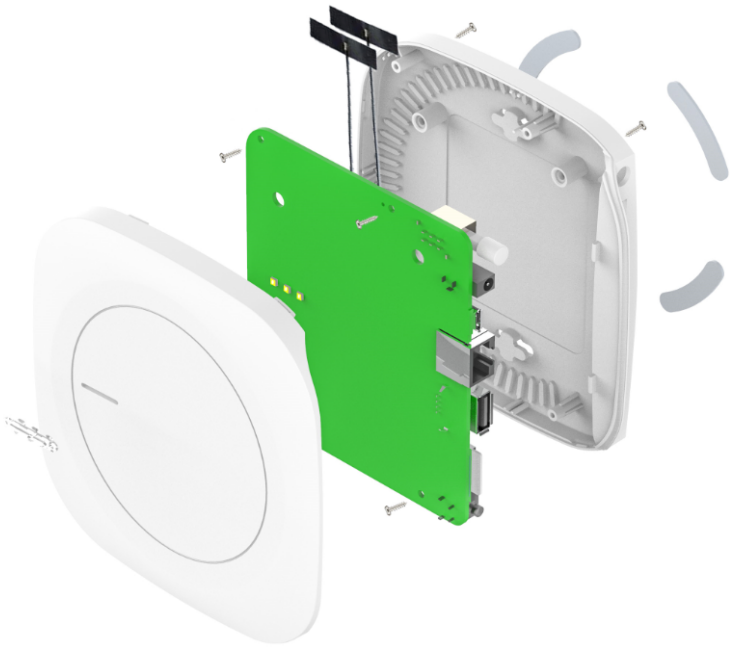
MKGW1 Gateway Datasheet

---

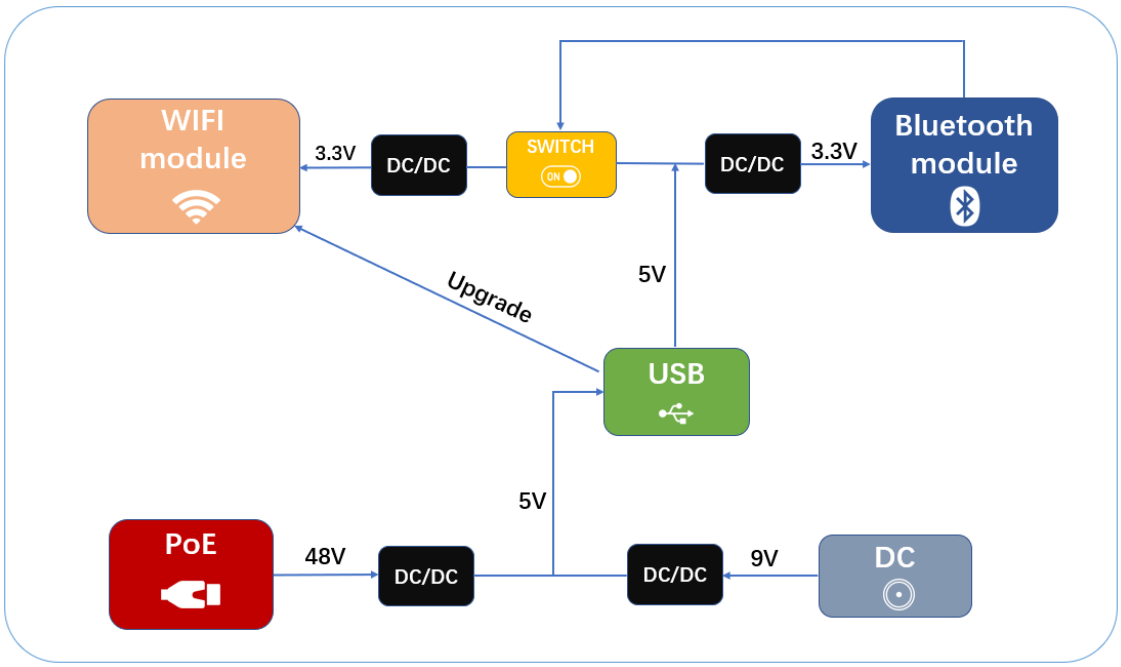
1. Product Description

- **MKGW1 Bluetooth gateway is mainly used for the MOKO BLE series Beacon products. It is convenient for users to get the data of the MOKO series Beacon, and advertising raw data of any Bluetooth device. It can upload the data to the server via MQTT or HTTP(S) protocol.**
- **MKGW1 can connect the standard MQTT Broker, Aws IOT, Azure IOT HUB, Aliyun IOT.**
- **PoE、DC and USB power supply.**
- **The WIFI data rate of MKGW1 can be 150Mbps.**
- **User can modify the gateway parameters on the web UI.**
- **Support Ethernet and WIFI internet access.**



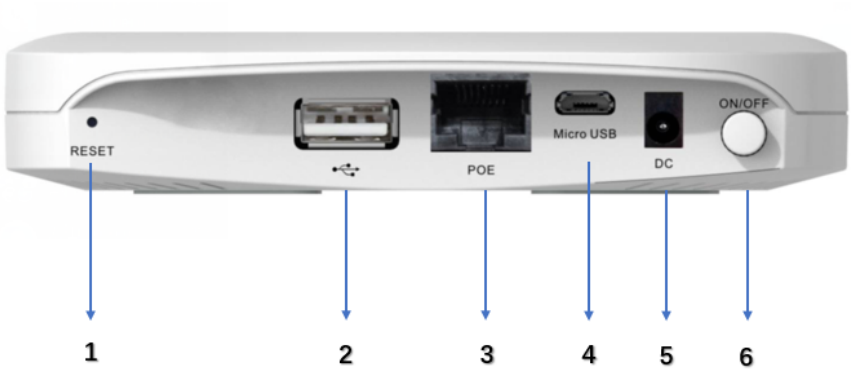
2. Product Features

2.1 Power Supply



Power Supply Block Diagram

2.2 Interface



No.	Interface	Function	Remark
1	Reset Button	1. Reset to factory setting 2. System upgrade	1. Long press for over 5seconds until the gateway restarts to reset 2. Short press to upgrade the system
2	USB Port	Insert a USB flash drive with upgrade file for system upgrade	The name of upgrade file is required to be: **MKGW-BW-Upgrade.bin**
3	PoE Port	1. PoE power supply 2. Ethernet Access	Power Specification: 48V/1A
4	Micro USB	USB power supply	Power Specification: 5V/1A
5	DC Power Port	DC power supply	Power Specification: 9V/1A
6	Switch Button	Power On / Power Off	-

2.3 Indicator LED

No.	Name	Function	Device Status	LED Status
1	Power LED	Display system status	System works normally	GREEN
			System works abnormally	RED
			System ugrade	GREEN (Blinking)
2	Network LED	Display network status	No network	YELLOW
			ETH connection	BLUE
			WIFI connection	GREEN
			Network abnormally	RED
3	Data LED	Display Bluetooth and server communication status	Bluetooth COMM √ Server COMM ×	BLUE
			Bluetooth COMM × Server COMM √	YELLOW
			Bluetooth COMM √ Server COMM √	GREEN
			Bluetooth COMM × Server COMM ×	RED

