设备发放

快速入门

文档版本 05

发布日期 2024-10-25

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 使用前必读

MQTT 概述

MQTT标准规范参见《**mqtt-v3.1.1-os.pdf**》。

说明

MQTT的语法和接口细节，请以此标准为准。设备发放目前仅支持MQTTS/HTTPS这种安全接入的设备进行发放，暂不支持MQTT/HTTP这种非安全接入的设备进行发放。

MQTT消息分为固定报头（Fixed header）、可变报头（Variable header）和有效载荷（Payload）部分。

固定报头（Fixed header）和可变报头（Variable header）格式的填写直接MQTT标准规范。有效载荷（Payload）部分在PUB消息中可以由应用定义，即设备和设备发放平台之间自己定义。

下面主要介绍CONNECT、SUB和PUB消息格式的填写。

- CONNECT - Client requests a connection to a server

  有效载荷（Payload）中的主要参数填写，具体参见**MQTT CONNECT连接鉴权**。
- SUBSCRIBE - Subscribe to named topics

  有效载荷（Payload）中的主要参数填写：Topic name，填写为设备想要订阅的主题消息，目前填写为设备自己的topic，具体参见**Topic说明**。
- PUBLISH - Publish message
  - 可变报头（Variable header）：Topic name，设备发往设备发放平台时，为平台的Topic name，设备接收消息时，为设备的Topic name，具体参见**Topic说明**。
  - 有效载荷（Payload）中的主要参数填写：为完整的数据上报和命令下发的消息内容，目前是一个JSON对象。

Topic 说明

- 设备发放平台作为消息接收方时，已默认订阅了相关Topic，设备只要向对应Topic发送消息，设备发放平台就可以接收。
- 设备作为消息接收方时，需要先订阅相关Topic，这样设备发放平台向对应Topic发送消息时，设备才能接收到。设备需要根据具体实现的业务来决定订阅哪些Topic。

表 1-1 设备发放 Topic

Topic	消息发送方（Publisher）	消息接收方（Subscriber）	说明
$oc/devices/{device_id}/sys/bootstrap/up	设备	设备发放平台	设备向发放服务请求对应设备接入实例的引导信息。
$oc/devices/{device_id}/sys/bootstrap/down	设备发放平台	设备	设备接收发放服务下发的引导信息。

场景示例矩阵

表 1-2 示例列表

注册/注册组	认证类型	策略类型	示例
注册	证书认证	证书策略	MQTT X.509证书认证设备使用证书策略发放示例
注册	密钥认证	静态策略	MQTT 密钥设备使用静态策略发放示例
注册组	证书认证	自定义策略	MQTT 注册组自定义策略发放示例
注册组	云证书认证	证书策略	MQTT 华为云证书注册组发放示例
注册组	证书认证	自定义策略	MQTT 注册组自定义策略发放示例
注册	密钥认证	静态策略（跨账号）	MQTT 密钥设备跨账号使用静态策略发放示例

2 设备安全认证

设备接入设备发放和接入平台之前，需要通过身份认证。当前，物联网平台支持密钥认证和X.509证书认证两种认证方式进行设备身份认证。

密钥认证

创建设备时，认证方式选择密钥认证，用户为设备指定或者平台自动生成设备密钥。设备接入平台时，携带密钥（为避免密钥在通信链路中直接传输，实际传输值为密钥衍生内容，衍生方式参见**MQTT CONNECT连接鉴权**章节中的Password参数说明）。

X.509 证书认证

X.509是一种用于通信实体鉴别的数字证书，物联网平台支持设备使用自己的X.509证书进行认证鉴权。使用X.509认证技术时，设备无法被仿冒，避免了密钥被泄露的风险。

使用X.509证书认证的完整操作流程为：

1. 在平台上传设备CA证书并完成验证（或使用华为云证书服务的私有CA）；

2. 创建设备或注册组时，认证方式选择X.509证书认证，并关联已认证的设备CA证书；

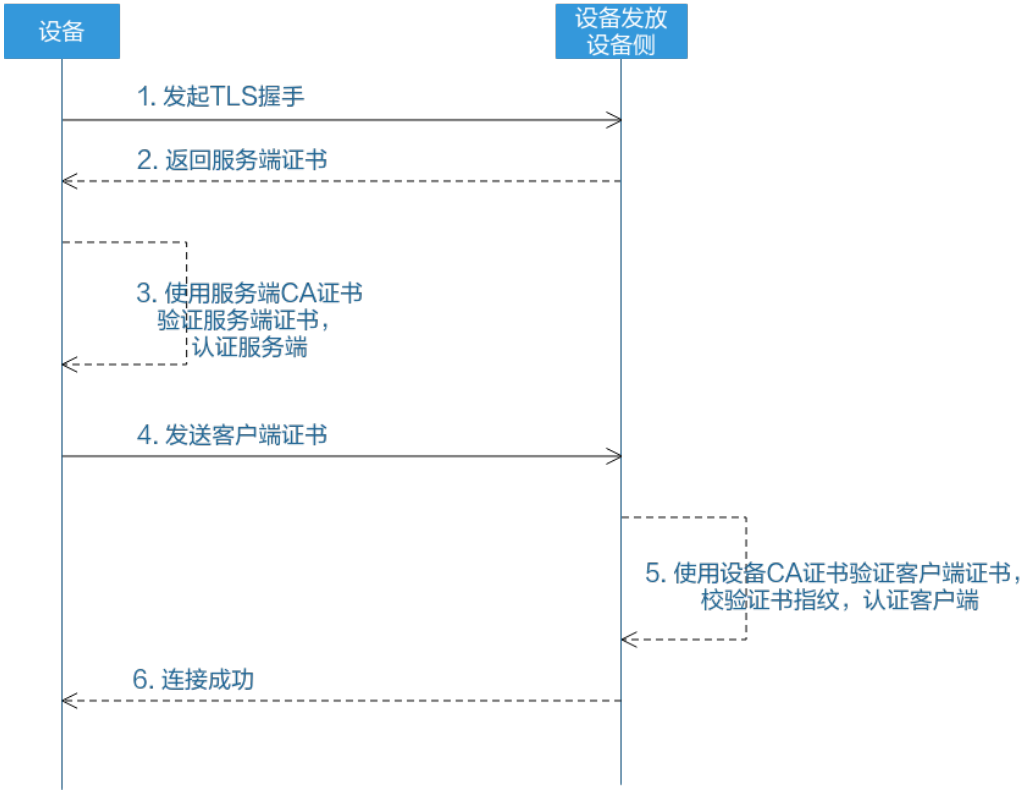
3. 开发设备端，将X.509证书及其私钥烧录到设备上；

4. 设备在与平台双向认证过程中，设备验证平台证书，平台使用设备CA证书验证设备证书并验证设备证书与设备的关联关系。

X.509 双向证书认证

X.509证书双向认证过程，涉及到设备发放（平台）和设备两端，过程如下图所示。

图 2-1 X.509 双向证书认证



双向证书认证过程中使用到了如下几类证书：

表 2-1 证书类型列表

证书	说明	证书及其私钥持有者	签发者
服务端证书	步骤2中，设备发放设备侧将该证书返回设备。	设备发放设备侧持有	权威CA（服务端证书的CA证书）签发
服务端CA证书	步骤3中，客户端使用该服务端CA证书验证服务端证书，通常为权威CA证书，获取方式见**MQTT CONNECT连接鉴权**。	权威CA机构持有	权威CA机构签发
设备证书（客户端证书）	步骤4中，设备将该证书发送给设备发放设备侧。	设备	CA证书

证书	说明	证书及其私钥持有者	签发者
CA证书（设备CA证书/客户端CA证书）	步骤5中，设备发放设备侧使用该CA证书验证来自设备的客户端证书。用户通过应用侧上传该证书到设备发放平台。	用户	通常为自签发

说明

双向认证，即双向证书认证，与单向认证中不同的是，不仅包含单向认证中的设备对平台的证书验证步骤，还包含了平台对设备的证书验证步骤。

3 接口说明

3.1 MQTT CONNECT 连接鉴权

接口功能

设备发放平台设备侧支持MQTT协议的connect消息接口，接口规范参考**MQTT标准规范**，鉴权通过后建立设备与平台间的MQTT连接。

说明

设备发放平台目前只支持MQTTS接入，设备通过connect消息接口和平台建立MQTT连接时，需要使用服务端CA证书验证服务端证书。服务端CA证书单击**huaweicloud-iot-root-ca-list**获取证书文件压缩包。 根据您使用的工具或语言取用压缩包内的证书文件：

- IoT Device SDK（C/C#）、MQTT.fx工具：使用压缩包中c目录下以pem或crt为后缀的文件；
- IoT Device SDK（Java）：使用压缩包中java目录下以jks为后缀的文件；
- IoT Device SDK（Android）：使用压缩包中android目录下以bks为后缀的文件。

参数说明

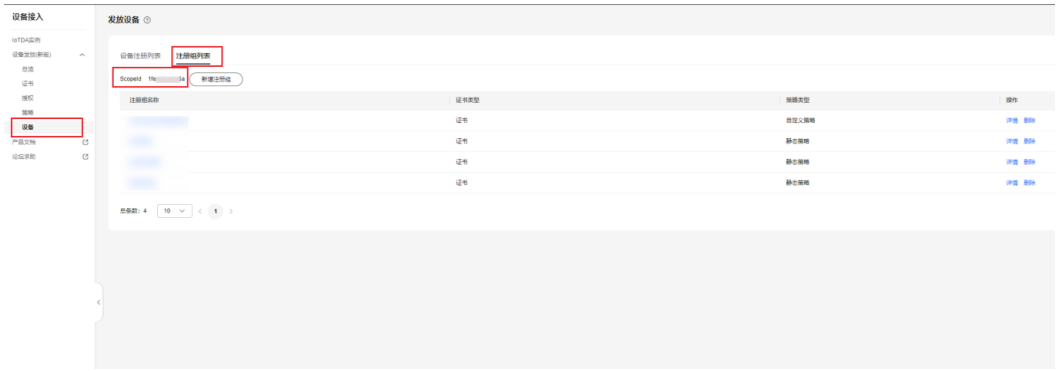
表 3-1 设备发放参数说明列表

参数	必选/可选	类型	参数描述

clientId	必选	String(256)	注册组选择非华为云证书场景： 设备clientId由3个部分组成：设备ID、设备身份标识类型、用户标识ID（ScopeID）。通过下划线“_”分隔，设备身份标识类型固定值为0 例：5f052ac562369102d42b0fb6_0_ff5bbx7a488f 其他场景： 设备clientId由4个部分组成：设备ID、设备身份标识类型、密码签名类型、时间戳。通过下划线“_”分隔，设备身份标识类型固定值为0 ● 密码签名类型：长度1字节，当前支持2种类型： – “0”代表HMACSHA256不校验时间戳。 – “1”代表HMACSHA256校验时间戳。 ● 时间戳：为设备连接平台时的UTC时间，格式为YYYYMMDDHH，如UTC 时间2018/7/24 17:56:20 则应表示为2018072417。 例：5f052ac562369102d42b0fb6_0_0_2019122614
Username	必选	String(256)	设备ID。
Password	必选	String(256)	Password的值为使用“HMACSHA256”算法以时间戳为密钥，对secret进行加密后的值（secret为注册设备时平台返回的secret）。 当设备认证类型使用密钥认证接入（SECRET）需填写“Password”，证书认证接入（CERTIFICATES）不需填写“Password”。

注：ScopeID可以在设备发放页面单击注册组查询，如下图所示。

图 3-1 查看 ScopeId



设备通过MQTT协议的connect消息进行鉴权，对于构造clientId的各个部分信息都必须包括进去，平台收到connect消息时，会判断设备的鉴权类型和密码摘要算法。

- 当采用“HMACSHA256”校验时间戳方式时，会先校验消息时间戳与平台时间是否一致，再判断密码是否正确。

- 当采用“HMACSHA256”不校验时间戳方式时，鉴权消息也必须带时间戳，但不检验时间是否准确，仅判断密码是否正确。

connect消息鉴权失败时，平台会返回错误，并自动断开MQTT链路。

说明

访问**参数生成工具**，填写注册设备后生成的设备ID（DeviceId）和密钥（DeviceSecret），生成设备连接鉴权所需的参数（ClientId、Username、Password）。

3.2 设备请求引导消息

接口功能

设备向发放服务请求对应设备接入实例的引导信息。

Topic

表 3-2 上报 Topic 说明

Topic	$oc/devices/{device_id}/sys/bootstrap/up
消息发送方	设备
消息接收方	设备发放平台

示例

设备向发放服务发送的payload为空。

3.3 设备接收引导信息

接口功能

设备接收发放服务下发的引导信息。

Topic

表 3-3 下发 Topic 说明

Topic	$oc/devices/{device_id}/sys/bootstrap/down
消息发送方	设备发放平台
消息接收方	设备

参数说明

表 3-4 下发参数说明

参数	必选/可选	类型	描述
address	必选	String	对应设备接入实例的接入地址。
initConfig	必选	String	客户在创建设备，或者创建注册组时自定义的初始化Json字符串。

示例

```
设备先订阅Topic后才能收到命令推送，设备接收到的payload:
{
    "address": "10.0.0.1:8883",
    "initConfig":"{\n\"init\":23\n}"
}
```

4 MQTT 场景--使用 MQTT.fx 接入设备发放示例

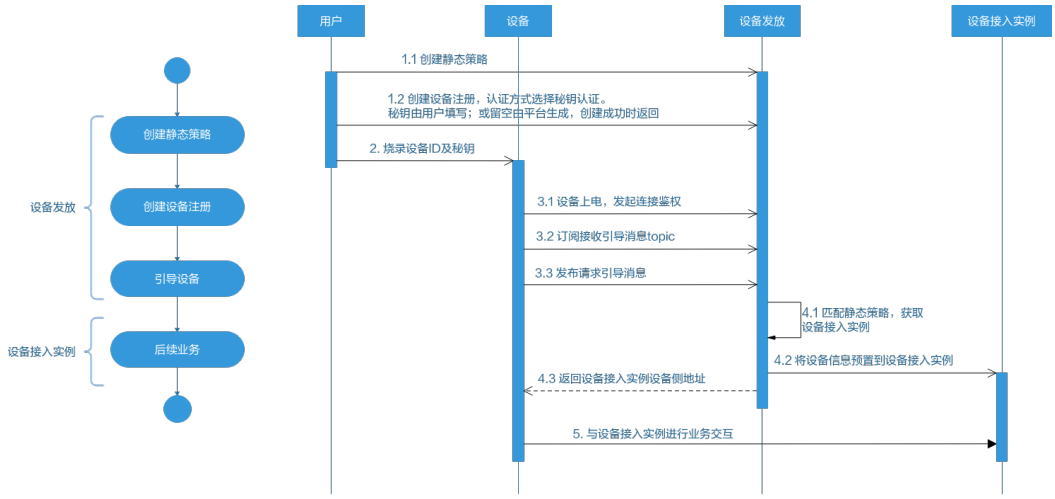
4.1 MQTT 密钥设备使用静态策略发放示例

获取设备发放终端节点

表 4-1 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



添加静态策略

添加静态策略，根据关键字发放到指定的IoTDA。

图 4-1 创建静态策略

图 4-2 创建静态策略详情

注册设备

在设备发放控制台，注册MQTT设备，其中安全模式选择密钥模式（如果需要下发初始化配置，那么对应在初始设备配置选项中填写对应的JSON字符串，设备发放不理解该字段，只是透传该JSON字符串，由设备理解解析。如果不需要下发改字段则不填）。

图 4-3 注册设备

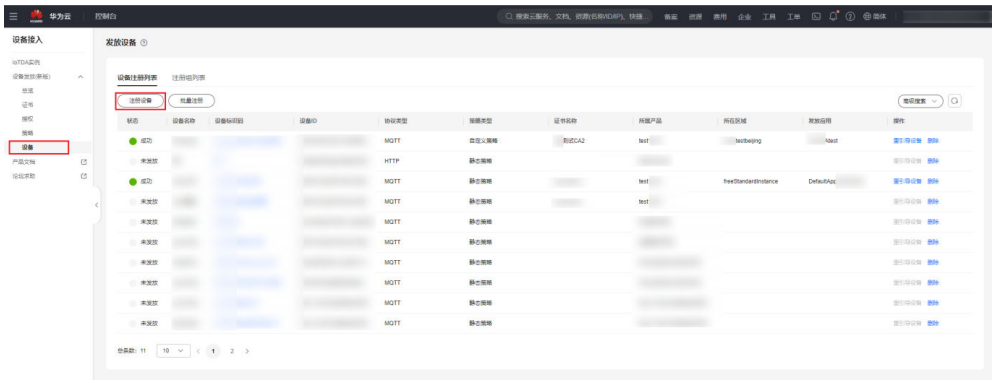
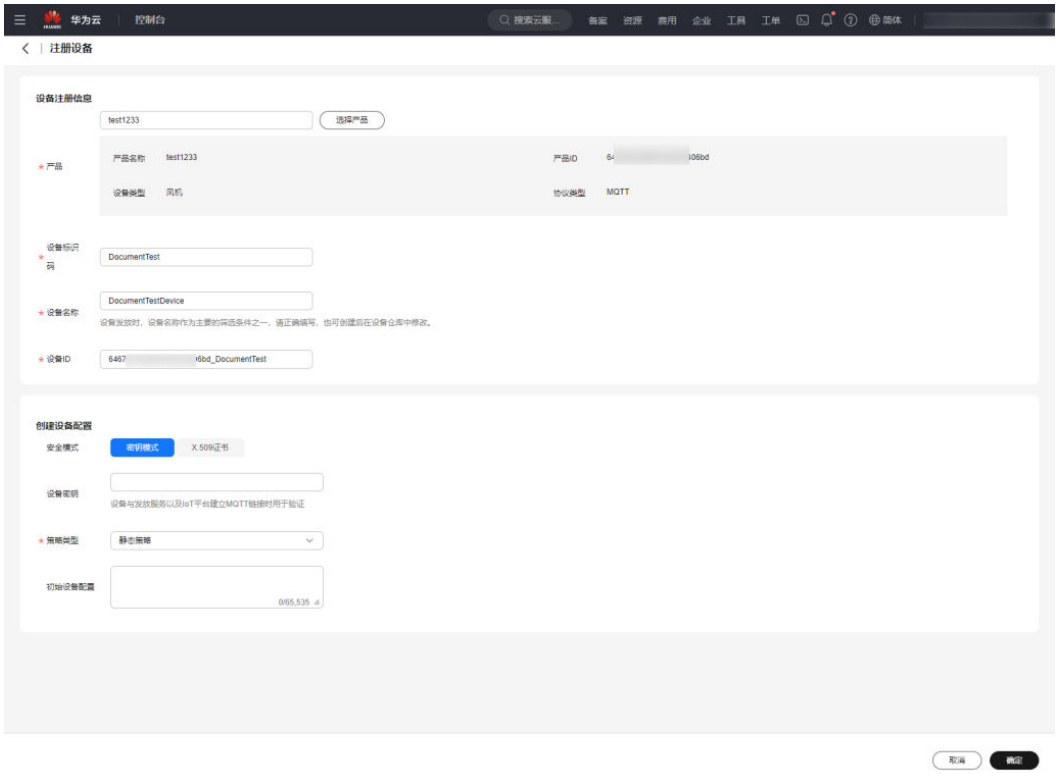


图 4-4 创建密钥模式静态策略设备



说明

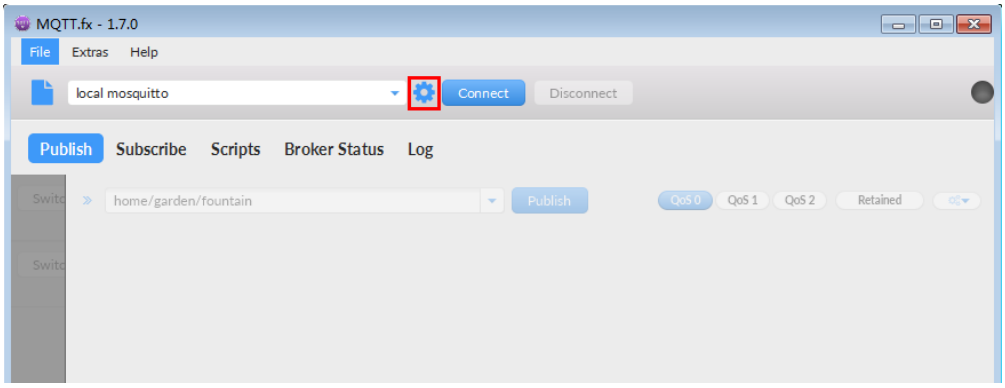
此处注册设备的设备名称需与**添加静态策略**步骤的策略实例关键字相匹配，方能触发该静态策略。

连接鉴权

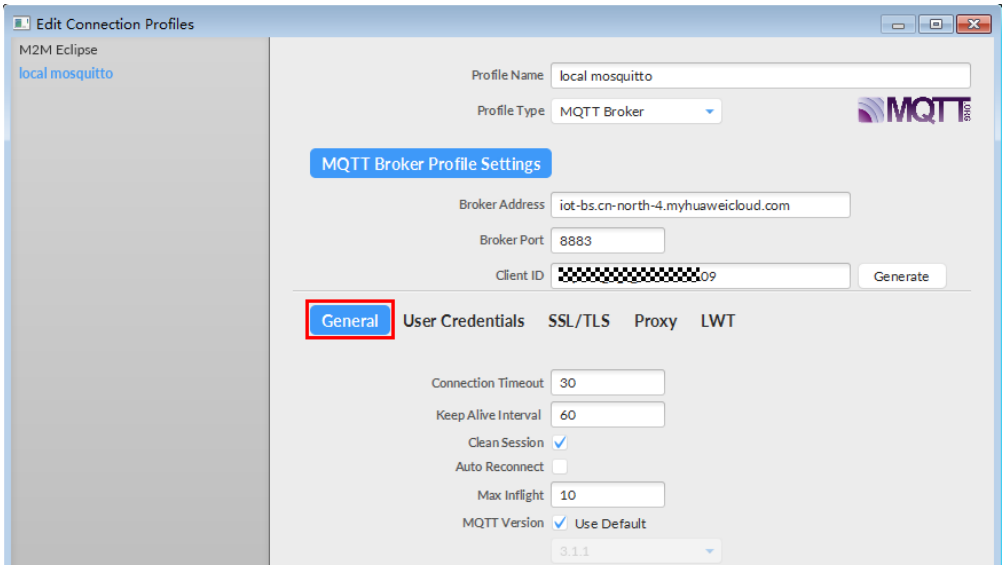
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

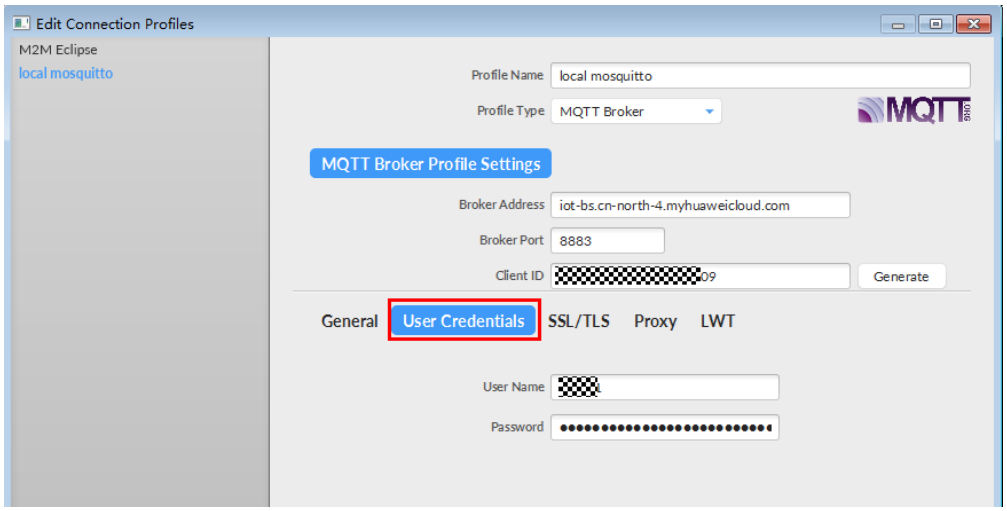
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



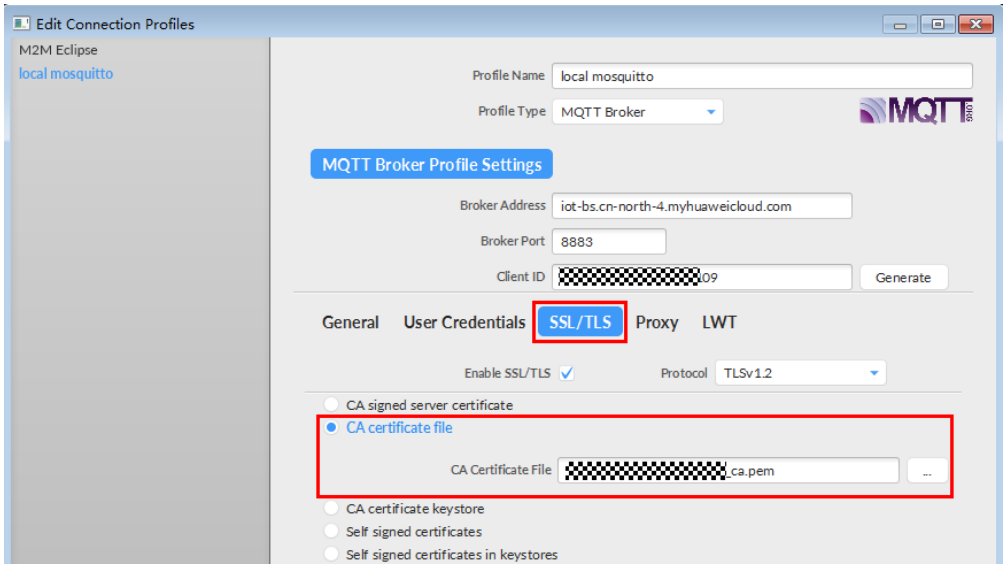
4. 填写 User Credentials 信息。



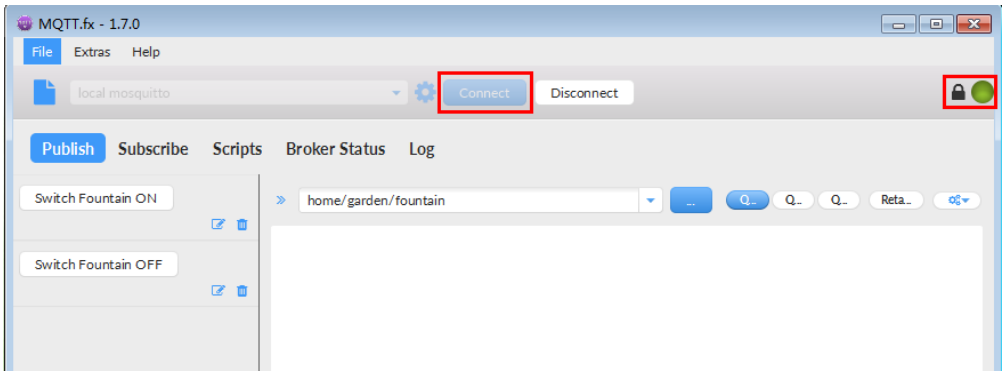
说明

其中Username 和Password 参数参考**MQTT CONNECT连接鉴权**参数说明。

5. 选择开启 SSL/TLS，勾选CA certificate file，CA Certificate File指定为物联网平台根证书（请先下载**物联网平台的根证书**，解压后，选择其中c或java目录下PEM后缀的文件）的本地路径。

