



Product Name	GAOTek Healthcare Ethernet Gateway
Product SKU	GAOTek-HI-144
Product URL	https://gaotek.com/product/gaotek-healthcare-ethernet-gateway/

Contact us: sales@gaotek.com

Based in New York City & Toronto, GAO Tek Inc. is ranked as one of the top 10 global B2B technology suppliers. GAO ships overnight within the U.S. & Canada & provides top-notch support thanks to its 4 decades of experience.



Contents

1. Overview	3
2. Payload Format	7
3. Button.....	9
4. LEDs.....	10
5. Configuration.....	11
6. Web User Interface	12

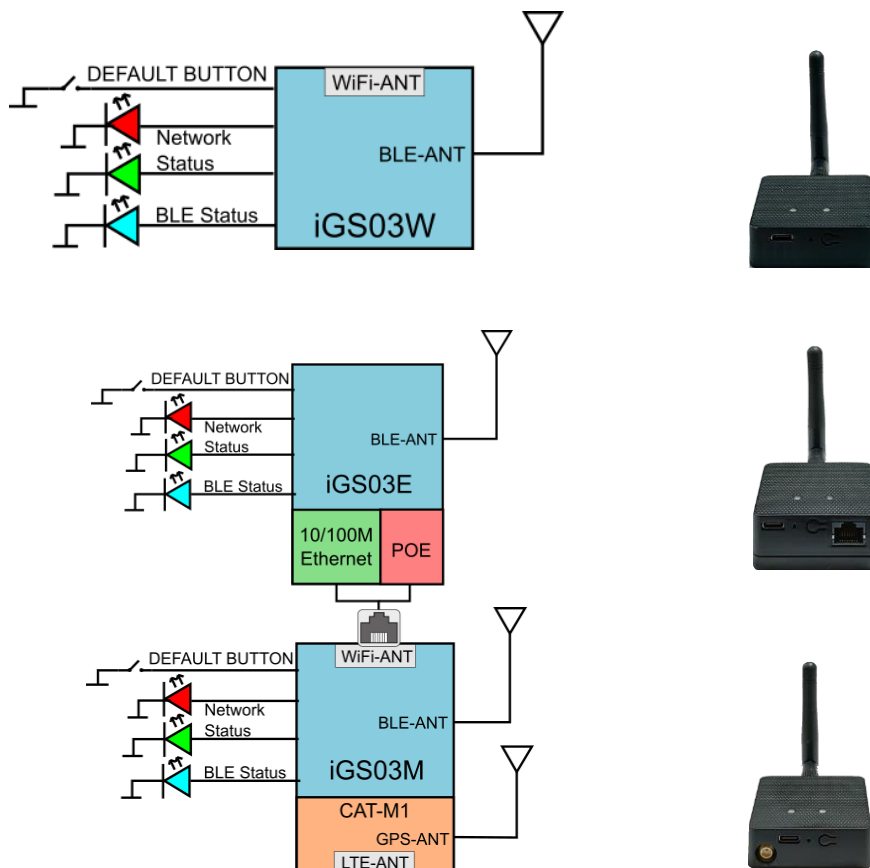
GAOTek Healthcare Ethernet Gateway

This gateway to bridge the local BLE (Bluetooth® Low Energy) tags, sensors, or beacons to remote server/cloud by WIFI, Ethernet 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 this model.

1. Overview

This gateway scans beacons, 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 three models, Model 01, Model 02, and Model 03, representing different uploading interfaces, WIFI, Ethernet, and LTE-M.

Block Diagram







Based in New York City & Toronto, GAO Tek Inc. is ranked as one of the top 10 global B2B technology suppliers. GAO ships overnight within the U.S. & Canada & provides top-notch support thanks to its 4 decades of experience.



SIM

To use LTE-M Model, you have to put a Cat-M1 micro-SIM card into the socket of this model. Please open the bottom cover to insert the SIM card. The steps to open the bottom cover are as below,

<p>Step 1. Remove external BLE antenna</p>	<p>Step 2. Remove the screw from bottom cover</p>
	
<p>Step 3. Use finger to press and hold the arrowpart</p>	<p>Step 4. Pull out the bottom cover</p>
	



WiFi (Model 01/ Model 03)

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

Ethernet (Model 02)

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

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. LE 1M PHY: including BLE4.2(Legacy)/BLE5, 1M in 100% duty cycle
2. LE Coded PHY: BLE5, 125K(Long Range) in 100% duty cycle

The default PHYMODE is 1, LE 1M PHY mode.

