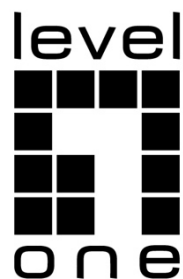


Web Management Guide

(WAP-8131)



Web Management Guide

WAP-8131

AX1800 Dual Band Wi-Fi 6 PoE Wireless Access Point

Contents

	Contents	3
	Default Settings	5
	Logging on to the equipment	5
Section I	Home	6
Section II	Wizard	9
	Gateway Mode	9
	Repeater Mode	15
	AP Mode	19
Section III	WiFi	22
Section IV	Network (for AP / Repeater Mode)	38
Section V	Manage (for AP / Repeater Mode)	39
Section VI	Network (for Gateway Mode)	43
Section VII	Firewall (for Gateway Mode)	45
Section VIII	Manage (for Gateway Mode)	55

Default Settings

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

Note: WAP-8131 cannot be managed with Wireless LAN Controller (WAC-2000 / WAC-2003)

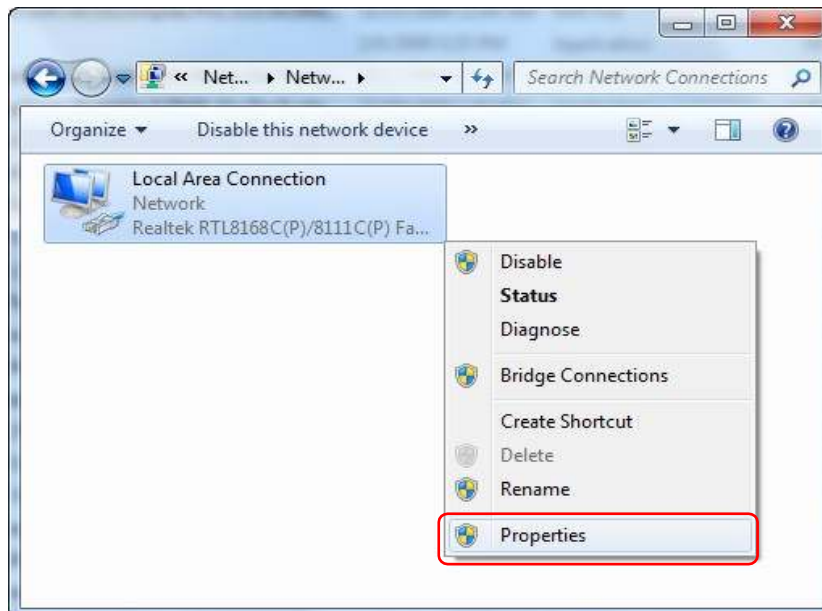
IP Address	192.168.188.253
Password	admin

Logging on to the equipment

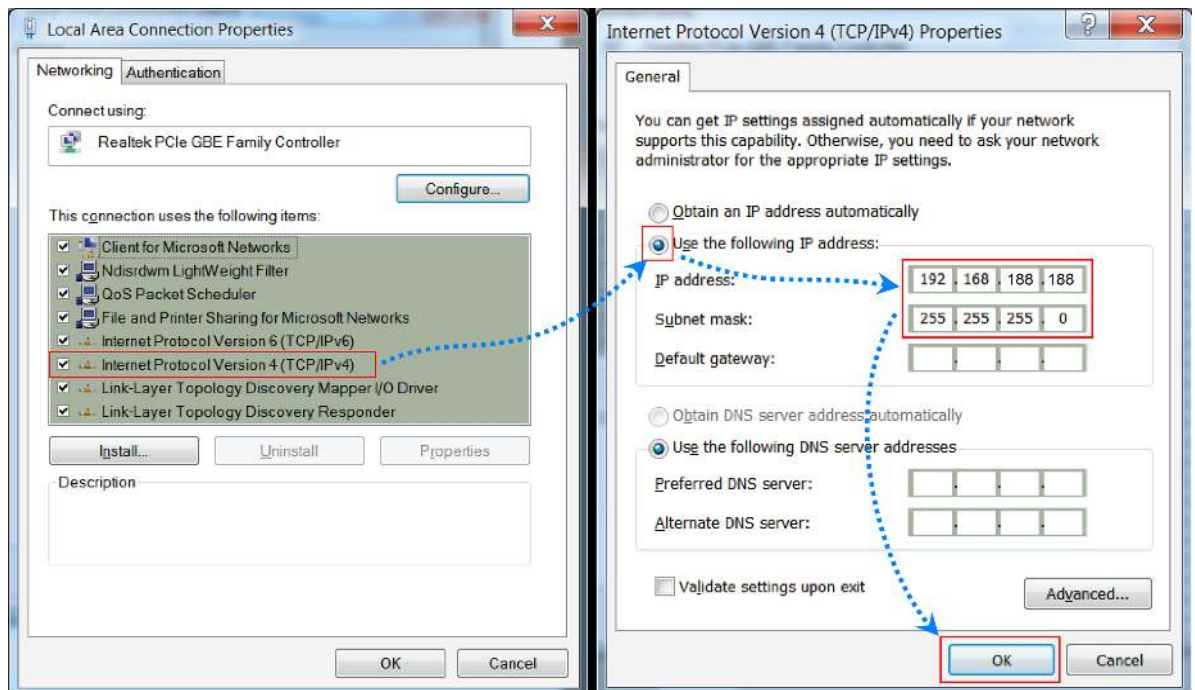
- Connect the RJ-45 interface cable of a switch with a computer using a network cable.
- Set the TCP/IP properties of the computer.

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**.



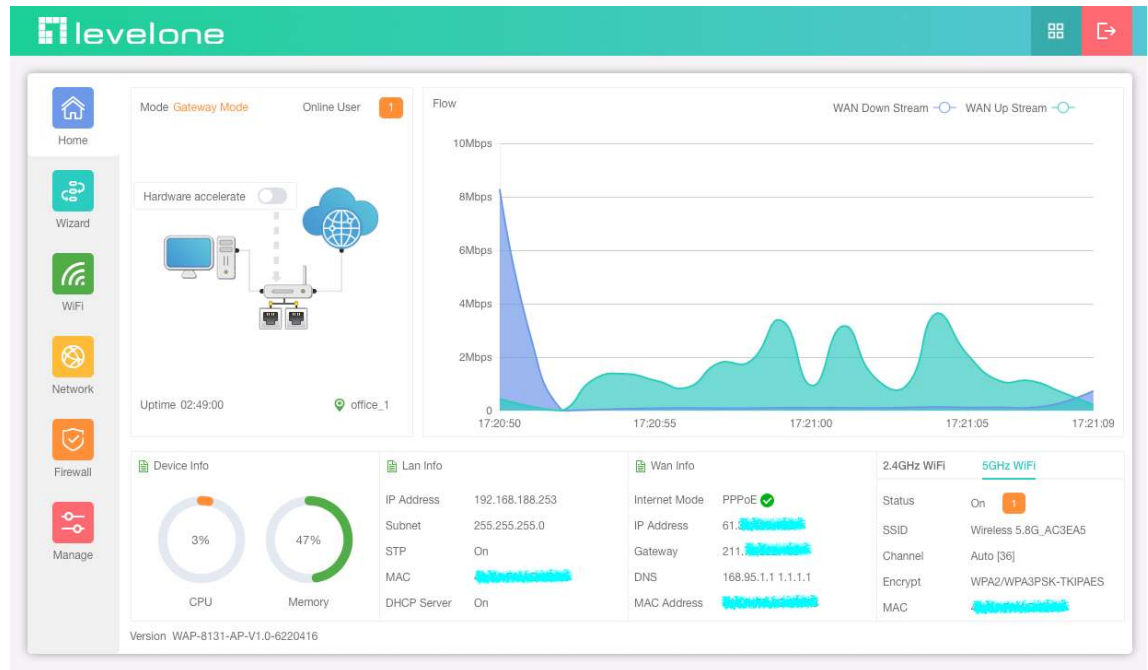
3. Logging on to the equipment: Open a browser and type 192.168.188.253 in the address bar, and then press Enter; in the pop-up login interface, enter the factory login password **"admin"** and click "Login".



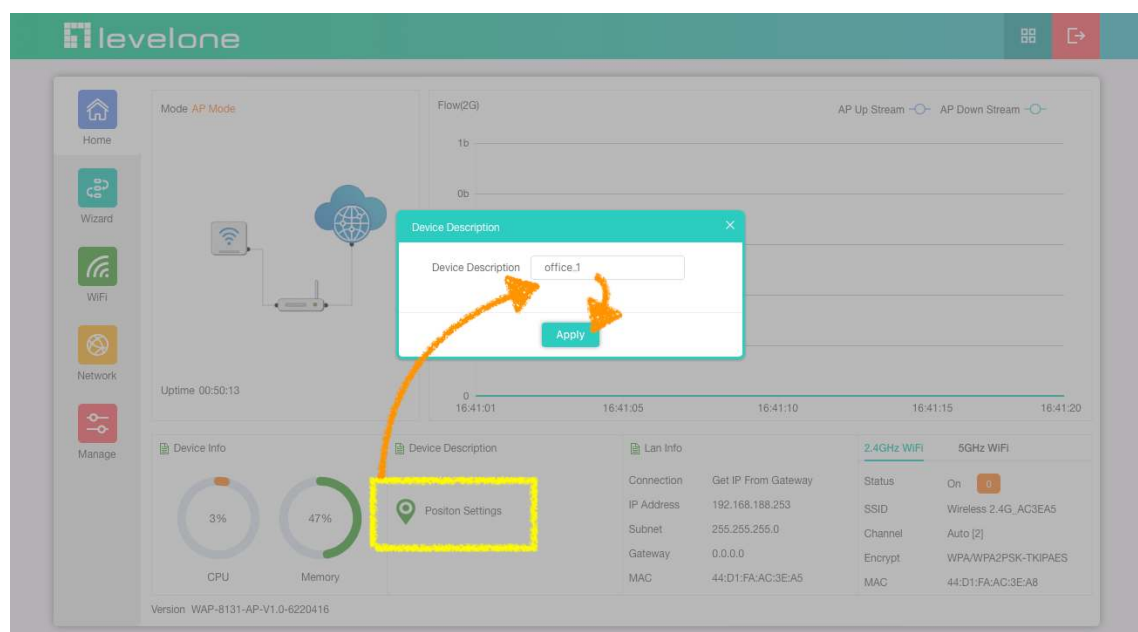
Section I Home

Introduction

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. It includes a management agent that allows you to configure the features listed in this manual.



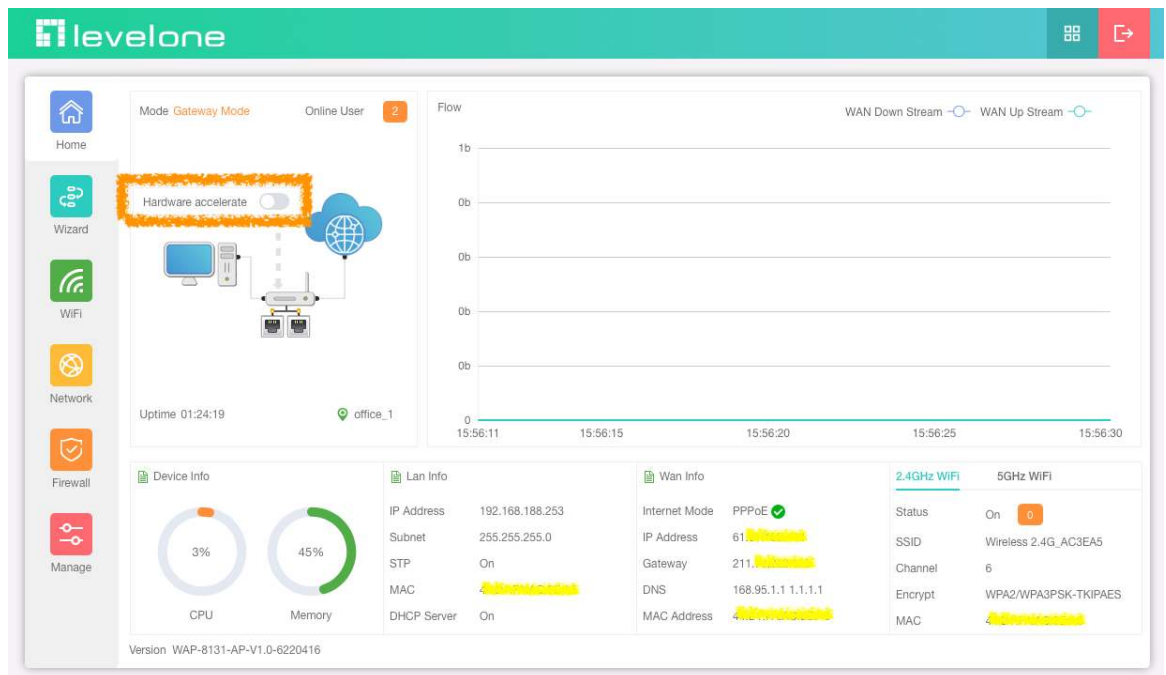
1. Different operation modes are slightly different on the Home screen. The example below is **AP Mode**. Can set the location of the remark AP, which is convenient for future management (Note: Device name can only be letters, numbers, underscores, middle horizontal lines; length 1-10 bits)



2. Confirm whether the location just set is displayed on the login page, which is convenient for future identification and management



3. Different operation modes are slightly different on the Home screen. The example below is **Gateway Mode**. set the hardware accelerate. but enabling the hardware forwarding will cause user traffic statistics, some firewall, and flow control to fail.



4.Can view the current Wireless Online User

The screenshot shows the Hlevelone web interface. The 'Online User' button in the top navigation bar is highlighted with a yellow box and an orange arrow pointing to a modal dialog box titled 'Online User'. The dialog box contains a table with the following data:

SN	Name	IP Address	MAC	Link count
1		192.168.188.3	76:1b:33:7d:11:11	154
2		192.168.188.1	00:11:22:33:44:55	1

Below the table, it says 'Total 2'. The background interface shows various system status indicators like CPU (4%), Memory (48%), and network settings.

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

The screenshot shows the Hlevelone web interface. The 'Online User' button in the top navigation bar is highlighted with a yellow box and an orange arrow pointing to a modal dialog box titled 'Client List'. The dialog box contains a table with the following data:

SN	Name	MAC	Signal	Connect Time
1		76:1b:33:7d:11:11	-56dBm	00:09:34

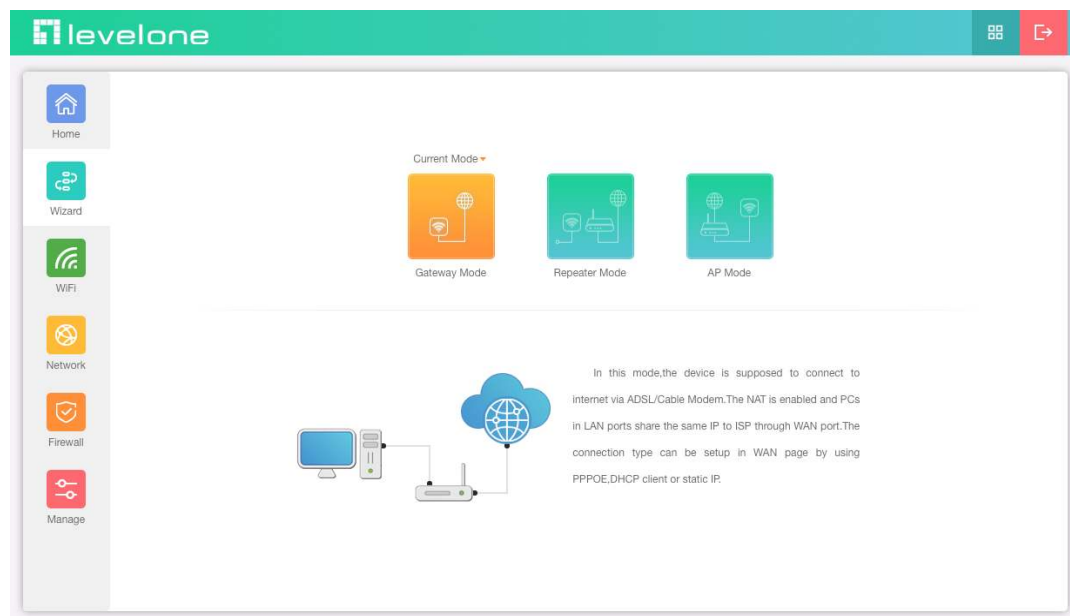
Below the table, it says 'Total 1'. The background interface shows various system status indicators like CPU (2%), Memory (48%), and network settings. The '5GHz WiFi' tab is selected in the bottom right corner, and the 'Client List' button is highlighted with a yellow box and an orange arrow.

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.

Gateway Mode

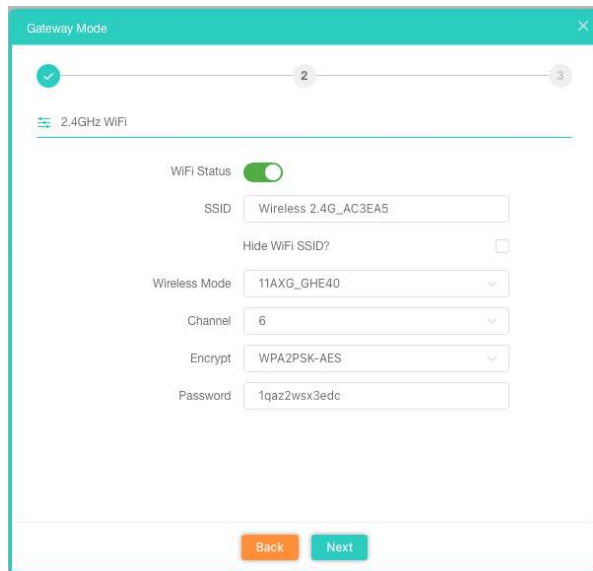
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.



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)

2. Wireless 2.4GHz Setting, Click Next



Gateway Mode

2.4GHz WiFi

WiFi Status ☒

SSID Wireless 2.4G_AC3EA5

Hide WiFi SSID? ☐

Wireless Mode T1AXG_GHE40

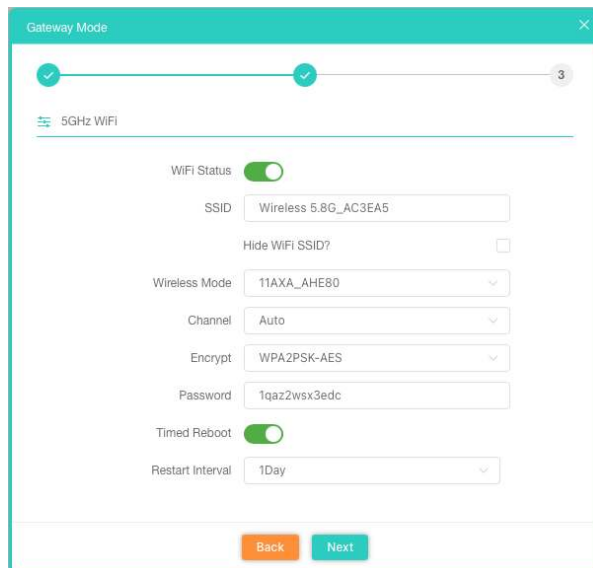
Channel 6

Encrypt WPA2PSK-AES

Password 1qaz2wsx3edc

Back Next

3. Wireless 5GHz Setting, Click Next



Gateway Mode

5GHz WiFi

WiFi Status ☒

SSID Wireless 5.8G_AC3EA5

Hide WiFi SSID? ☐

Wireless Mode T1AXA_AHE80

Channel Auto

Encrypt WPA2PSK-AES

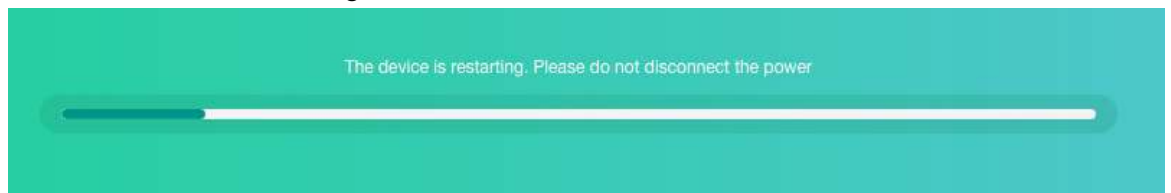
Password 1qaz2wsx3edc

Timed Reboot ☒

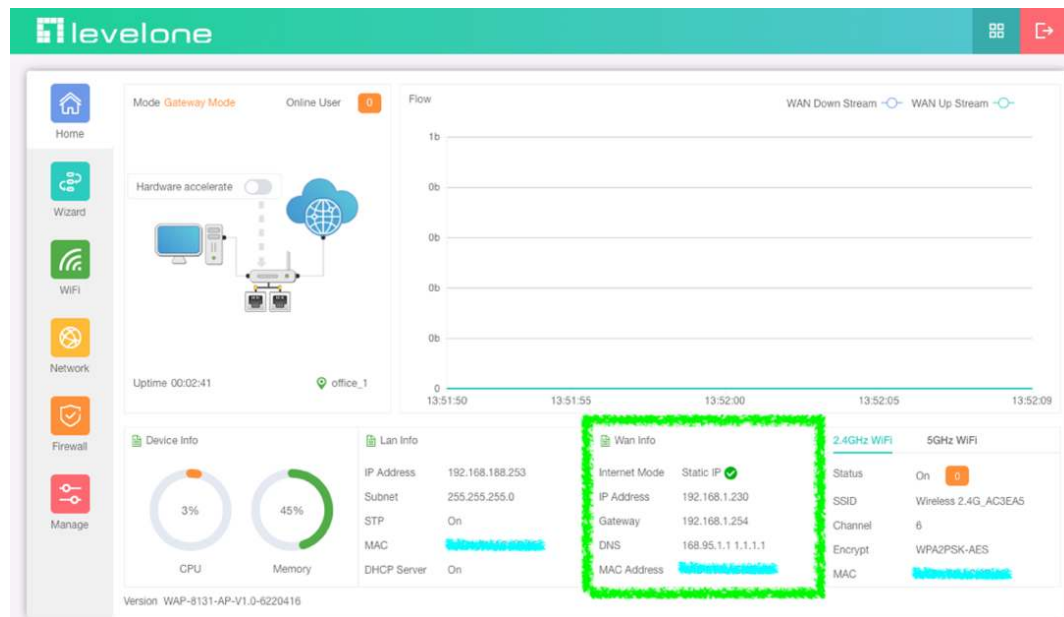
Restart Interval 1Day

Back Next

4. Please wait for the configuration to finish



5. 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)

