MOKO SMART

Bluetooth Gateway

MKGW1-BW Pro

User Guide

Revision History

Version	Data	Notes	Contributor(s)
V1.0	25-Sep-2021	Initial version	Kevin Huang
V1.1	13-Jan-2022	1. Chapter 4.2. Added the method to access the Web GUI by connecting a computer 2. Chapter 6.4.3. Updated the timestamp structure in message payload when using Hex format. Added UTC time zone to the timestamp 3. Chapter 7.1.4, 7.2, 7.3. Updated the type of JSON formats for uploading message to server 4. Chapter 7.1.4, 7.2, 7.3, 7.4. Added Online Message Interval function to indicate the gateway is online 5. Chapter 8.11. Added One-click configuration and upgrade feature 6. Corrected some description and figure errors	Kevin Huang
V1.2	08-Mar-2022	Modify some error descriptions.	Kevin Huang
V1.3	18-Mar-2022	Modify some error descriptions	Kevin Huang

About this User Guide

This User Guide was designed to help users to know and set up the gateway, from installation to configure the gateway to send message to your Cloud Server. This guide will not cover the sales administration and the ordering process. Some technical guides will be needed if further explanation is required. The Web GUI (Gateway User Interface) may change and functionality may be added over time, this guide will be updated for major updates.

- This guide applies to the firmware version of **MKGW1-BW Pro V1.1.0** or above.
- Look for the following items when reading this User Guide.

This checkmark means there is a note of interest and is something you should pay special attention to while using or ordering the MKGW1-BW Pro Gateway.

This exclamation point means there is a caution or warning and is something that could damage your property or the MKGW1-BW Pro Gateway.

This question mark reminds you that you may need to refer to other chapters or technical guides to understand or use some functions.

- Each figure (diagram, screenshot, or other image) and table are provided with a number and description:

  Figure 1: Packaging of MKGW1-BW Pro gateway
  Table 1: MKGW1-BW Pro gateway packaging list

  The numbers and descriptions of the figure can be found in the “List of Figures”.

- In this guide, we use a sample gateway with the MAC address of **0C:CF:89:66:60:47** as an example. When you use, please refer to the MAC address on the rear panel of your own gateway.
- In this guide, the dark orange content such as **“Network → Wireless AP”** indicates it is a function or setting on the Web GUI.

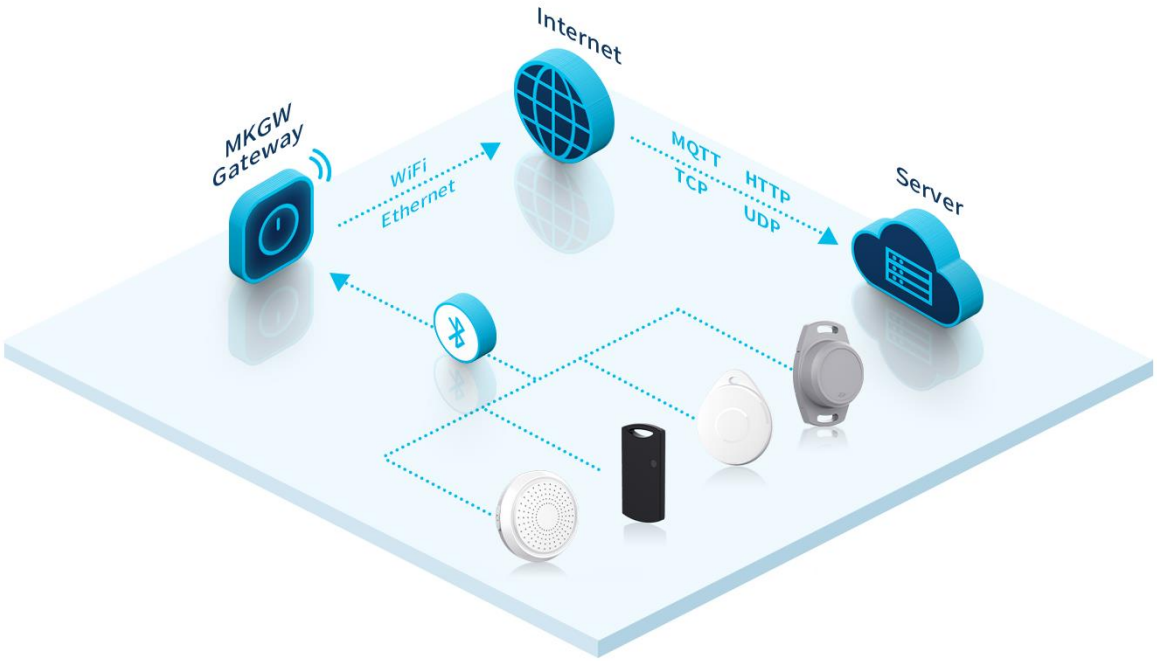
Table of Contents

List of Figures

1. Overview

MKGW1-BW Pro is a multi-wireless IoT Gateway with Bluetooth Low Energy (BLE) and Wi-Fi. It is based on the innovative integration of ***Nordic Semiconductor*** nRF52833 and ***MediaTek*** MT7688/MT7628 platform. This enables the MKGW1-BW Pro Gateway to support Bluetooth 5 features like Coded PHY (Long range), 2M PHY as well as IEEE 802.11b/g/n 2.4Ghz Wi-Fi and 10/100 FE PHY Ethernet. MKGW1-BW Pro captures multiple BLE peripherals information (such as *Apple iBeacon*, *Google Eddystone* and *MOKO Beacon*) and sends the data to Internet MQTT/HTTP server or local TCP/UDP server.

User can configure Bluetooth and server connection features through a simple and user-friendly Web GUI (Gateway User Interface). It makes the configuration easy and helps users to develop a fully featured IoT solution quickly.



1.1 Features

- Support Bluetooth 5 – 1M/2M PHY, Coded PHY (long range)
- Legacy 802.11b/g and HT 802.11n modes
- Support Ethernet and Wi-Fi to connect the Internet
- Support 5V Micro USB/9-15V DC/IEEE802.3af PoE power supply
- 4.2dBi gain Bluetooth antenna and 5dBi gain Wi-Fi antenna
- Bluetooth scanning up to 150m in the open area (1M PHY) and 319 BLE advertisement packets per second
- Support MQTT (SSL & Proxy)/HTTP (SSL/TLS)/TCP/UDP network protocols
- Support AWS IoT/Azure IoT/Google Cloud/Alibaba Cloud IoT platforms
- Support filtering *Apple iBeacon*, *Google Eddystone* and *MOKO Beacon* protocols intelligently
- Bluetooth device data filtering by regular expression

- Support uploading Beacon data by using JSON or hexadecimal data format
- Support cloud remote controlling and communicating with Bluetooth peripheral through the gateway
- Support cloud remote monitoring and configuring gateway (Cloud Management)
- Offline data storage in external USB flash drive
- Firmware upgrade via OTA (over-the-air) or USB flash drive

1.2 Applications

- iBeacon, Eddystone and other BLE Beacons receiver for location and navigation
- Real time location system (RTLS)
- Personnel/Livestock/Asset management and tracking
- Cold chain monitoring and alarming,
- Geofencing applications
- Anti-theft alarming
- Advertisement promotion
- Smart home and smart buildings
- Industrial automation
- Remote (Cloud) real-time operations and processing of Bluetooth IoT devices

2. Getting to Know MKGW1-BW Pro Gateway

2.1 What's in the Box

You will find the following items in the packaging box:

Table 1: MKGW1-BW Pro gateway packaging list

Item	Qty	Remark
MKGW1-BW Pro	1	Gateway
1meter Micro USB cable	1	Micro USB power cable
PET positioning sticker	1	Position the screws when installation
KA 3.5x25mm screws	2	Fix the gateway on the wall
Plastic wall plug	2	Drilled into the wall to hold screw

Figure 1: Packaging of MKGW1-BW Pro gateway

2.2 Appearance

2.2.1 Dimensions

The gateway's dimensions shown in the figure below:

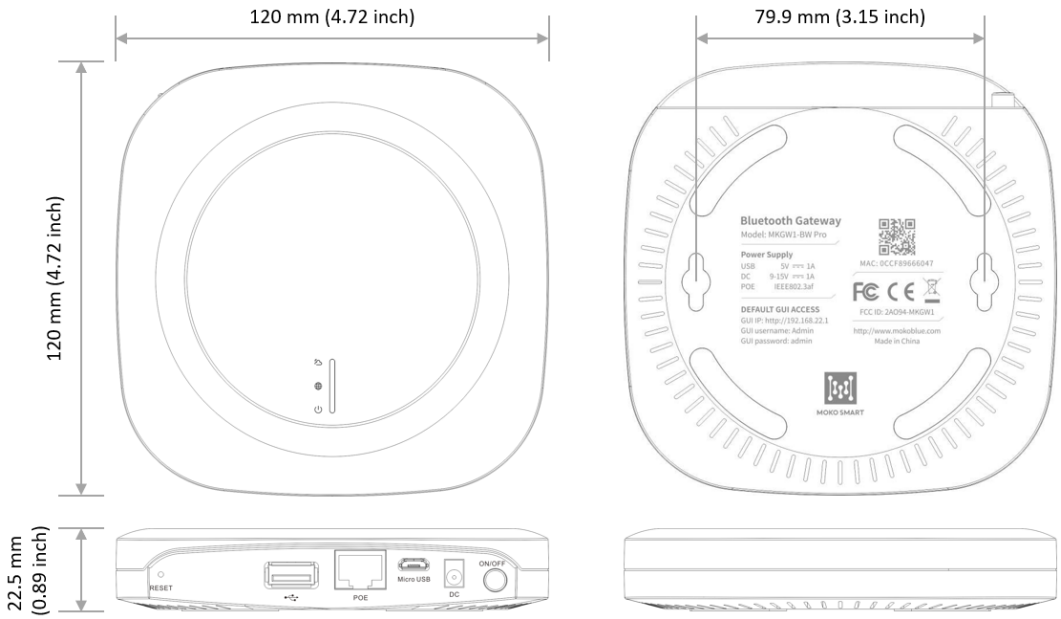
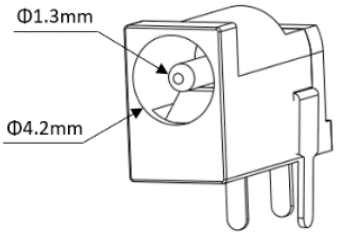


Figure 2: Dimensions of MKGW1-BW Pro gateway

2.2.2 Buttons and Ports

The gateway's buttons and ports include those shown in the figure below:

Figure 3: Buttons and ports of MKGW1-BW Pro gateway



- **Power supply ports** – Three different power supply ports for user to power up the gateway.
  - RJ45 PoE port: IEEE 802.11af standard
  - Micro USB port: standard 5V/1A (at least 0.5A) power supply
  - DC port: standard 9 - 15V/1A (at least 0.5A) power supply. The specification of the DC port is 4.2mm x 1.3mm male DC jack. It needs a female DC-IN plug to connect.
- **Power On/Off button** – Push the button to turn on or turn off the gateway.
- **Reset button** – Insert a needle-like object into the hole and long press the button to reset the gateway.
- **USB flash drive port** – For connecting an external USB flash drive. USB flash drive can be used to store offline data, certificate files, upgrade file and backup file. Gateway can load the files when needed.

2.2.3 Rear Panel

The rear panel of the gateway has laser printing text and graphics that contains important information to set-up the gateway.

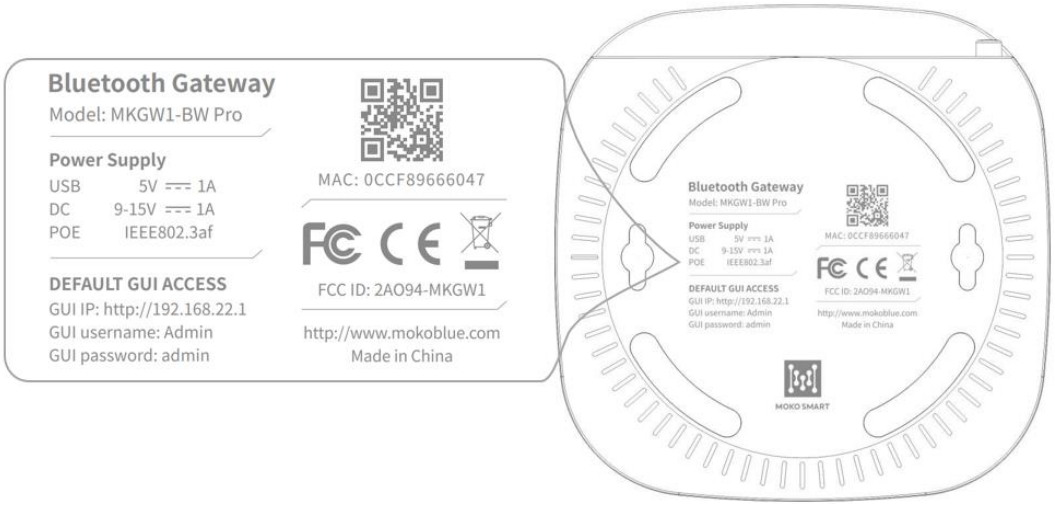


Figure 4: Laser printing text and graphics on the rear panel of MKGW1-BW Pro gateway

- **QR code (MAC address)** – The QR code is the MAC address of the MKGW1-BW Pro gateway. Each gateway has a unique MAC address.
- **GUI IP** – The default WLAN IP address of the gateway. You can use the IP address to access the Web GUI.
- **GUI username and GUI password** – The username and password to log in to the Web GUI when configuring the gateway. The username is fixed as "**Admin**". The password is modifiable and the initial password is "**admin**".

> ***Customization:*** *In mass production, laser printing text and graphics can be customized according to customer's requirements.*

2.2.4 LED Indicators

There are three RGB LEDs to indicate the gateway's status of power, network and system.

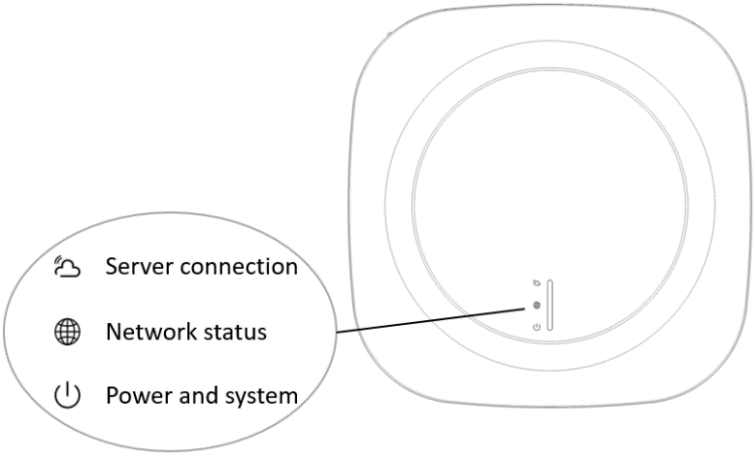


Figure 5: LED indicators of MKGW1-BW Pro gateway

The description of the gateway's LED indicators status is shown in the table below:

Table 2: Status of the gateway's LED indicators

Power and system	Network status	Server connection	Gateway status
Off	Off	Off	Not powered
Solid YELLOW	Solid YELLOW	Solid YELLOW	Gateway is booting or restarting.
Solid GREEN			Power is normal and gateway is ready.
	Solid YELLOW		No network or network communication error
	Solid BLUE		Internet access by using Wi-Fi and the network connection is ready.
	Solid GREEN		Internet access by using Ethernet and the network connection is ready.
		Solid YELLOW	No server connection or server connection error.
		Solid GREEN	Server connection is ready.
		Blinking GREEN	Data communication is normal. Gateway is transmitting or receiving data with server.
Blinking YELLOW twice	Blinking YELLOW twice	Blinking YELLOW twice	Reset the gateway successfully.
Blinking GREEN	Blinking GREEN	Blinking GREEN	Gateway's Wi-Fi firmware is upgrading.
Blinking BLUE	Blinking BLUE	Blinking BLUE	Gateway is restoring the backup file.
Blinking GREEN twice every 5 seconds			External USB flash drive is connected and ready.
Solid RED			Bluetooth function error

2.3 IoT Functions

2.3.1 Cloud Collecting BLE Beacons

MKGW1-BW Pro gateway is able to scan the advertisement packets of BLE Beacon or other Bluetooth peripherals around and upload the packets to your server via MQTT, HTTP, TCP or UDP network protocol.

The gateway has a variety of filtering strategies to enable you easily and real-time to get the message of your target Bluetooth Beacons, and reduce the interference of other invalid Bluetooth data. The gateway also has the ability to identify the common BLE Beacon protocols such as ***Apple iBeacon***, ***Google Eddystone*** and ***MOKO Beacon***, and can parse the identifiers from the raw advertisement packets. The BLE Beacon advertisement packets transmitted to the Cloud Server can be decoded in JSON array format or hexadecimal format. These can help you achieve a smart IoT monitoring application.


```
[ {
  "TimeStamp" : "2021-08-27T02:08:41.012Z",
  "Format" : "Gateway",
  "GatewayMAC" : "0CCF89666047"
}, {
  "TimeStamp" : "2021-08-27T02:08:33.176Z",
  "Format" : "iBeacon",
  "BLEMAC" : "DF0EB932DA96",
  "RSSI" : -83,
  "AdvType" : "Legacy-adv",
  "UUID" : "E2C56DB5DFFB48D2B060D0F5A71096E0",
  "Major" : 0,
  "Minor" : 15,
  "RSSI@1m" : -65
}, {
```


Figure 6: An example of Apple iBeacon packet transmitted to an MQTT Broker in JSON array format

2.3.2 Cloud Controlling Bluetooth Device

If you want to remotely control your Bluetooth smart device through the Cloud Server and get the returned messages, MKGW1-BW Pro gateway can help achieve this. Receiving the connection command from the Cloud Server, the gateway can scan and connect the specifical Bluetooth device, and then the two-way communication between your Bluetooth device and the Cloud Server will be set up by the gateway. This can achieve an IoT application of cloud monitoring and controlling Bluetooth peripherals.

Note: *This function is only available when using* ***MQTT*** *protocol by now, and the Bluetooth smart device need to use MOKO series Bluetooth module as the Bluetooth communication role. Contact MOKO SMART sales team for more information about MOKO series Bluetooth module.*

2.3.3 Cloud Monitoring and Configuring the Gateway

The following chapters will introduce the configuration method via the Web GUI, but after you connect the gateway to an **MQTT Broker** successfully, you can also use cloud management commands to monitor the status and set the parameters of the gateway remotely. We call this function **Cloud Management**. This can help you deploy and control the gateway on a large scale without too much manpower via cloud.

3. Getting Started

3.1 Position the Gateway

For the best wireless signal transmission between the gateway and the Bluetooth devices and between the gateway and the server:

- Place the gateway in a central area.
- Keep the gateway away from metal obstructions and away from direct sunlight.
- Keep the gateway away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.

3.2 Install the Gateway

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

Step 1: Use 5mm drill head, drill 2 holes on the wall according to the PET positioning sticker.

Step 2: Push or tap the plastic wall plugs into the holes, flush with the plaster.

Step 3: Put the screw into the wall plug, twisting the screw a tiny bit by hand or screwdriver till it bites. Do not insert the screw completely into the wall plug as a portion of the screw head must be exposed (no less than 3mm) to hang the gateway.

Step 4: Insert the screw heads into the hanging hole behind the gateway, then gently pull down to complete the installation.

