



**AWS: Amazon Web Services**

rev1.0 20/04/2020

## GOAL

**Introduction to AWS, create an account  
and generate certificates.**

# PREREQUISITES

## Software needed:

- **Internet Browser**

## Hardware used in this example:

- **none**

## What is it ?

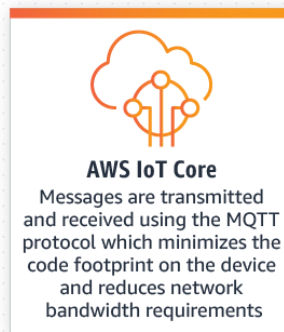
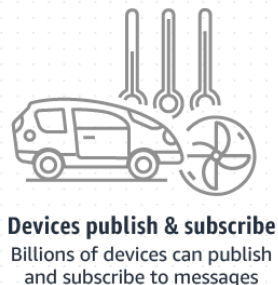
**Amazon Web Services (AWS)** is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.



# IoT functionality

Among all the AWS there is the **AWS IoT Core** service: allows to run a broker on the cloud with ease, create and manage any number of devices since it support HTTP, WebSockets and, more important, MQTT.

**Aws IoT core** provides end-to-end cryptography for secure connections, it's very easy to create and manage certificates too.



# Create an account

In order use the AWS you need to create and activate an account. Creating an account is very easy, go [here](#) and create a new one.

You will be asked for a credit card: the AWS are not all free and some services offer a free plan for only 12 months, anyway we will use only the AWS IoT Core, that with the free plan allows 250.000 messages sent and received per month for the first 12 months.



# Register a new device

The registry allows you to keep a record of all of the devices that are registered to your AWS IoT Core account. The process of registering your device includes these steps:

- Create and Activate a Device Certificate
- Create an AWS IoT Core Policy
- Attach an AWS IoT Core Policy to a Device Certificate
- Attach a Certificate to a Thing



# Create and Activate a Device Certificate

First of all sign in as Root user (use your AWS email and password to log in ) then go to IoT core.

If you can't find it in the recent services, simply search it in the bar.

## Console di gestione AWS

### Servizi AWS

#### Trova servizi

È possibile immettere nomi, parole chiave o acronimi.

Q Esemplio: Relational Database Service, database, RDS

#### ▼ Servizi visitati di recente



IoT Core



IoT Analytics



AWS Amplify



Kinesis



Mobile Hub

#### ▼ Servizi AWS



Calcolo

EC2

Lightsail

Lambda

Batch

Elastic Beanstalk

Serverless Application

Repository



Satellite

Ground Station



Quantum Technologies

Amazon Braket



Gestione e governance



Sicurezza, identità,

conformità

IAM

Resource Access Manager

Cognito

Secrets Manager

GuardDuty

Inspector



# Create certificate

Then go to **Security** → **Certificates** and click on the create button.

Select *One-Click certificate creation* in order to create the certificates and the keys that we will need in the next steps.

The screenshot shows the 'CREATE A THING' page in the AWS IoT console, specifically the 'Add a certificate for your thing' step (2/5). The page lists four options for certificate creation:

- One-click certificate creation (recommended)**: This will generate a certificate, public key, and private key using AWS IoT's certificate authority. The **Create certificate** button is highlighted with a red oval.
- Create with CSR**: Upload your own certificate signing request (CSR) based on a private key you own. The button is labeled **Create with CSR**.
- Use my certificate**: Register your CA certificate and use your own certificates for one or many devices. The button is labeled **Get started**.
- Skip certificate and create thing**: You will need to add a certificate to your thing later before your device can connect to AWS IoT. The button is labeled **Create thing without certificate**.

