WAVLINK

see the world

User Manual

Wi-Fi 7 BE5100 Whole Home Mesh Wi-Fi System

Model: HALO Nexus

@WavlinkOfficial

@WavlinkTechSupport

Table of contents:

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used :

Convention	Description
Underlined	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	The content and text that needs to be emphasized on the web page is the theme color `#1D428A` , including menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example,**More > Network > Mode Selection** means the Mode Selection function page is under the Network menu that is located in the More tab.
Note:	Do not ignore this type of comment, it is to remind you to better use the device, to avoid the operation of the error that will cause the function to be invalid.
Tips:	Indicates important information that helps you make better use of your device.

More Info

The latest software, management app and utility are available from the Download Center at **https://docs.wavlink.xyz/Firmware/** .

A quick installation guide can be found in this guide.

Specifications can be found on the product page at **https://docs.wavlink.xyz/**.

If you encounter any issues, please don’t hesitate to email *contact@wavlink.com*/*techsupport@wavlink.com*/*postsales@wavlink.com* to provide feedbacks or contact online customer service, thank you !

Speed/Coverage Disclaimer

Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

Information in this document is subject to change without notice.The manufacturer does not make any representations or warranties (implied or otherwise) regarding the accuracy and completeness of this document and shall in no event be liable for any loss of profit or any commercial damage,including but not limited to special, incidental, consequential, or other damage.

Safety Instructions

Always read the safety instructions carefully.

Keep this Quick Start Guide for future reference.

Keep this equipment away from humidity.

If any of the following situation arises, get the equipment checked by a service technician:

The equipment has been exposed to moisture.

The equipment has been dropped and damaged.

The equipment has an obvious sign of breakage.

The equipment has not been working well or you cannot get it work according to Quick start Guide.

Copyright Statement

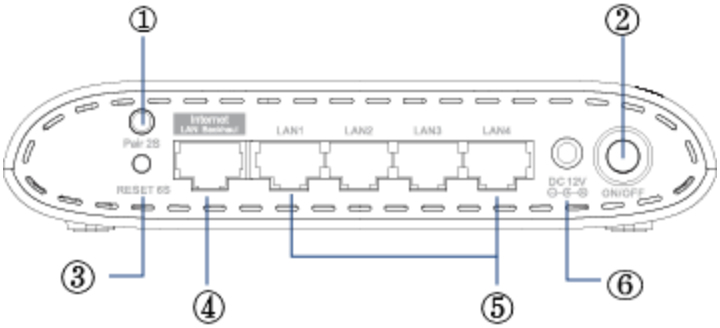
WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic eauipment, or returned to the supplier for disposal.

Chapter 1 Overview

This chapter contains the following sections :

Hardware Overview



① PAIR

② Power Switch

③ RESET

④ 1×2.5 Gigabit WAN Port

⑤ 4×Gigabit LAN Port

⑥ DC 12V

⑦ LED Indicator

Basic Info

2.4G SSID:WAVLINK-Mesh_XXXX
5G SSID:WAVLINK-Mesh_XXXX
Default IP: http://192.168.20.1
Login:http://wavlogin.link

LED Indicator

Mode	LED Status and Description
Router Mode	Blue on:The Internet connected Fast blinking in red:No Internet connected Slow blinking in blue:In pairing
Repeater Mode	Blue on:The Internet connected Slow blinking in red:Upper router connected but the Internet disconnected Fast blinking in red: Upper router disconnected
AP Mode	Blue on: The Internet connected Fast blinking in red:No Internet connected Slow blinking in blue:In pairing

Pair Button: Press and hold Pair for 2 seconds then release, and the LED will turn slow-flashing blue to add an extra mesh device to the existing Wi-Fi system.

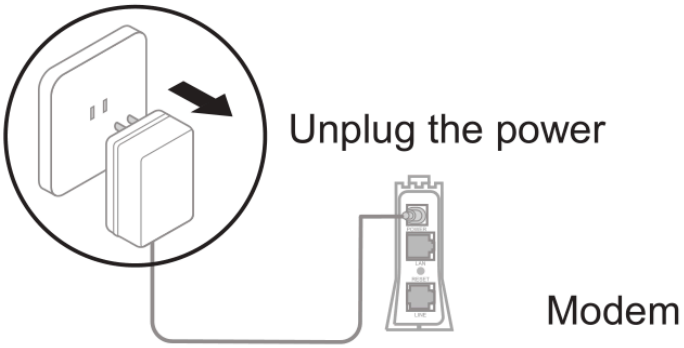
Reset Button: Press and hold Reset for 6 seconds then release, and the LED will turn solid purple to reset the mesh devices.

Chapter 2 Initial Setup Guide

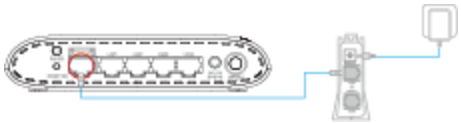
This chapter contains the following sections :

Prepare the Modem

1. Unplug the power adapter from your DSL modem. If the modem has backup battery, please remove it.
   Note : If using a DSL Internet connection, obtain the login credentials(username/password) from your Internet Service Provider (ISP) to properly configure your wireless router.



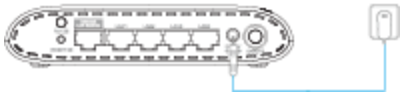
2. Use the provied Ethernet cable to connect the modem to the WAN port of the router.
3. Plug the modem into a power outlet and turn it on.



4. Check the indicator lights on the modem to confirm a stable internet connection.

Install Your Router

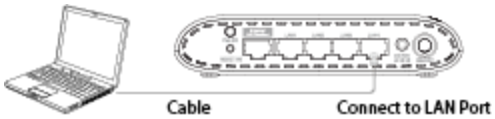
1. Insert the power adapter into the router’s DC IN port and press the power switch (if applicable; some models lack a physical switch).



2. Wait for about 2-3 minutes, then the router is ready.

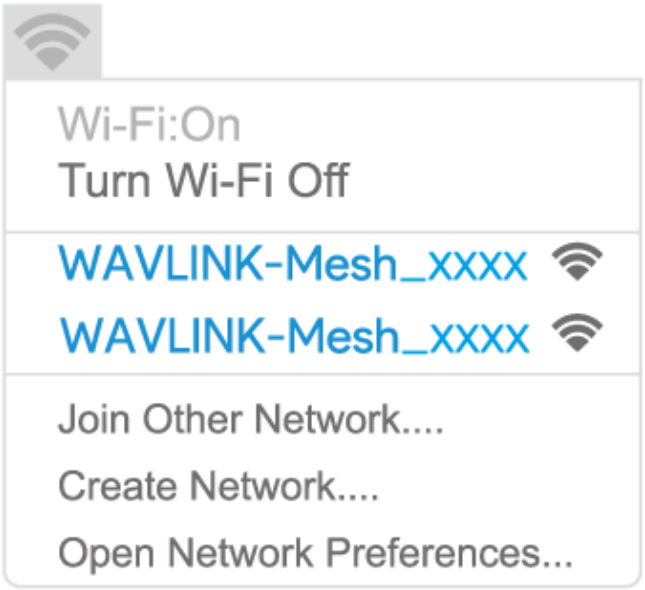
Configure the Router via Web Browser

1. **Wired Connection:** Use another Ethernet cable to connect your computer to one of the LAN ports on the router.



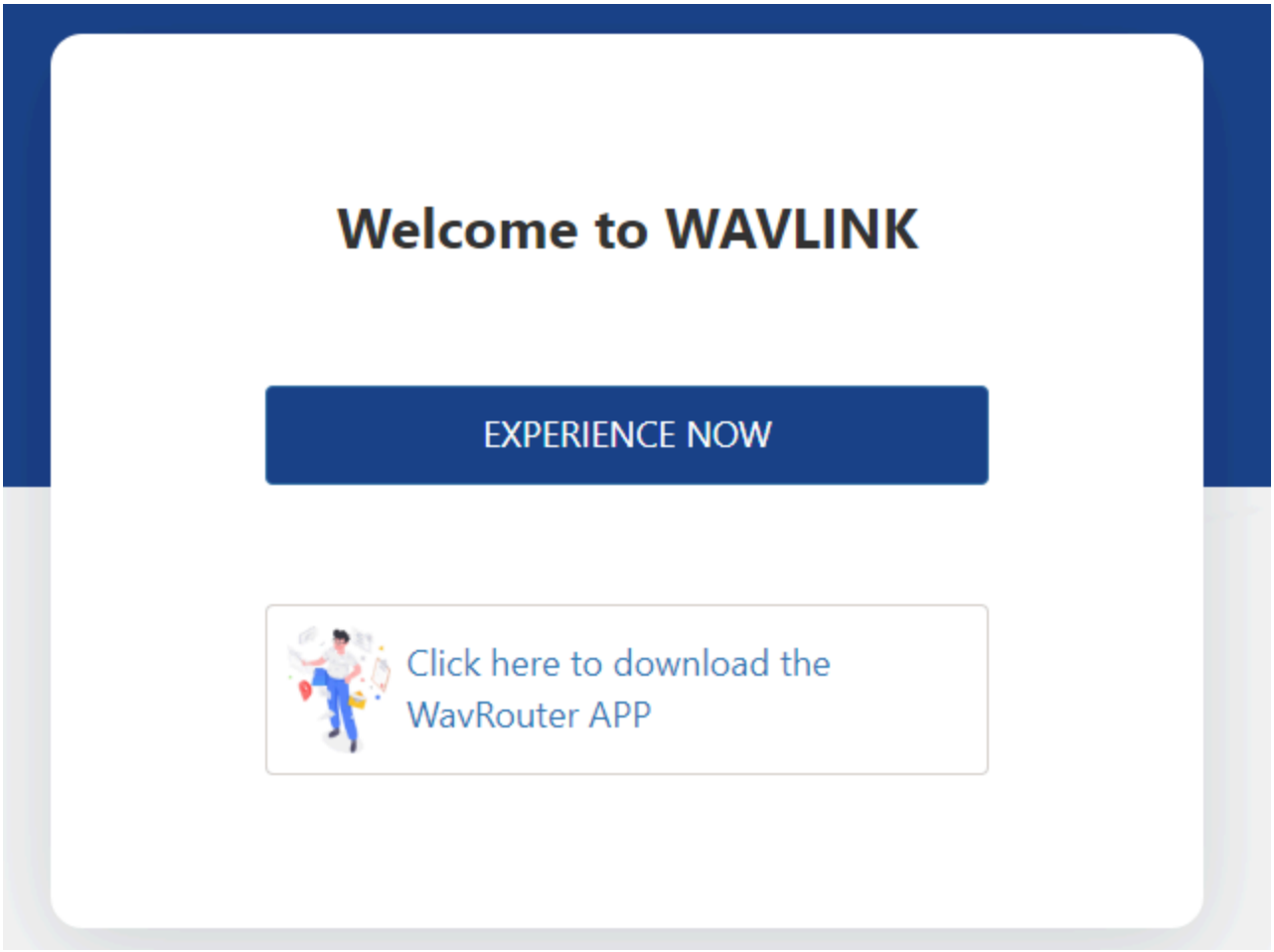
2. **Wireless Connection:** On your laptop or smartphone, connect to the default SSID printed on the router: **WAVLINK-Mesh_XXXX**.

For Windows Users

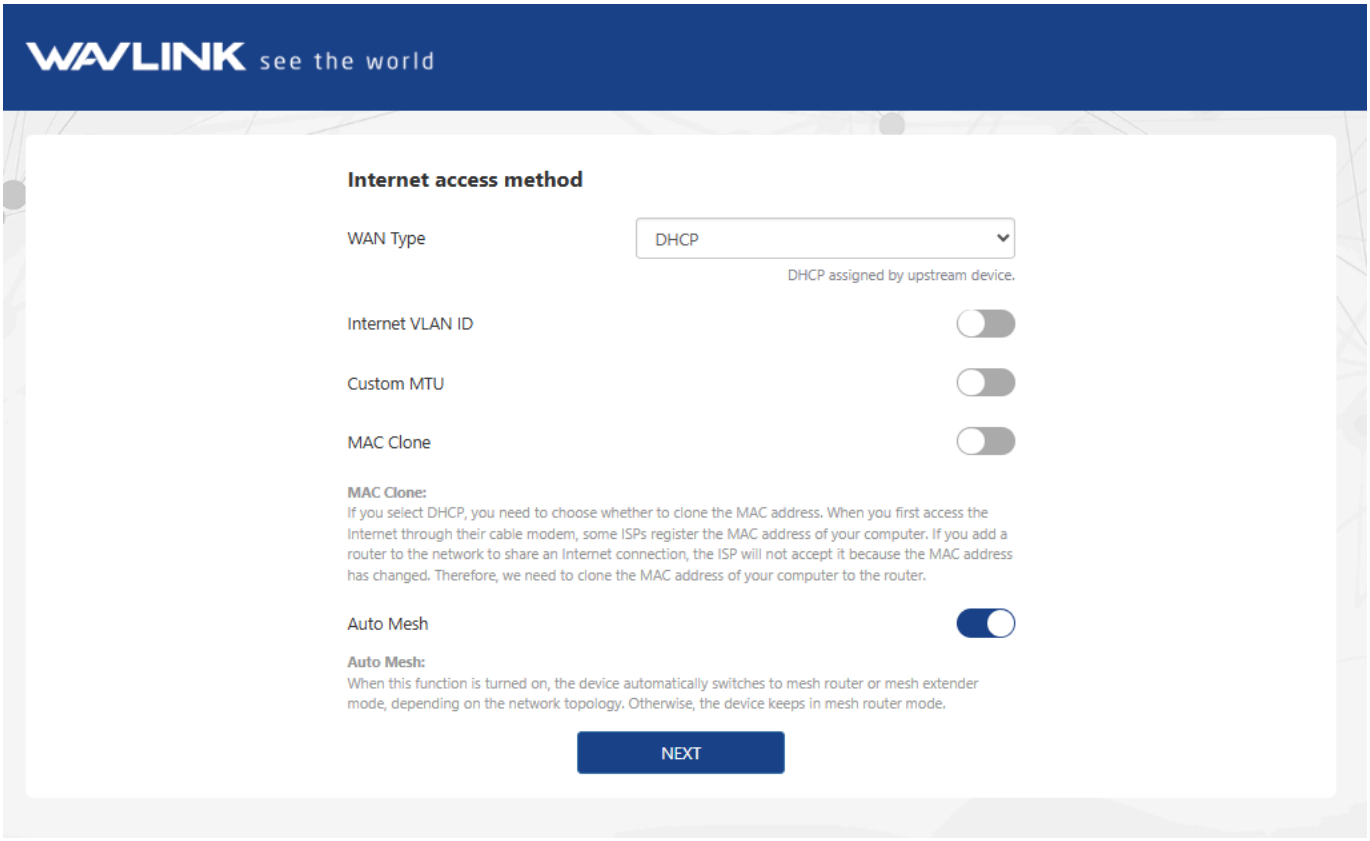


For Mac Users

3. Open a web browser(via wired or wireless connection) and enter http://wavlogin.link in the address bar. You will automatically enter the Wavlink router initial setup page. If not, manually enter **192.168.20.1** in the browser's address bar and follow the instructions.

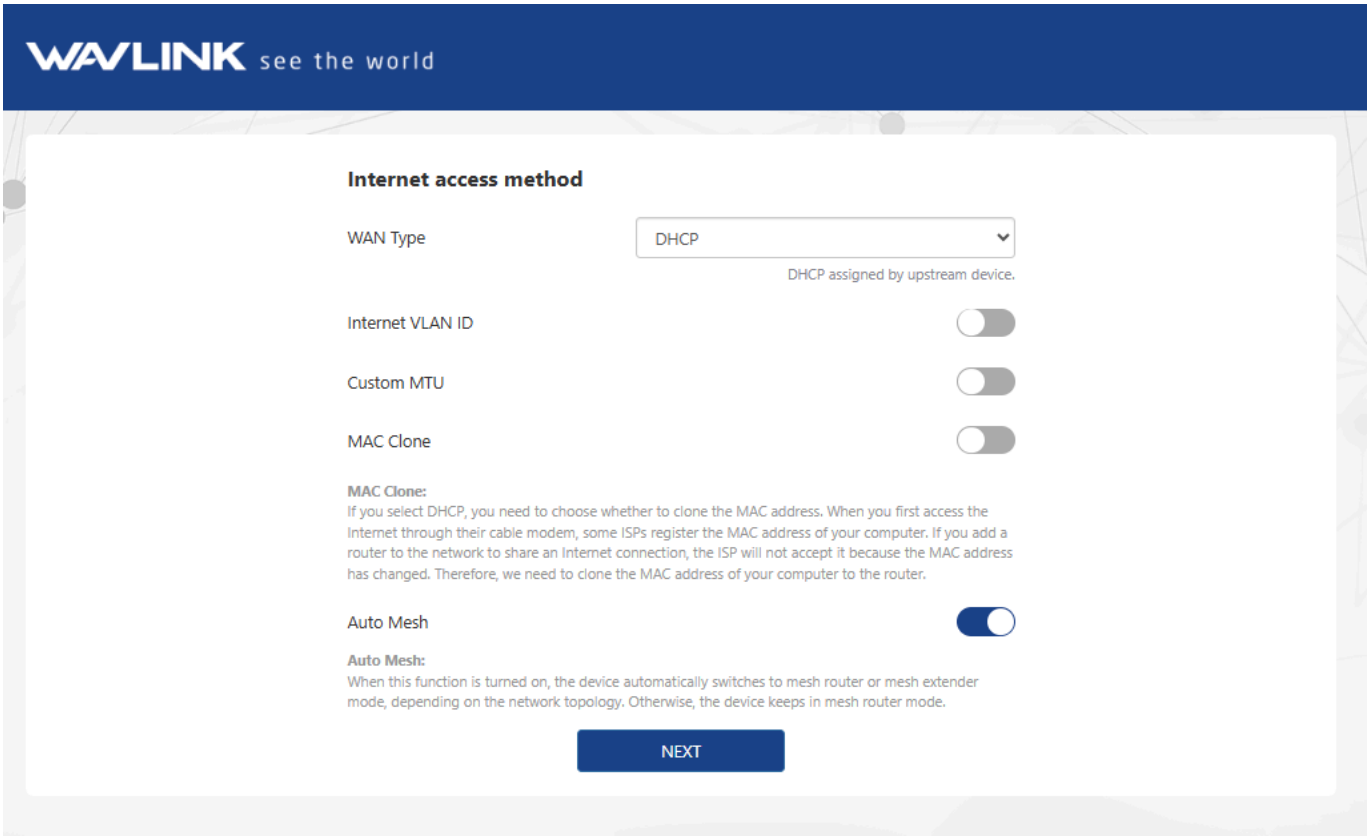


4. It is **Router Mode** by default. Select the corresponding **WAN Type**.

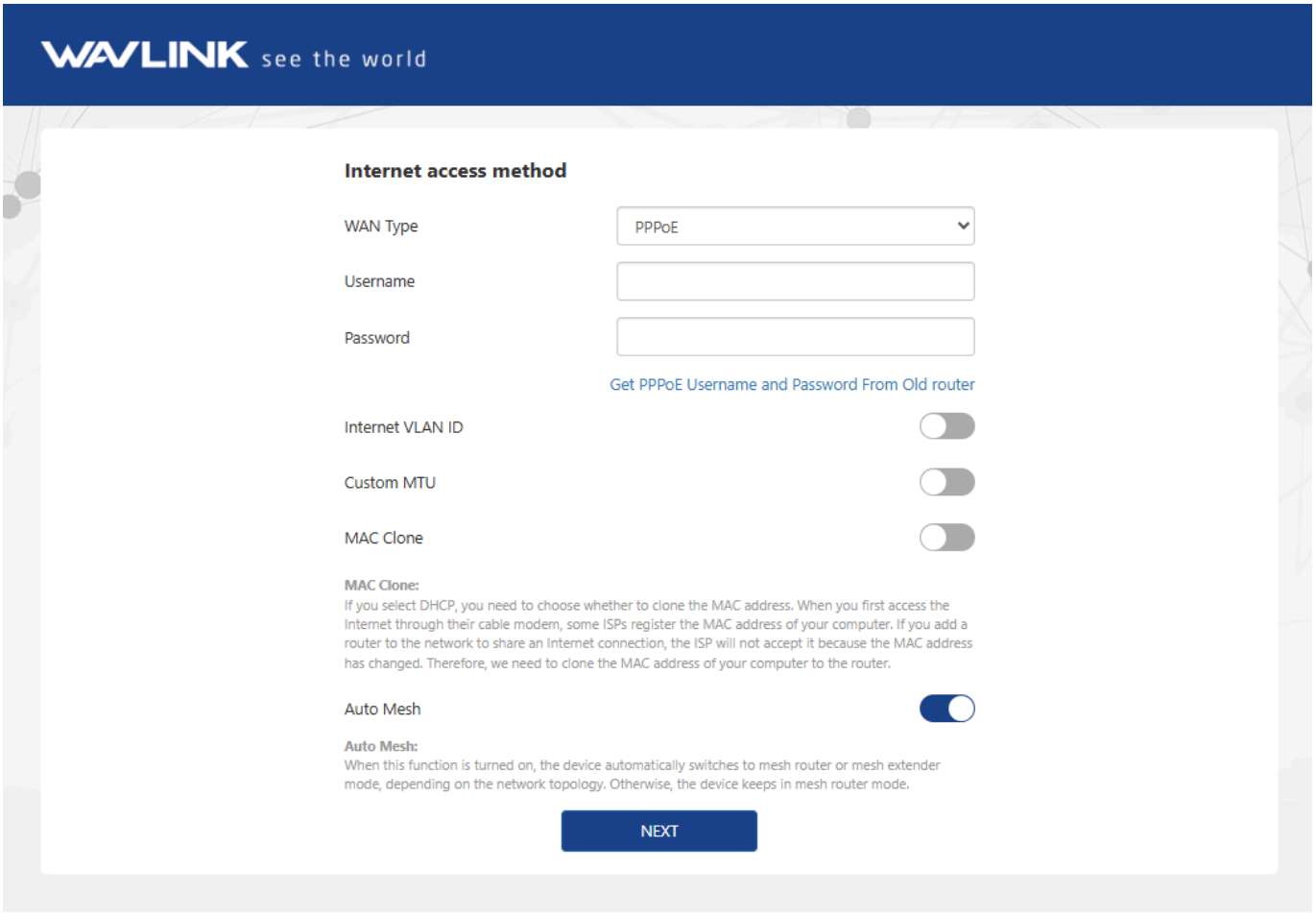


① If you choose **DHCP**, you will need to decide whether to enable the MAC clone. Some ISPs register the MAC address of your computer when you firstly access the

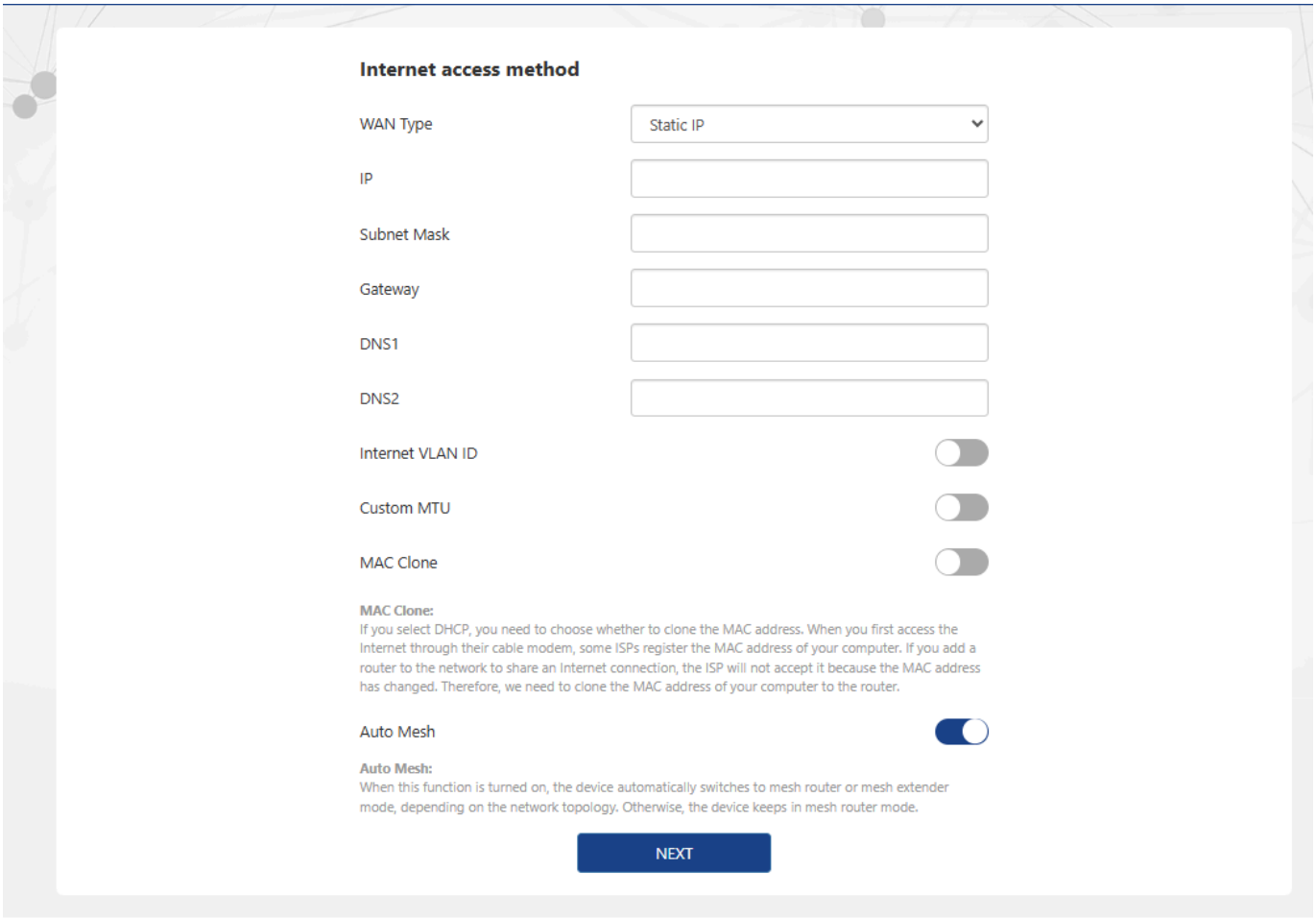
Internet through their cable modem, we need to clone the MAC address of your computer to the router. The **Custom MTU(Maximum Transmission Unit)** is the largest size of a data packet that can be transmitted over the network. If your ISP requires you to adjust the MTU size, enable this option. Otherwise, we recommend you to keep it disabled for optimal network performance.



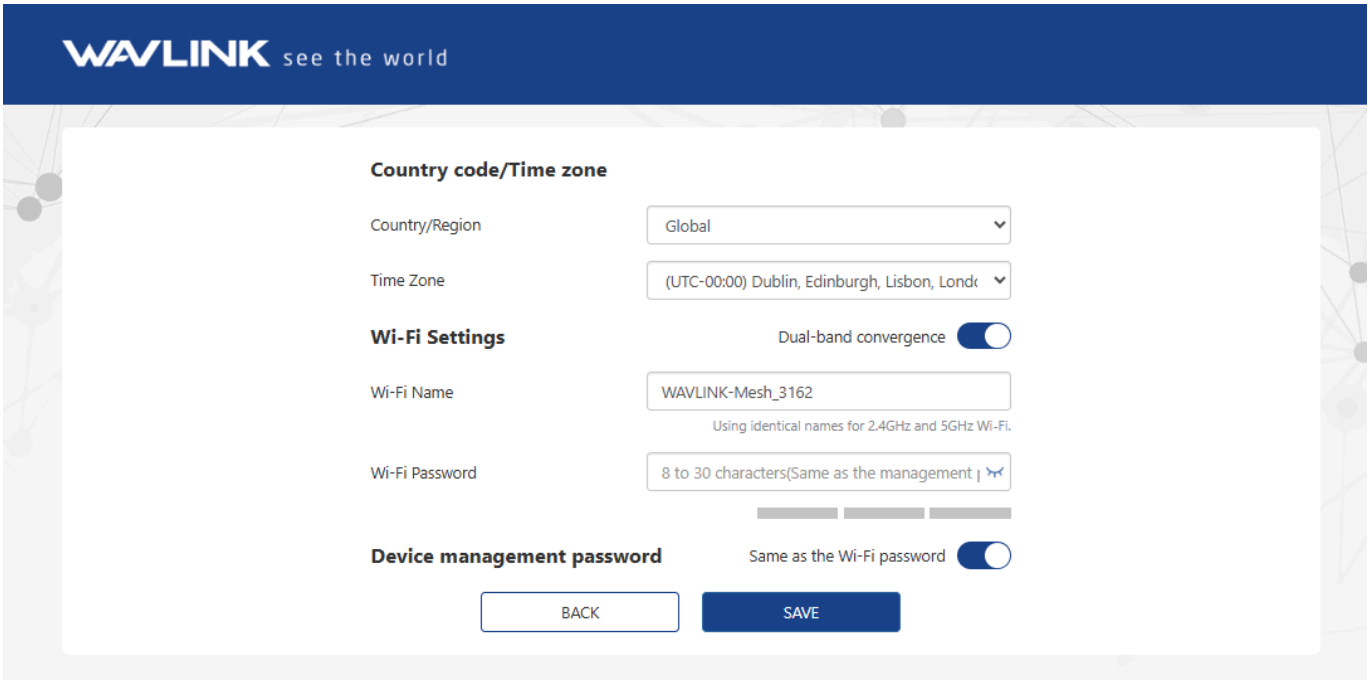
② If you choose **PPPoE**, enter the **Username** and **Password** provided by your ISP. PPPoE is usually designed for such as DSL or fiber optics.



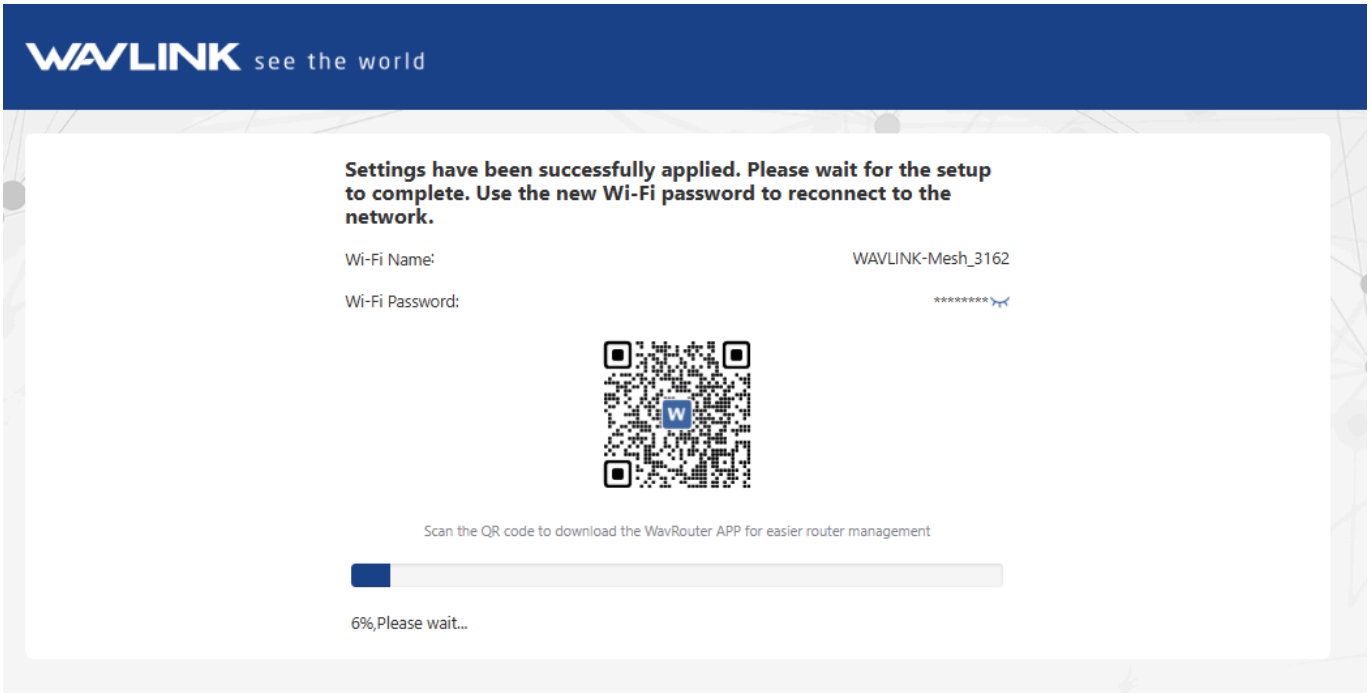
③ If you choose **Static IP**, enter a specified IP parameters including IP address, Subnet Mask, Gateway, DNS1 and DNS2 provided by your ISP.



