MKGW3 BLE to POE Gateway

User Manual

Version V2.0

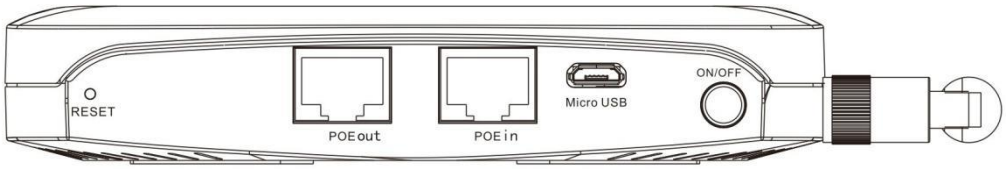
Contents

1. About this document 1
2. Hardware description 1
3. LED status 1
4. Install gateway 2
5. Power on the gateway 3
6. Configure gateway with APP 3
    6.1 Configure mobile APP 4
    6.2 Configure gateway 5
    6.3 Scan BLE devices 9
    6.4 Manage BLE devices 10
    6.5 Set scanner and upload option 11
    6.6 Gateway parameter settings 21
    6.7 OTA 24
    6.8 Modify Network settings 25
    6.9 Device Information 26
    6.10 Reboot 27
    6.11 Reset Device 27
Appendix A: WPA2 Enterprise Security 28
Appendix B: Connect to AWS IoT 28

1. About this document

This User Guide was designed to help users to know the MOKO MKGW3 gateway and set up the gateway with MOKO APP.

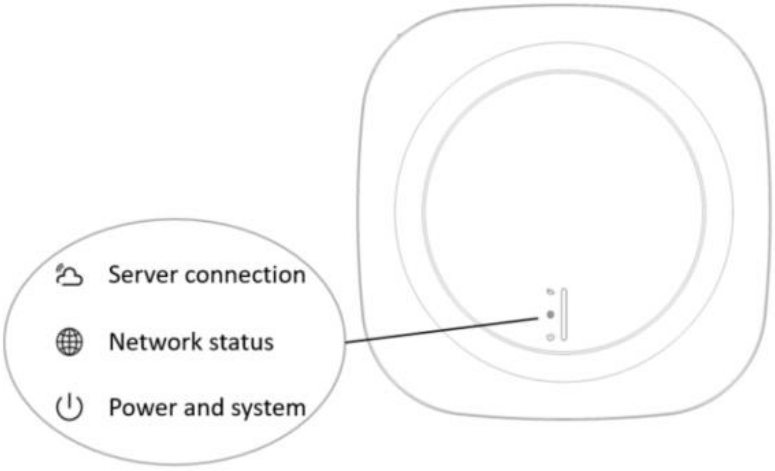
2. Hardware description



- On/off button: to turn on/off the gateway
- Micro USB: Inject a Micro USB cable to power on the gateway
- POE in: Inject an Ethernet cable from a POE switch, the gateway can be powered on and obtain network access.
- POE out: To cascade to the next gateway, can provide power and network to the next gateway
- Reset hole: Insert a needle-like object into the hole and press the button for 5 seconds to reset the gateway.

3. LED status

There are three RGB LEDs to indicate the gateway power status, network status and server connection status.



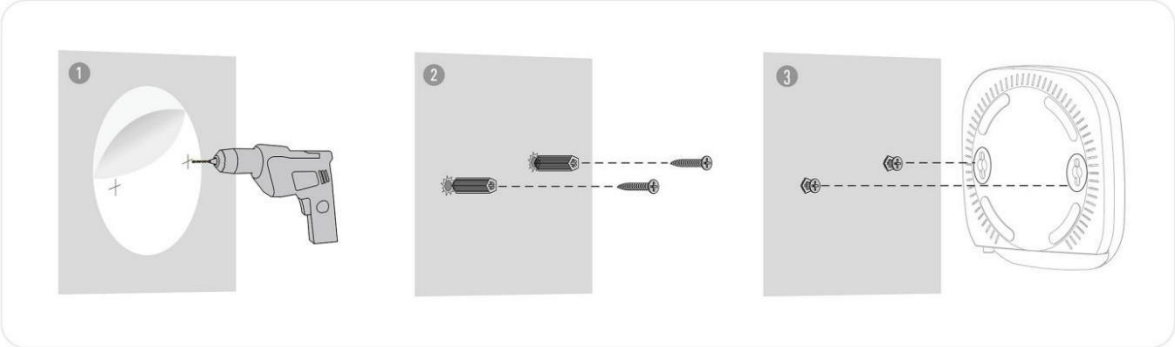
The LED status and gateway status are shown as below:

Gateway status	Power/system LED	Network LED	Server LED
Not powered	off	off	off
Power is normal and gateway is ready	Solid **Green**		
Bluetooth is advertising (Pairing mode)		Flash **Blue**	
Bluetooth is connected		Solid **Blue**	
Connecting to network by Ethernet		Flash **Green**	
Connected to network by Ethernet		Solid **Green**	
Connecting to network by WiFi		Flash **Yellow**	
Connected to network by WiFi		Solid **Yellow**	
Connecting to server			Flash **Green**
Connected to server			Solid **Green**
Factory reset	Alternately flash **Blue** and **Green** once		
OTA process	Flash **Yellow**		
OTA succeed	Solid **Yellow**		
OTA failed	Solid **Red**		

4. Install gateway

You can place the gateway on a table or hang the gateway on the wall. The tools provided with the gateway (PET positioning sticker, screws and plastic wall plug) can help you easily hang the gateway on the wall, you can follow the steps below to install it.

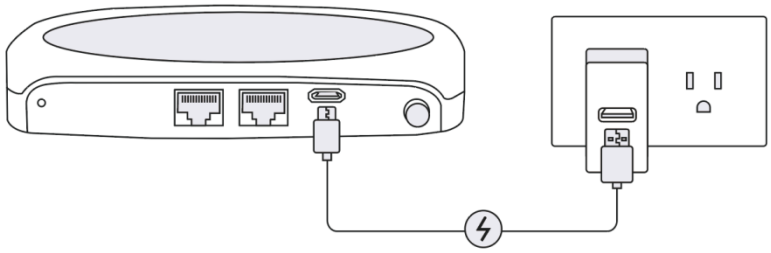
Step 1: Use 5mm drill head, drill 2 holes on the wall according to the PET positioning sticker.
Step 2: Push or tap the plastic wall plugs into the holes, flush with the plaster.
Step 3: Put the screw into the wall plug, twisting the screw a tiny bit by hand or screwdriver till it bites. Do not insert the screw completely into the wall plug as a portion of the screw head must be exposed no less than 3mm to hang the gateway.
Step 4: Insert the screw heads into the hanging hole behind the gateway, then gently pull down to complete the installation.



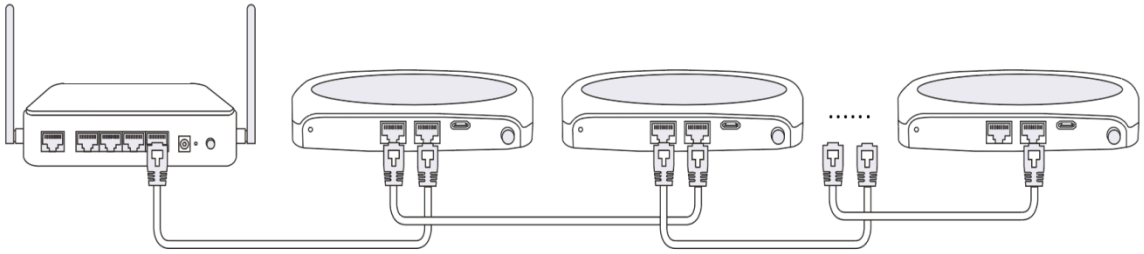
5. Power on the gateway

Please select the compliant cable to power up the gateway,we can select one power supply method to use. When the power cable is connected, please don't forget to click the ON/OFF button to power up the gateway.

