Renesas RA Family

RA AWS Cloud Connectivity on CK-RA6M5v2 with Wi-Fi DA16600– Getting Started Guide

Introduction

This document provides instructions for running AWS cloud connectivity Application Project on CK-RA6M5 v2 using Wi-Fi DA16600 interface.

Applies to:

- RA6M5 MCU Group

Required Resources

To build and run the MQTT/TLS application example, the following resources are needed.

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® 10/11 and an installed web browser (Google Chrome, Internet Explorer, Microsoft Edge, Mozilla Firefox, or Safari)
- DA16600 PMOD: US159-DA16600EVZ - Ultra-Low-Power Wi-Fi + Bluetooth® Low Energy Combo Pmod™ Board (Renesas Quick-Connect IoT) | Renesas
- Micro USB cables (included as part of the kit. See *CK-RA6M5 v2 – User's Manual*).
- USB-C cable for Power supply (See *CK-RA6M5 v2 – User's Manual)*

Prerequisites and Intended Audience

This application note assumes that the user is adept at operating the Renesas e² studio IDE with 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 e² 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 Wi-Fi modems.

The intended audience is users who want to develop applications with MQTT/TLS modules using Wi-Fi DA16600 modules on Renesas RA6 MCU Series.

Note: If you are a first-time user of e² studio and FSP, we highly recommend you install e² studio and FSP on your system to run the Blinky Project and to get familiar with the e² studio and FSP development environment before proceeding to the next 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 to latest documentation for identified Renesas Flexible Software Package.
3. Prior knowledge of operating e² studio and 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_wifi_da16600_app`" can be imported into the e² studio using the instructions provided in the RA *FSP User's Manual*. See section *Starting Development > e2 studio ISDE User Guide > Importing an Existing Project into e² studio ISDE.*

1.2 Building the Latest Executable Binary

Upon successfully importing and/or modifying the project into e² 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 > e2 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 e² studio

Instructions to program the executable binary are found in the latest RA FSP User Manual. See Section *Starting Development > e2 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.

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 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.

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* before proceeding with the next set of instructions.

Note: For this Wi-Fi based cloud connectivity application project and application note, the user is required to connect the DA16600 PMOD module to the connector (J26 – PMOD1) on the board.

1.5 Powering up the Board

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

Then run the debug application, with the instructions in the next 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 down the COM port number for reference in the next step.

   Note: JLink CDC UART drivers are required to communicate between the CK-RA6M5 v2 board and the terminal application on the host PC.

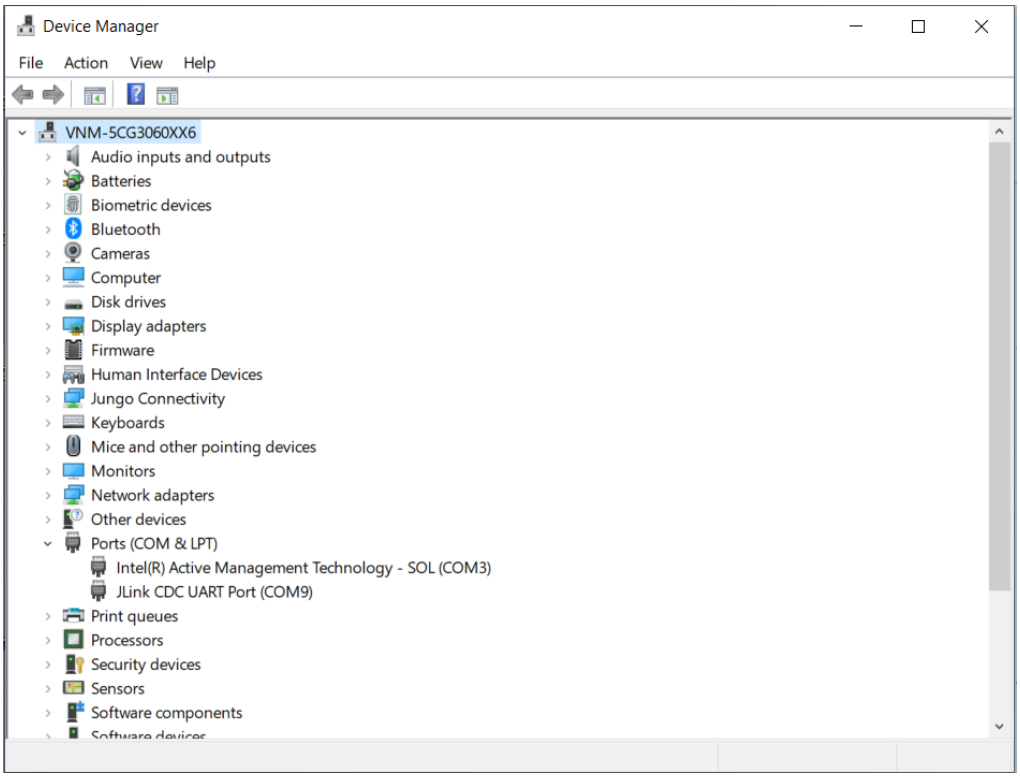

Figure 1. JLink CDC UART in Windows Device Manager

2. Open Tera Term select **New connection** and select **Serial** and **COMxx: JLink CDC UART Port (COMxx)** and click **OK**.
   Note: Please use Tera Term **version 4.99** to ensure the application functions correctly.

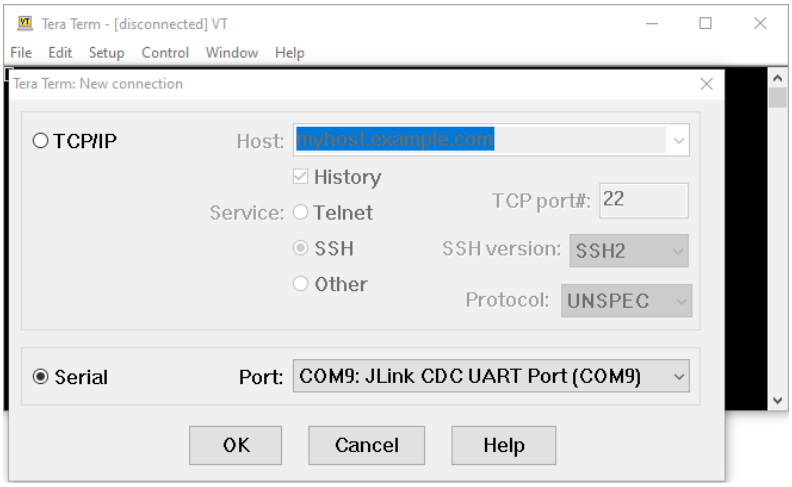

Figure 2. Selecting the UART Port on Tera Term

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

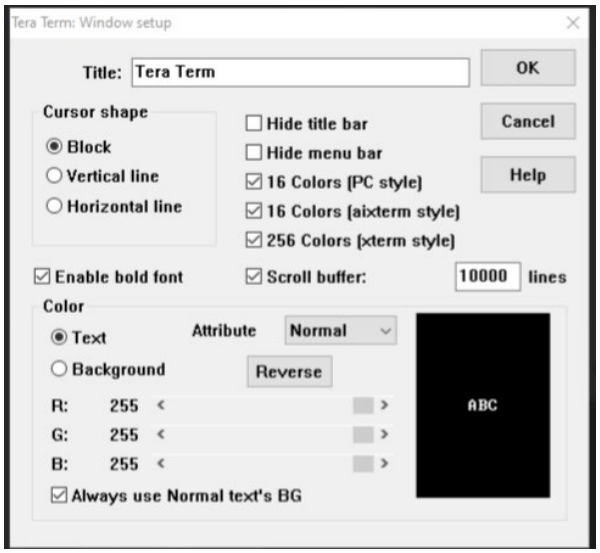

Figure 3. Configuring the Black Background for JLink CDC UART Port on Tera Term

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

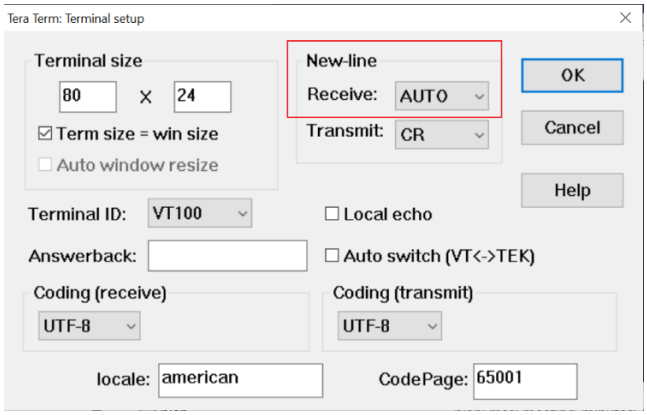

Figure 4. Configuring Terminal

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

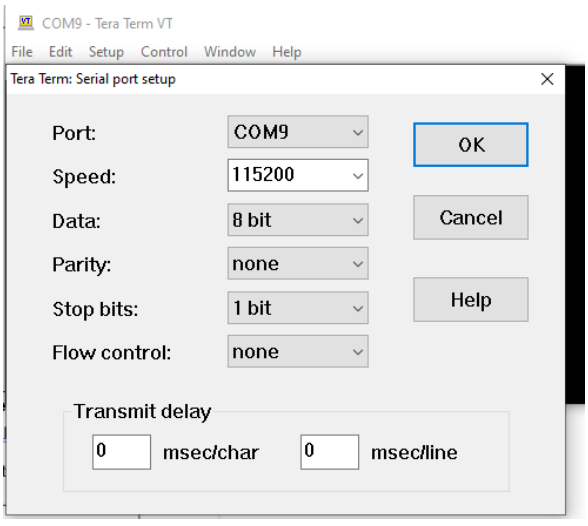

Figure 5. Select 115200 on the Speed Pulldown Menu

6. Complete the connection. The Configuration CLI Menu will be displayed on the console as shown below.
   Note: Please reset the board by pressing the **S1** user switch if the menu is not displayed.

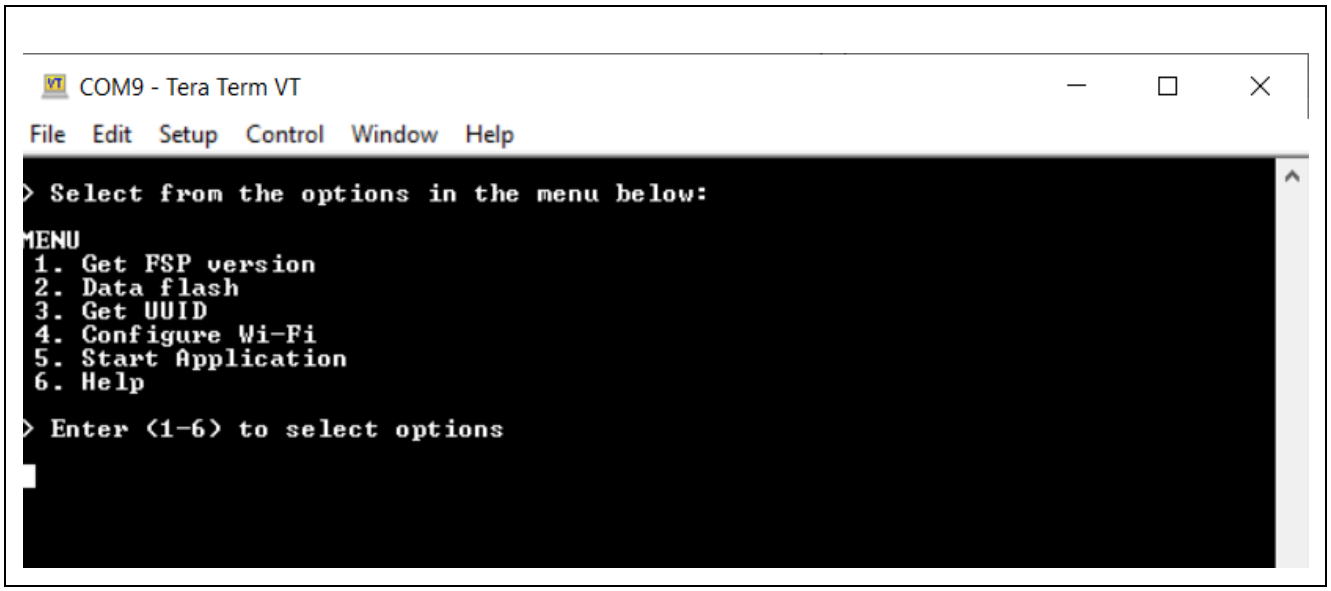

Figure 6. Main Menu

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 of time, press the space bar to return to the previous menu.

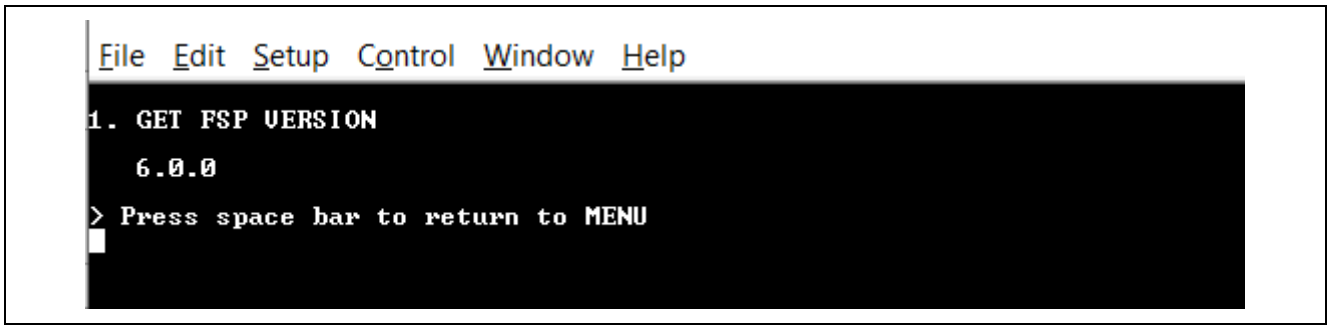

Figure 7. FSP Version Information

2.2 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 for registering to the Renesas AWS Cloud Dashboard.

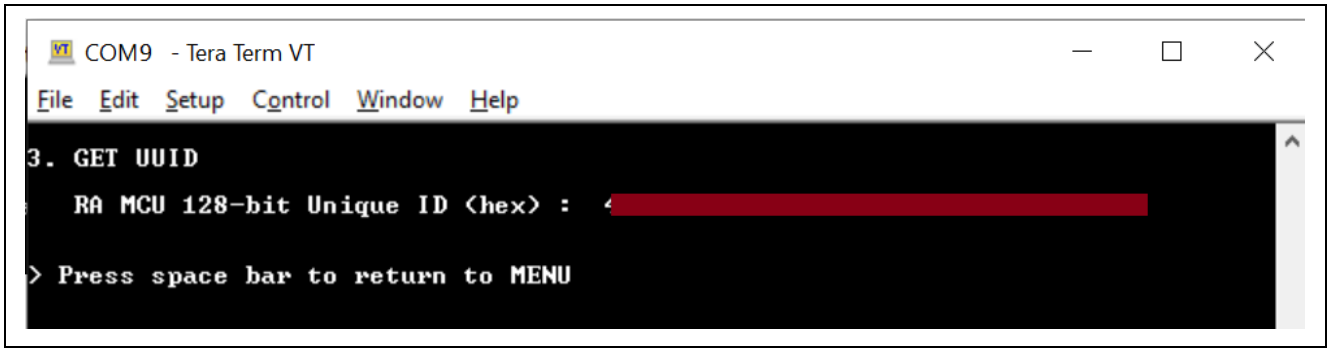

Figure 8. Getting Board UUID Information

2.3 Registering to 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 full potential.
To allow users to experience a hassle free first experience of the cloud kits, every cloud kit is credited with $10 USD AWS credits upon registration.
The dashboard can be accessed at https://renesas.cloud-ra-rx.com/

2.3.1 Sign up.

After establishing the access of the RA and RX kit to 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 UUID, you can skip and go to section 2.3.2

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.

