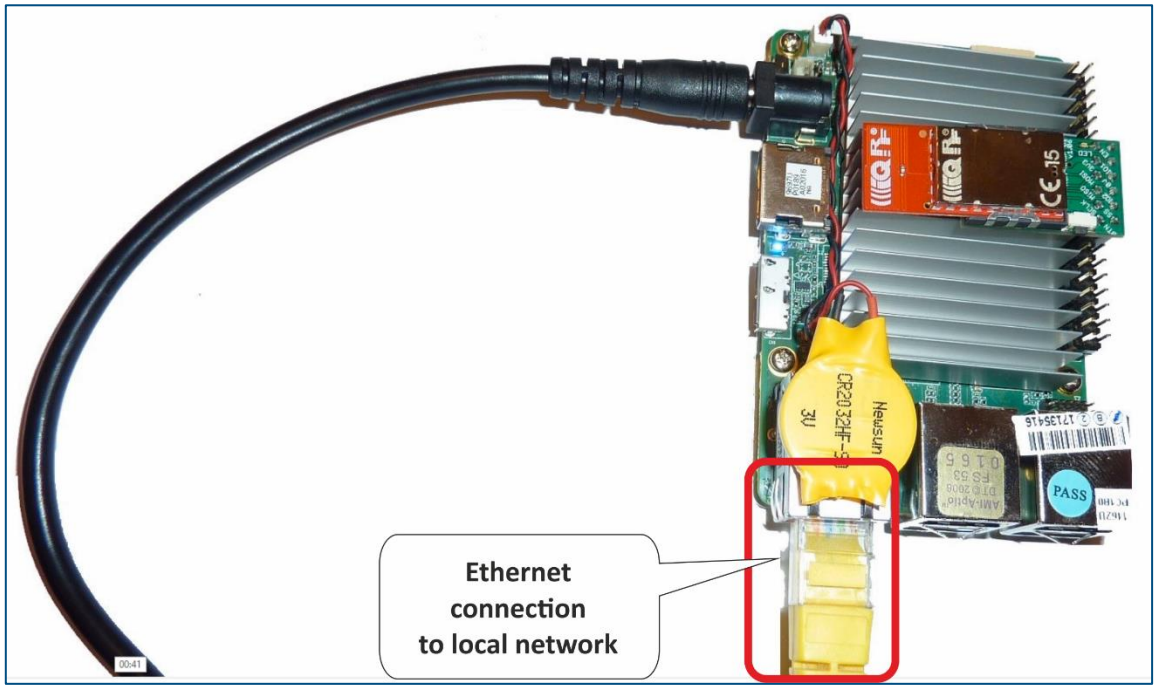
UP-IQRF IoT Starter Kit – Part 3: Connect to the cloud – AWS IoT

***Note**: If the PDF Guide is opened in a viewer mode, we strongly recommend downloading it and open on your computer locally to have hyperlinks functional and to be able to copy strings. The Download button you will find at the top of the page with a PDF preview.*

IoT Starter Kit is designed in the way to be connectable to different clouds via bidirectional MQTT channel. So, you can collect, store, process and visualize data in a cloud or you can send your commands to the IQRF network remotely. In this part, we will configure the UP board to communicate with the Amazon Web Services (AWS) through the MQTT channel.

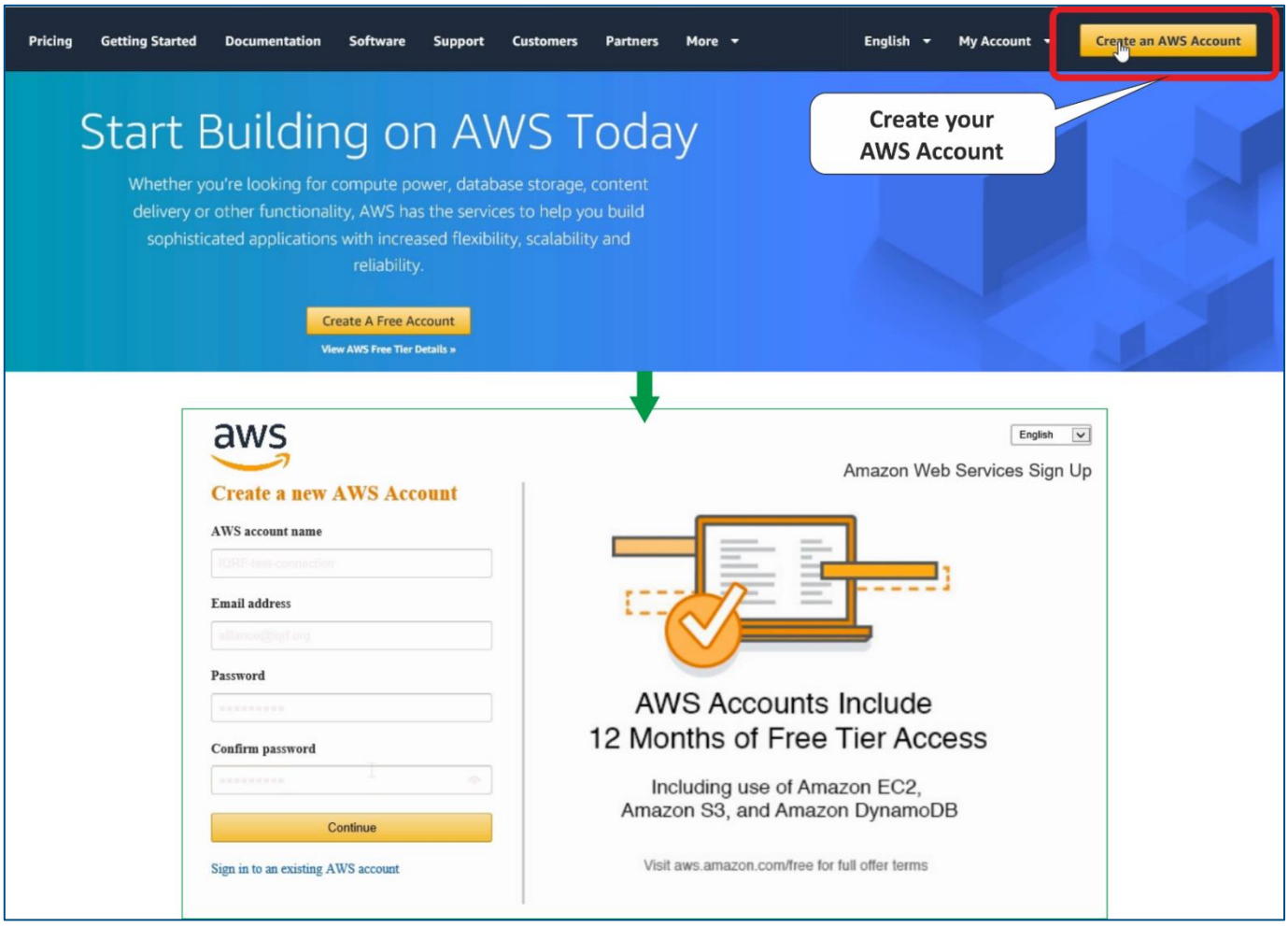
1 Local network

Connect your UP board to your local network so it can obtain an IP address using DHCP. In the following steps, you will enter this address into your web browser on your computer (which is in the same local network as the UP board) and configure your gateway through the IQRF Daemon Web application.



2 Amazon Web Services account

First, create an Amazon Web Services account (aws.amazon.com). You must fill in your personal or company data and add your credit card details. Your credit card will be used for payments in a case you exceed limits of the selected services.

