Quick Start Guide

Security Starter Kit with Giant Gecko 11, Xbee3 and OPTIGA™ Trust M

Date: November 5, 2020 | Version 1.0
FINAL

CONTENTS

DEFINITION, ACRONYMS AND ABBREVIATIONS

Definition/Acronym/Abbreviation	Description
AWS	Amazon Web Services
LTE-M	Long Term Evolution for Machines
OTA	Over the Air
SSK	Security Starter Kit
RTOS	Real Time Operating System
SIM	Subscriber Identity Module
APN	Access Port Name
MQTT	Message Queuing Telemetry Transport
ARN	Amazon Resource Name

1 INTRODUCTION

1.1 Purpose of the Document

The Quick Start guide for Security Starter Kit with GG11, XBee3 and OPTIGA™ Trust M will showcase FreeRTOS & MQTT demo running on the Silicon Labs Giant Gecko Starter Kit, LTE-M Expansion Kit and the Infineon OPTIGA™ Trust M (shield2go) for secure communication between the End Node and Cloud. This demo also shows the integration of AWS IoT Core for provisioning, authentication, and secure communication over LTE-M connectivity.

1.2 Prerequisite

This guide presumes that the below hardware is available to enable demonstration of FreeRTOS running on the Giant Gecko 11 Starter Kit, LTE-M Expansion Kit and OPTIGA™ Trust M security:

- SSK kit
  - Silicon Labs Giant Gecko 11 Starter Kit (SLEXP8021A)
  - Silicon Labs LTE-M Expansion Kit (SLSTK3701A)
  - Cellular SIM card (Hologram SIM – not shown)
  - LTE Antenna (not shown)
  - Infineon Shield2Go Cloud Security OPTIGA™ Trust M
  - Custom cable to connect OPTIGA™ Trust M board with the Giant Gecko 11 Starter Kit
  - Micro USB cable (required for power and communication with the Host PC
- HOST PC - Linux or Windows system

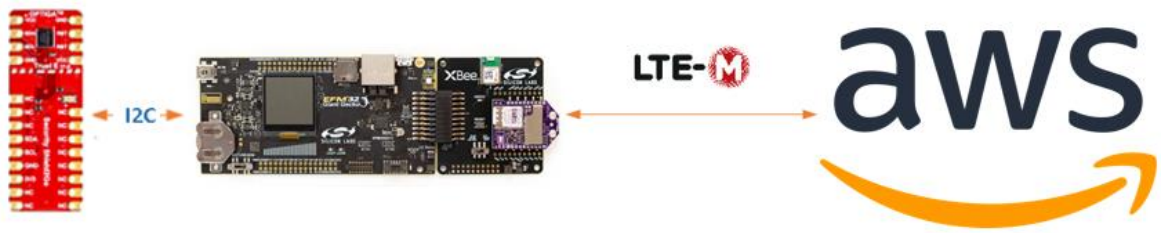


Figure 1: Hardware Architecture

2 INSTALLATION STEPS

2.1 Hardware setup

The Security Starter Kit with GG11, XBee3 and OPTIGA™ Trust M has been shipped pre-configured and assembled for proper operation.

If this is not a new kit right out of the box, please refer to the GG11-LTE-M-SSK Developers Guid.pdf Section 2 for the proper hardware, software and SIM card configuration.
https://www.arrow.com/en/products/gg11-lte-m-ssk/arrow-development-tools

- Connect the Mini USB (Power Cable) cable from the Giant Gecko 11 Starter Kit to PC as shown for power & the Micro USB cable (Debug Cable) for serial console as shown below:

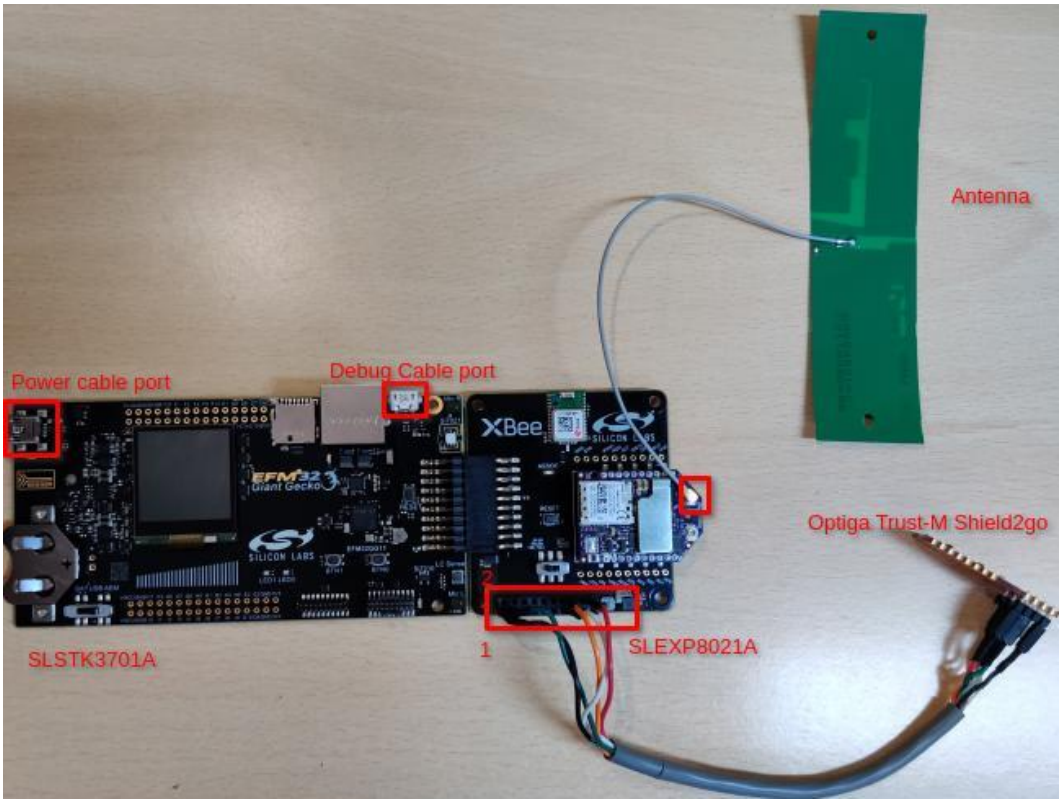


Figure 2: Hardware Setup

2.2 Software Setup

2.2.1 Setup Serial console on your PC.

For Linux:

1. Ensure **Minicom** is installed in Linux PC
2. Use Minicom on the Linux PC.

3. Open minicom serial setup window using below command

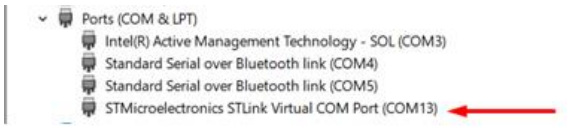
   Linux_PC:~$ sudo minicom –s

4. Set baud rate and other setting as per below
   - Baud rate = 115200
   - Data = 8 bits
   - Parity = none
   - Stop = 1 bit
   - Flow control = none
   - Serial device /dev/ttyACM0
   - save setup as dfl

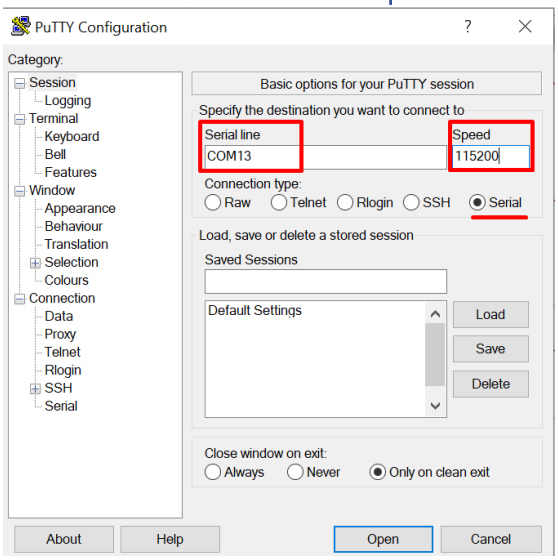
For Windows:

Use Putty for the windows PC.

1. Open the Host PC Device Manager and make note of the COM port assigned to the USB connection as shown below.



2. Launch Putty application, select the connection type: Serial, set the COM Port: (as noted in step #2), Speed: 115200 as shown below and click on "Open" button.



2.2.2 Power ON the GG11-LTE-M-SSK Board

Assuming that the Hardware is setup correctly and the SIM card is inserted in the slot, Power ON the board. The serial console will start showing logs as seen below.

```
Silabs Xbee3 LTE-M AWSFreeRTOS demo 2020 version 0.0.1
Please Enter Your Endpoint ARN
e.g- xxxxxxxxxxx-ats.iot.xx-xxx-1.amazonaws.com
Endpoint ARN_URL = a3vwfgdm06d0xb-ats.iot.us-west-2.amazonaws.com


Xbee LTE-M init done !

Initializing
............

Successful initialization of XBee Done

Attempting to apply
the new APN
The APN was already
set correctly!
.
Xbee3 info : Hardware Version:4b42, Firmware Version:11415, Baud Rate:115200, Connection:0.

Module IMEI:352753090127893
UID: 35:27:53:10:00:12:78:93
.

Wait for cell signal
.........
```

