

阿里云 MQTT 与 “一机一密” & “一型一密” 应用与参考

— 潘先强(Herbert Pan) —



目 录

一、前 言.....	3
二、Aliyun 阿里云平台.....	3
三、Aliyun 物联网平台.....	4
3.1 创建产品.....	4
3.2 创建物模型.....	7
3.3 产品发布与撤销.....	9
3.4 添加设备.....	10
四、终端连接.....	12
4.1 一机一密.....	13
4.1.1 认证三元组.....	13
4.1.2 Username 与 Password.....	15
4.1.3 Topic 订阅与发布.....	16
4.2 一型一密.....	18
4.2.1 一型一密预注册.....	18
4.2.2 一型一密免预注册.....	23
4.2.3 基于 HTTPS 协议连接.....	26

一、前言

目前 QUECTEL 模组基本都支持对接阿里云基于 MQTT 的物联网平台，同时阿里云物联网平台在“云物联”中也占据重要地位和广泛应用；本文档针对 Quectel 模组基于 MQTT 协议接入阿里云物联网平台的应用以及“一机一密”与“一型一密”注册方式的使用方法进行整理，从而可以更加快捷高效的了解该平台的应用流程和模组对接方法。

二、Aliyun 阿里云平台

Aliyun 平台：<https://www.aliyun.com/>



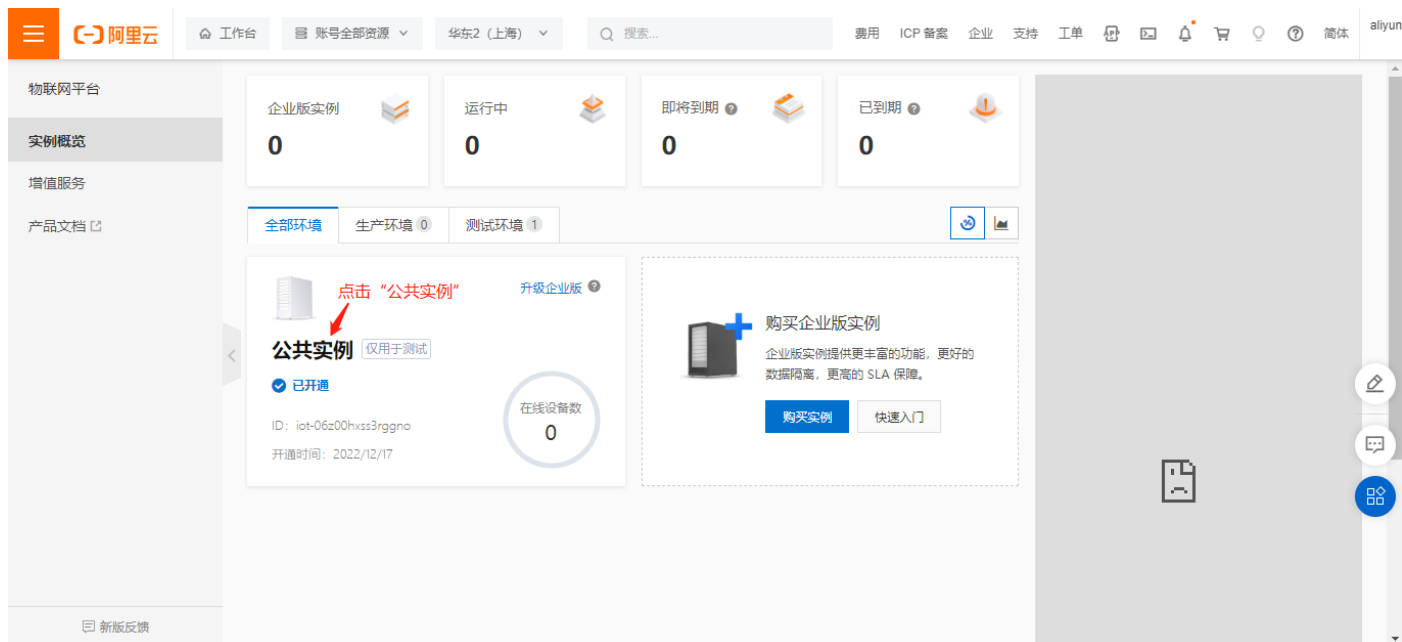
三、Aliyun 物联网平台

Aliyun 物联网平台: https://www.aliyun.com/product/iot/iot_instc_public_cn

如下图所示, 登录阿里云物联网平台后, 点击“进入控制台”;



如下图所示, 进入控制台后, 点击“公共实例”, 进入公共实例详细页面;



3.1 创建产品

在“公共实例”的左侧管理窗口中, 选择“产品”, 如下图所示; 相关配置参数可参考图中说明;



公共实例

实例详情

设备管理

产品

设备

分组

设备模拟器

设备分发

IoT孪生引擎

消息转发

监控运维

安全中心

新版反馈

数据格式

ICA 标准数据格式 (Alink JSON)

数据校验级别

弱校验 免校验

认证方式

设备密钥

确认 取消

若上报数据类型为JSON格式，选择当前Alink JSON格式；若为其他数据格式，选择“透传/自定义”

公共实例

实例详情

设备管理

产品

设备

分组

设备模拟器

设备分发

IoT孪生引擎

消息转发

监控运维

安全中心

新版反馈

物联网平台 / 设备管理 / 产品

产品 (设备模型)

设备接入流程概览

查看流程图 隐藏指引

01 创建产品
产品是同类设备的集合

02 创建设备
创建设备获取连接平台所需的身份信息

03 编辑物模型
产品下的设备都会继承产品的物模型

04 设备端开发
集成Link SDK，开发设备程序

创建产品 快速入门 请输入产品名称查询 请选择产品标签

产品名称	ProductKey	节点类型	创建时间	操作
SmartKit	i2uqc2dloOI	设备	2023/04/05 14:31:28	查看 管理设备 删除

公共实例

实例详情

设备管理

产品

设备

分组

设备模拟器

设备分发

IoT孪生引擎

消息转发

监控运维

安全中心

新版反馈

物联网平台 / 设备管理 / 产品 / SmartKit

SmartKit

发布

ProductKey i2uqc2dloOI 复制 ProductSecret ***** 查看

设备数 0 前往管理

产品信息 Topic 列表 功能定义 消息解析 服务端订阅 设备开发 文件上传配置

产品信息 编辑

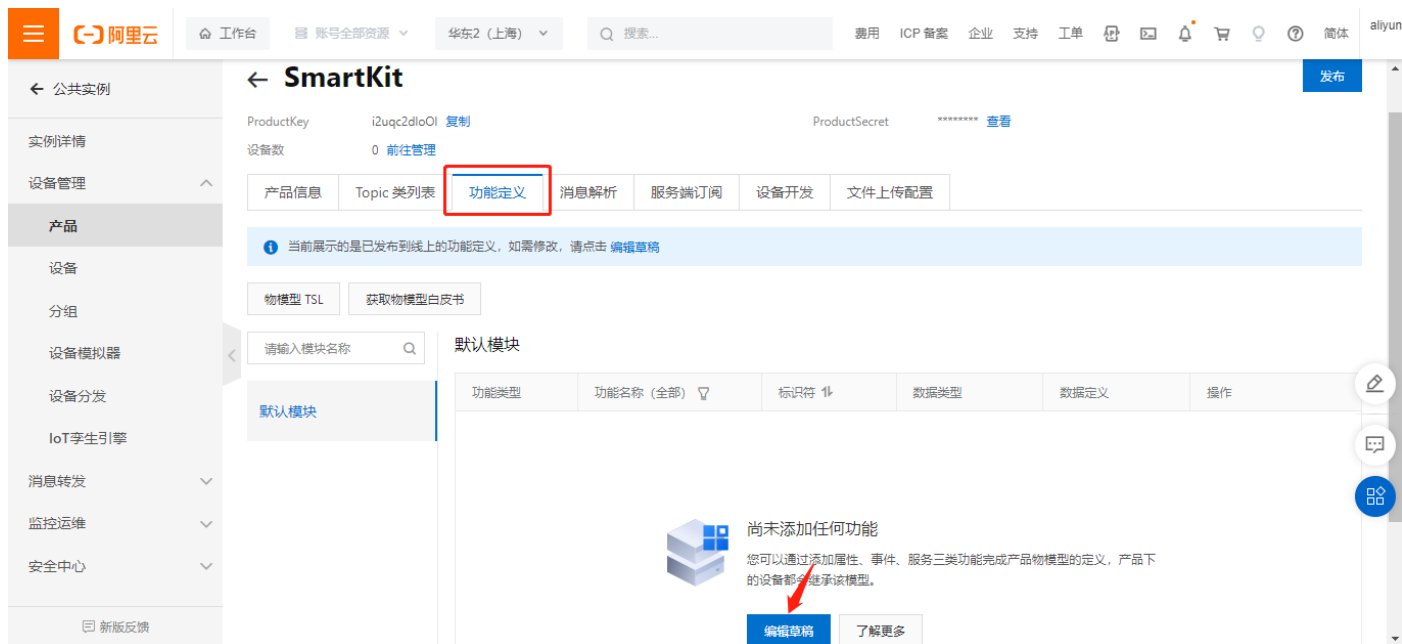
属性	值
产品名称	SmartKit
所属品类	自定义品类
认证方式	设备密钥
直连设备	ICA 标准数据格式 (Alink JSON)
数据校验级别	弱校验
动态注册	已关闭
状态	开发中
节点类型	设备
产品描述	智能物件
创建时间	2023/04/05 14:31:28
连网协议	蜂窝 (2G / 3G / 4G / 5G)

