Wireless IoT Controller R206 User Manual

For IPK Version 0.0.0.45 and above

Table of Content

1. Introduction

R206 is a highly reliable wireless integrated control box. R206 can communicate with the devices of LoRa protocol. It acts as a gateway between the devices of LoRa protocol and can automatically join the network and execute the configuration. It is the core control of Netvox M2 Internet of Things network. R206 is equipped with Wi-Fi technology; therefore, mobile devices (such as mobile phone) can easily control local IoT devices.

R206 connects to the Internet and combines with the Netvox cloud service platform to achieve remote monitoring. When going out, the user can connect to the cloud to access R206 through the Internet that is achieving remote control of IoT devices

The user can also remotely browse the surveillance camera, master all changes on the other side, and easily realize the Internet of Things remote control.

LoRa wireless technology:

LoRa is a wireless communication technology dedicated to long-distance low-power consumption. Its spread-spectrum modulation method greatly increases the communication distance compared with other communication methods, and can be widely used in long-distance low-rate IoT wireless communication fields in various occasions. Such as automatic meter reading, building automation equipment, wireless security systems, industrial monitoring and control. It has the characteristics of small size, low power consumption, long transmission distance and strong anti-interference ability.

Netvox Private LoRa Protocol:

A private wireless communication protocol based on LoRa long distance, low power consumption, CSMA/CA mechanism, and AES128 encryption mode.

Netvox Private LoRa Protocol band is as follows:

500.1 MHz_China Region

920.1 MHz_ Asia Region (includes Japan, Singapore, Southeast Asia and other regions)

865.2 MHz_ India Region

868.0 MHz_ EU Region

915.1 MHz_ AU/US Region

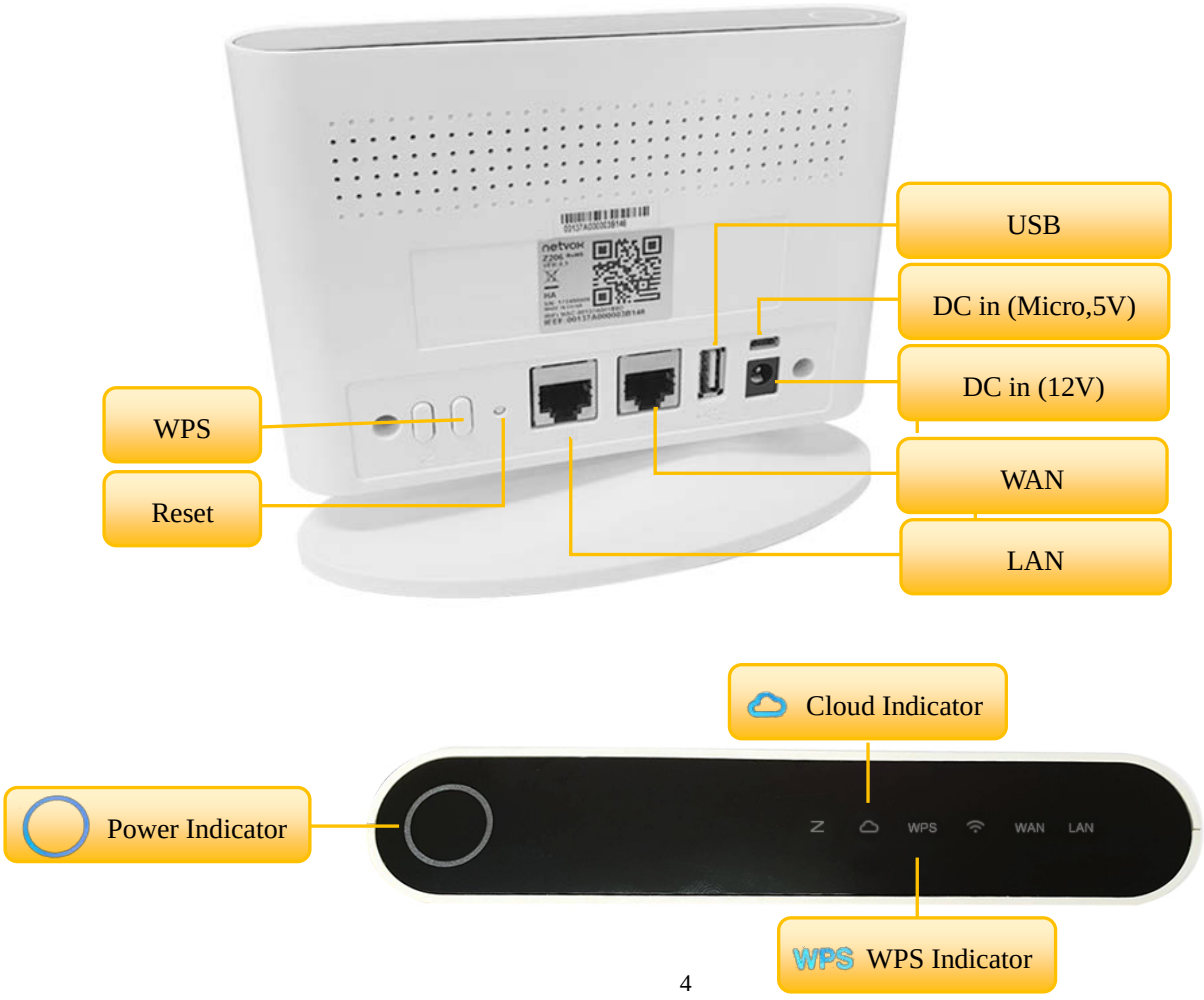
2. Product Appearance

3. Main Characteristics

- Support Wi-Fi 1～14 channels (according to the regulation of each country)
- Two RJ-45 data interfaces
- RTC real-time clock
- Support backup power
- Provide a web interface which can be set through a browser and is easy to operate
- As a Proprietary LoRa gateway, it can limit the devices that be added to the network
- LoRa communication distance 10 kilometers (depending on the specific environment)
- Support LoRa single channel, can connect 100 LoRa devices
- Support Netvox LoRa private protocol wireless smart network

4. Installation and Preparation

4.1 R206 Port/Indicator Instruction



4.2 Hardware Connection

A. Hardware Connection

(1) When use R206 alone

Connect the external network cable to the WAN of R206.

(2) When connect with an IP camera

Connect one end of the network cable to the LAN of R206, and connect the other end to the network port of the IP Camera to form an internal network. Then, connect the WAN port of R206 to the external network cable. (It doesn't matter if do not connect the external network.)

(3) When connect with several IP cameras

It can connect the LAN of R206 to network expansion equipment (such as Router, Switch, or Hub) to increase the number of LANs. The network port of each IP Camera is connected to the network expansion device to form an internal network and connect the WAN port of R206 to the external network cable. (It doesn't matter if do not connect the external network.)

(4) When connect IP Camera wirelessly

Connect the Wi-fi of the IP Camera to the R206 Wi-fi to form an internal network, and connect the WAN port of R206 to the external network cable. (It doesn't matter if do not connect the external network.)

B. Power On

Plug in the DC 12V transformer, and then turn it on after the power indicator lights up, or use a 5V Micro US transformer for power supply.

C. Reset Key Function

(1) Press the Reset button in the power-on state, and the device will restart.

(2) Press and hold the Reset button for more than 5 seconds in the power-on state, and the device will restore to the factory setting.

D. WPS Button Function

(1) In the power-on state, press the WPS button to turn on the WPS function. Press the WPS of the device you want to connect to Wi-fi within three minutes (such as mobile phone, tablet), and the device can connect to Wi-fi.

(2) If press the WPS button again within three minutes, the WPS function will be cancelled.

E. Indicator

Power Indicator	After power on, it stays on.
	After power off, the light turns off.
Cloud Indicator	When connected to the cloud, it stays on.
	When not connected to the cloud, the light is off.
WPS Indicator	After pressing the WPS button, the indicator light starts flashing to indicate that the WPS function is activated. If it successfully connects to the network, the light will stay on.
	If it doesn't connect to the network within three minutes, the light will flash for 5 seconds and then turns off, indicating that the WPS function is off.
Wi-Fi Indicator	When the Wi-Fi function is turned on, the light keeps on.
	When the Wi-Fi function is turned off, the light turns off.
WAN/LAN Indicator	When the WAN/LAN is connected and operating normally, the light stays on.
	When the WAN/LAN is removed, the light turns off.
Zigbee Indicator	R206 does not support this light

F. Backup Power

R206 provides Micro 5v backup power which can be externally connected to mobile power, UPS power supply, etc.

Example:

Power Bank Capacity: 4400mAh/ Input: 100V-240V AC/ Output: 12V 1A

The power bank can make R206 work continuously for more than 6 hours.

(For reference only, please refer to the capacity of each brand.)

5. Network Management Interface Description

5.1 Connect to the device

Please connect the R206 LAN port to your computer with a network cable, power on the R206, and turn on the power switch.

5.2 Check Computer Network Setting

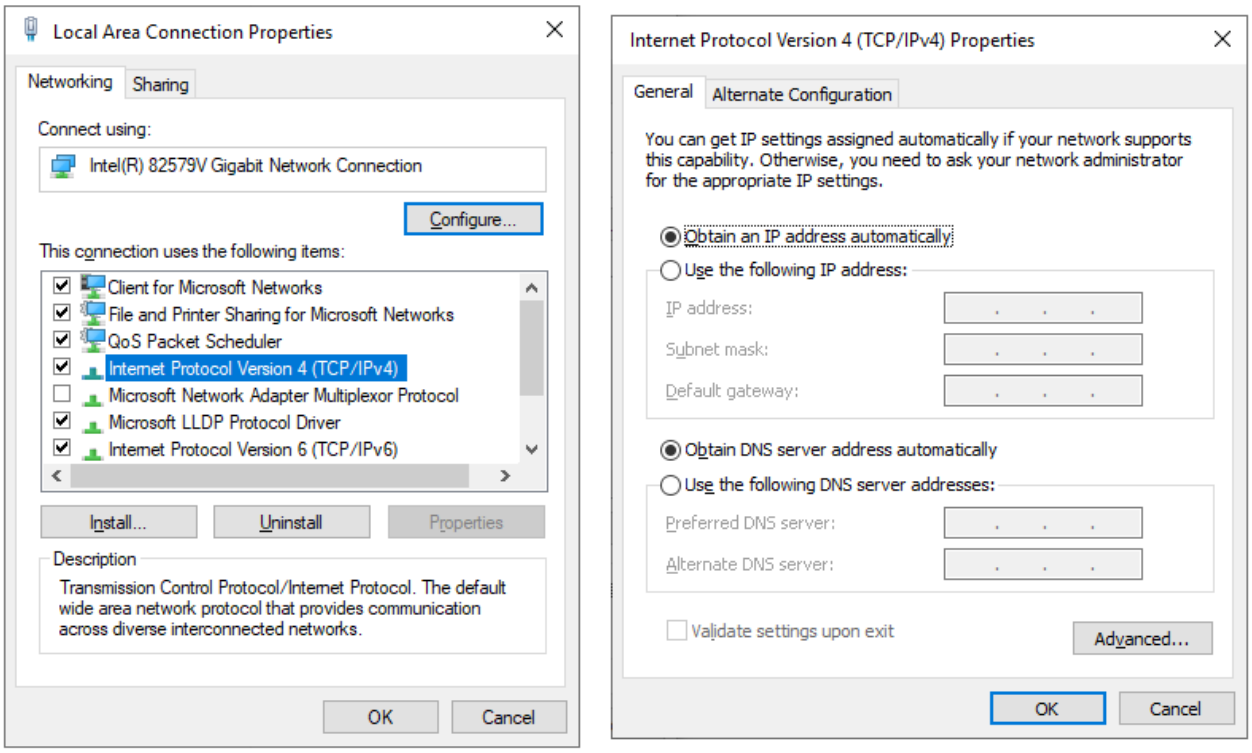
When setting up the network, please make sure that the computer obtains an IP automatically.

(1) Please connect the LAN of R206 to the computer and open the network setting.

(Take Win 10 operating system as an example.)

(2) Click the network icon in the lower right corner of the screen to enter the network setting.

(Or enter “Control Panel” > “Network and Internet” > “Network Connections” > Right click to open “Local Area Connection Properties” > “TCP/IPv4” > Obtain an IP address automatically)



5.3 Log in to the management interface of R206

Open the browser and log in to the setting screen of R206

Default IP:

192.168.15.1

Default account / password

●Administrator:

operator / operator (The applicable gateway version is the shipment before 0.0.0.163)

operator / the last six codes of DevEUI (The applicable gateway version is the shipment after 0.0.0.163)

●Client:

admin / admin (The applicable gateway version is the shipment before 0.0.0.163)

admin / the last six codes of DevEUI (The applicable gateway version is the shipment after 0.0.0.163)

Note:

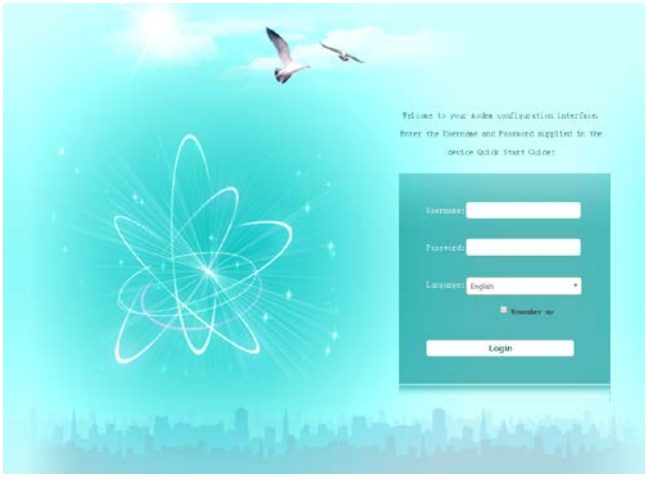
*It is recommended to change the password immediately when using it for the first time.

*Password Restriction: 1. It cannot be 123456.

2. The length must be greater than or equal to 6 digits.

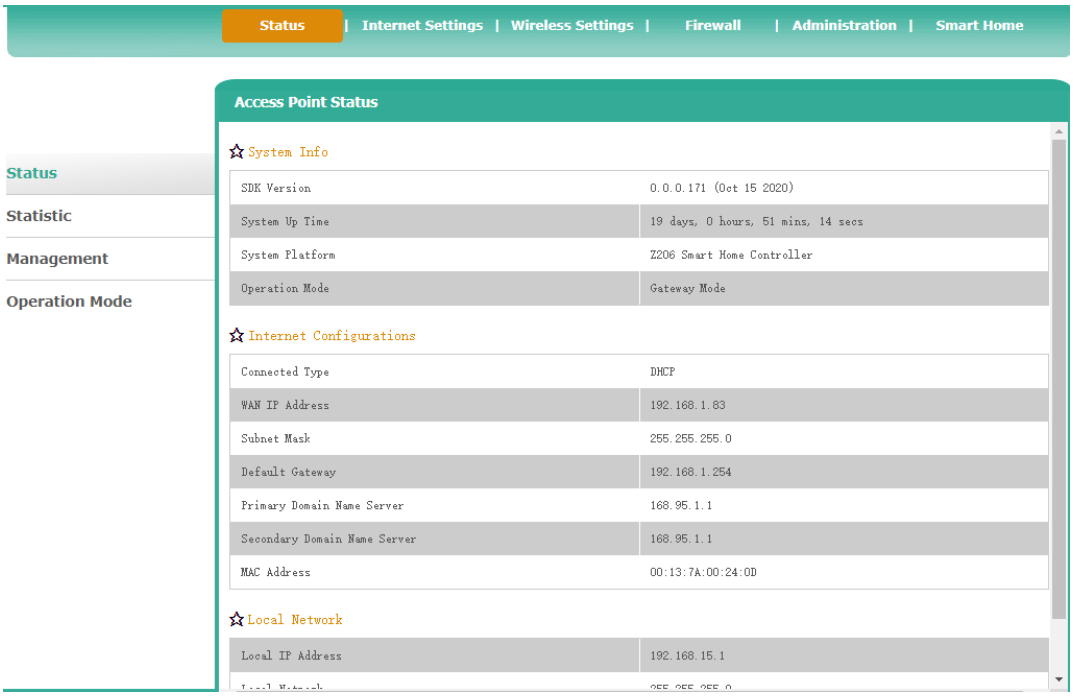
3. It cannot be the same as the account.

*If the user uses mobile phone or tablet to connect to the Wi-Fi of R206 to log in to the setting screen of R206, the Wi-Fi will be disconnected after setting. Therefore, the user needs to reconnect to the R206 Wi-Fi and then refresh the page.



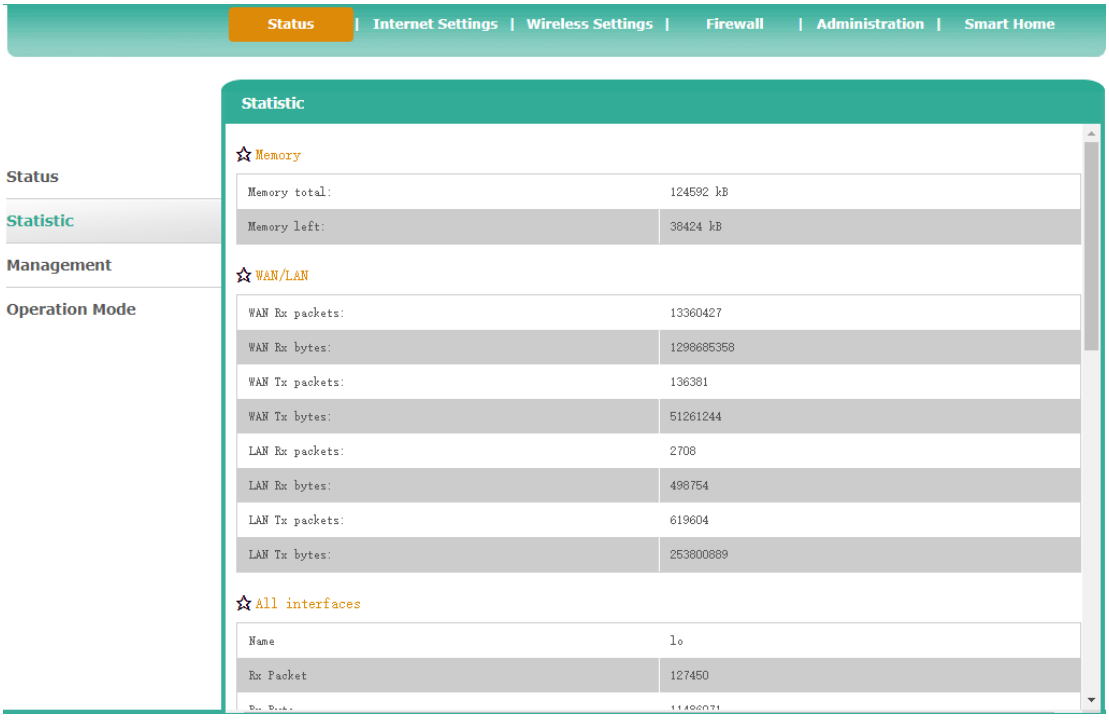
5.3.1 Status

Check the current system information and network status of the gateway



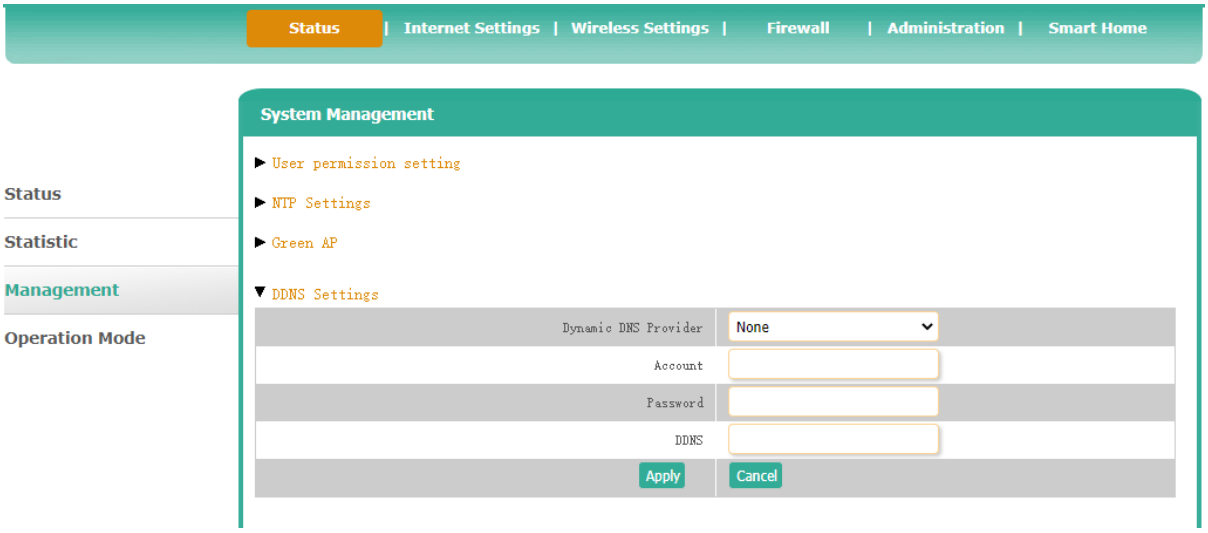
5.3.2 Statistic

Check the statistics of the gateway, including device memory capacity, WAN data packets, and LAN data packets.



5.3.3 Management

Set User permission, NTP, Green AP, and DDNS.



5.3.4 Operation Mode

Change the Operation Mode, such as Bridge mode, Gateway mode, AP Client mode, and decide whether to enable NAT.

A. Bridge mode

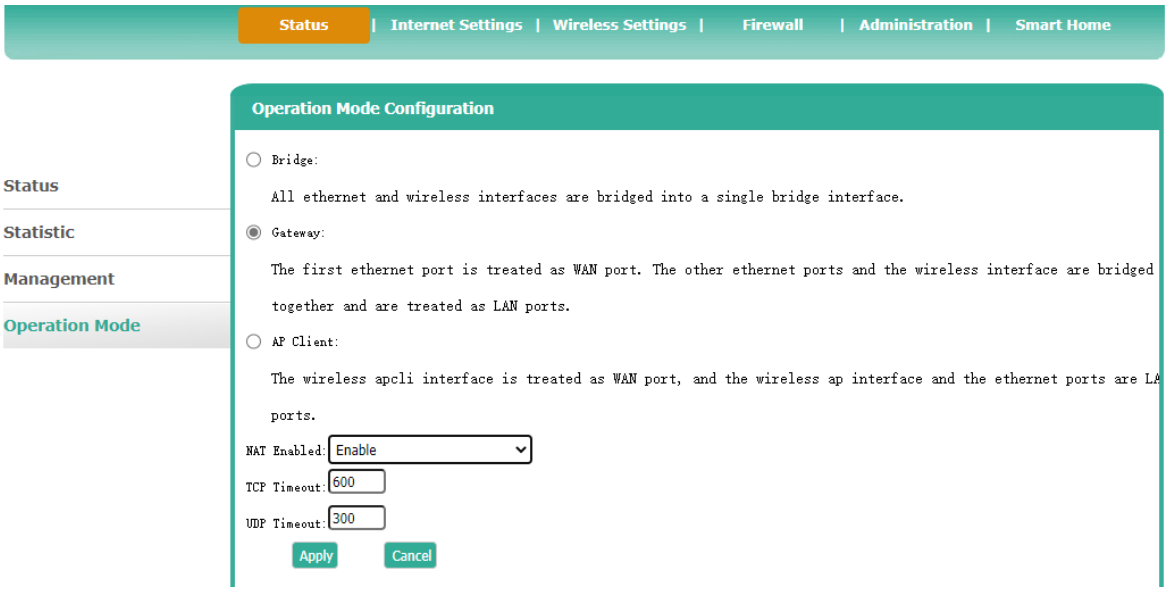
All ethernet and wireless interfaces are bridged into a single bridge interface.

