AP NOTE
Ver.3

iGS01S/iGS02E/iGS03 Google Cloud IoT Core Guide

Introduction

This application note provides a guide to connect Google Cloud IoT Core with iGS01S/iGS02E/iGS03 via mqtt bridge.

Get Started

The first step is to ensure you have a Google Cloud IoT Core account set up with IoT core.
Follow the IoT Core Quick start to create a Cloud IoT Core device registry and register a device.

After following the instructions in the Quickstart guide, you should have PROJECT_ID, REGION, REGISTRY_ID and DEVICE_ID settings. These settings will be used to configure iGS01S/iGS02E/iGS03. We suggest users to test your configurations on PC first to confirm your settings are correct.

Below shows the gcloud commands for publish and subscribe to verify your settings:
(Your pub/sub topics may be different from the example, please use your settings accordingly)

Publish some data to projects/igs01s-214703/topics/pub

```
$ gcloud pubsub topics publish projects/igs01s-214703/topics/pub  –message="TEST1"
```

Then check if you can receive the published data

```
$ gcloud pubsub subscriptions pull --auto-ack  projects/igs01s-214703/subscriptions/igs01s –limit=100
```

Configuration on iGS01S/iGS02E

The Google Cloud IoT Core uses JSON Web Tokens (JWT) for authentication.

The device uses a private key to sign a JSON Web Token (JWT) for authentication so the user must **upload the private key** to the device. In addition, the JWT requires **enabling NTP** settings to get correct expired time.

Notice, the firmware OTA is required for iGS01S/iGS02E to ensure the function to publish messages to Google Cloud IoT Core as expected.

Below shows the steps to config IGS02E to publish data to Google Cloud IoT Core.

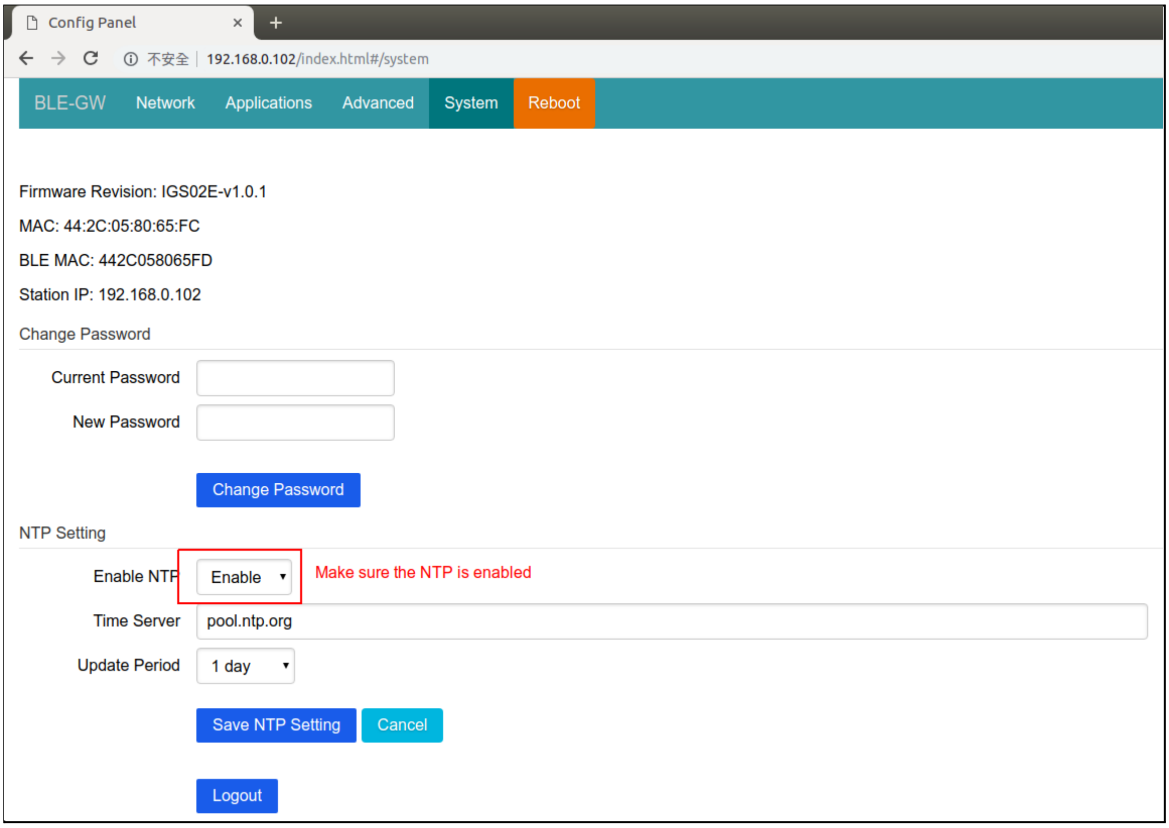
1. Enable NTP via the system tab of webUI.
2. Upload private key via advanced table of webUI
3. Configure the device as MQTT client with below settings:

   - MQTT HOST mqtt.2030.ltsapis.goog

- MQTT PORT 8883
- MQTT PUBTOPIC /devices/{DEVICE_ID}/events
- MQTT CLIENTID projects/{PROJECT_ID}/locations/{REGION}/registries/{REGISTRY_ID}/devices/{DEVICE_ID}
- MQTT USERNAME unused
- MQTT PASSWORD {PROJECT_ID}
- Enable MQTTS
- Select Google-Cloud-IoT-Core RootCA
- Disable use certificate

Note, the standard authenticate method is using JWT in mqtt password field. Due to the very short expiration time of the JWT, we support runtime generation of the JWT. So users need to set “PROJECT_ID” in the password field then the gateway will automatically generate the JWT as password for connecting the server.

Below shows the screenshot of IGS02E settings:



Firmware Revision: IGS02E-v1.0.1

MAC: 44:2C:05:80:65:FC

BLE MAC: 442C058065FD

Station IP: 192.168.0.102

Change Password

Current Password

New Password

Change Password

NTP Setting

Enable NTP: Enable

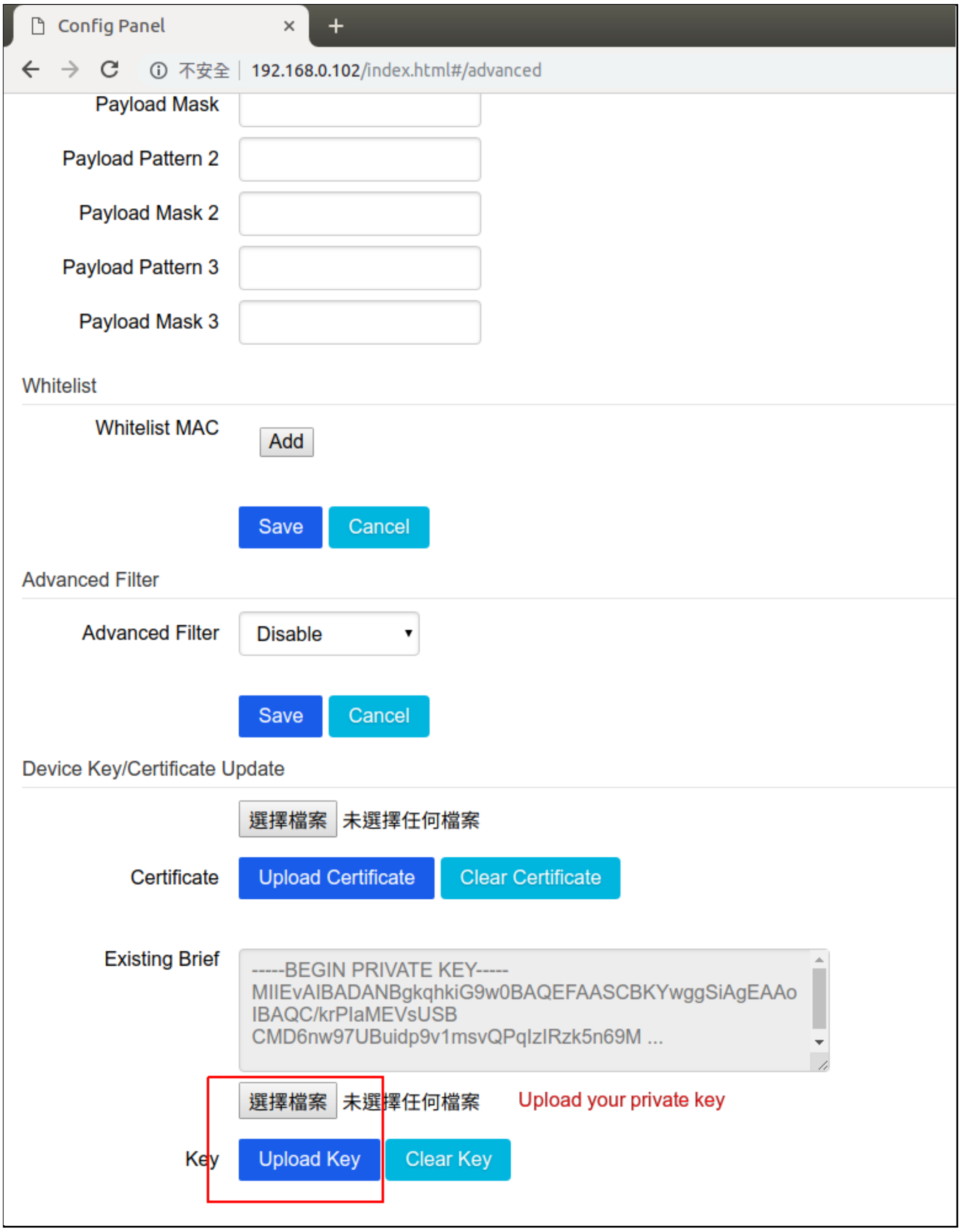
Make sure the NTP is enabled

Time Server: pool.ntp.org

Update Period: 1 day

Save NTP Setting   Cancel

Logout



Payload Mask

Payload Pattern 2

Payload Mask 2

Payload Pattern 3

Payload Mask 3

Whitelist

Whitelist MAC Add

Save Cancel

Advanced Filter

Advanced Filter: Disable

Save Cancel

Device Key/Certificate Update

選擇檔案 未選擇任何檔案

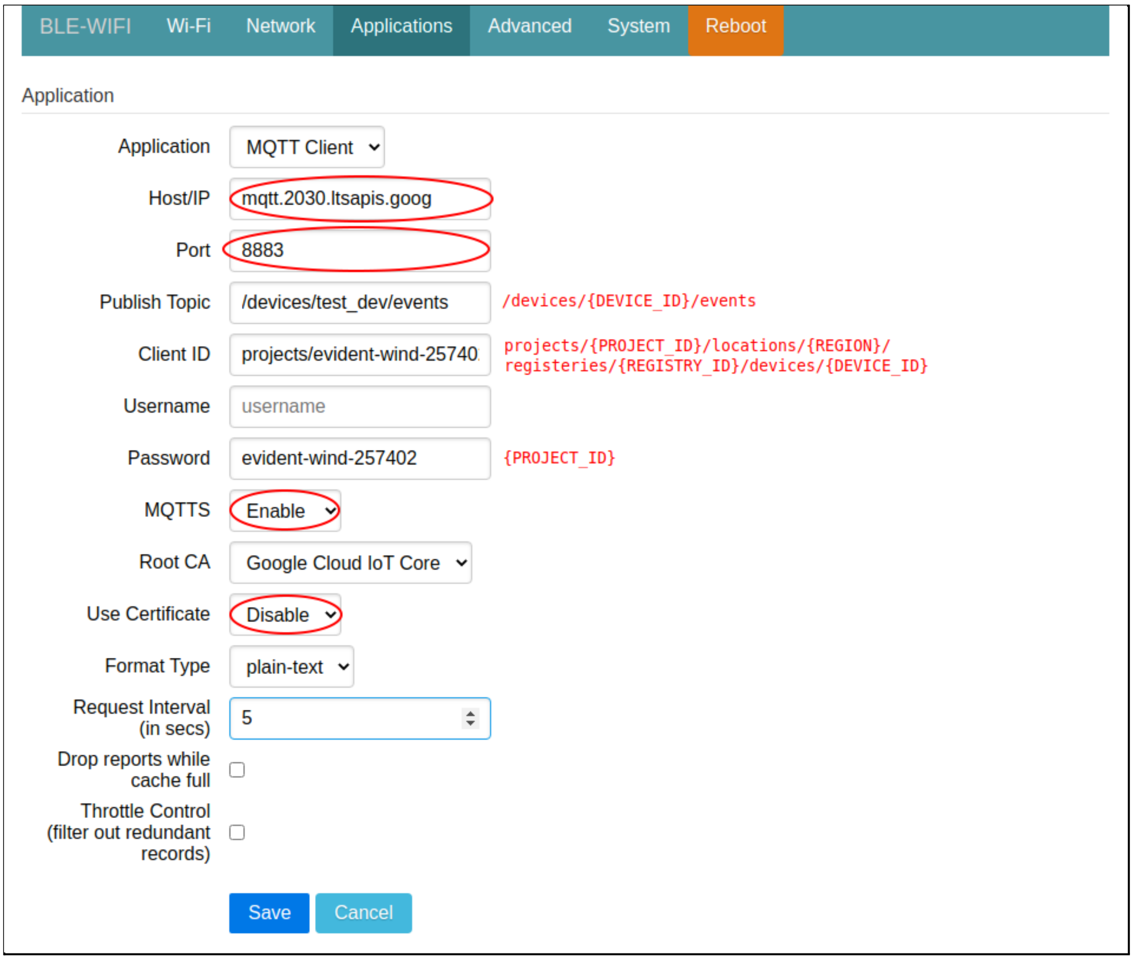
Certificate: Upload Certificate | Clear Certificate

