PUSR®
www.pusr.com

USR-M300 Quick Start Guide with AWS IoT

Be Honest & Do Best

Your Trustworthy Smart Industrial IoT Partner

1. Introduction

USR-M300 is a high-performance and scalable edge IOT gateway. This device integrates edge collection, data calculation, data reading and writing, active reporting, linkage control, IO collection and control and other functions. The collection protocol includes standard Modbus protocol and a variety of common PLC protocols, as well as industry-specific protocols. At the same time, the product also has routing and VPN as well as graphical programming functions to ensure data transmission security. Using graphical programming, users can develop independently to achieve the required functions.

USR-M300 is embedded in Linux kernel, with a main frequency of up to 1.2Ghz. It can access the Internet via Ethernet port, ADSL and LTE cat4 cellular network to achieve easy network deployment.

It is widely used in various industrial intelligent solutions such as industrial robot, smart factories, smart agriculture, smart water management system etc.

2. AWS IoT

USR-M300 supports connecting to AWS IoT platform via MQTT, which can be achieved via simple MQTT and SSL parameter configuration. At the same time, the device's edge computing and AWS functions support combined configuration, which is very flexible and practical.

2.1. Basic Parameters

- Protocol Select: MQTT version, supports MQTT-3.1 and MQTT 3.1.1.
- Client ID: MQTT client identifier.
- Remote Server Address: MQTT server domain name or IP address.
- Remote Port: MQTT server port.
- Heartbeat time: MQTT protocol heartbeat time.
- Reconnection Internal: The interval between the current connection failure and the next MQTT connection.
- Connection Verification: When enabled, after connecting to the MQTT server, the username and password will be sent for connection authentication.
- Username: MQTT connection username, used for connection authentication.
- Password: MQTT connection password, used for connection authentication.
- Last Will: MQTT connection flag. When the network connection is closed, the server must publish this will message.

- SSL protocol: Supports TLS1.0 and TLS1.2 versions, and the authentication mode can choose none certificate authentication, CA signed server and self signed certificate.

2.2. Publish Settings

- Topic: Publish topic name.
- QOS: Message quality of published topics.
- Message retained: MQTT retains the message flag, which is used by the server to store this application message and its quality of service (QoS).

2.3. Subscribe Settings

- Topic: Subscribe topics.
- QOS: Message quality of subscribed topics.

3. AWS Connection Test

In this case, we will show how to connect M300 to AWS.

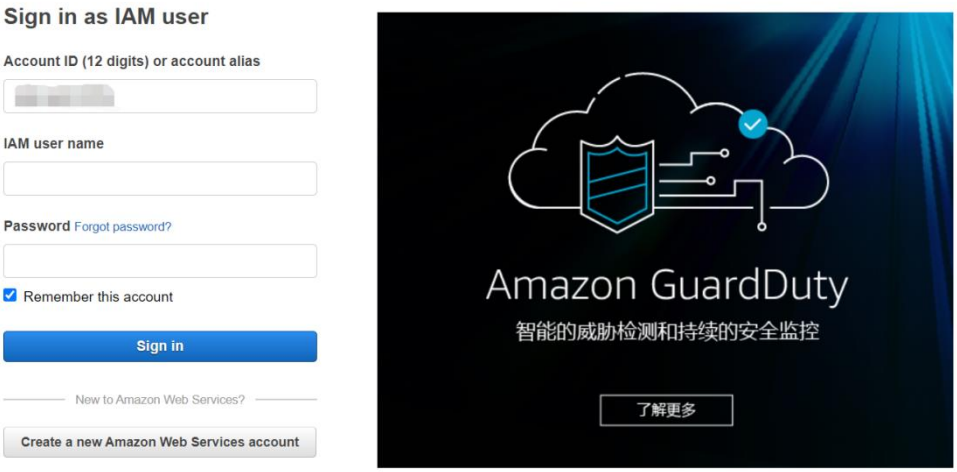
3.1. Preparations

- USR-M300*1
- RS485 serial to USB cable*1
- Ethernet cable*1
- 12V/1A power adaptor*1

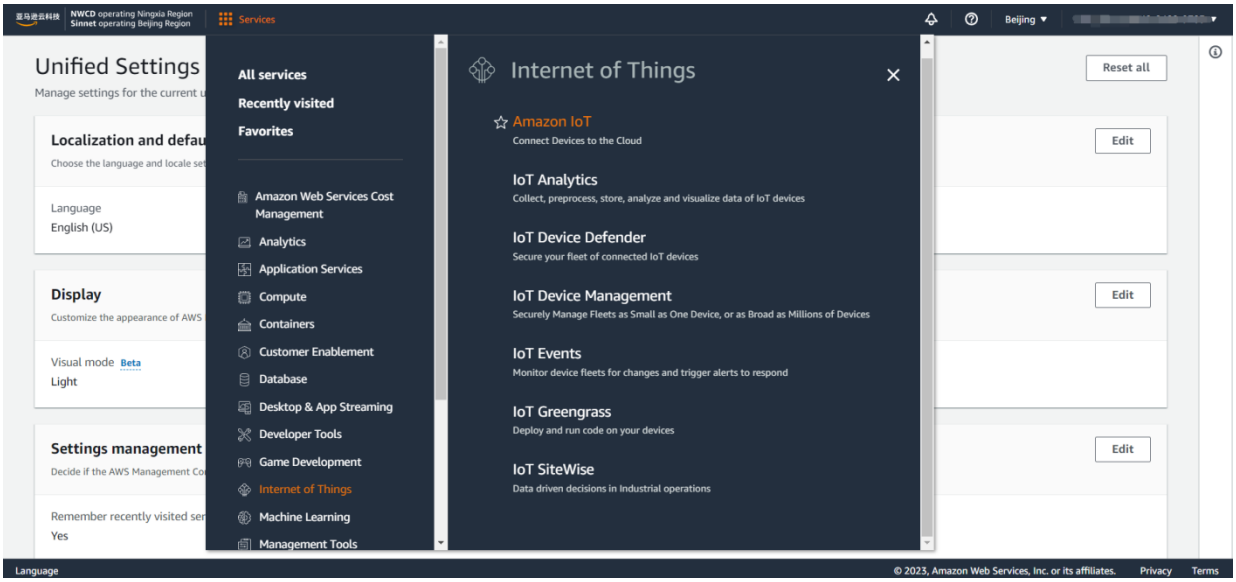
3.2. Configuration of AWS

3.2.1. Login

1. Login **https://www.amazonaws.cn/en/**
2. Login to the account. If you do not have an account, please create one firstly.