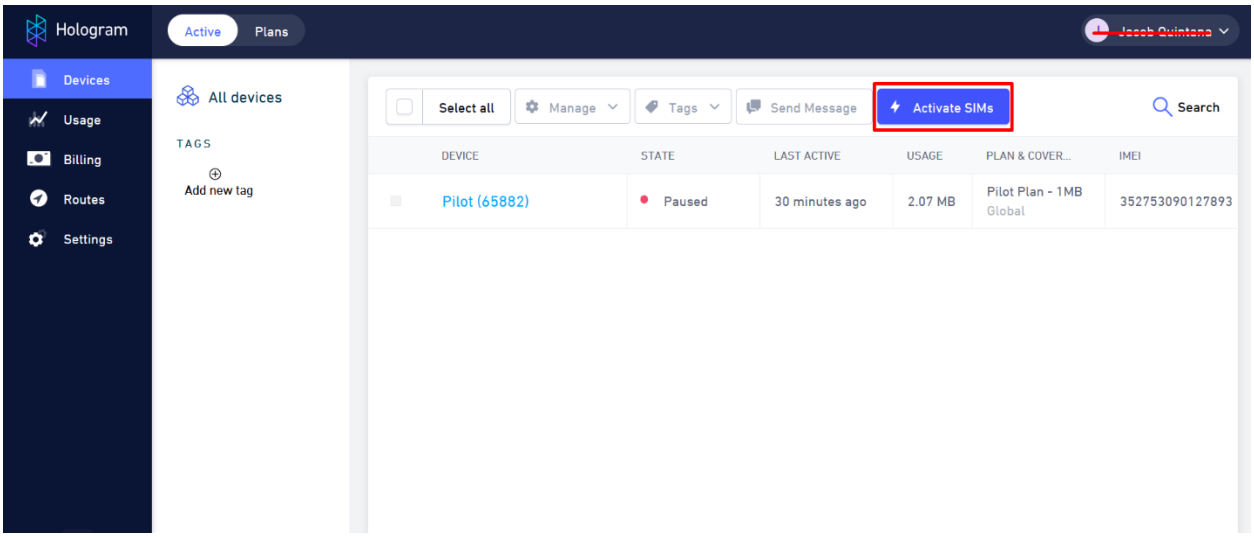
Important: Please make note of the UID highlighted in red above. This will be required when configuring the Security Starter Kit Cloud Connect Tool outlined in section 2.1.4.

2.2.3 Activate the included SIM card

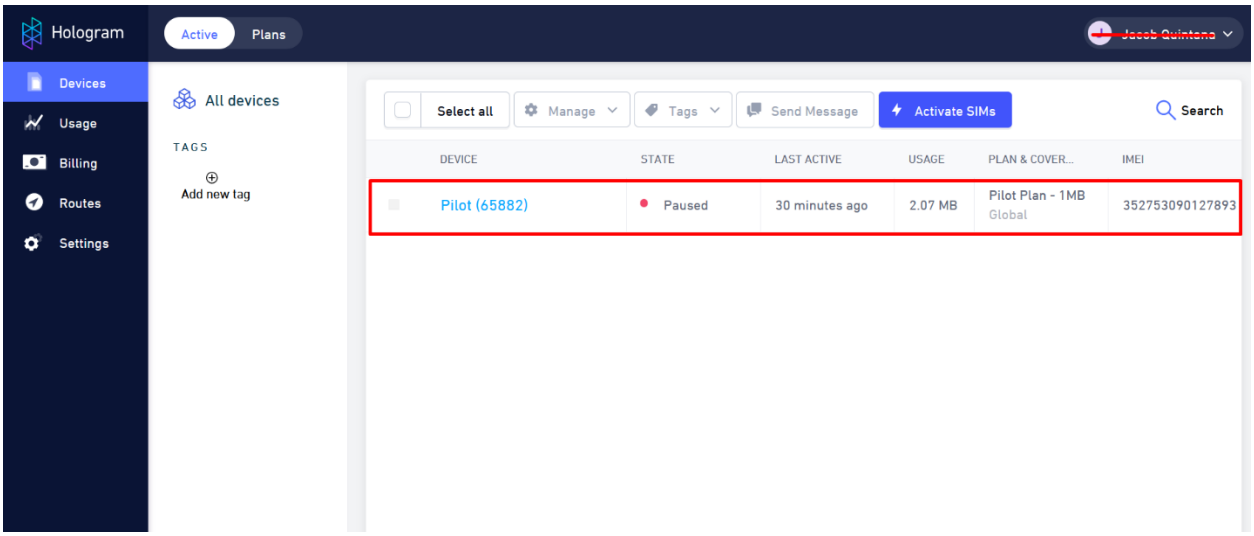
The included Hologram SIM card must be activated before it can be used with the DIGI® XBee3® LTE-M cellular module. This can be done by following these instructions:

1. In the browser, navigate to https://hologram.io/ and create a new account.

2. Once the account has been activated, navigate to https://dashboard.hologram.io/activate and follow the instructions to complete the activation of your SIM card.