Existing Brief:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAo
IBAQC/krPlaMEVsUSB
CMD6nw97UBuidp9v1msvQPqlzIRzk5n69M ...
```

選擇檔案 未選擇任何檔案 Upload your private key

Key: Upload Key | Clear Key



Application

Application	MQTT Client	
Host/IP	mqtt.2030.ltsapis.goog	
Port	8883	
Publish Topic	/devices/test_dev/events	/devices/{DEVICE_ID}/events
Client ID	projects/evident-wind-25740	projects/{PROJECT_ID}/locations/{REGION}/ registeries/{REGISTRY_ID}/devices/{DEVICE_ID}
Username	username	
Password	evident-wind-257402	{PROJECT_ID}
MQTTS	Enable	
Root CA	Google Cloud IoT Core	
Use Certificate	Disable	
Format Type	plain-text	
Request Interval (in secs)	5	
Drop reports while cache full	□	
Throttle Control (filter out redundant records)	□	

Configuration on iGS03 Series

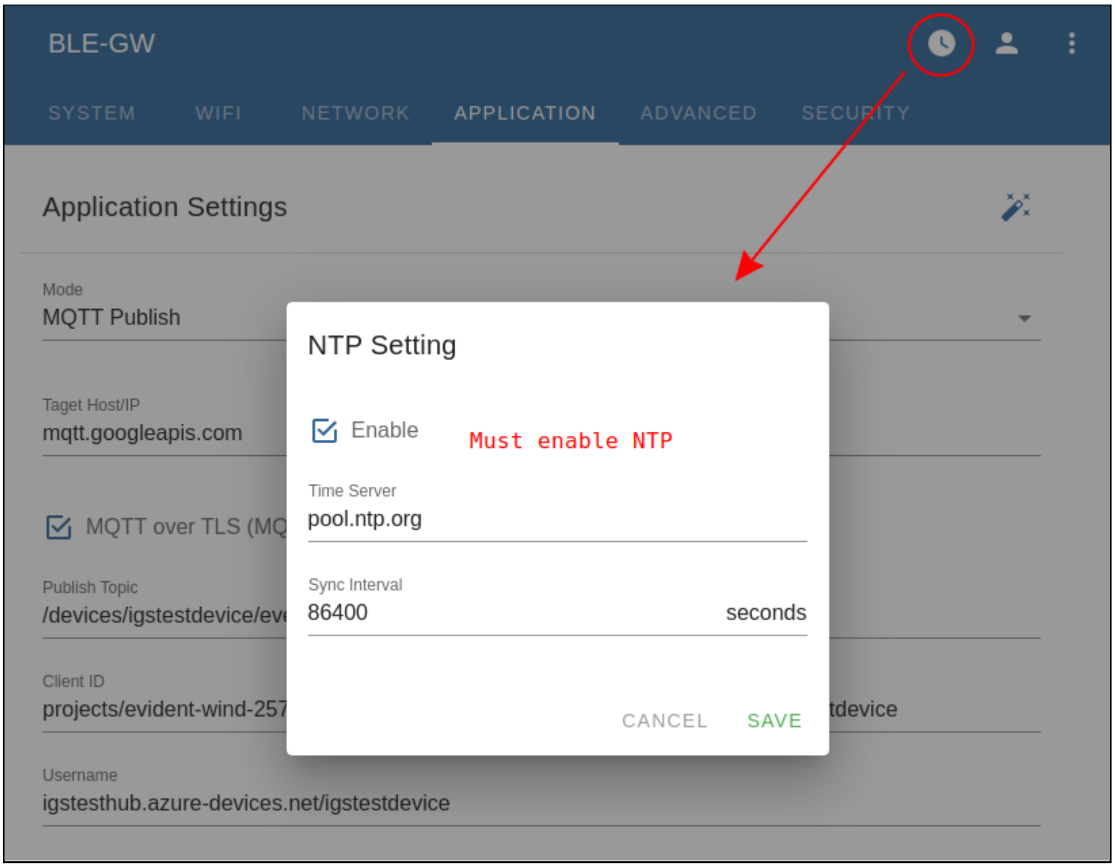
Please be mindful that the current primary root certificate (GlobalSign R2) will expire on December 15, 2021.
Please upgrade iGS03 devices to v1.0.9.0+ to ensure the function to publish messages to Google Cloud IoT Core works as expected.
The wizard now uses "mqtt.2030.ltsapis.goog" instead of "mqtt.googleapis.com" by default.

The configuration is basically the same as iGS01S/iGS02E in the previous section. But iGS03 Series provides a new functionality called ‘Cloud IoT Helper’ to make things easier. You can manually configure the MQTT settings like iGS01S/iGS02E, or try to use the helper.

The steps to config IGS03 using the ‘Cloud IoT Helper’.

1. Enable NTP
2. Open ‘Cloud IoT Helper’, choice the ‘Google Cloud IoT Core’
