



MK110 Plus 03 BLE Gateway

User Manual

Version V1.0

Contents

1. About this document	1
2. LED status	1
3. Install the Gateway	1
4. Configure gateway with APP	2
4.1 Configure mobile APP	2
4.2 Configure gateway	4
4.3 Scan BLE devices	9
4.4 Manage BLE devices	9
4.5 Filter and upload	10
4.6 Power metering	20
4.7 Gateway parameter settings	21
4.8 OTA	24
4.9 Modify Network settings	25
4.10 Device Information	26
4.11 Reboot	27
4.12 Reset Device	27
Appendix A: WPA2 Enterprise Security	28
Appendix B: Connect to AWS IoT	28
Revision History	30

1. 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.

2. 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

3. 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**.





4. 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.

4.1 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:

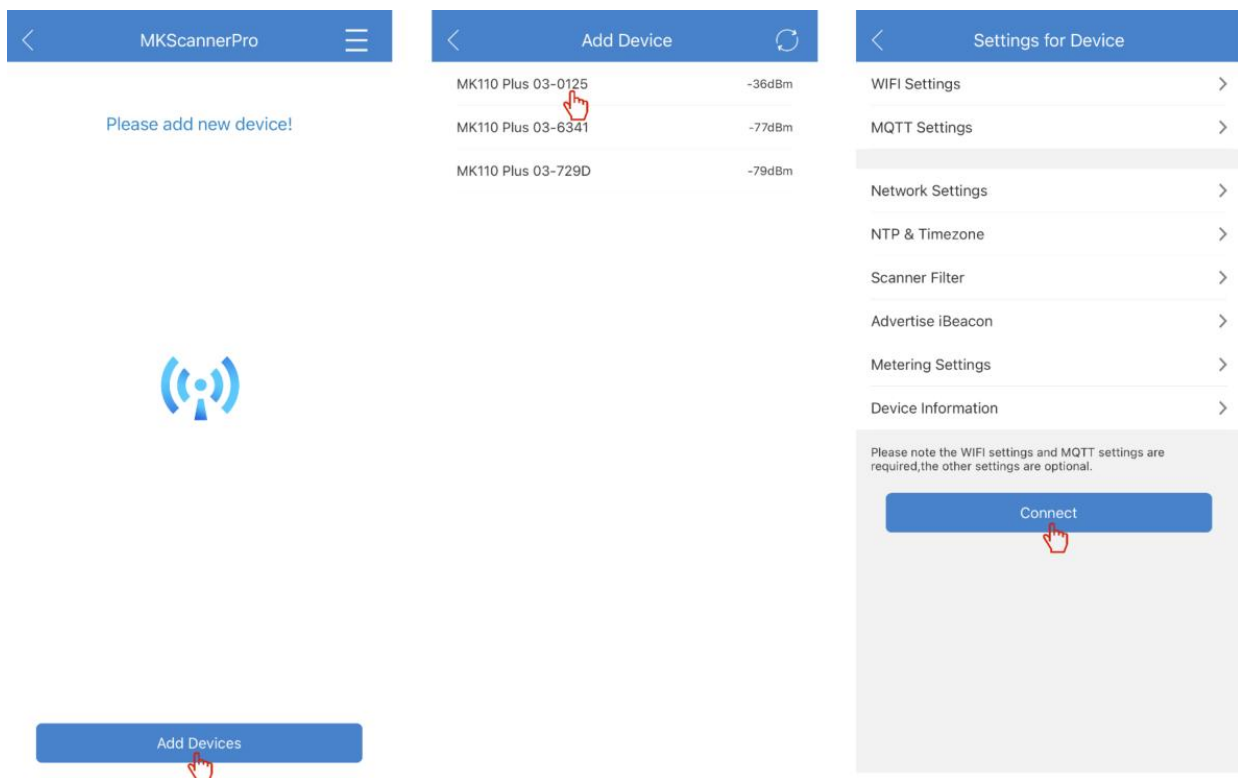
Type	Parameter	Description
Broker setting	Host	Server IP address or domain name
	Port	Server port
	Client id	MQTT client id, each device connected to the server should have a different client id.
Topics	Subscribe	These two settings are used for connecting to Alibaba cloud. If connect to a MQTT broker 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

4.2 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.

4.2.1 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.

4.2.2 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

4.2.3 NTP&Timezone

To configure the NTP server and timezone for the gateway.

4.2.4 Scanner filters

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

4.2.5 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.

4.2.6 Metering settings

To configure the power metering parameters.

