INGICS TECHNOLOGY

Guide
Ver.01a

BLE_WiFi Gateway iGS01S User Manual

iGS01S is a bridge to connect the local BLE devices, sensors, or beacons to the internet by WiFi. Through an easy web UI interface, one can configure the internet connection to a general cloud server, like TCP, HTTP(S), or MQTT. Management through the cloud to the BLE devices becomes simple through iGS01S. This guide is to help the user to figure out how to operate and configure the iGS01S.

Contents

Contents

Overview
- Inside the box
- WiFi
- BLE

Input and Output
- Multi-function button
  - WPS
  - Reset to Default
  - Firmware Upgrade
- LEDs

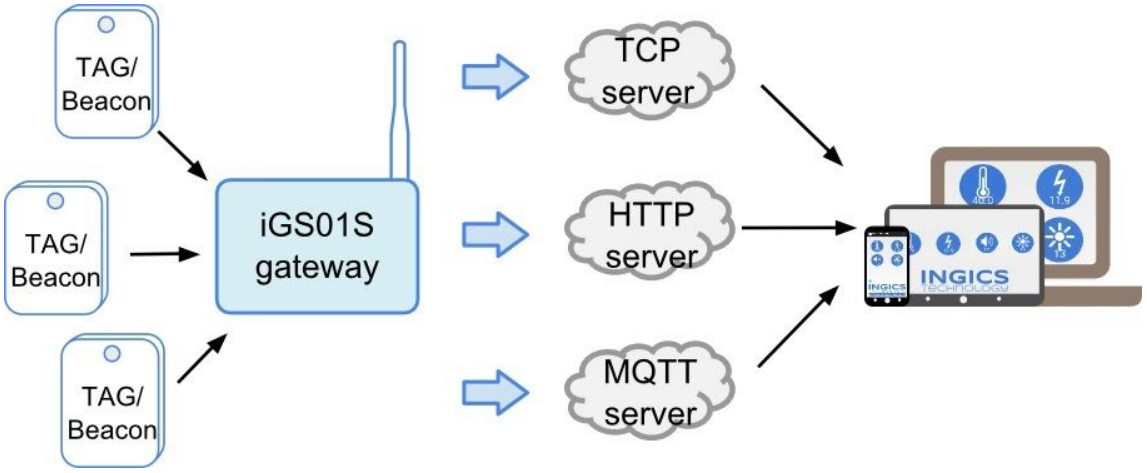
Create Connection

Web User Interface
- Wi-Fi
  - Simple AP
  - Station
- Network
  - AP Client Setting
  - AP Server Setting
- Applications
  - M2M TCP Server
  - M2M TCP Client
  - HTTP Client
    - Force HTTPS
    - Keep-Alive
    - Request Interval
    - Throttle Control
  - MQTT Client
    - MQTTS
    - Request Interval and Throttle Control, please refer to HTTP client.

Advanced
BLE Filter
RSSI
Payload Whitelist
Device Key/Certification Update
System
NTP setting
Revision History
Statement

Overview

The iGS01S gateway reads beacons(like iBeacon or Eddystone), customized tags, or BLE sensors and sends the information to the local TCP server or internet HTTP or MQTT server. User can configure the transmit period and server information through a simple web UI. Below is the typical application diagram of iGS01S.



Inside the box

There are one iGS01S unit, one 1M USB cable, and one 2dBi dipole antenna included in one full shipping package. iGS01S is powered by a standard micro-USB cable, rated at 5V&500mA. You can

power this device with a standard smartphone charger or the USB port of any host device that can support 500mA or above.

WiFi

For WiFi connection, it provides two modes -- Access Point mode(AP mode) and Station mode. In AP mode, it acts as a simple AP supporting DHCP. The main purpose of this mode is for configuration. In Station mode, a client device keeps trying to join to the AP in your home or office. After joining the AP, the gateway can bridge your BLE devices to the local TCP server or cloud server for management.