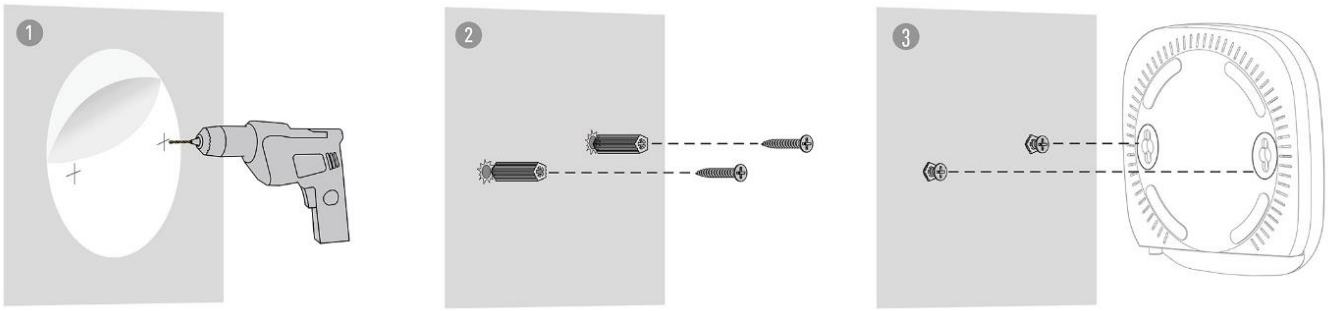


Figure 7: Installing the gateway on the wall

3.3 Power up the Gateway

After installation, please refer to ***Chapter 2.2.2*** to select the compliant cable and adapter to power up the gateway. You only need to select one power supply method to use.

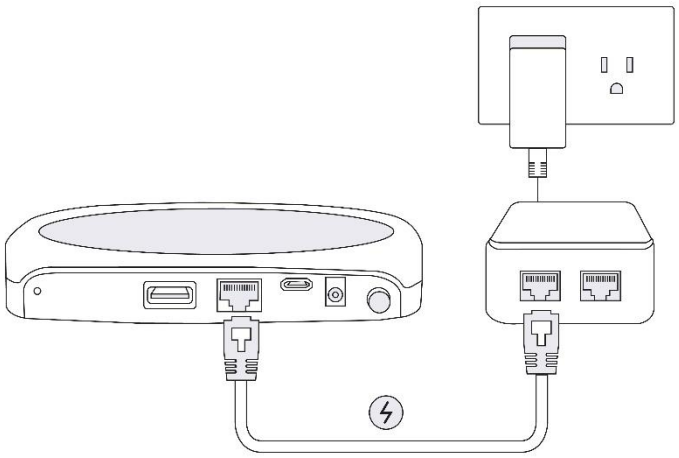


Figure 8: Power up the gateway through PoE adapter

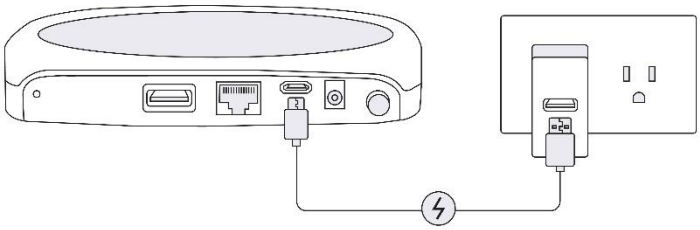


Figure 9: Power up the gateway through Micro USB

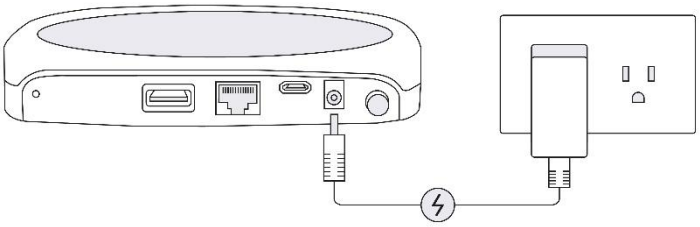


Figure 10: Power up the gateway through DC plug

> ***Note:*** *MKGW1-BW Pro gateway contains a Micro USB cable and does not provide Ethernet cable, DC cable and adapter. User needs to prepare a compliant cable and adapter to connect the gateway.*

After the gateway is powered on, it needs to push-down the power on/off button to start the gateway. The LED indicators will light when the gateway starts to work.

The gateway will automatically work if you have set all the parameters of the Network, Server and Bluetooth. If it is the first time to use the gateway, you need to refer to the following chapter to set up the gateway.

4. Access the Web GUI

You can configure the gateway's Network Connection, Server Access, Bluetooth and System Settings by using the Web Gateway User Interface (Web GUI). All the parameters will be stored and the gateway can start to work automatically after it reboots.

MKGW1-BW Pro has three methods to access the Web GUI, one is to connect the Wi-Fi of the gateway and then access the Web GUI via WLAN IP address, the gateway has enabled the AP function by default and is pre-set with the WPA2 security, but you should immediately modify the default password as well as the Web GUI login password. The other two methods are to connect the gateway with a computer or router by using a network cable and then visit the IP address to access the Web GUI.

4.1 Access the Web GUI via Wi-Fi

You need to prepare a computer or smartphone which has the IEEE 802.11b/g/n wireless capability and is configured to obtain an IP address automatically. Follow the steps below to connect to the gateway and access the Web GUI.

Step 1: Turn on the gateway and wait for about 1 minute until the gateway system is ready (the power and system LED turns green).

Step 2: Use a computer or smartphone to scan the available Wi-Fi networks around.

Step 3: Select the gateway's SSID (Wi-Fi name) **MKGW1-BW-XXXX** (XXXX represents the last 4 characters of the gateway's MAC address, you can find the MAC address on the label attached to the rear panel of the gateway).

Figure 11: Gateway's SSID (Wi-Fi name)

Step 4: The default password is "**Moko4321**". For security reasons, it is recommended to modify the Wi-Fi password or turn off the AP function of the gateway after your configurations.

Step 5: Open the web browser (we suggest the web browser such as *Microsoft Edge*, *Firefox*, *Safari* or *Google Chrome*) and type the gateway's WLAN IP address **192.168.22.1** (by default), and then the Web GUI will be loaded.

> ***Configuration:*** *Modify the default parameters.*
> *Go to* ***Network → Wireless AP*** *Web GUI page to modify the SSID (Wi-Fi name), password and the WLAN IP address.*

4.2 Access the Web GUI via Ethernet

4.2.1 Connect the Gateway to a Computer

User can visit the static IP address **192.168.253.253/24** to access the Web GUI of the gateway and the static IP address can be enabled or disabled by single clicking the reset button. Every time you power off the gateway, the static IP will be disabled, that means if you want to use the static IP address when you use the gateway for the first time or restart the gateway, you need to click the reset button to enable it.

Step 1: Use a network cable to connect the PoE port of the gateway to a computer.

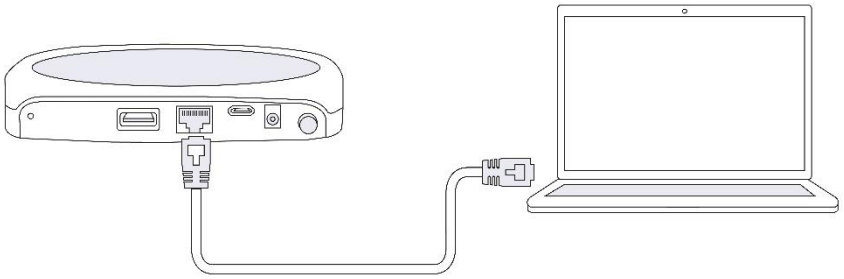


Figure 12: Connect the gateway to a computer via network cable

Step 2: Set the Ethernet IPv4 address of the computer to make it on the same subnet as the gateway, such as **192.168.253.10.**

Step 3: Specify the Subnet Mask of the computer as **255.255.255.0**.

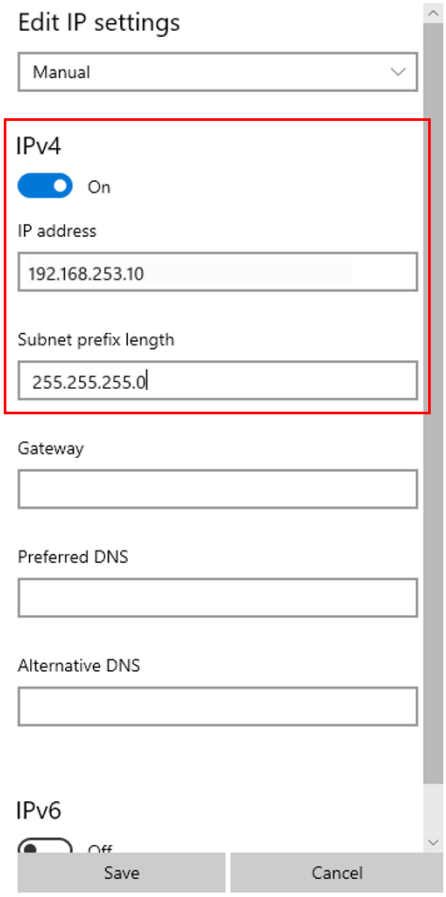


Figure 13: Set the IP address and the Subnet Mask of the computer

Step 4: Type the gateway's static IPv4 address **192.168.253.253** on the web browser of the computer after the static IP address of the gateway has been enabled, and then the Web GUI will be loaded.

4.2.2 Connect the Gateway to a Router or Switch

Use an ethernet cable to connect the PoE port of the gateway with a router or switch and then make your computer in the same Local Area Network (LAN) with the gateway. And then you can access the Web GUI by using the computer to visit the IP address of the gateway.

You need to view the Address Resolution Protocol (ARP) lists (lists of IP addresses corresponding to MAC addresses) to find the IP address of the gateway. The following example describes the method of using ***"ARP-SCAN"*** (an IP scanner tool) to scan the network to find the IP address.

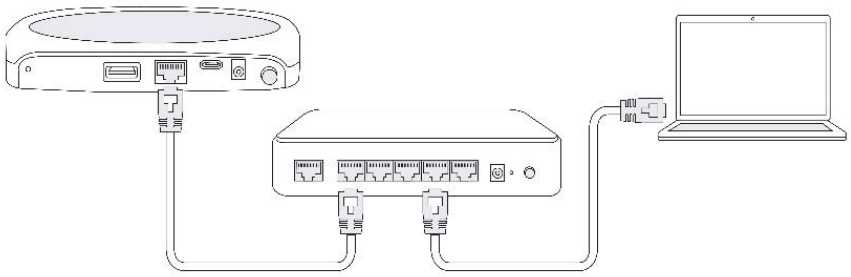


Figure 14: Making the gateway in your Local Area Network (LAN)

> ***Contribution:*** *How to make your computer in a same local area network.*
> *For example:*
> *- Connect the computer's network port to the router or switch which is connected with the gateway*
> *- Connect the computer to the Wi-Fi of the wireless router which is connected with the gateway through Ethernet cable.*

Follow the steps bellow to find the IP address of the gateway (the following steps are operated on ***Windows OS***):

Step 1: Open the CMD window in the path where the "***ARP-SCAN.exe***" file is stored.

Step 2: Type "**ipconfig**" and press the Enter key to obtain the upstream network device's parameters. Note down the *Subnet Mask* and the *Default Gateway IP address*. In the example figure below, the Subnet Mask is 255.255.255.0 and the Default Gateway IP address is 10.0.0.1.

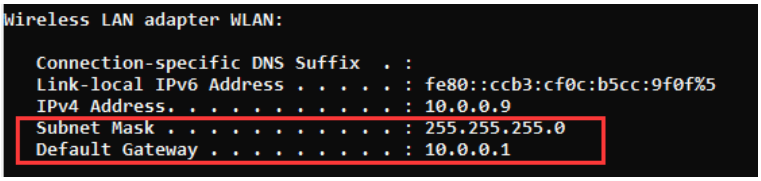


Figure 15: Network parameters on Windows CMD window

Step 3: Type the command "**arp-scan -t 10.0.0.1/24**" and note down the IP address which is corresponding to the gateway's *MAC address* on the IP address lists. In the figure below, the MAC address is 0C:CF:89:66:60:47 and the IP address is 10.0.0.21**.**

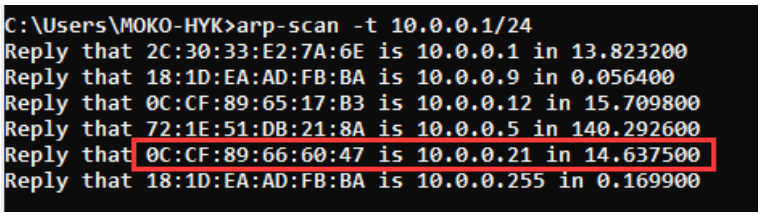


Figure 16: ARP lists of the Network

The command "**arp-scan -t -10.0.0.1/24" -** "**10.0.0.1**" refers to the default gateway IP address and the "**24**" refers to the CIDR (Classless Inter-Domain Routing) number of the subnet mask.

The CIDR number comes from the number of ones in the subnet mask when converted to binary. The common subnet mask 255.255.255.0 is 11111111.11111111.11111111.00000000 in binary. This adds up to 24 ones, hence /24. A subnet mask of 255.255.255.192 is 11111111.11111111.11111111.11000000 in binary, adds to 26 ones, hence /26.

Step 4: Open the web browser and type the gateway's WAN IP address **10.0.0.21** (the example above), and then the Web GUI will be loaded.

Contribution: *ARP-SCAN tools for Network scanning*
1. Download the "arp-scan.exe" file for Windows OS from the link:
https://cloud.mokosmart.com/index.php/s/j6BrkMTEEF5Kdtm
2. For more information about ARP-SCAN tool on Linux or MacOS, refer to the link:
http://www.royhills.co.uk/wiki/index.php/Arp-scan_Documentation

4.3 Log in to the Web GUI

You can log in to the Web GUI by using the default user name: **Admin** and password: **admin**. For security reasons, it is recommended to modify the password after your configurations. If there is no any operation within 1 hour, the gateway will automatically sign out of the Web GUI.

Figure 17: Log in to the Web GUI

Configuration - *Modify the default parameters.*
Go to ***System → Device Settings - Login*** *setting to modify the login password.*

4.4 Home Page of the Web GUI

After login, the gateway comes with an intuitive Web GUI that allows you to easily setup and check all parameters.

The home page of the Web GUI displays the status of the gateway. The following figure shows the **Status** page, which contains two sections: **Device Status** and **Network Status**. Contents on this page will be refreshed when some of your configurations take effect.

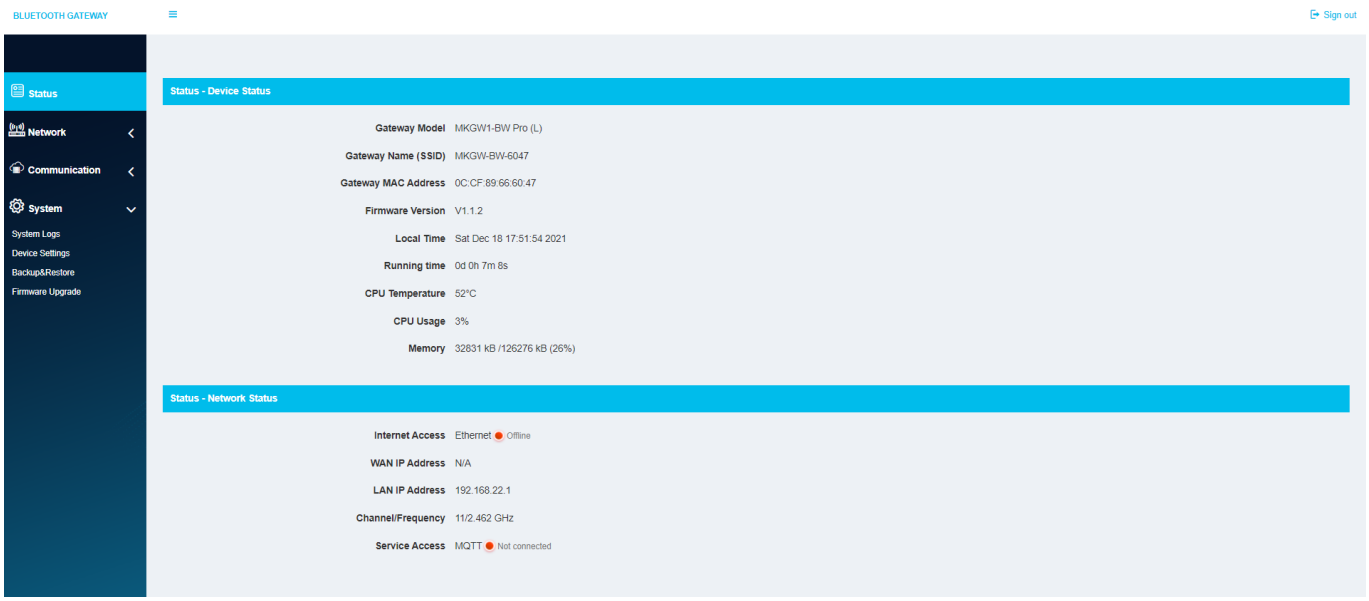


Figure 18: Gateway Status page on the Web GUI

5. Set up an Internet Connection

The gateway can access the Internet via network cable (Ethernet) or Wi-Fi. It is able to configure the Internet connection function on the **Network → Internet Access** page of the Web GUI. The factory default of the gateway is to use Ethernet to connect the Internet.

After the network configuration is completed, wait for the gateway to access the network. You can check the network status on the **Status** page of the Web GUI and also can check the network LED indicator.

5.1 Internet Connection via Ethernet

Follow the steps below to access an Internet connection via Ethernet.

Step 1: Use an Ethernet cable to connect the PoE port of the gateway to a network device such as router or switch that is connected to the Internet. the gateway will search the network and get the WAN IP address automatically (DHCP) when using Ethernet.

Step 2: On the **Network → Internet Access** page of the Web GUI, select the **Ethernet** from the **Internet Access Mode** drop-down menu, and then click the **Save&Apply** button at the bottom to restart the network and make the configuration take effect.

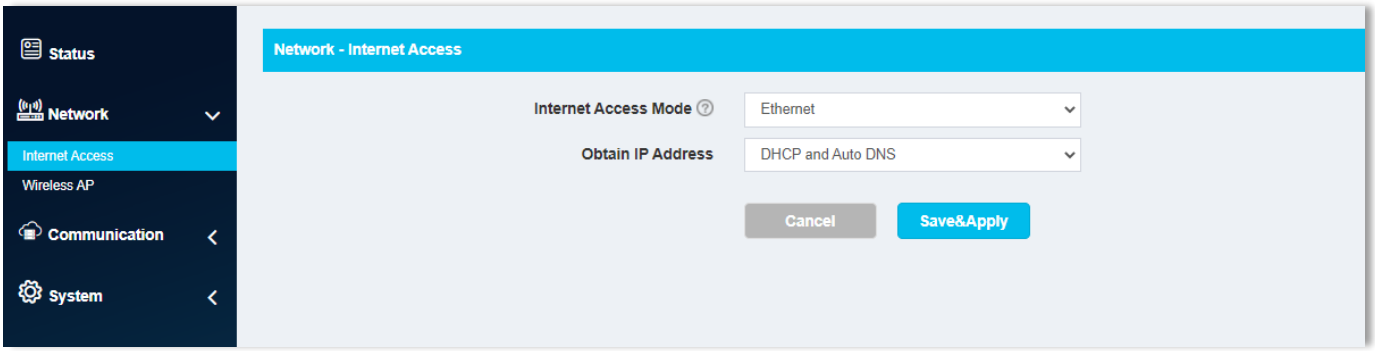


Figure 19: Internet Connection via Ethernet

Note: *By default, the gateway is pre-set with the Ethernet to access the Internet connection and enables the DHCP and Auto DNS to obtain IP and DNS addresses dynamically.*

5.2 Internet Connection via Wi-Fi

5.2.1 Add a Wi-Fi Connection

On the **Network → Internet Access** page of the Web GUI, selecting the **WLAN** from the **Internet Access Mode** drop-down menu can set the gateway to access an Internet connection via Wi-Fi from a wireless router.

