

**Activity** : Node-RED Dashboard for AWS IoT Core

**Goal** : Place the data coming from AWS IoT Core onto a Node-RED Dashboard

# Data coming from AWS IoT Core

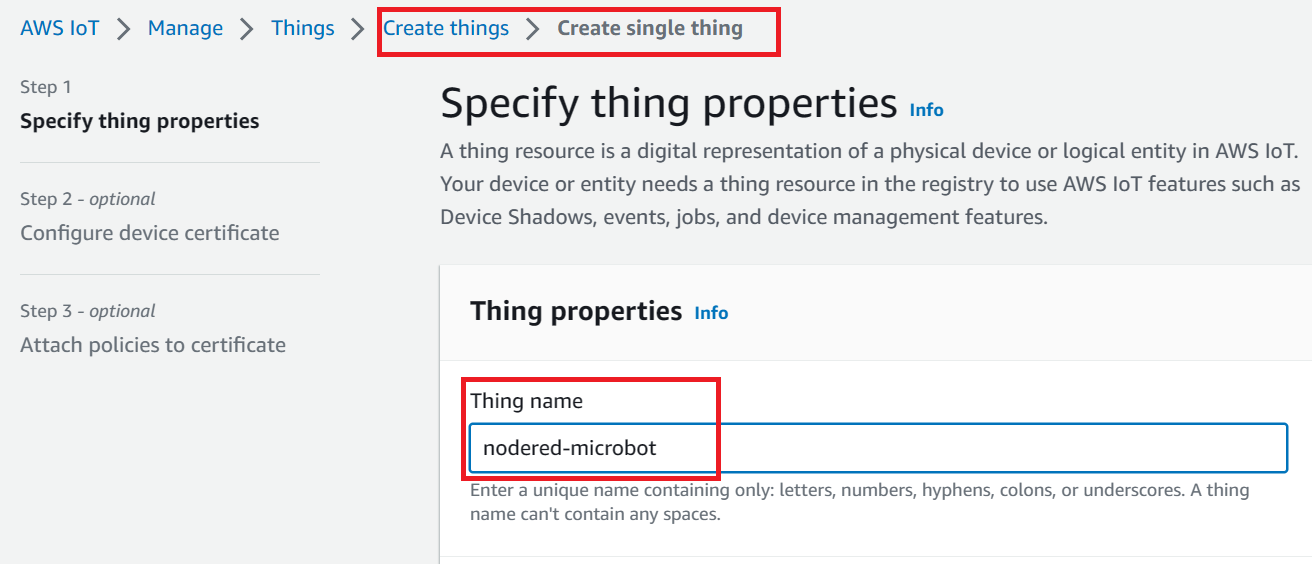
Topic: espeye/count

Message:

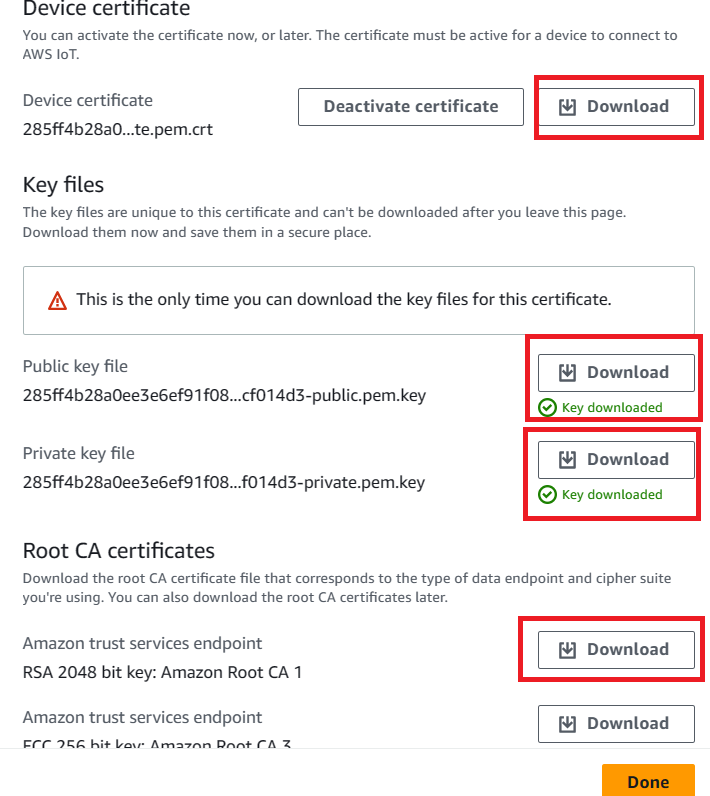


# Node-RED is a “thing” from the view of AWS IoT Core

On AWS IoT management console, create a “thing”, as shown below.

