

Web Management Guide



Digital Data Communications GmbH.

<http://www.level1.com>

Web Management Guide

WAB-5010

N300 5GHz Outdoor PoE Wireless Access Point

Contents

	Contents	4
	Default Settings	5
	Logging on to the equipment	5
Section I	Home	6
Section II	Wizard	8
	Repeater Mode	8
	AP Mode	13
Section III	WiFi	16
	5G WiFi	16
	MAC ACL	20
	WiFi Timer Off	24
	Advanced Setting	24
Section IV	Network	27
	LAN Settings	27
	VLAN Settings	27
Section V	Manage	28
	Configure	28
	Reboot	28
	Modify Password	29
	Upgrade	29
	Time	30
	Log	30

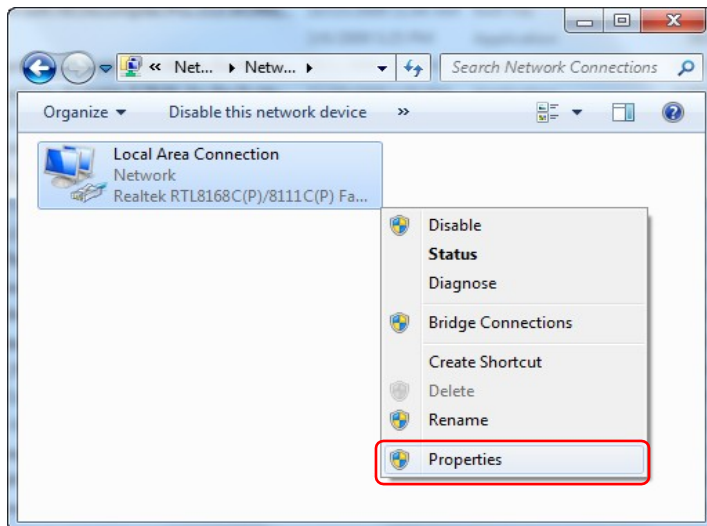
Default Settings

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.

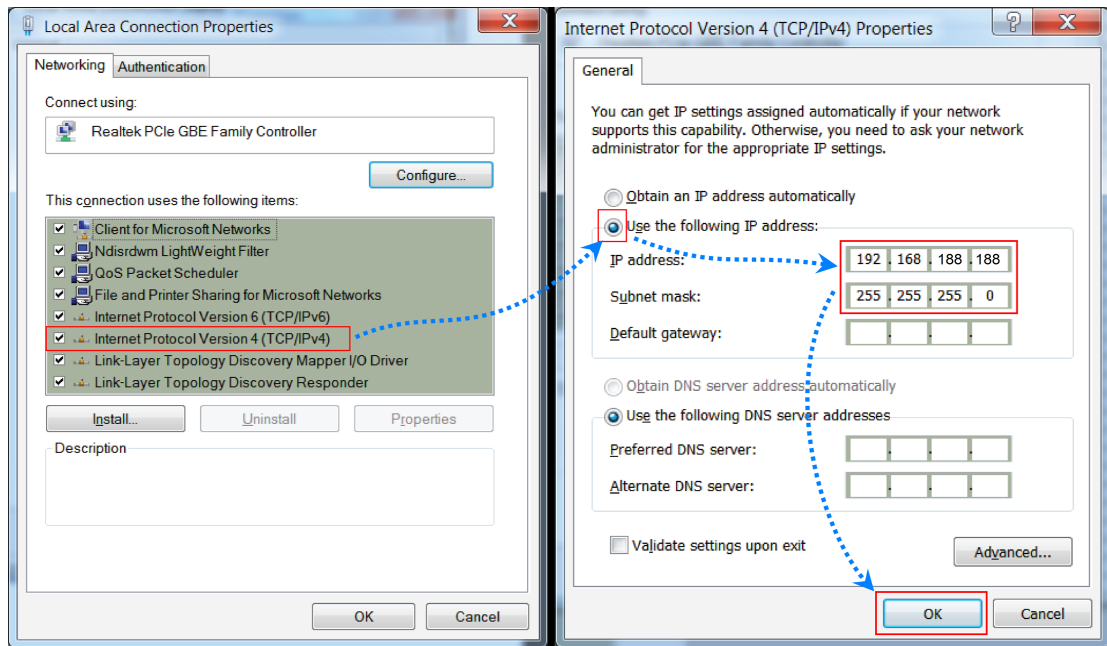
IP Address	192.168.188.253
Password	admin

Logging on to the equipment

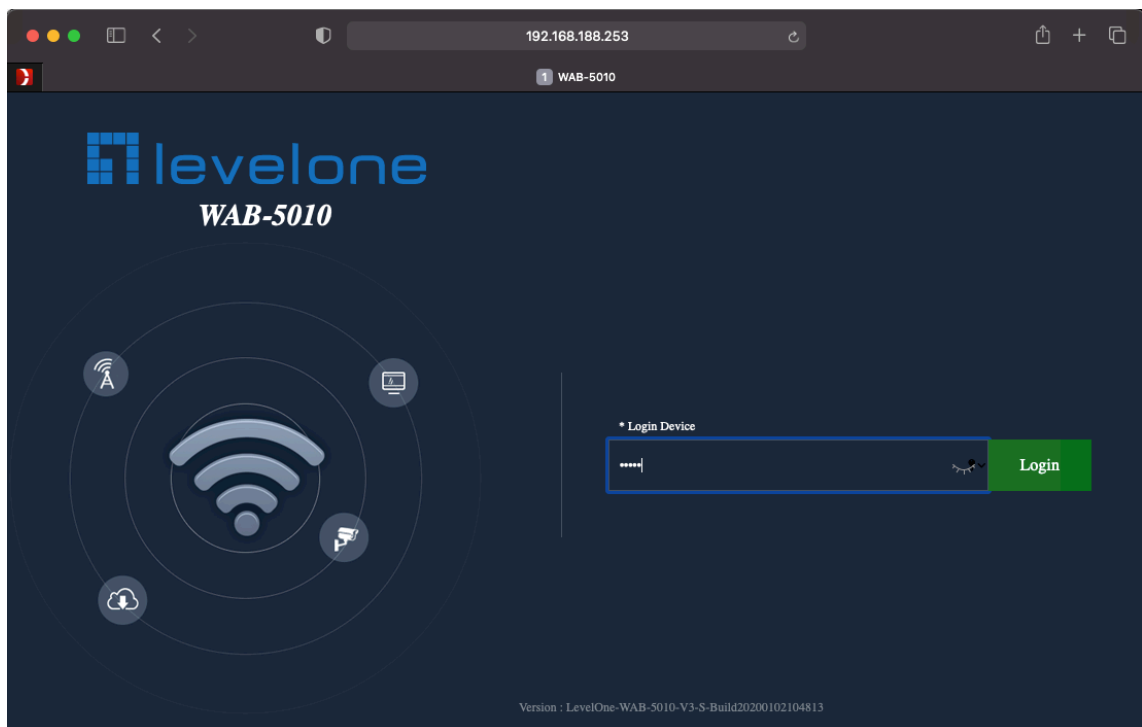
- Connect the RJ-45 interface cable of a switch with a computer using a network cable.
 - Set the TCP/IP properties of the computer.
- **Windows**
 1. Click **Start**→ **Control Panel**→ **Network and Internet**→ **Network and Sharing Center**→ **Change adapter settings**, right click **Local connection**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

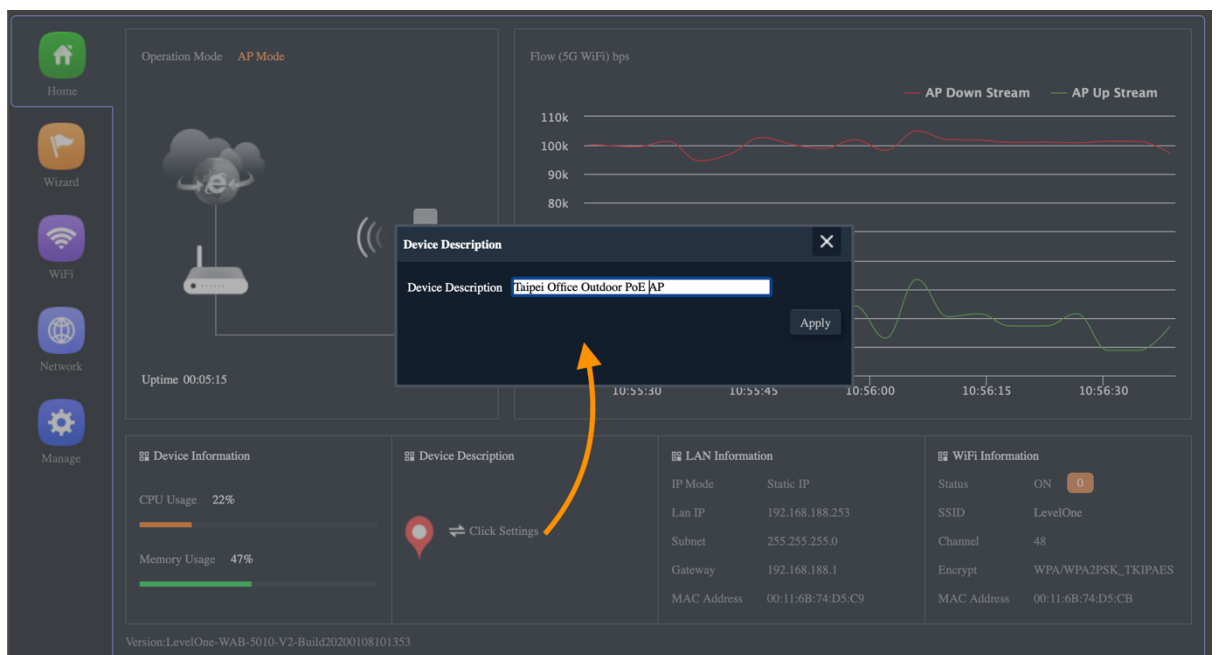


Section I Home

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.Can view the current wireless online users of 5G

Home


Wizard

WiFi

Network

Manage

Operation Mode **AP Mode**



Uptime 00:13:06

Device Information

CPU Usage 15%

Memory Usage 70%

Device Description

Taipei Office Outdoor PoE AP

Click Settings

LAN Information

IP Mode Static IP

Lan IP 192.168.188.253

Subnet 255.255.255.0

Gateway 192.168.188.1

MAC Address 00:11:6B:74:D5:C9

WiFi Information

Status ON

SSID LevelOne 5GHz

Channel 48

Encrypt WPA/WPA2PSK_TKIP/AES

MAC Address 00:11:6B:74:D5:CB

Version:LevelOne-WAB-S010-V2-Build20200108101353

Client List

SN	Name	MAC Address	Signal	Connect Time
1	MiMIX3-Phone	00:11:6B:74:D5:C9	-43dBm	00:00:16

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 2 operation mode including Repeater/AP Mode. Please confirm the operation mode first before configuration starting.