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

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

Gateway Mode

5GHz WiFi

WiFi Status: ☒

SSID: Wireless 5.8G_AC3EA5

Hide WiFi SSID?: ☐

Wireless Mode: 11AXA_AHE80

Channel: Auto

Encrypt: WPA2PSK-AES

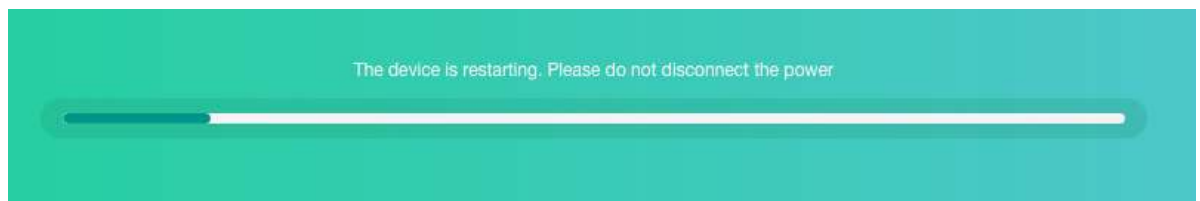
Password: 1qaz2wsx3edc

Timed Reboot: ☒

Restart Interval: 1Day

Back Next

4. Please wait for the configuration to finish



5. This page will show the connection PPPoE status

LevelOne

Mode: Gateway Mode Online User: 0

Hardware accelerate: ☐

Uptime: 00:02:40 office_1

Flow: WAN Down Stream - WAN Up Stream -

Device Info: CPU 3% Memory 44%

Lan Info: IP Address 192.168.188.253 Subnet 255.255.255.0 STP On MAC 48:2e:13:4d:13:4d DHCP Server On

Wan Info: Internet Mode PPPoE IP Address 61.134.134.134 Gateway 211.134.134.134 DNS 168.95.1.1 1.1.1.1 MAC Address 48:2e:13:4d:13:4d

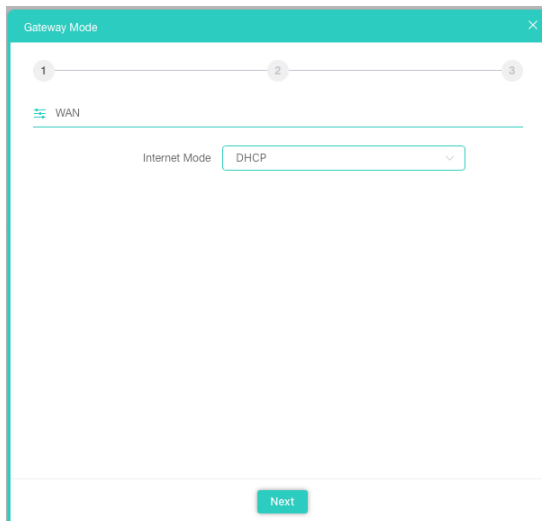
2.4GHz WiFi: Status On SSID Wireless 2.4G_AC3EA5 Channel 6 Encrypt WPA2PSK-AES MAC 48:2e:13:4d:13:4d

5GHz WiFi: Status On SSID Wireless 5.8G_AC3EA5 Channel 6 Encrypt WPA2PSK-AES MAC 48:2e:13:4d:13:4d

Version: WAP-8131-AP-V1.0-6220416

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)



Gateway Mode

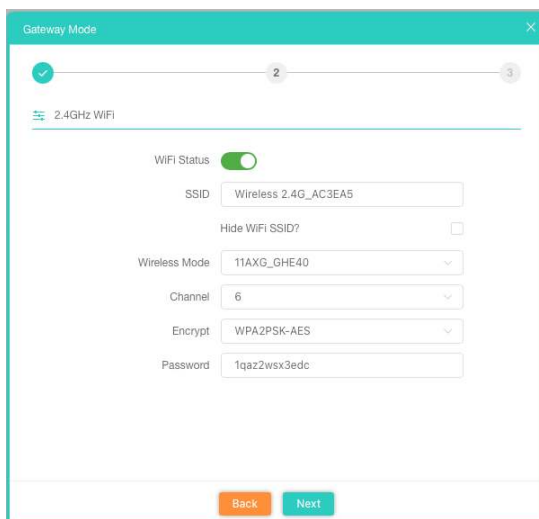
1 2 3

WAN

Internet Mode: DHCP

Next

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



Gateway Mode

1 2 3

2.4GHz WiFi

WiFi Status: ☒

SSID: Wireless 2.4G_AC3EA5

Hide WiFi SSID?: ☐

Wireless Mode: 11AXG_GHE40

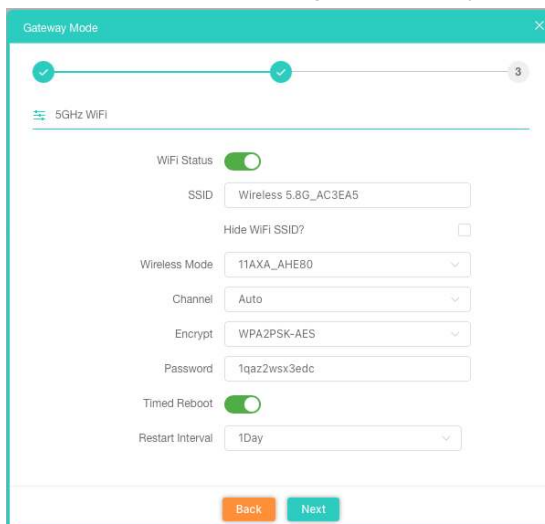
Channel: 6

Encrypt: WPA2PSK-AES

Password: 1qaz2wsx3edc

Back Next

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



Gateway Mode

1 2 3

5GHz WiFi

WiFi Status: ☒

SSID: Wireless 5.8G_AC3EA5

Hide WiFi SSID?: ☐

Wireless Mode: 11AXA_AHE80

Channel: Auto

Encrypt: WPA2PSK-AES

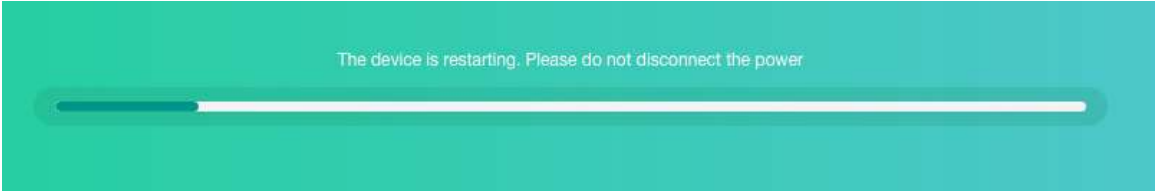
Password: 1qaz2wsx3edc

Timed Reboot: ☒

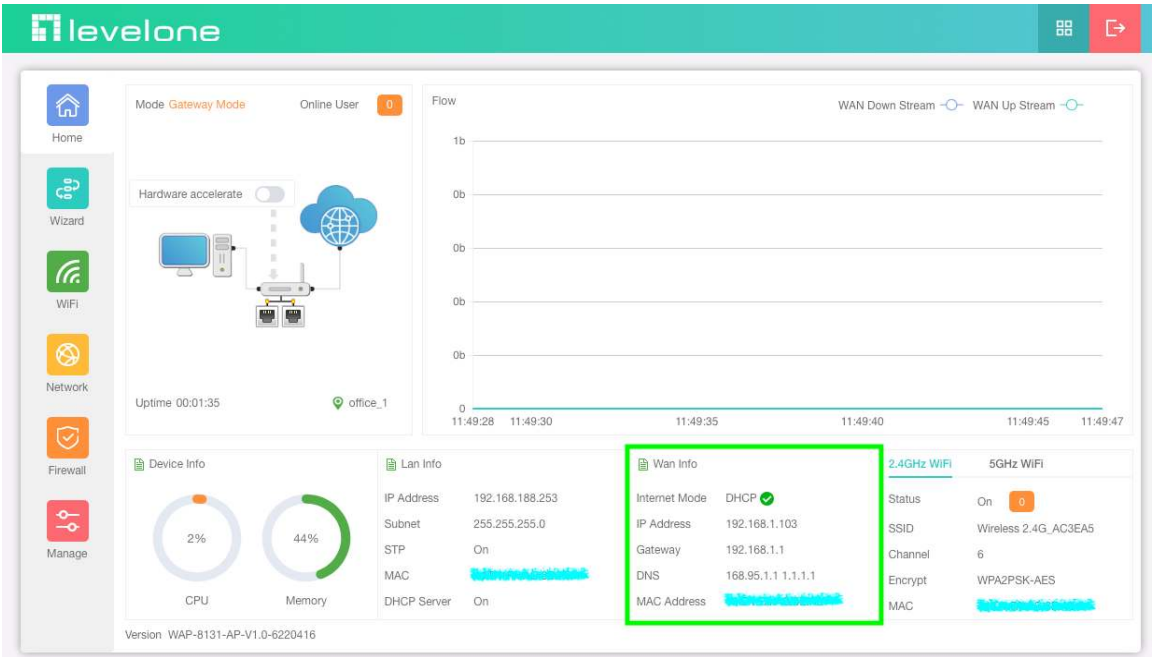
Restart Interval: 1Day

Back Next

4.Please wait for the configuration to finish

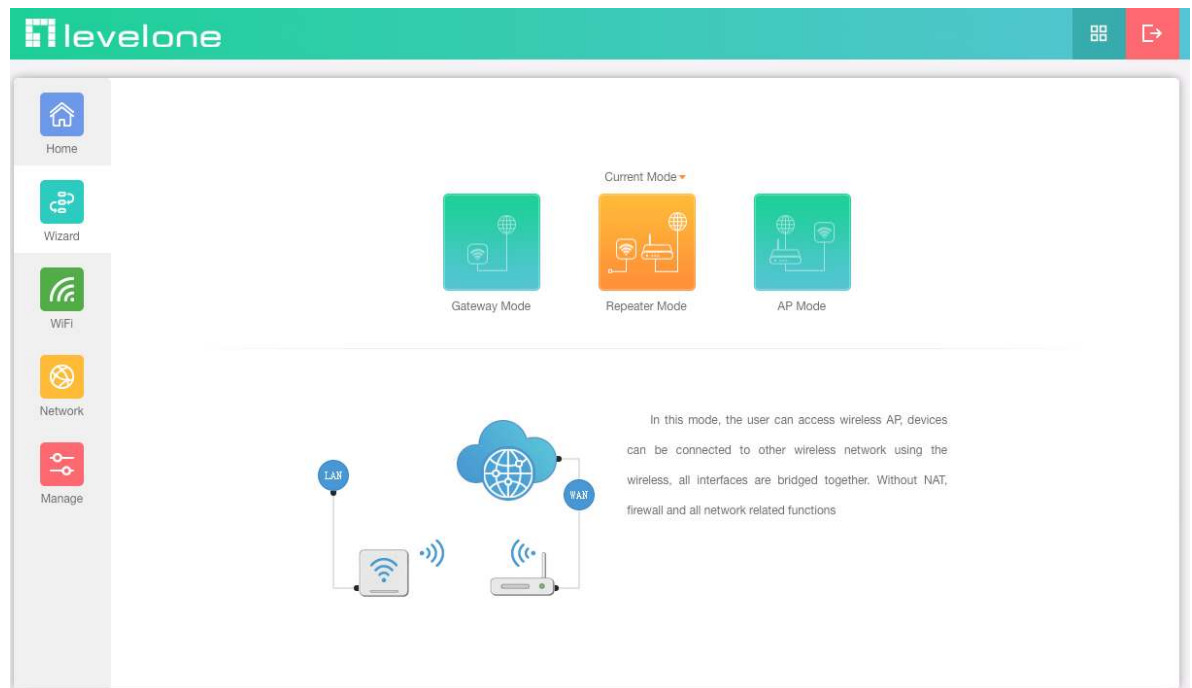


5. This page will show the connection DHCP status

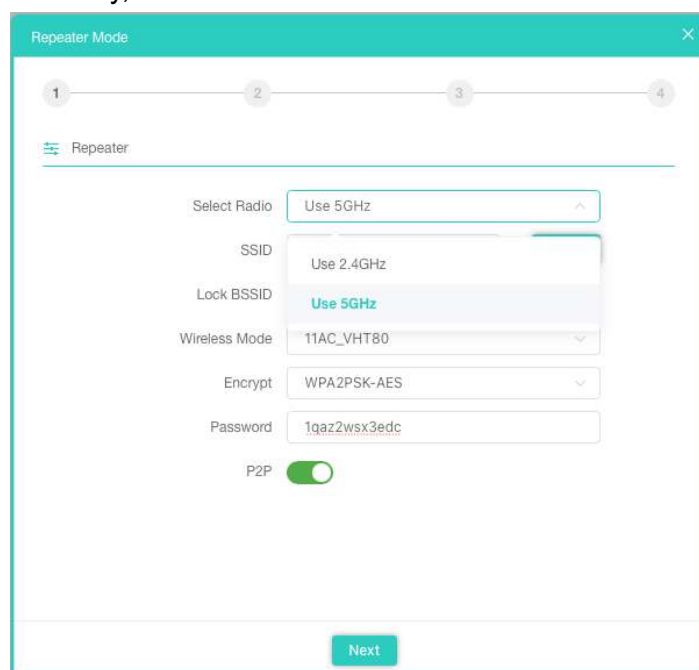


Repeater mode

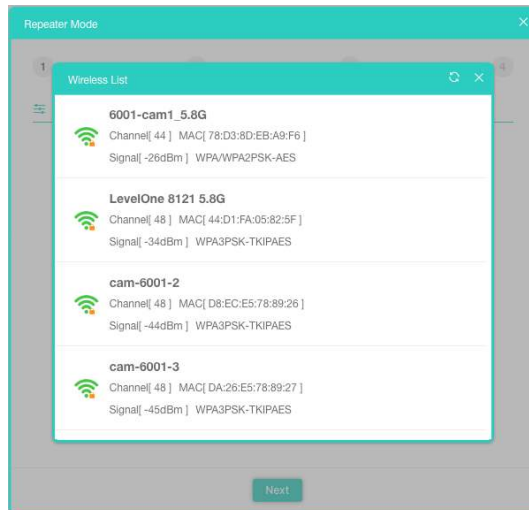
In this mode, the user can access wireless AP, devices can be connected to other wireless network using the wireless, all interfaces are bridged together. Without NAT, firewall and all network related functions



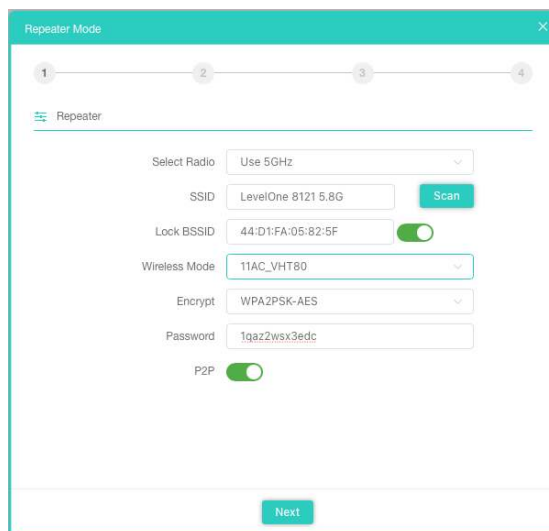
1. Can choose to relay the front-end 2.4G or 5G wireless signal to extend the wireless signal range. Select the AP's SSID want to bridge, take "wireless 5G" for example, then input the AP's key, click Scan AP



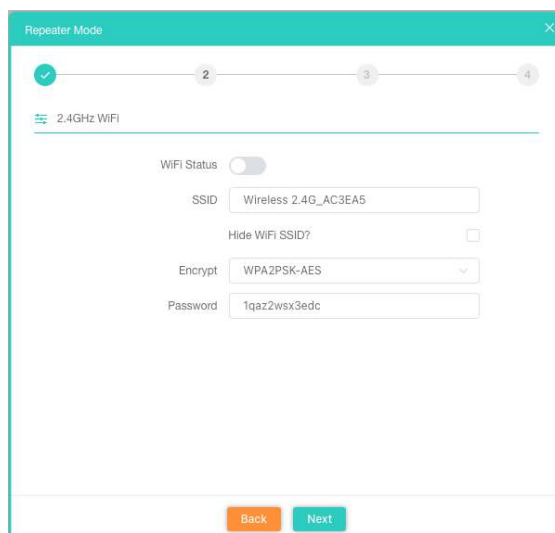
2. Please select WIFI SSID to connect



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.

The screenshot shows the 'Repeater Mode' configuration window, specifically the '5GHz WiFi' tab. At the top, there is a progress bar with four steps; the first three are marked with green checkmarks, and the fourth is marked with the number '4'. Below the progress bar, the '5GHz WiFi' section is active. It contains the following settings: 'WiFi Status' is a green toggle switch; 'SSID' is a text field containing 'Wireless 5.8G_AC3EA5'; 'Hide WiFi SSID?' is an unchecked checkbox; 'Encrypt' is a dropdown menu set to 'WPA2PSK-AES'; 'Password' is a text field containing '1qaz2wsx3edc'; 'Timed Reboot' is a green toggle switch; and 'Restart Interval' is a dropdown menu set to '3Day'. At the bottom of the window are 'Back' and 'Next' buttons.

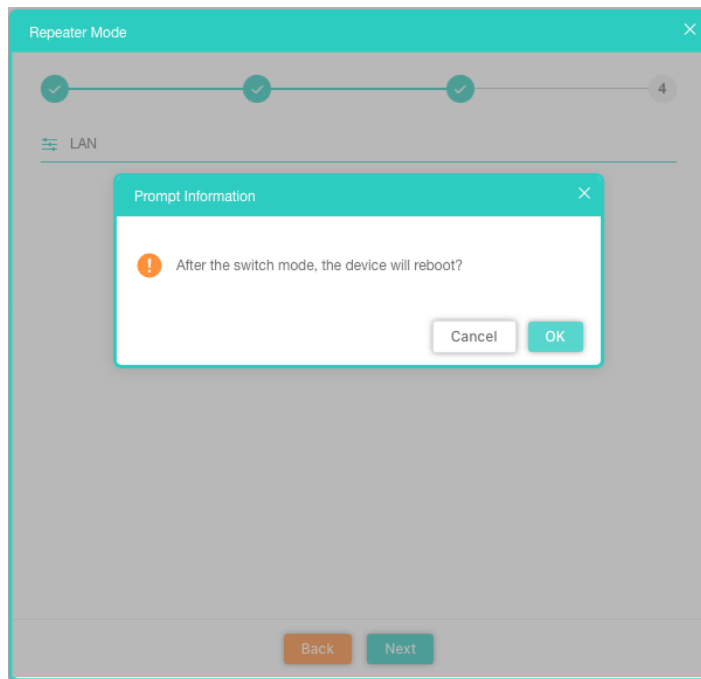
6. Set up the LAN according to the front-end relay 2.4 / 5G wireless signal :

a) If the front-end wireless signal is Static IP, you can click "Static IP" to set an unused IP address.

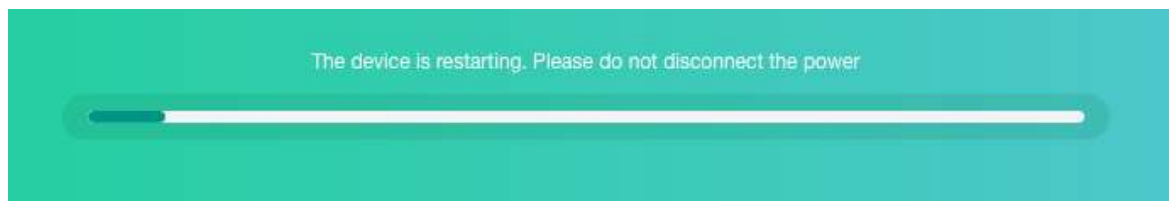
b) If the gateway of the front-end wireless signal will automatically assign an IP address, you can click "Get IP From Gateway"

The screenshot shows the 'Repeater Mode' configuration window, specifically the 'LAN' tab. At the top, the progress bar shows the first three steps with green checkmarks and the fourth step with the number '4'. The 'LAN' section is active. It features a 'Connection' dropdown menu currently set to 'Get IP From Gateway'. A dropdown menu is open below it, showing two options: 'Static IP' and 'Get IP From Gateway', with the latter highlighted in blue. At the bottom of the window are 'Back' and 'Next' buttons.

