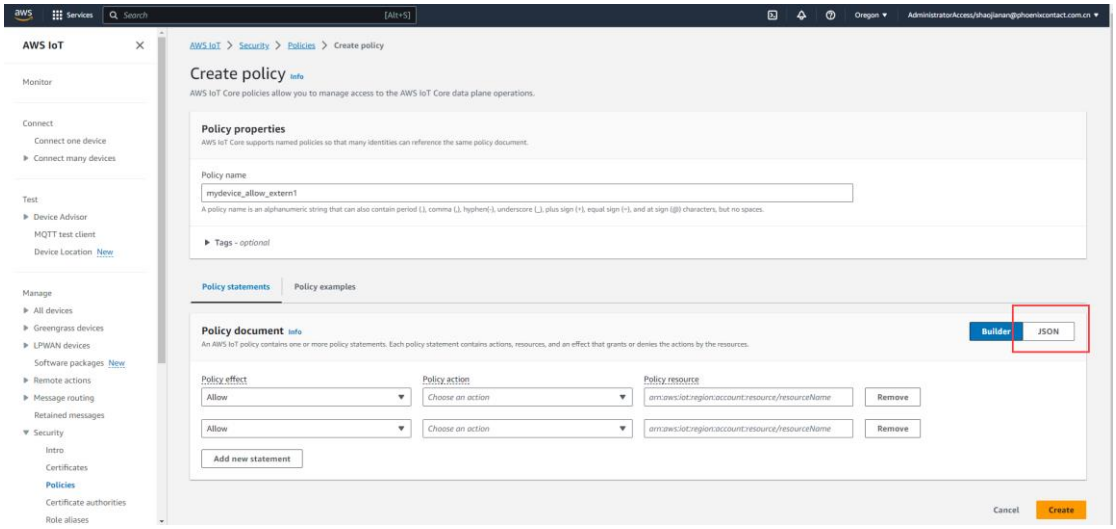
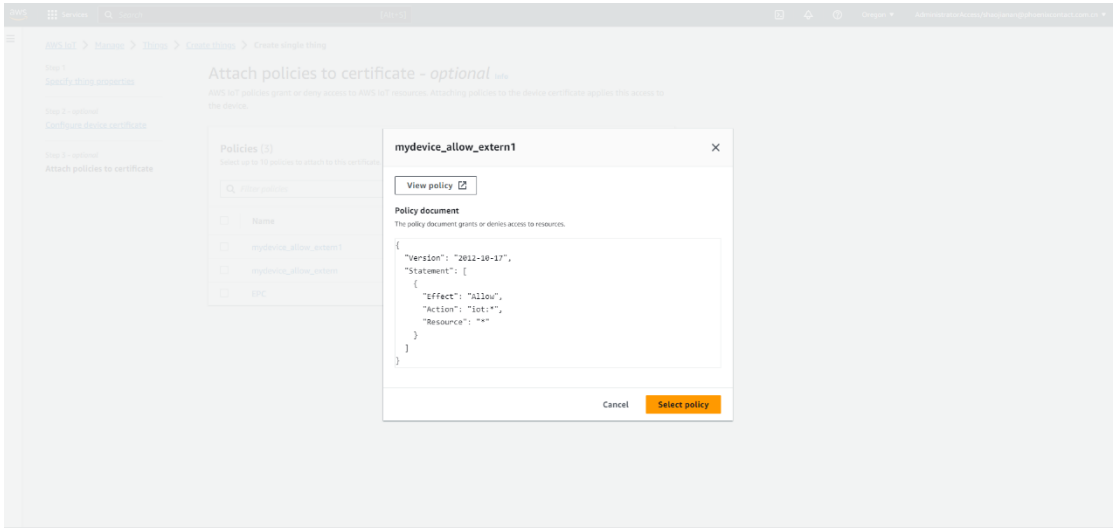
- The files in this folder are just used as example and will not work. Expecially the certificates are invalid.
- You must create your own certificates with your own AWS account and use it in the PLCnext Engineer project.

