设备发放

用户指南

文档版本 02

发布日期 2022-04-24

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 从这里开始

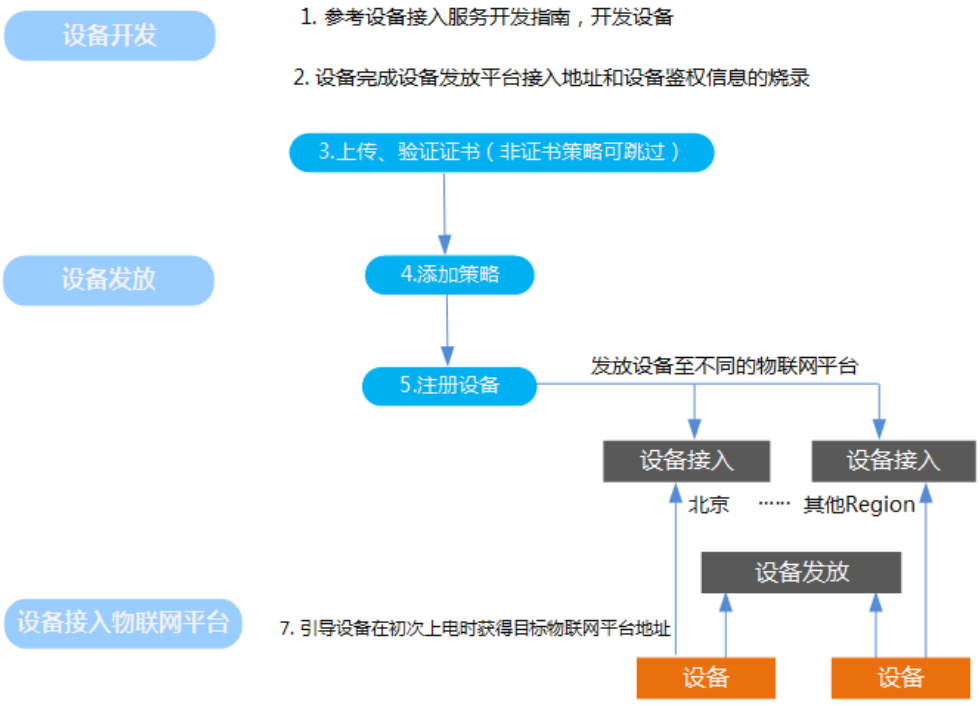


表 1-1 设备发放操作步骤列表

使用阶段	步骤
设备开发	1. 开通设备接入服务，参考开发指南，完成设备开发。 • LiteOS设备（LwM2M），设备需要具有设备发放功能。 • 原生MQTT协议设备，需要完成**设备引导接口**开发，使设备具有设备发放功能。 **注：**若设备需要使用物联网卡，可在**全球SIM联接**服务购买物联网卡和套餐。

使用阶段	步骤
	2. 设备完成设备发放平台接入地址和设备鉴权信息的烧录。**设备发放平台接入地址请在控制台中获取。** ● LiteOS设备（LwM2M）：需要烧录设备发放平台接入地址、设备标识码、引导服务端PSK。 ● 原生MQTT协议设备，需要烧录设备发放平台接入地址、设备ID、设备密钥。
设备发放	3. **证书**：用于证书策略发放的设备需要上传证书，防止通信数据在传输过程被篡改造成安全风险。
	4. **策略**：策略用于控制设备按照指定策略或规则发放至不同的物联网平台。
	5. **设备**：将设备基本信息导入设备发放平台中，用于后续发放至不同的物联网平台。
设备接入物联网平台	6. 设备初次上电时，先接入到设备发放平台，随后通过Bootstrap流程引导设备获得目标物联网平台地址。

2 证书

概述

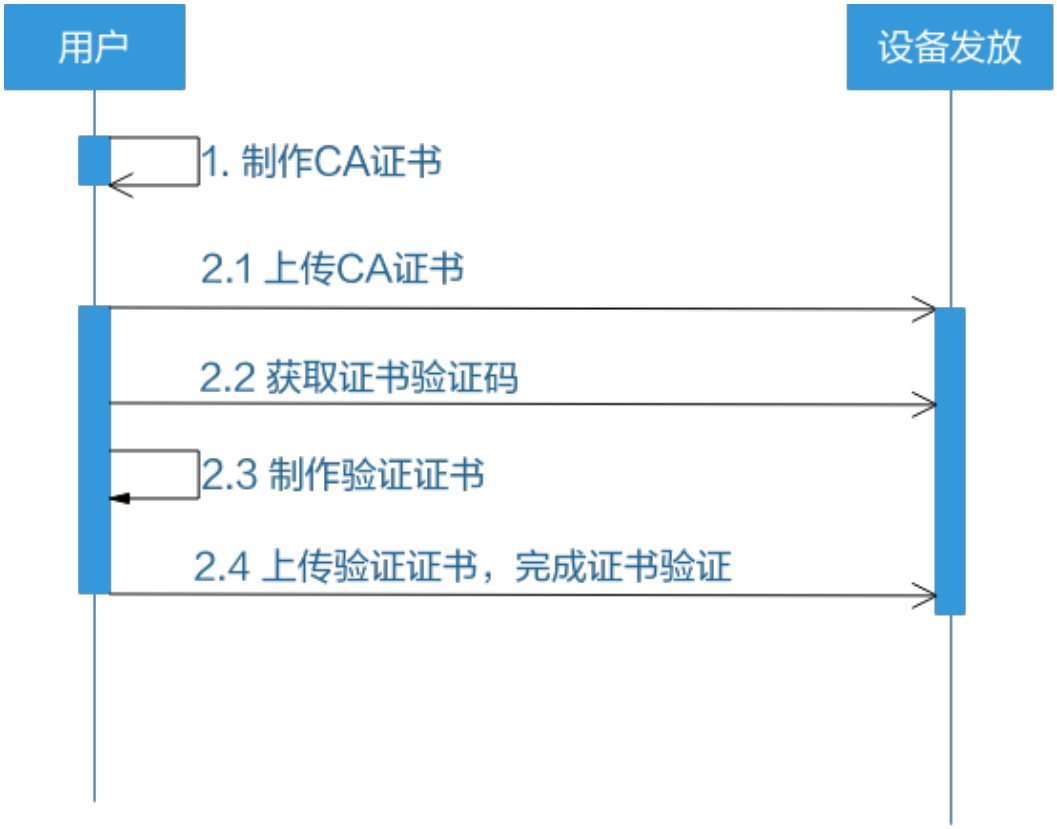
数字证书保证系统内各服务及系统与外部通信的安全性，防止通信数据在传输过程被篡改造成安全风险。

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。

设备 CA 证书管理

本章节介绍设备CA证书的制作，以及如何在物联网平台上传、验证和管理设备CA证书。

图 2-1 设备 CA 证书制作



本章节样例中的各类证书常用文件名：

表 2-1 常用文件名列表

证书	文件名	MQTT.fx中的字段名
服务端证书	-	-
服务端CA证书	如下其中之一： huaweicloud-iot-root-ca-list.bks（android） huaweicloud-iot-root-ca-list.pem（c或java） huaweicloud-iot-root-ca-list.jks（java） bsca.jks（java） bsrootcert.pem（c）	CA File
设备证书（客户端证书）	deviceCert.crt	Client Certificate File
设备证书（客户端证书）私钥	deviceCert.key	Client Key File
CA证书（设备CA证书/客户端CA证书）	rootCA.crt	-

2.1 制作 CA 证书

本文以Windows环境为例，介绍通过Openssl工具制作CA证书和验证证书的方法。

说明

以下“生成密钥对（rootCA.key）”和“生成CA证书（rootCA.crt）”为操作过程中需要使用到的两个文件。

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 2-2 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.

