
# MOKO MK110 Plus 03 BLE Gateway User Manual



Contents



MOKO

**MOKO MK110 Plus 03 BLE Gateway**

**Specifications**

- **Product Name:** MK110 Plus 03 BLE Gateway
- **Version:** V1.0
- **Functionality:** BLE to WiFi plug gateway with power metering
- **Features:** Collects Beacon advertising data, transfers data to cloud, remote control for on/off switching, power consumption monitoring

## Product Usage Instructions

**Install the Gateway**
Insert the gateway into a power socket. The LED will blink to indicate the status:

- If never configured, LED blinks Blue (pairing mode).
- If previously configured, LED blinks Green (reconnecting to the network).

**Configure Gateway with APP**
To configure the gateway:

1. Download the MKScannerPro app from the APP Store or Google Play.
2. When installing, allow location and storage permissions.
3. Configure the app to connect to MQTT broker.
4. Configure the gateway to connect to MQTT broker.

**Configure Mobile APP**
To configure the mobile app

1. Run the mobile app and select “Remote gateway with metering” for configuration.
2. Click to configure MQTT settings for the app. You can use default settings or customize as needed.
3. If connection is successful, the app will show success; if failed, check settings and try again.

**FAQ**

- **Q: How do I know if the gateway is in pairing mode?**
  - A: The LED will blink Blue when the gateway is in pairing mode.
- **Q: What permissions are required for the mobile app?**
  - A: The mobile app requires location and storage permissions for installation and configuration.

**MK110 Plus 03 BLE Gateway**

**User Manual**

**Version V1.0**

**About this document**
MK110 Plus 03 is a BLE to WiFi plug gateway with power metering. The gateway collects Beacon advertising data and transfers to cloud, at the same time, it is an intelligent and metering plug, it can be remotely controlled to switch on/off and monitor the power consumption of connected load, users can easily realize Beacon data collecting, intelligent control and power monitoring together by the one device.

This User Guide was designed to help users to know the MOKO MK110 Plus 03 gateway and set up the gateway with MOKO APP.

**LED status**

| Function | Action | LED Patterns |
|---|---|---|
| Bluetooth status (Pairing mode) | Bluetooth is advertising | Flash **Blue** |
| | Bluetooth is connected | Solid **Blue** |
| WIFI status | Connecting to the WIFI | Slowly flash **Green** (every 2s) |
| | Connecting to the server | Quickly flash **Green** (every 500ms) |
| | Connected to the server successfully | Solid **Green** |
| Downlink communication | Connected with Beacon | Solid **Purple** |
| Restore to factory settings | Press button for 10 seconds in 1 minute after powered, the gateway will be reset and enter pairing mode. | Alternately flash **Blue** and **Green** once |
| OTA status | OTA process | Flash **Yellow** |
| | OTA succeed | Solid **Yellow** |
| | OTA failed | Solid **Red** |

## Install the Gateway

Insert the gateway into a power socket, the gateway will start work immediately, we can see the LED blinking.

If the gateway has been never configured, it will enter pairing mode, the LED will blink Blue. If the gateway has been configured before, it will try re-connecting to the network, the LED will blink Green.

## Configure gateway with APP

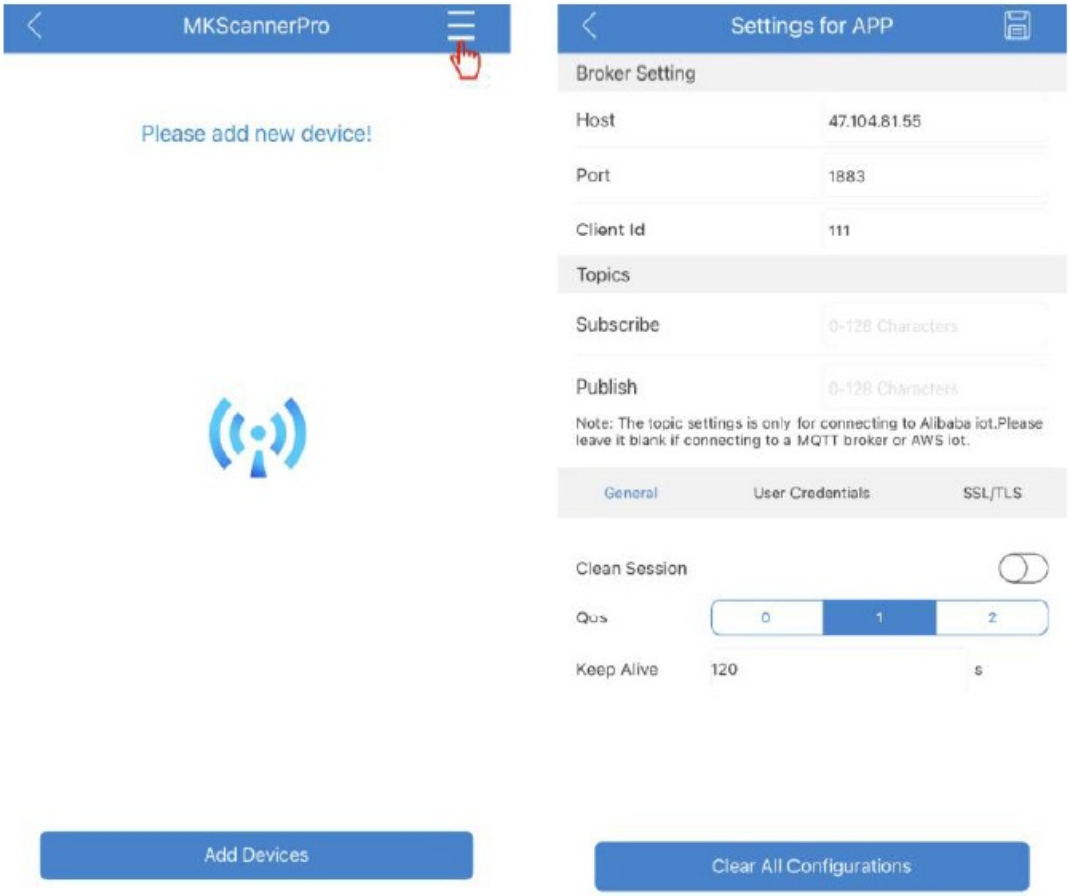
MOKO provides a demo APP with users to configure the gateway, please search “MKScannerPro” in APP Store or Google Play to download the APP. When install it, please allow the location and storage permissions.

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.

### Configure mobile APP

Run the mobile APP on your mobile phone, select “Remote gateway with metering” 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.

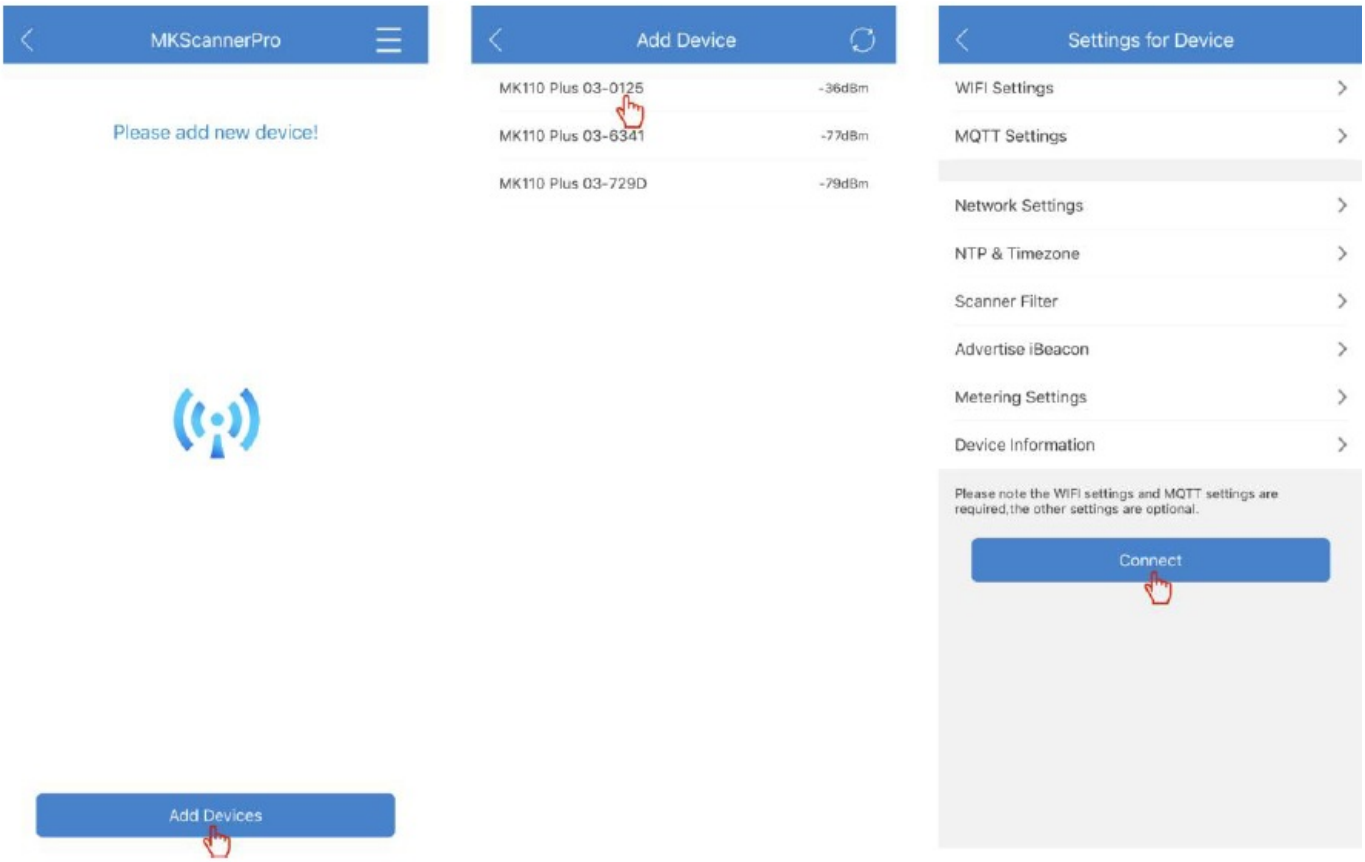
If configure with customer server, please follow these settings description as below

| 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. I f 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 |

**Configure gateway**
When the gateway LED flashes Blue, click “Add Devices” . We can see some advertisers named “MK110 Plus 03-XXXX”, select the correct device and enter password Moko4321. After APP connects with the gateway Bluetooth, the 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 the WiFi 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.

