Cloud Setup Procedure

Table of Contents

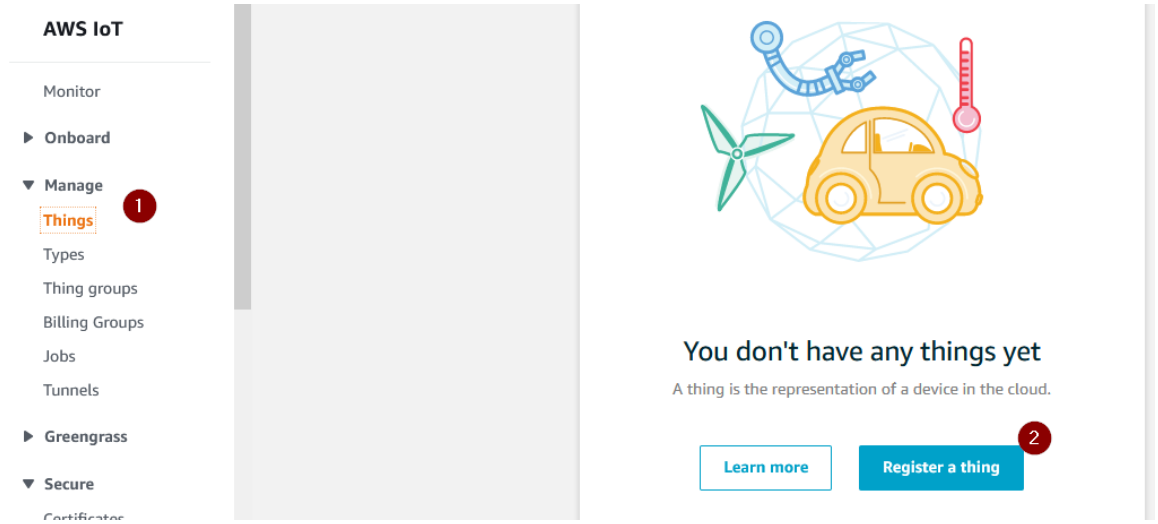
1. Connecting to Different Cloud Vendors:

This document talks about setting up/ configuring the different cloud vendors for use with microchip Wi-Fi solutions.

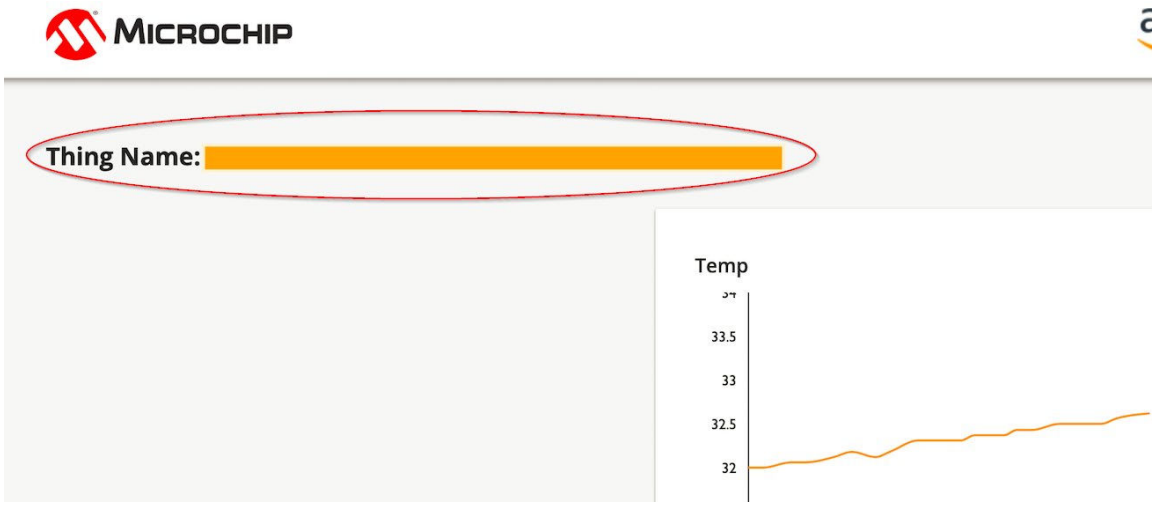
1.1 Connecting to AWS Cloud Instance

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 and Create AWS IoT resources for details.
2. Navigate to IoT Core console -> Manage -> Things and click on “Create” / “Register a Thing”.

