



MKGW4 Cellular Gateway

User Manual

Version V1.1

Contents

1. About this document	1
2. LED status	1
3. Preparation before configuration	2
4. Configure the gateway	3
4.1 Search and connect gateway Bluetooth	3
4.2 Network Configuration	4
4.2.1 Network settings	4
4.2.2 MQTT settings	5
4.3 Scanner Configuration	6
4.3.1 Scan and report mode	7
4.3.2 Mode automatic switch	8
4.3.3 Scan filter settings	8
4.3.4 Filter Relationship	17
4.3.5 Duplicate Data Filter	17
4.3.6 Upload payload Settings	18
4.4 Position Configuration	19
4.4.1 Positioning mode	19
4.4.2 3-axis parameters	20
4.4.3 GPS fix parameters	21
4.5 Settings	21
4.5.1 Indicator settings	21
4.5.2 Bluetooth parameters	21
4.5.3 Heartbeat report settings	22
4.5.4 System time	23
4.5.5 Battery management	23
4.5.6 Power disconnect notification	23
4.5.7 Delete buffer data	23
4.5.8 Power on when charging	23
4.6 Reboot	24
4.7 Power off	24
4.8 Reset	24
4.9 Read device information	24
Appendix A: Connect to AWS IoT	25
Revision History	26

1. About this document

MOKO provides a local configure tool and remote config tool for users to test the MKGW4 gateway. The local configure tool is a configuration APP, all configurations are done via Bluetooth. The remote config tool is a computer software, all configurations are done by MQTT commands.

This User Guide was designed to help users to know the MOKO MKGW4 gateway and set up the gateway with MOKO configuration APP.

2. LED status

There are four LEDs to indicate the gateway power supply status, power on/off status, network status and GPS status. The LED status and gateway status are shown as below:

1. In most situations, the device status is shown by the single LED.

Icon	LED description	LED status	Gateway status
	Power supply status BLUE	On	Powered by external DC power
		Off	Powered by internal battery
		Slowly flash every 2 seconds	Battery voltage is low
		Slowly flash every 5 seconds	Battery is charging
		Quickly flash for 5 seconds (flash every 500 milliseconds)	Battery is fully charged
	Power on/off status GREEN	Quickly flash for 5 seconds (flash every 500 milliseconds)	Power on
		Keep on for 5 seconds	Power off
		Flash once	Hall switch detected
	Cellular status GREEN	Slowly flash every 2 seconds	Network connecting
		Quickly flash every 500 millisecond	Server connecting
		Keep on for 5 seconds	Server connected
	GPS status BLUE	Slowly flash every 2 seconds	GPS fixing
		Keep on for 5 seconds	GPS fix succeed
		Quickly flash for 5 seconds (flash every 500 milliseconds)	GPS fix failed

2. In some situations, the device status is indicated by the two LEDs together.

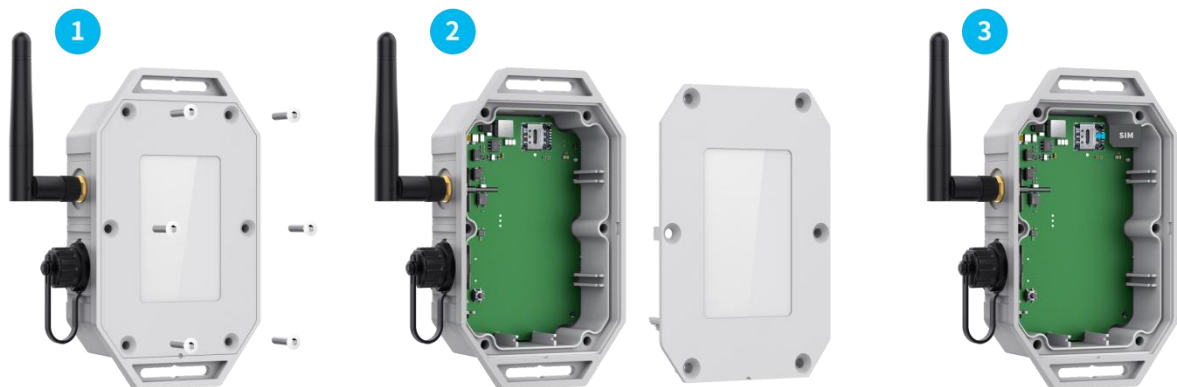
LED status	Gateway status
The first two LEDs flash three times	Restore to factory settings