3. Enter the PROJECT_ID, REGION, REGISTRY_ID and DEVICE_ID on helper
4. Upload the private key of the device on helper
5. Click ‘OK’ on helper, review the configurations
6. Click ‘SAVE’ to save the configuration, click ‘reboot’ to apply the new settings

Screenshots for iGS03 series.



Mode
MQTT Publish

Taget Host/IP
mqtt.googleapis.com

☑ MQTT over TLS (MQ

Publish Topic
/devices/igstestdevice/eve

Client ID
projects/evident-wind-257 … tdevice

Username
igstesthub.azure-devices.net/igstestdevice

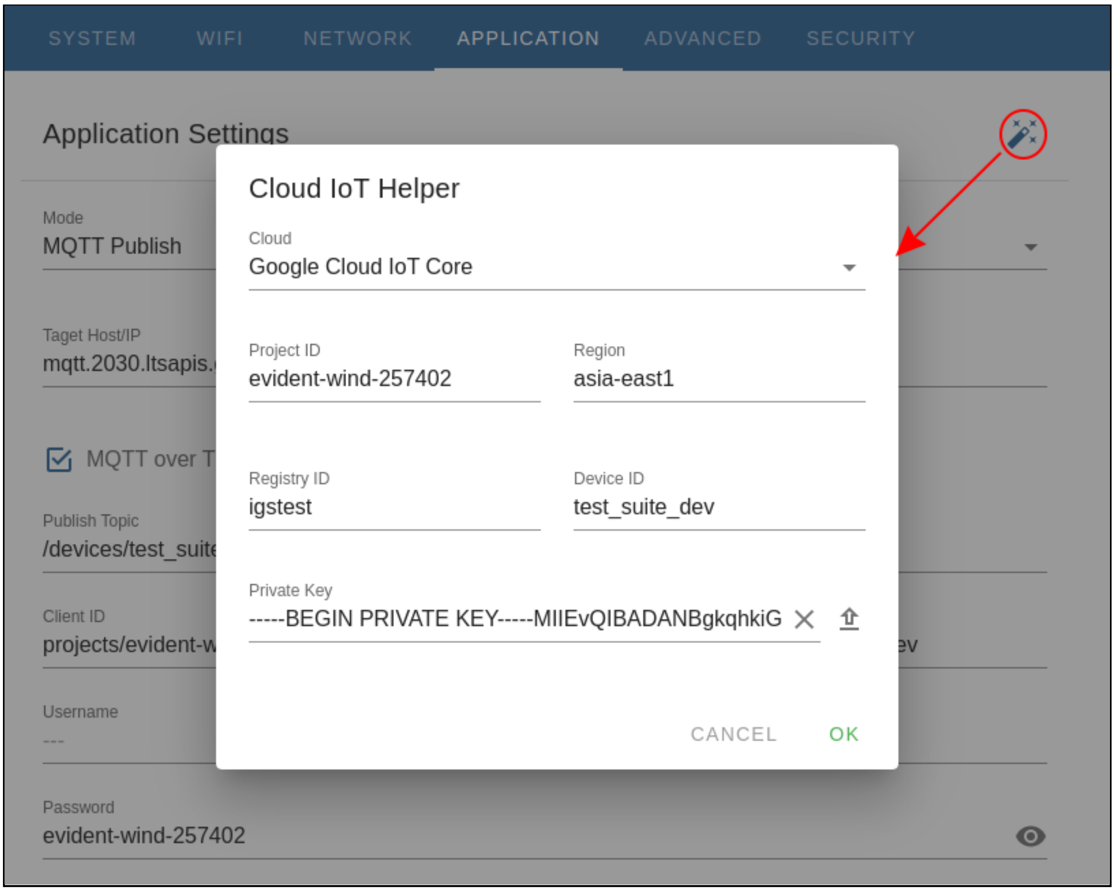
NTP Setting

☑ Enable

Must enable NTP

Time Server
pool.ntp.org

Sync Interval
86400 seconds



Application Settings

Mode
MQTT Publish

Taget Host/IP
mqtt.2030.ltsapis.

☑ MQTT over T

Publish Topic
/devices/test_suite

Client ID
projects/evident-w

Username

Password
