设备发放

快速入门

文档版本05发布日期2024-10-25





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 使用前必读	1
2 设备安全认证	3
3 接口说明	6
3.1 MQTT CONNECT 连接鉴权	6
3.2 设备请求引导消息	8
3.3 设备接收引导信息	
4 MQTT 场景使用 MQTT.fx 接入设备发放示例	10
4.1 MQTT 密钥设备使用静态策略发放示例	
4.2 MQTT X.509 证书认证设备使用证书策略发放示例	
4.3 MQTT 注册组自定义策略发放示例	26
4.4 MQTT 华为云 X.509 证书认证设备使用证书策略发放示例	
4.5 MQTT 华为云证书注册组发放示例	
4.6 MQTT 注册组静态策略发放示例	
4.7 MQTT 注册组密钥认证静态策略发放示例	
4.8 MQTT 密钥设备跨账号使用静态策略发放示例	
5 MQTT 场景使用华为 SDK 接入设备发放示例	75
5.1 MQTT 密钥设备使用静态策略发放	75
5.2 MQTT 注册组静态策略发放示例	

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

Торіс	消息发 送方 (Pub lisher)	消息接 收方 (Subs criber)	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。





双向证书认证过程中使用到了如下几类证书:

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 使用该服务端 书验证服务端 书,通常为权 证书,获取方 MQTT CONN 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。



MQTT CONNECT连接鉴权 设备请求引导消息 设备接收引导信息

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<mark>huaweicloud-iot-root-ca-list</mark>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
----	-----------	----	------

-			•
clien	必选	String(注册组选择非华为云证书场景:
tld		256)	设备clientld由3个部分组成:设备ID、设备身份标识类 型、用户标识ID(ScopelD)。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clientld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
User nam e	必选	String(256)	设备ID。
Pass word	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: ScopelD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 Scopeld

设备接入		发放设备 ①			
loTDA変例 设备发放(新版) 总成 证书	^	公報注任何対策 12 19 1			
接权		注册组名称	证书类型	预建类型	操作
0.6			还书	普度文描略	1718 859
产量文档	C		证书	静态施地	1710 859
论结束物	C		还16	静态策略	1712 879
			还有	静态策略	993 BS9
		BBB:4 [10 ∨] < [1] >			

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<mark>参数生成工具</mark>,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

Торіс	<pre>\$oc/devices/{device_id}/sys/bootstrap/up</pre>	
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

Торіс	<pre>\$oc/devices/{device_id}/sys/bootstrap/down</pre>		
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

MQTT 密钥设备使用静态策略发放示例 MQTT X.509证书认证设备使用证书策略发放示例 MQTT 注册组自定义策略发放示例 MQTT 华为云X.509证书认证设备使用证书策略发放示例 MQTT 华为云证书注册组发放示例 MQTT 注册组静态策略发放示例 MQTT 注册组密钥认证静态策略发放示例

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

📃 🌺 华为云	控制台			Q. 搜索云服务、文档、资	I際(名称/ID/IP)、快捷备	案 资源 费用 企业		. ⊾ (° ⊕ 166≉	
设备接入	iQi	备发放策略 ③							
IoTDA实例									
(香发放(新坂) ノ	^	菜膳名件	菜釀说明						
证书		◇ 自定文策略	通过函数服务实现的	自定义策略,快速实现个性化设备发放业务流	9.				
接权		◇ 征书鏡略	根描述书篇性终设备	发放到描述的目标区域,可模描篇要配置多个	定例 .				
策略		へ 静态策略	按关键字筛远符合条	件的设备,发放到描空的目标区域,可根据要	要配置多个实例。				
·品文档	8	(ALCEN)							
	<	关键字	优先级别	腰权佃户	发放区域	双放后	細	III作	
			4级					数据金	
			2级					#site	
			162					259	
			162					899	
			162					819	
			162					859	
			162					254	

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

ŧλ	发放设备 ①										
2月 2(奈旺) へ	设备注册列表	注册电列表	E.								
	200		D								
	秋市	设备名称	设备标识的	記録の	协议类型	服務末型	延带名称	新聞产品	所在医域	和放在用	提作
	 1270 				MOTT	自定义策略	RIECA2	hest	testbeijing	4dest	第1月1日 新林
C	*25				HTTP	静态描绘					103/10 (21 BP+
C	😑 stiti				MQTT	静态策略		test	heeStandardInstance	DefaultApp	量引导设备 肥料
	< ****				MQTT	静态描述		test			10.000 M
	*35				MQTT	静态接缩					BIGGS BA
	*33				MOTT	静态策略					-
	*33				MOTT	静态策略					233968 20
	*33				MQTT	静力振荡					2317129 231
	未发力				MQTT	静态策略					25989 BH
	#30				MOTT	静态策略					25/9/28 23

图 4-4 创建密钥模式静态策略设备

三 🌺 华为	R 控制台			新嘉 资源	费用 企业		⑦ ● 简体	
く 注册设备								
设备注册信息	(
	18611233	10/0/10						
* 产品	产品名称 test1233		产品の	64	l06bd			
	设备类型 同机		协议类型	MQTT				
设备标识	DesumentTert							
- 76	and an intervention of the second sec							
+ 0925	DocumentTestDevice							
- Caller	设备发放时,设备名称作为主要的算远条件之一,语正确编写,也可	可创建后在设备仓库中修改。						
★ 设备ID	6467 /6bd_DocumentTest							
创建设备配置								
安全模式	810月403C X 509迁书							
设备密明	设备与发放服务以及IoT平台建立MQTT链接时用于检证							
* 策略类型	静态策略							
初始设备配置	DIRE 575 /							
	860(303 m)							
								ROM

🛄 说明

此处注册设备的设备名称需与<mark>添加静态策略</mark>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。

- 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。

Edit Connection Profiles			- • •
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	200000000000000000000000000000000000000	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Connection Timeout	30	
	Keep Alive Interval	60	
	Clean Session	✓	
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	✓ Use Default	
		3.1.1	

4. 填写 User Credentials 信息。

Edit Connection Profiles			- • •
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	*************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password	•••••	

🛄 说明

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

 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。

Edit Connection Profiles		×
M2M Eclipse		
local mosquitto	Profile Name local mosquitto	
	Profile Type MQTT Broker	
	MQTT Broker Profile Settings	
	Broker Address iot-bs.cn-north-4.myhuaweicloud.com]
	Broker Port 8883	
	Client ID Client ID	Generate
	General User Credentials SSL/TLS Proxy LWT	
	Enable SSL/TLS 🗸 Protocol TLSv1.2	•
	CA signed server certificate	
	CA certificate file	
	CA Certificate File	
	CA certificate keystore	
	Self signed certificates	
	 Self signed certificates in keystores 	

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。

🥶 MQTT.fx - 1.7.0		
File Extras Help		
local mosquitto	Connect Disconnect	
Publish Subscribe	Scripts Broker Status Log	
Switch Fountain ON	> home/garden/fountain	Reta. 😋
Switch Fountain OFF		

引导消息订阅

按照<mark>设备接收引导信息</mark>topic填写对应的topic,单击"Subscribe"进行订阅。订阅成功 如下所示:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS1 QoS1 QoS2	Autoscroll 08-
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1
Dump Messages Mute Unsubscribe		Qusu

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。

Publish Subscribe Scripts Broker Status I	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS 1 QoS 2 Autoscrol	.
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0
Topics Collector (0) Scan Stop CC+		
	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down</pre>	1
	28-02-202015:07:01:54421329 {"address":"iot-acc.cn-north-5.myhuaweicloud.com:8883","dnsFlag":0}	QoS 0

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loTDA所需的** 必要信息】预置到了loTDA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loTDA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 loTDA>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loTDA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<mark>表1</mark> 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

门 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

0.元 征书	-	給证状态	证书名称	证书使用表	证书部段者	过期状态
992	-	~ 882				可用
210 210		~ 882				利用
1278	C	✓ 未設正				可用
末和	C	✓ 未检证				可用
		~ 886				可用
		✓ BNZ				可用
		✓ E8€				

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

设备接入		♥ CA证书上传成功						
loTDA实例		证书列表 ③						
(史聲发放(刺版) 总第	^	L(#CALE#)				请输入要按	第80征书名称 Q)
征书								
10日18 1月17日		检证状态	证书名称	证书使用者	证书颁发者	过期状态	到期时间	現作
延书 授权 策略 设备		始証状态 ~ 未放证	征书名称 文档则试证书	证书使用者 conname	证书稿录音 CN=conname, OU=cqursd, O=cvive, L=qurt, ST=zouxhit, C=CN	过期状态	2161/07/20 19:08:51 GMT+08:00	操作 更新 勤除 验证证
 任书 授权 策略 设备 产品文档 	c	始近秋の ~ 本設近 ~ 日始近	证书名称 文档则试证书	证书使用者 conname	延生物源安排 CNicconname, OUroperd, Onovee, Lingert, STinzburtst, CinCN	 过期状态 可用 可用 	5(#85%) 2161(07/20 19:08:51 GMT+08:00 2161(07/28 11:28:23 GMT+08:00	100年 東新 100年 18日2日 東新 100年 18日日