The later two LEDs slowly flash(flash every 2 seconds)	Firmware upgrading
The later two LEDs keep on for 3 seconds	Firmware upgrade successfully
The later two LEDs quickly flash for 5 seconds (flash every 500 milliseconds)	Firmware upgrade failed

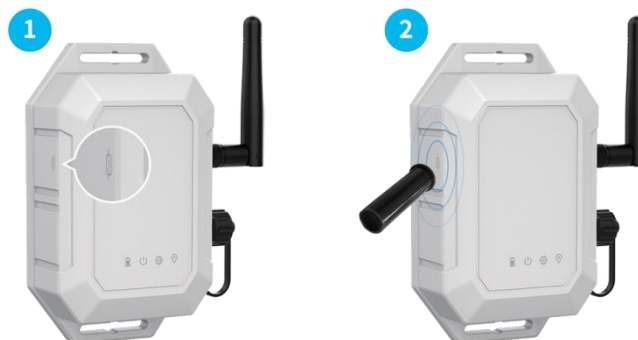
3. Preparation before configuration

Step 1: Remove the six screws at the bottom to disassemble the casing

Step 2: Find the SIM card slot on the hardware, and install the SIM card into the slot



Step 3: Use a magnet to power on the gateway, move the magnet close and away from the Hall sensor for three times, the gateway will be turned on. Please note, the operation needs to be completed in 3 seconds.



Step 4: If the gateway is tested in a lab, we can use a DC power supply source to charge it, just need to connect the black and red lines to the power supply negative and positive. If the gateway is installed in a vehicle, we can connect the lines with the engine contacts, the digital input (yellow line) can be connect with the ACC contact to detect engine on/off status.



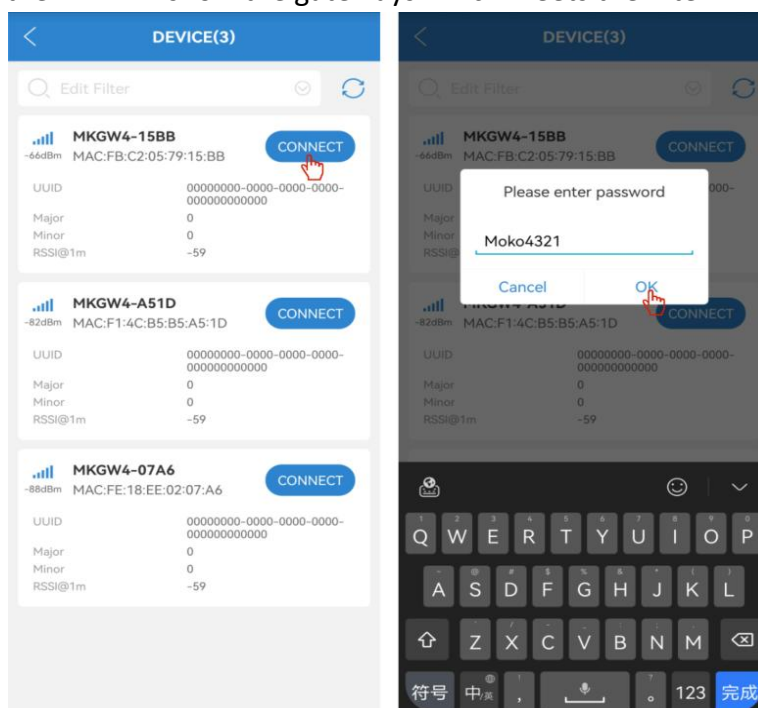
4. Configure the gateway

MOKO provides a configuration APP with users to quickly configure the gateway, please search and download “MKScannerPro” in APP Store or Google Play, then install it in your mobile. When install the app, please allow the location and storage permission.