Method 1: Power on gateway by Micro USB cable



Method 2: Power on gateway by POE cable



6. Configure gateway with APP

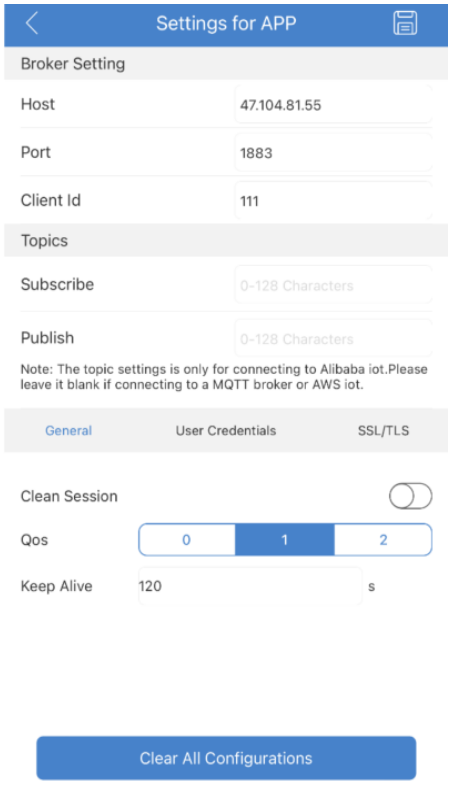
MOKO provides a demo APP with users to configure the gateway, please search "MKScannerPro" in APP Store or Google Play to download the APP.

In the configuration, we will firstly configure the app connecting to MQTT broker and then configure gateway connecting to MQTT broker. After the APP and gateway are both connected with MQTT broker, then users can use the APP to remotely manage the gateway.

6.1 Configure mobile APP

Run the MKScannerPro APP on your mobile phone, and allow the location and storage permissions. Select “POE gateway” to start the configuration.

Click ☰ to configure MQTT settings for the APP. The APP has default MQTT settings, if using default settings for testing purpose, just click 💾. It also allows to change the settings, after enter and save new settings, app will connect to the MQTT server. If connect successfully, it will show “success”, otherwise it will show “connect failed”. If connect failed, please check the settings and connect again.



There are three buttons in the very bottom of this page to help users quickly complete the configuration:

- Clear all configurations: Delete all the current settings, so that users can input new settings.
- Export config file: Export the current settings from the APP, it will create a excel file and can be sent by email.
- Import config file: With the exported file, users can change the settings and import the new file to the APP, then the APP will use the new settings.

If connecting with customer server, please follow the below descriptions to finish the configuration:

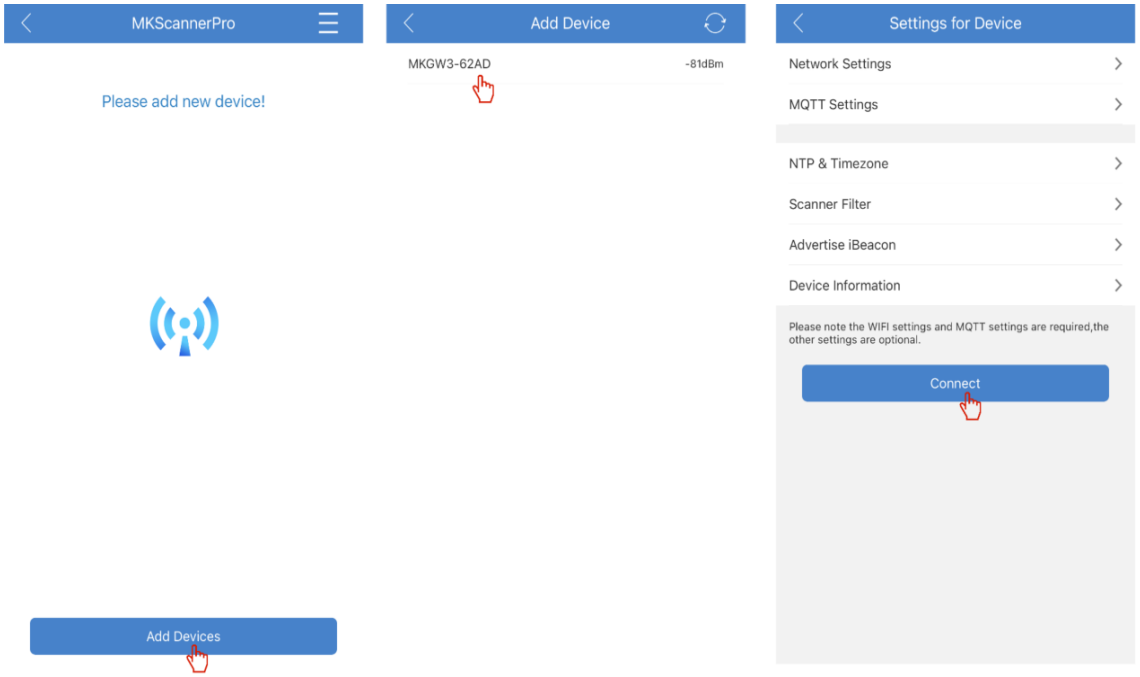
Type	Parameter	Description
Broker setting	Host	Server IP address or domain name
	Port	Server port

	Client id	MQTT client id, each device connected to the server should have a **different** client id.
Topics	Subscribe	**These two settings are used for connecting to Alibaba cloud. If connect to a MQTT broker or AWS IoT, please leave it blank.**
	Publish	
General	Clean session	Default: Enable, range: Enable/Disable
	Qos	Quality of service. Default: 1, range: 0-2
	Keep Alive	Default: 60, range: 10-120
User Credentials	Username	If access to your server doesn't require a username and password, it can be blank.
	Password	
SSL/TLS	SSL/TLS	on: SSL encryption. off: no encryption
	Certificates	It supports CA signed server certificate/CA certificate file/Self signed certificates

6.2 Configure gateway

When the gateway Network LED flashes **Blue**, click "Add Devices" to connect the gateway Bluetooth. We can see some advertisers named "MKGW3-XXXX", select the gateway and enter password **Moko4321**. After that, the Network LED will turn to solid **Blue**.

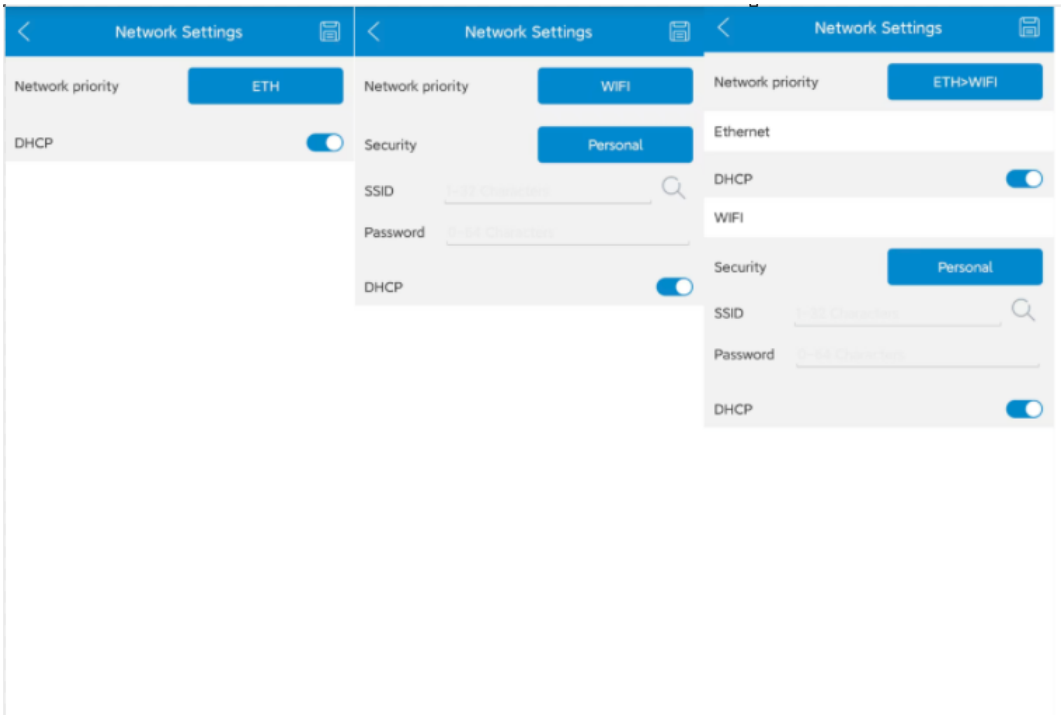
Then we can configure the Network, MQTT and some other settings for the gateway. After all settings are finished, click "Connect" button, the gateway will connect to network and then connect to the server. If it cannot connect to server in 90 seconds, the gateway will go back to pairing mode, we can configure it again.