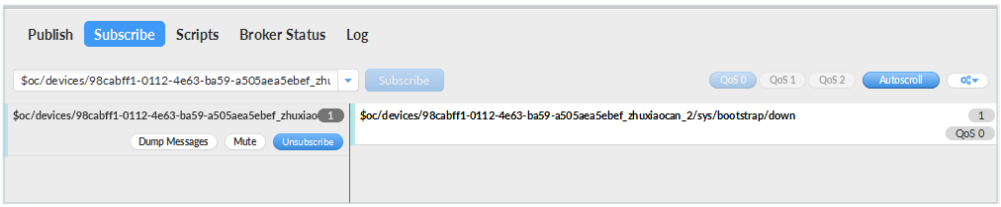


6. 完成以上步骤后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



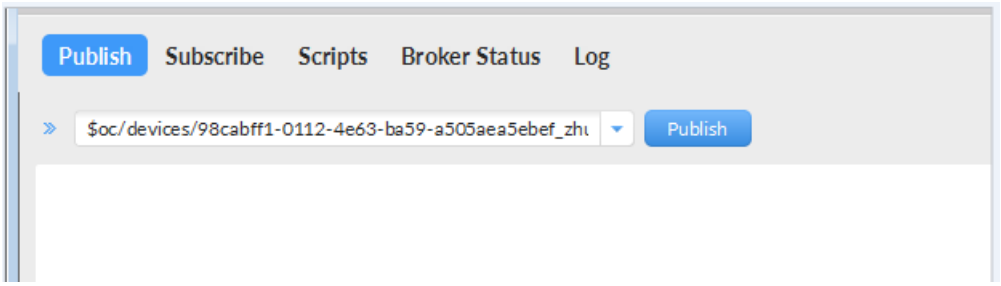
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



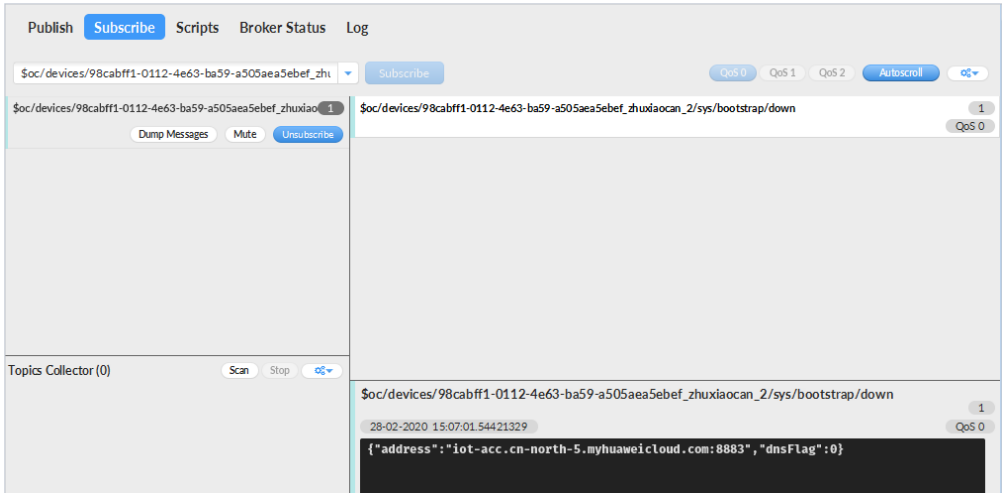
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

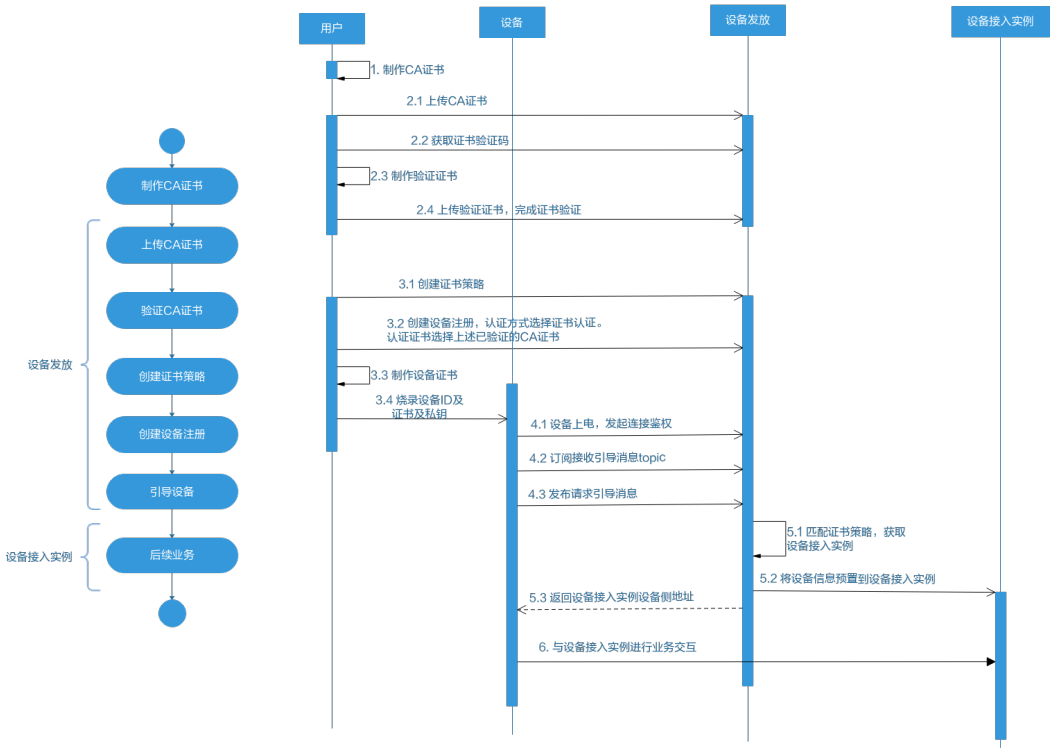
4.2 MQTT X.509 证书认证设备使用证书策略发放示例

获取设备发放终端节点

表 4-2 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



制作 CA 证书

步骤1 在浏览器中访问这里，下载并进行安装OpenSSL工具，安装完成后配置环境变量。

步骤2 在 D:\certificates 文件夹下，以管理员身份运行cmd命令行窗口。

步骤3 生成密钥对（rootCA.key）：

说明

生成“密钥对”时输入的密码在生成“证书签名请求文件”、“CA证书”，“验证证书”以及“设备证书”时需要用到，请妥善保存。

```
openssl genrsa -des3 -out rootCA.key 2048
```

步骤4 使用密钥对生成证书签名请求文件：

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下表1 所示。

表 4-3 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong

提示	参数名称	取值样例
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

```
openssl req -new -key rootCA.key -out rootCA.csr
```

步骤5 生成CA证书（rootCA.crt）：

```
openssl x509 -req -days 50000 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
```

说明

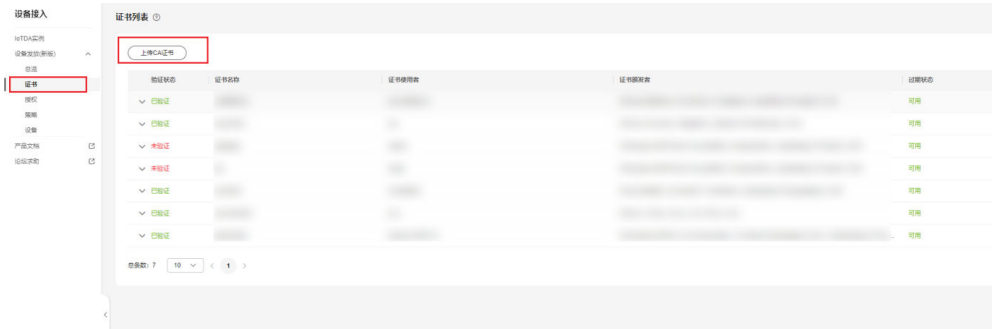
“-days”后的参数值指定了该证书的有效天数，此处示例为50000天，您可根据实际业务场景和需要进行调整。

----结束

上传并验证 CA 证书

步骤1 登录设备发放控制台，进入“证书”界面，单击右上角“上传CA证书”，填写“证书名称”并上传上述“制作CA证书”步骤后生成的“CA证书（rootCA.crt文件）”，单击“确定”。

图 4-5 上传 CA 证书

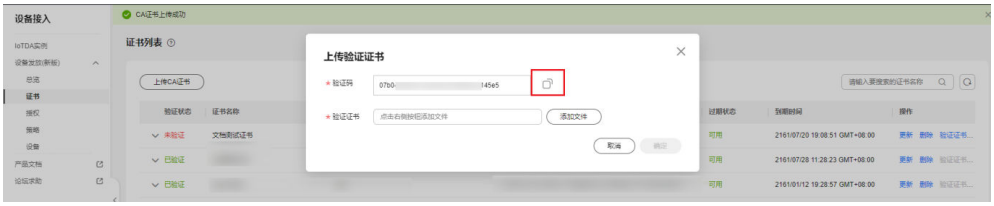


步骤2 验证步骤1中上传的CA证书，只有成功验证证书后该证书方可使用。

1. 为验证证书生成密钥对。
```
openssl genrsa -out verificationCert.key 2048
```
2. 获取随机验证码。

图 4-6 上传 CA 证书完成页

图 4-7 复制验证码



3. 利用此验证码生成证书签名请求文件CSR。
```
openssl req -new -key verificationCert.key -out verificationCert.csr
```

说明

CSR文件的Common Name (e.g. server FQDN or YOUR name) 需要填写前一过程中获取到的随机验证码。

4. 使用CA证书、CA证书私钥和CSR文件创建验证证书（verificationCert.crt）。
```
openssl x509 -req -in verificationCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out verificationCert.crt -days 500 -sha256
```

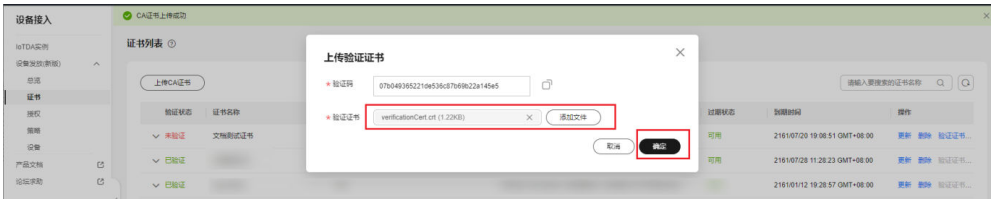
说明

生成验证证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件。

“-days”后的参数值指定了该证书的有效天数，此处示例为500天，您可根据实际业务场景和需要进行调整。

5. 上传验证证书进行验证。

图 4-8 上传验证证书



----结束

生成设备证书

步骤1 使用OpenSSL工具为设备证书生成密钥对（设备私钥）：
```
openssl genrsa -out deviceCert.key 2048
```


步骤2 使用设备密钥对，生成证书签名请求文件：

```
openssl req -new -key deviceCert.key -out deviceCert.csr
```

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下表2所示。

表 4-4 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

步骤3 使用CA证书、CA证书私钥和CSR文件创建设备证书（deviceCert.crt）。

```
openssl x509 -req -in deviceCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out deviceCert.crt -days 36500 -sha256
```

说明

生成设备证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件，且需要完成“上传并验证CA证书”。

“-days”后的参数值指定了该证书的有效天数，此处示例为36500天，您可根据实际业务场景和需要进行调整。

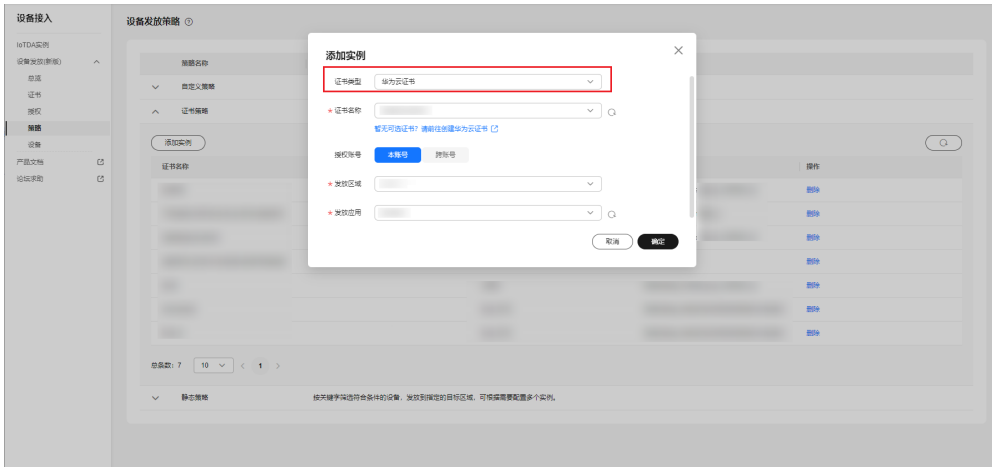
----结束

添加证书策略

添加证书策略，发放CA证书到指定的IoTDA，并且由此CA签发的设备证书都会发放到指定的IoTDA。

图 4-9 添加证书策略

图 4-10 添加证书策略详情



注册设备

在设备发放控制台，注册MQTT设备，其中安全模式选择X.509认证模式，选择对应的CA证书，填写证书指纹，注册X.509认证设备。

图 4-11 注册设备

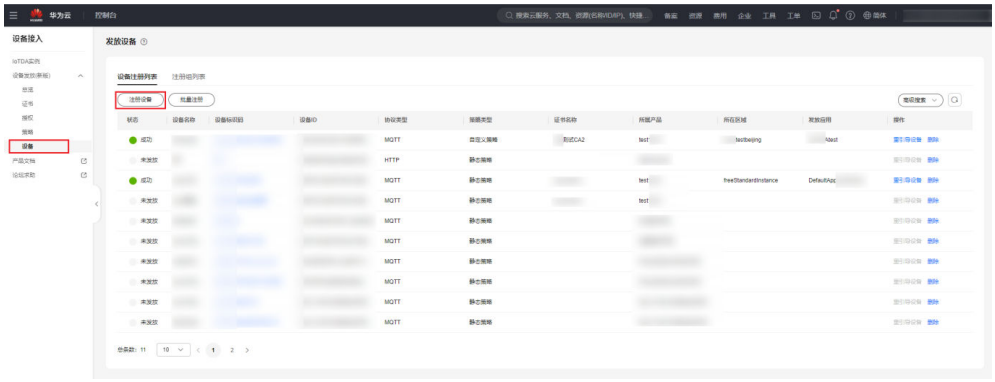
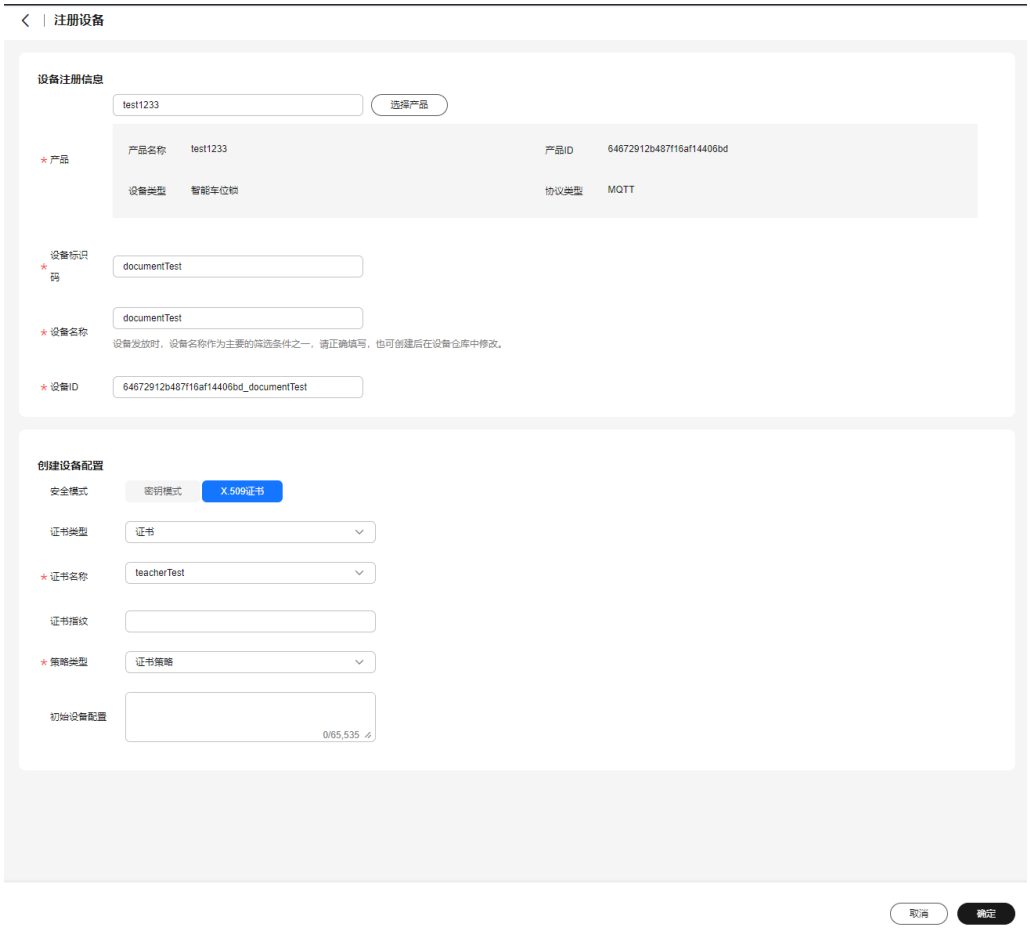


图 4-12 创建证书模式证书策略设备



说明

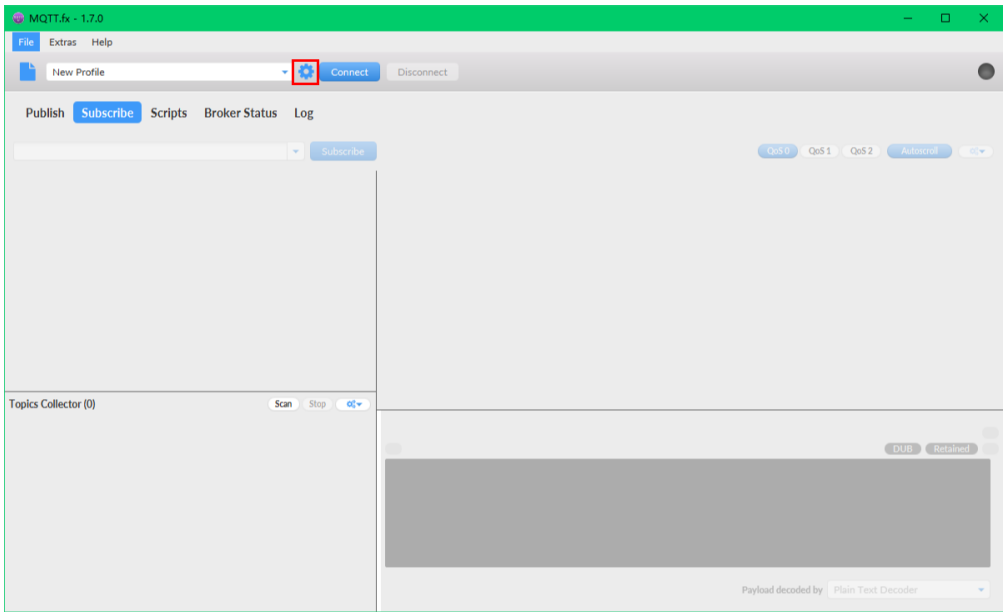
证书指纹是根据证书生成的唯一识别证书的标识。如果支持设备自注册，在设备首次认证时不会去认证设备ID和设备证书的关系。

连接鉴权

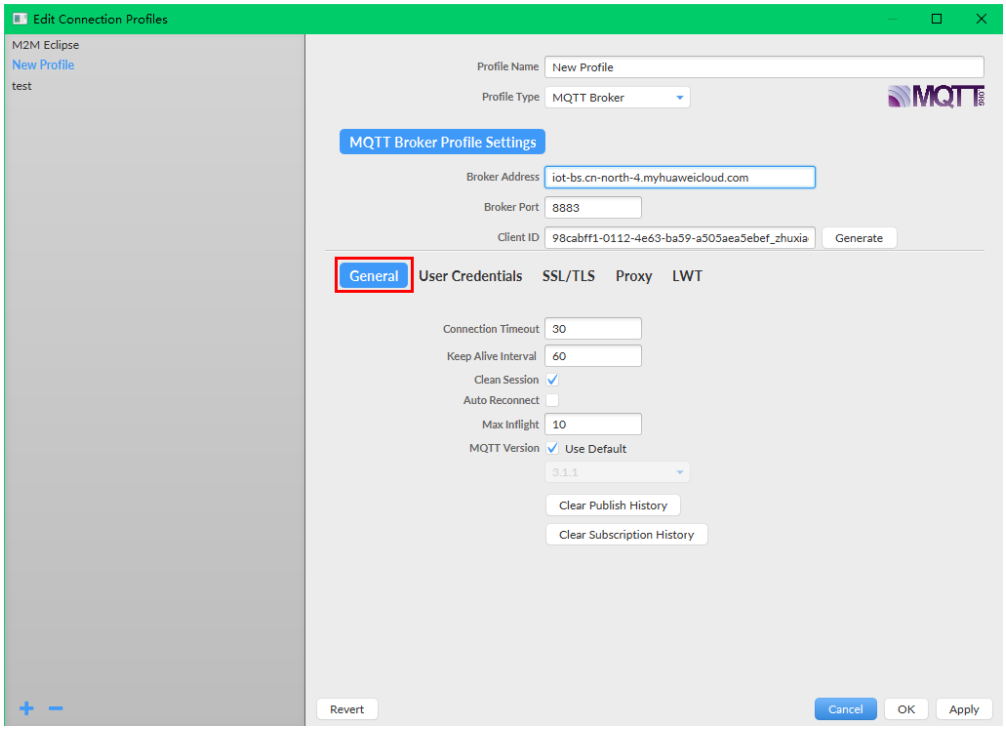
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



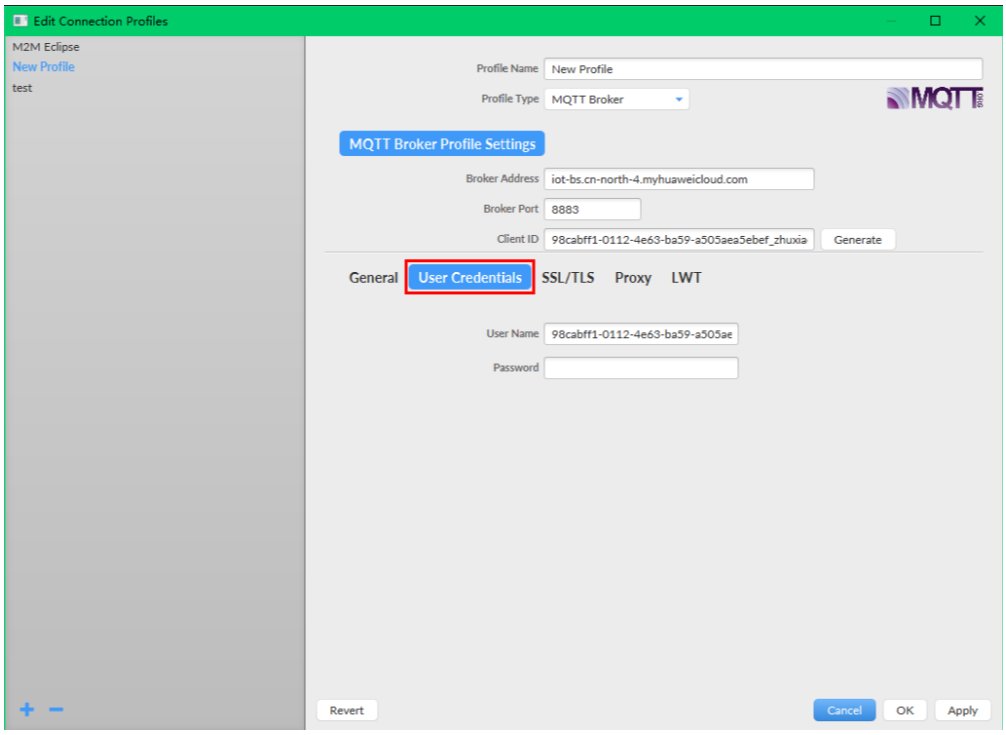
3. 填写 Connection Profile 相关信息。其中General 可以使用工具默认信息。



说明

其中Broker Address和Broker Port可以参考**获取终端节点**，Client ID 可以参考**MQTT CONNECT连接鉴权**参数说明，访问**这里**填写设备ID（DeviceId）等设备信息，生成连接信息（ClientId、Username、Password）。

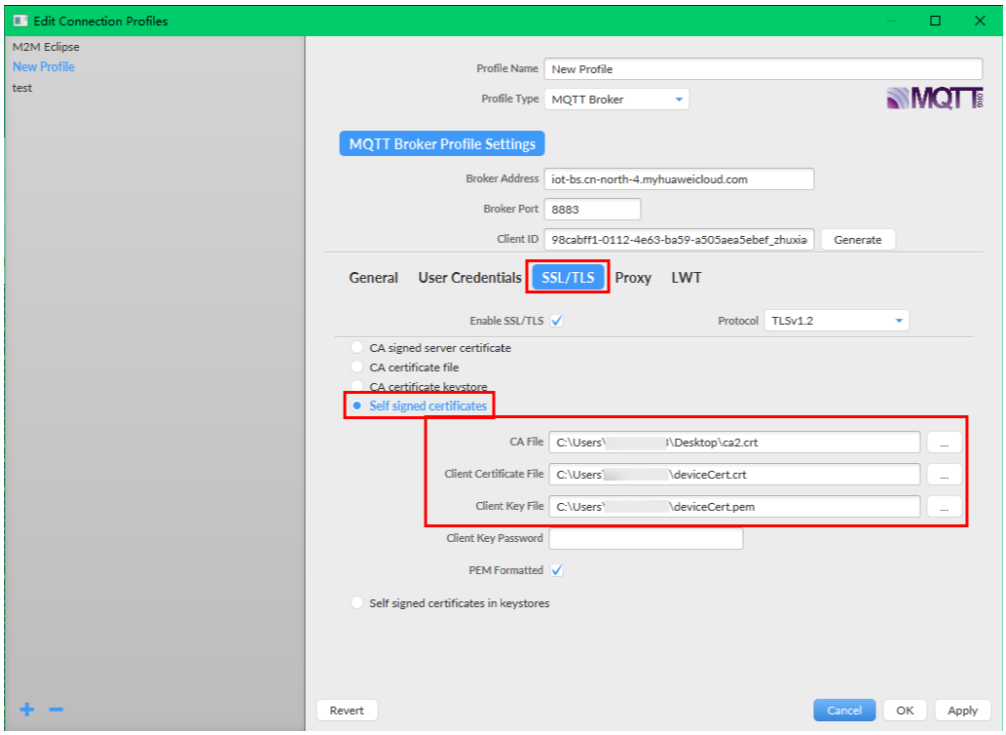
4. 填写 User Credentials 信息。



说明

其中Username 参考**MQTT CONNECT连接鉴权**参数说明（无需填写Password）。

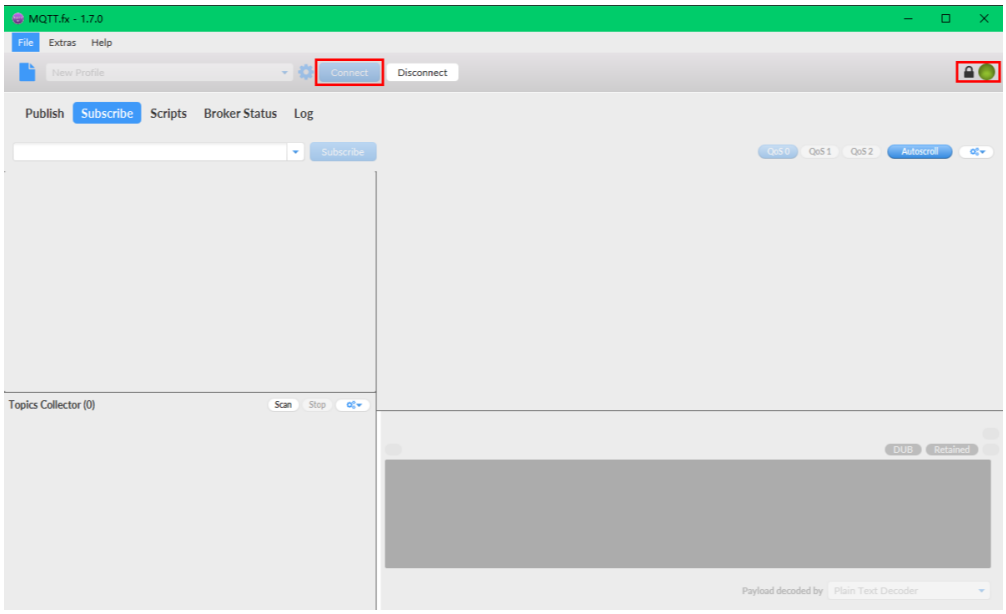
5. 选择开启 SSL/TLS，勾选 Self signed certificates，配置相关证书内容。