3. After activation, the SIM card shows in list as shown below



[Note: The activation process will ask you to configure the SIM's APN to "hologram" with username and password empty. This will be done automatically through the demo on the EFM32GG11 STK.]

2.2.4 AWS Account creation and Arrow Cloud Connect tool configuration

The items mentioned below are specific to enabling AWS Cloud Services with the Security Starter Kit and only need to be completed once. The output from these configuration steps can be reused to connect other Security Starter Kits to AWS Cloud Services. These steps must be completed prior to running the included demo.

1. It is presumed that the user has an AWS Management Console account needed to complete the steps listed below. Otherwise you will need to create and account; https://aws.amazon.com/console/

2. Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

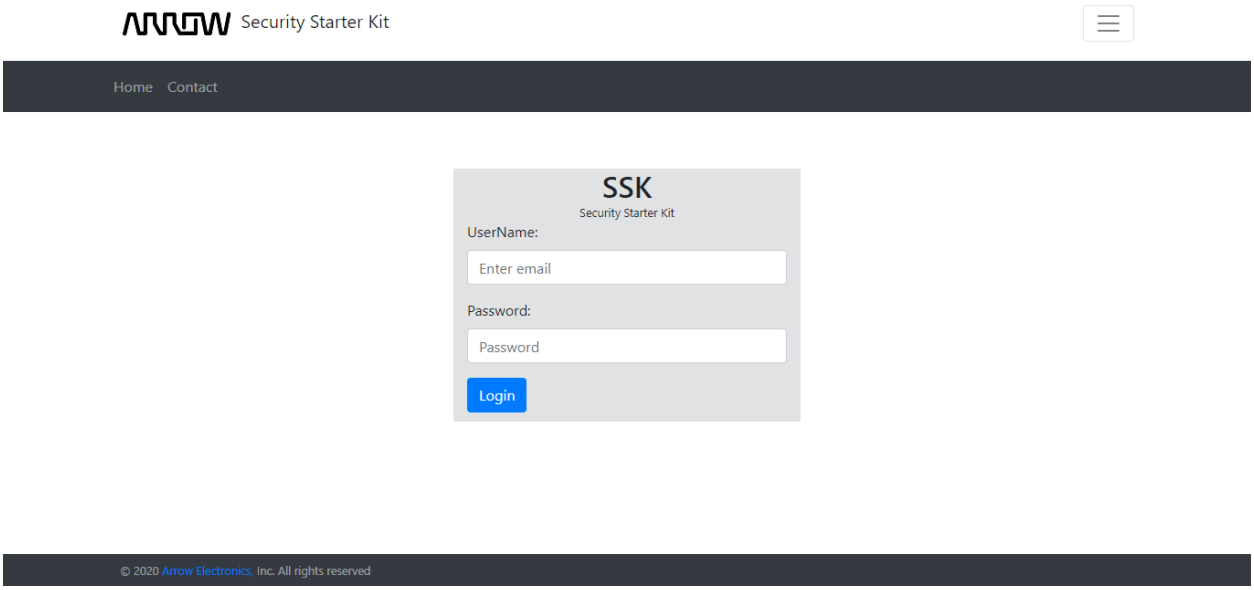
    - The user will need to configure a unique EC2 instance, which will provide a unique URL and login credentials tied to your AWS account, for the Arrow Cloud Connect Tool. The EC2 configuration instructions are outlined in SSK_Cloud_Connect Quick Start Guide.pdf ; https://www.arrow.com/en/products/gg11-lte-m-ssk/arrow-development-tools