提示	参数名称	取值样例
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

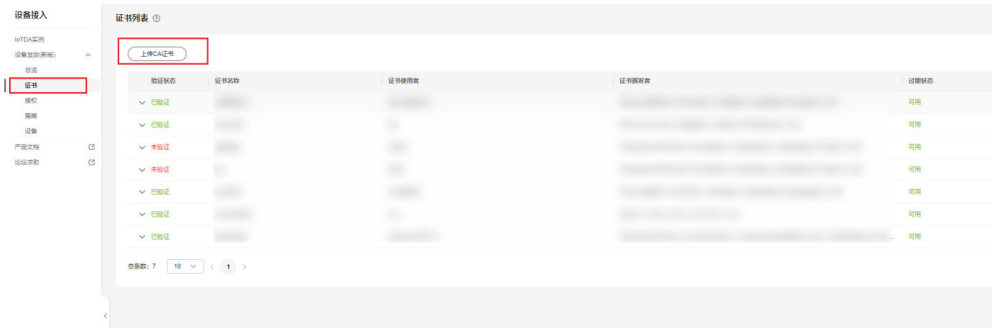
2.2 上传 CA 证书

操作步骤

步骤1 登录**设备发放控制台**。

步骤2 在设备发放控制台，左侧导航窗格中，选择“证书”，单击右上方的“上传CA证书”。

图 2-2 上传 CA 证书



步骤3 在“上传CA证书”页面，填写“证书名称”，单击“添加文件”，上传此前“**制作CA证书**”步骤中生成的“CA证书（rootCA.crt文件）”，单击“确定”。

图 2-3 上传 CA 证书详情页

----结束

说明

上传的CA证书初始状态为“未验证”，需要完成“**验证CA证书**”过程，方可正常使用该CA证书。

表 2-3 证书状态列表

CA证书状态	说明
已验证	可正常使用。
未验证	不可正常使用，待验证通过后，方可正常使用。
已过期	CA证书已过期，需更新，但不影响平台使用该CA证书验证对应的设备证书。
即将过期	CA证书30天内即将过期，需及时更新。

