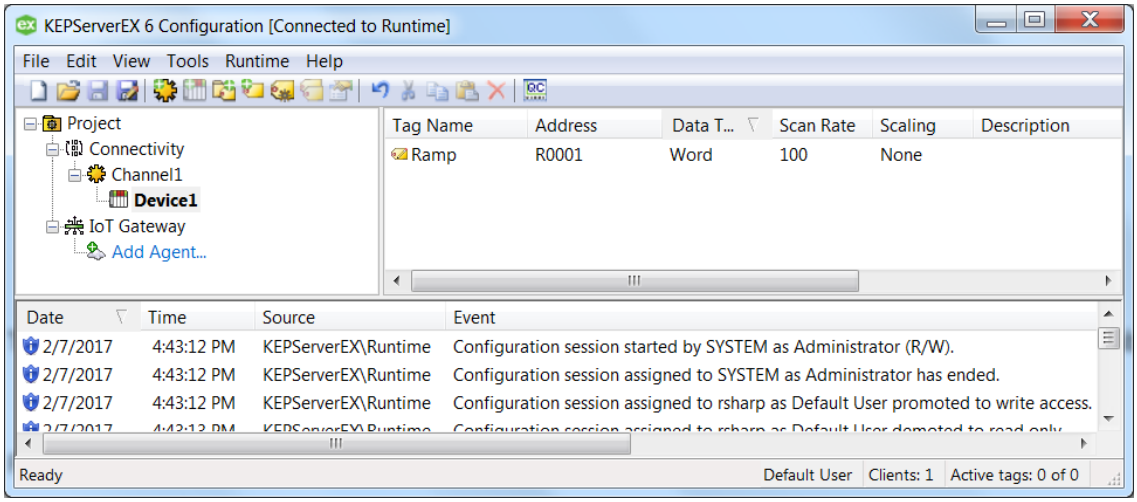
Technical Note

MQTT Client and Microsoft Azure IoT

This document is intended to help you connect our MQTT client to a Microsoft Azure IoT hub.