标签信息 编辑

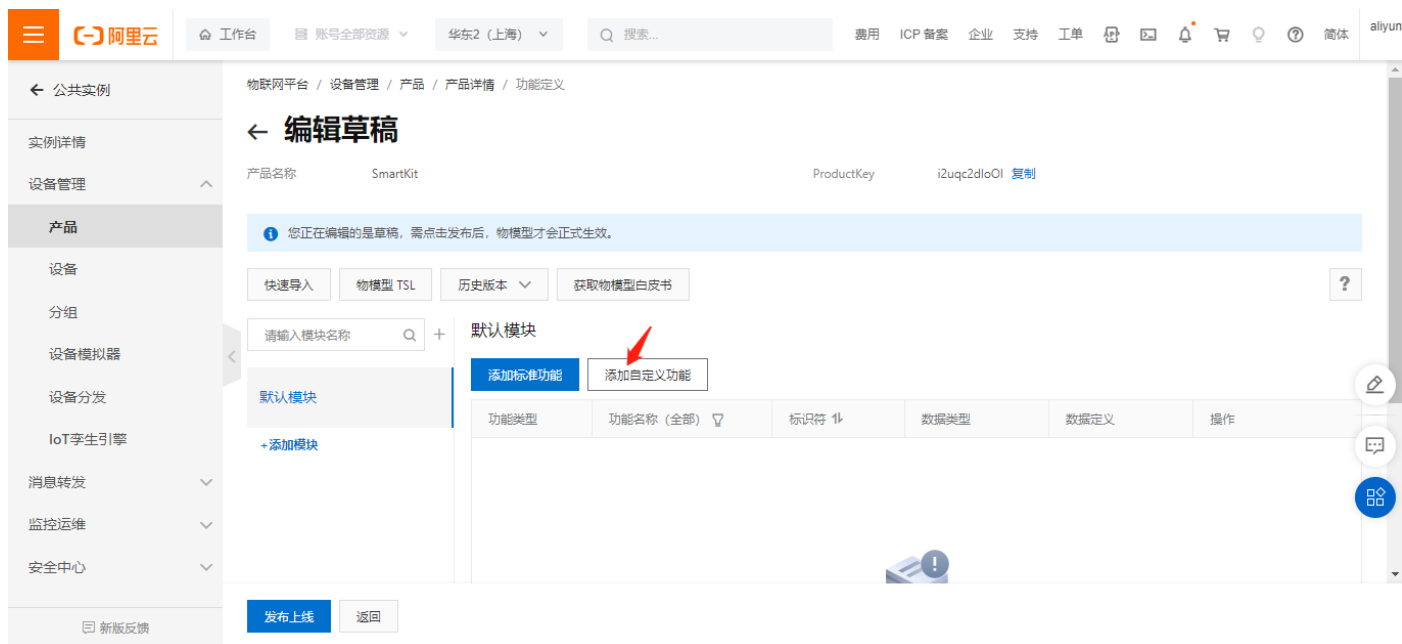
产品标签 无标签信息

3.2 创建物模型

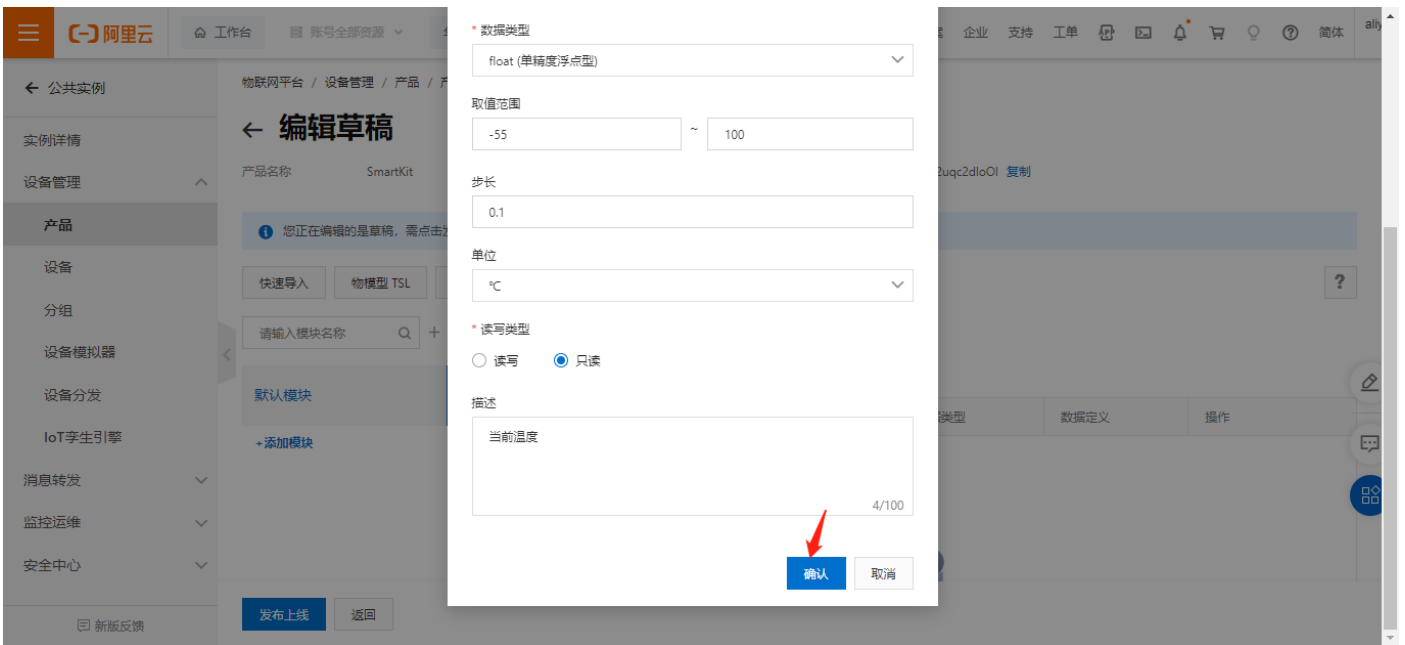
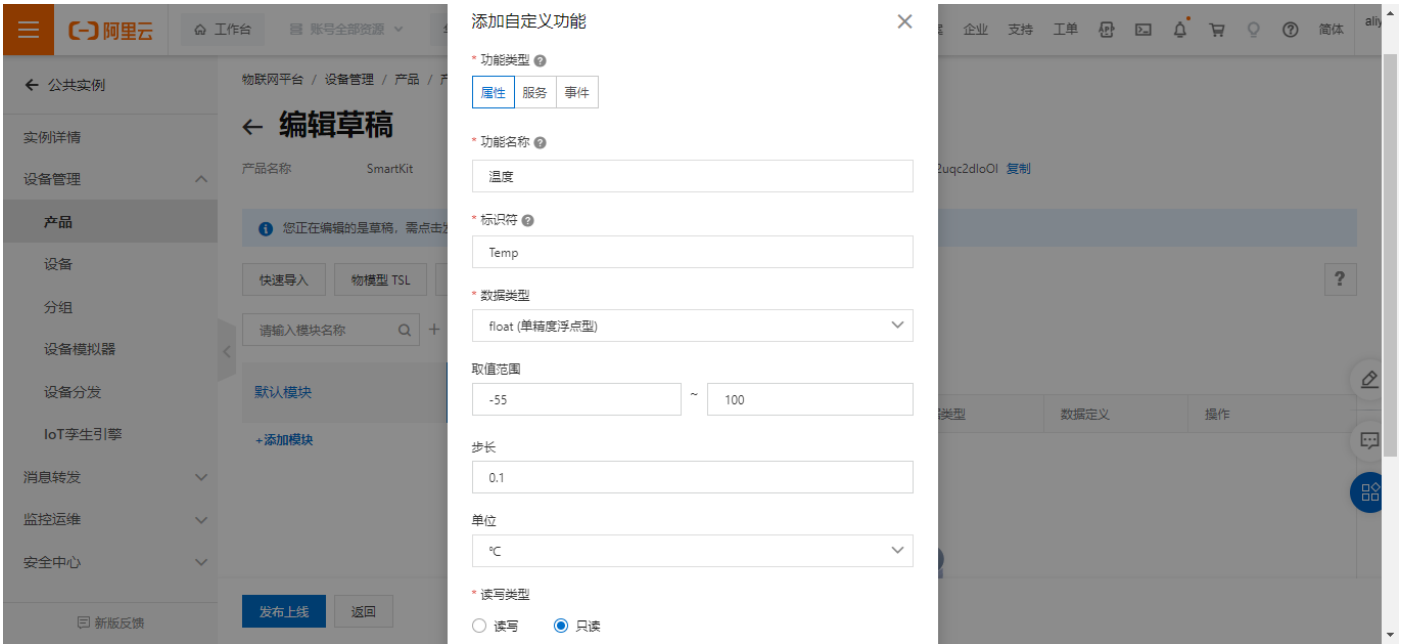
在产品详情中选择“功能定义”，根据应用需求和使用场景，创建相应的“物模型”，如下图所示；