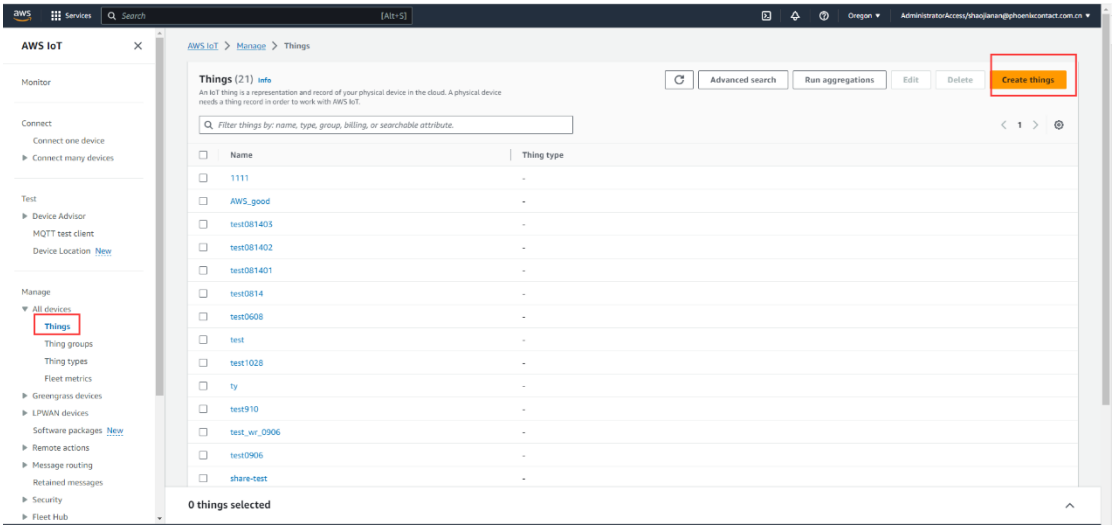
1. Log in AWS IoT, And create a goods.
   1) Log-in into your AWS account
   2) Create a policy