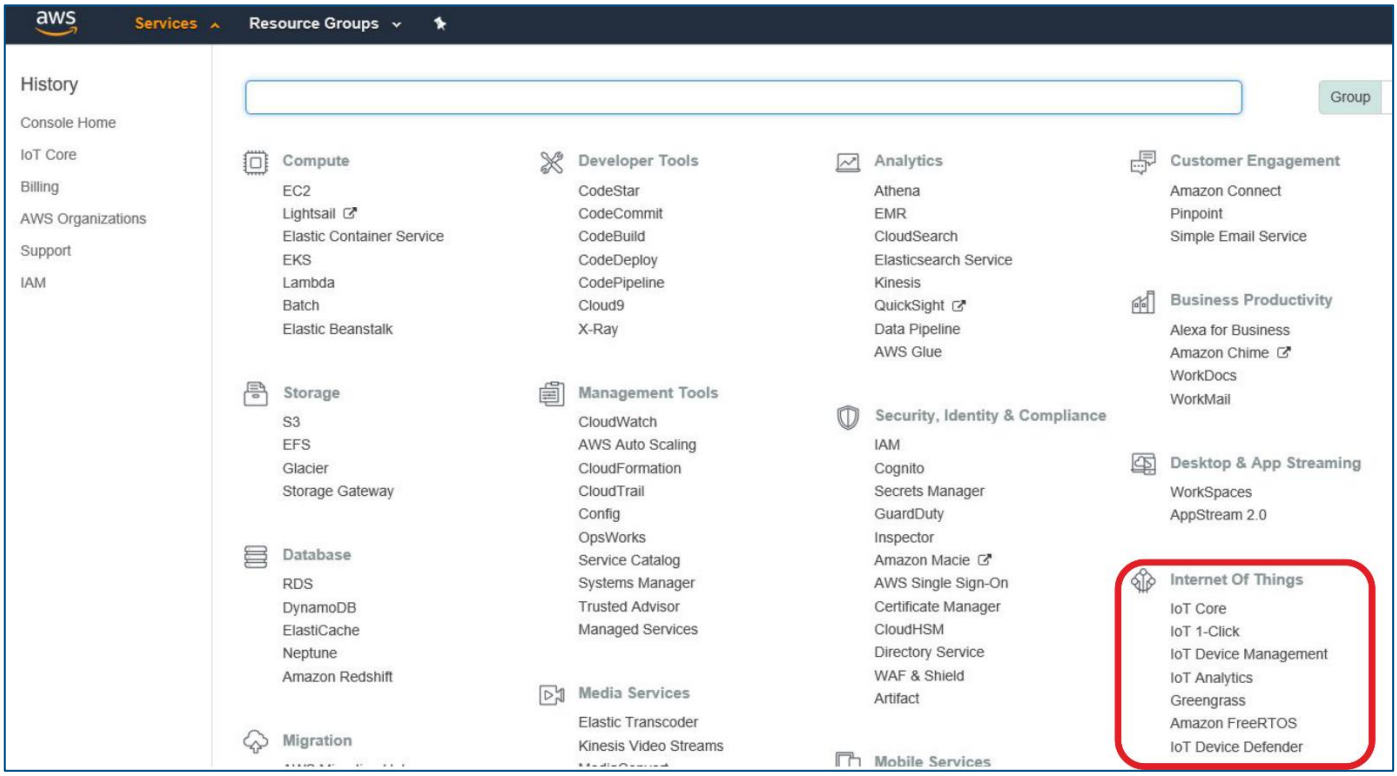


3 Set up the connection

To set up the connection between AWS and your UP board, you need to do some configuration steps on both sides.

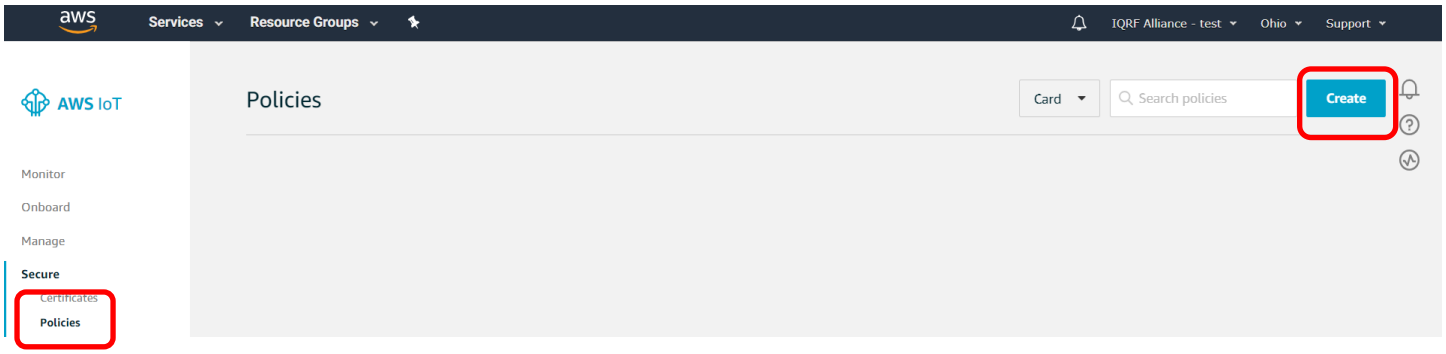
In **Services**, in the **Internet of Things** section of AWS, find **IoT Core**.

***Note**: the environment of AWS may look different because of often changes and its personalization. This guide shows the status of October 2018. You need to look for appropriate items to configure the MQTT connection.*



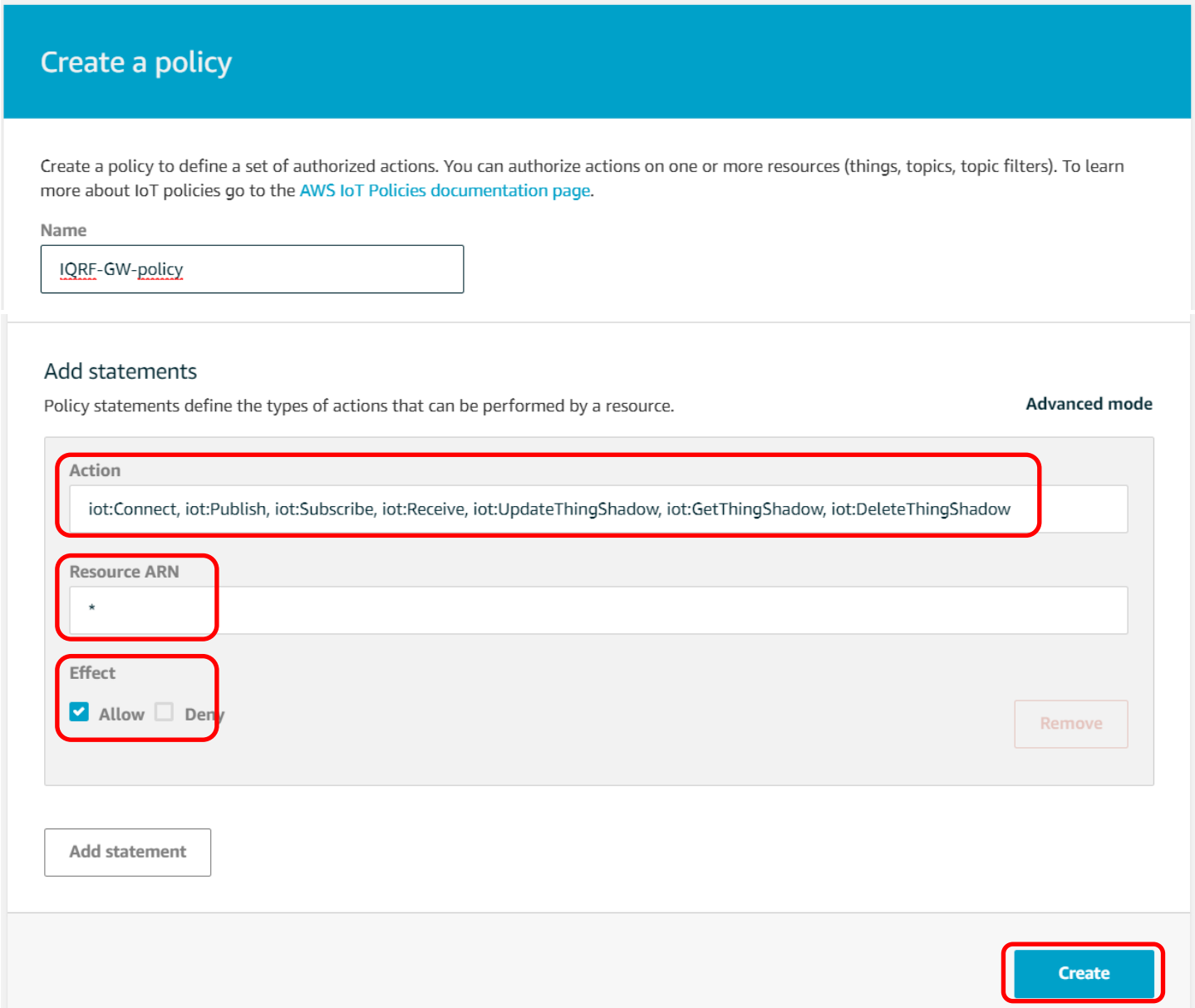
Create a default policy for the device. This step involves creating a default policy for the new device, skip if an existing policy is already available.