2.3 验证 CA 证书

对于已上传的CA证书，平台要求用户完成“验证CA证书”过程，以验证用户具备该CA证书的签发能力。

操作步骤

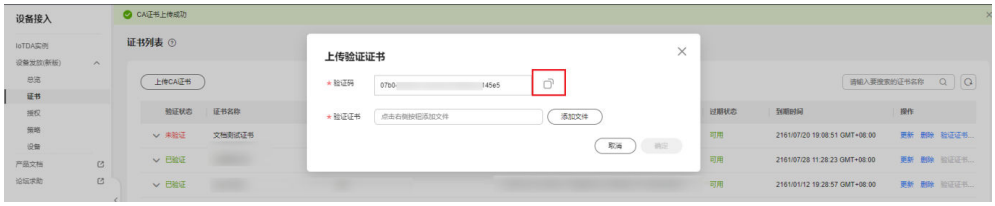
步骤1 登录**设备发放控制台**。

步骤2 在设备发放控制台，左侧导航窗格中，选择“证书”，单击“证书列表”条目的操作栏中的“验证证书”。

图 2-4 上传 CA 证书完成页

步骤3 在上传验证证书页面，单击“生成验证码”，单击“复制图标”复制此CA证书的随机验证码。

图 2-5 复制验证码



说明

CA证书验证码有效期为一天，请及时使用验证码生成验证证书并完成验证。

验证码的生成为替换机制，即对于一个CA证书，即使此前的验证码未过期，也将被新生成的验证码替换。

步骤4 使用OpenSSL工具为验证证书生成密钥对。

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

步骤5 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) 需要填写此验证码。

步骤6 使用CA证书、CA证书私钥和上一步骤中生成的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 36500 -sha256
```

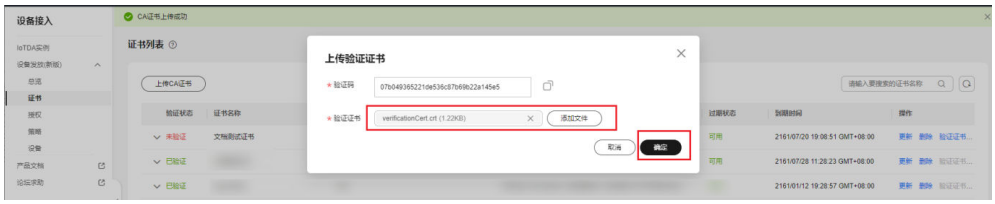
说明

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36500天，您可根据实际业务场景和需要进行调整。

步骤7 上传验证证书进行验证。

图 2-6 上传验证证书



----结束

2.4 签发设备证书

已上传并验证CA证书后，就可以使用此CA证书签发设备证书供设备使用。

操作步骤

步骤1 使用OpenSSL工具为设备证书生成密钥对，即”设备证书（客户端证书）私钥”。

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

步骤2 使用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1所示。

表 2-4 证书签名请求文件列表

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	/

提示	参数名称	取值样例
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证书私钥和上一步骤中生成的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”**验证CA证书**”流程。

“-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

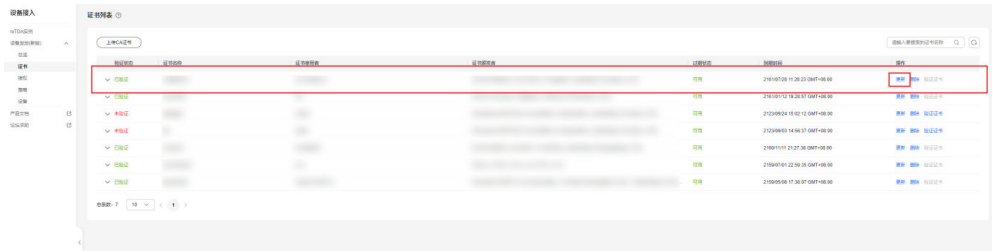
----结束

2.5 更新 CA 证书

步骤1 登录**设备发放控制台**。

步骤2 在设备发放控制台，左侧导航窗格中，选择“证书”，单击“证书列表”条目的操作栏中的“更新”。

图 2-7 更新 CA 证书



说明

更新CA证书前，要求该证书未被设备、策略、注册组关联。

更新CA证书后，该证书状态将变为未验证，请重新完成验证CA证书过程。

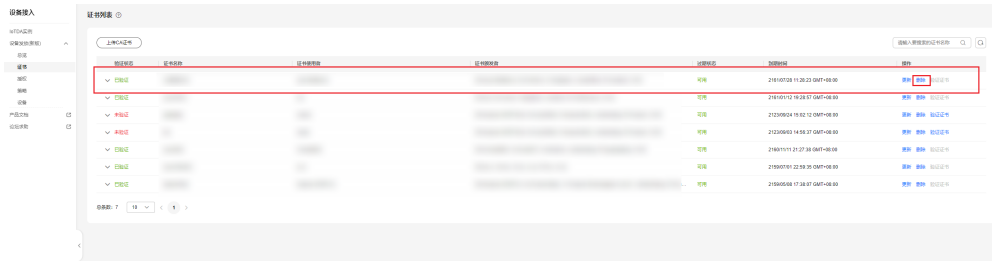
----结束

2.6 删除 CA 证书

步骤1 登录**设备发放控制台**。

步骤2 在设备发放控制台，左侧导航窗格中，选择“证书”，单击“证书列表”条目的操作栏中的“删除”。

图 2-8 删除 CA 证书



说明

关联了至少一个设备、策略或注册组的CA证书，不允许删除。

请谨慎操作，删除后的CA证书的所有数据将被删除且不可恢复。

----结束

3 授权

概述

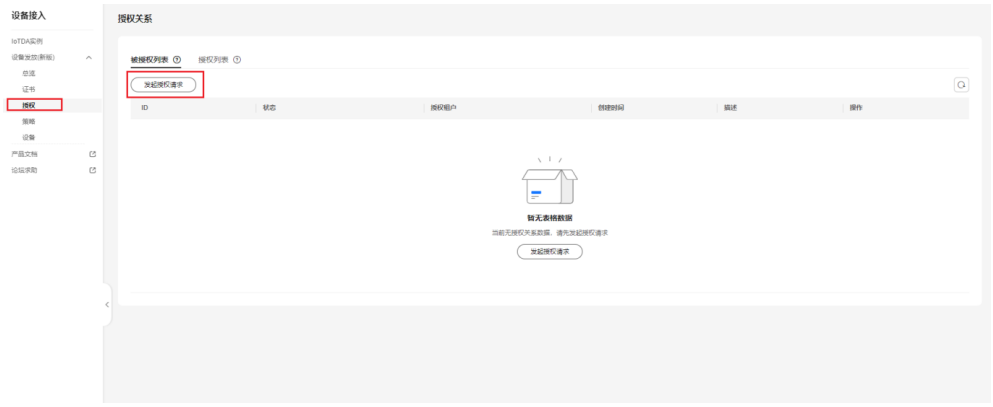
授权，即授权关系，是两个租户在设备发放中建立的一种租户间单向的资源共享的关系。

通过授权功能，授权租户向被授权租户共享授权租户下的设备接入实例，被授权租户可使用授权租户的设备接入实例作为发放策略的目的接入点，从而实现跨账号发放设备的能力。

创建授权关系

1. 被授权方进入“授权”界面，单击在“被授权列表”下的“发起授权请求”。

   图 3-1 发起授权请求

2. 被授权方填写授权方的账号名称或者账号ID（即IAM的Domain Name或Domain ID），单击“获取短信验证码”。

图 3-2 发起授权请求详情

3. 系统将向授权方绑定的手机号发送短信验证码，被授权方从授权方获取到短信验证码，填入验证码输入框，填写“描述”信息。
4. 被授权方单击“确定”，授权请求完成，授权关系建立。
5. 被授权方将在“被授权列表”中查看到与其他租户建立的授权关系，授权方将在“授权列表”中查看到与其他租户建立的授权关系。被授权方可删除某一条授权关系，授权方可禁用或删除某一条授权关系。

删除或禁用授权关系

删除授权关系，将导致授权方与被授权方之间授权关系的解除。禁用授权关系，将导致授权关系处于禁用状态。

说明

授权关系的删除或禁用，将导致与之关联的跨账号功能不可用，请谨慎操作。

图 3-3 被授权方删除授权关系

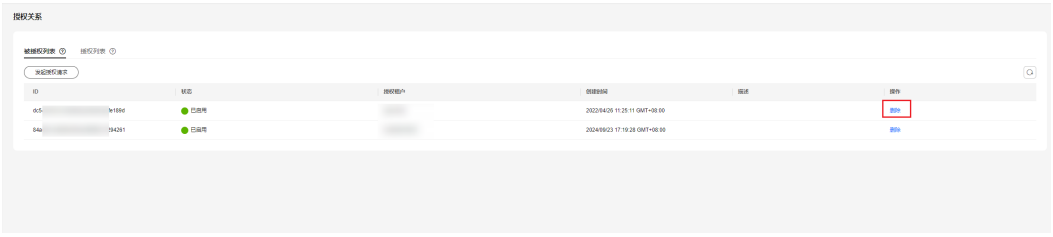
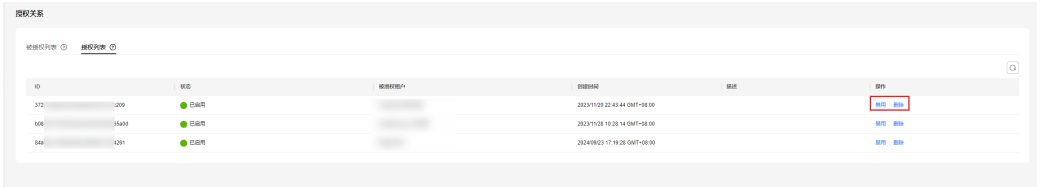


图 3-4 授权方禁用或删除授权关系



4 策略

策略用于控制设备按照指定策略或规则发放至不同的物联网平台。当前支持自定义策略、证书策略、静态策略。

自定义策略

证书策略

静态策略

4.1 自定义策略

与静态策略和证书策略相比，自定义策略为您提供更灵活的策略机制。自定义策略实例指示函数关联的设备接入实例，一个函数可关联多个设备接入实例。

设备匹配自定义策略实例的机制为：

1. 设备的发放策略指定为“函数策略”时，需同时指定其关联的函数，设备与自定义策略实例关联同一个函数时，即被认为该设备匹配上该条策略实例；
2. 一个设备可匹配多条自定义策略实例。

4.1.1 创建自定义策略函数

了解函数接口定义

函数服务对函数有明确的接口定义。

说明

以java语言为例，接口定义为：*作用域 返回参数 函数名（函数参数，Context参数）*。

- 作用域：提供给FunctionGraph调用的用户函数必须定义为public。
- 返回参数：用户定义，FunctionGraph负责转换为字符串，作为HTTP Response返回。对于返回参数对象类型，HTTP Response该类型的JSON字符串。
- 函数名：用户定义函数名称。
- 用户定义参数：当前函数只支持一个用户参数。对于复杂参数，建议定义为对象类型，以JSON字符串提供数据。FunctionGraph调用函数时，解析JSON为对象。
- Context参数：runtime提供函数执行上下文，其接口定义在**SDK接口**说明。

创建Java函数时，函数入口参数需要提供函数完整的名字空间，参数格式为：包名.类名.函数名。

设备发放在此基础上，要求函数代码满足如下条件：

- 返回参数：需满足**设备发放对返回参数的约束**；
- 函数参数：需满足**设备发放对函数参数的约束**；
- 函数接口实现：从函数参数中的备选接入点中选择一个接入点，调用**发放设备接口**，根据接口响应拼接参数返回。

编写自定义函数

步骤1 创建函数工程，编写函数。

首先建立一个普通的Java项目，添加FunctionGraph函数**JavaSDK**为工程依赖，可下载设备发放提供**函数Demo**，参照Demo创建工程编写函数。

说明

FunctionGraph函数JavaSDK提供了Event事件接口、Context接口和日志记录接口。其中Runtime-x.x.x.jar包含了函数执行上下文，其他Jar包为附带的第三方库，可按需添加。

Java函数开发指南参见**函数工作流 FunctionGraph > 开发指南 > 如何开发函数 > Java函数开发指南**。

参照如下代码编写函数，实现必要逻辑。