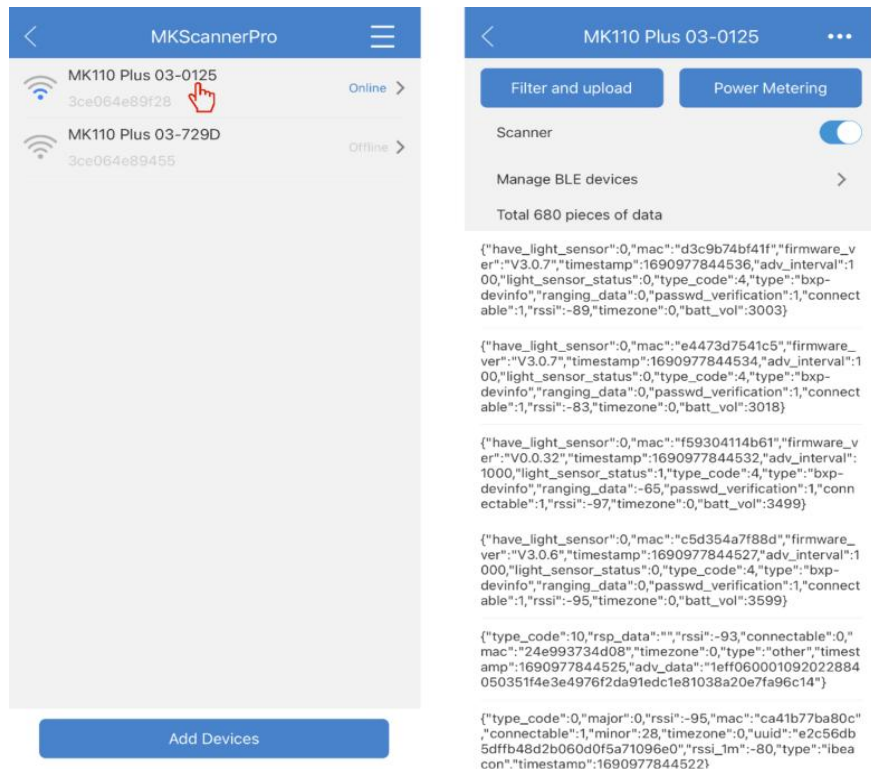
- Metering switch: if it is on, the gateway will periodically report power and energy data after it connects to cloud. If it is off, the data reporting will be off.
- Load detection notification: if it is on, when the gateway detects the electrical load is removed or inserted, it will report a notification 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





4.2.7 Device information

To read the device information of the gateway.

4.3 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.