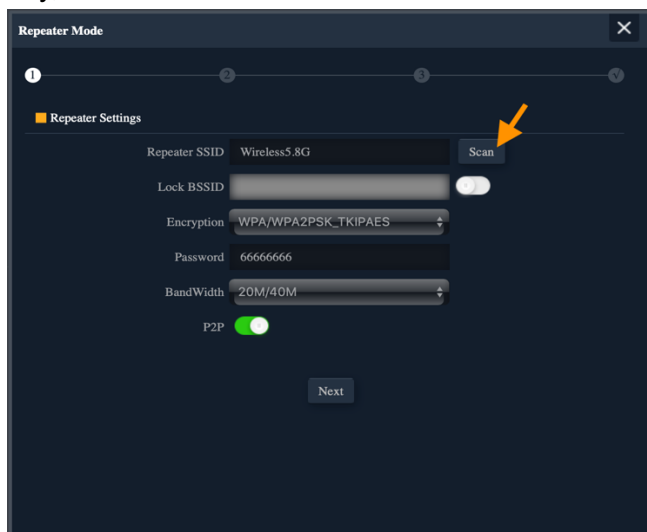


Repeater mode

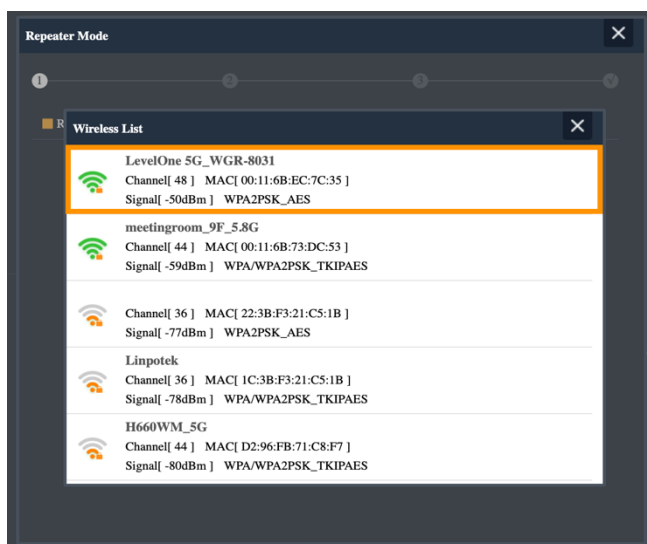
In the Repeater mode, WAB-5010 extends your wireless network coverage and provides you with higher quality wireless radio signal. The NAT, firewall, and IP sharing services are disabled.



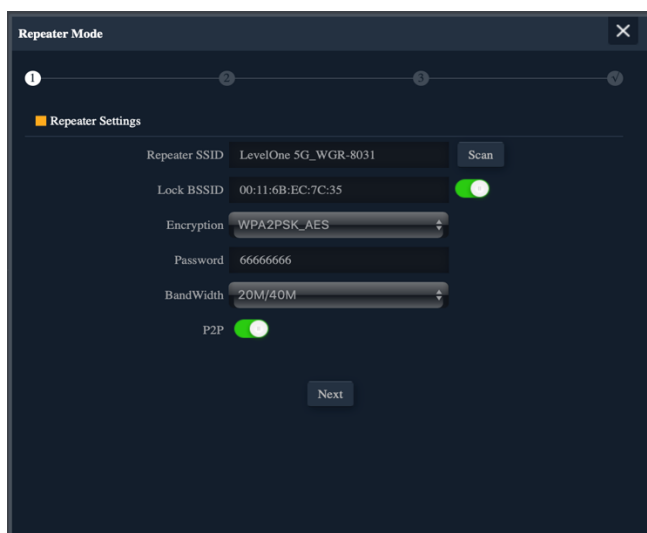
1. Can choose to relay the front-end 5G wireless signal to extend the wireless signal range. Select the AP's SSID want to Repeater, take "wireless 5G" for example, then input the AP's key, click Scan AP



2. Please select WIFI SSID to connect



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



4. In addition to relaying wireless signals at the front end, you can also choose whether to activate another wireless signal to isolate the LAN side for wireless connection.

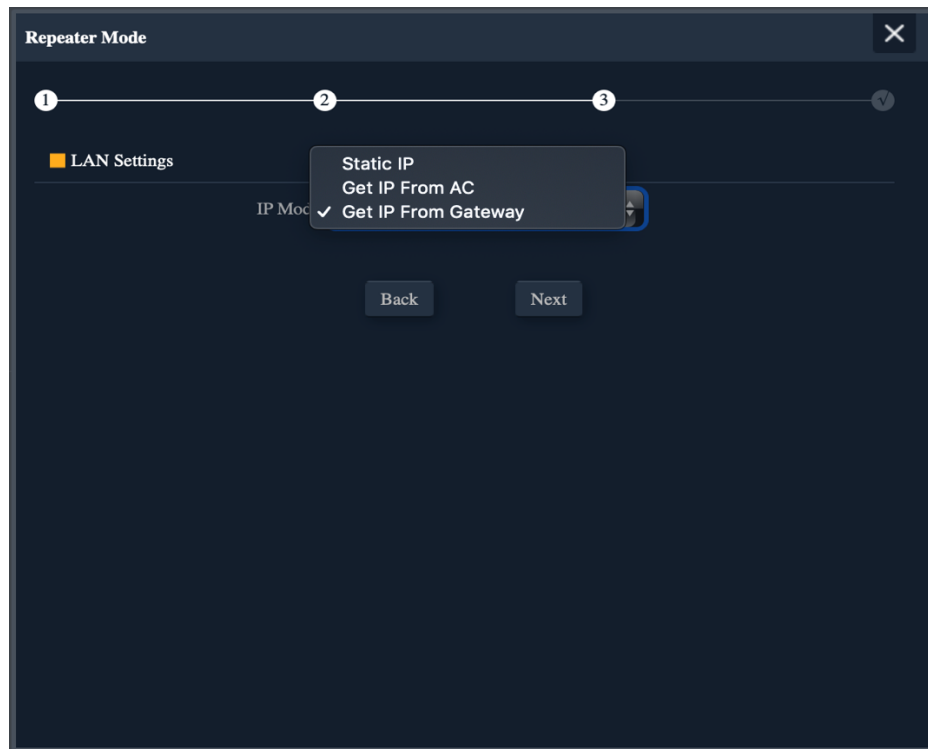
The screenshot shows the 'Repeater Mode' configuration window. At the top, a progress bar has four steps: 1 (active), 2, 3, and 4 (completed). Below the progress bar is the title '5G WiFi Setting'. The 'WiFi Status' toggle switch is turned off (grey). The 'SSID' field contains 'LevelOne 5GHz'. The 'Hide your SSID ?' toggle switch is turned off (grey). The 'Encrypt' dropdown menu is set to 'Auto Encryption'. The 'WiFi Password' field contains '66666666'. The 'Timing' dropdown menu is set to '1Day'. At the bottom, there are 'Back' and 'Next' buttons.

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

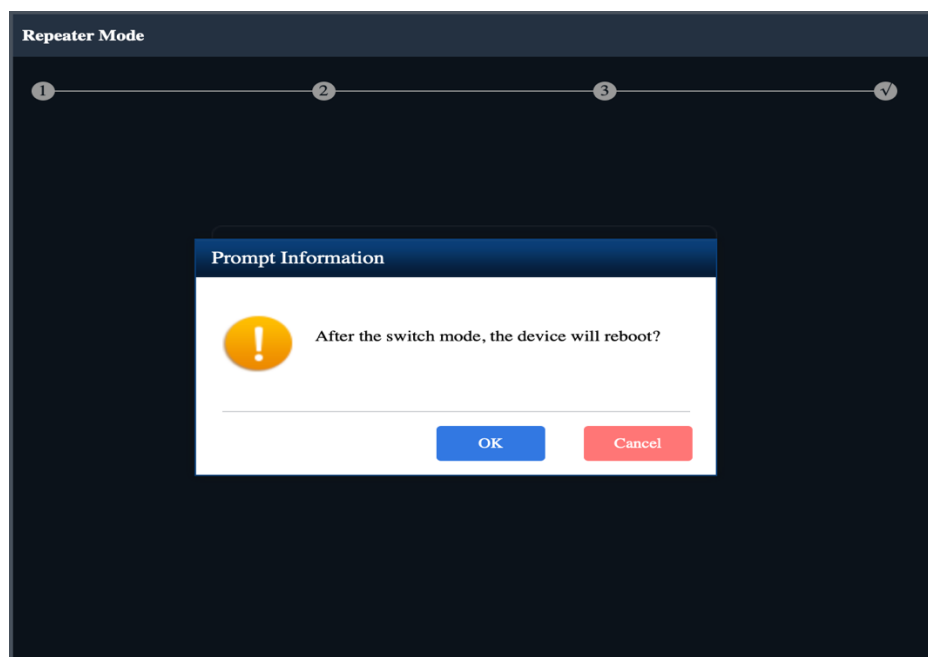
This screenshot is identical to the one above, showing the 'Repeater Mode' configuration window. The only difference is that the 'WiFi Status' toggle switch is now turned on (green), indicating that the 5G wireless broadcast is enabled.

