Guide
Ver.01

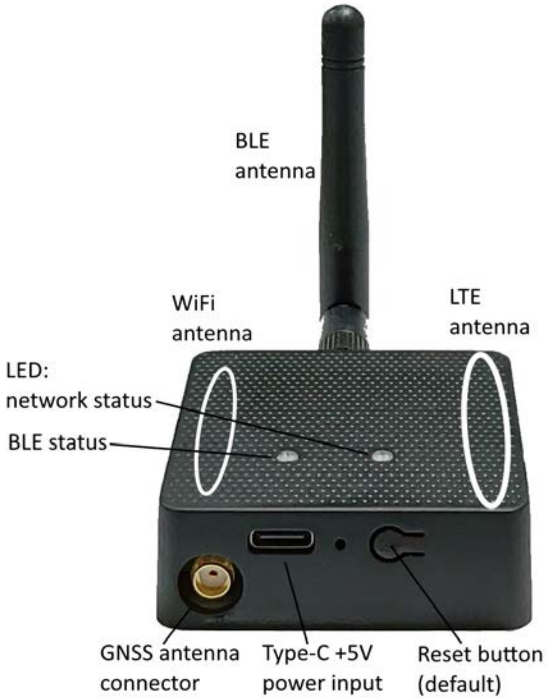
Beacon Gateway iGS03W/M User Guide

iGS03W/M is a gateway to bridge the local BLE tags, sensors, or beacons to remote server/cloud by WiFi, or LTE-M. Through an easy web UI interface, user can configure the Internet access to upload reports to cloud server by TCP, HTTP(S), or MQTT(S). This guide is to help the user to figure out how to operate and configure the iGS03.

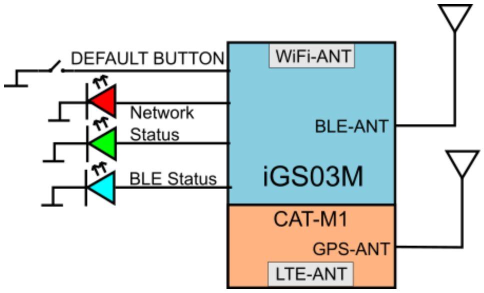
Contents:

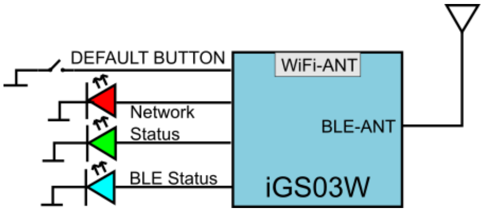
Overview

The iGS03 BLE gateway scans beacons(like iBeacon or Eddystone), proprietary tags, or BLE sensors then sends the payload to TCP, HTTP or MQTT server. Users can configure the transmit period and server endpoint through a simple web UI. There are two models, iGS03W and iGS03M, representing different uploading interfaces, WiFi and LTE-M.



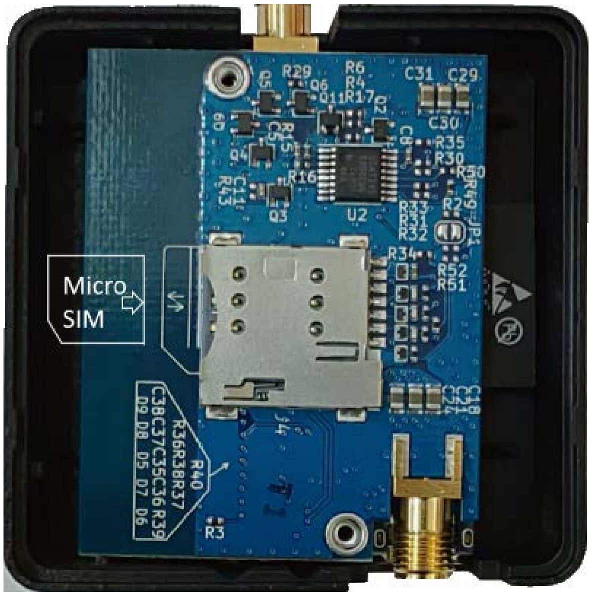
Block Diagram





SIM

To use iGS03M (LTE-M Model), you have to put a Cat-M1 micro SIM card into the socket of iGS03M. Please open the bottom cover to insert the SIM card.