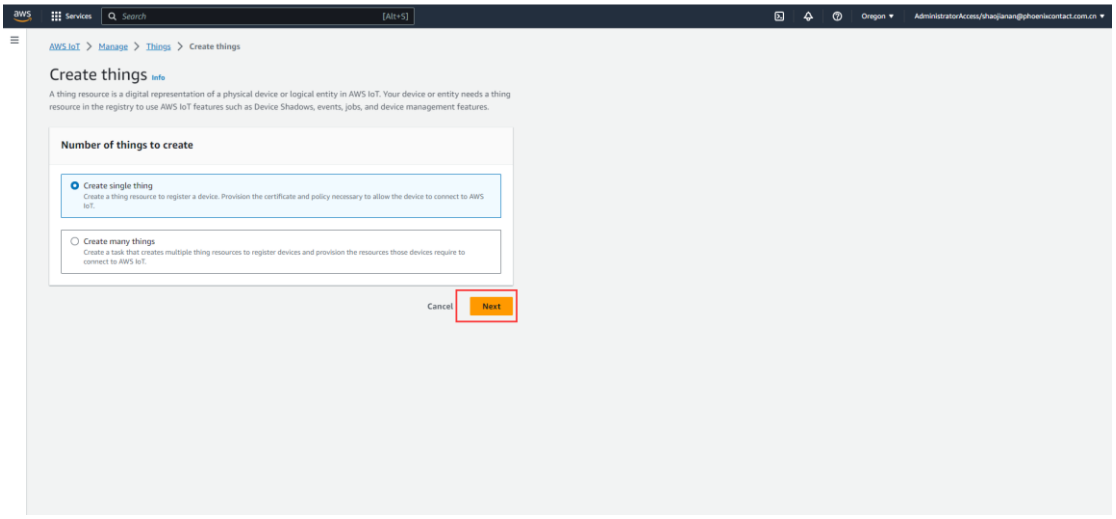
   3) The content of the policy



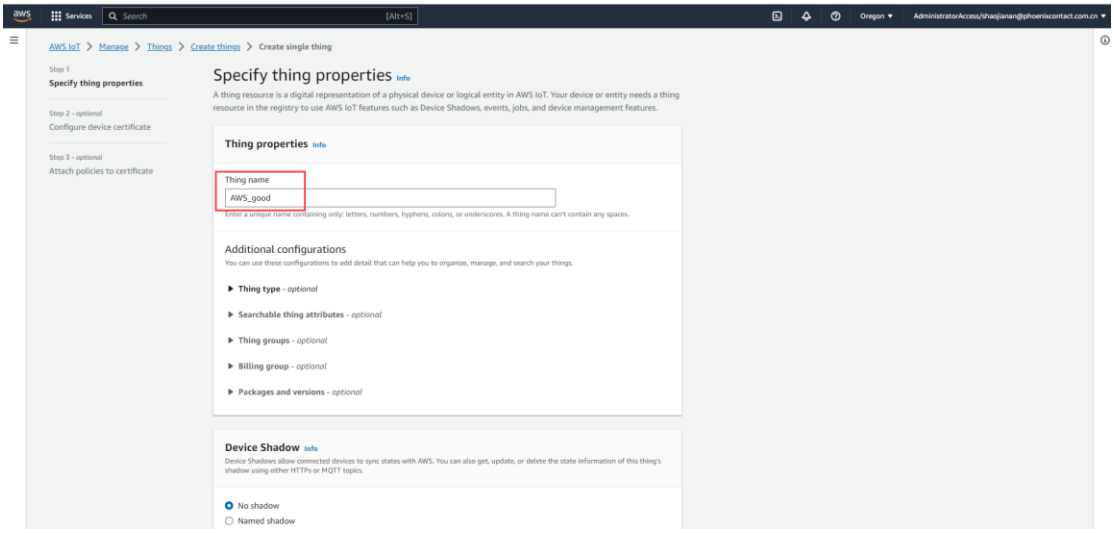
   4) Create a new good.



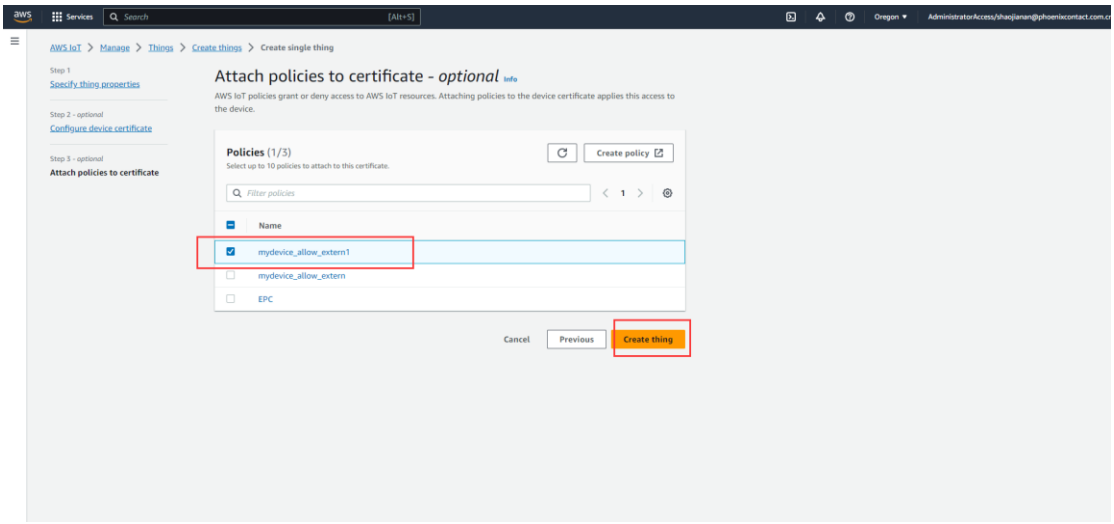
5) Choose the “Create single thing”, and then click the Next