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

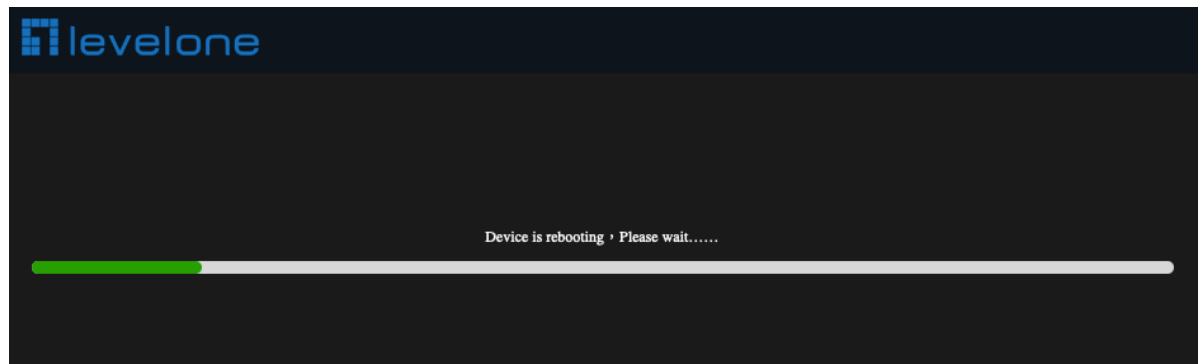
- a) If the front-end wireless signal is Static IP, you can click "Static IP" to set an unused IP address.
- b) If the front-end assigned DHCP IP address by the controller WAC-2000 / WAC-2003, you can click "Get IP From AC"
- c) If the Router of the front-end will automatically assign an IP address,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



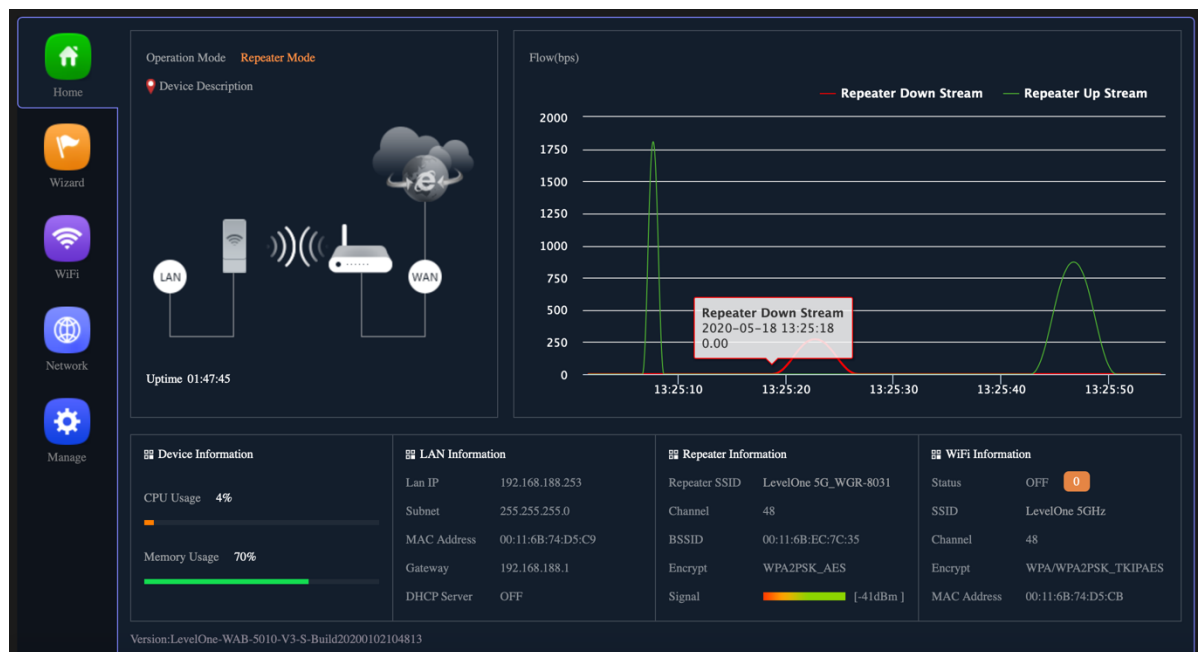
7. Please click the ok button, After the switch mode, the device will reboot



8. Please wait more than 20 seconds

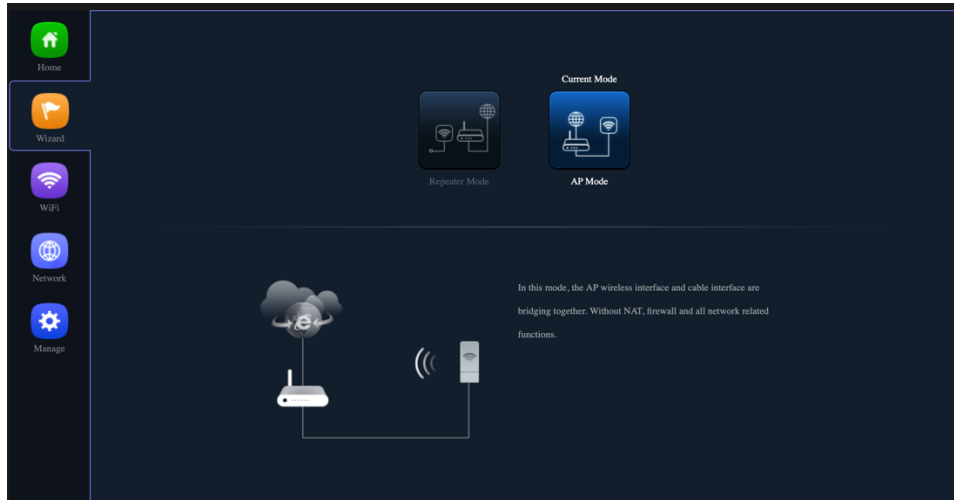


9. Please log in again ,This page will show the connection Repeater mode status



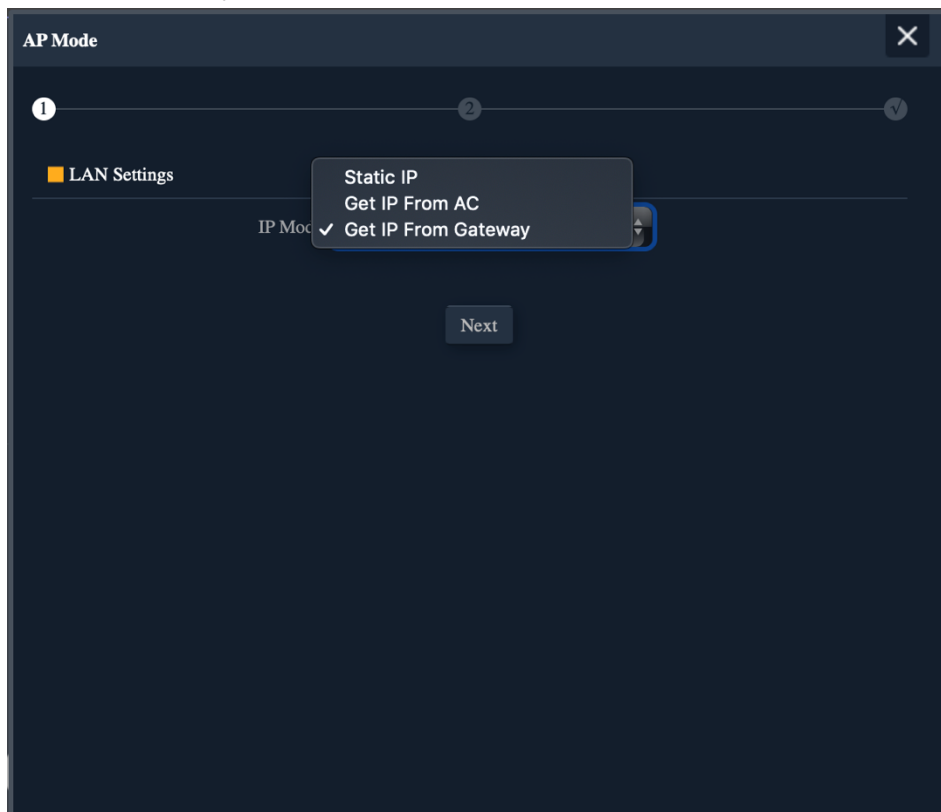
AP Mode

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

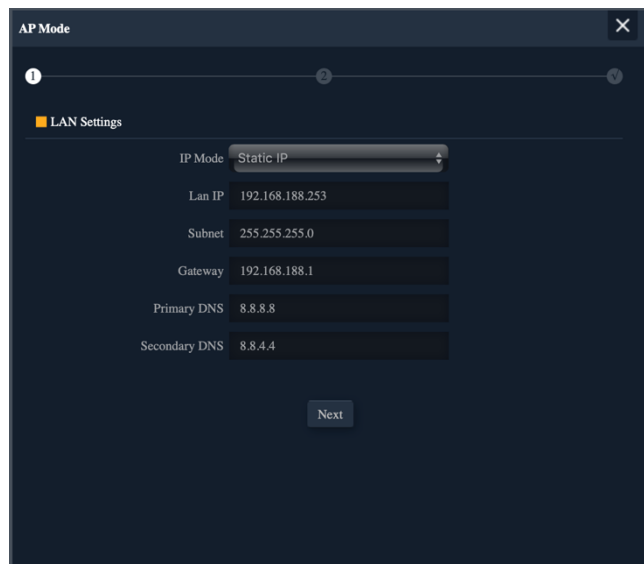


1.Set according to LAN environmental requirements :

