

Web Management Guide



Digital Data Communications GmbH.

<http://www.level1.com>

Web Management Guide

WAB-8011

AC1200 Dual Band Outdoor PoE Wireless Access Point

WAP-8021

AC1200 Dual Band Wireless Access Point

WAP-8121

AC750 Dual Band PoE Wireless Access Point

WAP-8122

AC1200 Dual Band PoE Wireless Access Point

WAP-8123

AC1200 Dual Band PoE Wireless Access Point

WAP-8221

AC750 Dual Band PoE Wireless Access Point

Contents

	Contents	4
	Default Settings	5
	Logging on to the equipment	5
Section I	Home	7
	Fit AP (Mode switching instructions)	9
	Fat AP (Mode switching instructions)	14
Section II	Wizard	15
	Gateway Mode	15
	Repeater Mode	22
	WISP Mode	26
	AP Mode	30
Section III	WiFi	33
	2G WiFi	33
	5G WiFi	38
	MAC ACL	42
	WiFi Timer Off	46
	Advanced Setting	46
Section IV	Network (for AP/Repeater Mode)	49
	LAN Settings	49
	VLAN Settings	49
Section V	Manage (for AP/Repeater Mode)	50
	Configure	50
	Reboot	50
	Modify Password	51
	Upgrade	51
	Time	52
	Log	52

Section VI	Network (for Gateway/WISP Mode)	53
	LAN Settings	53
	Static DHCP	53
	WAN Settings	54
	WAN Advanced Settings	54
	URL Mapping	55

Section VII	Security (for Gateway/WISP Mode)	56
	URL Filter	56
	IP Filter	57
	MAC Filter	58
	Security	59
	DMZ	60

Section VIII	Manage (for Gateway/WISP Mode)	61
	Configure	61
	Reboot	61
	Modify Password	62
	Upgrade	62
	Time	63
	Log	63
	Flow Control	64
	IP Group	65
	Time Group	66
	DDNS Settings	66

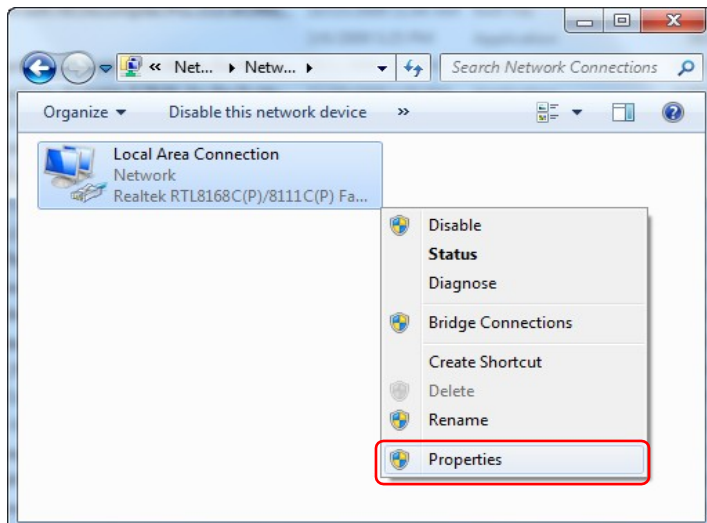
Default Settings

AP provides Web-based management login, you can configure your computer's IP address manually to log on to the AP. The default settings of the AP are shown below.

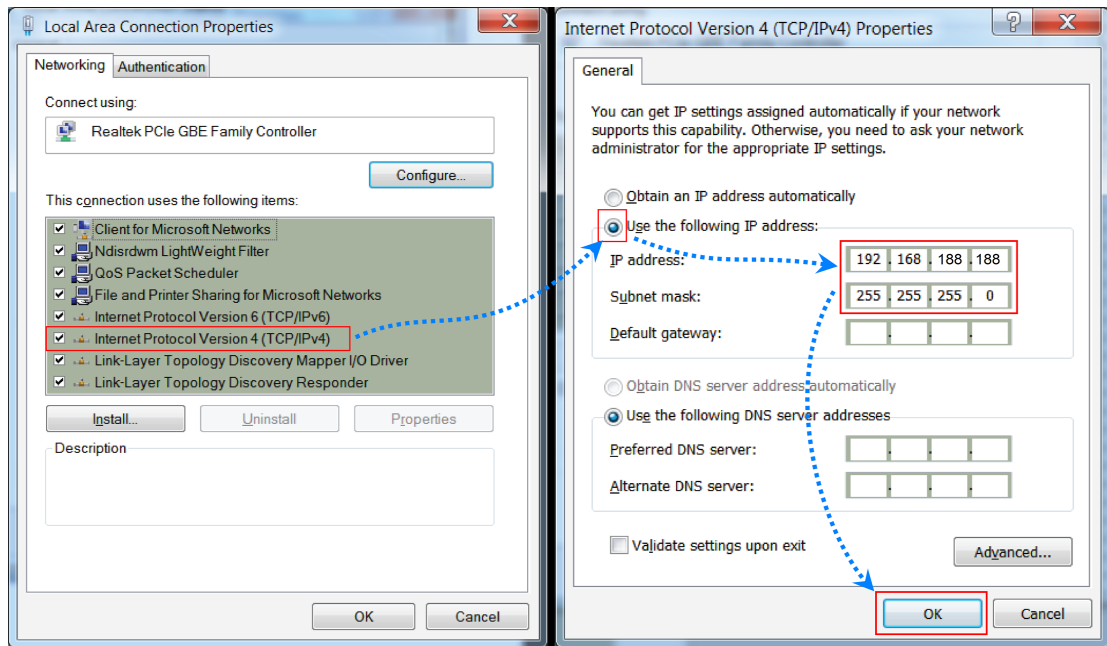
IP Address	192.168.188.253
Password	admin

Logging on to the equipment

- Connect the RJ-45 interface cable of a switch with a computer using a network cable.
 - Set the TCP/IP properties of the computer.
- **Windows**
 1. Click **Start**→ **Control Panel**→ **Network and Internet**→ **Network and Sharing Center**→ **Change adapter settings**, right click **Local connection** and select **Properties**;



2. Double-click **Internet Protocol 4 (TCP/IPv4)**; Set the computer's IP address: The computer's IP address should be any one of the following free IP addresses 192.168.188.2 ~ 192.168.188.252, and then click **OK**, to return to the previous page, click **OK**.



3. Logging on to the equipment: Open a browser and type 192.168.188.253 in the address bar, and then press Enter; in the pop-up login interface, enter the factory logon password **"admin"** and click "Login".

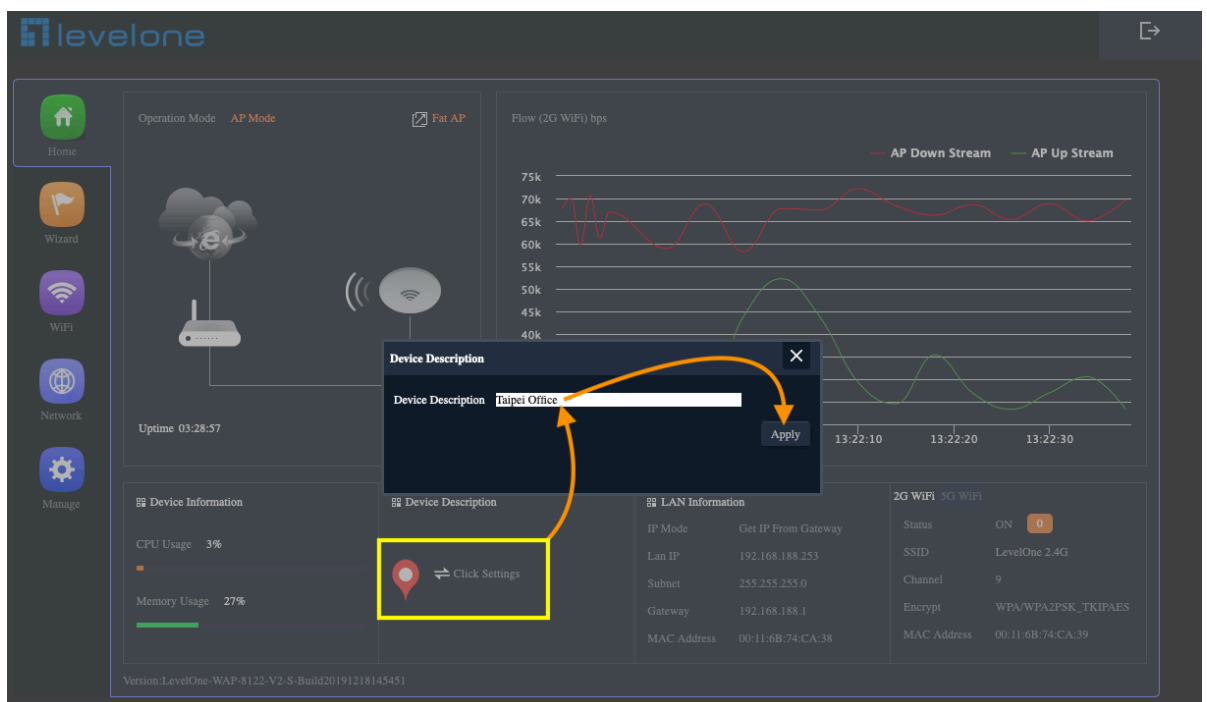


Section I Home

After login, This page will show the Wireless AP's default operation mode, channel, connection status, CPU usage, Wireless settings, LAN Setting, Wireless AP's Location, hardware/firmware version.



1. Different operation modes are slightly different on the Home screen. The example below is AP Mode. Can set the location of the remark AP, which is convenient for future management



2. Different operation modes are slightly different on the Home screen. The example below is **Gateway Mode**. Can set the location of the remark AP, which is convenient for future management

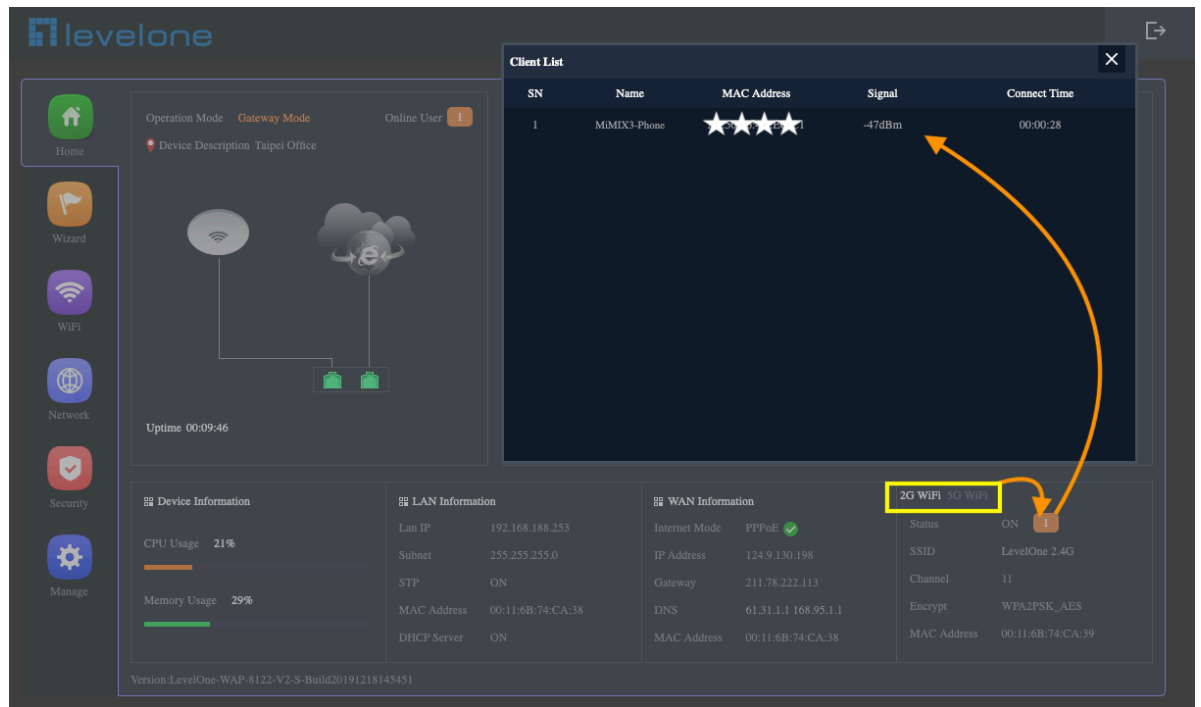
The screenshot shows the LevelOne Gateway Mode Home screen. The 'Device Description' dialog box is open, allowing the user to set the location of the remark AP. The dialog box contains a text input field with 'Taipei Office' and an 'Apply' button. The background screen shows the 'Operation Mode' as 'Gateway Mode', 'Online User' as 1, and a 'Flow' graph. The 'Device Information' section shows CPU Usage at 18% and Memory Usage at 29%. The 'LAN Information' section shows LAN IP as 192.168.188.253. The 'WAN Information' section shows Internet Mode as PPPoE. The '2G WIFI' and '5G WIFI' sections show Status as ON, SSID as LevelOne 2.4G, Channel as 11, and Encrypt as WPA2PSK_AES.

3. Can view the current Wireless Online User

The screenshot shows the LevelOne Gateway Mode Home screen. The 'Online User' dialog box is open, displaying a table of current wireless online users. The table has columns for SN, Name, IP Address, MAC Address, Up, Down, and Link count. The background screen shows the 'Operation Mode' as 'Gateway Mode', 'Online User' as 1, and a 'Flow' graph. The 'Device Information' section shows CPU Usage at 16% and Memory Usage at 29%. The 'LAN Information' section shows LAN IP as 192.168.188.253. The 'WAN Information' section shows Internet Mode as PPPoE. The '2G WIFI' and '5G WIFI' sections show Status as ON, SSID as LevelOne 2.4G, Channel as 11, and Encrypt as WPA2PSK_AES.

SN	Name	IP Address	MAC Address	Up	Down	Link count
1	MiMIX3-Phot	192.168.188.85	*****	1Mb	6Mb	33

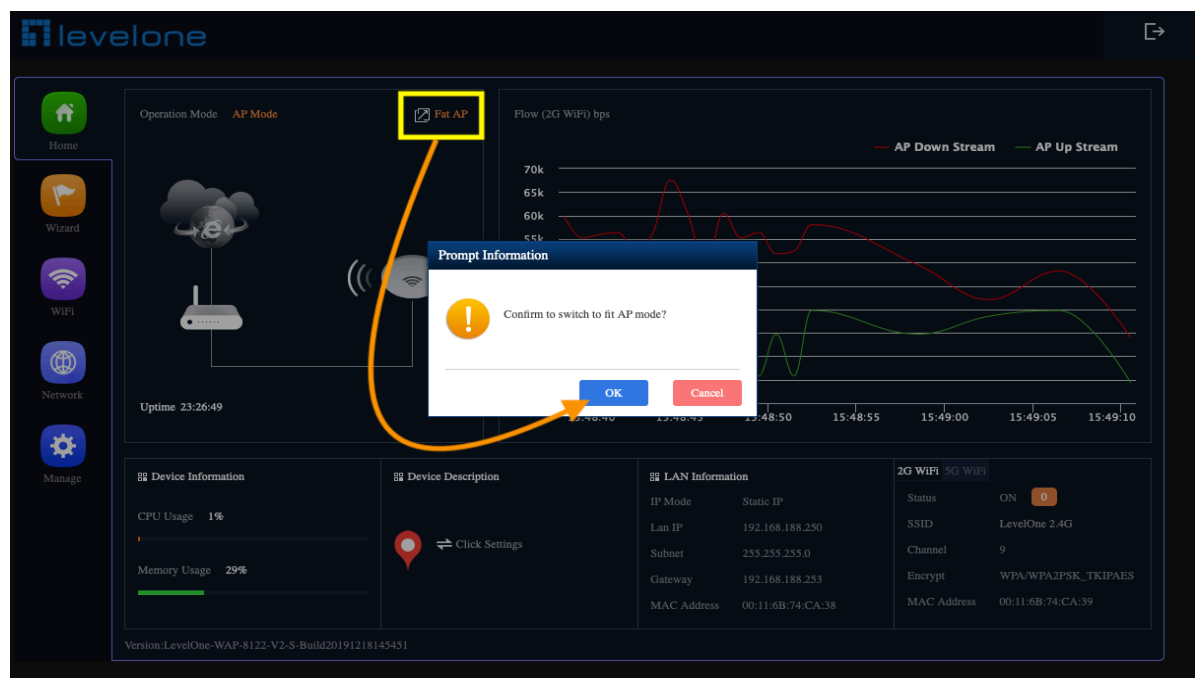
4.Can view the current wireless online users of 2.4G or 5G respectively



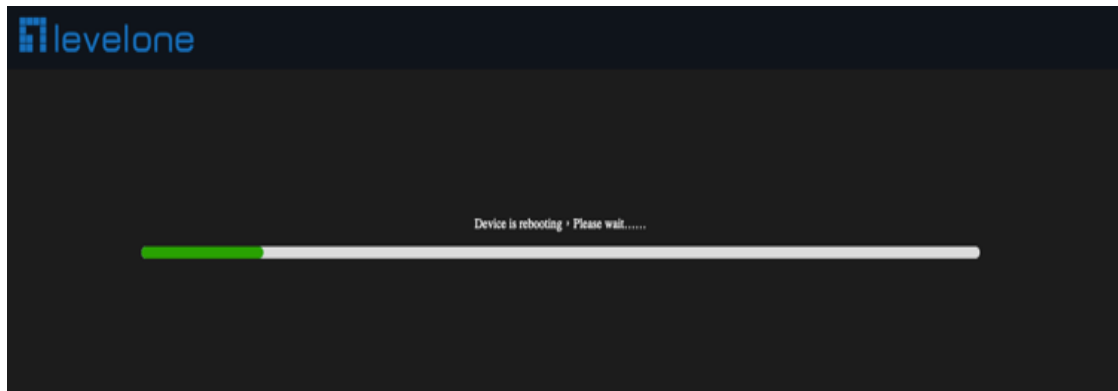
Fit AP (Mode switching instructions)

Simple operation function, can be used with the new wireless control platform in the future
(Not applicable to WAC-2000 / WAC-2003)

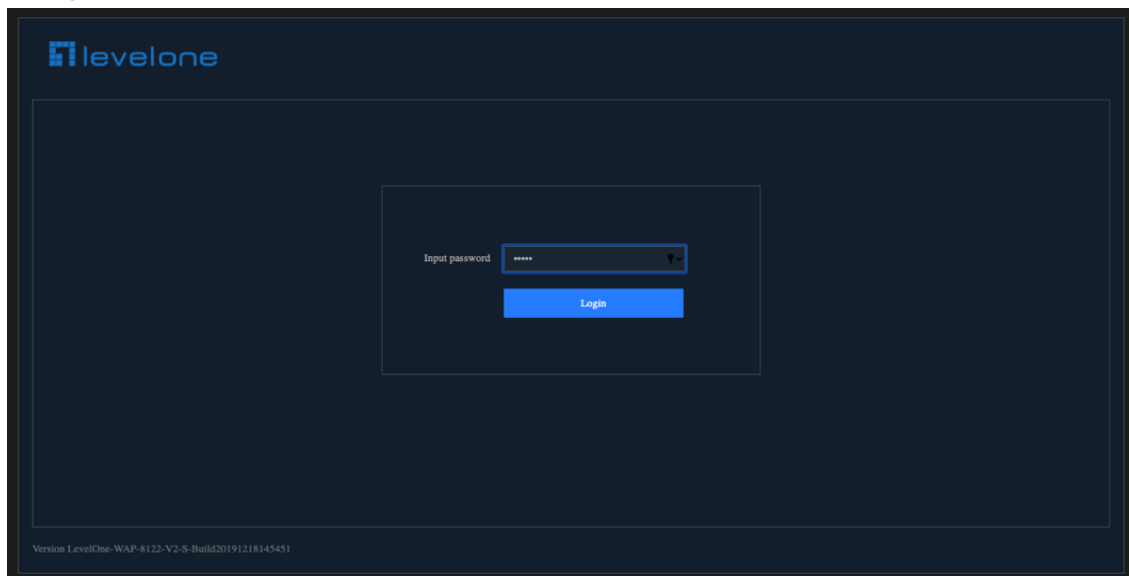
1.The following is a demonstration of switching to Fit AP mode



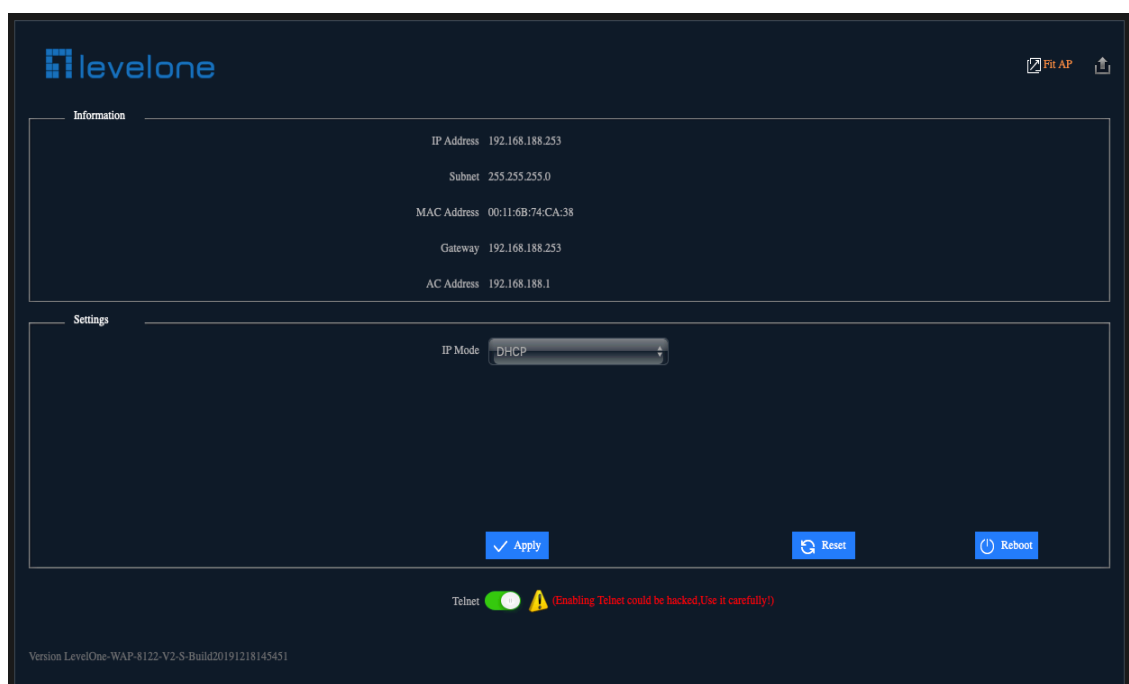
2. Please wait more than 30 seconds



3. Login to Fit AP mode. Default password: admin



4. There are 2 modes for IP Mode in Fit AP (DHCP, Static IP)



5. There are 2 modes for IP Mode in Fit AP (DHCP, Static IP)

The screenshot shows the LevelOne Fit AP configuration interface. The 'Information' tab is active, displaying the following details:

- IP Address: 192.168.188.253
- Subnet: 255.255.255.0
- MAC Address: 00:11:6B:74:CA:38
- Gateway: 192.168.188.253
- AC Address: 192.168.188.1

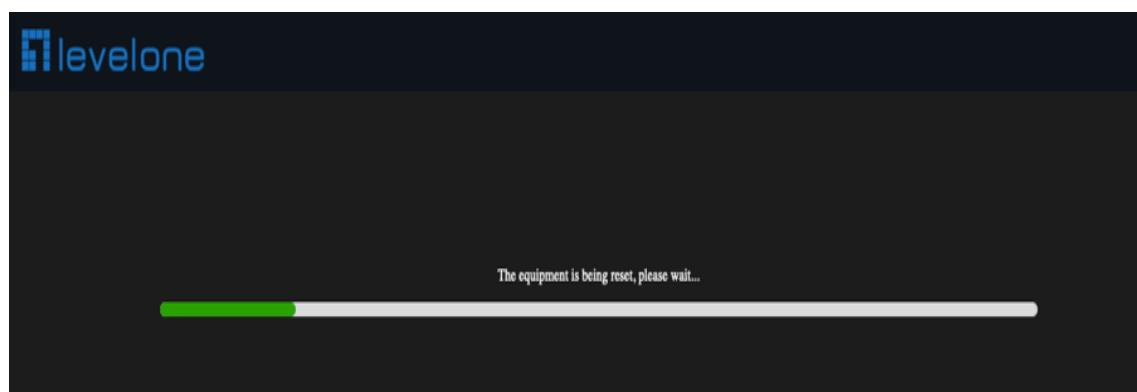
The 'Settings' tab is also visible, showing the 'IP Mode' set to 'Static IP'. Below this, the same IP, Subnet, Gateway, and AC Address are listed. At the bottom of the settings section, there are three buttons: 'Apply' (with a checkmark icon), 'Reset' (with a circular arrow icon), and 'Reboot' (with a power icon). Below these buttons, there is a 'Telnet' toggle switch which is currently turned on, accompanied by a warning icon and the text '(Enabling Telnet could be hacked, Use it carefully!)'. The footer of the interface shows the version: 'Version LevelOne-WAP-8122-V2-S-Build20191218145451'.

Reset the Fit AP settings

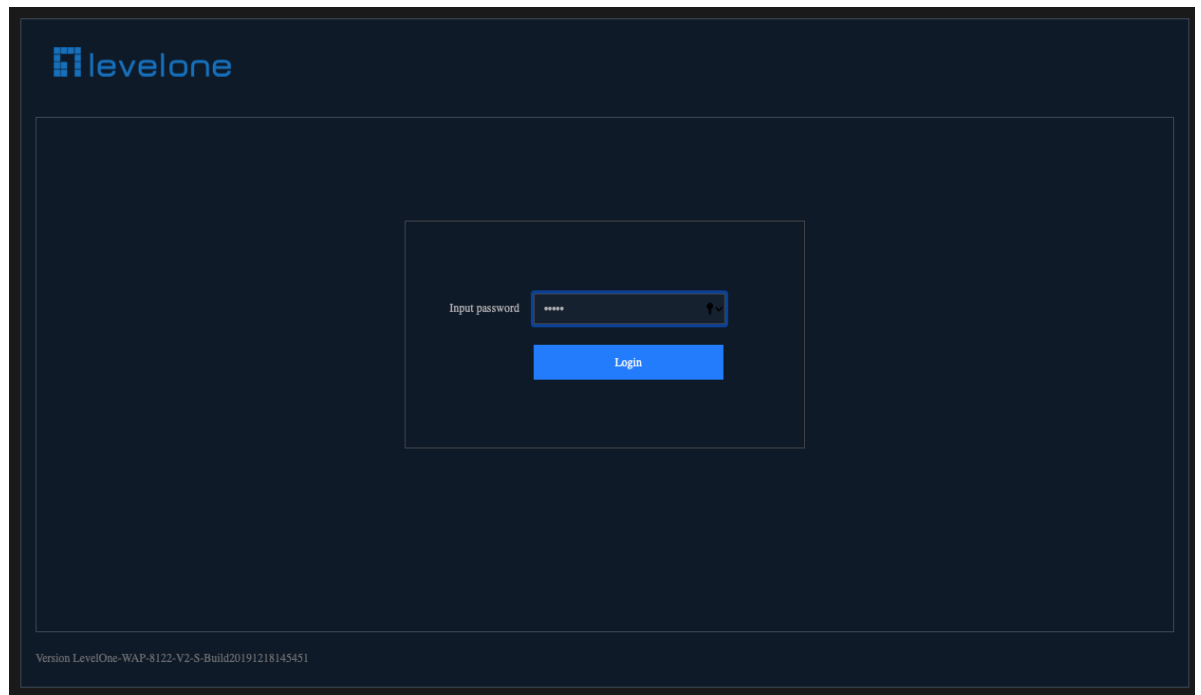
1. unless you manually click to switch to the Fat AP, it will remain in the Fit AP after reset

This screenshot shows the same LevelOne Fit AP configuration interface as before, but with a 'Prompt Information' dialog box overlaid in the center. The dialog box contains a yellow warning icon and the text: 'Are you sure you want to restore the factory settings?'. It has two buttons: 'OK' (blue) and 'Cancel' (red). An orange arrow points from the 'Reset' button in the background settings area to the 'OK' button in the dialog box. The background settings are partially obscured by the dialog box, but the 'Apply', 'Reset', and 'Reboot' buttons are still visible at the bottom. The 'Telnet' toggle is also visible at the bottom, showing the same warning as in the previous screenshot. The footer version remains the same.