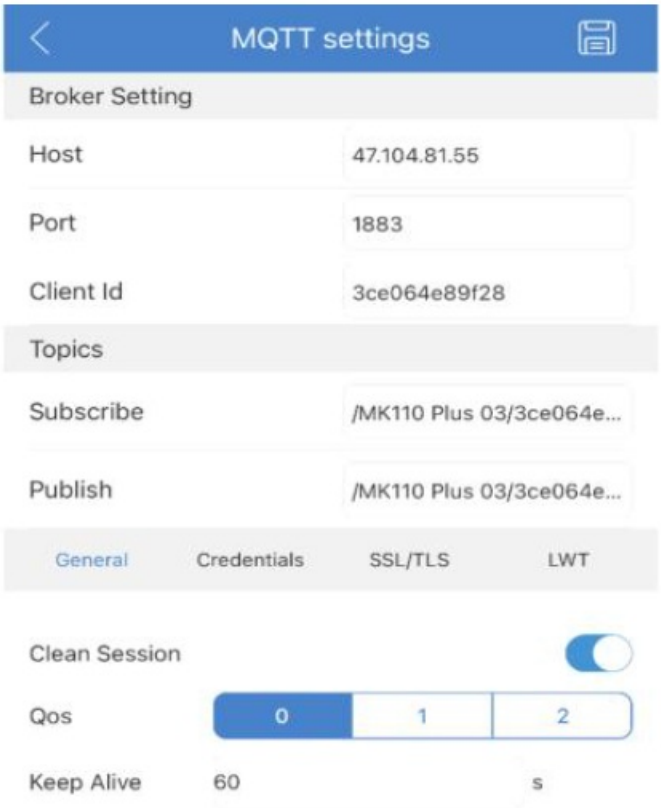
**WiFi settings**

- To configure network type and IP for the gateway.
- The gateway supports both personal and Enterprise WiFi security. 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.
- If connect to a 5GHZ WIFI, the country&Band is required to select.


**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.

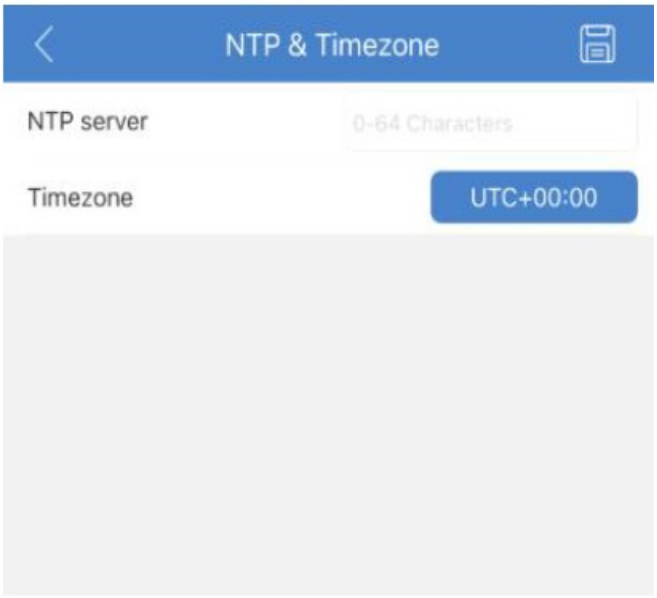
In the very bottom of this page, there are also three buttons used to help users quickly complete the configuration.



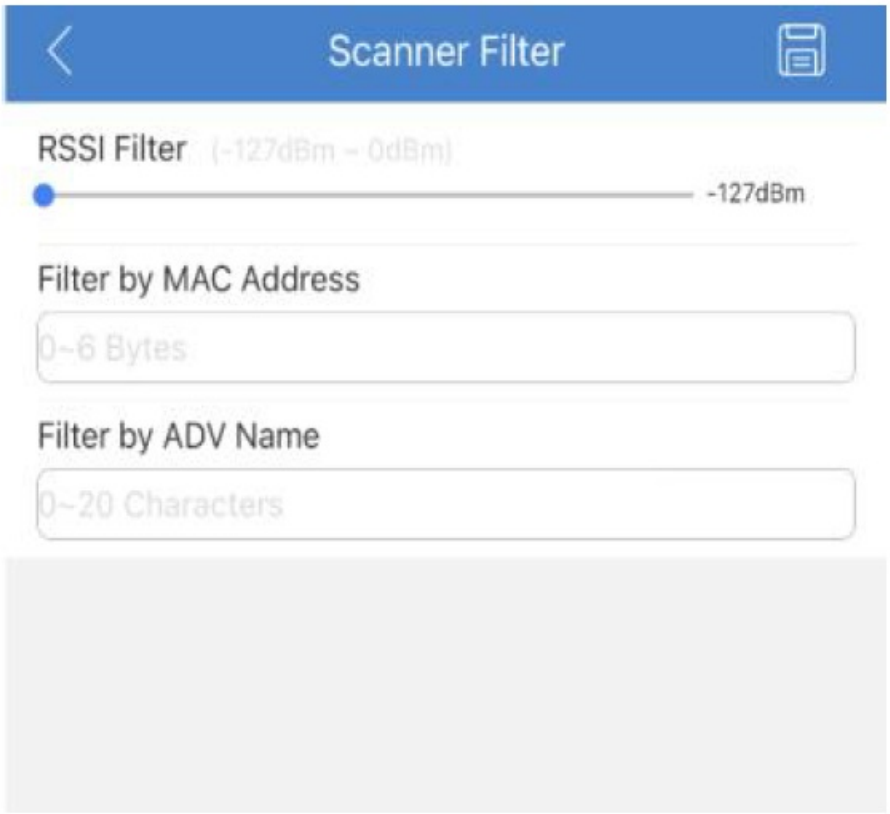

If connecting with customer server, please follow the below descriptions to finish the configuration

| 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 signe d 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 |

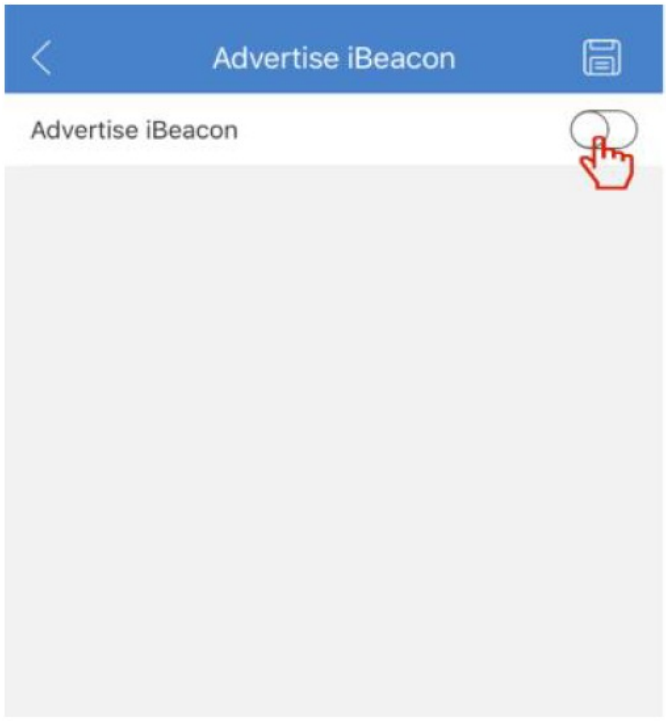
**NTP&Timezone**
To configure the NTP server and time zone for the gateway.

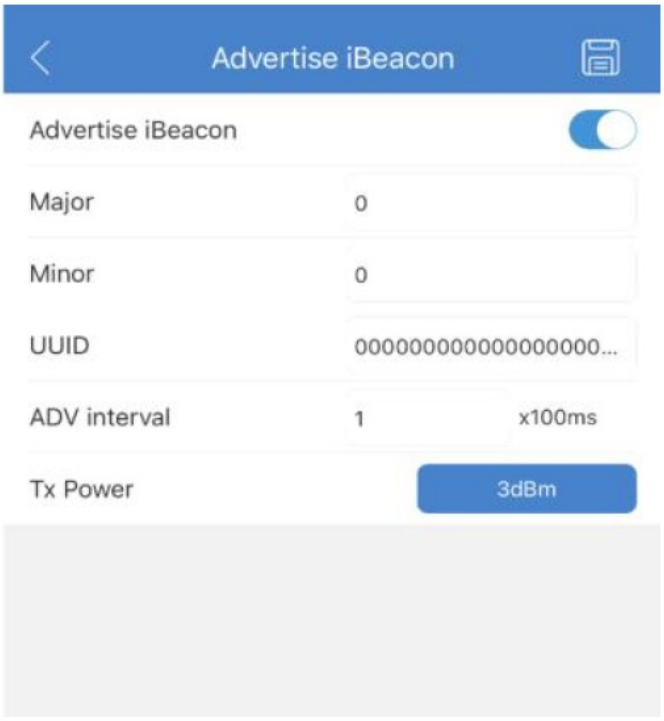



**Scanner filters**
To configure the scanner filter for the gateway. It supports filter by RSSI, MAC and advertising name.



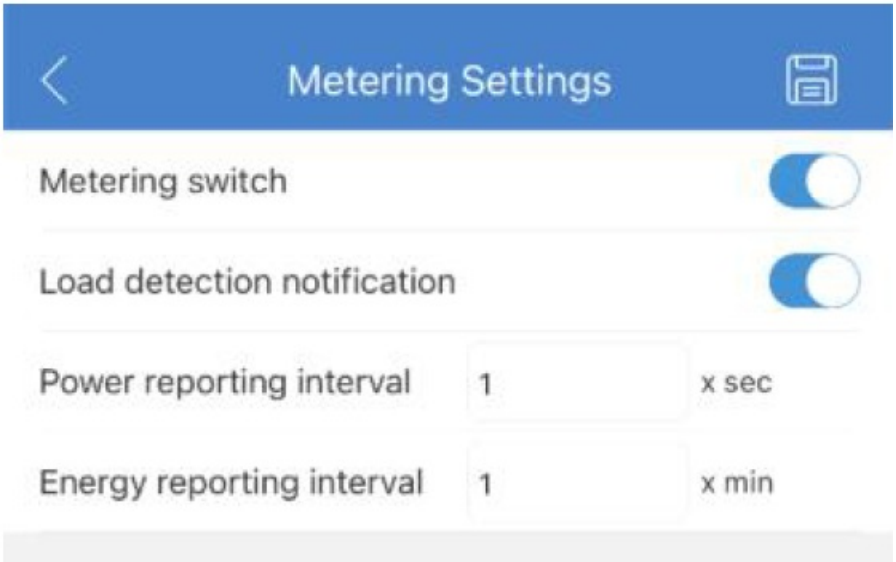

**Advertise iBeacon**
To set the gateway advertise iBeacon and setup advertising parameters. By default, iBeacon advertisement is turned off. if it is turned to on, the gateway will advertise iBeacon frame after it connects to server.