- 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 assigned DHCP IP address by the controller WAC-2000 / WAC-2003, you can click "Get IP From AC"
- c) If the Router of the front-end will automatically assign an IP address, you can click "Get IP From Gateway"



2.Static IP setting



AP Mode

1 2 3

LAN Settings

IP Mode: Static IP

Lan IP: 192.168.188.253

Subnet: 255.255.255.0

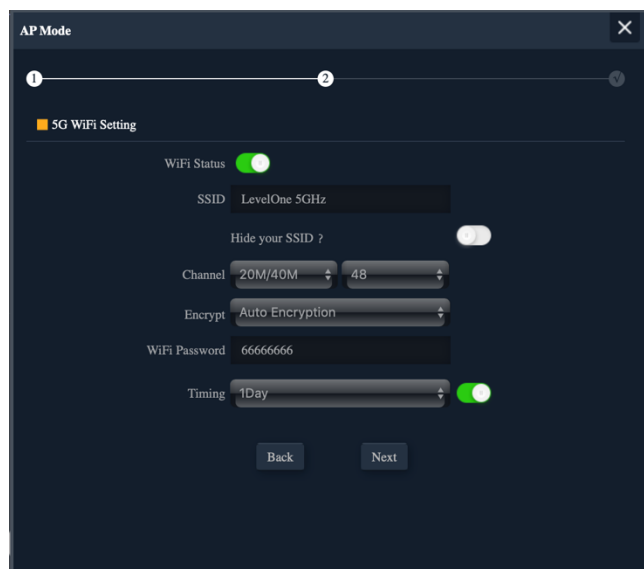
Gateway: 192.168.188.1

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

Next

3.Configure the 5G Wireless SSID and password



AP Mode

1 2 3

5G WiFi Setting

WiFi Status: ☒

SSID: LevelOne 5GHz

Hide your SSID?: ☐

Channel: 20M/40M 48

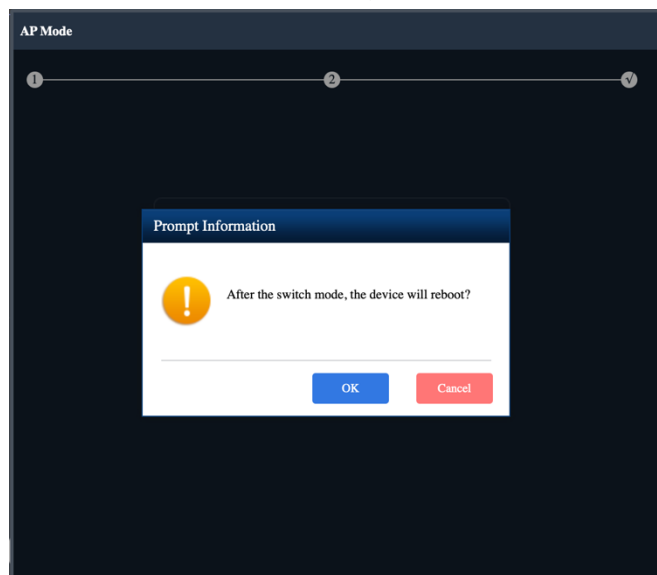
Encrypt: Auto Encryption

WiFi Password: 66666666

Timing: 1Day ☒

Back Next

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



AP Mode

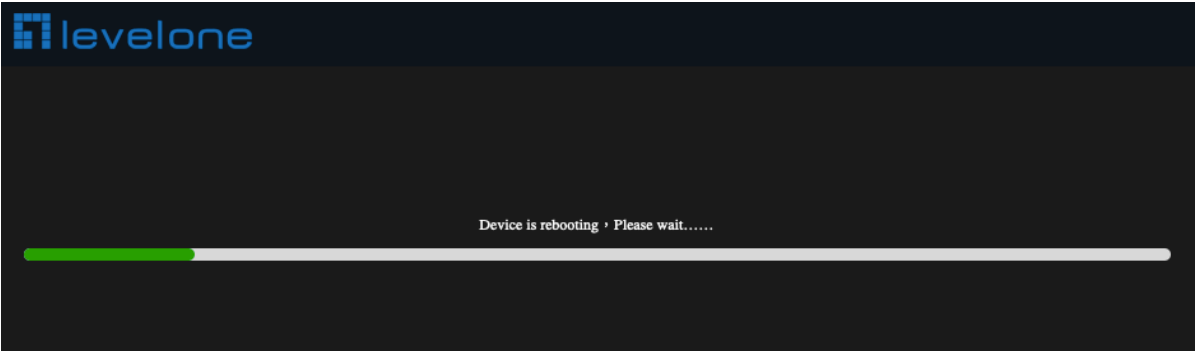
1 2 3

Prompt Information

! After the switch mode, the device will reboot?

OK Cancel

5.Please wait more than 20 seconds



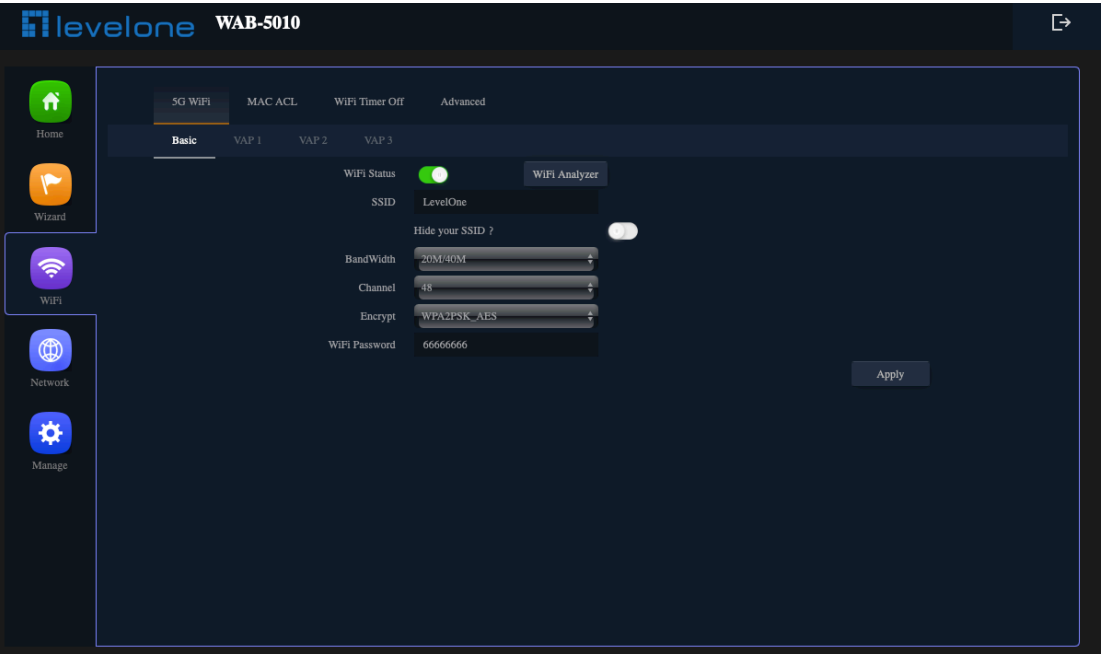
7.Check AP Mode Status

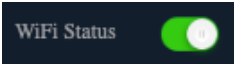
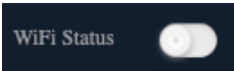
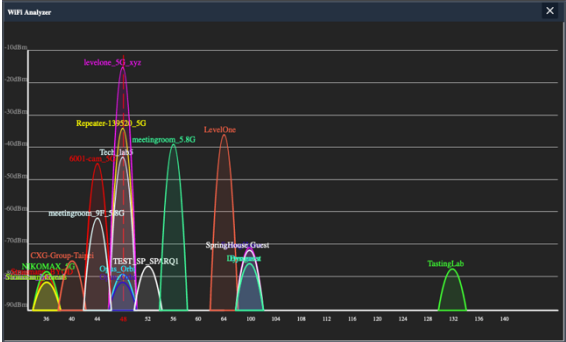


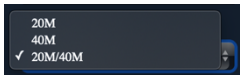
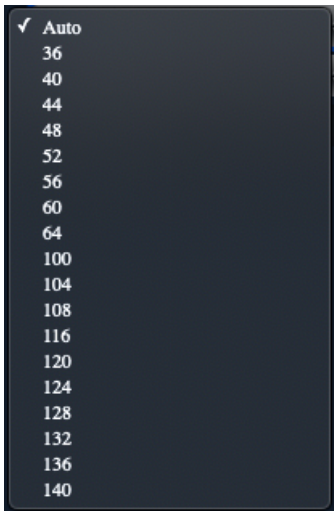
Section III WiFi

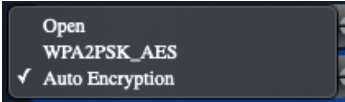
Basic (5G WiFi)

