CK-RX65N

SIM activation, Creating the trial account and using Dashboard with RYZ014A or Ethernet Application for AWS - Getting Started Guide

Introduction

This document describes a system that uses the CK-RX65N Cloud Kit board from Renesas. This system incorporates the CK-RX65N running Amazon FreeRTOS and via an Ethernet connection visualizes HS3001, ZMOD4410, ZMOD4510, OB1203, ICP10101 and ICM20948 sensors information on Amazon Web Services (AWS) and controls LEDs on the board.

There are two ways of connectivity for CK-RX65N. One is the Ethernet, second is the Cellular CAT M1 using RYZ014A.This document shows both connectivity.

And this document shows the way of below items:

- ✓ **How to activate the SIM card that is contained the CK-RX65N**
- ✓ **How to create the 10 USD of free trial account for AWS**
- ✓ **How to operate and install the information of certification for cloud**
- ✓ **How to see and run the sensor data on the dashboard**

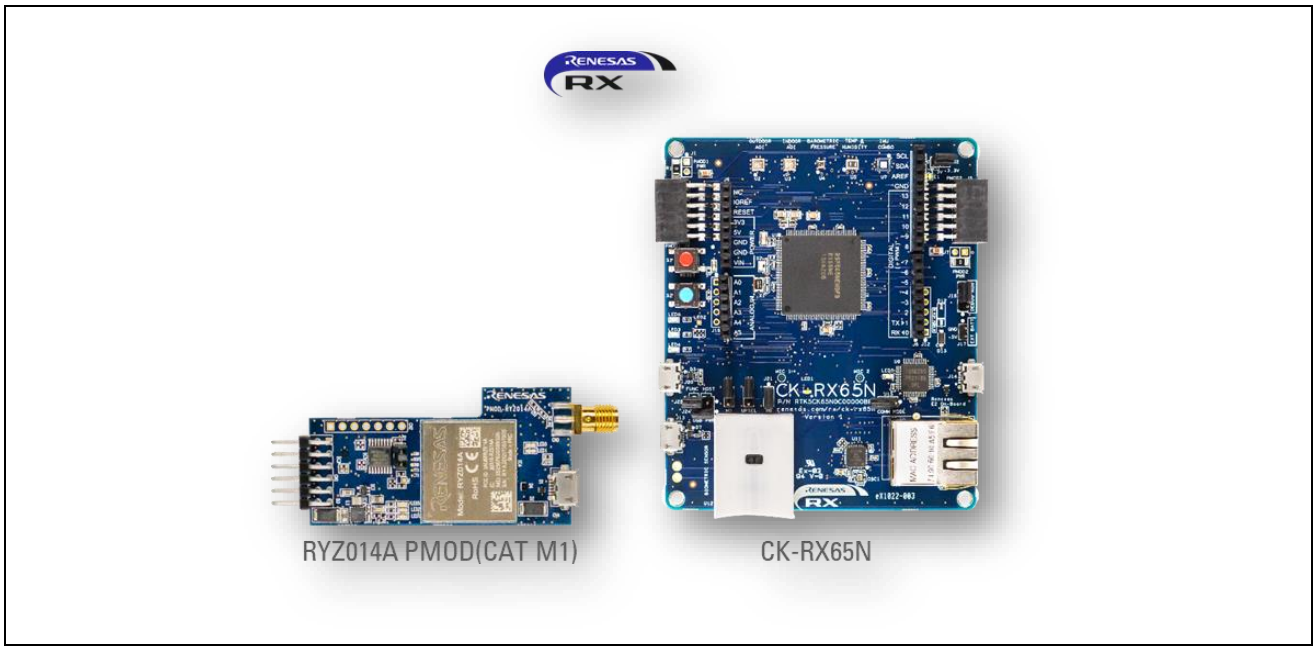


Figure 1 CK-RX65N(with RYZ014A Pmod)

Web site

- RX Cloud solution Web

https://www.renesas.com/rx-cloud

- CK-RX65N Web

https://www.renesas.com/rx/ck-rx65n

Contents

1. Terms 4
2. Preparation 4
2.1 Hardware Configuration 4
2.2 Software Configuration 4
2.3 Tera term Setting 4
3. System Diagram 5
4. Connection to AWS 5
4.1 Common users: To import the project, activate SIM card 6
4.1.1 Import the project 6
4.1.2 Data Publishing Interval Settings (Optional) 15
4.1.3 Running the Application Project 16
4.1.4 Running the application & activation of SIM card contain with CK-RX65N 19
4.1.5 Activating a SIM card on Truphone 19
4.1.6 Activating a SIM card on MicroAI Launchpad 23
4.2 For Users who use provided dashboard and AWS account of Kit 29
4.2.1 Getting the UUID Information of the Board 30
4.2.2 To get the account 10USD of trial of AWS 30
4.3 Hardware Preparation 32
4.4 Software Preparation-Run Project from IDE 33
4.4.1 Storing the Device Certificate, Key, MQTT Broker endpoint and IoT Thing name 33
4.5 For User using their own AWS Account 39
4.5.1 For install the credential 48
4.6 About Connecting to AWS IoT 49
4.7 Verifying the Application Project using AWS Dashboard and Renesas Dashboard 49
4.8 LED Alerts 51
5. Restrictions 53
5.1 Communication time (Cellular version of Project) 53
6. Note and trouble shooting 54
6.1 About stabilization time for sensor 54
6.2 Connection issue when using Ethernet (Wired cable) 54
6.3 About the trouble of current supply short when using RYZ014A 54
6.4 About when build errors occur 54
6.5 About when unable to log in to the Dashboard (Grafana account) 54
6.6 Notes on Performing Firmware Update Over-The-Air on AWS FreeRTOS 55

Revision History 56

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products 1

Notice 1

Corporate Headquarters 1

Contact information 1

Trademarks 1

1. Terms

Terms

Terms used in this document are explained below.

Table 1.1 Terms

Term	Meaning
AWS	AWS Amazon Web Service

2. Preparation

2.1 Hardware Configuration

The hardware configuration of the demo project is listed in the table below.

Item	Content	Description
CK-RX65N Cloud Kit	Target board for CK-RX65N	Please see detail https://www.renesas.com/rx/ck-rx65n
RYZ014A Cellular PMOD module	SIM card	This Pmod is contained with CK-RX65N of kit with SIM card
PC	Windows 10 Google chrome	Recommended OS Web browser used

2.2 Software Configuration

The software configuration of the demo project is listed in the table below.

Item	Content	Version
Integrated development environment	e2 studio	2022-01
Complier	CC-RX GCC(Planning)	V3.03 -
Communication Software	Tera term	Version 4.106
Emulator	E2 emulator Lite (on-board)	-
RTOS	AWS FreeRTOS	V202107.00

2.3 Tera term Setting

Item	Settings
Baud rate	115200
Data length	8
Parity	none
Stop bits	1
Flow Control	none

3. System Diagram

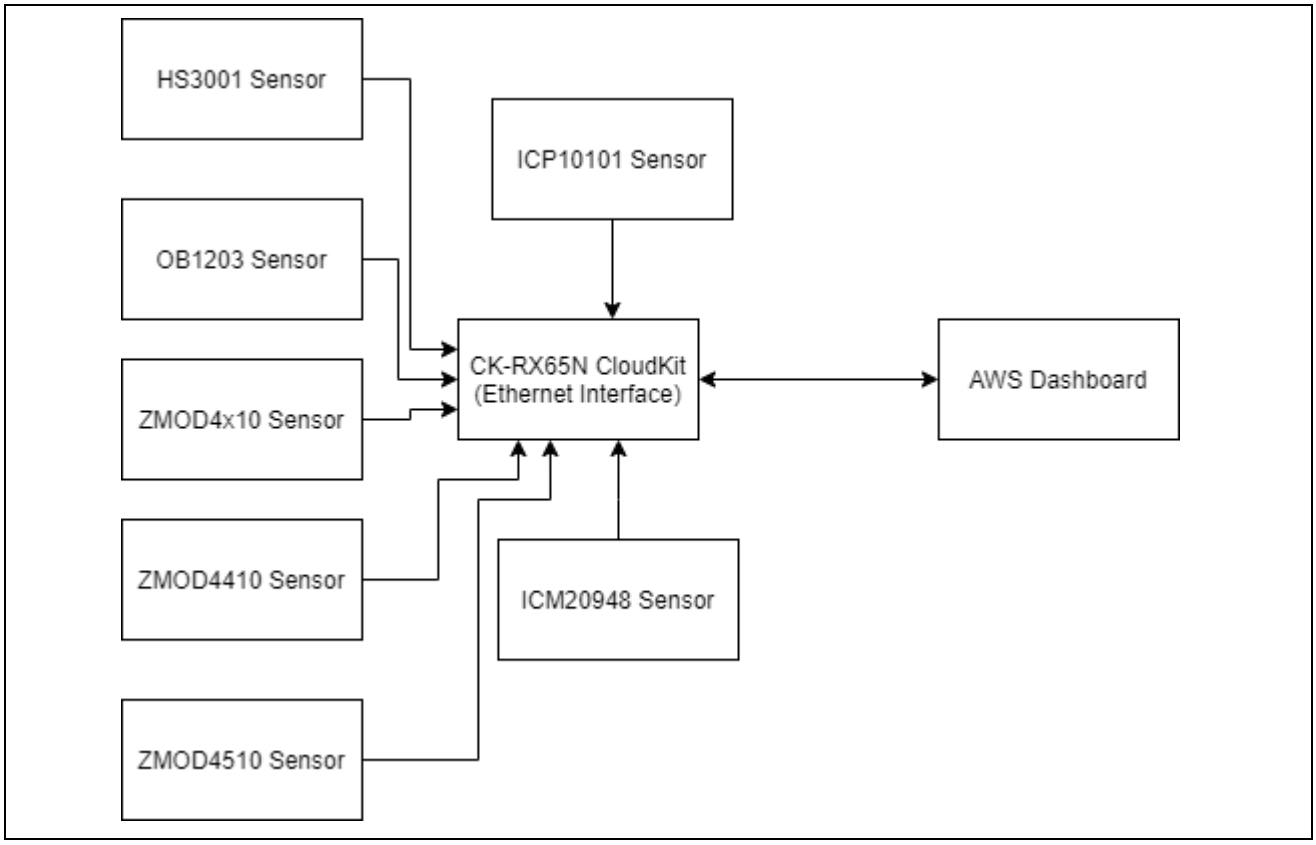


Figure 2 System Diagram

4. Connection to AWS

The following preparation is necessary in order to connect CK-RX65N Cloud Kit to AWS.

We provide the 10USD of AWS account to Users who buy the CK-RX65N.

So, this document both case of way to connect AWS account.

- **Case 1** :**you are the User who bought the kit**, please see "**4.1 Common**" section and from "**4.2 For Users who use provided dashboard and AWS account of Kit**" section.
- **Case 2** : Other users please see "**4.1 Common**" section from "**4.5 For User using their own AWS Account"** section.

4.1 Common users: To import the project, activate SIM card

4.1.1 Import the project

Follow the steps below to prepare the software for the demo program.

1. Extract the project files from the archive and copy them to the C drive.
   Please unzip it the project file to **the short path of your PC**.
   If the path is deep, it happened the build error due to the file path length issue.

2. Launch e2 studio and specify a workspace directory and click Launch

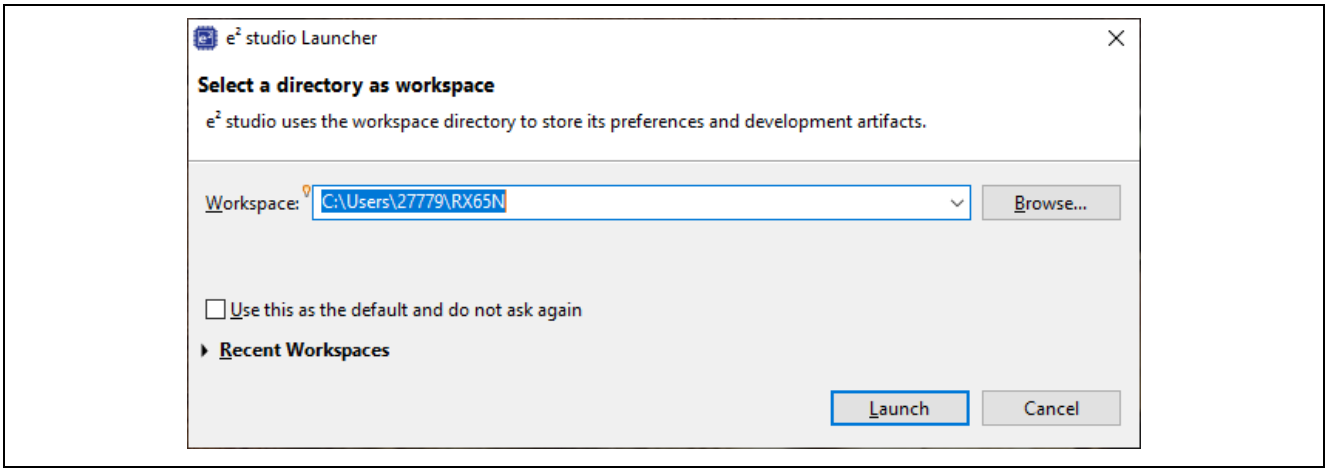


Figure 3 Launch e2 studio

3. Select File → Import….

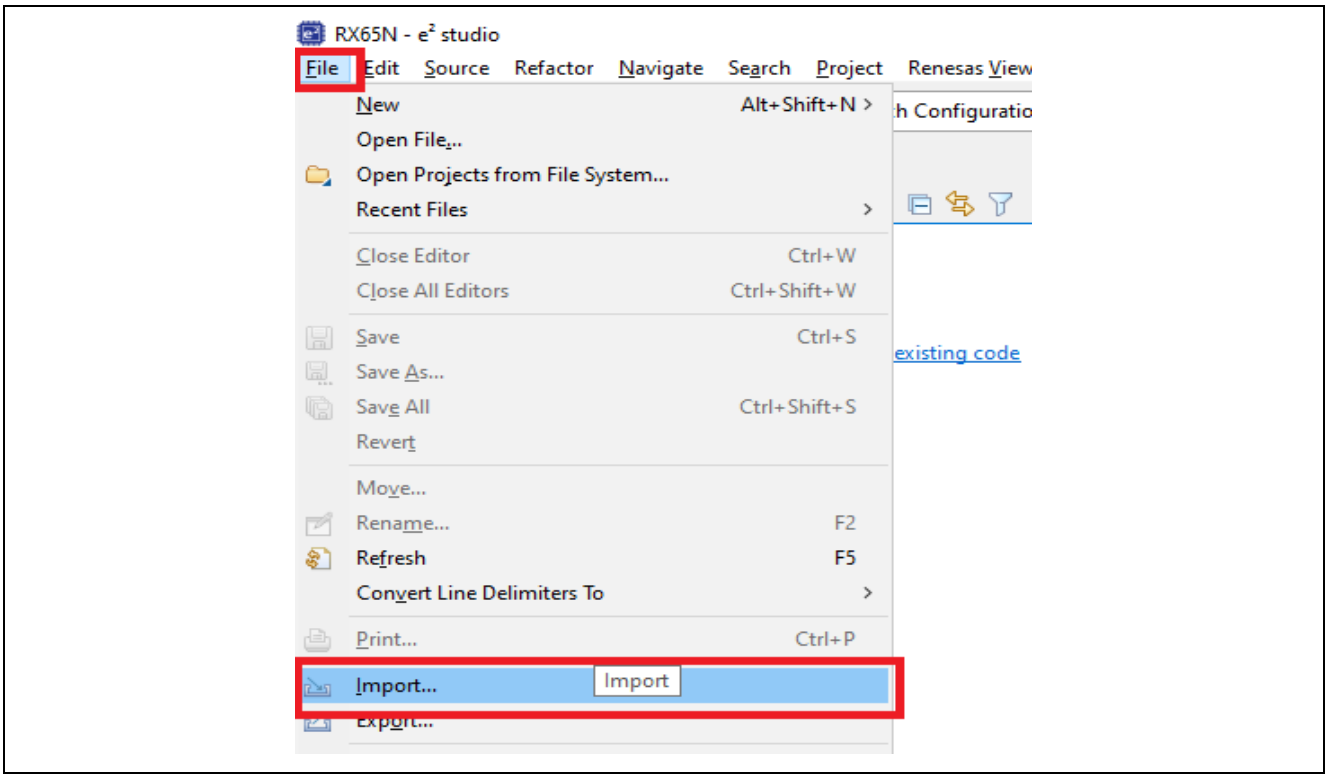


Figure 4 select import

4. Click General → Existing Projects into Workspace → Next >.

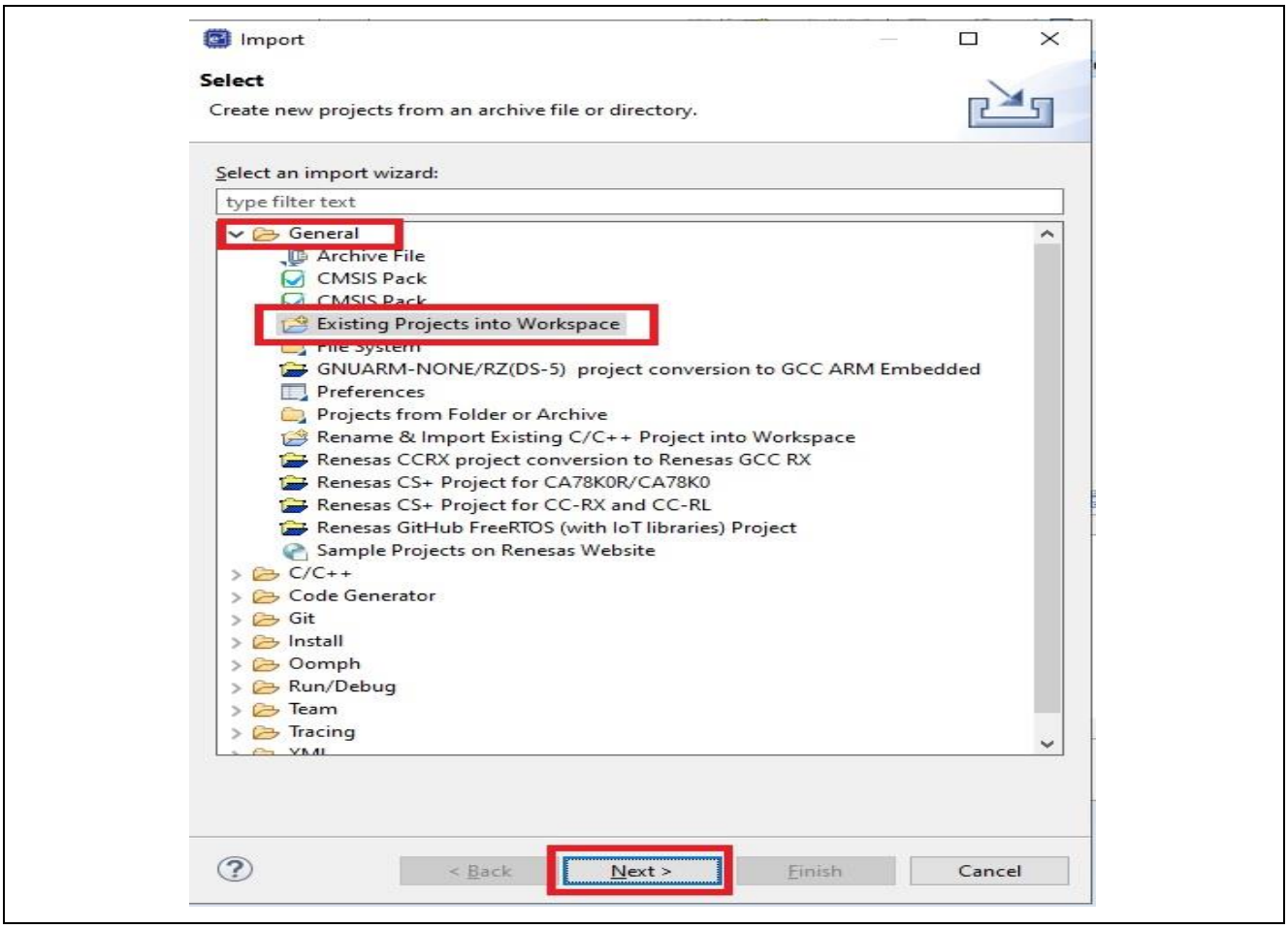


Figure 5 select Existing Projects into Workspace

5. Click Browse…, then specify the root directory as follows.

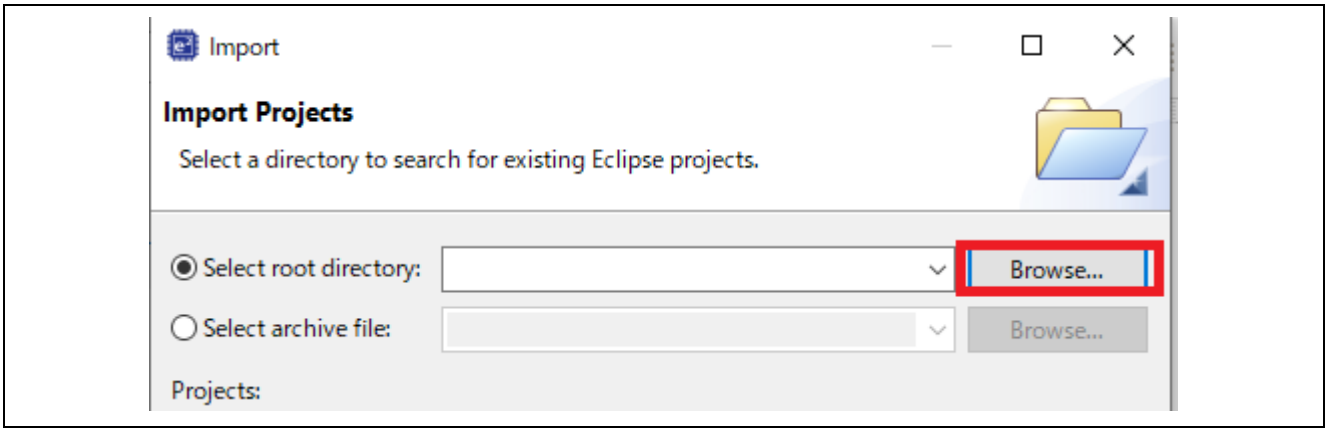


Figure 6 find the project

And you can choose two types of connectivity and compiler when import the project.
Please go to **" [Project Root folder]\projects\renesas\"** folder

Detail of each project

Project Name	Compiler	Connectivity
rx65n-new-ck in the “source-rx-eth” zip	CC-RX	Ether
rx65n-new-ck-cellular in the “source-rx-cell” zip		Cellular
rx65n-new-ck-gcc (**Planning**)	GCC	Ether
rx65n-new-ck-cellular-gcc (**Planning**)		Cellular

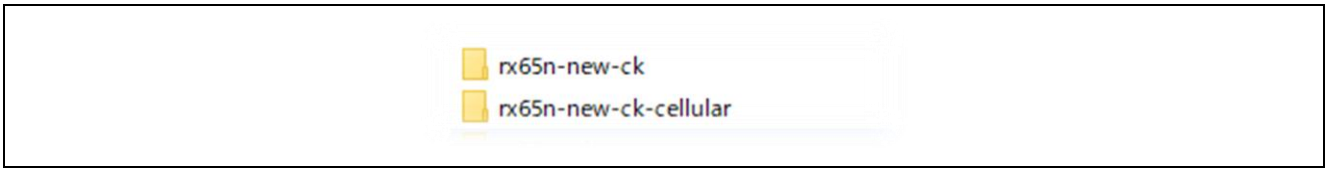


Figure 7 Project files

This case, it explains when selecting “**rx65n-new-ck-cellular**” of cellular project.
Open the **“ [Project Root folder]\projects\renesas\rx65n-new-ck-cellular\e2studio\aws_demos” folder**
If you use other one, please open **“\aws_demos”** folder of your selecting project.

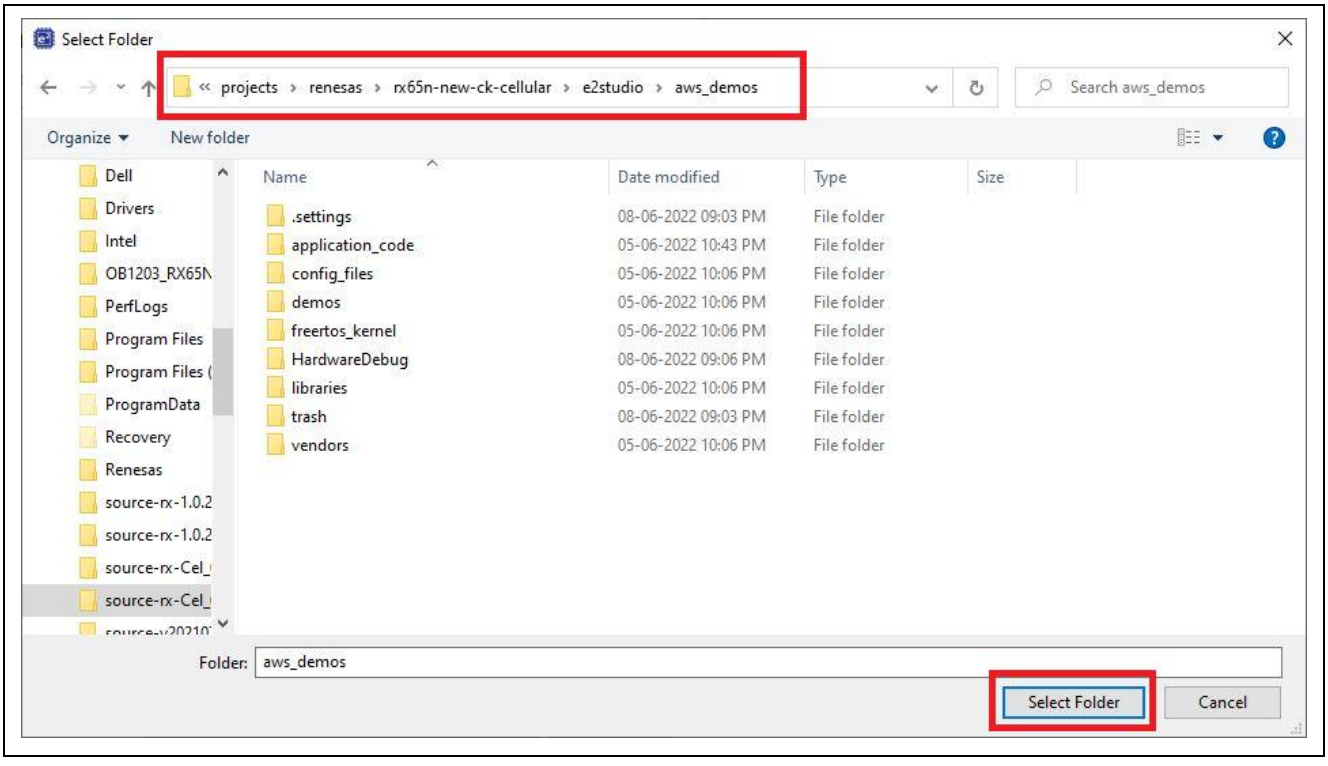


Figure 8 select the project folder

Finally, click Finish. (Note: Make sure Copy projects into workspace is unchecked.)

