



Product Name	GAOTek Wireless IoT Network
Product SKU	GAOTek-HCI-114
Product URL	https://gaotek.com/product/gaotek-wireless-iot-network/



CONTENTS

1. Purpose:	4
2. Introduction:	4
Specifications:	4
3. External interface.....	6
3.1. Network interface.....	6
3.2. Power supply interface:	6
3.3. LED indicator.....	6
3.4. Reset Button.....	6
3.5. Insert SIM Card (If needed)	7
4. Configuration.....	8
4.1. Connect to Product.....	9
4.2. Network interface.....	10
4.2.1. Configure WAN interface	10
4.2.2. View the WAN interface status.....	15
4.2.3. Configure Product Wi-Fi AP	17
4.3. Service configuration	18
4.3.1. Advertisement Upload Parameters	18
4.3.2. MQTT without SSL configuration	23
4.3.3. MQTT with SSL configuration.....	25
4.3.4. HTTP configuration.....	27
4.3.5. Cache Message	28
4.3.6. Upload GPS Configuration.....	28
4.3.7. BLE Scan Mode.....	29
4.3.8 BLE Active Scan	30
4.4. Modify the Web Portal Login Password	30
4.5. Network diagnostics.....	31
5. Quick verify Product API	32
5.1. How to verify HTTP API	32
5.2. How to verify MQTT API.....	33
6. More System Settings.....	33



- 6.1. System clock 33
- 6.2. System update 35
- 6.3. BLE Firmware..... 36
- 7. Trouble shooting..... 36
 - 7.1. The Product flash red LED..... 36
 - 7.2. The Cellular signal is very poor 42
- 8. Appendix1 Advertisement Upload Filter for different scenario 44
 - 8.1. Scenario 1: Only upload nearby beacon advertisement 45
 - 8.2. Scenario 2: Reduce advertisement message to clouds 46
 - 8.3. Scenario 3: Only upload specific MAC address to clouds..... 46
 - 8.4. Scenario 4: Only upload iBeacon advertisement 47
 - 8.5 Scenario 5: Only upload Eddystone advertisement..... 49
 - 8.6. Scenario 6: Filter advertisement packet by service ID..... 50
 - 8.7. Scenario 7: Beacon Location..... 50
- 9. Appendix2 Setup your own MQTT Server 51



GAOTek Wireless IoT Network - GAO Tek

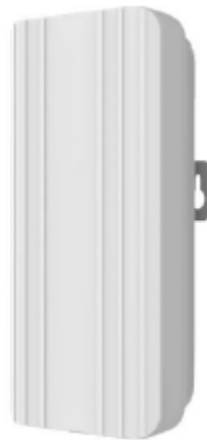
1. Purpose:

This document describes the basic functions and physical interfaces of the product, which is mainly used to guide users to install and configure the product.

2. Introduction:

The product is used to collect the data from the devices and then sends to the cloud server. Also, it can accept data command from the cloud server and forward it, such as updating the configuration. The product uses open MQTT + JSON API interface for third-party integration.

GAOTEK supply two model. Below are the details:



KG01

Specifications:

- Waterproof IP54, suitable for outdoor use cases.
- Material: ABS
- Product size: 173 x 90 x 40mm, installed by wall mounting.
- BLE chipset: Nordic nRF52833; support BLE4.0/4.1/4.2/5.0
- WIFI chipset (MCU): MTK7628
- Power supply: POE or DC 5V

- Scanning ability: 240 Beacons per second
- Wireless distance: 150 meters
- MAX TX power: 8dBm
- Transmitting way: WIFI / WIFI hopping / Ethernet / Cellular(optional)
- API protocol: HTTP / MQTT
- Certification: CE / FCC



KG02

Specifications:

- Suitable for indoor use cases.
- Material: ABS
- Product size: 165 x 165 x 25mm, installed by wall mounting.
- BLE chipset: Nordic nRF52832; support BLE4.0/4.1/4.2/5.0
- WIFI chipset (MCU): MTK7628
- Power supply: POE or DC 5V
- Scanning ability: 240 Beacons per second
- Wireless distance: 300 meters
- MAX TX power: 8dBm
- Transmitting way: WIFI / WIFI hopping / Ethernet / Cellular(optional)
- API protocol: HTTP / MQTT
- Certification: CE / FCC



3. External interface

3.1. Network interface

The supports to connect to the internet through following ways:

1. Through Wi-Fi.
2. Through Ethernet cable.
3. Though Cellular network (optional, only available when the LTE USB dongle is inserted).
4. The supports Wi-Fi Hopping, which means one product can connect to internet by another product.

3.2. Power supply interface:

There are two interfaces for power supply: micro-USB interface and Ethernet POE port.

- POE power supply, directly supply power by Ethernet cable interface using POE (802.3af) to supply power.
- Micro USB power supply, powered by DC 5V/1A.

Warning: The product can use only one of the two power supplies at a time. Please don't insert two power supplies at the same time, otherwise product may be damaged.

3.3. LED indicator

Product has 2 LED indicators. The specific meanings are as follows:

1. Red LED indicator:

- **Quick flash** (flash 3 times every second): indicates that the product is booting.
- **Slow flash** (flash every 2 seconds): indicates that the product boots successfully but cannot connect to the cloud.

2. Green LED indicator

- **Quick flash** (flash every 2 seconds): indicates that the Product successfully connects to the cloud and report advertisement packet successfully.
- **Slow flash** (flash every 10 seconds): indicates that the Product connects to the cloud successfully, but it didn't find any devices.

3.4. Reset Button

1. Single press button can reboot the gateway.

2. Long press button for more than 8 seconds can restore the gateway to factory settings.

3.5. Insert SIM Card (If needed)

Please note: This procedure is provided only for the Product with USB dongle and LTE module installed.

For Product KG01 & KG02, insert SIM card from the hole in the side of the picture below:



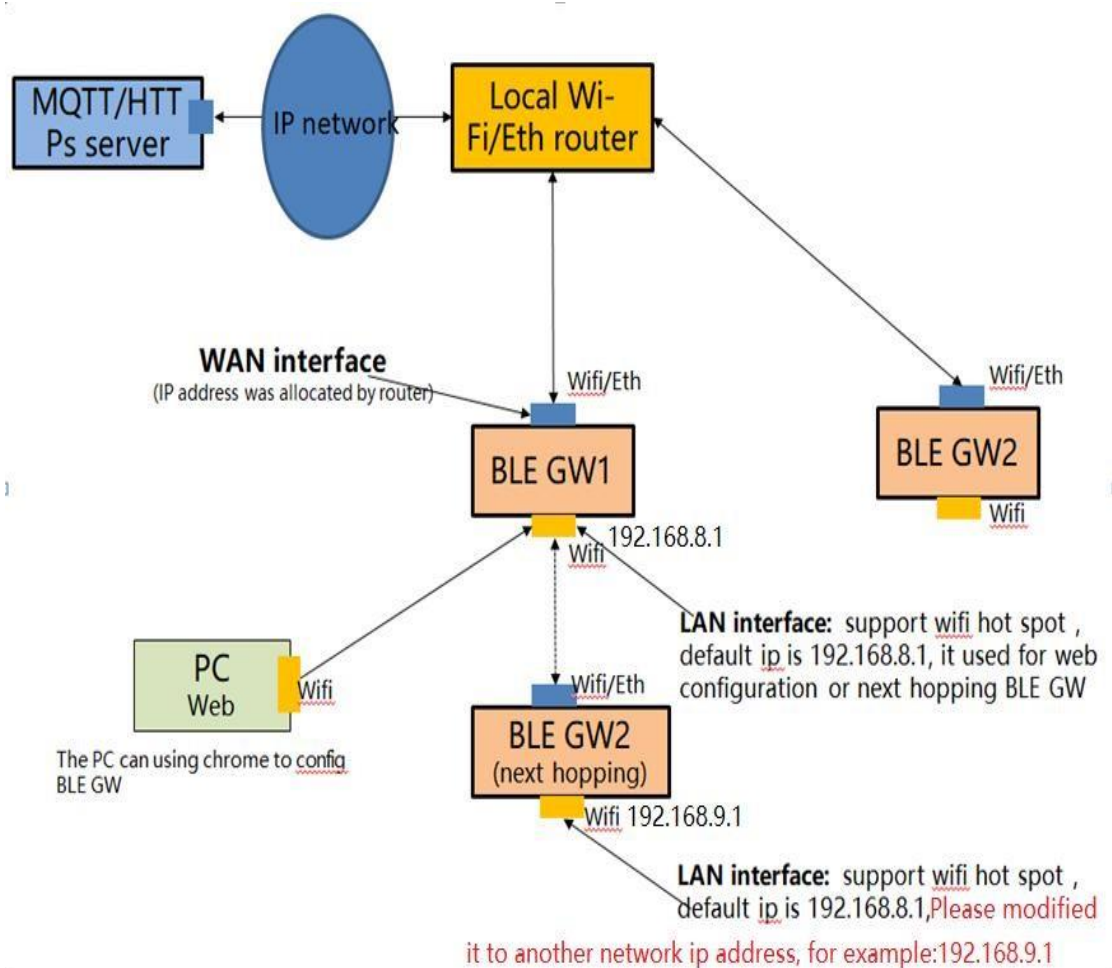
KG01



KG02

4. Configuration

The Product is configured in web portal mode. You can use a web browser to configure it. Chrome browser is recommended to use for the configuration.



As shown above, each GW has two interfaces with different IP addresses. One of these IP addresses (referred to as the WAN port) is used to connect to the internet network (MQTT server), which has a series of firewall rule protection. The other IP address (referred to as LAN port, also known as the intranet interface) is used for Wi-Fi hotspot broadcasting.



WAN Port: This interface supports Wi-Fi and ETH (network wire). Product can connect to routers via Wi-Fi or network wire, where IP addresses are assigned by routers. The Product is connected to the MQTT/HTTPs server through this interface, so you need to ensure that the network between this interface and the MQTT server is interconnected. WAN address IP address configuration see "4.3.2 configuration WAN port network connection".

LAN port: This interface only supports Wi-Fi. The default IP address of this interface is 192.168.8.1, PC can connect to this interface through Wi-Fi, or the next hopping Product can connect to the internet by Upper level.

If you need to configure the gateway, you can only configure it through Wi-Fi, and you cannot configure it through the network line (for security reasons, the network line interface only supports the WAN interface).

4.1. Connect to Product

- After power on, the Product will automatically broadcast Wi-Fi signal, and the default Wi-Fi name is “beacongw_mac address”



- The default Wi-Fi connection password is “12345678”
- The default Product configuration IP address is 192.168.8.1
- Login to the gateway by typing http://192.168.8.1 in the browser.
- Enter the user’s name: ‘admin’ and password: ‘admin’



Gateway

Authorization Required

Please enter your username and password.

Username

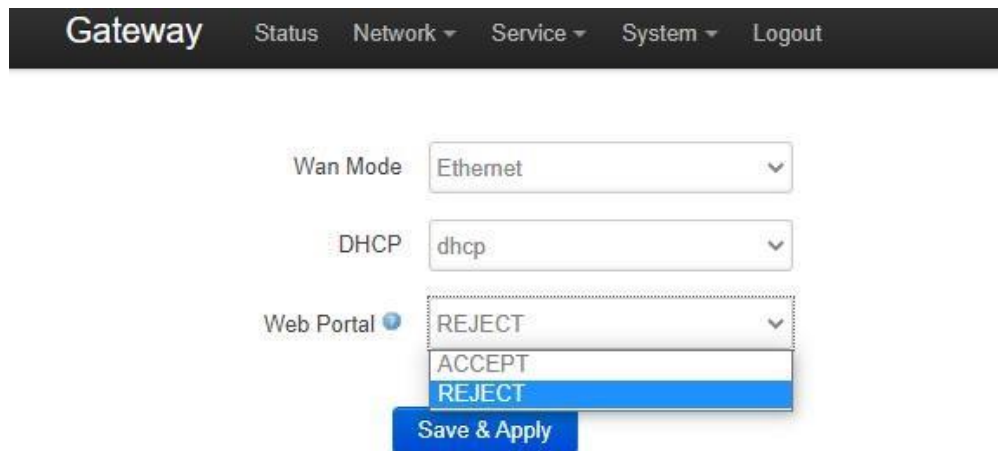
Password

4.2. Network interface

4.2.1. Configure WAN interface

Tap on **Network-Interface** to go to the network configuration page. You can choose to connect to the internet network using Wi-Fi /Ethernet/Cellular connection.

4.2.1.1. Connect to internet by Ethernet

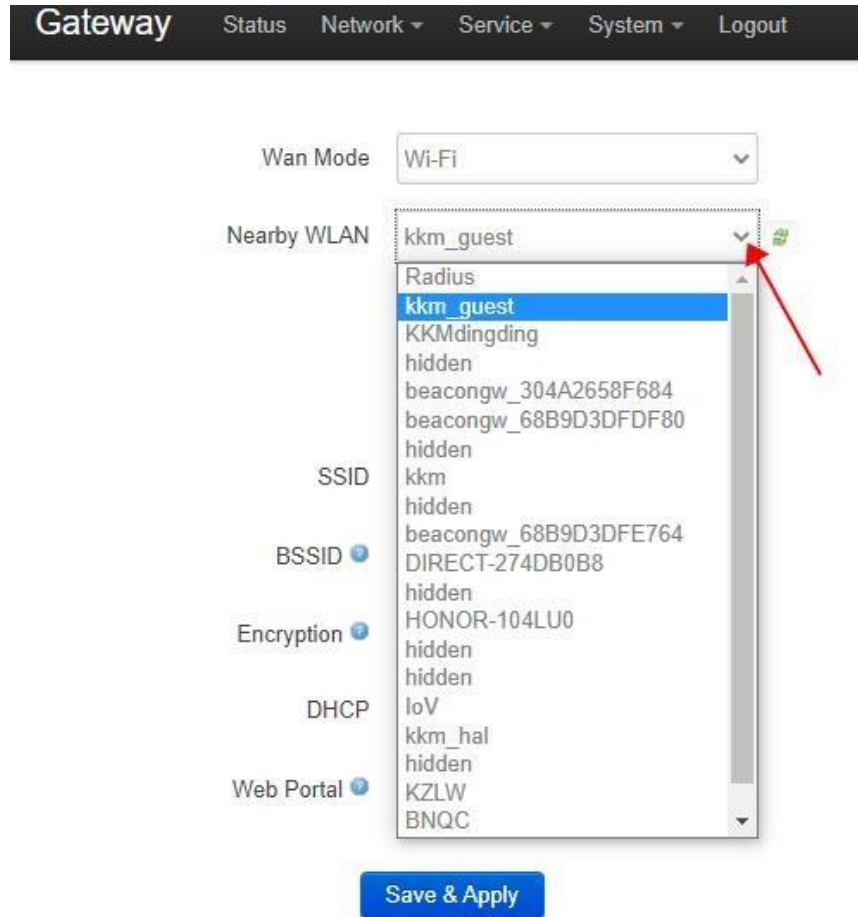


The screenshot shows the 'Gateway' configuration page with a navigation bar containing 'Gateway', 'Status', 'Network', 'Service', 'System', and 'Logout'. The 'Network' section is active. It features three dropdown menus: 'Wan Mode' set to 'Ethernet', 'DHCP' set to 'dhcp', and 'Web Portal' set to 'REJECT'. The 'Web Portal' dropdown is open, showing 'REJECT' (selected), 'ACCEPT', and 'REJECT'. A blue 'Save & Apply' button is at the bottom.