WiFi

The 2.4G WiFi AP connection is used to configure the unit through web UI. iGS03 works as an WiFi Access Point(AP) supporting DHCP. Users must connect to this AP to configure the unit.

BLE

The BLE subsystem operates in listening mode. It collects the messages advertised by BLE devices. These messages are then sent to the cloud server configured by the user.

iGS03 supports two BLE modes

1. 1M Phy: including BLE4.2(Legacy)/BLE 5 1M in 100% duty cycle
2. Coded Phy: BLE 5 long range in 100% duty cycle

User can use following command to set BLE mode: (telnet console)

BLE PHYMODE (1: 1M Phy only, 2: Coded Phy only)

The default PHYMODE is 1, 1M Phy

GNSS

GNSS function is off by default.   User can below commands to manage the GNSS behavior:

GNSS ENABLE   Enable/Disable GNSS, default off

GNSS FIXCOUNT   Number of attempts for positioning, 0 indicates continuous positioning. default 0

GNSS FIXRATE   The interval time between the first and second time positioning, default 1 (1 second)

GNSS RPTRATE   The interval time for sending GPSR report, default 600 (10 minutes)

GNSS INFO   To get latest GPS status

Example case 1: The device is in fixed position:

e.g.

```
GNSS ENABLE 1
GNSS FIXCOUNT 5
GNSS FIXRATE 60
GNSS RPTRATE 60
```

Then GNSS will be enabled and get position for 5 times with 60 seconds interval.

GNSS will be off automatically after getting position for 5 times.

Example case 2: The device is moving:

e.g.

```
GNSS ENABLE 1
GNSS FIXCOUNT 0
GNSS FIXRATE 1
GNSS RPTRATE 60
```

Then GNSS will be enabled and continuously get position with 1 second interval, and it will send a GPSR report every 60 sec.

You can also use the "GNSS INFO" command to get the latest coordinates.

Payload Format

There are several kinds of payload format iGS03 will send to the server.

BLE

General format:

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

<report type>	Different report type to distinguish the source of the report.
<tag id>	MAC address or ID of tag/beacon
<gateway id>	MAC address of gateway
<rssi>	RSSI of tag/beacon
<raw packet content>	Raw packet received by the gateway
<unix epoch timestamp>	Optional timestamp configured in applications page

Report Type:

$GPRP	BLE4.2 General Purpose Report
$SRRP	BLE4.2 Scan Response Report
$LRAD	BLE5 Long Range ADV
$LRSR	BLE5 Long Range Scan Response
$1MAD	BLE5 1M ADV
$1MSR	BLE5 1M Scan Response

Examples:

```
$GPRP,CCB97E7361A4,CB412F0C8EDC,-49,1309696773206D65736820233220285445535429020106,1574921085
$GPRP,E5A706E3923A,CB412F0C8EDC,-
87,0201041AFF590002150112233445566778899AABBCCDDEEFF0000100C3BB,1574921085
$LRAD,51A88AD374B7,CC4B73906F96,-87,02010212FF0D0083BC280100AAAAFFFF000010030000,1574921085
$GPRP,0C61CFC1452E,E7DAE08E6FC3,-44,0201061AFF4C000215B9A5D27D56CC4E3AAB511F2153BCB9670001452ED6
(iBeacon, UUID: B9A5D27D56CC4E3AAB511F2153BCB967, Major: 0001, Minor: 452E)
```

GPS

General format:

```
$GPSR,<tag_mac>,<reader_mac>,<rssi>,yymmdd,hhmmss.ss,latitude,longitude,speed,hdop(,timestamp)
```

The "$GPSR,<tag_mac>,<reader_mac>,<rssi>" fields are for compatibility with other reports.