5. Click **NEXT**.
6. Choose **Country/Region** and **Time Zone**, and set **Wi-Fi Name** and **Wi-Fi Password**.



7. Click **SAVE** and wait the settings to be successfully applied. Then use the new Wi-Fi password to reconnect to the network.


WAVLINK see the world
Settings have been successfully applied. Please wait for the setup to complete. Use the new Wi-Fi password to reconnect to the network.
Wi-Fi Name:
WAVLINK-Mesh_3162
Wi-Fi Password:
****
Scan the QR code to download the WavRouter APP for easier router management
6%,Please wait...

Chapter 3 Network Management

This chapter contains the following sections :

Network Setting

The way of network access can be changed as your requirement through configurating the network setting.

Connection Configuration

1. Access **Network** setting or **More>Network>Network Setting**.
2. Select your network connection way from the **WAN Type** list.

1）DHCP(Dynamic Host Configuration Protocol)

- It assigns network information including IP, Subnet Mask, default Gateway and others for the computer, designed for small network environments such as a home or a small office, managing and assigning IP without manual configuration.
- If the ISP(Internet Service Provider) has provided Auto Assign Feature for you, select DHCP from the WAN Type list.

2）PPPoE(Point-to-Point Protocol over Ethernet)

- It functions as a secure connection constructor, including verifying user identity, assigning IP, and others. It is designed for broadband access methods such as ADSL, fiber optics and others to provide a secure network connection.
- If the ISP has provided a **Username** and **Password** for you, enter them after selecting PPPoE from **WAN Type** list, then select **CONNECT**.

3）Static IP

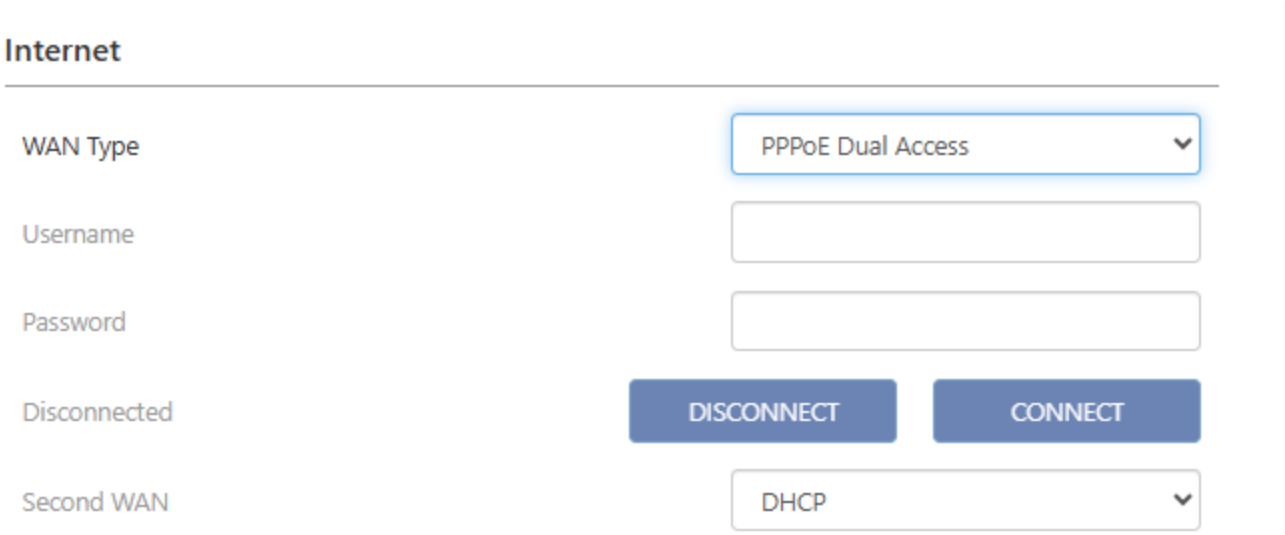
- It assigns fixed IP address for the computer automatically. It is designed for network connections, servers, remote access, etc., which require long-term stability to ensure the stability of network connections.
- If the ISP has provided a specificed IP parameters including IP address, Subnet Mask, Gateway, DNS1 and DNS2, select Static IP from the list and enter the information provided by the ISP.

4）PPPoE Dual Access

- Using dual PPPoE broadband lines, PPPoE Dual Access achieves balanced distribution via the technology of Load Balancing. Designed for improving the network

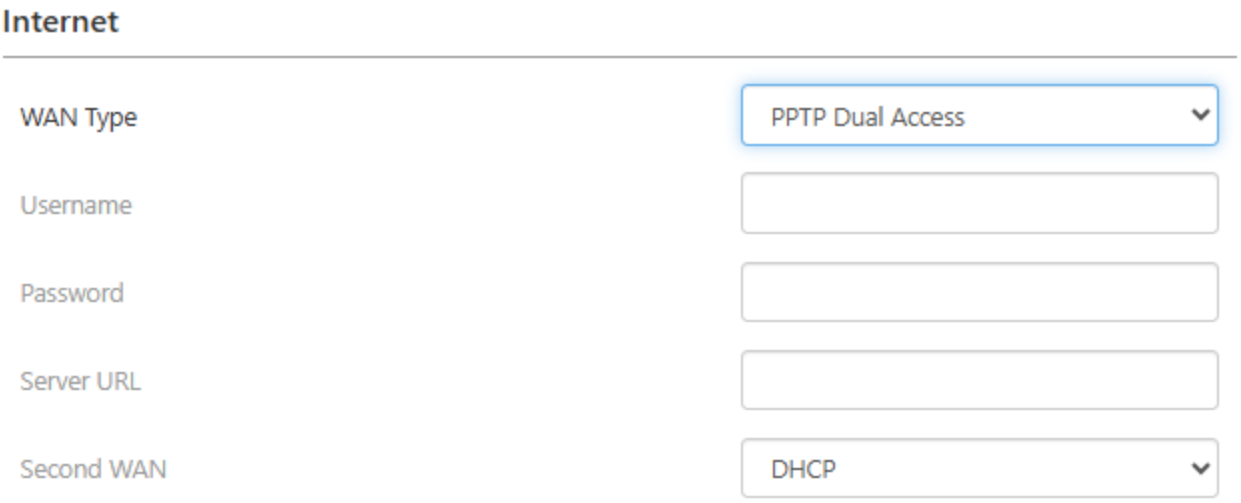
bandwidth and stability, so it is for the occassion that requires large data transmission.

- Enter the account and password provided by the ISP in **Username** and **Password**. Then select **DHCP** or **Static IP** from **Second WAN** list, one note is that **IP** and **Subnet Mask** are required for **Static IP**. Click **CONNECT**



5）PPTP Dual Access

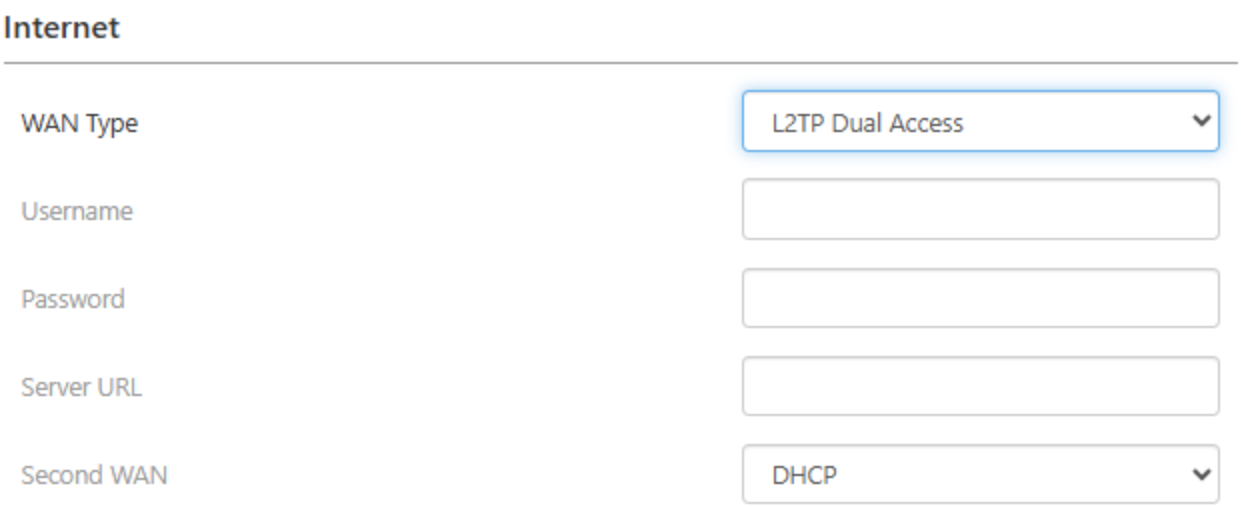
- PPTP Dual Access refers to the dual-network accessing method of using two PPTP VPNs. With it, users can configure two PPTP VPN to simultaneously access the Internet, enhancing the reliability of bandwidth and network.
- Enter **Username**, **Password**, **Server URL**, then select **DHCP** or **Static IP**, one note is that **IP** and **Subnet Mask** are required for selecting **Static IP**.



6）L2TP Dual Access

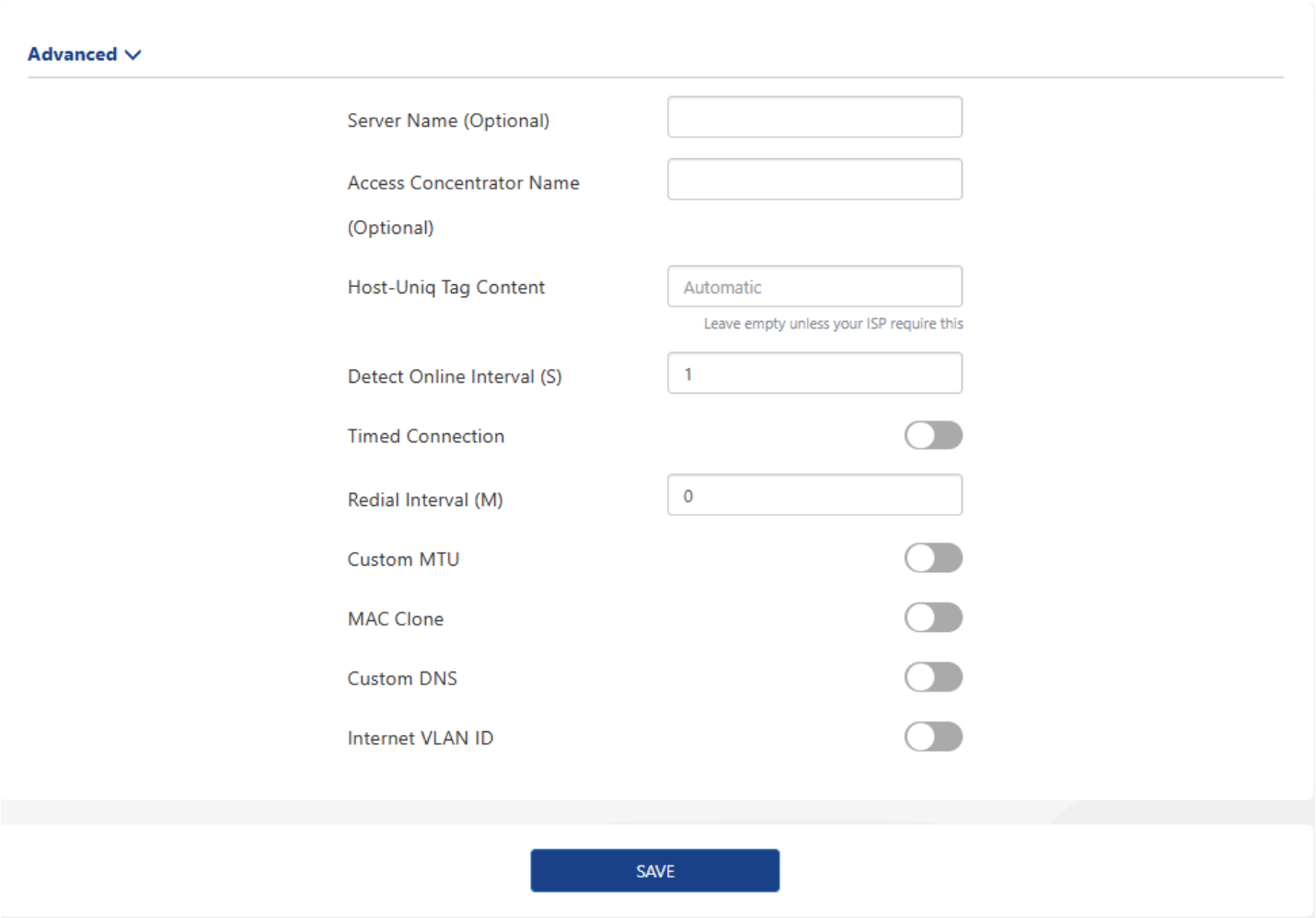
- L2TP Dual Access uses two L2TP VPN connections to access the Internet. it allows users to use two VPNs to access the Internet, enhancing the reliability of bandwidth and network.

- Enter **Username**, **Password** and **Server URL**, then select **DHCP** or **Static IP**, one note is that **IP** and **Subnet Mask** are required for **Static IP**.



Advanced Configuration

In **Advanced**, open and configure **Custom MTU**, **MAC Clone**, **Custom DNS** and **Internet VLAN ID** and others as your requirements.



- **Custom MTU(Maximum Transmission Unit)**
  - The Ethernet MTU(MaximumTransmission Unit) is the largest size of a data packet that can be transmitted over the network. If your ISP requires you to adjust the MTU size, enable this option. Otherwise, we recommend you to keep it disabled for optimal network performance.
- **MAC Clone**
  - The MAC clone allows you to copy the MAC address from the computer to the WAN interface of the router. When an ISP restricts internet access to a single MAC address, by cloning the MAC address of the device, the router will masquerade as authorised devices, ensuring an uninterrupted internet connection.
- **Custom DNS**
  - The custom DNS allows you to configure optimal DNS server for the network manually, instead of using the default DNS provided by the ISP.
- **Internet VLAN ID**
  - The Internet VLAN ID is setted to recognizing the feature of Internet data. For specific settings, please consult your network operator's customer service or technical support staff.

PPPoE Advanced Configuration

- **Server Name**
  - The Server name, provided by ISP, indicates the name or address of PPPoE server.
- **AC(Access Concentrator) Name**
  - The AC name is the name of the Access Concentrator, used to differentiate between different access points. It is typically designated by the Internet Service Provider (ISP).
- **Host-Uniq Tag Content**
  - In PPPoE protocol, the Host-Uniq field is optional, used to uniquely identify requests from a host. In the same network, it ensures every request connected is unique while using PPP to connect to multi-users, avoiding confusion and conflicts. Keep it null if your ISP doesn't provide any information about it.
- **Detect Online Interval**
  - The detect online interval is used to set the time interval for sending a message verifying link validity and data transmission capability, the appropriate interval

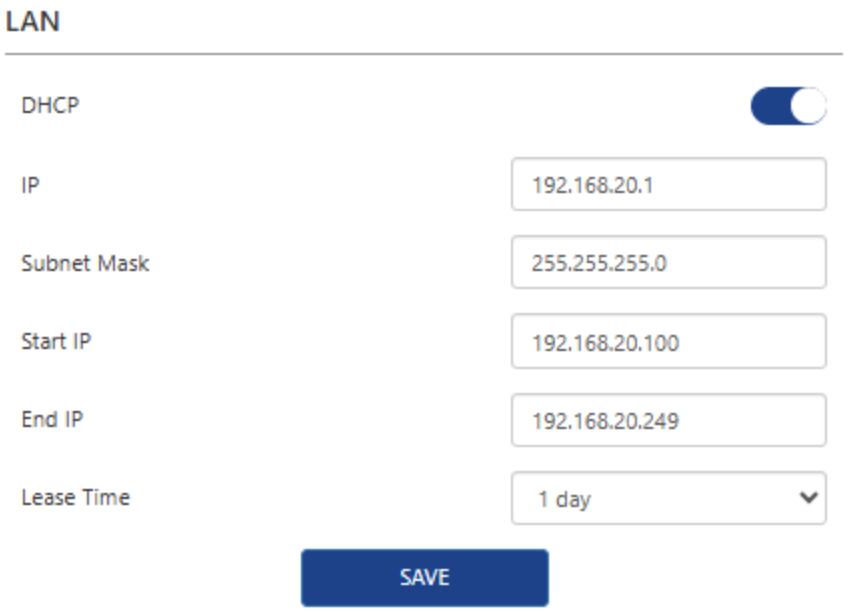
is helpful for timely detecting and addressing link issue.

Click **SAVE** to finish configuration.

LAN Setting

DHCP server automatically assigns IP for the devices in the LAN. If it is required, you can change its setting.

1 . Click **More**>**Network**>**LAN**.
2 . Click to enable **DHCP**.

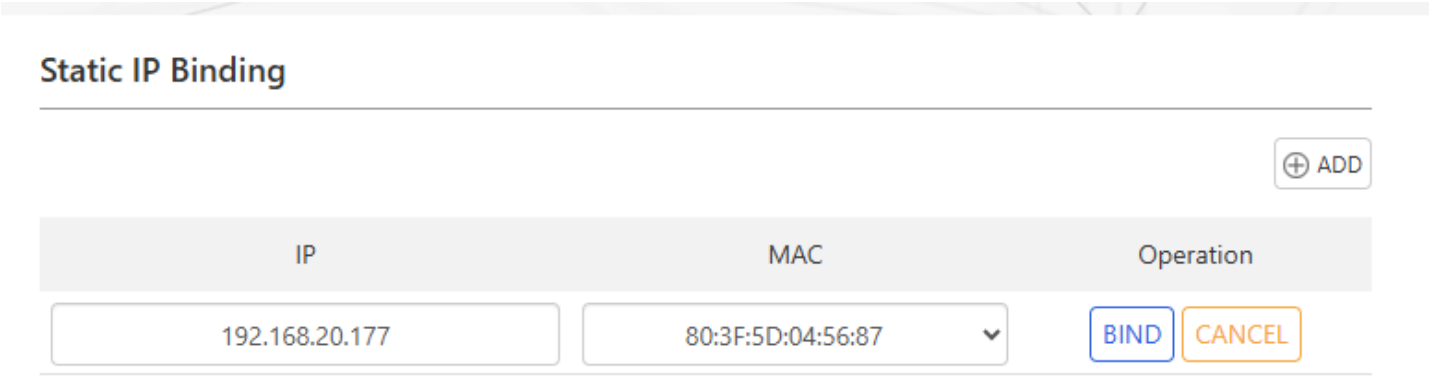


- **IP Address**: The IP address from which the router connects to the LAN. This can be used to log in to the router's network management page.
- **Subnet Mask**: The subnet mask that the router connects to the LAN.
- **Set IP Address Pool**: When DHCP is enabled, the router automatically assigns IP addresses to devices in the LAN from the address pool. If you need to change the address pool range, modify the Start Address and End Address.
- **Lease Time**: This is the lease time of the IP address that the device obtains when accessing the router. If you need to modify it, please select it again in the Lease Time drop-down list.

3 . Click **SAVE** to finish the configuration.

Setting Static IP Binding

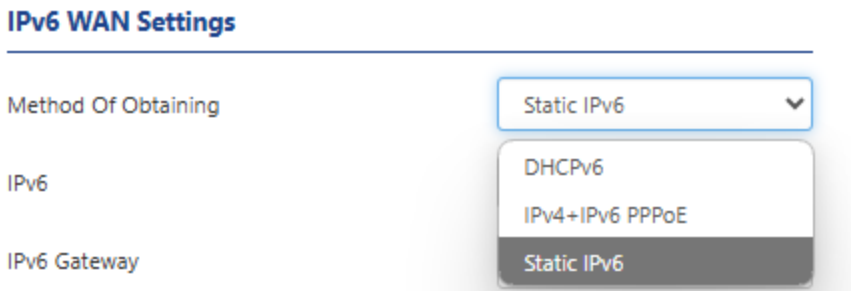
It allows you to link the specific IP to the MAC address of customer devices. Using it, you can assign a fixed IP for the specific device so that the device can automatically obtain the same IP everytime it connects to the network.



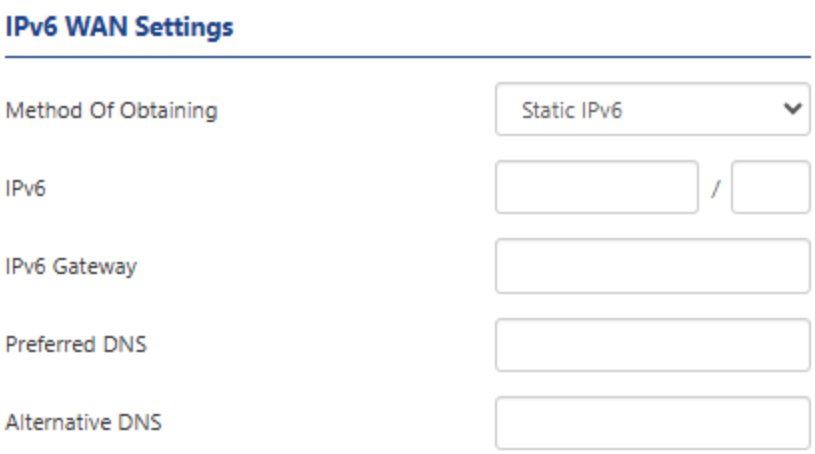
1 . Click **More**>**Network**>**Static IP Binding**.
2 . Click **ADD** in the top right corner to add a binding rule.
3 . Input the **IP** and **MAC**, then click **BIND**.

Setting IPv6

The IPv6 is the next generation Internet protocol, has more space for address, more advanced functions and enhanced security. It aims to solve more issues on interconnectio devices and provide better network performance and security.



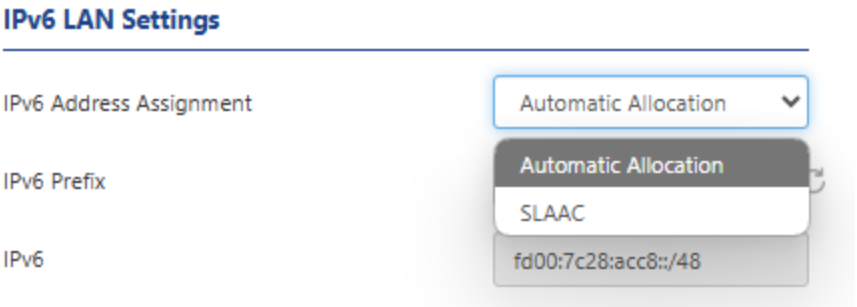
1 . Click **More**>**Network**>**IPv6**.
2 . Click once to enable **IPv6**.
3 . **IPv6 WAN Settings**.



3.1 Select corresponding **Method Of Obtaining** from the list, then input corresponding information:

- **DHCPv6**: The router automatically obtains the parameters such as IPv6 address. No manual requirements.
- **IPv4+IPv6 PPPoE**: When IPv4 Internet access is also PPPoE, you can select IPv4+IPv6 PPPoE. After enabled, IPv6 will use the IPv4 account and password to dial the number, and you do not need to manually enter the IPv6 account and password. Please note that this requires operator's support.
- **Static IPv6**: Manually input **IPv6(address)**, **IPv6 Gateway**, **Preferred DNS** and **Alternative DNS**.

4 . **IPv6 LAN Settings**.



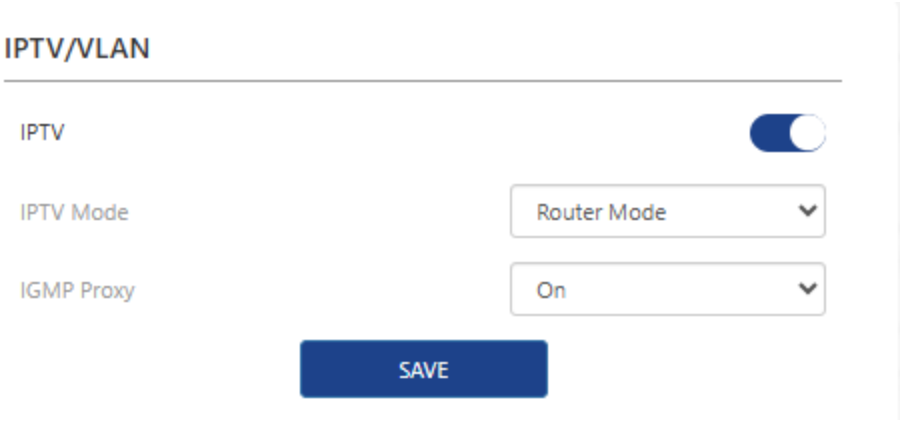
- Selecting appropriate address assignment method from the **IPv6 Address Assignment** list:
  - **Automatic Allocation**: It will automatically assign IPv6 addresses to devices on the LAN network.
  - **SLAAC**: In the SLAAC, The terminals on the LAN will automatically create IPv6 addresses according to the router.

5 . Click **SAVE** to finish the configuration.

IPTV Setting

Setting IPTV allows you to enjoy multimedia service while using the network. You should consult IPTV's service provider about **VLAN ID** and how to select **IPTV Mode**. Then you can select the corresponding VLAN Port, and connect IPTV's cable to the corresponding LAN port on the router.

Configuring IPTV

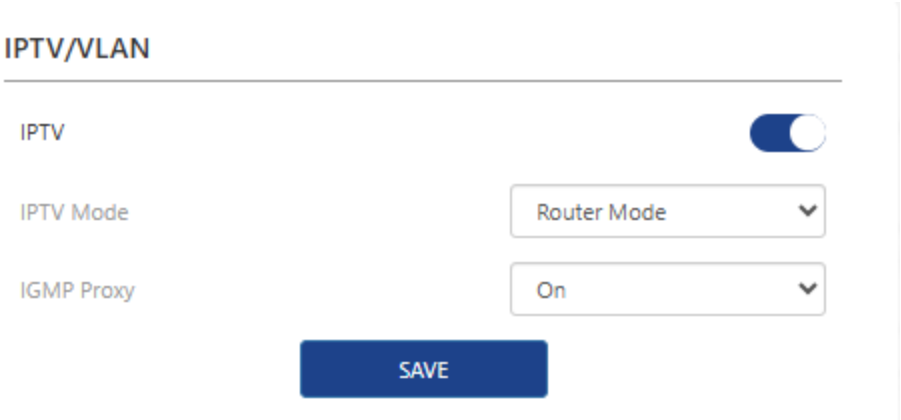


1 . Enter **More**>**Network**>**IPTV/VLAN**.

2 . Click once to enable **IPTV**.

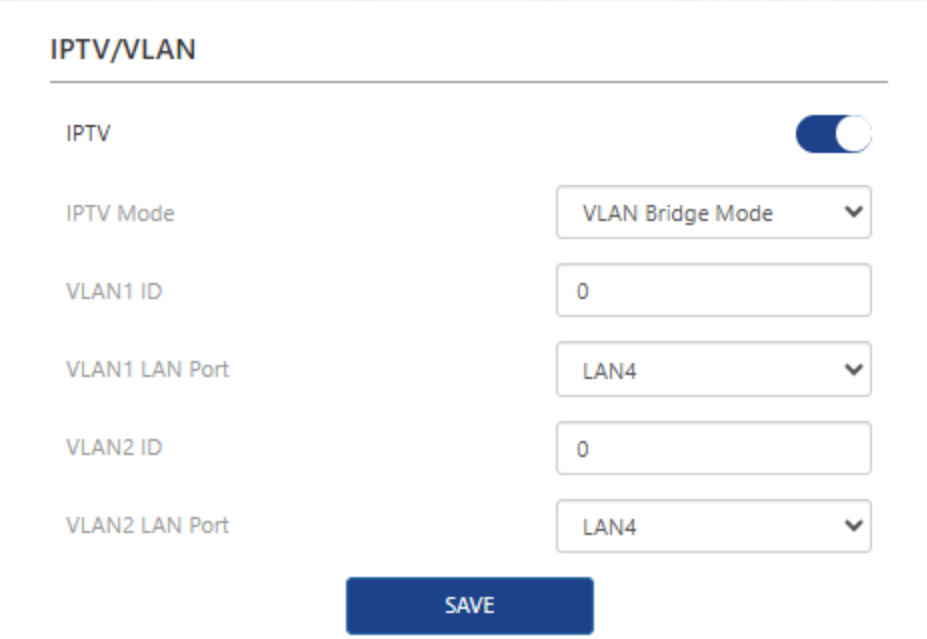
3 . Select appropriate working mode from the **IPTV Mode** list.

3.1 Router Mode



Enable **IGMP Proxy** if you use IPTV service on multiple devices at the same time.

3.2 VLAN Bridge Mode: Enter **VLAN ID** and select **VLAN Port**.

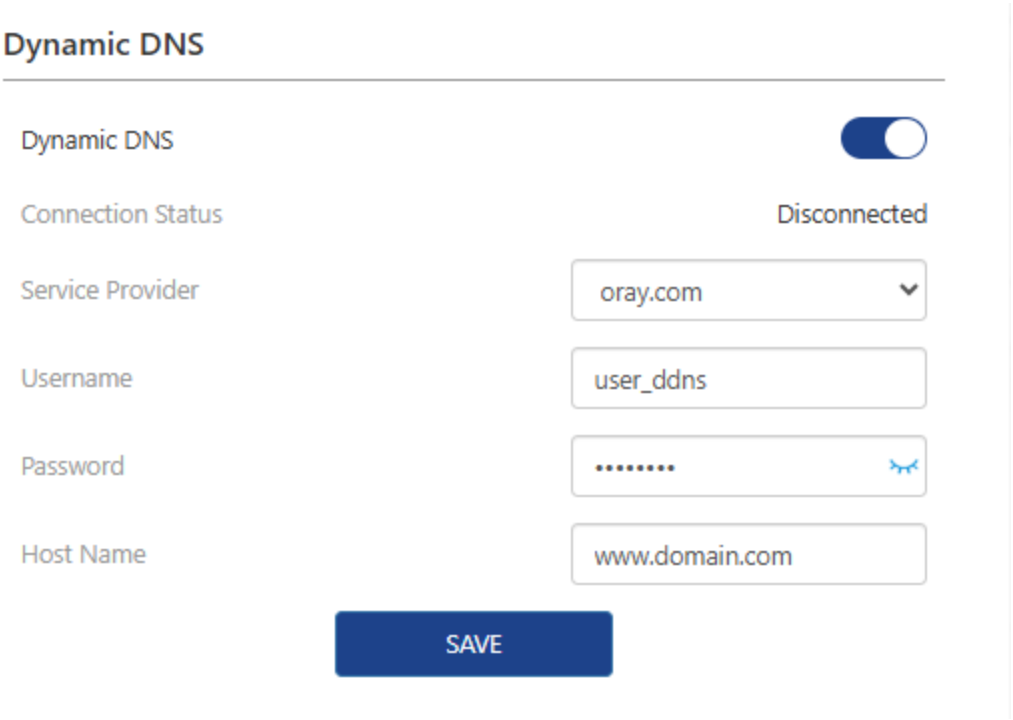


4 . Click **SAVE** to finish the configuration.

- **VLAN1 ID and VLAN1 LAN Port**: The VLAN1 ID indicates the VLAN1, and the VLAN1 LAN Port indicates the LAN port associated with VLAN1.
- **VLAN2 ID and VLAN2 LAN Port**: The VLAN2 ID indicates the VLAN2, and the VLAN2 LAN Port indicates the LAN port associated with VLAN2.

