Fibocom
PERFECT WIRELESS EXPERIENCE

MTC

Application Guide_Integrated Cloud

V1.0

Disclaimer

Any action you take in the course of using this document is at your own risk, and Fibocom shall not be liable for any damages or losses under any circumstances. Due to product version upgrade or other reasons, Fibocom reserves the right to modify any information in this document at any time without prior notice and any responsibility. Unless otherwise agreed, all statements, information and suggestions in this document do not constitute any express or implied guarantee.

This document may include the third-party information covering products, services, software, data, and so on. Fibocom does not control and assumes no responsibility for the third-party content, including but not limited to the accuracy, compatibility, reliability, availability, legitimacy, appropriateness, performance, non-infringement, and status update, unless otherwise specified in this document. Fibocom does not provide any guarantee or authorization for the third-party content mentioned or referenced in this document. If you need a third-party license, obtain it in an authorized or legal way, unless otherwise specified in this document.

Copyright Notice

Unless specially authorized by Fibocom, the recipient of the documents shall keep the documents and information received confidential, and shall not use them for any purpose other than the implementation and development of this project. Without the written permission of Fibocom, no unit or individual shall extract or copy part or all of the contents of this document without authorization, or transmit them in any form. Fibocom has the right to investigate legal liabilities for any offense and tort in connection with violation of confidentiality obligations, or unauthorized use or malicious use of the said documents and information in other illegal forms.

Trademark Statement

Fibocom The trademark is registered and owned by Fibocom Wireless Inc.

Other trademarks, product names, service names and company names appearing in this document are owned by their respective owners.

Contact Information

Website: https://www.fibocom.com

Address: 10/F-14/F, Block A, Building 6, Shenzhen International Innovation Valley, Dashi First Road, Xili Community, Xili Subdistrict, Nanshan District, Shenzhen

Tel: 0755-26733555

Contents

Applicable Model

No.	Applicable Model	Description
1	All MTC products	NA

Change History

V1.0 (2024-03-18)	Initial version.

1 Overview

This document is to guide the basic operations for connecting the current module to the cloud platforms.

2 Amazon AWS

AWS IoT provides cloud services to connect IoT devices to other devices or AWS. AWS IoT communication supports MQTT (Message Queuing Telemetry Transport) and HTTPS (Hyper Text Transfer Protocol).

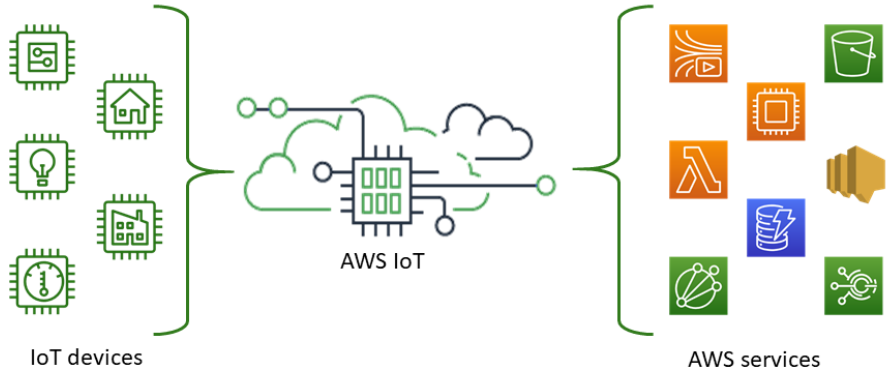

Figure 1. Amazon IoT cloud structure

2.1 Create an AWS Account

Before using AWS IoT Core for the first time, complete the following tasks:

- Register an AWS account.
  https://docs.aws.amazon.com/zh_cn/iot/latest/developerguide/setting-up.html#aws-registration
- Create a user and grant permissions
  https://docs.aws.amazon.com/zh_cn/iot/latest/developerguide/setting-up.html#create-iam-user
- Open the AWS IoT control panel
  https://docs.aws.amazon.com/zh_cn/iot/latest/developerguide/setting-up.html#iot-console-signin

If you already have an AWS account and an IAM user, you can use them and jump forward to open the AWS IoT control panel.

2.2 AWS IoT Account Configuration

After entering the AWS control panel, you will see the following interface. This interface contains all the portals of Amazon Cloud. Select **IoT Core** to enter.

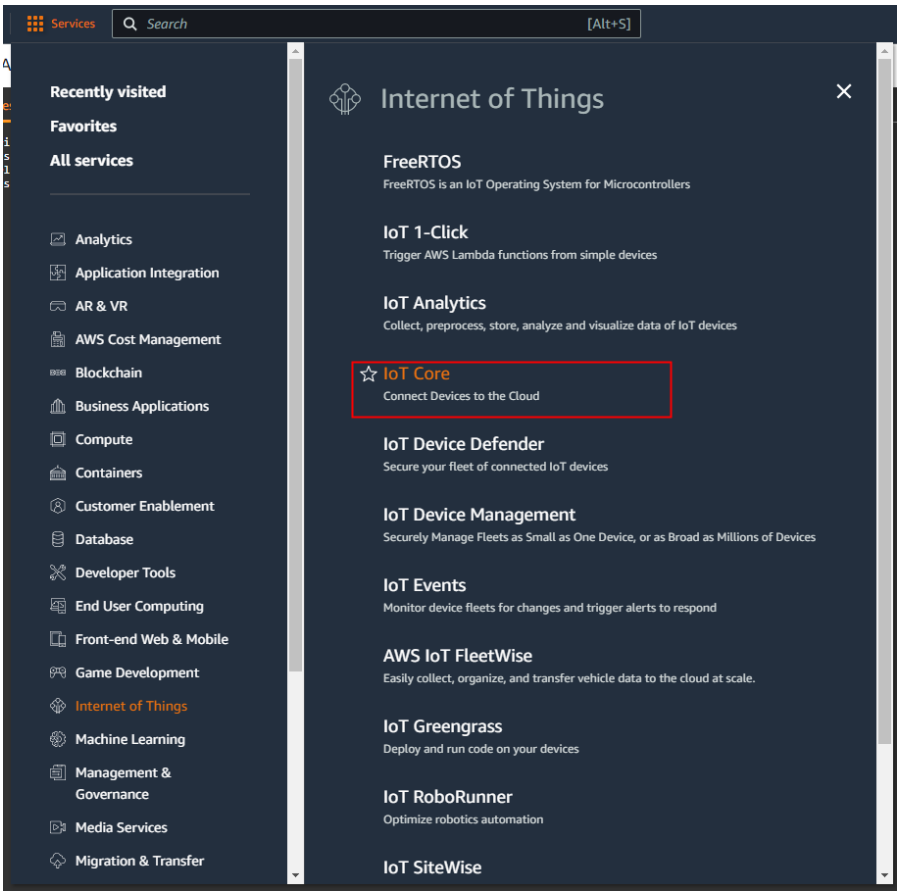

Figure 2. Amazon cloud control panel

The interface of AWS IoT is as follows:

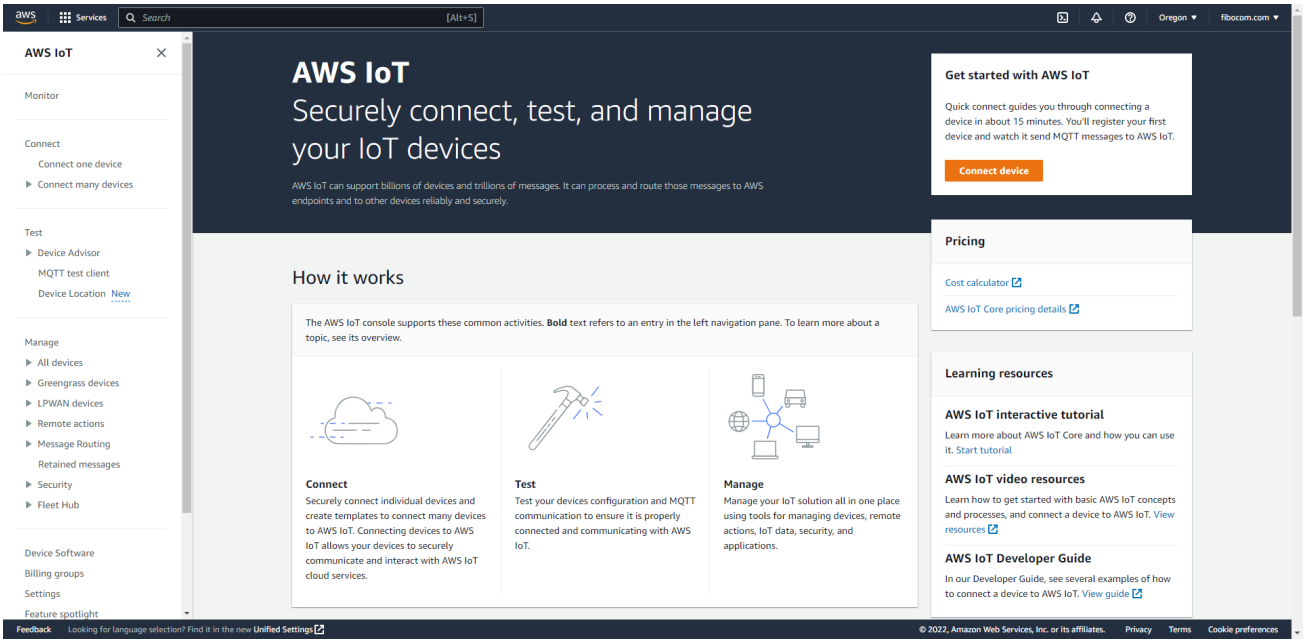

Figure 3. Amazon cloud IoT interface

Select **Manage** > **Things** to enter the Items interface, and click **Create things**. This interface is a list of devices to be created, as shown in the following figure.

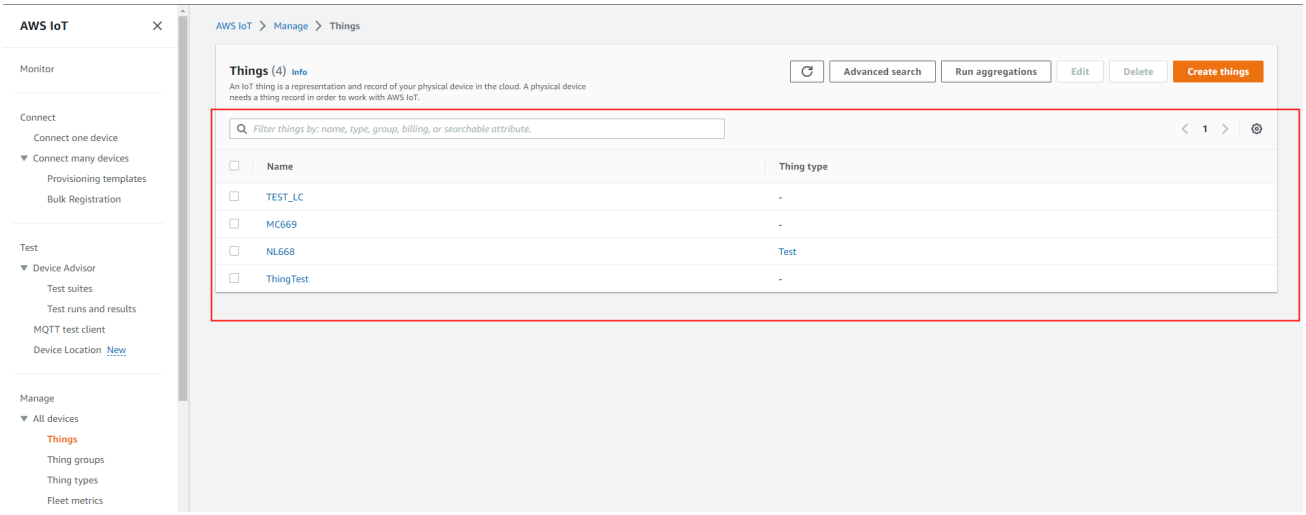

Figure 4. Amazon cloud device creating

2.2.1 Create Items

Enter the **Create things** interface, and select **Create single thing**, and click **Next**.