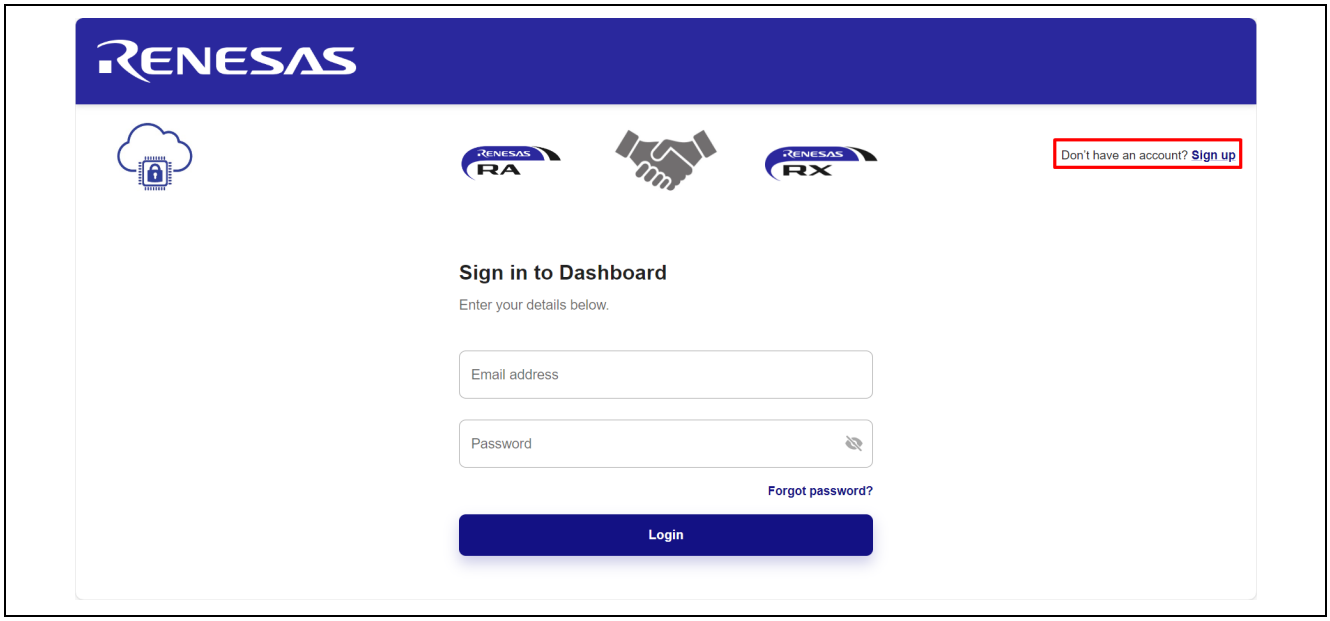

Figure 9. Creating Account

3. Enter your first name, last name, email address and password and press on the button **Register**.

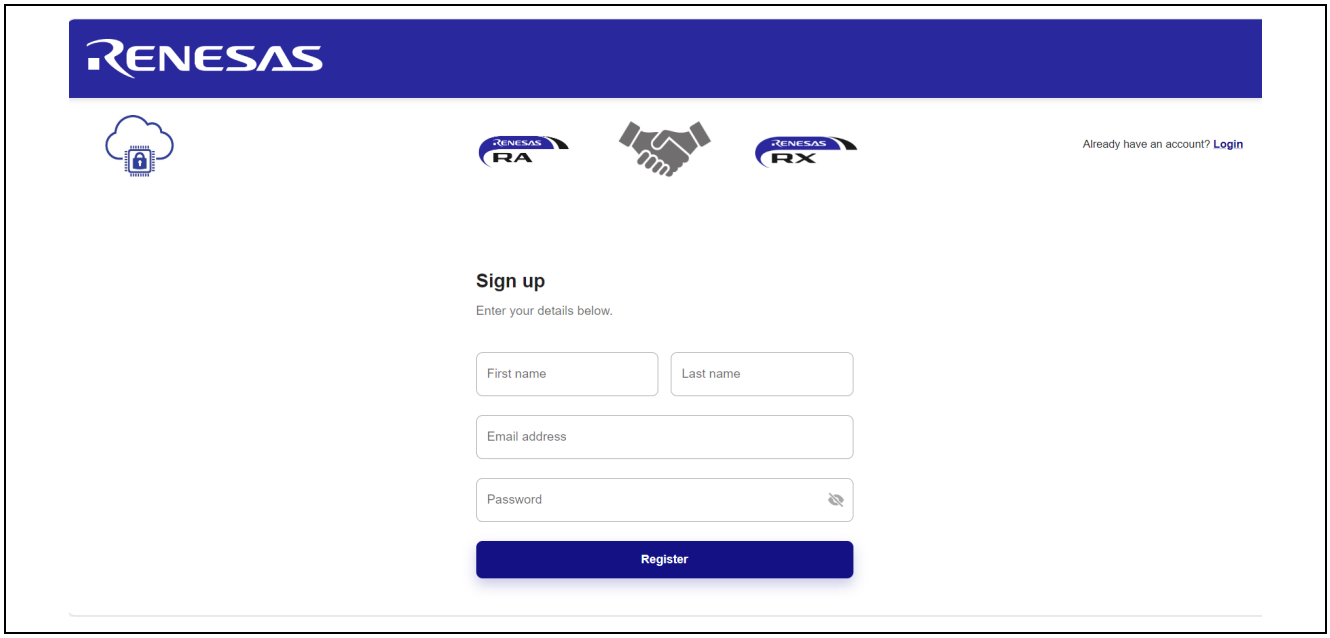

Figure 10. Registering Information

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

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

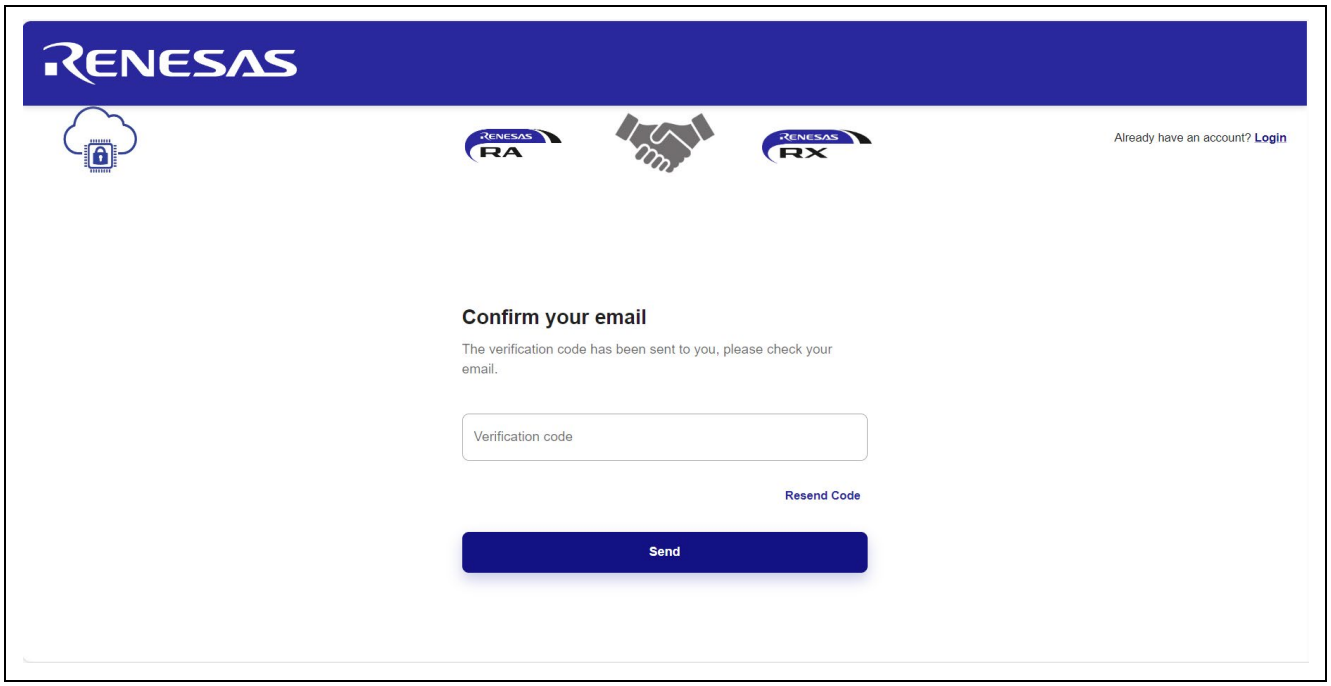

Figure 11. Confirming Email

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 AWS Application Project” for steps for obtaining the UUID of the kit (Go to section 2.2).
   Note: Only 1 device will be assigned to an account.

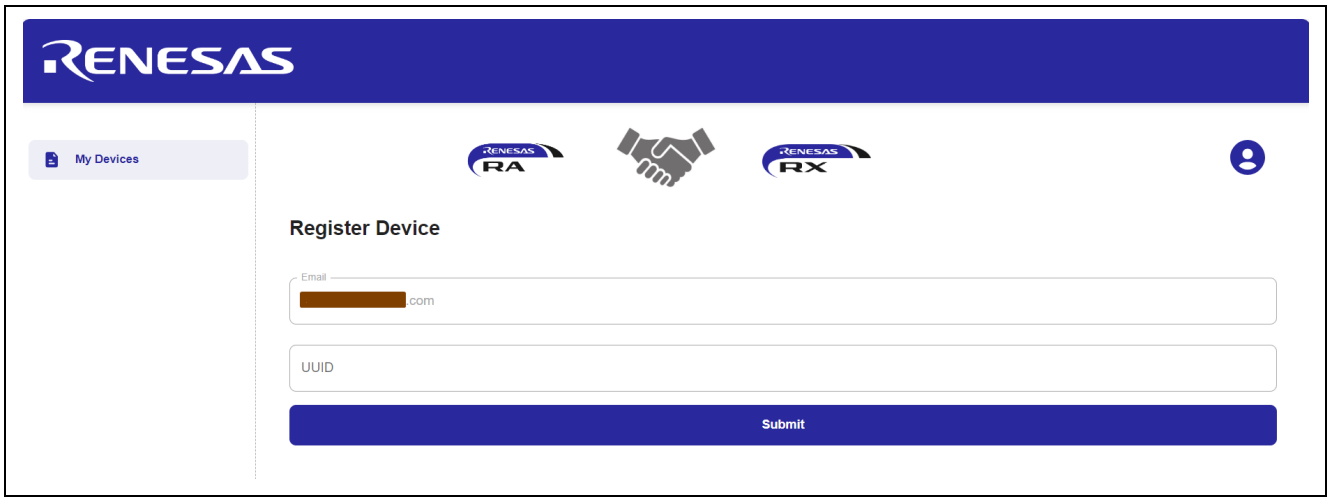

Figure 12. Registering Device

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

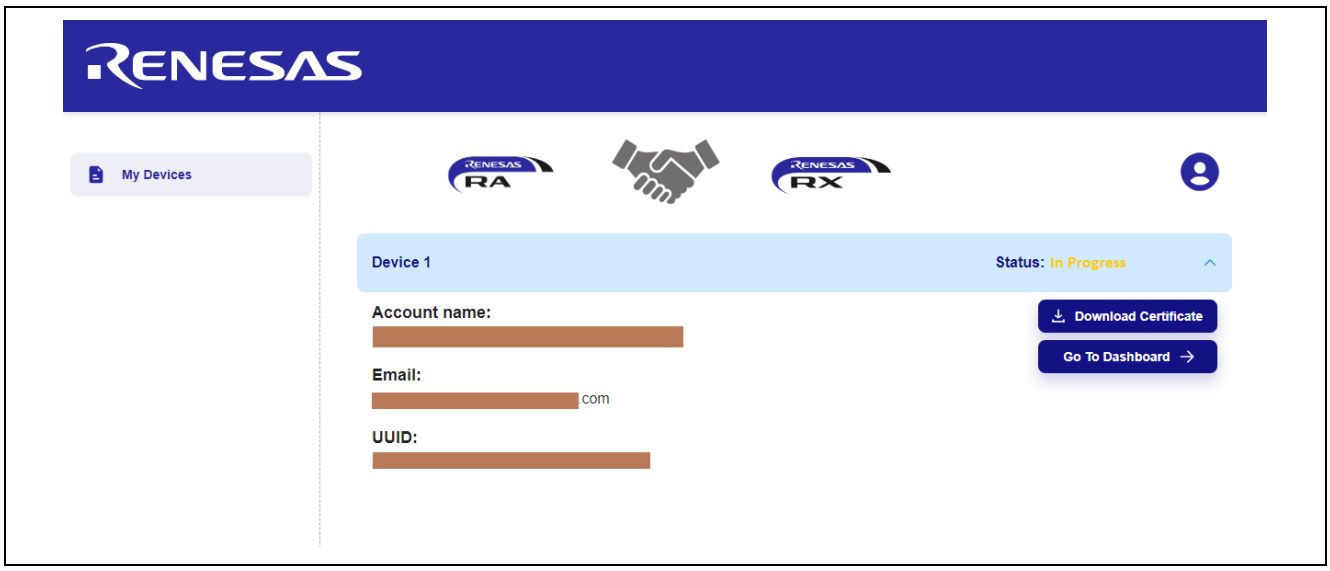

Figure 13. Device Registration in Progress

7. Refresh the page and the status of the registration changes to ‘Online’

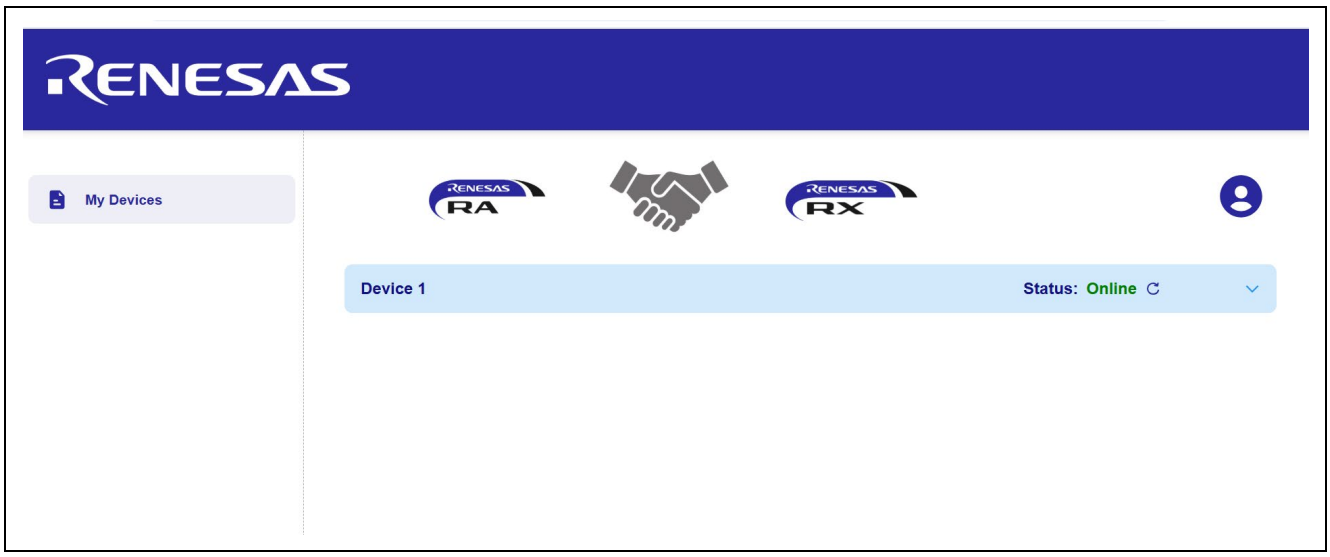

Figure 14. Sub Account Registration

8. The dropdown button next to the status displays the device information and option for downloading the certificates.

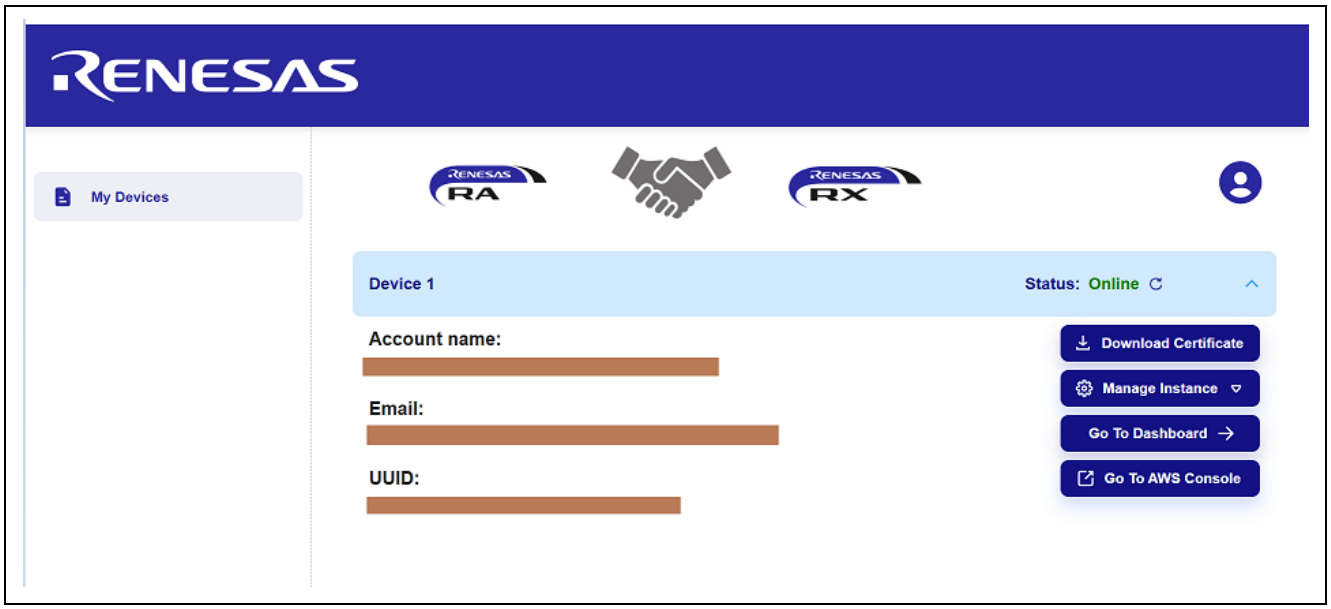

Figure 15. Completing Device Provisioning

2.3.2 Sign in

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

2.3.3 Forgot password

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

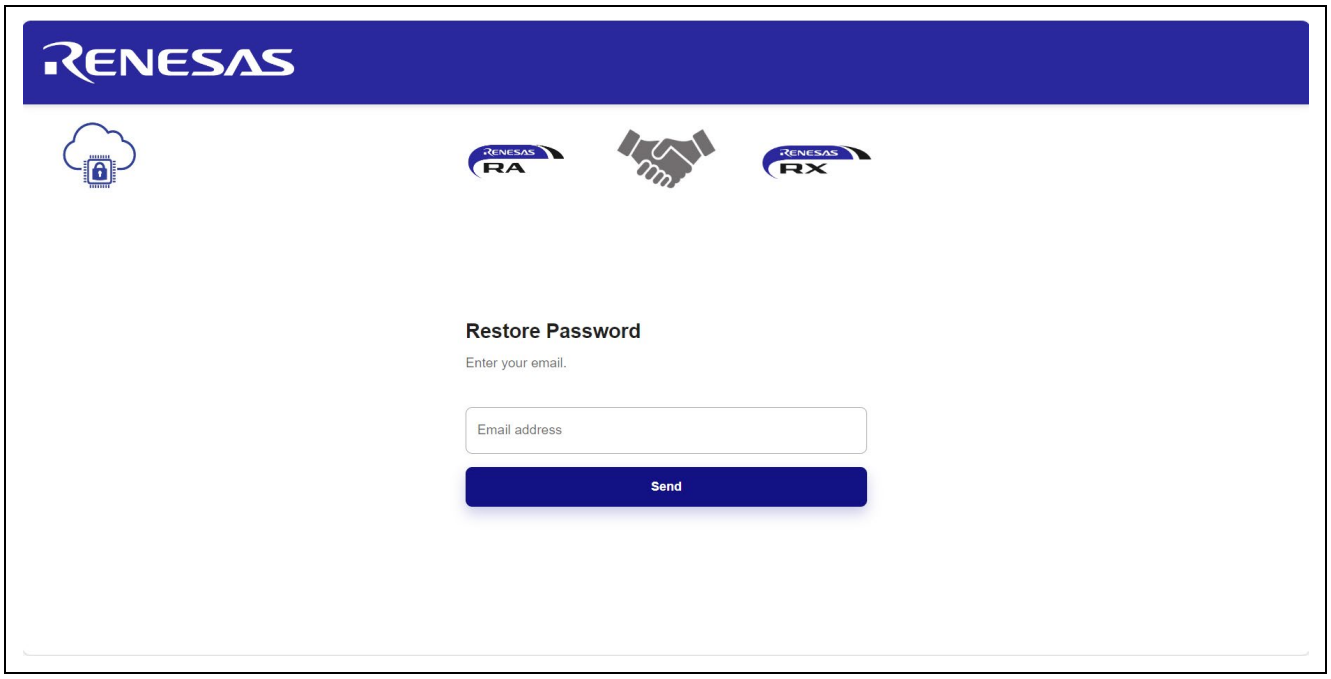

Figure 16. Restoring Password 1

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

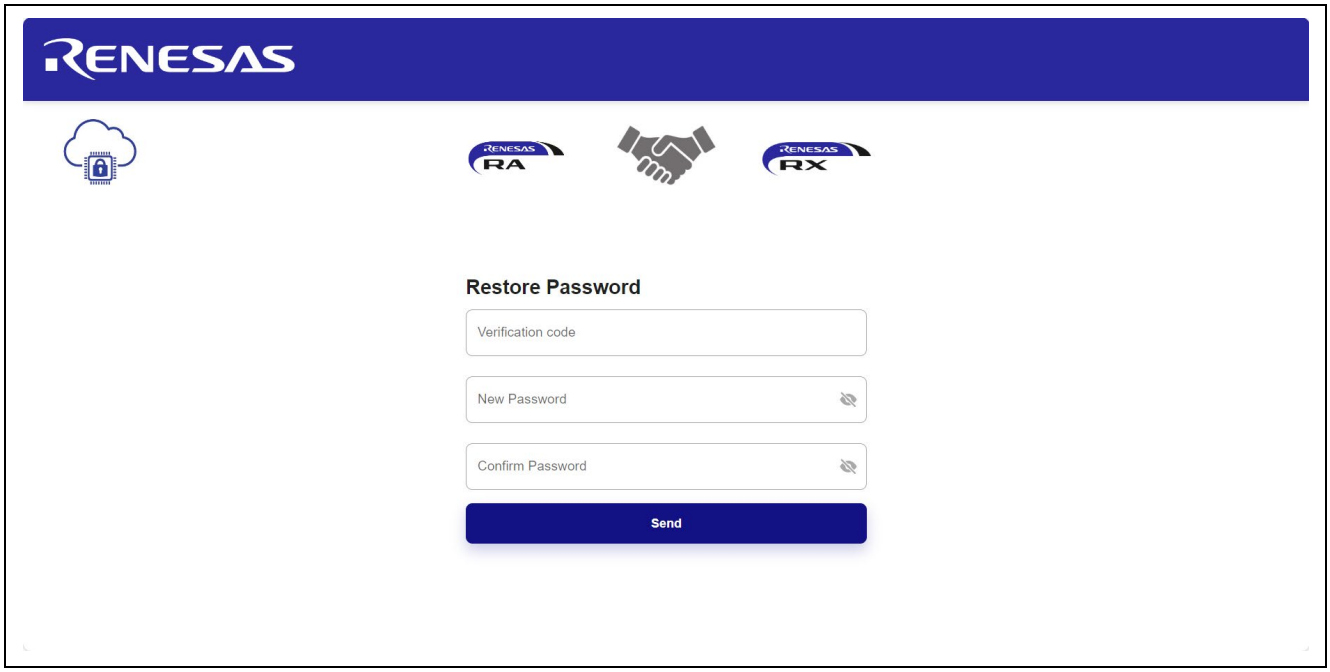

Figure 17. Restoring Password 2

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

2.3.4 Profile page

To see your profile page:

