User Guide

SSK Cloud Connect

Date: November 23, 2020 | Version 1.0

FINAL

eInfochips An Arrow Company | The Solutions People ARROW Five Years Out

CONTENTS

1 INTRODUCTION

1.1 Purpose of the Document

The SSK cloud connect guide provides an overview of the application to setup IAM User, Devices, AWS Greengrass, Certificate and Policies.

1.2 Prerequisite

This guide assumes that below configurations have been completed, as outlined in the SSK Cloud Connect Installation & Setup Guide:

- AWS Account
- AWS User Programmatic access
- AWS EC2 Instance service
- AWS RDS service
- AWS OTA Role Access
- User should be login in application by following below URL:

URL: http://ec2-13-233-137-7.ap-south-1.compute.amazonaws.com/#/login

Default details
User name: seed.dev@einfochips.com
Password: 123456

Commented [TM1]: I thought we agreed that we were not going to provide the EC2 Instance URL and Login information and force the user to create their own, as stated in the Installation and Setup Guide.

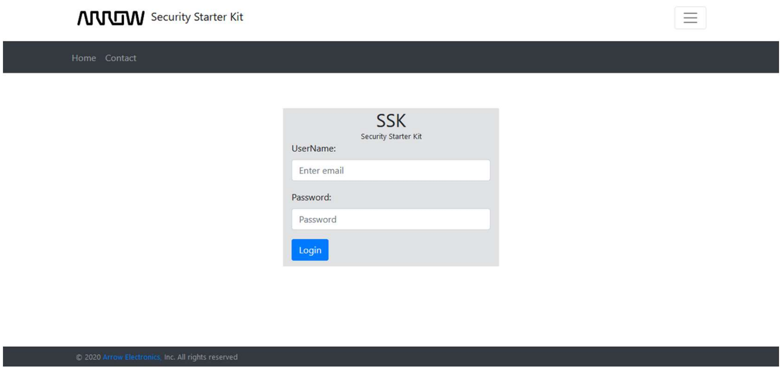

ARROW Security Starter Kit
Home
Contact
SSK
Security Starter Kit
UserName:
Enter email
Password:
Password
Login
© 2020 Arrow Electronics, Inc. All rights reserved

Figure 1: Login page

Note: Aws cloud doesn't support any kind of field Email ID at user level, due to that the forgot password operation not supported.

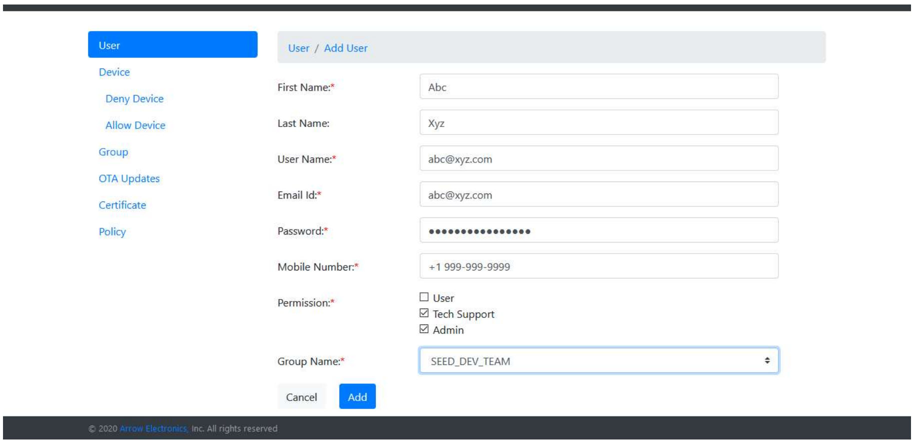
2 IAM USER

2.1 Description

An AWS Identity and Access Management (IAM) user is an entity that you create in SSK Cloud connect to represent the person or application that uses it to interact with SSK Cloud connect. A user in SSK Cloud connect consists of a name and credentials.

2.2 Creating IAM User

An IAM user is a resource in IAM that has associated credentials and permissions. An IAM user can represent a person or an application that uses its credentials to make SSK Cloud connect requests.



First Name:* Abc

Last Name: Xyz

User Name:* abc@xyz.com

Email Id:* abc@xyz.com

Password:* ••••••••••••••••

Mobile Number:* +1 999-999-9999

Permission:*
☐ User
☑ Tech Support
☑ Admin

Group Name:* SEED_DEV_TEAM

© 2020 Arrow Electronics, Inc. All rights reserved

Figure 2: Add I AM User

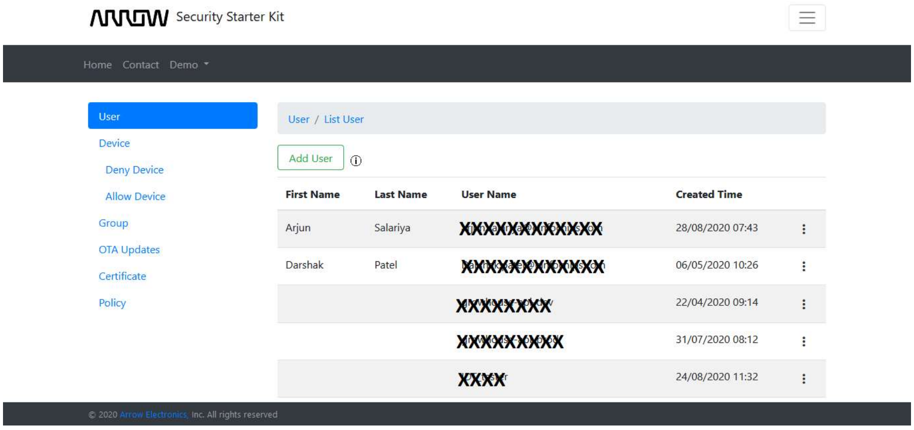
An IAM user can be described by the following:

1. First Name
   The first name of the user with min 4 chars.
2. Last Name
   The last name of the user.
3. User Name
   The unique name of the user with min 4 chars. Using that user can login into system. It should unique across AWS account.
4. Password
   The password of the user. At least 16 chars with combination of one Upper case, Lower case, Digit and Special character.

5. Email Id
   The Email Id of the user. It is not unique.
6. Mobile Number
   The Mobile number of the user with min 8 chars.
7. Permission
   a. **User** - can access only dashboard access and demo page
   b. **Tech Support** - can manage device, group, OTA, certificate, policy
   c. **Admin** - can manage all functionality.
8. Group Name
   Upon selection of group name user will be added in AWS Group to manage access

2.3 Listing I AM User

Once you create An IAM user, you can list down an IAM user at List User page. Which is shown Here in below images.



