Renesas RA Family

RA AWS Cloud Connectivity on CK-RA6M5 v2 with Cellular GM02S – Getting Started Guide

Introduction

This document provides instructions for running the AWS cloud connectivity Application Project on CK-RA6M5 v2 using the Cellular interface.

Applies to:

- RA6M5 MCU Group

Required Resources

The following resources are needed to build and run the MQTT/TLS application example.

Development Tools and Software

- Flexible Software Package (FSP) v6.0.0 and required tools (renesas.com/us/en/software-tool/flexible-software-package-fsp)

Hardware

- Renesas CK-RA6M5 v2 kit (renesas.com/ra/ck-ra6m5)
- PC running Windows® 10 installed Tera Term (v4.99) and an installed web browser (Google Chrome, Internet Explorer, Microsoft Edge, Mozilla Firefox, or Safari)
- Micro USB cable (included as part of the kit. See *CK-RA6M5 v2 User's Manual*).
- USB-C cable for Power supply (included as part of the kit. See *CK-RA6M5 v2 — User's Manual)*
- Renesas LTE Cat-M1 Cellular IoT Module (GM02S)

Prerequisites and Intended Audience

This application note assumes the user can operate the Renesas e^2 studio IDE with the Flexible Software Package (FSP). If not, we recommend reading and following the procedures in the *FSP User's Manual* sections for 'Starting Development', including 'Debug the Blinky Project.' Doing so enables familiarization with e^2 studio and FSP and validates proper debug connection to the target board. In addition, this application note assumes prior knowledge of MQTT/TLS and its communication protocols and knowledge of Cellular modems.

The intended audience is users who want to develop applications with MQTT/TLS modules using Cellular modules on the Renesas RA6 MCU Series.

Note: If you are a first-time user of e^2 studio and FSP, we highly recommend installing them on your system to run the Blinky Project and familiarize yourself with the development environment before proceeding to the following sections.

Note: This Application Project and Application Note are guaranteed to work only with FSP v6.0.0

Prerequisites

1. Access to online documentation is available in the Cloud Connectivity References section.
2. Access the latest documentation for the Renesas Flexible Software Package.
3. Prior knowledge of operating e^2 studio and the built-in (or standalone) RA Configurator.
4. Access to associated hardware documentation such as User Manuals, Schematics, and other relevant kit information (renesas.com/ra/ck-ra6m5).

Contents

1. Importing, Building, and Loading the Project

1.1 Importing

This project, "`aws_ck_ra6m5_v2_cellular_gm02s_app`", can be imported into the e^2 studio using the instructions provided in the RA *FSP User's Manual*. See section *Starting Development > e^2 studio ISDE User Guide > Importing an Existing Project into e^2 studio ISDE.*

1.2 Building the Latest Executable Binary

Upon successfully importing and/or modifying the project into the e^2 studio IDE, follow the instructions provided in the RA *FSP User's Manual* to build an executable binary/hex/mot/elf file. See Section *Starting Development > e^2 studio ISDE User Guide > Tutorial: Your First RA MCU Project > Build the Blinky Project.*

1.3 Loading the Executable Binary into the Target MCU

The executable file may be programmed into the target MCU through any one of three means.

1.3.1 Using a Debugging Interface with e^2 studio

Instructions on how to program the executable binary are found in the latest RA FSP User Manual. See Section *Starting Development > e^2 studio ISDE User Guide > Tutorial: Your First RA MCU Project > Debug the Blinky Project.*

This is the preferred method for programming as it allows additional debugging functionality to be available through the on-chip debugger.

Follow the instructions for programming the board and proceed to section 1.4 Connection Settings and Deviation.

1.3.2 Using J-Link Tools

SEGGER J-Link Tools, such as J-Flash, J-Flash Lite, and J-Link Commander, can be used to program the executable binary into the target MCU. Refer to User Manuals UM08001 and UM08003 on www.segger.com. Use the `.srec` or `.hex` file in the Application Project to program the board and proceed to section 1.4.

1.3.3 Using Renesas Flash Programmer

Renesas Flash Programmer provides usable and functional support for programming the on-chip flash memory of Renesas microcontrollers in each phase of development and mass production. Use the `.srec` or `.hex` file in the Application Project folder to program the board and proceed to section 1.4 Connection Settings and Deviation.

1.4 Connection Settings and Deviation

Reset the board assembly associated with this application note to the default electrical jumper settings as specified in the *CK-RA6M5 v2 User's Manual,* and refer to the note for PMOD2 settings below before proceeding with the next set of instructions.

Note: For this cellular-based cloud connectivity application project and application note, the user must connect the Cellular PMOD (GM02S) module to the connector (J25 – PMOD2) on the board. And we need to use the configuration below for PMOD2 to work with Cellular PMOD (GM02S):

- Open J21 1-2 and 3-4
- Close E20
- Close E8

1.5 Powering Up the Board

To power the board, connect the USB-C cable to the CK-RA6M5 v2 board's J28 connector and the other end to the PC USB port. Connect the micro-USB Cable to the J10 (USB_DBG) connector of the CK-RA6M5 v2 board and the other end to the second USB Port of the PC (this will be the Console Port for the Application). Users are required to use the Command Line Interface (CLI) to configure and run the Application.

Then, run the debug application using the instructions in the following sections.

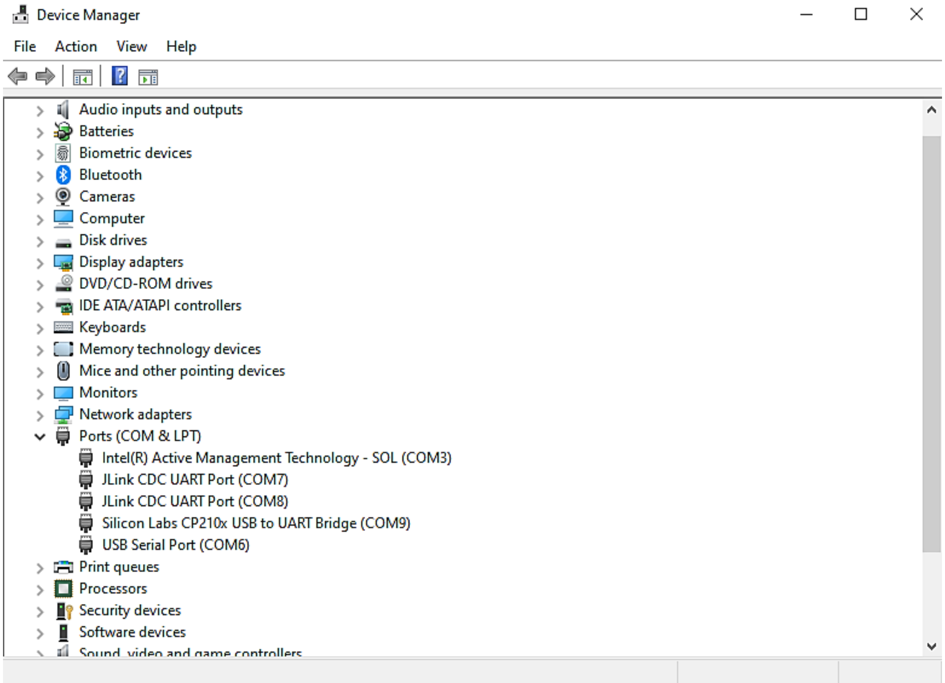
2. Running the Application Project

Note: The steps indicated below are tested on Window® OS only.

2.1 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 **JLink CDC UART Port (COMxx),** and note the COM port number for reference in the next step.

Note: JLink CDC UART drivers are required to communicate between the CK-RA6M5v2 board and the terminal application on the host PC.

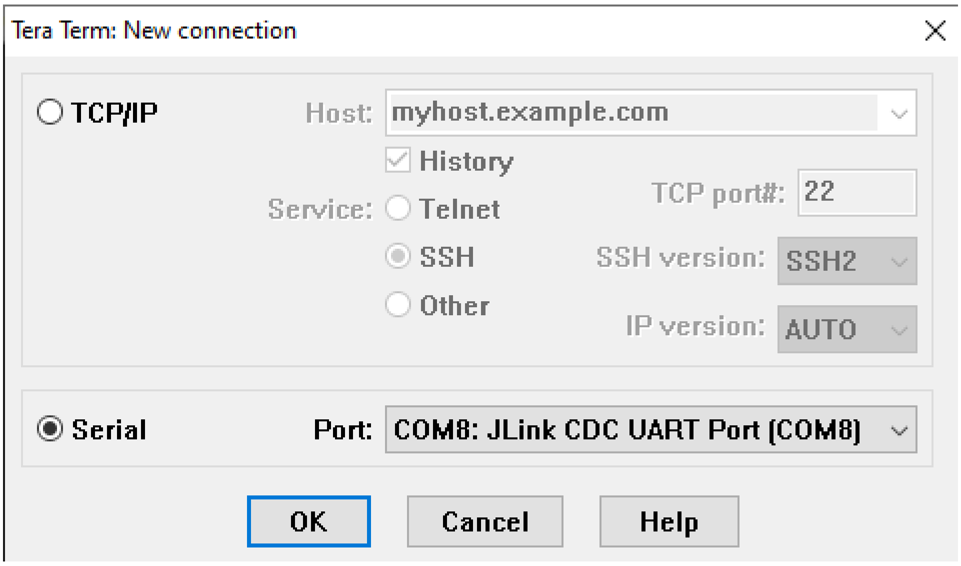


Device Manager

- Audio inputs and outputs
- Batteries
- Biometric devices
- Bluetooth
- Cameras
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- IDE ATA/ATAPI controllers
- Keyboards
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Ports (COM & LPT)
  - Intel(R) Active Management Technology - SOL (COM3)
  - JLink CDC UART Port (COM7)
  - JLink CDC UART Port (COM8)
  - Silicon Labs CP210x USB to UART Bridge (COM9)
  - USB Serial Port (COM6)
- Print queues
- Processors
- Security devices
- Software devices
- Sound, video and game controllers

Figure 1. JLink CDC UART Port in Windows Device Manager

2. Open Tera Term, select **New connection,** select **Serial** and **COMxx: JLink CDC UART Port (COMxx),** and click **OK**.



Tera Term: New connection

○ TCP/IP Host: myhost.example.com

☑ History

Service: ○ Telnet TCP port#: 22

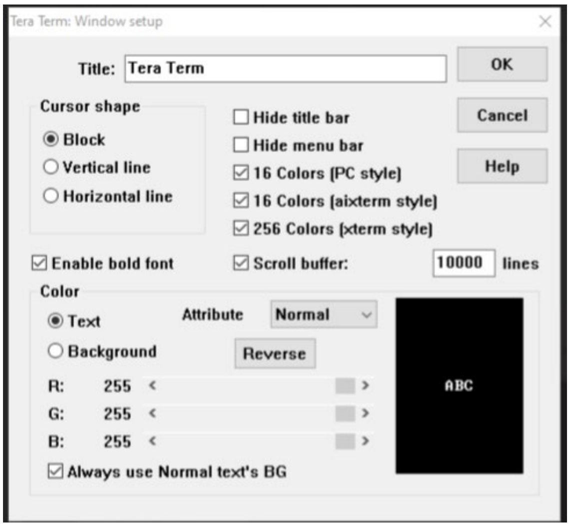
● SSH SSH version: SSH2

○ Other IP version: AUTO

● Serial Port: COM8: JLink CDC UART Port (COM8)

Figure 2. Selecting the UART Port on Tera Term

3. Make sure Tera Term selects the black background; if not, configure it from **Setup > Window** and make the following selections.



Tera Term: Window setup

Title: Tera Term

Cursor shape
- ● Block
- ○ Vertical line
- ○ Horizontal line

- □ Hide title bar
- □ Hide menu bar
- ☑ 16 Colors (PC style)
- ☑ 16 Colors (aixterm style)
- ☑ 256 Colors (xterm style)

☑ Enable bold font

☑ Scroll buffer: 10000 lines

Color
- ● Text
- ○ Background

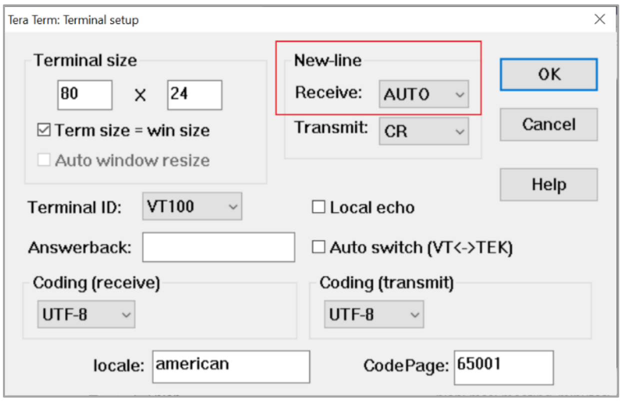
Attribute: Normal

R: 255
G: 255
B: 255

☑ Always use Normal text's BG

Figure 3. Configuring the Black Background for JLink CDC UART on Tera Term

4. Configure for the terminal from **Setup > Terminal…**, select **New-line Receive** as **AUTO**.



Tera Term: Terminal setup

Terminal size: 80 X 24

☑ Term size = win size

□ Auto window resize

New-line
Receive: AUTO
Transmit: CR

Terminal ID: VT100

□ Local echo

Answerback:

□ Auto switch (VT<->TEK)

Coding (receive): UTF-8

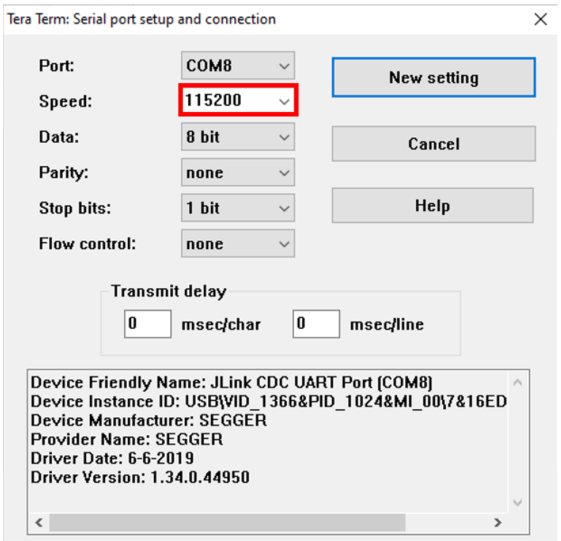
Coding (transmit): UTF-8

locale: american

CodePage: 65001

Figure 4. Configuring Terminal

5. Use the Setup > Serial port… and ensure the speed is set to **115200**, as shown below.



Tera Term: Serial port setup and connection

Port: COM8
Speed: 115200
Data: 8 bit
Parity: none
Stop bits: 1 bit
Flow control: none

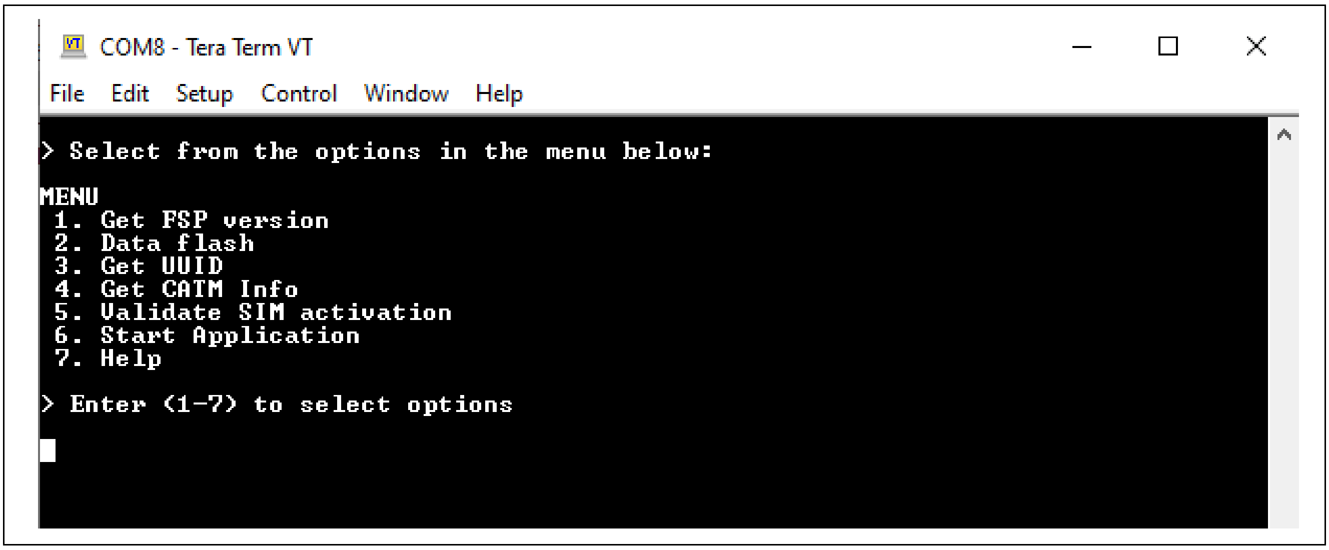
Transmit delay
0 msec/char 0 msec/line

```
Device Friendly Name: JLink CDC UART Port (COM8)
Device Instance ID: USB\VID_1366&PID_1024&MI_00\7&16ED
Device Manufacturer: SEGGER
Provider Name: SEGGER
Driver Date: 6-6-2019
Driver Version: 1.34.0.44950
```

Figure 5. Select 115200 on the Speed Pulldown Menu

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

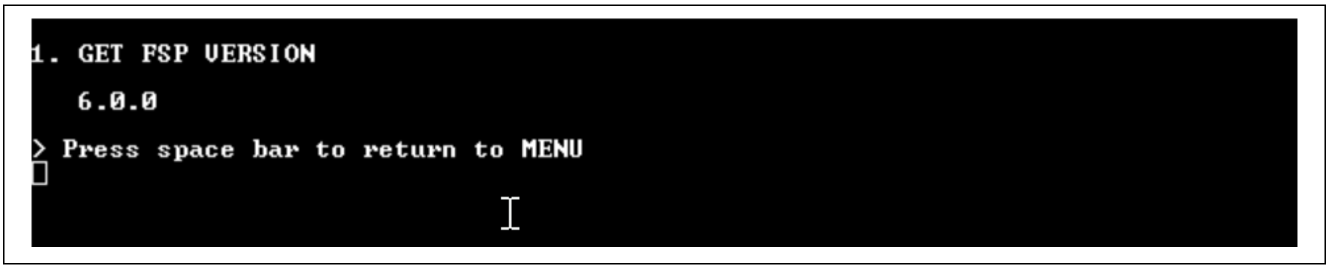
Note: If the menu is not displayed, please reset the board by pressing the S1 user switch.



```
> Select from the options in the menu below:

MENU
 1. Get FSP version
 2. Data flash
 3. Get UUID
 4. Get CATM Info
 5. Validate SIM activation
 6. Start Application
 7. Help

> Enter (1-7) to select options
```

Figure 6. Main Menu

7. In the CLI shown in the preceding screenshot, choose the number to select the commands. For example, when you press **1**, the FSP version of the application is displayed as shown below. At any point in time, press the space bar to return to the previous menu.

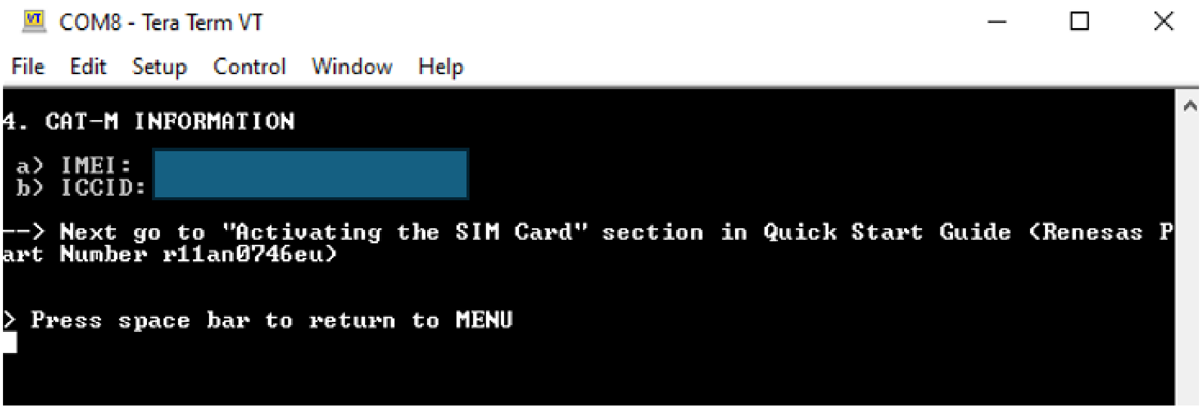


```
1. GET FSP VERSION

   6.0.0

> Press space bar to return to MENU
```

Figure 7. FSP Version Information

2.2 Setting the SIM and Modem Information for Activation

1. Press **4** to display **CAT-M Information**. This menu will communicate with the Cellular PMOD (GM02S) module to obtain the ICCID value 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 Cellular PMOD (GM02S) module until it has successfully connected or timed out. After obtaining the ICCID value, go to Truphone https://www.truphone.com/connectit/ to activate the SIM card (see section 2.3 Activating a SIM card).