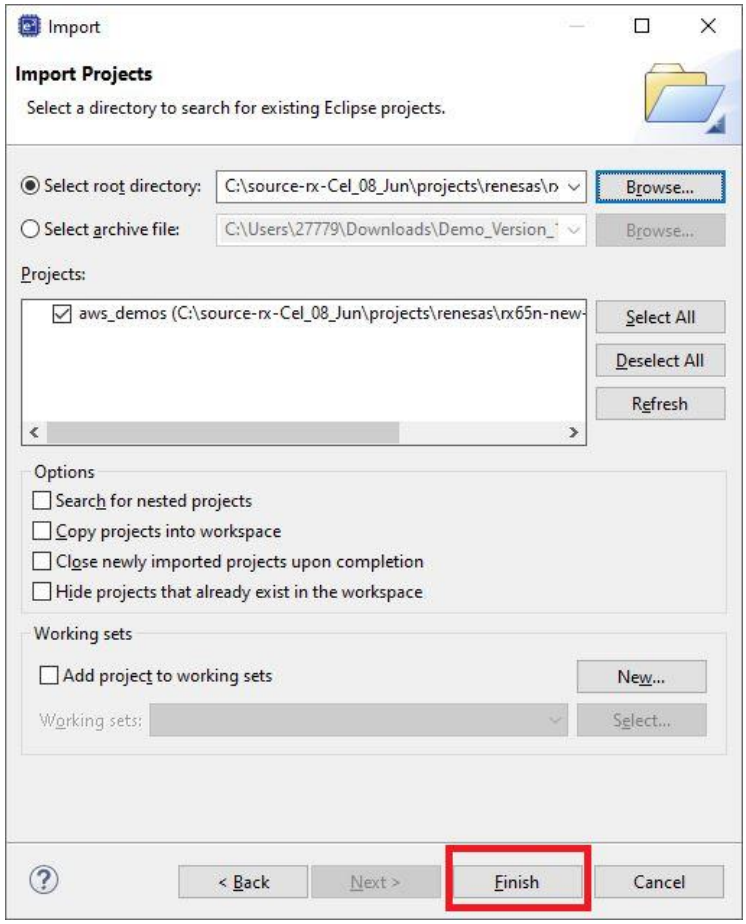


Figure 9 Finish the import the project

6.Check and set the SIM card information

Doble click the “aws_demos.scfg” to open the smart configurator.

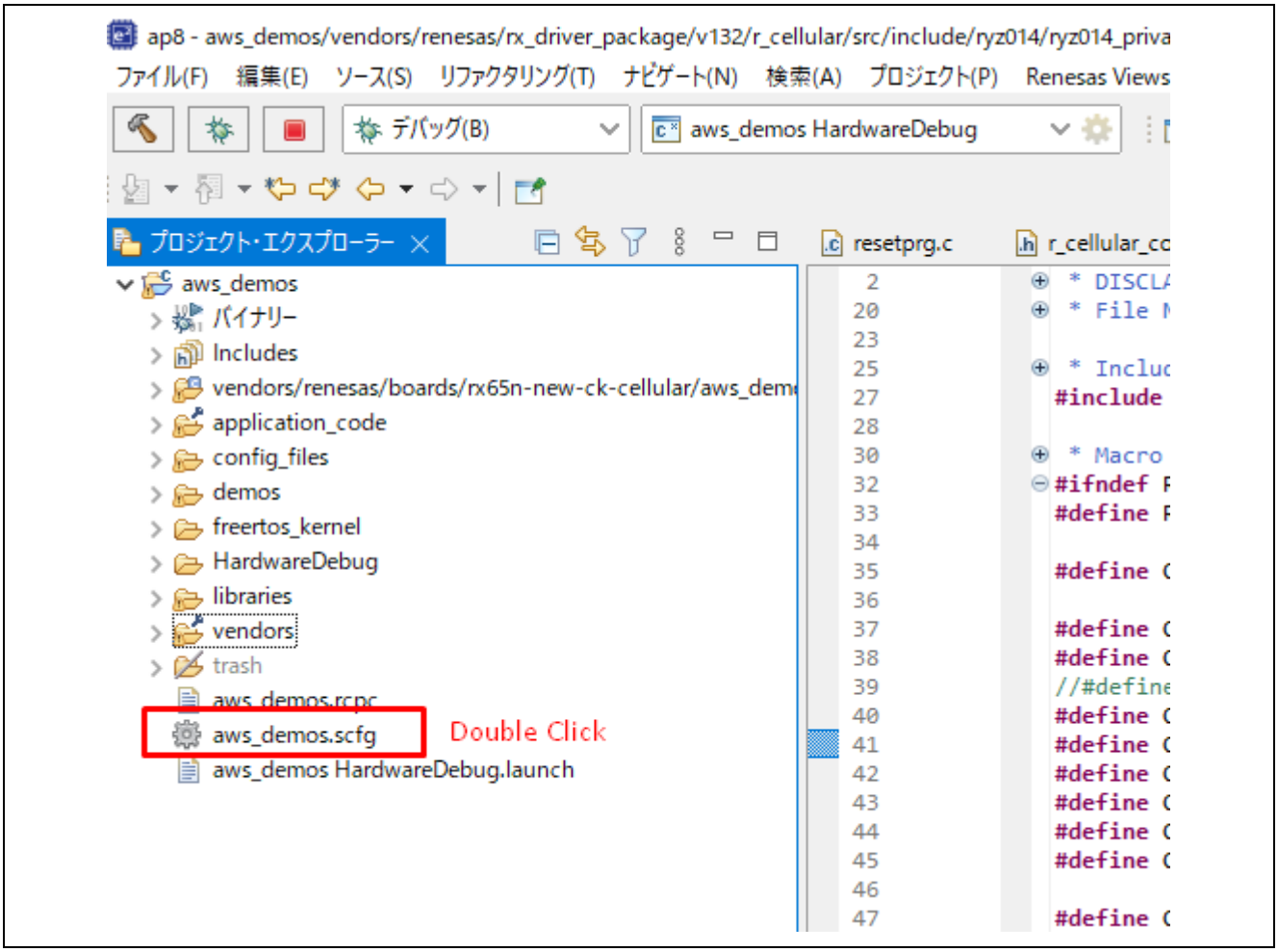


Figure 10 Open the Smart Configurator

Information for setting SIM of Cellular driver when using contained SIM card in the kit

Items	Truphone	MicroAi Launchpad
APN(Access point name)	iot.truphone.com	globaldata.iot
UserID(Access point login ID)	- (Null)	- (Null)
Password(Access point password)	- (Null)	- (Null)
SIM card PIN cord	- (Null)	- (Null)
Authentication protocol type	1 (PAP)	1 (PAP)

Note: One of two SIM cards is included in this kit. Please use the configuration of the included SIM card.

Set the above configuration values when using the SIM contained the kits.

If you have different SIM card and use it, please set the value SIM provider provided.

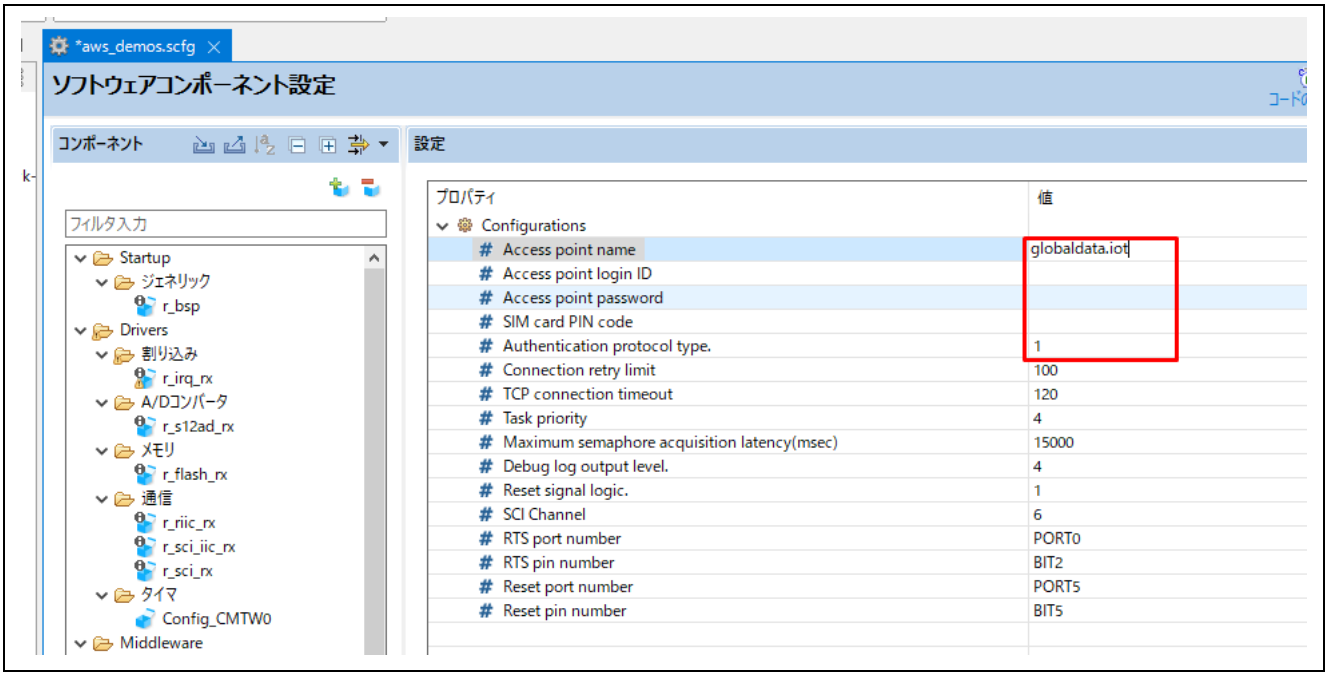


Figure 11 Set the SIM information when using contained SIM card in the kit

7. Execute code generation

If you have changed the Smart Configurator settings, click Generate Code.

Figure 12 Generate Code

8. Apply Patch files
This project must be patched after code generation. When running code generation, the source code will be overwritten by code generator. For this reason, please apply the patch each time after running code generation.
Refer to “[Project Root folder]\readme-path-memo.txt” for how to apply the patch.
The patch sources are located in “[Project Root folder]\sorce_patch” folder.

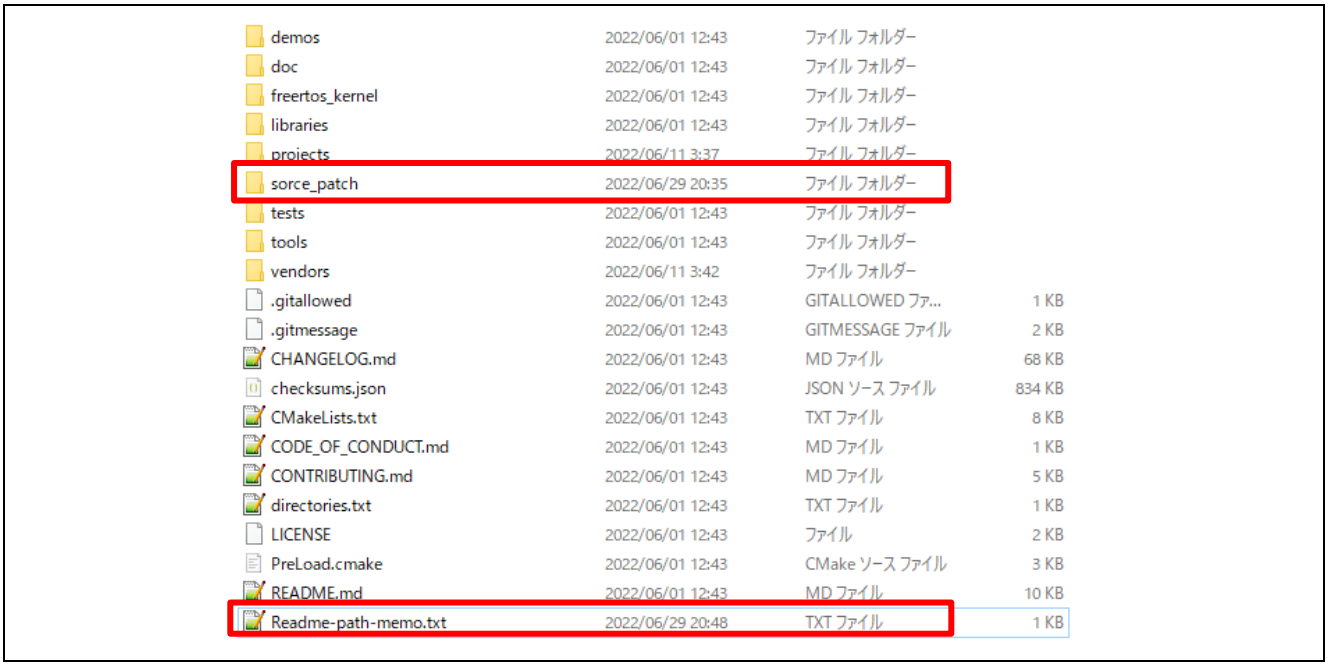


Figure 13 readme-path-memo.txt and sorce_patch folder

9. Select Project → Build All and confirm that 0 errors are reported.

Note: Make sure to clean the project before building it for the first time. If a demo build error occurs after the initial build, clean the project again and then build it.

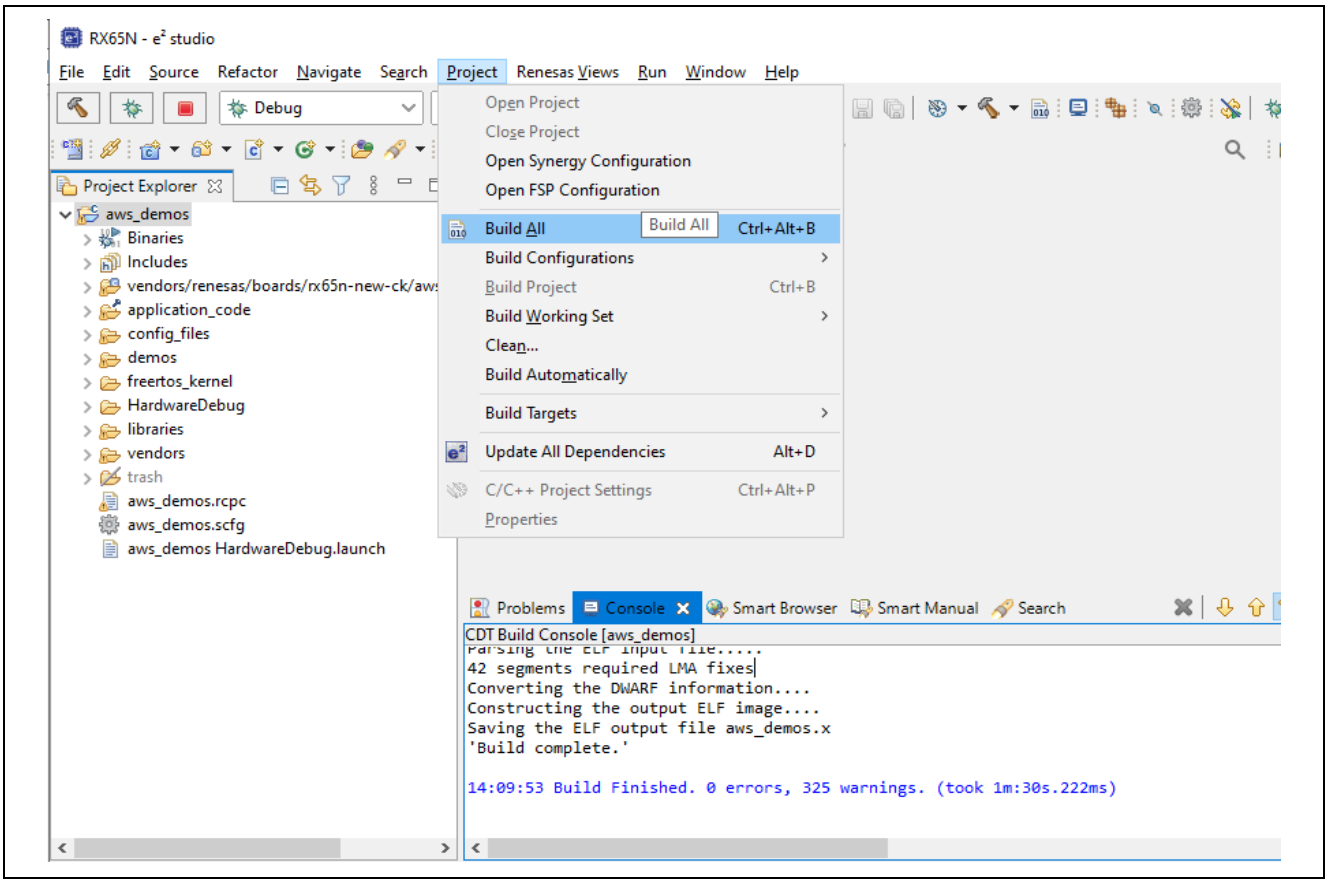


Figure 14 Build the project

10.Debug Configuration

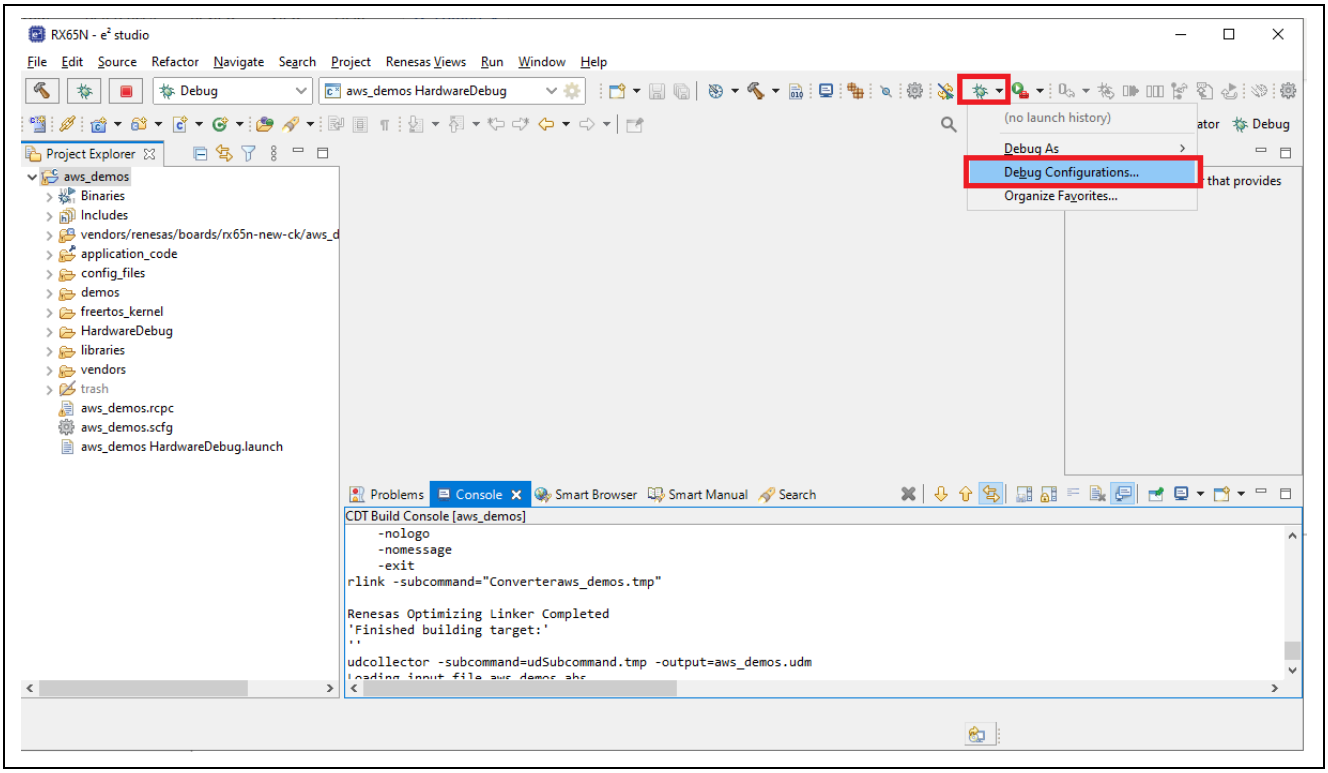


Figure 15 Configuration debugger 1/2

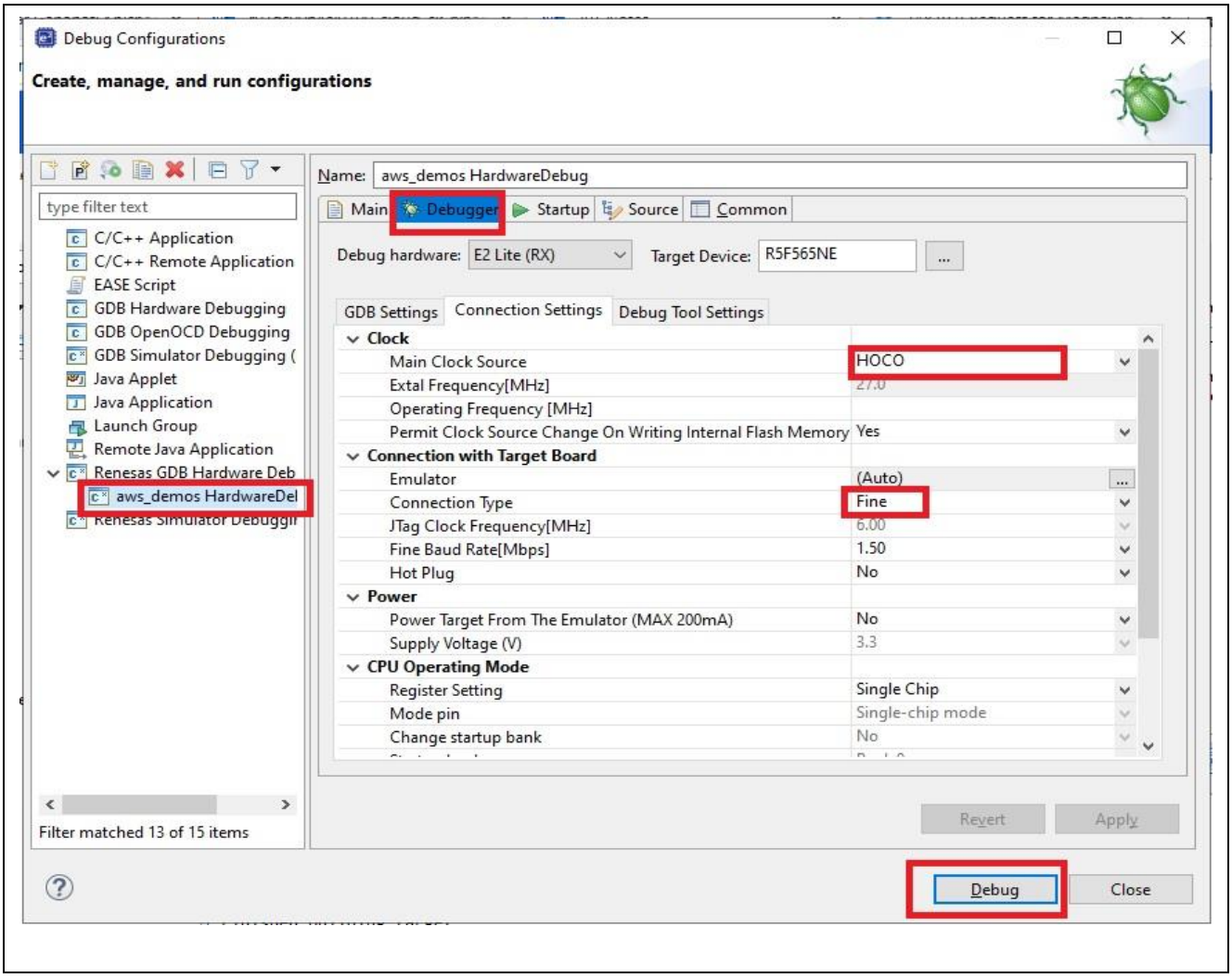


Figure 16 Configuration debugger 2/2

4.1.2 Data Publishing Interval Settings (Optional)

Data publish interval can be set by the user. Default publishes interval time 10 Sec

“mqtt_demo_mutual_auth.c” file has the macro to change the publish time interval.

```
#define DATA_PUBLISH_INTERVAL_IN_SEC 10U
```

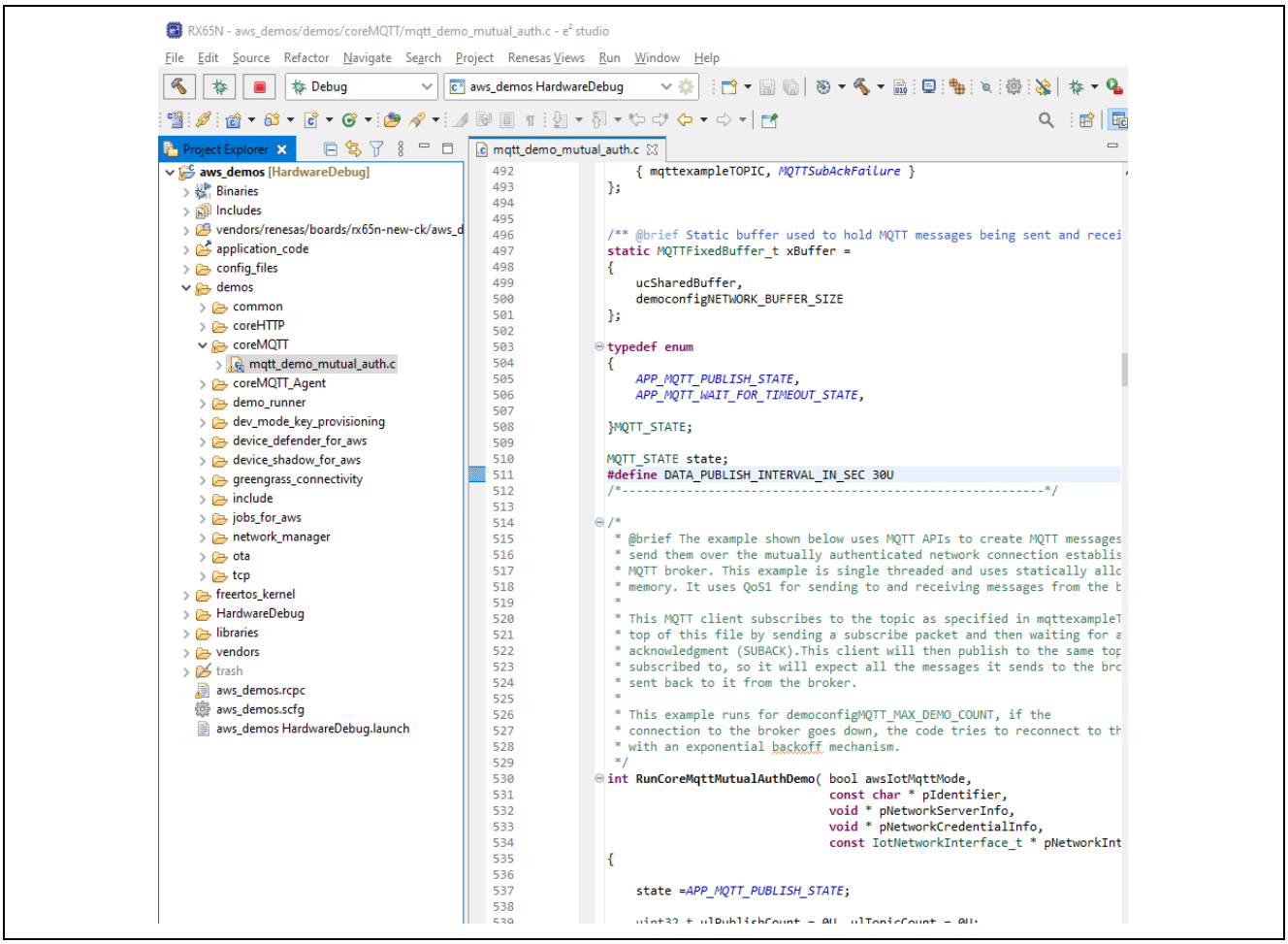


Figure 17 Data Publishing Interval Settings(Optional)

4.1.3 Running the Application Project

To run the Application project, use the following instructions to setup the board.