Users can use web UI or telnet command to configure the mode.

GNSS (Model 03)

The GNSS function is turned “off” by default. Users can use webUI to enable or disable GNSS. For detail settings, use below telnet 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 positioned for 5 times with a 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.



2. Payload Format

There are several kinds of payload format that 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

\$RSPR 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,157
4921085

\$LRAD,51A88AD374B7,CC4B73906F96,-
87,02010212FF0D0083BC280100AAAAFFFF000010030000,1574921085

\$GPRP,0C61CFC1452E,E7DAE08E6FC3,-
44,0201061AFF4C000215B9A5D27D56CC4E3AAB511F2153BCB9670001452ED6
(iBeacon, UUID: B9A5D27D56CC4E3AAB511F2153BCB967, Major: 0001, Minor: 452E)

GNSS (Model 03)

General format:

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

- "\$GPSR,<tag_mac>,<reader_mac>,<rsi>" fields are for compatibility with other reports. The tag_mac is always the same as reader_mac and the rsi is always -127.
- yymmdd,hhmmss.ss is the UTC time when the position is acquired.
- speed: The unit is knots.
- hdop: Horizontal dilution of position

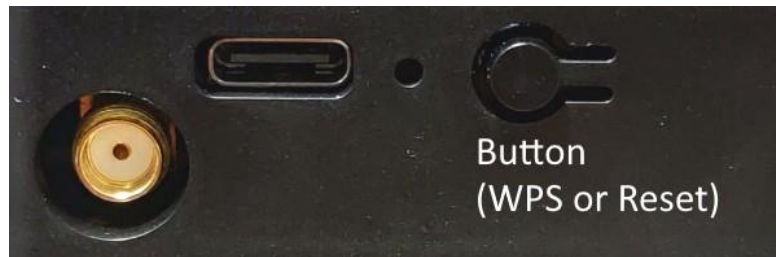
Example:

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

3. Button

One button is located on the back panel. It is used for WPS function or Reset to default settings.

Function	Trigger Condition
WPS (iGS03W/M)	short press for over 1sec and release
Reset to default settings	long press for over 3 sec



Reset to Default

Pressing the reset button on your device for over 3 secs to retrieve the default setting. While the network status LED turns into red light, release the button, and the iGS03M will reboot with its default settings.

WPS

Users can use the WPS button to join Model 01/03 to the WiFi Access Point. First press the WPS button on your Access Point, when it is ready, then press the WPS button for over 1 sec on the Model 03 device to join the Access Point.

4. LEDs

There are two LEDs indicating the current status. 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/LTE-M connection success (This only implies the network is connected. It doesn't mean the server is connected)	<p>Green: WiFi/LTE-M network transmission happening</p> <p>Orange: If Model 03 does not insert SIM card and being used as WiFi device</p>



Network Behavior	Status LED	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
ORANGE LED on		Network ready (If SIM card is not inserted)	Ready/Idle
GREEN LED blink (200ms on/off)		Network is transferring data (If SIM card is not used on iGS03M, shows ORANGE LED blink instead)	Busy
RED LED ON (1sec)		Connect failure	Error
RED LED blink (5sec on/off)		Misconfiguration	Error
RED LED ON (5sec)		LTE init failure	Error

5. Configuration

Model 01 & Model 03

To configure the unit, you have to connect it through the 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 below 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”. The following sections describe details of the web UI.

Model 02

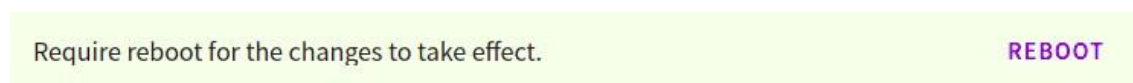
Model 02 is a DHCP client by default. To configure it, you have to connect it to a router with DHCP enabled. The first thing is to find model’s IP address in this network so that you can get into it’s webUI for configuration. If you don’t know the IP address, you may need to use some tool to find it.(For 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)

6. Web User Interface

You can review current configuration or modify it on the web UI. There are various function groups listed on the top of UI.



Any change in the page needs to be saved first before switching to another page, otherwise the modification will be lost. And after all changes made, click reboot to make the changes effective.





System

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

Wi-Fi

Users can configure Model03's WiFi device as an WiFi AP or join to the other AP. The relateds

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.