evident-wind-257402

Cloud IoT Helper

Cloud
Google Cloud IoT Core

Project ID
evident-wind-257402

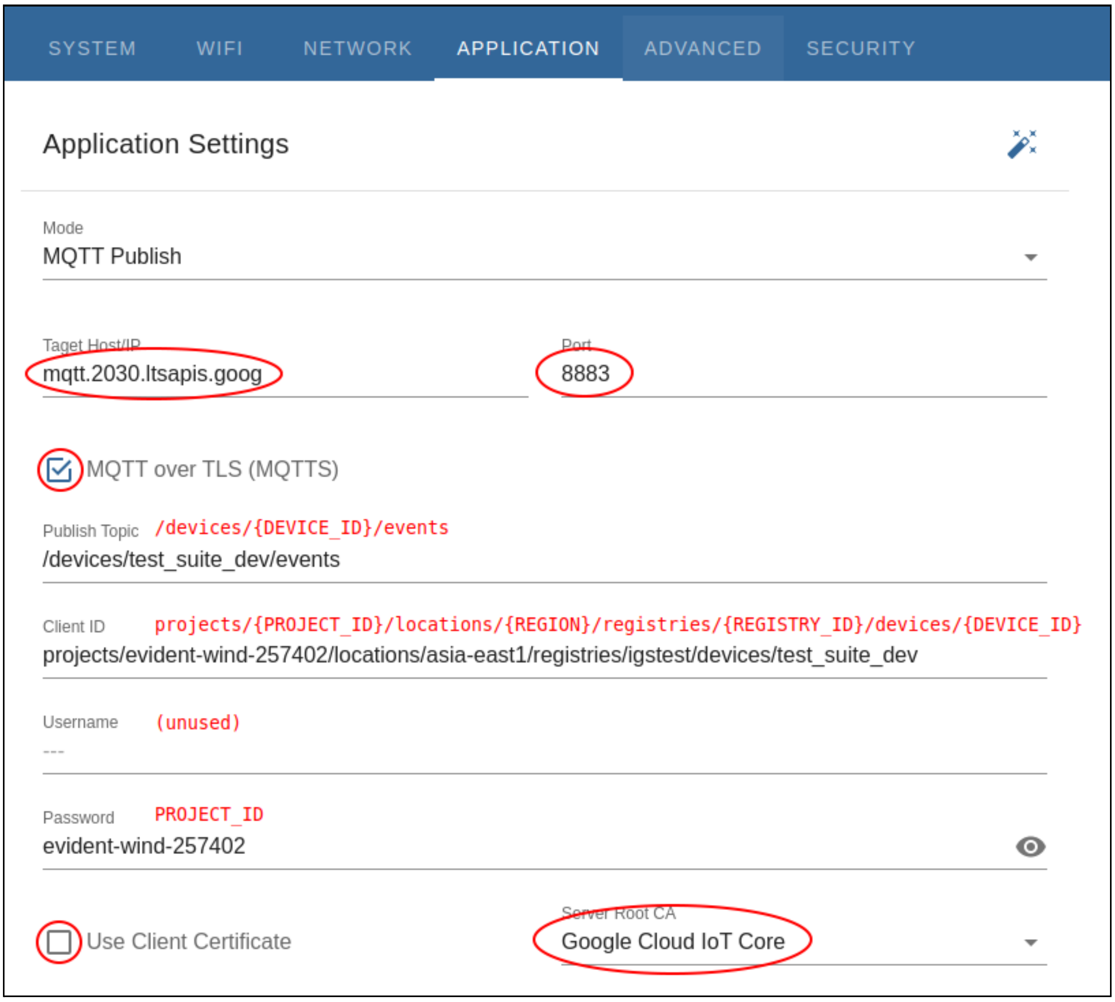
Region
asia-east1

Registry ID
igstest

Device ID
test_suite_dev

Private Key
-----BEGIN PRIVATE KEY-----MIIEvQIBADANBgkqhkiG

Choose ‘Google Cloud IoT Core’, fill PROJECT_ID, REGION, REGISTRY_ID and DEVICE_ID, upload the device private key.



Application Settings

Mode
MQTT Publish

Taget Host/IP
mqtt.2030.ltsapis.goog

Port
8883

☑ MQTT over TLS (MQTTS)

Publish Topic `/devices/{DEVICE_ID}/events`
/devices/test_suite_dev/events

Client ID `projects/{PROJECT_ID}/locations/{REGION}/registries/{REGISTRY_ID}/devices/{DEVICE_ID}`
projects/evident-wind-257402/locations/asia-east1/registries/igstest/devices/test_suite_dev