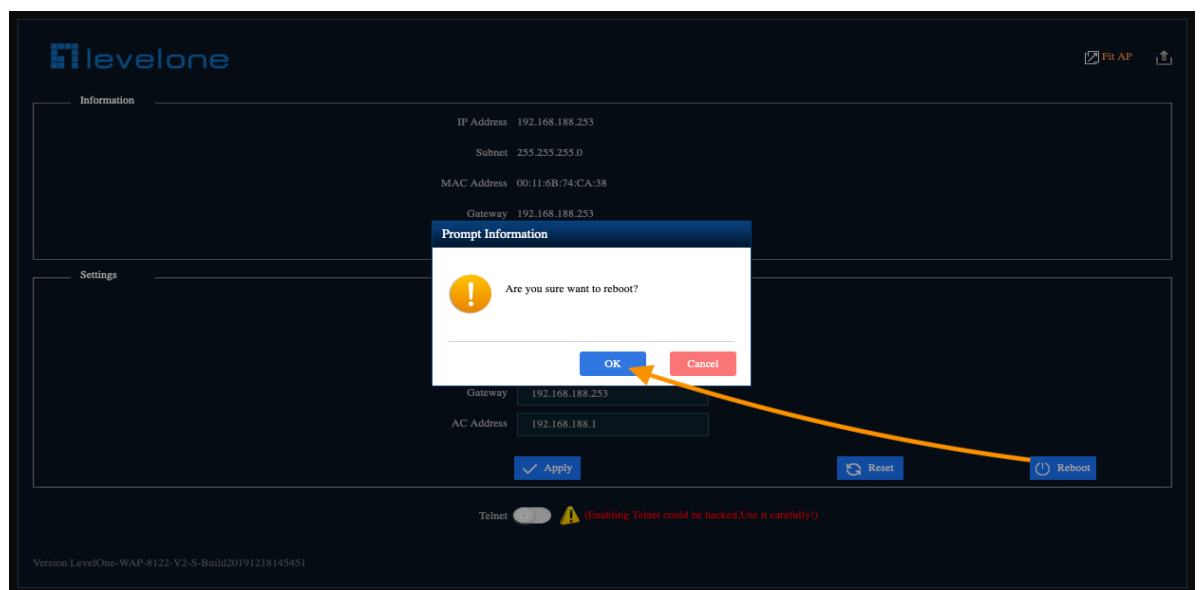
2. Please wait more than 30 seconds



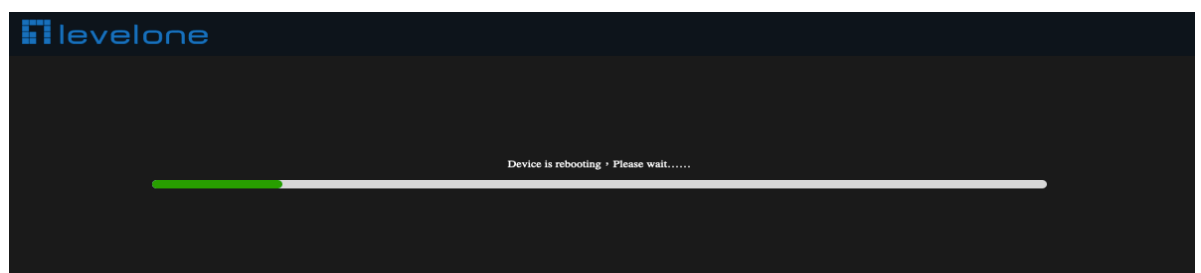
3.Login to Fit AP mode. Default password: admin



Reboot the Fit AP settings

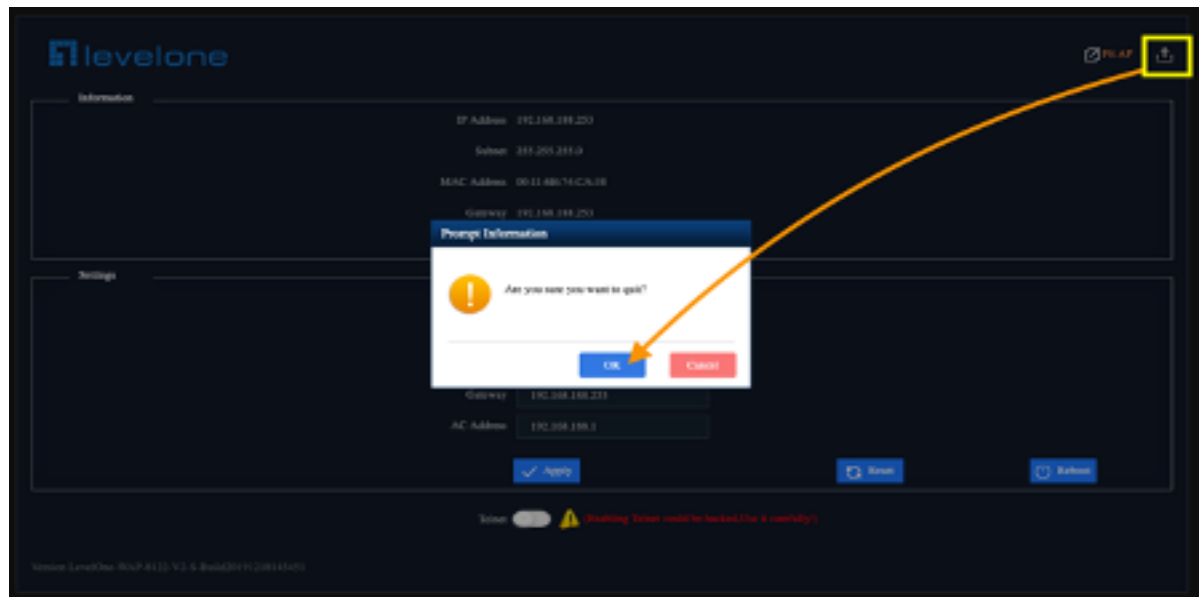


Please wait more than 20 seconds

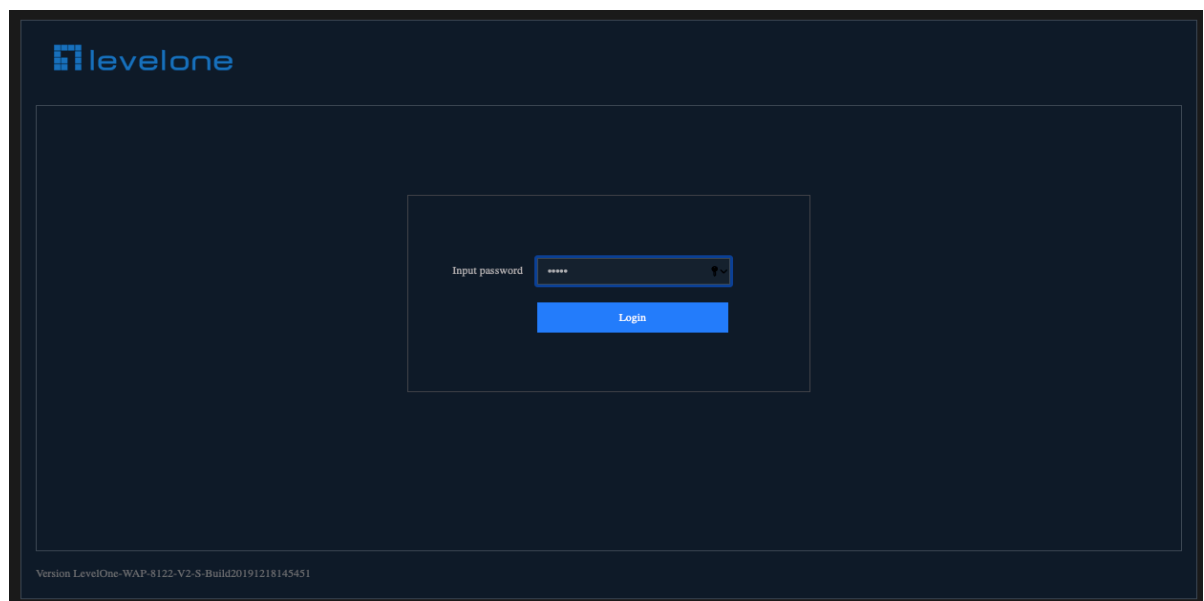


Sign out of the settings screen

1. When you confirm that all settings are completed, it is recommended to click the logout button to exit the setting page

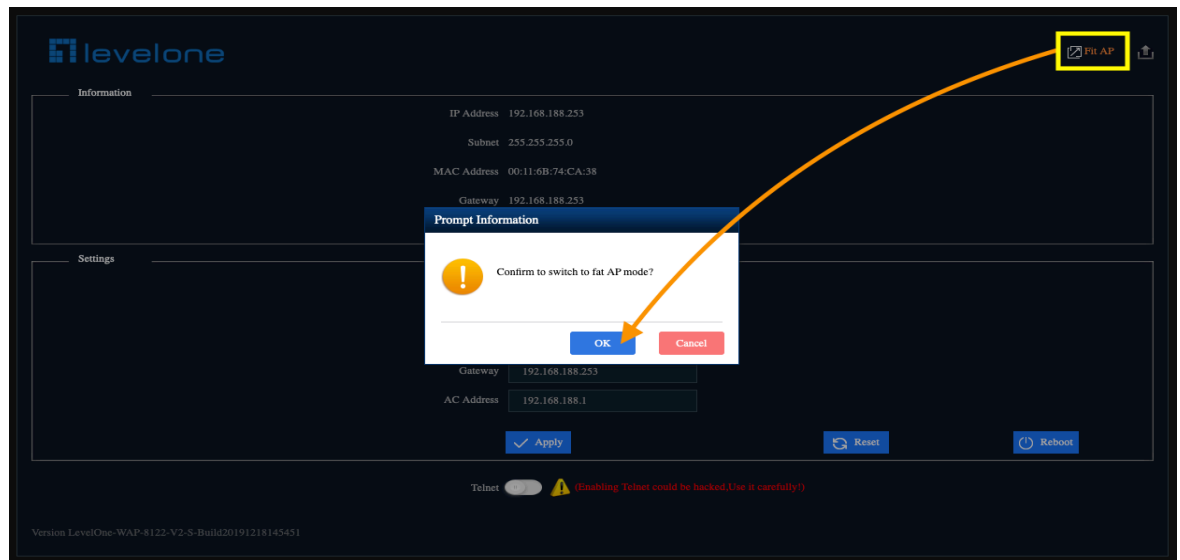


2. After returning to the login device screen, click to close the page

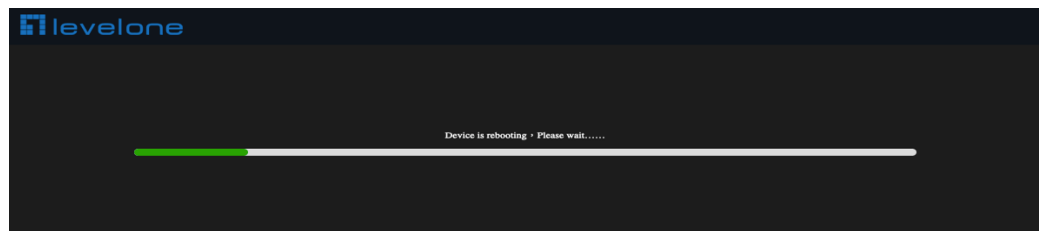


Fat AP (Mode switching instructions)

1.Fat AP Mode can operate independently, and can also be used multiple AP management for WAC-2000/WAC-2003, the following is a demonstration of switching to Fat AP mode



2.Please wait more than 40 seconds



3.Confirm switch back to the login screen of Fat AP mode



Section II Wizard

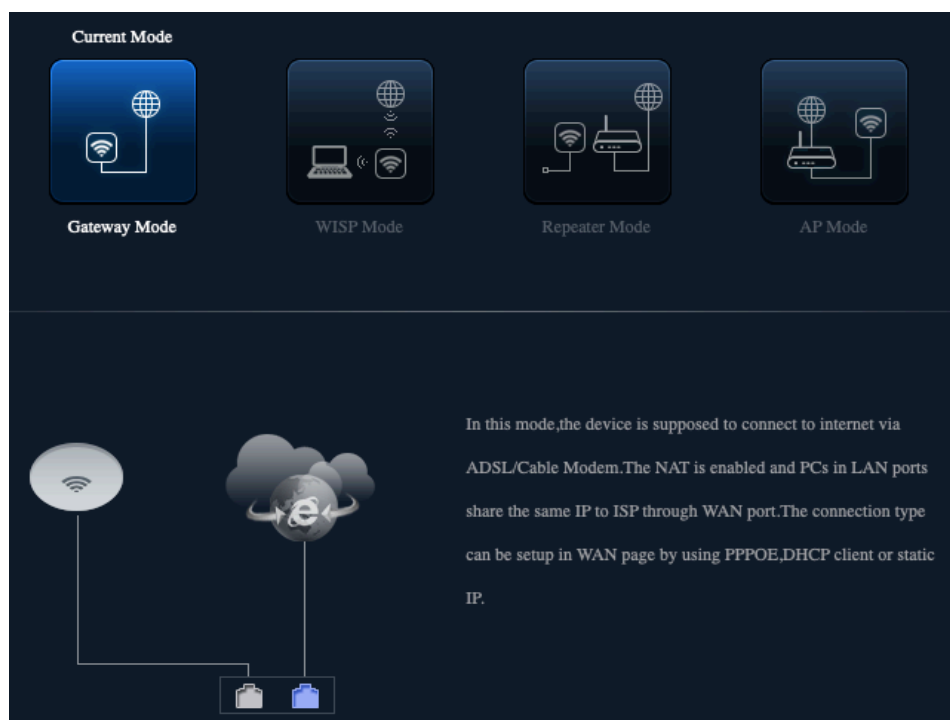
Click Wizard in Status page, will pop up following page to configure the operation mode and there are explanation for each operation mode for better application. It instruct users to configure wireless AP's operation mode based on needs: there are four operation mode including gateway, repeater, WISP, Wireless AP. Please confirm the operation mode first before configuration starting.



Gateway Mode

Before Click Gateway mode, confirm your internet will be static IP, PPPoE, or DHCP :

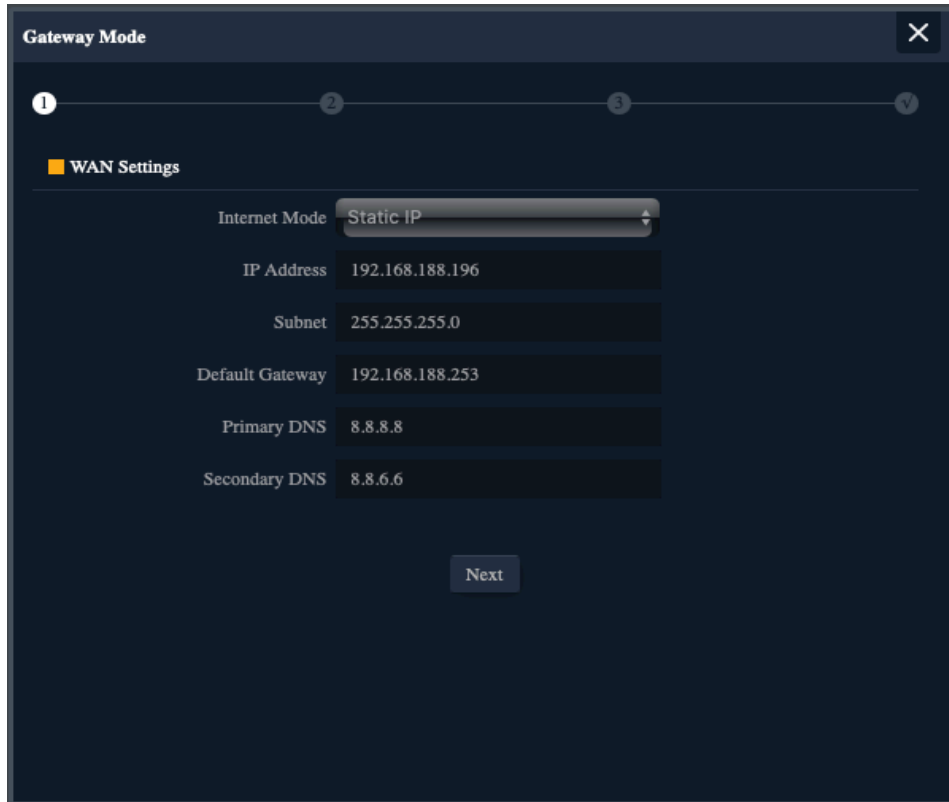
Then will pop up following picture after click it, Please choose the right WAN setting mode, then click next to continue



Static IP setting in Gateway Mode :

1. Sample Static IP mode setting method, then click next to continue.

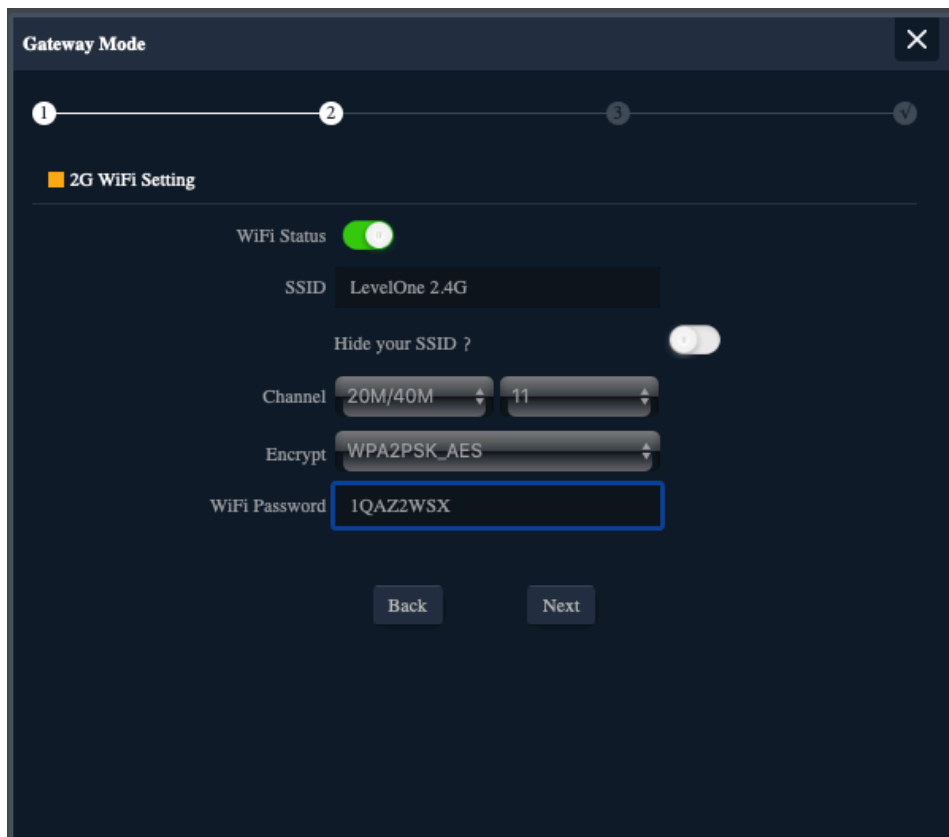
(Please contact with ISP for correct IP address and DNS address)



The screenshot shows the 'Gateway Mode' window with a progress bar at the top indicating four steps. Step 1 is active. Below the progress bar, the 'WAN Settings' section is highlighted. The 'Internet Mode' is set to 'Static IP'. The following fields are filled: 'IP Address' (192.168.188.196), 'Subnet' (255.255.255.0), 'Default Gateway' (192.168.188.253), 'Primary DNS' (8.8.8.8), and 'Secondary DNS' (8.8.6.6). A 'Next' button is located at the bottom right.

Field	Value
Internet Mode	Static IP
IP Address	192.168.188.196
Subnet	255.255.255.0
Default Gateway	192.168.188.253
Primary DNS	8.8.8.8
Secondary DNS	8.8.6.6

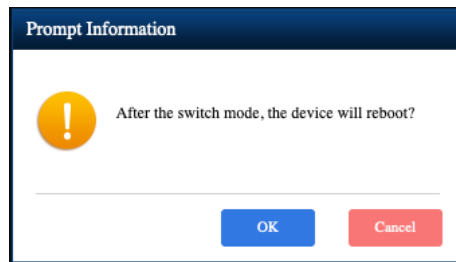
2. Wireless Setting in Gateway Mode (static IP) , Click Next



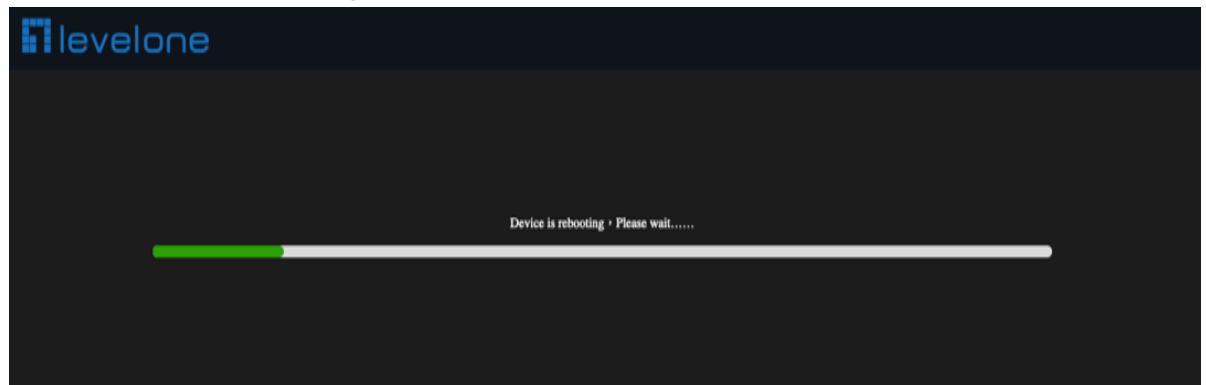
The screenshot shows the 'Gateway Mode' window with the progress bar indicating Step 2 is active. The '2G WiFi Setting' section is highlighted. The 'WiFi Status' is turned on. The 'SSID' is 'LevelOne 2.4G'. The 'Hide your SSID ?' toggle is off. The 'Channel' is set to '20M/40M' and '11'. The 'Encrypt' is set to 'WPA2PSK_AES'. The 'WiFi Password' is '1QAZ2WSX'. 'Back' and 'Next' buttons are at the bottom.

Field	Value
WiFi Status	On
SSID	LevelOne 2.4G
Hide your SSID ?	Off
Channel	20M/40M, 11
Encrypt	WPA2PSK_AES
WiFi Password	1QAZ2WSX

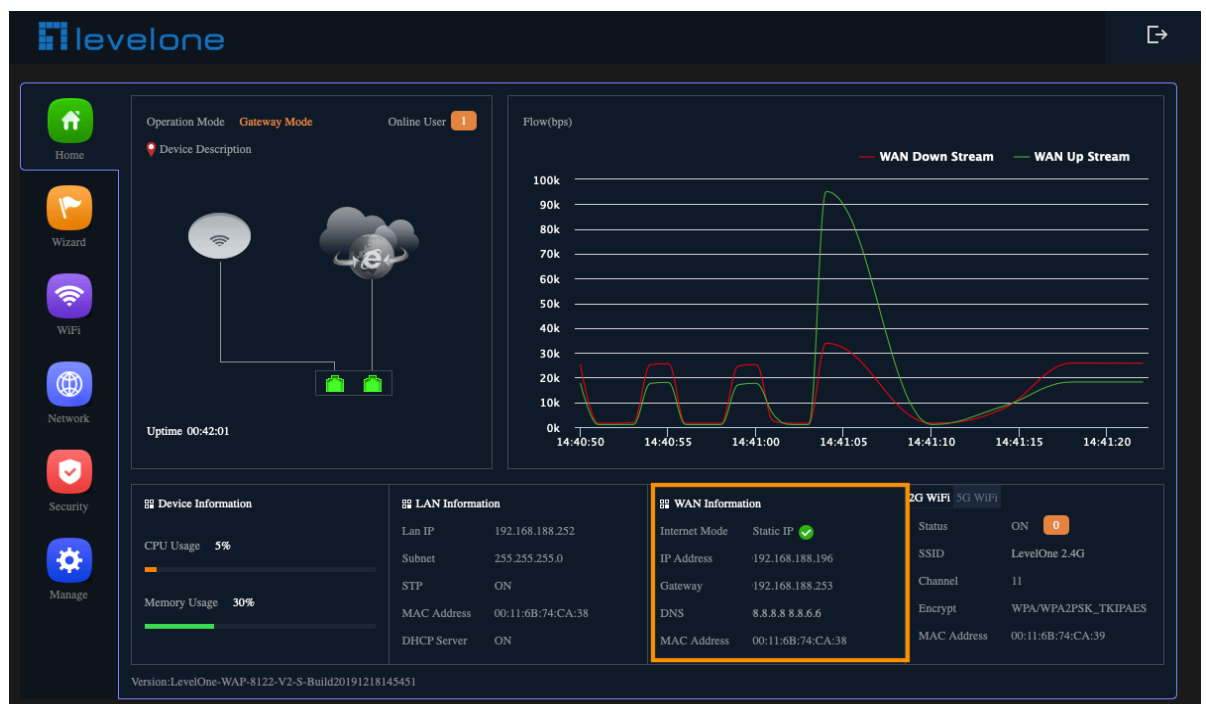
3. Please click the ok button, After the switch mode, the device will reboot



4. Please wait for the configuration to finish



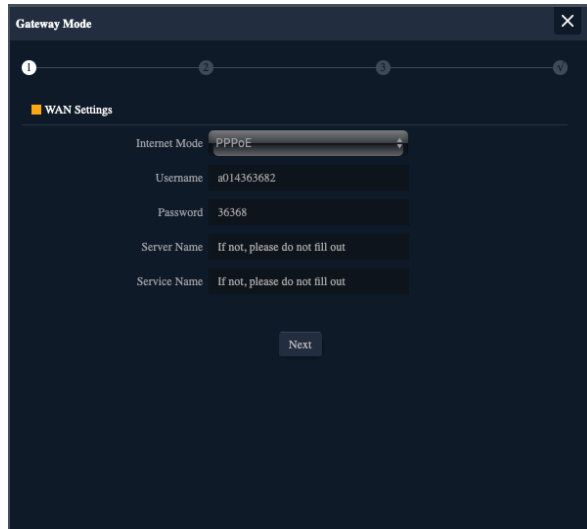
5. Please log in again ,This page will show the connection Static IP status



PPPoE(ADSL, VDSL) setting in Gateway Mode :

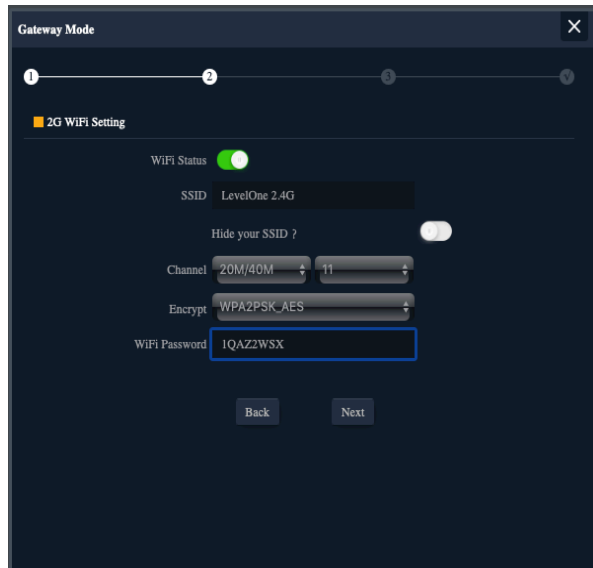
1.Sample PPPoE mode setting method, then click next to continue.

(Please contact with ISP for correct PPPoE Name and Password)



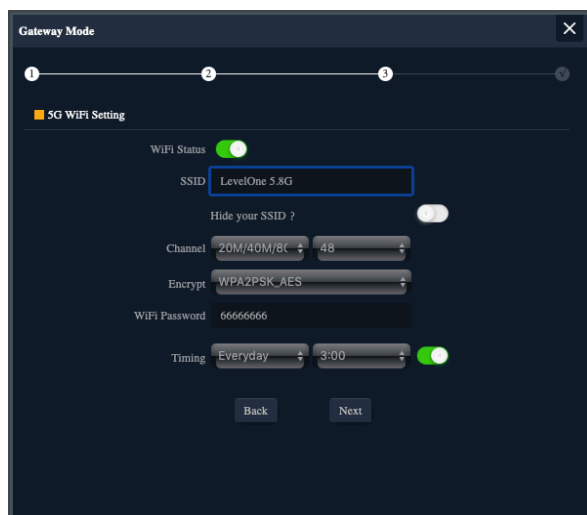
The screenshot shows the 'Gateway Mode' window with a progress bar at the top indicating four steps. Step 1 is active, showing 'WAN Settings'. The 'Internet Mode' is set to 'PPPoE'. The 'Username' field contains 'a014363682' and the 'Password' field contains '36368'. The 'Server Name' and 'Service Name' fields both have the placeholder text 'If not, please do not fill out'. A 'Next' button is located at the bottom center.

2.Wireless 2.4GHz Setting in Gateway Mode (PPPoE), Click Next



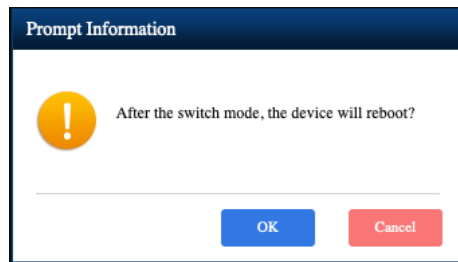
The screenshot shows the 'Gateway Mode' window with the progress bar at step 2, '2G WiFi Setting'. The 'WiFi Status' is turned on. The 'SSID' is 'LevelOne 2.4G'. The 'Hide your SSID ?' toggle is off. The 'Channel' is set to '20M/40M' and '11'. The 'Encrypt' is set to 'WPA2PSK_AES'. The 'WiFi Password' is '1QA2ZWSX'. 'Back' and 'Next' buttons are at the bottom.

