

Guide  
Ver.0a

# Ethernet Beacon Gateway iGS02E User Guide

iGS02E is a bridge to connect the local BLE devices, sensors, or beacons to the internet through Ethernet. With an easy web UI interface, one can configure the internet connection to a general cloud server, like TCP, HTTP(S), or MQTT(s). Through iGS02E, one can develop his application based on the collected BLE devices information on the cloud . This guide is to help the user to figure out how to operate and configure the iGS02E.

## Contents

[Contents](#)

[Overview](#)

[Inside the box](#)

[Ethernet](#)

[BLE](#)

[Input and Output](#)

[Default Setting button](#)

[LEDs](#)

[How to configure](#)

[Web User Interface](#)

[Network](#)

[DHCP client](#)

[STATIC IP](#)

[Applications](#)

[TCP Server](#)

[TCP Client](#)

[Request Interval](#)

[Throttle Control](#)

[HTTP POST](#)

[HTTPS](#)

[Keep-Alive](#)

[MQTT Client](#)

[MQTTS](#)

[Advanced](#)

[BLE Filter](#)

[RSSI](#)

[Payload Whitelist](#)

[Advanced Filter](#)

[Enter/Leave](#)

[Status Change](#)

[Device Key/Certification Update](#)

[System](#)

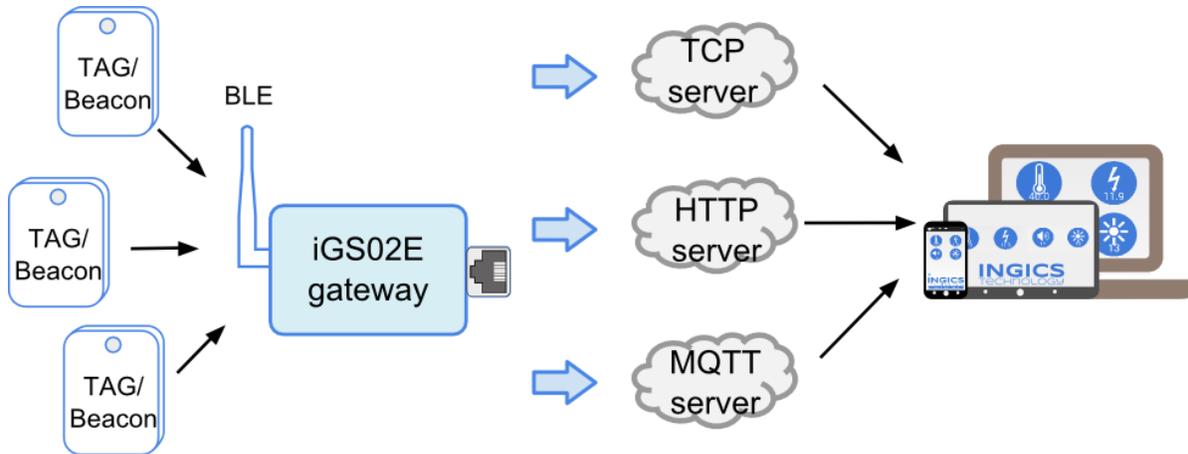
[NTP setting](#)

[Revision History](#)



## Overview

The iGS02E 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 iGS02E.



## Inside the box



There are one iGS02E unit, one 1M USB cable, one holder, and one 2dBi dipole antenna included in one full shipping package. iGS02E 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.

## Ethernet

It supports 10BASE-T and 100BASE-TX with HP Auto-MDIX. Through the Ethernet, 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 WiFi
<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

### Default Setting button

One button is on one side of the iGS02E as the figure showed.



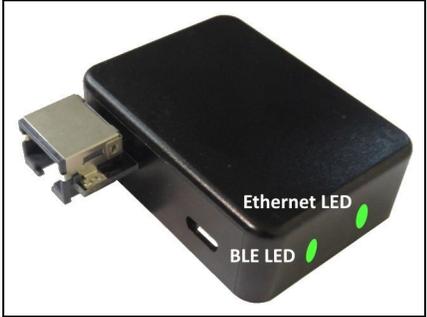
It is used to reset to default settings. In case you need to go back to the original settings, keep pressing the reset/default button in your device for over 5 secs no matter in which mode the device is. The

Ethernet LED will be turned off and when you release the button, the iGS02E will reboot to its default settings.