4.1.3.1 Connecting the Board to the Serial port Console of the PC

1. On the host PC, open Windows Device Manager. Expand **Ports (COM & LPT)**, locate **USB Serial Device (COMxx)** and note down the COM port number for reference in the next step.

   Note: USB Serial Device drivers are required to communicate between the CK-RX65N board and the

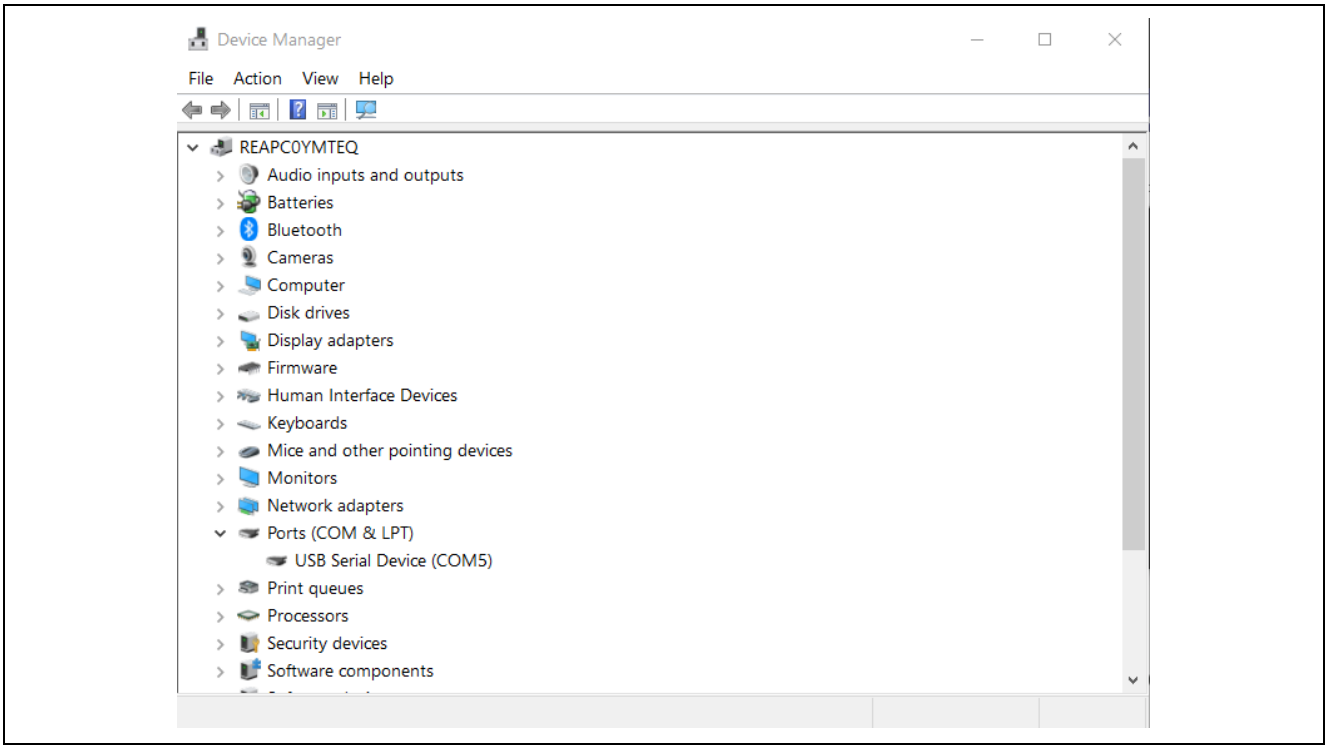


Figure 18. USB Serial Device in Windows Device Manager

2. Open Tera Term select **New connection** and select **Serial** and **COMxx: USB Serial Device (COMxx)** and click **OK**.

Figure 19. Selecting the Serial Port on Tera Term

3. Using the **Setup** menu, select Setup -> **Terminal…** and select “AUTO” as Reveive and “enable” local echo, as shown below.

Setup->Terminal

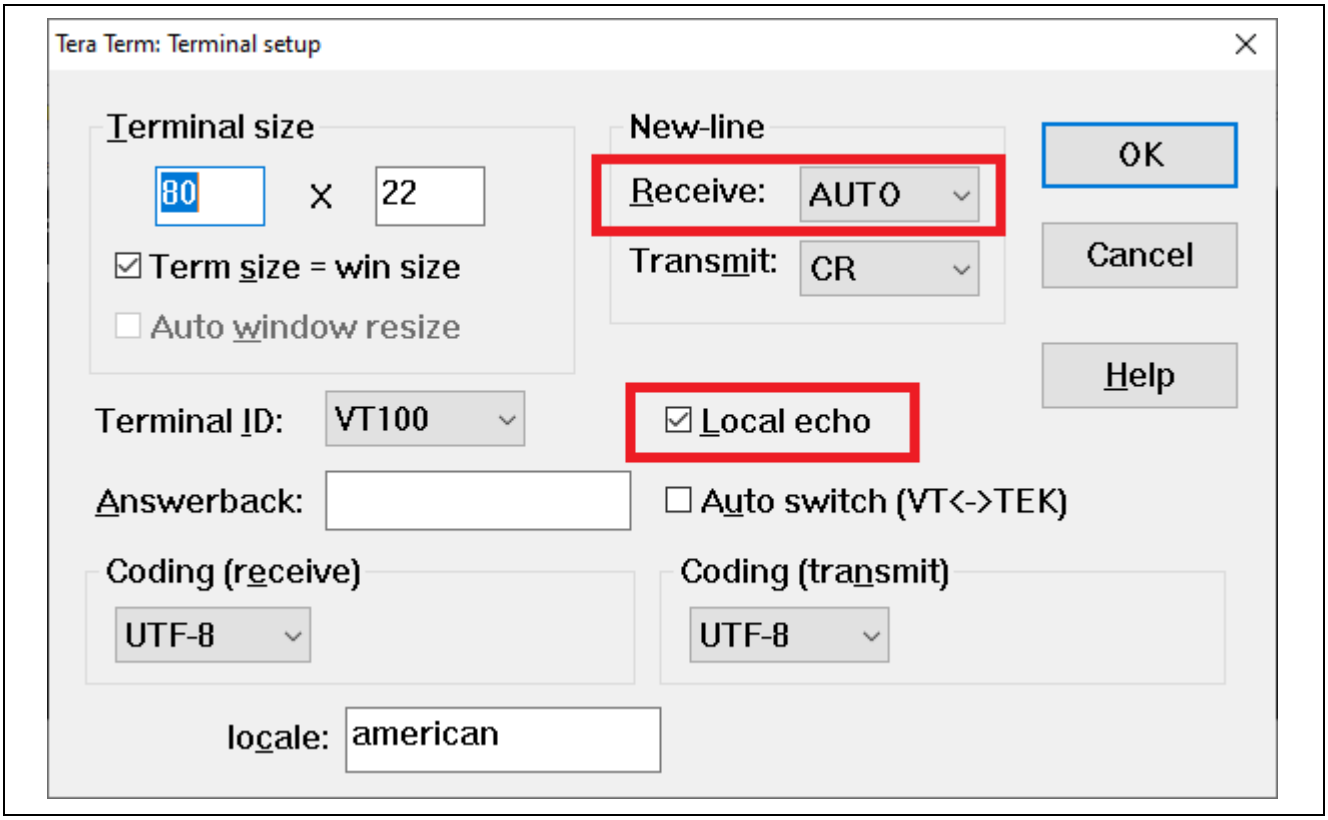


Figure 20. Select Receive: ”Auto” and enable “Local echo” on the Terminal setting

4. Using the **Setup** menu pull-down, select **Serial port…** and ensure that the speed is set to 115200, as shown below.

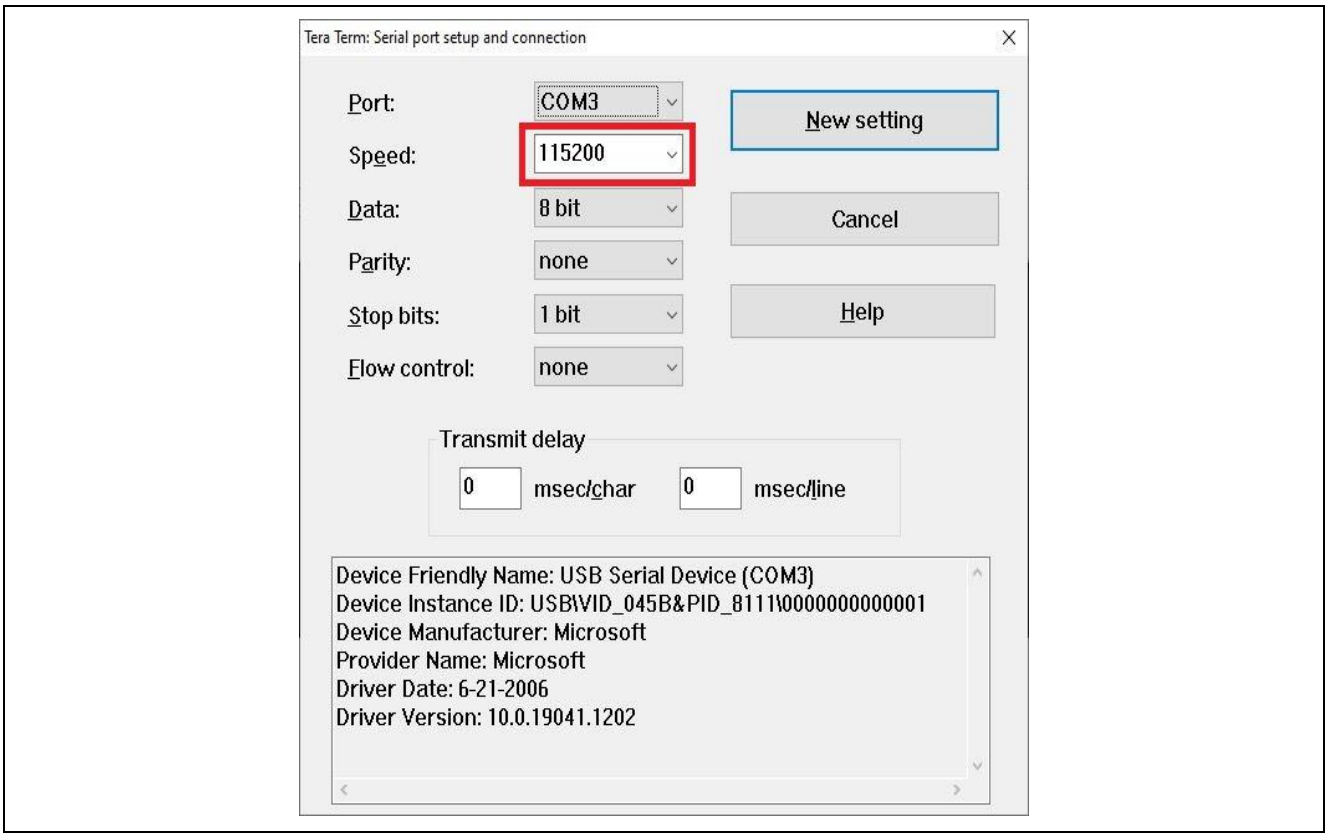


Figure 21. Select 115200 on the Speed Pulldown

5. Complete the connection. The ‘Configuration CLI Menu will be displayed on the console as shown below.

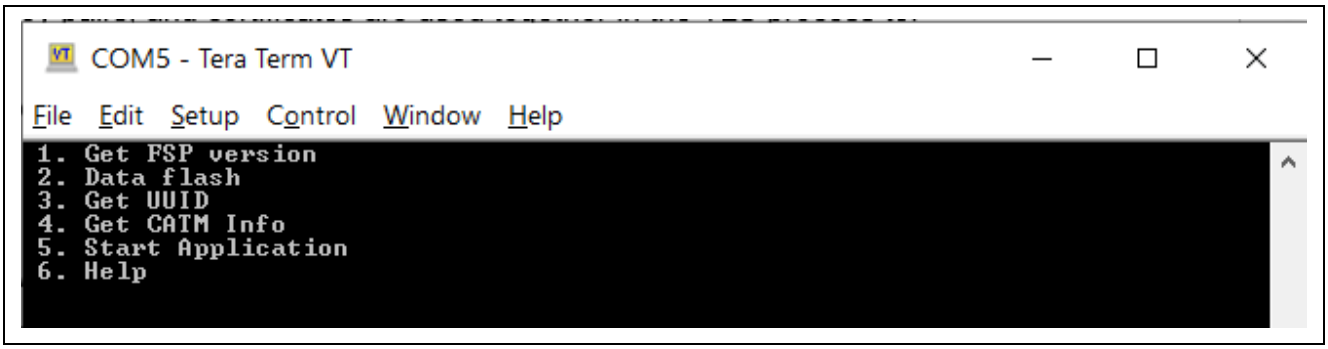


Figure 22. Main Menu

6. In the CLI shown in the above snapshots, choose the number to select the commands. For E.g. When you press '**1**' Firmware Version of the application is displayed as shown below. To return to the main menu press "space bar" key.

Figure 23. Get Version Information

4.1.4 Running the application & activation of SIM card contain with CK-RX65N

This section explains how to activate SIM card that is contained in CK-RX65N.If you use ether, you can skip this step.

1. Press '**4'** to display **CAT-M Information (IMEI &ICCID)**. This menu will communicate with the CAT-M module to obtain the IMEI and ICCID values needed for activating the SIM card. Upon success, the IMEI and ICCID values will be displayed on the terminal screen. The program will continue to attempt to communicate with the CAT-M module until it has successfully connected or timed out. The IMEI and ICCID values are used to activate the SIM card.

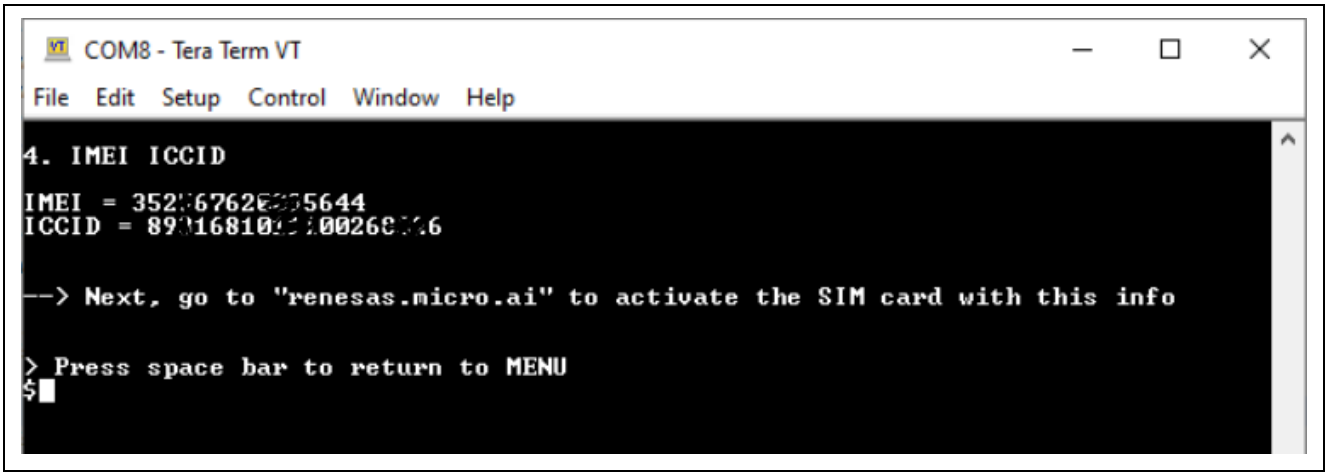


Figure 24. CAT-M Information

4.1.5 Activating SIM card

One of two SIM cards is included in this kit that is Truphone or MicroAI Launchpad.
Please activate the SIM card as following steps depending on the included SIM card.

4.1.5.1 Activate on Truphone

To activate the included Truphone SIM card, please visit the Truphone SIM Activation platform at truphone.com/connectit and use the following steps:

1. On the Business page, click **Start activation** button under **IoT SIM Activation.**

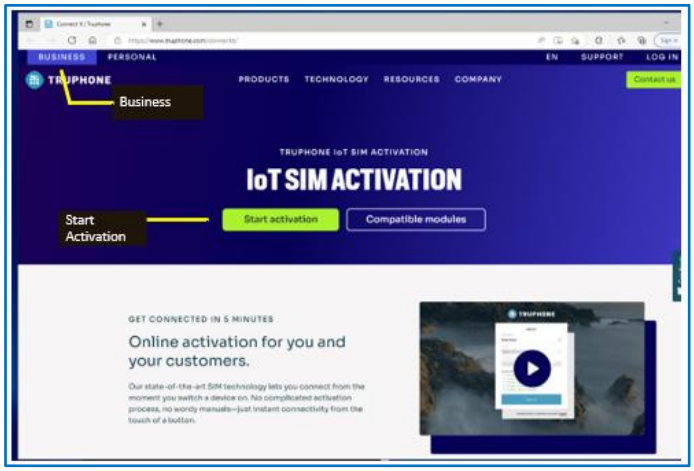


Figure 25. Activating the SIM Card on Truphone

2. Create a new Truphone Account by selecting **Sign up** (next to **Don't have an account yet?**) and fill-in your full name, Email, and a password. Then click **Sign up** to create a new account.

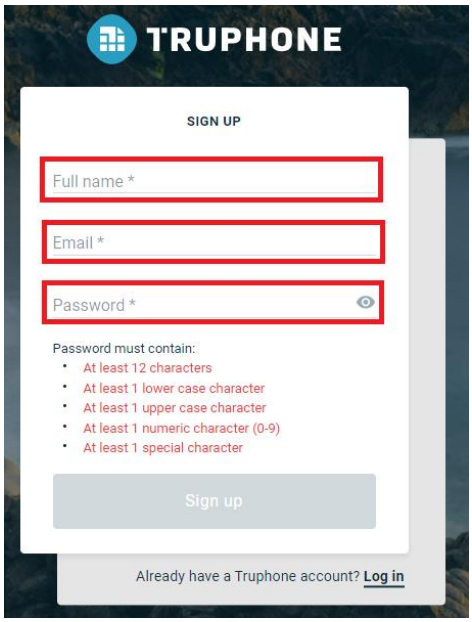


Figure 26. Signing in

3. Select **Personal** as the account type and press **Get Started**.

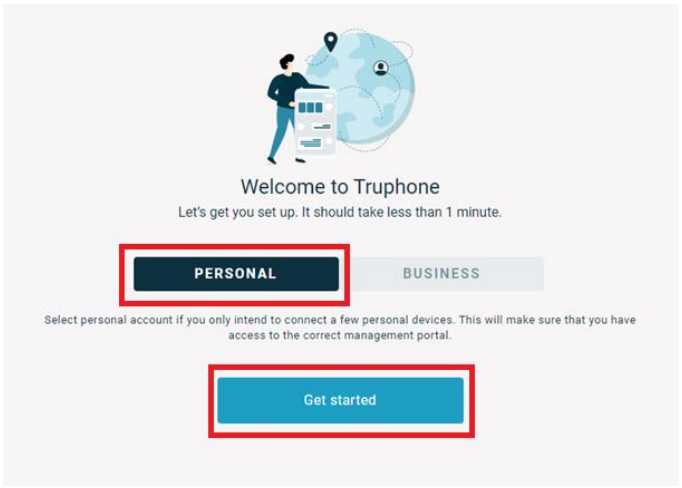


Figure 27. Selecting the account type

4. Verify your email by entering the activation code sent to your email account.

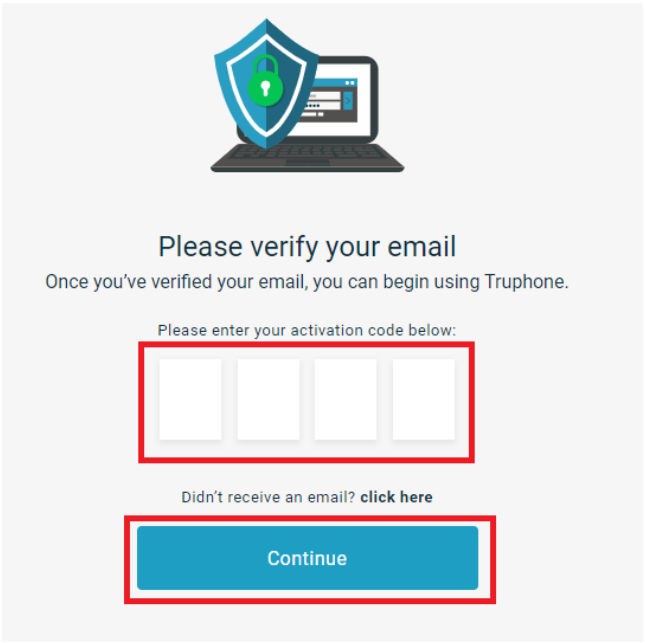


Figure 28. Verifying the email

5. Complete the **Profile information** form – then select **Create account**.

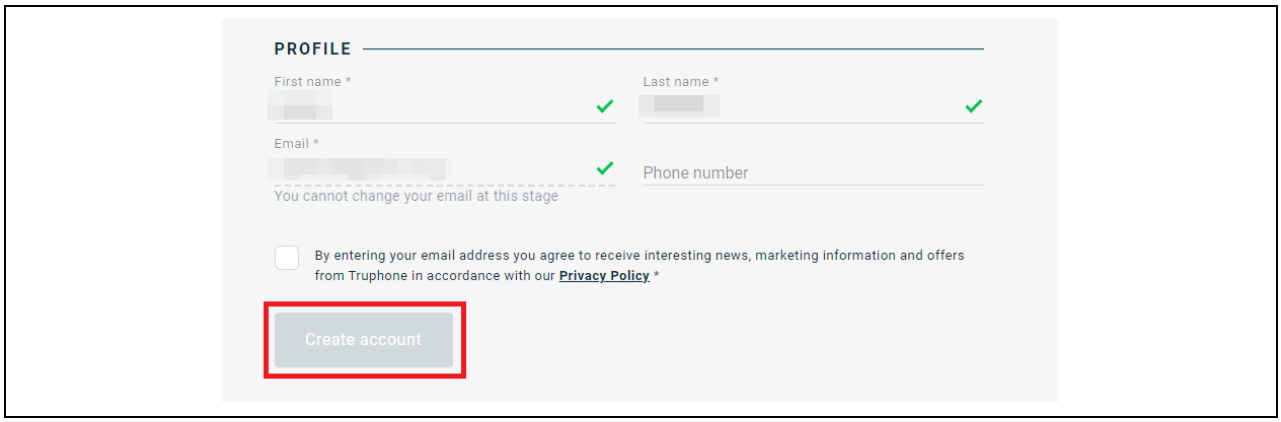


Figure 29. Completing the Profile information

6. Select **Activate SIMS** to activate your individual SIM by **ICCID**.

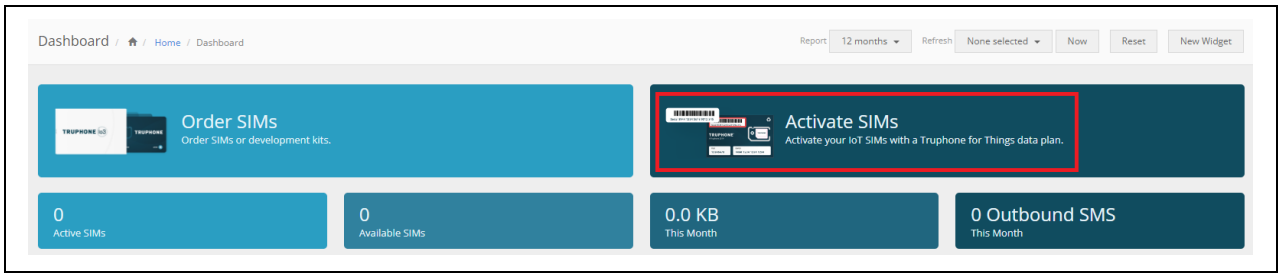


Figure 30. Activating SIM

7. Enter the **ICCID** value.

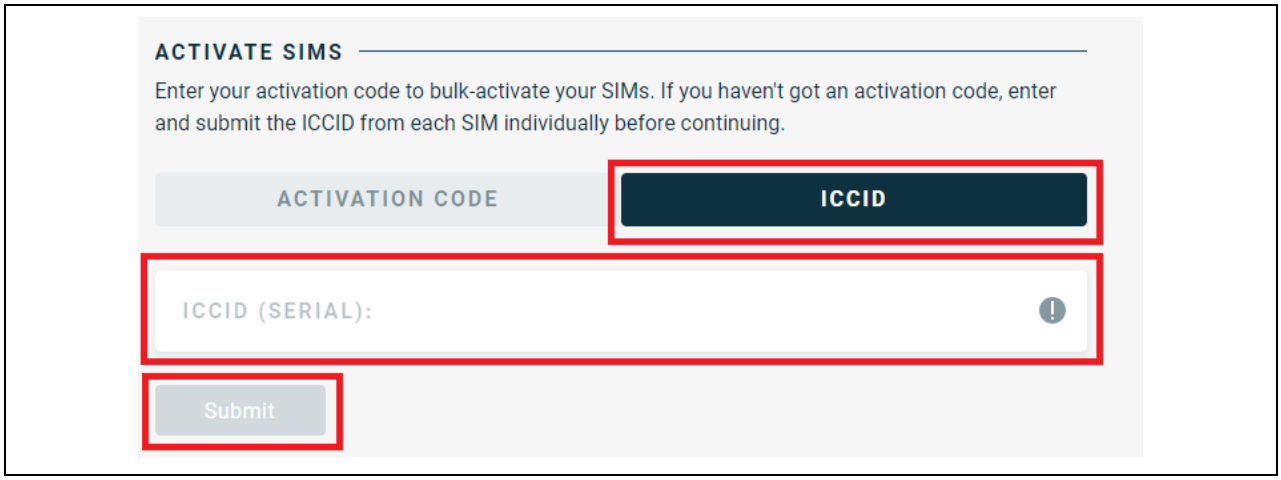


Figure 31. Entering the ICCID

8. You will receive email confirmation when the SIM card activation is complete.
   The **CK-RX65N** kit and SIM card should be activated and can be validated on the Tera Term terminal.