The IP address can be assigned in DHCP or static configuration.

Web Portal: When the option is ACCEPT, you can login to the web portal through WAN IP.

4.2.1.2. Connect to internet by WIFI



The screenshot shows the 'Gateway' configuration interface. At the top, there is a navigation bar with 'Gateway' in bold and 'Status', 'Network', 'Service', 'System', and 'Logout' as menu items. Below this, the 'Wan Mode' is set to 'Wi-Fi'. The 'Nearby WLAN' section is expanded, showing a list of detected networks. A red arrow points to the dropdown arrow on the right side of the 'Nearby WLAN' list, which is currently set to 'kkm_guest'. The list includes the following entries:

Property	Value
Radius	kkm_guest
Radius	KKMdingding
Radius	hidden
Radius	beacongw_304A2658F684
Radius	beacongw_68B9D3DFDF80
Radius	hidden
SSID	kkm
SSID	hidden
BSSID	beacongw_68B9D3DFE764
BSSID	DIRECT-274DB0B8
BSSID	hidden
Encryption	HONOR-104LU0
Encryption	hidden
Encryption	hidden
DHCP	loV
DHCP	kkm_hal
DHCP	hidden
Web Portal	KZLW
Web Portal	BNQC

At the bottom of the configuration area, there is a blue 'Save & Apply' button.



Gateway Status Network ▾ Service ▾ System ▾ Logout

Wan Mode: Wi-Fi ▾

Nearby WLAN: KKMdingding ▾

Encryption: WPA2 PSK (CCMP)
BSSID: 18:BC:5A:90:92:C0
Signal: -31dBm
Channel: 11

SSID: KKMdingding

BSSID : 18:BC:5A:90:92:C0

Encryption : WPA2-PSK ▾

Cipher : CCMP(AES) ▾

Key : * (highlighted with a red box)

DHCP: dhcp ▾

Web Portal : REJECT ▾

Save & Apply

Click on the down arrow of “Nearby WLAN”, then you can select a Wi-Fi that is available. Enter the Wi-Fi password to the “Key” column to connect to this Wi-Fi.

Connect to a hidden Wi-Fi AP:

You can see some Wi-Fi hidden. You should input the Wi-Fi name and password if you want to connect to it.

If your Wi-Fi AP name does not appear in the nearby WLAN list, please try to reboot the Product. (In “System” page, you can reboot the device)



Encryption: Product support many types of Encryptions, including WPA2-EAP. This encryption is also known as 802.1x/EAP, 802.1x Enterprise WPA2 or Enterprise WPA2. It is suitable for Enterprise Gateway deployment.

Wan Mode	Wi-Fi
Nearby WLAN	kkm
SSID	kkm
BSSID	
Encryption	WPA2-PSK
Cipher	No Encryption WEP Open System WEP Shared Key WPA-PSK
Key	WPA2-PSK
DHCP	WPA-PSK/WPA2-PSK WPA-EAP WPA2-EAP
Web Portal	REJECT



4.2.1.3. Connect to internet by cellular

Wan Mode	<input type="text" value="Cellular"/>
APN	<input type="text"/>
Pin Code	<input type="text"/>
PAP/CHAP username	<input type="text"/>
PAP/CHAP password	<input type="text"/>
Authentication Type	<input type="text" value="Customer"/>
DHCP	<input type="text" value="dhcp"/>
Web Portal	<input type="text" value="REJECT"/>

Please make sure SIM card is inserted in the KGateway.



4.2.2. View the WAN interface status

4.2.2.1. Ethernet status

Gateway	
Status	Network ▾
Service ▾	System ▾
Logout	
System information	
Model	KG02
AP MAC	68:B9:D3:DF:E7:64
Local Time	Thu Aug 18 22:20:59 2022
Uptime	0h 26m 22s
Load Average	0.83, 0.46, 0.31
Memory Free	76356 kB / 125016 kB (61%)
Network information	
WAN MAC	68:B9:D3:DF:E7:66
WAN Type	Ethernet
WAN IP	N/A
Router IP	N/A
DNS IP	N/A
Connected Time(Sec)	N/A
RX Bytes	140527
TX Bytes	181236
Cellular Info	

Model: The model's name of the connected Product The **AP MAC** is also printed in the Product shell.

WAN IP: The gateway IP address in WAN interface.

Router IP: Your router IP address.



Uptime: How long the network interface has been active.

RX Bytes: received data from WAN interface.

TX Bytes: sent data to WAN interface.

4.2.2.2. Cellular status

Network information	
WAN MAC	30:4A:26:5B:FA:32
WAN Type	Cellular
WAN IP	N/A
Router IP	N/A
DNS IP	N/A
Connected Time(Sec)	N/A
RX Bytes	39263427
TX Bytes	23625648
Cellular Info	Type:lte; RSRP:-92; SNR:264

If the Product connect to internet by cellular, the cellular signal will show in this page.

- Very good signal: RSRP>-85dBm.
- Good signal: RSRP=-85 to -95dBm.
- Middle signal: RSRP=-95 to -105dBm.
- Pool signal: RSRP=-105 to -115dBm.
- Very pool signal: RSRP<-115dB.



4.2.3. Configure Product Wi-Fi AP

Check status about Product, you can change the AP LAN IP address.

WIFI AP CONFIGURATION

AP SSID	<input type="text" value="beacongw_68B9D3DFE764"/>
AP LAN IP	<input type="text" value="192.168.8.1"/>
AP Password	<input type="password" value="*****"/> *
AP SSID Hidden	<input type="checkbox"/>
AP Disabled	<input type="checkbox"/>



If 'AP Disabled' is selected, you will not be able to connect to the product.

Through Wi-Fi. You can only connect to the Product through WAN IP for configuration.

And when AP is disabled, you need to set Web Portal as 'ACCEPT' so you can login the web portal through WAN IP. If you disable the AP but web portal is not ACCEPT, you can restore the Product to factory settings.

Gateway Status Network ▾ Service ▾ System ▾ Logout

Wan Mode	<input type="text" value="Ethernet"/>
DHCP	<input type="text" value="dhcp"/>
Web Portal	<input type="text" value="REJECT"/>



4.3. Service configuration

Click “Service”-” Filter Setting” and “Cloud Setting”-” Others Setting” to go to the gateway setting page, where each field is defined as follows:

4.3.1. Advertisement Upload Parameters

Gateway	Status	Network	Service	System	Logout
Upload Interval(Unit:Sec)					
Filter by RSSI(Unit:dBm)					
Filter by ServiceID					
Filter by mac					
Filter by BLE name					
Filter by raw					
Filter duplicate data					
Upload iBeacon					
Upload Eddystone					
Upload KSensor					
Upload Proximity					
Upload Unknown					
Upload without BLE data					
Advertisement timestamp					

[Save & Apply](#)

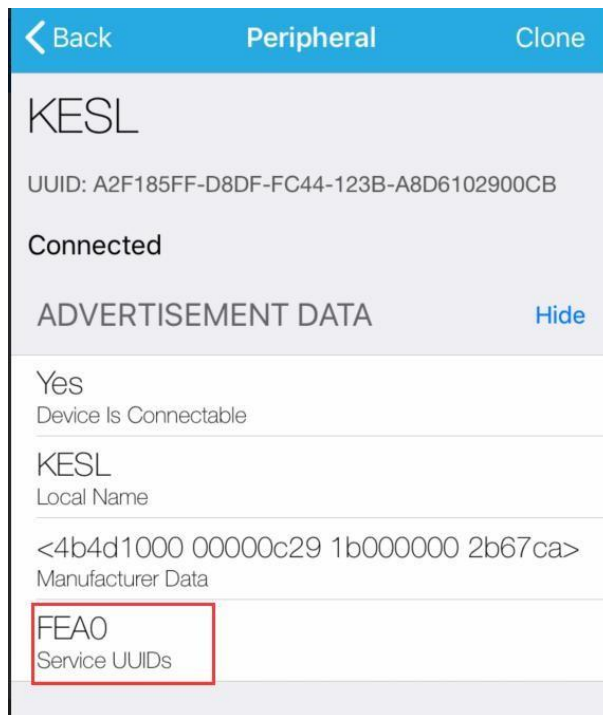
1. Upload Interval: Product uses this parameter to control upload period of modified advertisement data of Product to Cloud.

