MQTT

Connecting to the AWS, Amazon Web Services

Vers. 1.1 – Jul 2021

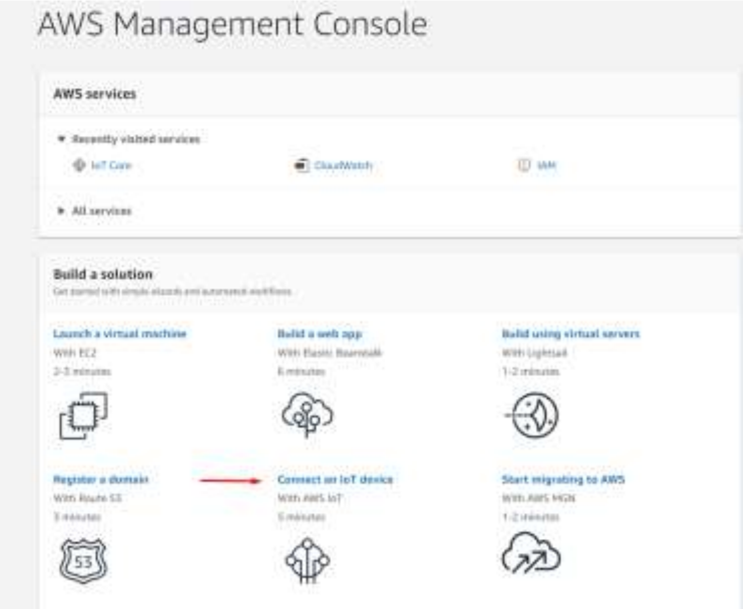
1. Introduction

All of Infinite’s devices that support the MQTT protocol, are capable to connect to any local or remote MQTT Broker. Amazon Web Services is a subsidiary of Amazon providing on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis.

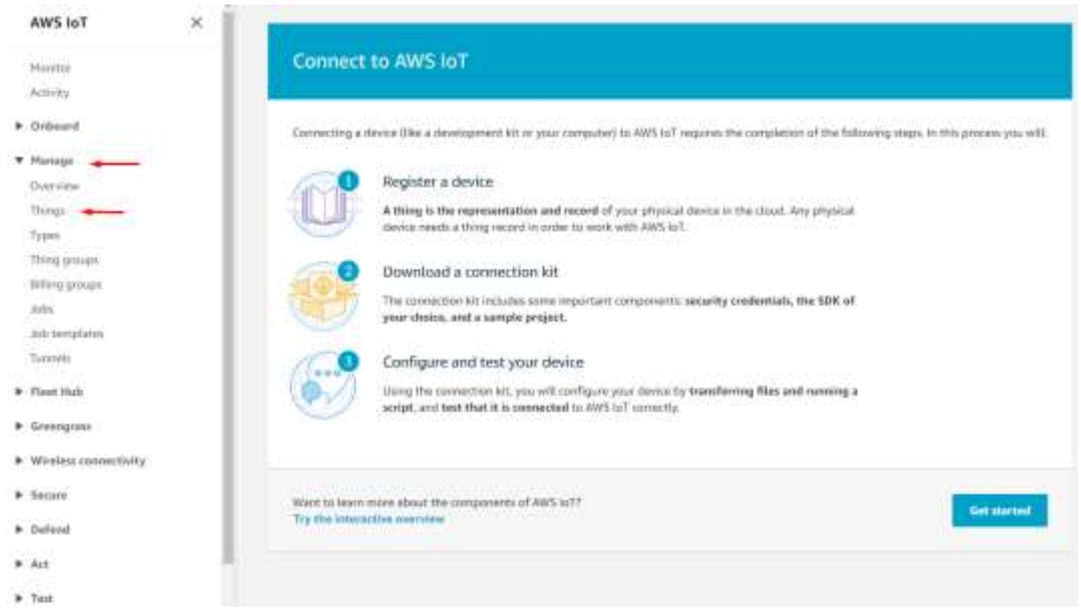
This document is a brief how-to guide for all device communications between Infinite’s devices and the AWS which supports MQTT connectivity.

2. AWS Console

After creating an AWS account, navigate to the AWS Management Console page and click Connect an IoT device.



Open the Manage tab and click Things.



Connect to AWS IoT

Connecting a device (like a development kit or your computer) to AWS IoT requires the completion of the following steps. In this process you will:

1. Register a device

A thing is the representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT.