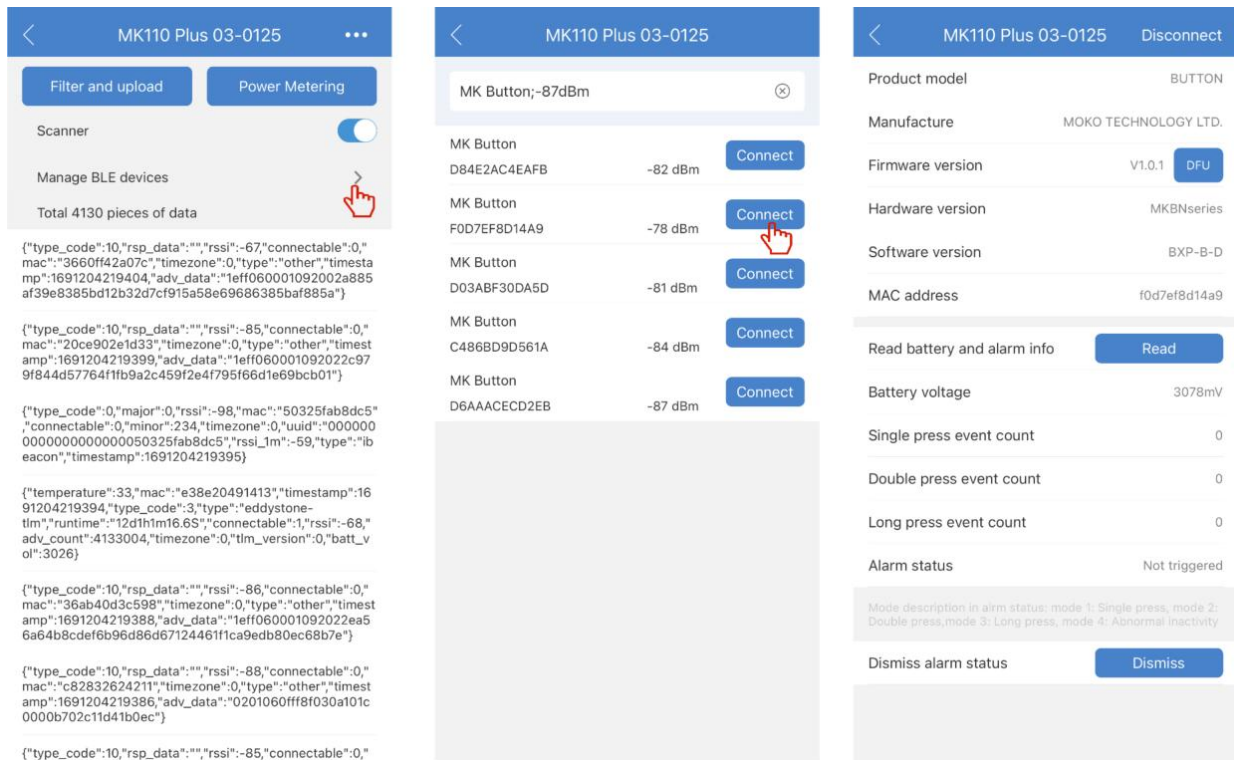


Icon	Network status	RSSI
	OFFLINE	/
	POOR WiFi	<-65 dBm
	MEDIUM WiFi	-65~-50 dBm
	GOOD WiFi	>-50 dBm

4.4 Manage BLE devices

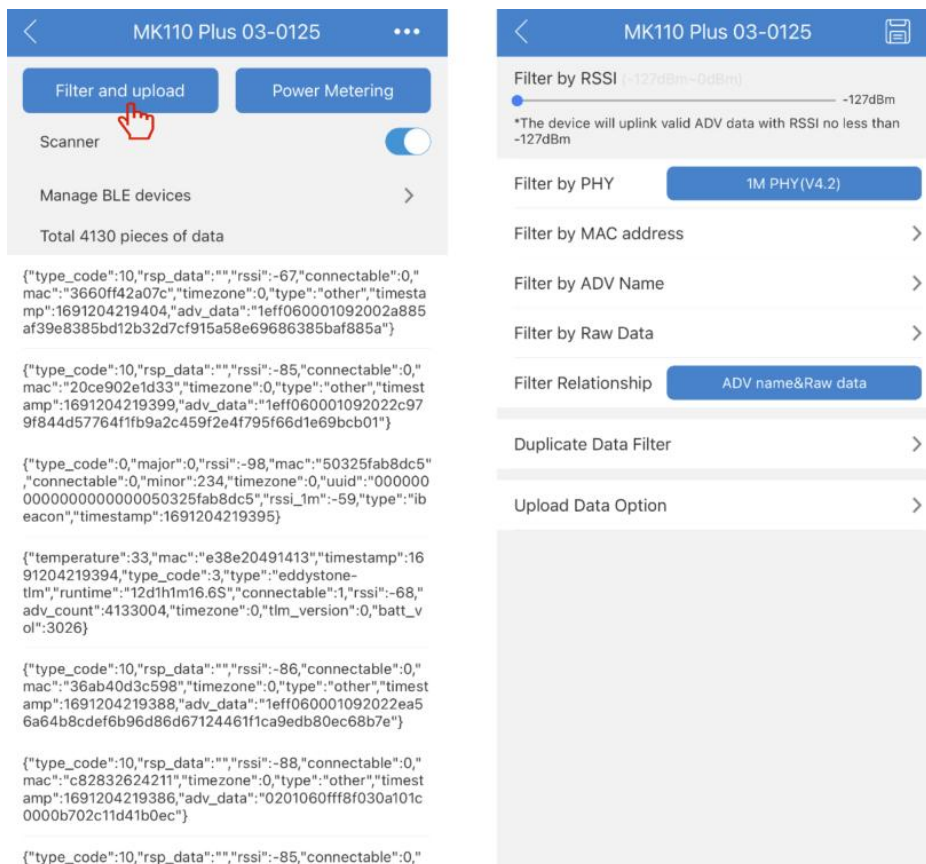
Click the manage BLE device button, it will jump to the next page where you can search and connect the nearby Beacon device.

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.



4.5 Filter and upload

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



4.5.1 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.

