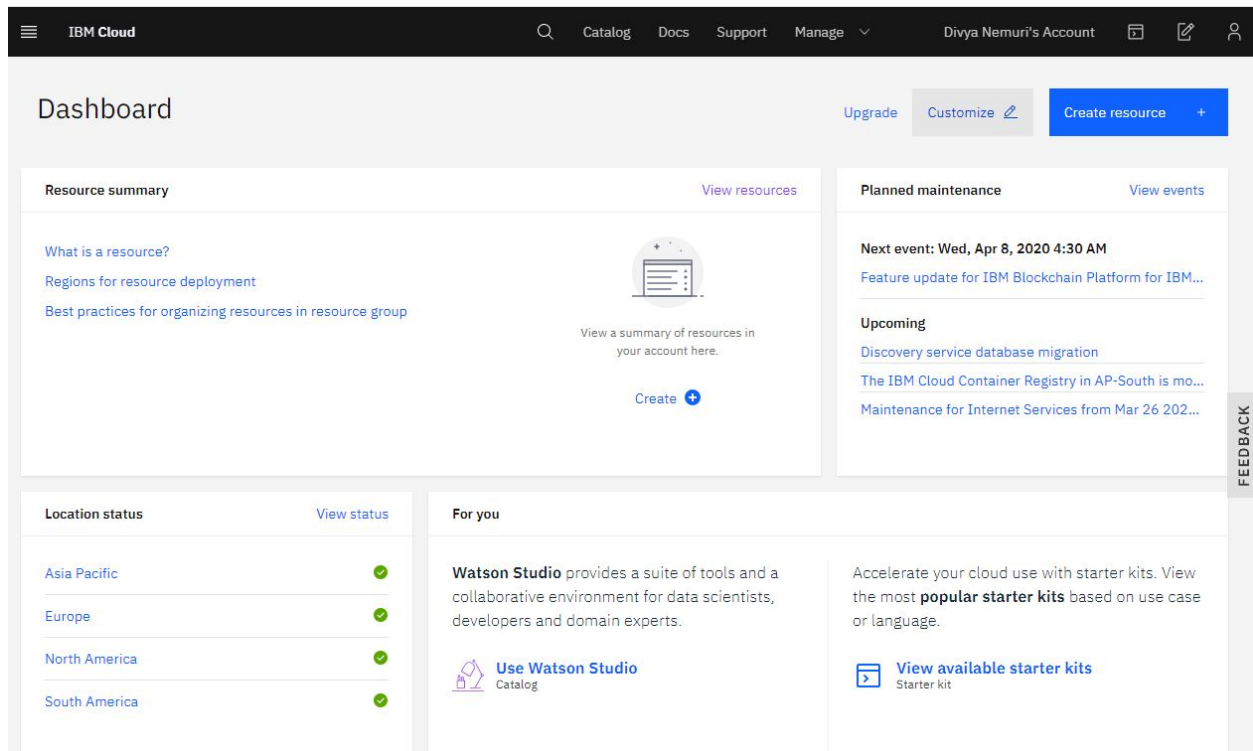
Outcome:

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.