2. Download a connection kit

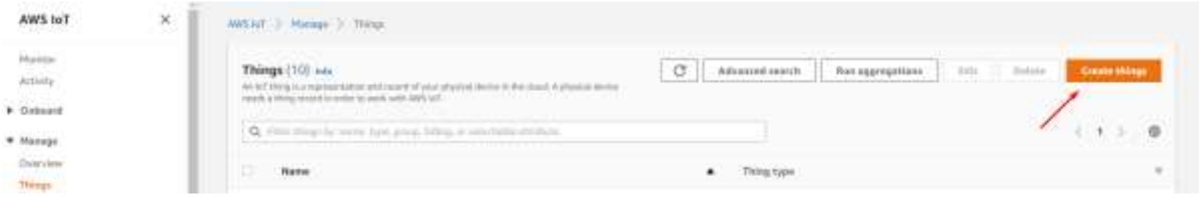
The connection kit includes some important components: **security credentials, the SDK of your choice, and a sample project.**

3. Configure and test your device

Using the connection kit, you will configure your device by **transferring files and running a script**, and **test that it is connected** to AWS IoT correctly.

Want to learn more about the components of AWS IoT?
Try the interactive overview

Click Create things.

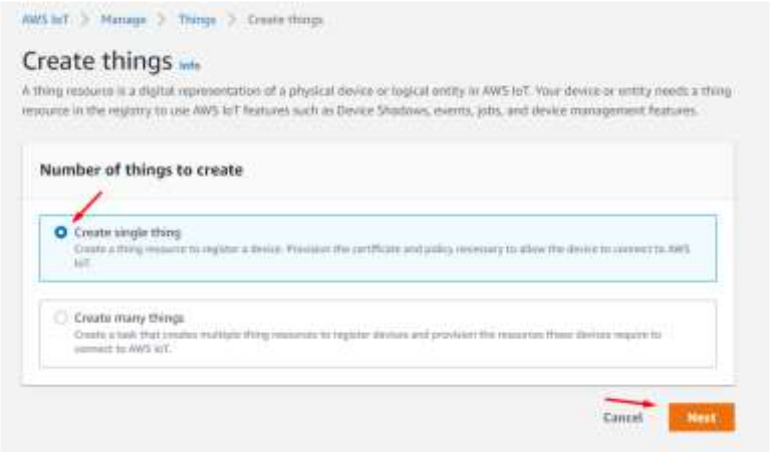


Things (10)

An IoT thing is a representation and record of your physical device in the cloud. A physical device needs a thing record in order to work with AWS IoT.

Filter things by: name, type, group, billing, or searchable attribute.

Create a single thing.



Create things

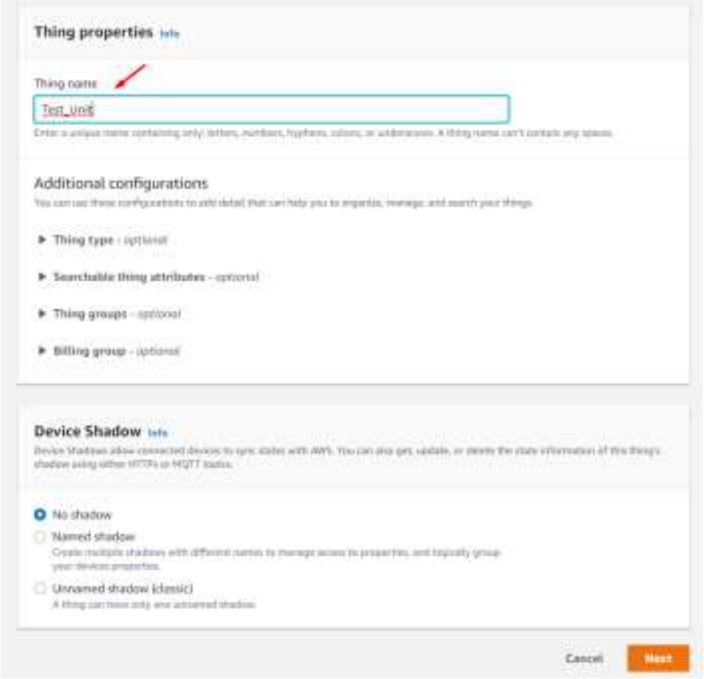
A thing resource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing resource in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.

Number of things to create

● Create single thing
Create a thing resource to register a device. Provision the certificate and policy necessary to allow the device to connect to AWS IoT.

○ Create many things
Create a task that creates multiple thing resources to register devices and provision the resources those devices require to connect to AWS IoT.

Give the Thing a name.



Thing properties Info

Thing name

Test_Unit

Enter a unique name containing only: letters, numbers, hyphens, colons, or underscores. A thing name can't contain any spaces.

Additional configurations

You can use these configurations to add detail that can help you to organize, manage, and search your things.