Please note: the network and MQTT settings are must-required, while other settings are optional.

6.2.1 Network settings

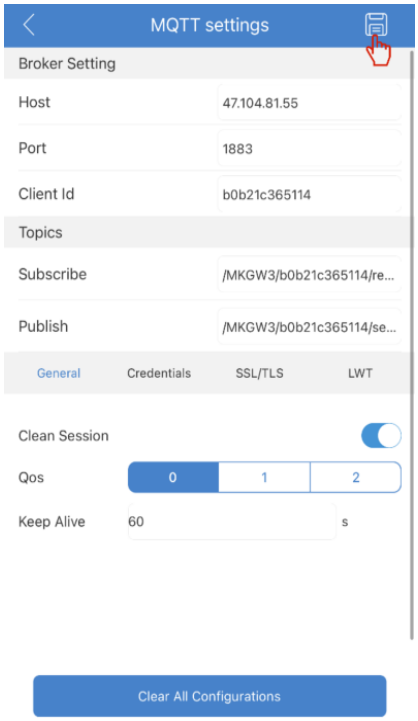
To configure network type and IP for the gateway.
The network type can be selected as: Ethernet, WiFi, and Ethernet->WiFi
When select Ethernet, we need make sure the gateway is powered by a POE network cable.
When select WiFi, we can scan the nearby WIFI, personal and Enterprise security are both supported.
When select Ethernet->WiFi, we need to configure both Ethernet and WiFi, gateway will first try the Ethernet connection, if Ethernet fails to connect to Internet, the gateway will auto switch to WiFi.
The personal WiFi requires only the SSID and password. The enterprise WIFI supports different EAP types and requires different authentication. Please see the ***Appendix A: WPA2 Enterprise Security*** to get more details.



6.2.2 MQTT settings

To configure MQTT parameters for the gateway. The gateway has default MQTT settings, if use default settings for testing purpose, just click . It also allows to change the settings. If connect the gateway to AWS IoT, please see ***Appendix B Connect to AWS IoT*** to get more details.

In the very bottom of this page, there are also three buttons used to help users quickly complete the configuration.



If connecting with customer server, please follow the below descriptions to finish the configuration:

Type	Parameter	Description
Broker setting	Host	Server IP address or domain name
	Port	Server port
	Client id	MQTT client id, each device connected to the server should have a **different** client id. The default id is device MAC address.
Topics	Subscribe	It has a default topic, can be changed
	Publish	It has a default topic, can be changed
General	Clean session	on/off
	Qos	Quality of service. Default: 1, range: 0-2
	Keep Alive	Default: 60, range: 10-120
User Credentials	Username	If access to your server doesn't require a username and password, it can be blank.
	Password	
SSL/TLS	SSL/TLS	on: SSL encryption. off: no encryption
	Certificates	It supports CA signed server certificate/CA certificate file/Self signed certificates
LWT	LWT	on/off
	Retain	on/off

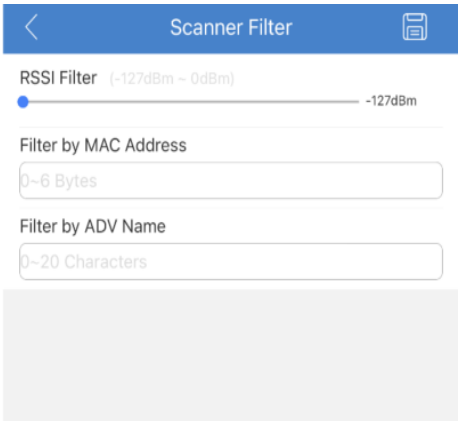
	Qos	Quality of service. Default: 1, range: 0-2
	Topic	It has a default topic, can be changed
	Payload	It has a default topic, can be changed

6.2.3 NTP&Timezone

To configure the NTP server and timezone for the gateway.

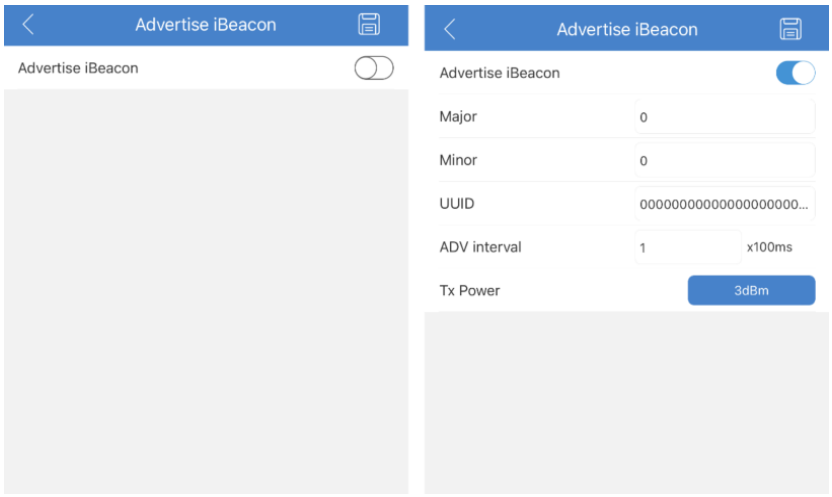
6.2.4 Scanner filters

To configure the scanner filter for the gateway. It supports filter by RSSI, MAC and advertising name.



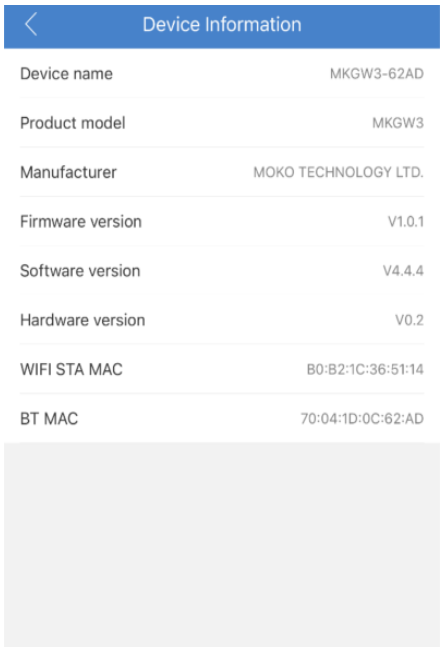
6.2.5 Advertise iBeacon

To set the gateway advertise iBeacon and setup advertising parameters. By default, iBeacon advertisement is turned off. if it is turned to on, the gateway will advertise iBeacon frame after it connects to server.



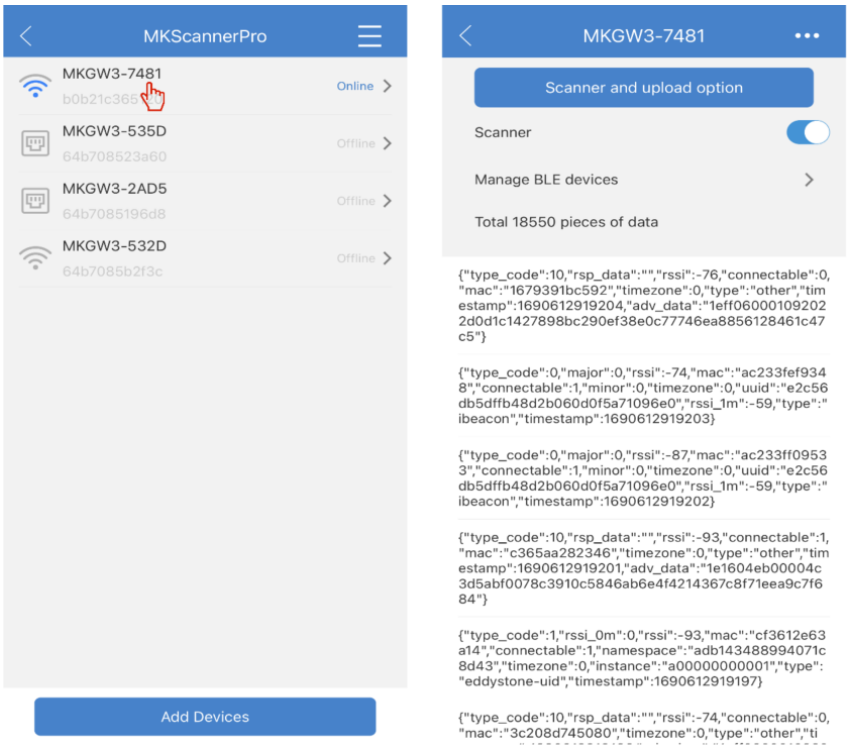
6.2.6 Device information

To read the device information of the gateway.