## LEDs

There are two LEDs to indicate current status like the right figure. One is BLE LED and the other is Ethernet LED. Below is their behaviors.

	On	Flash
BLE LED	find tag/beacon in range	BLE transmission happening
Ethernet LED	Network connection is built up	Transmission happening  The device quickly blinking while power on



## How to configure

iGS02E is a DHCP client by default. To configure it, you have to connect it to a router with DHCP enabled. The first thing is to find iGS02E's IP address in this network so that you can get into it's webUI for configuration. If you don't know the IP address, you may need to use some tool to find it.(For example, "Fing" APP in Android & iOS. Join your smartphone or tablet with "Fing" in the same network. And use it to scan all the devices in this network)

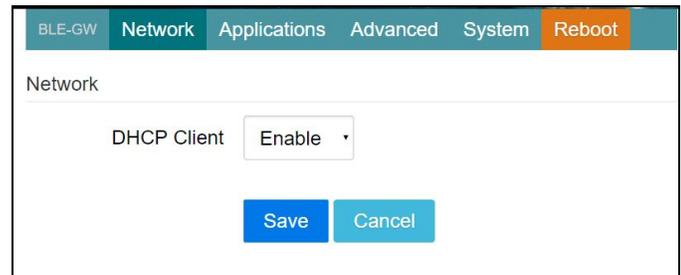
Once you know iGS02E's IP, enter the IP address in your browser. The default account/password are both "admin". You can change the password later. In web UI, any change need to be saved first. After all changes made, click reboot to make the changes effective. The following sections describe details of the web UI.

## Web User Interface

### Network

#### DHCP client

By default, iGS02E is a DHCP client.



## STATIC IP

If user wants to manually assign an IP address for iGS02E, the DHCP client should be disabled. Once disabled, user should assign the IP, Netmask, Gateway, and/or DNS server.

BLE-GW Network Applications Advanced System Reboot

Network

DHCP Client

Static IP Setting

Static IP

Static Netmask

Static Default Gateway

Static DNS Server

## Applications

### TCP Server

iGS02E is a TCP server. The default port is 8080 and user can also assign the port.

BLE-GW Network Applications Advanced System Reboot

Application

Application

Server Port

Request Interval (in secs)

Throttle Control (filter out redundant records)

### TCP Client

If there is already a TCP server, one can set iGS02E as a TCP client to communicate with the server. Enter the address and port number of the TCP server to connect them.

### Request Interval

One can also assign the request interval to upload the data to the server. This is useful and it can reduce the network traffic. 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 user select to enable throttle control, iGS02E will keep the last record for each

BLE-GW Network Applications Advanced System Reboot

Application

Application

Client Destination Host/IP

Client Destination Port

Request Interval (in secs)

Throttle Control (filter out redundant records)

TAG/Beacon ID in the given interval(request interval). In this way, one can reduce the upload

connections to the server.

## HTTP POST

Another popular server type is HTTP(s). iGS02E can use HTTP POST to communicate with the server. 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.

## HTTPS

In URL, start with https://.

## Keep-Alive

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

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

## MQTT Client

MQTT server is supported by the iGS02E. 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.