- ▸ **Thing type** - optional
- ▸ **Searchable thing attributes** - optional
- ▸ **Thing groups** - optional
- ▸ **Billing group** - optional

Device Shadow Info

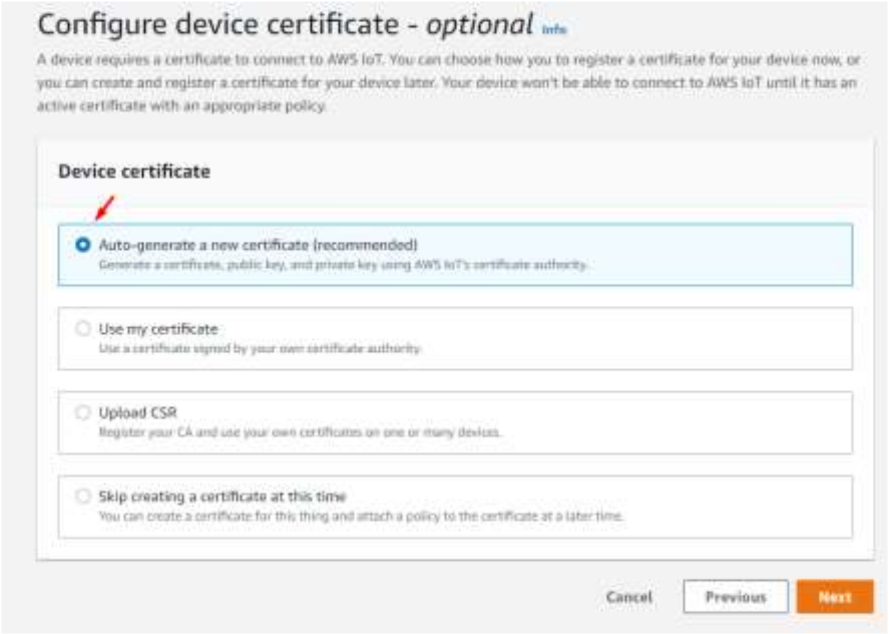
Device Shadows allow connected devices to sync states with AWS. You can also get, update, or delete the state information of this thing's shadow using either HTTPs or MQTT topics.

● No shadow

○ Named shadow
Create multiple shadows with different names to manage access to properties, and logically group your devices properties.

○ Unnamed shadow (classic)
A thing can have only one unnamed shadow.

Auto-generate a new certificate. (AWS requires TLS communications)



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

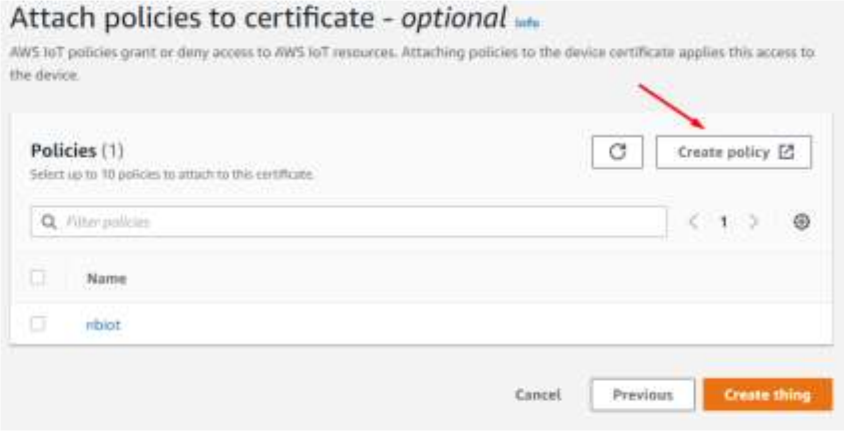
● Auto-generate a new certificate (recommended)
Generate a certificate, public key, and private key using AWS IoT's certificate authority.

○ 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.

Create a policy to attach to the certificate.



