本文档旨在帮助用户如何将网控设备接入到百度天工物联网平台。让用户能够快速的将网控物联网设备投入“使用”，即通过云平台与设备进行交互性测试，在此期间了解物接入的基础概念和业务逻辑，为后续的开发和业务部署工作提供基础。

一、创建项目

在使用物接入服务前，您需要创建一个百度智能云账号，请自行注册和登录。

1、登录百度智能云官网后，导航栏选择“产品服务”->“物联网服务” -> “物接入 IoT Hub”，即可开始使用物接入服务。

2、新用户在创建项目之前应先创建计费套餐并设定每个月收发消息的额度，系统将根据额度自动计算每个月的服务费用。每个用户只能创建一个计费套餐，所有项目将共享该套餐的额度。

① 按照步骤一进入物接入服务页面，点击立即使用进入天工物联网总览页面

② 选择“概览” -> “华南”或“华北” -> “创建计费套餐”，进入创建套餐页面。

③ 在创建套餐页面选择：

* 资源类型：物接入
* 当前地域：（由上一步选择的地区决定）

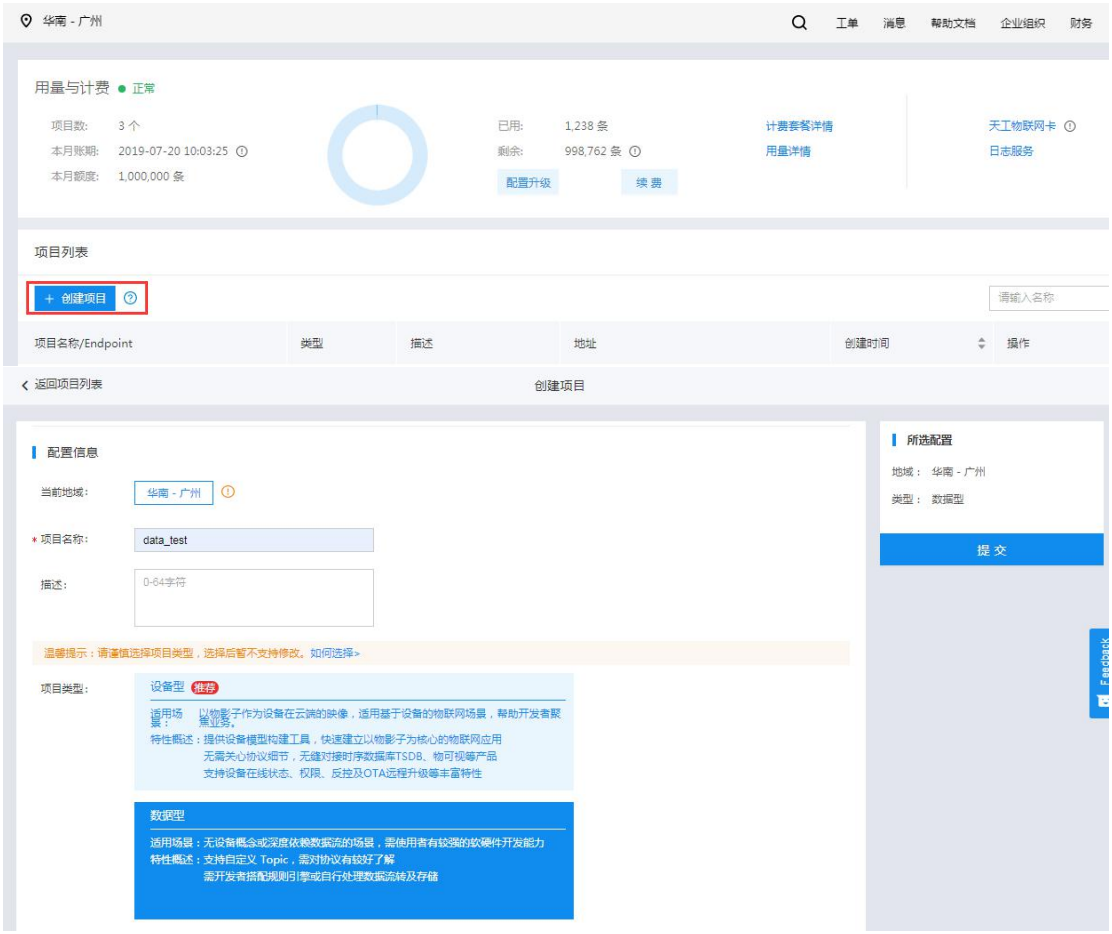
用户可根据需要自行选择付费套餐，以下为免费测试套餐选项：

* 购买规格：1 百万
* 购买信息：1/2/3 个月（最长 3 个月）

选择“下一步”进入付费页面，付费成功后，可进入“项目列表”创建项目。

连接物接入服务需要先创建一个项目，每个项目会为您对应一个接入点（endpoint）。一个项目表示一个完整的物接入服务。

2、登录物接入控制台页面，点击“创建项目”，填写需要创建 IoT Hub 服务的项目名称、选择项目类型设备型或数据型，并提交即可。通过项目可以将不同项目的设备进行隔离和管理。免费测试用户可以创建 1 个设备型项目，99 个数据型项目。



创建项目后，在项目列表页可以看到物接入默认提供的三类地址。选择不同的地址，意味着您可以通过不同的方式连接到百度智能云物接入。

项目名称/Endpoint	类型	描述	地址
m2a	设备型		tcp://[redacted].mqtt.iot.gz.baidubce.com:1883 ssl://[redacted].mqtt.iot.gz.baidubce.com:1884 wss://[redacted].mqtt.iot.gz.baidubce.com:443
data_test	数据型		tcp://[redacted].mqtt.iot.gz.baidubce.com:1883 ssl://[redacted].mqtt.iot.gz.baidubce.com:1884 wss://[redacted].mqtt.iot.gz.baidubce.com:443

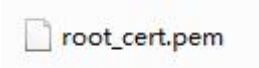
tcp://yourendpoint.mqtt.iot.gz.baiduce.com:1883，端口 1883，不支持传输数据加密，可以通过 MQTT.fx 客户端连接。

ssl://yourendpoint.mqtt.iot.gz.baiduce.com:1884，端口 1884，支持 SSL/TLS 加密传输，MQTT.fx 客户端连接，参考配置 MQTT 客户端。

wss://yourendpoint.mqtt.iot.gz.baidubce.com:8884，端口 8884，支持 Websockets 方式连接，同样包含 SSL 加密，参考 Websockets Client。

物接入提供设备型和数据型两种项目类型。后续步骤中，将分别予以描述，用户请根据自己期望使用的项目类型，选其一进行了解即可。

后续文档关于 SSL/TLS 方式连接的操作中需多处用到**百度天工根证书**：



请下载后妥善保存，下载地址：
https://sdk.bce.baidu.com/console-sdk/root_cert.pem

二、设备型项目

步骤一. 获取连接信息

成功创建物接入设备型项目后，点击项目名称，进入项目配置页面。下面以网控物联网多功能输入输出模块 GNC-NIO 为例，进行创建物模型、物影子和权限组，获取物接入设备型连接信息，具体操作步骤如下：

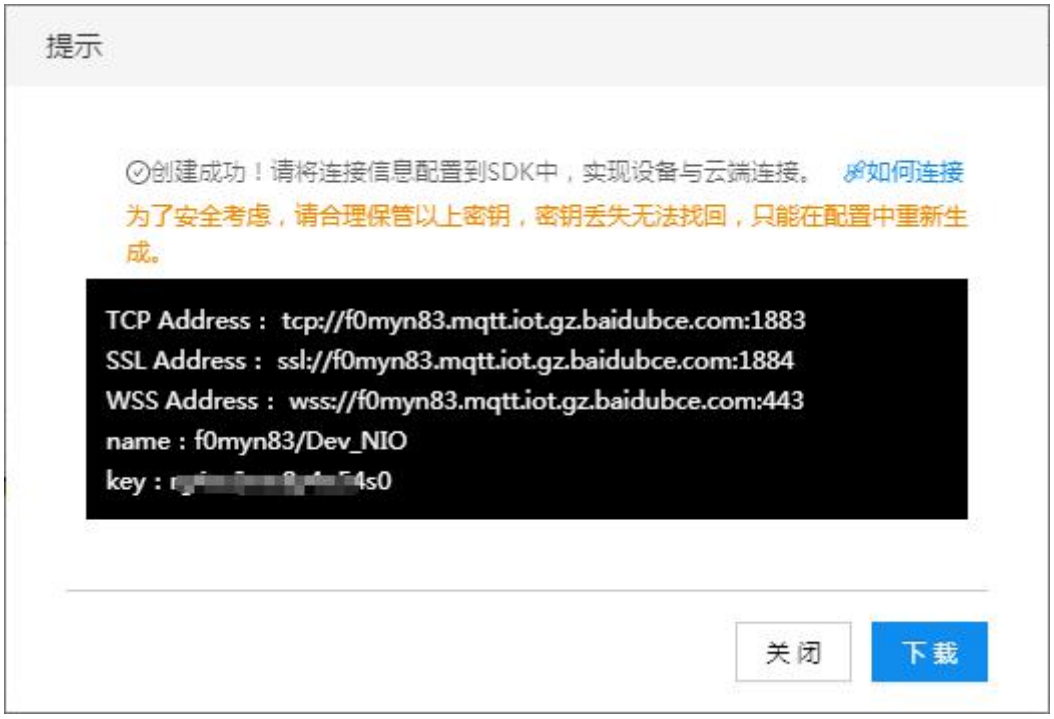
1、创建物模型： 点击项目名称进入后，选择“物模型”，进入物模型列表页面，点击”新建物模型“。

说明： 物模型用来表示一类（或同一型号的一批）设备。可为设备定义一套属性模板，在创建物影子时可以引用该模板，实现业务的快速部署。

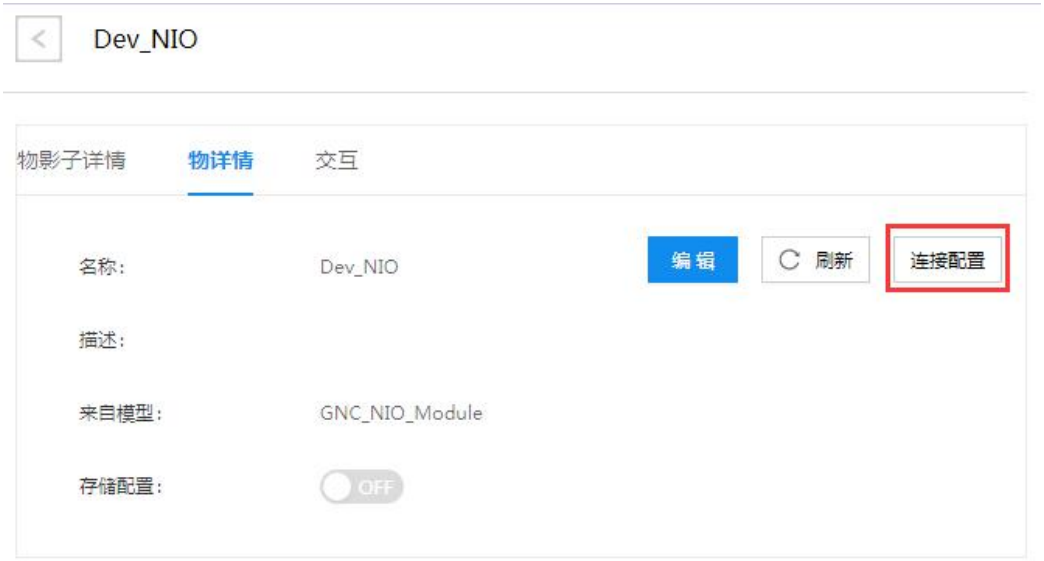
输入名称、描述，然后添加 GNC-NIO 的全部物模型属性，然后创建。物模型属性说明详见附录 1。

2、**创建物影子：**左侧选择“物影子”，进入物影子管理页面，点击“新建物影子”。输入物影子名称，并选择物模型（这里选择上一步创建的GNC_NIO_Model），点击“创建”，进入下一步。

