KGateway(for KBeacon) Configuration Manual

Revision History

Version	Date	Change Description	Author
V1.0	2017/7/1	Initial	Ning
V1.1	2018/8/20	Add hidden Wi-Fi function	Hogen
V1.2	2018/12/1	Modify network architecture picture	Hogen
V1.31	2020/03/1	Add MQTT configuration example	Hogen
V1.32	2020/11/24	Modify mac filter example	Hogen
V1.33	2020/12/28	Add reset button description	Hogen
V1.4	2021/3/30	Add new functions	Hogen
V1.41	2021/9/22	Add cache message function	Claire
V1.43	2022/9/5	Modify filter setting	Elaine

Catalogue

1. Purpose

This document describes the basic functions and physical interfaces of the KGateway, which is mainly used to guide users to install and configure KGateway.

2. Introduction

KGateway is used to collect the data from KBeacon devices and then sends to the cloud server. Also it can accept data command from the cloud server and forward it to KBeacon, such as updating KBeacon configuration. The KGateway uses open MQTT + JSON API interface for third-party integration.

KG03 is designed for outdoor environment, with IP67 waterproof design and supporting holding pole installation. The hardware and structure inside the KG03 are designed to be reinforced and shockproof, so it can be deployed on moving objects such as vehicles.

The main chip of KG03 is QCA9531, which is an industrial CPU. Therefore, KG03 can be deployed in various harsh outdoor environments, and the equipment can work stably in an outdoor environment of - 30~75℃. In addition, the housing of KG03 can be locked.

Specification

- Suitable for deployment in outdoor environment.
- Material: ABS
- Product size: 220*125*77mm, Installed by wall mounting.
- BLE chipset: Nordic nRF52833; support BLE5.0
- WiFi chipset (MCU): QCA9531
- Power supply: POE or 9~12 VDC
- Scanning ability: 240 Beacons per second

- Wireless distance: 300 meters
- Transmitting way: WiFi / Ethernet
- API protocol: HTTP / MQTT
- Operation temperature：-30 ~ 75℃

3. External interface

3.1 Network interface

The KGateway supports to connect to the internet through following ways:

1. Through Wi-Fi;
2. Through Ethernet cable;

3.2 Power supply interface

There are two interfaces for power supply: micro USB interface and Ethernet POE port;

- POE power supply, directly supply power by Ethernet cable interface, using POE(802.3af) to supply power.
- Micro USB power supply, powered by DC 12V/1A

⚠**Warning: The KGateway can use only one of the two power supplies at a time. Please don't insert two power supplies at the same time, otherwise KGateway may be damaged.**

3.3 LED indicator

KGateway has 2 LED indicators. The specific meanings are as follows:

1. **Red LED indicator:**
   - **Quick flash** (flash 3 times every seconds): indicates that the KGateway is booting.
   - **Slow flash** (flash every 2 seconds): indicates that the KGateway boots successfully but can not connect to the cloud.

2. **Green LED indicator:**
   - **Quick flash** (flash every 2 seconds): indicates that the KGateway

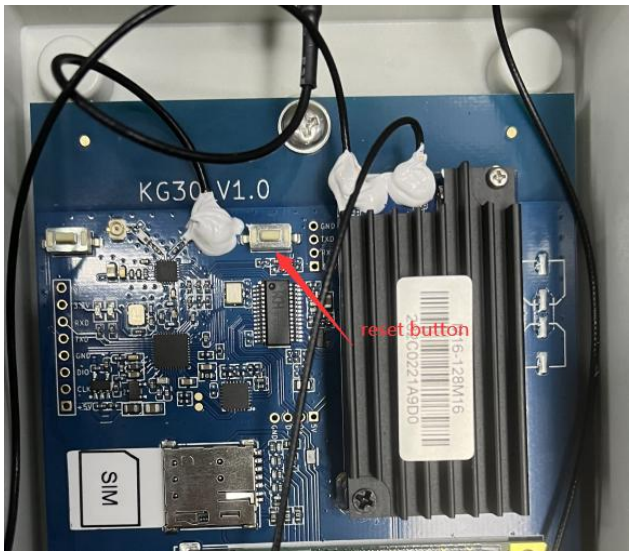
successfully connects to the cloud and report KBeacon advertisement packet successfully.

- **Slow flash** (flash every 10 seconds): indicates that the KGateway connects to the cloud succesfully, but it didn't find any KBeacon devices.

3.4 Reset Button

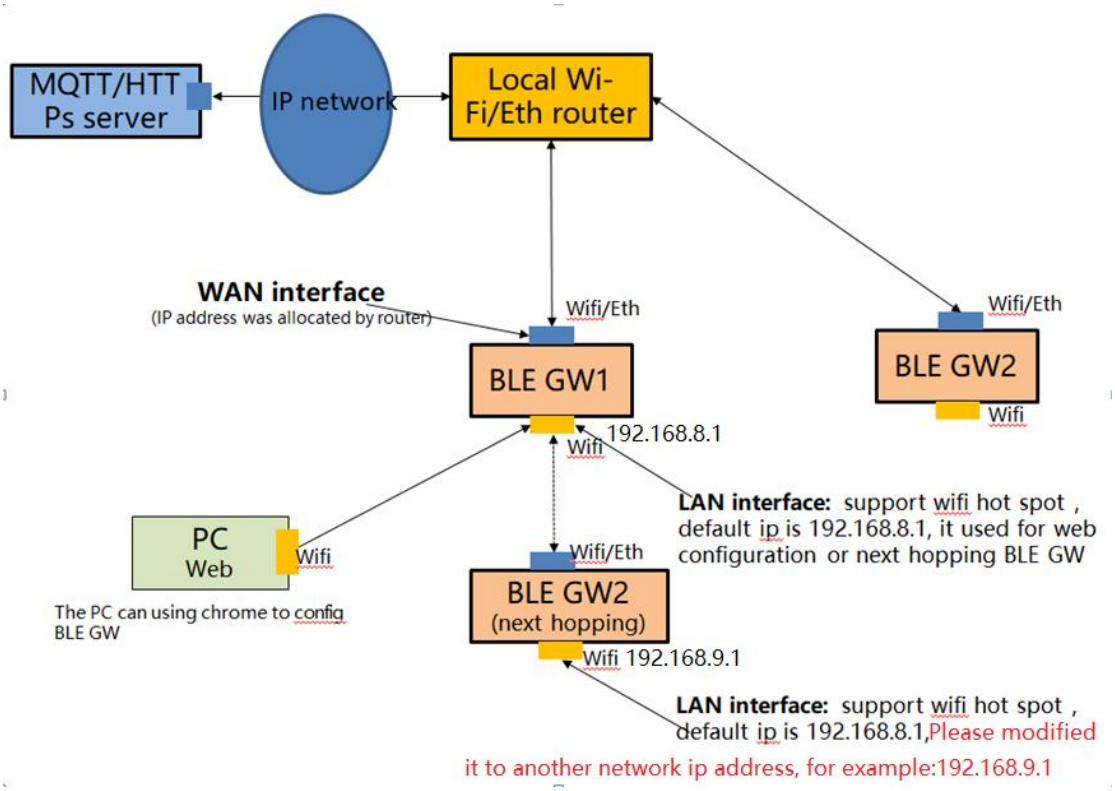
1. Single press button can reboot the gateway.
2. Long press button for more than 8 seconds can restore the gateway to factory settings.

For KG03, the reset button is like below:



4. Configuration

The KGateway is configured in web portal mode. You can use an web browser to configure it. Chrome browser is recommended to use for the configuration.



As shown above, each GW has two interfaces with different IP addresses. One of these IP addresses (referred to as the WAN port) is used to connect to the internet network (MQTT server), which has a series of firewall rule protection. The other IP address (referred to as LAN port, also known as the intranet interface) is used for

Wi-Fi hotspot broadcasting.

WAN Port: This interface supports Wi-Fi and ETH (network wire). KGateway can connect to routers via Wi-Fi or network wire, where IP addresses are assigned by routers. The KGateway is connected to the MQTT/HTTPs server through this interface, so you need to ensure that the network between this interface and the MQTT server is interconnected. WAN address IP address configuration see "4.3.2 configuration WAN port network connection".

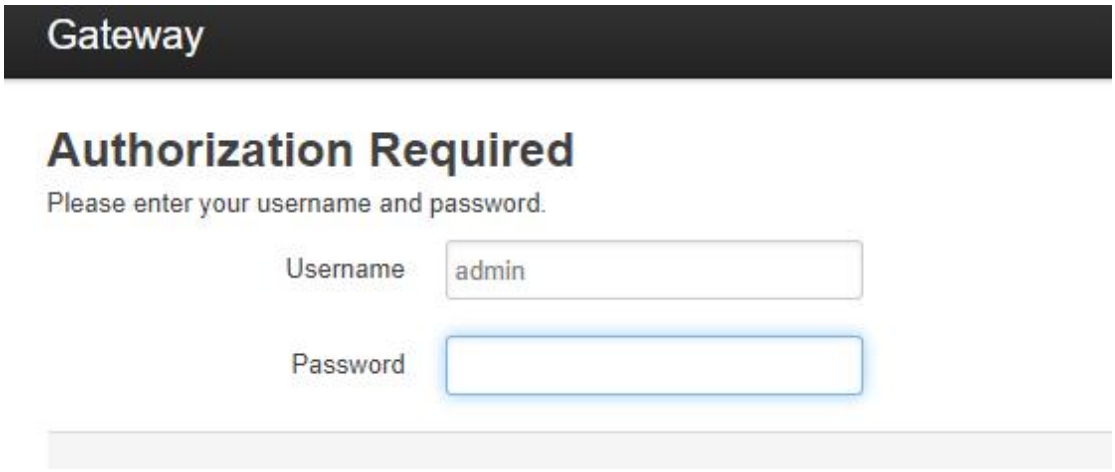
LAN port: This interface only supports Wi-Fi. The default IP address of this interface is 192.168.8.1, PC can connect to this interface through Wi-Fi.

If you need to configure the gateway, you can only configure it through Wi-Fi, and you cannot configure it through the network line (for security reasons, the network line interface only supports the WAN interface).

4.1 Connect to KGateway

- After power on, the KGateway will automatically broadcast Wi-Fi signal, and the default Wi-Fi name is “beacongw_mac address”

- The default Wi-Fi connection password is“12345678”
- The default KGateway configuration IP address is 192.168.8.1
- Login to the gateway by typing http://192.168.8.1 in the browser.
- Enter the user name: ‘admin’ and password: ‘admin’

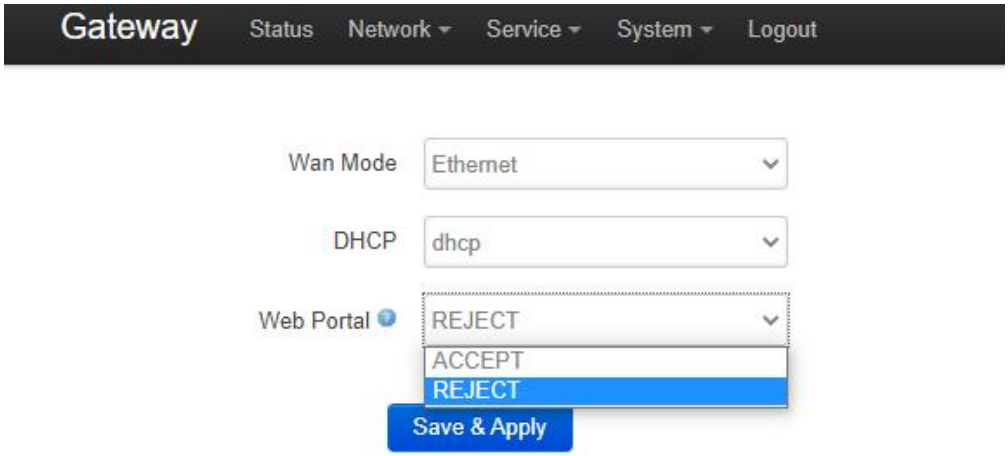


4.2 Network interface

4.2.1 Configure WAN interface

Tap on ***Network-Interface*** to go to the network configuration page. You can choose to connect to the internet network using Wi-Fi /Ethernet connection.