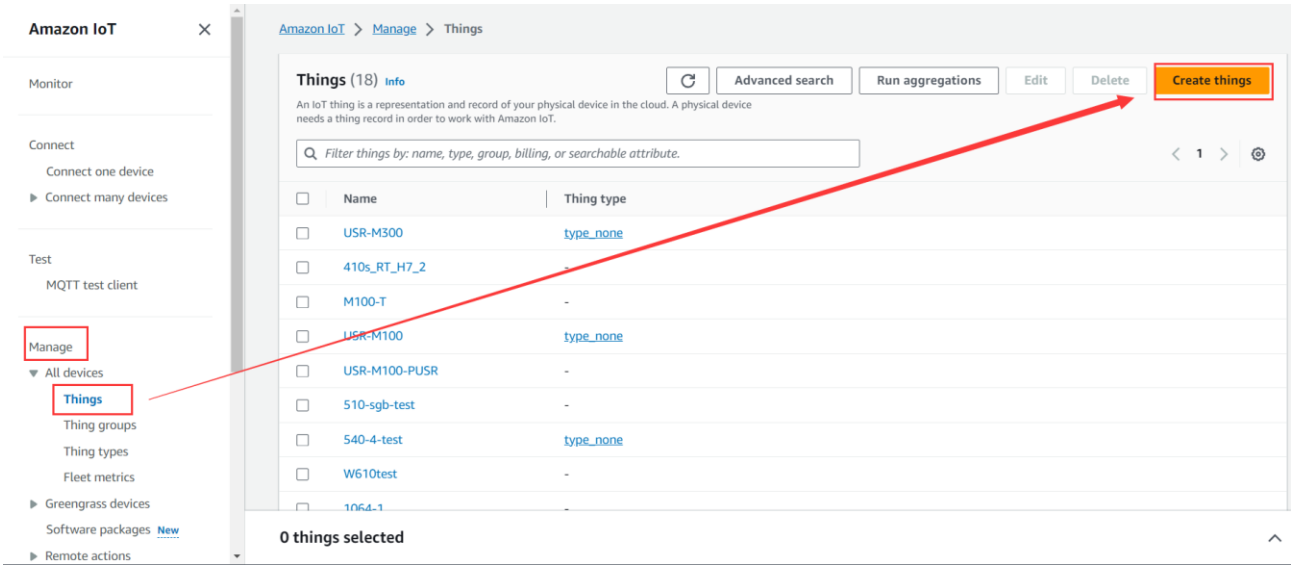


3. Find **Amazon IoT** in **Internet of Things**.

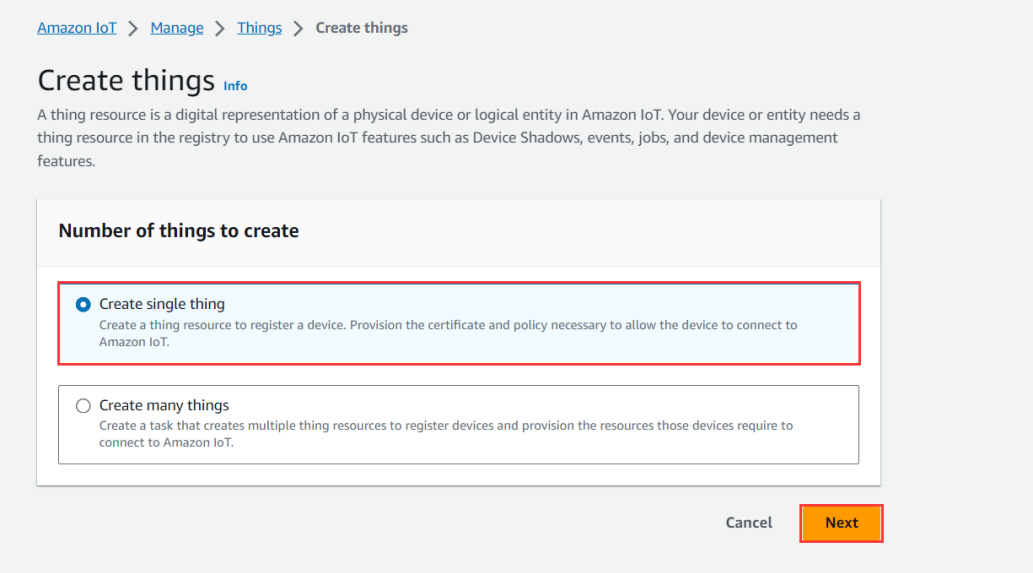


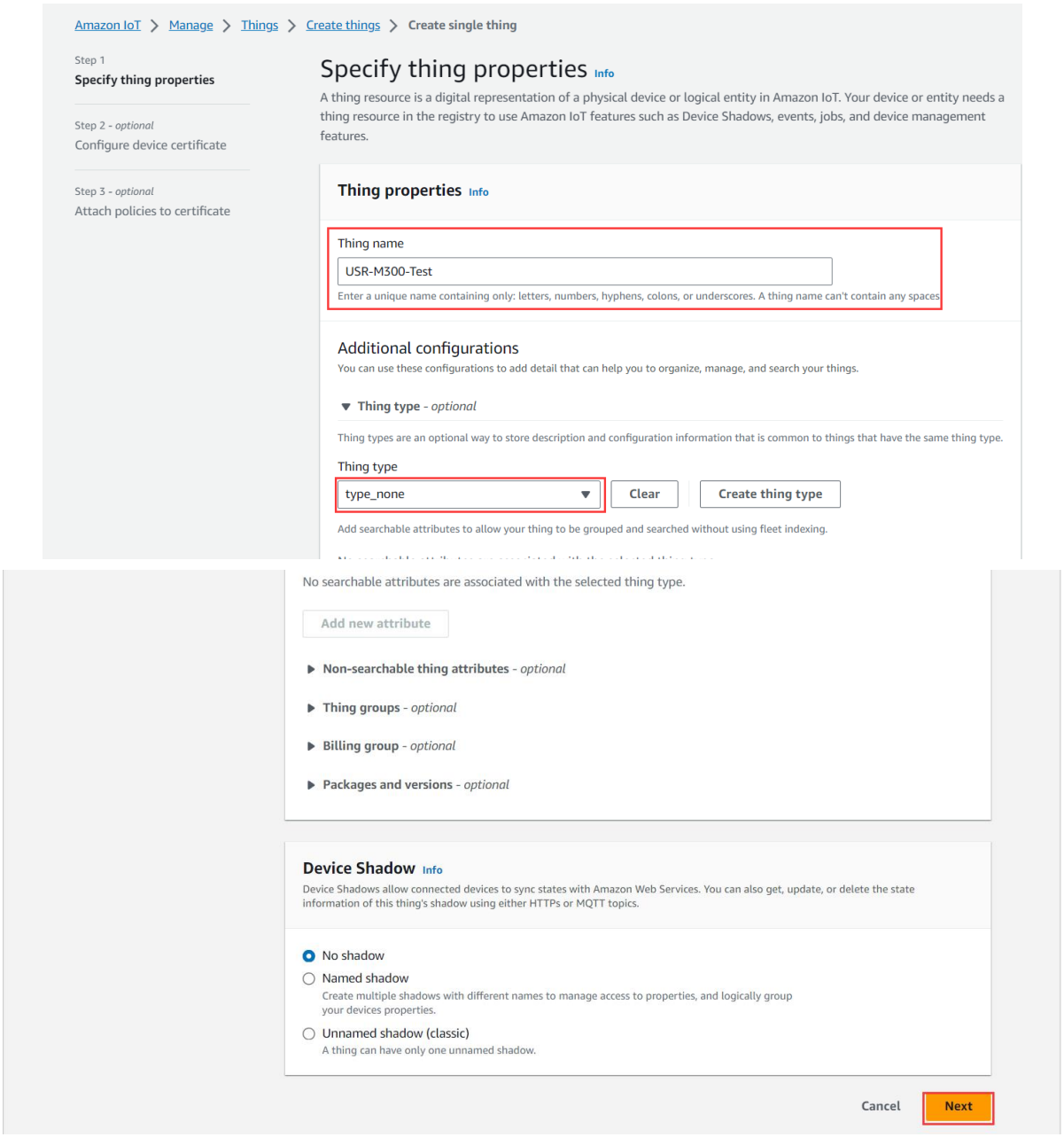
3.2.2. Create Things and Certificates

1. In **Manage->All devices->Things**, click **Create things** to add the device.

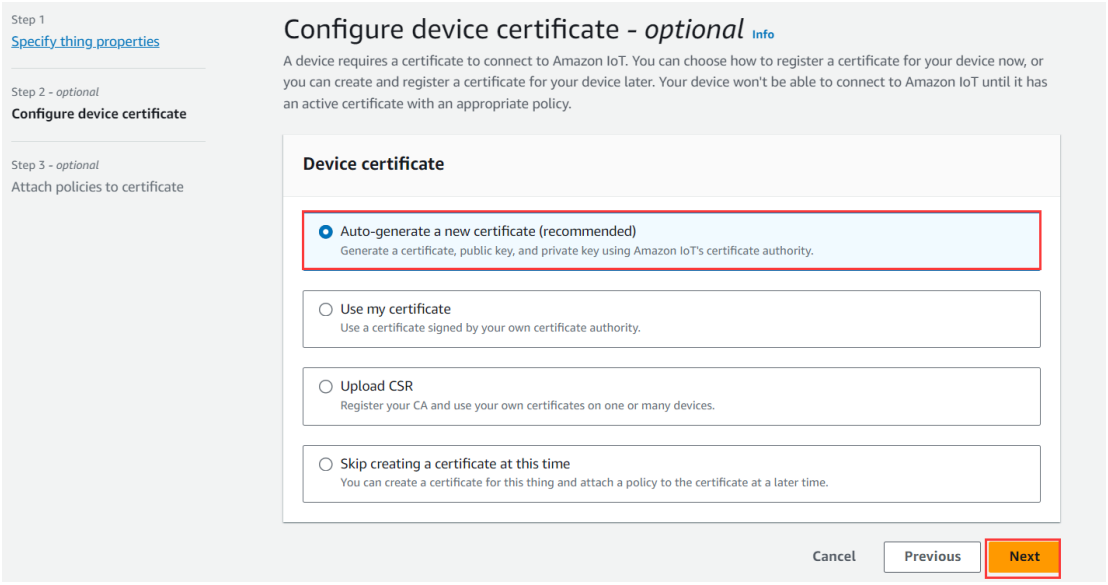


2. Choose **Create signal thing**, fill in the **Thing name** and **Thing type**, here we configure the thing name to "USR-M300-Test", configure the thing type to "type_none".