3.Wireless 5GHz Setting in Gateway Mode (PPPoE), Click Next

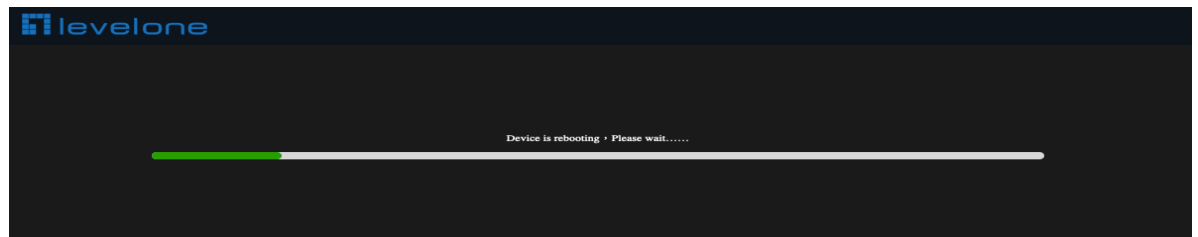


The screenshot shows the 'Gateway Mode' window with the progress bar at step 3, '5G WiFi Setting'. The 'WiFi Status' is turned on. The 'SSID' is 'LevelOne 5.8G'. The 'Hide your SSID ?' toggle is off. The 'Channel' is set to '20M/40M/8C' and '48'. The 'Encrypt' is set to 'WPA2PSK_AES'. The 'WiFi Password' is '66666666'. The 'Timing' is set to 'Everyday' and '3:00', with a toggle switch turned on. 'Back' and 'Next' buttons are at the bottom.

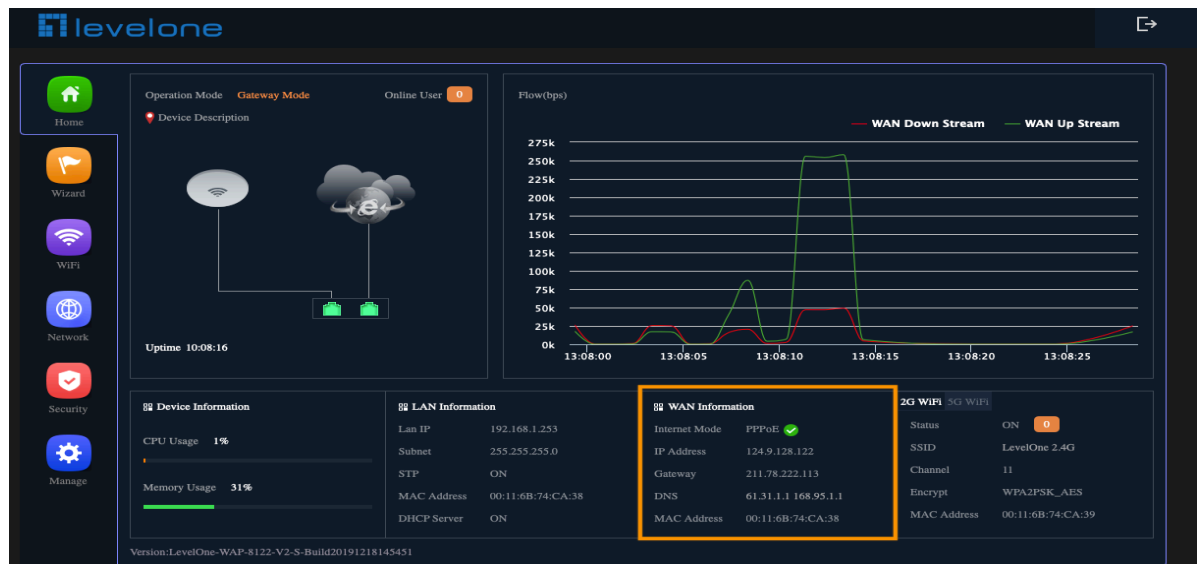
4. Please click the ok button, After the switch mode, the device will reboot



5. Please wait for the configuration to finish

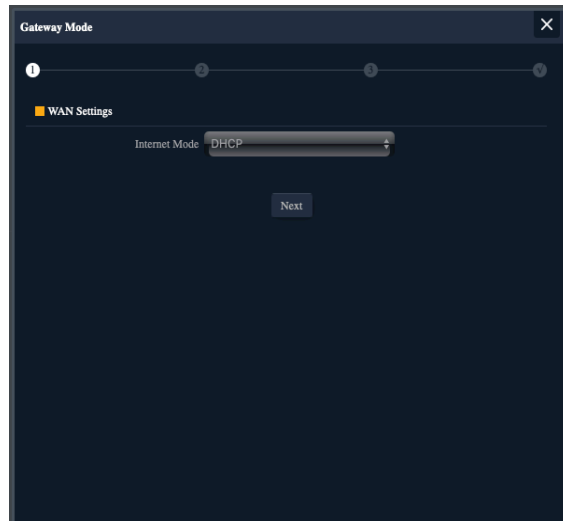


6. Please log in again ,This page will show the connection PPPoE status

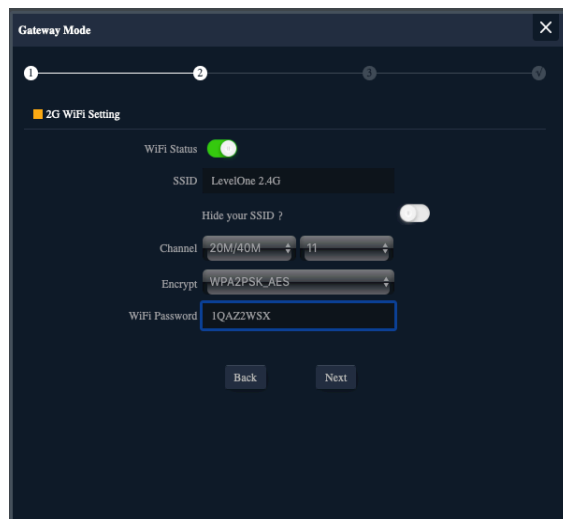


DHCP Setting in Gateway Mode

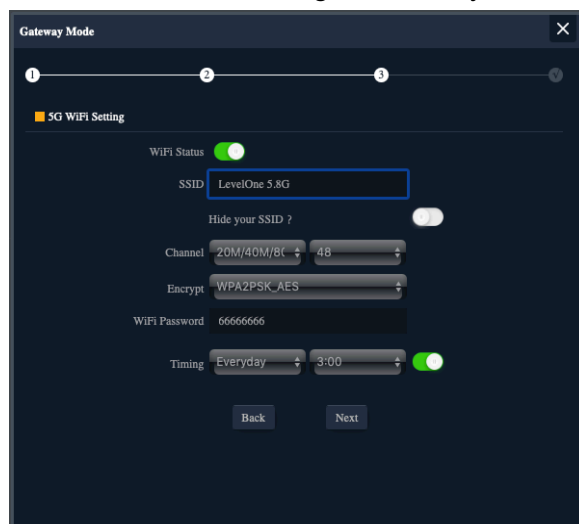
1. Sample DHCP mode setting method, then click next to continue.
(Please contact with ISP for correct IP address and DNS address)



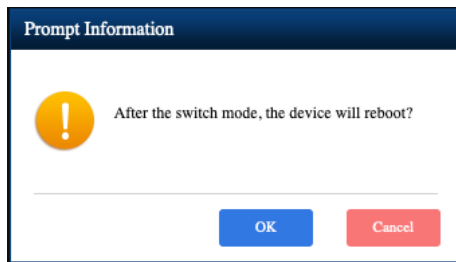
2. Wireless 2.4GHz Setting in Gateway Mode (DHCP), Click Next



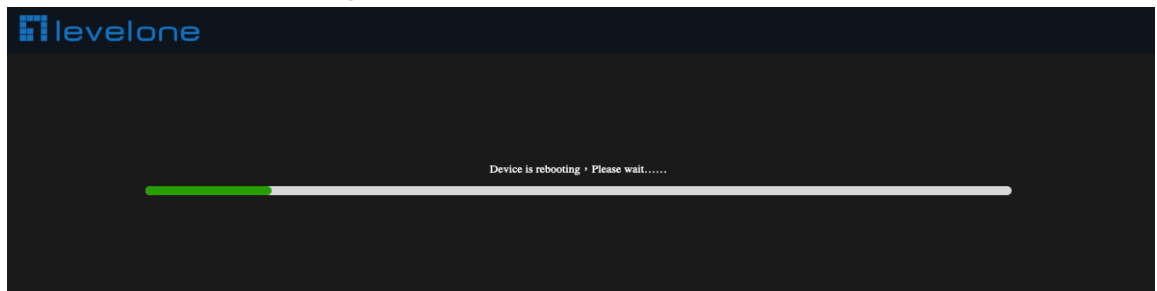
3. Wireless 5GHz Setting in Gateway Mode (DHCP), Click Next



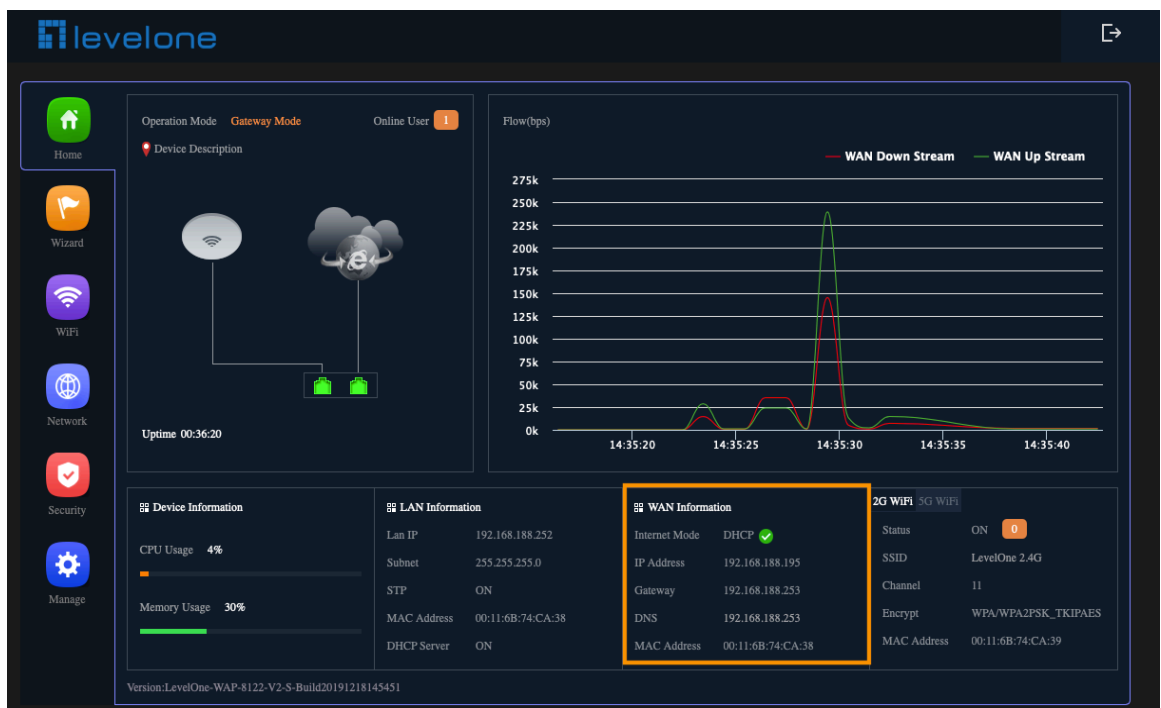
4. Please click the OK button, After the switch mode, the device will reboot



5. Please wait for the configuration to finish

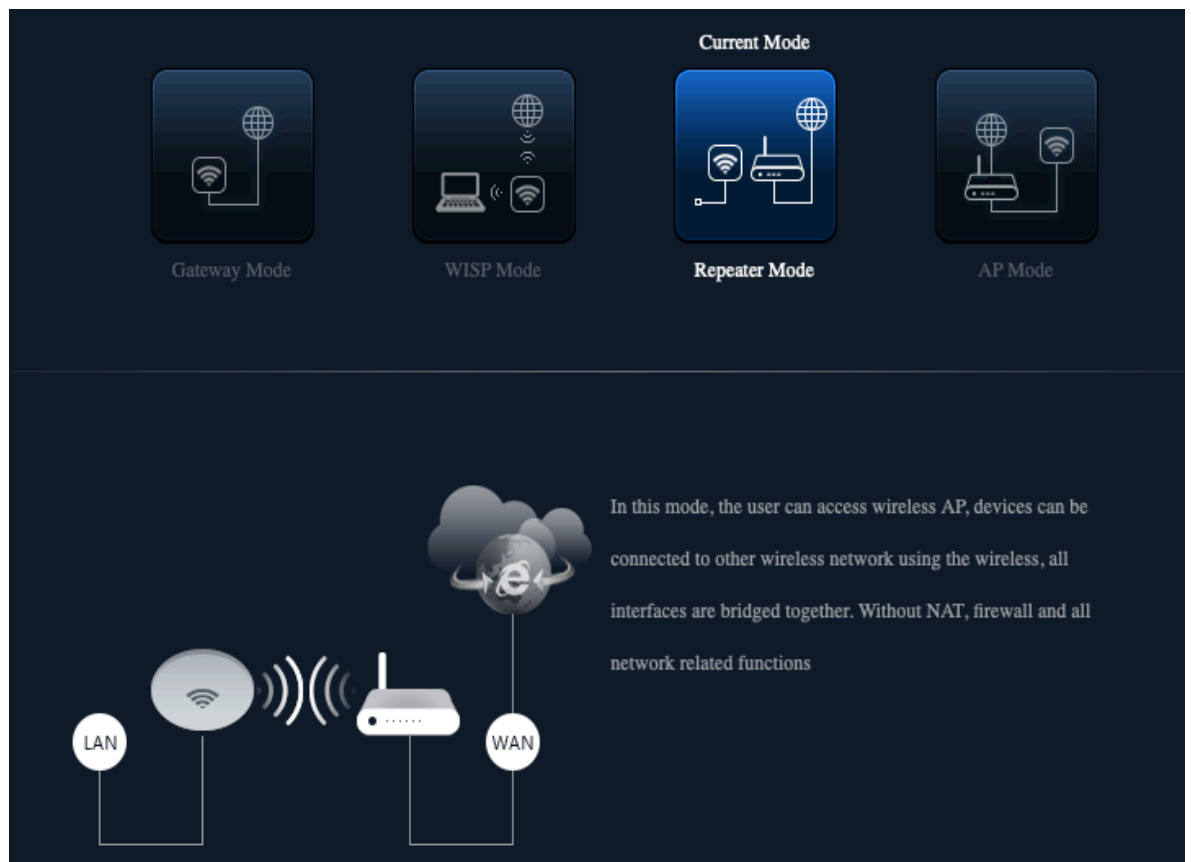


6. Please log in again ,This page will show the connection DHCP status



Repeater mode

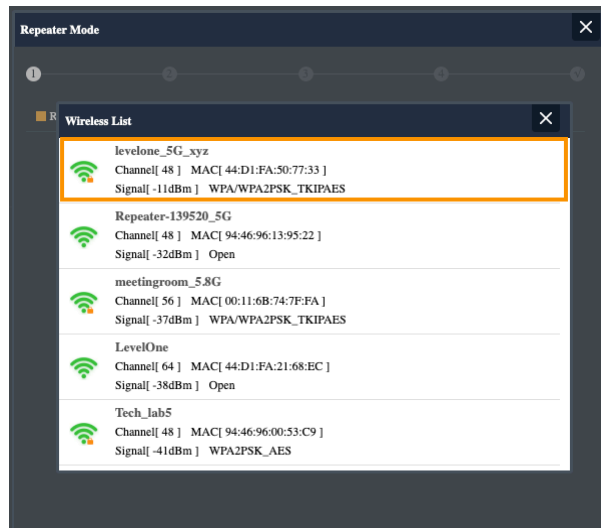
In this mode, the user can access wireless AP, devices can be connected to other wireless network using the wireless, all interfaces are bridged together. Without NAT, firewall and all network related functions



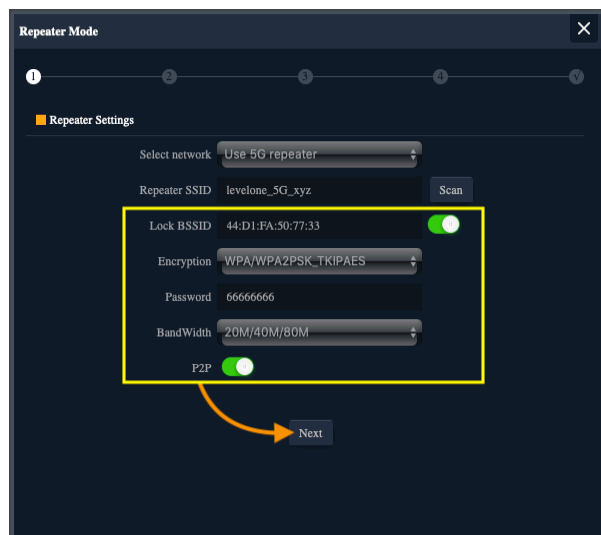
1.Can choose to relay the front-end 2.4G or 5G wireless signal to extend the wireless signal range. Select the AP's SSID want to bridge, take "wireless 5G" for example, then input the AP's key, click Scan AP

The screenshot shows the 'Repeater Mode' configuration window. It has a progress bar at the top with steps 1 through 5. Step 1 is 'Repeater Settings'. The 'Select network' dropdown is set to 'Use 5G repeater'. The 'Repeater SSID' is 'Wireless5.8G'. The 'Lock BSSID' toggle is off. The 'Encryption' is 'WPA/WPA2PSK_TKIPAES'. The 'Password' field is empty. The 'BandWidth' is '20M/40M/80M'. The 'P2P' toggle is off. A 'Scan' button is next to the SSID field. A 'Next' button is at the bottom.

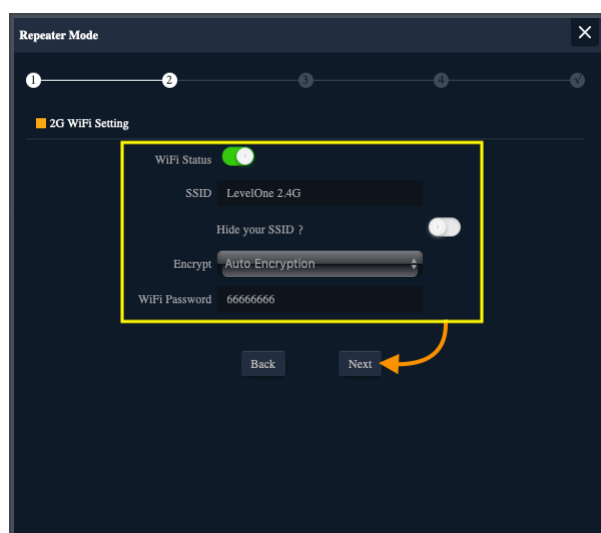
2. Please select WIFI SSID to connect



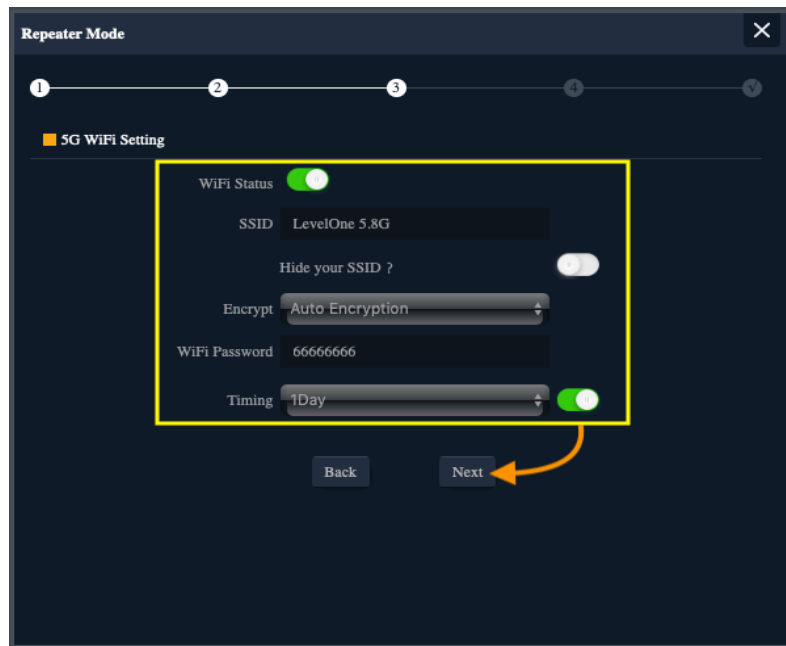
3. Enter the WIFI SSID password to be linked, When click Next.



4. If choose to relay the front-end 5G wireless signal to extend the wireless signal range. Can choose to enable or disable the 2.4G wireless broadcast of the itself.

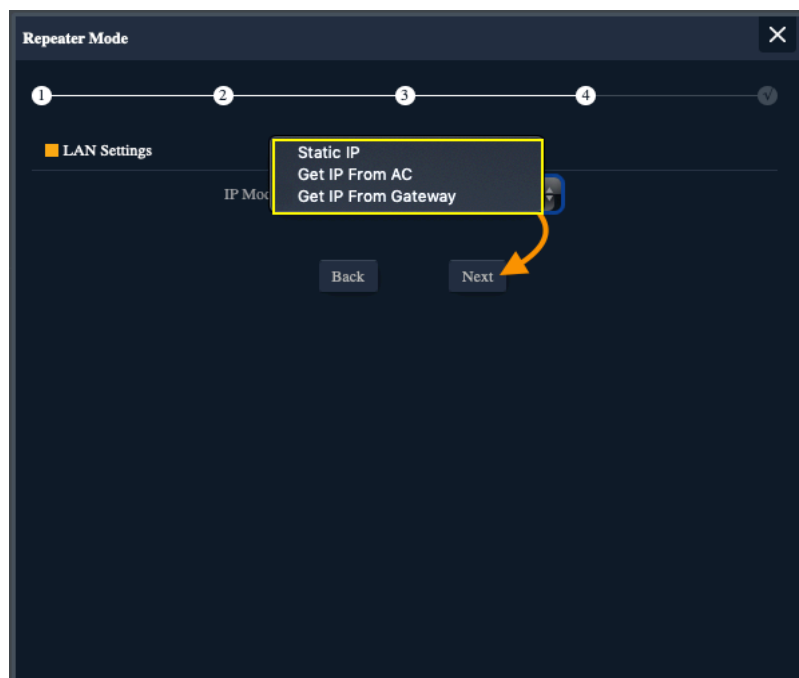


5. Can choose to enable or disable the 5G wireless broadcast of the itself.

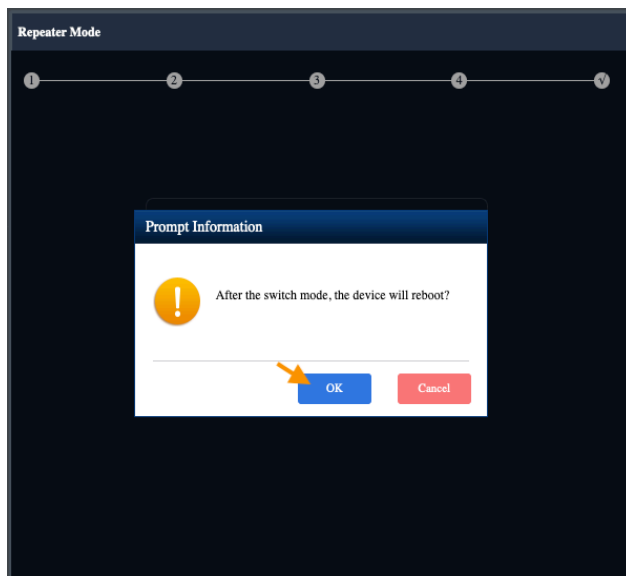


6. Set up the LAN according to the front-end relay 2.4 / 5G wireless signal :

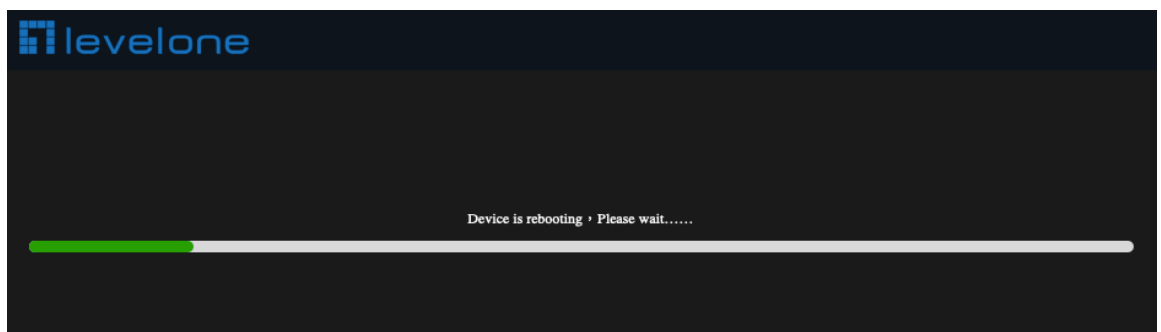
- a) If the front-end wireless signal is Static IP, you can click "Static IP" to set an unused IP address.
- b) If the front-end wireless signal is automatically assigned by the wireless controller WAC-2000 / WAC-2003, you can click "Get IP From AC"
- c) If the gateway of the front-end wireless signal will automatically assign an IP address, you can click "Get IP From Gateway"



7. Please click the ok button, After the switch mode, the device will reboot



8. Please wait more than 20 seconds



9. Please log in again ,This page will show the connection Repeater mode status

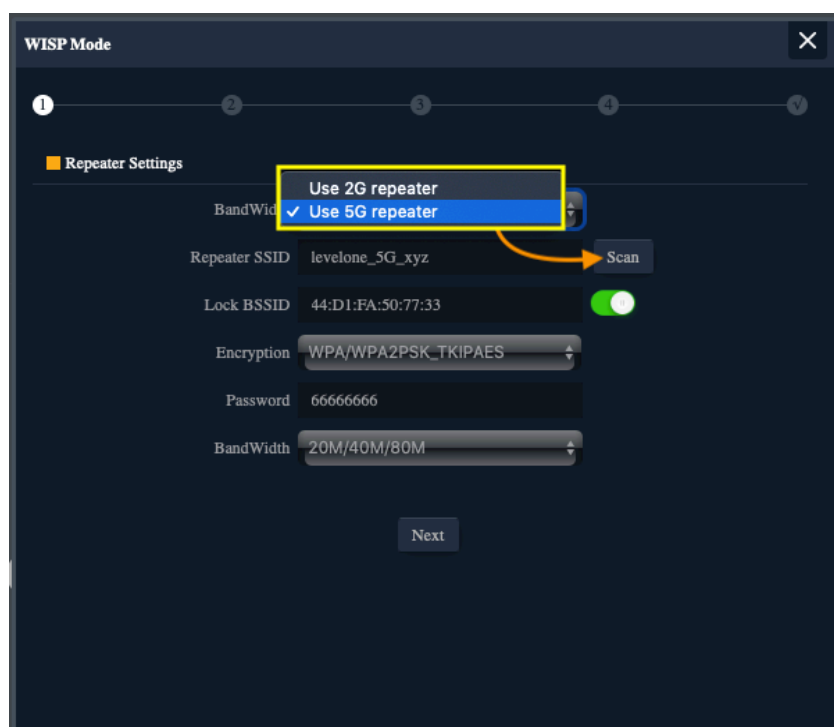


WISP Mode

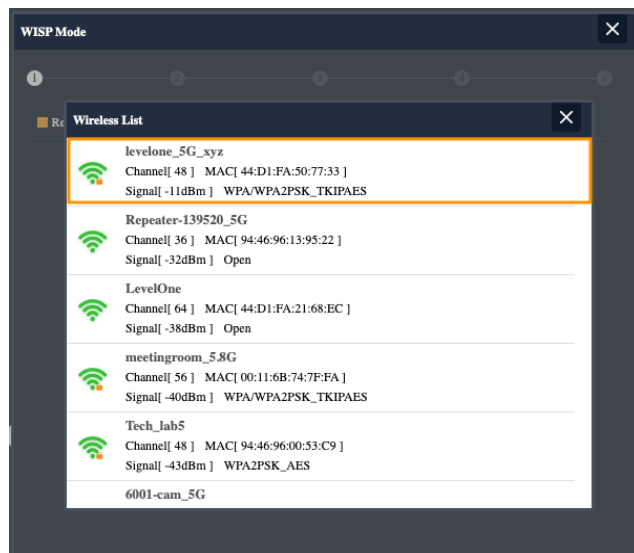
In this mode, all ethernet ports are bridged together and wireless client will connect ISP access point. The NAT is enabled and PCs in ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client and static IP.



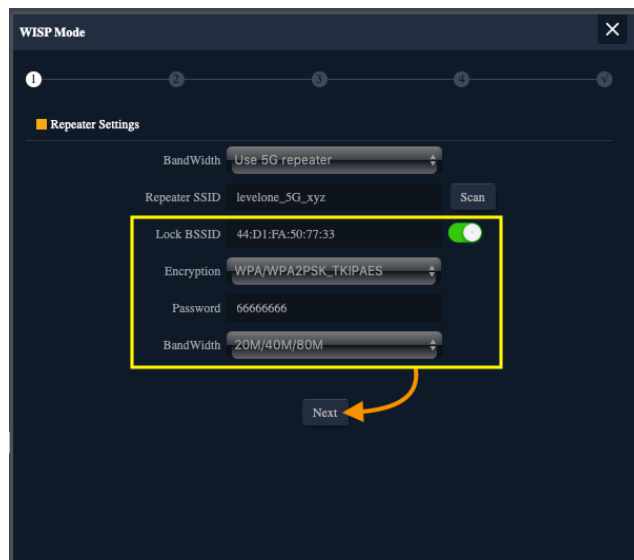
1. Choose to relay the front-end 2.4/5G wireless signal to wireless client will connect ISP access point.