BLE

BLE is normally in listening mode. It collects the messages advertised by other BLE devices. These messages are then transferred to WiFi and sent to the cloud server configured by the user. The packet format sent to the cloud server as below:

$<report type>,<tag id>,<gateway id>,<rssi>,<raw packet content>,*<unix epoch timestamp>\r\n

examples:

```
$GPRP,CCB97E7361A4,CB412F0C8EDC,-49,1309696773206D6573682023322028544553542902010 6
$GPRP,E5A706E3923A,CB412F0C8EDC,-87,0201041AFF59000215011223344556677889 9AABBCCDDEEFF0000100C3BB
$GPRP,0C61CFC1452E,E7DAE08E6FC3,-44,0201061AFF4C000215B9A5D27D56CC4E3AAB511F2153BCB9670001452ED6
(iBeacon, UUID: B9A5D27D56CC4E3AAB511F2153BCB967, Major: 0001, Minor: 452E)
```

```
*Note:
When NTP is enabled, a timestamp field is added to the packet. Check System section for the NTP setting.
```

<report type>	GPRP: general purpose report . RSPR: active scan response report
<tag id>	MAC address or ID of tag/beacon
<gateway id>	MAC address of gateway's BLE
<rssi>	RSSI of tag/beacon
<raw packet content>	Raw packet received by the gateway
<unix epoch timestamp>	Optional timestamp when NTP is enabled

Input and Output

Multi-function button

One multi-function button is on one side of the iGS01S as the figure showed.

It is used to act WPS, reset to default settings, and OTA (over-the-air FW upgrade). Below is how it functions.

Function	Mode	Trigger Condition
WPS	Station	short press for over 1sec and release
Reset to default settings	Any	long press for over 5 sec
OTA	Boot up	press then power on, keep pressing till LEDs flash

WPS

iGS01S supports WPS to connect to your Access Point. First press the WPS button on your Access Point, when it is ready, then press the WPS button on the iGS01S device(the WPS button needs to be pressed for over 1 sec) to join it.

Reset to Default

In case you need to go back to the original settings, keep pressing the reset/default button in your device for over 5 secs no matter in which mode the device is. The WiFi LED will be turned off and when you release the button, the iGS01S will reboot to its default settings(AP mode).

Firmware Upgrade

Check *AP002_iGS01_Firmware_Upgrade* for details.

LEDs

There are two LEDs to indicate current status like the right figure. The upper one is BLE LED and the lower one is WiFi LED. Below are their behaviors.

	On	Flash
BLE LED	find tag/beacon in range	BLE transmission happening
WiFi LED	AP mode: AP is ready for connect	WiFi transmission

	Station mode: connect to assigned AP successfully	happening The device quickly blinking while joining AP during boot

Create Connection

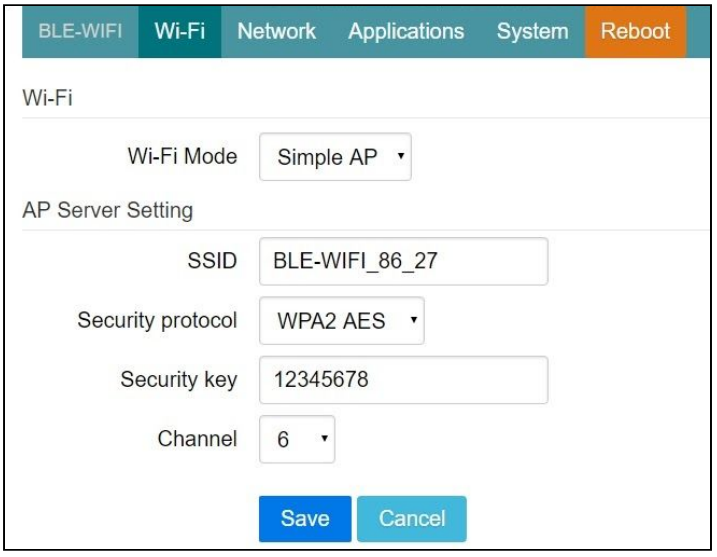
iGS01S is in Access Point(AP) mode defaultly. If you have no idea what mode currently it is in, please press the multi-function button to reset it to the default state. In AP mode, you could scan and connect it with the WiFi of your NB/PC/Mac/Tablet/Smartphone. It's name is just like the above figure with part of the mac address. The default key to connect with it is "**12345678**". You can change it later when you get into the web UI.