For $GPSR, the tag_mac is always the same as reader_mac and the rssi is always -127.

yymmdd,hhmmss.ss is the UTC time of position acquired.

speed: unit is knots.

hdop: Horizontal dilution of position

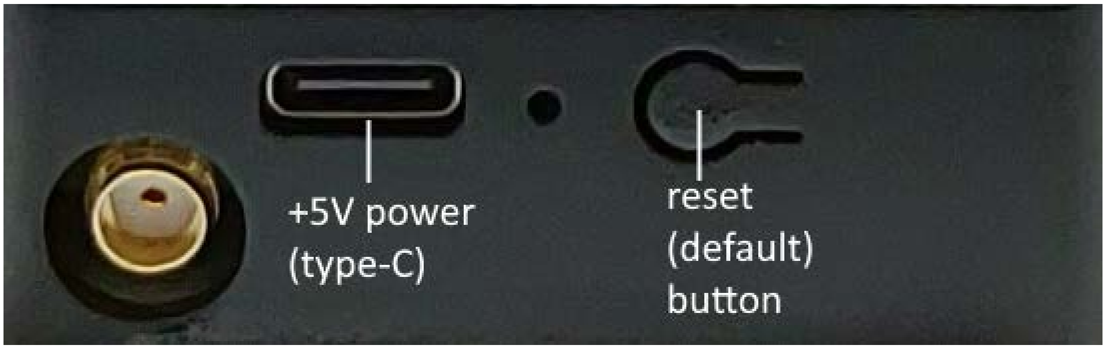
Example:

```
$GPSR,CC4B73906F96,CC4B73906F96,-127,191127,233821.00,24.993631,121.423264,0.0,2.4,1574897900
```

Buttons

Get default button

One reset(default) button is located on the back side of iGS03 as shown in the figure below.



In case you need to go back to the original settings, keep pressing the reset/default button in your device for over 3 secs no matter in which mode the device is. The network status LED will be turned off and when you release the button, the iGS03 will reboot to its default settings.

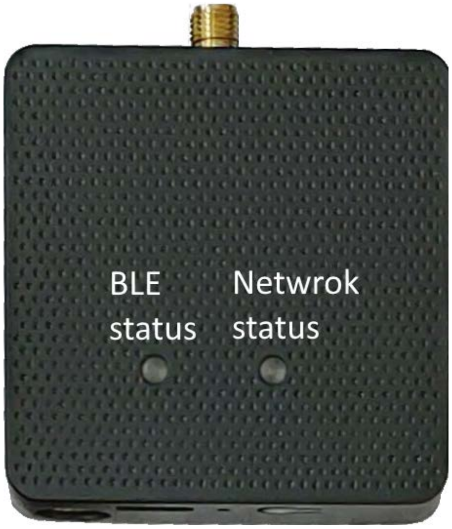
OTA

Reset(default) button can be used as Over-The-Air(OTA) firmware upgrade. This firmware upgrade is through WiFi interface only. To use it, press it then power on, keep pressing till network status LEDs flashes.

LEDs

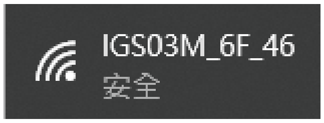
There are two LEDs to indicate current status as the right figure. The left one is BLE status LED and the right one is Network status. Below are their behaviors.

	On	Flash
BLE Status LED	find tag/beacon in range	BLE transmission happening
Network Status LED	WiFi/Ethernet/LTE-M connection success (This only implies the network is connected. It doesn't mean the server is connected)	Green: WiFi/Ethernet/LTE-M network transmission happening Orange: If IGS03M does not insert SIM card and being used as WiFi device



Network Status LED behavior	**Description**	**Status**
ORANGE LED on (500ms)	Boot start	Booting
RED LED blink (100ms on/off)	Joining AP (If WiFi in STA mode)	Booting
RED LED blink (500ms on/off)	LTE connecting carrier	Booting
GREEN/ORANGE LEDs blink interleaved (100ms)	WPS enrollee	WPS
GREEN LED on	Network ready	Ready/Idle
GREEN LED blink (200ms on/off)	Network is transfering data	Busy
ORANGE LED on	Network ready (If SIM card is not inserted)	Ready/Idle
ORANGE LED blink (200ms on/off)	Network is transfering data (If SIM card is not used)	Busy
RED LED ON (1sec)	Connect failure	Error
RED LED blink (5sec on/off)	Misconfiguration	Error
RED LED ON (5sec)	LTE init failure	Error
RED LED ON (1sec)	Button pressed	Indication

