# 设备发放

# 用户指南

文档版本02发布日期2022-04-24





#### 版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

#### 商标声明

#### 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	1
2 证书	3
2.1 制作 CA 证书	5
2.2 上传 CA 证书	6
2.3 验证 CA 证书	7
2.4 签发设备证书	9
2.5 更新 CA 证书	10
2.6 删除 CA 证书	10
3 授权	
4 策略	
<b>4 策略</b> 4.1 自定义策略	<b>14</b> 
<b>4 策略</b>	<b>14</b> 
<b>4 策略</b> 4.1 自定义策略	<b>14</b> 
<b>4 策略</b>	<b>14</b> 
4 策略	<b>14</b> 14 14 22 23 23 24
4 策略	<b>14</b> 14 14 22 23 23 24 <b>27</b>
4 策略	<b>14</b> 14 14 14 22 23 23 24 <b>27</b>





#### 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。
	<ul> <li>LiteOS设备(LWM2M),设备需要具有设备反放功能。</li> <li>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。</li> </ul>
	<b>注:</b> 若设备需要使用物联网卡,可在 <mark>全球SIM联接</mark> 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。 <b>设备发</b> 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. <mark>证书</mark> :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. <b>策略</b> :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. <mark>设备</mark> :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。

# <mark>2</mark> <sub>证书</sub>

## 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。



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	-	

制作CA证书 上传CA证书 验证CA证书 签发设备证书 更新CA证书

删除CA证书

# 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

#### 🛄 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<mark>表1</mark> 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.		

步骤4 使用密钥对生成证书签名请求文件:

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

设备接入		证书列表 ①			
loTDA实例 设备发放(新版)	~	LINCALEN			
证书		验证状态 征书名称	证书使用者	证书部以来	过期状态
授权		~ BRE			可用
策略 设备		~ ENE			利用
产品文档	C	✓ #验证			司用
论组末期	C	→ 未始征			司用
		✓ B8€			初用
		✓ BRE			可用
		✓ E8€			
		意発数:7 10 ~ (1)			

**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

设备接入	证书列表 ⑦		
IoTDA实例 设备发放(新版)	上传CA证书	上传CA证书	
证书	验证状态 证书	* CA证书名称 神	到期时间
授权	✓ 日絵運	* CA证书 ③ 点击右侧按钮添加文件 汤加文件 周	2161/07/28 11:2
策略	→ 已验证	取済の構成	2161/01/12 19:
产品文档	2 ~ 未验证	"Я	2123/09/24 15:0
论坛求助	3 ~ 未验证	可用	2123/09/03 14:

#### ----结束

#### 🛄 说明

上传的CA证书初始状态为"未验证",需要完成"<mark>验证CA证书</mark>"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

设备接入		♥ CA证书上传成功								
IoTDA案例		证书列表 ①								
设备发放(制版) 总派	^	LICALE#	)				法输入要投资	的证书名称	٩	0
1215 15亿		检证状态	证书名称	证书使用者	证书跟发表	过期状态	到期时间	现作		
策略 设备		~ 未設证	文档表试证书	conname	CN=conname, OU=cqursd, O=cvvve, L=qurf, ST=zouxtst, C=CN	司用	2161/07/20 19:08:51 GMT+08:00	更新 動	in Inga	i#i
产品文档	C	~ BRE				可用	2161/07/28 11:28:23 GMT+08:00	更新意	<b>19</b> 1922	H
010101088	12						ALC: 10 10 10 10 10 10 10 10 10 10	-		

**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

设备接入		🕑 CAIE书上传成功								>
IoTDA案例		证书列表 ①		上传验证证	正书		×			
88 88		LI@CAIE#	1	*脸证明	07b0 145e5	đ			请编入要按定	BERSK Q Q
授权		验证状态	证书名称	* 12EE#	综击右侧按图英加文件	(1830文/#		过期状态	到期时间	證件
策略 设备		◇ 未設证	文档则试证书				ARE .	可用	2161/07/20 19:08:51 GMT+08:00	<b>RA: 89</b> 8225
产品文档	C	✓ 已給证						可用	2161/07/28 11:28:23 GMT+08:00	<b>EN BON</b> BREES
论纸求助	C	✓ B## 8						可用	2161/01/12 19:28:57 GMT+08:00	<b>EM 800</b> 10225

#### 🛄 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"<mark>制作CA证书</mark>"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

