

WAVLINK



see the world

User Manual

AX3000 Wi-Fi 6 VPN Travel Router

Model: AERIAL BayTrek

@WavlinkOfficial

@WavlinkTechSupport

Table of contents:

- About This Guide
 - Conventions
 - More Info
 - Speed/Coverage Disclaimer
 - Safety Instructions
 - Copyright Statement
 - WEEE Directive & Product Disposal
- Chapter 1 Product Basic Info
 - Overview
 - Basic Info
 - LED Indication
- Chapter 2 Hardware Connection
 - Hardware Connection
- Chapter 3 Initial Setup
 - Setup Guide
- Chapter 4 Network Management
 - Network Setting
 - LAN Setting
 - Setting IPv6
 - Setting Static IP
 - Setting Dynamic DNS
 - Mode Selection
 - Router Mode
 - AP Mode
 - Repeater Mode
 - Wireless Repeater
 - Setting Multi-WAN
 - Failover Mode Setup
 - Load Balancing Mode Setup
 - URL Filter
- Chapter 5 Managing Wireless Network
 - Wireless
 - Configuring Wireless Network
 - Advanced Settings
 - Schedule (Wireless Timer Switch)

- Guest Wi-Fi
- Parental Wi-Fi
- Chapter 6 Net Guardian
 - Secure DNS
 - AdGuard Home
 - Initial Settings
- Chapter 7 NAT Forwarding
 - UPnP Settings
 - Port Forwarding
 - DMZ Host
 - Hardware NAT
- Chapter 8 Network Security
 - Firewall
- Chapter 9 VPN Server and Client
 - VPN Server and Client
 - VPN Server Configuration
 - Open VPN Server Configuration
 - Use WireGuard VPN Server
 - VPN Client Configuration
 - PPTP/L2TP VPN Client Configuration
 - OpenVPN Client Configuration
 - WireGuard Client Configuration
 - ZeroTier Configuration
- Chapter 10 USB Setting
 - Storage Server
 - USB Tethering
- Chapter 11 Remote Access
 - Remote Web Access
 - Cloud APP
- Chapter 12 NET Tools
 - Diagnostics
 - Wake On LAN
- Chapter 13 System Setting
 - Firmware Update
 - Local Upgrade
 - Online Upgrade
 - Change Password

- System Log
- Time Zone
- Led Control
- Restore Factory Settings
- Scheduled Reboot
- Mode Switch
- Router Reboot
- Chapter 14 Developer Options
 - SSH
 - LUCI
- Chapter 15 Logout
 - Logout
- Chapter 16 FAQ
 - FAQ
 - Q1. Why doesn't the login page appear after entering <http://wavlogin.link> ?
 - Q2. What should I do if I can't access the Internet?
 - Q3. How can I restore the router to its factory default settings?
 - Q4. What can I do if I forget my Administration Management password?
 - Q5. What can I do if I forget my wireless network password?
 - Q6. How to deploy the router to get the best Wi-Fi signal?
 - GNU General Public License Notice
 - Aftersale Service
- Chapter 17 After Sale Service_CE_FCC
 - Safety and Emission Statement

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
<u>Underlined</u>	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 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

No part of this publication may be reproduced in any form by any means without the prior written permission.

Other trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

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 equipment, or returned to the supplier for disposal.