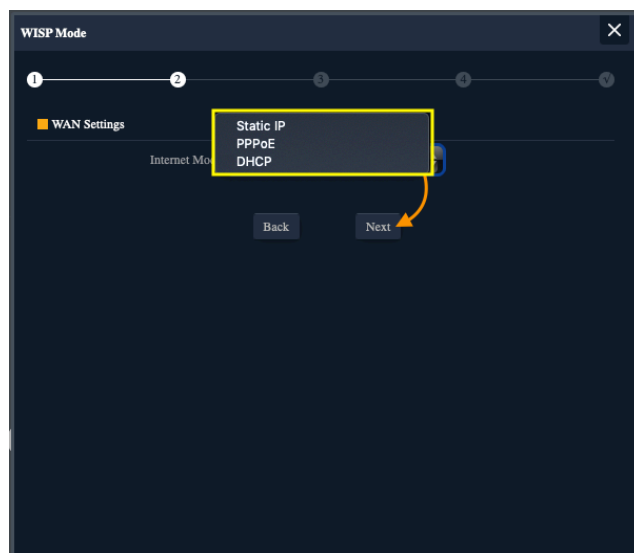
2. Please Select ISP Wireless SSID to Connect.



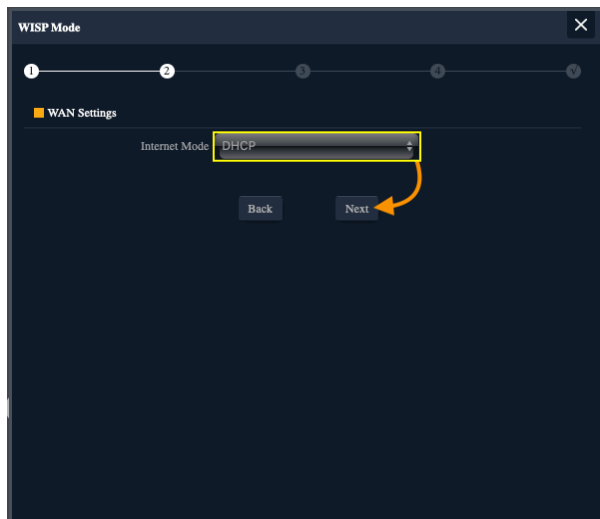
3. Please Key in ISP Wireless Password to Connect.



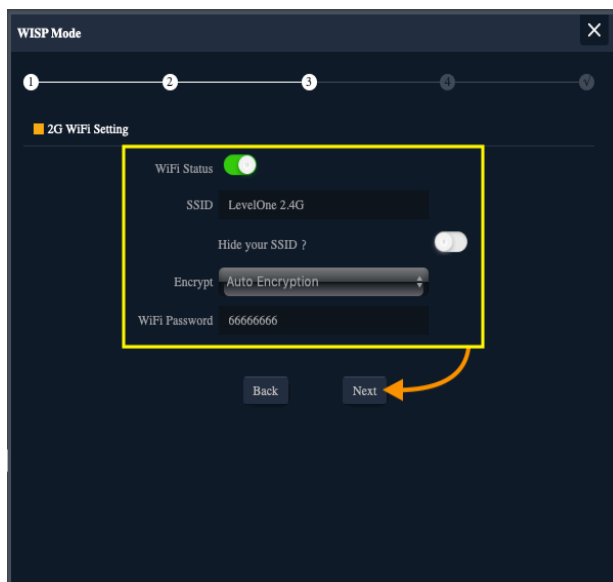
4. Please choose the ISP right WAN setting mode, then click next to continue.



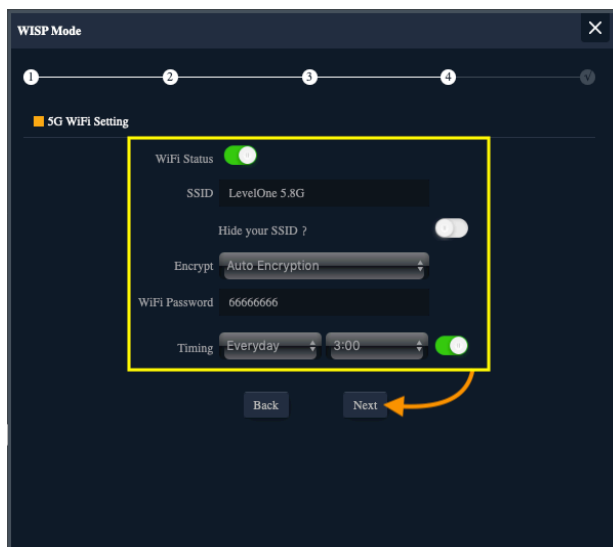
5. Take **DHCP** for example



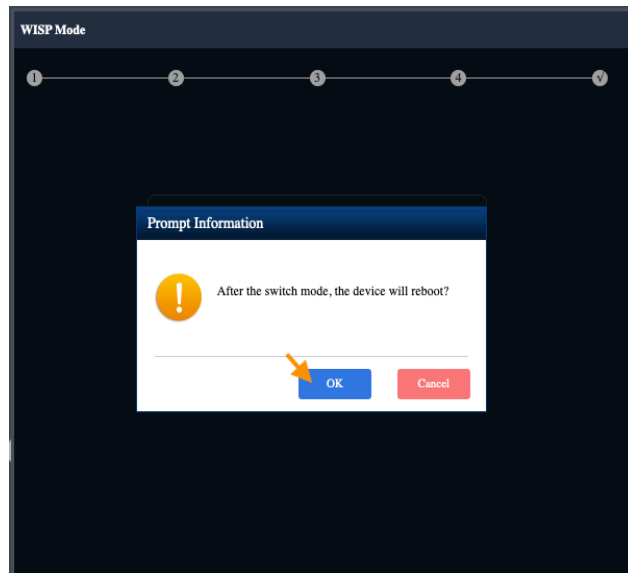
6. Configure the 2.4G Wireless SSID and password



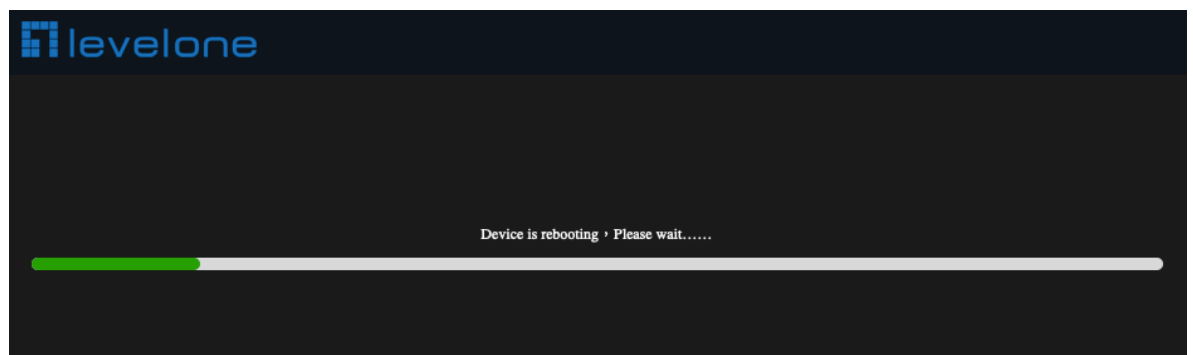
7. Configure the 5G Wireless SSID and password



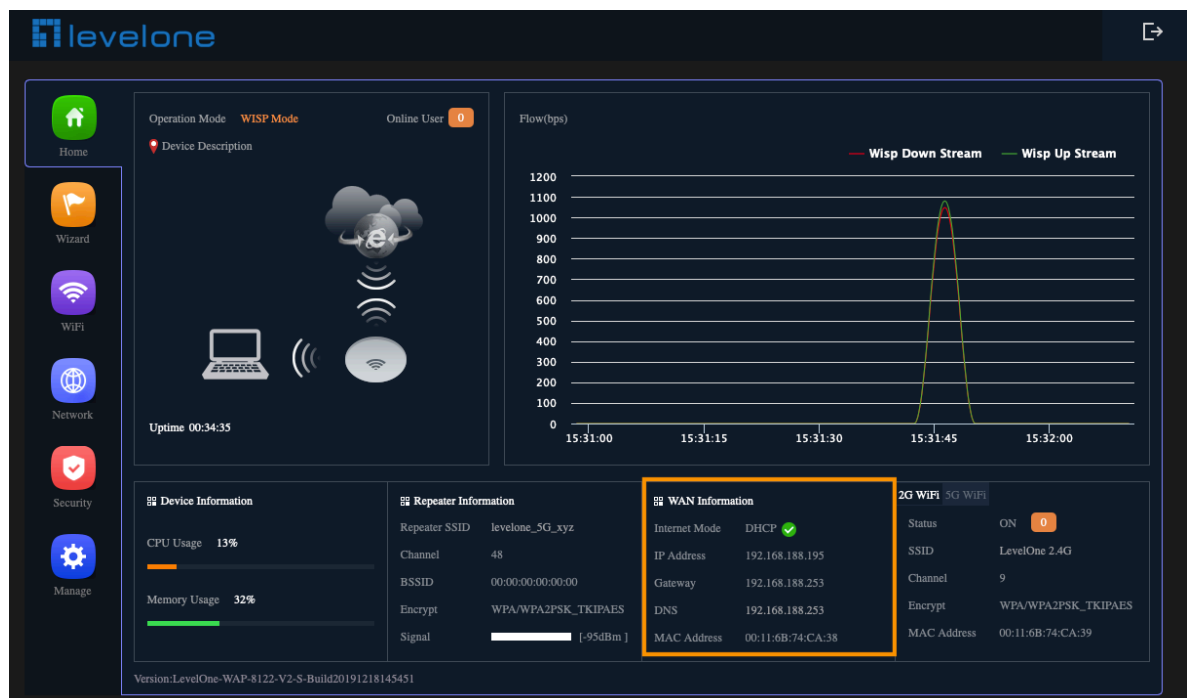
8. Please click the ok button, After the switch mode, the device will reboot



9. Please wait more than 20 seconds



10. Please log in again ,This page will show the connection WISP mode status



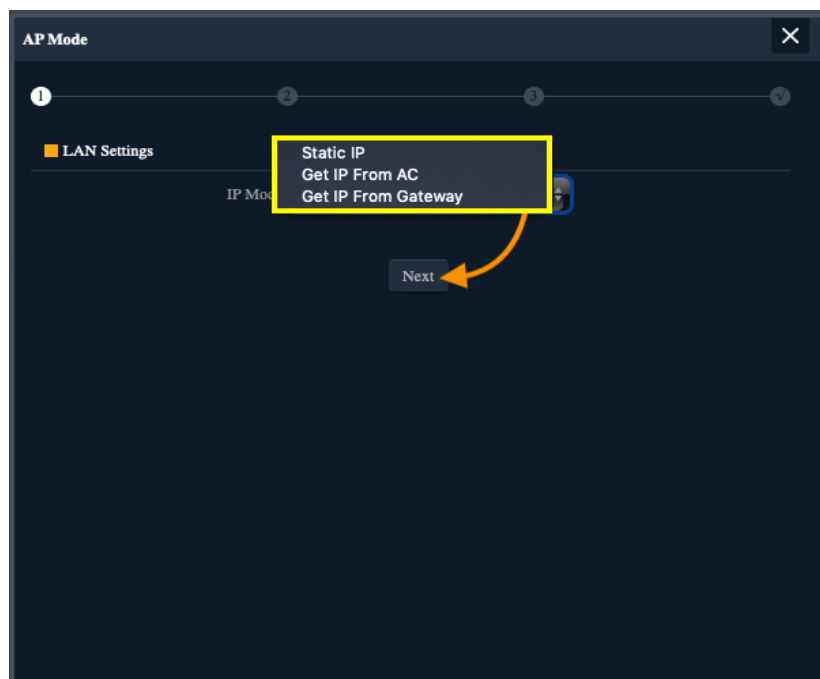
AP Mode

In this mode, the AP wireless interface and cable interface are bridging together. Without NAT, firewall and all network related functions.



1.Set according to LAN environmental requirements :

- If the front-end is Static IP, you can click "Static IP" to set an unused IP address.
- If the front-end is automatically assigned by the wireless controller WAC-2000 / WAC-2003, you can click "Get IP From AC"
- If the gateway of the front-end will automatically assign an IP address, you can click "Get IP From Gateway"



2.Static IP setting

The screenshot shows the 'AP Mode' configuration window with a progress bar at the top indicating step 1 of 4. The 'LAN Settings' section is highlighted with a yellow box. Inside the box, the following settings are visible: IP Mode is set to 'Static IP'; Lan IP is '192.168.188.250'; Subnet is '255.255.255.0'; Gateway is '192.168.188.253'; Primary DNS is '8.8.8.8'; and Secondary DNS is '8.8.4.4'. A 'Next' button is located below the settings, with an orange arrow pointing to it from the right side of the yellow box.

AP Mode

1 2 3 4

LAN Settings

IP Mode Static IP

Lan IP 192.168.188.250

Subnet 255.255.255.0

Gateway 192.168.188.253

Primary DNS 8.8.8.8

Secondary DNS 8.8.4.4

Next

3. Configure the 2.4G Wireless SSID and password

The screenshot shows the 'AP Mode' configuration window with a progress bar at the top indicating step 2 of 4. The '2G WiFi Setting' section is highlighted with a yellow box. Inside the box, the following settings are visible: WiFi Status is turned on; SSID is 'LevelOne 2.4G'; 'Hide your SSID?' is turned off; Channel is '20M/40M' with a value of '9'; Encrypt is 'Auto Encryption'; and WiFi Password is '66666666'. 'Back' and 'Next' buttons are at the bottom, with an orange arrow pointing to the 'Next' button from the right side of the yellow box.

AP Mode

1 2 3 4

2G WiFi Setting

WiFi Status ☒

SSID LevelOne 2.4G

Hide your SSID ? ☐

Channel 20M/40M 9

Encrypt Auto Encryption

WiFi Password 66666666

Back Next

4.Configure the 5G Wireless SSID and password

The screenshot shows the 'AP Mode' configuration window with a progress bar at the top indicating step 3 of 4. The '5G WiFi Setting' section is highlighted with a yellow box. Inside the box, the following settings are visible: WiFi Status is turned on; SSID is 'LevelOne 5.8G'; 'Hide your SSID?' is turned off; Channel is '20M/40M/80' with a value of '48'; Encrypt is 'Auto Encryption'; WiFi Password is '66666666'; and Timing is '1Day' with a toggle switch turned on. 'Back' and 'Next' buttons are at the bottom, with an orange arrow pointing to the 'Next' button from the right side of the yellow box.

AP Mode

1 2 3 4

5G WiFi Setting

WiFi Status ☒

SSID LevelOne 5.8G

Hide your SSID ? ☐

Channel 20M/40M/80 48

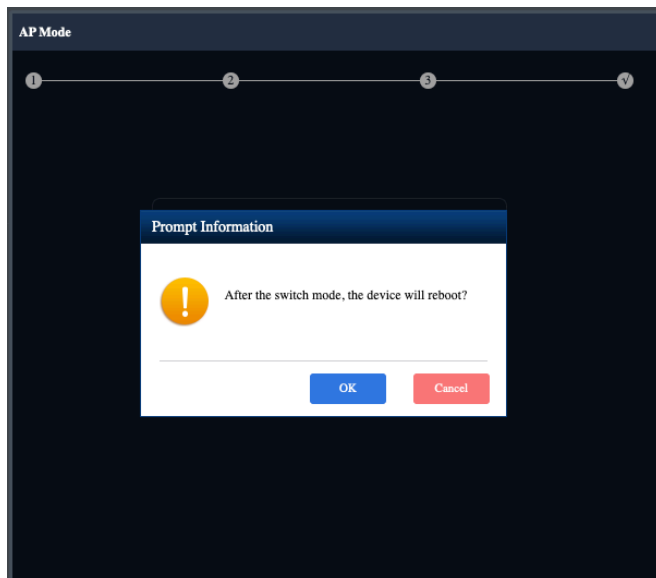
Encrypt Auto Encryption

WiFi Password 66666666

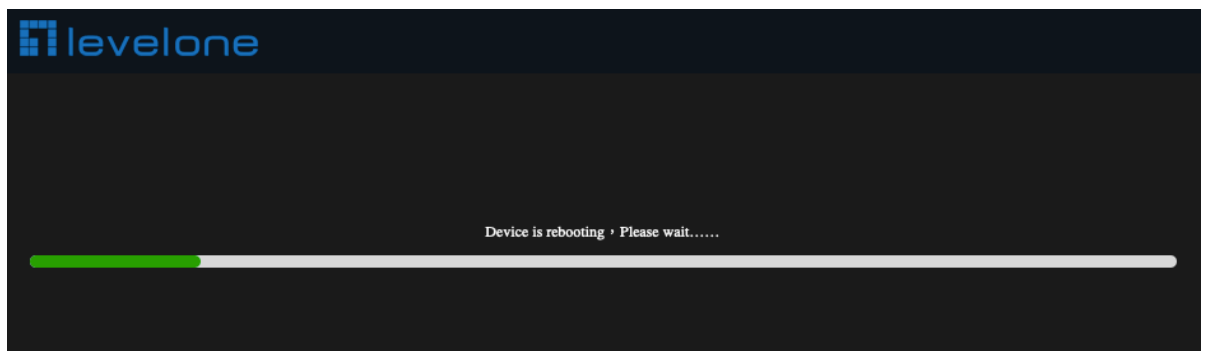
Timing 1Day ☒

Back Next

5. Please click the ok button, After the switch mode, the device will reboot



6. Please wait more than 20 seconds



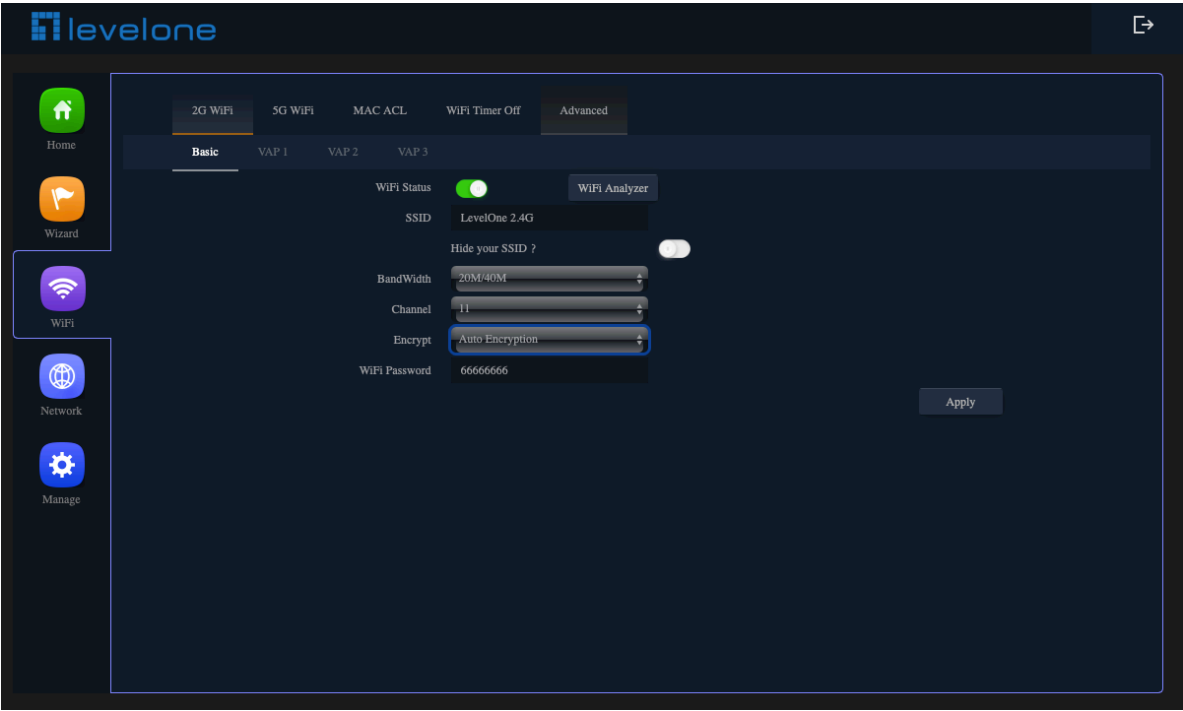
7. Check AP Mode Status



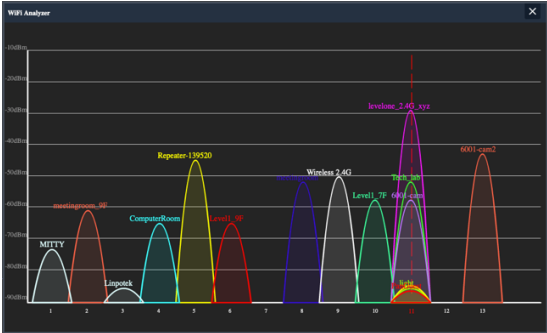


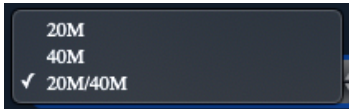
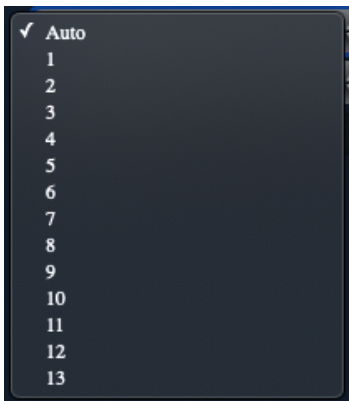
Section III WiFi

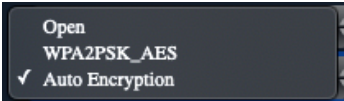
Basic (2G WiFi)

Select the types of 2.4GHz wireless security you want to setup:



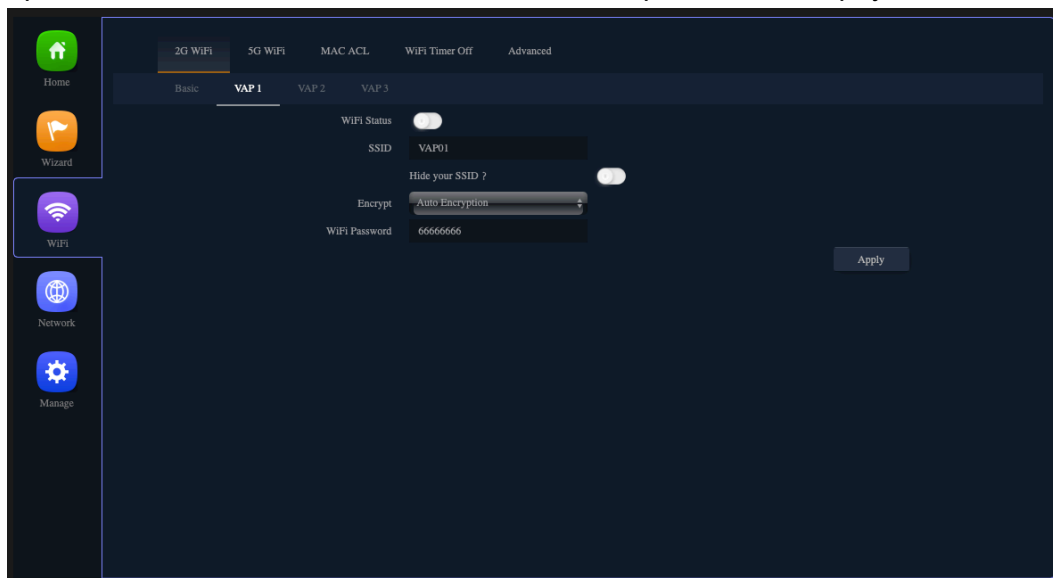
Basic Features Description	
WiFi Status	2.4GHz WiFi on / off
	<div><div>WiFi Status </div><div>WiFi Status </div></div>
WiFi Status	WiFi Analyzer :
	Wireless analyzer Look for Unoccupied channel (2.4GHz) 

SSID	Custom 2.4GHz WiFi Name
Hide your SSID?	<p>Public SSID : Anyone in this area can find SSID</p> <p>Hidden SSID : Everyone in this area cannot search for the SSID. You can only connect successfully by manually entering the correct SSID and password.</p>
BandWidth	<p>The 802.11n specification allows a 40 MHz wide channel in addition to the legacy 20 MHz channel available with other modes, The 40 MHz channel enables higher data rates.</p> 
Channel	<p>Shows the Channel on which the AP is currently broadcasting. The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected.</p> <p>The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).</p> 
Encrypt	<p>Open : No encryption state, all wireless devices in the area can directly connect wirelessly. It is not recommended to use the unencrypted state directly, except for the wireless connection test under a short turn on</p>

	<p>WPA2PSK_AES :</p> <p>If all WiFi client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.</p> <p>Auto Encryption :</p> <p>If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select of the Auto Encryption. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more inter-operability, at the expense of some security.</p> 
WiFi Password	<p>The key can be a mix of alphanumeric and special characters, The key is case sensitive</p>

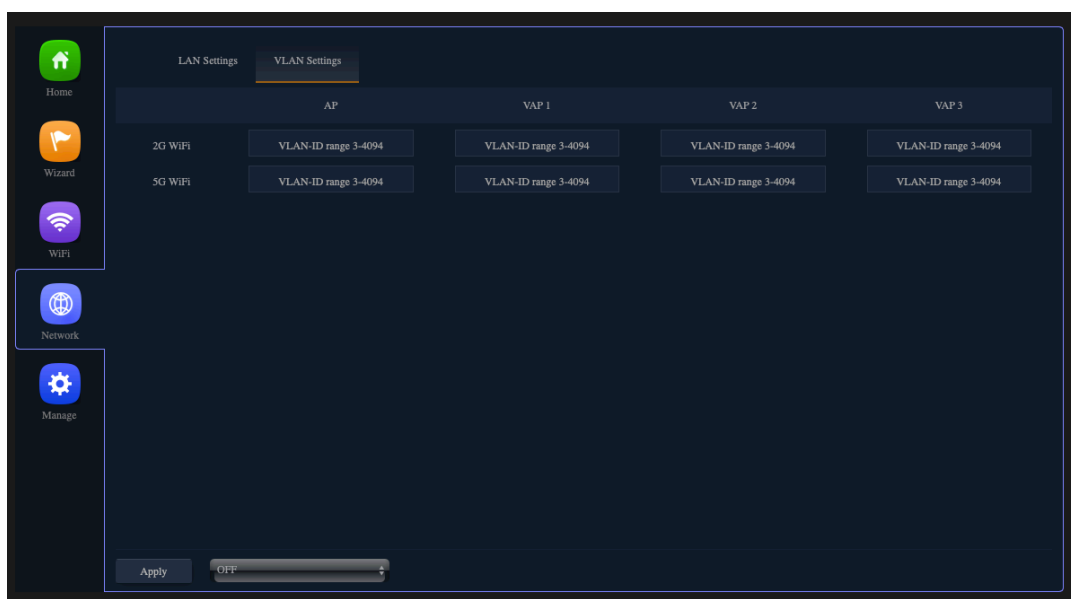
VAP1/ VAP2/ VAP3 (2G WiFi)

Not activated on the virtual access point by default, You configure secure wireless client access by configuring security for each virtual access point (VAP) that you enable. configure up to 3 VAPs on 2.4GHz radio that simulate multiple APs in one physical access point.



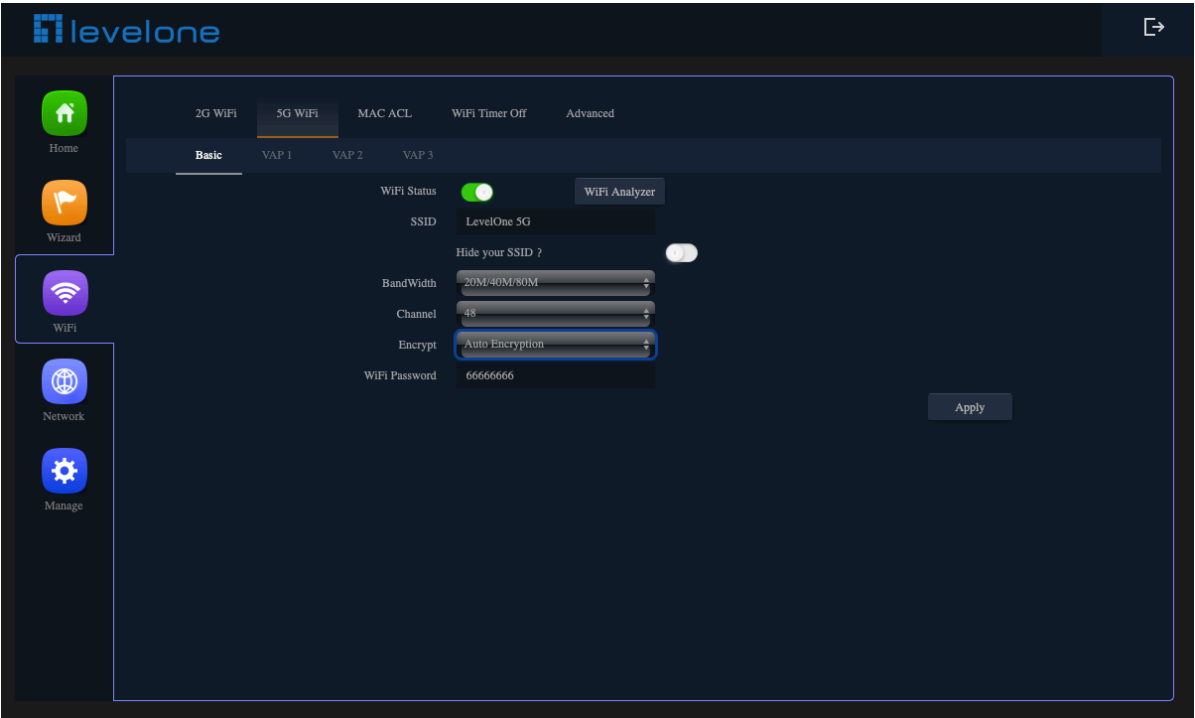
VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. For each VAP, you can customize the security mode to control wireless client access. Each VAP can also have a unique SSID. Multiple SSIDs make a single AP look like two or more APs to other systems on the network. By configuring VAPs, you can maintain better control over broadcast and multicast traffic, which affects network performance.

