

Advantech AE Technical Share Document

Date	2021/7/8	SR#	1-4582346031
Category	<input checked="" type="checkbox"/> FAQ <input type="checkbox"/> SOP	Related OS	N/A
Abstract	How to use SimpleMQTT to send data to AWS IoT Core with modifiable topic?		
Keyword	MQTT, AWS		
Related Product	ADAM-3600, ECU-1152, ECU-1251, ECU-1051		

■ **Problem Description:**

This document shows how to use SimpleMQTT to send data to AWS IoT Core with modifiable topic.

■ **Answer:**

About AWS information, please reference the developer guide on the website.

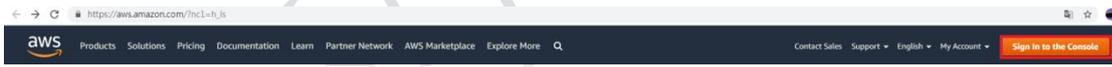
https://docs.aws.amazon.com/zh_tw/iot/latest/developerguide/iot-gs.html

1. Enter IoT core

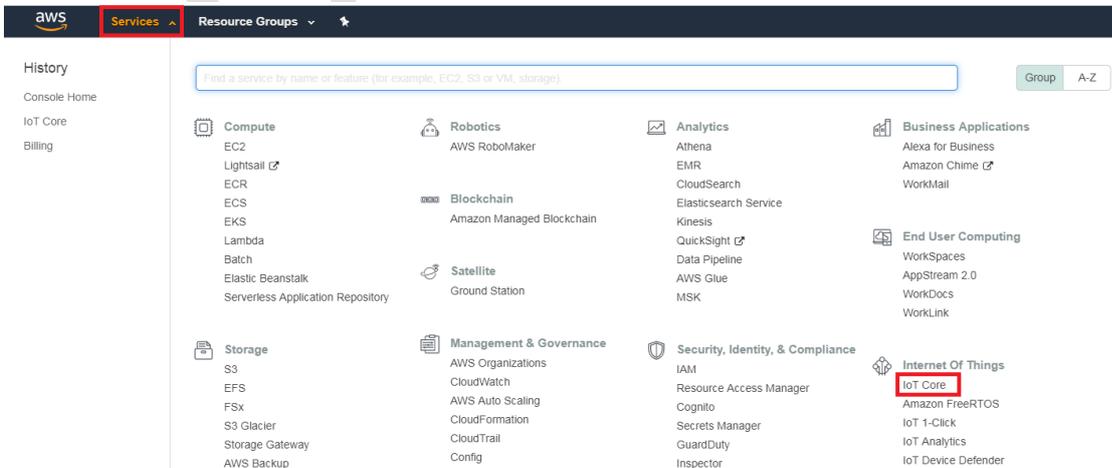
User needs to have AWS account and login in. Please refer to the website of AWS:

https://aws.amazon.com/?nc1=h_ls

Sign in or create new account on the top.

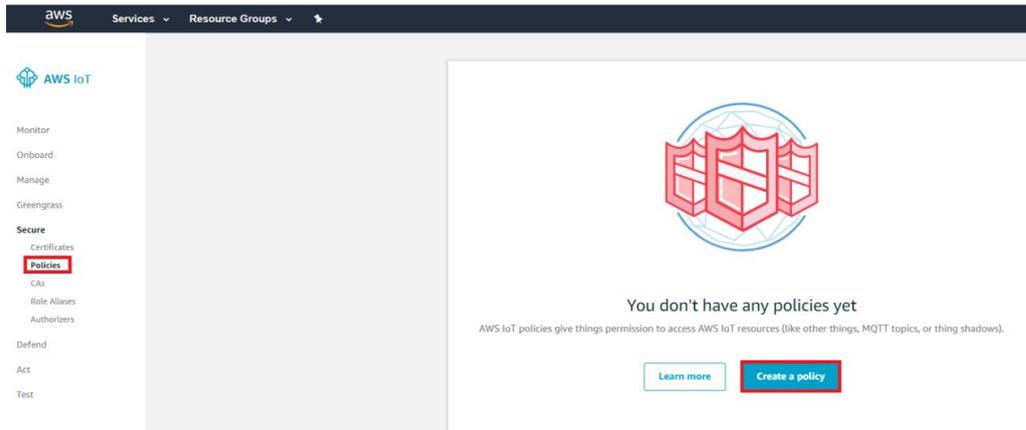


Click “Services” on the top and choose “IoT Core” on the page.