6.3 Scan BLE devices

When the gateway is successfully configured, it will automatically start scanning. At the same time, the gateway will measure the network status and show it in the app.

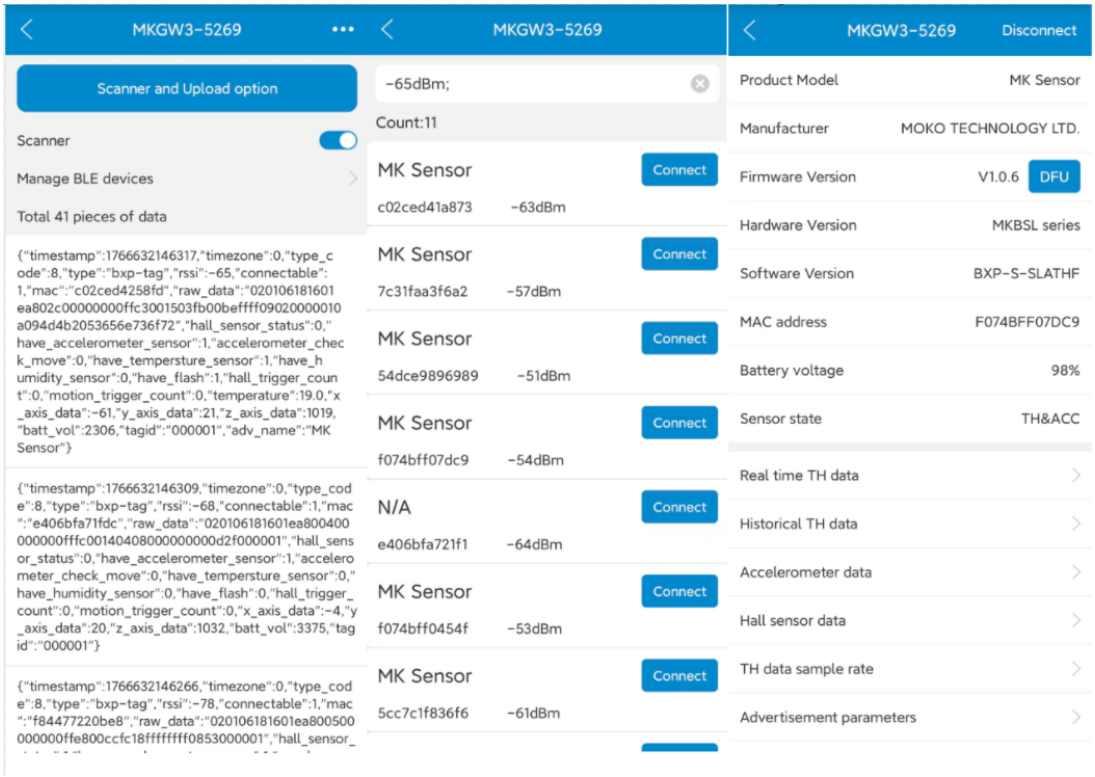


Icon	Network status	RSSI
	OFFLINE	/
	POOR WiFi	<-65 dBm
	MEDIUM WiFi	-65~-50 dBm
	GOOD WiFi	>-50 dBm
	Ethernet	/

6.4 Manage BLE devices

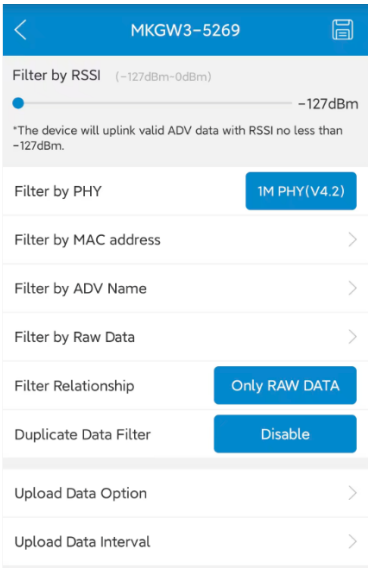
Click the manage BLE device button, it will jump to the next page where you can search and connect the nearby Beacon device.

When we want to connect to the beacon, we can click the “connect” button, then select the beacon type, and input the password. After the gateway is connected with the Beacon, we can get the product information, battery and history temperature and humidity data. The “disconnect” button in the top used to disconnect from the beacon.



6.5 Set scanner and upload option

To set the scanning filter and uploading data content for the gateway.



6.5.1 Filter By RSSI

The gateway will upload the beacon advertising data with RSSI no less than the setting value.

Parameter	Description
RSSI	Default: -127 dBm, range: -127~0 dBm.

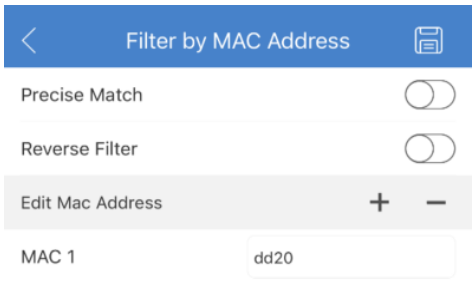
6.5.2 Filter By PHY

The gateway will upload the beacon advertising data with RSSI no less than the setting value.

Parameter	Description
Filter by PHY	Options: ➢ 1M PHY (V4.2) ➢ 1M PHY (V5.0) ➢ 1M PHY (V4.2) and 1M PHY (V5.0) ➢ Coded PHY

6.5.3 Filter By MAC address

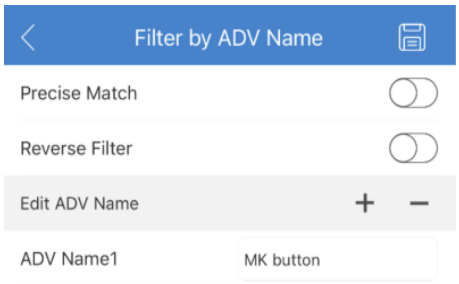
The gateway filters beacon data according to beacon MAC address, it supports up to 10 sets of MAC address at the same time.



Parameter	Description
Precise match	OFF: Upload the advertising data of the beacon whose MAC address contains the input expression. ON: Upload the advertising data of Beacon whose first N (N<=6) bytes of MAC is the same as the input expression.
Reverse filter	OFF: Upload advertising data of Beacon whose MAC address conforms the input expression. ON: Upload advertising data of Beacon whose MAC address doesn't
MAC address	Click the "＋" icon, it can add at most 10 sets of MAC address, the relationship of each MAC is "or", and case insensitive. Click the "—" icon, it will delete the MAC address input box.

6.5.4 Filter by ADV Name

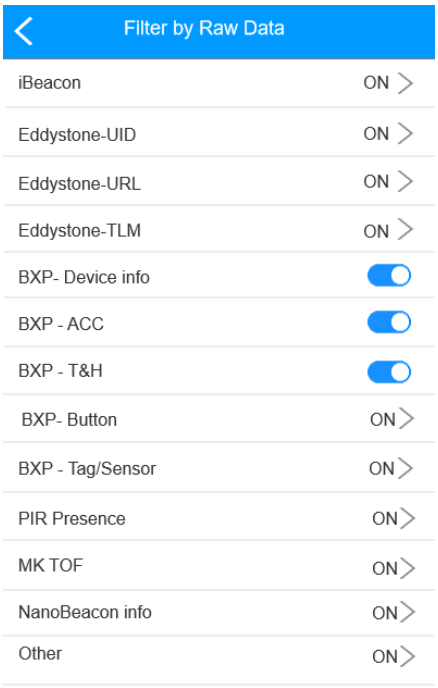
The gateway filters beacon data according to beacon advertising name, and it supports up to 10 set of advertising name at the same time.