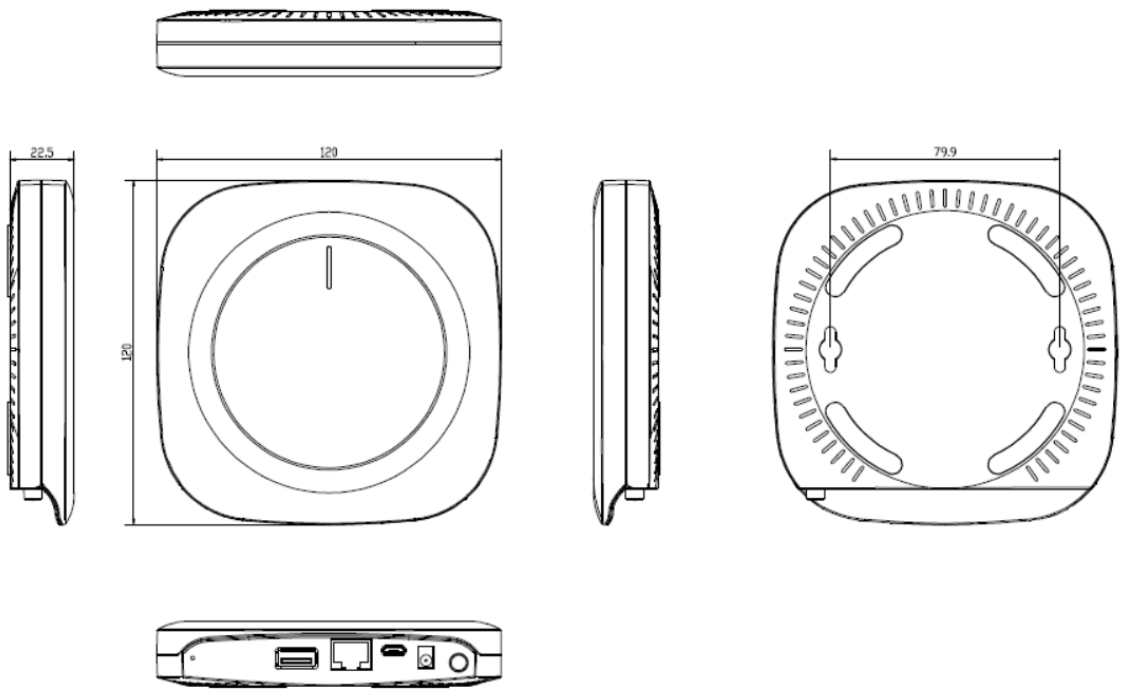
Note: All LEDs display yellow when the system starts up.

3 Product Specification and Performance

3.1 Technical Parameters

No.	Item	Value	Remark
1	Colour	White	Other colors can be customized
2	Dimension	120mm x 120mm x 22.5mm	Refer to mechanical draws for details
3	Net Weight	138.2g	
4	Interface	PoE Port DC Power Port Micro USB Port RJ45 Network Port USB Upgrade Port	
5	Operating Temperature	0 ~ 55ºC	
6	Storage Temperature	20 ~ 30ºC	
7	Wireless Standard	IEEE 802.11b/g/n	
8	WIFI Data Rate	150Mbps	Maximum
9	WLAN Transmit power	18dBm	
10	WIFI coverage	300m	Maximum，In the open space
11	Wireless encryption type	WPA1PSKWPA2PSK/TKIPAES WPA1PSKWPA2PSK/AES WPA2PSK/TKIPAES WPA2PSK/AES WPA2PSK/TKIP WPAPSK/TKIPAES WPAPSK/AES WPAPSK/TKIP WEP	
12	Bluetooth Standard	BLE 5.0	Chip model:nRF52832
13	Bluetooth Scanning Range	120m	Maximum，In the open space
14	Maximum Scanning Capability	300/s	
15	Server Protocol	MQTT(TCP/SSL) HTTP/HTTPS	-

3.2 Mechanical Draws



All units is mm.

---

4. Gateway Instructions

4.1 Operating Procedures

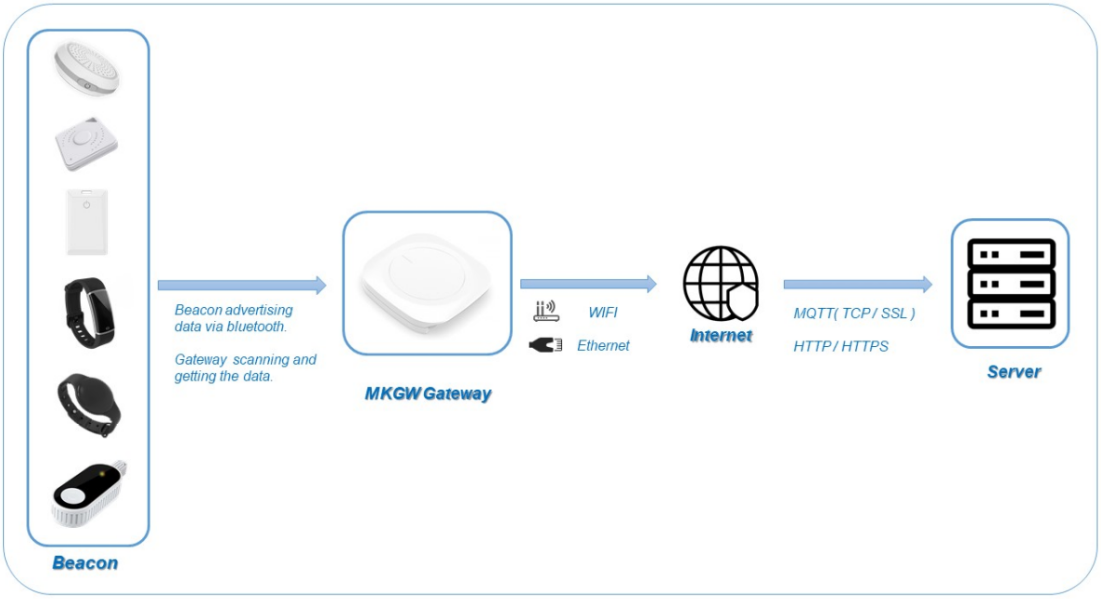
Step 1. Search for and connect to the gateway using mobile phone or PC with WIFI;

Step 2. Connect the gateway to the Internet through Ethernet or WIFI;

Step 3. Configure the gateway to upload data to the server (MQTT, HTTP/HTTPS) and check the communication status;

Step 4. Select the Beacon type for Bluetooth scanning and configure the scanning parameters.

4.2 Application Process



Application Block Diagram

Remark:

1. The Bluetooth module on the gateway scans the advertising data of surrounding Beacons;

2.The Bluetooth module sends the advertising data of Beacons to the WIFI module;

3. The gateway uploads the Beacon data to the server in json format according to the established network communication protocol.

4.3 Default Parameters

No.	Item	Value	Remark
1	WLAN SSID	MKGW-BW-XXXX	XXXX is the last 2 bytes of the gateway MAC address
2	WLAN Password	Moko4321	
3	LAN IP	192.168.22.1	
4	User Name	Admin	Unmodifiable
5	Password	admin	
6	Time Zone	Asia/Shanghai	-

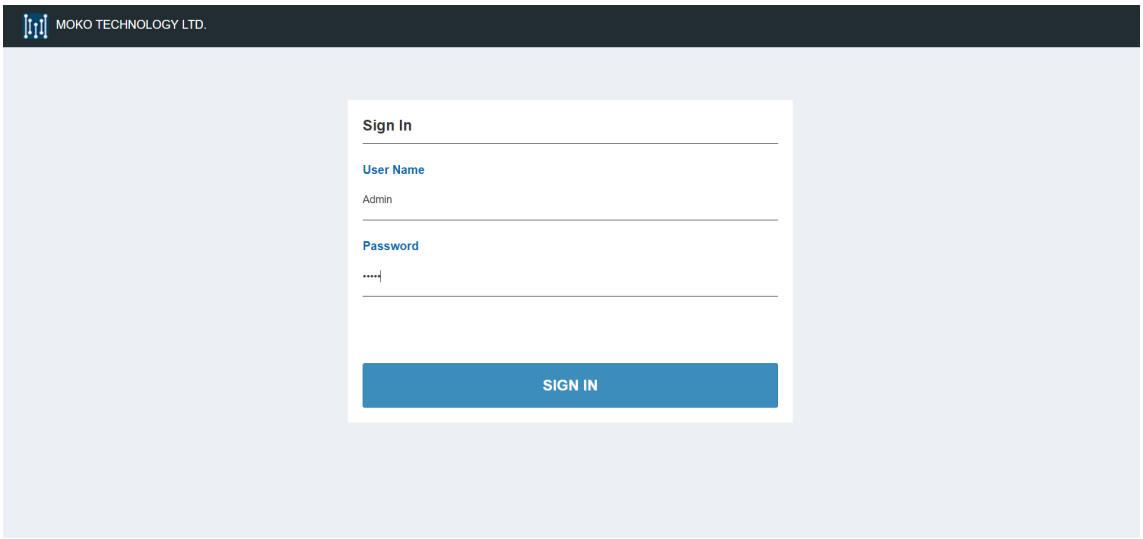
4.4 Connect And Login

Step 1. Power on the gateway;

Step 2. Use PC or mobile phone, open WIFI to search gateway SSID (Default: MKGW-BW-XXXX), verify the password (Default: Moko4321) and connect to the gateway;

Step 3. Use a browser① to open the link **http://192.168.22.1 (http://192.168.22.1)** (Default) ;

Step 4. Enter the password (Default: admin) to go to the gateway configuration web UI. Note that the configuration web UI will be automatically logged out if there is no operation within 1 hour.