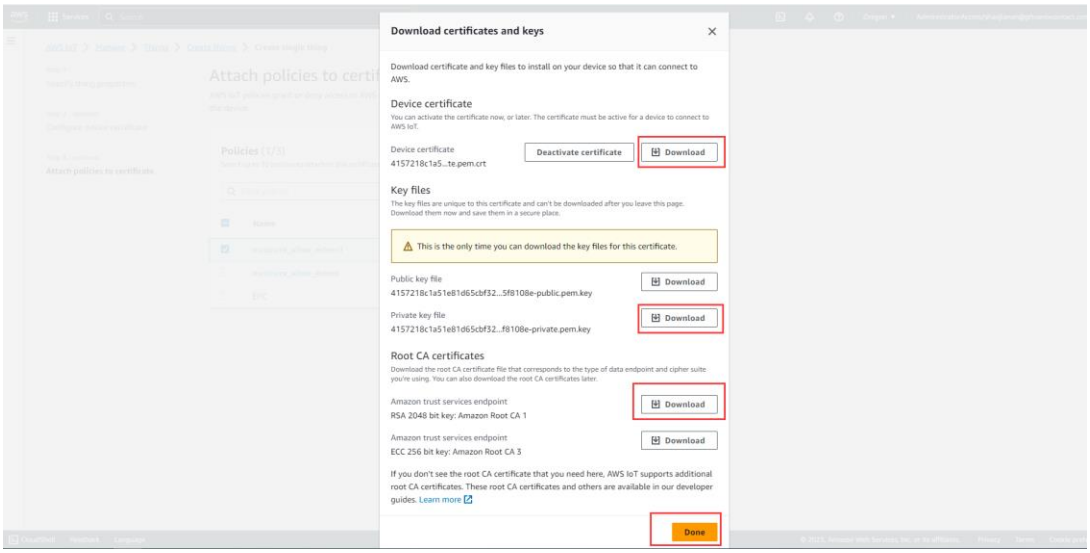
6) Fill in the name of the goods and then click "Next". In the example project the name of the good corresponds to the "device_id"



7) Select the policy you want to attach to the certificate, and click the “Create thing”.



8) Click "Create a certificate" to generate the certificate and key. Then download the certificate for the item, Private key and the root CA of AWS IoT to your local computer and rename them with a shorter name. After that click "activation". Attention: you should add the additional policies.



2. Copy the certificates to the controller

1) You can use SCP to copy the generated certificates to the PLCnext controller. Please copy them to the directory "/opt/plcnext/certs/"

private.pem.key	2 KB	2023/8/14 9:54:28
certificate.pem.crt	2 KB	2023/8/14 9:54:29
AmazonRootCA1.pem	2 KB	2023/6/8 15:48:07

ca_path	STRING	本地	☐		STRING#'/opt/plcnext/certs/AmazonRootCA1.pem'
cert_path	STRING	本地	☐		STRING#'/opt/plcnext/certs/certificate.pem.crt'
key_path	STRING	本地	☐		STRING#'/opt/plcnext/certs/private.pem.key'

3. Update PLCnext Engineer project

1) Open the project of PLCnext Engineer, e.g. IIOT_TEST_AWS_PUB_4.pcwex. Open the programs variables list and find "ca_path", "cert_path" and "key_path". Set the iinitial values of these variables corresponding to the full path of the files on the

controller e.g. STRING#'/opt/plcnext/certs/certificate.pem.crt'

2) Replace the host_name by your own AWS account.

host_name	STRING	本地	☐	STRING#'a1ln6wa5mlce3f-ats.iot.us-west-2.amazonaws.com'
device_id	STRING	本地	☐	STRING#'AWS_good'
ca_path	STRING	本地	☐	STRING#'/opt/plcnext/certs/AmazonRootCA1.pem'
cert_path	STRING	本地	☐	STRING#'/opt/plcnext/certs/certificate.pem.crt'
key_path	STRING	本地	☐	STRING#'/opt/plcnext/certs/private.pem.key'