There are two ways to add a Wi-Fi hotspot for the gateway to connect, one is to set all the router's network parameters manually and the other is to choose a Wi-Fi hotspot and obtain some general parameters automatically by the gateway.

Follow the steps below to add a Wi-Fi hotspot:

Step 1: You can type the router's Wi-Fi name in the input box of the **SSID** or click the icon to scan the surrounding Wi-Fi hotspots automatically, and then the Web GUI page will display a table list of the general information of the surrounding Wi-Fi hotspots.

SSID	BSSID	Channel	Signal(%)	Security
MOKO	08:68:8d:52:1f:e9	13/2.472 GHz	24	WPAWPA2-PSK[AES]
MOKO	08:68:8d:51:82:96	13/2.472 GHz	100	WPAWPA2-PSK[AES]
lala	26:13:79:36:84:27	13/2.472 GHz	81	WPA2-PSK[AES]
7777777	c0:a5:dd:2a:b4:a1	13/2.472 GHz	31	WPAWPA2-PSK[AES]
LieBaoWiFi964	26:6a:6a:42:65:b5	11/2.462 GHz	99	WPA2-PSK[AES]
zhang	2a:6f:38:09:4d:5d	11/2.462 GHz	86	WPA2-PSK[AES]
DIRECT-WLLAPTOP-7G0QS32UmsJs	de:b0:da:b4:00:53	11/2.462 GHz	76	WPA2-PSK[AES]
newfitpolo	2c:30:33:e2:7a:6e	10/2.457 GHz	100	WPA-PSK[TKIP]+WPA2-PSK[AES]

Figure 20: Surrounding Wi-Fi hotspots

Step 2: If you select one Wi-Fi hotspot from the table list, the web page will be filled with SSID (Wi-Fi name), BSSID (Wi-Fi MAC address) and the security type automatically.

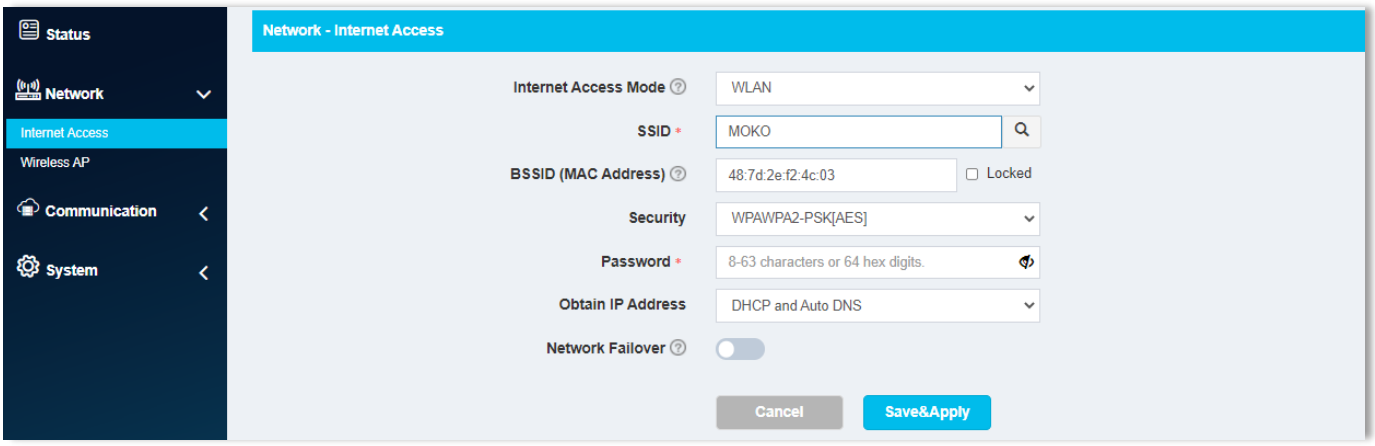


Figure 21: Adding a Wi-Fi hotspot

BSSID (MAC Address) - If you want the gateway will connect to the only corresponding Wi-Fi hotspot according to the SSID and the BSSID (MAC address), you can check the **Locked** box. As you manually set the Wi-Fi hotspot's parameters and want to use BSSID function, you need to type the right BSSID of the hotspot and check the **Locked** box.

Step 3: Select the security and encryption type of the Wi-Fi hotspot from the **Security** drop-down menu and type the password in the input box of **Password**. The gateway supports WEP, WPA, WPA2, and mixed WPA/WPA2 security types and AES, TKIP, and mixed TKIP+AES encryption types.

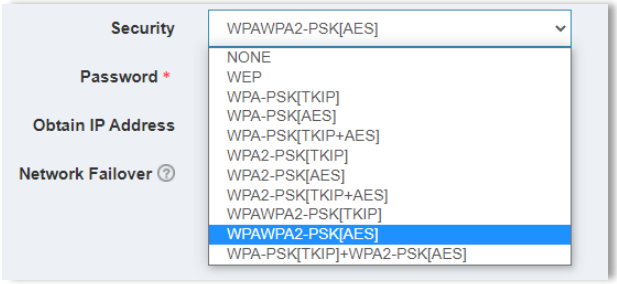


Figure 22: Security and encryption types supported by the gateway

Step 4: Click the **Save&Apply** button at the bottom in the page to restart the network and make the configuration take effect.

After you have set the gateway to connect the Internet via Wi-Fi, the gateway will automatically scan and connect the Wi-Fi hotspot every time you restart it.

5.2.2 Network Failover

You must have noticed the **Network Failover** switch at the bottom of the Web GUI page. When you active this switch, it will enable the functions of switching the Wi-Fi hotspots and checking the network communication. Network failover is a backup network mode that automatically switches to an available network if the ever one fails, it is an extremely important function for critical systems that require always-on Internet accessibility.

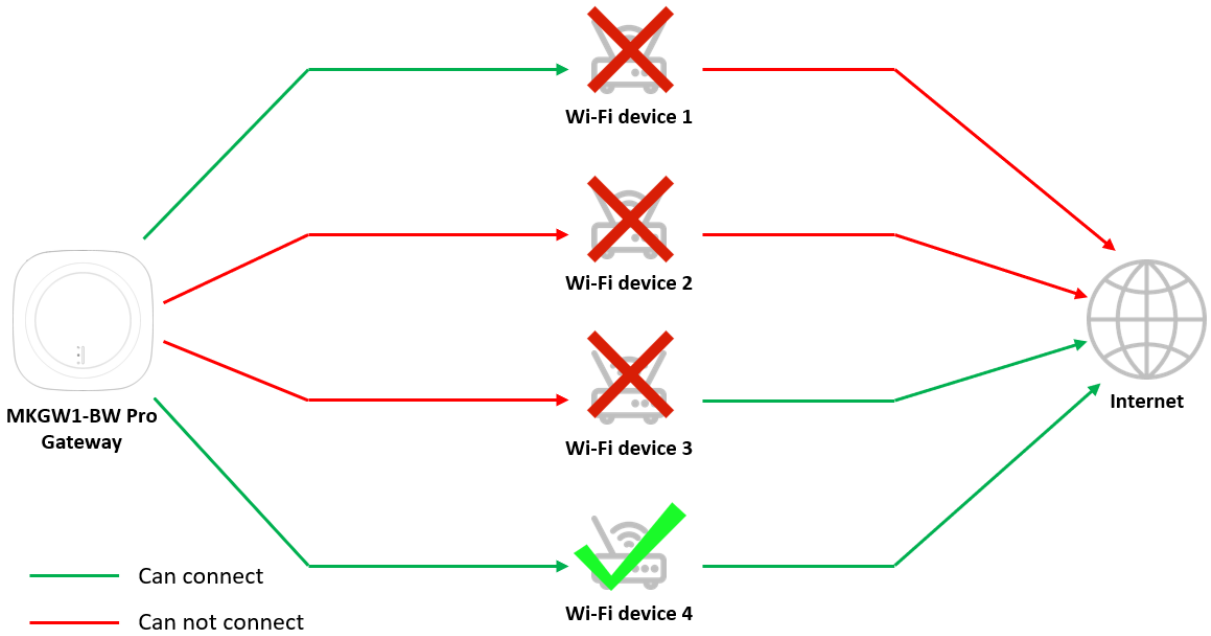


Figure 23: Diagram of Network Failover

- The **Network Failover** table list displays the Wi-Fi hotspots those have been saved and applied ever, and the gateway will select the available hotspot to connect to the Internet. Up to 4 historical hotspots can be recorded. If you have checked the **Locked** box of the **BSSID (MAC Address)** function, the list will show the BSSID value of the hotspot. The status bar will show which Wi-Fi hotspot is connected to the gateway.

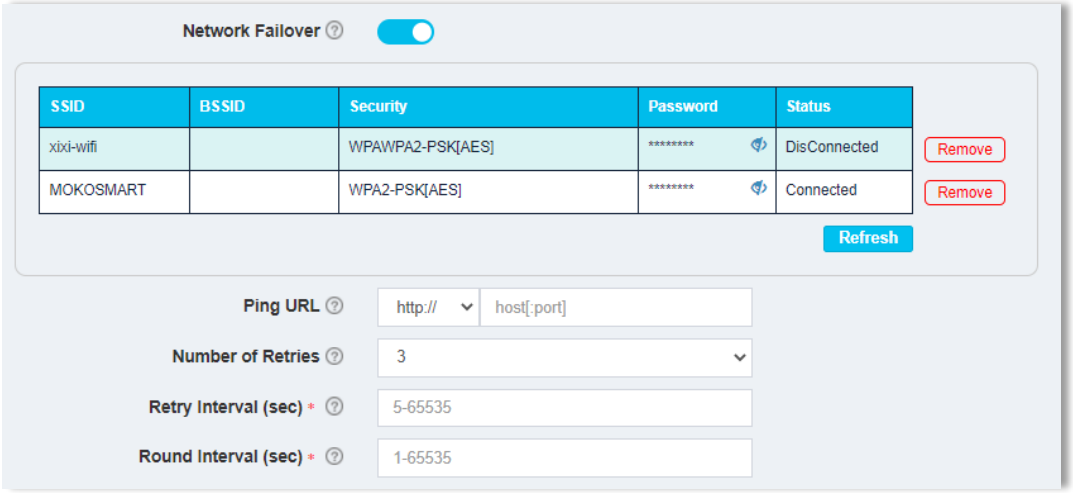


Figure 24: Configurations of Network Failover

- **Ping URL** – The gateway will use the URL to check the Internet connection and communication to verify the hotspot is available. In some cases, a successful network connection does not mean that the Internet traffic works well. If you set a URL link (you can use the common link such as *www.google.com*). If you leave the input box blank, the gateway will only check the connection between the gateway and the Wi-Fi hotspot instead of the Internet communication.

- **Number of Retries** – The number of retries for each time the gateway verifies that the current Wi-Fi hotspot is available. The number can be selected from the drop-down menu is from 3 to 8. For example, when you select 3, the gateway will verify a Wi-Fi hotspot 3 times, and if it fails all the 3 times, the gateway will switch to the next hotspot to check.

- **Retry Interval (sec)** – The interval between retries to check if one Wi-Fi hotspot is available. This value and the number of **Number of Retries** determine the maximum time required to check one Wi-Fi hotspot in one round. The unit of the interval is 1 second and the range is from 5s to 65535s.

- **Round Interval (sec)** – The gateway will stop checking the network if all Wi-Fi hotspots in the network failover list have failed. After the round interval, the gateway will start a new round to check the network of the Wi-Fi hotspots. The unit of the value is 1 second and the range is from 1s to 65535s.

5.3 Obtain IP Address

Whether using Ethernet or Wi-Fi to access the Internet, the **Obtain IP Address** setting allows you to reserve a static IP address and DNS address(es) for the gateway on the network, rather than being assigned a new (dynamic) IP address and DNS address(es) by the network device's (router or switch) DHCP Server every time the gateway connects to the network.

Static IP address can be useful for using various services on the local network. The gateway is identified by a unique MAC address, and the IP address can be bound to the MAC address.

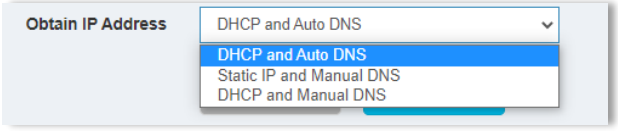


Figure 25: Selections of obtain IP address

There are three selections of this setting:

- **DHCP and Auto DNS** – The gateway obtains an IP address and DNS address(es) from the upstream network device's DHCP Server. The upstream network device connected to the gateway needs to enable the DHCP function.
- **Static IP and Manual DNS** – Once you select this option, you need to type the IPv4 address, Subnet Mask, Default Gateway IP address, and the DNS address(es) on the page.
  - **IPv4 Address** – This is the gateway's WAN IP address you need to specify when seen from the network. Be sure it is on the same network segment as the upstream network device and not occupied by other network devices.
  - **Subnet Mask** – This is the gateway's Subnet Mask, as seen by users on the network. Confirm it is the same as the subnet mask of the upstream network device.
  - **Default Gateway** – The private IP address assigned to the upstream network device. Sometimes your ISP (Internet Service Provider) can provide it.
  - **Primary DNS** & **Secondary DNS** – The Domain Name Server (DNS), is an Internet service that translates the domain names into IP addresses. Your ISP will provide you with at least one DNS (primary DNS).

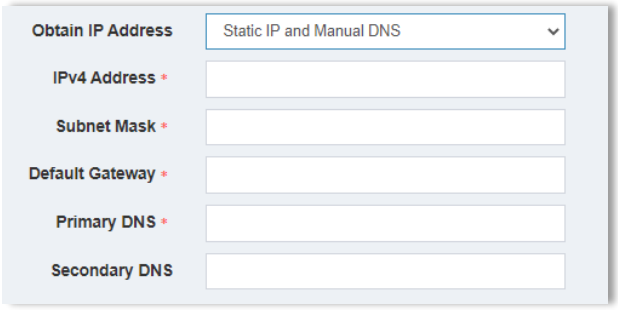


Figure 26: Obtain IP address - Static IP and Manual DNS

- **DHCP and Manual DNS** – The gateway obtains an IP address from the DHCP Server of the upstream network device, but the DNS address(es) needs to be typed manually.

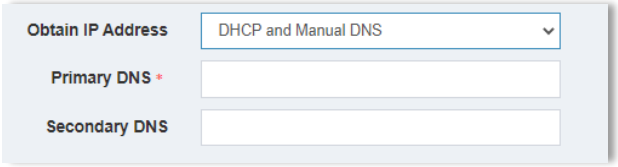


Figure 27: Obtain IP address - DHCP and Manual DNS

Caution: *If you have no experience with the networking, please leave the preference setting - **DHCP and Auto DNS**, otherwise it may cause the gateway offline.*

6. Collect Beacon Packets

MKGW1-BW Pro gateway can be as a Bluetooth Center Device to scan and discover the advertisement packets (ADV packets) of Bluetooth Low Energy (BLE) Beacons or other Bluetooth peripherals. The gateway provides multiple strategies to filter the Bluetooth packets and that can help you capture the required Bluetooth peripherals directly and easily. The gateway also has the Bluetooth 5 features and can be set to scan on 1M PHY, 2M PHY or Coded PHY (long range).

6.1 Filter Beacon Packets

When the gateway starts to work, it will constantly scan and listen on all Bluetooth ADV channels to pick up as many ADV packets as possible from surrounding Bluetooth peripherals. This will cause a lot of non-required data to occupy the network traffic and increase the difficulty of parsing them. Because of this, the gateway provides different strategies to filter the data to ignore the packets that does not match the filtering rules and only uploads the required packets to your server.

On the Web GUI **Communication → Bluetooth Scanning** page, set the scanning filter function and all the parameters will take effect immediately after the configuration is completed.

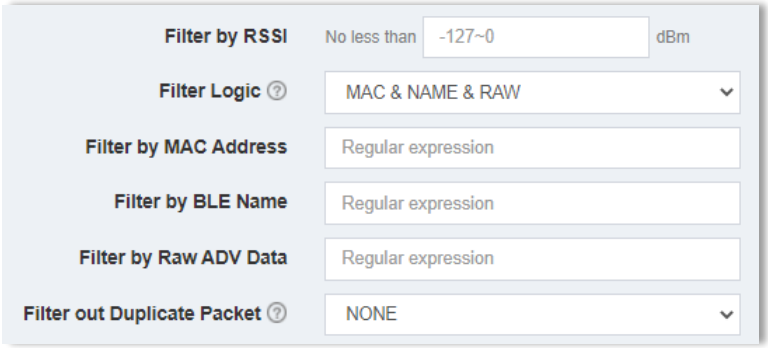


Figure 28: Configurations of Scanning Filter Settings

- **Filter by RSSI** – Only the ADV packet with RSSI not less than the filter value will be uploaded. This filter parameter has the highest priority and is not mandatory.

  Example: When setting the RSSI value to -70, the ADV packets with RSSI of -70dBm or greater than -70dBm will be uploaded to server.

- **Filter Logic** – This is "**OR**" and "**AND**" logical settings for filtering by MAC Address, BLE Name and Raw ADV Data.

  AND (&) – Both relations must be true for the complex expression to be true.

  OR (|) – If either relation is true, the complex expression is true.

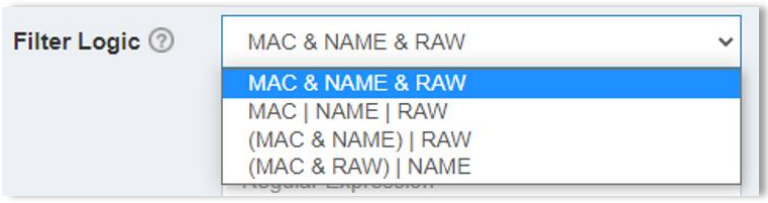


Figure 29: Selections of Filter Logic

- **Filter by MAC Address** – The regular expression to filter the MAC address of the Bluetooth peripherals. Only peripherals with the MAC address matching the expression will be uploaded to server.

  Example: Only uploading Beacons whose MAC address starts with "78 50 05", the regular expression can be ***"^785005.*"*** (without the quotation marks).

  Note: Only HEX values (in uppercase letters) can be recognized as MAC address.

- **Filter by BLE Name** – The regular expression to filter the Bluetooth name of the Bluetooth peripherals. Only peripherals with the Bluetooth name matching the expression will be uploaded to server.

  Example: Only uploading Beacons whose Bluetooth name starts with "MkiBeacon_", the regular expression can be ***"^MkiBeacon_.*"*** (without the quotation marks).

- **Filter by Raw ADV Data** – The regular expression to filter the raw advertisement packets of the Bluetooth peripherals. Only peripherals whose ADV packet data matching the expression will be uploaded to server.

  Example: Only uploading *Apple iBeacon* and the iBeacon UUID is E2C56DB5DFFB48D2B060D0F5A71096E0, the regular expression can be ***"^.*E2C56DB5DFFB48D2B060D0F5A71096E0.*"*** (without the quotation marks).