设备接入	0	CA证书上传成功								
IoTDA实例 设备发放(南版)	ü	正书列表 ①		上传验证证	ĒĦ		×			
<sup>田元</sup> (1745		LINCALE#	)	* 脸证符	07b049365221de536c87b69b22a145e5	ď			清能入要搜加	REFERE Q
授权		输证状态	证书名称	* 1225	verificationCert.crt (1.22KB)	× (通加文件 )		过期状态	Sector Sector	理作
策略		~ 未設定	文档则试证书	L				可用	2161/07/20 19:08:51 GMT+08:00	<b>则新 劉玲 松正正书</b>
产品文档	c	~ BRE						可用	2161/07/28 11:28:23 GMT+08:00	<b>24 80 1</b> 0328
论结正常用的	C	✓ E82							2161/01/12 19:28:57 GMT+08:00	

----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<mark>表</mark>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
---------	-------	-----

ARR	THICKEN						INARESOLUTION Q
2.11. E#1	NUKO	<u>ii 1920</u>	<u>1</u> 79/10	สารสะ	1289425	SOUTH	R6
82	~ 682				-	21610728 112823 GMT-98.00	<b>RB 89</b> 1022-5
08 08	~ 082				15.11	216101/12 18 28 57 GMT+08.00	RP BO SERV
28 C	→ #85E				28	2123/09/24 15 02 12 GMT+00:00	MM 800 1223-6
50 (K	~ *#cZ				11.11	2123/09/03 14 56 37 GMT+08 00	## ### 1052-#
	✓ Bk∉					216011111 21:27:38 GM7+08:00	Re die inizien
	✓ Ettiz				1211	2159/07/01 22:59:35 GMT+08:00	R# 809 10221
	~ eng					2159/05/06 17:38:07 OMT+08:00	R8 80 1023

📋 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

设备接入		₩#Ħ₩表 ⊙						
NTOADH RH3355500	•	Tacyže						
10		89348	臣书名称	证书影响和	近49802 <b>位</b>	対要核応	2020KR	12/1
202		✓ Bbd.				<b>R</b> 28	216107/381126/23 GMT+88:00	<b>200</b> 00000
29		✓ DBE				যান	2161/01/12 19:28:57 GMT+08:00	RN BH BEEK
产品文档	в	- #80Z				यत	2123/09/24 15 82 12 OMT+08 80	RM 894 10224
论记录数	C	✓ #820				10	2123/09/03 14:55:37 GMT+08:00	RN 899 10224
		✓ BNE				বাৰ	2160/11/11 21:27:38 GMT+08:08	<b>RH 89</b> 1022-0
		✓ BNZ				मन	2159/07/01 22:59:35 OMT+08:00	Mar ada kolizira
		× 086				- <b>ব</b> ৰ	2159/05/08 17:38:07 GMT+08:00	28 29 20224
		888:7 <u>11 v</u>	] < <b>1</b> >					

## 🛄 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** <sub>授权</sub>

## 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"。

设备接入		授权关系						
ioTDA案例 设備发放(新版) 位述 征书	^	被撥权列表 ③ 接权列表 发起毁权请求	•					٩
捕捉		ID	秋志	接权相户	创建时间	描述	操作	
策略								
设备								
产品文档	C				<1.7			
论证书的	C			HE THE REPORT OF				

#### 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

设备接入	授权关系		
loTDA实例 设备发放(新版) へ 思定	★ 通報初期表 ⑦ 振行列表 ⑦	<b>发起授权请求</b> × 我们所有 <b>第552時</b> 所有10	
近形	355 CI	* 预号备称	損送 現作
策略 设备		* 1127 (RR:261127)	
产品文档 C 论版求助 C		描述	
		0/490 %	
	<		

- 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。
- 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

投权关系						
<b>1000712 ()</b> 100712 ()						
TRINGER						Q
10	uz.	2007000	0189344	1971 E	1017	
dc5 Ve189d	BR		2022/04/26 11:25:11 GMT+08:00		809	
840 194261	E85		2024/09/23 17:19:28 GMT+06.00		804	

#### 图 3-4 授权方禁用或删除授权关系

18191070 () <b>181070 ()</b>						
						Q
10	KE.	6236678D/1	202200	51.15	50 S	
372 :209	<ul> <li>Exist</li> </ul>		2823/11/28 22:43:44 GMT=88.00		MA Bik	
606 35a0d	E84		2023/11/28 10:28:14 GMT-08:00		MAT BOX	
84a 4291	e er		2824/08/23 17:19:28 GMT+08:00		870 B94	