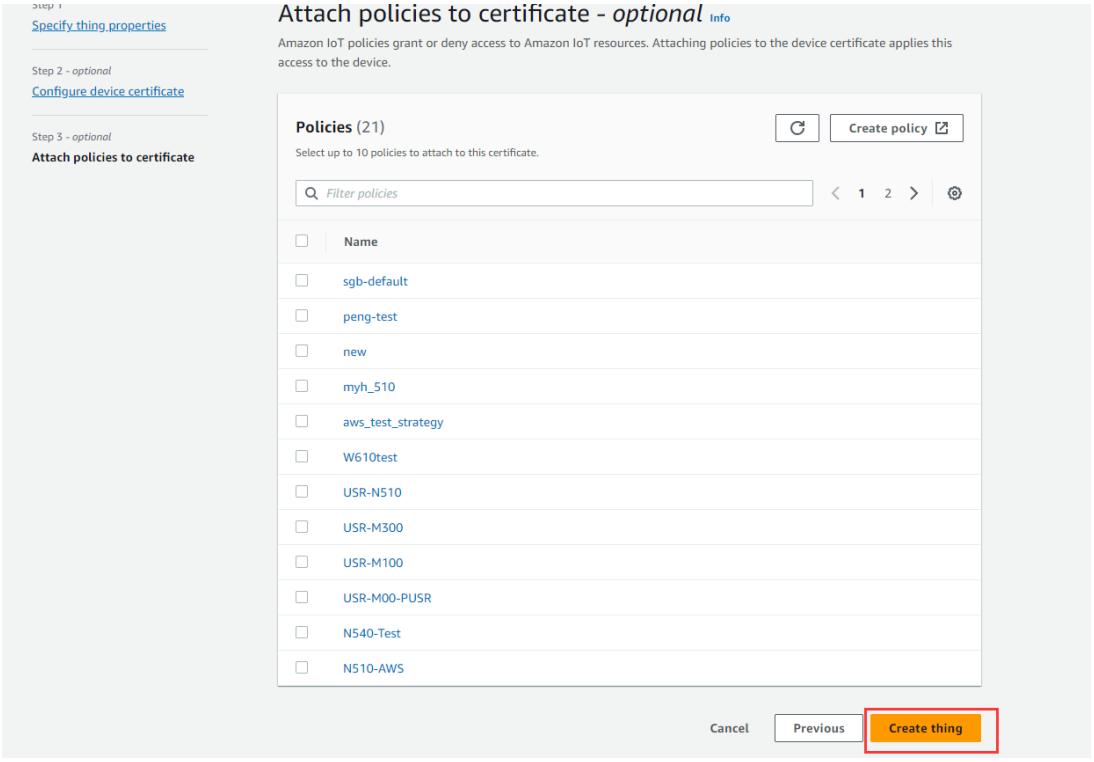


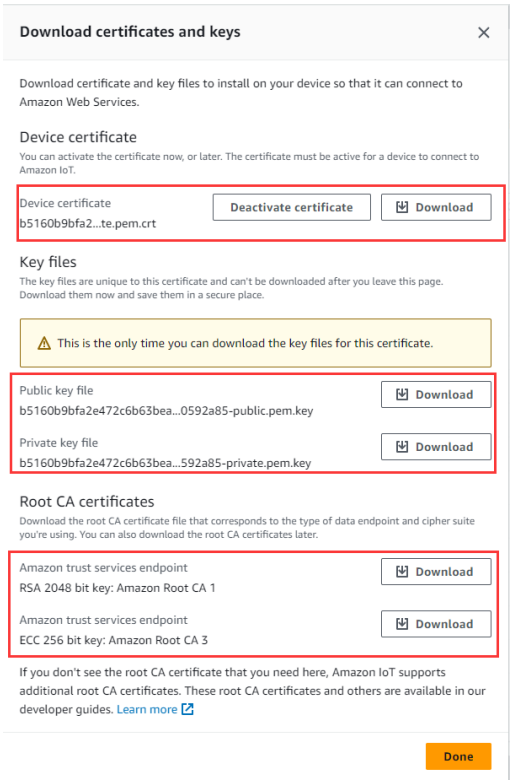


3. Next, choose **Auto-generate a new certificate**, you can also choose others if you have your own certificates. Then click **Next**.



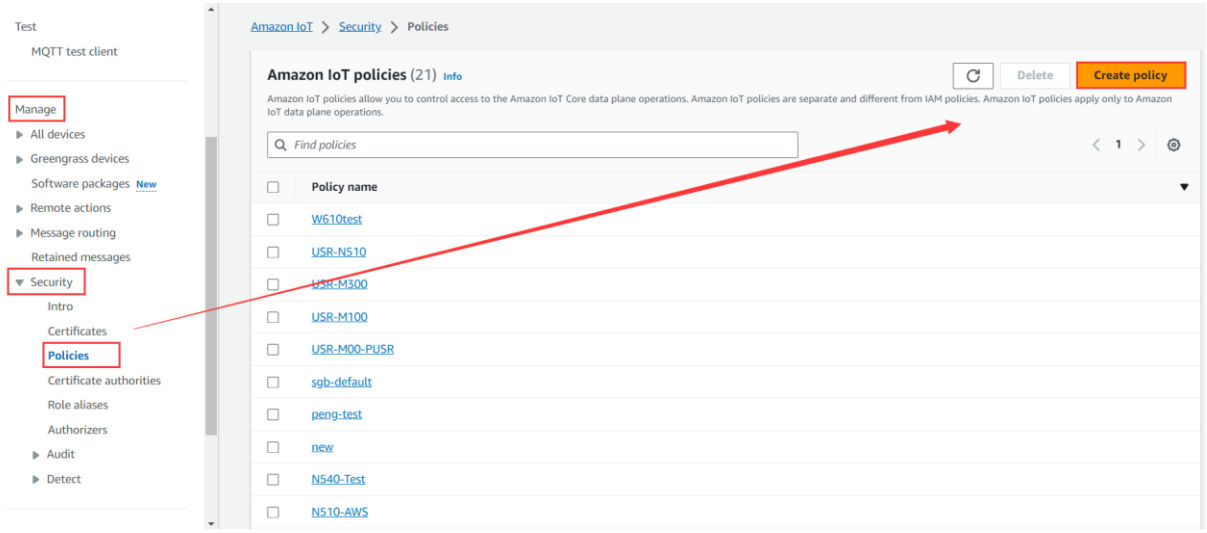
4. Do not create policies, directly click **Create thing.** Then it will show the certificates interface. Download the certificate and key files, then click **Done** to back to the things interface.



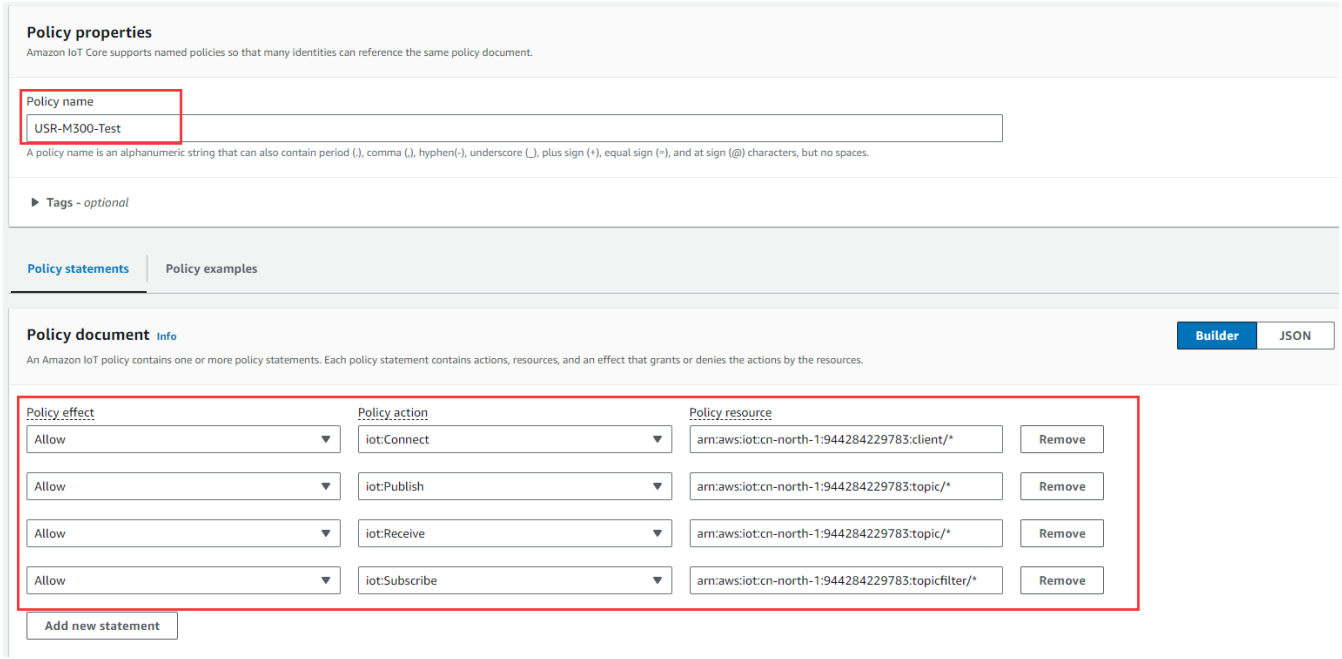


3.2.3. Create Policies

1. In **Manage->Security->Policies** interface, click **Create policy**.

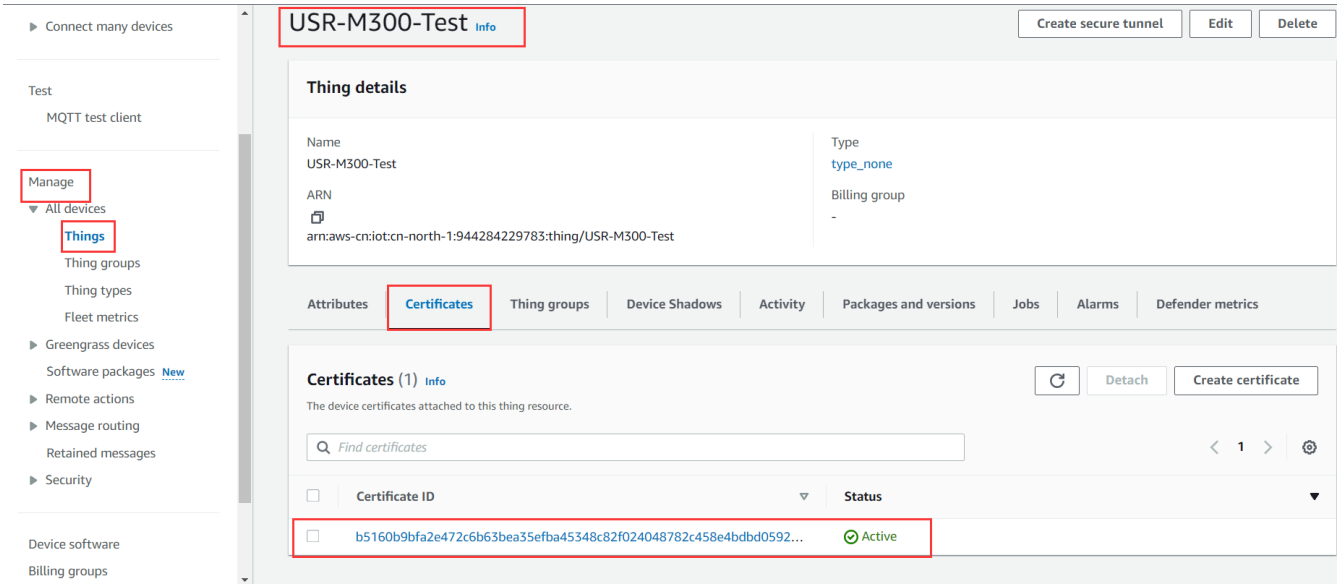


2. Fill in the **Policy name**, add new statement in **Policy document**. There is a default statement which can be directly operated.
3. Add 4 policies: iot:Connect, iot:Publish, iot:Receive, iot:Subscribe.
4. Policy resource format: arn:aws:iot:region:AWS-account-ID:Resource-type/Resource-name, AWS-account-ID is your account ID of AWS.
5. Then click **Create** to create the policies.