3、**获取连接信息：**物影子创建完成后，弹出连接信息，建议下载后妥善保存。



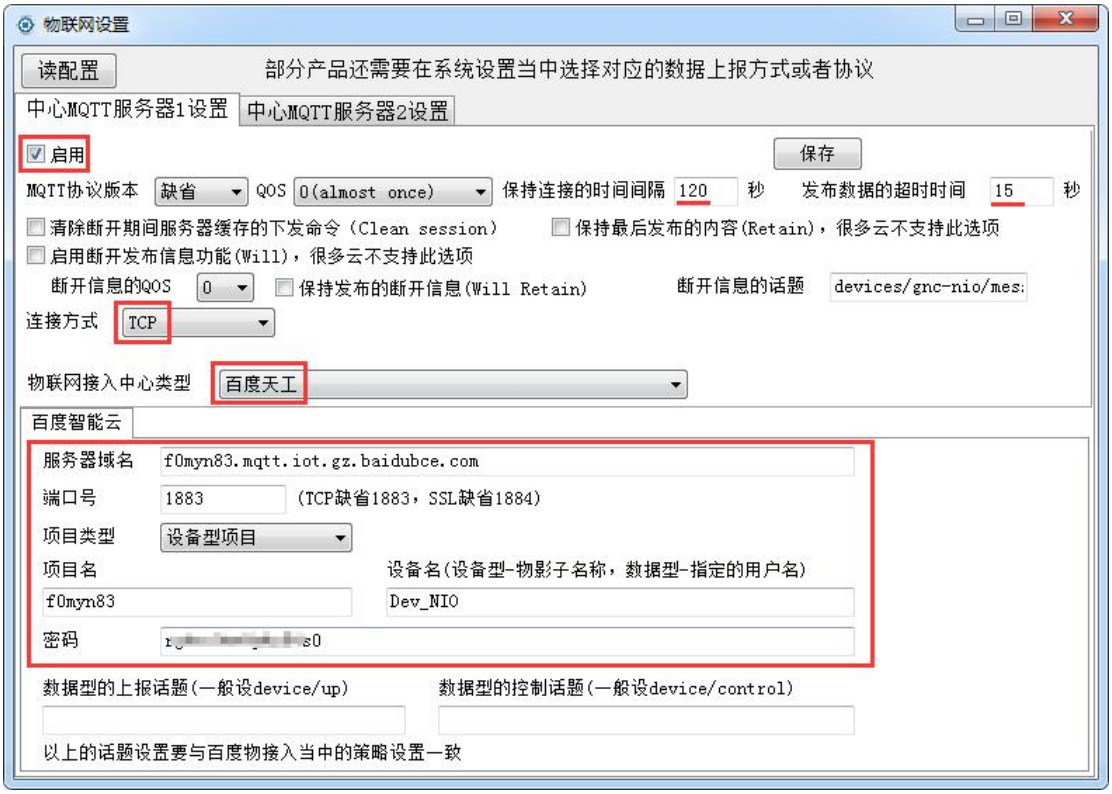
若连接信息未及时保存或密码丢失，亦可点击相应影子的卡片，进入物影子详情页面，随后通过以下路径查看连接信息或重新生成密钥。



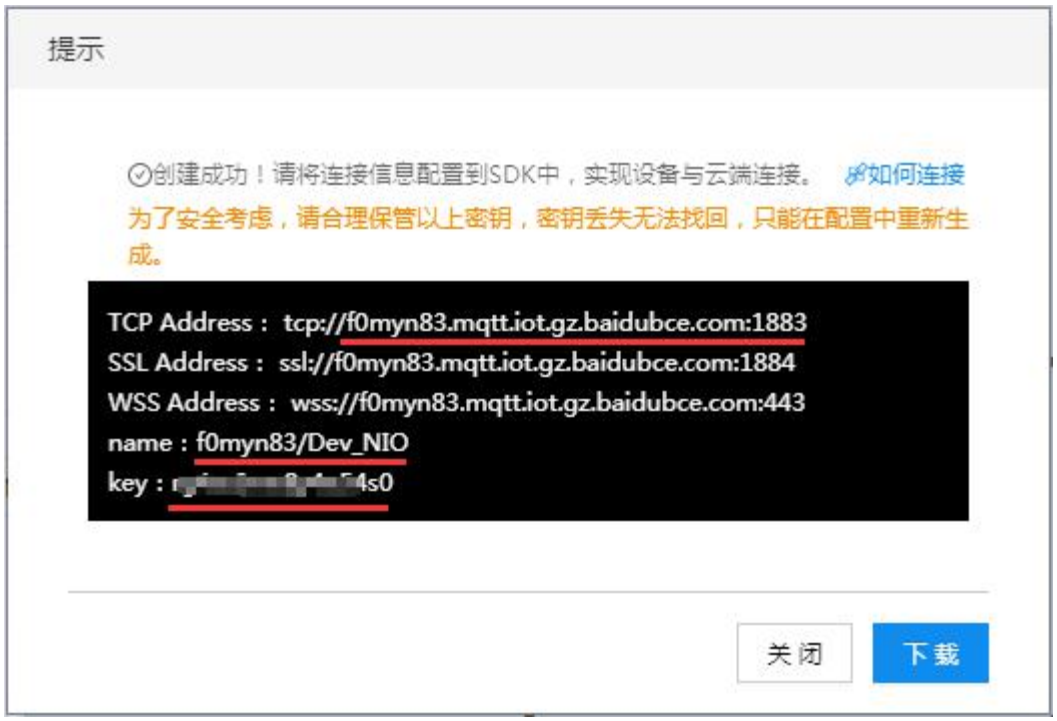
步骤二. 网控物联网设备配置

打开 GNC 设备发现与管理工具，发现认证登陆设备后进入设备物联网配置界面。

勾选**启用**。保持连接的时间间隔 120 秒，发布数据的超时时间 15 秒。
连接方式：TCP
物联网接入中心类型：百度天工。下方的参数框自动切换到百度智能云设置界面。
服务器域名：yourendpoint.mqtt.iot.gz.baiduce.com
端口号：TCP 方式缺省 1883
项目类型：设备型项目
项目名：yourendpoint
设备名：物影子名称
密码：物影子连接信息里的密钥
之后“保存”，”重启”设备。至此，设备的物联网配置完成。



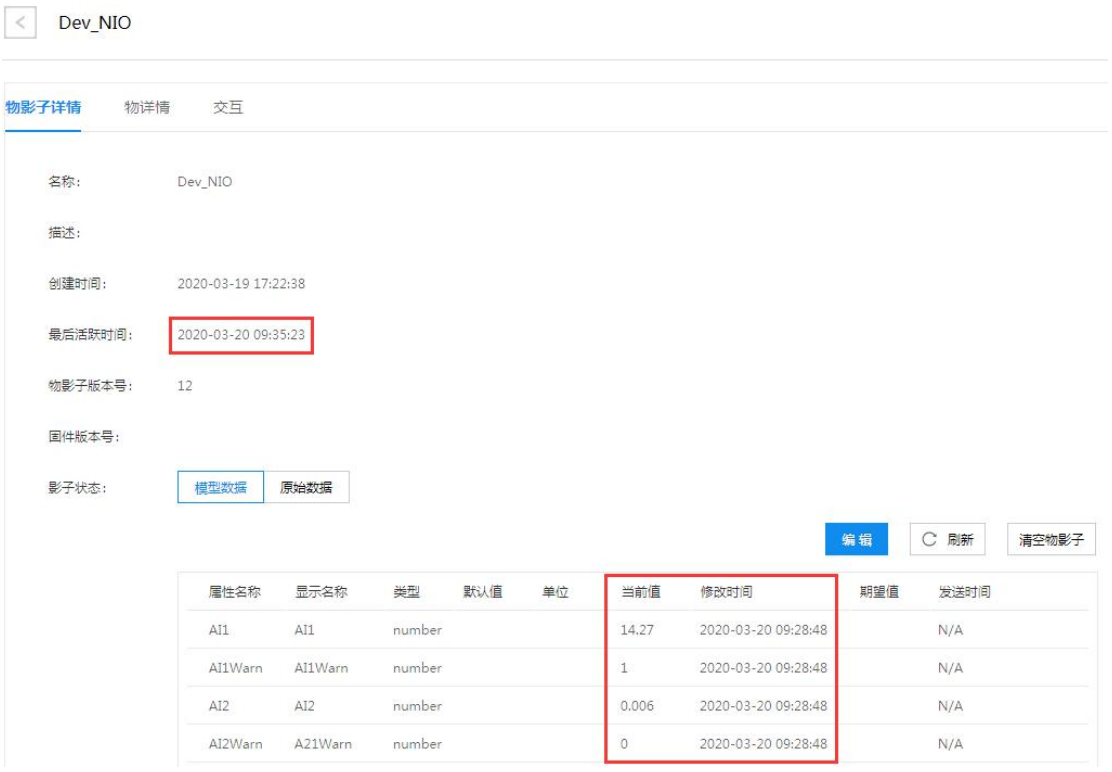
服务器域名、端口号、项目名、设备名和密钥见如图的连接信息。



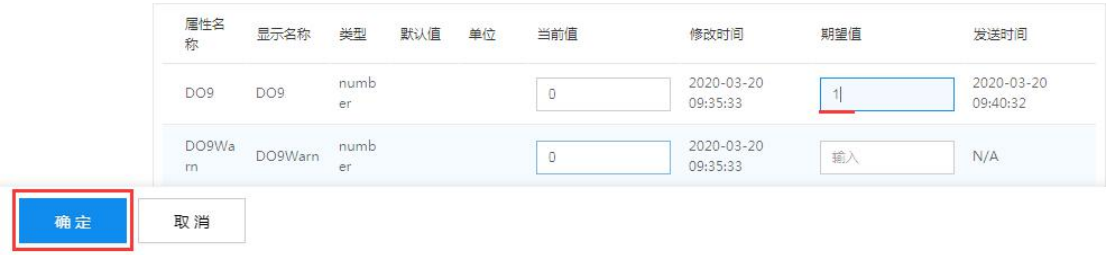
步骤三. 查看设备运行状态

在项目物影子管理页面，可以看到添加的 GNC-NIO 已显示在线。

点击物影子卡片查看影子详情，动作接入到 DI1~DI8 的测试开关或改变 AI1~AI8 输入的模拟量大小，刷新即可看到各属性的当前值和对应的告警值同步更新。



例如要控制 NIO 的继电器 1~4 闭合（D09~D012），选择“编辑”然后在“期望值”栏输入“1”（“0”：断开），点击下方“确定”即可控制继电器动作。

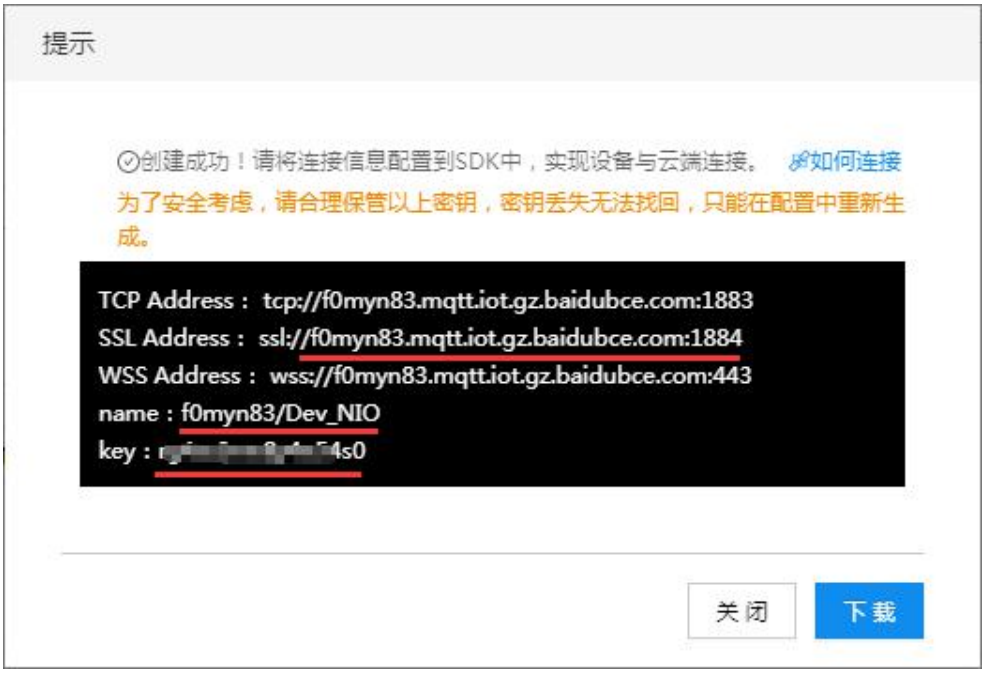


步骤四. SSL/TLS 连接

上述步骤一到三，演示了网控物联网设备以 TCP 方式连接到百度天工设备型项目，并进行控制测试。对于安全级别要求较高的场合，TCP 方式便不再适用，此时需要通过 SSL/TLS 连接云平台，以提高数据传输安全性。物模型和物影子的创建过程，以及连接成功后查看设备运行状态和在线调试等功能对于两种连接方式均相同，此处不多赘述。