Setting Dynamic DNS

Dynamic DNS(DDNS, Dynamic Domain Name System) is a function of mapping dynamic IP addresses to fixed domain names. After enabling it, the router bind dynamic WAN IP with the fixed domain so that you can connect to the router using the domain remotely. In order to use this service, you need to register for the DDNS service with your service provider.



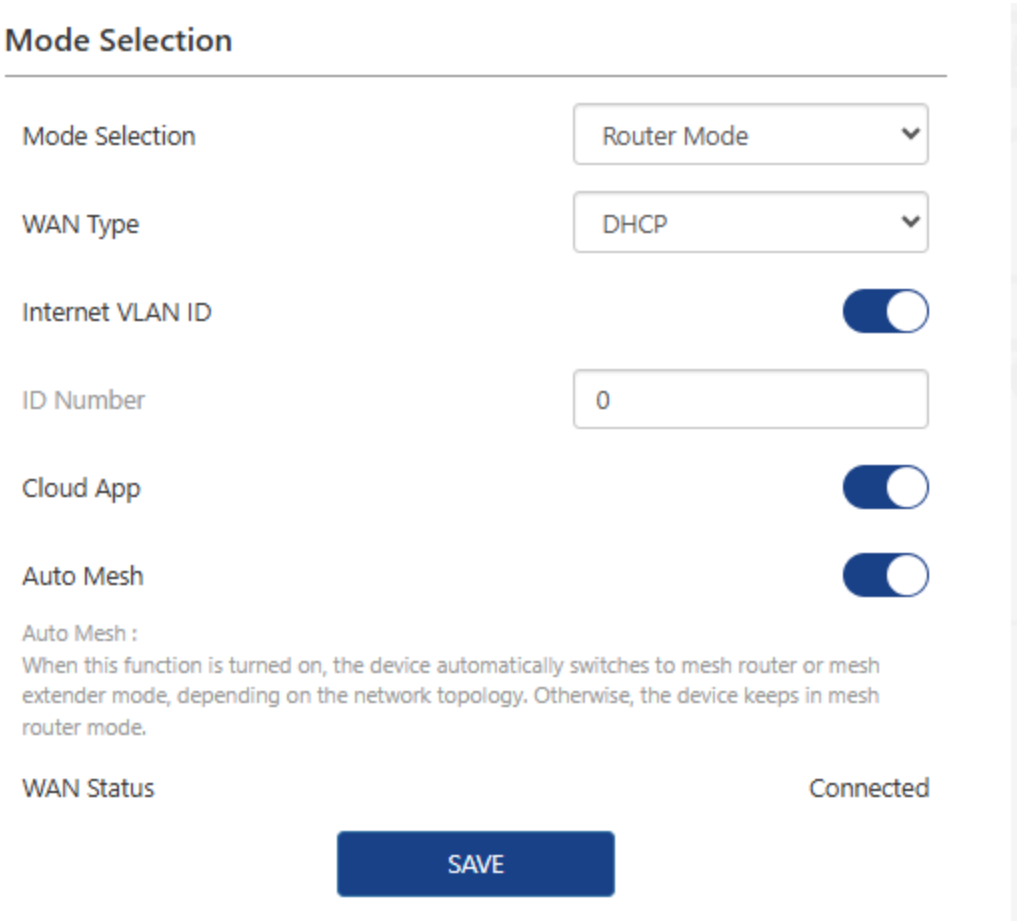
1 . Enter **More**>**Network**>**Dynamic DNS**.
2 . Click once to enable **Dynamic DNS**.
3 . Select **oray.com** or **NO-IP** from the **Service Provider** list.
4 . Input corresponding **Username**, **Password** and **Host Name** from your DNS registration information.
5 . Click **SAVE** to finish configuration.
Note: Different dynamic DNS service provider may provide various parameters, and the name or indication may vary. Therefore, you should look up the corresponding explanation so that the correct parameters are inputed.

Mode Selection

Configure router's working mode according to your actual requirement.
1 . Enter **More**>**Network**>**Mode Selection**.
2 . Select appropriate working mode from the **Mode Selection** list: **Router Mode**, **LAN Bridge(AP Mode)** or **Repeater Mode**。

Router Mode

In routing mode, the router provides Wi-Fi Internet access point for the client by connecting to the Internet signal from the Internet Service Provider. Also provides wired internet by connecting to router's LAN via the cable.



WAN Type:

① **DHCP:** If the **ISP(Internet Service Provider)** has provided Auto Assign Feature for you, select DHCP from the WAN Type list.

② **PPPoE:** Use this when your Internet Service Provider (ISP) has given you a **Username** and **Password**.

③ **Static IP:** Use this when your Internet Service Procider(ISP) has given a set of IP parameter including **IP Address**, **Subnet Mask**, **Gateway** and **DNS**.

Note: If you are unsure of the **WAN Type**, connect the network cable from your main router to the device's WAN port. Once you access this settings page, the device will automatically detect the appropriate WAN Type.

Internet VLAN ID: After enabling it, input **ID Number**.You should consult the ISP about the detailed configurations.

Cloud App: It allows you to control devices remotely from the cloud using the APP.

Auto Mesh: In a Mesh networking setup, the Mesh routers can automatically switch between the primary router and sub-router based on the Internet connection status. If you need to configure this device as the primary router for scenarios such as a secondary router setup, please disable this feature.

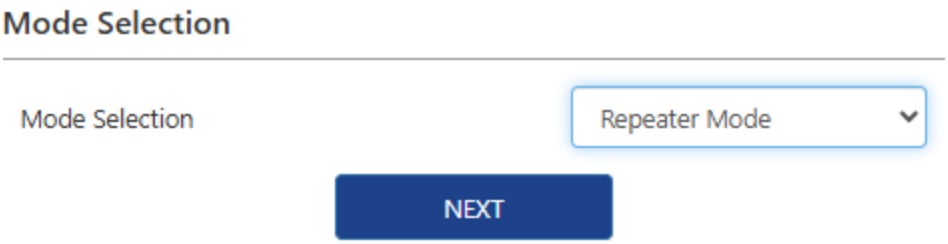
LAN Bridge(AP Mode)

In the AP mode of extending the existing network, you should confirm your device's WAN port has connected to the Internet using the Ethernet cable. One note is that some functions are not available in this mode.

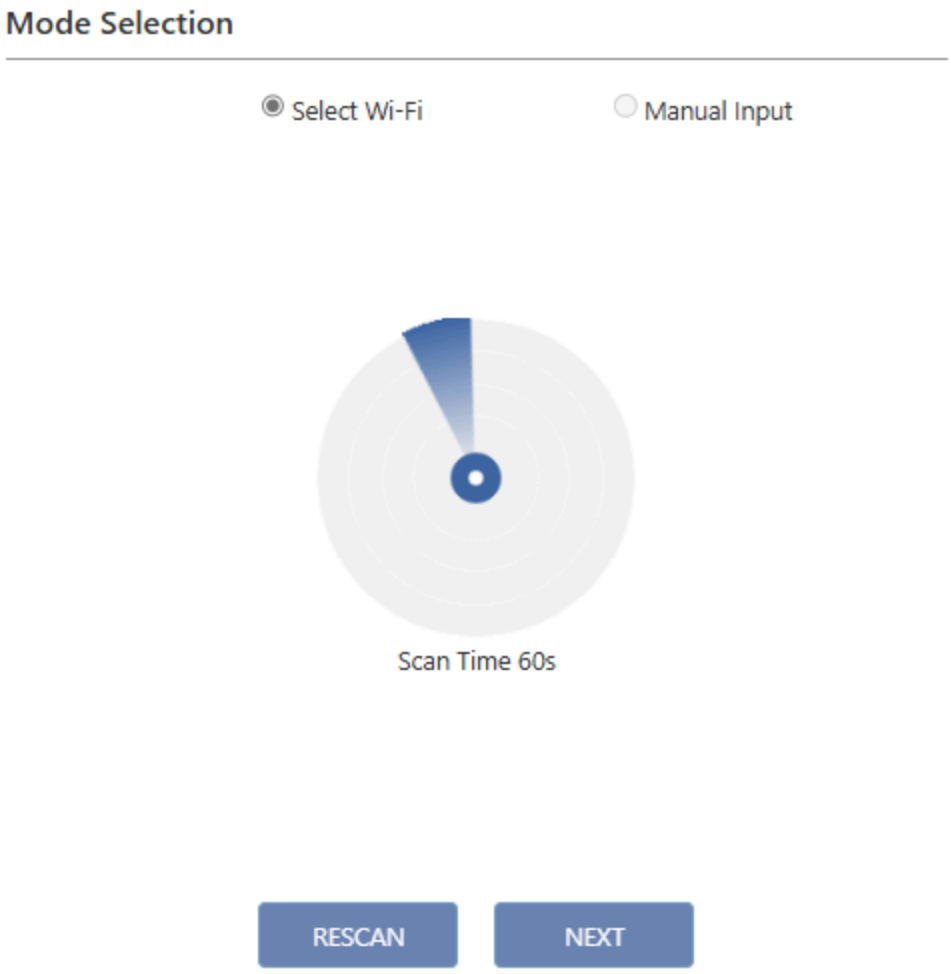
- **Smart DHCP Service**: If it is enabled, the router will configure IP service without connecting to the upper router. Please disable it if it is not required.

Repeater Mode

In the repeater mode, to extend the Wi-Fi coverage, this router works as a wireless repeater of the upper router. One note is that some functions are not available in this mode.

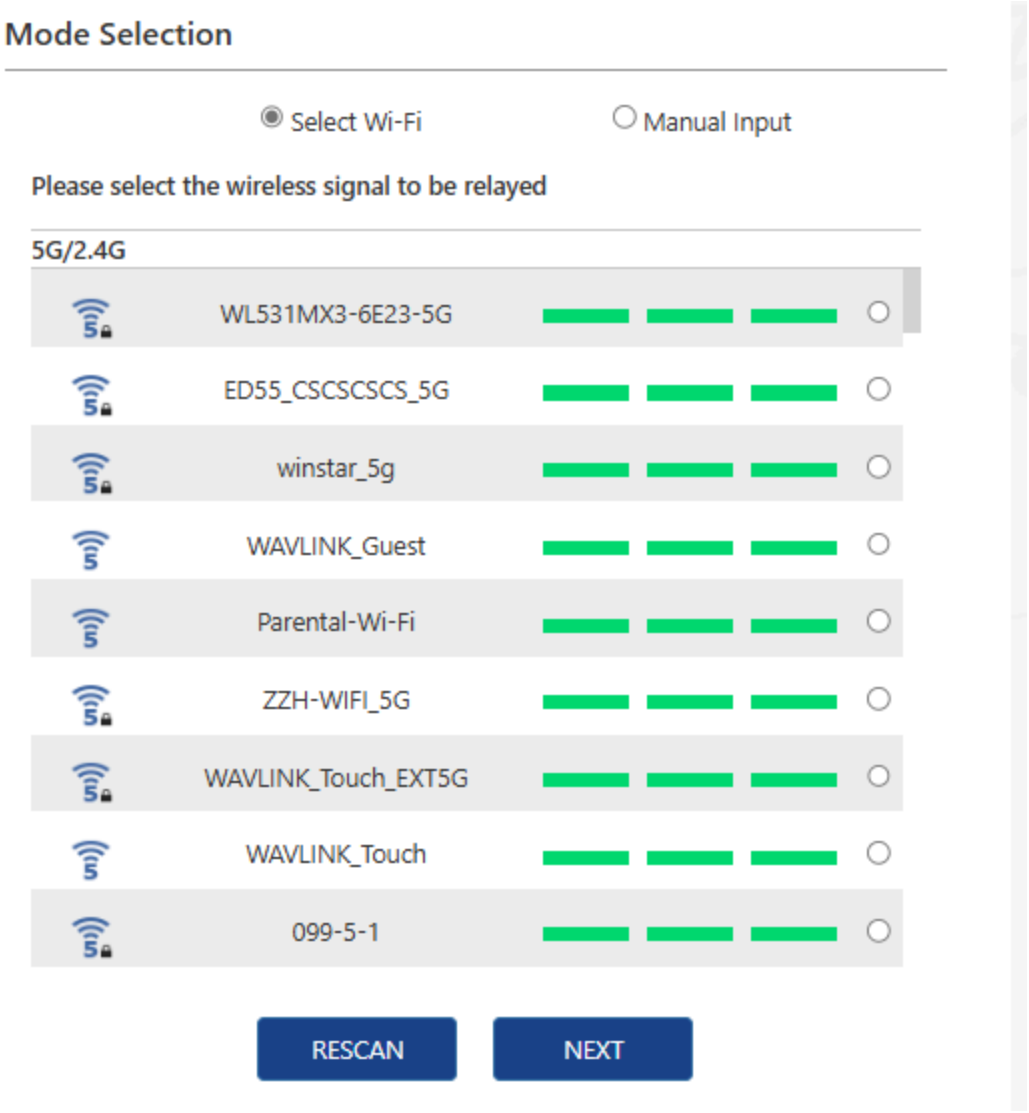


1）Click **NEXT** to rescan the Wi-Fi signal.

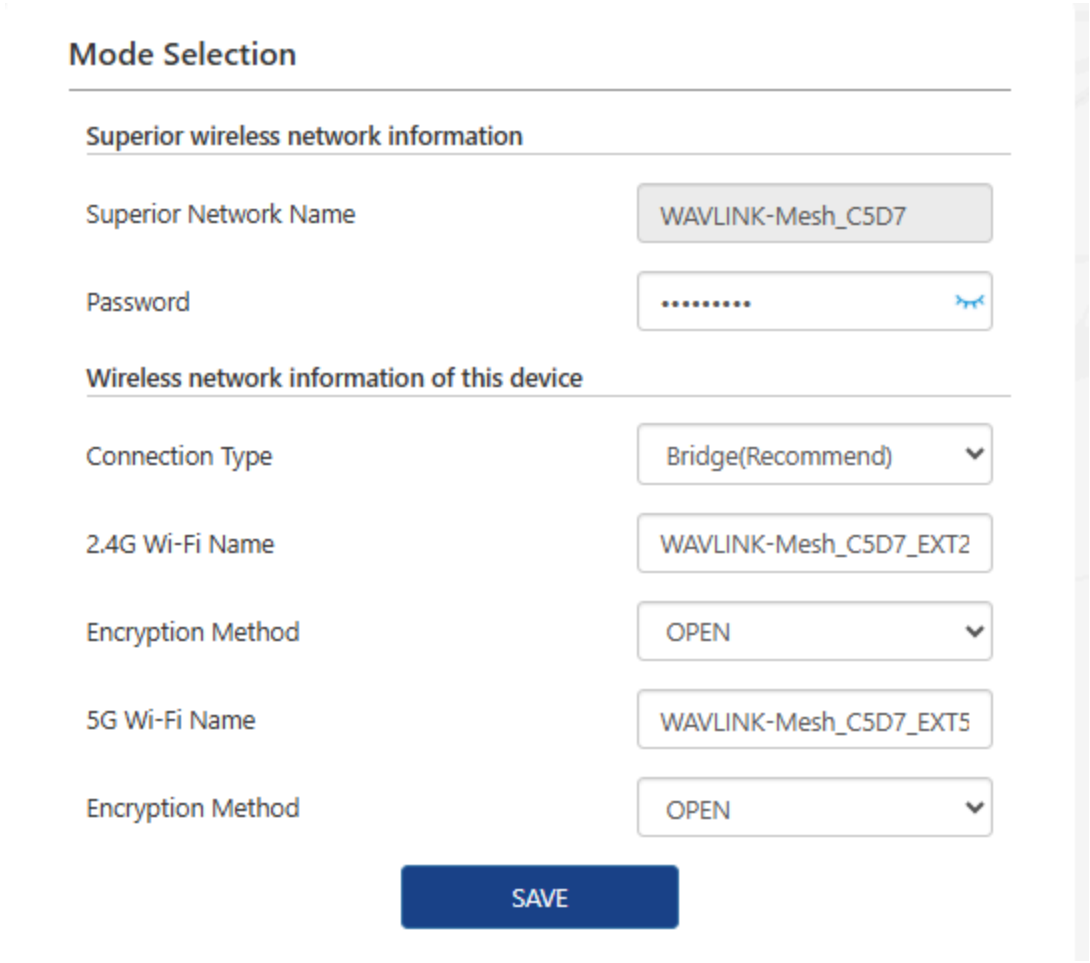


2） Select the wireless signal to be relayed, click **NEXT**.

3） If the network to be added is not found, click **Rescan** to rediscover the network.Or select **Manual Input** to set it up.

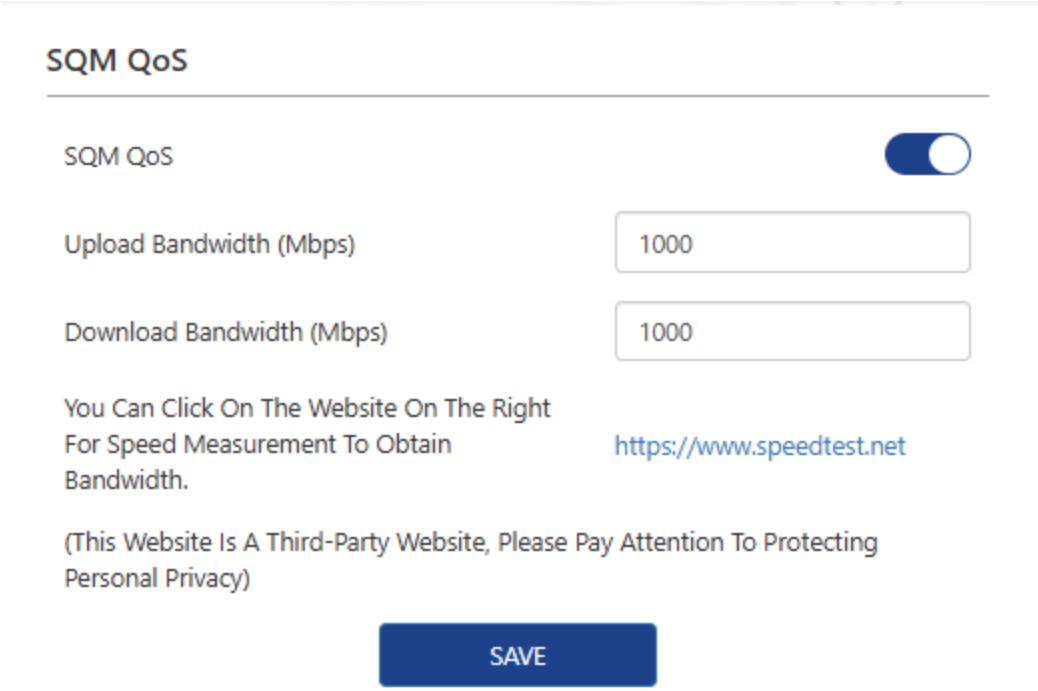


4）Enter the password of the superior wireless network and the wireless network information of this device. Click **Save** to complete the setup.



SQM QoS

SQM QoS is designated for optimizing the adjustment for network bandwidth, providing better network performance and lower latency. When the bandwidth is less than 100Mbps and multi-users is using the internet, this function can be enabled to optimize the network performance, ensuring appropriate bandwidth is allocated to each application; When the bandwidth is 100Mbps+, it is not recommended to enable it.

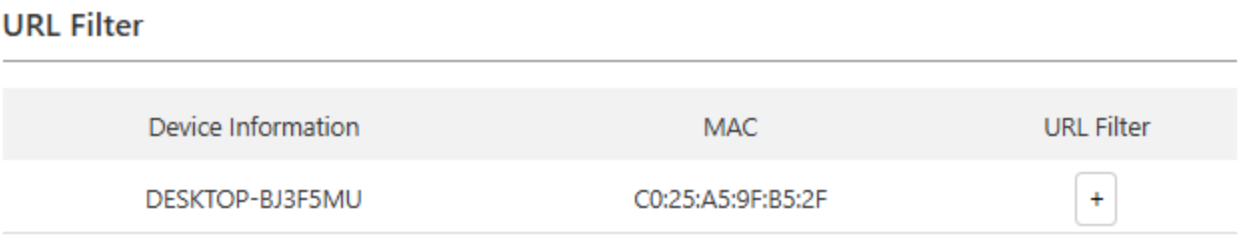


1. Navigate to **More** > **Network** > **SQM QoS**.
2. Click to enable **SQM QoS**.
3. Set the maximum **Upload Bandwidth** and the maximum **Download Bandwidth**.
4. Click **SAVE** to complete the configuration.

URL Filter

You can block any device connected to this router from accessing specific websites by entering keywords or the full domain name.

1. Click **+** icon in **URL Filter**.



2. After entering the keywords or the full domain name, click **SAVE** to take effect.

Website Block

Please Enter The Keywords Or Domain Names You Want To Block:

Please enter a keyword or domain name.

Example:Baidu,Google,Youtube

CANCEL SAVE

Restricted Keywords Or Domain Names:

DELETE

Chapter 4 Managing Wireless Network

This chapter contains the following sections:

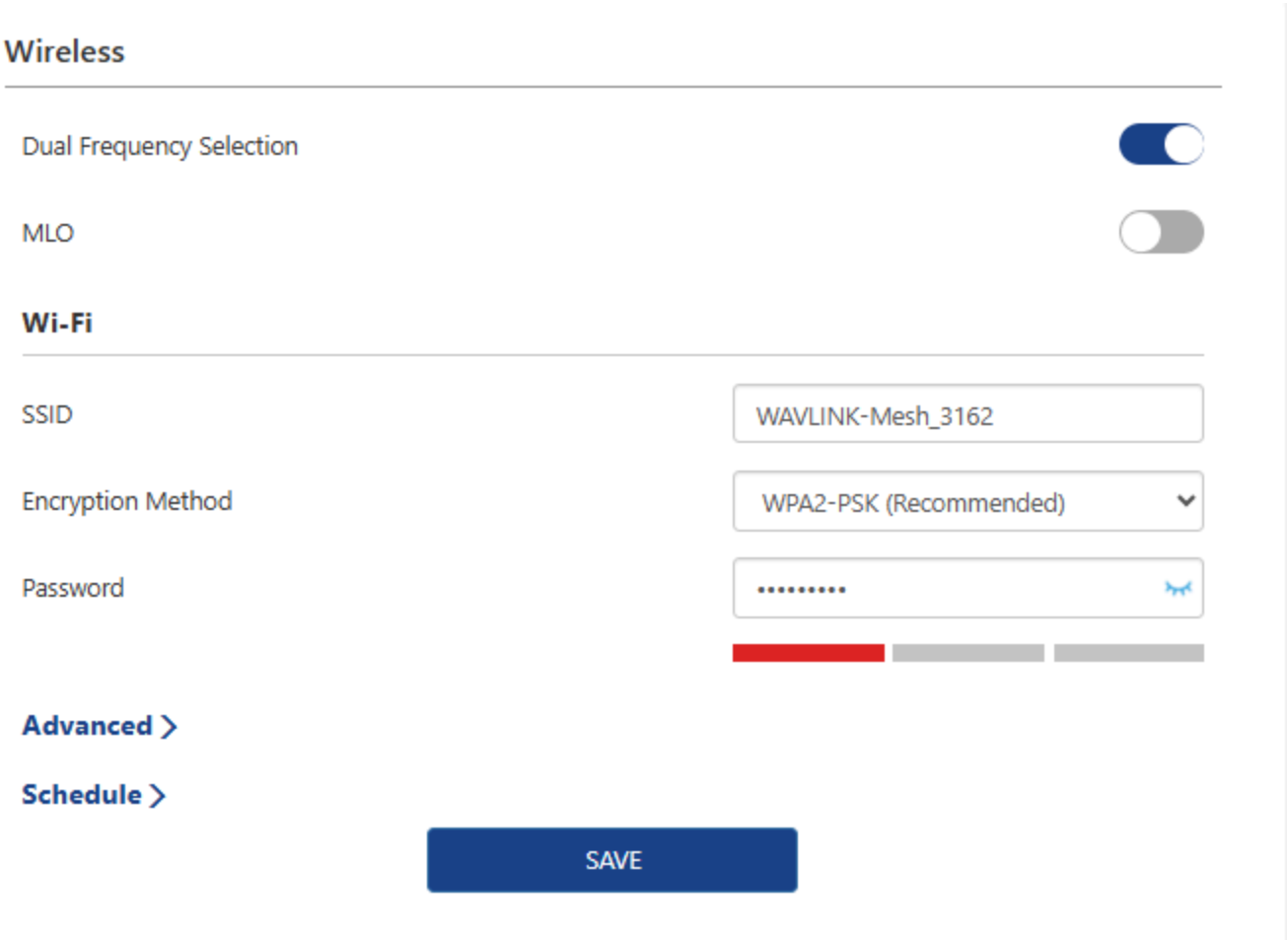
Wireless

Configure the SSID, encryption method, password, and other wireless parameters for both the 2.4G and 5G networks.

1. Navigate to **Wireless** or go to **More** > **Wireless** > **Wireless**.

Configuring Wireless Network

1） **Dual Frequency Selection** Enabling Dual Frequency Selection combines the 2.4GHz and 5GHz Wi-Fi bands into the same **Wi-Fi Name(SSID)**, when the terminal connect to the Wi-Fi, the router will automatically select network band for the terminal according to the internet status. Disabling it to configure the 2.4G and 5G band separately. 2） **MLO** When it is enabled, the terminal can establish multi-connection with the router to speed up the network and lower latency. This function requires two bands use the same Wi-Fi name(SSID) and wireless password, and the working mode should supports 802.11be.
3）**Change Wi-Fi Name and Password** Create a new Wi-Fi name in **SSID** and customize Wi-Fi password in **Password**.



Advanced Settings

1）**Channel**

Changing the wireless network channel as you need. If you are unsure which one to select, it is recommended to choose **Automatic**. The device will automatically select the optimal channel based on the surrounding environment for the best experience.

2）**Bandwidth**

The bandwidth indicates the frequency range of the wireless data transmission from the router.

3）**Disable Wi-Fi**

The Wi-Fi signal will be off after disabling the Wi-Fi.

4）**Hide SSID**

Enable this feature, the Wi-Fi signal will be hidden, which means SSID(Wi-Fi Name) will not be broadcasted or visible to devices searching for available networks. The user must manually input **SSID(Wi-Fi Name)** and **Password**.

5）**DFS**

It block interference from radar systems by automatically selecting and switching to the workable channel that has not used by the radar system. It is recommended to turn on

this switch to ensure compliance with local regulations and to maintain a stable and uninterrupted wireless network.

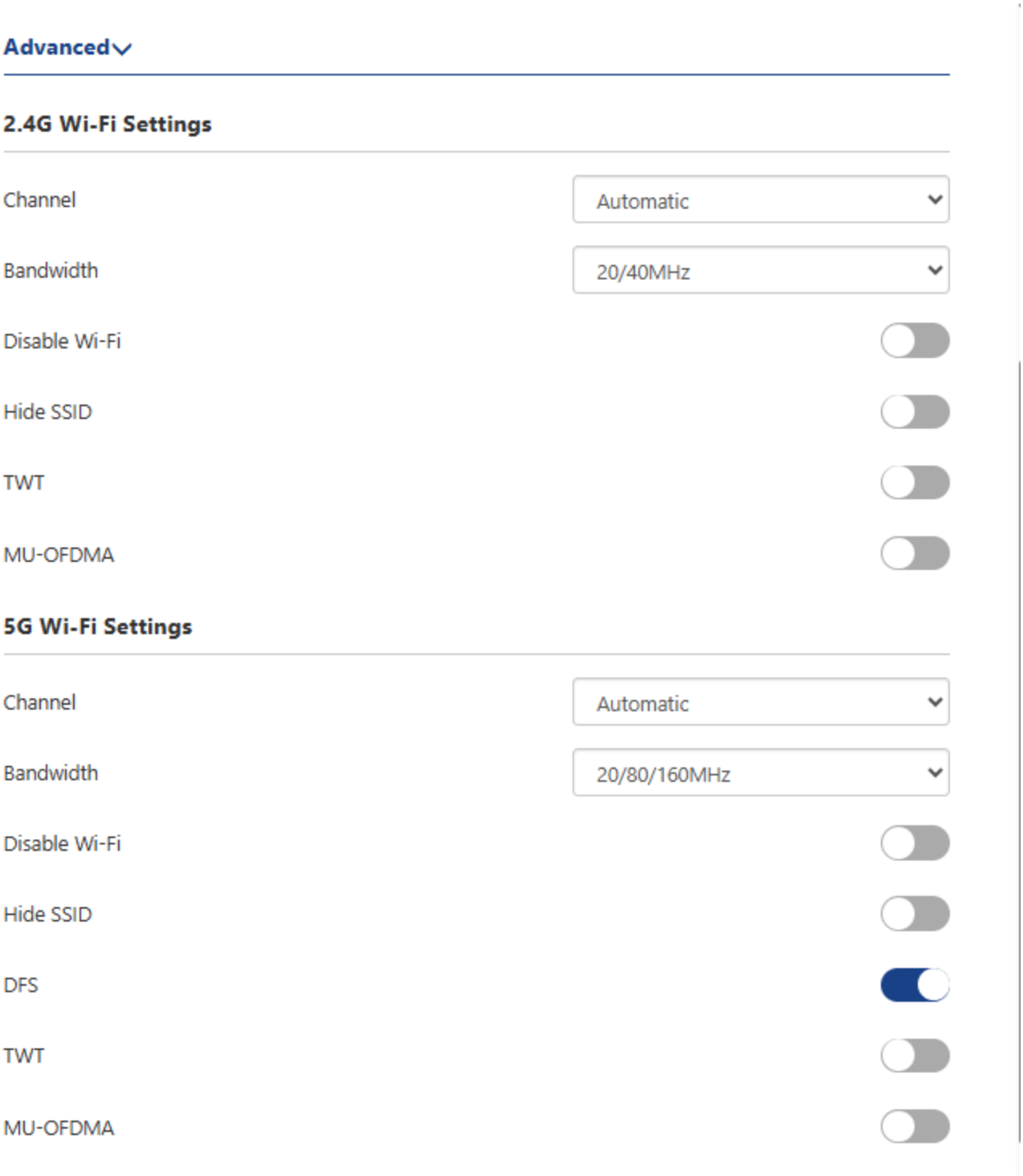
6）**TWT**

TWT is a power-saving mechanism. Once enabled, the router will automatically optimize resource scheduling between devices, negotiate wake-up schedules, reduce unnecessary contention, and extend device sleep time, thereby prolonging the lifespan of connected devices.

Note: Some of the terminals may occurs compatibility on TWT function.