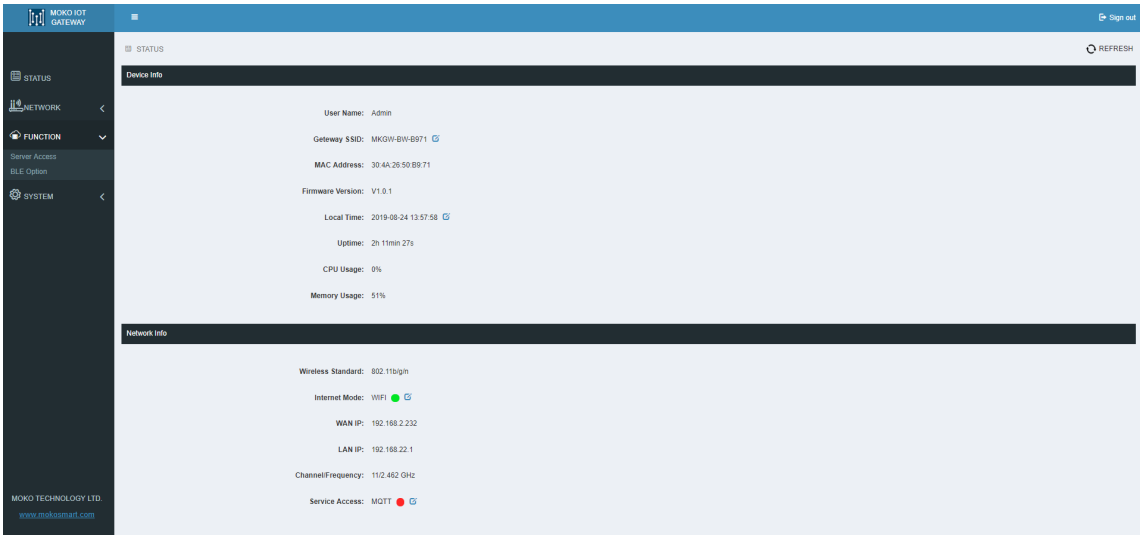


① *It is recommended to use the latest version of the mainstream browsers such as IE11, Chrome, Firefox, Safari, etc.*

4.5 Gateway Status

After logging in, you can view the current configuration status of the gateway. See the figure below for details.

You can refresh the current status by clicking the **"REFRESH"** button on the right.



STATUS

- **Device information description**

No.	Item	Description	Remark
1	User Name	Username of the configuration web UI	Admin
2	Gateway SSID	Gateway WLAN SSID	Default: MKGW-BW-XXXX. XXXX is the last 2 bytes of the gateway MAC address
3	MAC Address	Gateway MAC Address	
4	Firmware Version	Gateway Firmware Version	
5	Local Time	System time	The time zone is configurable. Press the **"REFRESH"** button to refresh
6	Uptime	Run time after the gateway is started	Press the **"REFRESH"** button to refresh
7	CPU Usage	Device CPU usage	Press the **"REFRESH"** button to refresh
8	Memory Usage	System memory usage	Press the **"REFRESH"** button to refresh

- **Network information description**

No.	Item	Description	Remark
1	Wireless Standard	WIFI wireless network standard	IEEE 802.11b/g/n

No.	Item	Description	Remark
2	Internet Mode	Network connection mode. Two modes: ETH and WIFI. Display N/A when no network connection.	The red mark indicates abnormal network connection or no network; The green mark indicates that the network connection is normal.
3	WAN IP	IP of the gateway WAN port. Display N/A when no network connection.	-
4	LAN IP	LAN IP of the gateway	Configurable
5	Channel/Frequency	The channel and frequency of the current network	There are 13 channels in total. The current channel is related to the uplink network channel.
6	Service Access	Network communication protocol for uploading data to the server. Display N/A when there is no communication.	Support MQTT(TCP/SSL), HTTP/HTTPS. The red mark indicates that the server connection is abnormal or no connection; The green mark indicates that the server connection is normal.

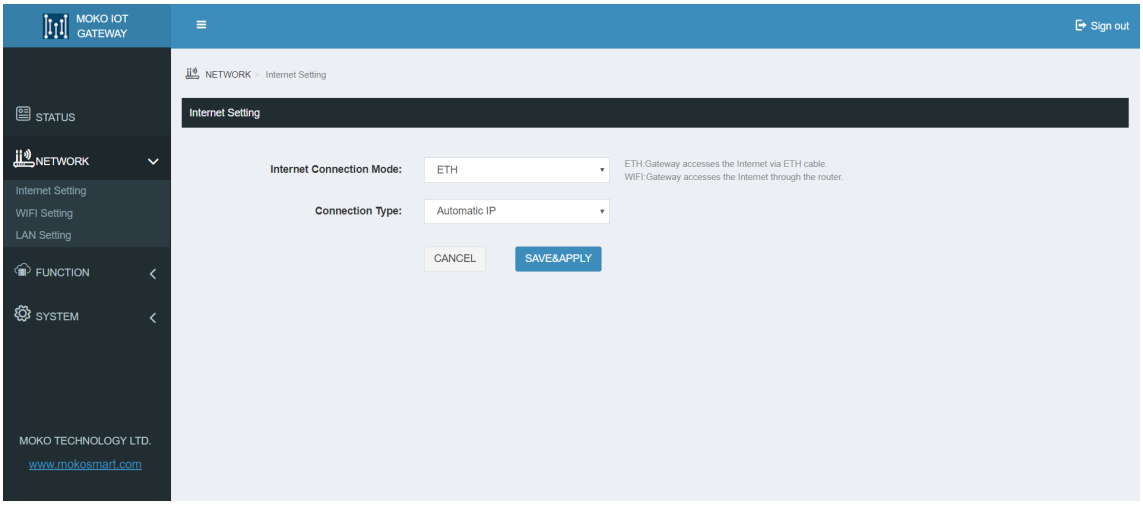
4.6 Internet Setting

The gateway can access the Internet through **Ethernet(ETH) or WIFI**, and can access the network by **Automatic IP or Static IP**.

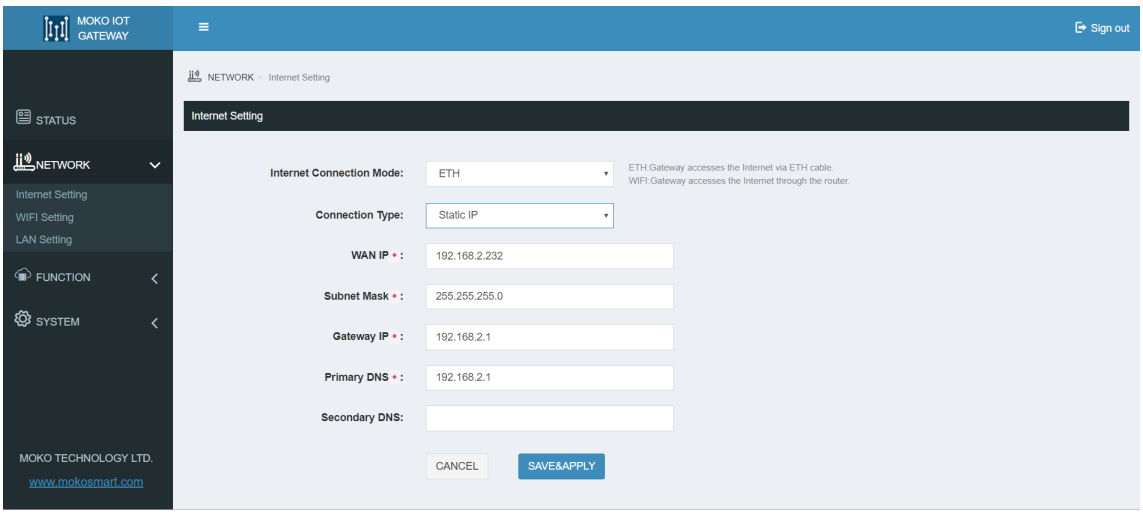
Static IP requires WAN IP, subnet mask, gateway IP, DNS, etc.