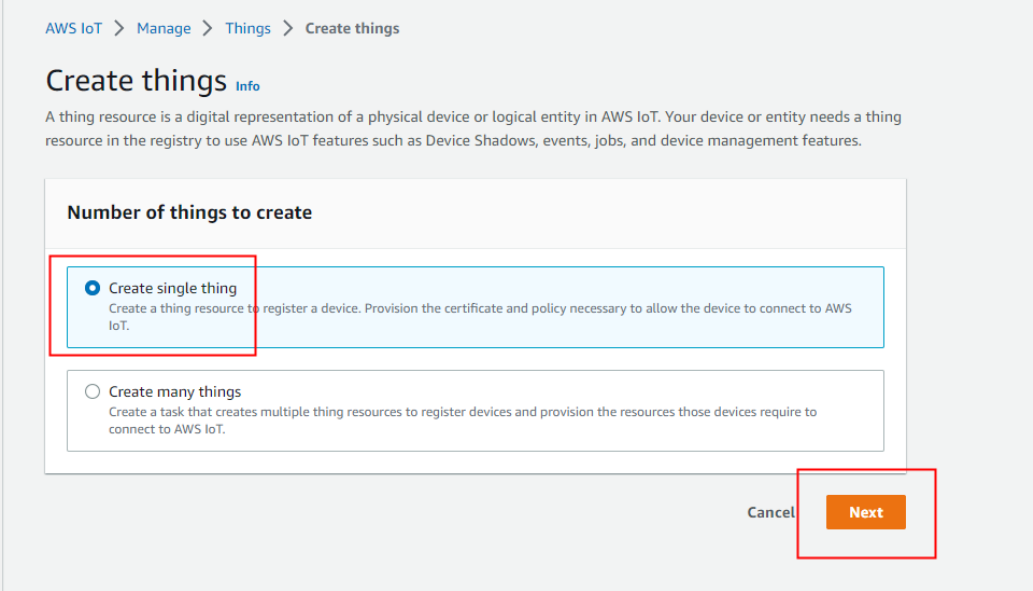

Figure 5. Creating single thing

In the interface of **Specify thing properties**, enter the thing name, for example, **fibocomTest**, and select the **Thing type**. If there is no creation type, you need to create types. Click the next step at the bottom page after creation.

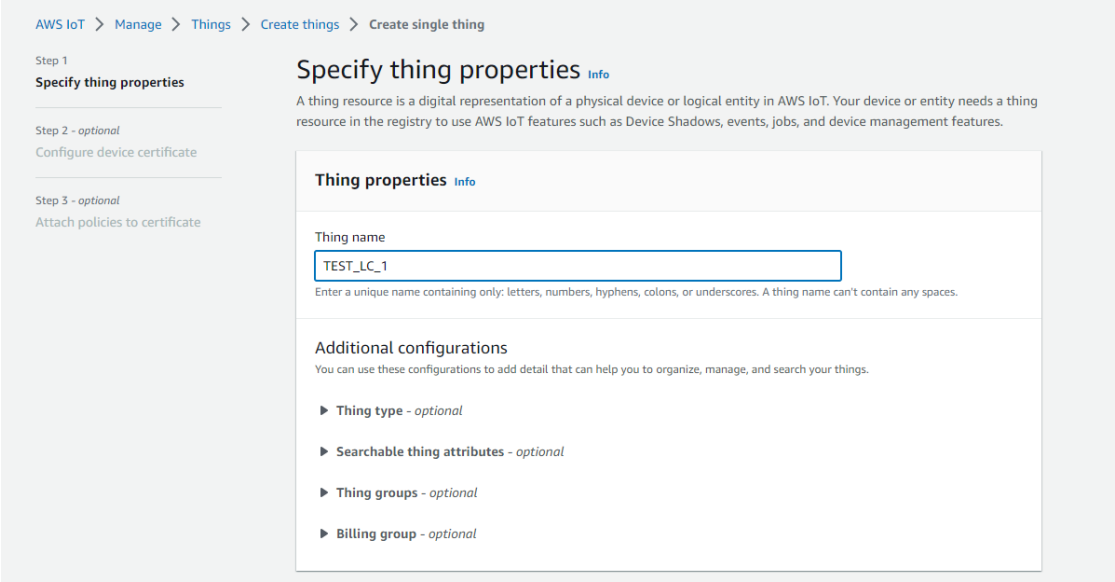

Figure 6. Creating thing

Create type interface: select **Create thing type** when you are finished.

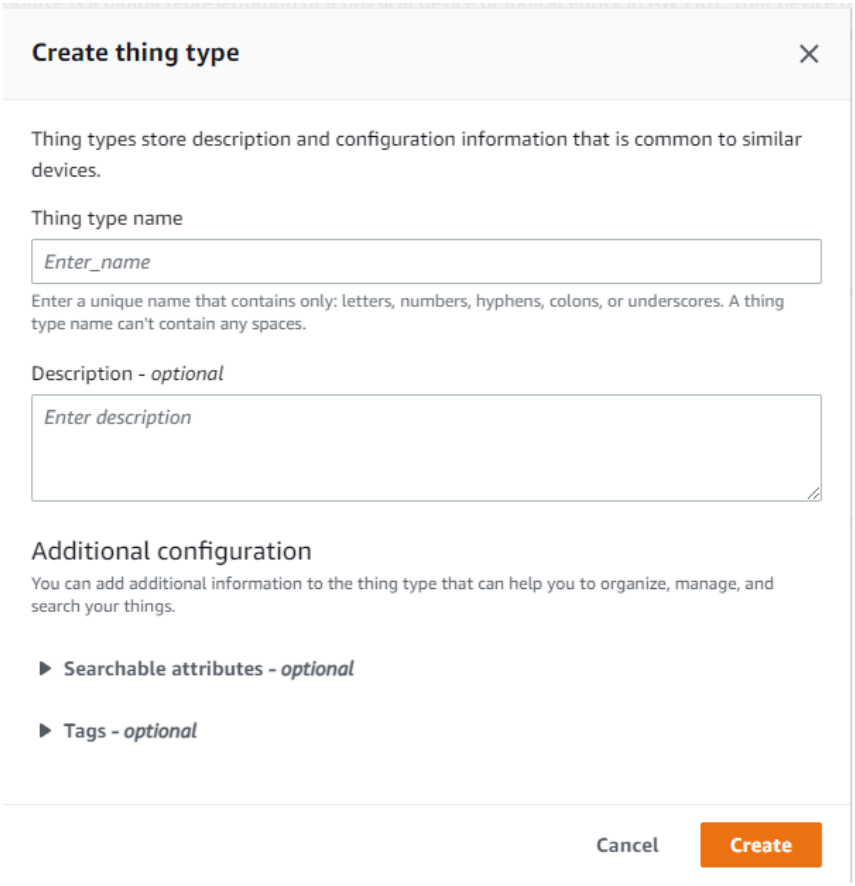

Figure 7. Creating thing type

Create item certificates.

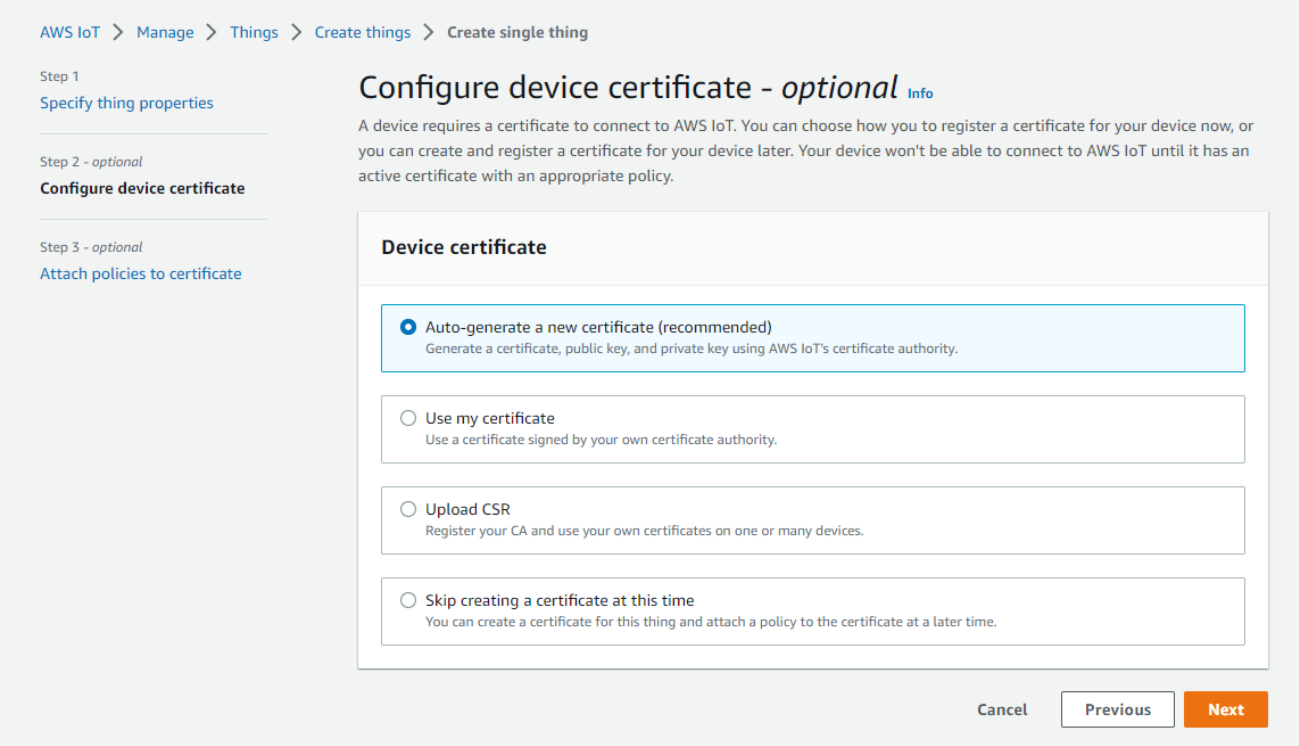

Figure 8. Configure device certificate

After the creation, it will display the created certificates.