  Note: Only HEX values (in uppercase letters) can be recognized as raw advertising data.

> ***Link: Regular Expression*** *is extremely and amazingly powerful in searching and manipulating text strings. Know more about the reference of regular expression, refer to the links:*
> *https://www.regular-expressions.info/*

- **Filter out Duplicate Packet** – The gateway will filter out the ADV packet with the same content of the selected option as the ADV packet which has been uploaded once within an upload interval.

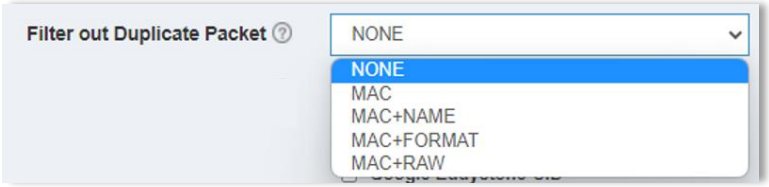


Figure 30: Selections of Filter out Duplicate Packet

  - **NONE** – Disable this function
  - **MAC** – Only check for the duplicate ADV packets according to the MAC address
  - **MAC+NAME** – Check for the duplicate ADV packets according to the MAC address and Bluetooth name
  - **MAC+FORMAT** – Check for the duplicate ADV packets according to the MAC address and Beacon format
  - **MAC+RAW** – Check for the duplicate ADV packets according to the MAC address and raw advertising data

  Example: When "**MAC+NAME**" is selected from the drop-down menu, and an ADV packet with the MAC address of AABBCCDDEEFF and Bluetooth name of MOKO001 has been uploaded once, the gateway will not upload the ADV packet with the same MAC address and BLE name again within an uploading interval. But if another ADV packet with the same MAC address of AABBCCDDEEFF and different BLE name of MOKO002, it will also be uploaded once.

6.2 Identify Beacon Protocols

There is a special and convenient filter function – **Filter and Parse Beacon Format**. That means the gateway will recognize and parse the identifiers of different Beacon protocol formats such as ***Apple iBeacon***, ***Google Eddystone (UID, TLM, URL)*** and ***MOKO Beacon*** and only upload the corresponding packets according to the checked options.

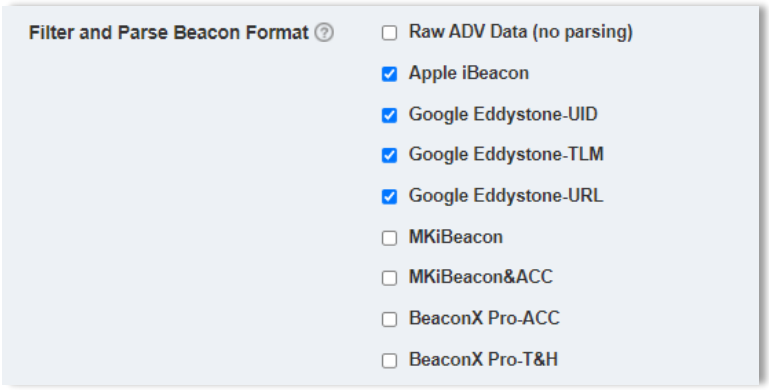
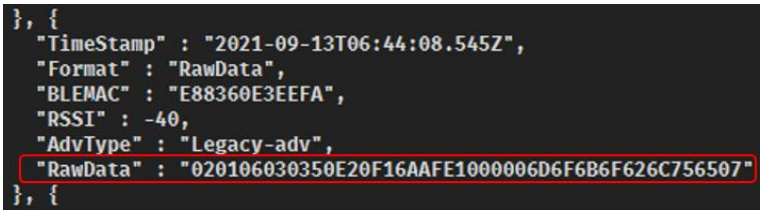


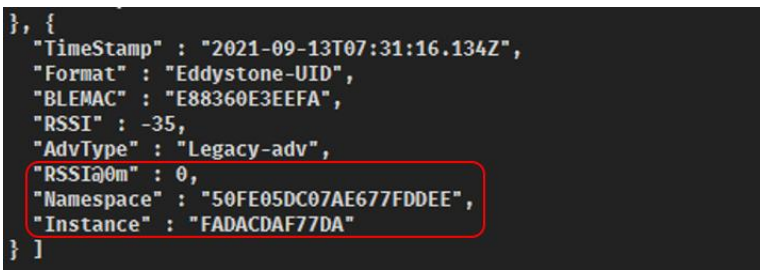
Figure 31: Beacon Formats supported to be filtered by the gateway

- **Raw ADV Data (no parsing)** – The gateway will upload the Bluetooth ADV packets scanned according to the filtering configuration and will not parse the structure of the raw ADV data. The figure below shows an example of raw advertising data in JSON array format.

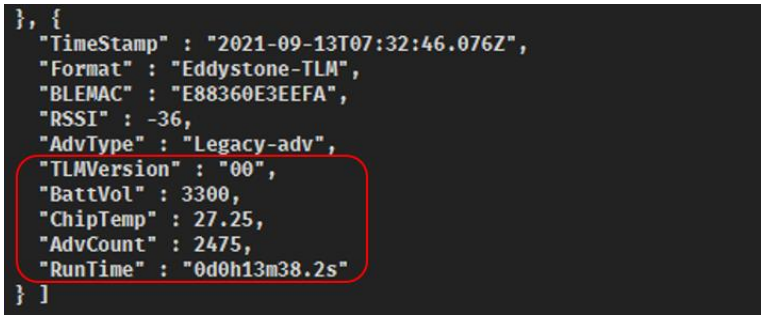


- **Apple iBeacon** – The gateway will identify the ***Apple iBeacon*** ADV packet and parse the structure of the packet into **UUID**, **Major**, **Minor** and **RSSI@1m**. The figure below shows an example of *Apple iBeacon* in JSON array format.

- **Google Eddystone-UID** – The gateway will identify the ***Google Eddystone-UID*** ADV packet and parse the structure of the packet into **RSSI@0m**, **Namespace ID** and **Instance ID**. The figure below shows an example of *Google Eddystone-UID* in JSON array format.

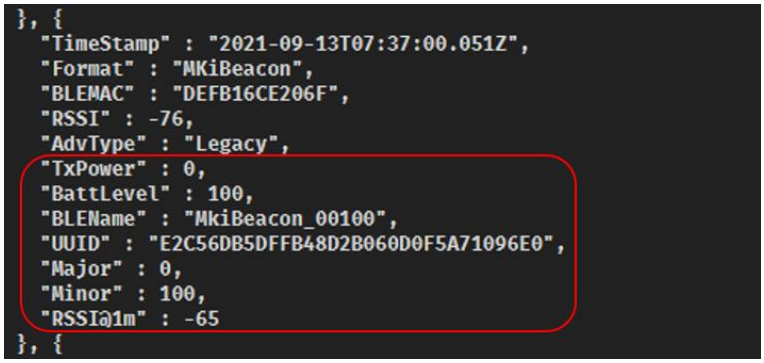


- **Google Eddystone-TLM** – The gateway will identify the ***Google Eddystone-TLM*** ADV packet and parse the structure of the packet into **TLM version**, **Battery voltage**, **Chipset temperature**, **Advertising counts** and **Beacon running time**. The figure below shows an example of *Google Eddystone-TLM* in JSON array format.



- **Google Eddystone-URL** – The gateway will identify the ***Google Eddystone-URL*** ADV packet and parse the structure of the packet. The figure below shows an example of *Google Eddystone-URL* in JSON array format.

- **MKiBeacon** – It is one Beacon type of ***MOKO Beacon***. The gateway will identify the ***MKiBeacon*** ADV packet and parse the structure of the packet. The figure below shows an example of *MKiBeacon* in JSON array format.



- **MKiBeacon&ACC** – It is one Beacon type of ***MOKO Beacon*** and can work with 3-axis accelerometer sensor. The gateway will identify the ***MKiBeacon&ACC*** ADV packet and parse the structure of the packet. The figure below shows an example of *MKiBeacon&ACC* in JSON array format.

- **BeaconX Pro-ACC** – It is one type of ***MOKO Beacon*** and can work with 3-axis accelerometer sensor. The gateway will identify the ***BeaconX Pro-ACC*** ADV packet and parse the structure of the packet. The figure below shows an example of *BeaconX Pro-ACC* in JSON array format.

```
}, {
  "TimeStamp" : "2021-09-13T07:37:59.546Z",
  "Format" : "BXP-ACC",
  "BLEMAC" : "E88360E3EEFA",
  "RSSI" : -39,
  "AdvType" : "Legacy-adv",
  "TxPower" : 0,
  "RSSI@0m" : 0,
  "AdvInterval" : 1000,
  "BattVoltage" : 3300,
  "DataRate" : 10,
  "Scale" : "2g",
  "3-axisData" : "FB00,FDC0,3FC0"
}, {
```


- **BeaconX Pro-T&H** – It is one type of ***MOKO Beacon*** and can work with temperature&humidity sensor. The gateway will identify the ***BeaconX Pro-T&H*** ADV packet and parse the structure of the packet. The figure below shows an example of *BeaconX Pro-T&H* in JSON array format.


```
}, {
  "TimeStamp" : "2021-09-13T06:44:08.418Z",
  "Format" : "BXP-T&H",
  "BLEMAC" : "E88360E3EEFA",
  "RSSI" : -40,
  "AdvType" : "Legacy-adv",
  "TxPower" : 0,
  "RSSI@0m" : 0,
  "AdvInterval" : 1000,
  "BattVoltage" : 3283,
  "Temperature" : 29.299999,
  "Humidity" : 54.400002
}, {
```


Note:

*1. If **Raw ADV Data (no parsing)** and other options are checked, for example, **Raw ADV Data (no parsing)** and **Apple standard iBeacon**, the gateway will identify and parse the Apple iBeacon ADV packet and upload it in Apple iBeacon format. It will also upload all other advertisement packets (excluding the Apple iBeacon) in raw data format.*

*2. **MOKO Beacon** is a series Beacon products designed by **MOKO SMART**, and it has a variety of models and Beacon formats. You can contact MOKO SMART sales team for more information about MOKO Beacon.*

6.3 Bluetooth Scan Settings

AT the bottom of **Communication → Bluetooth Scanning** page on the Web GUI, you can view **Bluetooth Scan Settings** to set the scanning parameters. This can enable the Bluetooth 5.0 feature like Coded PHY (long range). All the parameters will take effect immediately after the configuration is completed.

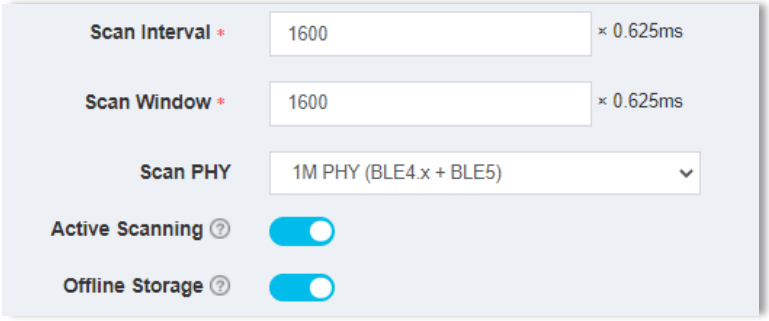


Figure 32: Bluetooth Scan Settings

- **Scan Interval / Scan Window** – The **Scan Interval** and the **Scan Window** are usually used together. Scan Window is the duration in which the Bluetooth Link Layer scans on one channel and Scan Interval is the interval between the start of two consecutive scan windows. When the values of Scan Interval and Scan Window are equal, the gateway will always keep scanning (duty cycle is 100%).

  The range of the two parameters is 2.5ms to 10s and the default value is 1s (1600x0.625ms, it is not recommended to change). The following figure visually shows the Scan Interval and Scan Window.

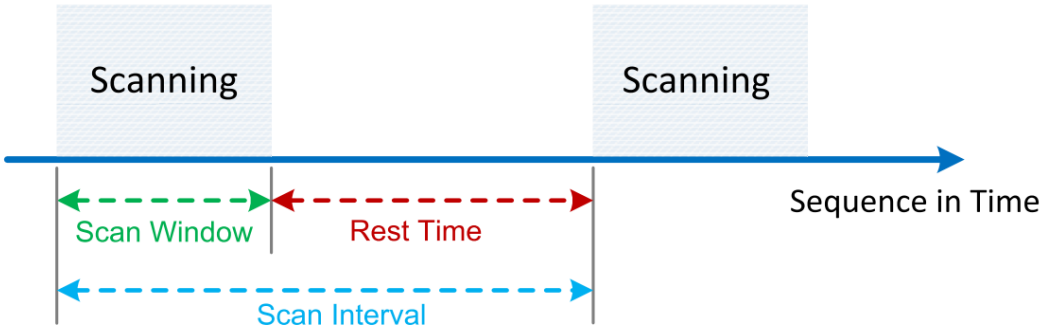


Figure 33: Scan Interval and Scan Window

- **Scan PHY** – The gateway supports to switch its scan physical layer (PHY) to scan for the ADV packets on different PHYs.

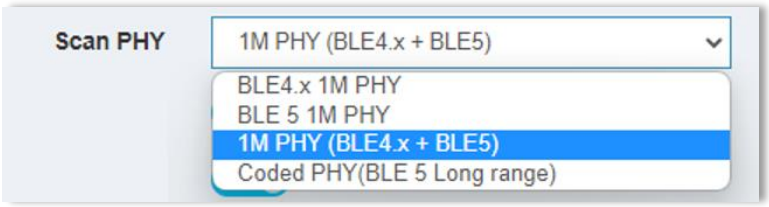


Figure 34: Scan PHY

  - **BLE4.x 1M PHY** – Only scan for the Bluetooth **Legacy Advertisement** packets (the versions of BLE 4.0, 4.1, 4.2). The **Legacy Advertisement** packets advertise on 1M bps PHY and 37, 38, 39 PHY channels.
  - **BLE5 1M PHY** – Only scan for the Bluetooth **Extended Advertisement** packets (the version of BLE5) and the Primary Advertisements of the packets advertise on 1M bps PHY and 37, 37, 38 PHY channels. The Secondary Advertisements can advise on any of 1M PHY, 2M PHY or Coded PHY.

    After the gateway captures the primary ADV packet, it will continuously to scan for the Secondary ADV packet according to the Primary Advertisement PDU.
  - **1M PHY (BLE4.x+BLE5)** – It is the function that contains the **BLE4.x 1M PHY** and **BLE 5 1M PHY**. The gateway scan for not only the **Legacy Advertisement** packets, but also the **Extended Advertisement** packets whose Primary Advertisements advertise on 1M PHY.
  - **Coded PHY (BLE5 Long range)** – Only scan for the Bluetooth **Extended Advertisement** packets (the version of BLE5) and the Primary Advertisements of the packets advertise on Coded PHY and 37, 37, 38 PHY channels. The Secondary Advertisements can advise on any of 1M PHY, 2M PHY or Coded PHY.

- **Active Scanning** – There are two types of scanning: **Active** and **Passive**. The difference is that an Active Scanning can send a scan request to request additional information (**scan response packets**) from the Bluetooth peripheral advertiser, while a Passive Scanning can only receive **advertising packets** from Bluetooth peripheral advertiser.

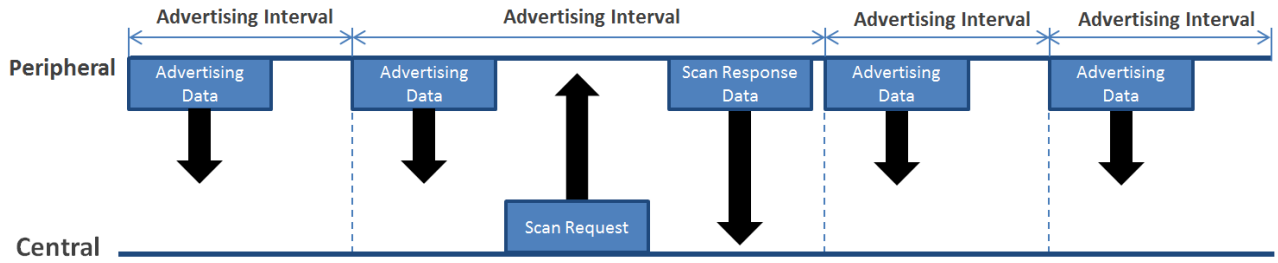


Figure 35: Active Scanning

> ***Note:***
> *If you want to scan for MKiBeacon and MKiBeacon&ACC, you need to enable Active Scanning, because both the two Beacon protocols are composed of advertising packet and scan response packet. And if your Bluetooth peripherals do not have the scan response packet, it is recommended to disable Active Scanning to improve the scanning rate of the advertising packets.*

6.4 Upload Beacon Packets

MKGW1-BW Pro gateway can upload the Bluetooth advertisement packets of BLE Beacon or other Bluetooth peripherals to server. When uploading data to the accessed server, there will be a large number of Bluetooth ADV packets will be loaded in the message payload. In order to facilitate users to identify and read the packets, the gateway upload the message payload in JSON array format or hexadecimal format and parses them in different items according to the type and format of the Beacon packets data.

6.4.1 How to Upload Message Payload

The time between the start of two consecutive upload events is **upload interval**. Each upload event may contain one or more message payload packets. You can set the number of ADV packets in a message payload packet when using JSON array format.

The gateway has capacity limit for storing ADV packets in its cache, and the maximum number of stored ADV packets is 3840. When the storage capacity reaches the maximum but the upload interval is not reached, the gateway will upload the message payload packets ahead of the upload interval is reached to prevent data loss.

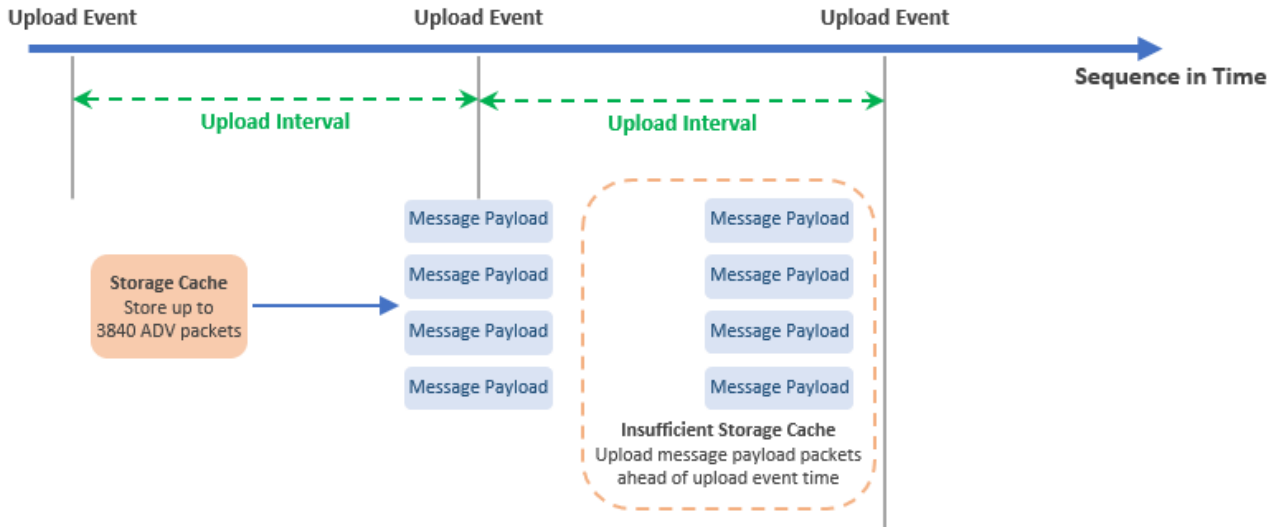


Figure 36: Upload message payloads

6.4.2 What is in the Message Payload

Each message payload packet contains the **Gateway Information** and **Bluetooth ADV packet (Beacon packet)**, and the gateway will translate all the information into different items in message payload packet.