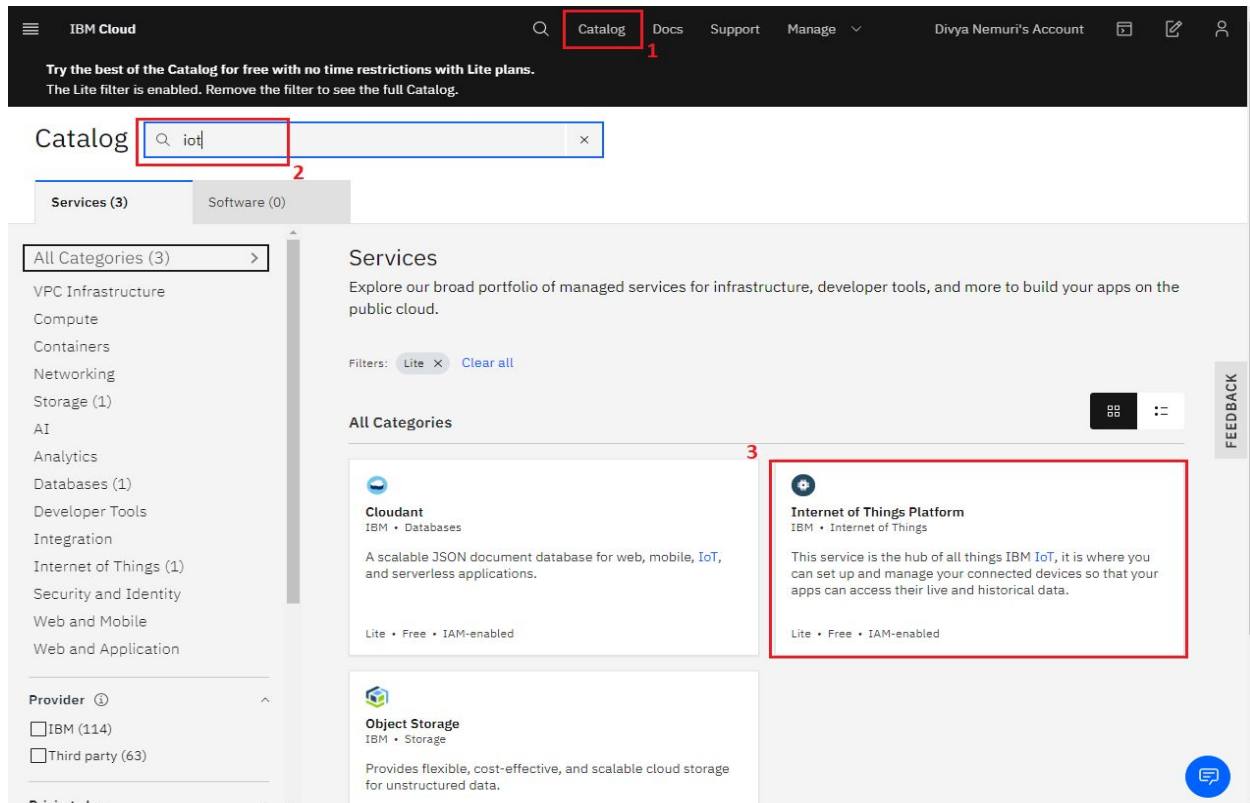


The screenshot shows the IBM Cloud Dashboard. At the top, there's a navigation bar with 'IBM Cloud', a search icon, and links for 'Catalog', 'Docs', 'Support', and 'Manage'. The user's account 'Divya Nemuri's Account' is also visible. The main dashboard area is divided into several sections: 'Resource summary' with links for 'What is a resource?', 'Regions for resource deployment', and 'Best practices for organizing resources in resource group'; 'Planned maintenance' showing the next event on Wed, Apr 8, 2020 4:30 AM; 'Location status' with a table showing regions like Asia Pacific, Europe, North America, and South America, all with green checkmarks; and 'For you' which includes a 'Watson Studio' recommendation and a 'View available starter kits' link. A 'FEEDBACK' button is visible on the right side of the dashboard.