B. Gateway mode

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

C. AP Client

The wireless AP Client interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.



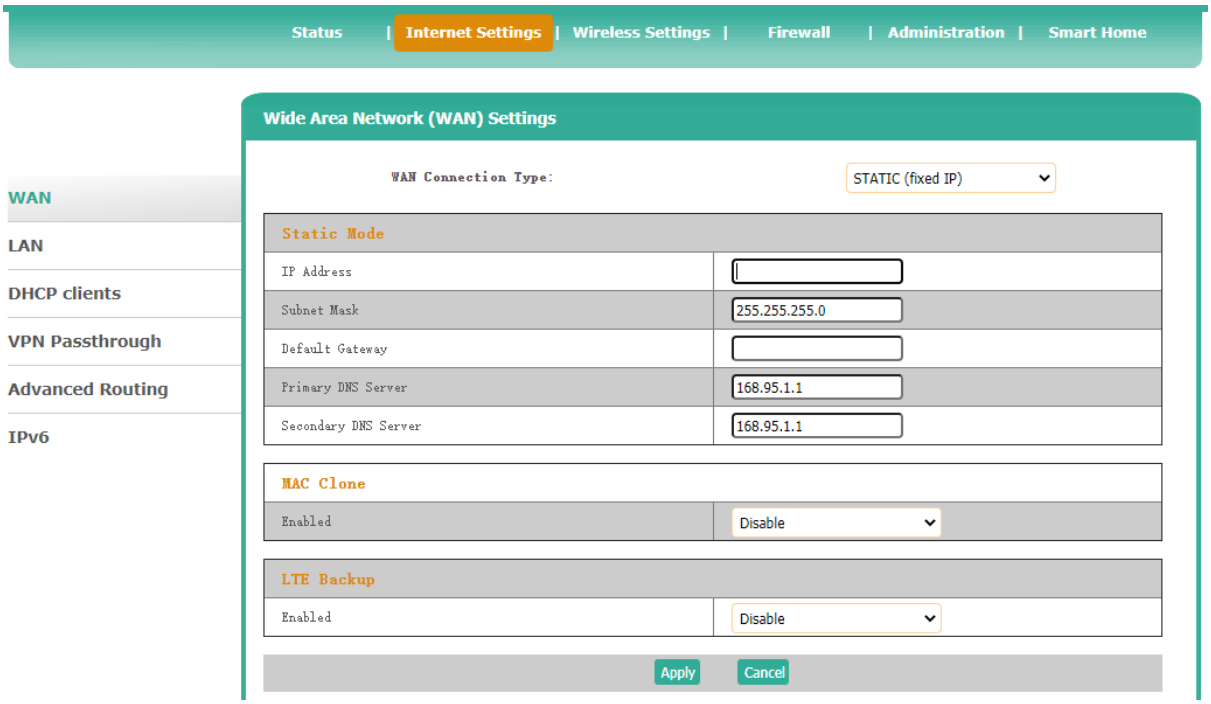
5.4 Internet Setting

5.4.1 WAN

Please select the connection type of WAN according to the environment.

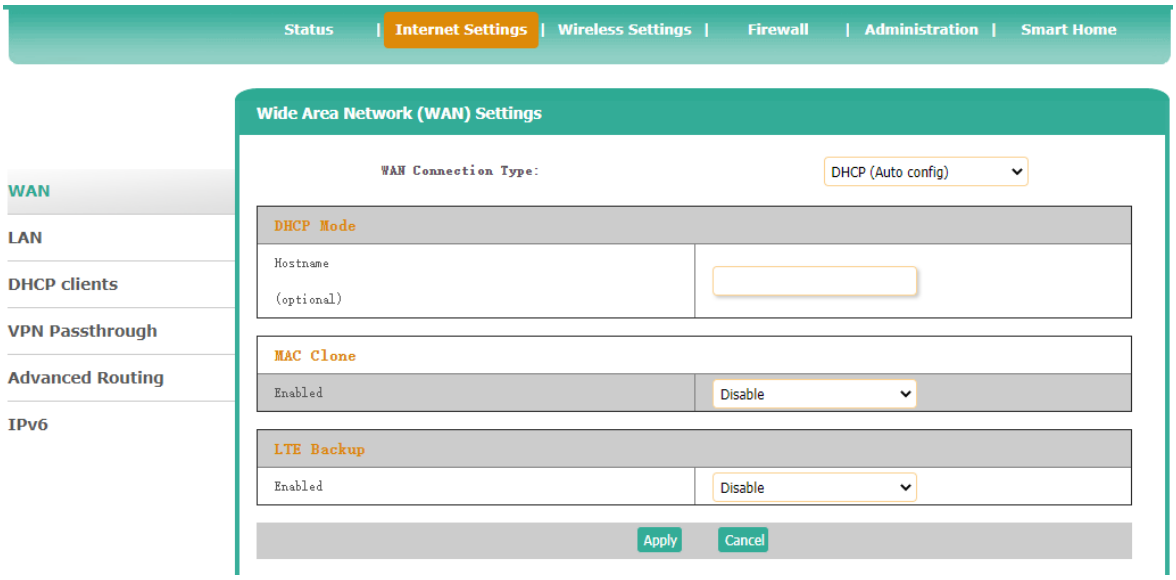
A. Static IP

It needs to enter IP Address, Subnet Mask, Default Gateway, and DNS Server.



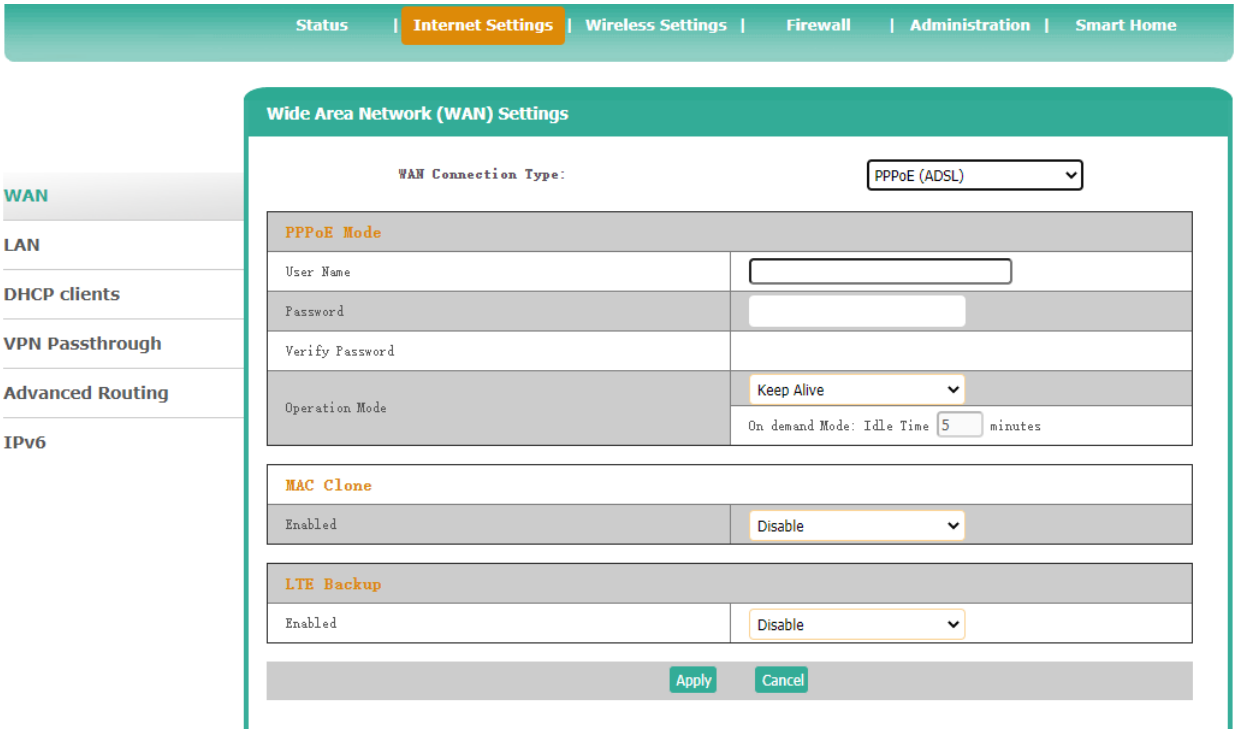
B. DHCP

The network will automatically obtain an IP



C. PPPoE

It need to enter User Name and Password provided by the ISP



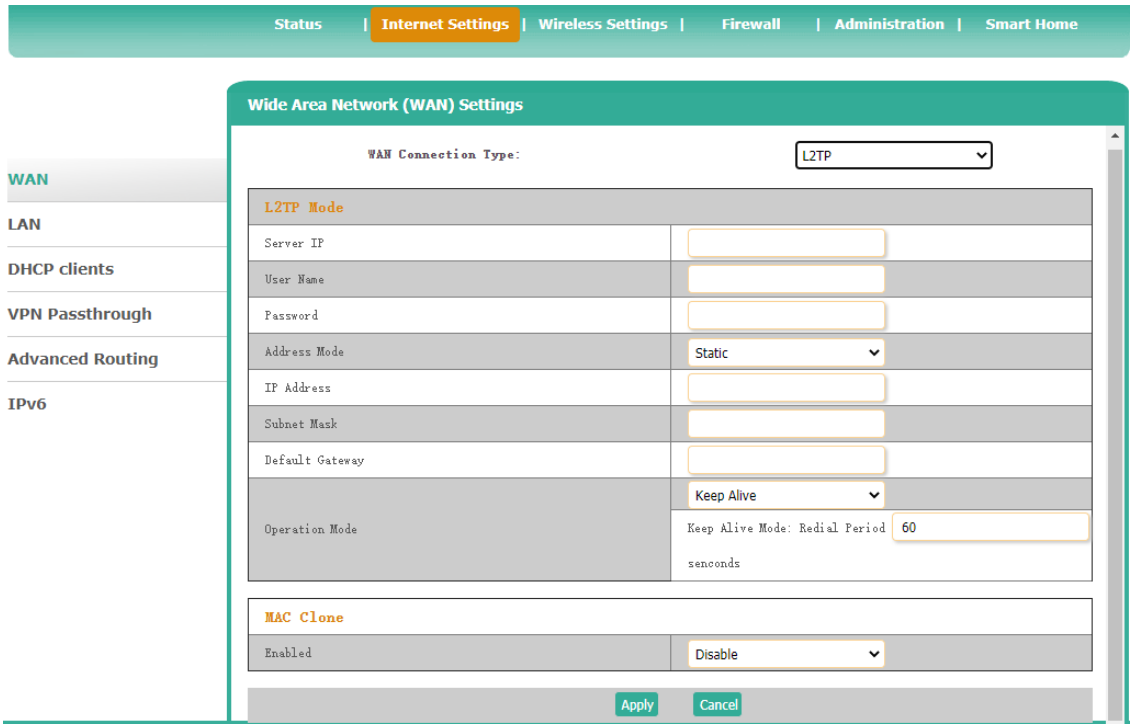
If the setting is the above three network modes-- static IP, dynamic IP, and PPPoE, and enables LTE support, it can automatically switch to 4G dongle to continue connecting to the network when the original mode cannot connect to the network . At present, it will check whether the 4G dongle is plugged in and the switch function is turned on every five minutes. If both are done, it will check the current network for about 10 minutes. During the process, if it connects to the network via the current mode successfully, the switch will be stopped. if it fails to connect to the network, the mode will be switched.

After switching, the gateway will not automatically switch to the original network mode, and the user needs to set the mode by self.

D. L2TP

When the IP Address Mode is Static, the user needs to manually enter the IP Address information.

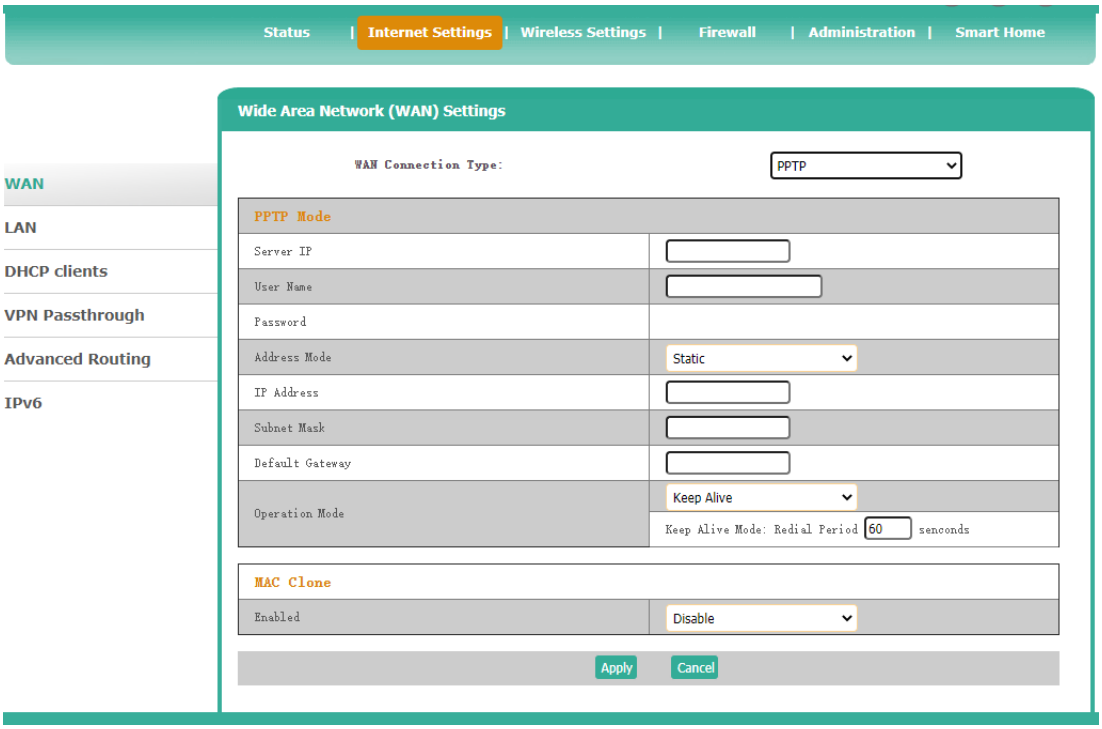
When the IP Address Mode is Dynamic, the IP Address information can be obtained automatically.



E. PPTP

When the IP Address Mode is Static, the user needs to manually enter the IP Address information.

When the IP Address Mode is Dynamic, the IP Address information can be obtained automatically.



F. 3G

It need to match a supported 3G USB Dongle and plug in the USB port of the gateway.

Default APN: internet

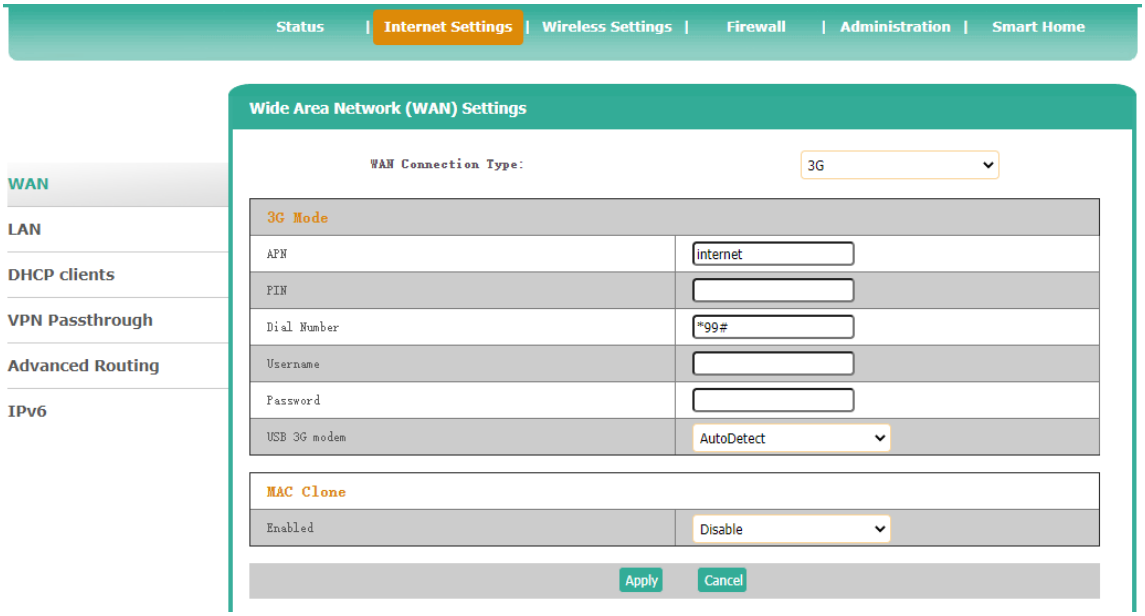
Default Dial Number:*99# (The rest of the setting items can be defaulted.)

Supported 3G USB Dongle: HUAWEI 169/E169u/E1750(StarHub)/E270/E166/EC1260/EC226/EC122/EC189/E181/170/E172/E180/E219/E220/E230/E180/E1552/E160E/Emobile D01HW/Emobile D02HW/E122(2010), Vodafone K4605/K3770/K3772, etc.

Note:

*Please fill in the APN and other information according to the information provided by the telecom.

*3G network card must be genuine. The parallel import and pirated version will be different and will not be used.



G. LTE

It needs to match a supported LTE (4G) USB Dongle and plug in the USB port of the gateway.

Default APN: internet

Default Dial Number:*99# (The rest of the setting items can be defaulted.)

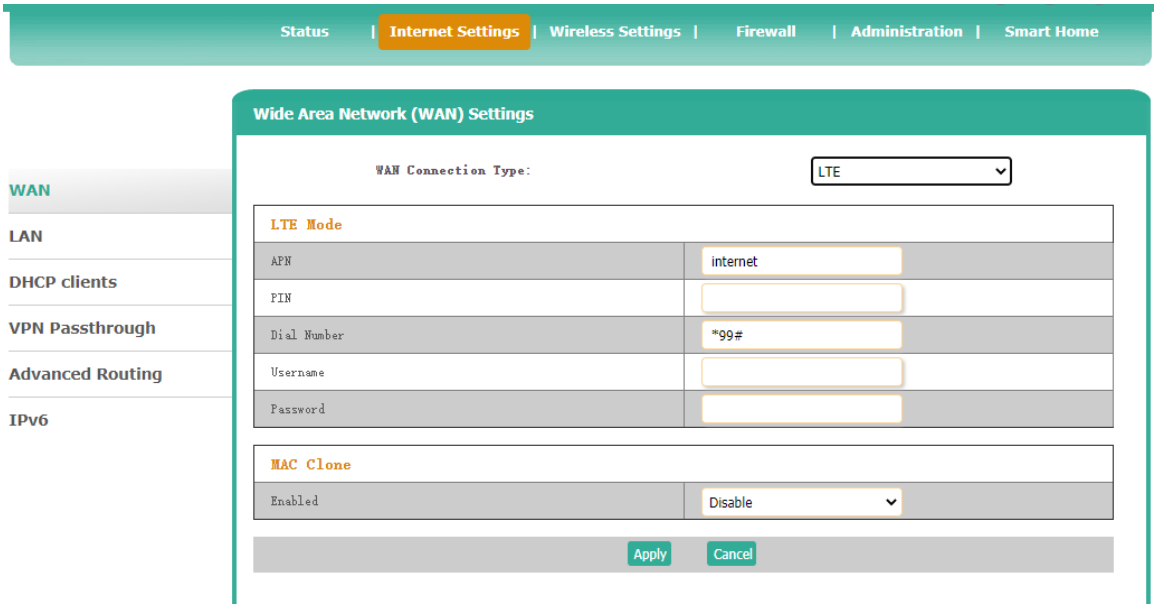
Supported 4G USB Dongle: Huawei EC3372h-607, Huawei EC3372-871, Huawei E3372h-607

Alcatel Link Key 4G LTE IK 40

Note:

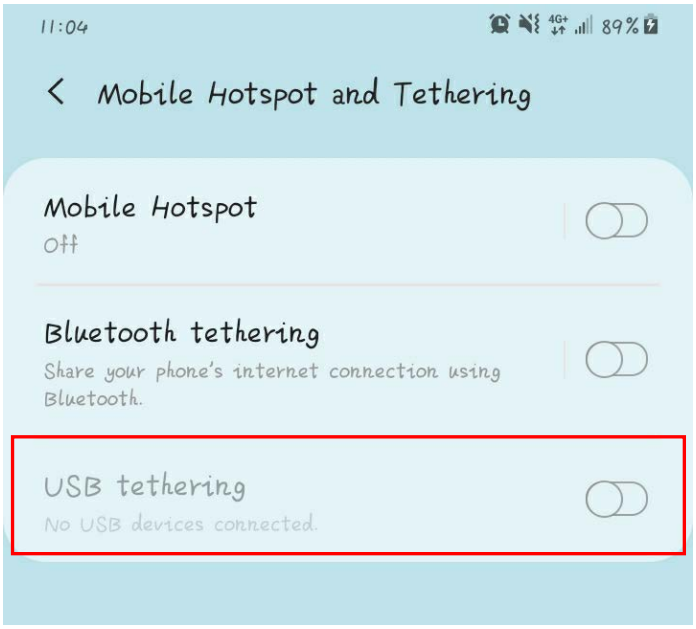
*Please fill in the APN and other information according to the information provided by the telecom.

*4G network card must be genuine. The parallel import and pirated version will be different and will not be used.



In addition to using the 3G/4G USB Dongle to surf the Internet, the user can also connect to the USB port of the gateway through an Android phone to surf the Internet.

After plugging it in, the user must first turn on "USB Tethering" on the phone. When the phone is used as an LTE dongle, it can also provide the gateway with the Internet.

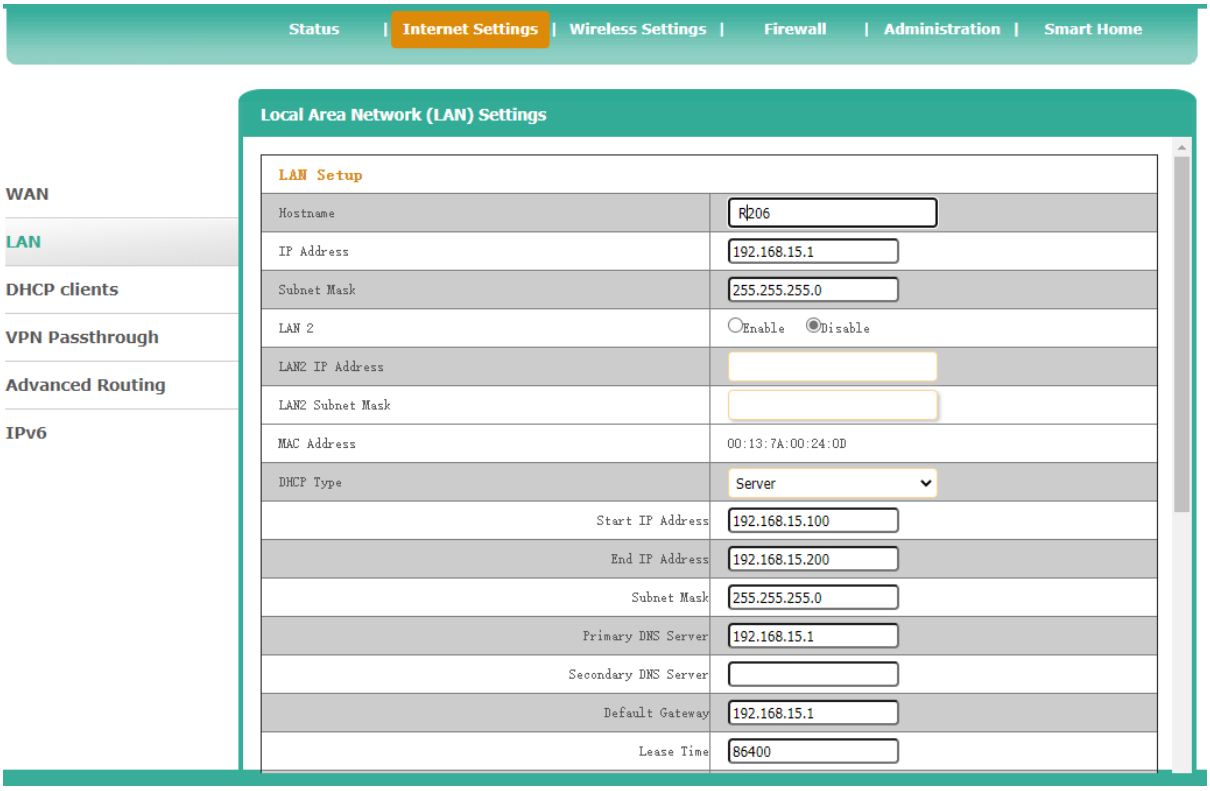


Note:

*Some Android phones may not support.