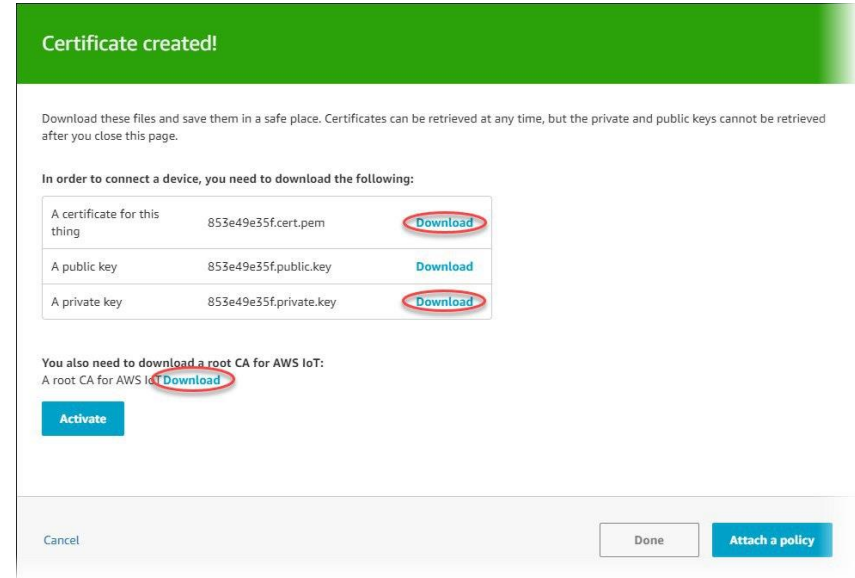
# Download

On the **Certificate created** page, choose the **Download** links to download the certificate, private key, and root CA for AWS IoT Core. (You do not need to download the public key).

When click for generating the CA certificate, you will be redirected to another page: right click on [Amazon Root CA 1](#) and “save as” the link as a .pem file.

Save each of them to your computer, and then choose **Activate** to continue.

Choose **Done** to return to the main page of the AWS IoT console.



# Create an AWS IoT Core Policy

To create an AWS IoT Core policy:

- In the left navigation pane, choose **Secure**, and then choose **Policies**. On the You don't have a policy yet page, choose **Create a policy**.
- On the **Create a policy** page, in the **Name** field, enter a name for the policy (for example, **MyIotPolicy**). Do not use personally identifiable information in your policy names.

Create 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). To learn more about IoT policies go to the [AWS IoT Policies documentation page](#).

Name

My\_IoT\_Policy

Add statements

Policy statements define the types of actions that can be performed by a resource. [Advanced mode](#)

Action
iot:*
Resource ARN
*
Effect
<input checked="" type="checkbox"/> Allow <input type="checkbox"/> Deny
<a href="#">Remove</a>

[Add statement](#)

[Create](#)

# Create an AWS IoT Core Policy

- In the **Action** field, enter `iot:Connect`. In the **Resource ARN** field, enter `*`. Select the **Allow** check box. This allows all clients to connect to AWS IoT Core.
- Choose the **Add Statement** button to add another policy statement. In the **Action** field, enter `iot:Publish`. In the **Resource ARN field**, enter the ARN of the topic to which your device publishes.
- Finally, select the **Allow** check box. This allows your device to publish messages to the specified topic.
- After you have entered the information for your policy, choose **Create**.

For more information, see [Managing AWS IoT Core Policies](#).

## Note

You can restrict which clients (devices) can connect by specifying a client ARN as the resource. The client ARNs follow this format:

```
arn:aws:iot:your-region:your-aws-account:client/<my-client-id>
```

## Note

The topic ARN follows this format:

```
arn:aws:iot:your-region:your-aws-account:topic/<your/topic>
```