It needs at least **Upload Interval** seconds for Product to send advertisement to cloud.

2. Filter by RSSI: If this parameter is set, the Product will only report the advertisement packet which signal is > **Min Rssi** value.

3. Filter by Service ID: If this parameter is set, the Product will only report the advertisement packet which includes the setting BLE service ID.

Following example use Lightblue App on IOS to view the device service UUIDs, then you can set the services filter to 0xFEAO.



4. Filter by mac: Product can use this parameter to filter Product mac address. This parameter uses Regular express.

For example, if Ble Mac filter value set to ^20DD, then following Product advertisement packet will report to cloud.



1 Product1: ble mac = 0x20DD01000002 : report to cloud
1 Product2: ble mac = 0xA133DD010002 : not report to cloud
1 Product3: ble mac = 0xA10005033DD2 : not report to cloud

5. Filter by BLE name: Product can use this parameter to filter device name. This parameter uses Regular express.

Note: BLE name can be carried in the message of advertisement or the scanning response. If you want to filter the advertisement, please ensure that BLE name is carried in the advertisement message.

The device name of Product is carried in the Scan response message.

6. Filter by raw: Product can use this parameter to filter raw packet. This parameter uses Regular express.

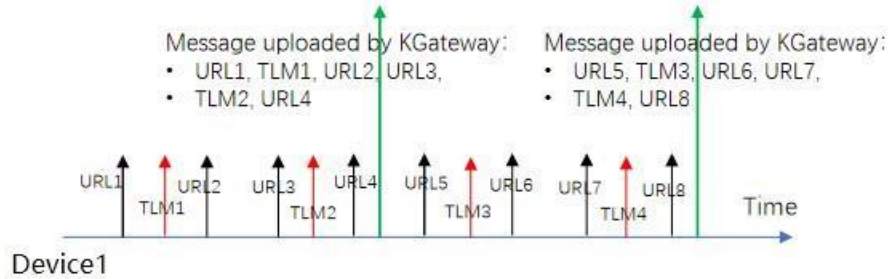
7. Filter duplicate data: Product can use different parameter combinations to filter duplicate data to reduce the advertisement message to cloud.

- No filter: Product will not filter the data.
- By mac: Product can use this parameter to filter the data of the same mac address.
- By mac+type: Product can use this parameter to filter the data of the same mac address and advertisement packet type.
- By mac+raw: Product can use this parameter to filter the data of the same mac address and raw packet.

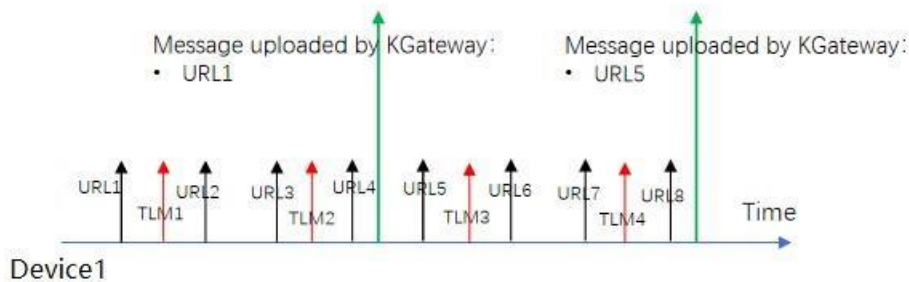
The following is an example of the message uploading of the device1 device:

1. Device1 is configured to broadcast 2 slots, where Slot0 broadcasts URL and the Adv interval is set to 1 second. Slot1 broadcasts the TLM, and the Adv interval is set to 2 seconds.
2. The Upload Interval of Product is set to 4 seconds.

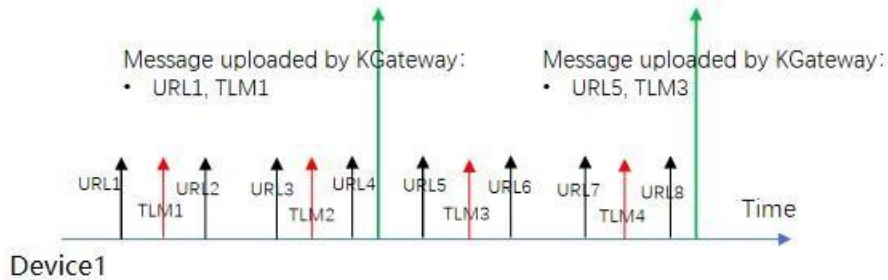
Config1: No filter



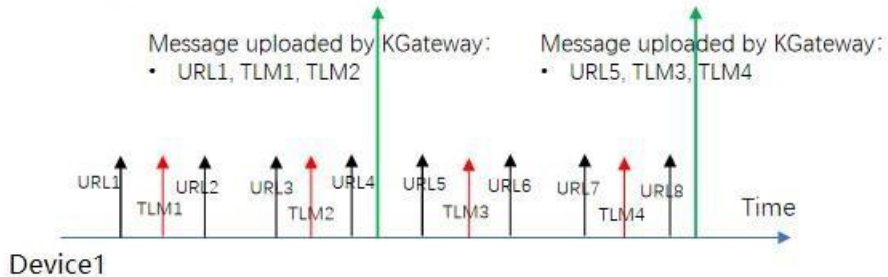
Config2: Filter by MAC



Config3: Filter by MAC + Type



Config4: Filter by MAC + Raw





Since the URL message does not change, it is only reported once each interval. The TLM content changes every time, both TLM1 and TLM2 will upload.

8. Upload iBeacon: ‘Yes’ means Product will report iBeacon protocol advertisement.

9. Upload Eddystone: ‘Yes’ means Product will report Eddystone (URL / TLM / UID) protocol advertisement.

10. Upload KSensor: ‘Yes’ means Product will report GAOTEK KSensor protocol advertisement.

11. Upload Proximity: ‘Yes’ means Product will report GAOTEK social distancing products advertisement that using hex string.

12. Upload Unknown: ‘Yes’ means Product will report unknown advertisement that using hex string.

13. Upload without BLE data: ‘Yes’ means Product will report the advertisement without BLE parameters data. Only report the Mac address and RSSI of device to reduce the advertisement message to cloud.

14. Advertisement timestamp: The three formats of advertisement time.

- yyyy-MM-dd HH:mm:ss.Z
- yyyy-MM-dd HH:mm:ss
- UTC second



4.3.2. MQTT without SSL configuration

Gateway				
Status	Network	Service	System	Logout
Service Access	MQTT			
MQTT Type	tcp://			
MQTT URL	mqtt.kkmiot.com			
MQTT Port	61613			
Client ID	kb_client_68B9D3DFE764			
Publish Qos	0			
Action&Admin Qos	0			
User Name	kkmtest			
Password*			
Publish Topic	kbeacon/publish/68B9D3DFE764			
Pubaction Topic	kbeacon/pubaction/68B9D3DFE76			
Subaction Topic	kbeacon/subaction/68B9D3DFE76			
Pub Admin Topic	kbeacon/pubadmin/68B9D3DFE76			
Sub Admin Topic	kbeacon/subadmin/68B9D3DFE76			
Max Packet Size(KB)	60			

[Save & Apply](#)

1. **Service Access:** select MQTT and the Product will use MQTT protocol to connect to cloud server.