First Name	Last Name	User Name	Created Time	
Arjun	Salariya	[redacted]	28/08/2020 07:43	⋮
Darshak	Patel	[redacted]	06/05/2020 10:26	⋮
		[redacted]	22/04/2020 09:14	⋮
		[redacted]	31/07/2020 08:12	⋮
		[redacted]	24/08/2020 11:32	⋮

© 2020 Arrow Electronics, Inc. All rights reserved

Figure 2: Listing I AM User

3 DEVICE

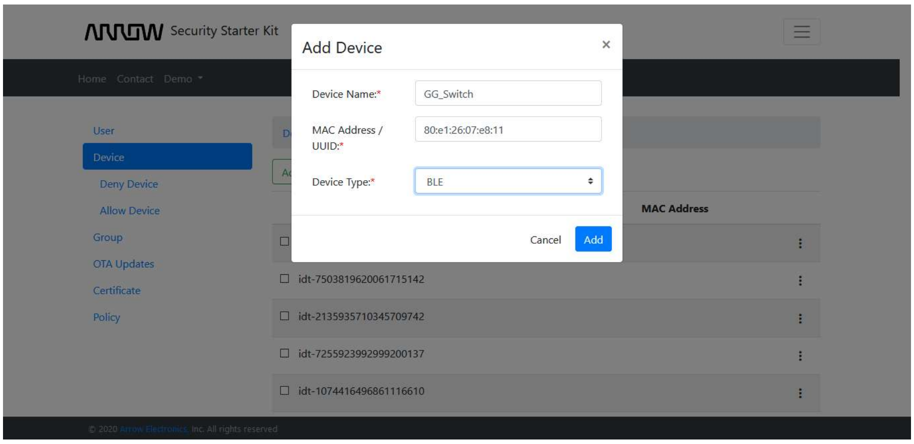
3.1 Description

AWS IoT provides a device registry that helps you manage your devices. A device is the representation of a device or logical entity. It can be a physical device or sensor (for example, a light bulb or a switch on a wall). It can also be a logical entity like an instance of an application or physical entity that does not connect to AWS IoT, but is related to devices that do (for example, a car that has engine sensors or a control panel).

Devices are identified by a name. Devices can also have attributes, which are name-value pairs you can use to store information about the device, such as its serial number or manufacturer. Adding your devices to the device registry allows you to manage and search for them more easily.

3.2 Add a Device

A device is the representation of a device or logical entity in the cloud. A device can be described by the following:



Add Device

Device Name:* GG_Switch

MAC Address / UUID:* 80:e1:26:07:e8:11

Device Type:* BLE

□ idt-7503819620061715142

□ idt-2135935710345709742

□ idt-7255923992999200137

□ idt-1074416496861116610

Figure 1: Add a device

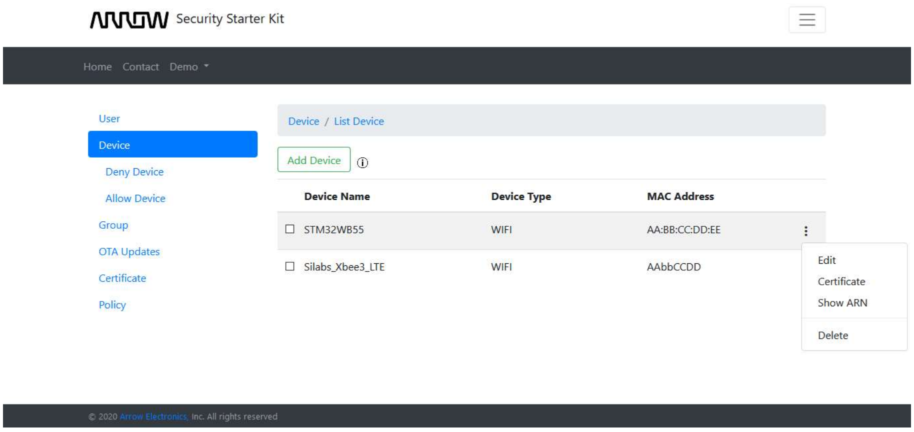
1. Device Name
   The name of the device.

2. MAC Address
   The MAC Address of the device.

3. Device Type
   Device types allow you to store description and configuration information that is common to all devices associated with the same device type. i.e. BLE, LTE-M, WIFI

3.3 Listing Devices

Listing of Devices can be seen in following figure with path SSK -> Device.



Device Name	Device Type	MAC Address
□ STM32WB55	WIFI	AA:BB:CC:DD:EE
□ Silabs_Xbee3_LTE	WIFI	AAbbCCDD

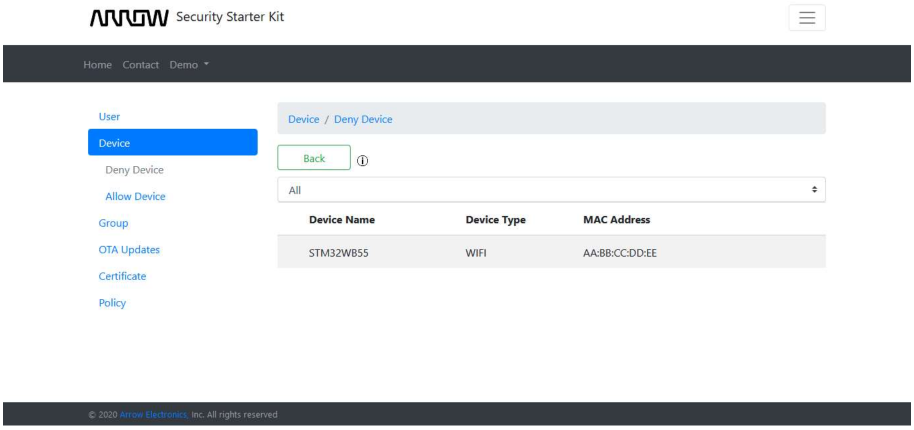
Figure 2: Listing devices

3.4 Deny Device

A Device which don’t have at least one active certificate or added in Deny by MAC Address/UUID.

1. Deny by Certificate
   You can remove device from Deny list by attaching certificate.

2. Deny by MAC Address
   You can remove device from Deny list by clicking remove button.



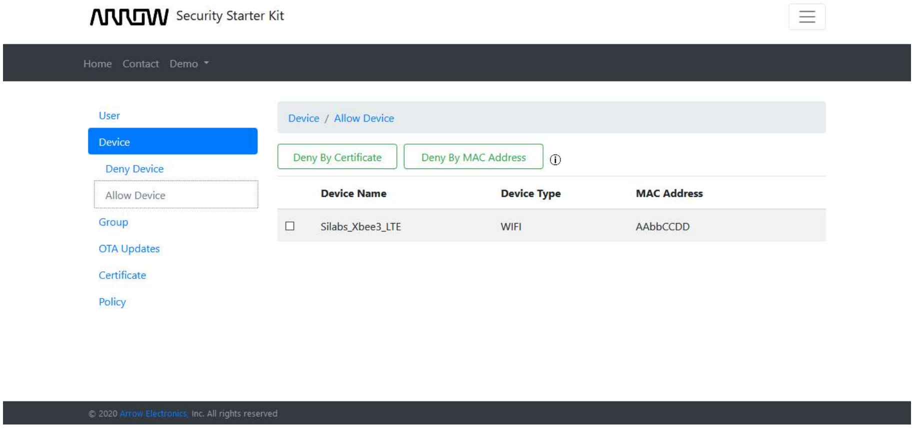
Device Name	Device Type	MAC Address
STM32WB55	WIFI	AA:BB:CC:DD:EE

Figure 3: Listing blacklist devices

3.5 Allow Device

A Device which have at least one active certificate and not added in Deny by MAC Address/UUID.