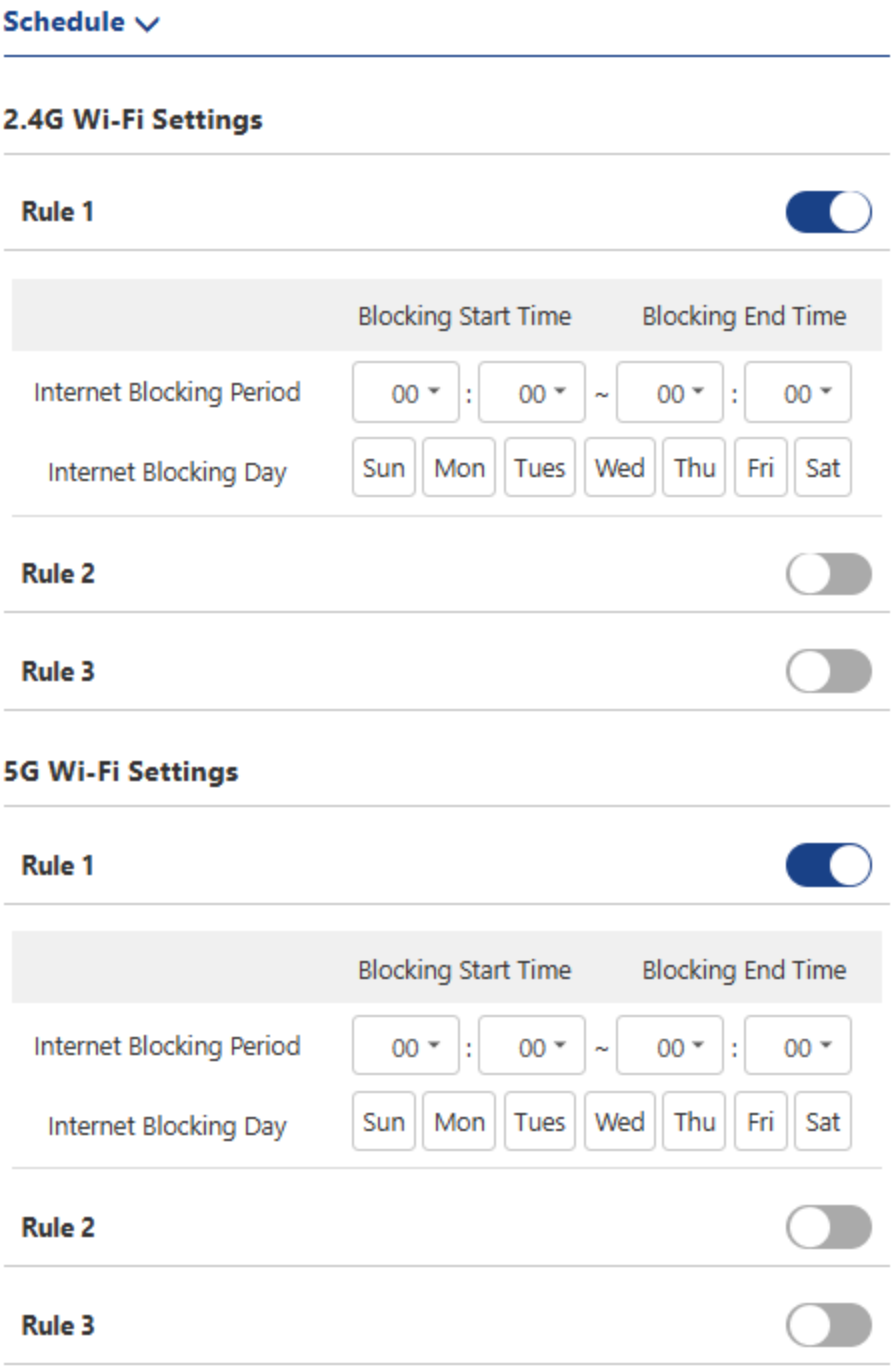
7）**MU-OFDMA**

Once enabled, the router will use multiplexing technology to improve transmision efficiency and reduce network latency. The multiplexing technology make several users share available bandwidth, and cut them into smaller channel and time slots. This enables simultaneous data transmission for different devices, enhancing network performance and ensuring smoother communication for all users.



Schedule (Wireless Timer Switch)

The schedule function allows you to customize event rules to control the wireless network switch, with up to three rules definable. This feature only takes effect after obtaining the network time and only affects the main network. For the guest network, you need to manually enable or disable this feature or define separate rules within the guest network settings.



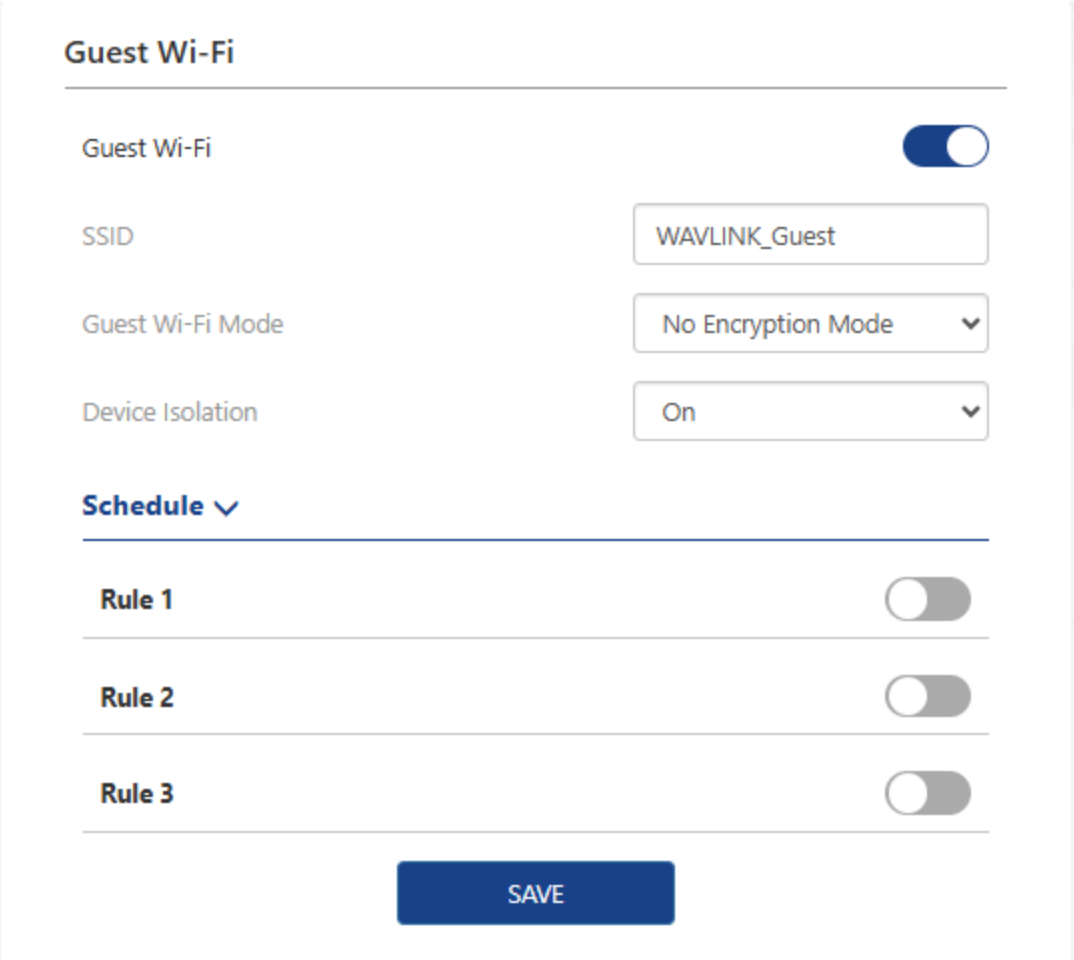
1. Navigate to **Wireless** > **Schedule** or go to **More** > **Wireless** > **Wireless** > **Schedule**.
2. Click on **Rule 1/2/3** under either the **2.4G Wi-Fi Settings** or **5G Wi-Fi Settings** to set the timing rules.
3. Click **SAVE** to complete the settings.

Note:

- The schedule is based on the router's time. You can modify the time by going to **More** > **System** > **Time Zone**.
- The wireless network will automatically turn on after the set time period.

Guest Wi-Fi

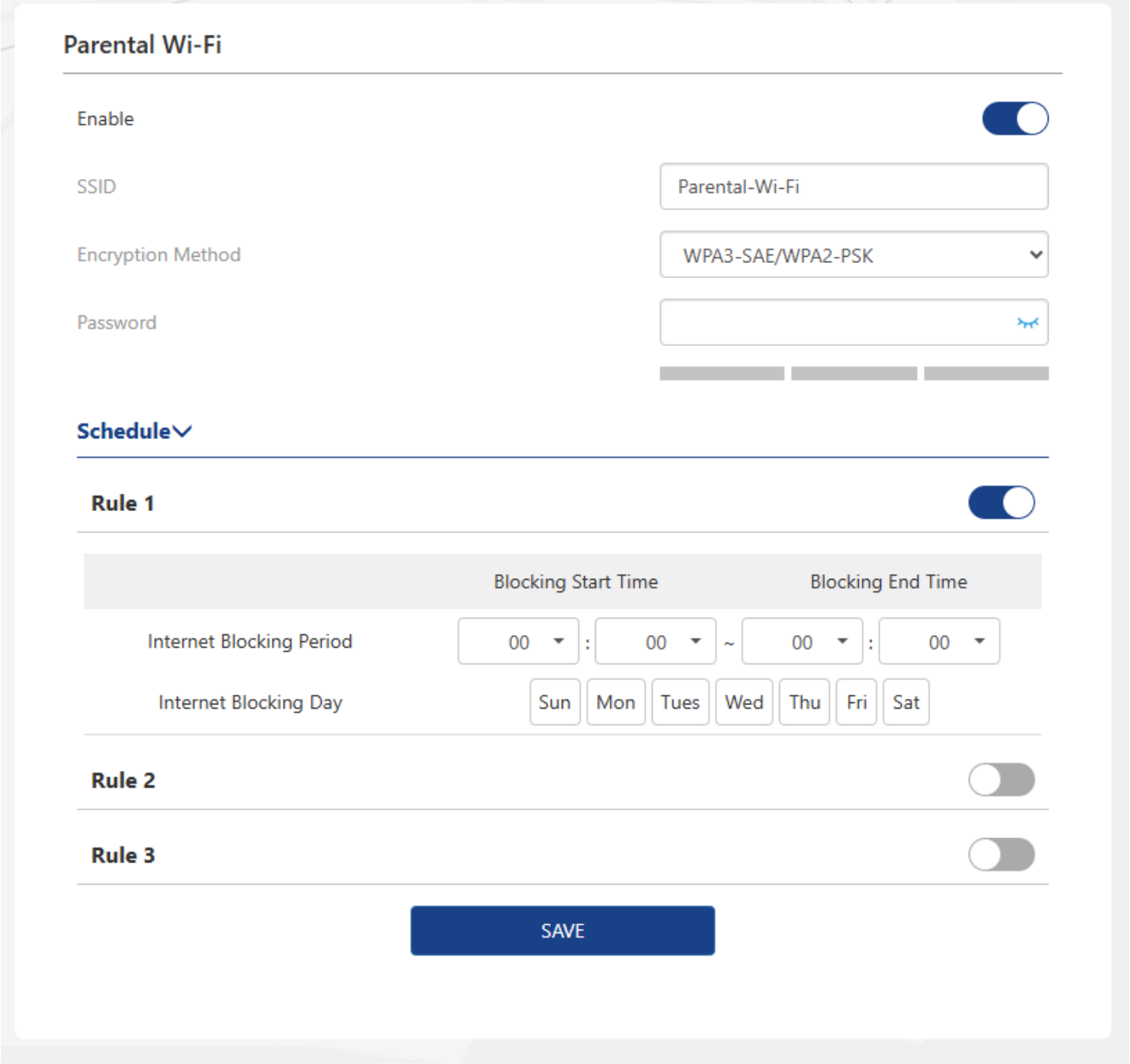
The guest Wi-Fi provides guests(visitor, client or temporary device) with a independent and secure network environment isolated from the main network. Network administrators offer convenient access while protecting the security and resources of the primary network.



1. Navigate to **More** > **Wireless** > **Guest Wi-Fi**.
2. Click to enable **Guest Wi-Fi**.
3. Set the **SSID**.
4. In the **Guest Wi-Fi Mode**, set the encryption method: Encryption Mode, No Encryption Mode, and WPA/WPA2. If you select WPA/WPA2, you will need to set the RADIUS server IP, RADIUS port, and RADIUS password.
5. Set the **Device Isolation**. Once on, this feature will isolate devices connected to the same LAN from each other, enhancing network security and privacy protection.
6. Set the guest Wi-Fi open time in the **Schedule**.
7. Click **SAVE** to complete the settings.

Parental Wi-Fi

Parental Wi-Fi allows you to set up a wireless network with separate SSID(Wi-Fi name) and separate password for family members. You can configure its SSID, encryption method, and rules as you need.



1. Navigate to **More** > **Wireless** > **Parental Wi-Fi**.
2. Click to enable **Parental Control**.
3. Set the **SSID, Encryption Method, and Password**.
4. Set the Internet Blocking Period and Internet Blocking Day in **Rule 1/2/3** to control your child's internet access time.

5. Click **SAVE** to complete the settings.

Chapter 5 Mesh

This chapter contains the following section:

Mesh Configuration

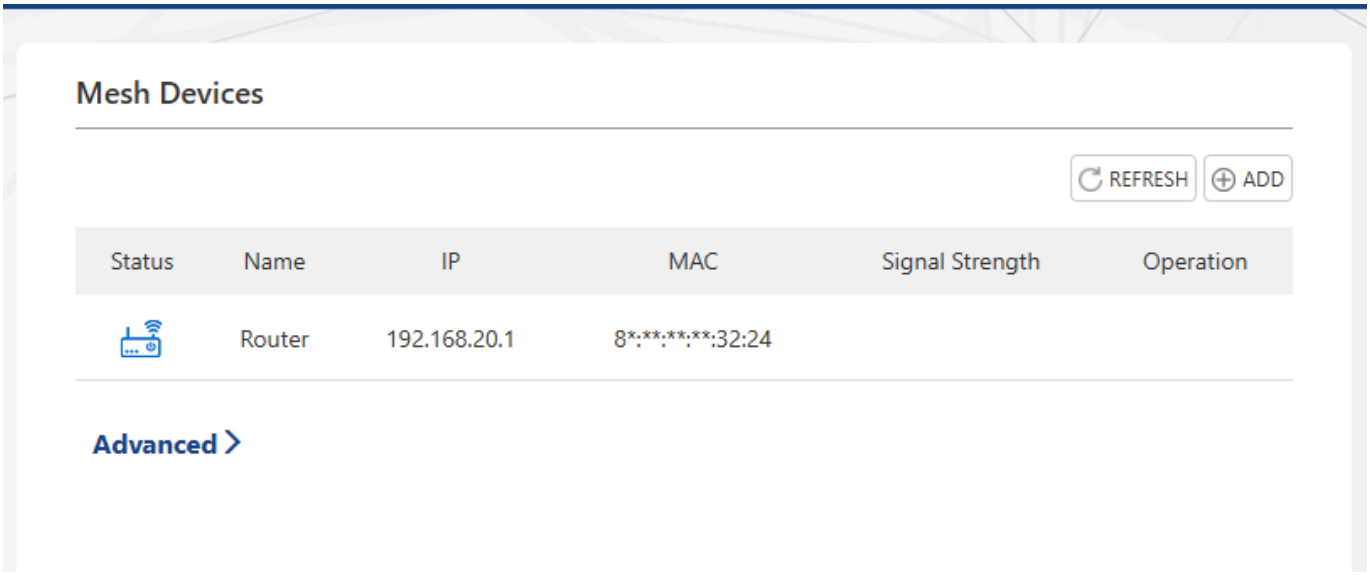
If a single router cannot provide adequate wireless coverage for large homes, you can purchase multiple WAVLINK routers that support Mesh networking to achieve full Wi-Fi coverage throughout your home.

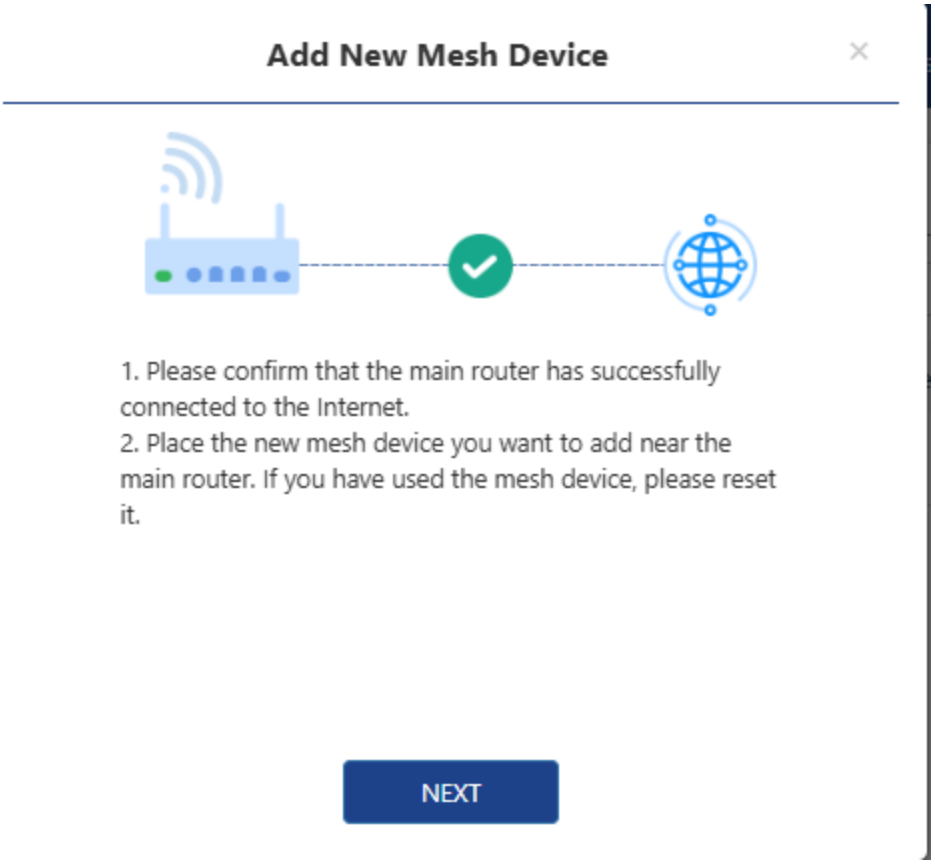
Adding New Mesh Device

Before setting up the Mesh network, ensure that:

The main router is connected to the internet, and the setup wizard is complete. The indicator light shows a solid blue.

1. Navigate to **More** > **Mesh** > **Mesh Devices**.
2. Click on **⊕Add**. Follow the on-screen instructions to prepare your mesh device, then click **NEXT**.

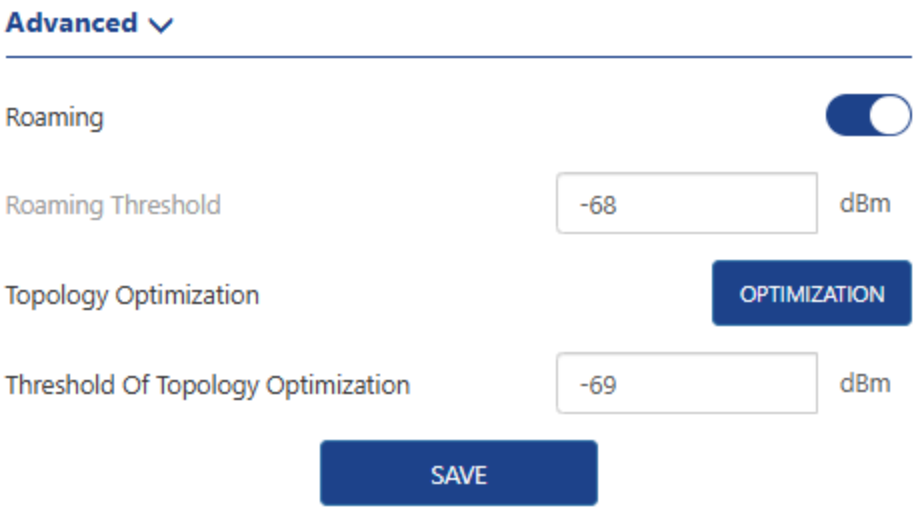




3. Follow the on-screen instructions to power on the mesh device and press the pair button when the mesh device starts operating. Click **“SCAN”**. The main router will automatically scan the mesh device that is attempting to pair.

4. Once the scan is completed, select the mesh device you want to add.

Advanced Settings



1）Roaming (Wireless Roaming Technology)

Enabling Roaming allows devices to seamlessly switch between two Mesh routers. As you move away from one router and get closer to another, the device will automatically disconnect from the current router and connect to the nearer one to provide a smoother network experience.

1. Navigate to **More** > **Mesh** > **Mesh Devices** > **Advanced**.
2. Click to enable **Roaming**.
3. Set the **Roaming Threshold** to an appropriate parameter.

Note: The wireless roaming trigger threshold should only be set by experienced professionals. If you lack professional experience in setting this, it is recommended to keep the default settings to avoid negatively impacting the network user experience.

2）Topology Optimization

When you have three or more paired devices and all devices have completed pairing, you can enable the topology optimization feature. This function can automatically adjust the optimal path based on the signal strength between devices to ensure that all sub-routers and corresponding upper-level devices have the best signal connection status, achieving optimal network coverage.

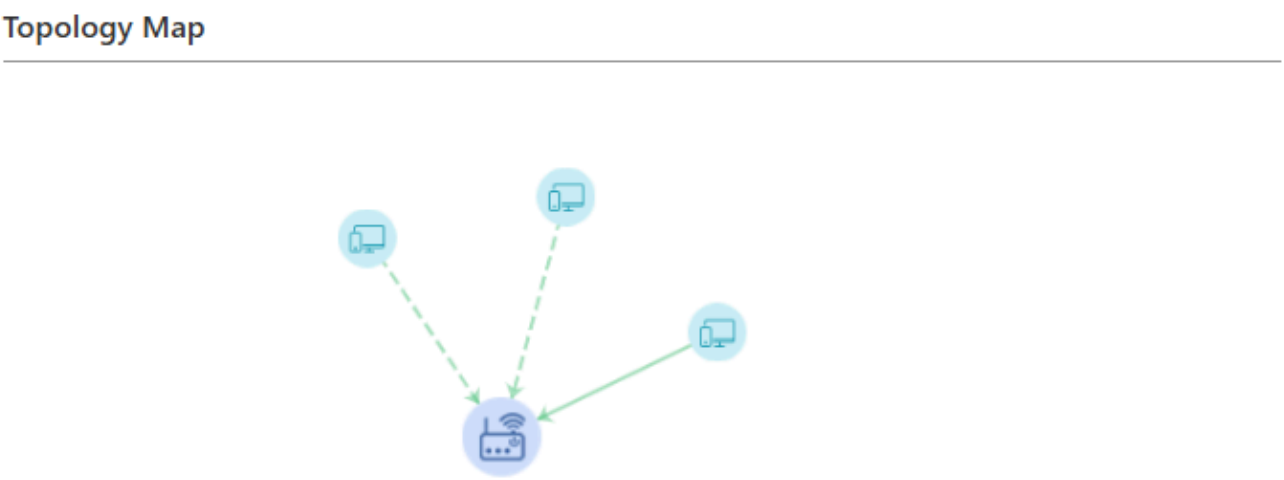
1. Navigate to **More** > **Mesh** > **Mesh Devices** > **Advanced**.
2. Click the **OPTIMIZATION** button after **Topology Optimization**.
3. Ensure the **Threshold Of Topology Optimization** is set to an appropriate parameter.

Note: You can adjust the signal threshold that triggers topology optimization to achieve the best mesh network coverage. If you do not have professional setup experience, it is recommended to use the default settings.

Topology Map

In this interface, you can see the network topology map, which shows the device access relationships and network connection status. It will also display the MAC address of each connected device, making it easier to see which terminals the devices are connected to.

1. Navigate to **More** > **Mesh** > **Topology Map**.



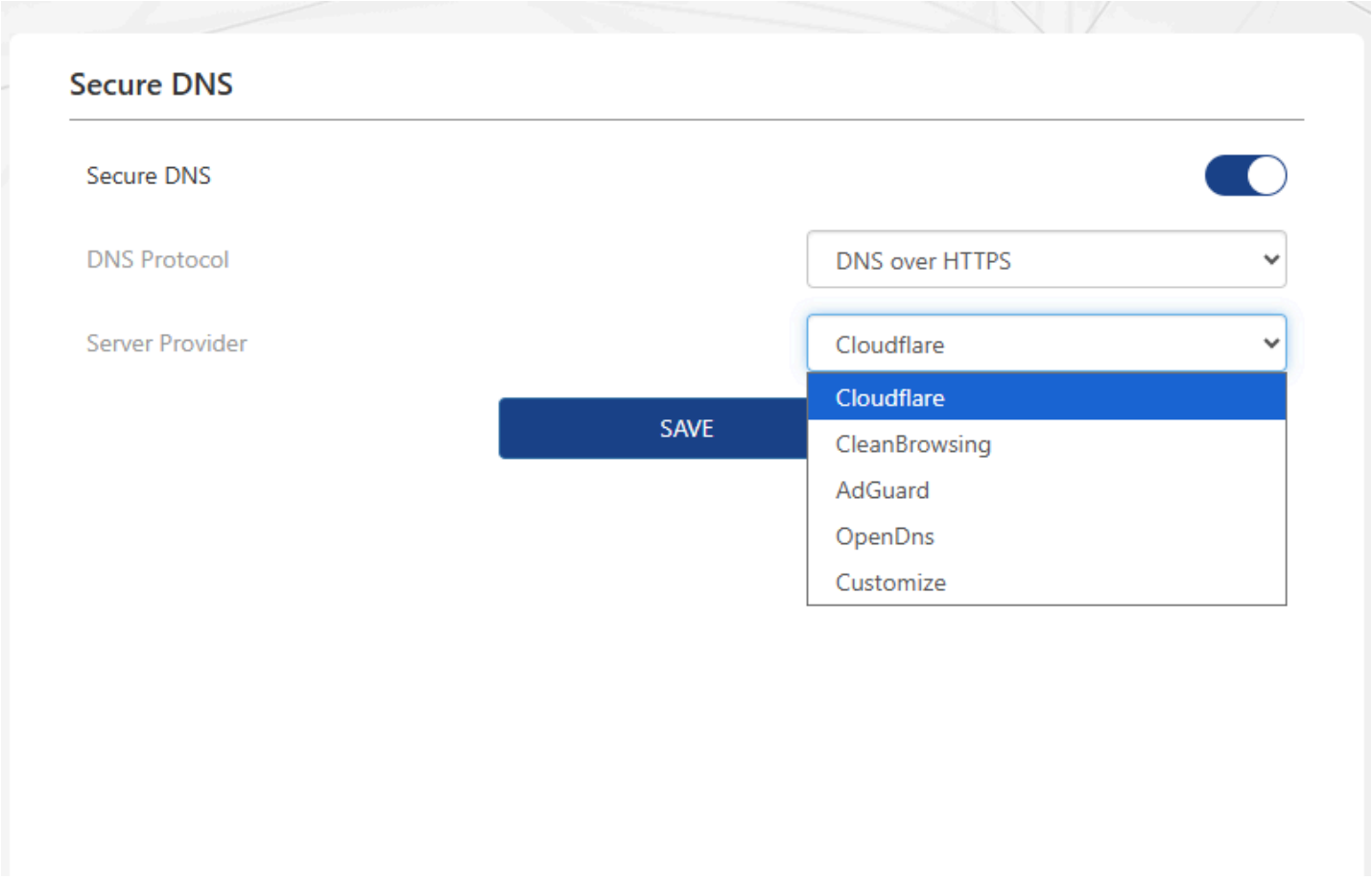
Chapter 6 Net Guardian

This chapter contains the following sections:

Secure DNS

This feature encrypts your DNS traffic to enhance security and privacy, preventing DNS leaks and DNS hijacking.

1. DNS Navigate to **More** > **Net Guardian** > **Secure DNS**
2. Click to enable **Secure DNS**.
3. Set the **DNS Protocol** and **Server Provider**.
4. Click **SAVE** to complete the configuration.



AdGuard Home

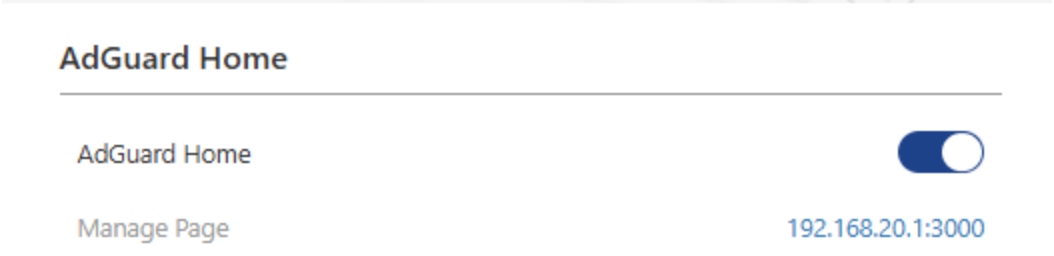
AdGuard Home acts as a global DNS blocker to filter harmful content from the network, such as ads, malwares, trackers, and more.

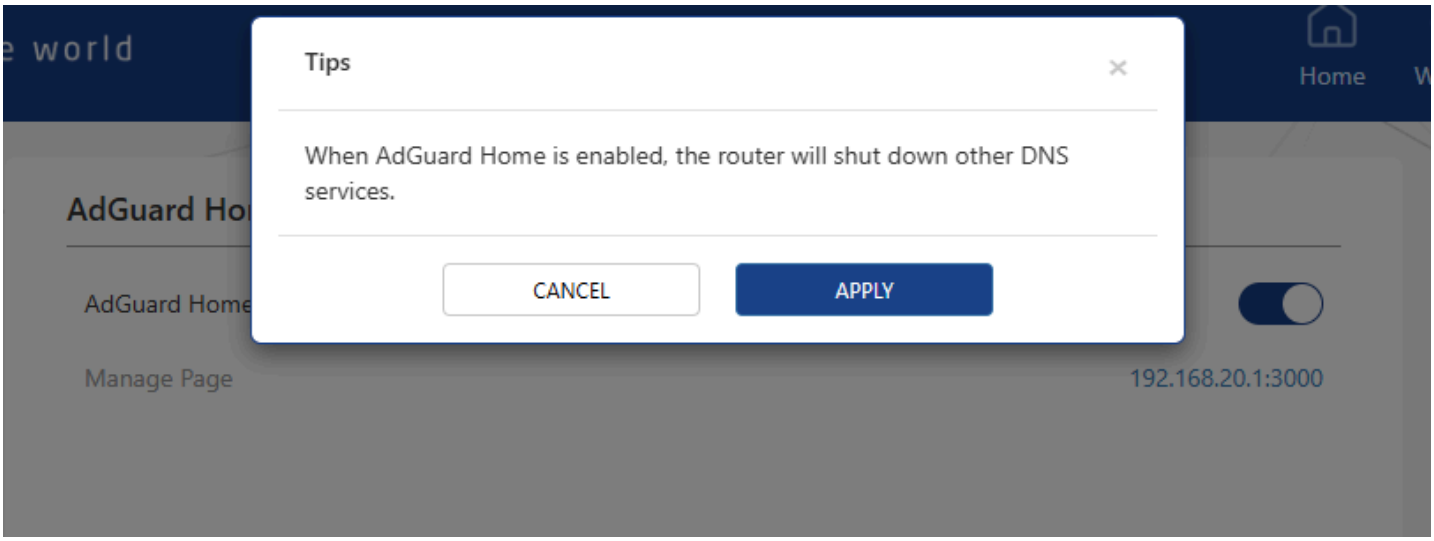
AdGuard Home also offers advanced functions such as parental control, statistics, custom rule, and more so you can better manage network traffic and protect privacy. By running AdGuard Home on your router, you can have one-stop ad blocking and privacy protection for your entire network without installing separate software or browser plug-ins on each device.

Initial Settings

1 . Access **More> Net Guardian > AdGuard Home**.

2 . Open **AdGuard Home**. When AdGuard Home is enabled, the router will shut down other DNS services.



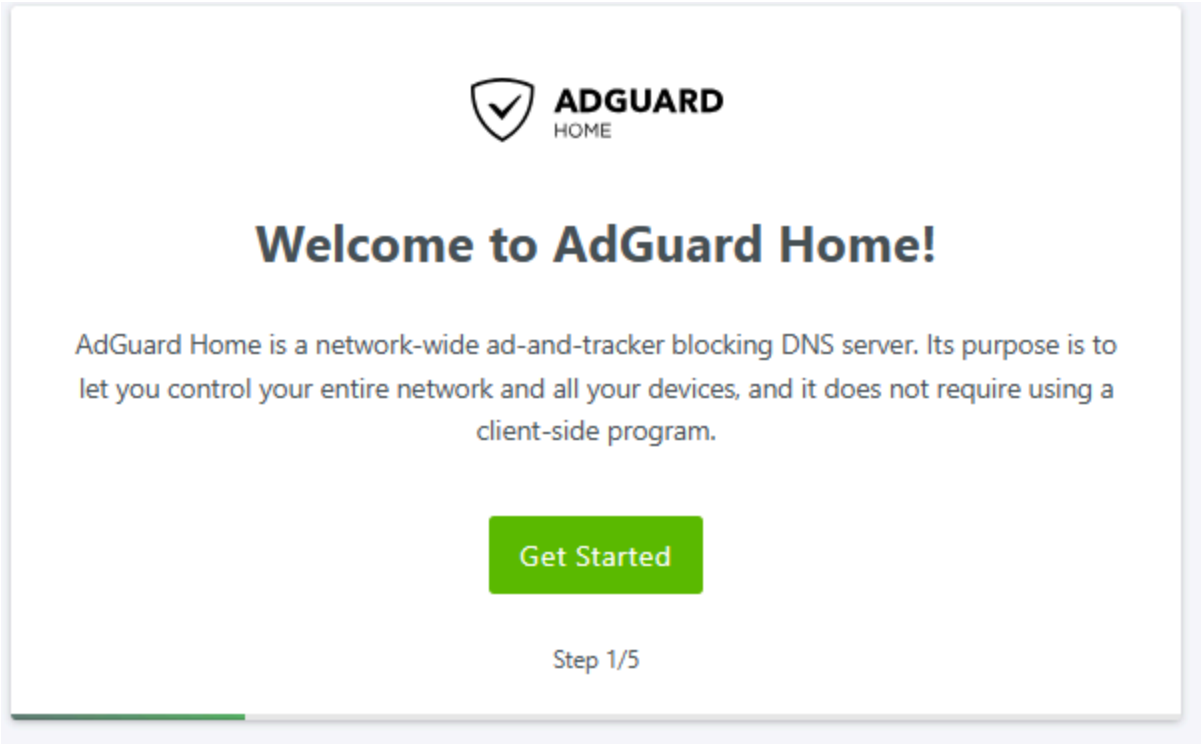


3 . Click **the URL** behind Manage Page or enter http://192.168.20.1:3000 manually on the browser. Access the AdGuard Home manage page and enter the installation guard page.