4.1 Search and connect gateway Bluetooth

Select Cellular Gateway option, it will go to the search page. Make sure your gateway is powered on, the gateway Bluetooth name will appear in the list. Connect it and enter the password, the APP will connect to the gateway Bluetooth, the default password is **Moko4321**.

The Edit Filter can help to filter the target gateways, type the MAC address or name of the target gateway here, then the APP will show the gateways which meets the filter.



4.2 Network Configuration

4.2.1 Network settings

After the gateway is connected by APP, we can see the network and MQTT connection status of the gateway.

Connecting=>Connecting to network or MQTT now.

Connected=>Connected to network or MQTT now.

Unconnected=> Not connect now

Click the network settings, it will go to the configuration page where we can change the cellular network settings.

The screenshot displays the MQTT settings configuration page for the MKGW4-15BB gateway. The interface is divided into a left sidebar and a main content area. The sidebar shows 'Network settings' with a 'Connecting' status and 'MQTT settings' with an 'Unconnected' status. The main content area is titled 'MQTT settings' and includes a 'Network priority' dropdown set to 'NB-IOT'. Below this are input fields for 'APN' (0-100 Characters), 'Username' (0-127 Characters), and 'Password' (0-127 Characters). A 'Connect timeout' field is set to '180' with a unit of 'Second'. A bottom navigation bar contains icons for 'Network', 'Scanner', 'Position', and 'Settings'.

Type	Parameter	Description
Network setting	Network priority	The gateway supports global NB-IOT, CAT.M and GSM connectivity, to set the network order for connectivity
	APN	Related to the SIM card, can be empty.
	Username	
	Password	
	Connect timeout	The timeout for gateway connects to network. When there is no network coverage, the gateway will stop connection after the timeout.

4.2.2 MQTT settings

Click the MQTT settings, it will go to the configuration page where we can change the MQTT settings. The gateway is using MOKO MQTT endpoint (**47.104.81.55:1883**) as the default settings, users can directly use them or change to other MQTT endpoints.

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

- Clear all configurations: To clear all configurations in this page, you can edit totally new configurations for the gateway
- Export config file: Export current configurations, an excel file will be created and can be sent via email. The file can be edited and used for other gateway configuration.
- Import config file: Directly input the configurations in current page by uploading an excel file.

The screenshot displays the MQTT settings interface. On the left, a sidebar shows 'Network settings' with a status of 'Connecting' and 'MQTT settings' with a status of 'Unconnected'. A red hand icon points to the 'MQTT settings' link. The main content area is titled 'MQTT settings' and includes a 'Broker Setting' section with input fields for Host (47.104.81.55), Port (1883), and Client Id (fbc2057915bb). Below this is the 'Topics' section with 'Subscribe' and 'Publish' fields. The 'General' tab is active, showing 'Clean Session' as a toggle switch (on), 'Qos' as a dropdown menu (0), and 'Keep Alive' as a text input (60s). At the bottom of the page, there are three buttons: 'Clear All Configurations', 'Export Config File', and 'Import Config File'.

If the MQTT connection requires SSL/TLS encryption, please turn on the the SSL/TLS, and select the certificate type. If it needs to verify certificates, please click ... to upload the files. After everything is configured, please do not forget to click the save button.

For more details to configure SSL and certificates, please see [Appendix A Connect to AWS IoT](#)