说明

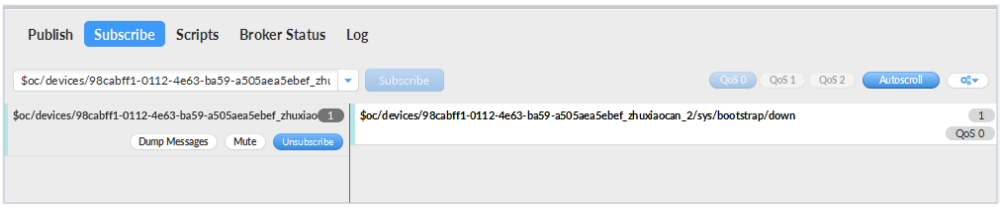
- CA File为设备发放对应的CA证书。
- Client Certificate File为设备的设备证书。
- Client Key File为设备的私钥。

6. 完成以上步骤设置后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



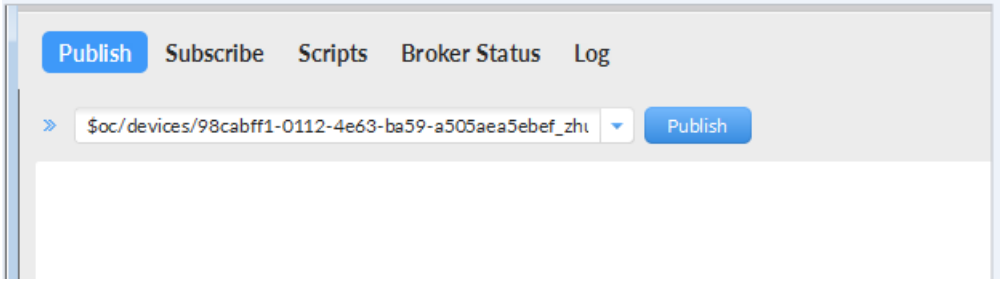
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



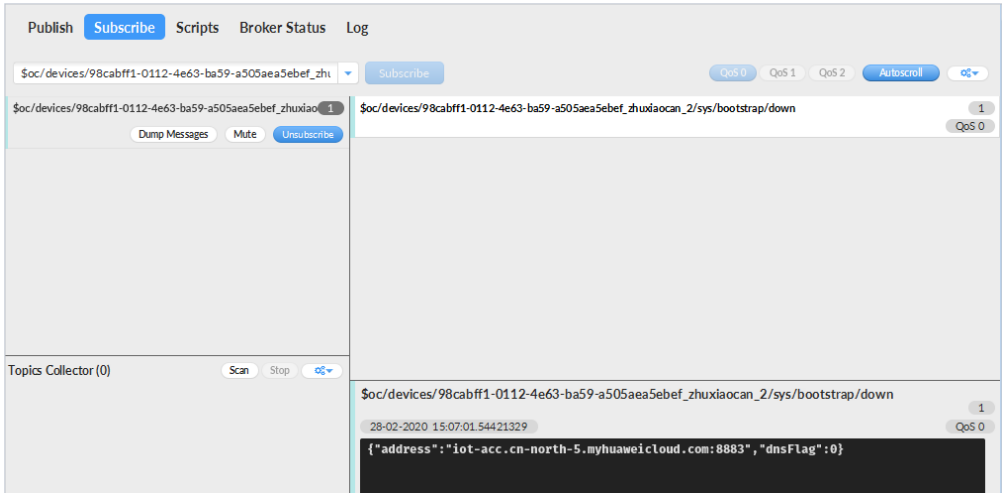
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

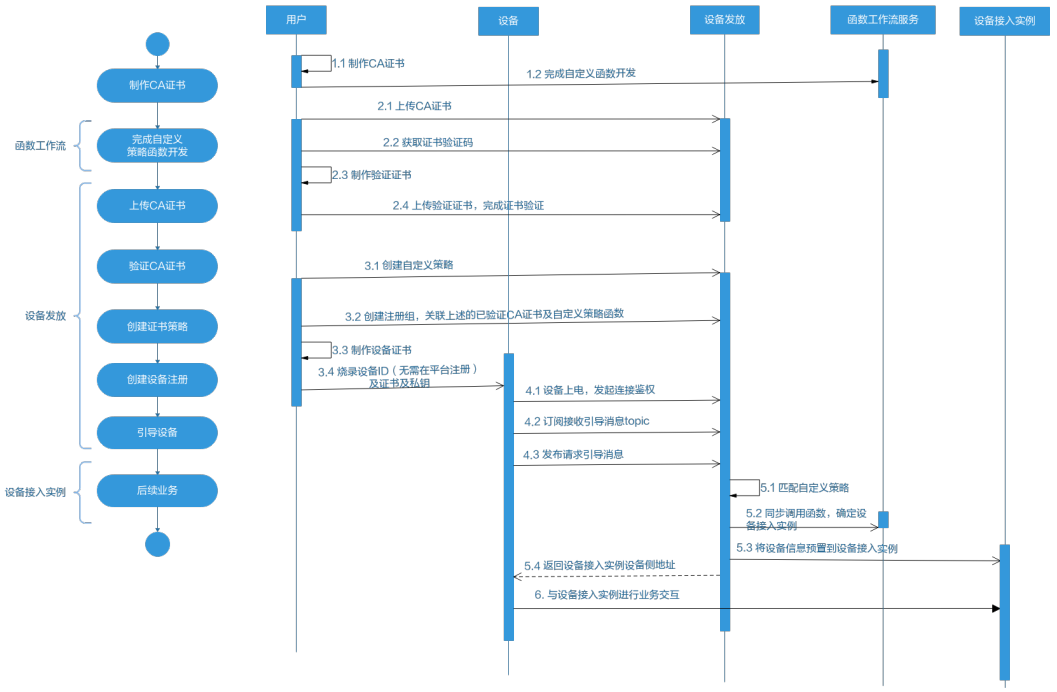
4.3 MQTT 注册组自定义策略发放示例

获取设备发放终端节点

表 4-5 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



制作 CA 证书

步骤1 在浏览器中访问**这里**，下载并进行安装OpenSSL工具，安装完成后配置环境变量。

步骤2 在 D:\certificates 文件夹下，以管理员身份运行cmd命令行窗口。

步骤3 生成密钥对（rootCA.key）：

说明

生成“密钥对”时输入的密码在生成“证书签名请求文件”、“CA证书”，“验证证书”以及“设备证书”时需要用到，请妥善保存。

```
openssl genrsa -des3 -out rootCA.key 2048
```

步骤4 使用密钥对生成证书签名请求文件：

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下**表1** 所示。

表 4-6 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen

提示	参数名称	取值样例
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

```
openssl req -new -key rootCA.key -out rootCA.csr
```

步骤5 生成CA证书（rootCA.crt）：

```
openssl x509 -req -days 50000 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
```

说明

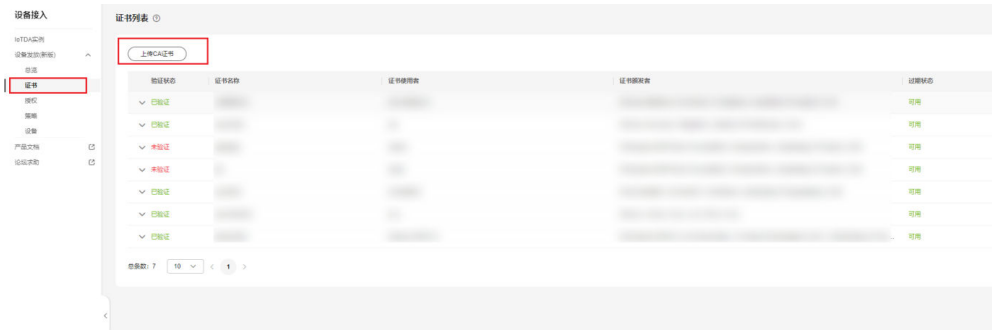
“-days”后的参数值指定了该证书的有效天数，此处示例为50000天，您可根据实际业务场景和需要进行调整。

----结束

上传并验证 CA 证书

步骤1 登录设备发放控制台，进入“证书”界面，单击右上角“上传CA证书”，填写“证书名称”并上传上述“制作CA证书”步骤后生成的“CA证书（rootCA.crt文件）”，单击“确定”。

图 4-13 上传 CA 证书

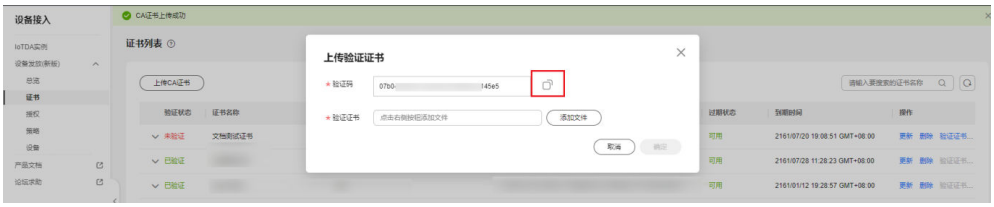


步骤2 验证步骤1中上传的CA证书，只有成功验证证书后该证书方可使用。

1. 为验证证书生成密钥对。
   ```
   openssl genrsa -out verificationCert.key 2048
   ```
2. 获取随机验证码。

图 4-14 上传 CA 证书完成页

图 4-15 复制验证码



3. 利用此验证码生成证书签名请求文件CSR。

```
openssl req -new -key verificationCert.key -out verificationCert.csr
```

说明

CSR文件的Common Name (e.g. server FQDN or YOUR name) 需要填写前一过程中获取到的随机验证码。

4. 使用CA证书、CA证书私钥和CSR文件创建验证证书（verificationCert.crt）。

```
openssl x509 -req -in verificationCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out verificationCert.crt -days 500 -sha256
```

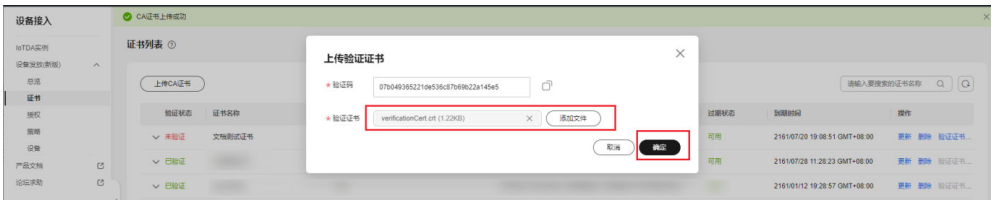
说明

生成验证证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件。

“-days”后的参数值指定了该证书的有效天数，此处示例为500天，您可根据实际业务场景和需要进行调整。

5. 上传验证证书进行验证。

图 4-16 上传验证证书



----结束

生成设备证书

步骤1 使用OpenSSL工具为设备证书生成密钥对（设备私钥）：

```
openssl genrsa -out deviceCert.key 2048
```

步骤2 使用设备密钥对，生成证书签名请求文件：

```
openssl req -new -key deviceCert.key -out deviceCert.csr
```


说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下表2所示。

表 4-7 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

步骤3 使用CA证书、CA证书私钥和CSR文件创建设备证书（deviceCert.crt）。

```
openssl x509 -req -in deviceCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out deviceCert.crt -days 36500 -sha256
```

说明

生成设备证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件，且需要完成“上传并验证CA证书”。

“-days”后的参数值指定了该证书的有效天数，此处示例为36500天，您可根据实际业务场景和需要进行调整。

----结束

添加自定义策略

添加自定义策略。

图 4-17 添加自定义策略

创建注册组

图 4-18 新增注册组

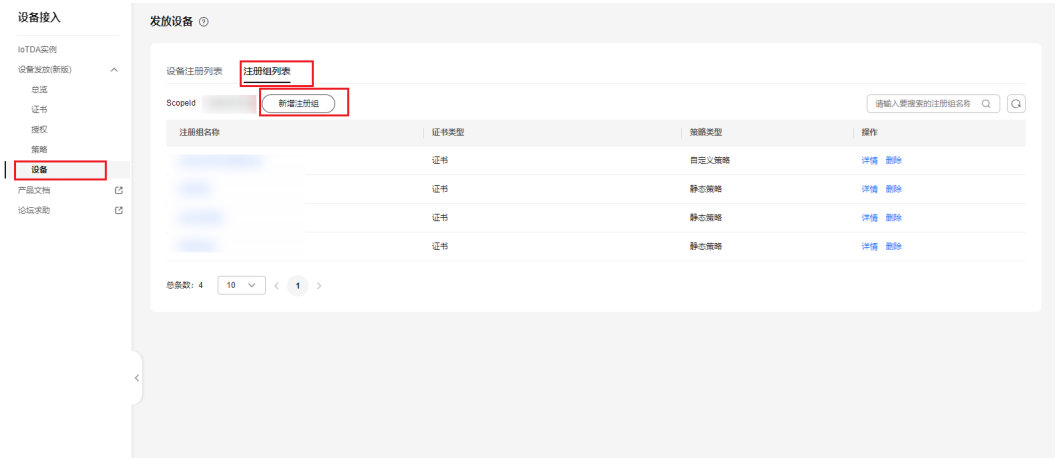
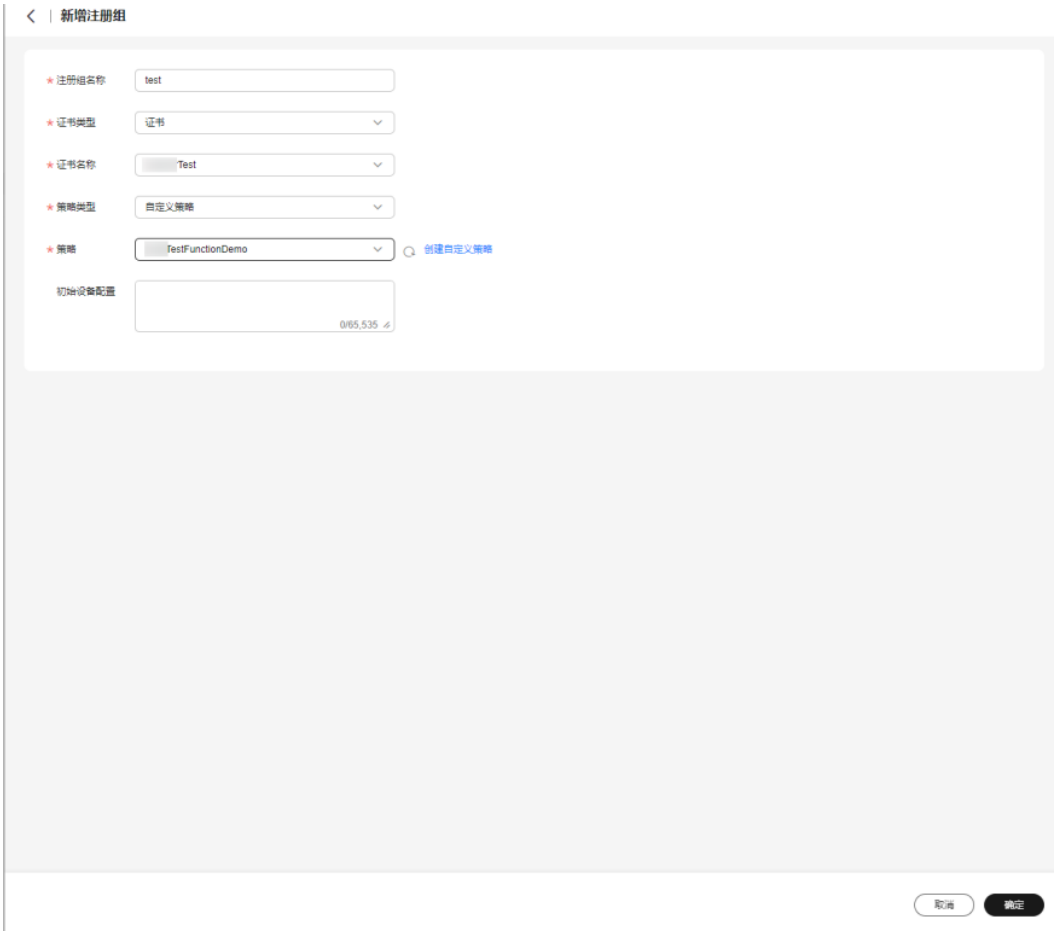


图 4-19 创建证书自定义注册组

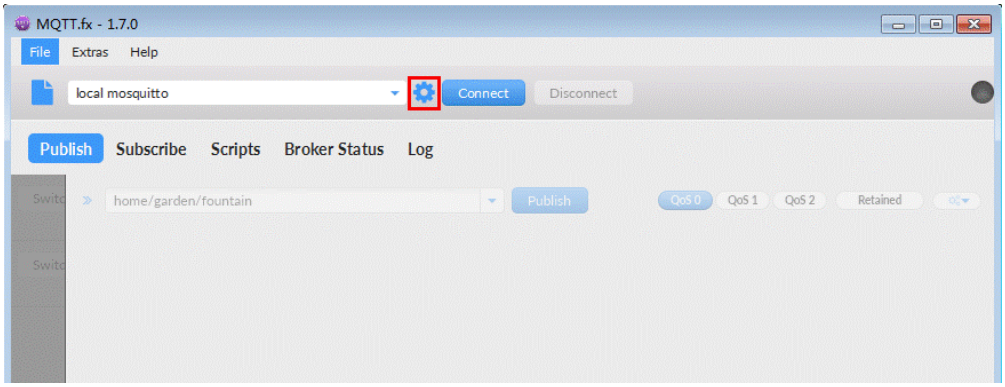


连接鉴权

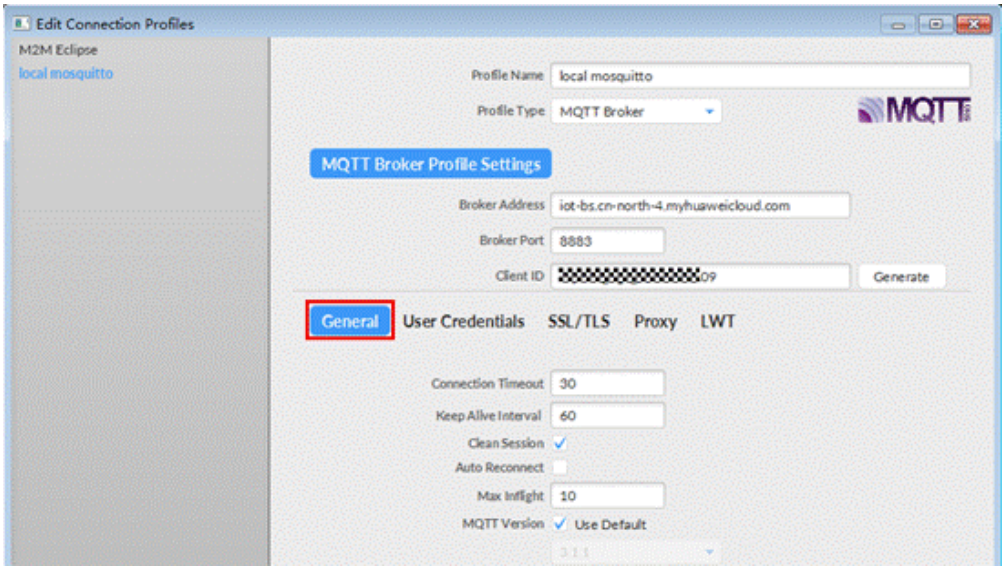
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

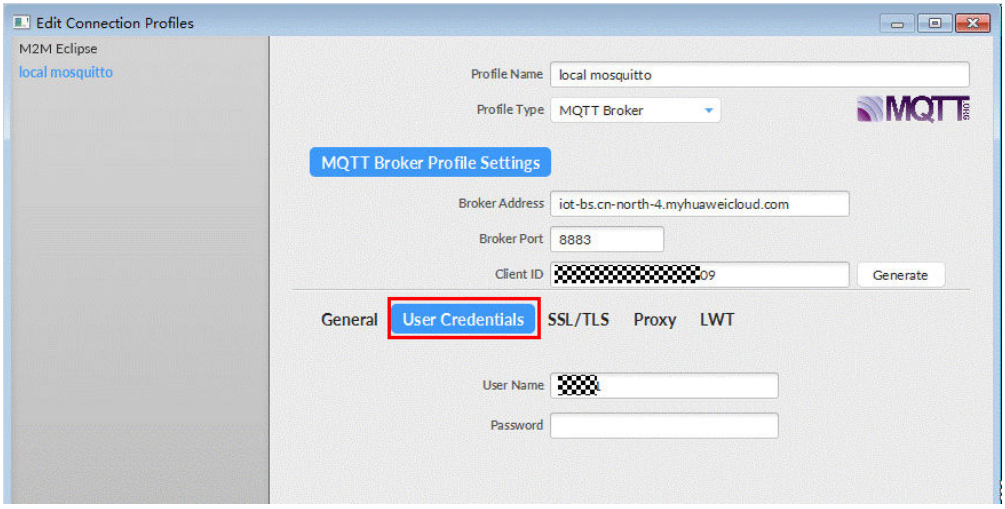
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



4. 填写 User Credentials 信息。

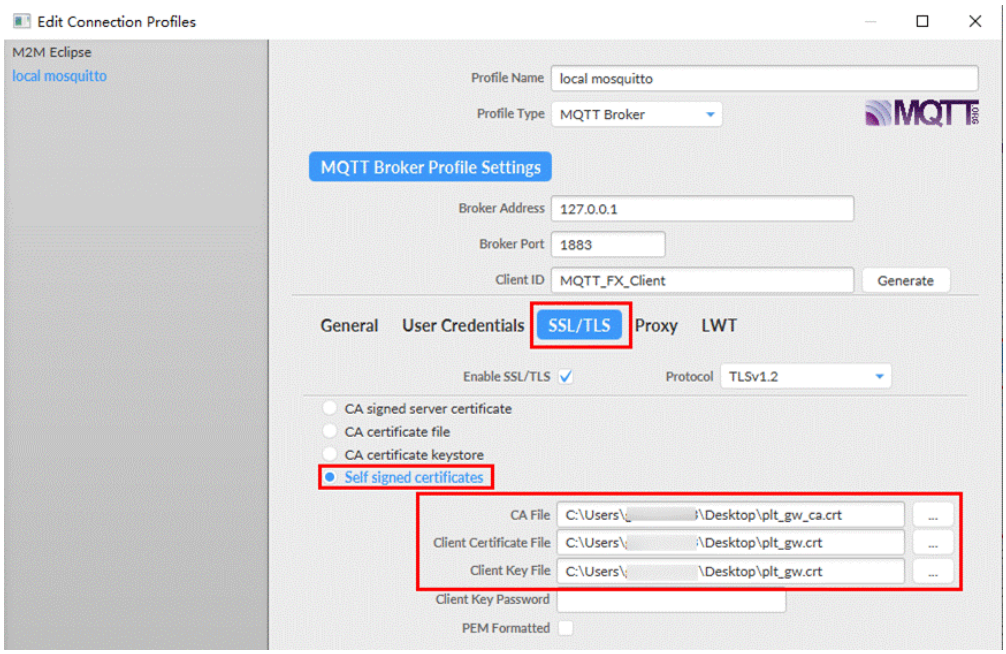


说明

其中Username 参考**MQTT CONNECT连接鉴权**参数说明（无需填写Password）。

注：注册组的场景不存在选择产品，所以命名需要注意：如果命名字符串有“_”，那么第一项必须为对应设备接入已经存在的产品ID，如果不包括“_”，那么可以随意命名。

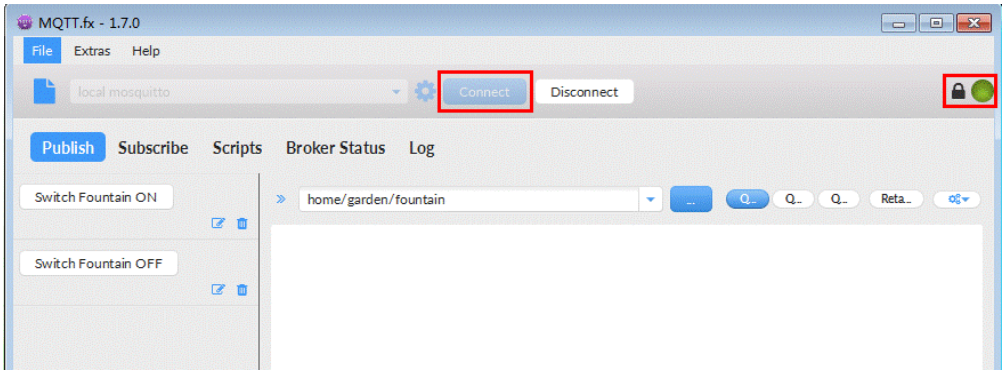
5. 选择开启 SSL/TLS，勾选Self signed certificates，配置相关证书内容。



说明

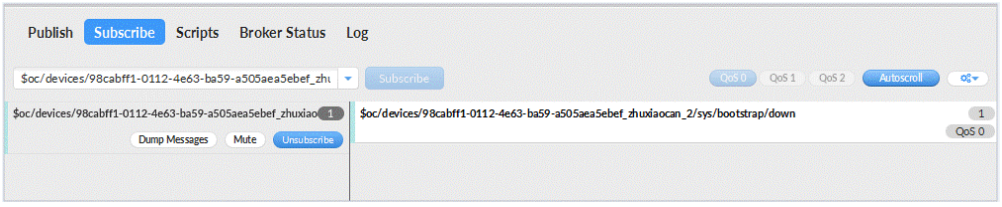
- CA File为设备发放对应的CA证书。
- Client Certificate File为设备的设备证书。
- Client Key File为设备的私钥。

6. 完成以上步骤后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



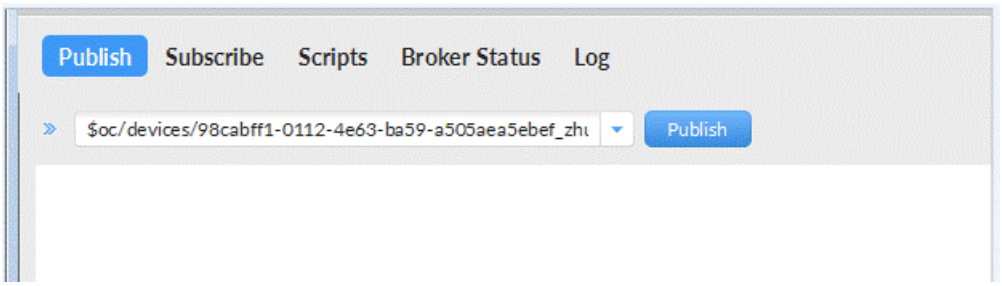
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