**Metering settings**
To configure the power metering parameters.

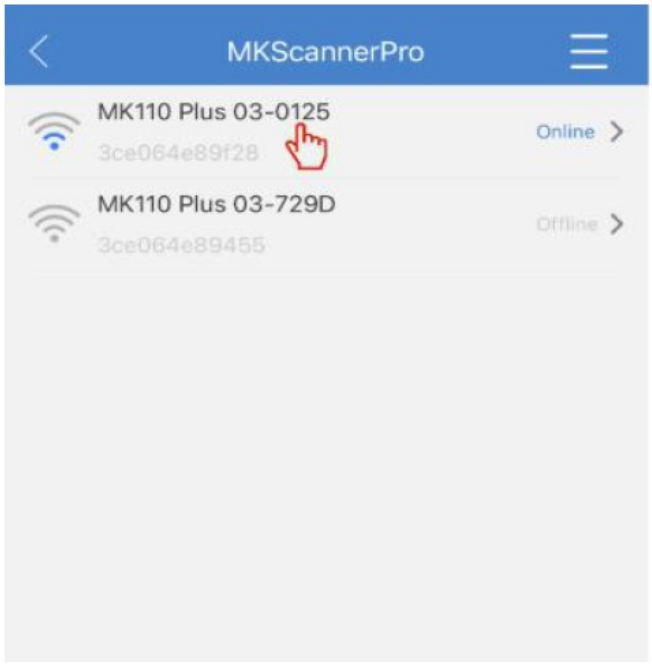
- **Metering switch**: if it is on, the gateway will periodically report power and energy data after it connects to cloud. If it if off, the data reporting will be off.
- **Load detection notification**: if it is on, when the gateway detects the electrical load is removed or inserted, it will report a notification to cloud. If it is off, the reporting will be off.
- **Power reporting interval**: to determine the reporting interval of current, voltage and active power data. Range: 1-86400, unit: second
- **Energy reporting interval:** to determine the reporting interval of active energy. Range: 1-60, unit: minute

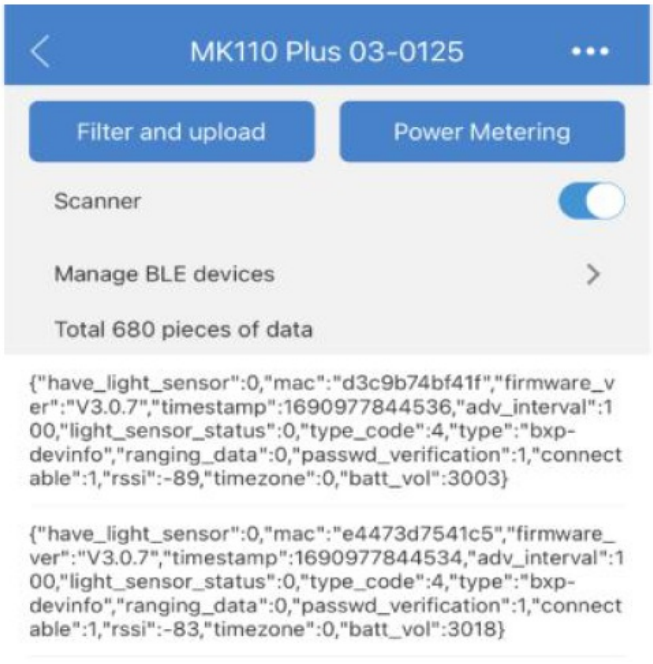


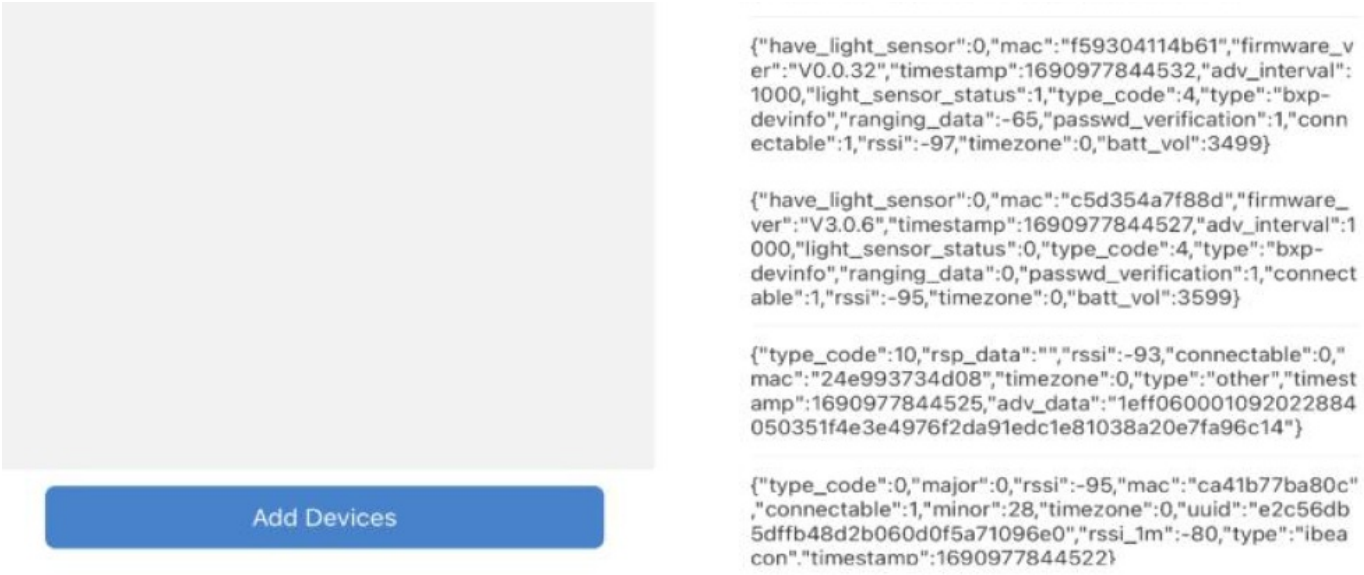

**Device information**
To read the device information of the gateway.


**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.



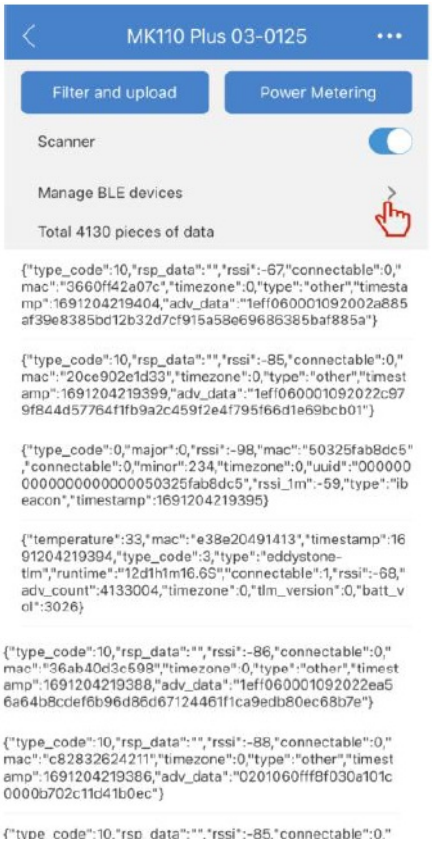


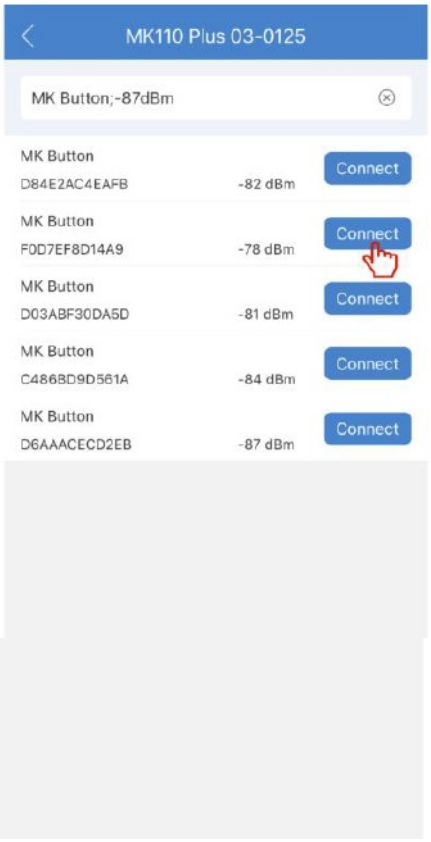

| Icon | Network status | RSSI |
|---|---|---|
| | OFFLINE | / |
| | POOR WiFi | <-65 dBm |
| | MEDIUM WiFi | -65~-50 dBm |
| | GOOD WiFi | >-50 dBm |

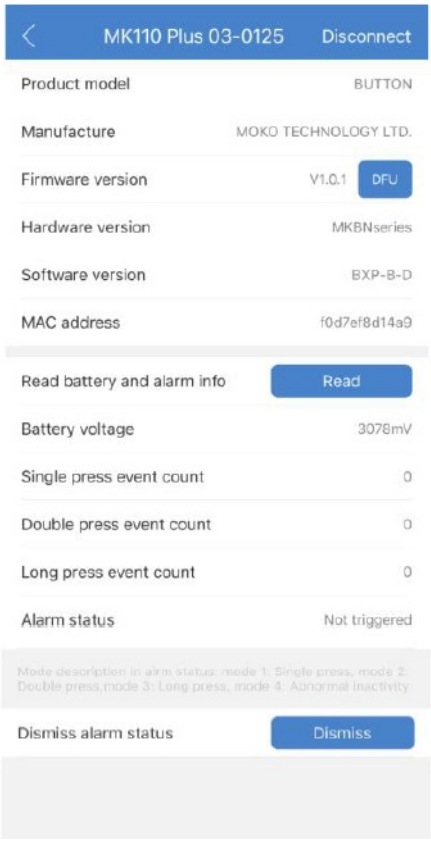
**Manage BLE devices**

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

We can research a MK Button device for connection. After the gateway is connected with the Beacon, we can get the product information, battery and alarm information, and dismiss the alarm status. The “disconnect” button in the top used to disconnect from the beacon.

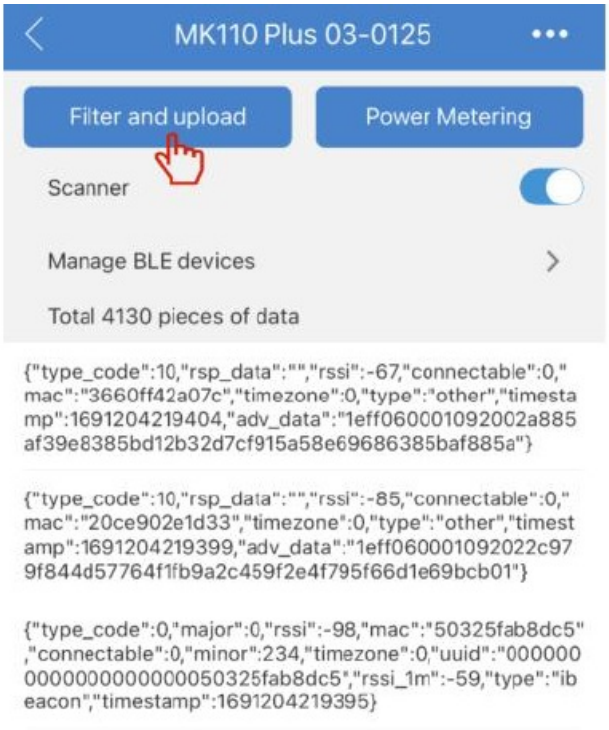


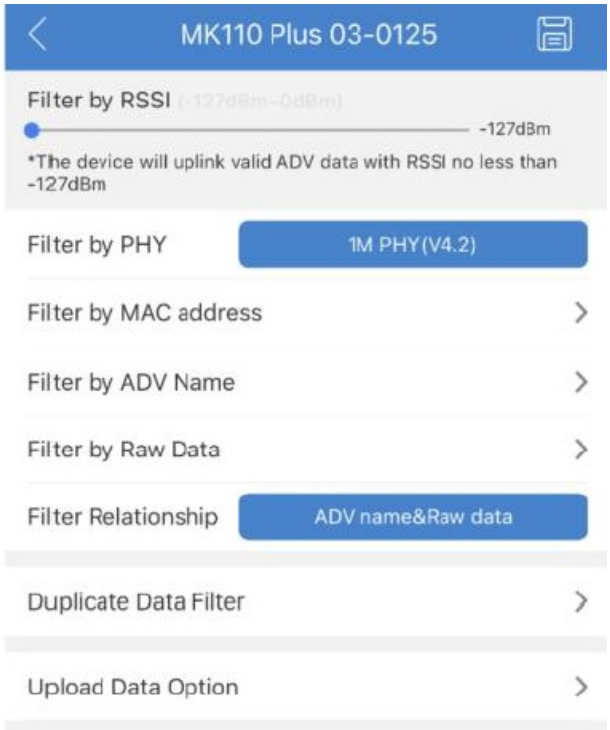




**Filter and upload**

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




**Filter By RSSI**
The gateway filters beacon data according to the RSSI, it will upload the beacon advertising data with RSSI no less than the setting value.