Note: The SIM card includes free credit for the first 90 days/50MB.
After expiring the free data charge, Communication charges will be incurred.

Disclaimer

The activation steps above are provided by SIM Provider Truphone. They are the most current at the time of publishing this application note. If you need help activating your SIM card, contact Truphone support iot.truphone.com or Contact Support | Truphone.

If you have a SIM card from any other provider then contact the technical support for that provider.

For any other issue that cannot be resolved please contact Renesas Support at Technical Support.

Note: The SIM card provider for the Quick Start Guide example project is Truphone. If you use any other SIM card provider you must change the Access Point Name required for the SIM card provider in your global region. Failure to do so could result in the RYZ014A not connecting to the cellular network.

4.1.5.2 Activate a SIM card on MicroAI Launchpad

The MicroAI Launchpad platform will be needed for the activation of the SIM card. To activate the SIM card, use the following steps:

1. Create a Launchpad account. Do so by registering on the sign-up page and verifying the account through the verification email sent after registration.
2. Login to the new Launchpad account and click on the **Create Device Profile** tile. Make sure **Renesas CK-RX65N**(or Renesas RSK-RX65N when missing CK-RX65N) is selected for the Device Type and **CAT-M** for the Connectivity Type. Fill other fields as desired then click Next.

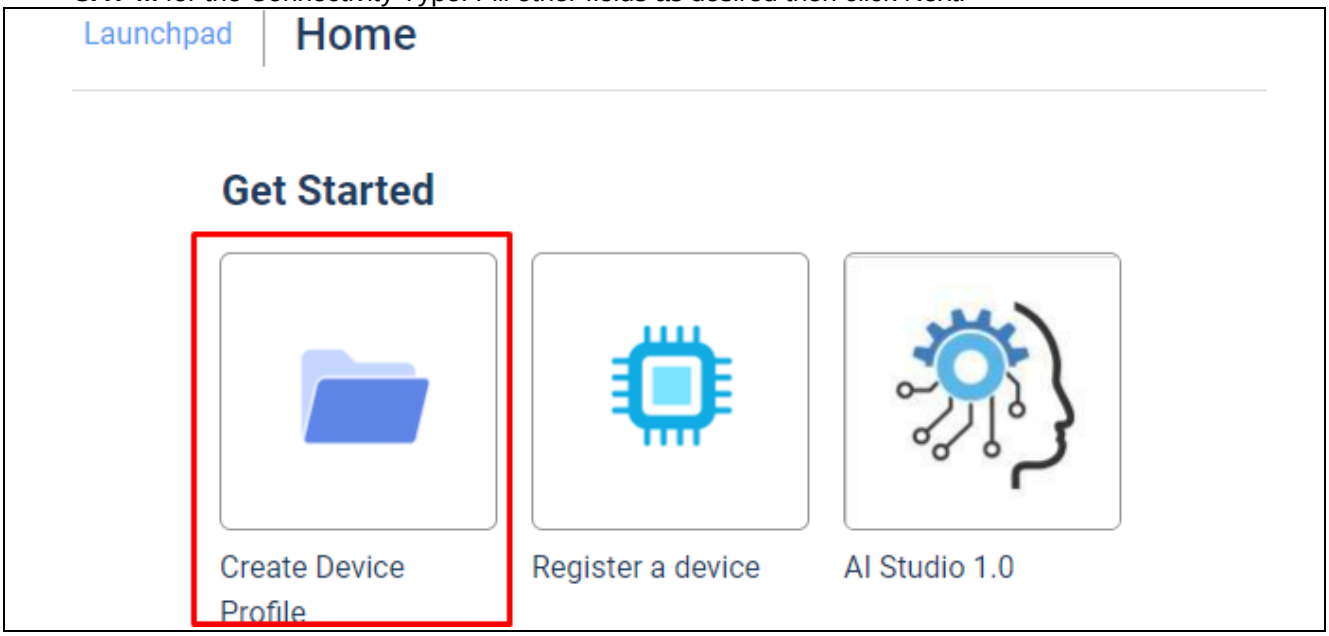


Figure 32. Create Device Profile on MicroAI Launchpad

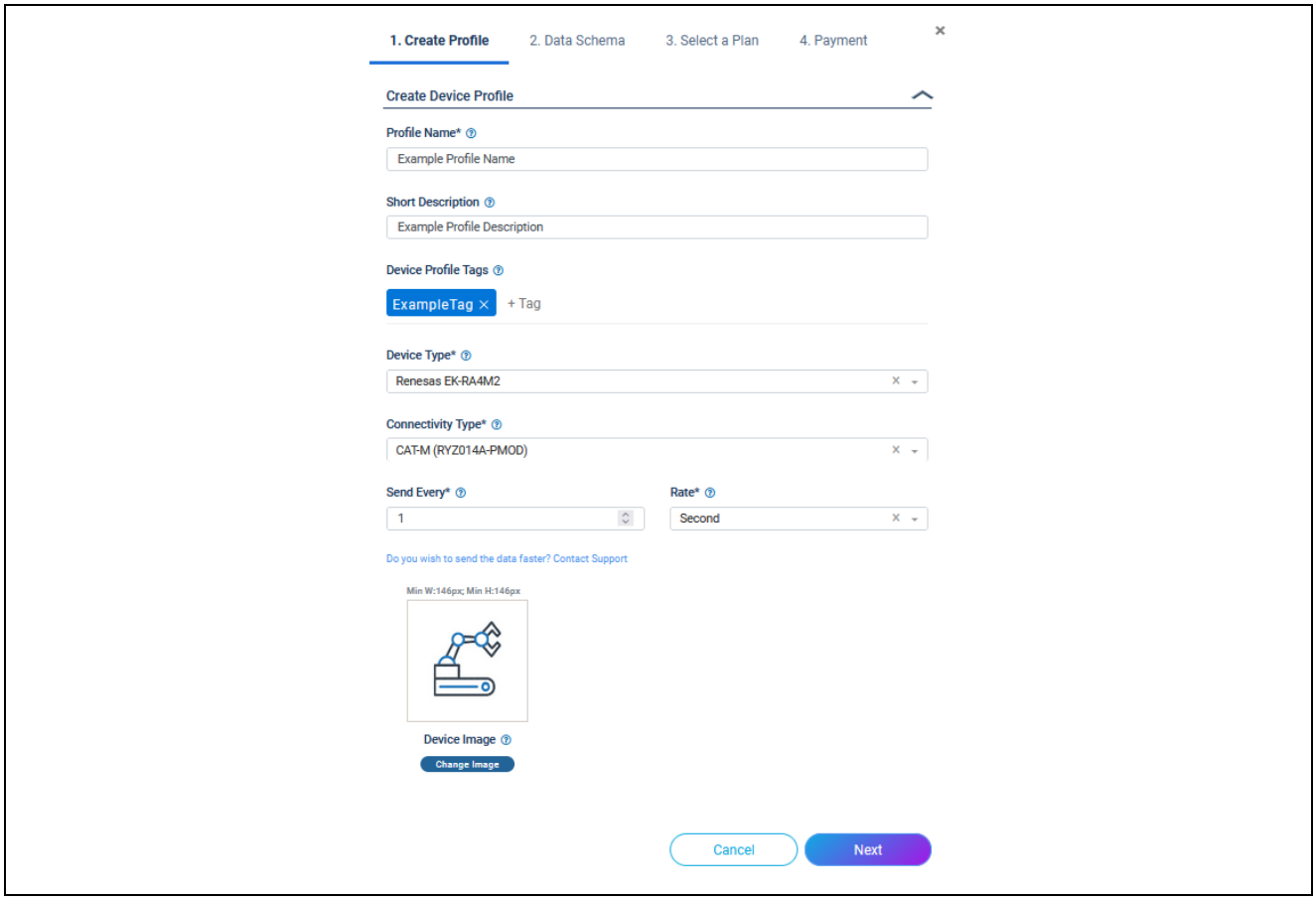


Figure 33. Input the information of Profile

3. On Data Schema, click Next.

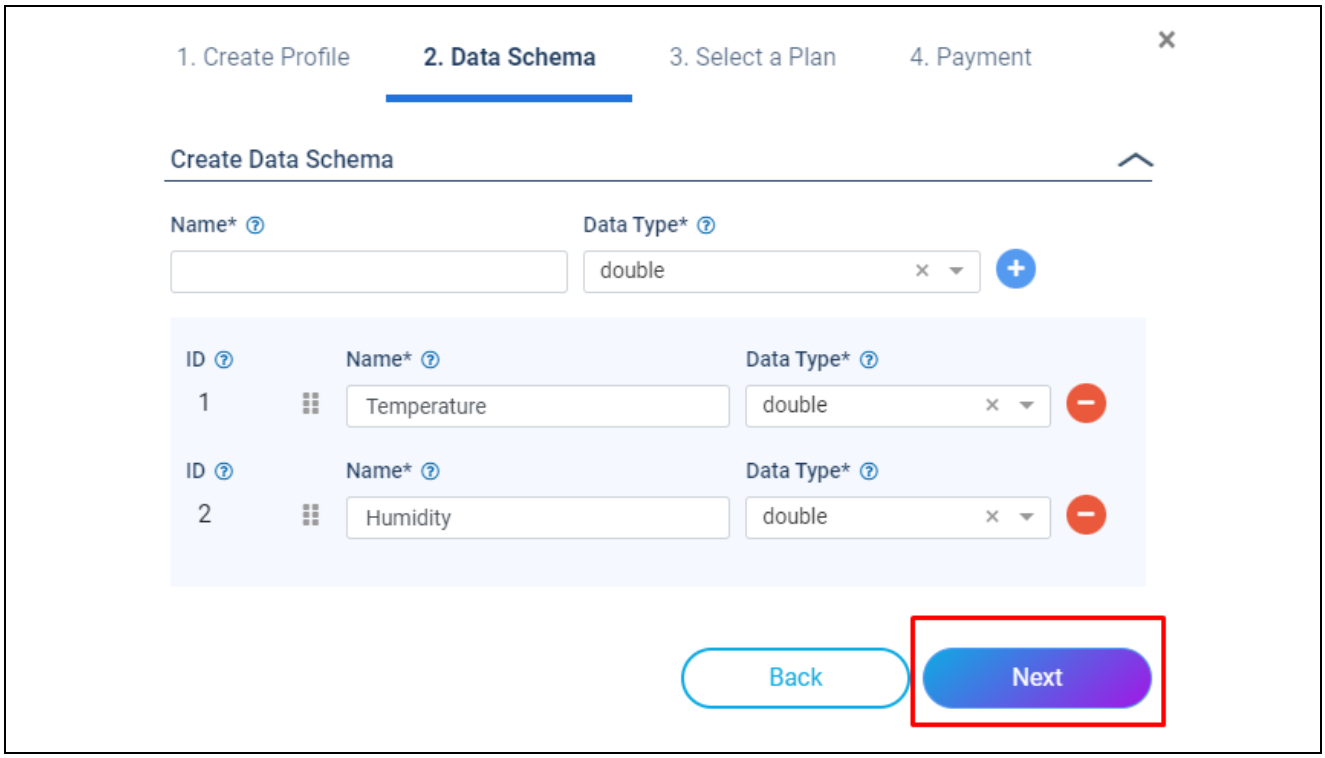


Figure 34. Data schema

4. On Select a Plan, apply any valid promo codes if applicable and click Next.

Note: The SIM card includes free credit for the first 1 month/50MB. You can see credited information in invoice center on your account.
After expiring the free data charge, Communication charges will be incurred.
If you need that it doesn't need to use this SIM card with payment, please set the device status to "suspended" to stop the communication charge.

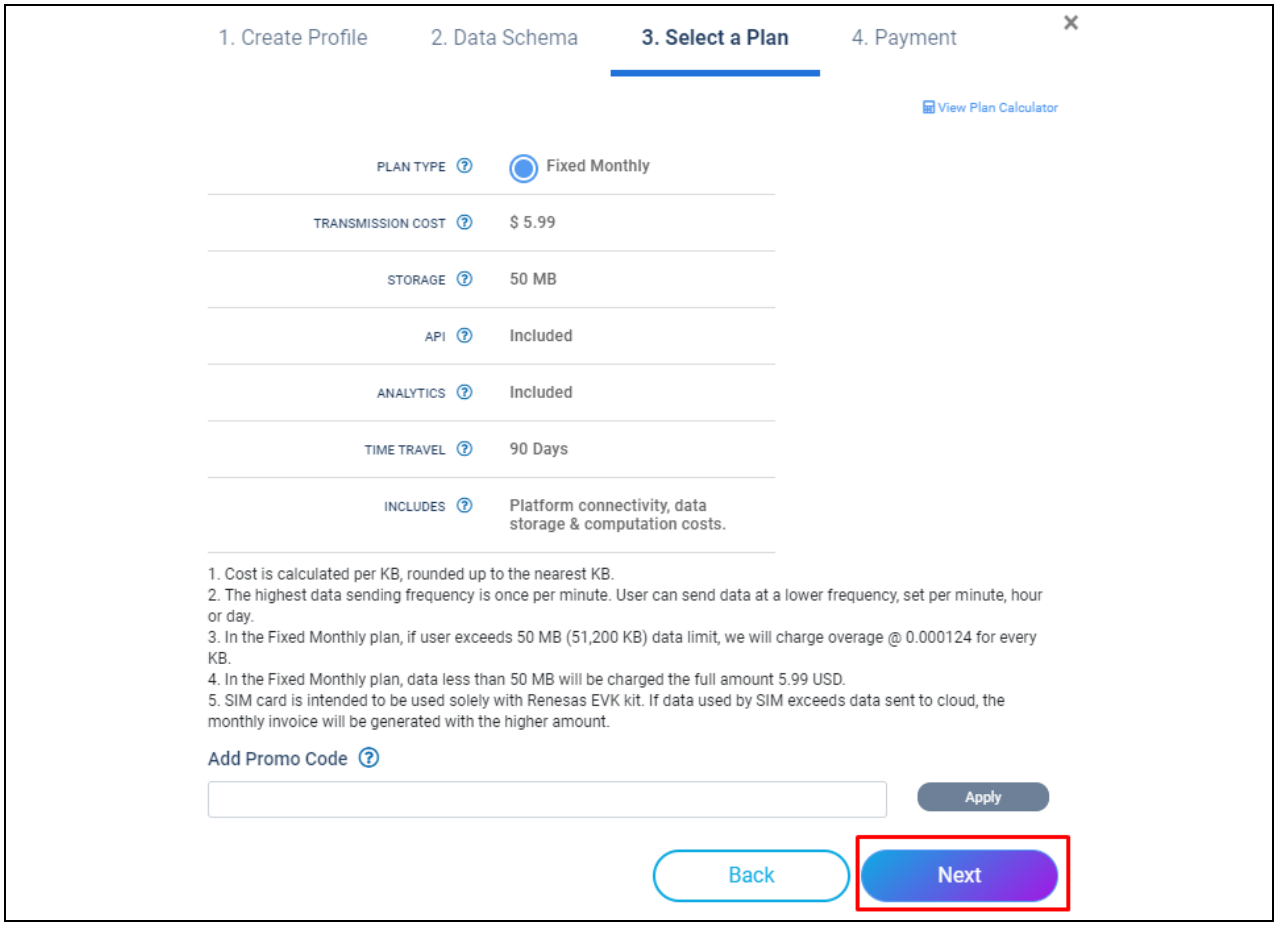


Figure 35. See the plan of SIM and trial time

5. Provide a Payment Method and accept the terms and conditions. Click Finish.

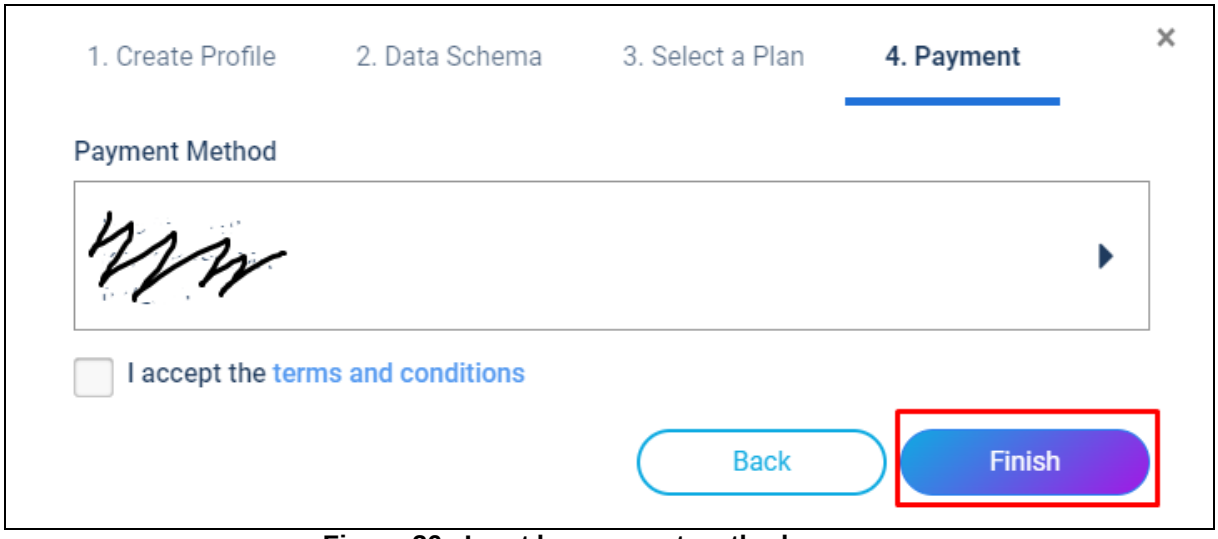


Figure 36. Input he payment method

6. Click the **Register a Device** tile to begin registering the **CK-RX65N** kit and SIM card. Select the device profile created from the device profile drop-down.

7. Select your Device Profile you created previous step.
8. Enter the **IMEI** value obtained from the CLI of section “4.1.4 Running the application & activation of SIM card contain with CK-RX65N” into the “**Device ID**”. Fill other fields as needed.

Note: Please be careful, the “Device ID” cannot change after registration of this step.