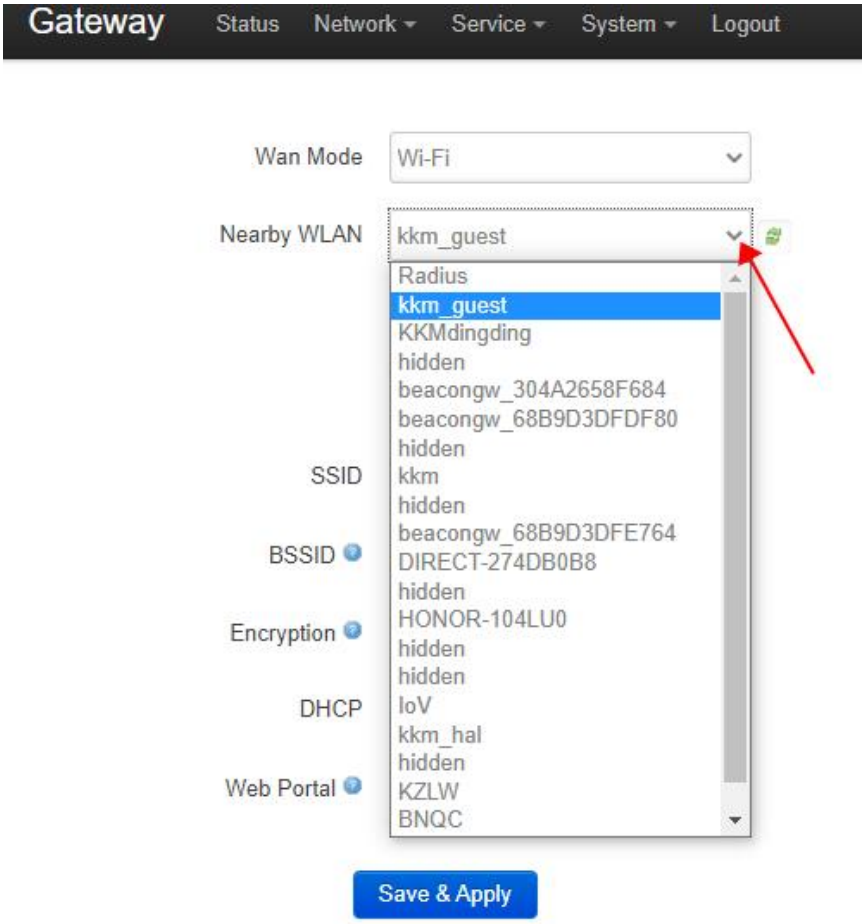
4.2.1.1 Connect to internet by Ethernet

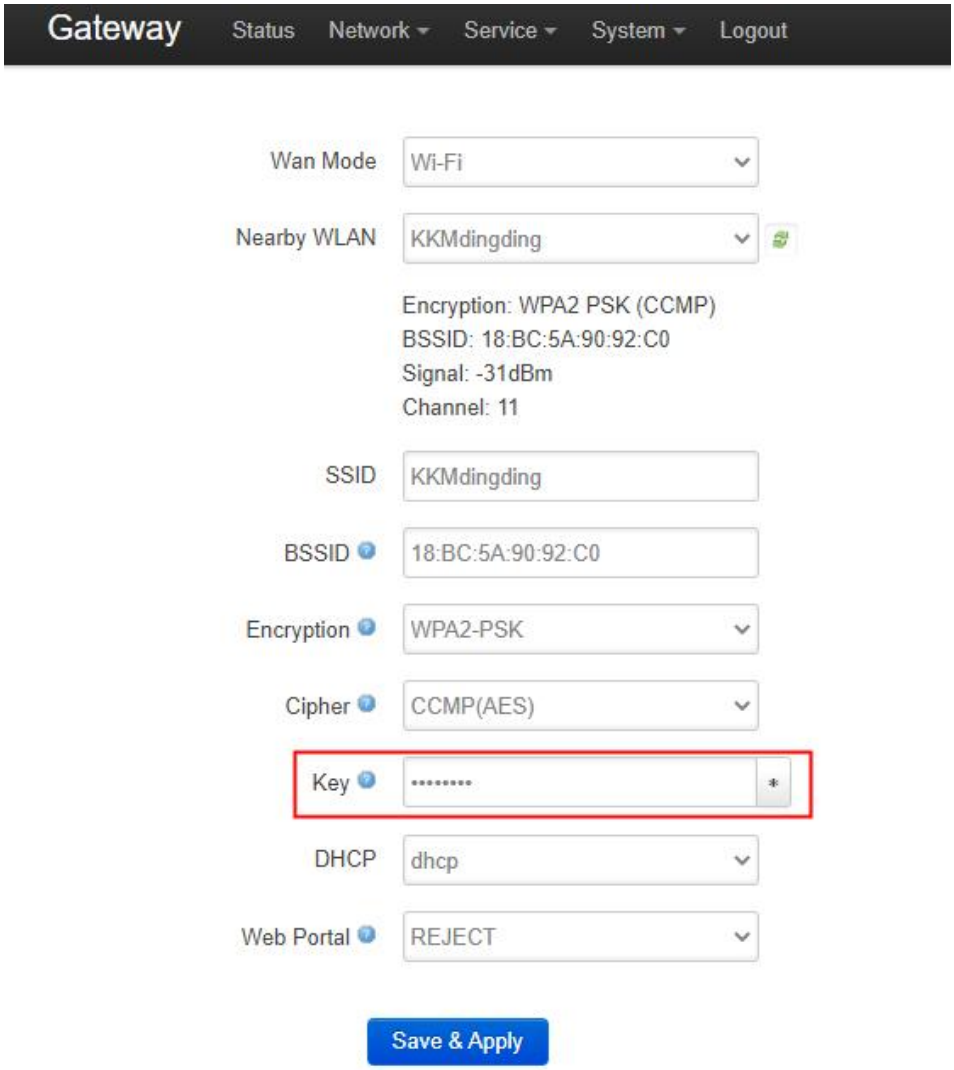


The IP address can be assigned in DHCP or static configuration.

Web Portal: When the option is ACCEPT, you can login to the web portal through WAN IP.

4.2.1.2 Connect to internet by Wi-Fi





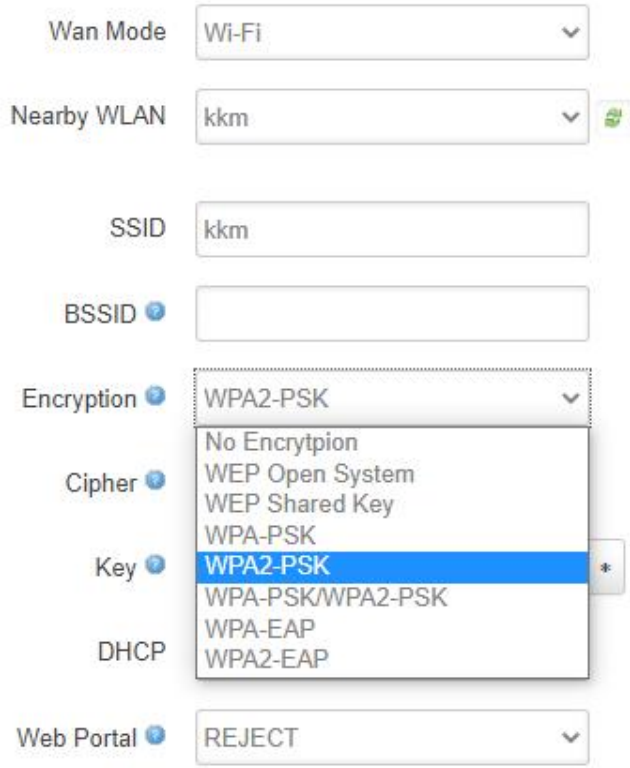
Click on the down arrow of “Nearby WLAN”, then you can select a Wi-Fi that is available.Enter the Wi-Fi password to the “Key” column to connect to this Wi-Fi.

Connect to an hidden Wi-Fi AP:

You can see some Wi-Fi hidden. You should input the Wi-Fi name and password if you want to connect to it.

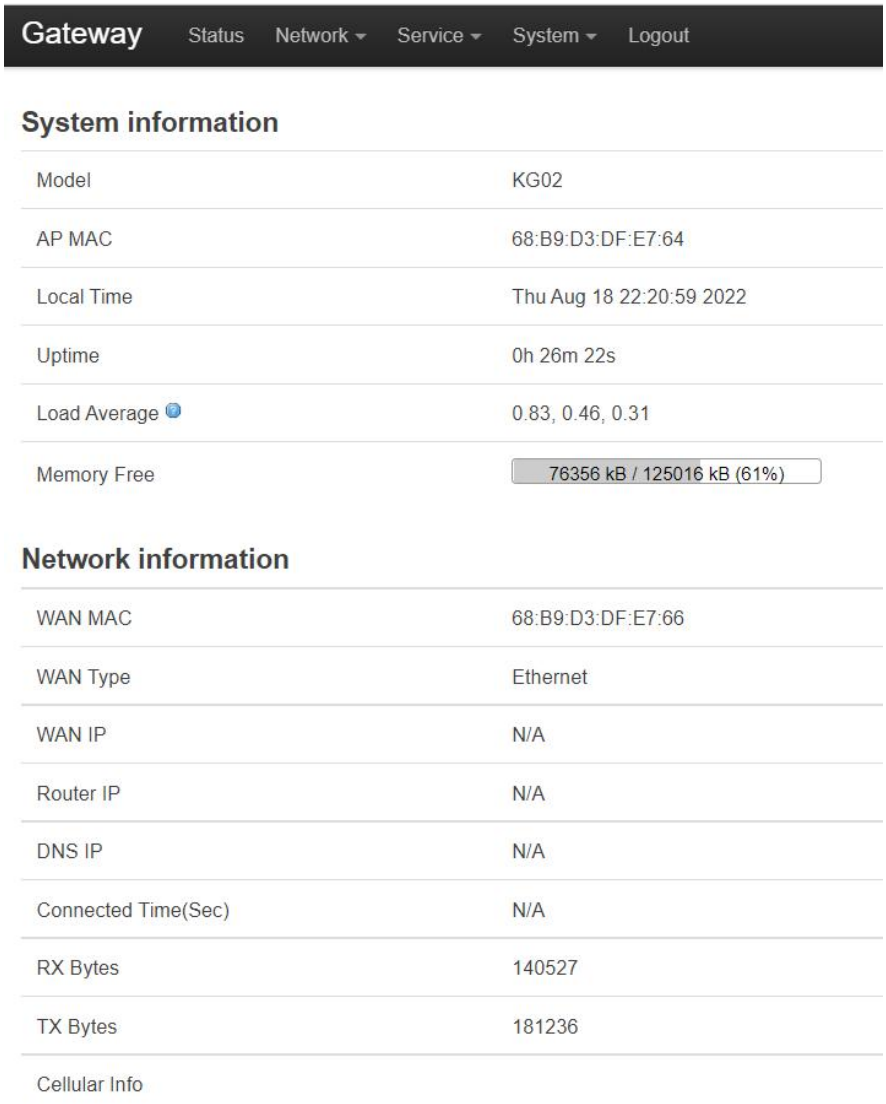
If your Wi-Fi AP name does not appear in the nearby WLAN list, please try to reboot the KGateway. (In “System” page, you can reboot the device)

Encryption: KGateway support many types of Encryption, including WPA2-EAP. This encryption is also known as 802.1x/EAP, 802.1x Enterprise WPA2 or Enterprise WPA2. It is suitable for Enterprise Gateway deployment.