1. Click on your user's picture – top right. Select Profile.

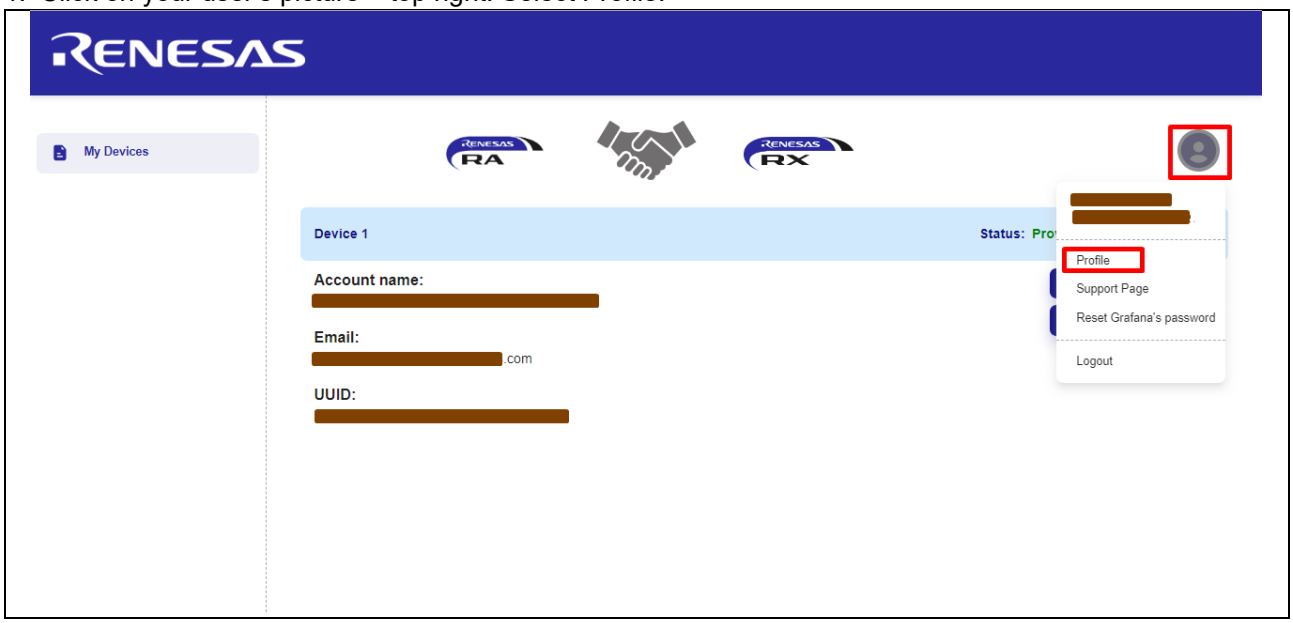

Figure 18. Selecting Profile

You are redirected to the Profile page:

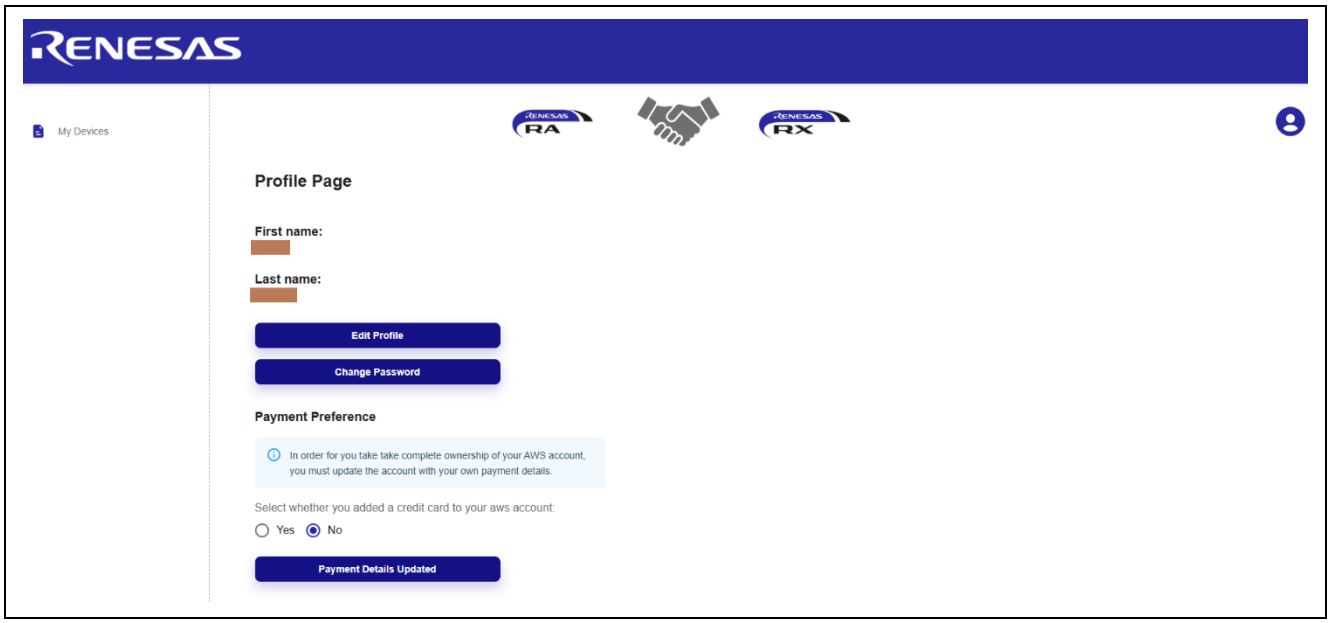

Figure 19. Profile Page

On the page you can edit your profile:

A. Press on the button Edit Profile.
B. Change your First name and Last name.
C. Press on the button Send.
D. Your Account Name is updated.

Figure 20. Updated Profile Page

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

A. Press on the button 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.

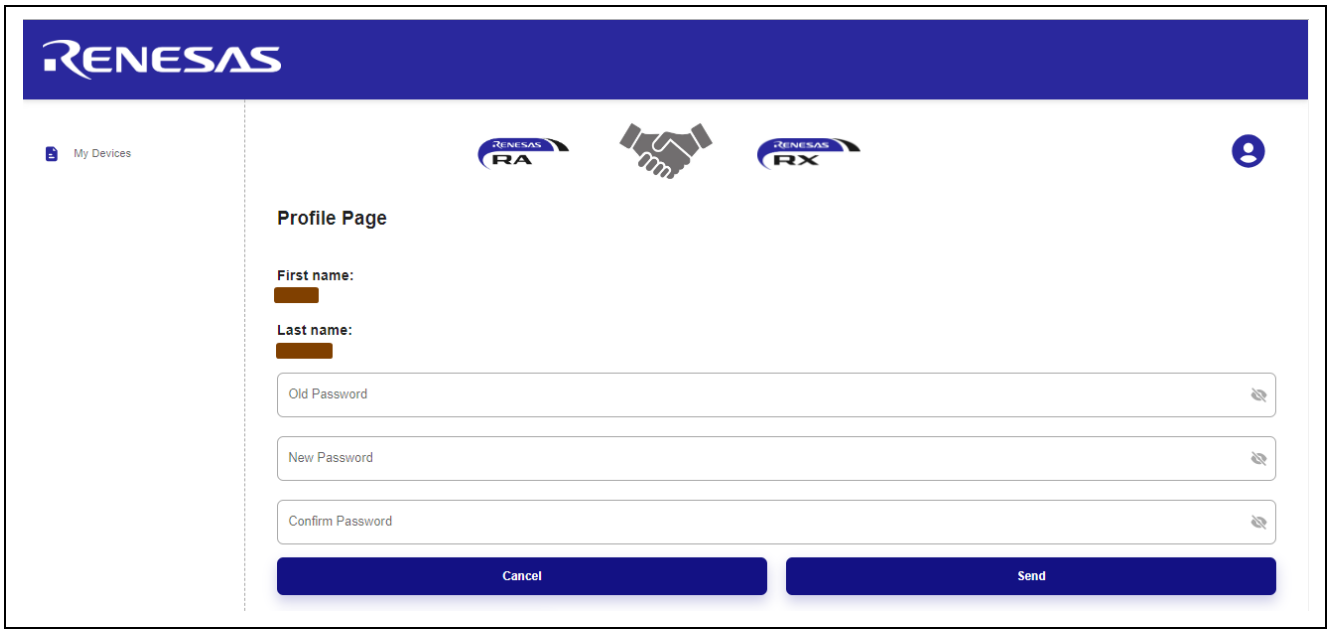

Figure 21. Changing Password on Profile Page

2.3.5 Support Page

To see your support page:
Click on your user's picture – top right. Select Support page.

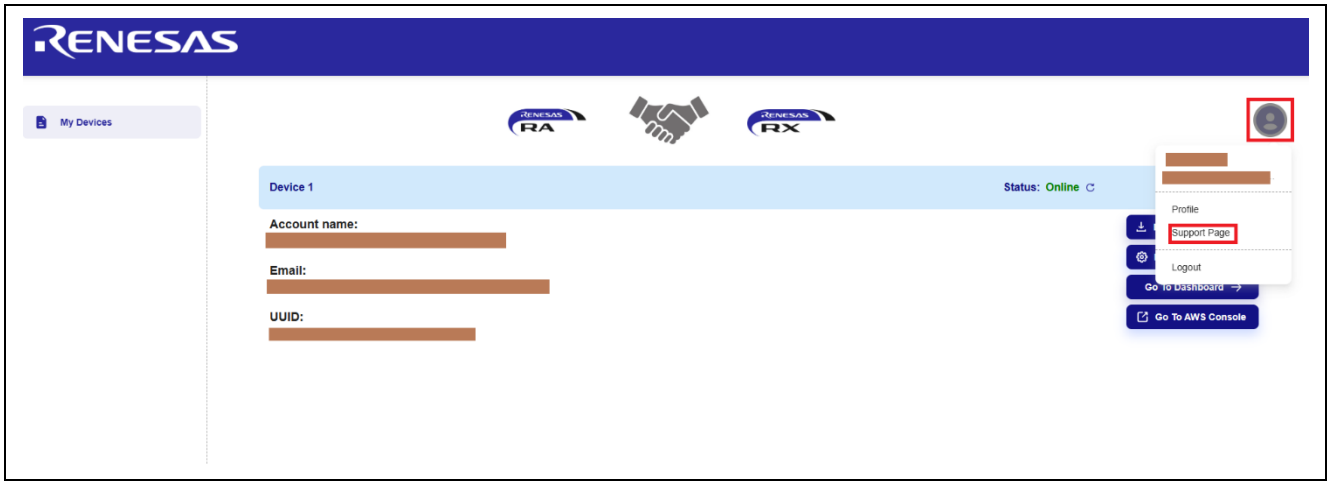

Figure 22. Selecting Support Page

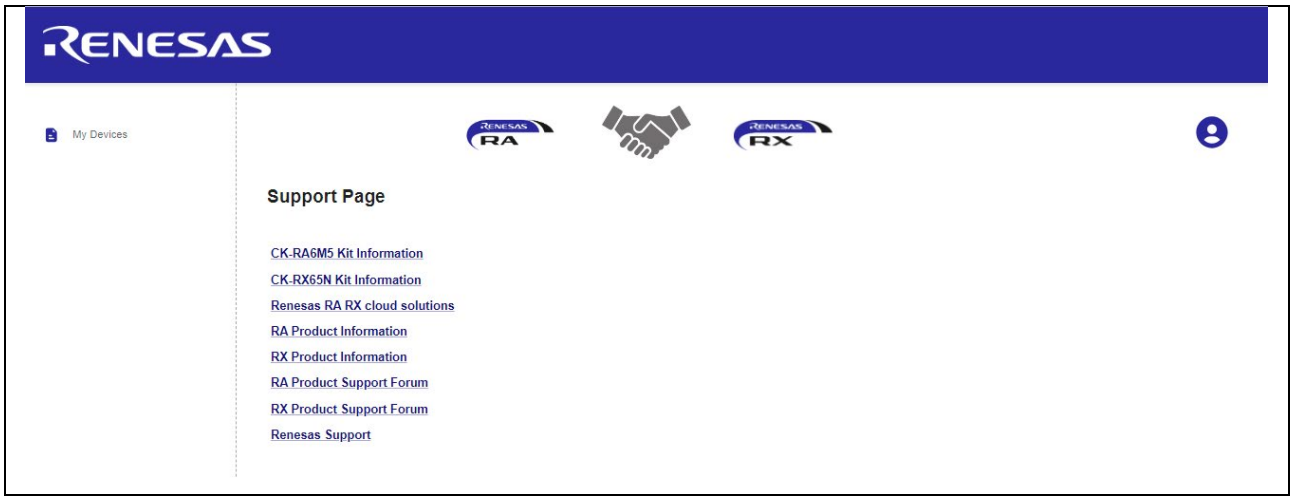

Figure 23. Support Page

2.3.6 Downloading the Certificate

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

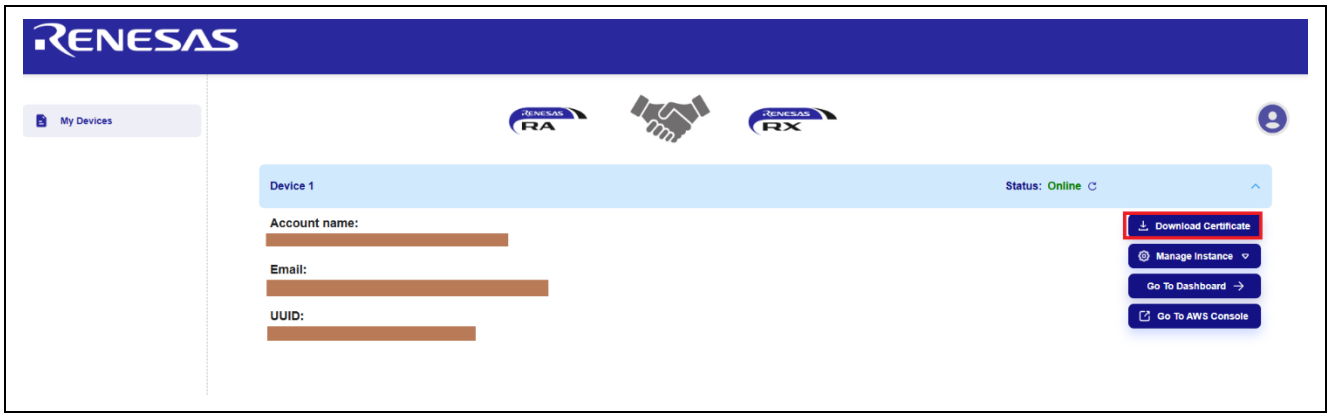

Figure 24. Downloading the Certificate

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

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

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

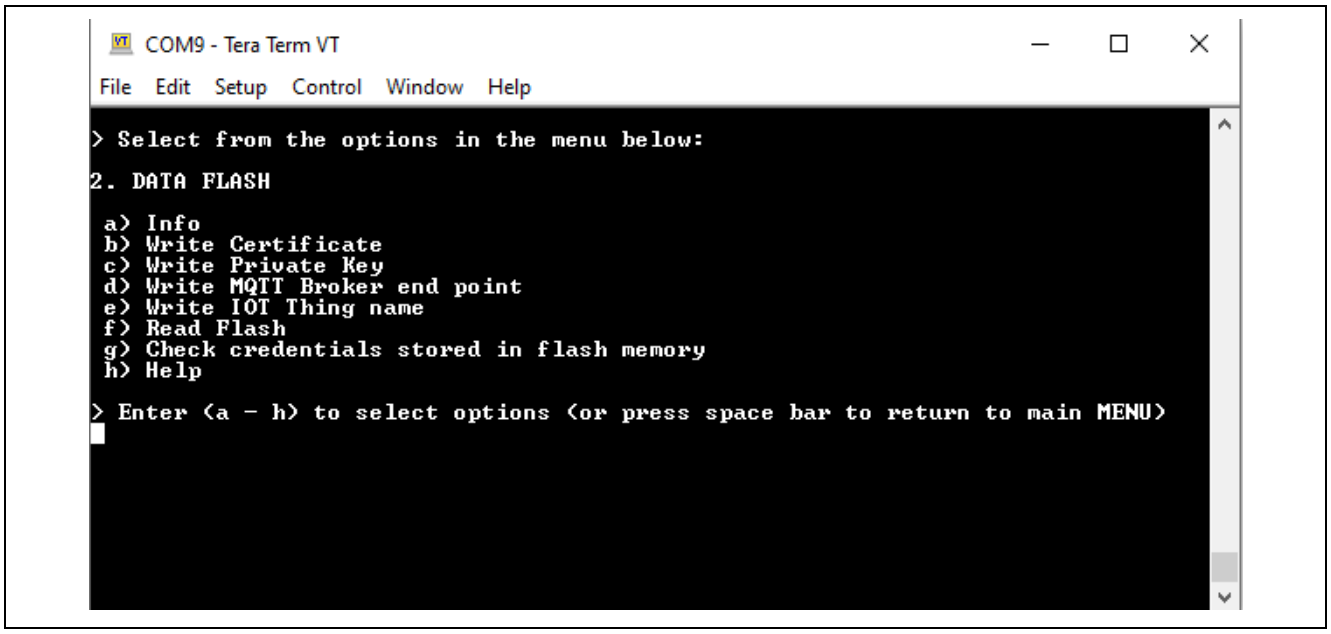

Figure 25. Data Flash related Menu and Commands

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 2.3.6.