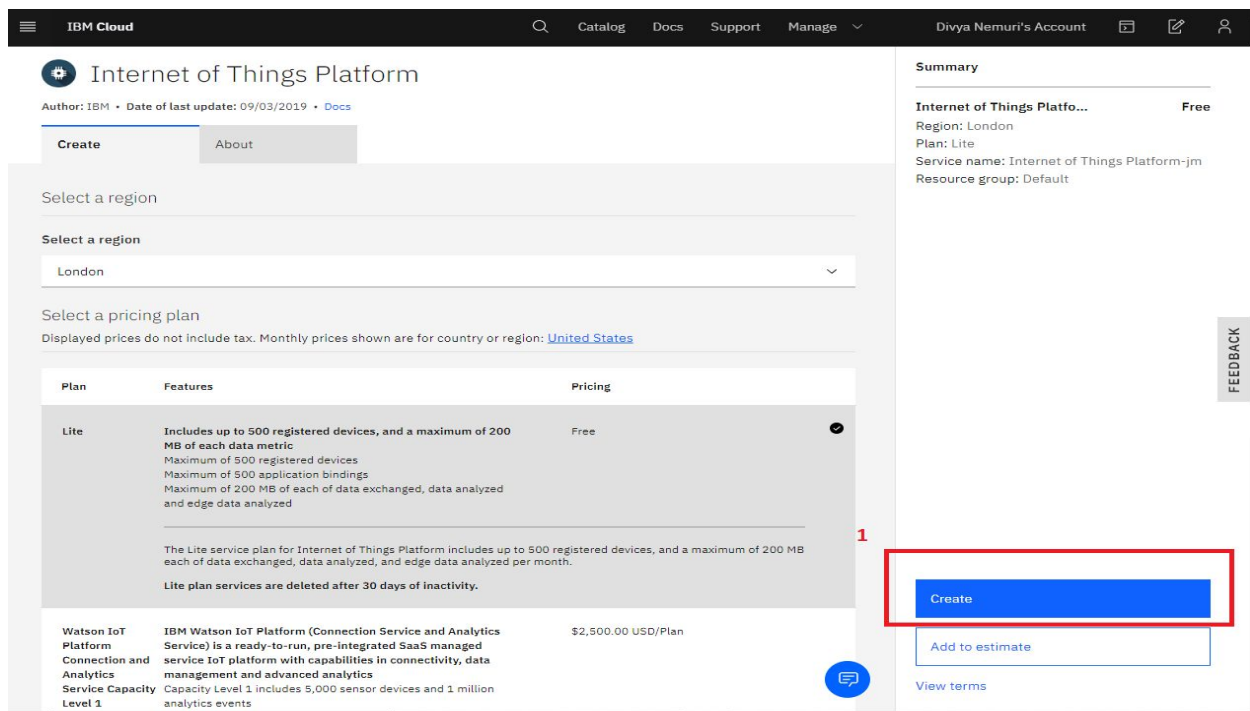
Location status	View status
Asia Pacific	✓
Europe	✓
North America	✓
South America	✓

Task-1: Launch the IBM Watson IoT platform

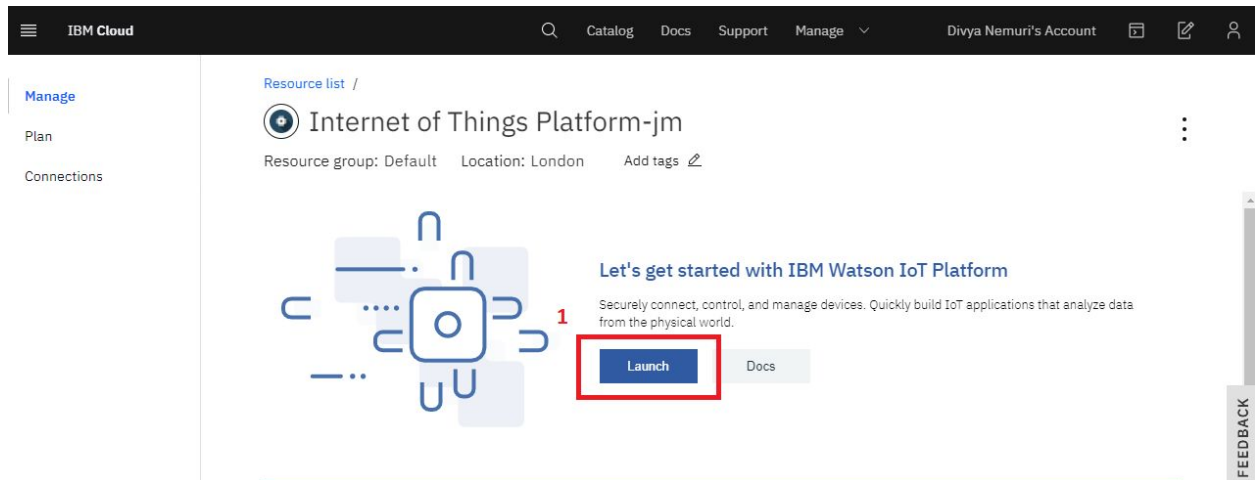
- Click on the catalog on the dashboard.
- Search for iot in the search bar provided.
- Click on the Internet of Things Platform to launch the IoT platform.