After the network configuration is completed, wait for the gateway to access the network. You can check the network status in gateway **STATUS**.

- **Ethernet** — Use a network cable to connect to the PoE port of the gateway and connect the gateway to a **Network Switch** that is connected to the Internet.

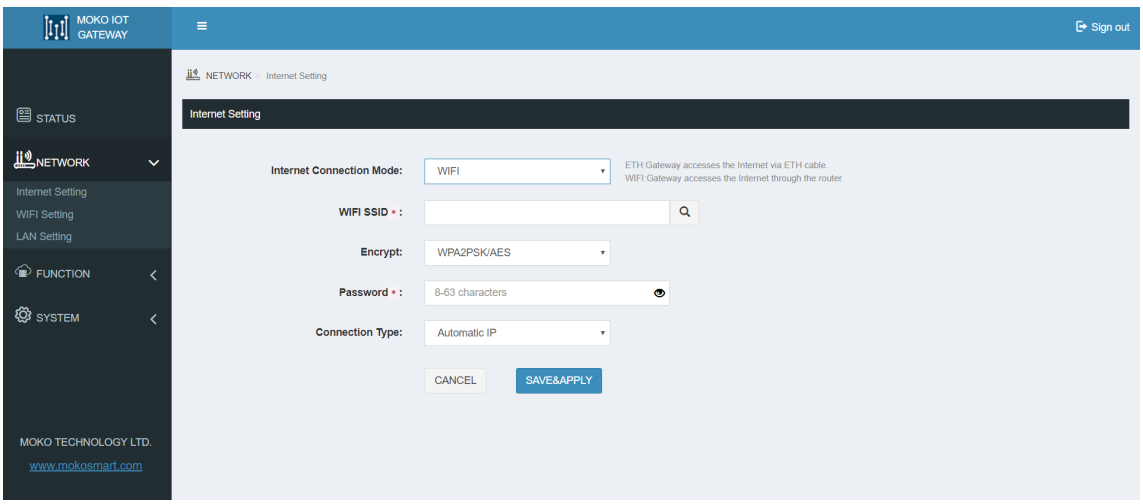


Ethernet / Automatic IP

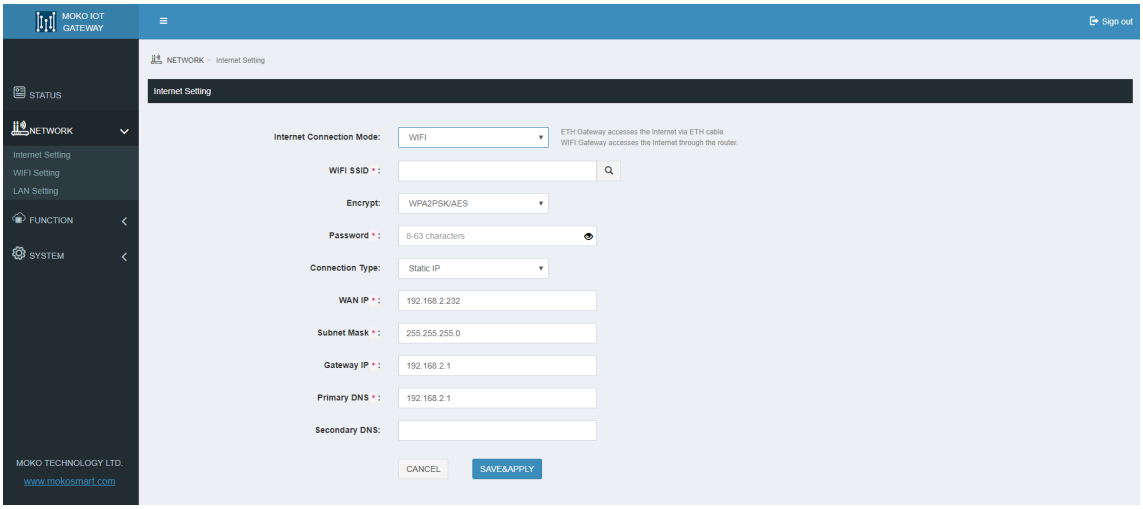


Ethernet / Static IP

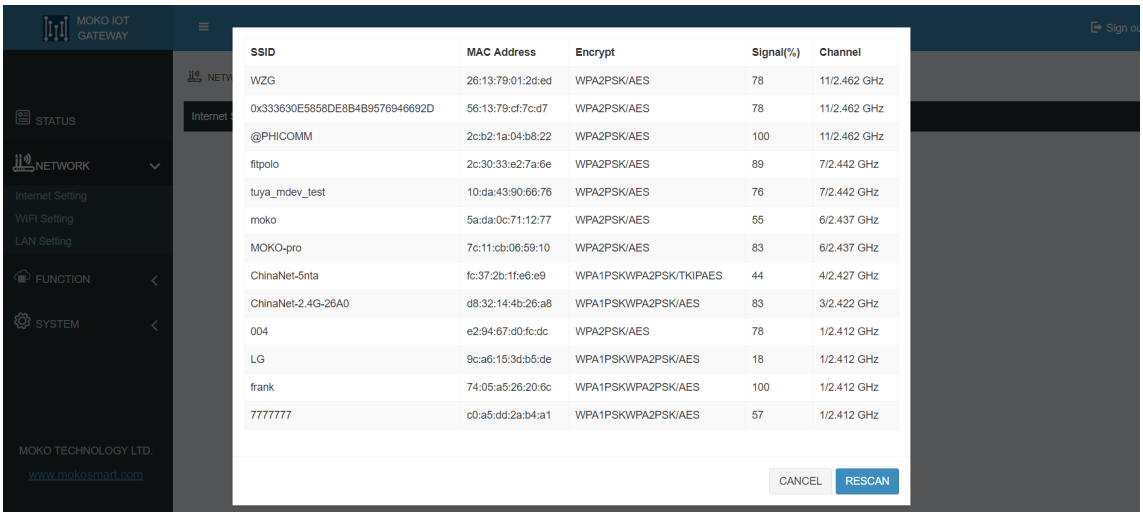
- **WIFI** — Connect to a **Wireless Router** via WLAN to access the internet. Select a wireless router and connect. After the configuration is complete, the gateway will restart.