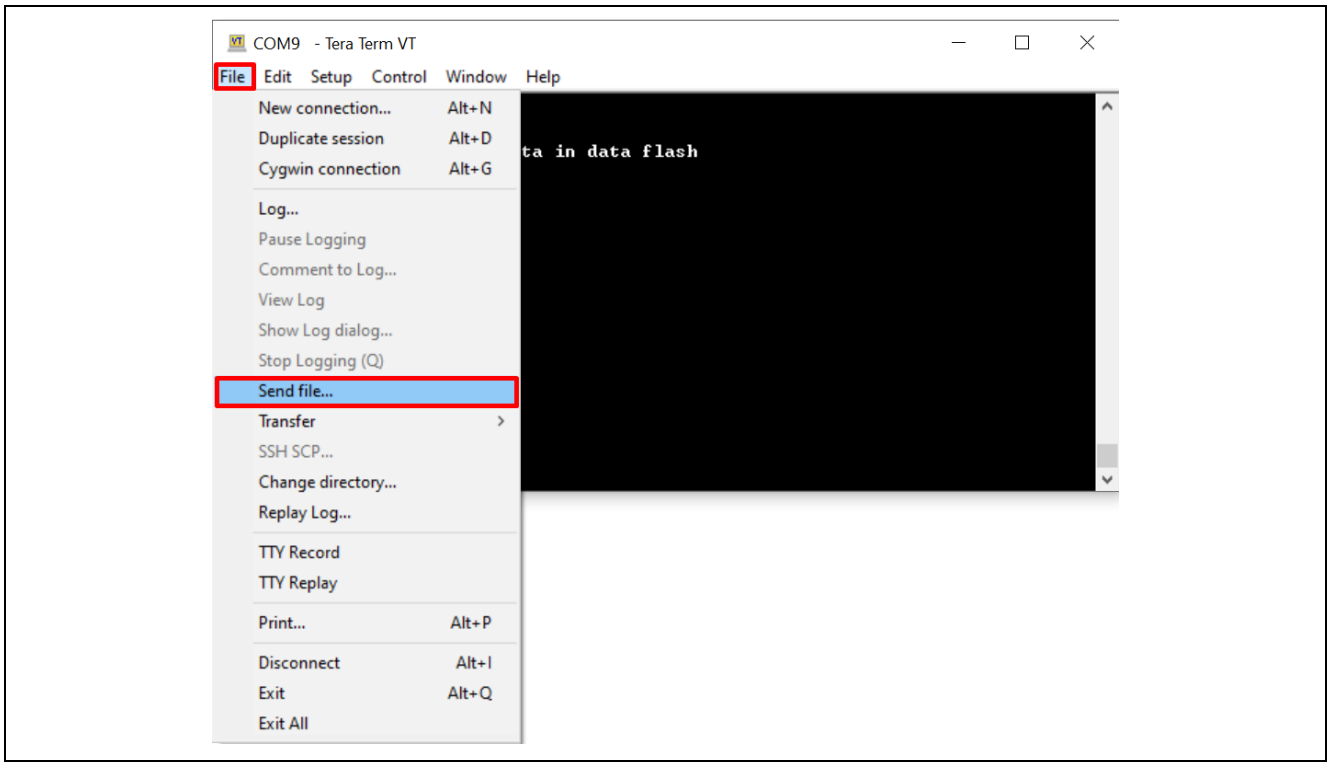

Figure 26. Accessing the Device Certificate

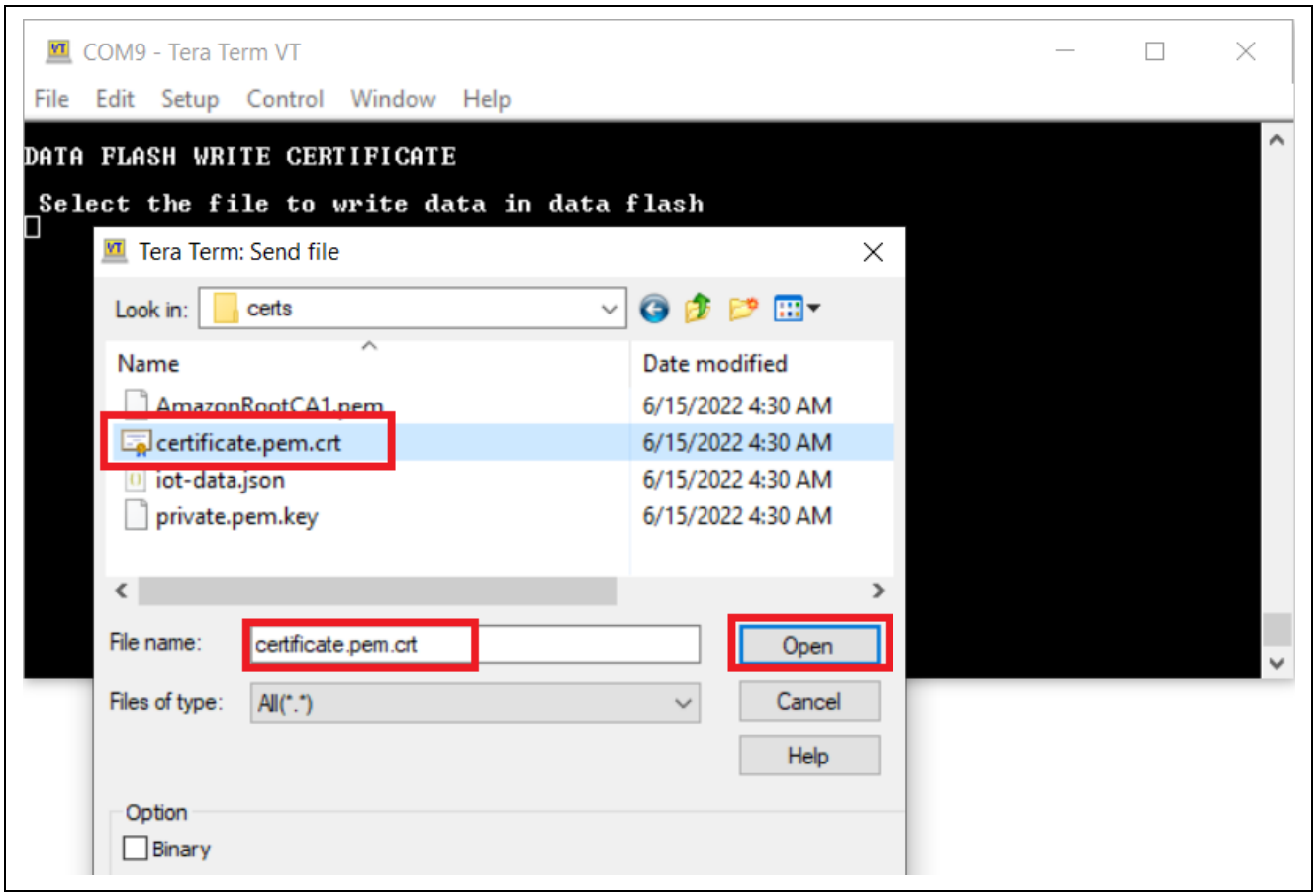

Figure 27. Downloading the Device Certificate into the Data Flash

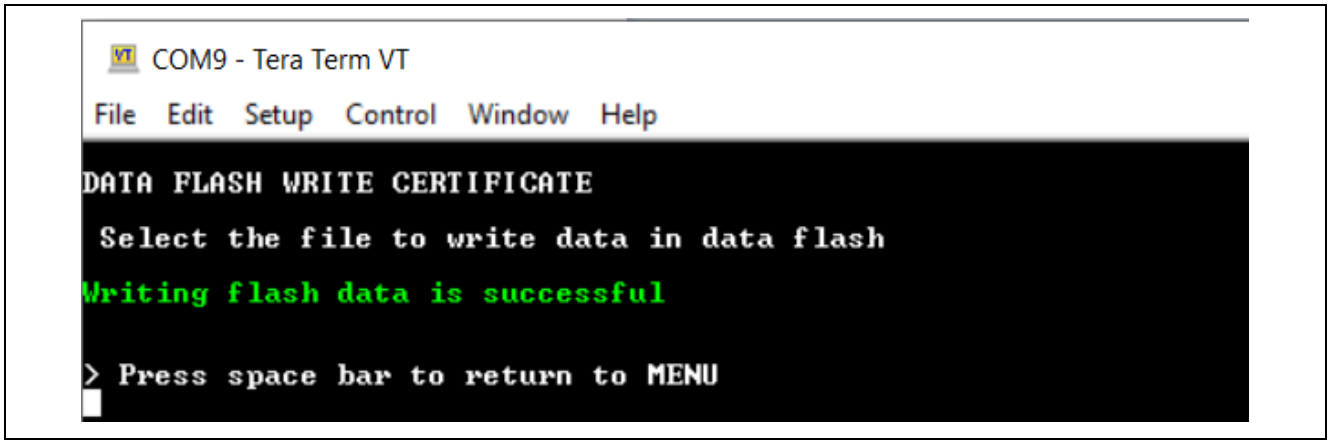

Figure 28. Status of the Downloaded Device Certificate into the Data Flash

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 2.3.6.
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: Make sure to NOT copy the double quotes when copying the MQTT Broker end point.

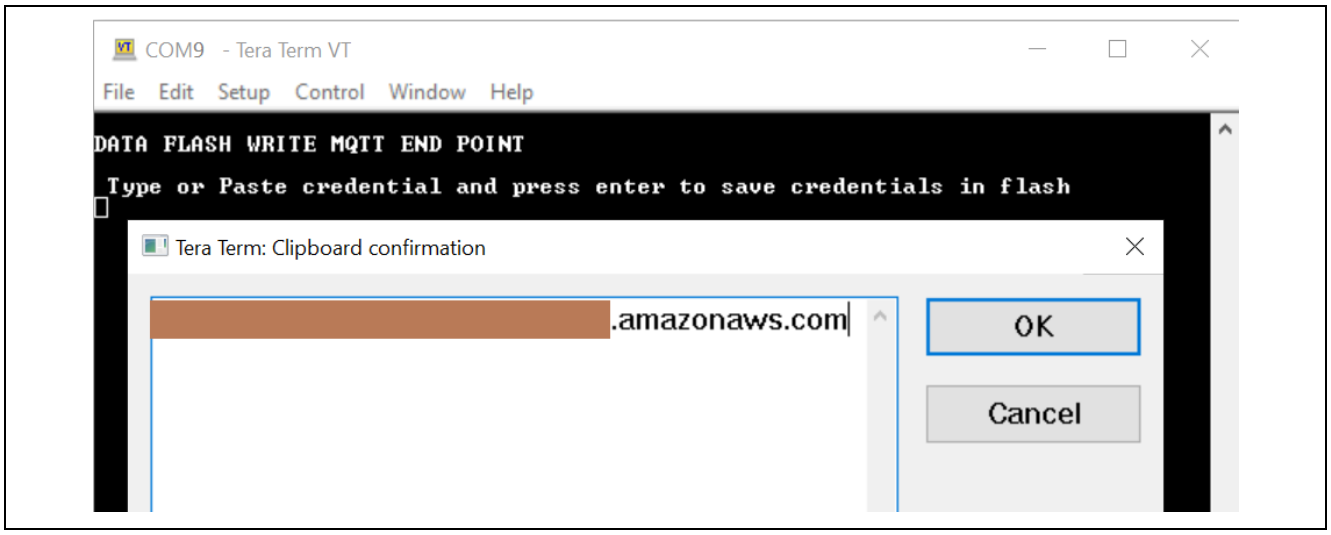

Figure 29. Storing the MQTT Endpoint into the Data Flash

5. To store the IOT Thing Name, copy the Thing Name string `xxxxxxxx-xxxxxxxx-xxxxxxxx-4e4bxxxx` from the **iot-data.json** file in **certs.zip** file in section 2.3.6. 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: Make sure to NOT copy the double quotes when copying the Thing Name.

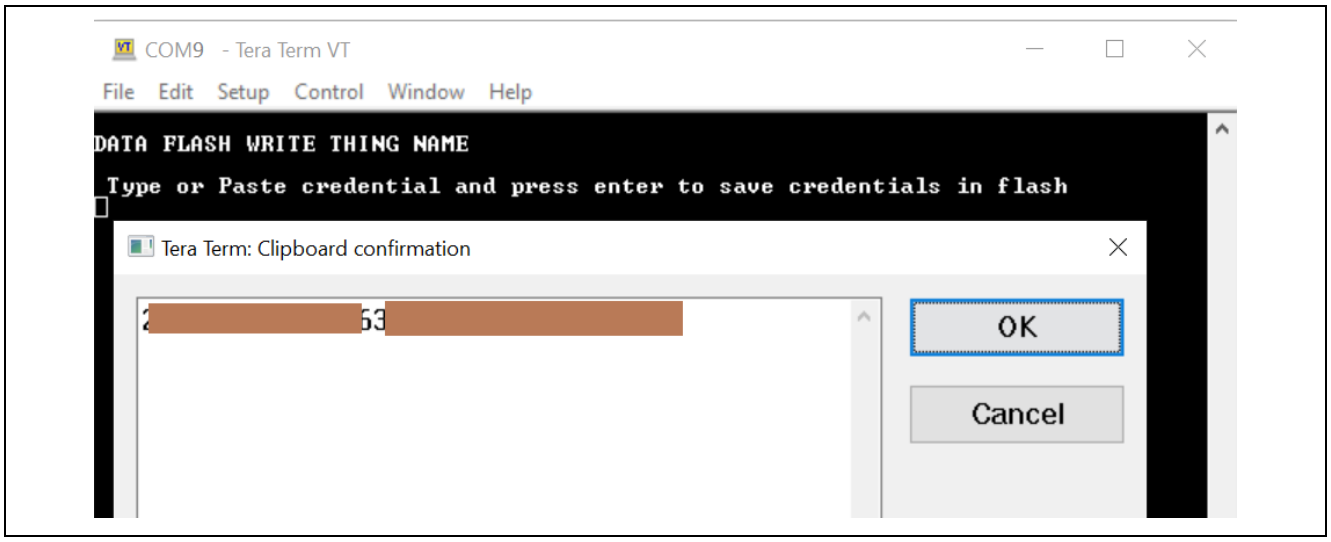

Figure 30. Storing the MQTT Endpoint into the Data Flash

6. Press option **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 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.

2.5 Storing the SSID Name, Password and Security Option

SSID Name, Password and Security option need to be stored in the data flash for the Wi-Fi connection of application.

1. Press '**4'** on the **Main Menu** to display **CONFIGURE Wi-Fi** related commands as shown in the snapshot below. This sub menu has commands to store and read the data.

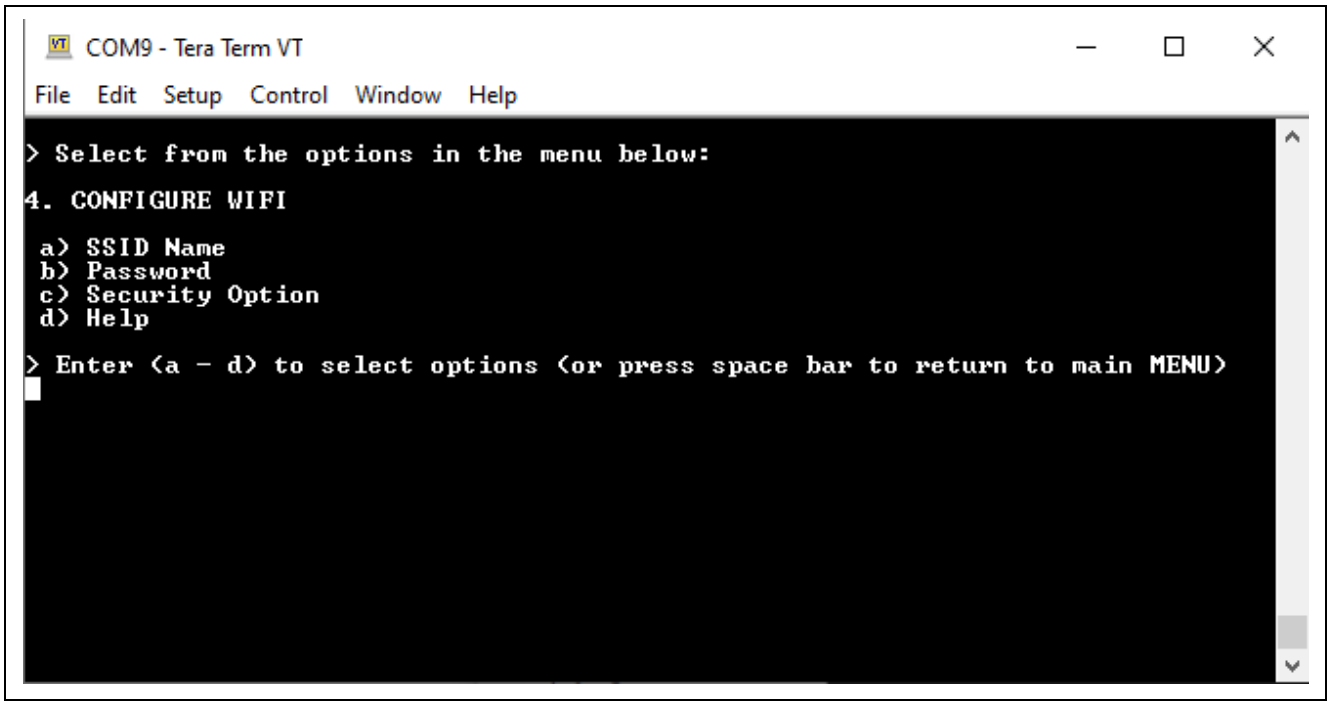

Figure 31. Configure Wi-Fi related Menu and Commands

2. To store the SSID Name, press the option **'a)** SSID Name' and input the SSID. The maximum length of SSID is 32 characters and the minimum length is 2 characters.

Note: For verify the input, click the **"Setup -> Terminal -> Local echo"** of the Tera Term as below.

