AP NOTE 002
Ver.1

iGS01S/iGS02E Azure IoT Hub Guide

Introduction

This application note provides a step-by-step setup to connect iGS01S/iGS02E with Azure IoT Hub. Azure-IoT allows Symmetric Key or X.509 Certificates for internal authorization (https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-security).
Both should work with IGS01S/iGS02E.

References

For new users of Azure IoT Hub, please check below link first:
https://github.com/intel-iot-devkit/iot-samples-cloud-setup/blob/master/azure-mqtt.md
Above link also provides a sastoken program to generate SAS token for connecting Azure IoT Hub.

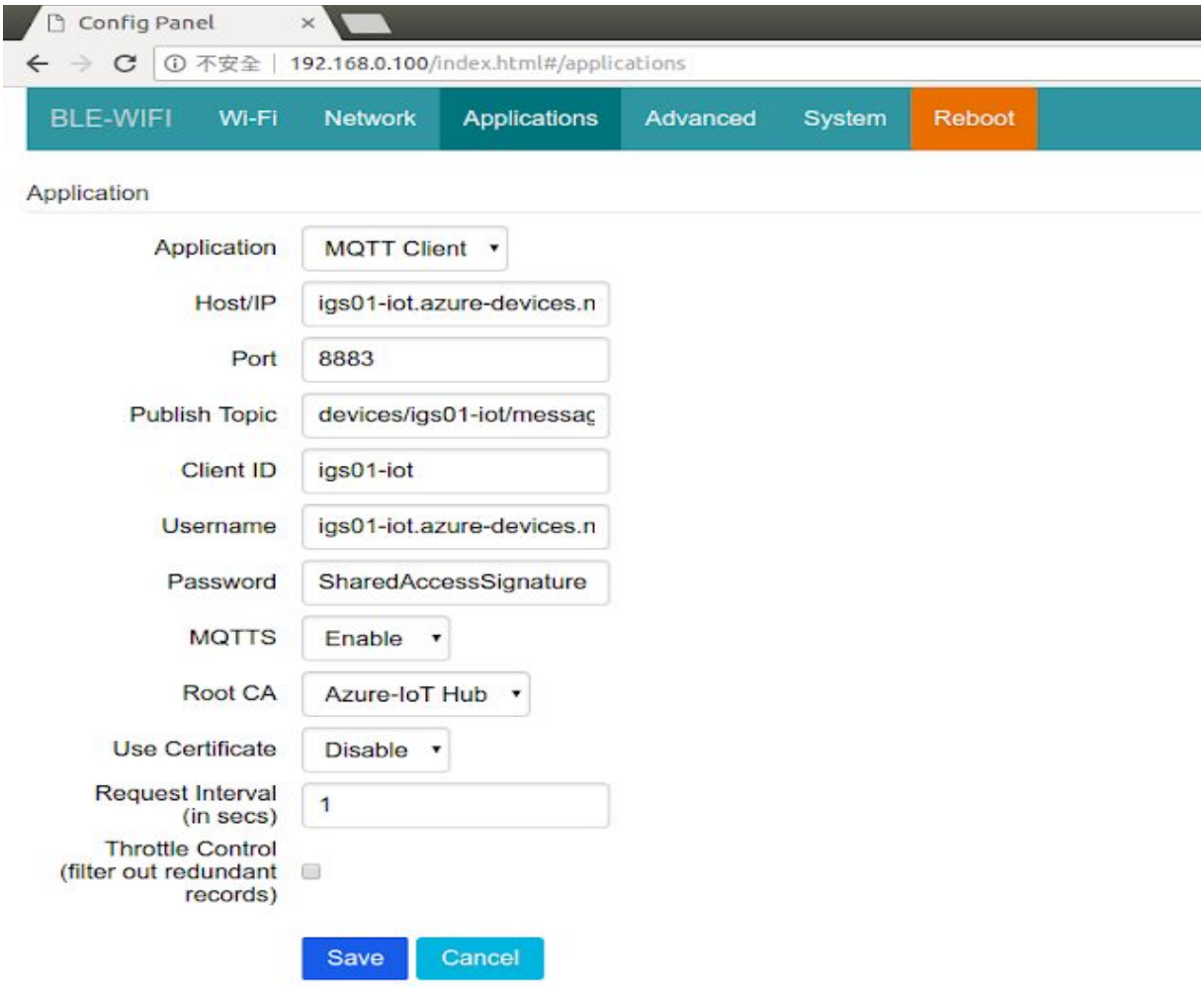
We also suggest users to test your configurations on PC first to confirm your settings are correct.
You can download the mosquitto tool to test connecting Azure IoT Hub with mqtt.
https://mosquitto.org/download/

Below shows an example to publish “hello” message to azure IoT using mosquitto tool.

```
$ mosquitto_pub -h igs01.azure-devices.net -p 8883 -i igs01 -t
"devices/igs01/messages/events/" -u "igs01.azure-devices.net/igs01" -P
"SharedAccessSignature
sr=igs01.azure-devices.net%2Fdevices%2Figs01&sig=E0Oxjv4uctk9ItknayEe4ED5aczXwELkC%2BhaBhjrfg
A%3D&se=1486135461"
 --capath /etc/ssl/certs/ --tls-version tlsv1 -d -V mqttv311 -q 0  -m
"hello"
```