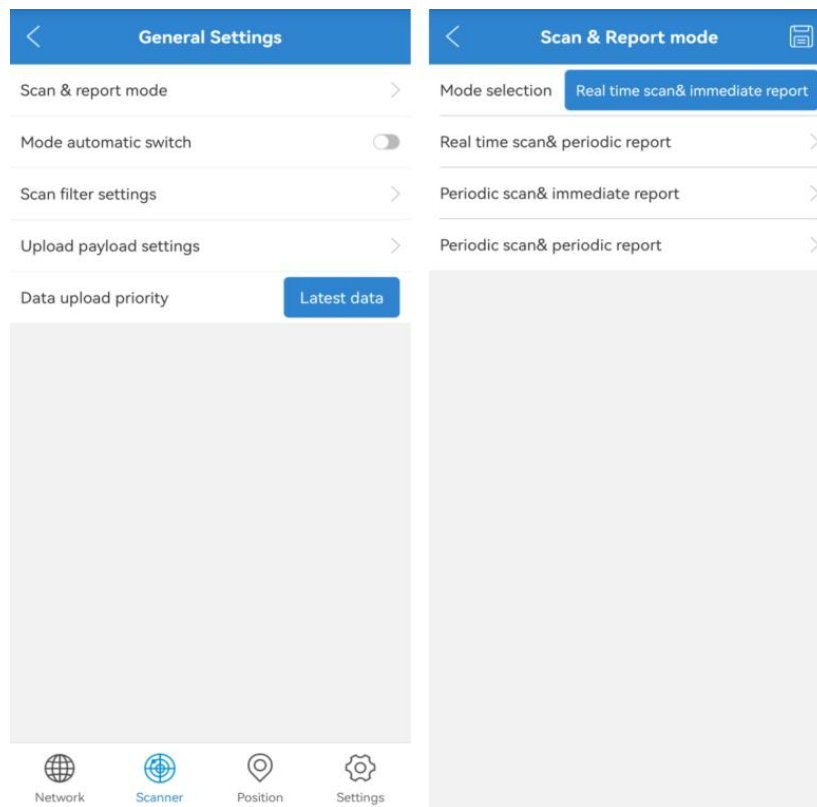
The image shows three sequential screenshots of the SSL/TLS configuration page. Each screenshot has a 'General', 'Credentials', and 'SSL/TLS' tab, with 'SSL/TLS' being the active tab. In all three, the 'SSL/TLS' toggle switch is turned on. The first screenshot shows the 'Certificate' dropdown set to 'CA signed server certificate'. The second screenshot shows the 'Certificate' dropdown set to 'CA certificate', with a 'CA File' upload button (indicated by three dots) below it. The third screenshot shows the 'Certificate' dropdown set to 'Self signed certificates', with 'CA File', 'Client Key', and 'Client Cert File' upload buttons (each indicated by three dots) below it.

To get more details for the MQTT parameters, please check the below chart:

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
	Certificate	➤ CA signed server certificate: no certificate is required ➤ CA certificate file: CA root certificate is required to upload ➤ Self signed certificates: CA root certificate, client certificate and client key files are required to upload.

4.3 Scanner Configuration

To configure the BLE scan & report mode, filters and upload data payload for the gateway.



4.3.1 Scan and report mode

To select the gateway scan and report mode, there are 5 modes:

- Real time scan&immediate report: The gateway BLE scan is always on, it reports the captured BLE data to cloud immediately.
- Real time scan&periodic report: The gateway BLE scan is always on, the captured BLE data is saved in the gateway. When the report interval comes, the gateway connects cellular network and starts BLE data reporting
- Periodic scan&immediate report: In most time, the gateway is in sleep mode. When the scan interval comes, the gateway turns on scanning for a preset duration. After the duration expires, the gateway immediately reports the captured BLE data to cloud
- Periodic scan& periodic report: In most time, the gateway is in sleep mode. When the scan interval comes, the gateway turns on scanning for a preset duration, and saves the captured data in itself. When the report interval comes, the gateway connects cellular network and start BLE data reporting
- Turn off scan: The gateway BLE scan is turned off, there will be no any BLE data reporting

The scan&report mode parameters are as below:

Type	Parameter	Description
Scan&report mode	Mode selection	Options: ➤ Real time scan&immediate report ➤ Real time scan&periodic report(Default mode) ➤ Periodic scan&immediate report ➤ Periodic scan& periodic report ➤ Turn off scan