图 4-7 复制验证码

设备接入		🕑 CAIE书上传成功								
IoTDA实例		证书列表 ①		上传验证证	正书		×			
(1) 日泊 (近市)		上传CA证书)	* 脸证明	07b0 145e5	D'			请输入要按定	NEBSR Q
授权		验证状态	证书名称	* 脸还还带	综击右侧按图英加文件	(液如文件)		过期状态	到期时间	ISH:
策略		✓ 未設正	文档则试证书				确定	可用	2161/07/20 19:08:51 GMT+08:00	R# ## 8225
产品文档	C	~ 日始注						可用	2161/07/28 11:28:23 GMT+08:00	JEST BOX INCIDENT
论坛求助	ß	~ BRE						可用	2161/01/12 19:28:57 GMT+08:00	

 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

设备接入		🕑 CA证书上传成功								
IoTDA实例		证书列表 ③		上传验证证	E#		×			
(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(^	LitecalEts)	* 检证码	07b049365221de536c87b69b22a145e5	o			清榆入要搜约	1910-1948 Q
授权		输证状态	证书名称	* 18225	verificationCert.crt (1.22KB)	× 滴加文件		过期状态	100000	操作
策略		✓ 未验证	文册则式证书	L				可用	2161/07/20 19:08:51 GMT+08:00	
设备 产品文档	C	~ Bite				ROM	-	गम	2161/07/28 11:28:23 GMT+08:00	EM 200 10323
论结束物	C	~ Elez		-					2161/01/12 19:28:57 GMT+08:00	-

----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<mark>表</mark>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loTDA,并且由此CA签发的设备证书都会发放到 指定的loTDA。

图 4-9 添加证书策略

设备接入		设备发放策略 ③					
loTDA实例 设备发放(新板) 台店	^	输送的	策略说明				
证书 授权		・ 自定义质略 ・ 正形策略	通过回数服务实现的自定义策略,快速实现个性/ 根据证书属性将设备发放到描述的目标区域,可作	8役聲发放业务流程。 9据需要配置多个实例。			
除器 设备		182050					
产品文档	C	证书名称	质权能产	发展区域	发放应用	提作: 1939年	
		が最数:1 10 ~ < 1 >					
		→ 静态策略	接关键字保造符合条件的设备,发放到描述的目标	5区域、可模提需要配置多个实例。			

图 4-10 添加证书策略详情

设备接入		设备发放策略 ①		
IoTDA範例 设備发放(新版)	^	施路名称	添加实例 ×	
息風 近书		→ 自定义策略	④ 2015年 ○	
授权		∧ 证书编辑	*@188% V Q	
988 3045			警天可告任书:请前在创建体为元任书 ⑦	
产型文档	C	EB80	90%9 986 986 986	
(3tE(RB)	C		* ##E	
			*##### V Q. BB#	
			RUM MCE BBB	
			89	
			59	
			89	
			899	
		意楽数:7 10 ~ (1 >		
		✓ 静态策略	接关腰掌探遗符合条件的设备,发放到探觉的目标运输,可得描着要配置多个实例。	

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

≡ 🌺 \$733	æ I	2W2					Q #8	教云服务、文档、资源(名称)1	DAP), tRB. MÆ S	138 鹿用 企业 工用 .	I# ⊾ Ç [*] @ ∰##	
设备接入		发放设备 ①										
IoTDA实例 设备发放(条板)	~	设备注册列表	注册唱列声	e e e e e e e e e e e e e e e e e e e								
80萬 近年		2000	R #20	\supset								
推校		秋市	设备名称	02/04/6/72/83	収益の	协议类型	接路类型	证书名称	所聞产品	所在区域	和放应用	操作
策略 设备		😑 ಷರು				MOTT	自定义策略	RIECA2	test	testbeijing	4dest	21.908 BR
产品文档	C	未发放				HTTP	静态端端					183119-088 189
论组界数	C	😑 1520				MQTT	静态策略		test	theeStandardInstance	DefaultApp	第1月中心教 影响
						MQTT	静态质略		test			10.000 M
		未发放				MOTT	静态策略					BIGGS BR
		*32				MQTT	静态策略					1930-04 19
		*22				MQTT	静态策略					91909 89
		*22				MQTT	静力振聴					233929 80
		未发放				MOTT	静态策略					231929 BB
		*323				MOTT	静态策略					25988 20
		652: II	10 🗸 <	1 2 5								

V IIIIVA Validades * Fill * Extra 1233 * Extra 1233 * Extra 1233 * Extr 1233 * Extra 12333							
bitter r.m. r.m. r.m. r.m. r.m. r.m. r.m. r.m. r.m. <	く 注册设备						
Ubitation Ubitation Ubitation PER Weining PER WEINING PER Weining WEINING WEINING							
with the set of the set	设备注册信息						
PBAR Wattram Wattram DAME Wattram DAME <td></td> <td>test1233</td> <td></td> <td>选择产品</td> <td></td> <td></td> <td></td>		test1233		选择产品			
*F8 F80 6472912648711681140863 088507 0600000000000000000000000000000000000							
Weiger OutmentTell • Weiger • Weiger <td>* 产品</td> <td>产品名称 test123</td> <td></td> <td></td> <td>产品ID</td> <td>64672912b487f16af14406bd</td> <td></td>	* 产品	产品名称 test123			产品ID	64672912b487f16af14406bd	
ender		设备类型 智能车位	280		协议类型	MQTT	
with the time time time time time time time tim							
088x7 8 ocumentTest 082x057, 082x01104114000d_documentTest 086x7 9 04729124477164114000d_documentTest 085x6x82 8x8x 04729124477164114000d_documentTest 018054628 04729124477164114000d_documentTest 01805478 04729124477164114000d_documentTest 01805478 04729124477164114000d_documentTest 01805478 04729124477164144000d_documentTest 01805478 04729124477164144000d_documentTest 01805478 04729124477164144000d_documentTest 01805478 04729124477164144000d_documentTest							
7	设备标识 *	documentTest					
* @rax incurrent Test * @rax incurrent Test * @rax incurrent Test Ørskijds ACET incurrent Test	69						
 ・ 倉倉谷 正 世 2010년 1. 住 会 名称 わ 为 土 里 2010년 26 4 1 1 4 4 0 0 b d _ document Test ・ 住 留 2010 6 4 6 7 2 9 1 2 1 4 3 0 1 4 4 0 0 b d _ document Test ● 5 5 5 5 4 ● 5 5 5 5 4 		documentTest					
* 依照D 647231224377168f14408bd_documentTest	* 设备名称	设备发放时,设备名称作为	主要的筛选条件之一,请正确填望	6,也可创建后在设备仓库中修改。			
・ 安全时 4405804_documentTest							
・ 新時姓祖 ・ 江中規碑 ・ 江中規碑 ・ 江中規碑 ・ 江中規碑 ・ 江中規碑 ・ 江中規幅 ・ ① の055.555 - 0 の の の	★ 设备ID	64672912b487f16af144)6bd_documentTest				
SHEYARCE 安建筑、 医树熊、 1000年1 证书典型 证书 证书余校 aacherTest 证书描述							
的建設備記録 学会現式 取得数式 X399245 证书典型 证书 ✓ + 证书名称 ● ● 证书指纹 ● ● 初始会報題 ● ● 0005,535.4 ● ●							
安全規式 取得規式 ▲2000年6 证书供型 证书 ✓ 米 证书名称 ● 证书指纹 ● 2.节指纹 ● 初始党書取型 ● 0005,535.4 ●	创建设备配置						
 ① 行発型 ① 行名 ◆ 征书名称 ● 信息therTest ◆ ● 常時発型 ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ①	安全標式	密钥模式	(.509)正书				
 ・ 征书会称 ● 福祉世祖 ◆ 原始姓型 ① 005,535 - 4 	证书类型	证书					
 ・ 征书名称 ▲ 征书名称 ▲ 征书名称 ▲ 御殿世型 ① 005,535 - 0 							
运行指纹 * 寬晴世辺 辽千策略 初始设备取置 005,535 /*	* 证书名称	teacherTest	``````````````````````````````````````				
ut 特面α * 集時共型 辺 出有無 辺 出行有略 0005,535 / 0005,535							
* 集時共型 辺治没者設置 0005,535 A	业均信权						
初始快音配置 0005,535 4	* 策略类型	证书策略	· · · · · · · · · · · · · · · · · · ·				
初始设备股盟0065,535.4							
005,535 #	初始设备配置						
			0/65,535	4			

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。

- 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"。

MQTT.fx - 1.7.0	– o x.
File Extras Help	
New Profile - Connect	Disconnect
Publish Subscribe Scripts Broker Status Log	
▼ Subscribe	QoS 0 QoS 1 QoS 2 Autorrol Cov
Topics Collector (0) Scan Stop Of .	
	DUB Retaived