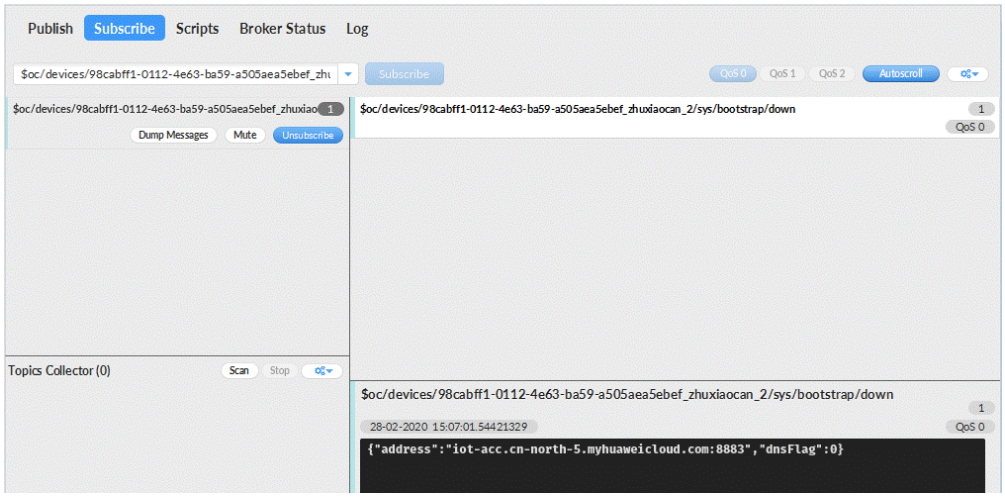
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

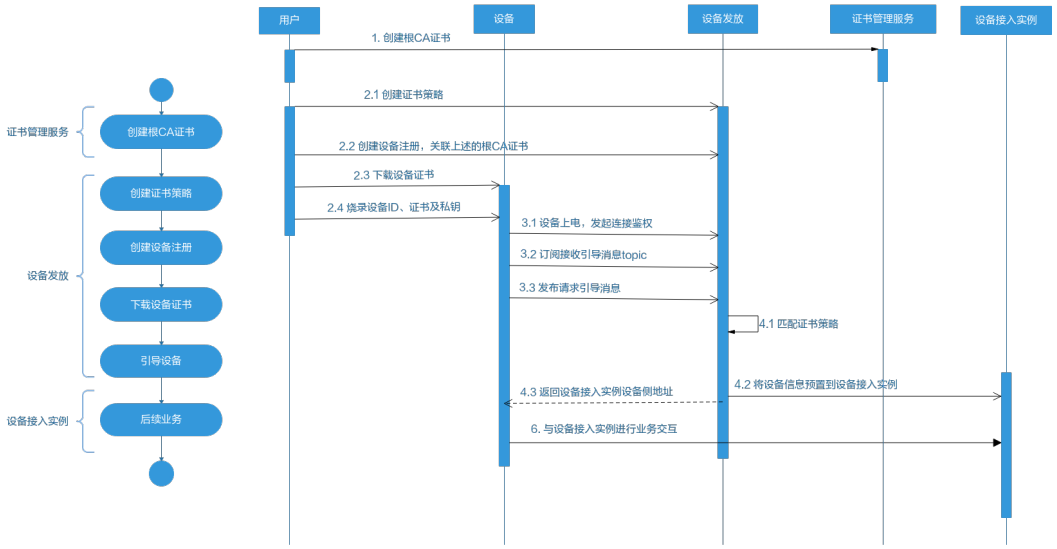
4.4 MQTT 华为云 X.509 证书认证设备使用证书策略发放示例

获取设备发放终端节点

表 4-8 设备发放节点列表

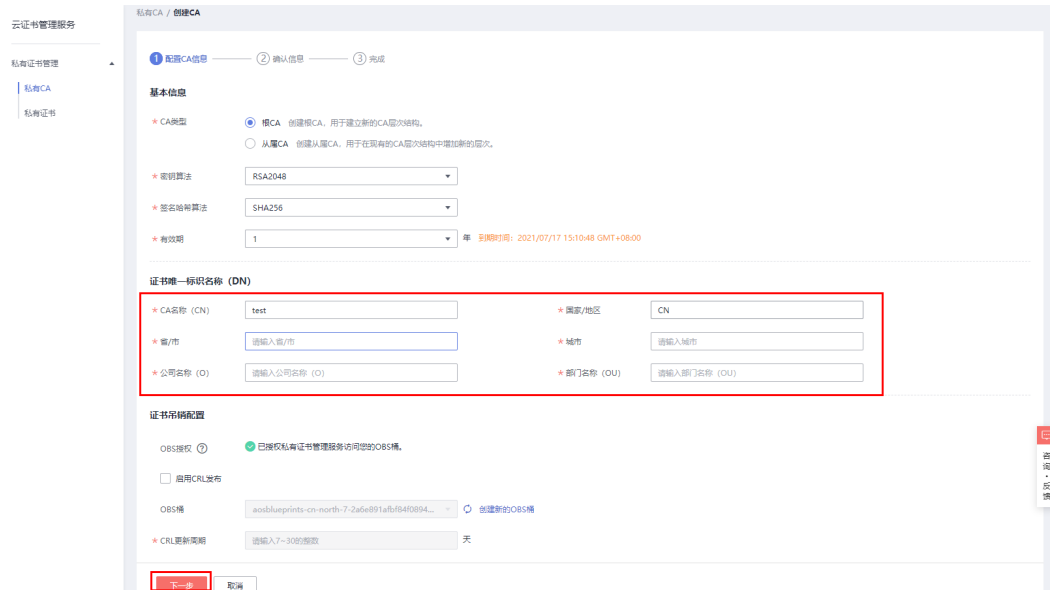
区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



在证书管理服务创建根 CA 证书

根据**云证书管理服务**的指导说明，在云证书管理服务控制台创建根CA证书。

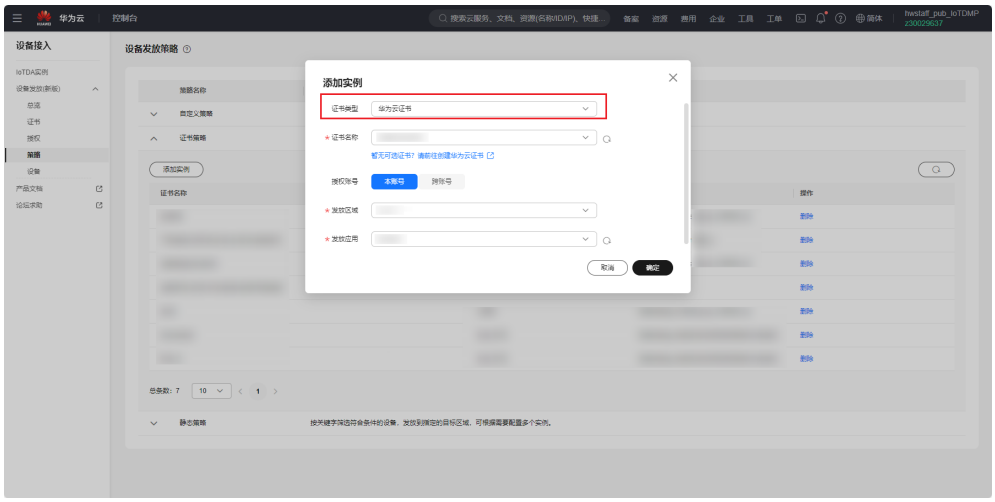


添加证书策略

采用华为云证书认证的设备，三种策略都支持引导，以“证书策略”为例，在“设备发放”创建对应“华为云证书”的证书策略。

图 4-20 添加证书策略

图 4-21 添加云证书策略详情



创建设备

在设备发放控制台，注册MQTT设备，其中安全模式选择X.509认证模式，证书类型选择云证书，填写设备证书名称，注册X.509认证设备。

图 4-22 注册设备

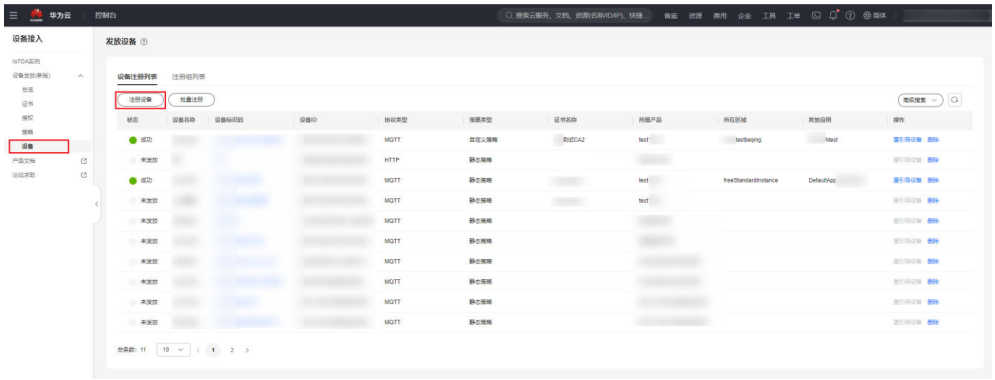
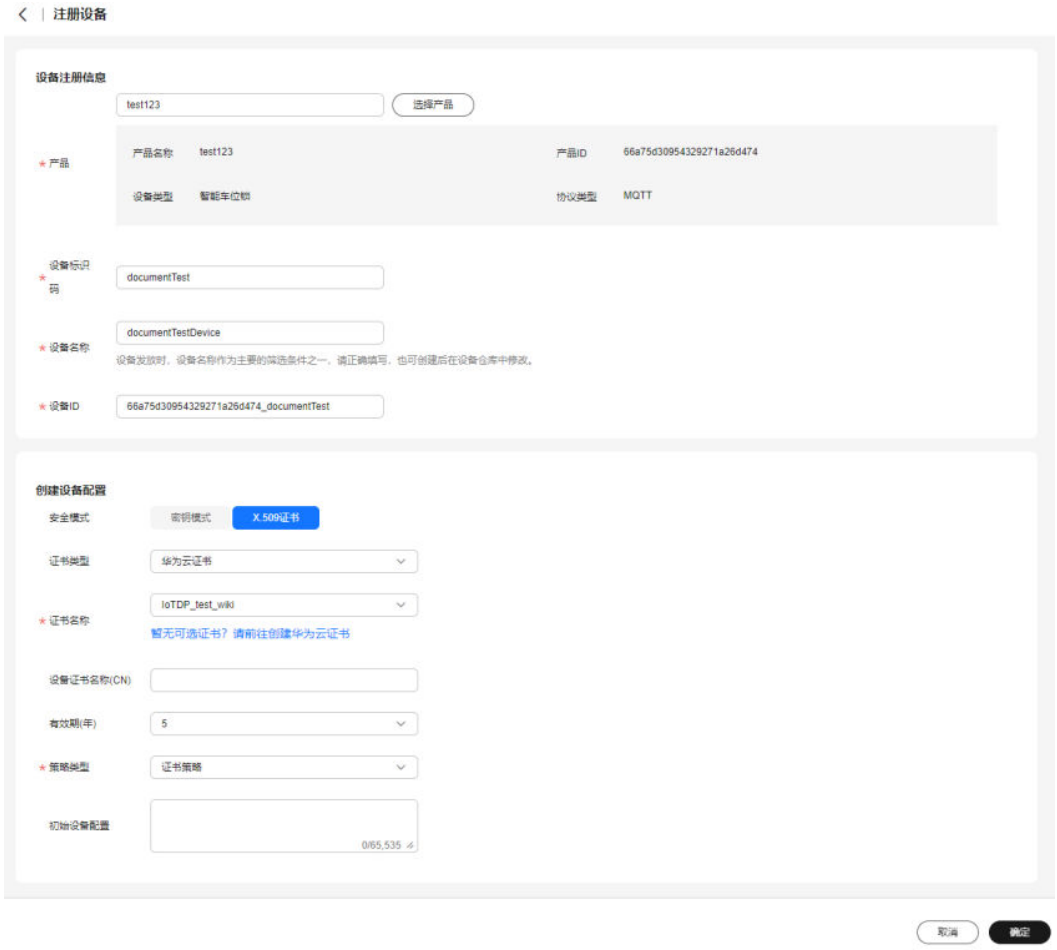


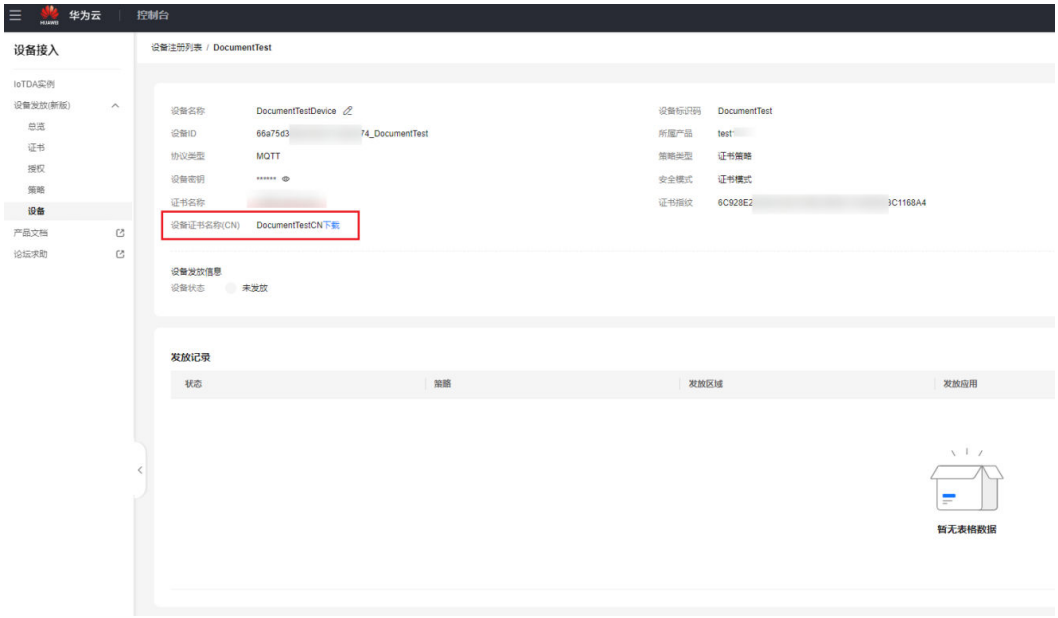
图 4-23 注册云证书设备



下载设备证书

设备注册成功后，单击设备进入设备详情页面，单击“下载”按钮下载设备证书，并烧录到设备。

图 4-24 下载云证书设备证书

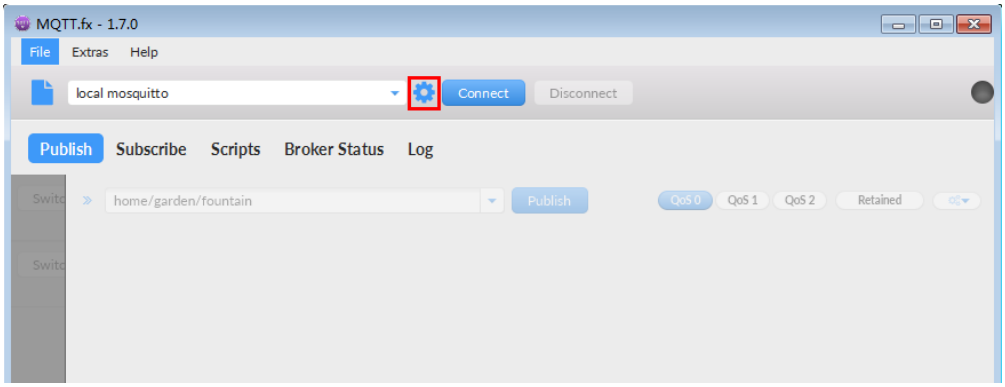


连接鉴权

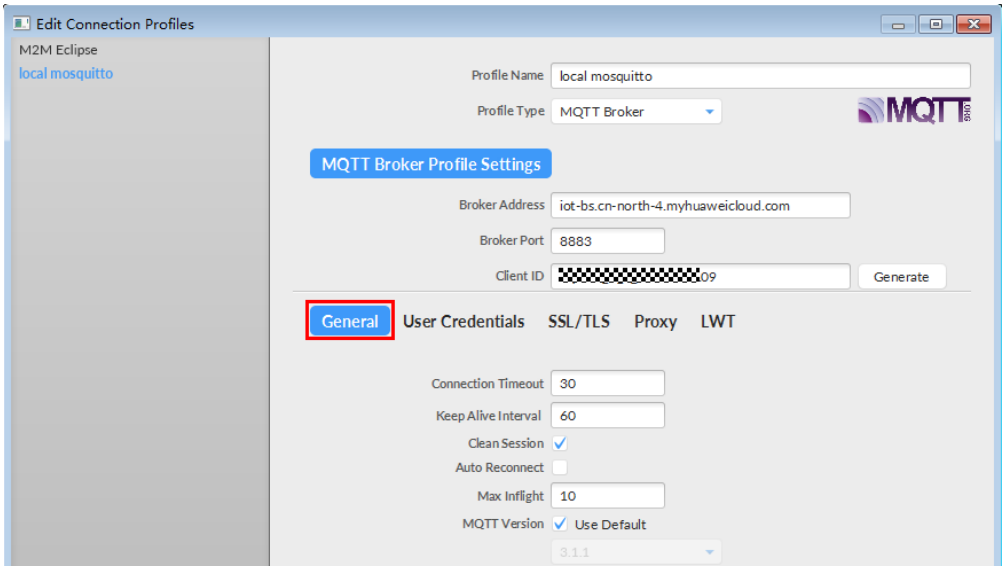
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

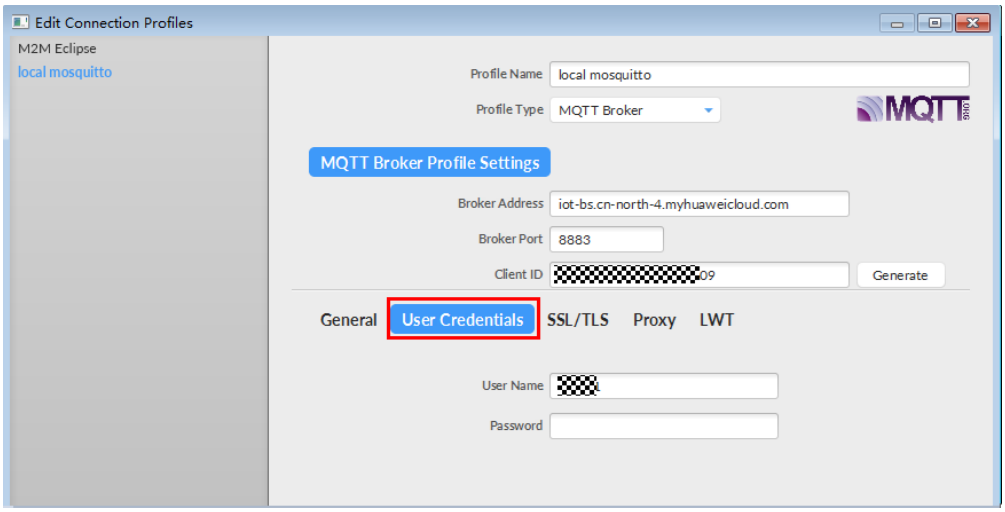
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



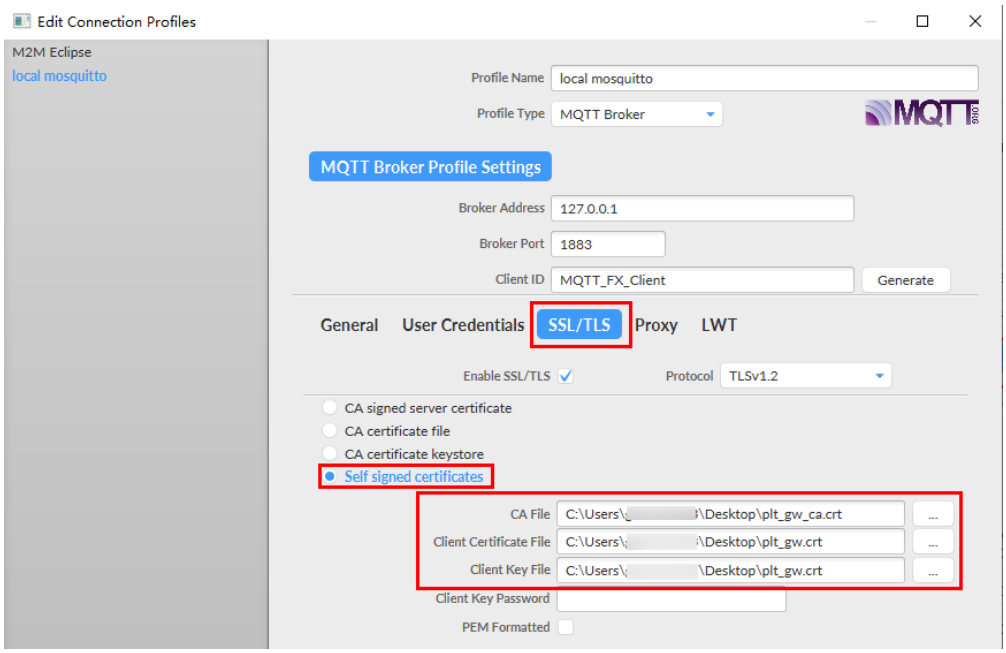
4. 填写 User Credentials 信息。



说明

其中Username 参考**MQTT CONNECT连接鉴权**参数说明（无需填写Password）。

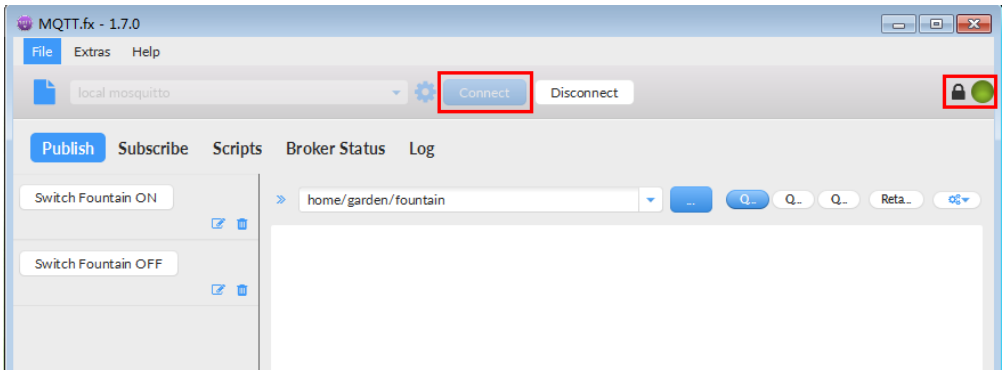
5. 选择开启 SSL/TLS，勾选Self signed certificates，配置相关证书内容。



说明

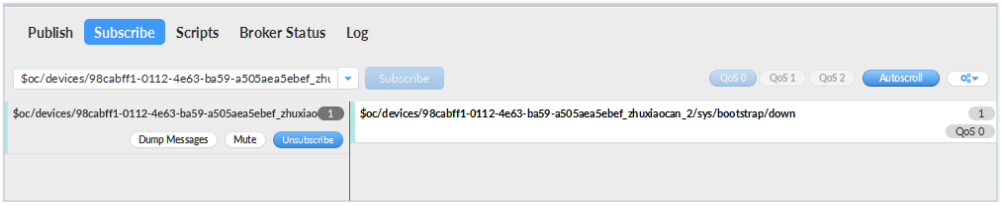
- CA File为设备发放对应的CA证书。
- Client Certificate File为设备的设备证书。
- Client Key File为设备的私钥。

6. 完成以上步骤后，单击“Apply”和“OK”进行保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



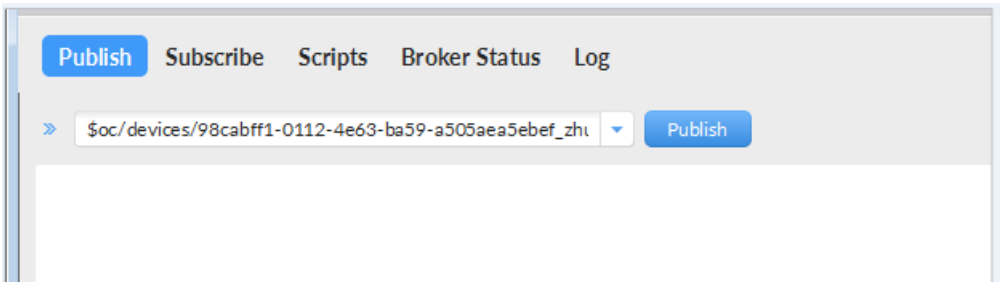
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



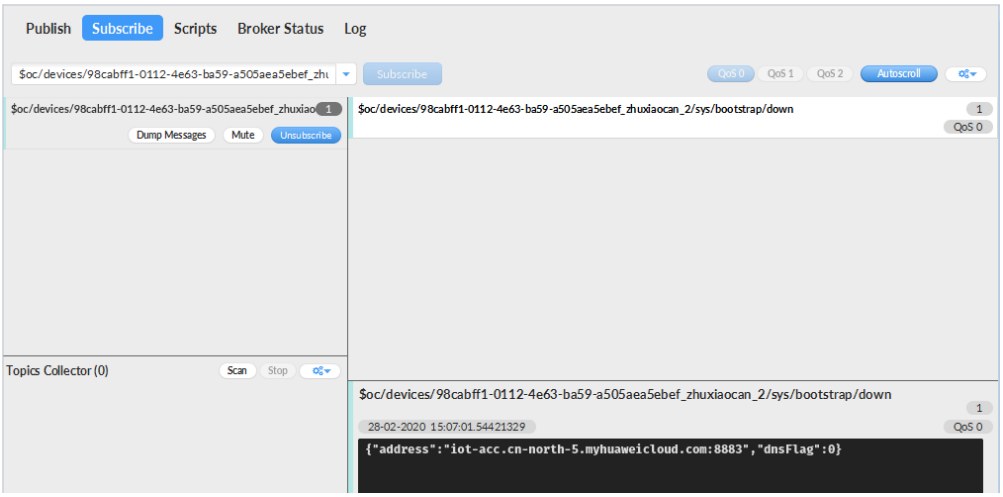
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

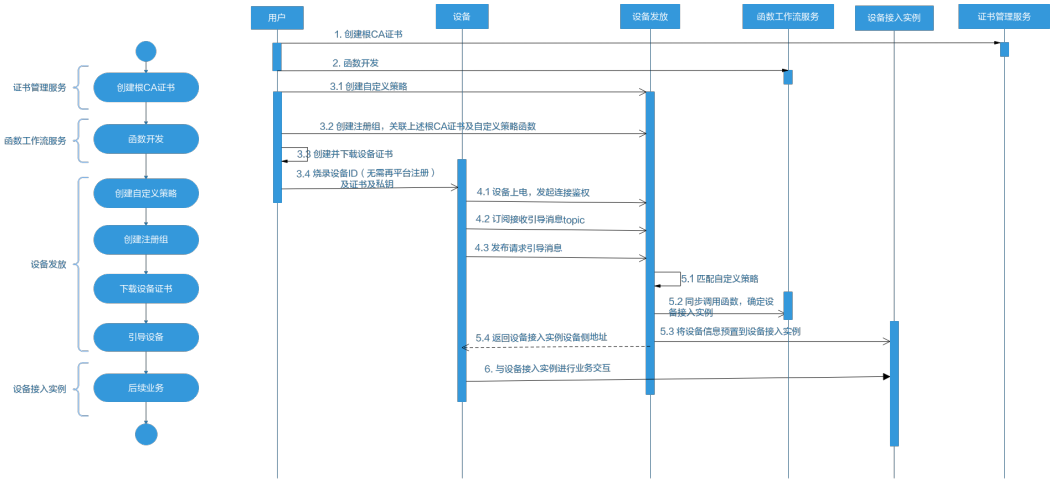
4.5 MQTT 华为云证书注册组发放示例

获取设备发放终端节点

表 4-9 设备发放节点列表

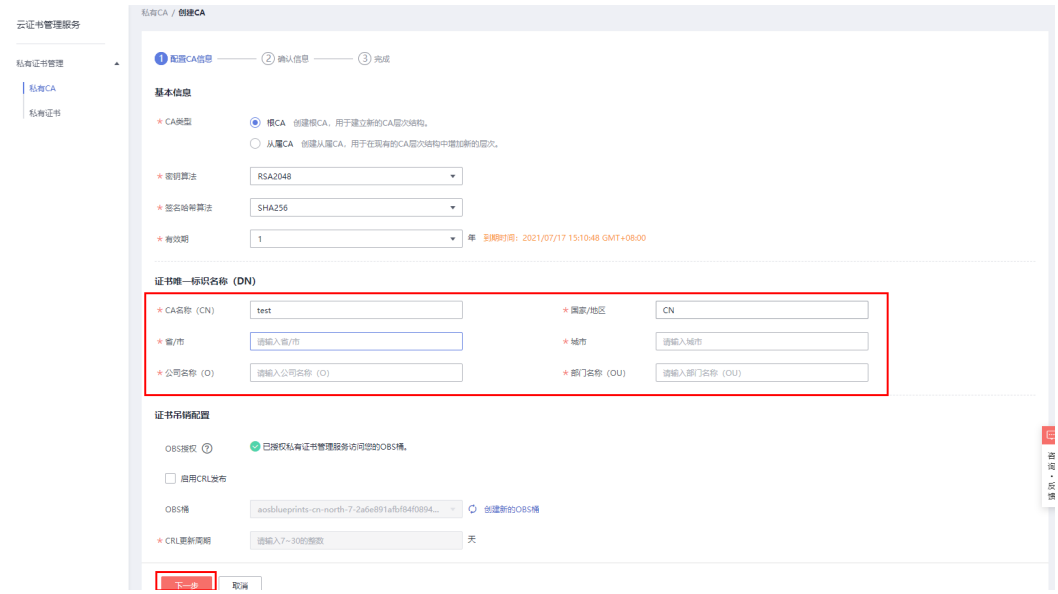
区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