Real time scan & periodic report	Report interval	The BLE data report interval, default: 600 Range: 10-86400, unit: second
Periodic scan & immediate report	Scan duration	The BLE scan duration, default: 60 Range: 3-3600, unit: second
	Scan interval	The BLE scan interval, default: 600 Range: 10-86400, unit: second
Periodic scan & periodic report	Scan duration	The BLE scan duration, default: 60 Range: 3-3600, unit: second
	Scan interval	The BLE scan interval, default: 600 Range: 10-86400, unit: second
	Report interval	The BLE data report interval, default: 600 Range: 10-86400, unit: second
	Data upload priority	If current period data is sending, the next period BLE data is coming, to determine which period of data is kept and uploaded. ➤ Current period ➤ Next period

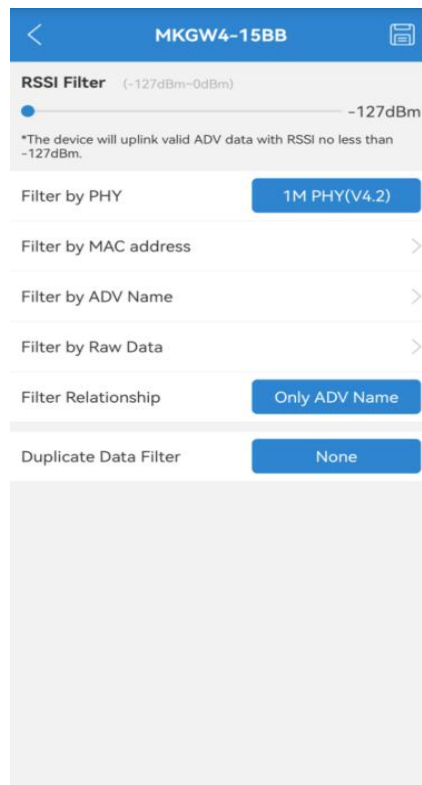
4.3.2 Mode automatic switch

When the gateway is connected with the external power supply, and working on Real time scan&immediate report mode, if the external power is disconnected, the working mode will switch to Real time scan&periodic report. To determine the automatic switch will work or not.

Type	Parameter	Description
Scan&report mode	Mode automatic switch	ON/OFF. Default: OFF

4.3.3 Scan filter settings

To set the BLE scanning filter for the gateway.



4.3.3.1 Filter By RSSI

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

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

4.3.3.2 Filter By PHY

The gateway will upload the BLE data advertised on the corresponding PHY layer.

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

4.3.3.3 Filter By MAC address

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

Type	Parameter	Description
Filter by MAC address	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 to add MAC address. 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 latest MAC address input box.

4.3.3.4 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.

Type	Parameter	Description
Filter by ADV name	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.

4.3.3.5 Filter by Raw Data

The gateway filters beacon data according to advertising data type.

The first 11 types are supported by MOKO beacon, other beacon data apart from the 11 types will be called “Other”.

Filter by Raw Data	
iBeacon	ON >
Eddystone-UUID	ON >
Eddystone-URL	ON >
Eddystone-TLM	ON >
BXP - Device Info	☒
BXP - ACC	☒
BXP - T&H	☒
BXP - Button	ON >
BXP - Tag	ON >
PIR Presence	ON >
MK TOF	ON >
Other	ON >

4.3.3.5.1 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.

4.3.3.5.2 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

4.3.3.5.3 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	0-114 characters, for example: www.mokosmart.com

4.3.3.5.4 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 Or 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: Un-encrypted TLM; ➤ Version 1: Encrypted TLM

4.3.3.5.5 BXP-Device info

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

4.3.3.5.6 BXP-ACC

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

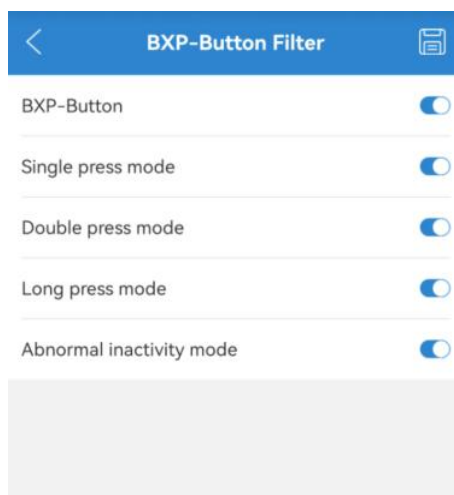
4.3.3.5.7 BXP-T&H

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

4.3.3.5.8 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.