Access the main screen of the console and select **Secure** -> **Policies** from the left side menu and then press the **Create** button, in the top right area of the screen.

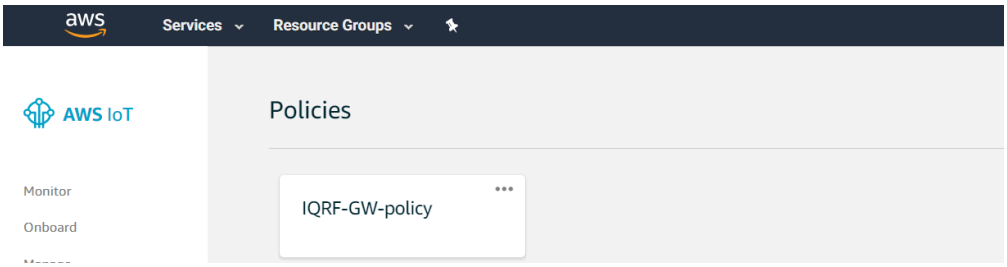


Fill the form as follows and then press the **Create** button:

- Action -> iot:Connect, iot:Publish, iot:Subscribe, iot:Receive, iot:UpdateThingShadow, iot:GetThingShadow, iot:DeleteThingShadow
- Resource ARN -> *
- Effect -> Allow

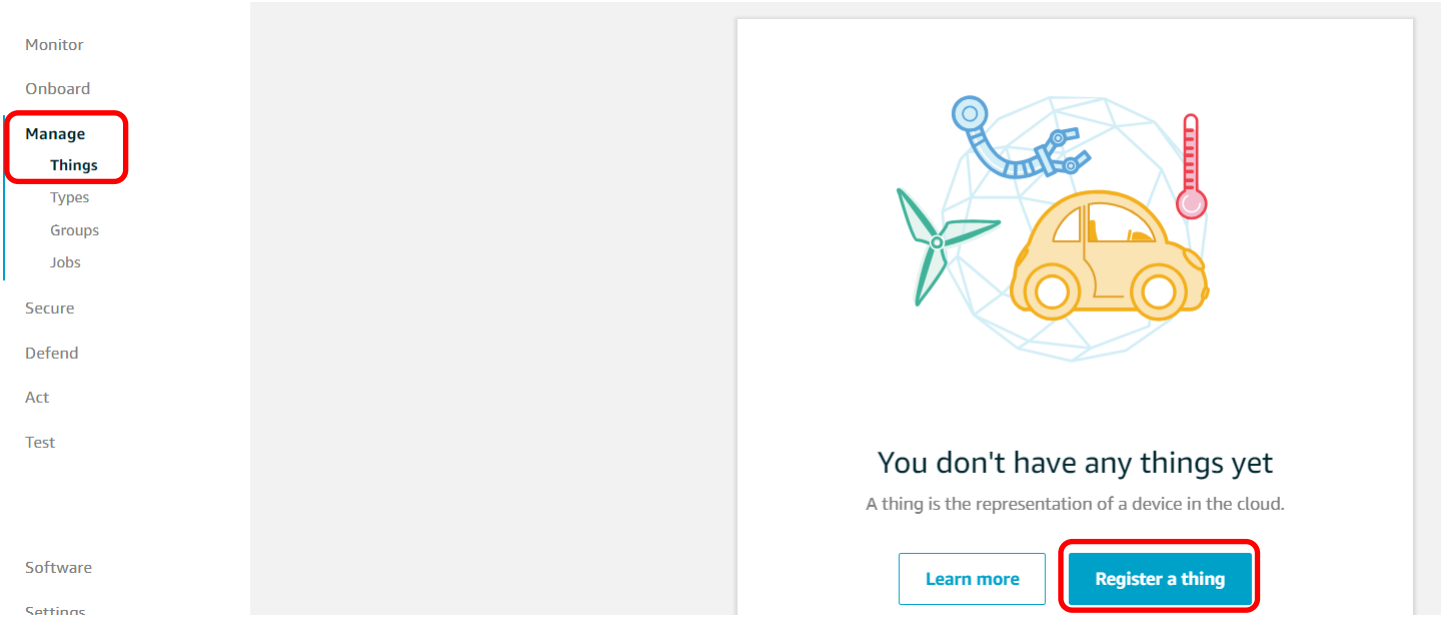


This will create a policy that allows a device to connect to the platform, publish/subscribe on any topic and manage its *thing shadow*.

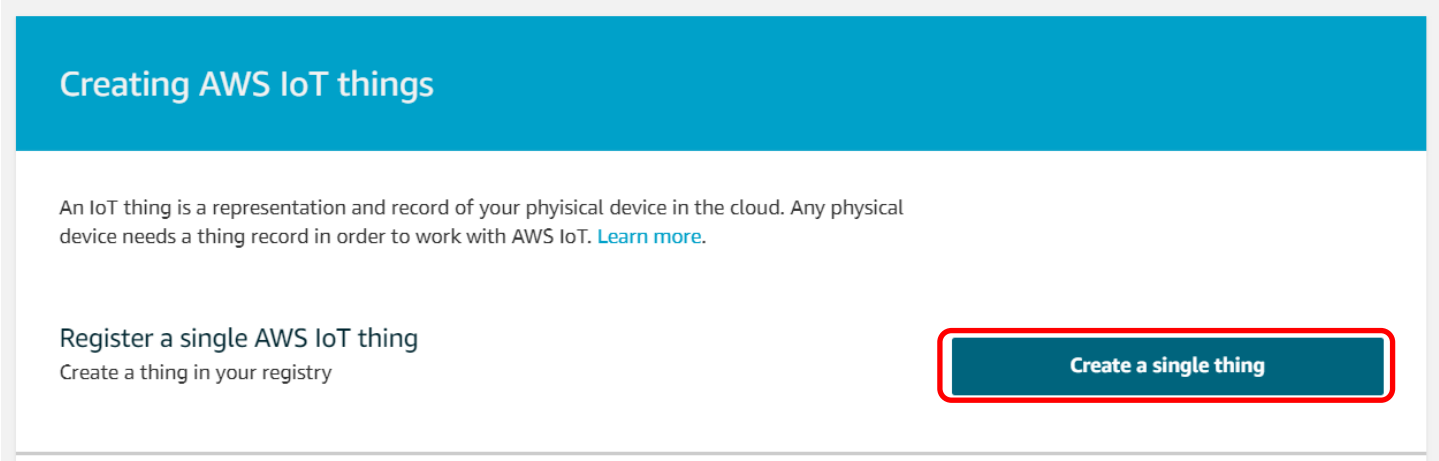


Register a new device.