Wan Mode
Wi-Fi
Nearby WLAN
kkm
SSID
kkm
BSSID
Encryption
WPA2-PSK
No Encrytpion
WEP Open System
WEP Shared Key
WPA-PSK
WPA2-PSK
WPA-PSK/WPA2-PSK
WPA-EAP
WPA2-EAP
Cipher
Key
DHCP
Web Portal
REJECT

4.2.2 View the WAN interface status

4.2.2.1 Ethernet status



Model: The model name of the connected KGateway

The **AP MAC** is also printed in the KGateway shell.

WAN IP: The gateway IP address in WAN interface.

Router IP: Your router IP address.

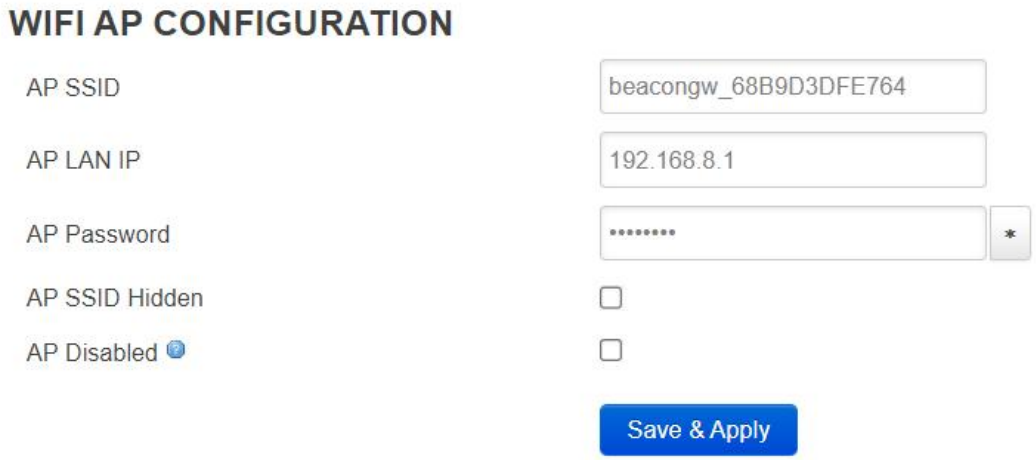
Uptime: How long the network interface has been active.

RX Bytes: received data from WAN interface.

TX Bytes: sent data to WAN interface.

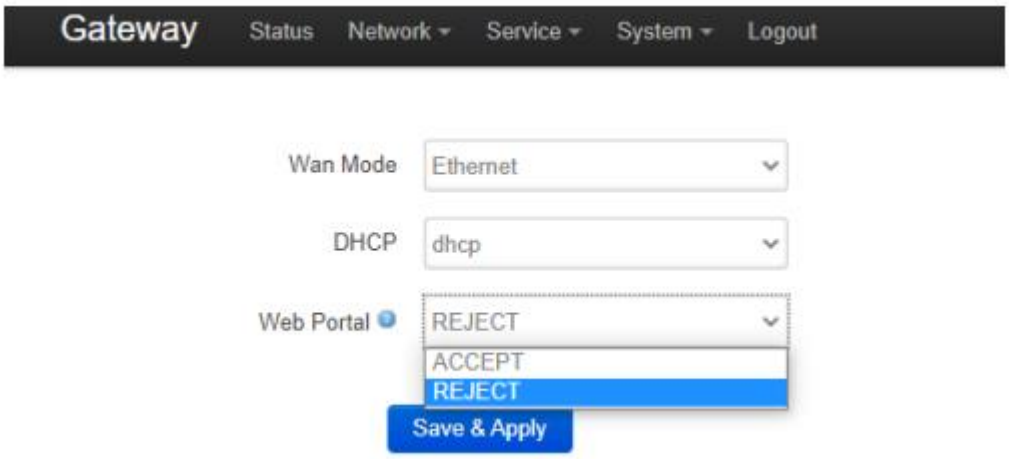
4.2.3 Configure KGateway Wi-Fi AP

Check status about KGateway, you can change the AP LAN IP address.



If 'AP Disabled' is selected, you will not be able to connect to the KGateway through Wi-Fi.You can only connect to the KGateway through WAN IP for configuration.

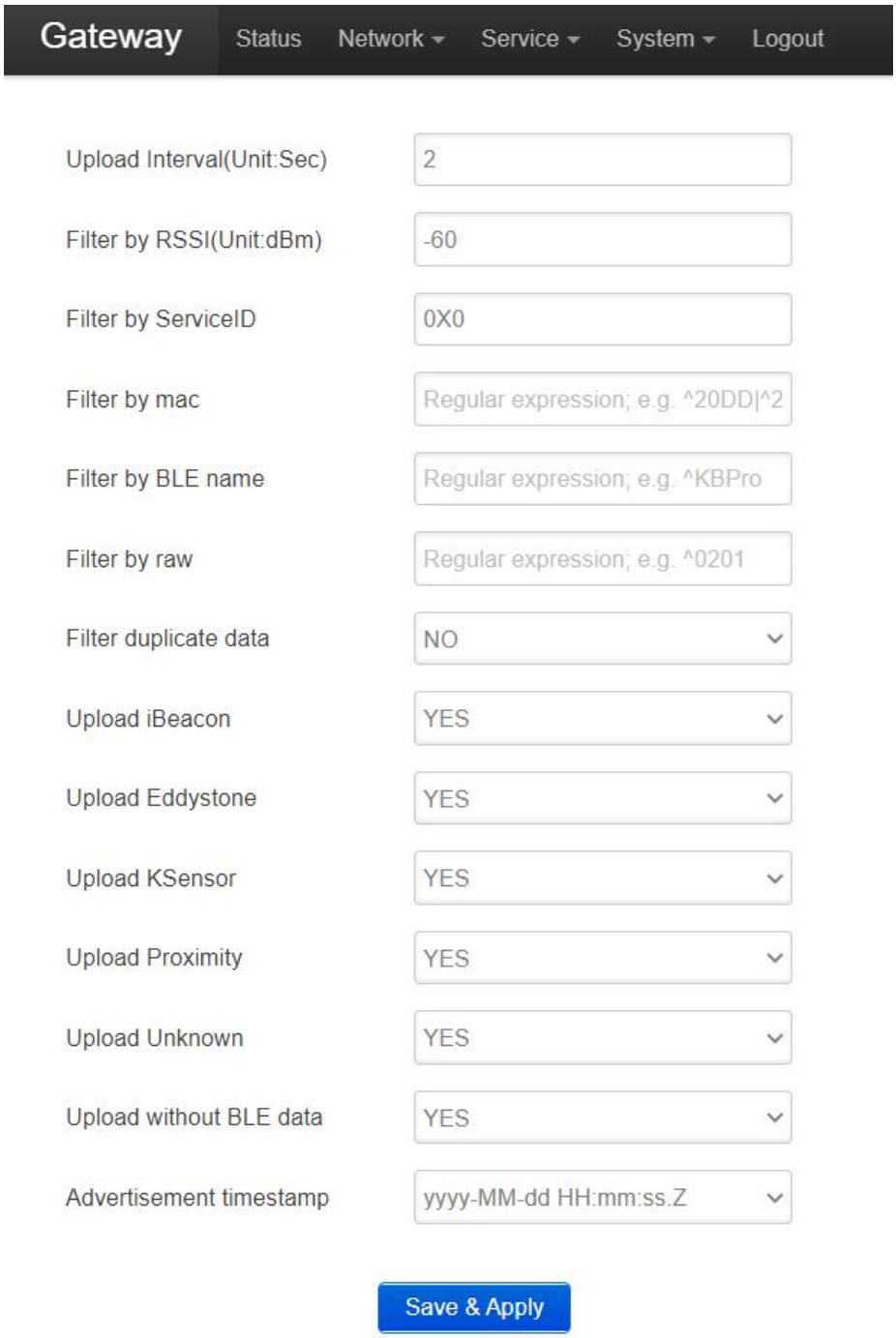
And when AP is disabled, you need to set Web Portal as 'ACCEPT' so you can login the web portal through WAN IP. If you disable the AP but web portal is not ACCEPT, you can restore the KGateway to factory settings.



4.3 Service configuration

Click "Service"-"Filter Setting" and "Cloud Setting"-"Others Setting" to go to the gateway setting page, where each field is defined as follows:

4.3.1 Advertisement Upload Parameters



1. Upload Interval: KGateway uses this parameter to control upload period of modified advertisement data of KBeacon to Cloud.

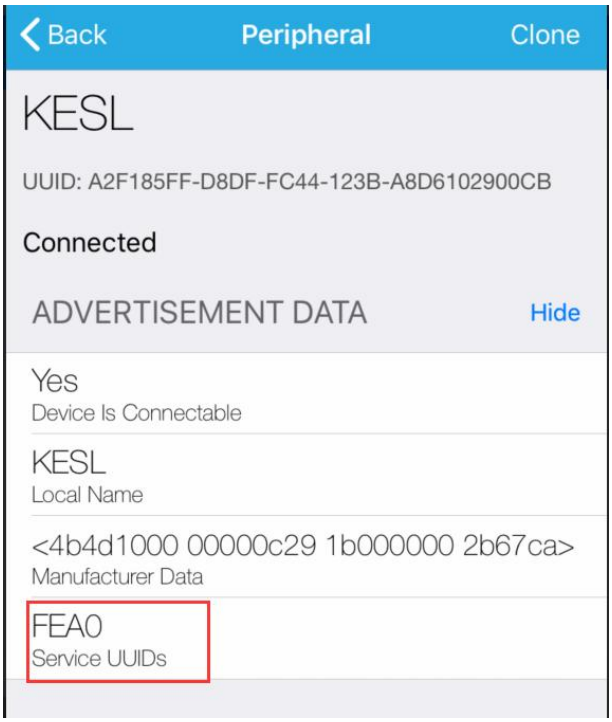
It needs at least **Upload Interval** seconds for KGateway to send advertisement to cloud.

2. Filter by RSSI: If this parameter is set, the KGateway will only report the advertisement packet which signal is > **Min Rssi** value.

3. Filter by Service ID: If this parameter is set, the KGateway will only report the

advertisement packet which includes the setting BLE service ID.

Following example use Lightblue App on IOS to view the device service UUIDs, then you can set the services filter to 0xFEA0.



4. Filter by mac: KGateway can use this parameter to filter KBeacon mac address. This parameter uses Regular express.

For example, if Ble Mac filter value set to ^20DD, then following KBeacon advertisement packet will report to cloud.

- KBeacon1: ble mac = 0x20DD01000002 : report to cloud
- KBeacon2: ble mac = 0xA133DD010002 : not report to cloud
- KBeacon3: ble mac = 0xA10005033DD2 :not report to cloud

5. Filter by BLE name: KGateway can use this parameter to filter device name. This parameter uses Regular express.

Note: BLE name can be carried in the message of advertisement or the scanning response. If you want to filter the advertisement, please ensure that BLE name is carried in the advertisement message.

The device name of KBeacon is carried in the Scan response message.

6. Filter by raw: KGateway can use this parameter to filter raw packet. This parameter uses Regular express.

7. Filter duplicate data: KGateway can use different parameter combinations to filter duplicate data to reduce the advertisement message to cloud.

- No filter: KGateway will not filter the data.

