



Document Number	BQW_02_0020.003
-----------------	-----------------

MiniHub Pro

Quick Installation Guide

-with Basic Station & AWS IoT Core for LoRaWAN

Version 1.11



Index

Index	1
Release History	2
About this Document	3
Required Equipment	3
Onboard LoRaWAN Gateways	4
Configure the Gateway(Web Provision)	7
Connect to Web GUI	7
AWS & LoRa Setting	9
WiFi Setting	11
LED Behavior	12
Onboard LoRaWAN Devices	13
Reset to Default	18
OTA	19
Get Firmware	19
Configure MiniHub Pro	20
Create an Amazon S3 bucket to store your update	20
Create an OTA Update service role	25
To create an OTA service role	25
5To add OTA update permissions to your OTA service role	30
To add the required IAM permissions to your OTA service role	33
To add the required Amazon S3 permissions to your OTA service role	37
Create an OTA user policy	42
To create an OTA user policy	42
To attach the OTA user policy to your IAM user	51
Create a FreeRTOS OTA update job	57



Release History

Date	Version	Author	Comment
2020/01/21	1.1	Jason Andrew Lin Andrew Shiu Crux	<ul style="list-style-type: none">• First release.
2020/04/16	1.2	Jason Andrew Lin Andrew Shiu Crux	<ul style="list-style-type: none">• Add Web GUI for AWS IoT provision.• Add Web GUI for Basic Station provision.• Add writing station EUI command.• Add LED behavior.
2020/04/16	1.3	Jason Andrew Lin Andrew Shiu Crux	<ul style="list-style-type: none">• Fix some typos.
2020/05/27	1.4	Jason Andrew Lin Andrew Shiu Crux	<ul style="list-style-type: none">• Add Q&A.
2020/06/22	1.5	Jason Joey	<ul style="list-style-type: none">• Add OTA flow.
2020/06/30	1.6	Jason	<ul style="list-style-type: none">• Correct some wording• Browan Official Release, add Document Number
2020/07/15	1.7	Jason Andrew Shiu	<ul style="list-style-type: none">• Modify OTA Flow. User no needs to power off and power on to trigger the OTA.
2020/08/24	1.8	Crux	<ul style="list-style-type: none">• Add chapter ISM Band and LoRa MAC Troubleshooting.• Remove chapter Station EUI Writing.
2020/08/26	1.9	Jason	<ul style="list-style-type: none">• Add more detailed steps of the OTA jobs.
2020/10/29	1.10	Jason	<ul style="list-style-type: none">• Add AWS IoT Core for LoRaWAN(Sailboat)
2022/8/25	1.11	Jason	<ul style="list-style-type: none">• Remove Breakout board



About this Document

This document explains the configuration after powering up. The Web GUI usage for AWS IoT provision and Basic Station provision.

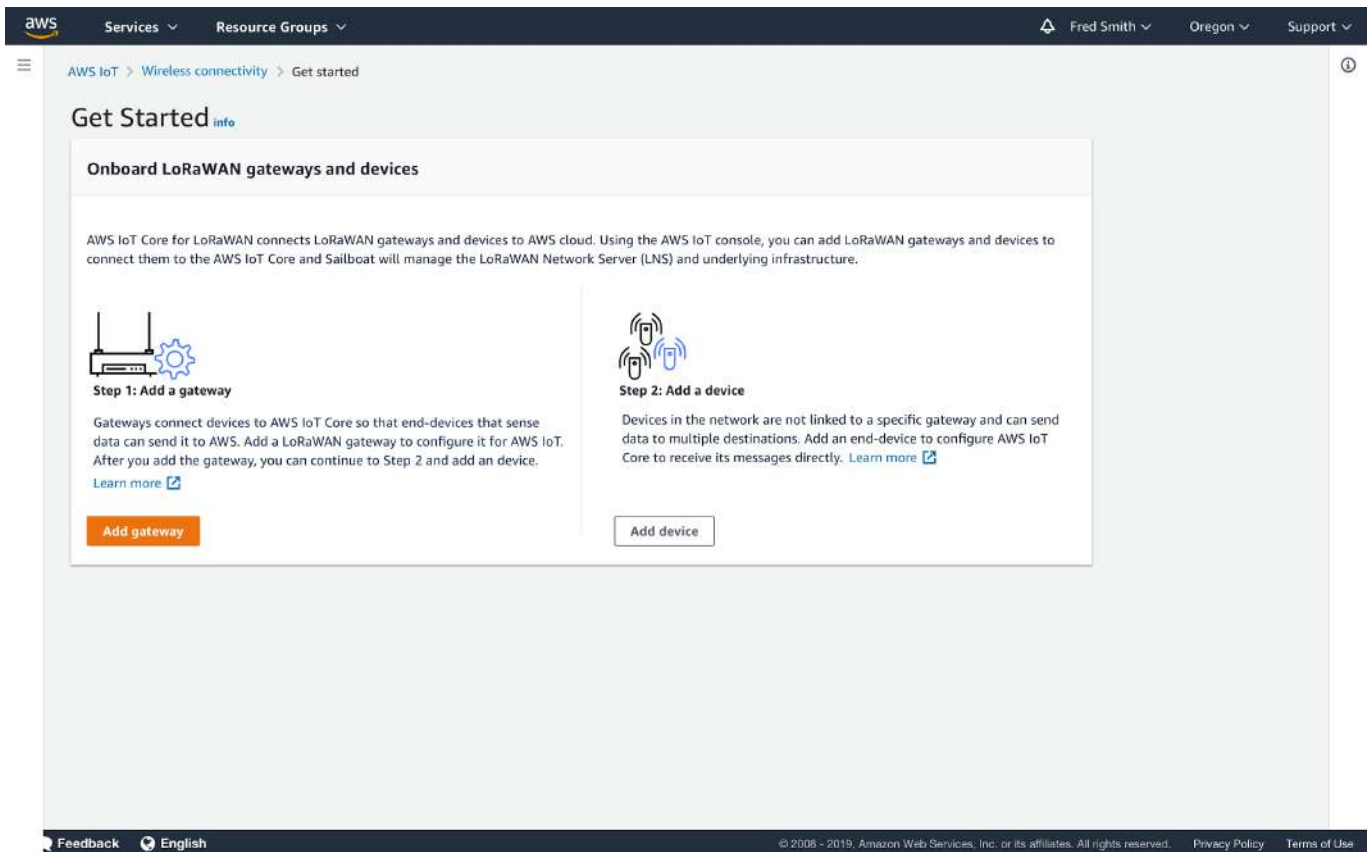
Required Equipment

- MiniHub Pro



Onboard LoRaWAN Gateways

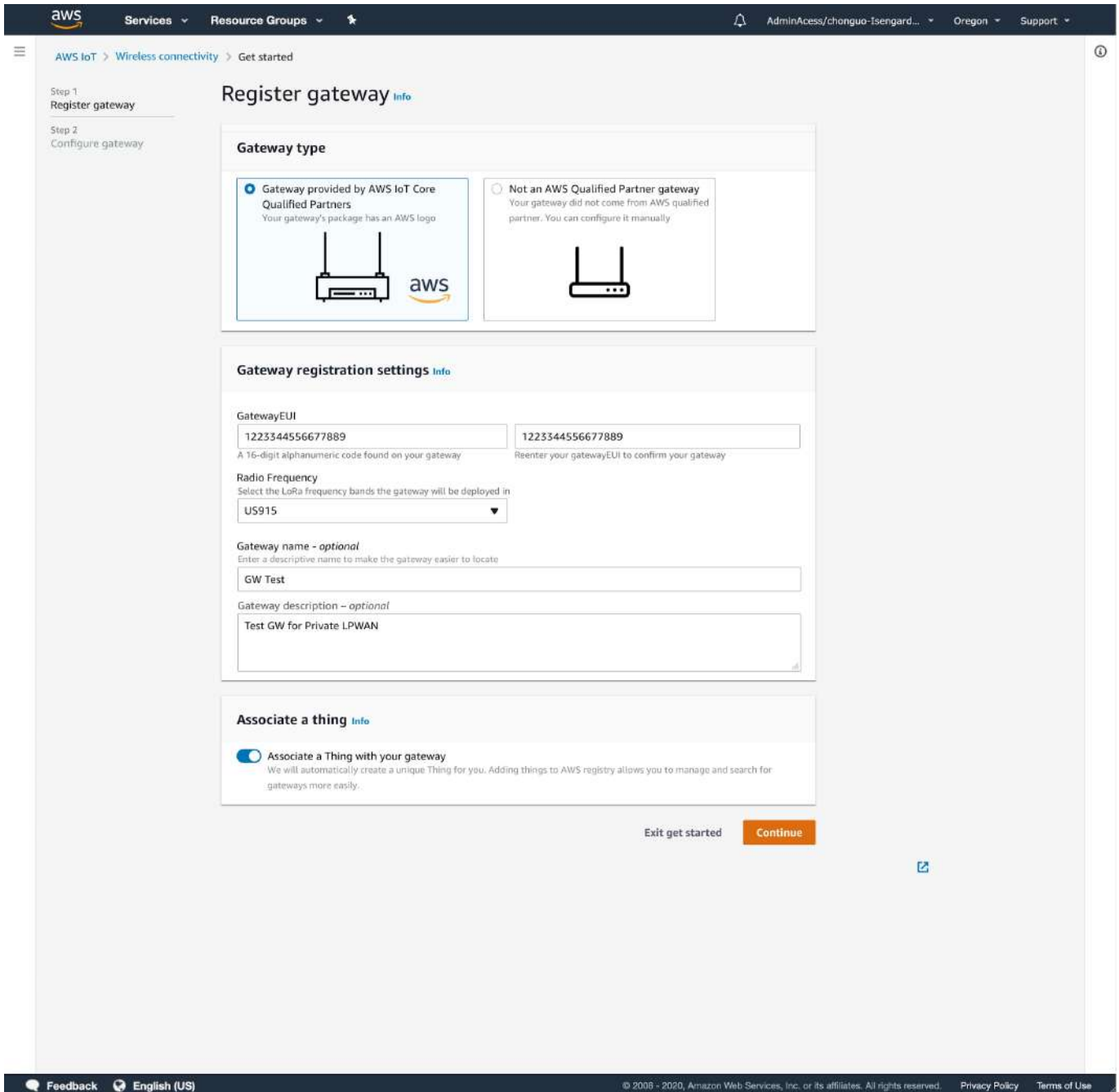
- Step1.
Click “Add gateway”



The screenshot shows the AWS IoT console interface. At the top, there's a navigation bar with 'aws', 'Services', 'Resource Groups', and user information 'Fred Smith', 'Oregon', and 'Support'. Below the navigation bar, the breadcrumb trail reads 'AWS IoT > Wireless connectivity > Get started'. The main content area is titled 'Get Started' and contains a section 'Onboard LoRaWAN gateways and devices'. This section includes a paragraph explaining that AWS IoT Core for LoRaWAN connects gateways and devices to the AWS cloud. It then presents two steps: 'Step 1: Add a gateway' and 'Step 2: Add a device'. Each step has an icon, a brief description, and a corresponding 'Add gateway' or 'Add device' button. The 'Add gateway' button is highlighted in orange. At the bottom of the page, there is a footer with 'Feedback', 'English', and copyright information for Amazon Web Services, Inc. (© 2008 - 2019).

- Step2.

Select “Gateway provided by AWS IoT Core Qualified Partners”. Input GatewayEUI, Radio Frequency, Gateway name(Optional), Gateway description(Optional) and click “Continue”



The screenshot shows the AWS IoT console interface for registering a gateway. The breadcrumb trail is "AWS IoT > Wireless connectivity > Get started". The page title is "Register gateway".

Gateway type

- Gateway provided by AWS IoT Core Qualified Partners
Your gateway's package has an AWS logo
- Not an AWS Qualified Partner gateway
Your gateway did not come from AWS qualified partner. You can configure it manually

Gateway registration settings

GatewayEUI
1223344556677889 (A 16-digit alphanumeric code found on your gateway)
1223344556677889 (Reenter your gatewayEUI to confirm your gateway)

Radio Frequency
Select the LoRa frequency bands the gateway will be deployed in
US915

Gateway name - optional
Enter a descriptive name to make the gateway easier to locate
GW Test

Gateway description - optional
Test GW for Private LPWAN

Associate a thing

- Associate a Thing with your gateway
We will automatically create a unique Thing for you. Adding things to AWS registry allows you to manage and search for gateways more easily.

Buttons: Exit get started, Continue






- Step3.

Configure Gateway. Please refer to the next chapter. Click “Continue”

Configure gateway Info

Your gateway is registered with AWS IoT. You must complete these steps by logging on the local gateway GUI provided by your vendor to configure the gateway settings before it can pass messages to AWS.

Configure on local gateway network

		
Step 1: Connect to your gateway's local network <small>Connect to the gateway device and open its configuration settings interface. Refer to the gateway device's documentation for information about how to do that.</small> How to connect	Step 2: Choose LoRaWAN for AWS IoT Core <small>In the <placeholder> menu, choose Sailboat from the dropdown selector.</small>	Step 3: Choose your RF region <small>In the menu, choose the RF region option that matches the RF region shown here.</small> <input type="text" value="US 902-928"/>

After you add the gateway, it can take up to XX minutes to complete the configuration. To view your gateway visit the "Gateway" section in the navigation You can onboard devices while waiting.

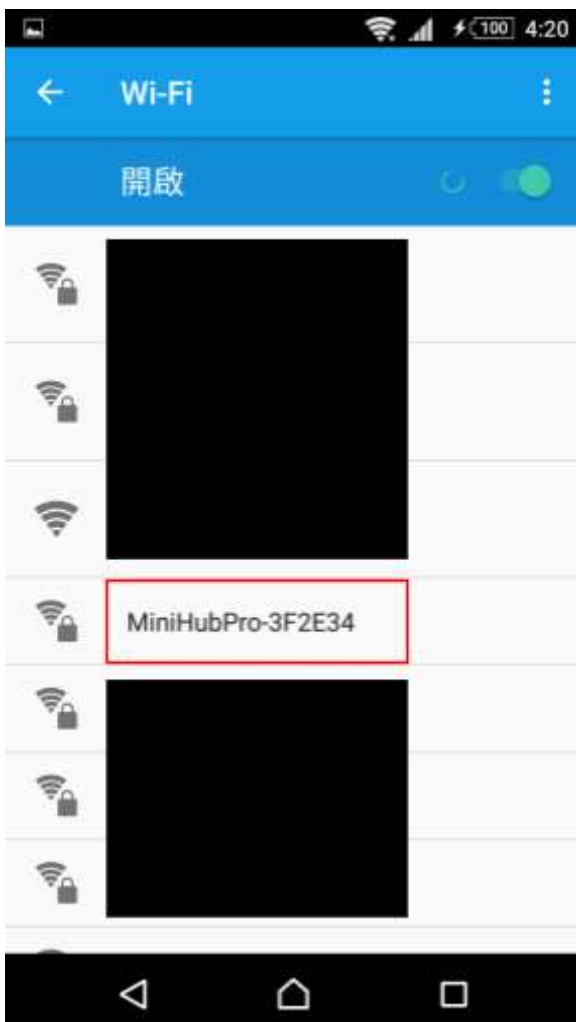
[Exit get started](#) [Continue](#)

Configure the Gateway(Web Provision)

Connect to Web GUI

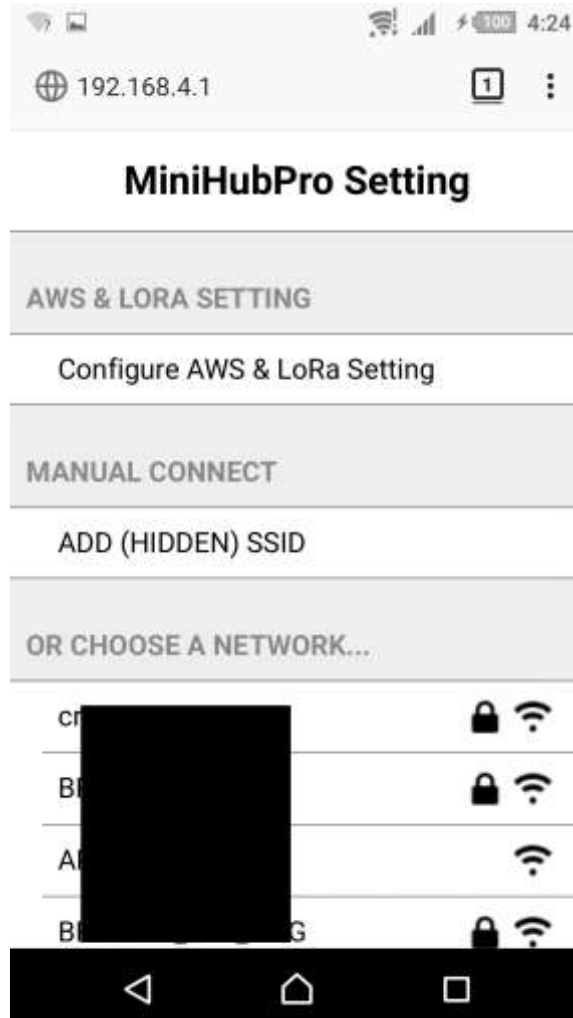
The device can run as WiFi AP mode or WiFi Station mode. When the device is in the initial state, such as first boot-up time or after reset-to-default. It will run with the WiFi AP mode. That means it accepts any WiFi client to connect to it.