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

Edit Connection Profiles			– D X
M2M Eclipse			
New Profile	Profile Name	New Profile	
test	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxia	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Connection Timeout	30	
	Keep Alive Interval	60	
	Clean Session	✓	
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	✓ Use Default	
		3.1.1	
		Clear Publish History	
		Clear Subscription History	
+ -	Revert		Cancel OK Apply

🗀 说明

其中Broker Address和Broker Port可以参考<mark>获取终端节点</mark>,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。

Edit Connection Profiles			– 🗆 X
M2M Eclipse			
New Profile	Profile Name	New Profile	
test	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxia	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	98cabff1-0112-4e63-ba59-a505ae	
	Password		
+ -	Revert		Cancel OK Apply

🗀 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。

Edit Connection Profiles			– 🗆 X
M2M Eclipse			
New Profile	Profile Name	New Profile	
test	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxia	Generate
	General User Credentials	SL/TLS Proxy LWT	
	Enable SSL/TLS	Protocol TLSv1.2	•
	CA signed server certificate CA certificate file CA certificate keystore Self signed certificates		
	CA File	C:\Users\ }\Desktop\ca2.crt	
	Client Certificate File	C:\Users' \deviceCert.crt	
	Client Key File	C:\Users\ \deviceCert.pem	
	Client Key Password		
	PEM Formatted	✓	
	Self signed certificates in keystores		
+ -	Revert		Cancel OK Apply

🗀 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 。

Publish Subscribe Scripts Broker Status L	og	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS 0 QoS 1 QoS 2 Autoscrol	0 ;•
Soc/devices/98cabff1-0112-4e63-ba59-a505aea5ebet_zhuviao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_ahuxiaocan_2/sys/bootstrap/down	1 QoS 0
Topics Callector (0) Scan Stop 😋	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 28-02-0200 15:07:0154421329 {"address":"iot-acc.cn-north-5.myhuaweicloud.com:8883","dnsFlag":0}</pre>	1 QoS 0

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loTDA所需的** 必要信息】预置到了loTDA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loTDA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loTDA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<mark>表1</mark> 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

设备接入		证书列表 ①			
IoTDA实例 设备发放(新板)	^	Linca(245			
证书		输证状态 证书名称	征书使用者	证书的政策	过爆状态
授权		~ ENE			司用
(注意) (注意)		✓ Bhe			可用
产品文档	C	◆ ★粒正			可用
论组末期	C	✓ 非检正			司用
		✓ DBE			可用
		✓ Bike			可用
		✓ E8G			
		意発数:7 10 ッ (1)			

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

设备接入		♥ CA证书上传成功								
IoTDA实例		证书列表 ①								
设备发放(制版)	^									
总规		上传CAIE书					请输入要搜索	的证书名称	Q (Q
证书			-							
授权		检证状态	证书名称	证书使用者	证书跟发者	过期状态	對用的问	EQ:11		
策略		→ 未能证	文档购试证书	conname	CN=conname, OU=cqwsd, O=cvwe, L=qwf, ST=zouxtst, C=CN	可用	2161/07/20 19:08 51 GMT+08:00	更新 動	AN BEET	B
设备						2263				-
产品文档	C	✓ BHE				可用	2161/07/28 11:28:23 GMT+08:00	更新量	A BEET	
论坛求助	C	✓ B総征				可用	2161/01/12 19:28:57 GMT+08:00	更新 動	IR INTER	IS

图 4-15 复制验证码

设备接入		🕑 CAIE书上传成功								>
IoTDA案例		证书列表 ③		上传验证证	E书		×			
(日本) 日第 証书		上体CA证书)	* 12(25)	07b0 145e5	Ō			请输入要按照	WERR Q Q
授权		验证状态	证书名称	* 检逻证书	点击右侧按胆原加文件	()(()()()()()()()()()()()()()()()()()()(过期状态	TUNEDIA	操作
策略		◇ 朱融道	文档则试证书				補定	可用	2161/07/20 19:08:51 GMT+08:00	R# 89 8225
产品文档	C	~ 日始年						可用	2161/07/28 11:28:23 GMT+08:00	ES EN BEES
论运求助	ß	✓ BNG						可用	2161/01/12 19:28:57 GMT+08:00	RM RM NEEK.

 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

设备接入	⊘ CA证书上传成功					
loTDA实例 设备发放(素板)	证书列表 ①	上传验证证书	×			
思惑 延時	LIRCALES	★ 输送研 07b0493652210e536c87b69b228145e5			请输入要搜加	REFERE Q Q
接权	给证状态 证书名称	* 验证证书 verificationCert.crt (1.22KB) × (清加文件)		过期状态	MARINA	1211:
策略 没备	◇ 未給证 文極約式近书	(70)	H (HS	可用	2161/07/20 19:08:51 GMT+08:00	RH 899 10225
产品文档	0 V BARE			可用	2161/07/28 11:28:23 GMT+08:00	EM EM 10323
论组织物	C V ERE				2161/01/12 19:28:57 GMT+08:00	-

----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<mark>表</mark>2所示。

耒	4-7	证1	这名	请求文	件参数说明
~	• •		<u></u>		<i>></i> x^ 007 J

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

设备接入		设备发放策略 ③				
IoTDA实例						
设备发放(新版)	^	狼鼯名称	油網研測			
总统 证书		> 自定义策略	遭过回数服务实现的自定义策略,快速实现个性化设备发	放业务流程。		
授权 除務	_	(#1050)				
0.98	_	函数名称	拨权图户	发放区域	操作	
产品文档	C				2010 ×	
论短求数	C				809	
		<				
		意奈歌:2 10 く 1				

创建注册组

图 4-18 新增注册组

设备接入	*	发放设备 ①					
loTDA实例 设备发放(新版) へ 总克 证书		设备注册列表 Scopeld 新增生册组			(清峻入要提案的注册组名称 Q) (Q)		
授权		注册组名称	证书类型	策略类型	操作		
策略			证书	自定义策略	洋情 勤除		
产品文档(3		证书	静态策略	洋情 翻除		
论坛求助 (3		证书	静态策略	洋倩 翻除		
			证书	静态策略	洋情 勤除		
		息祭数:4 10 ~ < 1 >					
	<						

图 4-19 创建证书自定义注册组

<	新增注册组		
	★ 注册组名称	test	
		[]]] []]] []]	
	* SETTIMENT	÷۳۳	
	* 证书名称	Test V	
	* 策略举型	自定义策略	
	★ 策略	TestFunctionDemo V	Q 创建自定义策略
	初始设备配置		
		0/65.535 4	
			取消的

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。

- 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。

Edit Connection Profiles			- • •
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings	1	
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	200000000000000000000000000000000000000	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Keep Allve Interval	60	
	Clean Session	~	
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	✓ Use Default	
		311	

4. 填写 User Credentials 信息。

Edit Connection Profiles			
M2M Eclipse	Des file Marra	land man lan	
local mosquitto	Prome Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	*************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password		

🛄 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。

Edit Connection Profiles			— 🗆 X
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	127.0.0.1	
	Broker Port	1883	
	Client ID	MQTT_FX_Client	Generate
	Enable SSL/TLS	Protocol TLSv1.2	
	CA signed server certificate		
	 CA certificate keystore Self signed certificates 		
	CA File	C:\Users\}\Desktop\plt_gw_ca	.crt
	Client Certificate File	C:\Users\; /\Desktop\plt_gw.crt	
	Client Key File	C:\Users\; \Desktop\plt_gw.crt	
	Client Key Password		
	PEM Formatted		

🛄 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。

🌐 MQTT.fx - 1.7.0		
File Extras Help		
local mosquitto	Connect Disconnect	A ()
Publish Subscribe	Scripts Broker Status Log	
Switch Fountain ON	» home/garden/fountain . Q. Q. Q.	Reta. 08-
Switch Fountain OFF		

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:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS1 QoS1 QoS2 Autoscrol	•:•
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 105 0

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。

Publish Subscribe	Scripts Broker	Status Lo. Sebef_zhi 💌	g Subscribe QoS1 QoS2 Autoscrob	
\$oc/devices/98cabff1-0112-4e6	3-ba59-a505aea5ebef_ Wessages Mute	zhuxiao 1	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/5ys/bootstrap/down	
Topics Collector (0)	Scan Str	op 02+	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 28-02-020 15-07-01.54421329 {"address":"iot-acc.cn-north-5.myhuaweicloud.com:88883","dnsFlag":0}</pre>	

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loTDA所需的 必要信息**】预置到了loTDA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loTDA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 loTDA> 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loTDA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。

云证书管理服务	私	有CA ⑦									
私有证书管理 ▲ 私有CA		创建CA 一共可以创新	100个CA,您还可	以创建89个CA。			所有类型	▼ 所有状态	▼ 请输入CA非	称进行搜索	QC
61-00/T-02		CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间		状态	操作	
10000			根CA	shenzhen		2020/07/04 23:38:46 GMT+08:00	2021/07/04 2	3:39:46 GMT+08:00	🕑 已激活	导出CA证书 禁用	