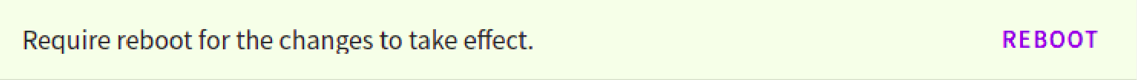
Configuration


IGS03M_6F_46
安全

To configure the unit, you have to connect it through WiFi interface. When it is powered on, you could scan its native AP and connect it with the WiFi of your NB/PC/Mac/Tablet/Smartphone. It's SSID 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 (SAVE). After all changes made, click reboot to make the changes effective. The following sections describe details of the web UI.


Require reboot for the changes to take effect.

Web User Interface

System

Firmware and device information, including MAC address and IP address in station mode are shown here.

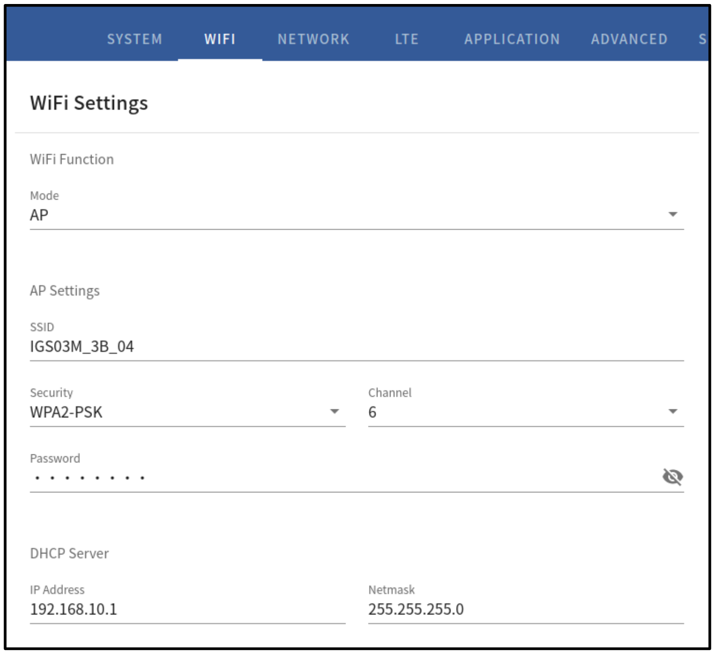
Wi-Fi

Users can configure iGS03 through connecting to its AP. The related settings can be managed on this page.

AP Mode

SSID: The default name is IGS03 plus the last digits of the mac address.

Security: Open, WPA-PSK, WPA2-PSK and WPA-PSK/WPA2-PSK are supported. WPA2-PSK is recommended.



WiFi Settings

WiFi Function

Mode: AP

AP Settings

SSID: IGS03M_3B_04

Security: WPA2-PSK

Channel: 6

Password: ••••••••

DHCP Server

IP Address: 192.168.10.1

Netmask: 255.255.255.0

Password: 8-63 characters can be input

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

DHCP Server: The default IP address of iGS03 in WiFi AP mode is 192.168.10.1 and the netmask is 255.255.255.. 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 iGS03 AP will be 192.168.0.X.