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

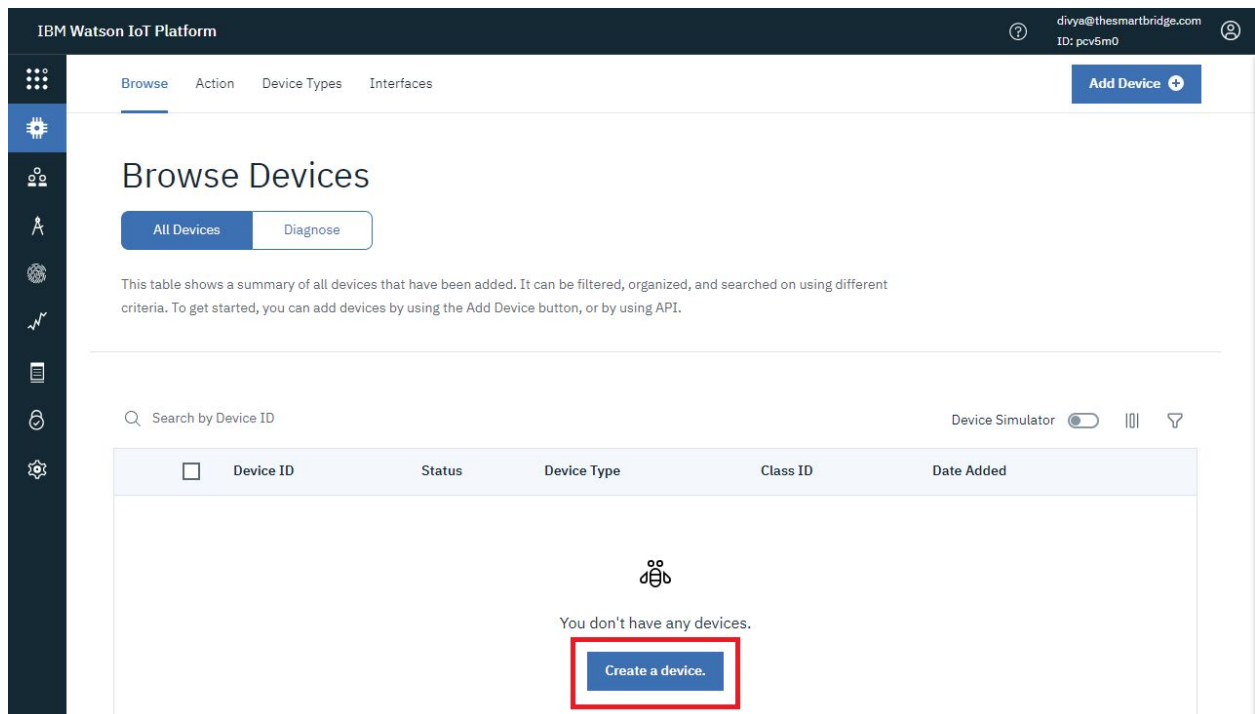


- After creating the IoT platform you are redirected to the IBM Watson IoT platform launch page. Click on the launch button to launch your IoT platform



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 to 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.

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse Action Device Types Interfaces

Add Device

Identity Device Information Security Summary

Select a device type for the device that you are adding and give the device a unique ID.

Device Type NodeMCU

Device ID mcu123

Cancel 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.

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse Action Device Types Interfaces

Add Device

Identity Device Information Security Summary

There are two options for selecting a device authentication token.

Auto-generated authentication token (default)

Allow the service to generate an authentication token for you. Tokens are 18 characters and contain a mix of alphanumeric characters and symbols. The token is returned to you at the end of the device registration process.

Self-provided authentication token

Provide your own authentication token for this device. The token must be between 8 and 36 characters and contain a mix of lowercase and uppercase letters, numbers, and symbols, which can include hyphens, underscores, and periods. Do not use repeated characters, dictionary words, user names, or other predefined sequences.

Authentication Token smarthome123

Make a note of the generated token. Lost authentication tokens cannot be recovered. Tokens are encrypted before being stored.

Authentication token are encrypted before we store them.