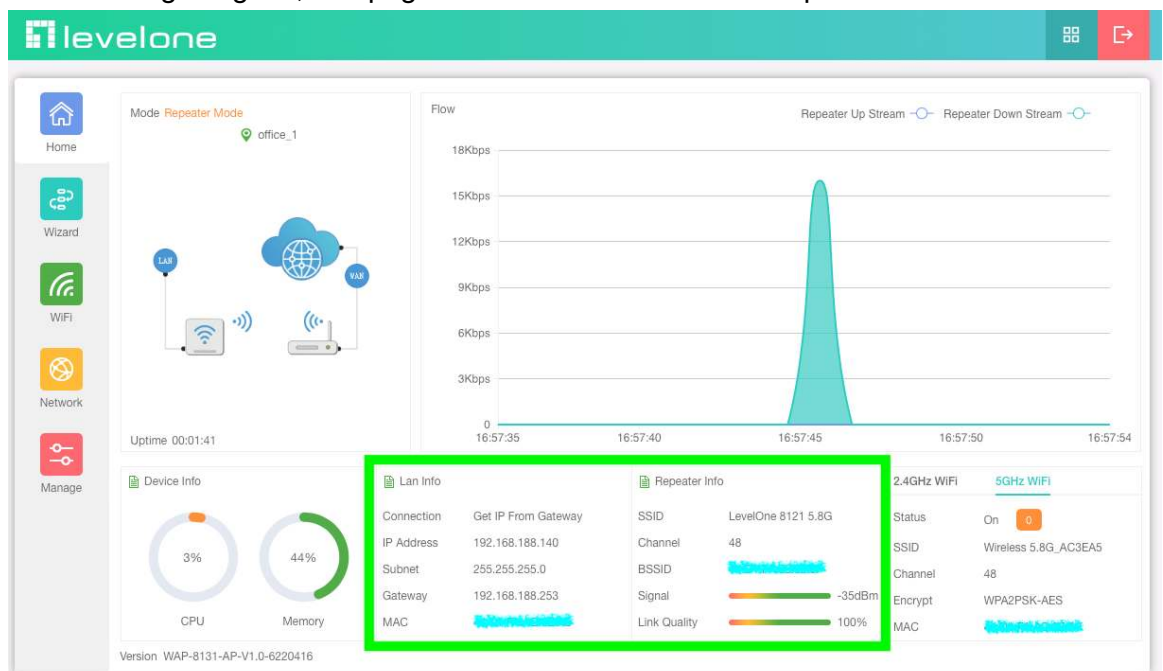
7. Please click the ok button, After the switch mode, the device will reboot



8. Please wait more than 40 seconds

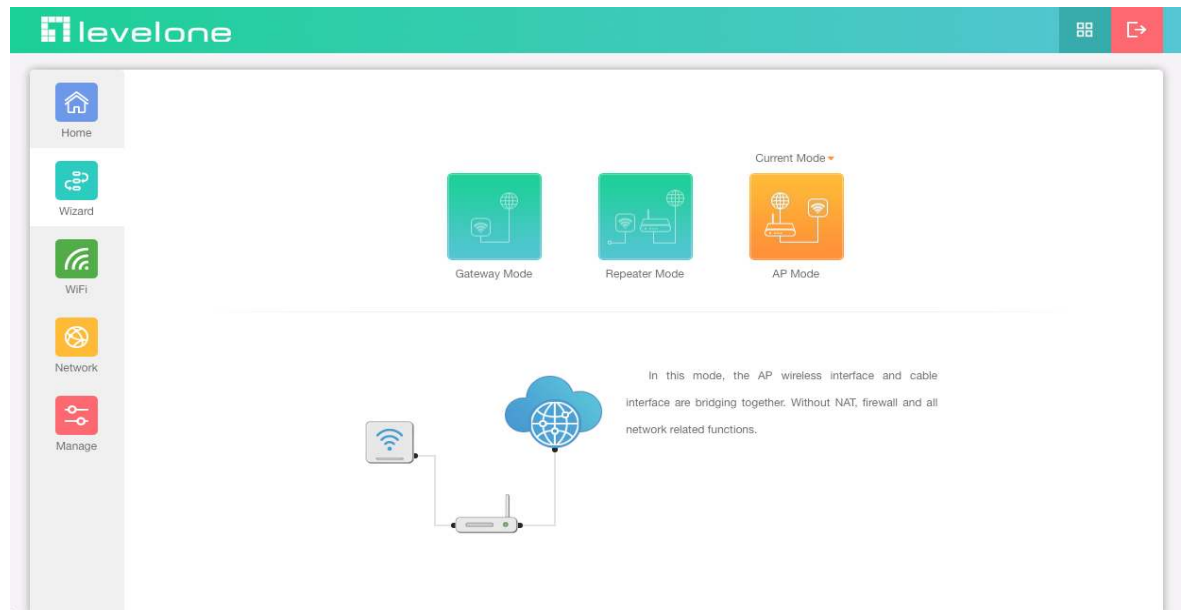


9. Please log in again ,This page will show the connection Repeater mode status



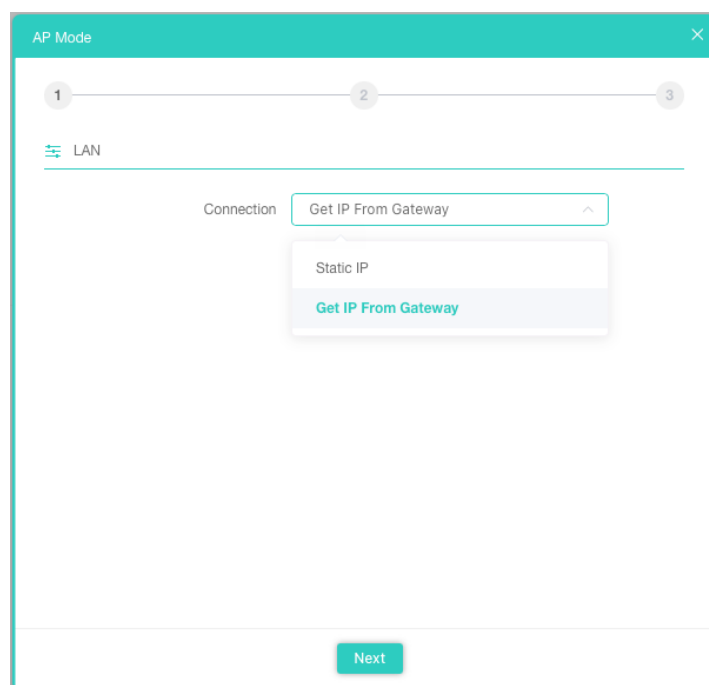
AP Mode

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

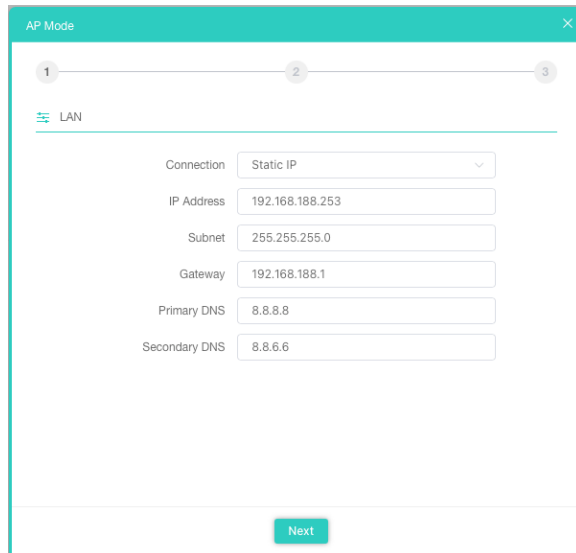


1.Set according to LAN environmental requirements :

- a) If the front-end is Static IP, you can click "Static IP" to set an unused IP address.
- b) 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

Connection: Static IP

IP Address: 192.168.188.253

Subnet: 255.255.255.0

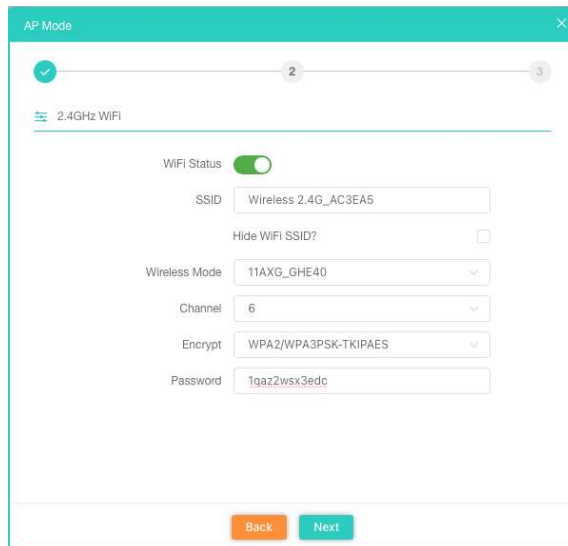
Gateway: 192.168.188.1

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.6.6

Next

3. Configure the 2.4G Wireless SSID and password



AP Mode

1 2 3

2.4GHz WiFi

WiFi Status: ☒

SSID: Wireless 2.4G_AC3EA5

Hide WiFi SSID?: ☐

Wireless Mode: 11AXG_GHE40

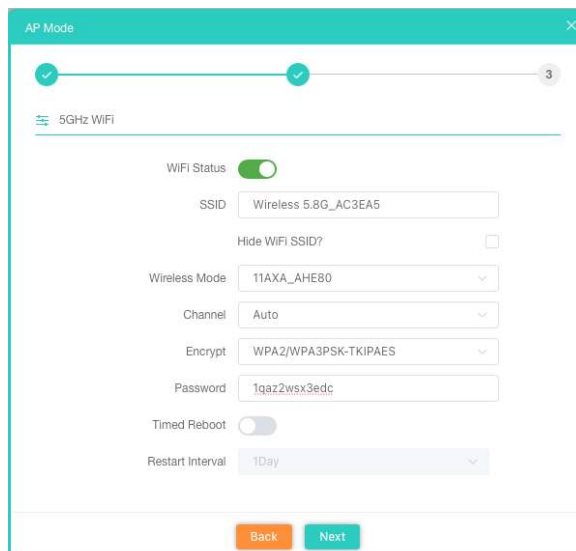
Channel: 6

Encrypt: WPA2/WPA3PSK-TKIPAES

Password: 1qaz2wsx3edc

Back Next

4.Configure the 5G Wireless SSID and password



AP Mode

1 2 3

5GHz WiFi

WiFi Status: ☒

SSID: Wireless 5.8G_AC3EA5

Hide WiFi SSID?: ☐

Wireless Mode: 11AXA_AHE80

Channel: Auto

Encrypt: WPA2/WPA3PSK-TKIPAES

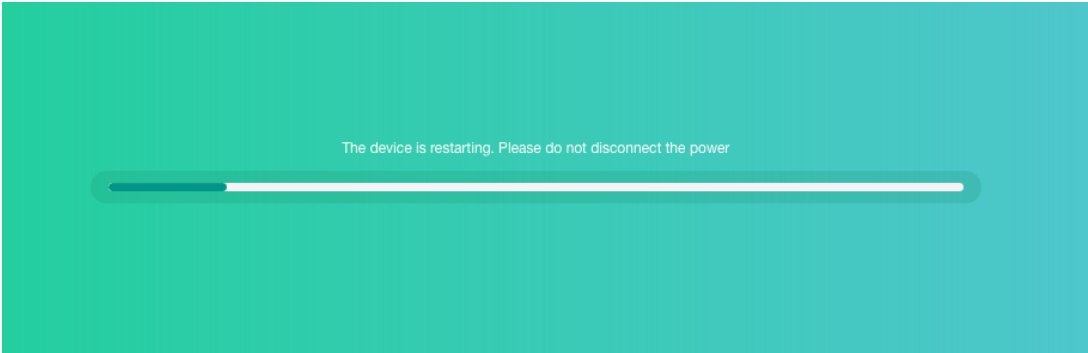
Password: 1qaz2wsx3edc

Timed Reboot: ☐

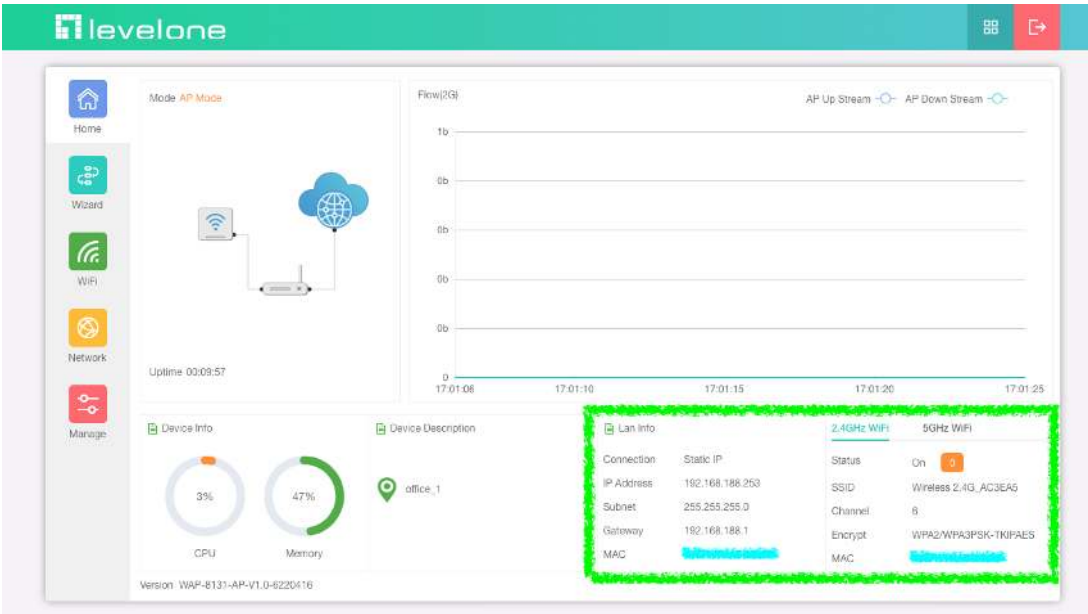
Restart Interval: 1Day

Back Next

5.Please wait more than 30 seconds



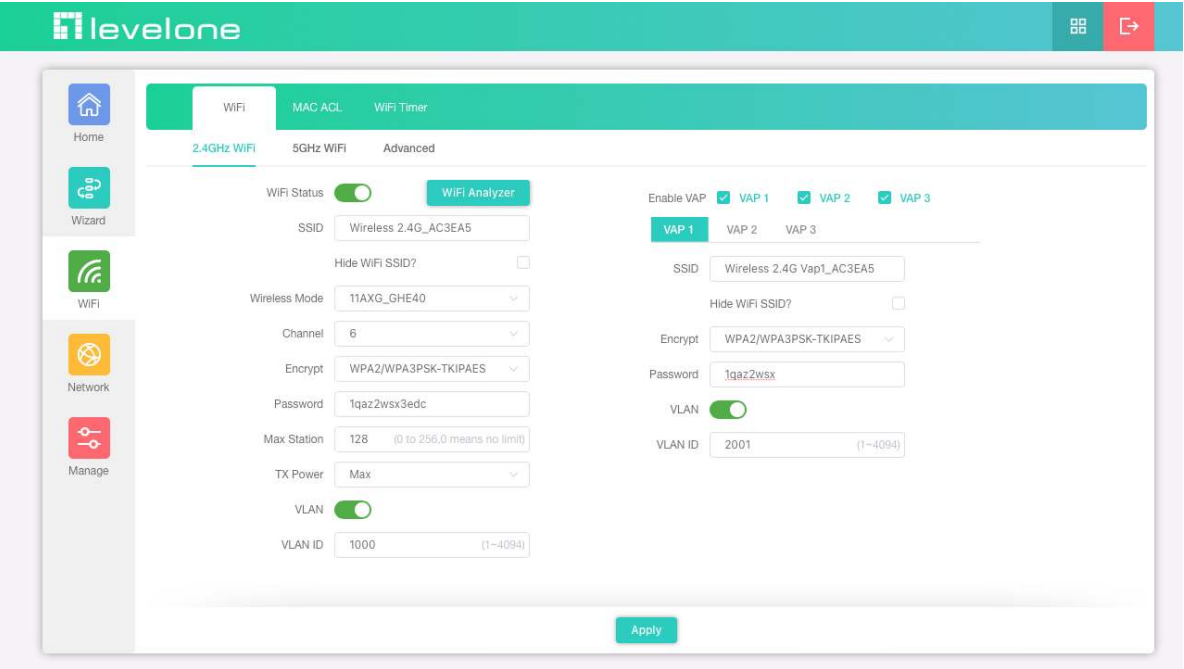
6.Check AP Mode Status

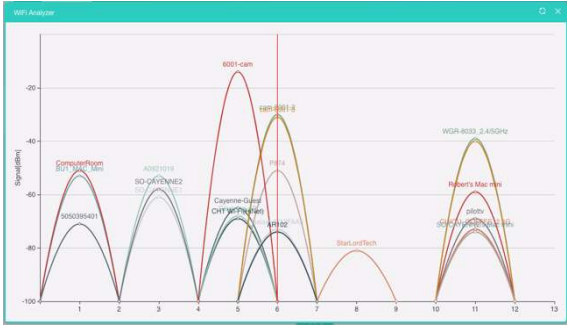


Section III WiFi

2.4GHz WiFi

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



Basic Features Description	
WiFi Status	2.4GHz Wireless Radio - Select On or Off the radio wave. WiFi Status  WiFi Status  WiFi Analyzer : Wireless analyzer Look for Unoccupied channel (2.4GHz) 
SSID	Custom 2.4GHz WiFi Name
	Radiate SSID : Anyone in this area can find SSID

Hide WiFi SSID?	Hidden SSID : Everyone in this area cannot search for the SSID. You can only connect successfully by manually entering the correct SSID and password.
Wireless Mode	
Channel	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). 

Encrypt	NONE (Open System) An open wireless network is one where you have no password. None of your network traffic will be encrypted which means it's visible to anyone who wants to look. WPA/WPA2-PSK (TKIP/AES) This uses the modern WPA standard with older TKIP encryption. This option isn't very secure, and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network. WPA2/WPA3-PSK (TKIP/AES) This enables both WPA2 and WPA3 with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have, but also ensures an attacker can breach your network by cracking the lowest-common-denominator encryption scheme. This TKIP+AES option may also be called WPA3-PSK "mixed" mode. WPA3-PSK (TKIP/AES) (recommended) It's the most secure of the bunch at the moment. It uses WPA3, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. You should be using this option. but doesn't offer compatibility with any ancient devices you might have. If you are sure to use WPA3-Personal Mode, please first check whether your terminal device also supports WPA3. If your device does not support it, your device cannot connect to the wireless network properly. Before you enable other authorization modes with special encryption, such as: NONE(Open System),
-----------------------	---

	WPA/WPA2PSK-TKIP/AES, WPA2PSK-AES, WPA2/WPA3-PSK (TKIP/AES), we recommend you to confirm the compatibility of the end device at the same time. If the terminal device cannot be connected after changing to the above mode, please change it to WPA2PSK-AES first to ensure connection. [Note] Terminal devices include mobile phones, computers, IoT devices...etc. To confirm whether your device supports WPA3-personal authorization mode, please contact the original product manufacturer or check on the WiFi Alliance website: https://www.wi-fi.org/product-finder
Password	The key can be a mix of alphanumeric and special characters, The key is case sensitive
Max Station	Default 128, the maximum number of WiFi device connections
TX Power	
VLAN	If your network uses VLANs, you might need to configure the management VLAN ID or untagged VLAN ID on the WAP-8131 in order for it to work with your network. VLAN ☐ VLAN ID : 1~4094 (Set the management VLAN ID) VLAN ☒ VLAN ID (1~4094)

Enable VAP

Enable VAP ☒ VAP 1 ☒ VAP 2 ☒ VAP 3

VAP 1 VAP 2 VAP 3

SSID Wireless 2.4G Vap3_AC3EA5

Hide WiFi SSID? ☐

Encrypt WPA2/WPA3PSK-TKIPAES

Password 1qaz2wsx

VLAN ☒

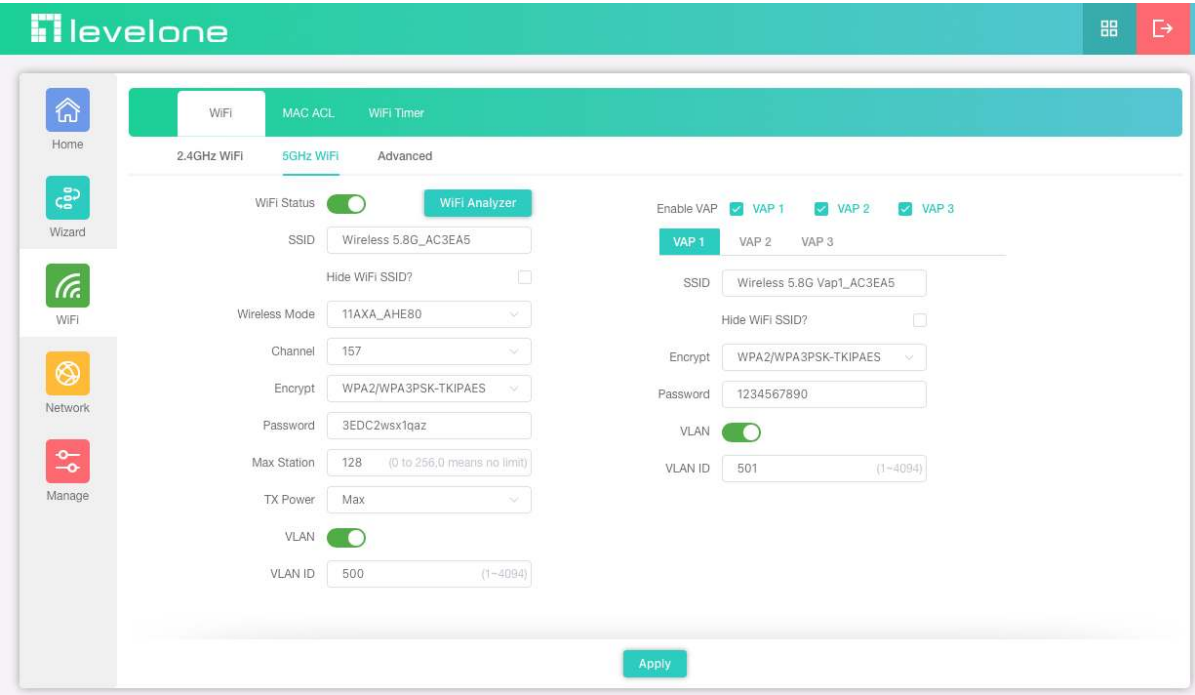
VLAN ID 2003 (1-4094)

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.

5GHz WiFi

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



Basic Features Description	
WiFi Status	5GHz Wireless Radio - Select On or Off the radio wave.
	WiFi Status
	WiFi Status
WiFi Status	WiFi Analyzer :
	Wireless analyzer Look for Unoccupied channel (5GHz)

SSID	Custom 5GHz WiFi Name
Hide your SSID?	Radiate SSID : Anyone in this area can find SSID Hidden SSID : Everyone in this area cannot search for the SSID. You can only connect successfully by manually entering the correct SSID and password.
Wireless Mode	The 80 MHz channel enables higher data rates but leaves fewer channels available for use by other 5 GHz devices. 
Channel	Wireless Mode 11NA_HT20 (Country Region: ETSI) CH 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 11NA_HT40 (Country Region: ETSI) CH 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 11AC_VHT20 (Country Region: ETSI) CH 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 11AC_VHT40 (Country Region: ETSI) CH 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

	11AC_VHT80 (Country Region: ETSI) CH 36, 40, 44,48, 52, 56, 60, 64, 100,104,108, 112, 116, 120, 124, 128 11AXA_AHE20 (Country Region: ETSI) CH 36, 40, 44,48, 52, 56, 60, 64, 100,104,108, 112, 116, 120, 124, 128, 132, 136, 140 11AXA_AHE40 (Country Region: ETSI) CH 36, 40, 44,48, 52, 56, 60, 64, 100,104,108, 112, 116, 120, 124, 128, 132, 136, 140 11AXA_AHE80 (Country Region: ETSI) CH 36, 40, 44,48, 52, 56, 60, 64, 100,104,108, 112, 116, 120, 124, 128 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).
Encrypt	 NONE WPA2PSK-AES WPA/WPA2PSK-TKIPAES WPA2/WPA3PSK-TKIPAES WPA3PSK-TKIPAES

NONE (Open System)

An open wireless network is one where you have no password. None of your network traffic will be encrypted which means it's visible to anyone who wants to look.

WPA/WPA2-PSK (TKIP/AES)

This uses the modern WPA standard with older TKIP encryption. This option isn't very secure, and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network.

WPA2/WPA3-PSK (TKIP/AES)

This enables both WPA2 and WPA3 with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have, but also ensures an attacker can breach your network by cracking the lowest-common-denominator encryption scheme. This TKIP+AES option may also be called WPA3-PSK "mixed" mode.

WPA3-PSK (TKIP/AES) (recommended)

It's the most secure of the bunch at the moment. It uses WPA3, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. You should be using this option. but doesn't offer compatibility with any ancient devices you might have.