2. **URL:** the MQTT cloud address.
 - TCP:// select TCP for connection.
3. **MQTT port:** The default port is 61613.
4. **Client ID:** MQTT client ID
5. **Publish Qos:** MQTT Qos value for publish topic. The publish Topic Qos is fixed to 0.
6. **Action&Admin Qos:** MQTT Qos value for follow topic:
 - Pubaction Topic, Subaction Topic
 - Pubadmin Topic, Subadmin Topic
7. **Username:** MQTT client user name
8. **User Password:** MQTT client password
9. **Publish Topic:** The Product report alive and band broadcast messages to the cloud server through this topic.
10. **Pubaction Topic:** Product configuration request response topic. . If a configuration request is sent to Product, the Product will send an execution result message through this topic.
11. **Subaction Topic:** Product configuration request subscription topic. If the server needs to send a configuration request to the beacon, it will send a configuration message to the gateway through this topic.
12. **Pub Admin Topic:** The Product configuration command response topic. If the cloud server configures the gateway parameters, such as the filter signal threshold, or the restart command, the gateway responds through this topic.
13. **Sub Admin Topic:** The configuration command topic subscribed by the Product. The cloud server can send configuration commands or restart commands to the gateway through this topic.
14. **Max packet size (KB):** This parameter is used to control max packet size when upload advertisement data to cloud.’

When the packet size of a message uploaded by the Product at one time is greater than Max packet size, the gateway will split the message into multiple messages, and the size of each message will not exceed Max packet size for uploading.



4.3.3. MQTT with SSL configuration

Service Access	<input type="text" value="MQTT"/>
MQTT Type	<input type="text" value="ssl://"/>
MQTT URL	<input type="text" value="192.168.3.205:61613"/>
Client ID	<input type="text" value="kb_client_68B9D3DFDF80"/>
Qos	<input type="text" value="0"/>
User Name	<input type="text" value="kkmtest"/>
Password	<input type="password" value="....."/> *
Publish Topic	<input type="text" value="kbeacon/publish/68B9D3DFDF80"/>
Pubaction Topic	<input type="text" value="kbeacon/pubaction/68B9D3DFDF8"/>
Subaction Topic	<input type="text" value="kbeacon/subaction/68B9D3DFDF8"/>
Pub Admin Topic	<input type="text" value="kbeacon/pubadmin/68B9D3DFDF8"/>
Sub Admin Topic	<input type="text" value="kbeacon/subadmin/68B9D3DFDF8"/>
CA	<input type="button" value="选择文件"/> 未选择任何文件
Client Certificate	<input type="button" value="选择文件"/> 未选择任何文件
Client Certificate Key	<input type="button" value="选择文件"/> 未选择任何文件



1. **Service Access:** select MQTT and the Product will use MQTT protocol to connect to cloud server.
2. **URL:** the MQTT cloud address.
3. **MQTT port:** Our test MQTT server SSL port is 61613.
4. **Client ID:** MQTT client id
5. **Publish Qos:** MQTT qos value for publish action and subscribe action topic. The publish Topic Qos is fixed to 0.
6. **Username:** MQTT client user name
7. **User Password:** MQTT client password
8. **Publish Topic:** The Product report alive and band broadcast messages to the cloud server through this topic.
9. **Pub action Topic:** Product configuration request response topic. . If a configuration request is sent to Product, the Product will send an execution result message through this topic.
10. **Sub action Topic:** Product configuration request subscription topic. If the server needs to send a configuration request to the beacon, it will send a configuration message to the gateway through this topic.
11. **Pub Admin Topic:** The Product configuration command response topic. If the cloud server configures the gateway parameters, such as the filter signal threshold, or the restart command, the gateway responds through this topic.
12. **Sub Admin Topic:** The configuration command topic subscribed by the Product. The cloud server can send configuration commands or restart commands to the gateway through this topic.

SSL Parameters, the Product support self-signed certificates MQTT access.

13. **CA:** the CA file about the MQTT server. You can select the CA file about MQTT test server from your PC.
14. **Client Certificate:** MQTT Client certificate file. You can select the CA file about MQTT test server from your PC.
15. **Client Key:** MQTT Client Key file: You can select the CA file about MQTT test server from your PC.



4.3.4. HTTP configuration

Service Access	<input type="text" value="HTTP"/>
Url	<input type="text" value="https://post.kkmiot.com:8092/postd"/>
Authentication	<input type="text" value="None"/>
Max Packet Size(KB)	<input type="text" value="60"/>

1. **Service Access:** select HTTP and the Product will use HTTP protocol to connect to cloud server.
2. **Authentication:** The Product support single password authentication for HTTP post.
3. **Url:** The cloud HTTP service.

We provide a test HTTP server and the URL address is:
<https://post.GAOTekiot.com:8092/postdata>

And the Product can support simple password that connect to clouds.

Service Access	<input type="text" value="HTTP"/>
Url	<input type="text" value="https://post.kkmiot.com:8092/postd"/>
Authentication	<input type="text" value="BasicAuth"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Max Packet Size(KB)	<input type="text" value="60"/>

Also, the Product HTTP protocol can support APIkey to connect



Service Access	<input type="text" value="HTTP"/>
Url	<input type="text" value="https://post.kkmiot.com:8092/postd"/>
Authentication	<input type="text" value="APIKey"/>
Key Name	<input type="text" value="undefined"/>
Key Value	<input type="password" value="....."/>
Max Packet Size(KB)	<input type="text" value="60"/>

4.3.5. Cache Message

- In some areas, the network may be unstable, and it may be frequently interrupted.
- The gateway can cache the message to memory while the network is down and upload it automatically after network restored.
- Max Cache Time can be set from 60~3600 seconds.

Cache Message	<input type="text" value="YES"/>
Max Cache Time(Sec)	<input type="text" value="Sec:60~3600; e.g 1800"/>

4.3.6. Upload GPS Configuration

Click “Services”-” Others setting” to go to the GPS configuration page.



Please make sure LTE USB dongle is installed in the Product and the

LTE module need to support GPS. Please contact GAOTEK sales team for more information.



Upload GPS Location	YES
GPS Measure Period(Sec)	Sec:3~7200; e.g 60
advData with GPS	YES

When choosing to upload GPS location, you can set the interval of GPS positioning. After the Product obtains the GPS information successfully, the Product will report the GPS location information to the cloud in the Alive message by default.

When "advData with GPS" is Yes, the Product will carry GPS location information every time it reports Product's advertisement message.

4.3.7. BLE Scan Mode

Product support BLE4.0(Legacy) and BLE 5.0 long range (PHY), and also Hybrid Mode (Legacy +PHY Code).

When gateway use the BLE5.0 long range (PHY code), the corresponding BLE Product device also need to support PHY Mode.

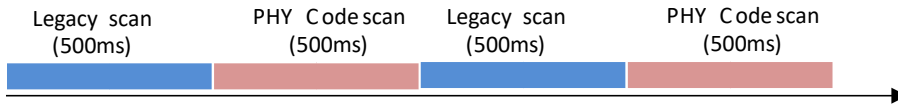
BLE Scan Mode	Legacy
---------------	--------

- Legacy
- PHY Code
- Hybrid Mode

Since the Product can only scan Legacy device or PHY Code device at the same time, you need to further set the alternate scanning time when selecting to set to Hybrid mode:

BLE Scan Mode	Hybrid Mode
Scan Alternately Interval	uint is ms. 300~7000; e.g 700

For example, the Scan alternate interval is 500ms, the scan mode is as follows:



4.3.8 BLE Active Scan

“Yes” means Product supports active scanning the BLE device, at this time, the Product will report the Scan response message of Product to the cloud.

This function takes effect only when the “Upload Unknown” filter switch was enabled.

BLE Active Scan

4.4. Modify the Web Portal Login Password

Click “System”-” Change password”. The default login password is “admin” and users can change it to another password.