You can configure each VAP to use a different VLAN, or you can configure multiple VAPs to use the same VLAN, The AP adds VLAN ID tags to wireless client traffic based on the VLAN ID you configure on the **Network Option > VLAN Settings**.

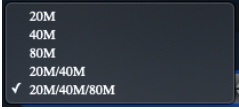
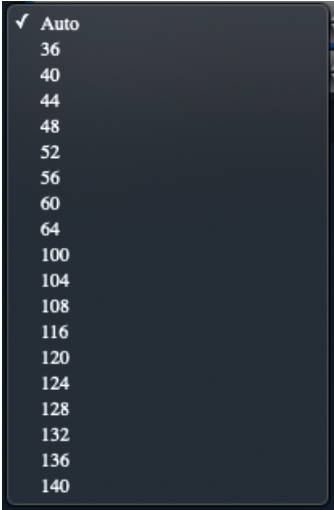


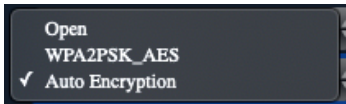
Basic (5G WiFi)

Select the types of 5GHz wireless security you want to setup:



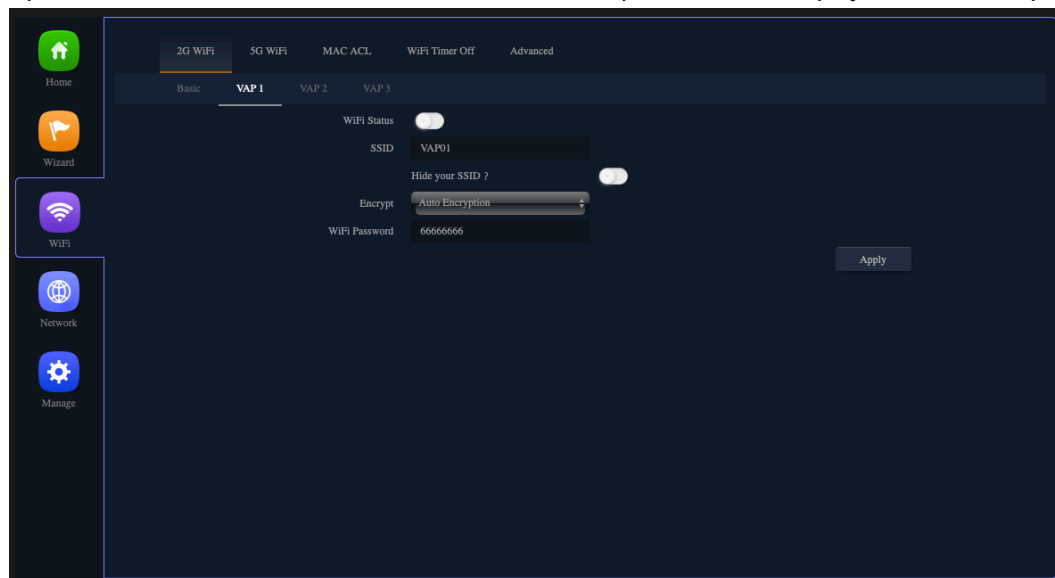
Basic Features Description	
WiFi Status	<div>5GHz WiFi on / off</div> <div><div>WiFi Status </div><div>WiFi Status </div></div> <div>WiFi Analyzer : Wireless analyzer Look for Unoccupied channel (5GHz)</div> <div></div>
SSID	Custom 5GHz WiFi Name
	Public SSID :

<p>Hide your SSID?</p>	<p>Anyone in this area can find SSID</p> <p>Hidden SSID :</p> <p>Everyone in this area cannot search for the SSID. You can only connect successfully by manually entering the correct SSID and password.</p>
<p>BandWidth</p>	<p>The 802.11n specification allows a 40 MHz wide channel in addition to the legacy 20 MHz channel available with other modes. The 40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 802.11ac specification allows an 80 MHz-wide channel in addition to the 20 MHz and 40 MHz channels.</p> 
<p>Channel</p>	<p>Shows the Channel on which the AP is currently broadcasting. The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected. The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).</p> 
<p>Encrypt</p>	<p>Open :</p> <p>No encryption state, all wireless devices in the area can directly connect wirelessly. It is not recommended to use the unencrypted state directly, except for the wireless connection test under a short</p>

	<p>turn on</p> <p>WPA2PSK_AES :</p> <p>If all WiFi client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.</p> <p>Auto Encryption :</p> <p>If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select of the Auto Encryption. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more inter-operability, at the expense of some security.</p> 
WiFi Password	<p>The key can be a mix of alphanumeric and special characters, The key is case sensitive</p>

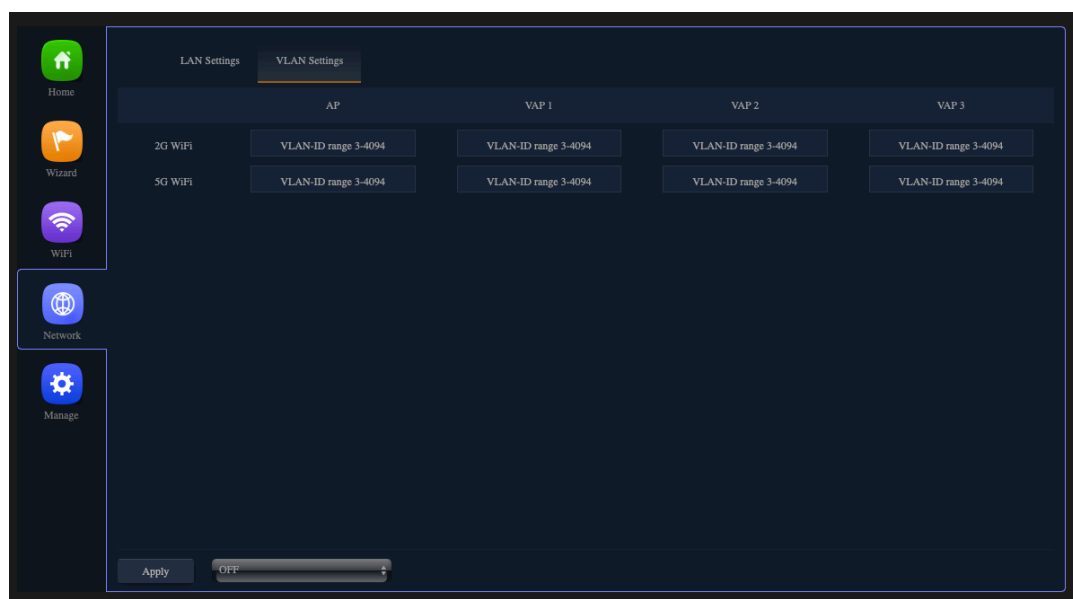
VAP1/ VAP2/ VAP3 (5G WiFi)

Not activated on the virtual access point by default, You configure secure wireless client access by configuring security for each virtual access point (VAP) that you enable. configure up to 3 VAPs on 5GHz radio that simulate multiple APs in one physical access point.



VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. For each VAP, you can customize the security mode to control wireless client access. Each VAP can also have a unique SSID. Multiple SSIDs make a single AP look like two or more APs to other systems on the network. By configuring VAPs, you can maintain better control over broadcast and multicast traffic, which affects network performance.

You can configure each VAP to use a different VLAN, or you can configure multiple VAPs to use the same VLAN, The AP adds VLAN ID tags to wireless client traffic based on the VLAN ID you configure on the **Network Option > VLAN Settings**.

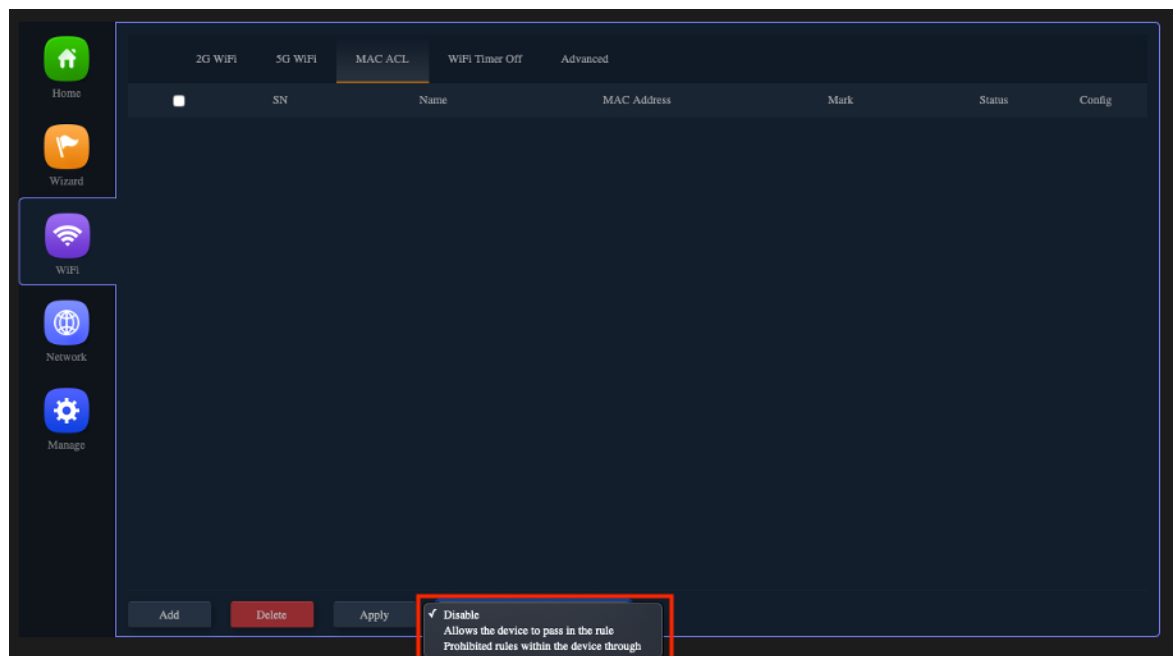


MAC ACL

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect fields of a frame such as the source or destination MAC address, the VLAN ID, or the Class of Service 802.1p priority. When a frame enters or exits the AP port (depending on whether the ACL is applied in the up or down direction), the AP inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

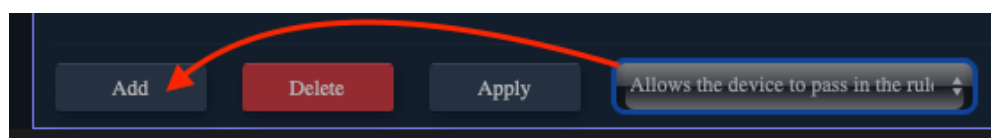
There are 3 types of MAC ACL rules, listed below

- 1) Disable
- 2) Allows the device to pass in the rule (**Whitelist** : Only the MAC ID devices in the list can connect normally)
- 3) Prohibited rules within the device through (**Blacklist** : Only the MAC ID devices in this list cannot connect normally)

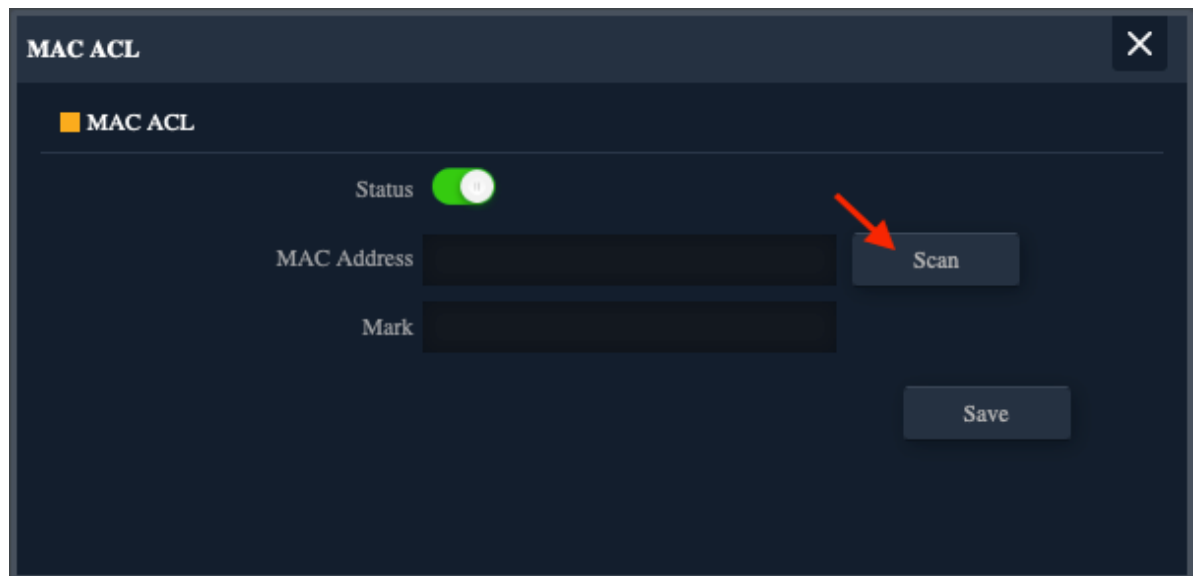


The following will demonstrate the "Allows the device to pass in the rule" setting

Click "Allows the device to pass in the rule" >> Add

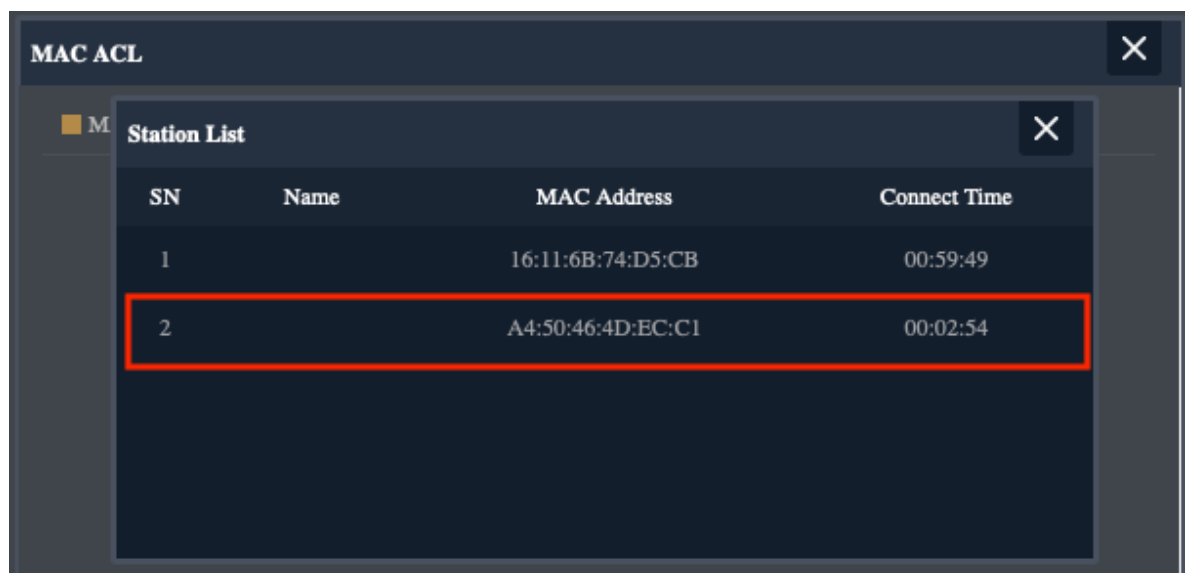


Click Scan



The image shows a 'MAC ACL' configuration window. At the top, there is a title bar with a close button. Below it, a section titled 'MAC ACL' contains a 'Status' toggle switch which is turned on (green). There are two input fields: 'MAC Address' and 'Mark'. To the right of the 'MAC Address' field is a 'Scan' button, which is highlighted by a red arrow. Below the 'Mark' field is a 'Save' button.

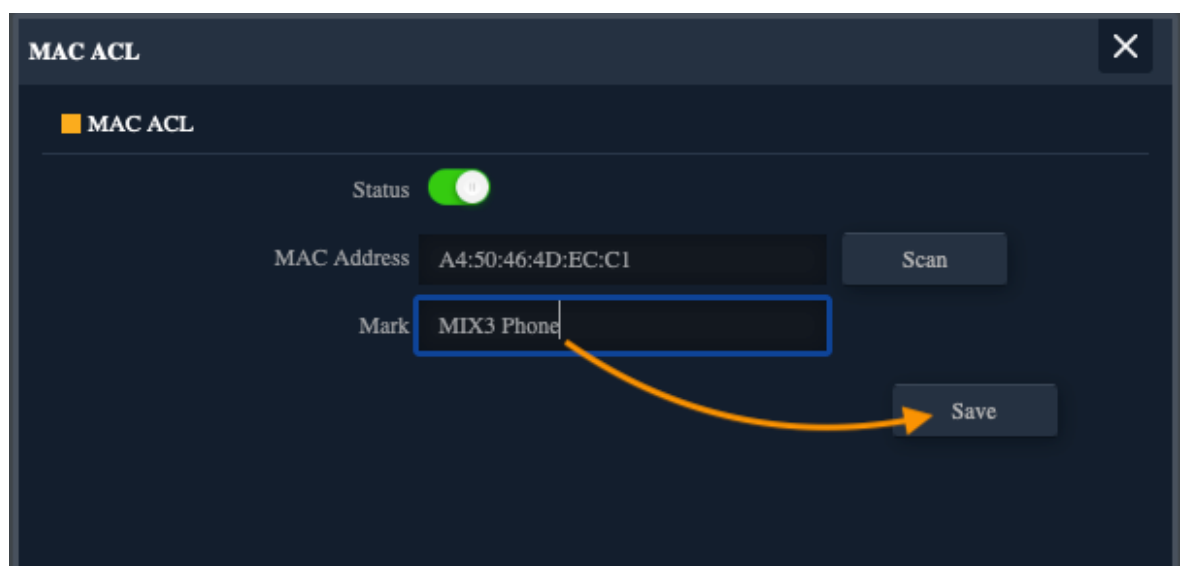
Click the MAC ID of the device to be whitelisted



The image shows the 'MAC ACL' configuration window with a 'Station List' table. The table has four columns: 'SN', 'Name', 'MAC Address', and 'Connect Time'. The second row is highlighted with a red box.

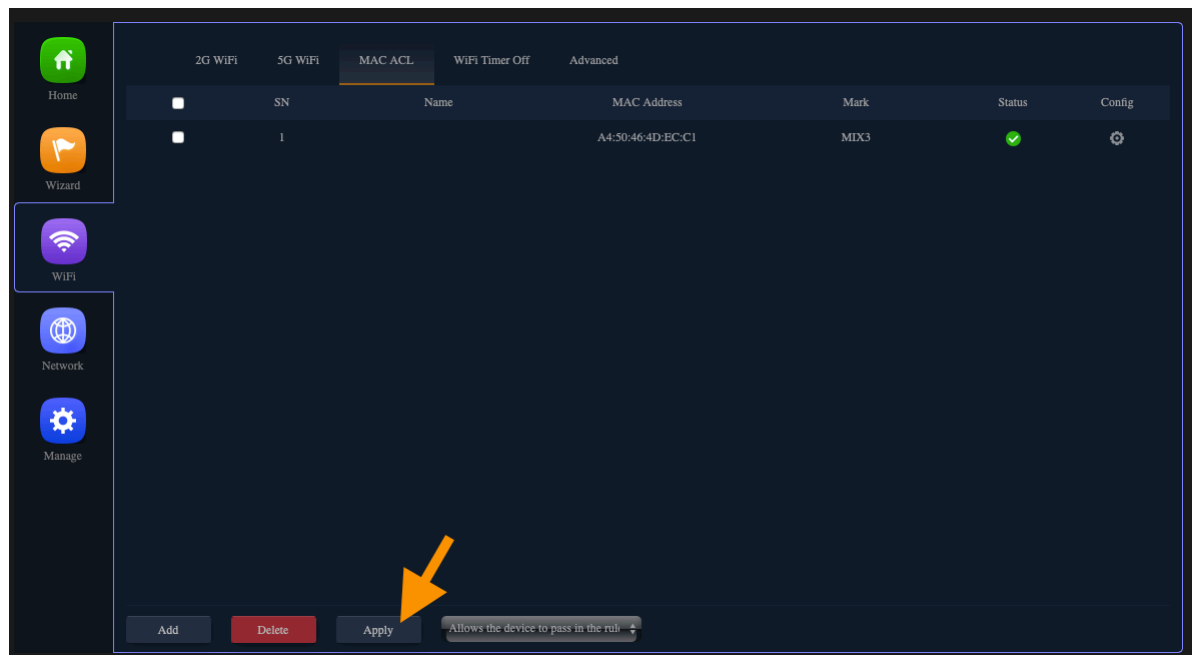
SN	Name	MAC Address	Connect Time
1		16:11:6B:74:D5:CB	00:59:49
2		A4:50:46:4D:EC:C1	00:02:54

Custom Mark



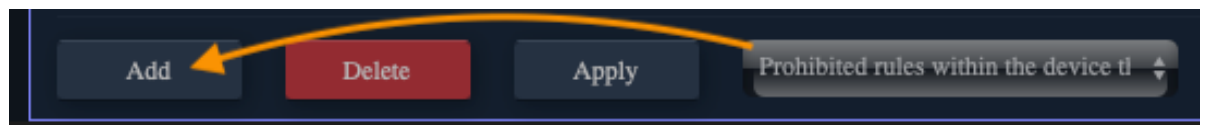
The image shows the 'MAC ACL' configuration window. The 'Status' toggle switch is turned on. The 'MAC Address' field contains the value 'A4:50:46:4D:EC:C1'. The 'Mark' field contains the text 'MIX3 Phone' and is highlighted with a blue box. An orange arrow points from the 'Mark' field to the 'Save' button.

Click Apply, Only the MAC ID devices in the list can connect normally

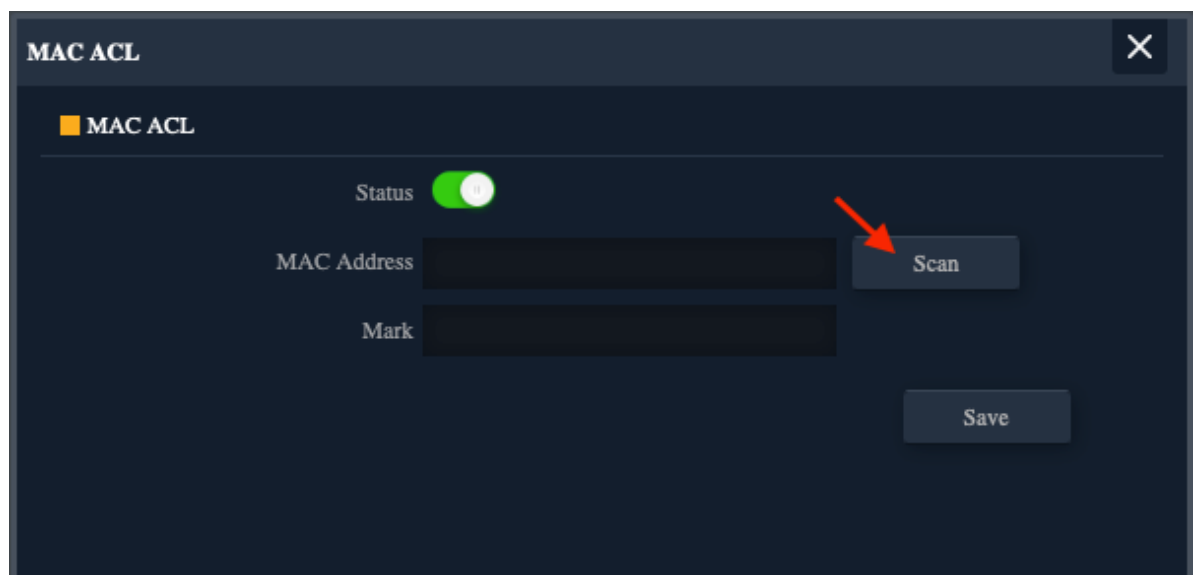


The following will demonstrate the "Prohibited rules within the device through" setting

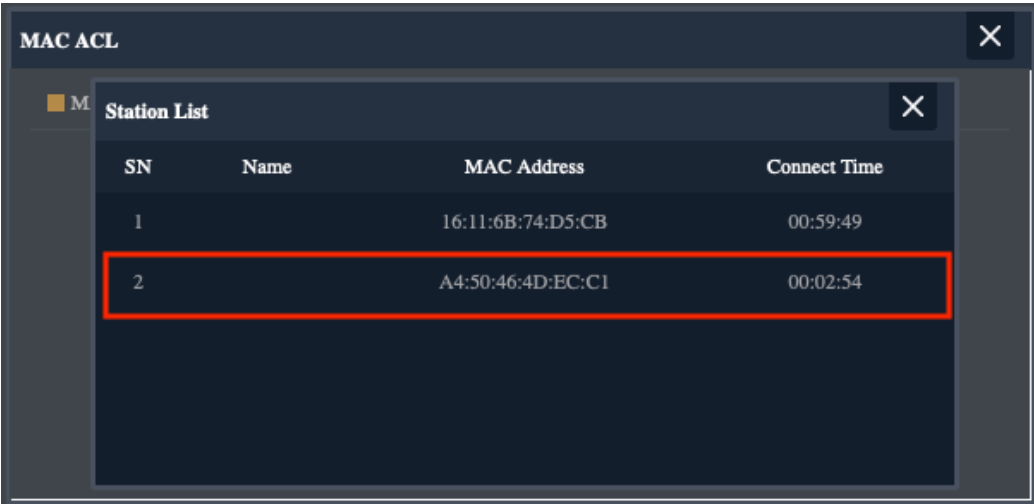
Click "Prohibited rules within the device through" >> Add



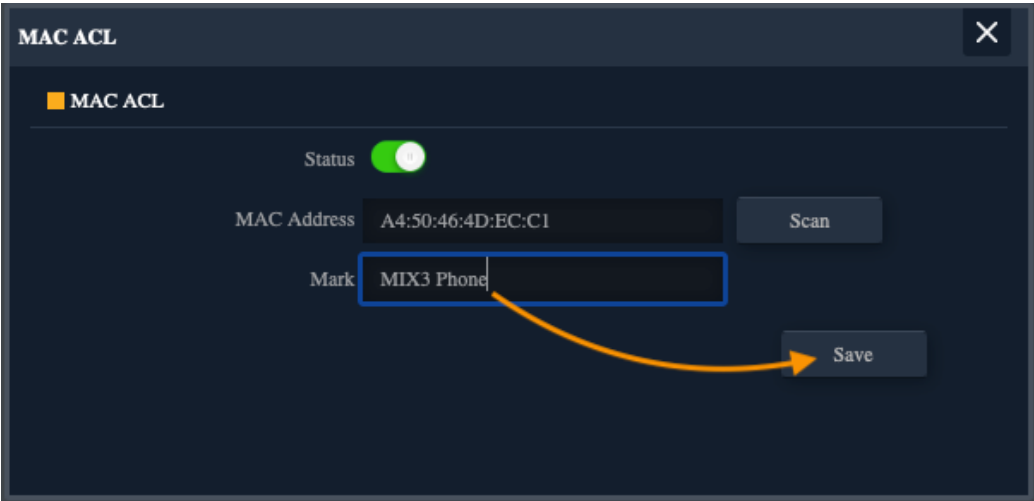
Click Scan



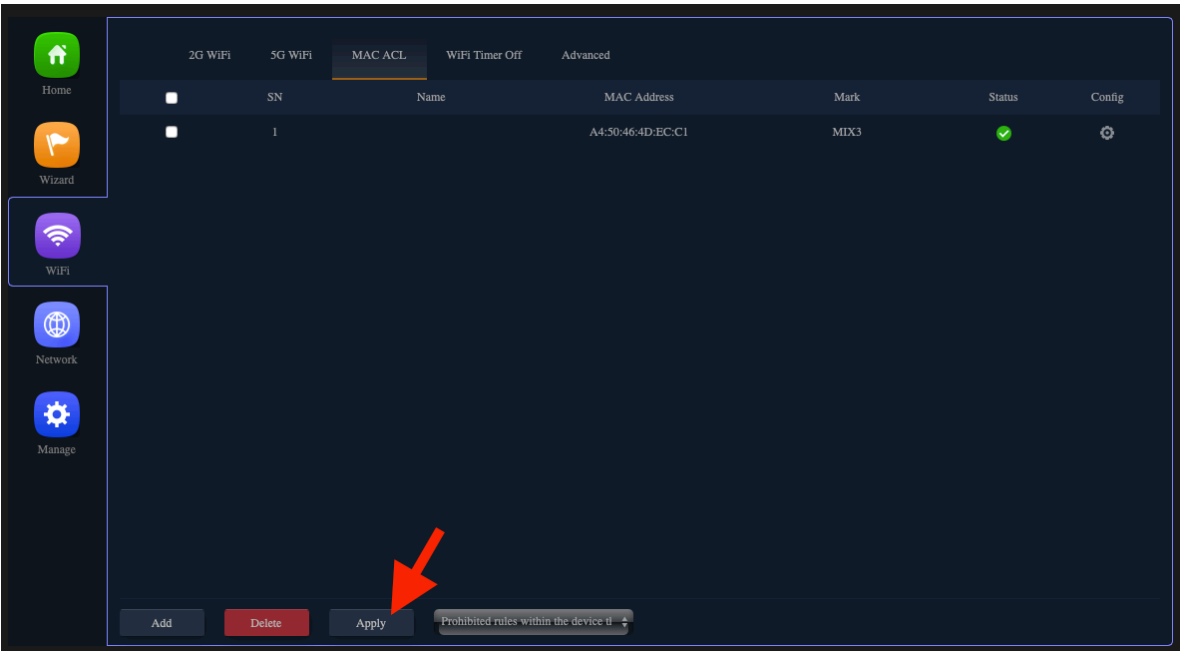
Click the MAC ID of the device to be whitelisted