1. Deny by Certificate
   You can add device to deny list by clicking button Deny By Certificate.
2. Deny by MAC Address
   You can add device to deny list by clicking button Deny By MAC Address/UUID.



	Device Name	Device Type	MAC Address
□	Silabs_Xbee3_LTE	WIFI	AAbbCCDD

Figure 4: Listing whitelist devices

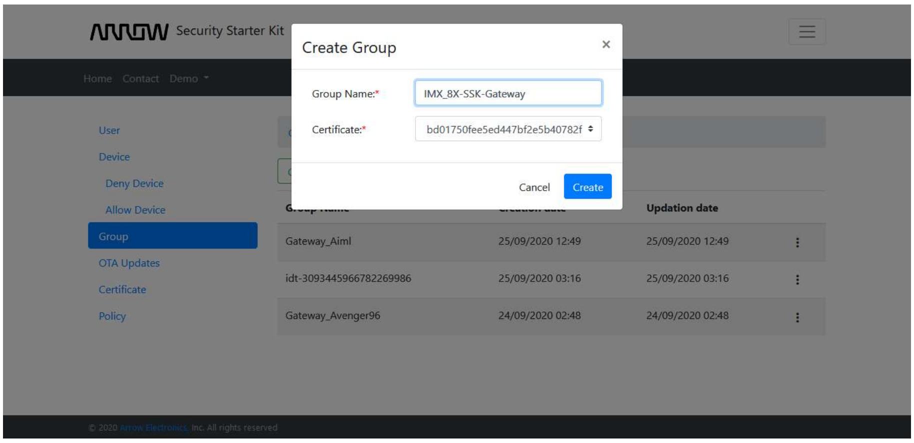
4 GREENGRASS

4.1 Description

An AWS IoT Greengrass lets your devices process the data they generate locally, while still taking advantage of AWS services when an internet connection is available.

4.2 Creating a Green grass Group

Setting up your Group requires you to provision a Core device in the IoT Registry, acquire a certificate for your Core, and assign an IAM role to your Group. A Group can be described by the following:



Create Group

Group Name:* IMX_8X-SSK-Gateway

Certificate:* bd01750fee5ed447bf2e5b40782f

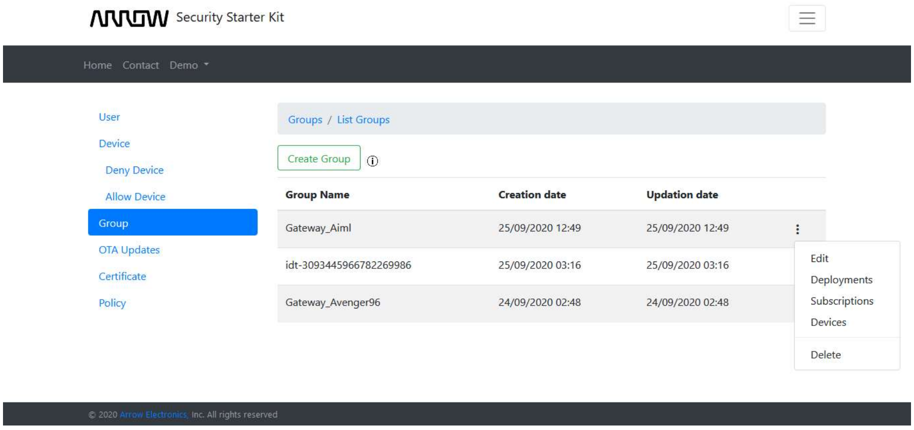
		Updation date
Gateway_Aiml	25/09/2020 12:49	25/09/2020 12:49
idt-3093445966782269986	25/09/2020 03:16	25/09/2020 03:16
Gateway_Avenger96	24/09/2020 02:48	24/09/2020 02:48

Figure 1: Create a Green grass Group

1. Group Name
   The name of the Green grass Group
2. Certificate Id
   The Certificate ID of the Green grass Core.

4.3 Listing Green grass Group

Listing of Greengrass group can be seen in following figure.



Group Name	Creation date	Updation date
Gateway_Aiml	25/09/2020 12:49	25/09/2020 12:49
idt-3093445966782269986	25/09/2020 03:16	25/09/2020 03:16
Gateway_Avenger96	24/09/2020 02:48	24/09/2020 02:48

Figure 2: Listing Green grass Groups

4.4 Green grass Subscription

A Subscription consists of a source, target, and topic. The source is the originator of the message. The target is the destination of the message. The first step is selecting your source and target.

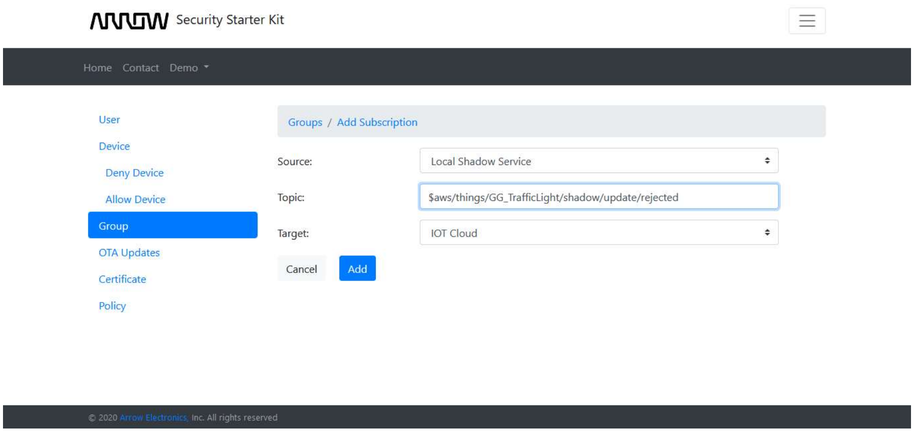
4.4.1 Creating a Subscription

A Subscription can be added to group by the following figure:

1. Source
   The name of the Source. Source can be Services like IoT Cloud, Local Shadow Service or Green grass devices.

2. Topic
   The name of the Topic. AWS Cloud and device can communicate on given topic over MQTT.

3. Target
   The name of the Target. Target can be Services like IoT Cloud, Local Shadow Service or Green grass devices.



Source: Local Shadow Service

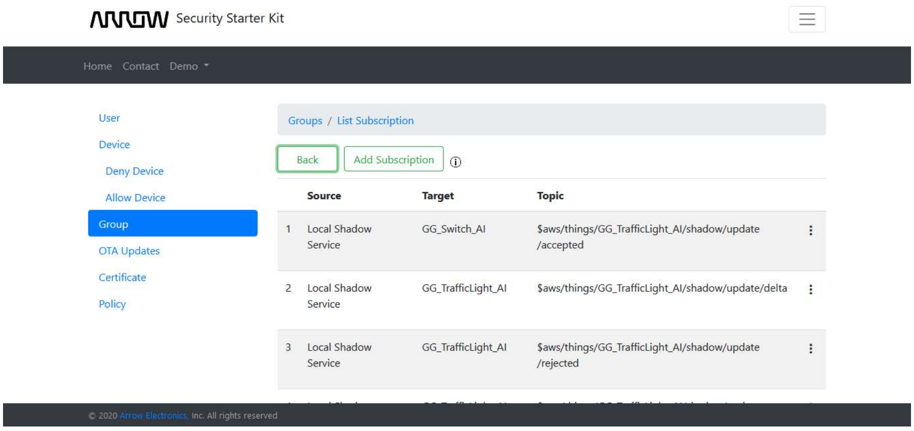
Topic: $aws/things/GG_TrafficLight/shadow/update/rejected