网控设备的连接到百度天工设备型项目的物联网设置中，SSL/TLS 连接的配置类型分为两种，对应两个不同的安全级别，由低到高分别为 CA 签名的服务器（不强制证书检查），CA 签名的服务器（强制证书检查）。

后续配置中服务器域名、端口号、项目名、设备名和密钥见连接信息。



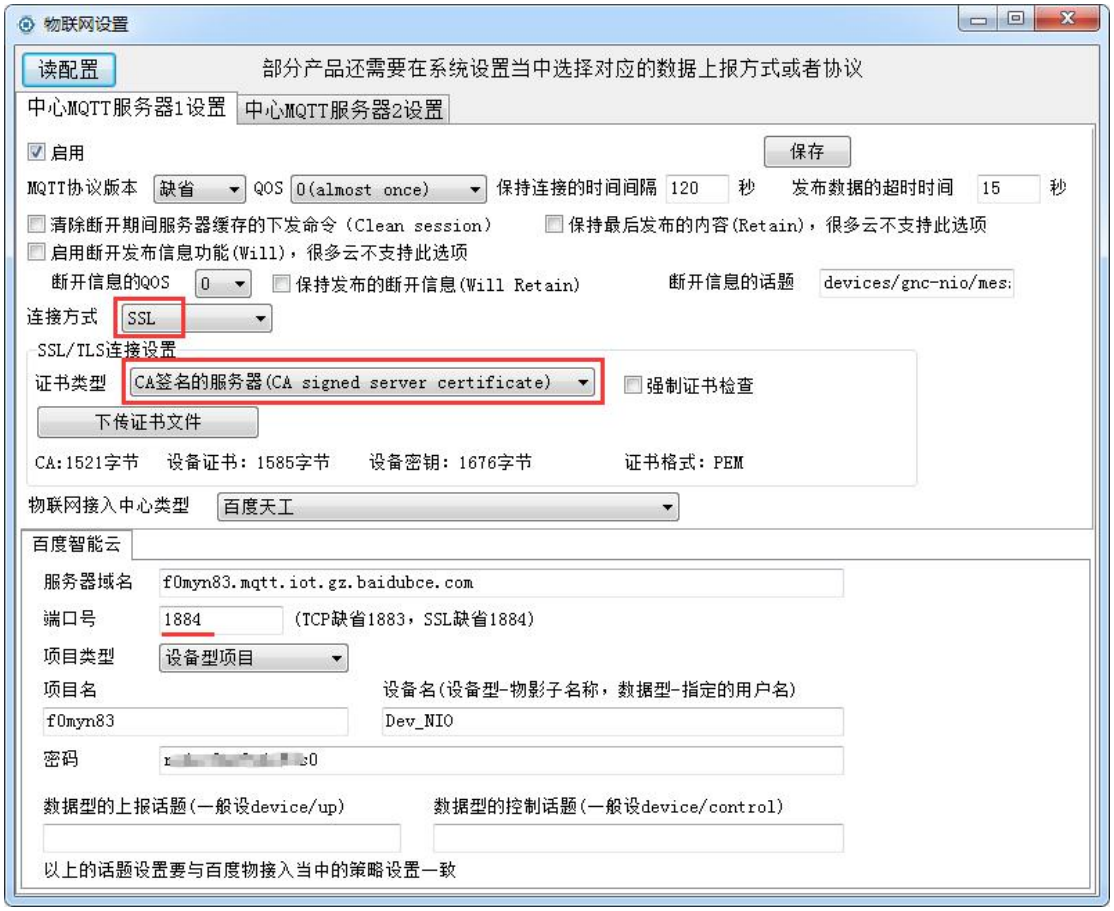
1、CA 签名的服务器（不强制证书检查）

连接方式：SSL

证书类型：CA 签名的服务器

端口号：1884

保存，重启即可。



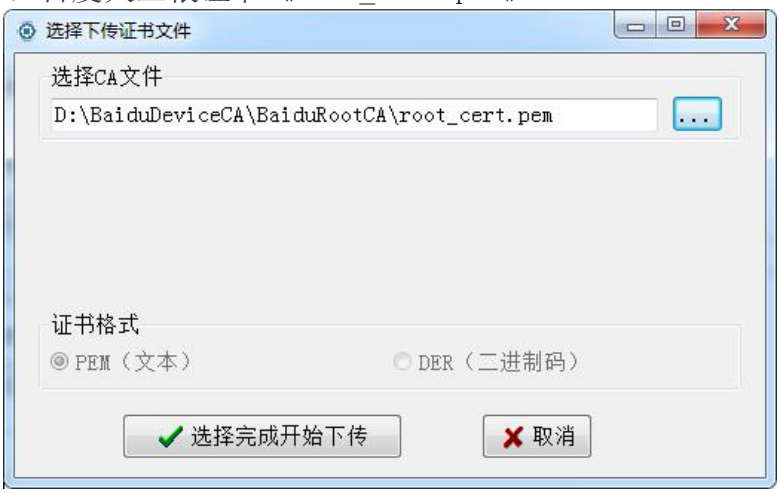
2、CA 签名的服务器（强制证书检查）

连接方式：SSL

证书类型：CA 签名的服务器

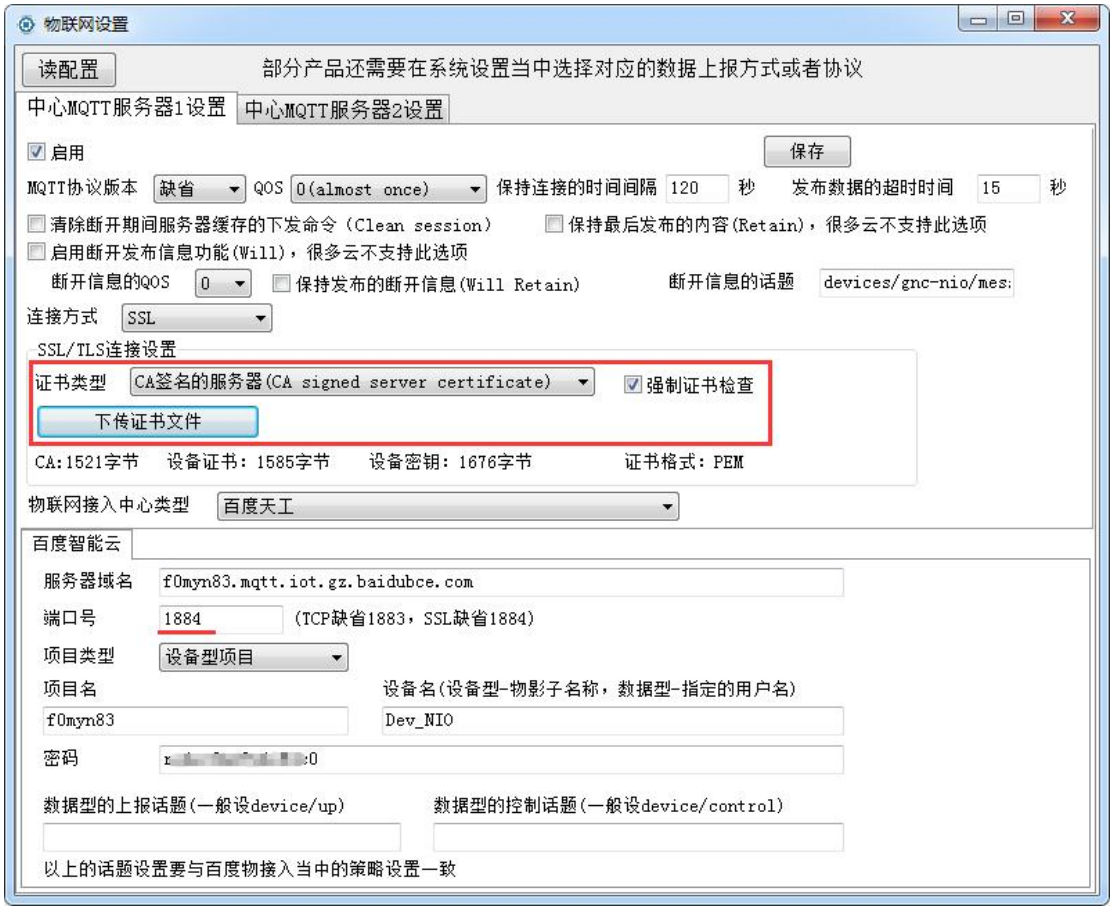
勾选强制证书检查。

下传证书文件：百度天工根证书《root_cert.pem》



端口号：1884

保存，重启即可（新下传的证书文件会覆盖旧文件）。



三、数据型项目

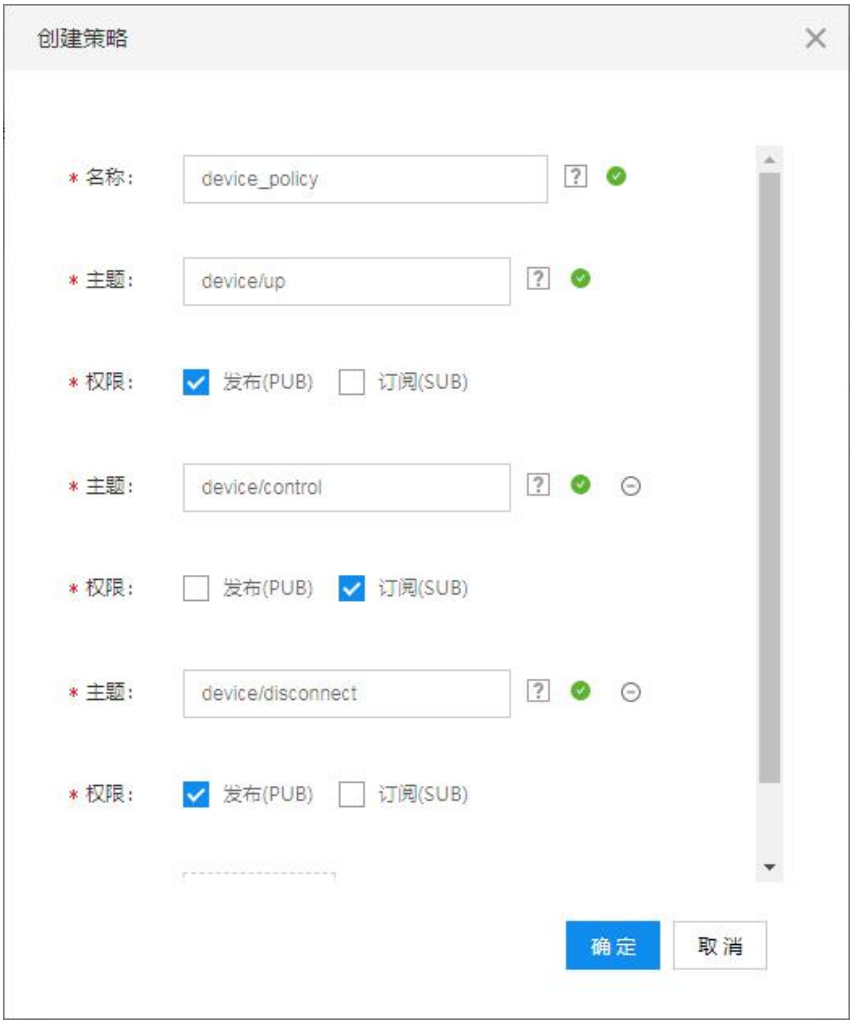
步骤一. 获取连接信息

成功创建物接入数据型项目后，点击项目名称，进入项目配置页面。下面以网控物联网多功能输入输出模块 GNC-NIO 为例，进行创建用户、身份和策略，获取物接入连接信息，具体操作步骤如下：