The **Gateway Information** is in the header of each message payload packet and includes **upload time** and **gateway MAC address**. The following figure shows an example in the message payload using JSON array format.

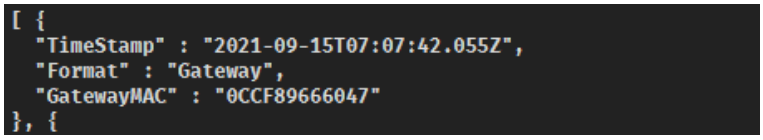


Figure 37: Gateway Information in message payload

Bluetooth ADV packet includes the items of **Timestamp, Format, BLE MAC, RSSI, Adv Type** and **Raw Data**. You can select the items you want to upload on the **Communication → Bluetooth Scanning** page of the Web GUI.

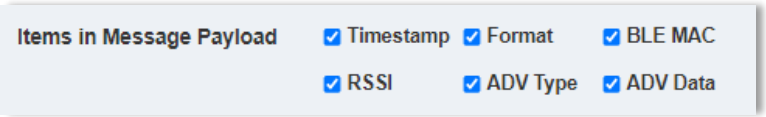


Figure 38: Selectable items in Bluetooth ADV packet

- **Timestamp** – The time when the ADV packet is captured by the gateway. The time format uses Epoch Timestamp when uploading message in Hex format and ISO8601 format when uploading message in JSON array format.
- **Format** – Corresponding to the checked option(s) of Beacon protocols. Refer to ***Chapter 6.2***.
- **BLE MAC** – The MAC address of the Bluetooth peripheral.
- **RSSI** – The signal strength value when the gateway receives the ADV packets. It is generally used to measure the distance between the Beacon and the gateway.
- **ADV Type** – It refers the Bluetooth version, advertisements property and PHY of the ADV packet. It contains the following items:
  - **Legacy-adv** – A Bluetooth 4.x advertising packet.
  - **Legacy-res** – A Bluetooth 4.x scan response packet.
  - **Legacy** – A Bluetooth 4.x advertisement packet combining advertising packet and scan response packet together.
  - **Extended** – A Bluetooth 5 Extended advertisement packet. And the items of Primary PHY (PriPHY) and Secondary PHY (SecPHY) will be shown under the **Adv Type** item.
- **ADV Data** – The Bluetooth raw advertisement payload data of the Bluetooth peripheral. When using JSON array format, BLE name and other identifiers of Beacon protocol (such as *Apple iBeacon UUID*, *iBeacon Major*, *Eddystone-UID Namespace ID*, etc.) parsed by the gateway all belong to **ADV Data**.

```
}, {
  "TimeStamp" : "2022-01-13T08:22:28.674Z",
  "Format" : "RawData",
  "BLEMAC" : "F46B0DE188BB",
  "RSSI" : -52,
  "AdvType" : "Legacy-res",
  "BLEName" : "MOKO SMART",
  "RawData" : "0B094D4F4B4F20534D415254"
}, {
  "TimeStamp" : "2022-01-13T08:22:29.248Z",
  "Format" : "iBeacon",
  "BLEMAC" : "F46B0DE188BB",
  "RSSI" : -70,
  "AdvType" : "Legacy-adv",
  "UUID" : "24ADCE5D5CDBD0805DCE267CD765D889",
  "Major" : 12,
  "Minor" : 66,
  "RSSI@1m" : -59
}, {
  "TimeStamp" : "2022-01-13T08:22:29.472Z",
  "Format" : "Eddystone-URL",
  "BLEMAC" : "F46B0DE188BB",
  "RSSI" : -52,
  "AdvType" : "Legacy-adv",
  "RSSI@0m" : 0,
  "URL" : "https://www.mokosmart.com"
}, {
```


Figure 39: Example of ADV Data item in the Bluetooth ADV packet by using JSON array format

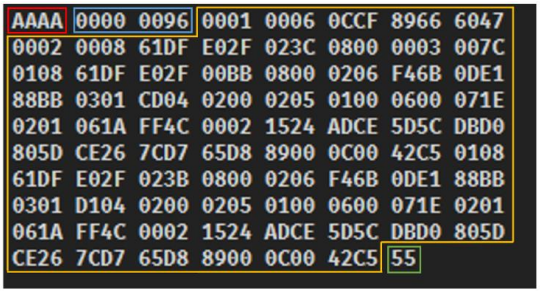
6.4.3 Data Format of Message Payload

The gateway support uploading the message payload in **JSON array** format when using MQTT, HTTP and TCP or **hexadecimal** format when using MQTT, HTTP, TCP and UDP.

The JSON array format will cost more bandwidth and network traffic than hexadecimal format. If the bandwidth of a gateway's deployed network environment is small, it is recommended to use hexadecimal format. The following will describe how to parse the upload message when using hexadecimal format.

- **Message payload**

The message payload consists of a message header (0xAA AA), a message tail (0x55) and the message body between the header and tail. The frame format is defined as follows:



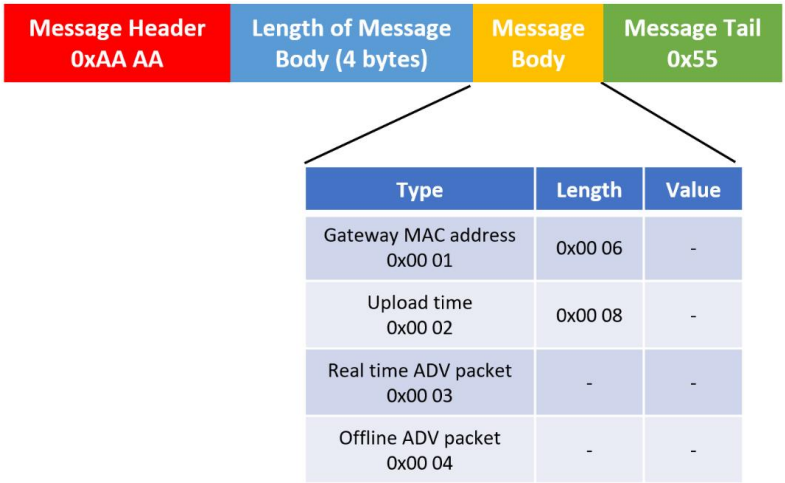


Figure 40: Frame format of message payload when using hexadecimal format

> ***Note:*** *When using hexadecimal format, the maximum length of the message payload is* ***65535bytes*** *when using MQTT, HTTP or TCP and* ***1460bytes*** *when using UDP to upload data to server.*

- **Message body**

The payload uses the Type-length-value (TLV) encoding scheme to format the message body. Each message consists of a gateway MAC address message, an upload time message and one or more ADV packets.

There will be four ***Types*** in message body – **Gateway MAC address**, **Upload time**, **Real time ADV packet** and **Offline ADV packet** (the offline data stored in the USB flash drive when the network is unavailable). The "***Length***" field occupies 2bytes.

The following table provides the details about message body (taking the contents in the yellow box of ***Figure 40*** as an example).

Table 3: Information about message body

Byte	Byte Value	Description
0 - 1	0x00 01	Type value of gateway MAC address
2 - 3	0x00 06	Length of gateway MAC address – 6bytes
4 - 9	0x0C CF 89 66 60 47	6bytes gateway MAC address
10 - 11	0x00 02	Type value of upload timestamp
12 - 13	0x00 08	Length of upload timestamp – 8bytes
14 - 21	0x61 DF E0 2F + 0x02 3C + 0x08 00	The upload timestamp uses **Epoch Timestamp** to convert time. The first 4bytes are second(s) part, the middle 2bytes are millisecond(ms) part and the last 2bytes are UTC time zone (int8_hour and unit8_minute). 0x61 DF E0 2F is 1,642,061,871s / 0x02 3C is 572ms UTC time zone is +08:00 The example timestamp in ISO8061 is 2022-01-13T16:17:51.572+08:00
22 - 23	0x00 03	Type value of real time ADV packet
24 - 25	0x00 7C	Length of real time ADV packet – 124bytes
26 - 149	0x01 08 - 0x00 02	ADV packet data

- **ADV packet data**

ADV packet data (including the real time ADV packet and offline ADV packet) is also formatted by TLV encoding scheme. There are **7 Types** and each type flag occupies 1byte. You can refer to ***Chapter 6.4.2*** to correspond to these *Types***.**

The following table describes the values and properties of the *Types* of ADV packet data.

Table 4: Type values of ADV packet data

Type Flag	Description	
0x01	**Timestamp** - The time when the ADV packet is captured by the gateway. It uses **Epoch Timestamp** to convert time and the length of the value occupies 8bytes. The first 4bytes are second(s) part, the middle 2bytes are millisecond(ms) part and the last 2bytes are UTC time zone (int8_hour and unit8_minute).	
0x02	The **BLE MAC** address of the Bluetooth peripheral. The length of the value occupies 6bytes.	
0x03	**RSSI** – The signal strength value when the gateway receives the ADV packet. The value of RSSI is int8 type.	
0x04	**Format** – Corresponding to the checked option(s) of	0x00 01 – Bluetooth raw advertising data

Type Flag	Description		
	Beacon protocols. View ***Chapter 6.2*** The length of the value occupies 2bytes.	0x00 02 – Apple standard iBeacon	
		0x00 04 – MKiBeacon	
		0x00 08 – MKiBeacon&ACC	
		0x00 10 – BeaconX Pro-ACC	
		0x00 20 – BeaconX Pro-T&H	
		0x00 40 – Google Eddystone-UID	
		0x00 80 – Google Eddystone-URL	
		0x01 00 – Google Eddystone-TLM	
0x05	**AdvType** – The Bluetooth version, advertisements property and PHY. The length of the value occupies 1byte. Value of this type is expressed by bitmask.	Bit0-1	0b00 – Legacy-adv
			0b01 – Legacy-res
			0b10 – Legacy
			0b11 – Extended
		Bit2-3	0b00 – Primary PHY = 1M PHY
			0b10 – Primary PHY = Coded PHY
		Bit4-5	0b00 – Secondary PHY = 1M PHY
			0b01 – Secondary PHY = 2M PHY
			0b10 – Secondary PHY = Coded PHY
0x06	**BLE name** – The Bluetooth name. You need to convert the hexadecimal data to ASCII to parse the BLE name.		
0x07	**Raw Data** – The Bluetooth raw advertisement payload data of the Bluetooth peripheral.		

The following table takes the ADV packet data contents in the yellow box of ***Figure 40*** as an example to provide you with more detailed information. The "***Length***" field occupies 1byte.

Table 5: Data format of ADV packet data

Byte	Byte value	Description
0	0x01	Type flag of timestamp
1	0x08	Length of timestamp – 8bytes
2 - 9	0x61 DF E0 2F + 0x00 BB + 0x08 00	0x61 42 51 56 is 1,631,736,150s / 0x00 BB is 187ms UTC time zone is +08:00 The example timestamp in ISO8061 is 2022-01-13T16:17:51.187+08:00
10	0x02	Type flag of BLE MAC address
11	0x06	Length of BLE MAC address – 6bytes
12 - 17	0xF4 6B 0D E1 88 BB	6bytes BLE MAC address
18	0x03	Type flag of RSSI.
19	0x01	Length of RSSI – 1byte
20	0xCD	RSSI value. It is int8 type and 0xCD is equivalent to -51dBm.
21	0x04	Type flag of Beacon Format

Byte	Byte value	Description
22	0x02	Length of Beacon Format – 2bytes
23 - 24	0x00 02	Beacon Format. 0x00 02 refers to Apple standard iBeacon
25	0x05	Type flag of AdvType
26	0x01	Length of AdvType – 1byte
27	0x00	AdvType, 0x00 = 0b00000000, the advertisement is a legacy advertising packet
28	0x06	Type flag of BLE name
29	0x00	Length of BLE name – 0byte, no BLE name
30	0x07	Type of Raw Data
31	0x1E	Length of Raw Data – 30bytes
31 – 60	0x0201 – 0x42C5	The raw advertisement payload data. It is parsed as follows: iBeacon UUID – 0x24 AD CE 5D 5C DB D0 80 5D CE 26 7C D7 65 D8 89 iBeacon Major – 0x00 0C iBeacon Minor – 0x00 42 RSSI@1m – 0xC5 (equivalent to -59dBm)

7. Access a Server to Transmit Message

MKGW1-BW Pro gateway can be as a client to upload Bluetooth ADV packets to your cloud or local server by using MQTT, HTTP, TCP or UDP network protocols. You can also use MQTT to send management commands to monitor and configure the parameters of the gateway, this can achieve Cloud Management function. Besides this, when the gateway receives the command to connect to a Bluetooth peripheral, it can make a communication between the Bluetooth peripheral and the cloud to transmit data each other.

Note: *Only MQTT supports the functions of cloud monitoring and configuring the gateway and data transmission between Bluetooth peripheral and cloud. HTTP, TCP and UDP do not support these functions.*

We recommend using MQTT protocol. If you have no idea about this, you can use the default demonstration server address to have a quick experience.

7.1 Access a Server via MQTT

7.1.1 What is MQTT

Message Queuing Telemetry Transport (MQTT) is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely simple and lightweight protocol that runs over TCP/IP sockets and supports SSL (Secure Sockets Layer). MKGW1-BW Pro gateway supports the *MQTT v3.1.1* standard protocol.

MQTT is a publish-subscribe architecture that is developed primarily to connect bandwidth and power-constrained devices over wireless networks. It has two components:

MQTT Broker: An MQTT broker is a central point of communication. The broker is responsible for dispatching all messages between the clients.

MQTT Client: An MQTT client is any device (the gateway is an MQTT client) that connects to the broker. A client that sends messages is a publisher and a client that receives messages is a subscriber. To receive a message, the client must subscribe to the topic of that message.

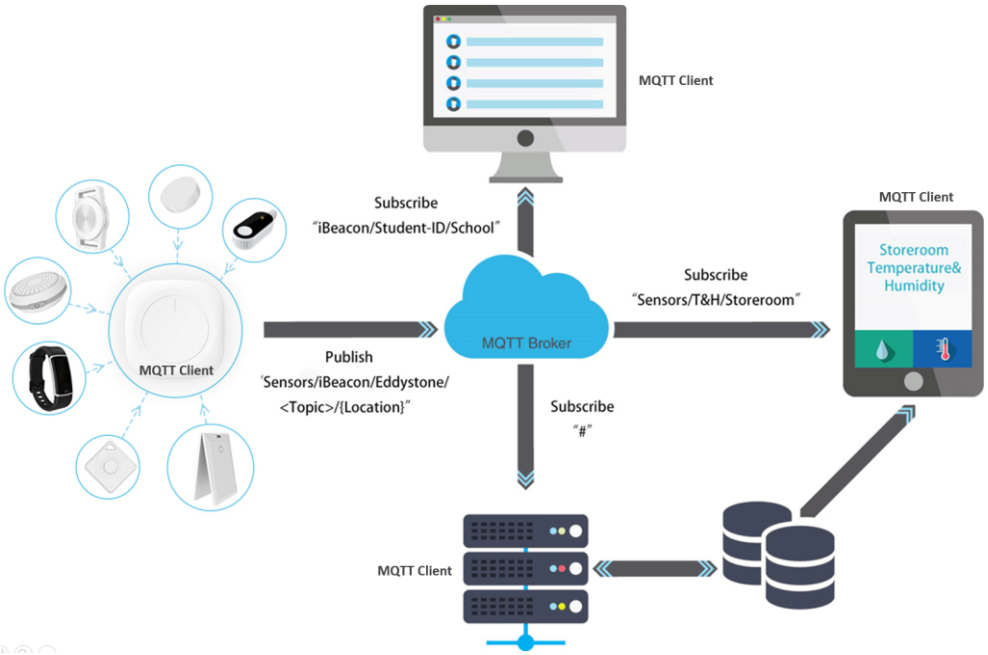


Figure 41: MQTT Publish/Subscribe architecture

Link: *Know more about MQTT and the related libraries, refer to the links:*
http://mqtt.org
https://github.com/mqtt/mqtt.org/wiki

7.1.2 Set up an MQTT Client

When using MQTT protocol, you need to configure the gateway as an MQTT client to connect an MQTT broker. On the Web GUI **Communication → Server Access** page, select **MQTT** from the **Server Access Protocol** drop-down menu and set the configurations. In some other platforms, the parameters may have different functions or descriptions, and you need to comply with the specifications of the platform to set the configurations. The gateway will take effect immediately after filling in and applying all the MQTT information.

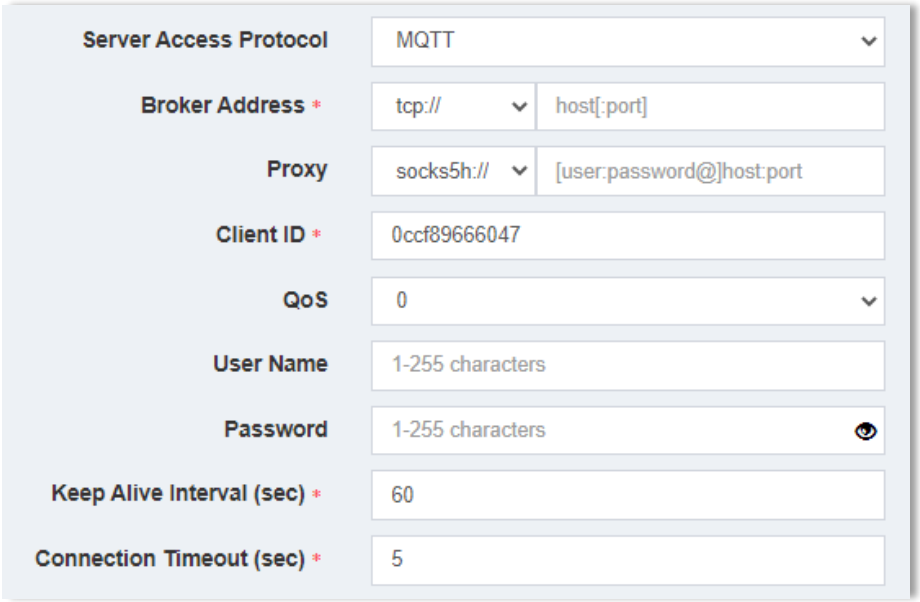


Figure 42: Basic configurations of MQTT

- **Broker Address** – A broker is a server that routes published messages to subscribers, following the format and type the address of the broker. The format is **scheme** + **domain name/IP address: port**.

  The scheme in the drop-down menu contains "**tcp://**" and "**ssl://**". If ssl:// is selected, it enables the message encryption by using SSL security. View ***Chapter 7.1.3*** for more details about ssl:// configuration. Generally, default **port** value is **1883** when selecting tcp:// and **8883** when selecting ssl://.

- **Proxy** – MKGW1-BW Pro supports Proxy Socks5 Server for MQTT network access. The format of the address is: **[username:password]@host: port**.

- **Client ID** – The client identifier (Client ID) identifies each MQTT client that connects to an MQTT broker. The gateway sets the MAC address as the default Client ID.

- **QoS** – There are three levels of QoS (Quality of Service):**:**

  - **QoS=0** (by default)**,** at most once. This is the simplest, lowest-overhead method of sending a message and there is no guarantee of delivery. The sender simply publishes the message, and there is no acknowledgement by the receiver.