If you are sure to use WPA3-Personal Mode, please first check whether your terminal device also supports WPA3. If your device does not support it, your device cannot connect to the wireless network properly. Before you enable other authorization modes with special encryption, such as: NONE(Open System), WPA/WPA2PSK-TKIP/AES, WPA2PSK-AES, WPA2/WPA3-PSK (TKIP/AES), we recommend you to confirm the compatibility of the end device at the same time. If the terminal device cannot be connected after changing to the above mode, please change it to WPA2PSK-AES first to ensure connection.

[Note] Terminal devices include mobile phones, computers, lot devices...etc.

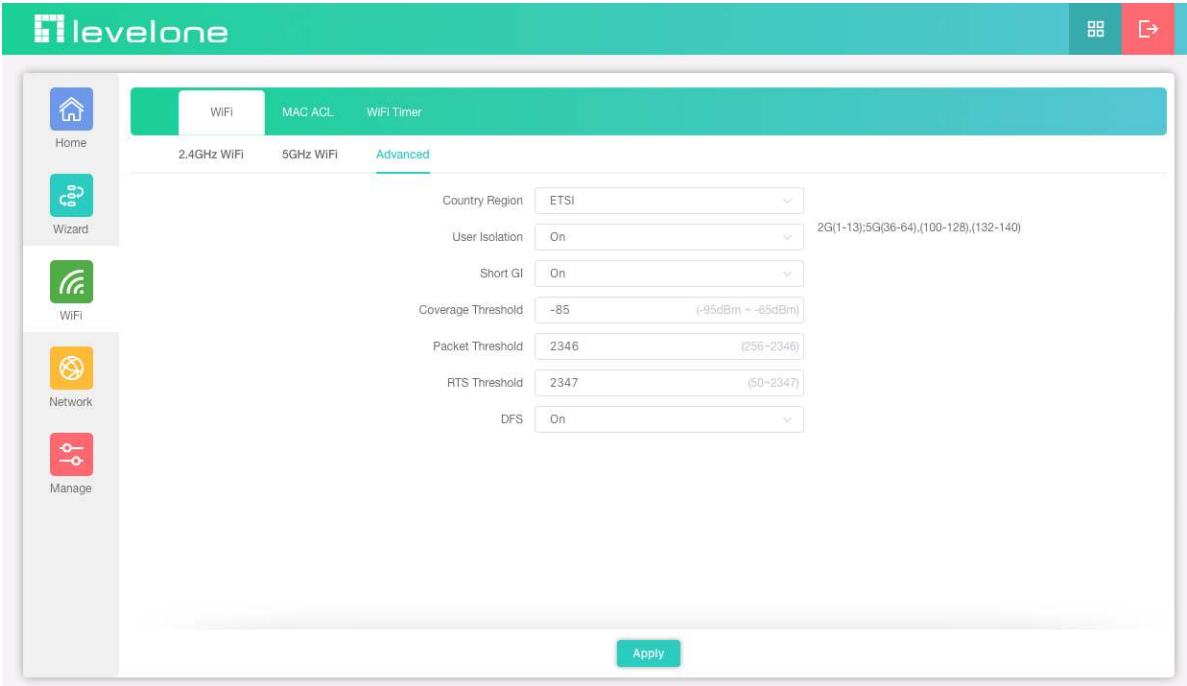
To confirm whether your device supports WPA3-personal authorization mode, please contact the original product manufacturer or check on the WiFi Alliance website:

	https://www.wi-fi.org/product-finder
Password	The key can be a mix of alphanumeric and special characters, The key is case sensitive
Max Station	Default 128, the maximum number of WiFi device connections
TX Power	
VLAN	If your network uses VLANs, you might need to configure the management VLAN ID or untagged VLAN ID on the WAP-8131 in order for it to work with your network. VLAN ☐ VLAN ID : 1~4094 (Set the management VLAN ID) VLAN ☒ VLAN ID
Enable VAP	 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.
--	--

Advanced

Advanced related settings of WiFi function, which will be explained in detail below.



Advanced Setting Description	
Country Region	China (Applicable to Singapore) U.S.A UAE ETSI India Brazil Select the country in which the AP is operating 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 transmission power of the radio. 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. Devices that operate in unlicensed bands do not require any formal licensing process, but when operating in these bands, the user is

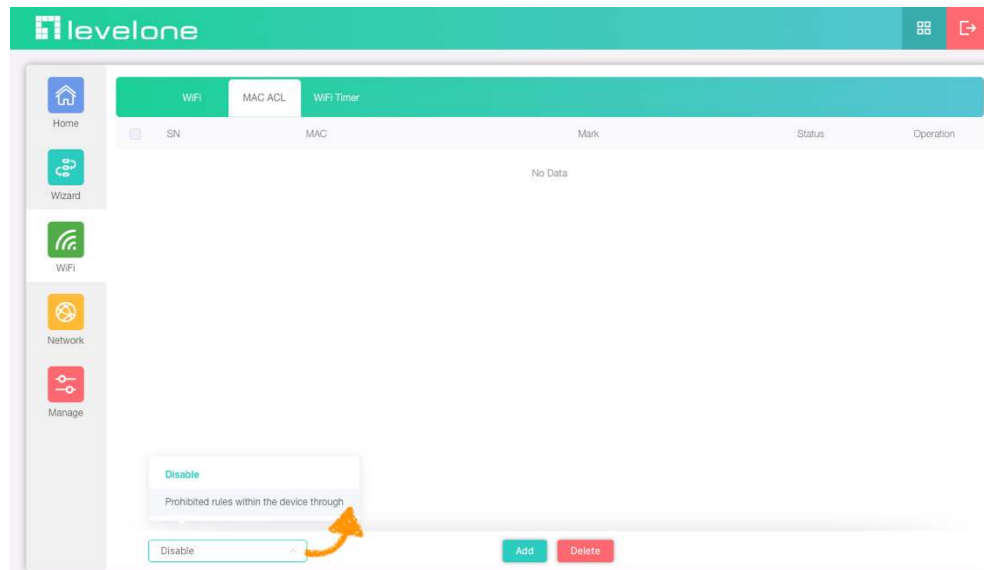
	obligated to follow the government regulations for that region.
User Isolation	This feature effectively segregates the wireless of your choice from the rest of the Network. With Ethernet-to-WLAN Access disabled, information sent from the Ethernet side will not be passed to the Wireless Clients. However, wireless clients will still be able to transmit across Ethernet for browsing, etc. User Isolation On
Short GI	Short GI (Short Guard Interval) Short Guard Interval shortens the waiting time to 400 ns, Guard Interval is intended to avoid signal loss from multipath effect. Short GI On
Coverage Threshold	Perform a Network Planning and Deployment Analysis Install your access points strategically to maximize network coverage. It is recommended to perform a network performance diagnosis prior to the wireless network deployment. Network performance is usually reduced by a retry packet rate close to or over 10%. This deficiency could be caused by frequency interference or screened devices. if a first analysis does not meet the expected network quality standards. need to be improved and the access points that need to be repositioned or have their settings reconfigured to improve network coverage, signal quality and overall user experience. Coverage Threshold -85 (-95dBm ~ -65dBm)
Packet Threshold	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. Setting the fragmentation threshold too low may result in poor performance. Packet Threshold 2346 (256~2346)
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 50-2347 are recommended.

	RTS Threshold 2347 (50~2347)
DFS	DFS(Dynamic Frequency Selection) 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. NOTE: For EU Wireless Regulations, Please turn on the DFS DFS On Off On

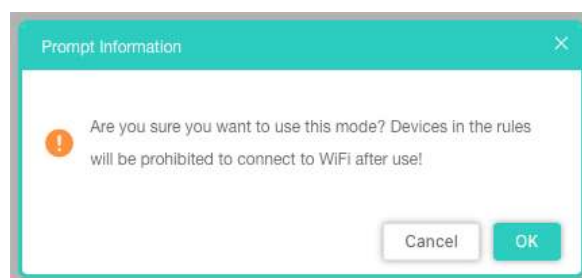
MAC ACL (MAC Filter Configuration)

The MAC filter configuration rule has the following 2 options:

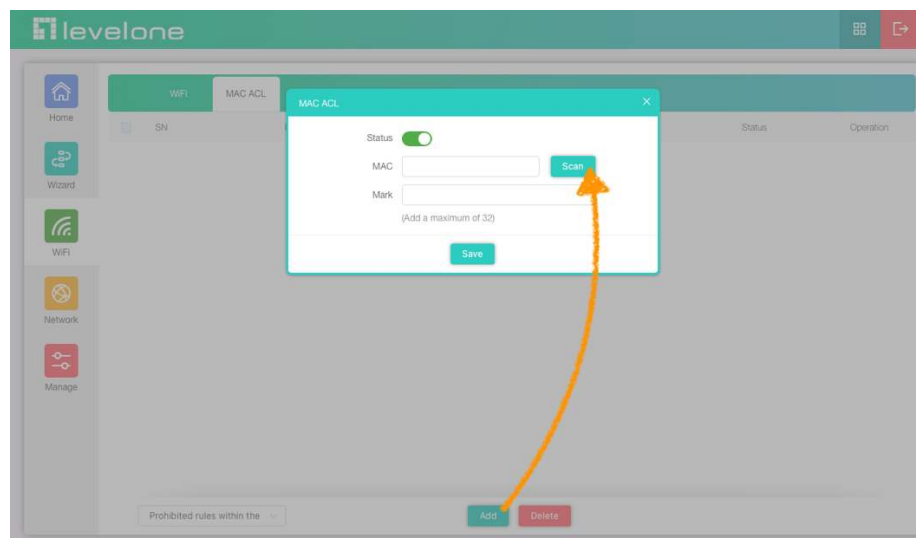
1. Disable
2. Prohibited rules within the device through



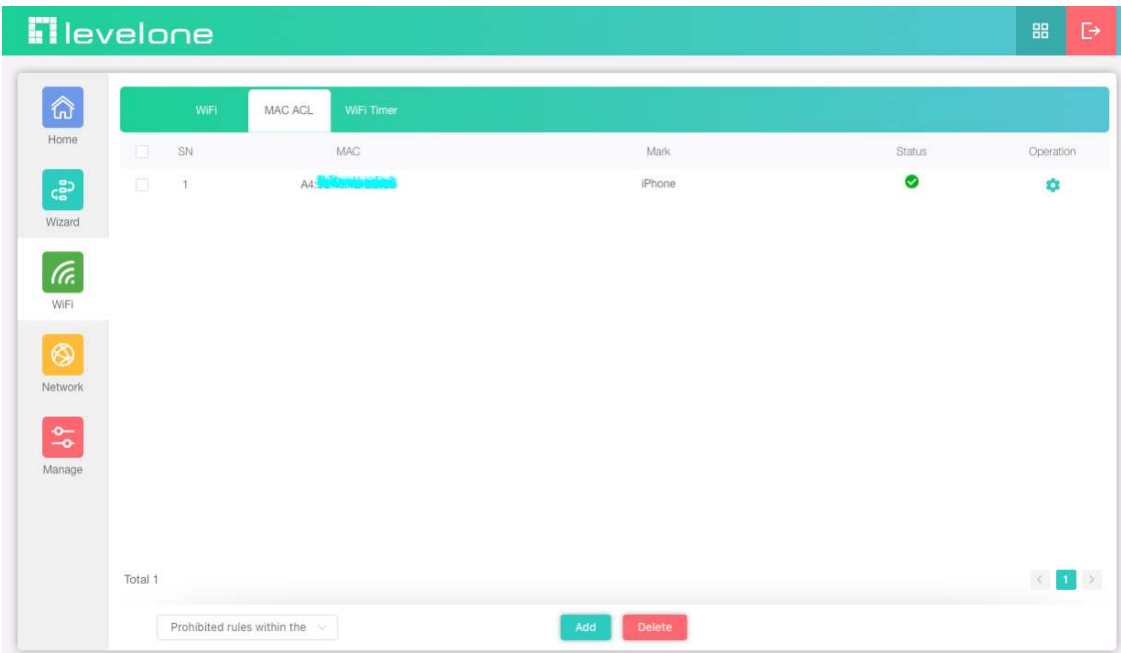
Prohibited rules within the device through - When this is selected, only devices with a MAC address in the list are not granted access.



MAC Address - Add MAC addresses to the MAC Address Control List.

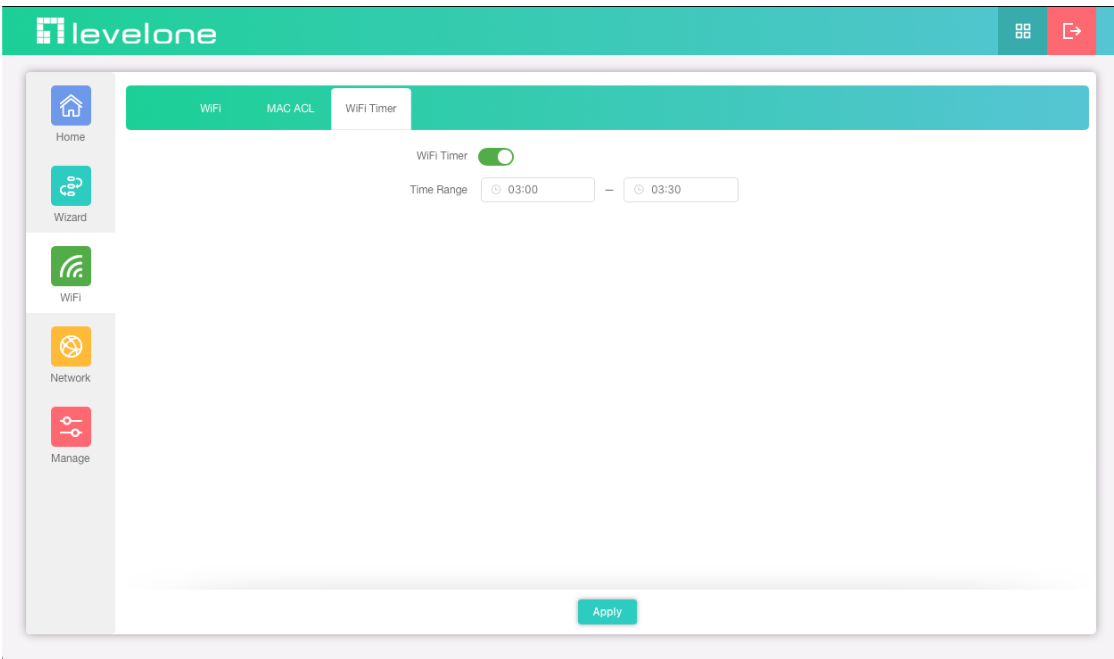


Prohibited rules within the device through - When this is selected, only devices with a MAC address in the list are not granted access.



WiFi Timer

You can customize the AP device reboot time range



Section IV Network (For AP/Repeater Mode)

LAN

Can choose 2 kinds of usage modes (Static IP/ Get IP From Gateway)
which can be selected according to the current network architecture environment.

1. Static IP

The screenshot shows the LevelOne web interface for LAN configuration. The 'LAN' tab is selected. The 'Connection' dropdown is set to 'Static IP'. The following fields are filled in:

Field	Value
IP Address	192.168.188.253
Subnet	255.255.255.0
Gateway	192.168.188.253
Primary DNS	8.8.8.8
Secondary DNS	8.8.6.6

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

2. Get IP From Gateway

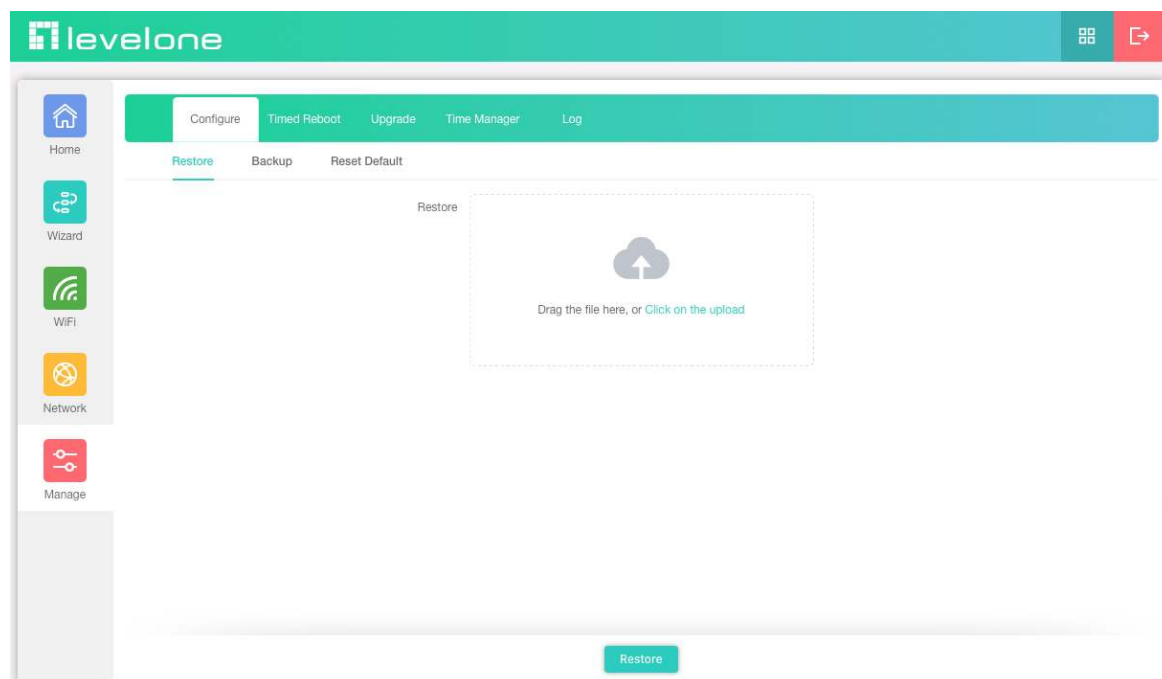
The screenshot shows the LevelOne web interface for LAN configuration. The 'LAN' tab is selected. The 'Connection' dropdown is set to 'Get IP From Gateway'. No other fields are visible, indicating that these settings are managed by the gateway. An 'Apply' button is located at the bottom right of the configuration area.

Section V Manage (For AP/Repeater Mode)

Configure

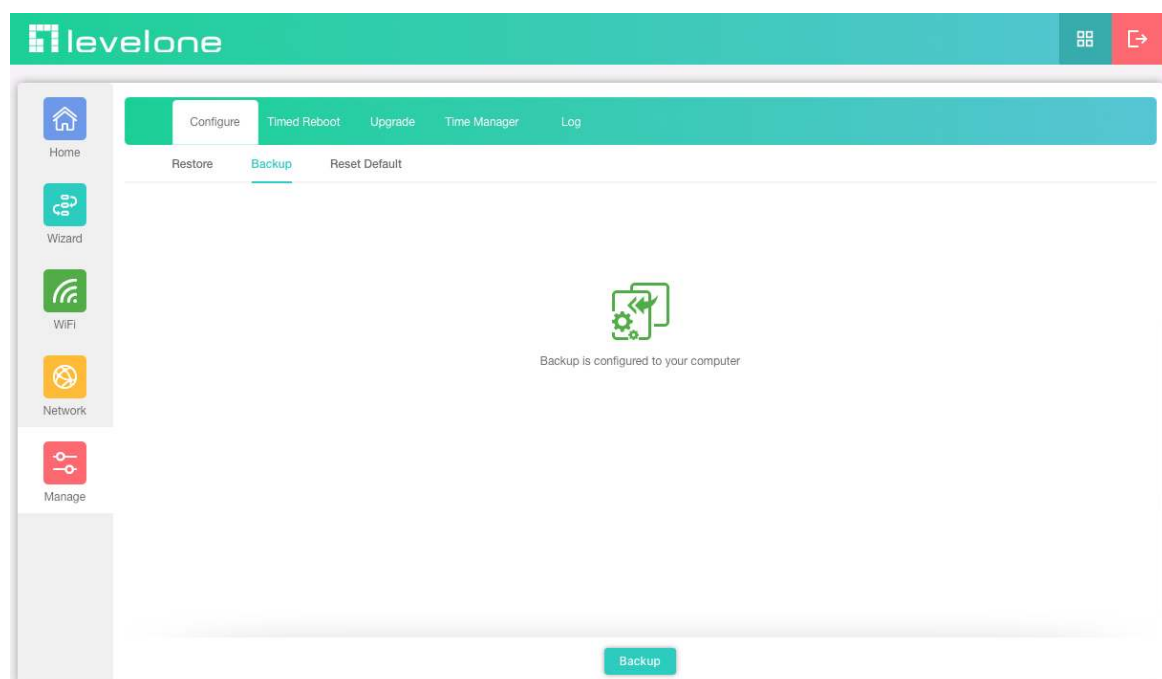
1. Restore

Drag the file here, or Click on the upload, upload the configuration file to overwrite the current configuration.