云证书管理服务	私有CA / 创建CA					
私有证书管理 ▲		— ② 确认信息 ——— ③ 完成				
私有CA	基本信息					
私有证书	* CA英型	● 根CA 创建根CA,用于建立新的CA层次结构。				
		○ 从屬CA 创建从届CA,用于在现有的CA层次结构中增加	明新的层次。			
	* 密钥算法	RSA2048 *				
	* 签名哈希算法	SHA256 *				
	* 有效期	1 · ·	年 到期时间: 2021/07/	17 15:10:48 GMT+08:00		
	证书唯一标识名称(DI	N)				
	* CA名称 (CN)	test]	★ 国家/地区	CN	
	* 畲/市	语输入省/市)	* 城市	请输入城市]
	* 公司名称 (O)	请输入公司名称 (O)		★部(]名称 (OU)	请输入部门名称 (OU)]
	证书吊销配置					
	OBS授权 ⑦	✓已接収私有证书管理服务访问您的○BS播。				E
	启用CRL发布					1 词:
	OBS桶	aosblueprints-cn-north-7-2a6e891afbf84f0894 *	O 创建新的OBSMA			18
	* CRL更新周期	请输入7~30的整数	Ŧ			
	下−∌ R:#	í l				

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

设备接入		设备发放策略 ③					
IoTDA实例 设备发放(新板)	^	策嚴名符	就路记则				
52 征书		✓ 自定义频略	通过函数服务实现的自定义策略,快速实现个性化设计	■发放业务汽程。			
漫校		入 证书策略	根据证书属性将设备发放到描述的目标区域,可根据即	9要配置多个实例。			
设备 产品文档	c	16.1956	质权相户	32.05.16	发放后用	操作	
设运求助	C <					819	
		想保護:1 10 ~ (1)					
		→ 静态策略	接关键字保透符合条件的设备,发放到描述的目标区的	d. 可按接需要配置多个实例。			



📃 🌺 华为云 🗆	控制台	Q. 搜索云服务、文档、资源(名称IDAP)、快速… 备案 治疫 應用 企业 工具 工	単 E
设备接入	设备发放策略 ⊙		
ioTDA案例 设施发放(新版) へ 単選 正书 授权	 第554年 一 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	諸加定利 × - 任年紀 単功万正年 ✓ ・ 正年紀年 ✓ ○	
 第 役幣 产品文档 ご 	(表加來例) (正书名称)	85596 580 1995	C.
125570 C		• XINEM	200
			856 856
			200
	总条数:7 10 🗸 1 >		89
	✓ ₩念旗略	使光镜子来四年尚年代创作者,发现多洲在时间将已成,可有原用尊称整整个字的。	

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

¥为云	128/2	3					0.88	R云服务、文档、资源(名称vi	DMP)、快速 新宏 3	11茶 鹿川 企业 工具)	[# ⊵ ၞ ၳ ၳ ᡧ) ##
备拨入	X	放设备 ①										
DA案例 B(2放) 奈阪) へ		设备注册列表	注册电列表	E.								
5.8 2.6		(1100 R	RB 29	\supset								
862		秋市	设备名称	0.646-0.03	(QBBID)	协议类型	服務支型	证书名称	新聞产品	所在困难	和政府用	操作
105 0.46		 1000 				MQTT	自定义策略	RIECA2	test	testbeijing	40012	重计学设备 影响
216 (2		*20				нттр	静态端端					103/07/231 BD4
68 C		🔵 গ্রহাচ				MQTT	静态抽地		test	heeStandardInstance	DefaultApp	服务-导动物 動物
	<	*22				MQTT	静态策略		test			10.00 M
		*22				MQTT	静态策略					21909 BM
		*333				MOTT	静态策略					10000 100
		*222				MOTT	静力策略					231008 20
		*22				MQTT	熱な筋筋					2349-039 209
		未发放				MQTT	静态振动					251929 20
		未放放				MOTT	静态策略					25928 23

图 4-23 注册云证书设备

く|注册设备

	test123	(」這擇产品			
* 产品	产品名称 test123		产品ロ	66a75d30954329271a26d474	
	设备类型 智能车位物		协议类型	MQTT	
设备标识					
· 89	documentTest				
设备实施	documentTestDevice				
- 美麗山谷	设备发放时,设备名称作为主要的菜选条件之一。	请正确填写,也可创建后在设备仓库中修改	κ.		
★ 设备ID	66a75d30954329271a26d474_documentTest				
创建设备配置					
安全模式					
	密钥模式 X.509让书				
证书类型	密钥模式 X.509延书 编为云证书	~			
证书类型 	能物機式 X 509延春 修为云证者 IoTDP_test_wiki	×]			
证书类型 ★ 证书名称	 取例使式 X-509运转 体力云证书 IoTDP_lest_wis 輸売可添证书? 清前社包建华为云(
 ④书典型 ★ ④书名称 ②音④ ●名称 	 取例使式 X-509运转 参为云证书 IoTDP_Jest_wki N无可指证书? 请前往创建华为云(CN) 	✓			
 近书类型 * 近书名称 设備近书名称 有效期(年) 	 取例使式 X-509运转 \$\$ \$\$ 	 、 ご 、 、 、 			
 近书类型 * 近书名称 设备证书名称 有效期(年) * 策略类型 	 本均去证书 经为去证书 经为去证书 InTDP_lest_web 服无可添证书? 请前往创建华为云((CH) 5 证书策略 	 × 正书 × × × × × × 			
 	 取例使式 X-509运转 	 × ○ 正书 ○ ○ ○ 			

RA

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。

三 🌺 华为	1.2	控制台					
设备接入		设备注册列表 / Document	Test				
IoTDA实例							
设备发放(新版)	^	设备名称	DocumentTestDevice 🖉		设备标识码	DocumentTest	
83		设备ID	66a75d3 74_DocumentTest		所厦产品	test-	
12日 1981日		协议类型	MQTT		笛略类型	证书策略	
短风		设备密钥	©		安全模式	证书模式	
设备		证书名称			证书指纹	6C928E2	3C1168A4
产品文档	C	设备证书名称(CN)	DocumentTestCN下载				
论坛求助	C						
		没备发放信息					
		设置状态 未2	ROX				
		发放记录					
		状态	3	腦	发放	区域	发放应用
		< Comparison of the second sec					
							HAAKTERNIN

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。

- 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"。

🕘 MQTT.fx -	1.7.0									
File Extra	s Help									
local	mosquitto				Connect	Disconnect				•
Publish	Subscribe	Scripts	Broker Status	Log						
Swite >>	home/garden/	'fountain				Publish	Qo5 0	Qo51 Qo52	Retained	

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。

Edit Connection Profiles			
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	200000000000000000000000000000000000000	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Connection Timeout	30	
	Keep Alive Interval	60	
	Clean Session	✓	
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	✓ Use Default	
		3.1.1	

4. 填写 User Credentials 信息。

Edit Connection Profiles			
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	*************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password		

🛄 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。

Edit Connection Profiles			– 🗆 X
M2M Eclipse			
local mosquitto	Profile Name loc	cal mosquitto	
	Profile Type MC	QTT Broker	
	MQTT Broker Profile Settings		
	Broker Address 12	27.0.0.1	
	Broker Port 18	383	
	Client ID MC	QTT_FX_Client	Generate
	General User Credentials 55L	/TLS Proxy LWT	
	Enable SSL/TLS 🧹	Protocol TLSv1.2	•
	O CA signed server certificate		
	 CA certificate file 		
	 CA certificate keystore Self signed certificates 		
	CA File C:	:\Users\}\Desktop\plt_gw_ca.crt	
	Client Certificate File C:	:\Users\; \Desktop\plt_gw.crt	
	Client Key File C:	:\Users\; \Desktop\plt_gw.crt	
	Client Key Password		
	PEM Formatted		

🗀 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。

👜 MQTT.fx - 1.7.0		
File Extras Help		
local mosquitto	Connect Disconnect	A
Publish Subscribe	Scripts Broker Status Log	
Switch Fountain ON	» home/garden/fountain	• Q Q Reta. 😋
Switch Fountain OFF		

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:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe Qos 0 Qos 1 Qos 2	Autoscroll 00
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1
Dump Messages Mute Unsubscribe		4000

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。

Publish Subscribe Scripts	Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-bat	59-a505aea5ebef_zhu	Subscribe QoS0 QoS1 QoS2 Autoscrol	06*
\$oc/devices/98cabff1-0112-4e63-ba59-a5	05aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0
Topics Collector (0)	Scan Stop cov		
		\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 28-02-2020 15:07:01.54421329	1 QoS 0
		<pre>{"address":"iot-acc.cn-north-5.myhuaweicloud.com:8883","dnsFlag":0}</pre>	

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loTDA所需的** 必要信息】预置到了loTDA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loTDA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 loTDA>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loTDA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。

云证书管理服务	私有CA ②								
私有证书管理 ▲ 私有CA	创建CA一共可以创	建100个CA,您还可以	(创建89个CA.			所有英型 マ 所有状态	▼ 遺編入CAS	称进行捜索 Q C	;
\$1.407.7	CA名称 (CN)	类型	部门名称 (OU)	签发CA名称	创建时间	到期时间	状态	操作	
4249.42TD		根CA	shenzhen		2020/07/04 23:38:46 GMT+08:00	2021/07/04 23:39:46 GMT+08:00	📀 已激活	导出CA证书 禁用	