You can find the SSID `MiniHubPro-XXXXXX` in the WiFi site-survey list. The suffix 6 characters are the last 6 hex string of WiFi MAC address. The password is in the back label.



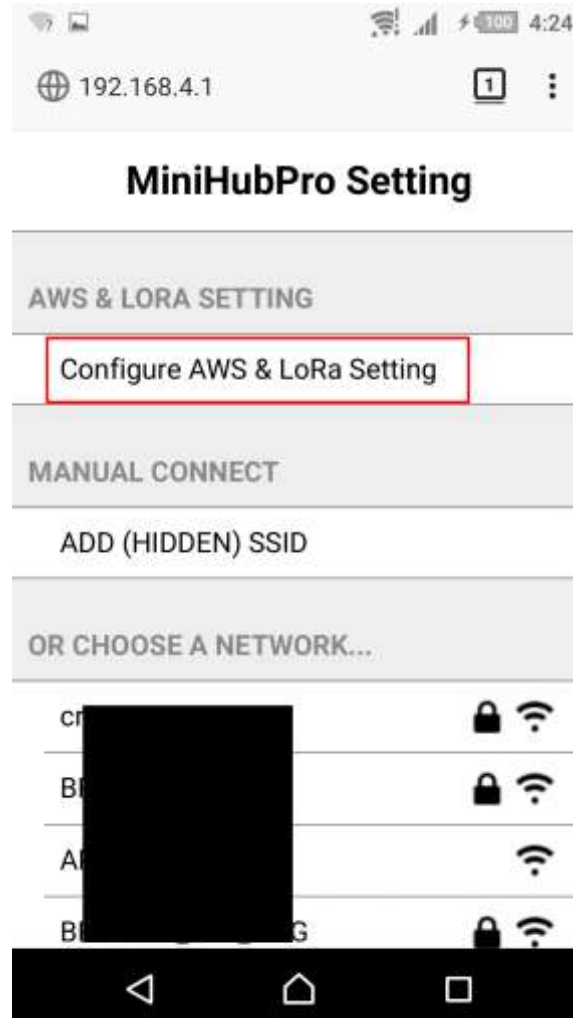


After connecting to **MiniHubPro-XXXXXX** AP, it will open the setup page. If web page doesn't open automatically, please use **Firefox or Chrome** to open **192.168.4.1** manually.



AWS & LoRa Setting

Click "Configure AWS & LoRa Setting" to open the setting page.



There are two parts, one is for AWS, and another one is for LoRa. Please configure your setting and click the "Save" button at the bottom. If you don't want to change any setting, please click the "Cancel" button at the bottom.

🌐 192.168.4.1
📄 1
⋮

AWS & LNS Setting

GATEWAY MAC

246F283F2E34

AMAZON WEB SERVICES (AWS)

AWS IoT Endpoint URI:

AWS IoT Endpoint Thing Name:

Certificate: (*.der)

Private Key: (*.der)

LORA NETWORK SERVER (LNS)

CUPS Enable:

CUPS

Type: Boot Regular

CUPS URI:

CUPS Trust: (installed)

CUPS CRT: (installed)

CUPS Key: (installed)

LNS

LNS URI:

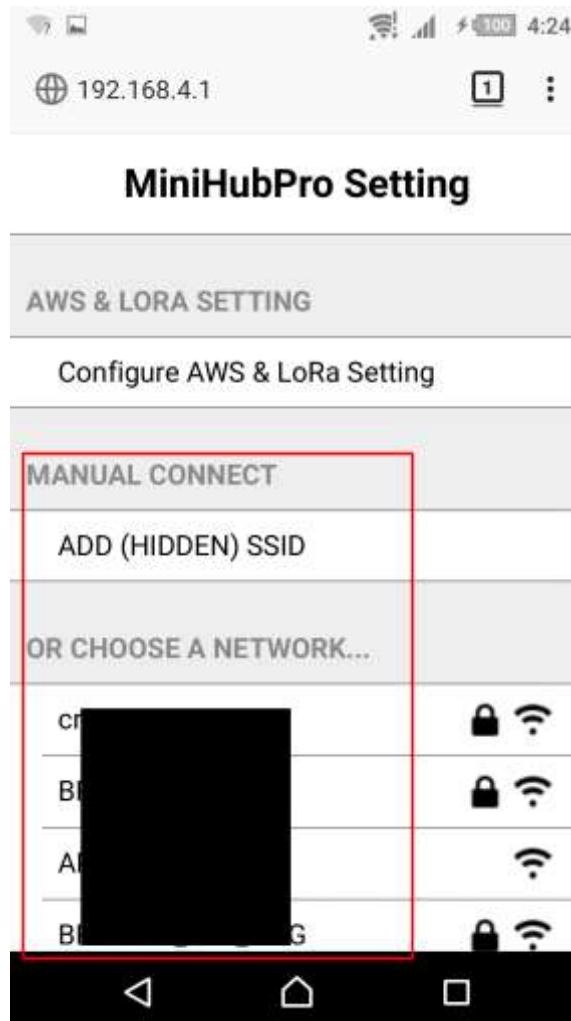
LNS Trust: (non-install)

LNS CRT: (non-install)

LNS Key: (non-install)

WiFi Setting

Choose one of the WiFi AP which you prefer to connect to the internet. You also can add SSID manually by yourself on this page. After that, the MiniHub Pro will store the connection information and switch to the WiFi Station mode.





LED Behavior

Colors	Blink Pattern	Mode	Status
Green	Blinking 1 sec	WIFI_STA	WiFi station not connected
Green	Blinking 1/4 sec	WIFI_STA	WiFi station connected, establishing the connection to LNS, configuring radio
Green	Solid	WIFI_STA	WiFi station connected, Sta is connected to LNS, radio listening
Green/ Orange	Blinking 1/4 sec	WIFI_STA	WiFi station connected, CUPS transaction in progress * Note: Do not unplug device in this state
Orange	Blinking 1/4 sec	CONFIG	Scanning WiFi networks, setting up configuration AP
Orange	Blinking 1 sec	CONFIG	Configuration AP active

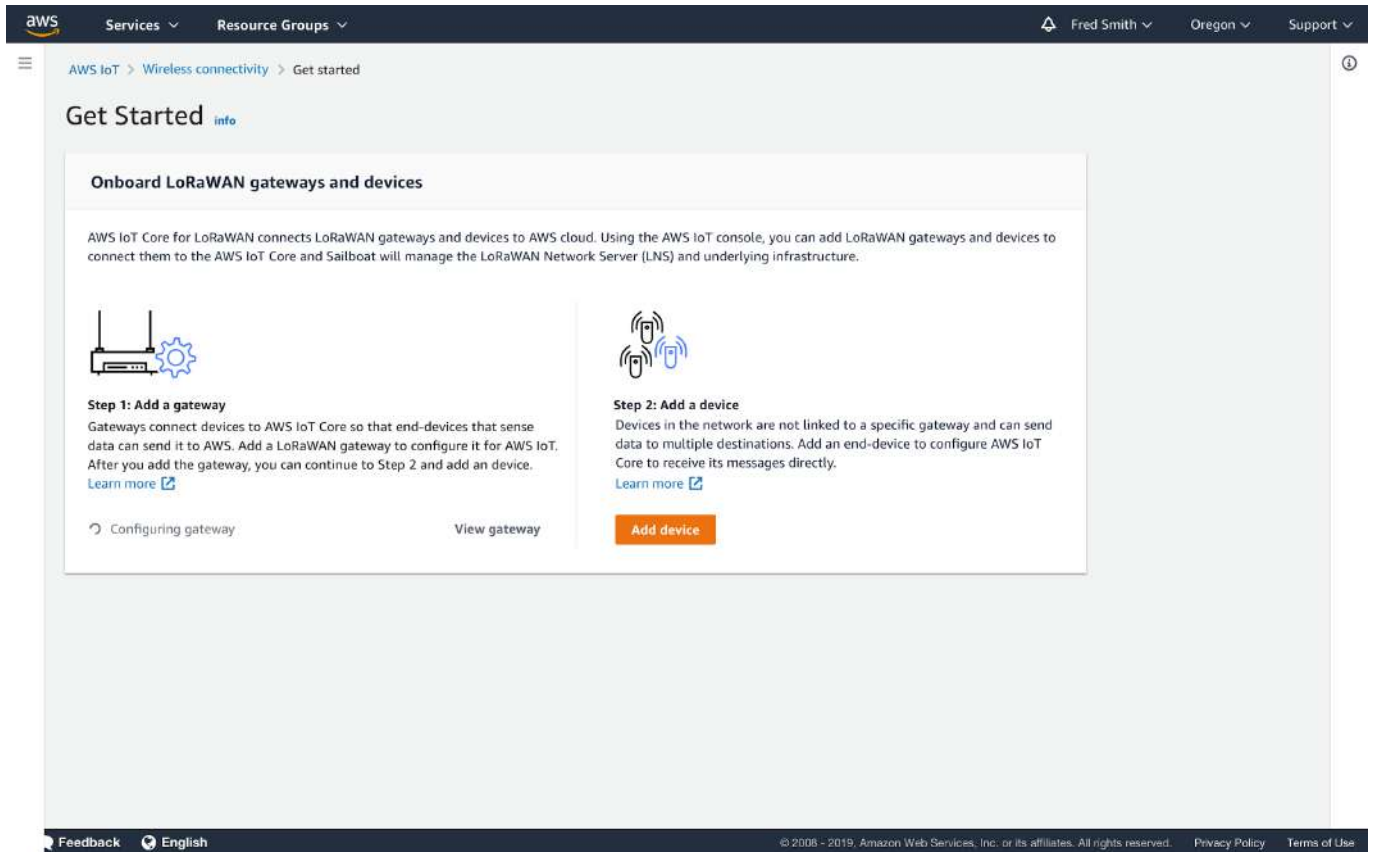
* Note:

WIFI_STA is WiFi Station Mode

CONFIG is Configuration Mode

Onboard LoRaWAN Devices

- Step 1.
Click “Add device”



The screenshot shows the AWS IoT console interface. At the top, there's a navigation bar with 'aws', 'Services', 'Resource Groups', and user information. The main content area is titled 'Get Started' and contains a section 'Onboard LoRaWAN gateways and devices'. This section includes a brief introduction and two main steps:

- Step 1: Add a gateway**
Gateways connect devices to AWS IoT Core so that end-devices that sense data can send it to AWS. Add a LoRaWAN gateway to configure it for AWS IoT. After you add the gateway, you can continue to Step 2 and add an device. [Learn more](#)
- Step 2: Add a device**
Devices in the network are not linked to a specific gateway and can send data to multiple destinations. Add an end-device to configure AWS IoT Core to receive its messages directly. [Learn more](#)

At the bottom of the main content area, there are three buttons: 'Configuring gateway', 'View gateway', and 'Add device' (highlighted in orange).



Step 2.

Register device - Select device specification. Click "Continue"

The screenshot displays the AWS IoT console interface for configuring a device. The breadcrumb navigation shows 'AWS IoT > Wireless connectivity > Get started'. The left sidebar indicates the current step is 'Step 2: Configure device'. The main content area is titled 'Configure device' and includes the instruction: 'Your device has been registered with AWS IoT Core. Now you must configure your device profiles so it can pass messages to your gateway.' The 'Device profile' section features a radio button to 'Select a device profile' and a dropdown menu with the following options: 'US915-B-OTAA', 'US915-C-OTAA', 'EU868-B-OTAA', and 'EU868-C-OTAA'. The 'Service profile' section has a toggle for 'Add metadata to the uplink message', which is currently turned on. At the bottom right, there are three buttons: 'Exit get started', 'Previous', and 'Continue'.



Step 3.

Register device - Input DevEUI, AppEUI, Appkey, Device name(Optional) and Device description(Optional). Click“Continue”.

The screenshot shows the AWS IoT console interface for registering a device. The breadcrumb trail is 'AWS IoT > Wireless connectivity > Get started'. The left sidebar shows a progress indicator with three steps: 'Step 1 Register device' (active), 'Step 2 Configure device', and 'Step 3 Set up destination'. The main content area is titled 'Register device' and contains the following sections:

- LoRaWAN specification version** (Info): A dropdown menu is set to 'Lorawan v1.0.x OTAA'.
- Select device specifications**: A note states 'Your device specifications consist of the LoRaWAN version (1.1 or 1.0.x) and your authentication process (Over The Air Authentication or Authentication By Personalisation.)'. Below this are three pairs of input fields:
 - DevEUI**: Input field contains '1234567890123456'. Confirmation field contains '1234567890123456'. Note: 'A 16-digit alphanumeric code found on your end-device'.
 - AppEUI**: Input field contains '1234567890123456'. Confirmation field contains '1234567890123456'. Note: 'A 16-digit alphanumeric code provided by your vendor'.
 - Appkey**: Input field contains '01020304050607080910111213141516'. Confirmation field contains '01020304050607080910111213141516'. Note: 'A 32-digit alphanumeric code provided by your vendor'.
- Device name - optional**: Input field contains 'Hallway 3rd Floor'. Note: 'Enter a descriptive name to make the end-device easier to locate'.
- Device description - optional**: Input field contains 'Company - Hallway 3rd Floor'. Note: 'Provide a user-friendly description of the gateway'.
- Associate a thing** (Info): A checkbox labeled 'Associate a Thing with your device' is checked. Note: 'We will automatically create a unique Thing for you. Adding things to AWS registry allows you to manage and search for devices more easily.'

At the bottom right of the form, there are two buttons: 'Exit get started' and 'Continue'.



Step 4.

Configure devices - Select device profile. Click "Continue"

Configure device

Your device has been registered with AWS IoT Core. Now you must configure your device profiles so it can pass messages to your gateway.

Device profile [Info](#)

Select a device profile
Select a default device profile dependent on your chosen hardware. Check your device details provided by your vendor.

US915-B-OTAA

Variable name	Value
Channel	US915
MacVersion	v1.1
MaxEIRP	16dBm
RegParamsRevision	8
ClassBTimeout	30
PingSlotDr	0
PingSlotPeriod	128
PingSlotFreq	924.5

Advanced Setting - Create new device profile
Enter required information to create a new device profile

Service profile [Info](#)

The service-profile defines the features that are enabled for the associated devices and the rate of messages that the associated devices can send over the network.

Add metadata to the uplink message
Metadata added by gateway includes RSSI, SNR, Data rate

Exit get started



Step 5.