After connection, enter IP address **192.168.10.1** in your browser. The default account/password are both "**admin**". You can change the password later. In web UI, any change need to be saved first. After all changes made, click reboot to make the changes effective. When In Station mode, the IP address of the iGS01S is assigned by the other AP. To get into the web UI, you have to find the assigned IP address. The following sections describe details of the web UI.

Web User Interface

Wi-Fi

iGS01S can work in Simple AP mode and Station mode. These modes and the related settings can be managed on this page.



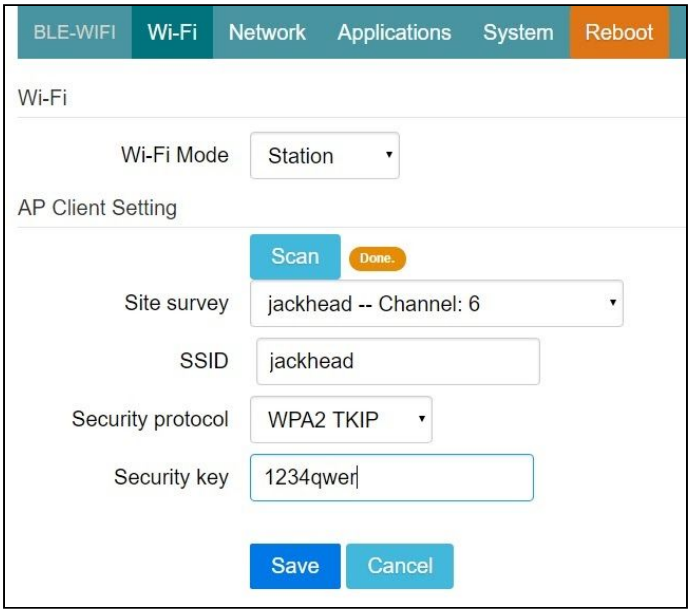
Simple AP

SSID: The default name is BLE-WiFi plus the last digits of the mac address. It's configurable by user.

Security Protocol: Open, WPA TKIP, WPA AES, WPA2 TKIP, WPA2 AES are supported. WPA2 AES is recommended.

Security Key: 8-63 characters can be input

Channel: 1~11(ch12 and ch13 could be supported by request)



Station

Scan: Click it to scan available APs.

Site Survey: The scan result is listed here and users can choose the correct AP from the list. The WiFi channel of the AP is also listed.

SSID: No manual input required. It is automatically filled once a user chooses an AP from the scan list.

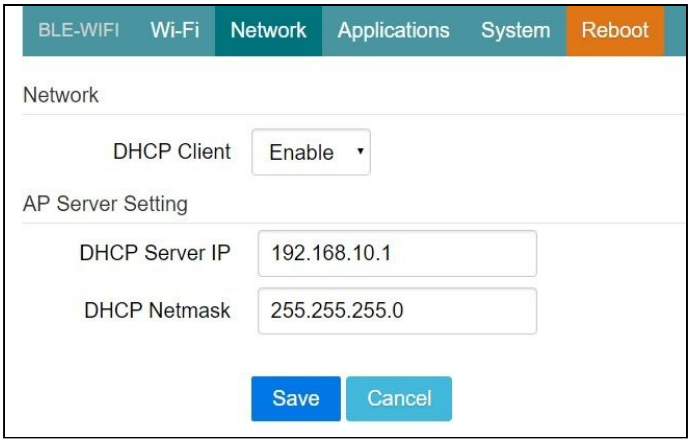
Security Protocol: Basically it is automatically detected and selected after choosing an AP from the scan list. But in case the AP setting is in WEP open or WEP shared, user has to confirm it by himself.