```
package com.huawei.demo;

import com.huawei.demo.common.logger.DefaultLogger;
import com.huawei.demo.model.AccessPointPara;
import com.huawei.demo.model.FunctionGraphPara;
import com.huawei.demo.model.TdpFuncResult;
import com.huawei.services.runtime.Context;

import java.util.Optional;

/**
 * 实现该类。
 * WARNING：{@link #apiHandle(FunctionGraphPara, Context)} 该方法必须在子类中定义，否则函数无法触发该函数接口！！！
 * <pre>
 * {@code
 *     @Override
 *     public TdpFuncResult apiHandle(FunctionGraphPara para, Context context) {
 *         return super.apiHandle(para, context);
 *     }
 * }
 * </pre>
 */
public abstract class TdpFunction {
    protected static final DefaultLogger LOGGER = new DefaultLogger(TdpFunction.class);

    /**
     * 函数定义
     */
    public TdpFuncResult apiHandle(FunctionGraphPara para, Context context) {
        // 获取日志
        DefaultLogger.init(Optional.ofNullable(context)
            .map(Context::getLogger)
            .orElse(null));

        // 校验入参
        TdpFuncResult result = checkPara(para, context);
        if (result != null) {
            return result;
        }
```



```
        // 确定接入点
        AccessPointPara accessPointPara = determineAccessPoint(para);

        // 发放设备
        result = provisionDevice(para, accessPointPara);

        LOGGER.info("result:{}", result);
        return result;
    }

    /**
     * 校验入参
     */
    protected abstract TdpFuncResult checkPara(FunctionGraphPara para, Context context);

    /**
     * 从备选的接入点中选择合适的接入点
     */
    protected abstract AccessPointPara determineAccessPoint(FunctionGraphPara para);