3 DEMO SETUP

3.1 AWS FreeRTOS MQTT Demo configuration

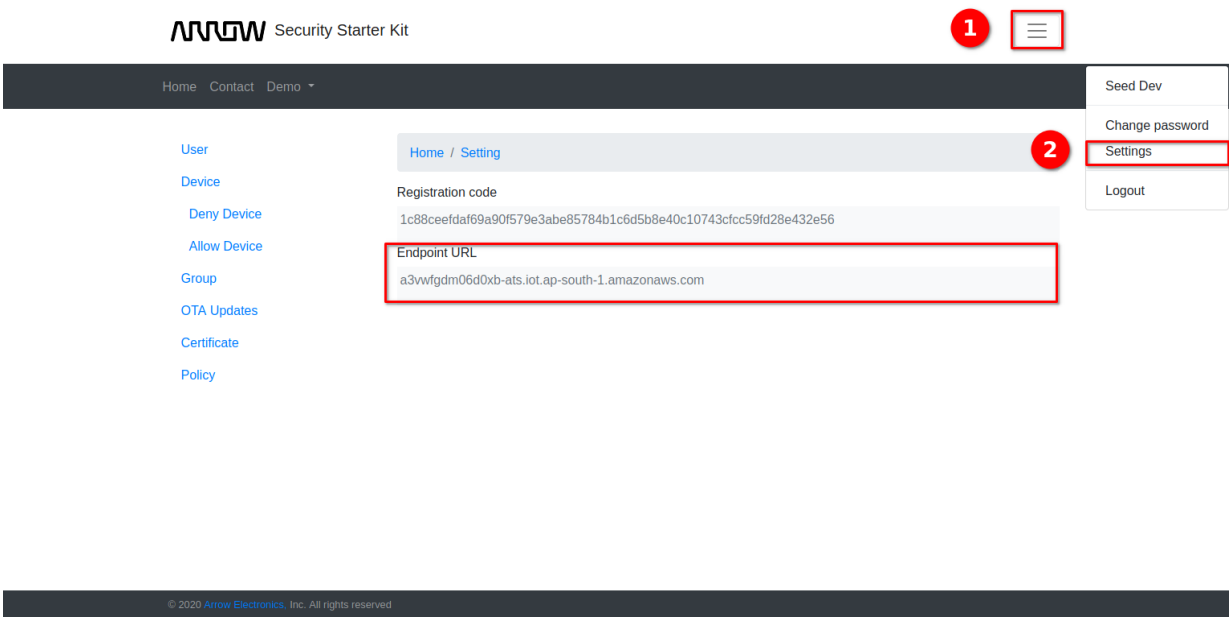
Note: It is presumed that user has successfully created their own AWS account and completed the creation of an AWS EC2 instance for the Cloud Connect Tool, as outlined in Section 2.1.4.

1. Enter the URL that was created during the configuration of the AWS EC2 instance, which is outlined in the SSK Cloud Connect Quick Start Guide
2. Login to the SSK Cloud Connect tool with your AWS Active Credentials, which were created when configuring your AWS EC2 instance.



1. Configure Endpoint URL into device and Collect device certificate

- Copy Endpoint URL from SSK Cloud Connect>> settings



- Press and hold the BTN0 button, while pressing the Reset on the SLSTK3701A board, then release.
- After “Resetting” the SLSTK3701A kit. It will ask to enter endpoint URL on Serial console screen as below.

```
Silabs Xbee3 LTE-M AWSFreeRTOS demo 2020 version 0.9.2
Please Enter Your Endpoint ARN
e.g- xxxxxxxxxxx-ats.iot.xx-xxx-1.amazonaws.com
Endpoint ARN_URL =                    -ats.iot.                .amazonaws.com
```

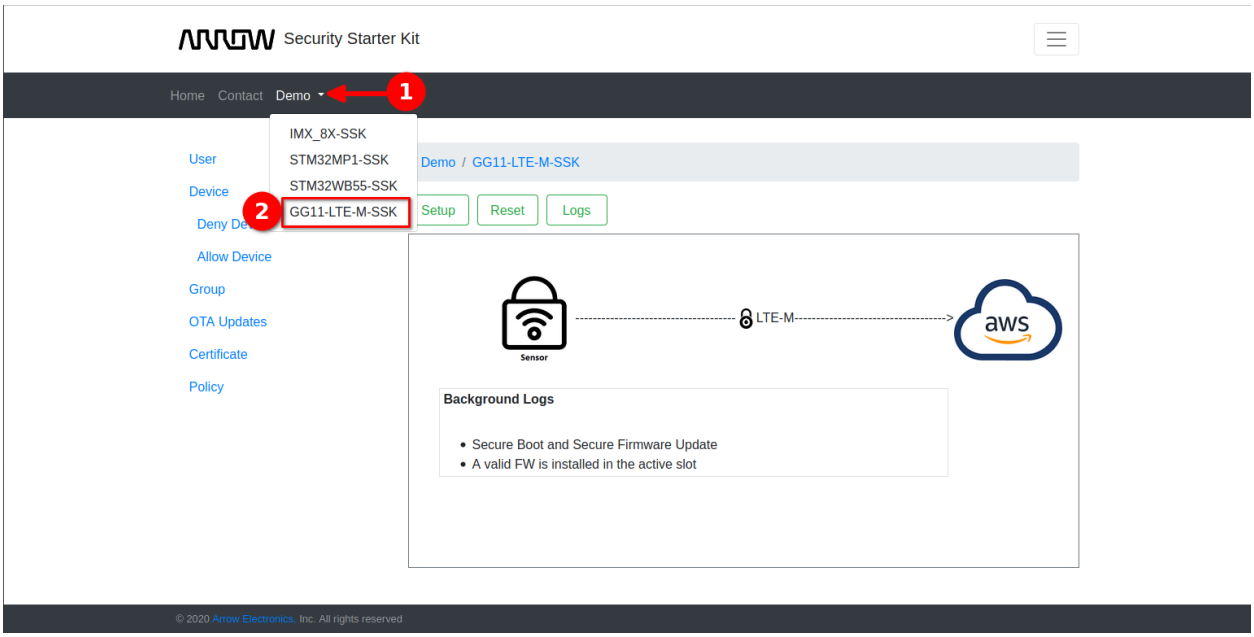
Paste the Endpoint URL here and press the “Enter” key on keyboard.

