

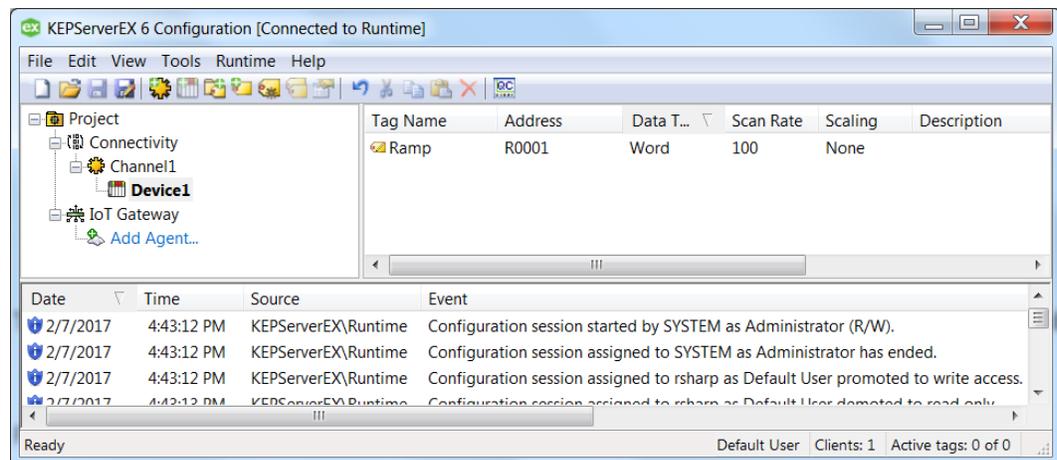
Technical Note

MQTT Client and Microsoft Azure IoT

This document facilitates connecting an MQTT client