    This is the fastest method and requires only 1 message. It is the lowest-cost in terms of volume of data transfer. This is suitable when you have a reliable connection between client and broker.

- **QoS=1**, at least once. This method guarantees that the message will be transferred successfully to the receiver. The sender stores the message until it gets a *PUBACK* packet from the receiver that acknowledges receipt of the message. But in the event that the acknowledgement is lost the sender won't realize the message has got through, so will send the message again after a reasonable amount of time. The sender will re-send the message until it gets the receiver's acknowledgement.

  This means that sending is guaranteed, although the message may reach the receiver more than once.

- **QoS=2**, exactly once. This is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS=2 is the safest and slowest quality of service level. The guarantee is provided by at least two request/response flows (a four-part handshake) between the client and the broker. When the handshake has been completed, both client and broker are sure that the message was sent exactly once. The sender and receiver use the packet identifier of the original published message to coordinate delivery of the message.

  This level guarantees that the message will be delivered only once, but has a relatively high cost in terms of data transfer.

- **User Name / Password** – The username and password for client authentication and authorization. The username/password combination is transmitted in clear text and is not secure without some form of transport encryption.
- **Keep Alive Interval(sec)** – Keep alive ensures that the connection between the broker and client is still open and that the broker and the client are aware of being connected. When the client establishes a connection to the broker, the client communicates a time interval in seconds to the broker. This interval defines the maximum length of time that the broker and client may not communicate with each other. 60s by default and the minimum values is 5s, the maximum keep alive interval is 65535s.
- **Connection Timeout(sec)** – The maximum timeout period for the client and broker to wait for the connection. 5s by default and the range is from 1s to 65535s.

7.1.3 Configure Security Settings with SSL

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

MKGW1-BW Pro gateway provides the ability to run MQTT client over SSL (OpenSSL version 1.0.2).

The **Broker Address** setting has a drop-down menu which contains "**tcp://**" and "**ssl://**". You can select **ssl://** to enable SSL. The port of the broker defaults to 8883 when SSL is enabled.

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

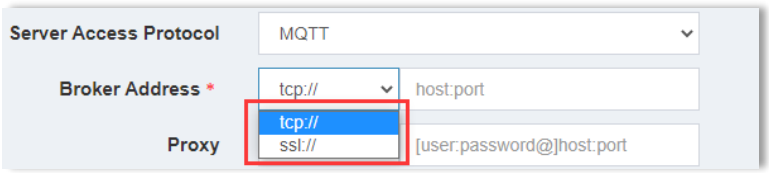


Figure 43: Selecting SSL in MQTT

When using SSL, there are three optional authentication methods to encrypt the data transfer. Both one-way SSL authentication and two-way SSL authentication are supported.

- **One-way SSL authentication** – Only the Client (gateway) verifies the identity of the server (broker) using server certificate.
- **Two-way SSL authentication** – The client (gateway) and the server (broker) authenticate each other to create the secure MQTT connection.

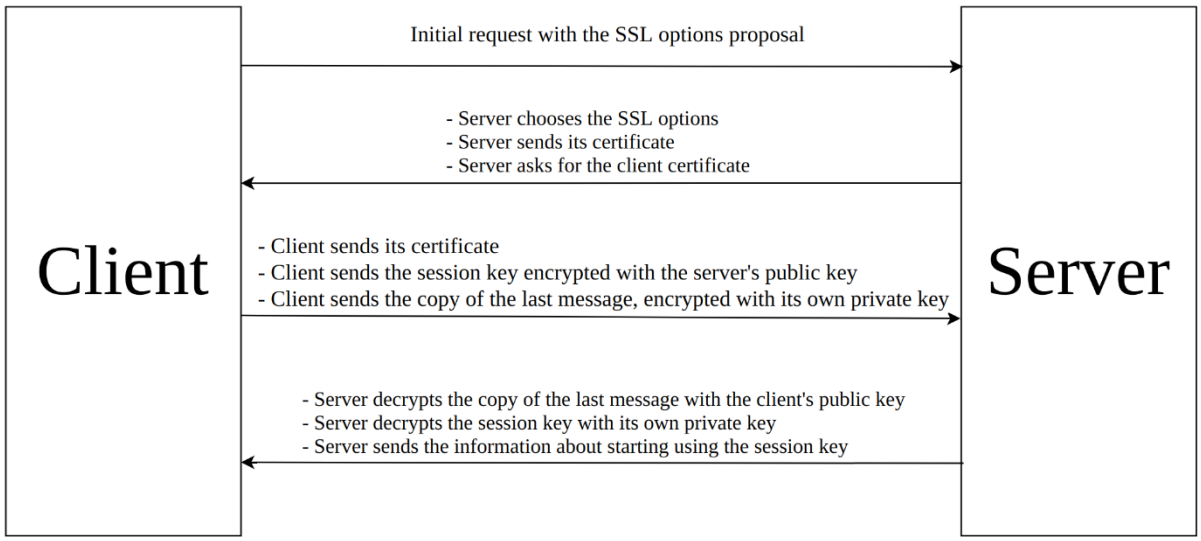


Figure 44: Example of the simplified two-way SSL authentication handshake

The gateway and broker must use the same CA (Certificate Authority) for the client and server certificates.

The **Certification Type** setting provides three authentication methods to select:

Figure 45: Selections of authentication methods for SSL

- **CA signed Server certificate** – One-way SSL authentication. The gateway only verifies if the broker certificate is a valid CA signed certificate to authenticate the identity of the broker.
- **CA certificate** – One-way SSL authentication. You need to upload a CA root certificate file or self-signed certificate file. The file is trusted by the gateway and will be used to verify if the broker certificate is valid.
- **Self-signed certificates** – Two-way SSL authentication. You need to upload three files for the gateway and the broker to authenticate each other.
  - **CA File Name** – The CA root certificate file or self-signed certificate file. The file is trusted by the gateway and will be used to verify if the broker certificate is valid.
  - **Client Certificate File Name** – The gateway certificate presented to the broker to verify the identity of the gateway.
  - **Client Key File Name** – The private key file of the gateway.

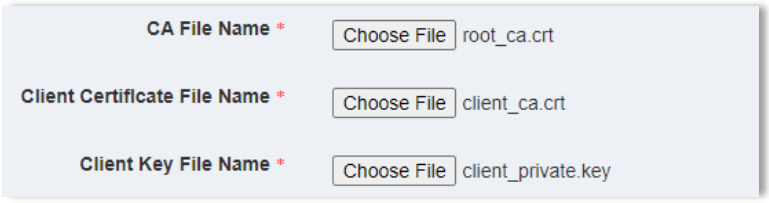


Figure 46: Self-signed certificate files

Caution: *Ensure all the certificate and key files are generated through OpenSSL in PEM format.*

There are three methods to upload the certificate and key files for SSL authentication.

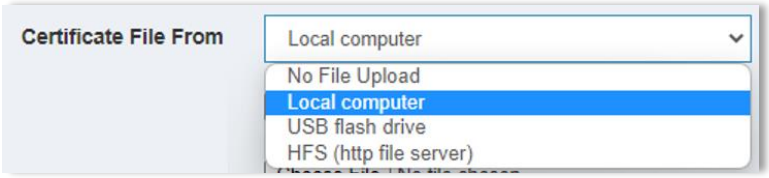


Figure 47: Methods to upload file(s) to the gateway

- From **Local computer** – Choose the file on your computer or smartphone to upload it to the gateway.
- From **USB flash drive** – Copy the files to the root directory of your USB flash drive in advance and insert the USB flash drive into the USB port of the gateway. Then you need to type the complete filename (including the filename extension) in the corresponding input box. After clicking the **Save&Apply** button at the bottom of the Web GUI page, the gateway will search for and obtain the file(s) according to the filename(s), and return the result after a few seconds.

Figure 48: Type the filenames into the input boxes

- From **HFS (http file server)** – Http file server, otherwise known as HFS, is a free web server specifically designed for publishing and sharing files. When using HFS to upload file(s), follow the steps below.

Step 1: Open the ***HFS.exe*** software in ***Windows OS*** and add the file(s) to the path of HFS, as shown in the following figure:

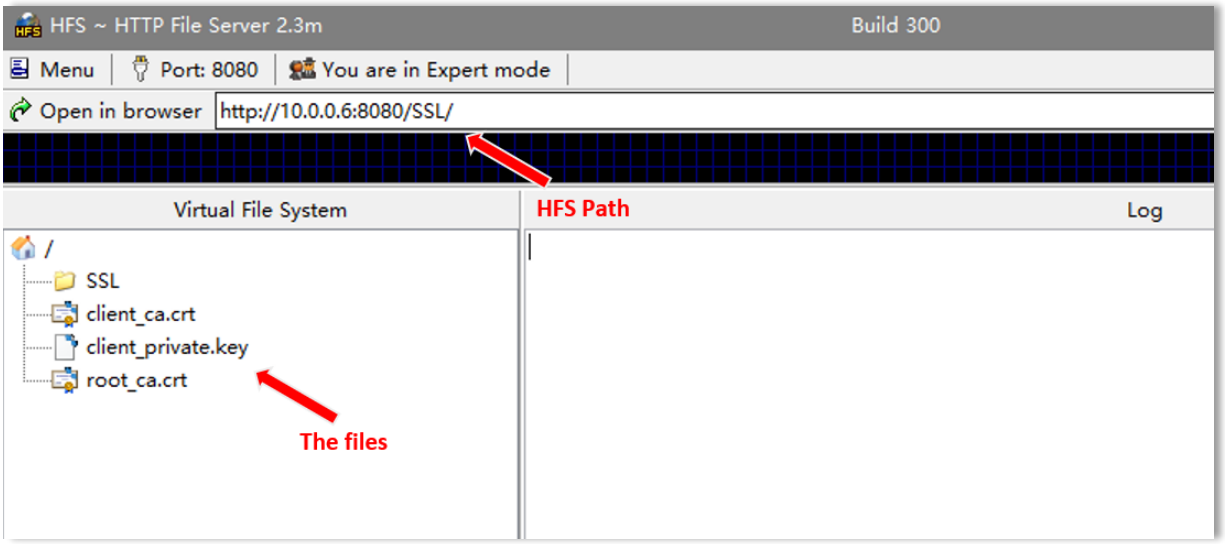


Figure 49: Add file(s) to the path of HFS

Step 2: Type the HFS URL link into the **HFS URL** input box. If the HFS and the gateway are in the same Local Area Network (LAN), the HFS URL link is the HFS path, as the figure shown above: *http://10.0.0.6:8080/SSL/*

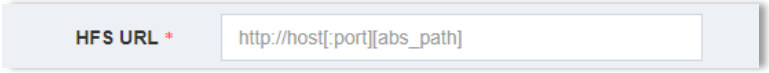


Figure 50: HFS URL link

Step 3: Type the complete filename (including the filename extension) in the corresponding input box and click the **Save&Apply** button at the bottom of the Web GUI page, the gateway will connect to the HFS and search for and obtain the file(s) according to the filename(s), and return the result after a few seconds.

Contributions: *HFS.exe software*
1. Download the "HFS.exe" file for Windows from the link:
https://cloud.mokosmart.com/index.php/s/RNAWNDCAMe7fsrC
2. For more information about HFS tool, refer to the link:
https://www.rejetto.com/hfs/

7.1.4 MQTT Topic for Uploading Beacon Packets

A topic is an identifier (ID) used by the MQTT broker to identify rightful clients for delivering messages. Each client that wants to send messages publishes them on a certain topic, and each client that wants to receive messages subscribes to a certain topic.

In MQTT, the word topic refers to an UTF-8 string that the broker uses to filter messages for each connected client. The topic consists of one or more topic levels. Each topic level is separated by a forward slash "/" (topic level separator). You can also refer to the default design of the MKGW1-BW Pro gateway.

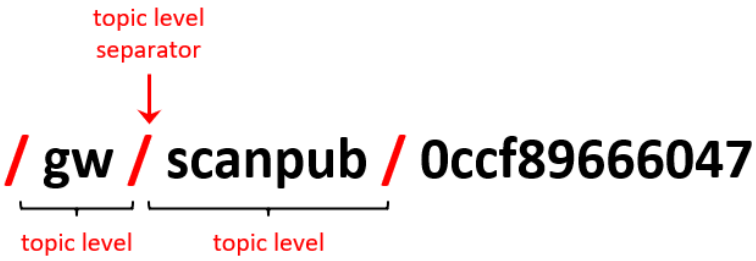


Figure 51: Format of MQTT topic

MKGW1-BW Pro supports three types of MQTT topic to achieve different functions. The **Upload Beacon Packets** is the topic to publish the Bluetooth Beacon packets scanned by the gateway to the broker.

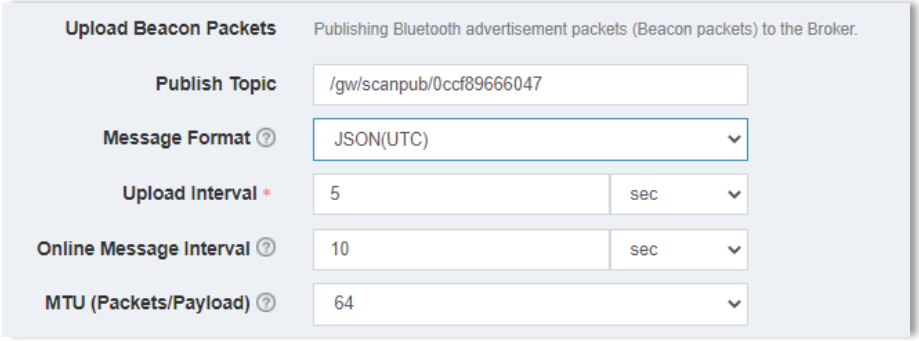


Figure 52: Configurations of Upload Beacon Packets topic

- **Publish Topic** – It is used to send the message payload which contains the Bluetooth ADV packets scanned by the gateway to the broker. You need to subscribe to this topic on your local client to receive the message.

  The default topic is: */gw/scanpub/${gatewayMAC}*

${gatewayMAC} refers to the MAC address of the gateway in hexadecimal format.

- **Message Format** – Select the data format of the message payload from the drop-down menu.

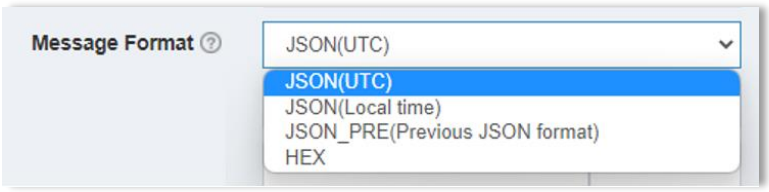


Figure 53: Selections of Message Format

  - **JSON (UTC)** – JSON array format and the timestamp will use GMT time zone (UTC+00:00).

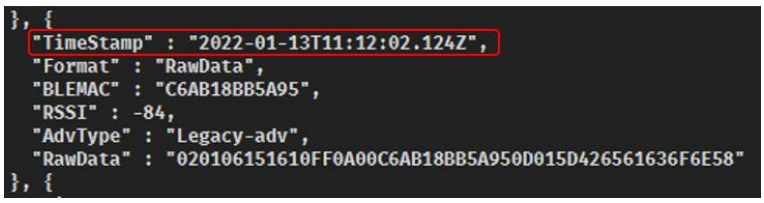


Figure 54: JSON (UTC) format

  - **JSON (Local time)** – JSON array format and the timestamp will be added with UTC time zone offsets according to the Date and Time settings.

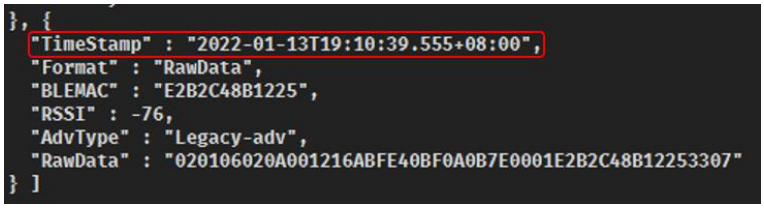


Figure 55: JSON (Local time) format

  - **JSON_PRE (Previous JSON format)** – JSON array format, which is used in the previous MKGW1-BW gateway (the version before 2021). It is not recommended to use this format. For more information, please contact the sales team of MOKO SMART.
  - **HEX** – Message uploaded in hexadecimal format.

- **Upload Interval** – Upload interval is the time between the start of two consecutive upload events. The value of the time ranges from 0 to 65535, and the unit can be set to seconds (s), minutes (min) or hours (h). When you set the value to 0, the gateway will not cache data and upload them immediately.
- **Online Message Interval** – A heartbeat message to indicate the gateway is online. The gateway will send the gateway information including timestamp and gateway MAC address to the Broker if there are no Bluetooth advertisement packets uploaded after the interval. If the field is left blank, this mechanism will be deactivated. The value of Online Message Interval must not be less than the value of Upload Interval.

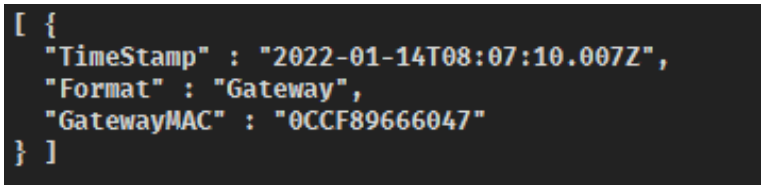


Figure 56: The heartbeat message to indicate the gateway is online

- **MTU (Packets/Payload)** – The maximum number of ADV packets in a message payload when using JSON array format. The ***Chapter 6.4.1*** introduces the details of the upload method. You can choose **64**, **128**, **256**, **512** or **1024** from the drop-down menu.

7.1.5 MQTT Topic for Remotely Managing the Gateway

When you want to remotely monitor and configure the gateway via the cloud, you can use **Remote Management** topic to receive the message of cloud management commands from the cloud and respond the action results to the cloud. The data of commands and response uses **JSON** array format.

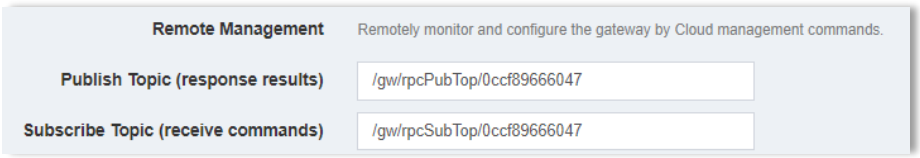


Figure 57: Remote Management topic

- **Publish Topic (response results)** – Used for the gateway to send the response message of the action results to the broker after the gateway received the commands. You need to subscribe to this topic on your local client if you want to receive any action results from the gateway.

  The default topic is: */gw/rpcPubTop/${gatewayMAC}*

  ${gatewayMAC} refers to the MAC address of the gateway in hexadecimal format.

- **Subscribe Topic (receive commands)** – Used for the gateway to receive the management commands. You need to publish to this topic on your local client to send commands to the gateway.

  The default topic is: */gw/rpcSubTop/${gatewayMAC}*

  ${gatewayMAC} refers to the MAC address of the gateway in hexadecimal format.

You can use the cloud management commands to query and check the gateway's status and logs in real time, query and configure the parameters of network settings, Bluetooth scanning and filter settings, server access settings and system settings. You can also remotely restart, restore and upgrade the gateway by using the remote management commands.