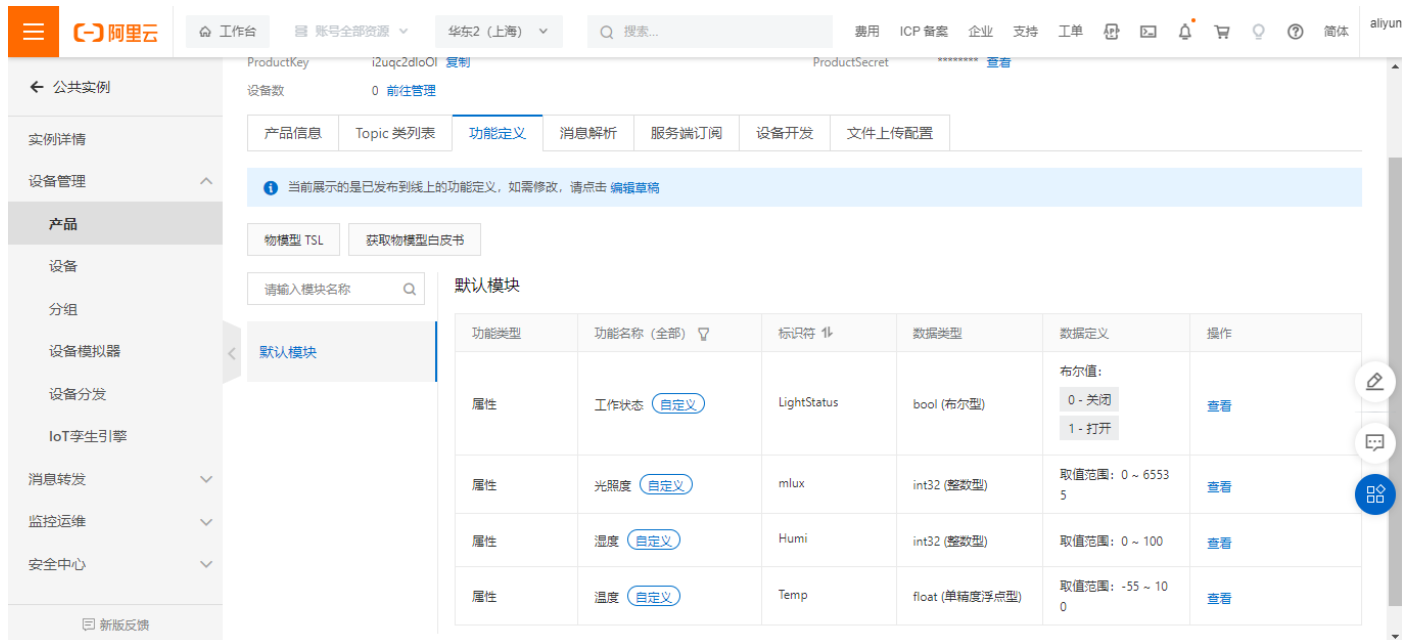


根据产品应用或场景，可以选择“添加标准功能”或“添加自定义功能”；



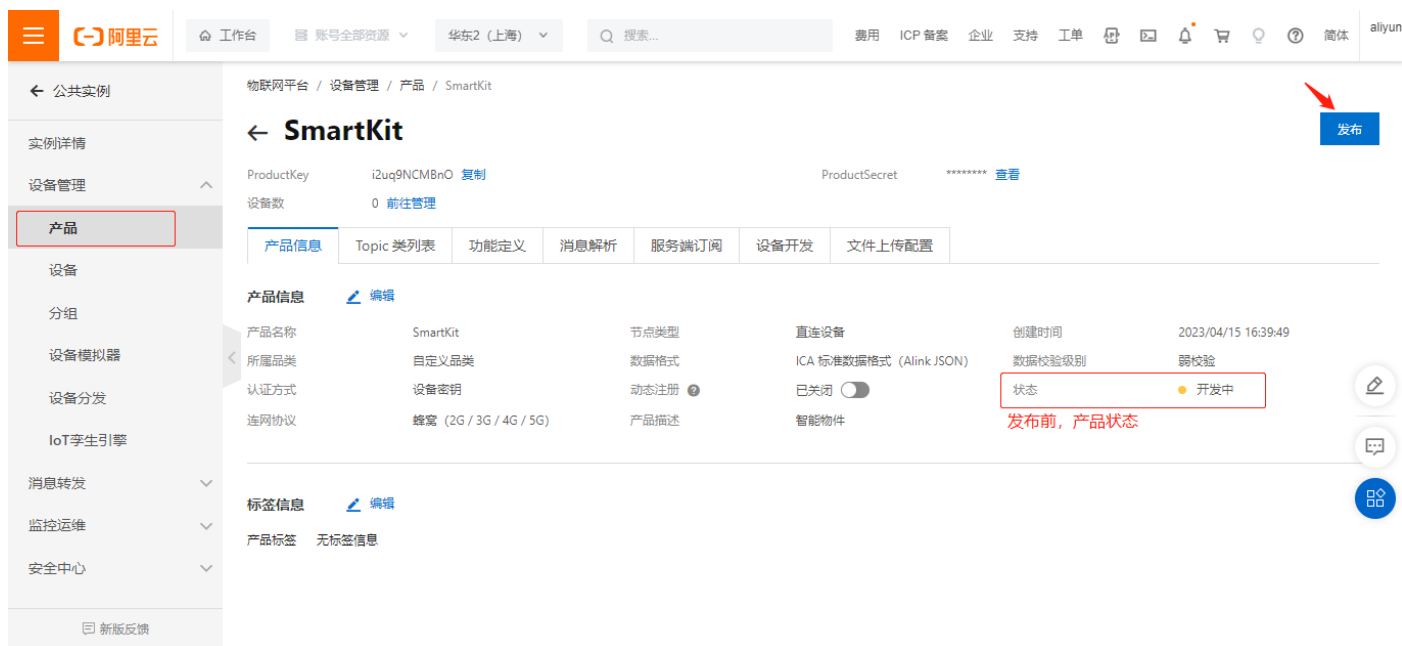
如下图所示，添加产品所需的功能（属性、服务、事件），完成后，点击“发布上线”；

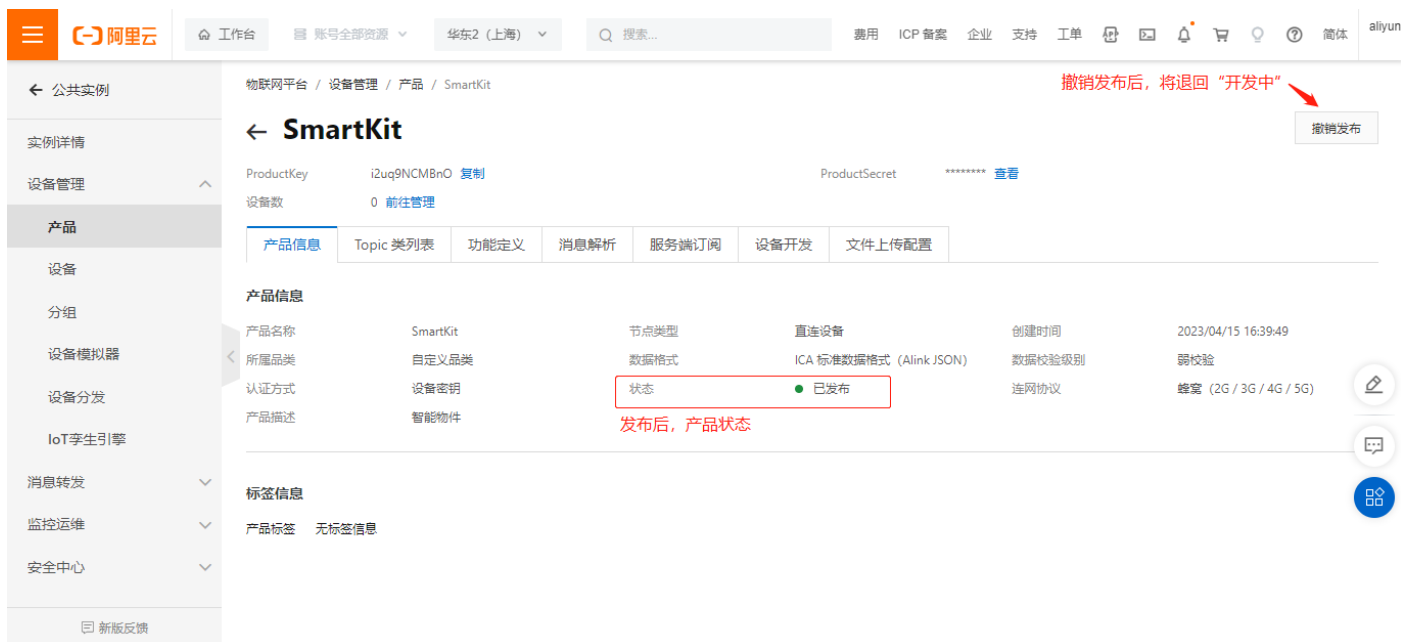
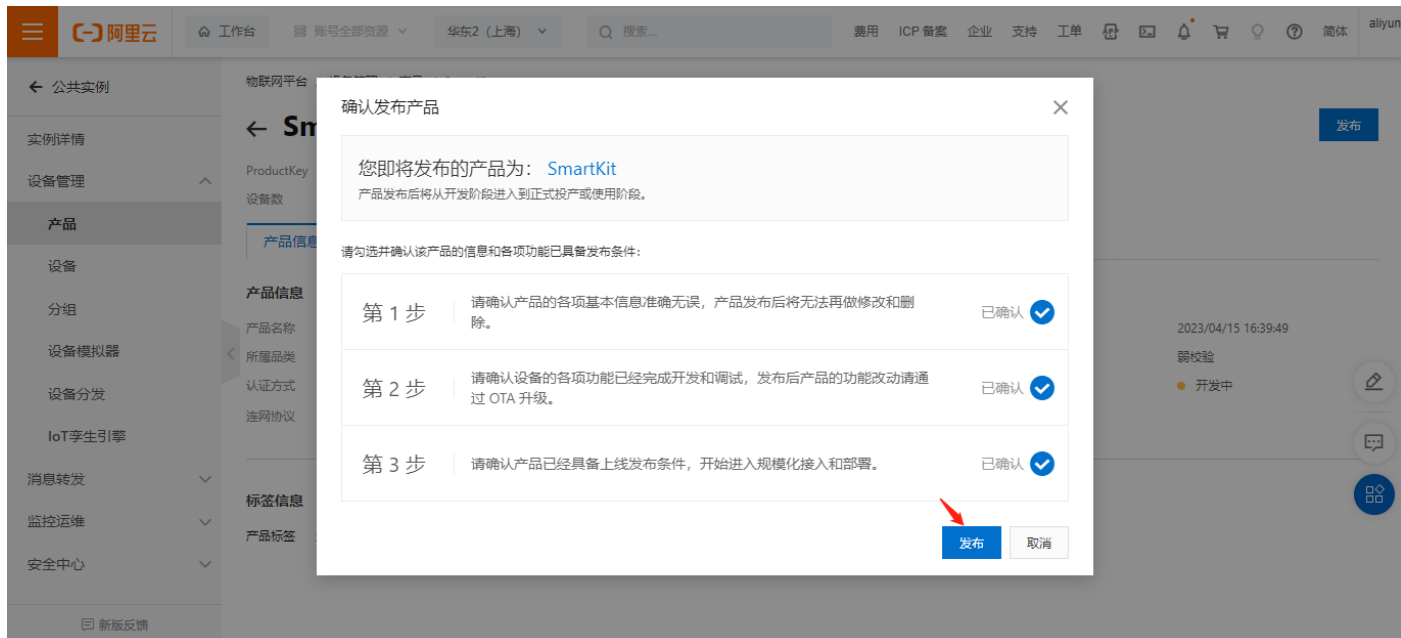