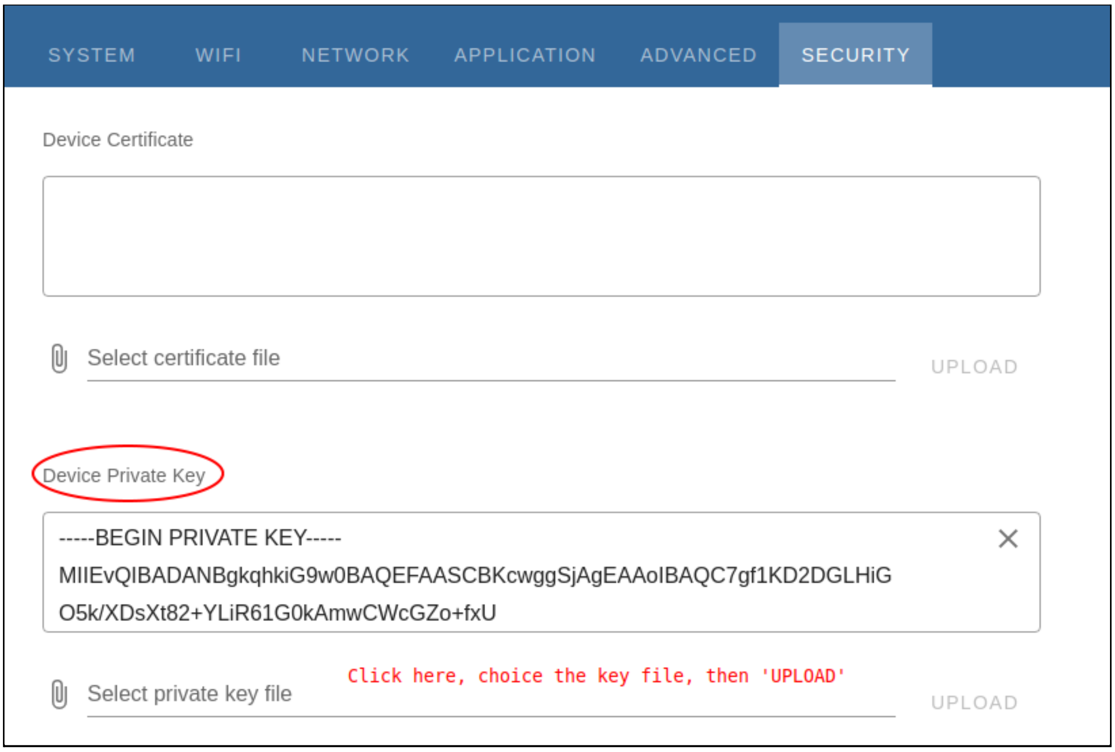
Username `(unused)`

Password `PROJECT_ID`
evident-wind-257402

□ Use Client Certificate

Server Root CA
Google Cloud IoT Core

The ‘Cloud IoT Helper’ will fill the settings for you, or you can input the settings manually.



Device Certificate

Select certificate file

Device Private Key

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7gf1KD2DGLHiG
O5k/XDsXt82+YLiR61G0kAmwCWcGZo+fxU
```

Select private key file
`Click here, choice the key file, then 'UPLOAD'`

The device key should already be uploaded on ‘Cloud IoT Helper’. Or you can upload the key in the ‘SECURITY’ tab if you did not use the helper.

Revision History

DATE	REVISION	CHANGES
Apr 8, 2019	1	Initial release
Jul 22, 2021	2	Add iGS03 support
Aug 6, 2021	3	Update MQTT host to use LTE domain