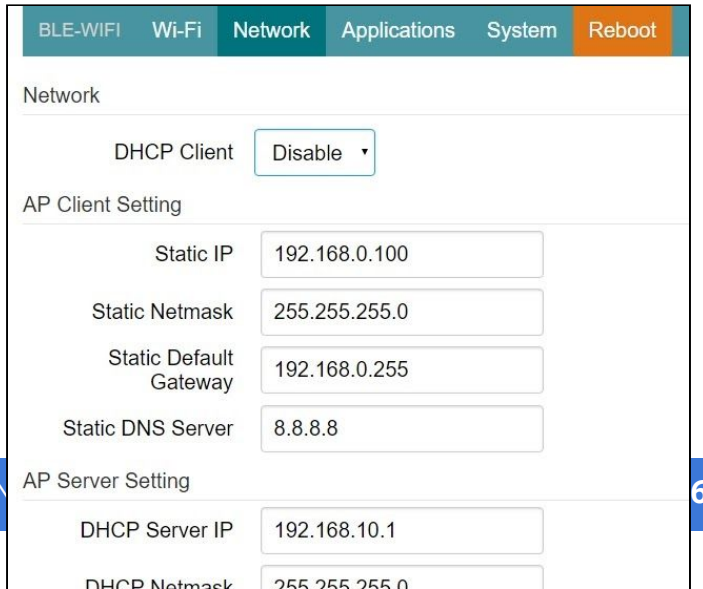
Security Key: Type the one assigned in your AP.

Network

AP Client Setting

This setting is mainly for Station mode. Normally a DHCP client is enabled to join a WiFi AP w/ DHCP. If one wants to manually assign an IP address for iGS01S, the DHCP client should be disabled. Once disabled, users should assign the IP, Netmask, Gateway, and/or DNS server.



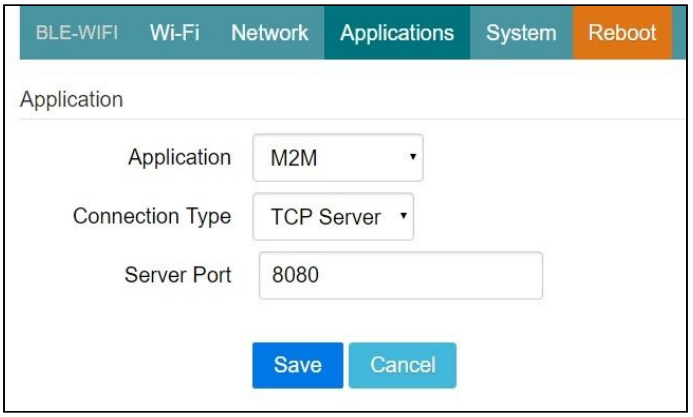


AP Server Setting

This setting is for AP mode. The default IP address of iGS01S in AP mode is 192.168.10.1 and the netmask is

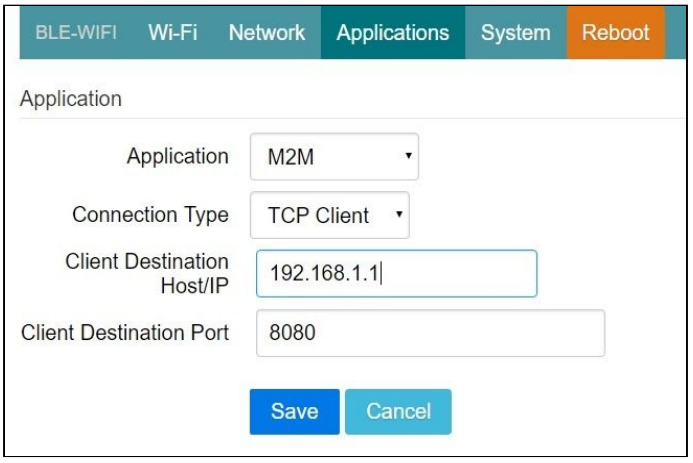
255.255.255.0. In case the user want to change the IP address in AP mode, just set the IP and Netmask here. The corresponding DHCP client address will be changed too. For example, if the DHCP server IP address is changed to 192.168.0.1, the DHCP clients associated with iGS01S AP will be 192.168.0.X.

Applications



M2M TCP Server

iGS01S is a TCP server with fixed IP address 192.168.10.1. The default port is 8080 and users can also assign the port.