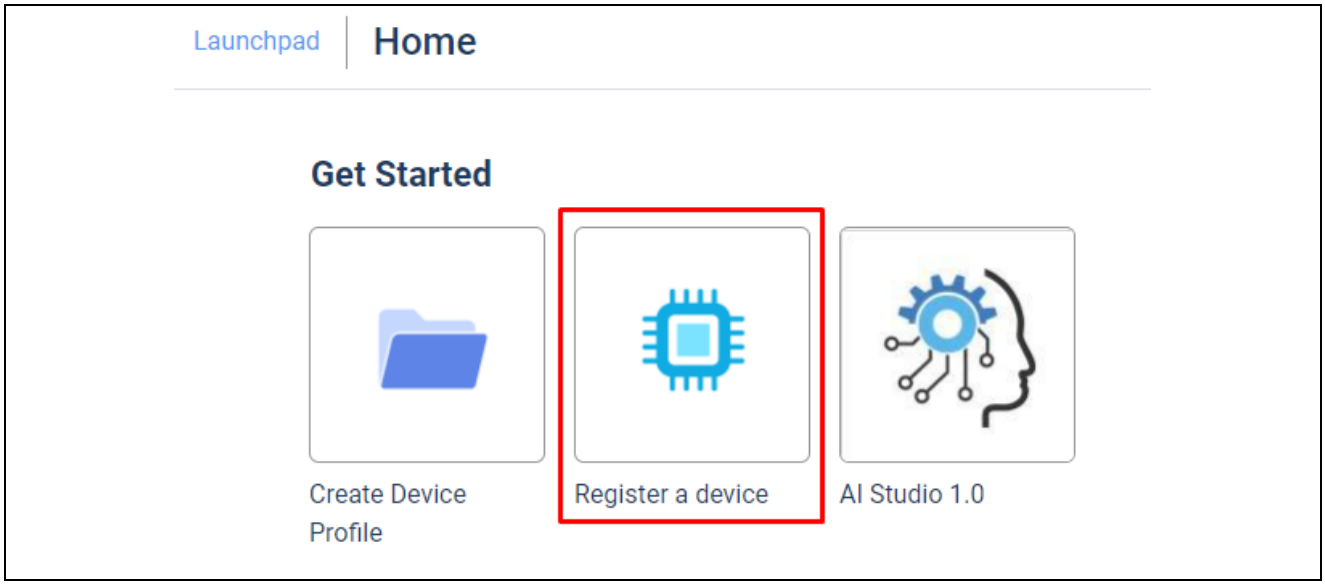


Figure 37. Registering a device of CK-RX65N on MicroAI Launchpad

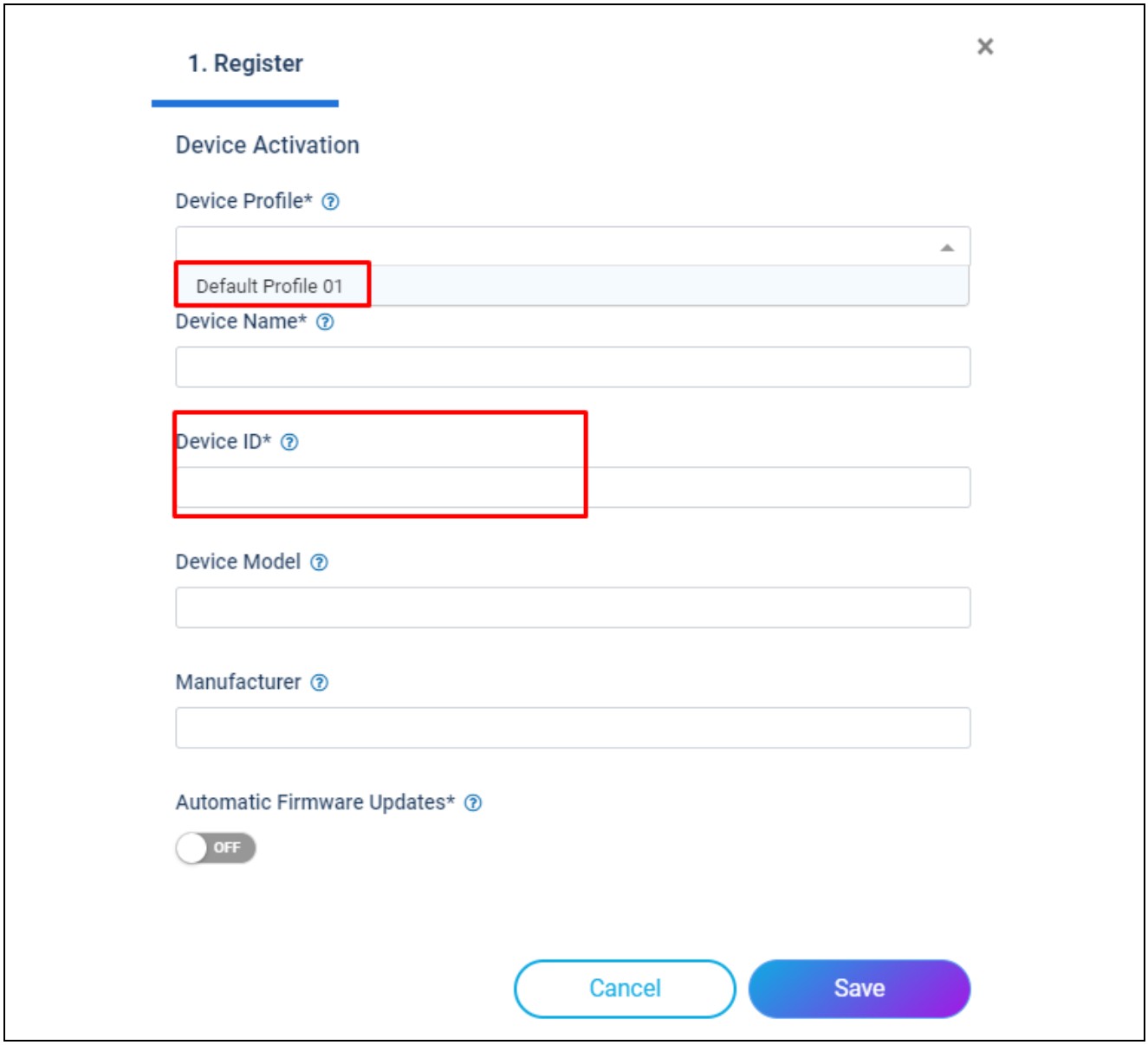


Figure 38. Enter Device ID

9. Click Next and click **Add New SIM**. Enter the **ICCID** value for the SIM EID field and click Save SIM.

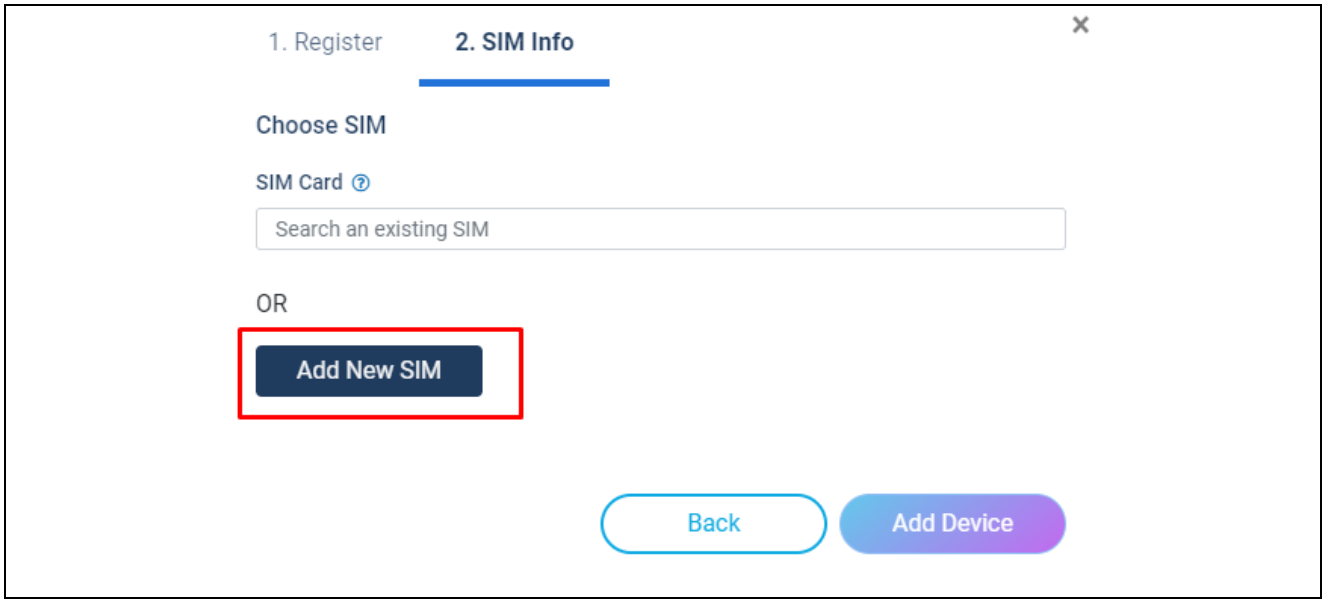


Figure 39. Add new SIM

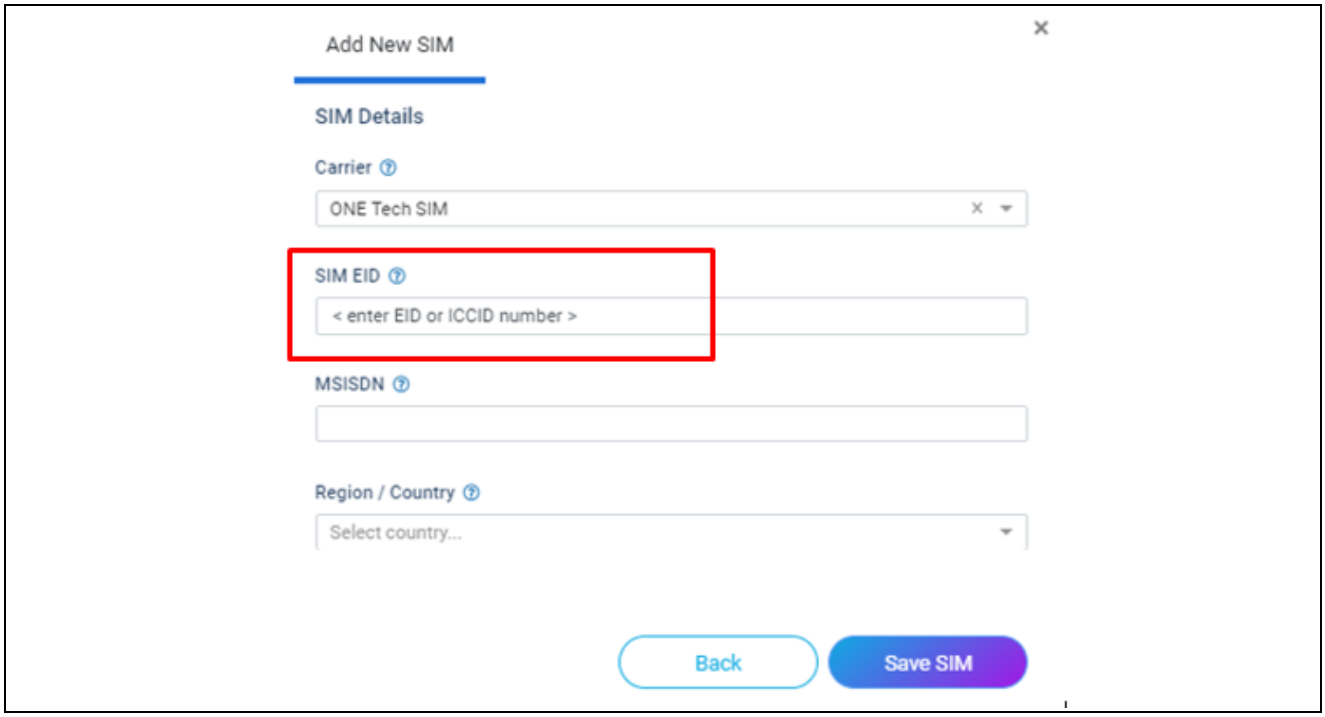


Figure 40. Activating the SIM card on MicroAI Launchpad

10. Finish the device registration. The **CK-RX65N** kit and SIM card should be activated on the Launchpad platform and can be validated on the Tera Term terminal.

4.2 For Users who use provided dashboard and AWS account of Kit

This section explains about registration account and access dashboard.

It needs to get “UUID” of the kit

4.2.1 Getting the UUID Information of the Board

1. Press '**3**' from the **Main Menu** to display **Board UUID**. This command obtains the UUID information of the board and displays on the console similar to the snapshot shown below. You will need this info for registering to the Cloud Dashboard.

Figure 41. Getting Board UUID Information

4.2.2 To get the account 10USD of trial of AWS

1. Register/sign up at "https://renesas.cloud-ra-rx.com/" with **an email account that was not used previously for signing up to an AWS account.**

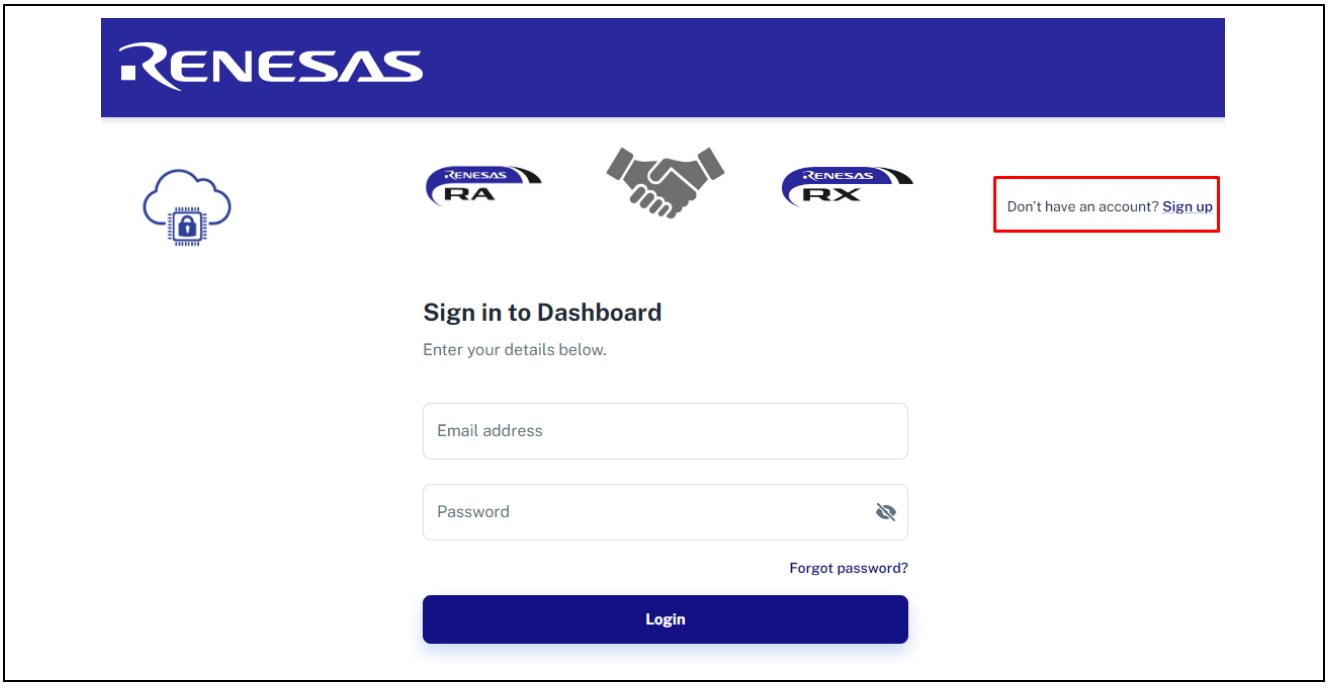


Figure 42 Get the account 10 USD of traial of AWS

1. Wait for AWS verification email (~10 min) UUID is the unique ID of your board. You can get it from **4.2.1 Getting the UUID Information of the Board** section.

2. **Verify the AWS account** in your email that you registered.
3. Wait for the status change on the registration page/ wait for provisioning to complete. May take up to **1 hour** for the device to be active. Please refresh the page in case Registration in progress screen still shows up.

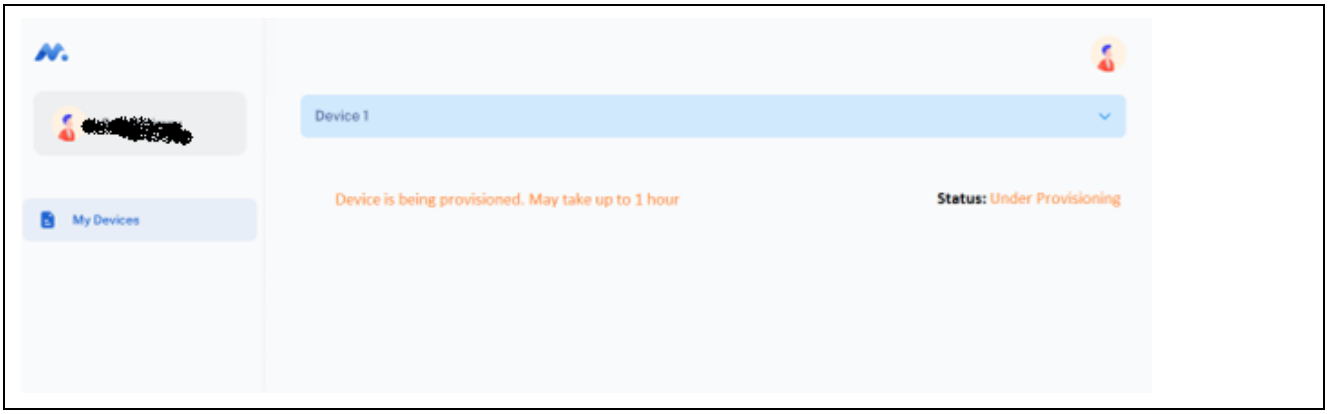


Figure 43 in progress of the building dashboard

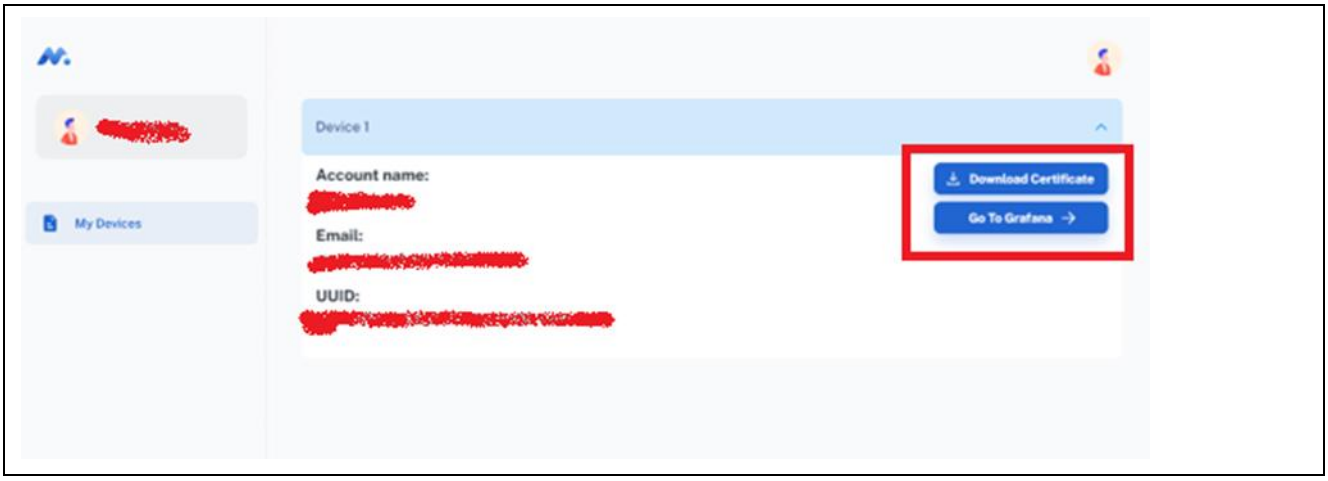


Figure 44 After finished building the dashboard

4. Once the account status shows up as active in the registration page, click on device to see device UUID.

5. After finishing the progress, you can get the file of certification to connect dashboard from “Download Certificate” button. It is used for installation on the application demo of kits that you got previous step.

6. Click to “go to Dashboard” to access the dashboard. First time users will access the dashboard with credentials **“admin” for both username and password** and will be directed to change the password. Once completed, users can access the dashboard.

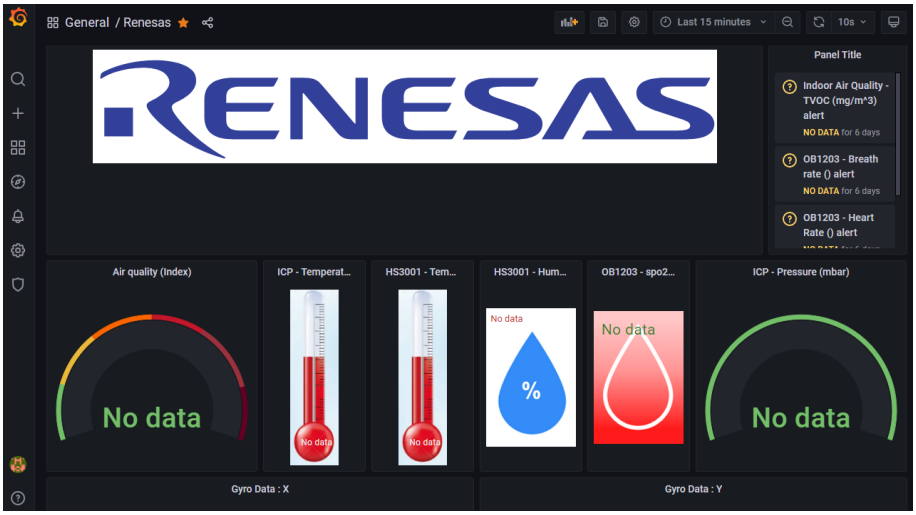


Figure 45 Dashboard for this application

Next step please see from **4.3 Hardware Preparation** section

4.3 Hardware Preparation

- ✓ Connect micro-USB cables to debug port (J14 on the CK-RX65N board)
- ✓ Connect micro-USB cables to serial port (J20 on the CK-RX65N board)
- ✓ Connect the RYZ014A Cellular PMOD module to the **PMOD1**
- ✓ **Set the Jupmer of J16 "Debug"**
- ✓ Connect RYZ014A Cellular PMOD module and insert sim card

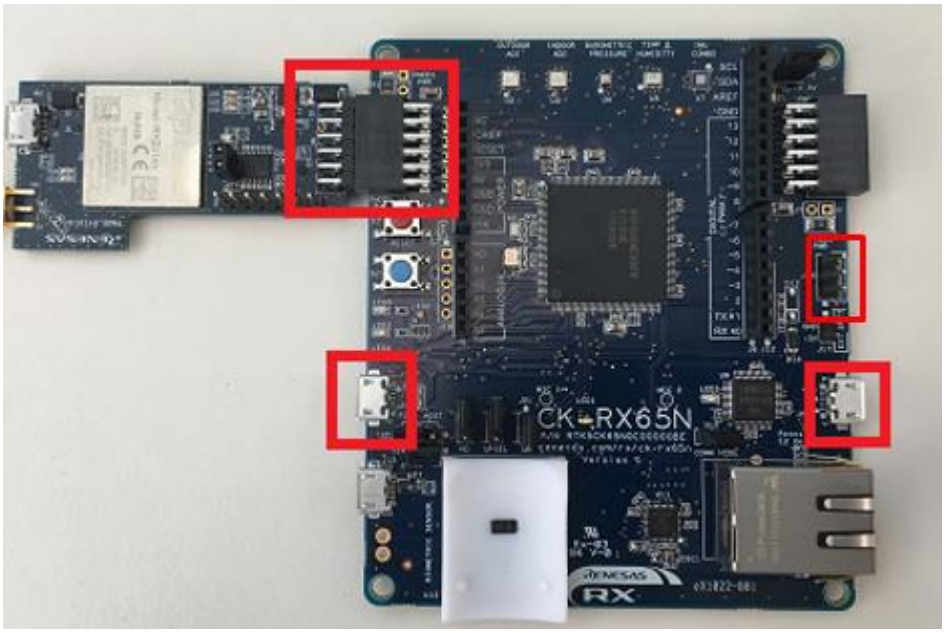


Figure 46 Connecting the USB and RYZ014A Pmod

4.4 Software Preparation-Run Project from IDE

4.4.1 Storing the Device Certificate, Key, MQTT Broker endpoint and IoT Thing name

Device Certificate, Device Private Key, MQTT Broker Endpoint and IOT Thing name needs to be stored in the data flash for the application to work. These are obtained after registering to the Cloud Dashboard.

1. Press '**2'** on the **Main Menu** to display **Data Flash** related commands as shown in the below snapshots. This sub menu has commands to store, read and validate the data.

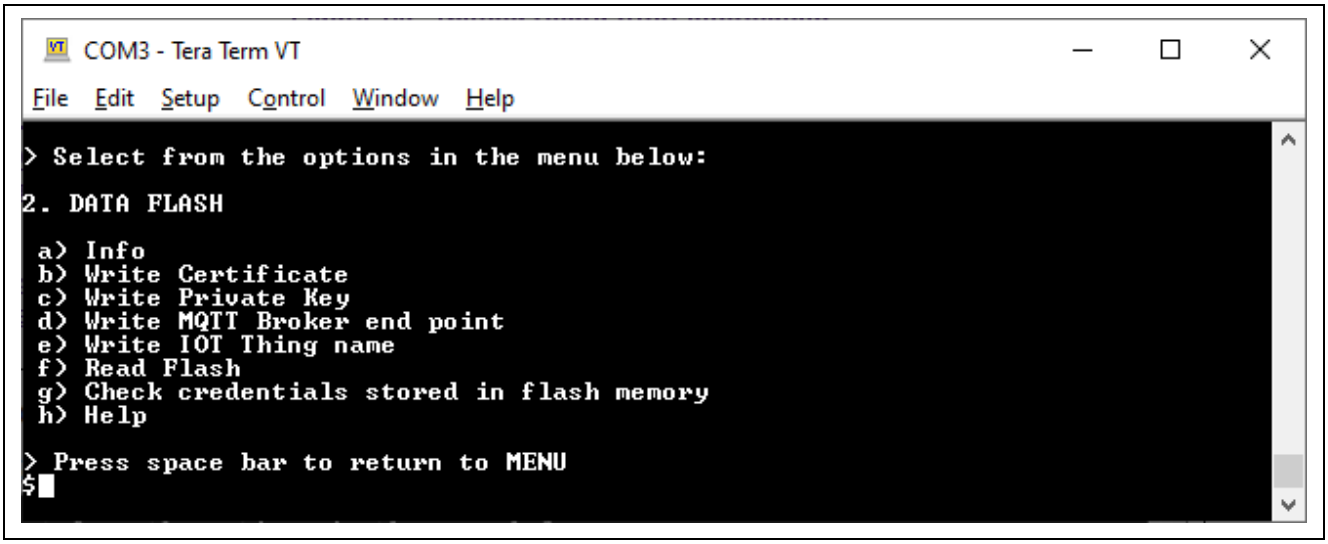


Figure 47. Data Flash related Menu and Commands

2. Please unzip the cert.zip from dashboard.
3. To store the **Device Certificate** press the option '**b**' and Click the "**File" tab**" of the Tera Term and "**Send File**" option and choose the downloaded Device certificate file from the dashboard "**xxxxxcertificate.pem.crt**". The details of downloading the certificates are explained in the Dashboard document linked as part of this App Note.