to a Microsoft Azure IoT hub.

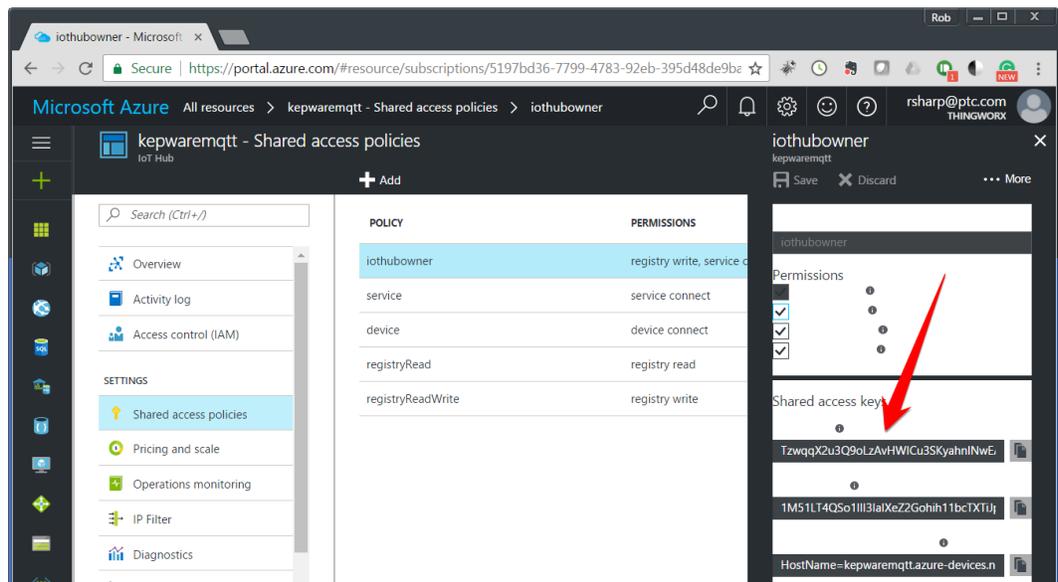
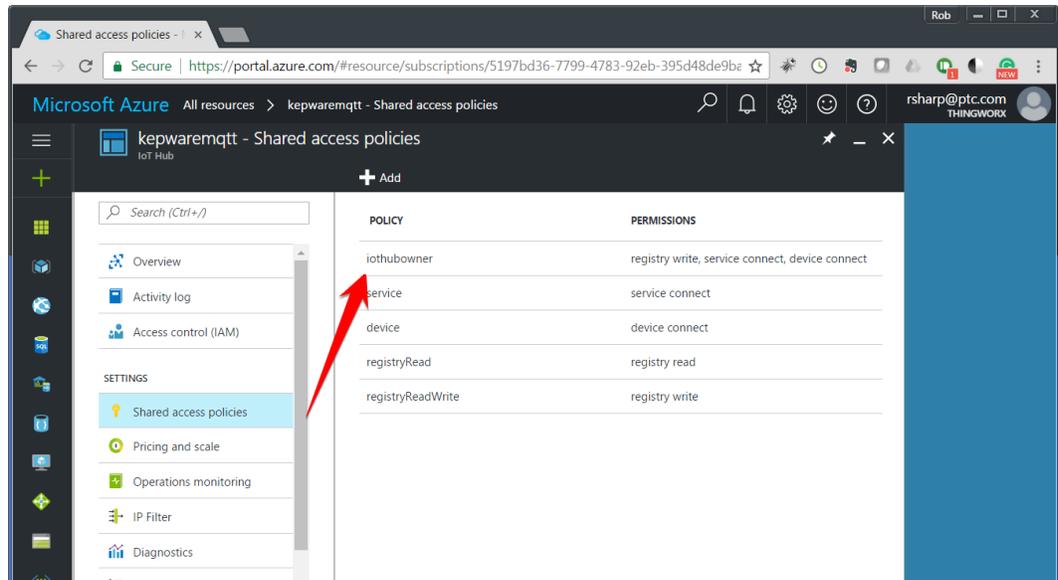
1. Connecting MQTT Client to Azure