在证书管理服务创建根 CA 证书

根据**云证书管理服务**的指导说明，在云证书管理服务控制台创建根CA证书。



添加自定义策略

图 4-25 添加自定义策略

新增注册组

图 4-26 新增注册组

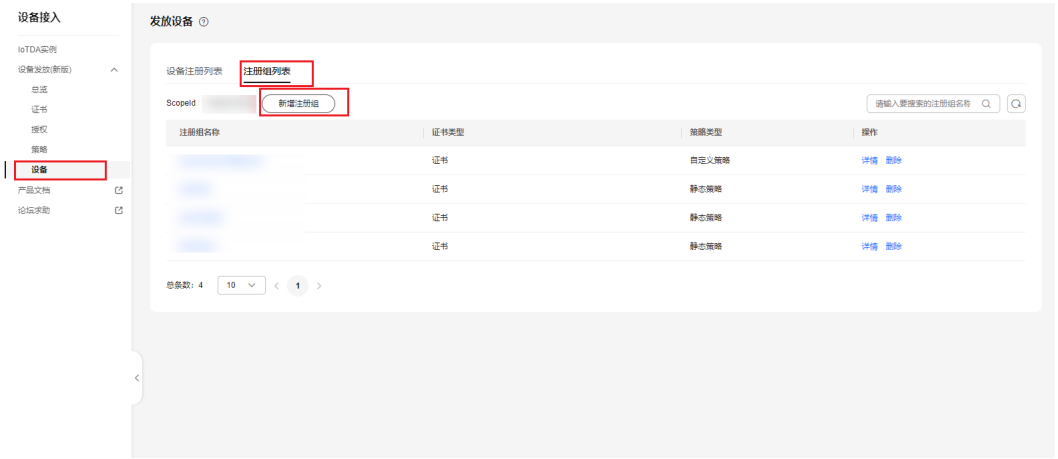


图 4-27 添加云证书自定义策略注册组

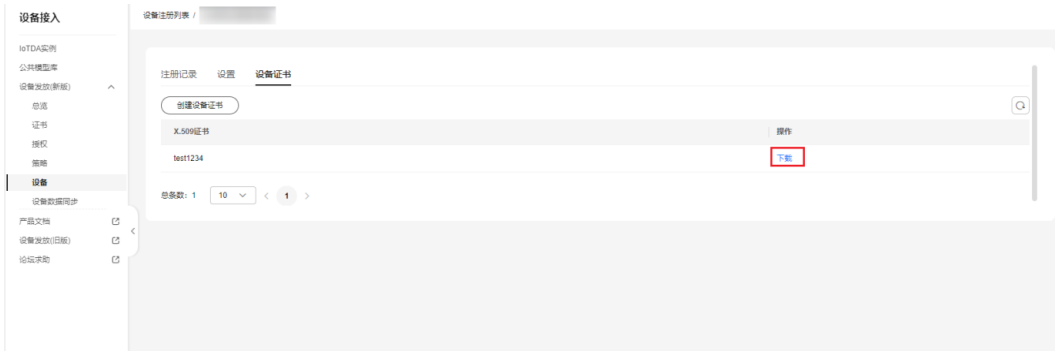
创建并下载设备证书

图 4-28 创建云证书注册组设备证书

图 4-29 创建云证书注册组设备证书详情

设备证书创建成功后，单击“下载”设备证书和私钥，并烧录到设备。

图 4-30 下载云证书注册组设备证书

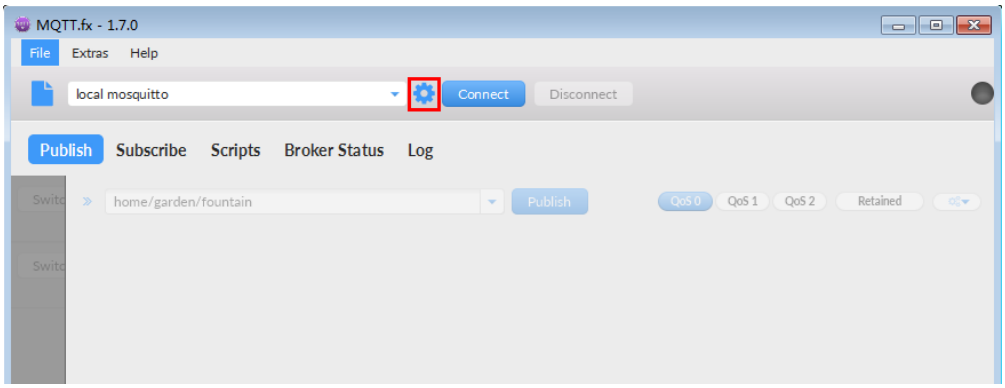


连接鉴权

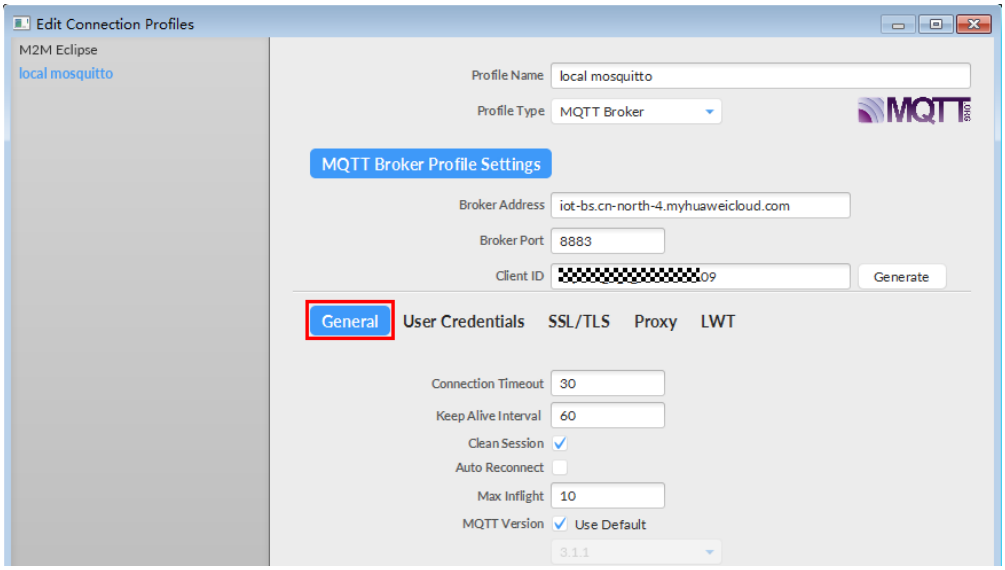
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

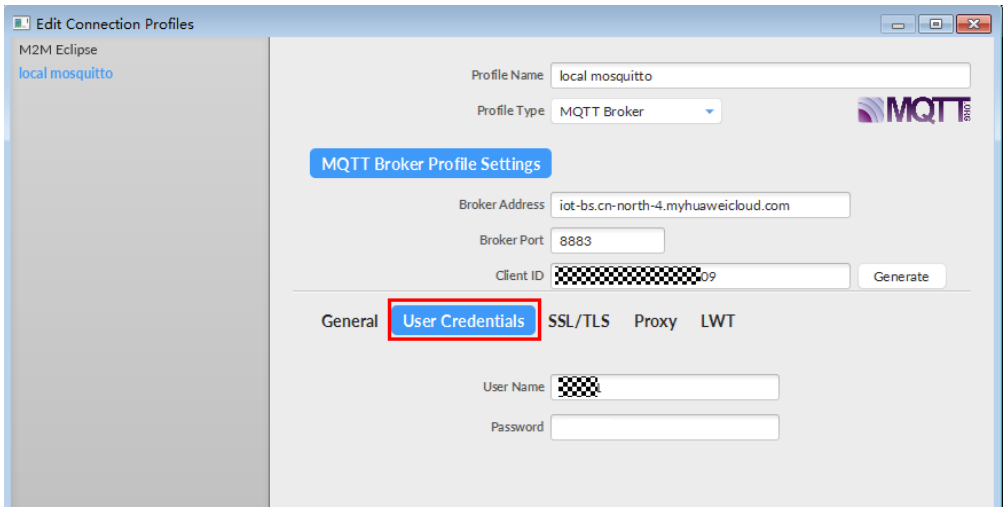
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



4. 填写 User Credentials 信息。

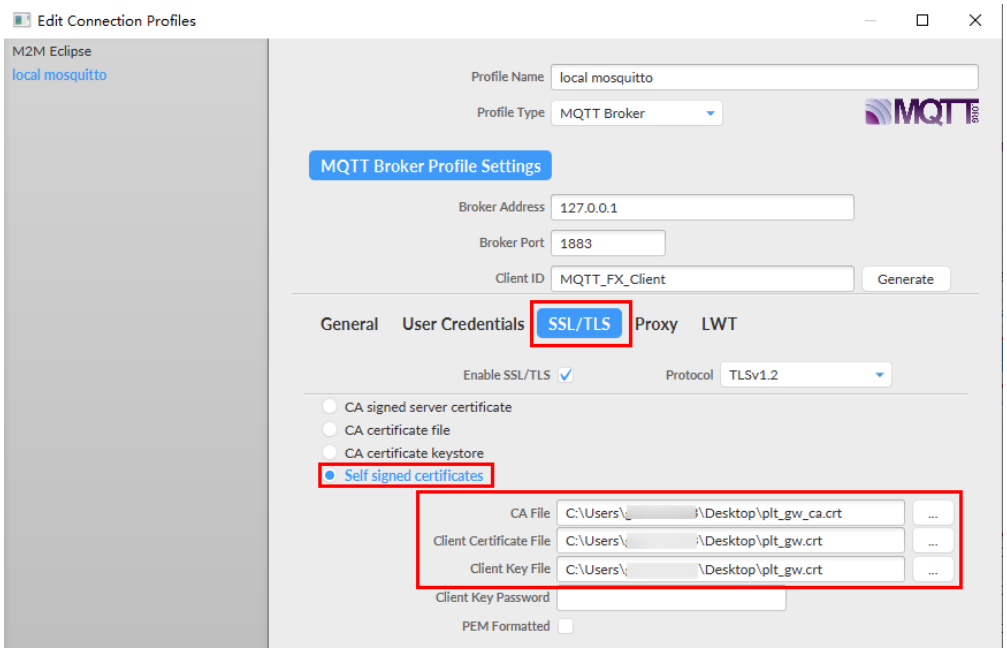


说明

其中Username 参考**MQTT CONNECT连接鉴权**参数说明（无需填写Password）。

注：注册组的场景不存在选择产品，所以命名需要注意：如果命名字符串有“_”，那么第一项必须为对应设备接入已经存在的产品ID，如果不包括“_”，那么可以随意命名。

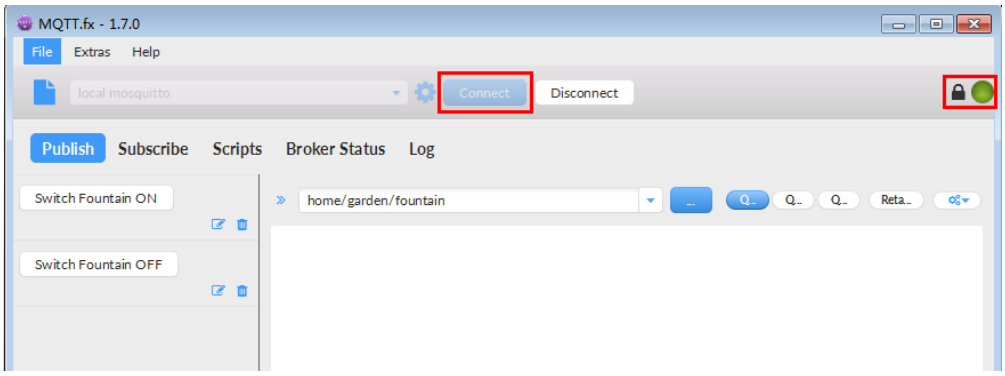
5. 选择开启 SSL/TLS，勾选Self signed certificates，配置相关证书内容。



说明

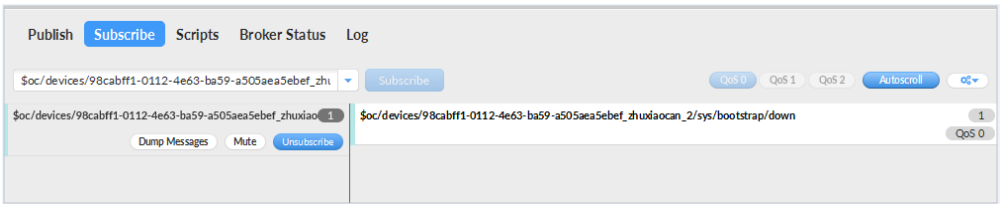
- CA File为设备发放对应的CA证书。
- Client Certificate File为设备的设备证书。
- Client Key File为设备的私钥。

6. 完成以上步骤后，单击“Apply”和“OK”进行保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



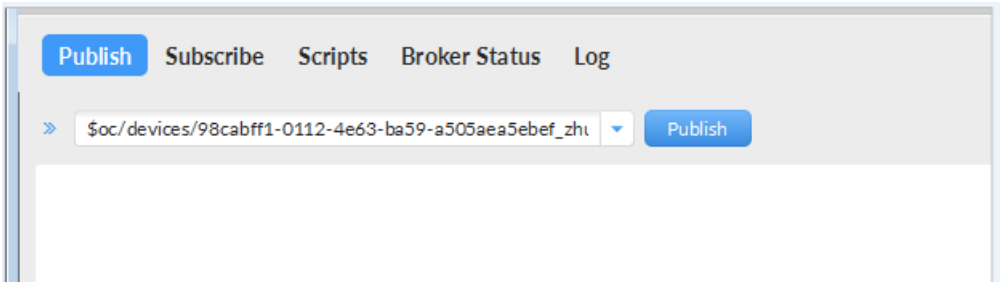
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



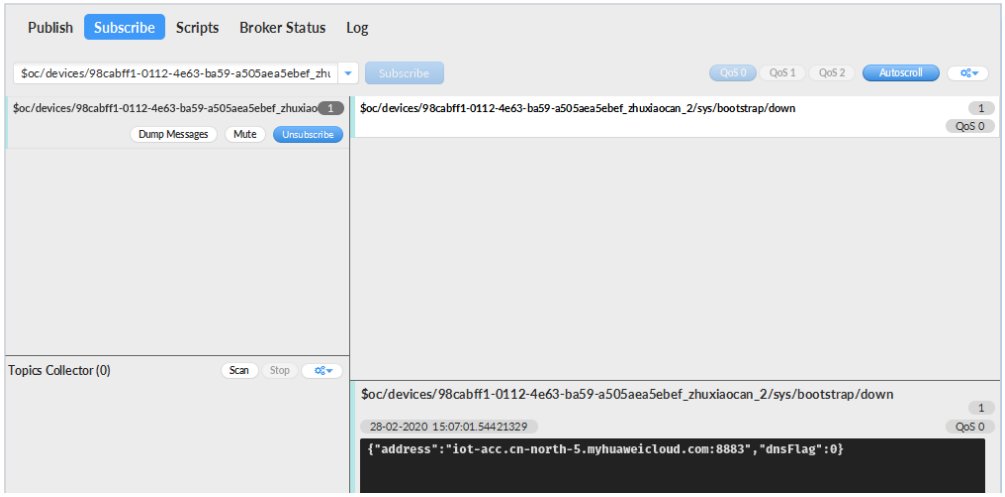
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

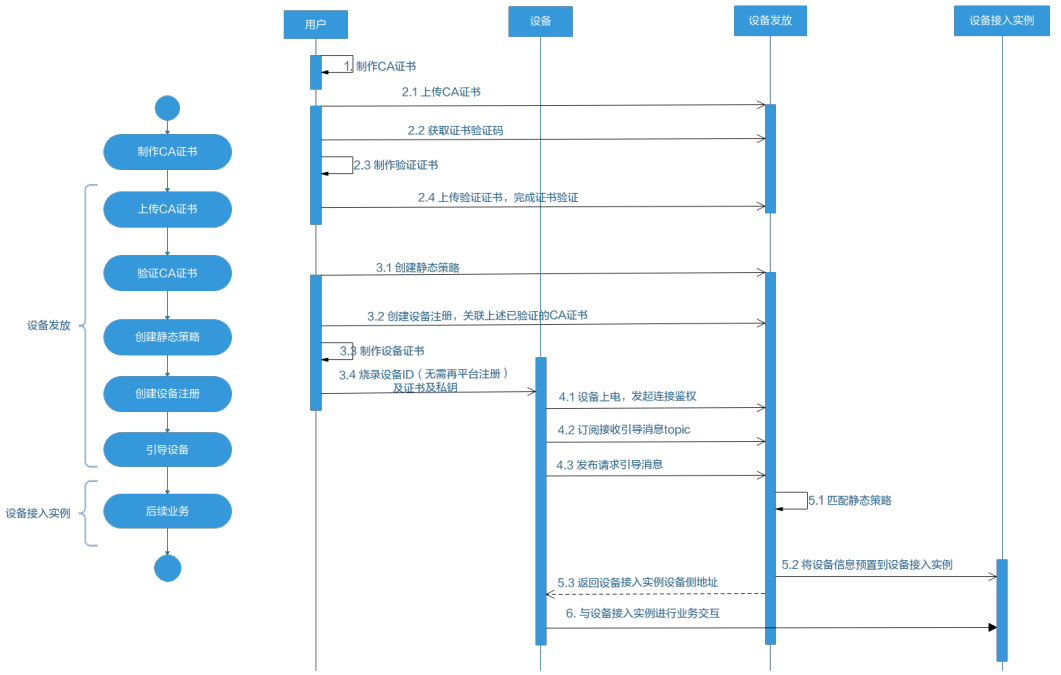
4.6 MQTT 注册组静态策略发放示例

获取设备发放终端节点

表 4-10 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

整体流程



制作 CA 证书

步骤1 在浏览器中访问**这里**，下载并进行安装OpenSSL工具，安装完成后配置环境变量。

步骤2 在 D:\certificates 文件夹下，以管理员身份运行cmd命令行窗口。

步骤3 生成密钥对（ rootCA.key ）：

说明

生成“密钥对”时输入的密码在生成“证书签名请求文件”、“CA证书”，“验证证书”以及“设备证书”时需要用到，请妥善保存。

```
openssl genrsa -des3 -out rootCA.key 2048
```

步骤4 使用密钥对生成证书签名请求文件：

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（ Distinguished Name，DN ）信息，参数说明如下**表1** 所示。

表 4-11 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen

提示	参数名称	取值样例
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

```
openssl req -new -key rootCA.key -out rootCA.csr
```

步骤5 生成CA证书（rootCA.crt）：

```
openssl x509 -req -days 50000 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
```

说明

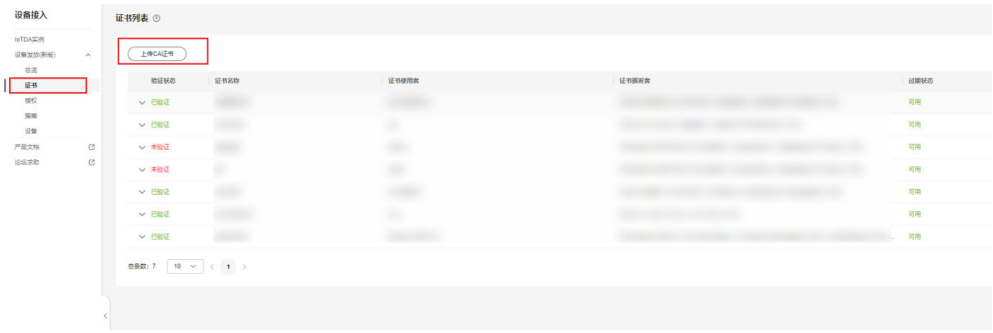
“-days”后的参数值指定了该证书的有效天数，此处示例为50000天，您可根据实际业务场景和需要进行调整。

----结束

上传并验证 CA 证书

步骤1 登录设备发放控制台，进入“证书”界面，单击右上角“上传CA证书”，填写“证书名称”并上传上述“制作CA证书”步骤后生成的“CA证书（rootCA.crt文件）”，单击“确定”。

图 4-31 上传 CA 证书

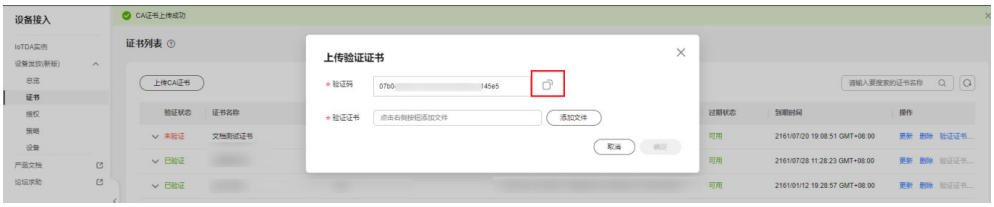


步骤2 验证步骤1中上传的CA证书，只有成功验证证书后该证书方可使用。

1. 为验证证书生成密钥对。
   ```
   openssl genrsa -out verificationCert.key 2048
   ```
2. 获取随机验证码。

图 4-32 上传 CA 证书完成页

图 4-33 复制验证码



3. 利用此验证码生成证书签名请求文件CSR。

```
openssl req -new -key verificationCert.key -out verificationCert.csr
```

说明

CSR文件的Common Name (e.g. server FQDN or YOUR name) 需要填写前一过程中获取到的随机验证码。

4. 使用CA证书、CA证书私钥和CSR文件创建验证证书（verificationCert.crt）。

```
openssl x509 -req -in verificationCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out verificationCert.crt -days 500 -sha256
```

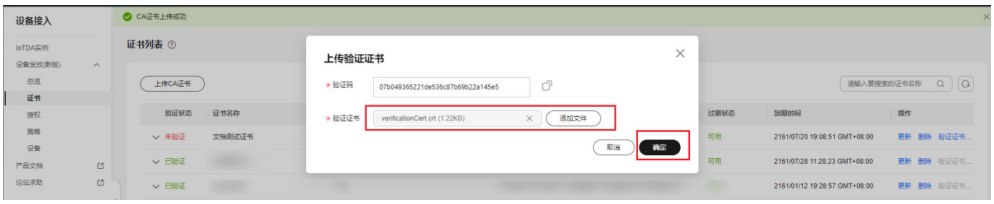
说明

生成验证证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件。

“-days”后的参数值指定了该证书的有效天数，此处示例为500天，您可根据实际业务场景和需要进行调整。

5. 上传验证证书进行验证。

图 4-34 上传验证证书



----结束

生成设备证书

步骤1 使用OpenSSL工具为设备证书生成密钥对（设备私钥）：

```
openssl genrsa -out deviceCert.key 2048
```

步骤2 使用设备密钥对，生成证书签名请求文件：

```
openssl req -new -key deviceCert.key -out deviceCert.csr
```


说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下表2所示。

表 4-12 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

步骤3 使用CA证书、CA证书私钥和CSR文件创建设备证书（deviceCert.crt）。

```
openssl x509 -req -in deviceCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out deviceCert.crt -days 36500 -sha256
```

说明

生成设备证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件，且需要完成“上传并验证CA证书”。

“-days”后的参数值指定了该证书的有效天数，此处示例为36500天，您可根据实际业务场景和需要进行调整。

----结束

添加静态策略

“关键字”为注册组名称中的关键字。设备发放时，注册组下的设备的设备名称为“注册组名称+设备ID”，如果包含设置的关键字，则可按该实例进行发放。

图 4-35 创建静态策略

新增注册组

创建注册组（如果需要下发初始化配置，那么对应在初始设备配置选项中填写对应的JSON字符串，设备发放不理解该字段，只是透传该JSON字符串，由设备理解解析。如果不需要下发该字段则不填）。

图 4-36 新增注册组

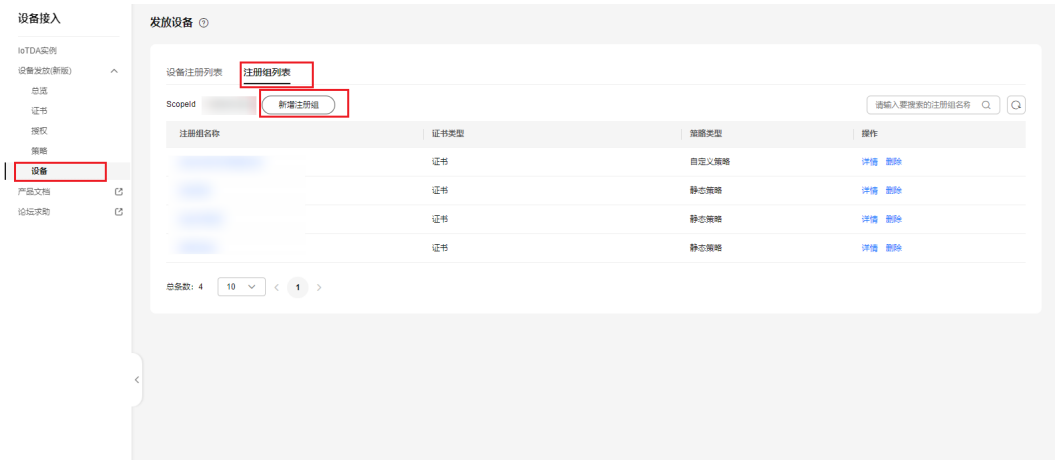
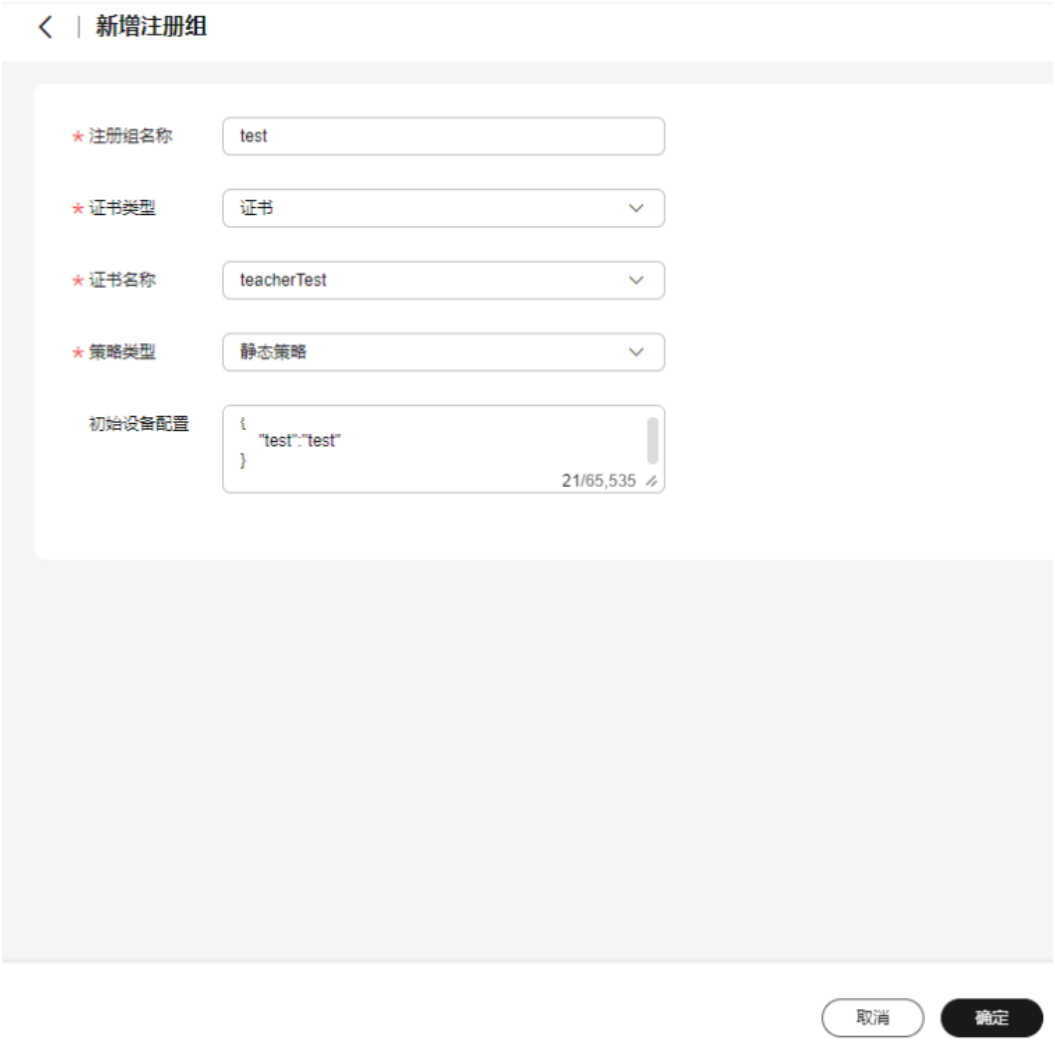