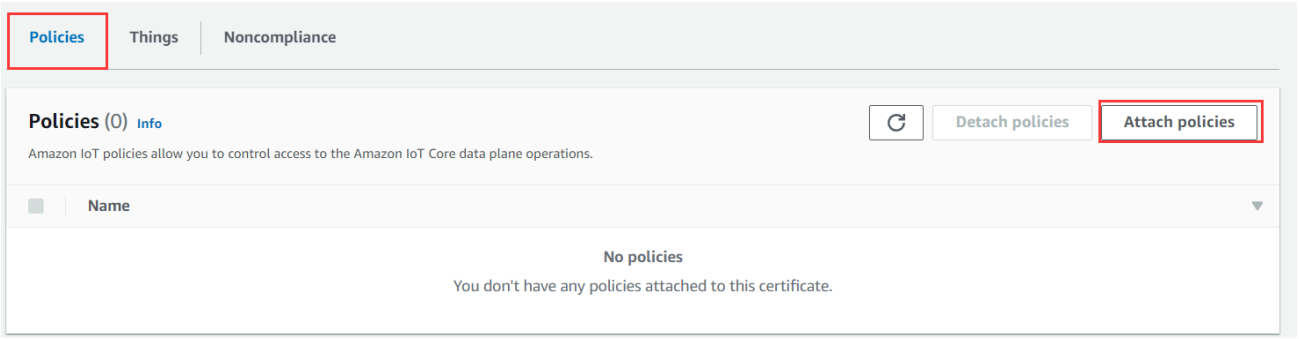


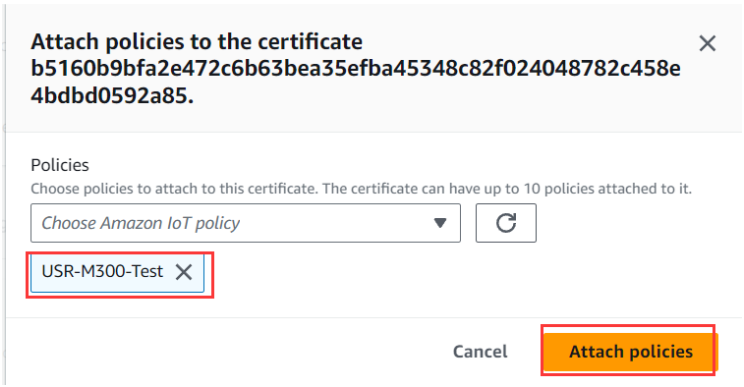
3.2.4. Attach Polices to Certificate

1. We have bound certificate and the thing when creating the device, so we can directly find the device in **Manage->All devices->Things**, click **Certificates** in **USR-M300-Test**.



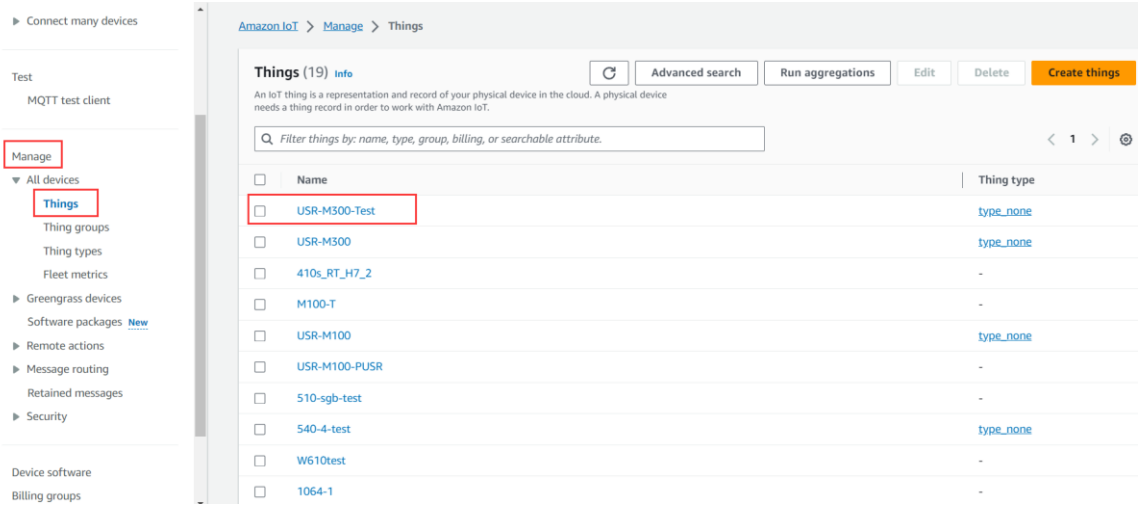
2. Find **Polices** under certificate, click **Attach policies**, choose the polices you have created.