Parameter	Description
Precise match	OFF: Upload the advertising data of the beacon whose adv name contains the input expression. ON: Upload the advertising data of Beacon whose first N (N<=20) bytes of adv name is the same as the input expression.
Reverse filter	OFF: Upload advertising data of Beacon whose adv name conforms the input expression. ON: Upload advertising data of Beacon whose adv name doesn't conform the input expression.
ADV name	Click the "＋" icon, it can add at most 10 sets of advertising names, the relationship of each ADV name is "or", and case insensitive. Click the "—" icon, it will delete the ADV name input box.

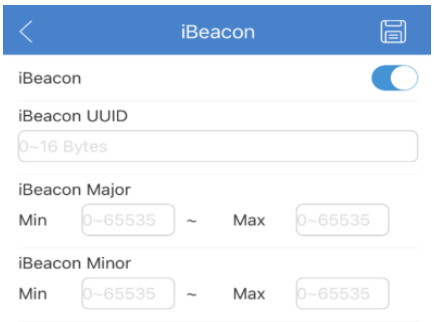
6.5.5 Filter by Raw Data

The gateway filters beacon data according to advertising data type.
The first 10 types are supported by MOKO beacon, the gateway will decode all MOKO beacon data. Other beacon data apart from the 10 types will be called "Other", gateway will not decode the data, directly upload raw data to cloud.



6.5.5.1 iBeacon

To determine upload iBeacon data or not.
If the iBeacon switch is on, the iBeacon UUID, major and minor are empty, the gateway will upload all detected iBeacon data. If the iBeacon UUID, major and minor are filled with some value, the gateway will upload only the iBeacon data which conforms the value.

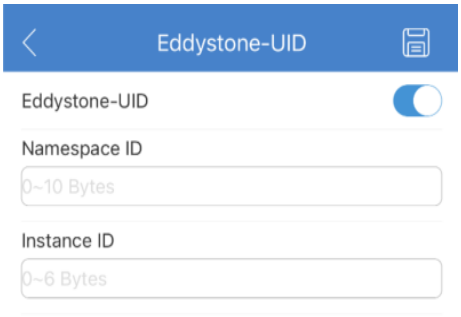


Parameter	Description
Switch	On: upload, off: not upload
iBeacon UUID	0-16 bytes iBeacon UUID with Hex format
iBeacon major	From 0 to 65535, the Max value must be no less than the Min value.
iBeacon minor	From 0 to 65535, the Max value must be no less than the Min value.

6.5.5.2 Eddystone - UID

To determine upload Eddystone-UID data or not.

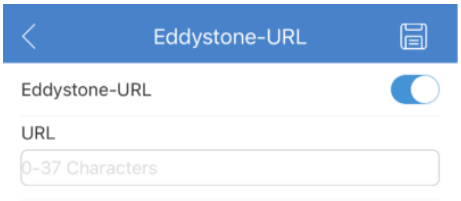
If the Eddystone-UID switch is on, the Namespace ID and Instance ID are empty, the gateway will upload all detected Eddystone - UID data. If the Namespace ID and Instance ID are filled with some value, the gateway will upload only the Eddystone - UID data which conforms the value.



Parameter	Description
Switch	On: upload, off: not upload
Namespace ID	0-10 bytes Hex data
Instance ID	0-6 bytes Hex data

6.5.5.3 Eddystone - URL

To determine upload Eddystone-URL data or not.
If the Eddystone - URL switch is on, the URL is empty, the gateway will upload all detected Eddystone - URL data. If the URL is filled with some value, the gateway will upload only the Eddystone - URL data which conforms the value.

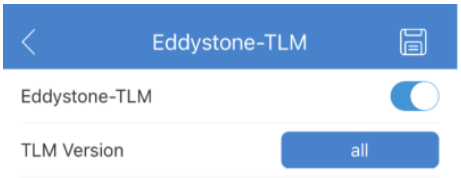


Parameter	Description
Switch	On: upload, off: not upload
URL	0-37 characters, for example: www.mokosmart.com

6.5.5.4 Eddystone - TLM

To determine upload Eddystone-TLM data or not.

If the Eddystone - TLM switch is on, the TLM version is all, the gateway will upload all detected Eddystone - TLM data. If the TLM version is configured to 0 0r 1, the gateway will upload only the Eddystone - TLM data whose TLM version conforms the configuration.



Parameter	Description
Switch	On: upload, off: not upload
TLM version	Range: All/ version 0/ version 1 ➢ Null: All versions will be uploaded; ➢ Version 0: Unencrypted TLM; ➢ Version 1: Encrypted TLM

6.5.5.5 BXP- Device info

Parameter	Description
Switch	To determine upload BXP-device info data or not. On: upload, off: not upload

6.5.5.6 BXP- ACC

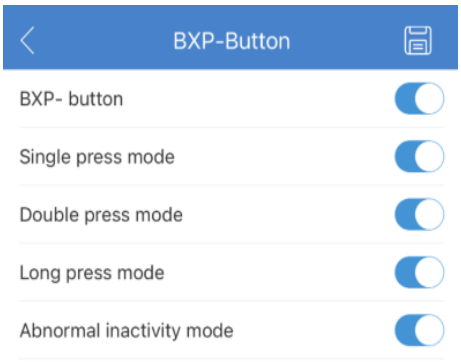
Parameter	Description
Switch	To determine upload BXP-ACC data or not. On: upload, off: not upload

6.5.5.7 BXP- T&H

Parameter	Description
Switch	To determine upload BXP-T&H data or not. On: upload, off: not upload

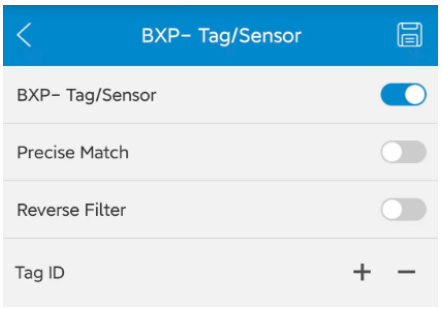
6.5.5.8 BXP- Button

To determine upload BXP-Button data or not.
It supports filter the specified data by trigger modes. If all modes are on, the gateway will upload all detected BXP-button data. If the modes are off, the gateway will not upload the advertising data triggered by the modes.



6.5.5.9 BXP- Tag/Sensor

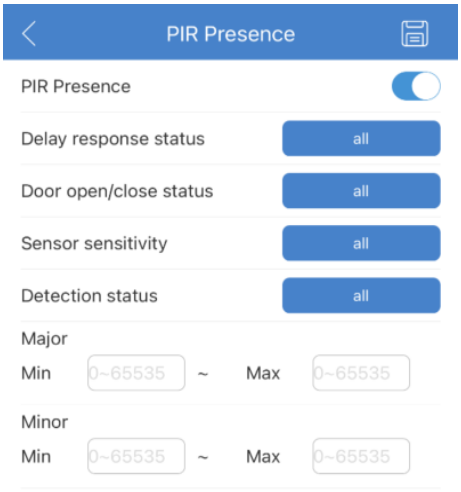
To determine upload BXP-Tag/Sensor data or not. It supports filter the specified data by Tag ID, allows to set up to 10 sets of Tag id at the same time.



Parameter	Description
Switch	On: upload, off: not upload
Precise match	OFF: Upload adverting data of Beacon whose tag id contains the input expression. ON: Upload adverting data of Beacon whose first N (N<=6) bytes of tag id is the same as the input expression.
Reverse filter	OFF: Upload advertising data of Beacon whose tag id conforms the input expression. ON: Upload advertising data of Beacon whose tag id doesn't conform the input expression.
Tag id	Click the "＋" icon, it can add at most 10 sets of tag id, the relationship of each tag id is "or", and case insensitive. Click the "—" icon, it will delete the tag id input box.