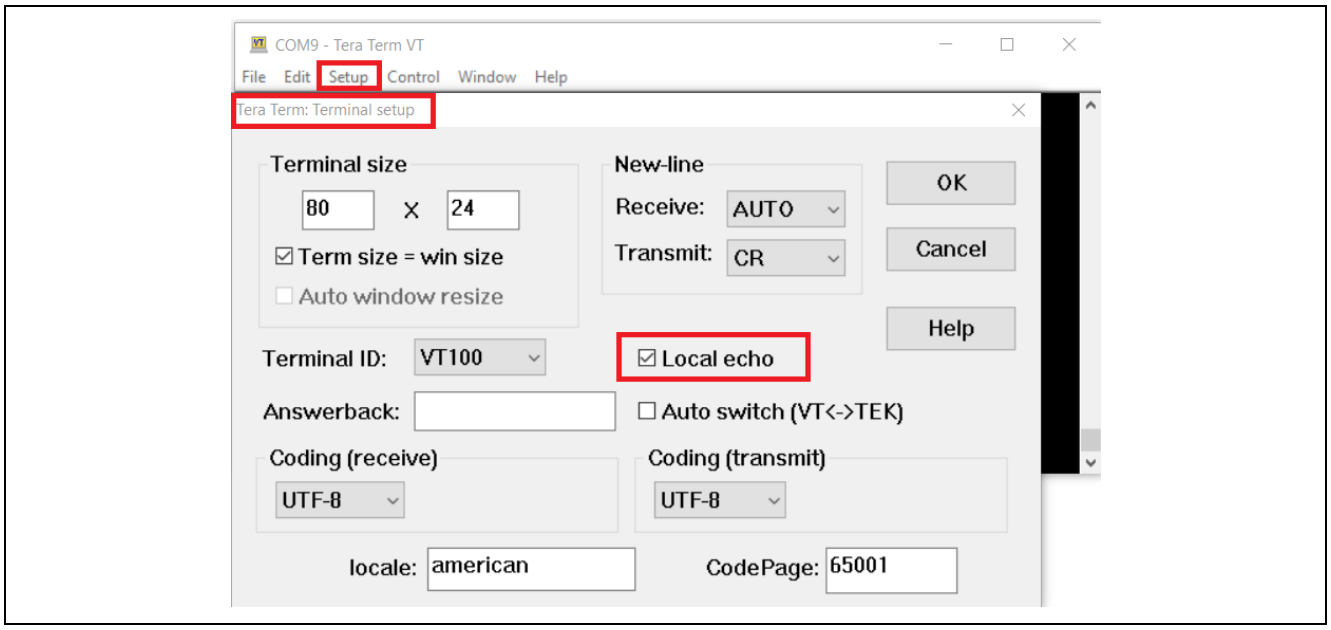

Figure 32. Terminal setup for the Local echo mode

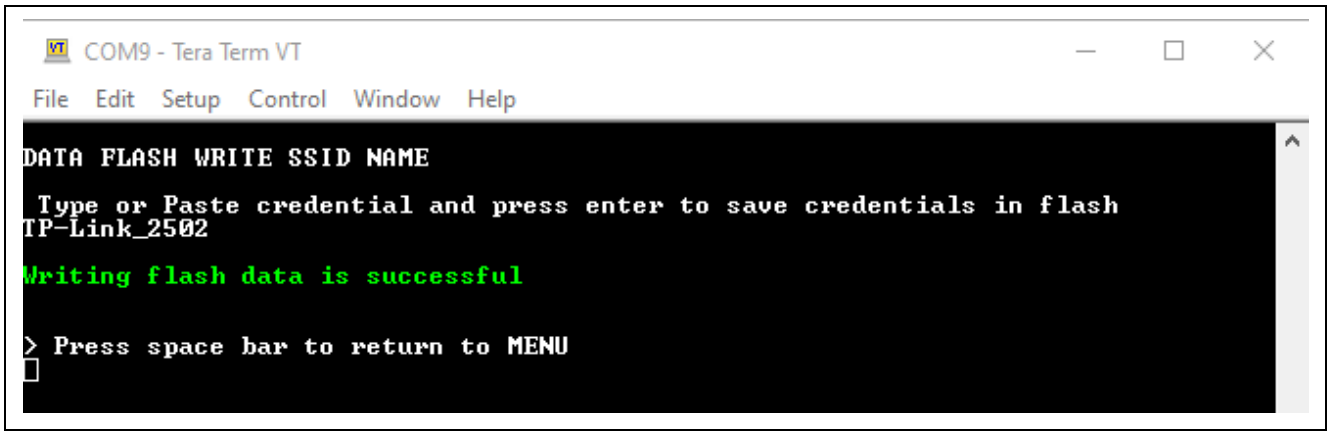

Figure 33. Storing the SSID Name into the Data Flash

3. To store the password, press the option **"b) Password"**, input the password, and confirm the valid string then press OK. The maximum length of password is 32 characters, and the minimum length is 1 character.

Figure 34. Storing the Wi-Fi password into the Data Flash

4. To store the security type, press the option "c) Security Option." The available options are **"a) None"** for **Open Wi-Fi**, **"b) WPA"** for **WPA security**, and **"c) WPA2"** for **WPA2 security.** The option should match the correct security settings for the Wi-Fi's configuration.

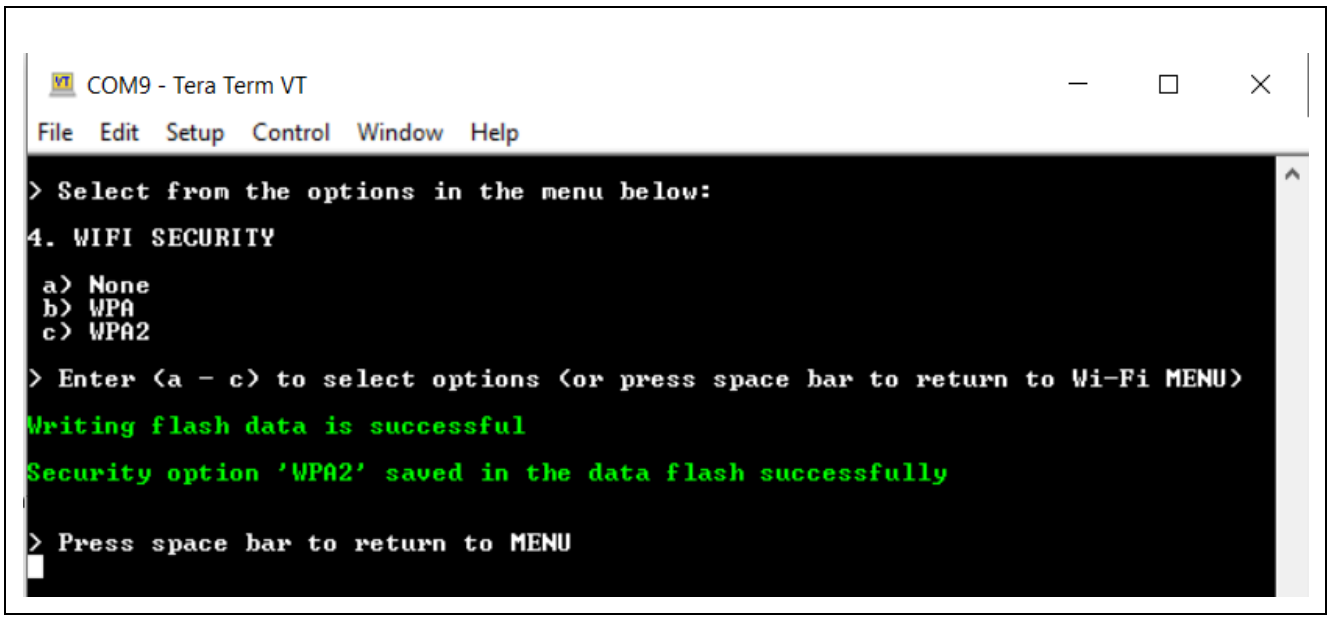

Figure 35. Storing the WPA2 security into the Data Flash

Note: Users can verify the information of Wi-Fi credentials stored in flash by going back to the “Main Menu” and choosing option “2. Data flash” > “f) Read Flash” or “g) Check credentials stored in flash memory” as described in step 6 in section 2.4.

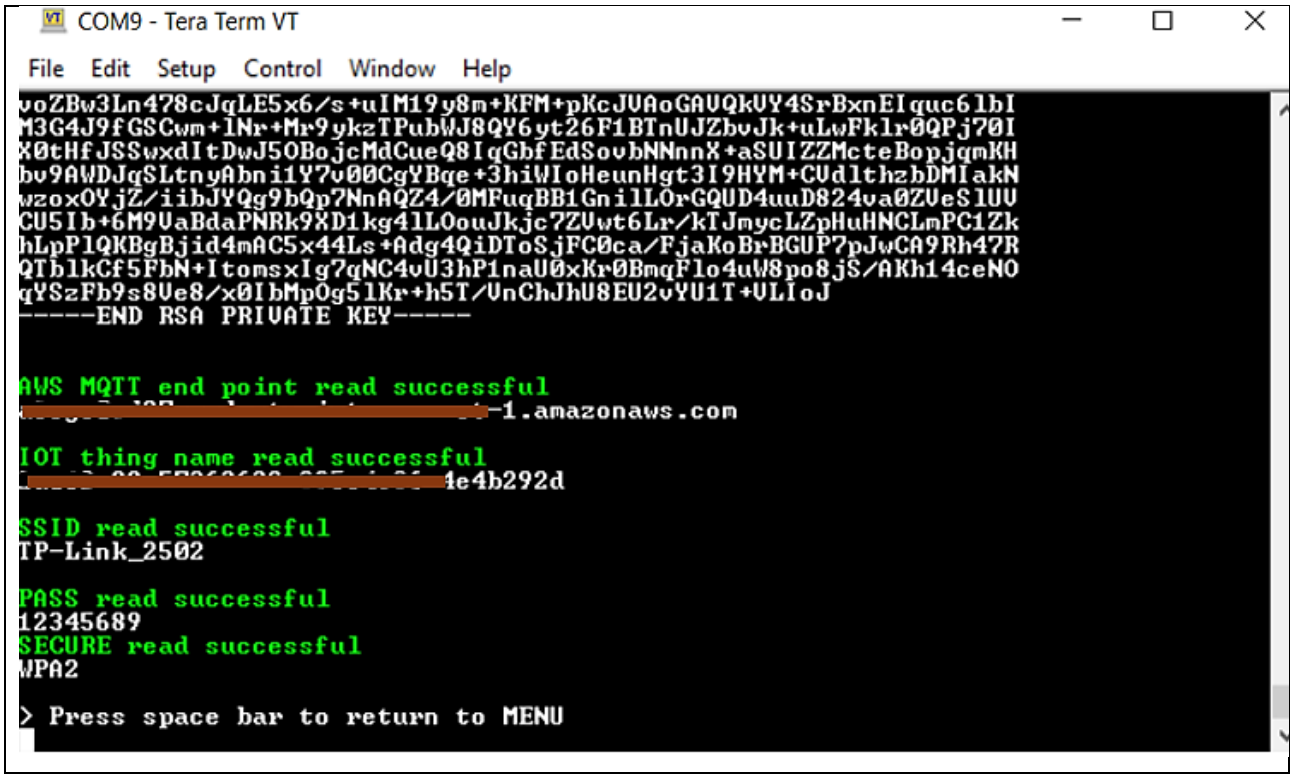

Figure 36. Checking Wi-Fi Credentials by Reading Flash

2.6 IoT Cloud Configuration and Connecting to AWS IoT

If you are first time user of the Application, Sign in to Renesas AWS dashboard at https://renesas.cloud-ra-rx.com/login using an email account that has not been used to sign up for AWS account previously.

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

Note: If you have used your aaaaa.bbbbb@ccccc.com email address earlier and still wants to use you email for AWS sign up and sign in, use aaaaa.bbbbb+zzzz@ccccc.com as new email and still you receive your invitation to your inbox.

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

2.7 Starting the Application

After registering to the Dashboard, configuring the required Cloud credentials and configuring the required Wi-Fi credentials through the CLI, the application is ready to run. Press option "**5. 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.

Note: If choosing "Open security" for Wi-Fi credentials, the application will not require the Wi-Fi password.

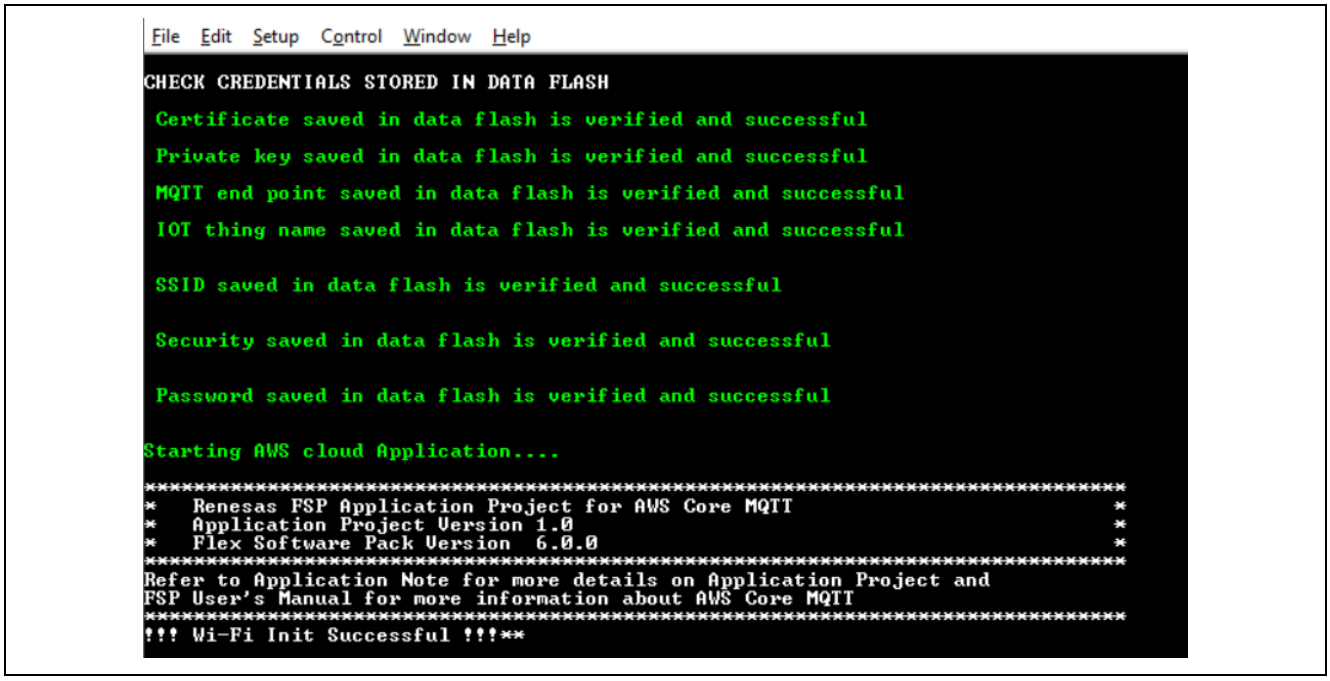

Figure 37. Welcome Screen on the Console

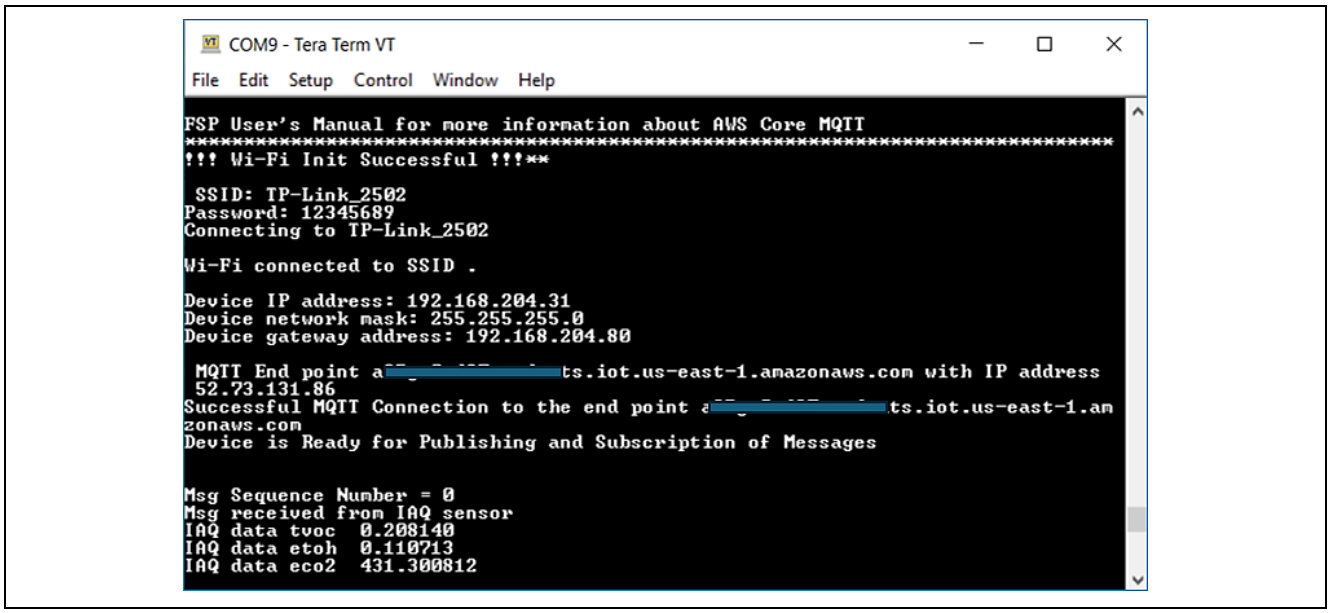

Figure 38. Connecting to the Network and AWS IoT

2.8 Verifying the Application Project from the Renesas Dashboard

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

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

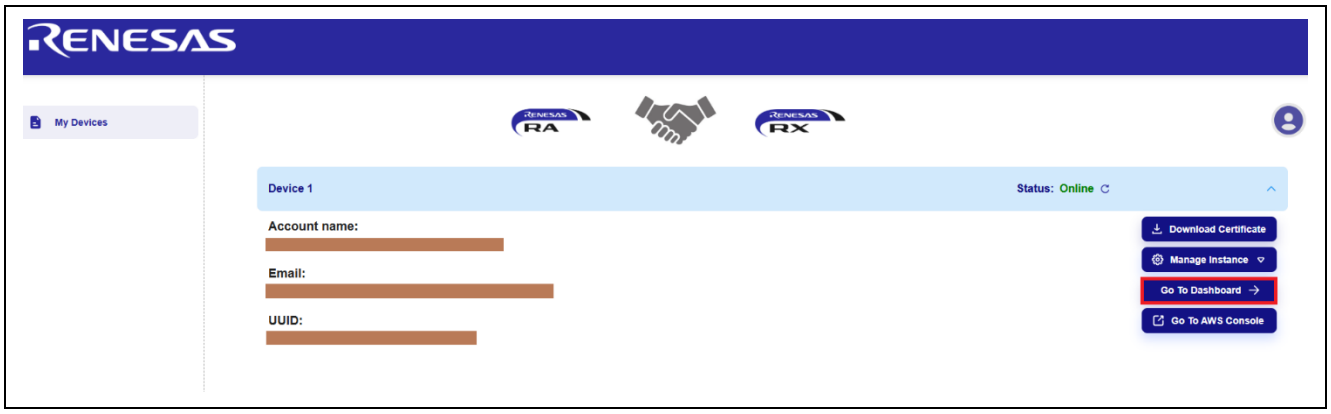

Figure 39. Accessing Renesas AWS Cloud Dashboard

The default ‘username’ is **admin** and default ‘password’ is **admin1234**.