Back Next

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

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse Action Device Types Interfaces

Add Device

Identity Device Information Security Summary

Verify that the following information is correct then select Done

Device Type
NodeMCU

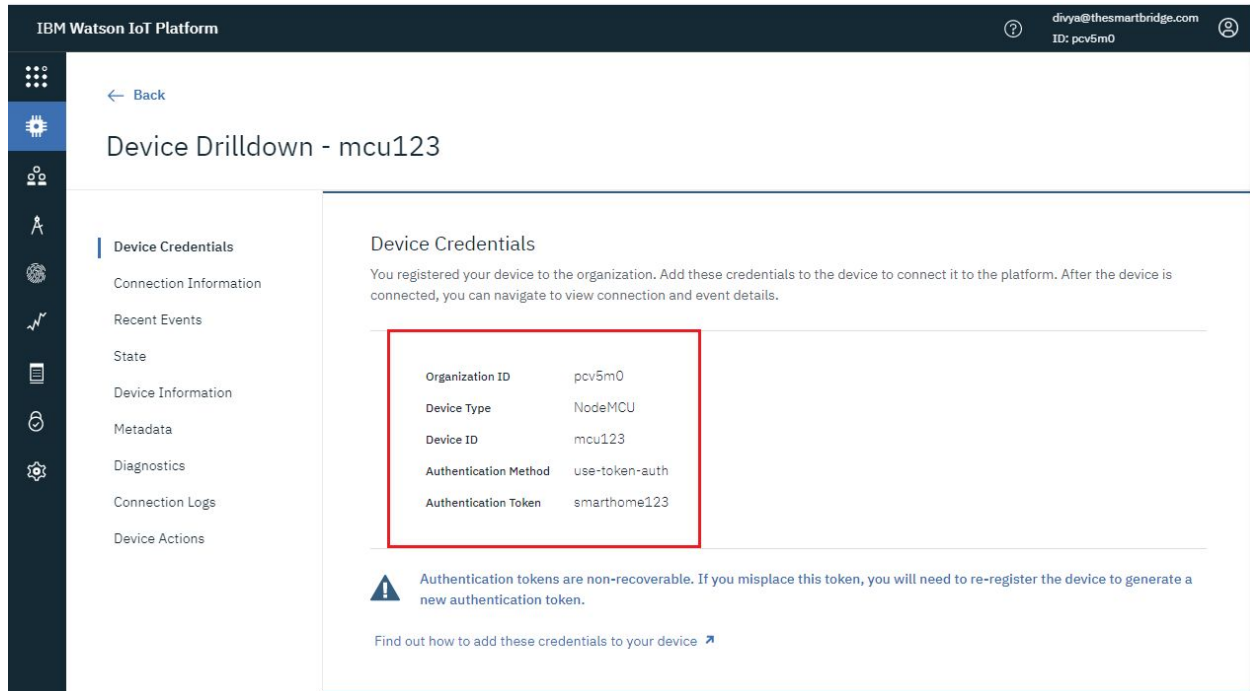
Device ID
mcu123

[View Metadata](#)

Security Token
smarhome123

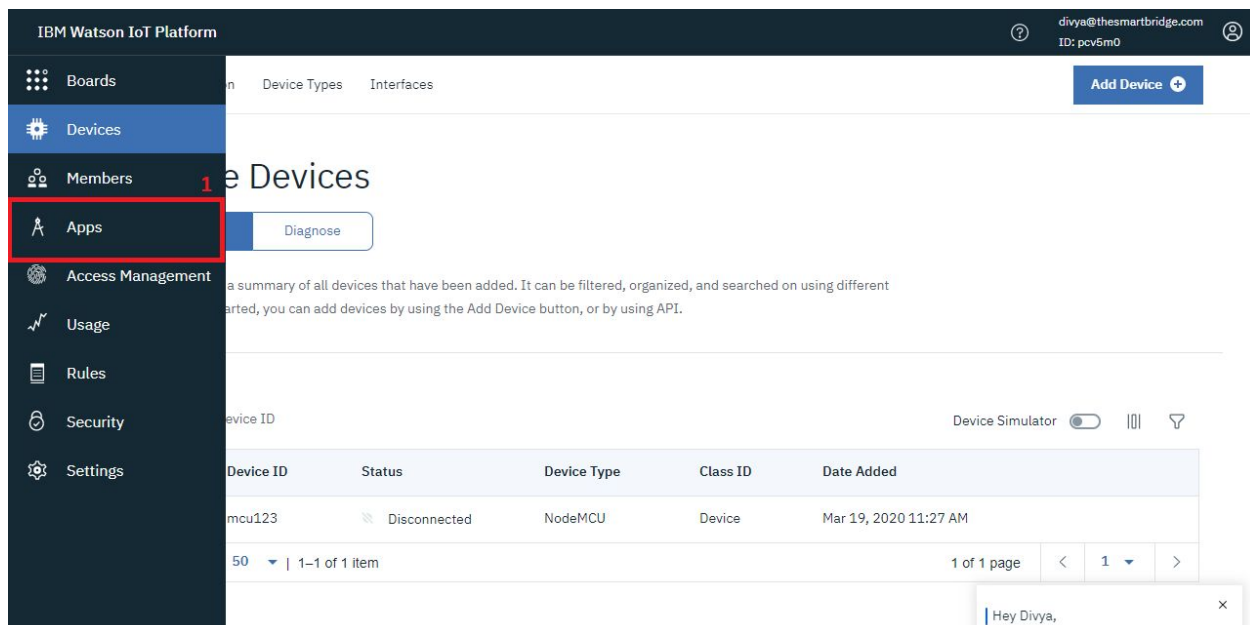
[Back](#) [Finish](#)