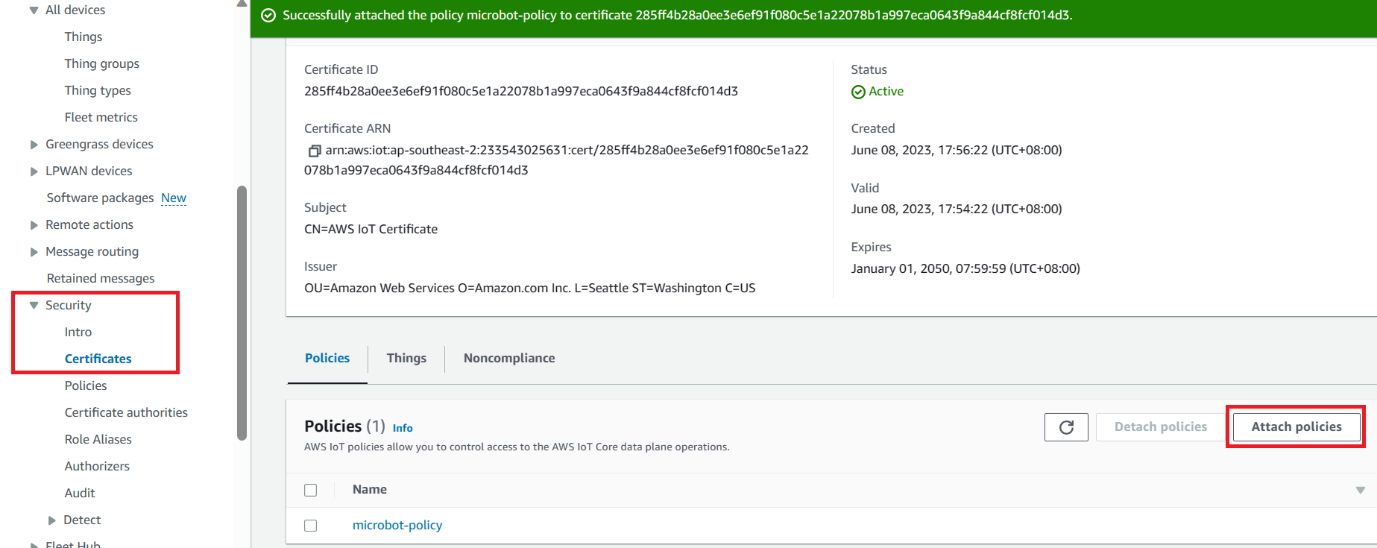


Choose the option to auto-generate a new device certificate. Then download all the four files, as shown below.



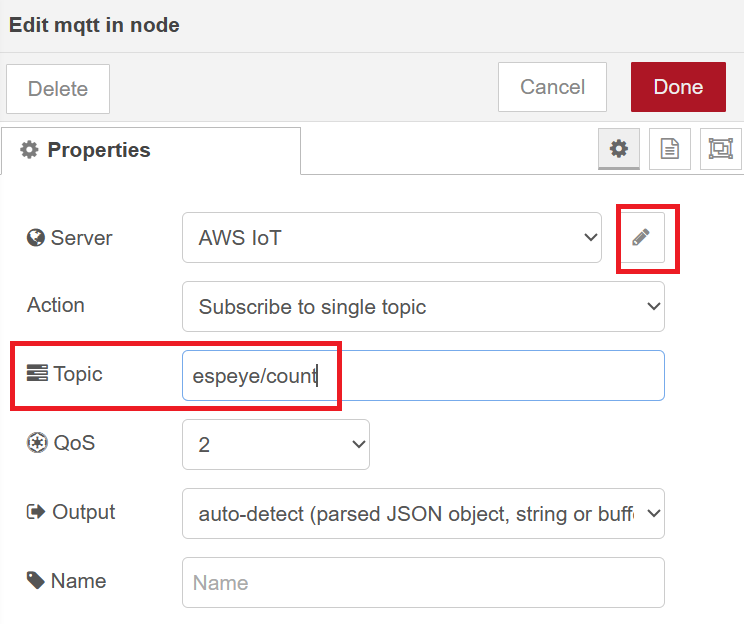
## Attach Policy to the “thing”

Attach the micorbot-policy to the “thing”.