Set up destination- Select IAM role and input rule name. Click“Finish”

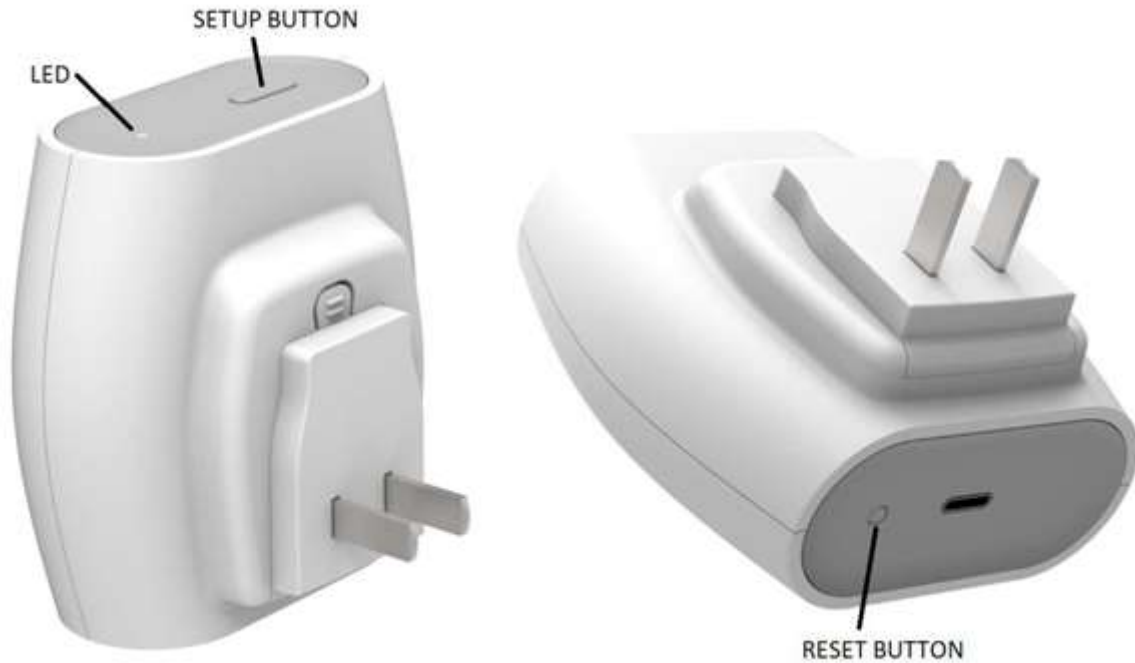
The screenshot shows the AWS IoT console interface for setting up a destination. The page title is "Set up destination". On the left, there is a navigation pane with three steps: "Step 1 Register device", "Step 2 Configure device", and "Step 3 Set up destination" (which is currently selected). The main content area is divided into three sections:

- Permissions**: Under "Select IAM Role", a dropdown menu is set to "LoRaWAN for AWS IoT Core-IAM".
- Create a destination**:
 - Name destination**: A text input field contains "destination-device-semtech-1".
 - Enter rule name**: A text input field contains "company-device-semtech-1". A "Copied to clipboard" notification is visible above the field.
- Rules engine configuration - skip and set up later**: A section with instructions to open the Rules engine and enter the rule name copied above.

At the bottom of the page, there are three buttons: "Exit get started", "Previous", and "Finish". The footer contains "Feedback", "English (US)", and copyright information for Amazon Web Services, Inc. (2008-2020).



Reset to Default



Press the reset button over 5 seconds to reset the system to default status. After reset to default, the orange LED will blink every 1 second.

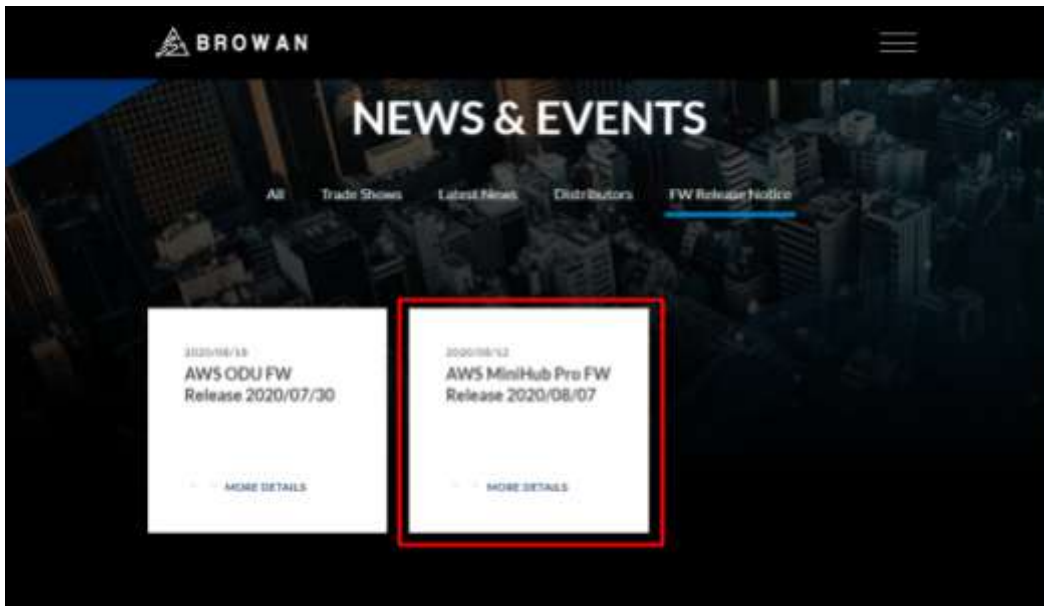


OTA

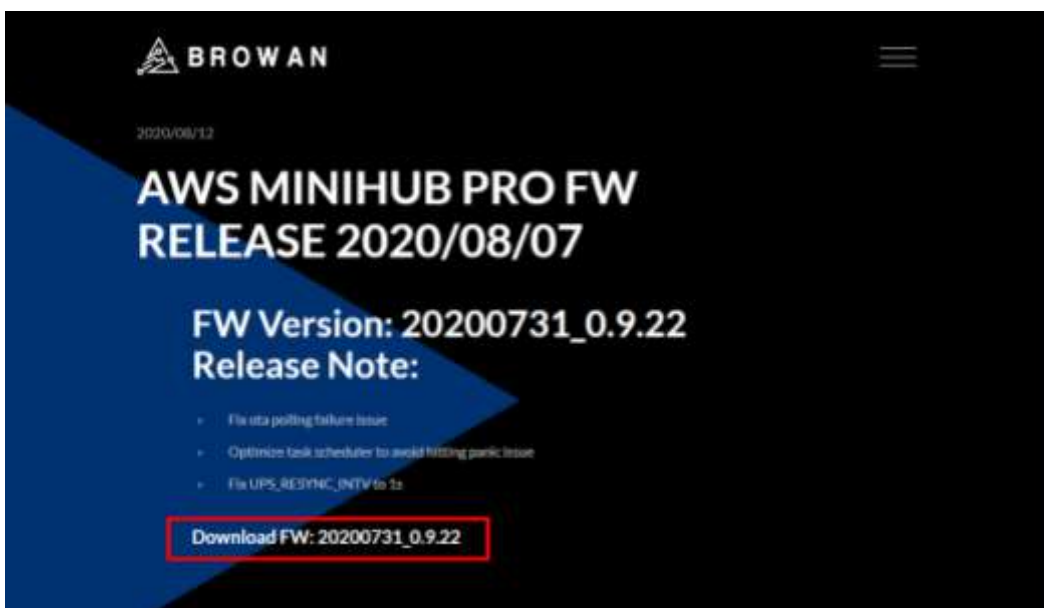
Get Firmware

1. Please visit Browan's website and click release note for MiniHub Pro.

<https://www.browan.com/news/9V>



2. Download the latest MiniHub Pro's firmware.



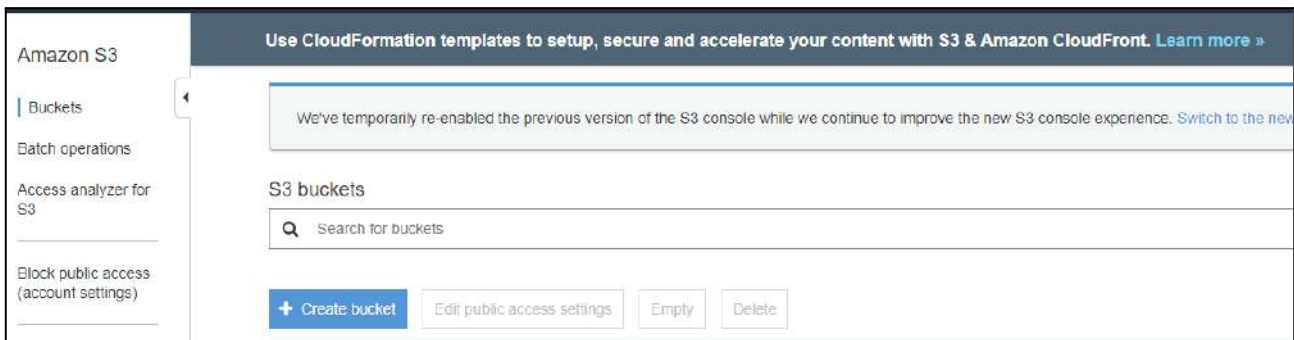
Configure MiniHub Pro

Please register things for MiniHub Pro on the AWS IoT and configure the AWS & LNS Setting.

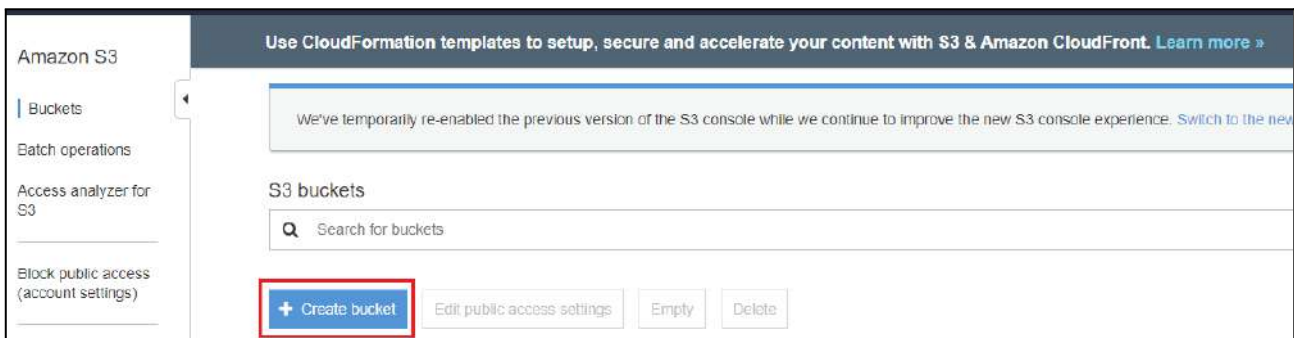
AWS & LNS Setting	
GATEWAY MAC	246F283D807C
AMAZON WEB SERVICES (AWS)	
AWS IoT Endpoint URI:	<input type="text" value="aws.iot.us-east-1.amazonaws.com:8883"/>
AWS IoT Endpoint Thing Name:	<input type="text" value="MiniHubPro-3D807C"/>
Certificate: (*.der)	<input type="button" value="Choose File"/> cert.der
Private Key: (*.der)	<input type="button" value="Choose File"/> privatekey.der

Create an Amazon S3 bucket to store your update

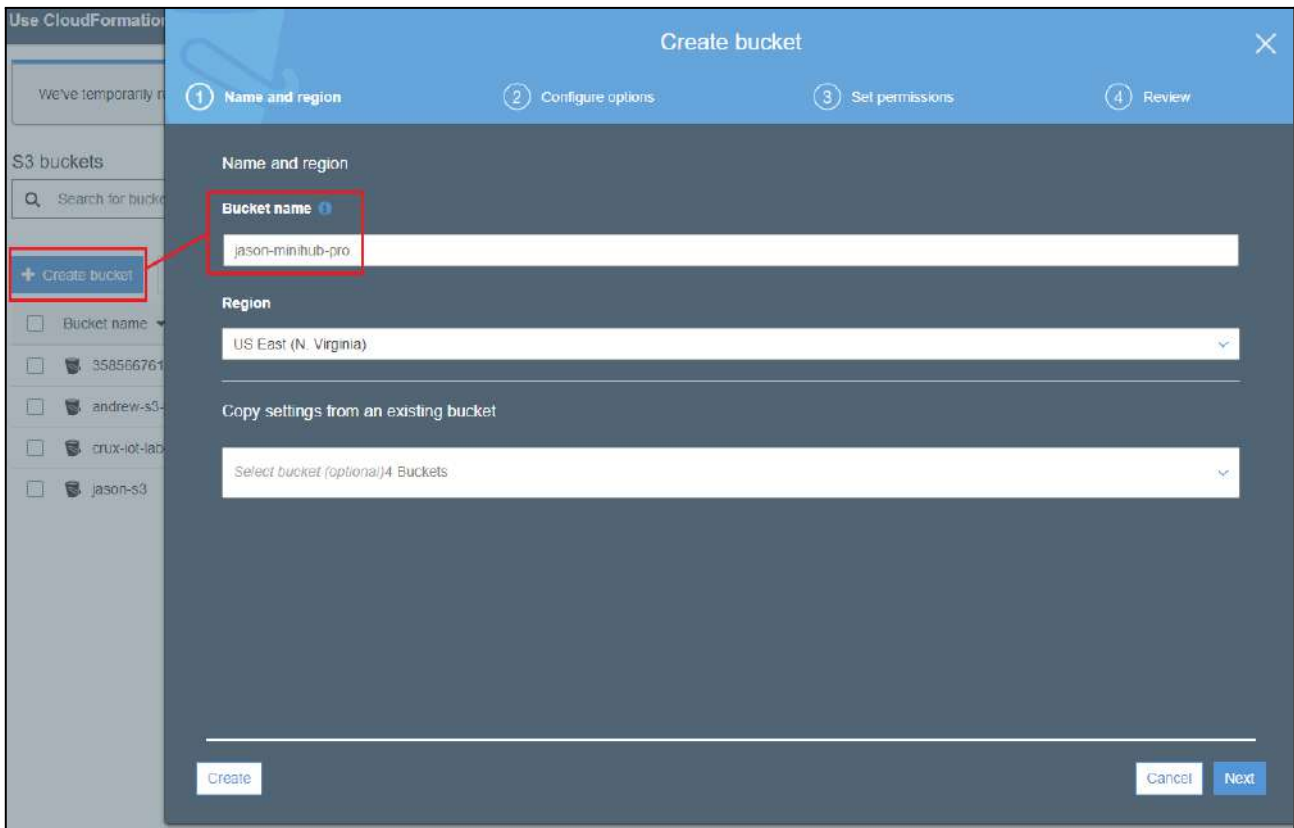
1. Sign in to the Amazon S3 console at <https://console.aws.amazon.com/s3/>.