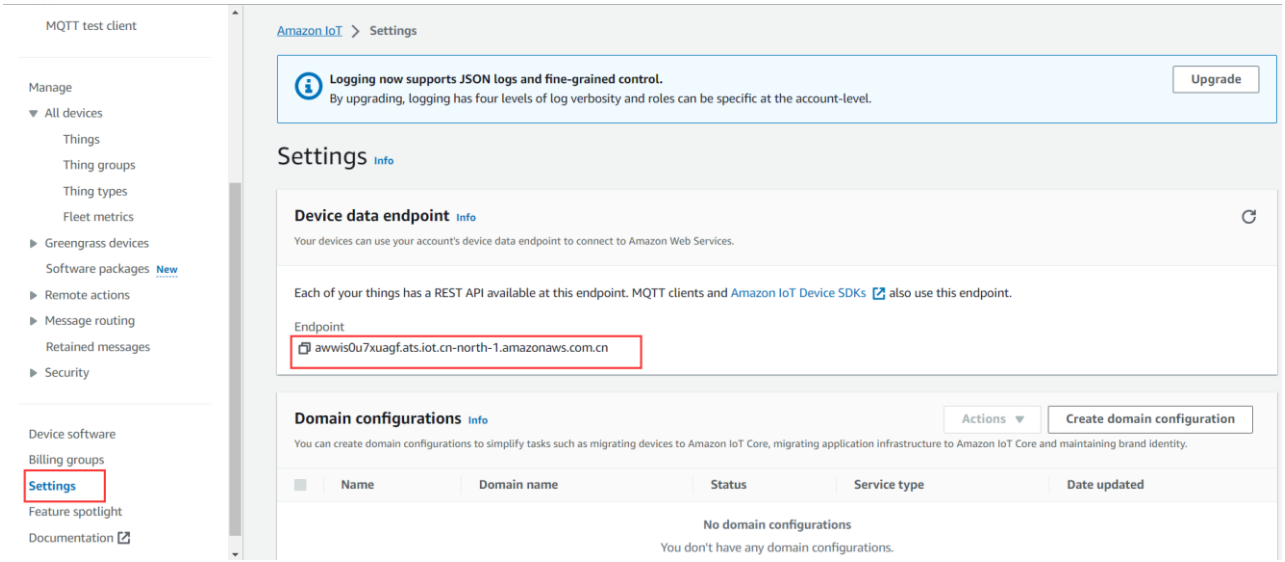


3.2.5. Obtain Product Information

1. Client ID is the Things name of the device, you can find the device name in **Manage->All devices->Devices**.



2. Find the server domain address that M300 device needs to connect in **Settings**, port defaults to **8883**.



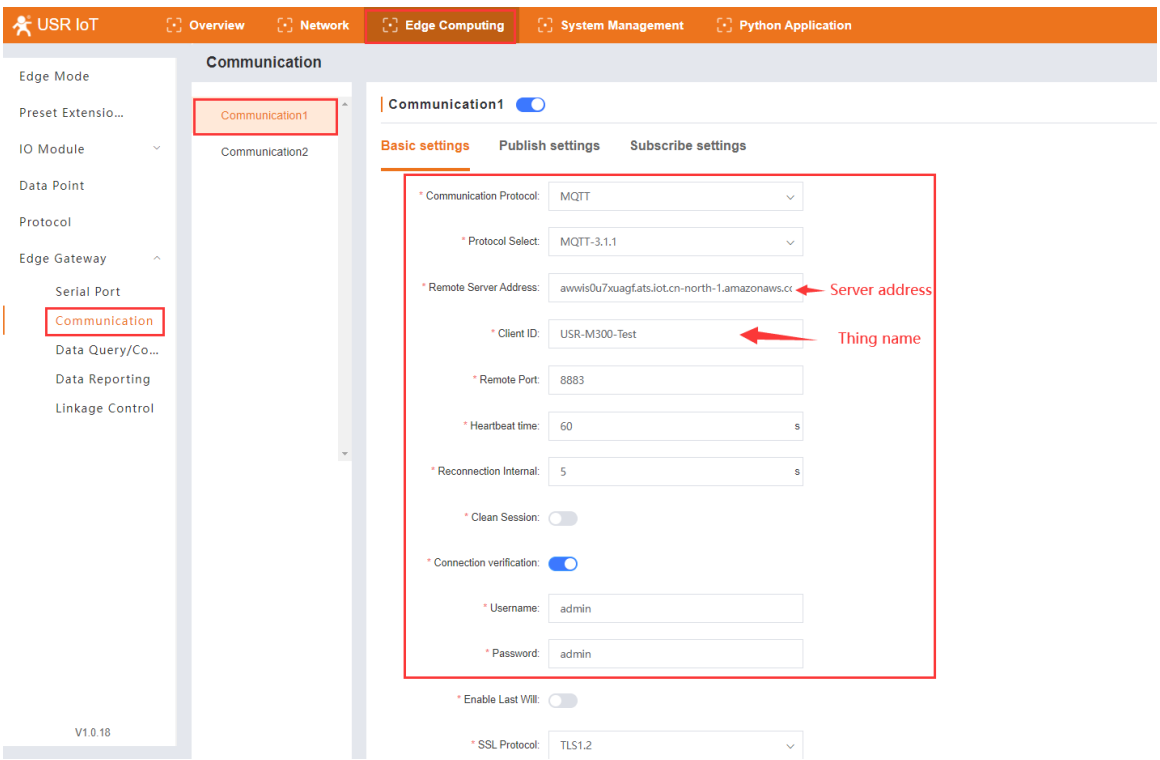
3.3. Device Configuration

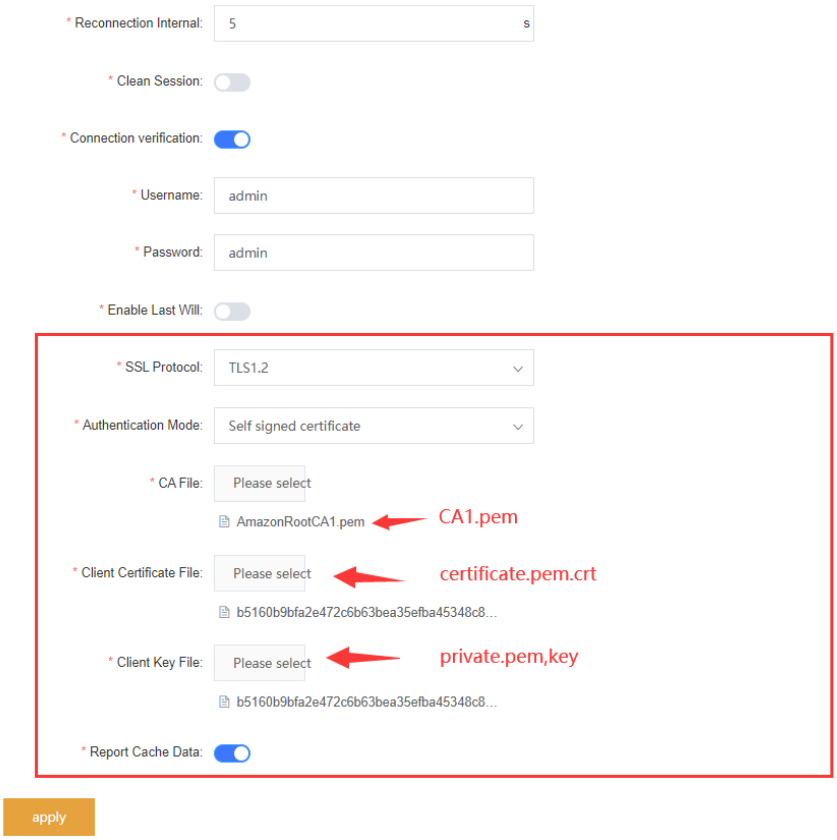
(1) Enable MQTT communication protocol.

(2) Configure the **Client ID**, **Remote port** 8883 and **Remote server address**.

(3) Enable **Connection verification**, **Username** and **Password** can be custom.

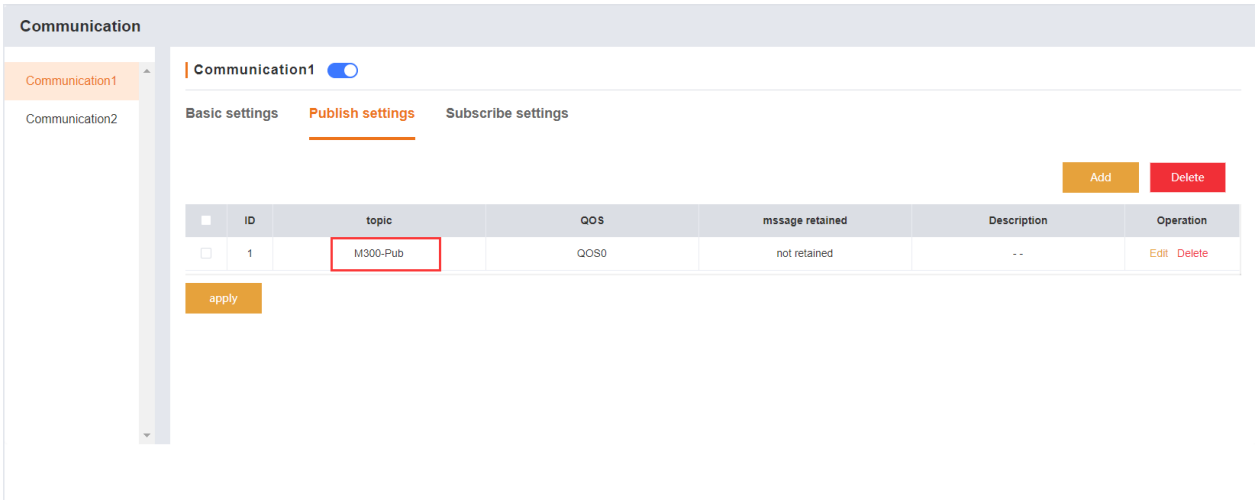
(4) Add the SSL certificates, configure the **SSL protocol** to **TLS1.2**, **Self signed certificate**. Upload **AmazonRootCA1.pem** in **CA File**.



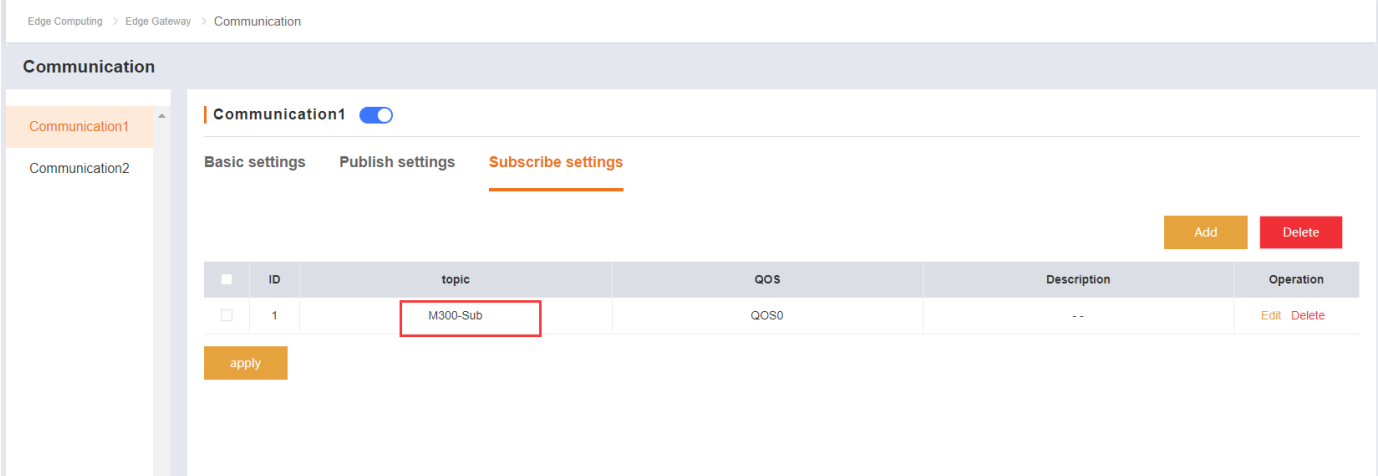


(5) After above configurations, click **Apply** and then configure the topics.

(6) Publish settings: Configure the publish topic to **M300-Pub**, click A**pply**.

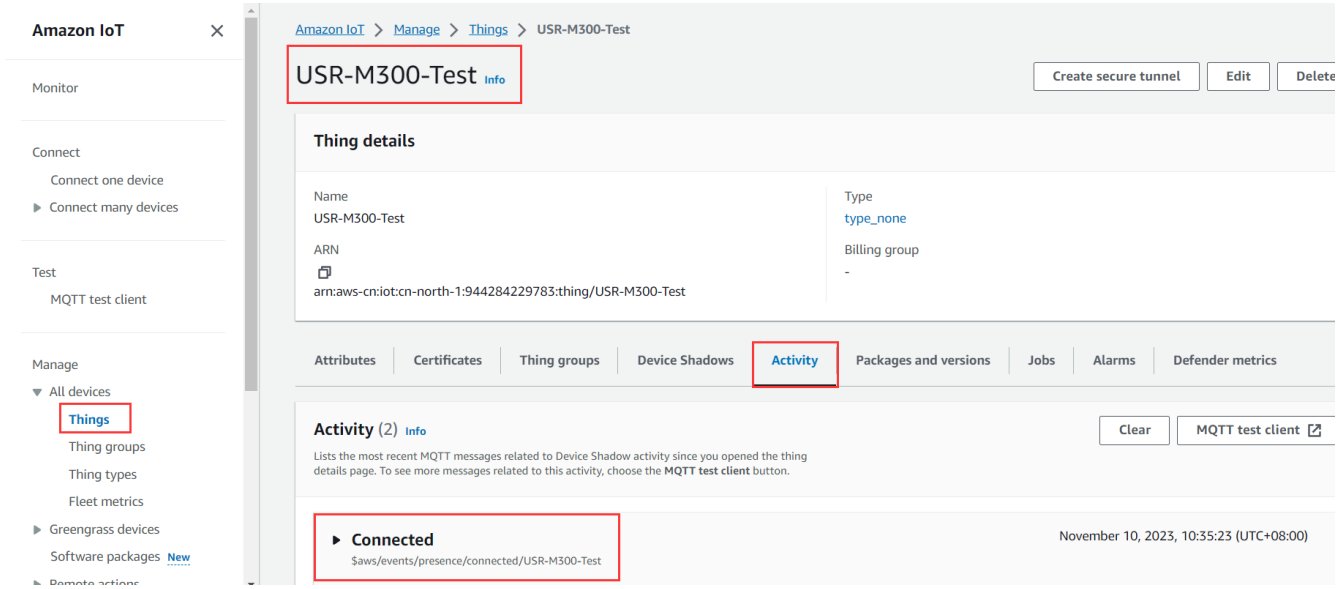


(7) Subscribe settings: Configure the subscribe topic to **M300-Sub**, click **Apply**, then restart the device to take the parameters effect.