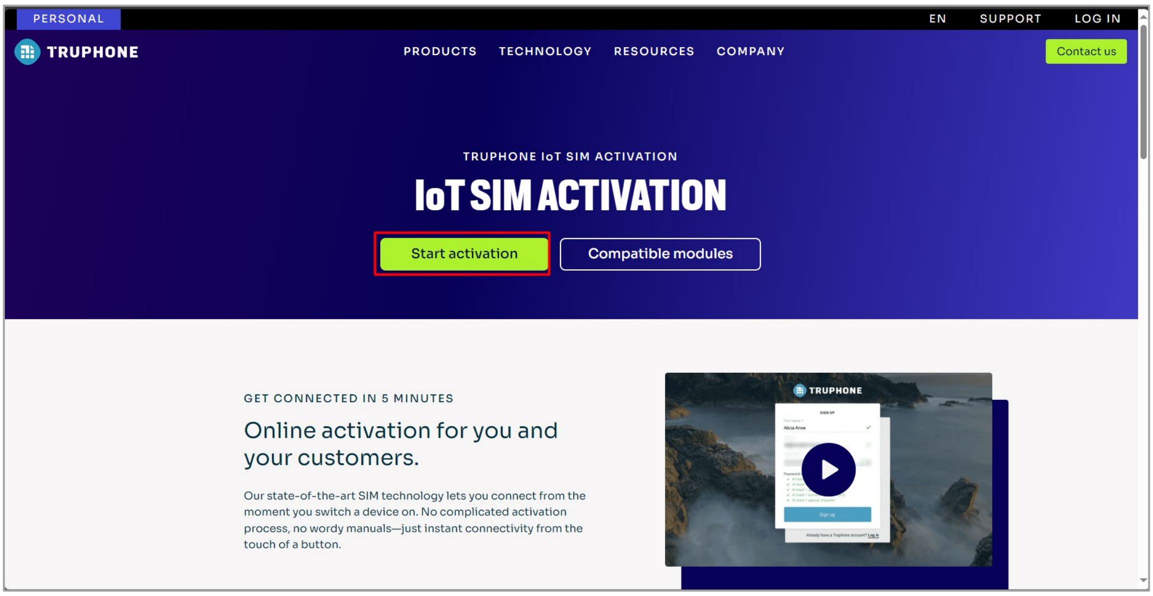
```
4. CAT-M INFORMATION

 a> IMEI:  [redacted]
 b> ICCID:

--> Next go to "Activating the SIM Card" section in Quick Start Guide (Renesas P
art Number r11an0746eu)

> Press space bar to return to MENU
```

Figure 8. CAT-M Information

2.3 Activating a SIM card

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

1. On the opened webpage (snapshot shown in the Figure 9. Activating the SIM card), click the **Start activation** button under **IoT SIM Activation.**



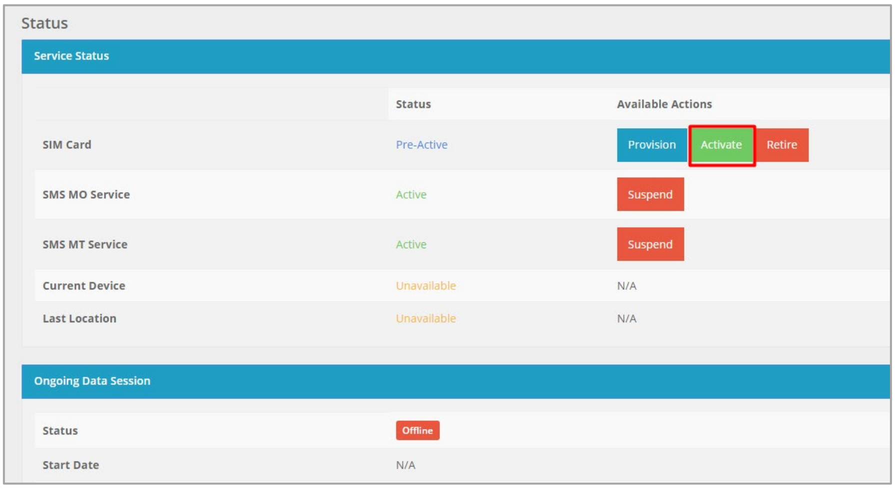
Online activation for you and your customers.

Our state-of-the-art SIM technology lets you connect from the moment you switch a device on. No complicated activation process, no wordy manuals—just instant connectivity from the touch of a button.

Figure 9. Activating the SIM card

2. Create a new Truphone Account by selecting **Sign up** (next to **Don't have an account yet?**) and filling in your full name, email, and password. Then click **Sign up** to create a new account.
3. After signing up, on the welcome page, Select **Personal** as the account type.
4. Select **Get Started**.
5. Verify your email by entering the activation code sent to your email account (Note: check your Junk folder if the email is not received in your Inbox).
6. Complete the **Profile information** form – then select **Create account**.

7. Select **Activate SIMS** to activate your individual SIM by **ICCID** and **PUK** found on the SIM Card packaging. Note: The **ICCID** value can also be obtained from section 2.2 Setting the SIM and Modem Information for Activation. See the **ICCID** value in Figure 8. CAT-M Information**.** Fill in other fields as needed.
8. You can open the page using the link https://account.truphone.com/login and select Home > SIM Cards > ICCID#xxx", and "Activate" the SIM from the status page, as shown in the Figure 10. After activating the SIM, the status changes from Pre-Active to Active.



Status

Service Status

	Status	Available Actions
SIM Card	Pre-Active	Provision Activate Retire
SMS MO Service	Active	Suspend
SMS MT Service	Active	Suspend
Current Device	Unavailable	N/A
Last Location	Unavailable	N/A

Ongoing Data Session

Status	Offline
Start Date	N/A

Figure 10. Activating the SIM card

9. Ensure the SIM card is inserted in the GM02S PMOD. From the Console **Main Menu 5 Validate SIM activation** to verify that the SIM card is activated.
   Note: The SIM card should be activated on the Truphone SIM Activation platform after 15 minutes and can be validated on the Tera Term terminal, as shown in Figure 11. The time for the SIM Card to be activated by Truphone can vary depending on their system demand. In most cases, if PING Response fails, wait a few more minutes and repeat **Menu 5 Validate SIM activation.**

Disclaimer

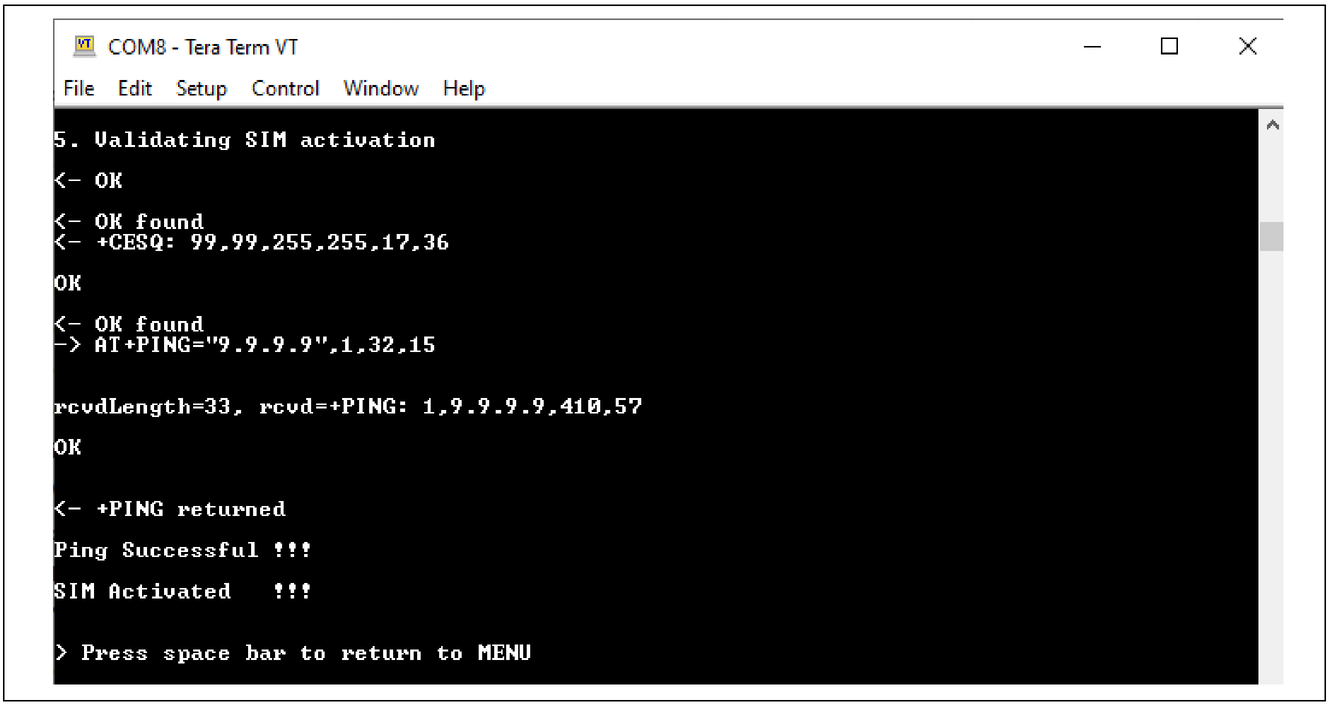
The activation steps above are provided by SIM Provider Truphone. They are the most current at the time of publishing this application note. If you need help activating your SIM Card, contact Truphone support iot.truphone.com or Contact Support | Truphone.

If you have a SIM card from any other provider, 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 Application 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 GM02S not connecting to the Cellular network.

To set the Access Point Name (APN) for SIM Card providers other than Truphone, the APN is set in the Application project in `/src/cellular_setup.c`
See `#define CELLULAR_APN "iot.truphone.com"    /* APN : Truphone SIM Card */`

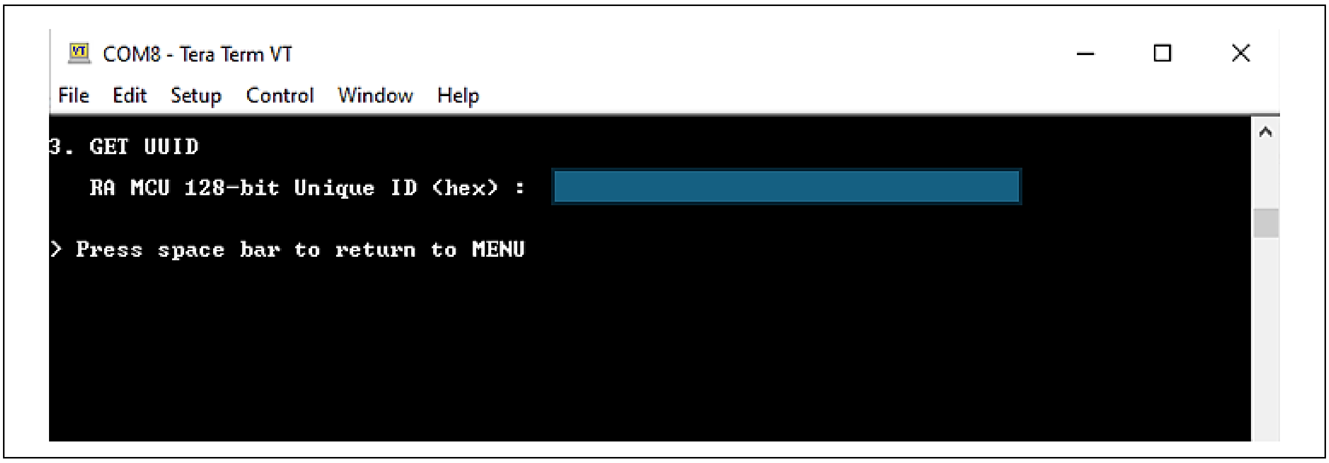


```
5. Validating SIM activation
<- OK
<- OK found
<- +CESQ: 99,99,255,255,17,36
OK
<- OK found
-> AT+PING="9.9.9.9",1,32,15

rcvdLength=33, rcvd=+PING: 1,9.9.9.9,410,57
OK

<- +PING returned
Ping Successful !!!
SIM Activated   !!!

> Press space bar to return to MENU
```

Figure 11. Validating SIM Activation – SIM Card Active

2.4 Getting the UUID Information of the Board

1. Press **3** from the **Main Menu** to display the board UUID. This command obtains the UUID information of the board and displays it on the console, as shown in the screenshot below. You will need this information to register for the Renesas AWS Cloud Dashboard.



```
3. GET UUID
   RA MCU 128-bit Unique ID (hex) : [redacted]

> Press space bar to return to MENU
```

Figure 12. Getting Board UUID Information

2.5 Registering for the Renesas AWS Cloud Dashboard

AWS dashboard for Renesas CK-RA6M5 v2 cloud kit is custom-designed to visualize the data of all the sensors on the cloud kits. The dashboard connects to AWS IoT services through AWS IoT Core and enables users to utilize the cloud services to their full potential.

To allow users to experience a hassle-free first experience with the cloud kits, every cloud kit is credited with USD 10 AWS credits upon registration.

The dashboard can be accessed at https://renesas.cloud-ra-rx.com/

2.5.1 Sign up

After establishing access to the RA and RX kit to the kit-associated AWS sub-account, where all necessary infrastructure will be provisioned, each user should sign up. If you have signed up earlier and registered the device with a UUID, you can skip and go to section 2.5.2 Sign in:

1. Go to the https://renesas.cloud-ra-rx.com/
2. If you don't have an account, click on the **Sign up** button. You are directed to the **Sign up** page.

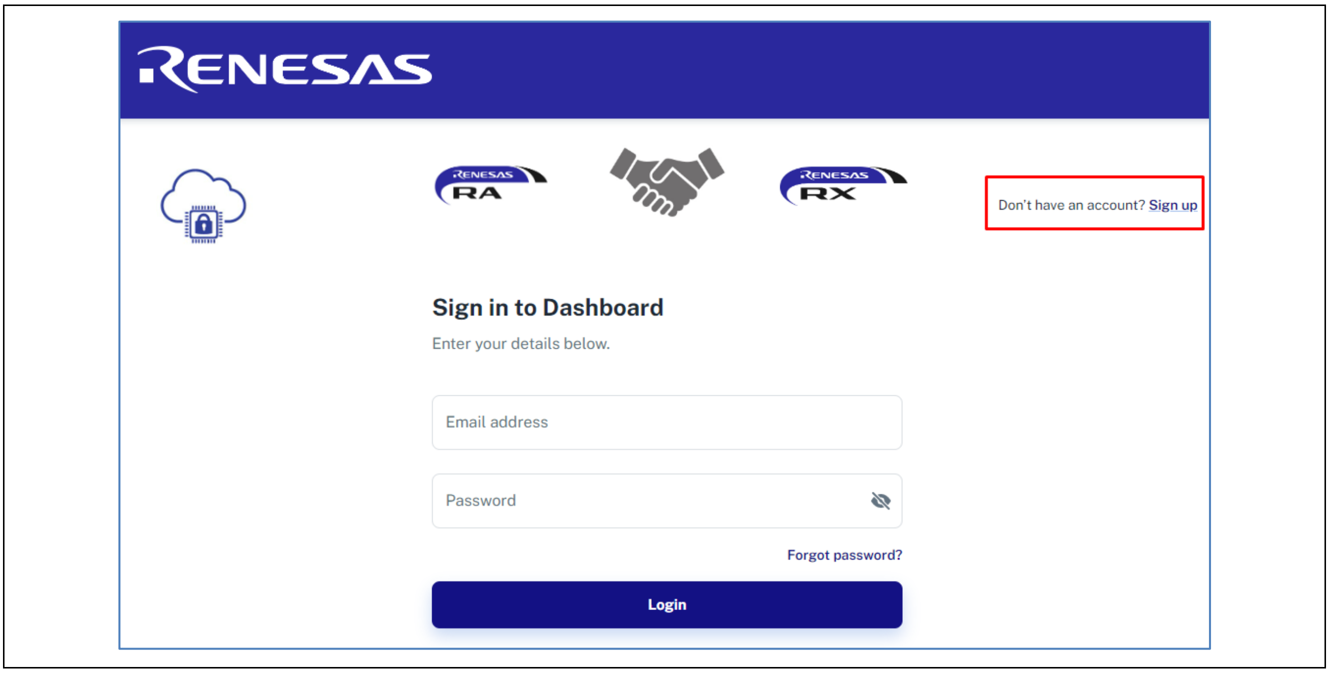


Figure 13. Creating Account

3. Enter your first name, last name, email address and password and click **Register**.

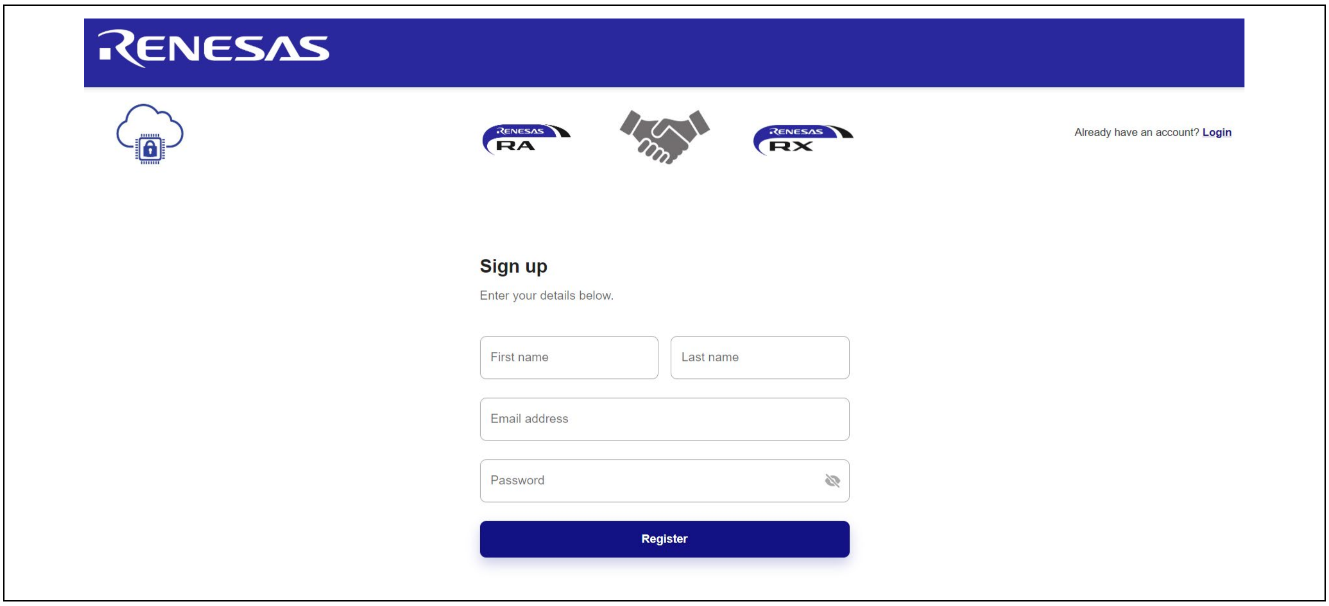


Figure 14. Registering Information

The rules for a valid first name and last name:

- Length Constraints: Minimum length of 2. Maximum length of 24.
- Information must be entered in English or another Latin character-based language.

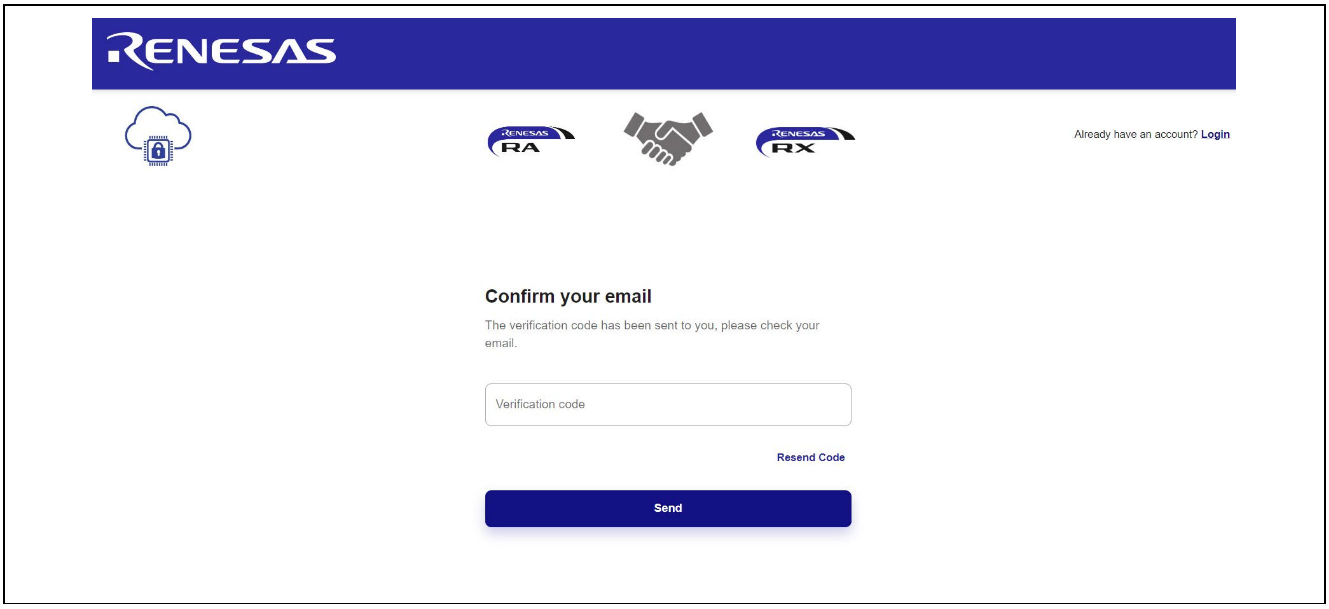
The rules for a valid email address:

- The address must be a minimum of 6 and a maximum of 64 characters long.
- Use the email address that has not been used previously for signup.
- All characters must be 7-bit ASCII characters.
- There must be one and only one @ symbol, which separates the local name from the domain name.
- The local name cannot contain any of the following characters: whitespace, " ' () < > [ ] : ; , \ | % &
- The local name cannot begin with a dot (.)
- The local name cannot contain double Plus, for example: account+rnss+alpha@domain.com
- The domain name can consist of only the characters [a-z],[A-Z],[0-9], hyphen (-), or dot (.)
- The domain name cannot begin or end with a hyphen (-) or dot (.)
- The domain name must contain at least one dot.