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:

- 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<mark>函数Demo</mark>,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!!!
* 
* {@code
    @Override
    public TdpFuncResult apiHandle(FunctionGraphPara para, Context context) {
      return super.apiHandle(para, context);
    }
* }
* 
*/
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。

To	pFunctionDemo-1.0.0-RELEASE.zip		当前目录查找(支持包内查找)	Q、高级
<	* 名称			
^	(上层目录)			
	🕌 annotations-13.0.jar			17
	🕌 converter-jackson-2.9.0.jar			3
	🛃 jackson-annotations-2.10.0.jar			66
	🕌 jackson-core-2.10.0.jar			340
	🛃 jackson-databind-2.10.0.jar			1.
	🕌 kotlin-stdlib-1.3.50.jar			1.
	🕌 kotlin-stdlib-common-1.3.50.jar			166
	🕌 okhttp-4.2.2.jar			693
	🍰 okio-2.2.2.jar			1
	🔬 retrofit-2.9.0.jar	_		122
	ldp-function-demo-1.0.0-RELEASE.jar			50
	🔬 validation-api-2.0.1.Final.jar			90

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。

模板	使用空模板 选择已有模板	日則配直	
* 函数名称 * 所属应用 <b>②</b>	functionDemo-20210413       可包含字母、数字、下划线和中划线,以大/小写字母开头,以字母或数字结尾,长度不超过60个字符。       default       可以选择一个应用,或输入一个应用名称。	函数名称 委托名称 运行时语言 函数执行入口	functionDemo-20210 13 不使用任何委托 Java 8 com.huawei.demo.Td FunctionImpl.apiHanc e
	可包含字母、数字、下划线和中划线,以大/小写字母开头,以字母或数字结尾,长度不超过60个字符。	配置费用	
委托名称 🕜	▼ C 创建委托 → 対函数执行单独设置委托	按用量收费	
描述	不超过512个字符 0/512	回建光费,便用附借 了解计费详情 函数运行过程中产。 需收取。 了解应用运维管理题	x1xr11里似费。 主的日志管理费用按 服务计费详情
法行时语言	lava 8	创建函数	取消
	查看Java函数开发指南		
• 函数执行入口	com.huawei.demo.TdpFunctionImpl.apiHandle		
	格式为[包名].[关名].[执行函数名], 不趨过128个字符		
代码上传方式	上传ZIP文件 上传JAR包 从OBS上传文件		

# 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。

函数工作流 	函数 > default > functionDer	10-20210413: LATEST URN	開田協致
忠況 函数模板	代码 配置 触发的	着 挂载文件系统 函数指标 日志 别名配置	
6款 *	描述	不超过512个字符	
工具相			
体验增		0/512	
	委托名称 🕥	不使用任何乘托 · C 创建实托	数执行单独设置委托
	内存 (MB)	128 <b>256</b> 512 768 1024 1280 1536 1792 2048 2560	3072 3584 4096
	* 执行题时时间 (秒) ⑦	300	
	VPC访问 🕜	需要始函数配置拥有VPC管理权限的委托。了解更多	
	环境变量 ③	() 注意:环境变量会明文展示所输入信息, 游注意不要直接输入敏感信息,以助泄露。	
		stat dat	<b>接册</b> 个性
		()	0
			•
		質无敗還,還加配置标签	ß

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。

函数 > default > functionDemo-20210413: LATES	T URN	幕用函数   版本: LATEST ▼ 操作 ▼ 満造達測試事件 ▼ 刻 试 保存
(代码 配置 触发器 挂蛇文件系统 触发器(共0个)②	CETHING : Constraints : Con	X () () () () () () () () () ()