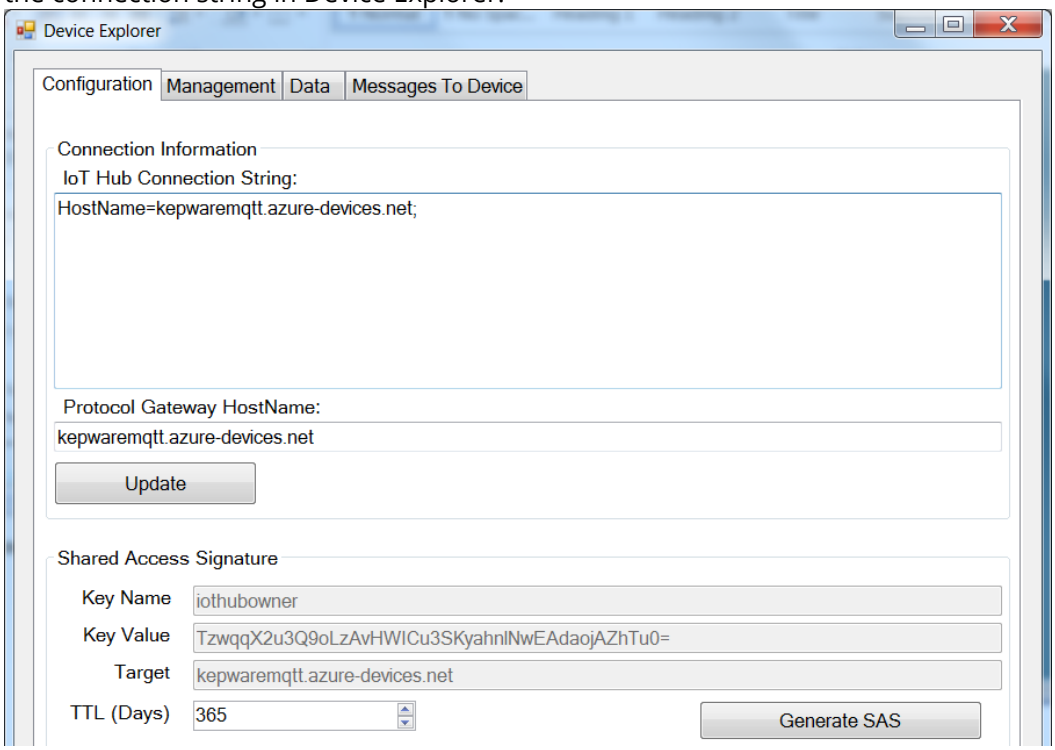
1. Connecting MQTT client to Azure

1. Open a KEPServerEX® instance with the IoT Gateway advanced plug-in. In this example, one channel and device are configured with the Simulator driver, and there is one tag that ramps up on scan.