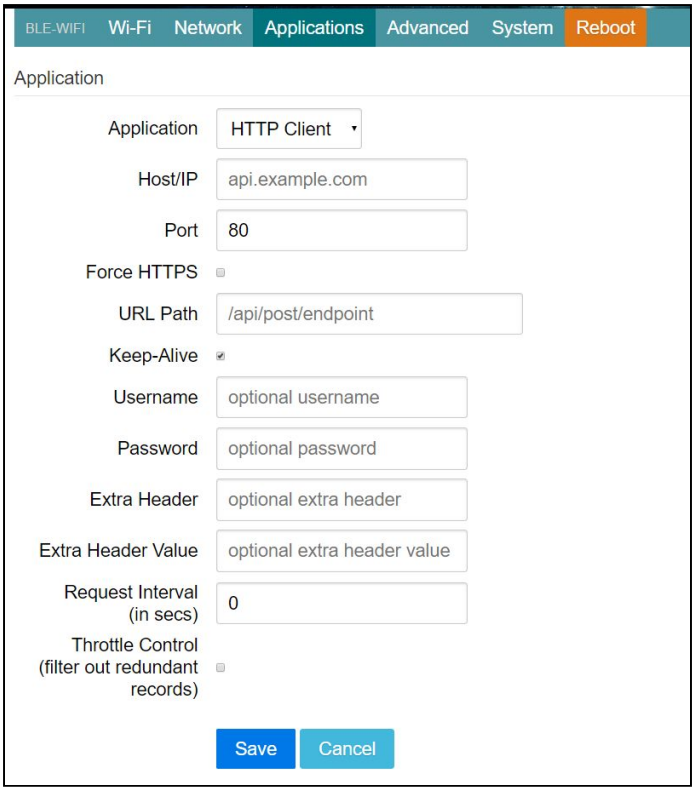


M2M TCP Client

If there is already a TCP server, one can set iGS01S as a TCP client to communicate with the server. Enter the address and port number of the TCP server to connect them.

HTTP Client

Another connection in application is through setting iGS01S as a HTTP client. In this scenario, one has to assign the HTTP host address and port number. Also the url path is necessary to bring the BLE data to the HTTP server through the gateway. Some HTTP servers may need username and password. The others may need extra header and value.



Force HTTPS

Check it to use HTTPS. No matter which port is used, it will be HTTPS

Keep-Alive

Check it to enable http keep alive which will improve network throughput.

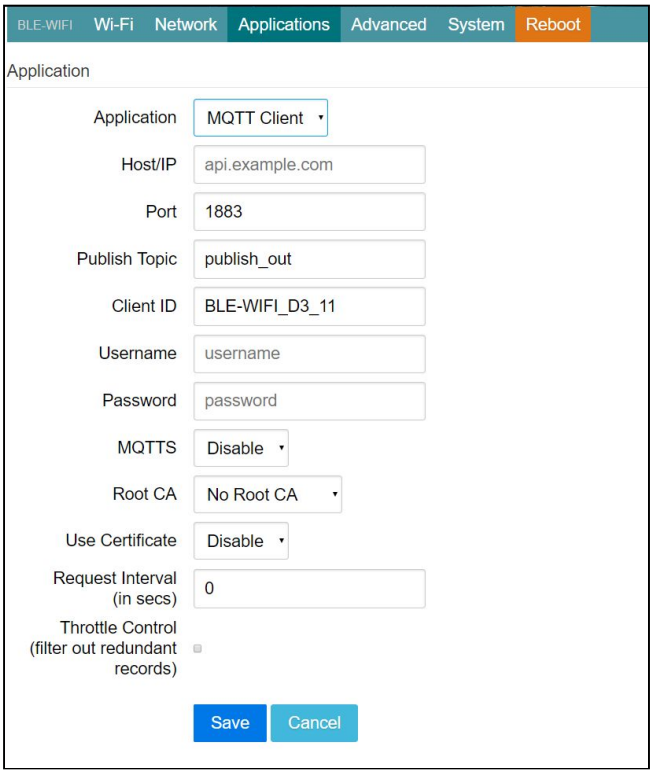
Request Interval

One can also assign the request interval to upload the data to the HTTP server. This is useful and it can reduce the HTTP connections. When the interval is set as 0, the data will be sent immediately.When it is set as a non-zero value in second, the data will be sent whenever the buffer is full or the time interval is reached.

