

# BLE\_WiFi Gateway iGS01S User Guide

iGS01S is a bridge to connect the local BLE devices, sensors, or beacons to the internet by the 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](#)

#### [Request Interval](#)

#### [Throttle Control](#)

#### [MQTT Client](#)

#### [MQTTS](#)

#### [Advanced](#)

#### [BLE Filter](#)

#### [RSSI](#)

#### [Payload Whitelist](#)

#### [Device Key/Certification Update](#)

#### [System](#)

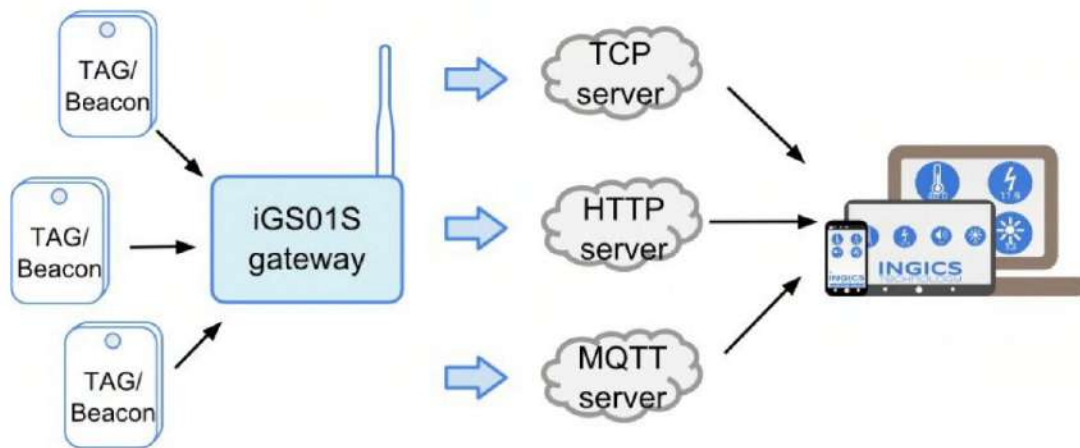
#### [NTP setting](#)

### [Revision History](#)



## 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, it is a client device that 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,-49,1309696773206D65736820233220285445535429020106
```