1. Save the public and private key files of the certificates
2. Download the root certificates.
3. After the saving the certificates, click activate, indicating that the certificates are available.
4. After the activation, select additional policy to complete the creation.

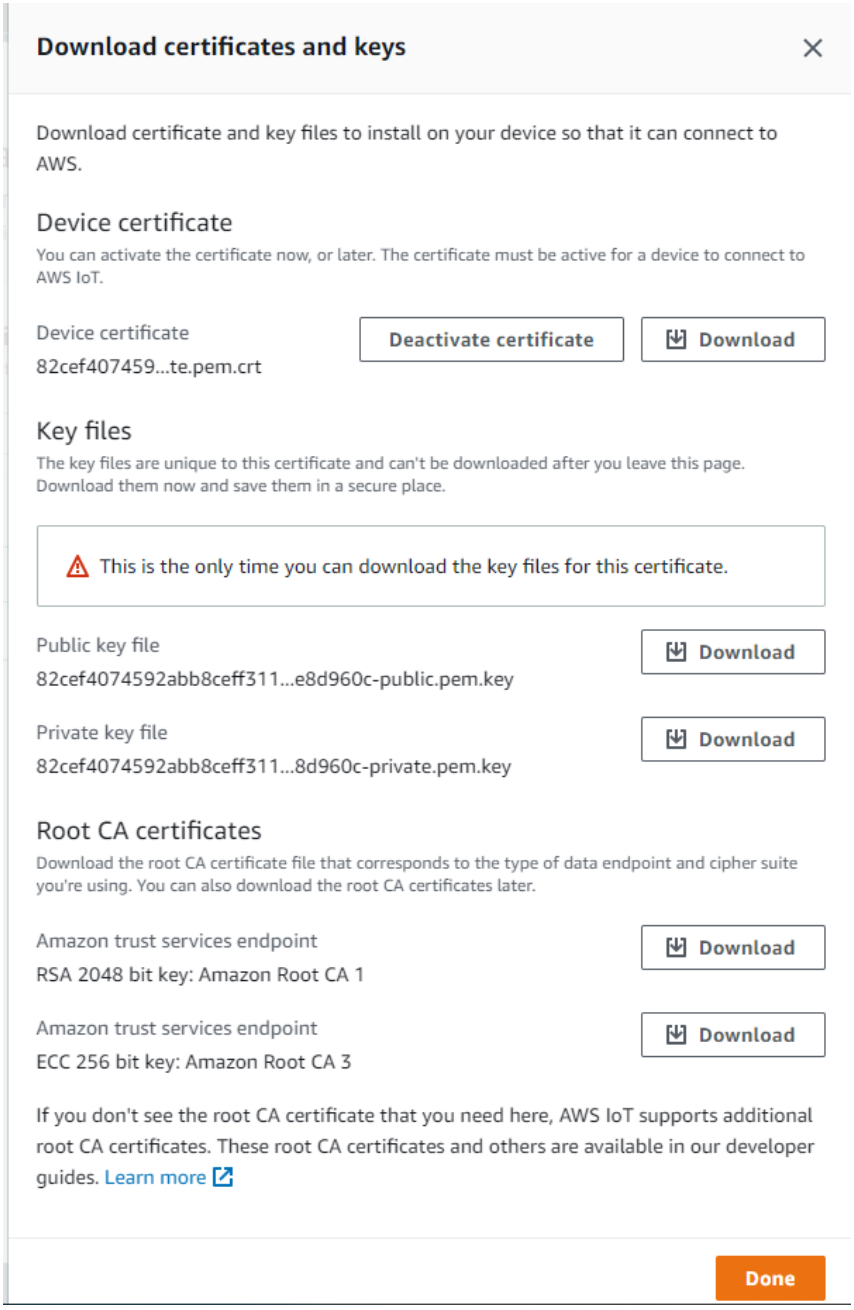

Figure 9. Saving and activating certificates

Register things.

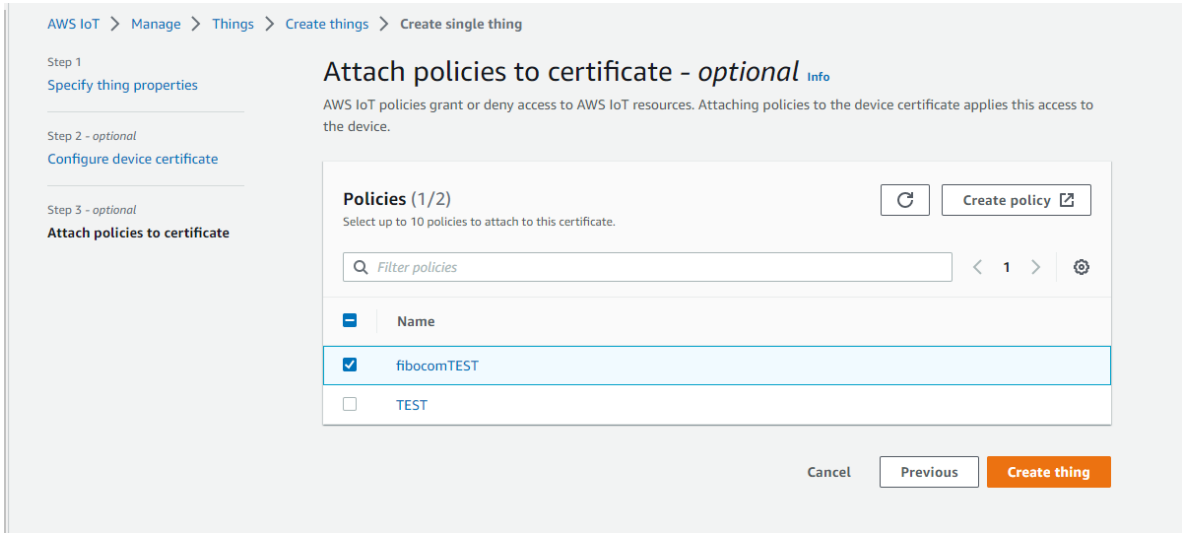

Figure 10. Thing creation completed

You need to select a policy here, and if there is no policy, you can omit it.

2.2.2 Create Policy

You need to configure the policy because Amazon cloud policy will affect the access logic. You can select policies on Amazon Cloud IoT homepage.

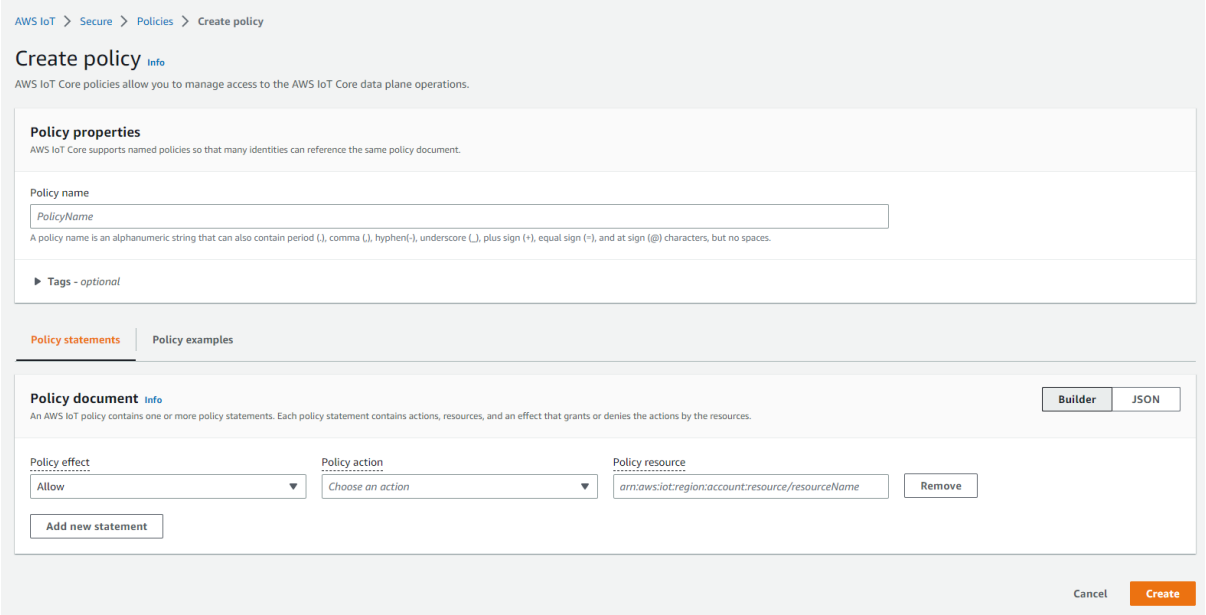

Figure 11. Policy creation

On the **Create Policy** interface, enter a policy name, and select advanced mode to write the policy configuration. Click **Create** after the configuration.