Throttle Control

If the user selects to enable throttle control, iGS01S will keep the last record for each TAG/Beacon ID in the given interval(request interval). In this way, one can reduce the upload connections to the HTTP server.

MQTT Client



MQTT server is supported by the iGS01S. In this scenario, one has to assign the MQTT host address and port number. Also the publish topic needs to be assigned. Client ID is defaultly assigned as the gateway name with part of MAC address, users can change it as well. If the Client ID is not set, the system will generate a random number for it. Username and password are optional.

MQTTS

Users can enable MQTTS support. Users can also enable RootCA/Use Certificate based on the server requirement. For example, to enable AWS-IOT, the user has to enable MQTTS/ROOT CA/ Use Certificate options and upload certificate and private key in the advanced page.

Request Interval and Throttle Control, please refer to HTTP client.

Advanced

There are several features in this page that can help users to deal with the incoming BLE packet.

BLE Filter

Users can set BLE filters to filter out the unwanted BLE information. There are two kinds of filters. One is by BLE RSSI value and the other is by pattern/mask combination.

RSSI

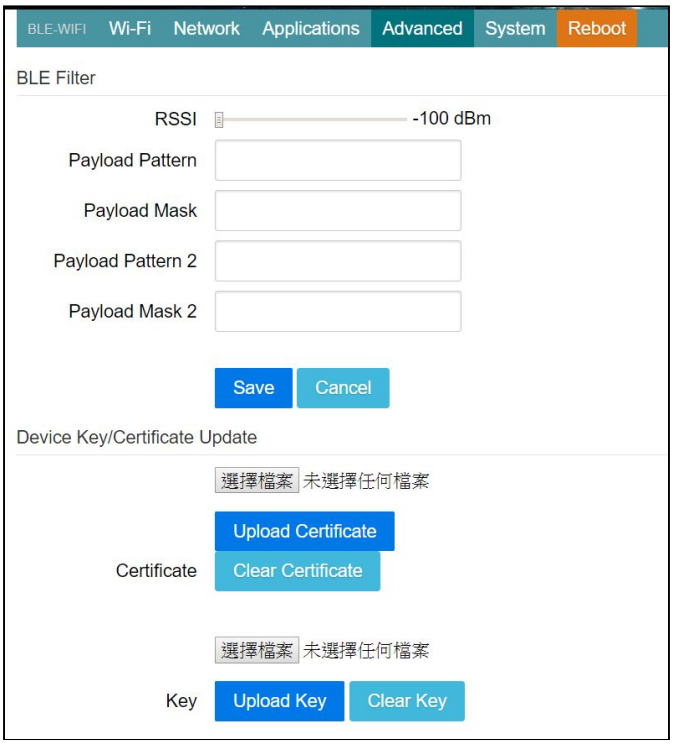
If the bar is pulled right to -50dBm, only the BLE tag/beacon with RSSI larger than or equal to -50dBm(say -45dBm) will be sent out to the server.

Payload Whitelist

Two sets of payload masks are provided for filtering the unwanted beacon. Set pattern/mask fields to configure the whitelist.

If payload & mask != pattern & mask, the entry will be filtered out.

Some examples are provided in *AP007_iGS01_payload_filter*.



Device Key/Certification Update

Users can upload certification and key here.