- Display the device certificate stored in OPTIGA™ Trust M, copy from serial console.

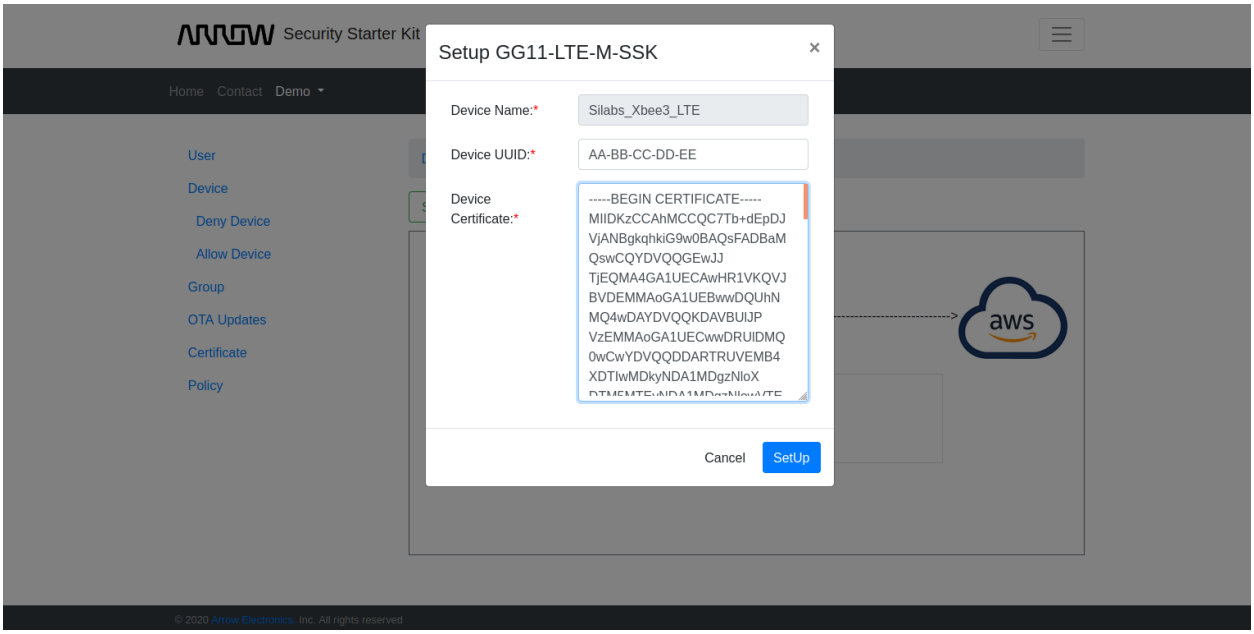
```
Silabs Xbee3 LTE-M AWSFreeRTOS demo 2020 version 0.9.2
Please Enter Your Endpoint ARN
e.g- xxxxxxxxxxx-ats.iot.xx-xxx-1.amazonaws.com
Endpoint ARN_URL = [redacted]-ats.iot.[redacted].amazonaws.com


Xbee LTE-M init done !

Initializing
............

Successful initialization of XBee Done

Attempting to apply
the new APN
The APN was already
set correctly!
.

Wait for cell signal
......
.........
.........
..........
..
cell signal available
-----BEGIN CERTIFICATE-----
MIIB2DCCAX6gAwIBAgIEbfa1qDAKBggqhkjOPQQDAjByMQswCQYDVQQGEwJERTEh
MB8GA1UECgwYSW5maW5lb24gVGVjaG5vbG9naWVzIEFHMRMwEQYDVQQLDApPUFRJ
R0EoVE0pMSswKQYDVQQDDCJJbmZpbmVvbiBPUFRJR0EoVE0pIFRydXN0IE0gQ0Eg
MTAxMB4XDTE5MDYxODA2MjgyM1oXDTM5MDYxODA2MjgyM1owHDEaMBgGA1UEAwwR
SW5maW5lb24gSW9UIE5vZGUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASz1W99
FiKdtwISAeUdz9+610NcUllgt3c3A4pfCXhwbfRqwOAKwq9NHUidbFh6DoYV72Nl
BeVwzRp+y+Pkh5u9o1gwVjAOBgNVHQ8BAf8EBAMCAIAwDAYDVR0TAQH/BAIwADAV
BgNVHSAEDjAMMAoGCCqCFABEARQBMB8GA1UdIwQYMBaAFDwwjFzViuijXTKA5FSD
sv/Nhk0jMAoGCCqGSM49BAMCA0gAMEUCIQCn4O7FfY2wTl1gSlKMN0Y6oArSwyZr
nZ7LzUrqp7loYwIgaeIKz82jhKr0YlDpnu0PquDSR558FkdAD5C9rMscF/M=
-----END CERTIFICATE-----

-------------- DEMO_RUNNER --------------
```