1、创建策略：在项目配置页面选择“策略列表”->“创建策略”。

输入策略名称，主题(Topic)，选择主题的权限：发布(Publish)、订阅(Subscribe)。

（1） 创建**设备端策略**“device_policy”。



（2） 创建软件**客户端策略**“software_policy”。

说明：每个策略可以创建多个主题(Topic)，点击“+”可以新增更多的主题。

`device/up`

描述：设备（GNC-NIO）上报数据的主题。由设备端发布，软件客户端订阅。

`device/control`

描述：为客户端下发给设备控制命令的主题。由软件端发布，设备端订阅。

`device/disconnect`

描述：遗嘱消息主题。在设备网络连接断开后，IoT Hub 将会自动向该主题发送遗嘱消息。

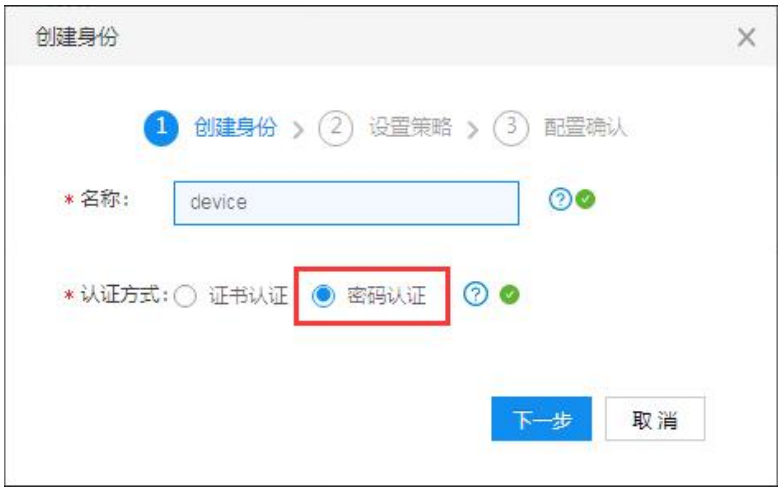
也可使用自定义主题，如 device/gncnio/up，后续设备的物联网设置的话题和连接测试的话题需与策略的设置一致。

添加主题时，可以使用“#”或“+”作为通配符，关于通配符的介绍，请参看关于关于通配符的使用方法。

2、创建身份：在项目配置页面选择“身份列表”->“创建身份”。

（1） 创建**设备端身份**

① 输入名称，认证方式选择“密码认证”。



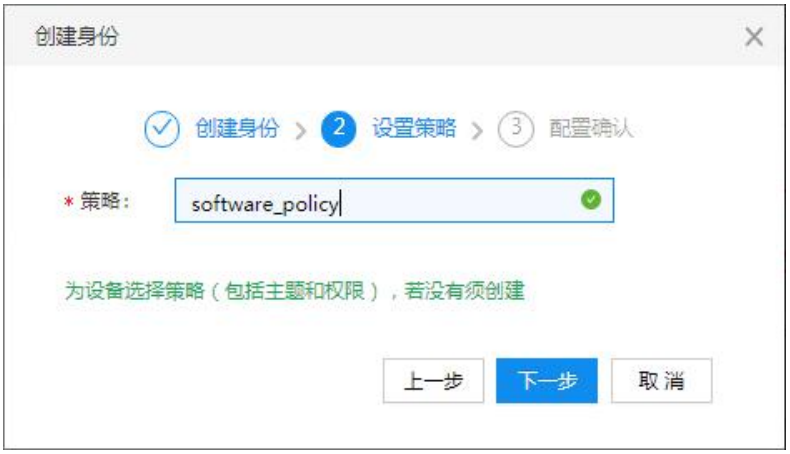
② 策略选择之前创建的设备端策略“device_policy”。

③ 生成**设备身份密钥**。用于后续网控设备物联网配置，请妥善保管。

（2） 创建**客户端身份**

① 输入名称，认证方式选择“密码认证”。

② 策略选择之前创建的客户端策略“software_policy”。



③ 生成客户端身份密钥。用于客户端连接测试，请妥善保管。

3、创建用户：在项目配置页面选择“用户列表”->“创建用户”。

（1） 创建**设备端用户**

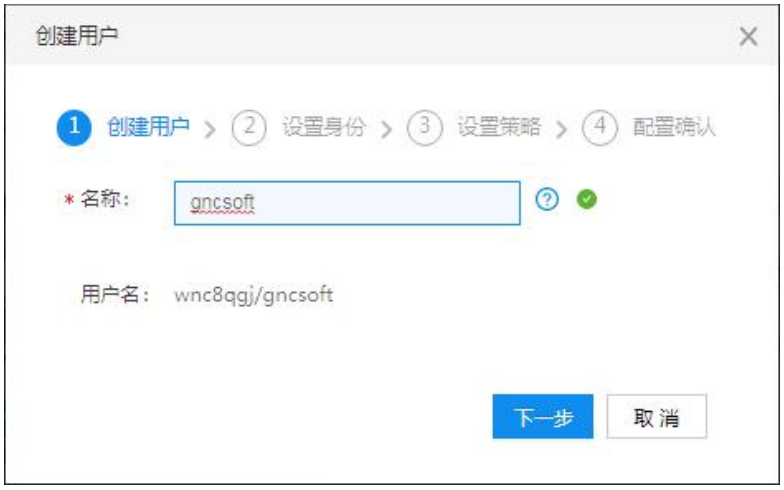
① 输入名称，然后下一步。

② 设置身份选择之前创建的设备端身份“device”。

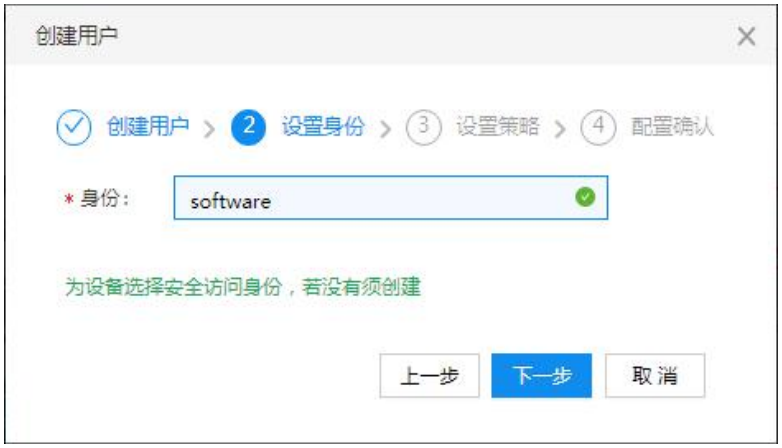
③ 配置确认。

（1） 创建**客户端用户**

① 以测试客户端为例，输入名称，然后下一步。



② 设置身份选择之前创建的客户端身份"software"。



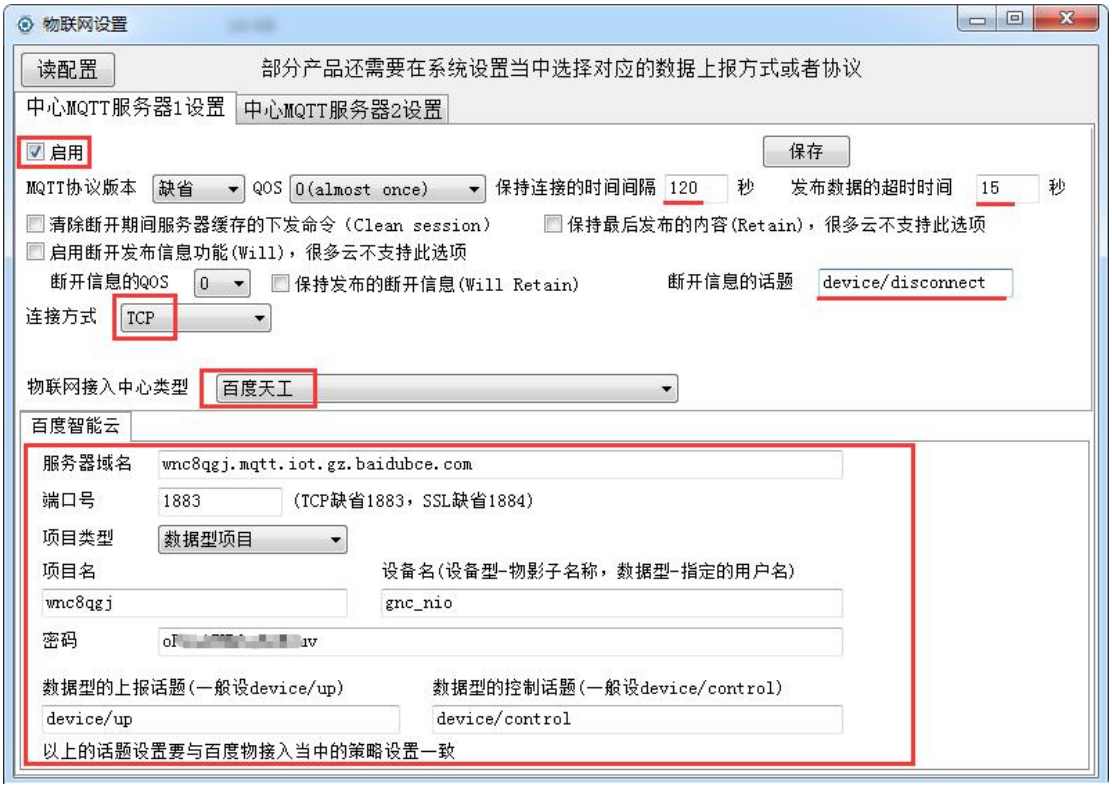
③ 配置确认。

至此，网控物联网设备接入百度天工数据型项目的配置完成，并获得连接信息。

步骤二. 网控物联网设备配置

打开 GNC 设备发现与管理工具，发现并认证登陆设备后点击进入设备物联网配置界面。

勾选**启用**。保持连接的时间间隔 120 秒，发布数据的超时时间 15 秒。
断开信息的话题：可选。遗嘱消息主题，device/disconnect
连接方式：TCP
物联网接入中心类型：百度天工。下方的参数框自动切换到百度智能云设置界面。
服务器域名：yourendpoint.mqtt.iot.gz.baiduce.com
端口号：TCP 方式缺省 1883
项目类型：数据型项目
项目名：yourendpoint
设备名：创建的设备端用户名
密码：为步骤一中，2.1.3 创建 device 身份生成的**设备身份密钥**
数据型的上报话题：device/up，若使用自定义主题注意与策略保持一致
数据型的控制话题：device/control，若使用自定义主题注意与策略保持一致
之后“保存”，”重启”设备。至此，设备的物联网配置完成。



服务器域名和端口号：

项目名称/Endpoint	类型	描述	地址
data_test wnc8qgj	数据型		tcp://wnc8qgj.mqtt.iot.gz.baidubce.com:1883 ssl://wnc8qgj.mqtt.iot.gz.baidubce.com:1884 wss://wnc8qgj.mqtt.iot.gz.baidubce.com:443