2. Choose **Create bucket**.

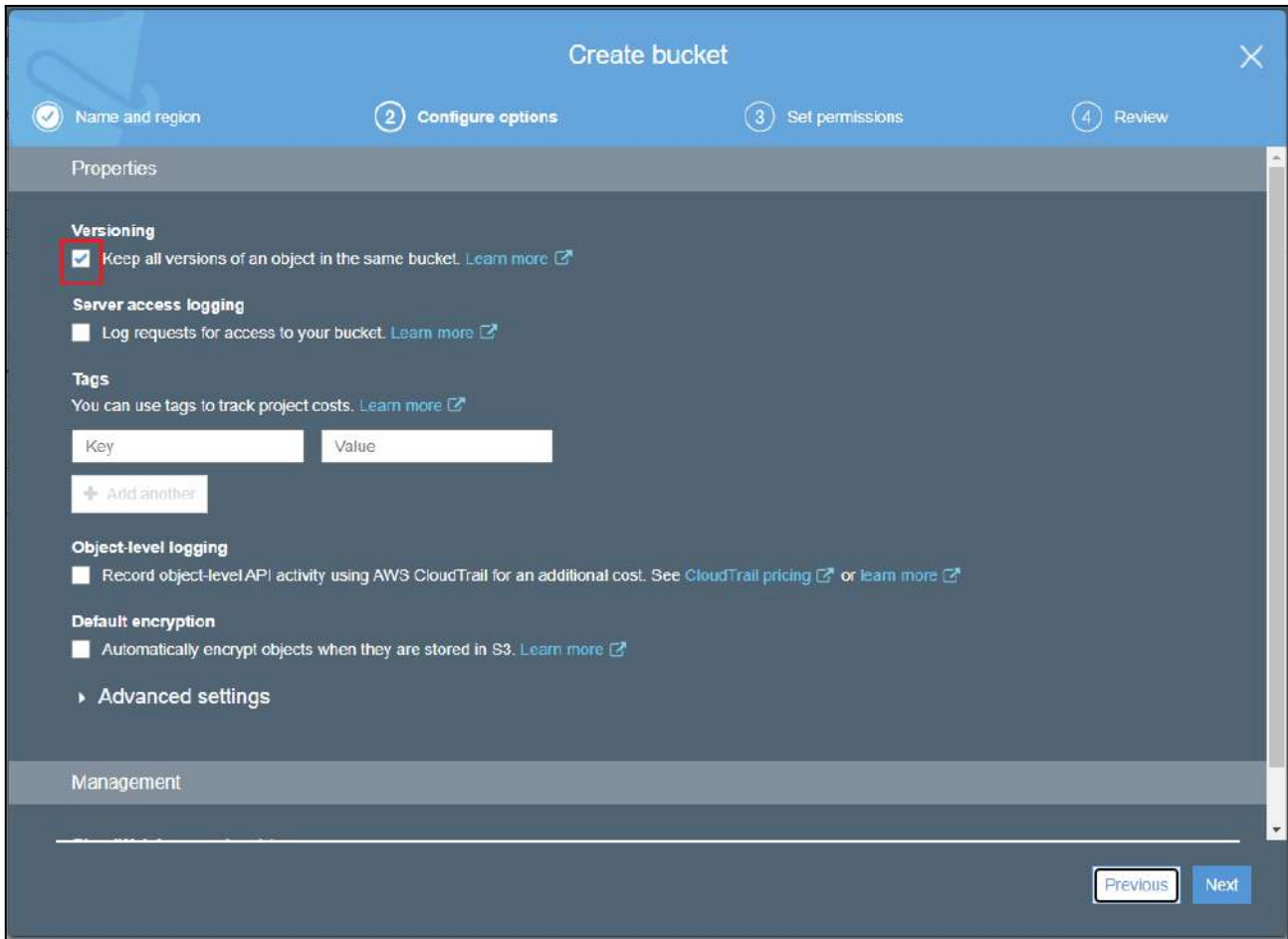


3. Enter a **bucket name**.



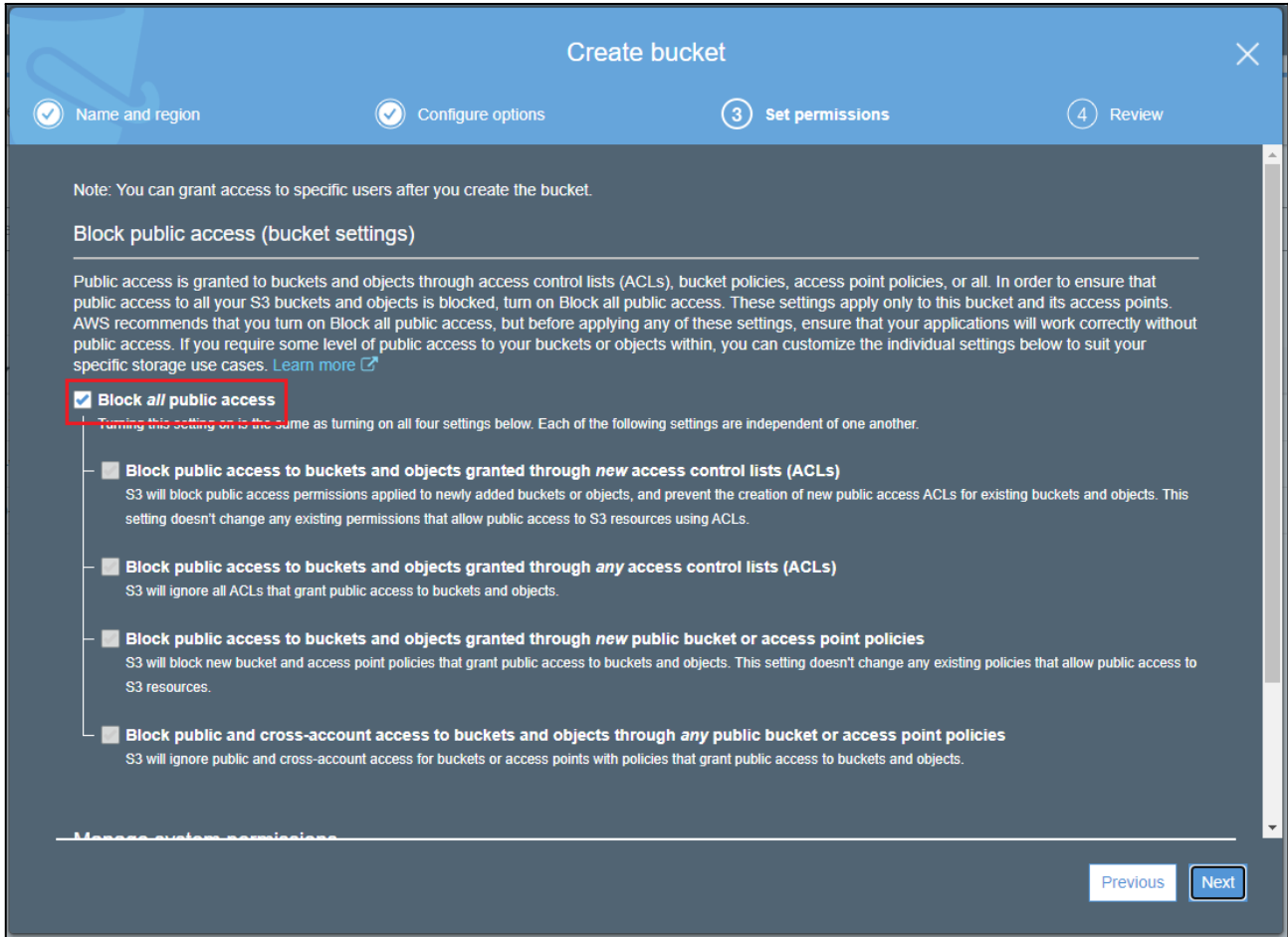


4. Under **Bucket Versioning**, select **Enable** to keep all versions in the same bucket.





5. Under **Bucket settings for Block Public Access** keep **Block all public access** selected to accept the default permissions.





6. Choose **Create bucket**.

The screenshot shows the 'Create bucket' wizard in the AWS console, specifically the 'Review' step (indicated by a '4' in a circle). The wizard has four steps: 'Name and region', 'Configure options', 'Set permissions', and 'Review'. The 'Review' step is active, showing a summary of the configuration. At the bottom right, the 'Create bucket' button is highlighted with a red box.

Create bucket

✓ Name and region ✓ Configure options ✓ Set permissions 4 Review

Name and region [Edit](#)

Bucket name jason-minihub-pro **Region** US East (N. Virginia)

Options [Edit](#)

Versioning	Enabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions [Edit](#)

Block all public access On

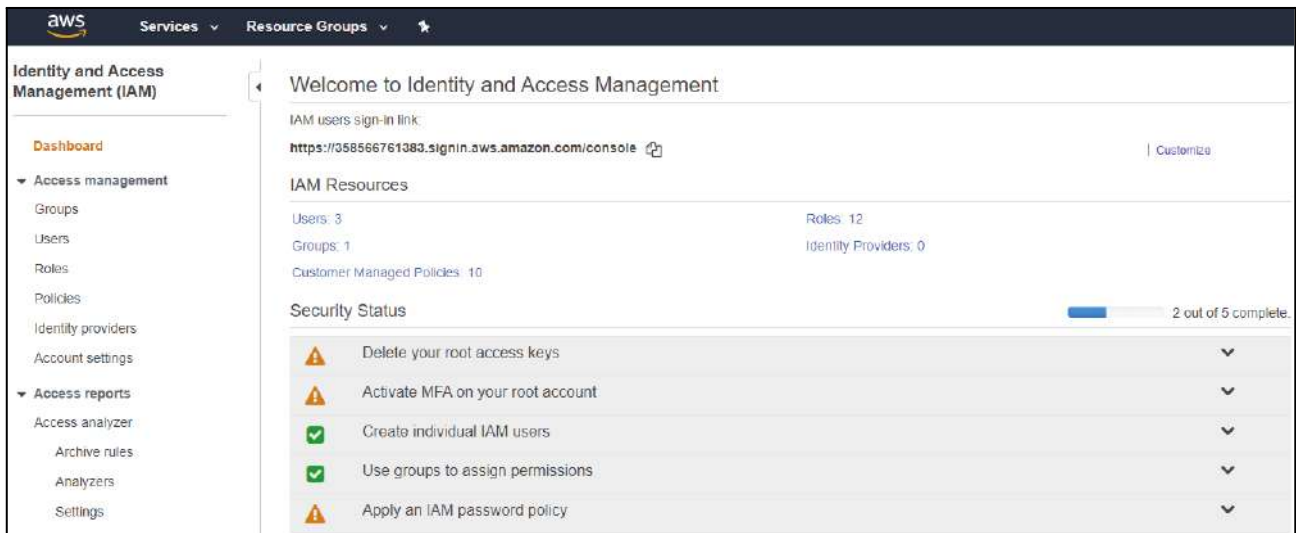
- Block public access to buckets and objects granted through *new* access control lists (ACLs) On
- Block public access to buckets and objects granted through *any* access control lists (ACLs) On

[Previous](#) [Create bucket](#)

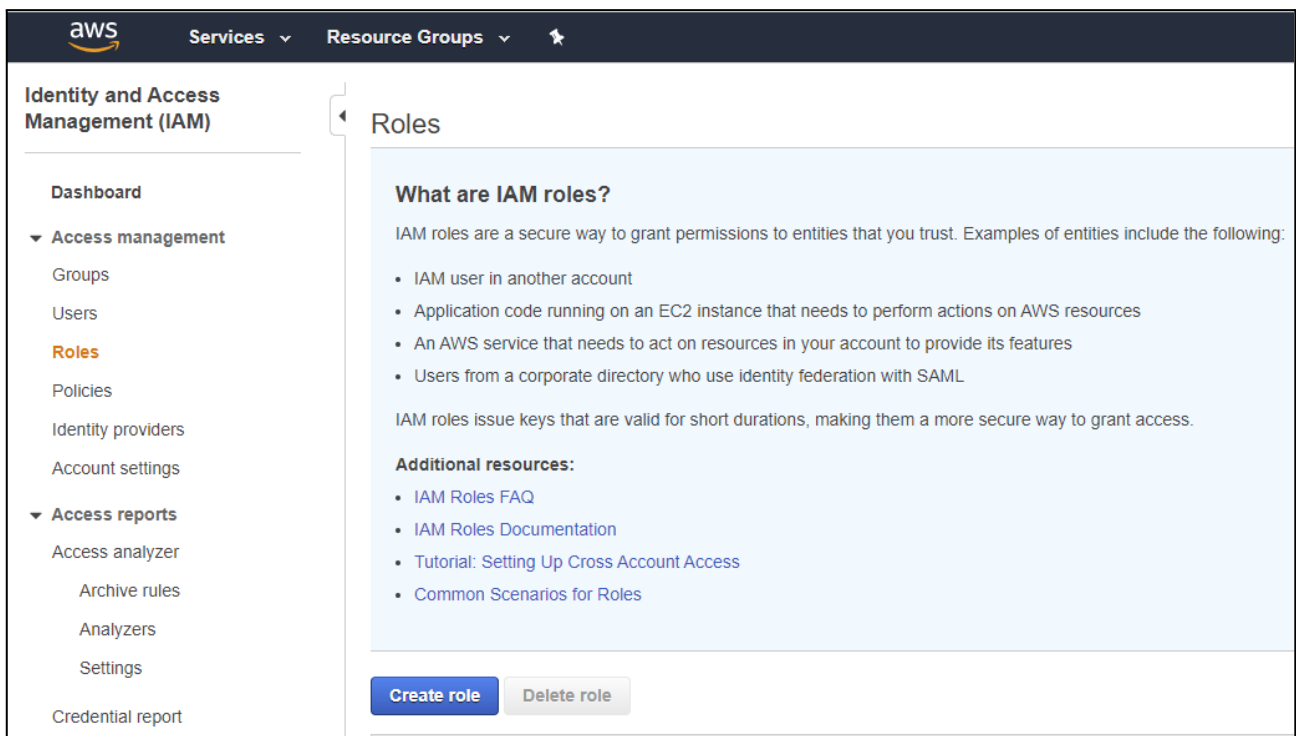
Create an OTA Update service role

To create an OTA service role

1. Sign in to the <https://console.aws.amazon.com/iam/>.



2. From the navigation pane, choose **Roles**.



3. Choose **Create role**.

Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)


Create role Delete role


4. Under **Select type of trusted entity**, choose **AWS Service**.


Create role


1 2 3 4

Select type of trusted entity

 **AWS service**
EC2, Lambda and others

 **Another AWS account**
Belonging to you or 3rd party

 **Web identity**
Cognito or any OpenID provider

 **SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.



5. Choose IoT from the list of AWS services.

AWS Support	Comprehend	Elastic Container Service	Lambda	SMS
Amplify	Config	Elastic Transcoder	Lex	SNS
AppStream 2.0	Connect	ElasticLoadBalancing	License Manager	SWF
AppSync	DMS	Forecast	Machine Learning	SageMaker
Application Auto Scaling	Data Lifecycle Manager	GameLift	Macie	Security Hub
Application Discovery Service	Data Pipeline	Global Accelerator	Managed Blockchain	Service Catalog
Batch	DataSync	Glue	MediaConvert	Step Functions
Certificate Manager	DeepLens	Greengrass	Migration Hub	Storage Gateway
Chime	Directory Service	GuardDuty	OpsWorks	Systems Manager
CloudFormation	DynamoDB	Health Organizational View	Personalize	Textract
CloudHSM	EC2	IAM Access Analyzer	Purchase Orders	Transfer
CloudTrail	EC2 - Fleet	Inspector	QLDB	Trusted Advisor
CloudWatch Application Insights	EC2 Auto Scaling	IoT	RAM	VPC
CloudWatch Events	EC2 Image Builder	IoT SiteWise	RDS	WorkLink
CodeBuild	EKS	IoT Things Graph	Redshift	WorkMail

6. Under Select your use case, choose IoT.

Chime	DynamoDB	Health Organizational View	Personalize	Textract
CloudFormation	EC2	IAM Access Analyzer	Purchase Orders	Transfer
CloudHSM	EC2 - Fleet	Inspector	QLDB	Trusted Advisor
CloudTrail	EC2 Auto Scaling	IoT	RAM	VPC
CloudWatch Application Insights	EC2 Image Builder	IoT SiteWise	RDS	WorkLink
CloudWatch Events	EKS	IoT Things Graph	Redshift	WorkMail
CodeBuild				

Select your use case

IoT Allows IoT to call AWS services on your behalf
IoT - Device Defender Audit Provides AWS IoT Device Defender read access to IoT and related resources.
IoT - Device Defender Mitigation Actions Provides AWS IoT Device Defender write access to IoT and related resources for execution of Mitigation Actions.



7. Choose **Next: Tags**.

Select your use case

IoT
Allows IoT to call AWS services on your behalf.

IoT - Device Defender Audit
Provides AWS IoT Device Defender read access to IoT and related resources.

IoT - Device Defender Mitigation Actions
Provides AWS IoT Device Defender write access to IoT and related resources for execution of Mitigation Actions.

* Required Cancel **Next: Permissions**

8. Choose **Next: Review**.

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel **Next: Review**



9. Enter a role name and description, and then choose **Create role**.

Review

Provide the required information below and review this role before you create it.