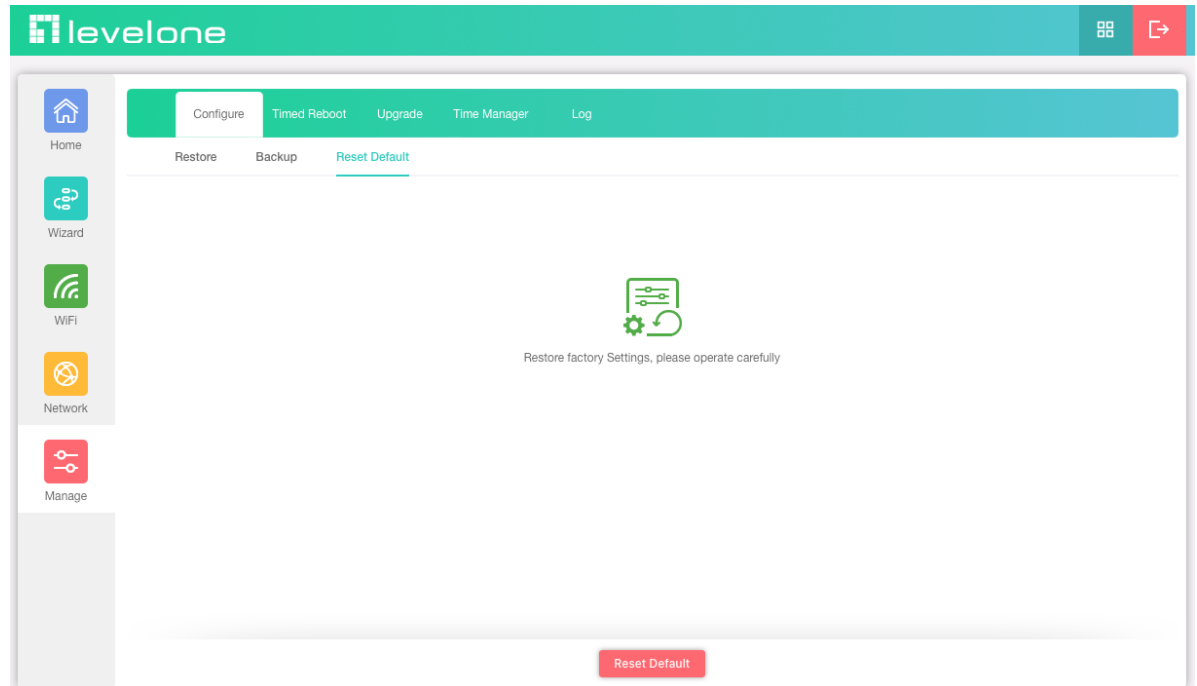
2. Backup

Backup configured to your computer



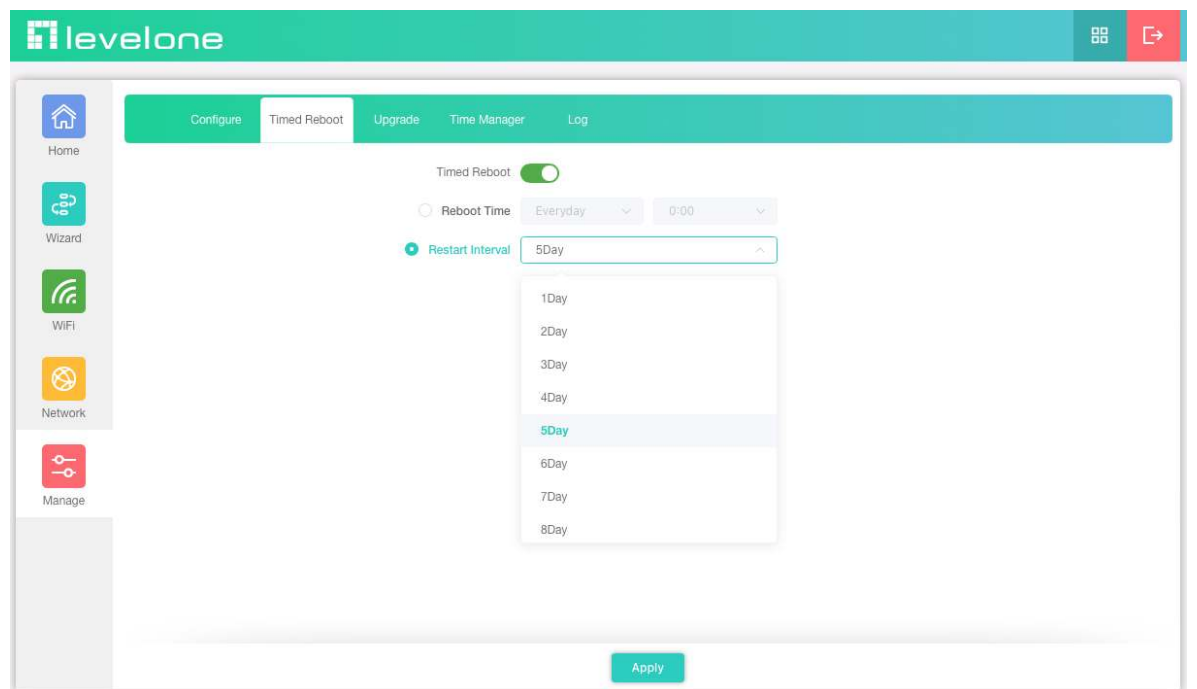
3. Reset Default

Restore the factory default settings, please press this Reset button



Timed Reboot

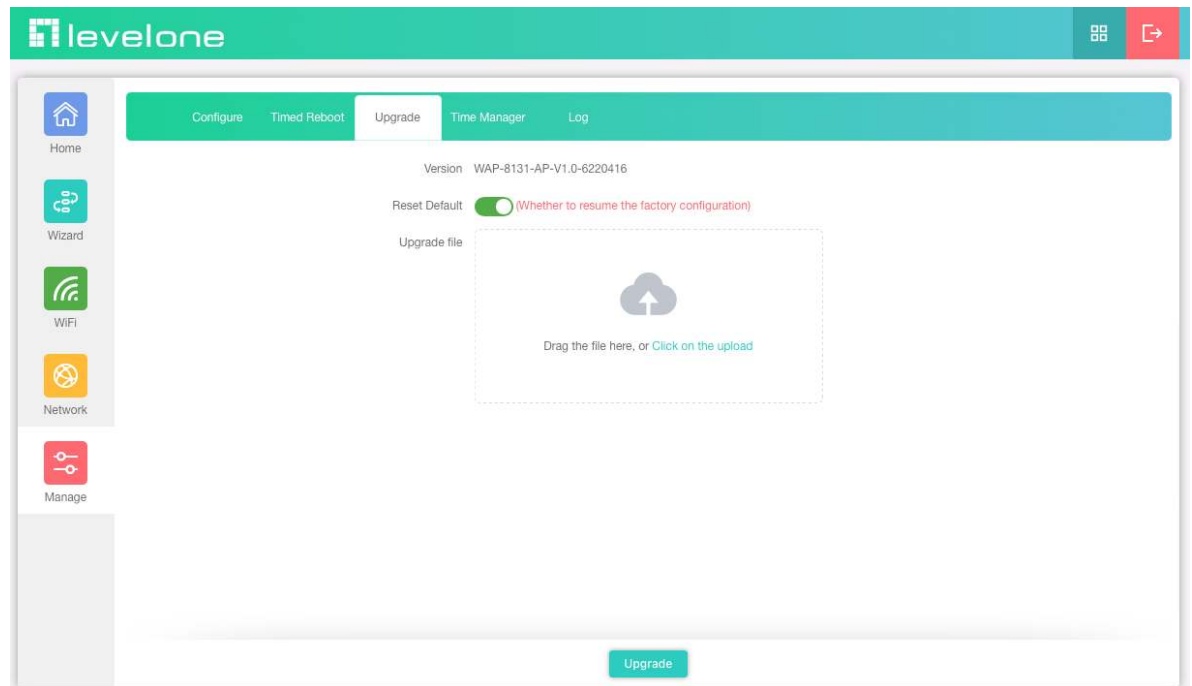
Set the scheduling time for rebooting the device yourself.



Upgrade

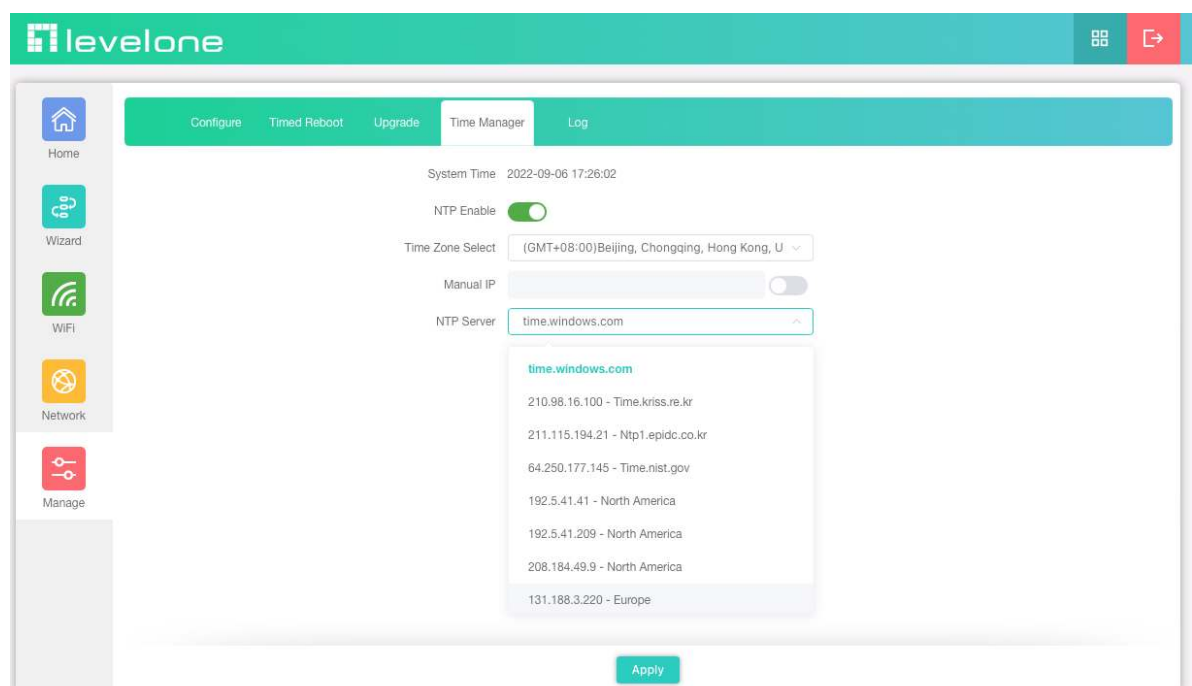
Click on the upload. The Firmware Upgrade window will appear. Insert the Firmware Path (or you can Browse for one) that you are going to use and click Upgrade. Please wait for the Upgrade Successful message to appear to complete the firmware upgrade.

Note: Please use to local computer is connected to the AP Lan port through an RJ45 cable to update the firmware first. After completing the update, empty the browser cache, otherwise the user interface may not be displayed correctly.



Time Manager

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



Log

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

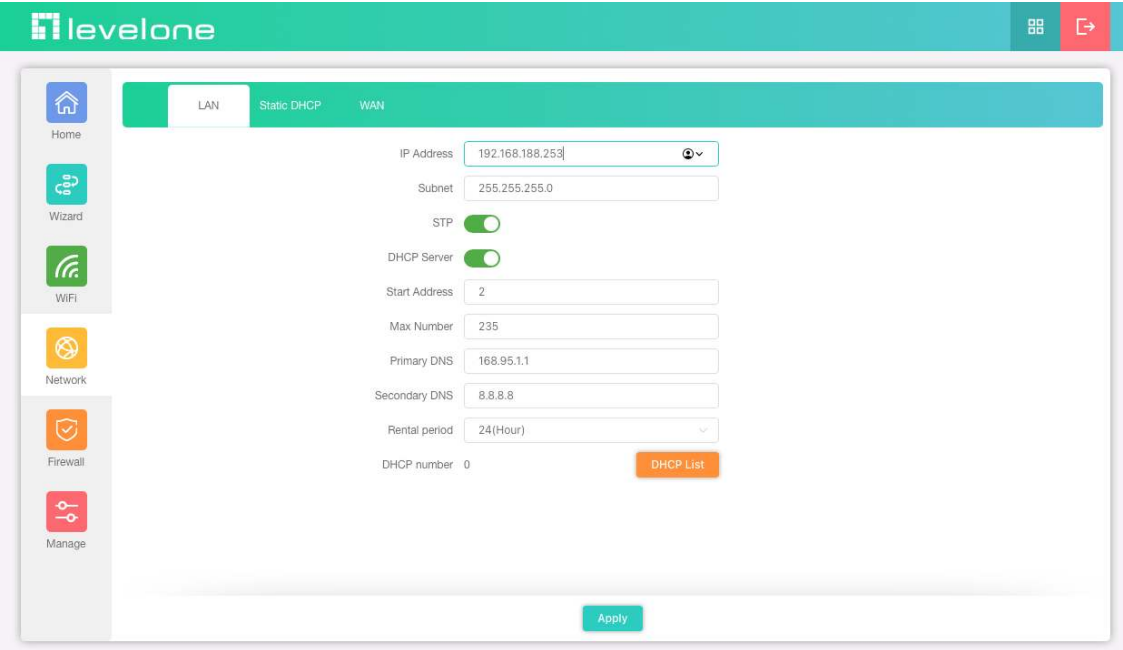
The screenshot displays the LevelOne web interface for device management. The top navigation bar includes the LevelOne logo and a menu icon. The left sidebar contains icons for Home, Wizard, WiFi, Network, and Manage. The main content area is titled 'Log' and shows a list of system logs. The logs are organized into columns: Date, Time, Device ID, Log Level, and Log Message. The log messages include system boot information, kernel notices, and hardware details. At the bottom of the log list, there are controls for the log service, including a toggle switch for 'Log', a 'Remote Log Service' toggle, a version number '0.0.0.0', and buttons for 'Apply', 'Export', 'Delete', and 'Refresh'.

Date	Time	Device ID	Log Level	Log Message
2022/09/06	16:57:24	WAP-8131	syslog.info	syslogd started: BusyBox v1.28.3
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] fixed : 0xffffffffbdc00000 - 0xffffffffbdc00000 (7 MB actual)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] PCI I/O : 0xffffffffbfae00000 - 0xffffffffbfae00000 (16 MB)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] modules : 0xffffffffb000000 - 0xffffffffb00000000 (64 MB)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] memory : 0xffffffffc00000000 - 0xffffffffc01000000 (496 MB)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] .init : 0xffffffffc00082f000 - 0xffffffffc00086a000 (236 KB)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] .text : 0xffffffffc00080000 - 0xffffffffc00082f000 (786 KB)
2022/09/06	16:57:24	WAP-8131	kern.notice	kernel: [0.000000] .data : 0xffffffffc00087b000 - 0xffffffffc00091c000 (644 KB)
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] SLUB: Hwalign=64, Order=0-3, MinObjects=0, CPUs=4, Nodes=1
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] Preemptible hierarchical RCU implementation.
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] Build-time adjustment of leaf fanout to 64.
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] NR_IRQS:64 nr_irqs:64 0
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] Architected cp15 timer(s) running at 24.00MHz (virt).
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000000] clocksource: arch_sys_counter: mask: 0xffffffffffffff max_cycles: 0x588fe9dc0, max_id
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000005] sched_clock: 56 bits at 24MHz, resolution 41ns, wraps every 4398046511097ns
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000409] Calibrating delay loop (skipped), value calculated using timer frequency.. 48.00 Bogo
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000421] pid_max: default: 32768 minimum: 301
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000517] Mount-cache hash table entries: 1024 (order: 1, 8192 bytes)
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.000527] Mountpoint-cache hash table entries: 1024 (order: 1, 8192 bytes)
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001066] Initializing cgroup subsys io
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001082] Initializing cgroup subsys memory
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001099] Initializing cgroup subsys devices
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001123] Initializing cgroup subsys freezer
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001135] Initializing cgroup subsys net_cls
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001145] Initializing cgroup subsys pids
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001391] EFI services will not be available.
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.001412] ASID allocator initialised with 65536 entries
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.051842] MSM Memory Dump base table set up
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.051866] MSM Memory Dump apps data table set up
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.090153] Detected VIPT I-cache on CPU1
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.090194] CPU1: Booted secondary processor [51af8014]
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.120143] Detected VIPT I-cache on CPU2
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.120170] CPU2: Booted secondary processor [51af8014]
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.150172] Detected VIPT I-cache on CPU3
2022/09/06	16:57:24	WAP-8131	kern.info	kernel: [0.150196] CPU3: Booted secondary processor [51af8014]

Section VI Network (For Gateway Mode)

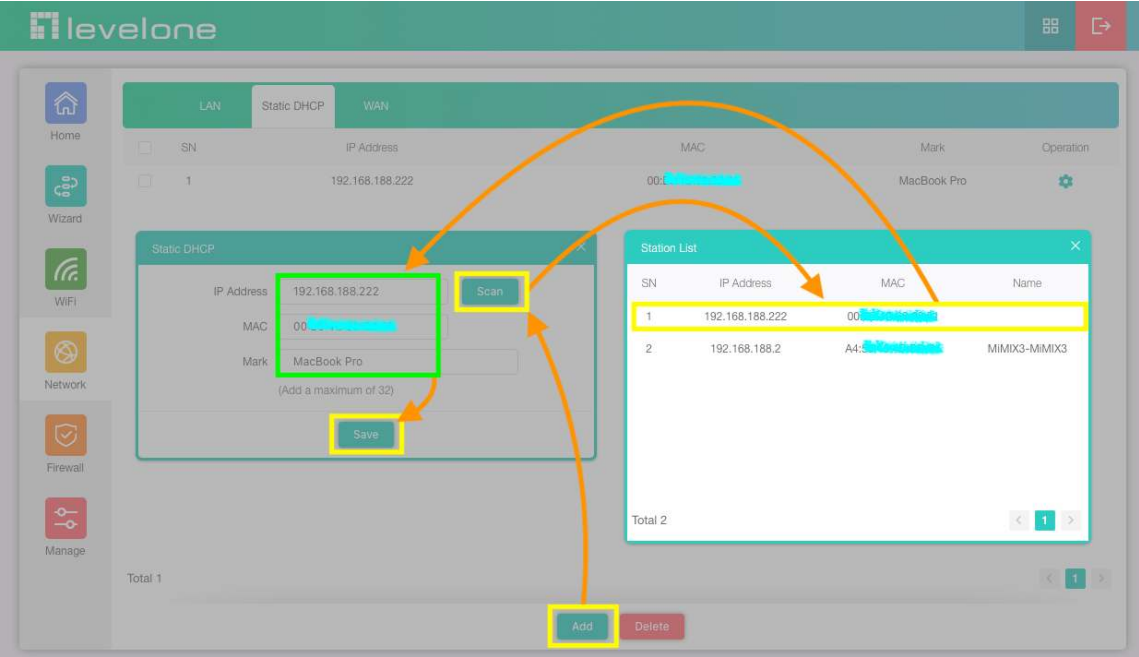
LAN Settings

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

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

Internet Mode: Static IP

The screenshot shows the LevelOne WAN configuration interface. The 'WAN' tab is selected. The 'Internet Mode' is set to 'Static IP'. The configuration fields are as follows:

Field	Value
Internet Mode	Static IP
IP Address	192.168.1.230
Subnet	255.255.255.0
Default Gateway	192.168.1.254
MTU	1500
Primary DNS	168.95.1.1
Secondary DNS	1.1.1.1
Band Type	1000M Fiber
Up	1000000 Kbps
Down	1000000 Kbps

On the right side, there are checkboxes for various features:

- ☐ Enable web server access on WAN port
- ☐ MAC Clone
- ☐ Enable Ping Access on WAN
- ☒ Enable IPsec pass through on VPN connection
- ☒ Enable PPTP pass through on VPN connection
- ☒ Enable L2TP pass through on VPN connection
- ☐ Line Detection

An 'Apply' button is at the bottom right.

Internet Mode: DHCP

The screenshot shows the LevelOne WAN configuration interface. The 'WAN' tab is selected. The 'Internet Mode' is set to 'DHCP'. The configuration fields are as follows:

Field	Value
Internet Mode	DHCP
MTU	1500
Set DNS Manually	Off
Primary DNS	168.95.1.1
Secondary DNS	1.1.1.1
Band Type	1000M Fiber
Up	1000000 Kbps
Down	1000000 Kbps

On the right side, there are checkboxes for various features:

- ☐ Enable web server access on WAN port
- ☐ MAC Clone
- ☐ Enable Ping Access on WAN
- ☒ Enable IPsec pass through on VPN connection
- ☒ Enable PPTP pass through on VPN connection
- ☒ Enable L2TP pass through on VPN connection
- ☐ Line Detection

An 'Apply' button is at the bottom right.

Internet Mode: PPPoE

The screenshot shows the LevelOne WAN configuration interface. The 'WAN' tab is selected. The 'Internet Mode' is set to 'PPPoE'. The configuration fields are as follows:

Field	Value
Internet Mode	PPPoE
Username	[Redacted]
Password	[Redacted]
Server Name	No Need, Don't fill
Service Name	No Need, Don't fill
MTU	1492
Set DNS Manually	Off
Primary DNS	168.95.1.1
Secondary DNS	1.1.1.1
Band Type	1000M Fiber
Up	1000000 Kbps
Down	1000000 Kbps

On the right side, there are checkboxes for various features:

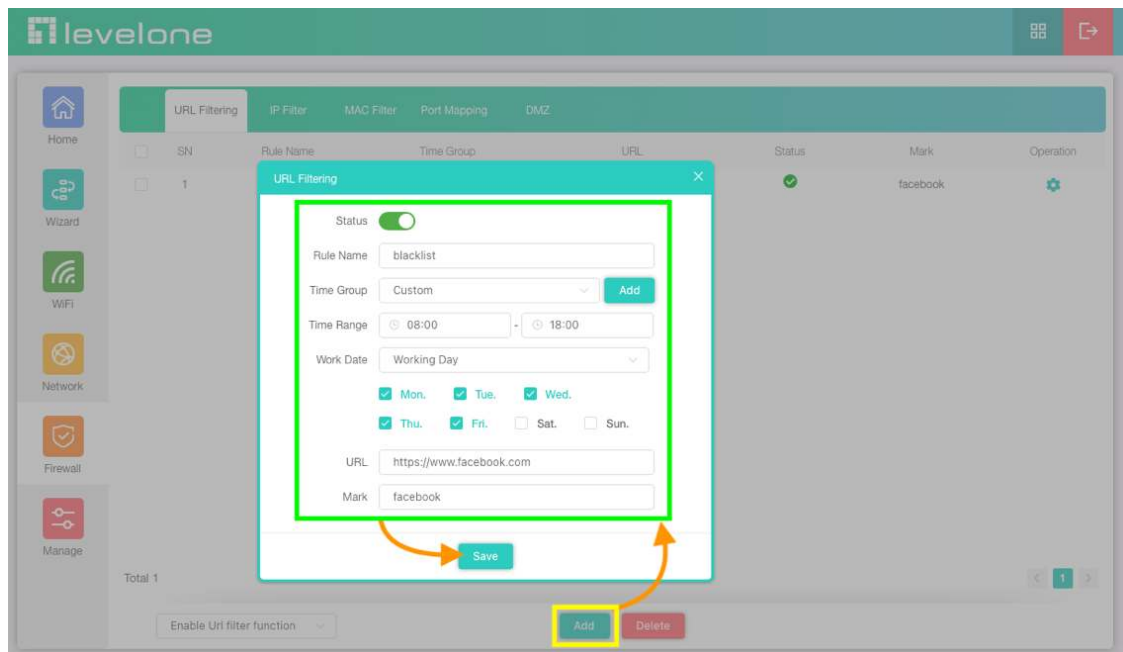
- ☐ Enable web server access on WAN port
- ☐ MAC Clone
- ☐ Enable Ping Access on WAN
- ☒ Enable IPsec pass through on VPN connection
- ☒ Enable PPTP pass through on VPN connection
- ☒ Enable L2TP pass through on VPN connection
- ☐ Line Detection

An 'Apply' button is at the bottom right.