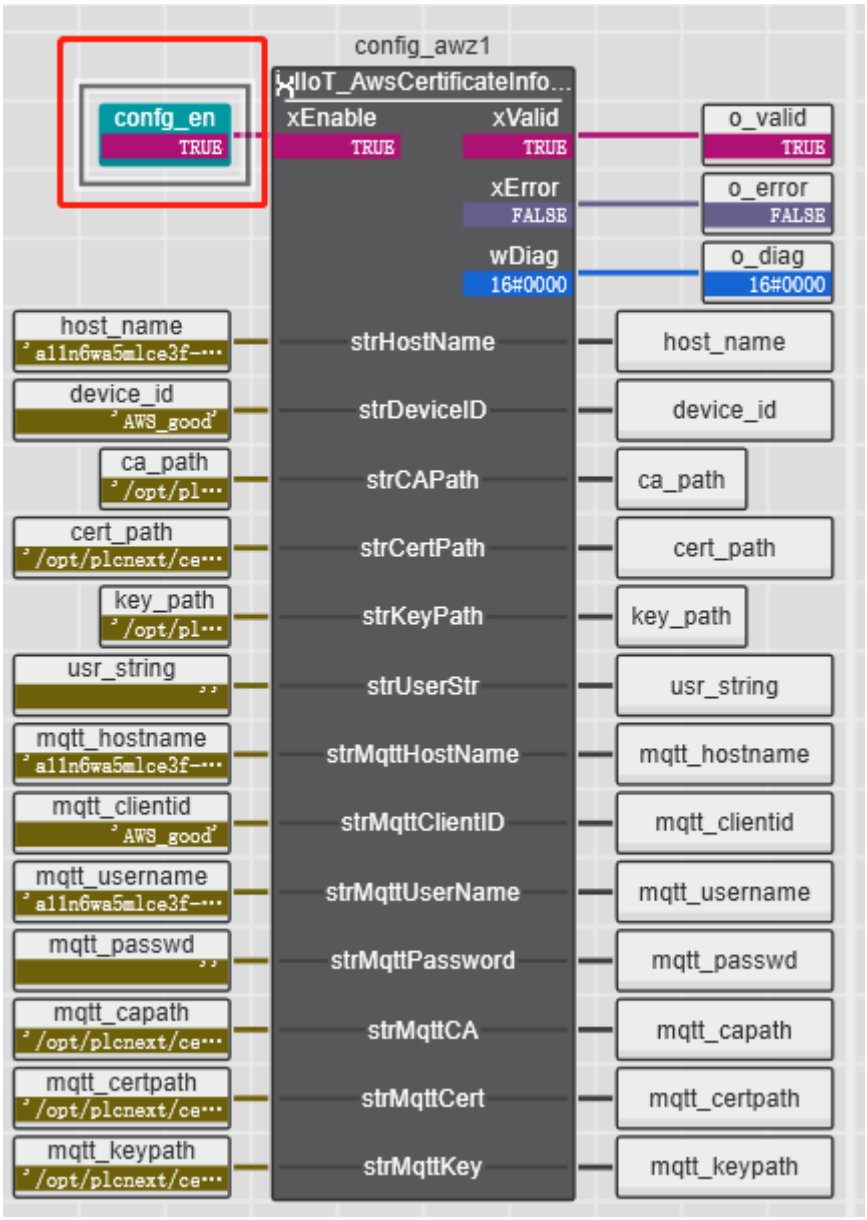
3) Connect to PLCnext and go into debug mode.

4. Connect to AWS cloud

1) Execute "Write And Start Project" by pressing F5 in the PLCnext Engineer project.

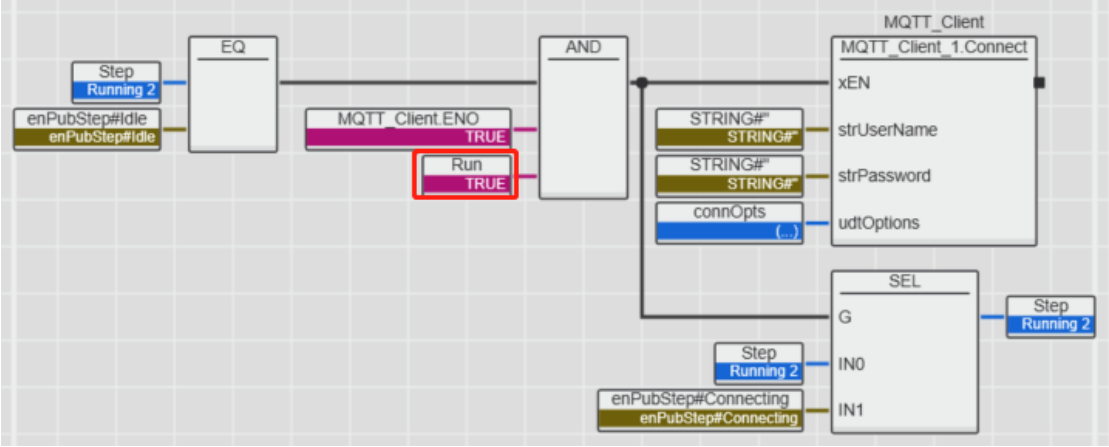
2) Open the FBD code worksheet and find the function block IIOT_AwsCertificataInfo_1.