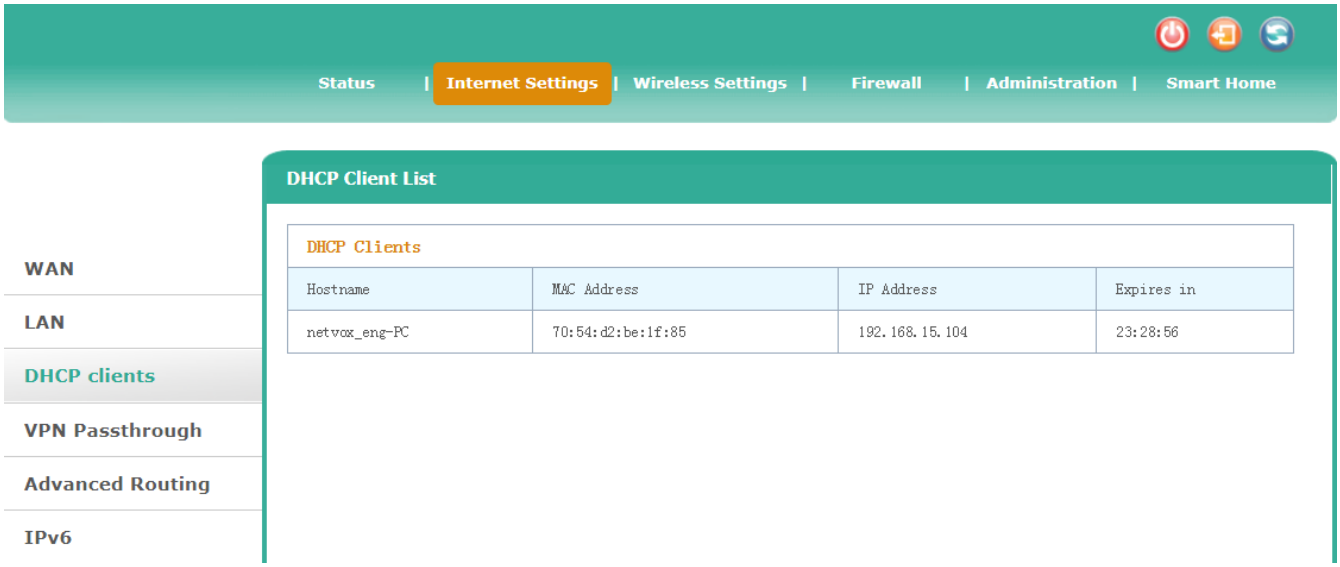
5.4.2 LAN

The information of LAN can be set, such as changing IP and IP range, enabling/disabling UPNP, etc.



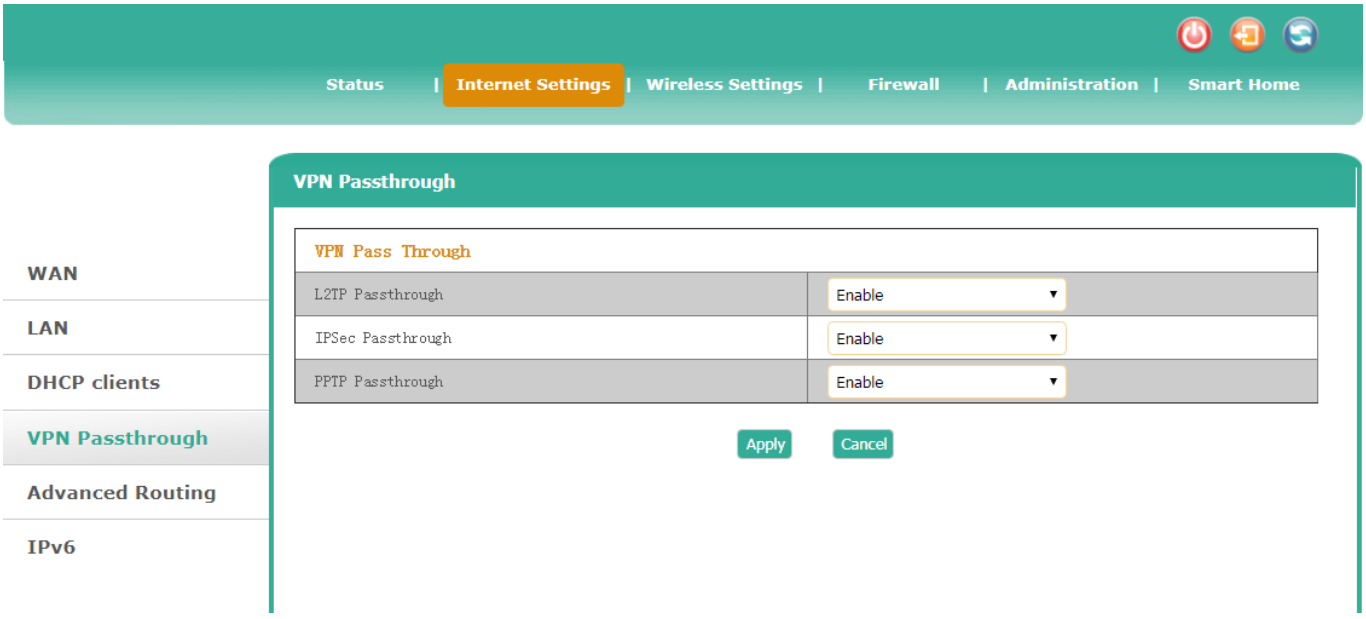
5.4.3 DHCP Clients

Check the information of the devices connected with the gateway. Users can get the assigned IP address based on the network name or MAC address.



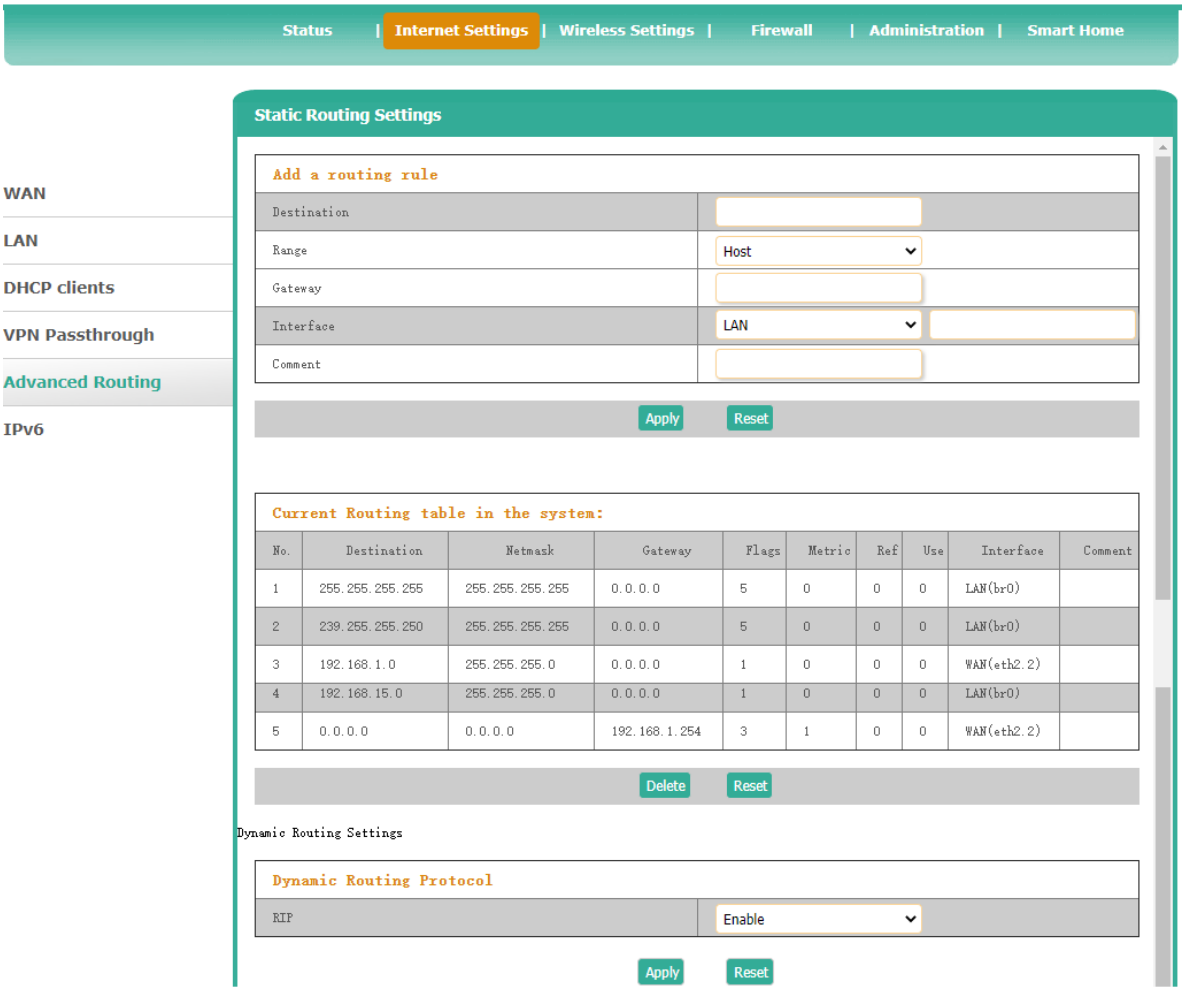
5.4.4 VPN Passthrough

Users can enable/disable the VPN passthrough here, including: L2TP, IPSec, and PPTP passthrough.



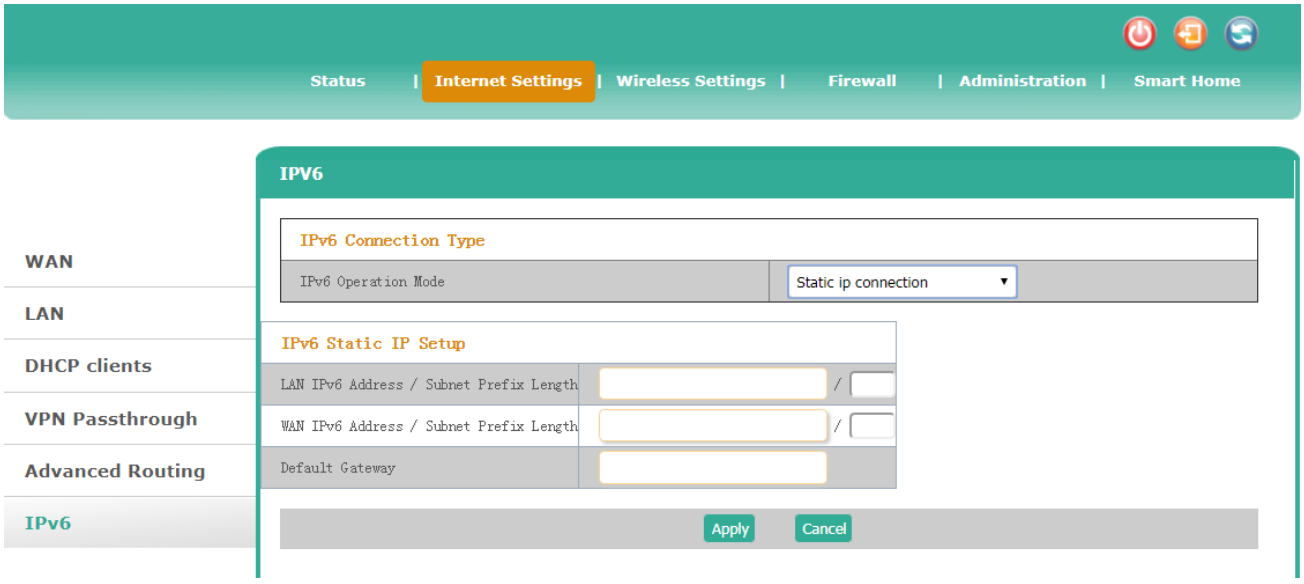
5.4.5 Advanced Routing

Users can add/remove static routing rules or enable/disable dynamic routing rules.



5.4.6 IPv6

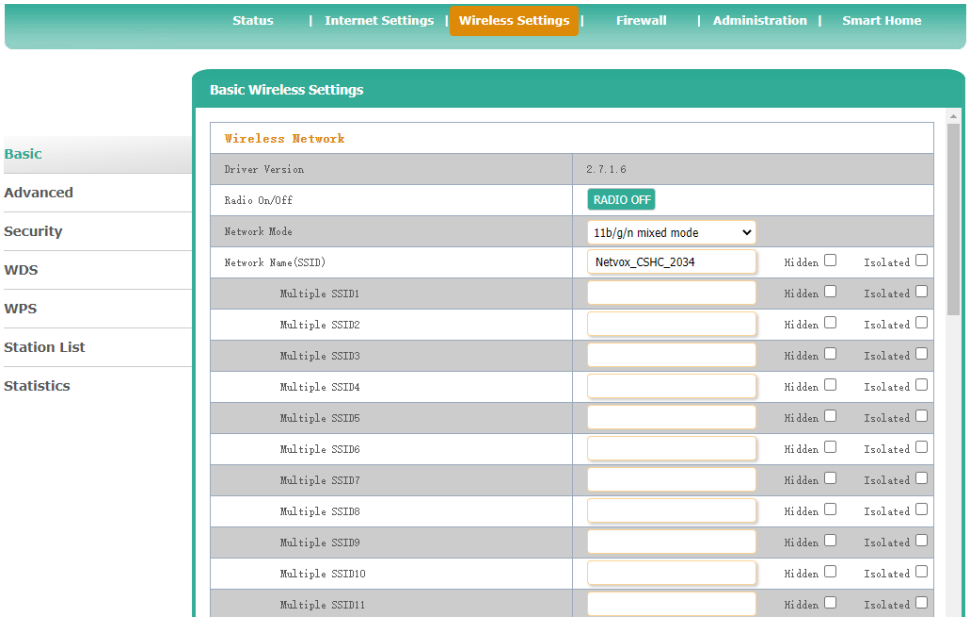
Enable IPv6 setting



5.5 Wireless Setting

5.5.1 Basic

Basic wireless network setting, such as changing wireless SSID, adding wireless SSID, and enabling/disabling Wi-Fi signal (Radio On/Off).

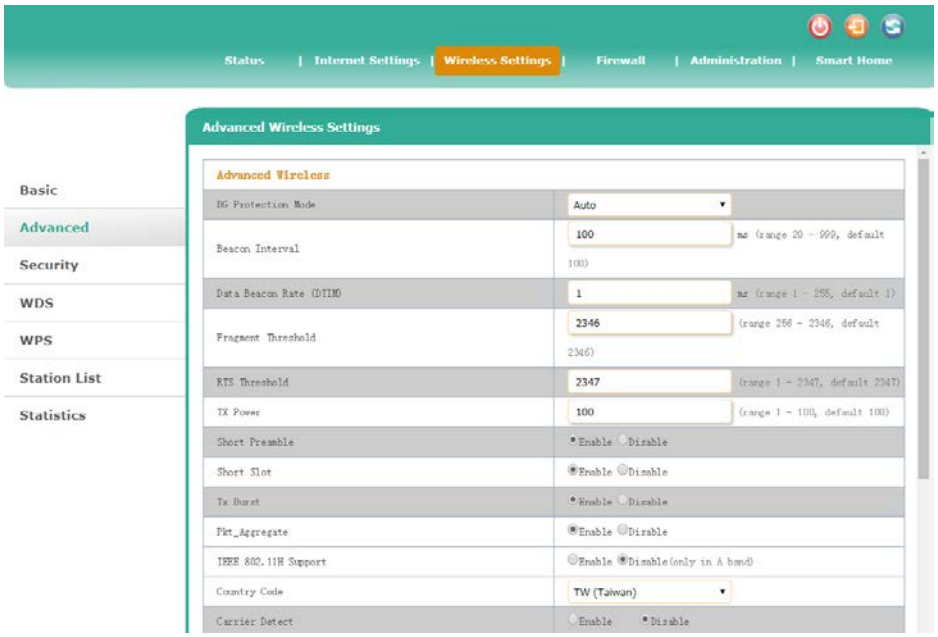


Note:

*The Wi-Fi function of the gateway is turned off. The user needs to use the wired connection to enter the setting page of the gateway and reopen it before connecting to Wi-Fi.

5.5.2 Advanced

Users can set Beacon Interval, control transmission rate and basic data transmission rate, etc.