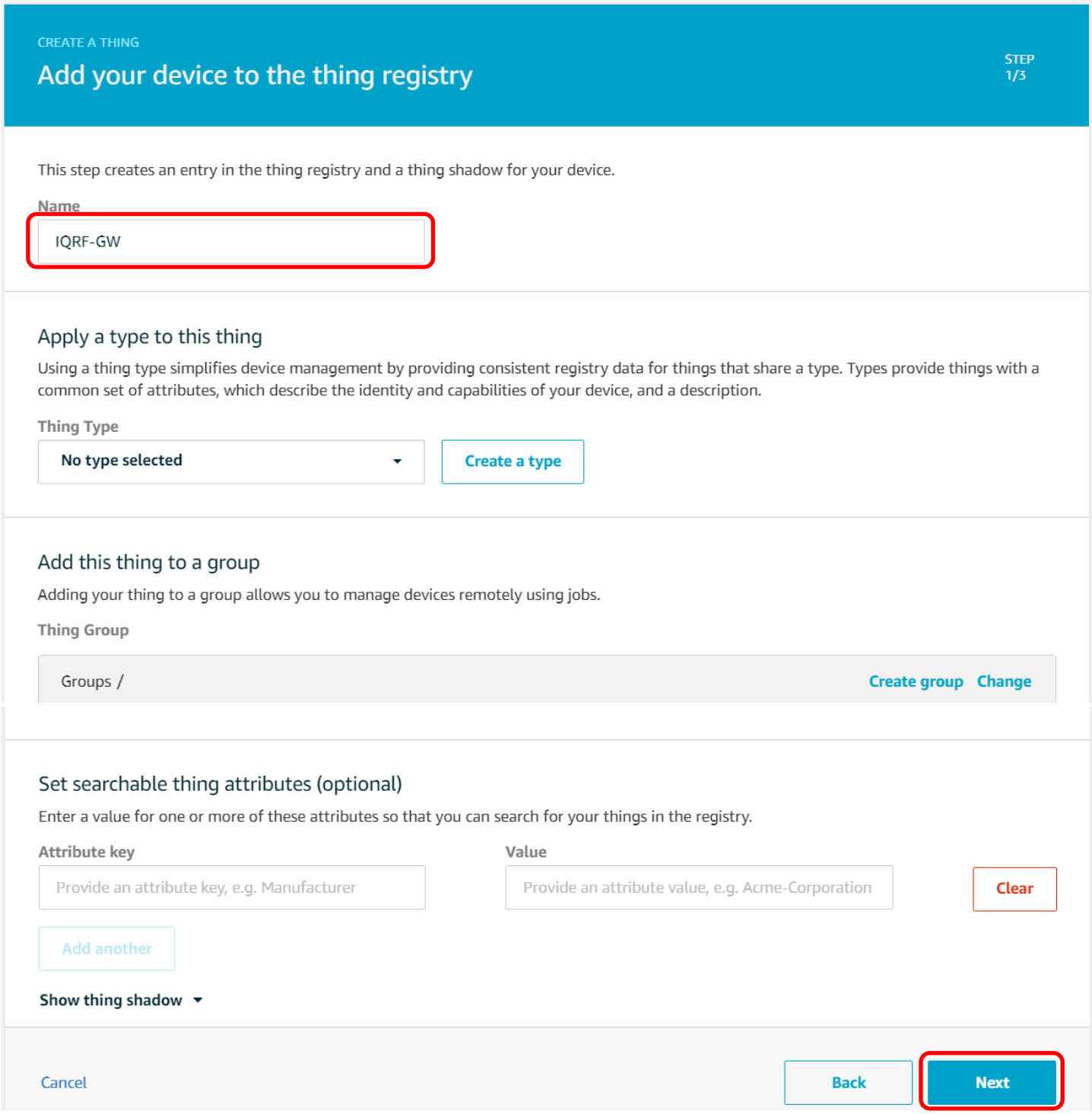
Devices on the AWS IoT platform are called things. In order to register a new thing, select **Manage** -> **Things** from the left side menu and then press the **Create** button, in the top right section of the screen (or press the **Register a thing button**).



Select **Create a single thing**.

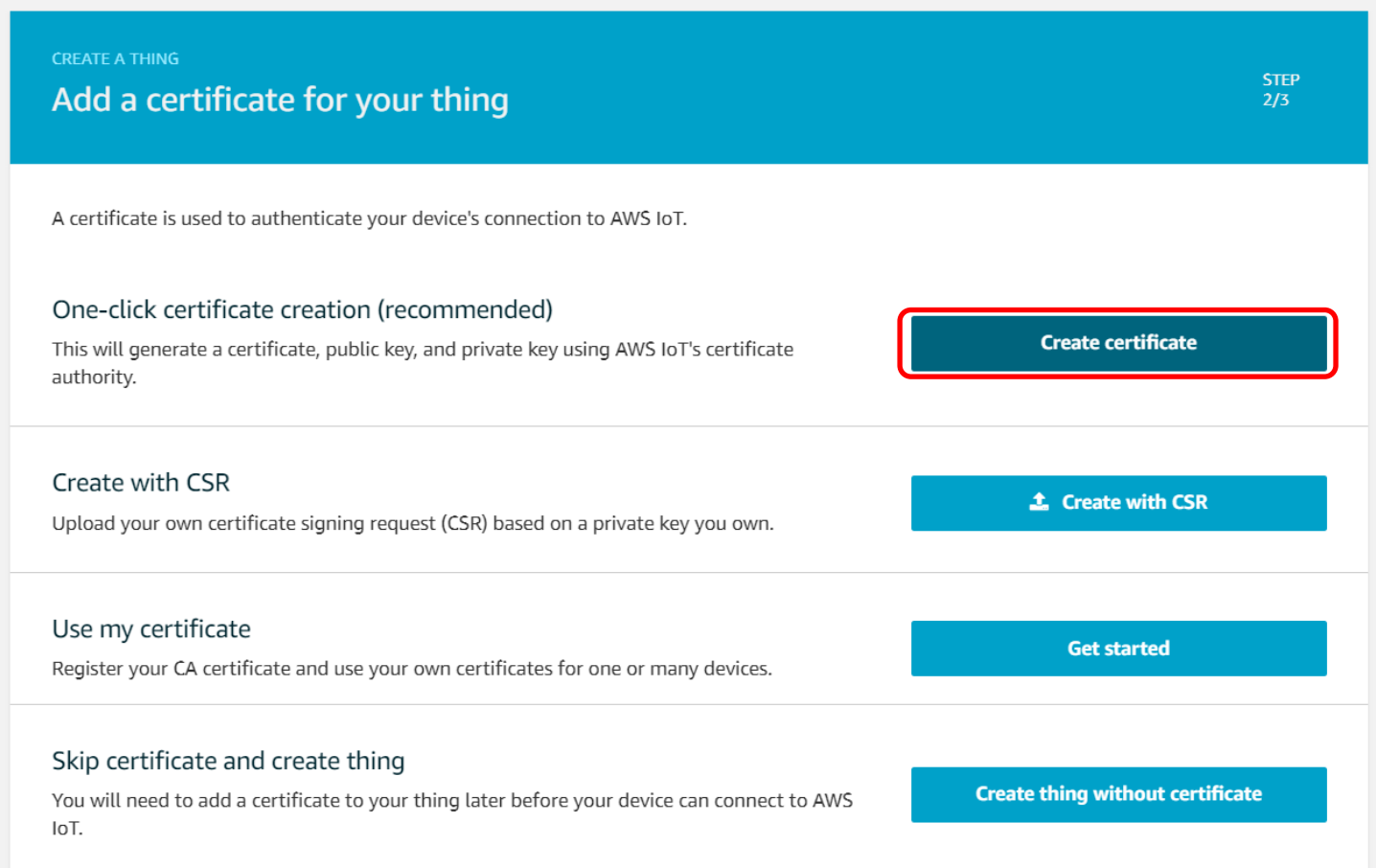


Enter a name for the new device and then press the **Next** button.

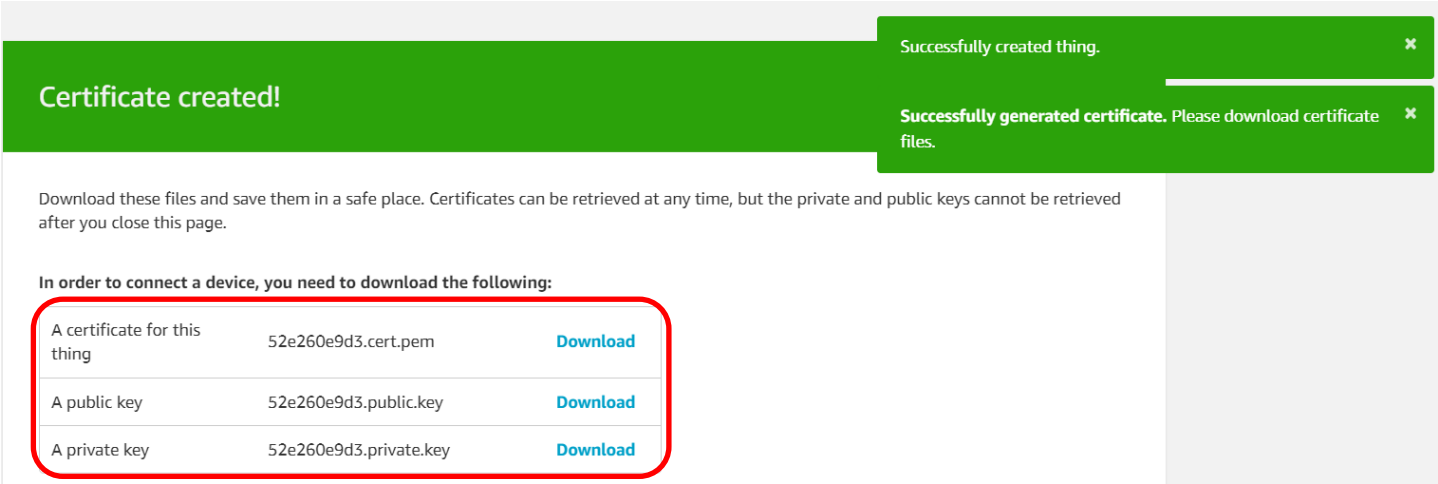


Create a new certificate for the device.