2. GG11-LTE-M-SSK Quick Demo Setup

- Go to SSK Cloud Connect.
- Open the GG11-LTE-M-SSK demo page. Go to SSK Cloud Connect >> Demo>> GG11-LTE-M-SSK.



- Click on “Setup” button.
- Enter UID Number and paste collected device certificate then click on “setup” button.



Successfully completed setup and it shows the message as below.

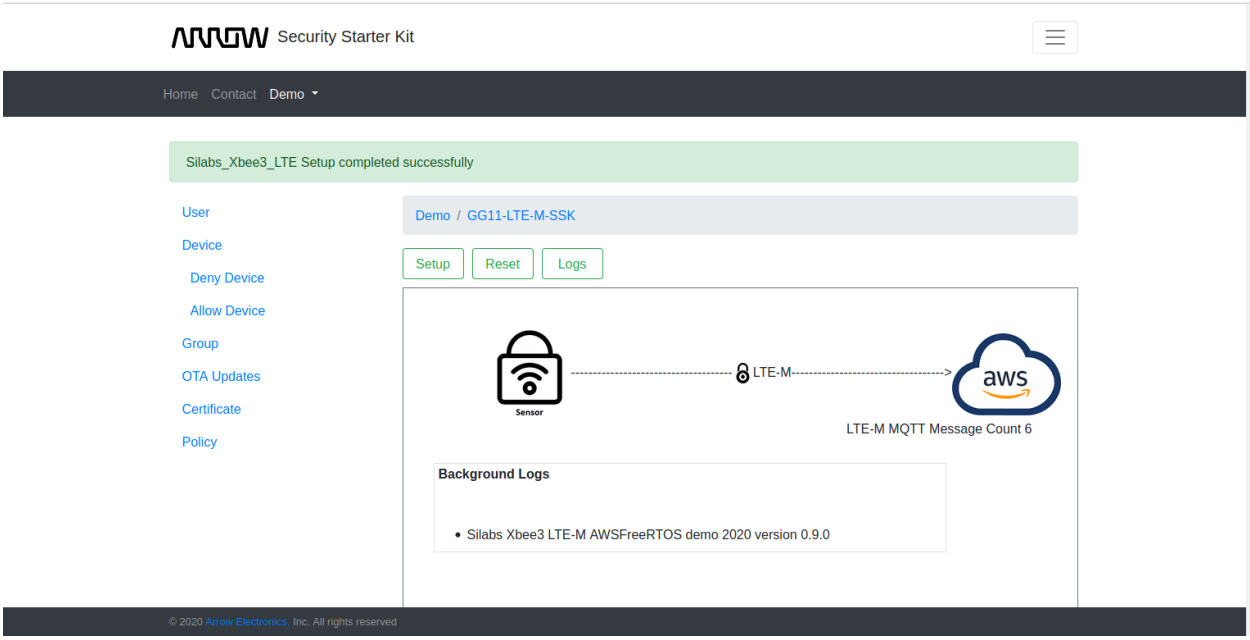
Silabs_Xbee3_LTE Setup completed successfully

3.2 SSK GG11-LTE-M-SSK- MQTT Demo

This Demo shows how AWS FreeRTOS based LTE-M device can securely communicate with AWS Cloud.

On SSK Cloud Connect, one can check the demo by configuring as shown below;

- Please follow SSK Cloud Connect >> Demo >> GG11-LTE-M-SSK >> Press "Reset" button
- Reboot the GG11-LTE-M board by pressing the "Reset" Button.