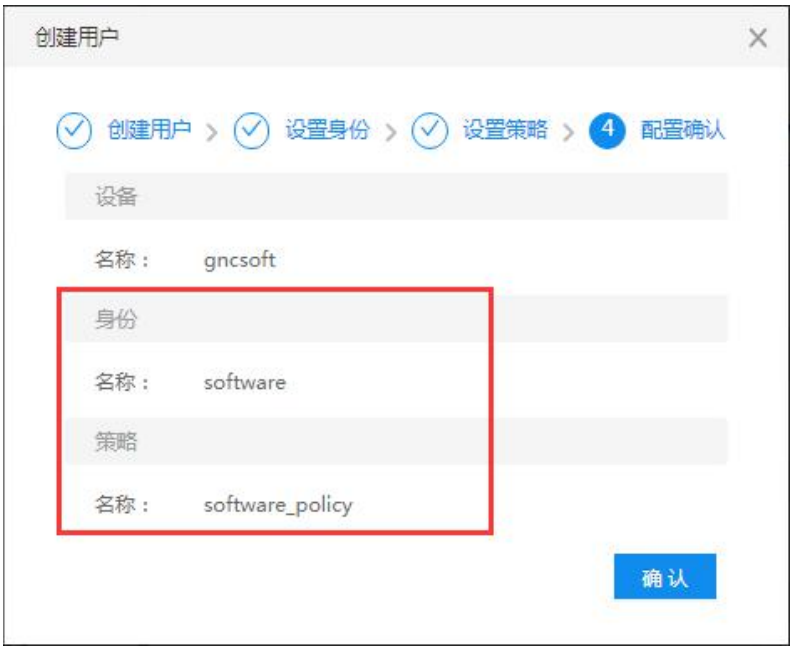
项目名和设备名：

用户名	描述	创建时间
wnc8qgj/gnc_nio		2020-03-18 17:15:36

步骤三. 通过百度天工物接入平台测试

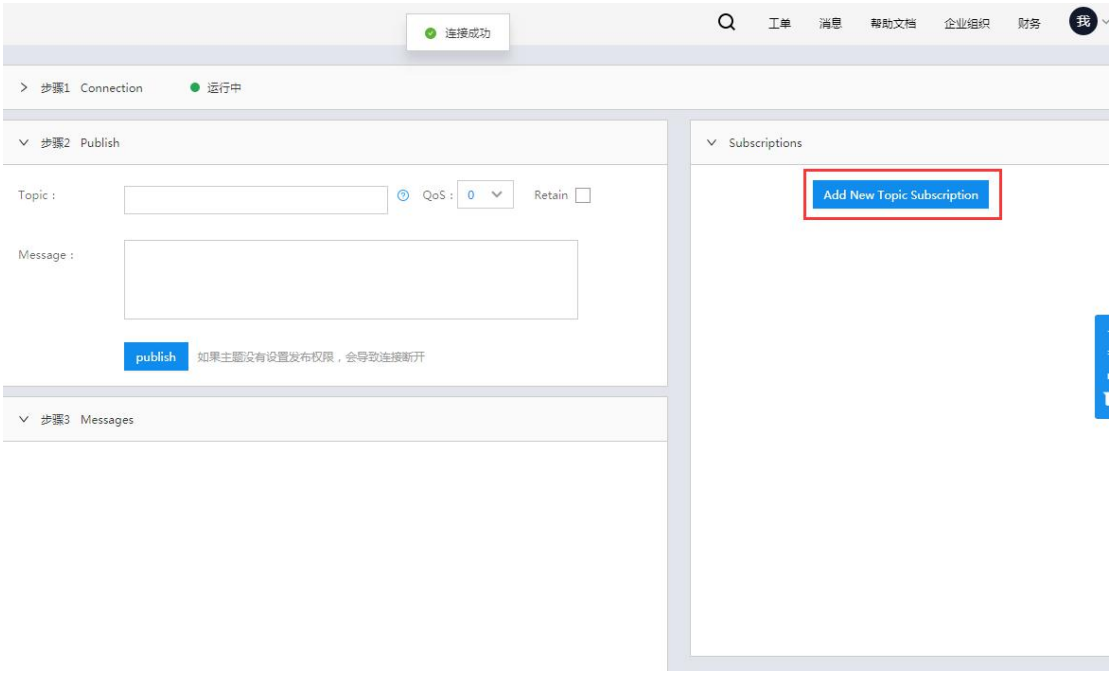
1、在用户列表页面选择“连接测试”，可以创建多个用户同时进行连接测试。

注意：进行连接测试的用户须是绑定了 software 身份或对应策略的主题和权限相同。

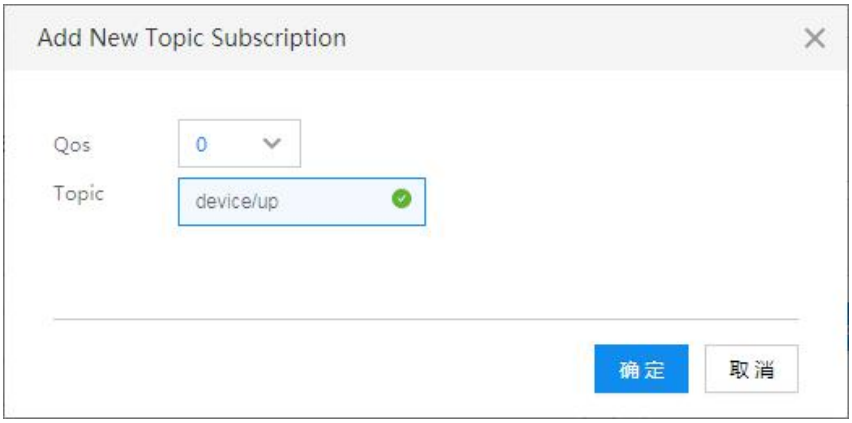


2、以 gncsoft 用户为例，进入天工物接入测试页面，身份密码为步骤一中，2.2.3 创建的 software **客户端身份密钥**，点击“connect”，提示连接成功。

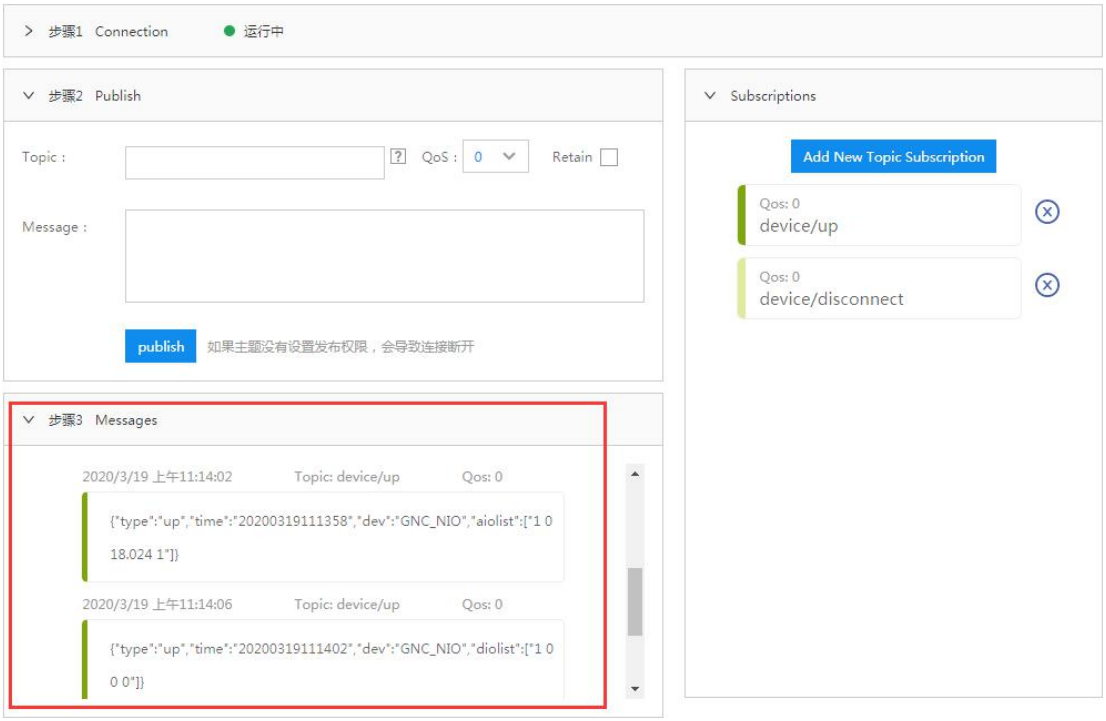
3、点击右侧的 Add New Topic Subscription，订阅主题。



4、在弹出的 **Topic** 栏输入 device/up，Qos 默认 0 即可，点击“确定”即订阅这个主题。



5、在 **Message** 下就可看到主机上报的数据。也可订阅主题 device/disconnect 查看设备断开连接的信息，需设备配置物联网相关选项，详细操作说明见附录 2。

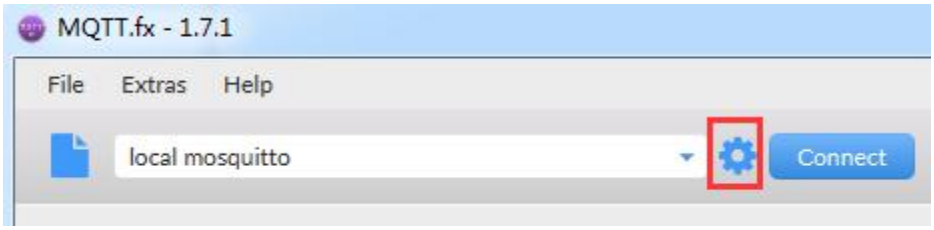


6、在 **Publish** 下的 **Topic** 栏输入控制命令的主题：device/control

可控制测试设备 GNC-NIO 的继电器 1~4 闭合（DO9~DO12），下发的控制命令的 JSON 格式请参考设备说明。

步骤四. 通过 MQTT.fx 客户端连接测试

安装并打开 MQTT.fx 客户端，点击配置按钮。



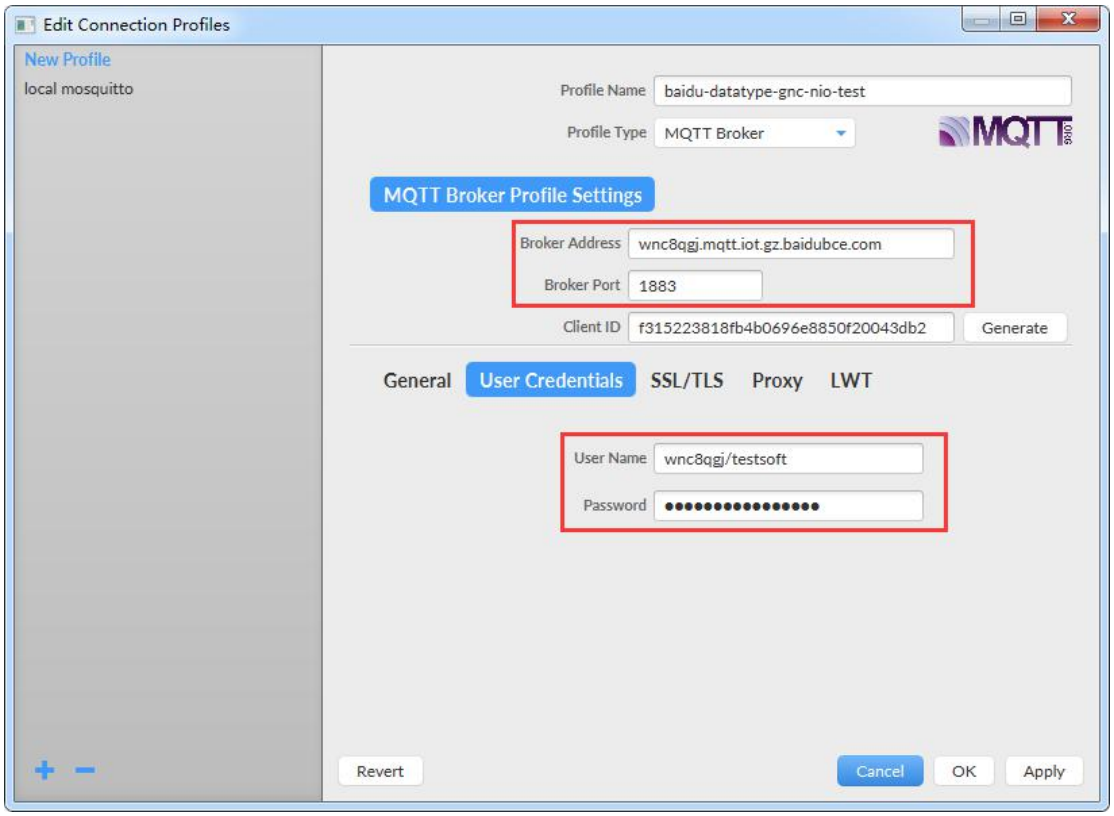
点击"+"，新建连接。以上述创建的 testsoft 用户为例，连接配置如下：

Profile Name：自定义

Profile Type：MQTT Borker

Broker Address：yourendpoint.mqtt.iot.gz.baiduce.com
Boker Port：1883
Clinet id：自定义或随机生成