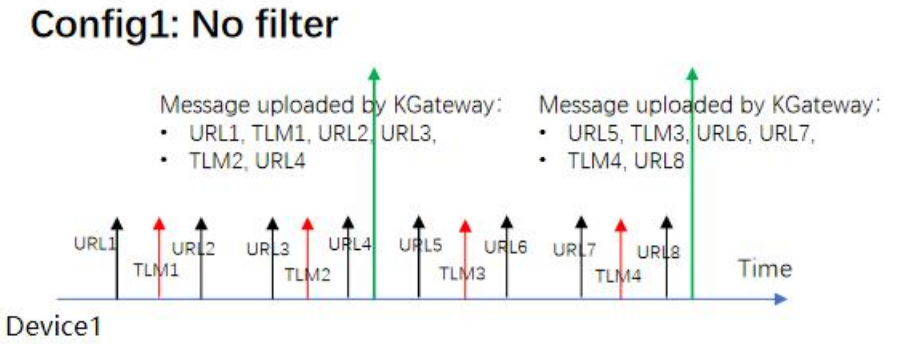
● By mac: KGateway can use this parameter to filter the data of the same mac address.

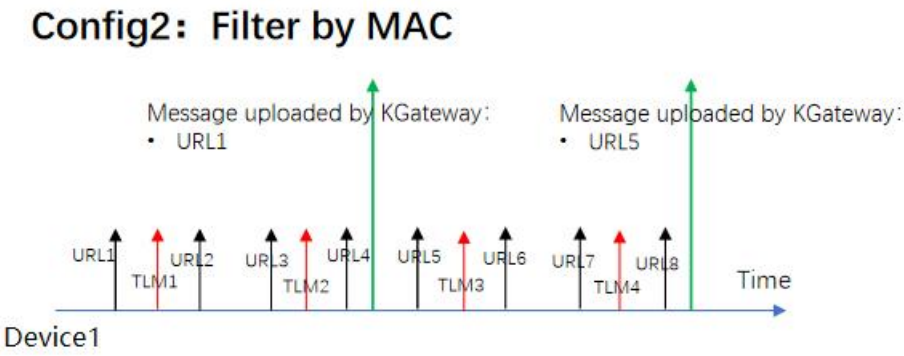
● By mac+type: KGateway can use this parameter to filter the data of the same mac address and advertisement packet type.

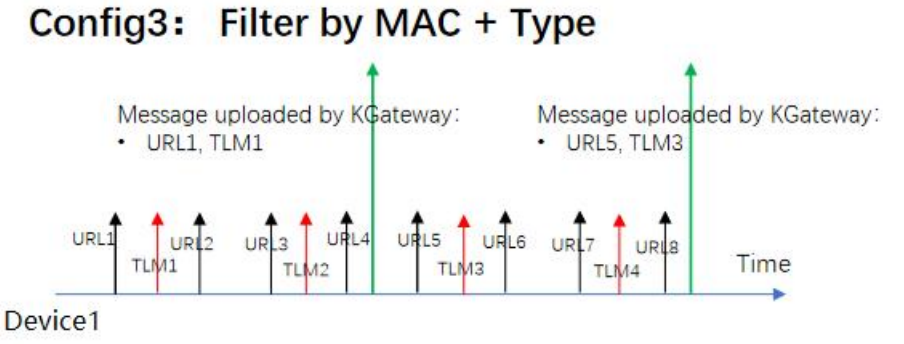
● By mac+raw: KGateway can use this parameter to filter the data of the same mac address and raw packet.

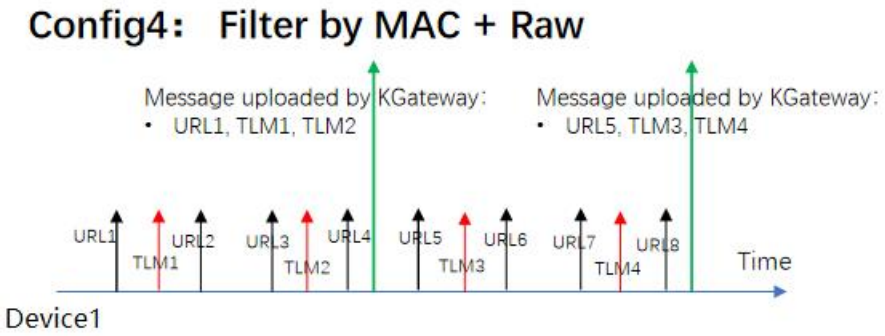
The following is an example of the message uploading of the device1 device:

1. Device1 is configured to broadcast 2 slots, where Slot0 broadcasts URL and the Adv interval is set to 1 second. Slot1 broadcasts the TLM, and the Adv interval is set to 2 seconds.
2. The Upload Interval of KGateway is set to 4 seconds.









Since the URL message does not change, it is only reported once each interval. The TLM content changes every time, both TLM1 and TLM2 will upload.

8. Upload iBeacon: 'Yes' means KGateway will report iBeacon protocol advertisement.

9. Upload Eddystone: 'Yes' means KGateway will report Eddystone (URL / TLM / UID) protocol advertisement.

10. Upload KSensor: 'Yes' means KGateway will report KKM KSensor protocol advertisement.

11. Upload Proximity: 'Yes' means KGateway will report KKM social distancing products advertisement that using hex string.

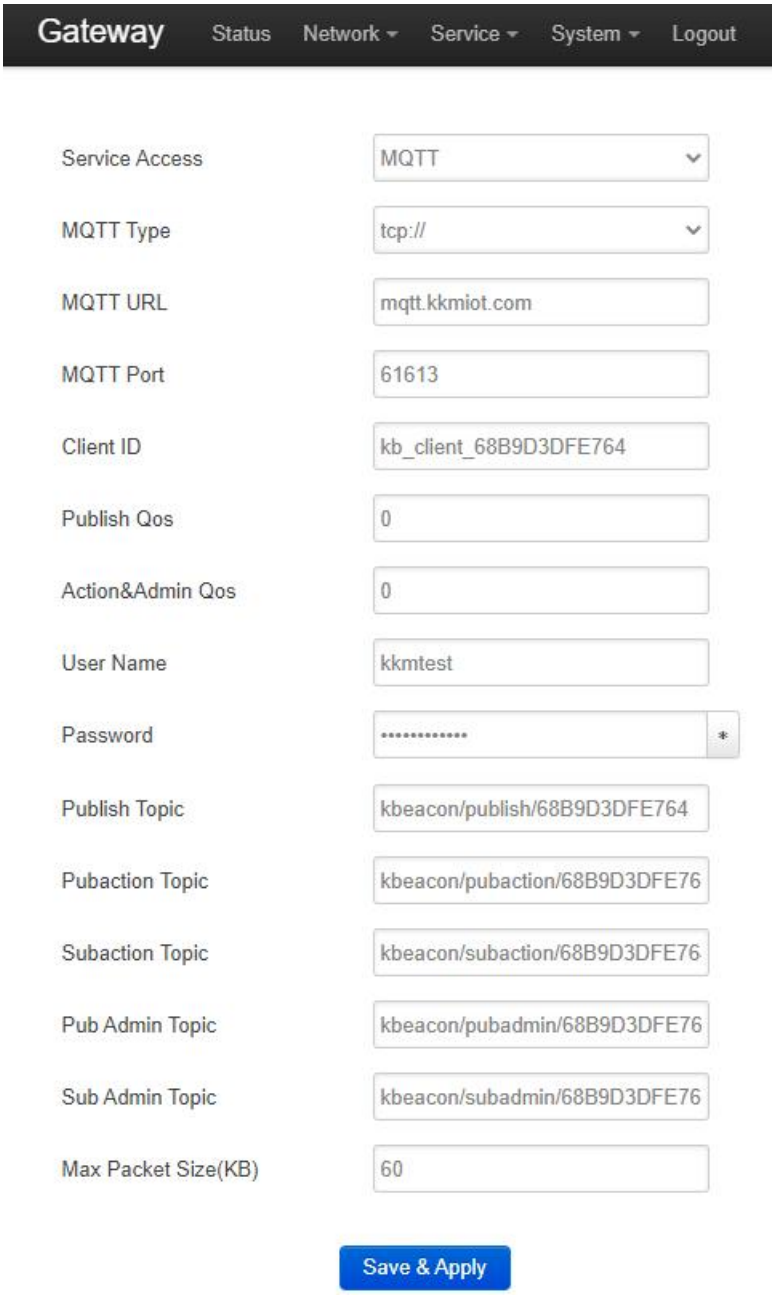
12. Upload Unknown: 'Yes' means KGateway will report unknown advertisement that using hex string.

13. Upload without BLE data: 'Yes' means KGateway will report the advertisement without BLE parameters data. Only report the Mac address and RSSI of device to reduce the advertisement message to cloud.

14. Advertisement timestamp: The three formats of advertisement time.

- yyyy -MM-dd HH:mm:ss.Z
- yyyy-MM-dd HH:mm:ss
- UTC second

4.3.2 MQTT without SSL configuration

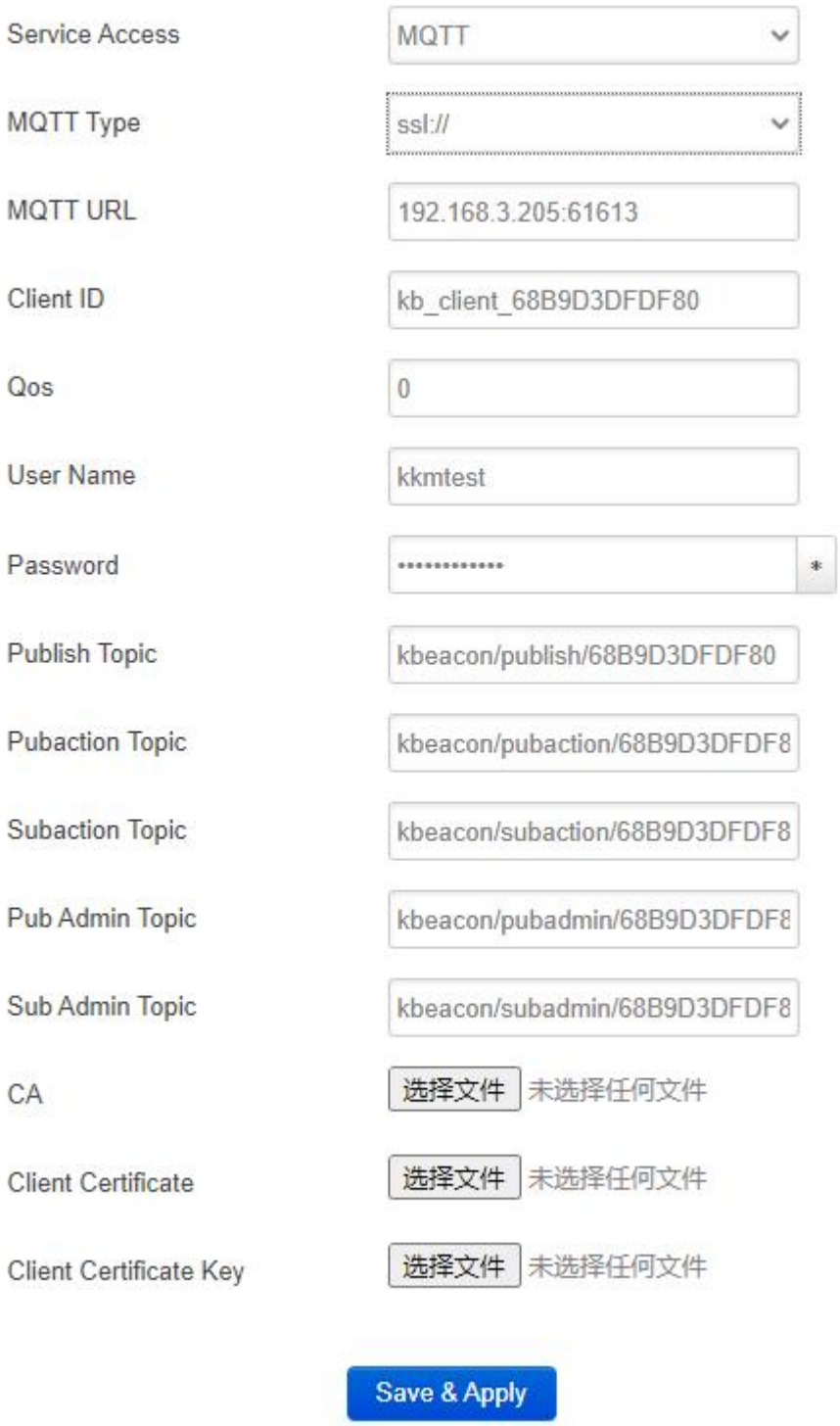


1. **Service Access**: select MQTT and the KGateway will use MQTT protocol to connect to cloud server.
2. **URL:** the MQTT cloud address.
   - TCP:// select TCP for connection.
3. **MQTT port:** The default port is 61613.
4. **Client ID:** MQTT client ID
5. **Publish Qos:** MQTT Qos value for publish topic. The publish Topic Qos is fixed to 0.