安证书管理服务	私有CA / 创建CA					
▲有证书管理 ▲						
私有CA	基本信息					
私有证书	* CA英型	● 根CA 创建根CA,用于建立新的CA层次结构。				
		○ 从屬CA 创建从屬CA,用于在現有的CA层次结构中增加	明的层次。			
	* 密钥算法	RSA2048 *				
	* 签名哈希算法	SHA256 •				
	* 有效期	1 · · ·	年 到期时间: 2021/07/17 15:10:48	GMT+08:00		
	证书唯一标识名称(D	N)				
	* CA名称 (CN)	test	* 国家/地区	<u>z</u> [CN	
	* 曾/市	请编入做/市	* 城市		请输入城市	
	* 公司名称 (O)	请输入公司名称 (O)	* 部门名称	(OU)	请输入部门名称 (OU)	
	证书吊销配置					
	OBS授权 ⑦	<> 已接权私有证书管理服务访问您的OBS桶。				C
	启用CRL发布					词 • 反
	OBS桶	aosblueprints-cn-north-7-2a6e891afbf84f0894 v	↓ 创建新的OBSM			15
	* CRL更新周期	遺輸入7~30的整数	Ŧ			
		~				

添加自定义策略

图 4-25 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)	^	服務名称	36.88.62.09			
忠逸 征书		へ 自定义策略	通过函数服务实现的自定义策略,快速实现个性化设备3	1放业务流程。		
授权 策略		海加柴利				G
(2 9		函数名称	质权相户	双放区域	操作	
产品文档	C				the	
论坛求助	C				899	
		単発数:2 10 > < 1				

新增注册组

图 4-26 新增注册组

设备接入	发放设备 ②			
loTDA实例 设备发放(新版) へ 总路 证书	设备注册列表 Scopeld			· 请输入要提来的注册组名称 Q Q
授权	注册组名称	证书类型	策略类型	操作
策略		证书	自定义策略	洋橋 勤除
产品文档 🖸		证书	静态策略	洋情 删除
论坛求助 🖸		证书	静态策略	洋情 删除
		证书	静态策略	洋情 勤除
	总统数: 4 10 V < 1 >			
	<			

图 4-27 添加云证书自定义策略注册组

く|新増注册组

* 注册组名称	云证书文档注册组		
* 认证方式	茨纽模式 X 50%正式)	
* 证书类型	华为云证书	~	
* 证书名称	製ますの洗证书2 法前注创建化为子证书	~	
+ 笠略光刑		~	
★泉市大王			
* 策略	Test_	~	Q. 创建自定义策略
初始设备配置			
		0/65,535 🥢	

创建并下载设备证书

10 6 14 1		况表注册到末 (
设备接入		设审注册列表 /		
IoTDA实例				
公共模型库		注册记录	边罢	边客证书
设备发放(新版)	^	1200 LOAK	×4	
总览		创建设备	hīt#	
证书		X.509证书	5	
授权				
策略				
设备				
设备数据同步				
产品文档	C			
设备发放(旧版)	Ľ			
论坛求助	C			

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

设备接入		设备注册列表 / wiki绑定注册细(勿删)						
IoTDA实例 公共模型库 设备发放(新板) 参览	^	注册记录 设置 设备证书	创建设备证书 *设备证书名称(CN)	test1234		×		Q
道书 授权 策略		X.509征书	有效期(年)	5	取消	ME	服作	
设备								
设备数据同步					< 1 /			
产品文档 设备发放(旧版)	с с							
论证明的	C				暂无表格数据			
					当前无设备证书数据,请先创建设备证书			
					创建设集证书			

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

设备接入	设备注册列表 /		
IoTDA实例			
公共模型库 设备分为(新新)	注册记录 设置 设备证书		
总选	创建设新证书		0
证书	X.509证书	现作	
· (文)	test1234	下數	
设备			
设备数据同步			
产品文档	C (
设备发放(旧版)	C)		
论坛求助	C		

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。

文档版本 05 (2024-10-25)

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。

- 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"。

😻 MQTT.fx -	1.7.0						
File Extra	s Help						
local	mosquitto			Connec	Disconnect		•
Publish	Subscribe	Scripts	Broker Status	Log			
Switc »	home/garden/	fountain		•	Publish	QoS 0 QoS 1 QoS 2	Retained OST
Switc							

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。

Edit Connection Profiles			- • •
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Connection Timeout	30	
	Keep Alive Interval	60	
	Clean Session	×	
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	✓ Use Default	
		3.1.1	

4. 填写 User Credentials 信息。

Edit Connection Profiles			
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	*************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password		

🛄 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。

Edit Connection Profiles		— 🗆 X
M2M Eclipse		
local mosquitto	Profile Name local mosq	uitto
	Profile Type MQTT Bro	iker
	MQTT Broker Profile Settings	
	Broker Address 127.0.0.1	
	Broker Port 1883	
	Client ID MQTT_FX	_Client Generate
	General User Credentials SSL/TLS	Proxy LWT
	Enable SSL/TLS 🗸	Protocol TLSv1.2
	CA signed server certificate	
	CA certificate file	
	CA certificate keystore Self signed certificates	
	CA File C:\Users\	}\Desktop\plt_gw_ca.crt
	Client Certificate File C:\Users\	Desktop\plt_gw.crt
	Client Key File C:\Users\	\Desktop\plt_gw.crt
	Client Key Password	
	PEM Formatted	

🛄 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。

🥶 MQTT.fx - 1.7.0		
File Extras Help		
local mosquitto	Connect Disconnect	
Publish Subscribe	Scripts Broker Status Log	
Switch Fountain ON	> home/garden/fountain	Reta. 😋
Switch Fountain OFF		

引导消息订阅

按照<mark>设备接收引导信息</mark>topic填写对应的topic,单击"Subscribe"进行订阅。订阅成功 如下所示:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS1 QoS2 Autoscrol	06*
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0

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。

Publish Subscribe Scripts Broker Status L \$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht *	Og Subscribe Q050 QoS1 QoS2 Autoscrol	0 5*
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0
Topics Collector (0) Scan Stop Cor	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 20-02-2020 15-07-01-54421329 {*address*:*iot-acc.cn-north-5.myhuaweicloud.com:8883*,*dnsFlag*:0}</pre>	1 QoS 0

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loTDA所需的** 必要信息】预置到了loTDA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loTDA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 loTDA>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loTDA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<mark>表1</mark> 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

设备接入		证书列表 ①			
IoTDA实例 设备发放(新板)	^	Linca(245			
证书		输证状态 证书名称	征书使用者	证书的政策	过爆状态
授权		~ ENE			司用
(注意) (注意)		✓ Bhe			可用
产品文档	C	◆ ★粒正			可用
论组末期	C	✓ 非检正			司用
		✓ DBE			可用
		✓ Bike			可用
		✓ E8G			NR
		意発数:7 10 ッ (1)>			

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

设备接入		♥ CA证书上传成功							
IoTDA实例		证书列表 ①							
设备发放(制版) 总说 (F15	^	LIGCALE#)				请输入更按定	的证书名称	Q Q
授权		检证状态	证书名称	证书使用者	证书很发表	过期状态	医糖的间	现作	
策略 设备		✓ 未給证	文档则试证书	conname	CN=conname, OU=cquisd, O=cvive, L=quif, ST=zourtst, C=CN	可用	2161/07/20 19:08:51 GMT+08:00	更新 影	IR INCET.
产品文档	C	✓ BBE				可用	2161/07/28 11:28:23 GMT+08:00	更新 對	B BEEK
论坛求助	C	V FREE				可用	2161/01/12 19:28 57 GMT+08:00	-	NUTLIN .