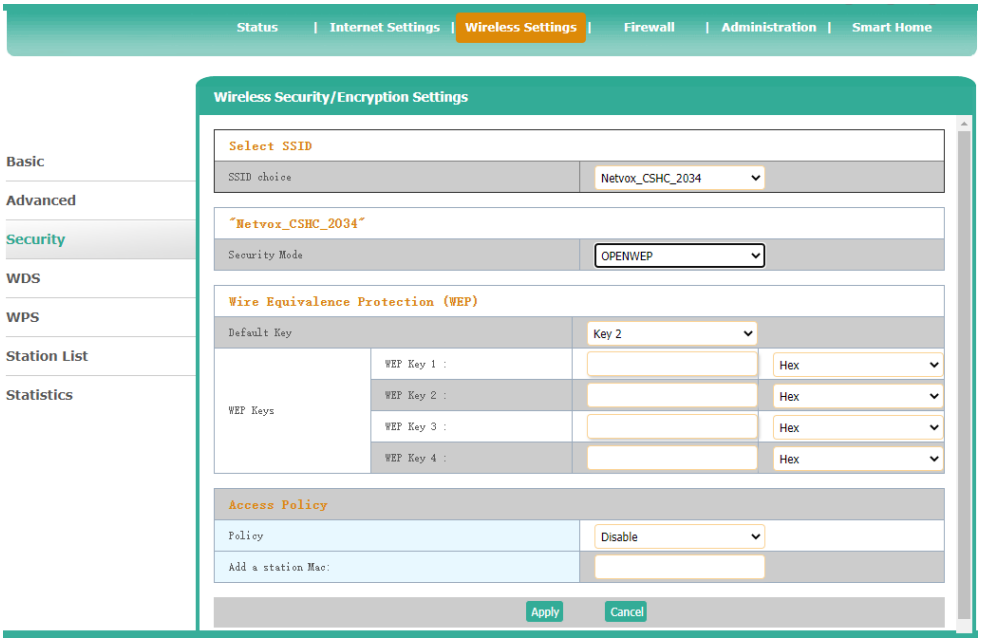


5.5.3 Security

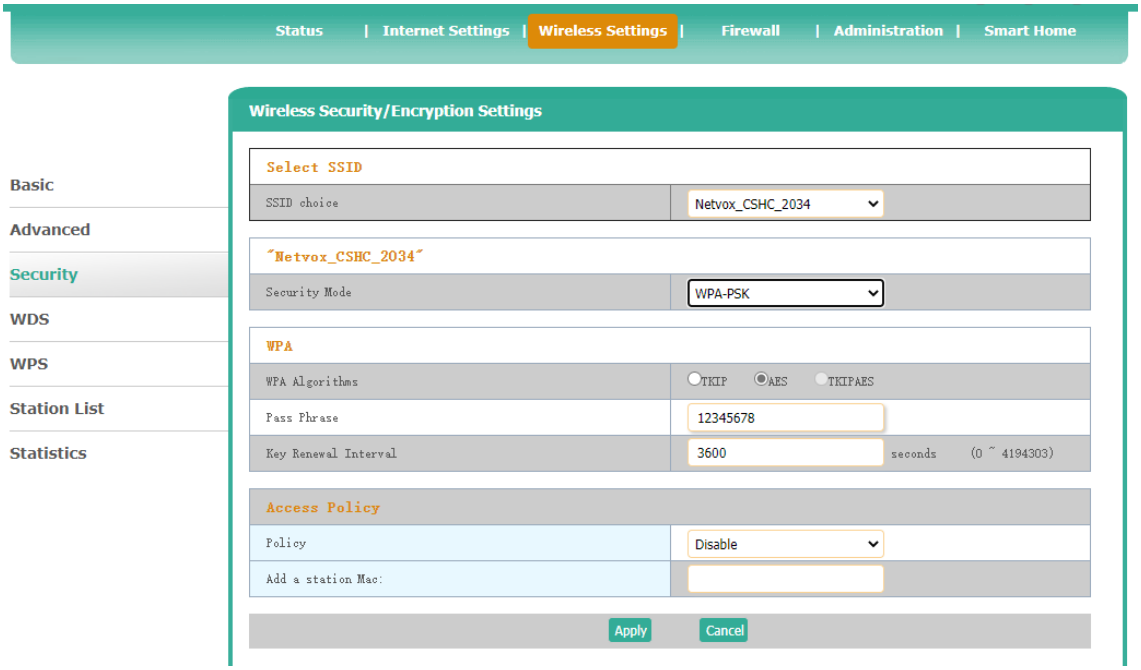
Set the wireless SSID encryption method

A. Security Mode: OPENWEP

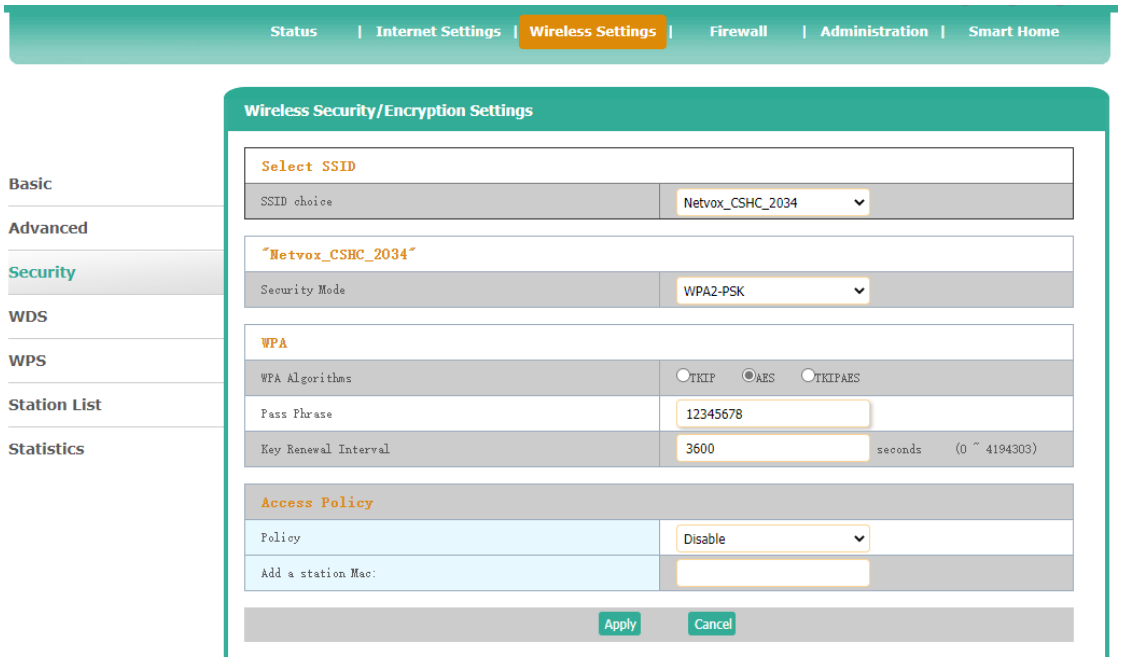
Network Mode does not support 11n



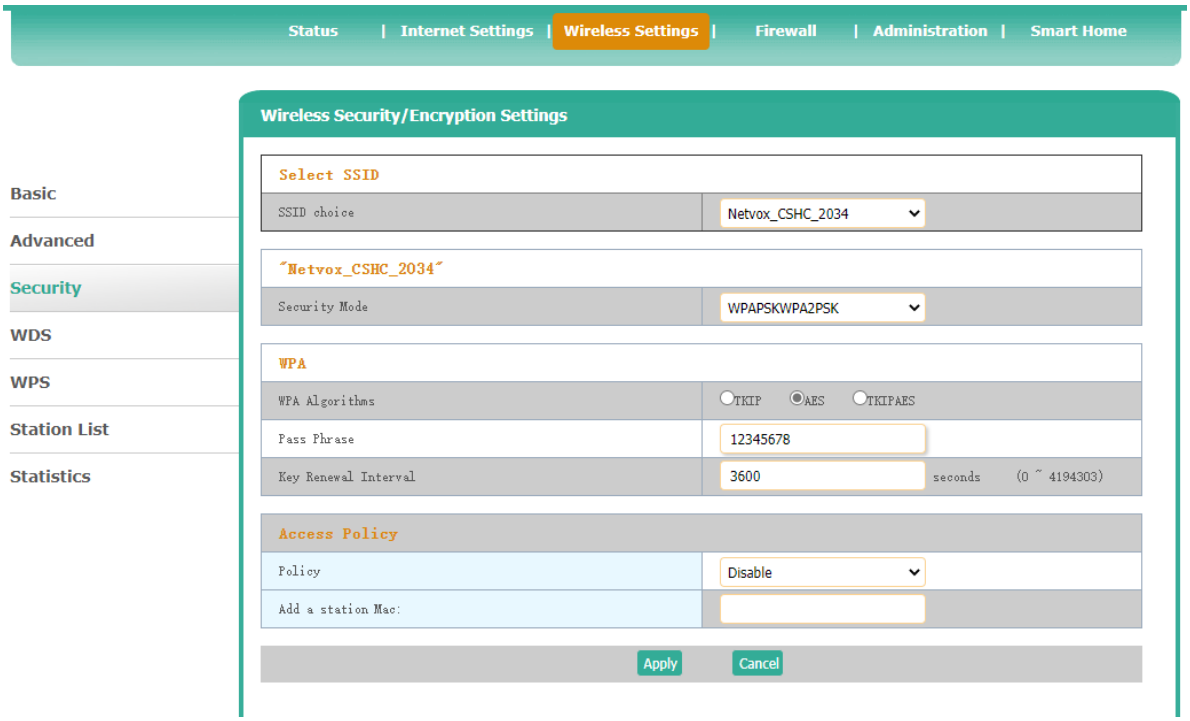
B. Security Mode: WPA-PSK



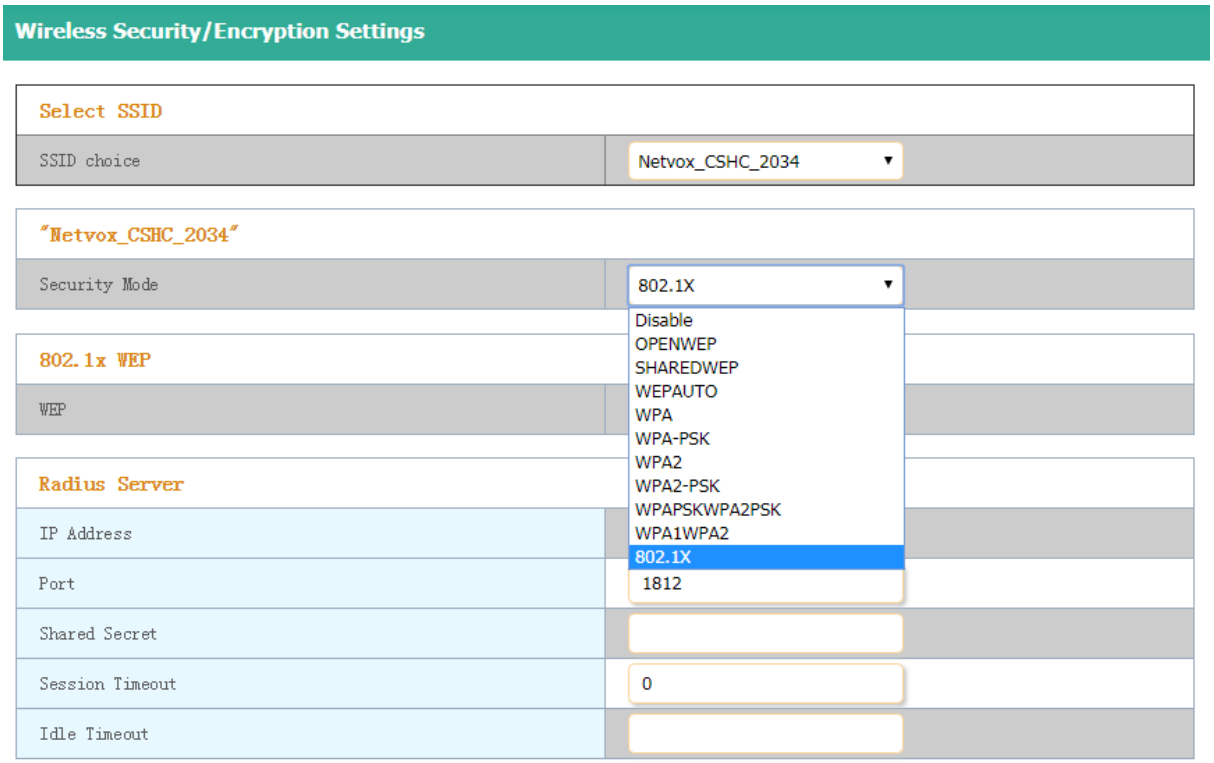
C. Security Mode: WPA2-PSK (Recommend)



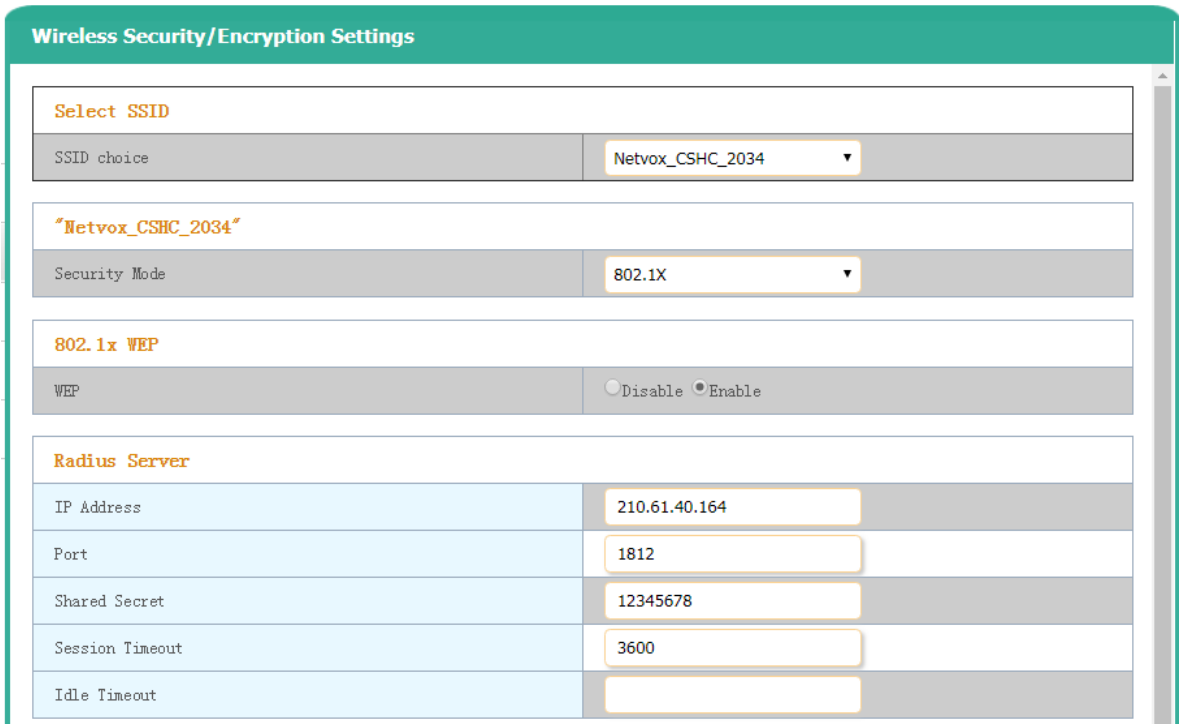
D. Security Mode: WPAPSKWPA2PSK



If WPS is disabled, the security mode will add the option about Radius Server: WPA, WPA2, WPA1, WPA2, and 802.1X



The method of setting Radius Server is as follows



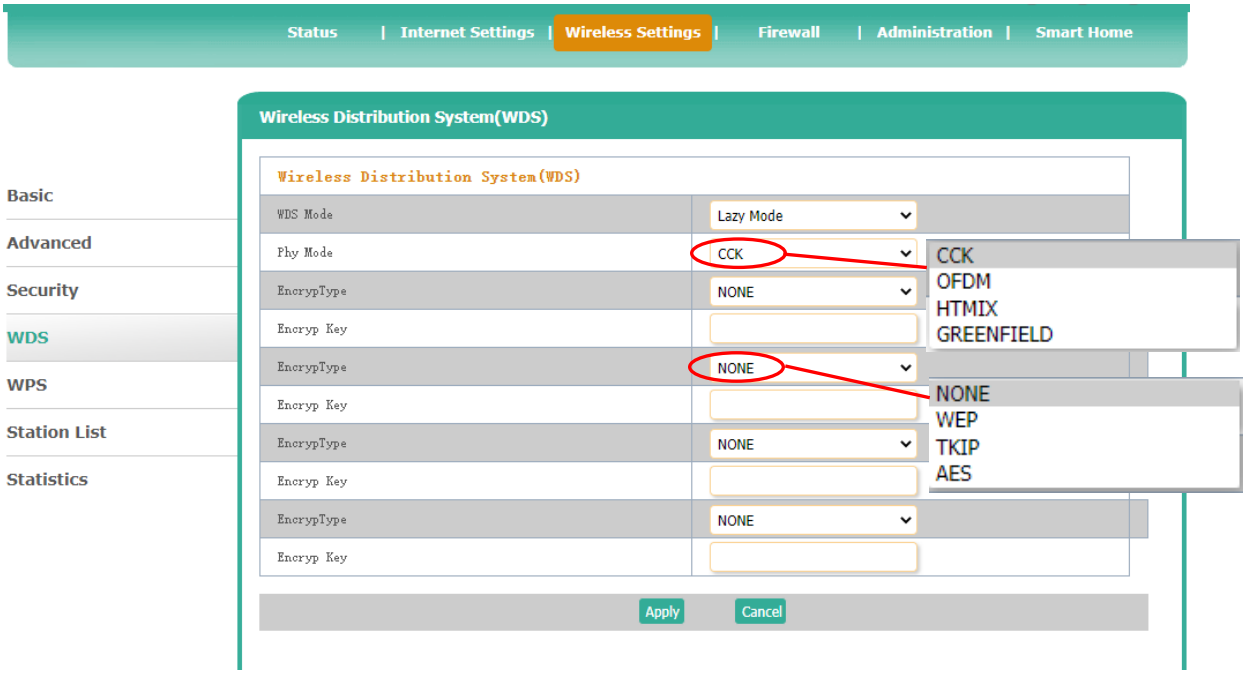
5.5.4 WDS

Enable/Disable WDS

A. Lazy Mode

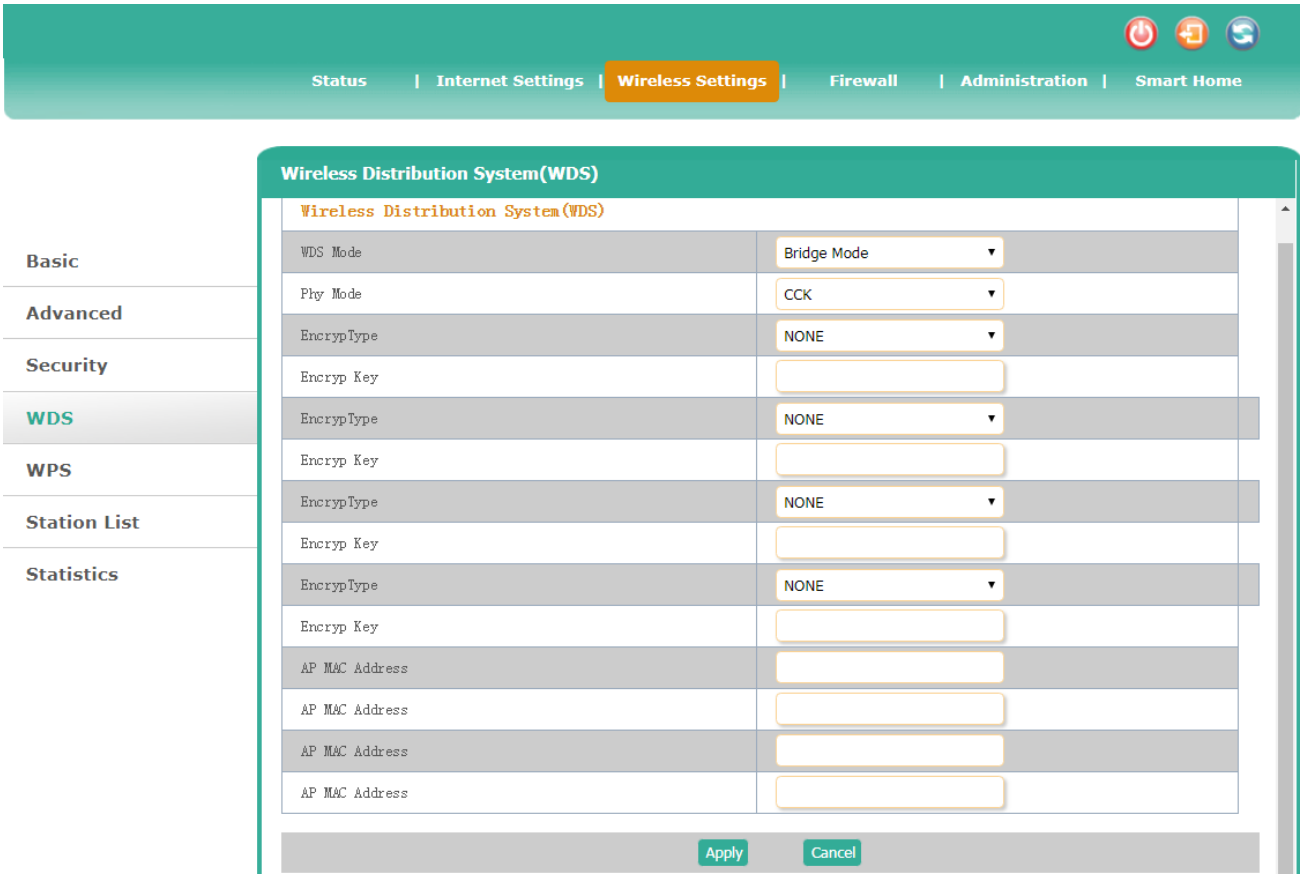
Physical Mode support: CCK、OFDM、HTMIX、GREENFIELD

Encryption Key support: WEP、TKIP、AES



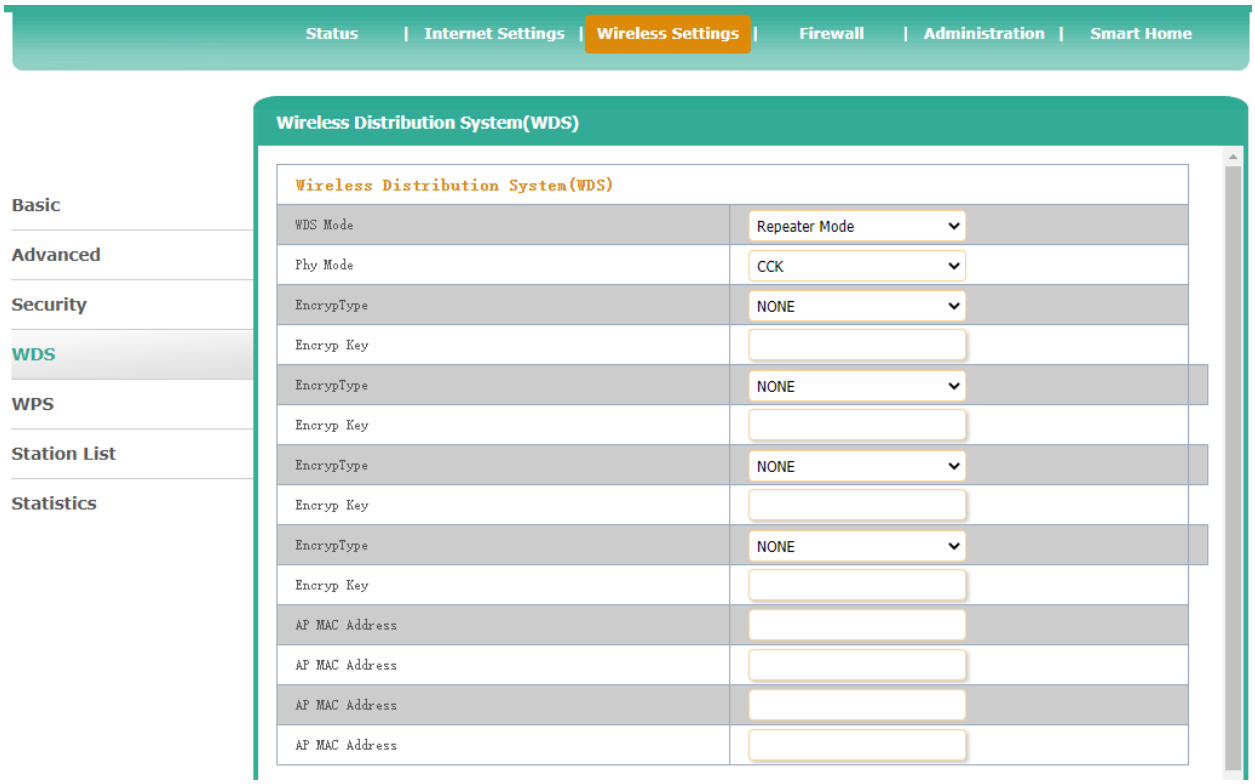
B. Bridge Mode

Users need to manually enter AP MAC Address.



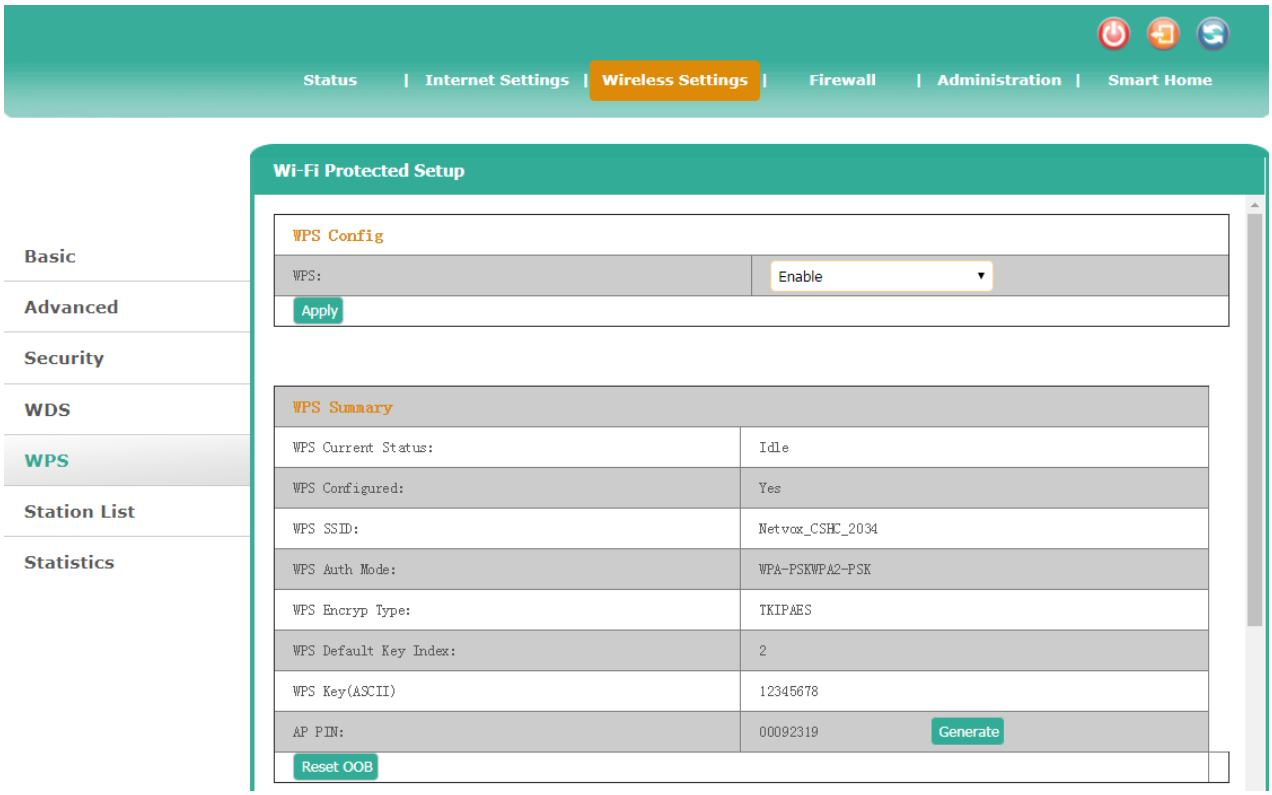
C. Repeater Mode

Users need to manually enter AP MAC Address.



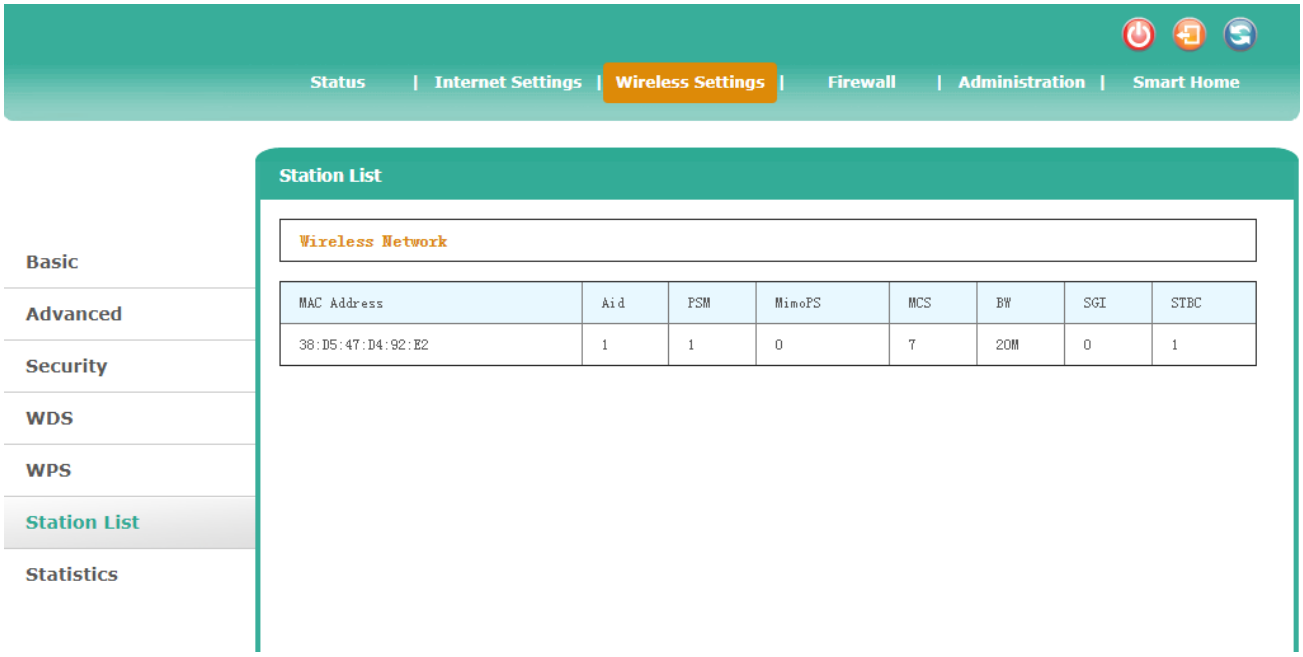
5.5.5 WPS

You could setup security easily by choosing PIN method to do Wi-Fi Protected Setup.



