How to Integrate Gateway Data in AWS IoT
How to Integrate Softing Gateway Data in AWS IoT

Preliminary Remarks

This Configuration Manual describes how to configure the Softing gateway *uaGate SI*, *uaGate MB* or *edgeGate* as *AWS* IoT device ("Thing"). The specific used gateway is referred to in this manual as *gateway*. It is based on the AWS Developer Guide <https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>.

Additional information about the Softing products can be found at the following web pages:

*AWS Preparation Steps*

1. **Register Gateway as Device in the Registry**

Follow the instructions given at <https://docs.aws.amazon.com/iot/latest/developerguide/register-device.html>. In step 4, define unique *gateway* name, e.g. by using its serial number.

2. **Create and Activate Certificate for Gateway**

Follow the instructions given at <https://docs.aws.amazon.com/iot/latest/developerguide/create-device-certificate.html>. In step 2, download certificate and key files. These files need to be uploaded as MQTT Client certificate into the *gateway* in a later step.
3. **Create AWS IoT Policy for MQTT Client Certificate**

Follow the instructions given at https://docs.aws.amazon.com/iot/latest/developerguide/create-iot-policy.html. Define *gateway* permission for *iot:Connect* and *iot:Publish* actions.

**NOTE:**
For some unknown reasons the attachment of policies as described in step 3. does not work. Instead, it looks like the policy must be created before attaching it to a certificate. However, the certificate dialog does not trigger the creation of a policy.

It is possible to create and attach a policy after the creation of a certificate by following these steps:

- Return to *AWS IoT Console* main screen and navigate to *Secure/Policies*
  
  ![AWS IoT Console](image)

- Press *Create a policy* button
- Define policy name
- Define *gateway* permission for *iot:Connect* action
• Enter user-defined client ID in **Resource ARN** field
  It is recommended to use the **gateway** name here. Remember this client ID for a later step.

  ![Create a policy](image)

  Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the AWS IoT Policies documentation page.

  **Name**
  
  uagate-163300167-policy

  **Add statements**

  Policy statements define the types of actions that can be performed by a resource.

  **Action**
  
  iotconnect

  **Resource ARN**
  
  arn:aws:iot:eu-central-1:9x6:client/uagate-163300167:

  **Effect**
  
  [ ] Allow  [ ] Deny

  ![Add statement button](image)

  ![Create button](image)

• Press **Add Statement** button

• Define **gateway** permission for **iot:Publish** action

• Define user-specific ARN topic. Remember this topic for a later step.

**NOTE:**

The placeholder “*” allows publishing to any topic.
• Press **Create** button

![Configuration Manual](59x376 to 374x722)

Add statements
Policy statements define the types of actions that can be performed by a resource.

<table>
<thead>
<tr>
<th>Action</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>iotconnect</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resource ARN</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>arnaws:iot:eu-central-1:9x6:client/uagate-163300167</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effect</th>
<th>Action</th>
<th>Value</th>
<th>Resource ARN</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Allow</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iotpublish</td>
<td></td>
<td>arnaws:iot:eu-central-1:9x6:topic/uagate-163300167</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deny</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add statement

4. **Attach AWS IoT Policy to Gateway**

- Return to **AWS IoT Console** main screen and navigate to **Manage/Things** page
- Click on device name of **gateway**
- Click on **Security**
- Click on hash value of created device certificate

Select **Attach policy** in **Actions** menu

Attach created policy to certificate

Attach policies to certificate(s)

Search for the policy and select it.
5. **Determine AWS MQTT Broker Address**

- Return to **AWS IoT Console** main screen and navigate to **Settings**
- MQTT Broker address can be found in **Custom Endpoint** field

**NOTE:**
The address looks similar to "123456789-ats.iot.eu-central-1.amazonaws.com"

### Gateway Configuration Steps

6. **Configure MQTT Broker**

- In **Internet Browser** connect to configuration webpage of **gateway**
- Login as **Administrator** or **ITAdmin**
- Navigate to **MQTT Broker Configuration** page

![Gateway ConfigurationSteps](image)

- Set **URI kind** to `ssl://`
- Set **Hostname** field by **AWS** MQTT Broker address (see section 5, **Determine AWS MQTT Broker Address**)
- Set **Port** field to “**8883**”
- Set **Client ID** field to defined gateway name
- Enable MQTT **Clean Session** flag

**NOTE:**
AWS Broker disconnects, if flag is not set
(see [https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html](https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html))

- Set **Authentication** to “**anonymous**”
- Set **Enable MQTT** checkbox
- Press **Save** button
7. **Define MQTT Client Certificate**

- Navigate to *MQTT Client Certificate* page
  
  - Define MQTT Client certificate as created in section 2, *Create and Activate Certificate for Gateway*
  
- Set *Use MQTT Client Certificate* checkbox
- Press *Save* button
- Press *Apply Pending Changes* button

8. **Verify Connection**

- Navigate to *Gateway Status* page for verifying that connection has been established
9. **Select MQTT Topics**

- Navigate to *MQTT Topic Selection* page

- Select PLC items to be published
10. Define MQTT Topic Settings

- Navigate to **MQTT Topic Settings** page

- If user-specific ARN topic has been defined
  (see section 3, *Create AWS IoT Policy for MQTT Client Certificate*):
  - Do **not** define **MQTT Root Topic (Topic Prefix)**
  - Set **Hierarchy** to **Suppressed PLC symbols**
  - Enter defined unique gateway name from section 1, *Register Gateway as Device in the Registry*, **MQTT Suffix Topic** field

- If placeholder "*" has been defined as ARN topic
  (see section 3, *Create AWS IoT Policy for MQTT Client Certificate*):
  - Enter user-defined root topic in **MQTT Root Topic (Topic Prefix)** field
  - Select **Hierarchy** radio button as needed
  - Enter user-defined suffix topic in **MQTT Suffix Topic** field

- Do not activate **Enable MQTT Retain** checkbox

**NOTE:**
AWS Broker closes connection, if retain flag is set for MQTT Publish message
(see [https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html](https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html))

- Set **Collect PLC values in one MQTT message** checkbox for reducing the amount of MQTT messages sent from the gateway to the AWS cloud
- Press **Save** button
- Press **Apply Pending Changes** button
11. Monitor Values in AWS

- Return to **AWS IoT Console** main screen and navigate to **Test**
- Subscribe to all topics using the wildcard “#”
- Received MQTT messages look different, depending on topic format settings and options for the collected PLC values

**MQTT client for single value**

**MQTT client for multi value**