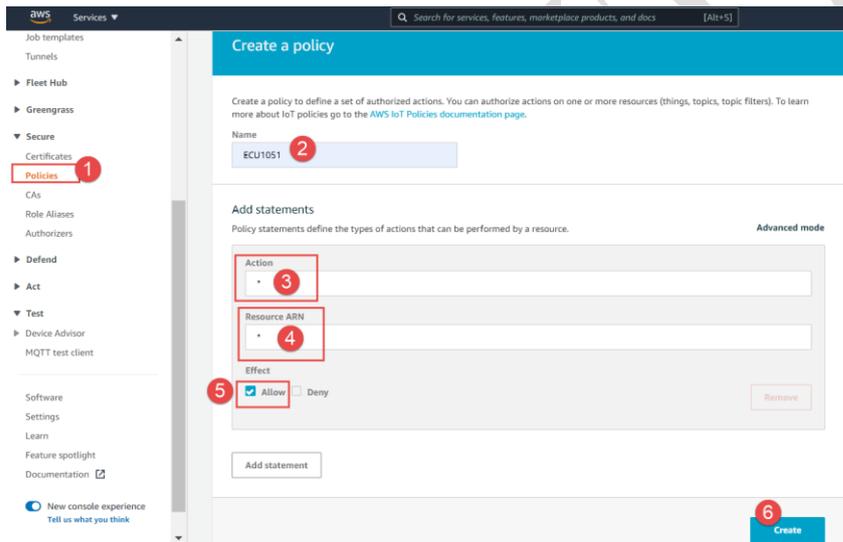
2. Create policies

Secure → Policies → Create a policy



Key in policy name, add statements and click "Create".

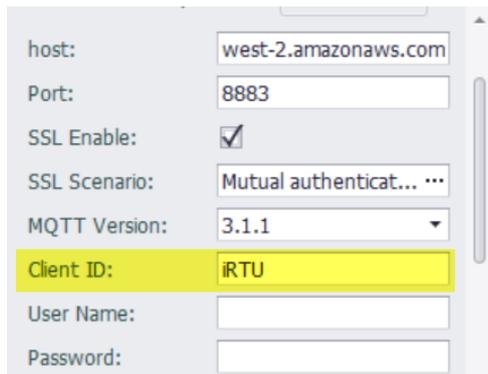
- Name: (policy name)
- Action: *
- Resource ARN: *
- Effect: **Allow**