The rules for a valid password:

- The password must be a minimum of 8 and a maximum of 64 characters long.
- Password must contain at least one uppercase character, one lowercase character, one number, and one special character: ! # $ % & * ? @.

4. Verification code will be sent to your email. Enter the code and press the **Send** button. You are redirected to the **Register Device** page.



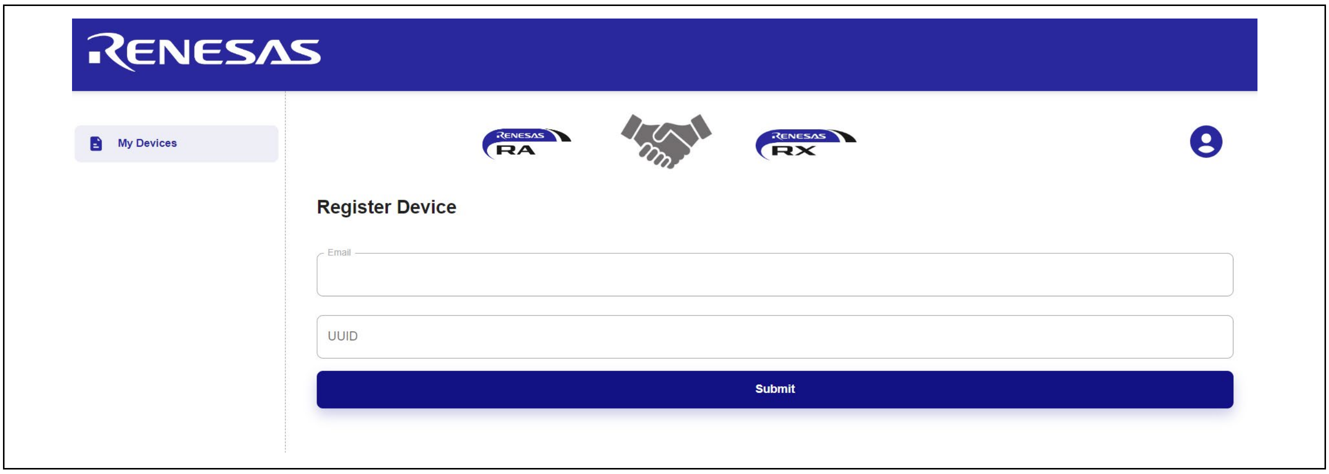
Confirm your email

The verification code has been sent to you, please check your email.

Figure 15. Confirming Email

If you do not receive an email with the code, please click on **Resend Code**.

5. Enter the UUID of the kit to complete the registration process. UUID is the unique ID of your board. Refer to “CK-RA6M5 v2 AWS Application Project” for steps for obtaining the UUID of the kit.
   Note: Only 1 device will be assigned to an account.



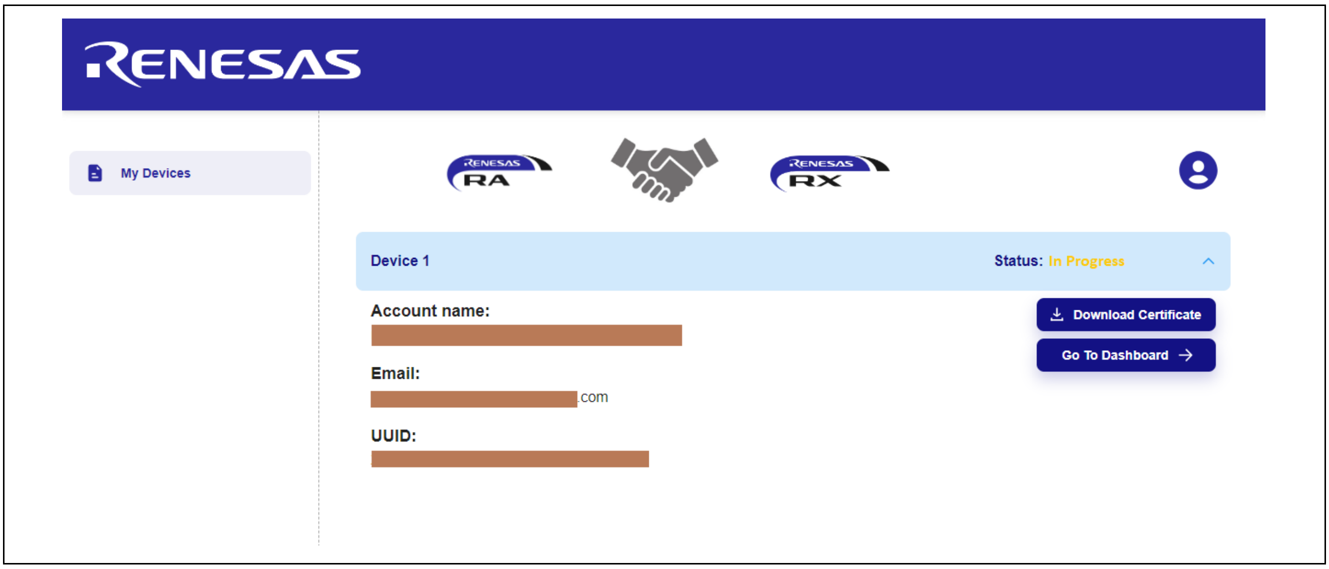
Register Device

Email

UUID

Figure 16. Registering Device

6. The registration page indicates that the device registration is in progress.



Device 1 Status: In Progress

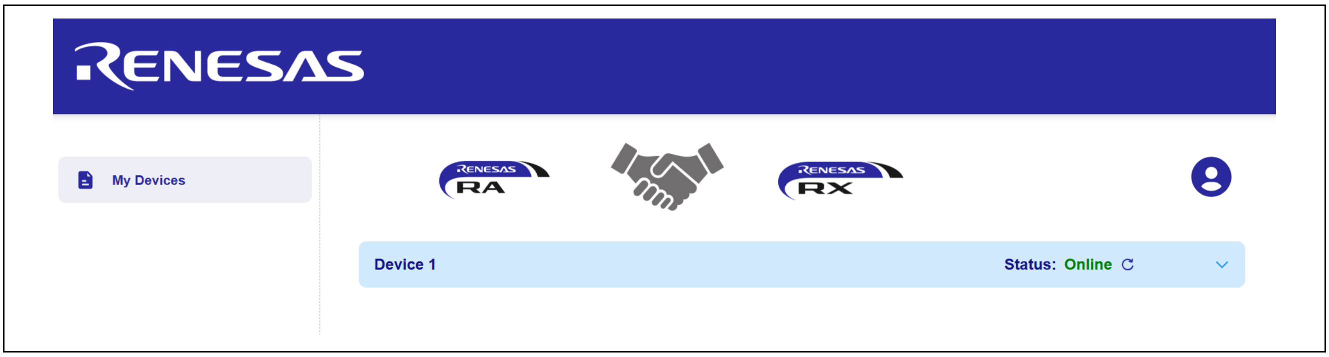
Account name:
[redacted]

Email:
[redacted].com

UUID:
[redacted]

Figure 17. Device Registration in Progress

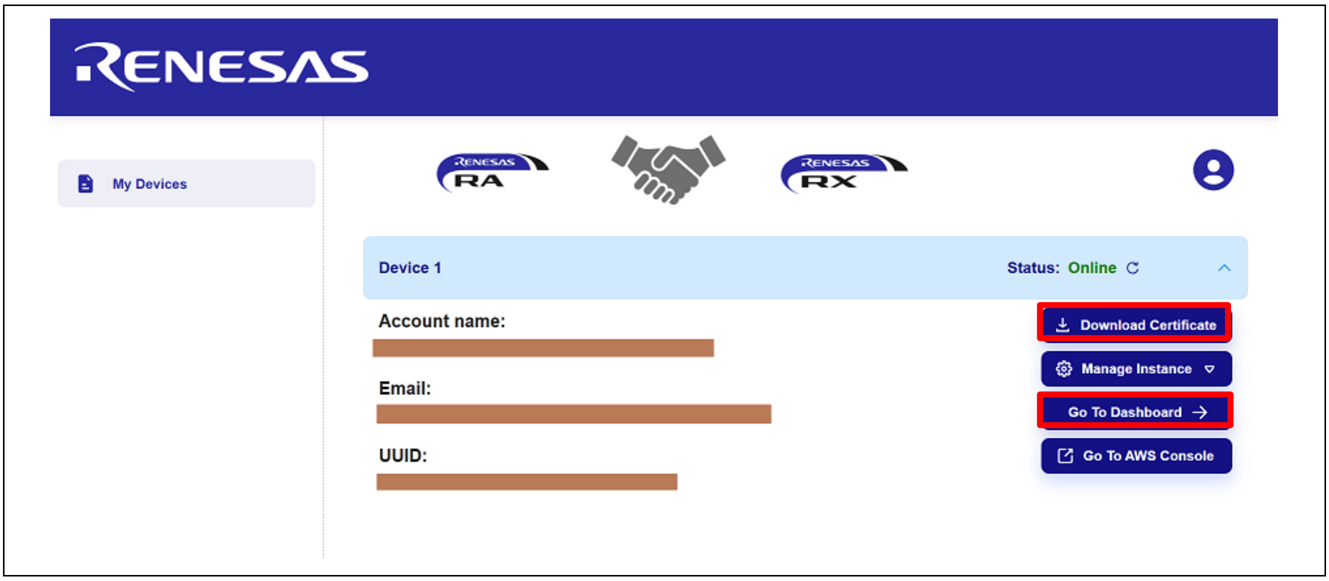
7. After the sub-account is registered, it is provisioned. The status of the registration changes to ‘Online’.



Device 1 Status: Online

Figure 18. Sub-Account Registration

8. Refresh the page and wait for the buttons **Download Certificate** and **Go To Dashboard** to become available on the registration page. This process may take up to **1 hour** for device provisioning to complete.



Device 1 Status: Online

Account name: [redacted]

Email: [redacted]

UUID: [redacted]

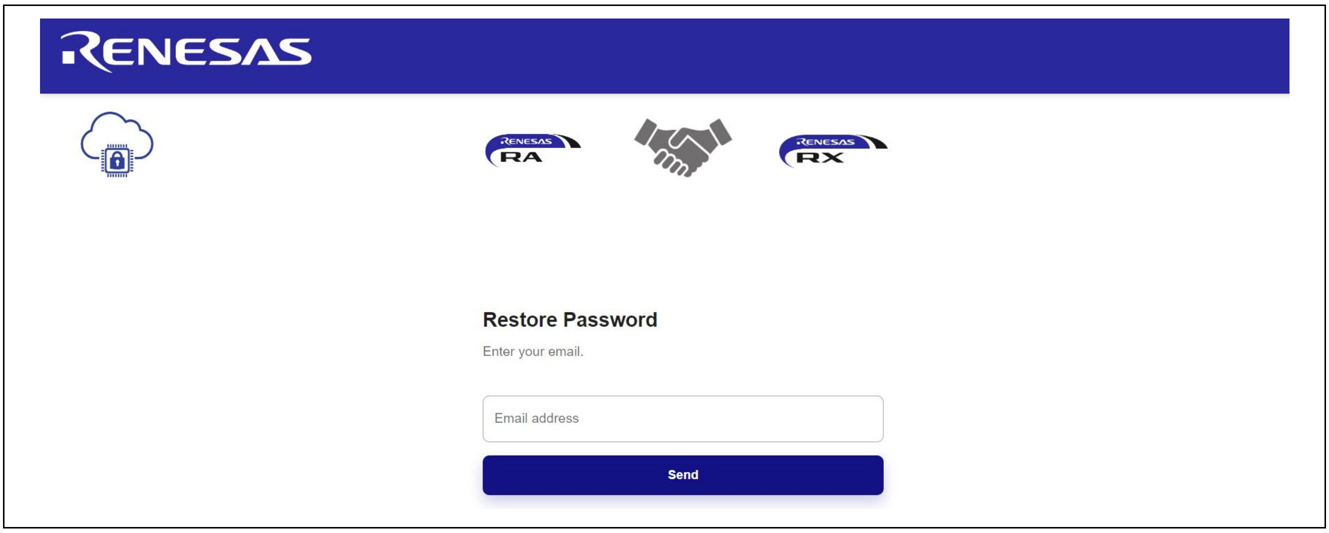
Figure 19. Completing Device Provisioning

2.5.2 Sign in

If you have already registered on our web portal, you need to sign in and enter your email and password.

2.5.3 Forgot Password

1. Click **Forgot password** on the **Sign in to the Dashboard** page. You are directed to the **Restore Password** page.



Restore Password

Enter your email.

Figure 20. Restoring Password 1

2. Enter your email and click on the button **Send**.

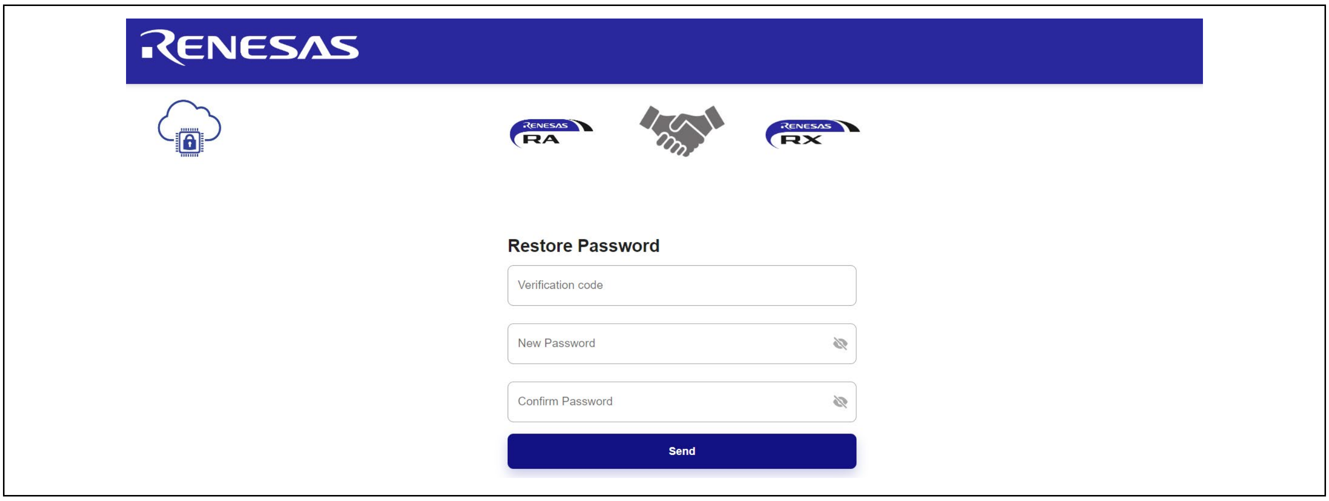
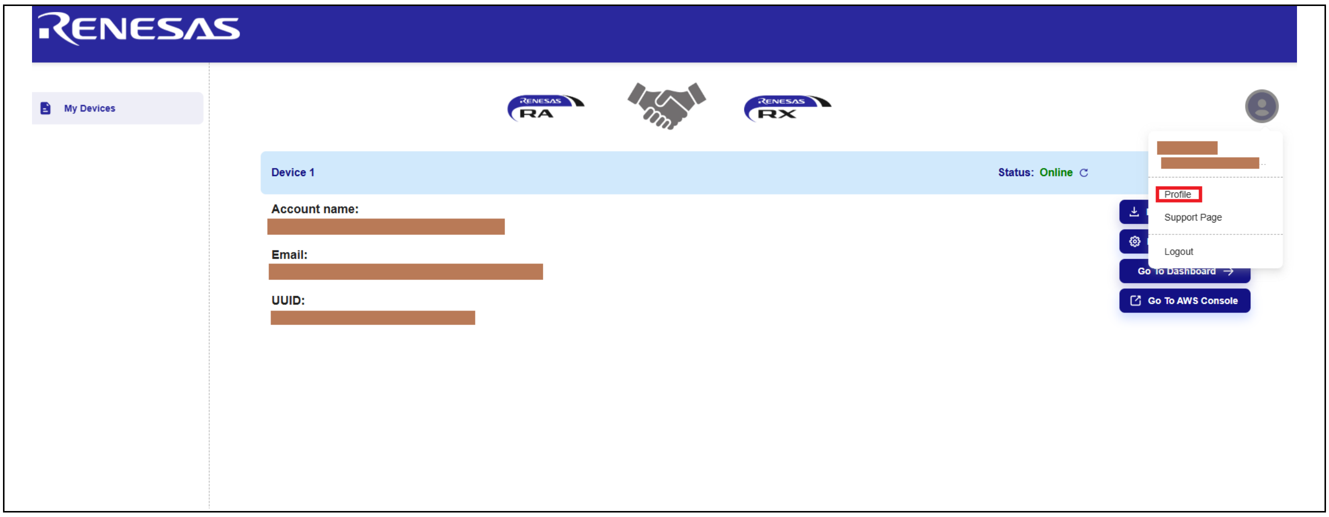


Figure 21. Restoring Password 2

3. You should receive a verification code in your email.
4. Enter the code and your new password and confirm it.
5. To end the process, press the button **Send**.

2.5.4 Profile page

To see your profile page:
Click on your profile picture on the top right. Select Profile.



[redacted]

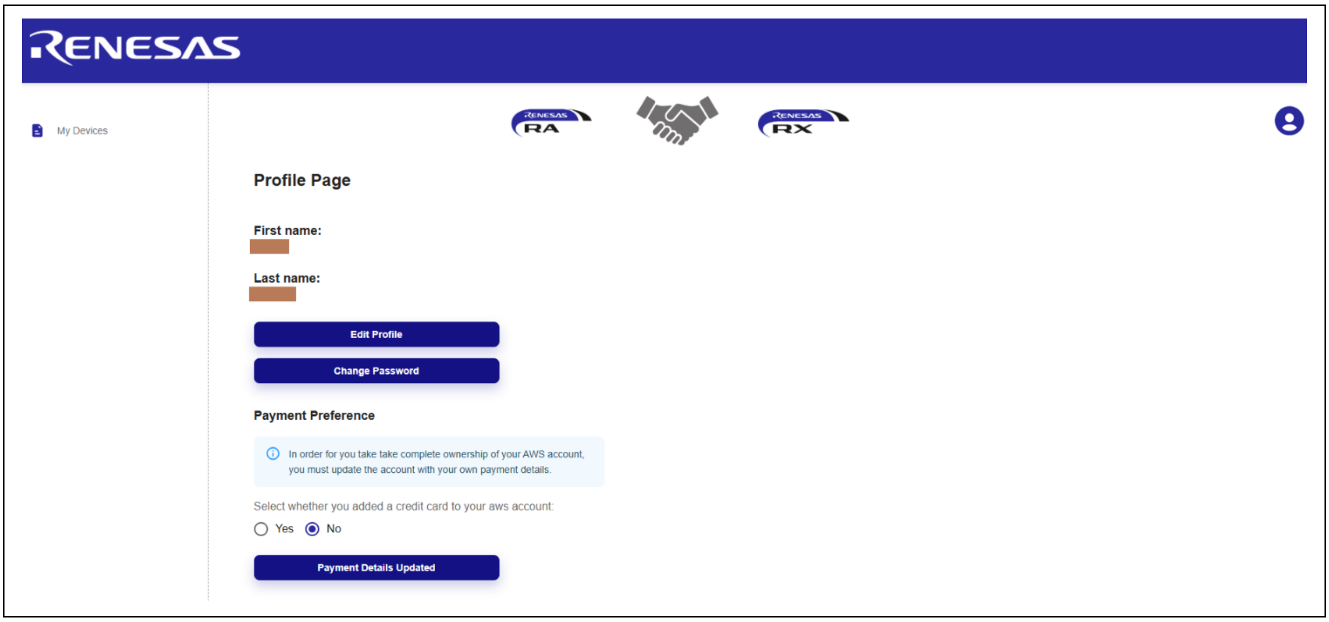
Account name: [redacted]

Email: [redacted]

UUID: [redacted]

Figure 22. Selecting Profile

You are redirected to the Profile page:



My Devices

Profile Page

First name:

[redacted]

Last name:

[redacted]

Payment Preference

In order for you take take complete ownership of your AWS account, you must update the account with your own payment details.