Custom Mark

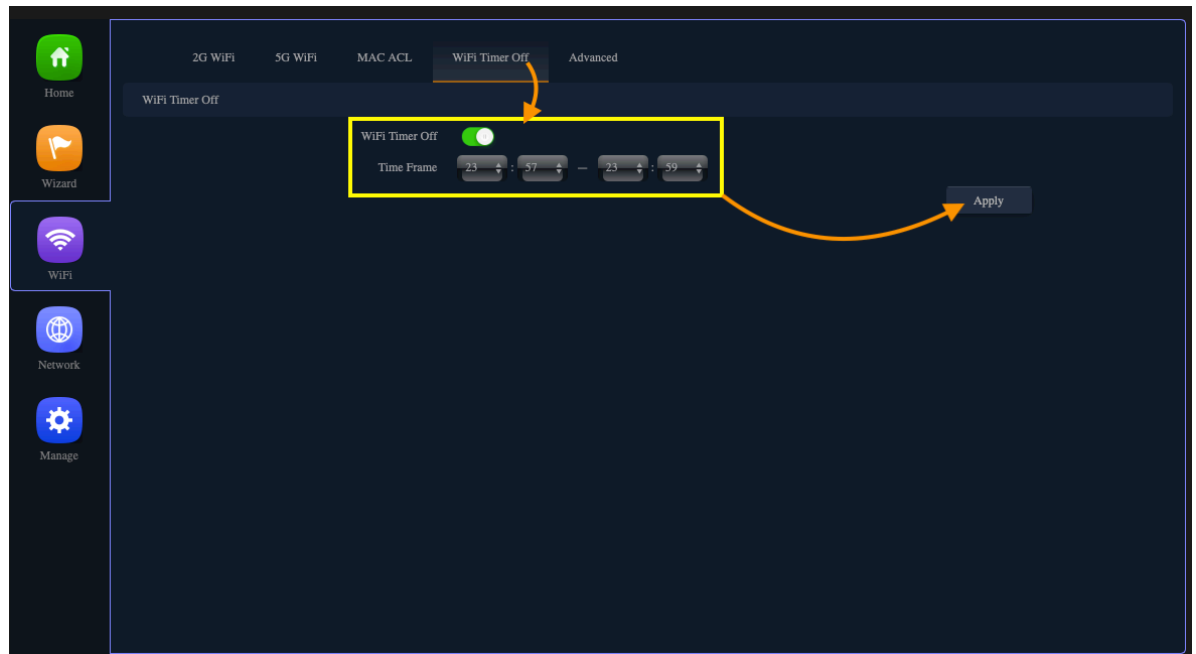


Click Apply, Only the MAC ID devices in this list cannot connect normally



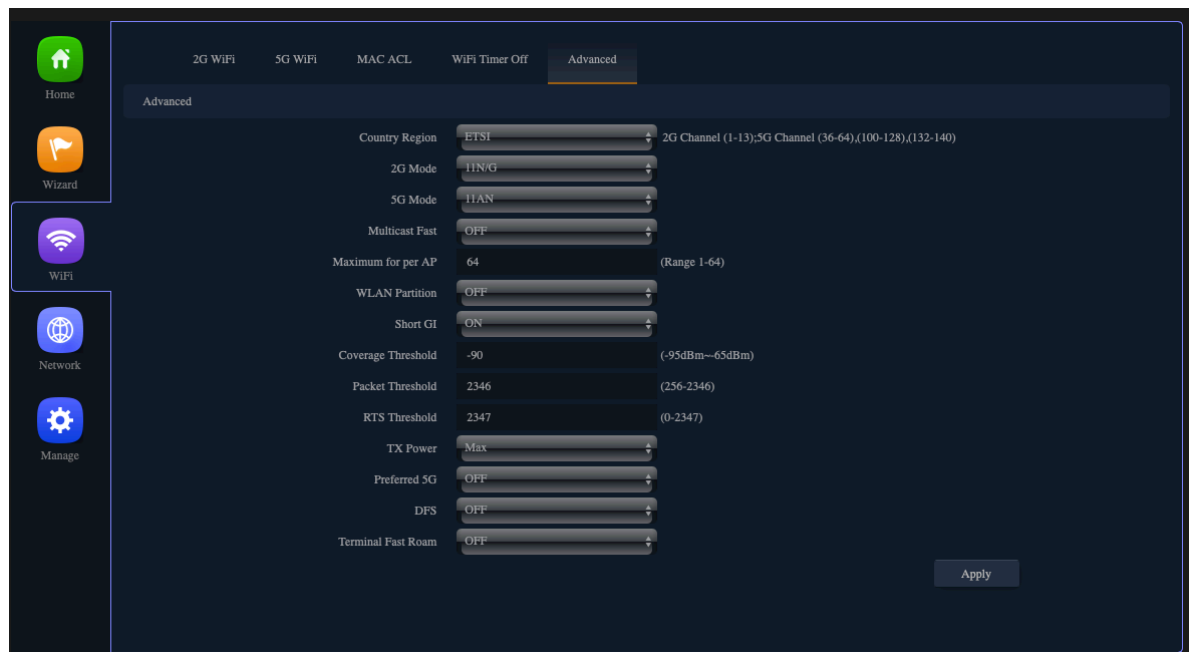
WiFi Timer Off

You can customize the AP device restart time range

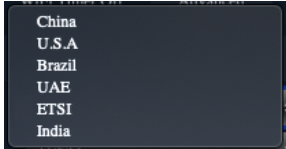

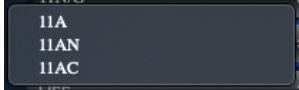
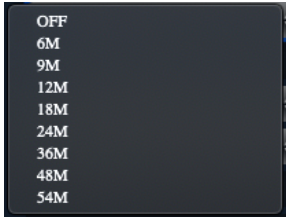


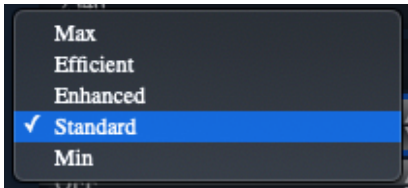
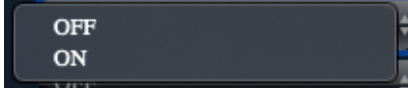
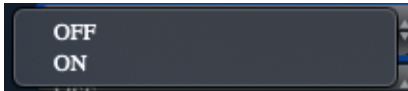
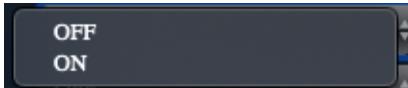
Advanced Setting

Please refer to the following options



Advanced Setting Description	
Country Region	<p>Select the country in which the AP is operating</p> <p>Wireless regulations vary from country to country. Make sure you select the correct country code so that the AP complies with the regulations in your country. The country code selection affects the radio modes the AP can support as well as the list of channels and</p>

	<p>transmission power of the radio.</p> <p>Each range has different characteristics. The lower frequencies exhibit better range, but with limited bandwidth and thus lower data rates. The higher frequencies exhibit less range and are subject to greater attenuation from solid objects.</p> <p>Devices that operate in unlicensed bands do not require any formal licensing process, but when operating in these bands, the user is obligated to follow the government regulations for that region.</p> 
2G Mode	<p>11N / G is recommended</p> 
5G Mode	<p>11AC is recommended</p> 
Multicast Fast	<p>By default the Multicast Fast option is disabled.</p> 
Maximum for per AP	<p>Specify the maximum number of stations allowed to access this AP at any one time. You can enter a value between 1 and 64.</p>
WLAN Partition	<p>This feature effectively segregates the wireless of your choice from the rest of the Network. With Ethernet-to-WLAN Access disabled, information sent from the Ethernet side will not be passed to the Wireless Clients. However, wireless clients will still be able to transmit across Ethernet for browsing, etc.</p>
Short GI	<p>Short GI(Short Guard Interval)</p> <p>Short Guard Interval shortens the waiting time to 400 ns, Guard Interval is intended to avoid signal loss from multipath effect.</p>
Coverage Threshold	<p>based on a receive threshold that evaluates the carrier for activity. It is generally a good practice to consider -85 decibels per milliwatt (dBm) as that threshold.</p>
	<p>This value should be left at the default value of 2346. If you are</p>

Packet Threshold	<p>experiencing high packet error rate, slightly increase your fragmentation threshold within the value range of 256-2346.</p> <p>Setting the fragmentation threshold too low may result in poor performance.</p>
RTS Threshold	<p>This value should be left at the default value of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 256-2347 are recommended.</p>
TX Power	<p>The less TX Power you set can save the electronic power, but comparatively reduce the range of the wireless signal of AP.</p> <p>according to local national Radio frequency power regulations,</p> <p>To comply effective isotropic radiated power (EIRP) <20dBm,</p> <p>Please click Standard mode</p> 
Preferred 5G	
DFS	<p>DFS(Dynamic Frequency Selection)</p> <p>Enable wireless products to actively detect the frequency used by the military and actively choose another frequency to avoid the military frequency. which allows WLANs to avoid interference with incumbent radar users in instances where they are collocated.</p> <p>NOTE: For EU Wireless Regulations, Please turn on the DFS</p> 
Terminal Fast Roam	<p>After opening, Wireless roaming for multiple APs, you need to set the same WiFi SSID / WiFi PASSWORD</p> 

Section IV Network

(For AP/Repeater Mode)

LAN Settings

Can choose 3 kinds of usage modes (Static IP/Get IP From AC/ Get IP From Gateway) which can be selected according to the current network architecture environment.

The screenshot shows the 'LAN Settings' page. On the left is a sidebar with icons for Home, Wizard, WiFi, Network, and Manage. The main area has two tabs: 'LAN Settings' (active) and 'VLAN Settings'. Under 'LAN Settings', there is a dropdown menu for 'IP Mode' with options: 'Static IP' (selected), 'Get IP From AC', and 'Get IP From Gateway'. Below this are input fields for 'Lan IP', 'Subnet' (255.255.252.0), 'Gateway' (192.168.188.1), 'Primary DNS' (168.95.1.1), and 'Secondary DNS' (8.8.8.8). A 'DHCP Server' section has a toggle switch labeled 'DHCP Server' which is currently turned off. An 'Apply' button is at the bottom right.

VLAN Settings

Can be selected according to the current VLAN Settings network architecture environment.

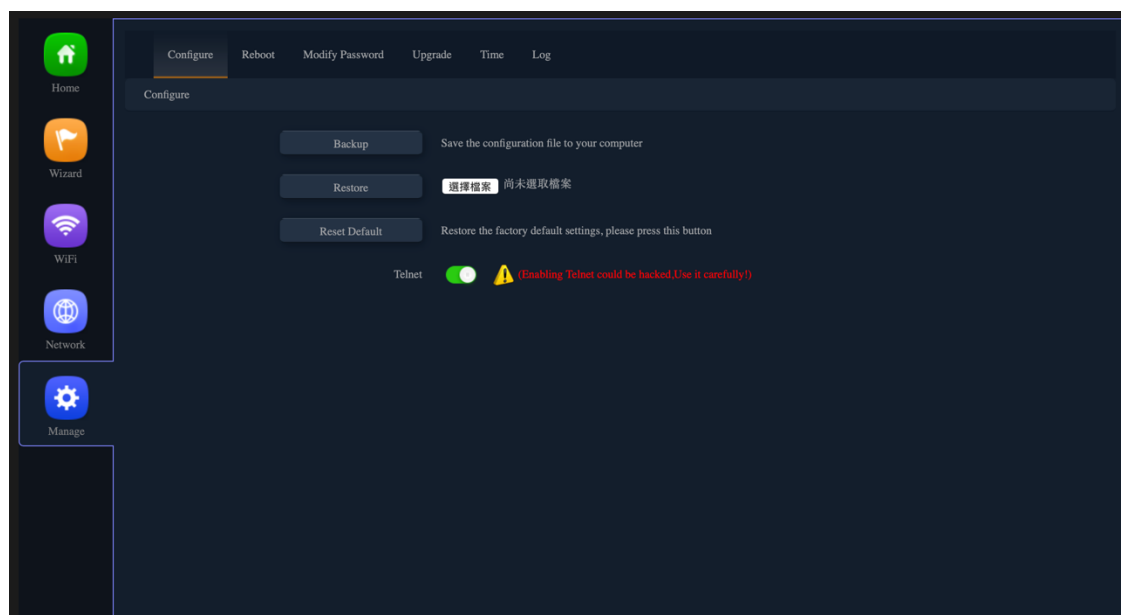
The screenshot shows the 'VLAN Settings' page. The sidebar is the same as in the LAN Settings page. The main area has two tabs: 'LAN Settings' and 'VLAN Settings' (active). Below the tabs is a table with columns for 'AP', 'VAP 1', 'VAP 2', and 'VAP 3'. The rows are '2G WiFi' and '3G WiFi'. Each cell in the table contains a dropdown menu showing 'VLAN-ID range 3-4094'. At the bottom, there is an 'Apply' button and a toggle switch labeled 'ON'.

Section V Manage

(For AP/Repeater Mode)

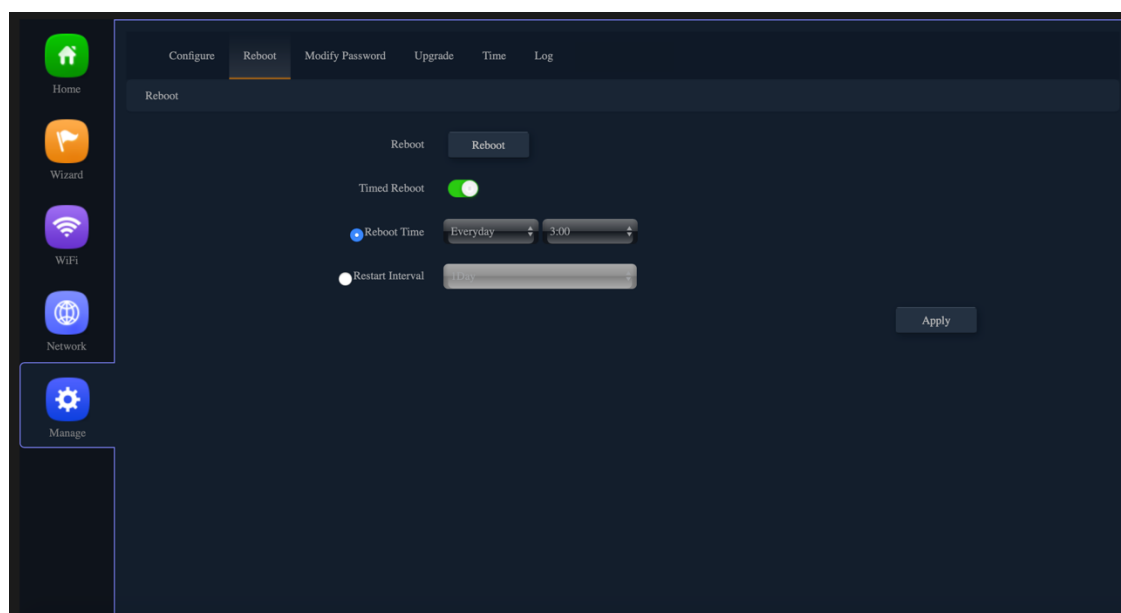
Configure

- Save the configuration file to your computer, You can also upload the configuration file to overwrite the current configuration.
- Restore the factory default settings, please press this Reset button



Reboot

Set the scheduling time for rebooting the device yourself



Modify Password

Change the admin password for Log in.

The screenshot shows a web interface with a dark blue sidebar on the left containing icons for Home, Wizard, WiFi, Network, and Manage. The main area has a top navigation bar with tabs: Configure, Reboot, Modify Password (selected), Upgrade, Time, and Log. Below the tabs, the title 'Modify Password' is displayed. The form contains three input fields: 'Old Password', 'New Password', and 'Confirm Password'. An 'Apply' button is located at the bottom right of the form.

Upgrade

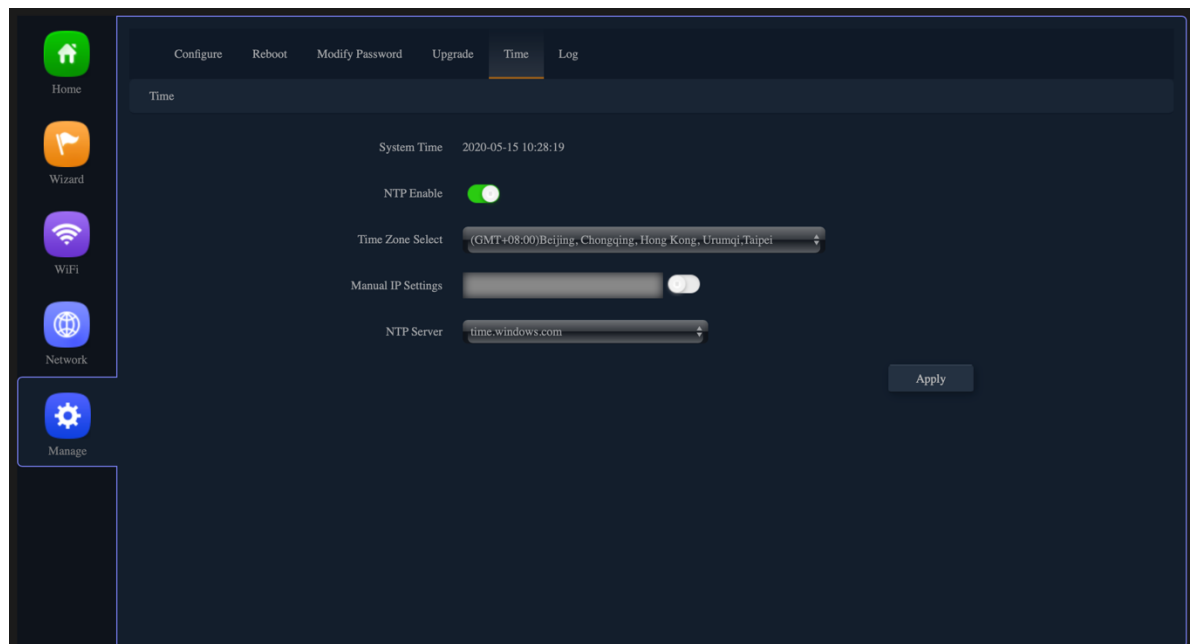
You can browse the new firmware in your computer and upgrade. Please do not power off the device during upgrade.

(The update firmware is recommended to use the connection RJ45 Network Cable update. Not recommended to use the wireless connection method to update the firmware)

The screenshot shows the 'Upgrade' section of the web interface. The sidebar is the same as in the previous image. The top navigation bar has tabs: Configure, Reboot, Modify Password, Upgrade (selected), Time, and Log. The main area has the title 'Upgrade'. It displays the firmware version: 'Version:LevelOne-WAP-8122-V2-S-Build20191218145451'. Below this is a file selection area with a button labeled '選擇檔案' and the text '尚未選取檔案'. There is a toggle switch for 'Whether to resume the factory configuration'. A warning message with a yellow triangle icon states: 'Note: Do not power off during the process of upgrading the software'. An 'Upgrade' button is located at the bottom right.

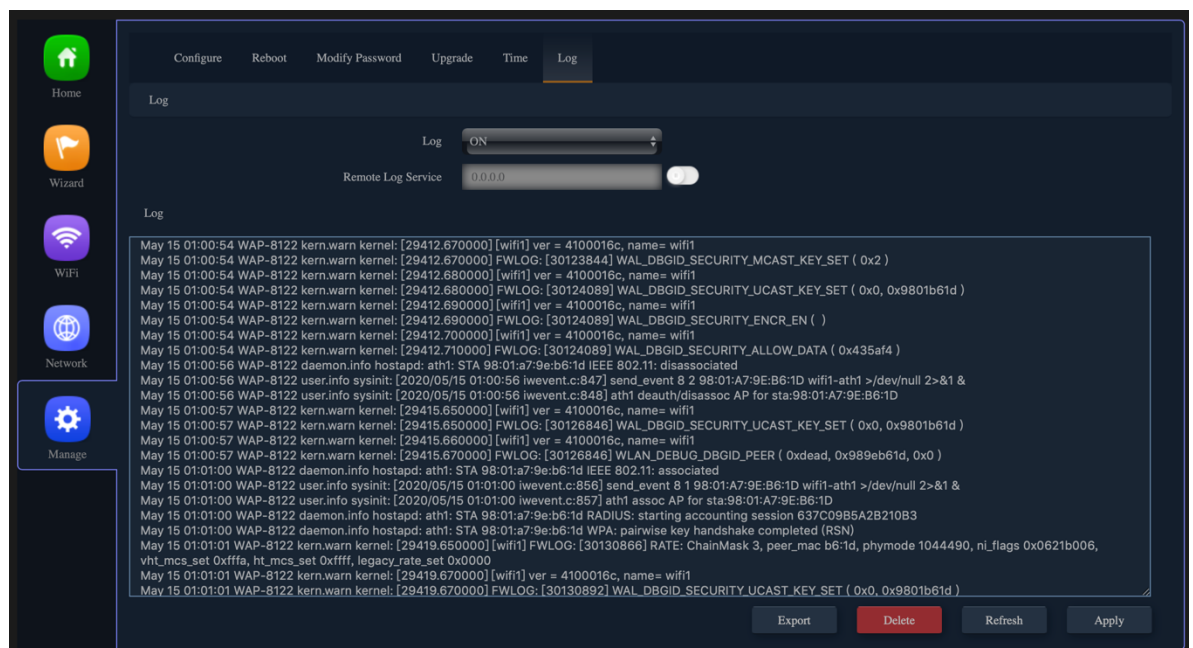
Time

Before sync with host, please select your Time zone. Get time from NTP server can only be available under Gateway and WISP Mode.



Log

Can use Log to find errors to check the cause of the problem.

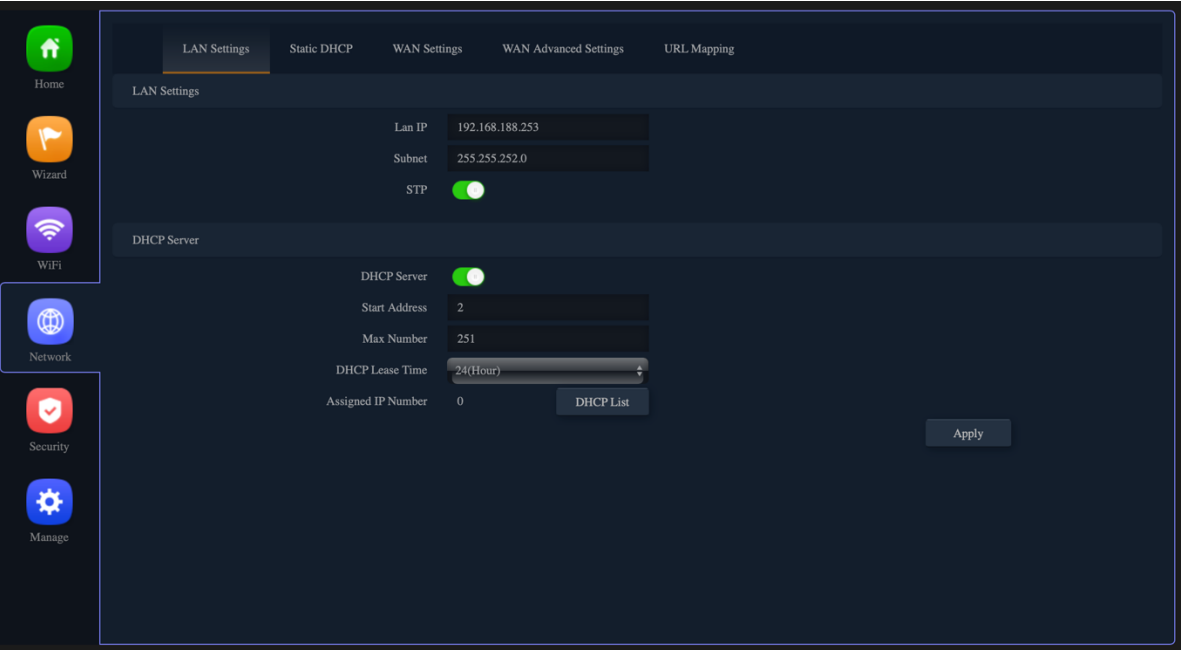


Section VI Network

(For Gateway/WISP Mode)

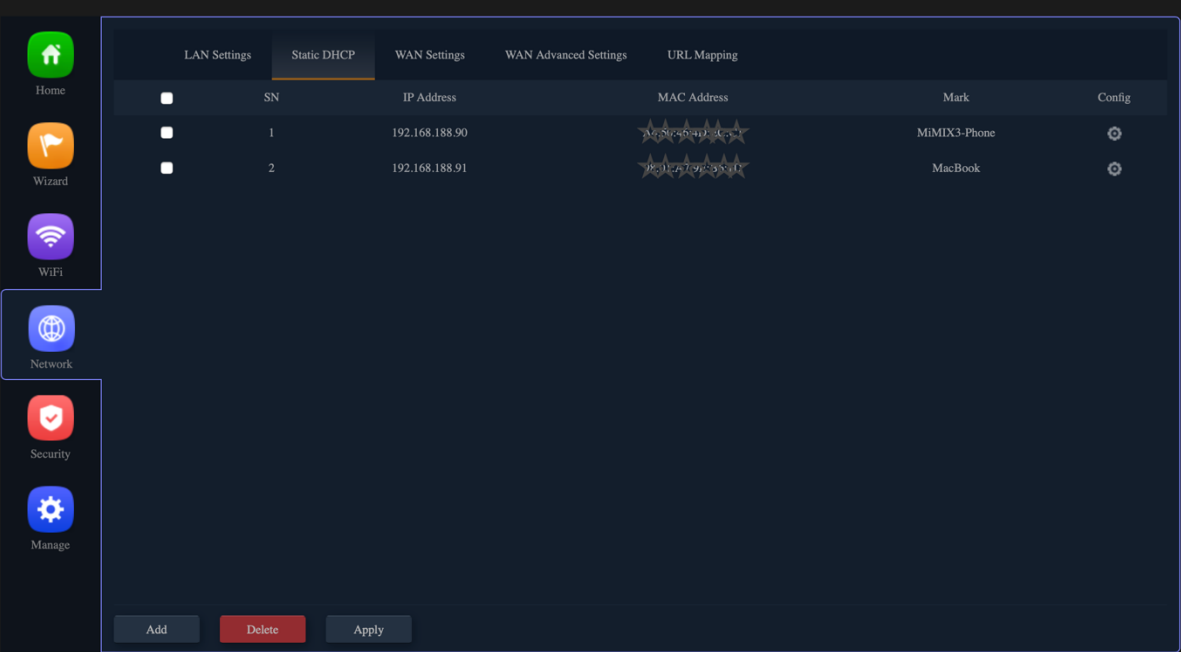
LAN Settings

You can set to change Lan IP address and Subnet and choose whether to turn off the STP function (Spanning Tree Protocol), the default is enabled. also set up basic functions in the DHCP Server



Static DHCP

Click the Add option, through the Static DHCP function, you can manage the specified distribution IP address and edit device name.



WAN Settings

Connect Internet Method can be set, there are 3 modes of Static IP / PPPoE / DHCP to choose

The screenshot shows the 'WAN Settings' page. On the left is a sidebar with icons for Home, Wizard, WiFi, Network (selected), Security, and Manage. The top navigation bar includes 'LAN Settings', 'Static DHCP', 'WAN Settings' (active), 'WAN Advanced Settings', and 'URL Mapping'. The main content area is titled 'WAN Settings' and contains the following fields:

Connect Method	PPPoE
Username	ac0143636
Password	143636
Server Name	If not, please do not fill out
Service Name	If not, please do not fill out
MTU	1452 (1400-1492)
Set DNS Manually	<input type="checkbox"/>
Primary DNS	8.8.8.8
Secondary DNS	4.4.4.4
Band Type	1000M Fiber
Upstream	1000000 Kbps
Downstream	1000000 Kbps

An 'Apply' button is located at the bottom right of the settings area.