The AWS IoT platform uses SSL mutual authentication, for this reason it is necessary to download a public/private key pair for the device and a server certificate. Click on **Create certificate** to quickly generate a new certificate for the new device. Certificates can be managed later on by clicking on **Secure** -> **Certificates**, in the left part of the console.

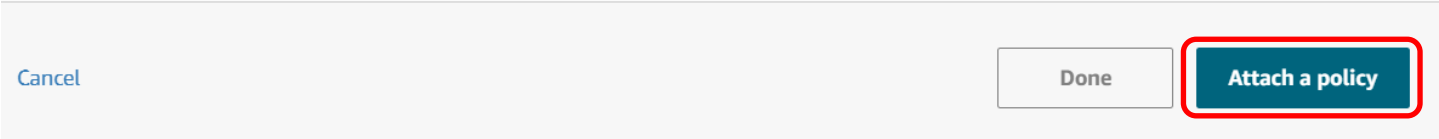


Download the device SSL keys.



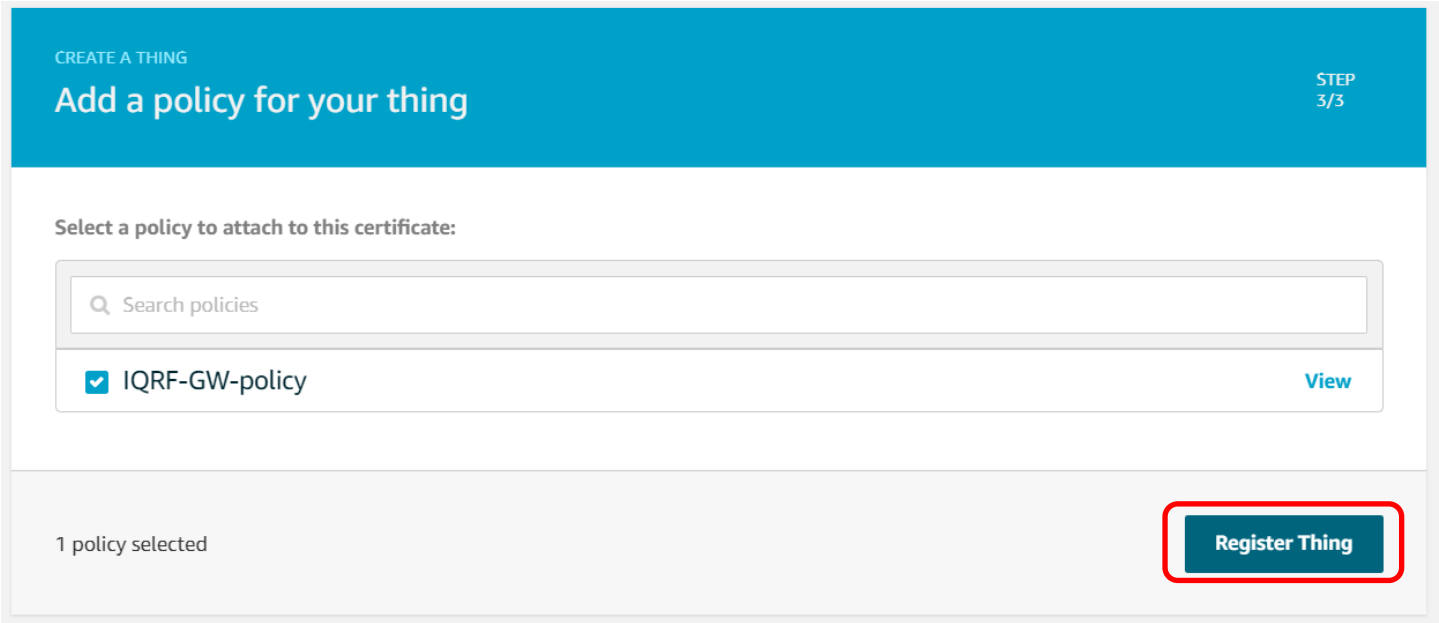
Download the 3 files listed in the table and store them in a safe place, they will be needed later.

Press the **Activate** button, and then on **Attach a policy**.

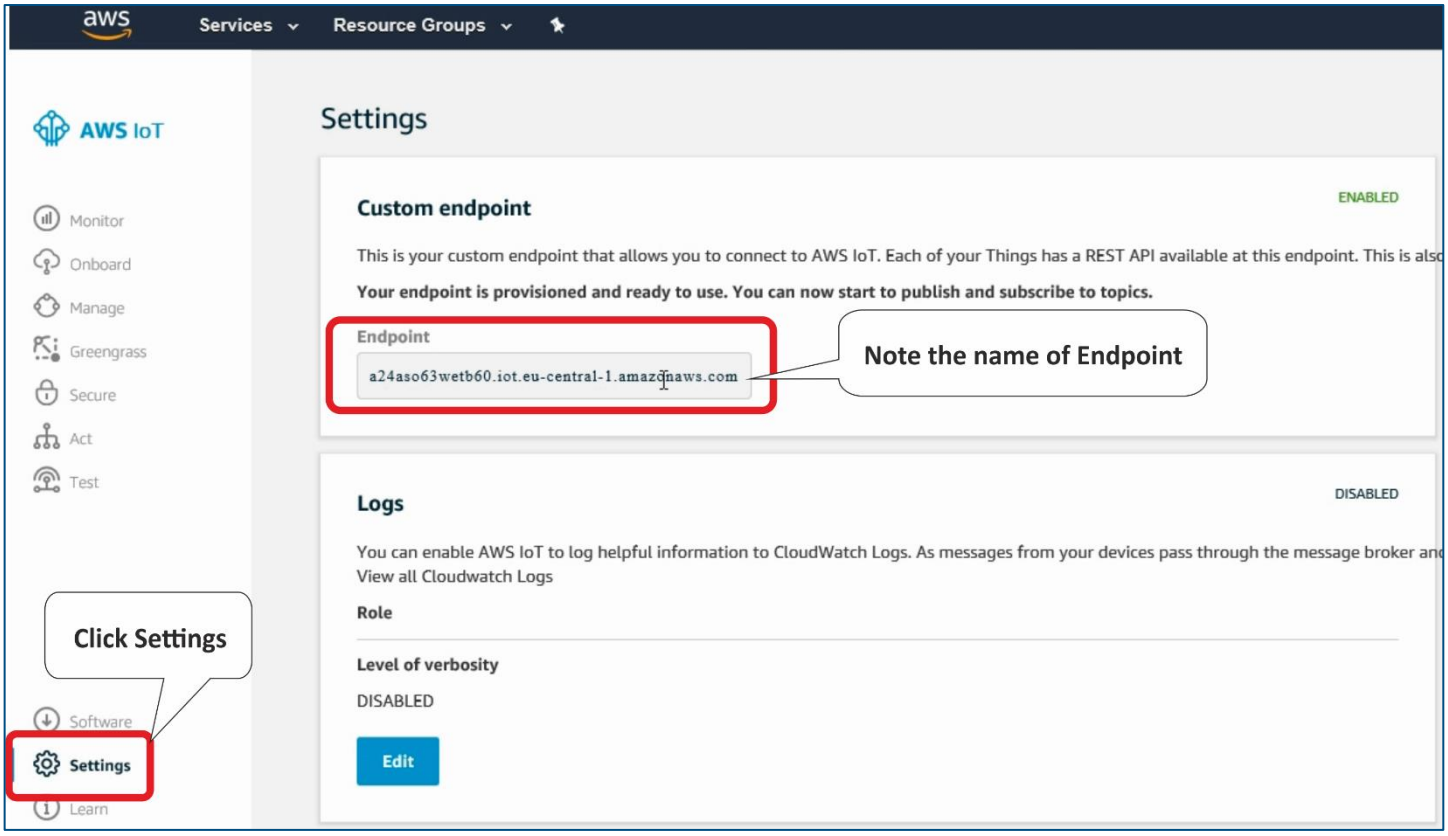


Assign the default policy to the device.

