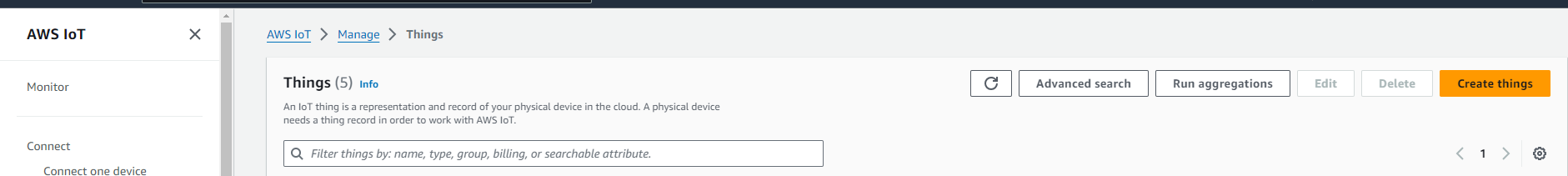
# Connecting to AWS Cloud Instance

Perform the following steps to get the device connected to your own AWS cloud instance.

1. Create an AWS account or log in to your existing AWS account.

- Please refer to [Set up your AWS account](https://docs.aws.amazon.com/iot/latest/developerguide/setting-up.html) and [Create AWS IoT resources](https://docs.aws.amazon.com/iot/latest/developerguide/create-iot-resources.html) for details.

1. Navigate to IoT Core console -> Manage -> Things and click on “Create” / “Register a Thing”.



1. Select “Create a single thing”.

A screenshot of a computer

Description automatically generated

1. For thing name, you can have a unique name or the name that originates from the device certificate.

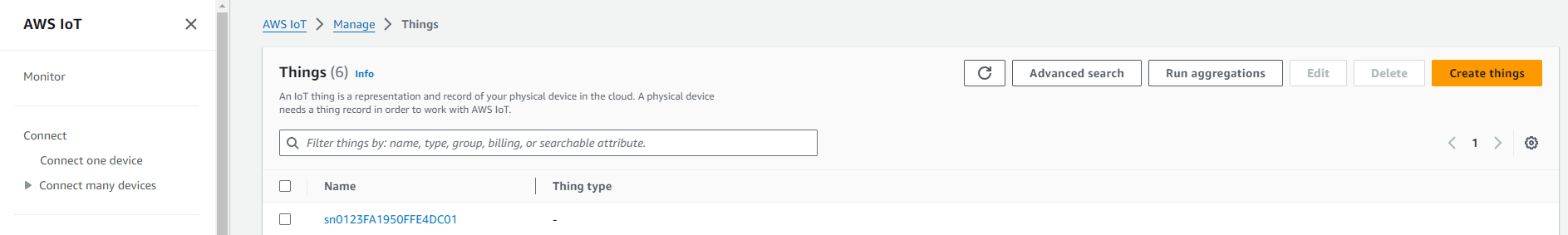
A screenshot of a computer

Description automatically generated

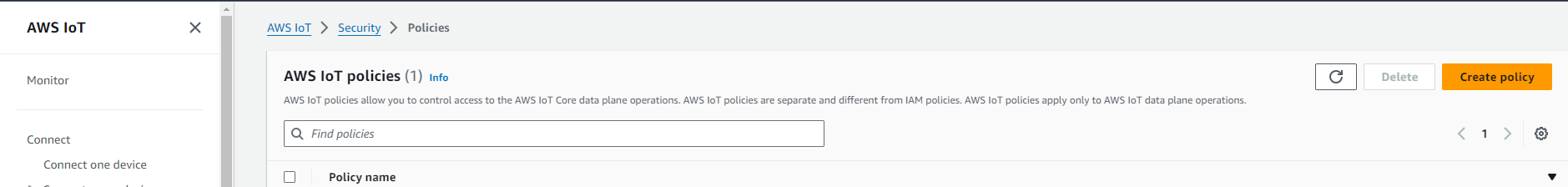
1. Select defaults for the other fields and click “Next” at the bottom of the page.
2. Select “Create thing without certificate” in the next page.