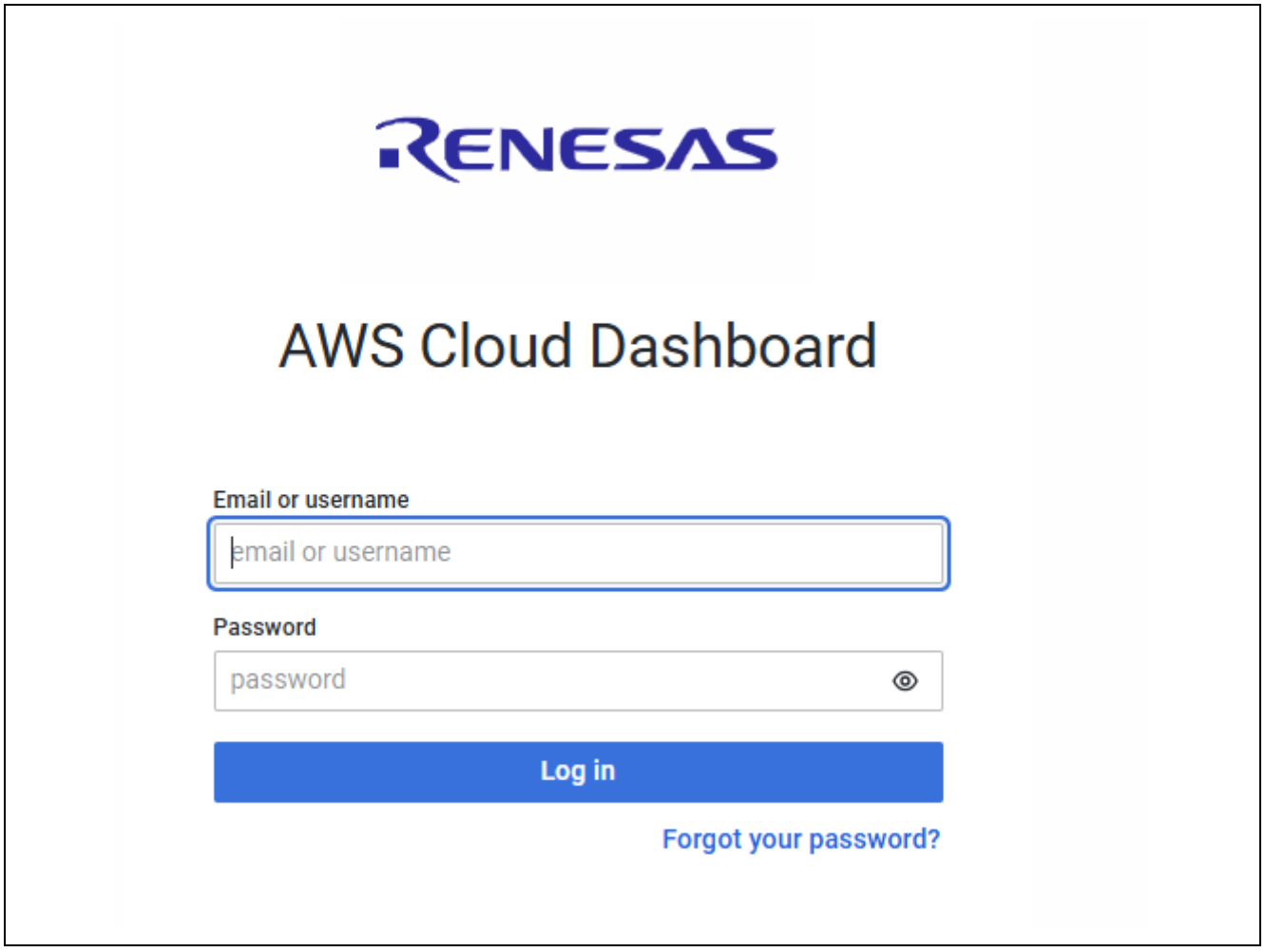

Figure 40. Welcome to Grafana Screen

On the Renesas dashboard page, the sensors 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.

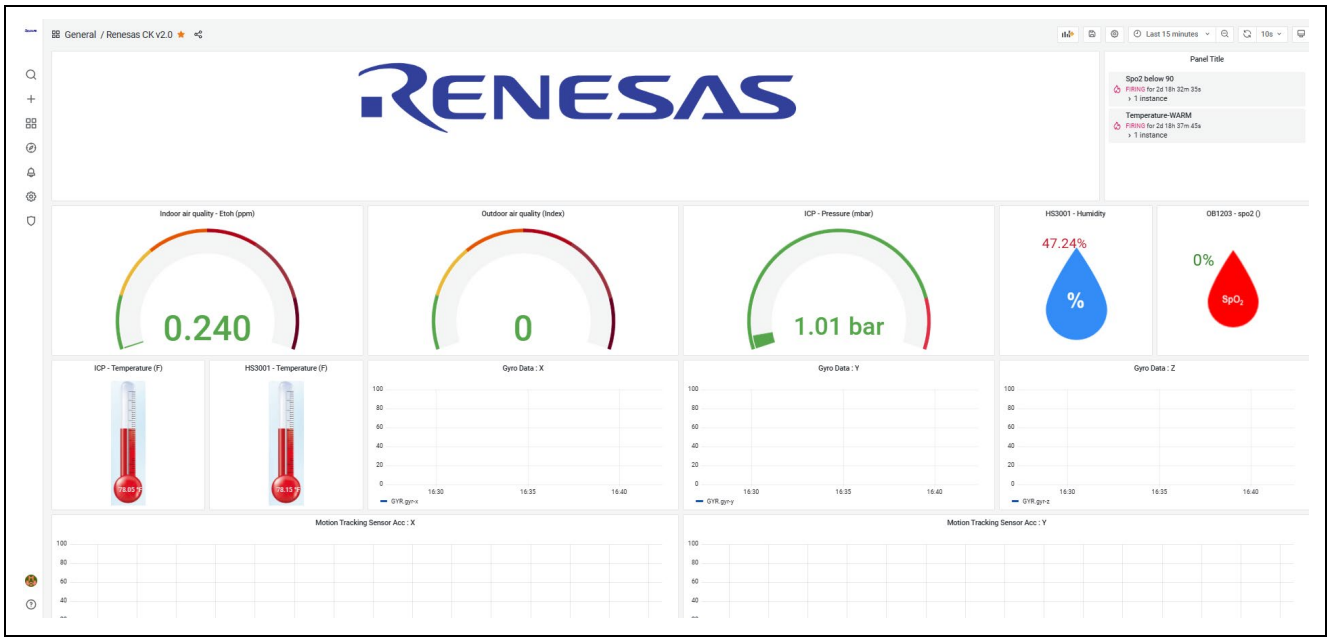

Figure 41. Renesas AWS Cloud Dashboard

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

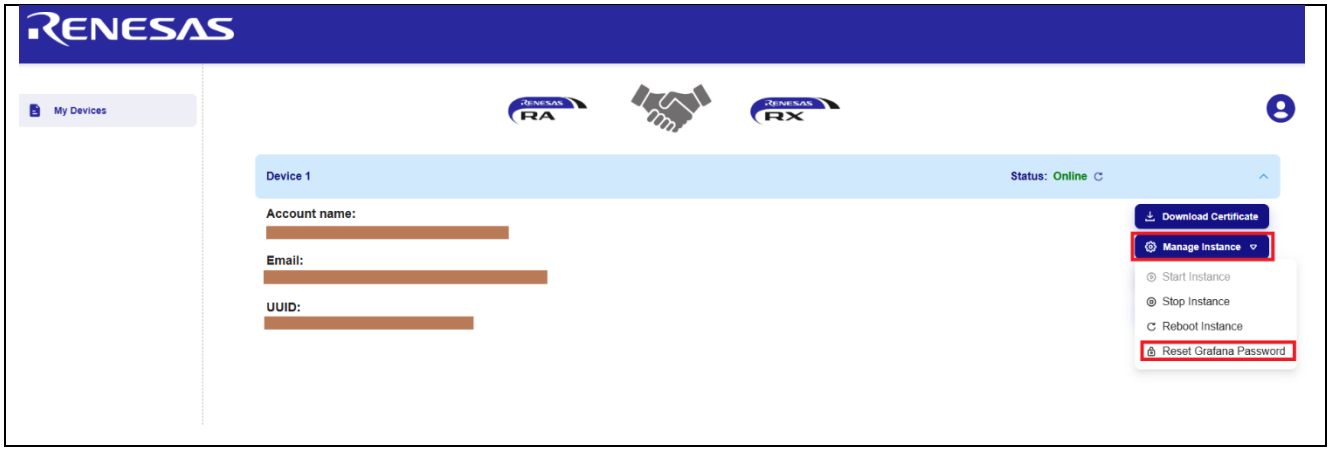

Figure 42 Grafana Password Reset

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.

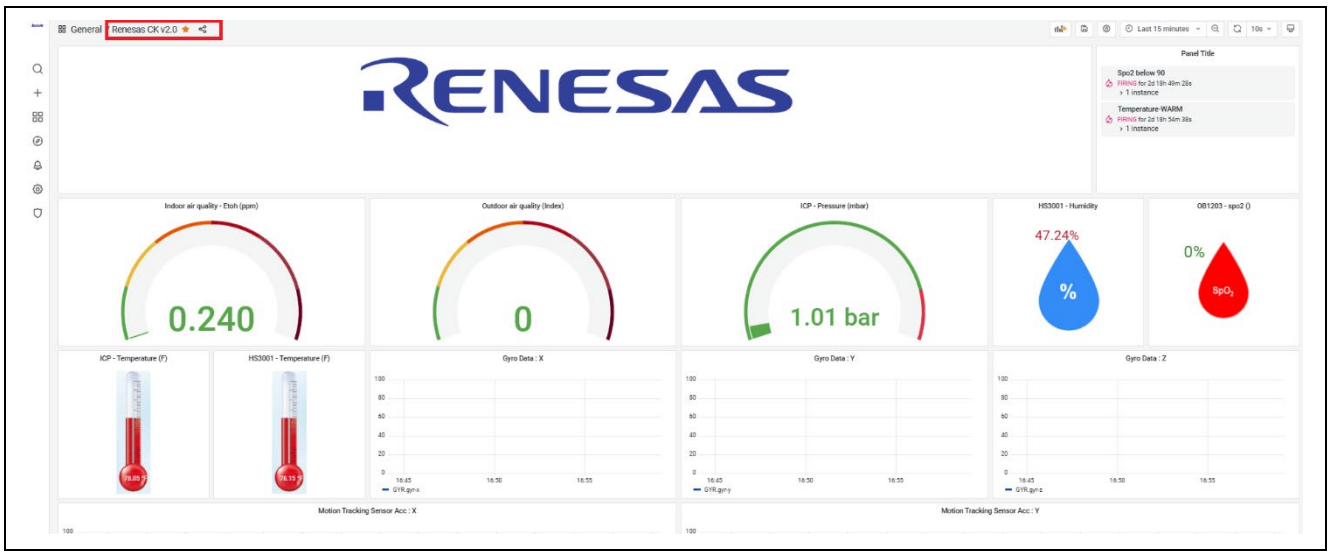

Figure 43. Renesas AWS Cloud Dashboard Types

Choose Renesas dashboards based on the cloud kit version.

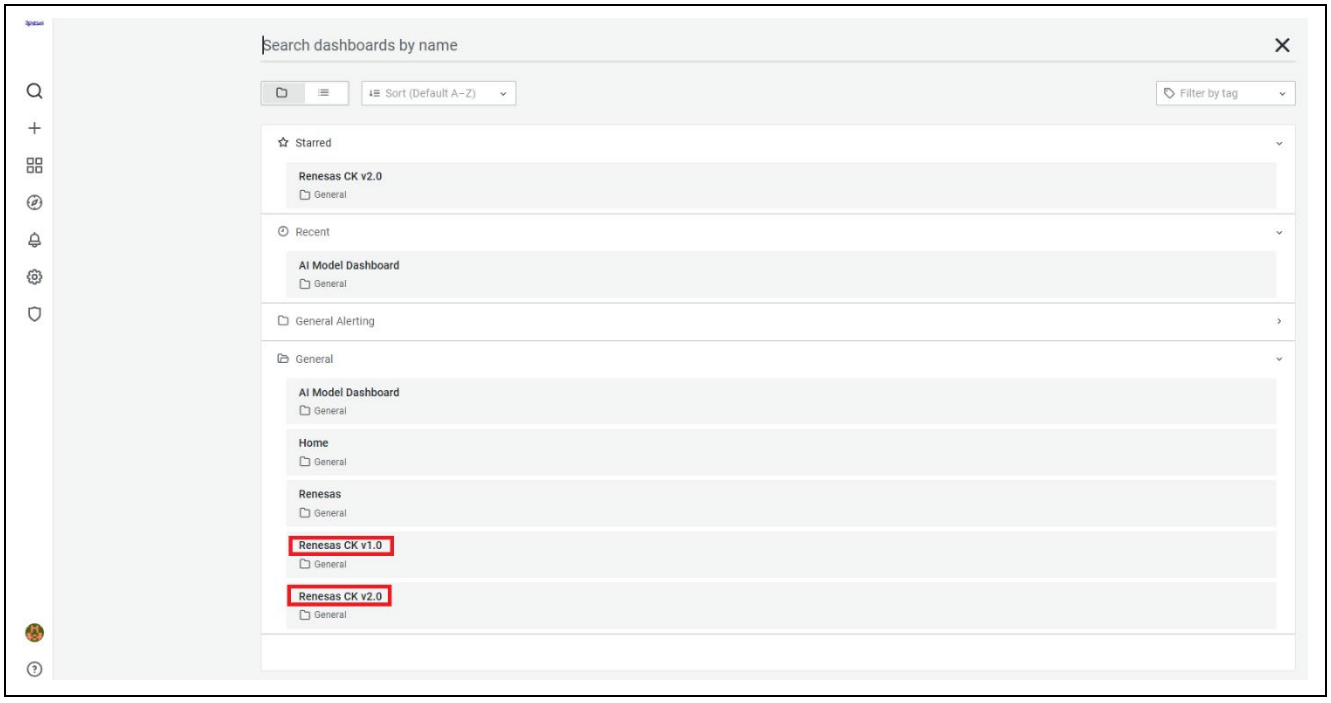

Figure 44. Choosing Renesas dashboards based on the cloud kit version

In CK-RA6M5 v2, only supports 6 Axis sensors (Gyroscope, Accelerometer), 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 Volatile Organic Compounds, mg/m^3
OB1203 - Heart Rate, Respiration Rate, Blood Oxygen Concentration, Pulse Oximetry,	SPO2, %
	HR (Heart Rate), bpm (beats per minute)
	RR (Respiration Rate), breaths per minute
	P2P (Perfusion Index)
ICP20100 - 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)
	Mag Data, unit: mT
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 **10s** refresh rate to allow timely and frequent updates.

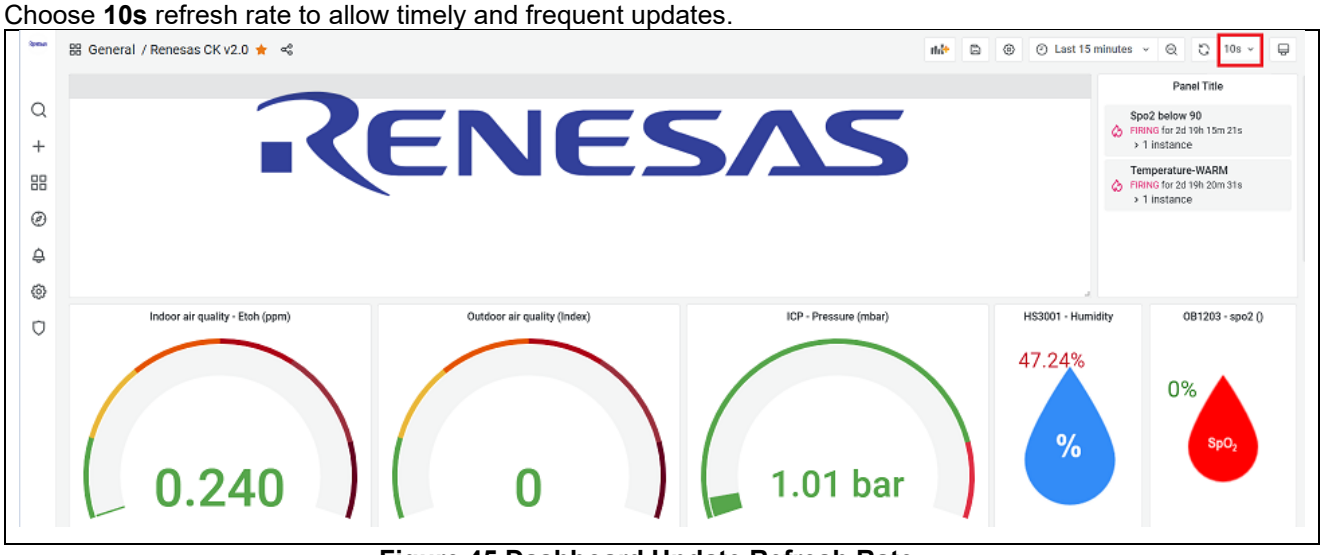

Figure 45 Dashboard Update Refresh Rate

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 range from 65 to 85
  - Temperature – Hot: above 85