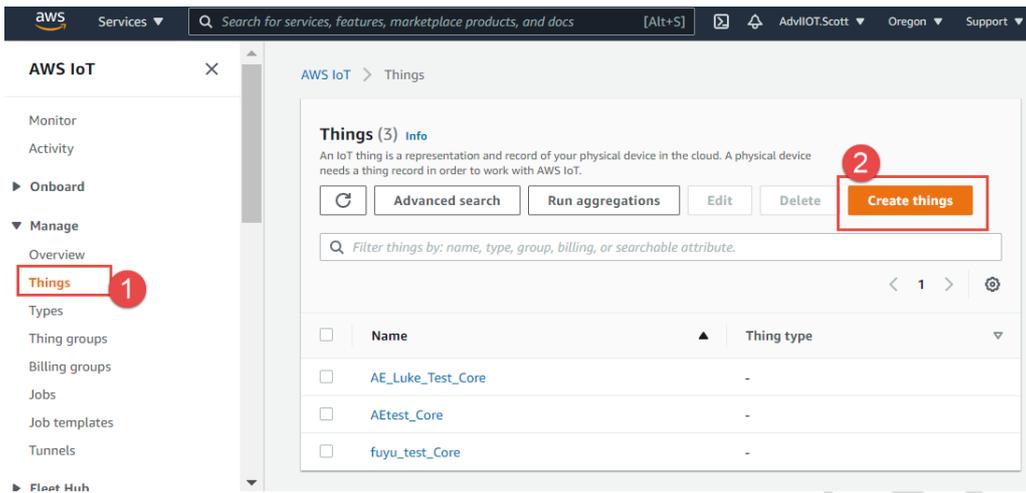


3. Register a "Things" which name should match with the client ID in EdgeLink studio.

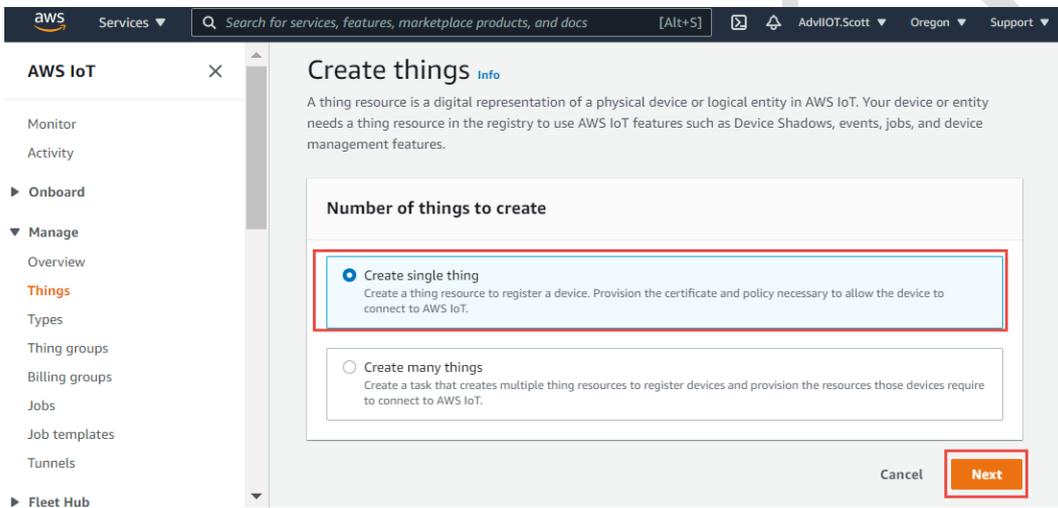
Select "management" → "things" → "create things".

The thing name is used as the default MQTT client ID if not setting anything in EdgeLink.