WIFI / Automatic IP



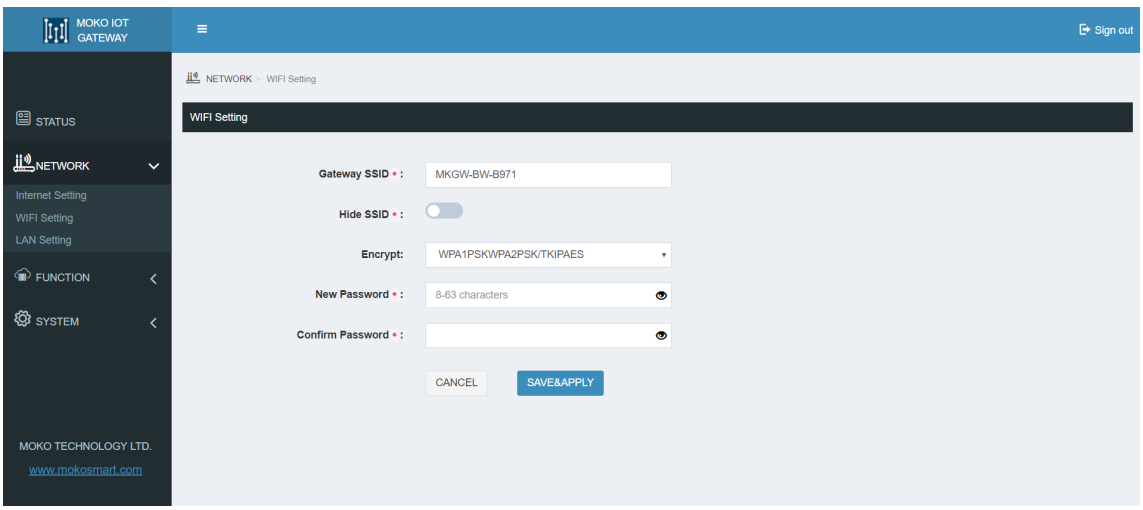
WIFI / Static IP



Select a Wireless Router

4.7 WIFI Setting

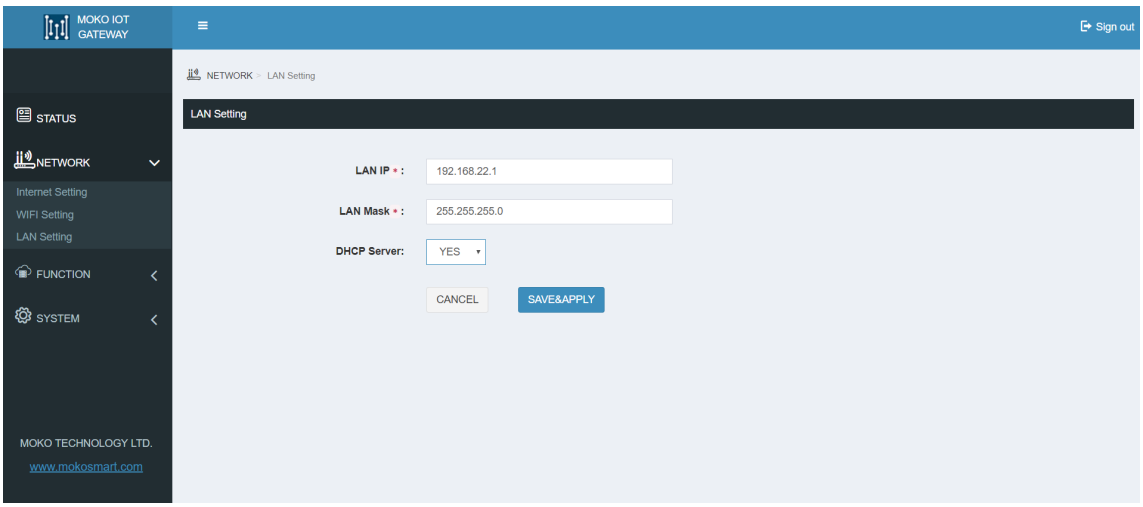
You can configure the SSID of the gateway, whether to hide the SSID, encryption mode, and password. After the configuration is complete, the gateway will be restarted for the configuration to take effect.



```
Supported encryption methods:

    WPA1PSKWPA2PSK/TKIPAES（Default）

    WPA1PSKWPA2PSK/AES

    WPA2PSK/TKIPAES

    WPA2PSK/AES

    WPA2PSK/TKIP

    WPAPSK/TKIPAES

    WPAPSK/AES

    WPAPSK/TKIP

    WEP

    NONE(No encryption)
```

4.8 LAN IP Setting

You can configure the gateway LAN IP and subnet mask. After the configuration is complete, the gateway will be restarted for the configuration to take effect.



Remark:
Gateway LAN IP and uplink LAN IP cannot be on the same network segment
The DHCP server generally chooses **YES**.

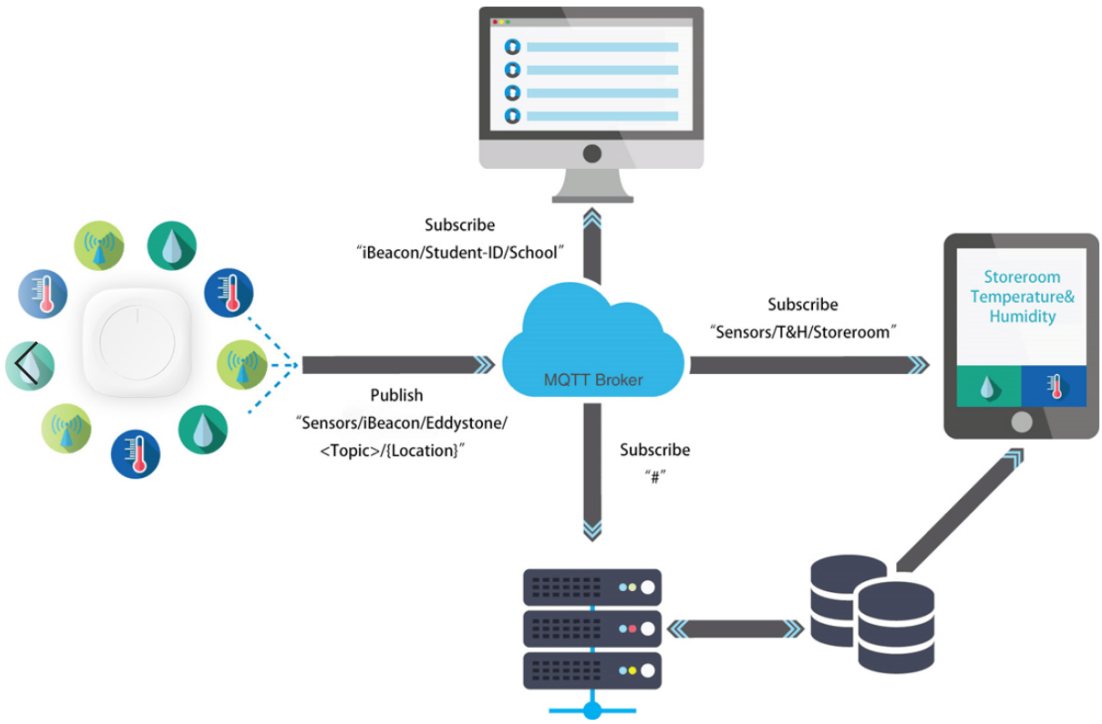
4.9 Server Access

Users can choose **MQTT (TCP/SSL)** or **HTTP/HTTPS** to upload data to the server.
The communication takes effect immediately after the configuration is completed.

4.9.1 MQTT

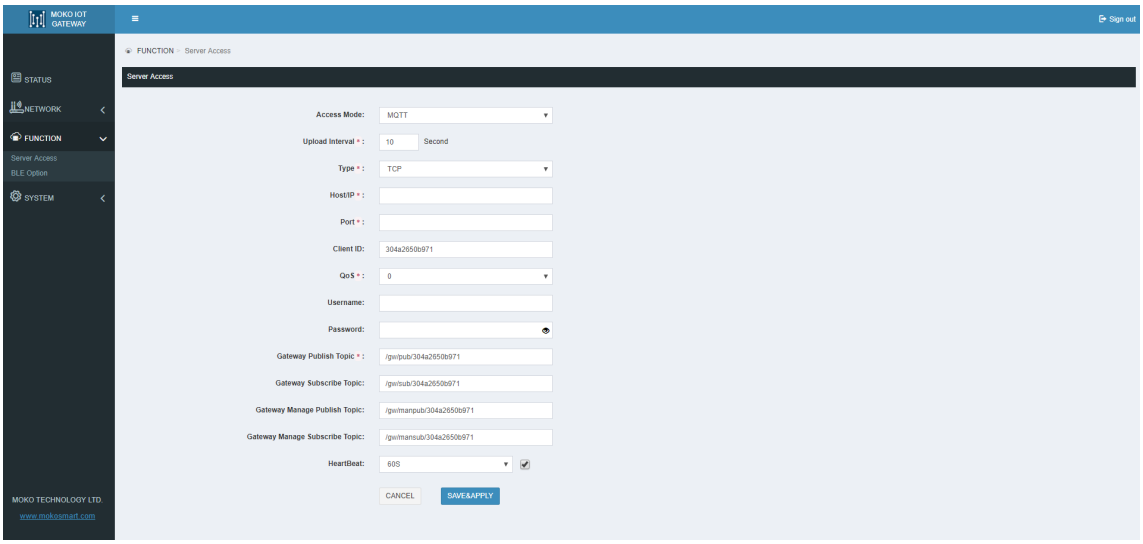
- MQTT is designed as a lightweight messaging protocol that uses publish/subscribe operations to exchange data between client and MQTT broker;