Station Mode

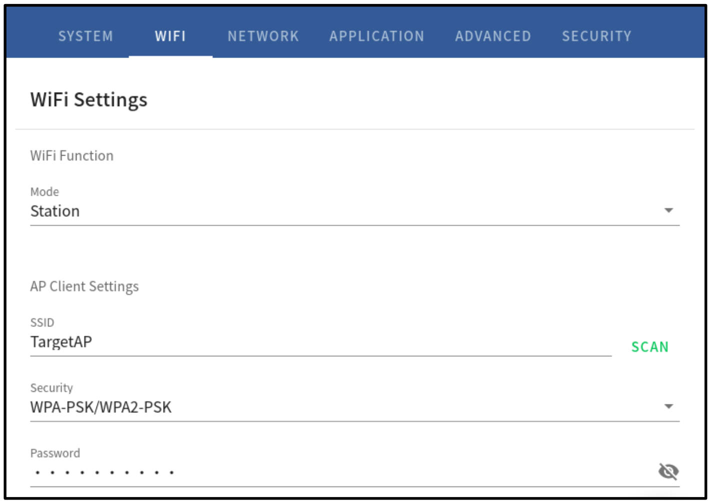
This mode is used for the WiFi version which has no LTE.

Scan: Click it to scan available APs. The scan result will list in the popup window, and the user can choose the correct AP from the list.

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

Security: 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, the user has to confirm it by himself.

Password: Type the one assigned in your AP**.**



WiFi Settings

WiFi Function

Mode
Station

AP Client Settings

SSID
TargetAP

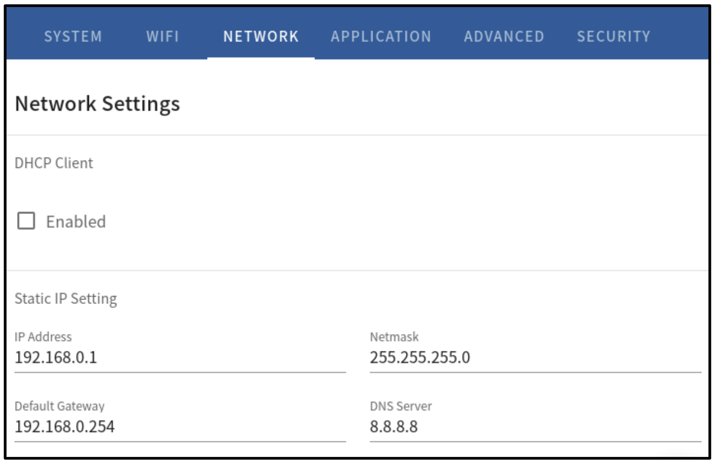
Security
WPA-PSK/WPA2-PSK

Password
• • • • • • • • • •

Network

This setting is mainly for configuring WiFi 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 iGS03, the DHCP client should be disabled. Once disabled, users should assign the IP, Netmask, Gateway, and/or DNS server.



Network Settings

DHCP Client

☐ Enabled

Static IP Setting

IP Address
192.168.0.1

Netmask
255.255.255.0

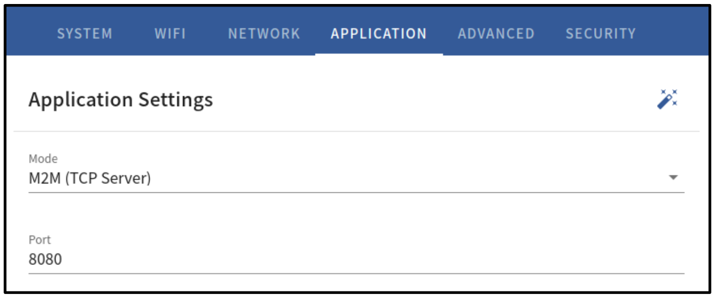
Default Gateway
192.168.0.254

DNS Server
8.8.8.8

Applications

TCP Server

This mode is mainly for testing purposes. Users can check the received data immediately via connecting to the tcp server through WiFi interface.



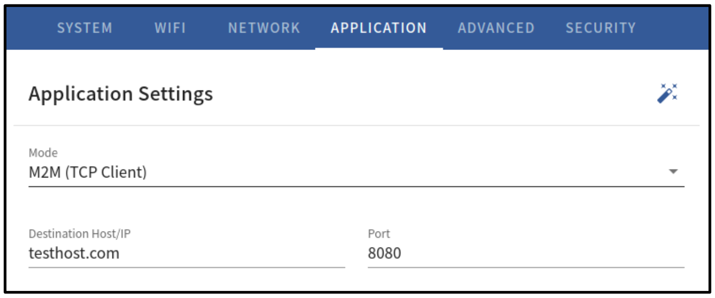
Application Settings

Mode
M2M (TCP Server)

Port
8080

TCP Client

iGS03 plays as a TCP client to communicate with a raw TCP server. Enter the address and port number of the TCP server to connect it.