6. **Action&Admin Qos:** MQTT Qos value for follow topic:
   - Pubaction Topic, Subaction Topic
   - Pubadmin Topic, Subadmin Topic
7. **Username:** MQTT client user name
8. **User Password**: MQTT client password
9. **Publish Topic:** The KGateway report alive and band broadcast messages to the cloud server through this topic.
10. **Pubaction Topic:** KBeacon configuration request response topic. . If a configuration request is sent to KBeacon, the KGateway will send an execution result message through this topic.
11. **Subaction Topic:** KBeacon configuration request subscription topic. If the server needs to send a configuration request to the beacon, it will send a configuration message to the gateway through this topic.
12. **Pub Admin Topic:** The KGateway configuration command response topic. If the cloud server configures the gateway parameters, such as the filter signal threshold, or the restart command, the gateway responds through this topic.
13. **Sub Admin Topic:** The configuration command topic subscribed by the KGateway. The cloud server can send configuration commands or restart commands to the gateway through this topic.
14. **Max packet size(KB):** This parameter is used to control max packet size when upload advertisement data to cloud.

When the packet size of a message uploaded by the KGateway at one time is greater than Max packet size, the gateway will split the message into multiple messages, and the size of each message will not exceed Max packet size for uploading.

4.3.3 MQTT with SSL configuration



1. **Service Access**: select MQTT and the KGateway will use MQTT protocol to connect to cloud server.
2. **URL:** the MQTT cloud address.
3. **MQTT port**: Our test MQTT server SSL port is 61613.

4. **Client ID:** MQTT client id
5. **Publish Qos:** MQTT qos value for publish action and subscribe action topic. The publish Topic Qos is fixed to 0.
6. **Username:** MQTT client user name
7. **User Password**: MQTT client password
8. **Publish Topic:** The KGateway report alive and band broadcast messages to the cloud server through this topic.
9. **Pubaction Topic:** KBeacon configuration request response topic. . If a configuration request is sent to KBeacon, the KGateway will send an execution result message through this topic.
10. **Subaction Topic:** KBeacon configuration request subscription topic. If the server needs to send a configuration request to the beacon, it will send a configuration message to the gateway through this topic.
11. **Pub Admin Topic:** The KGateway configuration command response topic. If the cloud server configures the gateway parameters, such as the filter signal threshold, or the restart command, the gateway responds through this topic.
12. **Sub Admin Topic:** The configuration command topic subscribed by the KGateway. The cloud server can send configuration commands or restart commands to the gateway through this topic.

SSL Parameters, the KGateway support self-signed certificates MQTT access.

13. **CA**: the CA file about the MQTT server

    You can select the CA file about MQTT test server from your PC.

14. **Client Certificate**: MQTT Client certificate file.

    You can select the CA file about MQTT test server from your PC.

15. **Client Key:** MQTT Client Key file:

    You can select the CA file about MQTT test server from your PC.

4.3.4 HTTP configuration

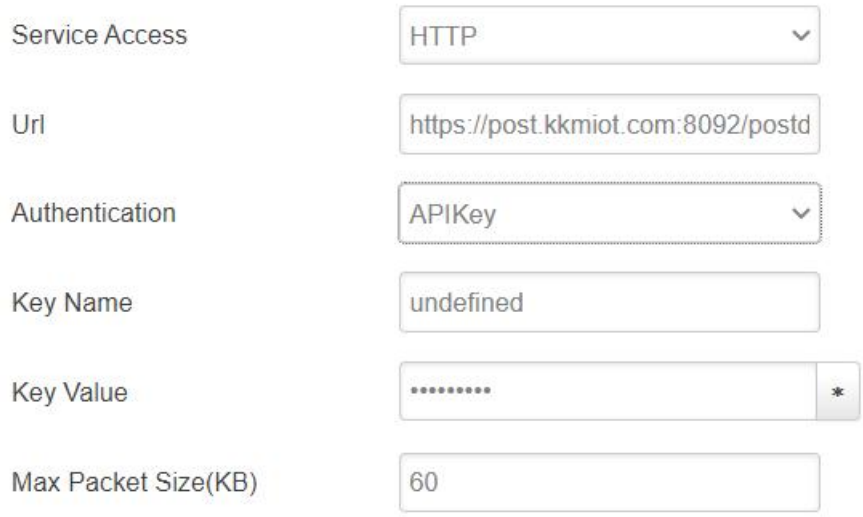
1. **Service Access**: select HTTP and the KGateway will use HTTP protocol to connect to cloud server.
2. **Authentication**: The KGateway support single password authentication for HTTP post.
3. **Url**: The cloud HTTP service.

   We provide a test HTTP server and the URL address is:

   https://post.kkmiot.com:8092/postdata

And the KGateway can support simple password that connect to clouds.

Also the KGateway HTTP protocal can support APIkey to connect



4.3.5 Cache Message

- In some areas, the network may be unstable, and it may be frequently interrupted.
- The gateway can cache the message to memory while the network is down and upload it automatically after network restored.
- Max Cache Time can be set from 60~3600 seconds.

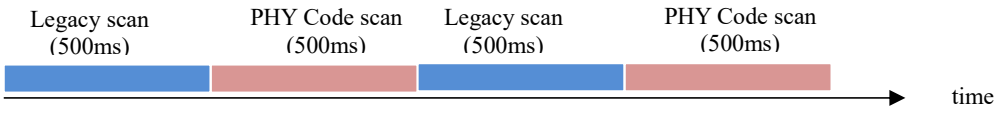
4.3.6 BLE Scan Mode

KGateway support BLE4.0(Legacy) and BLE 5.0 long range (PHY), and also Hybid Mode (Legacy +PHY Code).

When gateway use the BLE5.0 long range (PHY code), the corresponding BLE KBeacon device also need to support PHY Mode.

Since the KGateway can only scan Legacy device or PHY Code device at the same time, you need to further set the alternate scanning time when selecting to set to Hybrid mode:

For example, the Scan alternate interval is 500ms, the scan mode is as follows:



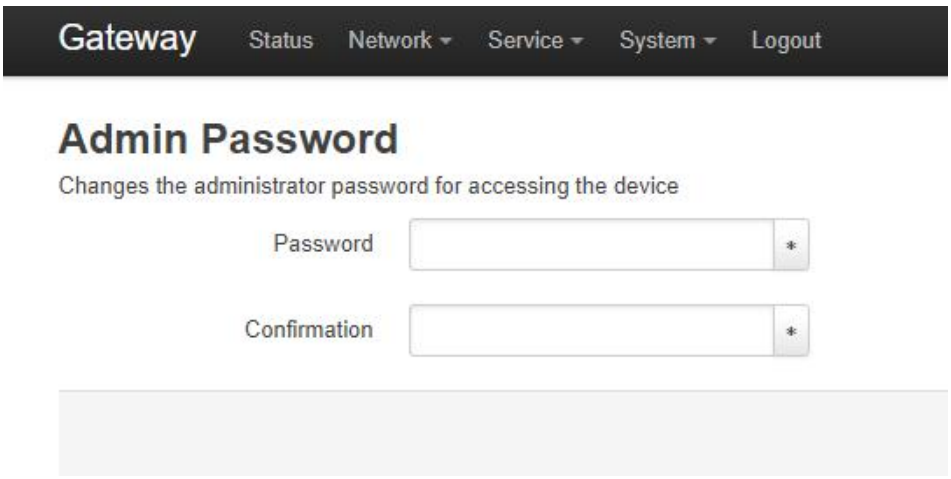
4.3.7 BLE Active Scan

"Yes" means KGateway supports active scanning the BLE device, at this time, the KGateway will report the Scan response message of KBeacon to the cloud.

This function takes effect only when the "Upload Unknown" filter switch was enabled.

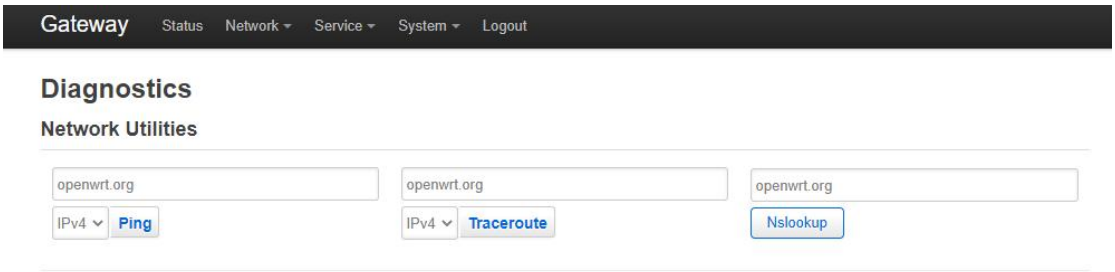
4.4 Modify the Web Portal Login Password

Click "System"-"Change password". The default login password is "admin" and users can change it to other password.