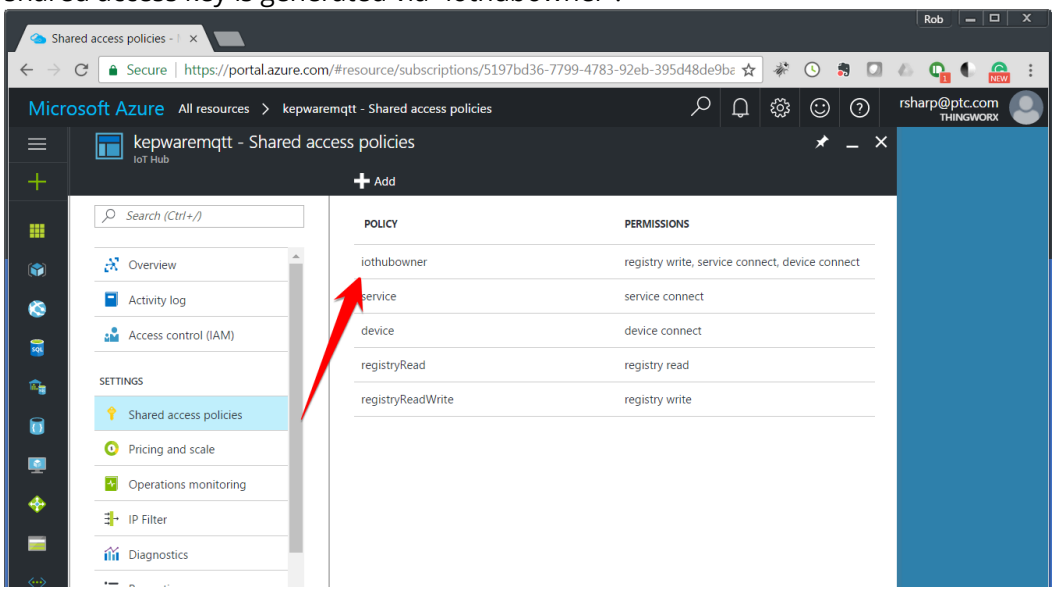


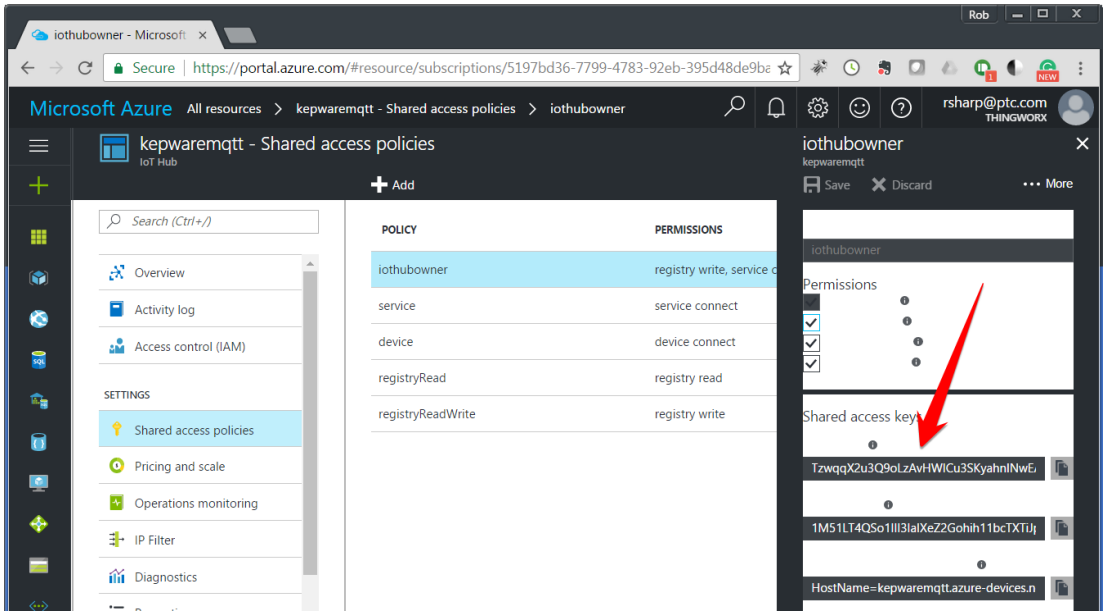
2. Access a Microsoft Azure instance.
3. The third piece of software required is a tool from Microsoft called Device Explorer, which is available to download from https://github.com/Azure/azure-iot-sdk-csharp/tree/master/tools/DeviceExplorer
4. Create an IoT hub in the Azure instance. Assign a unique name and a resource group.

5. Acquire the host name once the hub is created. This hostname is the first part of the connection string in Device Explorer.

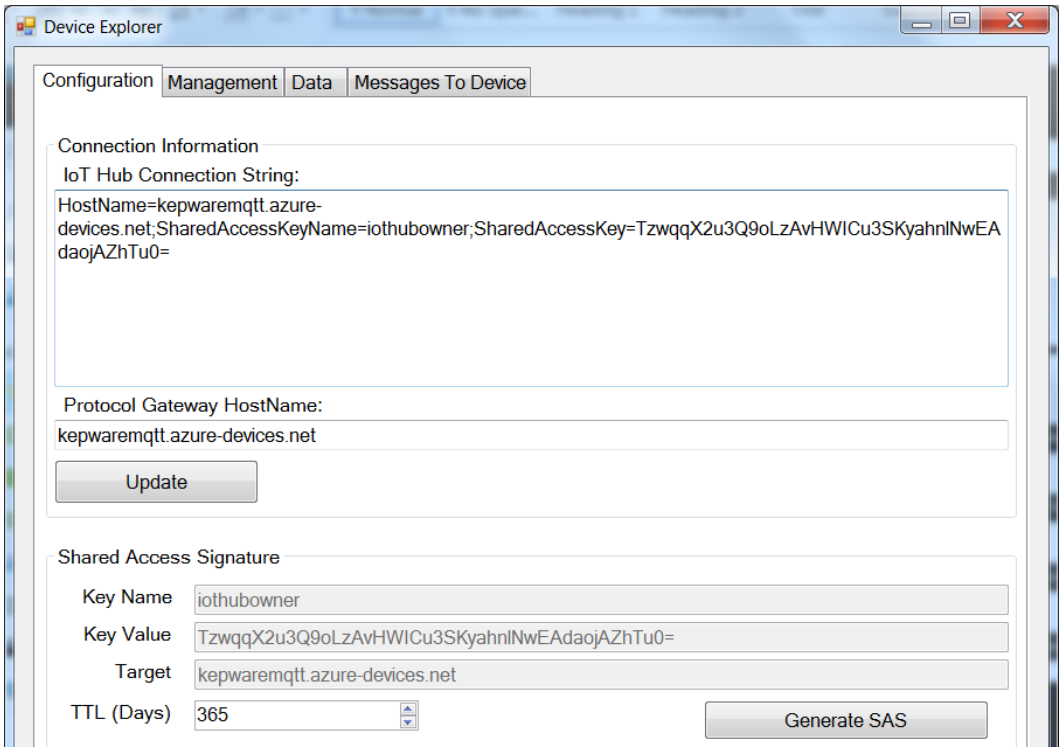


6. Click **Shared Access policies** under Settings in the IoT hub. In this example, a shared access key is generated via "iothubowner".

