

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 mosquito tool to test connecting Azure IoT Hub with mqtt.

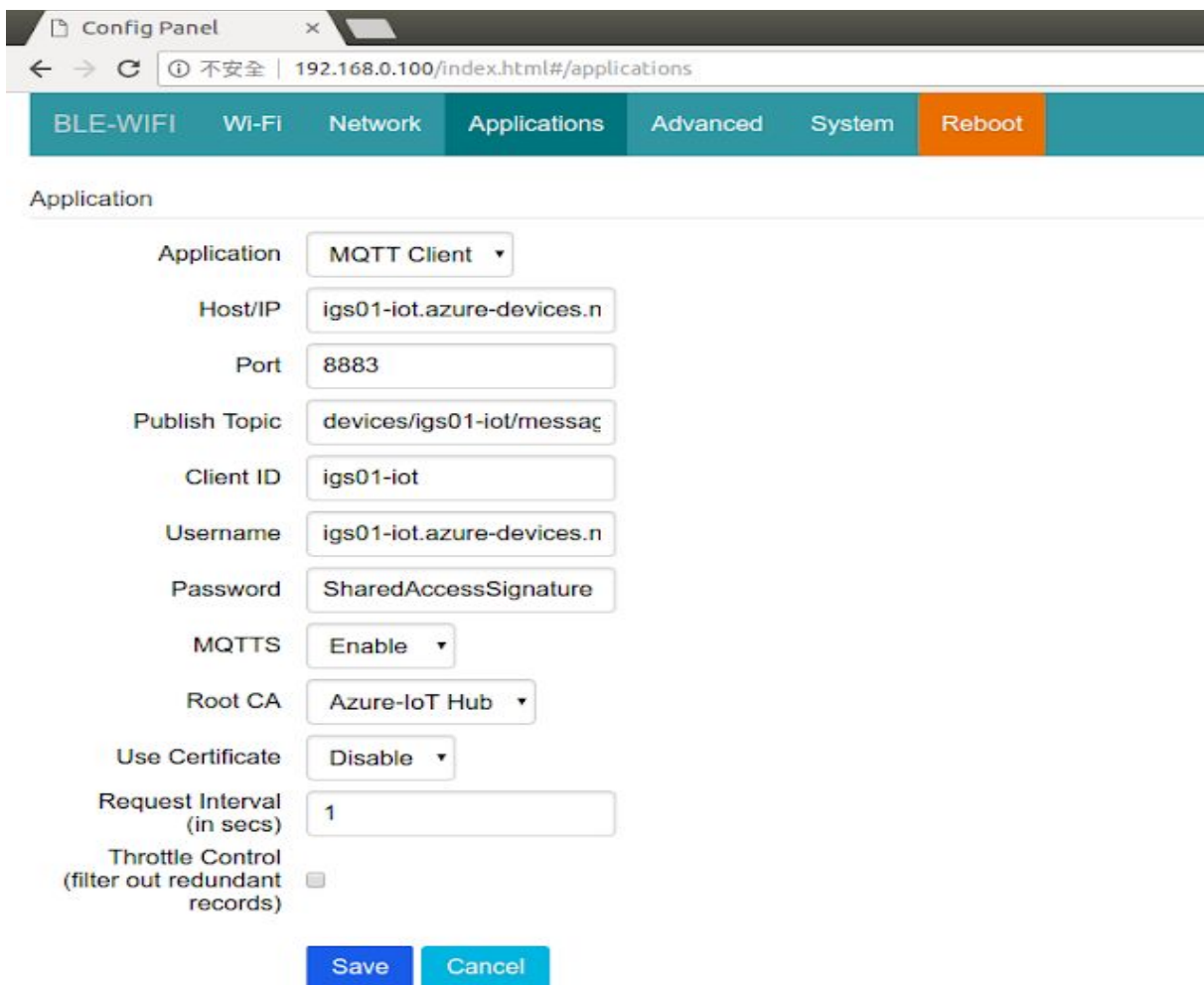
<https://mosquitto.org/download/>

Below shows an example to publish "hello" message to azure IoT using mosquito tool.

```
$ mosquito_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



The screenshot shows a web browser window titled "Config Panel" with the address bar displaying "192.168.0.100/index.html#/applications". The navigation menu includes "BLE-WIFI", "Wi-Fi", "Network", "Applications", "Advanced", "System", and "Reboot". The "Applications" section is active, showing the "Application" configuration page. The configuration fields are as follows:

Application	MQTT Client
Host/IP	igs01-iot.azure-devices.n
Port	8883
Publish Topic	devices/igs01-iot/messag
Client ID	igs01-iot
Username	igs01-iot.azure-devices.n
Password	SharedAccessSignature
MQTTS	Enable
Root CA	Azure-IoT Hub
Use Certificate	Disable
Request Interval (in secs)	1
Throttle Control (filter out redundant records)	<input type="checkbox"/>

At the bottom of the form, there are two buttons: "Save" and "Cancel".

Example By Using X.509 certificates

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

The screenshot shows the 'Config Panel' web interface for IGS01S. The 'Advanced' tab is selected in the top navigation bar. The 'BLE Filter' section includes an RSSI slider set to -100 dBm and four input fields for Payload Pattern, Payload Mask, Payload Pattern 2, and Payload Mask 2. Below these are 'Save' and 'Cancel' buttons. The 'Device Key/Certificate Update' section contains two text areas for 'Existing Brief' (one for Certificate and one for Key) with 'Choose File' buttons and 'Upload Certificate/Clear Certificate' and 'Upload Key/Clear Key' buttons.

Config Panel x

← → ↻ 不安全 | 192.168.0.100/index.html#/advanced

BLE-WIFI WI-FI Network Applications **Advanced** System Reboot

BLE Filter

RSSI -100 dBm

Payload Pattern

Payload Mask

Payload Pattern 2

Payload Mask 2

Device Key/Certificate Update

Existing Brief

```
-----BEGIN CERTIFICATE-----
MIIDBjCCAE4CCQD+et24PhVMczANBgkqhkiG9w0BAQsFAD
BFMQswCQYDVQQGEwJB
VTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB ...
```

未選擇任何檔案

Certificate

Existing Brief

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA+JcurAsBbbXhV4k1SISVrdBaOMquON
URhAjQDehocK/y0SZ
MUovb69yALnNfdquRqJ7GikkQGeO1P ...
```

未選擇任何檔案

Key

Revision History

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