An example of command and response is as follows:

Command to query the gateway's status: *{"action":"get_status","requestId":"000001"}*

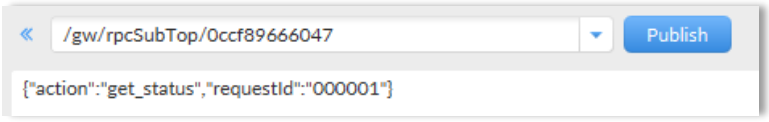


Figure 58: Command to query the gateway's status

```
{
  "state" : {
    "code" : 0,
    "msg" : "Success"
  },
  "requestId" : "000001",
  "data" : {
    "deviceinfo" : {
      "model" : "MKGW1-BW Pro (L)",
      "ssid" : "MKGW-BW-6047",
      "macaddr" : "0C:CF:89:66:60:47",
      "sysversion" : "V1.1.2",
      "localtime" : "Thu Jan 13 19:29:05 2022",
      "uptime" : "15089",
      "cputemp" : "56",
      "cpuinfo" : "0%",
      "meminfo" : "0 kB /126276 kB (0%)"
    },
    "networkinfo" : {
      "wifimode" : "802.11b/g/n",
      "wanmode" : "WLAN",
      "wanip" : "10.0.0.7",
      "lanip" : "192.168.22.1",
      "channel" : "10/2.457 GHz",
      "access" : "MQTT",
      "wanlink" : "1",
      "aclink" : "1"
    }
```


Figure 59: Response message of gateway's status

Contribution: *Contact the sales of* ***MOKO SMART*** *to get the document "****MKGW1-BW Pro Bluetooth Gateway Cloud Management Commands****" to get the complete commands and learn how to use them.*

7.1.6 MQTT Topic for Communicating with Remote Bluetooth Peripheral

After the gateway has connected to a remote Bluetooth peripheral and accessed to a Cloud Server, it can make a communication process between Bluetooth peripheral and server. You can use **Bluetooth Communication** topic to transmit data and the gateway acts as a bridge role for transmission.

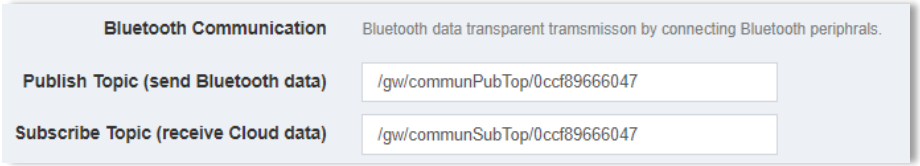


Figure 60: Bluetooth Communication topic

- **Publish Topic (send Bluetooth data)** – The gateway will send the data received from the Bluetooth peripheral connected to the gateway to server via this topic. When you want to receive any returned data from the remote Bluetooth peripheral, you need to subscribe to the topic on your local client.

  The default topic is: */gw/communPubTop/${gatewayMAC}*

  ${gatewayMAC} refers to the MAC address of the gateway in hexadecimal format.

- **Subscribe Topic (receive Cloud data)** – The gateway will receive the data from server by subscribing to this topic and send the data to the Bluetooth peripheral connected to the gateway. You can transmit the data you want to send to the remote Bluetooth peripheral by publishing to this topic on your local client.

The default topic is: */gw/communSubTop/${gatewayMAC}*

${gatewayMAC} refers to the MAC address of the gateway in hexadecimal format.

> ***Note:*** *Before making a communication between the Bluetooth peripheral and the Cloud Server. You need use the* ***Remote Management*** *topic to send management commands to control the gateway to find and connect to the required Bluetooth peripheral, and you can also use the commands to set the connection and communication parameters of the gateway.*

7.2 Access a Server via HTTP

MKGW1-BW Pro gateway supports **HTTP (HTTP/1.1)** protocol to send the Bluetooth advertisement packets scanned by the gateway to the HTTP Server. It uses the **POST** request method and **HTTP persistent connections (HTTP Keep-alive)** to connect and send data to server. Also, **HTTPS** - a combination of SSL/TLS protocol and HTTP to provide encrypted and secure identification of a network server is supported.

You need select **HTTP** from the **Server Access Protocol** drop-down menu on the **Communication → Server Access** page of the Web GUI to set the HTTP configurations. The gateway will take effect immediately after filling in and applying all the HTTP information.

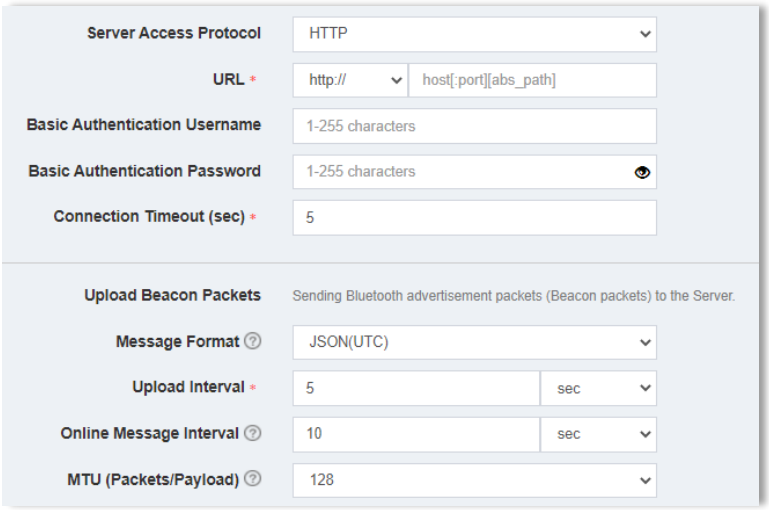


Figure 61: Configurations of HTTP

- **URL** – Uniform Resource Locator (URL) of the HTTP Server. The format is **scheme** + **host[:port][abs_path]**.

  The scheme in the drop-down menu contains "**http://**" and "**https://**". "https://" allows the secure transactions by encrypting the entire communication with SSL. Generally, the "**port**" is not a required value, and the default port value is **80** when selecting **http://** and **443** when selecting **ssl://**.

- **Basic Authentication Username / Basic Authentication Password** – The username and password for the basic access authentication of the client and they are encoded by using base-64.

  As the username and password are passed over the network as clear text (it is base64 encoded, but base64 is a reversible encoding), the basic authentication scheme is not secure.

- **Connection Timeout (sec)** – The maximum timeout period for the client and server to wait for the connection. 5s by default and the range is from 1s to 65535s.

- **Message Format** – Select the data format of the message payload from the drop-down menu. View ***Chapter7.1.4*** to get the description of all the formats.

- **Upload Interval** – Upload interval is the time between the start of two consecutive upload events. The value of the time ranges from 0 to 65535, and the unit can be set to seconds (s), minutes (min) or hours (h). When you set the value to 0, the gateway will not cache data and upload them immediately.
- **Online Message Interval** – A heartbeat message to indicate the gateway is online. The gateway will send the gateway information including timestamp and gateway MAC address to server if there are no Bluetooth advertisement packets uploaded after the interval. If the field is left blank, this mechanism will be deactivated. The value of Online Message Interval must not be less than the value of Upload Interval.
- **MTU (Packets/Payload)** – The maximum number of ADV packets in a message payload when using JSON array format. The ***Chapter 6.4.1*** introduces the details of the upload method. You can choose **64**, **128**, **256**, **512** or **1024** from the drop-down menu.

7.3 Access a Server via TCP

MKGW1-BW Pro gateway can be as a client to send the Bluetooth advertisement packets scanned by the gateway to server via TCP protocol. Select the **TCP** from the drop-down menu of **Server Access Protocol** setting, you can add a TCP Server to connect to. The gateway will take effect immediately after filling in and applying all the TCP information.

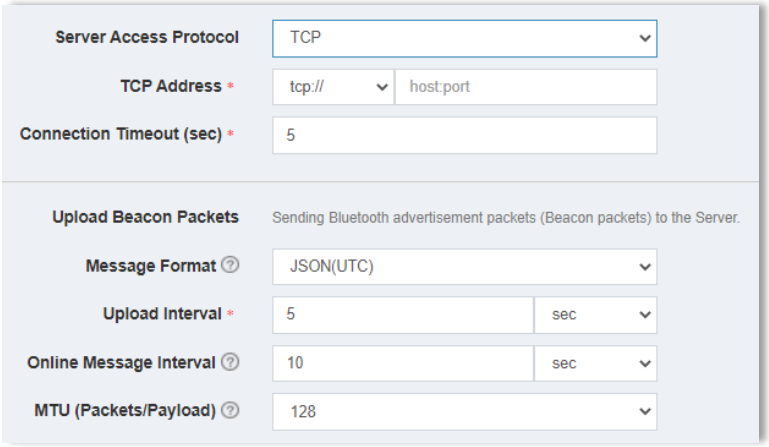


Figure 62: Configurations of TCP

- **TCP Address** – IP address of the TCP Server. The format is tcp://**host:port**
- **Connection Timeout (sec)** – The maximum timeout period for the client and server to wait for the connection. 5s by default and the range is from 1s to 65535s.
- **Message Format** – Select the data format of the message payload from the drop-down menu. View ***Chapter7.1.4*** to get the description of all the formats.
- **Upload Interval** – Upload interval is the time between the start of two consecutive upload events. The value of the time ranges from 0 to 65535, and the unit can be set to seconds (s), minutes (min) or hours (h). When you set the value to 0, the gateway will not cache data and upload them immediately.
- **Online Message Interval** – A heartbeat message to indicate the gateway is online. The gateway will send the gateway information including timestamp and gateway MAC address to server if there are no Bluetooth advertisement packets uploaded after the interval. If the field is left blank, this mechanism will be deactivated. The value of Online Message Interval must not be less than the value of Upload Interval.
- **MTU (Packets/Payload)** – The maximum number of ADV packets in a message payload when using JSON array format. The ***Chapter 6.4.1*** introduces the details of the upload method. You can choose **64**, **128**, **256**, **512** or **1024** from the drop-down menu.

7.4 Access a Server via UDP

You can also use UDP protocol to send the Bluetooth advertisement packets scanned by the gateway to a Server. You need to select the **UDP** from the drop-down menu of **Server Access Protocol** setting, you can add a UDP Server to connect to. The gateway will take effect immediately after filling in and applying all the UDP information.

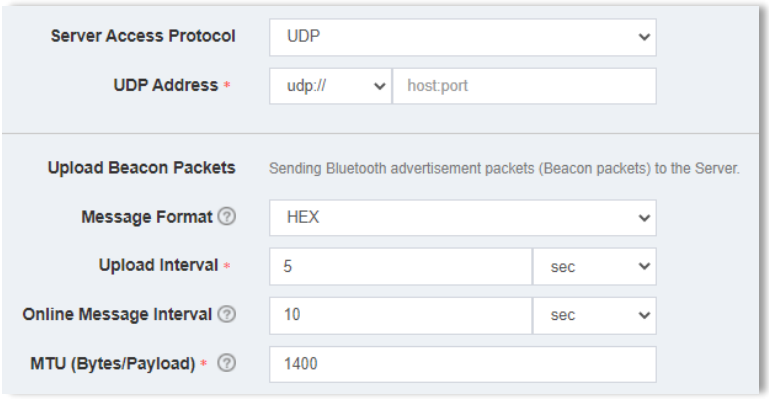


Figure 63: Configurations of UDP

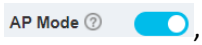
- **UPD Address** - IP address of the UDP Server. The format is upd://**host:port**
- **Message Format** – UDP only supports using hexadecimal format to upload the message payload.
- **Upload Interval** – Upload interval is the time between the start of two consecutive upload events. The value of the time ranges from 0 to 65535, and the unit can be set to seconds (s), minutes (min) or hours (h). When you set the value to 0, the gateway will not cache data and upload them immediately.
- **Online Message Interval** – A heartbeat message to indicate the gateway is online. The gateway will send the gateway information including timestamp and gateway MAC address to server if there are no Bluetooth advertisement packets uploaded after the interval. If the field is left blank, this mechanism will be deactivated. The value of Online Message Interval must not be less than the value of Upload Interval.
- **MTU (Bytes/Payload)** – The maximum length (bytes) of the message payload. It can be set from **128bytes** to **1460bytes** and 1400bytes is pre-set as the default value.

8. Device Settings

Various administrative functions of the gateway can be configured. Most of the functions can be viewed on the Web GUI **System** option and are easy to configure.

8.1 AP Mode Settings

After you have configured all the functions to make the gateway run successfully, we recommend you to change the default parameters of the connection to the gateway's Wi-Fi or disable the AP function of the gateway.

On the **Network → Wireless AP** page of the Web GUI, you can manage the AP mode of the gateway. If you disable the **AP Mode** 

, it means the gateway will turn off the Wi-Fi hotspot and other people will not be able to scan the gateway's Wi-Fi signal.

If the AP mode is enabled, you can set the parameters of the gateway's AP mode, and the gateway will restart to make all configurations take effect.

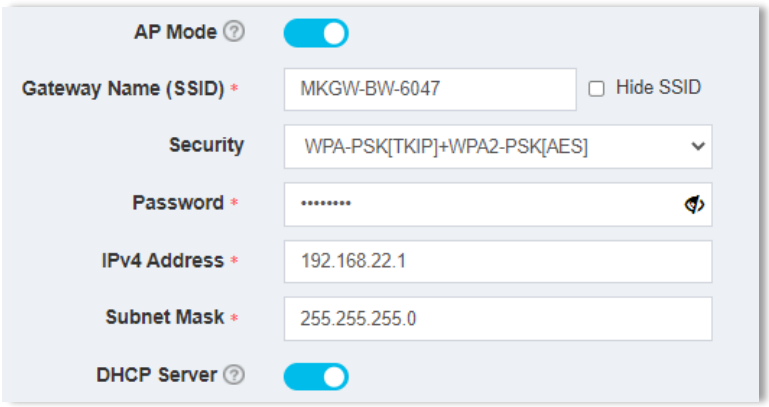


Figure 64: Configurations of gateway's AP mode

- **Gateway Name (SSID)** – The gateway's Wi-Fi name. The default SSID is **MKGW1-BW-XXXX** (XXXX represents the last 4 characters of the gateway's MAC address). If you want to disable the gateway's SSID broadcast feature (make the gateway invisible in the wireless network), you can check the **Hide SSID** option, and you need to type the SSID when you want to connect to the gateway's Wi-Fi.
- **Security** – Select a Wi-Fi security type from the drop-down menu. **WPA-PSK[TKIP]+WPA2-PSK[AES]** is the default setting and the most secure. Security can be disabled by selecting **NONE** but this is not recommended.
- **Password** – The gateway's Wi-Fi password. The default password is **Moko4321** and it is better to change it. A complex, hard-to-guess password is recommended.
- **IPv4 Address** – The WLAN IP address of the gateway. The default IP address is **192.168.22.1**. You can visit this IP address to access the Web GUI.
- **Subnet Mask** – Specify a subnet mask. The default value is 255.255.255.0.
- **DHCP Server** – If the DHCP Server is enabled, the gateway will automatically assign IP address to the client which has connected to the gateway's Wi-Fi network and set to obtain the IP address dynamically. If you disable the DHCP Server, you need to set the IP address of the client manually so that they can access the gateway's Wi-Fi.

8.2 Offline Storage

The gateway supports to store the scanned Bluetooth ADV packets on an external USB flash drive when the network is unavailable. When the network is available, the gateway will first upload the stored packets in the USB flash drive to server.

The offline packets will be stored in separate file in the root directory of the USB flash drive and the maximum capacity of one file is 1GB. The file will be named as ***cachebeacon+timestamp*** (the last file name will not contain the timestamp if it does not reach 1GB capacity).

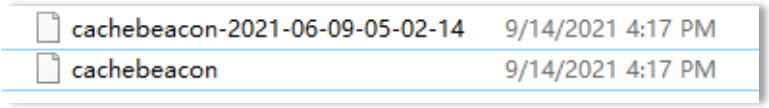


Figure 65: Offline file stored in USB flash drive

You can disable this function 

on the bottom of the **Communication → Bluetooth Scanning** page of the Web GUI.

8.3 System Logs

Gateway will record the important operations and events when it works to help users or engineers to check the gateway when some abnormal faults occur. You can download the Log file on the Web GUI **System → System Logs** page and send it to ***MOKO SMART*** to help you diagnose the gateway.

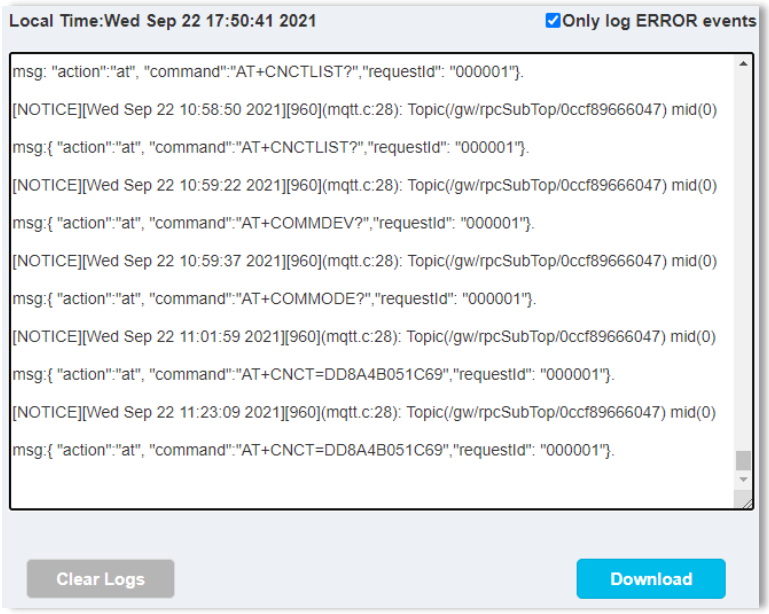


Figure 66: Logs of the gateway

8.4 Login Password

On the **System → Device Settings - Login** page of the Web GUI, it allows you to modify the login password to access the Web GUI. You need to confirm the current password before setting a new password.

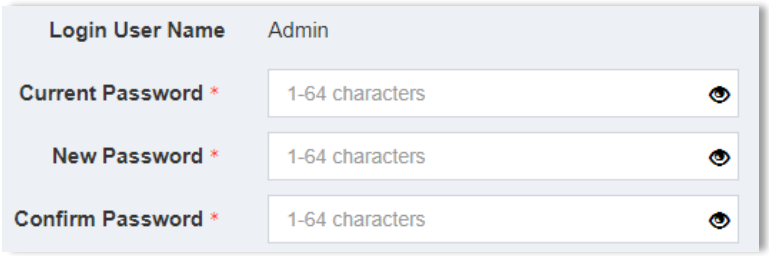


Figure 67: Modify the login password to access Web GUI

8.5 Sync Date and Time

On the **System → Device Settings – Date and Time** page of the Web GUI, you can set the date and time for the gateway.

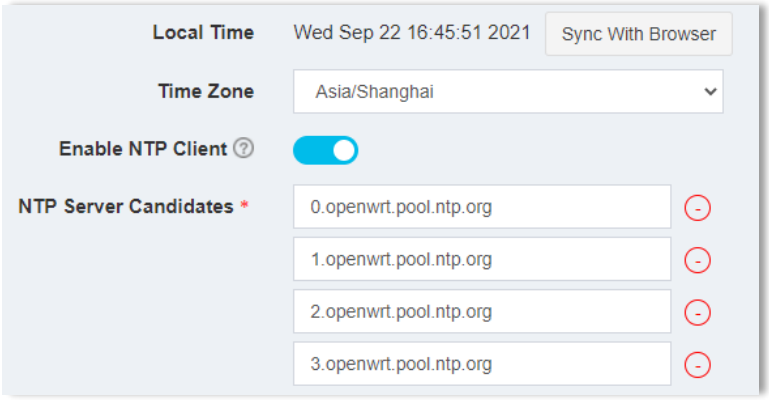


Figure 68: Configurations of setting date and time

- **Synchronize date and time manually**

You can synchronize the date, time and the time zone with the browser by clicking the **Sync with Browser** button. You can also change the time zone manually from the drop-down menu of **Time Zone**, and the local time will be adjusted automatically according to the time zone you choose.