- In MQTT the process of sending messages is called publishing, and to receive messages an MQTT client must subscribe to an MQTT topic.
- In MQTT, the word topic refers to an UTF-8 string that the broker uses to filter messages for each connected client. The topic consists of one or more topic levels. Each topic level is separated by a forward slash "/ " (topic level separator). Also you can refer to the default design of the MKGW1 gateway.
- The gateway publishes Bluetooth advertising data to the MQTT broker in **Json format**;



Gateway publishes data through MQTT

- **MQTT TCP**



MQTT TCP

Configuration instructions

No.	Item	Description	Remark

No.	Item	Description	Remark
1	Upload Interval	Time interval for uploading data	Unit: s Input must be a positive integer
2	Host/IP	The HOST or IP address of the MQTT broker	
3	Port	MQTT port	MQTT is an application-level protocol. It works over TCP/IP, using **1883** port by default. If SSL is used, the TCP port is **8883**.
4	Client ID	Client identifier of gateway	The Client ID identifies each MQTT client that connects to the MQTT broker.
5	QoS	Quality of service in MQTT messaging	There are three levels of QoS:: 1. **QoS=0**, at most once. This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode. 2. **QoS=1**, at least once. This level guarantees that the message will be delivered at least once, but may be delivered more than once. 3. **QoS=2**, exactly once. This level guarantees that the message will be delivered only once.
6	Username	Client username	The username states your identity and entry of the password authenticates you as the rightful owner of that identity. MQTT authentication with username/password. The MQTT protocol provides username and password fields in the CONNECT message for authentication. The client has the option to send a username and password when it connects to an MQTT broker. Username can be empty.
7	Password	Client password	Reference to the above. Password can be empty.
8	Gateway Publish Topic	Client publish topic	Default：/gw/pub/304a2650b971 The last level is the MAC address of the lowercase character of the device.

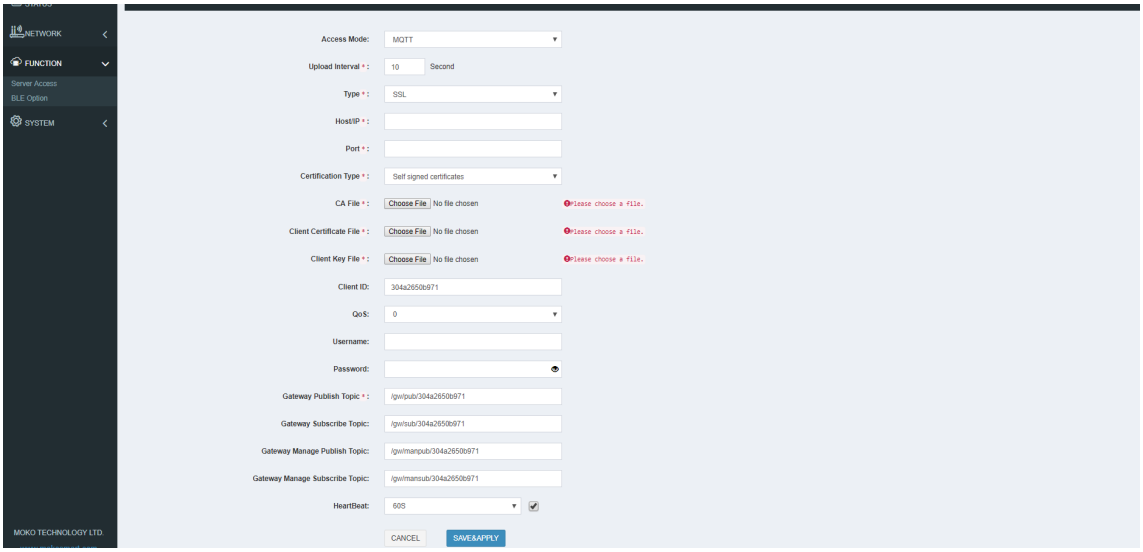
No.	Item	Description	Remark
9	Gateway Subscribe Topic	Client subcribe topic	Unused, reserved for subscribing topic from MQTT broker.
10	Gateway Manage Publish Topic	Client publish topic 2	Unused, reserved for configuring the gateway.
11	Gateway Manage Subscribe Topic	Client subcribe topic 2	Unused, reserved for configuring the gateway.
12	HeartBeat	Heartbeat packet	Used by the MQTT broker to determine whether the client is online. It can be turned on and off.

- **MQTT SSL**

Secure Sockets Layer (SSL) provides a secure communication channel between a client and a server. At the core, SSL is cryptographic protocols which use a handshake mechanism to negotiate various parameters to create a secure connection between the client and the server. After the handshake is complete, an encrypted communication between client and server is established and no attacker can eavesdrop any part of the communication. Servers provide a X509 certificate (typically issued by a trusted authority) that clients use to verify the identity of the server.

MQTT relies on the TCP transport protocol. By default, TCP connections do not use an encrypted communication. To encrypt the whole MQTT communication, many MQTT brokers allow use of SSL instead of plain TCP. If you use the username and password fields of the MQTT CONNECT packet for authentication and authorization mechanisms, you should strongly consider using SSL.

Port 8883 is standardized for a secured MQTT connection. The standardized name at IANA is “secure-mqtt”. Port 8883 is exclusively reserved for MQTT over SSL.

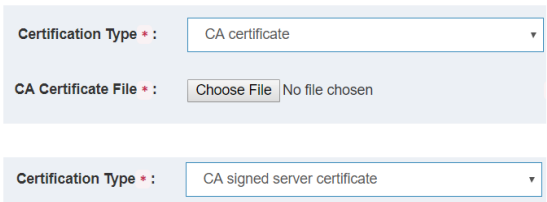


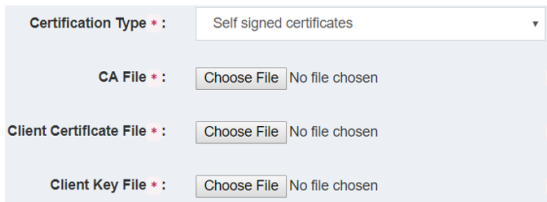
MQTT SSL

The user has to load certificate file, client key file. The configure items is the same as MQTT TCP type.

Supporting to verify the certification ways as following form:

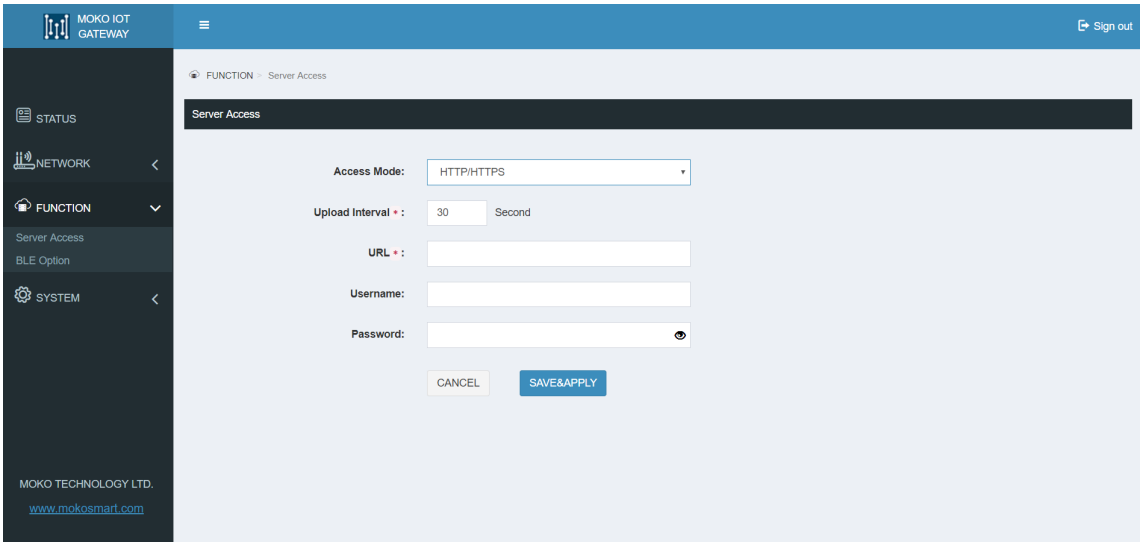
No.	Item	File	Remark
1	CA certificate	CA Certificate File	One-way authentication.
2	CA signed server certificate	-	One-way authentication.
3	Self signed certificates	CA File Client Certiflcate File Client Key File	Mutual authentication.