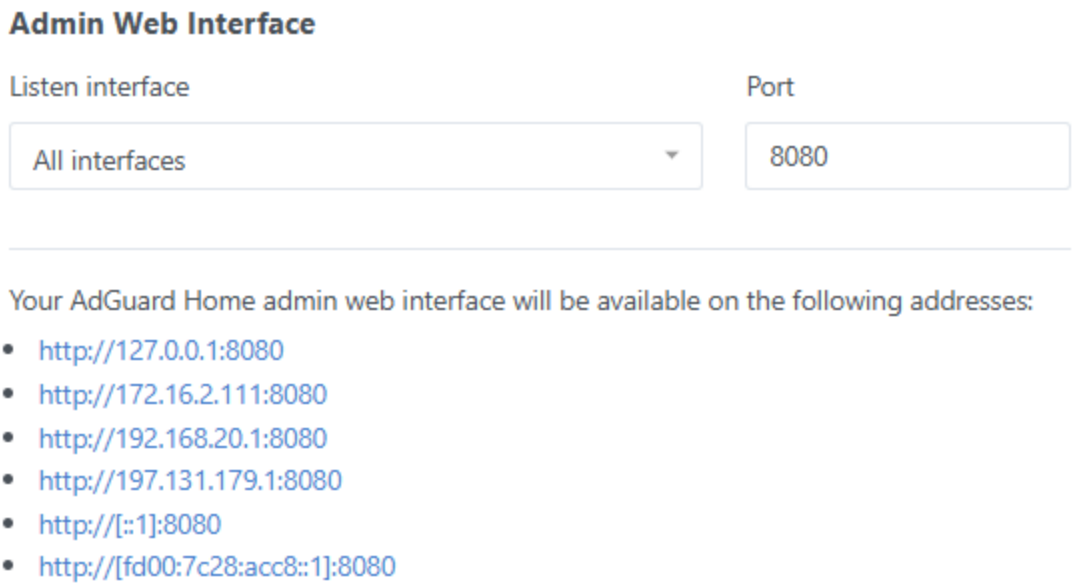
NOTE

If your router IP is not 192.168.20.1, please change 192.168.20.1 to your router IP.

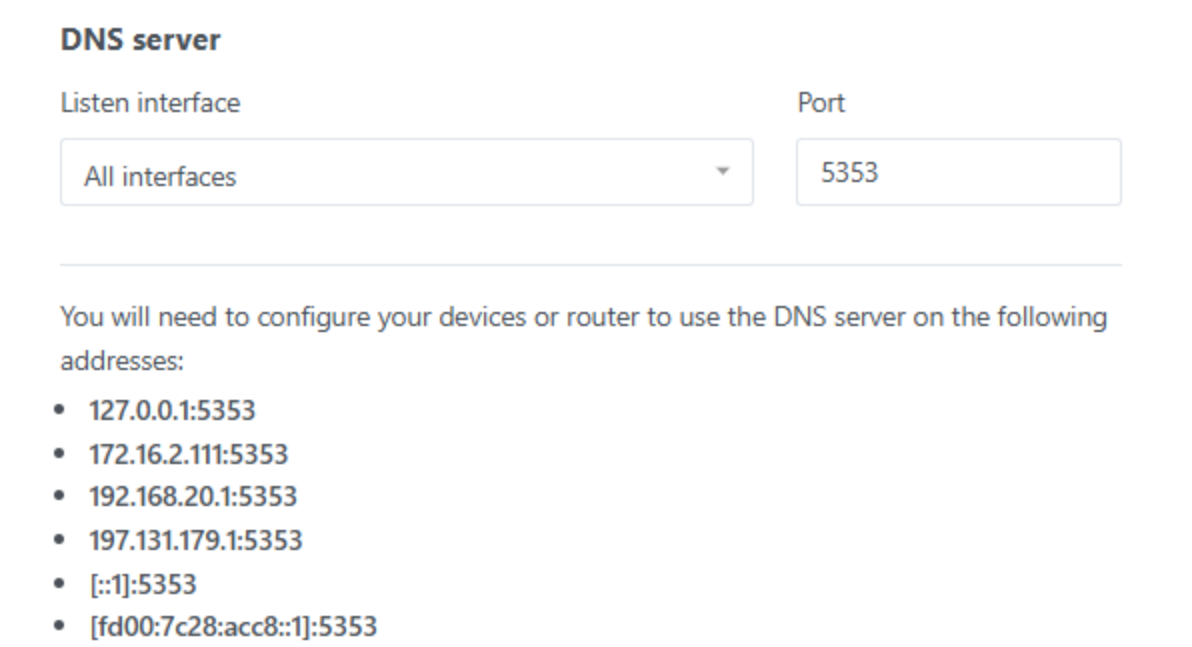
1） Enter the AdGuard Home manage page, and click **Get Started**.



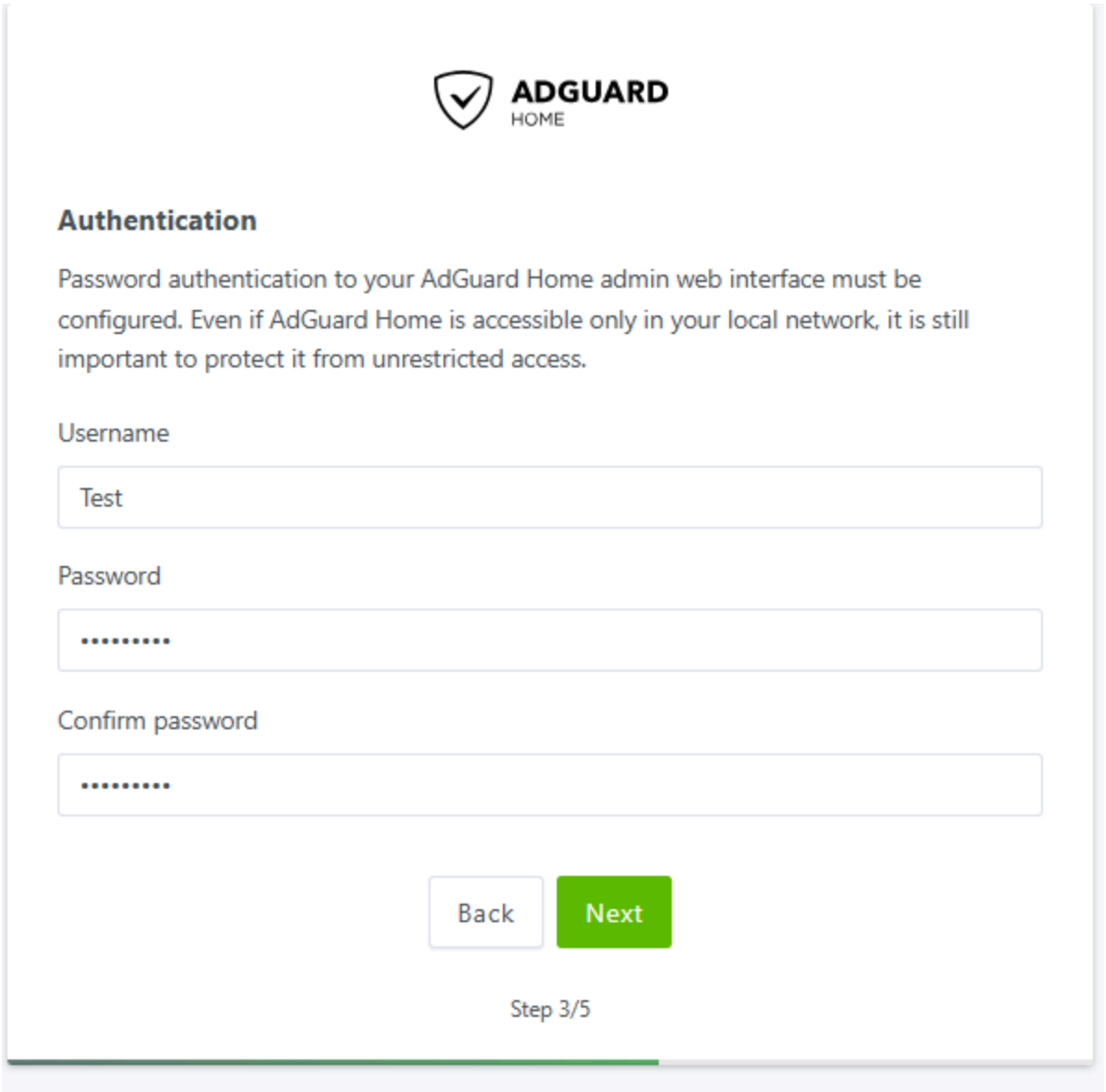
2） Select the **Listen interface** and bind **Port** on the Admin Web Interface.



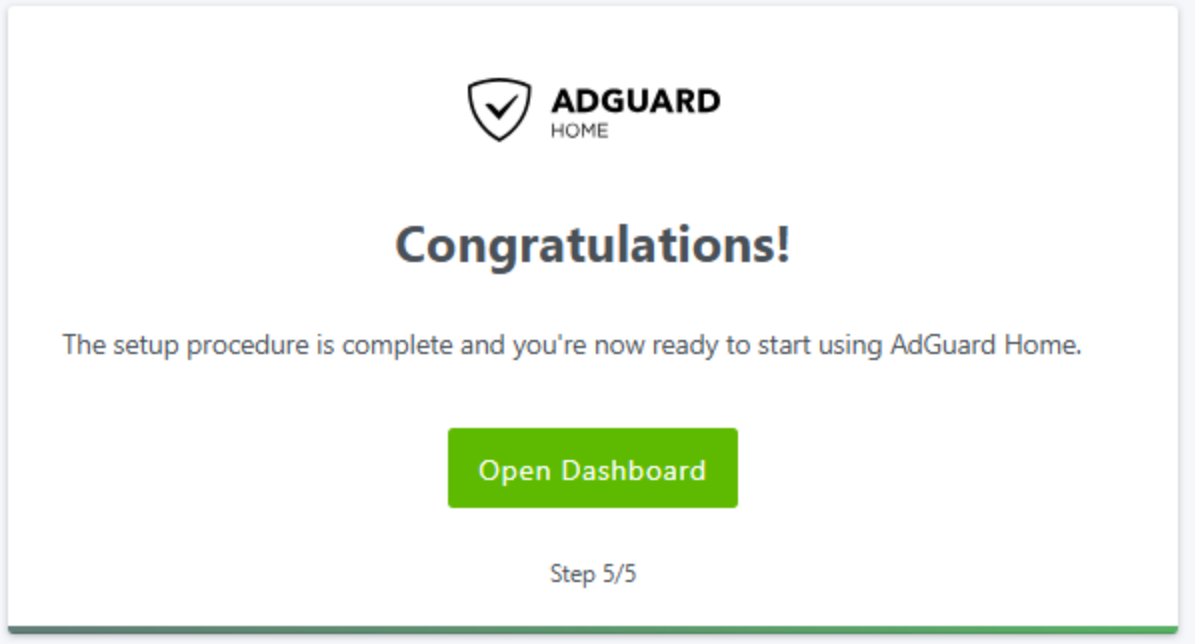
3） Select the **Listen interface** and bind **Port** on the DNS server.



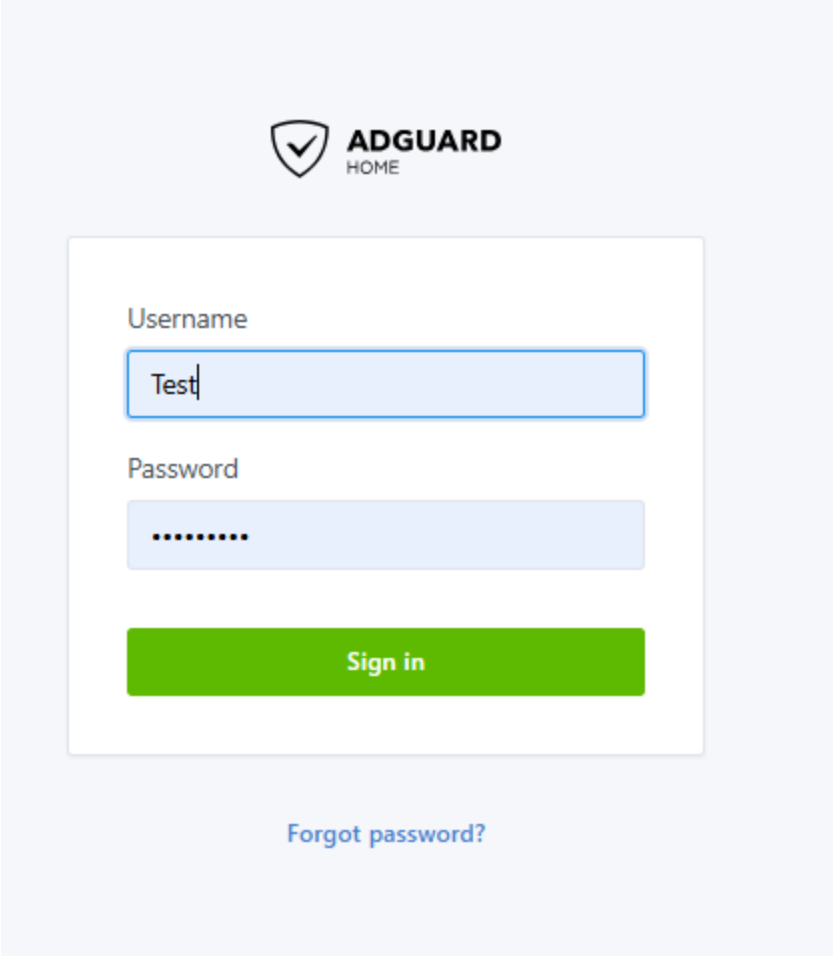
4） Set the username and password for AdGuard Home login. Click **Next**.



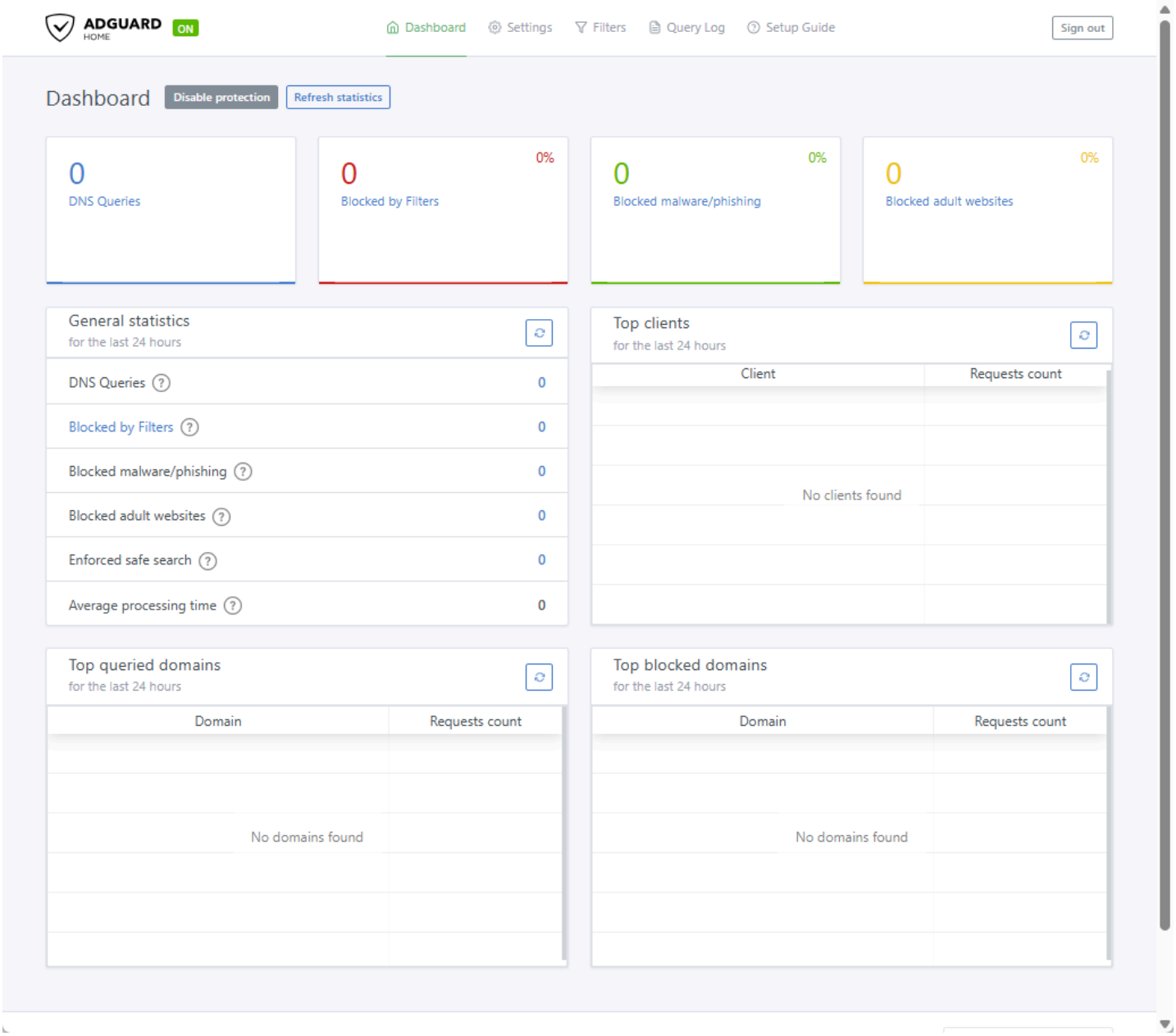
5) Click **Open Dashboard**.



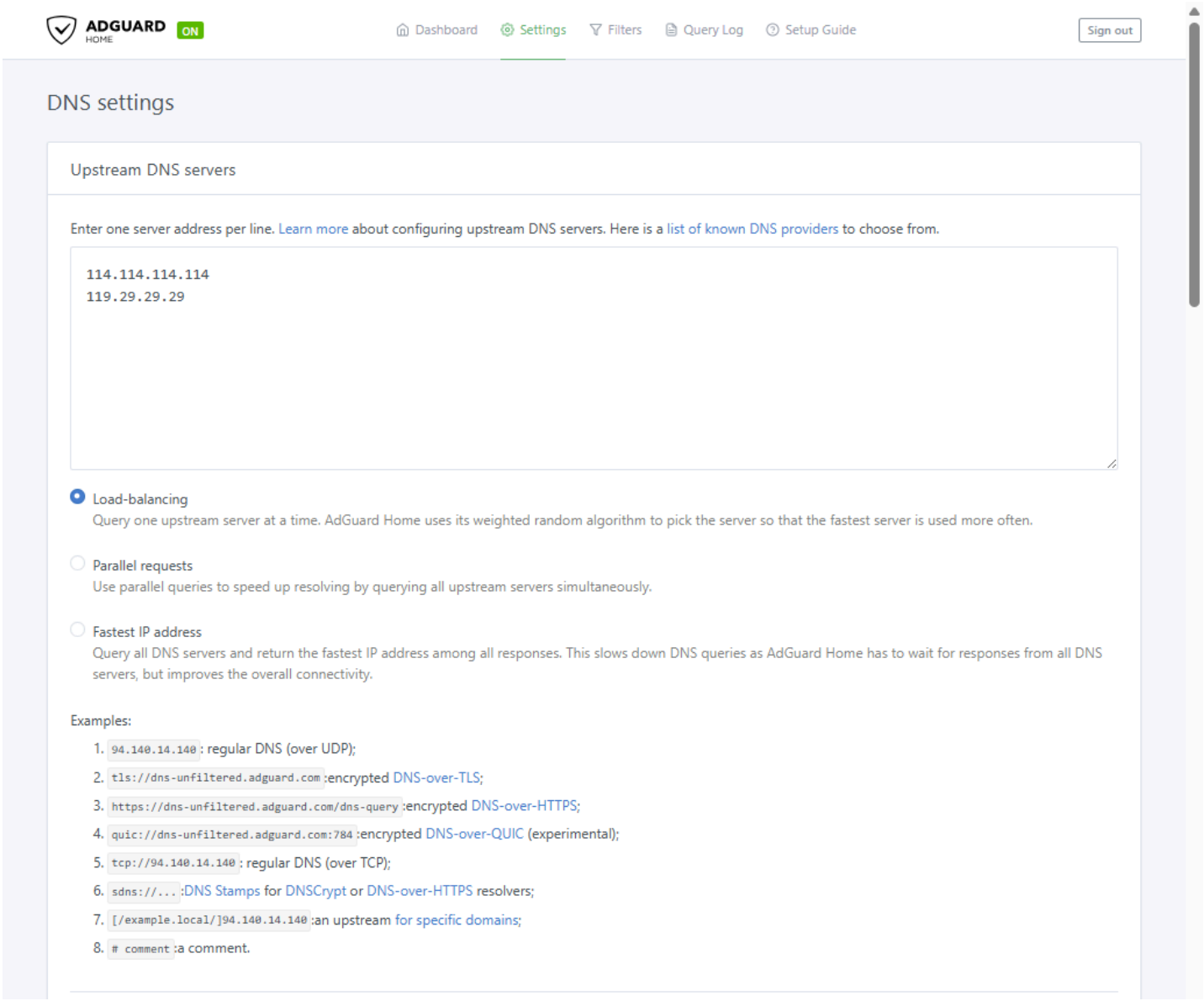
6) Enter your **Username and Password** to log in to the dashboard.



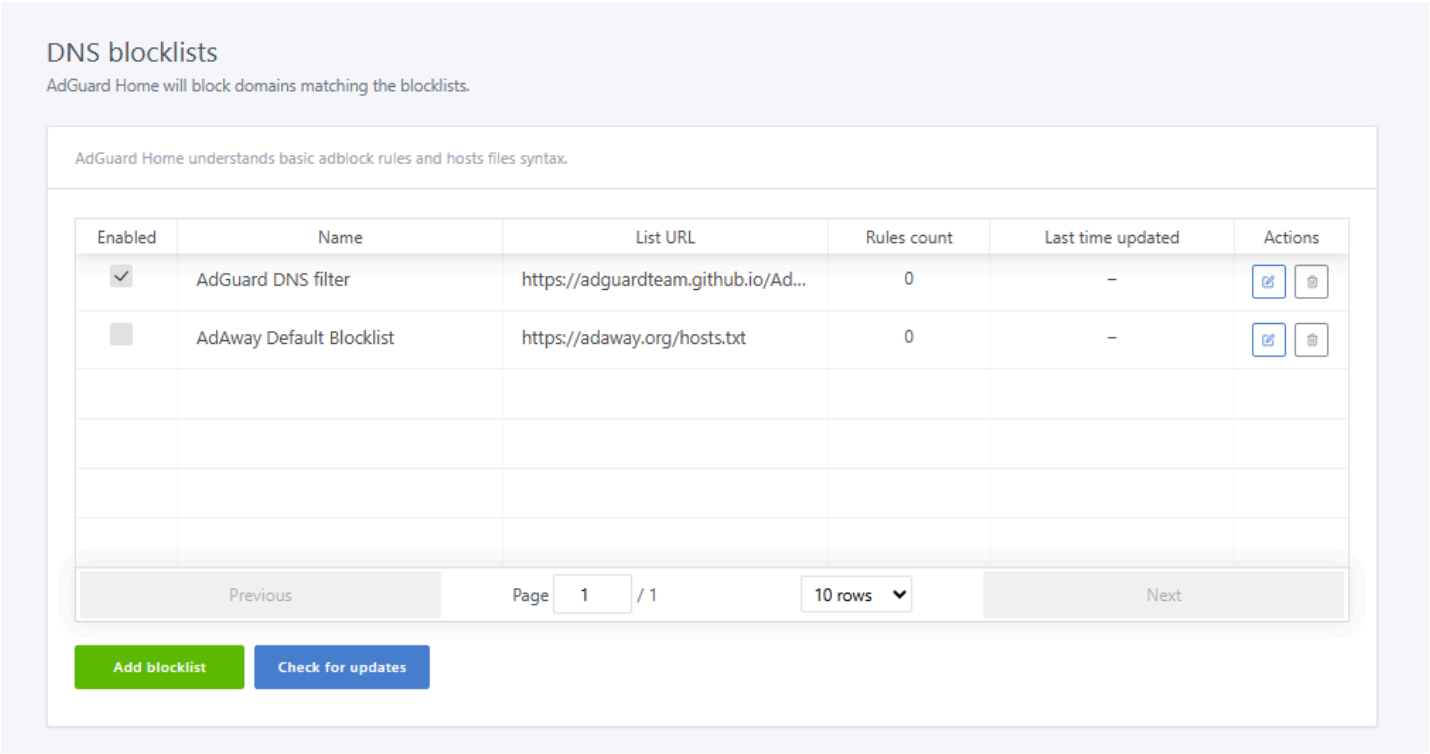
7) In the dashboard, you can monitor the number of DNS blocks and some lists in real time.



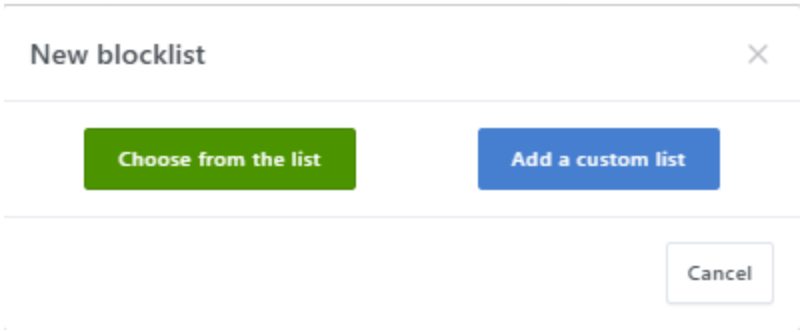
8) If you can not use a default DNS server, you can add a new DNS in **Settings**.



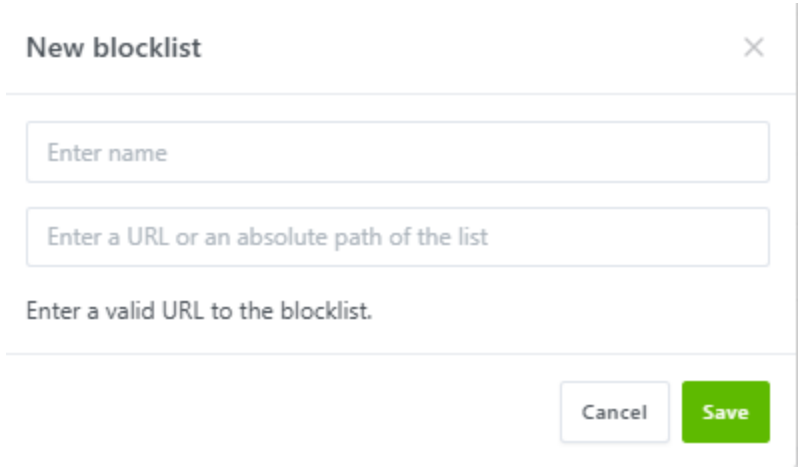
9） If you set DNS blacklists, please access **Filter>DNS blocklists**.



10) Click **New blocklist>Add a custom list**.



11) Enter the name and URL of the new blocklist. Click **Save**.



Chapter 7 NAT Forwarding

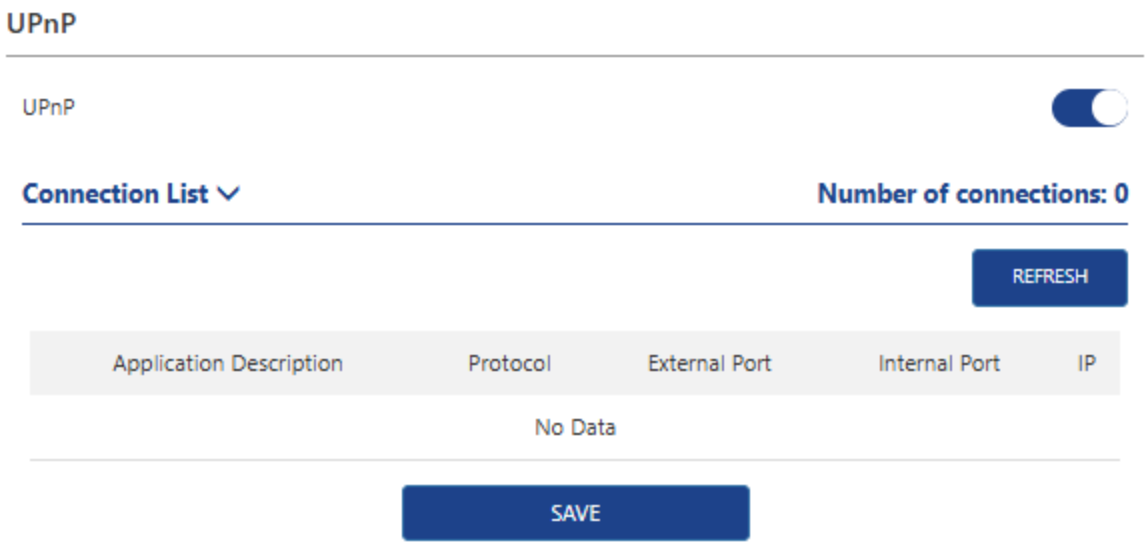
This chapter contains the following sections:

UPnP Settings

UPnP (Universal Plug and Play) is a network protocol designed to make connecting devices simpler and more automated. Using the UPnP protocol, devices can automatically discover each other on the network and establish communication connections without requiring manual configuration or setup.

UPnP allows devices to share resources such as files, printers, and other multimedia content. The UPnP protocol is widely used in home networks and office environments to facilitate communication and interaction between devices.

1. Access **More>NAT Forwarding>UPnP**.
2. Set **ON/OFF UPnP**.
3. Click **SAVE** to finish configuration.

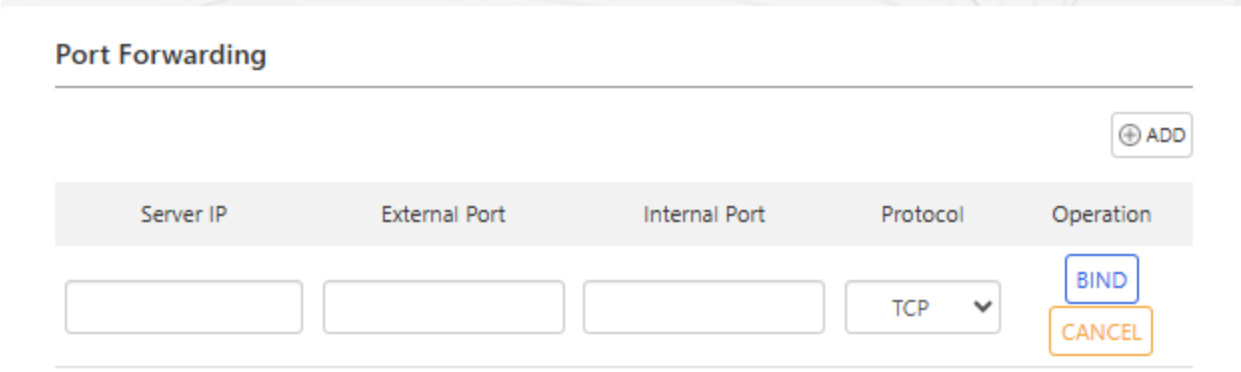


NOTE

The computer operation system and application program you used need to support the UPnP function.