```
$GPRP,E5A706E3923A,CB412F0C8EDC,-87,0201041AFF590002150112233445566778899AABBCCDDEEFF0000100C3BB
```

\*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 . SRRP: 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 support WPS to connect to your Access Point. First press the WPS button on your Access Point, when it ready, then press the WPS button on the iGS01S device( the WPS button need 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 is their behaviors.

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

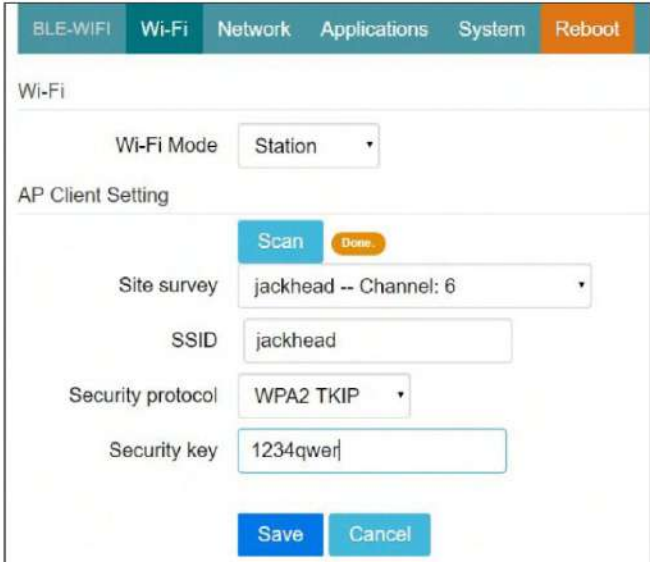
**Security Key:** 8-63 characters can be input

**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 user 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 user choose 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 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, user 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 to iGS01S AP will be 192.168.0.X.



BLE-WIFI Wi-Fi **Network** Applications System Reboot

Network

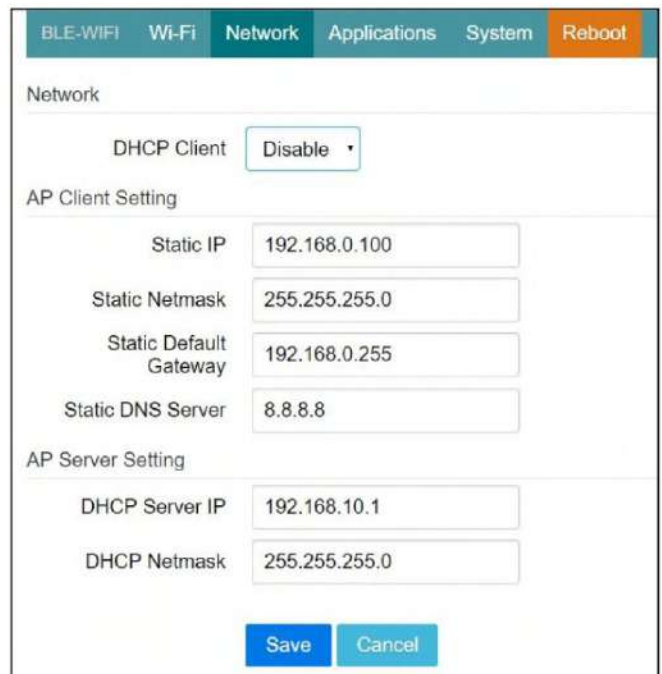
DHCP Client **Enable**

AP Server Setting

DHCP Server IP 192.168.10.1

DHCP Netmask 255.255.255.0

Save Cancel



BLE-WIFI Wi-Fi **Network** Applications System Reboot

Network

DHCP Client **Disable**

AP Client Setting

Static IP 192.168.0.100

Static Netmask 255.255.255.0

Static Default Gateway 192.168.0.255

Static DNS Server 8.8.8.8

AP Server Setting

DHCP Server IP 192.168.10.1

DHCP Netmask 255.255.255.0

Save Cancel

## Applications

### M2M TCP Server

iGS01S is a TCP server with fixed IP address 192.168.10.1. The default port is 8080 and user 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 keepalive 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



The screenshot shows the 'Applications' tab with the following configuration:

- Application: M2M
- Connection Type: TCP Server
- Server Port: 8080
- Buttons: Save, Cancel



The screenshot shows the 'Applications' tab with the following configuration:

- Application: M2M
- Connection Type: TCP Client
- Client Destination Host/IP: 192.168.1.1
- Client Destination Port: 8080
- Buttons: Save, Cancel



The screenshot shows the 'Applications' tab with the following configuration:

- Application: HTTP Client
- Host/IP: api.example.com
- Port: 80
- Force HTTPS: ☐
- URL Path: /api/post/endpoint
- Keep-Alive: ☐
- Username: optional username
- Password: optional password
- Extra Header: optional extra header
- Extra Header Value: optional extra header value
- Request Interval (in secs): 0
- Throttle Control (filter out redundant records): ☐
- Buttons: Save, Cancel



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 user select 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 need to be assigned.