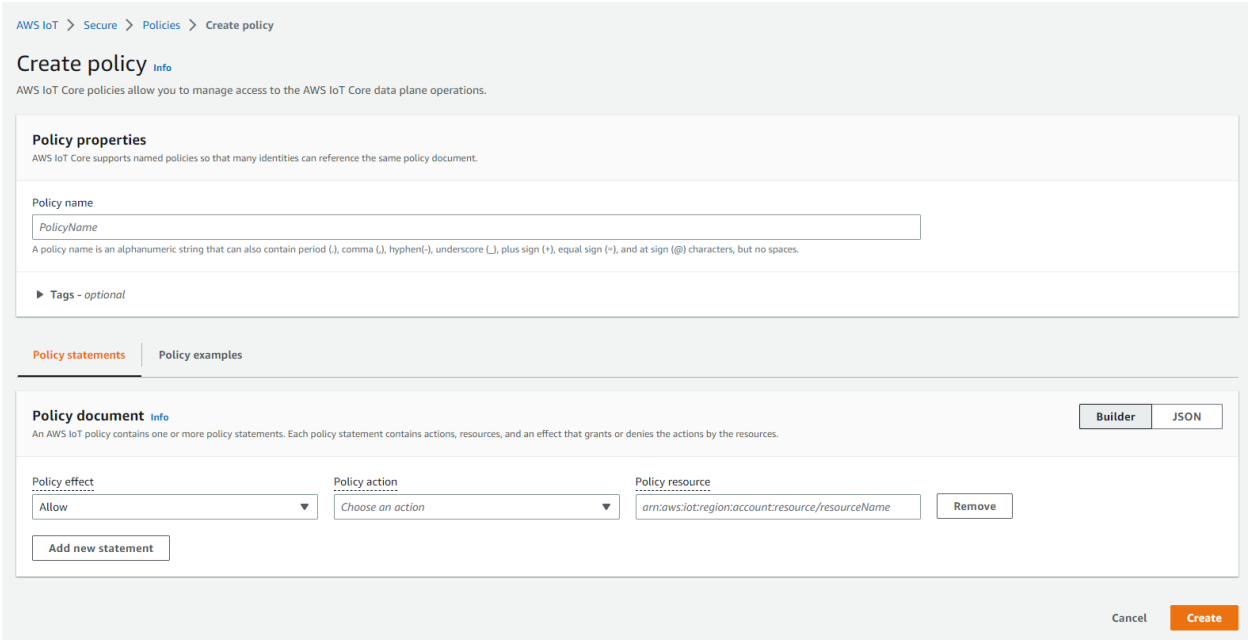

Figure 12. Policy statement

The policy used in the example is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Publish",
      "Resource": "arn:aws:iot:us-west-2:014957689912:topic/my/TEST"
    }
  ]
}
```

2.2.3 Certificate Attachment Policy

Select the certificate you have created on the **Certificates** interface, and enter the configuration page.

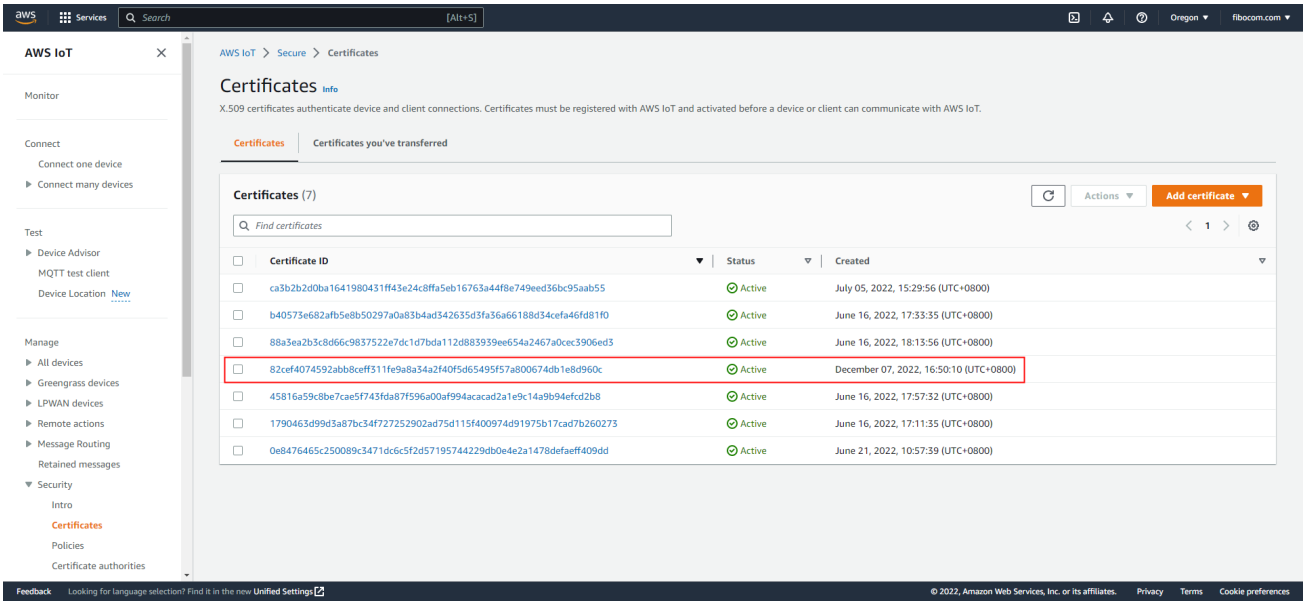

Figure 13. Selecting certificates

Choose **Actions** > **Attach to things**. Choose the created fibocomPolicy.

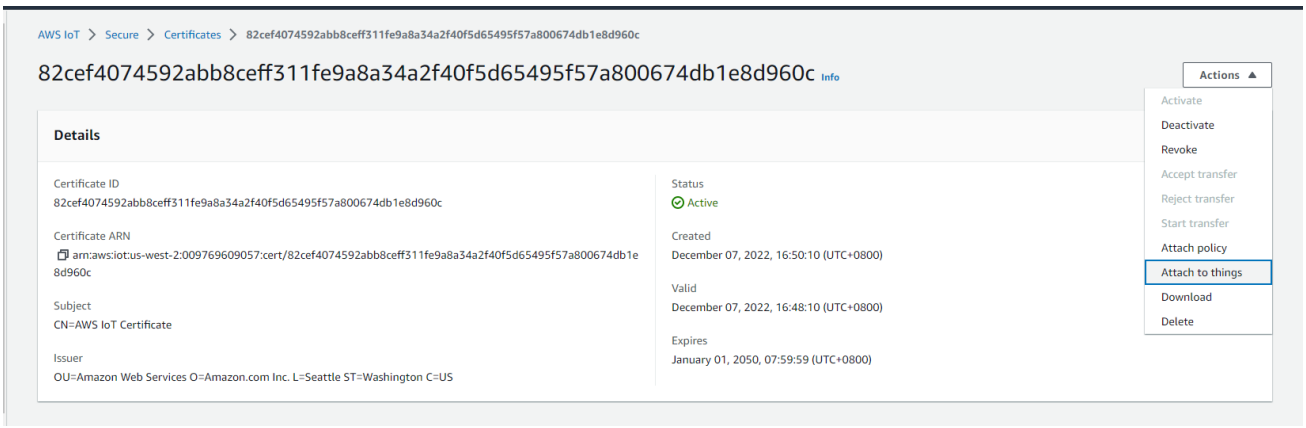

Figure 14. Attachment policy

Select the fibocomPolicy:

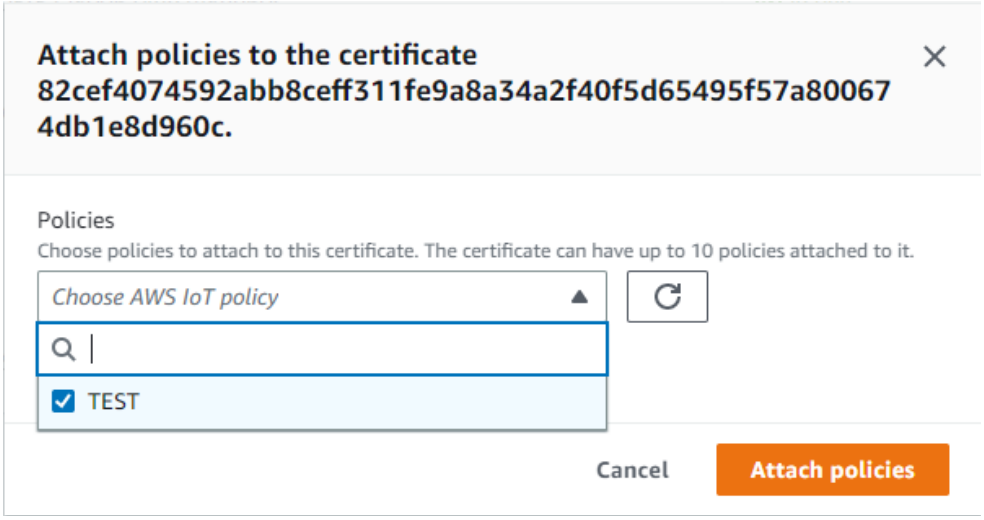

Figure 15. Attaching policies to certificate

After the above operations, the process of creating items, certificates and policies in Amazon Cloud has been completed. Items can be accessed normally.

2.3 Connection Example

```
AT                    // Send AT commands to the module continuously until the module returns OK.
AT                    // Echo. If the first AT command is a setting command, it's recommended to resend it after OK is returned.
AT command ready      // Active report upon startup; it indicates the module is ready, its time is not fixed, and it can be disabled using AT+MSTART.

+SIM READY        // Active report that indicates the SIM card is identified upon startup; its time is not fixed, and it can be disabled using AT+MSTART.

AT
AT                    // Echo. It can be disabled using ATE0. Subsequent echoes are omitted for brevity.
OK
// The baud rate adaptation may cause the first setting command to be invalid. ATE0 is not saved upon power-down but takes effect immediately.
ATE0                  // Disable echo.
ATE0
OK
AT+GTRAT=6,3,2       // Prioritize LTE in the network search sequence.
OK
AT+CFUN=1             // Set the operating mode to normal operating mode.
```

```
OK
AT+CPIN?              // Check whether the SIM card is identified.
+CPIN: READY       // READY indicates that the SIM card is identified. If it’s ERROR, the SIM card may not be identified or may require a PIN to enter.

OK
AT+CIMI?            // Query IMSI
+CIMI: 460027295794151

OK
AT+CGDCONT=1,"IP","cmnet"  // Set the APN first.
OK
AT+CSQ?               // Confirm the current signal strength.
+CSQ: 25,99           // 25 indicates the reference value of signal strength.

OK
AT+COPS?            // Query operator information.
+COPS: 0,0,”CHINA MOBILE”,7   // 7 indicates 4G.

OK
AT+CGREG?        // Query whether the PS domain is registered. For 4G SIM card, it's recommended to run the AT+CEREG? command to check again.
+CGREG: 0,1          // The value 1 or 5 indicates the SIM card is available.

OK
AT+CGREG?        // Query whether the LTE is registered.
+CEREG: 0,1          // The value 1 or 5 indicates the SIM card is available.

OK
AT+CREG?         // Query whether the CS domain is registered; this command can be ignored if the CS domain related services are not required.
+CREG: 0,1           // The value 1 or 5 is returned. // The value 1 or 5 is returned.

OK
AT+MIPCALL?
+MIPCALL: 0

OK
AT+MIPCALL=1          // The module works with the network to activate PDP and requests
```

```
IP address from the operator.
OK                    // Due to the influence of network environment, an OK response
does not indicate the end of processing, and it indicates the processing.

+MIPCALL: 10.119.166.56  // Subsequent operation can proceed only after receiving
+MIPCALL or ERROR or timeout.
AT+MIPCALL?           // Query whether the IP address has been obtained.
+MIPCALL: 1,104.48.68  // If 1 is returned, an IP address is assigned.