图 4-37 创建证书静态注册组

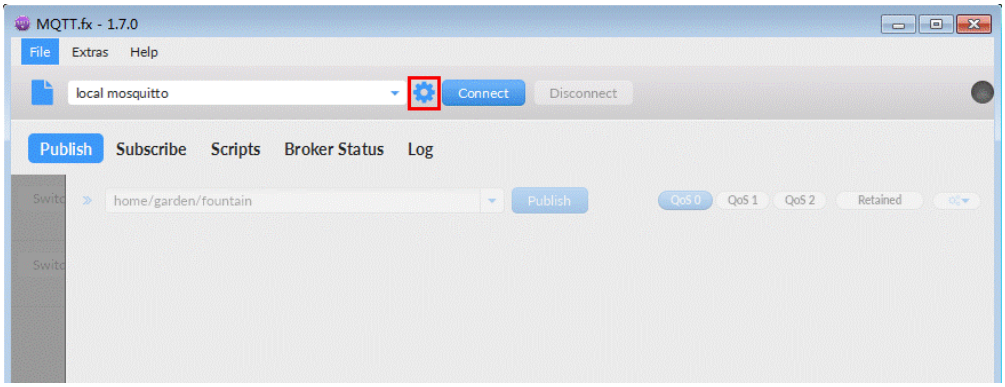


连接鉴权

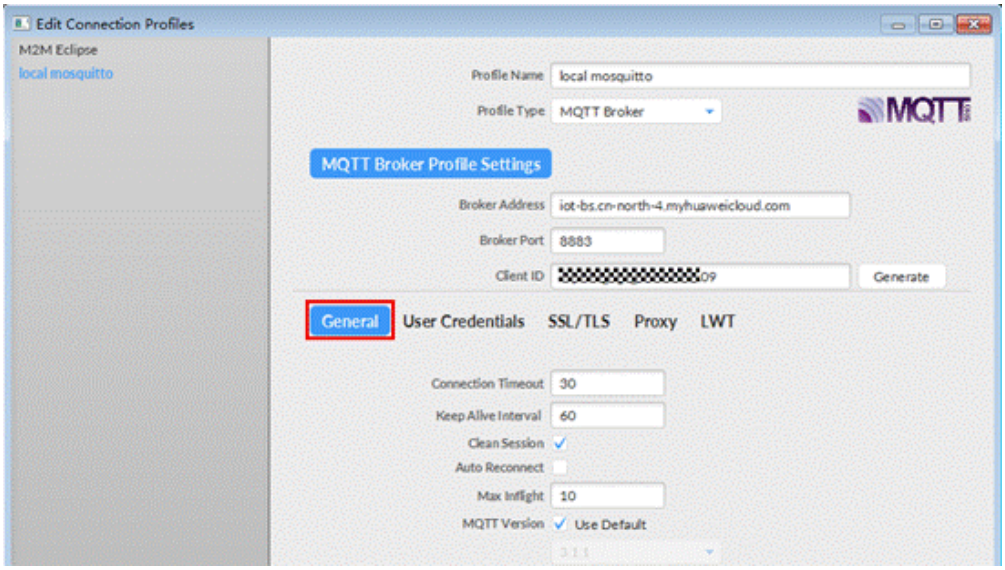
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

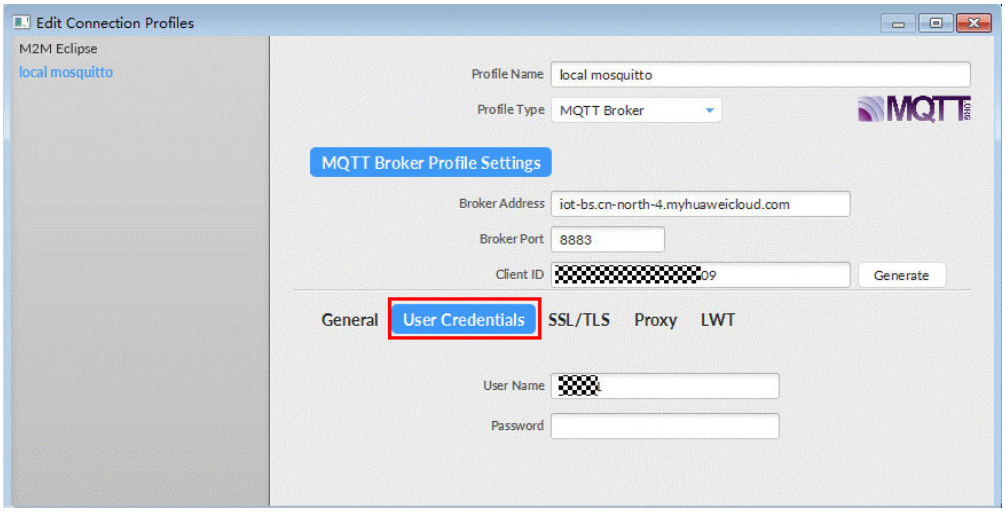
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



4. 填写 User Credentials 信息。

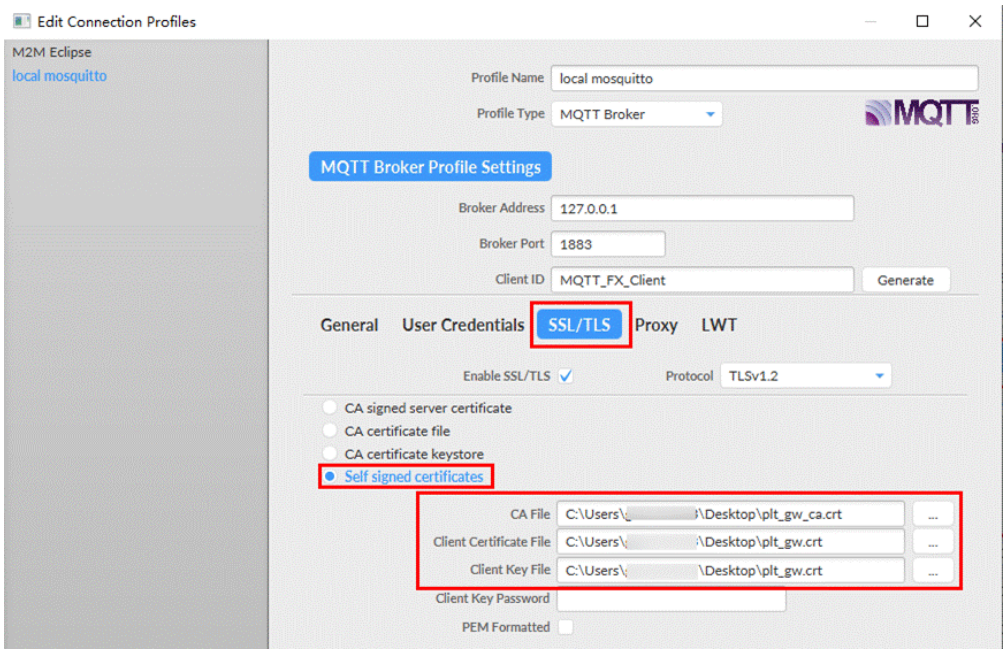


说明

其中Username 参考**MQTT CONNECT连接鉴权**参数说明（无需填写Password）。

注：注册组的场景不存在选择产品，所以命名需要注意：如果命名字符串有“_”，那么第一项必须为对应设备接入已经存在的产品ID，如果不包括“_”，那么可以随意命名。

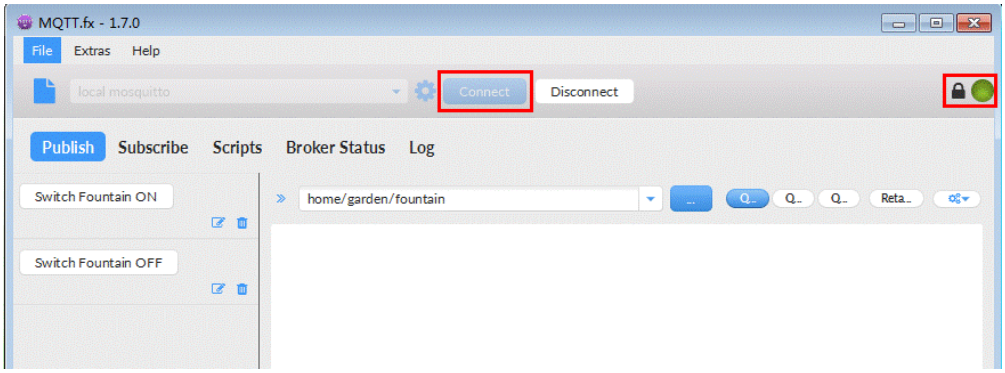
5. 选择开启 SSL/TLS，勾选Self signed certificates，配置相关证书内容。



说明

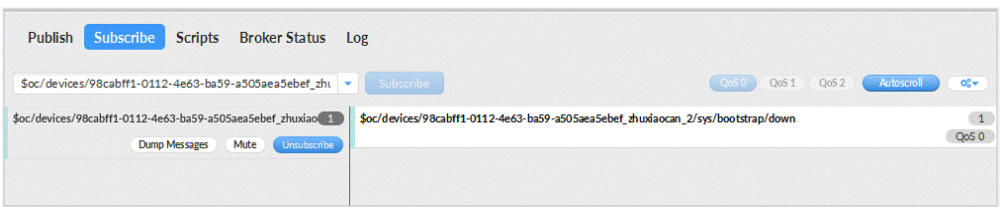
- CA File为设备发放对应的CA证书。
- Client Certificate File为设备的设备证书。
- Client Key File为设备的私钥。

6. 完成以上步骤后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



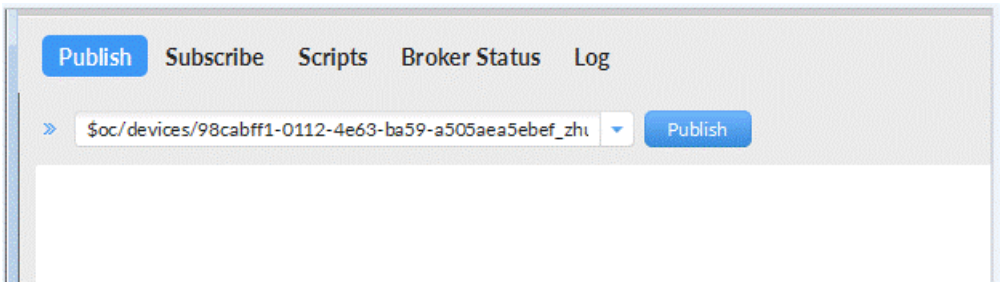
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



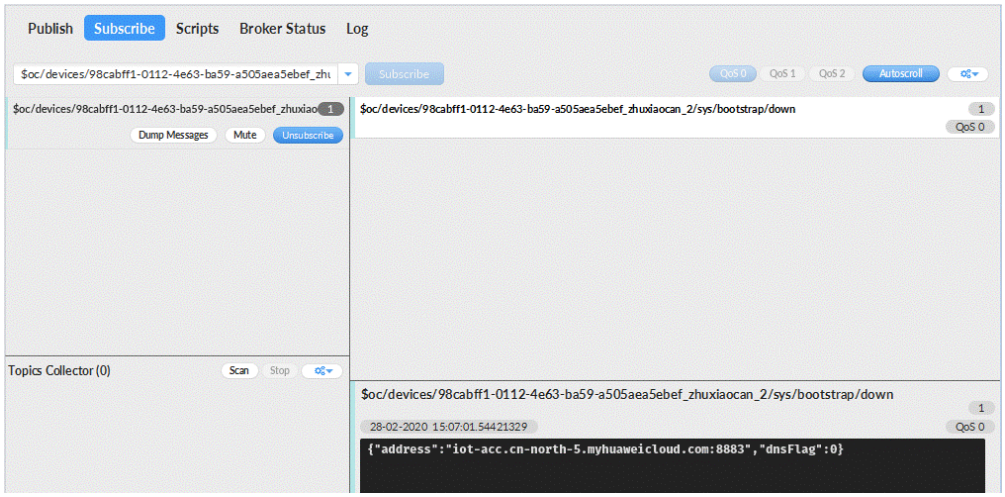
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

4.7 MQTT 注册组密钥认证静态策略发放示例

获取设备发放终端节点

表 4-13 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

场景说明

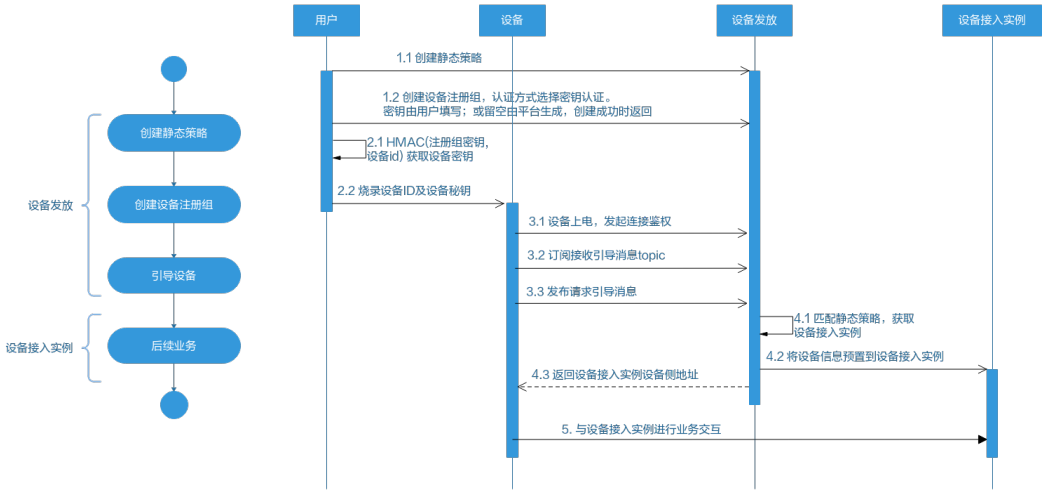
有些设备可能没有证书，又需要使用设备发放功能。对于此类设备，设备发放提供密钥注册组功能。

说明

密钥认证类型的设备组是一个安全性不完备的方案，建议使用证书作为注册组的认证方式。

每个设备的设备代码应该只包含该设备的相应派生设备密钥。 不要在设备代码中包含你的注册组密钥。 泄露的注册组密钥可能会危及所有使用该密钥进行身份验证的设备的安全。

整体流程



添加静态策略

“关键字”为“设备名称”中的关键字。设备发放时，“设备名称”为“注册组名称”+“设备ID”。

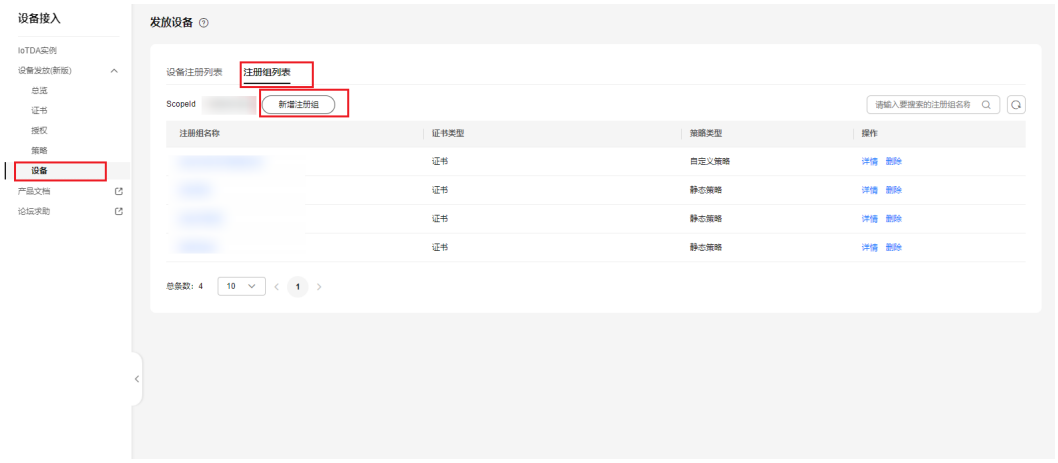
使用静态策略的注册组中，若注册“设备名称”中包含“关键字”，则按照“关键字”对应策略指定的区域与应用实例进行发放。

图 4-38 创建静态策略

新增注册组

创建注册组。

图 4-39 新增注册组

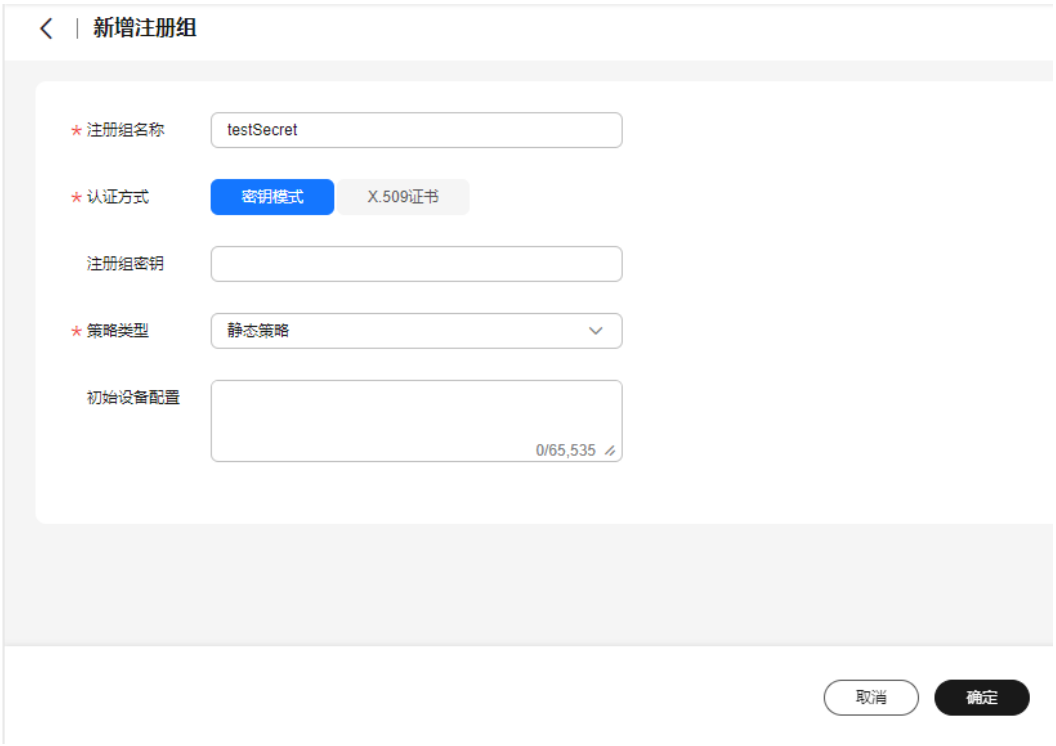


注册组密钥为长度在”32~128“字节的字节码。在创建密钥注册组时，返回的注册组密钥为“base64编码后的注册组密钥字符串”。

若不指定注册组密钥，则注册组密钥由设备发放服务生成。

若指定注册组密钥，在创建中注册组时需在密钥输入框内填写“指定字节码Base64编码后生成的字符串”。

图 4-40 创建密钥注册组



说明

如果需要下发初始化配置，那么对应在初始设备配置选项中填写对应的JSON字符串，设备发放不理解该字段，只是透传该JSON字符串，由设备理解解析。如果不需要下发该字段则不填

创建完成后会返回注册组密钥，单击复制保存注册组密钥。

图 4-41 创建密钥注册组响应

说明

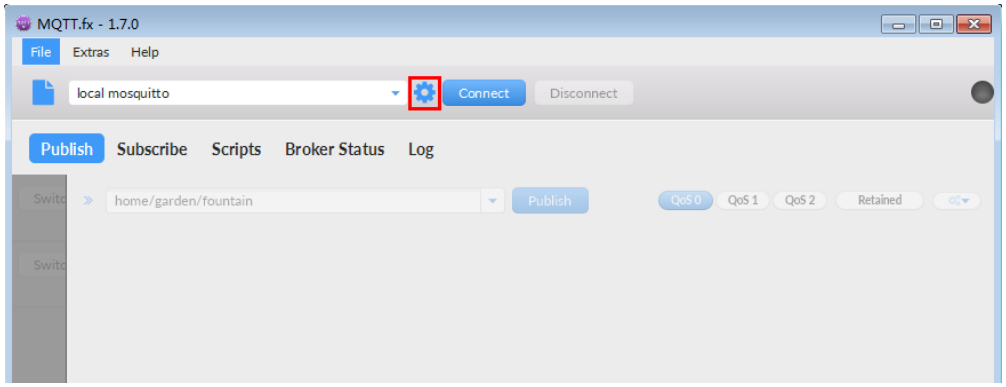
此处注册设备的设备名称需与**添加静态策略**步骤的策略实例关键字相匹配，方能触发该静态策略。

连接鉴权

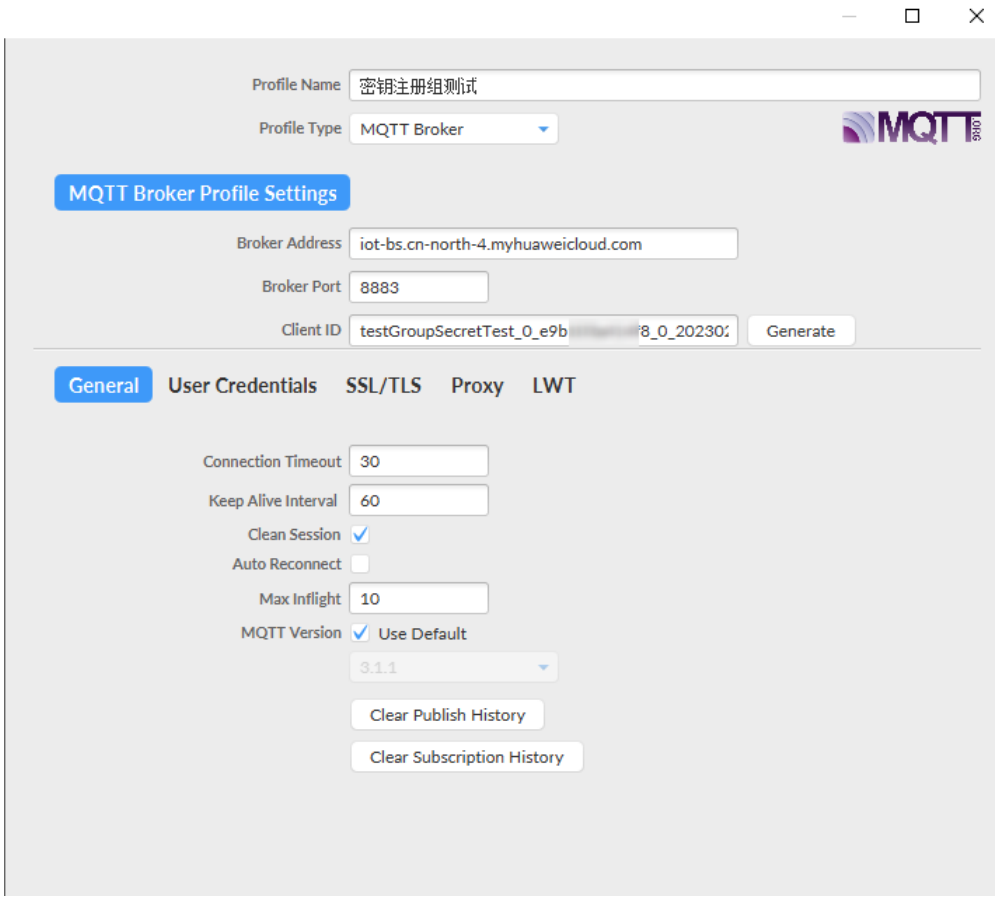
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。