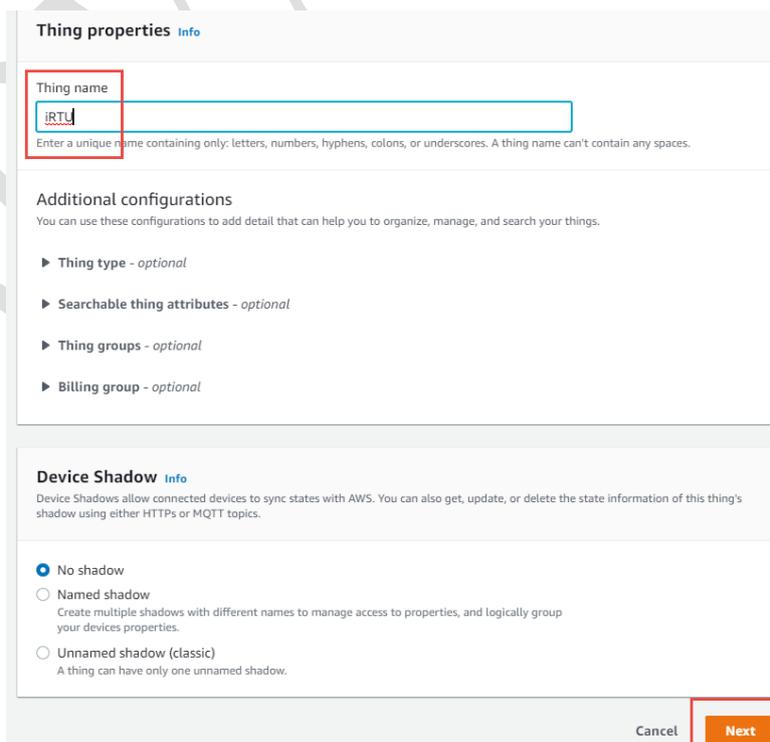




Crate single thing.



Type-in the thing name.



Create a certificate for the thing.

AWS IoT > Things > Create things > Create single thing

Step 1
Specify thing properties

Step 2 - optional
Configure device certificate

Step 3 - optional
Attach policies to certificate

Configure device certificate - optional Info

A device requires a certificate to connect to AWS IoT. You can choose how you to register a certificate for your device now, or you can create and register a certificate for your device later. Your device won't be able to connect to AWS IoT until it has an active certificate with an appropriate policy.

Device certificate

Auto-generate a new certificate (recommended)
Generate a certificate, public key, and private key using AWS IoT's certificate authority.

Use my certificate
Use a certificate signed by your own certificate authority.

Upload CSR
Register your CA and use your own certificates on one or many devices.

Skip creating a certificate at this time
You can create a certificate for this thing and attach a policy to the certificate at a later time.

Cancel Previous **Next**

Attach the policy.

> Create single thing

Attach policies to certificate - optional Info

AWS IoT policies grant or deny access to AWS IoT resources. Attaching policies to the device certificate applies this access to the device.

Policies (1/4) Create policy

Select up to 10 policies to attach to this certificate.

Filter policies

Name
<input type="checkbox"/> fuyu_test_Core-policy
<input checked="" type="checkbox"/> ECU1051
<input type="checkbox"/> AETest_Core-policy
<input type="checkbox"/> AE_Luke_Test_Core-policy

Cancel Previous **Create thing**

Download the certificates. Note! This is **the only chance** to download the certificates.

Device certificate

You can activate the certificate now, or later. The certificate must be active for a device to connect to AWS IoT.

Device certificate: 4554e8bf5f1...te.pem.crt Deactivate certificate Download

Key files

The key files are unique to this certificate and can't be downloaded after you leave this page. Download them now and save them in a secure place.

⚠ This is the only time you can download the key files for this certificate.

Public key file: 4554e8bf5f1d778326a07b3...0a9e1e3-public.pem.key Download
Key downloaded

Private key file: 4554e8bf5f1d778326a07b3...a9e1e3-private.pem.key Download
Key downloaded

Root CA certificates

Download the root CA certificate file that corresponds to the type of data endpoint and cipher suite you're using. You can also download the root CA certificates later.

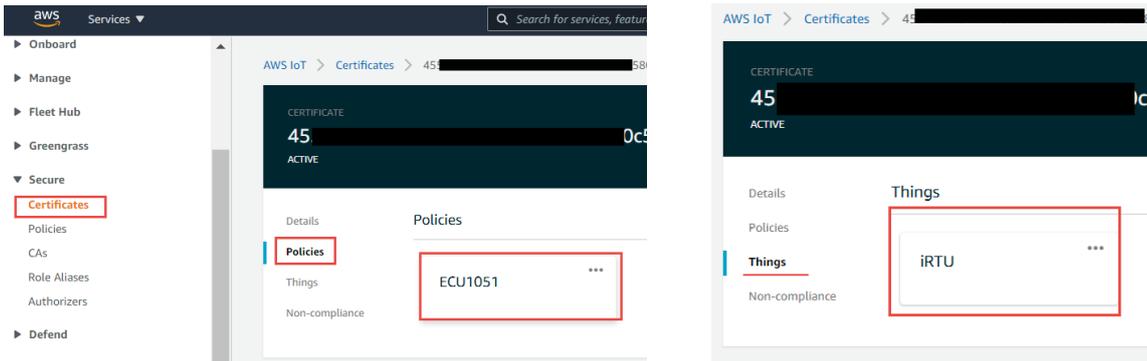
Amazon trust services endpoint: RSA 2048 bit key: Amazon Root CA 1 Download