WAN Advanced Settings

The default is On

- Enable PPTP pass through on VPN connection
- Enable IPsec pass through on VPN connection
- Enable L2TP pass through on VPN connection

The default is off (for network security)

- Enable web server access on WAN port
- MAC Clone
- Enable Ping Access on WAN
- Line Detection Host Name 1/Name 2

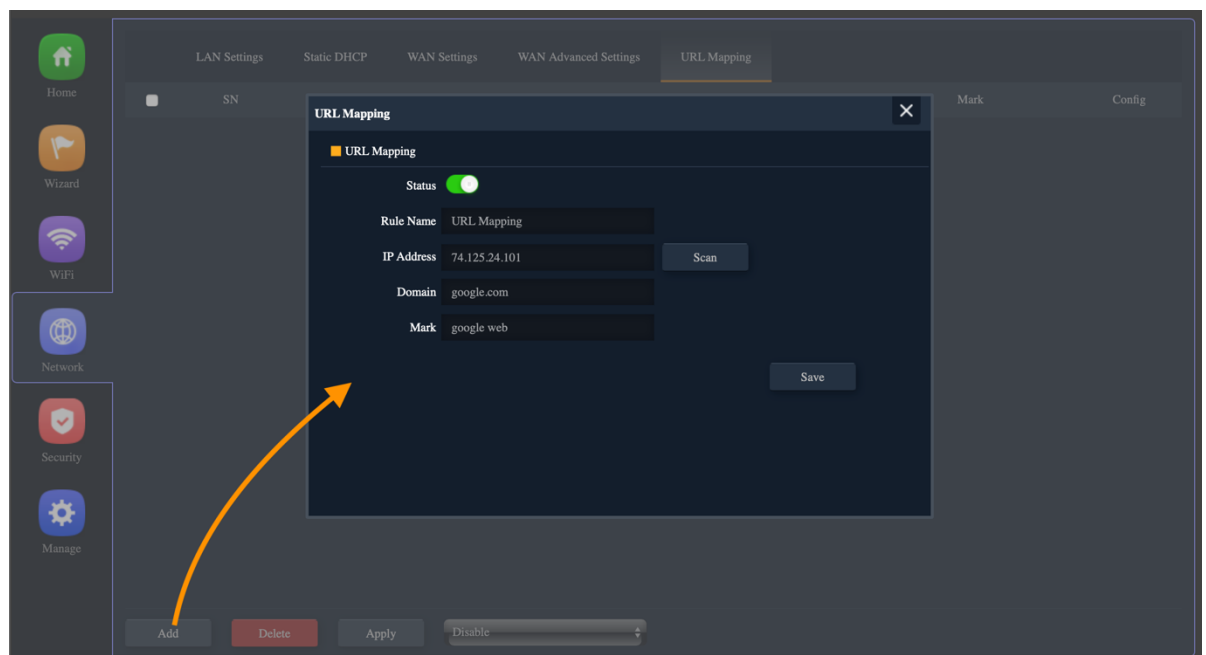
The screenshot shows the 'WAN Advanced Settings' page. The sidebar and top navigation bar are identical to the previous screenshot. The main content area is titled 'WAN Advanced Settings' and contains the following options:

<input type="checkbox"/>	Enable web server access on WAN port	8080 (1-65535)
<input type="checkbox"/>	MAC Clone	<input type="text"/> Scan
<input type="checkbox"/>	Enable Ping Access on WAN	
<input checked="" type="checkbox"/>	Enable IPsec pass through on VPN connection	
<input checked="" type="checkbox"/>	Enable PPTP pass through on VPN connection	
<input checked="" type="checkbox"/>	Enable L2TP pass through on VPN connection	
<input type="checkbox"/>	Line Detection	Host Name 1: 114.114.114.114 Host Name 2: 114.114.115.115

An 'Apply' button is located at the bottom right of the settings area.

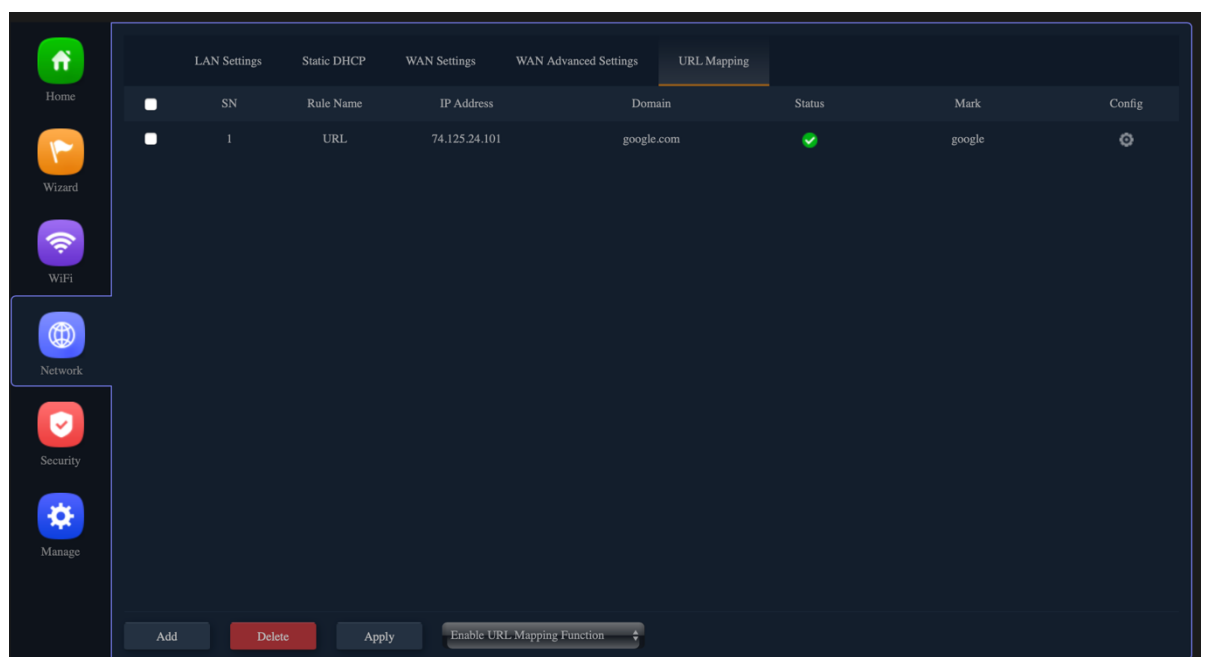
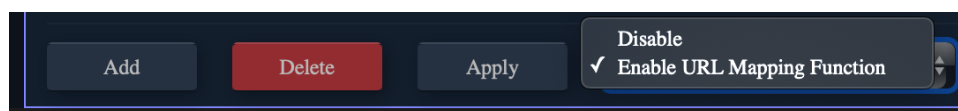
URL Mapping

1. Click the Add option, through the URL Mapping function, you can manage the Used in URLs to IP addresses identify particular Web pages.



2. Choose according to the current use needs. After selecting, please click Apply.

- Disable
- Enable URL Mapping Function

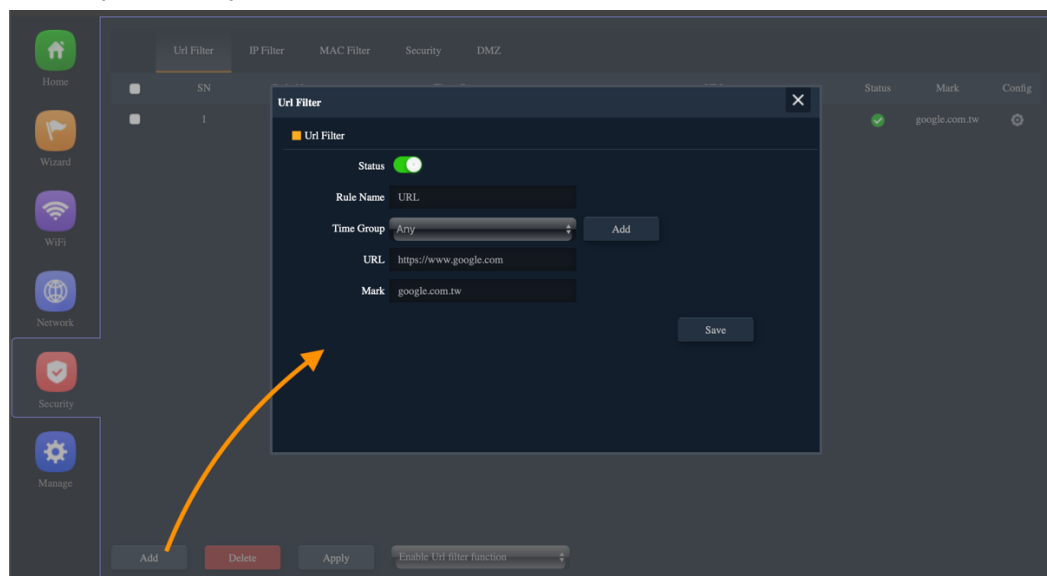


Section VII Security

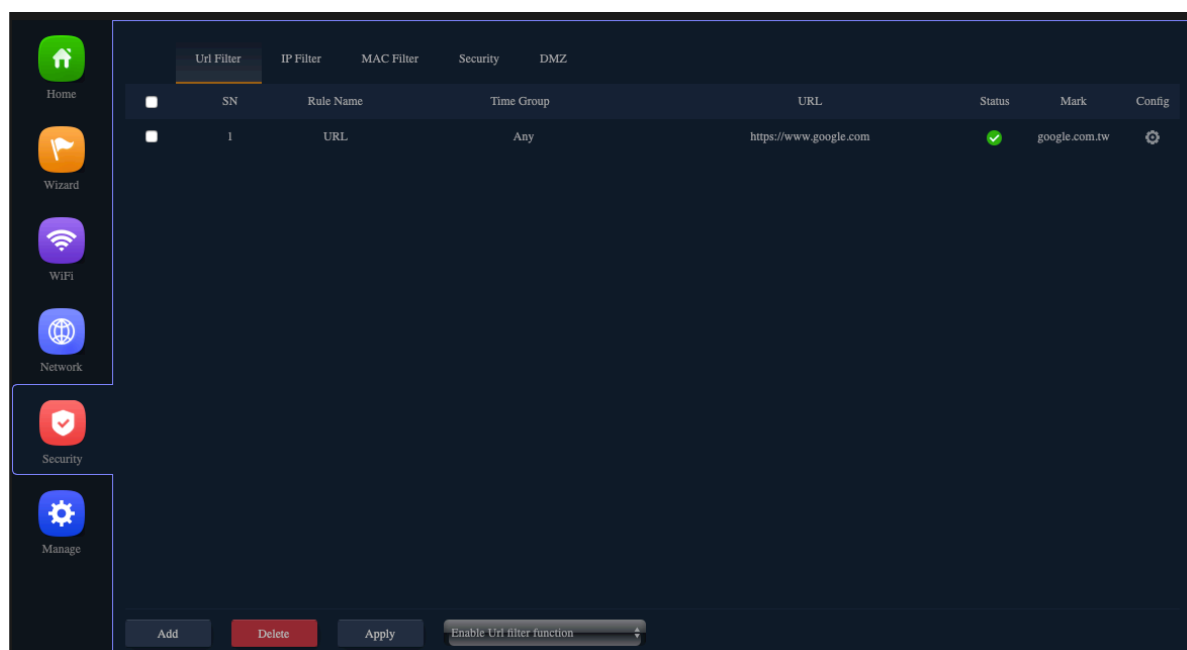
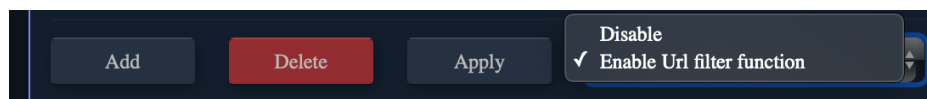
(For Gateway/WISP Mode)

URL Filter

1. Set URL Filter list, Manage which websites cannot be accessed within a specified time, Need to cooperate to open MAC Filter function

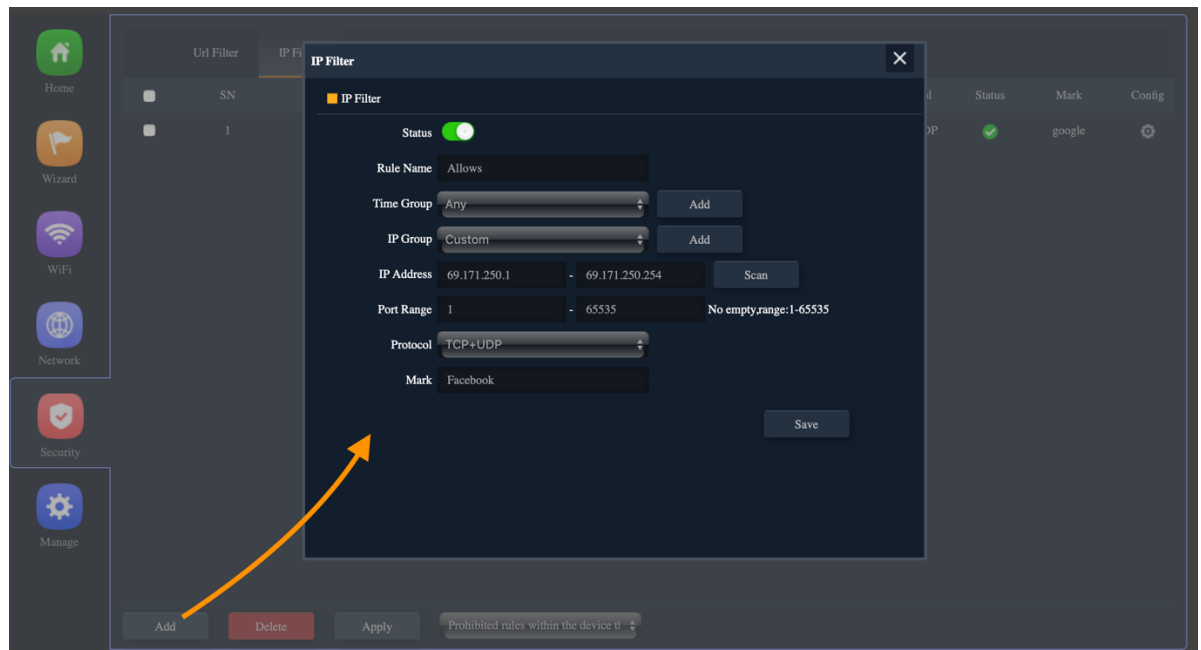


2. Choose according to the current use needs. After selecting, please click Apply.
 - Disable
 - Enable URL Filter function,



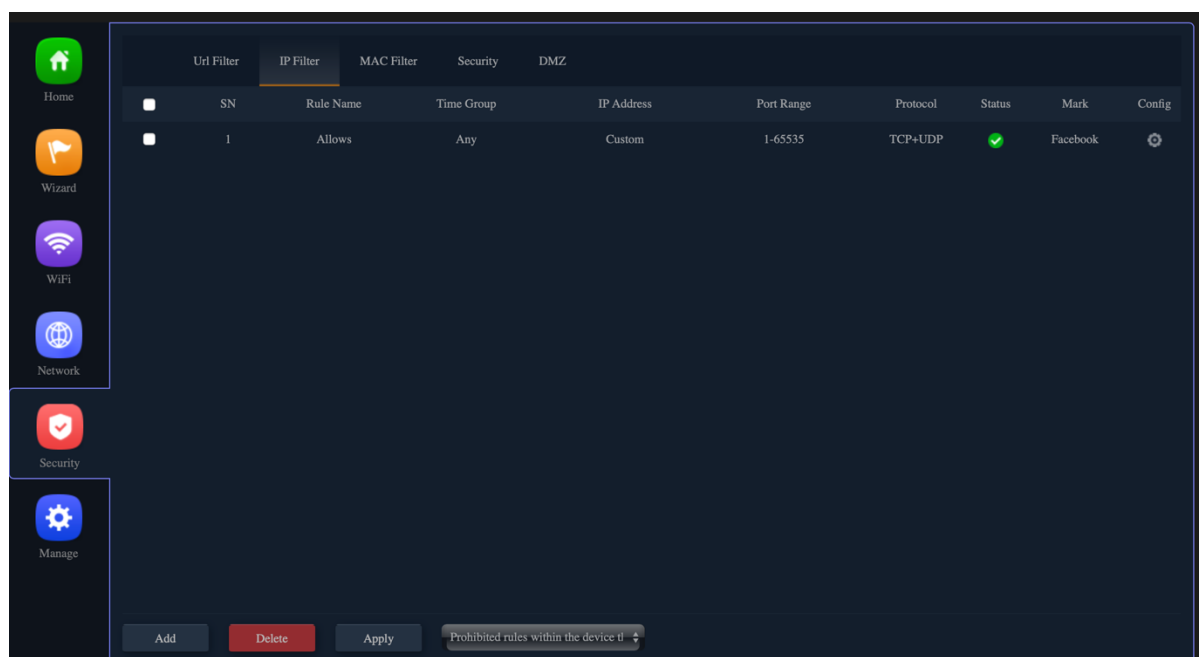
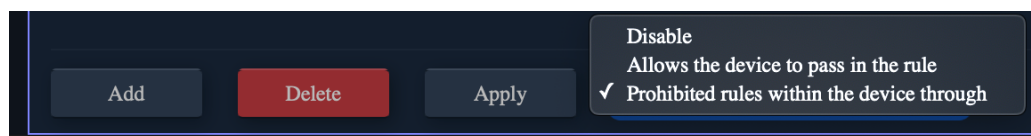
IP Filter

1. Set the IP filter list to manage the inability to access the specified ip address within a specified time, you need to cooperate with the MAC filter function



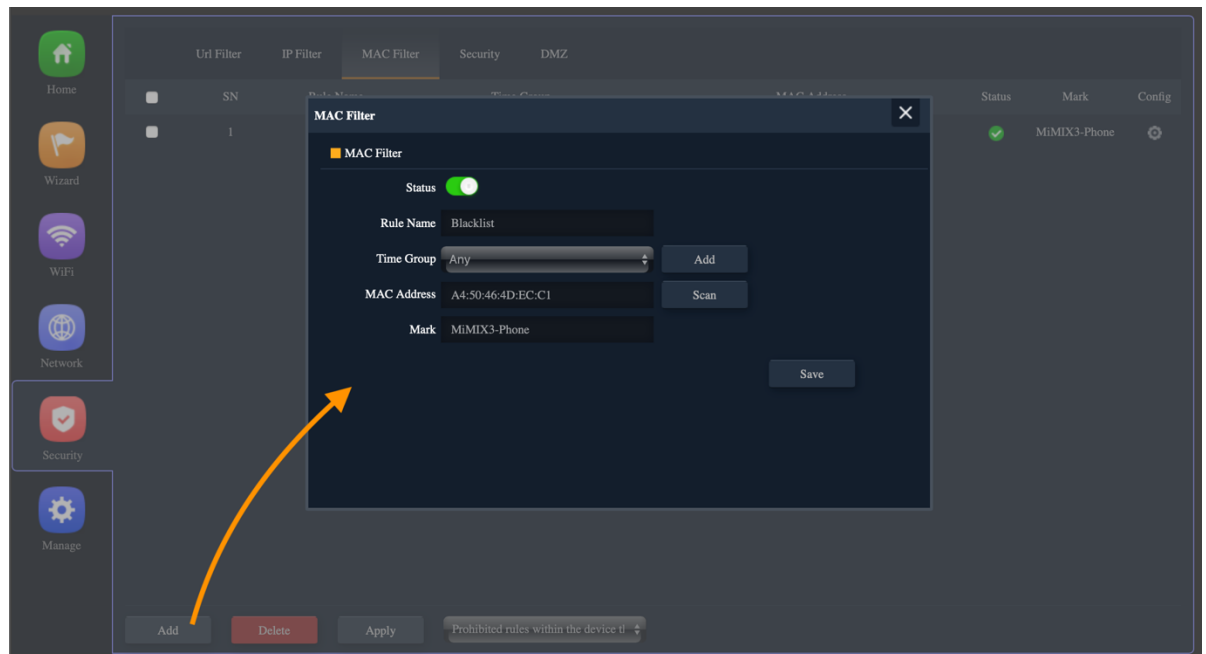
2. Choose according to the current use needs. After selecting, please click Apply.

- Disable
- Allows the device to pass in the rule
- Prohibited rules within the device through



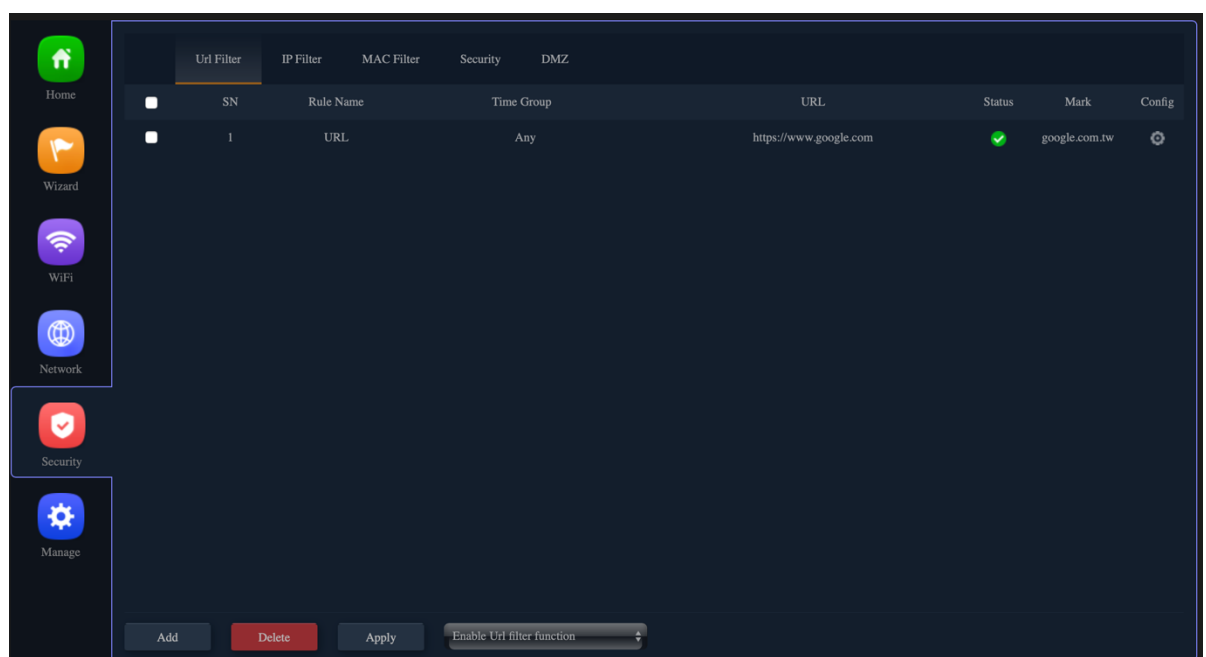
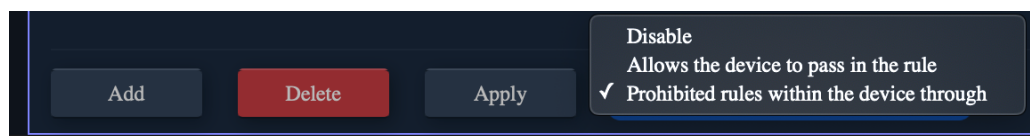
MAC Filter

1. Choose two kinds of usage modes (Static IP, DHCP for Controller) which can be selected according to the current network architecture environment.



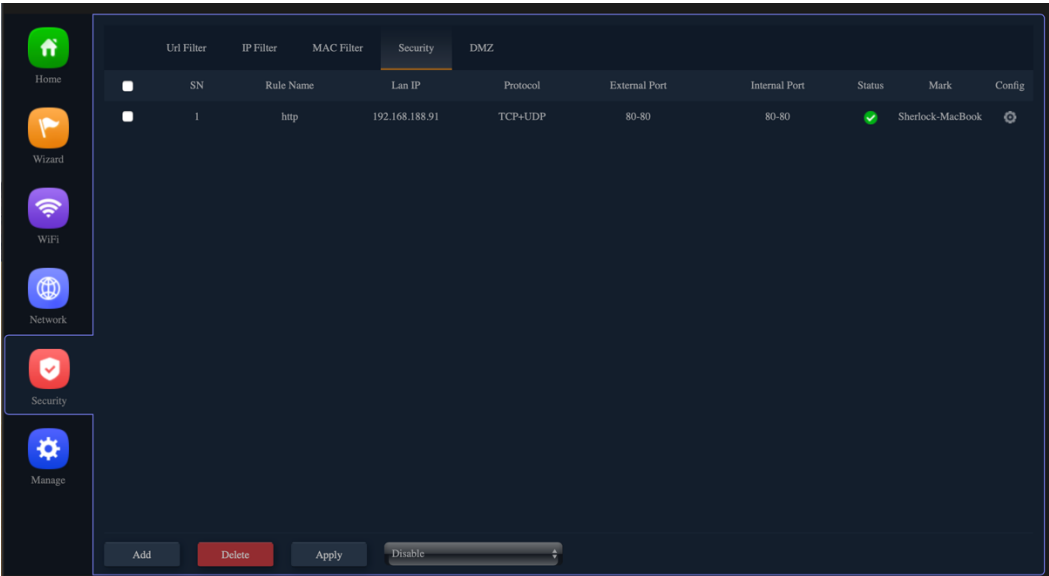
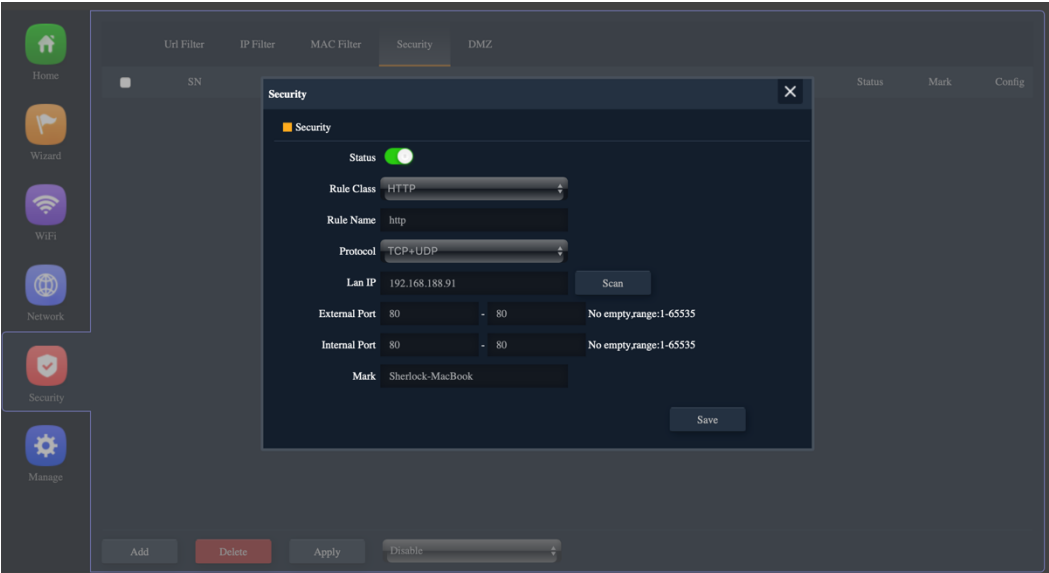
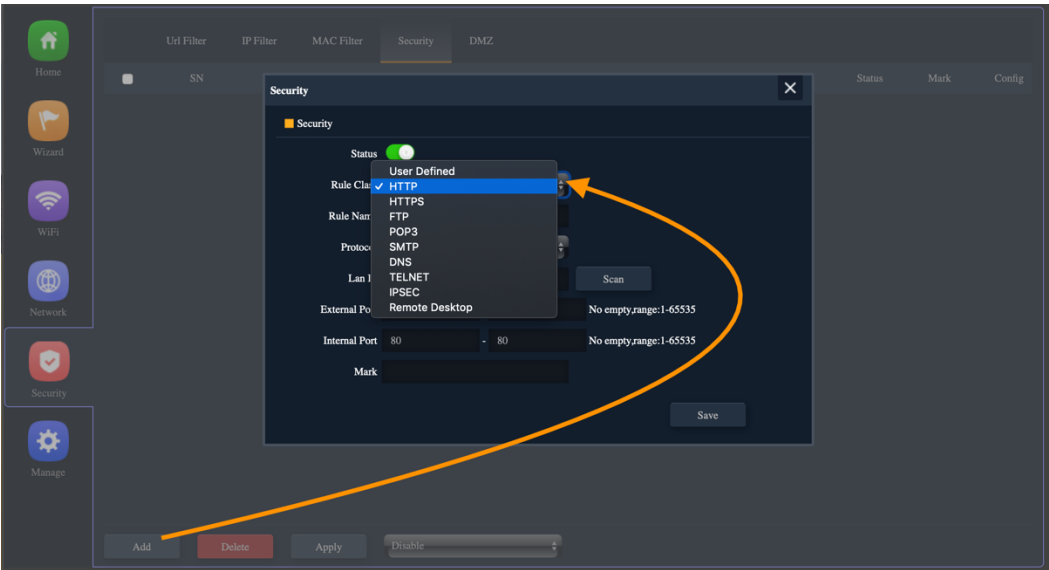
2. Choose according to the current use needs. After selecting, please click Apply.