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。

函数工作流	國	総 > default > functionDemo-20210413: LATEST URN 版本: LATEST V 現作 V event-iotdp-te V 園話 保存
<i>1015</i>		
函数模板		۵ المجنوب المالي ال المالي المالي
函数 マ		* (2018)
工具相		3.9%EP
体验物		{     "fabaciced": 200,     "body 1 {         "statuciced": 200,         "body 1 {         "statuciced": 200,         "body 1 {         "statuciced": 200,         "statuciced": 200,         "statuciced: 200,         "statucice
		<b>执行接</b> 着
		(第次): 2353dx04944x42x36x8838x8b< 第255.00 第 第255.00 第 第255.00 第 第255.00 m):
		<b>日本</b> (現520万44)
		2012/AUI 10:056 070400 % User lower reads: "JISSOB 940-4c2-bit-PBacr3980", version leter 2012/AUI 10:056 070400 % 2016-984-94-c2-bit-PBacr3980", version leter lation: ***** encluit: testissing encluit: testissing encret: ***** encould: testissing encret: ***** encould: testissing encret: ***** encould: testissing encret: ***** encould: testissing encould: testissing enco

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
statusC ode	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	TdpFuncB odyContex t	扩展字段,用于承载函数执行结果。

#### 表 4-3 TdpFuncBodyContext

名称	说明	类型
allocati onResu lt	String	发放结果,存放发放接口返回的响应结构体。
errorCo de	String	错误码,如发放失败,则此值需不为空。
errorM sg	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 <accesspo intPara&gt;</accesspo 	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。
authorizingD omainId	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 <devicece rtPara&gt;</devicece 	设备证书信息。