Application Settings

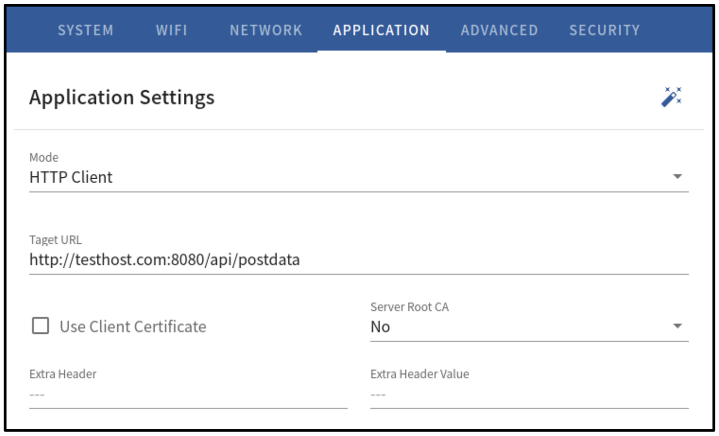
Mode
M2M (TCP Client)

Destination Host/IP
testhost.com

Port
8080

HTTP Client

Another connection in application is through setting iGS03M as a HTTP client. In this scenario, one has to assign the HTTP URL 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.



Application Settings

Mode
HTTP Client

Taget URL
http://testhost.com:8080/api/postdata

☐ Use Client Certificate

Server Root CA
No

Extra Header

Extra Header Value

HTTPS

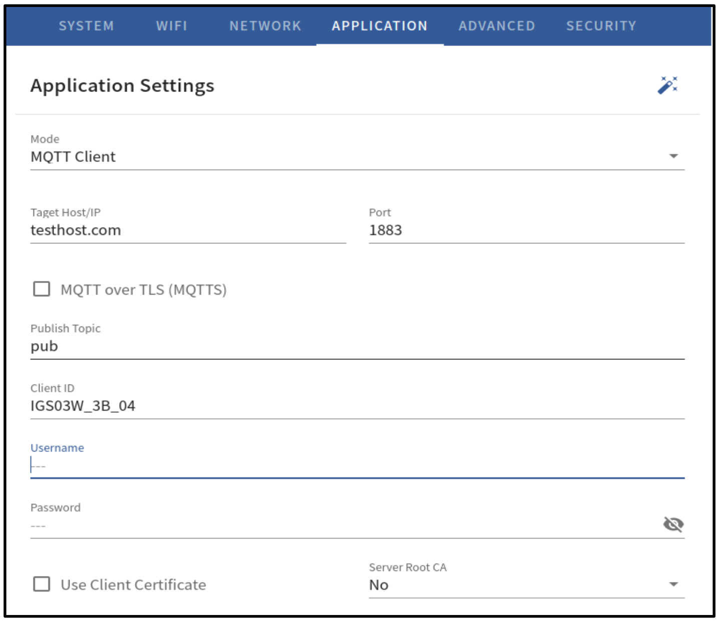
Users can simply use https:// in URL to enable HTTPS. And users can also enable Server Root CA/User Client Certificate based on the server requirement.

MQTT Client

MQTT server is supported by the iGS03. 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. And also can enable Server Root CA/Use Client 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 security page.