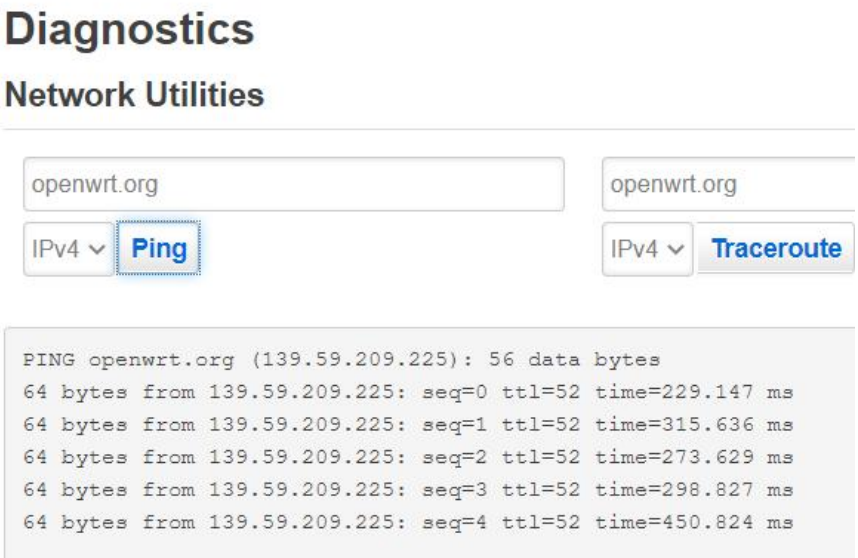


4.5 Network diagnostics

Click “Network”-”Diagnostics” to diagnose the network

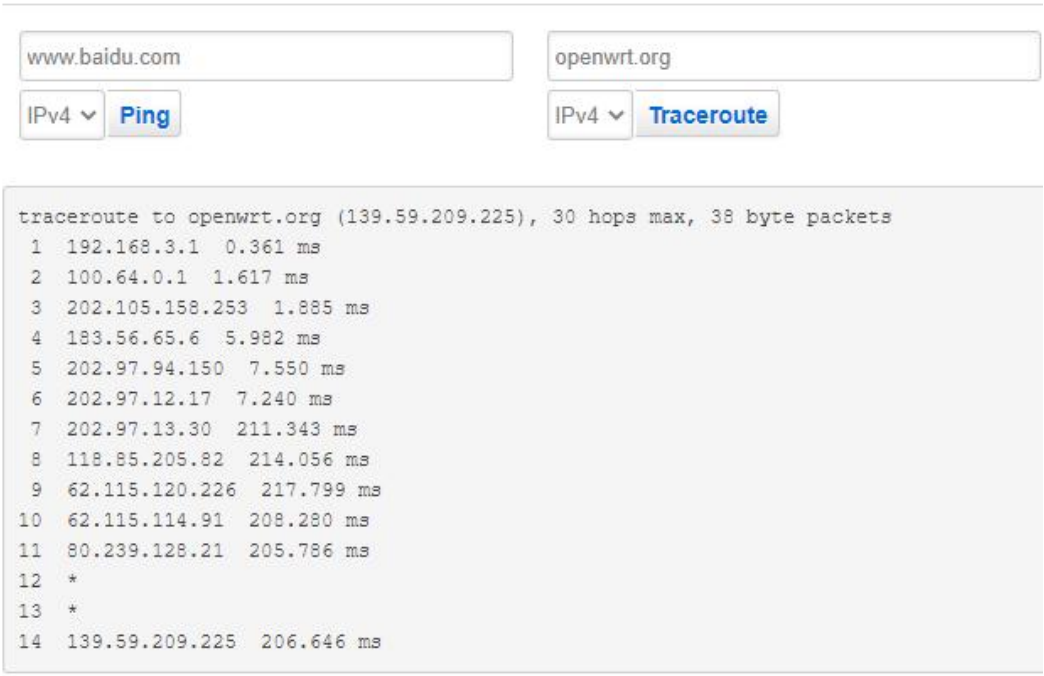


Ping: Enter a website. If the website can be pinged successfully, it means the Network is well connected. If the website can not be pinged, the network might have connection problem.



Traceroute: If Ping fails, use Traceroute to check which procedure caused the

network connection problem.



5. Quickly verify KGateway API

In order for customer easily integrates our gateway, KKM provides test servers for HTTP and MQTT.

5.1 How to verify HTTP API

1. The gateway is setting to MQTT server by default factory setting. So please reference section<< 4.3.4 HTTP configuration>> to change the service's type.

2. KKM provides a test HTTP server, and the address is:

https://post.kkmiot.com:8092/postdata

3. After KGateway connect to the HTTP service success, it will flash green LED and periodically send the KBeacon advertisement data to HTTP server.

4. You can view the reported data on HTTP server by follow address. You should replace the mac address to your KGateway.

https://post.kkmiot.com:8092/viewdata.jsp?mac=D03304001182

5.2 How to verify MQTT API

Download MQTT.fx software:

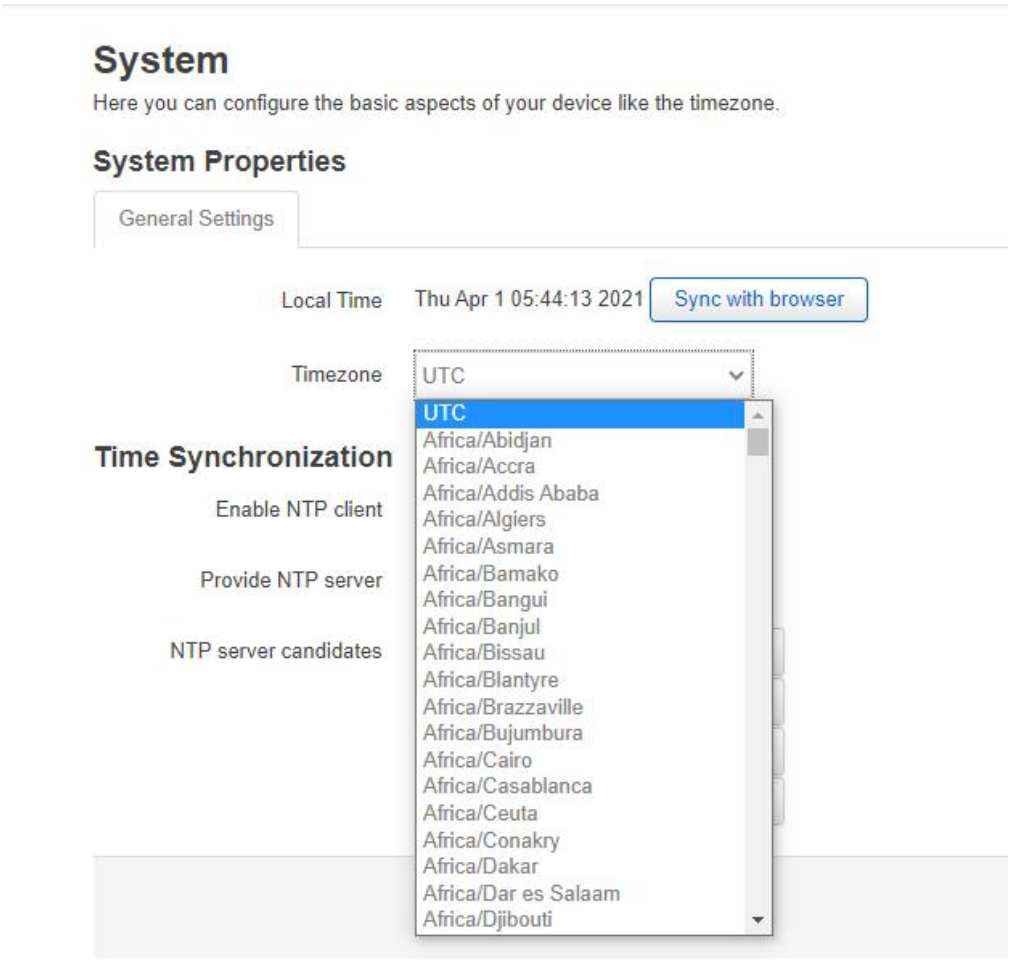
http://www.jensd.de/apps/mqttfx/1.5.0/

Please refer to the document << KGateway API Specification.pdf>> for other details.

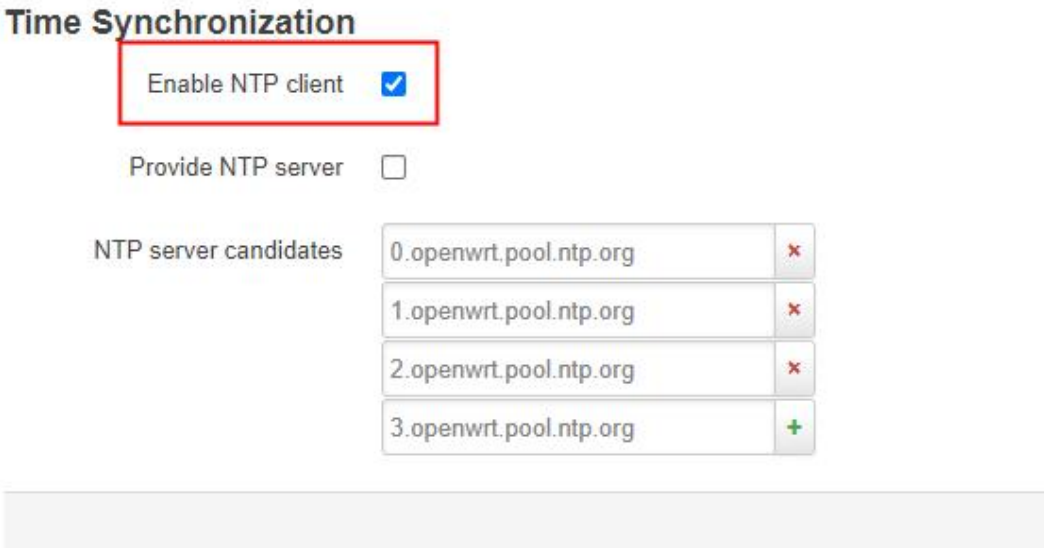
6. More System Settings

6.1 System clock

Click “System”-”Clock”-’Sync with browser’, the gateway automatically synchronize the local UTC time (KGateway uses UTC time by default). If you need the KGateway to use your local time, you can also select the same timezone as your local time.



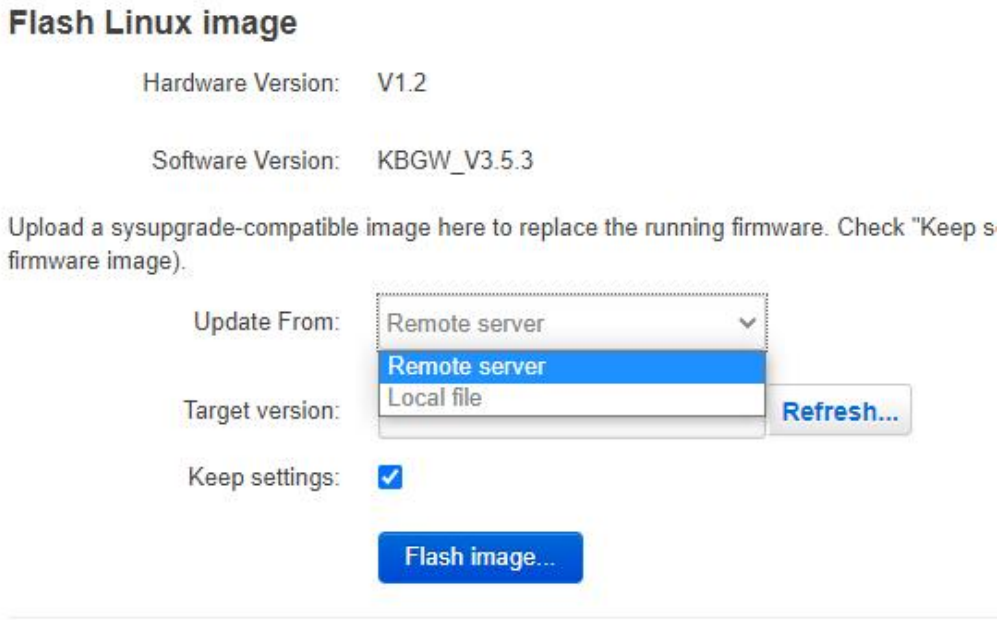
With NTP client enabled, the KGateway also synchronize the UTC time automatically.

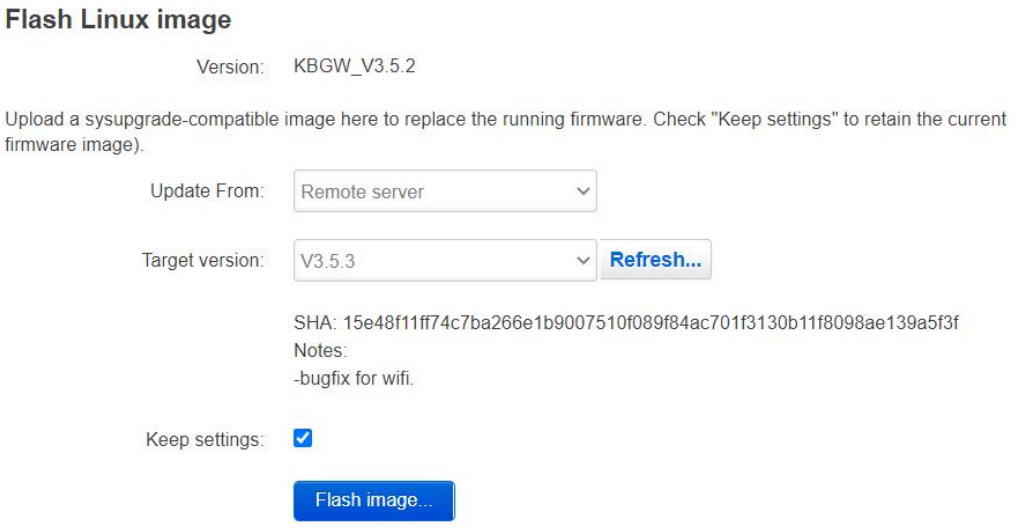


6.2 System update

KGateway support OTA update, and the firmware can be updated from Remote Server or Local file. If update from Remote server, click 'Refresh' to check if there are any new firmware images available.