3) Set the variable "config_en" to to TRUE. The variable o_valid shoult become TRUE which indicates that the certificate, the key and the CA are valid.



4) Find the MOTT_Client_1.Connect method. Set the variable "Run" to TRUE. The variable "Step" should become the value "Running 2" which means that the connect as been

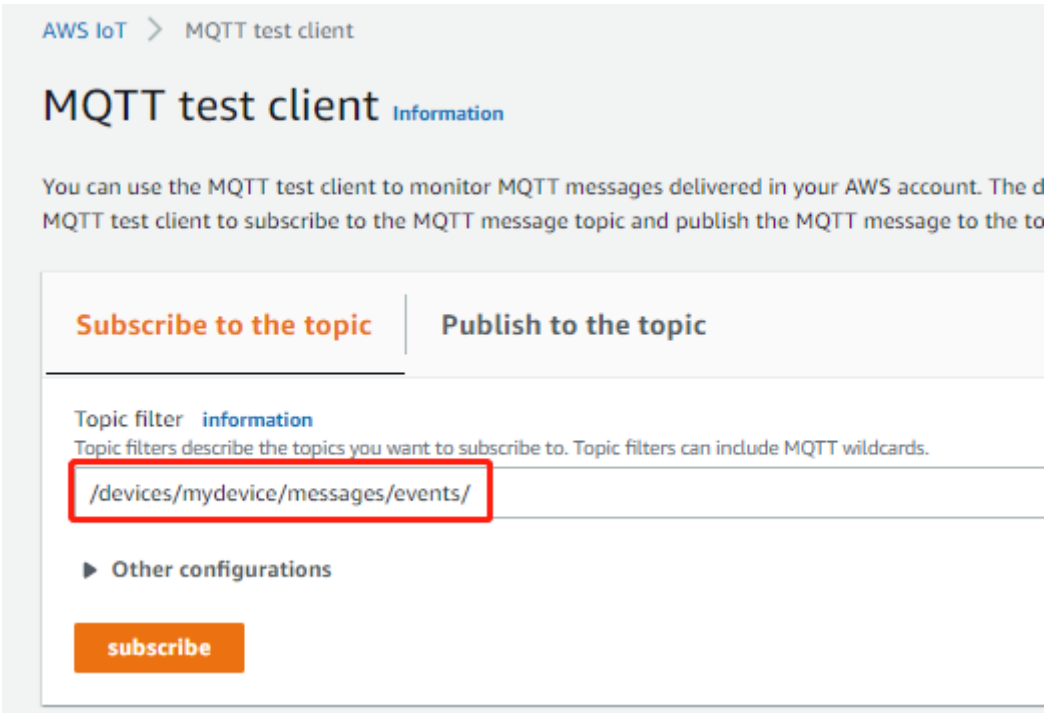
succeed.