Amazon trust services endpoint: ECC 256 bit key: Amazon Root CA 3 Download

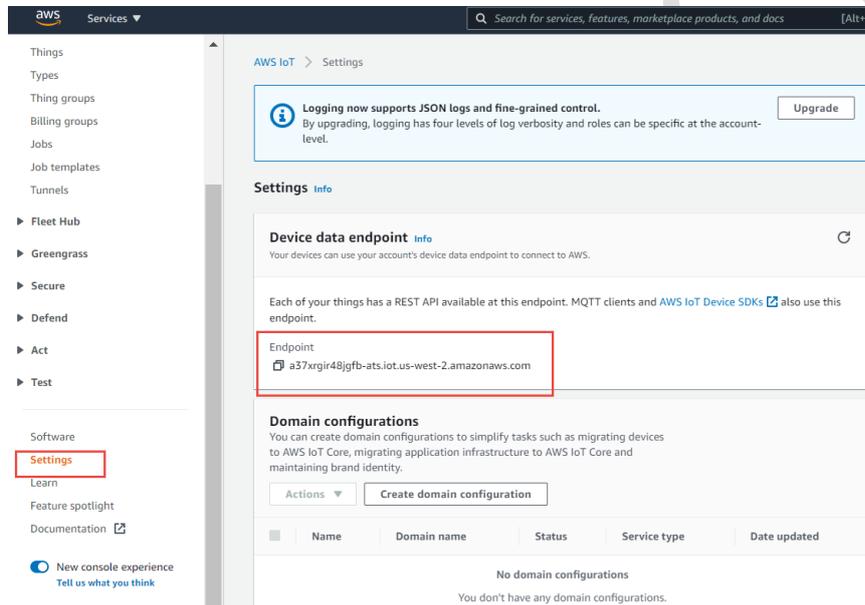
If you don't see the root CA certificate that you need here, AWS IoT supports additional root CA certificates. These root CA certificates and others are available in our developer guides. [Learn more](#)

Done

Check the setting. In “secure” → “certificates” → “policies” will have the policy you created. And the “things” content the thing name you created.



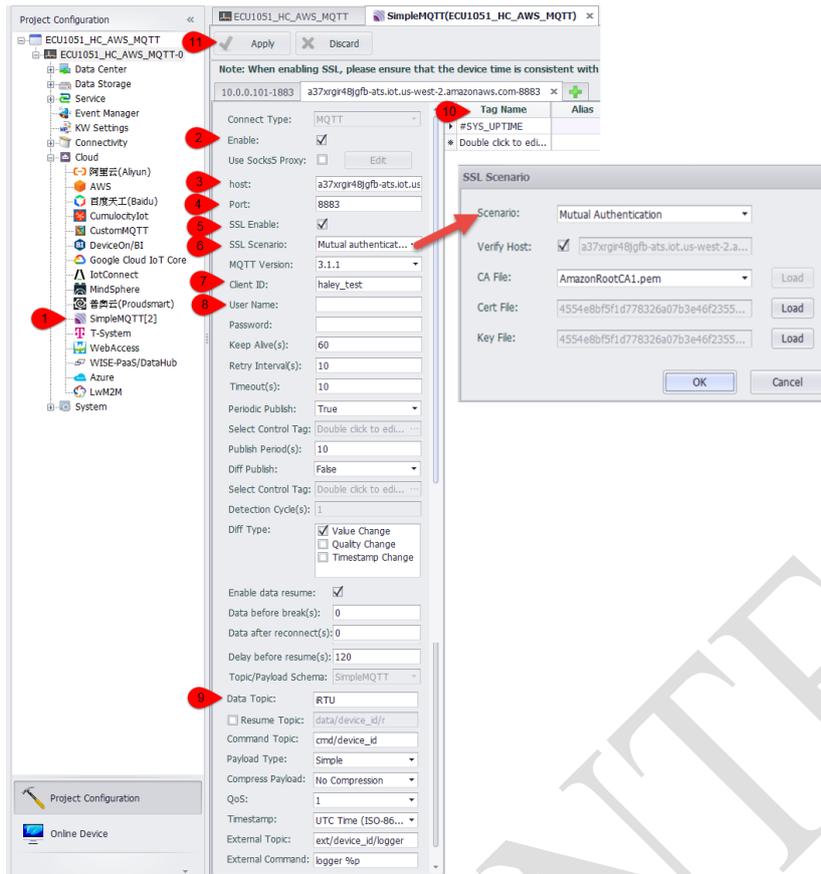
4. Go to “setting” and copy the “endpoint”, paste it into the EdgeLink setting.