Select the desired policy and then click on **Register thing**.

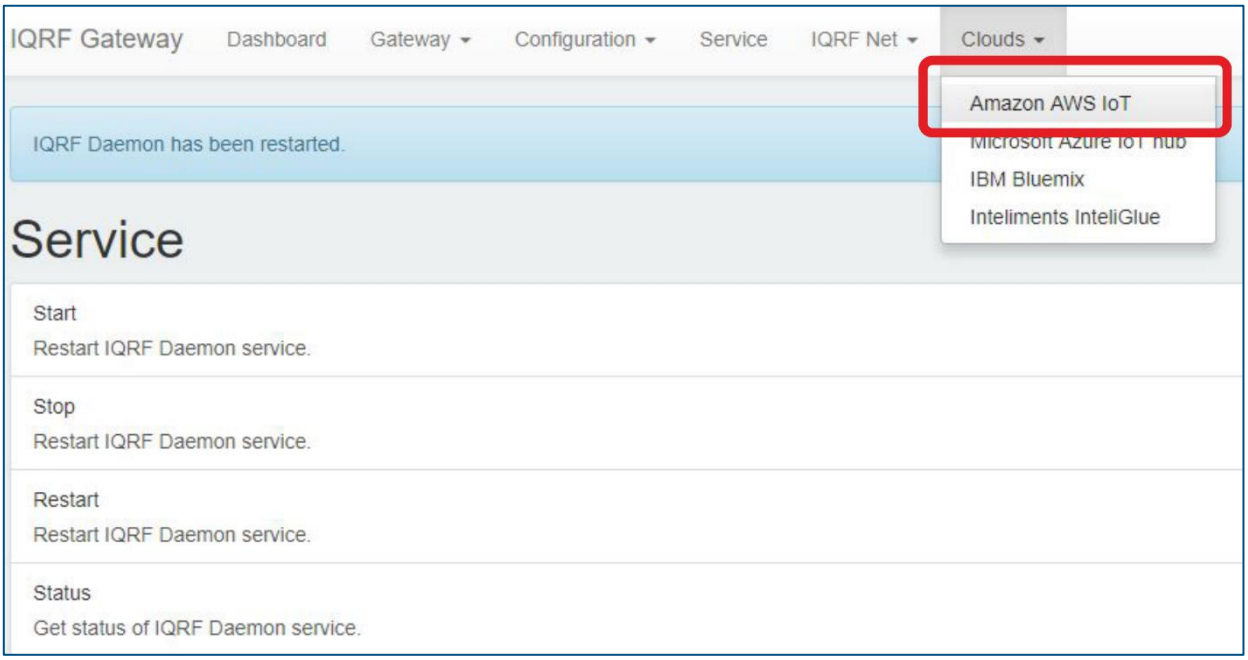


In the **Settings**, copy the name of your **endpoint,** you will need it for the UP board configuration in next steps.

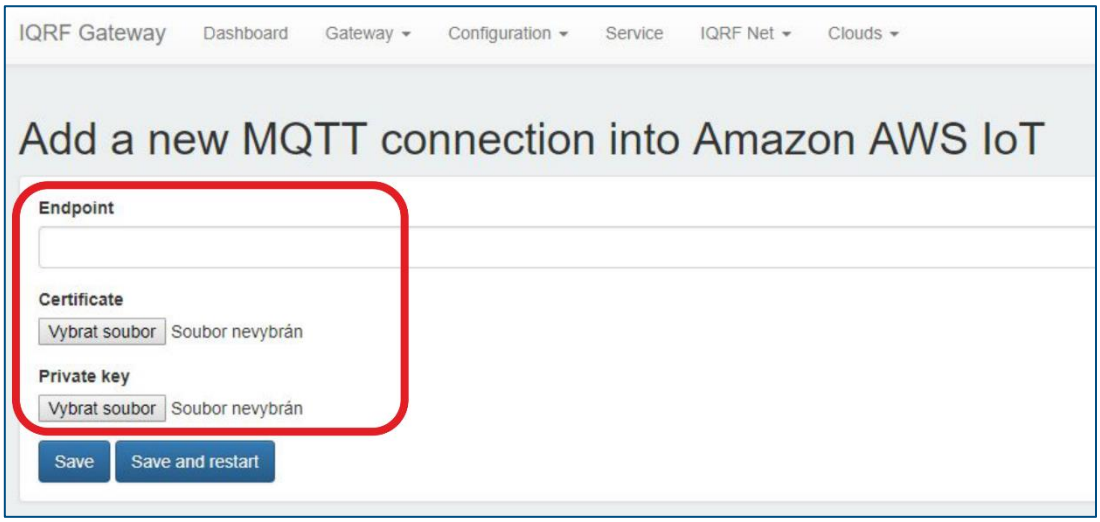


Files private key and certificate file (SSL keys) should be already downloaded. You will transfer them to the UP board through the IQRF Gateway Daemon web application.

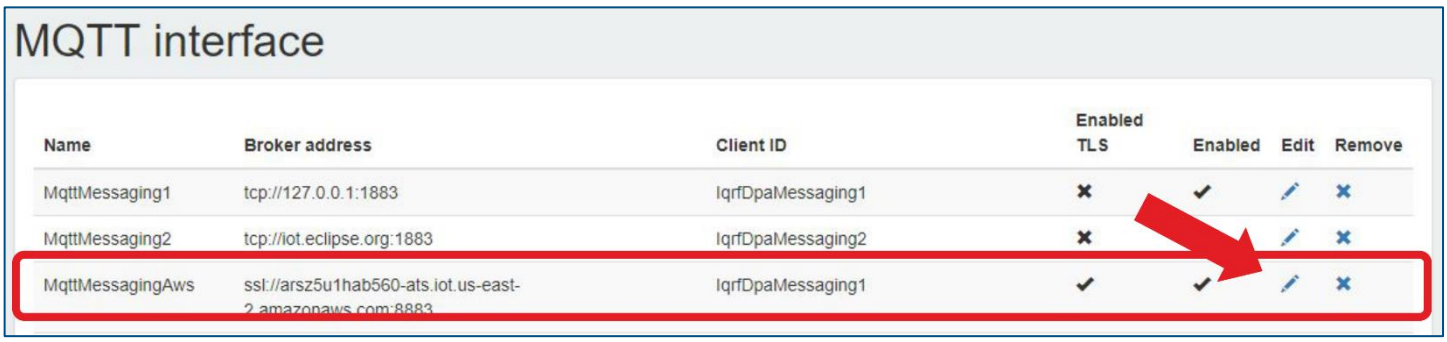
In the web browser on your computer, insert the IP address of your UP board, and login to it as *admin* with password *iqrf*. Ask your network administrator how to find out your IP address or you can use common network tools.
In the **IQRF Gateway Daemon web application,** click on the **Amazon AWS IoT** item in the **Clouds** menu.