4.3.3.5.9 BXP-Tag

To determine upload BXP-Tag 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.

4.3.3.5.10 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.

4.3.3.5.11 MK TOF

To determine upload BXP-Tag data or not

It supports filter the specified data by the MFG code, up to 10 codes can be set at one time.

Parameter	Description
Switch	On: upload, off: not upload
MFG code	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 input box.

4.3.3.5.12 Other

The Beacon data other than the above 10 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.

4.3.4 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.

4.3.5 Duplicate Data Filter

To reduce too many duplicate data uploaded to the cloud in a period.

In the periodic can or periodic report modes, if the gateway scans a new data, it will cache the data immediately, and throw the following data which are same as that one, finally report only one piece of data which is latest scanned in the period.

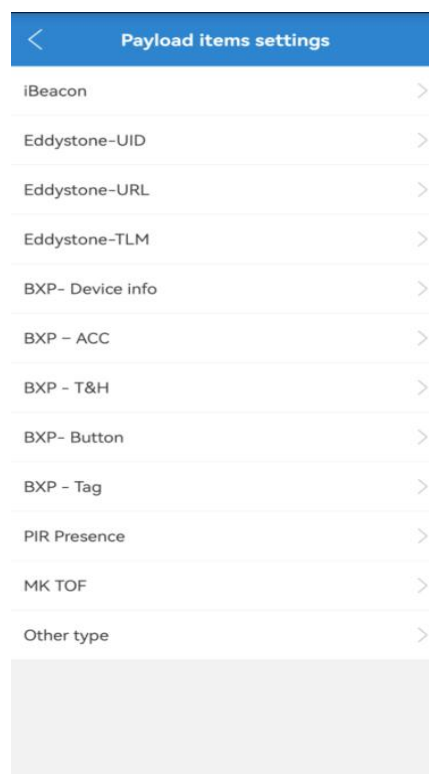
Parameter	Description
Filter by	Default: MAC, options: None/MAC/MAC + Data Type/MAC + Raw Data ➤ None: Duplicate data filter is disabled. ➤ MAC: The BLE data comes from the same beacon will be judged as duplicate ➤ MAC+ Data Type: The BLE data comes from the same beacon and the data type of the BLE raw data are the same, will be judged as duplicate ➤ Mac+ Raw Data: The BLE data comes from the same beacon and the BLE raw data are the same, will be judged as duplicate

4.3.6 Upload payload Settings

To determine the data payload of BLE packet which will be uploaded to cloud.

The payload of standard iBeacon, Eddystone and MOKO defined data types can be selected by the specific data field, the payload of other type can be selected by the data blocks.

The checked options will be upload, the unchecked options will be not upload.



Here takes the iBeacon and Other type as the examples:

The RSSI, Timestamp, raw data -advertising and raw data -response are common used in all types.

In iBeacon type: the UUID, major, minor, RSSI@1m can selected separately

In other type: it can add 10 groups of data blocks. Each data block includes the BLE data type, the data start byte and end byte under the data type.

Eddystone-UID payload

RSSI ☒

Timestamp ☒

RSSI@0m ☒

Namespace ☒

Instance ☒

Raw data- Advertising ☐

Raw data- Response ☐

Other type payload

RSSI ☒

Timestamp ☒

Data block options +

Data block 1 Data Type 1-29 ~ 1-29 Byte —

Raw data- Advertising ☐

Raw data- Response ☐

4.4 Position Configuration

To configure the GPS fix mode and related parameters.

Position

Fix mode >

GPS parameters >

3-Axis parameters >

Fix mode

Periodic fix

Periodic fix >

Motion fix >



Network



Scanner



Position



Settings

4.4.1 Positioning mode

To select the GPS fix mode, there are 3 modes for selection:

- Periodic fix: The gateway fixes and report location periodically.
- Motion fix: The gateway fix location based on the movement status. The fix interval in different movement status can be set separately.
- Turn off GPS: The gateway GPS function will be disabled.