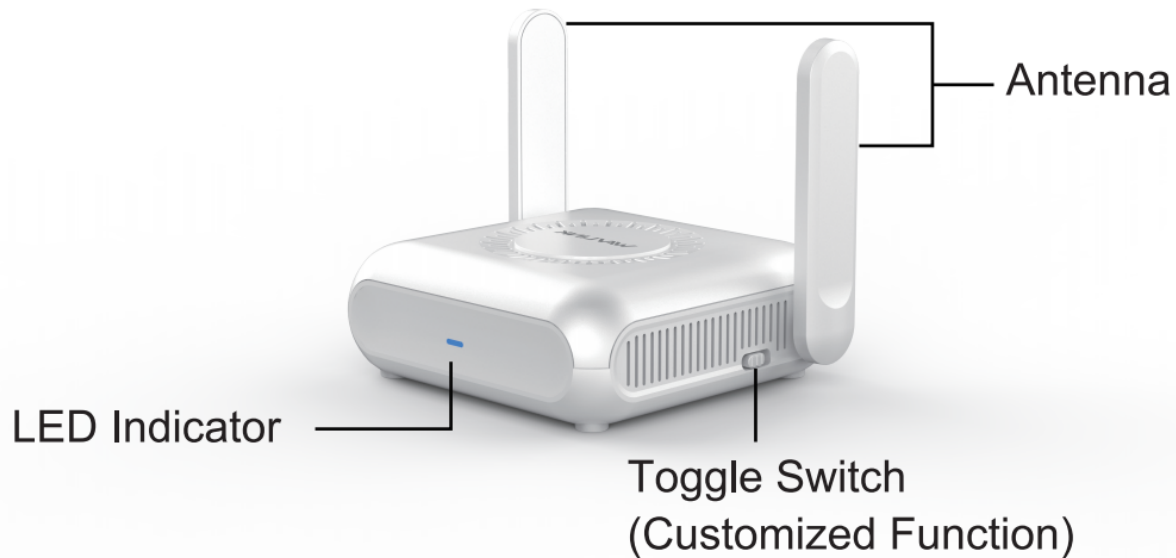


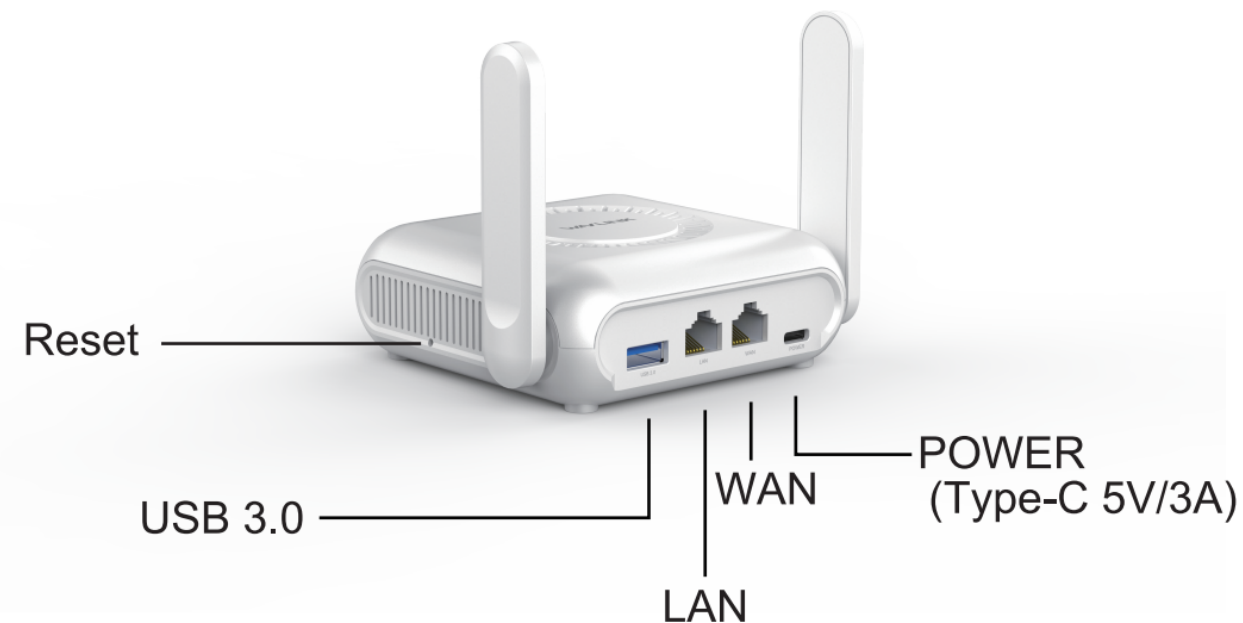
Chapter 1 Product Basic Info

This chapter contains the following sections:

- [Overview](#)
- [Basic Info](#)
- [LED Indication](#)

Overview





Basic Info

2.4G SSID: **WAVLINK_XXXX**

5G SSID: **WAVLINK_XXXX**

Default IP: **192.168.20.1**

Login: **<http://wavlogin.link>**

LED Indication

Mode	LED Status	Description
Router Mode	Solid	Connected to the network
	Flashing	Disconnected from the network

Toggle Switch Button: A customizable switch button. No specified function by default.

Reset Button: Press and hold it for **6s** to reset the device.