Role name* Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities AWS service: [iot.amazonaws.com](#)

Policies

- [AWSIoTLogging](#)
- [AWSIoTRuleActions](#)
- [AWSIoTThingsRegistration](#)

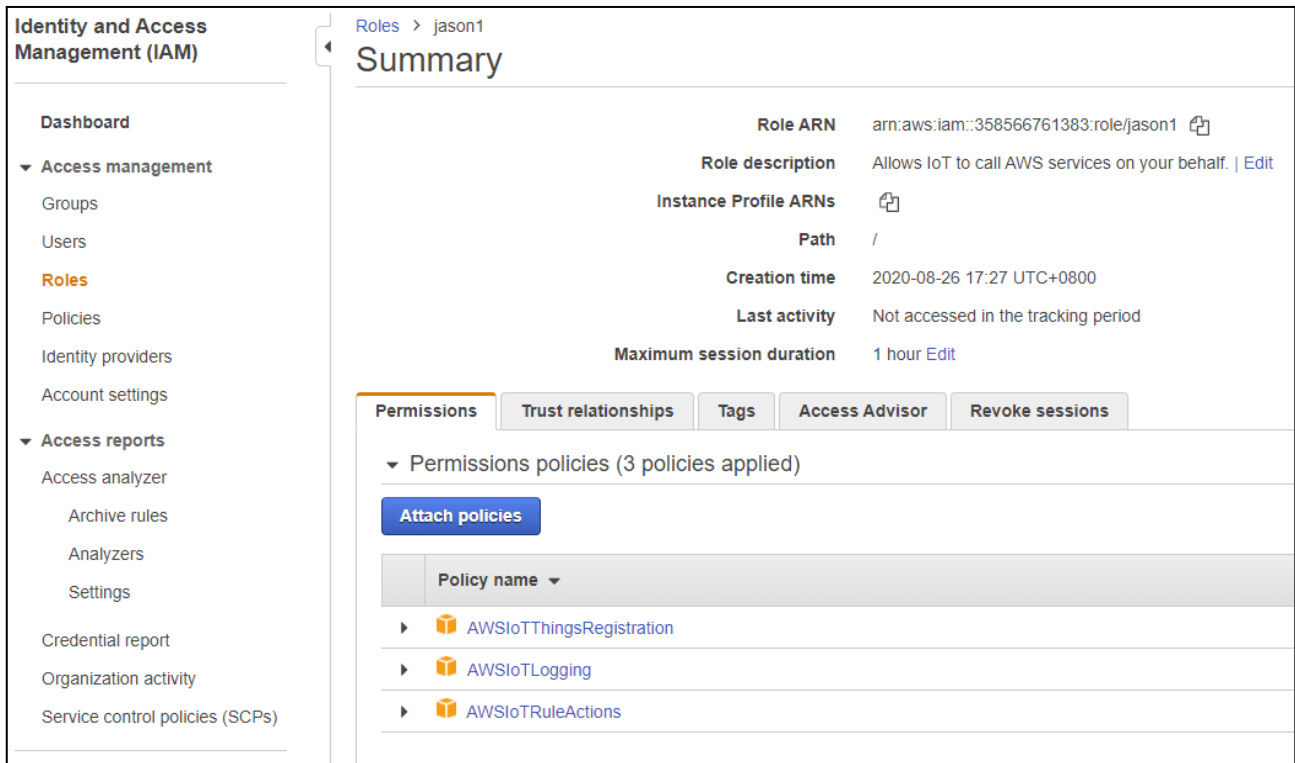
Permissions boundary Permissions boundary is not set

No tags were added.

* Required Cancel Previous **Create role**

5 To add OTA update permissions to your OTA service role

1. In the search box on the IAM console page, enter the name of your role, and then choose it from the list.



Identity and Access Management (IAM)

Roles > jason1

Summary

Role ARN	arn:aws:iam::358566761383:role/jason1 Copy
Role description	Allows IoT to call AWS services on your behalf. Edit
Instance Profile ARNs	Copy
Path	/
Creation time	2020-08-26 17:27 UTC+0800
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (3 policies applied)

[Attach policies](#)

Policy name
AWSIoTThingsRegistration
AWSIoTLogging
AWSIoTRuleActions



2. Choose **Attach policies**.

Roles > jason1

Summary

Role ARN	arn:aws:iam::358566761383:role/jason1
Role description	Allows IoT to call AWS services on your behalf. Edit
Instance Profile ARNs	
Path	/
Creation time	2020-08-26 17:27 UTC+0800
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

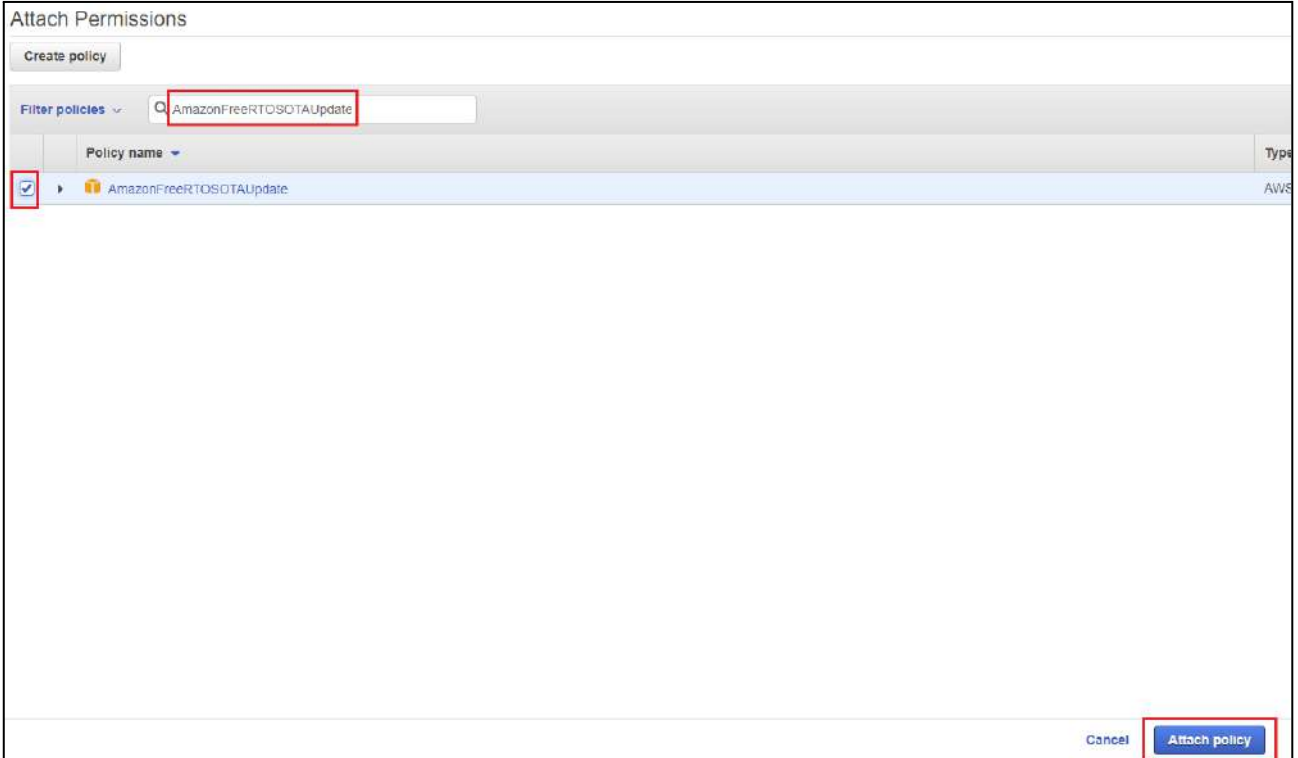
▼ Permissions policies (3 policies applied)

Attach policies

Policy name ▼
▶ AWSIoTThingsRegistration
▶ AWSIoTLogging

[Show 1 more](#)

- In the **Search** box, enter "AmazonFreeRTOSOTAUpdate", select **AmazonFreeRTOSOTAUpdate** from the list of filtered policies, and then choose **Attach policy** to attach the policy to your service role.



Attach Permissions

Create policy

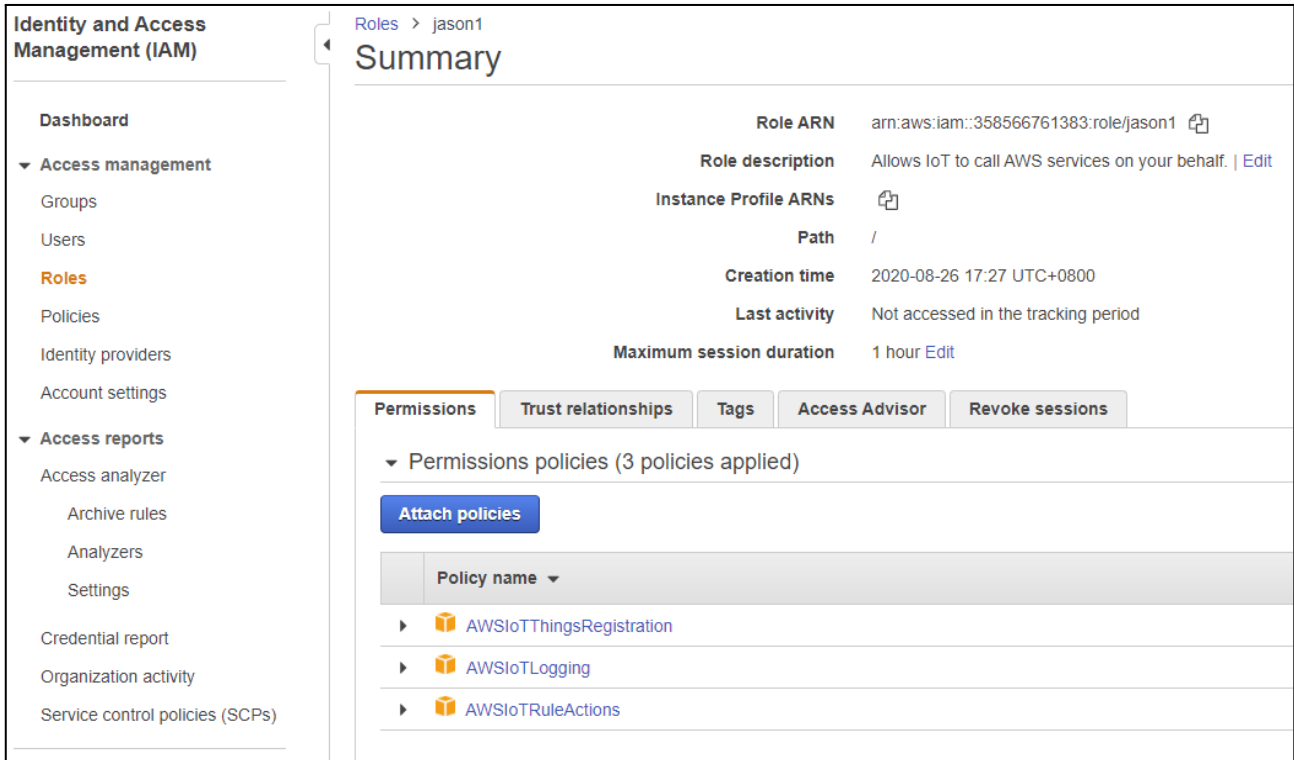
Filter policies

Policy name	Type
<input checked="" type="checkbox"/> AmazonFreeRTOSOTAUpdate	AWS

Cancel

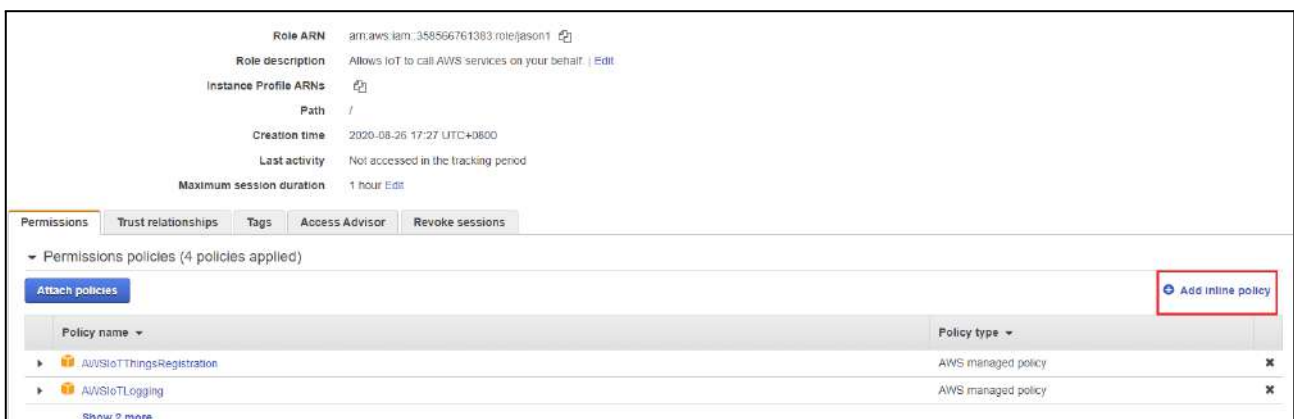
To add the required IAM permissions to your OTA service role

1. In the search box on the IAM console page, enter the name of your role, and then choose it from the list.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with categories like 'Access management' and 'Access reports'. The main content area is titled 'Roles > jason1 Summary'. It displays role details such as Role ARN, Role description, Instance Profile ARNs, Path, Creation time, Last activity, and Maximum session duration. Below this, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Permissions' tab is active, showing 'Permissions policies (3 policies applied)'. An 'Attach policies' button is visible, and a table lists three policies: AWSIoTThingsRegistration, AWSIoTLogging, and AWSIoTRuleActions.

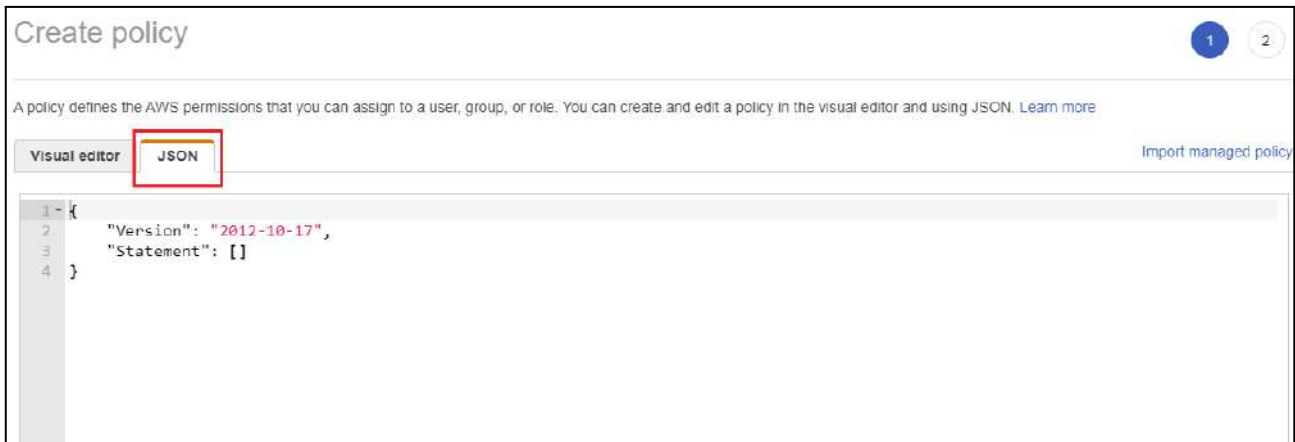
2. Choose **Add inline policy**.



This screenshot shows the same IAM console page as above, but with an additional policy attached. The 'Permissions policies (4 policies applied)' section now includes a fourth policy. A red box highlights the 'Add inline policy' button in the top right corner of the policy list area. The table below shows the first two policies: AWSIoTThingsRegistration and AWSIoTLogging, both identified as 'AWS managed policy'.