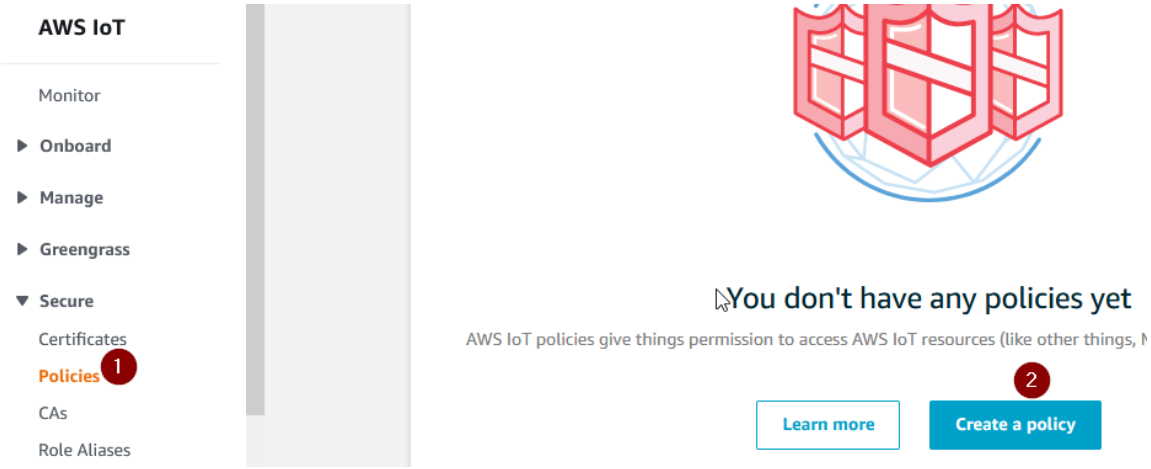


3. Select “Create a single thing”.
4. For thing name, you can have a unique name or the name that originates from the device certificate.