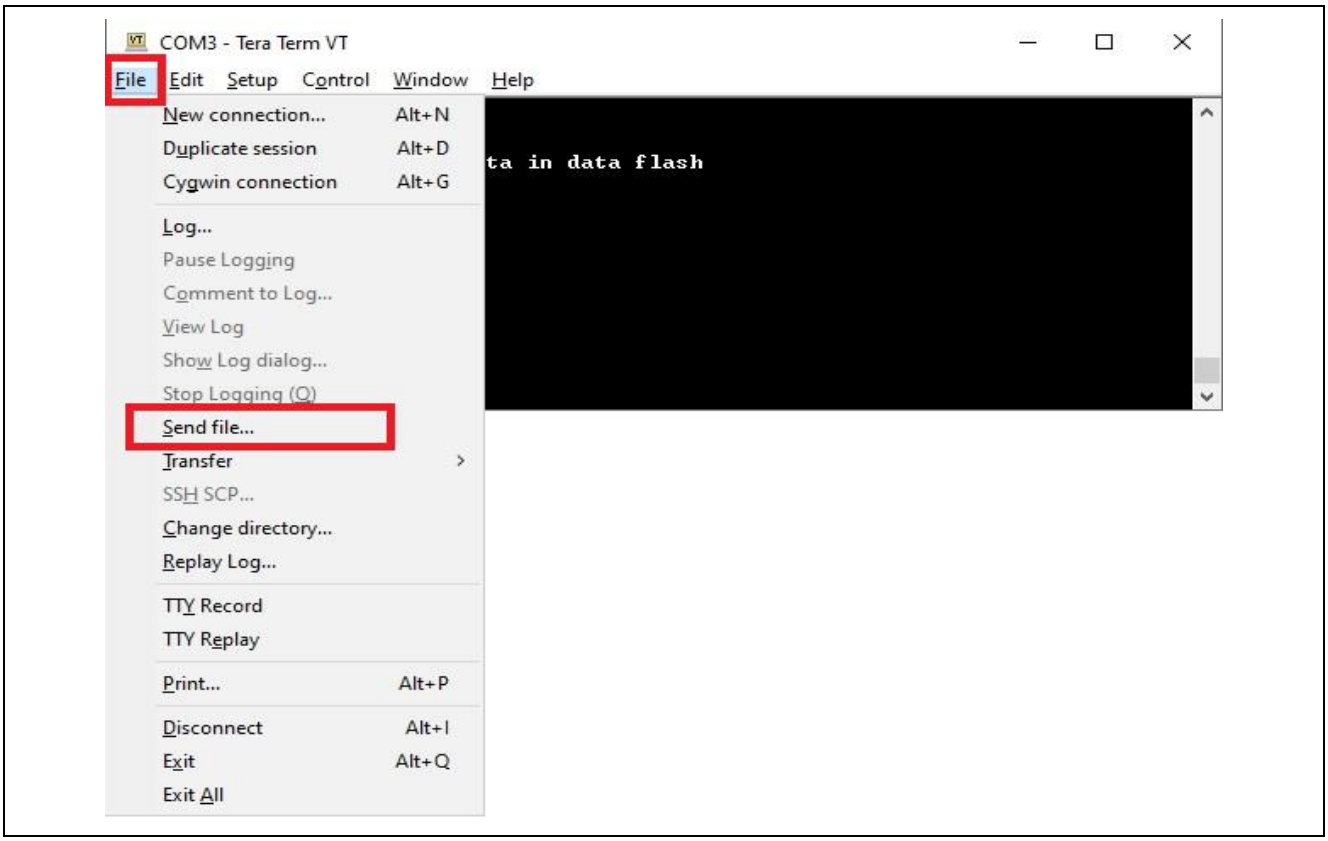


Figure 48. Accessing the Device Certificate

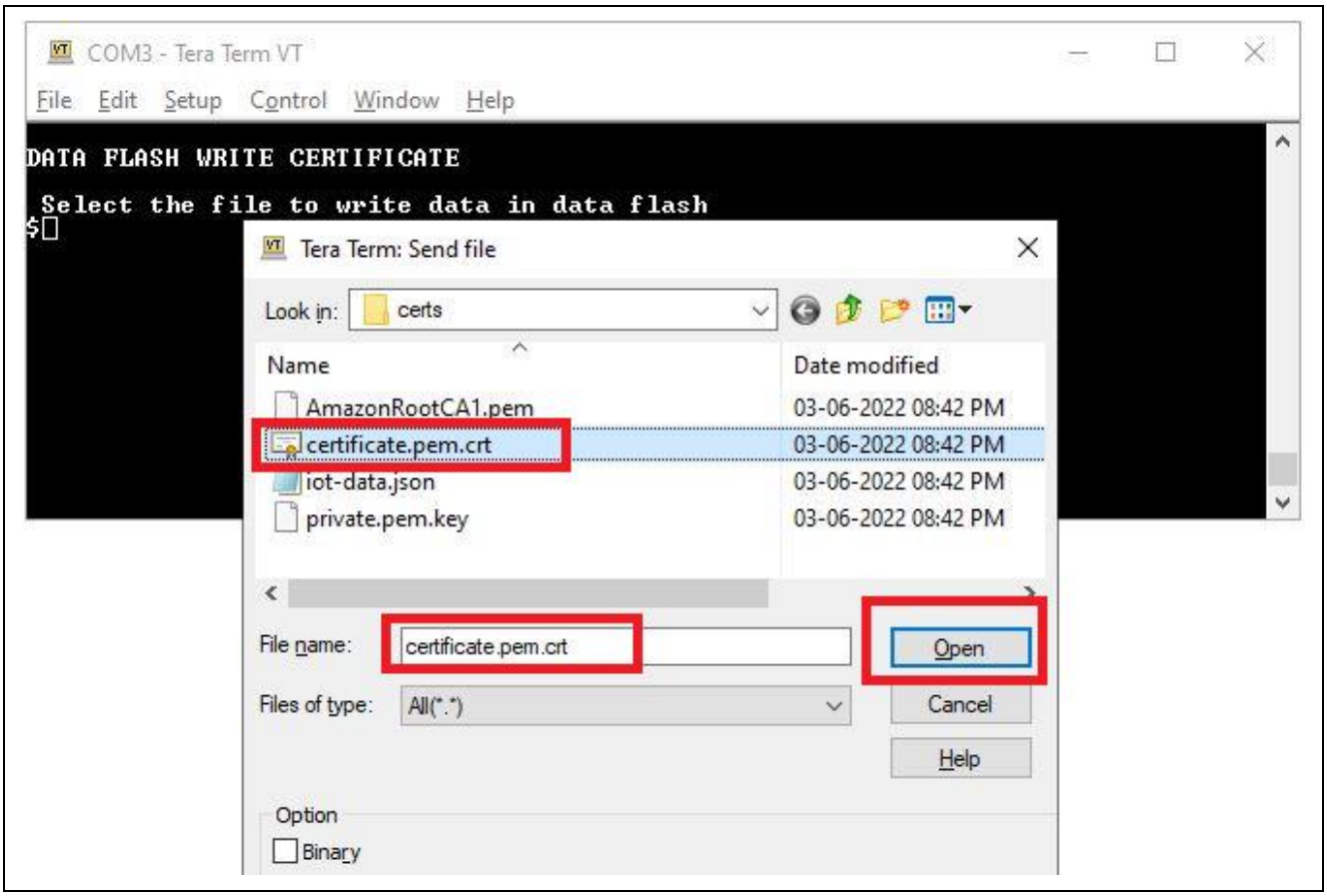


Figure 49. Downloading the Device Certificate into the Data Flash

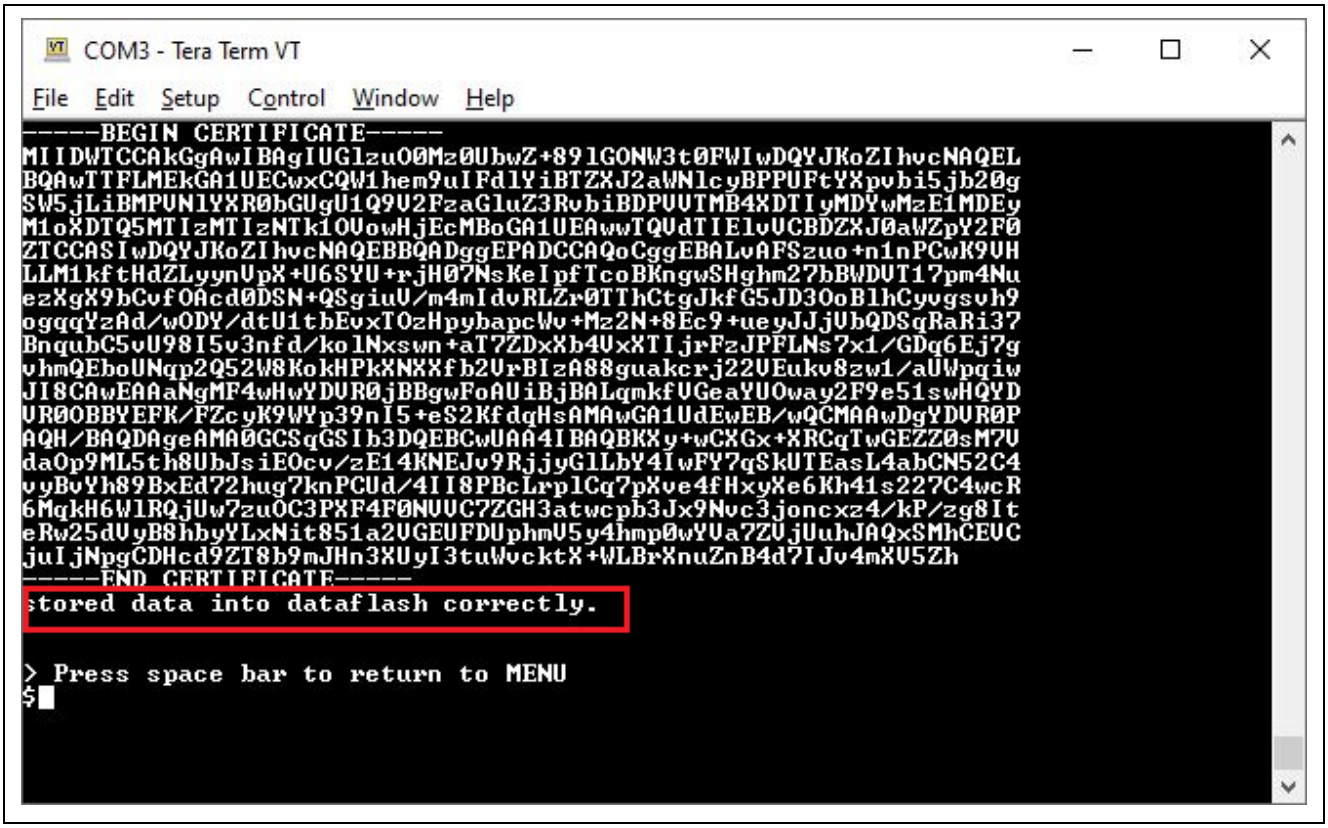


Figure 50. Status of the Downloaded Device Certificate into the Data Flash

4. To store the **Device Key** press the option '**c**' and Click the "**File" tab**" of the Tera Term and "**Send File**" option and choose the downloaded Device Key "xxxxxxxprivate.pem.key" which is downloaded from the Dashboard download link.
5. **Open the "iot-data.json" file**
   There is information about IoT things name and IoT endpoint.

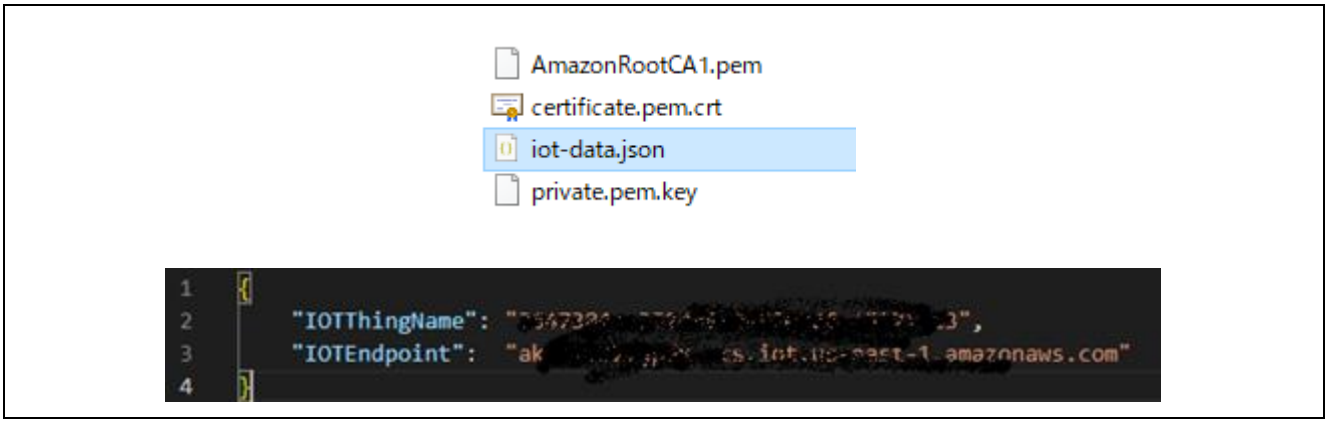


Figure 51 getting the IoT things name and IoT endpoint information

6. To store the **MQTT Broker end point,** copy the end point string between the quotes **xxxxxxxxxx.iot.us-east-1.amazonaws.com** from the downloaded certificate link, press the option '**d**' and Click the "**Edit" tab**" of the Tera Term and "**Paste<CR>**" and verify and confirm the valid string and press OK
Note: Please copy the IOTEndpoint without "".

Figure 52 Copy the Iot endpoint

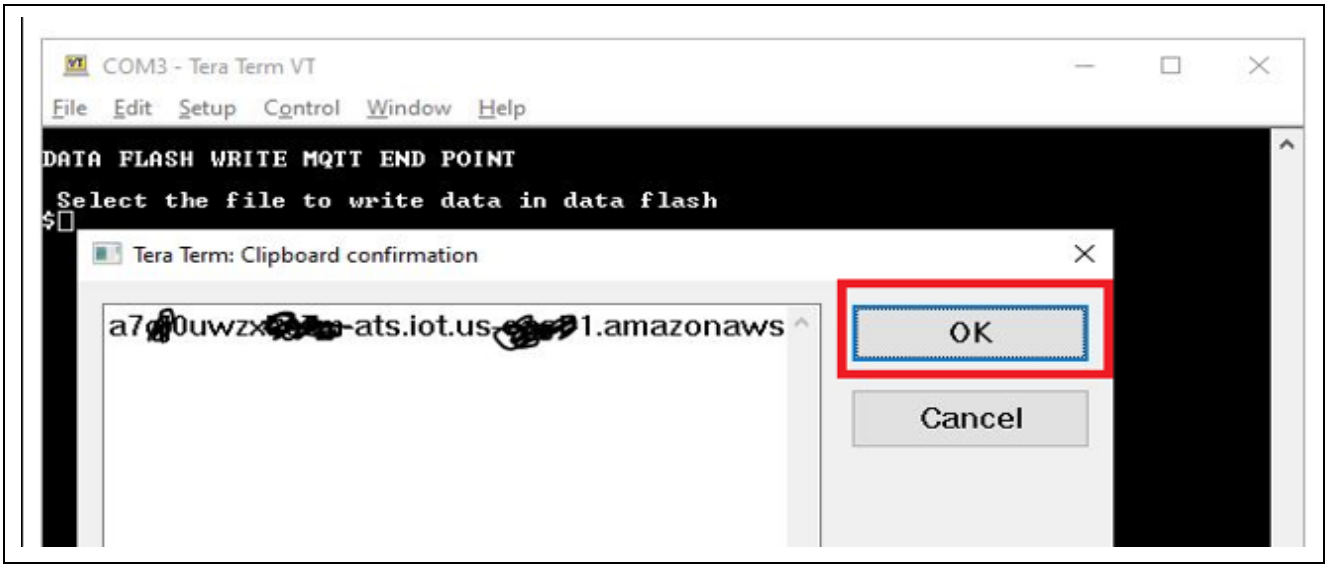


Figure 53 Storing the MQTT IoT endpoint into the Data Flash

7. To store the **IOT Thing Name,** copy the Thing Name string between the quotes **xxxxxxxx-xxxx-xxxxxxxx-xxxx** of IoT thing Name from the downloaded certificate link, press the option '**e**' and click the "**Edit" tab**" of the Tera Term and "**Paste<CR>**" and verify and confirm the valid string and press OK
Note: Please copy the IOTthingName without "".

Figure 54 copy the IoT thing Name

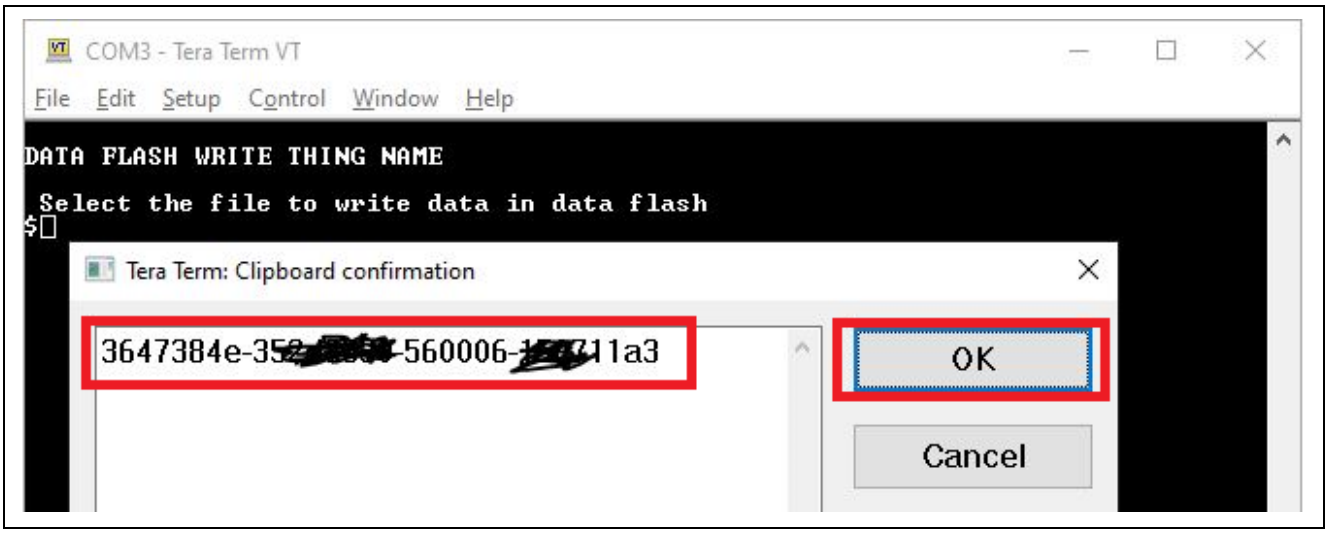


Figure 55. Storing the Thing Name into the Data Flash

8. Press option '**f' and '**g' to read and validate the stored information in the data flash.

Note: Validation of the stored data is very limited and validates minimum set of data points**.** Users are required to input the valid data to the flash obtained from the Dashboard for the proper working of the Application.

4.4.1.1 Starting the Application

After activating the SIM card, registering to the Dashboard and configuring the required Cloud credentials via the CLI, the application is ready to run. Press the option '6' to Start the Application. The Application prints Welcome screen along with the status of validating the Cloud credentials data present in the data flash as shown below.

When the connection is success, the data is showed.

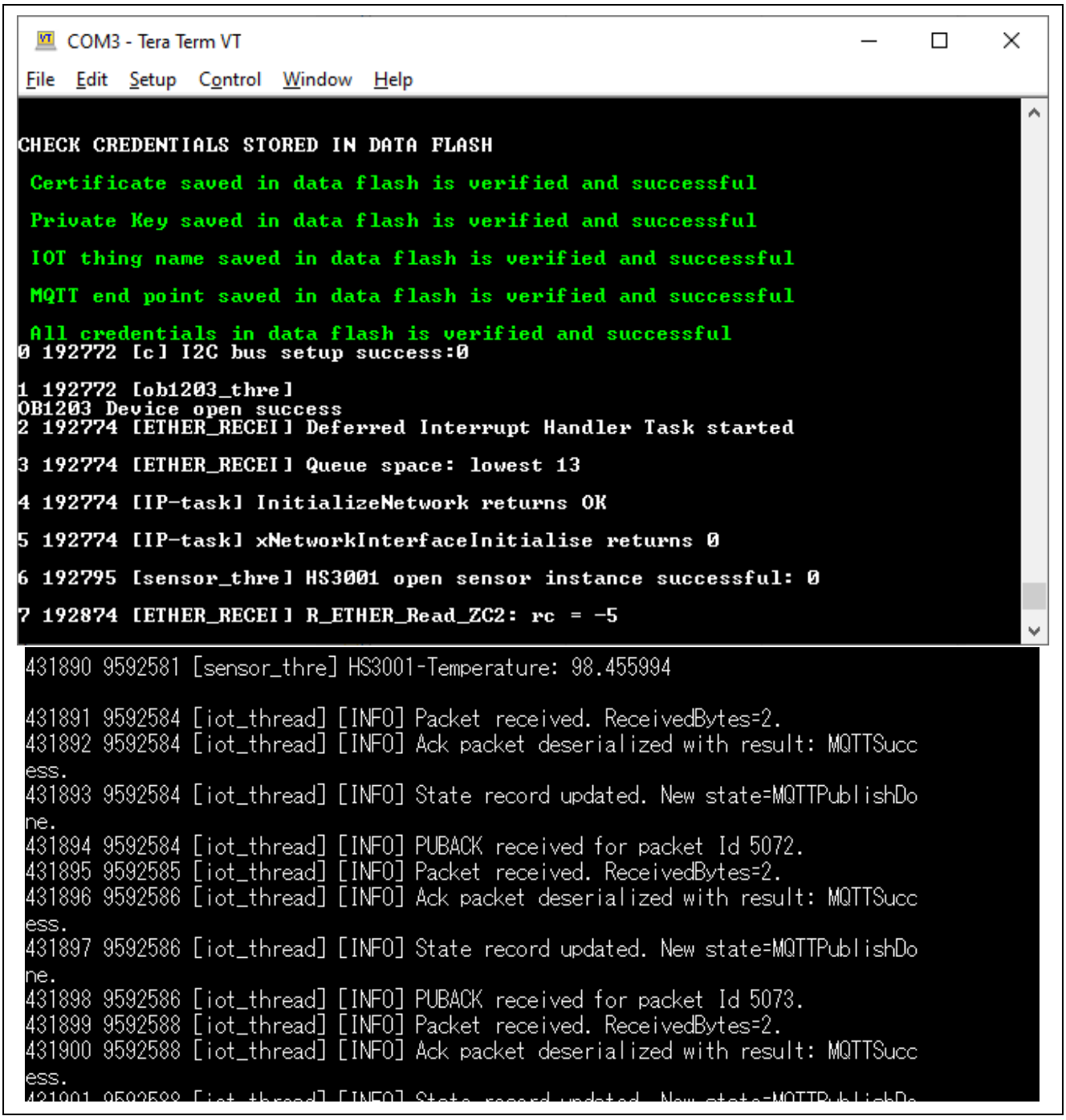


Figure 56. Welcome Screen on the Console

Note: Sensor data will be able to read correctly after having stabilization time.

About the detail of stabilization time, please see “Table 1 Sensor Stabilization Time”.

4.5 For User using their own AWS Account

Note: Complete the steps up to "Check AWS IoT endpoints."

Get an AWS account

Get an AWS account -> From the best "Sign into the Console" button.

When considering using AWS, you can use the AWS free tier.