Gateway
Status
Network ▾
Service ▾
System ▾
Logout

Admin Password

Changes the administrator password for accessing the device

Password

Confirmation



4.5. Network diagnostics

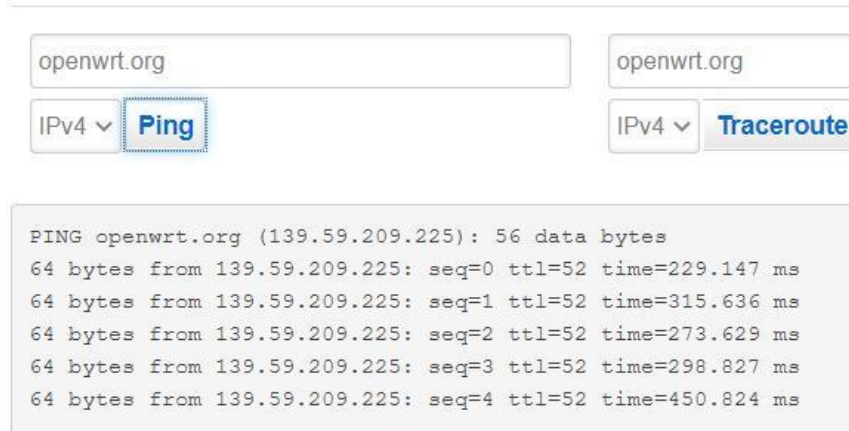
Click “Network”-” Diagnostics” to diagnose the network



Ping: Enter a website. If the website can be pinged successfully, it means the Network is well connected. If the website can not be pinged, the network might have connection problem

Diagnostics

Network Utilities



Traceroute: If Ping fails, use Traceroute to check which procedure caused the network connection problem.



www.baidu.com openwrt.org

IPv4 ▾ Ping IPv4 ▾ Traceroute

```
traceroute to openwrt.org (139.59.209.225), 30 hops max, 38 byte packets
 1  192.168.3.1  0.361 ms
 2  100.64.0.1  1.617 ms
 3  202.105.158.253  1.885 ms
 4  183.56.65.6  5.982 ms
 5  202.97.94.150  7.550 ms
 6  202.97.12.17  7.240 ms
 7  202.97.13.30  211.343 ms
 8  118.85.205.82  214.056 ms
 9  62.115.120.226  217.799 ms
10  62.115.114.91  208.280 ms
11  80.239.128.21  205.786 ms
12  *
13  *
14  139.59.209.225  206.646 ms
```

5. Quick verify Product API

In order for customer easily integrates our product, we provide test servers for HTTP and MQTT.

5.1. How to verify HTTP API

1. The gateway is setting to MQTT server by default factory setting. So please reference section<< 4.3.4 HTTP configuration>> to change the service's type.
2. GAOTEK provides a test HTTP server, and the address is:
<https://post.kkmiot.com:8092/postdata>
3. After Product connect to the HTTP service success, it will flash green LED and periodically send the Product advertisement data to HTTP server.
4. You can view the reported data on HTTP server by follow address. You should replace the mac address to your Product.

<https://post.kkmiot.com:8092/viewdata.jsp?mac=D03304001182>



api.ieasygroup.com:8091/viewdata.jsp?mac=D03304003262

#Ble gate way data

mac	data1	time
020100544EC0	{"rssi":-43,"dmac":"020100544EC0","time":"2020-01-08 00:44:07","type":16,"url":"026E74702E696D2F41514E4D5F357A397741","refPwr":4}	2020-01-08 08:44:08.0
CC1E24EA7DE0	{"rssi":-67,"majorID":1,"dmac":"CC1E24EA7DE0","minorID":1,"refpower":-59,"time":"2020-01-08 00:44:06","type":4,"uuid":"7777772E6B66D636E2E636F6D000001"}	2020-01-08 08:44:08.0

5.2. How to verify MQTT API

Download MQTT.fx software:

<http://www.jensd.de/apps/mqttx/1.5.0/>

Please refer to the document << Product API Specification.pdf>> for other details.

6. More System Settings

6.1. System clock

Click “System”-” Clock”-’Sync with browser’, the gateway automatically synchronizes the local UTC time (Product uses UTC time by default). If you need the Product to use your local time, you can also select the same time zone as your local time.



System

Here you can configure the basic aspects of your device like the timezone.

System Properties

General Settings

Local Time Thu Apr 1 05:44:13 2021 [Sync with browser](#)

Timezone UTC

Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

- UTC
- Africa/Abidjan
- Africa/Accra
- Africa/Addis Ababa
- Africa/Algiers
- Africa/Asmara
- Africa/Bamako
- Africa/Bangui
- Africa/Banjul
- Africa/Bissau
- Africa/Blantyre
- Africa/Brazzaville
- Africa/Bujumbura
- Africa/Cairo
- Africa/Casablanca
- Africa/Ceuta
- Africa/Conakry
- Africa/Dakar
- Africa/Dar es Salaam
- Africa/Djibouti

With NTP client enabled, the Product also synchronize the UTC time automatically.

Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

0.openwrt.pool.ntp.org	x
1.openwrt.pool.ntp.org	x
2.openwrt.pool.ntp.org	x
3.openwrt.pool.ntp.org	+



6.2. System update

Product support OTA update, and the firmware can be updated from Remote Server or Local file. If update from Remote server, click 'Refresh' to check if there are any new firmware images available.

If you need to upgrade through Local file, please contact GAOTEK sales to obtain the corresponding firmware package.

Flash Linux image

Hardware Version: V1.2

Software Version: KBGW_V3.5.3

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep s firmware image).

Update From: Remote server

Target version: Local file

Keep settings:

Flash Linux image

Version: KBGW_V3.5.2

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current firmware image).

Update From: Remote server

Target version: V3.5.3

SHA: 15e48f11ff74c7ba266e1b9007510f089f84ac701f3130b11f8098ae139a5f3f
Notes:
-bugfix for wifi.

Keep settings:

Exception handling: please refer to “Gateway OTA Introduction” when the system cannot be started due to abnormal failure in upgrading the gateway.

6.3. BLE Firmware

The software of the Product is composed of two parts. The main software of the Product is the OpenWrt Linux system, another software is BLE firmware package. When the hardware version of KG02 is greater than or equal to V1.4 and the hardware version of KG01 is greater than V1.5, the Product system will automatically upgrade the BLE firmware when the Product upgrades the OpenWrt Linux system.

When the hardware version of KG02 is lower than V1.4 or the hardware version of KG01 is lower than V1.5, or when the system fails to upgrade the BLE firmware automatically, the BLE firmware package needs to be upgraded through the StartDFU mode. For the StartDFU, please refer to “Gateway Bluetooth OTA”.



7. Trouble shooting

7.1. The Product flash red LED

If the Product connect to HTTPs/MQTT server successfully, it will flash green LED, otherwise it will flash red LED.

If the Product flash red led, please check the connection by following steps:



Step1: Check if the network connection is normal

Admin Status **Network** Service Others Logout

Wan Mode Ethernet

Mode dhcp

Apply

Show/Hide Wifi Name

Apply

Check if the network type is right

192.168.8.1/cgi-bin/luci/stok=e780db0884ca5c1ec7700d4b75eab50d/admin/hstatus

Admin Status **Network** Service Others Logout

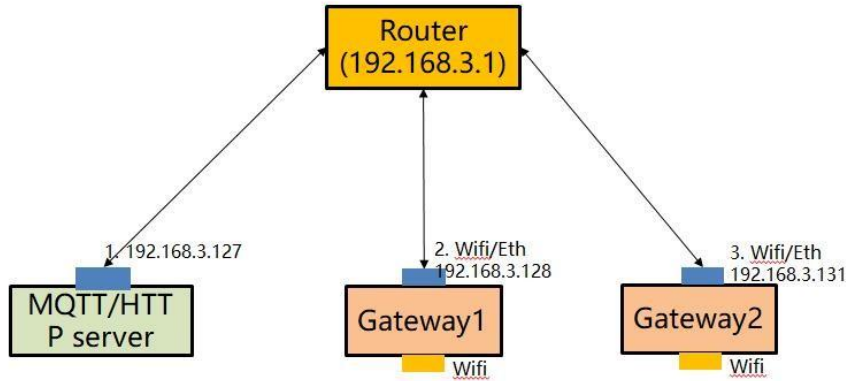
AP MAC	D0:33:04:00:64:52
WAN MAC	D0:10:04:00:64:53
WAN Type	Ethernet
WAN IP	192.168.3.162
Gateway IP	192.168.3.1
DNS IP	192.168.3.1
UP Time(Sec)	700
RX Bytes	5541423
TX Bytes	1259727
Cellular Info	N/A

Check the network status:

If Product connects to network successfully, it will get the IP address and DNS IP address. Also, the RX Bytes and TX Bytes will increase.