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

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

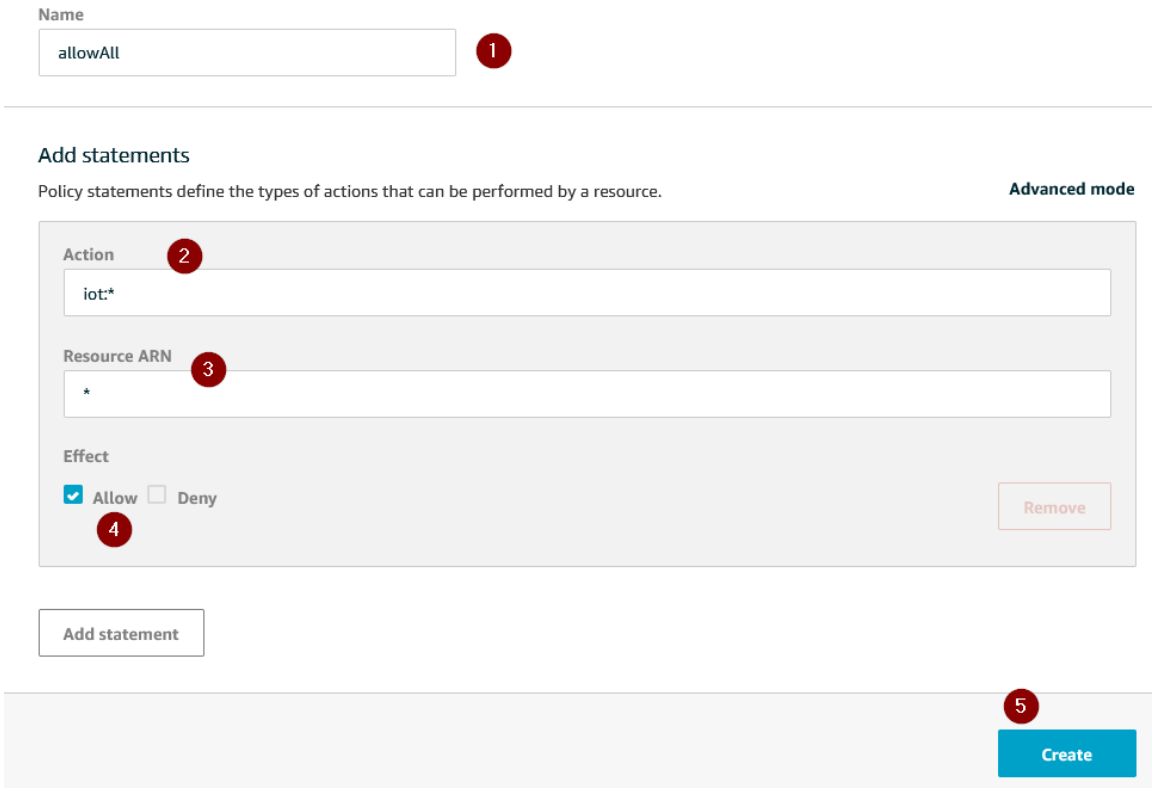


8. Create a new policy which allows all connected devices to perform all actions without restrictions

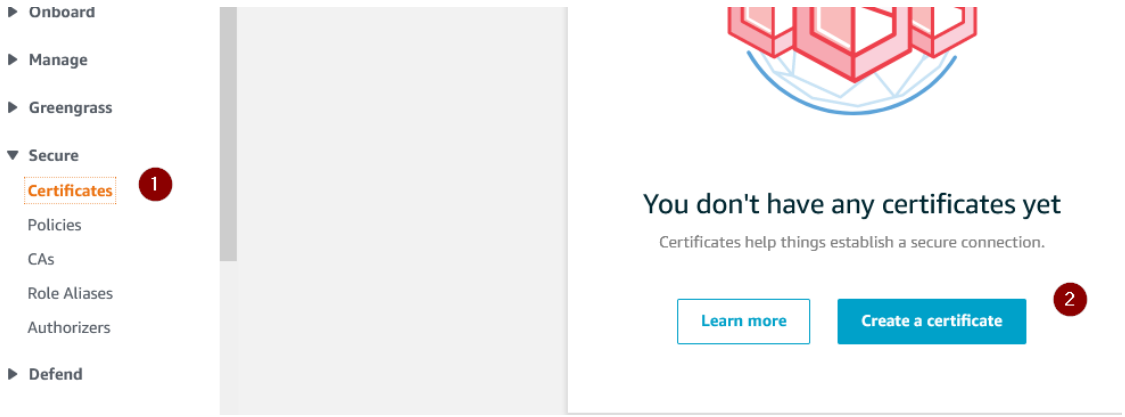
   This policy grants unrestricted access for all iot operations and is to be used only in a development environment. For non-dev environments, all devices in your fleet must have credentials with privileges that authorize intended actions only, which include (but not limited to) AWS IoT MQTT actions such 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 and security best practices.
   | Item | Policy Parameter |