5. Setup the EdgeLink project.

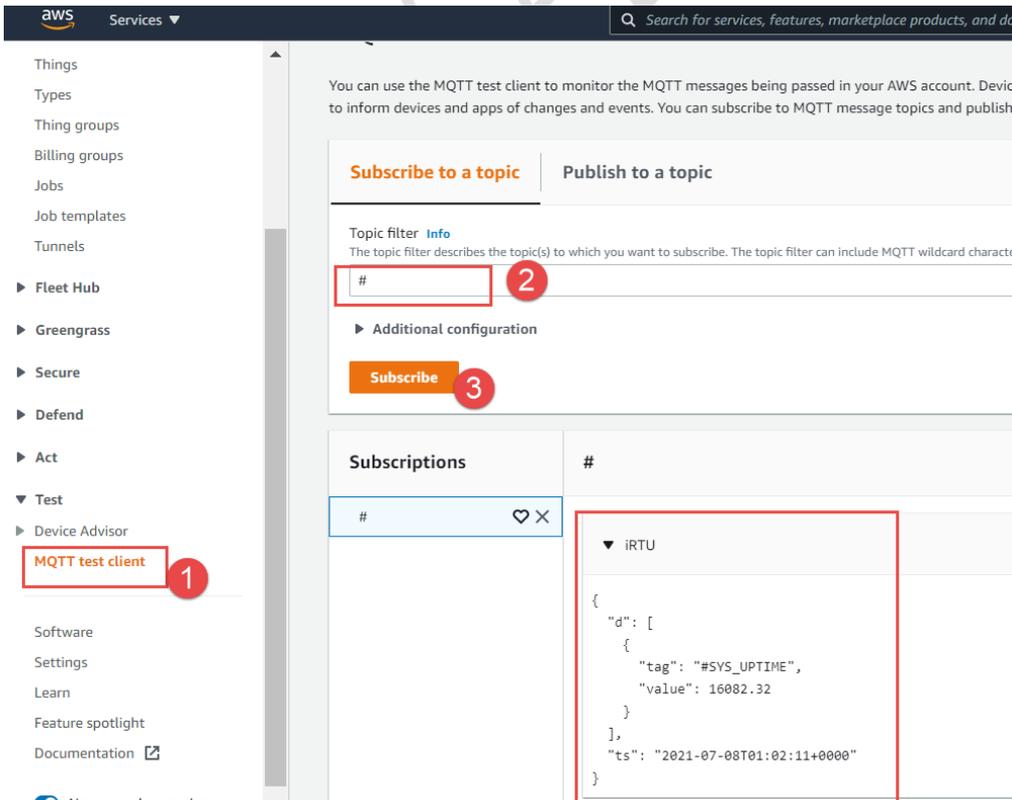
- (1) This example is using simpleMQTT.
- (2) Enable the function.
- (3) Host: endpoint
- (4) Port: 8883
- (5) Protocol: mqtt/tls
- (6) Certificate: mutual authentication.
Verify host.
CA file: AmazonRootCA1.pem
Client certificate file: *.certificate.pem.crt
Client key file: *.private.pem.key
- (7) Client ID: can be anything, but unique.
- (8) User name/ password: leave it empty.
- (9) Topic: can be anything.
- (10) Select given tags to upload.