Port Forwarding

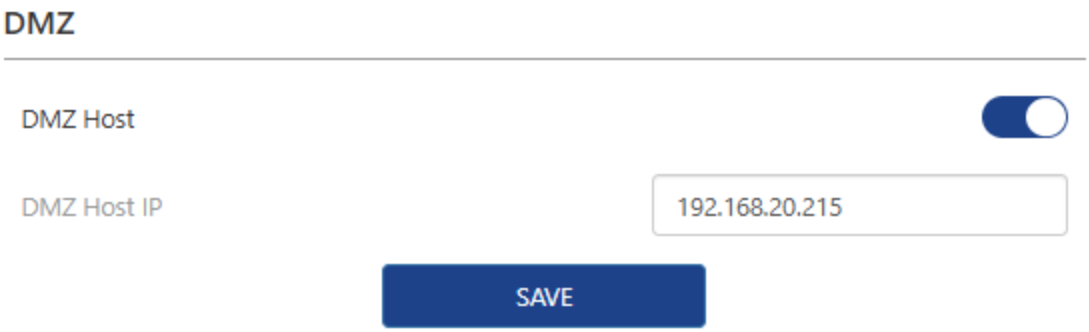
Port forwarding is a network technology. It maps a specific port on a public network to a specified server on the local network, allowing Internet users to access the local network server’s service by accessing the port.



1. Access **More>NAT Forwarding>Port Forwarding**.
2. Click **Add**.
3. Enter the parameters of **Server IP, External Port**, and **Internal Port**.
4. Select **Communication Protocol**.
5. Click **Bind** to finish the configuration.

DMZ

Enable DMZ（Demilitarized Zone）management function, only enter one IP address that connects this device, then this device can be DMZ host. So this device can be accessed via external network and open all ports to improve fluency of corresponding communication. Please note security software and firewall on this host need to be closed temporarily when you use this function. So please consider using this function carefully.



NOTE

DMZ is suitable for use when you are not sure of the ports that need to be opened. Computers will be completely exposed to the WAN after opening DMZ Host, which may bring security risks to computers. So please do not open it easily. Close it in time if you do not need to use DMZ Host.

1. Click **Network** > **Static IP Binding** to set a fixed IP for the host configured as DMZ device.
2. Access **More>NAT Forwarding>DMZ**.
3. Open **DMZ Host**.
4. Enter the **IP address** of the corresponding computer (192.168.20.215) in **DMZ Host IP**.
5. Click **SAVE** to finish the configuration.

Hardware NAT

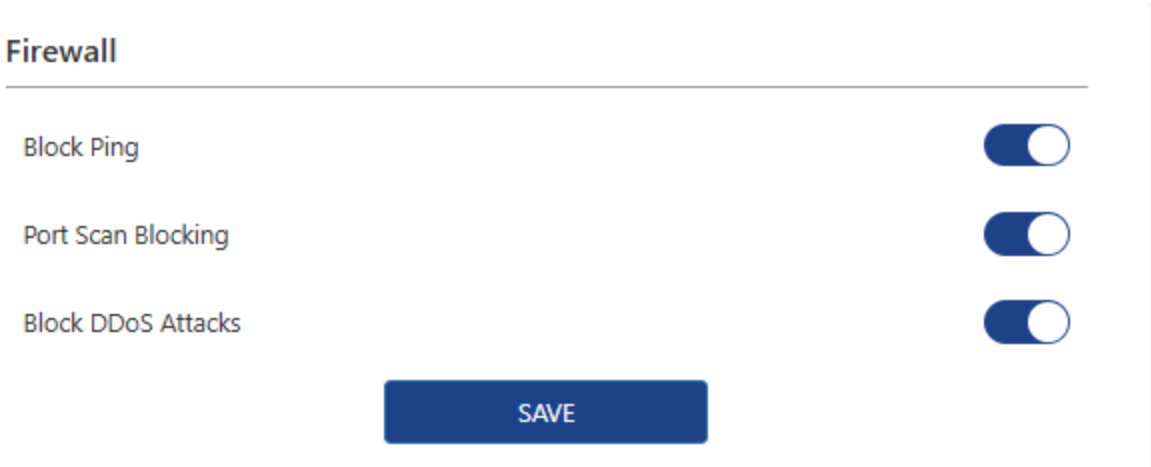
Data is forwarded by hardware instead of being processed by the CPU after enabling Hardware NAT, which can improve the device's performance. Turn off NAT if you need to calculate throughput rate, usage statistics of CPU and RAM.

1. Access **More>NAT Forwarding>Hardware NAT**.
2. Open **Hardware NAT**.
3. Click **SAVE** to finish the configuration.

Chapter 8 Network Security

This chapter contains the following sections:

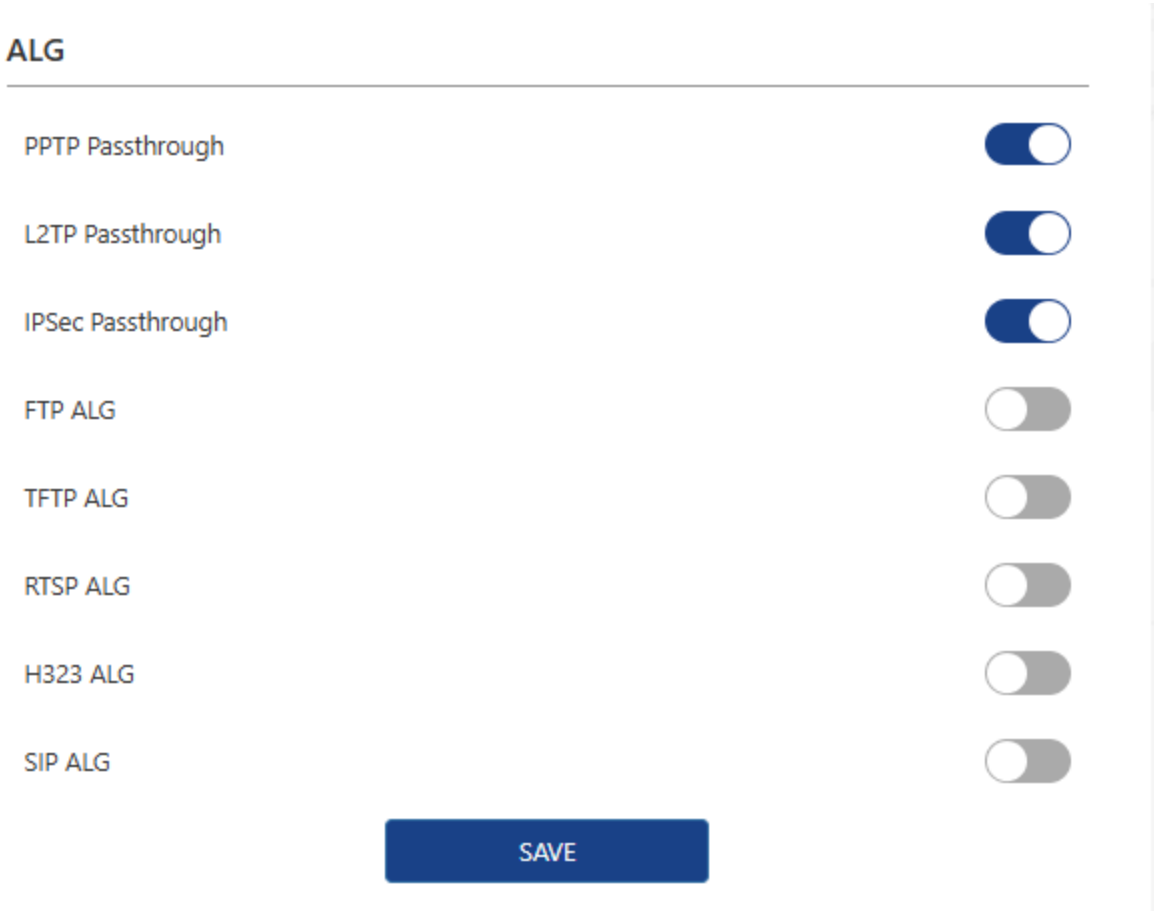
Firewall



1 . Access **More settings>Security>Firewall**.
2 . Open **Block Ping**: It can prevent ping attacks and scanning and reduce the risk of network attacks on this device.
3 . Open **Port Scan Blocking**: It can protect server ports on devices from attacks.
4 . Open **Block DDoS Attacks**: It enables the router to avoid the massive resource consumption caused by DDoS attacks and ensures normal services.
5 . Click **SAVE** to finish the configuration.

ALG Configuration

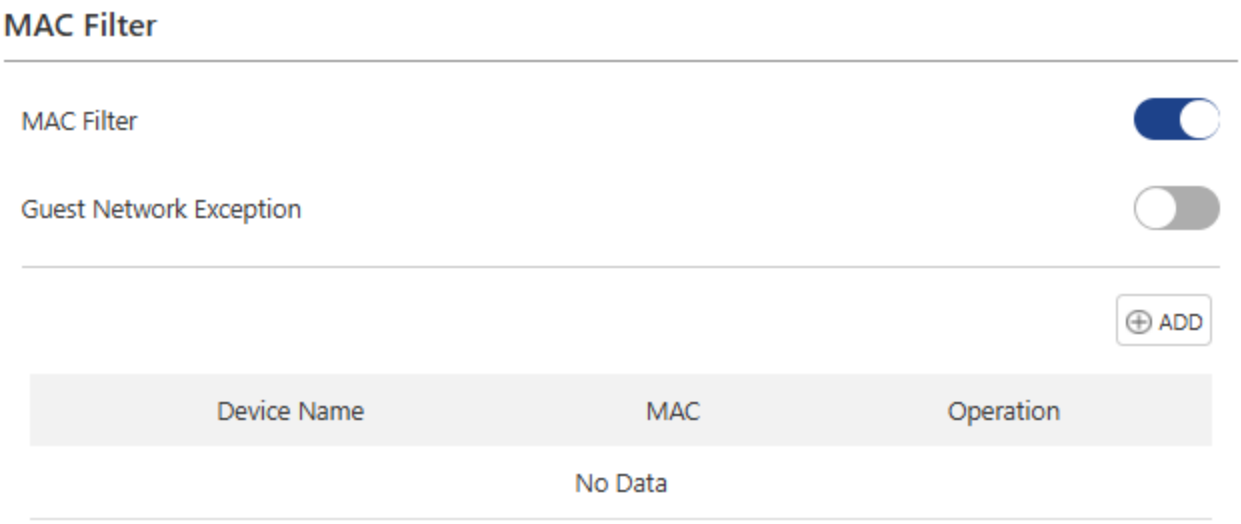
ALG（Application Layer Gateway）allows a custom NAT traversal filter to be inserted into the gateway to support the address and port translation of certain application layer “control/data” protocols. Keeping default settings is recommended. When you use voice and video applications to create or receive calls through the router, you may need to disable SIP ALG because some voice and video applications do not work well with SIP ALG.



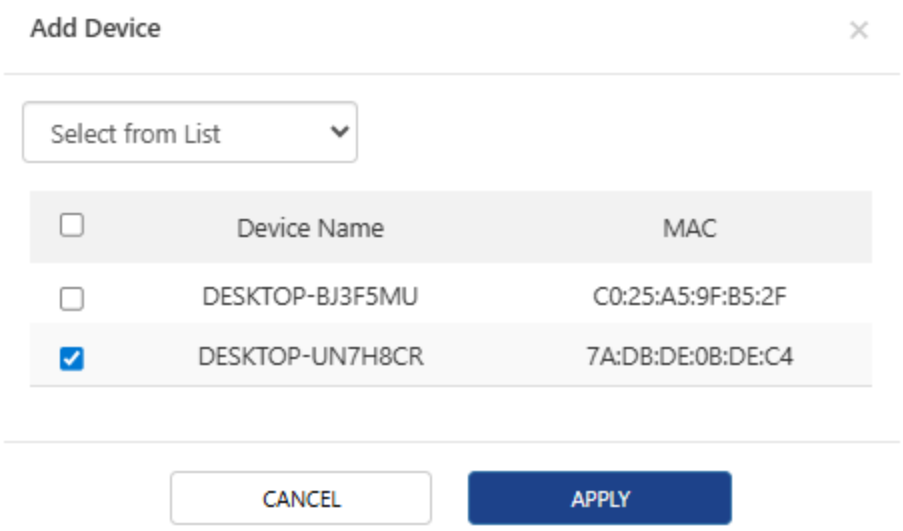
1 . Access **More>Security>ALG**.
2 . After configuration, please click **SAVE** to finish.

MAC Filter

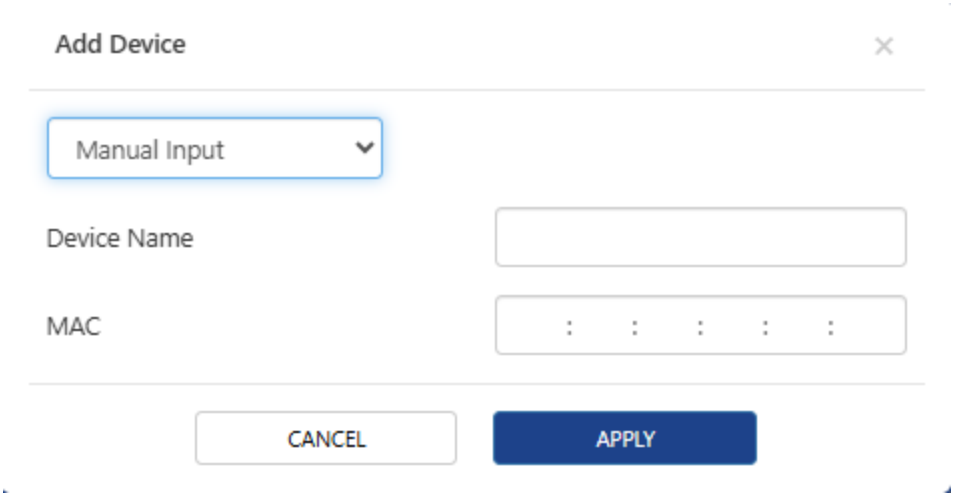
MAC address filtering applies to devices on the wireless/wired network. Devices on the filter list will be unable to access the Internet and will also be blocked from the router's management interface.
Note: This function may not work for terminals that use random MAC addresses.



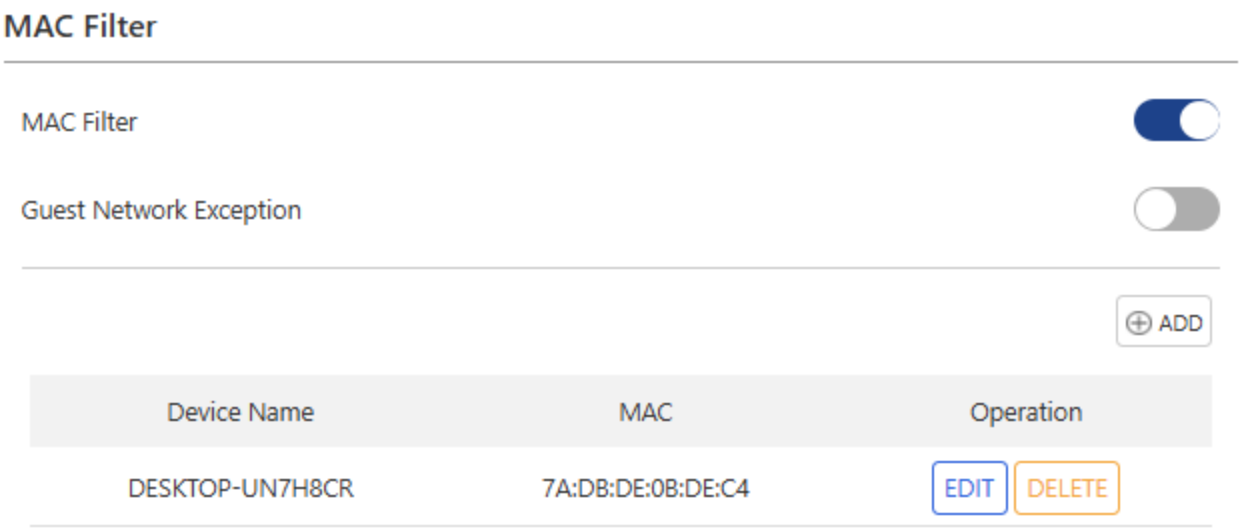
1. Click **Security** > **MAC Filter**.
2. Click **MAC Filter** to enable it.
3. If the **Guest Network Exception** is enabled, the devices in the guest Wi-Fi will not be blocked by this function.
4. Click **ADD** to add new rule.
   4.1 Select corresponding **Device Name** and **MAC address** from the list.



   4.2 Or manually input **Device Name** and **MAC address** to add device.



5. After adding the device, you can edit or delete the devices added.



This chapter contains the following sections:

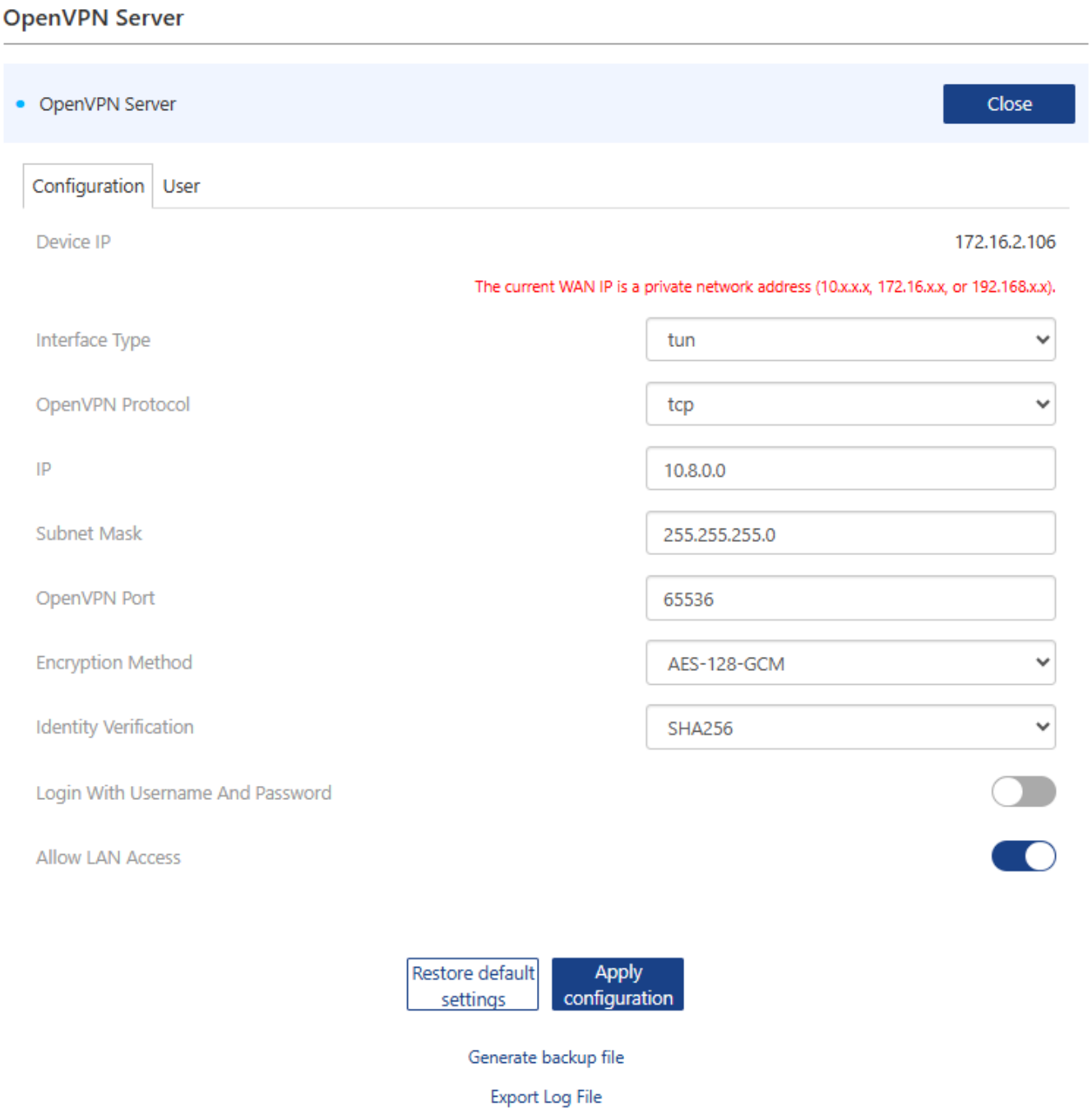
VPN Server and Client

VPN (Virtual Private Network) can encrypt your network connection to ensure the safe transfer of important data and avoid information stealing. Remote users (VPN clients) can safely connect VPN server.

VPN Server Configuration

Open VPN Server Configuration

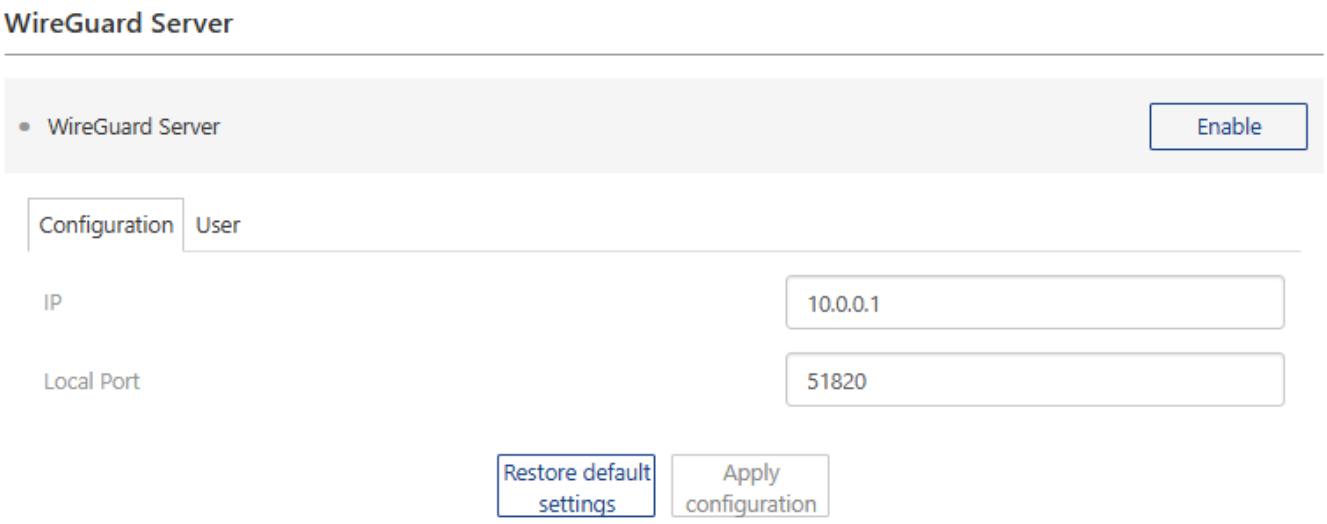
OpenVPN Server is used for remote devices to establish an OpenVPN connection to access your home network. If you use VPN function, you need to enable the OpenVPN server on a router and then install and run VPN client apps on remote devices.



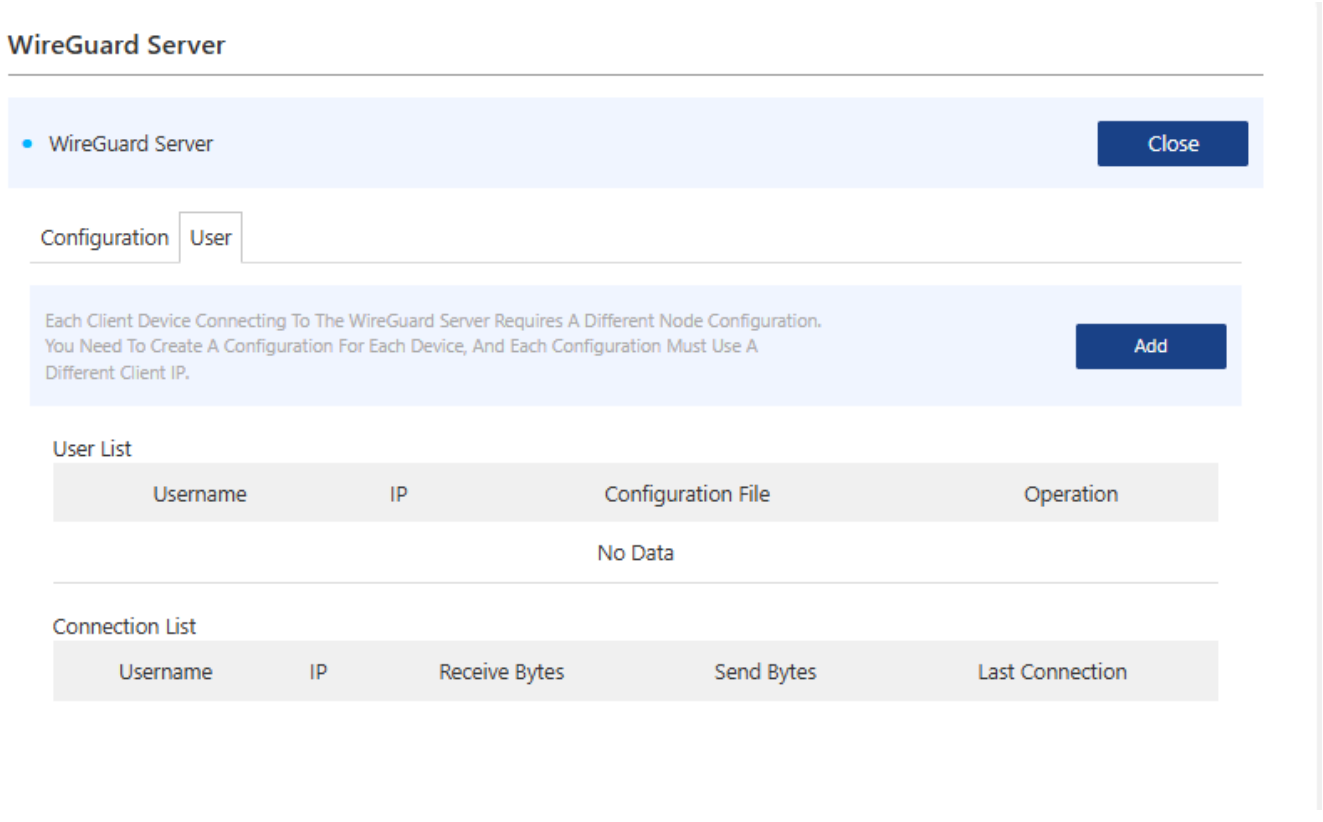
1. Access **More>VPN>OpenVPN Server**.
2. Open **OpenVPN Server**.
3. Select **Interface Type** and **OpenVPN Protocol**.
4. Input the **OpenVPN Port**, which should be from **1024-65535**.
5. In **IP** and **Subnet Mask**, enter the range of IP addresses the OpenVPN server can lease to devices.
6. Select **Encryption Method** and **Identity Verification** type.
7. Click **Apply configuration**.
8. Click **Generate backup file** to save it. VPN client device will establish VPN connection by using the file.

Note: Whenever the OpenVPN server settings are adjusted, the OpenVPN configuration file needs to be re-exported as **step 8**.

Use WireGuard VPN Server

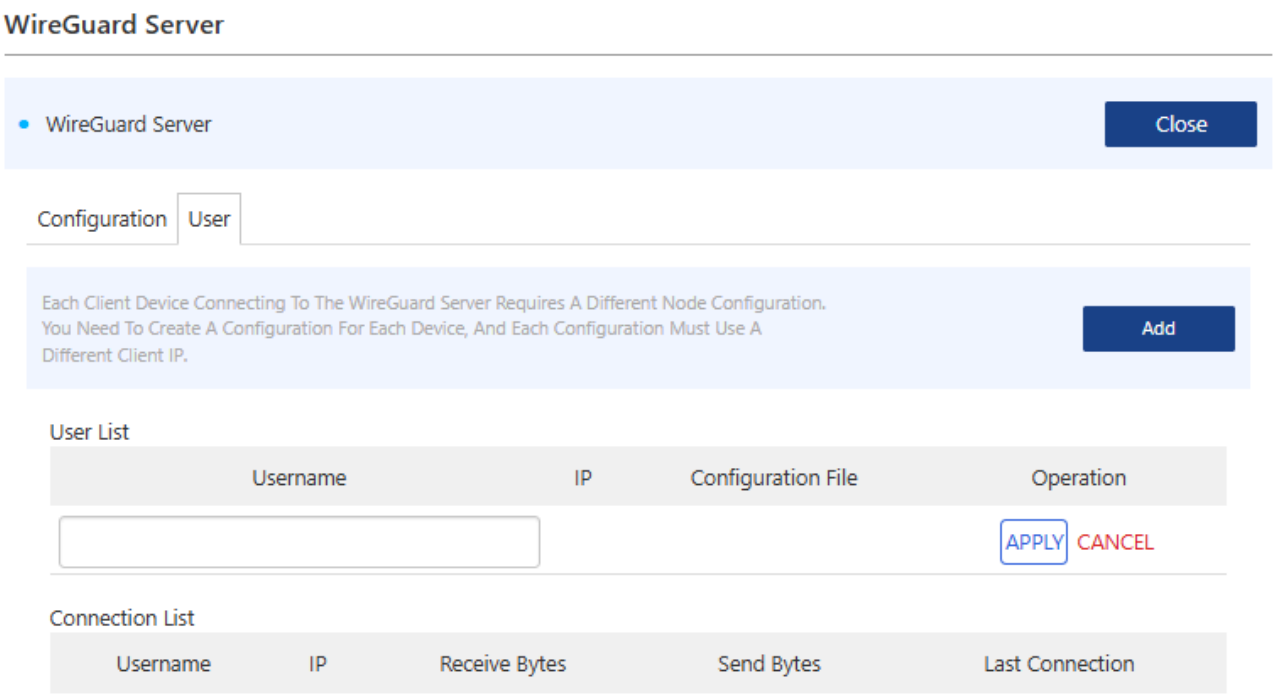


1. Review the preset WireGuard VPN settings. Do not change them unless necessary.
2. Click **Enable**.
3. **Downloading configuration files:** Each client that needs to connect to the WireGuard Server requires unique node configuration, so creating a configuration in unique client IP for each device as the following steps:

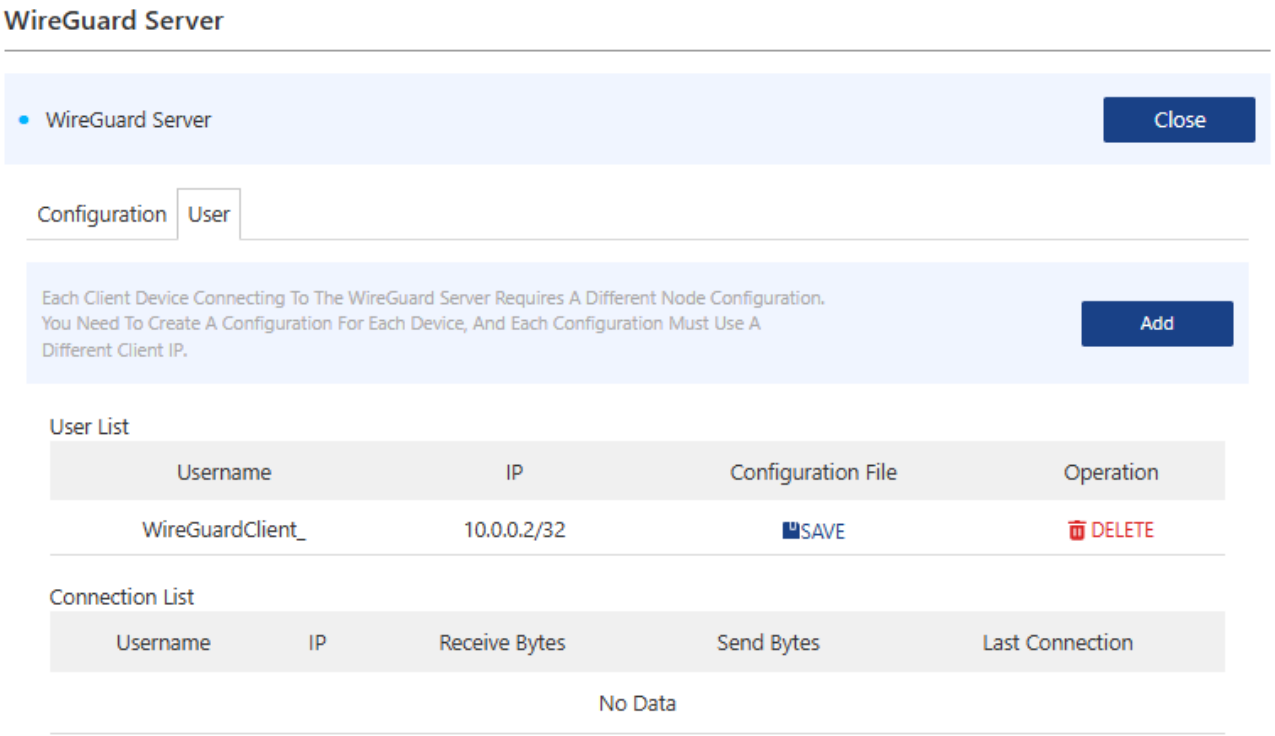


3.1 Click **User**.

3.2 Click **Add**, then input **Username** and click **APPLY**.



3.3 After adding successfully, click **SAVE** to obtain a **.conf** configuration file, then import this file into your WireGuard client.