Step 2: Check the connection between Product and cloud server

Scenario 1: The Product and Server are deployed in the same LAN



It is necessary to ensure that the Product and server are in the same network, that is, the assigned IP address is in the same network. For example, if the IP address of the MQTT server is 192.168.3.127, the Gateway 1 can be configured as the following address (192.168.3.128).

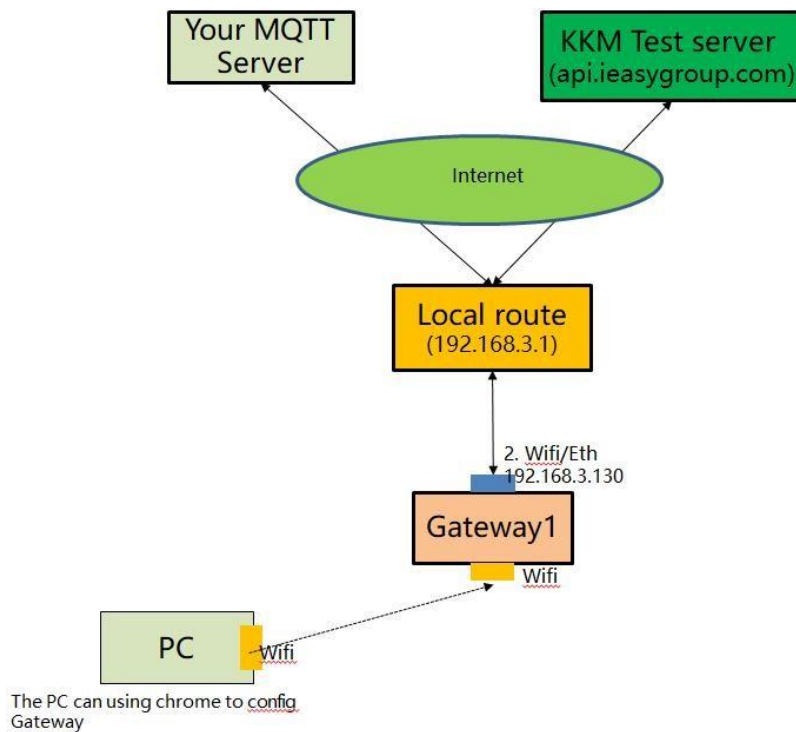
Admin	Status	Network	Service	Others	Logout
Wan Mode	Ethernet				
Mode	static				
IP Address	192.168.3.128				
Netmask	255.255.255.0				
Gateway Address	192.168.3.1				
Primary DNS Address	192.168.3.1				
Secondary DNS Address					
Apply					

Try to use PING command on MQTT/HTTP server. The PING command is used to detect whether the Product and the MQTT server network are connected. If the ping failed, please check whether the LAN is normal.

- Type: "Ping 192.168.3.128" on MQTT/HTTP server.

Scenario two: the Servers are deployed in the cloud

Please try to use GAOTEK test server to verify if Product can connect to cloud successfully. We provide a cloud-based test server with the IP address of the MQTT server: mqtt.GAOTEkiot.com; it supports both MQTT and HTTPs. The Product has been set up as the GAOTEK test server by default.



Assuming that the IP address of the router is 192.168.3.1, the IP address of the Product can be configured as 192.168.3.128.



Admin	Status	Network	Service	Others	Logout
Wan Mode	Ethernet				
Mode	static				
IP Address	192.168.3.128				
Netmask	255.255.255.0				
Gateway Address	192.168.3.1				
Primary DNS Address	192.168.3.1				
Secondary DNS Address					
Apply					

GAOTEK MQTT server information :

- Address: mqtt.kkmiot.com:61613
- Test user name: kkmtest
- password: testpassword



Admin	Status	Network	Service	Others	Logout
Scan Interval(Seconds:2~100)	<input type="text" value="5"/>				
Min Rssi filter(dBm:-100~20)	<input type="text" value="-100"/>				
Ble Services filter(Hex:e.g 0xFE40)	<input type="text" value="0xFE40"/>				
Ble Mac filter(Hex:e.g DD33)	<input type="text"/>				
Service Access	<input type="text" value="MQTT"/>				
Url	<input type="text" value="tcp://"/> <input type="text" value="api.ieasygroup.com:61613"/>				
Client ID	<input type="text" value="kb_client_D03304001402"/>				
Qos	<input type="text" value="0"/>				
Username	<input type="text" value="kkmtest"/>				
User Password	<input type="text" value="testpassword"/>				
Publish Topic	<input type="text" value="kbeacon/publish/D03304001402"/>				

Wait 30 seconds to 1 minute after saving the settings. If the Product flashes green light, the network connection between the Product and the cloud is normal. If it still flashes red LED, the network connection between Product and the Cloud maybe failed.

Check if the HTTP/MQTT server is running normally

Scenario 1: Using MQTT server

Please refer to section 7.2 Using third-party MQTT client to verify Product in <<Product API Introduction>> document.

If MQTT client connection fails, please check:

1. is there a firewall on the MQTT server to prevent other client connections? The default port of the MQTT server is 61613.
2. Whether the MQTT server is installed correctly.

Scenario 2: Using HTTPs server

You can use curl tools to verify if the connection and the key file is right.

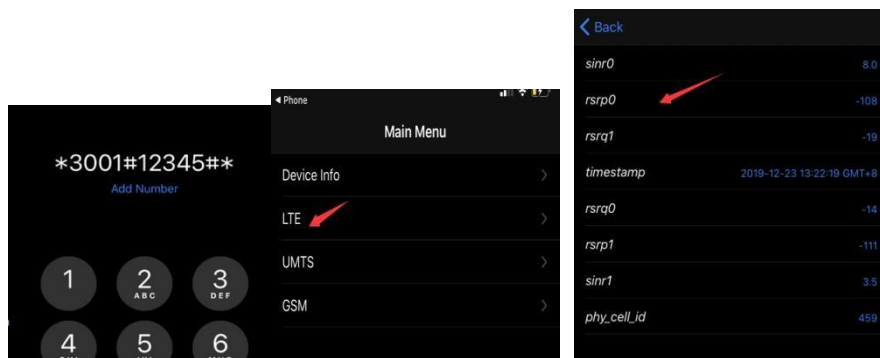
```
Example: curl --request POST--url
'http://post.GAOTekiot.com:8091/postdata' --header'content-type:
application/json' --data'{"msg":"advData","gmac":"A1A2A3A4A5A9","obj":
[{"dmac":"AE9639C51701","rssi":"-25","data1":"020106"},
{"dmac":"7E4395AB78CC","rssi":"-
25","data1":"020106030202180AFF4B4D027E4395AB78CC"}]}' --include pause
```

7.2. The Cellular signal is very poor

If cellular signal < -110dBm, it means the LTE signal was pool. Please check like follow:

Step1: Use iPhone to check your cellular provide signal.

Input *3001#12345##* on the dial UI, then tap on call.