3. Choose the **JSON** tab.



4. Copy and paste the following policy document into the text box:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetRole",  
        "iam:PassRole"  
      ],  
      "Resource": "arn:aws:iam::your_account_id:role/your_role_name"  
    }  
  ]  
}
```



Make sure that you replace `your_account_id` with your AWS account ID, and `your_role_name` with the name of the OTA service role.

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create an

Visual editor

JSON

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:GetRole",
8         "iam:PassRole"
9       ],
10      "Resource": "arn:aws:iam:██████████:role/jason1"
11    }
12  ]
13 }
14
```



5. Choose **Review** policy.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:GetRole",
8         "iam:PassRole"
9       ],
10      "Resource": "arn:aws:iam::[redacted]:role/jason1"
11    }
12  ]
13 }
14
```

Character count: 148 of 10,240.
The current character count includes character for all inline policies in the role: jason1.

Cancel Review policy

6. Enter a name for the policy, and then choose **Create** policy.

Review policy

Before you create this policy, provide the required information and review this policy.

Name*

Maximum: 128 characters. Use alphanumeric, and +, -, @, _ characters.

Summary

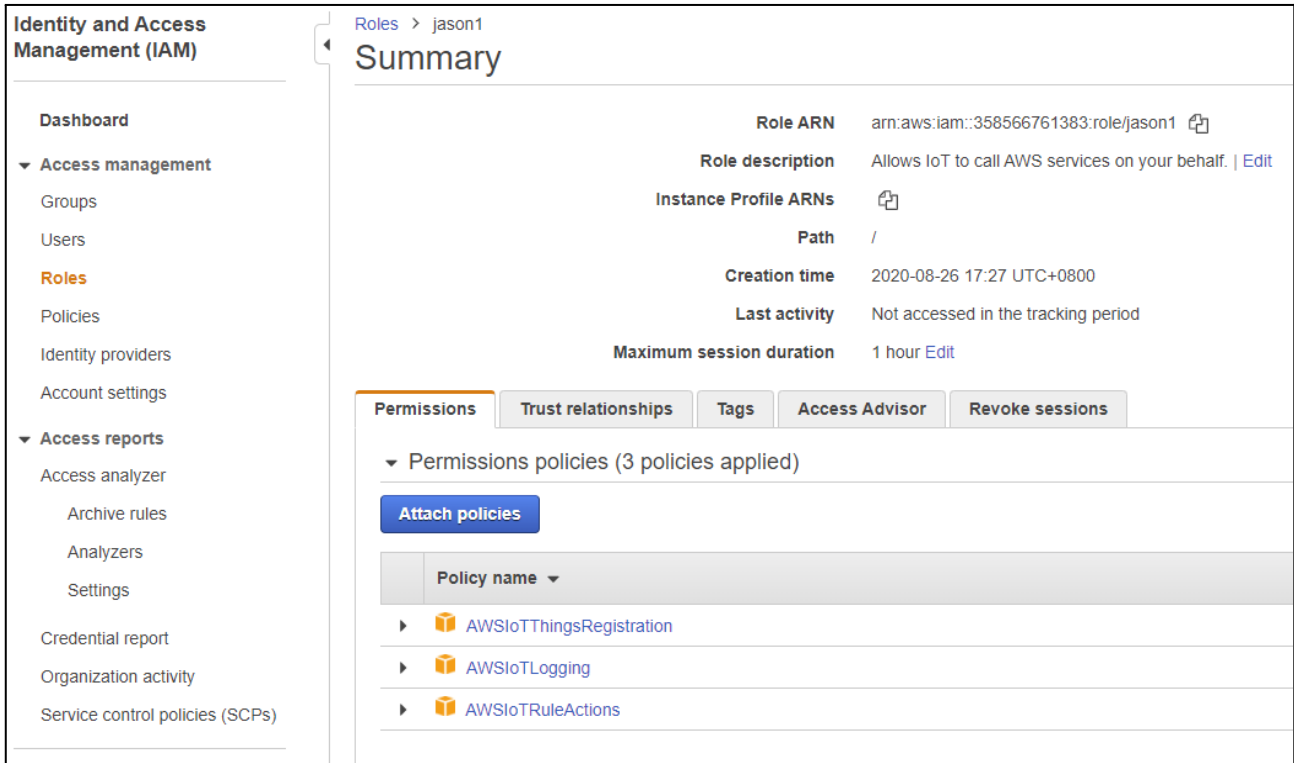
Service	Access level	Resource	Request condition
Allow (1 of 238 services) Show remaining 237			
IAM	Limited Read, Write	RoleName string like jason1	None

^ Required

Cancel Previous Create policy

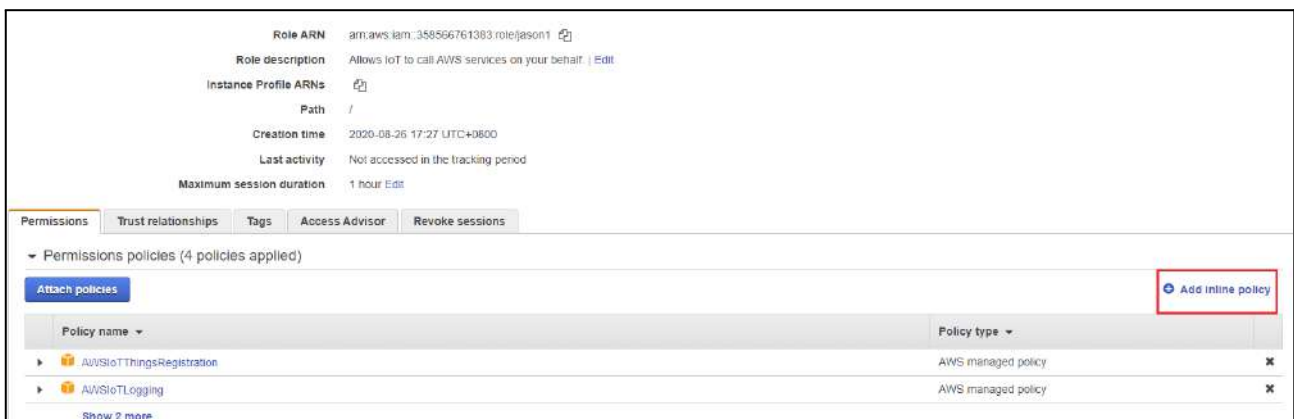
To add the required Amazon S3 permissions to your OTA service role

1. In the search box on the IAM console page, enter the name of your role, and then choose it from the list.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu for 'Identity and Access Management (IAM)'. The main content area is titled 'Roles > jason1 Summary'. It displays role details such as Role ARN, Role description, Instance Profile ARNs, Path, Creation time, Last activity, and Maximum session duration. Below this, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Permissions' tab is active, showing 'Permissions policies (3 policies applied)'. An 'Attach policies' button is visible, and a list of attached policies includes AWSIoTThingsRegistration, AWSIoTLogging, and AWSIoTRuleActions.

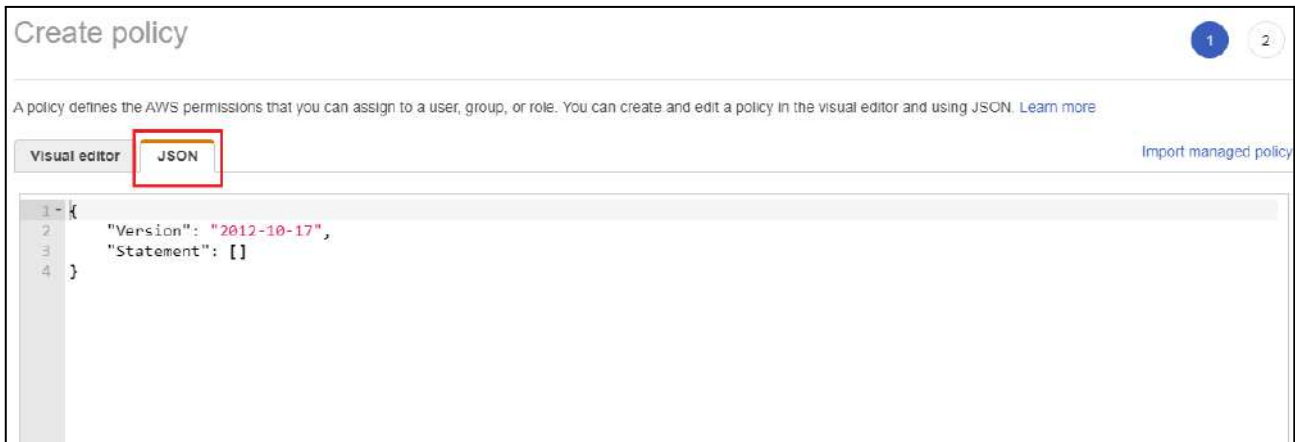
2. Choose **Add inline policy**.



This screenshot shows the same IAM console page as above, but with the 'Permissions' tab showing 'Permissions policies (4 policies applied)'. The 'Attach policies' button is still present. A red box highlights the 'Add inline policy' button in the top right corner of the permissions section. Below the button, a table lists the attached policies, including AWSIoTThingsRegistration and AWSIoTLogging, both identified as 'AWS managed policy'.



3. Choose the **JSON** tab.



4. Copy and paste the following policy document into the box.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:GetObjectVersion",  
        "s3:GetObject",  
        "s3:PutObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::example-bucket/*"  
      ]  
    }  
  ]  
}
```



This policy grants your OTA service role permission to read Amazon S3 objects. Make sure that you replace example-bucket with the name of your bucket.

```
Visual editor  JSON
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:GetObjectVersion",
8         "s3:GetObject",
9         "s3:PutObject"
10      ],
11      "Resource": [
12        "arn:aws:s3:::jason-minihub-pro/*"
13      ]
14    }
15  ]
16 }
17
```




5. Choose **Review policy**.

```
1- {  
2  "Version": "2012-10-17",  
3  "Statement": [  
4    {  
5      "Effect": "Allow",  
6      "Action": [  
7        "s3:GetObjectVersion",  
8        "s3:GetObject",  
9        "s3:PutObject"  
10     ],  
11     "Resource": [  
12       "arn:aws:s3:::jason-minihub-pro/*"  
13     ]  
14   }  
15 ]  
16 }  
17 }
```

Character count: 316 of 10,240.
The current character count includes character for all inline policies in the role: jason1.

Cancel **Review policy**



6. Enter a name for the policy, and then choose **Create policy**.

Review policy

Before you create this policy, provide the required information and review this policy.

Name*

Maximum 128 characters. Use alphanumeric and "+=, @-_" characters.

Summary

Q Filter

Service	Access level	Resource	Request condition
Allow (1 of 238 services) Show remaining 237			
S3	Limited Read, Write	BucketName string like jason-minihub-pro, ObjectPath string like All	None

* Required

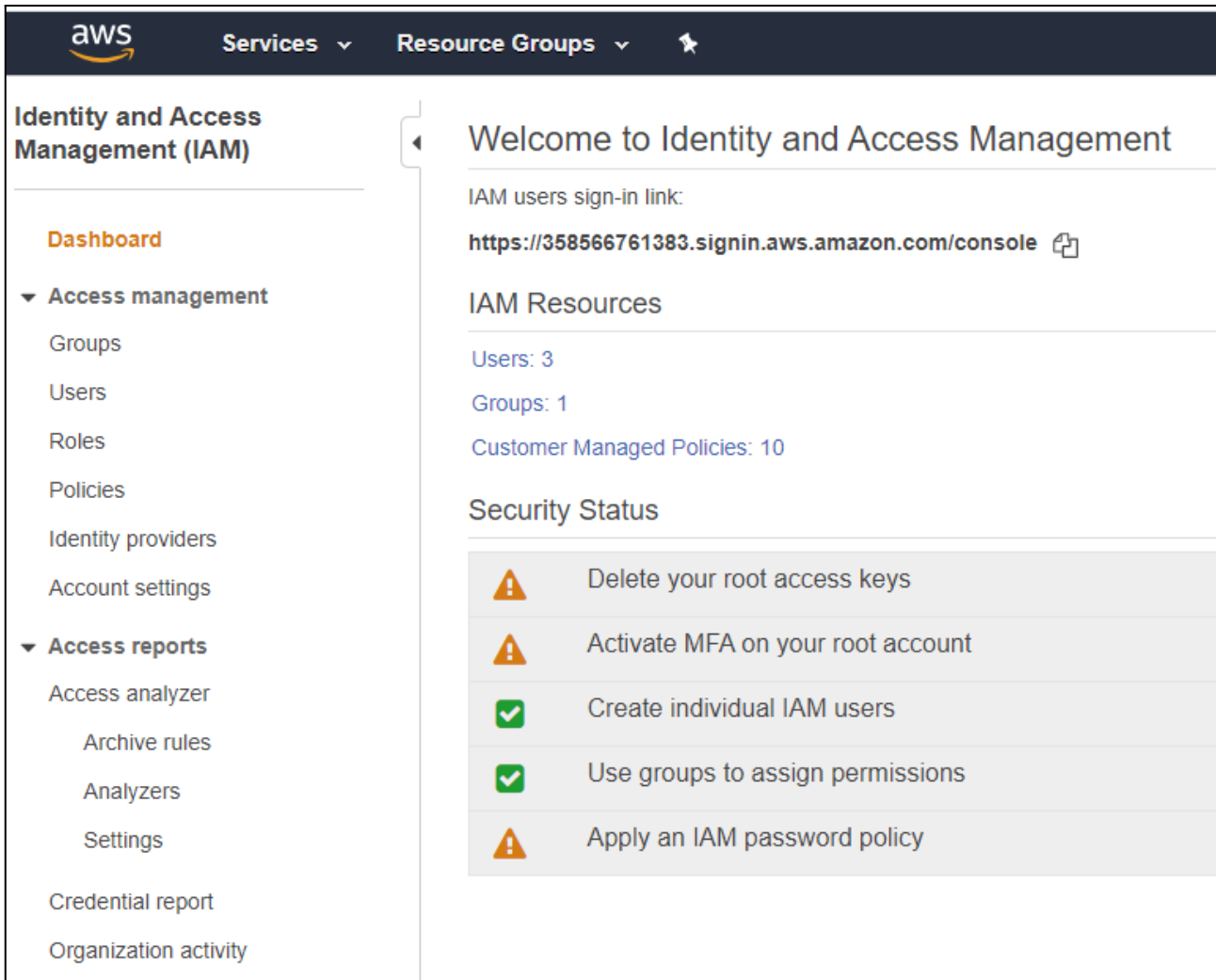
Cancel Previous **Create policy**

Create an OTA user policy

*If you use the "Administrator" user, you can skip this step.

To create an OTA user policy

1. Open the <https://console.aws.amazon.com/iam/> console.



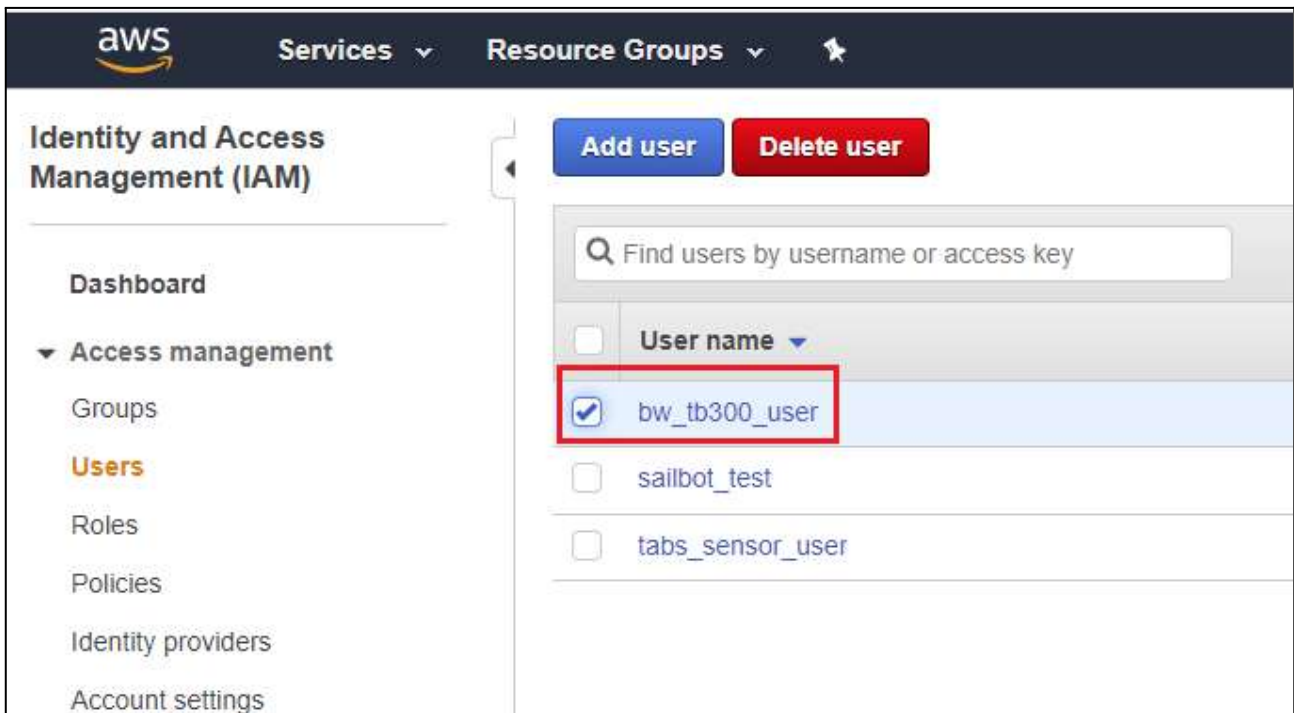
The screenshot displays the AWS IAM console dashboard. The left sidebar shows the navigation menu with categories like 'Access management' and 'Access reports'. The main content area is titled 'Welcome to Identity and Access Management' and provides a sign-in link for IAM users. Below this, it lists IAM resources: 3 Users, 1 Group, and 10 Customer Managed Policies. A 'Security Status' section contains five alerts: 'Delete your root access keys' (warning), 'Activate MFA on your root account' (warning), 'Create individual IAM users' (checkmark), 'Use groups to assign permissions' (checkmark), and 'Apply an IAM password policy' (warning).