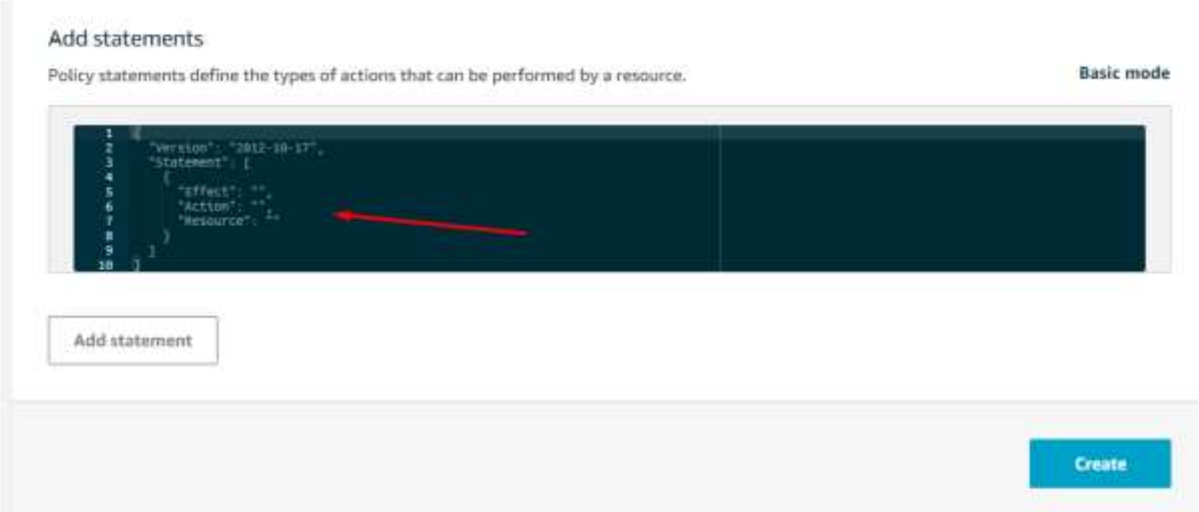
Attach policies to certificate - *optional* Info

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)

Select up to 10 policies to attach to this certificate

Name the policy and click advanced mode to define the types of actions that can be performed by our device.



Add statements

Policy statements define the types of actions that can be performed by a resource.