Select whether you added a credit card to your aws account:

○ Yes ● No

Figure 23. Profile Page

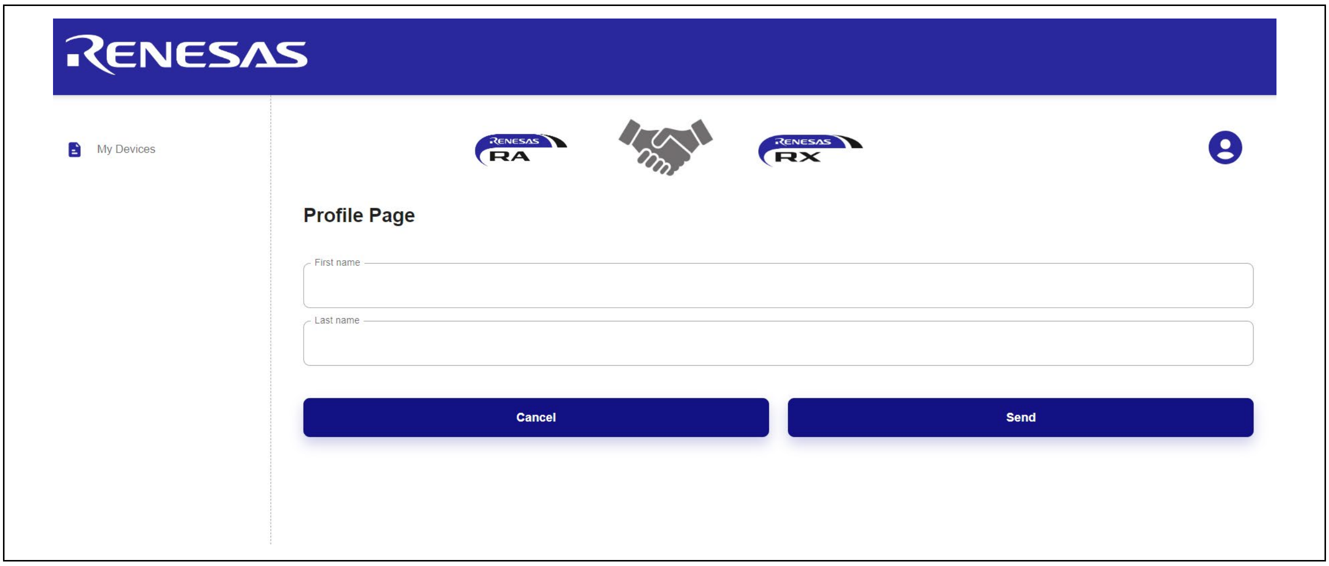
On the page, you can edit your profile:

A. Click on Edit Profile.

B. Change your first and last name.

C. Click on Send.

D. Your Account Name is updated.



My Devices

Profile Page

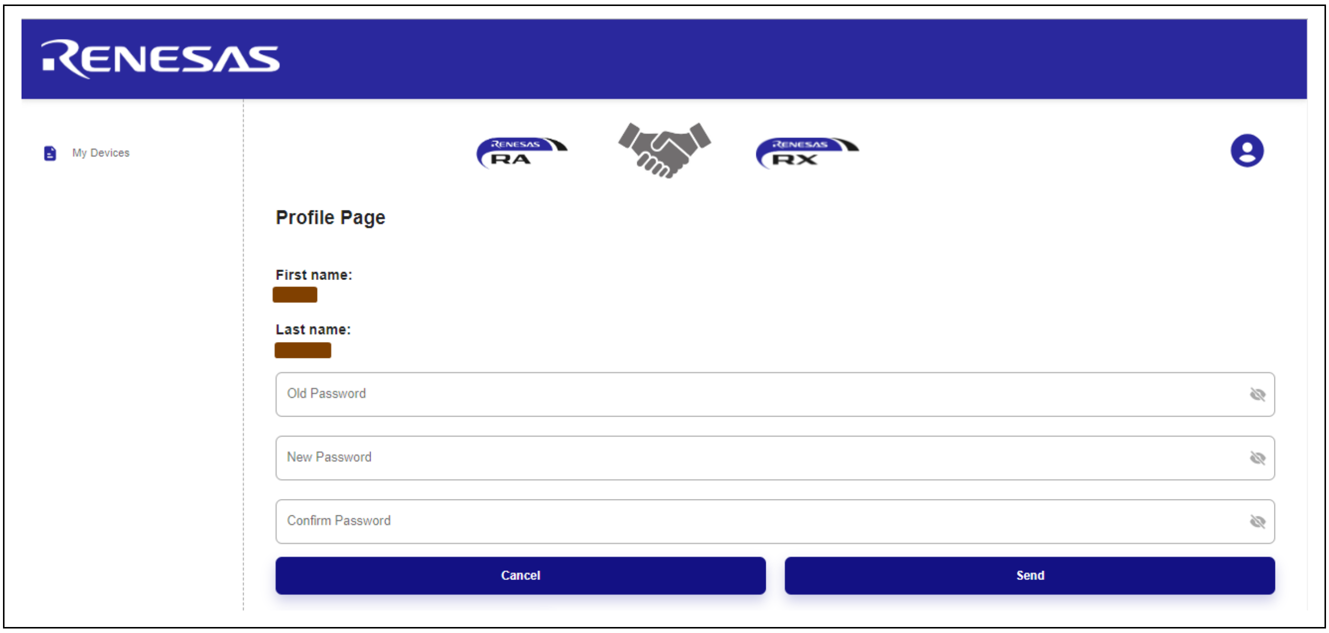
First name

Last name

Figure 24. Updated Profile Page

Also, you can change your password; the rules for a valid password have been mentioned above:

A. Click on Change Password.
B. Enter your Old Password.
C. Enter your New Password.
D. Confirm your New Password and press the button Send.
E. Your password is updated.



Profile Page

First name:
[redacted]

Last name:
[redacted]

Old Password

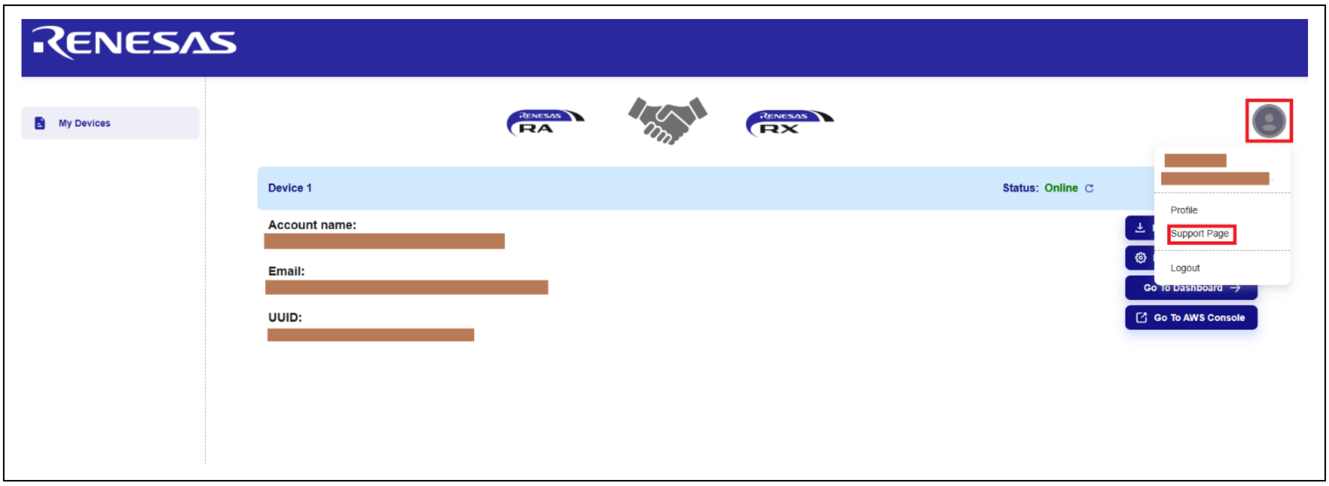
New Password

Confirm Password

Figure 25. Changing Password on Profile Page

2.5.5 Support Page

To see your support page:
Click on your profile picture on the top right. Select the **Support page**.



Device 1 Status: Online

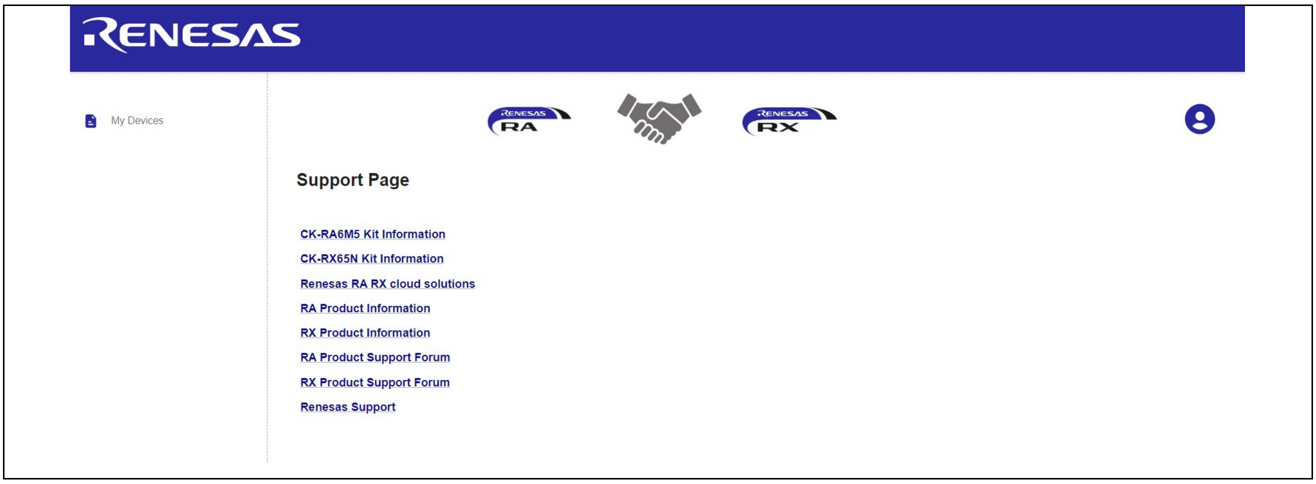
Account name:
[redacted]

Email:
[redacted]

UUID:
[redacted]

[redacted]

Figure 26. Selecting Support Page



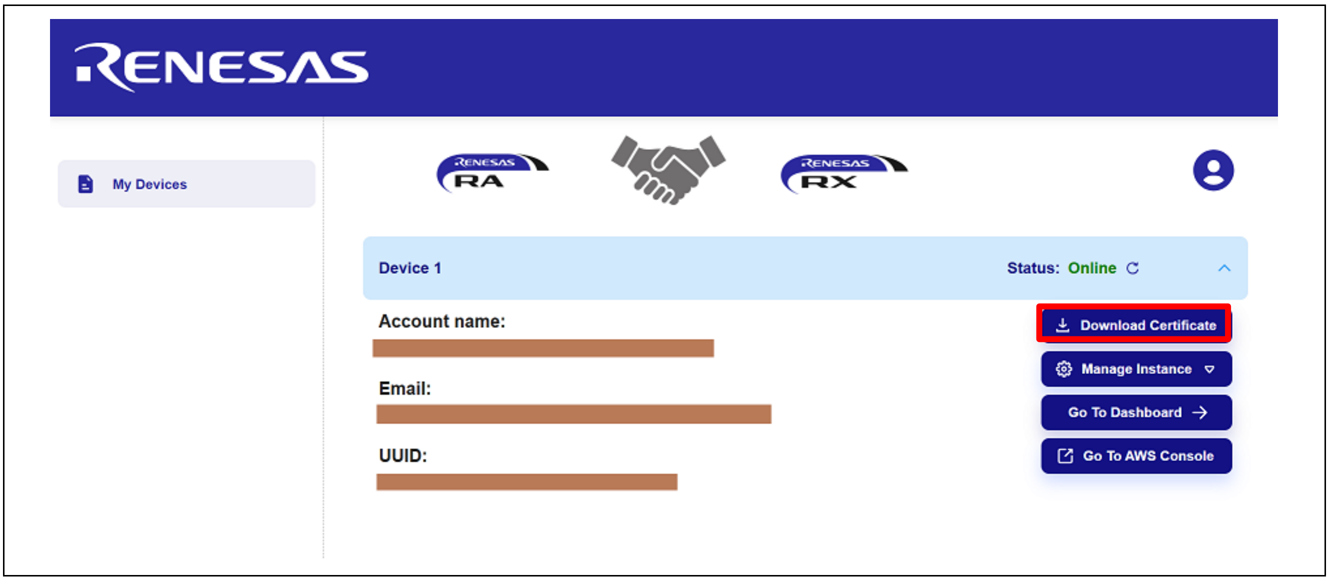
Support Page

CK-RA6M5 Kit Information
CK-RX65N Kit Information
Renesas RA RX cloud solutions
RA Product Information
RX Product Information
RA Product Support Forum
RX Product Support Forum
Renesas Support

Figure 27. Support Page

2.5.6 Downloading the Certificate

Click on the **Download Certificate** button to download the credentials, **certs.zip** file, and unzip this file.



Device 1 Status: Online

Account name:
[redacted]

Email:
[redacted]

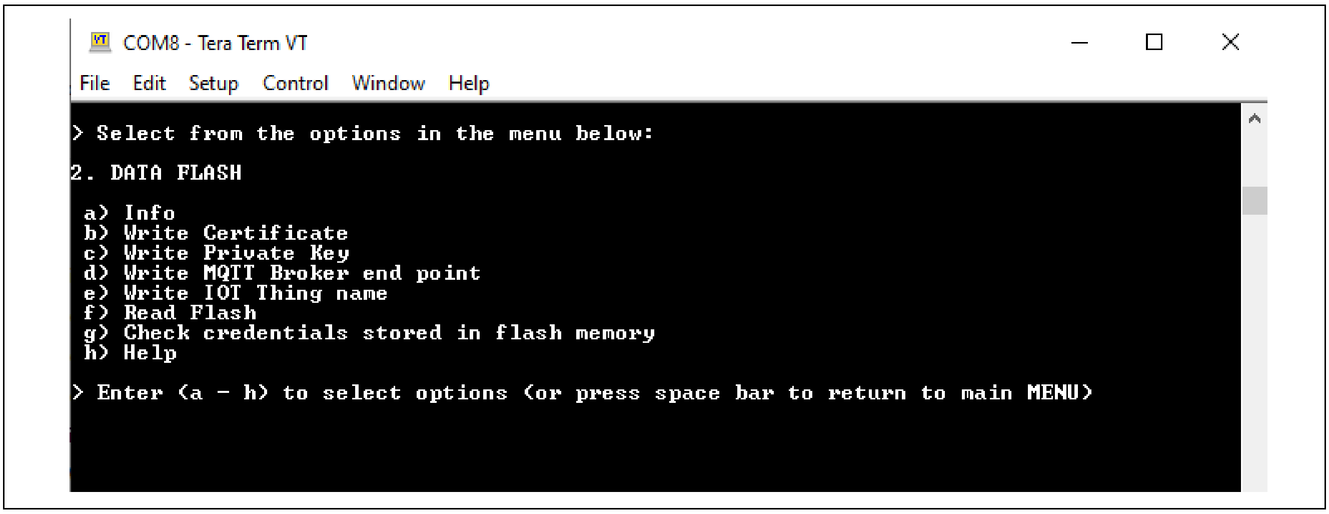
UUID:
[redacted]

Figure 28. Downloading the Certificate

2.6 Storing the Device Certificate, Key, MQTT Broker Endpoint, and IoT Thing Name

For the application to work, the Device Certificate, Device Private Key, MQTT Broker Endpoint, and IOT Thing name need to be stored in the data flash.

1. Press **2** on the **Main Menu** to display **Data Flash-related commands, as shown in the following screenshots. This submenu** has commands to store, read, and validate the data.



```
> Select from the options in the menu below:

2. DATA FLASH

 a) Info
 b) Write Certificate
 c) Write Private Key
 d) Write MQTT Broker end point
 e) Write IOT Thing name
 f) Read Flash
 g) Check credentials stored in flash memory
 h) Help

> Enter (a - h) to select options (or press space bar to return to main MENU)
```

Figure 29. Data Flash-related Menu and Commands

2. 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 device certificate file ‘`xxxxxcertificate.pem.crt`’ from the downloaded `certs.zip` file in section **2.5.6**.

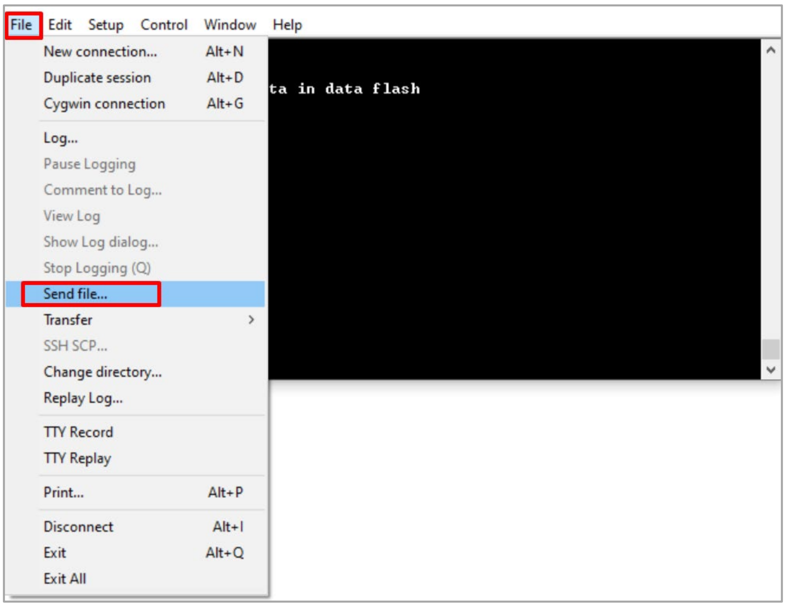
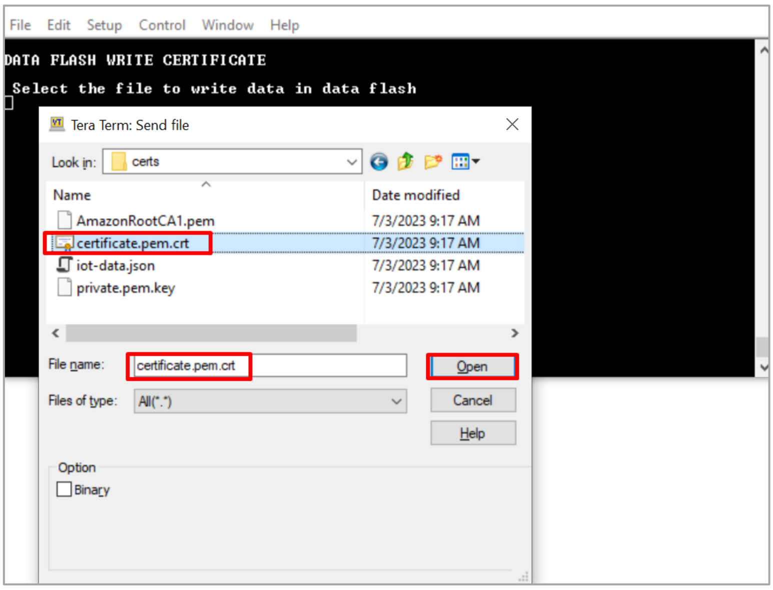


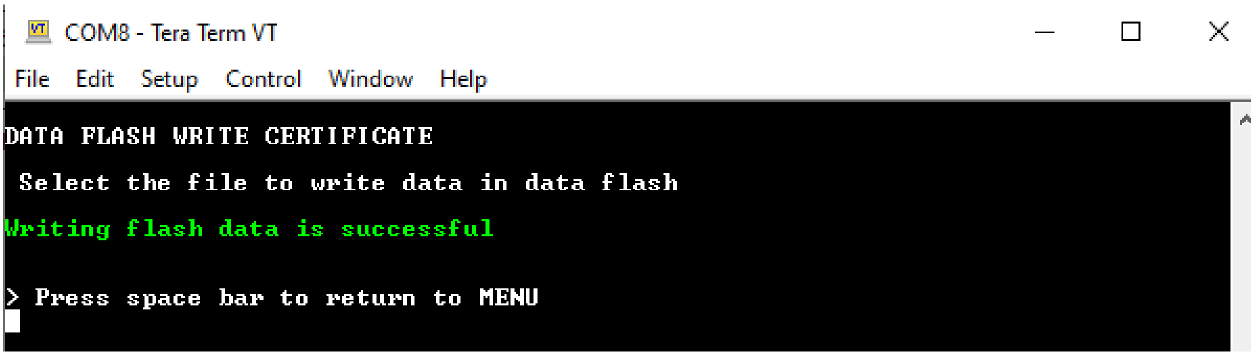
Figure 30. Accessing the Device Certificate



```
DATA FLASH WRITE CERTIFICATE
 Select the file to write data in data flash
```

File Edit Setup Control Window Help
Tera Term: Send file
Look in: certs
Name
Date modified
AmazonRootCA1.pem 7/3/2023 9:17 AM
certificate.pem.crt 7/3/2023 9:17 AM
iot-data.json 7/3/2023 9:17 AM
private.pem.key 7/3/2023 9:17 AM
File name: certificate.pem.crt
Files of type: All(*.*)
Open
Cancel
Help
Option
Binary

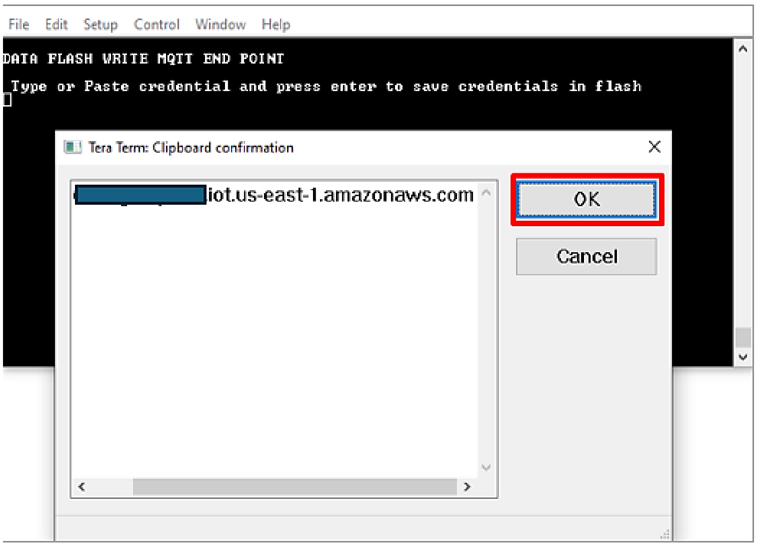
Figure 31. Downloading the Device Certificate into the Data Flash



```
DATA FLASH WRITE CERTIFICATE
 Select the file to write data in data flash
Writing flash data is successful

> Press space bar to return to MENU
```

Figure 32. Status of the Downloaded Device Certificate in the Data Flash

3. To store the **Device Private Key,** press option **c** and click the **File** tab of the Tera Term. Select the **Send File** option and choose the Device Private Key “`xxxxxxxprivate.pem.key`” from the downloaded **certs.zip** file in section **2.5.6**.
4. To store the MQTT Broker end-point, copy the end-point string `xxxxxxxxxx3ku-ats.iot.us-east-1.amazonaws.com` from the **iot-data.json** file in **certs.zip** file. Press option **d** and click the **Edit** tab of the Tera Term and **Paste<CR>**. Verify and confirm the valid string and press **OK.**
   Note: Do NOT copy the double quotes when copying the MQTT Broker endpoint.