If you need to upgrade through Local file, please contact KKM sales to obtain the corresponding firmware package.

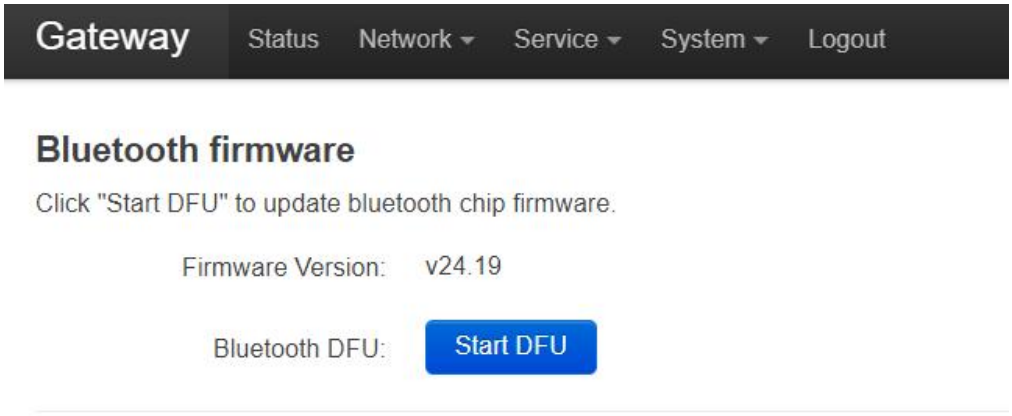




Exception handling: please refer to "Gateway OTA Introduction" when the system cannot be started due to abnormal failure in upgrading the gateway.

6.3 BLE Firmware

The software of the KGateway is composed of two parts. The main software of the KGateway is the OpenWrt Linux system, the another software is BLE firmware package.



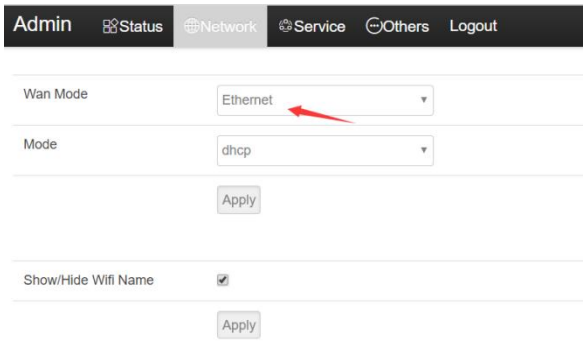
7. Trouble shooting

7.1 The KGateway flash red LED

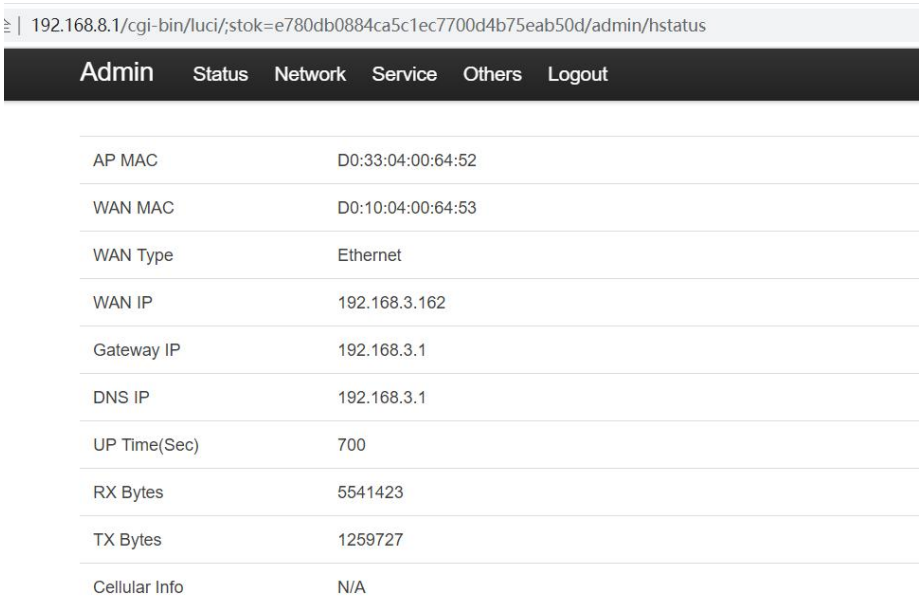
If the KGateway connect to HTTPs/MQTT server successfully, it will flash green LED, otherwise it will flash red LED.

If the KGateway flash red led, please check the connection by following steps:

Step1: Check if the network connection is normal



Check if the network type is right.

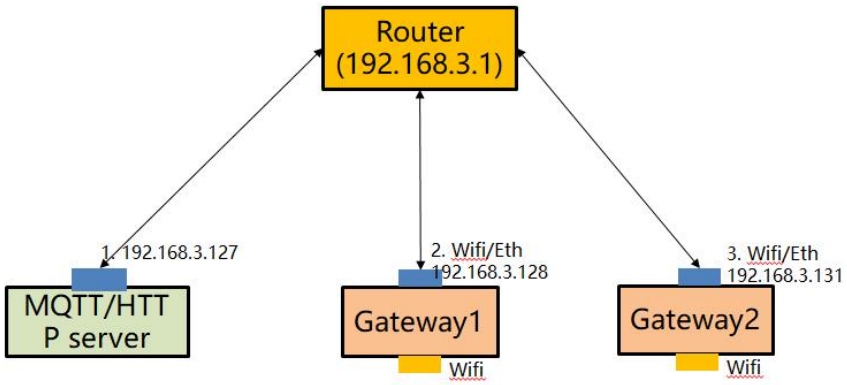


Check the network status:

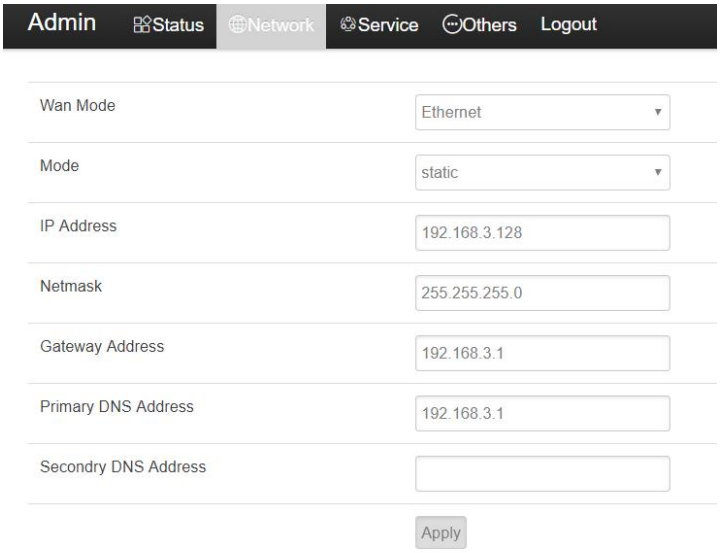
If KGateway connects to network successfully, it will get the IP address and DNS IP address. Also the RX Bytes and TX Bytes will increase.

Step 2: Check the connection between KGateway and cloud server

Scenario 1: The KGateway and Server are deployed in the same LAN



It is necessary to ensure that the KGateway and server are in the same network, that is, the assigned IP address is in the same network. For example, if the IP address of the MQTT server is 192.168.3.127, the Gateway 1 can be configured as the following address (192.168.3.128).

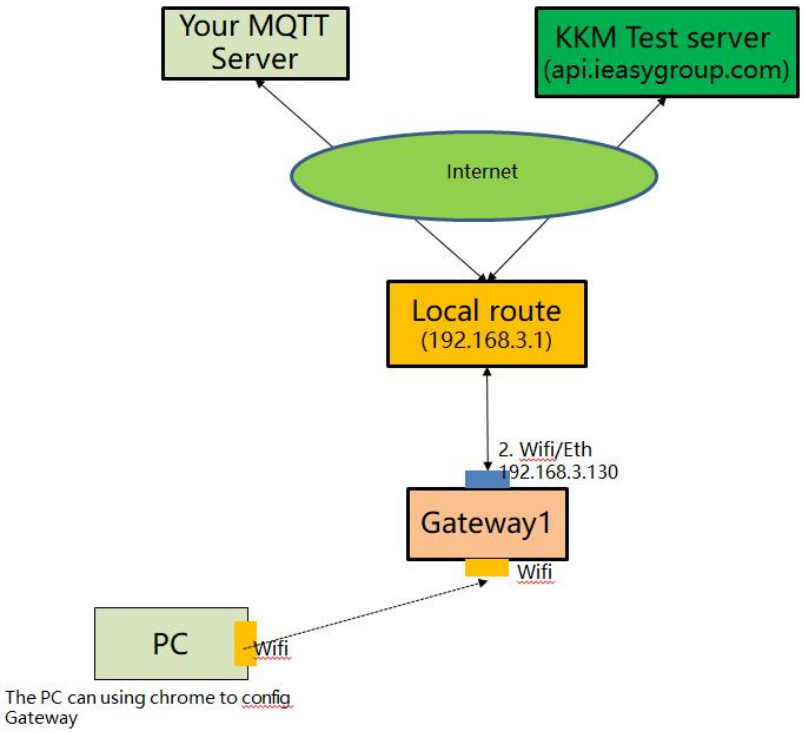


Try to use PING command on MQTT/HTTP server. The PING command is used to detect whether the KGateway and the MQTT server network are connected. If the ping failed, please check whether the LAN is normal.

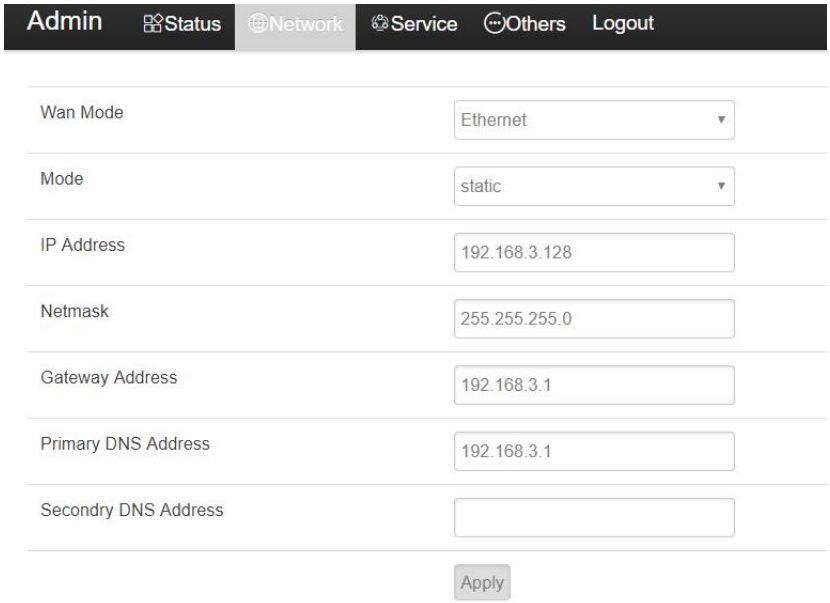
- Type: “Ping 192.168.3.128” on MQTT/HTTP server.

Scenario two: the Servers are deployed in the cloud

Please try to use KKM test server to verify if KGateway can connect to cloud successfully. We provide a cloud-based test server with the IP address of the MQTT server: mqtt.kkmiot.com; it supports both MQTT and HTTPs. The KGateway has been set up as the KKM test server by default.