3.3 产品发布与撤销

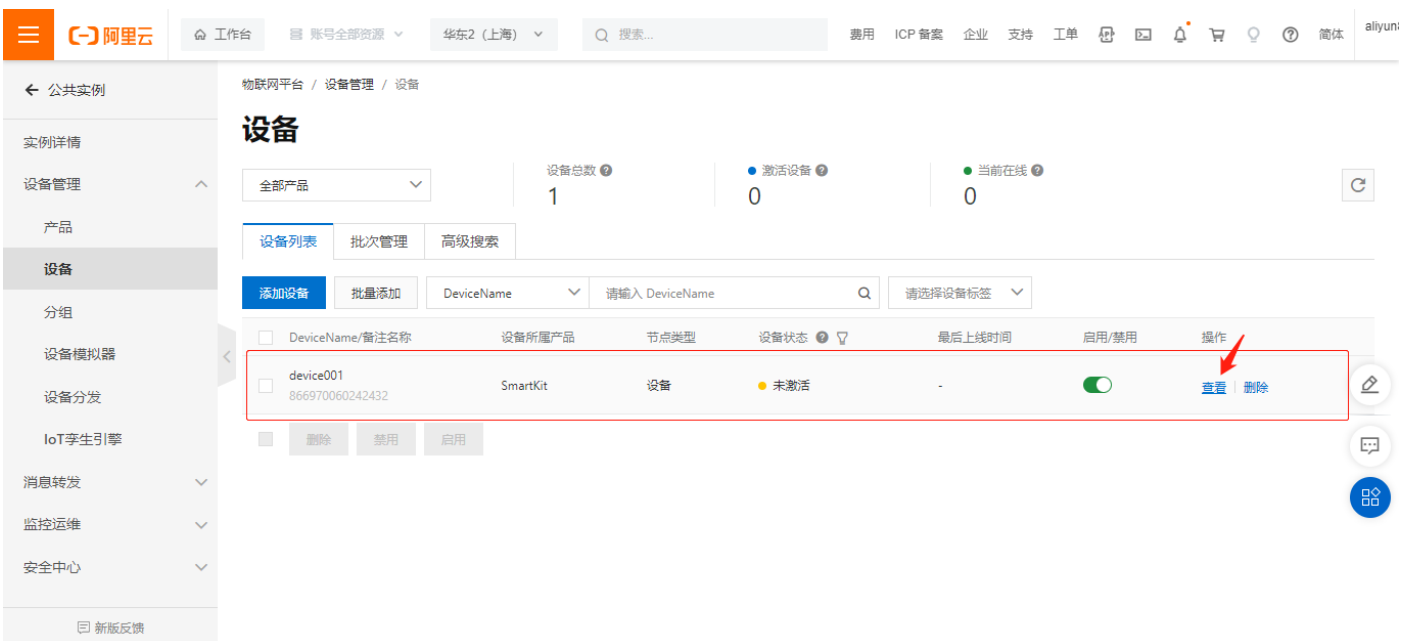
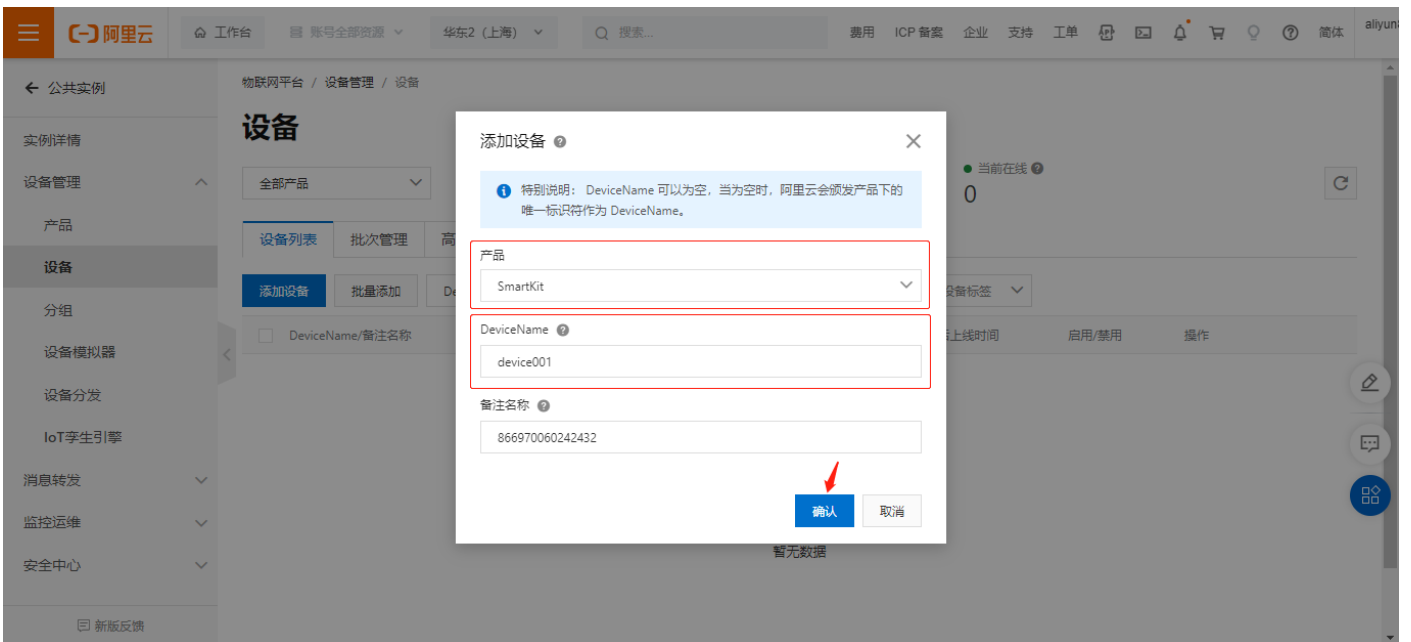
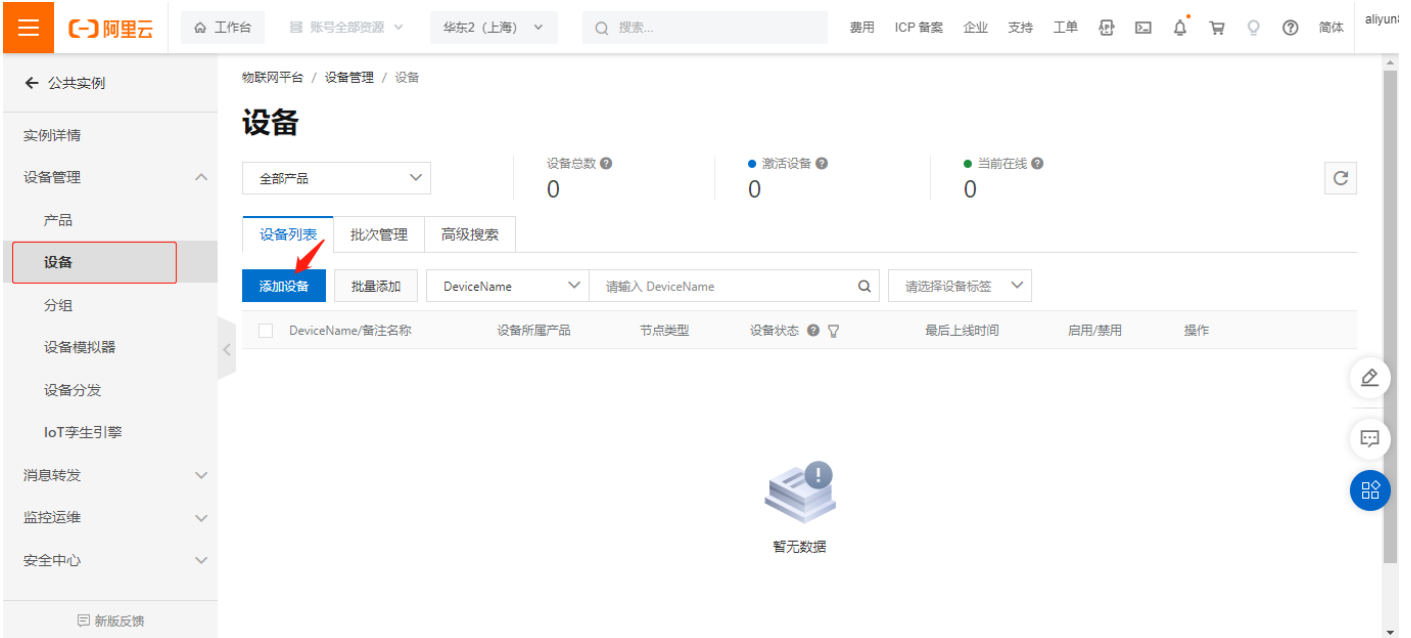
产品及功能定义等完成后, 产品状态显示“开发中”; 产品或终端在调试阶段, 在“开发中”状态不影响其调试; 也可以通过“发布”确定当前定义的产品, “发布”后, 状态变更为“已发布”, 如下图所示;



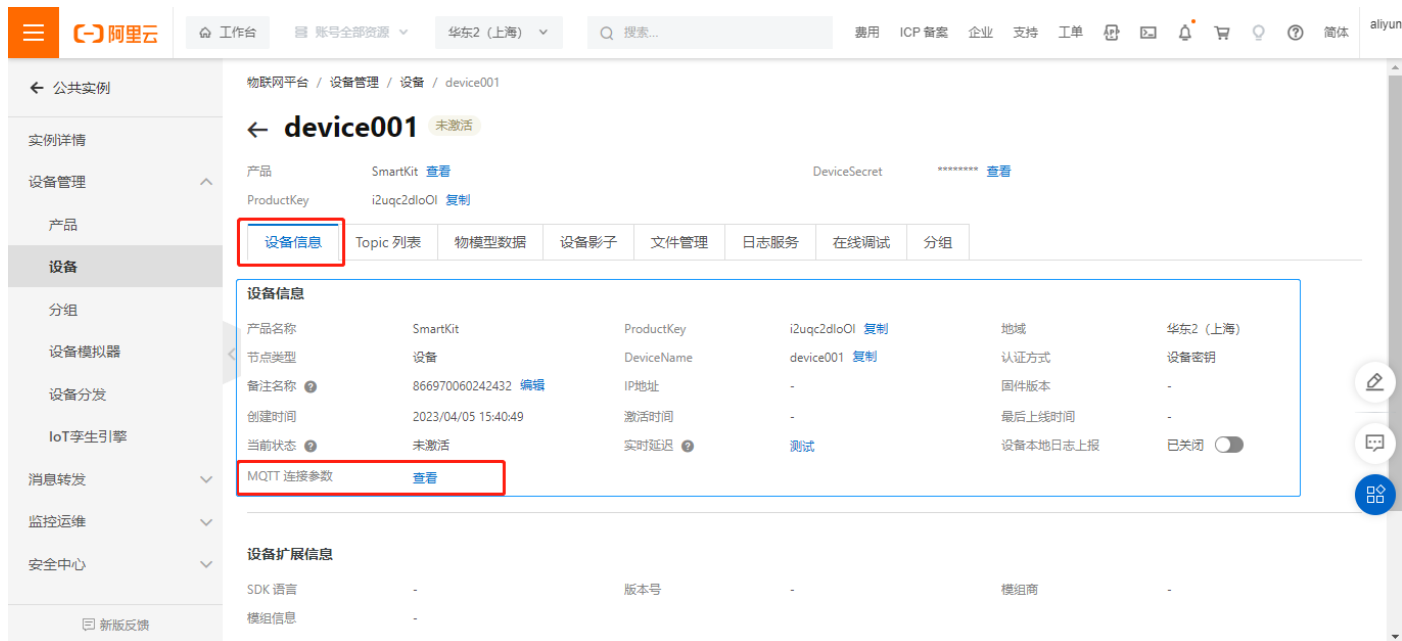


3.4 添加设备

在“公共实例”的左侧管理窗口中，选择“设备”，如下图所示；添加设备时需要选择添加到对应的产品中；



添加设备后，点击“查看”设备详情，如图所示，可以查看连接阿里云 MQTT 所需的“三元组”信息：ProductKey，DeviceName，DeviceSecret；也可以通过 MQTT 连接参数进行连接访问，具体参考下文例程；



在设备的“物模型数据”选项中，可以查看当前设备的相关功能及上报的功能数据；



四、终端连接

如下图所示，在“实例详情”中点击“查看开发配置”，确定当前阿里云 MQTT 连接的公网终端节点；

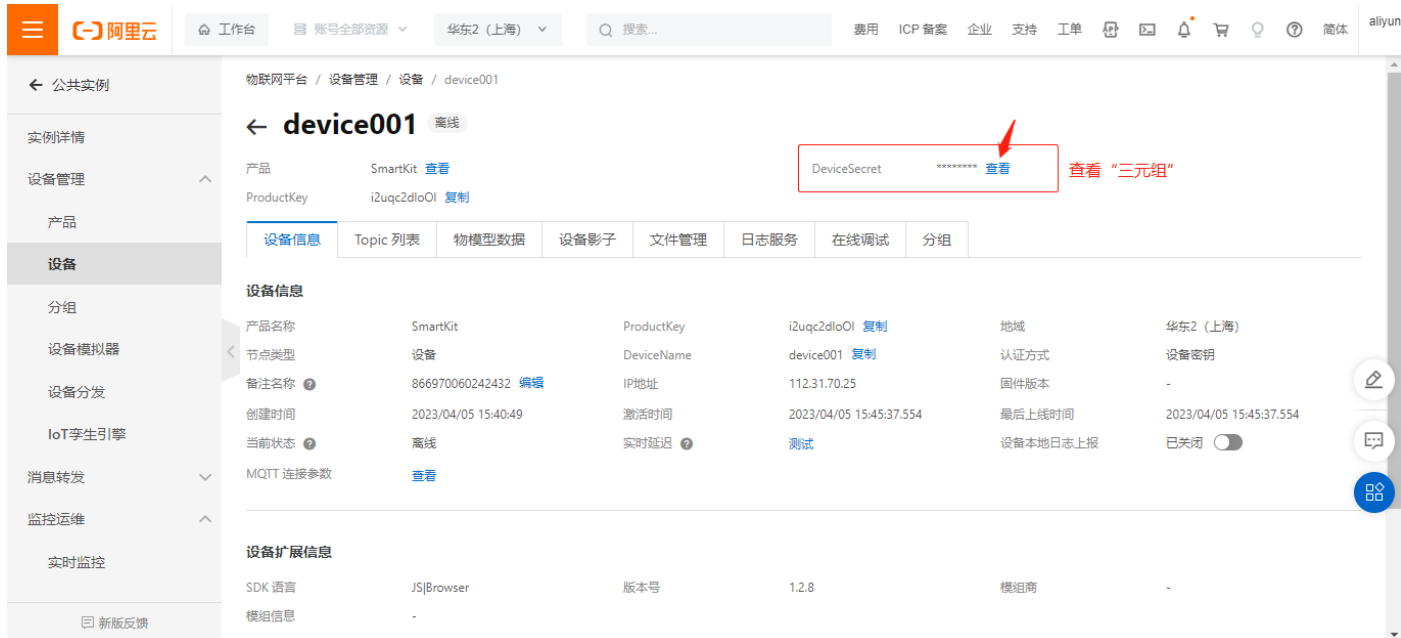


4.1 一机一密

4.1.1 认证三元组

在 QUECTEL 模组支持阿里云 MQTT 应用的情况下，都可以通过下面指令配置连接参数，分别对应 ProductKey, DeviceName, DeviceSecret; 具体值如下图所示方法查看;

```
AT+QMTCFG="aliauth",<client_idx>,<product key>,<device name>,<device secret>
```



基于 ProductKey, DeviceName, DeviceSecret 三元组连接访问的例程如下:

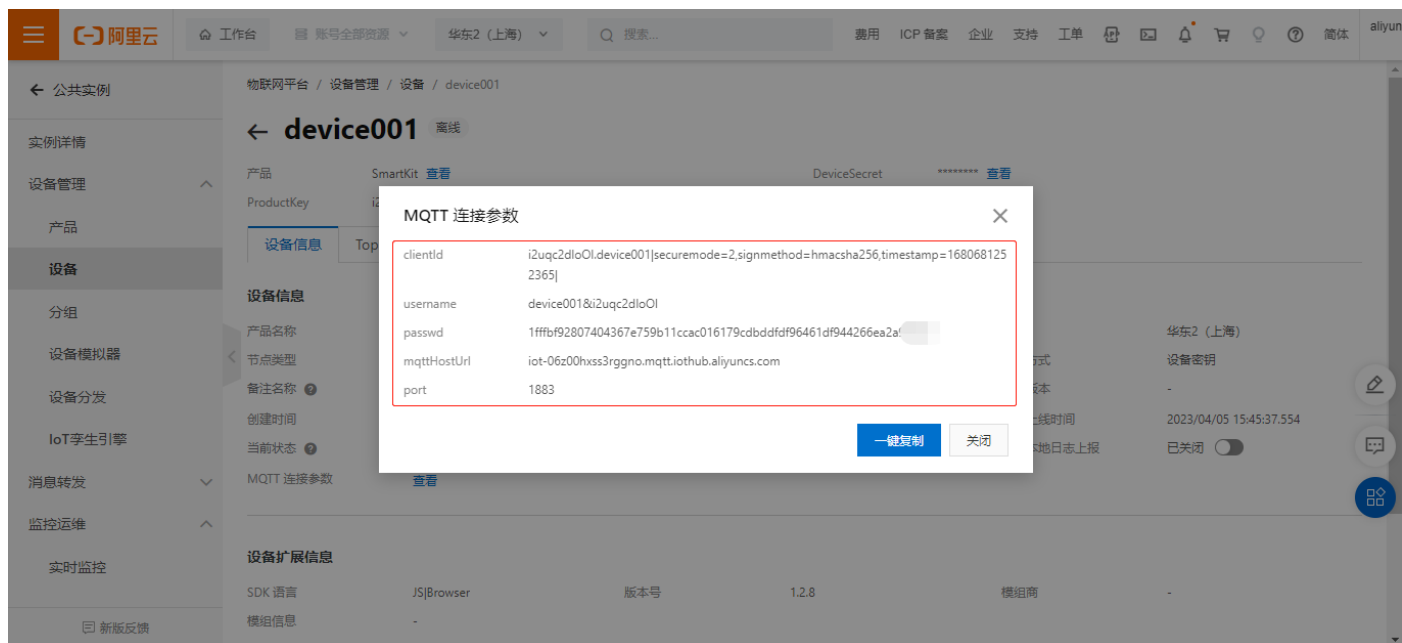
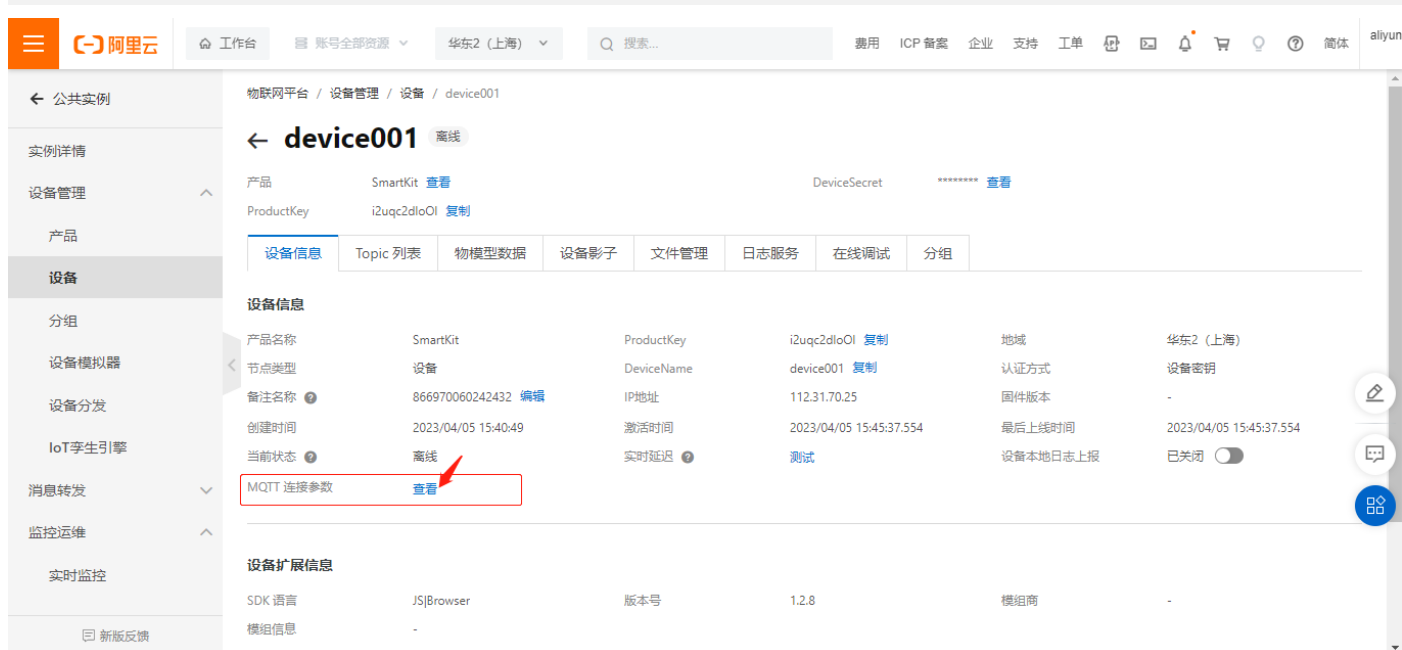
```
>> AT+QMTCFG="version",0,4
>> OK
>>
>> AT+QMTCFG="aliauth",0,"i2uqc2dloOl","device001","c4fa40df9c8078073d75a26be2bc8****"
>>
>> OK
>> AT+QMTOPE=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPE: 0,0
>> AT+QMTCO=0,"device001"
>>
>> OK
>>
```

```
>> +QMTCONN: 0,0,0
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0
```

4.1.2 Username 与 Password

若不执行基于 ProductKey, DeviceName, DeviceSecret 的三元组参数配置情况下, 也可以通过设备详情中的“MQTT 连接参数” clientId、username、passwd 进行连接; 具体如下图所示;

AT+QMTCONN=<client_idx>,<clientid>[,<username>,<password>]

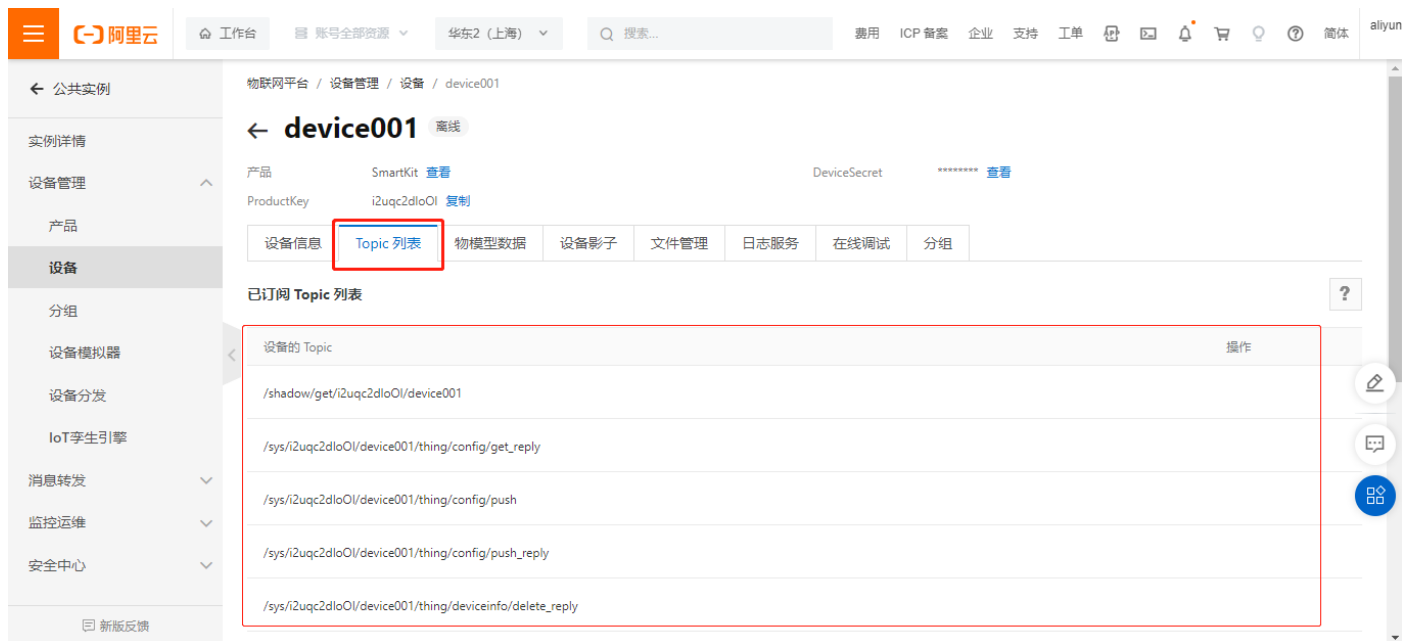


基于 clientId、username、passwd 连接访问的例程如下:


```
>> AT+QMTCFG="version",0,4
>> OK
>>
>> AT+QMTCFG="aliauth",0
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>>
AT+QMTCONN=0,"i2uqc2dloOI.device001|securemode=2,signmethod=hmacsha256,timestamp=1680937625134|","device001&i2uqc2dloOI","0309b31761c30d24d37a25558c5604de308c92eb6ac8656a1981f85783fb23**"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0
```