Target: IOT Cloud

Figure 3: Create subscription To Group

4.4.2 Listing Subscriptions

A Subscription List can be seen in following figure:



	Source	Target	Topic
1	Local Shadow Service	GG_Switch_AI	$aws/things/GG_TrafficLight_AI/shadow/update/accepted
2	Local Shadow Service	GG_TrafficLight_AI	$aws/things/GG_TrafficLight_AI/shadow/update/delta
3	Local Shadow Service	GG_TrafficLight_AI	$aws/things/GG_TrafficLight_AI/shadow/update/rejected

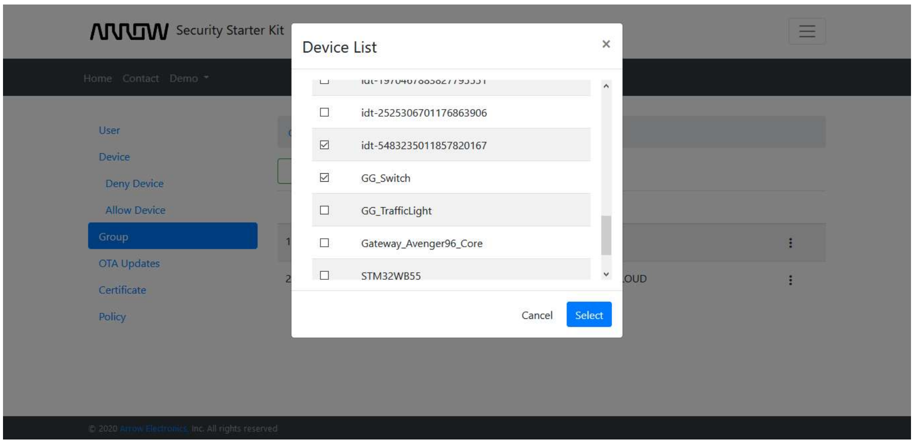
Figure 4: Listing subscriptions

4.5 Green grass Device

Greengrass Devices can be created by re-purposing an existing IoT Thing from your Registry or by creating new Registry items, and then adding them to a Greengrass Group.

4.5.1 Add a device

A device can be added to group by the following figure:



Device List

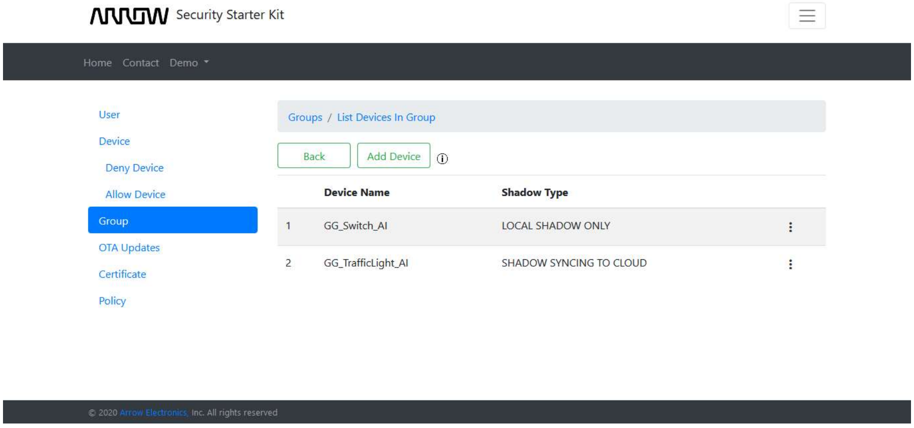
- □ idt-1970467883827795551
- □ idt-2525306701176863906
- ☑ idt-5483235011857820167
- ☑ GG_Switch
- □ GG_TrafficLight
- □ Gateway_Avenger96_Core
- □ STM32WB55

Figure 5: Add a device To Group

1. Device Name
   The name of the device.

4.5.2 Listing Devices

A Device List can be seen in following figure:

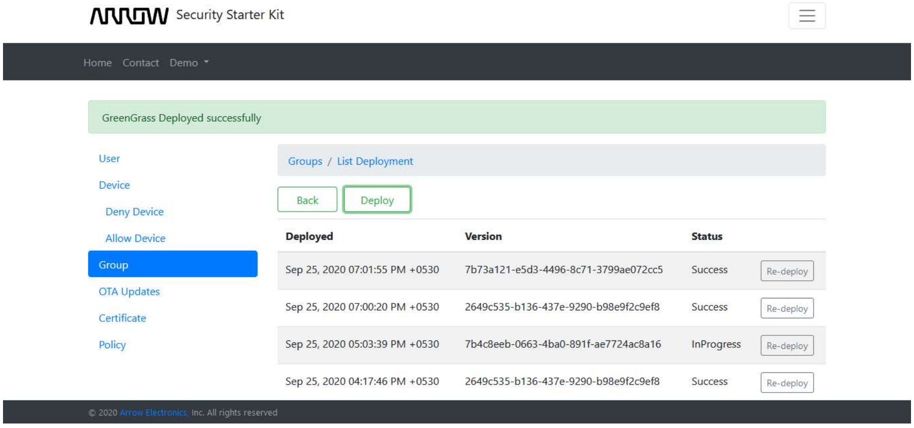


	Device Name	Shadow Type
1	GG_Switch_AI	LOCAL SHADOW ONLY
2	GG_TrafficLight_AI	SHADOW SYNCING TO CLOUD

Figure 6: Listing devices

4.6 Green grass Deployment

A deployment of green grass group & core to device can be setup by following figure:



GreenGrass Deployed successfully

Deployed	Version	Status	
Sep 25, 2020 07:01:55 PM +0530	7b73a121-e5d3-4496-8c71-3799ae072cc5	Success	Re-deploy
Sep 25, 2020 07:00:20 PM +0530	2649c535-b136-437e-9290-b98e9f2c9ef8	Success	Re-deploy
Sep 25, 2020 05:03:39 PM +0530	7b4c8eeb-0663-4ba0-891f-ae7724ac8a16	InProgress	Re-deploy
Sep 25, 2020 04:17:46 PM +0530	2649c535-b136-437e-9290-b98e9f2c9ef8	Success	Re-deploy

Figure 7: Deployment Greengrass

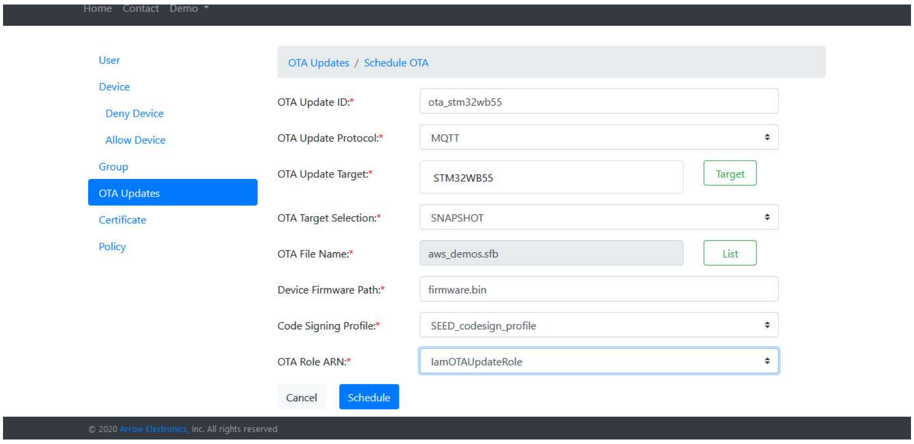
5 OTA UPDATES

5.1 Description

AWS IoT Device Management job orchestration and notification service allows you to define a set of remote operations called jobs that are sent to and executed on one or more devices connected to AWS IoT.