Name	allowAll
Action	iot:*
Resource Arn	*

| **_Effect_** | Allow |

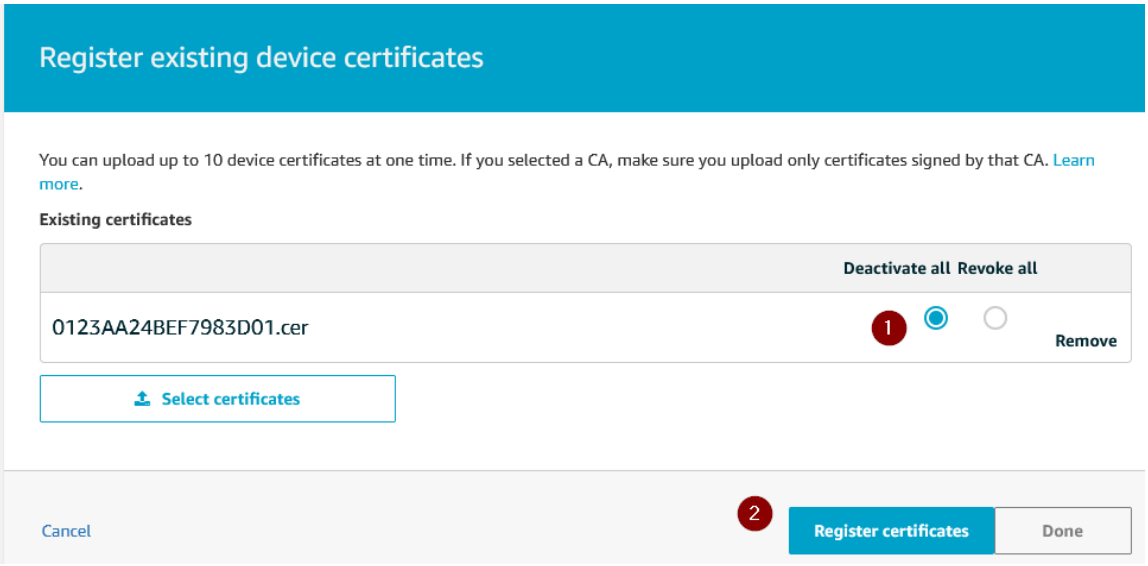


9. Navigate to “Certificates” -> “Create a certificate”.

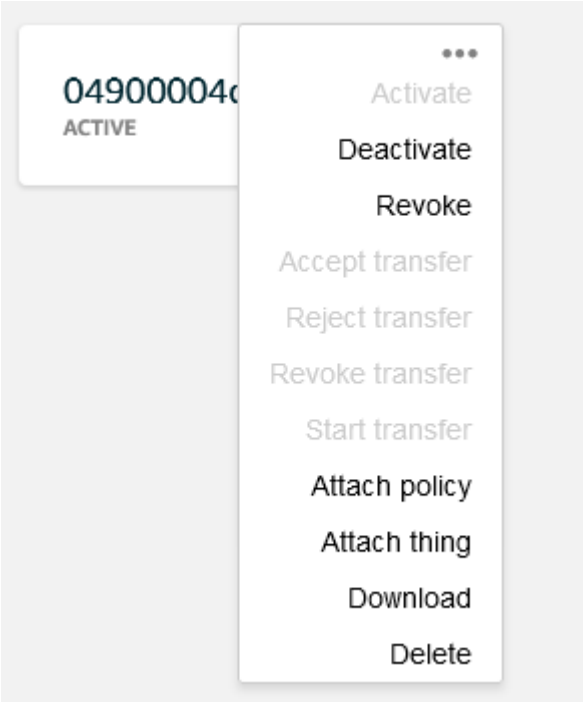


10. Select Create with “Get Started” under “Use my certificate”.
11. In the next screen, click “Next” without making any selections.
12. Click on “Select certificates”.
13. In the MSD enumerated when the Curiosity Board is plugged in, you can find a “.cer” file with an alphanumeric name. Select this file when prompted to select a certificate.