Section VII Firewall (For Gateway Mode)

URL Filtering

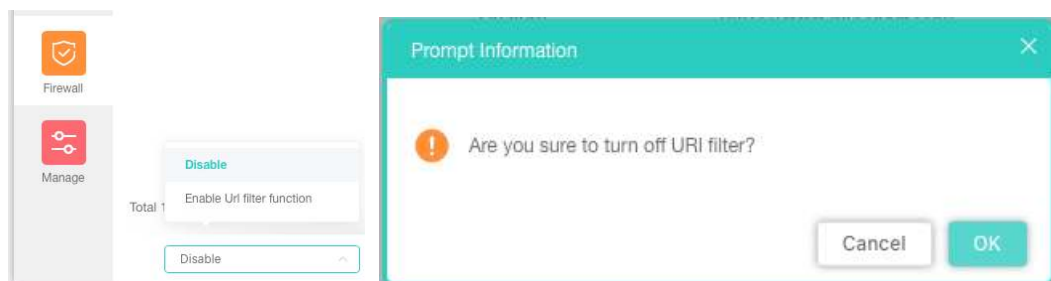
Set URL Filter list, Manage which websites cannot be accessed within a specified time.



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

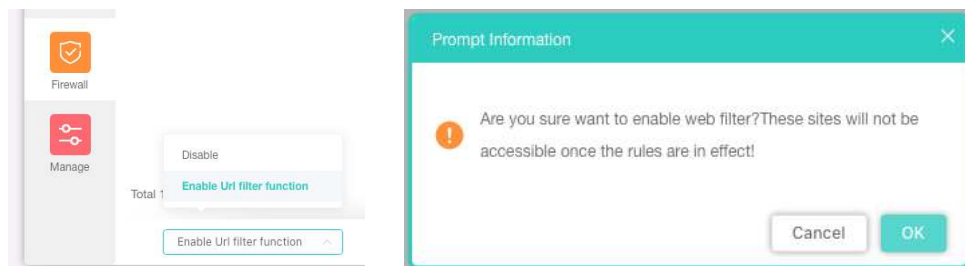
1. Disable

Turn off URI filter

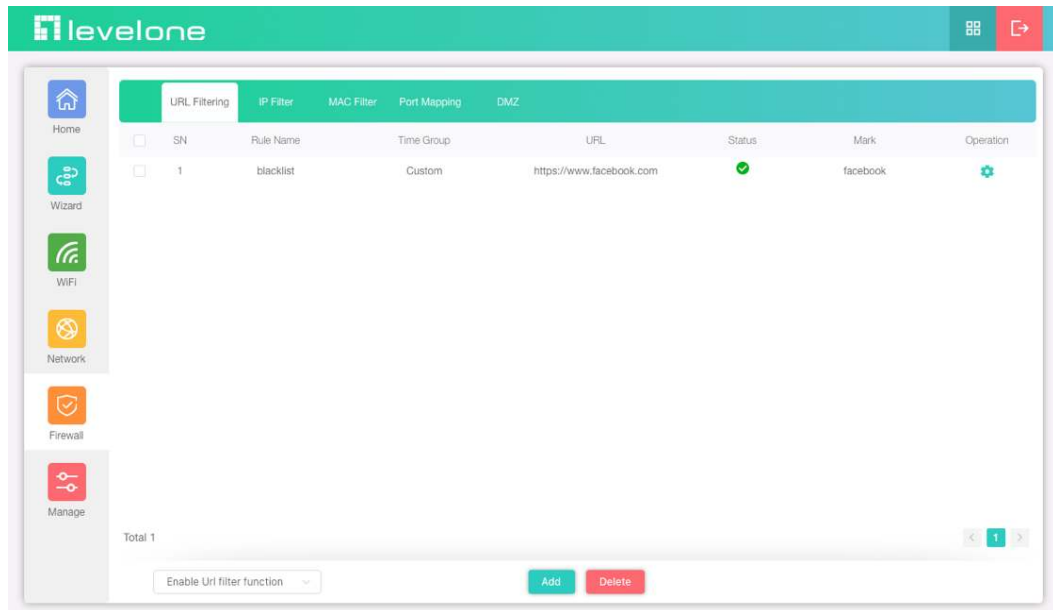


2. Enable URL Filter function

- These sites will not be accessible once the rules are in effect !

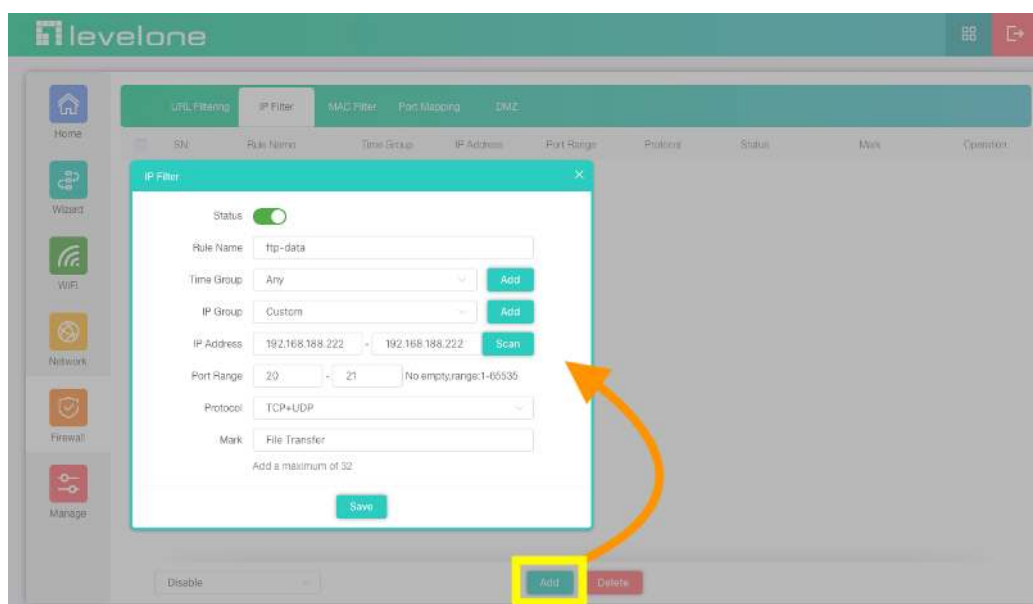


- These sites will not be accessible once the rules are in effect.



IP Filter

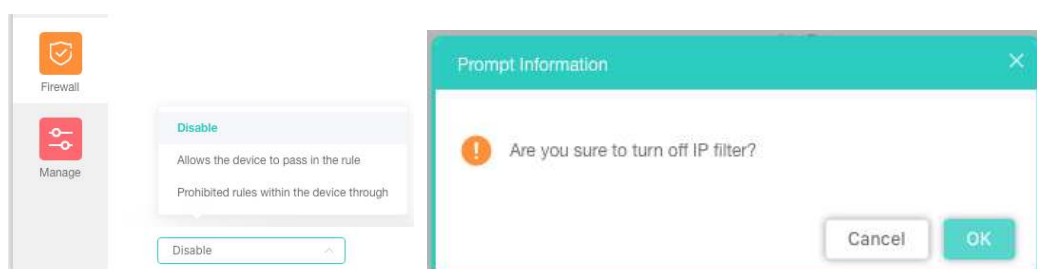
Set the IP Filter list to manage the inability to access the specified service transport protocol port number range(1-65535) within a specified time, need to cooperate with the IP Group function.



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

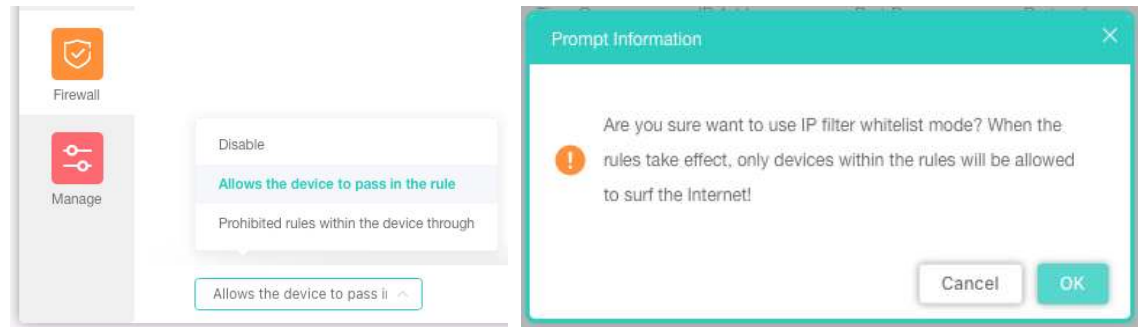
1. Disable

Factory default is disable

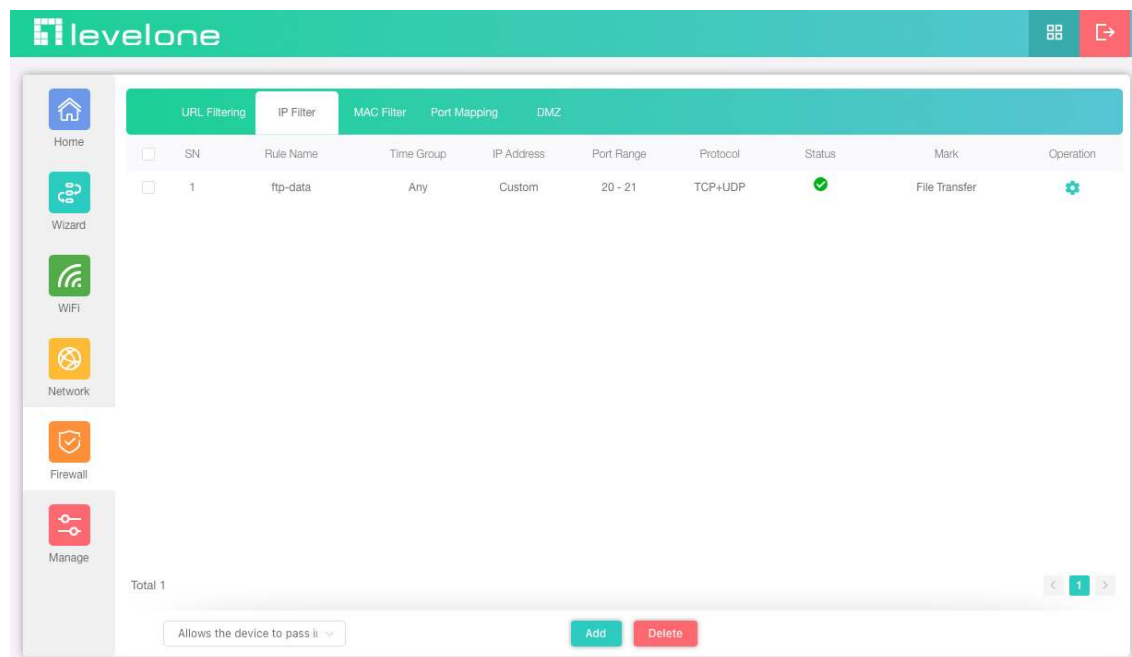


2. Allows the device to pass in the rule (IP filter whitelist mode)

- When the rules take effect, only devices within the rules will be allowed to surf the Internet

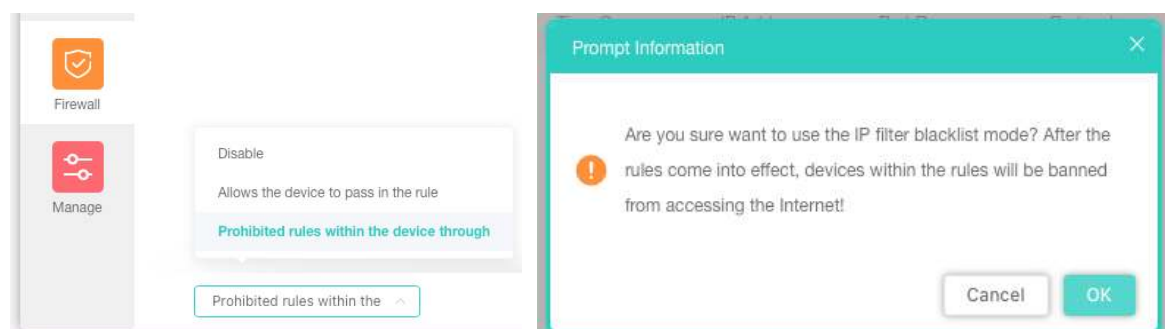


- When the rules take effect, only devices within the rules will be allowed to FTP service.

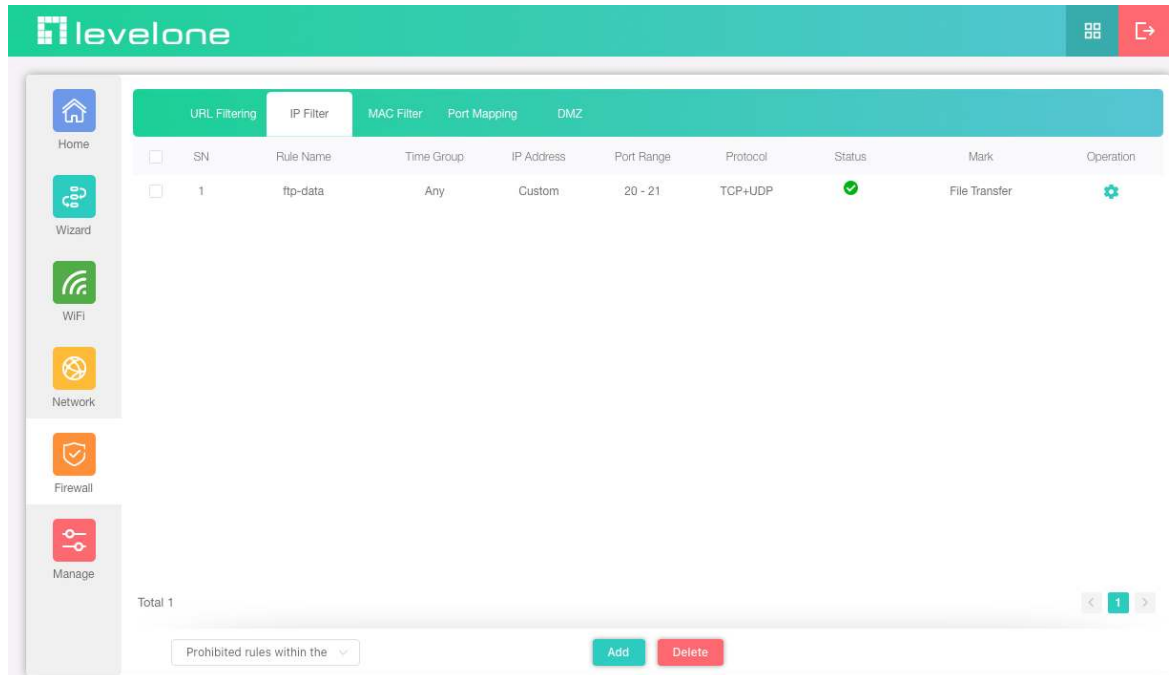


3. Prohibited rules within the device through (IP filter blacklist mode)

- After the rules come into effect, devices within the rules will be banned from accessing the Internet!

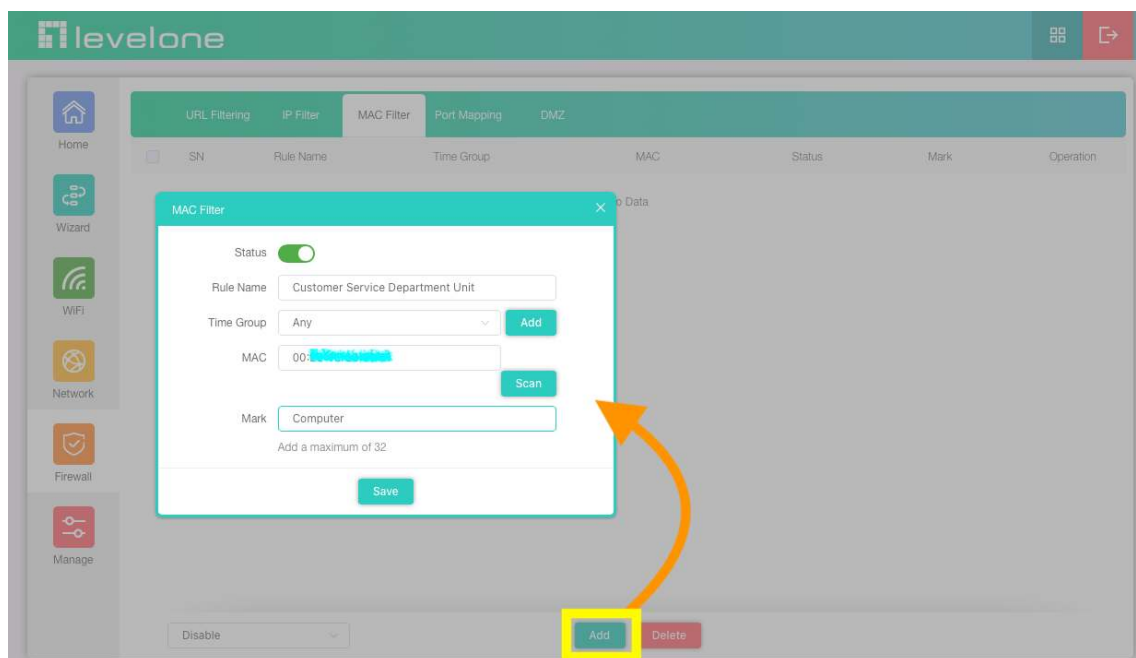


- The FTP service and service transport protocol port number range(20-21) will not be accessible once the rules are in effect.



MAC Filter

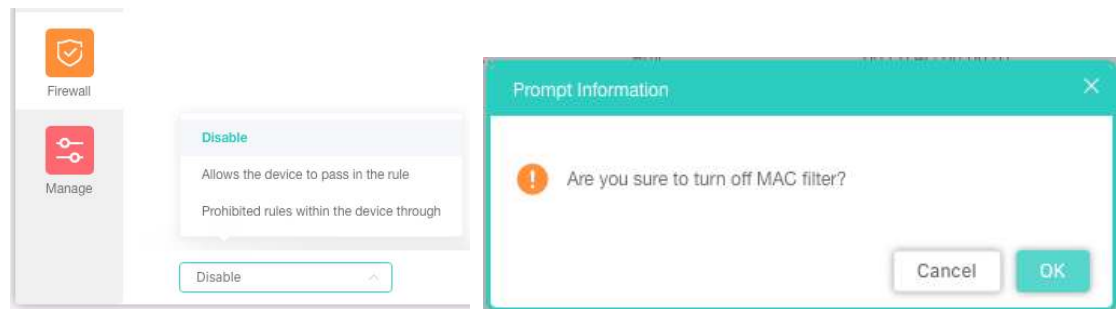
Establish MAC filtering to manage device online behavior.



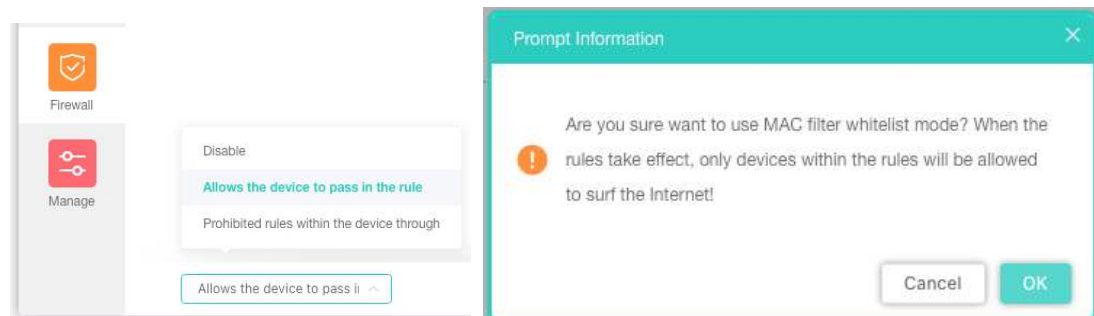
Choose according to the current use needs. After selecting, please click Apply.