5.2 Create a FreeRTOS OTA update job (Schedule OTA)

This Over-the-air (OTA) update job will send your firmware image securely over MQTT or HTTP to FreeRTOS-based devices.



OTA Update ID:* ota_stm32wb55

OTA Update Protocol:* MQTT

OTA Update Target:* STM32WB55

OTA Target Selection:* SNAPSHOT

OTA File Name:* aws_demos.sfb

Device Firmware Path:* firmware.bin

Code Signing Profile:* SEED_codesign_profile

OTA Role ARN:* IamOTAUpdateRole

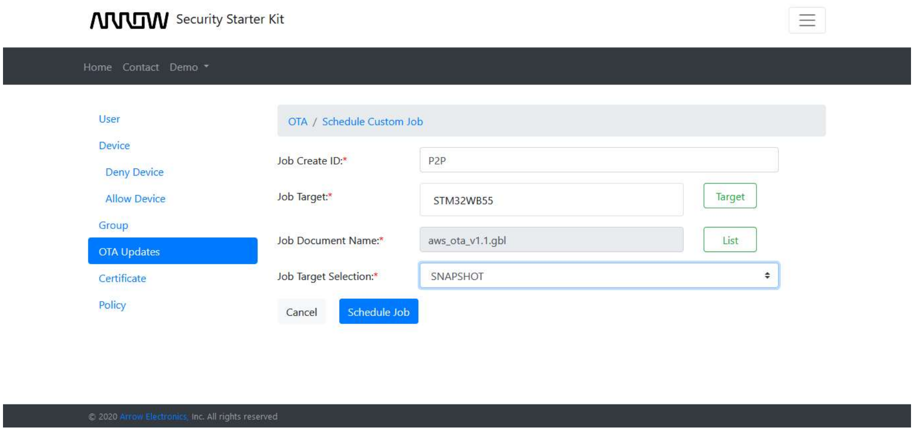
Figure 1: Schedule OTA

1. OTA Update ID
   A unique OTA update ID.
2. OTA Update Protocol
   The protocol that you choose must be supported by your device. If you select a protocol that is not supported by your device, the firmware update will be unsuccessful.
3. OTA Update Target
   Select the devices you want to include in this job.
4. OTA Target Selection
   Snapshot job is sent to all targets that when you create the job. After those targets complete the job (or report that they are unable to do so), the job is complete.
5. OTA File Name
   Name of firmware.

6. Device Firmware Path
   This is the location and name to use when storing the firmware on the FreeRTOS device during OTA update. It is an optional field since certain devices do not store the image to a filesystem and may instead write directly to internal flash memory.
7. Code Signing Profile
   Code signing ensures that devices only run code published by trusted authors and that the code has not been altered or corrupted since it was signed. You have three options for code signing.
8. OTA Role ARN
   A Role which grants AWS IoT access to the S3, AWS IoT jobs and AWS Code signing resources to create an OTA update job.

5.3 Create Custom Job (Schedule Job)

Send a request to acquire an executable job file from one of your S3 buckets to one or more devices connected to AWS IoT.



Job Create ID:* P2P

Job Target:* STM32WB55

Job Document Name:* aws_ota_v1.1.gbl

Job Target Selection:* SNAPSHOT

© 2020 Arrow Electronics, Inc. All rights reserved

Figure 2: Schedule custom job

1. Job Create ID
   A unique job Id.
2. Job Target
   Select the devices you want to include in this job.
3. Job Document Name
   Upload a job file that defines what your job should do.

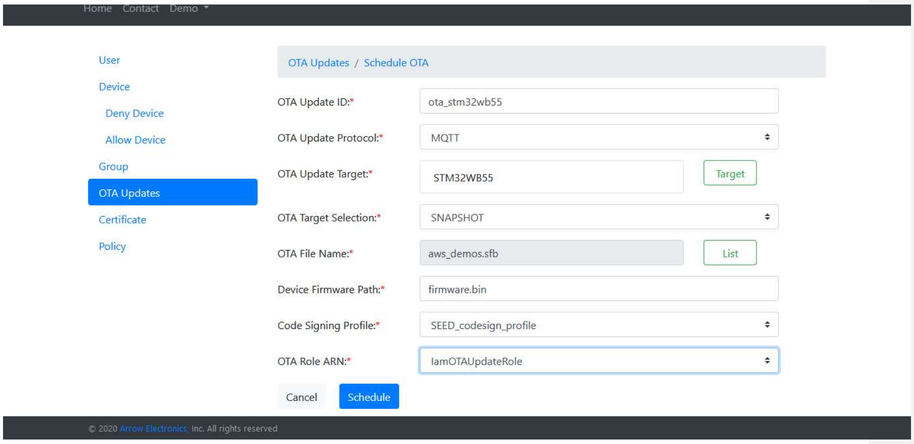
Job documents are JSON documents and should contain any information your devices need to perform a job. For example, a job document can contain one or more URLs where the device can download an update or some other data.

4. Job Target Selection

   Snapshot job is sent to all targets that when you create the job. After those targets complete the job (or report that they are unable to do so), the job is complete.

5.4 Listing OTA UPDATES

Listing of ota job can be seen in following figure:



OTA Updates / Schedule OTA

OTA Update ID:* ota_stm32wb55

OTA Update Protocol:* MQTT

OTA Update Target:* STM32WB55

OTA Target Selection:* SNAPSHOT

OTA File Name:* aws_demos.sfb

Device Firmware Path:* firmware.bin

Code Signing Profile:* SEED_codesign_profile

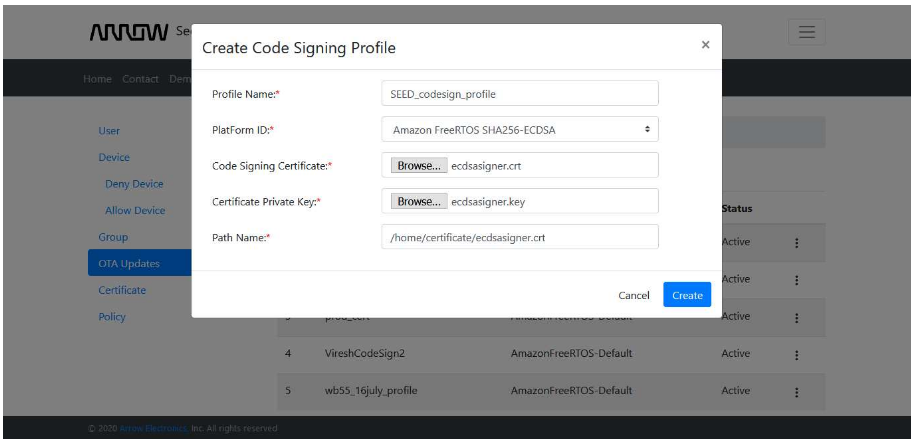
OTA Role ARN:* IamOTAUpdateRole

© 2020 Arrow Electronics, Inc. All rights reserved

Figure 3: Listing OTA Job

5.5 Create a Code Signing profile

The code signing profile contains information needed to create a code signing job. It specifies your device's hardware platform, certificate from AWS Certificate Manager, and the location of your code signing certificate path on your device.