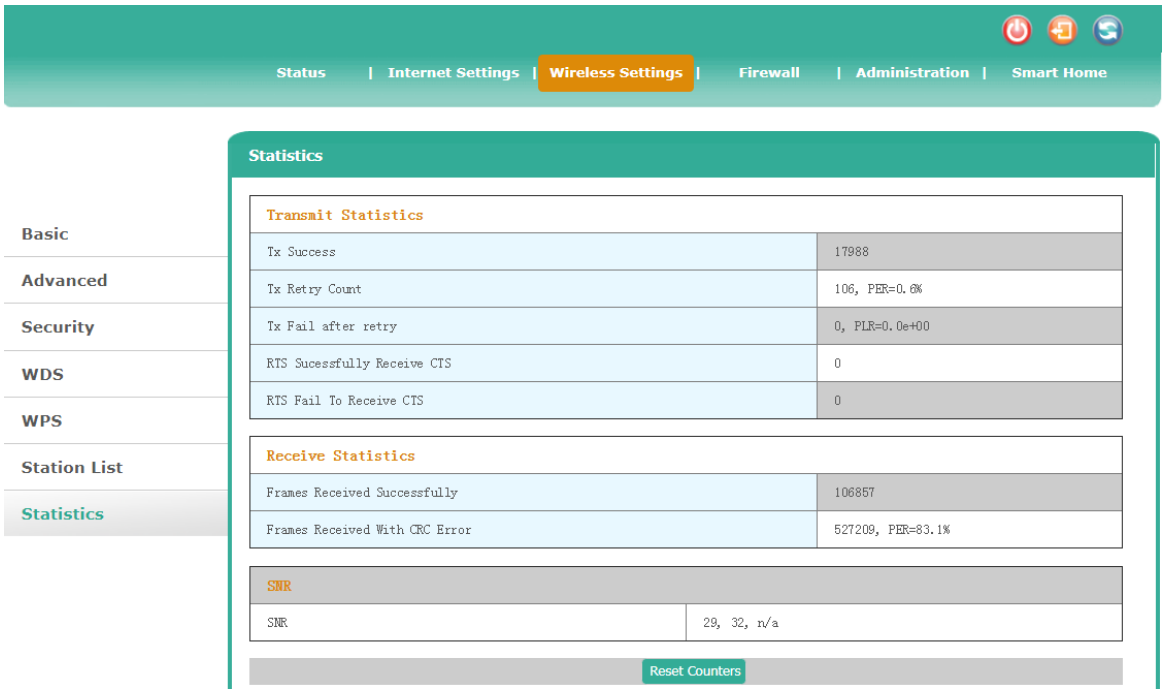
5.5.6 Station List

You could monitor stations which associated to this AP here.



5.5.7 Statistics

Statistics and Information Collection (Transmit Statistics & Receive Statistics)

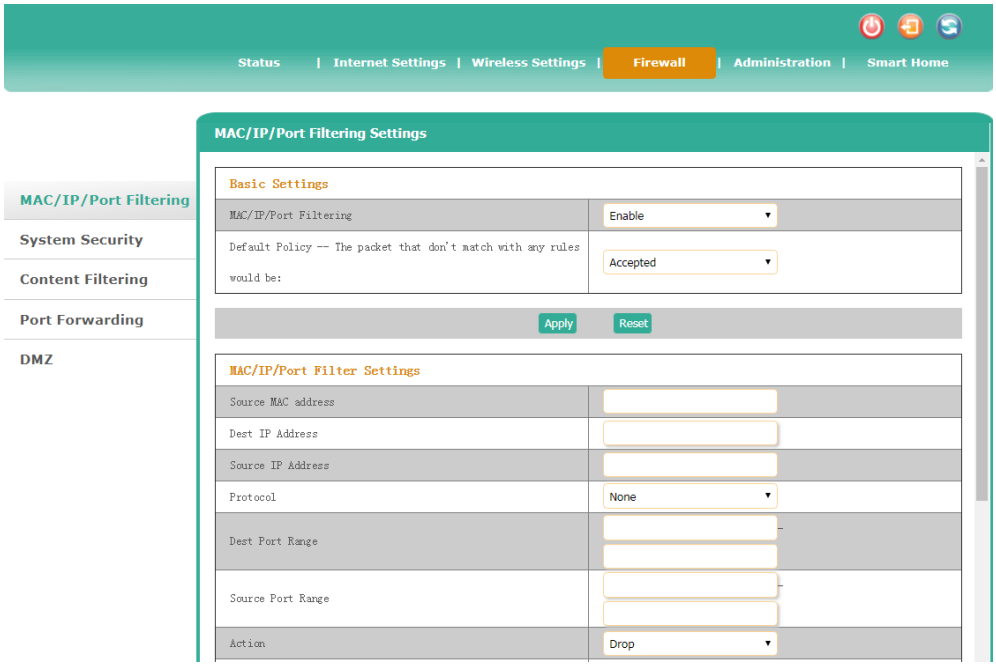


5.6 Firewall

Users can set up a firewall to protect against malicious attacks from the Internet.

5.6.1 MAC/IP/Port Filtering

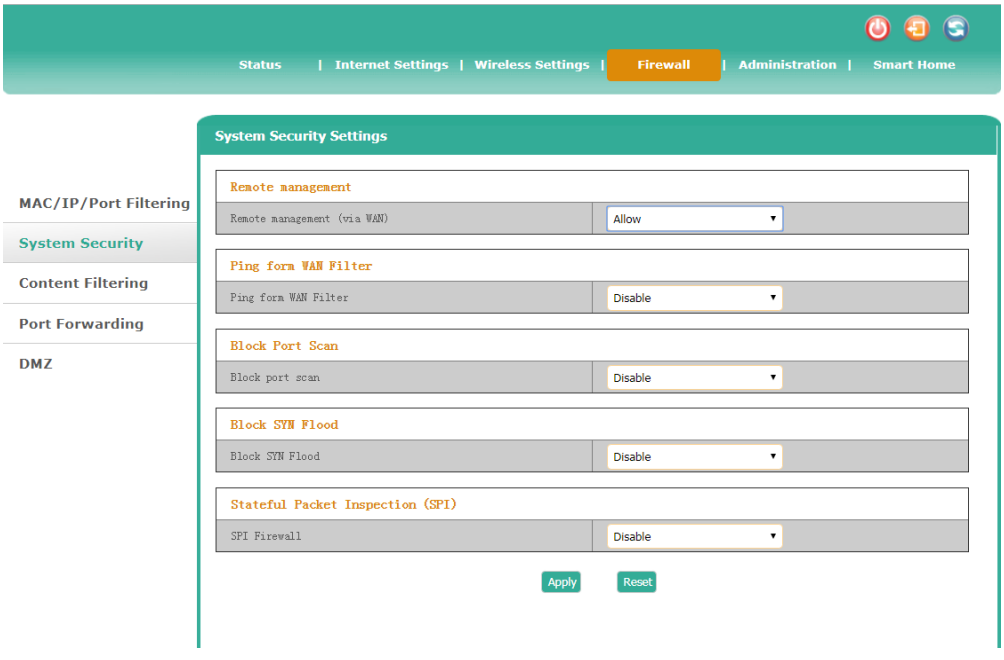
MAC/IP/Port Filtering is disabled by default. If users need to access the external IP, it need to enable the function of MAC/IP/Port Filtering.



5.6.2 System Security

The router or wireless access point can be protected by setting the system firewall.

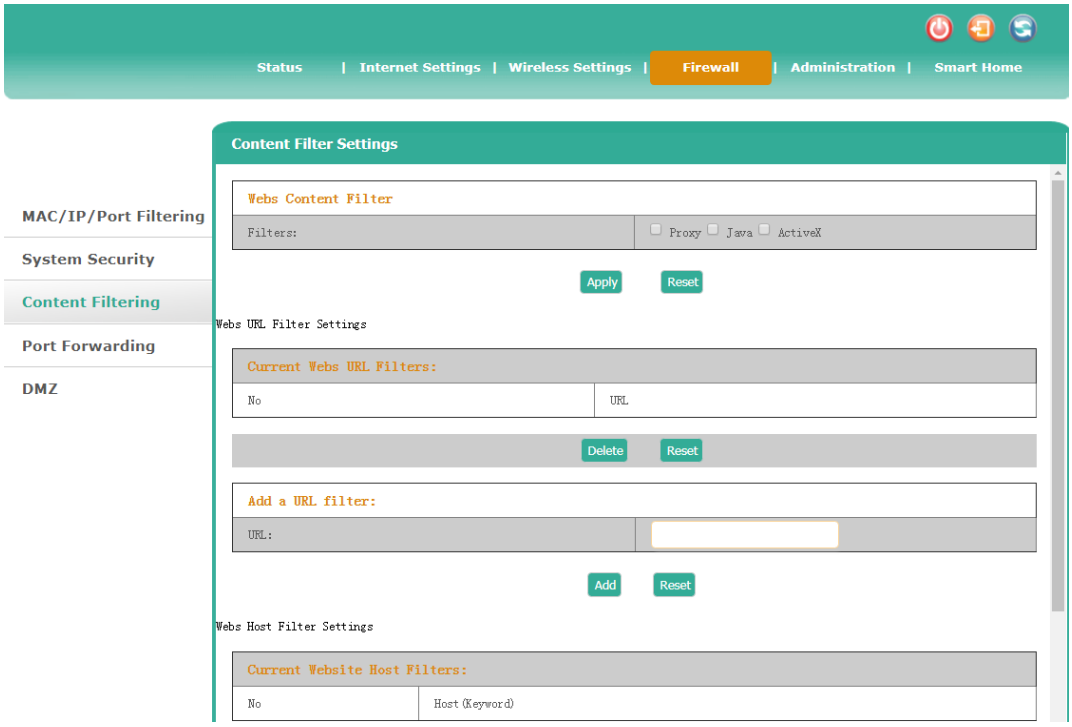
If users want to support the login operation of WAN, users need to set Remote management to the "Allow" state to support remote login. Other items are set according to users' different needs.



5.6.3 Content Filtering

Users can set Content Filter to limit inappropriate web pages.

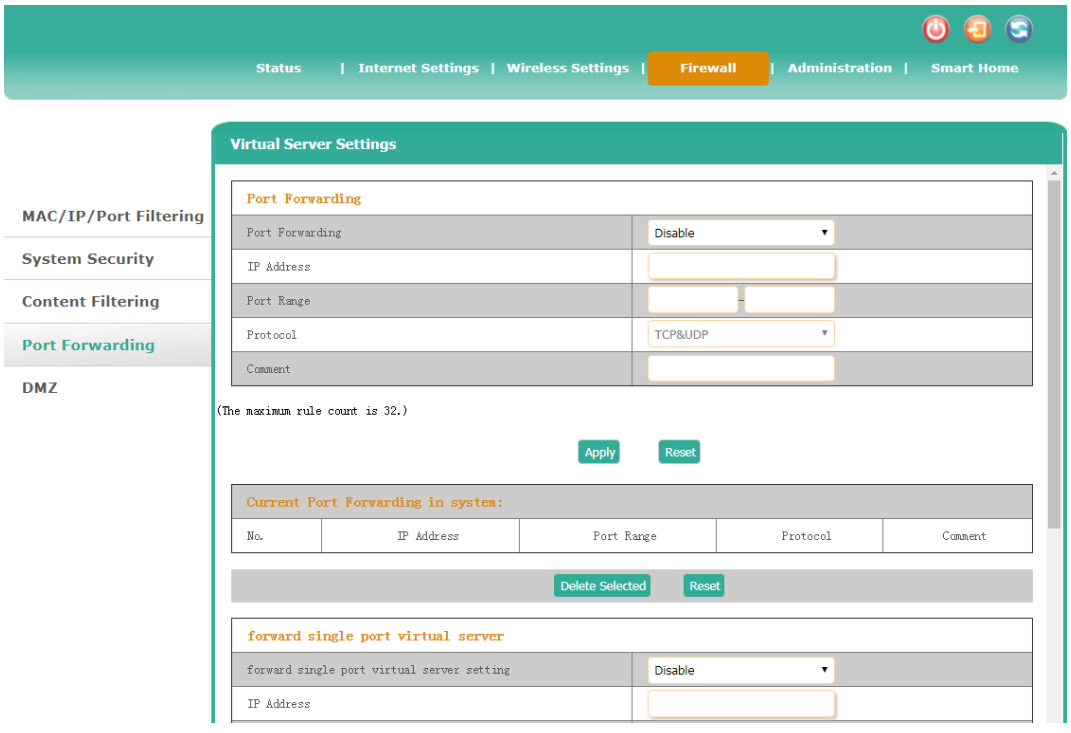
Enter the URL to be filtered and click Add to add a new rule of URL filtering.



5.6.4 Port Forwarding

Choose whether to enable Virtual Server Settings

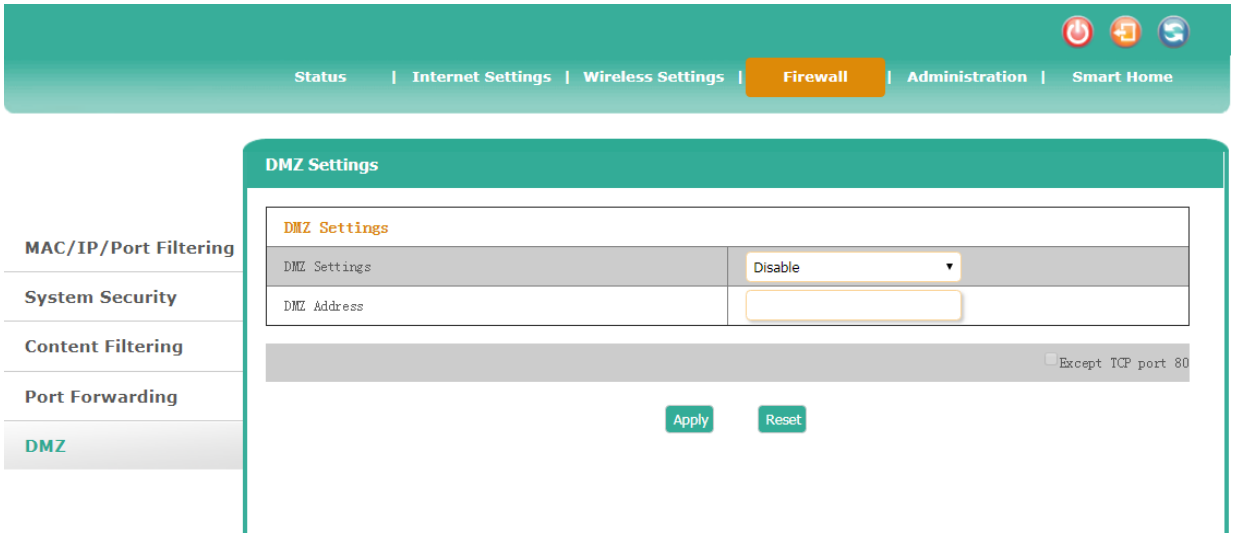
When users enable the virtual server, users should enter the IP Address, Port Range, and Comment to create a virtual server to provide network services



5.6.5 DMZ

Whether to enable DMZ Settings

Establish a DMZ to distinguish the internal network from the Internet. Users need to set the DMZ IP address when enabling it.



5.7 Administration

5.7.1 Management

Modify gateway login Account and Password, NTP, Green AP, DDNS

In NTP Settings, users can check the current time and time zone of the gateway, network server, etc. When the current time of the gateway is different from the local time, users can click [Sync with host] to synchronize the time of the computer.

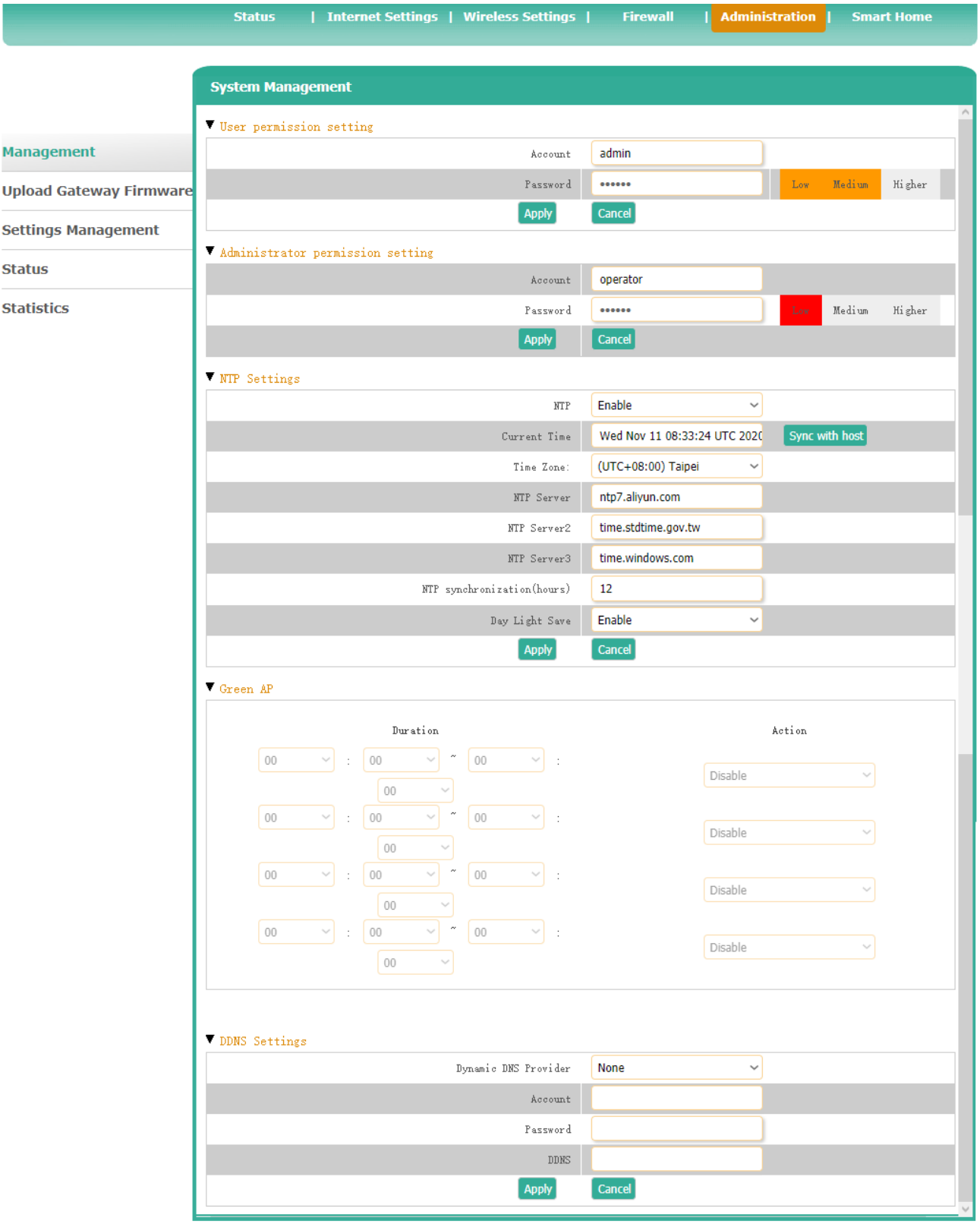
The NTP server is activated by default to ensure that the gateway synchronizes the time of the Internet every 12 hours. The time zone must be consistent with the local time.

There are three default network time servers:

NTP Server1：ntp7.aliyun.com

NTP Server2：time.stdtime.gov.tw

NTP Server3：time.windows.com



Note:

*Administrator permission setting will only be displayed after logging in to the operator account

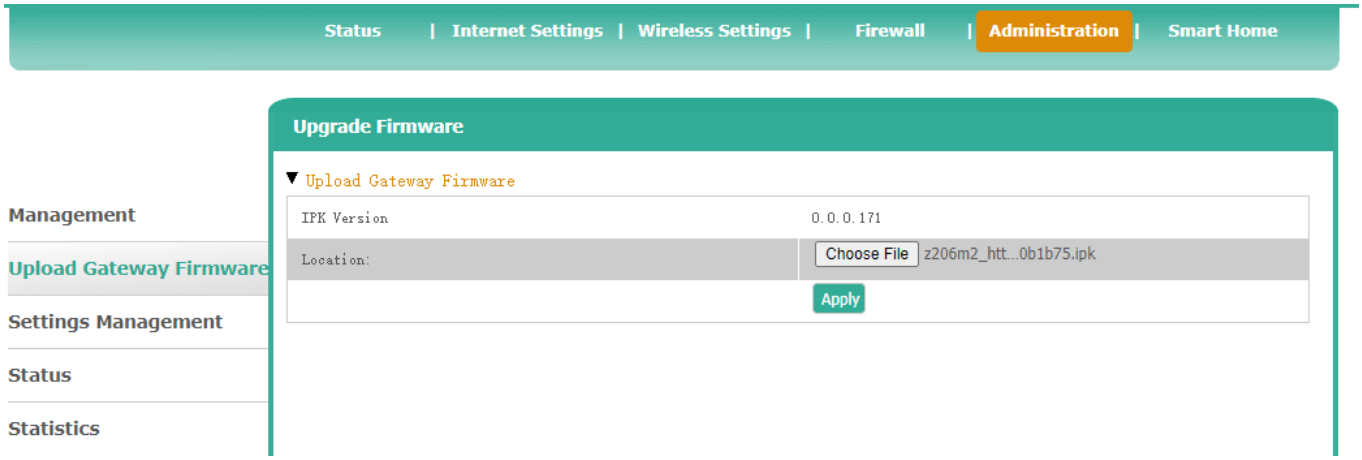
*Password Restriction: 1. It cannot be 123456.