The positioning parameters are as below:

Type	Parameter	Description
Fix mode	Mode selection	Options: ➤ Periodic fix (Default mode) ➤ Motion fix ➤ Turn off GPS
Periodic fix	Fix interval	The GPS fix interval, default: 3600 Range: 10-86400, unit: second
Motion fix	Fix when start	Fix when motion start is detected On/off, default is on.
	Fix in trip	Fix in the trip On/off, default is on.
	Fix interval in trip	Range: 10-86400, unit: second
	Fix when stops	Fix when motion stop is detected On/off, default is on.
	Motion stops timeout	Timeout to judge the motion is stopped Range: 3-180, unit: 10 second
	Fix in stationary	Fix when the gateway is in stationary. On/off, default is on.
	Fix interval in stationary	Range: 1-1440, unit: minute

4.4.2 3-axis parameters

To configure the accelerometer parameters,


3-Axis parameters


Wakeup Threshold x16mg

Wakeup Duration x10ms

Motion Threshold x2mg

Motion Duration x5ms

Parameter	Description
Wakeup threshold	The motion threshold to wake up the device Default: 3, range: 1-20, unit:16mg
Wakeup duration	The motion duration to wake up the device Default: 2, range: 1-10, unit:10ms
Motion threshold	The motion threshold to judge movement Default: 16, range: 10-250, unit:2mg

Motion duration	The motion duration to judge movement Default: 8, range: 1-15, unit:5ms
-----------------	--

4.4.3 GPS fix parameters

Parameter	Description
Fix timeout	The timeout for GPS fix, if the GPS can not get a fix in the timeout, it will give up trying.
PDOP	The upper limitation for Position Dilution of Precision. If the fixed position has a larger PDOP than the limitation, the position data will be considered invalid. Default: 100, range: 25-100, unit: 0.1

4.5 Settings

All parameters in the settings page can be modified.

4.5.1 Indicator settings

The 4*LED indicators can be turned on/off separately.

4.5.2 Bluetooth parameters

To change the gateway advertising name, advertising interval, BLE connect password and other Bluetooth parameters.

The gateway advertising data includes the advertising packet and response packet, the response packet is the standard iBeacon.



Bluetooth parameters

Advertisement

ADV name: MKGW4-15BB

ADV interval: 10 x 100ms

ADV timeout: 0 minute

Advertise response packet: ☒

Major: 0

Minor: 0

UUID: 00000000000000000000000000000000

RSSI@1m (-100dBm~0dBm): -59dBm

Tx power (-40~-20~-16~-12~-8~-4~0~2~3~4~5~6~7~8): 0dBm

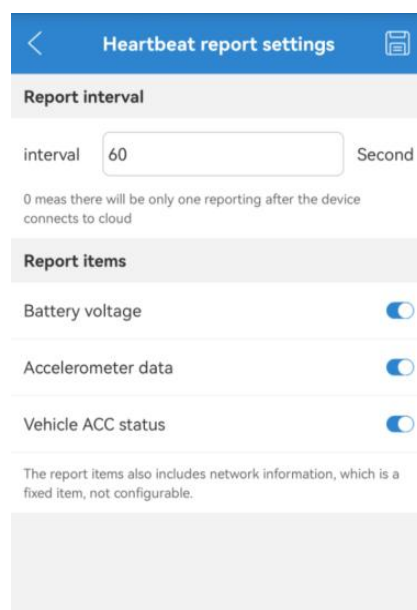
Connection

Password verification: ☒

Connection password: Moko4321

4.5.3 Heartbeat report settings

After the gateway connects to cloud, it will report heartbeat to cloud. The heartbeat includes network status, battery voltage and other status information. Here to change the heartbeat report interval and payload.



Heartbeat report settings

Report interval

interval: 60 Second

0 means there will be only one reporting after the device connects to cloud

Report items

Battery voltage: ☒

Accelerometer data: ☒

Vehicle ACC status: ☒

The report items also includes network information, which is a fixed item, not configurable.