图 4-33 复制验证码

设备接入		🔮 CAIE书上传成功								×
IoTDA实例		证书列表 ①		上传验证证	正书		×			
(1997) ()	* 脸证明	07b0 145e5	Ō			清榆入要按罗	WETSA Q
授权		验证状态	证书名称	* 脸还证书	点击右侧按图英加文件	(添加文件)		过期状态	10000	操作
策略		✓ 未設证	文档则该证书			Ru	28/22	初用	2161/07/20 19:08:51 GMT+08:00	846 800 12245
产品文档	C							司用	2161/07/28 11:28 23 GMT+08:00	
1215788 2	ß	~ Bitie						可用	2161/01/12 19:28:57 GMT+08:00	RM 80 8008

 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

设备接入	♥ CA证书上传成功					
loTDA实例 设备发放(素板)	证书列表 ①	上传验证证书	×			
思惑 延時	LIRCALES	★ 输送研 07b0493652216e536c87b69b228145e5			请输入要搜加	REFERE Q Q
接权	给证状态 证书名称	* 验证证书 verificationCert.crt (1.22KB) × (清加文件)		过期状态	MARINA	1211:
策略 没备	◇ 未給证 文極制式近书	(70)	H (HS	可用	2161/07/20 19:08:51 GMT+08:00	RH 899 10225
产品文档	0 V BARE			可用	2161/07/28 11:28:23 GMT+08:00	EM EM 10324
论组织物	C V ERE				2161/01/12 19:28:57 GMT+08:00	-

----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

门 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>2所示。

表 4-1	2 证书签名请求文件参数说明
\sim · · ·	

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

📃 🌺 华为云	控制台			Q. 搜索云服务、文档、资	國(名称/ID/IP)、快捷····································	资源 费用 企业 工具 工单	⊌ ₽°0 ⊕***	
设备接入	设备	「发放策略 ①						
IoTDA定例								
设备发放(新版)	^	策略名件	葉識说明					
征书		◇ 自定文策略	通过函数服务实现的	自定义编辑,快速实现个性化设备发放业务流	9.			
授权		◇ 征书策略	根据证书属性将设备	发放到描述的目标区域,可模描篇要配置多个	案例 .			
1018 019		へ 静态策略	投关键字描述符合条	件的设备,发放到描定的目标区域,可根据要	要配置多个实例。			
产品文档	C	(#10#M)					(
1002000	<	关键字	优先级别	版权租户	发放区域	发放应用	很作	
			4级				教師	
			210				#site	
			162				859	
			162				899	
			162				Bala	
			1級				把 54	
			162				2019	

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

设备接入		发放设备 ⑦			
loTDA实例 设备发放(新版) 总既 证书	^	设备注册列数 注册组列数 Scopeld 新潮注册组			(请输入要报账的注册组名称 Q) Q
授权		注册组名称	证书类型	策略类型	操作
領略			证书	自定义策略	洋橋 飽除
产品文档	C		证书	静态策略	洋病 胞除
论坛求助	C		证书	静态策略	洋情 删除
			证书	静态策略	洋債 删除
		总条数:4 10 ~ < 1 >			
	<				

图 4-37 创建证书静态注册组

く 新増注册组			
* 注册组名称	test		
* 证书类型	证书	~	
* 证书名称	teacherTest	~	
* 策略类型	静态策略	~	
初始设备配置	t "test":"test" }	21/65,535 %	
			取消 确定

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。

- 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"。

WQTT.fx -	1.7.0 s Help										
local	mosquitto			- 🔅	Connect	Disconnect					•
Publish	Subscribe	Scripts	Broker Status	Log							
Switc 🌫	home/garden/	fountain			•	Publish	Q05 0	QoS 1	QoS 2	Retained	
Switc											

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。

Edit Connection Profiles			
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker 👻	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	200000000000000000000000000000000000000	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	Keep Alive Interval	60	
	Clean Session		
	Auto Reconnect		
	Max Inflight	10	
	MQTT Version	Vise Default	
		311 -	

4. 填写 User Credentials 信息。

M2M Eclipse			
local mosquitto	Profile Name	local mosquitto)
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	XXXXXXXXXXXXXX 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password		

门 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。

Edit Connection Profiles			—
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	127.0.0.1	
	Broker Port	1883	
	Client ID	MQTT_FX_Client	Generate
	Enable SSL/TLS	Proxy LW1 Protocol TLSv1.2	•
	CA signed server certificate CA certificate file CA certificate keystore		
	Self signed certificates		
	CA File	C:\Users\}\Desktop\plt_	
	Client Certificate File	C:\Users\; \Desktop\plt	gw.crt
	Client Key File	C:\Users\; \Desktop\plt_	gw.crt
	Client Key Password		
	DEM Formatted		

🛄 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:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht	Subscribe QoS1 QoS1 QoS2 Autoscrol	0(*
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0

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。

Subscribe Scripts Broker Status I \$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zht •	Log Subscribe QoS 0 QoS 1 QoS 2 Autoscrol	0(*
Soc/devices/98cabff1-0112-4e63-ba59-a50Saea5ebet_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebet_zhuviaocan_2/sys/bootstrap/down	1 QoS 0
Topics Collector (0) Scan Stop 🔍	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 20-02-2020 15:07:01:54421329 {*address*:*iot-acc.cn-north-5.myhuaweicloud.com:8883*,*dnsFlag*:0}</pre>	1 QoS 0

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loTDA所需的 必要信息**】预置到了loTDA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loTDA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 loTDA>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loTDA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

📃 🌺 华为云	控制台			Q. 搜索云服务、文档、注	资源(名称/ID/IP)、快捷… 备实	资源 费用 企业 工具	Im & 4 () 🕀 📾 🗰 👘	
设备接入	设备	发放策略 ①						
IOTDA实例								
设备发放(新版) / 总流		策勝名件	業務説明					
证书 1940								
策略		 ● ●○原町 	投关键字体运符合条	件的设备,发放到描定的目标区域,可根据看	要配置多个实例。			
设备 产品文档	3							
论组求助	3	*1879	使失振制	活程順白	发展区域	发放运用	1975	
	<	7007	4级				104 N	
			218				859	
			1级				859	
			1级				899	
			16				859	
			1级				894	
			16				809	

新增注册组

创建注册组。

图 4-39 新增注册组

设备接入		发放设备 ③			
loTDA架例 设备发放(新版) 总览 证书	^	设备注册列表 Scopeld 新灌注预组			· 请输入要搜索的注册组名称 Q Q
授权		注册组名称	证书类型	策略类型	操作
策略	1		证书	自定义策略	洋情 删除
产品文档	C		证书	静态策略	洋情 删除
论坛求助	C		证书	静态策略	洋情 删除
			证书	静态策略	洋情 删除
		息祭数:4 10 × (1)>			
	×				

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

く 新増注册组	
* 注册组名称	testSecret
* 认证方式	密钥模式 X.509证书
注册组密钥	
* 策略类型	静态策略
初始设备配置	0/65.535.4
	003,337 %)
	取消 确定

🛄 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

く 新増注册组		
* 注册组名称	✓ 注册组创建成功	×
* 认证方式	为保证安全,密钥在注册组内不可见,如遗忘密钥,可通过"注册组详情 -> 设置 -> 重 置密钥"操作进行重置。	
注册组密钥	设备密钥 □ 点击复制	
* 策略类型	确定	
初始设备配置	0/65,535 1/2	
		取消 确定

🛄 说明

此处注册设备的设备名称需与<mark>添加静态策略</mark>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。

- 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"。

🎯 MQTT.fx - 1.7.0						
File Extras Hel	2 C					
local mosqui	ito	-	Connect	Disconnect		•
Publish Subs	cribe Scripts	Broker Status	Log			
Swite > home	garden/fountain			Publish	Qo50 Qo51 Qo52	Retained

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。

	_	×
Profile Name 密钥注册组测试		
Profile Type MQTT Broker		.ORG
MQTT Broker Profile Settings		
Broker Address iot-bs.cn-north-4.myhuaweicloud.com	1	
Broker Port 8883		
Client ID testGroupSecretTest_0_e9b 8_0_202302	Generate	
General User Credentials SSL/TLS Proxy LWT		
Connection Timeout 30		
Keep Alive Interval 60		
Clean Session 🗸		
Auto Reconnect		
Max Inflight 10		
MQTT Version 🗸 Use Default		
3.1.1 🔹		
Clear Publish History		
Clear Subscription History		

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。

Due d'a Marra		
Profile Name	密钥注册组则试	
Profile Type	MQTT Broker	
MQTT Broker Profile Settings		
Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
Broker Port	8883	
Client ID	testGroupSecretTest_0_e9b *8_0_202302 Generat	e
General User Credentials	SL/TLS Proxy LWT	
User Name	testGroupSecretTest	
Password	•••••••••••••••	
🗀 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<mark>物联网平台的根证书</mark>,解压后,选择其中c或java目录下PEM 后缀的文件)的本地路径。

	Profile Name	密钥注册组测试		
	Profile Type	MQTT Broker	i	MQ
MQTT Brok	er Profile Settings			
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com		
	Broker Port	8883		
	Client ID	testGroupSecretTest 0 e9 f8 0 202302	Generate	
	Enable SSL/TLS	Protocol TLSv1.2		•
CA signed	server certificate			
• CA certific	ate file			
	CA Certificate File	:ates\huaweicloud-iot-root-ca-list\c\huaweicloud-iot	-root-ca-list.j	pem
CA certifica	ate keystore			
Self signed	certificates			
Cale since d	and the second second			
Self signed	certificates in keystore.	2		

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。

MQTT.fx - 1.7.1		-	\times
File Extras Help			
🖹 密钥主册组别试 👻 🐼 Connect Discon	wnect		
Publish Subscribe Scripts Broker Status Log			
\$oc/devices/testGroupSecretTest/sys/bootstrap/down	QoS 0 QoS 1	QoS 2 Autoscro	X.*
\$oc/devices/testGroupSecretTest/sys/bootstrap/down			
Dump Messages Mute Unsubscribe			

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:

WQTT.fx - 1.7.1	
File Extras Help	
🖹 密钥注册组测试 🗸 🐼 Connec	Disconnect
Publish Subscribe Scripts Broker Status Log	
\$oc/devices/testGroupSecretTest/sys/bootstrap/down	
\$oc/devices/testGroupSecretTest/sys/bootstrap/down Dump Messages Mute	\$cc/devices/testGroupSecretTest/sys/bootstrap/down Unsubscribe

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。

WQTT.tx - 1.7.1	- L	×
File Extras Help		
🖹 密销注册组购试 👻 🐼 Connect Disco	nnect	a 🔵
Publish Subscribe Scripts Broker Status Log		
Soc/devices/testGroupSecretTest/sys/bootstrap/down	Qos 0 Qos 1 Qos 2 Automati	0(*
\$oc/devices/testGroupSecretTest/sys/bootstrap/down	\$oc/devices/testGroupSecretTest/sys/bootstrap/down	1 QoS 0
	\$oc/devices/testGroupSecretTest/sys/bootstrap/down	
	28-02-2023 14:42:25.52945565	1 OoS 0
Topics Collector (0) Scan Stop OC~	{"address":"100.95.185.49:8883","initConfig":null,"deviceSecret":"3d80fc260bf9434ebc38374db8ceccdc"}	

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loTDA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 loTDA> 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loTDA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

设备接入		授权关系						
IoTDA实例 设备发放(新版) 总笔 证书	^	被授权列表 ① 探 发起来权清求	双列表 ③					Q
接税		ID	秋志	接权租户	包建时间	描述	操作	
策略								
产品文档	C				<u> </u>			
12152783	S			U Markara Markara	 天表情数編 京原、埼元紀2年の清次 起降の清次 			
	<							
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

设备接入		授权关系					
loTDA変例 设備发放(新版) 总克 证书	^	被授权列表 ① 授权列表 ① 发起授权消表 ①		发起授权请求 进权法导 <u>集等28</u> 法号(0	×		
授权		ID	ŧs	★ 账号名称		描述	现作
策略 设备				* 1923 (
产品文档	C			描述			
1052RB	C	s		009 J	iir		

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

授权关系						
1000712 () 100712 ()						
26286387						Q
ID	88	淡较粗户	99936	编述	操作	
bC a65a0d	 已編用 		2823/11/28 10:28 14 GWT+08:00		89	

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

	x	控制台				數(名称/ID/IP)、快速… 备定 资源			
设备接入		设备	番发放策略 ③						
IoTDA实例									
设备发放(新版)	^		策略名称	始議说明					
总高			✓ 目定文策略	通过函数服务实现的	自定义策略,快速实现个性化设备发放业务流程	L			
授权			◇ 辺市策略	根據证书繼性時设备	发放到描述的目标区域。可根据需要配置多个实	iði.			
9698 1010			へ 静态策略	按关键字筛选符合多	件的设备,发放到描绘的目标区域,可根据需要	配置多个实例。			
产品文档	C		(RIDER)						Q
	0	<	关键字	优先级别	接权相户	发放区域	发放应用	操作	
				4级				899	
				2级				899	
				1級				854	
				1级				894	
				1级				este	
				1级				899	
				1级				影响	
				· · ·					

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

	_							
设备接入		设备发放策略 ⊙						
14TDAS08 公開設25(新期)	~	100.00	and sum	添加实例		×		
0.15 (1.15		~ REXEN	Acknieszinarym. 1982)	* 朱健宇				
86		✓ E+Ⅲ	根据证书增性利益单处的利用的艺术		如果设备名称和由设置的外继节,则可由自实所出行加速。如果设备名称不相当设置的外继节 带政设备名称。	F. 1812		
228		~ #c##	WARFIGHEBANDER. BURKE	* (1968)	12 28 38 48 58 O			
7782,018	C	BURN		1905×	±160 M60			
QUERE	C	关键字	成系統 制	10034	· · · · ·		RNOW	105
			48	+ X82#	584 ×			- 204
			28					209
			16.	· acoust	(mide:			80
			18		(RM)	RZ		89
			10					89
			12					899
			162					ESR .
		8588-7 10 V (1)						

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

λ	8	放设备 ①										
作 (奈板) へ		设备注册列表	注册电列带									
		(11HRR	RB 20	\supset								
		秋市	设备名称	0.046000	iQ盤iD	协议类型	後期末型	证书名称	新聞产品	所在困难	和政府用	服作
		😑 প্রহা				MOTT	曾迎义策略	RefCA2	test	testbeijing	4dest	#1.908 BM
C	3	未发放				HTTP	静态端端					103112 (211 104
C	3	🔵 প্লেফ				MOTT	静态崩竭		test	freeStandardInstance	DefaultApp	第3.49.01年 新社
	<	***				MQTT	静态质略		test			1819-09 89
		未发放				MOTT	静态策略					BIGGS BA
		未发放				MOTT	静态策略					1919/24 19 4
		未发放				MOTT	静态策略					91988 94
		未发放				MOTT	静态描格					21969 23
		未发放				MQTT	静态振荡					2019/20 20
		未放放				MOTT	静态策略					1979RR 199

图 4-48 创建密钥模式静态策略设备

≡	₩ 华为云	控制台	Q 搜索云影	表用 企业 工具 二	I# ⊡ Ç [®] @ ∰##	
<	注册设备					
	设备注册信息					
		test1233 (退程##蚕)				
	★ 严韻	严恶名称 test1233	产品(0 64	106bd		
		设备线型 风机	物议类型 MQTT			
	设备标识 * 码	DocumentTest				
	- 0927	DocumentTestDevice				
	- WHEN	设备发放时,设备名称作为主要的需选条件之一,骑正确编写,也可创建后在设备仓库中修改。				
	★ 设备ID	6467 i6bd_DocumentTest				
	创建设备配置					
	安全模式	被明核式 X.509证书				
	设备规则					
		设备与发放服务以及IoT平台建立MOTT链接时用于检证				
	* 策略类型	静态策略				
	初始设备配置					
		0/65,535 #				
						ROM

🛄 说明

此处注册设备的设备名称需与<mark>添加静态策略</mark>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。

- 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。

Edit Connection Profiles		
M2M Eclipse		
local mosquitto	Profile Name local mosquitto	
	Profile Type MOTT Proker	
	Home type High bloker	
	MQTT Broker Profile Settings	
	Broker Address iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port 8883	
	Client ID Client ID	Generate
	General User Credentials SSL/TLS Proxy LWT	
	Connection Timeout 30	
	Keep Alive Interval 60	
	Clean Session 🗸	
	Auto Reconnect	
	Max Inflight 10	
	MQTT Version 🗸 Use Default	
	3.1.1	

4. 填写 User Credentials 信息。

Edit Connection Profiles			
M2M Eclipse			
local mosquitto	Profile Name	local mosquitto	
	Profile Type	MQTT Broker	
	MQTT Broker Profile Settings		
	Broker Address	iot-bs.cn-north-4.myhuaweicloud.com	
	Broker Port	8883	
	Client ID	**************** 09	Generate
	General User Credentials	SSL/TLS Proxy LWT	
	User Name	****	
	Password	•••••	

🗀 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。

Edit Connection Profiles	
M2M Eclipse	
local mosquitto	Profile Name local mosquitto
	Profile Type MQTT Broker
	MQTT Broker Profile Settings
	Broker Address iot-bs.cn-north-4.myhuaweicloud.com
	Broker Port 8883
	Client ID Client ID Generate Generate
	General User Credentials SSL/TLS Proxy LWT
	Enable SSL/TLS V Protocol TLSv1.2 V
	CA signed server certificate
	CA certificate file
	CA Certificate File
	CA certificate keystore
	Self signed certificates
	Self signed certificates in keystores

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。

😻 MQTT.fx - 1.7.0		- • •
File Extras Help		
local mosquitto	Connect Disconnect	
Publish Subscribe	Scripts Broker Status Log	
Switch Fountain ON	» home/garden/fountain	Reta. 🔍
Switch Fountain OFF		

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:

Publish Subscribe Scripts Broker Status	Log	
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhu	Subscribe Qos 0 Qos 1 Qos 2 Autoscrol	0 \$ ~
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down	1
Dump Messages Mute Unsubscribe		050

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。

Subscribe Scripts Broker Status \$oc/devices/98cabff1-0112-4e63-ba39-a505aea5ebef_zht \$oc/devices/98cabff1-0112-4e63-ba39-a505aea5ebef_zht	Log Subscribe QoS 0 QoS 1 QoS 2 Autoscrol	057
\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiao	\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebet_zhuxiaocan_2/sys/bootstrap/down	1 QoS 0
Topics Collector (0) Scan Stop of *		
	<pre>\$oc/devices/98cabff1-0112-4e63-ba59-a505aea5ebef_zhuxiaocan_2/sys/bootstrap/down 28-02-020 15:07:01:54421329 {*address*:"iot-acc.cn-north-5.myhuaweicloud.com:8883*,"dnsFlag":0}</pre>	1 QoS 0

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loTDA所需的 必要信息】预置到了loTDA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loTDA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 loTDA>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loTDA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