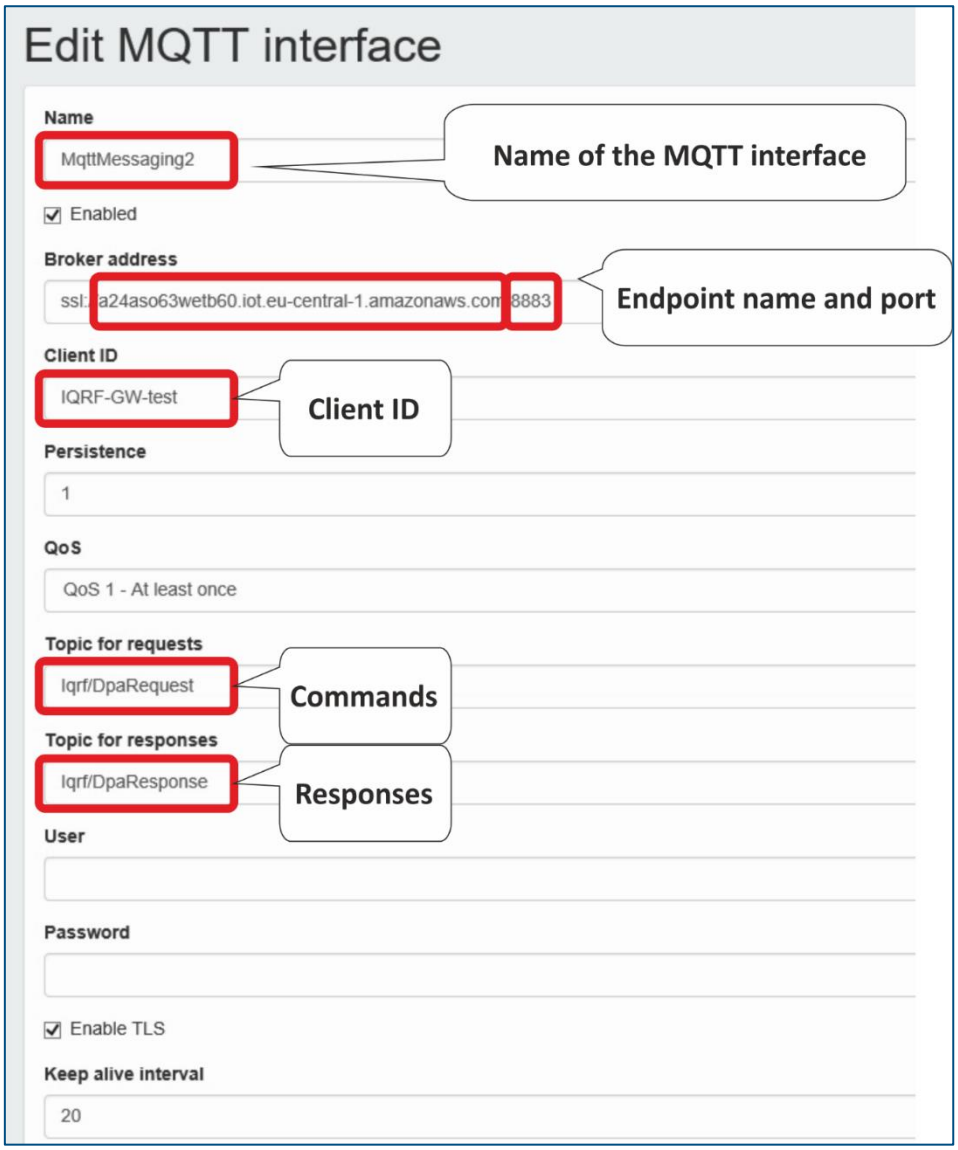
Paste the name of the **Endpoint** (you have copied it from Settings of your AWS IoT). Select certificate and a private key file. Save the configuration.



Inspect the new MQTT interface for AWS.

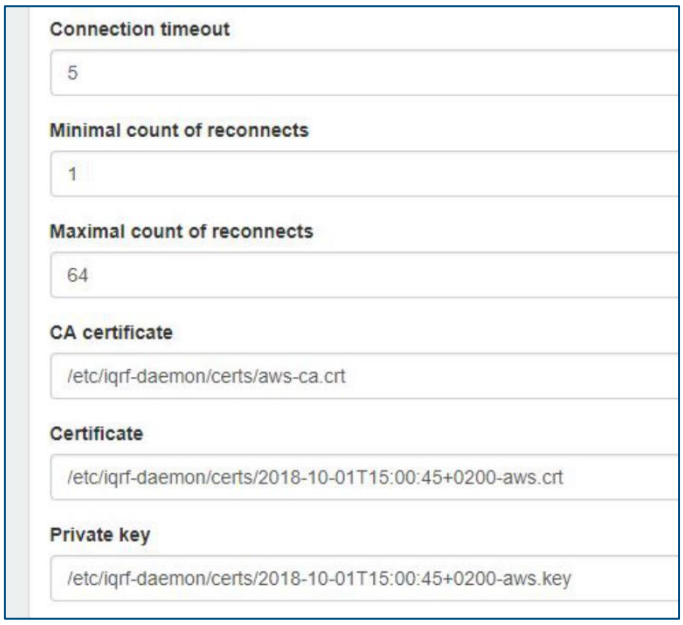


Address of the **endpoint** goes after the **SSL** protocol and at the end of Broker address is the port number **8883**. **Iqrf/DpaRequest** is set as the topic for commands, and **Iqrf/DpaResponse** is set as the topic for responses.

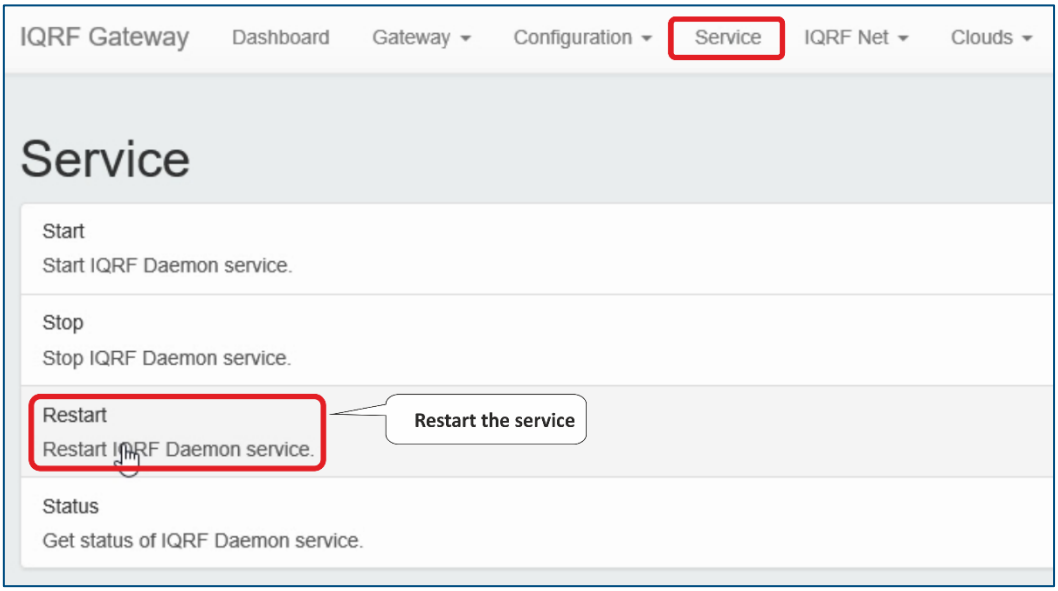


***Note**: your files and name of the endpoint may differ from the names shown in the pictures.*

There are the **timeout**, the **minimum,** and **maximum** connections set, and the path to the uploaded files that set up a secure connection between the gateway and the cloud.

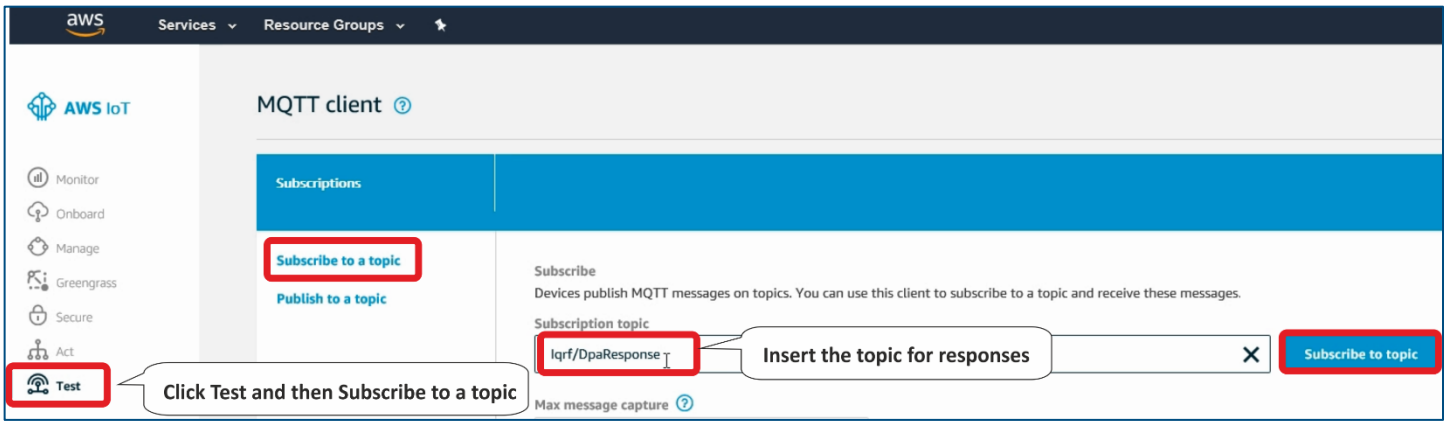


Restart IQRF Gateway Daemon. After restarting, check the status of the UP board if the selected services are running.