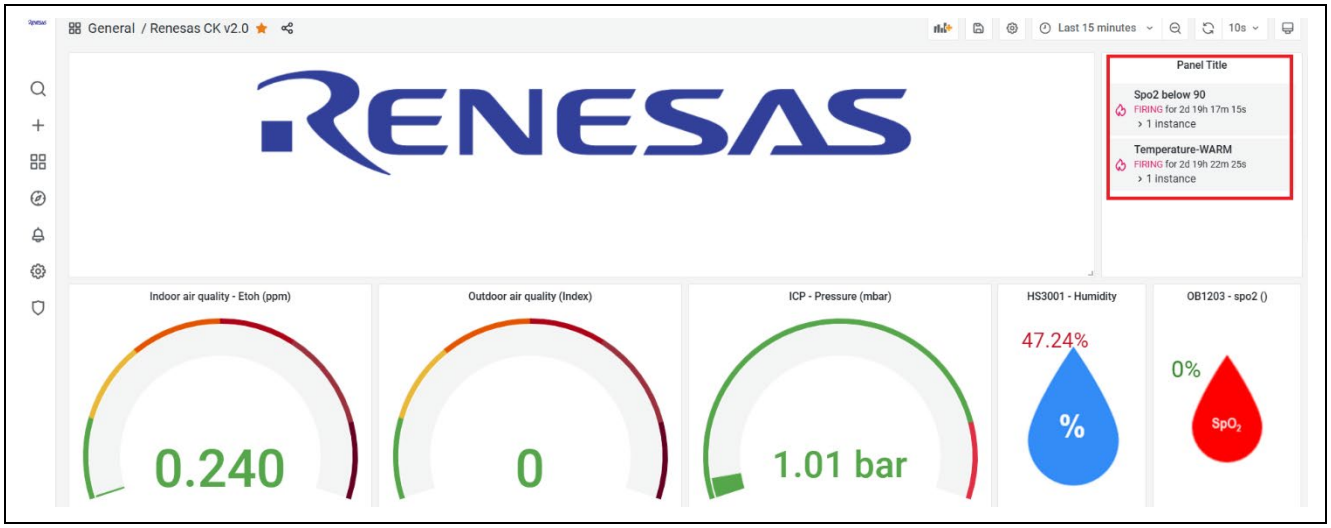

Figure 46. Sensor Status Feedback

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.**

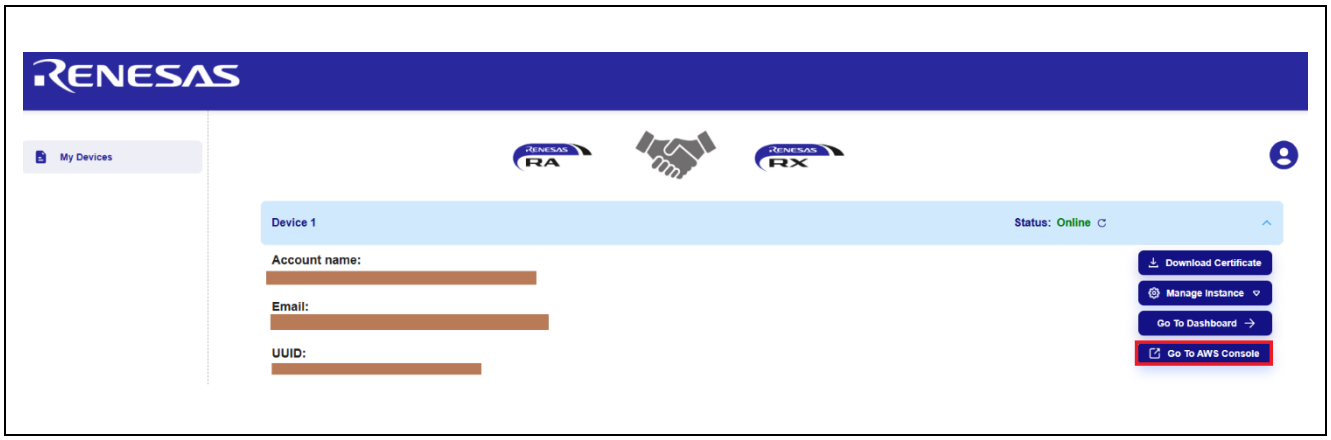

Figure 47. Accessing AWS Account from the Dashboard

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

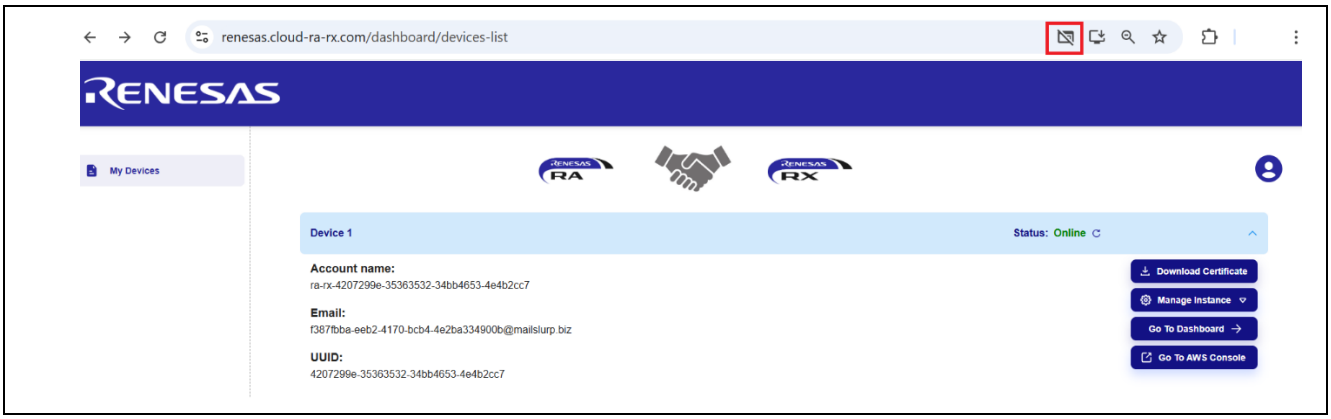

Figure 48. Pop Ups on the browser

After login you are redirected to AWS access portal page. The AWS sub account can be accessed from the AWSAdministratorAccess link.

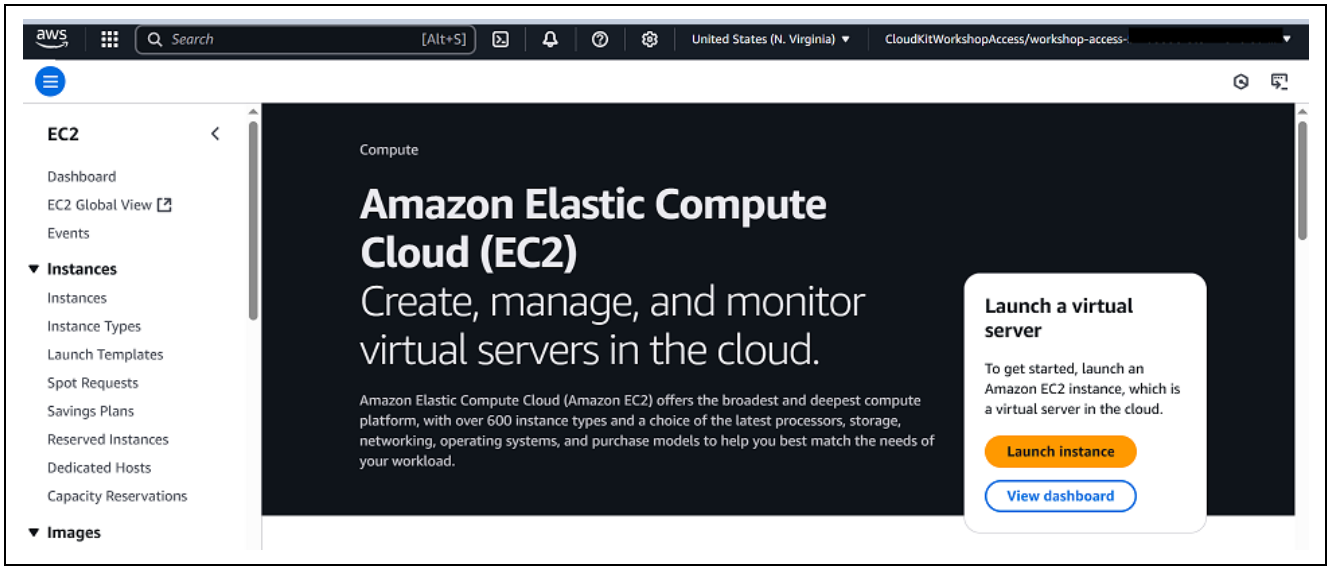

Figure 49. AWS account

6.1 Update payment options

Note: To avoid account from being quarantined when the $10 AWS credit is used up, payment information must be updated.