6.5.5.10 PIR Presence

To determine upload PIR Presence data or not.
It supports filter the specified data by sensor status and major, minor.



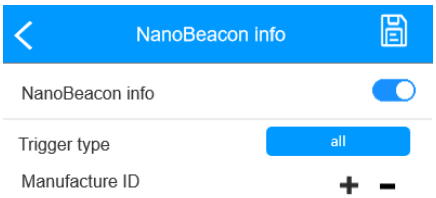
Parameter	Description
Switch	On: upload, off: not upload
Delay response status	Options: All/low delay/ medium delay/high delay All: All delay status advertising data will be uploaded
Door open/close response status	Options: All/close/open All: All door status advertising data will be uploaded
Sensor sensitivity	Options: All/low/medium/high All: All sensor sensitivity advertising data will be uploaded
Detection status	Options: All/no motion detected/motion detected All: All detection status advertising data will be uploaded
Major	From 0 to 65535, the Max value must be no less than the Min value.
Minor	From 0 to 65535, the Max value must be no less than the Min value.

6.5.5.11 MK TOF

To determine upload MK TOF data or not.
It supports filter the specified data by MFG Code.

6.5.5.12 Nanobeacon Info

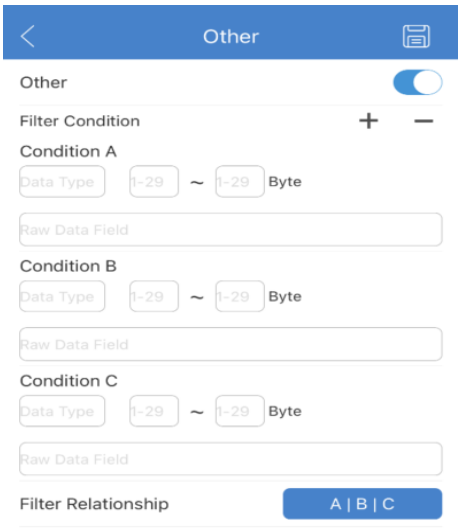
To determine upload Nanobeacon info data or not.
It supports filter the specified data by trigger type and manufacture ID.



Parameter	Description
Switch	On: upload, off: not upload
trigger type	Options: All/normal type/ trigger type All: All trigger type advertising data will be uploaded
manufacture ID	Click the “＋” icon, it can add at most 10 sets of manufacture id, the relationship of each manufacture id is “or”, and case insensitive. Click the “—” icon, it will delete the manufacture id input box.

6.5.5.13 Other

The Beacon data other than the above 12 types will be judged as “other”. The reporting format of other type is raw data, without decoder.



Parameter	Description
Switch	On: upload, off: not upload
Condition A	➢ Data type: 1 byte Bluetooth data type ➢ Data range: The start and end byte under the data type. It can be set to any two values from 1-29, the end value must be no less than the start value. ➢ Raw data field: Raw data value under the data type, and the data length should match the data range.
Condition B	The same as condition A
Condition C	The same as condition A
Filter relationship	The “AND/OR” logic setting for the conditions.

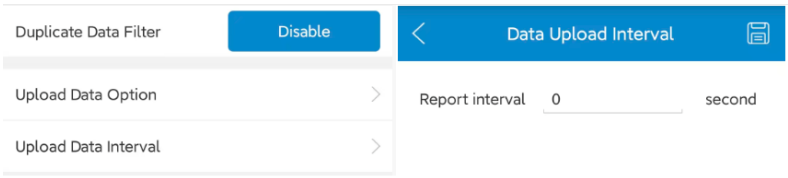
6.5.5 Filter Relationship

After the MAC filter, ADV name filter or raw data filter is set, it also needs to set the filter relationship, the relationship determines the processing logic.
If we set one or more filters, but relationship is set as “Null”, the filters will not take effect. The relationship should match the filters, otherwise there will be no data uploaded.

Parameter	Description
Relationship	Default: Null Range: Null/ Only MAC/ Only ADV name/ Only raw data/ ADV name & Raw data/ MAC & ADV name & Raw data/ ADV name| Raw data/ ADV name& MAC.

6.5.6 Duplicate Data Filter

To reduce too many duplicate data uploaded to your server. In a filtering period, If the gateway scans a new data, it will report the data immediately, and throw the following data which are same as that one, finally report only one piece which is latest scanned in the period.
Note: only when the gateway report interval is not 0, the duplicate data filter will take effect, otherwise the gateway will report real-time data, and the duplicate data filter won’t work.

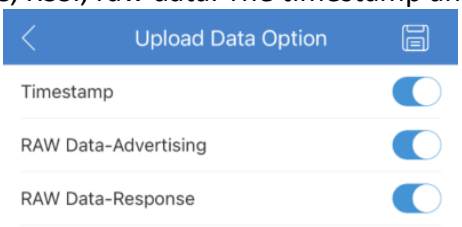


Parameter	Description

Duplicate Data Filter	Default: None, range: None/MAC/MAC + Data Type/MAC + Raw Data ➢ Disable: Duplicate data filter is disabled. ➢ MAC: Judge whether the data is duplicate according to the MAC address ➢ MAC+ Data Type: Judge whether the data is duplicate according to the MAC address and the data type. ➢ Mac+ Raw Data: Judge whether the data is duplicate according
Data upload interval	gateway upload data with the setting interval, if the interval is 0, means real-time scan and immediate report. Default: 0, range: 1-86400 (Unit: second)

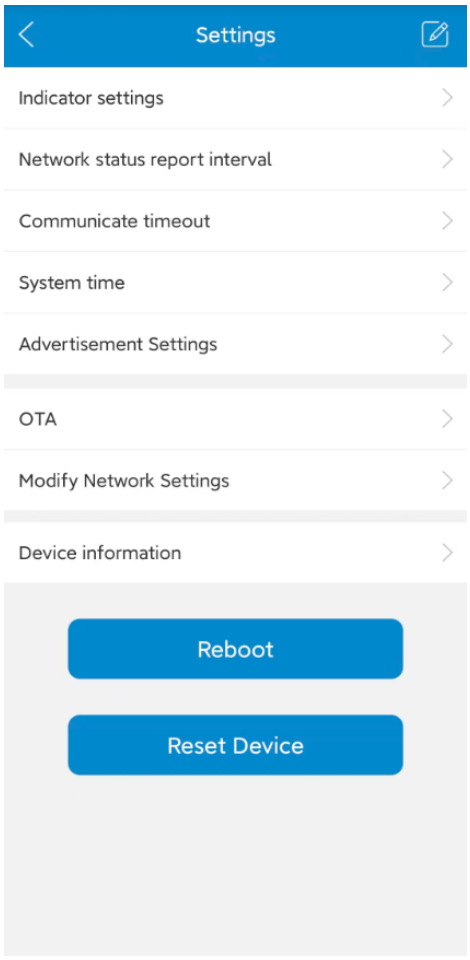
6.5.7 Upload Data Option

To determine the payload content uploaded to server. The Bluetooth data packet uploaded to the server includes timestamp, MAC, RSSI, raw data. The timestamp and raw data are optional.



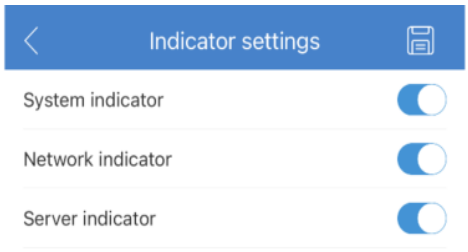
6.6 Gateway parameter settings

The gateway allows users to change its parameters. All parameters in the settings page can be modified.



6.6.1 Indicator settings

The LED indicator function in different device status can be configured.



Parameter	Description
System indicator	Default is enabled, when it is disabled, the LED will be OFF
Network indicator	Default is enabled, when it is disabled, the LED will be OFF
Server indicator	Default is enabled, when it is disabled, the LED will be OFF

6.6.2 Network Status Report Period

The gateway reports its network status to the server to notify the server that it is online. The report interval can be configured.