2. The length must be greater than or equal to 6 digits.

3. It cannot be the same as the account. (after the version 0.0.0.163)

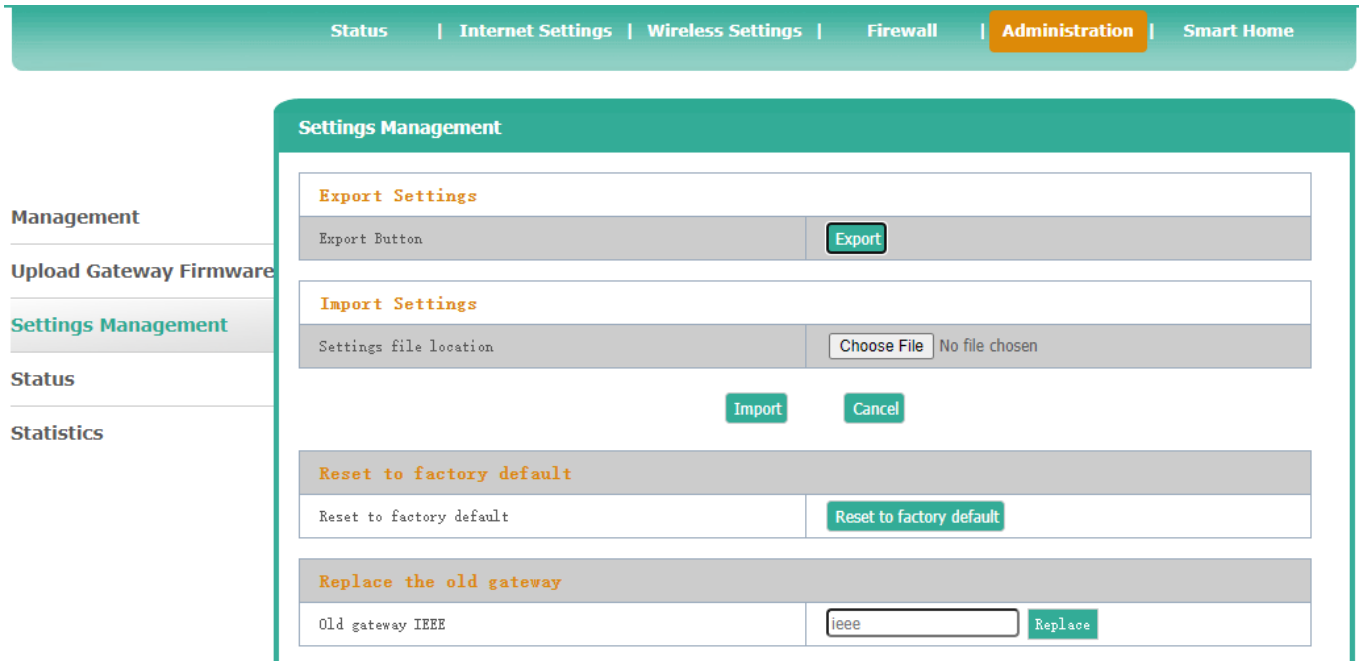
5.7.2 Upgrade Gateway Firmware

Upgrade the firmware of gateway



5.7.3 Settings Management

A. Export/import gateway system configuration file (.dat) / Restore to factory default



B. Replace the Gateway

When the LoRa gateway is damaged or fails to operate normally, users can purchase a new LoRa gateway to replace the old one and change the new IEEE to the old IEEE.

(1) Only support IEEE address replacement of LoRa gateway

(2) The IPK version must be 0.0.0.143 and above.

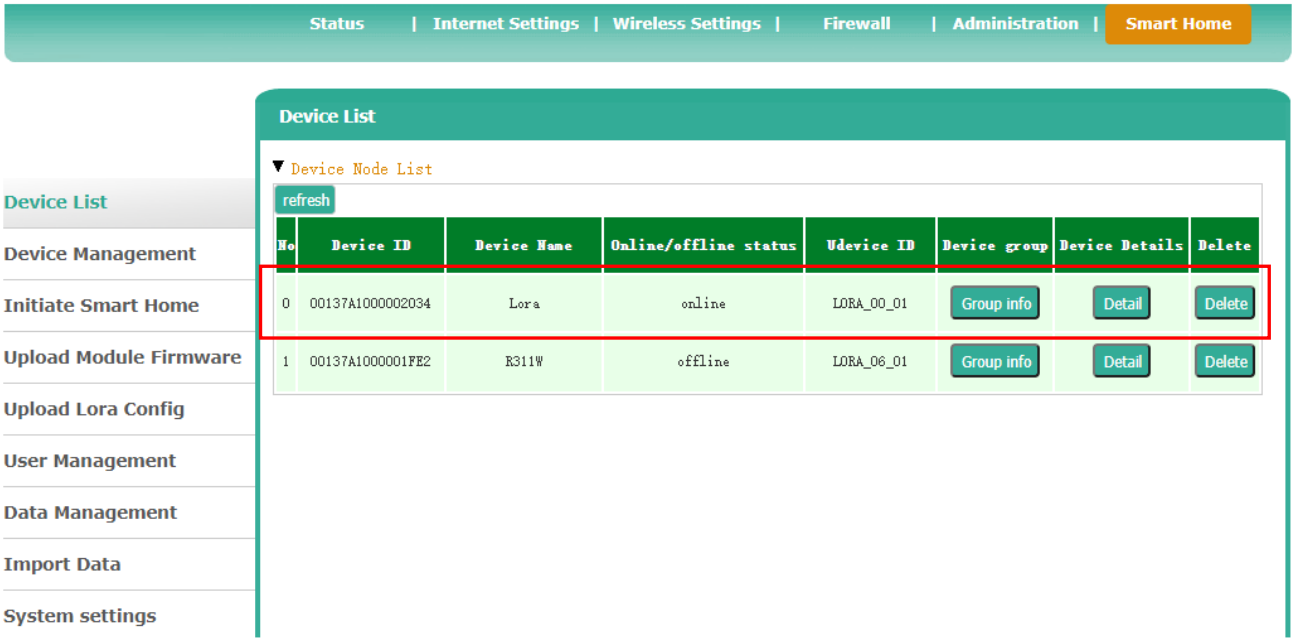
(3) After the replacement is successfully completed, the gateway is connected to the cloud and the backup data can be restored from the cloud. LoRa device needs to be powered on again to restore it.

1. Open the setting page of the new gateway, as the figure below

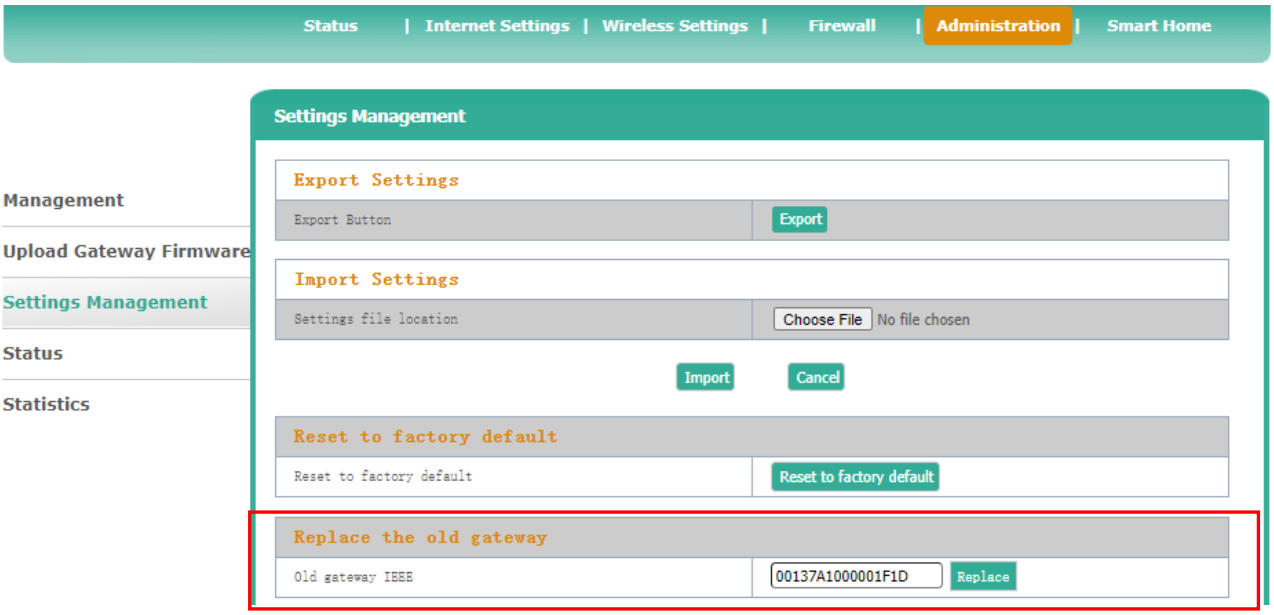
The IEEE of new gateway: 00137A1000002034

The IEEE of old gateway: 00137A1000001F1D

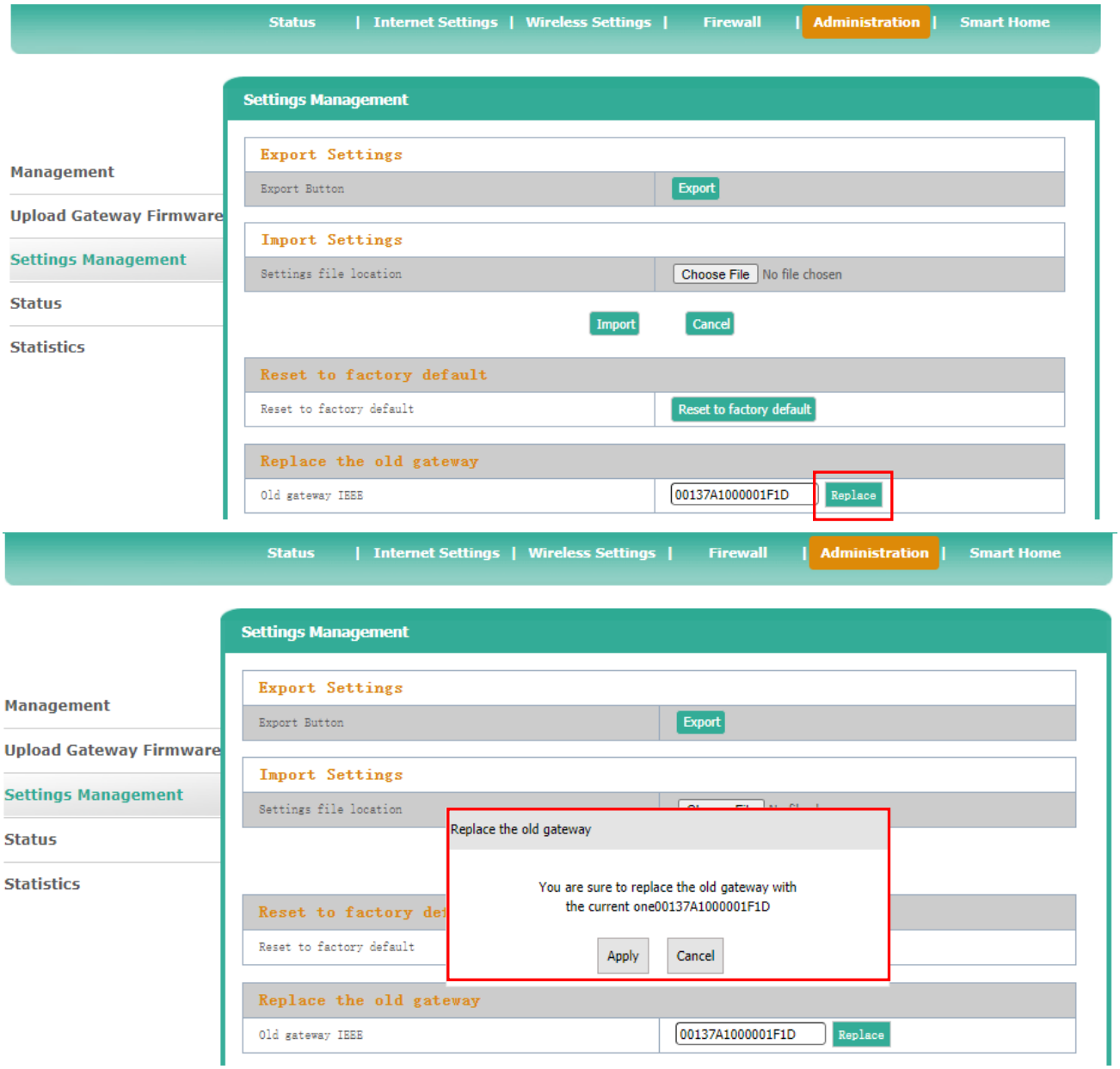
Replace the IEEE of new gateway with the IEEE of old gateway.



2. Click [Administration] > [Settings Management], and fill in the IEEE address of the old gateway in the input box, “Replace the old gateway”.

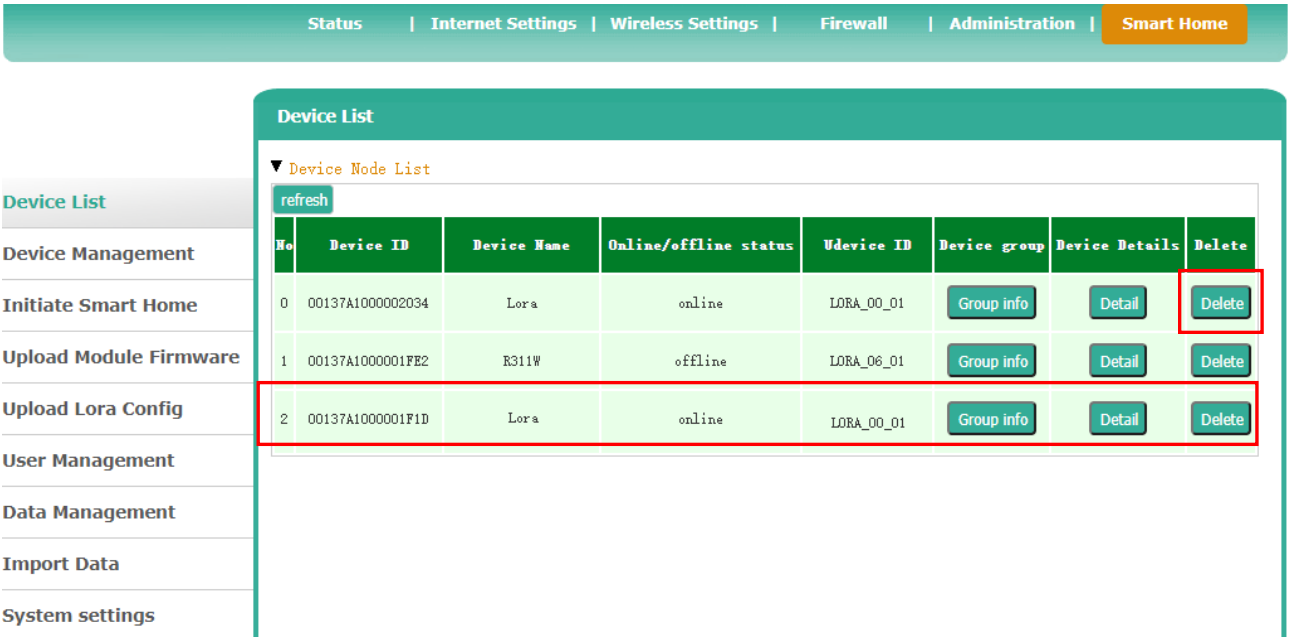


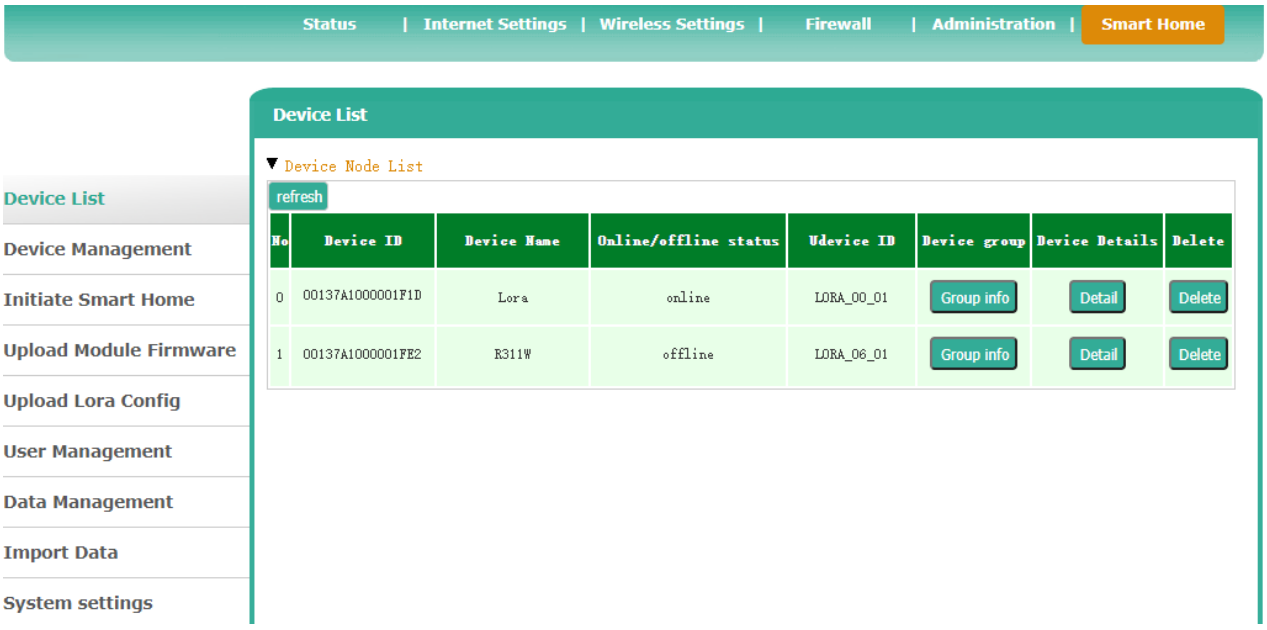
3. Click "Replace" and then click "Apply", and it can replace the IEEE address successfully



4. After the replacement is successful, click [Smart Home] > [Device List], and the IEEE of old gateway (00137A1000001F1D) will be displayed.

   Then, you can delete the IEEE of the new gateway (00137A1000002034).

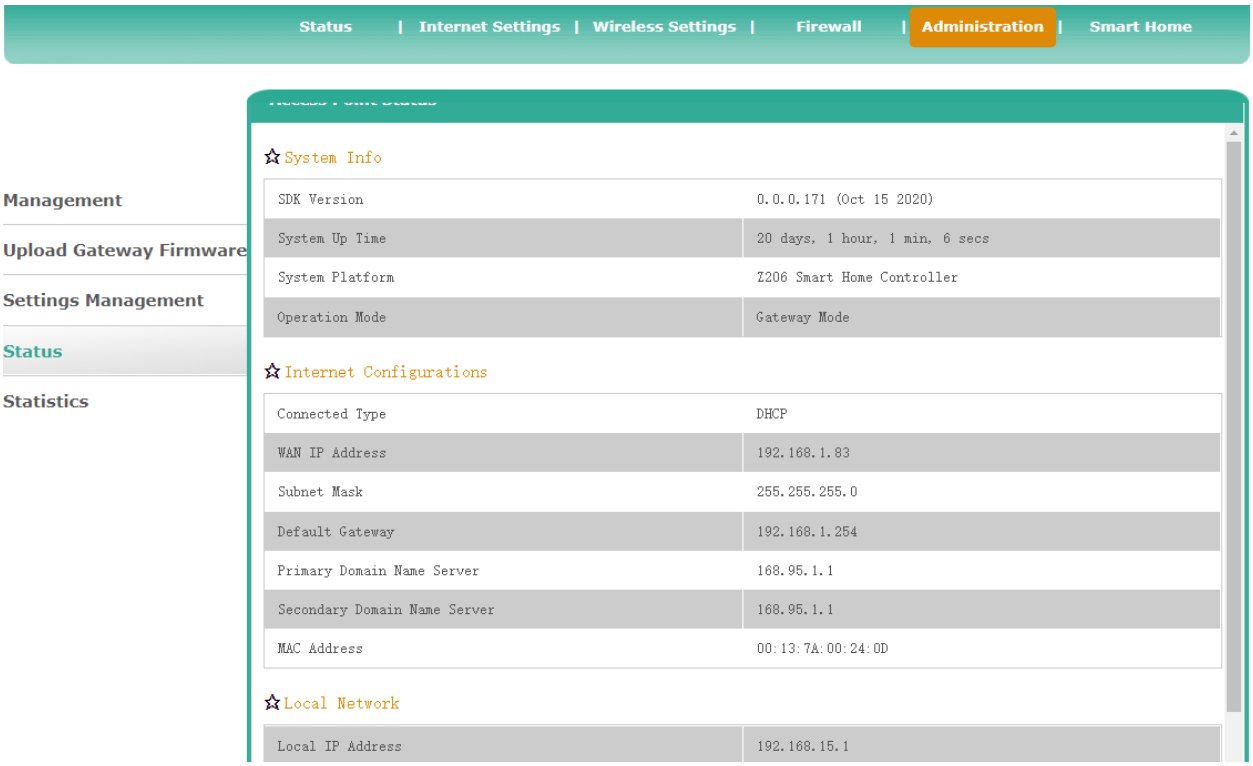




5. After the deletion is successful, click the restart button in the upper right corner to restart the gateway once and the replacement can be successful.

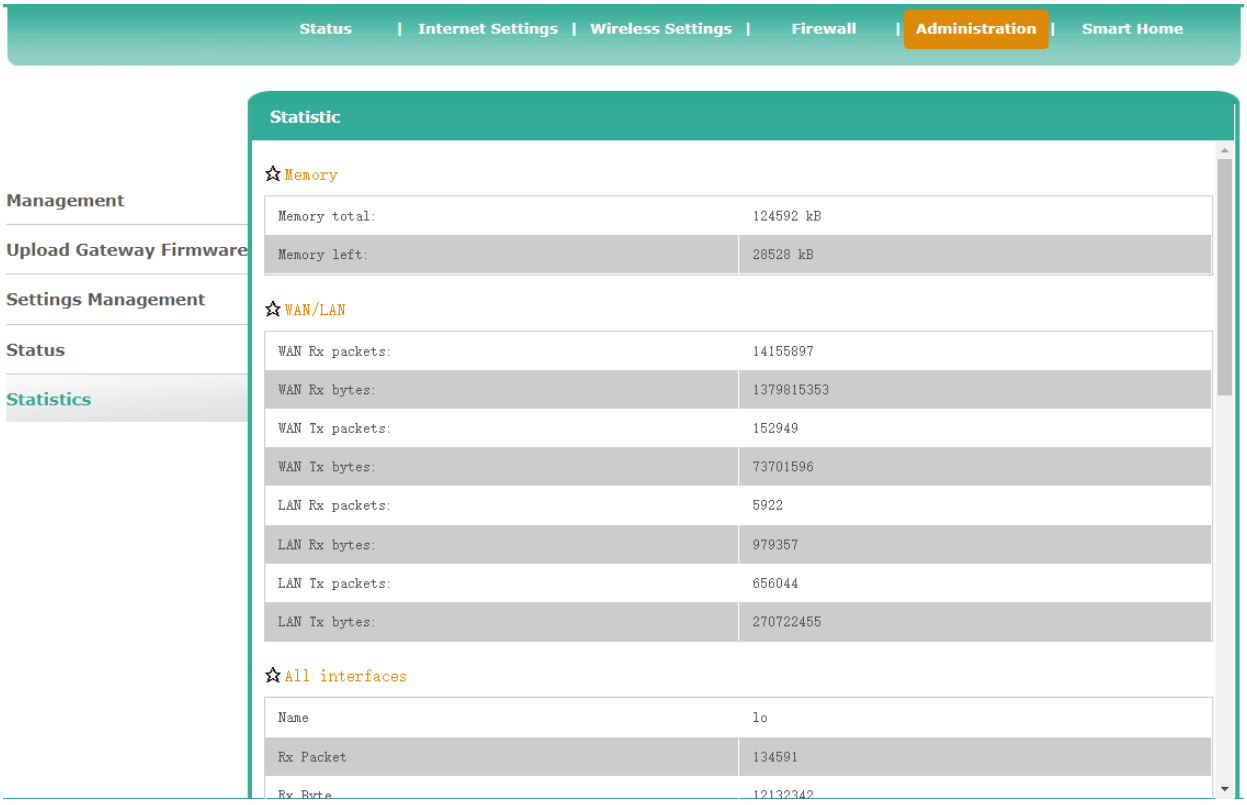
5.7.4 Status

Check the current system information and the network status of the gateway



5.7.5 Statistic

Check the statistics of the gateway, including device memory capacity, WAN data packets, and LAN data packets