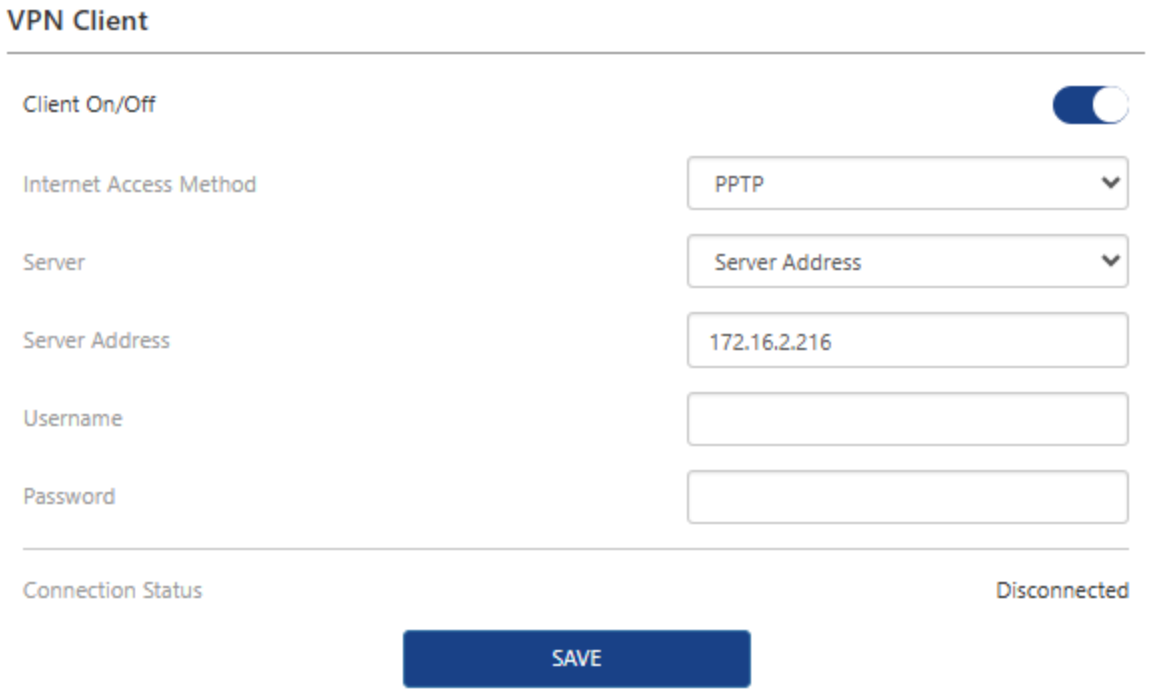


VPN Client Configuration

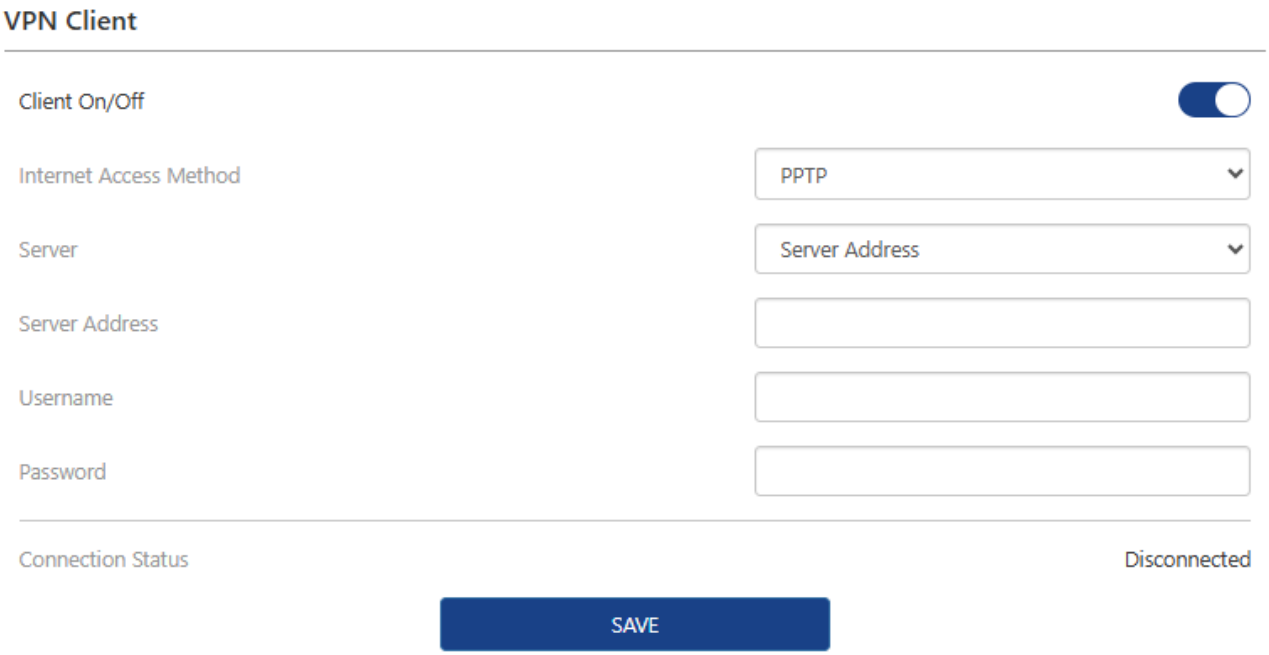
VPN client can establish VPN connection for devices in your home network to access remote a VPN server.

PPTP/L2TP VPN Client Configuration

VPN converts public networks (Internet, etc.) into private networks using encryption technology to offer greater security and privacy protection.



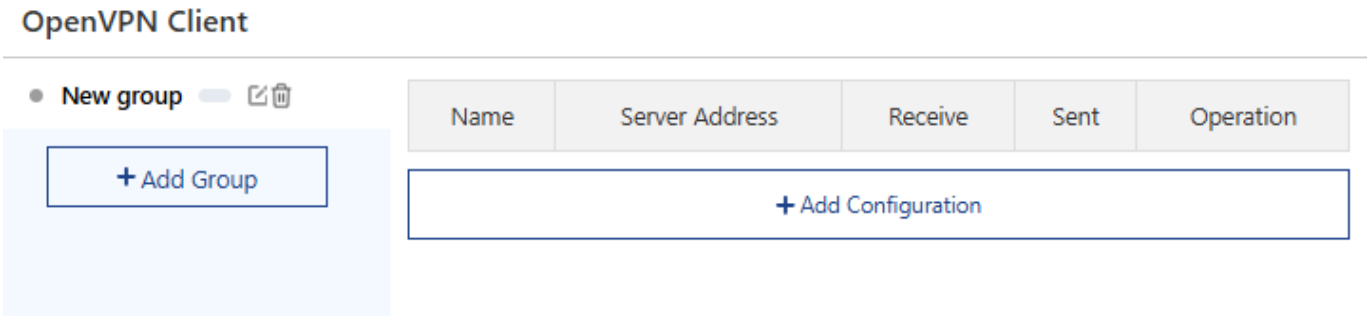
1. Access **More>VPN>VPN Client**.
2. Open **VPN Client**.
3. Select **Internet Access Method**.
4. Select server domain or server address in **Server**, then enter corresponding parameter in **Server Address**.



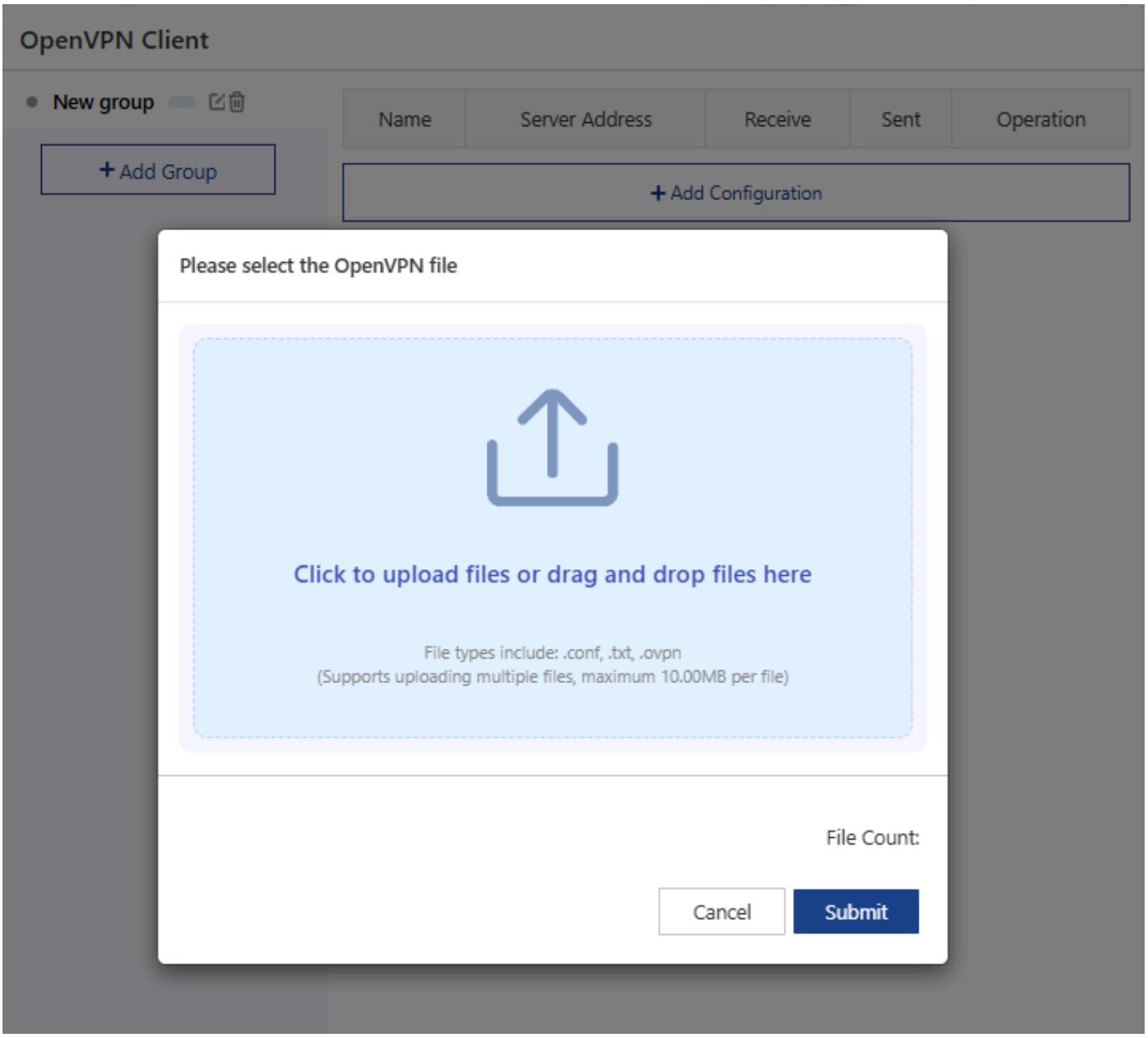
5. Click **SAVE** to finish the configuration.

OpenVPN Client Configuration

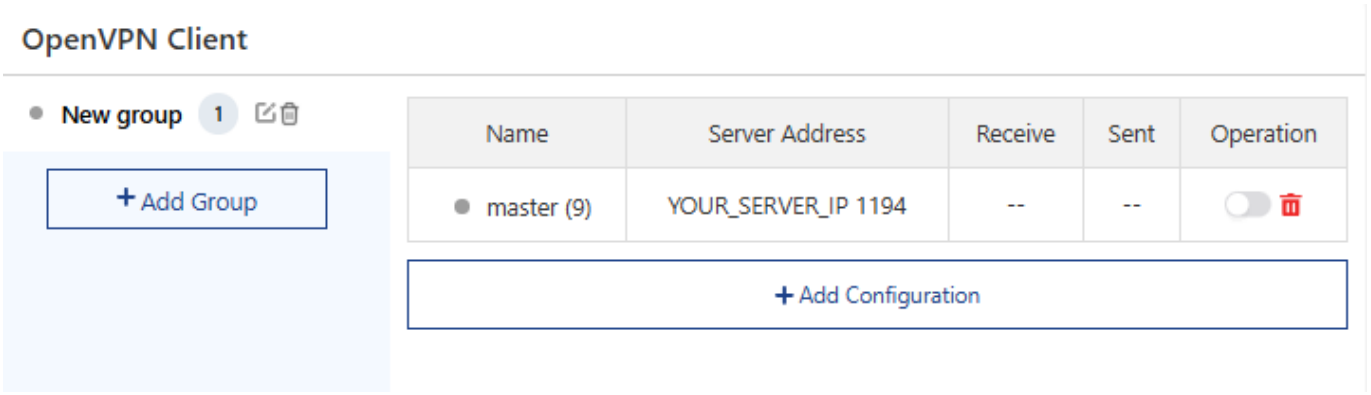
1. Access **More>VPN>OpenVPN Client**.
2. Click **Add Group** to add new group, then click **Add Configuration** to add new configuration.



3. Click to upload files or drag and drop files into the box.



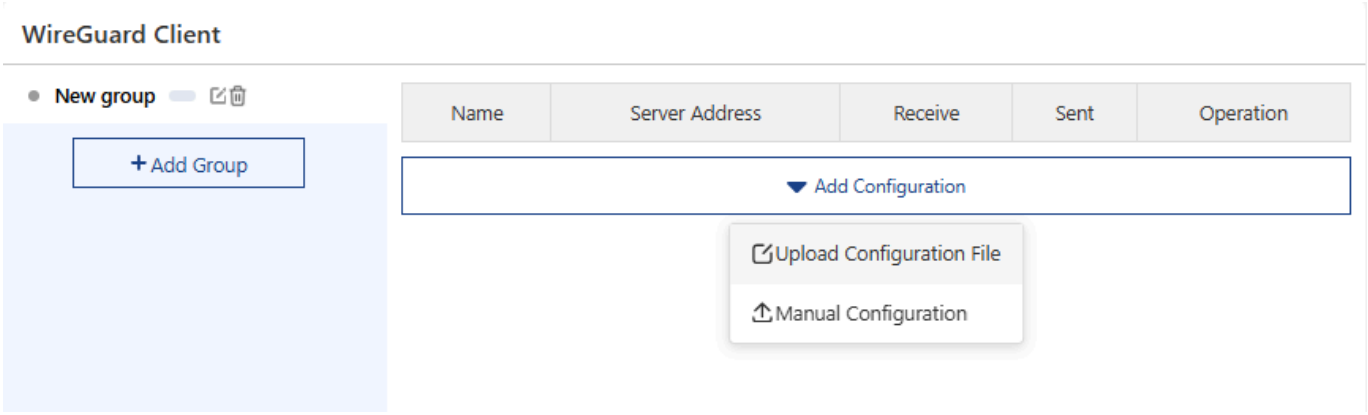
4. After a successful configuration, click the checkbox below the action bar to enable OpenVPN.



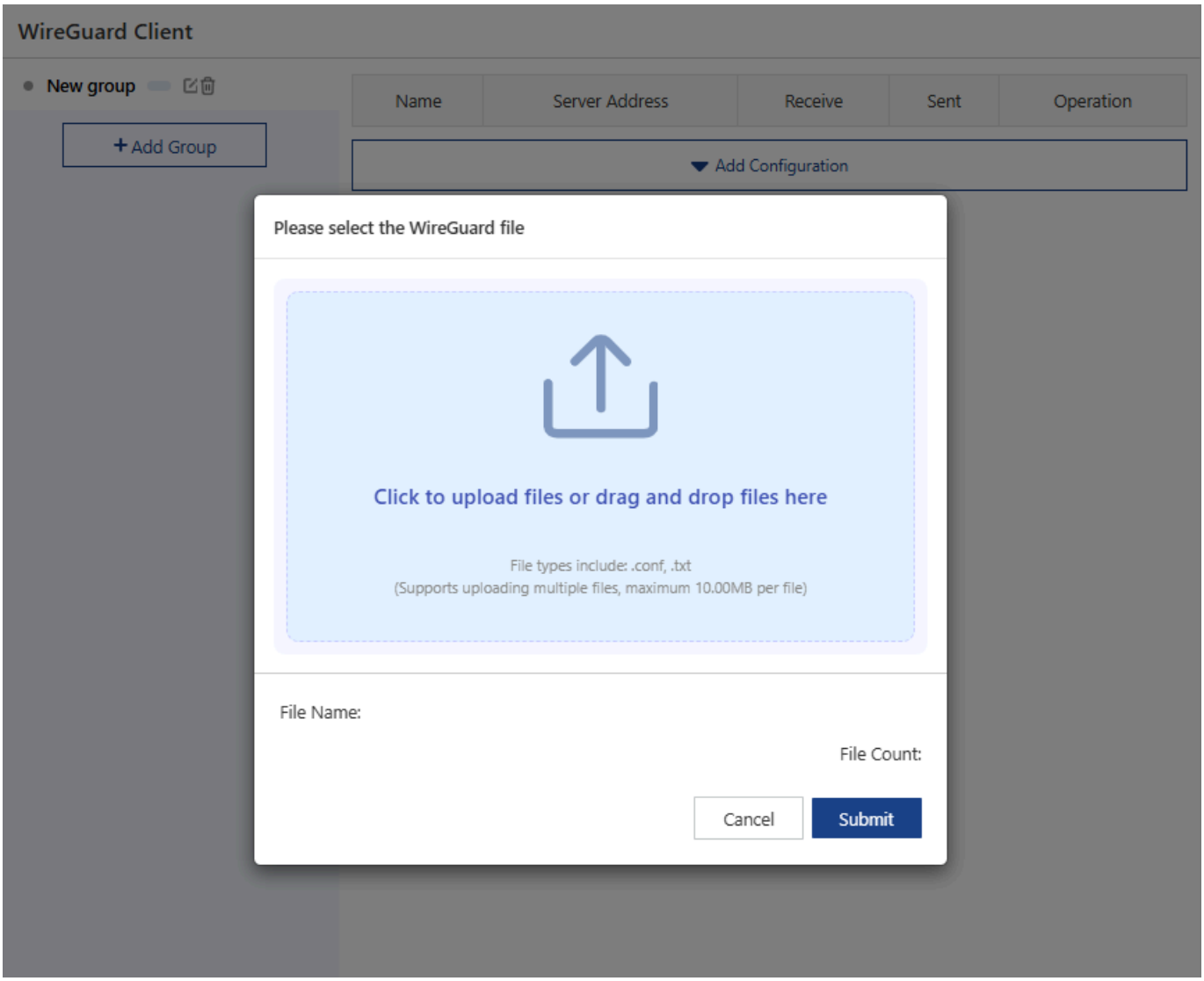
WireGuard VPN Client Configuration

1. Access **More>VPN>WireGuard VPN Client**.

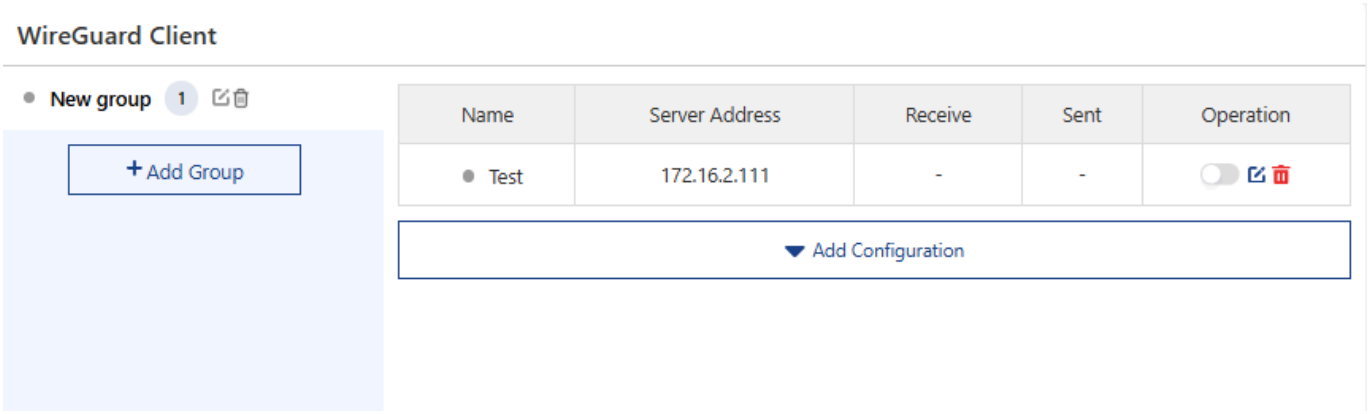
2. Click **Add Group** in **New group**, then click **Add Configuration**, select **Upload Configuration File** or **Manual Configuration**.



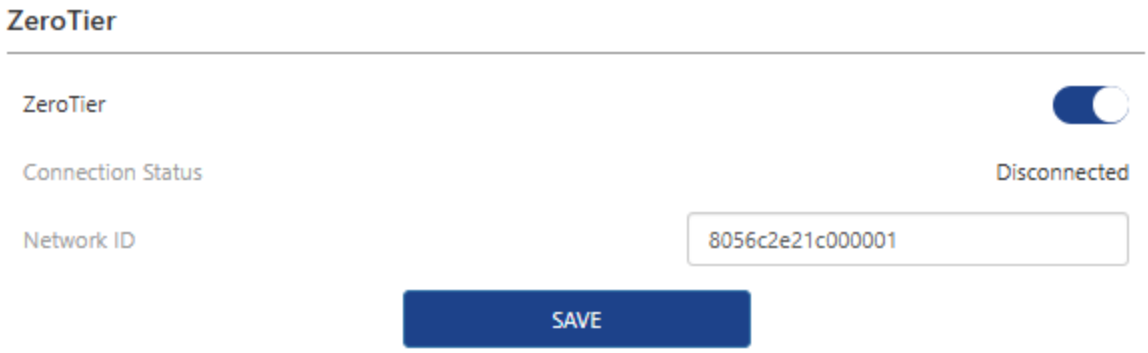
3. After selecting **Upload Configuration File**, click to upload files or drag and drop files into the box, then click **Submit**.



4. After a successful configuration, click the checkbox below the action bar to enable WireGuard.



ZeroTier Configuration



1. Access **More>VPN>ZeroTier**.
2. Open **ZeroTier**.
3. Enter **Network ID** obtained on the Zerotier manage page.
4. Click **SAVE** to finish the configuration.

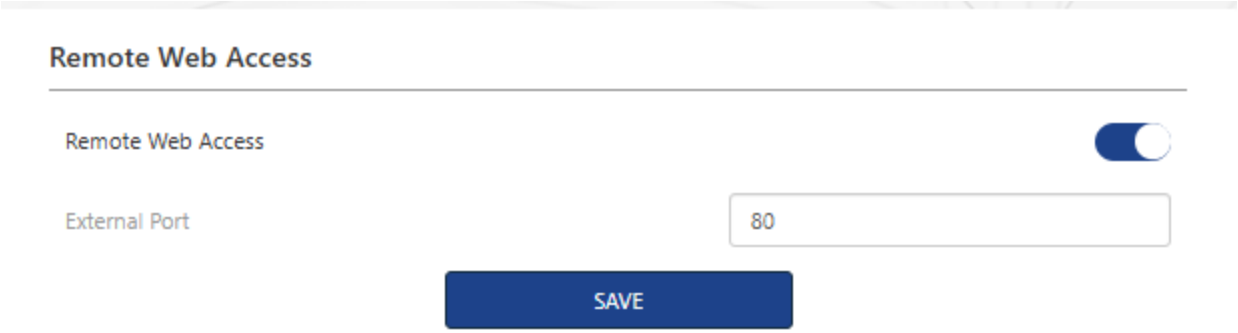
Chapter 10 Remote Access

This chapter introduces remote web access and cloud APP.

It contains the following sections:

Remote Web Access

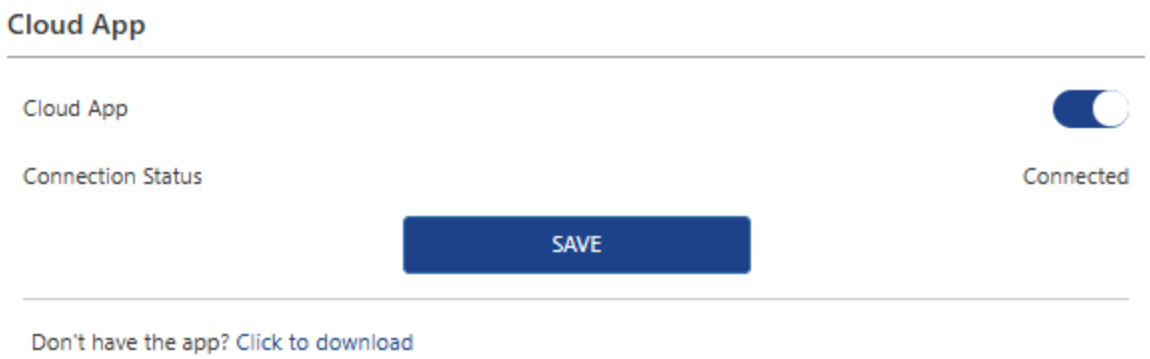
With this function, you can manage this router remotely via the Internet. Input **http://WAN IP: port number** for remotely accessing this device. We recommend you write this router's WAN port number down before using this function.



1. Access to **More**>**Remote Access**>**Remote Web Access**.
2. Turn on **Remote Web Access**.
3. Set **External Port**.
4. Click on **SAVE** to complete settings.

Cloud APP

With this function, you can control this router remotely from the cloud with the APP.



1. Access to **More**>**Remote Access**>**Cloud APP**.
2. Click on **Cloud APP** to enable the function.
3. Click on "**SAVE**" to complete settings.

NOTE:

If you didn't download APP, please click on **Click to download** to scan the pop-up QR code for downloading. You can also scan the QR code directly to obtain APP.

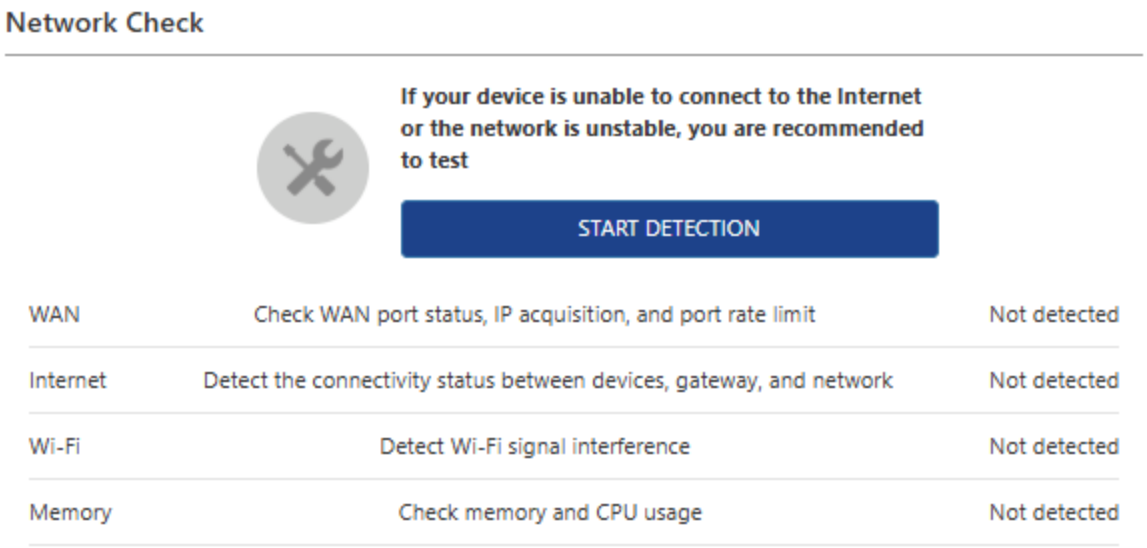
Chapter 11 NET Tools

This chapter introduces how to check network status, test network connection, and enable Wake-on-LAN function.

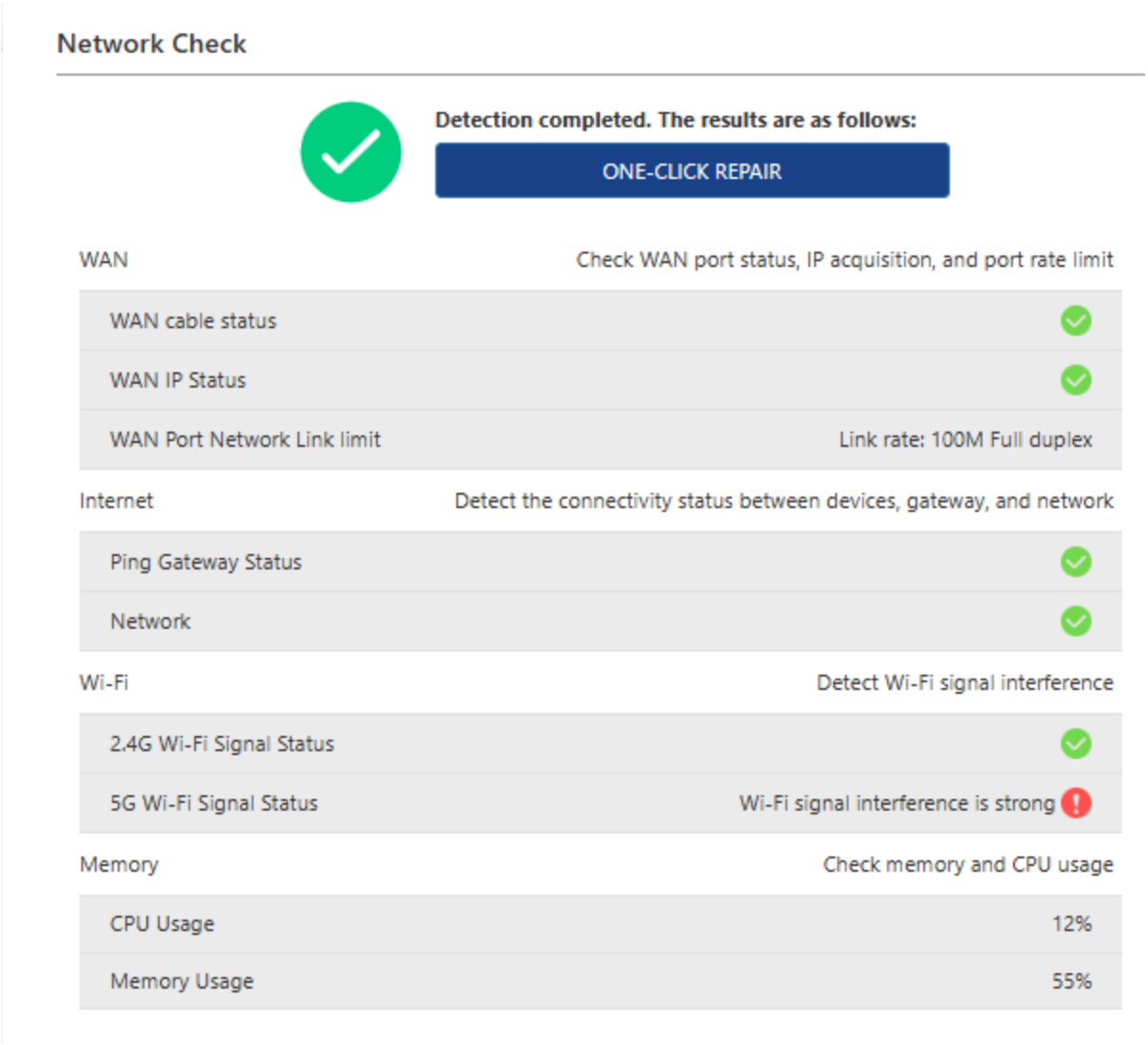
It contains the following sections:

Network Check

You can scan the entire network to analyse and optimize network status via network check.