Application Settings

Mode: MQTT Client

Taget Host/IP: testhost.com

Port: 1883

□ MQTT over TLS (MQTTS)

Publish Topic: pub

Client ID: IGS03W_3B_04

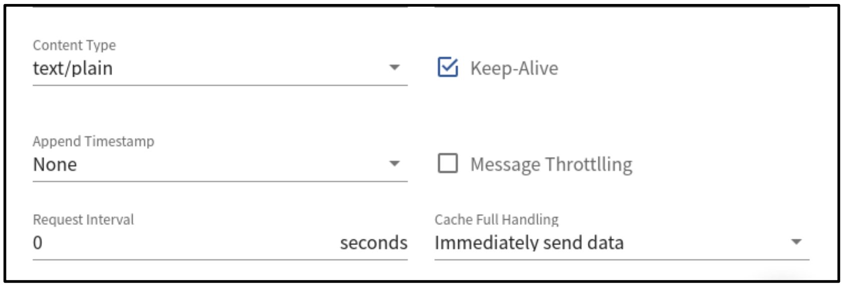
Username: ---

Password: ---

□ Use Client Certificate

Server Root CA: No

Common Settings



Content Type
text/plain

☑ Keep-Alive

Append Timestamp
None

☐ Message Throttling

Request Interval
0 seconds

Cache Full Handling
Immediately send data

Content Type

Users can choose the report data in plain text format or JSON string.

Keep Alive

This option is available for HTTP and MQTT clients. In HTTP client, the device will send HTTP persistent connection to reuse existing tcp session. This enhances the HTTP efficiency. In MQTT client, the device will send a PINGREQ packet to the broker to confirm that it is available and to make sure that the broker is also still available.

Append Timestamp

Devices add the timestamp information in the BLE package format as stated on the page. 5. Users can choose to use the unit in seconds or milliseconds. If the device did not enable NTP time synchronization or the NTP server is unreachable, the report timestamp will be unexpected.

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, iGS03 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.

Advanced

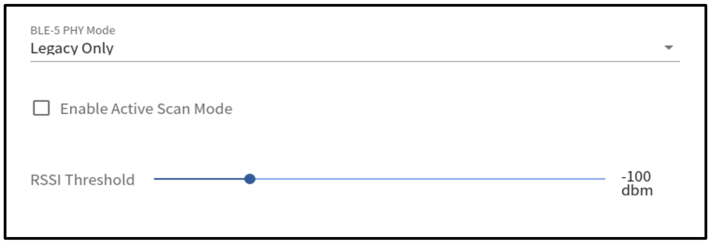
BLE Configuration

BLE-5 PHY Mode

Users can choose to use original BLE PHY or Coded PHT (Long-Range Mode).

Active Scan Mode

Enable active scanning.



BLE-5 PHY Mode
Legacy Only

☐ Enable Active Scan Mode

RSSI Threshold -100 dbm

BLE Filter

Users can set the BLE filter 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 Threshold

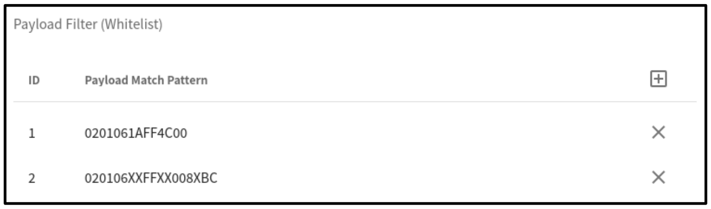
If the bar is pulled right to -50dBm, only the BLE tag/beacon with RSSI larger than or equal to -50dBm(say -45dBm) will be sent out to the server.

Payload Whitelist

Set patterns to configure the whitelist.

Devices will only report the BLE payload which matches one of the patterns.

The character ‘X’ in pattern means ignore.



Payload Filter (Whitelist)

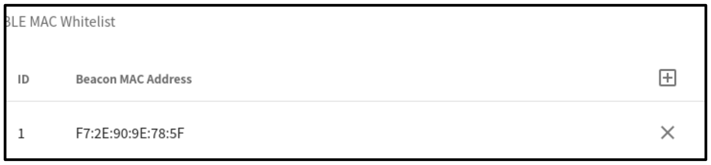
ID	Payload Match Pattern	⊞
1	0201061AFF4C00	×
2	020106XXFFXX008XBC	×

Users can set 6 entries of the payload filter to make sure only concerned information is received.

BLE MAC Whitelist

Set BLE MACs to configure the whitelist.

Users can set 10 MACs to make sure only concerned information is received.