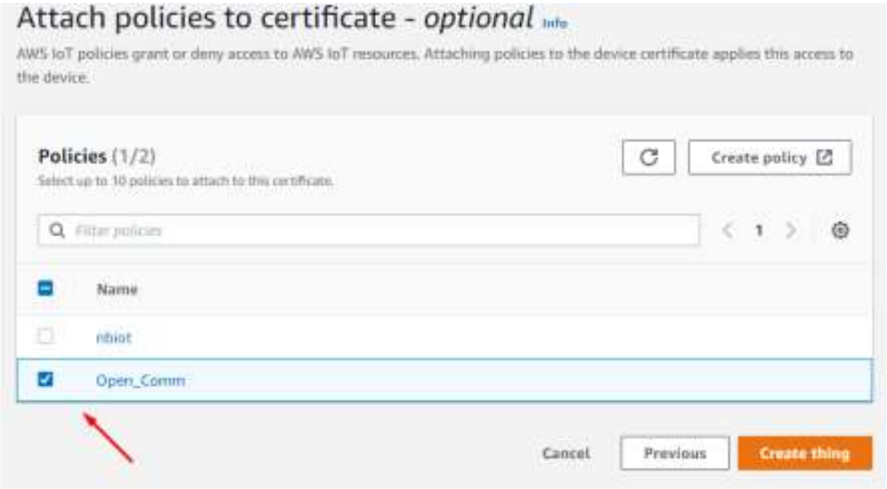
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "",
      "Action": "",
      "Resource": ""
    }
  ]
}
```

Delete the pre-existing statements and paste the following ones.

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

This policy is for testing purposes (it allows all communications to and from the device) and should be adjusted for your requirements.

Click refresh and choose the policy you just created and click Create thing.



Attach policies to certificate - *optional* Info

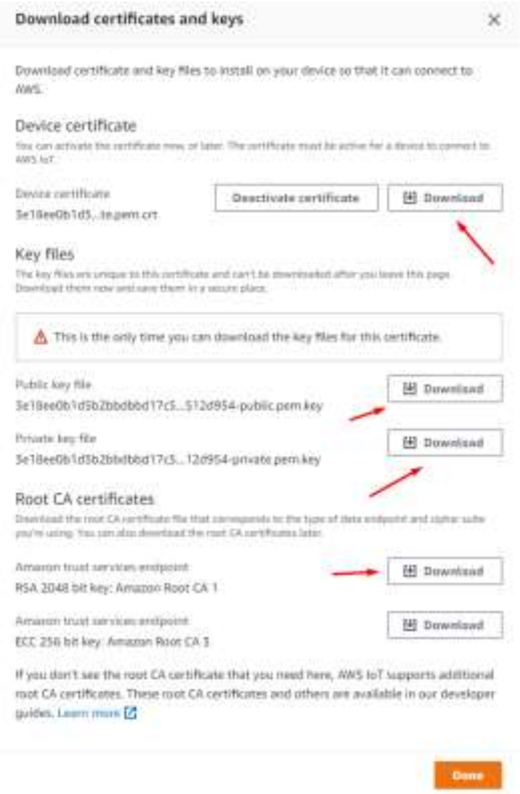
AWS IoT policies grant or deny access to AWS IoT resources. Attaching policies to the device certificate applies this access to the device.

Policies (1/2)

Select up to 10 policies to attach to this certificate.

	Name
□	rbiot
☑	Open_Comm

In the windows that pops up you can download the certificates that were created.



Download certificates and keys

Download certificate and key files to install on your device so that it can connect to AWS.

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
5e18ee0b1d5...te.pem.crt

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
5e18ee0b1d5b2bbdbbd17c5...512d954-public.pem.key

Private key file
5e18ee0b1d5b2bbdbbd17c5...12d954-private.pem.key

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.

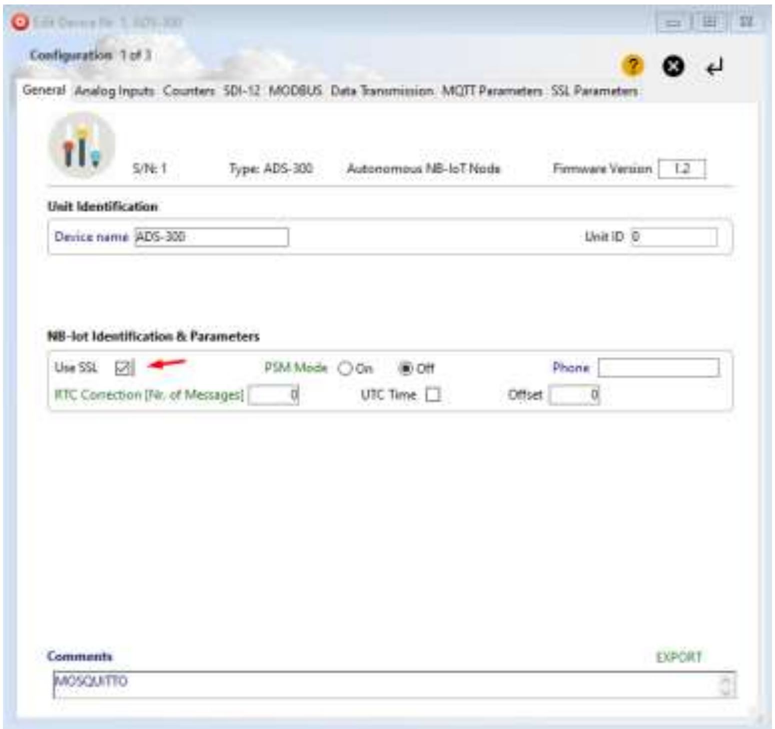
Amazon trust services endpoint
RSA 2048 bit key: Amazon Root CA 1

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

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