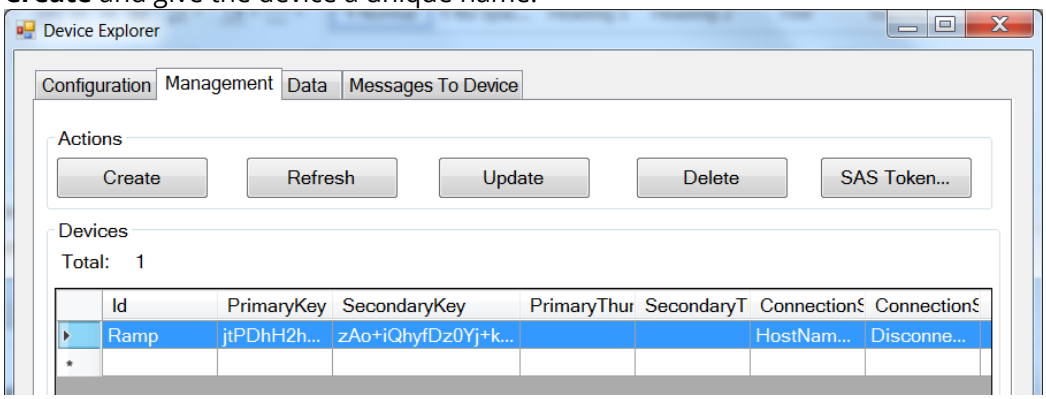




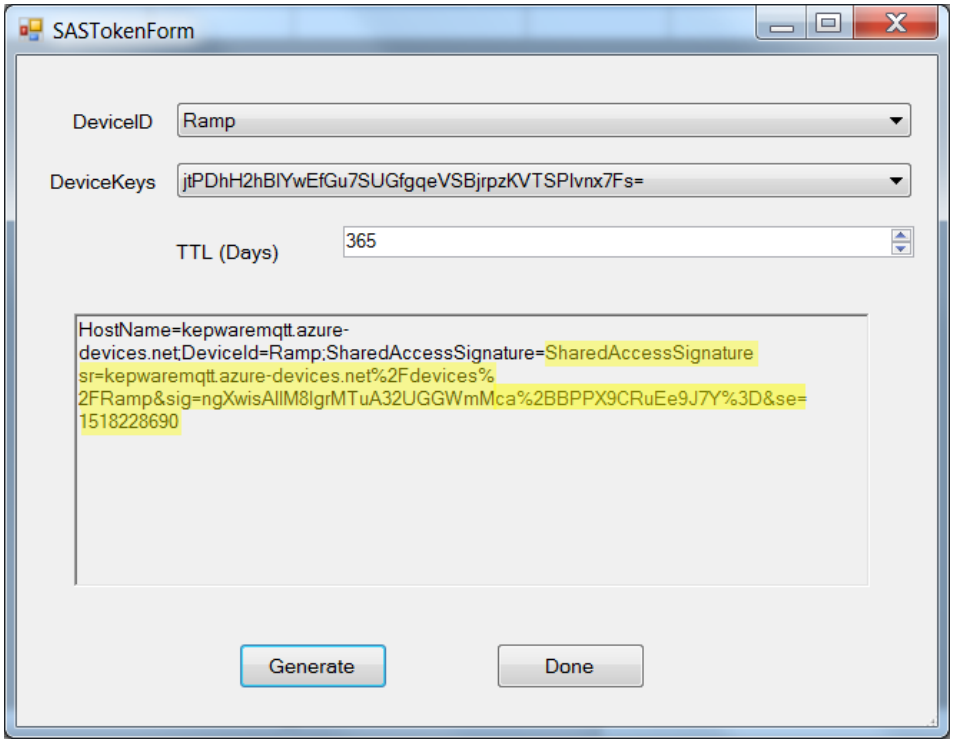
7. Both Azure and Device Explorer indicate that the connection string is "HostName=kepwaremqtt.azure-devices.net;SharedAccessKeyName=iothubowner;SharedAccessKey=TzwqqX2u3Q9oLzAvHWICu3SKyahnlNwEAdaojAZhTu0="



8. In Device Explorer, create a device by accessing the **Management** tab. Click **Create** and give the device a unique name.