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

**Filter By PHY**
The gateway filters beacon data according to the PHY type.
The coded PHY (V5.0) enables BLE long range feature. At the same time, your beacon need advertise data with coded PHY, otherwise the beacon can’t be detected by the gateway.

| Parameter | Description |
|---|---|
| PHY | Default: 1M PHY (V4.2)<br>Range: 1M PHY (V4.2)/ 1M PHY (V5.0)/ 1M PHY (V4.2) & 1M PHY (V5.0)/ Coded PHY |

**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.<br>**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.<br>**ON:** Upload advertising data of Beacon whose MAC address doesn't conform the input expression. |

| | |
|---|---|
| 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.<br>Click the “ ” icon, it will delete the MAC address input box. |

**Filter by ADV Name**

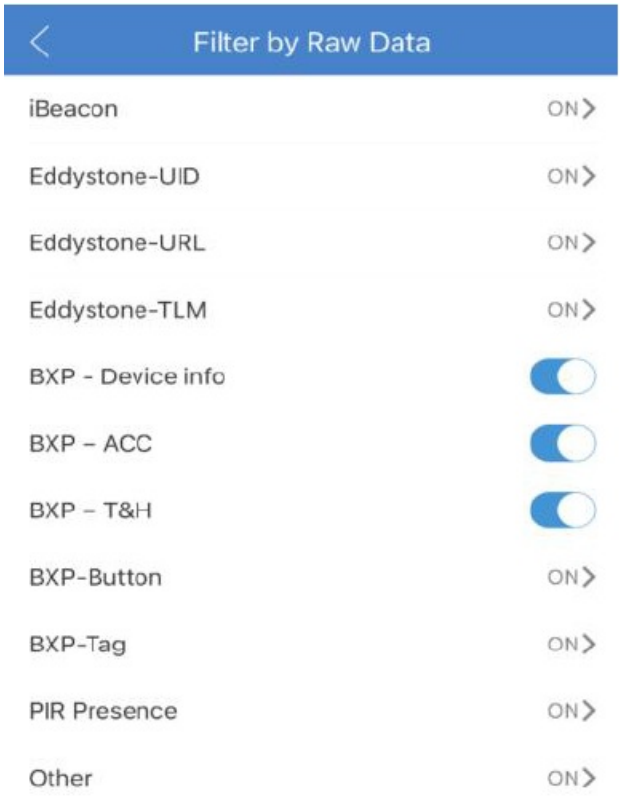
The gateway filters beacon data according to beacon advertising name, and it supports up to 10 set of advertising name at the same time.


| Parameter | Description |
|---|---|
| Precise match | **OFF:** Upload the advertising data of the beacon whose adv name contains the input expression.<br>**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.<br>**ON:** Upload advertising data of Beacon whose adv name doesn't conform the input expression. |
| ADV name | **OFF**: Upload the advertising data of the beacon whose adv name contains the input expression.<br>**ON:** Upload the advertising data of Beacon whose first N (N<=20) bytes of adv name is the same as the input expression. |

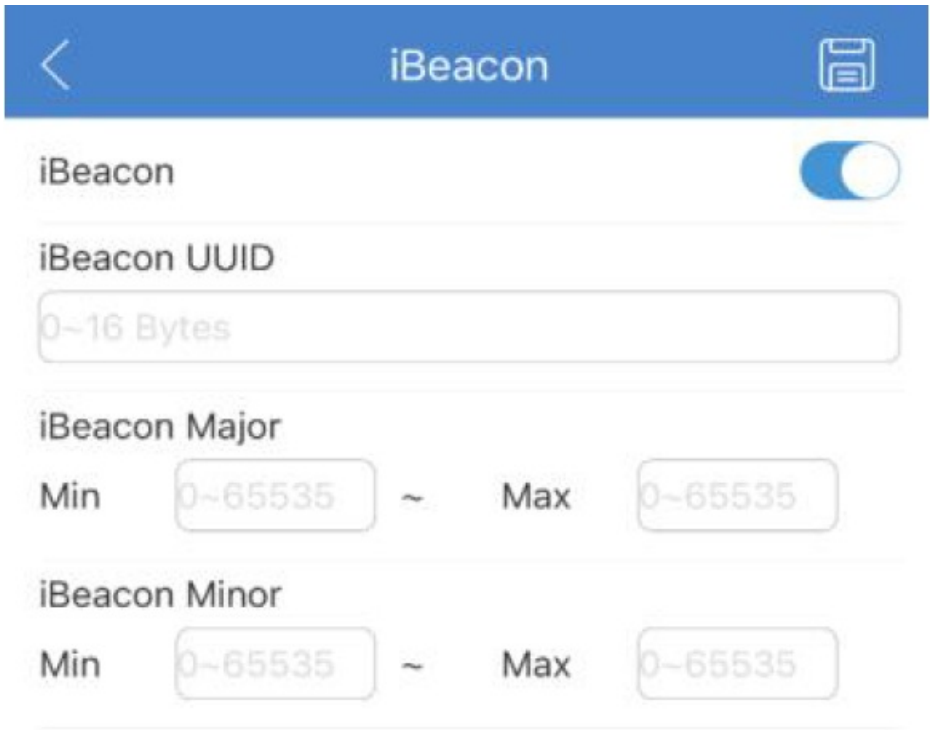
**Filter by Raw Data**

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.




**iBeacon**
To determine iBeacon frame is uploaded 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.

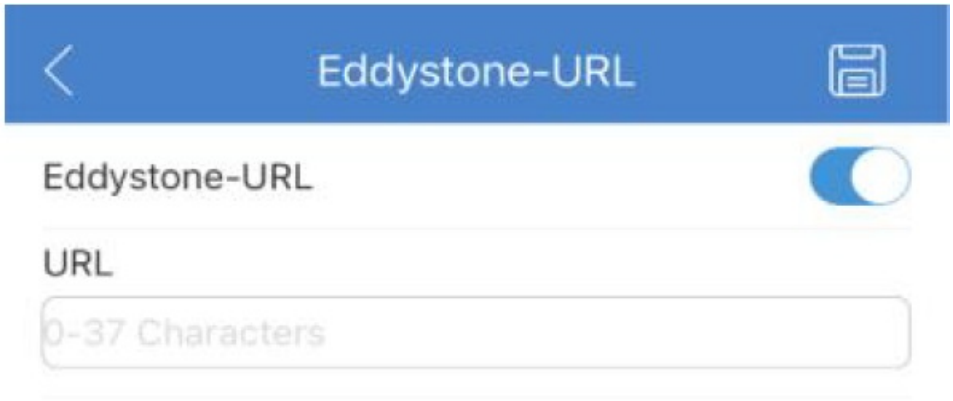


| Parameter | Description |
|---|---|
| Switch | **On**: upload, off: not upload |
| iBeacon UUID | 0-16 bytes iBeacon UUID with Hex format |
| iBeacon major | From 0 to 65535, the Max value must be no less than the Min value. |
| iBeacon minor | From 0 to 65535, the Max value must be no less than the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

**Eddy stone – UID**
To determine Eddystone-UID frame is uploaded or not.
If the Ecdysone-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.

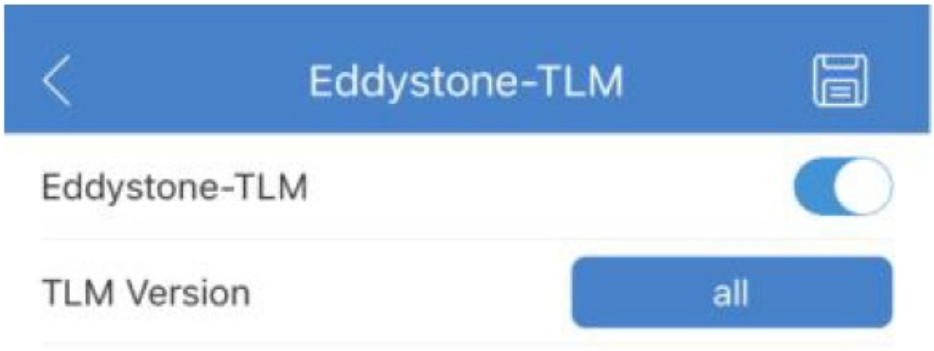

| Parameter | Description |
|---|---|
| Switch | **On**: upload, off: not upload |
| Namespace ID | 0-10 bytes Hex data |
| Instance ID | 0-6 bytes Hex data |

**Eddystone – URL**
To determine Eddystone-URL frame is uploaded 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** |

**Eddystone – TLM**
To determine Eddystone-TLM frame is uploaded 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<br>Ø **Null:** All versions will be uploaded;<br>Ø **Version 0**: Unencrypted TLM;<br>Ø **Version 1**: Encrypted TLM |

**BXP- Device info**
To determine MOKO BXP-Device info frame is uploaded or not.

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

**BXP- ACC**
To determine MOKO BXP-ACC frame is uploaded or not.

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

**BXP- T&H**
To determine MOKO BXP-T&H frame is uploaded or not.

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

**BXP- Button**
To determine MOKO BXP-Button frame is uploaded 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.

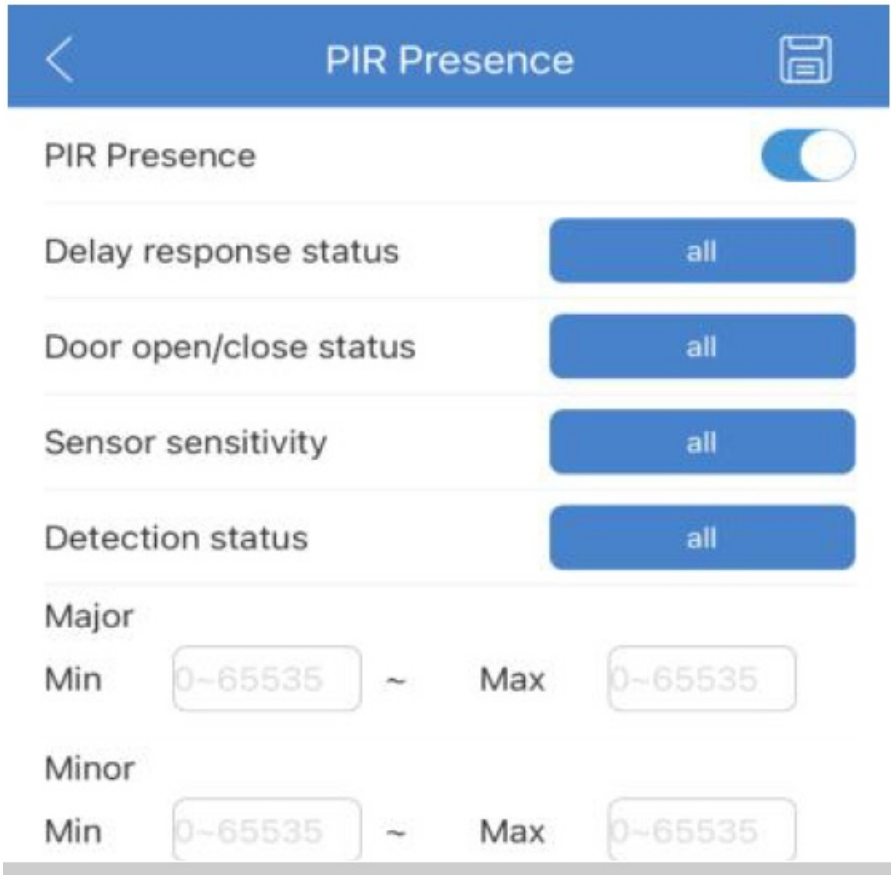

**BXP- Tag**
To determine MOKO BXP-Tag frame is uploaded or not. It supports filter the specified data by Tag ID, allows to set up to 10 sets of Tag id at the same time.


| Parameter | Description |
|---|---|
| Switch | **On**: upload, off: not upload |
| Precise match | **OFF:** Upload adverting data of Beacon whose tag id contains the input expression.<br>**ON**: Upload adverting data of Beacon whose first N (N<=3) 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.<br>**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.<br>Click the " " icon, it will delete the tag id input box. |

**PIR Presence**

To determine MOKO PIR Presence frame is uploaded or not.