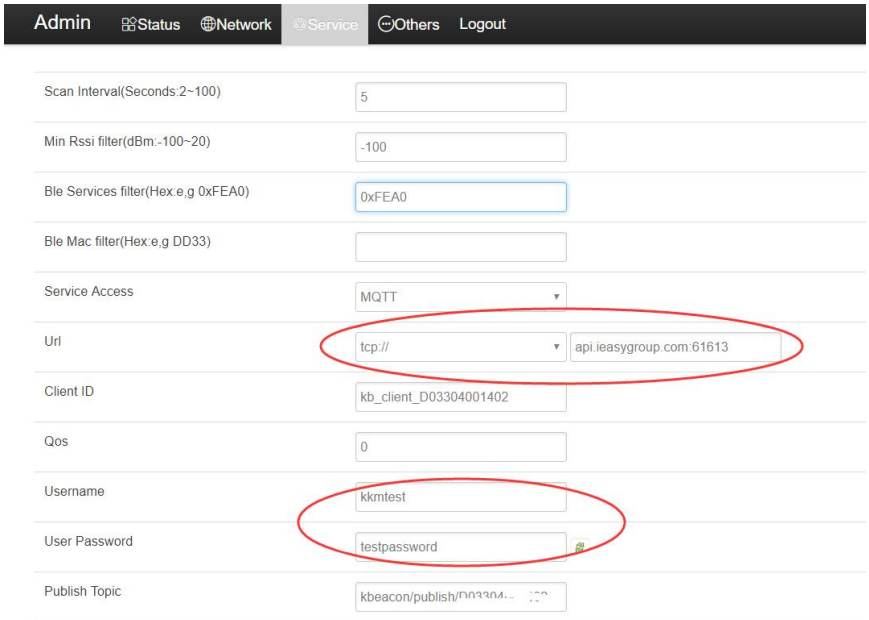


Assuming that the IP address of the router is 192.168.3.1, the IP address of the KGateway can be configured as 192.168.3.128.



KKM MQTT server information：

- Address: mqtt.kkmiot.com:61613
- Test user name: kkmtest
- password: testpassword



Wait 30 seconds to 1 minute after saving the settings. If the KGateway flashes green light, the network connection between the KGateway and the cloud is normal. If

it still flash red LED, the network connection between KGateway and the Cloud maybe failed.

Check if the HTTP/MQTT server is running normally

Scenario 1: Using MQTT server

Please refer to section 7.2 Using third-party MQTT client to verify KGateway in <<KGateway API Introduction>> document.

If MQTT client connection fails, please check:

1) is there a firewall on the MQTT server to prevent other client connections? The default port of the MQTT server is 61613.

2) Whether the MQTT server is installed correctly.

Scenario 2: Using HTTPs server

You can use curl tools to verify if the connection and the key file is right.

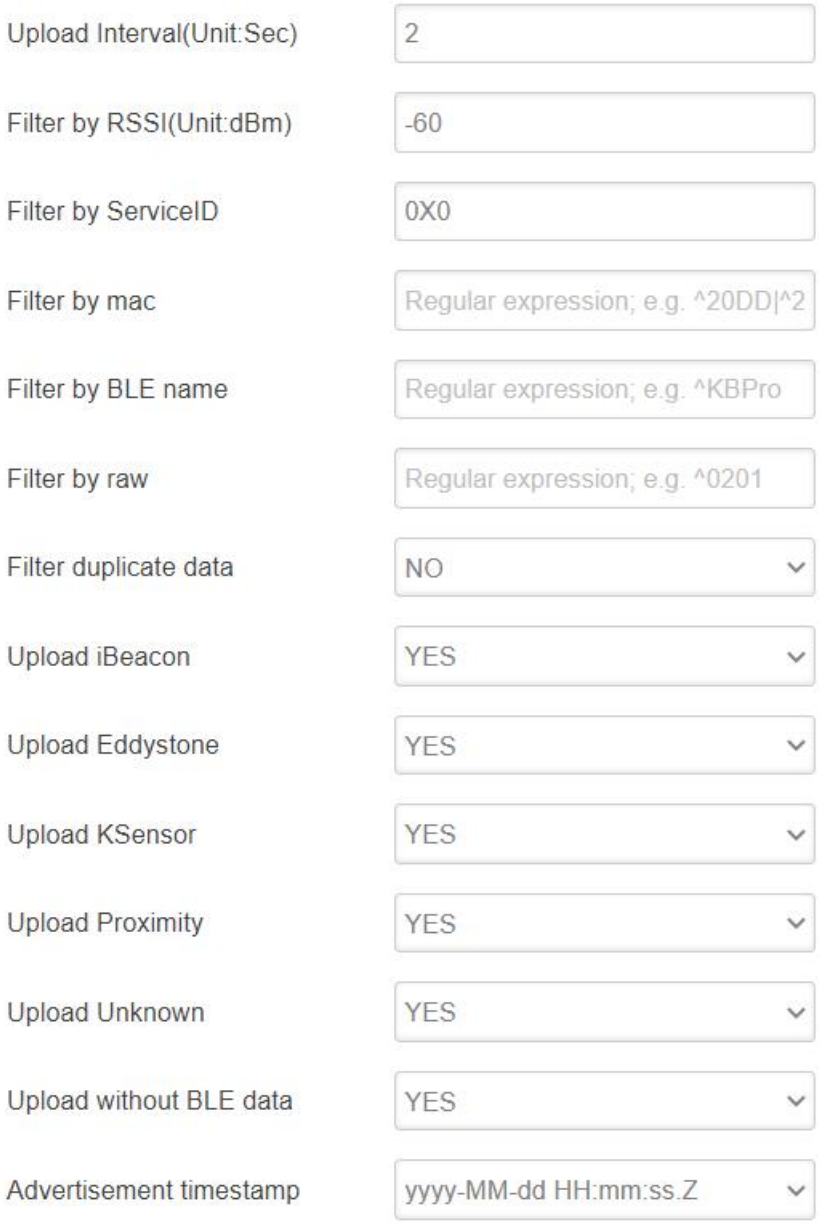
Example:

curl --request POST --url 'http://post.kkmiot.com:8091/postdata' --header 'content-type: application/json' --data '{"msg":"advData","gmac":"A1A2A3A4A5A9","obj":[{"dmac":"AE9639C51701","rssi":"-25","data1":"020106"},{"dmac":"7E4395AB78CC","rssi":"-25","data1":"020106030202180AFF4B4D027E4395AB78CC"}]}' --include

pause

8. Appendix1 Advertisement Upload Filter for different scenario

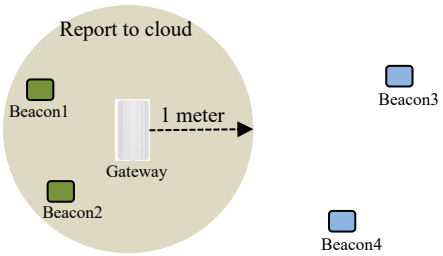
KGateway supports a variety of filtering conditions to meet the filtering requirements in different scenarios.



8.1 Scenario 1: Only upload nearby beacon advertisement

Sometimes we want the KGateway only report the KBeacon that is nearby.

For example, the Gateway is deployed on door, then we need the Gateway only report the beacons signal to clouds which is near the door.



Set the min RSSI filter to -59dBm.

8.2 Scenario 2: Reduce advertisement message to clouds

Sometimes we may use third part MQTT hub to receive advertisement. Then we need to reduce the advertisement message number. Also some MQTT hub may limit the max MQTT message size.

For example:

- If the advertisement packet changed, the Gateway sends the advertisement packet to cloud immediately. We set to 2 seconds.
- The max packet size is set to 60KB.

8.3 Scenario 3: Only upload specific MAC address to clouds

The KBeacon default mac address starts with DD33.

We can set the BLE mac filter to ^DD33 to filter KBeacon device. The Gateway only report KBeacon advertisement packet to clouds.

8.4 Scenario 4: Only upload iBeacon advertisement

Sometimes we want the KGateway only report the iBeacon advertisement packet to cloud, then we can set iBeacon to 'Yes' and others to 'NO'.


```
{
  "msg": "advData",
  "obj": [
    {
      "dmac": "51DC0EA4AE30",
      "refpower": -75,
      "uuid": "FB349B5F80000080001000003CFE0000",
      "majorID": "4115",
      "rssi": -80,
      "minorID": "077F",
      "type": 4,
      "time": "2019-09-02 09:47:42"
    },
    {
      "dmac": "231824EA7DE0",
      "refpower": -59,
      "uuid": "7777772E6B6B6D636E2E636F6D000001",
      "majorID": "0001",
      "rssi": -64,
      "minorID": "0001",
      "type": 4,
      "time": "2019-09-02 09:47:43"
    }
  ],
```

```
  "gmac": "D03304002122"
}
```


8.5 Scenario 5: Only upload Eddystone advertisement

Sometimes we want the KGateway only report the Eddystone advertisement packet to cloud, then we can set Eddystone to 'Yes' and others to 'NO'.


```
{
  "msg": "advData",
  "obj": [
    {
      "dmac": "0A2024EA7DE0",
      "advCnt": 13586020,
      "vbatt": 3050,
      "secCnt": 13655980,
      "temp": 33,
      "time": "2019-09-02 09:51:11",
      "rssi": -63,
      "type": 8
    },
    {
      "dmac": "7996010A33DD",
      "advCnt": 13848450,
      "vbatt": 3113,
      "secCnt": 13917330,
      "temp": 26,
      "time": "2019-09-02 09:51:12",
      "rssi": -75,
      "type": 8
    }
  ],
  "gmac": "D03304002122"
}
```

8.6 Scenario 6: Filter advertisement packet by service ID

The BLE advertisement packet can include Services ID. For example, the Eddystone beacon packet's services ID is 0xFEAA. If we set the service id, then the KGateway will only report Google Eddystone packet.

8.7 Scenario 7: Beacon Location

Sometimes the clouds only need to monitor beacon's RSSI for location. Then the Gateway only needs to scan device's RSSI and mac address. Because the Gateway will not scan advertisement packet data, so we cannot set the Upload iBeacon/Eddystone/KSensor to 'YES'.

In this scenario, the Gateway will only report the beacon's RSSI and mac address to clouds.

advertisement uploaded:


```
{
    "msg": "advData",
    "obj": [{
            "dmac": "3636000A33DD",
            "data1": "",
            "type": 32,
            "time": "2019-09-02 09:22:22",
            "rssi": -59
    }, {
            "dmac": "5055010A33DD",
            "data1": "",
            "type": 32,
            "time": "2019-09-02 09:22:23",
```

```
            "rssi": -44
        }, {
            "dmac": "7355010A33DD",
            "data1": "",
            "type": 32,
            "time": "2019-09-02 09:22:25",
            "rssi": -45
        }],
        "gmac": "D03304002122"
}
```


9. Appendix2 Setup your own MQTT Server

There is some third-party MQTT server software. Following example uses mosquito as an example which test in windows10 environment.

1. Download mosquito:

https://mosquitto.org/files/binary/

2. We installed the software to C:\Program Files\mosquitto

3. Create the password file with username:

```
mosquitto_passwd -c pwfile2.example test
```

3. edit mosquitto.conf file,

add follow line in the file

```
max_connections -1
listener 61613
protocol mqtt
allow_anonymous false
password_file pwfile2.example
```

uncomment follow line:

```
log_timestamp true
log_timestamp_format %Y-%m-%dT%H:%M:%S
websockets_log_level 0
```

4. Run mqtt server

mosquitto -c mosquitto.conf

5. Verify mqtt server

a. Subscribet all topic: we assume the username is test and the password is abcabc.

mosquitto_sub -h localhost -p 61613 -t mqtt -u test -P abcabc

b. publish message to mqtt server:

mosquitto_pub -h localhost -p 61613 -t mqtt -m "hello world" -u test -P abcabc

FCC Statement

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

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

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

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.

RF Exposure Information

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.