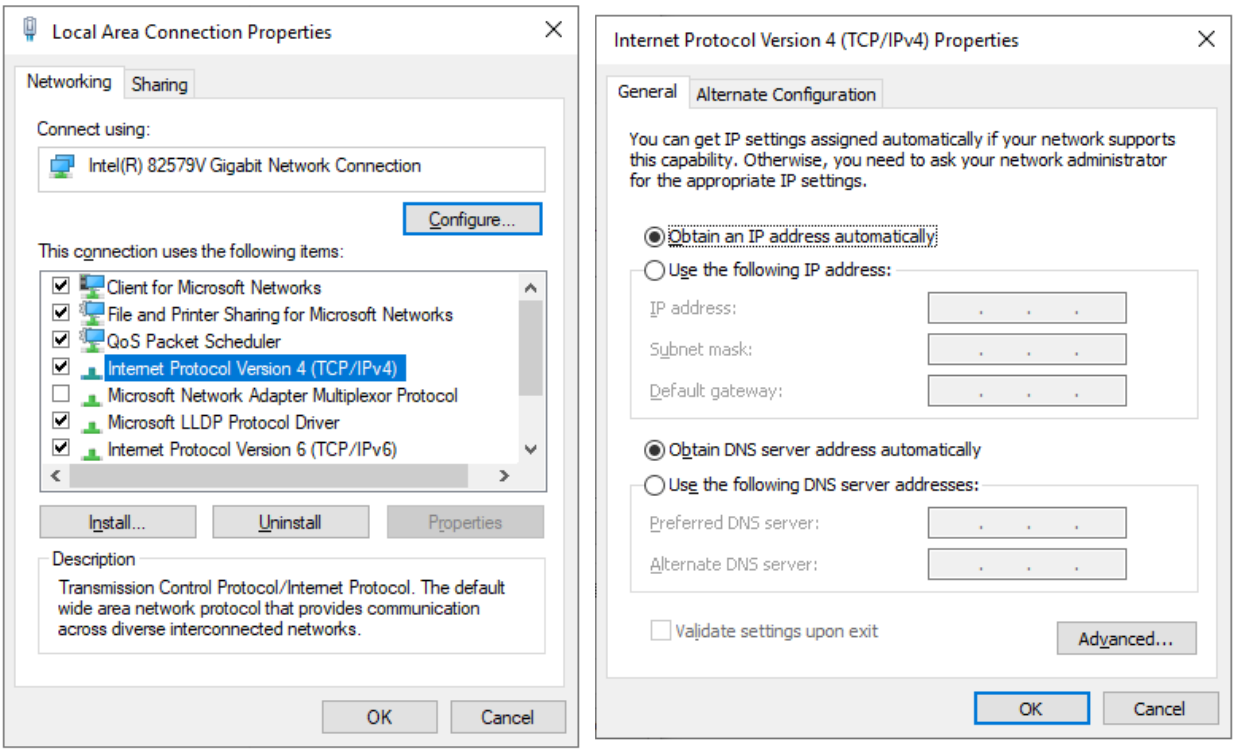


5.8 Bridging Settings

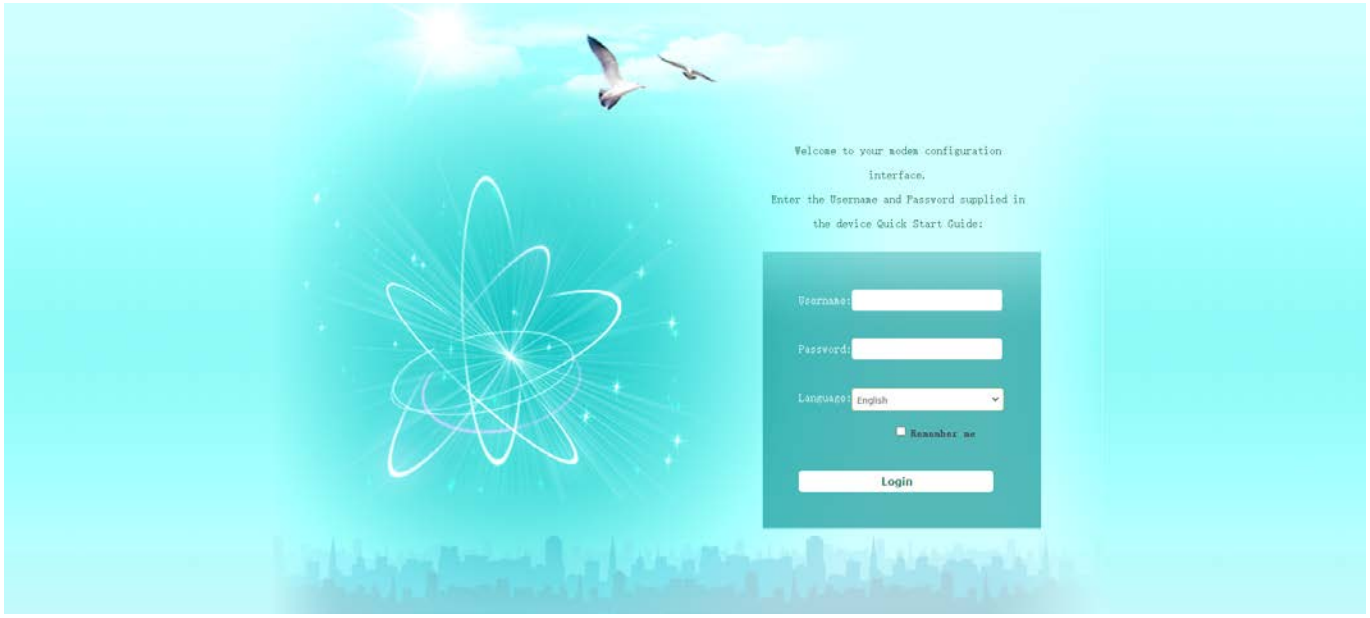
Please use a network cable to connect the LAN port of R206 to the network port of your computer, and use the matching switch transformer to power up R206.

Set the computer IP to be acquired automatically:

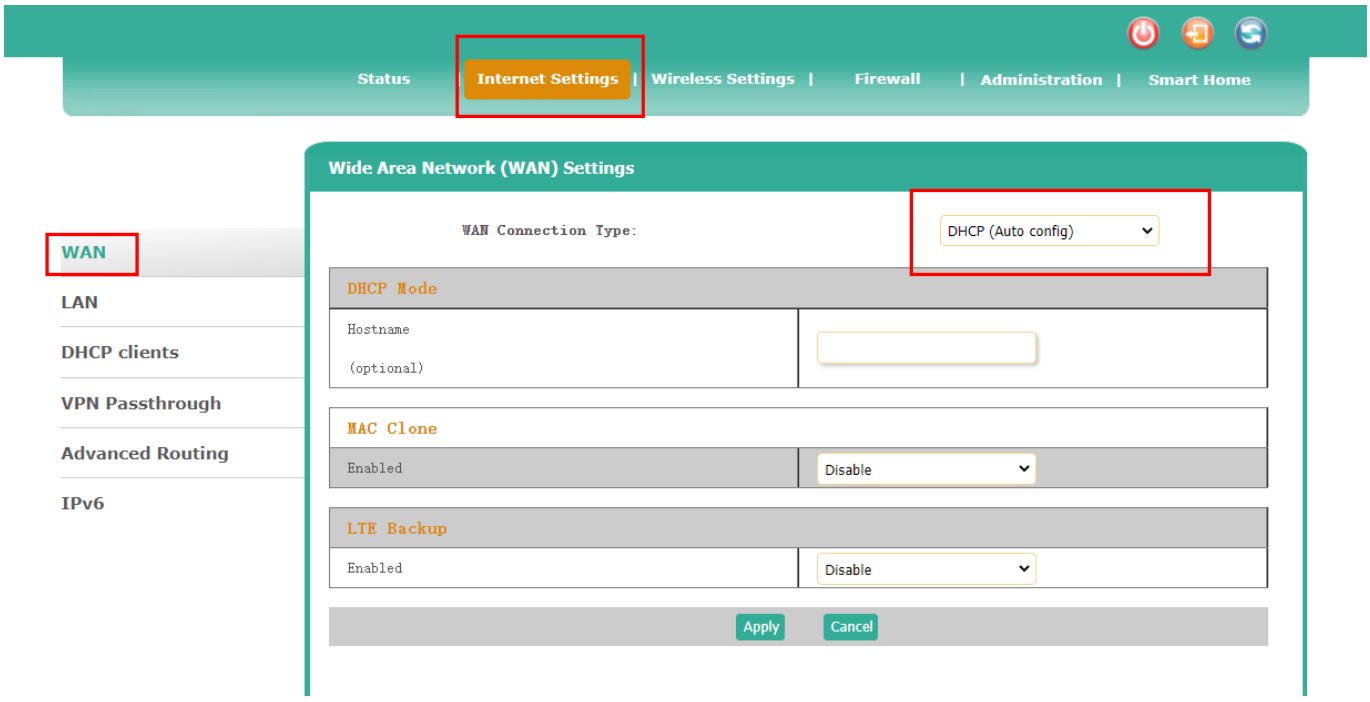
1.Click the network icon on the computer taskbar  ((Or enter “Control Panel” > “Network and Internet” > “Network Connections” > Right click to open“Local Area Connection Properties” > “TCP/IPv4” > Obtain an IP address automatically)



2. Wait for R206 startup to complete (WiFi light is on), open the browser to enter 192.168.15.1, and log in to R206 homepage.

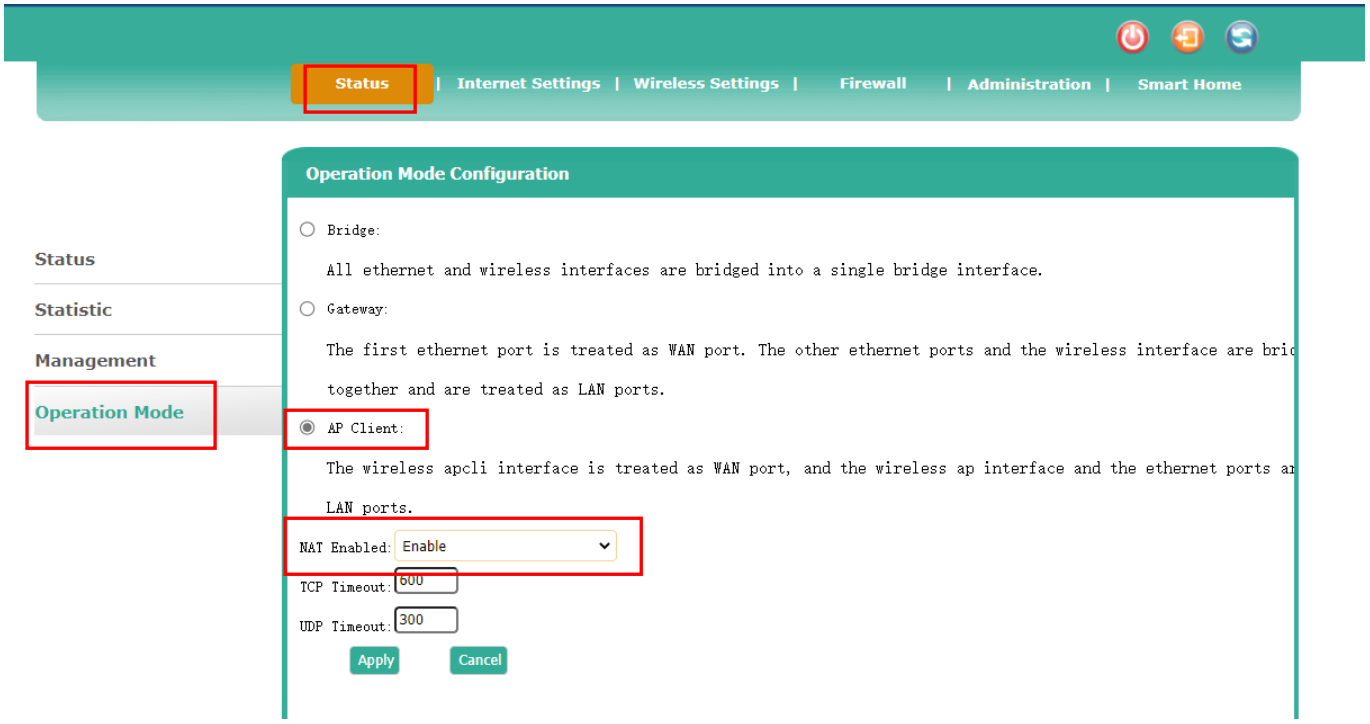


3. After logging in, click [Internet Settings], set the [WAN Connection Type] as DHCP (Auto config), and click "OK".

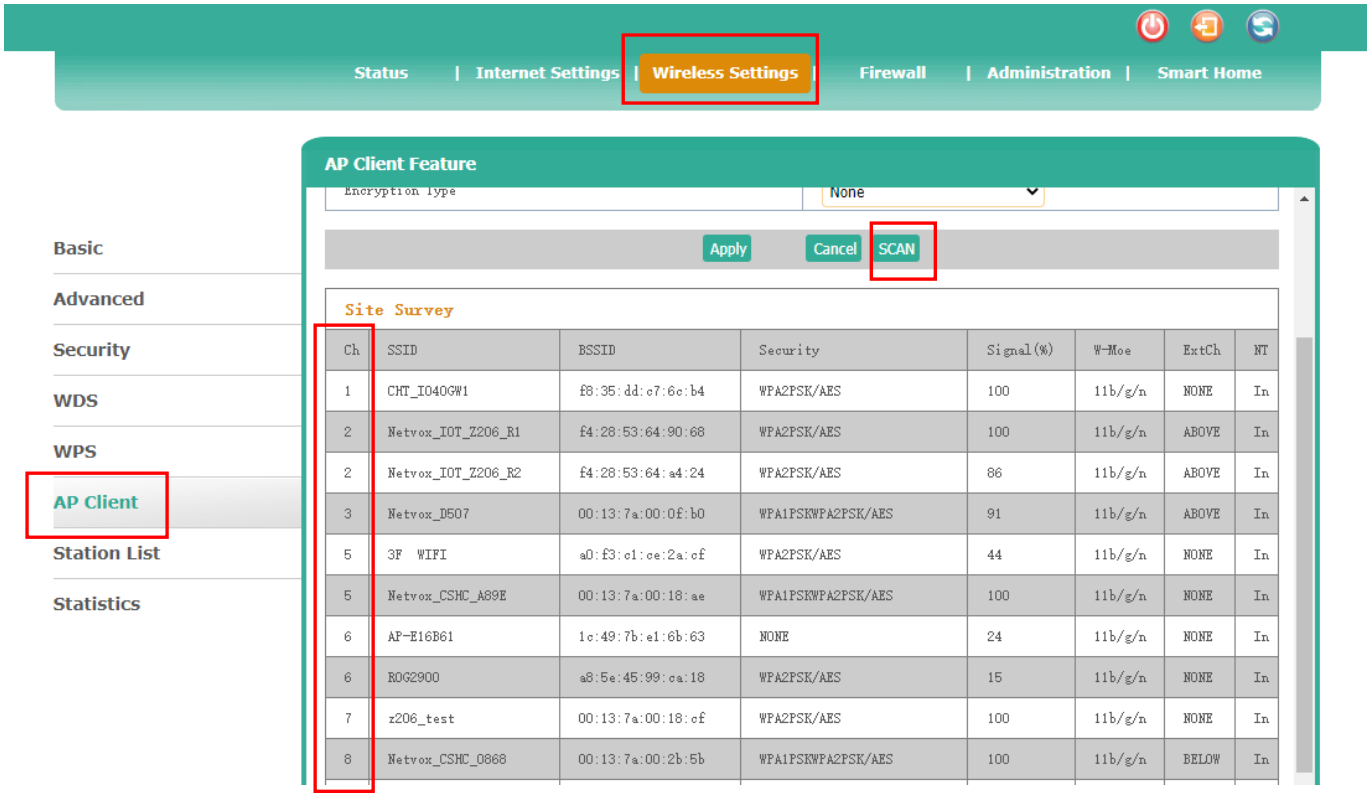


4. Click [Status] → [Operation Mode], select [AP Client], set [NAT Enabled] as enable, and click [Apply].

(Note: If it cannot be modified to AP client after confirmation, it is recommended to change Google, Firefox and IE browsers and try again. After setting, the web page will be disconnected. Please wait for reconnection.)

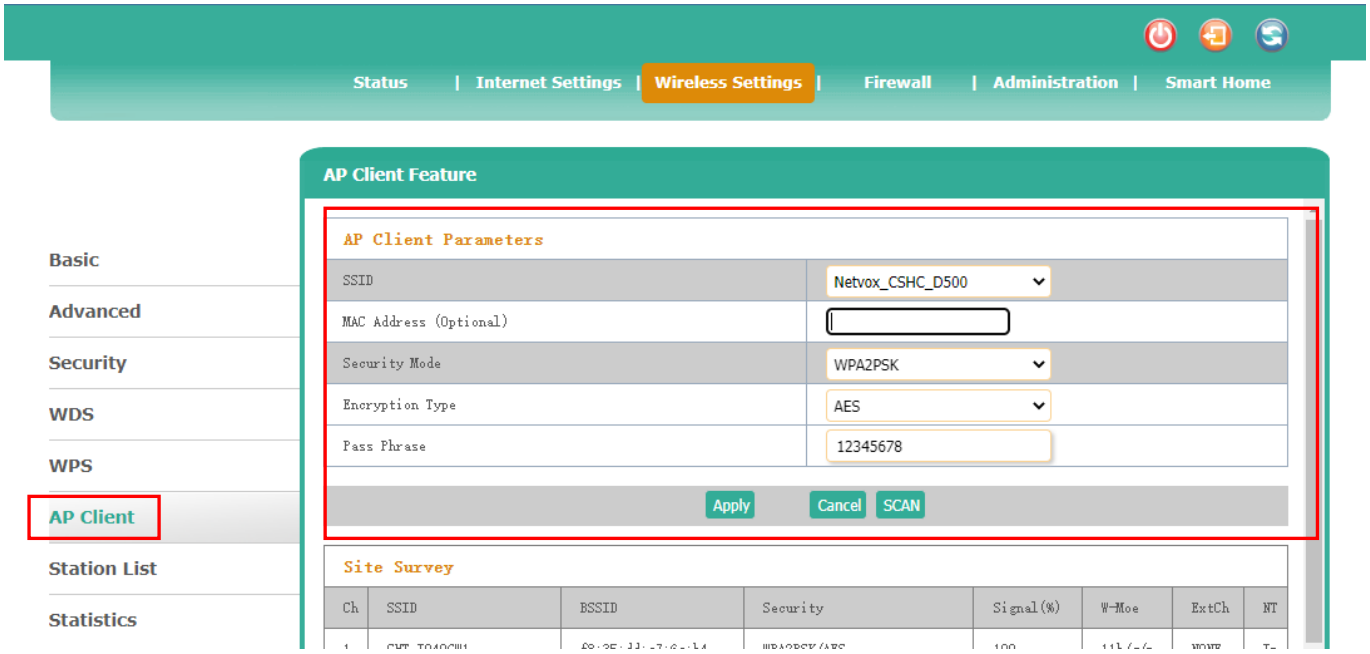


5. After the webpage is reconnected, click [Wireless Settings] → [AP Client] to view the WiFi channel of the router to be bridged in the WiFi list.



6. Enter the WiFi information of the router to be bridged (including WiFi name, Mac address, security mode, encryption method, WiFi password, etc.) in the [AP Client Feature] item, and then click [Apply]

   (Note: the web page will be disconnected after setting, please wait for reconnection). After the web page is reconnected, the bridging setting is completed.



Note:

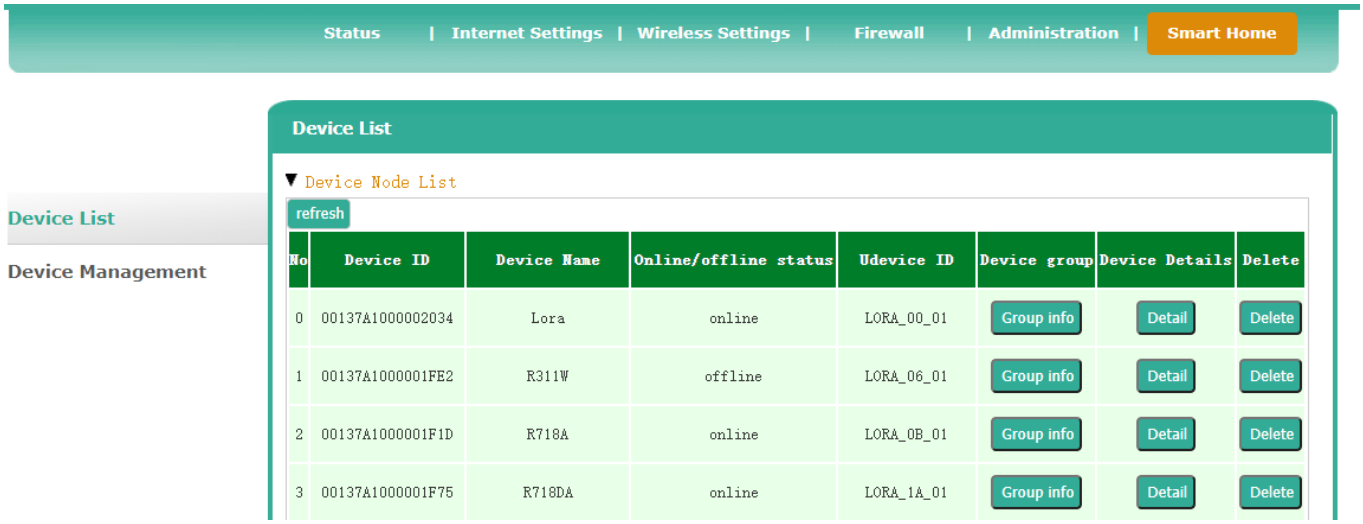
1. If the WiFi security mode of the router to be bridged is "WPAPSK/WPA2PSK", select "WPA2PSK" as the Security mode in "AP Client Feature".
2. If you log in to the R206 homepage with a mobile phone or tablet connected to the R206 WiFi, the WiFi will be disconnected after making some settings. Please reconnect to the R206 WiFi before refreshing the page.

5.9 Smart Home

LoRa devices management

5.9.1 Device List

It can check the current device information, including Device ID, Device Name, Online/offline status, Device Details, etc.