4.5.2 Filter By PHY

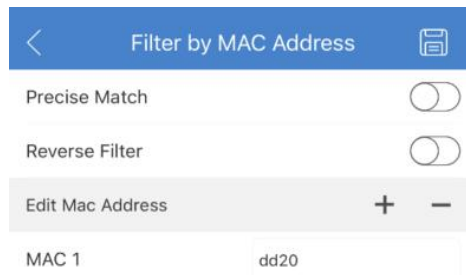
The gateway filters beacon data according to the PHY type.

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) Range: 1M PHY (V4.2)/ 1M PHY (V5.0)/ 1M PHY (V4.2) & 1M PHY (V5.0)/ Coded PHY

4.5.3 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 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. Click the “ — ” icon, it will delete the MAC address input box.
-------------	---

4.5.4 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	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.

4.5.5 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.

Filter by Raw Data

iBeacon

ON

Eddystone-UID

ON

Eddystone-URL

ON

Eddystone-TLM

ON

BXP - Device info

BXP - ACC

BXP - T&H

BXP-Button

ON

BXP-Tag

ON

PIR Presence

ON

Other

ON

4.5.5.1 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.

iBeacon

iBeacon

iBeacon UUID

0~16 Bytes

iBeacon Major

Min

0~65535

~

Max

0~65535

iBeacon Minor

Min

0~65535

~

Max

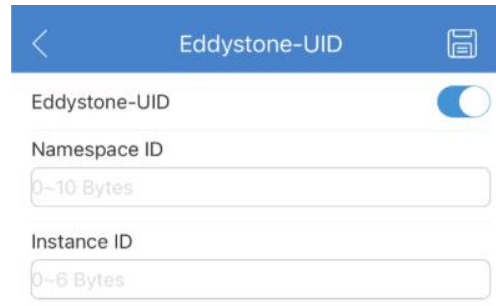
0~65535

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.

4.5.5.2 Eddystone - UID

To determine Eddystone-UID frame is uploaded 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.

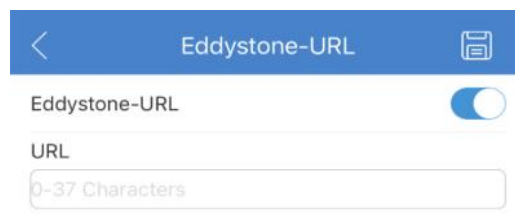


Parameter	Description
Switch	On: upload, off: not upload
Namespace ID	0-10 bytes Hex data
Instance ID	0-6 bytes Hex data

4.5.5.3 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.

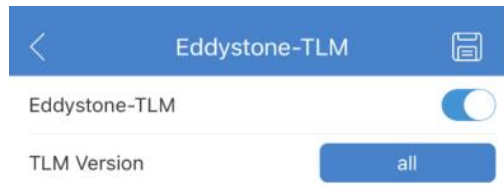


Parameter	Description
Switch	On: upload, off: not upload
URL	0-37 characters, for example: www.mokosmart.com

4.5.5.4 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 Or 1, the gateway will upload only the Eddystone - TLM data whose TLM version conforms the configuration.



The screenshot shows a configuration screen titled 'Eddystone-TLM'. At the top, there is a back arrow, the title, and a save icon. Below the title, there is a toggle switch labeled 'Eddystone-TLM' which is currently turned on. Underneath, there is a label 'TLM Version' followed by a button labeled 'all'.

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

4.5.5.5 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

4.4.5.6 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

4.4.5.7 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

4.4.5.8 BXP- Button

To determine MOKO BXP-Button frame is uploaded or not.

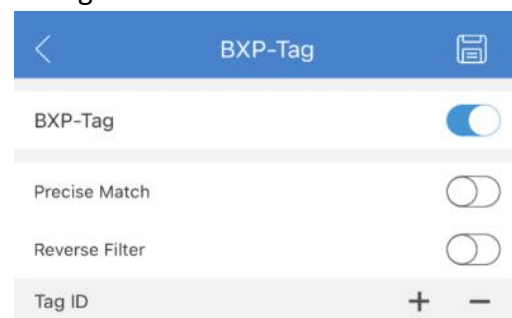
It supports filter the specified data by trigger modes. If all modes are on, the gateway will upload all detected BXP-button data. If the modes are off, the gateway will not upload the advertising data triggered by the modes.



BXP-Button	
BXP- button	<input checked="" type="checkbox"/>
Single press mode	<input checked="" type="checkbox"/>
Double press mode	<input checked="" type="checkbox"/>
Long press mode	<input checked="" type="checkbox"/>
Abnormal inactivity mode	<input checked="" type="checkbox"/>

4.4.5.9 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.