A screenshot of a web interface for AP Settings. It shows a form with the following fields: SSID (IGS03M_18_C4), Security (WPA2-PSK), Channel (6), and Password (represented by dots). There is a small icon to the right of the password field.

AP Settings

SSID
IGS03M_18_C4

Security WPA2-PSK Channel 6

Password
.....

Password: 8-63 characters can be input

Channel: 1~11(ch12 and ch13 could be supported by request)ettings can be managed on this page.

Station Mode

This mode is used for transferring data by *WiFi.

Scan: Click it to scan available APs. The scan result list will be displayed on 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 result list.

AP Client Settings

SSID
TargetAP SCAN

Security
WPA2-PSK ▼

Password
..... 🔒

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/herself.

Password: Type the one assigned in your AP.

***Note: In data transfer, by default, WiFi has higher priority than LTE. So for Model 03 if both interfaces are configured correctly and connected, the data will be transferred by WiFi.**

Users can change the priority through the Telnet command.

Network

WiFi Address (Device Address for Model 02)

WiFi Address

Mode
DHCP Client ▼

WiFi Address

Mode
Static IP ▼

IP Address	Netmask
192.168.0.1	255.255.255.0

Default Gateway
192.168.0.254

DNS Server 1	DNS Server 2
8.8.8.8	1.1.1.1



This setting is for configuring in WiFi Station mode or IGS03E. Normally the “DHCP Client” is used to obtain an IP Address from WiFi AP (or DHCP server for ethernet). If one wants to manually assign an IP address for iGS03, choose “Static IP” to to assign the IP Address, Netmask, Gateway, and/or DNS servers.

DHCP Server (WiFi AP)

DHCP Server (WiFi AP)	
IP Address	192.168.10.1
Netmask	255.255.255.0

The default IP address of iGS03 in WiFi AP mode is 192.168.10.1 and the netmask is 255.255.255.0. In case the user wants 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 192.18.0.X.

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.

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.

Mode M2M (TCP Client) ▼	
Destination Host/IP testhost.com	Port 8080

HTTP Client

Another connection in application is through setting iGS03 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.

Mode HTTP Client ▼	
Target URL http://testhost.com:8080/api/post_data	
<input type="checkbox"/> Use Client Certificate	Server Root CA No ▼
Extra Header ---	Extra Header Value ---
Content Type text/plain ▼	<input checked="" type="checkbox"/> Keep-Alive

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. The certificate files can be uploaded on the Security page.



MQTT Client

Configure iGS03 to connect MQTT broker for publishing data. 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.

A screenshot of a web-based configuration form for an MQTT Client. The form includes fields for Mode (MQTT Client), Target Host/IP (testhost.com), Port (1883), a checkbox for MQTT over TLS (MQTTS), Publish Topic (pub), Client ID (IGS03M_18_C4), Username (---), Password (---), a checkbox for Use Client Certificate, and a dropdown for Server Root CA (No).

Mode MQTT Client	
Target Host/IP testhost.com	Port 1883
<input type="checkbox"/> MQTT over TLS (MQTTS)	
Publish Topic pub	
Client ID IGS03M_18_C4	
Username ---	
Password ---	
<input type="checkbox"/> Use Client Certificate	Server Root CA No

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.



Common Settings

Content Type

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

Content Type text/plain	▼	<input checked="" type="checkbox"/> Keep-Alive
Append Timestamp None	▼	<input type="checkbox"/> Message Throttling
Request Interval 0	seconds	Cache Full Handling Immediately send data

Keep Alive

This option is available for HTTP

clients. The device will use HTTP persistent connection to reuse existing tcp sessions. This enhances the HTTP efficiency.

Append Timestamp

Devices add the timestamp information in the BLE package format as stated on the page. 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 server. This is useful for reducing data 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 (depends on Cache full handling option) or the time interval is reached.

Based in New York City & Toronto, GAO Tek Inc. is ranked as one of the top 10 global B2B technology suppliers. GAO ships overnight within the U.S. & Canada & provides top-notch support thanks to its 4 decades of experience.



Cache full handling

This model has a limited cache buffer. The user needs to decide “sending data immediately” or “discard new input data” if cache is full.

- If the user selects "sending data immediately", the device will keep on uploading data when cache is full to avoid data loss regardless of your "request interval setting". That will cause more data traffic.
- If the user selects "discard new input data", the device will not send data before reaching the request interval.