4.9.2 HTTP/HTTPS

- Gateway collect bluetooth advertising data, then publish it to the server via HTTP/HTTPS, data format is the same as MQTT **(json format)**.
- MKGW1 gateway just supports one-way authentication mechanism for verifying the certificate issued by the server.



HTTP/HTTPS

Configuration instructions

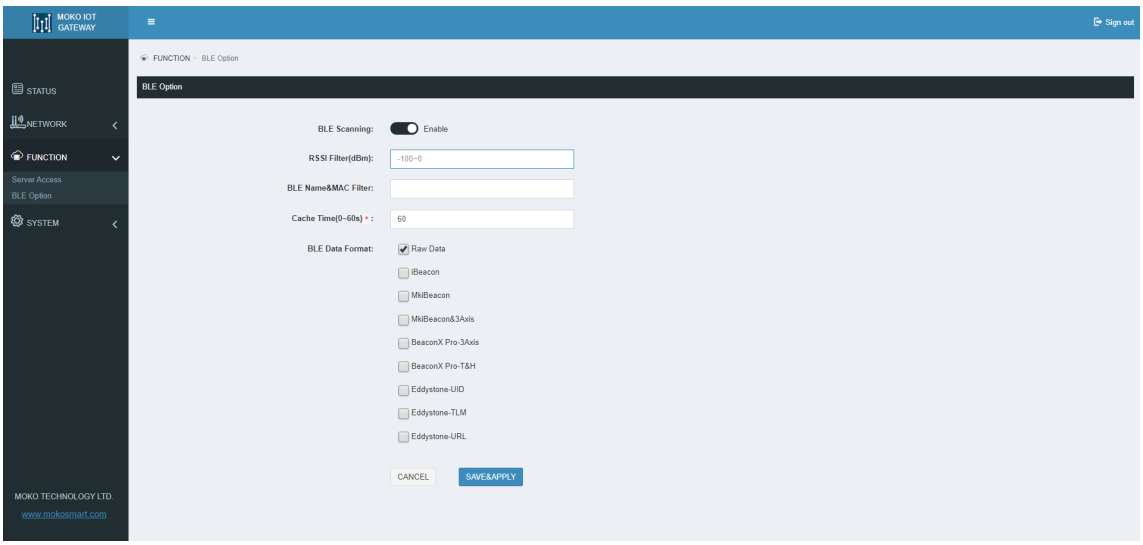
No.	Item	Description	Remark
1	Upload Interval	Time interval for uploading data	Unit: s Input must be a positive integer
2	URL	HTTP/HTTPS server address for data publishing	Deafult Port Number: HTTP — 80 HTTPS — 443
3	Username	Login username	Username and password upload with json format. Username can be empty.
4	Password	Login password	Username and password upload with json format. Password can be empty.

When need to verify username and password, the URL verification address uses **"login"** to replace the last level of the entered URL. If there is no last level in the entered URL, the URL verification address will add **"login"** after the entered URL.Refer to the following:

```
If the URL is: http://192.168.1.223/cgi-bin/cgitest.cgi

Then Login path should be: http://192.168.1.223/cgi-bin/login


If the URL is: http://192.168.1.223

Then Login path should be: http://192.168.1.223/login
```

4.10 BLE Option

User can select the type of Bluetooth advertising data that needs to be uploaded, and can filter the data by BLE name, MAC address, and RSSI.



BLE Option

Configuration instructions

No.	Item	Description	Remark
1	BLE Scanning	Turn On/Off BLE scanning	
2	RSSI Filter	Filter by RSSI	Scan devices with RSSI no less than input data.
3	BLE Name&MAC Filter	Filter by Bluetooth Name and MAC address	Scan devices with Bluetooth name or MAC address containing the input keywords.
4	Cache time	The length of time to cache data, ranging from 0 to 60 seconds	When the device has no communication with the server, the Bluetooth scanning data of the specified duration can be cached. Maximum support for storing 256 Bluetooth advertising data.
5	BLE data format	Filter advertising data format	Multiple-choice. Currently the advertising data format that can be filted is as follows:: Raw Data iBeacon MkiBeacon MkiBeacon&3Axis BeaconX Pro-3Axis BeaconX Pro-T&H Eddystone-UID Eddystone-TLM Eddystone-URL

Advertising data format

No.	Item	Description	Remark
1	Raw Data	Bluetooth advertising source data. It has not parsed according to a certain format.	Upload all scanned advertising data.
2	iBeacon	Standard iBeacon format	-
3	MkiBeacon②	Standard iBeacon format & MkiBeacon response packet format	Upload standard iBeacon frame data and MkiBeacon response packet frame data
4	MkiBeacon&3Axis③	Standard iBeacon format & MkiBeacon with 3-axis accelerometer response packet format	Upload standard iBeacon frame data and MkiBeacon with 3-axis accelerometer sensor response packet frame data
5	BeaconX Pro-3Axis	BeaconX Pro with 3-axis accelerometer sensor advertising data format	-
6	BeaconX Pro-H&T	BeaconX Pro with Temperature&Humidity sensor advertising data format	-
7	Eddystone-UID	Standard Eddystone-UID format	-
8	Eddystone-TLM	Standard Eddystone-TLM format	Unencrypted TLM
9	Eddystone-URL	Standard Eddystone-URL format	-

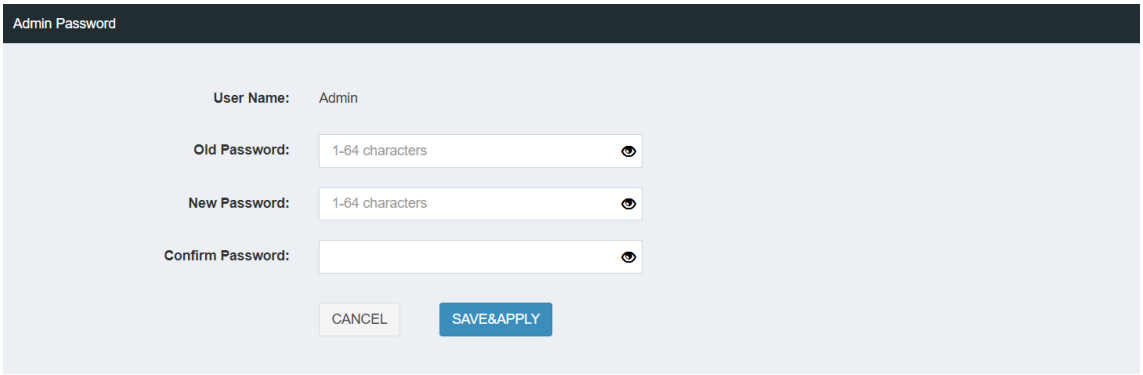
The Bluetooth advertising data scanned by the gateway is uploaded to server in **"json"** format.
If you need more information about the advertising data format of the MOKO series Beacon, please refer to **http://doc.mokotechnology.com/index.php?s=/page/105 (http://doc.mokotechnology.com/index.php?s=/page/105)**

②③ *The advertising data frame with the response packet will broadcast the advertising packet and the response packet separately. The gateway also will upload advertising packet and response packet separately. Developers need to merge advertising and response packets as needed.*
The advertising packets of MkiBeacon and MkiBeacon&3Axis are both standard iBeacon frames.