Client ID is defaultly assigned as the gateway name with part of MAC address, user can change it as well. If Client ID is not set, system will generate a random number for it. Username and password are optional.

## MQTTS

User can enable MQTTS support. User 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 advanced page.

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



## Advanced

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

### BLE Filter

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

### RSSI



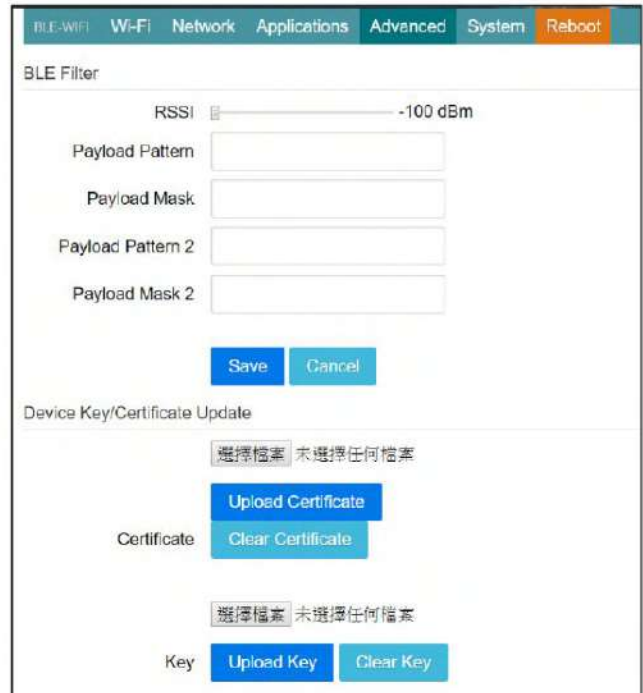
If the bar is pulled right to -50dBm, only the BLE tag/beacon with RSSI larger than or equal to -50dBm(say -45dBm) will be sent out to the server.

## Payload Whitelist

Two sets of payload mask 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*.



The screenshot shows the 'BLE Filter' configuration page. At the top, there is a navigation bar with tabs: BLE-WIFI, Wi-Fi, Network, Applications, Advanced, System, and Reboot. The 'Advanced' tab is selected. Below the navigation bar, the 'BLE Filter' section contains an RSSI slider set to -100 dBm, and four input fields for Payload Pattern, Payload Mask, Payload Pattern 2, and Payload Mask 2. There are 'Save' and 'Cancel' buttons. Below this is the 'Device Key/Certificate Update' section, which includes a 'Choose File' button, an 'Upload Certificate' button, a 'Clear Certificate' button, another 'Choose File' button, and 'Upload Key' and 'Clear Key' buttons.

## Device Key/Certification Update

User can upload certification and key here.

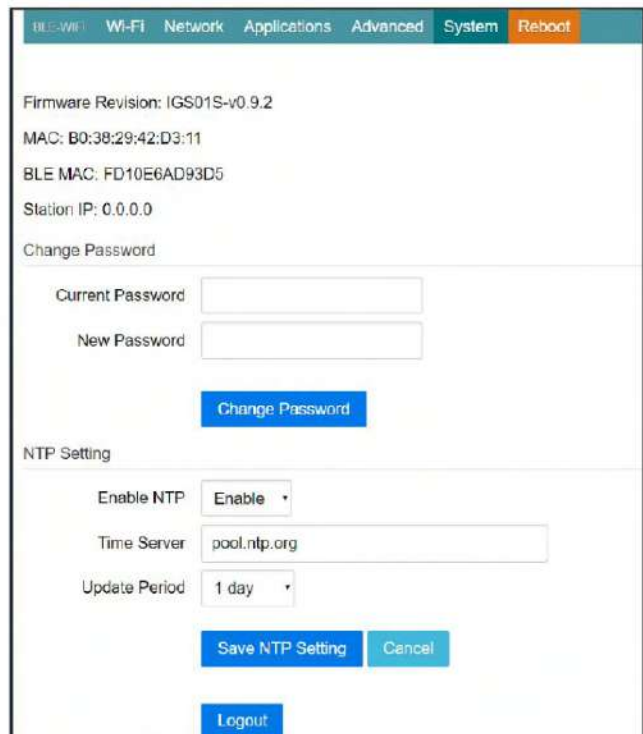
This is used by MQTTs. AWS-IOT users must upload the certificate and private key here to publish data to AWS-IOT.

## 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

User can enable the NTP to add the timestamp information in the BLE package format as stated in 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.



The screenshot shows the 'System' configuration page. At the top, there is a navigation bar with tabs: BLE-WIFI, Wi-Fi, Network, Applications, Advanced, System, and Reboot. The 'System' tab is selected. Below the navigation bar, the 'System' section displays firmware and device information: Firmware Revision: IGS01S-v0.9.2, MAC: B0:38:29:42:D3:11, BLE MAC: FD10E6AD93D5, and Station IP: 0.0.0.0. Below this is the 'Change Password' section with 'Current Password' and 'New Password' input fields and a 'Change Password' button. At the bottom is the 'NTP Setting' section with an 'Enable NTP' dropdown set to 'Enable', a 'Time Server' input field with 'pool.ntp.org', and an 'Update Period' dropdown set to '1 day'. There are 'Save NTP Setting', 'Cancel', and 'Logout' buttons.