AWS Free Tier

Log in to the AWS Management Console

Amazon Web Services -> My Account -> AWS Management Console

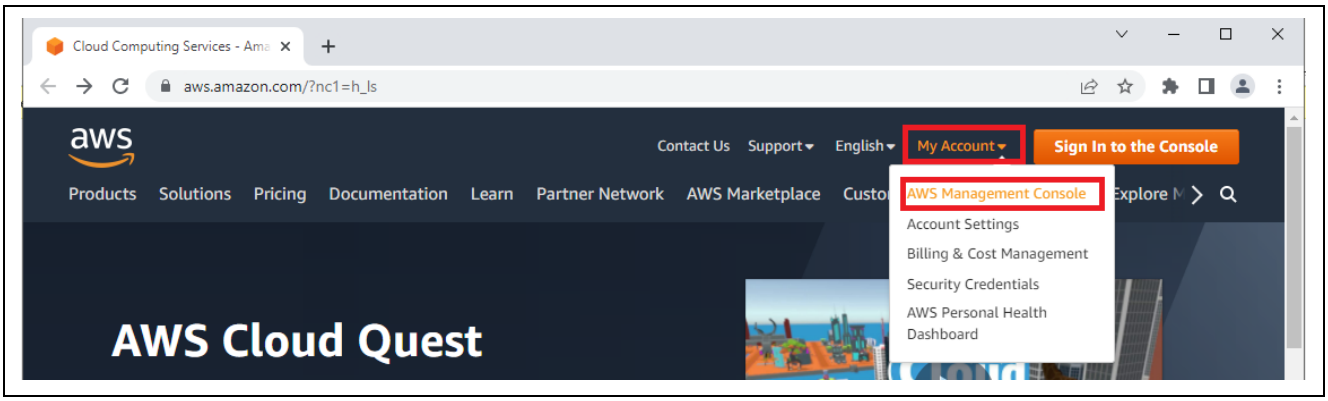


Figure 57 Login the AWS

Move to IoT Core Control Panel

- AWS services -> All services -> IoT Core

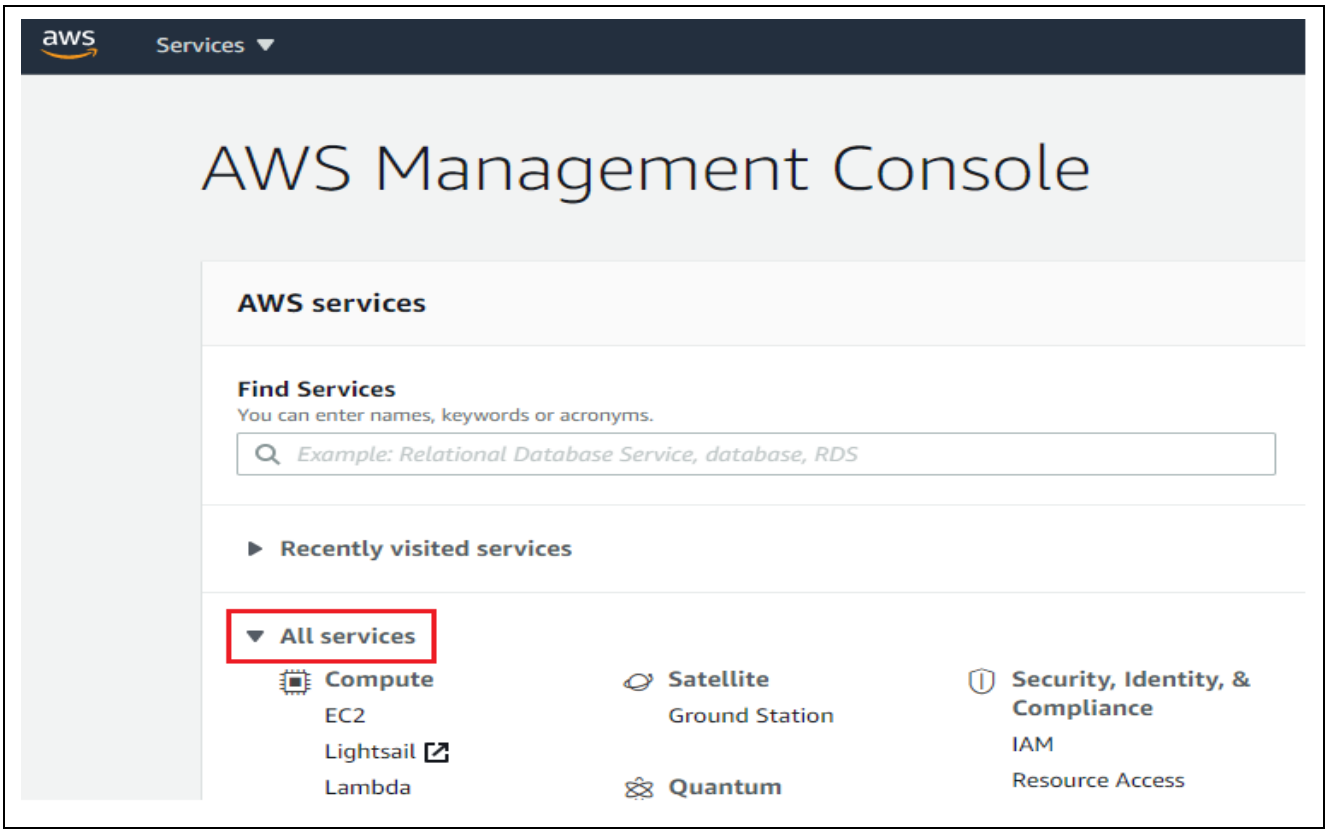


Figure 58 Search the IoT Core 1/2

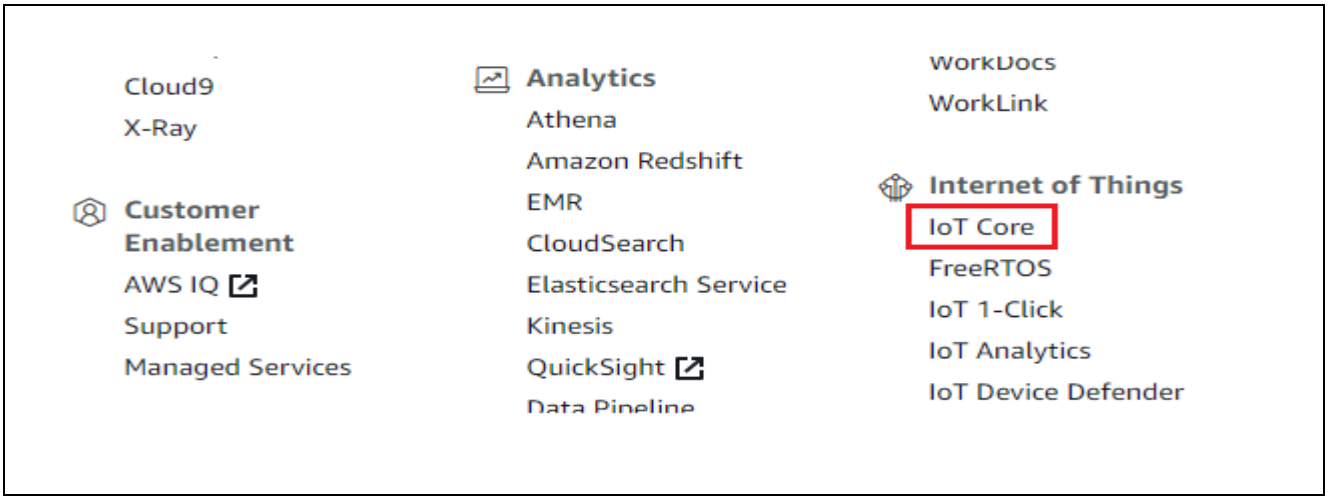


Figure 59 Search the IoT Core 2/2

Create a security policy

- Secure -> Policies -> Create a policy

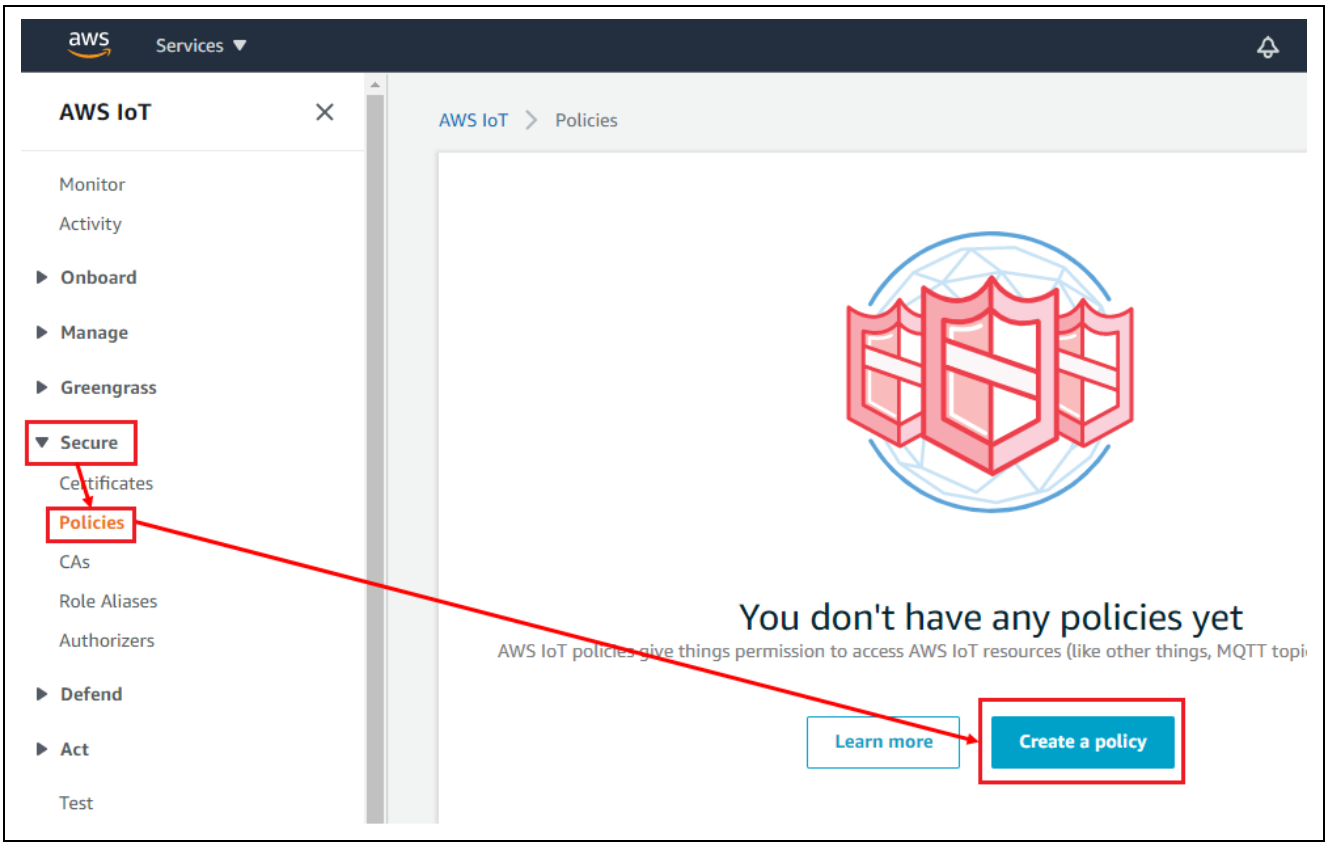


Figure 60 Create the policy1/3

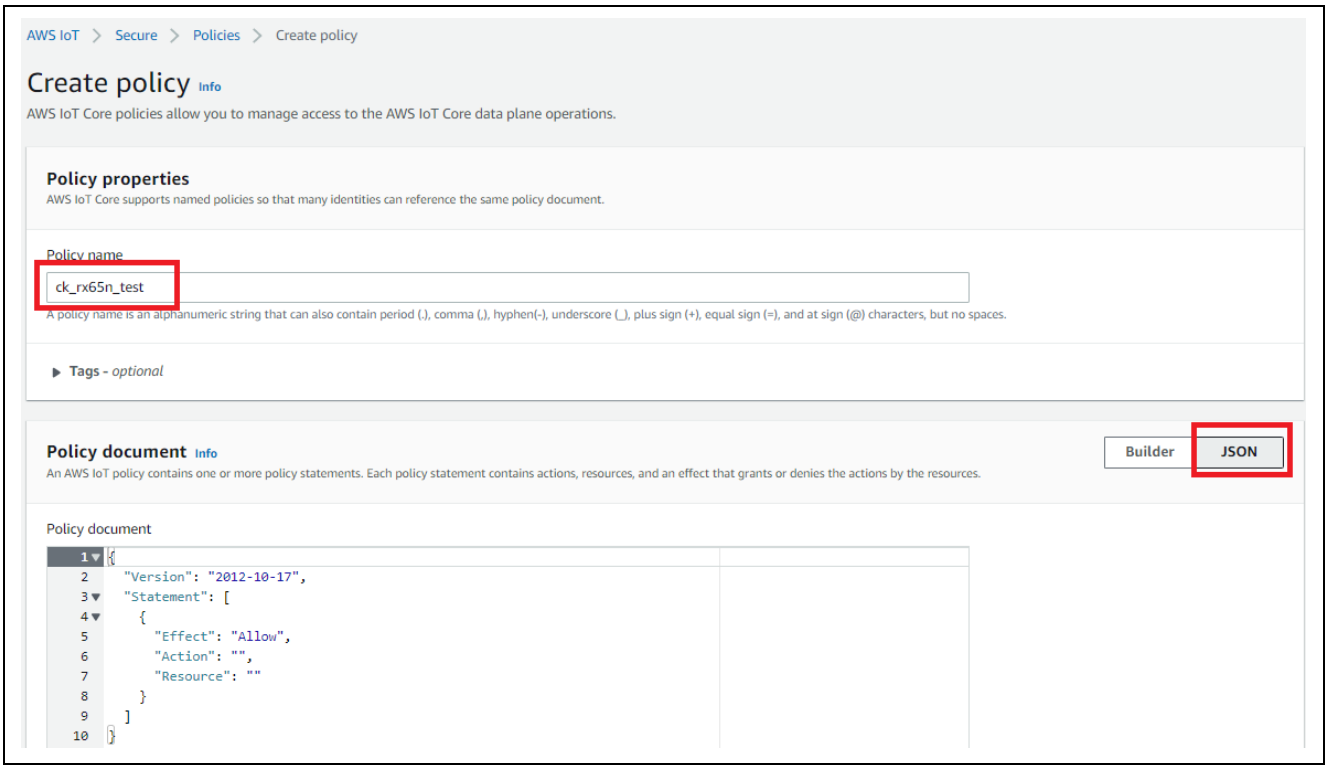


Figure 61 Create the policy2/3

Copy the code below

```
{

        "Version": "2012-10-17",
        "Statement":
        [
                {
                        "Effect": "Allow",
                        "Action": "iot:Connect",
                        "Resource": "*"
                },
                {
                        "Effect": "Allow",
                        "Action": "iot:Publish",
                        "Resource": "*"
                },
                {
                        "Effect": "Allow",
                        "Action": "iot:Subscribe",
                        "Resource": "*"
                },
                {
                        "Effect": "Allow",
                        "Action": "iot:Receive",
                        "Resource": "*"
                }
        ]
}
```

Paste the copied code into the policy syntax -> Create

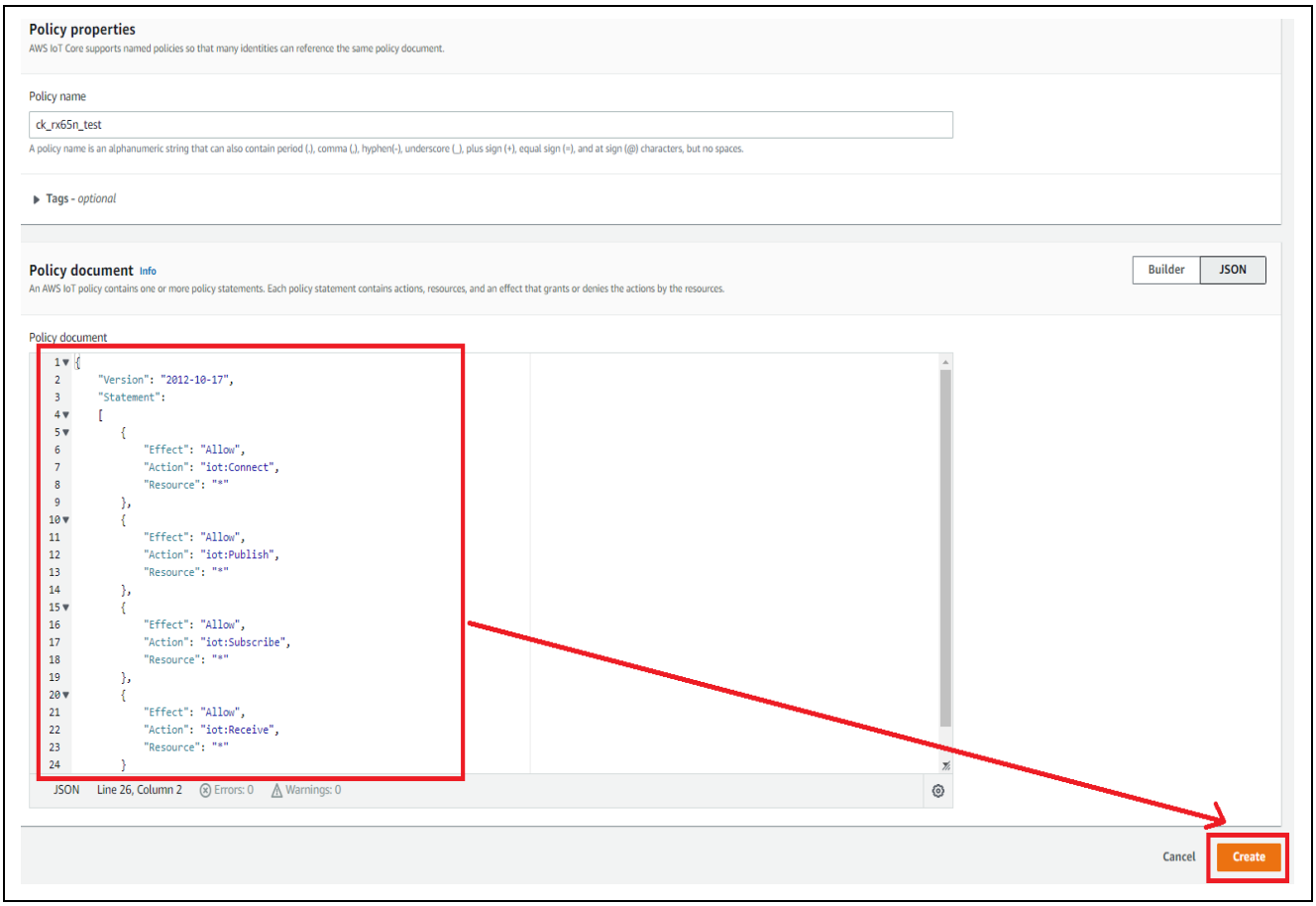


Figure 62 Create the policy3/3

Register your device (thing) with AWS IoT

- Manage -> Things -> Register a thing

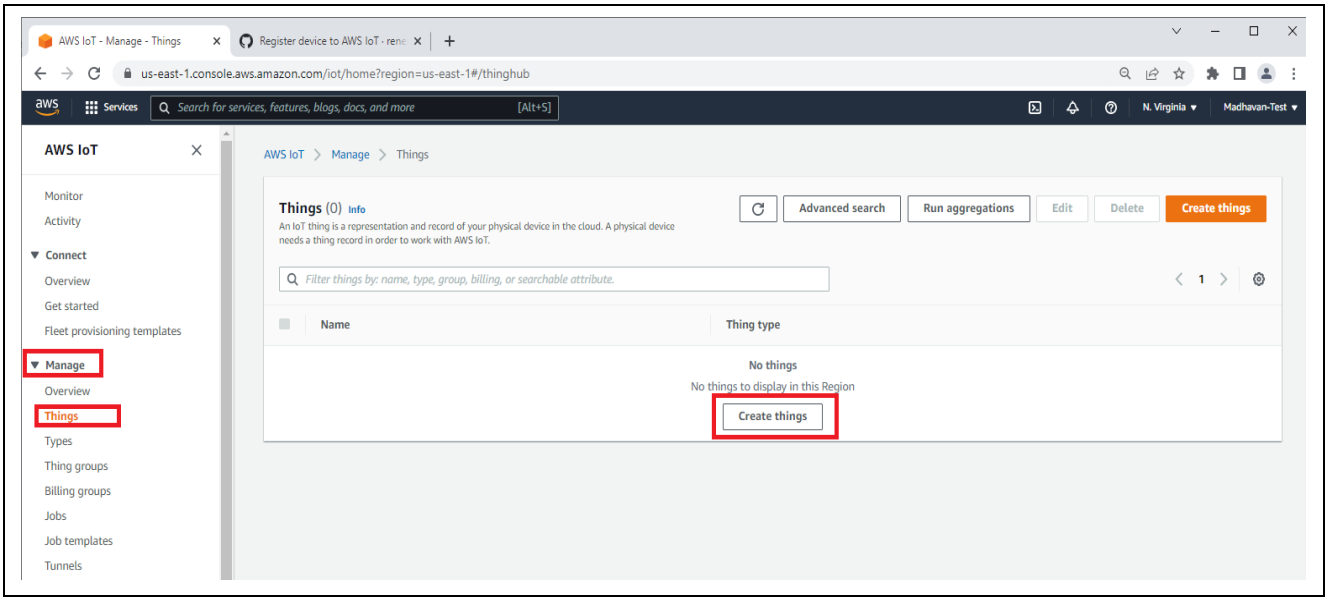


Figure 63 Creating the things 1/5

Creating AWS IoT things -> Create a single thing

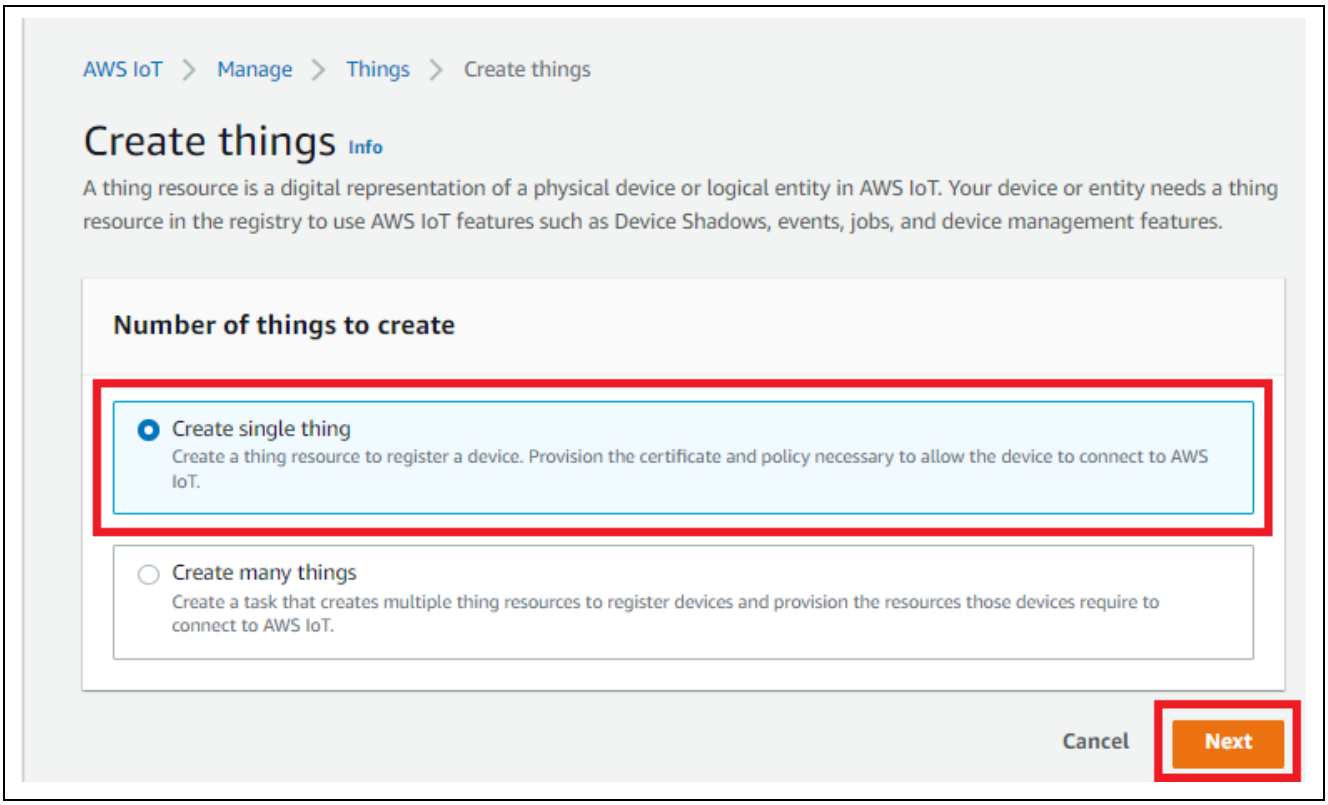


Figure 64 Creating the things 2/5

- Add your device to the thing name-> Next
- Make a note of the name with a text editor (will be used later)