BXP-Tag	
BXP-Tag	<input checked="" type="checkbox"/>
Precise Match	<input type="checkbox"/>
Reverse Filter	<input type="checkbox"/>
Tag ID	+ -

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<=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. 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.

4.4.5.10 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 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.

4.4.5.11 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	<ul style="list-style-type: none"> ➤ 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.

4.5.5 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 effect.

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.

4.5.6 Duplicate Data Filter

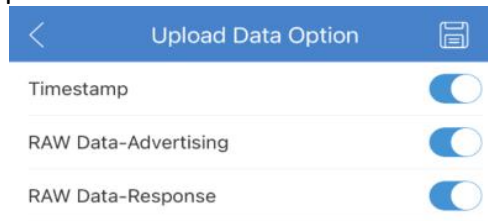
To reduce too many duplicate data uploaded to your server. In a filtering period, If the gateway scans a new data, it will report the data immediately, and throw the following data which are same as that one, finally report only one piece which is latest scanned in the period.

The screenshot shows a configuration window titled "Duplicate Data Filter". It has a blue header bar with a back arrow on the left and a save icon on the right. Below the header, there are two main sections. The first section is labeled "Filter by" and has a dropdown menu currently showing "MAC". The second section is labeled "Filtering Period" and has a text input field containing the number "10", followed by a unit selector dropdown showing "Sec".

Parameter	Description
Filter by	Default: None, range: None/MAC/MAC + Data Type/MAC + Raw Data ➤ None: 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 to the MAC address and the raw data.
Filtering Period	Only when the filter is enabled, the filtering period can be set. Default: 10, range: 1-86400 (Unit: second)

4.5.7 Upload Data Option

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

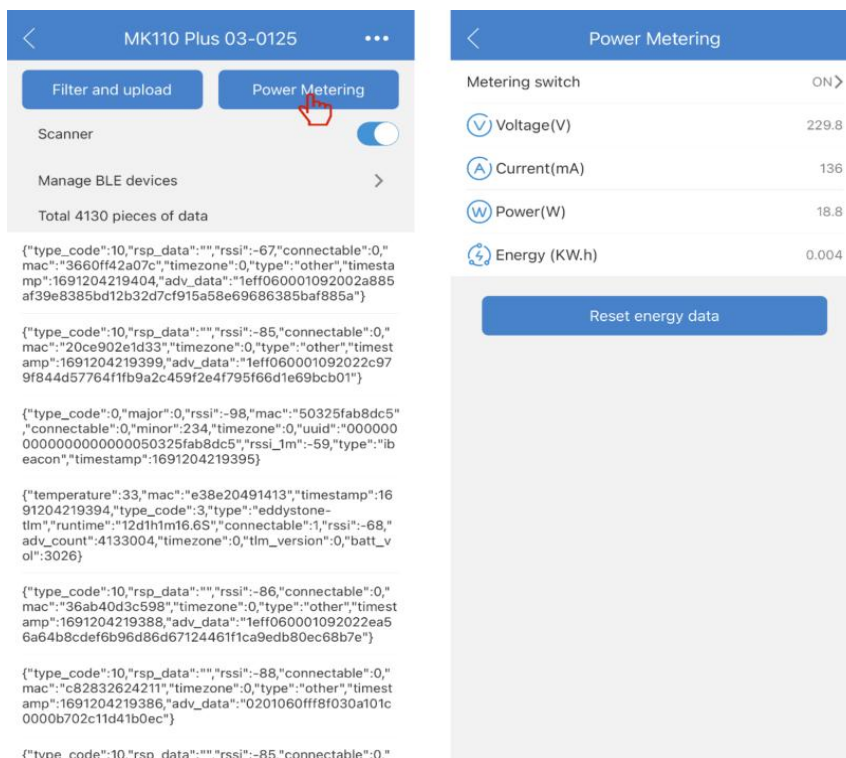


Upload Data Option	
Timestamp	<input checked="" type="checkbox"/>
RAW Data-Advertising	<input checked="" type="checkbox"/>
RAW Data-Response	<input checked="" type="checkbox"/>

4.6 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.