Username：yourendpoint/设备名称，见用户列表
Password：为步骤一中，2.2.3 创建的 software 客户端身份密钥



Broker Address 和 Boker Port：

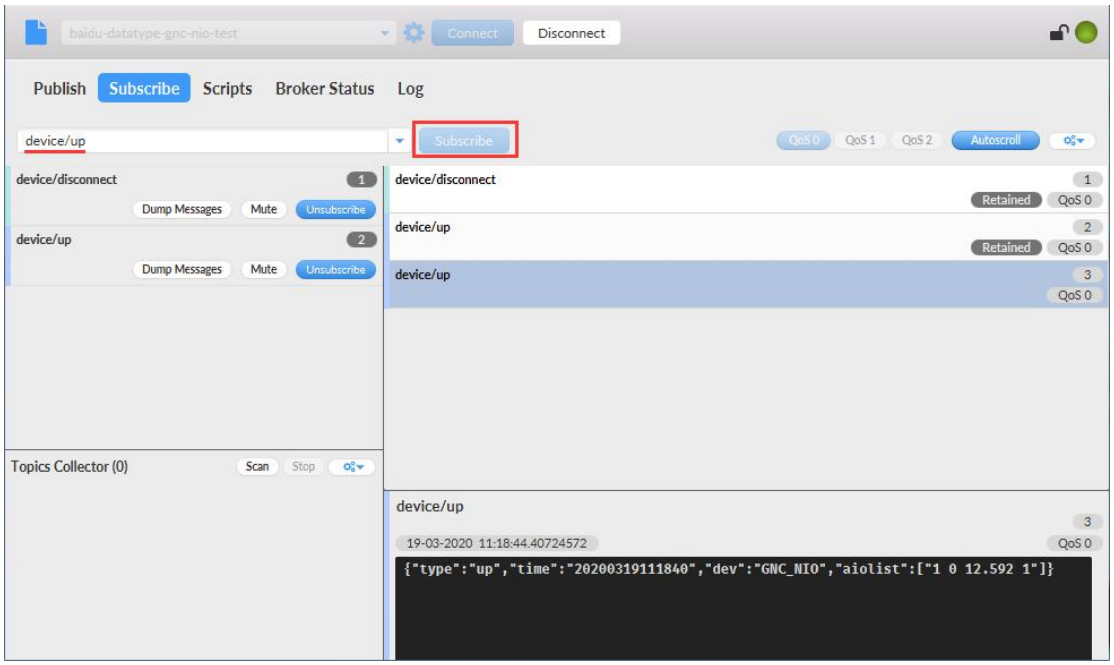
项目名称/Endpoint	类型	描述	地址
data_test wnc8qgj	数据型		tcp://wnc8qgj.mqtt.iot.gz.baidubce.com:1883 ssl://wnc8qgj.mqtt.iot.gz.baidubce.com:1884 wss://wnc8qgj.mqtt.iot.gz.baidubce.com:443

Username：

用户名	描述	创建时间
wnc8qgj/testsoft		2019-06-25 09:22:26

配置完成后，点击“Connect”，即可成功连接。

在 **Subscribe** 界面中订阅主题：device/up，即可在该界面看到设备的上报数据。也可订阅主题 device/disconnect 查看设备断开连接的信息。



步骤五. SSL/TLS 连接

上述步骤一到四，演示了网控物联网设备以 TCP 方式连接到百度天工数据型项目，并通过百度天工物接入平台和 MQTT 客户端进行双向通信。对于安全级别要求较高的场合，TCP 方式便不再适用，此时需要通过 SSL/TLS 连接云平台，以提高数据传输安全性。创建策略和用户，以及连接成功后进行在线调试等功能对于两种连接方式均相同，此处不多赘述。

网控设备的连接到百度天工数据型项目的物联网设置中，SSL/TLS 连接的配置类型分为三种，对应三个不同的安全级别，由低到高分别为 CA 签名的服务器（不强制证书检查），CA 签名的服务器（强制证书检查），自己签名的证书。

CA 签名的服务器用户身份：
以设备端为例，CA 签名的服务器（不强制证书检查）和 CA 签名的服务器（强制证书检查）两种连接方式的身份创建，与步骤一一致，即密码认证。