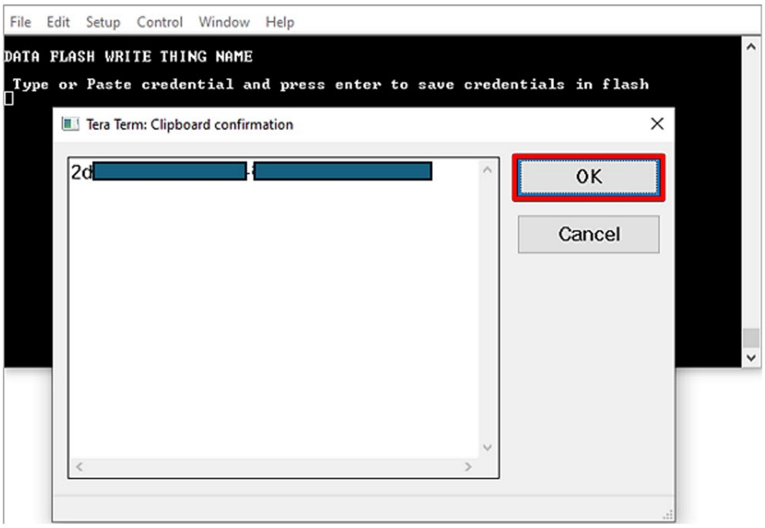

File Edit Setup Control Window Help
Tera Term: Clipboard confirmation
OK
Cancel

```
DATA FLASH WRITE MQTT END POINT
 Type or Paste credential and press enter to save credentials in flash
```

[redacted]iot.us-east-1.amazonaws.com

Figure 33. Storing the MQTT Endpoint into the Data Flash

5. To store the IOT Thing Name, copy the Thing Name string `xxxxxxxx-5736xxxx-xxxxxxxx-4e4bxxxx` from the **iot-data.json** file in **certs.zip** file in section **2.5.6**. Press option **e** and click the **Edit"** tab of the Tera Term and **Paste<CR>**. Verify and confirm the valid string and press **OK.**
   Note: Do NOT copy the double quotes when copying the Thing Name.


File Edit Setup Control Window Help
Tera Term: Clipboard confirmation
OK
Cancel

```
DATA FLASH WRITE THING NAME
 Type or Paste credential and press enter to save credentials in flash
```

2d[redacted]

Figure 34. Storing the MQTT Endpoint in the Data Flash

6. Press options **f** and **g** to read and validate the stored information in the data flash. Press the space bar to go to the previous menu.

   Note: Validation of the stored data is very limited and validates a minimum set of data points. Users are required to input the valid data into the flash obtained from the Dashboard for the application to work properly.

2.7 IoT Cloud Configuration and Connecting to AWS IoT

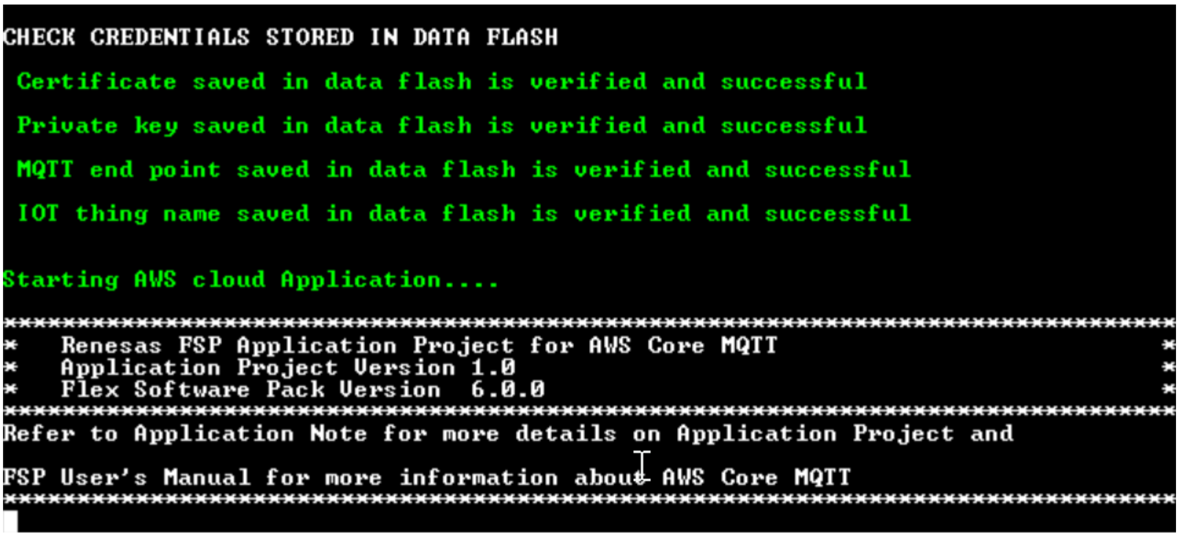
You can sign in to the Renesas AWS dashboard at https://renesas.cloud-ra-rx.com/login using an email account that you previously used to sign up for an AWS account.

Note: It is important to sign up with an email that has not been used previously to open an AWS account since the dashboard creates a new AWS account linked to the email address.

Note: Store the invitation email for the future; it may be required to access the AWS account.

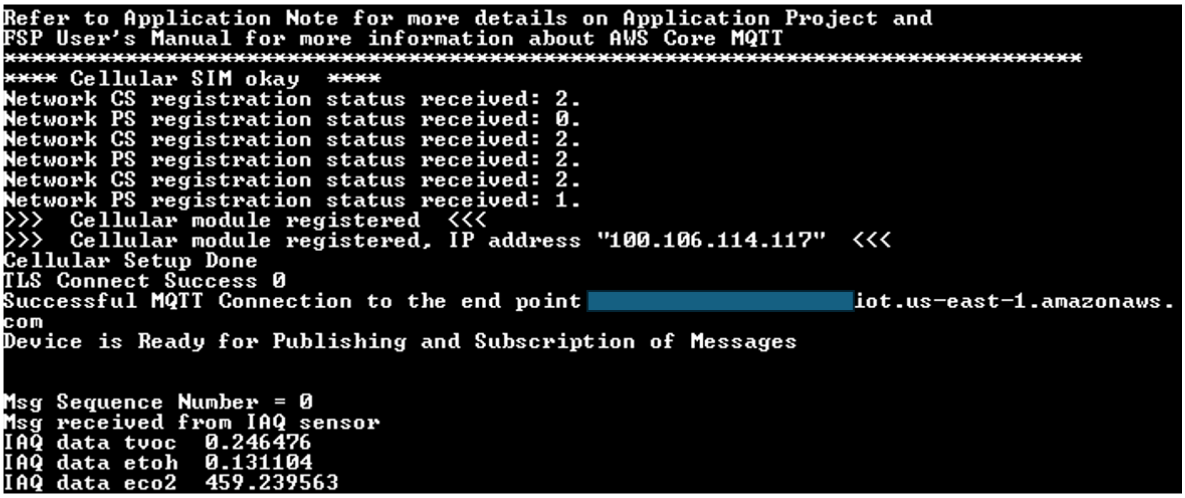
2.8 Starting the Application

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



```
CHECK CREDENTIALS STORED IN DATA FLASH

 Certificate saved in data flash is verified and successful

 Private key saved in data flash is verified and successful

 MQTT end point saved in data flash is verified and successful

 IOT thing name saved in data flash is verified and successful

Starting AWS cloud Application....

*******************************************************************************
*    Renesas FSP Application Project for AWS Core MQTT                        *
*    Application Project Version 1.0                                          *
*    Flex Software Pack Version  6.0.0                                        *
*******************************************************************************
Refer to Application Note for more details on Application Project and

FSP User's Manual for more information about AWS Core MQTT
*******************************************************************************
```

Figure 35. Welcome Screen on the Console



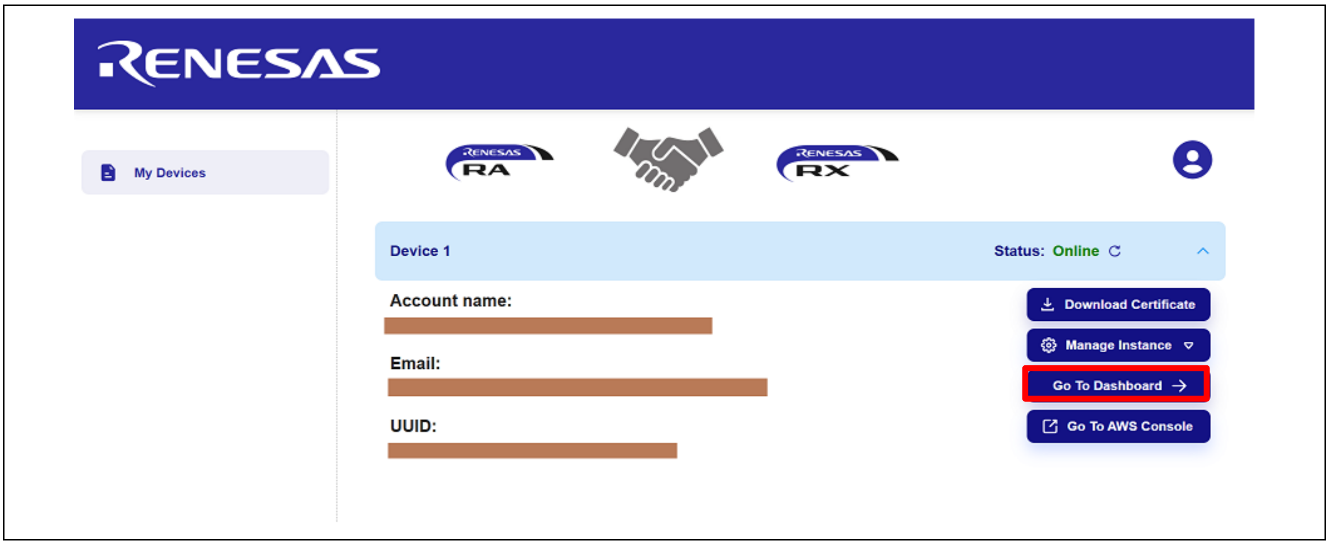
```
Refer to Application Note for more details on Application Project and
FSP User's Manual for more information about AWS Core MQTT
*****************************************************************************
**** Cellular SIM okay  ****
Network CS registration status received: 2.
Network PS registration status received: 0.
Network CS registration status received: 2.
Network PS registration status received: 2.
Network CS registration status received: 2.
Network PS registration status received: 1.
>>>  Cellular module registered  <<<
>>>  Cellular module registered, IP address "100.106.114.117"  <<<
Cellular Setup Done
TLS Connect Success 0
Successful MQTT Connection to the end point [redacted]iot.us-east-1.amazonaws.
com
Device is Ready for Publishing and Subscription of Messages


Msg Sequence Number = 0
Msg received from IAQ sensor
IAQ data tvoc   0.246476
IAQ data etoh   0.131104
IAQ data eco2   459.239563
```

Figure 36. Connecting to the Network and AWS IoT

2.9 Verifying the Application Project from the Renesas Dashboard

Renesas AWS dashboard can be accessed from https://renesas.cloud-ra-rx.com by clicking on **Go to Dashboard**.

Note: Users will have access to the Grafana dashboard only when the device is provisioned and its status is "Online".



Device 1 Status: Online

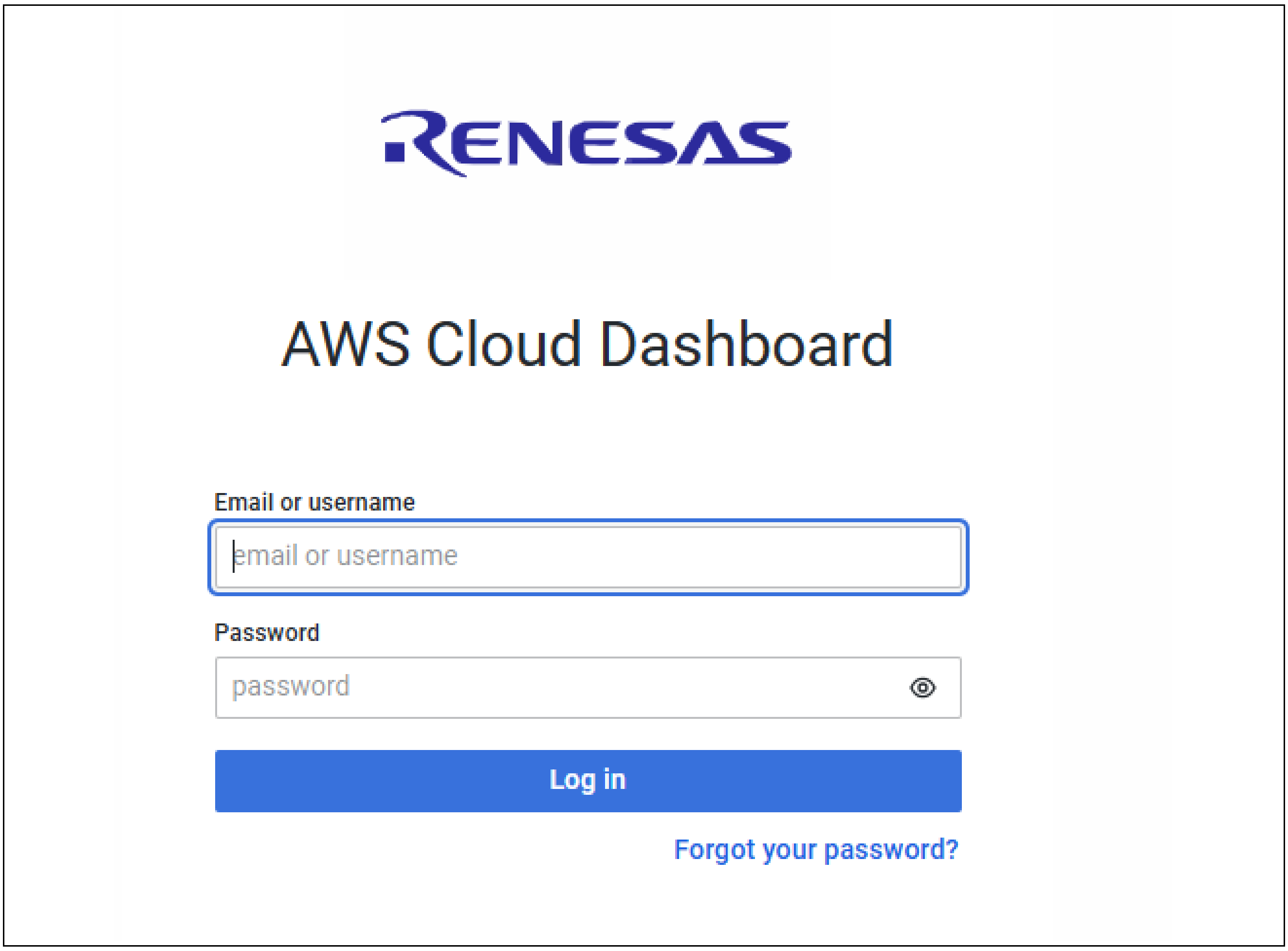
Account name: [redacted]

Email: [redacted]

UUID: [redacted]

Figure 37. Accessing Renesas AWS Cloud Dashboard

First time users will access the dashboard with a default ‘username’ is **admin** and a default ‘password’ is **admin1234**.



AWS Cloud Dashboard

Email or username: email or username

Password: password

Figure 38. Welcome to Grafana Screen

On the Renesas dashboard page, the sensor data can be viewed by clicking on the “arrow” next to each of the sensor data tabs. Allow up to 60 seconds for the data to be displayed on the dashboard. If the data is not updated as expected, refresh the page.

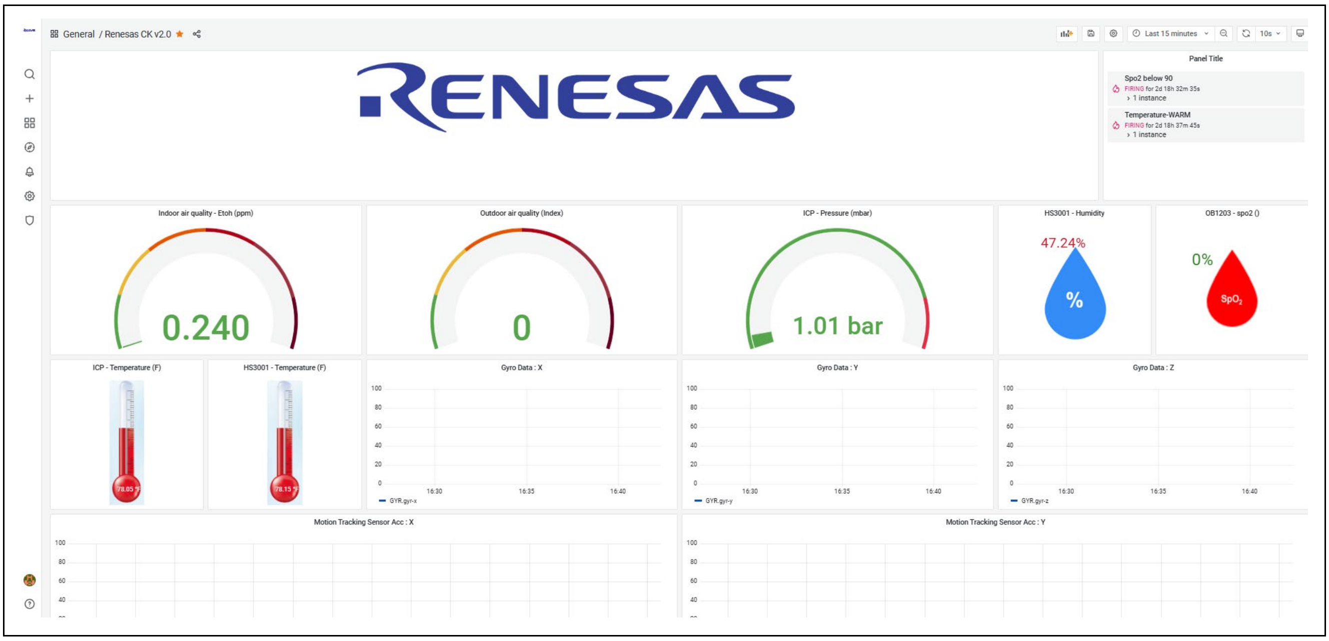
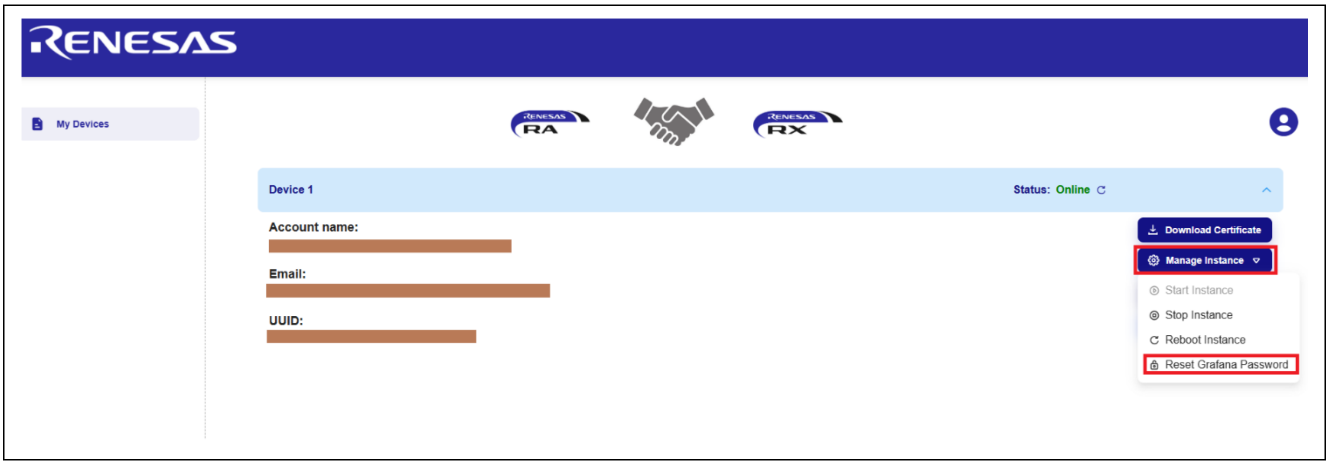


Figure 39. Renesas AWS Cloud Dashboard

To reset the forgotten password, choose ‘Reset Grafana Password’ from the ‘Manage instance’ dropdown menu.