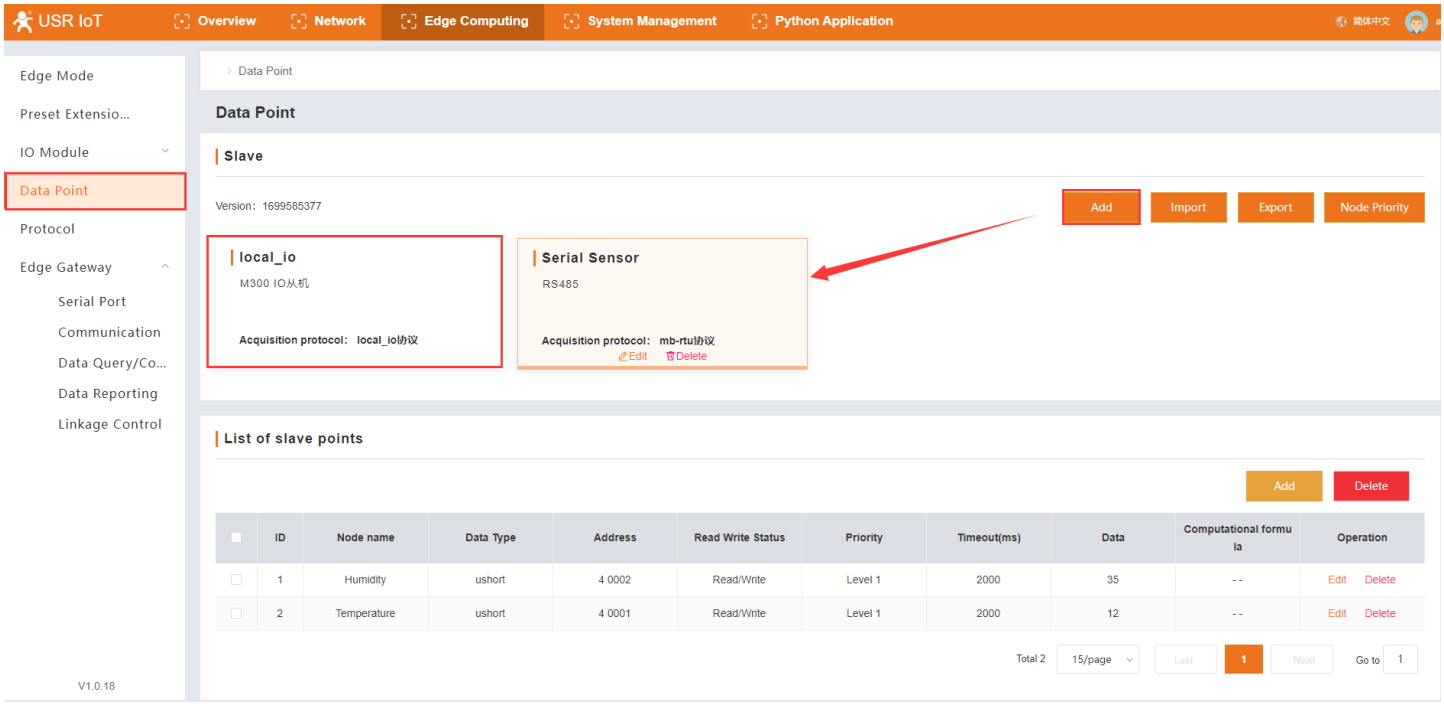
3.4. Device Activity

In **Manage->All devices->Things**, find the created device, click **Activity**, there will show **Connected.**

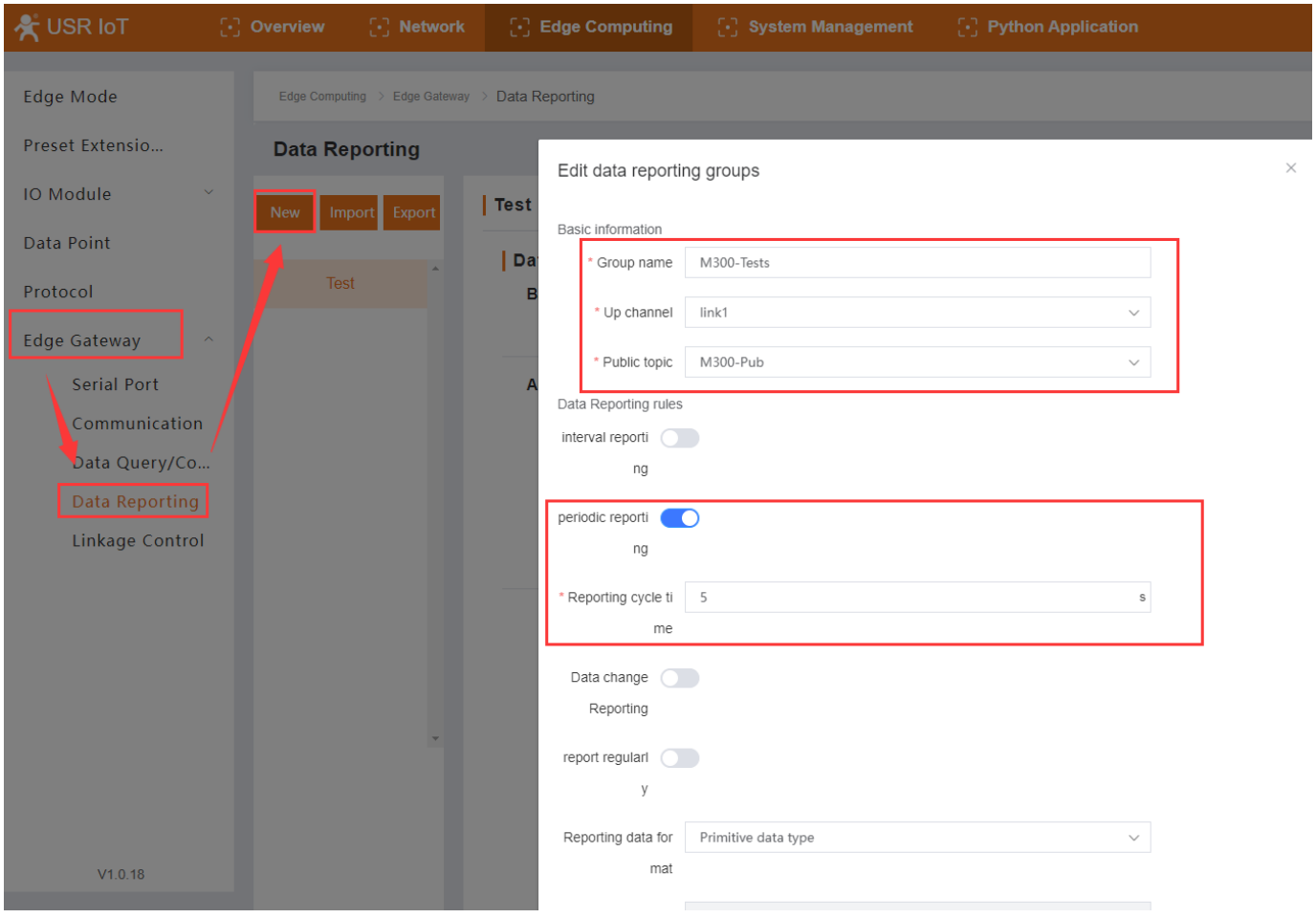


3.5. Data Transmission Test

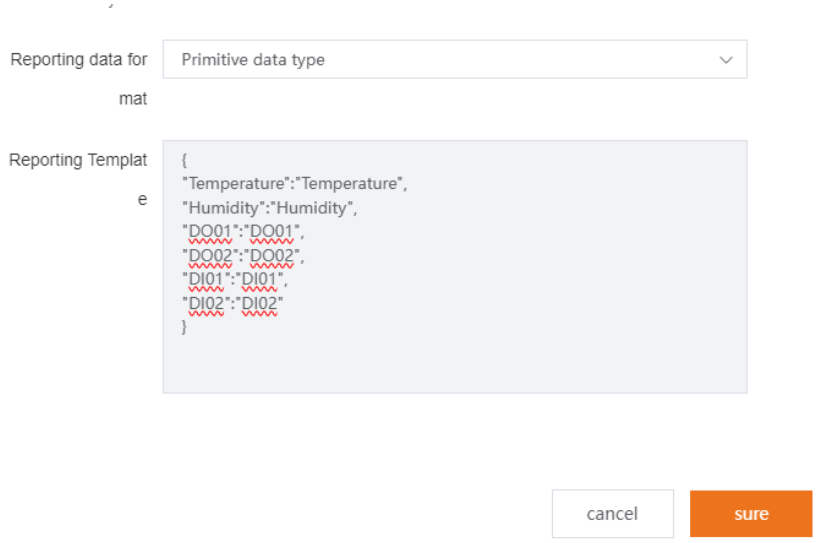
1. Add a new serial Modbus RTU sensor in **Data Point**. And configure the Modbus registers of the sensor.