这里依然使用之前创建的用户“gnc_nio”来连接。

wnc8qgj/gnc_nio

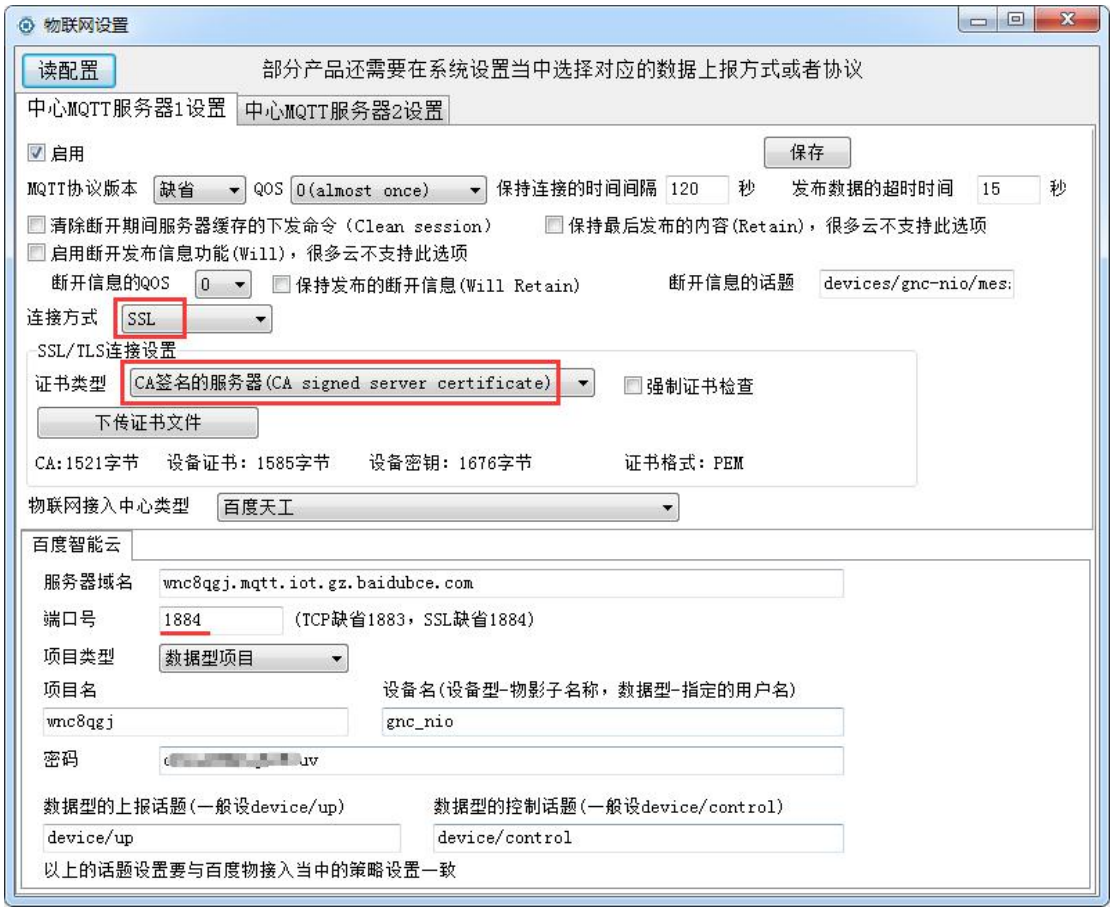
1、CA 签名的服务器（不强制证书检查）

连接方式：SSL

证书类型：CA 签名的服务器

端口号：1884

保存，重启即可。



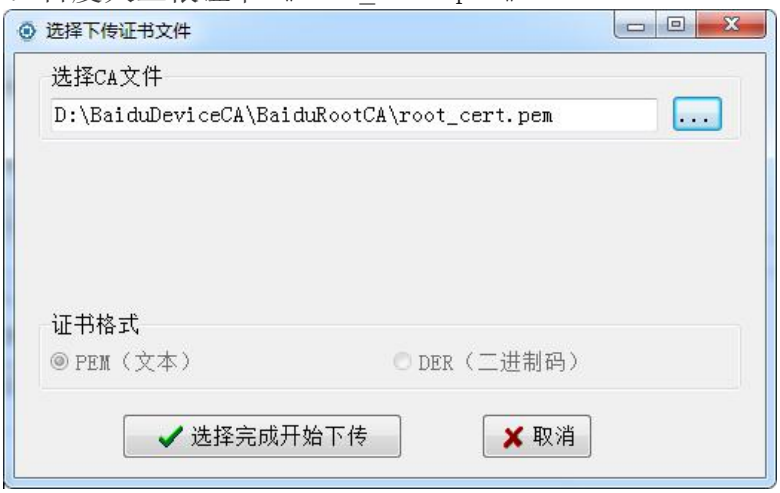
2、CA 签名的服务器（强制证书检查）

连接方式：SSL

证书类型：CA 签名的服务器

勾选强制证书检查。

下传证书文件：百度天工根证书《root_cert.pem》



端口号：1884

保存，重启即可（新下传的证书文件会覆盖旧文件）。

自己签名的证书用户身份：

设备端的 SSL/TLS 连接的配置为自己签名的证书时，创建身份选择证书认证。

同样的选择设备端策略 device_policy，然后在配置确认窗口“点击下载”证书及密钥。

会生成如图的证书文件，分别为设备证书、设备公钥、设备私钥和百度天工根证书。

设备的 SSL/TLS 配置要用到**设备证书、设备私钥和百度天工根证书**。

将 CERTIFICATE 这段复制到文本中另存为 clientcert.cer。

将 RSA PRIVATE KEY 这段复制到文本中另存为 prikey.key。

prikey.key

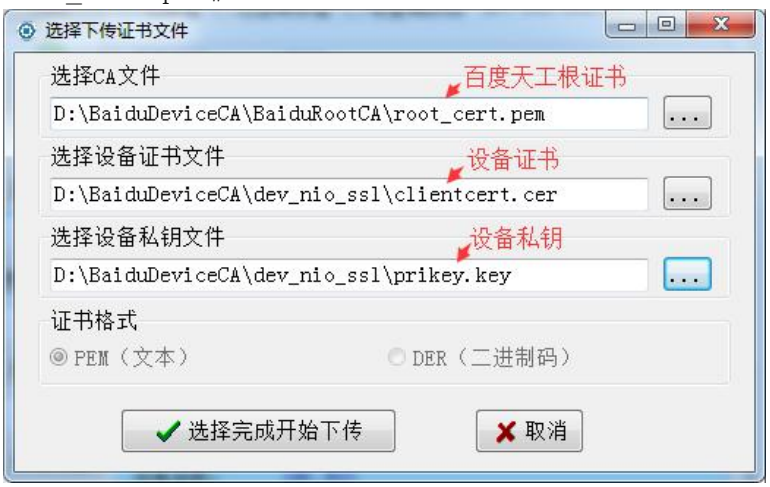
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoApPXdBt9bRuvdQTI5IAd8QkGb6/75dhrgo1N+ZBEWqDob7a
rp0iEA2RvofDTIVlMl27zPnImMBvBPKnSxbiyGjcb6P+tEC51GvfHhr9VbWRXtGF
PXC0370Ns5DaHxTQexziiO9steIj5hd3Wvt/JRHfvSHACBkyEJyDUVzOuIw3m1f0
Q8t4HVD2l8M/9LNQKCCvUzI4Ud5AnOnDFa5l7g6Gvlzioh2Yo+at5KWxtUyExCrp
zvbthQASKwFSrkXxsb6huFwZhE92aCVd3Bwg+nbkCHGF/g+K8cbmp62CoEXG34JY
LUOYsl0vQF/Xwu8lWZgqscqBaw/L831GGpcXmwIDAQABAoIBAGg4DpMzRkg5Zdxs
nMIPNArKShAR7f/ifxPNRfbPFRR4XpwYI2SOoz38+CoxUvcj71CrRb8n8n+24RVB
x7vYfXqw/swc6aMMe3dff/6k6NDF2pL6sl/eY4tIHAIRlFmlPlbN6p/t+sc/Ks2N
/oXbPWMwjpklv14Gulmi8skrPNtkPF08GFW3CvY7lDqV3/bzUYW4gye4MjAtvJtV
c2tGJL8TbWjeKk21S7IS4OHNhTNudZMVFm4uMsLMp6TcCnH/81ptd2DkOQmRtHdz
5v1B9CVgL7g9zx3bgFtBUrH/hJFWhVwatLTffZMvoT8Y85k+0m9MBinE1txy+8Ca
ERJqbwECgYEA1UmN9GBb9sAAWUOKIWj8j+xAHtSV92Jpt+phbBTGh9kVnygBwA8Z
bYnBOFW7ttHBwXWWwE9jjr8YtNCe8QHaJzA4Hl03ZpUz+TdOHNDyiMWvBylTJSOl
vEEEwUB8EtstV3fPwjqhBLiObYVSMD6VejdgOmoYECAC3k8b8UvlFEECgYEAwBb6
WWv5m8w/BkOecOxEvgtTbb0InxWIloLklC7VCEqY1MxtnXhr9+dM5iTuhVOL3E+h
aNV7J61+ZuGmd7YfxWew/reUyR4L5JiryXbjYXsRa7Do5n/q6nJRH9pG+r9zTo3V
x46g4kA+5n8dtsOF4PBMCVe4AVrsV/8QsM7dxNsCgYB3r5bhE1GH3aZUcPoKVYek
m8Y/hrvA3pDEi9mvdNkTUlY3wZN52v9B4JN0sWds57f6f6ngsKwFZmbO0GLgi1GH
vB9Bqr1z6zYHG2nR8c6nwYa+Vgo6RQ6z3Sh16WG2kxeWhb0oGQ5SP95sxuuf9v6a
Xoi5Pt/R7KSva2UauqQKAQKBgFvU4FyNrSgZbevtubpcicSdH4Zv/8YmAkWKUAKz
nO640vWwwZqtrlg2wOGpuEoPFeb+Prkijhz66Vn/+Jh0fh3eo5QyabP4ZFEl18KZ
zryUnFByo/VGJCVu/2+N568KhfKBBjm/6xQfCLMjBC6SrNdLqd4xjGtBb4nmC7Gr
RARPAoGBAM9JKR14aJUBt2XLGk0TcLiFPqo4WH1fDowQQkTPablv5Rx8ciYOOEZU
Ni6zlI11SftoxxcKSYFxF9SBkOc1Dey/h+tHaGPQr9juzYUpaGu0UhBYXaiFa3nP
G1gtYvfjT3kPUO9qnBPGuObAX1FoXvgqmcIt6e59XNM+vpMEI71e
-----END RSA PRIVATE KEY-----
```

开头下载的百度天工根证书《root_cert.pem》与这里复制文本另存得到的证书相同，可略过。

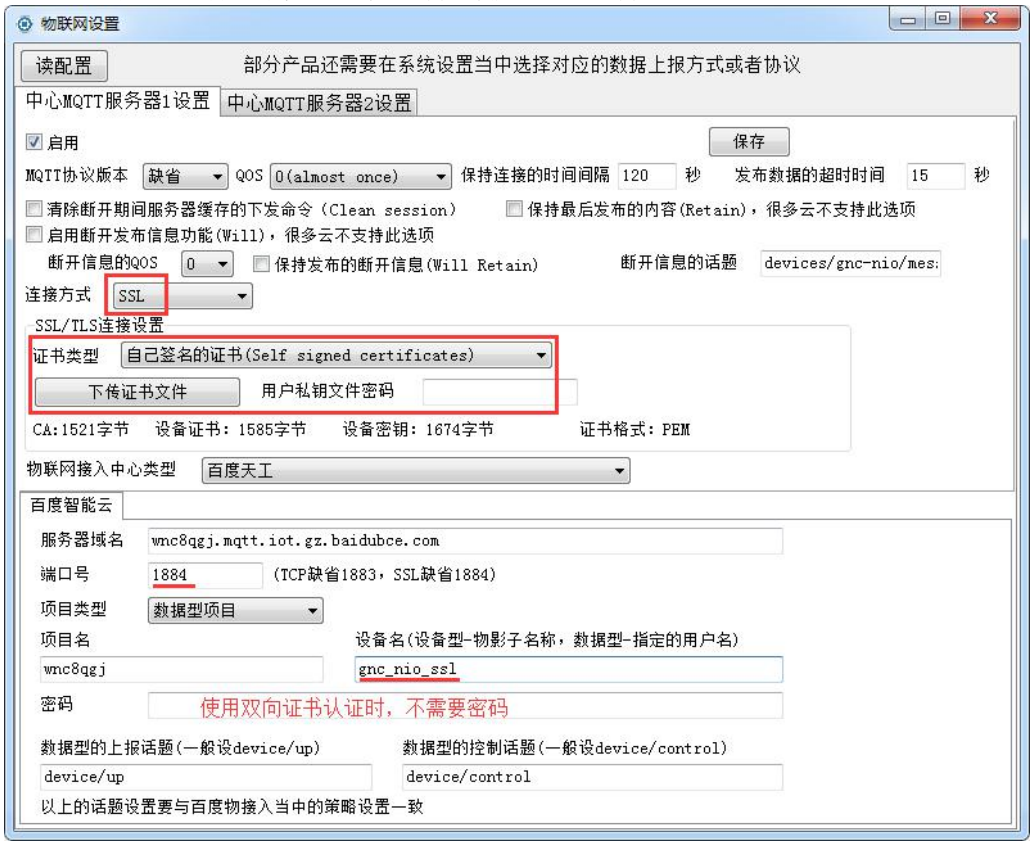
再创建一个身份设置为上述 device_ssl 的设备端用户 gnc_nio_ssl 用于设备配置。

3、自己签名的证书

连接方式：SSL
证书类型：自己签名的证书
下传证书文件：设备证书《clientcert.cer》、设备私钥《prikey.key》和百度天工根证书《root_cert.pem》



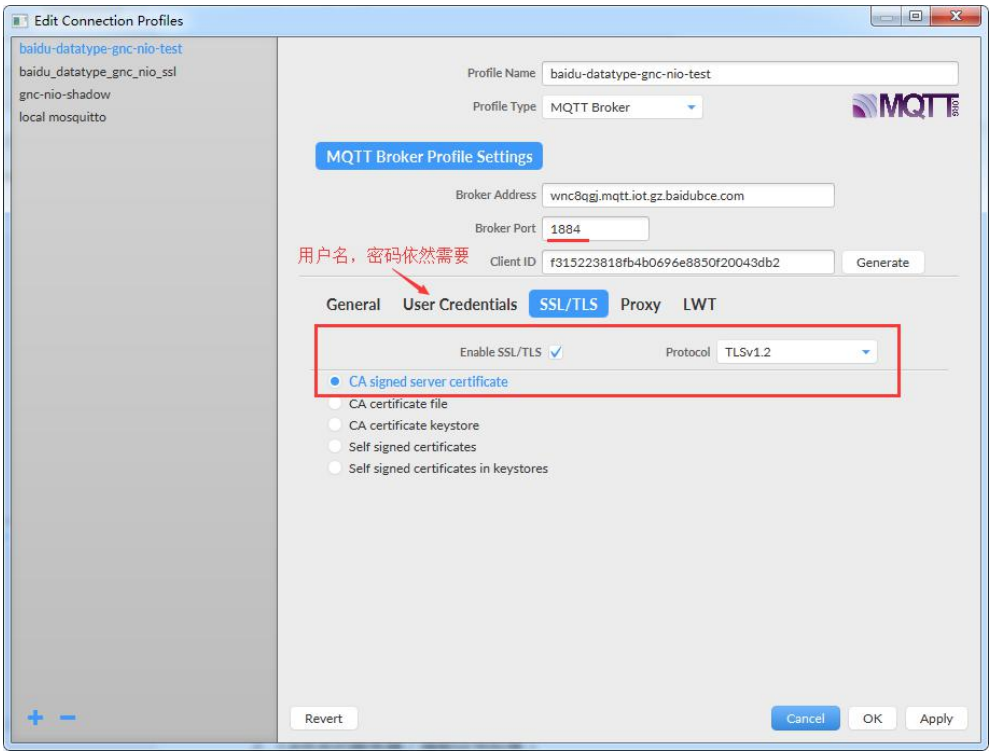
端口号：1884
设备名：设置了证书认证身份的用户名
密码：此时双向证书作为密码，此处为空。
保存，重启即可（新下传的证书文件会覆盖旧文件）。



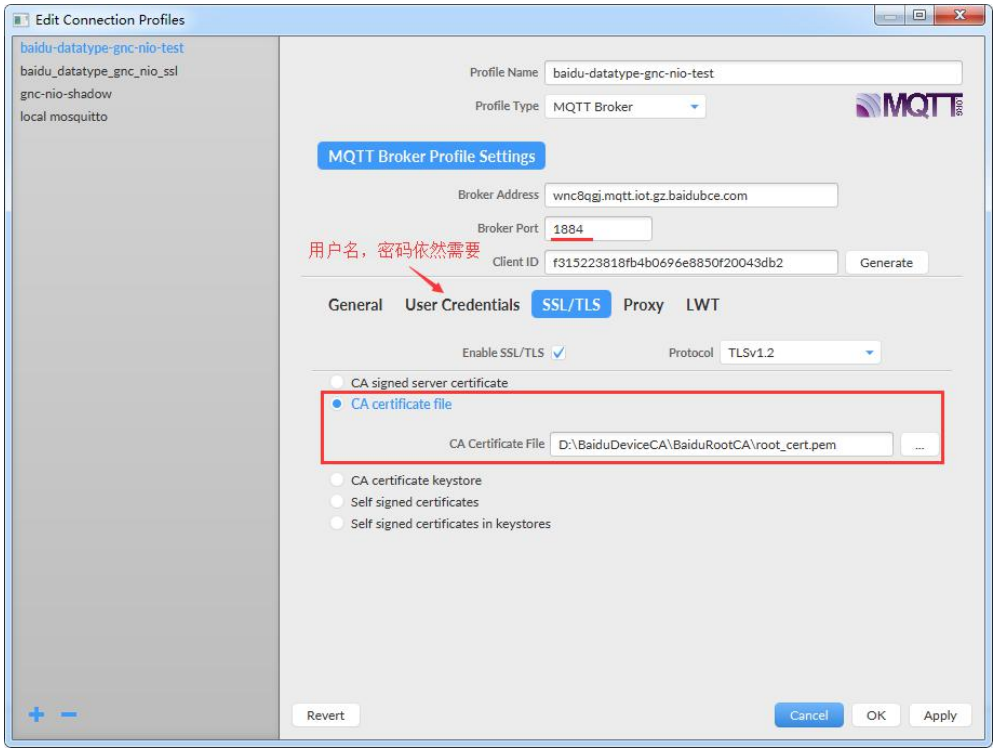