Create Code Signing Profile

Profile Name:* SEED_codesign_profile

PlatForm ID:* Amazon FreeRTOS SHA256-ECDSA

Code Signing Certificate:* Browse... ecdsasigner.crt

Certificate Private Key:* Browse... ecdsasigner.key

Path Name:* /home/certificate/ecdsasigner.crt

Cancel Create

			Status
			Active
			Active
			Active
4	VireshCodeSign2	AmazonFreeRTOS-Default	Active
5	wb55_16july_profile	AmazonFreeRTOS-Default	Active

Figure 4: Create code signing profile

1. Profile Name
   A unique profile name.
2. PlatForm ID
   Select the platform.
3. Code Signing Certificate
   Upload signing certificate
4. Certificate Private Key
   Upload private key
5. Path Name
   Select the path name of certificate on device

6 CERTIFICATE

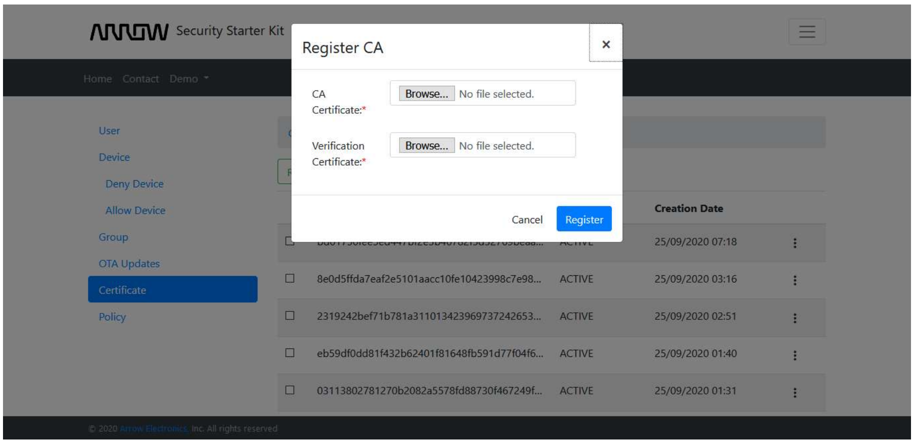
6.1 Description

A certificate is used to authenticate your device's connection to AWS IoT.

6.2 Register CA

To use your own X.509 certificates, you must register a CA certificate with AWS IoT. The CA certificate can then be used to sign device certificates. You can register up to ten CA certificates with the same subject field and public key per AWS account. This allows you to have more than one CA sign your device certificates.

- Step 1: Generate a key pair for the private key verification certificate
- Step 2: Copy this registration code (From Setting page at top-right corner)
- Step 3: Create a CSR with this registration code Put the registration code in the Common Name field
- Step 4: Use the CSR that was signed with the CA private key to create a private key verification certificate
- Step 5: Upload the CA certificate (rootCA.pem)
- Step 6: Upload the verification certificate (verificationCert.crt) :



Register CA

CA Certificate:* No file selected.

Verification Certificate:* No file selected.

			Creation Date
□	[illegible]	[illegible]	25/09/2020 07:18
□	8e0d5ffda7eaf2e5101aacc10fe10423998c7e98...	ACTIVE	25/09/2020 03:16
□	2319242bef71b781a311013423969737242653...	ACTIVE	25/09/2020 02:51
□	eb59df0dd81f432b62401f81648fb591d77f04f6...	ACTIVE	25/09/2020 01:40
□	03113802781270b2082a5578fd88730f467249f...	ACTIVE	25/09/2020 01:31

Figure 1: Register CA

1. Root CA File

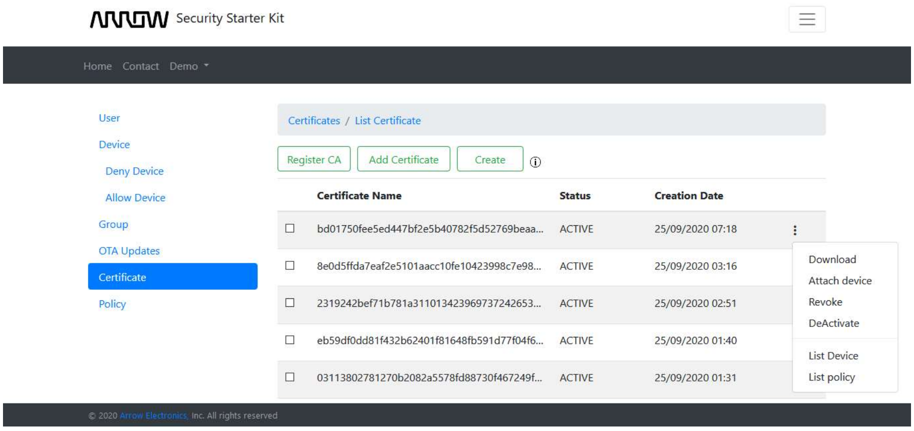
Select & upload root CA file.

2. Verification Certificate File

Select & upload verification certificate file.

6.3 Listing Certificates

Listing of register of all certificate can be seen in following figure:

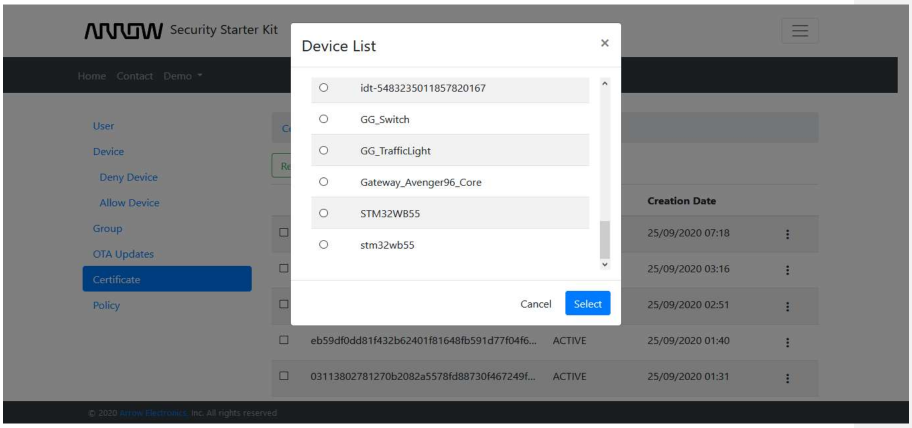


	Certificate Name	Status	Creation Date
☐	bd01750fee5ed447bf2e5b40782f5d52769beaa...	ACTIVE	25/09/2020 07:18
☐	8e0d5ffda7eaf2e5101aacc10fe10423998c7e98...	ACTIVE	25/09/2020 03:16
☐	2319242bef71b781a311013423969737242653...	ACTIVE	25/09/2020 02:51
☐	eb59df0dd81f432b62401f81648fb591d77f04f6...	ACTIVE	25/09/2020 01:40
☐	03113802781270b2082a5578fd88730f467249f...	ACTIVE	25/09/2020 01:31