Parameter	Description
Network status report period	Default: 30, range: 0 or 10-86400 (unit: second) Value 0 means that the gateway will report the network status only once when it successfully connects to the server, will not report it later.

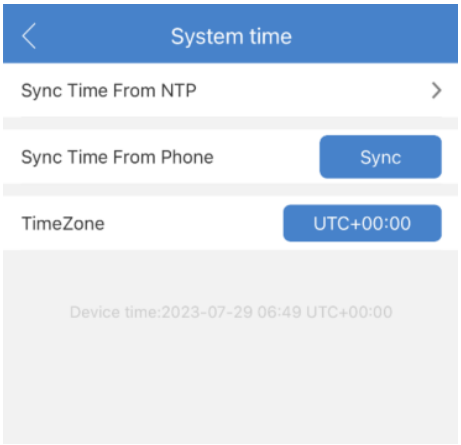
6.6.3 Communication timeout

If the gateway doesn't get any downlink message from the cloud in the timeout, it will automatically disconnect from the beacon.

Parameter	Description
Communicate timeout	Default: 10, range: 0-60 (unit: minute) Value 0 means no automatic disconnection

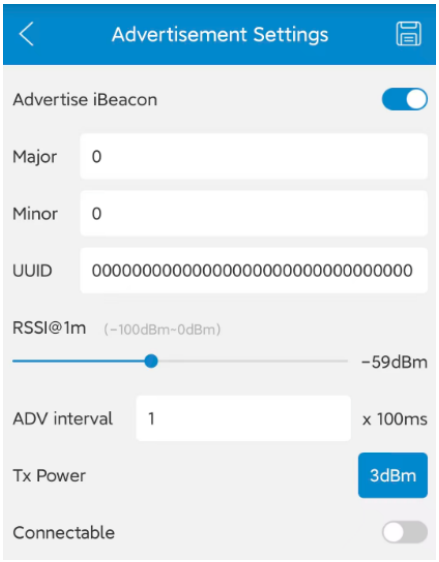
6.6.4 System Time

After the gateway connected with the server, it will synchronize time from the NTP server every 1 hour. If the NTP server is invalid, it also supports to synchronize time from user's phone.
The "Sync" button is used to require the UTC time from your phone, it also needs to select the TimeZone to obtain the local current time.



6.6.7 Advertise iBeacon

To set the gateway advertise iBeacon data.



Parameter	Description
Advertise iBeacon	On/off
Major	0-65535
Minor	0-65535
UUID	16 bytes
RSSI@1m	Range: -100~0, unit: dBm
ADV interval	Range: 1-100, unit: 100ms
Tx power	-24dBm~21dBm, step by 3 dBm.
Connectable	On/off

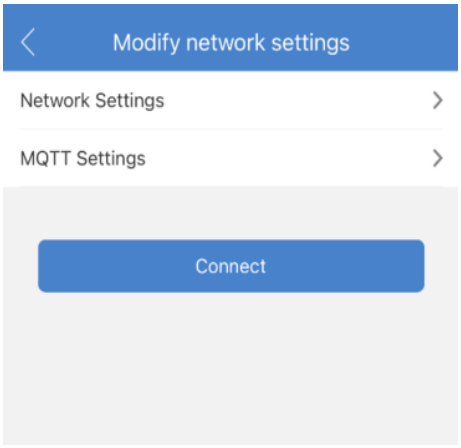
6.7 OTA

The gateway has an ability to update firmware over the air. When MOKO releases a new firmware, you can easily upgrade your gateway firmware by loading an upgrade Bin file with MOKO APP.
The firmware file URL will be like: http://47.104.172.169:8080/updata_fold/MKGW3_V1.0.4.bin

During upgrade process, LED will flash yellow, if upgrade succeed, LED turns solid yellow, if failed, LED turns solid red.

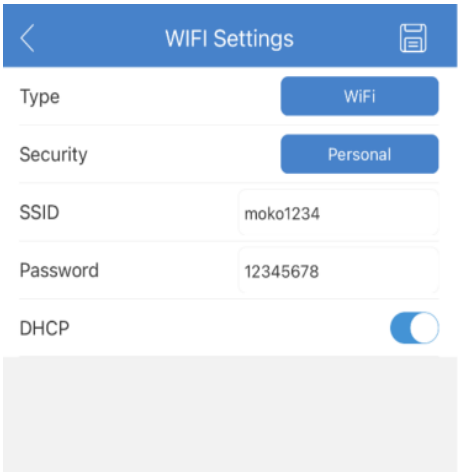
6.8 Modify Network settings

Change the WiFi, MQTT and network settings for the gateway, it allows users to change the settings independently. After the WIFI, MQTT or network settings are changed, click the “Connect” button, the gateway will reboot once and reconnect using the new settings.



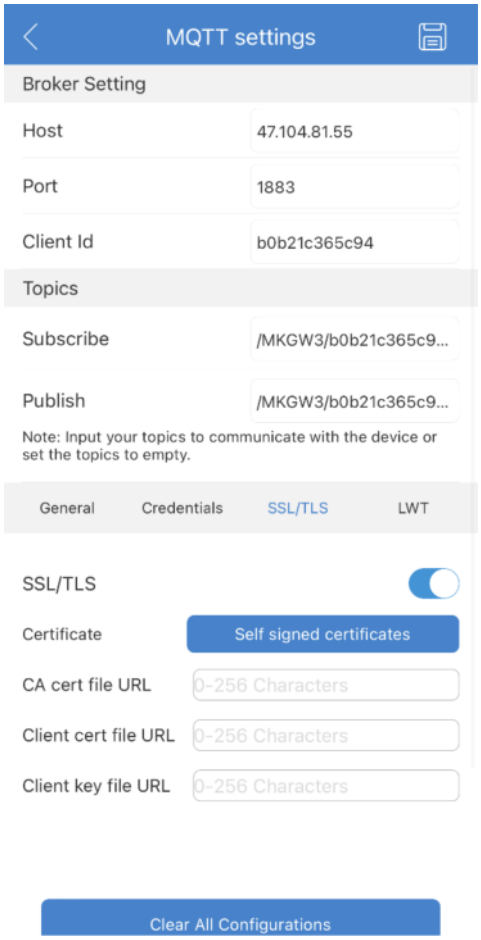
6.8.1 Modify Network settings

To change the WIFI settings for the gateway. If we change security from personal to Enterprise, it requires to upload WIFI certificates, the certificates will be obtained from your HTTP server.
The CA cert file URL will be like: http://47.104.172.169:8080/updata_fold/wifi_ca.pem



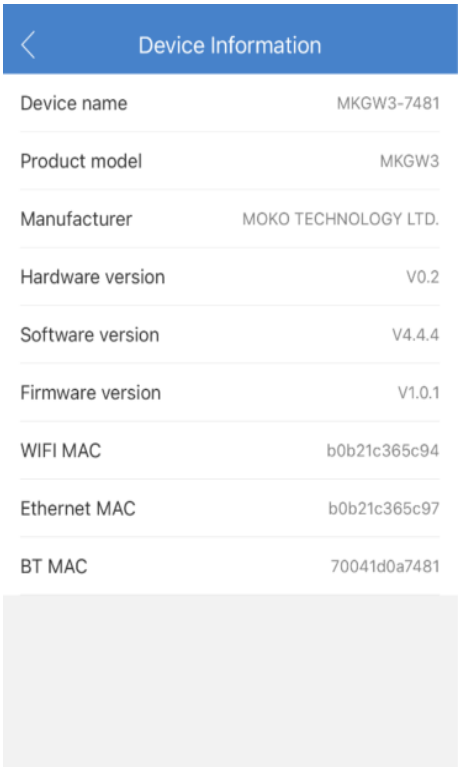
6.8.2 Modify MQTT settings

To change the MQTT settings for the gateway. If the new server requires SSL certificates, the certificates will be obtained from your HTTP server.
The certificates file URL will be like: http://47.104.172.169:8080/updata_fold/aws_ca.pem



6.9 Device Information

You can get the device information in this page.