A screenshot of a computer

Description automatically generated



1. Go to “Secure” -> “Policies” and select “Create Policy”.



1. Create a new policy which allows all connected devices to perform all actions without restrictions.

This policy grants unrestricted access for all iot operations and is to be used only in a development environment. For non-dev environments, all devices in your fleet must have credentials with privileges that authorize intended actions only, which include (but not limited to) AWS IoT MQTT actions such as publishing messages or subscribing to topics with specific scope and context. The specific permission policies can vary for your use cases. Identify the permission policies that best meet your business and security requirements. Please refer to [sample policies](https://docs.aws.amazon.com/iot/latest/developerguide/example-iot-policies.html) and [security best practices.](https://docs.aws.amazon.com/iot/latest/developerguide/security-best-practices.html)

|  |  |
| --- | --- |
| Item | Policy Parameter |
| Name | allowAll |
| Action | \* |
| Resource | \* |

A screenshot of a computer

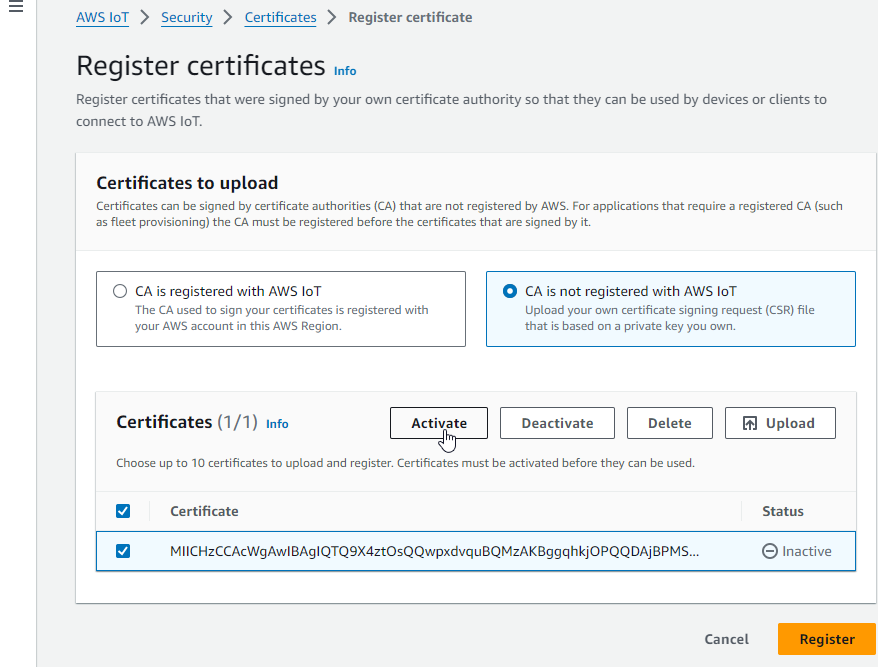
Description automatically generated

1. Navigate to “Certificates” -> “Add certificate”.

A screenshot of a computer

Description automatically generated

1. Select Create with “CA not registered with AWS IoT”.
2. “Upload” the device certificate
   1. The device certificate needs to be read from the device using the AT commands (more details available [here](https://github.com/MicrochipTech/RNWF11_Beta/blob/main/Reading%20certificate%20using%20AT%20command.docx)) or a Python script (mode details available TBD).
3. Select “Activate” and click “Register”.



1. Select the certificate and Click “Attach policy” and select the “allowAll” policy created earlier.

xxxxxxxxxxxxxxxxxxx

A screenshot of a computer

Description automatically generated

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxx

1. Click “Attach thing” and choose the “thing”.

A screenshot of a computer

Description automatically generated

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

1. Navigate to “Settings” and copy the endpoint URL. This URL would need to be configured in the firmware to enable it to connect to the AWS Broker.

A screenshot of a computer

Description automatically generated