The screenshot shows the 'Applications' configuration page for 'HTTP POST'. The 'Application' dropdown is set to 'HTTP POST'. The 'URL' field contains 'http://urlpath/api/gwpost/IGS02E\_6'. The 'Content Type' dropdown is set to 'plain-text'. The 'Keep-Alive' checkbox is checked. The 'Extra Header' and 'Extra Header Value' fields contain 'optional extra header' and 'optional extra header value' respectively. The 'Request Interval (in secs)' field is set to '0'. The 'Throttle Control (filter out redundant records)' checkbox is unchecked. 'Save' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Applications' configuration page for 'MQTT Client'. The 'Application' dropdown is set to 'MQTT Client'. The 'Host/IP' field contains 'api.example.com'. The 'Port' field contains '1883'. The 'Publish Topic' field contains 'topics/pub'. The 'Content Type' dropdown is set to 'plain-text'. The 'Client ID' field contains 'IGS02E\_65\_D8'. The 'Username' field contains 'username'. The 'Password' field contains 'password'. The 'MQTTS' dropdown is set to 'Disable'. The 'Root CA' dropdown is set to 'No Root CA'. The 'Use Certificate' dropdown is set to 'Disable'. The 'Request Interval (in secs)' field is set to '0'. The 'Throttle Control (filter out redundant records)' checkbox is unchecked. 'Save' and 'Cancel' buttons are at the bottom.

## 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 TCP 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

Three 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 'Advanced' configuration page for a BLE-GW device. The page has a navigation bar with tabs: BLE-GW, Network, Applications, Advanced (selected), System, and Reboot. The main content is divided into several sections:

- BLE Filter:** Includes an RSSI slider set to -100 dBm. Below it are three sets of 'Payload Pattern' and 'Payload Mask' input fields. A 'Whitelist MAC' section has an 'Add' button.
- Whitelist:** A section with a 'Save' and 'Cancel' button.
- Advanced Filter:** A dropdown menu set to 'Disable', with 'Save' and 'Cancel' buttons.
- Device Key/Certificate Update:** Contains two sections. The first is for 'Certificate', with a file selection button (显示檔案), a text label '未選擇任何檔案', and 'Upload Certificate' and 'Clear Certificate' buttons. The second is for 'Key', with a file selection button (显示檔案), a text label '未選擇任何檔案', and 'Upload Key' and 'Clear Key' buttons.

### Advanced Filter

There are two more advanced filters:

## Enter/Leave

User can set a ENTER/LEAVE RSSI threshold for detecting beacon in range / ENTER event (RSSI >= ENTER\_RSSI) and out of range / LEAVE event (RSSI < LEEAVE\_RSSI). If a beacon was in ENTER state but not updated for a period of time (EXPIRED TIMEOUT), consider it as leave.

The screenshot shows the 'Advanced Filter' configuration page. At the top, there is a dropdown menu labeled 'Advanced Filter' with 'Enter/Leave' selected. Below this is the 'Enter/Leave Setting' section, which includes two sliders: 'Enter RSSI' set to -60 dBm and 'Leave RSSI' set to -80 dBm. There is also a text input field for 'Expired Timeout (sec)' with the value '60'. At the bottom, there are 'Save' and 'Cancel' buttons.

## Status Change

This enables checking the entries in cache and filter out received report with the same payload. So only send out data if the BLE payload changes.

The screenshot shows the 'Advanced Filter' configuration page. At the top, there is a dropdown menu labeled 'Advanced Filter' with 'Status Change' selected. Below this is the 'Expired Timeout (sec)' text input field with the value '60'. At the bottom, there are 'Save' and 'Cancel' 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").

The screenshot shows the 'System' configuration page. At the top, there is a navigation bar with tabs: 'BLE-GW', 'Network', 'Applications', 'Advanced', 'System', and 'Reboot'. The 'System' tab is active. The page displays the following information: 'Firmware Revision: IGS02E-v0.5.0', 'MAC: 44:2C:05:80:65:D8', 'BLE MAC: 442C058065D9', and 'Station IP: 192.168.1.107'. Below this is the 'Change Password' section, which includes 'Current Password' and 'New Password' input fields, and a 'Change Password' button. At the bottom, there is the 'NTP Setting' section, which includes 'Enable NTP' (set to 'Enable'), 'Time Server' (set to 'pool.ntp.org'), and 'Update Period' (set to '10 mins'). There are 'Save NTP Setting', 'Cancel', and 'Logout' buttons.

## 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.

## Revision History

DATE	REVISION	CHANGES
Apr 17, 2018	0a	Initial release