1. Disable

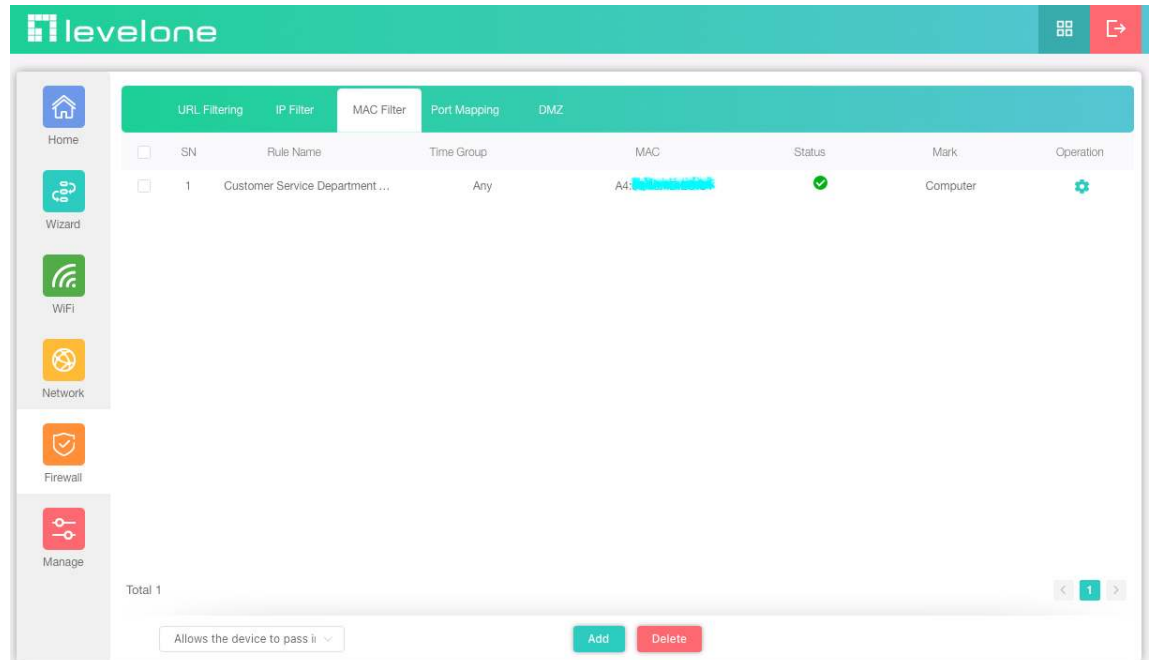
Factory default is disable



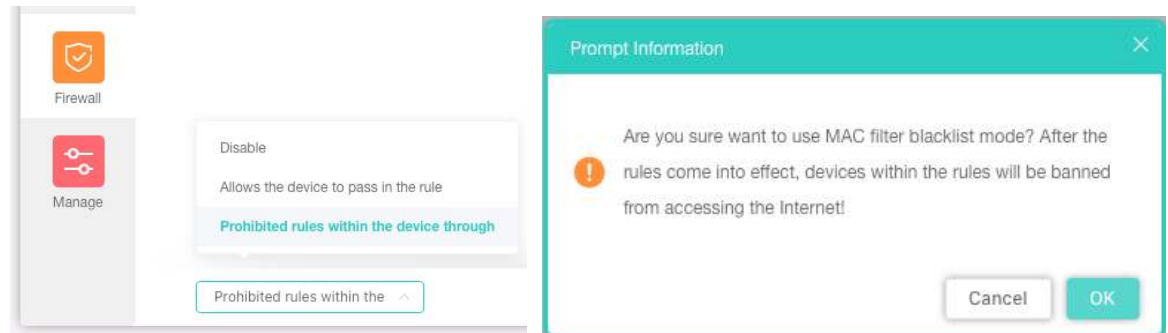
2. Allows the device to pass in the rule (IP filter whitelist mode)



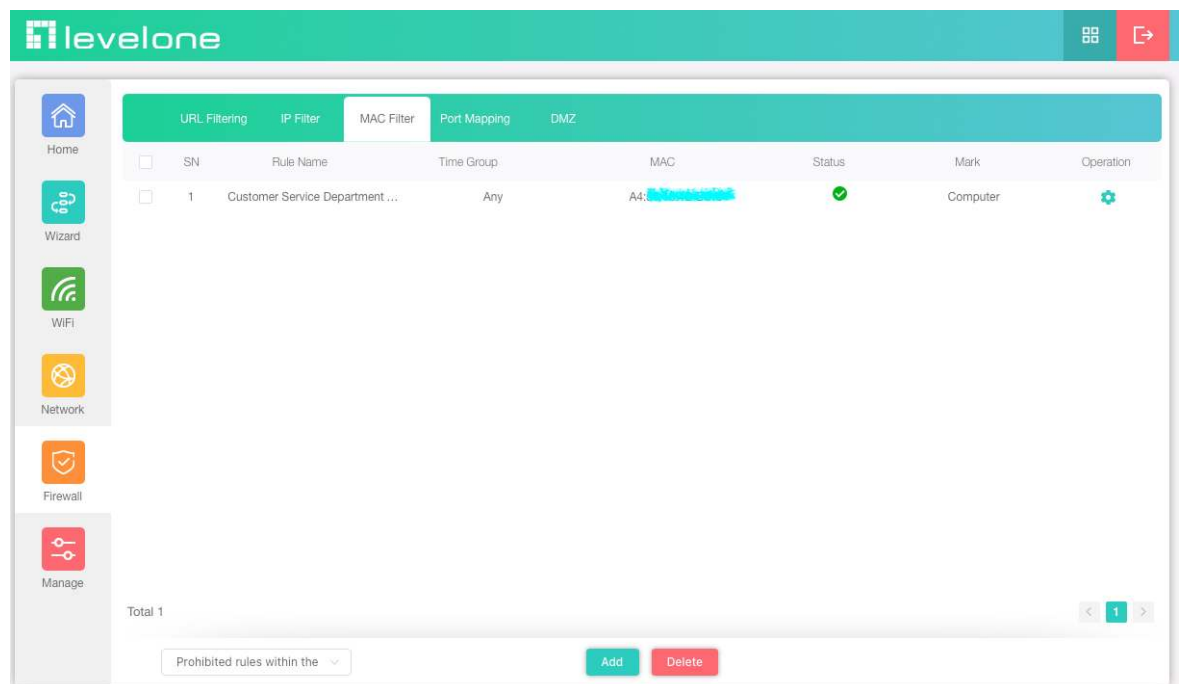
- When the rules take effect, only devices within the rules will be allowed to surf the Internet



3. Prohibited rules within the device through (IP filter blacklist mode)



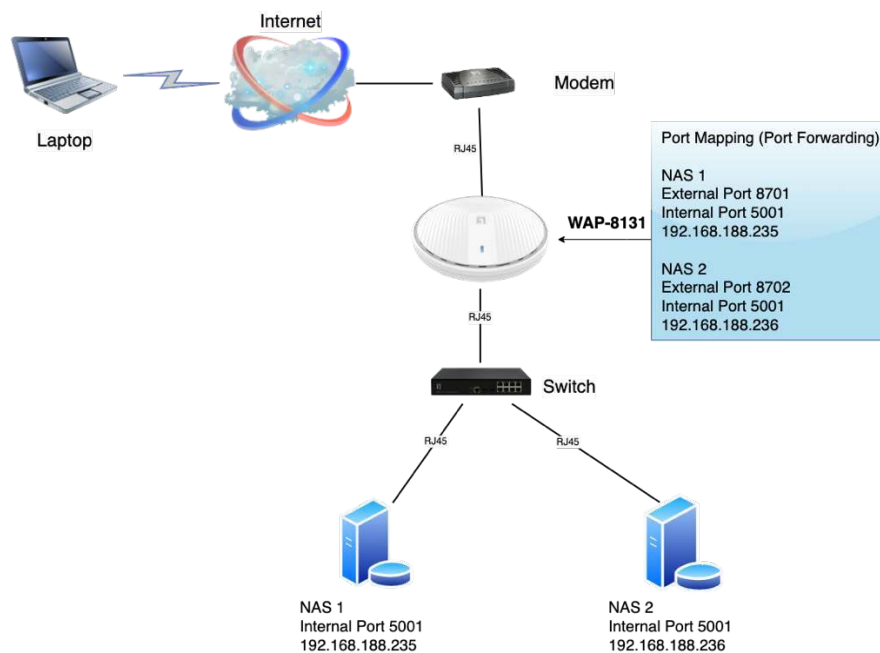
- After the rules come into effect, devices within the rules will be banned from accessing the Internet.



Port Mapping (Port Forwarding)

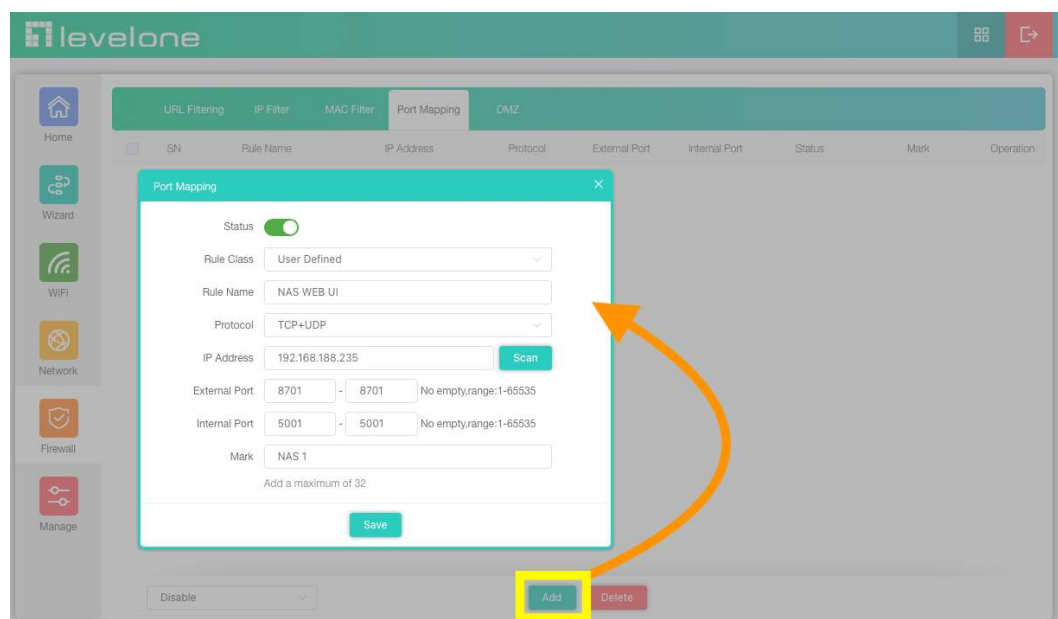
In computer networking, port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

Network Architecture Diagram Example



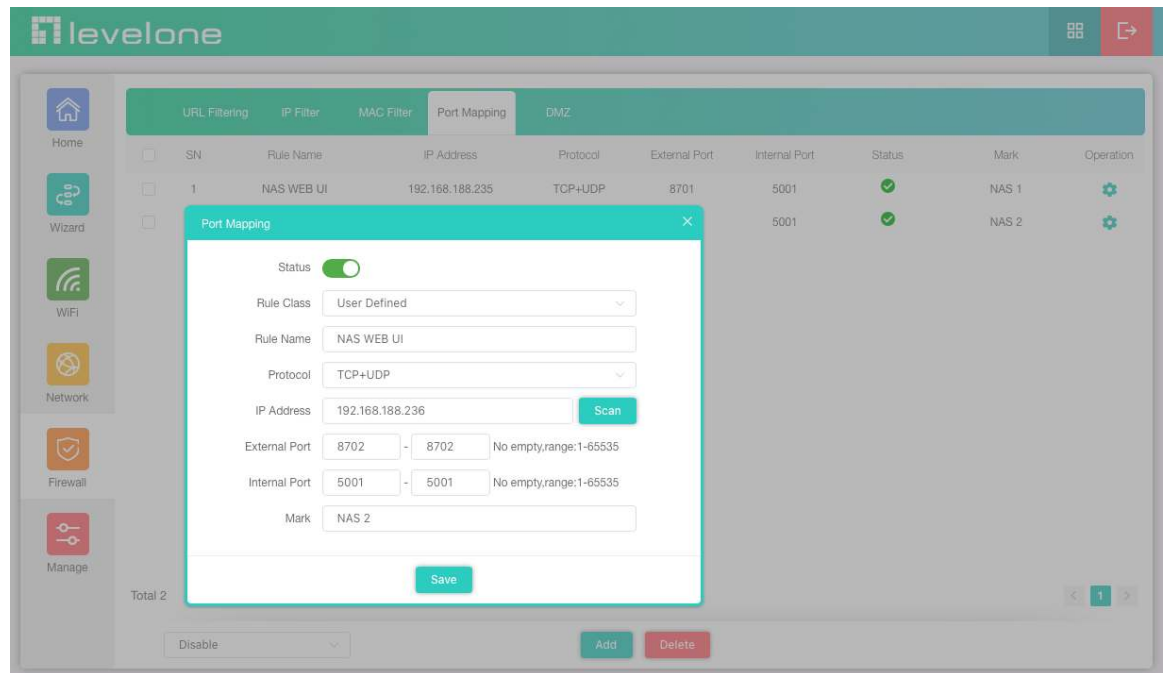
1. To configure Port Mapping for internal NAS1

- Through the Port Mapping function, service transport protocol port number 5001 to 8701, by remapping the destination IP address and port number of the communication to an internal NAS1 (192.168.188.235).

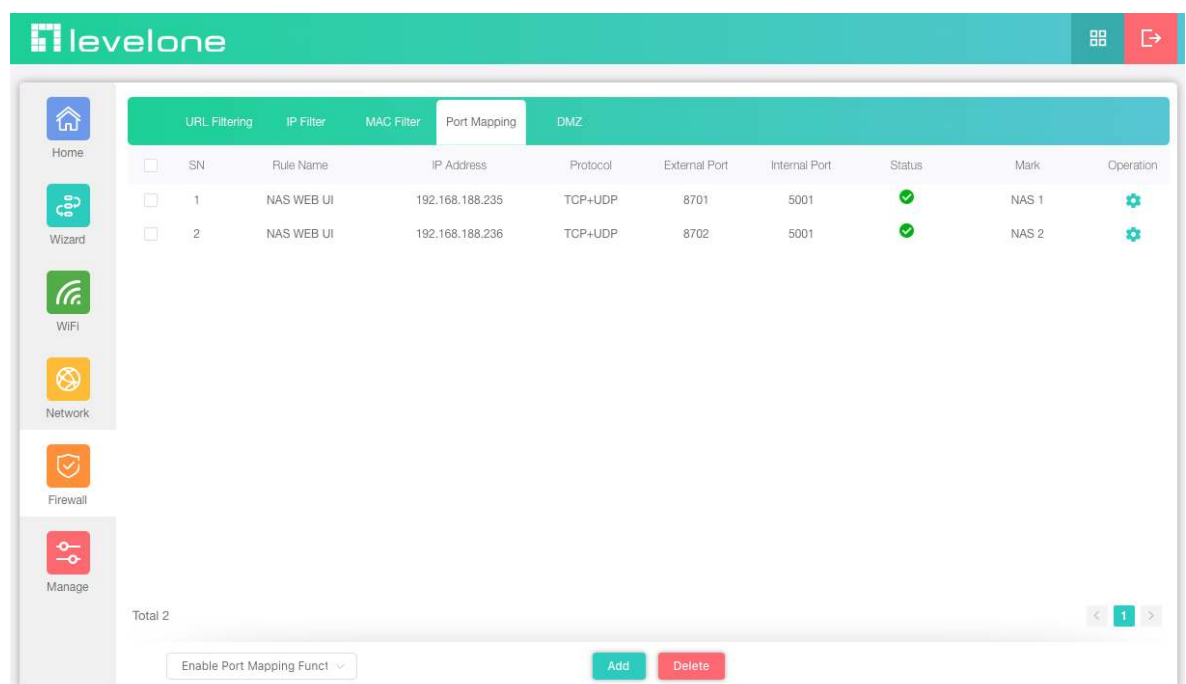
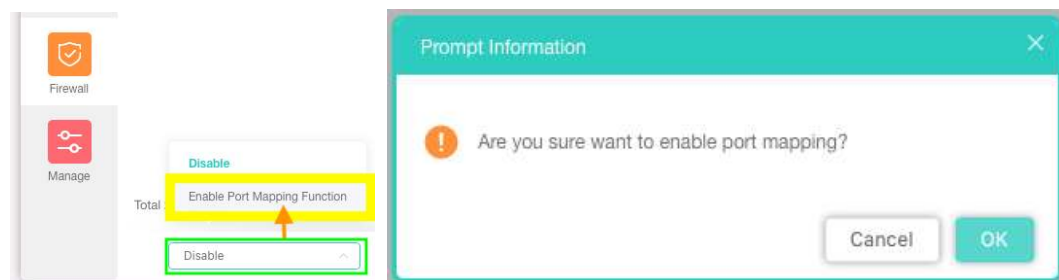


2. To configure Port Mapping for internal NAS2

- Through the Port Mapping function, service transport protocol port number 5001 to 8702, by remapping the destination IP address and port number of the communication to an internal NAS2(192.168.188.236).



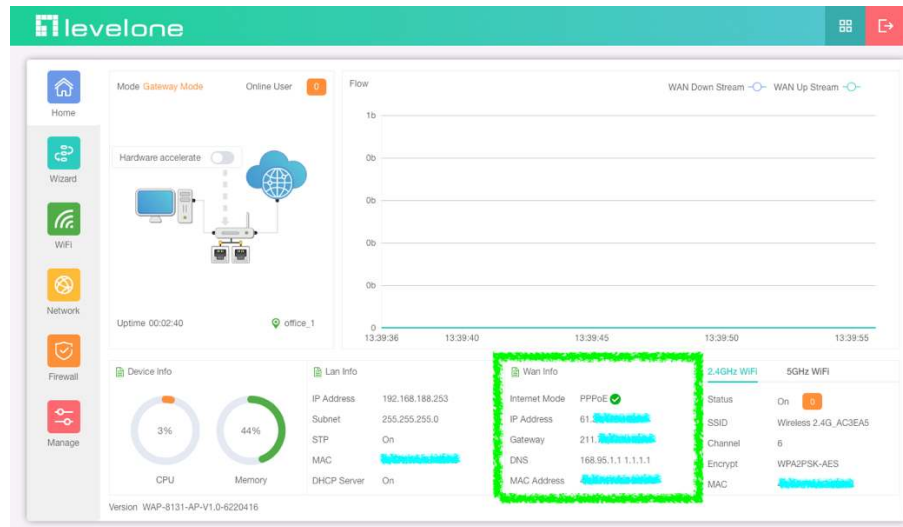
- Click below to Enable Port Mapping function



Verify confirmation

- Record the real IP address currently displayed in the WAN info.

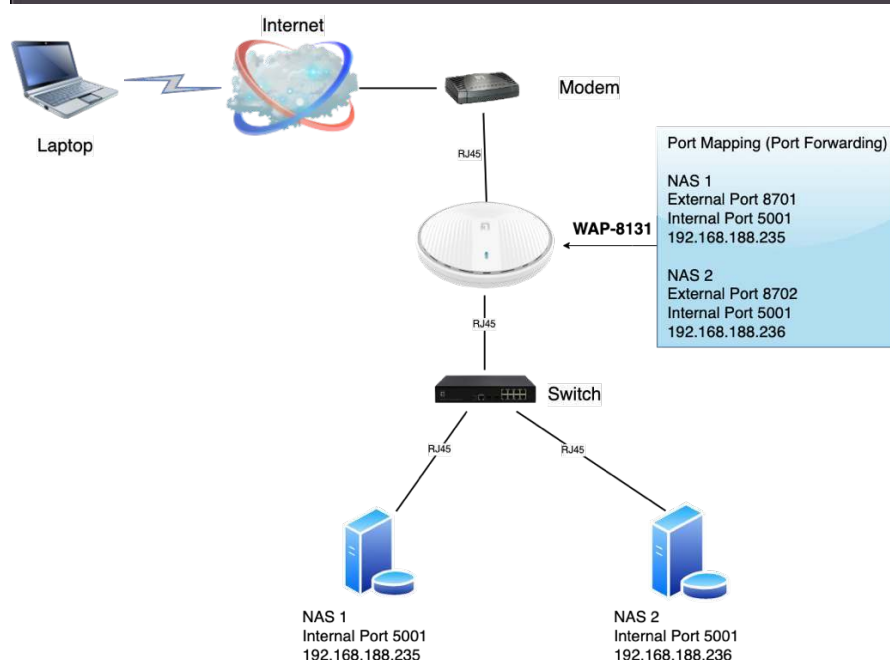
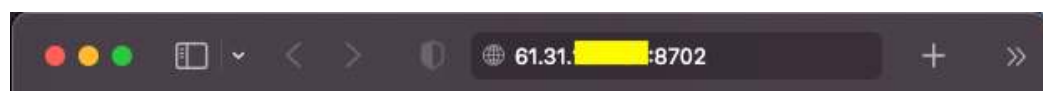
Note: IP Address of 192.168.X.X / 172.X.X.X / 10.X.X.X are displayed, it means that there is still a router on the upper end that is allocating IP address by DHCP, please confirm with the telecom provider that provides the network



- The Laptop of the external Internet can enter the real ip address and : 8701 Connect to the internal network NAS1 management page.



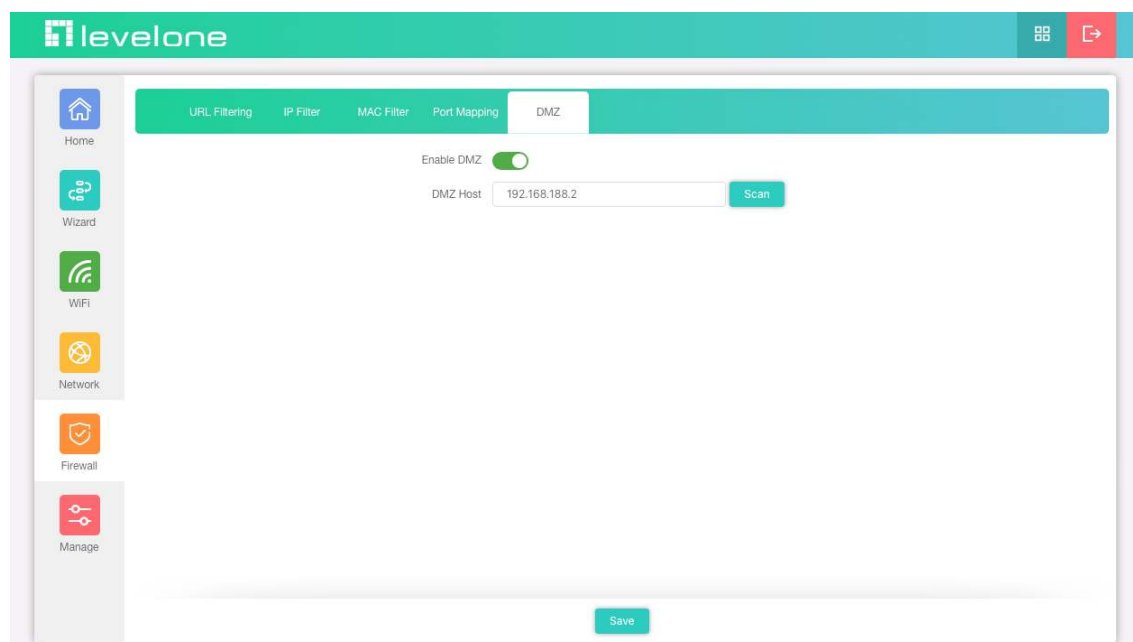
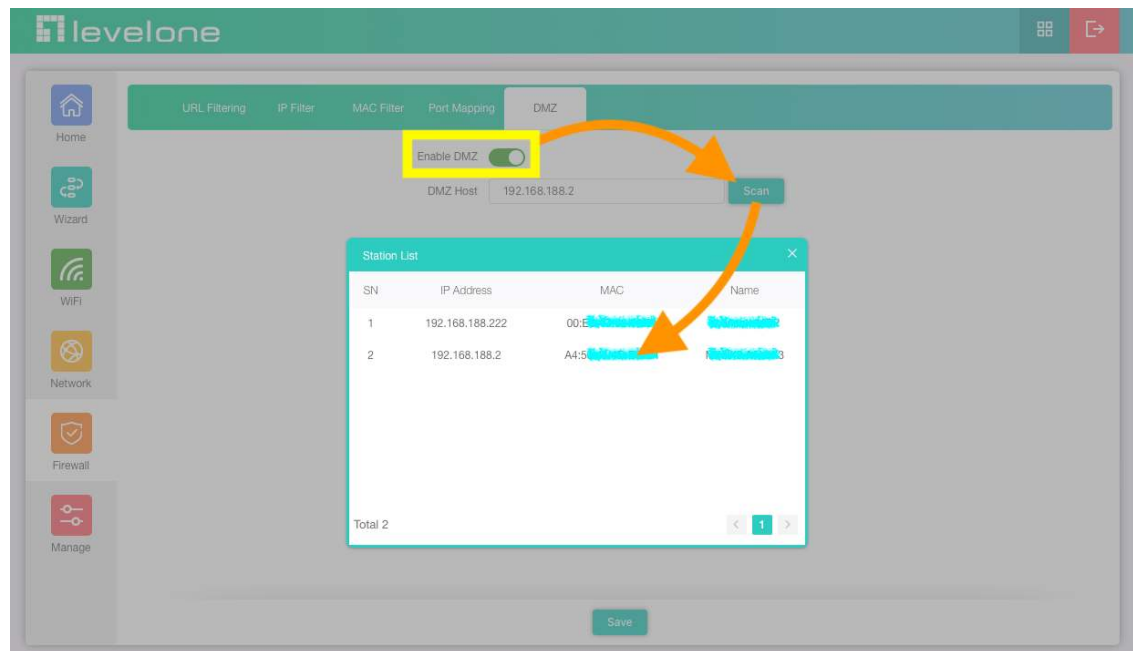
- The Laptop of the external Internet can enter the real ip address and : 8702 Connect to the internal network NAS2 management page.