- **Synchronize date and time automatically**

NTP (Network Time Protocol) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. We recommend you to enable **NTP Client** and add the NTP server candidates to make the gateway synchronize the date and time with public time servers automatically. The gateway supports adding up to 4 NTP servers.

8.6 Restart the Gateway

You can restart the gateway immediately by clicking the **Restart Now** button on the Web GUI **System → Device Settings – Restart** page or set a schedule to restart the gateway automatically at the scheduled time. You can set the restart time in **Daily**, **Weekly** or **Monthly**.

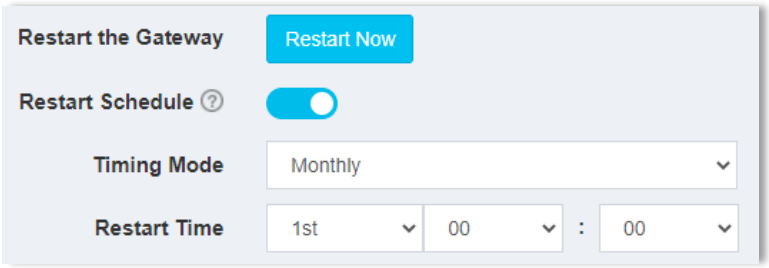
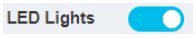


Figure 69: Configurations of restarting the gateway

8.7 Turn off the LEDs

Chapter 2.2.4 introduces the LEDs status when the gateway is in different working modes. On the **System → Device Settings – LED Control** page of the Web GUI, you can set the gateway to turn off the LEDs.

The **LED Lights** switch 

can manually turn on/off the gateway's LEDs. And you can also set a LED off schedule to turn off the LEDs automatically during the scheduled time period.

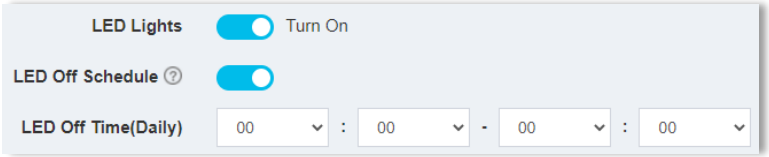


Figure 70: Configurations to turn off the gateway's LEDs

The gateway only supports the daily time to turn off the LEDs. If the end-time is less than the start-time, the gateway will turn off the LEDs from the start time of the first day till the end-time of the next day.

8.8 Backup and Restore the Gateway

On the **System → Backup&Restore** page of the Web GUI, you can back up the gateway and restore it by loading a backup file. The backup function can be used to recover all the configurations when the gateway is configured by some unexpected deletion or settings. Therefore, it is better to back up the gateway after you have completed all the configurations.

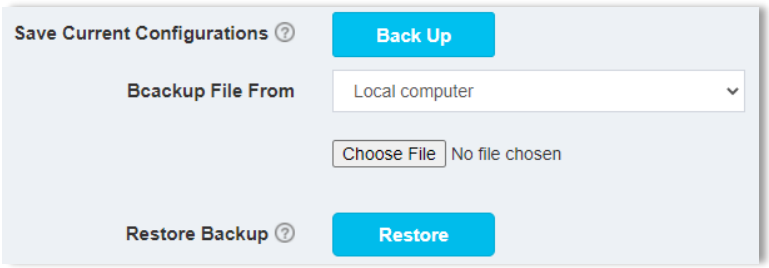
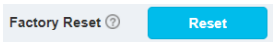


Figure 71: Backup and restore the gateway

You can click the **Back Up** button to download a backup file (a compressed file in *gzip* format). When you want to restore the gateway to an earlier status, you can load the backup file through **local computer**, **USB flash drive** or **HFS** (you can view *Chapter 7.1.3* to learn how to load file by using USB flash drive or HFS), and then click the **Restore** button to restore the gateway. The gateway will restart after the recovery completes. You can identify the status by the changes of the LEDs.

8.9 Reset the Gateway

There are two methods to reset the gateway. One is to click the **Reset** button 

on the bottom of the Web GUI **System → Backup&Restore** page and the gateway will reset to factory defaults and restart immediately.

The other way is to use a needle-like object to press the button for more than 3 seconds and then release, the gateway will reset and then restart. You can identify the reset operation by the changes of the LEDs.

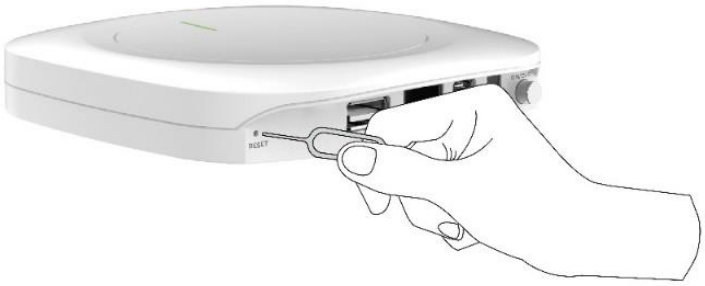


Figure 72: Use a needle-like object to reset the gateway

> ***Caution:*** *Reset the gateway will erase all of your settings (Network Connection, Server Access, Bluetooth Settings and other System Settings), and replace them with the factory defaults. You can save backup file before resetting the gateway in order to restore all the settings after the reset.*

8.10 Firmware Upgrade

Each of the two independent wireless modules (Bluetooth and Wi-Fi) of the MKGW1-BW Pro gateway runs a separate application. They can communicate with each other to achieve the complete functions.

The two types of the firmware have different upgrade methods.

8.10.1 Upgrade the Wi-Fi Firmware

When ***MOKO SMART*** releases new Wi-Fi firmware of MKGW1-BW Pro gateway, you can easily upgrade the gateway by loading an upgrade *Bin* file to the gateway. On the **System → Firmware Upgrade** page of the Web GUI, you can select the methods of loading upgrade file through **local computer**, **USB flash drive** or **HFS** (you can view ***Chapter 7.1.3*** to learn how to load file by using USB flash drive or HFS) to upgrade the gateway.

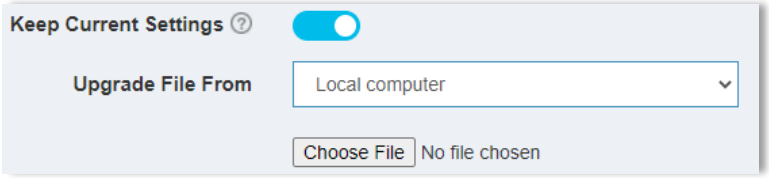


Figure 73: Upgrade the gateway

If you want to save and keep all current configurations, you can enable **Keep Current Settings** before upgrading the gateway. The gateway will restart after the upgrade completes. You can identify the upgrade status by the changes of LED indicators.

> ***Caution:*** *You need to keep the power of the gateway on during the upgrade process and do not do anything else to the gateway until it finishes restarting!*

8.10.2 Upgrade the Bluetooth Firmware

When the Bluetooth firmware of MKGW1-BW Pro gateway has been updated, ***MOKO SMART*** will generally release an upgrade package (a compressed *ZIP* file) for user to upgrade the Bluetooth module of the gateway.

You can use the "***nRF Connect***" App for smartphone to load the upgrade package and upgrade the Bluetooth of the gateway. The App has been released on *App Store* and *Google Play Store* and you can download it for free.

The *nRF Connect* APP uses the Bluetooth of the smartphone to scan and connect to the Bluetooth of the gateway, and transmits the upgrade data via OTA (over-the-air).

The gateway only starts to broadcast its wireless signal within 1 minute after the gateway is powered on or restarted. Therefore, you need to reboot the gateway so that the *nRF Connect* APP can scan and find the Bluetooth signal of the gateway.

The operations are different when using an Android smartphone or an iOS smartphone.

- **Using an Android smartphone to upgrade the firmware**

Step 1: Copy the upgrade package to a folder in the root directory of the smartphone.

Step 2: Turn on the Bluetooth of the smartphone and use the *nRF Connect* App to scan the Bluetooth of the gateway with the Bluetooth name of **MKBN-GW01** (you can use the filtering function of the App to filter the Bluetooth name).

Step 3: Click the **DFU** button on the top of the screen and select the **Distribution packet (ZIP)** from the file type list, and then select the upgrade package from the smartphone folder.

Step 4: The upgrade process will start automatically and wait for the upgrade to complete. Then disconnect the Bluetooth connection of the gateway.

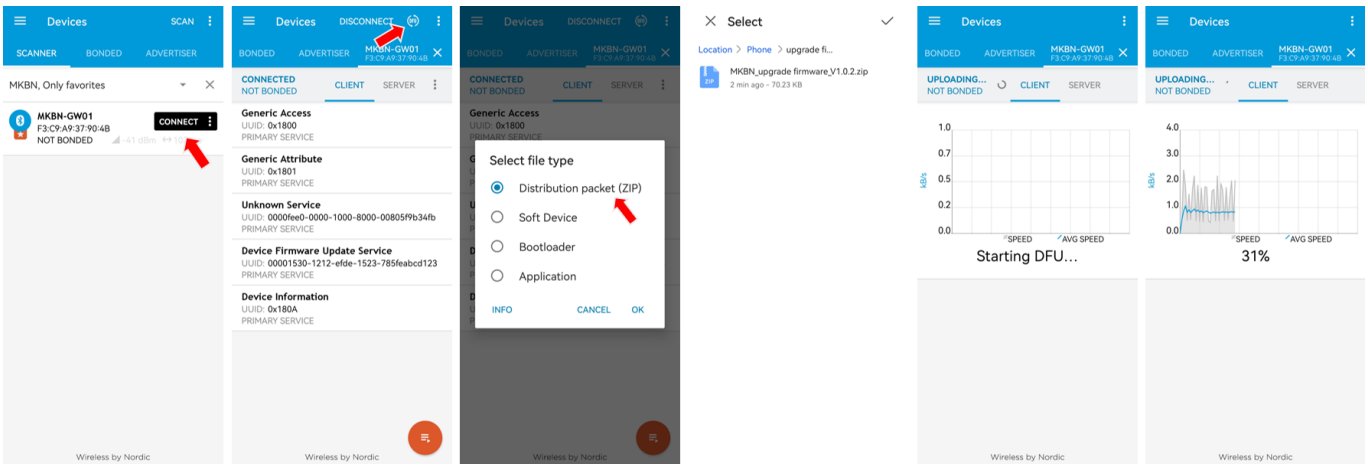


Figure 74: The process of upgrading the firmware by using Android nRF Connect APP

- **Using an iOS smartphone to upgrade the firmware**

Step 1: Use the desktop application **iTunes** to load the upgrade package to the *nRF Connect* App. You need connect your iPhone to your computer using the USB cable. Click your device in iTunes and then click **File Sharing** in the left sidebar of iTunes. You can find the *nRF Connect* on the Apps list and then drag and drop the upgrade

package from a folder or window onto the **Documents** list to copy it to the *nRF Connect* App on your smartphone.

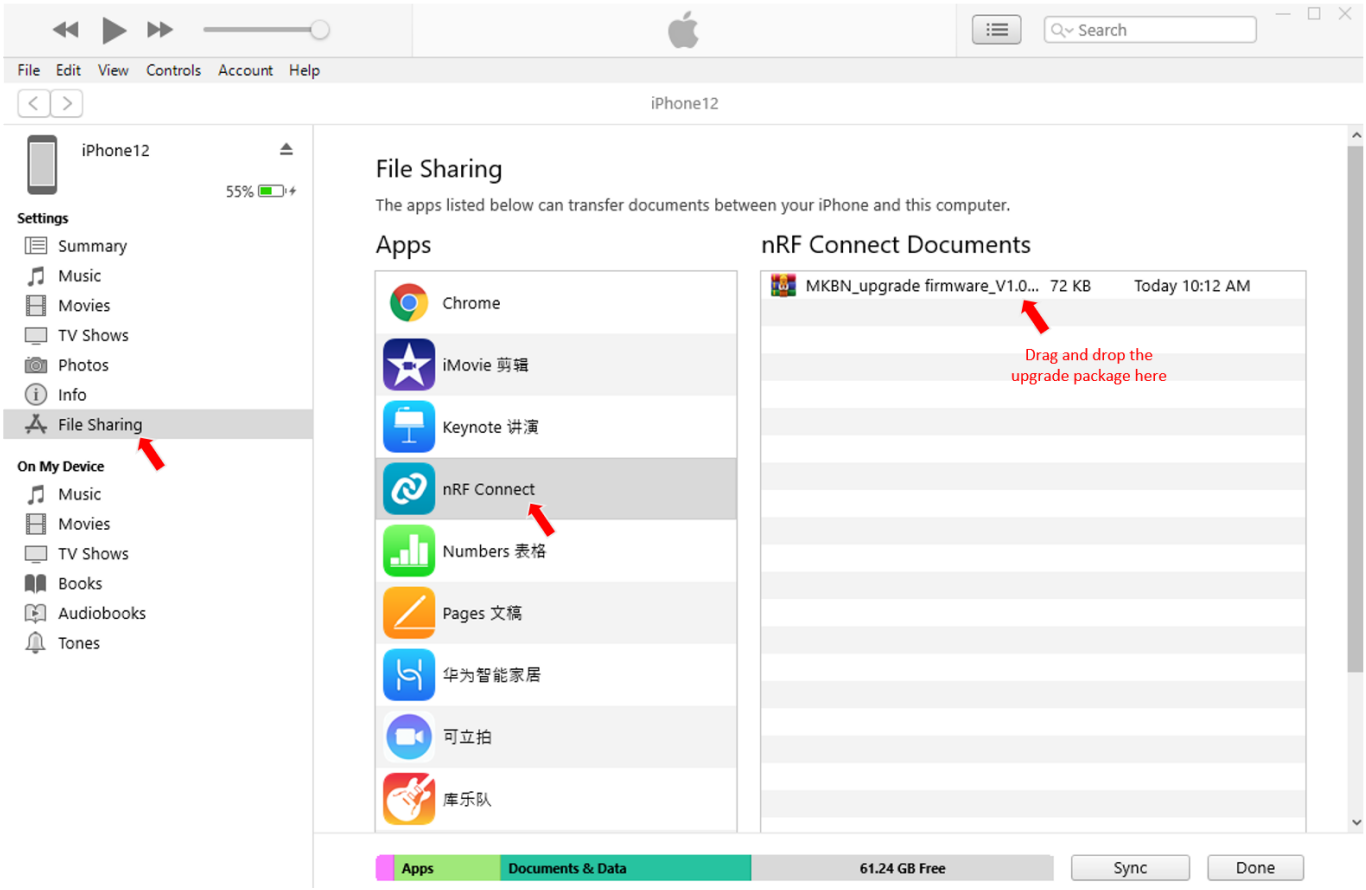


Figure 75: Load upgrade package to the nRF Connect App via iTunes

Step 2: Turn on Bluetooth of the smartphone and use *nRF Connect* App to scan the Bluetooth of the gateway with the Bluetooth name of **MKBN-GW01** (you can use the filtering function of the App to filter the Bluetooth name).

Step 3: Click the DFU option on the top of the screen and select the upgrade package.

Step 4: Click the Start button on the bottom of the screen and the upgrade process will start automatically. Wait for the upgrade to complete and then the connection will be disconnected.

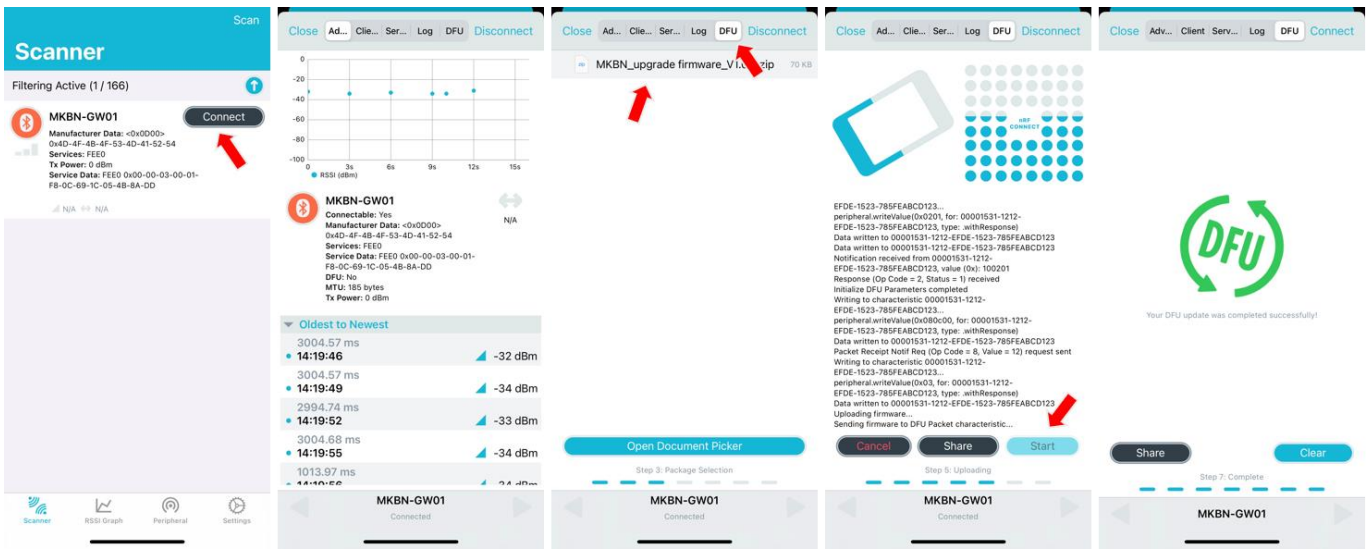


Figure 76: The process of upgrading the firmware by using iOS nRF Connect APP

8.11 One-click Configuration and Upgrade

Triple-click the reset button will automatically load the backup file or Wi-Fi firmware upgrade file from the USB flash drive to the gateway. But you need to name the file as follows:

Backup file name and format – MKGW-BW-Config.tar.gz

Upgrade file name and format (save current settings) – MKGW-BW-Upgrade.bin

Upgrade file name and format (restore factory settings) – MKGW-BW-Factory.bin

Note: *If backup file and upgrade file(s) are all copied to the USB flash drive, the gateway will load the highest priority file. The priority from high to low is the backup file, the Upgrade file that saves the current settings, and the upgrade file that restores factory settings.*

This feature can help you easily configure a mass of gateways without connecting each of them to set their parameters.

For example, after successfully configuring a gateway, copy the backup file of the gateway to a USB flash drive. If other gateways follow the same Bluetooth, Network and Server Settings, you can insert the USB flash drive to other gateways and triple-click the reset buttons to set their configurations.

Federal Communication Commission Interference 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.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement

The product complies with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

Contact

MOKO TECHNOLOGY LTD.

An original manufacturer for IoT smart devices

Address: *4F, Building 2, Guanghui Technology Park, MinQing Rd, Longhua, Shenzhen, Guangdong, China*

E-mail: *Support_BLE@mokotechnology.com*

Website: *www.mokosmart.com*

www.mokoblue.com