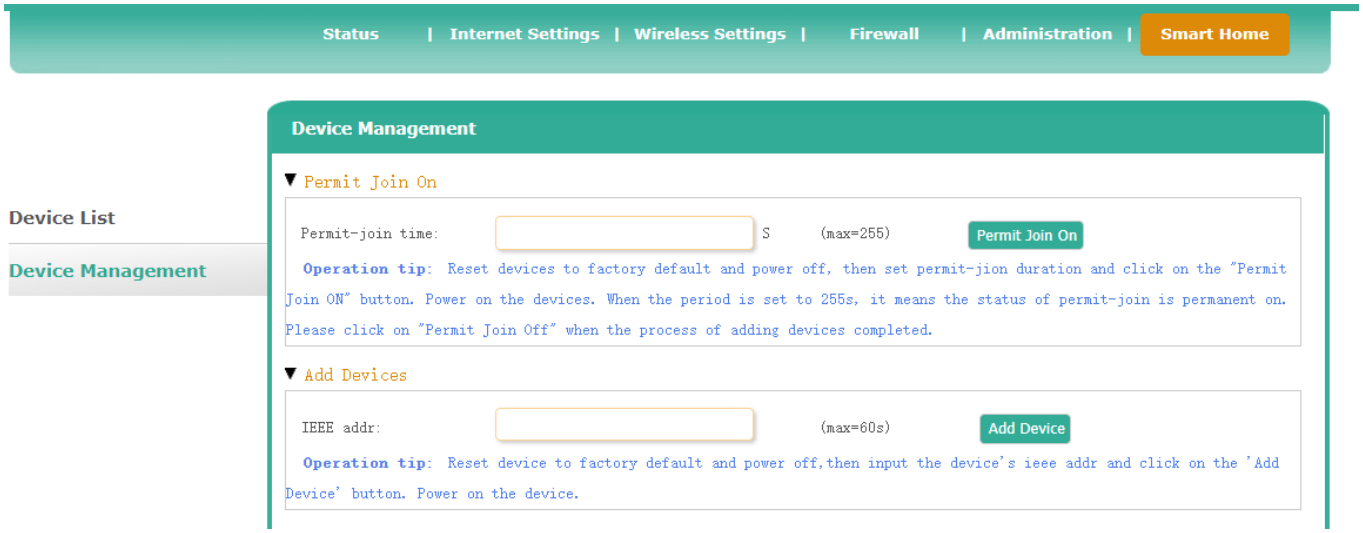


Note:

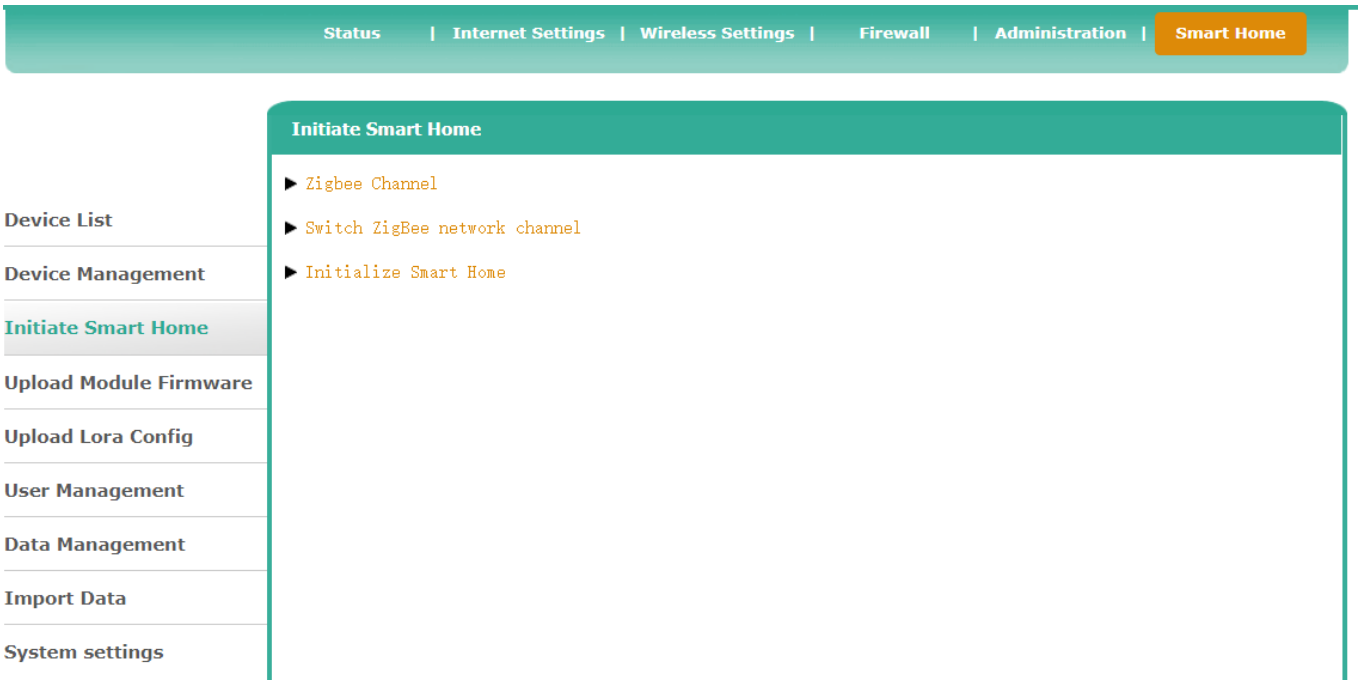
*LoRa doesn't support Group info.

5.9.2 Device Management

When Lora devices join to the network, users need to enter IEEE (DEVEUI) to enter the network. After joining, users can refresh the device list to check whether the device has been successfully joined.



5.9.3 Initiate Smart Home (This item will only be displayed for operator accounts.)

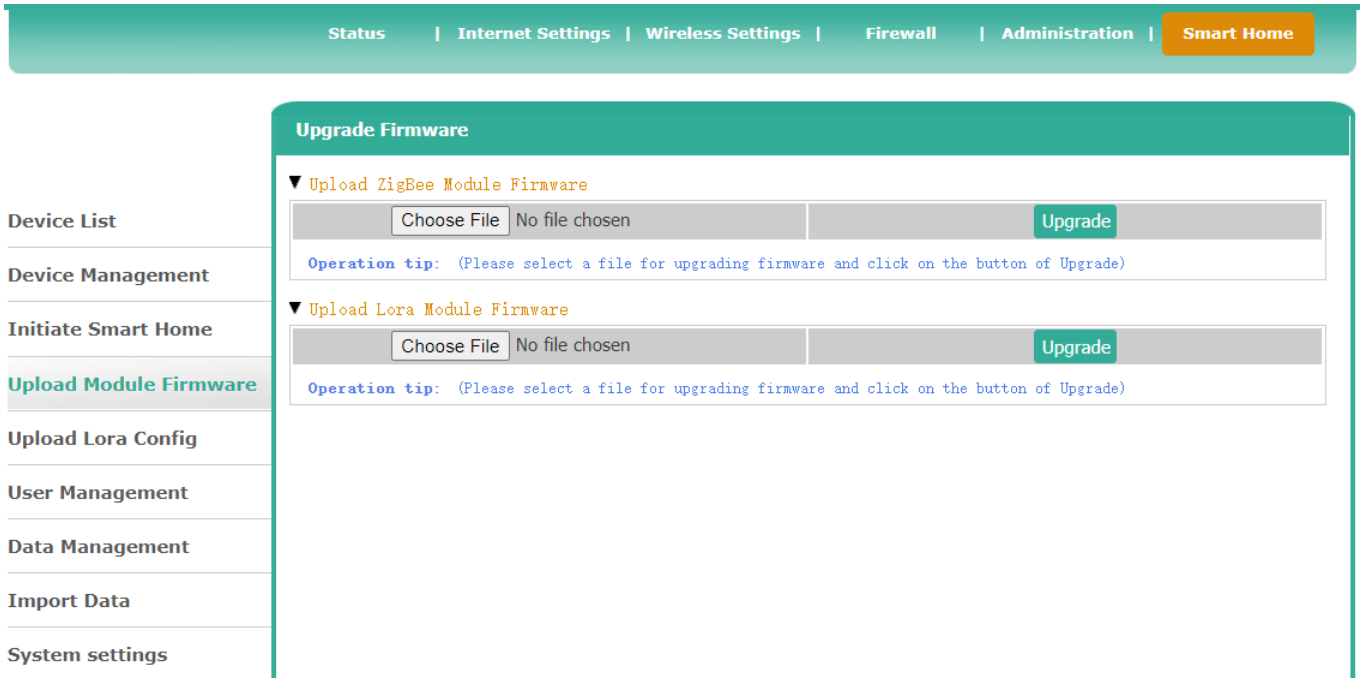


Note:

*R206 does not support this item.

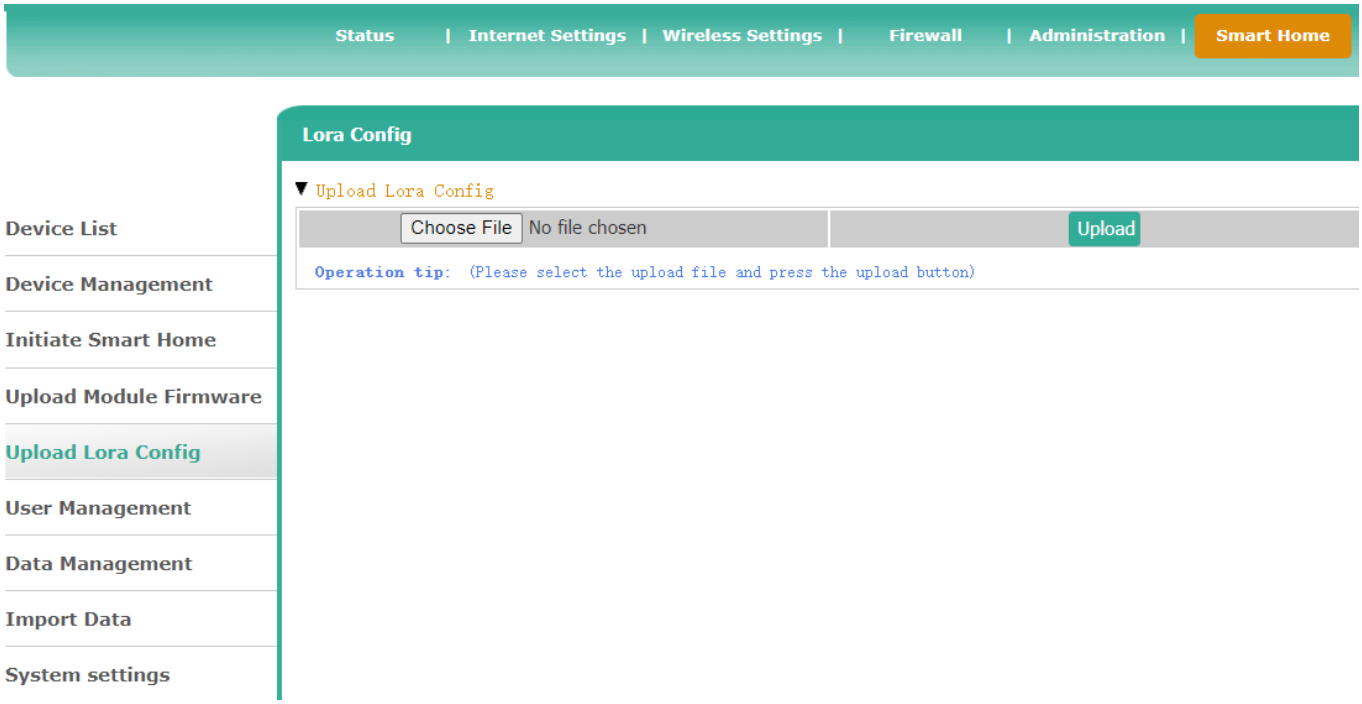
5.9.4 Upload Module Firmware (This item will only be displayed for operator accounts.)

Upgrade LoRa module firmware (Zigbee module firmware upgrade is not supported.)



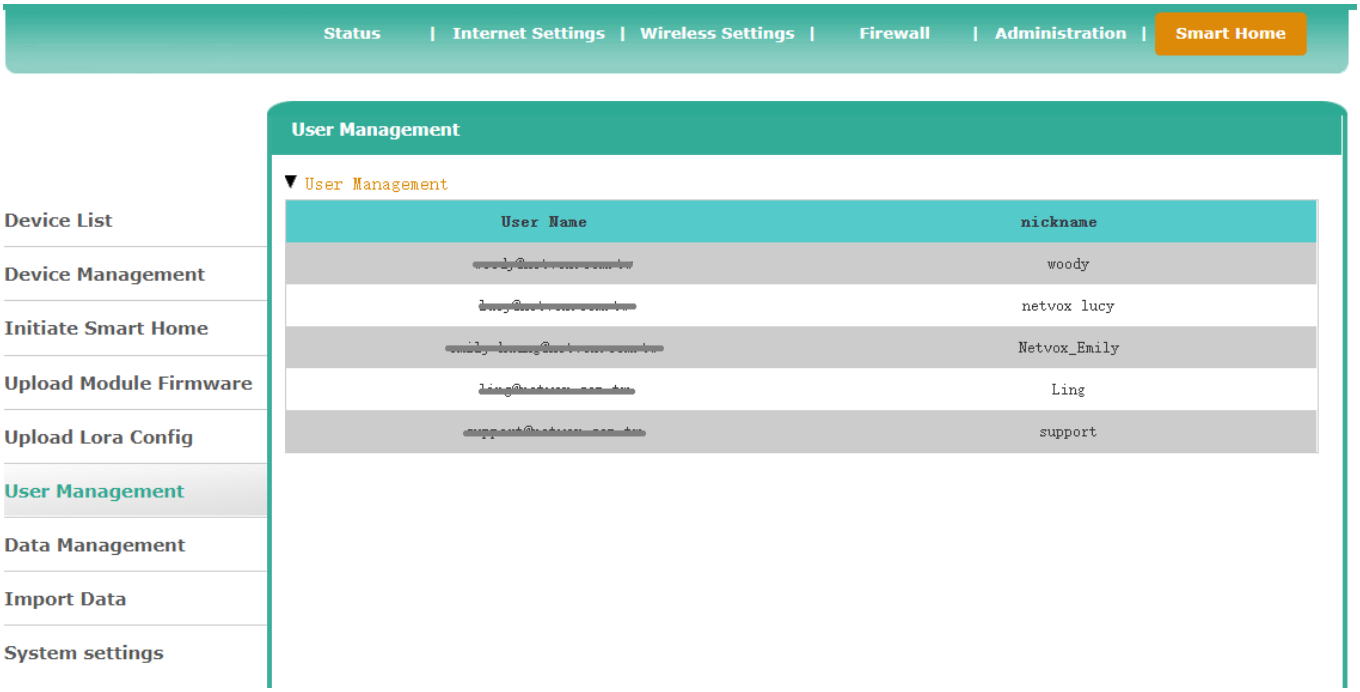
5.9.5 Upload Lora Config (This item will only be displayed for operator accounts.)

Upload the LoRa configuration file. When the new device cannot get the cloud information, users can upload the LoRa configuration file (LoraAttr.xml) to update by self.



5.9.6 User Management (This item will only be displayed for operator accounts.)

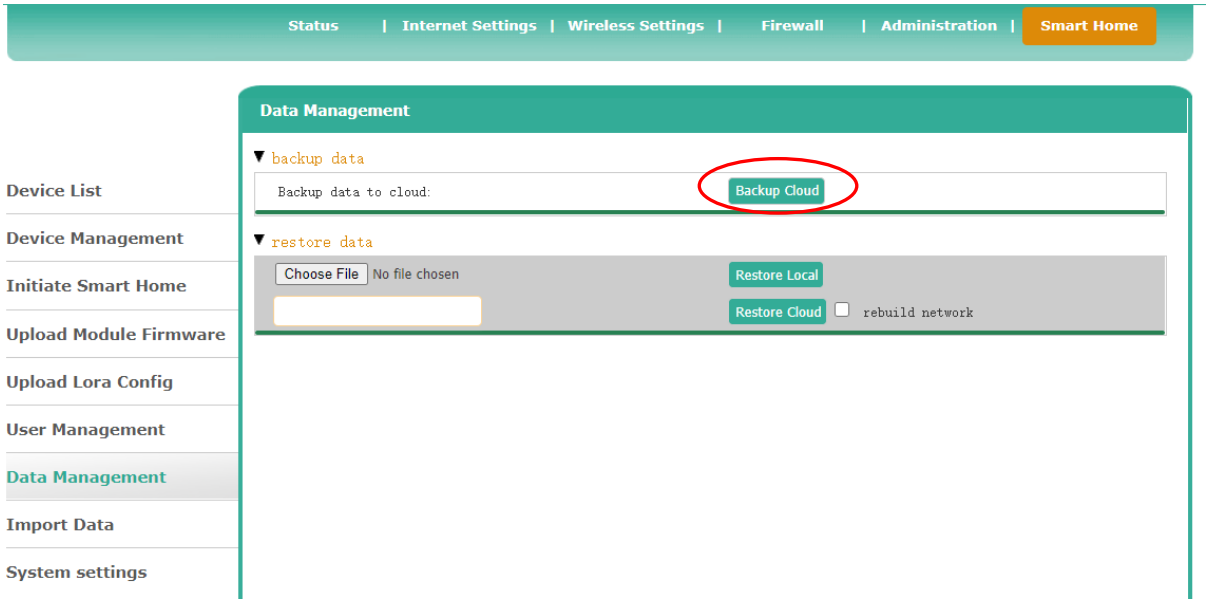
Check the registered account of the gateway



5.9.7 Data Management (This item will only be displayed for operator accounts.)

When the gateway is connected to the cloud, users can choose to manually back up the data to the cloud. Later, if the device is abnormally powered off and the file is lost, users can choose to restore the data backed up from the cloud.

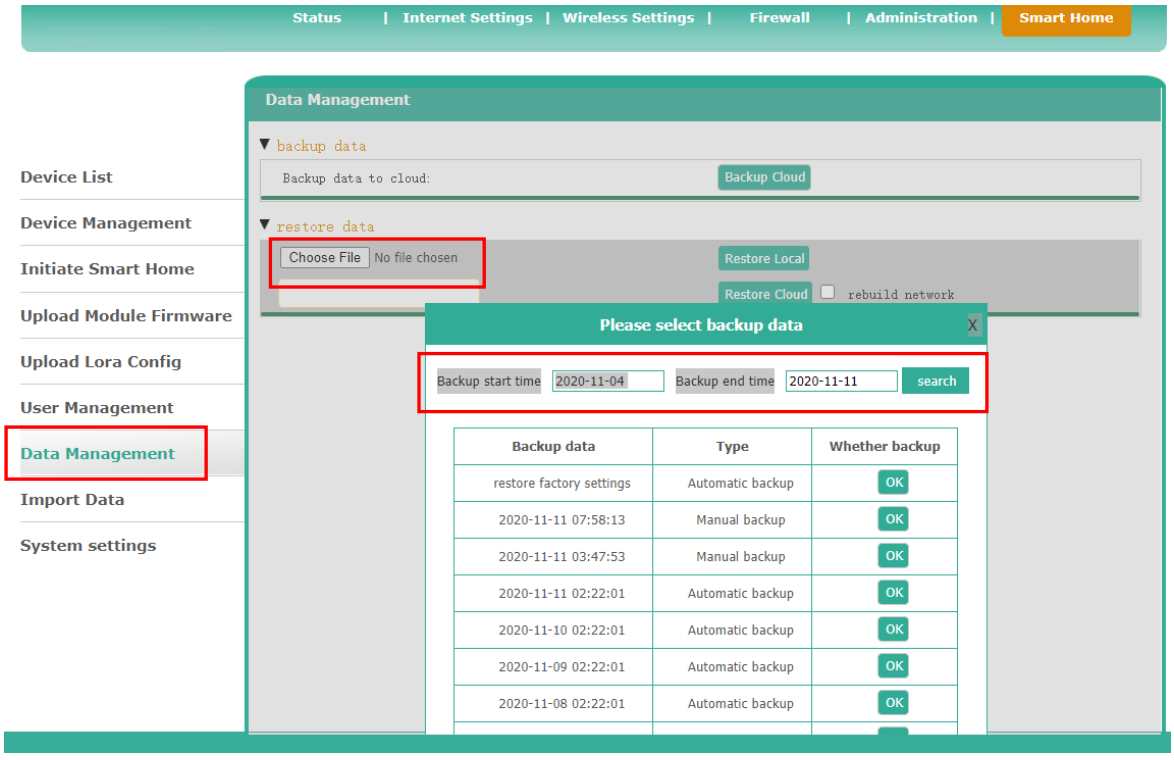
A. Backup the data of LoRa device to the cloud



B. Import cloud backup data

Select “Backup start time” and “Backup end time” in the restore data column, and click “search” to select the backup data of the corresponding date to restore.

After selecting the date, it will be displayed in the list, click the [OK] to restore the backed up data.



Note:

*When the gateway is damaged and needs to replace with a new gateway, users can choose to restore cloud backup.

* Rebuild network: LoRa gateway does not support rebuild network.

5.9.8 Import Data (This item will only be displayed for operator accounts.)

R206 doesn’t support this function.

5.9.9 System Settings

Enable https and timestamp, set cloud proxy server or MQTT

A. https

Enable/ Disable https

B. Timestamp authentication

The factory setting defaults that “Timestamp authentication” is selected. If the gateway time is incorrectly deviated by 10 minutes from the local time, the timestamp authentication will be timeout.

The factory setting defaults that timestamp authentication is 10 minutes. Namely, only if the time lag between the gateway time and the local time is within plus and minus 10 minutes, can the communication be normal.

C. Callback Authorization

The factory setting defaults that “Callback Authorization” is selected. Therefore, users do not need to modify it.

D. Cloud Connection

Default Cloud Address: mngm2.netvoxcloud.com:80

* Modifying to other URLs may cause the gateway to fail to connect to the cloud.

E. MQTT Connection

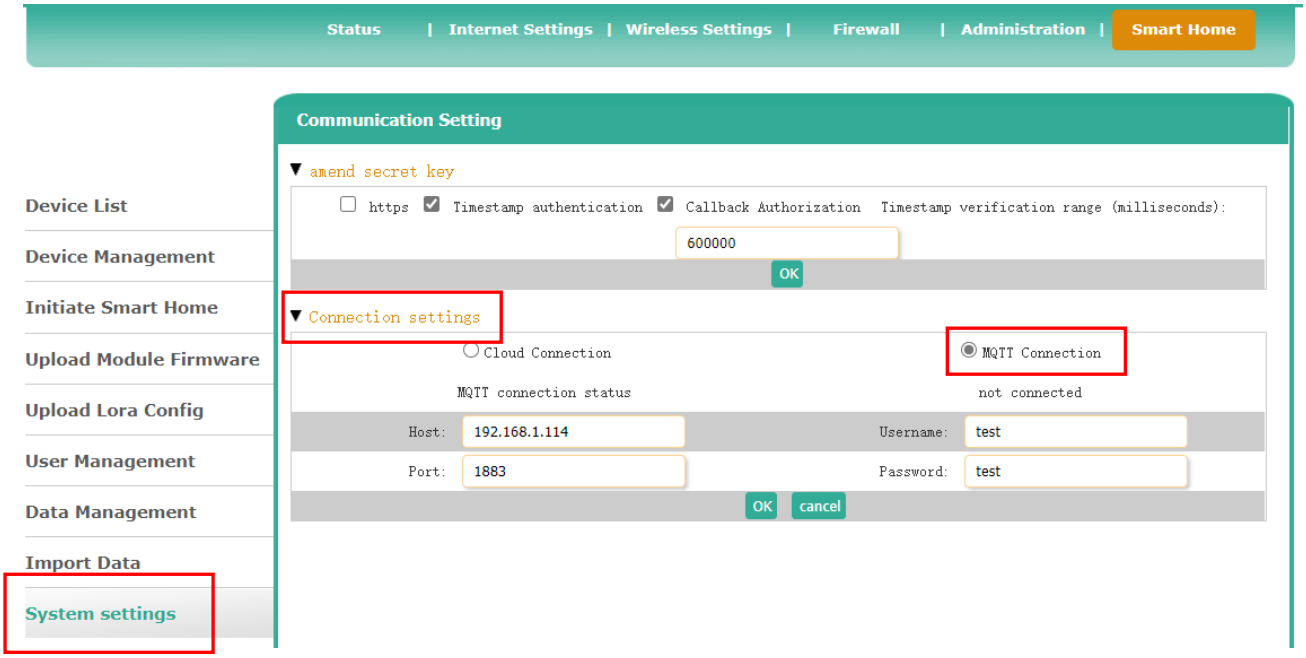
Please enter MQTT Host IP, Port, Username, and Password.

Note:

MQTT messages are encrypted.

The user needs to be authorized the GW REST API before using.

For the related matters, please contact the sales executive.



6. Related Product

R103 USB Dongle - Netvox Config Tool

7. Important Maintenance Instructions

Your device is a product of superior design and craftsmanship and should be used with care. The following suggestions will help you use the warranty service effectively.

- Keep the equipment dry. Rain, moisture, and various liquids or moisture may contain minerals that can corrode electronic circuits. In case the device is wet, please dry it completely.
- Do not use or store in dusty or dirty areas. This can damage its detachable parts and electronic components, destroy batteries, and deform or melt some plastic parts.
- Do not store in an excessive cold place. Otherwise, when the temperature rises to normal temperature, moisture will form inside, which will destroy the board.
- Do not throw, knock or shake the device. Rough handling of equipment can destroy internal circuit boards and delicate structures.
- Do not wash with strong chemicals, detergents or strong detergents.
- Do not apply with paint. Smudges can block debris in detachable parts and affect normal operation.
- Do not throw the battery into afire to prevent the battery from exploding. Damaged batteries may also explode.

All of the above suggestions apply equally to your device, battery and accessories. If any device is not working properly.

Please take it to the nearest authorized service facility for repair.