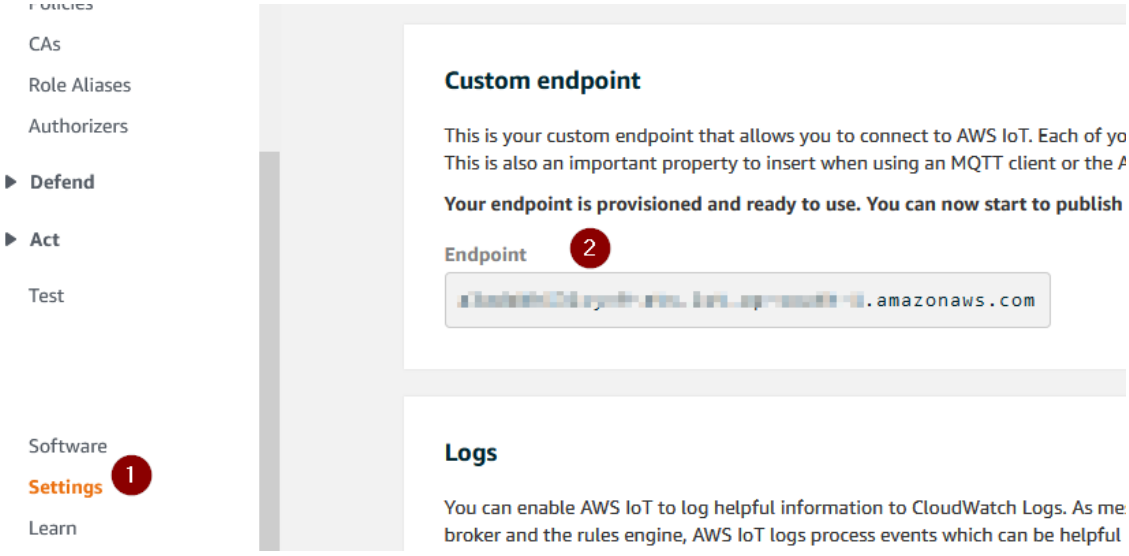
14. Select “Activate all” and click “Register certificates”.



15. Select the certificate and
    a. Click “Attach policy” and select the “allowAll” policy we created.
    b. Click “Attach thing” and choose the “thing” we created.