It supports filter the specified data by sensor status and major, minor.



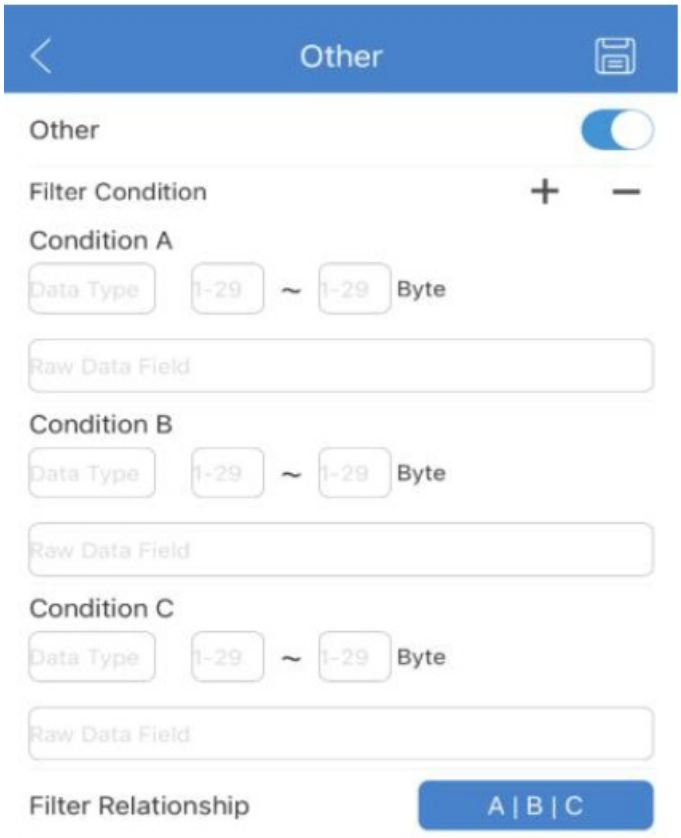

| Parameter | Description |
|---|---|
| Switch | **On:** upload, off: not upload |
| Delay response status | **Options**: All/low delay/ medium delay/high delay All: All delay status advertising data w ill be uploaded |
| Door open/close response status | **Options**: All/close/open<br>**All:** All door status advertising data will be uploaded |

| | |
|---|---|
| Sensor sensitivity | **Options**: All/low/medium/high<br>**All:** All sensor sensitivity advertising data will be uploaded |
| Detection status | **Options:** All/no motion detected/motion detected<br>**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. |

**Other**

The Beacon data other than the above 10 types will be judged as “other”. The gateway will transfer the other type data directly, without decoder.

To determine the other type is uploaded or not, the gateway can filter other type data by adv raw data.




| Parameter | Description |
|---|---|
| Switch | **On**: upload, off: not upload |
| Condition A | Ø **Data type: 1 byte Bluetooth data type**<br>Ø **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.<br>Ø **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. |

**Filter Relationship**

After the MAC filter, ADV name filter or raw data filter are set, it also needs to set the filter relationship, the relationship determines the processing logic.

If you set one or more filters, but relationship is set as “Null”, the filters will not take effect. The relationship should include the filters, then the filters will take affect.

| Parameter | Description |
|---|---|
| Relationship | **Default**: Null<br>**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. |

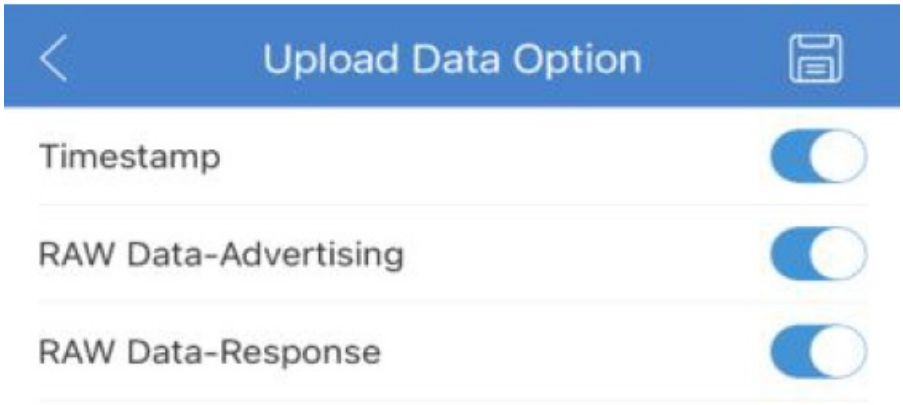
**Duplicate Data Filter**

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.


| Parameter | Description |
|---|---|
| Filter by | **Default:** None, range: None/MAC/MAC + Data Type/MAC + Raw Data<br>Ø **None**: Duplicate data filter is disabled.<br>Ø **MAC:** Judge whether the data is duplicate according to the MAC address<br>Ø **MAC+** Data Type: Judge whether the data is duplicate according to the MAC address and the data type.<br>Ø **Mac**+ Raw Data: Judge whether the data is duplicate according to the MAC addre ss and the raw data. |
| Filtering Period | Only when the filter is enabled, the filtering period can be set. Default: 10, range: 1-8 6400 (Unit: second) |