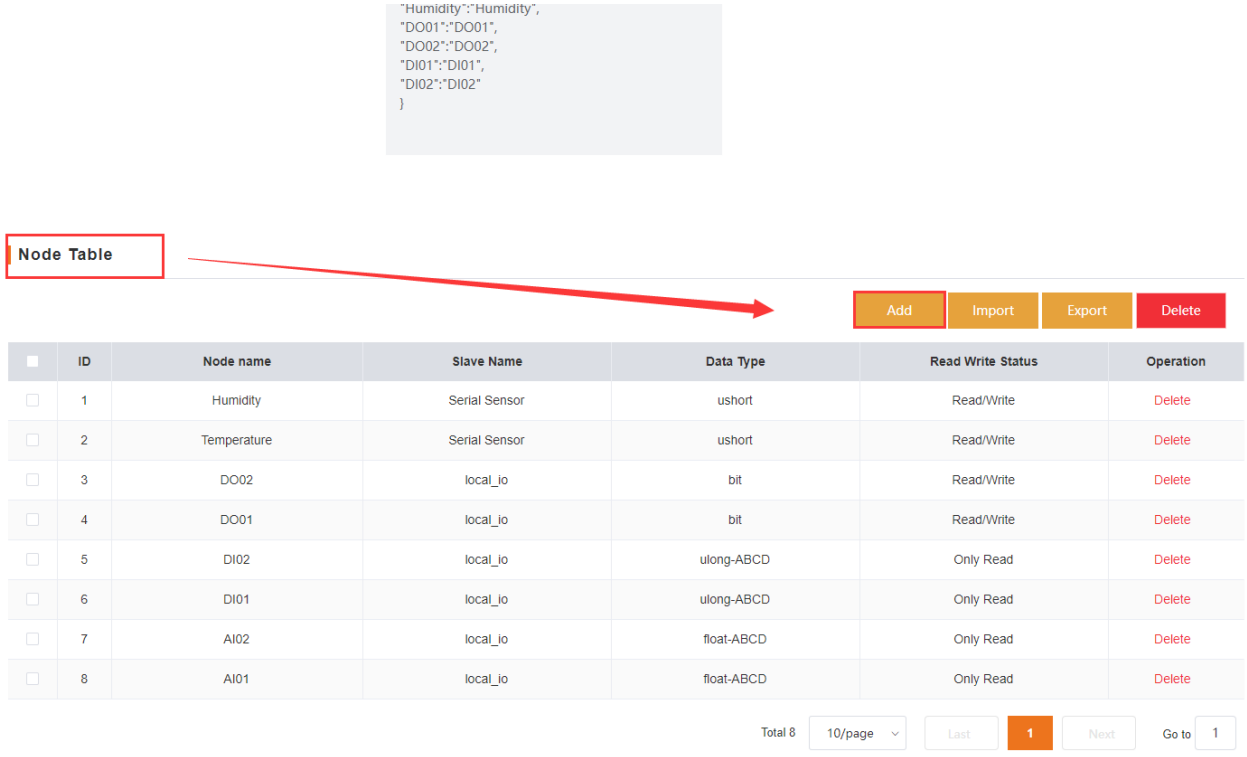
2. In **Edge Gateway->Data Reporting**, click **New** to add the **Data reporting groups.**



3. Configure the reporting template, here we configure the device reporting the RS485 sensor data and DO1/DO1/DI1/DI2 status to AWS.

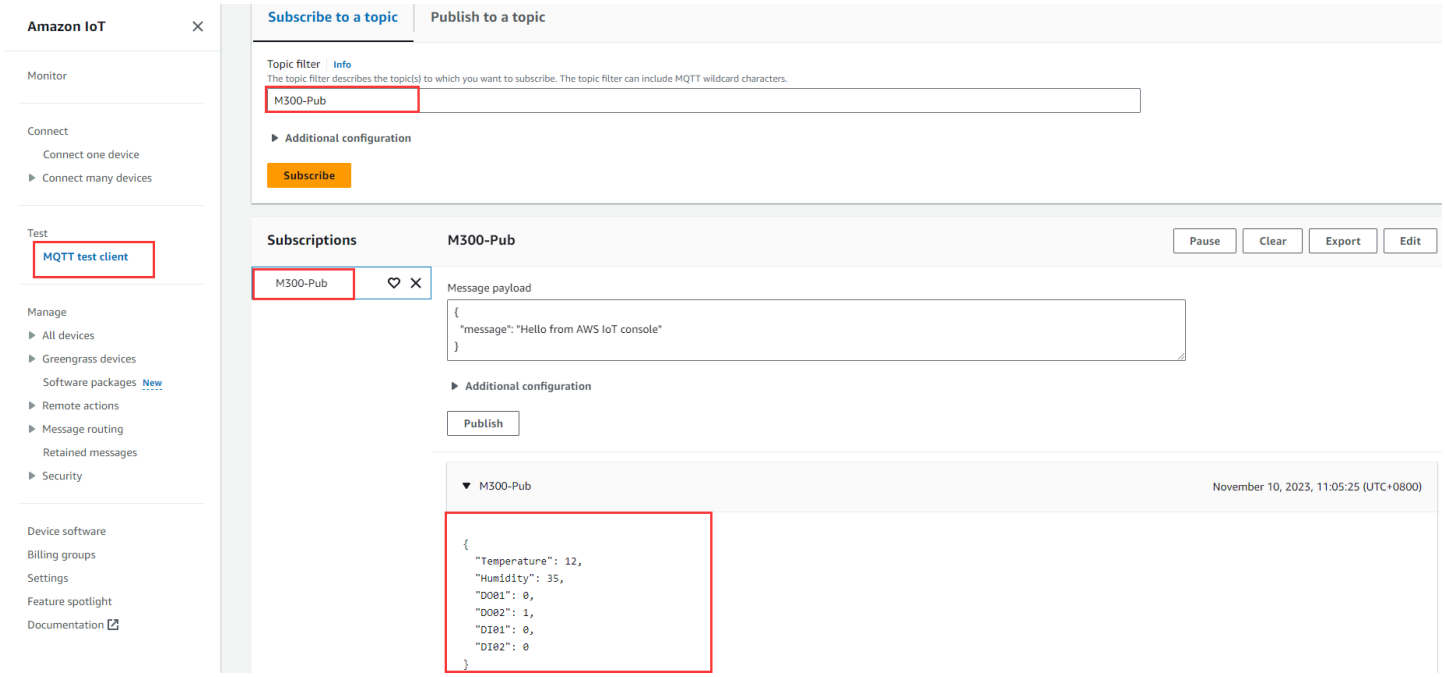


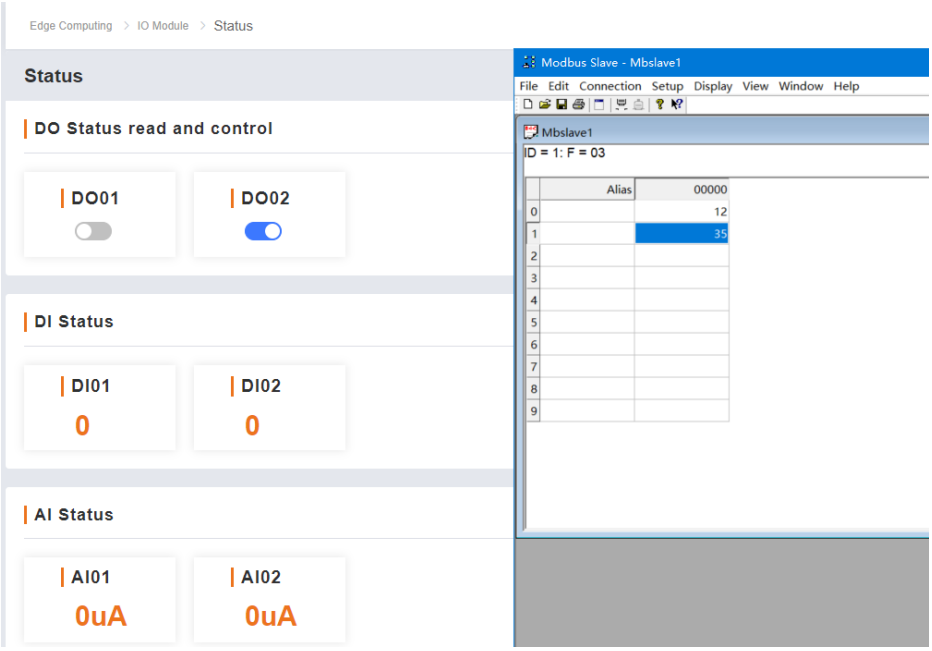
4. After configuring the reporting template, add the data points that need to be reported in **Node Table**.