- 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.

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse IBM Cloud Apps

Generate API Key

Browse API Keys

Type the app description to search for

This table shows a summary of the API keys that have been added for the organization. It can be filtered, organized, and search on using different criteria. To get started, you can add API keys by clicking Generate API Key, or by using the API. For more information about adding API keys, see [API key connection](#).

Key	Description	Role	Expires
0 results			

There are no API Keys

Generate API Key

- 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

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse IBM Cloud Apps

Generate API Key

Information Permissions

Description SmartHome application

API Key Expires Off On Don't turn on

Choose date

Cancel Next

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

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

Browse IBM Cloud Apps

Generate API Key

Information Permissions

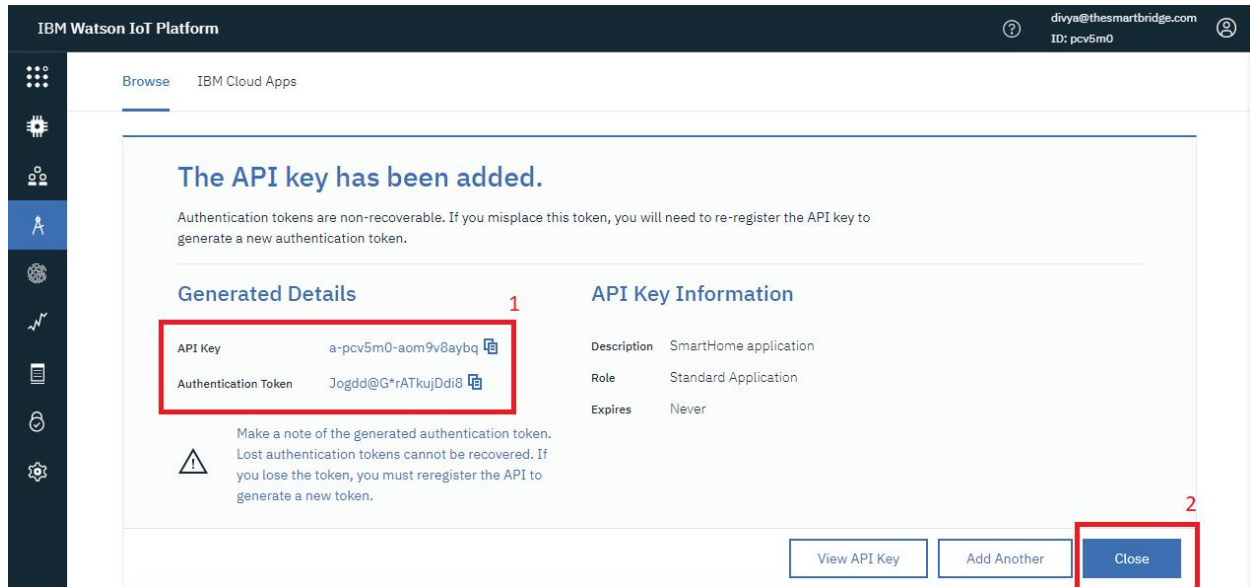
The application will have access for the following role:

Role Visualization Application

For more information: Backend Trusted Application Data Processor Application Device Application Operations Application Standard Application Visualization Application