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. Click **Shared access policies** under Settings in the IoT hub. In this example, a shared access key is generated via “iothubowner”. The text string presented for ‘iothubowner’ user includes both the Shared Access Key and the Hostname URL. Copy this string and place it into the “IoT Hub Connection String” field within the Device Explorer application downloaded in a previous step.



Configuration Management Data Messages To Device

Connection Information

IoT Hub Connection String:

HostName=kepwaremqtt.azure-devices.net;SharedAccessKeyName=iotechowner;SharedAccessKey=TzwqqX2u3Q9oLzAvHWICu3SKyahnlNwEAdaojAZhTu0=

Protocol Gateway HostName:

kepwaremqtt.azure-devices.net

Update

Shared Access Signature

Key Name: iotechowner

Key Value: TzwqqX2u3Q9oLzAvHWICu3SKyahnlNwEAdaojAZhTu0=

Target: kepwaremqtt.azure-devices.net

TTL (Days): 365

Generate SAS

- In Device Explorer, click on "Update", and then create a device by accessing the **Management** tab. Click **Create** and give the device a unique name.

Configuration Management Data Messages To Device

Actions

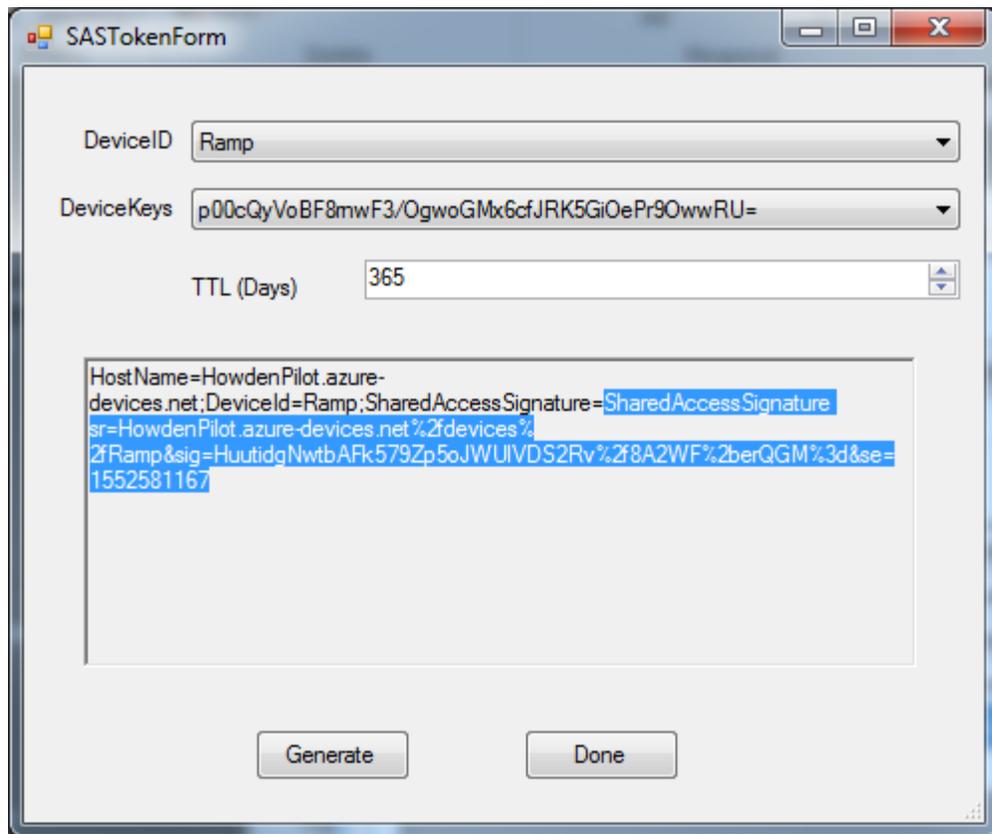
Create Refresh Update Delete SAS Token...

Devices

Total: 1

	Id	PrimaryKey	SecondaryKey	PrimaryThur	SecondaryT	ConnectionS	ConnectionS
▶	Ramp	jtPDhH2h...	zAo+iQhyfDz0Yj+k...			HostNam...	Disconne...
*							

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



8. In 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`

Property Groups	<input checked="" type="checkbox"/> MQTT Broker	
General	URL	ssl://kepwaremqtt.azure-devices.net:8883
Client	Topic	devices/Ramp/messages/events/
Message	<input checked="" type="checkbox"/> Publish	
Security	QoS	1 (At least once)
Last Will	Rate (ms)	10000
Subscriptions	Format	Narrow Format
Licensing	Max Events per Publish	1000
	Transaction timeout in (s)	5

9. Create security credentials. The expected formats are as follows:
 - a. Client ID: **deviceID**
 - b. Username: **HostName/deviceID**
 - c. Password: **SAS Key**

Property Groups	<input checked="" type="checkbox"/> Credentials	
General	Client ID	Keppure
Client	Username	kepwaremqtt.azure-devices.net/Ramp
Message	Password	*****
Security	<input checked="" type="checkbox"/> TLS Configuration	
Last Will	TLS Version	Default
Subscriptions	Client Certificate	Disable
Licensing		

- Next, add an IoT item.

- Verify that the resulting event log is similar to the following:

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

2. Connecting with self-signed X.509 Certificates

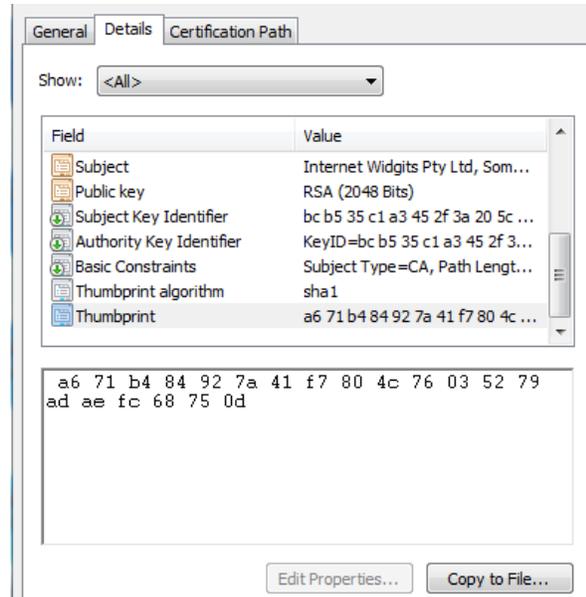
Microsoft Azure IoT Hub also supports self-signed certificates for authorization, which keeps a certificate and private key on the local machine and stores only a certificate thumbprint on the hub. For more information on how to connect with self-signed certificates, refer to <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-security>.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

- Generate self-signed certificates.
The output of this command will be a new generated certificate and private key:

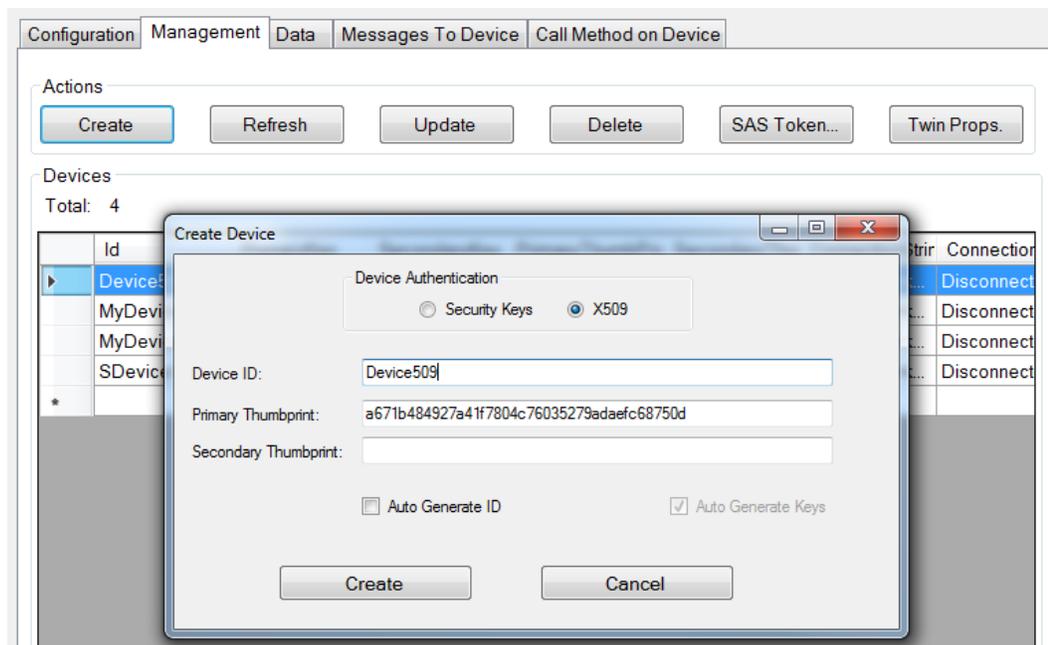
```
$ openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt
```
- To import the certificate and private key to IoT Gateway, right click Server Admin and select Settings. Access the IoT Gateway tab, then click **Manage Certificate...**

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 the 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/".

Property Groups	MQTT Broker	
General	URL	ssl://kepiot.azure-devices.net:8883
Client	Topic	devices/Device509/messages/events/
Message	Publish	
Security	QoS	1 (At least once)
Last Will	Rate (ms)	10000
Subscriptions	Format	Narrow Format
Licensing	Max Events per Publish	1000

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

Property Groups	Credentials	
General	Client ID	Device509
Client	Username	kepiot.azure-devices.net/Device509
Message	Password	*****
Security	TLS Configuration	
Last Will	TLS Version	v1.2
Subscriptions	Client Certificate	Enable
Licensing		

- 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.
- 8. Select the device from the drop-down menu and click **Monitor**.