6.10 Reboot

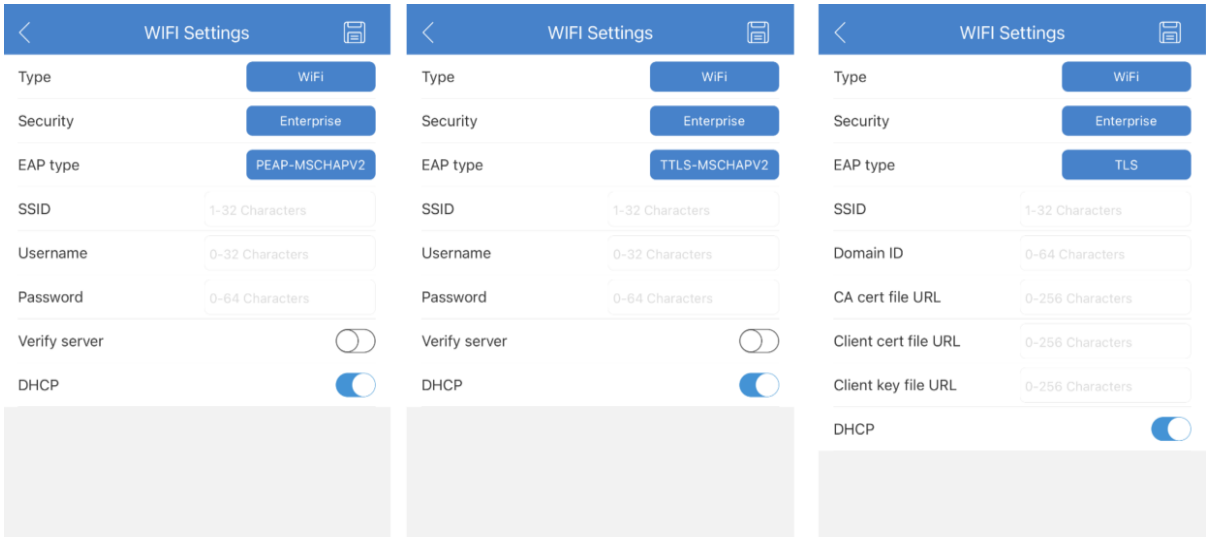
The “Reboot” button is used to send a reboot command to the device. After that, the gateway will reboot once.

6.11 Reset Device

The “Reset Device” button is used to send a reset command to the device. After that, the device will restore to factory settings, and the indicator will flash blue and green once.
You can also press and hold the reset button for 5 seconds to reset it.

Appendix A: WPA2 Enterprise Security

Go to network settings, select WIFI and Enterprise, then select EAP type and enter the correct settings.



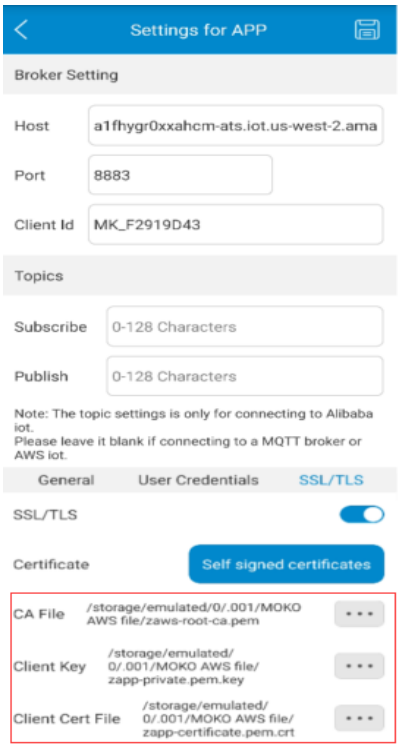
- PEAP-MSHCHAPV2: The user should enter the WIFI SSID, EAP username, EAP password. If verify server is enabled, it requires to upload the CA certificate from your phone.
- TTLS-MSHCHAPV2: The settings are the same as PEAP-MSHCHAPV2
- TTLS: The user should enter the WIFI SSID, domain ID, and upload certificates. The CA certificate is must-required, the client certificate and client key are optional.

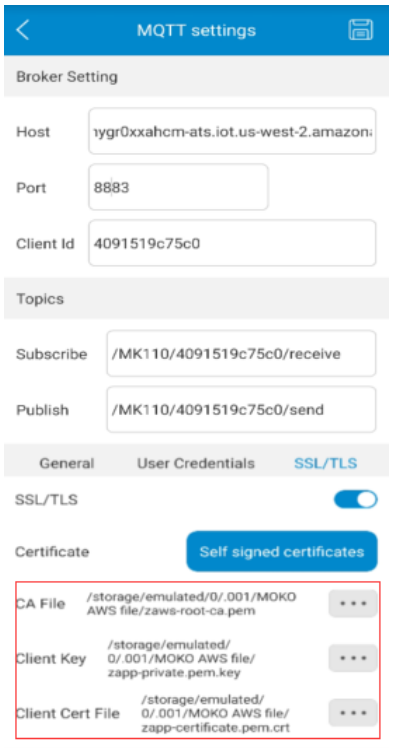
Appendix B: Connect to AWS IoT

Go to Settings for APP page, firstly users should configure the APP connecting to AWS IoT. Then go to settings for device- > MQTT settings, configure the gateway connecting to AWS IoT.

The host is AWS host URL, port is 8883, turn on the SSL/TLS, select CA self signed certificates as the certificate type, then upload the CA certificate, client key and client cert file from your phone.

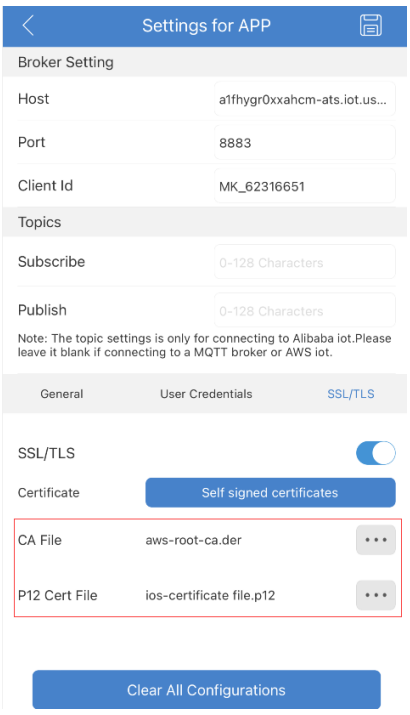
If using Android phone, the certificate files must be saved in the root directory of the local storage, otherwise the APP cannot obtain the files correctly.

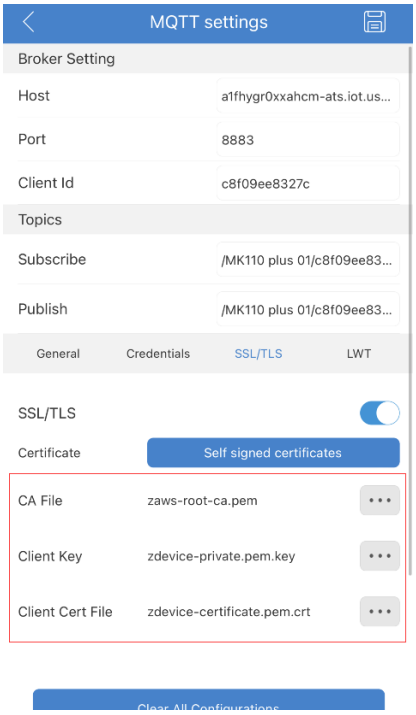




If using IOS phone, users need convert AWS certificates to required format, and import the certificates into your iOS phones through iTunes, then users can upload certificates from their phones.

Please note that only the APP settings require the converted certificate, while the device settings still use the CA root certificate, private key and client certificate original files.





Revision History

Revision	Description	Editor	Date
V1.0	Initial version	Weiguifen	2023.9.11
V2.0	applicable for V2 version	Damon	2025.12.25

MOKO TECHNOLOGY LTD.

4F, Building2, Guanghui Technology Park,
MinQing Rd, Longhua, Shenzhen, Guangdong, China

Tel: 86-755-23573370-829

sales@mokosmart.com

https://www.mokosmart.com