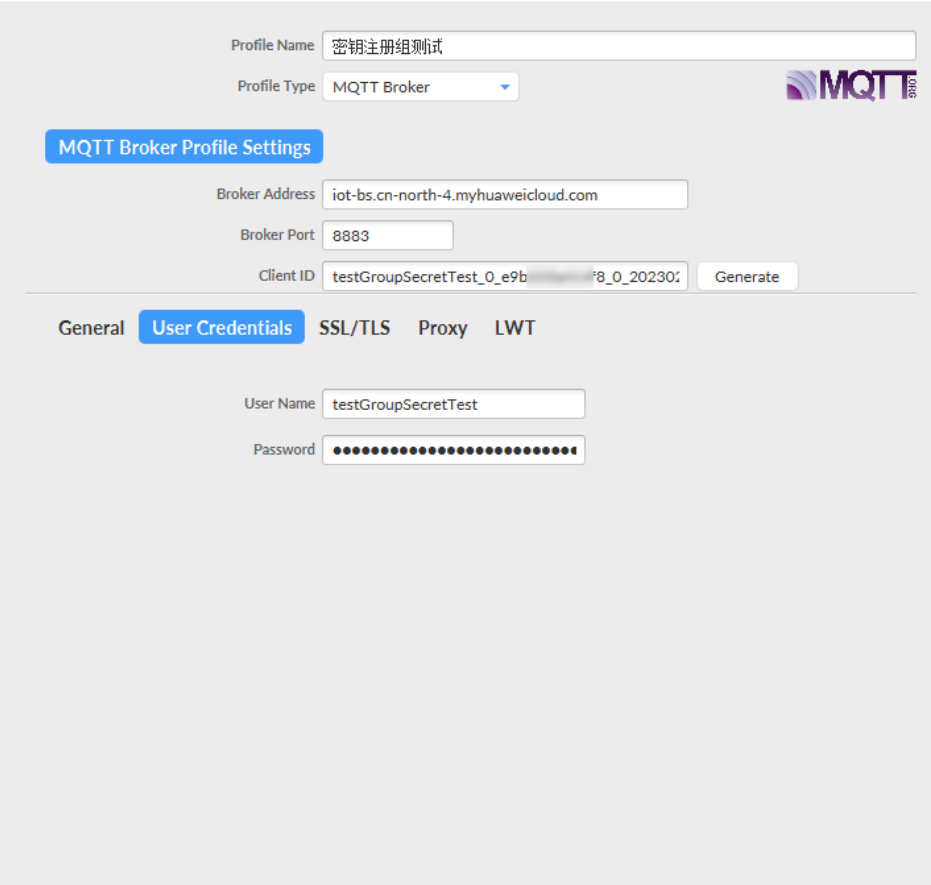


3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



4. 填写 User Credentials 信息。

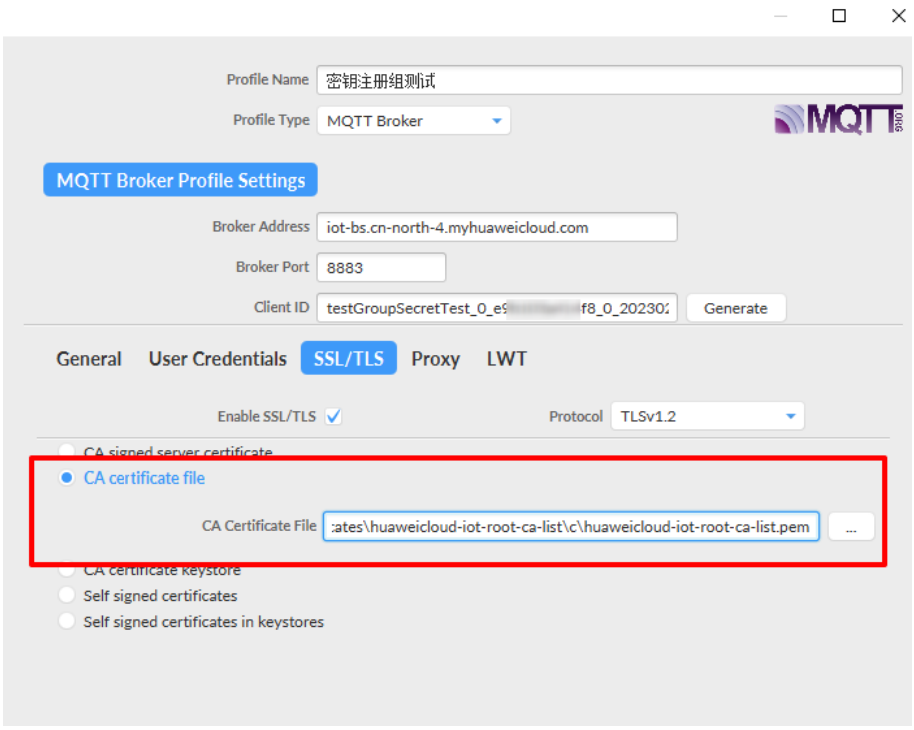
   对于设备而言，设备secret的值为使用“HMACSHA256”算法以“设备ID”为密钥，对“注册组密钥”进行加密后的值。



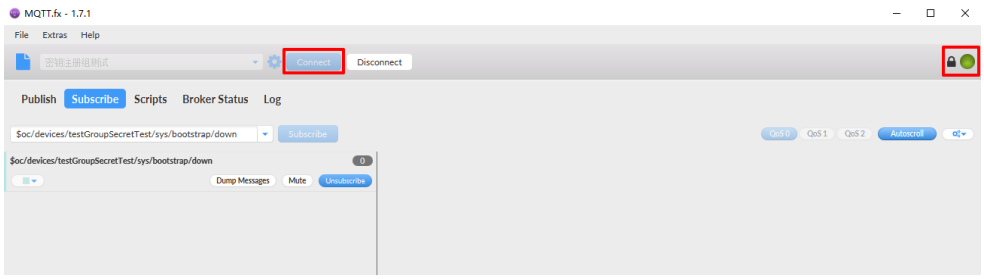
说明

其中Username 和Password 参数参考**MQTT CONNECT连接鉴权**参数说明。

5. 选择开启 SSL/TLS，勾选CA Certificate file，CA Certificate File指定为物联网平台根证书（请先下载**物联网平台的根证书**，解压后，选择其中c或java目录下PEM后缀的文件）的本地路径。

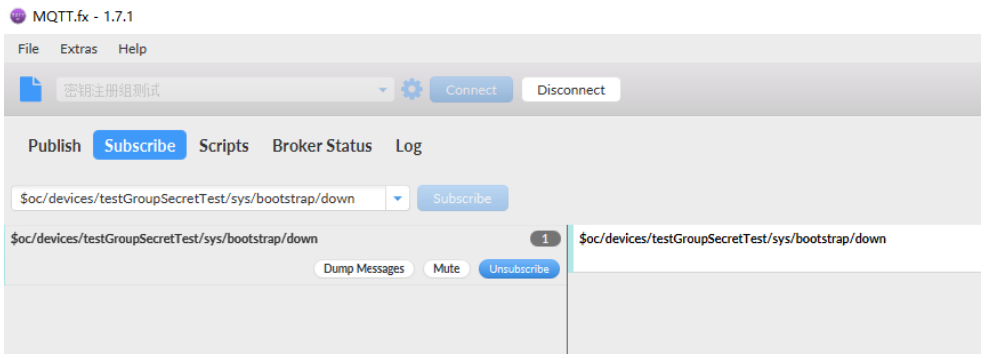


6. 完成以上步骤后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



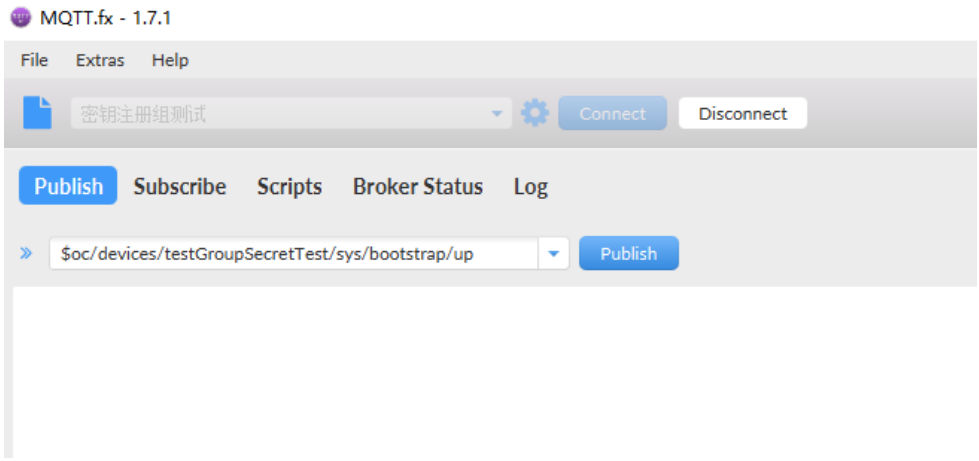
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



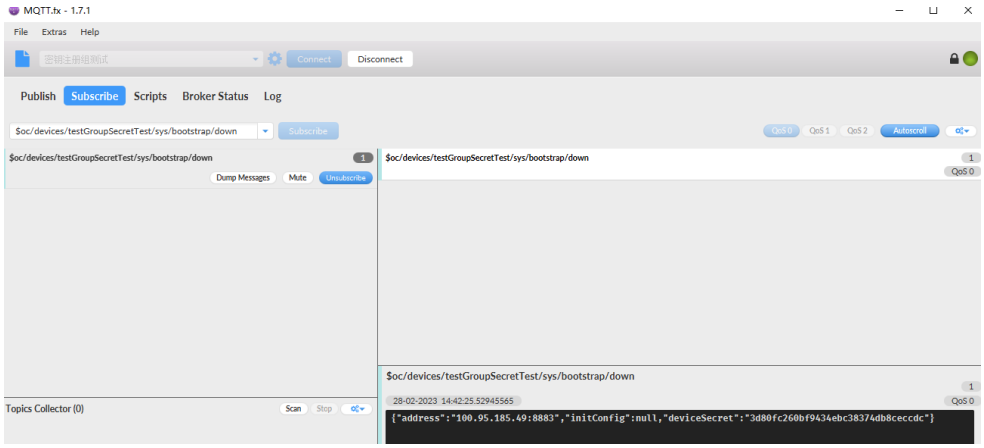
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址以及该设备的设备接入密钥。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址，设备接入密钥；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

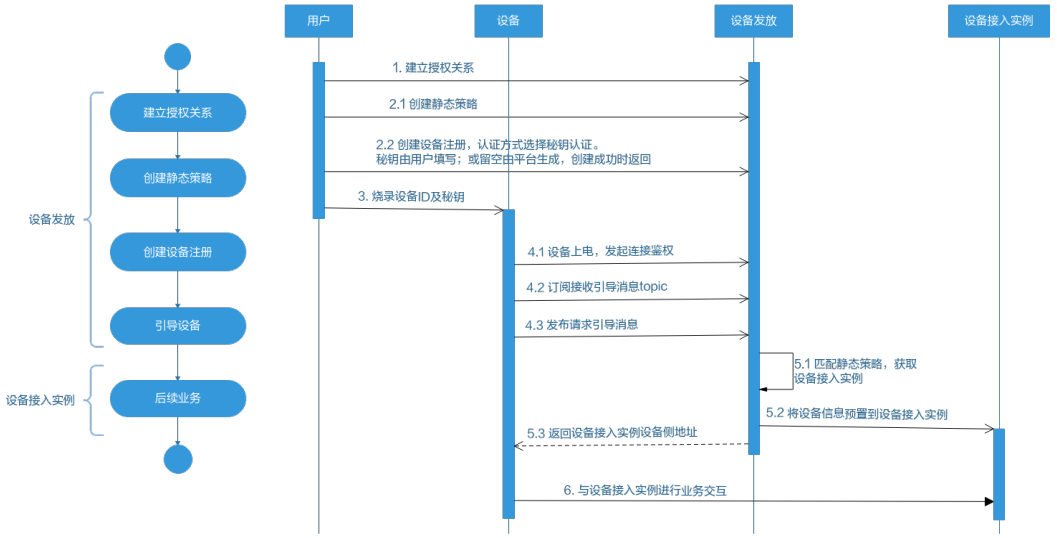
4.8 MQTT 密钥设备跨账号使用静态策略发放示例

获取设备发放终端节点

表 4-14 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

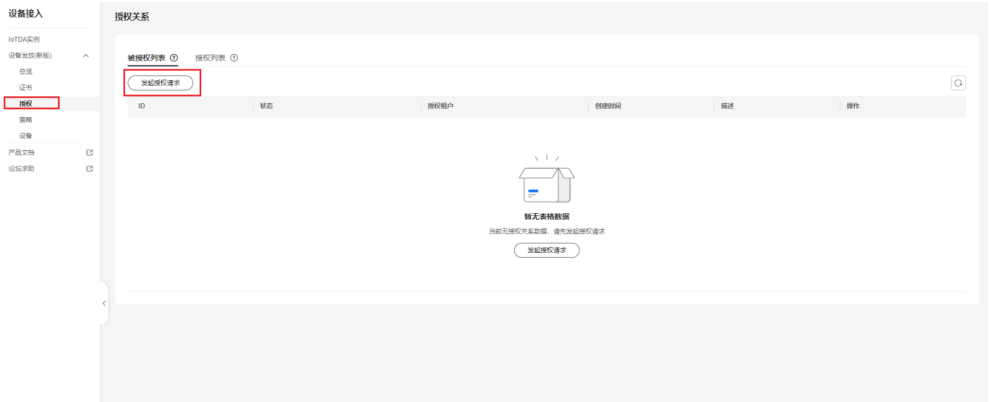
整体流程



被授权方发起授权请求

进入授权关系界面，发起授权请求。

图 4-42 发起授权请求

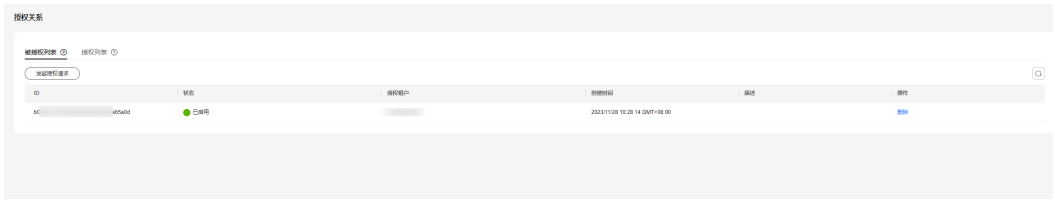


填写发起授权请求相关信息，单击“确定”。

图 4-43 发起授权请求详情

可以在被授权列表看到刚刚授权给本账号的用户账号信息。

图 4-44 被授权列表



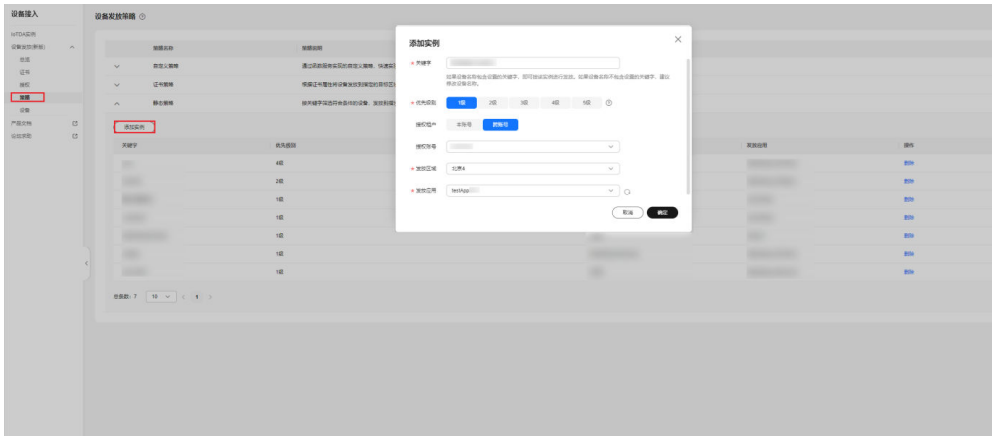
添加静态策略

添加静态策略，根据关键字发放到指定的IoTDA。

图 4-45 创建静态策略

发放方式选择“跨账号”，授权账号选择步骤3中授权给本账号的用户账号。

图 4-46 添加静态跨 region 策略



注册设备

在设备发放控制台，注册MQTT设备，其中安全模式选择密钥模式（如果需要下发初始化配置，那么对应在初始设备配置选项中填写对应的JSON字符串，设备发放不理解该字段，只是透传该JSON字符串，由设备理解解析。如果不需要下发该字段则不填）。

图 4-47 注册设备

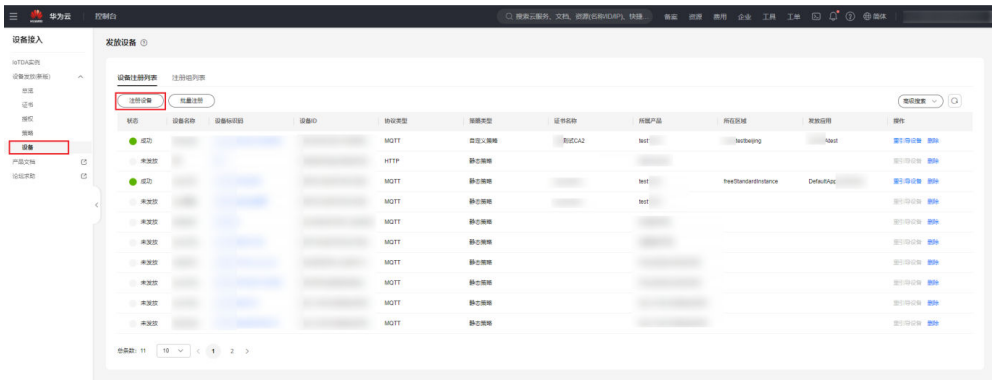
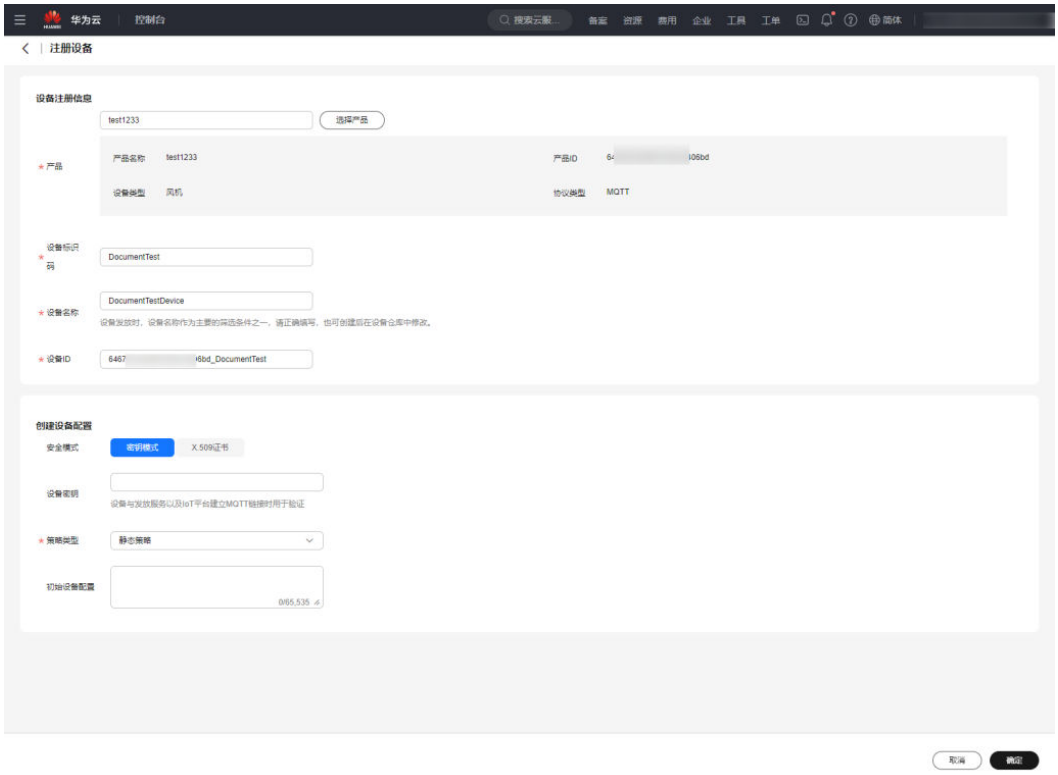


图 4-48 创建密钥模式静态策略设备



说明

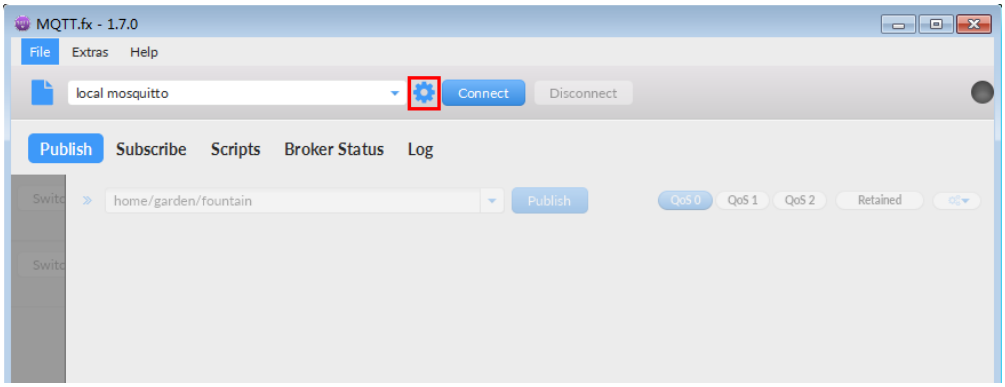
此处注册设备的设备名称需与**添加静态策略**步骤的策略实例关键字相匹配，方能触发该静态策略。

连接鉴权

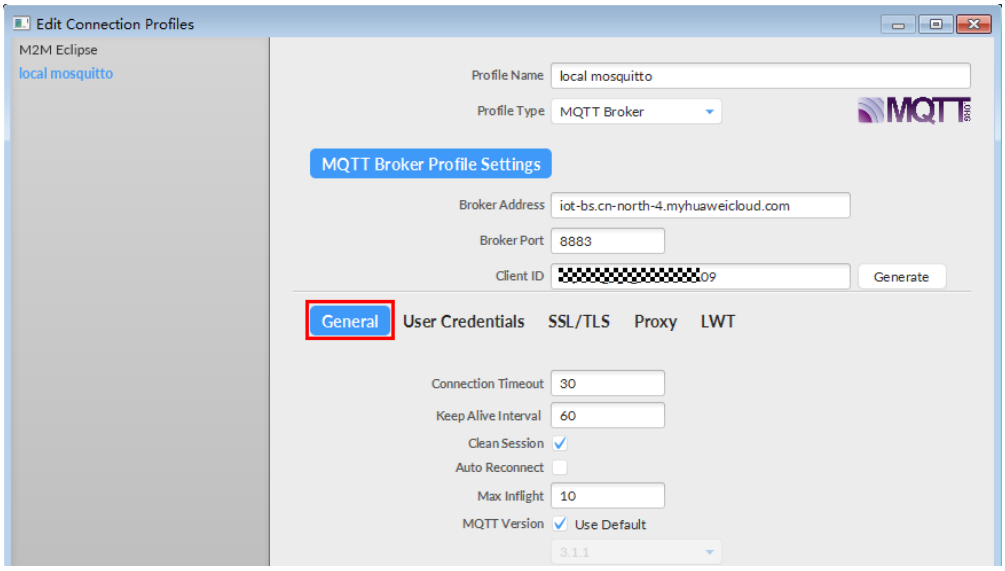
MQTT.fx 是目前主流的MQTT桌面客户端，它支持 Windows, Mac, Linux，可以快速验证是否可以与设备发放服务进行连接并发布或订阅消息。

本文主要介绍 MQTT.fx 如何与华为设备发放交互，其中设备发放服务MQTT的南向接入地址请参考**获取终端节点**。

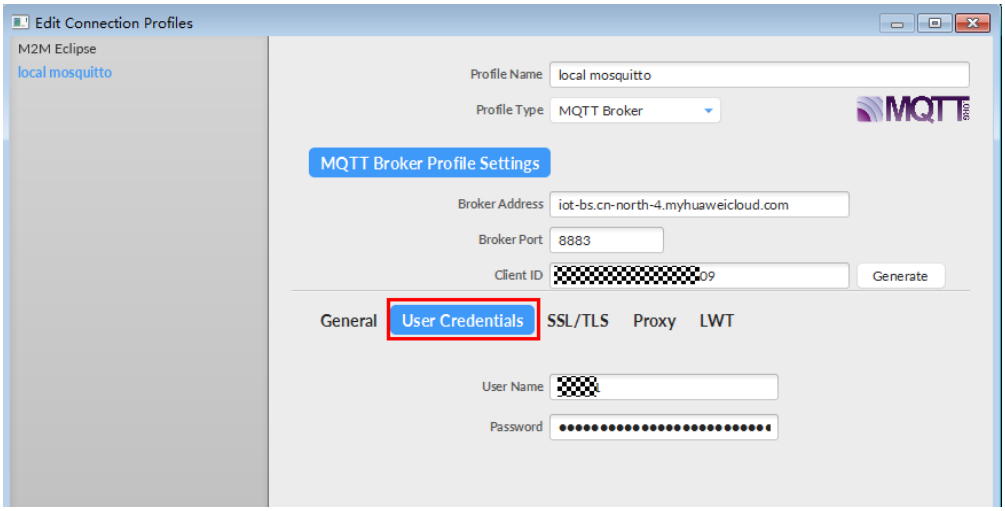
1. 下载 **MQTT.fx**（默认是64位操作系统，如果是32位操作系统，单击此处下载 **MQTT.fx** ），安装MQTT.fx工具。
2. 打开 MQTT.fx 客户端程序，单击“设置”。



3. 填写 Connection Profile 相关信息和 General 信息。其中General 信息可以用工具默认的参数配置。



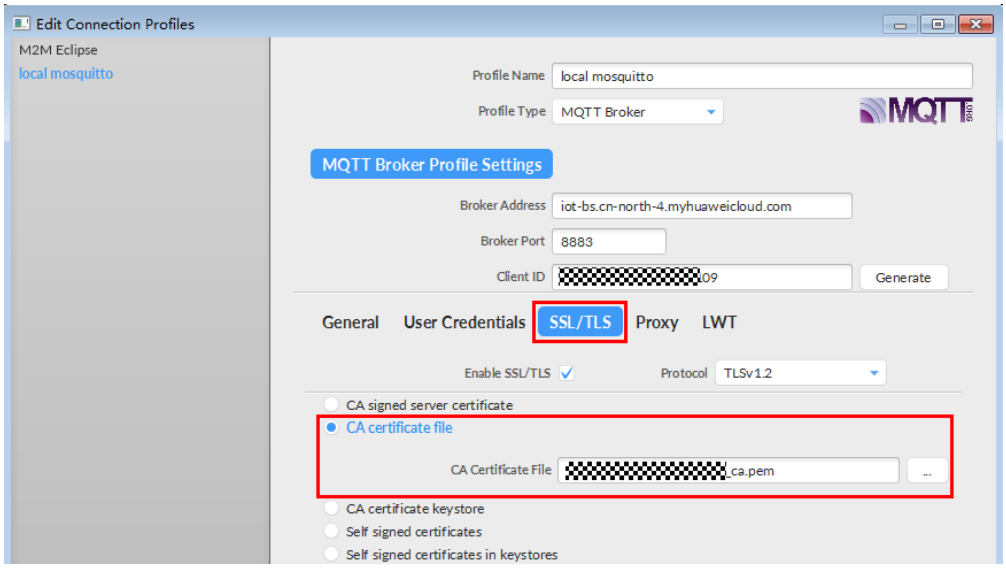
4. 填写 User Credentials 信息。



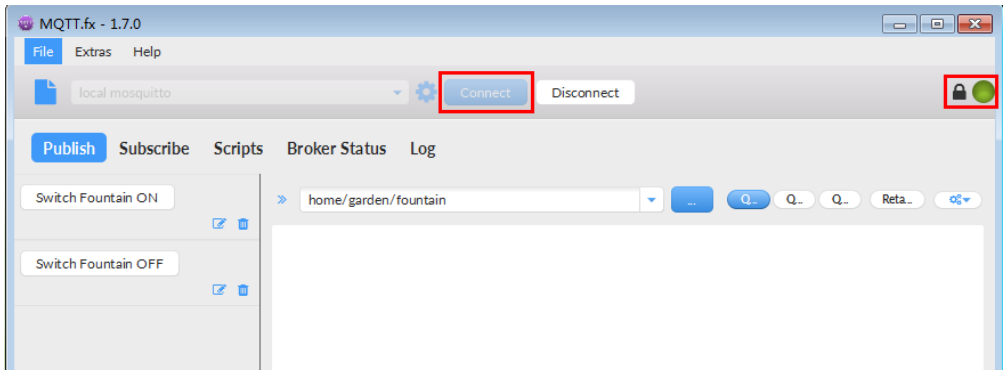
说明

其中Username 和Password 参数参考**MQTT CONNECT连接鉴权**参数说明。

5. 选择开启 SSL/TLS，勾选CA certificate file，CA Certificate File指定为物联网平台根证书（请先下载**物联网平台的根证书**，解压后，选择其中c或java目录下PEM后缀的文件）的本地路径。