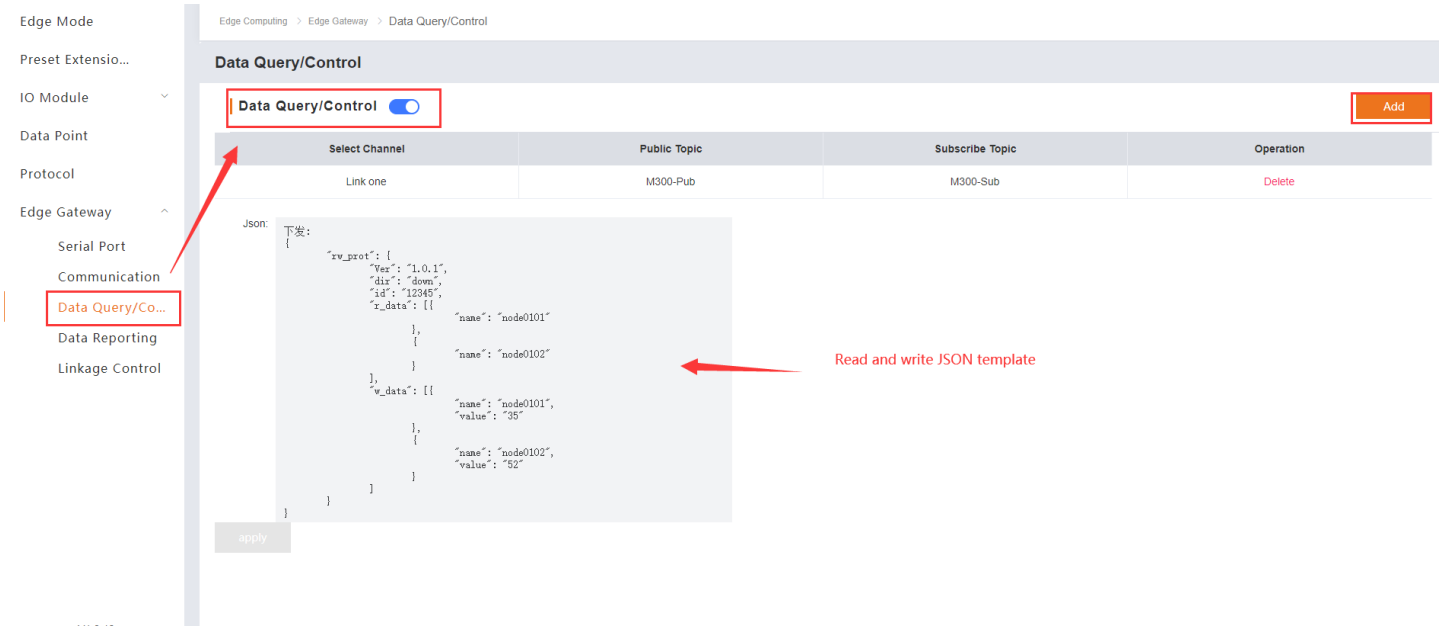
5. After configuring all the parameters, restart the M300 device to take the parameters effect.

6. After the device connecting to the AWS again, click **MQTT test client** in **Test**, subscribe the publish topic of M300: **M300_Pub**. Then we can receive the reporting message from M300.

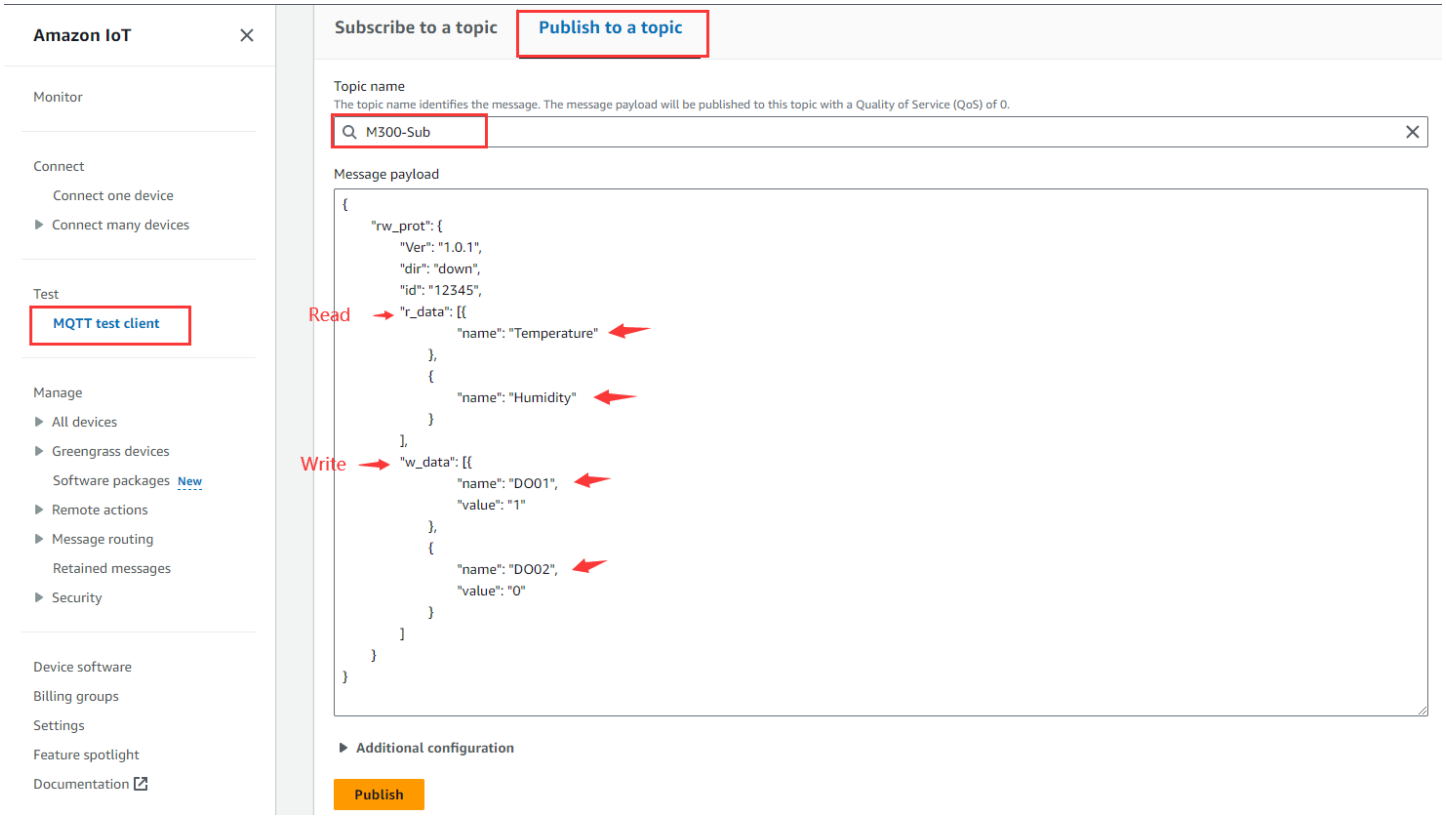




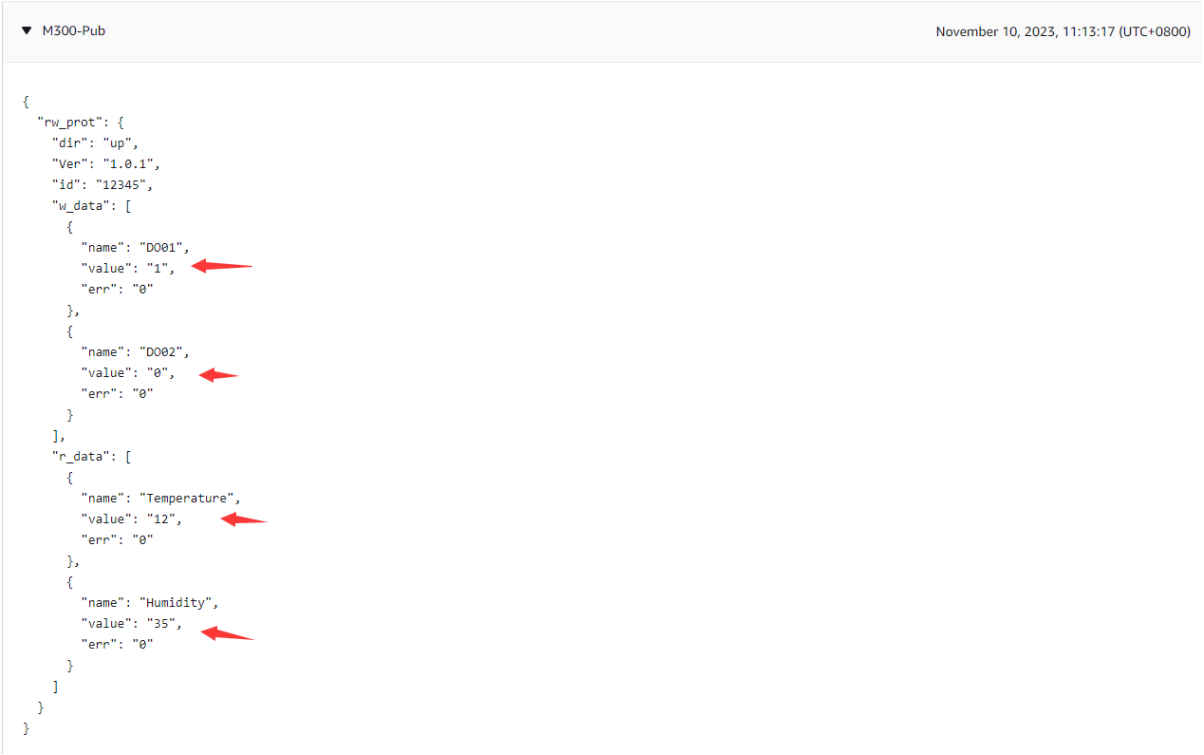
7. M300 also supports writing the register values from the server side, we can enable **Data Query/Control** function in M300 device firstly. Configure the writing and reading JSON message according to the JSON format in below interface.



8. Publish writing and reading JSON message to the subscribe topic of M300 from AWS.



9. Receive the response from M300 device.



Your Trustworthy Smart IOT Partner

PUSR®
www.pusr.com

Official Website: www.pusr.com

Official Shop: shop.usriot.com

Technical Support: h.usriot.com

Inquiry Email: inquiry@usriot.com

Skype & WhatsApp: +86 13405313834

Click to view more: Product Catalog & Facebook & Youtube