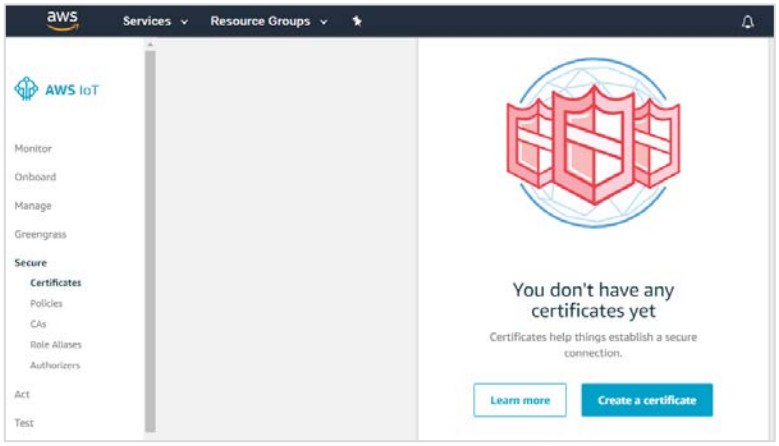
Technical Note

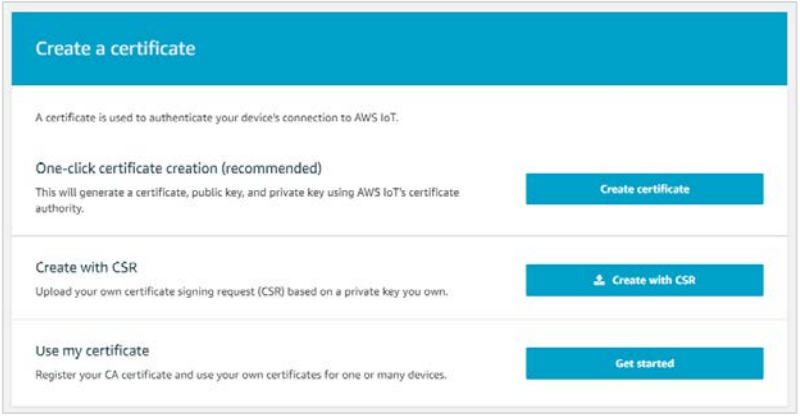
Connecting an IoT Gateway MQTT Client Agent to AWS IoT Platform

1. One-Click Certificate Creation (Recommended)

1. Log into the Amazon Web Services (AWS) IoT Platform.
2. Navigate to **Services | IoT Core.**
3. Select **Secure | Certificates** from the vertical navigation bar on the left side of the IoT Core landing page.
   a. Choose **Create a certificate**.

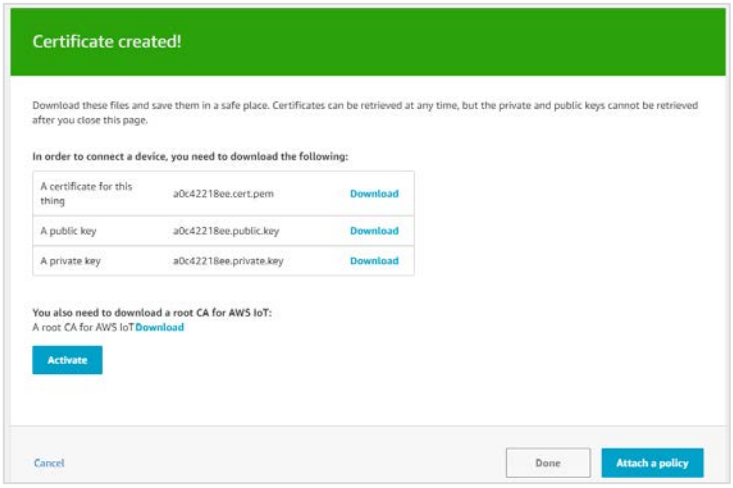


b. Choose **Create Certificate** under **One-Click Certificate Creation** (recommended).



4. Once created, download the thing certificate and private key. By default, AWS signs each certificate with a Symantec root certificate trusted by Windows. There is no need to get the root certificate in most cases.

Caution: This is the only chance to download the private key. It is inaccessible after creation.



5. Choose **Activate** to enable the new certificate.
6. Choose **Attach a Policy.**
7. Select an existing policy that enables `iot:connect`, `iot:receive`, `iot:publish`, and `iot:subscribe` or choose **Create a New Policy** and supply these actions.