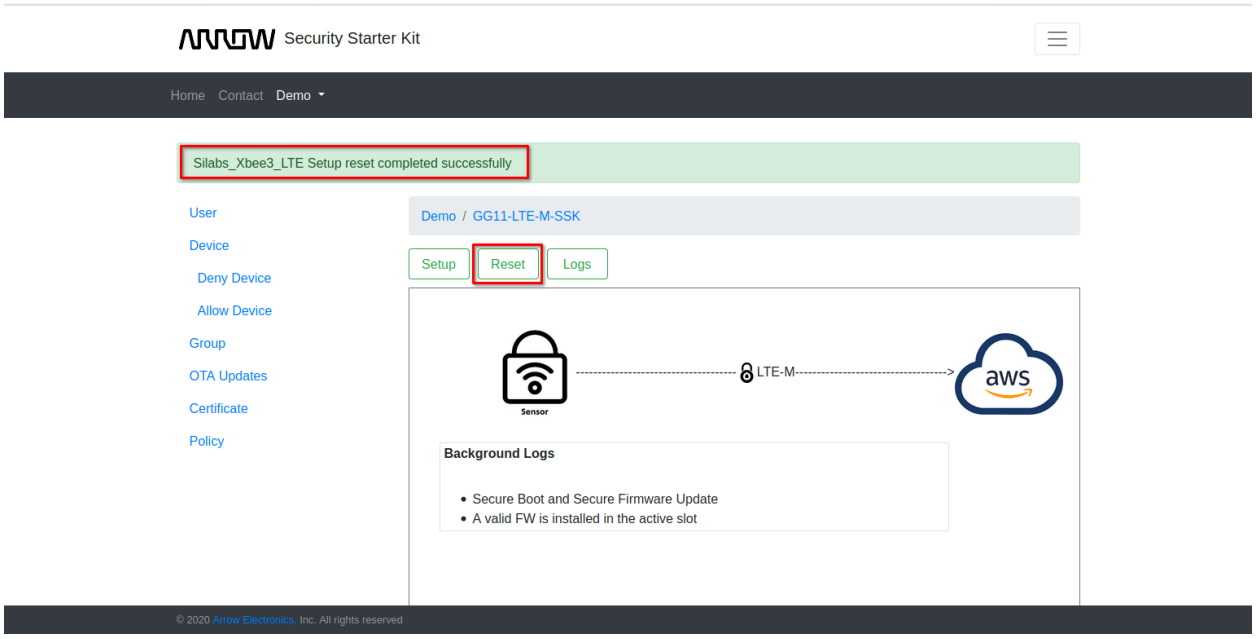


MQTT Message will display on the screen i.e. LTE-M MQTT Message Count 2

```
[INFO ][MQTT][lu] (MQTT connection 0x2000a3d0) MQTT PUBLISH operation queued.[INFO ][DEMO][lu] Acknowledgment message for PUBLISH 3 will be sent.
Incoming PUBLISH received:
Subscription topic filter: LTEiotdemo/topic/3
Publish topic name: LTEiotdemo/topic/3
Publish retain flag: 0
Publish QoS: 1
Publish payload: LTE-M MQTT Message Count 2

[INFO ][MQTT][lu] (MQTT connection 0x2000a3d0) MQTT PUBLISH operation queued.[INFO ][DEMO][lu] Acknowledgment message for PUBLISH 2 will be sent.
Incoming PUBLISH received:
Subscription topic filter: LTEiotdemo/topic/1
Publish topic name: LTEiotdemo/topic/1
Publish retain flag: 0
Publish QoS: 1
Publish payload: LTE-M MQTT Message Count 4

[INFO ][MQTT][lu] (MQTT connection 0x2000a3d0) MQTT PUBLISH operation queued.[INFO ][DEMO][lu] Acknowledgment message for PUBLISH 4 will be sent.
Incoming PUBLISH received:
Subscription topic filter: LTEiotdemo/topic/2
Publish topic name: LTEiotdemo/topic/2
Publish retain flag: 0
Publish QoS: 1
Publish payload: LTE-M MQTT Message Count 5
```

- On SSK Cloud Connect dashboard, MQTT Messages are received on AWS Cloud securely using hardware security chip - OPTIGA™ Trust M.

- Background Logs – Displays the Secure bootloader, Xbee3 Info and OPTIGA™ Trust M message on dashboard as a continuous scroller.



3.3 Demo Inference

Security Starter kit with GG11-LTE-M-SSKand OPTIGA™ Trust M Demo covers the below listed functionalities:

1. AWS Device Provisioning – AWS Device Provisioning using OPTIGA™ Trust M chip Pre-Provision certificate to register/install device into the AWS cloud.
2. AWS Authentication - OPTIGA™ Trust M chip Pre-Provision certificate authenticated by AWS.
3. Secure Communication – Using OPTIGA™ Trust M securely communicated between AWS and GG11-LTE-M-SSKby storing the session credentials.
4. AWS FreeRTOS – Used the AWS FreeRTOS for the Application development, includes securely connecting your small, low-power devices to AWS cloud services like AWS IoT Core
5. Secure Boot – Enabled secure bootloader features on GG11-LTE-M-SSK Board.

Note: For more details about all above functionalities, please refer the following documents, located here; https://www.arrow.com/en/products/gg11-lte-m-ssk/arrow-development-tools

GG11-LTE-M-SSK Developers Guid.pdf
Security Starter Kit Cloud Quick Start Guide.pdf
Security Starter Kit Cloud Connect Installation & Setup Guide.pdf
Security Starter Kit Cloud Connect Users Guide.pdf