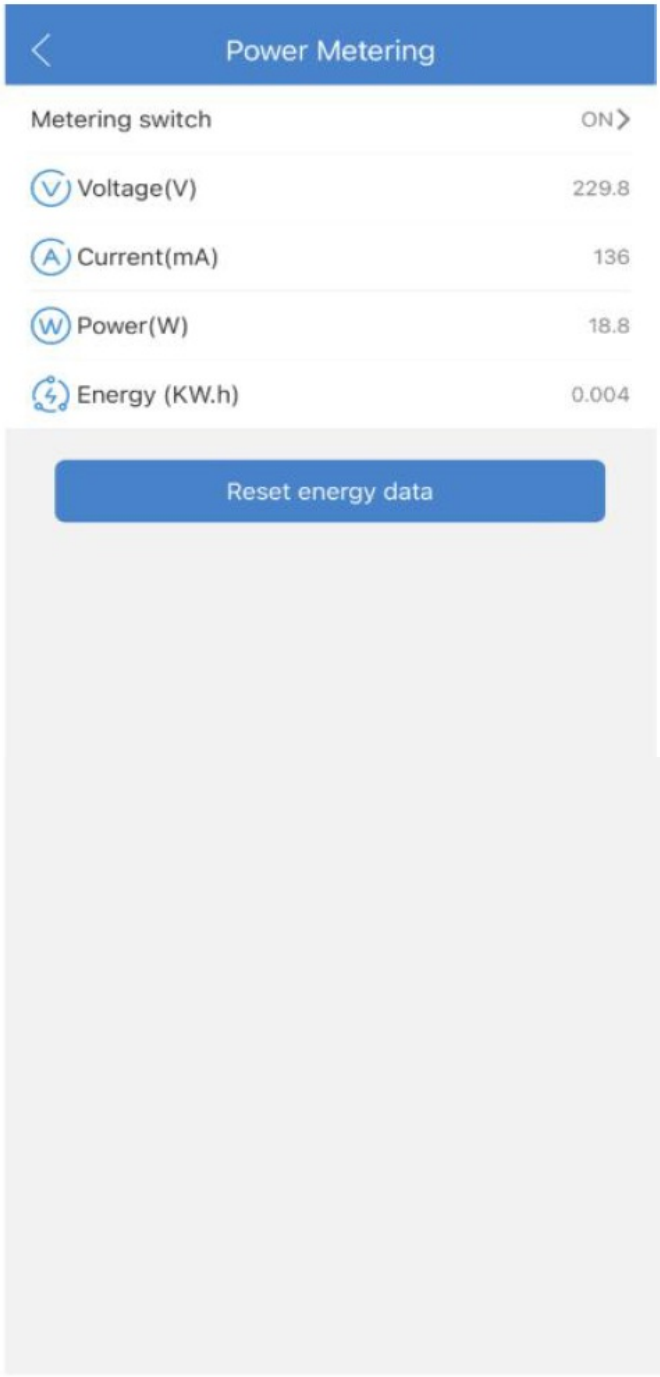
**Upload Data Option**

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



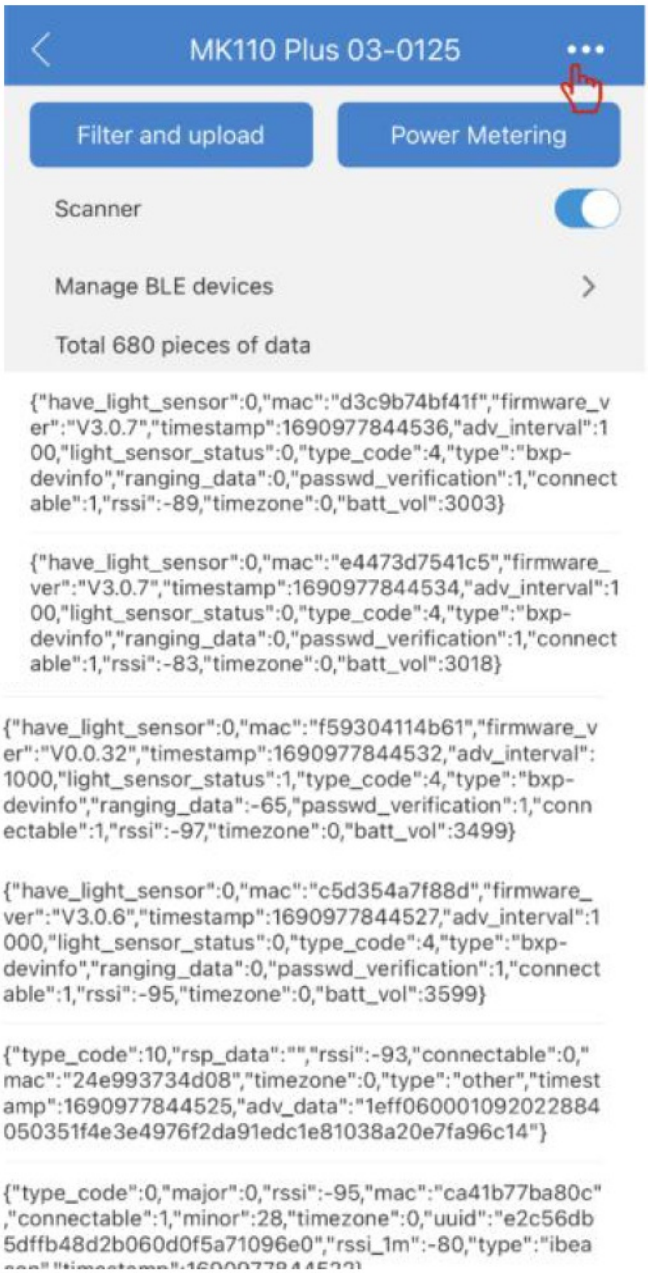

**Power metering**

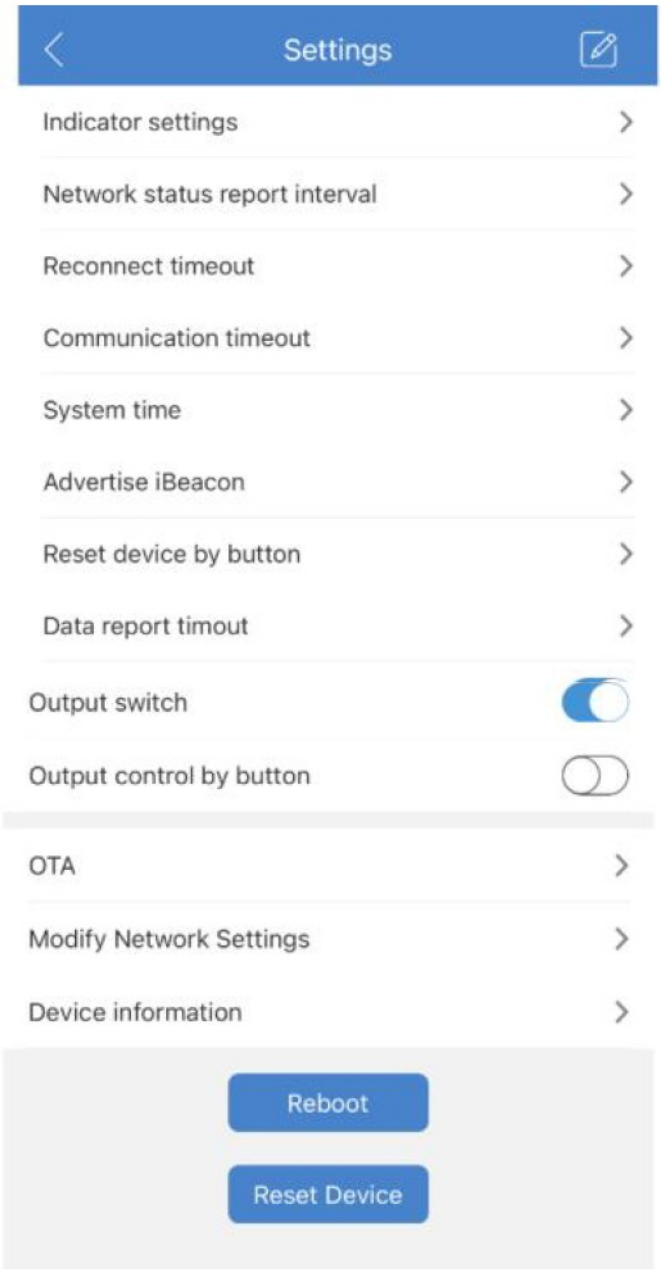
To enter the page where we can get set the metering parameters and get the power and energy consumption data. The metering switch is on, the gateway will periodically report the voltage, current, active power and energy data to cloud, we can set the reporting parameters. If the metering switch is off, the data reporting will be off.


**Gateway parameter settings**

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




**Indicator settings**

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

| Parameter | Description |
| --- | --- |
| Bluetooth advertising indicator | Default is enabled, when it is disabled, the LED will be OFF |
| Bluetooth connected indicator | Default is enabled, when it is disabled, the LED will be OFF |
| Server connecting indicator | Default is enabled, when it is disabled, the LED will be OFF |
| Server connected indicator | Default is enabled, when it is disabled, the LED will be OFF |

**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)<br>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. |

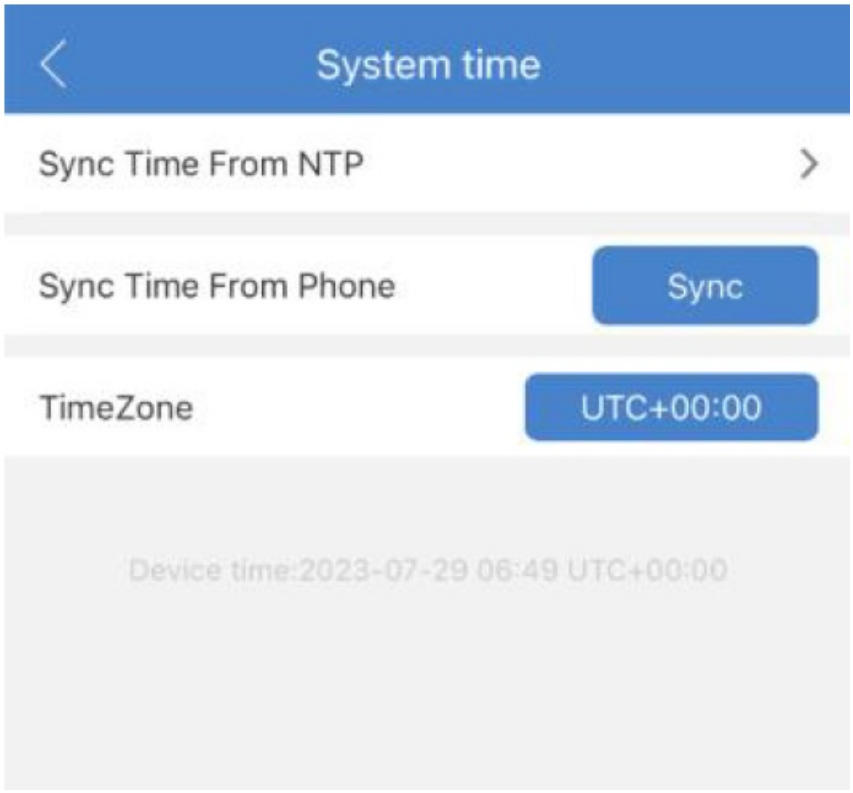
**Reconnect Timeout**
The gateway will automatically reboot once when it cannot connect to server in the configured timeout.

| Parameter | Description |
| --- | --- |
| Connect timeout | **Default:** 3, range: 0-1440 (unit: minute)<br>Value 0 means that the device will not reboot |

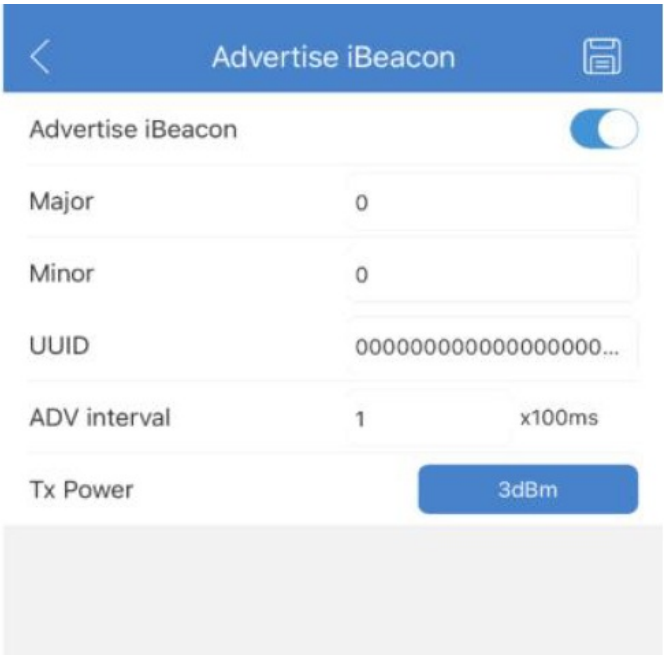
**Communication timeout**
If the gateway doesn't get any downlink message from the cloud in the timeout, it will automatically disconnect from the beacon.

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

**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 Time Zone to obtain the local current time.

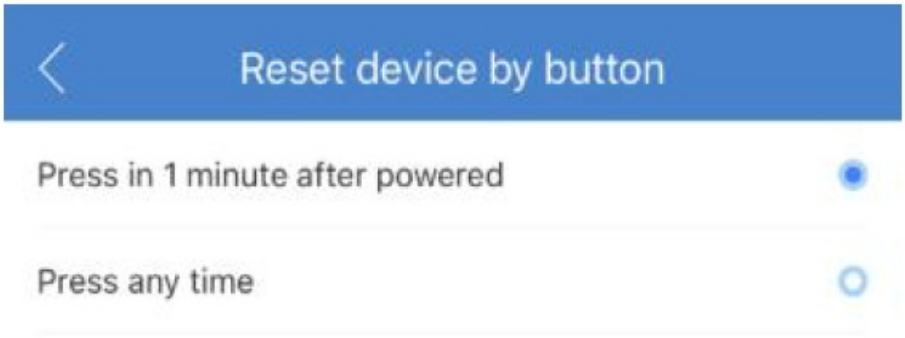



**Advertise iBeacon**
To set the gateway advertise iBeacon data.

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

**Reset device by button**
To determine the reset device mode triggered by the physical button.




**Output switch**
The gateway has an AC power output, to determine the output switch.

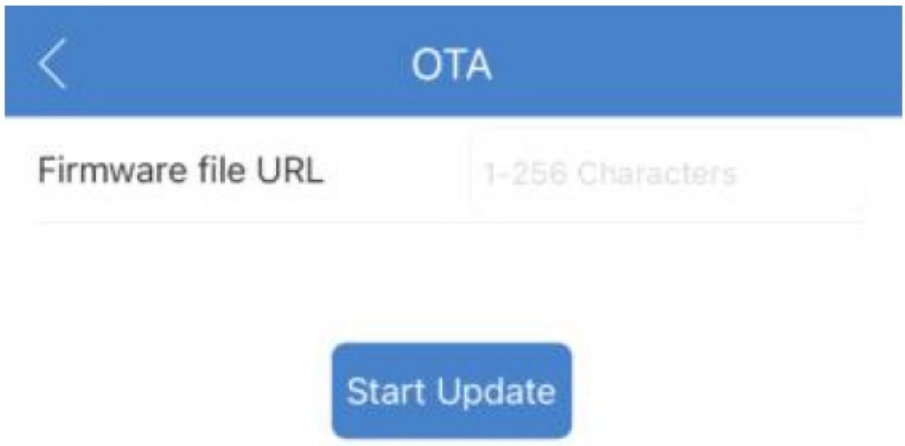
| Parameter | Description |
| --- | --- |
| Output switch | On: turn on the AC output Off: turn off the AC output |

**Output control by button**
To determine the AC output can be controlled by the physical button or not. By default, pressing the button will not switch output.

| Parameter | Description |
| --- | --- |
| Output control by button | **On:** Short click button will change the output switch Off: Short click butt on will not change the output switch |