Tip: Use * to supply all actions.

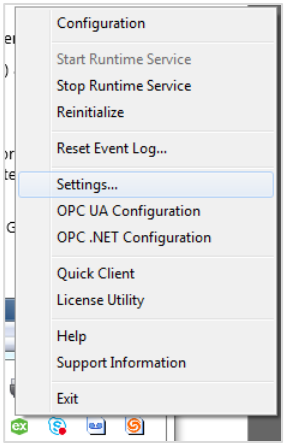
2. Using Custom CAT

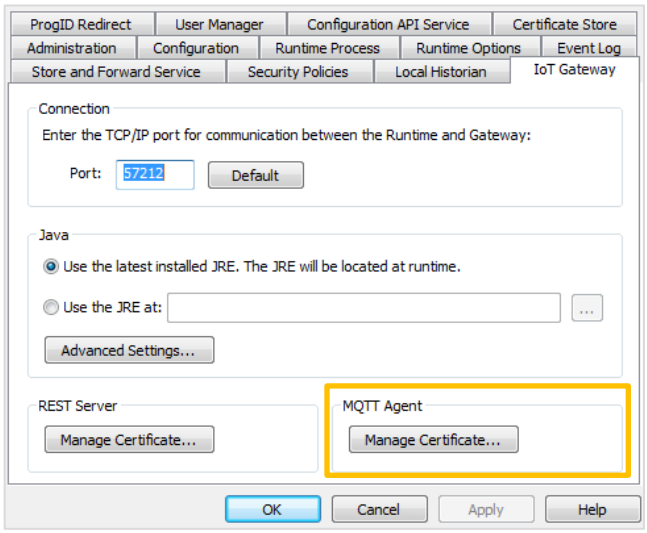
Caution: OPENSSL is required to perform the steps in this section.

1. Log into the AWS IoT Platform.
2. Navigate to **Secure | Certificates**.
3. Choose **Create**.
4. Choose **Get Started** next to Use My Certificate.
5. Choose **Register CA** and follow the instructions to import a CA certificate.
6. Select **Register Certificates**.
7. Browse for the imported certificate signed by the CA.
8. Return to the main console and choose **Secure | Certificates**.
9. Click **Browse (...)** for the newly registered certificate and choose **Activate**.
10. Select **Attach Policy**.
11. Choose an existing policy or create a new one (*see* *One-Click Certificate Creation (Reccommended)*).
12. Import the client certificate and private key into KEPServerEX® (*see* *Importing a Client Certificate into KEPServerEX*).

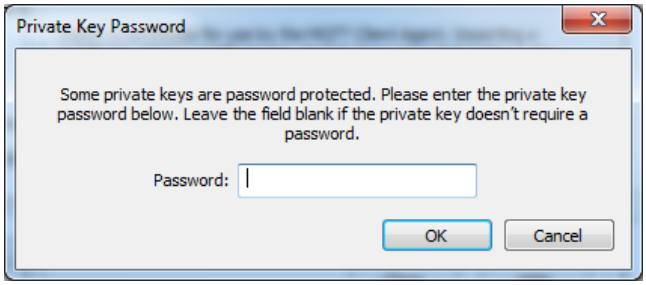
3. Importing a Client Certificate into KEPServerEX

1. Right click the KEPServerEX Administration icon and select **Settings...**.
2. Navigate to the **IoT Gateway** tab.
3. Click **Manage Certificate...** within the MQTT Agent area.