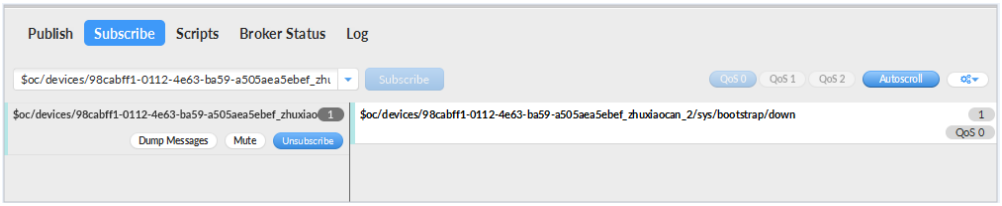


6. 完成以上步骤后，单击“Apply”和“OK”保存，并在配置文件框中选择刚才创建的文件名，单击“Connect”，当右上角圆形图标为绿色时，说明连接设备发放服务成功，可进行订阅（Subscribe）和消息推送（Publish）操作。



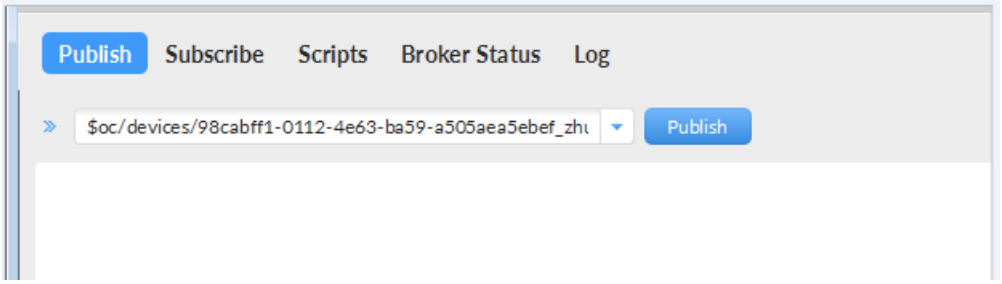
引导消息订阅

按照**设备接收引导信息**topic填写对应的topic，单击“Subscribe”进行订阅。订阅成功如下所示：



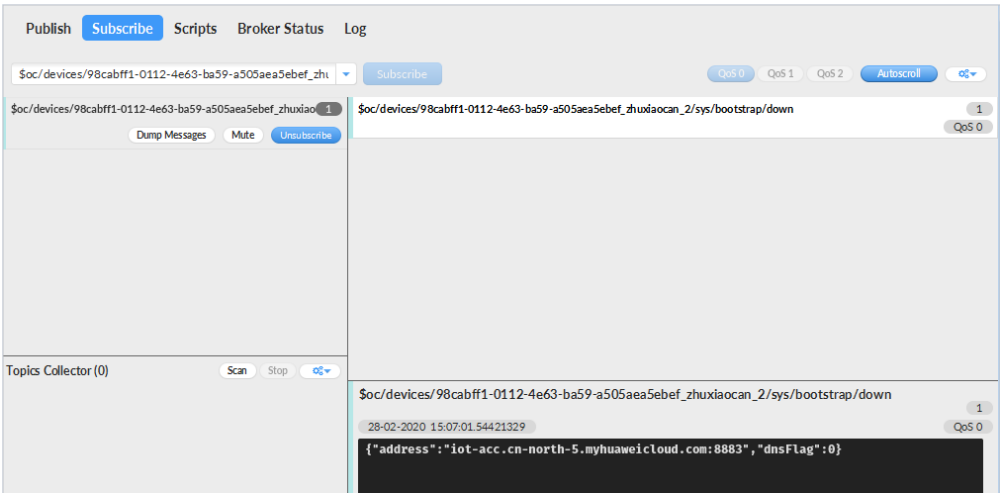
引导请求发布

按照**设备请求引导信息**topic填写对应的topic，单击“Publish”进行消息推送。



接收到引导消息

消息推送成功如下所示，在Subscribe的topic下会返回对应设备的设备接入服务的地址。



后续操作

至此，您已完成了设备发放的流程。设备发放已成功将您的设备【**接入IoTDA所需的必要信息**】预置到了IoTDA实例中。

如您想要体验物联网平台的更多强大功能，您可通过如下步骤完成对IoTDA的后续操作：

1. 取用引导消息中的设备接入地址；
2. 单击Disconnect，断开与设备发放的连接；
3. 将引导信息中的设备接入地址填入MQTT.fx的MQTT Broker Profile Settings中的Broker Address和Broker Port，建立与设备接入的连接；
4. 完成与设备接入的上报数据等业务交互。

您可参考指导：**设备接入 IoTDA> 开发指南> 设备侧开发> 使用MQTT Demo接入> 使用MQTT.fx调测**中的【**上报数据**】和【**进阶体验**】部分。

说明

得益于设备发放的预置功能，在参考IoTDA指导过程中，您无需再创建产品和设备。

5 MQTT 场景--使用华为 SDK 接入设备发放示例

5.1 MQTT 密钥设备使用静态策略发放

获取设备发放终端节点

表 5-1 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

添加静态策略

添加静态策略，根据关键字发放到指定的IoTDA。

图 5-1 创建静态策略

图 5-2 创建静态策略详情

注册设备

在设备发放控制台，注册MQTT设备，其中安全模式选择密钥模式。

图 5-3 注册设备

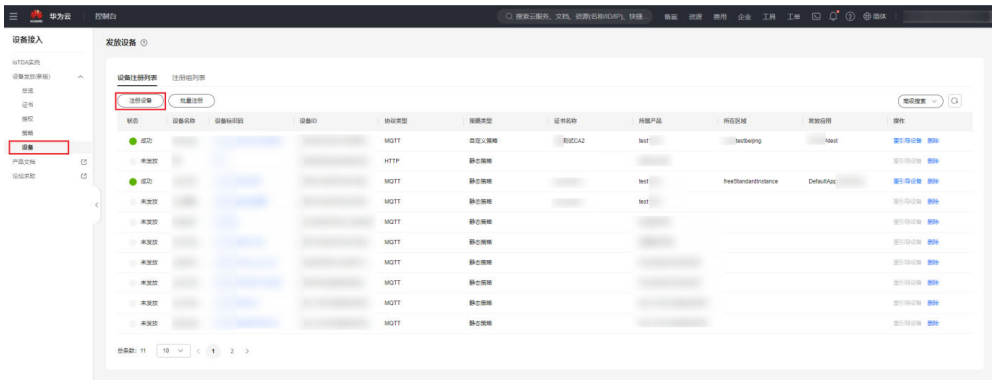
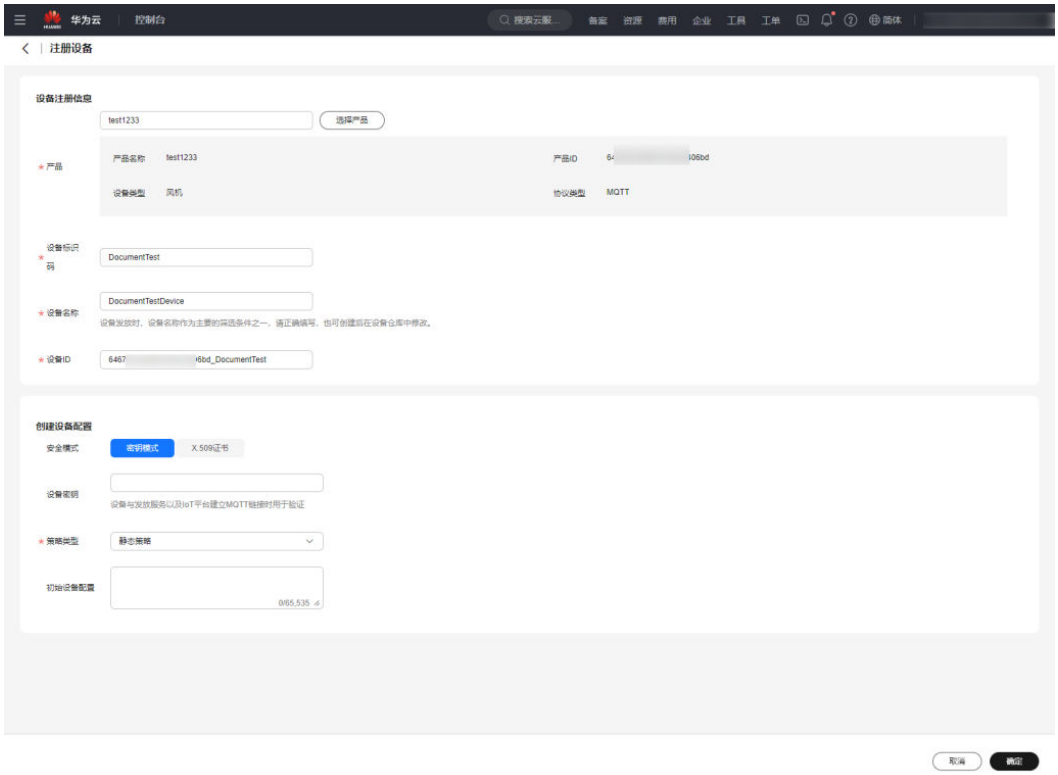


图 5-4 创建密钥模式静态策略设备



说明

此处注册设备的设备名称需与**添加静态策略**步骤的策略实例关键字相匹配，方能触发该静态策略。

设备引导

下载并修改华为SDK示例代码进行设备引导（这里以**java sdk代码**为示例）。

说明

用IDEA/Eclipse打开SDK代码工程，修改DEMO示例BootstrapSample中的参数，其中deviceId和secret替换为步骤3中生成的设备ID和密钥即可，bootstrapUri为**获取设备发放终端节点**对应的终端节点。

```
package com.huaweicloud.sdk.iot.device.demo;

import com.huaweicloud.sdk.iot.device.bootstrap.BootstrapClient;


/**
 * 演示设备启动时，通过引导服务获取真实的服务器地址
 */
public class BootstrapSample {

    public static void main(String[] args) {

        String deviceId = "60136b0682401c03e0b1ccf5_aaa_device2";
        String secret = "73ce5656f5d4a9919532";
        String bootstrapUri = "ssl://100.95.158.64:8883";

        //创建引导客户端，发起引导
        BootstrapClient bootstrapClient = new BootstrapClient(bootstrapUri, deviceId, secret);
        DefaultBootstrapActionListener defaultBootstrapActionListener = new DefaultBootstrapActionListener(deviceId,
            secret, bootstrapClient);
        bootstrapClient.bootstrap(defaultBootstrapActionListener);

    }
}
```

运行DEMO程序，看到如下日志，代表设备发放成功，并且已经收到设备发放下发的设备接入地址。如果程序运行没报错，在对应的设备接入平台可以看到设备，并已在线。

```
2021-01-29 14:46:47  INFO BootstrapClient:50 - create BootstrapClient: 60136b0682401c03e0b1ccf5_aaa_device2
2021-01-29 14:46:48  INFO MqttConnection:167 - try to connect to ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:200 - connect success ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:105 - Mqtt client connected. address :ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:240 - publish message topic =  $oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/up, msg =
2021-01-29 14:46:48  INFO DefaultBootstrapActionListener:30 - bootstrap success:$oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/down
2021-01-29 14:46:49  INFO DefaultBootstrapActionListener:30 - bootstrap success:null
2021-01-29 14:46:49  INFO MqttConnection:85 - messageArrived topic =  $oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/down, msg = {"address":"100.95.174.182:1883","initConfig":null}
2021-01-29 14:46:49  INFO BootstrapClient:102 - bootstrap ok address:100.95.174.182:1883
2021-01-29 14:46:49  INFO DefaultBootstrapActionListener:30 - bootstrap success:100.95.174.182:1883
```

5.2 MQTT 注册组静态策略发放示例

制作 CA 证书

步骤1 在浏览器中访问**这里**，下载并进行安装OpenSSL工具，安装完成后配置环境变量。

步骤2 在 D:\certificates 文件夹下，以管理员身份运行cmd命令行窗口。

步骤3 生成密钥对（rootCA.key）：

说明

生成“密钥对”时输入的密码在生成“证书签名请求文件”、“CA证书”，“验证证书”以及“设备证书”时需要用到，请妥善保存。

```
openssl genrsa -des3 -out rootCA.key 2048
```

步骤4 使用密钥对生成证书签名请求文件：

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下**表1** 所示。

表 5-2 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

```
openssl req -new -key rootCA.key -out rootCA.csr
```

步骤5 生成CA证书（rootCA.crt）：

```
openssl x509 -req -days 50000 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
```

说明

“-days”后的参数值指定了该证书的有效天数，此处示例为50000天，您可根据实际业务场景和需要进行调整。

----结束

获取设备发放终端节点

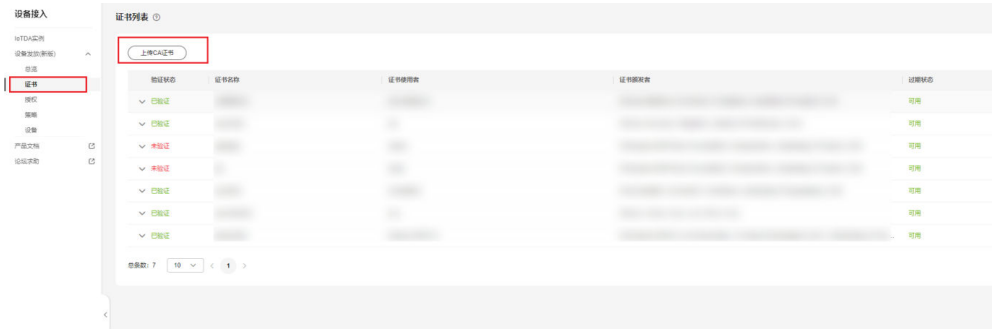
表 5-3 设备发放节点列表

区域名称	区域	终端节点（Endpoint）	端口	协议
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	8883	MQTTS

上传并验证 CA 证书

步骤1 登录**设备发放控制台**，进入“证书”界面，单击右上角“上传CA证书”，填写“证书名称”并上传上述“制作CA证书”步骤后生成的“CA证书（rootCA.crt文件）”，单击“确定”。

图 5-5 上传 CA 证书

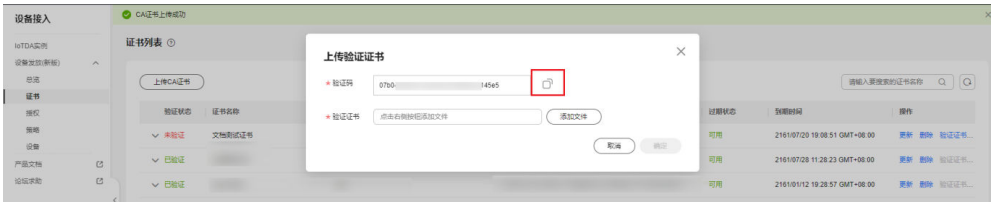


步骤2 验证**步骤1**中上传的CA证书，只有成功验证证书后该证书方可使用。

1. 为验证证书生成密钥对。
   ```
   openssl genrsa -out verificationCert.key 2048
   ```
2. 获取随机验证码。

图 5-6 上传 CA 证书完成页

图 5-7 复制验证码



3. 利用此验证码生成证书签名请求文件CSR。
   ```
   openssl req -new -key verificationCert.key -out verificationCert.csr
   ```

   说明

   CSR文件的Common Name (e.g. server FQDN or YOUR name) 需要填写前一过程中获取到的随机验证码。

4. 使用CA证书、CA证书私钥和CSR文件创建验证证书（verificationCert.crt）。
   ```
   openssl x509 -req -in verificationCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out verificationCert.crt -days 500 -sha256
   ```

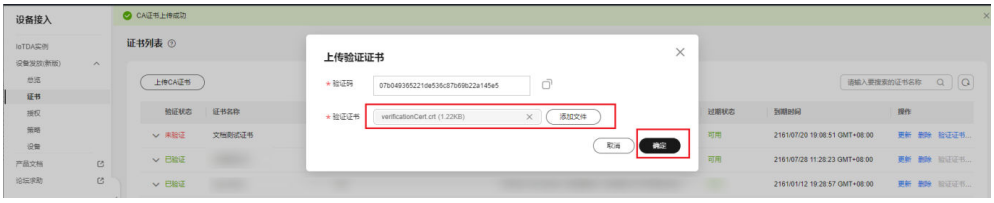

说明

生成验证证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件。

“-days”后的参数值指定了该证书的有效天数，此处示例为500天，您可根据实际业务场景和需要进行调整。

5. 上传验证证书进行验证。

图 5-8 上传验证证书



----结束

生成设备证书

步骤1 使用OpenSSL工具为设备证书生成密钥对（设备私钥）：

```
openssl genrsa -out deviceCert.key 2048
```

步骤2 使用设备密钥对，生成证书签名请求文件：

```
openssl req -new -key deviceCert.key -out deviceCert.csr
```

说明

生成证书签名请求文件时，要求填写证书唯一标识名称（Distinguished Name，DN）信息，参数说明如下表2所示。

表 5-4 证书签名请求文件参数说明

提示	参数名称	取值样例
Country Name (2 letter code) []:	国家/地区	CN
State or Province Name (full name) []:	省/市	GuangDong
Locality Name (eg, city) []:	城市	ShenZhen
Organization Name (eg, company) []:	组织机构（或公司名）	Huawei Technologies Co., Ltd.
Organizational Unit Name (eg, section) []:	机构部门	Cloud Dept.
Common Name (eg, fully qualified host name) []:	CA名称（CN）	Huawei IoTDP CA
Email Address []:	邮箱地址	/

提示	参数名称	取值样例
A challenge password []:	证书密码，如您不设置密码，可以直接回车	/
An optional company name []:	可选公司名称，如您不设置，可以直接回车	/

步骤3 使用CA证书、CA证书私钥和CSR文件创建设备证书（deviceCert.crt）。

```
openssl x509 -req -in deviceCert.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out deviceCert.crt -days 36500 -sha256
```

说明

生成设备证书用到的“rootCA.crt”和“rootCA.key”这两个文件，为“制作CA证书”中所生成的两个文件，且需要完成“上传并验证CA证书”。

“-days”后的参数值指定了该证书的有效天数，此处示例为36500天，您可根据实际业务场景和需要进行调整。

----结束

添加静态策略

“关键字”为注册组名称中的关键字。设备发放时，注册组下的设备的设备名称为“注册组名称+设备ID”，如果包含设置的关键字，则可按该实例进行发放。

图 5-9 创建静态策略

新增注册组

图 5-10 新增注册组

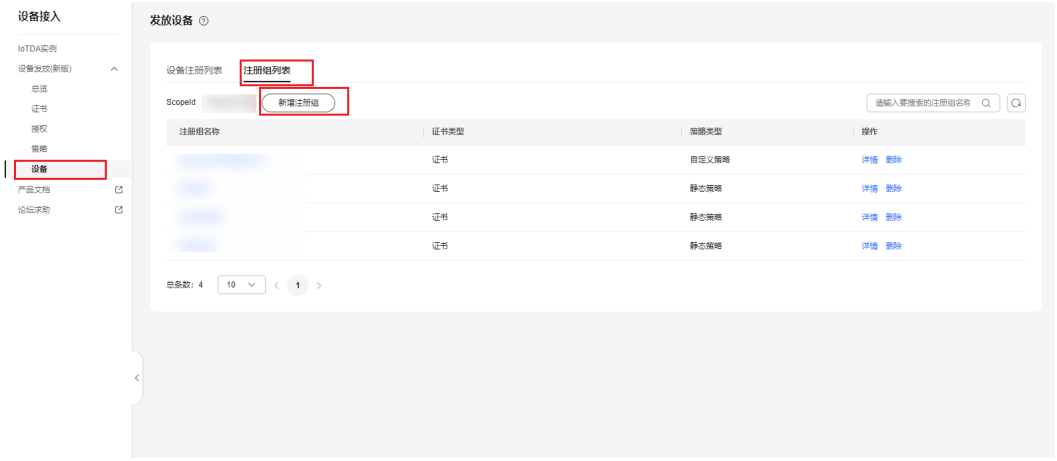
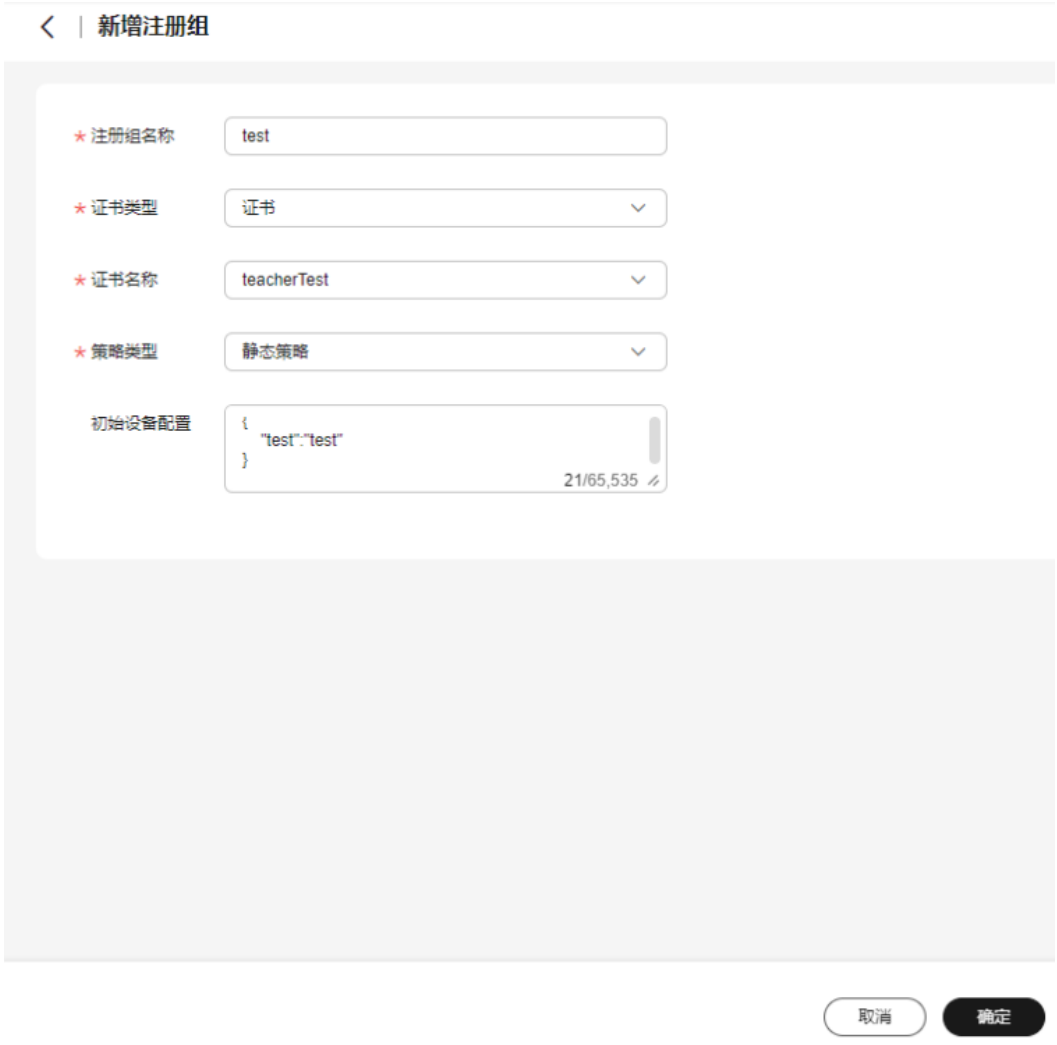


图 5-11 创建证书静态注册组



设备引导

步骤1 下载并修改华为SDK示例代码进行设备引导（这里以**java sdk代码**为示例）。

说明

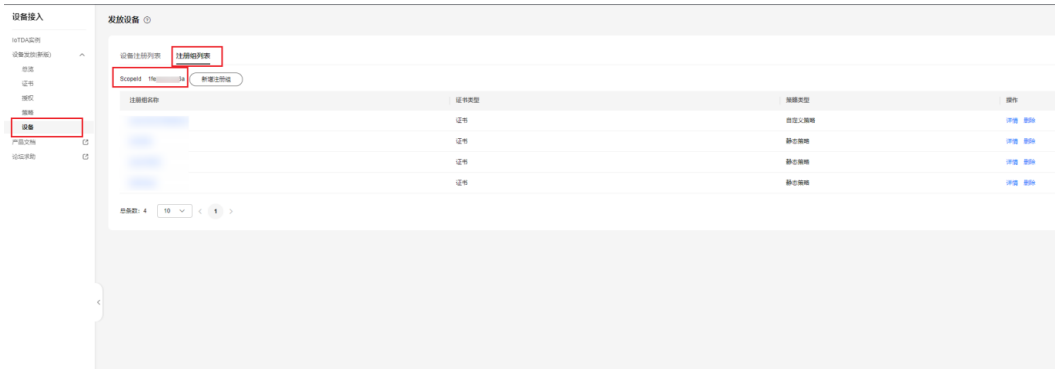
用IDEA/Eclipse打开SDK代码工程，修改DEMO示例BootsrapSelfRegSample中的参数。

其中deviceId可以自己随意命名，用一个唯一标识设备身份的ID，也可用设备证书的唯一标识身份，设备证书使用者的CN。(因为注册组的场景不存在选择产品所以命名需要注意：如果命名字符串有“_”，那么第一项必须为对应设备接入已经存在的产品ID，如果不包括“_”，那么可以随意命名)。

```
public class BootsrapSelfRegSample {
    private static final Logger log = LogManager.getLogger(BootsrapSelfRegSample.class);

    public static void main(String[] args) throws Exception {

        String deviceId = "iodpsDemo";
        String scopeId = "9b7906a5190a"; //设备组方式用到
        String bootstrapUri = "ssl://100.95.158.64:8883";

        //读取pem格式证书
        KeyStore keyStore = X509CertificateDeviceSample.getKeyStore( certificateFile: "D:\\cert\\deviceCert.pem",
            privateKeyFile: "D:\\cert\\deviceCert.key", keyPassword: "");

        /**
         * 读取keystore格式证书
         *
         * KeyStore keyStore = KeyStore.getInstance(KeyStore.getDefaultType());
         * keyStore.load(new FileInputStream("D:\\SDK\\cert\\my.keystore"), "huawei".toCharArray());
         *
         */

        //创建引导客户端，发起引导
        //BootstrapClient bootstrapClient = new BootstrapClient(bootstrapUri, deviceId, keyStore, "yourPassWord");

        BootstrapClient bootstrapClient = new BootstrapClient(bootstrapUri, deviceId, keyStore, keyPassword: "", scopeId);


        bootstrapClient.bootstrap(new ActionListener() {
```

ScopeId可以在设备发放页面单击 设备->注册组列表 查询。

图 5-12 查看 ScopeId



说明

bootstrapUri为**获取设备发放终端节点**对应的终端节点。

keyStore的参数为对应注册组的CA证书签发的设备证书，私钥文件对应的本地目录。如果私钥不加密，那么不需要填写keyPassword，对应bootstrapClient = new BootstrapClient(bootstrapUri, deviceId, keyStore, “”, scopeId)。

运行DEMO程序，看到如下日志，代表设备发放成功，并且已经收到设备发放下发的设备接入地址。如果程序运行没报错，在对应的设备接入平台可以看到设备，并已在线。

```
2021-01-29 14:46:47  INFO BootstrapClient:50 - create BootstrapClient: 60136b0682401c03e0b1ccf5_aaa_device2
2021-01-29 14:46:48  INFO MqttConnection:167 - try to connect to ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:200 - connect success ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:105 - Mqtt client connected. address :ssl://100.95.158.64:8883
2021-01-29 14:46:48  INFO MqttConnection:240 - publish message topic =  $oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/up, msg =
2021-01-29 14:46:48  INFO DefaultBootstrapActionListener:30 - bootstrap success:$oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/down
2021-01-29 14:46:49  INFO DefaultBootstrapActionListener:30 - bootstrap success:null
2021-01-29 14:46:49  INFO MqttConnection:85 - messageArrived topic =  $oc/devices/60136b0682401c03e0b1ccf5_aaa_device2/sys/bootstrap/down, msg = {"address":"100.95.174.182:1883","initConfig":null}
2021-01-29 14:46:49  INFO BootstrapClient:102 - bootstrap ok address:100.95.174.182:1883
2021-01-29 14:46:49  INFO DefaultBootstrapActionListener:30 - bootstrap success:100.95.174.182:1883
```

----结束