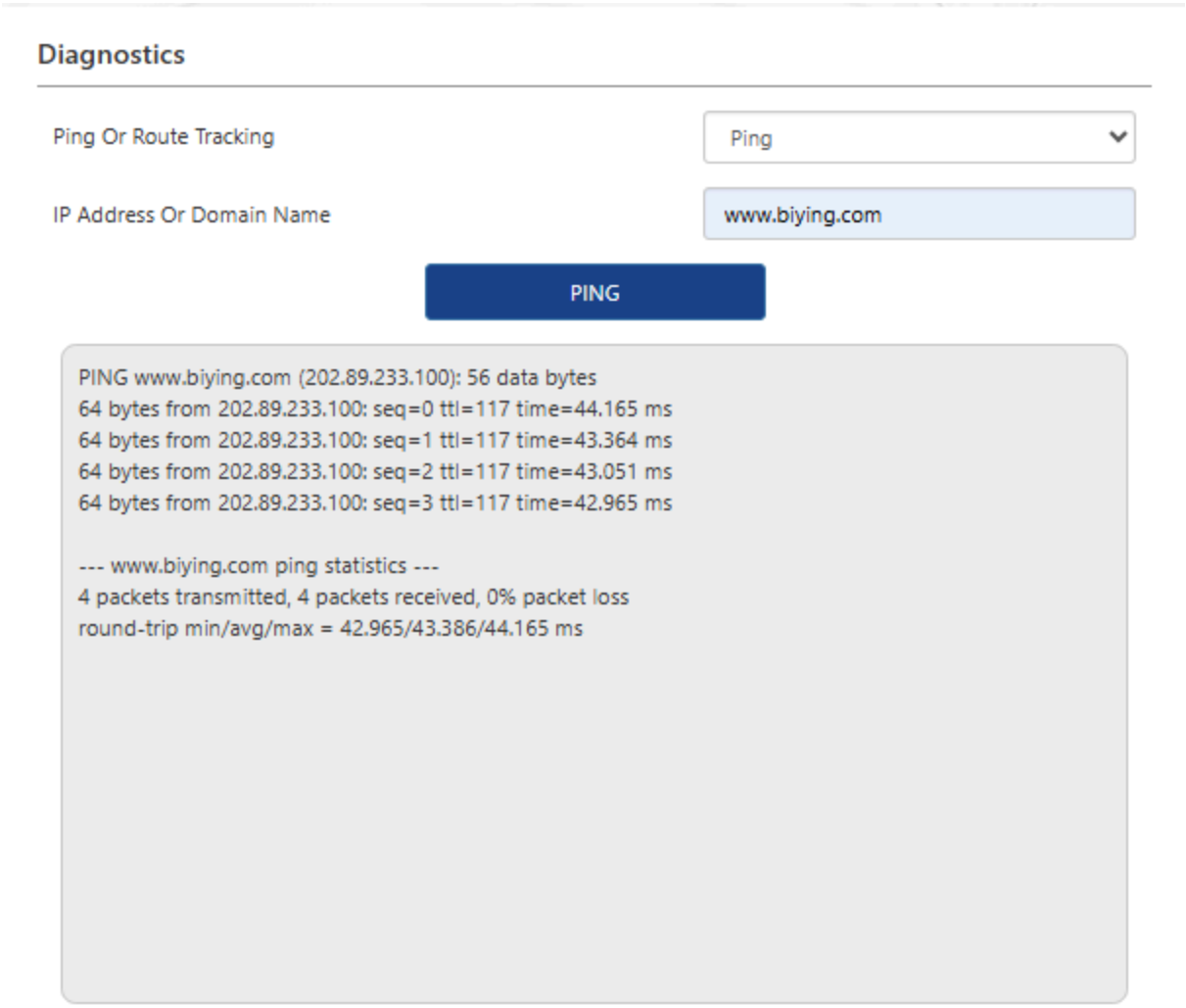


1. Access to **More**>**NET Tools**>**Network Check**.
2. Click on **START DETECTION**.



3. Click on "**ONE-CLICK REPAIR**" or manually optimize your network with prompts.

Diagnostics



1. Access to **More**>**NET Tools**>**Diagnostics**.
2. In the dropdown list **Ping Or Route Tracking**, choose **Ping** or **Traceroute**.

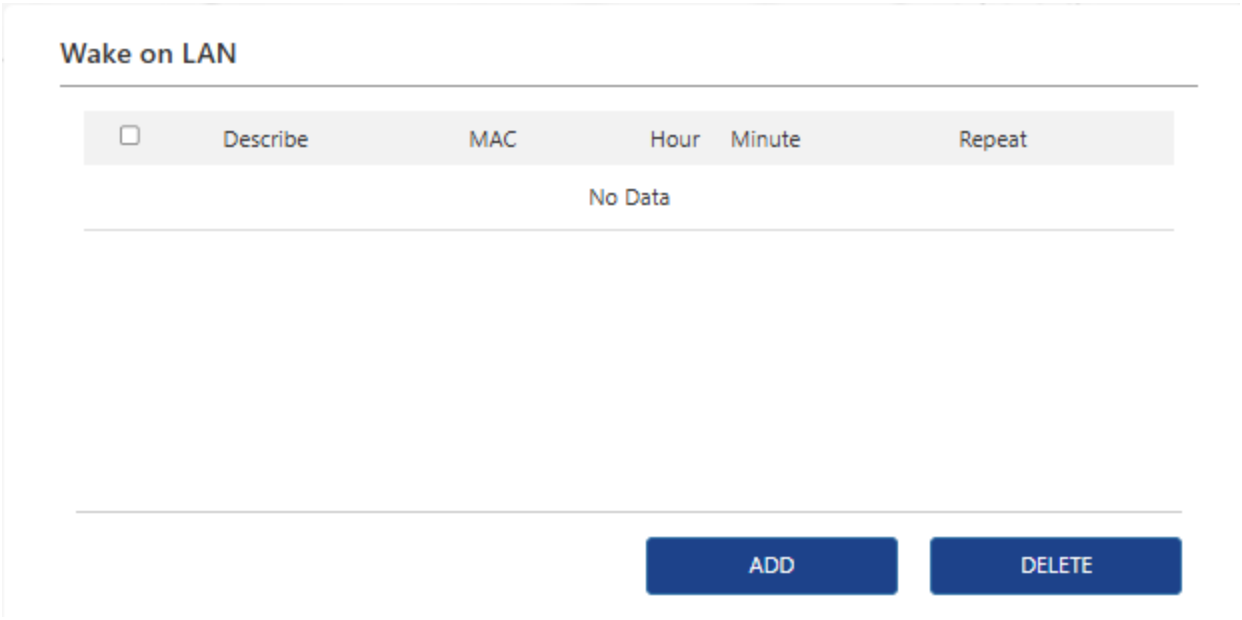
- **Ping** : used for checking the connection between the router and the target device whether normal or not.
- **Traceroute** : used for checking the node information between the router and the target device.

3. Input the **IP Address Or Dormain Name** that you want to test.
4. Click on **PING** or **Traceroute** button for testing.

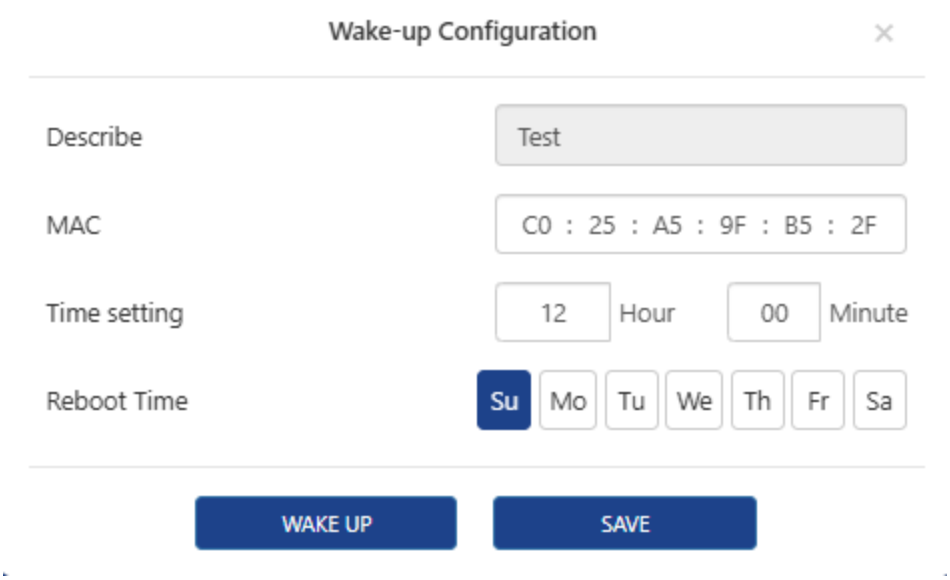
Wake-On-LAN

Wake-On-LAN (WOL) is a technology where the network interface card (NIC), along with other software and hardware, sends a specific data frame to the NIC that is in standby mode, enabling the computer to start up from a powered-off state.

1. Access to **More**>**NET Tools**>**Wake-On-LAN**.



2. Click on **Add** to start Wake-On-LAN setting.



3. Add the **Discribe** of the configuration.
4. Input the **Mac Address** of the device that you want to remotely wake up.
5. Set **Time setting** and **Reboot Time**.
6. Click on **SAVE**, complete the configuration.

Chapter 12 System Setting

This chapter introduces firmware update, password change, system log, system time setting, indicator setting, backup and restore, and how to restart router.

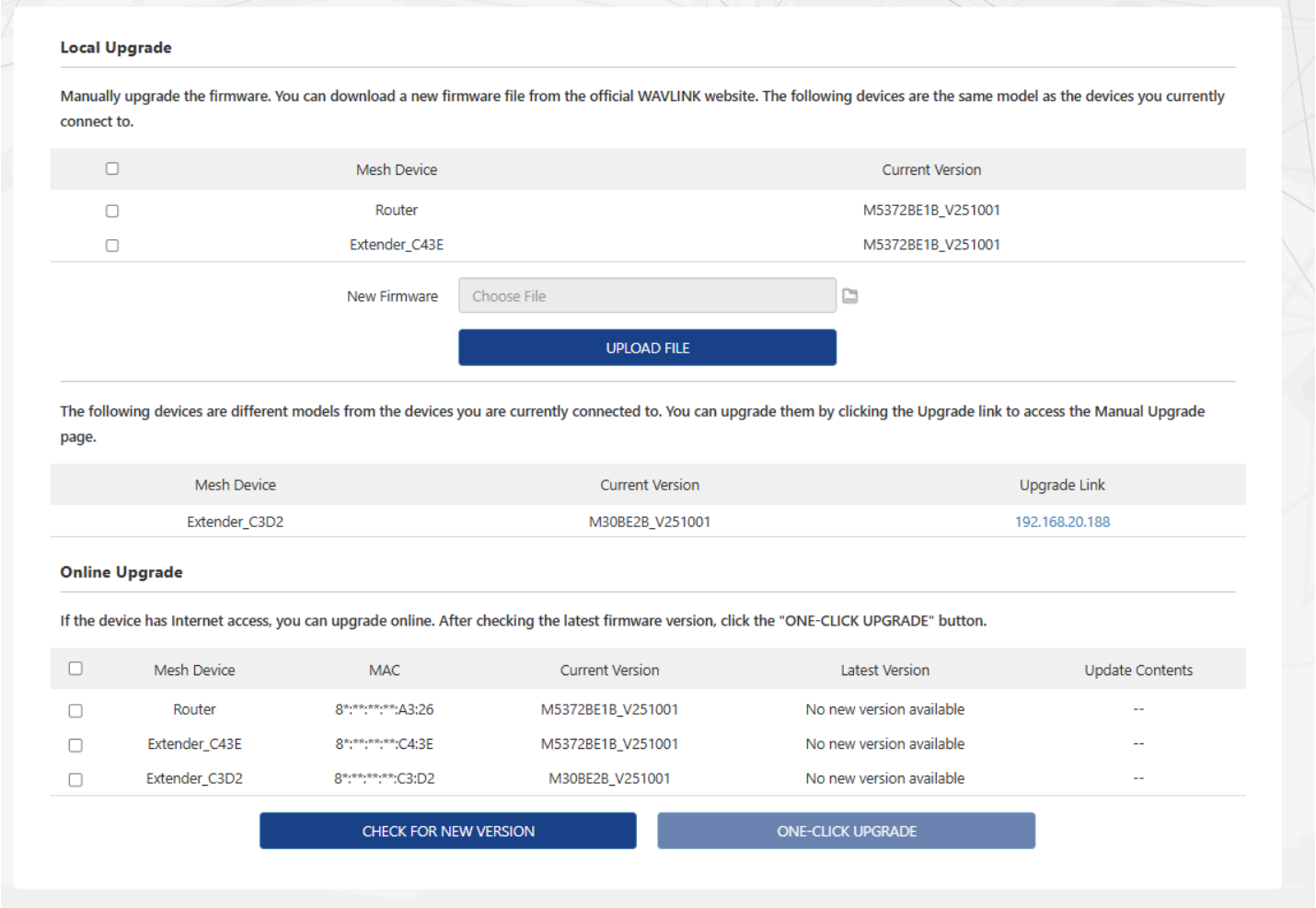
It contains the following sections:

Firmware Upgrade

Regular firmware upgrade can obtain the newest functions and security patches, improving the performance and stability of the router, and fixing possible bugs and security risks.

WAVLINK provides two ways to upgrade your firmware: local upgrade and online upgrade. You can choose one of them to update your firmware.

Access to **More**>**System**>**Firmware Upgrade**.



Local Upgrade

1. Access to WAVLINK official website: **www.wavlink.com**. Download the corresponding upgraded software of the current hardware version.
2. Select the device that needs to be updated.
3. Click on **Choose File** or **File** icon, and select the firmware file that needs to be uploaded. Click on **UPLOAD FILE**.
4. Wait for the completion of updating.

NOTE:

- After updating, the router will automatically reboot to apply new firmware. The process will take few minutes to complete, please wait patiently.
- During updating, the router can't be powered off in case the router's firmware gets damaged.

Online Upgrade

1. Choose the device that needs to be updated.

2. Click on **CHECK FOR NEW VERSION** to view the upgradable version to update. Or directly use **ONE-CLICK UPGRADE**.
3. Wait for the update completion.

NOTE:

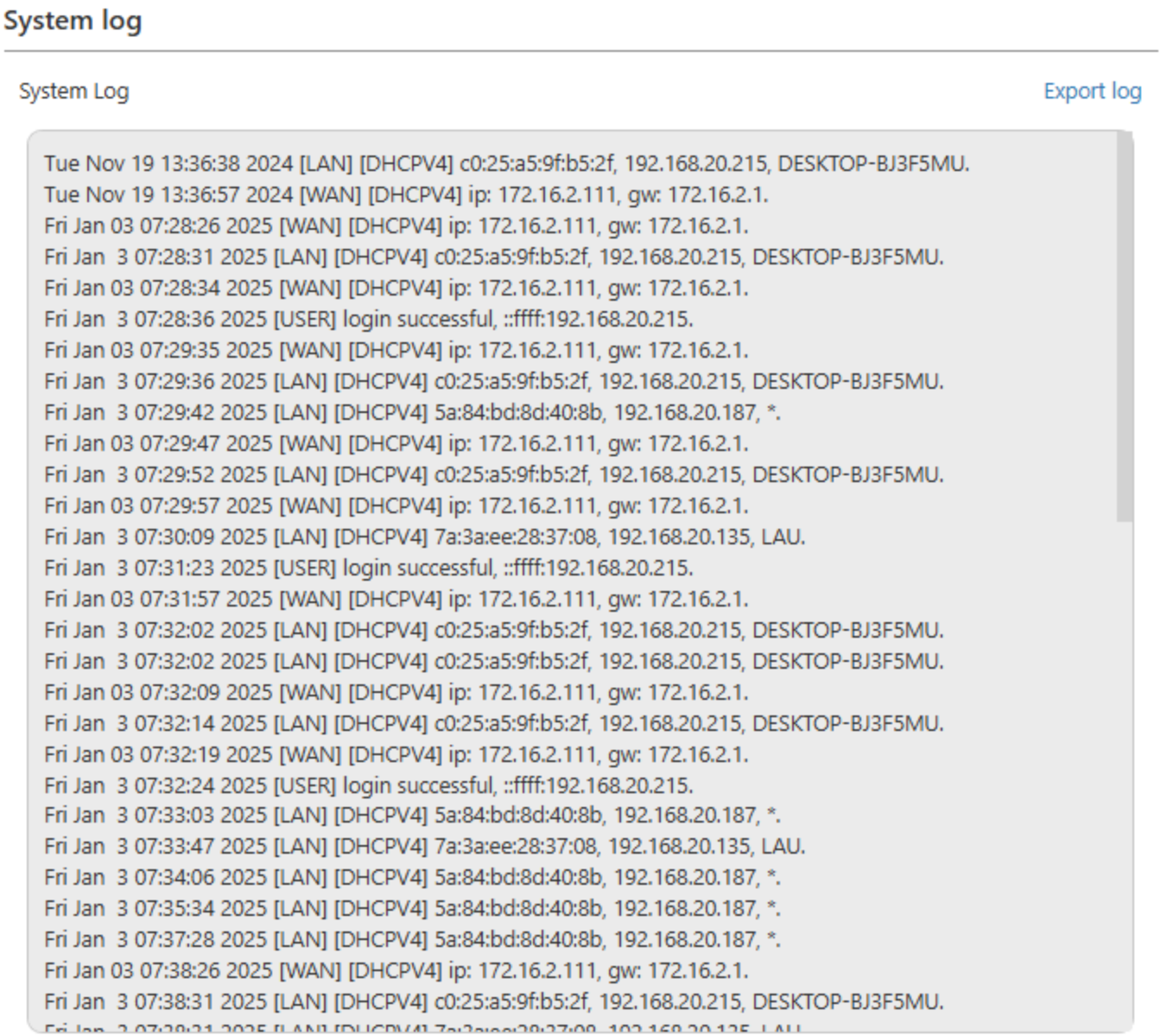
- After updating, the router will automatically reboot to apply new firmware. The process will take few minutes to complete, please wait patiently.
- During updating, the router can't be powered off in case the firmware gets damaged.
- When CHECK FOR NEW VERSION, if the prompts show that the firmware is the newest version, there is no need to upgrade the router.

Change Password

1. Access to **More**>**System**>**Change Password**.
2. Input the current one on the **Old Password** text field.
3. Input the new one on the **New Passowrd** text field.
4. Input the new one on the **Confirm New Password** text field, ensuring the inputed password is the same as the new password.
5. Click on **SAVE** to complete password changing.

System Log

When it comes to malfunction, reserve the system log and send it to technical support for trouble shooting.



1. Access to **More**>**System**>**System Log**.
2. Click on **Export log** to save the log to the computer.

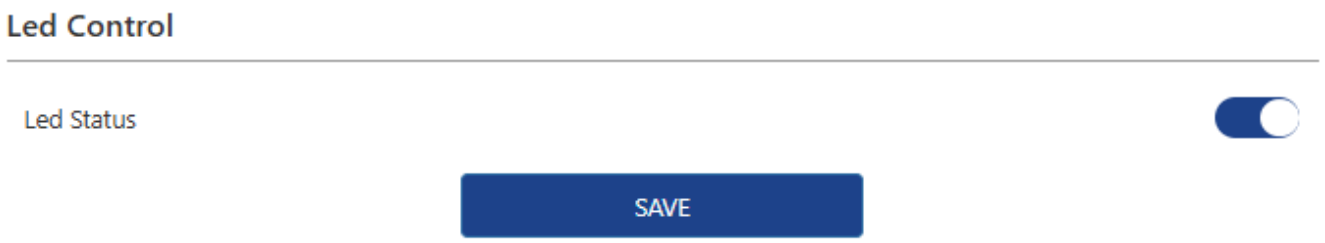
Time Zone

The system time is the time displayed when the router is running. The system time you set here is used for other time-based features, like Parental Control.

1. Access to **More**>**System**>**Time Zone**.
2. Choose the right time zone in the dropdwon list of **Time Zone**.
3. Turn on/off **Daylight Saving Time(DST)**.
4. Click on **SAVE** to complete the configuration.

Led Control

The router's indicators are used for indicating the device's status or running. By setting the indicator, you can know the device's working status more clearly, find and ban machine problems in time.



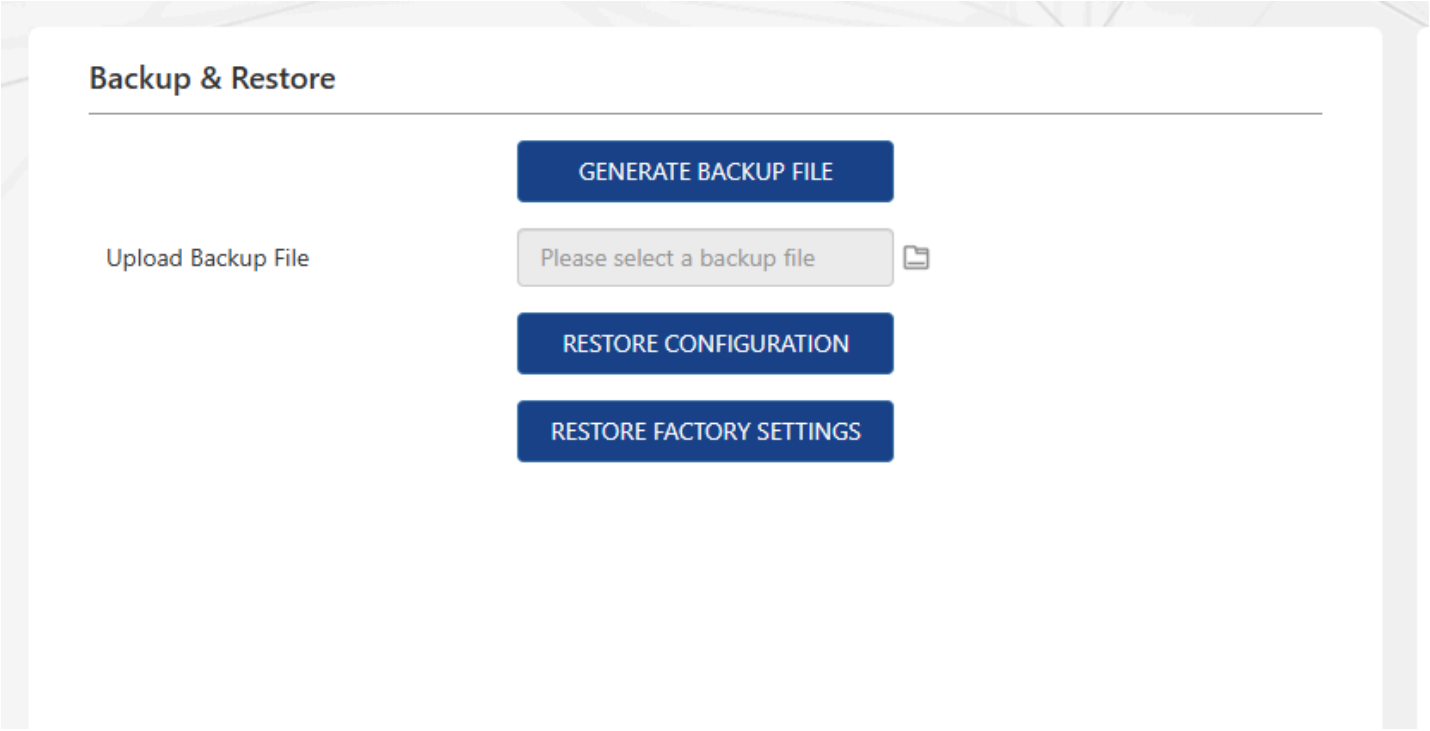
1. Access to **More**>**System**>**Led Control**.
2. Turn on/off **LED Status**.
3. Click on **SAVE** to complete the configuration.

Backup & Restore

Please configure settings as a configuration file stored in the router. You can backup this configuration file into your computer for future use, and restore the router to the

previous setting with this backup file. Furthermore, if necessary, you can delete the current system setting and reset the router to the default factory settings.

Access to **More**>**System**>**Backup & Restore**.



Backup the current configuration of the router

Click on **GENERATE BACKUP FILE** to store the copy of current setting on the local computer, and name the file **backupsettings**.

Restore the router's configuration:

1. Click on **UPLOAD**, and choose the backup configuration file that was stored on the computer.
2. Click on **RESTORE CONFIGURATION**, and wait a few minutes to restore the configuration and restart the router.

Reset the router to the default factory settings

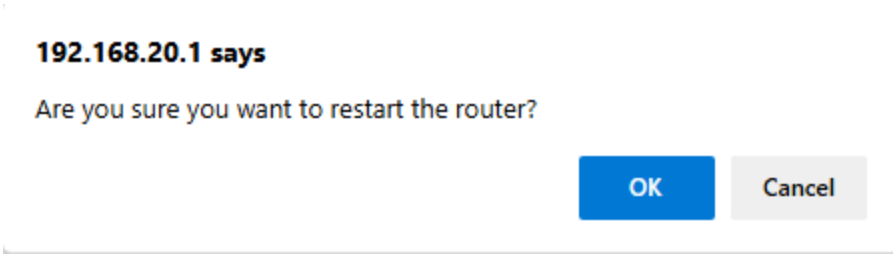
1. Click on **RESTORE FACTORY SETTINGS** to reset the router.
2. Wait a few minutes for the reset and reboot.

Scheduled Reboot

When your router has a network malfunction, you can try to use the reboot function to solve the problem. Sometimes, the router may experience software errors or memory overflow issues, leading to network instability. Under these circumstances, you can reboot the router to solve this problem and get the network back up.

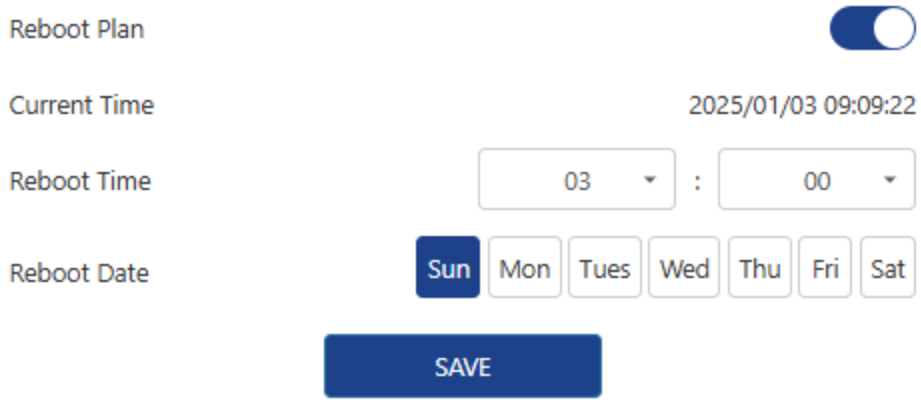
After modifying some settings of this router, you need to reboot the router to make the settings valid. Using the reboot function can quickly update the router's settings and make it valid.

1. Access to **More**>**System**>**Scheduled Reboot**.
2. Click on **ROUTER REBOOT**.



3. After clicking, a window will pop up, in which you will be asked whether to restart the router or not. If you want to reboot the router, choose **OK**. If not, choose **Cancel**.

Set Scheduled Reboot Plan



The automatic reboot function can clear unnecessary data in the router and automatically choose the best wireless channel.

Before turning on Reboot Plan, please ensure the system time is right. If the router's designated reboot time is less than 60 minutes, some unnecessary reboots won't be executed.

1.Access to **More**>**System**>**Scheduled Reboot**.

2.Turn on **Reboot Plan**.

3.Choose the router's **Reboot Time**, and the **Reboot Date** to decide on reboot frequency.

4.Click on **SAVE** to complete the configuration.

Chapter 13 Logoff

Logoff

If you need to log out, please access to **More** on the management page, then click on **Logout**.

Chapter 14 FAQ

This chapter contains the following sections :

FAQ

Q1. Why doesn't the login page appear after entering http://wavlogin.link ?

- Please make sure your computer is set to obtain an IP address automatically.
- Verify if http://wavlogin.link is correctly entered in the web browser.
- Use another web browser and try it again.
- Reboot your router and try it again.

Q2. What can I do if I cannot access the Internet?

- Restart your modem(wait 5 minutes). Disconnect extra Ethernet ports from the modem.
- Test by connecting a computer directly to the modem. If issues persist, contact your ISP.
- For cable modems, clone the MAC address of the device which could get Internet from the modem via Ethernet cable in **More>Network>Internet>MAC Clone>Custom MAC**, then reboot modem and router.

Q3. How can I restore the router to its factory default settings?

- While the router is powered on, press and hold the Reset button for more than **6** seconds.

Q4. What can I do if I forget my administration management password?

- Refer to **FAQ:Q3** to reset the router.

Q5.What can I do if I forget my wireless network password?

- Connect the router to the PC via Ethernet cable. Log in the router's web management page at http://wavlogin.link and go to **Wireless**, you can find your Wi-Fi password here.

- Refer to **FAQ > Q3** to reset the router.

Q6. How to deploy the router to get the best Wi-Fi signal?

- Keep the router in the most central spot in your home and away from anything that might block its signal.

GNU General Public License Notice

This product includes software codes developed by the third parties. These software codes are subject to either the GNU General Public Licence(GPL), Version 2, June 1991 or the GNU Lesser General Public License(LGPL), Version 2.1, February 1999. You can copy, distribute, and/or modify in accordance with the terms and conditions of GPL or LGPL. The source code should be complete, if you want us to provide any additional source code files under GNU General Public License (GPL), please contact us in these matters. We are committed to meeting the requirements of the GNU General Public License (GPL). You are welcome to contact our local office to get the corresponding sofware and licenses. Please inform us your contact details (full address) and the product code. We will send you a software package with the sofware and license for free. The respective programs are distributed WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY Or FITNESS FOR A PARTICULAR PURPOSE.Please refer to the GNU General Public License Website for further information.

http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html

http://www.gnu.org/licenses/gpl.html

After-sale Service

Need help?

We're here for you!

Online support: wavlink.com
Available Mon-Fri 8:30 am-5:30pm (UTC+8)

support@wavlink.com
Available Mon-Fri 8:30 am-5:30pm (UTC+8)

+1 8889730883
Mon-Fri 9:00 am - 6:00 pm (UTC-5)

www.wavlink.com

Thank you for purchasing WAVLINK product!

Chapter 15
Safety and Emission Statement

CE Mark Warning

This is a Class B product. In a domestic environment,
this product may cause radio interference,
in which case the user may be required to take adequate measures.

NOTE:
(1)The manufacturer is not responsible for any radio or TV interference caused by unaut horized modifications to this equipment. (2)To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

Declaration of Conformity Hereby, Winstars Technology Limited,
declares that the radio equipment type HALO
Nexus is in compliance with Directive 2014/53/EU.
The full text of the EU declaration of conformity is available at the following Internet add ress:https://www.wavlink.com/en_us/ce.html

FCC Statement This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

— Reorient or relocate the receiving antenna.

— Increase the separation between the equipment and receiver.

— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

— Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

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

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.