Figure 2: Listing Certificates

Certificate will be having following operations:

1. Download
   Download certificate file in PEM format.
2. Attach device
   Attach certificate to device.



○ idt-5483235011857820167
○ GG_Switch
○ GG_TrafficLight
○ Gateway_Avenger96_Core
○ STM32WB55
○ stm32wb55

		Creation Date
☐		25/09/2020 07:18
☐		25/09/2020 03:16
☐		25/09/2020 02:51
☐ eb59df0dd81f432b62401f81648fb591d77f04f6...	ACTIVE	25/09/2020 01:40
☐ 03113802781270b2082a5578fd88730f467249f...	ACTIVE	25/09/2020 01:31

Figure 3: Attach certificate to Device

3. Revoke
   To Revoke certificate, once certificate will be revoked then it will not be activate again. Only you can delete certificate.

4. Deactivate
   To Change status of certificate to inactive, once revoked certificate then deactivate option will not be available.

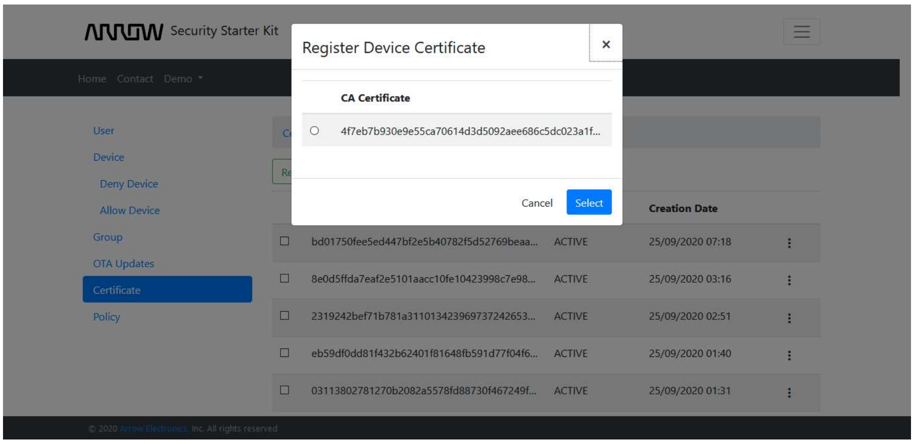
5. Delete
   To Delete certificate, if certificate exists other active then this option will be available.

6. List Device
   List down all devices attached to certificate.

7. List Policy
   List down all policy attached to certificate.

6.4 Add a Certificate

Select or register the CA certificate used to sign your device certificates. To use device certificates that are not signed by a registered CA, just select next.



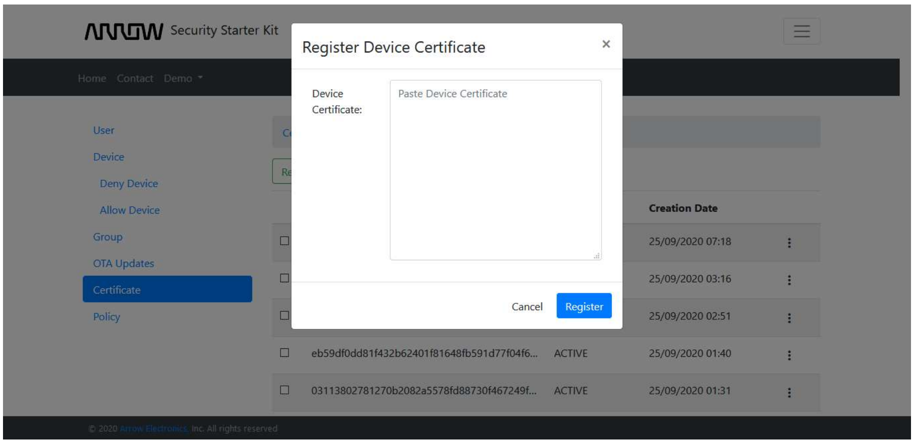
Register Device Certificate

	CA Certificate
○	4f7eb7b930e9e55ca70614d3d5092aee686c5dc023a1f...

			Creation Date
☐	bd01750fee5ed447bf2e5b40782f5d52769beaa...	ACTIVE	25/09/2020 07:18
☐	8e0d5ffda7eaf2e5101aacc10fe10423998c7e98...	ACTIVE	25/09/2020 03:16
☐	2319242bef71b781a31101342396973724265 3...	ACTIVE	25/09/2020 02:51
☐	eb59df0dd81f432b62401f81648fb591d77f04f6...	ACTIVE	25/09/2020 01:40
☐	03113802781270b2082a5578fd88730f467249f...	ACTIVE	25/09/2020 01:31

Figure 4: Add Certificate Part 1

Paste the existing certificate PEM file.



Register Device Certificate

Device Certificate: Paste Device Certificate

			Creation Date
□			25/09/2020 07:18
□			25/09/2020 03:16
□			25/09/2020 02:51
□	eb59df0dd81f432b62401f81648fb591d77f04f6...	ACTIVE	25/09/2020 01:40
□	03113802781270b2082a5578fd88730f467249f...	ACTIVE	25/09/2020 01:31

© 2020 Arrow Electronics, Inc. All rights reserved

Figure 5: Add Certificate part 2

1. Registered CA
   Select CA ID from list of CA.

2. Existing Certificate File
   Paste the Certificate PEM file.

6.5 Create a Certificate (One Click)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

7 POLICY

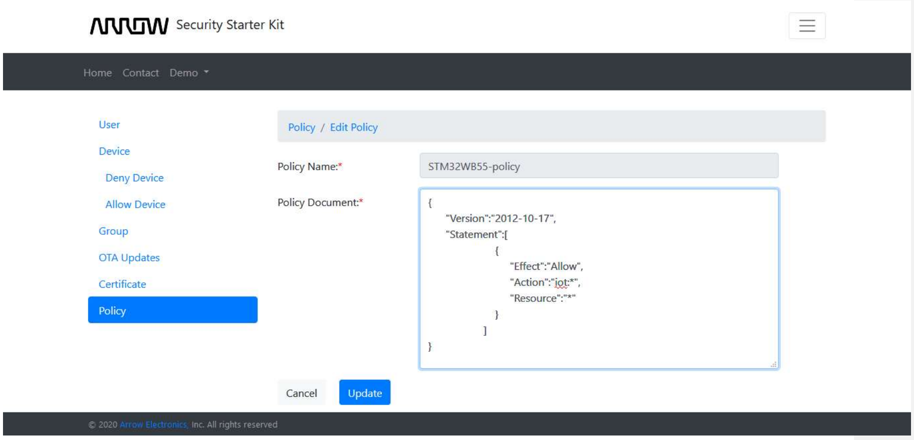
7.1 Description

AWS IoT policies grant or deny access to AWS IoT resources such as things, thing shadows, and MQTT topics. A device or user can invoke AWS IoT operations only if they are granted the appropriate permissions.