#### 表 4-8 CaCertPara

名称	类型	说明
subjectCnNa me	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
subjectCnNa me	String	证书使用者CN NAME。
issuerCnNam e	String	证书颁发者CN NAME。
sha1Fingerpr int	String	证书指纹(使用SHA-1算法计算)。
sha256Finger print	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": "MIIT3gYJKoZlhvcNAQcColIT...",
 "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"
     }
```



# 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

设备接入		设备发放策略 ③				
IoTDA实例 设备发放(新版)	~	说婚名称	加朗拉印刷			
息逸 征书		> 自定义策略	遭过困数服务实现的自定义策略,快速实现个性化设备3	政策业务资程。		
授权 <b>策路</b>		(RIDEN)				( <b>a</b> )
(2 <b>9</b>		函数名称	播权相户	发放区域	證作	
产品文档	C				<b>B</b> SDe	
论短求数	C				mte	

**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 <mark>函数服务</mark> 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 言四的物联网亚公
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。	<ul> <li>第四时初联网平台。</li> <li>需通过函数 "function"发放 的设备: WaterMeter- Beijing0001、 WaterMeter- Beijing0002</li> <li>函数: function</li> <li>发放区域:华北- 北京四</li> </ul>

----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:

- 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

设备接入		设备发放策略 ①					
ioTDA安例 设備发放(新板) 忠茂 证书	^	<ul> <li>業務名称</li> <li>         一 回至父祭時              ・ 正式公開時      </li> </ul>	開築説明 通过回動現外交流的自己文策時、快速交流个性化必要 地点に工業中に必須要やた時でからに下せ、万度点素	·发放业务/所理。 			
一 建整 设备 产品文档 论伝求的	C	ス 単しのMM 液防気(作) 延行的な(作)	1999年1997年1999年1999年1999年1999年1999年1999	RMEM	视放应用	操作	0
			统关键字符也符合条件的设备。发放多端在的目标区域	1. 可領接需要配置多个实例。		209	

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
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。	<ul> <li>的设备反放主华北- 北京四的物联网平 台。</li> <li>需通过证书 "certificates"发 放的设备: WaterMeter-</li> </ul>
	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。	<ul> <li>Beijing0001、</li> <li>WaterMeter-</li> <li>Beijing0002</li> <li>证书名称:</li> <li>certificates</li> <li>发放区域:华北-</li> <li>北京四</li> <li>发放应用:</li> <li>beijing-app1</li> </ul>

----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:

- 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

AD例				at the state (s)		<		
发放(新版)	^	策略名称		添加关闭				
.远		> 自定义策略		* 关键字	静态策略-设备名称中包含的一部分字符串	1		
9 2		◇ 迂舌策略			如果设备名称包含设置的关键字,即可按该实例进行发放。如果设备名称不包含设置的关键字,建议 参改设备名称。			
8		へ 静态策略		★ 优先级别	100 2x02 3x02 4x02 5x02 ①			
4 75	C	( MADERN		接权租户	本部分 排环场			(a
lo I	2	关键字	伏元	* 252%	×	放应用	操作	
			4段	★ 发放应用	× Q	and the second s	899	
			2级			and the second sec	809	
			152		nun vals	1000	809	
			162		北第4		899	
			1段		北京4		859	
			1级		freeStandardInstance		859	
			115		5784		804	

**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。
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。	<ul> <li>设备名称: WaterMeter- Beijing0001、 WaterMeter- Beijing0002</li> <li>关键字来源:设备名称</li> <li>关键字:Beijing</li> <li>发放区域:华北-北京四</li> <li>发放应用:beijing- ann1</li> </ul>
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。	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。
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 <mark>价格说明</mark> 。	<ul> <li>大键子米源: 数据上报</li> <li>topic "\$oc/devices/\$ {device_id}/sys/ bootstrap/up"上报信 息: { "baseStrategyKeywor d": "WaterMeter-</li> </ul>
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。	Beijing0003"} • 关键字: Beijing • 发放区域: 华北-北京四 • 发放应用: beijing- app1

----结束

# **5** 设备

注册设备

注册组

# 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。

门 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"。

λ		发放设备 ①										
門 (新祥)	~	设备注册列表	注册电列表									
		(1100 R										
		秋市	0880 0860	es in	810	协议类型	短期末型	证书名称	所聞戶品	所在医域	发放后用	即作
	1	<ul> <li>EX3)</li> </ul>				MQTT	自定义策略	RigiCA2	test	testbeijing	40012	
ŝ	C	*22				HTTP	静态策略					113/17/24 BM
	C	🔴 ನಮ				MQTT	静态策略		test	heeStandardInstance	DefaultApp	第3:90年 894
		****				MQTT	静态策略		test			101000 BD4
		未发放				MOTT	静态策略					BIGGS BM
		*322				MOTT	静态策略					9510-08 <b>95</b> 4
		*22				MQTT	静态策略					91969 <b>90</b>
		*22				MQTT	静态策略					23:9-29 <b>20</b>
		未发放				MOTT	静态振荡					21929 BM
		#365				MOTT	静态策略					25928 23

#### **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	仅在设备使用LwM2M协议时需要填写以下参数:					
议设备)	<ul> <li>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。</li> </ul>					
	<ul> <li>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。</li> <li>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。</li> </ul>					
	<ul> <li>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。</li> </ul>					
	<ul> <li>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)。</li> </ul>					
导入配置(MQTT协	仅在设备使用MQTT协议时需要填写以下参数:					
议设备)	● 安全模式:支持安全模式密钥模式和X.509证书模式。					
	<ul> <li>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。</li> </ul>					
	<ul> <li>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。</li> </ul>					
	<ul> <li>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。</li> </ul>					
	<ul> <li>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。</li> </ul>					

----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"。

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。

**表 5-2** 实例 1-发放到北京

- 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
nodeld	若有真实设备,填写为设备的IMEl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	nane	productId	strategyTypeId	funcName	psk	bootstrapPsk	secure	lifeTine	secret
MQTT_Beijing001	NQTT_Beijing001	productId001	0						
MQTT_Beijing002	MQTT_Beijing002	productId001	0						
NQTT_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.co m	5683	LwM2M
华北-北 京四	cn- north-4	iot-bs.cn- north-4.myhuaweicloud.co m	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"。

#### 5 设备

#### 表 5-6 LWM2M 设备模板填写说明列表

参数名称	说明
nodeld	若有真实设备,填写为设备的IMEl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	nane	productId	strategyTypeId	funcNane	psk	bootstrapPsk	secure	lifeTime	secret
NQTT_Beijing001	MQTT_Beijing001	productId002	0		12345678	87654321	BTLS		
MQTT_Beijing002	NQTT_Beijing002	productId002	0		12345678	87654321	DTLS		
NQTT_Hongkong000	NQTT_Hongkong001	productId002	0		12345678	87654321	DTLS		
		Ē	<b>.</b>						

- 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

设备接入	发放	女设备 ⑦			
loTDA实例 设备发放(新版) / 总流 证书		设备注册列表 <b>注册组列表</b> Scopeld 新审注册组			(清輸入要推測的注册組名称 Q) Q
援权		注册组名称	证书类型	策路类型	操作
策略			证书	自定义策略	洋街 勤除
产品文档	2		证书	静态策略	洋橋 勤除
论坛求助	2		证书	静态策略	洋情 删除
	总条数: •		证书	静态策略	洋情 删除
		总条款:4 10 ~ < 1 >			
	×				

#### 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