16. Navigate to “Settings” and copy the endpoint URL.

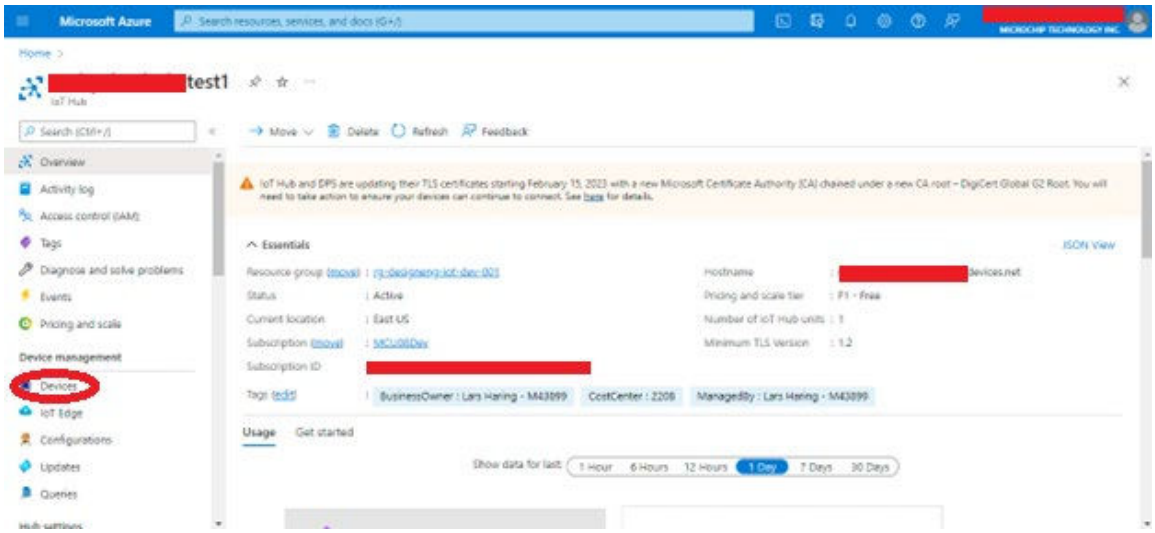


17. Follow below guide to replace the AWS MQTT broker name with the endpoint URL in the OOB project to connect to your own AWS account: microchipsupport.force.com/s/article/Change-the-MQTT-broker-name-in-the-WFI32-OOB-project-to-connect-to-own-AWS-account.
18. Program the updated code to the board, the device will connect to your own cloud instance.

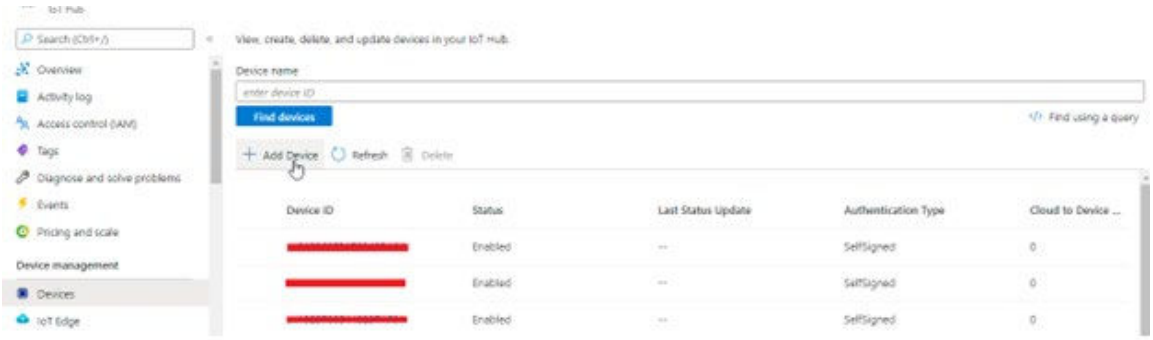
1.2 Connecting to Azure Cloud Instance

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

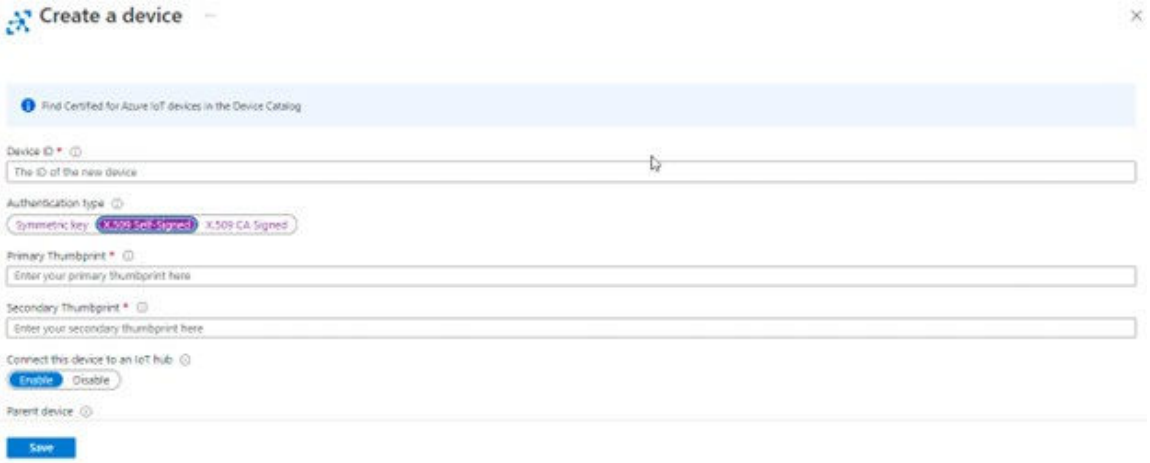
1. Create an Azure account or log in to your existing Azure account.
2. Click on “Devices” in the left column.