    /**
     * 调用设备发放的发放接口发放设备
     */
    protected abstract TdpFuncResult provisionDevice(FunctionGraphPara para, AccessPointPara
accessPointPara);
}
```

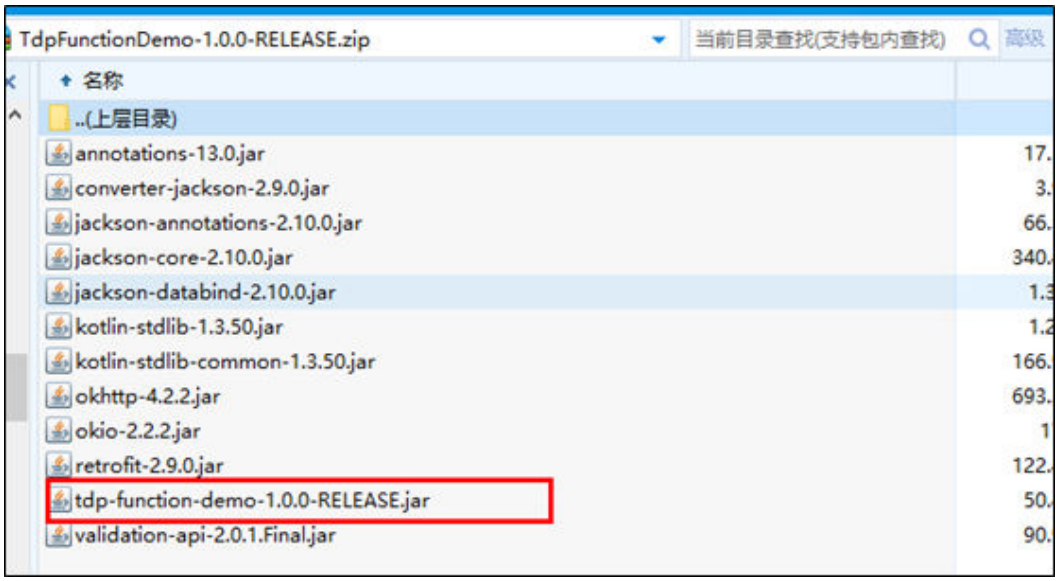
步骤2 打包函数，上传代码。

说明

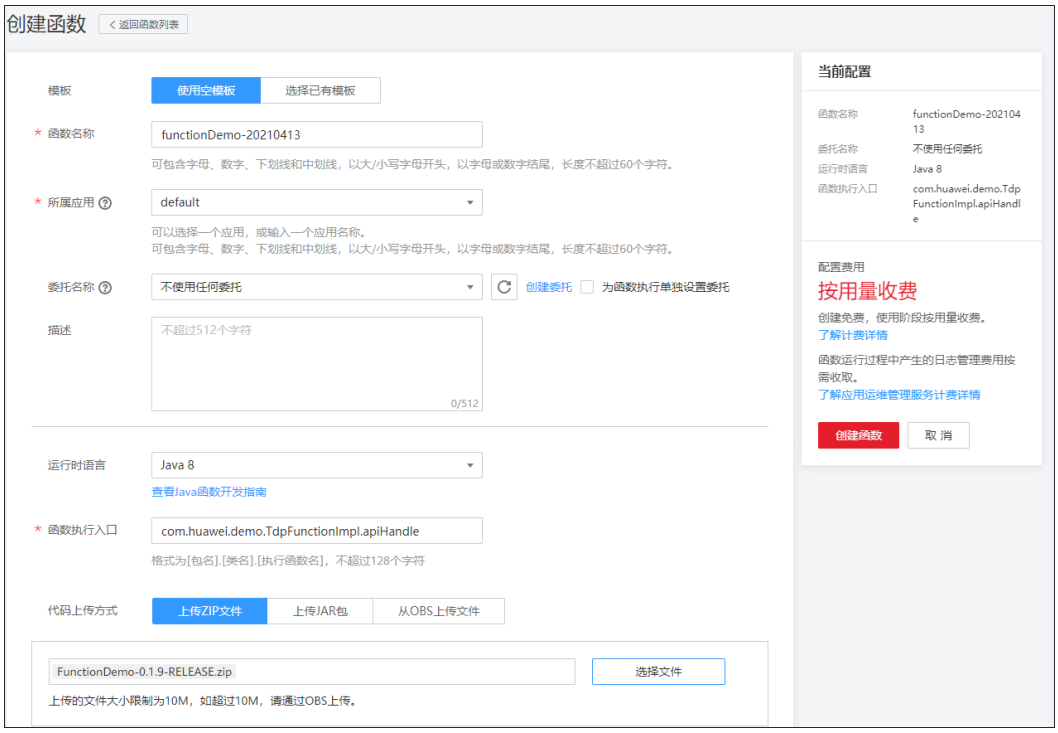
函数打包规范参见**函数工作流 FunctionGraph > 开发指南 > 概述 > 函数工程打包规范**。

如函数工程未使用到第三方库，则可将工程打成一个Jar包上传。如使用到第三方库，则需将工程Jar包和第三方Jar包打包成一个Zip包。

本文使用到了多个第三方库，因此，如下图所示，将工程Jar包和第三方Jar包打包成一个Zip包。



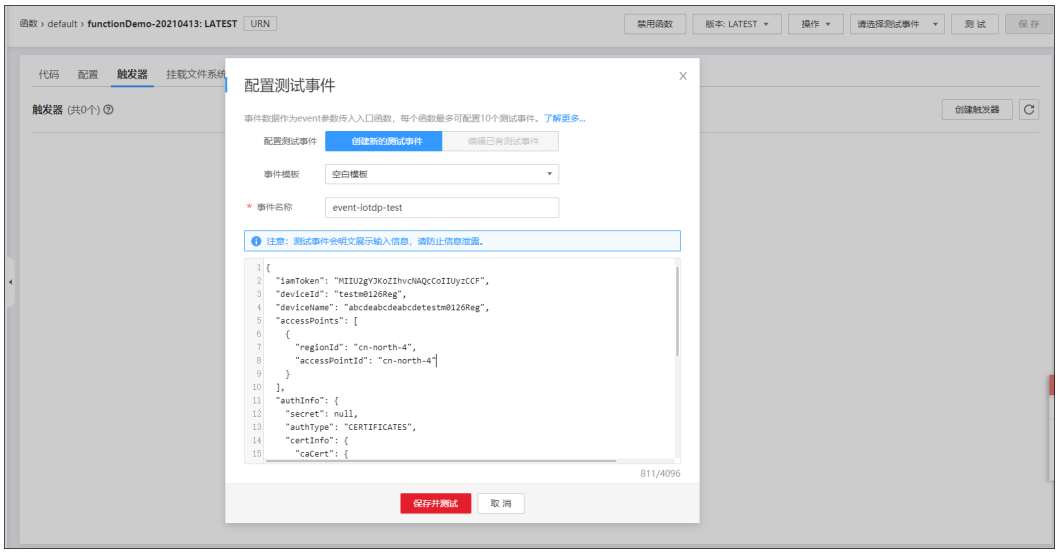
进入函数工作流服务控制台，创建函数并上传包含工程Jar包和第三方Jar包的Zip包。



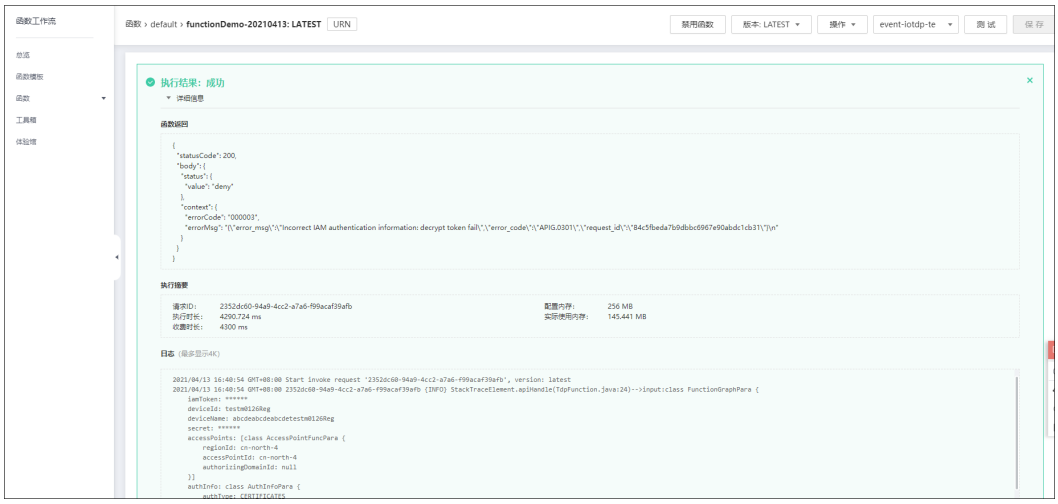
为避免调试过程中函数因内存不足或超时导致调用失败，视实际使用情况调整内存大小和超时时间。

步骤3 配置测试事件，调试函数。

创建测试事件，填写满足设备发放约束的函数参数的JSON格式。



单击“保存并测试”，查看函数运行结果，确认函数逻辑的正确性。



日志显示，已调用了发放设备接口，函数主要逻辑正确。至此，您已完成自定义策略函数的编写，可进行后续步骤。

----结束

后续操作

完成自定义策略函数的编写后，创建关联该函数的自定义策略实例以及设备或注册组，通过设备南向操作触发函数，将设备发放到指定目的接入点（设备接入实例）。

后续操作包括：

- **添加自定义策略实例**；
- **注册设备**或**创建注册组**；
- 南向接口：**MQTT CONNECT连接鉴权**、**设备请求引导消息**、**设备接收引导消息**。

最佳实践：

- 结合函数服务通过自定义策略发放证书认证的设备。

设备发放对返回参数的约束

表 4-1 TdpFuncResult

名称	说明	类型
statusCode	String	函数执行状态码，用于标识函数执行过程是否出现异常，遵循HTTP状态码含义。
body	String	字符串，但格式为JSON，结构为TdpFuncBody。

表 4-2 TdpFuncBody

名称	说明	类型
status	String	设备发放业务功能标识，allow表示发放成功，deny表示发放失败，设备发放使用此标识判断函数内业务功能执行成功与否。
context	TdpFuncBodyContext	扩展字段，用于承载函数执行结果。

表 4-3 TdpFuncBodyContext

名称	说明	类型
allocationResult	String	发放结果，存放发放接口返回的响应结构体。
errorCode	String	错误码，如发放失败，则此值需不为空。
errorMsg	String	错误描述，如发放失败，则此值需不为空。

发放设备成功的返回参数样例

```
{
  "statusCode": 200,
  "body": "{\"status\":\"allow\",\"context\":{\"allocationResult\":\"dps返回的下发结果\"}}"
}
```

发放设备失败的返回参数样例