DMZ (Demilitarized Zone)

The specified intranet device all service transport protocol port enabled and can be accessed from the external network.

Note: 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.

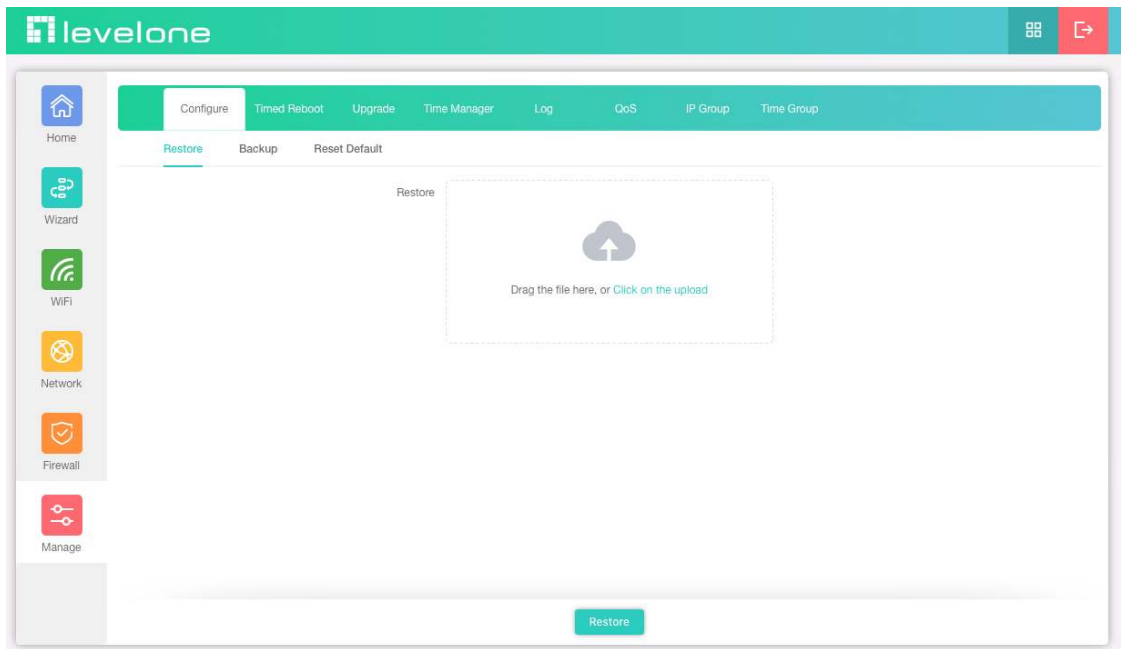


Section VIII Manage (For Gateway Mode)

Configure

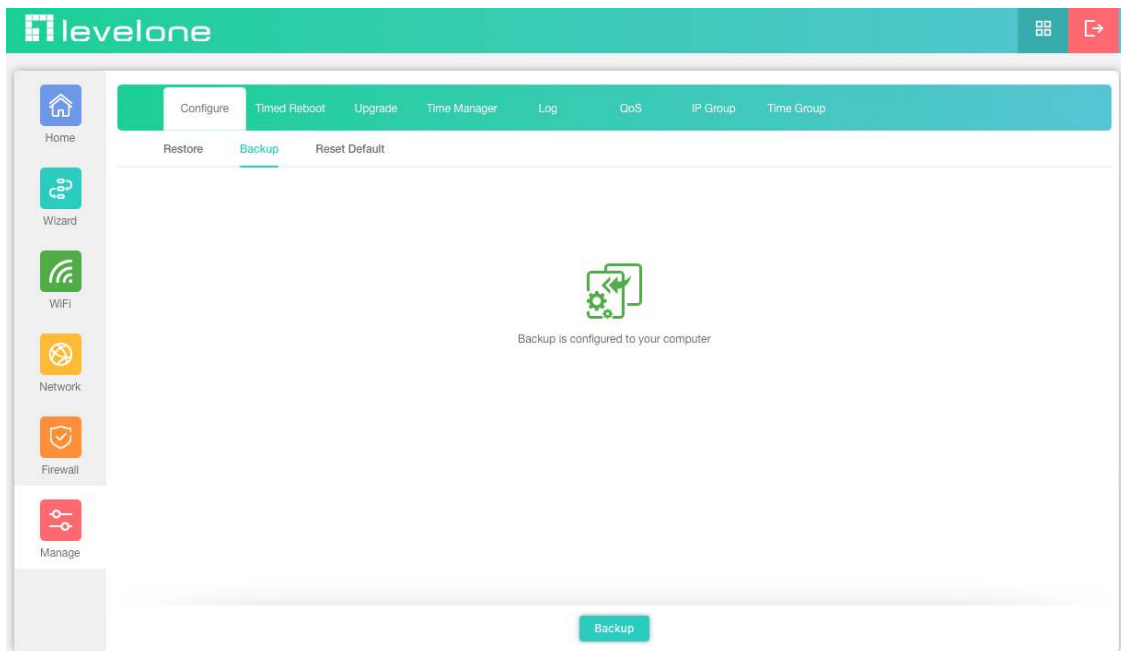
1. Restore

Drag the file here, or Click on the upload, upload the configuration file to overwrite the current configuration.



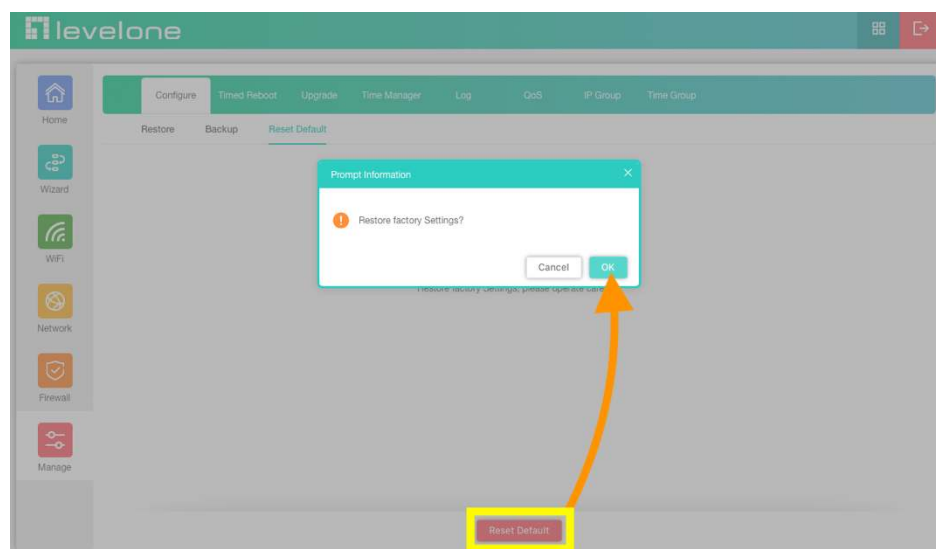
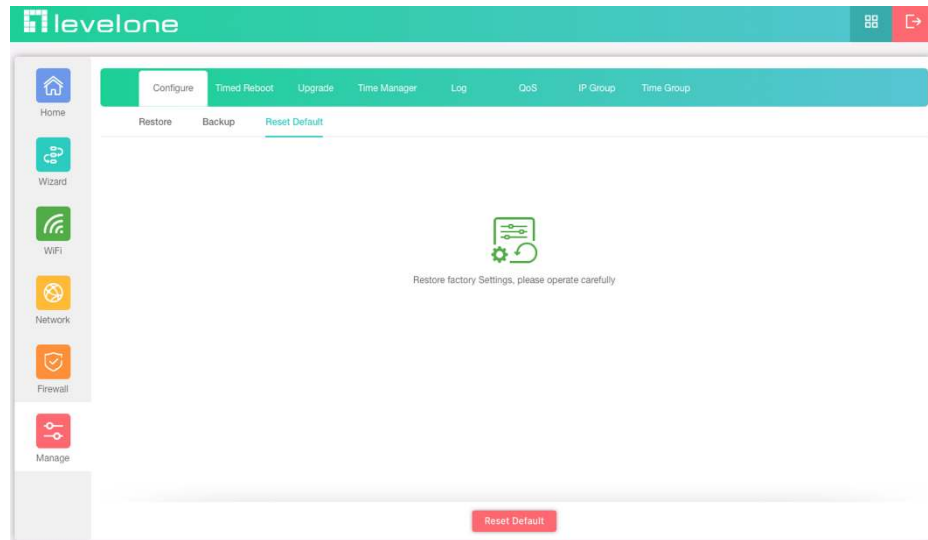
2. Backup

Backup configured to your computer



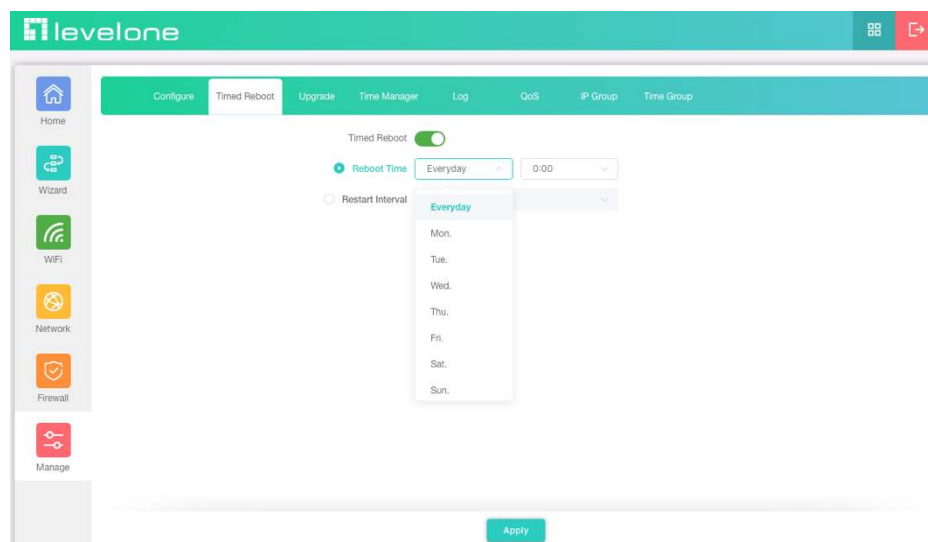
3. Reset Default

Restore factory Settings, please operate carefully.



Timed Reboot

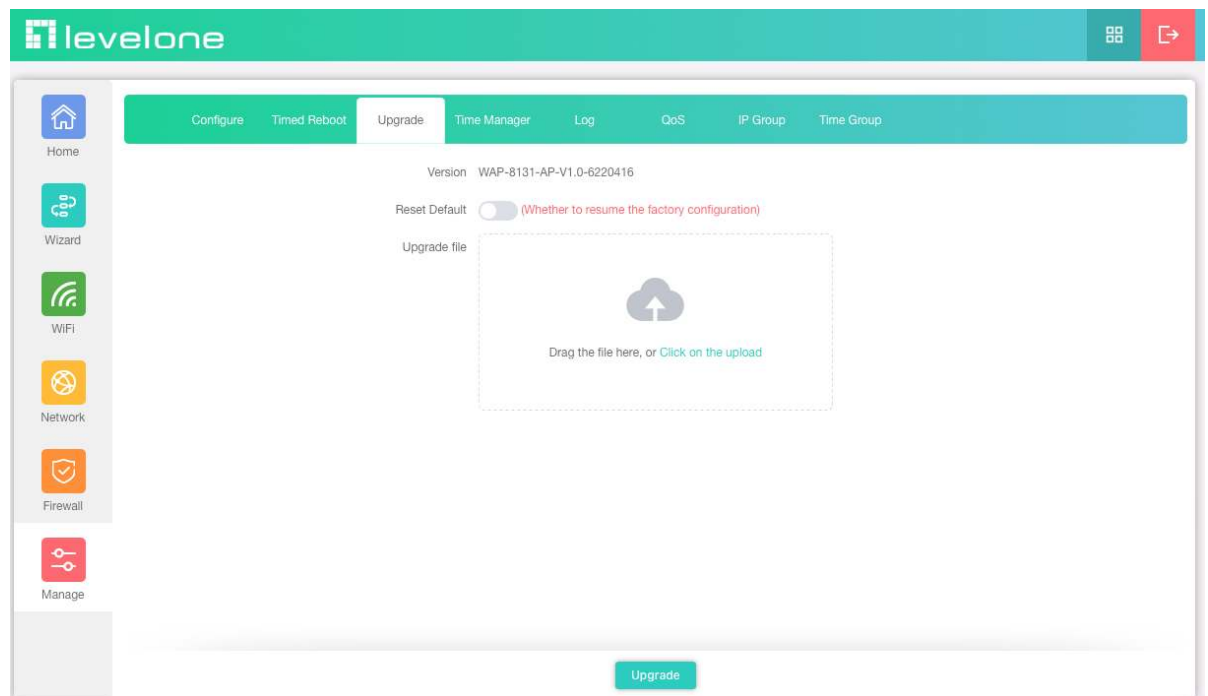
Set the scheduling time for rebooting the device yourself



Upgrade

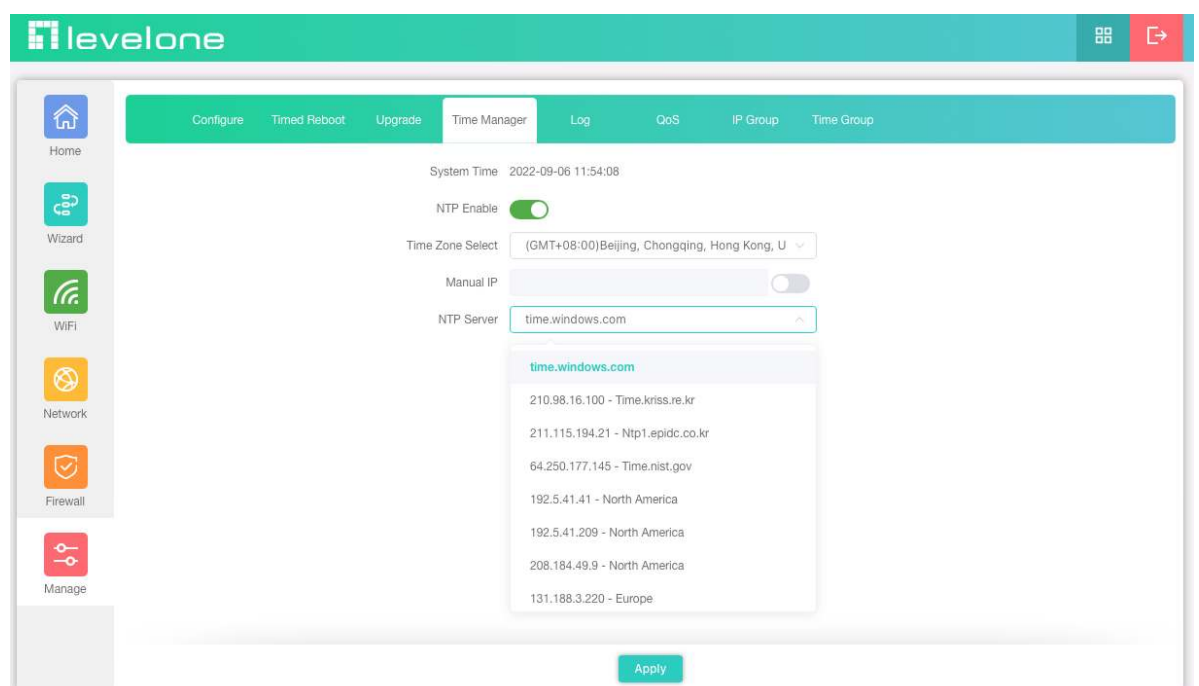
Click on the upload. The Firmware Upgrade window will appear. Insert the Firmware Path (or you can Browse for one) that you are going to use and click Upgrade. Please wait for the Upgrade Successful message to appear to complete the firmware upgrade.

Note: Please use to local computer is connected to the AP Lan port through an RJ45 cable to update the firmware first. After completing the update, empty the browser cache, otherwise the user interface may not be displayed correctly.



Time Manager

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



Log

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

The screenshot shows the LevelOne web interface with the 'Log' tab selected. The interface includes a sidebar with navigation icons (Home, Wizard, WiFi, Network, Firewall, Manage) and a top navigation bar with tabs (Configure, Timed Reboot, Upgrade, Time Manager, Log, QoS, IP Group, Time Group). The Log tab displays a list of system logs with timestamps and messages. At the bottom, there are controls for Log (toggle), Remote Log Service (toggle), and buttons for Apply, Export, Delete, and Refresh.

QoS (Quality of Service)

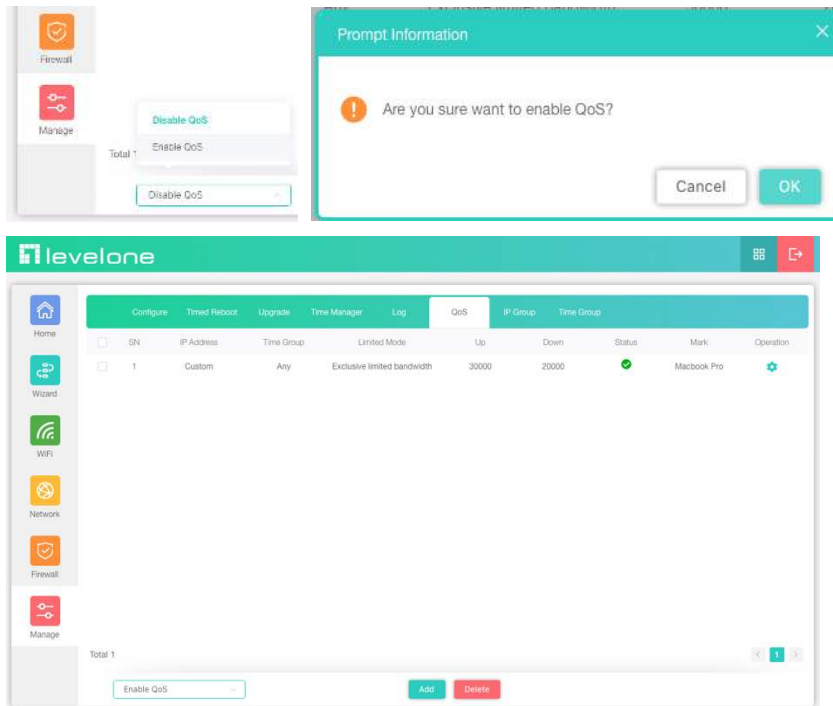
1. Can restrict Flow Control of specified device IP or IP Group.

Limited Mode

- Shared limited bandwidth
- Exclusive limited bandwidth

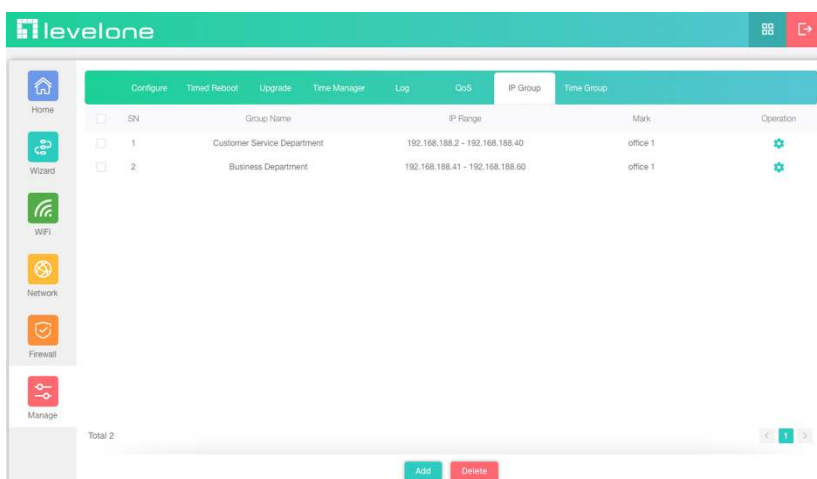
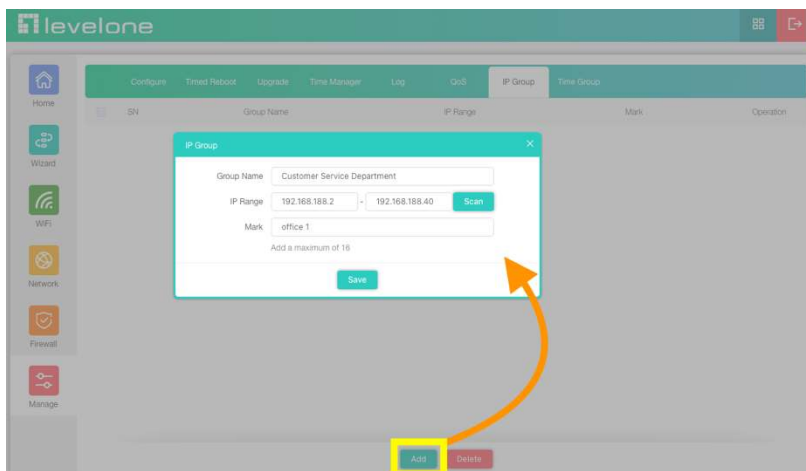
The screenshot shows the LevelOne web interface with the 'QoS' tab selected. The interface includes a sidebar with navigation icons (Home, Wizard, WiFi, Network, Firewall, Manage) and a top navigation bar with tabs (Configure, Timed Reboot, Upgrade, Time Manager, Log, QoS, IP Group, Time Group). The QoS tab displays a table with columns for SN, IP Address, Time Group, Limited Mode, Up, Down, Status, Mark, and Operation. An 'IP Filter' dialog box is open, showing fields for IP Group (Custom), IP Address (192.168.188.222), Time Group (Any), Limited Mode (Exclusive limited bandwidth), Up (30000 Kbps), Down (20000 Kbps), and Mark (Macbook Pro). The dialog box has a 'Save' button and a note 'Add a maximum of 32'. An orange arrow points from the 'Add' button in the bottom right of the QoS table to the 'Add' button in the IP Filter dialog box.

2. Click below to Enable QoS function



IP Group

The establishment of IP groups is easy to manage and can be applied to IP Filter / QoS functional options.



Time Group

Create a time management group, which can be applied to the following functional options.

- URL Filtering
- IP Filter
- MAC Filter
- QoS