同理，MQTT 客户端也可以 SSL/TLS 方式连接到百度天工物联网平台进行测试。CA 签名的服务器统一使用之前创建的 testsoft 用户。

wnc8qgj/testsoft

1、CA 签名的服务器（不强制证书检查）



2、CA 签名的服务器（强制证书检查）



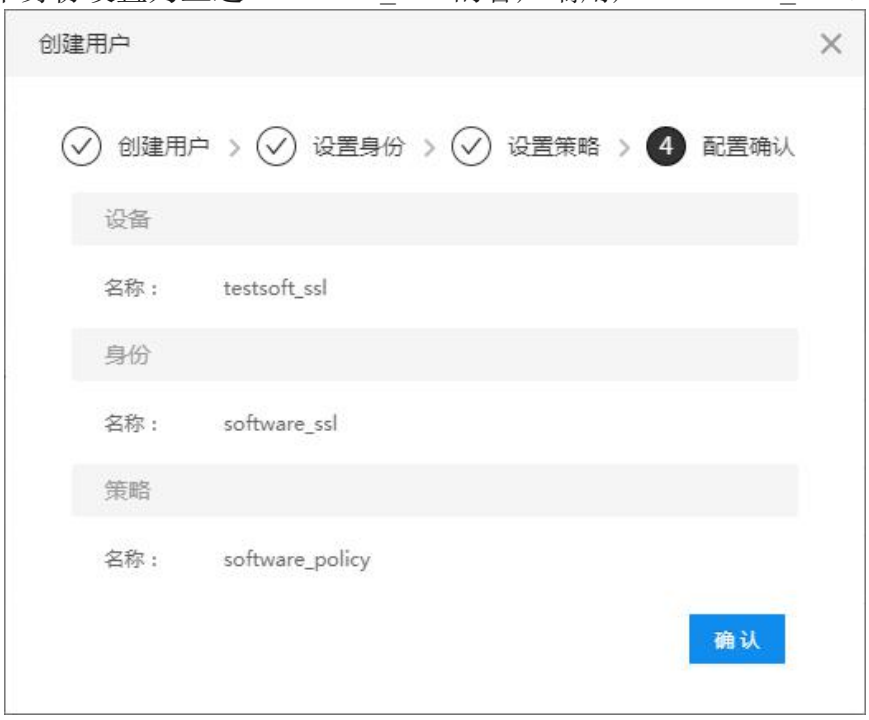
3、自己签名的服务器

创建一个证书认证的客户端身份 software_ssl。

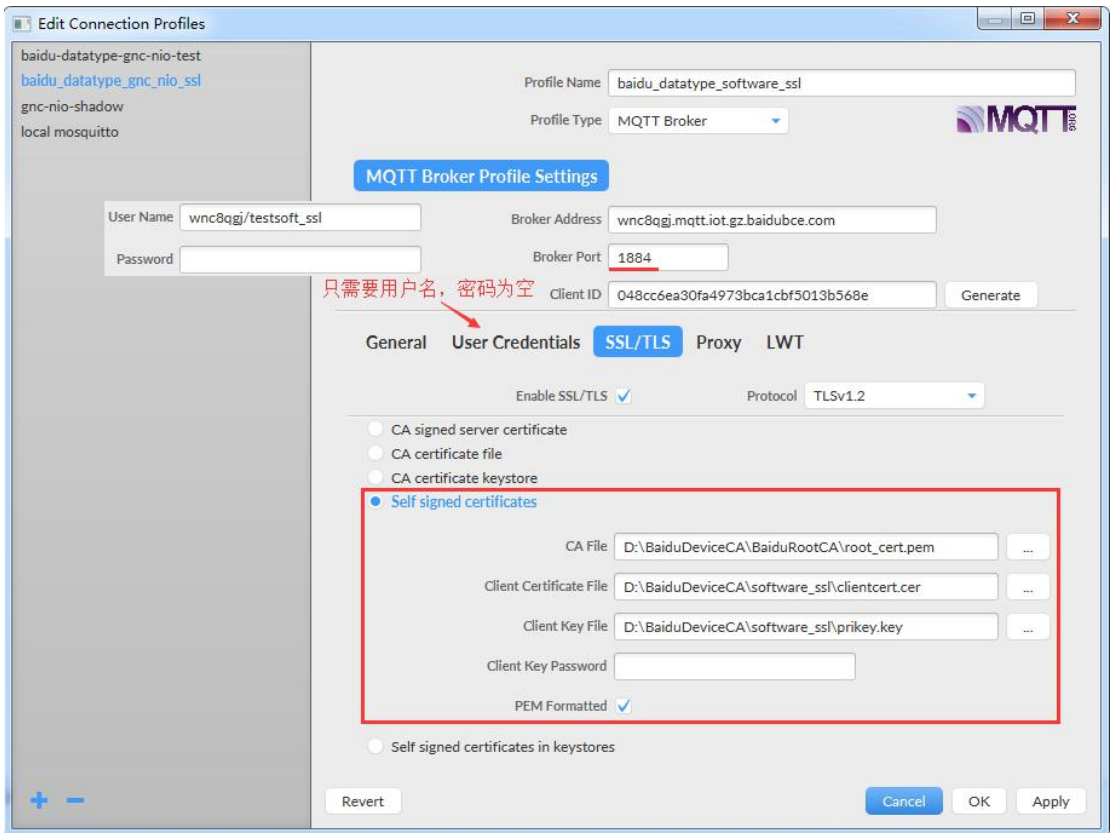
绑定客户端策略 software_policy，然后下载证书及密钥。

与设备端一样操作，得到 MQTT 客户端连接的设备证书、设备私钥和百度天工根证书。

再创建一个身份设置为上述 software_ssl 的客户端用户 testsoft_ssl。



MQTT 客户端的连接配置：



附录 1：GNC-NIO 物模型属性说明

每一条属性表示 GNC-NIO 的一个数据监测点，添加的属性名称和数据类型请严格参照物模，否则会导致设备上报数据/下发控制异常。以下给出主要属性和全部物模型快照。

GNC-NIO 模拟量输入 AI1~AI8 属性：

GNC-NIO 开关量输入 DI1~DI8 属性：

GNC-NIO 继电器输出 DO9~DO12 属性：

GNC-NIO 输入输出的告警：

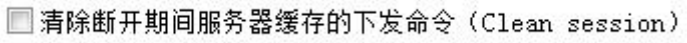
GNC-NIO 全部物模型：

属性名称	显示名称	类型	默认值	单位
AI1	AI1	number		
AI1Warn	AI1Warn	number		
AI2	AI2	number		
AI2Warn	A21Warn	number		
AI3	AI3	number		
AI3Warn	AI3Warn	number		
AI4	AI4	number		
AI4Warn	AI4Warn	number		
AI5	AI5	number		
AI5Warn	AI5Warn	number		
AI6	AI6	number		
AI6Warn	AI6Warn	number		
AI7	AI7	number		
AI7Warn	AI7Warn	number		
AI8	AI8	number		
AI8Warn	AI8Warn	number		
DI1	DI1	number		
DI1Warn	DI1Warn	number		
DI2	DI2	number		
DI2Warn	DI2Warn	number		
DI3	DI3	number		
DI3Warn	DI3Warn	number		
DI4	DI4	number		
DI4Warn	DI4Warn	number		
DI5	DI5	number		
DI5Warn	DI5Warn	number		
DI6	DI6	number		
DI6Warn	DI6Warn	number		
DI7	DI7	number		
DI7Warn	DI7Warn	number		
DI8	DI8	number		
DI8Warn	DI8Warn	number		
DO9	DO9	number		
DO9Warn	DO9Warn	number		
DO10	DO10	number		
DO10Warn	DO10Warn	number		

附录 2：数据型项目设备下线与遗嘱消息

百度天工数据型项目对于 MQTT 协议的一些特性支持较好，这里对网控设备物联网的 MQTT 协议部分的配置的使用作简要说明。MQTT 协议版本，QOS，保持连接的时间间隔（Keep Alive Time）和发布数据的超时时间（Timeout）略过。

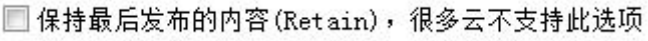
1、Clean session



未启用：MQTT 客户端发布的控制命令，物接入服务将该消息保留 24 小时，设备再次连接后控制命令立即生效。

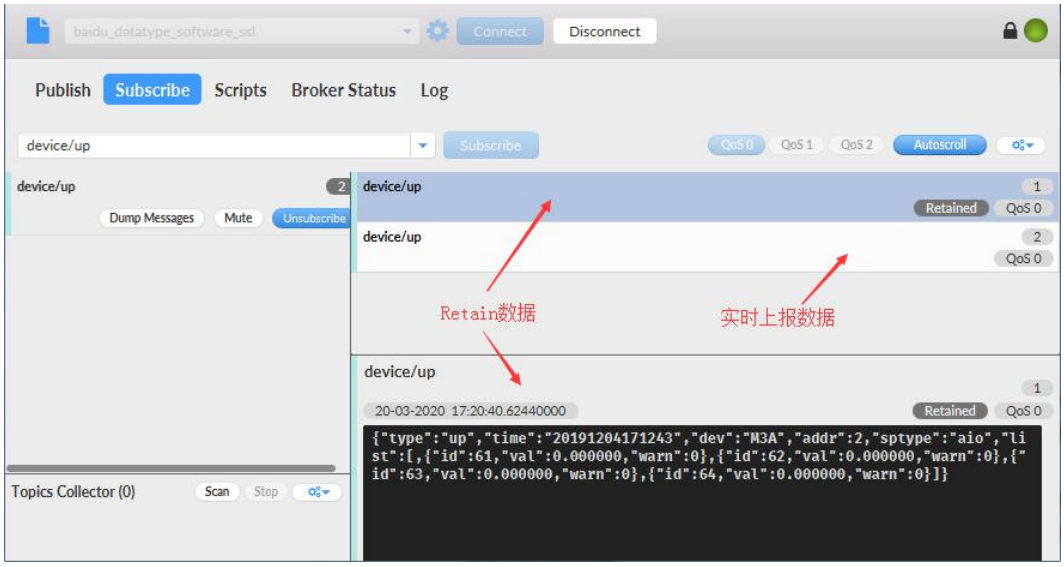
启用：设备断开连接期间，MQTT 客户端发布的控制命令则被服务器清除，设备再次连接后控制命令不会生效。

2、Retain

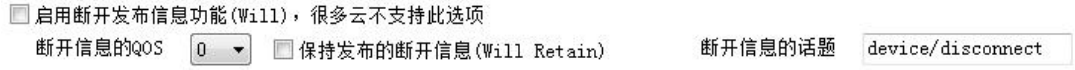


未启用：当有新的 MQTT 客户端订阅了主题 device/up 时，只能接收到设备向该主题发布的实时数据，若设备断开连接，则 MQTT 客户端只能等待设备重新连接发布数据。

启用：服务器会给设备断开连接之前，往主题 device/up 发布的最后一条数据添加一个 Retain 标记，当有新的 MQTT 客户端订阅该主题时，会立即接收到带有 Retain 标记的数据。



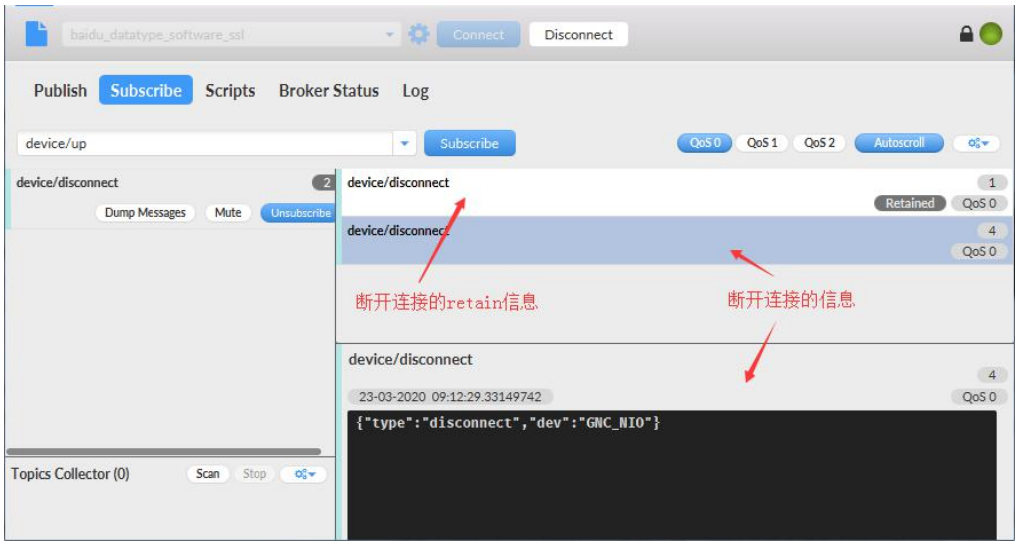
3、Will 功能



遗嘱功能与断开信息的话题（遗嘱主题）配合使用，须与策略设置的主题一致，即 device/disconnect。

启用 Will 功能：测试 MQTT 客户端首先订阅遗嘱主题，当设备断开连接后，由服务器向遗嘱主题发送设备预定义的遗嘱消息，通知已订阅了遗嘱主题的客户端，该设备已下线。（设备下线 3 倍的 Keep Alive Time 时间后，服务器发出遗嘱消息，120 秒时为 6 分钟）

启用 Will Retain：服务器会将设备最后一次断开连接时的遗嘱消息标记 Retain，当有新的 MQTT 客户端订阅遗嘱主题时，会立即收到设备最近一次下线的遗嘱消息。


baidu_datatype_software_ssl
Connect
Disconnect
Publish
Subscribe
Scripts
Broker Status
Log
device/up
Subscribe
QoS 0
QoS 1
QoS 2
Autoscroll
device/disconnect
2
Dump Messages
Mute
Unsubscribe
device/disconnect
1
Retained
QoS 0
device/disconnect
4
QoS 0
断开连接的retain信息
断开连接的信息
device/disconnect
4
23-03-2020 09:12:29.33149742
QoS 0
{"type":"disconnect","dev":"GNC_NIO"}
Topics Collector (0)
Scan
Stop