2. In the navigation pane, choose **Users**.

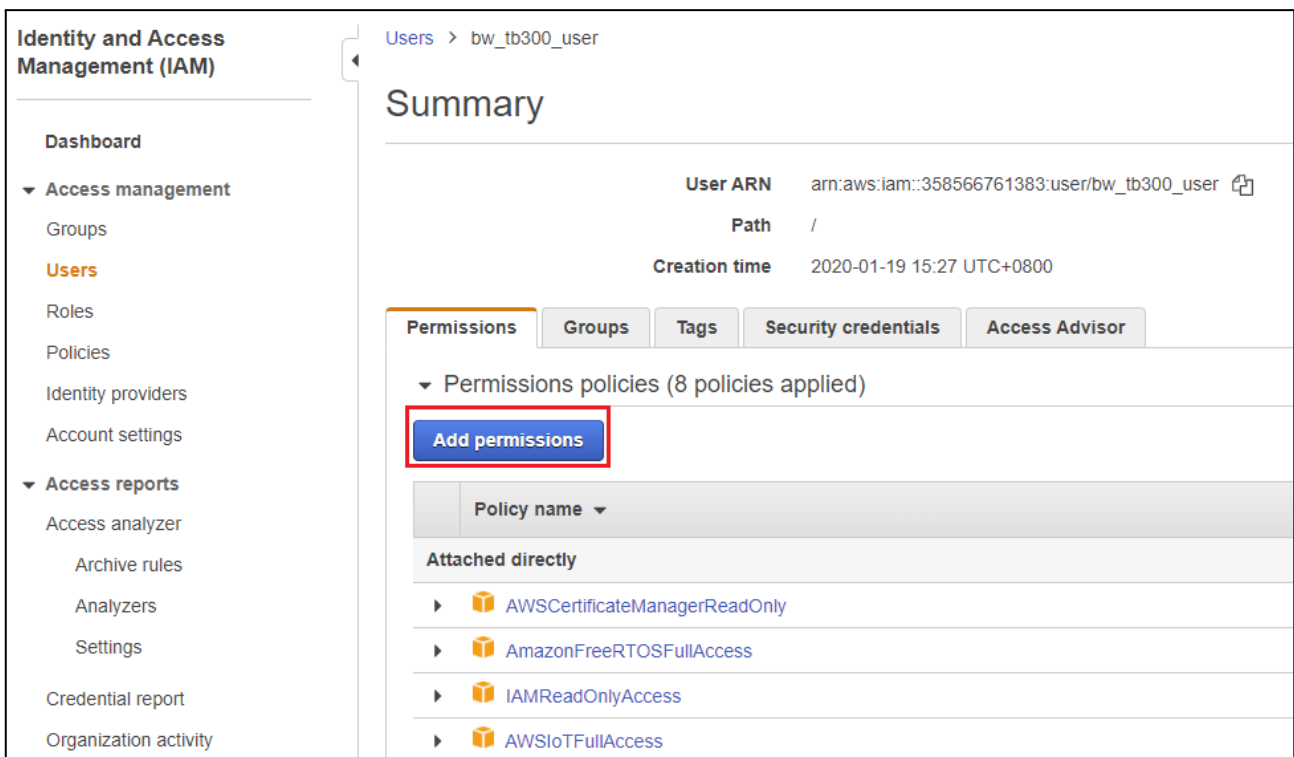
The screenshot displays the Identity and Access Management (IAM) interface. On the left, a navigation pane is titled "Identity and Access Management (IAM)". It contains several sections: "Dashboard", "Access management" (expanded), "Access reports" (expanded), and "Access analyzer". Under "Access management", the "Users" option is highlighted with a red rectangular box. Other options in this section include "Groups", "Roles", "Policies", "Identity providers", and "Account settings". Under "Access reports", there are "Access analyzer", "Archive rules", and "Analyzers". The main content area on the right features two buttons at the top: "Add user" (blue) and "Delete user" (red). Below these is a search bar with the placeholder text "Find users by username or access key". A dropdown menu is open, showing "User name" with a downward arrow. Below the dropdown, three user entries are listed, each with a checkbox on the left: "bw_tb300_user", "sailbot_test", and "tabs_sensor_user".

3. Choose your IAM user from the list.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Users' highlighted. The main area shows a search bar 'Find users by username or access key' and a list of users: 'bw_tb300_user' (checked), 'sailbot_test', and 'tabs_sensor_user'. The 'Add user' and 'Delete user' buttons are at the top right.

4. Choose **Add permissions**.



The screenshot shows the AWS IAM console for the user 'bw_tb300_user'. The 'Summary' tab is active, displaying 'User ARN', 'Path', and 'Creation time'. Below this, the 'Permissions' tab is selected, showing 'Permissions policies (8 policies applied)'. A red box highlights the 'Add permissions' button. Below the button, a list of policies is shown under 'Attached directly': 'AWSCertificateManagerReadOnly', 'AmazonFreeRTOSFullAccess', 'IAMReadOnlyAccess', and 'AWSIoTFullAccess'.



5. Choose **Attach existing policies directly**.

Add permissions to bw_tb300_user

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

[Create policy](#)

Filter policies ▾

	Policy name ▾
<input type="checkbox"/>	▶ AdministratorAccess
<input type="checkbox"/>	▶ AlexaForBusinessDeviceSetup
<input type="checkbox"/>	▶ AlexaForBusinessFullAccess
<input type="checkbox"/>	▶ AlexaForBusinessGatewayExecution



6. Choose **Create policy**.

Add permissions to bw_tb300_user

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies ▾ Search

	Policy name ▾
<input type="checkbox"/>	▶ AdministratorAccess
<input type="checkbox"/>	▶ AlexaForBusinessDeviceSetup
<input type="checkbox"/>	▶ AlexaForBusinessFullAccess
<input type="checkbox"/>	▶ AlexaForBusinessGatewayExecution

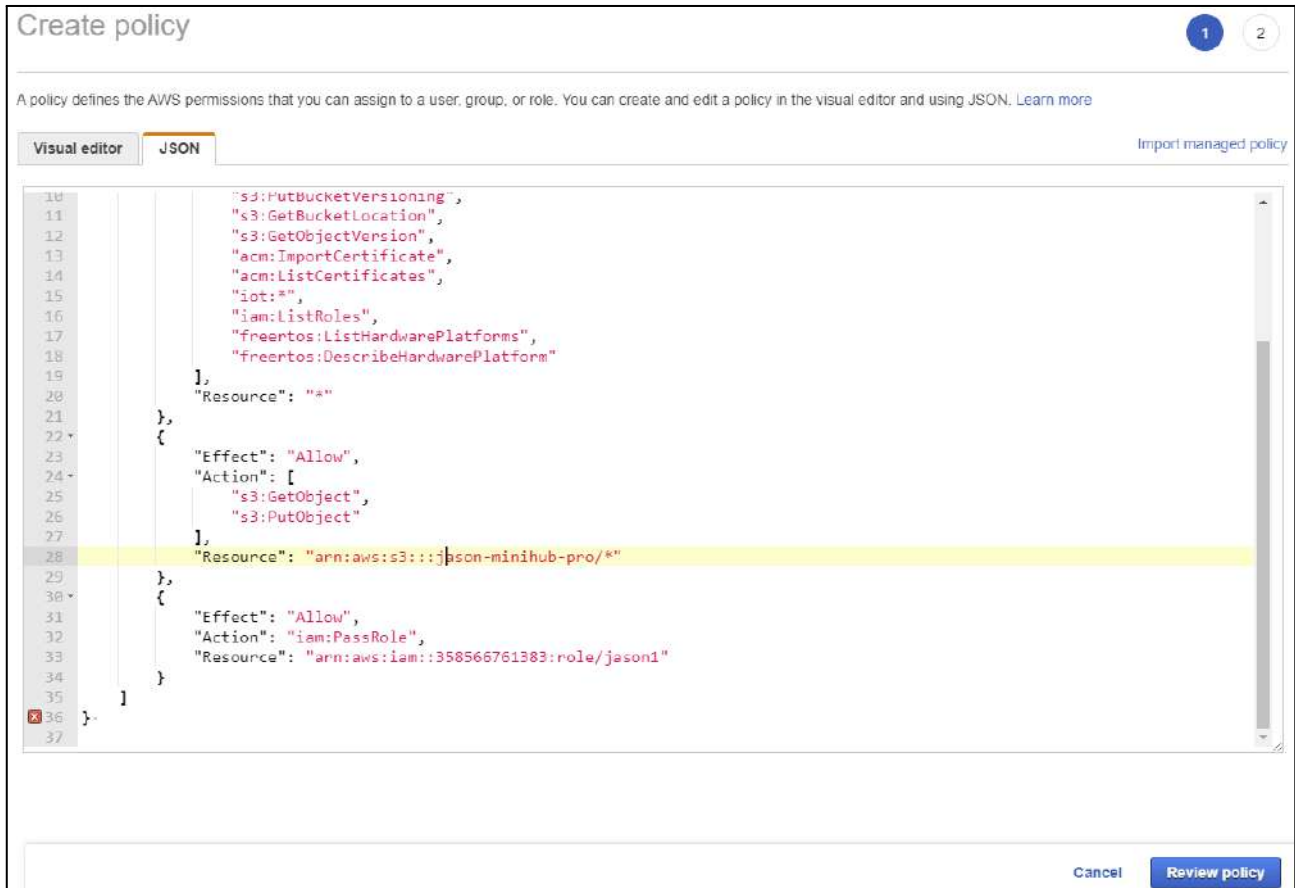
7. Choose the **JSON** tab, and copy and paste the following policy document into the policy editor:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetObjectVersion",
        "acm:ImportCertificate",
        "acm:ListCertificates",
        "iot:*",
        "iam:ListRoles",
        "freertos:ListHardwarePlatforms",
        "freertos:DescribeHardwarePlatform"
      ]
    }
  ]
}
```



```
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::example-bucket/*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::your-account-id:role/role-name"
  }
]
}
```


Replace `example-bucket` with the name of the Amazon S3 bucket where your OTA update firmware image is stored. Replace `your-account-id` with your AWS account ID. You can find your AWS account ID in the upper right of the console. When you enter your account ID, remove any dashes (-). Replace `role-name` with the name of the IAM service role you just created.



The screenshot shows the 'Create policy' interface in the AWS IAM console. The 'JSON' tab is selected, and the policy document is as follows:

```
10     "s3:PutBucketVersioning",
11     "s3:GetBucketLocation",
12     "s3:GetObjectVersion",
13     "acm:ImportCertificate",
14     "acm:ListCertificates",
15     "iot:*",
16     "iam:ListRoles",
17     "freertos:ListHardwarePlatforms",
18     "freertos:DescribeHardwarePlatform"
19   ],
20   "Resource": "*"
21 },
22 {
23   "Effect": "Allow",
24   "Action": [
25     "s3:GetObject",
26     "s3:PutObject"
27   ],
28   "Resource": "arn:aws:s3:::jason-minihub-pro/*"
29 },
30 {
31   "Effect": "Allow",
32   "Action": "iam:PassRole",
33   "Resource": "arn:aws:iam::358566761383:role/jason1"
34 }
35 ]
36 }
37
```

At the bottom right of the editor, there are 'Cancel' and 'Review policy' buttons.



8. Choose **Review policy**.

The screenshot shows the 'Create policy' interface in the AWS IAM console. The 'JSON' tab is selected, and the policy document is being edited. The document includes permissions for S3, ACM, IAM, and Freetos. A yellow highlight is placed on the resource path for the second policy effect. At the bottom right, the 'Review policy' button is highlighted with a red box.