# Configure MQTT IN node

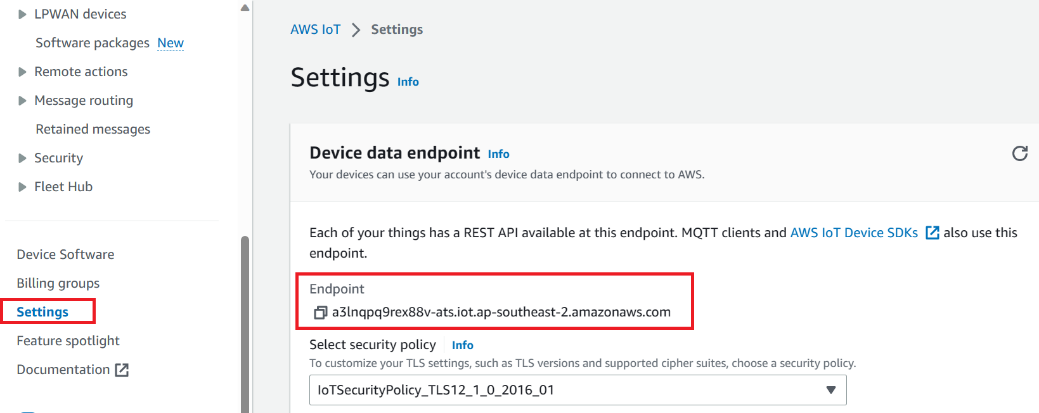
On Node-Red, enter the MQTT topic that is to be subscribed into the MQTT IN’s wizard.



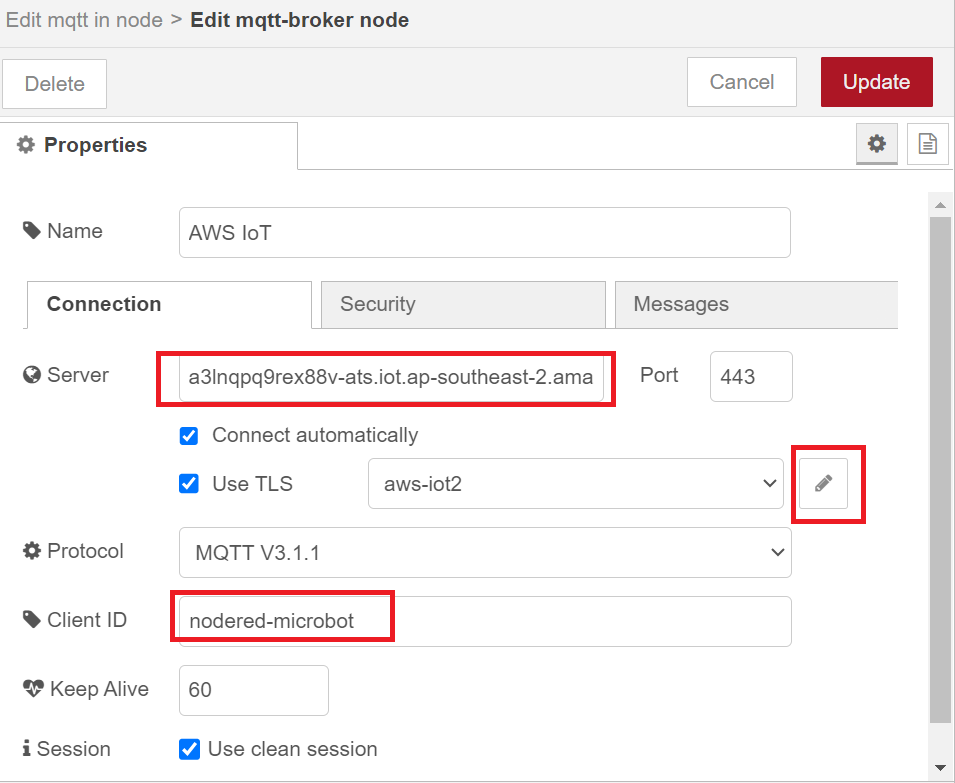
Then click on the edit icon to specify the MQTT Server.

## MQTT Server

On AWS IoT Management Console, copy the “endpoint” from the Setting section, as shown below.