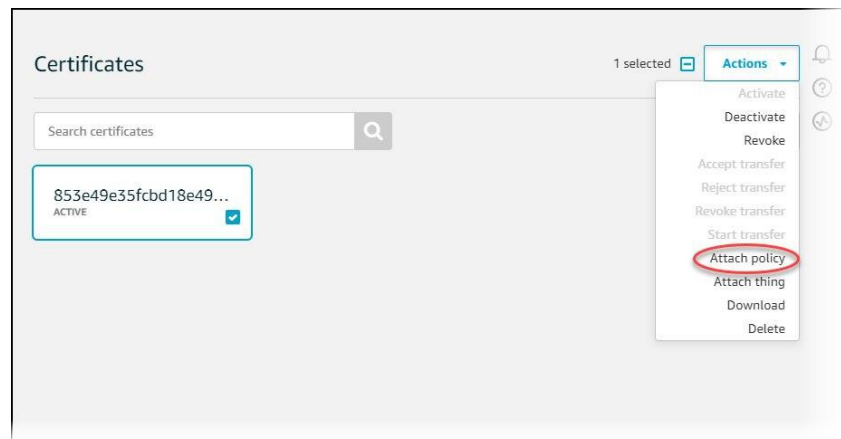
For example:

```
arn:aws:iot:us-east-1:123456789012:topic/my/topic
```

# Attach an AWS IoT Core Policy to a Device Certificate

Now that you have created a policy, you must attach it to your device certificate. Attaching an AWS IoT Core policy to a certificate gives the device the permissions specified in the policy.

1. In the left navigation pane, choose **Secure**, and then choose **Certificates**.
2. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose **Attach policy**.



# Attach an AWS IoT Core Policy to a Device Certificate

3. In **Attach policies to certificate(s)**, select the check box next to the policy you created in the previous step, and then choose **Attach**.

### Attach policies to certificate(s)

Policies will be attached to the following certificate(s):  
853e49e35fcbd18e4955a22a15c5120f2da761591b2f7b41b240fcd3a49b87cb

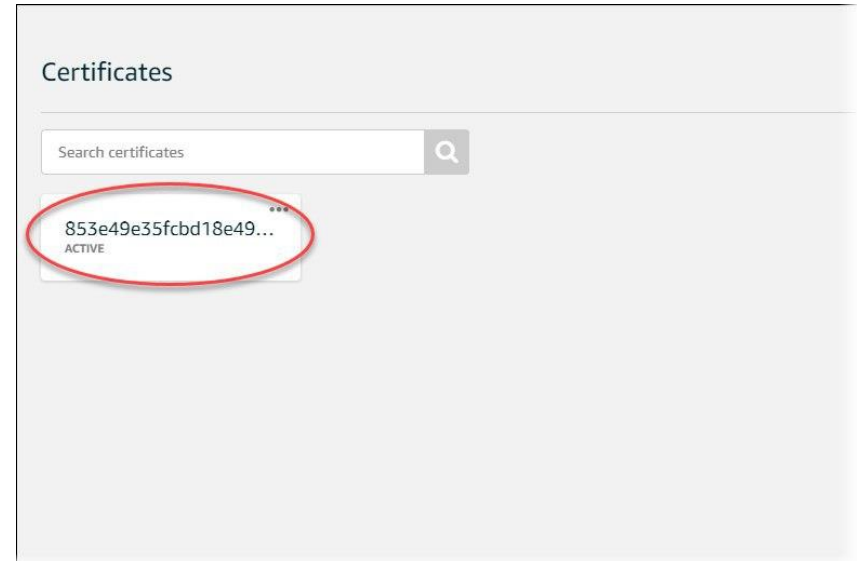
Choose one or more policies

<input type="checkbox"/>	MoistureSensorPolicy	<a href="#">View</a>
<input checked="" type="checkbox"/>	My_IoT_Policy	<a href="#">View</a>