```
{
  "statusCode": 200,
  "body": "{\"status\":\"deny\",\"context\":{\"errorCode\":\"错误码\",\"errorMsg\":\"错误描述\"}}"
}
```


设备发放对函数参数的约束

表 4-4 FunctionGraphPara

名称	类型	说明
iamToken	String	委托Token，便于用户调用发放接口。
deviceId	String	设备ID。
deviceName	String	设备名称。
accessPoints	List<AccessPointPara>	备选接入点列表。
authInfo	AuthInfoPara	设备认证信息。

表 4-5 AccessPointPara

名称	类型	说明
regionId	String	备选接入点的区域ID。
accessPointId	String	备选接入点的接入点ID。
authorizingDomainId	String	备选接入点的接入点授权租户，仅在授权场景下使用。

表 4-6 AuthInfoPara

名称	类型	说明
authType	String	认证类型。可选 SECRET 和 CERTIFICATES。
secret	String	设备密钥信息，当认证类型为 SECRET 时携带。
certInfo	CertInfoPara	证书信息，当认证类型为 CERTIFICATES 时携带。

表 4-7 CertInfoPara

名称	类型	说明
caCert	CaCertPara	设备CA证书信息。
deviceCert	List<DeviceCertPara>	设备证书信息。

表 4-8 CaCertPara

名称	类型	说明
subjectCnName	String	证书使用者CN NAME。
caCertName	String	证书名。
fingerprint	String	证书指纹。

表 4-9 DeviceCertPara

名称	类型	说明
subjectCnName	String	证书使用者CN NAME。
issuerCnName	String	证书颁发者CN NAME。
sha1Fingerprint	String	证书指纹（使用SHA-1算法计算）。
sha256Fingerprint	String	证书指纹（使用SHA-256算法计算）。

证书认证设备触发函数策略的函数参数样例：

```
{
  "iamToken": "MIIT3gYJKoZIhvcNAQcCoIIT...",
  "deviceId": "testDeviceId",
  "deviceName": "testDeviceName",
  "accessPoints": [
    {
      "regionId": "cn-north-4",
      "accessPointId": "cn-north-4",
      "authorizingDomainId": null
    },
    {
      "regionId": "cn-north-4",
      "accessPointId": "86a45e59-3003-24b8-4e81-df0a9a694639",
      "authorizingDomainId": "84fd2c95ddf03b840f18100a000d45c2"
    }
  ],
  "authInfo": {
    "authType": "CERTIFICATES",
    "certInfo": {
      "caCert": {
        "subjectCnName": "serverCommonName20200922204814",
        "caCertName": "ca20200922204814",
        "fingerprint": "dc0f1016f495157344ac5f1296335cff725ef22f"
      },
      "deviceCert": [
        {
          "subjectCnName": "deviceCommonName20200922204814",
          "issuerCnName": "serverCommonName20200922204814",
          "sha1Fingerprint": "b2217bd882968b0bc15b1c2b132ba8a598f11879",
          "sha256Fingerprint": "734326bb5f3065d8e90d95ce1910b831d3856a1318770768bf9b03923d641ddd"
        }
```