3. Device Configuration with WA Manager

In the Edit Device window in WA Manager, tick the Use SSL box.



S/N: 1 Type: ADS-300 Autonomous NB-IoT Node Firmware Version 1.2

Unit Identification

Device name ADS-300 Unit ID 0

NB-Iot Identification & Parameters

Use SSL ☑ PSM Mode ○ On ● Off Phone

RTC Correction [Nr. of Messages] 0 UTC Time ☐ Offset 0

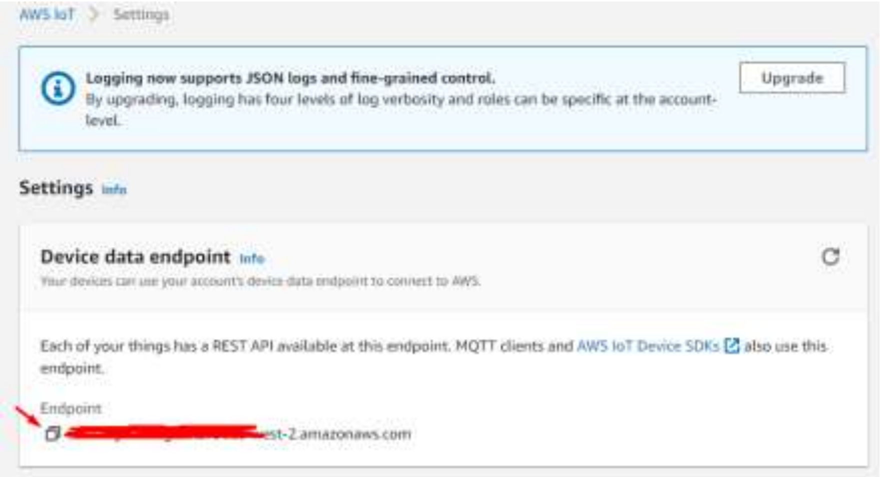
Comments

MOSQUITTO

Next, we configure the MQTT parameters.

Although AWS supports MQTT connectivity, it is not a pure MQTT Broker and so it has some limitations regarding its MQTT parameters.

For the Broker IP, the Device data endpoint must be used that can be found in the AWS IoT Settings tab.



Logging now supports JSON logs and fine-grained control.
By upgrading, logging has four levels of log verbosity and roles can be specific at the account-level.

Settings

Device data endpoint

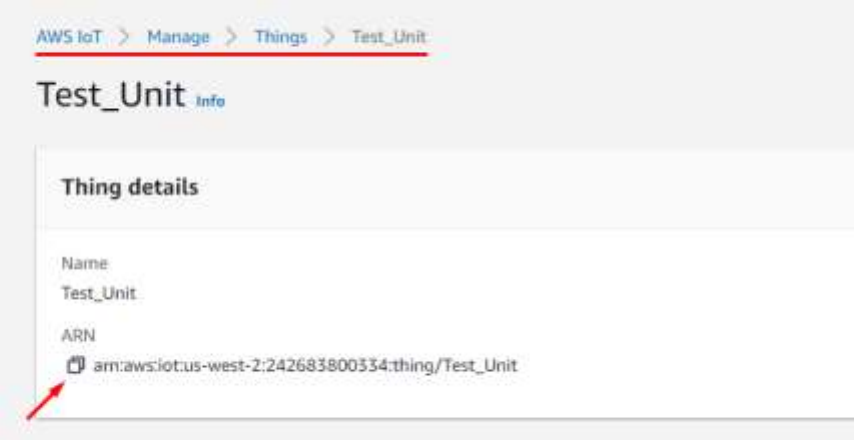
Your devices can use your account's device data endpoint to connect to AWS.

Each of your things has a REST API available at this endpoint. MQTT clients and AWS IoT Device SDKs also use this endpoint.

Endpoint

[redacted]est-2.amazonaws.com

For the Client ID, the ARN (Amazon Resource Name) must be used that can be found in the Things tab.

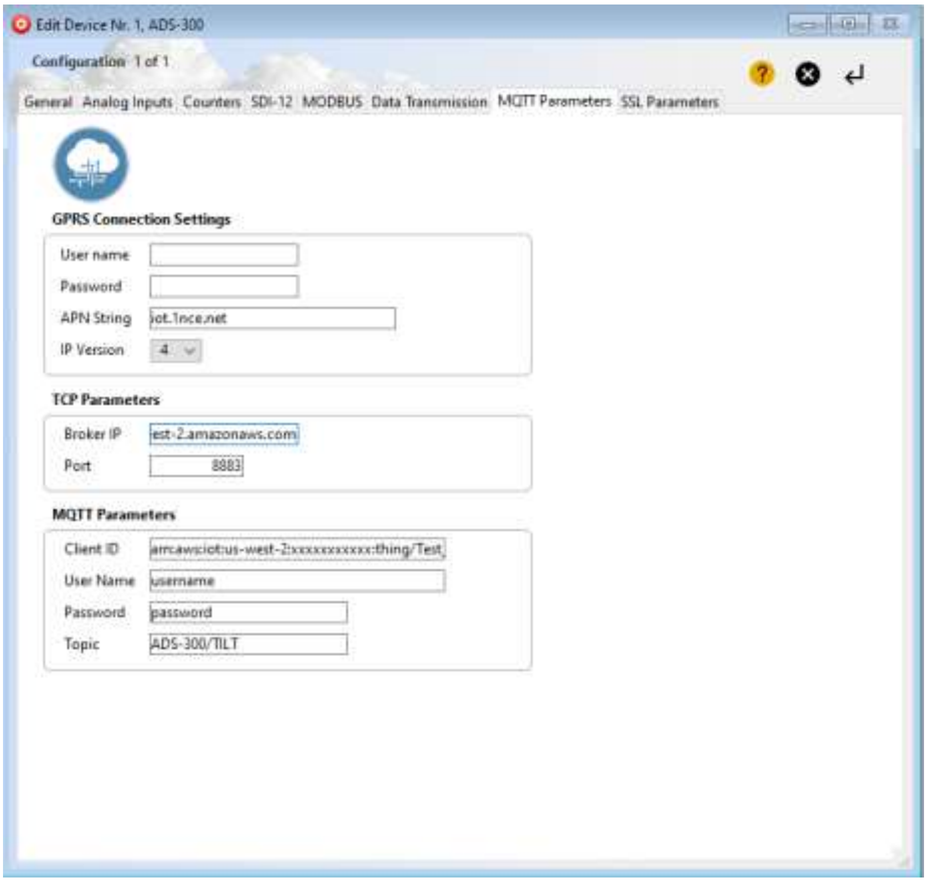


Test_Unit

Thing details

Name
Test_Unit

ARN
arn:aws:iot:us-west-2:242683800334:thing/Test_Unit



GPRS Connection Settings

User name	
Password	
APN String	iot.1nce.net
IP Version	4

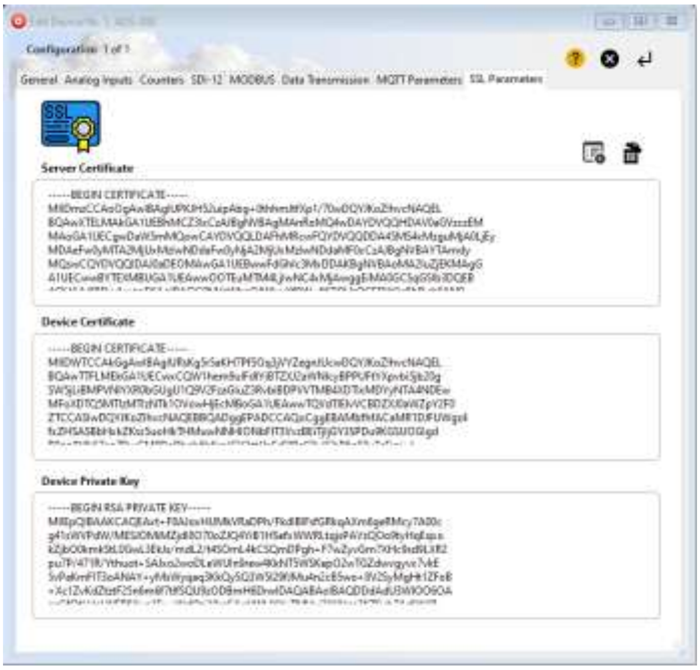
TCP Parameters