Throttle Control

If throttle control is enabled, iGS03 will keep the last record for each TAG/Beacon ID in the given interval (request interval). In this way, one can reduce the data transmission to the server.

Cloud IoT Helper

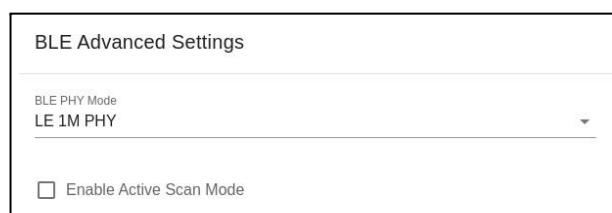
The cloud IoT helper can be launched by the “magic wand”, it is used to assist users to configure AWS IoT, Azure IoT or Google Cloud IoT usage.

Advanced

BLE Configuration

BLE PHY Mode

Users can choose to use LE 1M PHY or LE Coded PHY (Long-Range Mode).



Based in New York City & Toronto, GAO Tek Inc. is ranked as one of the top 10 global B2B technology suppliers. GAO ships overnight within the U.S. & Canada & provides top-notch support thanks to its 4 decades of experience.



Active Scan Mode

Enable active scanning.

BLE Filter

Users can set the BLE filter to filter out the unwanted BLE advertising data. There are three kinds of filters supported by this model

.

RSSI Threshold

If the bar is pulled right to -50dBm, only the BLE tag/beacon with RSSI larger than or equal to -50dBm will be transmitted to the server.



Payload Whitelist

Set patterns to configure the BLE payload whitelist. Devices will only report the BLE payload which matches one of the patterns.

Click on the “plus” button to add a new pattern. The character ‘X’ in pattern means ignore the character. Also you can click the “magic wand” to select a preset pattern for iBeacon, Eddystone, or INGICS beacons.

BLE MAC Whitelist

ID	Beacon MAC Address	
1	AA:BB:CC:12:13:45	×
2	AD:12:31:54:67:34	×



Users can set up to 6 entries of the payload filter to make sure only relevant information is received. If the pattern list is empty, it means the payload whitelist function is disabled, all payload will be allowed.

BLE MAC Whitelist

Set BLE beacon MAC addresses to configure the BLE MAC whitelist.

Gateway will only report the advertising data broadcasted from the beacons which match the whitelist.

Payload Filter (Whitelist)

ID	Payload Match Pattern	
1	0201061AFF4C00	×
2	020106XXFF5900XXBC	×

Users can set up to 10 MACs to make sure only relevant information is received. If the list is empty, it means the BLE MAC whitelist function is disabled. All BLE beacons are allowed.

Security

Device Key/Certification/Server CA Upload

Users can upload device certification, private key and server CA files in PEM format on this page. All these files may be used by MQTTS or HTTPS functions.



LTE

LET Settings

Access Point Name

The APN setting for the carrier setting.

Authentication

The auth type based on the carrier setting.

Username/Password

The username/password based on the carrier setting.

LTE Settings

Access Point Name
internet.iot

Authentication
PAP

Username

Password

DNS 1

DNS 2

GNSS Settings

Enabled

DNS Servers

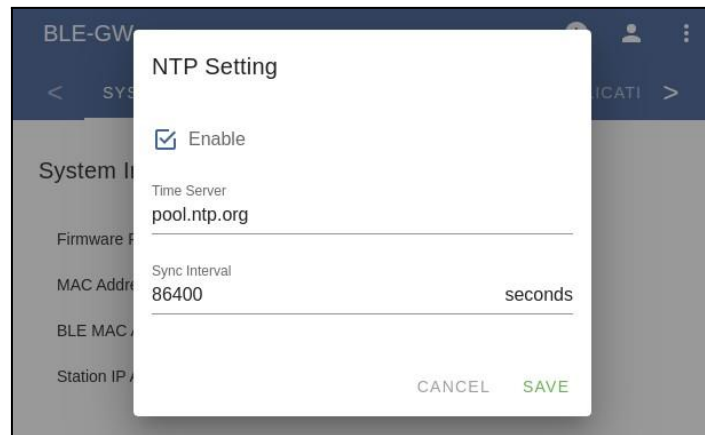
In case the users want to specify his/her own DNS servers.

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.



Login Password

One can change the login password from the “people” icon on the UI header. Be aware that it changes the login password of the telnet console, too.