OK



AT+GTSSLFILE= "TRUSTFILE", 1188 // Configure the root certificate.
>
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
b24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
9O6II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
VOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
93FcXmn/6pUCyziKrlA4b9v7LWIbxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
A4IBAQCY8jdaQZChGsV2USggNiMOruYou6r4lK5IpDB/G/wkjUu0yKGX9rbxenDI
U5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
N+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
o/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
rqXRfboQnoZsG4q5WTP468SQvvG5
-----END CERTIFICATE-----

OK

AT+GTSSLFILE= "CERTFILE", 1220// Configure the cert file.
>
```

```
-----BEGIN CERTIFICATE-----
MIIDWTCCAkGgAwIBAgIUUge6GqtXTDaOV6+ZoJVnaIjFuUQwDQYJKoZIhvcNAQEL
BQAwTTFLMEkGA1UECwxCQW1hem9uIFdlYiBTZXJ2aWNlcyBPPUFtYXpvbi5jb20g
SW5jLiBMPVNlYXR0bGUgU1Q9V2FzaGluZ3RvbiBDPVVTMB4XDTIwMTIzMDAzMDEy
NloXDTQ5MTIzMTIzNTk1OVowHjEcMBoGA1UEAwwTQVdTIElvVCBDZXJ0aWZpY2F0
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOzols0WJTAzUAjtVRU5
gKAFWiwfEN9mi9fQjCrfDInRe+EzTvpwrR7/KF2yPWdNh2H5pwpH3Lvw2jBq+o8J
LrtXkFNaUwl0LflMco0Vl6JvxmPhrpkh8aIW0+rolgpjUtcM/bhDTSaV0BsNQNbK
qjspP/OxUdUWsnVlXNZLuoM+r51AC2ywPsPC7MURG5I0ibYoPx5P+AidaafTBqk/
37+1utwBBWoRPUwESCIRzVRcZOcBWu7d87/FBUfcYzBdNbOIxpxasdAhZM+ayWh7
Kd0aRnXgUfZzqtxuWRMbf8WsiGdD3UDsmlzxq3AmRiMkToqBfboM2Yw7ggHp2e/z
ssUCAwEAAaNgMF4wHwYDVR0jBBgwFoAUsdG/NaSspjIj4aD8t8FbGKtuMLQwHQYD
VR0OBBYEFBt0zxEPXjlK21bI9PSVkqpx3+B/MAwGA1UdEwEB/wQCMAAwDgYDVR0P
AQH/BAQDAgeAMA0GCSqGSIb3DQEBCwUAA4IBAQClBB4ExyncVzFzAwgfbbJidZCS
baiaKvkr8lpsSYQVlD6Eqei3Ng3IgZ066N8moxE8WBAQ2MEnbM1LRvCgthJXzns/
4js8fWcHQh5VPxCTkPYXgWs81njwZzFFBRn/xSOoeAl0PKUWzQTFqx9Fd9S+4X3l
kiuMHPS+Jk9LLlmpy/HsDlmPSmDrSpcBsdR27NBE083PLPdZo8j0RCIISIXEQtbV
huzyatQXBXacpZcf6r8O0CnpbI/dg9fS/NzXDaybrqxZxzM/RtcD9+NYtZ4DRGNq
qXdFQu5gtpEX3q9O5vitrjN8jpZEzKWeuSoGaekNf6z4bM681UMIhDvlp68Z
-----END CERTIFICATE-----
OK

AT+GTSSLFILE="KEYFILE",1679 // Configure the private key file.
>
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA7OiWzRYlMDNQCO1VFTmAoAVaLB8Q32aL19CMKt8MidF74TNO
+nCtHv8oXbI9Z02HYfmnCkfcu/DaMGr6jwkuu1eQU1pTCXQt+UxyjRWXom/GY+Gu
mSHxohbT6uiWCmNS1wz9uENNJpXQGw1A1sqqOyk/87FR1RaydWVc1ku6gz6vnUAL
bLA+w8LsxREbkjSJtig/Hk/4CJ1pp9MGqT/fv7W63AEFahE9TARIIhHNVFxk5wFa
7t3zv8UFR9xjMF01s4jGnFqx0CFkz5rJaHsp3RpGdeBR9nOq3G5ZExt/xayIZ0Pd
QOyaXPGrcCZGIyROioF9ugzZjDuCAenZ7/OyxQIDAQABAoIBAALHo+VaKiuLnpfM
OSBboV+/UFSONMN6T4/DubFTFrGTTLHSyU10/wMLGW0oB0JsDXef107uku99nwHM
b444HF1EZMQlni3ROCzhscJoC3RzfU90uXjAhjZRsEDkY8ZRbgpp85wy5ffa8Csx
F56tmBvDmyV/4ibu8j8gZlt5XgHmN59dSg7SA2VRVlLvtO04SF8yiTGjBue/at8c
ex2VuSzkh3tvRvEtujhIgDrHsDEgLzmMWLCwEMl4cUB4NIuLOQzJmVR+3oAp2ToG
GPEqMgTOes8BMF53QASIrLSAXByuOmnHaH3u6321wjeVersHdQfZyXFfGEBN8Yz7
xY+p0E0CgYEA/B0/4qbeECMSLL+l3uJWQNHLMnYUI3e2xxk5DL9b/QZv9kigkyfi
DEdtfLc489gjCpHd+RNipnbECnv9PffYyzDj1fNEklAVSy8s50Y4br4DEJ/QTcbI
```

```
MdvGKyi1NKkDux3m/gUUJbZ3HBsuUpg6wqHyLro3D3n6V0uC29YxgwsCgYEA8I9X
53zka3AtCn/qc06Xg1KVgxys1fj9u1k4XG4a5NlUSmnYKjNQWUuW9O+zkvjvqlFJ
QOONdA5WS2MwXjrsv7qwODPW35KSy3ANBVV7Q0bfaUZAKZX/M9TRC+a3URc4QCJ5
FA0aOoQbX/IyxRmp8VckrtJhu5+sE28N7U+QQ28CgYA4mXRzNNUbuFPnOetKG3QT
v0WoAXxJ7iFZl18Ibpl/N4fBOdLa1pRX/10kJ5ognEBZqh+0QFbgWj9uvyE+XTsN
et9bc+7MDjCJnYCuN0SKEBxuCgLgwyTElLtriwsLVHpi8raeBpPcV5dr9uoyXryq
X2MYfHPKBK9gE7LAGdkpuwKBgQCz0aLXAm/Is/CnQZkimmP9oVTrzhqQU/BvBDFy
PkfSO3abrWUNno/4P93Wt/tW6MhWWy7T14VcdH8jGUEFnyxr4YRqbq23L9yVP+wr
yYs7bhYAnqfFrj83ImUlbVAoyJ+eqWYyi9zIUwoXfXdgCGAVbJuaJt8xnhjF6iTR
+MCQ9wKBgQDHQqNz6uZlnQwA58+krdAc7QrpqZHOkWYj8WaQC5GY/lkitkmMIYBZ
JVfYE5TYQ+Q0hoywhV49I4EXEvZ8BPQ51eyREbQhzVLAPG4PfB9yKKftn5SAtkTi
5Ua6x4rSxj6x/8hfsk6+AkP3YyiwcW9U5jjxu0F8MfXtvUMOMD1pQQ==
-----END RSA PRIVATE KEY-----

OK

AT+GTSSLMODE=1 // Set up authentication server certificates.
OK

AT+MQTTUSER=1, "", "", "test” // Configure authentication information. Amazon Cloud
uses certificate connection, so name and password are empty.
OK

AT+MQTTOPEN=1,"aqb3vda67tst3-ats.iot.us-west-2.amazonaws.com",8883,1,300,2        //
Establish a connection.
OK

+MQTTOPEN: 1,1: // Connection succeeded.

AT+MQTTSUB=1, "my/TEST", 0 // Subscribe to messages.
OK

+MQTTSUB: 1,1                // Subscribed successfully.

AT+MQTTPUB=1,"my/TEST",0,0,"11111111" // Subscribe to messages.
OK

+MQTTPUB: 1,1                // Published successfully.
```

```
+MQTTMSG: 1,0,"my/TEST","11111111” // Received the published messages.