Status: Online

Account name: [redacted]

Email: [redacted]

UUID: [redacted]

Figure 40. Grafana Password Reset

3. Dashboard Types

Depending on the version of the cloud kit being used, you can choose one of the dashboard types: Renesas CK v1.0 or Renesas CK v2.0. **Renesas CK v2.0** is the default; if not, choose Renesas CK v2.0.

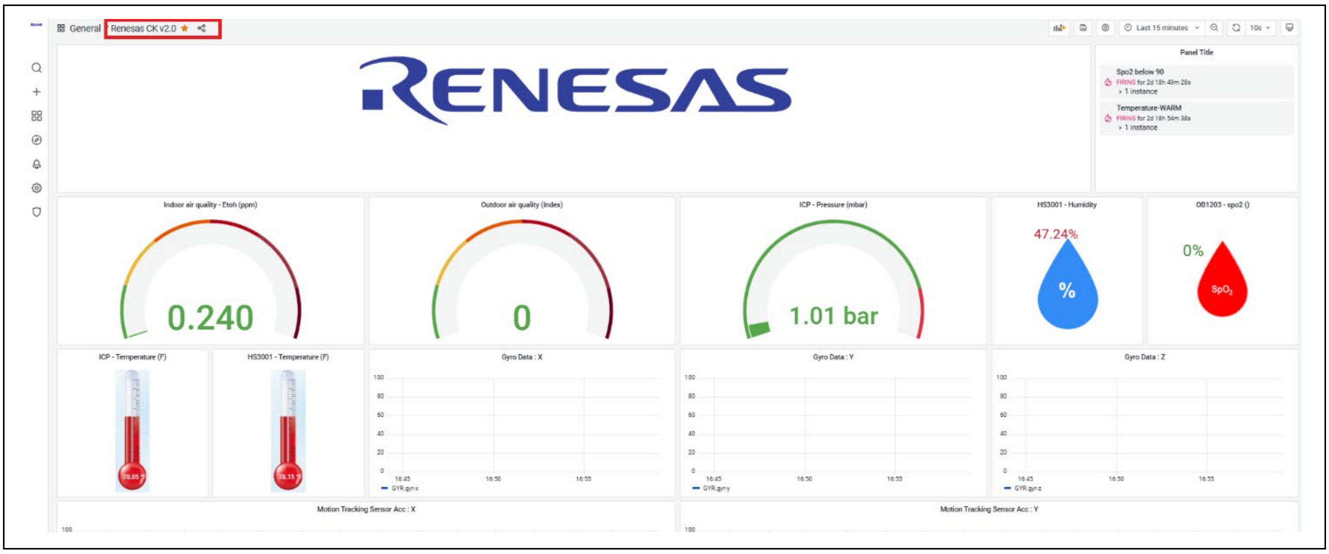
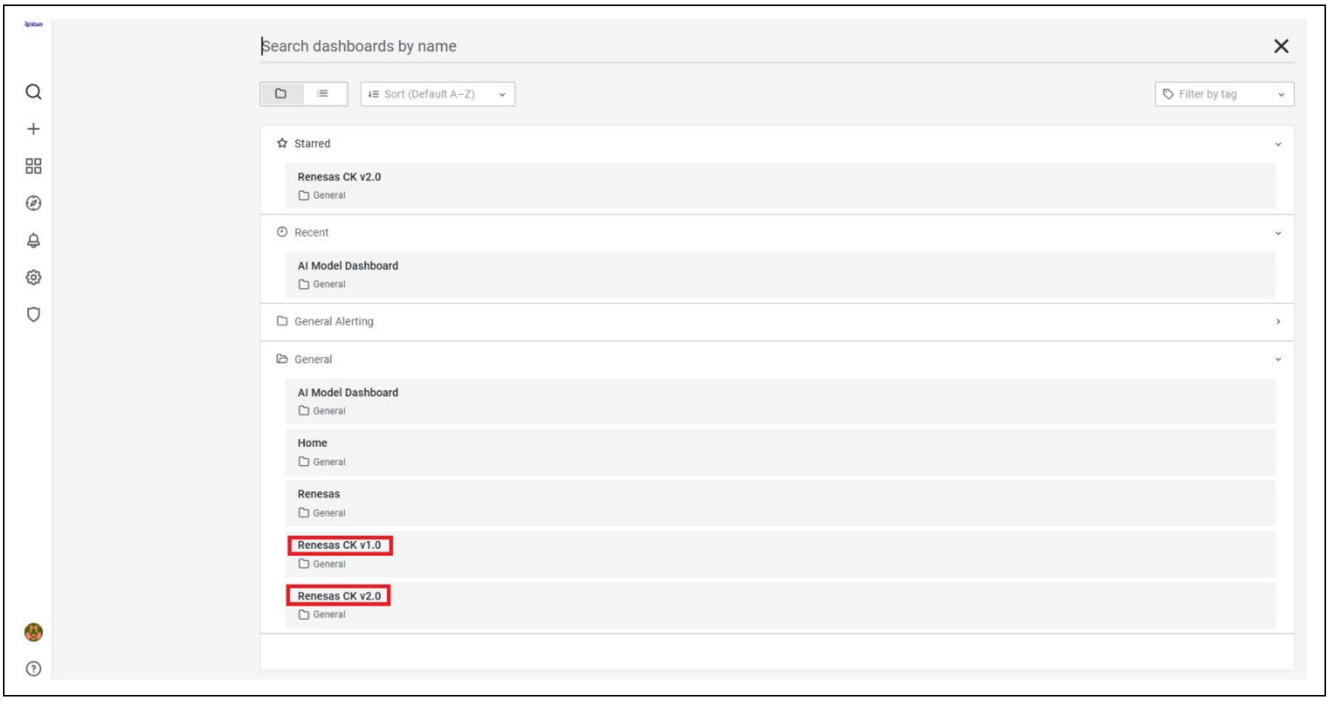


Figure 41. Renesas AWS Cloud Dashboard Types

Choose Renesas CK v2.0.



Search dashboards by name

Sort (Default A–Z)

Filter by tag

Starred
- Renesas CK v2.0 — General

Recent
- AI Model Dashboard — General

General Alerting

General
- AI Model Dashboard — General
- Home — General
- Renesas — General
- Renesas CK v1.0 — General
- Renesas CK v2.0 — General

Figure 42. Choosing Renesas dashboards based on the cloud kit version

CK-RA6M5 v2 only supports 6-Axis sensors (Gyroscope, Accelerometer), and the Magnetometer will always be zero.

4. Sensor Data for Cloud Kits

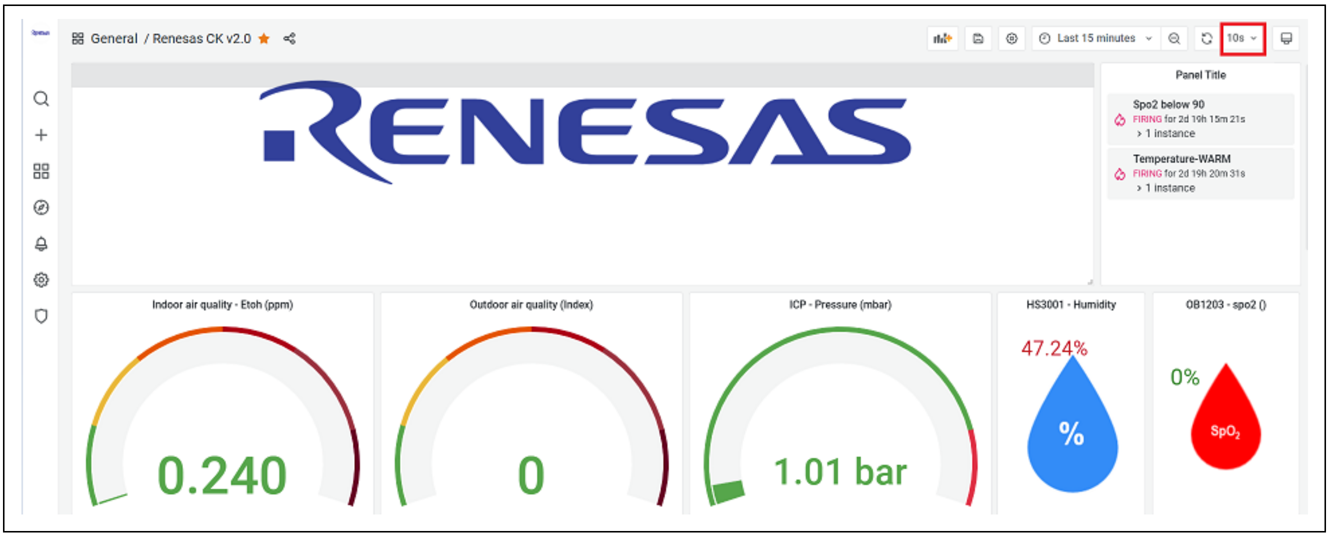
The Grafana dashboard displays the following Data from sensors.

Table 1. Sensor Data from Grafana Dashboard

Sensor	Data
HS3001- Humidity and Temperature Sensor	Temperature, F
	Humidity, %
ZMOD4410- Indoor Air Quality Sensor	Etoh, ppm
	ECO2- Estimated Carbon dioxide, ppm
	TVOC - Total Organic Compounds, mg/m^3
OB1203 - Heart Rate, Blood Oxygen Concentration, Pulse Oximetry, Proximity, Light and Color Sensor	SPO2, %
	HR (Heart Rate), bpm (beats per minute)
	RR (Respiration Rate), breaths per minute
	P2P
ICP-20100 - Barometric Pressure and Temperature Sensor	Temperature, F
	Barometric Pressure, mbar
ICM-42605 Motion Tracking Sensor	Acc values, unit: g
	Gyro Data, unit: dps (degrees per sec)
OAQ – Outdoor Air Quality	OAQ, ppm

5. Dashboard Sensor Updates, Alerts, and Anomaly Detection

Dashboard allows users to choose the ‘refresh rate’ for the incoming updates from the kit. Choose a **10s** refresh rate to allow timely and frequent updates.



General / Renesas CK v2.0

Last 15 minutes

10s

Panel Title

Spo2 below 90
FIRING for 2d 19h 15m 21s
› 1 instance

Temperature-WARM
FIRING for 2d 19h 20m 31s
› 1 instance

Indoor air quality - Etoh (ppm): 0.240

Outdoor air quality (Index): 0

ICP - Pressure (mbar): 1.01 bar

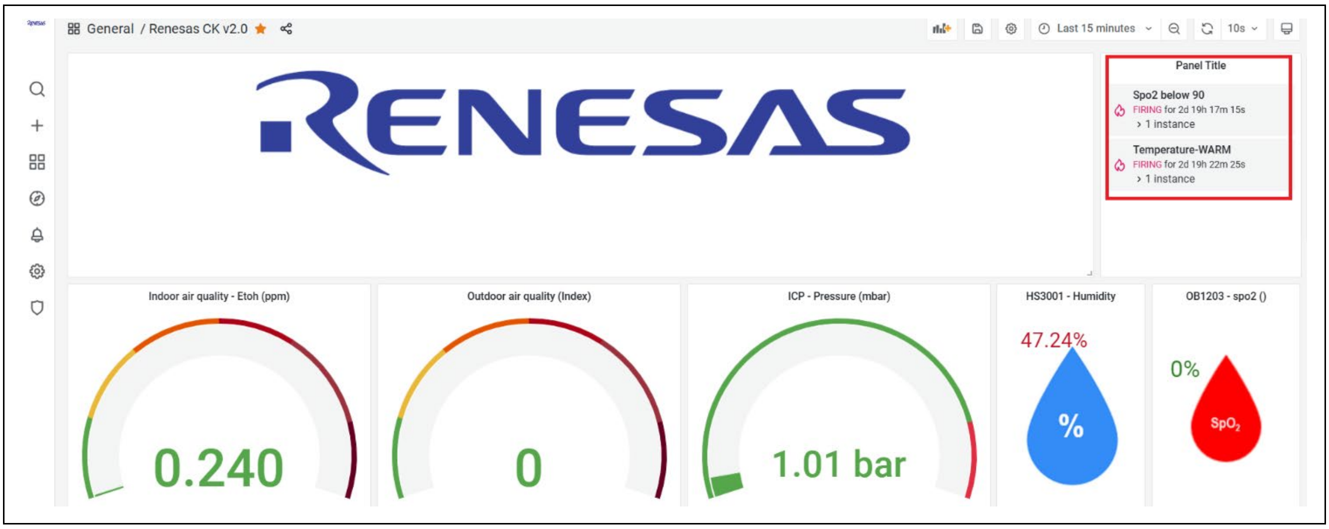
HS3001 - Humidity: 47.24%

OB1203 - spo2 (): 0%

Figure 43. Dashboard Update Refresh Rate

Grafana alerts are a way to send notifications when a metric crosses a threshold that has been configured. By default, the dashboard has thresholds for the following sensors:

- OB1203-SPO2: SPO2 above 90, SPO2 below 90
- HS3001 - Temperature, F:
  - Temperature – Cold: below 65
  - Temperature – Warm: within a range from 65 to 85
  - Temperature – Hot: above 85



Panel Title

Spo2 below 90
FIRING for 2d 19h 17m 15s
› 1 instance

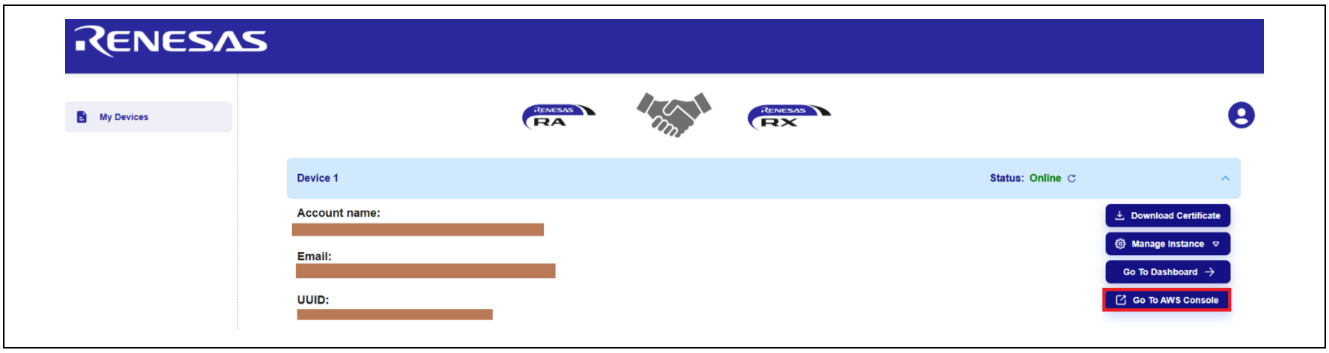
Temperature-WARM
FIRING for 2d 19h 22m 25s
› 1 instance

Figure 44. Sensor Status Feedback

Sensor status feedback is sent to the device, which is indicated by the LEDs.

6. AWS Account and Payment Options

Users can access their AWS account from the dashboard main page by clicking on **Go to AWS Console.**



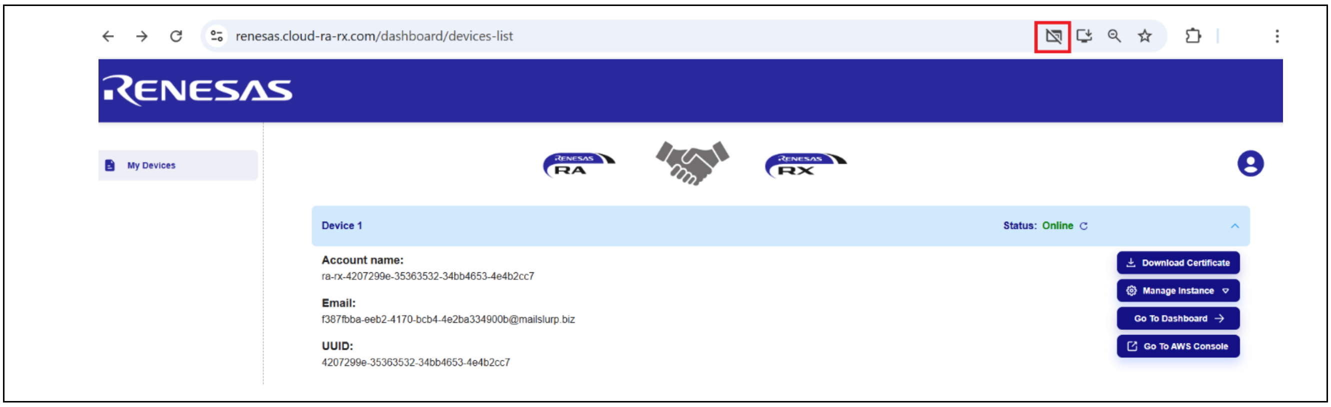
Account name:
[redacted]

Email:
[redacted]

UUID:
[redacted]

Figure 45. Accessing AWS Account from the Dashboard

Make sure to unblock the pop-ups on the browser to allow the AWS console to open.



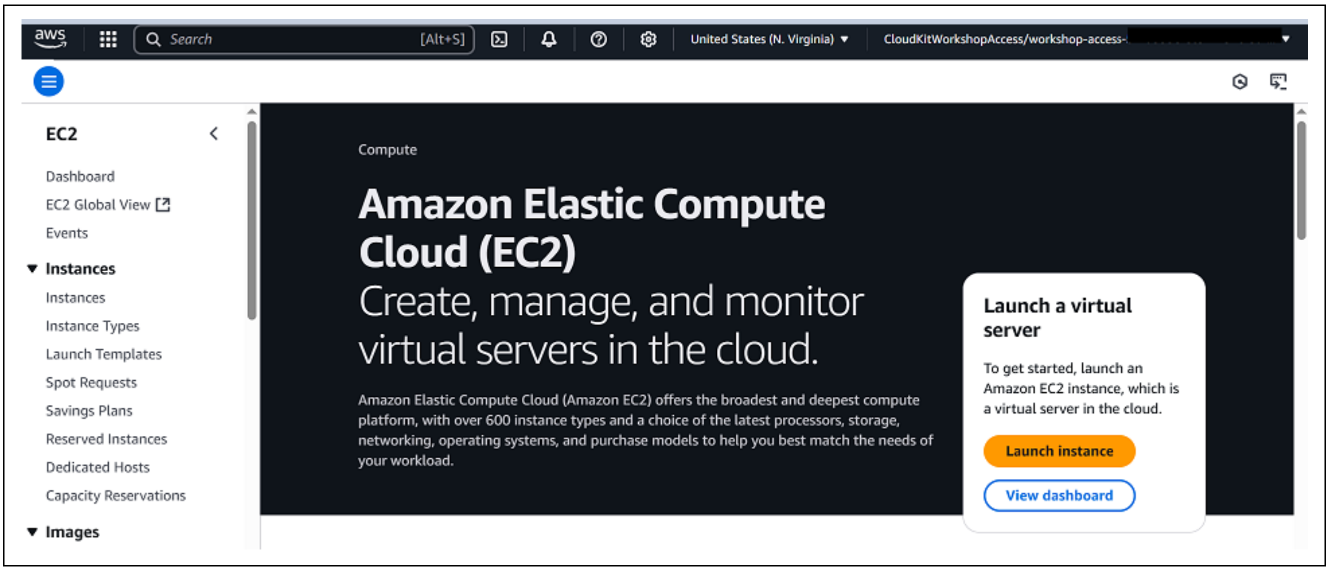
Account name:
ra-rx-4207299e-35363532-34bb4653-4e4b2cc7

Email:
f387fbba-eeb2-4170-bcb4-4e2ba334900b@mailslurp.biz

UUID:
4207299e-35363532-34bb4653-4e4b2cc7

Figure 46. Pop Ups on the browser

1. After logging in, you will be redirected to the AWS access portal page. The AWS sub-account can be accessed from the AWSAdministratorAccess link.



Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Figure 47. AWS account

6.1 Update Payment Options

Note: Payment options must be updated to prevent the account from being quarantined after using $10 AWS credits.

1. Payment options can be accessed from the ‘Billing and Cost Management’ section of the console.

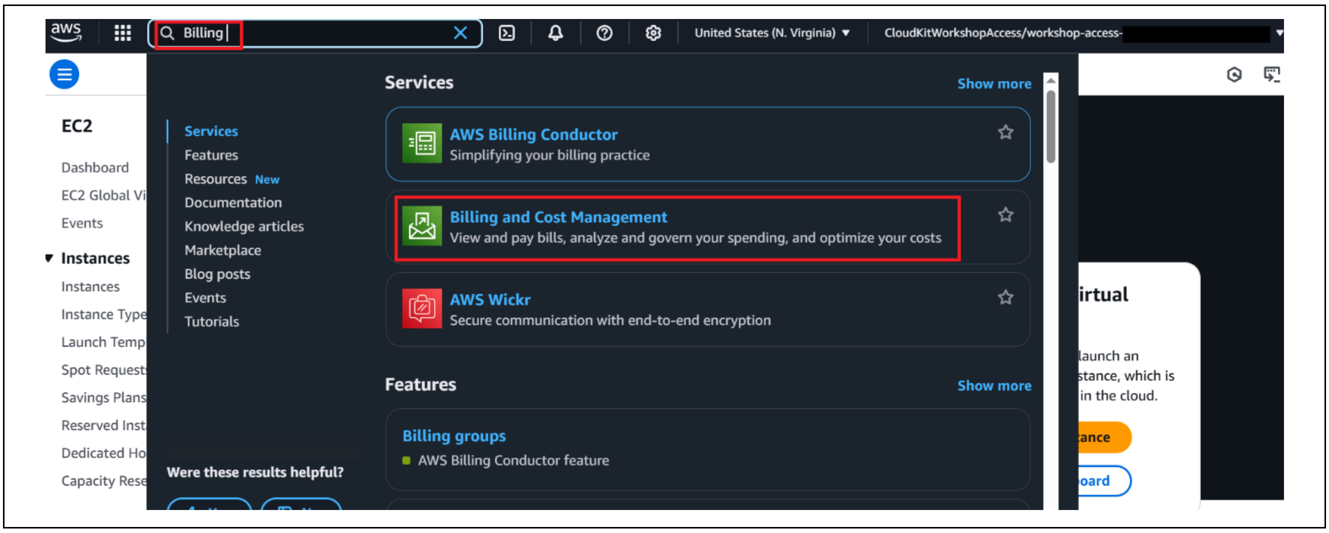
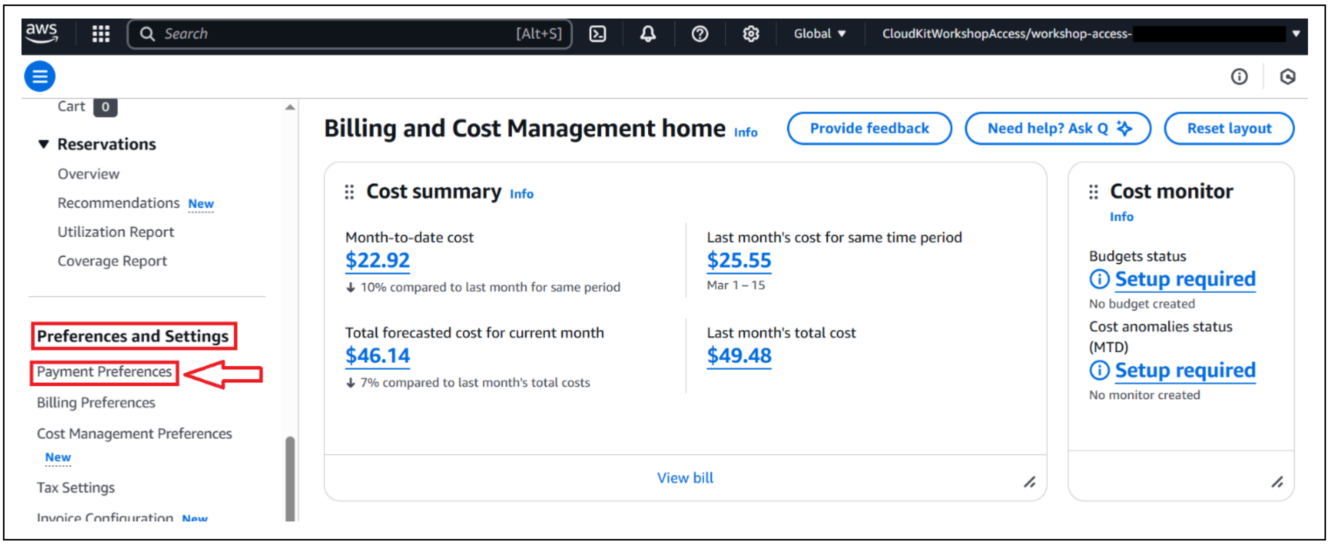


Figure 48. Billing and Cost Management

2. Scroll to the ‘Payment Preferences’



Month-to-date cost
$22.92
↓ 10% compared to last month for same period

Last month's cost for same time period
$25.55
Mar 1 – 15

Total forecasted cost for current month
$46.14
↓ 7% compared to last month's total costs

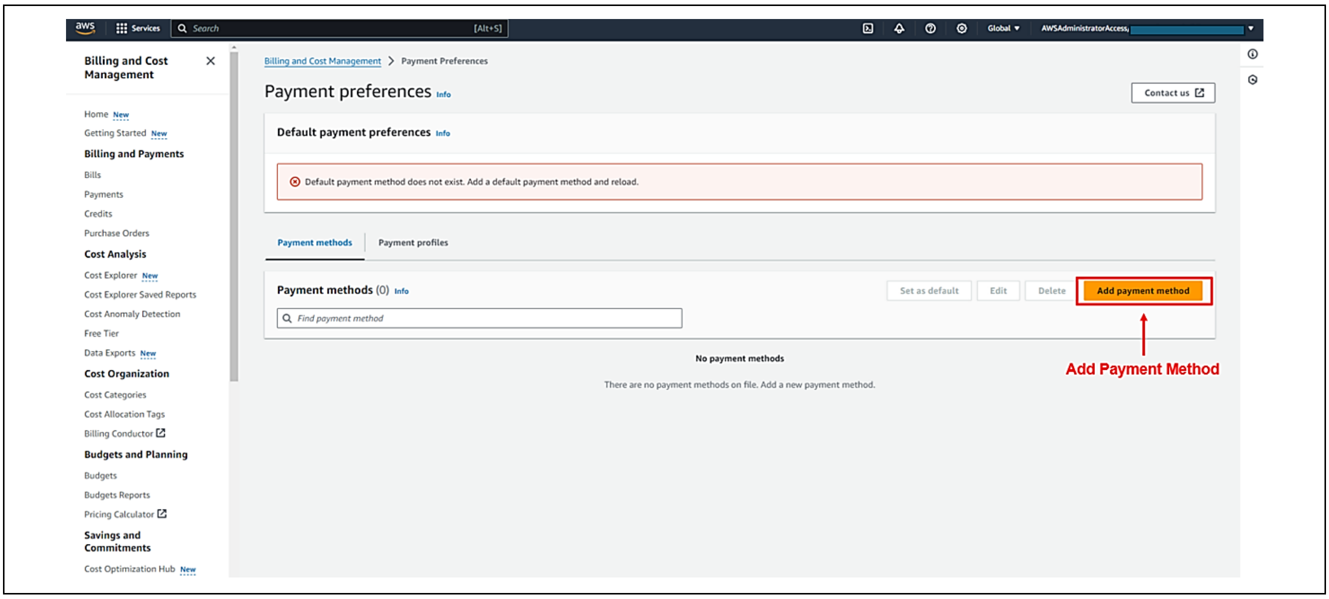
Last month's total cost
$49.48

Budgets status
ⓘ Setup required
No budget created

Cost anomalies status (MTD)
ⓘ Setup required
No monitor created

Figure 49. Payment Preferences

3. Add payment method.



Default payment method does not exist. Add a default payment method and reload.

No payment methods

There are no payment methods on file. Add a new payment method.

Figure 50. Add Payment Method

4. Go to ‘AWS Organizations’.

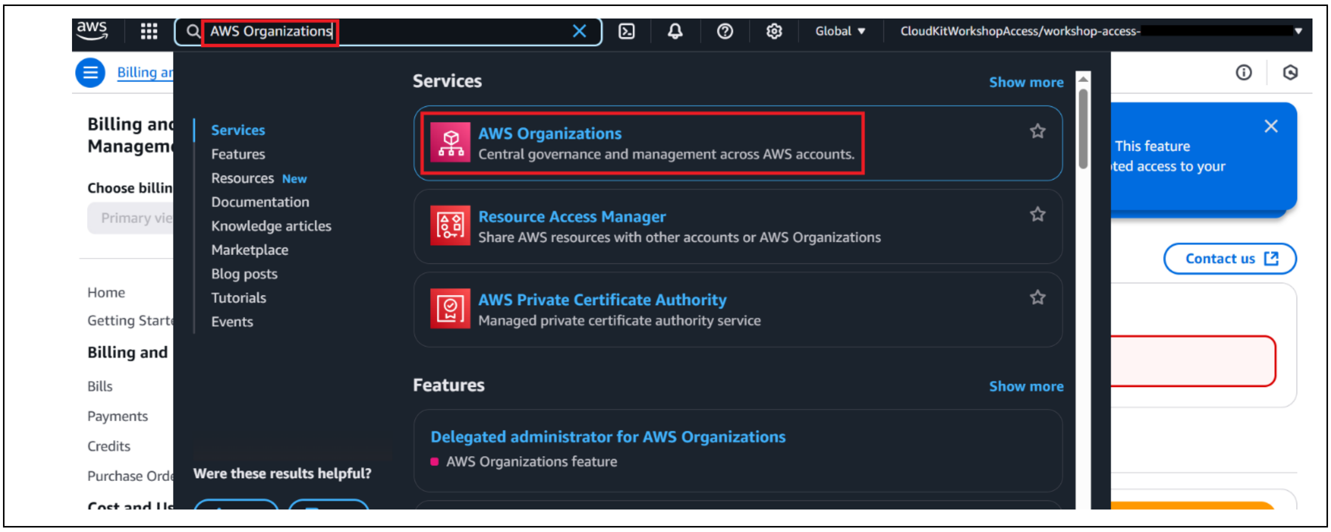
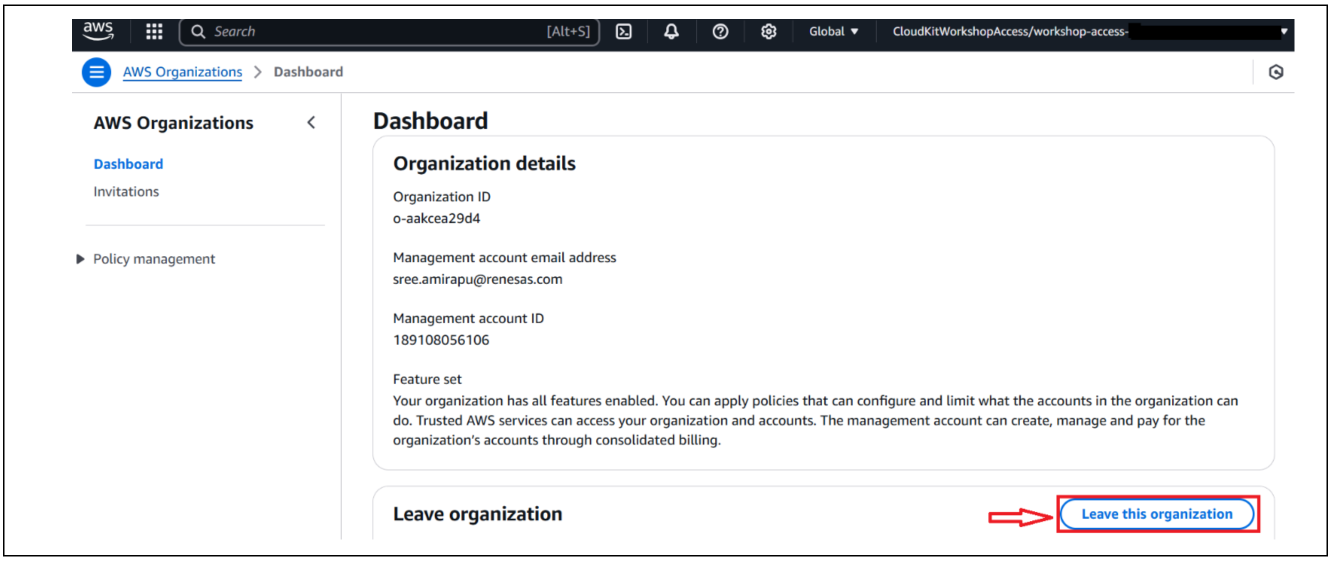


Figure 51. AWS Organizations

5. Leave the organization. This allows user accounts not to be affected by the $10 credit limit set by the organization.



Dashboard

Organization details

Organization ID
o-aakcea29d4

Management account email address
sree.amirapu@renesas.com

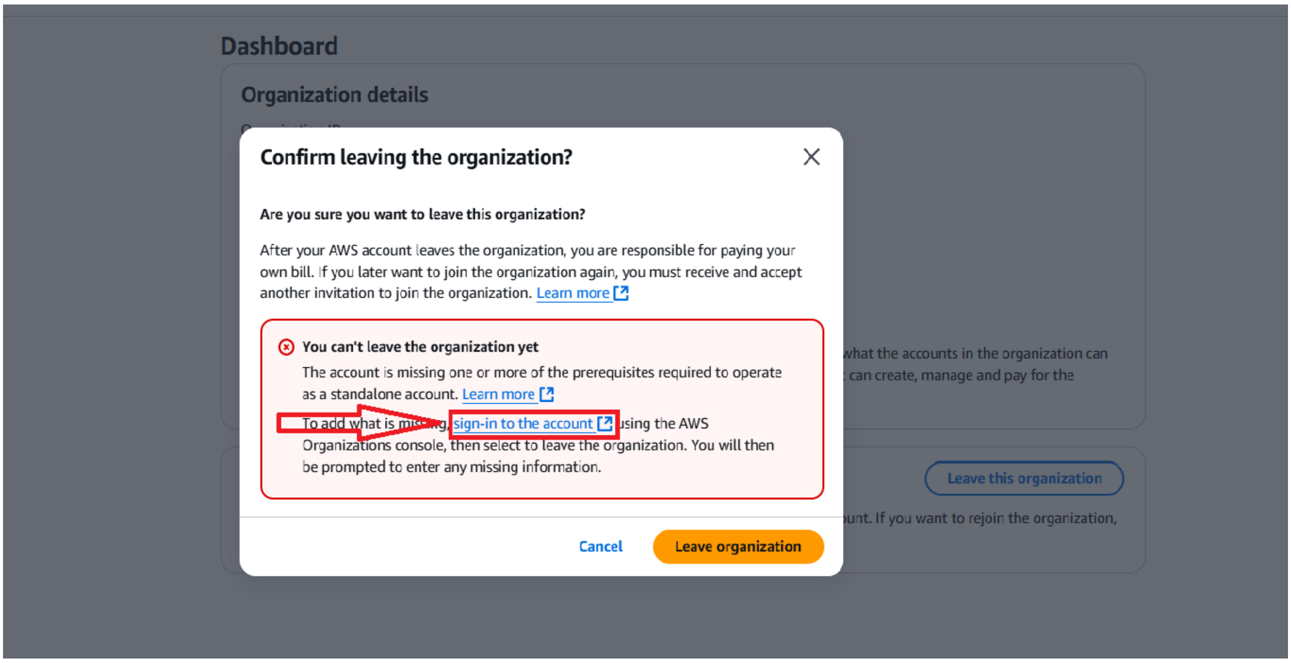
Management account ID
189108056106

Feature set
Your organization has all features enabled. You can apply policies that can configure and limit what the accounts in the organization can do. Trusted AWS services can access your organization and accounts. The management account can create, manage and pay for the organization's accounts through consolidated billing.

Leave organization

Figure 52. Leaving the organization

6. If the account is missing the prerequisites for leaving the organization, a dialog box appears prompting for the next steps. Click on ‘Sign in to the account’.



Dashboard

Organization details

what the accounts in the organization can can create, manage and pay for the

Leave this organization

unt. If you want to rejoin the organization,

Confirm leaving the organization?

Are you sure you want to leave this organization?

After your AWS account leaves the organization, you are responsible for paying your own bill. If you later want to join the organization again, you must receive and accept another invitation to join the organization. Learn more

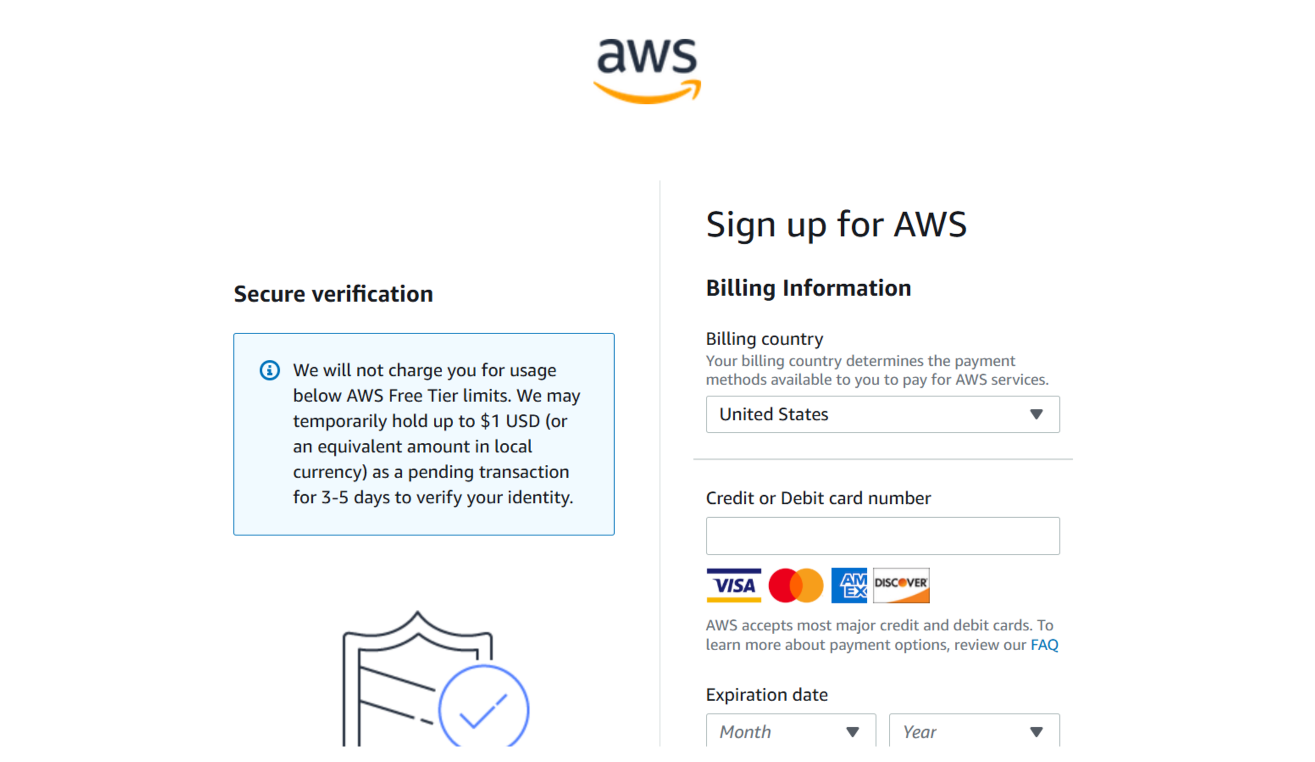
You can't leave the organization yet

The account is missing one or more of the prerequisites required to operate as a standalone account. Learn more

To add what is missing, sign-in to the account using the AWS Organizations console, then select to leave the organization. You will then be prompted to enter any missing information.

Figure 53. AWS Sign-up Process

7. Follow the steps to complete the requirements for sign-up.



Sign up for AWS

Billing Information

Billing country

Your billing country determines the payment methods available to you to pay for AWS services.

United States

Credit or Debit card number

AWS accepts most major credit and debit cards. To learn more about payment options, review our FAQ

Expiration date

Month Year

Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to $1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.

Figure 54. Prerequisites for leaving the organization

8. When the dialog box stating the sign-up process is complete appears, choose **'Leave organization'**.
9. A confirmation dialog box appears. Confirm your choice to remove the account. You are redirected to the **Getting Started** page of the AWS Organizations console, where you can view any pending invitations for your account to join other organizations.
10. Remove the IAM roles that grant access to your account from the organization.