Policies give permissions to AWS IoT clients regardless of the authentication mechanism they use to connect to AWS IoT. To control which resources a device can access, attach one or more AWS IoT policies to the certificate associated with the device.

7.2 Creating a Policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters).



Policy Name:* STM32WB55-policy

Policy Document:*

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

Figure 1: Create Policy

1. Policy Name
   The name of the policy.

2. Policy Document
   Policy document define the types of actions that can be performed by a resource. It will not allow any spaces

Policy document Description can be seen below:

Policy document has mainly three elements

- **i.** Effect – Allow/ Deny
- **ii.** Action

  Action can be define by following type.

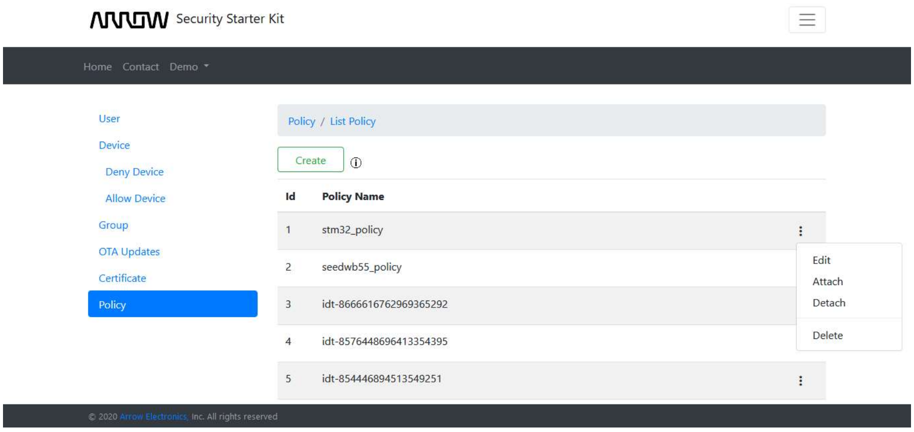
  a. iot:*
  b. iot:Publish
  c. iot:Subscribe
  d. iot:Connect
  e. iot:Receive
  f. iot:UpdateThingShadow
  g. iot:GetThingShadow
  h. iot:DeleteThingShadow

- iii. Resource ARN

  Resource could be client ID ARN, topic ARN or topic filter ARN

7.3 Listing the Policy

Listing of policy can be seen in following figure:

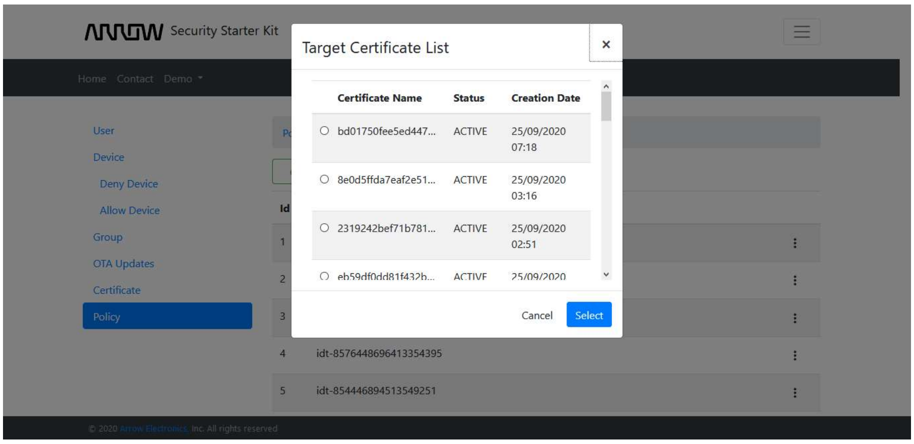


Id	Policy Name
1	stm32_policy
2	seedwb55_policy
3	idt-8666616762969365292
4	idt-8576448696413354395
5	idt-854446894513549251

Figure 2: Listing Green grass Groups

7.4 Attach Policy

Policy can be attach to resource like Certificate, cognito which can be seen here in following figure



Target Certificate List

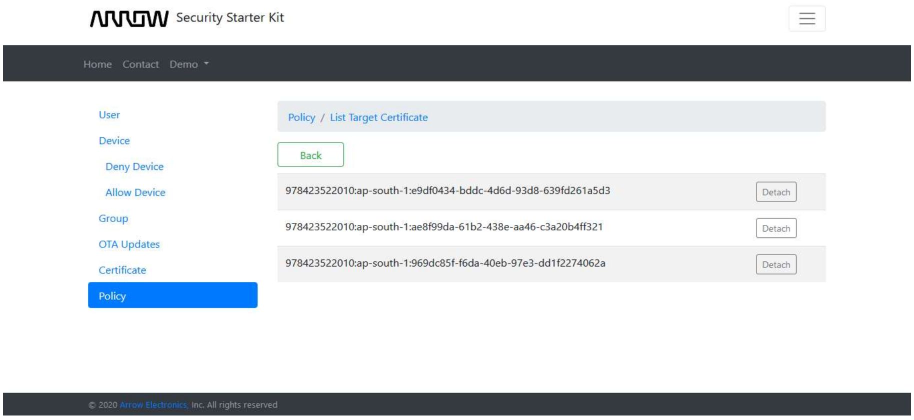
	Certificate Name	Status	Creation Date
○	bd01750fee5ed447...	ACTIVE	25/09/2020 07:18
○	8e0d5ffda7eaf2e51...	ACTIVE	25/09/2020 03:16
○	2319242bef71b781...	ACTIVE	25/09/2020 02:51
○	eb59df0dd81f432b...	ACTIVE	25/09/2020

Id	
1	
2	
3	
4	idt-8576448696413354395
5	idt-854446894513549251

Figure 3: Attach policy to Certificate

7.5 Detach Policy

Detach policy from resource like Certificate, cognito can be seen here in following figure:



Policy / List Target Certificate

978423522010:ap-south-1:e9df0434-bddc-4d6d-93d8-639fd261a5d3	Detach
978423522010:ap-south-1:ae8f99da-61b2-438e-aa46-c3a20b4ff321	Detach
978423522010:ap-south-1:969dc85f-f6da-40eb-97e3-dd1f2274062a	Detach

Figure 4: Detach policy from resource

8 REFERENCES

[1] https://docs.aws.amazon.com/greengrass/latest/developerguide/gg-dg.pdf

[2] https://aws.amazon.com/blogs/iot/using-a-trusted-platform-module-for-endpoint-device-security-in-aws-iot-greengrass/

[3] https://docs.aws.amazon.com/iot/latest/developerguide/register-CA-cert.html

[4] https://aws.amazon.com/console/