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

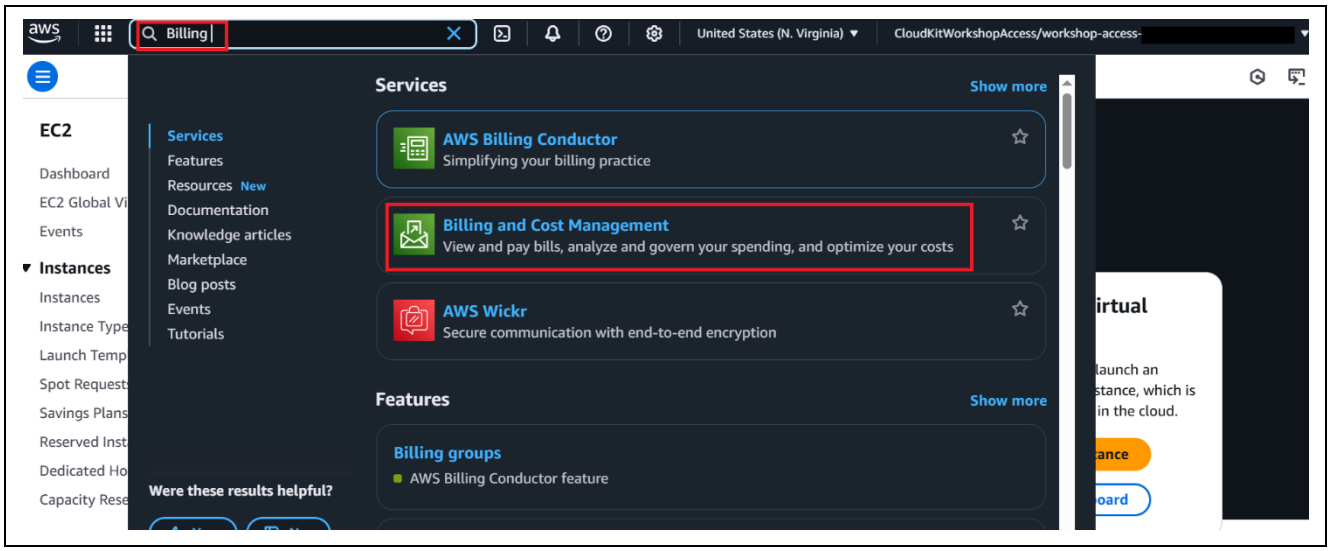

Figure 50. Billing and Cost Management

2. Scroll to the ‘Preferences and Settings’ section and click on ‘Payment Preferences’.

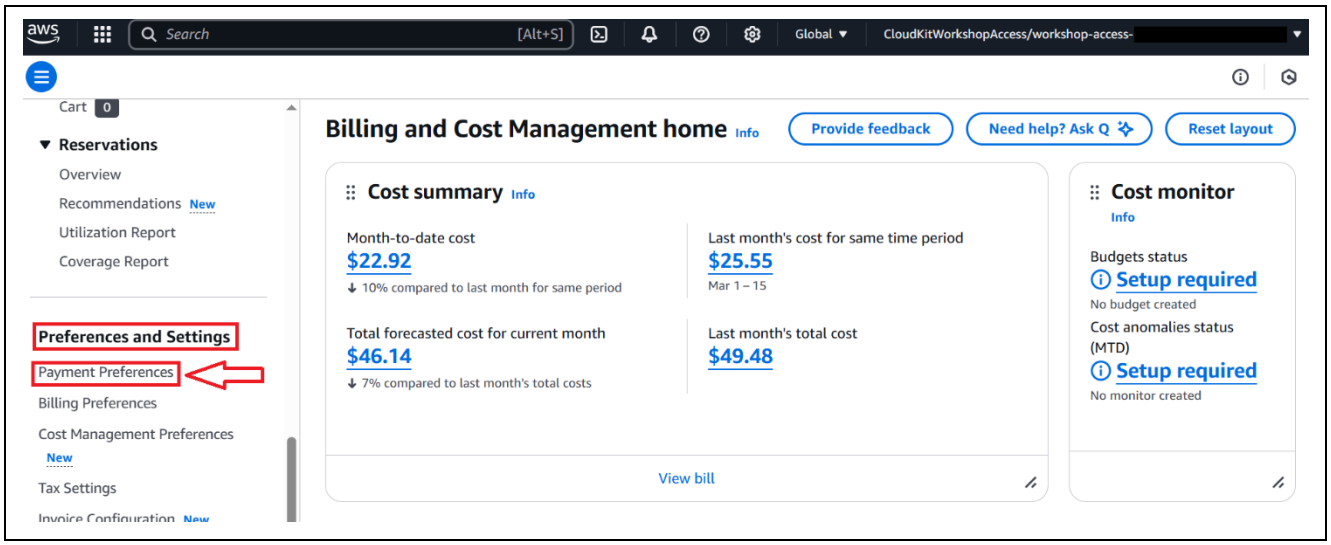

Figure 51. Payment Preferences

3. Add payment method.

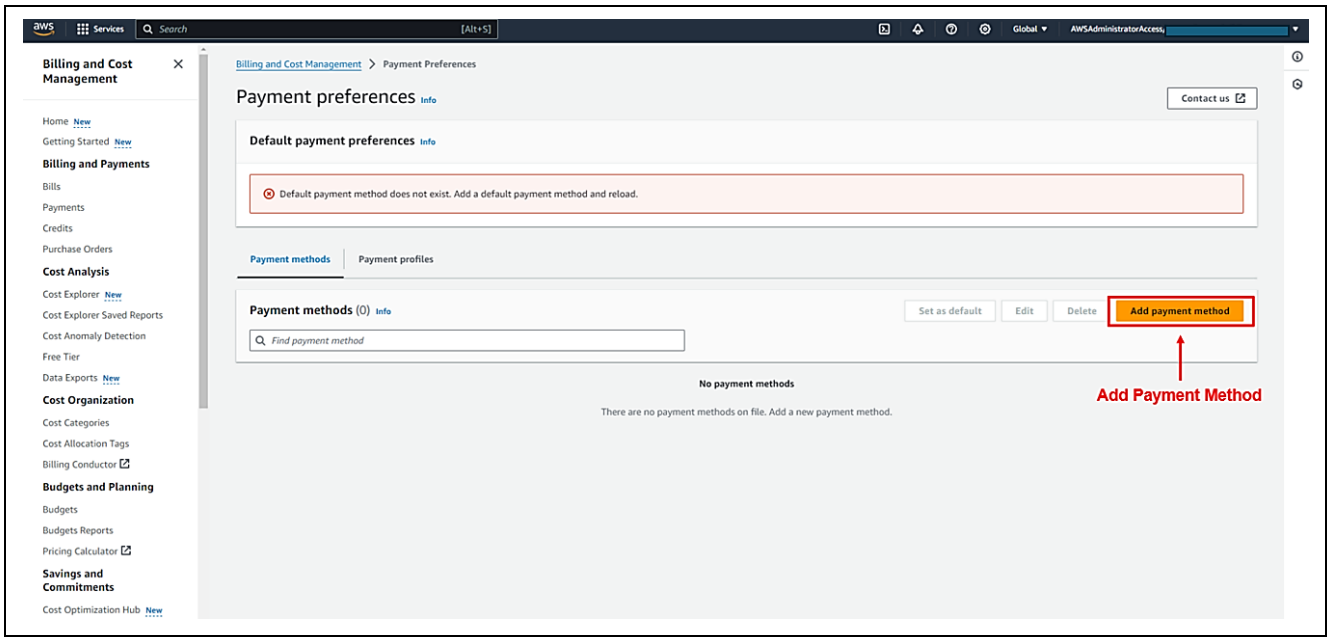

Figure 52. Add Payment Method

4. Go to ‘AWS Organizations’.

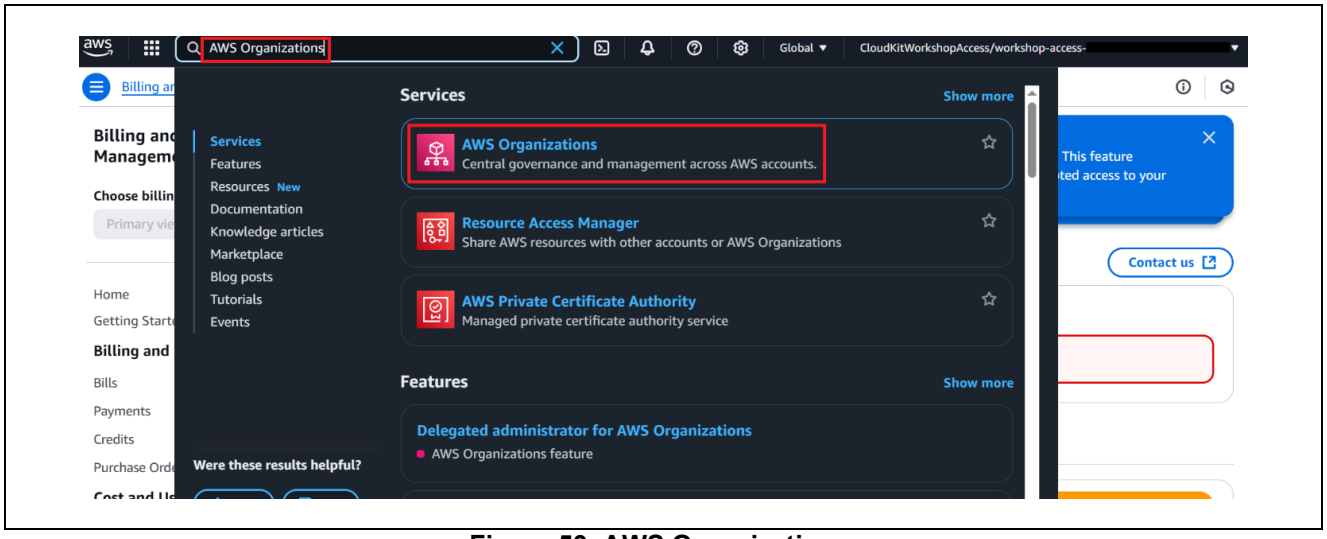

Figure 53 AWS Organizations

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

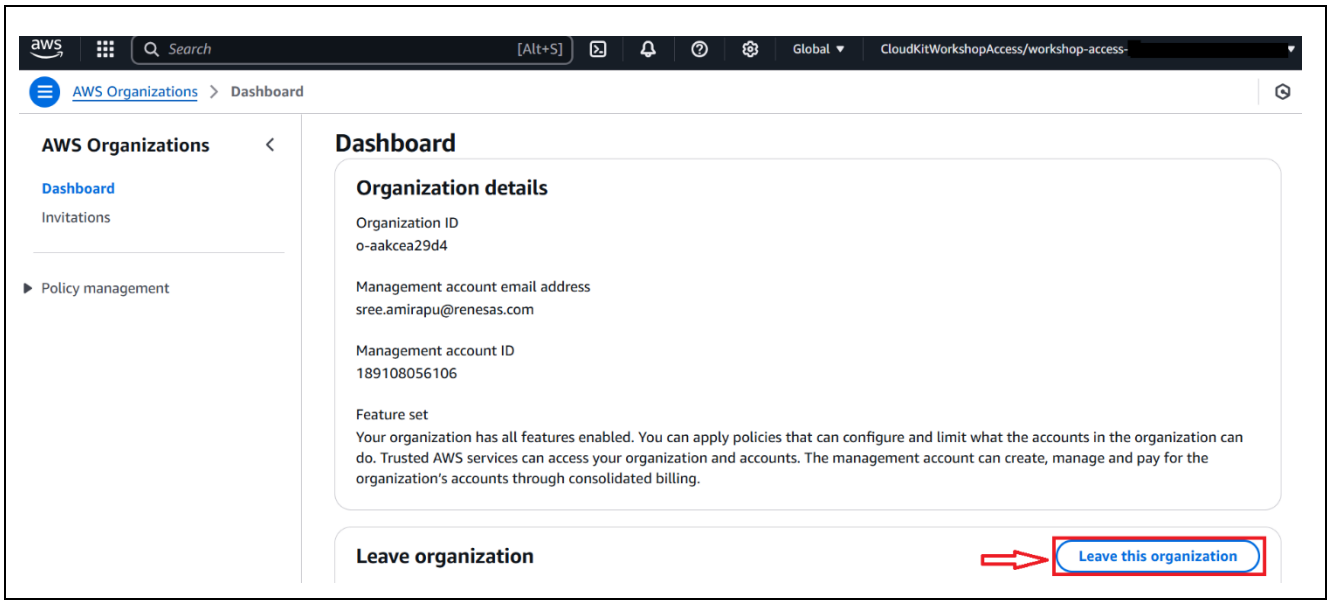

Figure 54 Leaving the organization

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

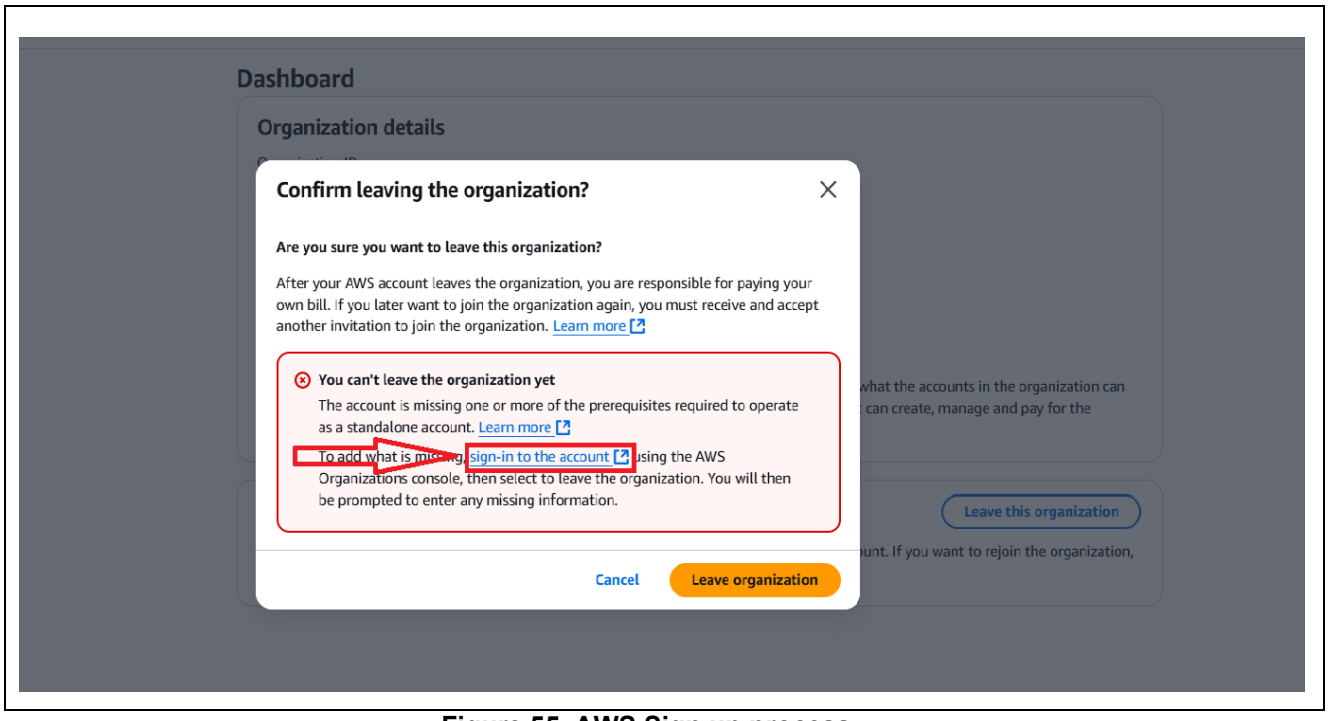

Figure 55 AWS Sign up process

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

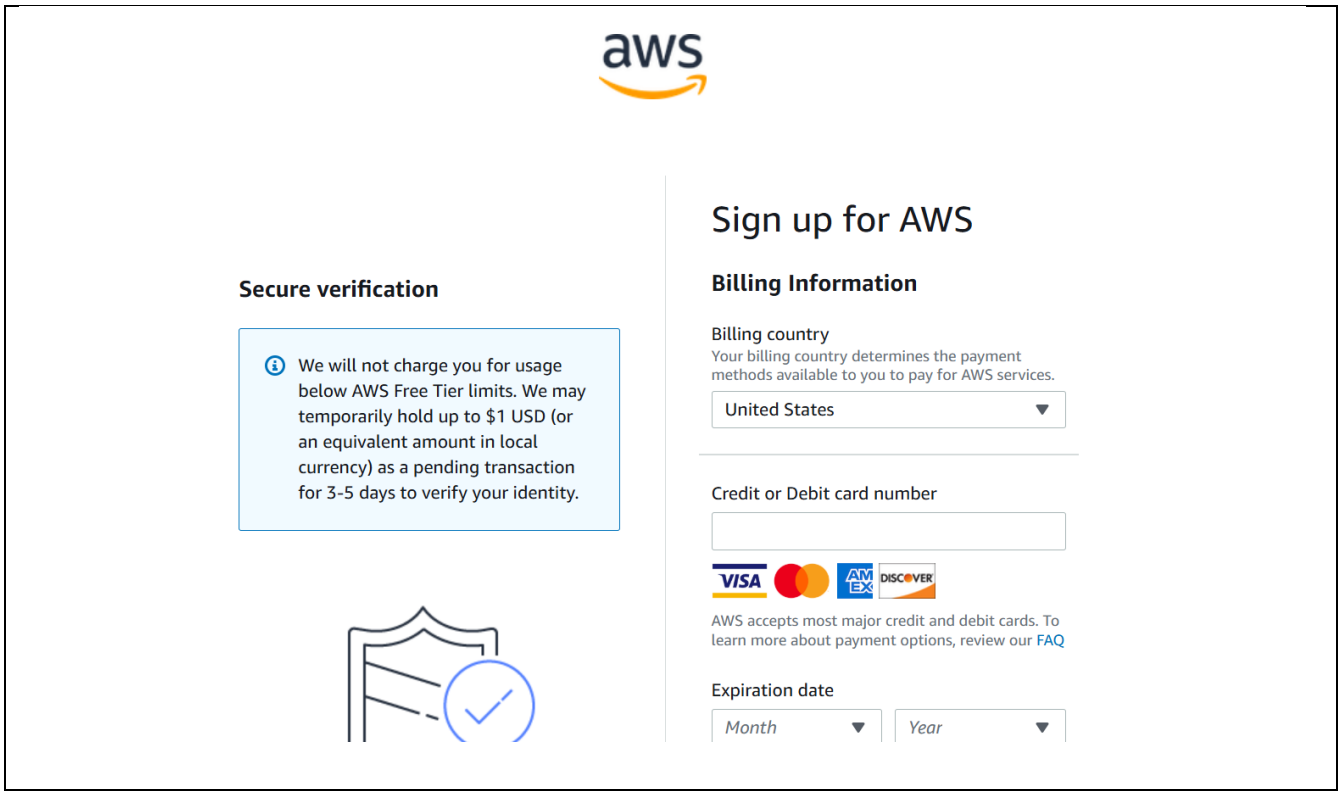

Figure 56 Prerequisites for leaving the organization

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.
2. In addition, the dashboard must be updated with the payment preference from the user profile on the dashboard page.
   A. Go to the user profile as shown in Figure 18.
   B. Update the payment preference.

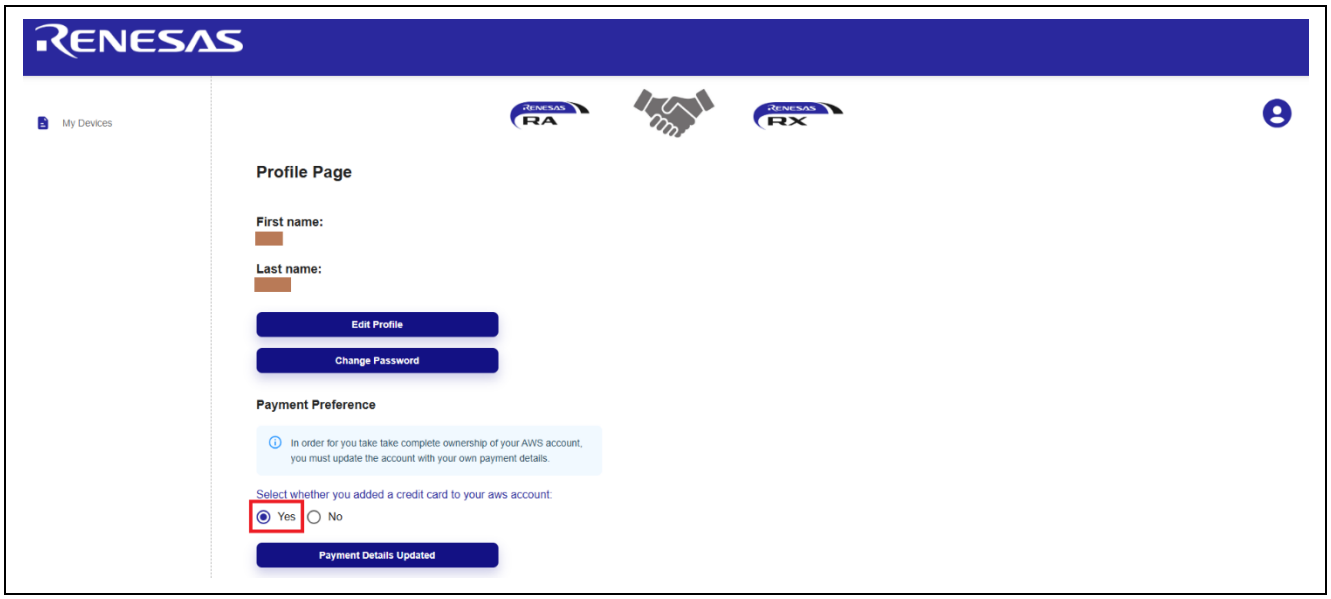

Figure 57. Payment Preference Update

Note: Failure to complete either of the steps 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.

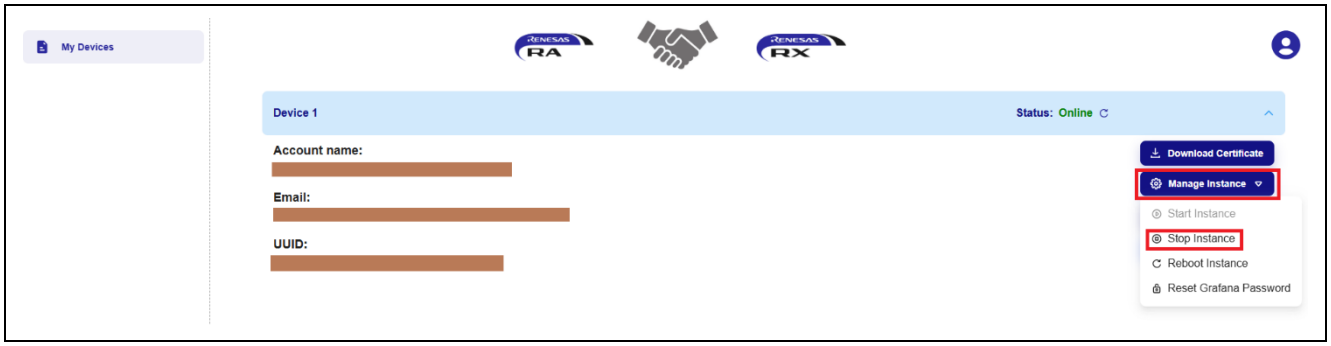

Figure 58. Stop EC2 instance

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

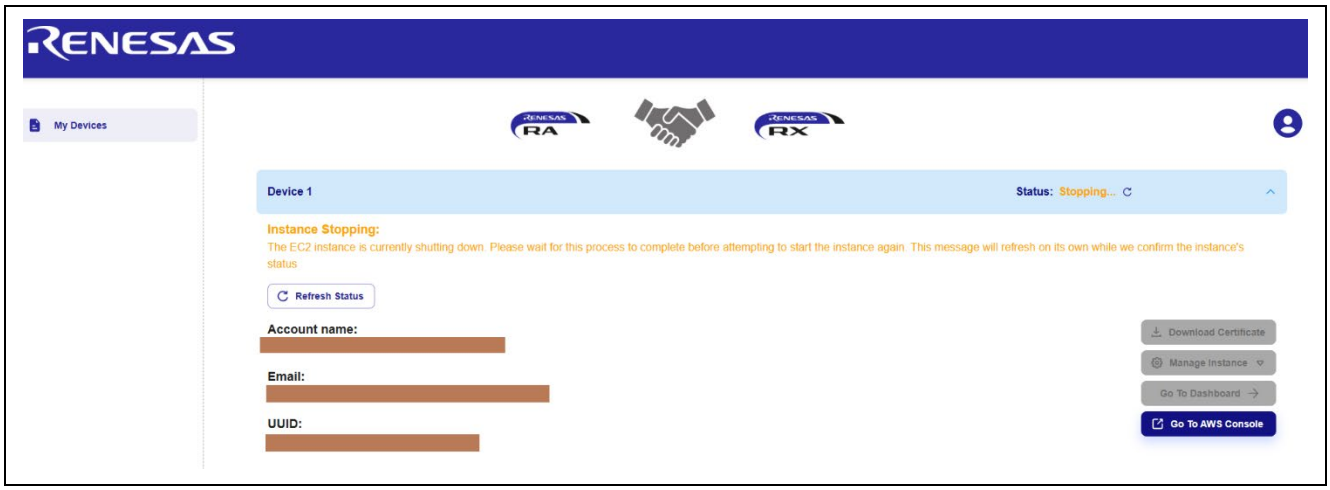

Figure 59. EC2 instance status

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

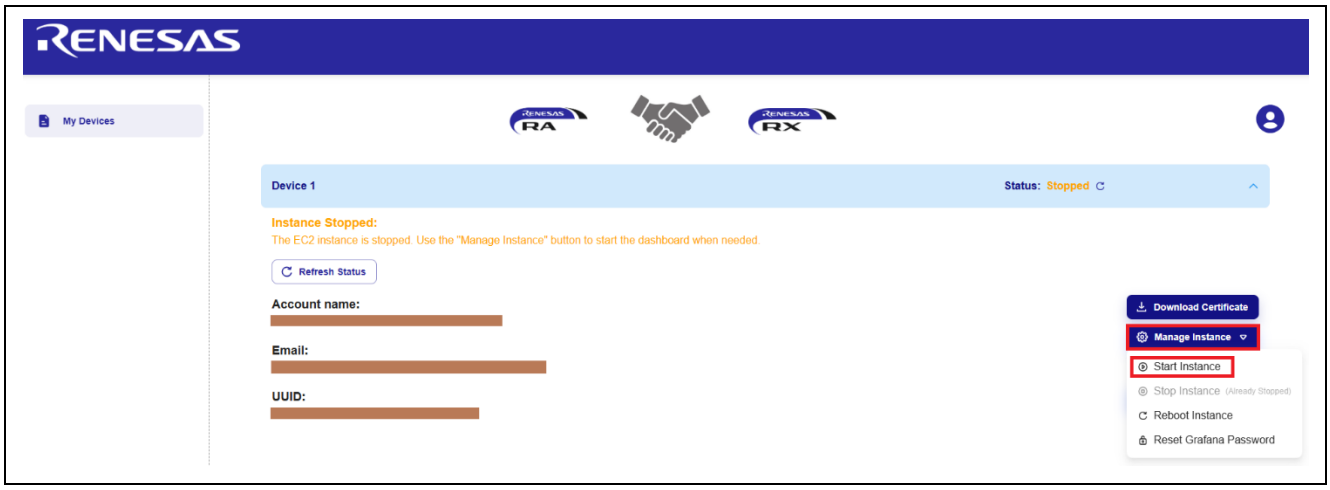

Figure 60. Restarting the EC2 Instance State

8. Sensor Stabilization Time

Table 2 gives the time required for the sensors to sense and provide the valid data to the users. Here you will see 2 columns, 1) when powered up for the first time 2) after soft or hard reset. If the system boots up from 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 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 data sheet.

Table 2. Sensor Stabilization Time

Sensor Name	When Powered 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 5 min
OB1203	Up to 20 min (After putting finger on sensor, it may take up to 60 seconds to sense data)	Up to 20 sec (After putting finger on sensor, it may take up to 60 seconds to sense data)
HS3001	Up to 30 sec	Up to 10 sec
ICP	Up to 30 sec	Up to 10 sec
ICM	Up to 30 sec	Up to 10 sec

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

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 to use the dashboard with Microsoft edge browser; it does not work properly with Google Chrome browser.
- In case the error related to `wifi_init(): "[ERR] In Function: wifi_init(),** Wi-Fi Init Failure **"` is seen on the console every time in spite of good Wi-Fi connectivity, it is recommended to check the SDK version in DA16600 PMOD. It is required to use DA16600 SDK v3.2.7.1 or later for the application to work correctly. To confirm DA16600 SDK version and update it, please refer guideline in DA16200/DA16600 SDK Update Guide
- When the application is running successfully, if the Wi-Fi connection goes down on the AP/router end, the application will not reconnect to the AP/Router. Reset of the Board is required in this case.
- Depending on security levels and configuration of Wi-Fi Router/Modem, sometimes the application may not connect to the network. Please try Simple AP or Hotspot using iOS/Android system.
- When running debug on e2studio, if the application is rerun multiple times, it might randomly occur issue with i2c communication of OB1203 sensor. Users need to reconnect the micro-USB cable (J10) to reset OB1203 sensor and run the application again.

10. Debugging

Enable the `USR_LOG_LVL (LOG_DEBUG)` macro in the application project for additional information of the error, during debugging.

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-RA6M5v2 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	Oct.19.23	—	Initial release
1.10	Dec.22.23	—	Updated to FSP 5.1.0
1.20	Sep.25.25Oct.03.24	—	Updated to FSP 5.3.0
1.30	Sep.25.25	—	Updated to FSP 6.0.0

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/.