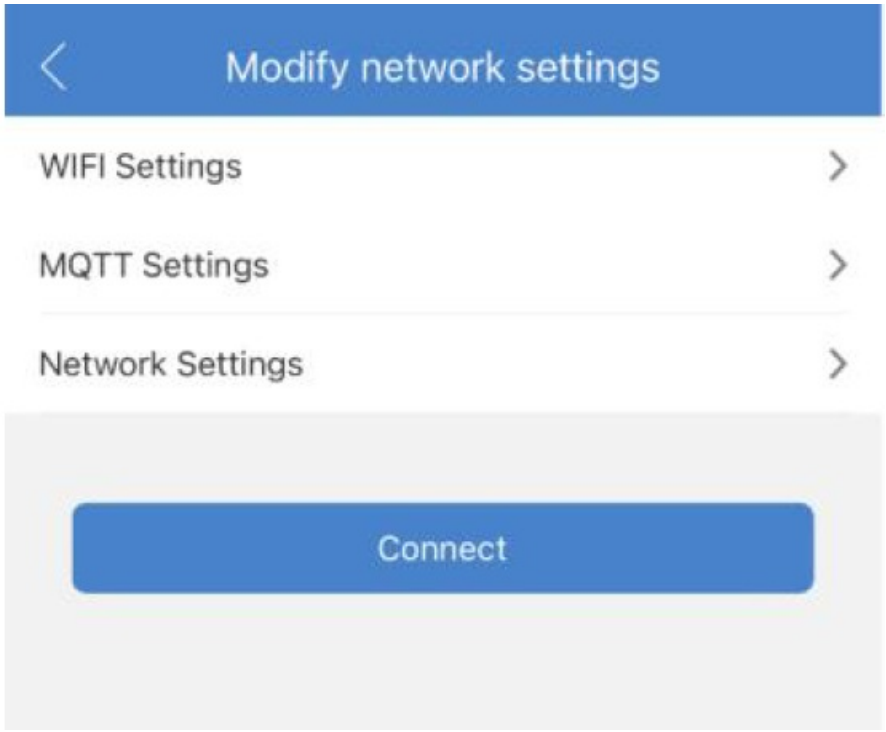
**OTA**
The gateway has an ability to update firmware over the air. When MOKO releases a new firmware, you can easily upgrade your gateway firmware by loading an upgrade Bin file with

**MOKO APP.** The firmware file URL will be like: http://47.104.172.169:8080/updata_fold/MK110_V1.0.4.bin
During upgrade process, LED will flash yellow, if upgrade succeed, LED turns solid yellow, if failed, LED turns solid red.



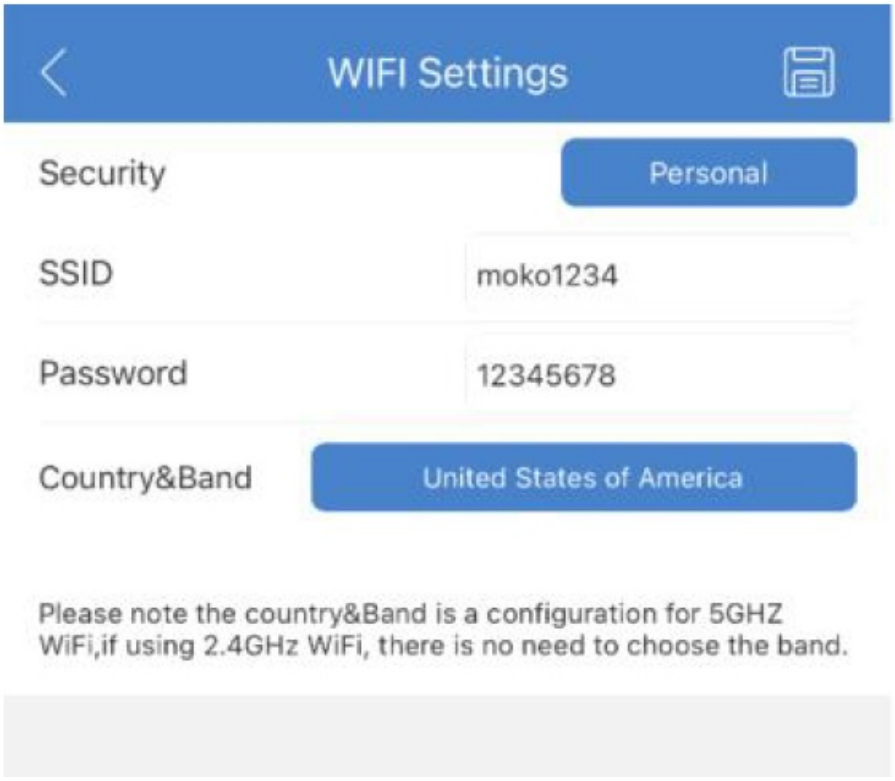

**Modify Network settings**

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.




**Modify WiFi settings**

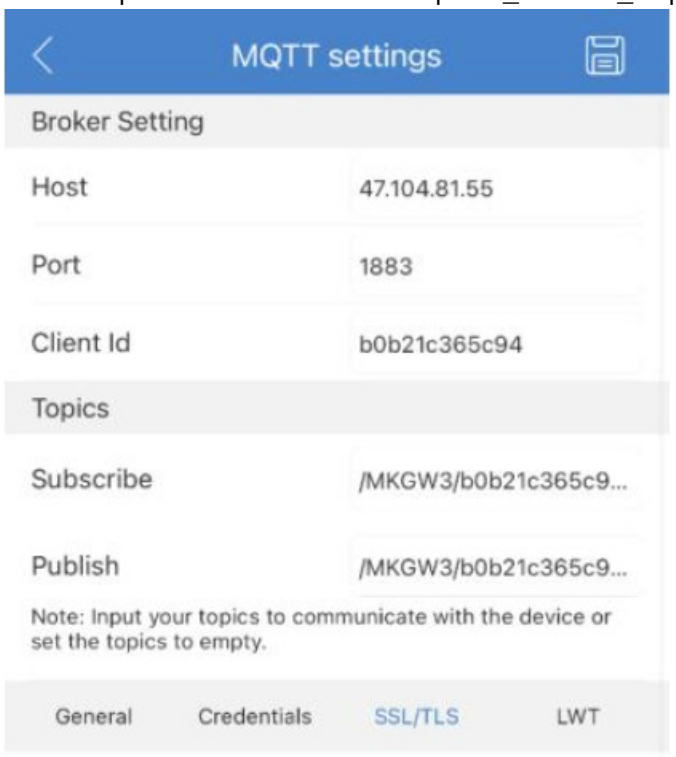
To change the WIFI settings for the gateway. If we change security from personal to Enterprise, it requires to upload WIFI certificates, the certificates will be obtained from your HTTP server. The CA cert file URL will be like: http://47.104.172.169:8080/updata_fold/wifi_ca.pem

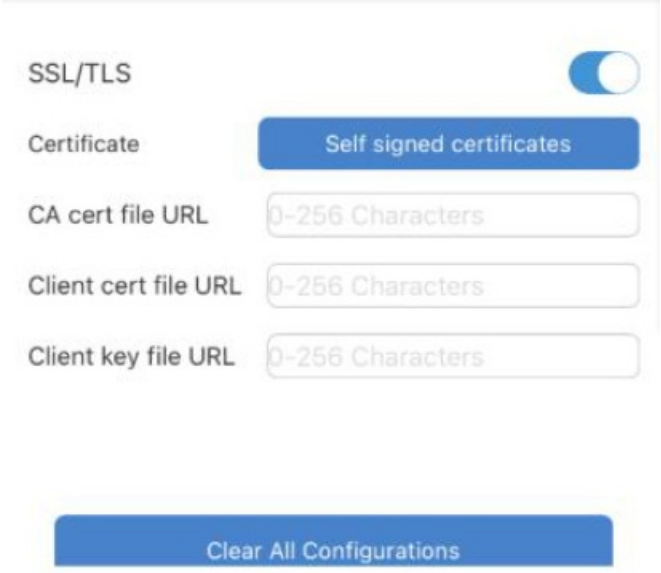



**Modify MQTT settings**

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





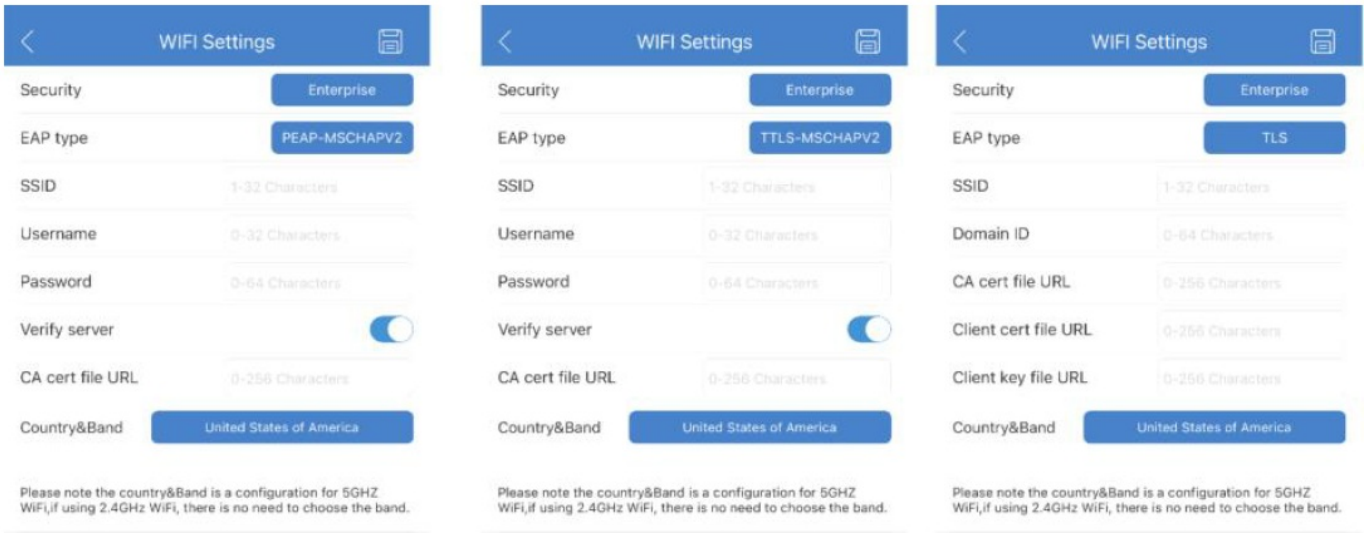

**Device Information**
You can get the device information in this page.


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

**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.
We can also press and hold the reset button for 10 seconds to reset it, please notice, with default settings, the reset will take effect only in 1minute after the gateway is powered up.

## Appendix A: WPA2 Enterprise Security

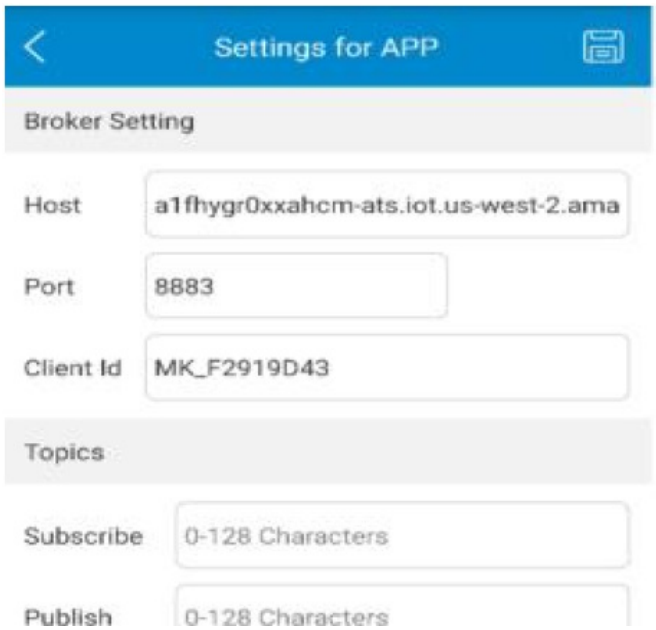
Go to WIFI settings, select Enterprise for security, then select EAP type and enter the correct settings.