5. Verification

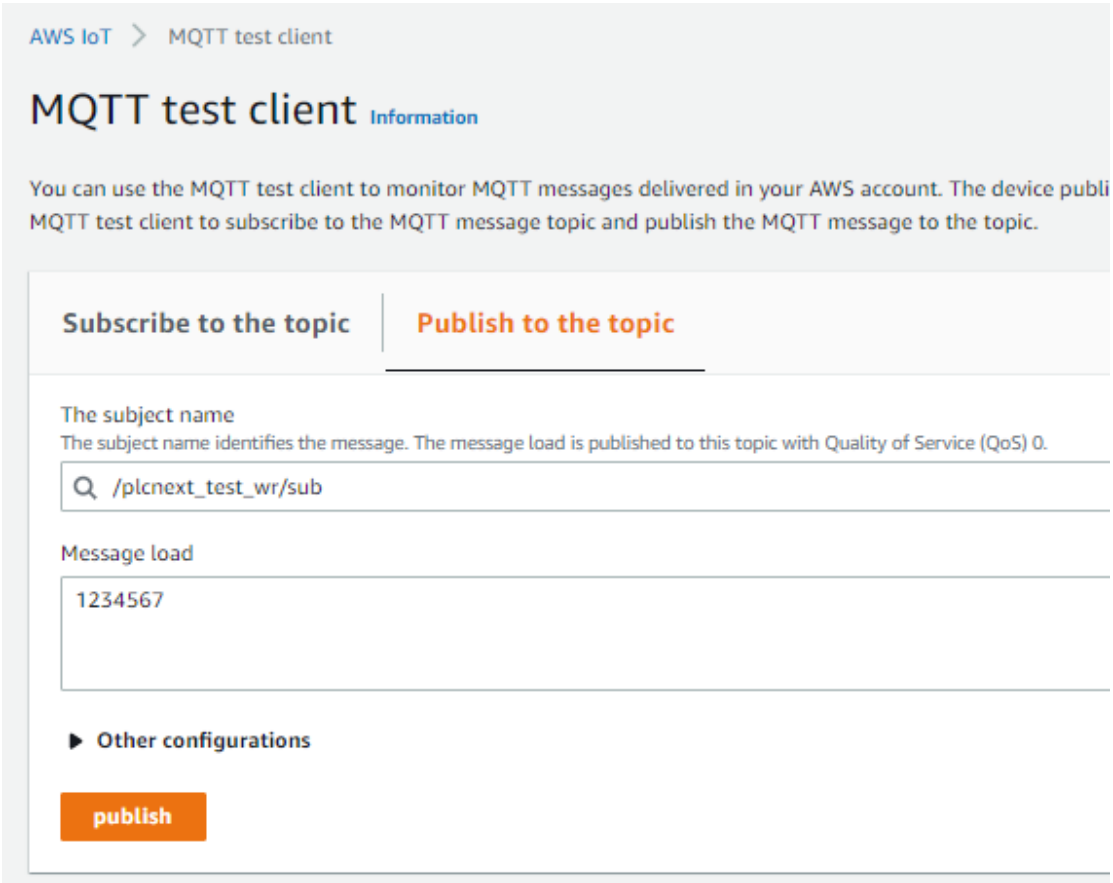
1) Open the MQTT test client in the AWS IoT. Copy the TOPIC value from the project to the AWS IoT. Press "Subscribe". After that you will receive the messages sent from PLCnext.

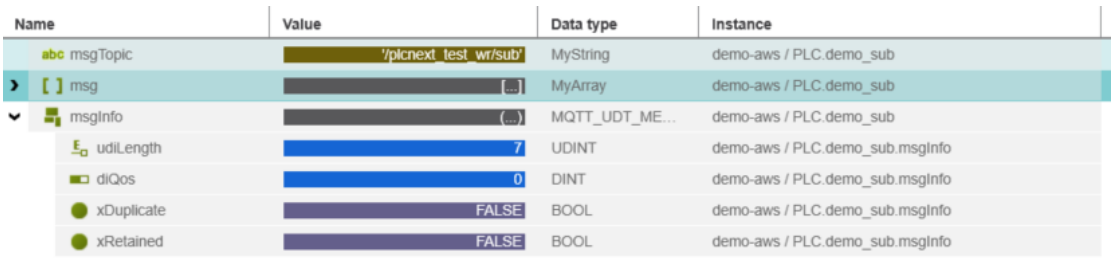
	TOPIC	STRING	Local	☐		STRING#'/devices/mydevice/messages/events/'



6. If you want to implement a subscribe-functionality in PLCnext, you can open the IIOT_TEST_AWS_SUB_2.pcwex project. Steps to run the project and establish the connection are the same.

In the Watch Window you can see three variables "msgTopic" "msg", which contains the received data, and "msgInfo".





Attention: If you have problems make sure your PC time is correct. Otherwise the certificate you have download are invalid.