4 Test the connection

In the web browser on your computer, in AWS IoT, click **Test**. Enter the **Iqrf/DpaResponse** to the Response topic to retrieve the gateway responses and click on **Subscribe to topic**.



To send commands from the cloud to the gateway, set the **Iqrf/DpaRequest** as the topic for requests. Gateway will expect commands in this topic.

Insert a DPA packet in the JSON format into the text box and click on **Publish to topic**. In our example, we sent a command to turn on the red LED on the coordinator.


```
{
"ctype": "dpa",
"type": "raw",
"msgid": "1510754980",
"request": "00.00.06.01.FF.FF",
"request_ts": "",
"confirmation": "",
"confirmation_ts": "",
"response": "",
"response_ts": ""
}
```

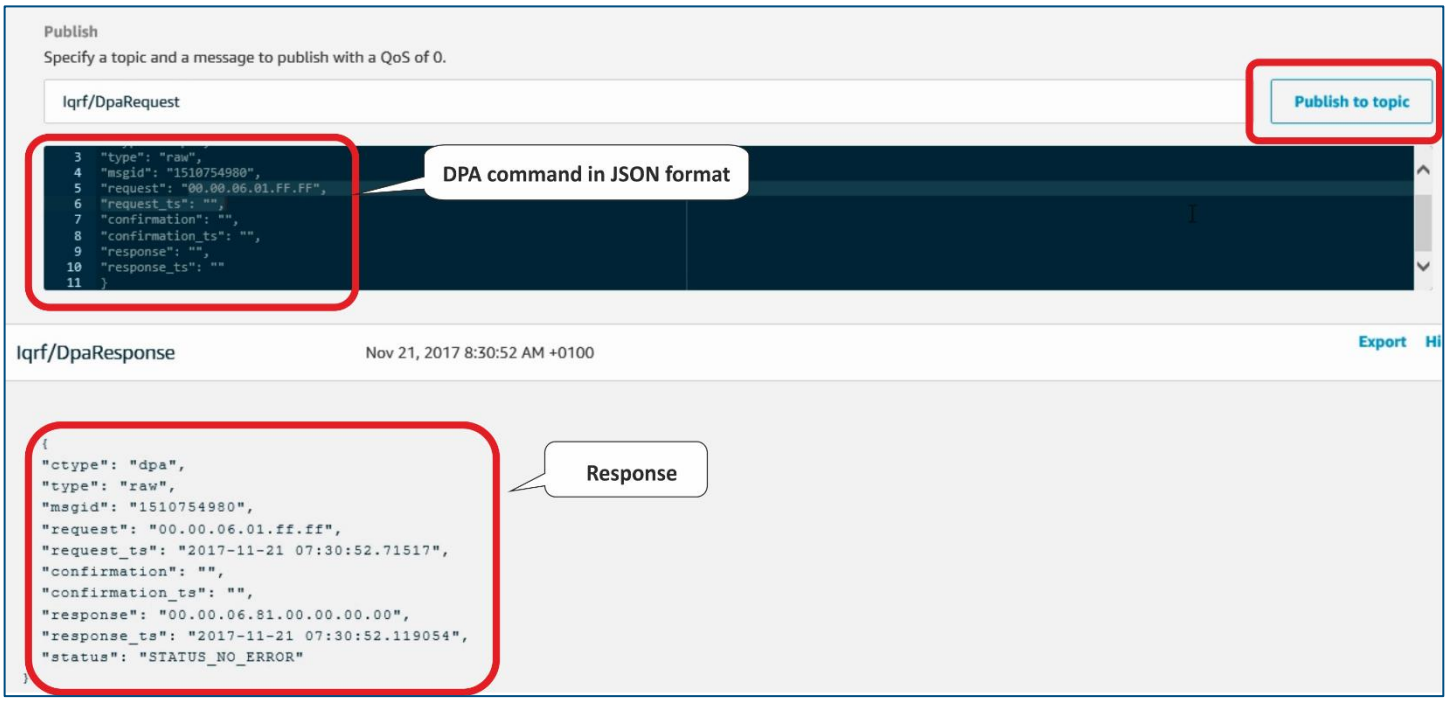

In the *"request"* item, you can insert other DPA commands for the network control and monitoring. You can find these commands in macros for IoT Starter Kit or you can set up them in the Terminal window in the IQRF IDE.

Examples:

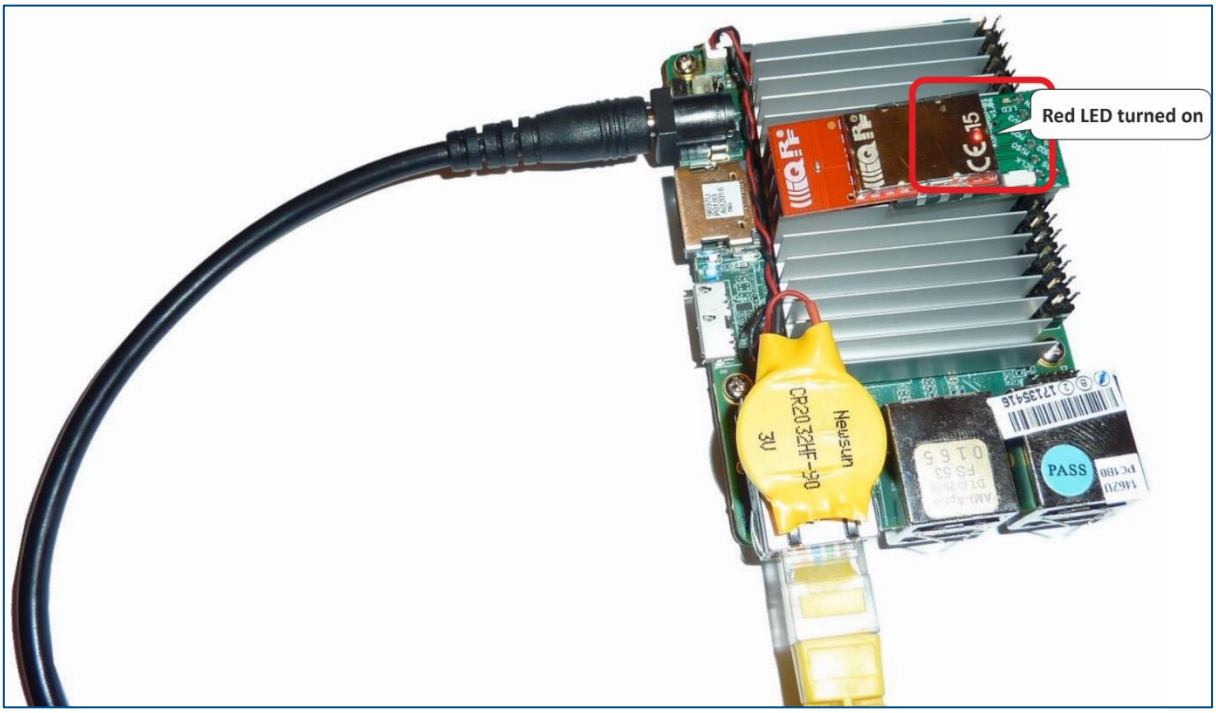
- Collecting all sensoric data from the Node #1 with the connected DDS-SE kit: 01.00.5E.01.FF.FF.FF.FF.FF.FF.
- Turning on both relays on the Node #2 with connected DDC-RE kit: 02.00.4B.00.FF.FF.0C.00.00.00.01.01.
- Getting temperature from the Node #3: 03.00.0A.00.FF.FF.

For more information about macros and the IQRF network read the [IoT Starter Kit – Part 1: Build your IQRF network](#).

We can see that the gateway picked up and executed the command, and sent a confirmation with "No Error" into the **Iqrf/DpaResponse** topic.



We can visually double check the result of this command. The red LED turned on.



5 Summary

The bidirectional communication between IQRF network and the Amazon Web Services is up and running. Now it's just up to you to use it for your own IoT solution. In next parts, we will show you how to add other sensors and actuators of our industrial partners (CO_2 sensor, wirelessly controlled power socket etc.).

IQRF transceivers have from a factory these default settings: TX power: 7, RX filter: 0, RF channel A: 52. Because of those settings (TX power, RX filter), you can cover with the wireless IQRF signal an area of 500 m radius in open space.