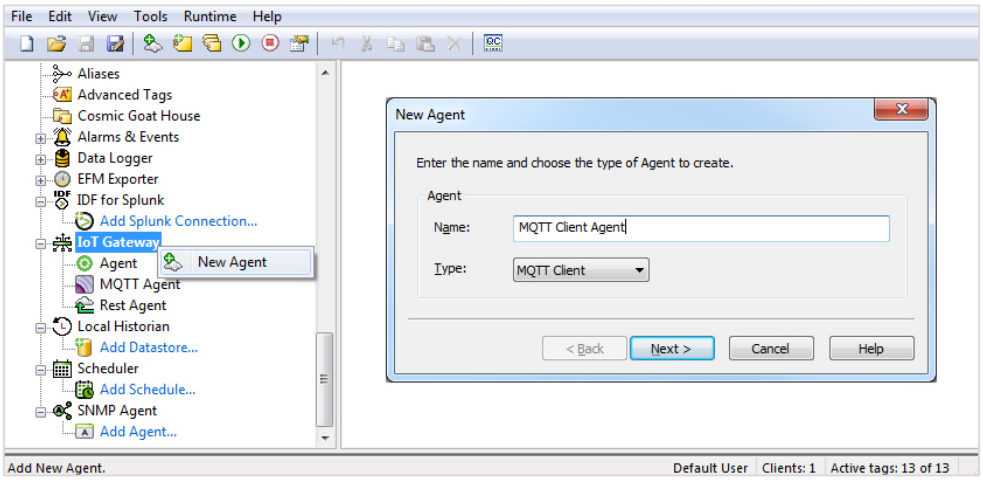


4. Click **Import New Certificate** and browse to open the thing certificate (`xxx.pem.crt`).
5. An Import dialogue will immediately open and prompt to import the private key. Browse to open the private key (`xxx.pem.key`).
6. A popup requesting a private key password will display. No password is needed for the private key provided by AWS IoT. It is permissible to click OK without completing the Password field.

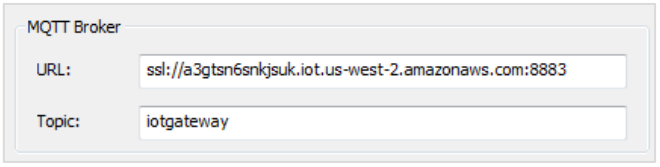


Note: The files required for this step depend on the format and contents of the file(s) being imported. For example, when a PFX file is imported, no additional files are required because it contains both the certificate and private key. AWS IoT and its One-click Certificate creation process creates both a xxx.pem.crt and xxx.pem.key file and both need to be imported independently (*as outlined in steps 4-6*).

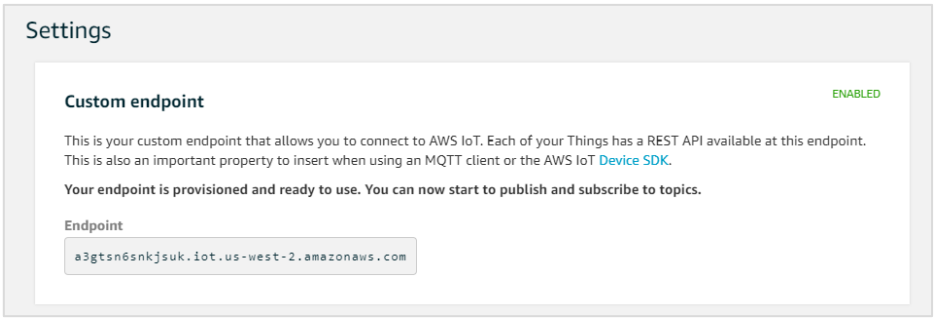
7. In the KEPServerEX Configuration tree view, navigate to the IoT Gateway Plug-In node.
8. Create a new MQTT Client Agent.



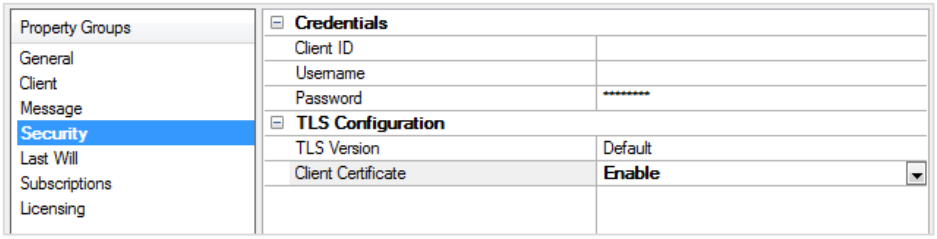
9. When prompted to enter the MQTT broker's URL, define the AWS MQTT URL in the format of `ssl://<Endpoint>:8883`.



Tip: Configure the <Endpoint> section of the URL exactly as shown in AWS's IoT Core page under **Settings**.



10. Open the new MQTT Client Agent properties and select the **Security** property group.
11. Under TLS Configuration, enable **Client Certificate** by selecting Enable from the drop-down menu.



12. Add at least one tag to the MQTT Client Agent to cause the agent to solicit a connection with AWS and begin publishing data related to the new tag.
13. Review the KEPServerEX event log for a message from the MQTT Client Agent to verify a successful connection.