MK110 Plus 03-0125

Filter and upload Power Metering

Scanner ☒

Manage BLE devices >

Total 4130 pieces of data

```
{ "type_code": 10, "rsp_data": "", "rssi": -67, "connectable": 0, "mac": "3660ff42a07c", "timezone": 0, "type": "other", "timestamp": 1691204219404, "adv_data": "1eff060001092002a885af39e8385bd12b32d7cf915a58e69686385baf885a" }
```

```
{ "type_code": 10, "rsp_data": "", "rssi": -85, "connectable": 0, "mac": "20ce902e1d33", "timezone": 0, "type": "other", "timestamp": 1691204219399, "adv_data": "1eff060001092022c979f844d57764f1fb9a2c459f2e4f795f66d1e69bcb01" }
```

```
{ "type_code": 0, "major": 0, "rssi": -98, "mac": "50325fab8dc5", "connectable": 0, "minor": 234, "timezone": 0, "uid": "0000000000000000050325fab8dc5", "rssi_1m": -59, "type": "ibeacon", "timestamp": 1691204219395 }
```

```
{ "temperature": 33, "mac": "e38e20491413", "timestamp": 1691204219394, "type_code": 3, "type": "eddystone-tlm", "runtime": "12d1h1m16.6S", "connectable": 1, "rssi": -68, "adv_count": 4133004, "timezone": 0, "tlm_version": 0, "batt_vol": 3026 }
```

```
{ "type_code": 10, "rsp_data": "", "rssi": -86, "connectable": 0, "mac": "36ab40d3c598", "timezone": 0, "type": "other", "timestamp": 1691204219388, "adv_data": "1eff060001092022ea56a64b8cdef6b96d86d67124461f1ca9edb80ec68b7e" }
```

```
{ "type_code": 10, "rsp_data": "", "rssi": -88, "connectable": 0, "mac": "c82832624211", "timezone": 0, "type": "other", "timestamp": 1691204219386, "adv_data": "02010600ff8f030a101c000b702c11d41b0ec" }
```

```
{ "type_code": 10, "rsp_data": "", "rssi": -85, "connectable": 0, "mac": "3660ff42a07c", "timezone": 0, "type": "other", "timestamp": 1691204219385, "adv_data": "1eff060001092002a885af39e8385bd12b32d7cf915a58e69686385baf885a" }
```