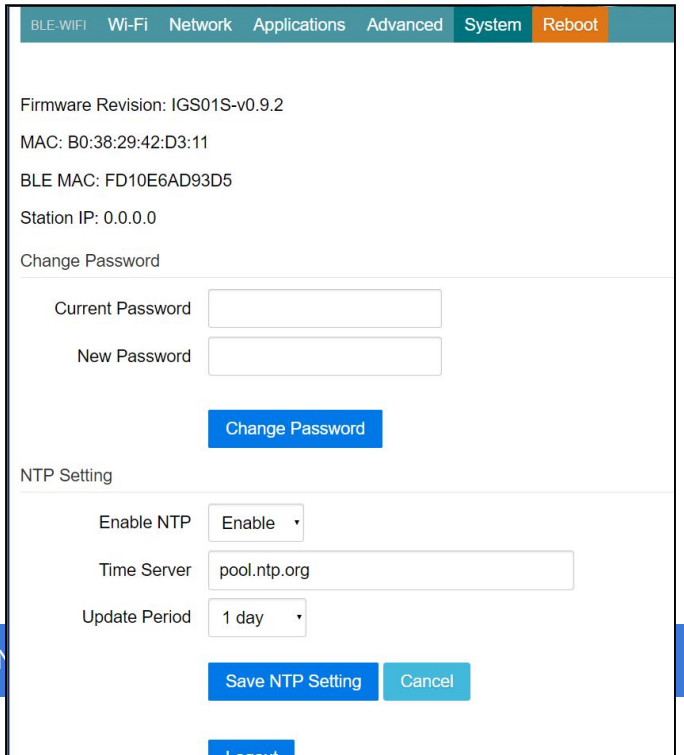
This is used by MQTTS. AWS-IOT users must upload the certificate and private key here to publish data to AWS-IOT.

System

Firmware and device information, including MAC address and IP address in station mode are shown here. The web UI password can also be changed here(the username is fixed as “admin”).

NTP setting

Users can enable the NTP to add the



timestamp information in the BLE package format as stated on the page. 3. User has to set the time server and the update period of the NTP. Remember to save the setting and reboot to make the setting effective.

Revision History

DATE	REVISION	CHANGES
Apr 16, 2018	01	Initial release
Feb 15, 2019	01a	Add CE DOC on the last page

Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures: . Reorient or relocate the receiving antenna. . Increase the separation between the equipment and receiver. . Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. . Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Statement

This device complies with Industry Canada licence-exempt RSS standard. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC Radiation Exposure Statement

This equipment complies with IC RSS-102 radiation exposure limit set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Cet équipement est conforme aux CNR-102 d'Industrie Canada. Cet équipement doit êtreinstallé et utilisé avec une distance minimale de 20 centimètres entre le radiateur et votrecorps. Cet émetteur ne doit pas être co-localisées ou opérant en conjonction avec autreantenne ou émetteur. Les antennes utilisées pour cet émetteur doivent être installés etfournir une distance de séparation d'au moins 20 centimètre de toute personne et doit pas être co-située ni fonctionner en conjonction avec une autre antenne ou émetteur.

NCC 警語

第十二條
經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者
均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條
低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有
干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、 科學及醫療用電波輻射性電
機設備之干擾
電磁波曝露量MPE標準值1mW/cm2，送測產品實測值 0.0103mW/cm2。

DECLARATION OF CONFORMITY

EU RED - DIRECTIVE 2014/53/EU -
EU-LOW VOLTAGE DIRECTIVE 2014/35/EU

This Declaration that the following designated product

BLE-WiFi Gateway
Model No.: IGS01S
Brand Name: INGICS

complies with the essential requirements of the EU RED - DIRECTIVE 2014/53/EU, EU-LOW VOLTAGE DIRECTIVE 2014/35/EU on the approximation of the laws of the Member States relating to ***Radio Spectrum Matters/RF Exposure.***
Assessment of compliance of the product with the requirements relating to radio spectrum matters was based on Annex IV of the Directive **2014/53/EU** and the following standard:

EMC	Radio Spectrum	Safety
EN 301 489 -1: V 2.2.0 (2017) EN 301 489 –17: V 3.2.0 (2017)	EN 300 328 (V 2.1.1, 2016-11)	IEC 62368-1:2014, modified and EN 62368-1:2014/A11:2017

(Identification of regulations / standards)

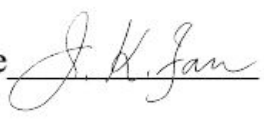
This declaration is issued by

INGICS TECHNOLOGY.
2F., No.15-2, Changshou St.,
Shulin Dist., New Taipei City 238,, Taiwan, R.O.C.

(Name / Address)

Furthermore we declare that our product will be produced in correspondence with all requirements according to the Directive 2014/53/EU and LOW VOLTAGE DIRECTIVE 2014/35/EU.

Name: J.K.Fan Title: President

Signature 

Date: May 28, 2018