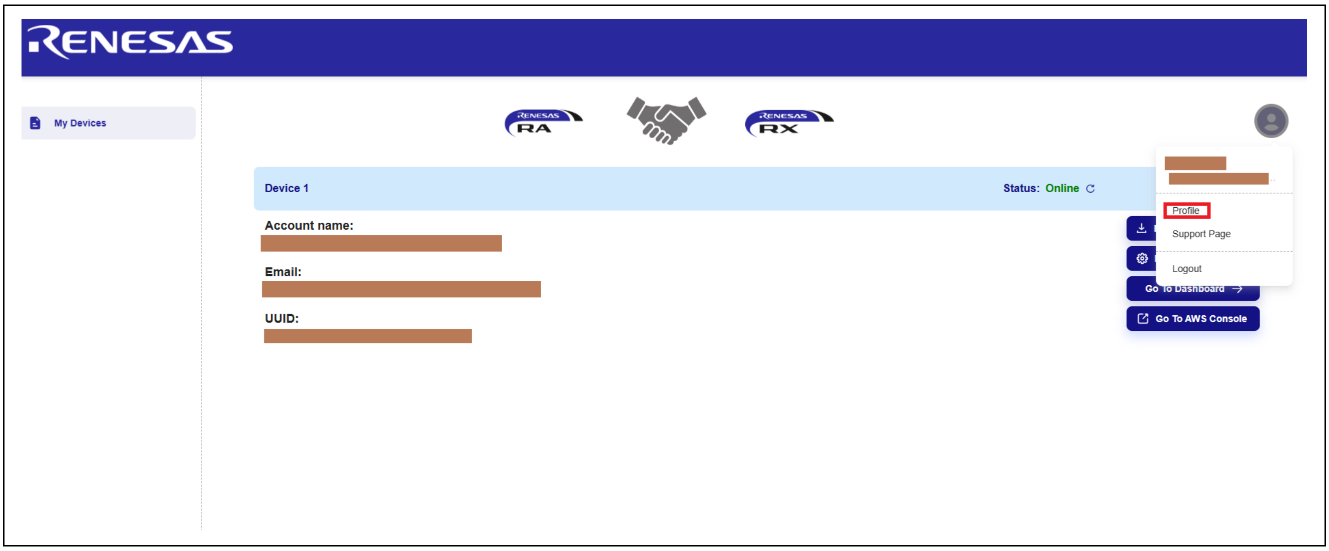
7. Renesas AWS Dashboard Account Credits and Quarantine

Every kit registered to the dashboard will include a $10 AWS credit. When the credit is exhausted, the account is quarantined.

To avoid the account from being quarantined,

1. Update the payment method in the AWS account as shown in section 6.1 Update Payment Options.
2. The dashboard must also be updated with the payment preference from the user profile on the dashboard page.

A. Go to the user profile.



Account name:
[redacted]

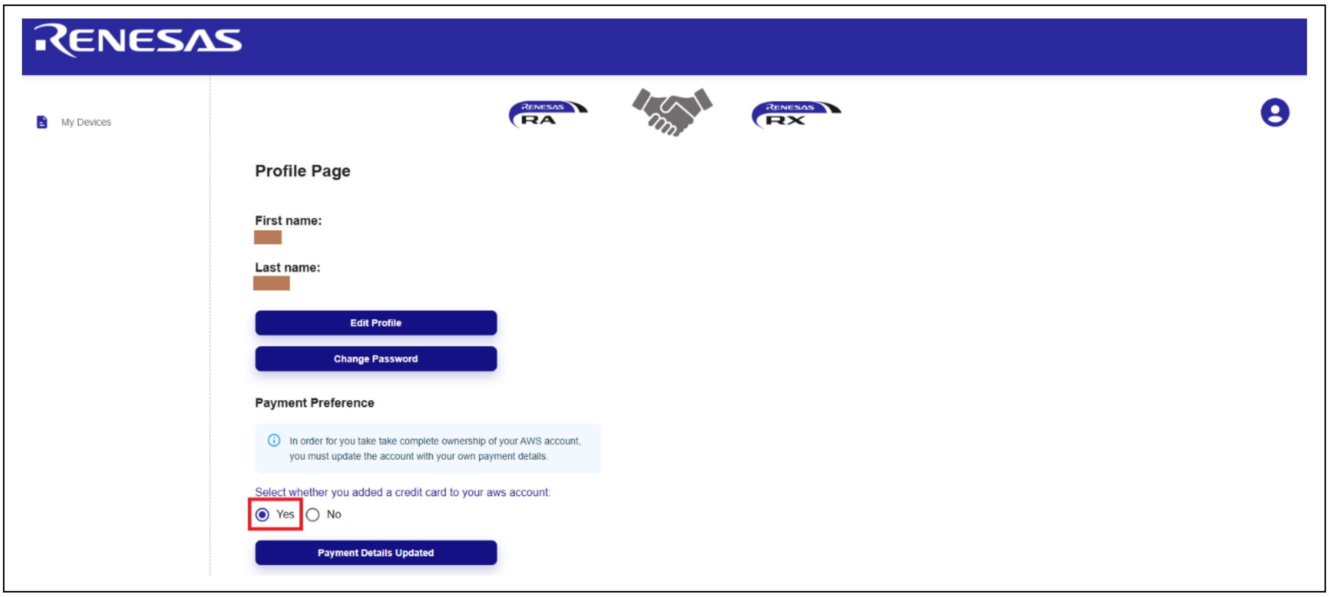
Email:
[redacted]

UUID:
[redacted]

[redacted]

Figure 55. User Profile on Dashboard

B. Update the payment preference.



Profile Page

First name:
[redacted]

Last name:
[redacted]

Payment Preference

In order for you take take complete ownership of your AWS account, you must update the account with your own payment details.

Select whether you added a credit card to your aws account:

● Yes ○ No

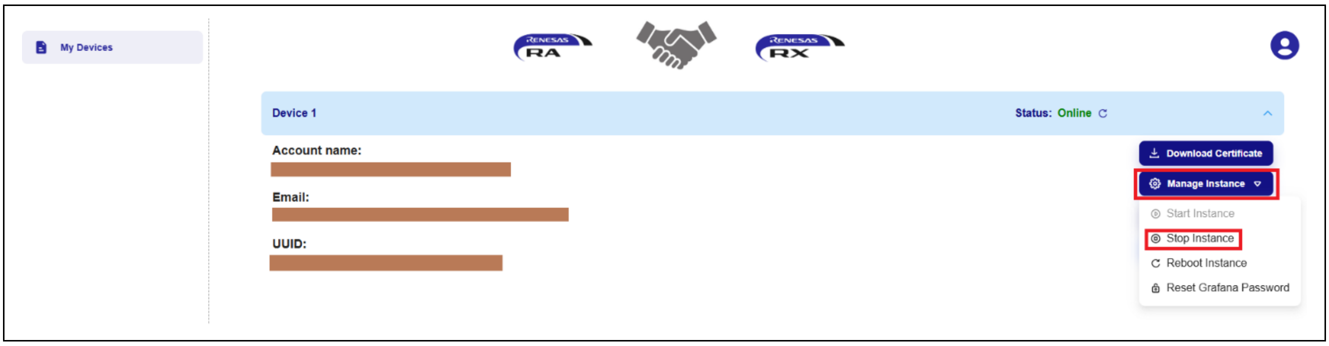
Figure 56. Payment Preference Update

Note: Failure to complete either step 1 or 2 will result in the account being quarantined. Quarantined accounts must leave the organization and remove the IAM roles as mentioned in section 6.1 to regain access to the accounts.

7.1 Manage EC2 Instance to Save Credits

To avoid excessive billing or AWS credit usage when the device is not in use, manage the EC2 instance from the dashboard main page.

1. When the device is not in use, stop the instance from the 'Manage Instance' dropdown menu.



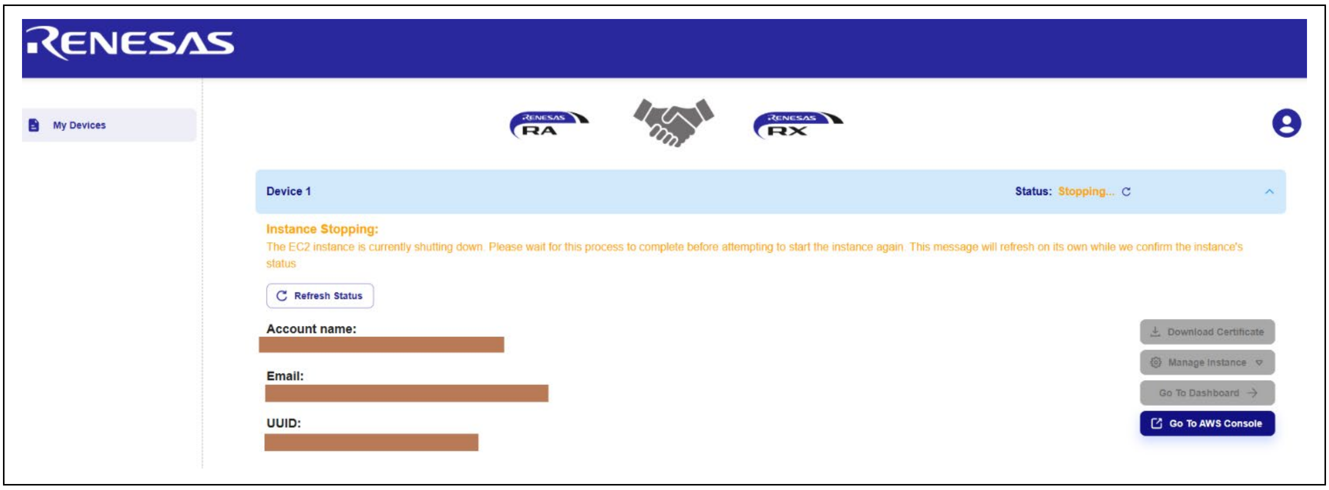
Account name:
[redacted]

Email:
[redacted]

UUID:
[redacted]

Figure 57. Stop EC2 instance

2. The screen prompt indicates the instance is stopping, and the dashboard cannot be accessed.



Instance Stopping:
The EC2 instance is currently shutting down. Please wait for this process to complete before attempting to start the instance again. This message will refresh on its own while we confirm the instance's status

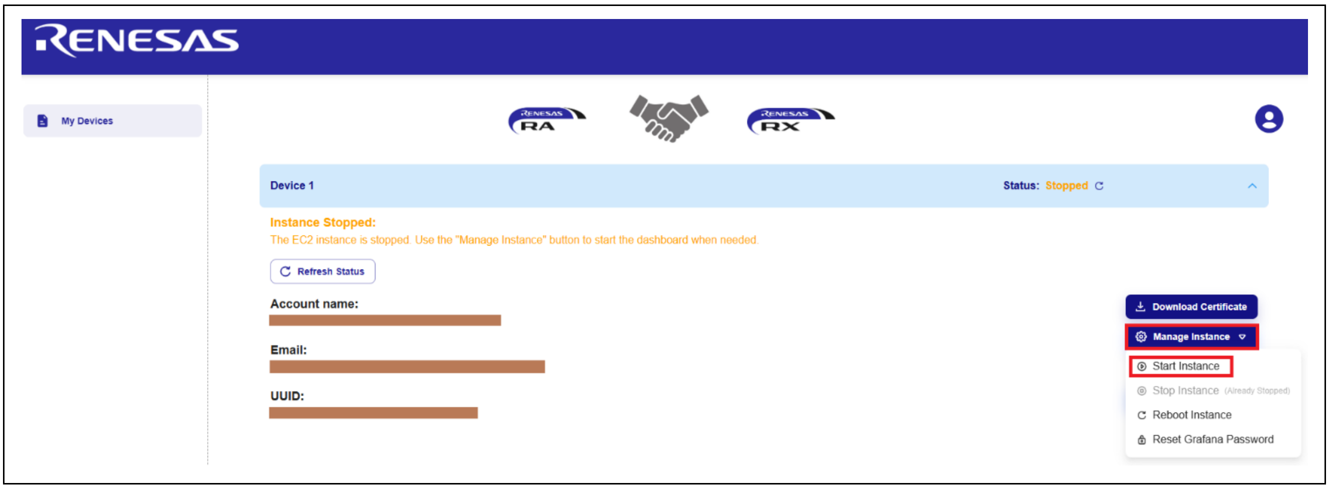
Account name:
[redacted]

Email:
[redacted]

UUID:
[redacted]

Figure 58. EC2 instance status

3. When the device is back in use, restart the EC2 instance.



Instance Stopped:
The EC2 instance is stopped. Use the "Manage Instance" button to start the dashboard when needed.

Account name:
[redacted]

Email:
[redacted]

UUID:
[redacted]

Figure 59. Restarting the EC2 Instance State

8. Sensor Stabilization Time

Table 2 gives the time required for the sensors to sense and provide valid data to the users. Here, you will see two columns: column 1 - when powered up for the first time, and column 2 - after soft or hard reset. If the system boots up from a cold start, the time for the sensors to provide the valid data is up to (1 min – 4 hours), whereas if the system boots up from a warm start, the time for the sensors to provide the valid data is up to (10 sec – 2 hours). For more details, refer to the specific sensor datasheet.

Table 2. Sensor Stabilization Time

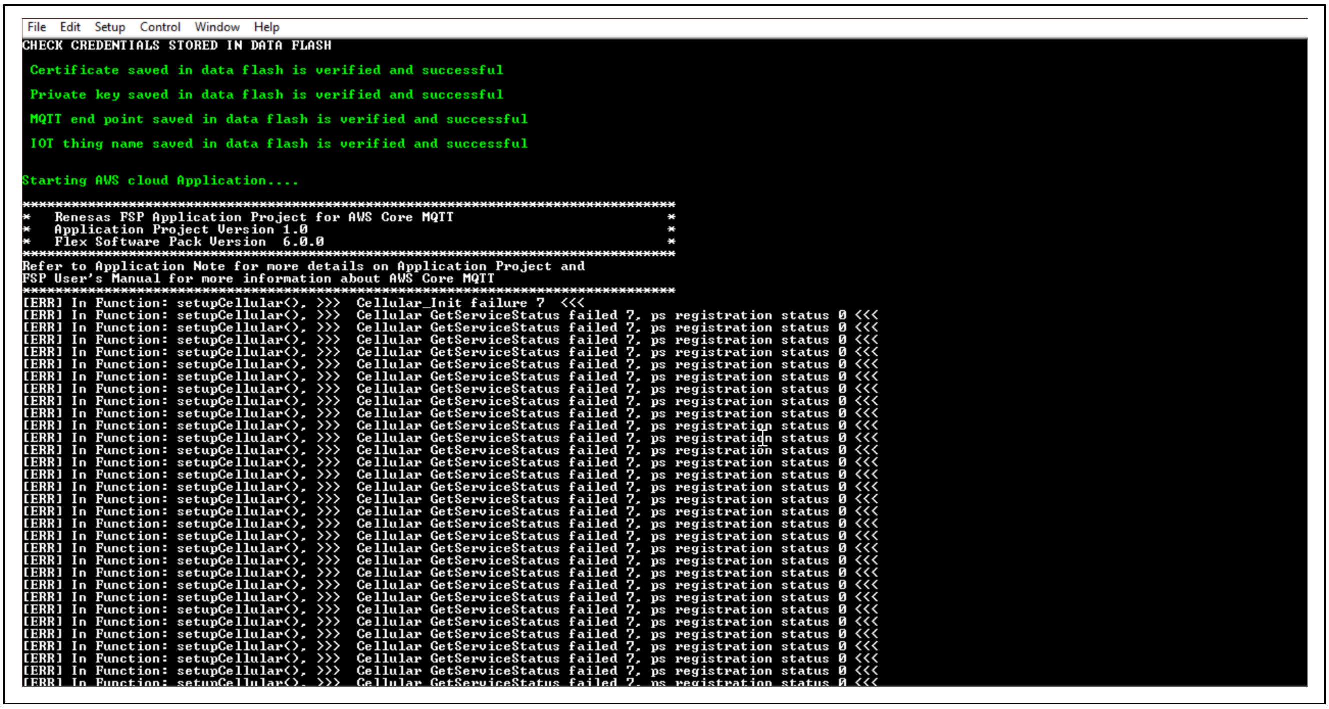
Sensor Name	When Powered Up First Time	After Soft or Hard Reset
ZMOD4410 IAQ	Up to 1 minute	Up to 1 minute
ZMOD4510 OAQ	Up to 4 hours	Up to 5 minutes
OB1203	Up to 20 minutes (After placing a finger on the sensor, it may take up to 60 seconds to sense data)	Up to 20 seconds (After placing a finger on the sensor, it may take up to 60 seconds to sense data)
HS3001	Up to 30 seconds	Up to 10 seconds
ICP	Up to 30 seconds	Up to 10 seconds
ICM	Up to 30 seconds	Up to 10 seconds

Note: The Stabilization time of the sensor provided above is from the point of sensor initialization.

9. Known Issues and Troubleshooting

- This section talks about the known FSP and tool-related issues. More details can be found at the link: https://github.com/renesas/fsp/issues.
- It is recommended that the dashboard be used with the Microsoft Edge browser; it does not work properly with the Google Chrome browser.
- When running debug on e^2 studio, if the application is rerun multiple times, an issue with the OB1203 sensor's i2c communication might randomly occur. Users need to reconnect the USB cable (J10) and USB-C cable (J28) to reset the OB1203 sensor and run the application again.

After activating the SIM Card, when running the application with the option **"6. Start Application"** (section **2.8**), if a user encounters the **"CELLULAR_TIMEOUT Failure 7"** issue **(Figure 60)**, although a user can get CATM Info via option 4 **(Figure 8)** and validate SIM activation via option 5 **(Figure 11)**, please check the PMOD2 jumper settings in section 1.4 Connection Settings and Deviation.



```
CHECK CREDENTIALS STORED IN DATA FLASH

 Certificate saved in data flash is verified and successful

 Private key saved in data flash is verified and successful

 MQTT end point saved in data flash is verified and successful

 IOT thing name saved in data flash is verified and successful

Starting AWS cloud Application....

********************************************************************************
*   Renesas FSP Application Project for AWS Core MQTT                          *
*   Application Project Version 1.0                                            *
*   Flex Software Pack Version  6.0.0                                          *
********************************************************************************
Refer to Application Note for more details on Application Project and
FSP User's Manual for more information about AWS Core MQTT
********************************************************************************
[ERR] In Function: setupCellular(), >>>  Cellular_Init failure 7  <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
[ERR] In Function: setupCellular(), >>>  Cellular GetServiceStatus failed 7, ps registration status 0 <<<
```

Figure 60. Cellular_Init failure issue

10. Debugging

Enable the `USR_LOG_LVL (LOG_DEBUG)` macro in the application project to obtain additional information about the error during debugging.

10.1 SIM Card Activation Problem

- If the SIM activation fails, verify that the ICCID number and PUK numbers are correctly entered when activating the SIM card on Truphone IoT SIM activation platform truphone.com/connectit
- If **Menu 5 Validate SIM activation** PING response returns a Ping Failed condition, it can take up to 15 minutes or longer for the card to be activated after performing **Activating the SIM Card** to obtain LTE Network access. In this case, wait at least 15 minutes (or longer) and repeat **Menu 5 Validate SIM activation**.
- SIM cards cannot be activated more than once. To verify whether the SIM card has already been activated, please monitor and manage your SIMs on the Truphone IoT Connectivity Management Platform or contact Truphone support through iot.truphone.com by logging into your account.
- If **Menu 5 Validate SIM activation** PING response continues to return Ping Failed condition, first check the external antenna is connected securely to the Cellular PMOD (GM02S) module and try again. The CSQ Network Signal Quality (RSSI) could be too low to connect. If the RSSI is 99, then check external antenna is connected. It may be possible that no Cell Network Signal could be detected in your area. An RSSI reading with RSSI = 15 or less indicates marginal or poor reception.
  CSQ Network Signal Quality (RSSI) [99 = No Cell Signal] = 15, Marginal Signal Quality
  It may be necessary to move the CK-RA6M5 v2 with PMOD to a different location to improve the Network Signal Quality (RSSI) to get an RSSI value in the range of 16 to 98.
- If **Menu 5 Validate SIM activation** continues to fail, verify that the APN is set for the Global Region where the Cellular PMOD (GM02S) module is trying to connect. The APN setting and LTE Band List depend on your Global Region and the SIM card provider.
  Access Point Name (APN) for SIM Card providers other than Truphone can be set in the Application project in `/src/cellular_setup.c`

  See `#define CELLULAR_APN "iot.truphone.com"   /* APN : Truphone SIM Card */`
- For all other SIM card issues that cannot be resolved with these troubleshooting steps, contact Truphone support through iot.truphone.com by logging into your account.

Website and Support

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

CK-RA6M5 v2 Kit Information	renesas.com/ra/ck-ra6m5
RA Cloud Solutions	renesas.com/cloudsolutions
RA Product Information	renesas.com/ra
RA Product Support Forum	renesas.com/ra/forum
RA Flexible Software Package	renesas.com/FSP
Renesas Support	renesas.com/support

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Jul.15.24	—	Initial release
1.10	Sept.06.24		Updated to v5.3.0
1.20	Jun.17.25		Updated to v6.0.0

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/.