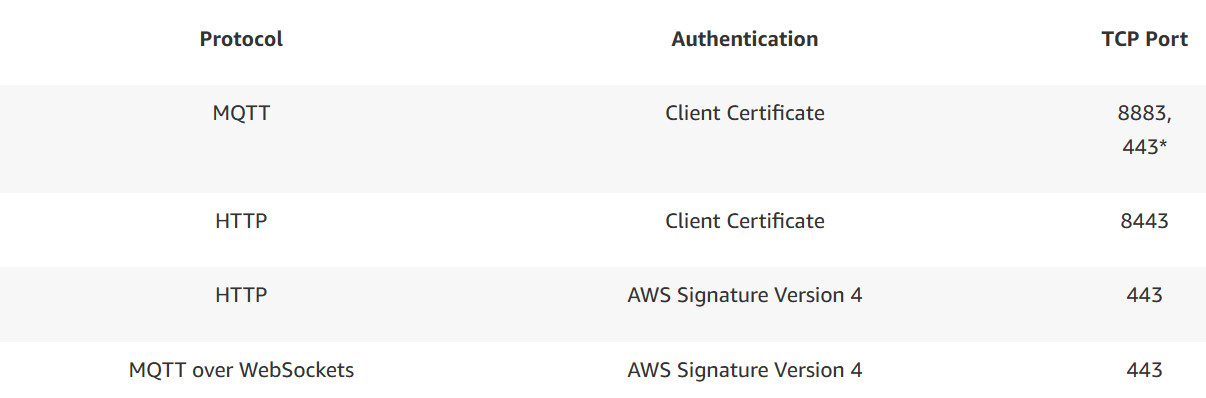


Insert the URL (endpoint) into the MQTT In’s wizard as shown below.



Use the client ID of the “thing” you had earlier specified for Node-RED on AWS IoT Management console.

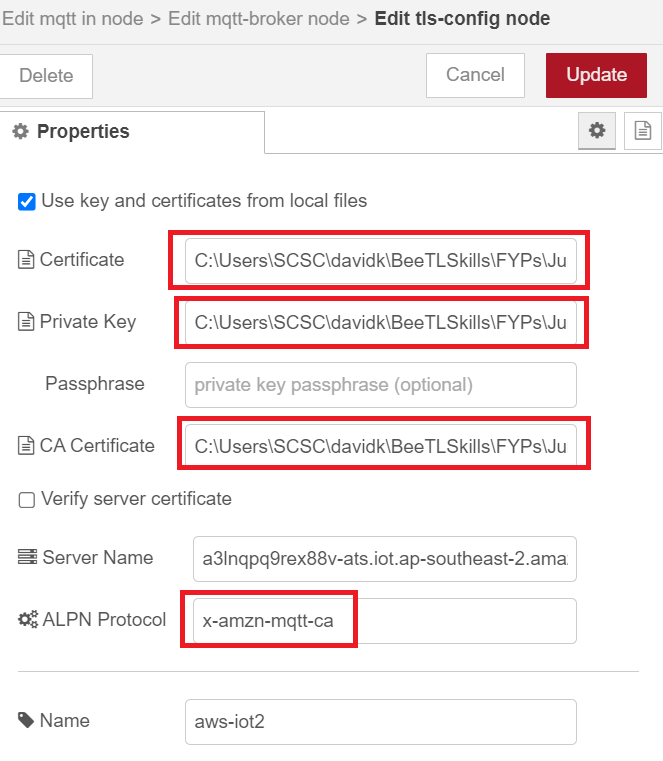
## Port



Using MQTT with client certificate authentication on port 443 requires the use of the ALPN TLS extension.

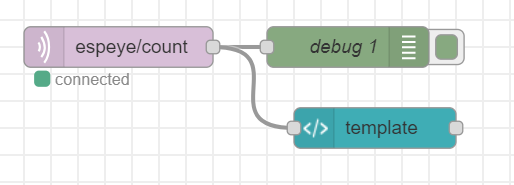
## Certificates

Click on the edit icon for “Use TLS” and a new wizard as shown below will appear. The FULL paths of the certificates and keys must be entered into the wizard. No spacing should be used in the paths.



The ALPN protocol should be as shown above.

# Node-RED Flow



If the green “connected” square does not appear when the flow is deployed, look for the debug messages for clue. If there is no clue there, it could be that there is no policy attached to the “thing” yet.

## Template node



## Dashboard