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



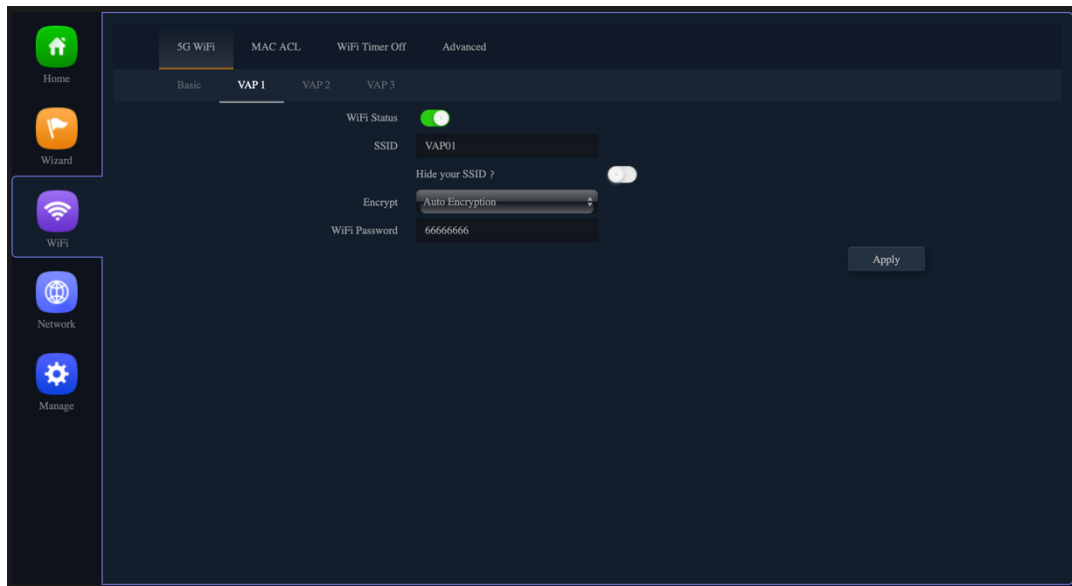
Basic Features Description	
WiFi Status	5GHz WiFi on / off  
	WiFi Analyzer : Wireless analyzer Look for Unoccupied channel (5GHz) 

SSID	Custom 5GHz 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>

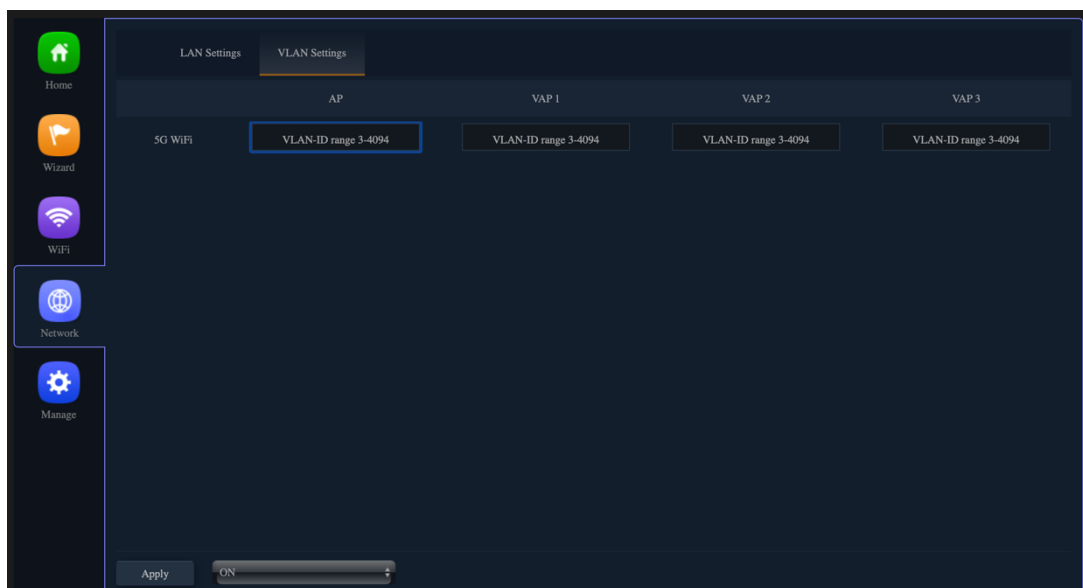
VAP1/ VAP2/ VAP3 (5G WiFi)

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**.

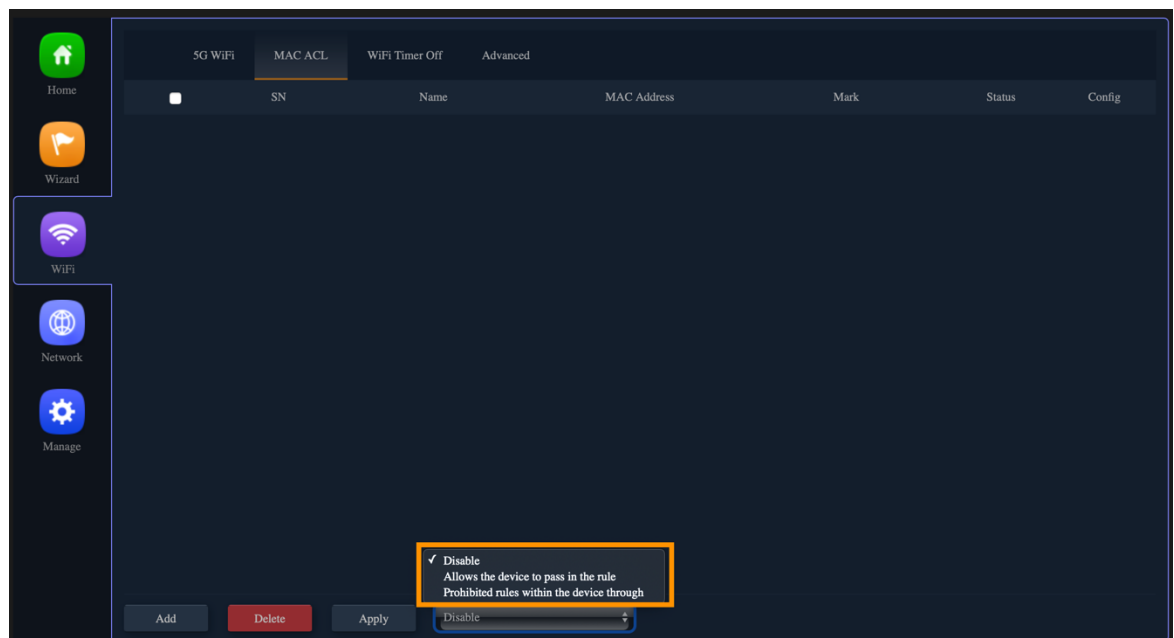


MAC ACL

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.

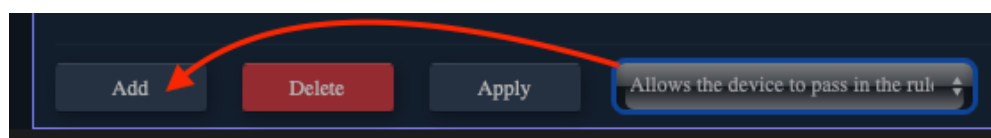
There are 3 types of MAC ACL rules, listed below

- 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)

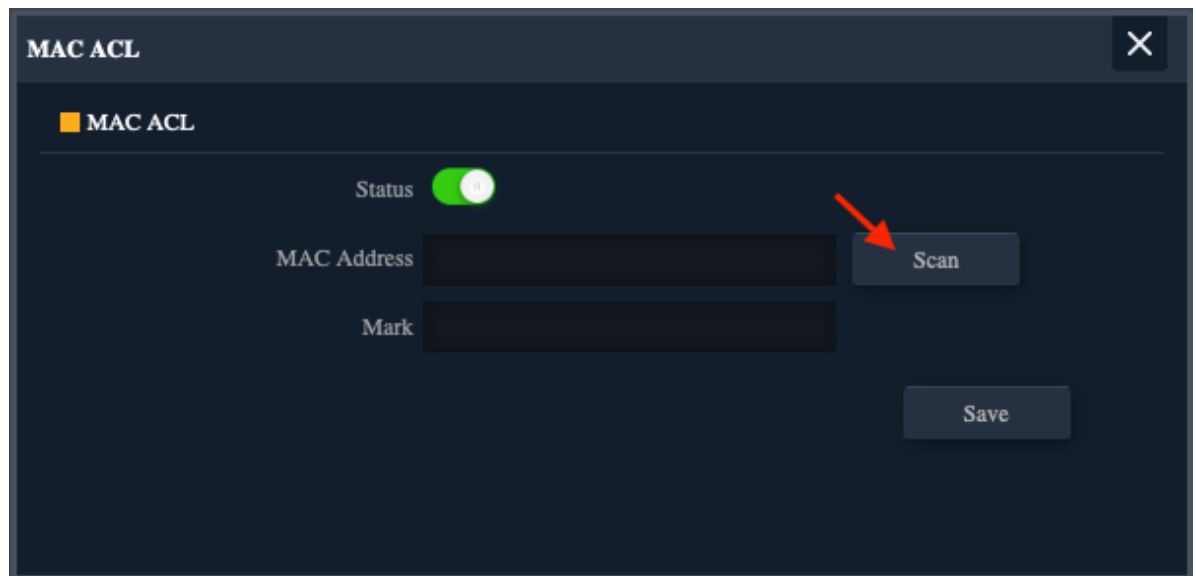


The following will demonstrate the "Allows the device to pass in the rule" setting

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 with a red arrow. Below the 'Mark' field is a 'Save' button.