4.5.4 System time

To set the NTP server and timezone for the gateway.

The image displays two side-by-side screenshots of a mobile application interface for configuring system time.

The left screenshot shows the 'System time' screen. At the top, there is a blue header with a back arrow and the title 'System time'. Below the header, there is a toggle switch labeled 'Sync Time From NTP'. Underneath, there is a 'TimeZone' label and a blue button labeled 'UTC'. The bottom half of the screen is a light gray placeholder.

The right screenshot shows the 'Sync Time From NTP' screen. It has a blue header with a back arrow, the title 'Sync Time From NTP', and a save icon. Below the header, there is a 'Sync Switch' toggle. Underneath, there is a 'Sync interval' field with the value '24' and a unit selector set to 'Hour'. Below that is an 'NTP Server' input field with the placeholder text '0-64 Characters'. The bottom half of the screen is a light gray placeholder.

4.5.5 Battery management

The gateway will report a notification to cloud if it detects the battery is low power. Here to set the notification switch and the low power threshold.

The image shows a screenshot of the 'Battery management' screen in a mobile application. It has a blue header with a back arrow, the title 'Battery management', and a save icon. Below the header, there is a 'Low power notification' toggle. Underneath, there is a 'Low power threshold' label and a blue button labeled '10%'. The bottom half of the screen is a light gray placeholder.

4.5.6 Power disconnect notification

The gateway will report a notification to cloud if it detects the external power supply is disconnected. Here to set the notification switch.

4.5.7 Delete buffer data

The gateway will store the offline data in the buffer, here to delete the buffer data.

4.5.8 Power on when charging

When the gateway is powered off due to battery low voltage, to determine the gateway power on/off status when the gateway is charging.

4.6 Reboot

To reboot the gateway. After click the Reboot button, the gateway will reboot once and the gateway Bluetooth will be disconnected from APP..

4.7 Power off

To power off the gateway. After that the gateway will be powered off and the gateway Bluetooth will be disconnected from APP..

4.8 Reset

To reset the gateway. After that, the gateway will be restored to factory settings.

4.9 Read device information

To read the basic information of the gateway, such as name, model, MAC address, firmware version and so on.

The DFU button is used to upgrade gateway firmware. Click the button to select the firmware zip file from the mobile phone and it will enter upgrade process. After the upgrade is complete, it will prompt “success/fail” to tell you the result.

Device Information	
Device Name	MKGW4-15BB
Product Model	MKGW4
Manufacturer	MOKO TECHNOLOGY LTD.
Hardware Version	V1.0
Software Version	nRF52-SDK17.0
Firmware Version	<button>DFU</button> V1.0.1
MAC Address	FB:C2:05:79:15:BB
IMEI	863251071059443
ICCID	89860487212070527458

Appendix A: Connect to AWS IoT

Go to MQTT settings page, 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.

MQTT settings

Broker Setting

Host: a1fhygr0xxahcm-ats.iot.us-west-2.ama.

Port: 8883

Client Id: d96a3675e9f3

Topics

Subscribe: /MKGW4/d96a3675e9f3/receive

Publish: /MKGW4/d96a3675e9f3/send

General Credentials SSL/TLS

SSL/TLS: ☒

Certificate: Self signed certificates

CA File: /storage/emulated/0/Android/data/com.moko.mkscannerpro/files/MKScannerPro/aws-root-ca (1).pem

Client Key: /storage/emulated/0/Android/data/com.moko.mkscannerpro/files/MKScannerPro/aws-privat...

Client Cert File: /storage/emulated/0/Android/data/com.moko.mkscannerpro...

Revision History

Revision	Description	Editor	Date
V1.0	Initial version	Weiguifen	2023.12.10
V1.1	Change some parameters range and default value. Add appendix A Connect to AWS IoT	Weiguifen	2024.6.28

FCC statement

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.

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

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.

RF Exposure Information (MPE)

This device has been tested and meets applicable limits for Radio Frequency (RF) exposure.

This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

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>