Please check the rsrp0 signal.

You can go to step2 if the iPhone’s signal was much bigger then Product showing. If it is almost same, please contact your cellular provider.



Step2: Open the shell box; please make sure that the antenna interface is firmly inserted.

The antenna may be loosened when the case is opened and insert SIM card, so we check the antenna interface.





8. Appendix1 Advertisement Upload Filter for different scenario

Product supports a variety of filtering conditions to meet the filtering requirements in different scenarios



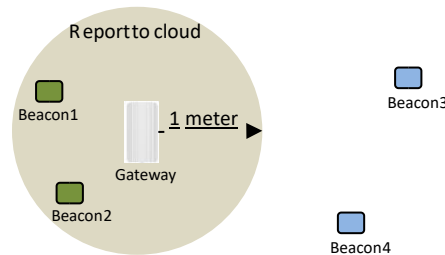
Upload Interval(Unit:Sec)	<input type="text" value="2"/>
Filter by RSSI(Unit:dBm)	<input type="text" value="-60"/>
Filter by ServiceID	<input type="text" value="0X0"/>
Filter by mac	<input type="text" value="Regular expression; e.g. ^20DD ^2"/>
Filter by BLE name	<input type="text" value="Regular expression; e.g. ^KBPro"/>
Filter by raw	<input type="text" value="Regular expression; e.g. ^0201"/>
Filter duplicate data	<input type="text" value="NO"/> ▼
Upload iBeacon	<input type="text" value="YES"/> ▼
Upload Eddystone	<input type="text" value="YES"/> ▼
Upload KSensor	<input type="text" value="YES"/> ▼
Upload Proximity	<input type="text" value="YES"/> ▼
Upload Unknown	<input type="text" value="YES"/> ▼
Upload without BLE data	<input type="text" value="YES"/> ▼
Advertisement timestamp	<input type="text" value="yyyy-MM-dd HH:mm:ss.Z"/> ▼

8.1. Scenario 1: Only upload nearby beacon advertisement

Sometimes we want the Product only report the Product that is nearby.



For example, the Gateway is deployed on door, then we need the Gateway only report the beacons signal to clouds which is near the door.



Set the min RSSI filter to -59dBm.

Upload Interval(Unit:Sec)

2

Filter by RSSI(Unit:dBm)

-59

8.2. Scenario 2: Reduce advertisement message to clouds

Sometimes we may use third part MQTT hub to receive advertisement. Then we need to reduce the advertisement message number. Also, some MQTT hub may limit the max MQTT message size.

For example:

- If the advertisement packet changed, the Gateway sends the advertisement packet to cloud immediately. We set to 2 seconds.
- The max packet size is set to 60KB.

Upload Interval(Unit:Sec)

2

Max Packet Size(KB)

60

8.3. Scenario 3: Only upload specific MAC address to clouds

The Product default mac address starts with DD33.



We can set the BLE mac filter to ^DD33 to filter Product device. The Gateway only report Product advertisement packet to clouds.

Filter by ServiceID	<input type="text" value="0X0"/>
Filter by mac	<input type="text" value="^DD33"/>
Filter by BLE name	<input type="text" value="Regular expression; e.g. ^KBPro"/>
Filter by raw	<input type="text" value="Regular expression; e.g. ^0201"/>

8.4. Scenario 4: Only upload iBeacon advertisement

Sometimes we want the Product only report the iBeacon advertisement packet to cloud, then we can set iBeacon to 'Yes' and others to 'NO'.

Upload iBeacon	<input type="text" value="YES"/>
Upload Eddystone	<input type="text" value="YES"/>
Upload KSensor	<input type="text" value="YES"/>
Upload Proximity	<input type="text" value="YES"/>
Upload Unknown	<input type="text" value="YES"/>



```
{
  "msg": "advData",
  "obj": [
    {
      "dmac": "51DC0EA4AE30",
      "refpower": -75,
      "uuid": "FB349B5F80000080001000003CFE0000",
      "majorID": "4115",
      "rssi": -80,
      "minorID": "077F",
      "type": 4,
      "time": "2019-09-02 09:47:42"
    },
    {
      "dmac": "231824EA7DE0",
      "refpower": -59,
      "uuid": "7777772E6B6B6D636E2E636F6D000001",
      "majorID": "0001",
      "rssi": -64,
      "minorID": "0001",
      "type": 4,
      "time": "2019-09-02 09:47:43"
    }
  ]
}

"gmac": "D03304002122"
}
```




8.5 Scenario 5: Only upload Eddystone advertisement

Sometimes we want the Product only report the Eddystone advertisement packet to cloud, then we can set Eddystone to 'Yes' and others to 'NO'.

Upload iBeacon	YES
Upload Eddystone	YES
Upload KSensor	YES
Upload Proximity	YES
Upload Unknown	YES

```
{
  "msg": "advData",
  "obj": [
    {
      "dmac": "0A2024EA7DE0",
      "advCnt": 13586020,
      "vbatt": 3050,
      "secCnt": 13655980,
      "temp": 33,
      "time": "2019-09-02 09:51:11",
      "rssi": -63,
      "type": 8
    },
    {
      "dmac": "7996010A33DD",
      "advCnt": 13848450,
      "vbatt": 3113,
      "secCnt": 13917330,
      "temp": 26,
      "time": "2019-09-02 09:51:12",
      "rssi": -75,
      "type": 8
    }
  ],
  "gmac": "D03304002122"
}
```



8.6. Scenario 6: Filter advertisement packet by service ID

The BLE advertisement packet can include Services ID. For example, the Eddystone beacon packet's services ID is 0xFEAA. If we set the service id, then the Product will only report Google Eddystone packet.

Filter by ServiceID

0xFEAA

8.7.Scenario 7: Beacon Location

Sometimes the clouds only need to monitor beacon's RSSI for location. Then the Gateway only needs to scan device's RSSI and mac address. Because the Gateway will not scan advertisement packet data, so we cannot set the Upload iBeacon/Eddystone/KSensor to 'YES'.

In this scenario, the Gateway will only report the beacon's RSSI and mac address to clouds.

Upload iBeacon	YES
Upload Eddystone	YES
Upload KSensor	YES
Upload Proximity	YES
Upload Unknown	YES

**advertisement uploaded:**

```
{
  "msg": "advData",
  "obj": [{
    "dmac": "3636000A33DD",
    "data1": "",
    "type": 32,
    "time": "2019-09-02 09:22:22",
    "rssi": -59
  }, {
    "dmac": "5055010A33DD",
    "data1": "",
    "type": 32,
    "time": "2019-09-02 09:22:23",
    "rssi": -44
  }, {
    "dmac": "7355010A33DD",
    "data1": "",
    "type": 32,
    "time": "2019-09-02 09:22:25",
    "rssi": -45
  }
],
  "gmac": "D03304002122"
}
```

9. Appendix2 Setup your own MQTT Server

There is some third-party MQTT server software. Following example uses mosquitto as an example which test in windows10 environment.



1. Download mosquito:
<https://mosquitto.org/files/binary/>
2. We installed the software to C:\Program Files\mosquitto
3. Create the password file with username:
`mosquitto_passwd -c pwfile2.example test`
4. edit mosquitto.conf file,
add follow line in the file

`max_connections -1 listener 61613
protocol mqtt allow_anonymous
false password_file pwfile2.example
uncomment follow line:
log_timestamp true
log_timestamp_format %Y-%m-%d
T%H:%M:%S
websockets_log_level 0`
5. Run mqtt server `mosquitto -c
mosquitto.conf`
6. Verify mqtt server
 - a. Subscribet all topic: we assume the username is test and the password is abcabc.
`mosquitto_sub -h localhost -p 61613 -t mqtt -u test -P abcabc`
 - b. publish message to mqtt server:
`mosquitto_pub -h localhost -p 61613 -t mqtt -m "hello world" -u test -P abcabc`