Broker IP	est-2.amazonaws.com
Port	8883

MQTT Parameters

Client ID	arn:aws:iot:us-west-2:xxxxxxxxxxx:thing/Test_
User Name	username
Password	password
Topic	ADS-300/TILT

Lastly, in the SSL Parameters tab, we copy and paste the three files needed for the TLS communication: Server Certificate (CA), Device Certificate and Device Private Key.



Server Certificate

-----BEGIN CERTIFICATE-----

Device Certificate

-----BEGIN CERTIFICATE-----

Device Private Key

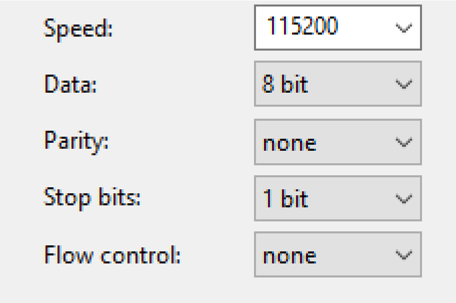
-----BEGIN RSA PRIVATE KEY-----

The Server Certificate is the Amazon trust services that you previously downloaded, the Device Certificate is the file you downloaded and the Device Private Key is the private key file. These files should be first opened with Notepad++ and their contents should be copy and pasted in the above tab. All files must be PEM formatted.

4. Load Certificates via Terminal

Alternatively, the certificates can also be loaded via a terminal program of your choice. This example uses Tera Term.

The serial port settings are shown in the image below.

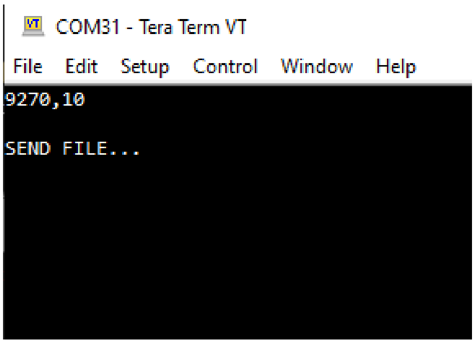


Speed:	115200
Data:	8 bit
Parity:	none
Stop bits:	1 bit
Flow control:	none

The commands for sending each of the certificates are shown in the table below.

9270	Send SSL Certificates	cmd,n	n: 10: Root Certificate, 20: Device Certificate, 30: Device Private Key

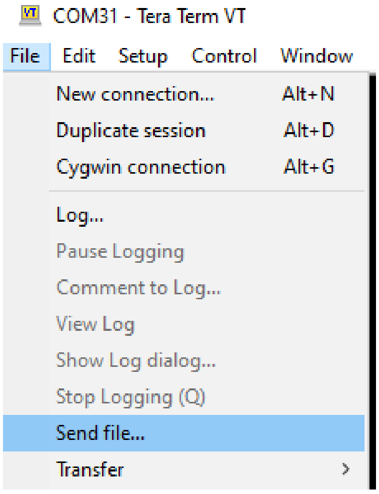
So, for sending the Root Certificate we should enter the command 9270,10 in the terminal.

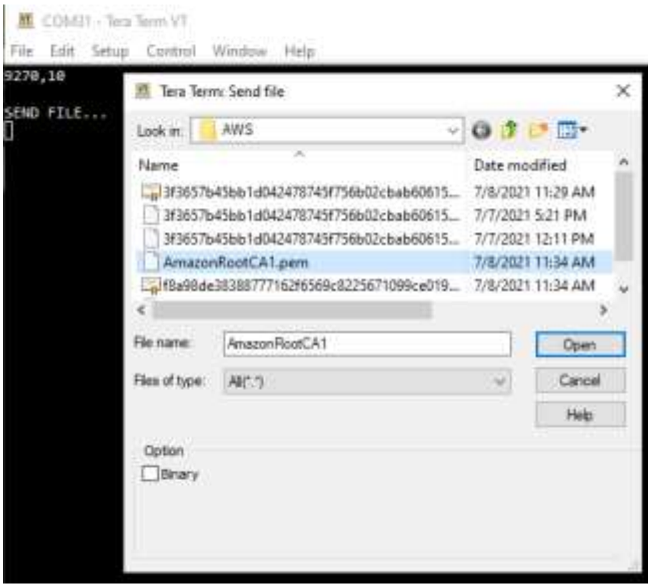