Power Metering

Metering switch ON >

Voltage(V) 229.8

Current(mA) 136

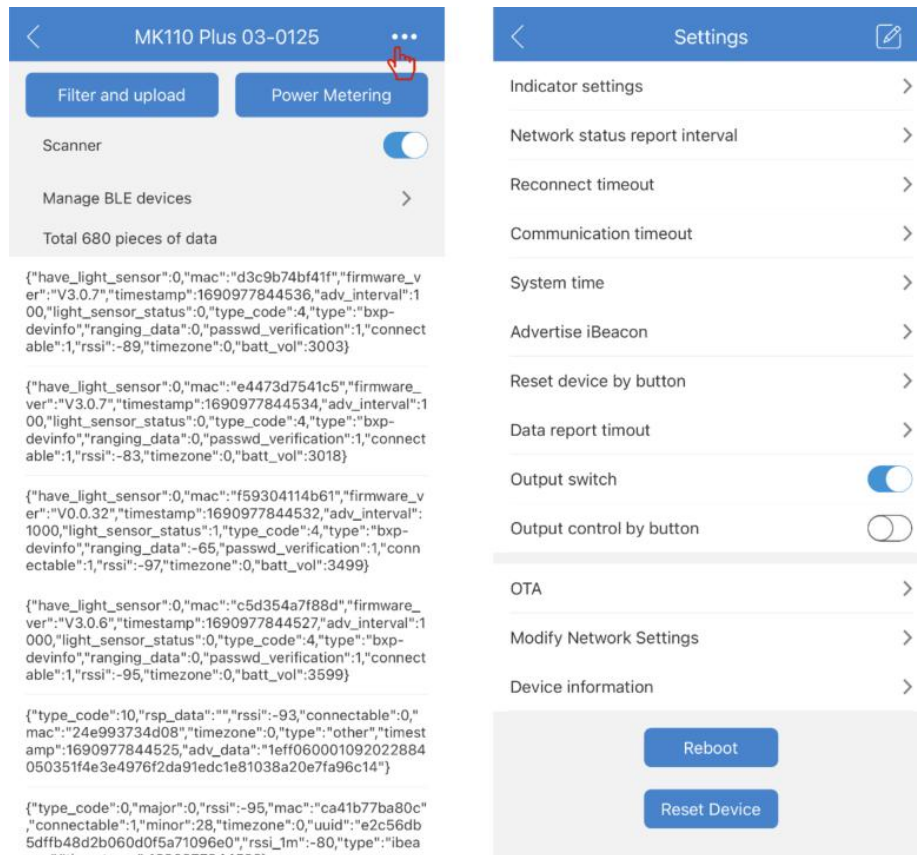
Power(W) 18.8

Energy (KW.h) 0.004

Reset energy data

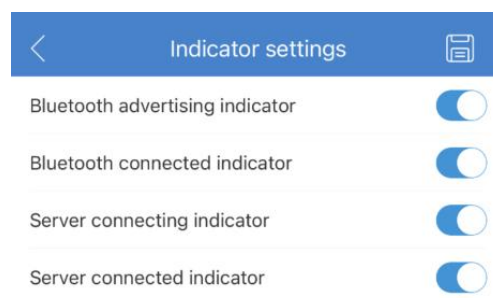
4.7 Gateway parameter settings

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



4.7.1 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

4.7.2 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.

4.7.3 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) Value 0 means that the device will not reboot

4.7.4 Communication timeout

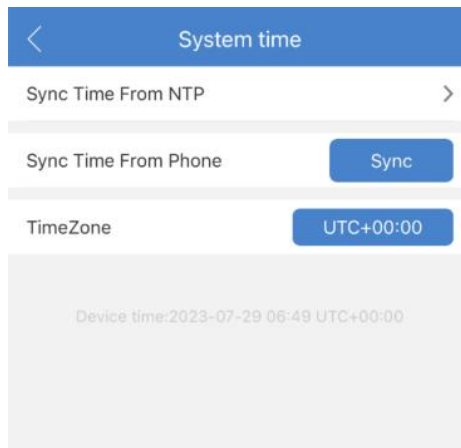
If the gateway doesn't get any downlink message from the cloud in the timeout, it will automatically disconnect from the beacon.

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

4.7.5 System Time

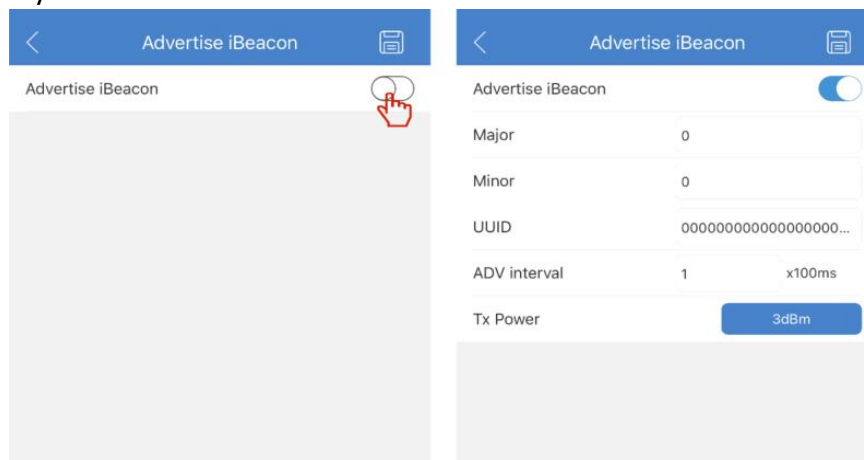
After the gateway connected with the server, it will synchronize time from the NTP server every 1 hour.

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.



4.7.6 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.

4.7.7 Reset device by button

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

Reset device by button

Press in 1 minute after powered ☒

Press any time ☐

4.7.8 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

4.7.9 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 button will not change the output switch

4.8 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.

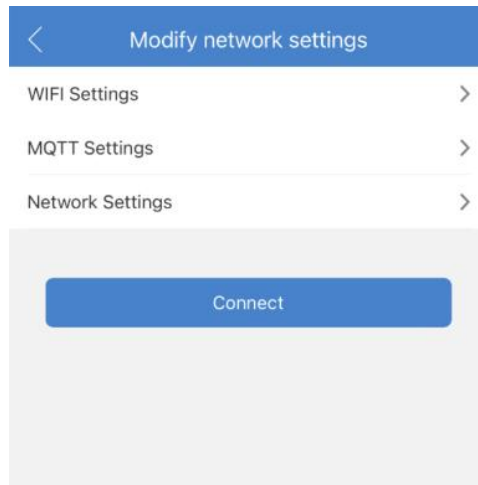
OTA

Firmware file URL 1-256 Characters

Start Update

4.9 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.



4.9.1 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



4.9.2 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

MQTT settings

Broker Setting

Host

47.104.81.55

Port

1883

Client Id

b0b21c365c94

Topics

Subscribe

/MKGW3/b0b21c365c9...

Publish

/MKGW3/b0b21c365c9...