MQTT 密钥设备使用静态策略发放 MQTT 注册组静态策略发放示例

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

☰ <u>₩</u> 华为著	ā	控制台			Q 搜索云服务、文档、普	翻《名称/ID/IP)、快速… 备案 创	察 费用 企业 工具 工单	© ↓ ? @ ∰##	
设备接入		设备发	放策略 ①						
IoTDA实例 设备发放(新版)	~		常務欠許	12181010					
总流 证书			✓ 自定义策略	通过函数服务实现的	自定义策略,快速实现个性化设备发放业务资	短.			
接权		1	✓ 证书鏡略	根据证书属性终设备	发放到描述的目标区域。可根据需要配置多个	实例 ,			
策略 设备			∧ 静态策略	按关键字简语符合条	件的设备,发放到描空的目标区域,可根据需	要配置多个实例。			
**品文档 045111111	C		18,00,00						
	0	<	关键字	优先级别	後权租户	发放区域	双放应用	操作	
				4段				1918 ·	
				242				2529	
				152				BSP	
				162				859	
				162				819	
				162				8 14	
				162				影除	

图 5-2 创建静态策略详情

设备接入		设备发放策略 ③					
IoTDA实例 设备发放(新版)	~	策略名称		添加实例	×		
#31		→ 自定文編略		* 关键字	静态策略-设备实际中包含的一部分字符串	1	
近书 授权		◇ 正形策略			如果设备各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 参次设备名称。		
1888 		へ 静态策略		* 优先级别	18 268 348 448 548 🕥		
设置 强文档	C	(READER)		接权租户	本第6 把所带		0
日本町	C	关键字	优先	★ 发放区域	×	激应用	1915
			4@	* 发放应用	v a	-	809
			2级				839
			1级				899
			1级		北東4		89
			102		北市4		89
			12		freeStandardInstance		899
			110		北東4		BSR

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。

ŧλ	2	比飲设备 ①										
(第版) へ		设备注册列表	注册电列声									
		(1110R	R# 200	\supset								
		₩Ø	设备名称	0200460783	収録の	协议类型	服務失型	臣书名称	新聞产品	所在困难	发放后用	彩作
		 1523) 				MOTT	自定义策略	RigtCA2	hest	testbeijing	Adest	21.908 BM
i e		未发放				HTTP	静态描绘					103/17/01 104
e		😐 1510				MQTT	静态策略		test	theeStandardInstance	DefaultApp	服务:导动物 肥料
	<	****				MQTT	静态策略		test			10.00 AM
		未发放				MQTT	静态接缩					21969 24
		*32				MOTT	静态策略					10000 BH
		*22				MOTT	静态策略					19312 CM 104
		*22				MQTT	静态描述					23/9/29 29
		未发放				MQTT	静态策略					201969 20
		未放放				MOTT	静态策略					25928 23

图 5-3 注册设备

图 5-4 创建密钥模式静态策略设备

≡	, 华为云	控制台	◎ 微素云素 …	
<	注册设备			
	设备注册信息			
		test1233 道府率册		
	* 产品	严嘉高称 test1233	严册/0 6- 1065d	
		2994 <u>8</u> Rf.	10080 MOTT	
	设备标识 * 码	DocumentTest		
	* 设备名称	DocumentTestDevice GB发动时,这是名称作为主要的网络条件之一,请正确保持,也可创建成在设备企和中等改。		
	★ 设备ID	6467 iSbd_DocumentTest		
- 29	创建设备配置			
	安全模式	都明構成 X.509证书		
	设备证明	设备与发放服务以及IoT平台建立MOTT链接时用于检证		
	★ 策略类型	最志策略 🗸		
	初始设备配置	045.535 #		

🛄 说明

此处注册设备的设备名称需与<mark>添加静态策略</mark>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。



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_mam 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 Default8ootstrapActionListener: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<mark>表1</mark> 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

TDADN		证书列表 ①			
(新版) (新版)	^	LincalE4			
证书		验证获态 征书名称	征书使用卖	证书部获需	过期转载
授权		~ BM2			可用
9506 (249		~ ENG			利用
1文相	C	→ #验证			可用
「木助	C	✓ 非批正			可用
		✓ E8€			可用
		✓ BNE			可用
		~ CRE			
		mest: 7 10 × (1)			

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

设备接入		♥ CA证书上传成	0.						
IoTDA定例		证书列表 ①							
设备发放(制版) 总流 延45	^	(Li¢CA)					法输入更投资	的证书名称 Q	0
860		检证	(1) 征书名称	证书使用者	证书酿发者	过期状态	如期时间	现作	
策略 设备		~ 未能	E 文档则试证书	conname	CN=conname, OU=cqwsd, O=cvwe, L=qwf, ST=zouvtst, C=CN	可用	2161/07/20 19:08:51 GMT+08:00	更新 動物 脸	
产品文档	C		E			可用	2161/07/28 11:28:23 GMT+08:00	更新 動脉 验	ŒЕВ
论坛求助	C	V Bas				可用	2161/01/12 19:28:57 GMT+08:00	更新 影泳 10	AESER

图 5-7 复制验证码

设备接入		O CA证书上传成功					×
loTDA实例 2048年1014年1月		证书列表 ①	上传验证证书	×			
8回 (111) (111) (111) (111) (111)		LIRCAEH	▲ 检证转 07b0 145e5			清榆入要按加	NUERER Q Q
授权		验证状态 证书名称	* 验证证书 《志古句般短期如文件 《汤如文件		过期状态	5000 Billios Al	IR45
策略		◇ 未验证 文档则试证书	Rw	24/2	可用	2161/07/20 19:08:51 GMT+08:00	BM BM 12235
(2)算 产品文档	C	✓ Bite			可用	2161/07/28 11:28 23 GMT+08:00	
论坛学物	ß	✓ Biti⊊	and the second sec		可用	2161/01/12 19:28:57 GMT+08:00	

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

门 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

设备接入		⊘ CAIE书上传成功								
loTDA实例 设备发放(新版)	~	证书列表 ①		上传验证证	EĦ		×			
0)元 征书		Lincaizes)	* 101259	07b049365221de536c87b69b22a145e5	D			诸输入要推动	RMETSER Q
授权		检证状态	征书名称	* 10225	verificationCert.crt (1.22KB)	× (適加文件)		过期状态	SAMABANG SAMABANG	现作
策略 役會		~ 未設注	文档和武正书			Rit	HE	可用	2161/07/20 19:08:51 GMT+08:00	-
产品文档	C	~ 日始征						可用	2161/07/28 11:28:23 GMT+08:00	EN DA BEES
论运序剧	C	~ E82							2161/01/12 19:28:57 GMT+08:00	-

----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<mark>表2</mark>所示。

表	5-4	证书签名请求文件参数说明	J
			,

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

- *** 华为	IZ 15	御台		Q. BORZAROS, X.M. 1	32数(名称VIDVIP)、快速… 备定 1	资源 獲用 企业 工具 工单		
设备接入		设备发放策略 ③						
TDA实例								
备发放(新版)	^	策略名件	除酪说明					
思戒 证书		◇ 自定文策略	通过函数服务实现的	自定义策略,快速实现个性化设备发放业务》	2里。			
授 权		◇ 迂村無暗	根据证书漏性将设备	发放到描述的目标区域。可根据需要配置多个	<u>መ</u> ብ.			
1988 0 49		へ 静态策略	接关键字筛选符合条	件的设备,发放到描述的目标区域,可模描言	要配置多个实例。			
LQH	C	(#1050)						
(B.S)	C (关键字	优先级别	接权电户	发放区域	发放应用	操作	
			4级				209	
			2级				259	
			1级				254	
			1级				259	
			1级				899	
			1级				894	
			162				影响	

新增注册组

图 5-10 新增注册组

设备接入	:	发放设备 ⑦			
IoTDA实例 设备发放(新版) へ 总流 证书		设备注册列表 Ecopeld 新憲注册组			(请编入要搜索的注册组名称 Q) Q
授权		注册细名称	证书类型	策略类型	操作
策略			证书	自定义策略	洋街 勤除
产品文档	5		证书	静态策略	洋橋 勤除
论坛求助 C	5		证书	静态策略	洋橋 删除
			证书	静态策略	洋債 删除
		思条数:4 10 × く 1 >			
	<				

图 5-11 创建证书静态注册组

く 新増注册组			
★ 注册组名称	test		
* 证书举型	ज ्म	~	
	21 I-1		
* 证书名称	teacherTest	~	
★ 策略类型	静态策略	~	
初始设备配置	"test":"test"		
	1	21/65,535 1/	
			(取消) 确定

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deviceld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)。



Scopeld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 Scopeld

设备接入	发放设备 💿			
ioTDA案例 设备发放(新板) へ 修造 证书	设备注册列页			
接权	注册相名称	证非类型	策勝类型	操作
10.00		E #	自定义描述	(F)) 859
严重文档 亿		(2H)	静态策略	1710 BSA
950AD ()		证书	基志策略	1732 859
		证书	静态策略	915 BB
	8988:4 10 × < 1 >			

🗀 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, deviceld, keyStore, "", scopeld)。 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 Default8ootstrapActionListener: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