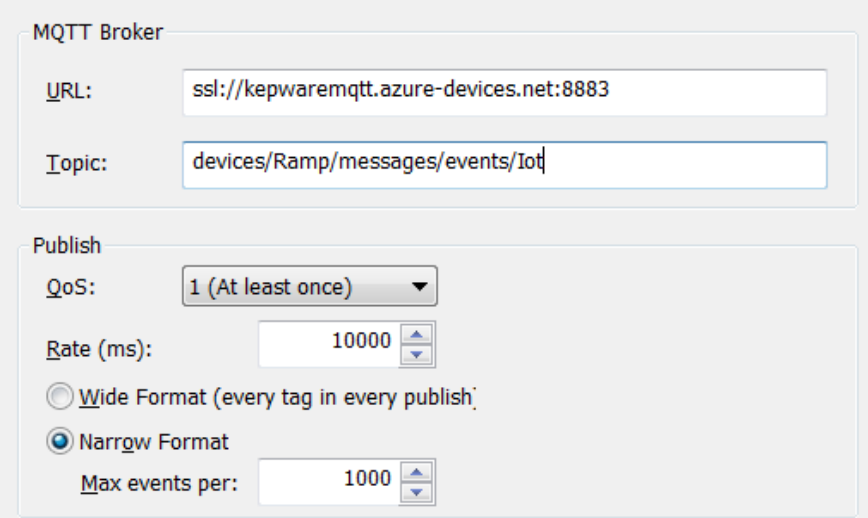
9. Click **SAS Token...** to generate the SAS token in Device Explorer. Part of the string from this dialog needs to be copied (starting with the second "SharedAccess"). This example will copy the highlighted text.



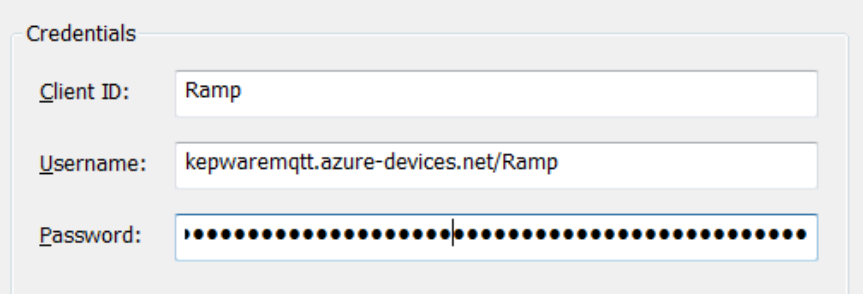
10. In the KEPServerEX add an IOT agent. Use the following formats for the indicated properties:

    a. URL format: ssl://**HostName**:8883

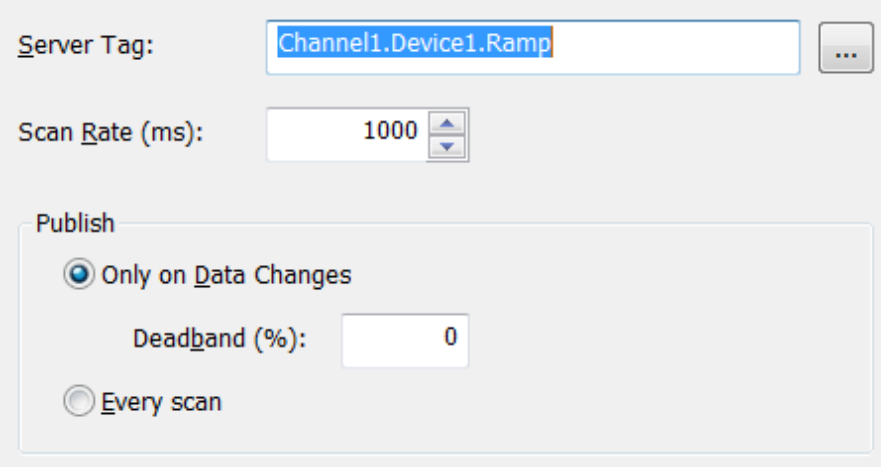
    b. Topic format: devices/**deviceID**/messages/events/topic