```
9270,10

SEND FILE...
```

Then, send the appropriate file.





```
9270,10

SEND FILE...
```

Look in: AWS

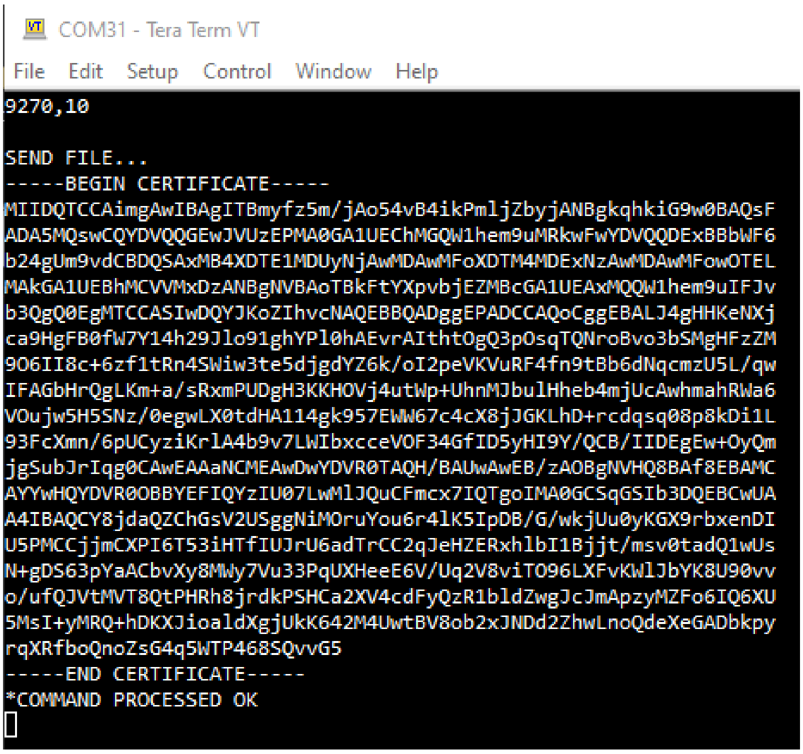
Name	Date modified
3f3657b45bb1d042478745f756b02cbab60615...	7/8/2021 11:29 AM
3f3657b45bb1d042478745f756b02cbab60615...	7/7/2021 5:21 PM
3f3657b45bb1d042478745f756b02cbab60615...	7/7/2021 12:11 PM
AmazonRootCA1.pem	7/8/2021 11:34 AM
f8a98de38388777162f6569c8225671099ce019...	7/8/2021 11:34 AM

File name: AmazonRootCA1

Files of type: All(*.*)

☐ Binary

And enter the special character *. This is achieved by pressing Ctrl+8.



```
9270,10

SEND FILE...
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
b24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
9O6II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
VOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
93FcXmn/6pUCyziKrlA4b9v7LWIbxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
A4IBAQCY8jdaQZChGsV2USggNiMOruYou6r4lK5IpDB/G/wkjUu0yKGX9rbxenDI
U5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
N+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
o/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
rqXRfboQnoZsG4q5WTP468SQvvG5
-----END CERTIFICATE-----
*COMMAND PROCESSED OK
```

The device will answer with the message COMMAND PROCESSED OK if the configuration was successful.

Do the same for the other two certificates with their respective commands.

Your device can now securely connect to the AWS and send your encrypted telemetry data safely.

Disclaimer:

AWS, Amazon Web services is registered trademark of Amazon.com Inc, USA. All products and software mentioned in this document for educational and demonstration purposes.

Revision: 1.2

Infinite Informatics, Ltd
1, Valaoritou Street
GR-54626 Thessaloniki, Greece
Phone: +30-2310-553545
E: info@indinf.gr
W: www.infinite.com.gr