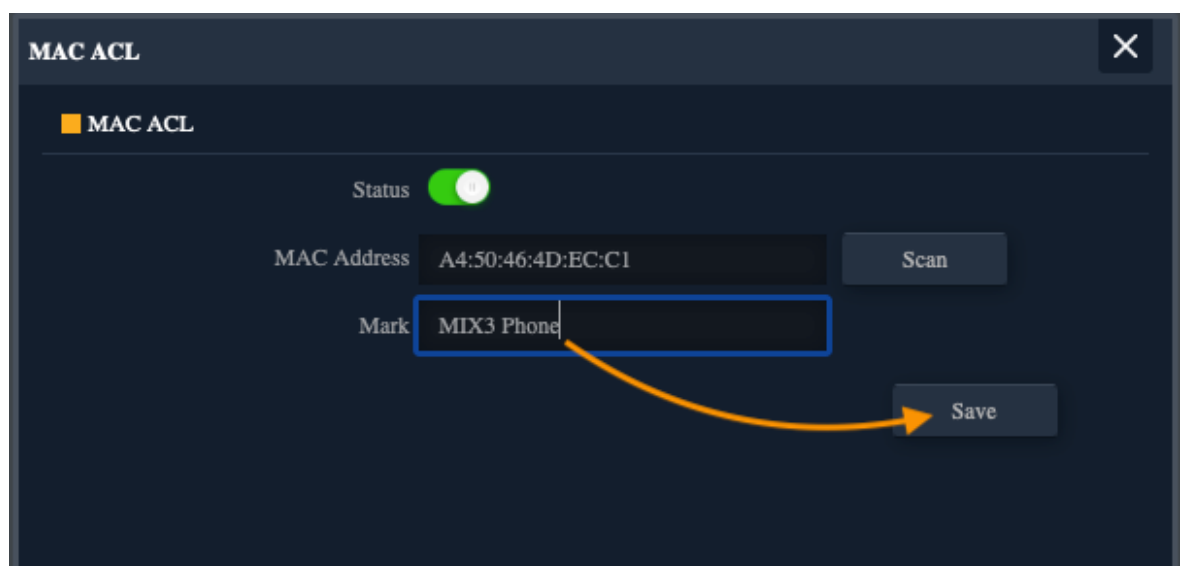
Click the MAC ID of the device to be whitelisted



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'. There are two rows of data. The second row is highlighted with a red rectangle.

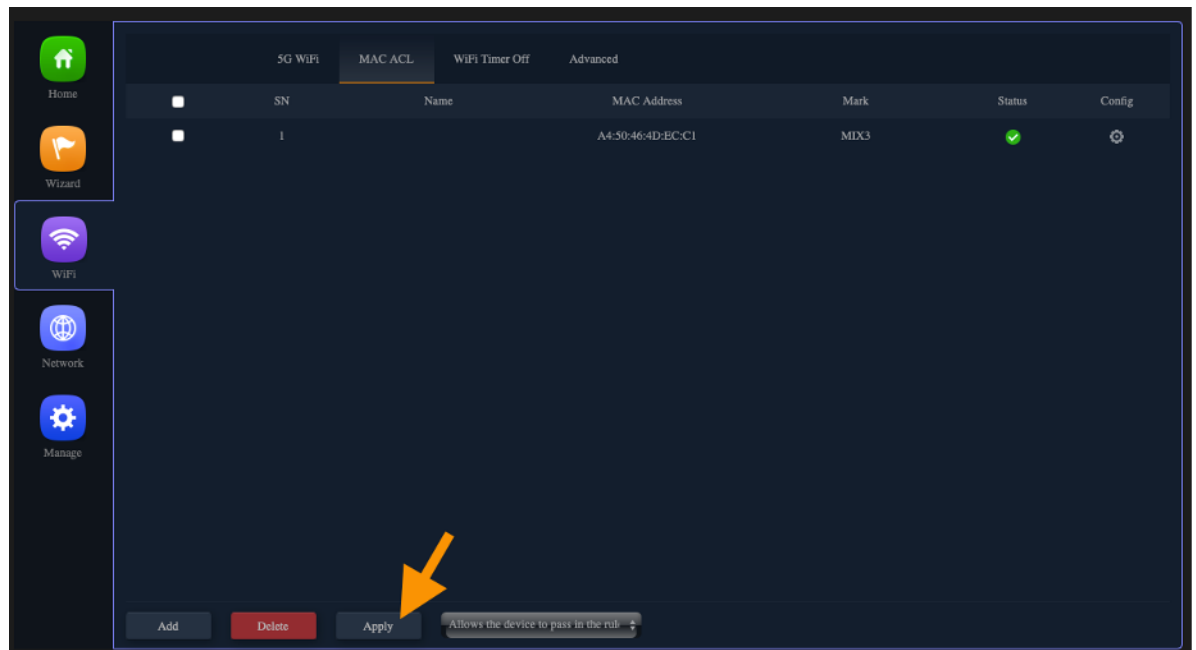
SN	Name	MAC Address	Connect Time
1		16:11:6B:74:D5:CB	00:59:49
2		A4:50:46:4D:EC:C1	00:02:54

Custom Mark



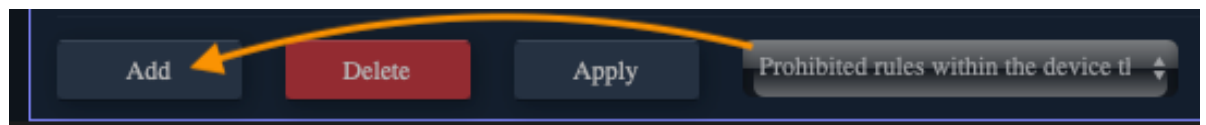
The image shows the 'MAC ACL' configuration window. The 'Status' toggle switch is turned on. The 'MAC Address' field is filled with 'A4:50:46:4D:EC:C1'. The 'Mark' field is filled with 'MIX3 Phone'. An orange arrow points from the 'Mark' field to the 'Save' button.

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

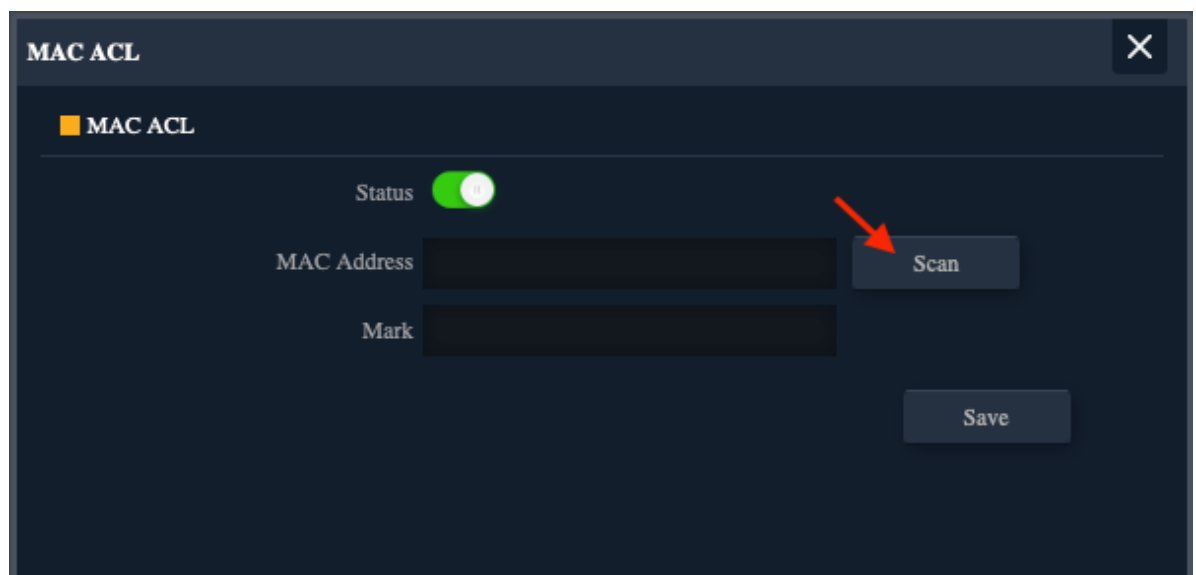


The following will demonstrate the "Prohibited rules within the device through" setting