```
    ]
   }
  }
}
```

密钥认证设备触发函数策略的函数参数样例：

```
{
 "iamToken": "MIIT3gYJKoZIhvcNAQcCoIIT...",
 "deviceId": "testDeviceId",
 "deviceName": "testDeviceName",
 "accessPoints": [
  {
   "regionId": "cn-north-4",
   "accessPointId": "cn-north-4",
   "authorizingDomainId": null
  },
  {
   "regionId": "cn-north-4",
   "accessPointId": "86a45e59-3003-24b8-4e81-df0a9a694639",
   "authorizingDomainId": "84fd2c95ddf03b840f18100a000d45c2"
  }
 ],
 "authInfo": {
  "authType": "SECRET",
  "secret": "29ccf3ff01247d731fef"
 }
}
```

4.1.2 添加自定义策略实例

步骤1 进入“策略”界面，单击展开“自定义策略”，单击“添加函数”。

图 4-1 添加自定义策略

步骤2 按照下方参数说明填写关键参数信息后，单击“确定”。

参数名称	说明	示例
函数	即在**函数服务**中实现的自定义策略。如果下拉框没有你想要的函数，可以单击创建新函数来实现你的自定义策略需求。	将需要通过函数“function”发放的设备发放至华北-北京四的物联网平台。 • 需通过函数“function”发放的设备：WaterMeter-Beijing0001、WaterMeter-Beijing0002 • 函数：function • 发放区域：华北-北京四
发放区域	发放到指定区域后，设备将接入对应区域的设备接入服务。 所选区域未开通设备接入服务时，如果确定添加实例，系统将自动为您开通设备接入服务。不同区域设备接入服务价格不同，收费详情请参考价格说明。	

----结束

4.2 证书策略

概述

证书策略，即通过平台认证设备的设备CA证书匹配的发放策略。每条证书策略实例指：匹配上该策略实例的设备，将会被发放到该策略实例关联的设备接入实例的对应资源空间（即应用）下。

设备匹配证书策略实例的机制为：

1. 设备的发放策略指定为“证书策略”时，其认证方式也必须为X.509证书认证且同时指定了认证设备的设备CA证书，当设备关联的设备CA证书与证书策略实例关联的证书为同一个证书时，即被认为该设备匹配上该条策略实例；
2. 一个设备最多匹配一条证书策略实例；一个CA证书最多被一条证书策略关联。

操作步骤

步骤1 进入“策略”界面，单击展开“证书策略”，单击“添加实例”。

图 4-2 添加证书策略

步骤2 按照下方参数说明填写关键参数信息后，单击“确定”。

表 4-10 证书策略参数列表

参数名称	说明	示例
证书名称	即所要根据证书属性将设备发放到指定的目标区域，选择对应的证书。	将需要通过证书“certificates”发放的设备发放至华北-北京四的物联网平台。 ● 需通过证书“certificates”发放的设备：WaterMeter-Beijing0001、WaterMeter-Beijing0002 ● 证书名称：certificates ● 发放区域：华北-北京四 ● 发放应用：beijing-app1
发放区域	发放到指定区域后，设备将接入对应区域的设备接入服务。 所选区域未开通设备接入服务时，如果确定添加实例，系统将自动为您开通设备接入服务。不同区域设备接入服务价格不同，收费详情请参考价格说明。	
发放应用	选择对应设备接入服务区域已创建的应用。在物联网平台中，设备由应用统一管理。 如果对应设备接入服务区域未创建应用，需要前往对应服务创建应用。	

----结束

4.3 静态策略

概述

静态策略，即设备关键字模糊匹配的发放策略。每条静态策略实例指：匹配上该策略实例的设备，将会被发放到该条策略实例关联的设备接入实例的对应资源空间（即应用）下。

设备匹配静态策略实例的机制为：

1. 设备的发放策略为“静态策略”，设备的关键字来源字符串包含某一静态策略实例的关键字，即被认为该设备匹配上该条策略实例。关键字来源有以下两种来源类型：
   a. 设备名称：如果设备名称包含设置的关键字，即可按照该行策略指定的发放应用进行实例发放。
   b. 数据上报：如果设备在连接后，进行发放publish时，上报Topic “$oc/devices/${deviceId}/sys/bootstrap/up” 中，json上报的属性“baseStrategyKeyword” 包含设置的关键字，即可按该实例进行发放。
2. 一个设备最多匹配一条静态策略实例；
3. 当一个设备匹配上多条静态策略实例时，则以优先级最高的策略实例为优先。

操作步骤

步骤1 进入“策略”界面，单击展开“静态策略”，单击“添加实例”。

图 4-3 创建静态策略详情

步骤2 按照下方参数说明填写关键参数信息后，单击“确定”。

表 4-11 静态策略参数列表

参数名称	说明	示例
关键字	即关键字来源中的关键字。设备发放时，如果关键字来源字符串中包含设置的关键字，则可按该实例进行发放。	将设备名称携带Beijing的设备发放至华北-北京四的物联网平台。 • 设备名称：WaterMeter-Beijing0001、WaterMeter-Beijing0002 • 关键字来源：设备名称 • 关键字：Beijing • 发放区域：华北-北京四 • 发放应用：beijing-app1 将上报信息中携带Beijing的设备发放至华北-北京四的物联网平台。 • 关键字来源：数据上报 • topic“$oc/devices/${device_id}/sys/bootstrap/up”上报信息：{ "baseStrategyKeyword": "WaterMeter-Beijing0003"} • 关键字：Beijing • 发放区域：华北-北京四 • 发放应用：beijing-app1
关键字来源	关键字来源指的是用于匹配关键字的字符串信息的数据来源。目前支持设备名称与数据上报两种形式。 如果为设备名称，则匹配关键字的字符串取设备创建后的设备名称。 如果为数据上报，则匹配关键字的字符串取设备发放过程中，发起发放请求Topic“$oc/devices/${device_id}/sys/bootstrap/up” 的上报信息json中的baseStrategyKeyword属性。	
优先级别	发放策略的优先级，取值范围1 - 5级，1级为最低优先级。当一个设备符合多个发放策略时，按照优先级最高的策略实例发放。	
发放区域	发放到指定区域后，设备将接入对应区域的设备接入服务。 所选区域未开通设备接入服务时，如果确定添加实例，系统将自动为您开通设备接入服务。不同区域设备接入服务价格不同，收费详情请参考**价格说明**。	
发放应用	选择对应设备接入服务区域已创建的应用。在物联网平台中，设备由应用统一管理。 如果对应设备接入服务区域未创建应用，需要前往对应服务创建应用。	

----结束

5 设备

5.1 注册设备

注册设备用于将设备基本信息导入设备发放平台中，用于后续发放至不同的物联网平台，支持批量注册和单个注册。设备注册成功后，可在“设备-注册”中查看设备的详细信息。

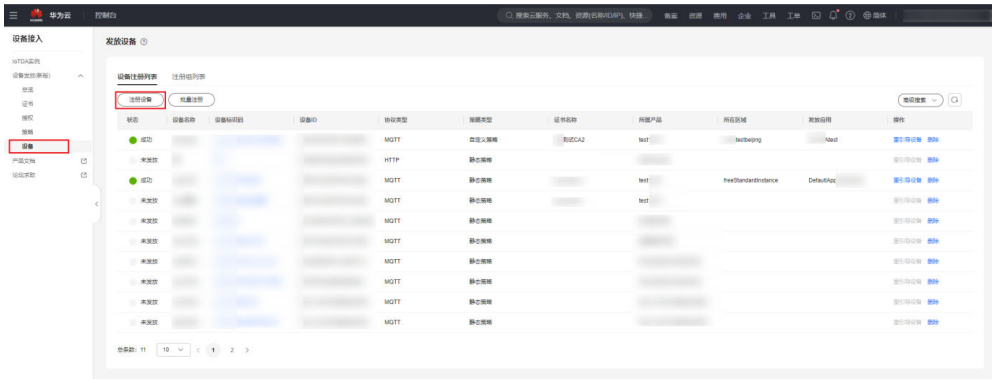
说明

所需“产品”来自 设备接入服务 创建的产品，相关信息参见 **创建产品**。

单个/批量导入

步骤1 进入“设备-注册”界面，单击右上角“注册”或“批量注册”。

图 5-1 注册设备



步骤2 按照下方参数说明填写关键参数信息后，完成注册。

表 5-1 注册设备参数列表

参数名称	说明
产品	选择设备所属的产品名称。 批量导入时，需要填写产品ID。
设备标识码	设备唯一物理标识，如IMEI、MAC地址等，用于设备在接入物联网平台时携带该标识信息完成接入鉴权。