4.1.3 Topic 订阅与发布

如下图所示，通过“设备”的 Topic 列表，可以详细了解该设备的 topic 及应用；



基于上述产品及设备物模型，通过 Topic 上报相关数据的例程如下：

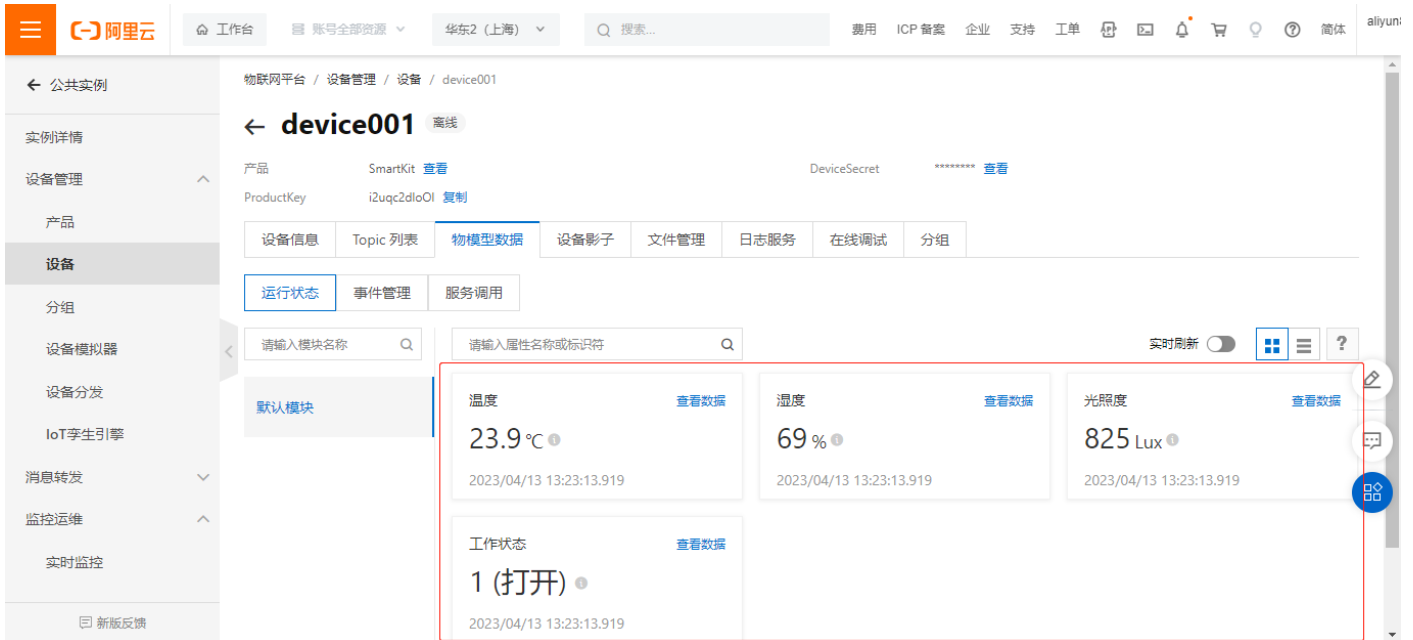
```
>> AT+QMTCFG="version",0,4
```

```

>>
>> OK
>> AT+QMTCFG="will",0
>>
>> +QMTCFG: "will",0
>>
>> OK
>> AT+QMTCFG="aliauth",0,"i2uqc2dloOI","device001","c4fa40df9c8078073d75a26be2bc8f58"
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"device001"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTSUB=0,1,"/sys/i2uqc2dloOI/device001/thing/event/property/post_reply",0
>>
>> OK
>>
>> +QMTSUB: 0,1,0,1
>> AT+QMTPUBEX=0,0,0,0,"/sys/i2uqc2dloOI/device001/thing/event/property/post",133
>>
>> >
{"id":"1681363292898","params":{"Temp":23.9,"Humi":69,"mlux":825,"LightStatus":1},"version":"1.0","method":"thing.event.property.post"}
}
>> OK
>>
>> +QMTPUBEX: 0,0,0
>>
>> +QMTRECV:
0,0,"/sys/i2uqc2dloOI/device001/thing/event/property/post_reply","{"code":200,"data":{},"id":"1681363292898","message":"success","method":"thing.event.property.post","version":"1.0"}"
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0

```

通过上述上报已定义的功能数据后，查看该设备的物模型数据如下图所示；

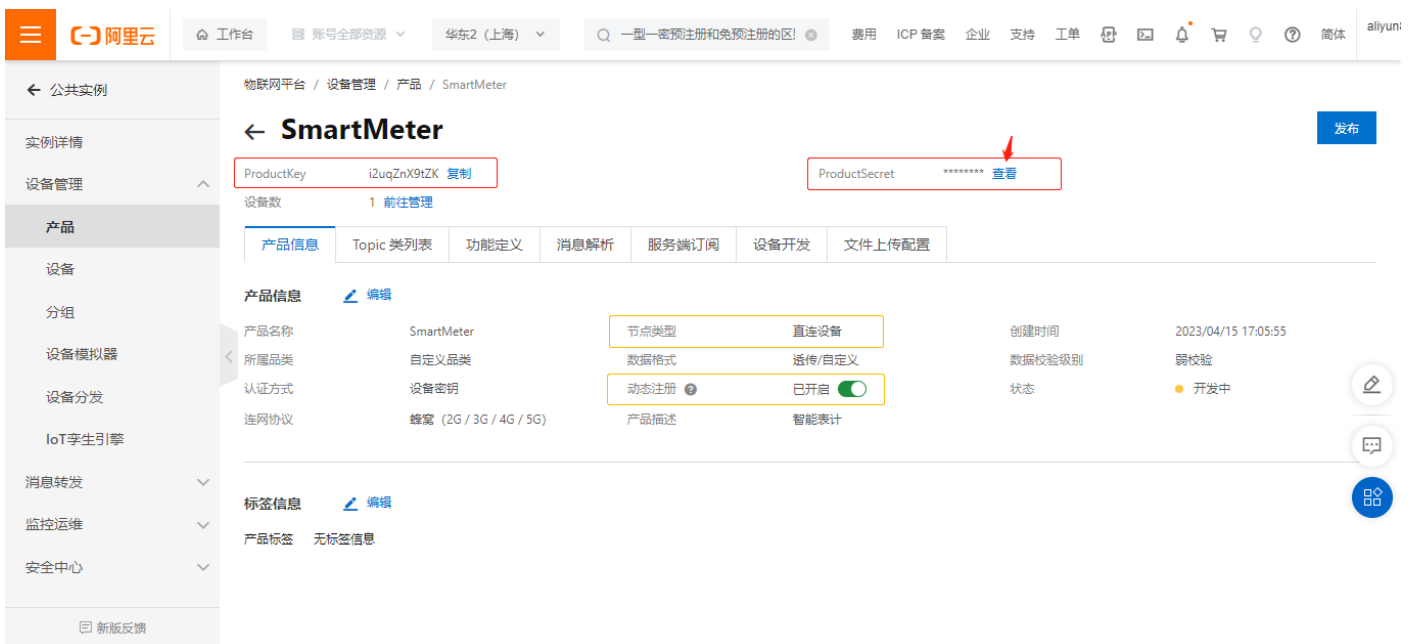


4.2 一型一密

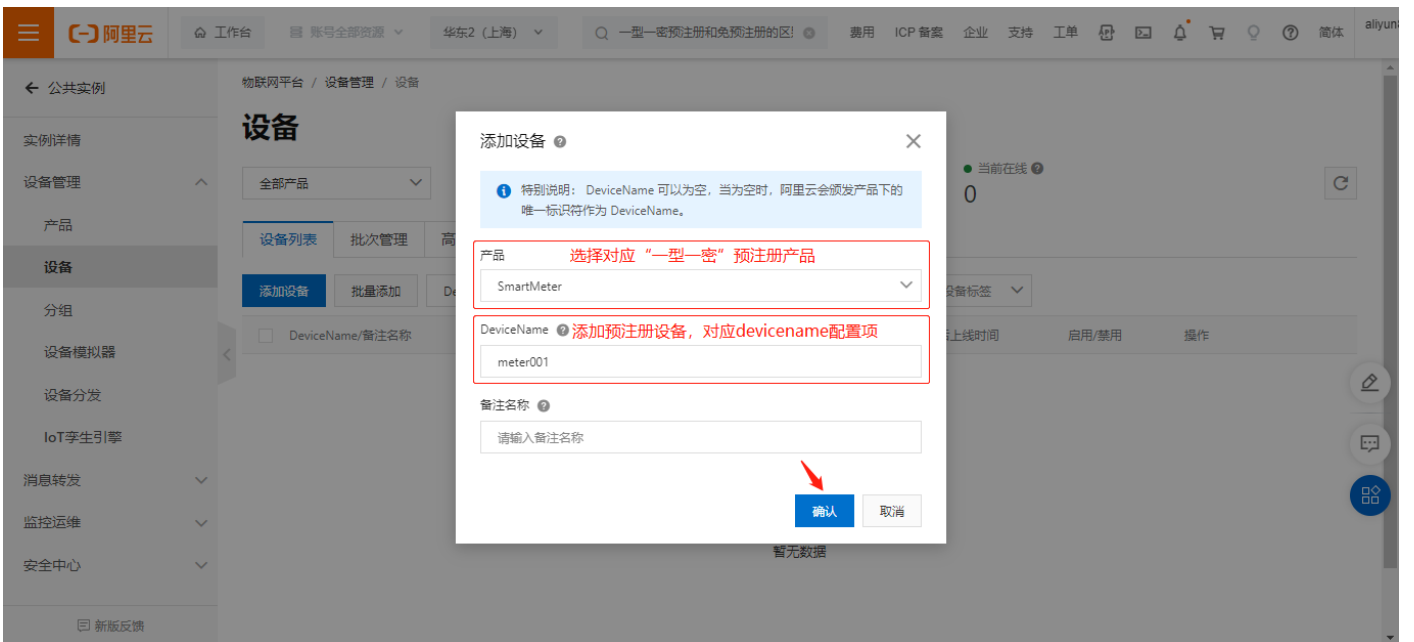
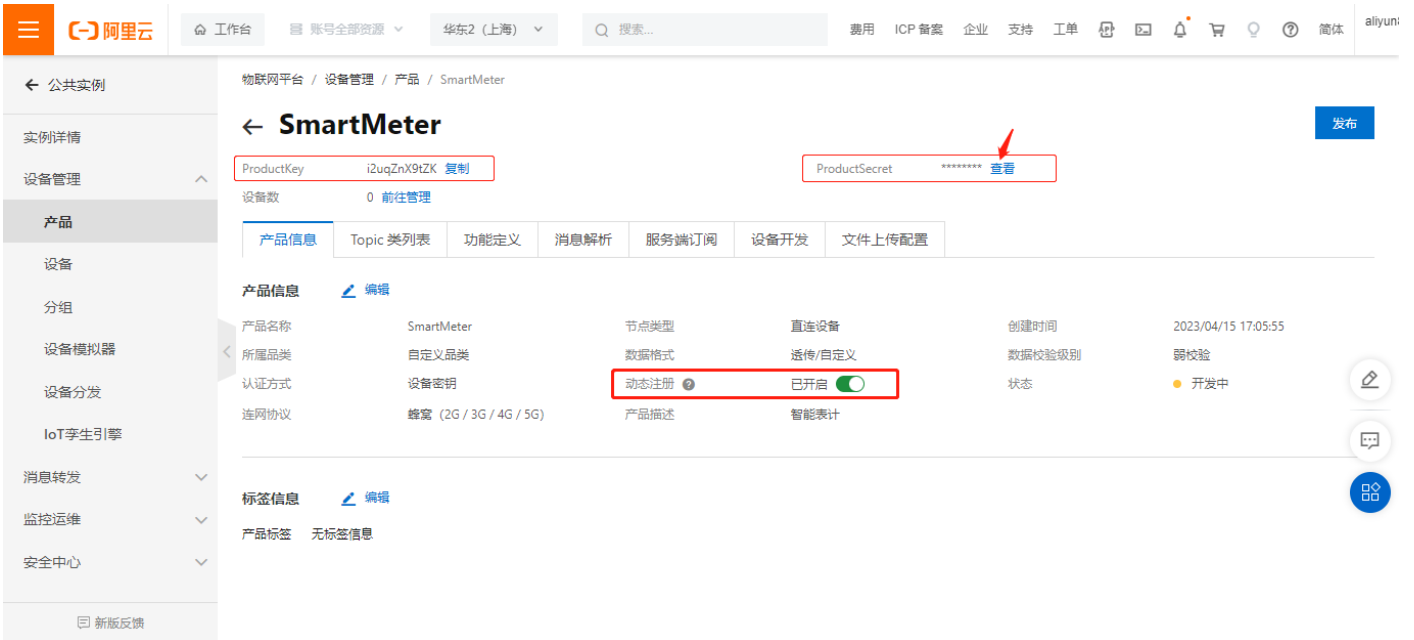
4.2.1 一型一密预注册