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



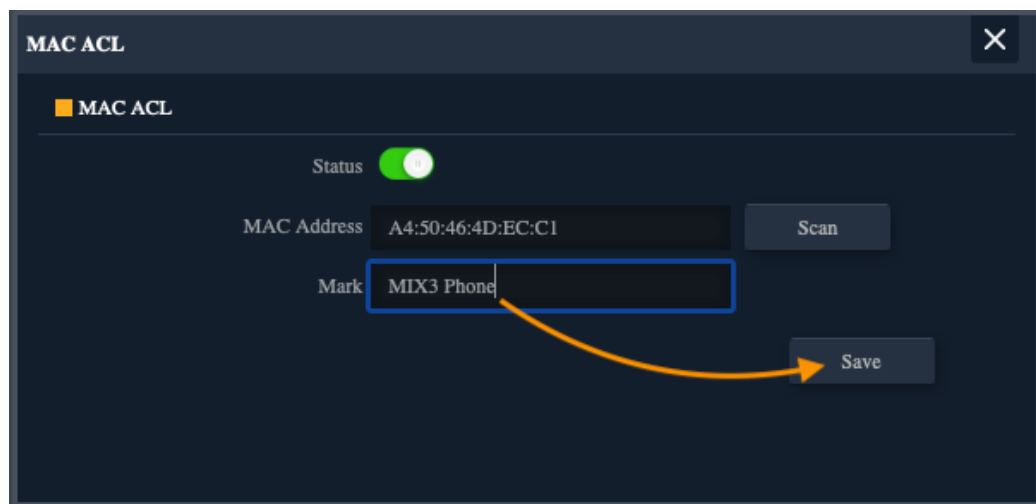
Click Scan



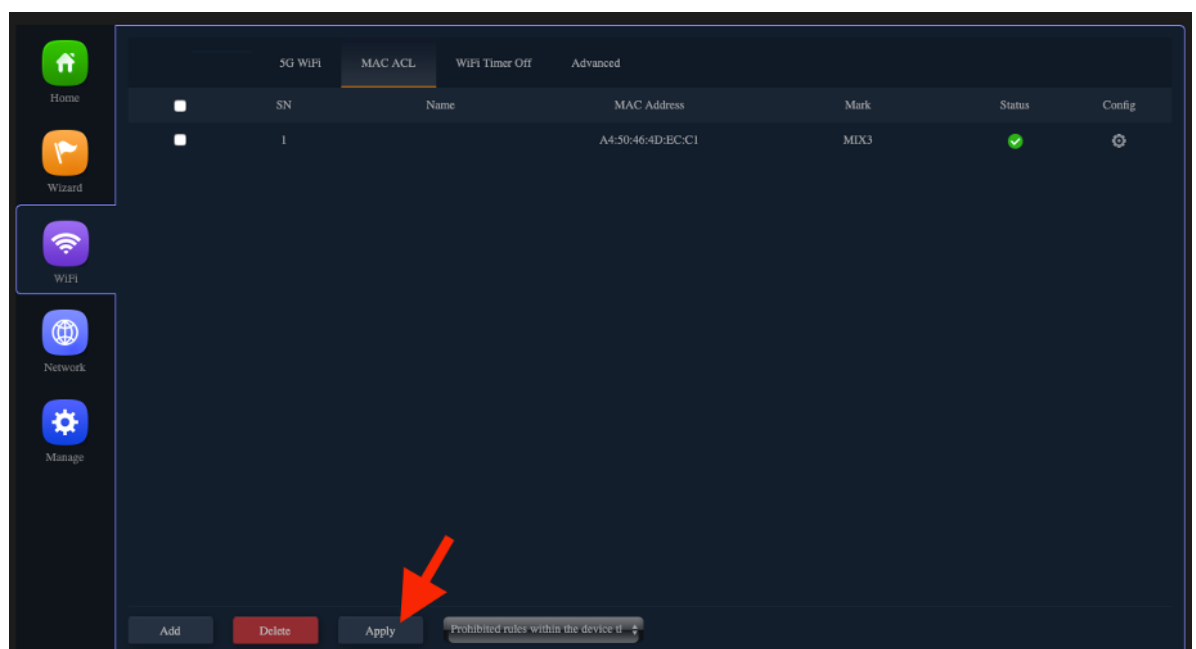
Click the MAC ID of the device to be whitelisted



Custom Mark

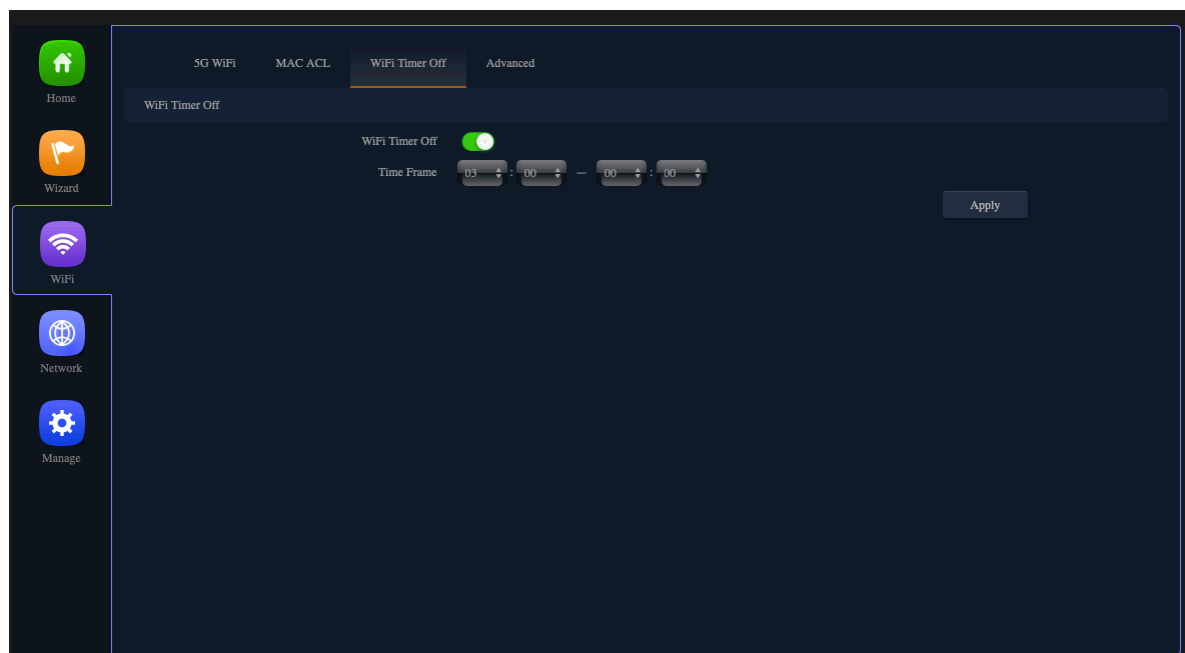


Click Apply, Only the MAC ID devices in this list cannot connect normally



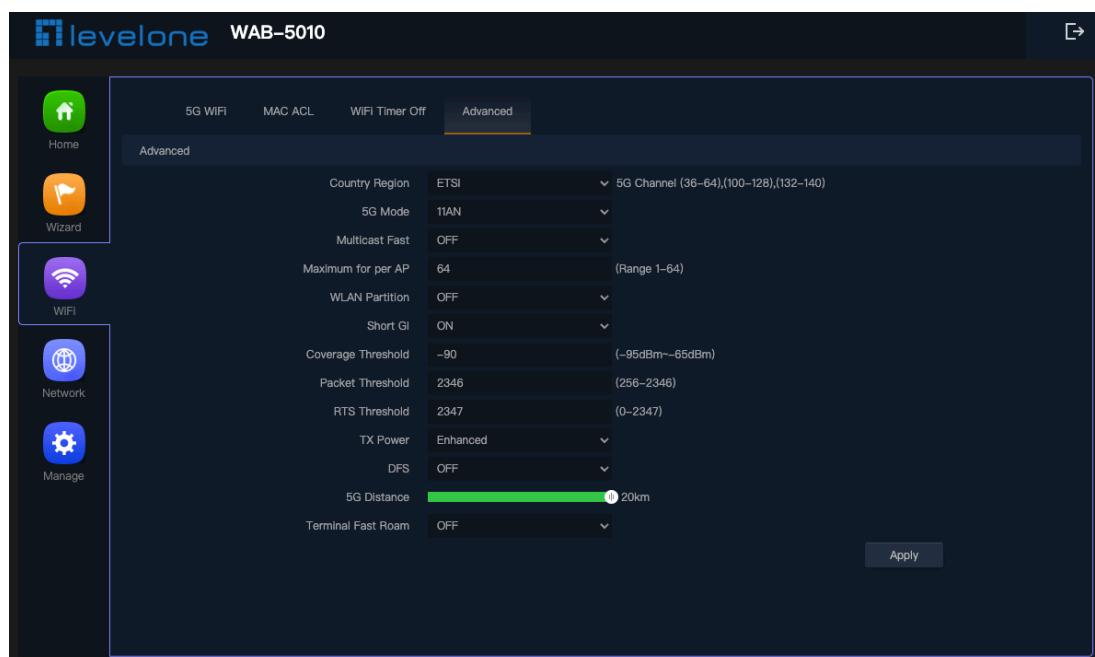
WiFi Timer Off

You can customize the AP device restart time range

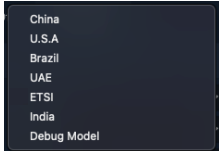

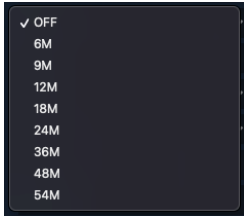


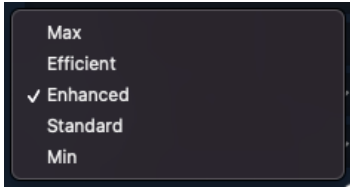
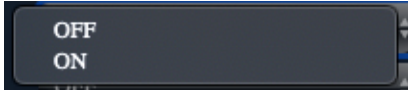
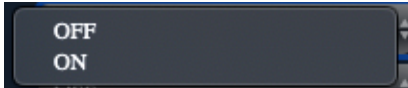
Advanced Setting

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> 
5G Mode	<p>11A / AN 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><i>Short GI(Short Guard Interval)</i></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.</p>
Packet Threshold	<p>This value should be left at the default value of 2346. If you are 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</p>

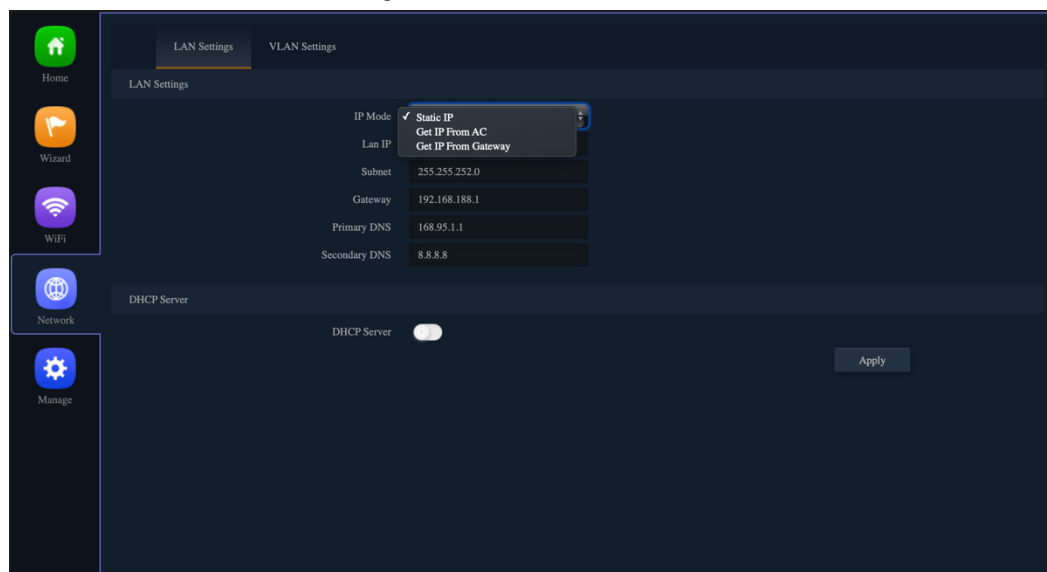
	performance.
RTS Threshold	This value should be left at the default value of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 256-2347 are recommended.
TX Power	<p>The less TX Power you set can save the electronic power, but comparatively reduce the range of the wireless signal of AP. according to local national Radio frequency power regulations,</p> <p>To comply effective isotropic radiated power (EIRP) <20dBm, Please click Standard mode</p> 
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> 
5G Distance	The radio frequency distance of 5G signal can be adjusted according to requirements (0-20km)
Terminal Fast Roam	<p>After opening, Wireless roaming for multiple APs, you need to set the same WiFi SSID / WiFi PASSWORD (Not supports 802.11k/v/r)</p> 