设备名称	设备发放时，设备名称将作为主要的筛选条件之一，建议按照统一的规则规划不同地区的设备名称。 例如：北京地区设备，设备名称都携带Beijing；香港地区设备，设备名称都携带Hongkong。
设备ID	设备ID默认为产品ID+“_”+设备标识码，用户也可自己定义。
发放策略	根据需求选择对应的发放策略类型，注册设备成功后，设备将按照对应的策略进行发放。
导入配置（LwM2M协议设备）	仅在设备使用LwM2M协议时需要填写以下参数： ● 引导服务端PSK：设备初次上电时，与设备发放服务建立DTLS连接，PSK验证通过后进行设备引导。 ● 连接服务端PSK：设备连接设备接入服务、与平台建立DTLS连接时用于验证。 **连接服务端PSK不需要烧录在设备中，设备首次上电后启动BootStrap流程时由平台下发。** ● 安全模式：支持安全模式DTLS/DTLS+和非安全模式。选择DTLS模式或DTLS+模式，设备将通过安全端口5684接入平台，否则将通过非安全端口5683接入。 ● 默认生命周期：设备开机后，如果没有归属物联网平台地址，且在默认生命周期内没有收到设备发放服务下发的地址，则根据注册的设备发放服务地址，向物联网平台发起请求。平台返回连接信息后，设备覆盖本地的注册的物联网平台地址，向指定的物联网平台地址发起注册。默认值为86400秒，最大值（7*86400秒）。
导入配置（MQTT协议设备）	仅在设备使用MQTT协议时需要填写以下参数： ● 安全模式：支持安全模式密钥模式和X.509证书模式。 ● 设备密钥：选择密钥模式时该参数选填，如果不填系统会返回密钥，或从设备详情获取。 ● 选择证书：选择X.509证书模式时该参数必填，选择当前注册设备所需要的证书。 ● 证书指纹：根据证书生成的唯一识别证书的标识。与“自注册开关”参数选填其一或都填。 ● 自注册开关：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。与“证书指纹”参数选填其一或都填。

----结束

MQTT 设备批量发放操作

本文以注册3个MQTT设备，发放到中国站“华北-北京四”为例演示如何发放MQTT设备。

- **前提条件**

  已在中国站“华北-北京四”的设备接入服务中创建应用。

- **操作步骤**

  a. 进入“策略”界面，单击展开“静态策略”，单击“添加实例”。

  b. 按照下方参数说明填写关键参数信息后，单击“确定”。

表 5-2 实例 1-发放到北京

参数名称	说明
关键字	Beijing
优先级别	1级
发放区域	华北-北京四
发放应用	选择在“华北-北京四”的设备接入服务中创建的应用。

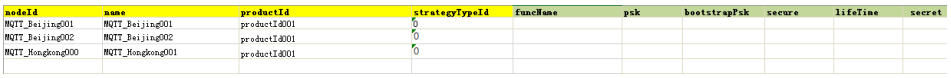
  c. 进入“设备”界面，单击右上角“批量注册”。

  d. 下载模版，按照下方参数说明分别填写三个设备的关键参数信息后，选择模板文件并单击“保存”。

表 5-3 MQTT 设备模板填写说明列表

参数名称	说明
nodeId	若有真实设备，填写为设备的IMEI或MAC地址；若没有真实设备，填写自定义字符串，不同设备的识别码不能重复。
name	分别填写为MQTT_Beijing001，MQTT_Beijing002，MQTT_Beijing003。
productId	填写所要注册的设备所属产品的产品ID。
strategyTypeId	策略类型，填写0（静态策略）。
其他参数	留空。

图 5-2 模板填写样例



nodeId	name	productId	strategyTypeId	funcName	psk	bootstrapPsk	secure	lifeTime	secret
MQTT_Beijing001	MQTT_Beijing001	productId001	0						
MQTT_Beijing002	MQTT_Beijing002	productId001	0						
MQTT_Hongkong000	MQTT_Hongkong001	productId001	0						

e. 在“操作记录”中查看注册结果，注册成功则继续下一步；注册失败则可单击“失败数”所在列的数字查看失败原因，修改模板后重新注册。

f. 设备初次上电，先接入到设备发放平台，随后通过Bootstrap流程引导设备获得目标物联网平台地址，完成设备发放。

LwM2M 设备批量发放操作

本文以注册3个LwM2M设备，发放到中国站“华北-北京四”为例演示如何发放LwM2M设备。

- **前提条件**
  - 已在中国站“华北-北京四”的设备接入服务中创建应用。
  - 获取终端节点。

    表 5-4 终端节点列表

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	5683	LwM2M
华北-北京四	cn-north-4	iot-bs.cn-north-4.myhuaweicloud.com	5684	LwM2M + DTLS

- **操作步骤**

  a. 进入“策略”界面，单击展开“静态策略”，单击“添加实例”。

  b. 按照下方参数说明填写关键参数信息后，单击“确定”。

  表 5-5 实例 1-发放到北京

参数名称	说明
关键字	Beijing
优先级别	1级
发放区域	华北-北京四
发放应用	选择在“华北-北京四”的设备接入服务中创建的应用。

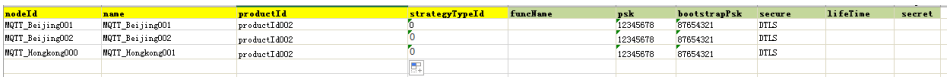
  c. 进入“设备”界面，单击右上角“批量注册”。

  d. 下载模版，按照下方参数说明分别填写三个设备的关键参数信息后，选择模板文件并单击“保存”。

表 5-6 LWM2M 设备模板填写说明列表

参数名称	说明
nodeId	若有真实设备，填写为设备的IMEI或MAC地址；若没有真实设备，填写自定义字符串，不同设备的识别码不能重复。
name	分别填写为LwM2M_Beijing001，LwM2M_Beijing002，LwM2M_Beijing003。
productId	填写所要注册的设备所属产品的产品ID。
strategyTypeId	策略类型，填写0（静态策略）。
psk	可填写为12345678。
bootstrapPsk	可填写为87654321。
secure	填写为DTLS。
其他参数	留空。

图 5-3 模板填写样例



nodeId	name	productId	strategyTypeId	funcName	psk	bootstrapPsk	secure	lifeTime	secret
MQTT_Beijing001	MQTT_Beijing001	productId002	0		12345678	87654321	DTLS		
MQTT_Beijing002	MQTT_Beijing002	productId002	0		12345678	87654321	DTLS		
MQTT_Hongkong000	MQTT_Hongkong001	productId002	0		12345678	87654321	DTLS		

e. 在“操作记录”中查看注册结果，注册成功则继续下一步；注册失败则可单击“失败数”所在列的数字查看失败原因，修改模板后重新注册。

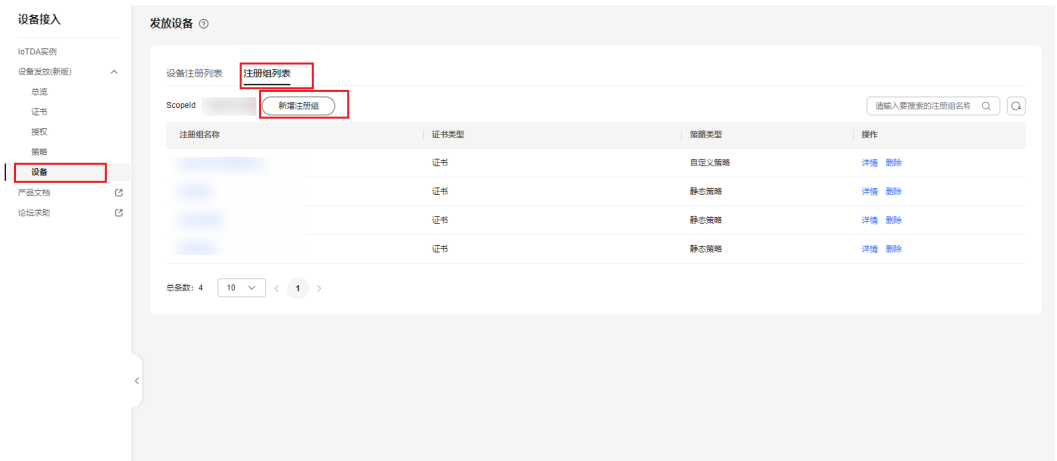
f. 设备初次上电，先接入到设备发放平台，随后通过Bootstrap流程引导设备获得目标物联网平台地址，完成设备发放。

5.2 注册组

MQTT证书接入的设备，可以在设备发放创建一个注册组，绑定对应的CA证书和自定义策略，可以实现批量设备的自注册，实现设备一键上电即可上云的动作，可在注册组详情中查看该注册组下所有的设备。

步骤1 进入“设备-注册组列表”界面，单击左上角“新增注册组”。

图 5-4 新增注册组



步骤2 按照下方参数说明填写关键参数信息后，完成创建。

表 5-7 注册组关键参数列表

参数名称	说明
注册组名称	注册组的唯一标识。
选择证书	用于和注册组绑定，同一个证书只能同时绑定一个注册组，不能同时绑定多个注册组。
发放策略	当前只支持“自定义策略”，同时需要选择所要运行的函数。

----结束