- * 创建的产品的节点类型为“直连设备”；
- * 创建的产品中，开启“动态注册”；
- * 使用一型一密预注册认证方式，需在已创建的产品下，添加设备；
- * 必须使用 TLS 加密方式连接/访问；

“一型一密预注册”需在阿里云物联网平台上创建产品，并开启动态注册；同时需添加相应的设备。



以下创建示例说明：Clientid 为当前终端模组的 IMEI: 864430010001091；添加设备 deviceName 为 meter001



CONNECT 报文的动态注册参数:

```
mqttClientId: clientId+"|securemode=-
2,authType=xxxx,random=xxxx,signmethod=xxxx,instanceId=xxxx|"
mqttUserName: deviceName+"&"+productKey
mqttPassword: sign_hmac(productSecret,content)
```

参数说明如下:

mqttClientId	clientId	客户端 ID, 可自定义, 长度在 64 个字符内。建议使用设备的 MAC 地址或 SN 码, 便于识别区分不同的客户端	
	securemode	安全模式: 一型一密预注册认证方式: 固定取值为 2。 一型一密免预注册认证方式: 固定取值为-2	864430010001091
	authType	一型一密认证方式, 不同类型将返回不同的认证参数: register: 一型一密预注册认证方式, 返回 DeviceSecret。 regnw1: 一型一密免预注册认证方式, 返回 DeviceToken、ClientID。	securemode=2, authType=register, random=123, signmethod=hmacsha1, instanceId=iot-06z00hxss3rggno
	random	随机数, 可自定义随机数。	
	signMethod	签名算法 目前支持 hmacmd5、hmacsha1、hmacsha256。	
	instanceId	实例 ID, 详见下图所示	
mqttUserName		deviceName+"&"+productKey	meter001&i2uqZnX9tZK
mqttPassword		password 计算方法: sign_hmac(productSecret,content) productSecret, 详见下图所示; content 由 deviceName、productKey、random 按照先后顺序拼接的字符串; sign_hmac 对应上述 signMethod 选择的哈希加密算法, 其中加密内容为 content, 加密密钥为 productSecret, 如下图所示	Content: deviceName+meter001+productKey i2uqZnX9tZK+random123 productSecret: xTzMxVmm9HUY19** Password: 25f4b80c3fab2ed6e41644 a38f2c5b67eac1b505



MqttPassword 加密方法如下:

在线散列/哈希加密工具: <https://www.fulimama.com/allencrypt/>



```
>> AT+QMTCFG="aliauth",0
>> +QMTCFG: "aliauth",,,

>> OK
>> AT+QMTCFG="ssl",0,1,2
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"864430010001091|securemode=2,authType=register,random=123,signmethod=hmacsha1,instanceId=iot-06z00hxss3rggno|","meter001&i2uqZnX9tZK","25f4b80c3fab2ed6e41644a38f2c5b67eac1b505"
>>
```

```

>> OK
>>
>> +QMTCONN: 0,0,0
>>
>> +QMTRECV:
0,0,"/ext/register","{"deviceSecret":"d2a03b64a5e06b051f481136668133cf","productKey":"i2uqZnX9tZK","deviceName":"meter001"}"
>>
>> +QMTSTAT: 0,1
>> AT+QMTCFG="aliauth",0,"i2uqZnX9tZK","meter001","d2a03b64a5e06b051f481136668133cf"
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"meter001"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0
    
```

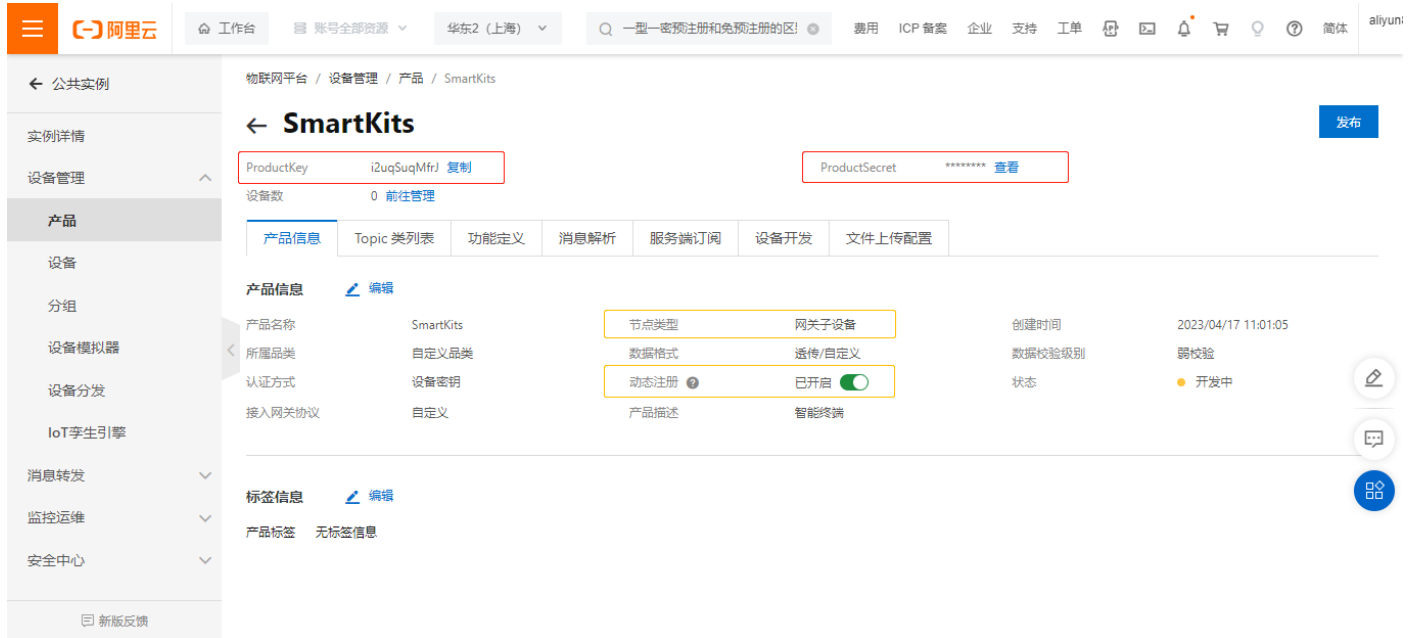
The screenshot shows the '设备管理' (Device Management) page in the Alibaba Cloud IoT Platform console. The page title is '设备' (Device). It displays a table of devices with the following columns: DeviceName/备注名称, 设备所属产品, 节点类型, 设备状态, 最后上线时间, 启用/禁用, and 操作. A single device, 'meter001', is listed with status '在线' (Online). The '设备状态' column for this device is highlighted with a red box. Below the table are buttons for '删除', '禁用', and '启用'.

DeviceName/备注名称	设备所属产品	节点类型	设备状态	最后上线时间	启用/禁用	操作
<input type="checkbox"/> meter001	SmartMeter	设备	● 在线	2023/04/17 09:44:38.618	<input checked="" type="checkbox"/>	查看 删除

4.2.2 一型一密免预注册

- * 创建的产品中，开启“**动态注册**”；
- * 使用一型一密免预注册认证方式，**无需添加设备**；
- * 必须使用 **TLS 加密** 方式连接/访问；

“一型一密免预注册”需在阿里云物联网平台上创建产品，并开启**动态注册**；无需添加设备。



以下创建示例说明：Clientid 为当前终端模组的 IMEI: 864430010001091；预注册设备 deviceName 为 Kit001

mqttClientid	clientId	客户端 ID，可自定义，长度在 64 个字符内。建议使用设备的 MAC 地址或 SN 码，便于识别区分不同的客户端	864430010001091 securemode=-2, authType=regnwl, random=123, signmethod=hmacsha1, instanceId=iot-06z00hxss3rggno
	securemode	安全模式： 一型一密预注册认证方式：固定取值为 2。 一型一密免预注册认证方式：固定取值为-2	
	authType	一型一密认证方式，不同类型将返回不同的认证参数： register：一型一密预注册认证方式，返回 DeviceSecret。 regnwl：一型一密免预注册认证方式，返回 DeviceToken、ClientID。	
	random	随机数，可自定义随机数。	
	signMethod	签名算法 目前支持 hmacmd5、hmacsha1、hmacsha256。	
	instanceId	实例 ID,详见下图所示	
mqttUserName	deviceName+"&"+"productKey	Kit001&i2uq9ORmOSM	

<p>mqttPassword</p>		<p>password 计算方法: sign_hmac(productSecret,content) productSecret, 详见下图所示; content 由 deviceName、productKey、random 按照先后顺序拼接的字符串; sign_hmac 对应上述 signMethod 选择的哈希加密算法, 其中加密内容为 content,加密密钥为 productSecret, 如下图所示</p>	<p>Content: deviceNameKit001productKey i2uq9ORmOSMrandom123 productSecret: cSsjZl19qkGDLv** Password: f9130cc77eff4d4474b28da22 5509a38e7e78b3a</p>
---------------------	--	--	---

免预注册连接如下:

```
>> AT+QMTCFG="aliauth",0
>>
>> +QMTCFG: "aliauth",,,
>>
>> OK
>> AT+QMTCFG="ssl",0,1,2
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"Kit001|securemode=-2,authType=regnwl,random=123,signmethod=hmacsha1,instanceId=iot-06z00hxss3rggno|","Kit001&i2uq9ORmOSM","f9130cc77eff4d4474b28da225509a38e7e78b3a"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>>
>> +QMTRECV:
0,0,"/ext/regnwl","{"clientId":"KzLKNeWyE7SxiWLuPpZQ000100","productKey":"i2uq9ORmOSM","deviceName":"Kit001","deviceToken":"^1^1681709523062^c5cce0a49b03685"}"
>>
>> +QMTSTAT: 0,1
>>
```

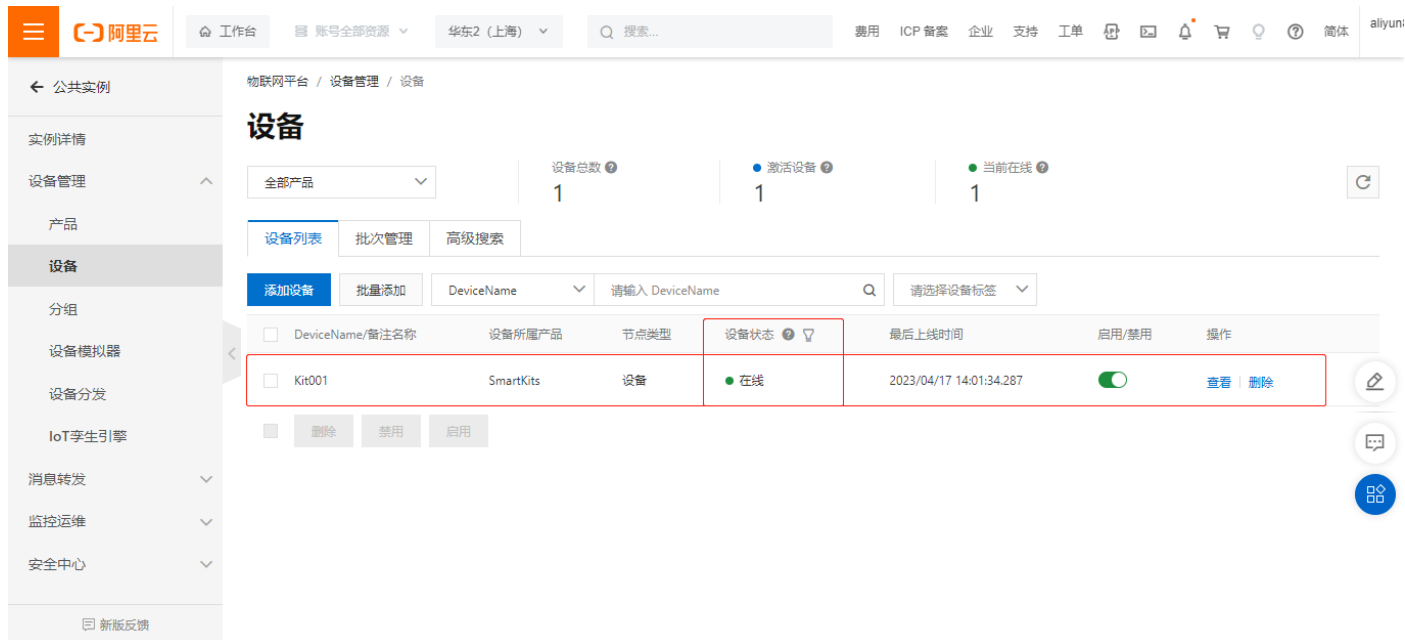


终端设备登录连接参数:

连接参数	参数组包说明
mqttClientId	clientId+" securemode=-2,authType=connwl "
mqttUserName	deviceName+"&"+productKey
mqttPassword	deviceToken

注意, 重新连接免预注册, 将重新下发新的 clientId 和 deviceToken;

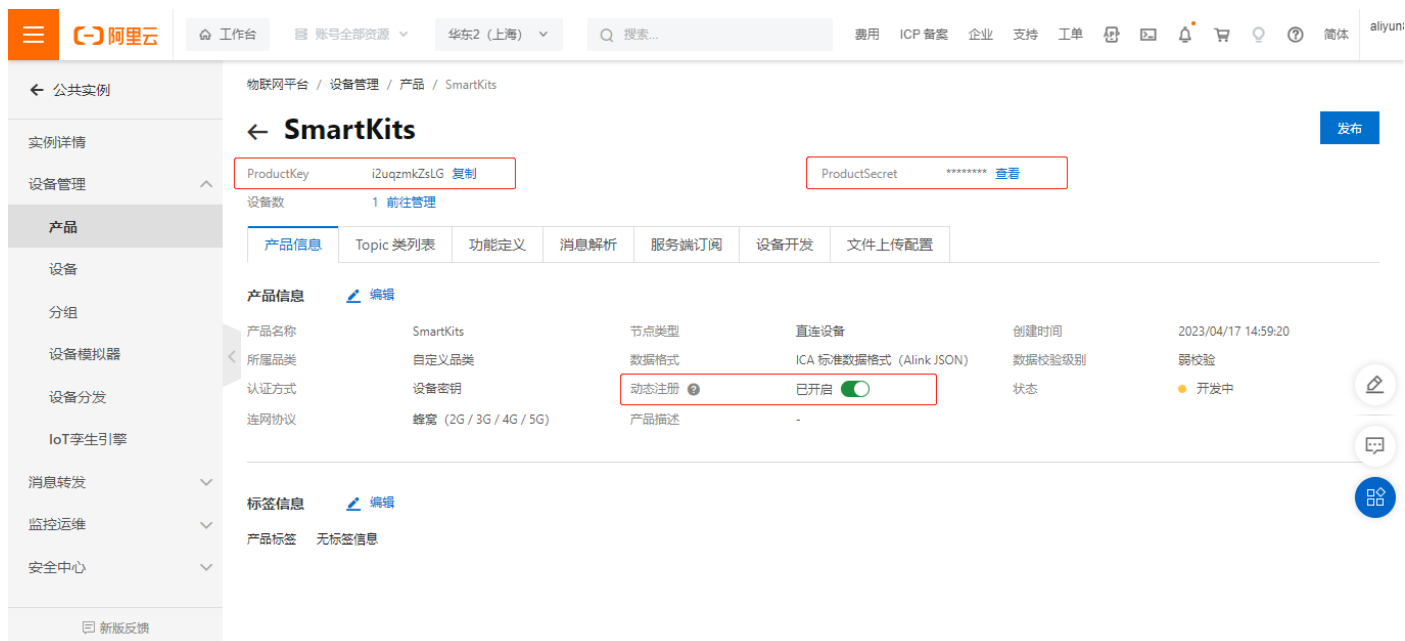
```
>> +QMTRECV:
0,0,"/ext/regnw|",{"clientId":"iXywJDuke7AKz0sfbvmZ000100","productKey":"i2uq9ORmOSM","deviceName":"Kit001","deviceToken":
"^1^1681710731098^563fbcf8c38f88"}"
>>
>> +QMTSTAT: 0,1
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"iXywJDuke7AKz0sfbvmZ000100|securemode=-
2,authType=connwl|","Kit001&i2uq9ORmOSM","^1^1681710731098^563fbcf8c38f88"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0
```

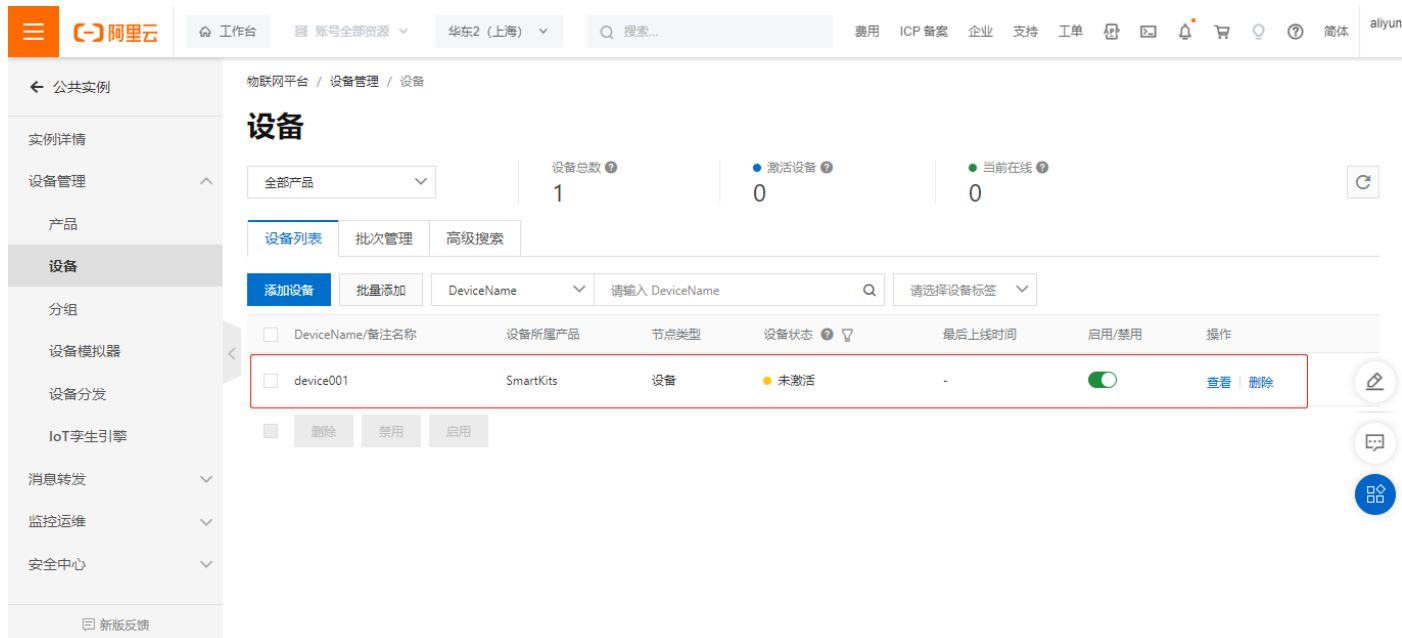


4.2.3 基于 HTTPS 协议连接

HTTPS 协议注册连接适用于除华北 2（北京）、华南 1（深圳）以外的所有地域。

连接参数	参数说明
URL	https://iot-auth.\$\{YourRegionId\}.aliyuncs.com/auth/register/device
POST 方法	POST /auth/register/device HTTP/1.1 Host: iot-auth.cn-shanghai.aliyuncs.com Content-Type: application/x-www-form-urlencoded Content-Length: 123 productKey=a1234*****&deviceName=deviceName1234&random=567345&sign=adfv123hdfdhd&signMethod=hmacsha1
signMethod	hmac_sha1(productSecret, deviceNamedeviceName1234productKeya1234*****random123)





示例连接参数	示例
URL	https://iot-auth.cn-shanghai.aliyuncs.com/auth/register/device
POST content	productKey=i2uqzmkZsLG&deviceName=device001&random=003&sign=277969e6c596f0d127fd1d3bf3229f396a3ddff6&signMethod=hmacsha1

测试例程:

```
>> AT+QHTTPURL=62,80
>>
>> CONNECT
>> https://iot-auth.cn-shanghai.aliyuncs.com/auth/register/device
>> OK
>> AT+QHTTPPOST=120,120,120
>>
>> CONNECT
>>
productKey=i2uqzmkZsLG&deviceName=device001&random=003&sign=277969e6c596f0d127fd1d3bf3229f396a3ddff6&signMethod=hmac
sha1
>> OK
>>
>> +QHTTPPOST: 0,200,143
>> AT+QHTTPREAD=200
>>
>> CONNECT
>>
{"code":200,"data":{"deviceName":"device001","deviceSecret":"3c35df4417faf854be8e780536d84c23","productKey":"i2uqzmkZsLG"},"me
ssage":"success"}
>> OK
>>
>> +QHTTPREAD: 0
>> AT+QMTCFG="aliauth",0
>>
```

```

>> +QMTCFG: "aliauth",,,
>>
>> OK
>> AT+QMTCFG="aliauth",0,"i2uqzmkZsLG","device001","3c35df4417faf854be8e780536d84c23"
>>
>> OK
>> AT+QMTOPEN=0,"iot-06z00hxss3rggno.mqtt.iothub.aliyuncs.com",1883
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"device001"
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTCLOSE=0
>>
>> OK
>>
>> +QMTCLOSE: 0,0
    
```

The screenshot shows the Alibaba Cloud IoT Platform console interface. The main content area displays the '设备' (Device) management page. At the top, there are statistics for '全部产品' (All Products): 1 total device, 1 activated device, and 1 currently online device. Below this, there are tabs for '设备列表' (Device List), '批次管理' (Batch Management), and '高级搜索' (Advanced Search). A search bar is present with a dropdown for 'DeviceName' and a text input field. Below the search bar is a table listing devices. The table has columns for 'DeviceName/备注名称', '设备所属产品', '节点类型', '设备状态', '最后上线时间', '启用/禁用', and '操作'. One device is listed: 'device001' under the product 'SmartKits', with a status of '在线' (Online) and an '启用' (Enable) toggle switch. Below the table are buttons for '删除' (Delete), '禁用' (Disable), and '启用' (Enable). The left sidebar contains navigation options like '公共实例', '实例详情', '设备管理', '产品', '设备', '分组', '设备模拟器', '设备分发', 'IoT孪生引擎', '消息转发', '监控运维', and '安全中心'. The top navigation bar includes the Alibaba Cloud logo, '工作台' (Workbench), '账号全部资源' (All Account Resources), '华东2 (上海)' (East China 2 (Shanghai)), a search bar, and various utility icons like '费用' (Billing), 'ICP 备案' (ICP Filing), '企业' (Company), '支持' (Support), '工单' (Tickets), '购物车' (Shopping Cart), '帮助' (Help), and '简体中文' (Simplified Chinese).