11. Create security credentials. The expected formats are as follows:
    a. Client ID: **deviceID**
    b. Username: **HostName/deviceID**
    c. Password: **SAS Key** (See highlighted text in #9.)



12. Next, add an IoT item.



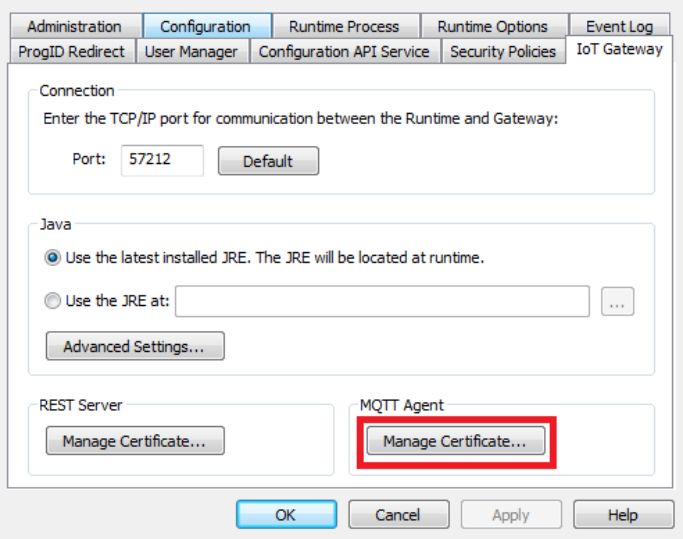
13. Verify that the resulting event log is similar to the following:

Date	Time	Level	Source	Event
2/10/2017	2:41:35 PM	Information	KEPServerEX\Runtime	MQTT agent 'Ramp_2_Cloud' is connected to broker 'ssl://kepwaremqtt.azure-devices.net:8883'

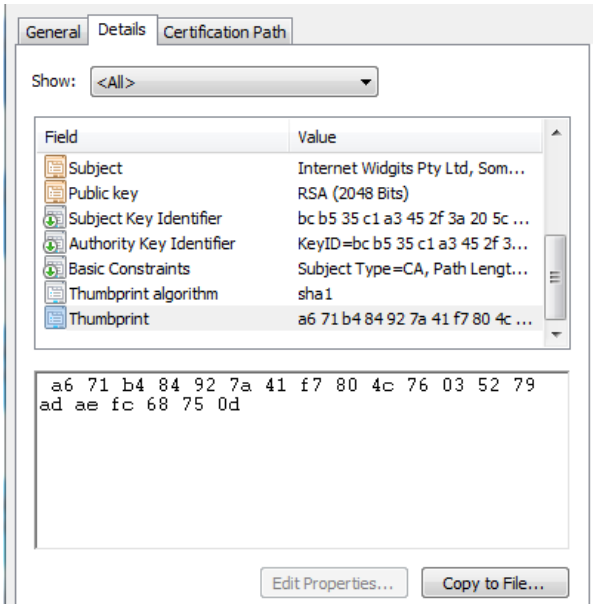
2. Connecting with self-signed X.509 Certificates

Microsoft Azure IoT Hub also supports self-signed certificates for authorization, which keeps a certificate and private key on the local machine and stores only a certificate thumbprint on the hub. For more information on how to connect with self-signed certificates, refer to https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-security. The following information describes how to connect IoT Gateway to the hub:

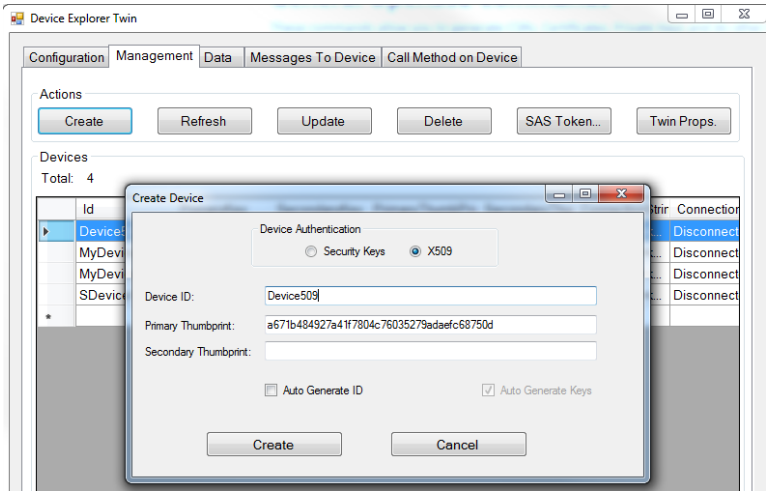
1. Generate self-signed certificates. The output of this command will be a new generated certificate and private key:
   $ openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt
2. To import the certificate and private key to IoT Gateway, right click Server Admin and select Settings. Access the IoT Gateway tab, then click **Manage Certificate...** .



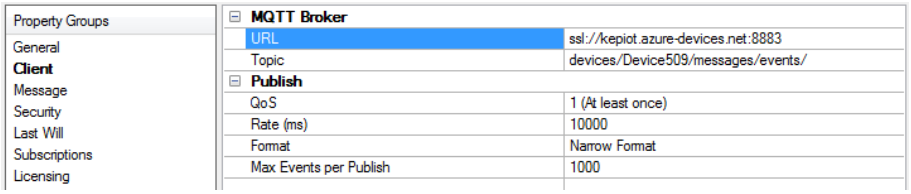
3. Obtain the certificate thumbprint by doing the following:
   a. Click **View Certificate**.
   b. Access the **Details** tab, and from the drop-down menu, select **<All>**.
   c. Select Thumbprint and copy the string.



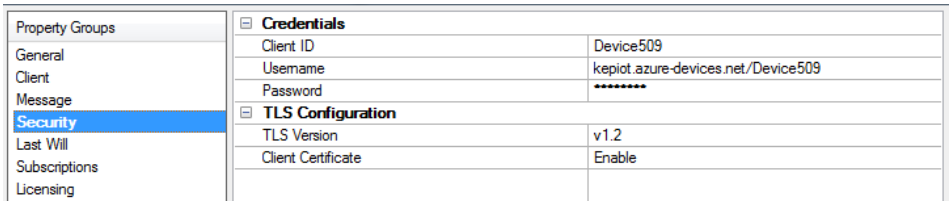
4. Create device using Device Explorer.
    a. Open Device Explorer, access the **Management** tab, and select **Create**.
    b. Select the **X509** option.
    c. Enter **Device ID** and paste the string into the **Primary Thumbprint** field.
    d. Click **Create**.



5. Create new MQTT Agent. The following property groups should be configured per the guidelines below:
    a. Client
        i. URL: "ssl://**Azure IoT Hub Host name**:8883".
        ii. Topic: "devices/**Device ID**/messages/events/".



    b. Security
        i. Client ID: **Device ID**
        ii. Username: "**Azure IoT Hub Host name/Device ID**"
        iii. Password: "HostName= **Azure IoT Hub Host name**; **DeviceID** = **Device ID**;x509=true"
        iv. TLS Version: v1.2
        v. Client Certificate: Enable



6. Add tags to MQTT Agent. Event log messages will indicate if the agent was successfully connected to the broker.

7. To monitor messages from IoT Gateway, open Device Explorer and access the **Data** tab. Select the device from the drop-down menu and click **Monitor**.