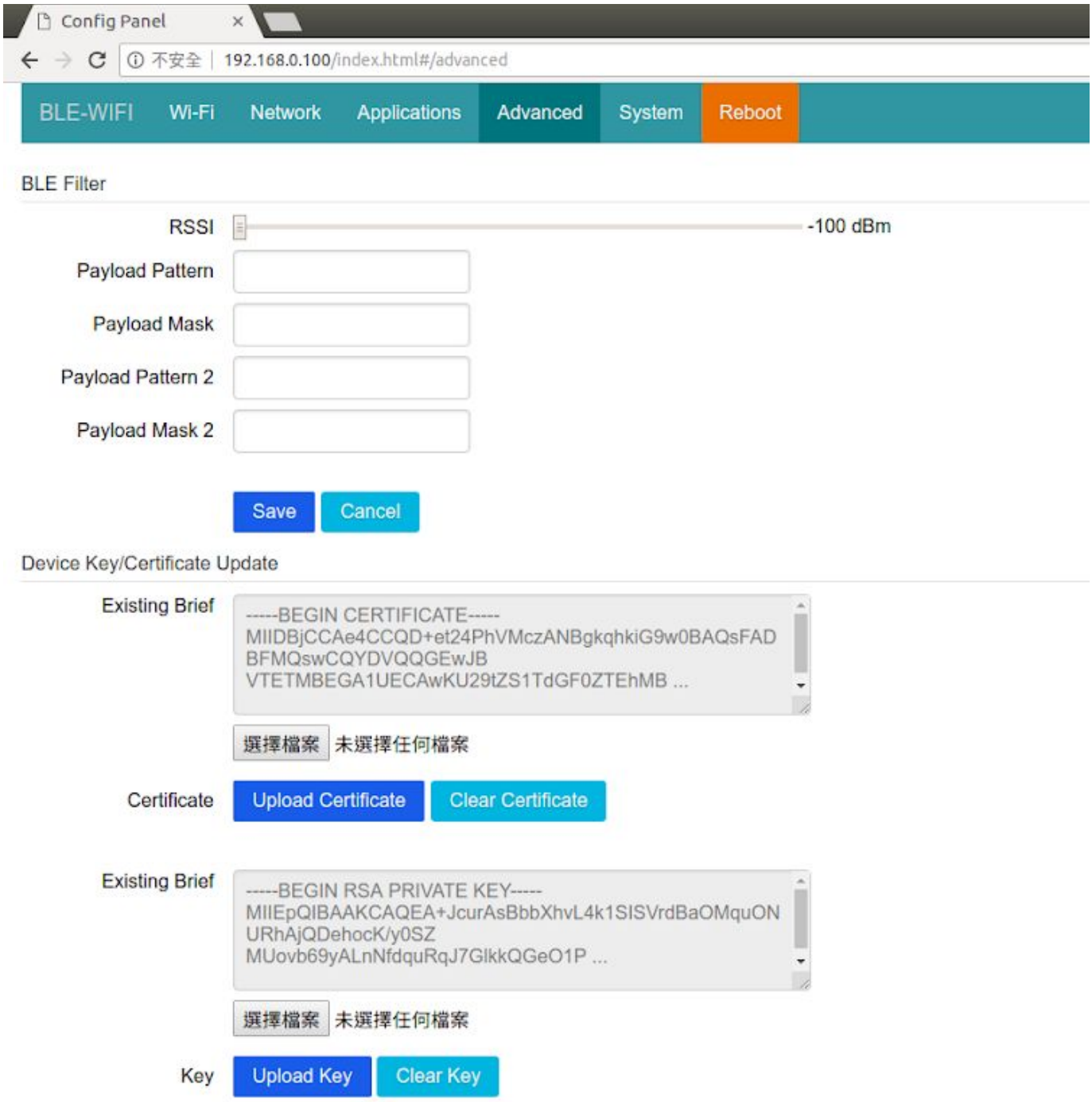
Example By Using Symmetric Key

- MQTT HOST [Your IoT Hub Name].azure-devices.net
- MQTT PORT 8883
- MQTT PUBTOPIC devices/[Your device name]/messages/events/
- MQTT CLIENTID [Your device name]
- MQTT USERNAME [Your IoT Hub Name].azure-devices.net
- MQTT PASSWORD [use the string with your device's SAS token]
- Enable MQTTS
- Select Azure-IoT-Hub RootCA
- Disable use certificate



Example By Using X.509 certificates

- Upload certificate & private key to IGS01S via webUI advanced page
- Make sure enable “Use Certificate” in application page.



Revision History

DATE	REVISION	CHANGES
Feb 11, 2019	1	Initial release
Mar 28, 2019	2	Update reference documents