



Connectivity Guide

Connect Kepware Server to Ali IoT

November, 2025
Ref. 1.02

1. Overview

This document explores how to configure an MQTT Client Agent within the IoT Gateway Plug-In to send data to Ali IoT. The connection can be made using MQTT over Transmission Control Protocol (TCP) and MQTT over Transport Layer Security (TLS).

- **Note:** Before connecting to Ali IoT via MQTT, ensure appropriate Ali IoT product and device configuration, getting ProductKey, DeviceName, DeviceSecret, and root CA certificate ready. Find this information on the console page of the website:
<https://iot.console.aliyun.com>.

2. Configure the Agent for MQTT over TCP

1. Launch Kepware Server and use the left panel to locate the IoT Gateway Plug-In.
2. Located and select the MQTT Client Agent.
3. Right-click and select **Create....**
4. Set the following parameters:
 - a. MQTT Broker URL has the format of `tcp://${YourProductKey}.iot-as-mqtt.${region}.aliyuncs.com:1883`
 - b. MQTT Broker Topic has the format of `/${YourProductKey}/${YourDeviceName}/${CustomizedString}`

Property Editor - IoT Gateway.Aliyun

Property Groups	
General	
Client	
Message	
Security	
Last Will	
Subscriptions	
Licensing	
MQTT Broker	
URL	<code>tcp://Xlabolgxcq.iot-as-mqtt.cn-shanghai.aliyuncs.com:1883</code>
Topic	<code>/Xlabolgxcq/Shanghai/iotgateway</code>
Publish	
QoS	1 (At least once)
Rate (ms)	10000
Format	Narrow Format
Max Events per Publish	1000
Transaction timeout in (s)	5

- c. Inside Credentials, specify Client ID in the format of `${clientId} |securemode=3,signmethod=hmacsha1 |` for TCP Connection
 `${clientId} |securemode=2,signmethod=hmacsha1 |` for TLS Connection
● **Tip:** {clientId} is customizable, but "Kepware" is used in this guide.
- d. For inside credentials, specify user name in the format of `${YourDeviceName}&${YourProductKey}`

Property Groups	
General	
Client	
Message	
Security	
Last Will	
Subscriptions	
Licensing	
Credentials	
Client ID	<code>Kepware securemode=3,signmethod=hmacsha1 </code>
Username	<code>Shanghai&Xlabolgxcq</code>
Password	*****
TLS Configuration	
TLS Version	v1.2
Client Certificate	Disable

e. For inside credentials, the password must be calculated by HMACSHA1 algorithm.

● **Note:** Ali IoT provides a tool to generate a password. The same password can be used for the TCP and TLS connections.

productKey:	<input type="text" value="XXXXXXXXXX"/>
deviceName:	<input type="text" value="Shanghai"/>
deviceSecret:	<input type="text" value="XXXXXXXXXXXXXXXXXXXXXX"/>
timestamp:	<input type="text"/>
clientId:	<input type="text" value="Kepware"/>
method:	<input style="width: 100px; height: 20px; border: 1px solid black; border-radius: 5px; padding: 2px 10px;" type="text" value="hmacsha1"/>
password:	<input style="width: 150px; height: 20px; border: 1px solid black; border-radius: 5px; padding: 2px 10px; margin-left: 10px;" type="text"/>
<input style="border: 1px solid black; border-radius: 5px; padding: 2px 10px;" type="button" value="Generate"/>	
password:	<input style="width: 150px; height: 20px; border: 1px solid black; border-radius: 5px; padding: 2px 10px; margin-left: 10px;" type="text" value="XXXXXXXXXXXXXXXXXXXXXX"/>

5. Set and Enable this MQTT Client Agent.

6. Verify it displays as connecting to Ali IoT.

Date	Time	Source	Event
2020/6/16	7:34:57	KEPServerEX\Runtime	MQTT agent 'Ali_IoT_TCP' is connected to broker 'tcp://Xlabolgxcq.1ot-as-mqtt.cn-shanghai.aliyuncs.com:1883'

7. Verify data is received in Ali IoT.

MessageID	1272673999763293185 复制
Topic	/Xlabolgxcq/Shanghai/iotgateway
时间	2020/06/16 07:35:01.340
内容	<div style="display: flex; align-items: center;"> Text (UTF-8) ▼ <div style="flex-grow: 1;"> <pre>{"timestamp":1592264101518,"values": [{"id":"Simulator.Device.Temperature","v":20,"q":true,"t":1592264085613}, {"id":"Simulator.Device.Temperature","v":31.125,"q":true,"t":1592264086619}, {"id":"Simulator.Device.Temperature","v":21.5,"q":true,"t":1592264087618}, {"id":"Simulator.Device.Temperature","v":21.125,"q":true,"t":1592264088613}, {"id":"Simulator.Device.Temperature","v":29.125,"q":true,"t":1592264089615}, {"id":"Simulator.Device.Setpoint","v":0,"q":true,"t":1592264085613}, {"id":"Simulator.Device.Humidity","v":40,"q":true,"t":1592264085613}, {"id":"Simulator.Device.Humidity","v":55.1666679,"q":true,"t":1592264086619}, {"id":"Simulator.Device.Humidity","v":45,"q":true,"t":1592264087618}, {"id":"Simulator.Device.Humidity","v":42.1666679,"a":true,"t":1592264088613}] }</pre> </div> </div>

3. Configure MQTT Over TLS (Optional)

8. Install the root CA Certificate from Ali IoT on the host operating system.
9. Change the broker URL in the client property group of the MQTT Client Agent to reflect the use of SSL (replace "tcp://" with "ssl://").

Property Groups	
General	
Client	
Message	
Security	
Last Will	
Subscriptions	
Licensing	
MQTT Broker	
URL	ssl://Xlabolgxcq.iot-as-mqtt.cn-shanghai.aliyuncs.com:1883
Topic	/Xlabolgxcq/Shanghai/iotgateway
Publish	
QoS	1 (At least once)
Rate (ms)	10000
Format	Narrow Format
Max Events per Publish	1000
Transaction timeout in (s)	5

10. Change the TLS version in the security property group to **v1.2**.

Property Groups				
General				
Client				
Message				
Security				
Last Will				
Subscriptions				
Licensing				
Credentials				
Client ID	Kepware securemode=2,signmethod=hmacsha1			
Username	Shanghai&Xlabolgxcq			
Password	*****			
TLS Configuration				
TLS Version	v1.2			
Client Certificate	Disable			
Date	/	Time	Source	Event
① 2020/6/16	7:39:43		KEPServerEX\Runtime	MQTT agent 'Ali_IoT_SSL' is connected to broker 'ssl://Xlabolgxcq.iot-as-mqtt.cn-shanghai.aliyuncs.com:1883'
① 2020/6/16	7:39:30		KEPServerEX\IoT Gateway	Running with Java 1.8.0_241 [Oracle Corporation Java HotSpot(TM) Client VM version 25.241-b26].
① 2020/6/16	7:39:30		KEPServerEX\IoT Gateway	IoT Gateway using JRE at [C:\Program Files (x86)\Java\jre1.8.0_241].