1 policy selectedCancelAttach

# Attach a Certificate to a Thing

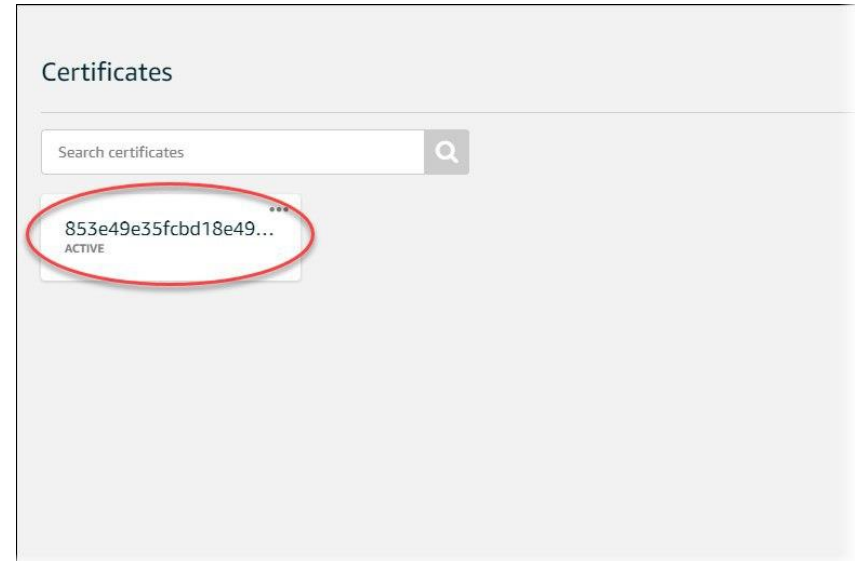
A device must have a certificate, private key, and root CA certificate to authenticate with AWS IoT Core. AWS recommend that you also attach the device certificate to the IoT thing that represents your device in AWS IoT Core.



# Attach a Certificate to a Thing

## To attach a certificate to the thing representing your device in the registry:

1. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose **Attach thing**.
2. In **Attach things to certificate(s)**, select the check box next to the thing you registered, and then choose **Attach**.
3. To verify the thing is attached, select the box for the certificate.
4. On the **Details** page for the certificate, in the left navigation pane, choose **Things**.
5. To verify the policy is attached, on the **Details** page for the certificate, in the left navigation pane, choose **Policies**.

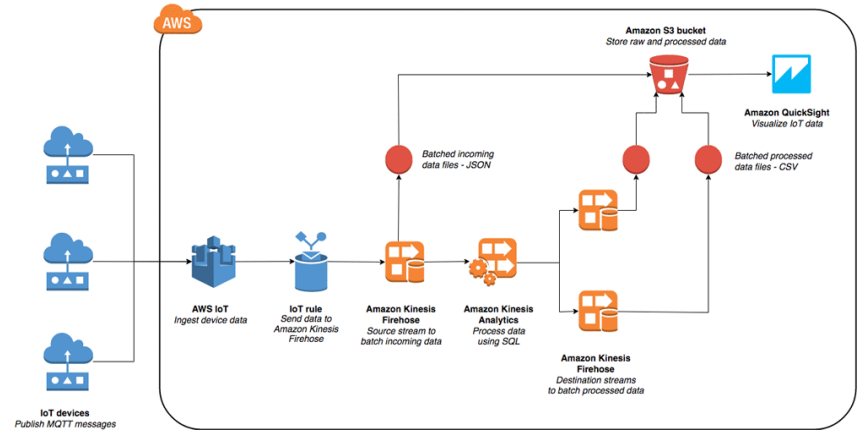




# Connect with AWS

At this point is possible to connect your device to the AWS IoT Core Thing and manage your data inside the AWS world.

Consider that some services like AWS Kinesis, AWS QuickSight or other services are not all free, so a solution could be connect **NodeRed** to the broker hosted on AWS and manage all the data inside NodeRed as we will see.



For more informations

**AWS IoT core :** <https://aws.amazon.com/it/iot-core/>

**Create an AWS Account :**

<https://aws.amazon.com/it/premiumsupport/knowledge-center/create-and-activate-aws-account/>

**Register a Device AWS IoT core:**

<https://docs.aws.amazon.com/iot/latest/developerguide/register-device.html>

**Example of real-time data monitoring using AWS:**

<https://aws.amazon.com/it/blogs/big-data/build-a-visualization-and-monitoring-dashboard-for-iot-data-with-amazon-kinesis-analytics-and-amazon-quicksight/>