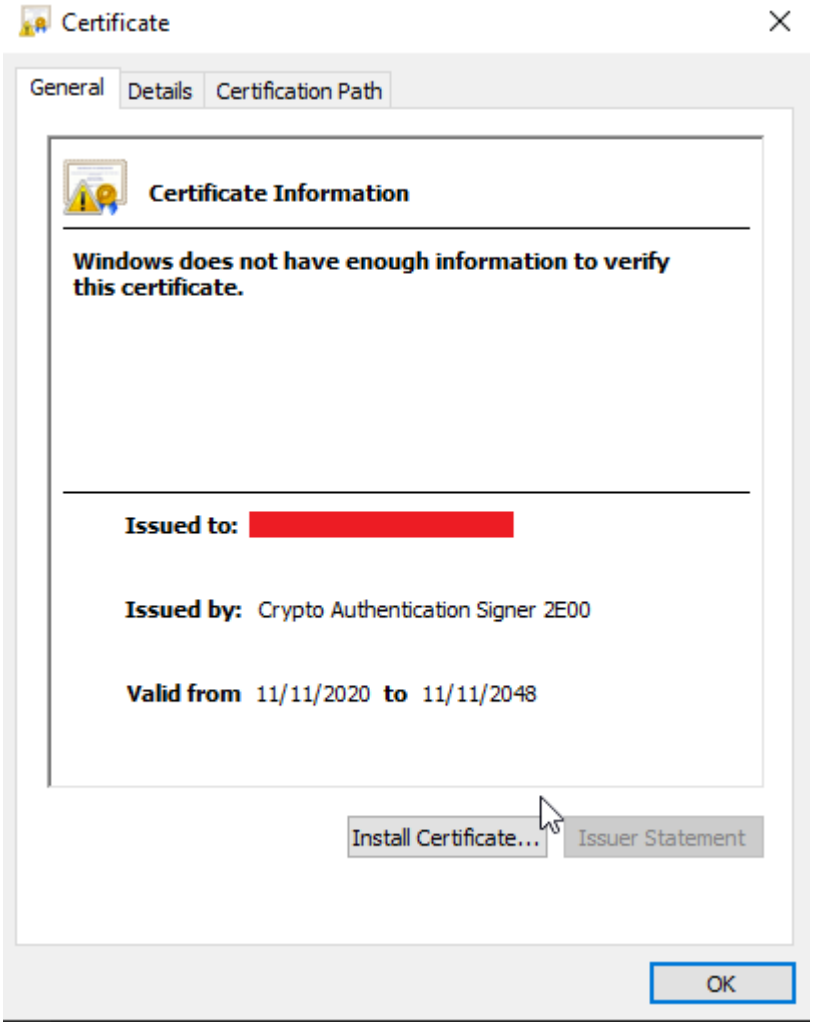
3. Click on “Add Device”.



4. Create the device with relevant configuration.



5. The Device ID is the id that is given as “Issued To” when you open the device certificate. If one double clicks on the device certificate, one can see the Device Id:



   In the MSD enumerated when the Curiosity Board is plugged in, you can find a “`.cer`” file with an alphanumeric name. Select this file when prompted to select a certificate.
6. Authentication type needs to “X.509 Self-Signed”.
7. Primary and Secondary Thumbprints will be same, and one can generate it by using the following openssl command:
   “openssl x509 -in device1.crt -noout -fingerprint”

   Note: The thumbprint generated by the above command contains ‘:’ which need to be removed before setting the thumbprint in the Azure Portal.
8. “Connect this device to an IoT hub” should be “Enable”.
9. Click “Save”.
10. The device would have been added to the Azure portal after this and it can be found in the list of devices displayed after clicking on the “Devices” in the left column of the web page.