Note: Input your topics to communicate with the device or set the topics to empty.

General

Credentials

SSL/TLS

LWT

SSL/TLS

Certificate

Self signed certificates

CA cert file URL

0-256 Characters

Client cert file URL

0-256 Characters

Client key file URL

0-256 Characters

Clear All Configurations

4.10 Device Information

You can get the device information in this page.

Device Information	
Device name	MK110 Plus 03-0125
Product model	MK110 Plus 03
Manufacturer	MOKO TECHNOLOGY LTD.
Firmware version	V1.0.3
Software version	V6.10.00.05
Hardware version	V2.1.1.0
WIFI STA MAC	3C:E0:64:E8:9F:28
BT MAC	64:E8:33:C8:01:25

4.11 Reboot

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

4.12 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.

The image displays three side-by-side screenshots of the 'WIFI Settings' application interface, each showing a different EAP type selected for Enterprise security.

- Left Screenshot (PEAP-MSCHAPV2):** Shows fields for SSID (1-32 Characters), Username (0-32 Characters), Password (0-64 Characters), Verify server (toggle on), CA cert file URL (0-256 Characters), and Country&Band (United States of America).
- Middle Screenshot (TTLS-MSCHAPV2):** Shows the same fields as the left screenshot, but with the EAP type set to TTLS-MSCHAPV2.
- Right Screenshot (TLS):** Shows fields for SSID (1-32 Characters), Domain ID (0-64 Characters), CA cert file URL (0-256 Characters), Client cert file URL (0-256 Characters), Client key file URL (0-256 Characters), and Country&Band (United States of America).

Below each set of fields is a note: 'Please note the country&Band is a configuration for 5GHz WiFi, if using 2.4GHz WiFi, there is no need to choose the band.'

- 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.

Settings for APP

Broker Setting

Hosta1fhygr0xxahcm-ats.iot.us-west-2.ama

Port8883

Client IdMK_F2919D43

Topics

Subscribe0-128 Characters

Publish0-128 Characters

Note: The topic settings is only for connecting to Alibaba
iot. Please leave it blank if connecting to a MQTT broker or
AWS iot.

GeneralUser CredentialsSSL/TLS

SSL/TLS

CertificateSelf signed certificates

CA File/storage/emulated/0/.001/MOKO
AWS file/zaws-root-ca.pem

Client Key/storage/emulated/
0/.001/MOKO AWS file/
zapp-private.pem.key

Client Cert File/storage/emulated/
0/.001/MOKO AWS file/
zapp-certificate.pem.crt

MQTT settings

Broker Setting

Hosttygr0xxahcm-ats.iot.us-west-2.amazon:

Port8883

Client Id4091519c75c0

Topics

Subscribe/MK110/4091519c75c0/receive

Publish/MK110/4091519c75c0/send

GeneralUser CredentialsSSL/TLS

SSL/TLS

CertificateSelf signed certificates

CA File/storage/emulated/0/.001/MOKO
AWS file/zaws-root-ca.pem

Client Key/storage/emulated/
0/.001/MOKO AWS file/
zapp-private.pem.key

Client Cert File/storage/emulated/
0/.001/MOKO AWS file/
zapp-certificate.pem.crt

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.

Settings for APP

Broker Setting

Hosta1fhygr0xxahcm-ats.iot.us...

Port8883

Client IdMK_62316651

Topics

Subscribe0-128 Characters

Publish0-128 Characters

Note: The topic settings is only for connecting to Alibaba iot.Please
leave it blank if connecting to a MQTT broker or AWS iot.

GeneralUser CredentialsSSL/TLS

SSL/TLS

CertificateSelf signed certificates

CA Fileaws-root-ca.der

P12 Cert Fileios-certificate file.p12

Clear All Configurations

MQTT settings

Broker Setting

Hosta1fhygr0xxahcm-ats.iot.us...

Port8883

Client Idc8f09ee8327c

Topics

Subscribe/MK110 plus 01/c8f09ee83...

Publish/MK110 plus 01/c8f09ee83...

GeneralCredentialsSSL/TLSLWT

SSL/TLS

CertificateSelf signed certificates

CA Filezaws-root-ca.pem

Client Keyzdevice-private.pem.key


Client Cert Filezdevice-certificate.pem.crt

Clear All Configurations

Revision History

Revision	Description	Editor	Date
V1.0	Initial version	Weiguifen	2023.9.12

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>



FCC Warning

15.19 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.

15.21 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.

15.105 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:

- 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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 is 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.