- Disable
- Allows the device to pass in the rule
- Prohibited rules within the device through



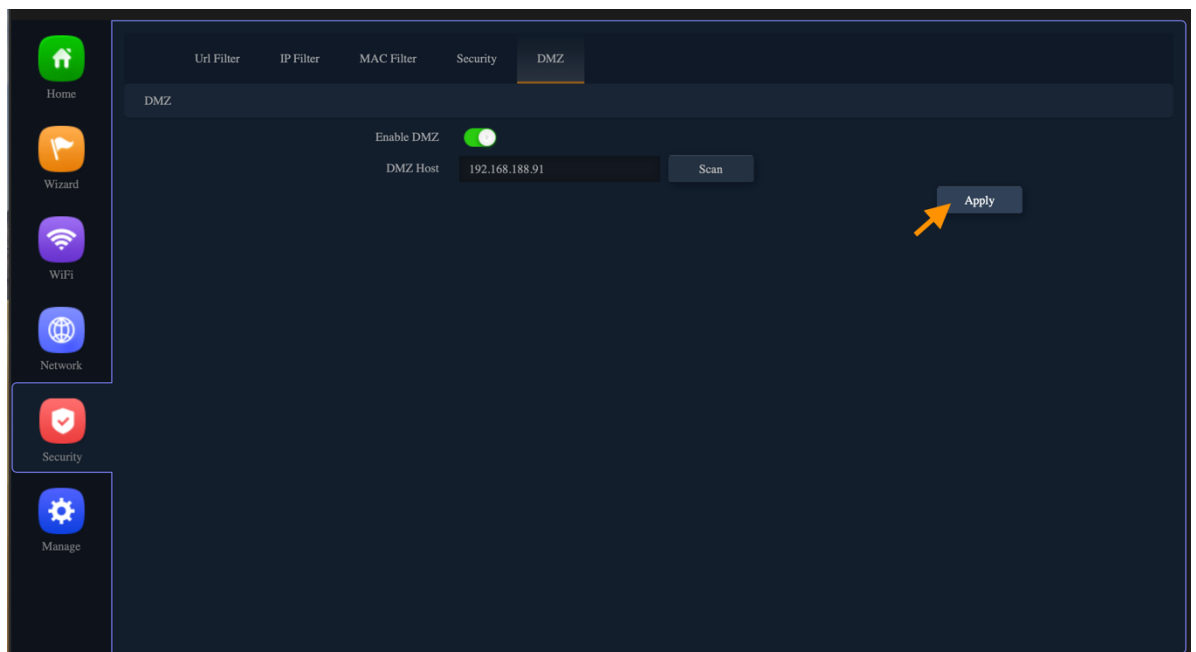
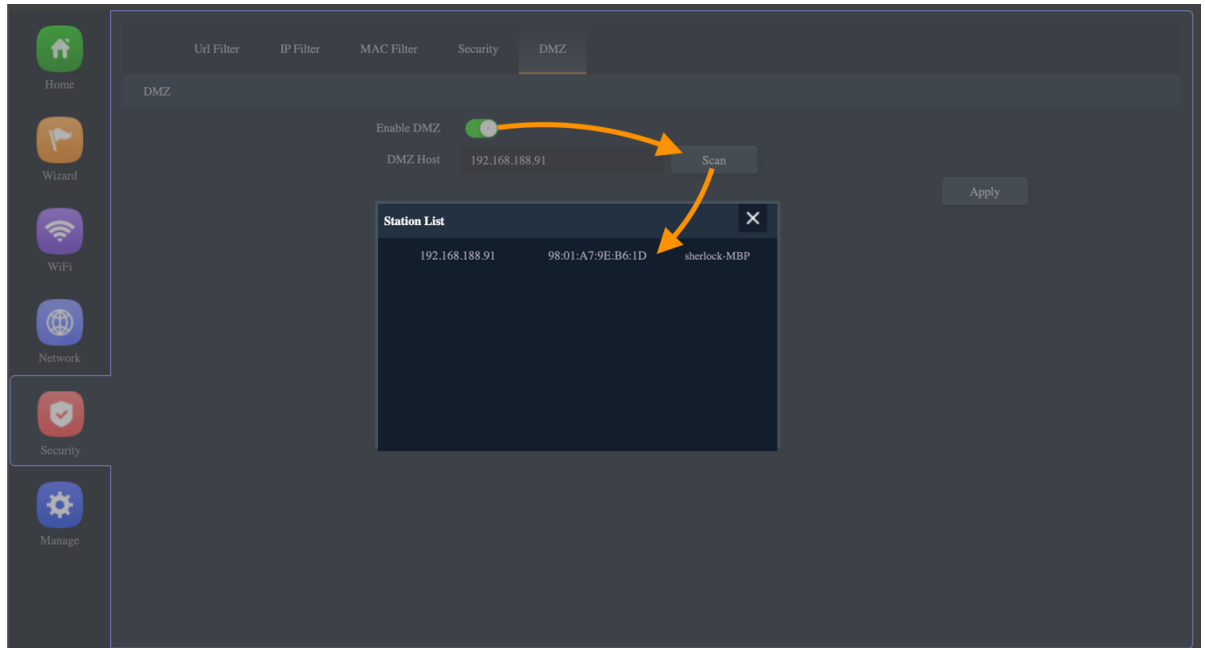
Security

Set "Rule Class" option as shown below, you can also manually enter other External/Internal Port 1-65535.



DMZ

DMZ(Demilitarized zone) refers to an internal network host where all ports are exposed to the external network, and all other ports are forwarded. Strictly speaking, this is not a real DMZ, because the host can still access the internal network, and it is not independent of the internal network.

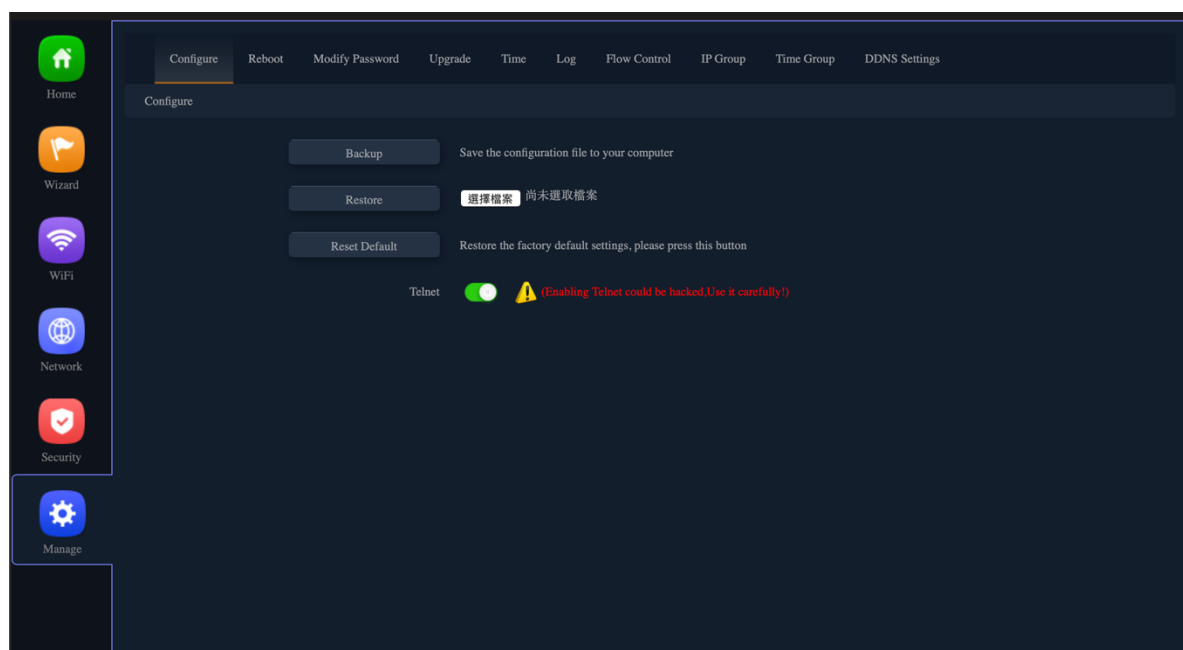


Section VIII Manage

(For Gateway/WISP Mode)

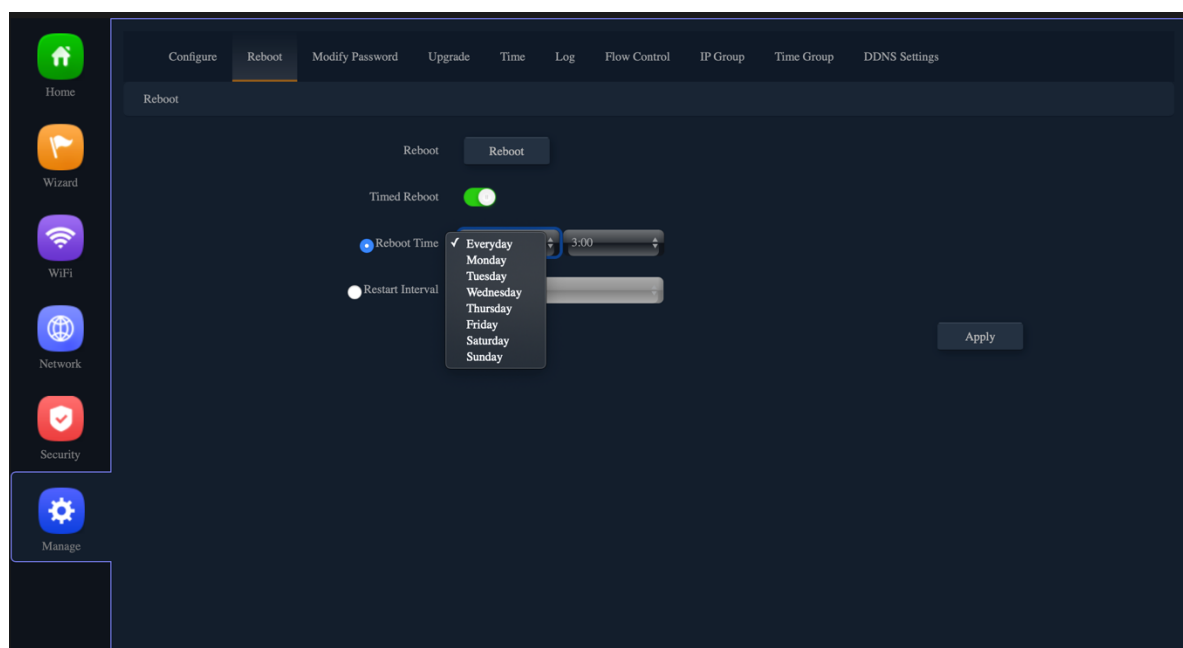
Configure

- Save the configuration file to your computer, You can also upload the configuration file to overwrite the current configuration.
- Restore the factory default settings, please press this Reset button



Reboot

Set the scheduling time for rebooting the device yourself



Modify Password

Change the admin password for Log in.

The screenshot shows the 'Modify Password' page in a web management interface. On the left is a sidebar with icons for Home, Wizard, WiFi, Network, Security, and Manage. The top navigation bar includes links for Configure, Reboot, Modify Password (which is highlighted), Upgrade, Time, Log, Flow Control, IP Group, Time Group, and DDNS Settings. The main content area is titled 'Modify Password' and contains three input fields: 'Old Password', 'New Password', and 'Confirm Password'. An 'Apply' button is located at the bottom right of the form.

Upgrade

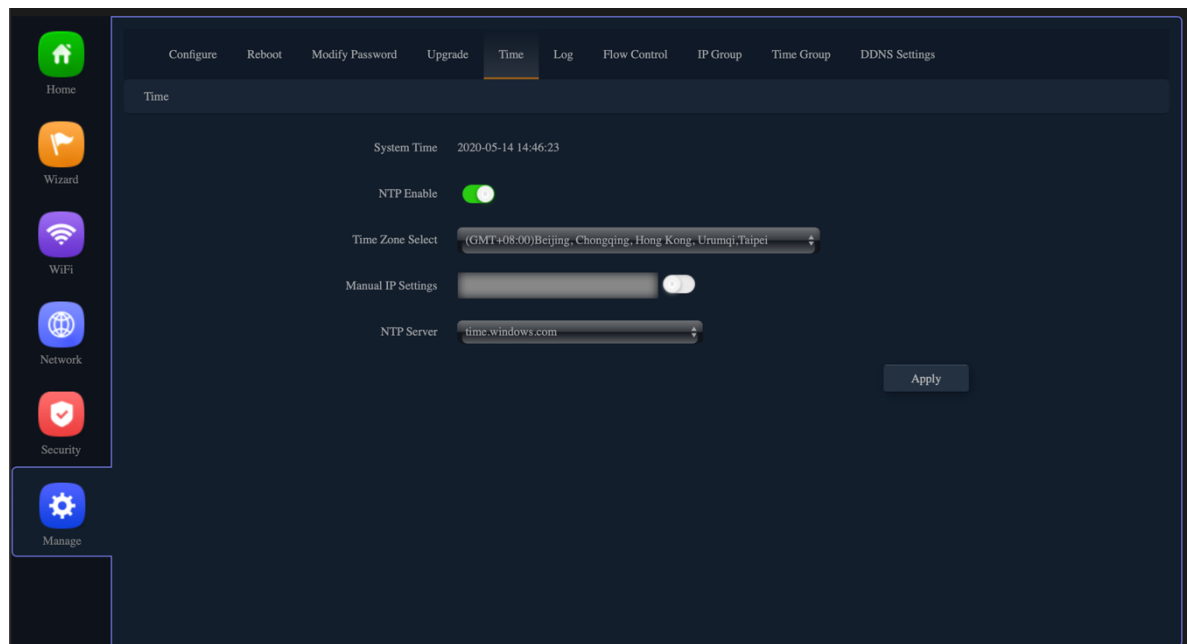
You can browse the new firmware in your computer and upgrade. Please do not power off the device during upgrade.

**(The update firmware is recommended to use the connection RJ45 Network Cable update.
Not recommended to use the wireless connection method to update the firmware)**

The screenshot shows the 'Upgrade' page in the same web management interface. The sidebar and top navigation bar are identical to the previous page. The main content area is titled 'Upgrade' and displays the current firmware version: 'Version:LevelOne-WAP-8122-V2-S-Build20191218145451'. Below this is a file selection area with a text box containing '選擇檔案' and '尚未選取檔案'. A toggle switch for 'Whether to resume the factory configuration' is shown in the off position. A red warning icon and text state: 'Note: Do not power off during the process of upgrading the software'. An 'Upgrade' button is located at the bottom right.

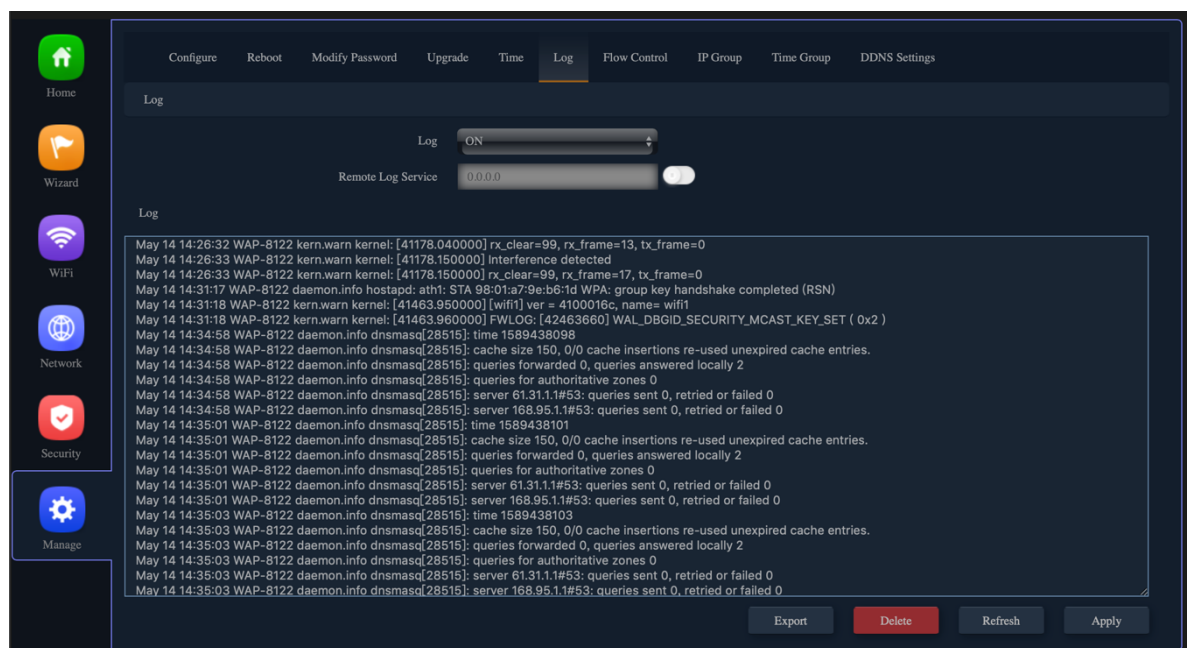
Time

Before sync with host, please select your Time zone. Get time from NTP server can only be available under Gateway and WISP Mode.



Log

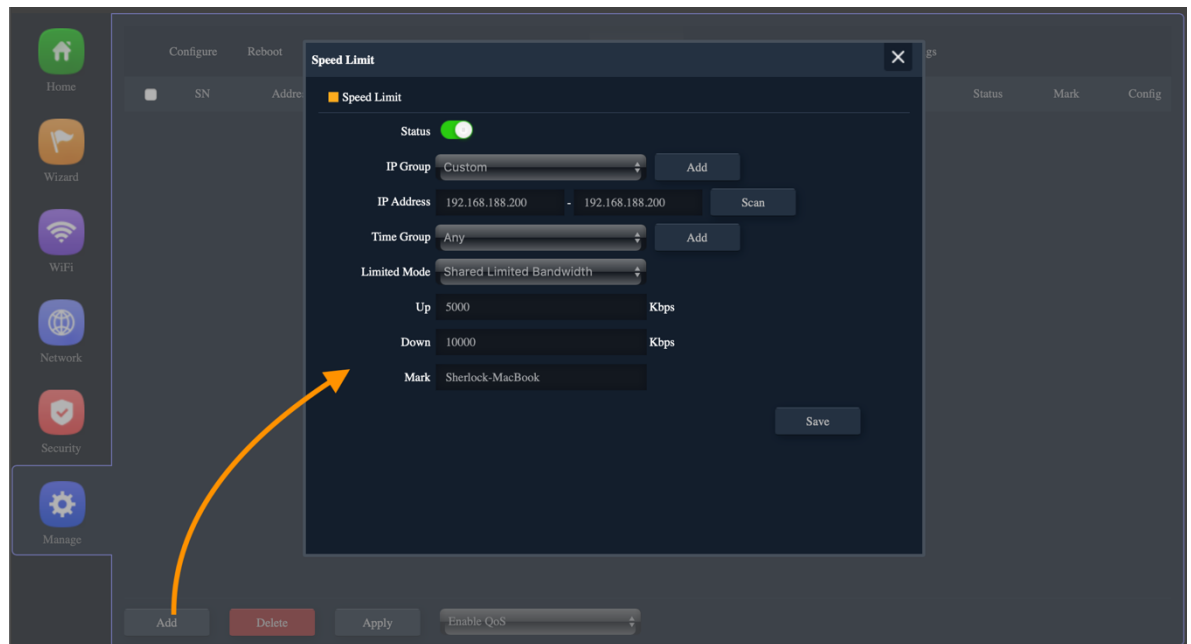
Can use Log to find errors to check the cause of the problem.



Flow Control

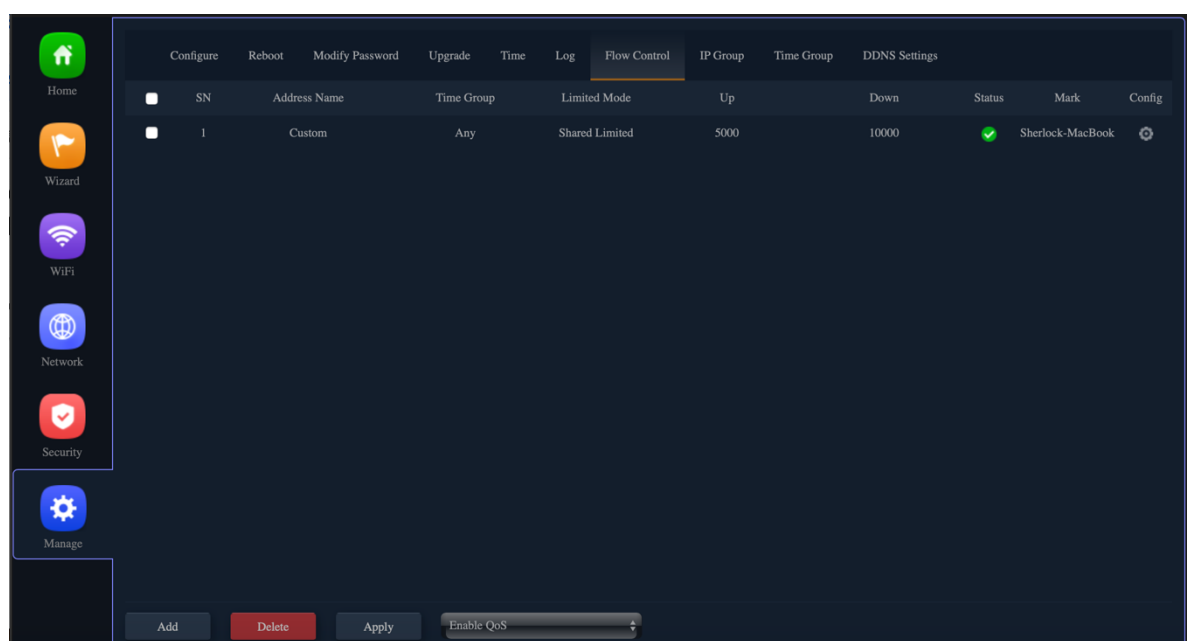
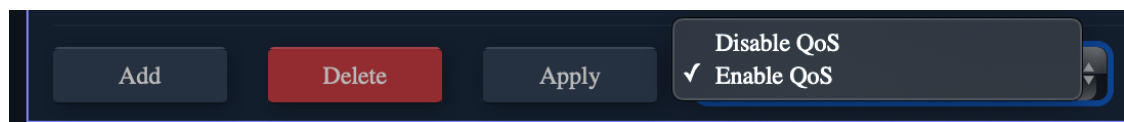
1. Can restrict Flow Control of specified device IP or IP Group.

- Shared limited bandwidth
- Exclusive limited bandwidth



2. Choose according to the current use needs. After selecting, please click Apply.

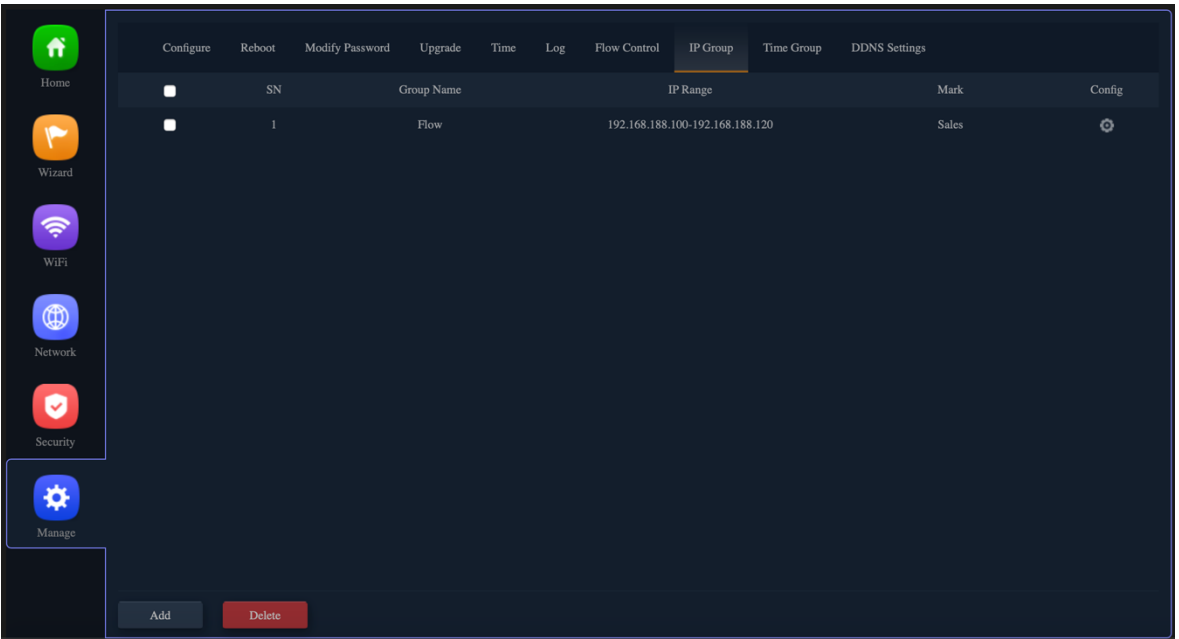
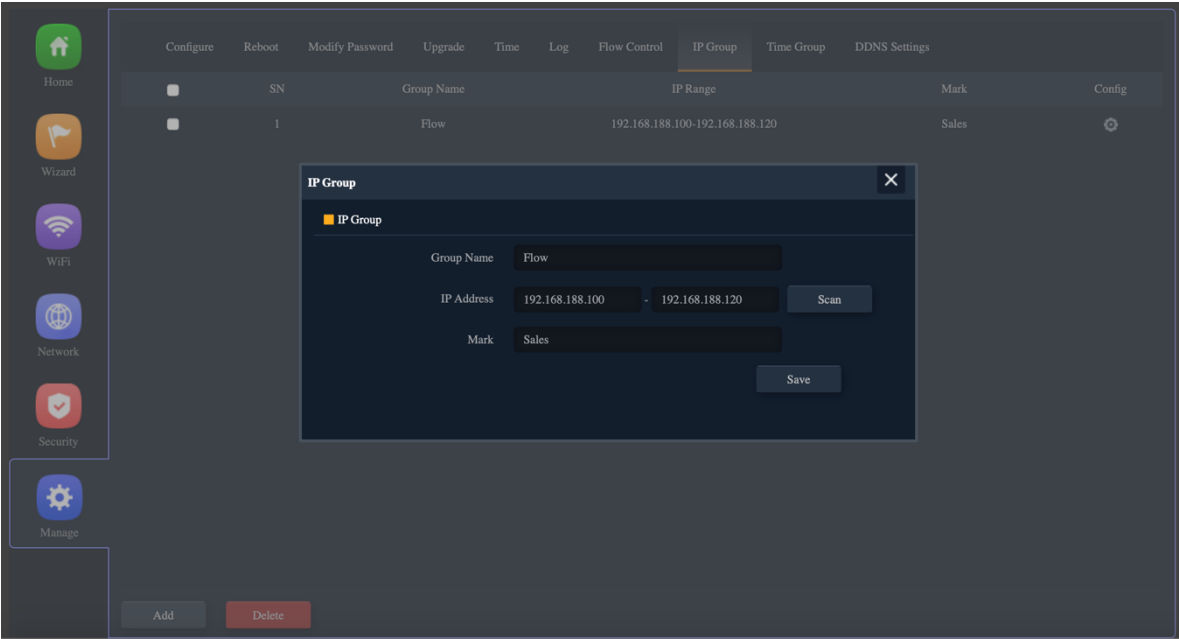
- Disable QoS
- Enable QoS



IP Group

Establish IP Group for easy management and can be applied to other functional options.

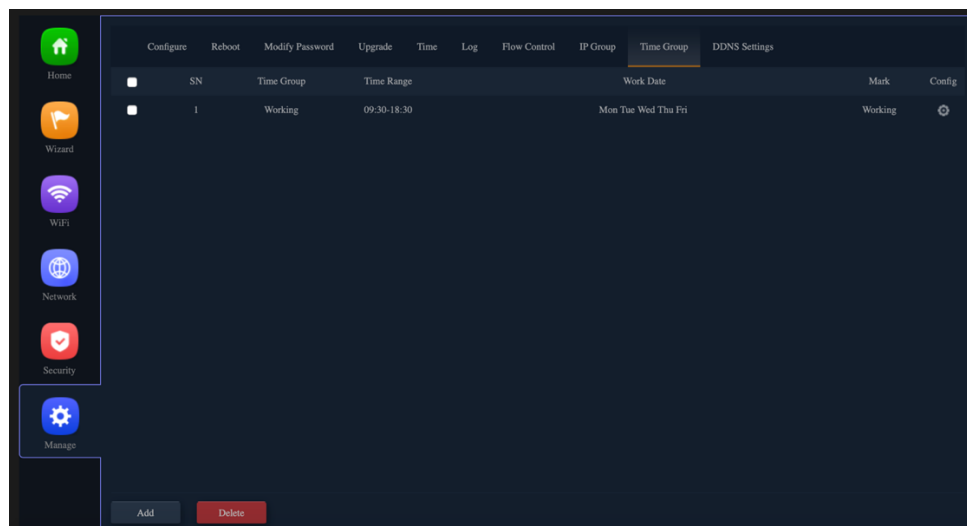
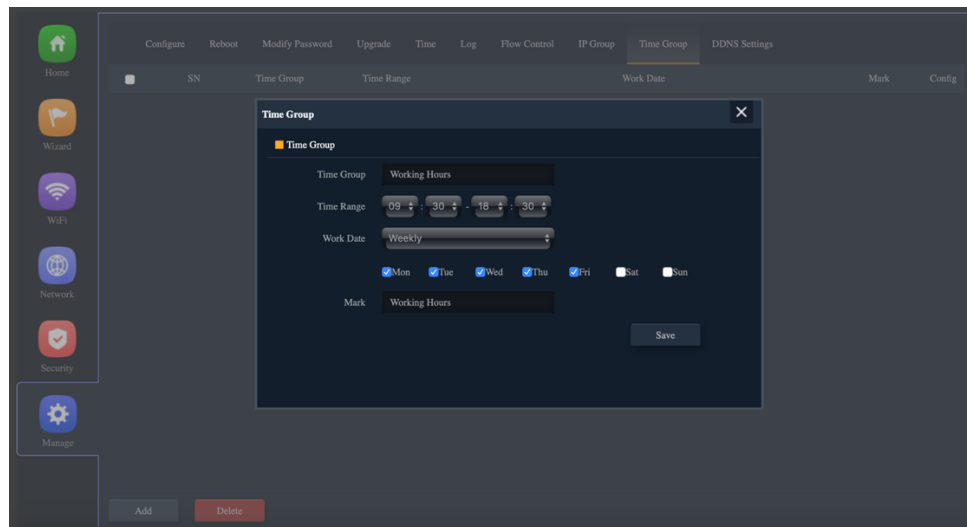
(Ex: Flow Control functional options)



Time Group

Establish time Group for easy management and can be applied to other functional options.

(Ex: Flow Control functional options)



DDNS Settings

For users not apply for an ISP fixed IP address, only Floating real IP address , you can also connect to the remote network device in through the DDNS service.