4.11 Device Setting

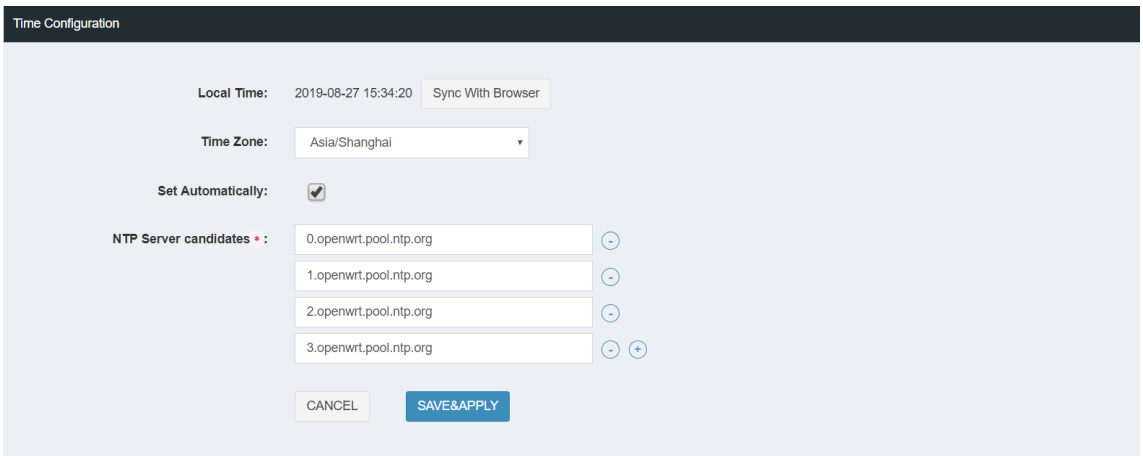
4.11.1 Modify Login Password

- User can modify the password for logging in configuration web UI;
- The login user name is **"Admin"** (Unmodifiable);
- The length of password is **1-64** characters and needs to be verified with the **old password**.



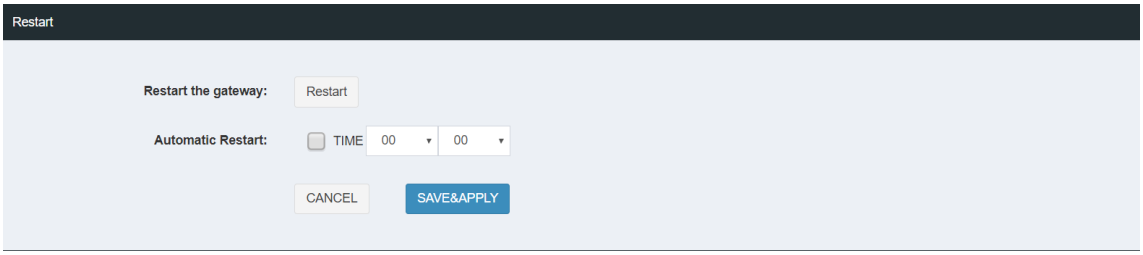
4.11.2 Time Configuration

- User selects the time zone, and then checks **"Set Automatically"**. The NTP server follows the default settings and automatically updates to the current time in the time zone;
- If the user needs to set the time to match the local browser time, close **"Set Automatically"** and click **"Sync With Browser"** to update to the current browser time.



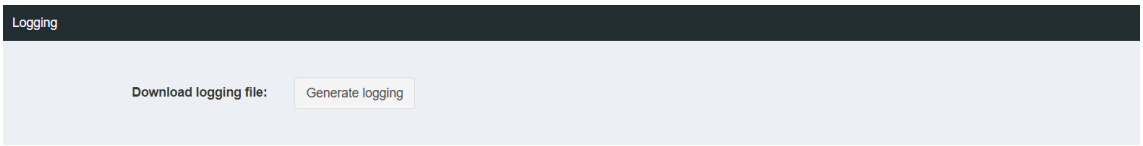
4.11.3 Restart

- Click **"Restart"** and the gateway will restart immediately;
- The user can turn on the **"Automatic Restart"** function (Closed by default) and set the time for the gateway to automatically restart each day. This operation can free up system RAM and ensures that the system runs smoothly and steadily.



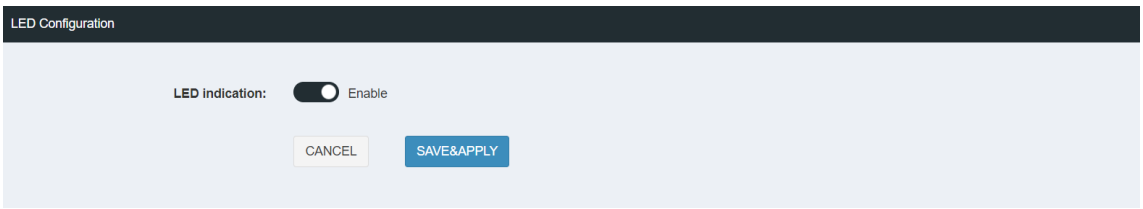
4.11.4 Log File

Once the user finds the device abnormal during use, the system log file can be downloaded to the local. Please send the log file to MOKO to check the system error.



4.11.5 LED Configuration

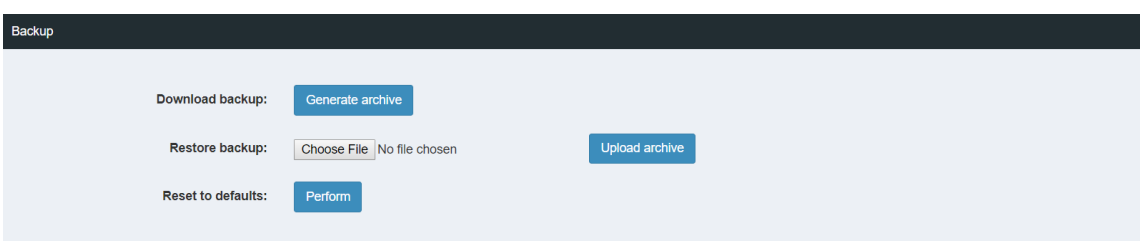
- User can turn off the device LED. After saving, the operation takes effect immediately
- In the state of turning off the LED, if the system is abnormal or the system is upgraded, the LED will still be enabled.



4.12 Backup & Upgrade

4.12.1 Backup

- User can download the configured parameter file of the gateway to the local;
- User can directly import the configured file into the current system. After the device is restarted, the configuration will take effect.

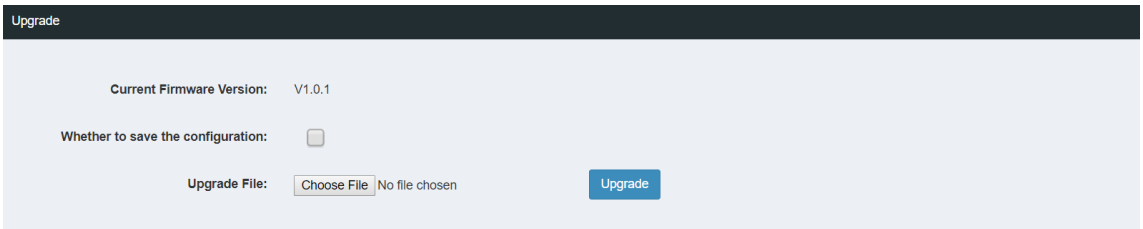


No.	Item	Description	Remark

No.	Item	Description	Remark
1	Download Backup	Download the configured parameter file	Download all currently configured parameters to the local.
2	Restore Backup	Restore gateway parameters according to backup file	You need to upload the saved local backup file.
3	Reset to Defaults	Restore the gateway to the factory default configuration	This feature is consistent with the following actions: Press and hold the gateway **"RESET"** button for over 5 seconds until the gateway restarts.

4.12.2 Upgrade

User can upgrade the system by uploading **Upgrade File**. You can check **"Whether to save the configuration"** to ensure that the upgraded system parameters are consistent with the current system configuration parameters.



USB upgrade method:

Step1. Copy the upgrade file named "MKGW-BW-Upgrade.bin" to the USB flash drive;

Step2. Insert the USB flash drive into the gateway **USB Port**, short press the **RESET** button, and the device will automatically upgrade. With USB upgrade, the gateway will automatically save the current system configuration parameters.

5. Declaration

The contents of this document are subject to change without prior notice for further improvement. MOKO team reserves all the rights for the final explanation.
Please contact MOKO sales team or visit **https://www.mokosmart.com/ (https://www.mokosmart.com/)** to get more related information if needed.

6. Contact Information

MOKO TECHNOLOGY CO. LTD
Address : 4F,Buidling2, Guanghui Technology Park, MinQing Rd, Longhua, Shenzhen, Guangdong, China
Telephone : 86-75523573370
Fax : 86-75523573370-808
Website : https://www.mokosmart.com/ (https://www.mokosmart.com/)

Revision History

Revision	Description of changes	Approved	Revision Date
V1.0	Initial Release	Kevin	2019.08.27