Section IV Network

(For AP/Repeater Mode)

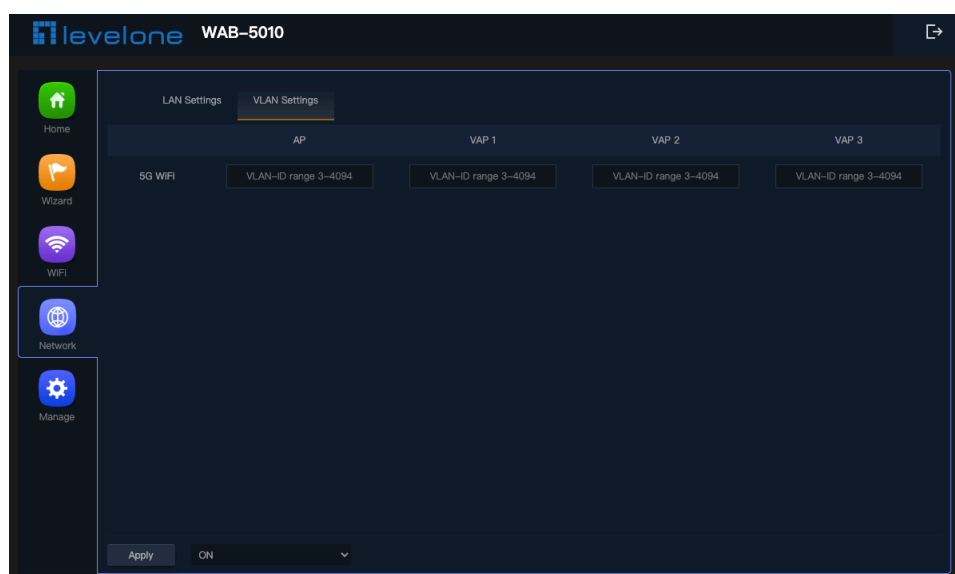
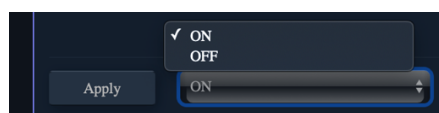
LAN Settings

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.



VLAN Settings

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

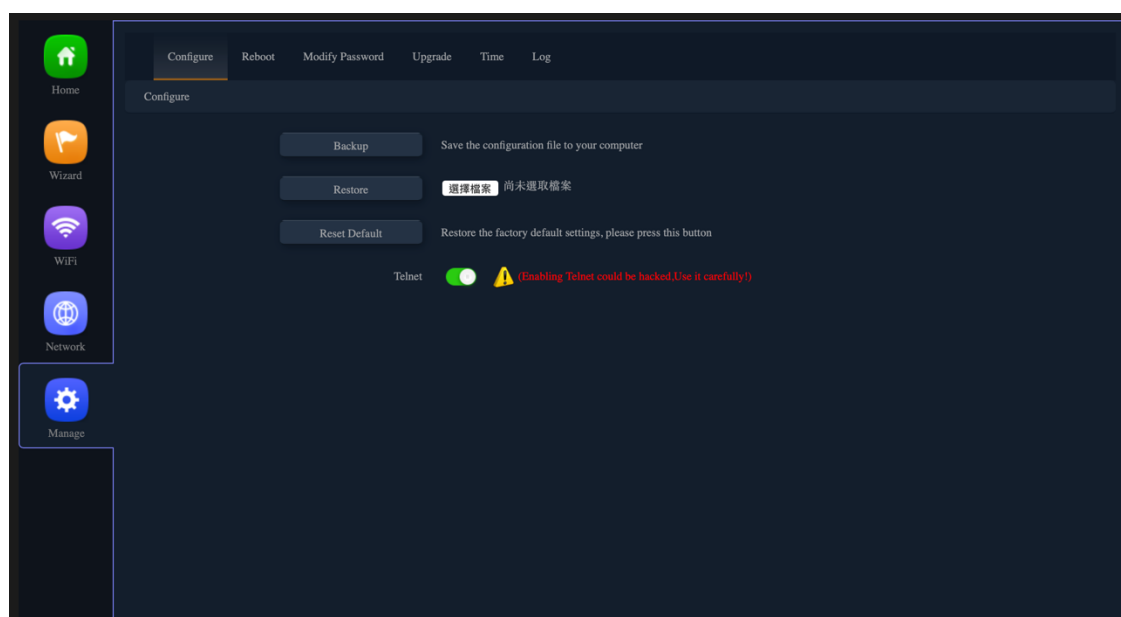


Section V Manage

(For AP/Repeater Mode)

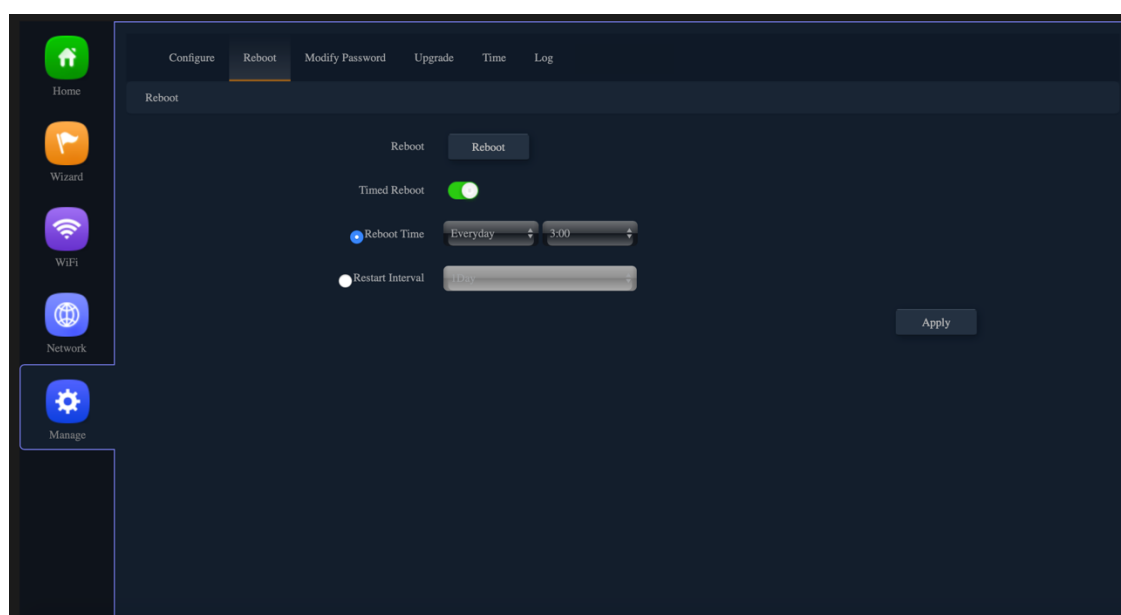
Configure

- 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 content 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

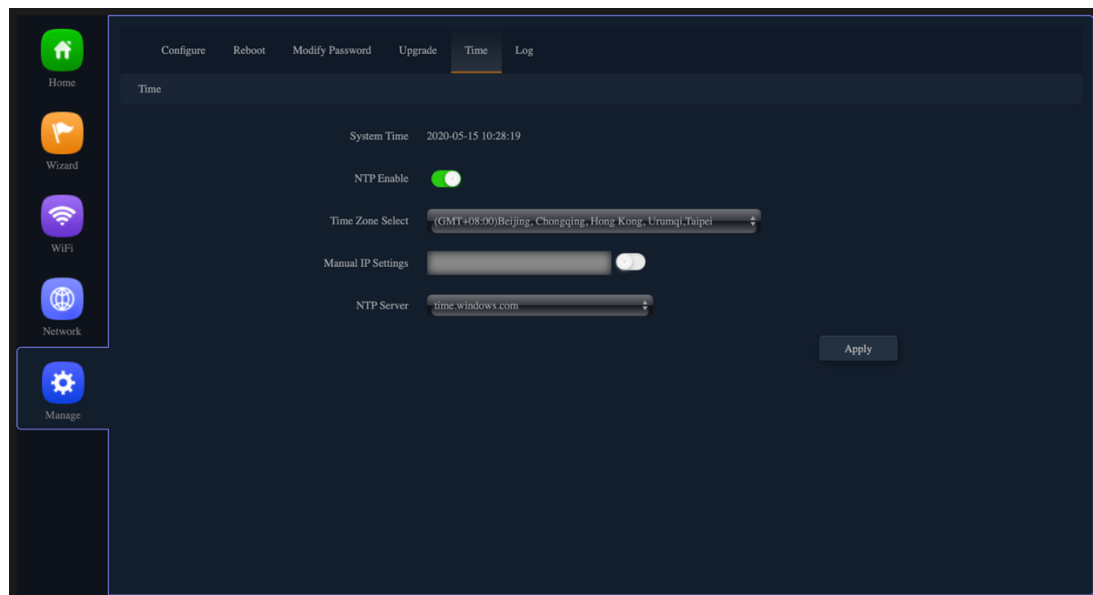
You can browse the new firmware in your computer and upgrade. Please do not power off the device during upgrade.

**(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 content area has the title 'Upgrade'. It displays the firmware version: 'Version:LevelOne-WAB-5010-V3-S-Build20200102104813'. Below this is a file selection area with a button labeled '選擇檔案' (Select File) and the text '尚未選取檔案' (No file selected). There is a toggle switch for 'Whether to resume the factory configuration'. A red 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.