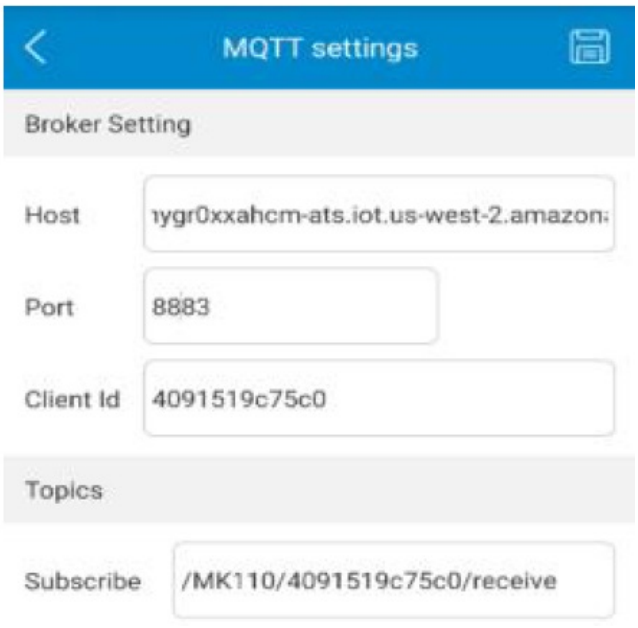


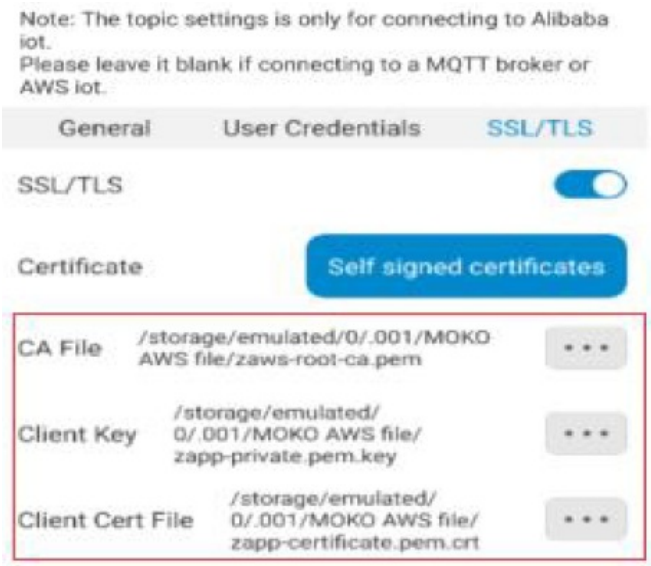

- **PEAP-MSHCHAPV2**: The user should enter the WIFI SSID, EAP username, EAP password. If verify server is enabled, it requires to upload the CA certificate from your phone.
- **TTLS-MSHCHAPV2:** The settings are the same as PEAP-MSHCHAPV2
- **TTLS:** The user should enter the WIFI SSID, domain ID, and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

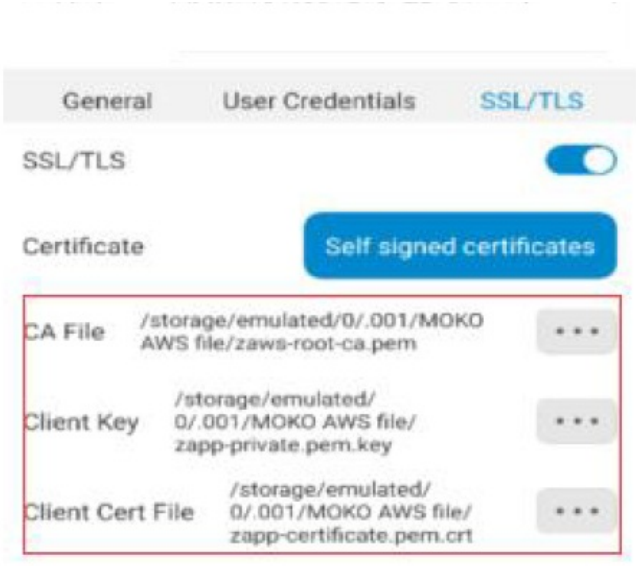
**Appendix B: Connect to AWS IoT**

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.



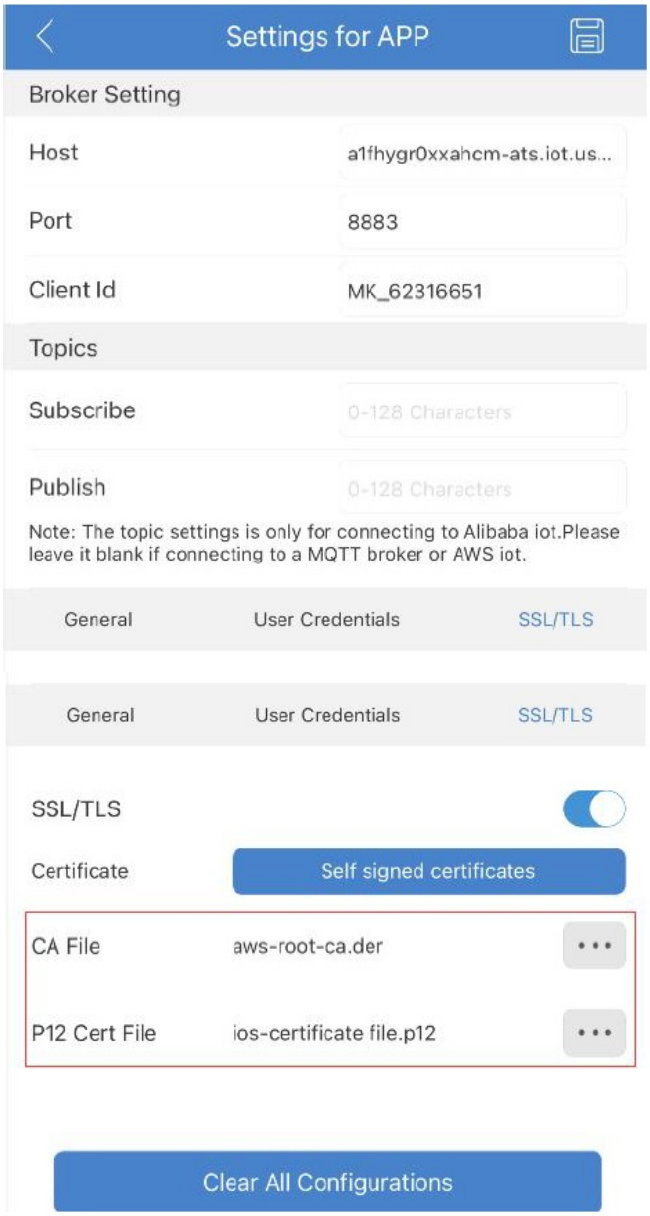



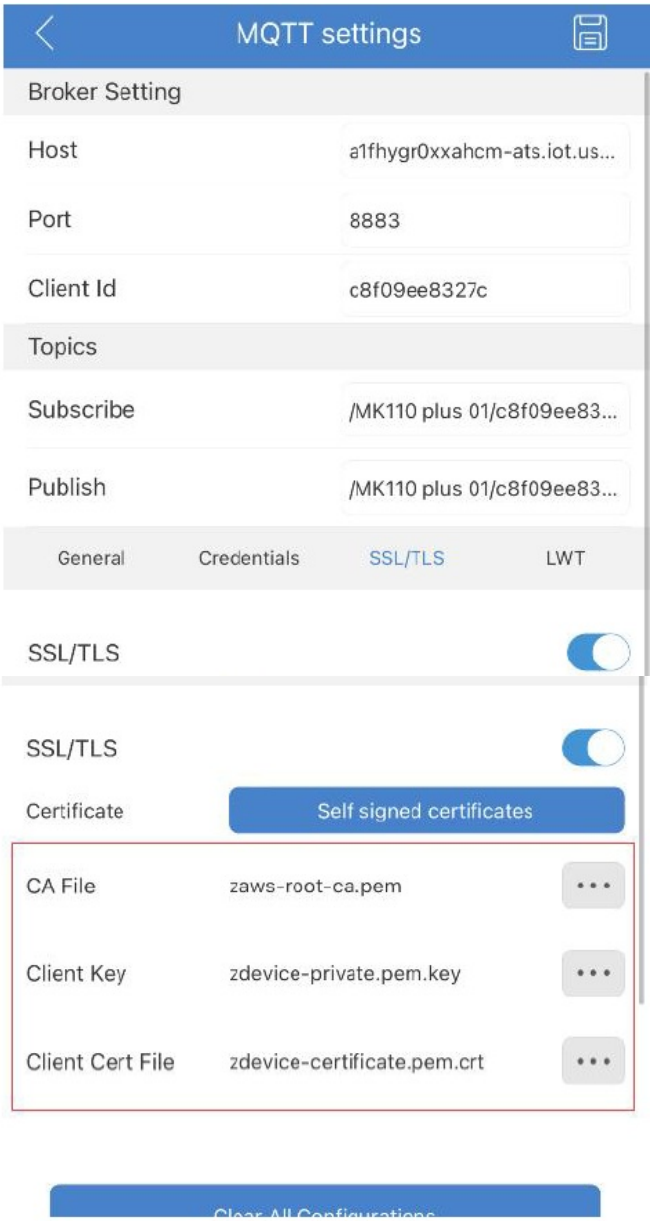



If using IOS phone, users need convert AWS certificates to required format, and import the certificates into your iOS phones through iTunes, then users can upload certificates from their phones.

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 | 2023.9.12 |

**MOKO TECHNOLOGY LTD.**

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

**Tel:** 86-755-23573370-829

sales@mokosmart.com

https://www.mokosmart.com

www.mokosmart.com

## FCC Warning

**Labeling requirements.**
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

**Information to user.**
Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**Information to the user.**
**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**FCC RF Radiation Exposure Statement**

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

**IC Warning**
This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions

1. This device may not cause interference;
2. This device must accept any interference, including interference that may cause undesired operation of the device.

The information listed above provides the user with information needed to make him or her aware of a RF exposure, and what to do to assure that this radio operates within the FCC exposure limits of this radio.

The device complies with RF specifications when the device used at 20cm from the body. Third-party belt-clips, holsters, and similar accessories used by this device should not contain any metallic components. Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided. Use only the supplied or an approved antenna.

The band 5150-5250MHz indoor use only.

## Documents / Resources

| | |
|---|---|
|   | MOKO MK110 Plus 03 BLE Gateway [pdf] User Manual<br>MK110 Plus, MK110 Plus 03 BLE Gateway, 03 BLE Gateway, BLE Gateway, Gateway |

## References

- Your IoT Devices ODM & JDM Partner - MOKOSmart #1 Smart Device Solution in China
- Your IoT Devices ODM & JDM Partner - MOKOSmart #1 Smart Device Solution in China
- User Manual