AT+MQTTCLOSE=1 // Disconnect from the server.
OK

+MQTTCLOSE: 1,1 // Disconnection succeeded.
```

3 Alibaba Cloud

Alibaba Cloud IoT platform, used as a device management platform, manages a large number of IoT devices to realize uplink and downlink data sending and receiving.

3.1 One Secret for One Device Authentication

One secret for one device authentication is to burn the unique certificate (ProductKey, DeviceName and DeviceSecret) for each device in advance. The IoT platform authenticates the device certificate information of the device when it is connected with the platform. After the authentication is passed, the device is activated and communicates with the IoT platform.

One secret for one device authentication for its high security to be recommended.

Before one secret for one device authentication, you should create products and devices. Select **Products** > **Create Product** on Alibaba Cloud menu page. Select **Directly Connected Device** for **Node Type** and **Device Secret** for **Authentication Mode**. The results are as follows:

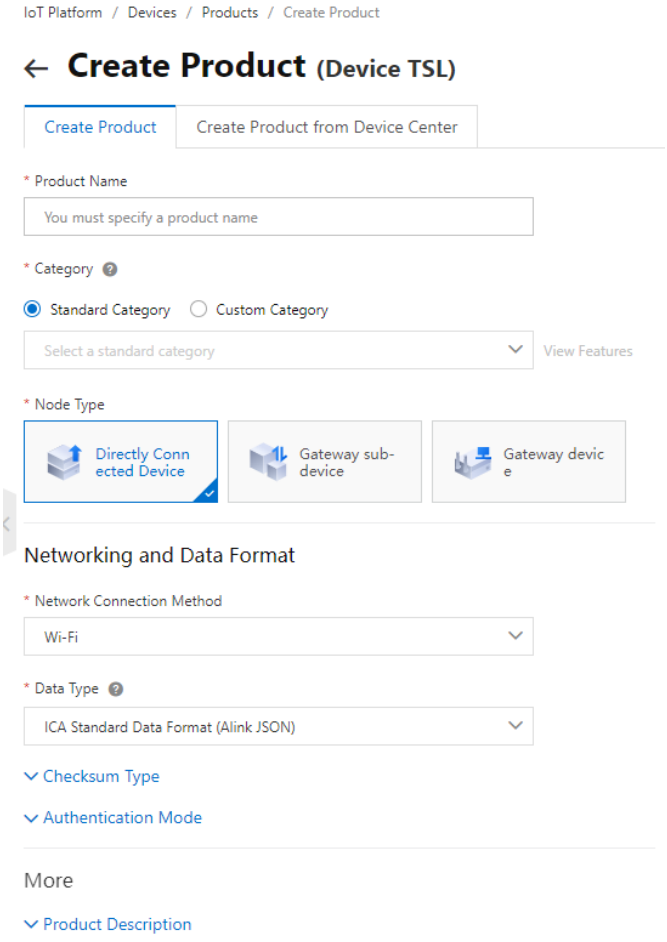

Figure 16. Creating device

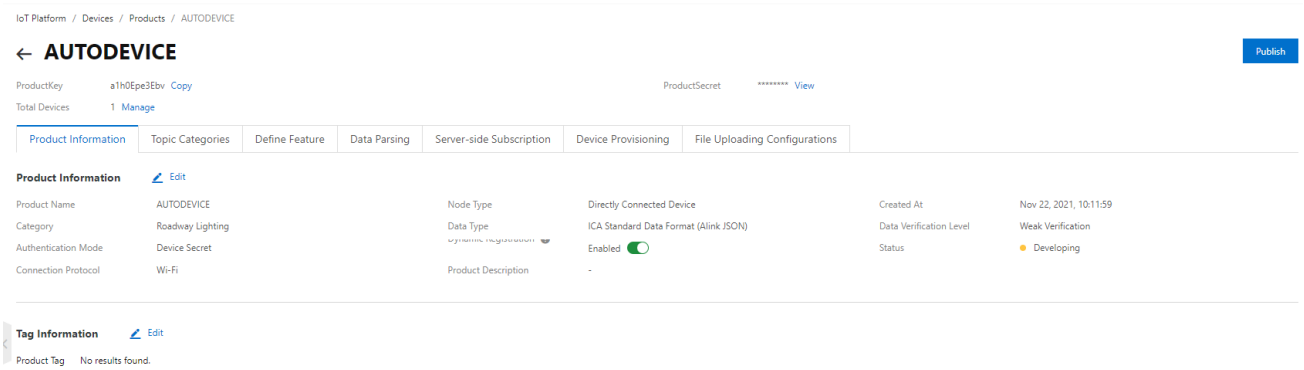

Figure 17. Product details

You can get the ProductKey and ProductSecret information on the product page, and then select **Devices** > add devices from the menu to create devices for the related products. The result is as follows:

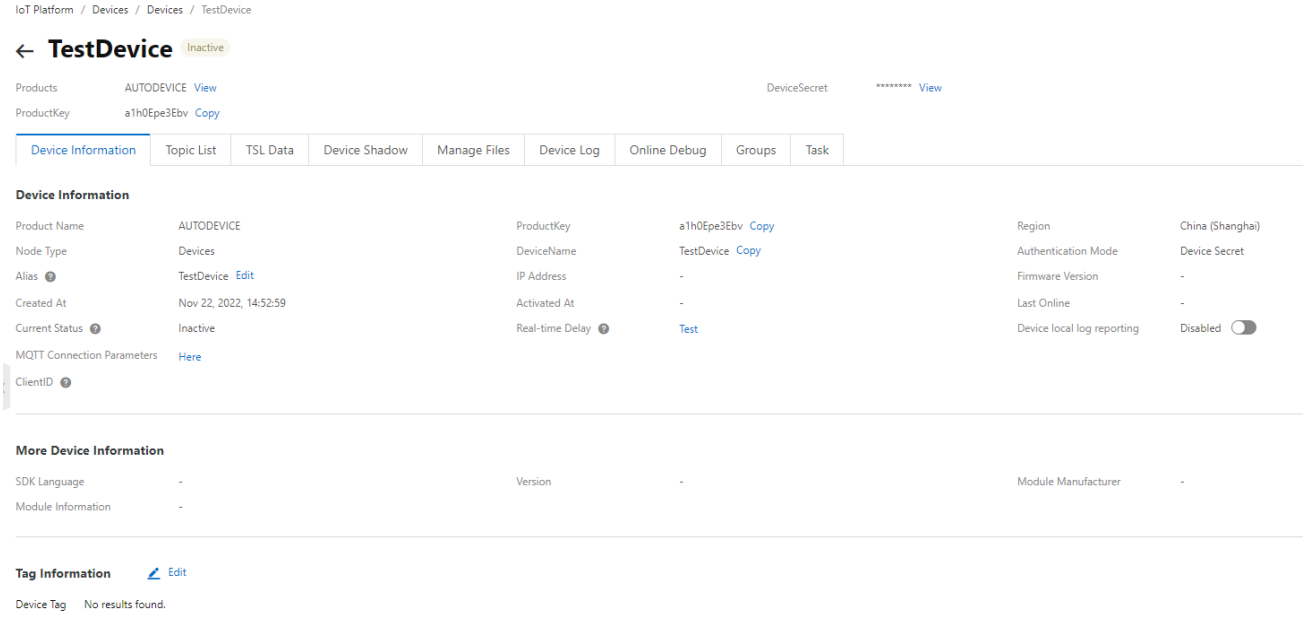

Figure 18. Device details

You can obtain the connection parameters of ProductKey, DeviceName, and DeviceSecret from the product page.

3.2 One Secret for One Type Authentication

In the one secret for one type authentication, all devices under the same product can burn the same device information, that is, the same product certificates (ProductKey and ProductSecret) that all devices contain. When a device sends an activation request, the IoT platform will confirm its identity and deliver the information required for the device access after it passes the authentication.

One secret for one type authentication supports two ways of use: free pre-registration (not supported at present) and pre-registration. The following figure describes the comparison.

Before one secret for one type authentication, you should create products and devices. Select **Products** > **Create Product** on Alibaba Cloud menu page. Choose **Directly Connected Device** for **Node Type** and **Device Secret** for **Authentication Mode**. The results are as follows:

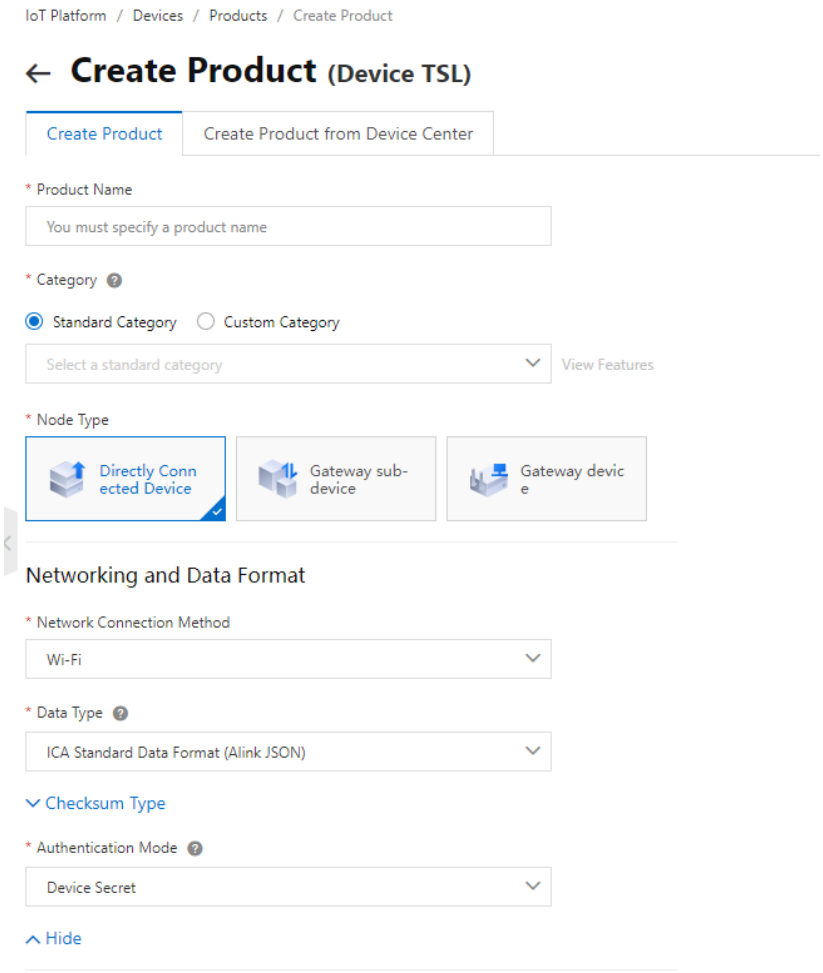

Figure 19. Creating product

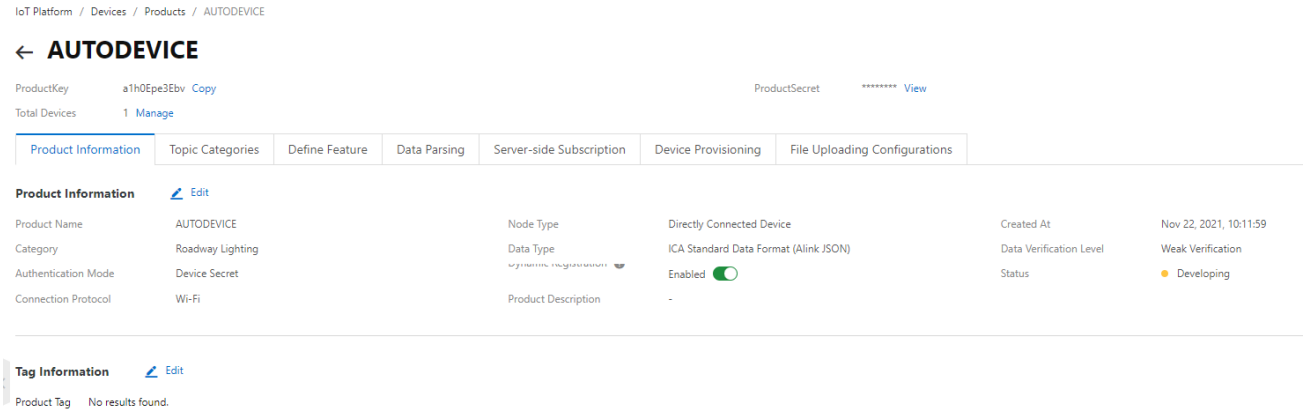

Figure 20. Product details

You can get the ProductKey and ProductSecret information on the product page, and then select

Devices > add devices from the menu to create devices for the related products. The result is as follows:

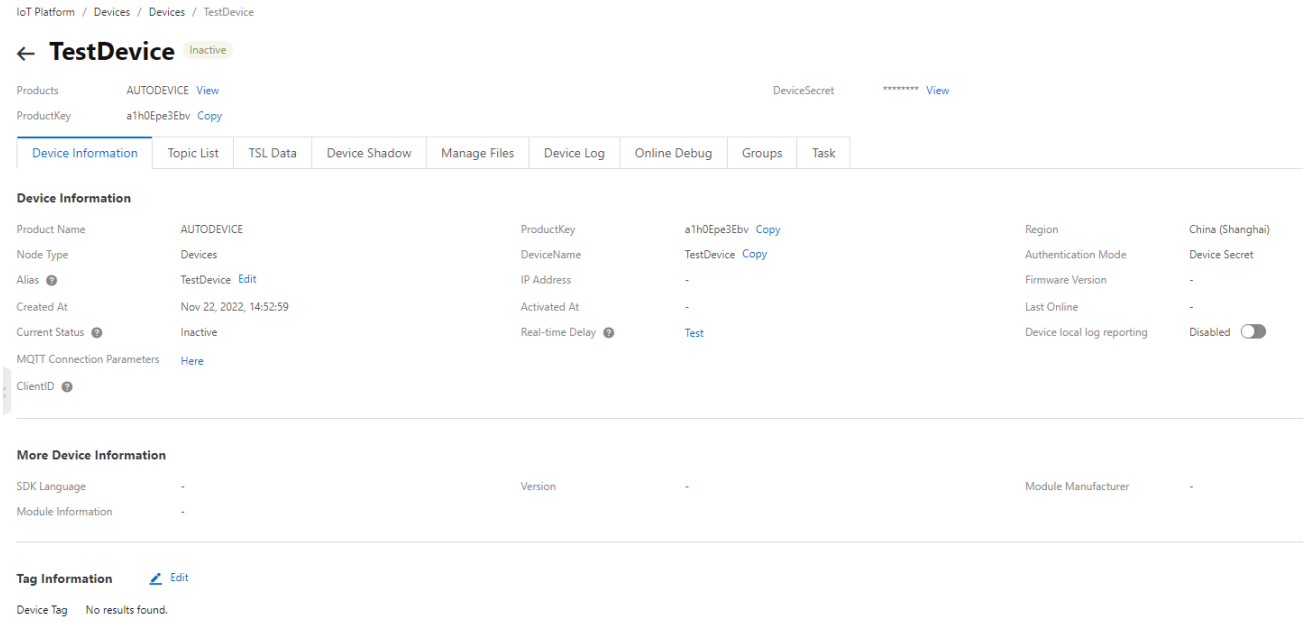

Figure 21. Device details

You can obtain the connection parameters of ProductKey, DeviceName, and DeviceSecret from the product page.

3.3 Connection Example

3.3.1 Unencrypted Connection of One Secret for One Device Authentication

```
AT+MIPCALL=1,"CMNET"    // Request the operator to allocate an IP.

OK


+MIPCALL: 10.32. 232.1 // The return value is the IP address assigned by the operator.