```
10     "s3:PutBucketVersioning",
11     "s3:GetBucketLocation",
12     "s3:GetObjectVersion",
13     "acm:ImportCertificate",
14     "acm:ListCertificates",
15     "iot:*",
16     "iam:ListRoles",
17     "freetos:ListHardwarePlatforms",
18     "freetos:DescribeHardwarePlatform"
19   ],
20   "Resource": "*"
21 },
22 {
23   "Effect": "Allow",
24   "Action": [
25     "s3:GetObject",
26     "s3:PutObject"
27   ],
28   "Resource": "arn:aws:s3:::jason-minihub-pro/*"
29 },
30 {
31   "Effect": "Allow",
32   "Action": "iam:PassRole",
33   "Resource": "arn:aws:iam::358566761283:role/jason1"
34 }
35 }
36 }
37 }
```



9. Enter a name for your new OTA user policy, and then choose **Create policy**.

Create policy

1 2

Review policy

Name*
Use alphanumeric and '+', '@', '-' characters. Maximum 128 characters.

Description
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Summary

Service	Access level	Resource	Request condition
Allow (6 of 238 services) Show remaining 233			
Certificate Manager	Full List Limited: Write	All resources	None
FreeRTOS	Limited: List, Read	All resources	None
IAM	Limited: List, Write	Multiple	None
IoT	Full access	All resources	None
S3	Limited: List, Read, Write	Multiple	None

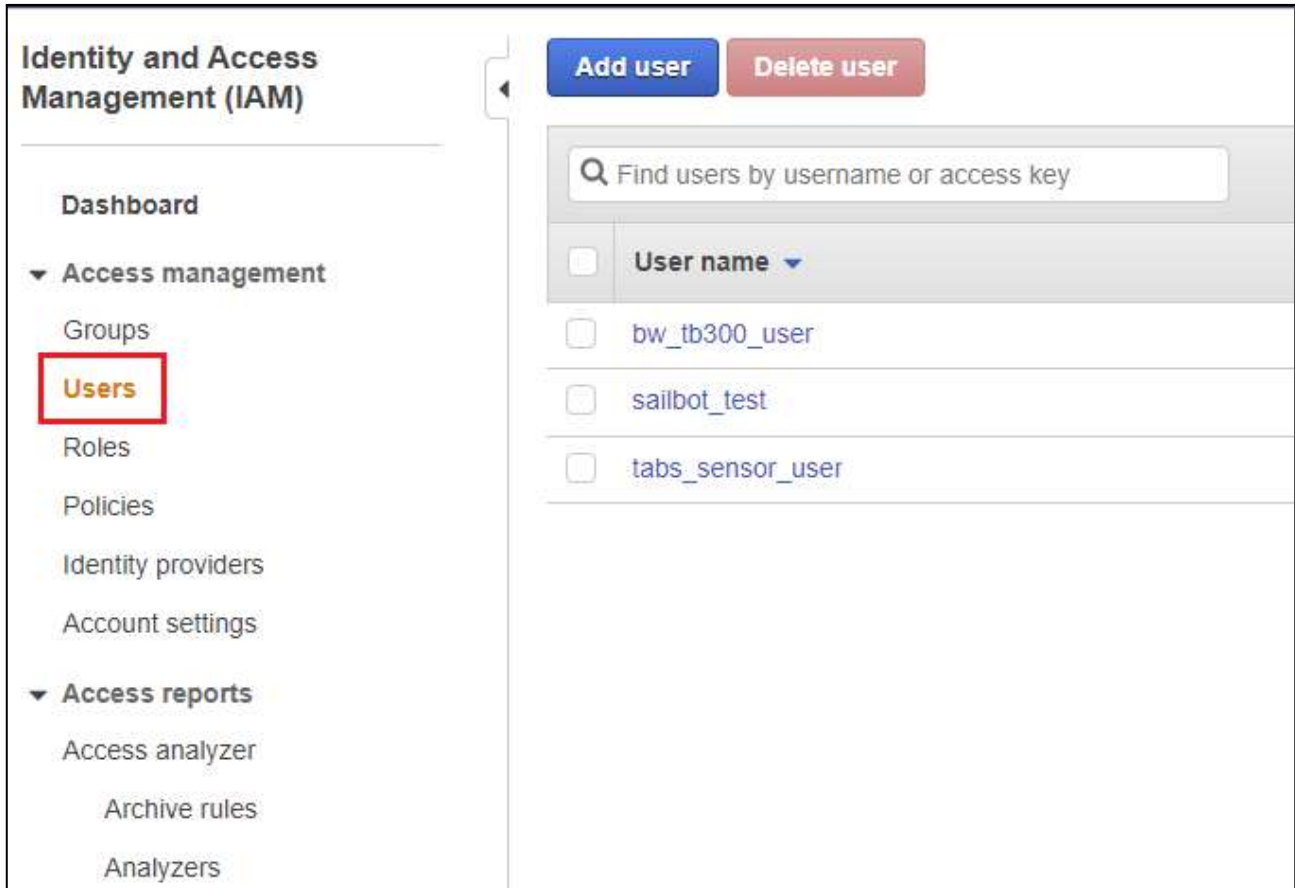
* Required

Cancel Previous **Create policy**

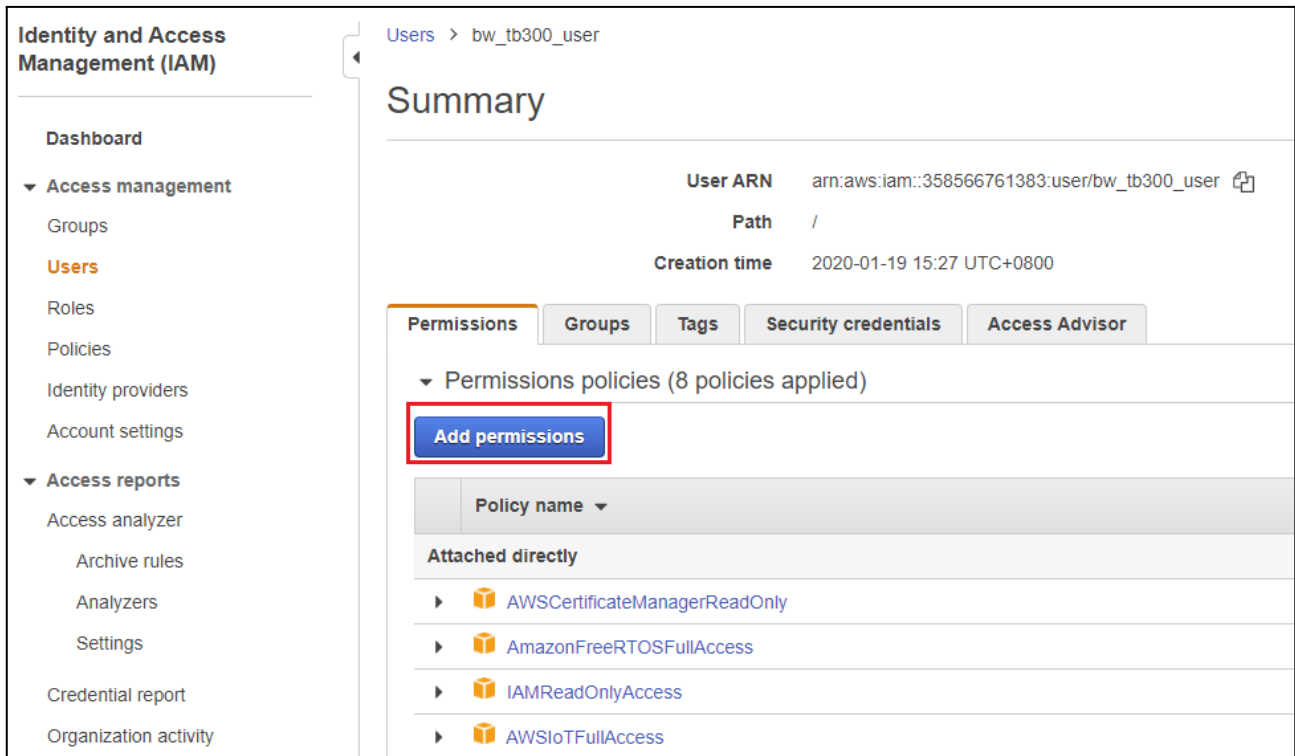


To attach the OTA user policy to your IAM user

1. In the IAM console, in the navigation pane, choose **Users**, and then choose your user.



2. Choose **Add permissions**.



The screenshot shows the AWS IAM console interface for a user named 'bw_tb300_user'. The left sidebar contains the navigation menu for 'Identity and Access Management (IAM)', with 'Users' selected. The main content area shows the 'Summary' page for the user, including details like 'User ARN', 'Path', and 'Creation time'. Below the summary, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing a list of 'Permissions policies (8 policies applied)'. A red box highlights the 'Add permissions' button. Below this, a table lists the policies attached directly to the user: AWSCertificateManagerReadOnly, AmazonFreeRTOSFullAccess, IAMReadOnlyAccess, and AWSIoTFullAccess.

Policy name
▶ AWSCertificateManagerReadOnly
▶ AmazonFreeRTOSFullAccess
▶ IAMReadOnlyAccess
▶ AWSIoTFullAccess



3. Choose **Attach existing policies directly**.

Add permissions to bw_tb300_user

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

[Create policy](#)

Filter policies ▾

	Policy name ▾
<input type="checkbox"/>	AdministratorAccess
<input type="checkbox"/>	AlexaForBusinessDeviceSetup
<input type="checkbox"/>	AlexaForBusinessFullAccess
<input type="checkbox"/>	AlexaForBusinessGatewayExecution

4. Search for the OTA user policy you just created and select the check box next to it.

Add permissions to bw_tb300_user

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies

	Policy name
<input type="checkbox"/>	▶ AmazonFreeRTOSOTAUpdate
<input type="checkbox"/>	▶ AWSIoTAnalyticsFullAccess
<input type="checkbox"/>	▶ AWSIoTAnalyticsReadOnlyAccess
<input type="checkbox"/>	▶ AWSIoTOTAUpdate
<input type="checkbox"/>	▶ AWSQuickSightIoTAnalyticsAccess
<input type="checkbox"/>	▶ GreengrassOTAUpdateArtifactAccess
<input type="checkbox"/>	▶ IoTAccess_Sailboat
<input checked="" type="checkbox"/>	▶ jason_OTA



5. Choose **Next: Review**.

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies

	Policy name	Type
<input type="checkbox"/>	▶ AmazonFreeRTOSOTAUpdate	AWS
<input type="checkbox"/>	▶ AWSIoTAnalyticsFullAccess	AWS
<input type="checkbox"/>	▶ AWSIoTAnalyticsReadOnlyAccess	AWS
<input type="checkbox"/>	▶ AWSIoTOTAUpdate	AWS
<input type="checkbox"/>	▶ AWSQuickSightToAnalyticsAccess	AWS
<input type="checkbox"/>	▶ GreengrassOTAUpdateArtifactAccess	AWS
<input type="checkbox"/>	▶ IoTAccess_Sailboat	CUSTOM
<input checked="" type="checkbox"/>	▶ jason_OTA	CUSTOM

Cancel **Next: Review**



6. Choose **Add permissions**.

Add permissions to bw_tb300_user

Permissions summary

The following policies will be attached to the user shown above.

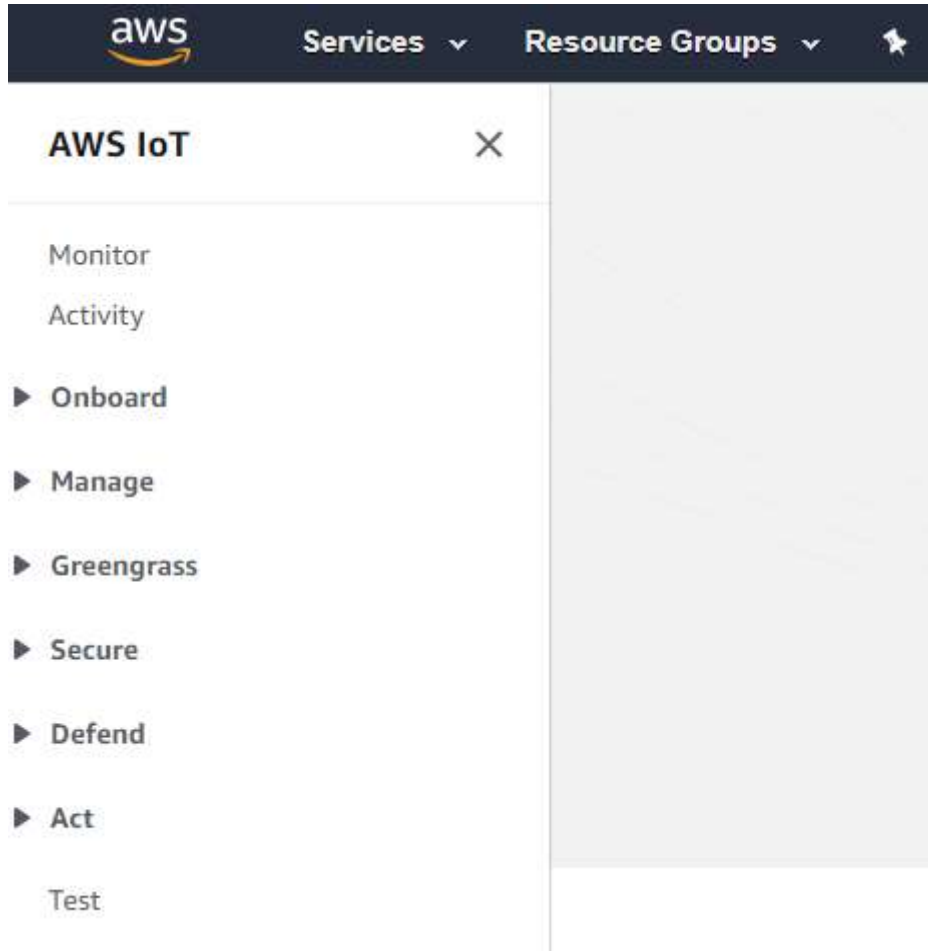
Type	Name
Managed policy	jason_OTA

Cancel Previous **Add permissions**



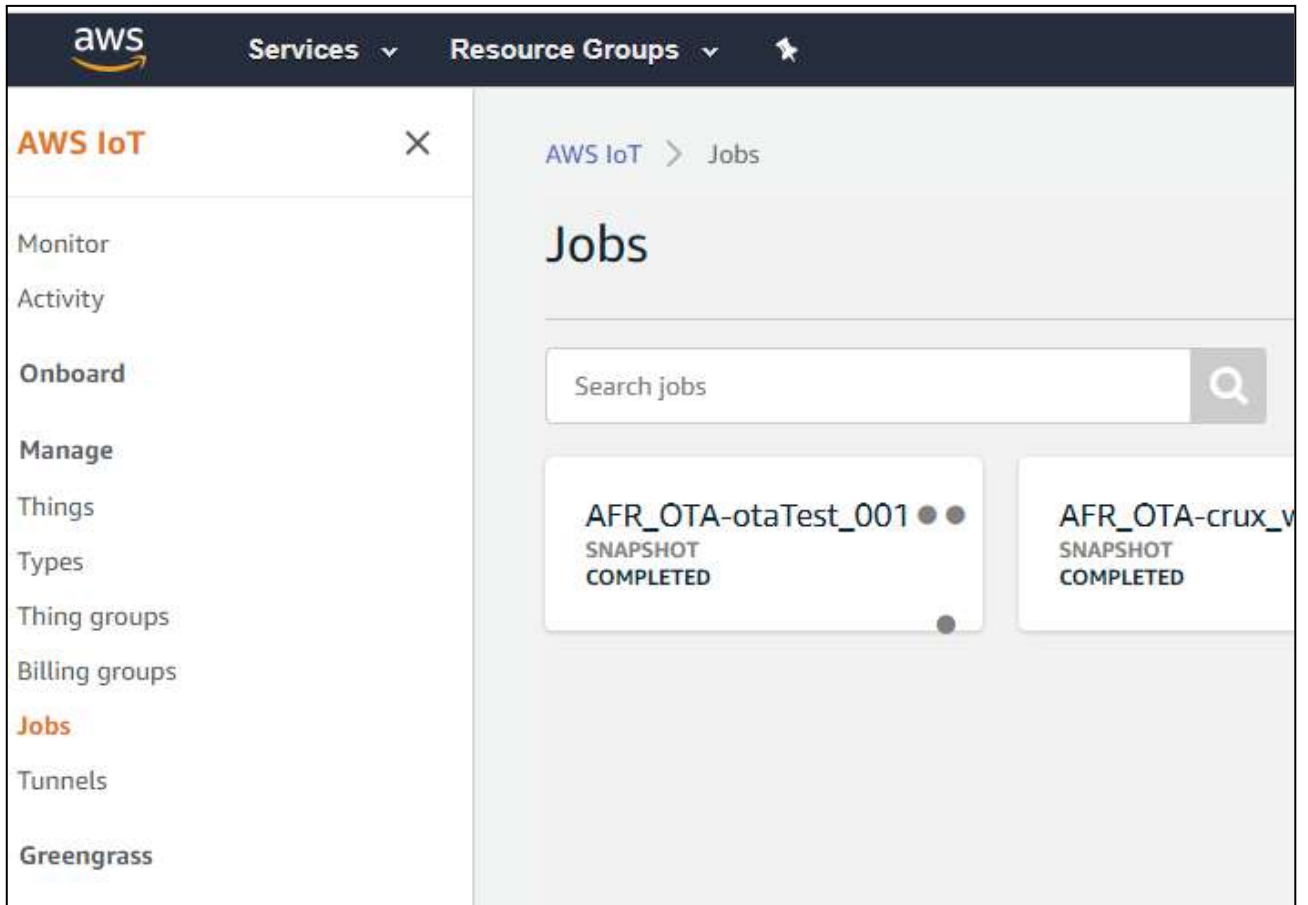
Create a FreeRTOS OTA update job

1. Go to "IoT Core" service.





2. Go to "Manage Jobs" and click the "Create" button.





3. Select "Create OTA update job"

AWS IoT > Jobs > Create job

CREATE JOB

Select a job

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.

Create a custom 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.

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

Create a Greengrass Core update job
Create a snapshot job to update one or more Greengrass Core devices with the latest Greengrass Core or OTA agent version.

Cancel

Create custom job

Create OTA update job

Create Core update job

Create custom job

4. Select the things name which configured to MiniHub Pro. And click "Next".



5. Select the "MQTT" protocol



6. Select the "Sign a new firmware image for me."



7. Create a new Code signing profile



- Click "Create"
- Input the "Profile name"
- Select hardware platform: **ESP-WROVER-KIT**
- Import the "Certificate"

Certificate:
<https://drive.google.com/file/d/1SFUXI1uqm3OWOhDs5TyDo62JlqlksmGO/view?usp=sharing>



Certificate private key:
<https://drive.google.com/file/d/1EavG36gmL3cdkQxqTrTZIWTjDPm4Mmz4/view?usp=sharing>

- Input the Pathname of code signing certificate on device: P11_CSK
- Click "Create"

*Next time you can select this profile directly.

8. Upload the firmware

Select your firmware image in S3 or upload it

Image not selected
Select

- Click "Select"
- Choose the bucket which store the firmware image.
- Click "Upload an image" Upload the image file: aws_demos.bin

Input the pathname of firmware image on the device: P11_CSK

Select "IAM role for OTA update job" (Created at step.2)

Input the OTA job unique ID and click the "Create" button.

You can find the successfully created job message.



The OTA job status is "Queued"

JOB
AFR_OTA-minihubpro_ota_demo_0001
IN PROGRESS Actions ▾

Overview All Statuses Refresh

Last updated Jun 16, 2020 8:24:41 PM +0800

1 <small>Queued</small>	0 <small>In progress</small>	0 <small>Timed out</small>	0 <small>Failed</small>	0 <small>Succeeded</small>	0 <small>Rejected</small>	0 <small>Canceled</small>	0 <small>Removed</small>
----------------------------	---------------------------------	-------------------------------	----------------------------	-------------------------------	------------------------------	------------------------------	-----------------------------

Resource	Last updated	Status
> MiniHubPro-3D807C	Jun 16, 2020 8:24:38 PM +0800	Queued <small>...</small>



Now please power on the MiniHub Pro. To trigger the OTA job process.

Go to AWS IoT to check the status. The status is "Succeeded"

The screenshot shows the AWS IoT Jobs console for a job named "AFR_OTA-minihubpro_ota_demo_0001". The job status is "COMPLETED". The console displays a summary table with the following data:

Queued	In progress	Timed out	Failed	Succeeded	Rejected	Canceled	Removed
0	0	0	0	1	0	0	0

Below the summary table, a table lists the resources for this job:

Resource	Last updated	Status
MiniHubPro-3D807C	Jun 16, 2020 8:30:22 PM +0800	Succeeded

Additional details for the resource MiniHubPro-3D807C are shown below:

- Jun 16, 2020 8:29:49 PM +0800
- Queued at Jun 16, 2020 8:24:38 PM +0800
- Updated at Jun 16, 2020 8:30:22 PM +0800
- [View thing details](#)



※Note:

OTA polling feature will be supported from the firmware **AWS APP Version 0.9.20** or latest so MiniHub Pro doesn't need power on again to trigger the OTA job process.