(11) Click “apply” to complete the setting.



Results:

In “test” ⇒ “MQTT test client” ⇒ “subscribe to a topic”, here shows the received data.



Use 3rd party MQTT client (ex: Paho, MQTTbox) to verify.

Setting in MQTTbox.

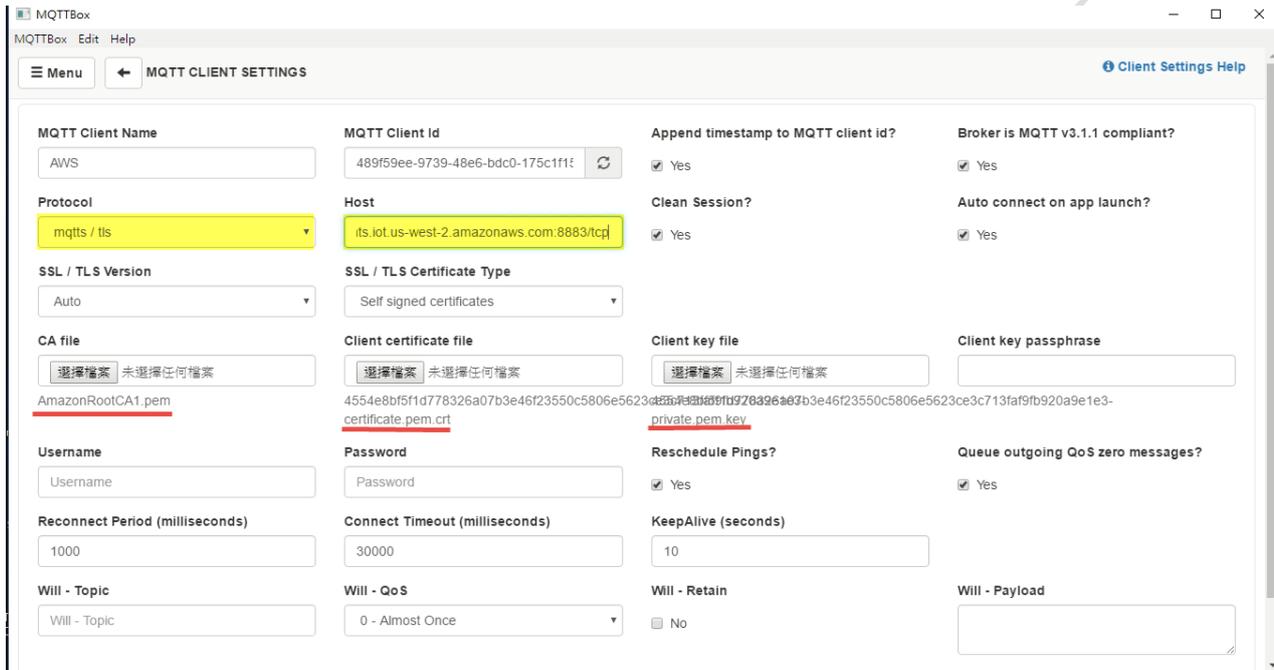
Protocol: mqtt/tls

Host: endpoint:8883/tcp

CA file: AmazonRootCA1.pem

Client certificate file: *.certificate.pem.crt

Client key file: *.private.pem.key



Subscribe the topic according to the EdgeLink setting.