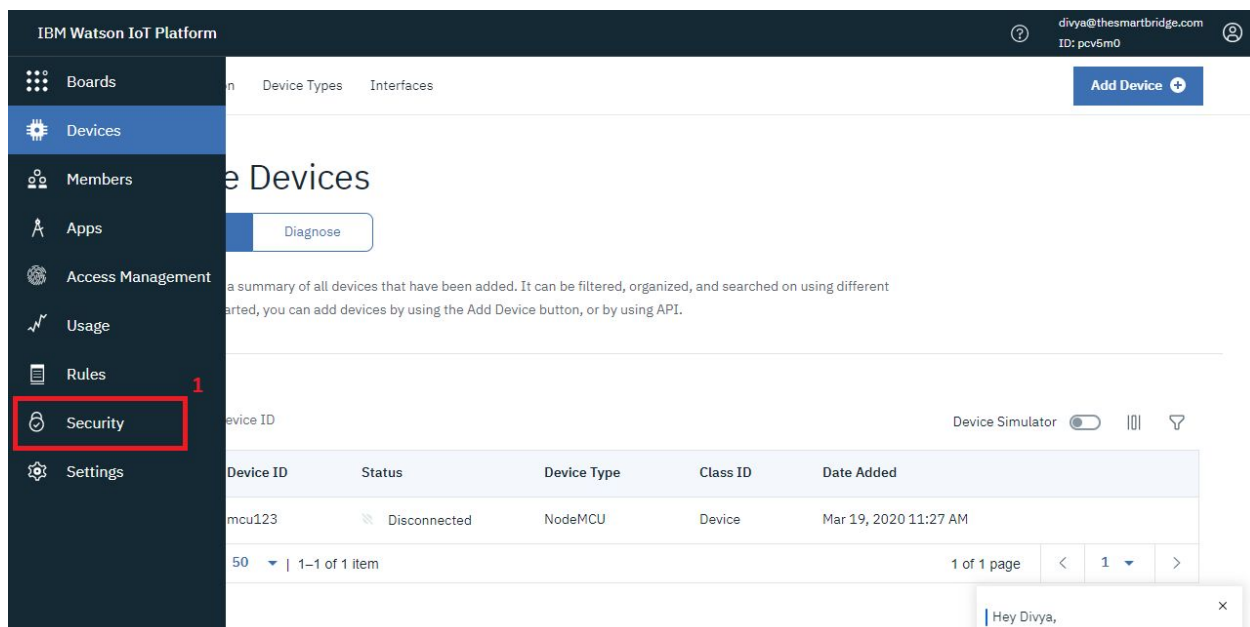
Back Generate Key

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

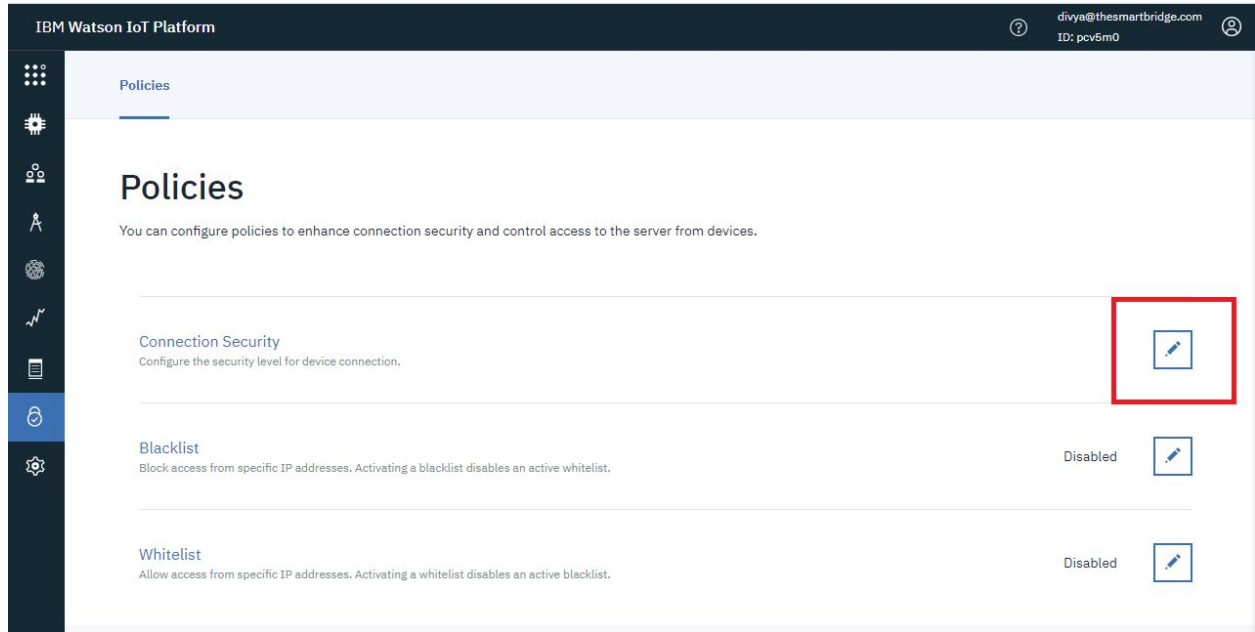


Task-4: Configuring the connection Security for the device created

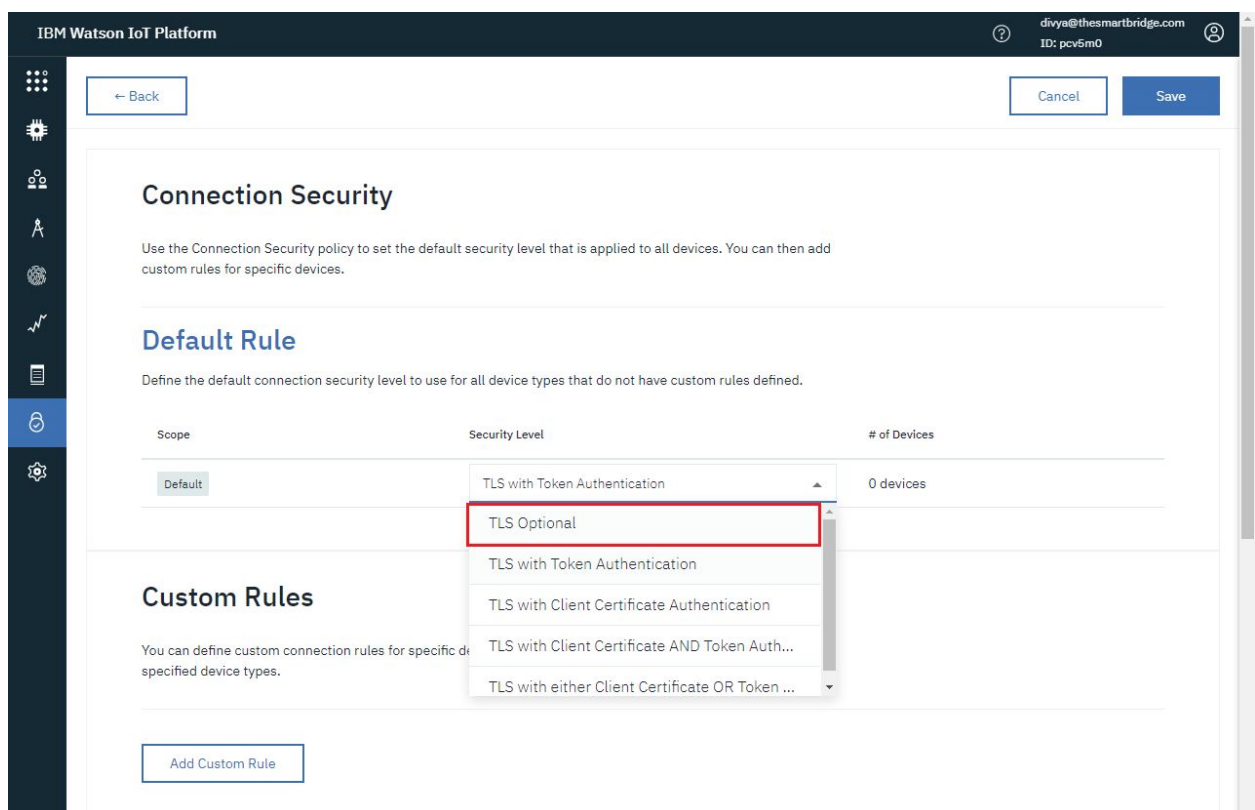
- Hover your mouse towards the navigation pane and click on Security for configuring the connection security.



- 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 to repeat the procedure of connection security again.

IBM Watson IoT Platform

divya@thesmartbridge.com
ID: pcv5m0

← Back

CancelSave

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 connection security policy.

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.

OK

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types.