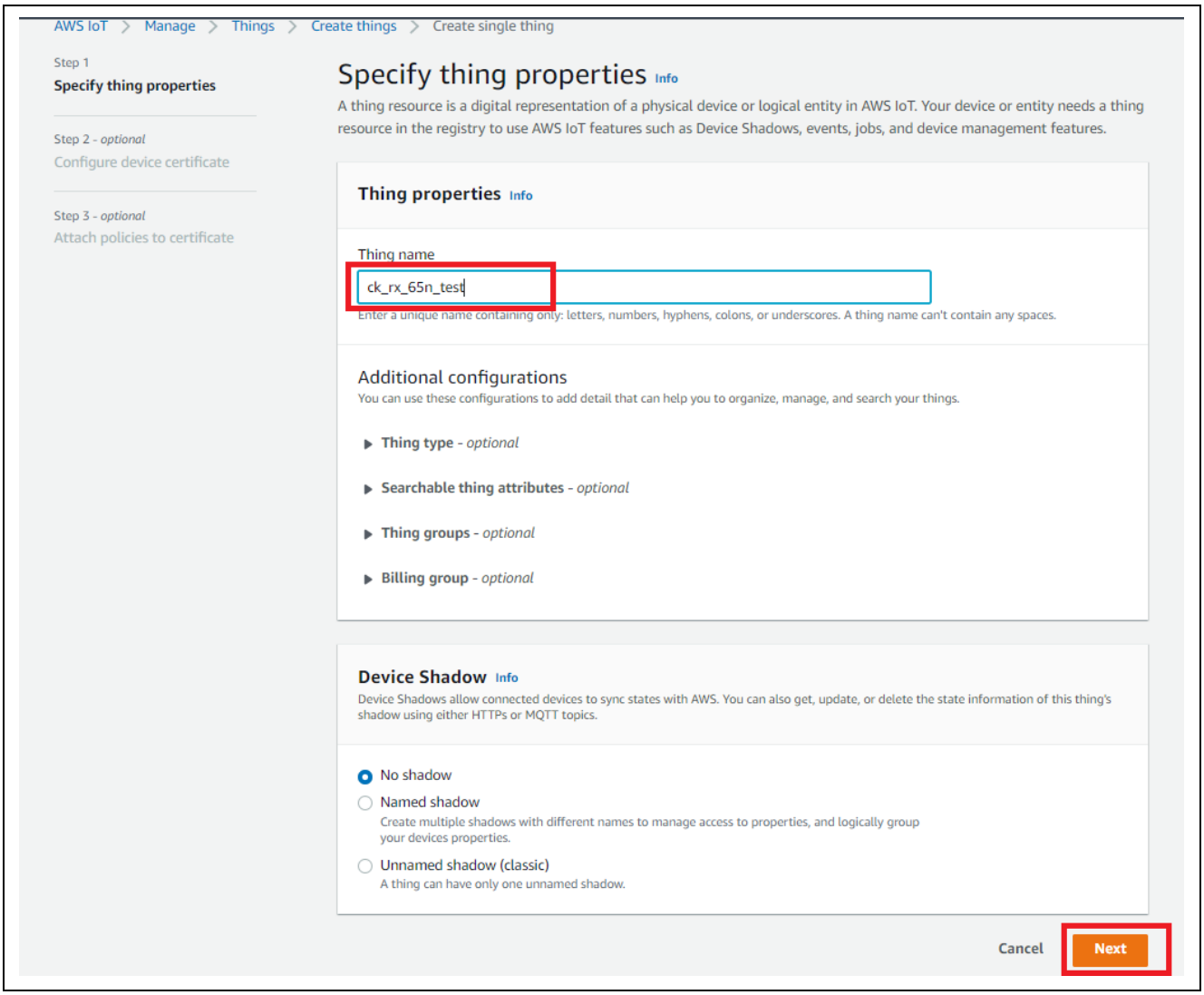


Figure 65 Creating the things 3/5

Auto-generate a new certificate

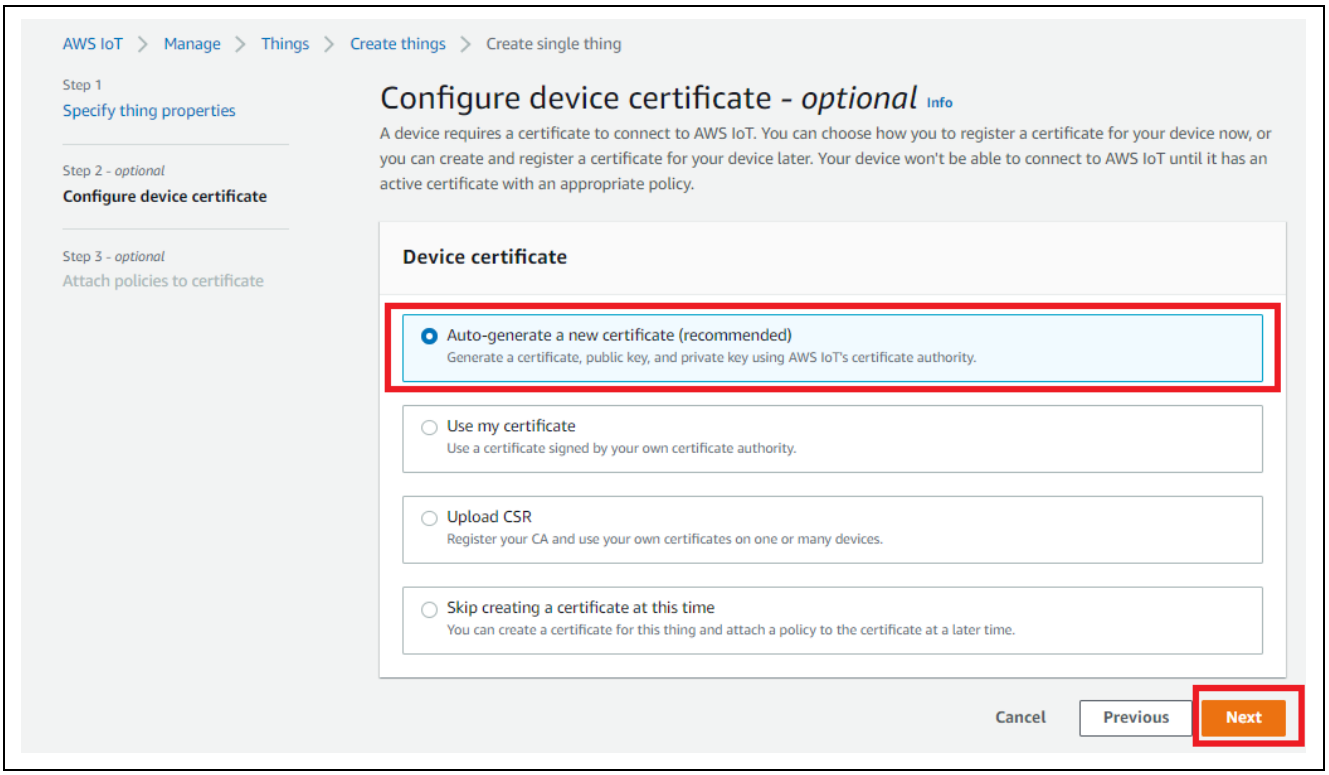


Figure 66 Creating the things 4/5

- Add a policy for your thing

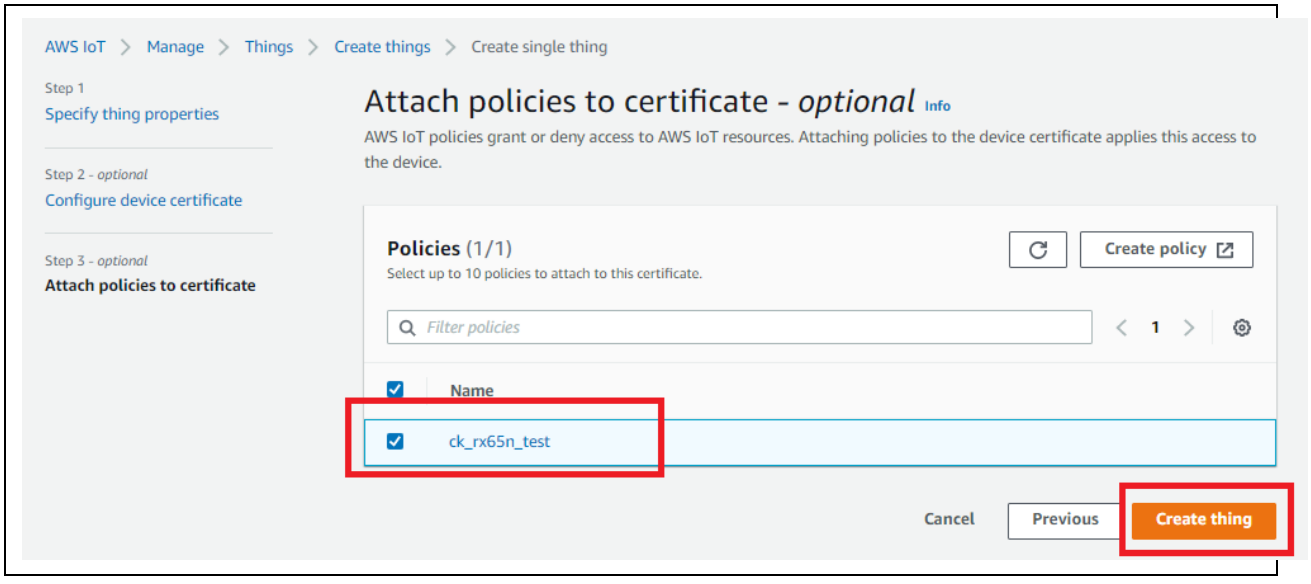


Figure 67 Creating the things 5/5

Download A certificate for this thing/A public key/A private key

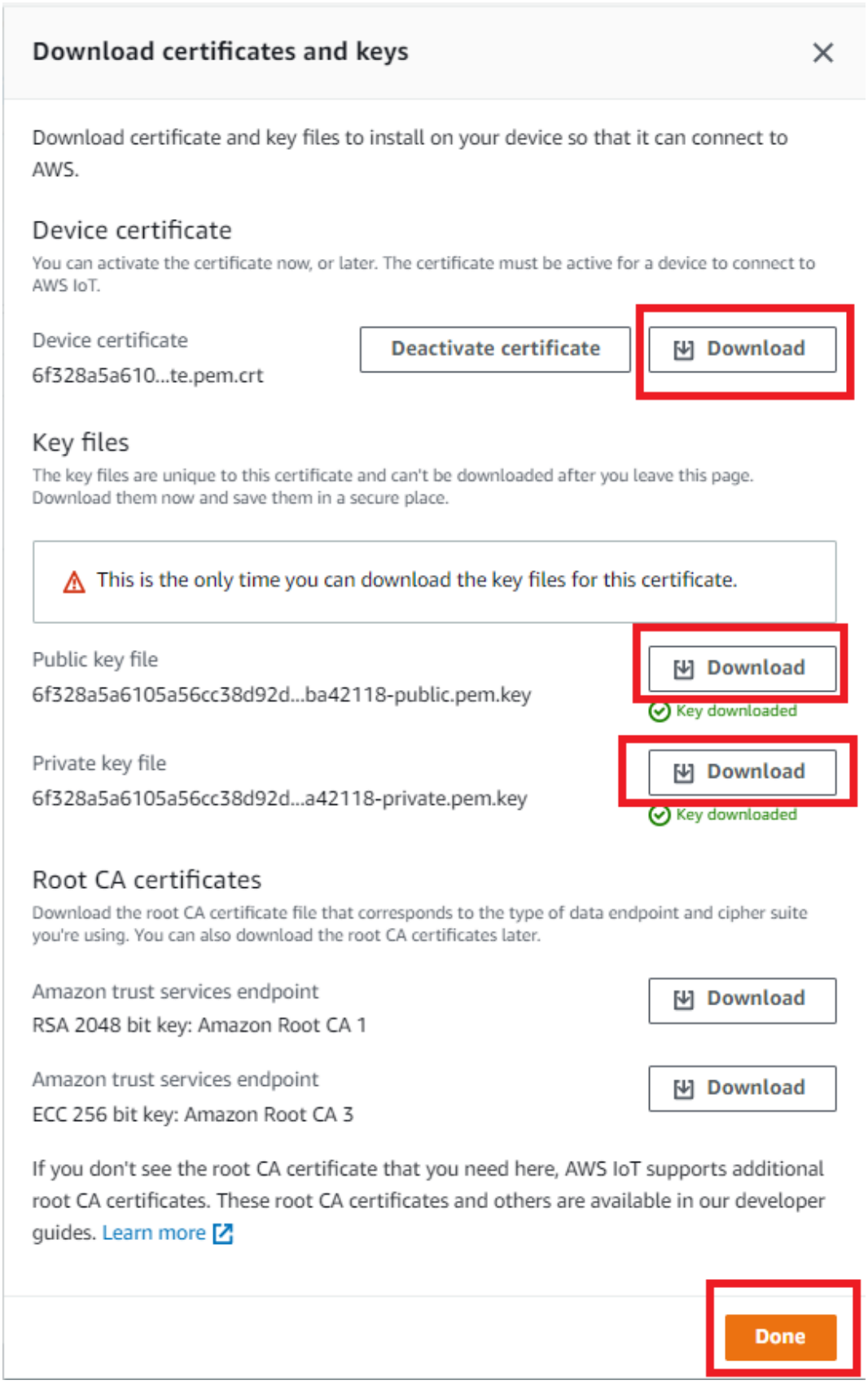


Figure 68 Download A certificate for this thing/A public key/A private key

Check AWS IoT endpoints

- **Make a note of the endpoint in a text editor etc. (will be used later)**

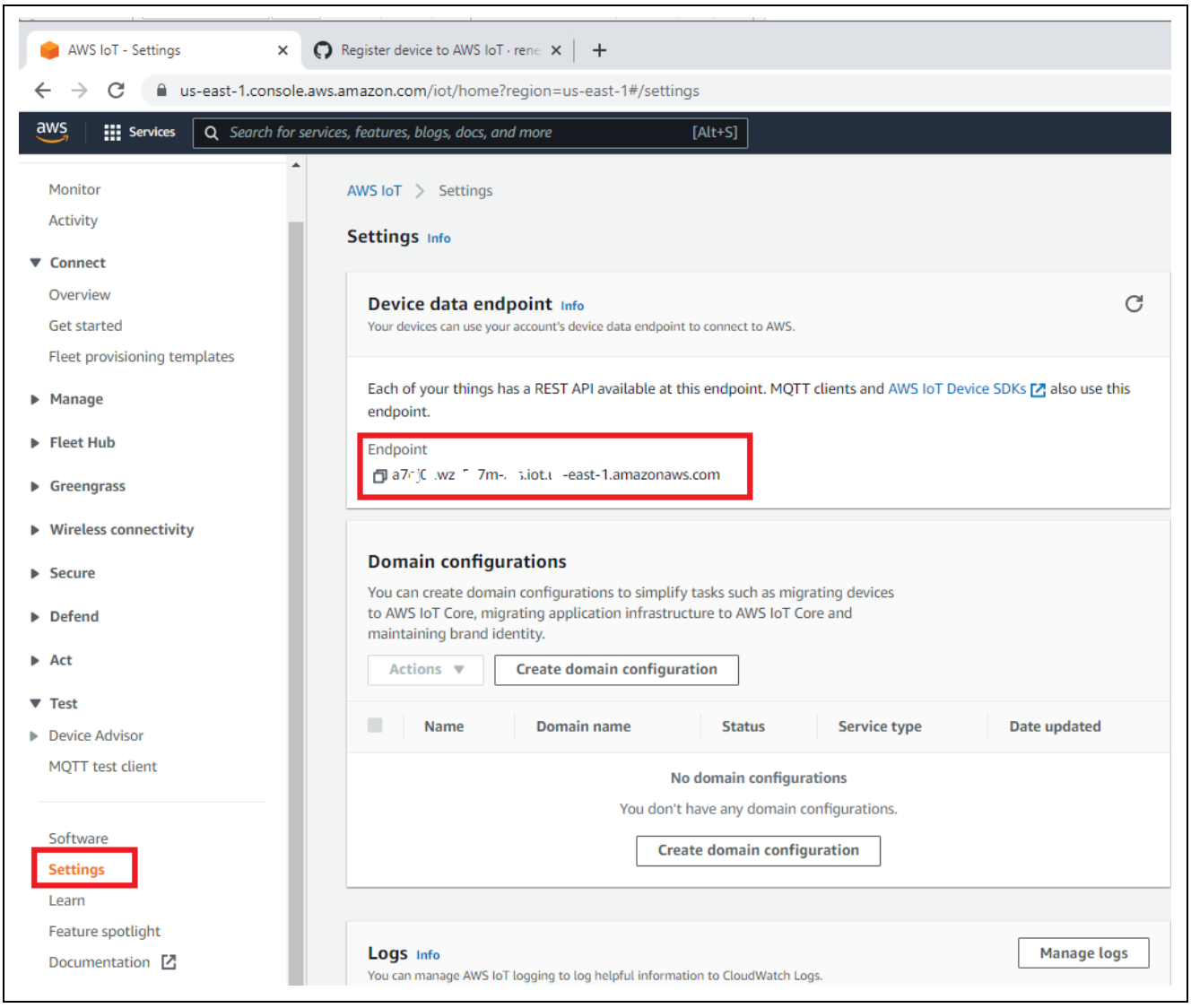


Figure 69 Check AWS IoT endpoints

Reference

Register device to AWS IoT tutorial also available GitHub.

Link: https://github.com/renesas/amazon-freertos/wiki/Register-device-to-AWS-IoT

4.5.1 For install the credential

Please see from **4.3 Hardware Preparation** section.

4.6 About Connecting to AWS IoT

This section describes the steps to be followed to connect the device to the AWS IoT.

Note: For Ethernet Applications, firewalls in the network may prevent connectivity to AWS IoT. Configure the network to allow access to the MQTT Port 8883.

4.7 Verifying the Application Project using AWS Dashboard and Renesas Dashboard

This section describes the steps on how to verify this application example's functions.

Note: Wait for the board to get the IP address from the service provider upon successful cellular initialization, and the board to resolve the DNS lookup for the endpoint. After the successful MQTT connection message on the Console "***Successful MQTT Connection to the end point***", the device is ready for Publishing and Subscription of Messages.

Note: This Application involves AWS MQTT IOT Core, user has an option to use the AWS IOT Dashboard for the Validation purpose, in addition to using the Renesas GUI based Dashboard for customized view of all the Sensor Data.

For the verification purposes, the user can use the AWS IOT core Dashboard for configuring and controlling the Subscription and Publishing of the Topics as described in the following sections.

On the AWS cloud Dashboard side, go to IoT Core and select **Test**, then choose **MQTT test client**. Subscribe to a topic listed below one at a time. The sample snapshot of subscribing to the topics are shown below.

Note: The messages shown under are **case sensitive**; users need to take care of this entering the publish or subscribe messages.
Only enter one message at a time. Copy the message 'as-is' between the quotes and do not include any extra spaces.

```
"aws/topic/iaq_sensor_data"
"aws/topic/oaq_sensor_data"
"aws/topic/hs3001_sensor_data"
"aws/topic/icm_sensor_data"
"aws/topic/icp_sensor_data"
"aws/topic/ob1203_sensor_data"
```

Note: After the subscription to the Topics, the Dashboard is ready to receive the messages being published from the device.

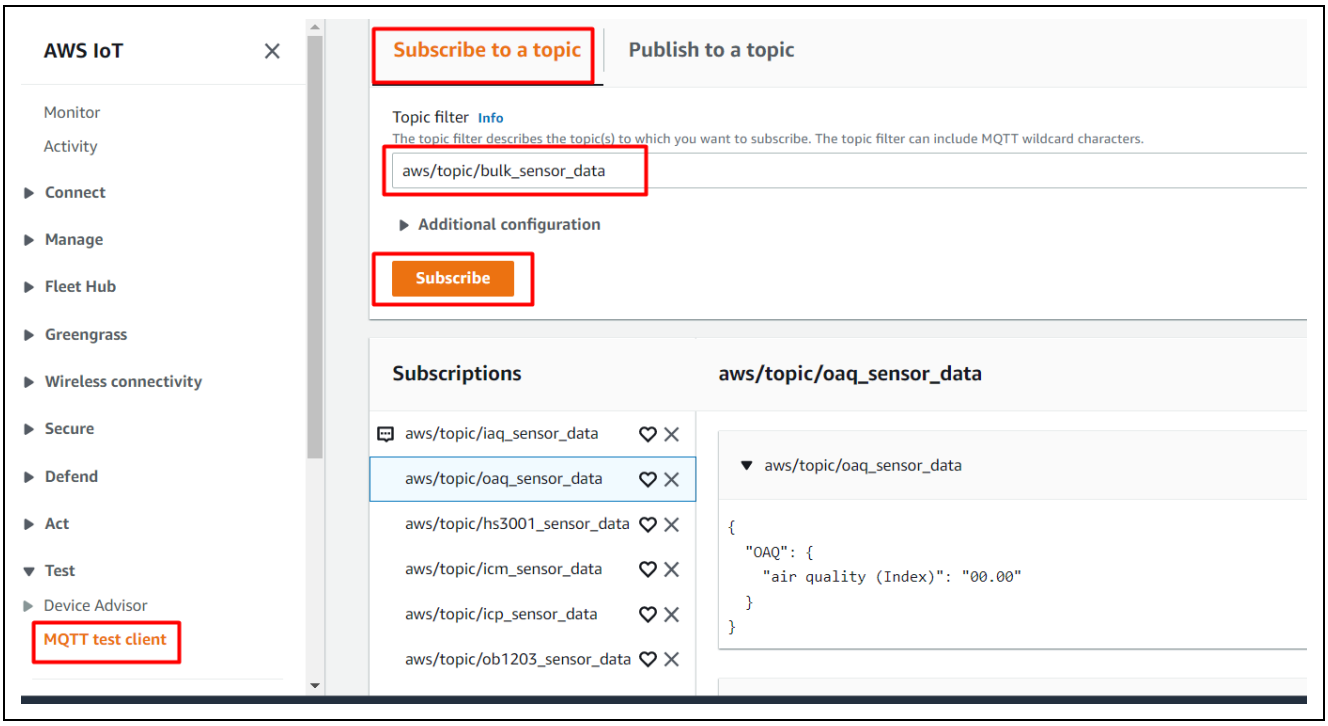


Figure 70. Subscribe to a Topic Messages on the AWS IoT Screen

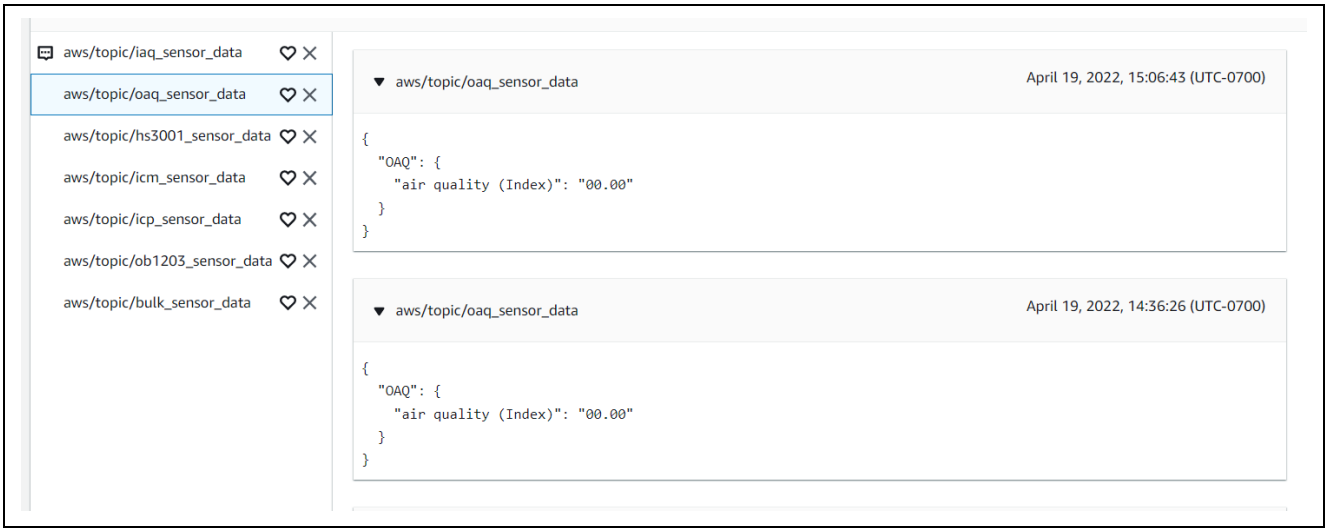


Figure 71. Subscribed Messages on the AWS IoT Screen

4.8 LED Alerts

The board subscribed the topic below.

ck_rx65n_test/example/topicRx

If we publish the below data from AWS console

HS3001 temperature alerts:

Based on temperature dashboard will send the alert messages to CK-RX65N kit via below topic

Topic : aws/topic/set_temperature_led_data

Message: {"Temperature_LED":"HOT"} Will turn on RED in Tri-Color LED
Message: {"Temperature_LED":"WARM"} Will turn on BLUE in Tri-Color LED
Message: {"Temperature_LED":"COLD"} Will turn on GREEN in Tri-Color LED

Example:

Click Test->MQTT test client

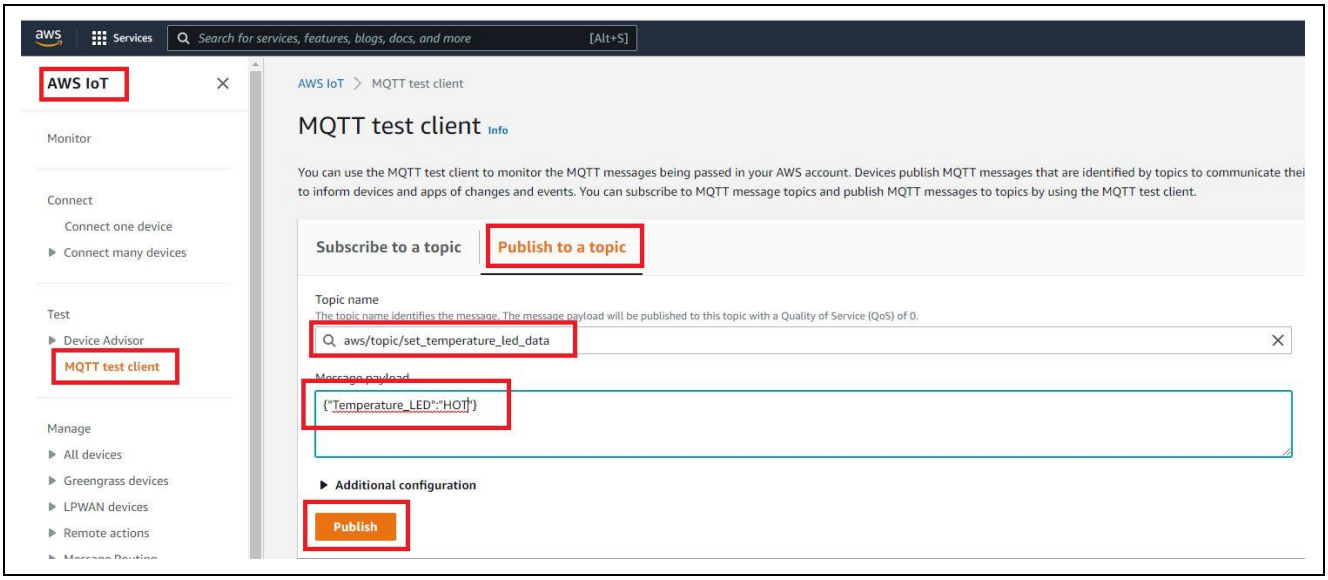


Figure 72 Publish the MQTT message 1/2

OB1203 SPO2 alert alerts:

Based on SP02 value dashboard will send the alert messages to CK-RX65N kit via below topic

Topic : aws/topic/set_spo2_led_data

Message: {"Spo2_LED":"ON"} Will turn off BLUE LED in CK-RX65N
Message: {"Spo2_LED":"OFF"} Will turn on BLUE LED in CK-RX65N

Figure 73 Publish the MQTT message 2/2

5. Restrictions

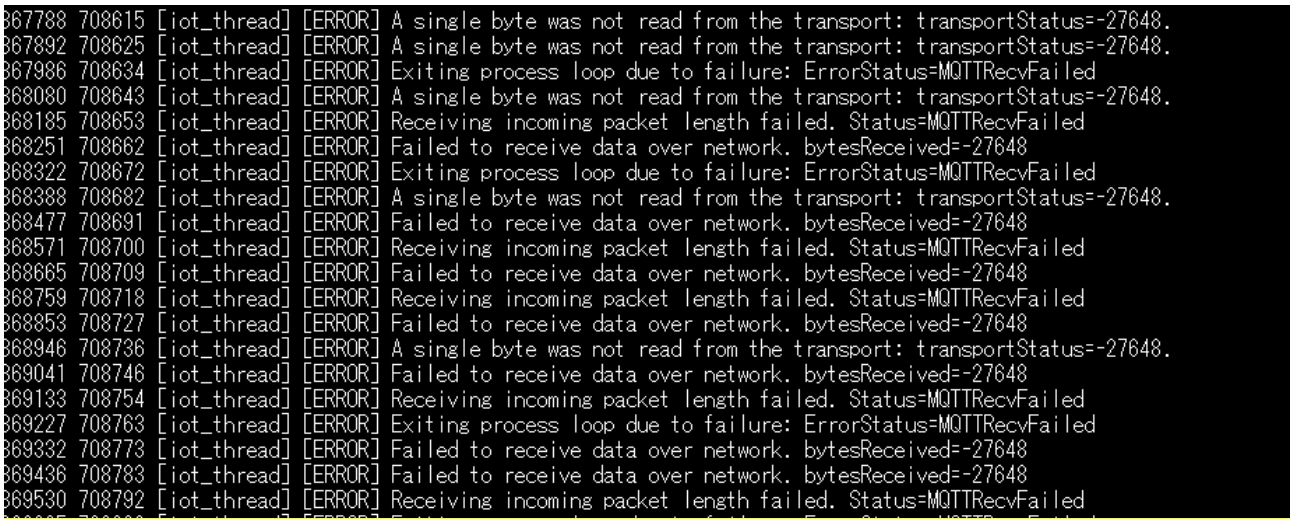
5.1 Communication time (Cellular version of Project)

This version of the cellular project may disconnect when running for more than 10 hours.

Then it shows below errors at the terminal.

It can re-communicate when you reset the device.

If you face this issue least a few hours, please do “**8. Apply Patch files**” step 4.1.1 section.



6. Note and trouble shooting

6.1 About stabilization time for sensor

There is stabilization time for each sensor. It cannot read correct values during the time.

See below the detail of stabilization time of each sensor of table.

Table 1 Sensor Stabilization Time

Sensor Name	When power up first time	After soft or hard reset
ZMOD4410 IAQ	Up to 1 Min	Up to 1 Min
ZMOD4510 OAQ	Up to 1.5 hours	Up to 1 Hours
OB1203	Up to 20 Min (After putting figure on sensor, it may take up to 60 seconds to sense data)	Up to 20 Sec (After putting figure on sensor, it may take up to 60 seconds to sense data)
HS3001	Up to 30 Sec	Up to 10 seconds
ICP	Up to 30 Sec	Up to 10 seconds
ICM	Up to 30 Sec	Up to 10 seconds

6.2 Connection issue when using Ethernet (Wired cable)

The Ether PYH only supports the full duplex communication. If your rooter or Ethernet hub only supports half duplex, it cannot connect the internet. Please use full duplex devices.

6.3 About the trouble of current supply short when using RYZ014A

If the CK-RX65N board is not powered through the Debug port (J14) the current available to the board may be limited to 100 mA. When using the supplied RYZ014A Pmod module with other code (found here: RYZ014A - LTE Cat-M1 Cellular IoT Module | Renesas) be aware that this Pmod has a maximum operating current of **480 mA** dependent upon the LTE band, Tx/Rx settings, and network coverage. Please ensure that the host board can supply sufficient power or provide supplemental USB power via CN4 on the Pmod to avoid RF instability.

6.4 About when build errors occur

If a 'No such file or directory' error occurs, the project path may be too long. When the path is longer than 256 characters, e² studio outputs errors at build time.
When this error occurs, move the project to a shorter path location (e.g., under C:\).

6.5 About when unable to log in to the Dashboard (Grafana account)

If you cannot log in to the Dashboard with the password you changed in step 6 of 4.2.2 To get the account 10USD of trial of AWS, try the following.

- Set “admin” in the Email or username field and set the changed password in the password field.

When changing the password for the initial session, the username is not changed from admin. Therefore, admin must be entered in the username field. To enable users to log in with your own username and email address, please change the user information in the Server Admin menu after logging in.

6.6 Notes on Performing Firmware Update Over-The-Air on AWS FreeRTOS

The following symptoms occur when performing Firmware Update Over-The-Air (FOTA) on AWS FreeRTOS.

1. Device (thing) names and credential information are overwritten.
2. Processing of OTA fails after recovering from low power consumption mode.

For more information, refer to the Tool News below.

[Notes] RX Family Notes on Performing Firmware Update Over-The-Air on AWS FreeRTOS (renesas.com)

Website and Support

Visit the following vanity URLs to learn about key elements of the RX family, download components and related documentation, and get support.

CK-RX65N Kit Information	renesas.com/rx/ck-rx65n
RX&RA Cloud Solutions	renesas.com/cloudsolutions
RX Cloud solution web	renesas.com/rx-cloud
RX Product Information	renesas.com/rx
RX Product Support Forum	renesas.com/rx/forum
RX Driver Package	renesas.com/RDP
Renesas Support	renesas.com/support

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	14-June-2022		First version
1.10	29-June-2022	15	Improved 5.1.4 Activating a SIM card on MicroAI Launchpad of activation way of SIM
		49	Added the restrictions section
		Program	Fixed the program about getting the issue of UUID lacking parts of the number.
1.20	06-July-2022	10-11	Added 8. Apply Patch files
		50	Removed “SpO2 sensor of OB1203 (Cellular version of Project)” from the restriction section. Updated 5.1 Communication time (Cellular version of Project).
		Program	Updated Cellular version of Project - Supported SpO2 sensor of OB1203. - Added patch file to project.
1.30	02-June-2023	11	Added the settings for Truphone SIM
		26	Added 4.1.6 about the activation procedure for Truphone SIM
		50	Added 6.4 about when build errors occur.
			Added 6.5 about when unable to log in to the Dashboard (Grafana account)
			Added 6.6 Notes on Performing Firmware Update Over-The-Air on AWS FreeRTOS

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.

© 2022 Renesas Electronics Corporation. All rights reserved.