AT+MQTTAUTHCFG=1,"a1Q0oULxrcp","TestDevice1","08ca857ade24c35ee06e37d225337599",0   // Obtain the cloud parameter configuration. The parameters are: cloudtype, ProductKey, DeviceName, DeviceSecret, and tls.

+MQTTAUTHCFG: 1,"TestDevice1&a1Q0oULxrcp","872ACD7B4758A99929B4CB58E5121B280C3F1C0D42B78492F62DE5CB1E9970D8","TestDevice1|securemode=3,signmethod=hmacsha256,timestamp=946745780|”     // The return value parameters are cloudtype, Username, Password, and ClientID Str.


OK
```

```
AT+MQTTUSER=1,"TestDevice1&a1Q0oULxrcp","872ACD7B4758A99929B4CB58E5121B280C3F1C0D42B
78492F62DE5CB1E9970D8","TestDevice1|securemode=3,signmethod=hmacsha256,timestamp=946
745780|”                // Set MQTT authentication information with the following parameters: Client ID,
Username, Password, and ClientIDStr.

OK


AT+MQTTOPEN=1,"iot-as-mqtt.cn-shanghai.aliyuncs.com",1883,0,300

// Establish an MQTT connection with the following parameters: Clientid, Remote IP/URL, RemotePort,
Cleanssession flag, and Keepalive time.

OK


+MQTTOPEN: 1,1          // MQTT connection established successfully.


AT+MQTTCLOSE=1          // Close MQTT connection.

OK


+MQTTCLOSE: 1,1             // MQTT connection closed successfully.
```

3.3.2 Pre-registration of One Secret for One Type

```
AT+MIPCALL=1    // Request the operator to allocate an IP.

OK


+MIPCALL: 100.104.156.37 // The return value is the IP address assigned by the operator.


AT+MQTTAUTHDYN=1,"iot-as-mqtt.cn-
shanghai.aliyuncs.com",1883,"a1klgAXldch","HPoiKreay5vmZEHJ","867567040119311"

// Dynamic authentication with the following parameters: cloudtype, Host, Port, ProductKey,
ProductSecret, and DeviceName.

OK


+MQTTAUTHDYN: 1,"a1klgAXldch","867567040119311","35057b24c65af058985d07cae8dcc2f8"

// The return value parameters are cloudtype, ProductKey, DeviceName, and DeviceSecret.


AT+MQTTAUTHCFG=1,"a1klgAXldch","867567040119311","35057b24c65af058985d07cae8dcc2f8",
0       // Obtain the cloud parameter configuration. The parameters are: cloudtype, ProductKey,
DeviceName, DeviceSecret, and tls.
```

```
+MQTTAUTHCFG:
1,"867567040119311&a1klgAXldch","26FD8D31AE53274507D43D4F5F8436004325AD8B78C5AFA1BFE
9742FD32BB490","867567040119311|securemode=3,signmethod=hmacsha256,timestamp=1631931
961|"
```

// Set MQTT authentication information with the following parameters: Client ID, Username, Password, and ClientIDStr.

```
OK
```

```
AT+MQTTUSER=1,"867567040119311&a1klgAXldch","26FD8D31AE53274507D43D4F5F8436004325AD8
B78C5AFA1BFE9742FD32BB490","867567040119311|securemode=3,signmethod=hmacsha256,times
tamp=1631931961|"
```

// Set MQTT authentication information with the following parameters: Client ID, Username, Password, and ClientIDStr.

OK

```
AT+MQTTOPEN=1,"iot-as-mqtt.cn-shanghai.aliyuncs.com",1883,0,300
```

// Establish an MQTT connection with the following parameters: Clientid, Remote IP/URL, RemotePort, Cleanssession flag, and Keepalive time.

```
OK
```

```
+MQTTOPEN: 1,1
```

// MQTT connection established successfully.

```
AT+MQTTCLOSE=1
```

// Close MQTT connection.