BLE MAC Whitelist

ID	Beacon MAC Address	⊞
1	F7:2E:90:9E:78:5F	×

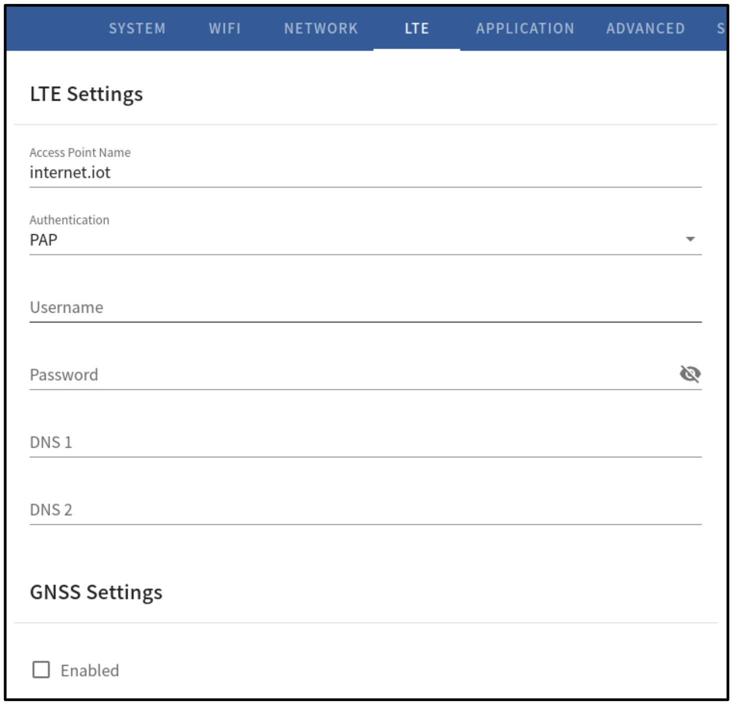
Security

Device Key/Certification/Server CA Upload

Users can upload certification and key here.

This is used by MQTTS and HTTPS.

LTE



LTE Settings

Access Point Name
internet.iot

Authentication
PAP

Username

Password

DNS 1

DNS 2

GNSS Settings

□ Enabled

LET Settings

APN

The APN setting for the carrier setting.

Auth

The auth type based on the carrier setting.

Username/Password

The username/password based on the carrier setting.

GNSS Settings

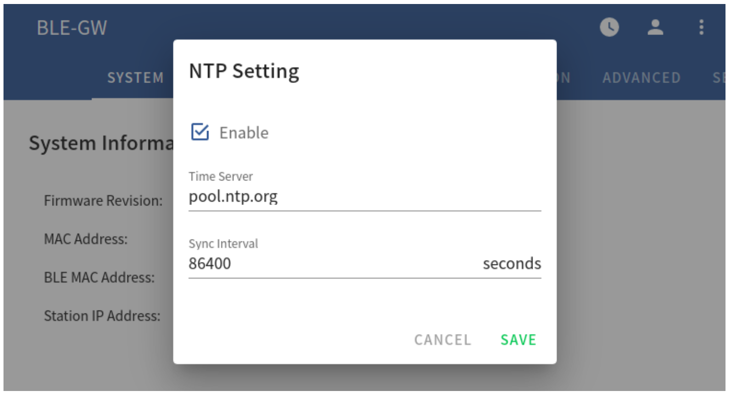
Users can enable the GNSS function here.

NTP Setting

To open the NTP Setting UI, click the "clock" icon in the UI header.

User has to set the time server and the update period to enable NTP.

Remember to save the setting and reboot to make the setting effective.



System Informa

Firmware Revision:

MAC Address:

BLE MAC Address:

Station IP Address:

NTP Setting

☑ Enable

Time Server
pool.ntp.org

Sync Interval
86400 seconds

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.

Revision History

DATE	REVISION	CHANGES
Dec 3, 2019	0a	Initial release
Apr 6, 2020	0b	Update screenshots
Jun 3, 2020	0c	Update photo and diagram
Jul 7, 2020	0d	Update LED behavior
Sep 24, 2020	01	Fix text and layout