```
OK
```

```
+MQTTCLOSE: 1,1
```

// MQTT connection closed successfully.

4 Huawei Cloud

4.1 Create Product

Enter the Huawei Cloud platform and click **Products** in the left-side navigation bar. On the **Products** page, click **Create Product** to enter the **Create Product** dialog box and complete product creation as instructed.

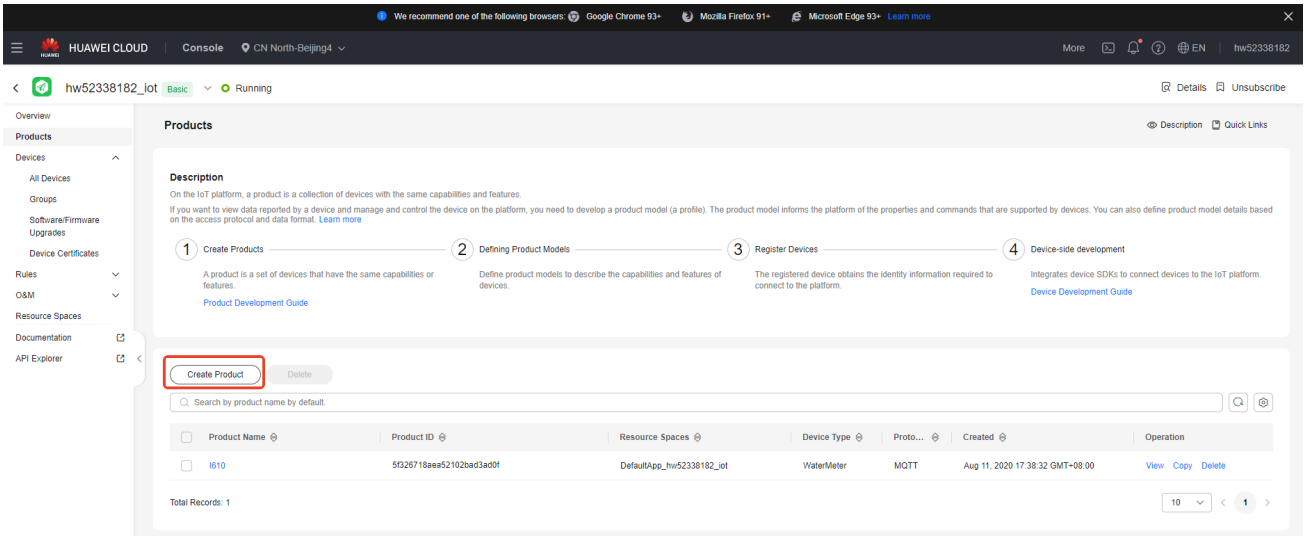

Figure 22. Products page

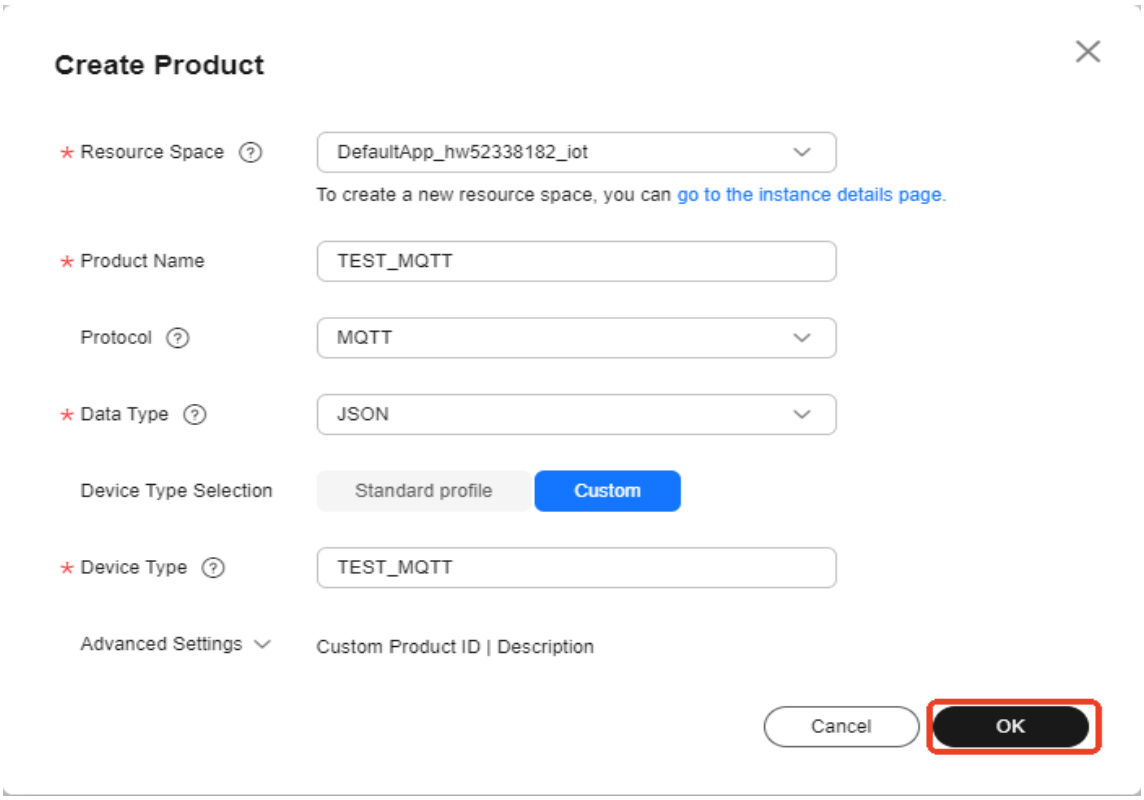

Figure 23. Create Product

On the **Basic Information** page of the product you just created, click **Customize Model** to add a service.

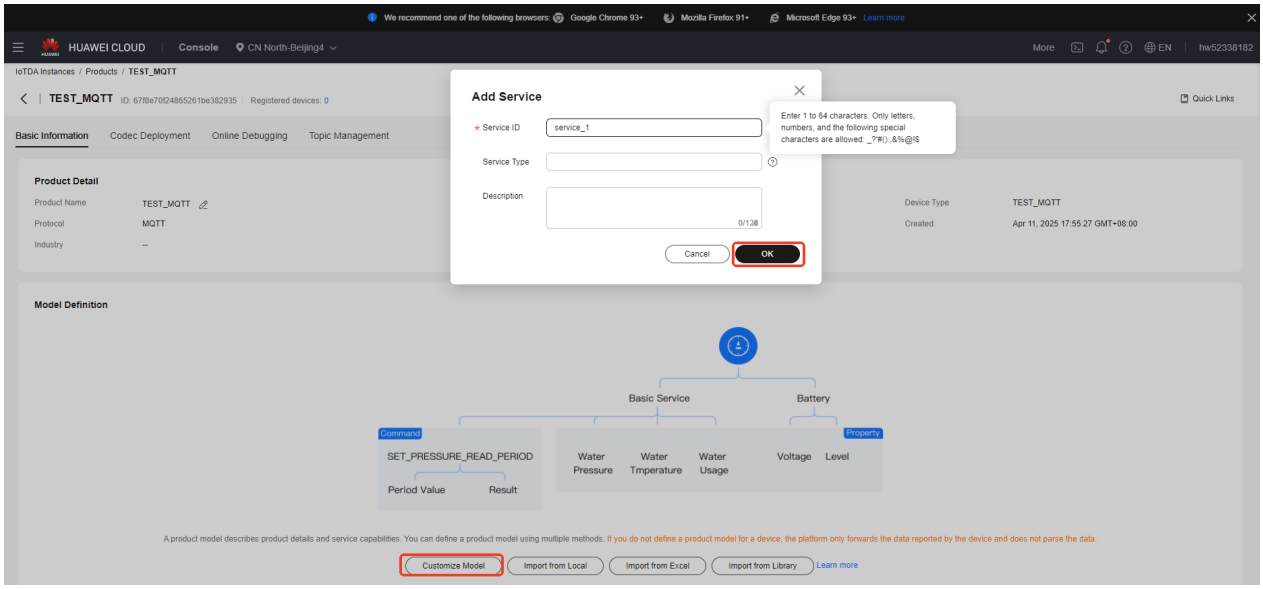

Figure 24. Add custom model

In the service list, select the service you added and add properties and commands for the service. You need to enter the correct parameter type and range based on the actual needs.

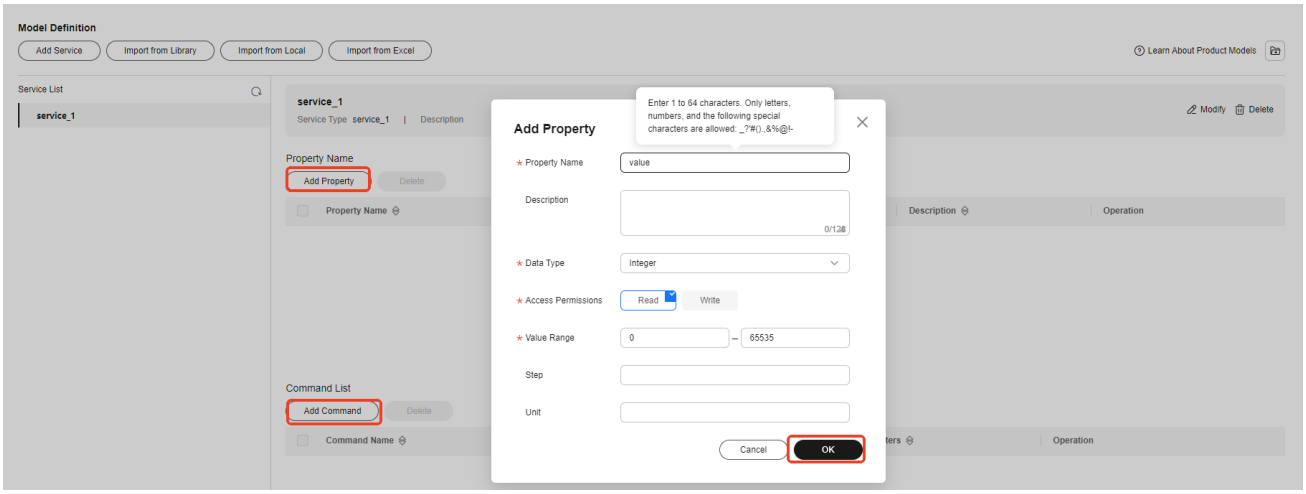

Figure 25. Add properties for custom service

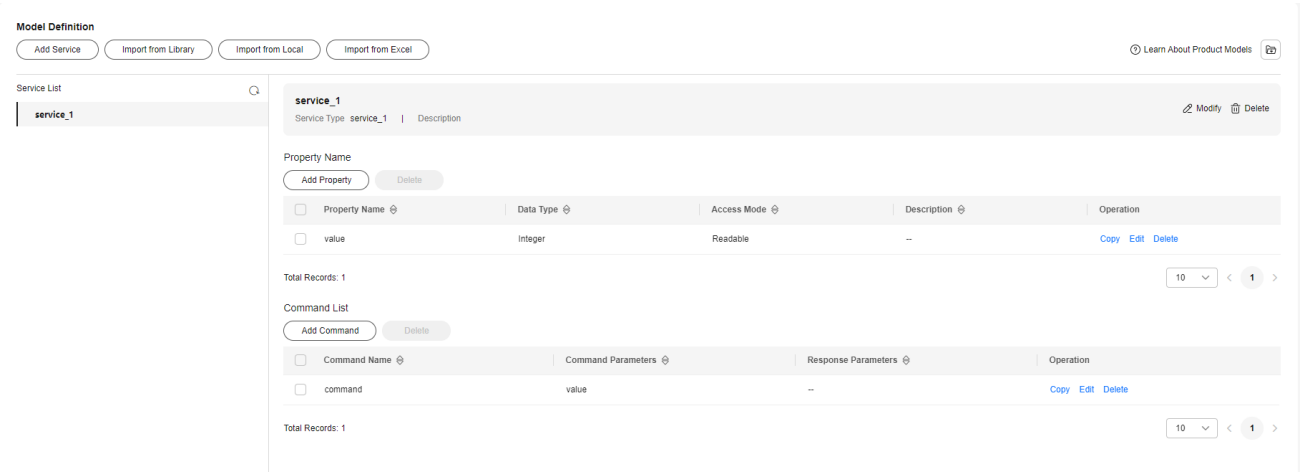

Figure 26. Result of adding custom model

After the custom model is added, the product creation is completed.

4.2 Create Device

Choose **Devices** > **All Devices** in the left-side navigation bar. Click the **Register Device** button and the **Register Device** dialog box will pop up. Fill in the product name you created and select the device ID to complete device creation.

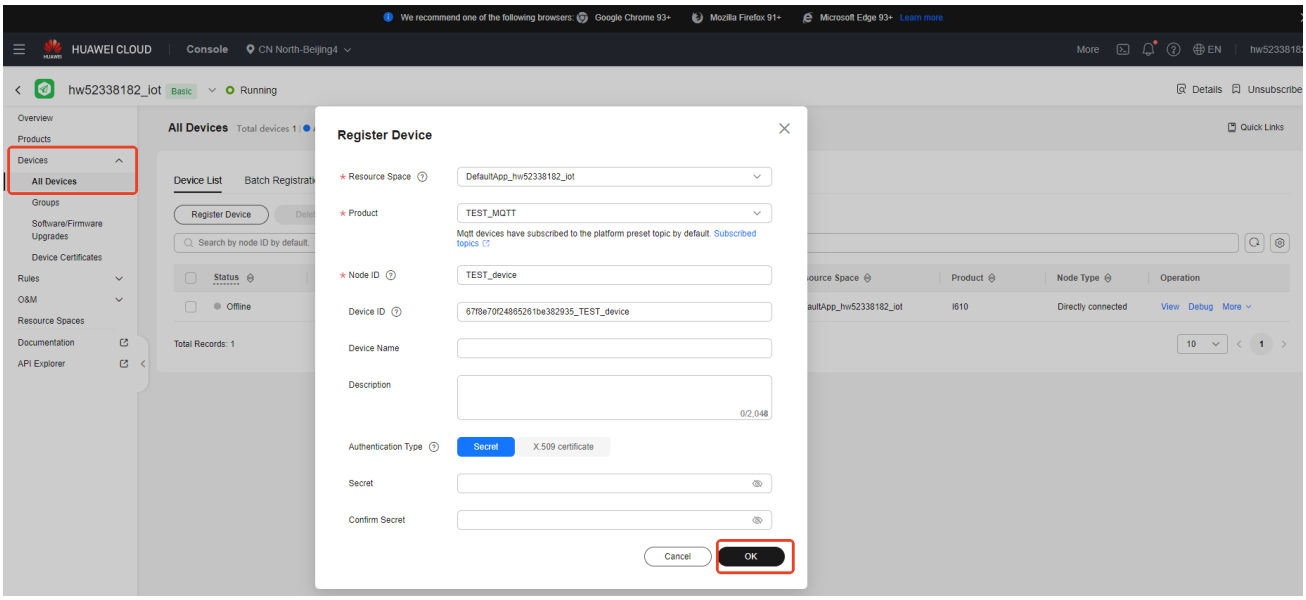

Figure 27. Create Device

4.3 Connection Example

```
AT+MIPCALL=1                    //Request the operator to assign an IP address.
OK
```

```
+MIPCALL: 100.100.87.143      //The return value is the IP address assigned by the operator.

AT + MQTTAUTHCFG = 3, "63351d7206cae4010b4b7750 _ TEST _ device", "059801b5b3c5fed33e0c51af0398fc38”  //Obtain the cloud parameter configuration. The parameters are cloudtype, DeviceName, DeviceSecret.

+MQTTAUTHCFG: 3,"63351d7206cae4010b4b7750_TEST_device","57c2a50ab8234600e26f85fcd84129058639d1d7a8fa94e6e3dfff1299ca347b","63351d7206cae4010b4b7750_TEST_device_0_0_2000000105" //The return value parameters are cloudtype, Username, Password, ClientIDStr.
OK

AT + MQTTUSER = 1, "63351 d7206cae4010b4b7750 _ TEST _ device", "57c2a50ab8234600e26f85fcd84129058639d1d7a8fa94e6e3dfff1299ca347b", "63351 d7206cae4010b4b7750 _ TEST _ device _ 0 _ 0 _ 2000000105”  //Set the user configuration. The parameters are clientid, Username, Password, ClientIDStr.
OK

AT+MQTTOPEN=1,"iot-mqtts.cn-north-4.myhuaweicloud.com",1883,1,300  //Establish an MQTT connection. The parameters are clientid, Remote IP/URL, RemotePort, Cleansession flag, Keepalive time.
OK

+MQTTOPEN: 1,1           //MQTT connection established successfully.

AT+MQTTCLOSE=1           //Close MQTT connection.
OK

+MQTTCLOSE: 1,1              //MQTT connection closed successfully.
```

5 AT Commands Used by MQTT Service

AT Command	Function Description
AT+MIPCALL	Ask the operator for an IP address. Fill the APN of the SIM card in the position of **cmnet**, which can be obtained from the SIM card supplier. Generally, China Mobile uses CMNET or CMIOT as its APN, and China Unicom uses 3gnet as its APN. If you need to configure a username and password, refer to +MIPCALL in AT Manual .
AT+MQTTAUTHDYN	Dynamic registration instruction configuration, supporting Alibaba Cloud and Tencent Cloud
AT+MQTTAUTHCFG	Cloud platform MQTT connection parameter calculation
AT+MQTTUSER	Set MQTT authentication information.
AT+MQTTOPEN	Establish MQTT connection.
AT+MQTTSUB	Subscribe to a topic.
AT+MQTTPUB	Publish a message to a topic.
AT+MQTTPUB	Publish a message to a topic (ODM mode. JSON supported).
AT+MQTTUNSUB	Unsubscribe from a topic.
AT+MQTTCLOSE	Close MQTT connection.
AT+MQTTWILL	Set the will message; the setting command must be sent before MQTT connection is established.
AT+GTSSLFILE	Load TLS certificate and key.
AT+GTSSLVER	Query or set TLS version.
AT+GTSSLMODE	Set whether to verify the server certificate.
AT+GTSSLERR	Get TLS error code.
AT+CCLK	Query command, query module current time