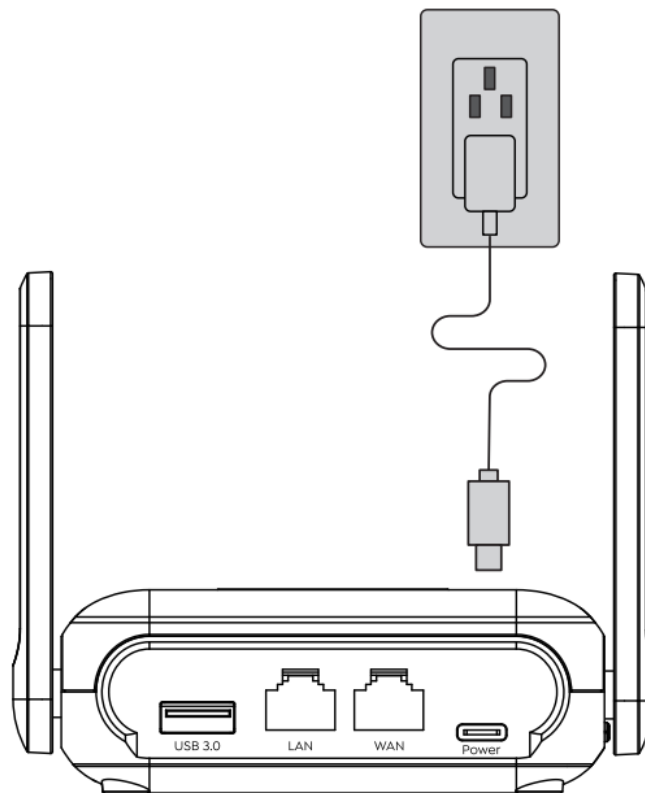
Chapter 2 Hardware Connection

This chapter contains the following sections:

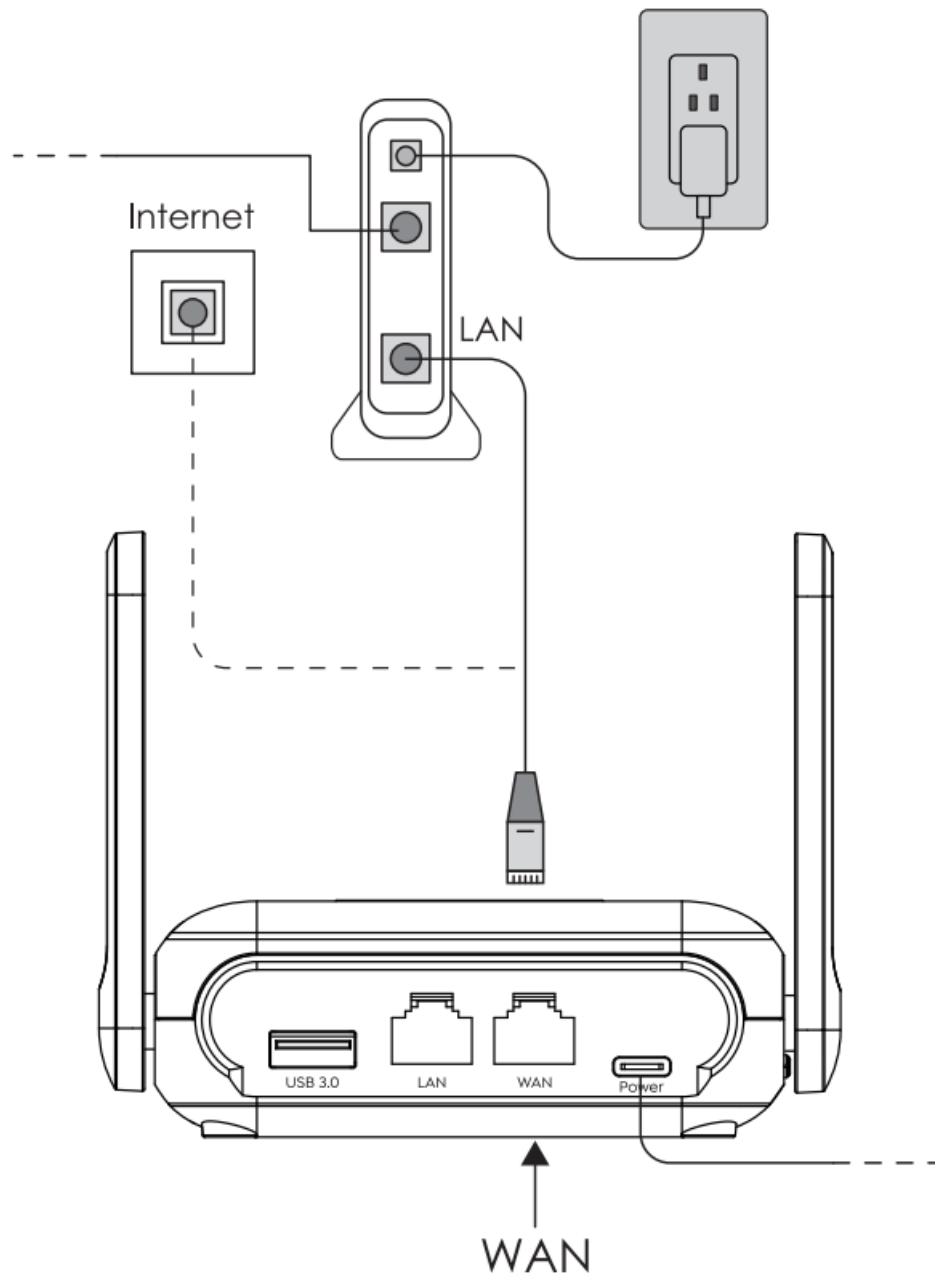
- [Hardware Connection](#)

Hardware Connection

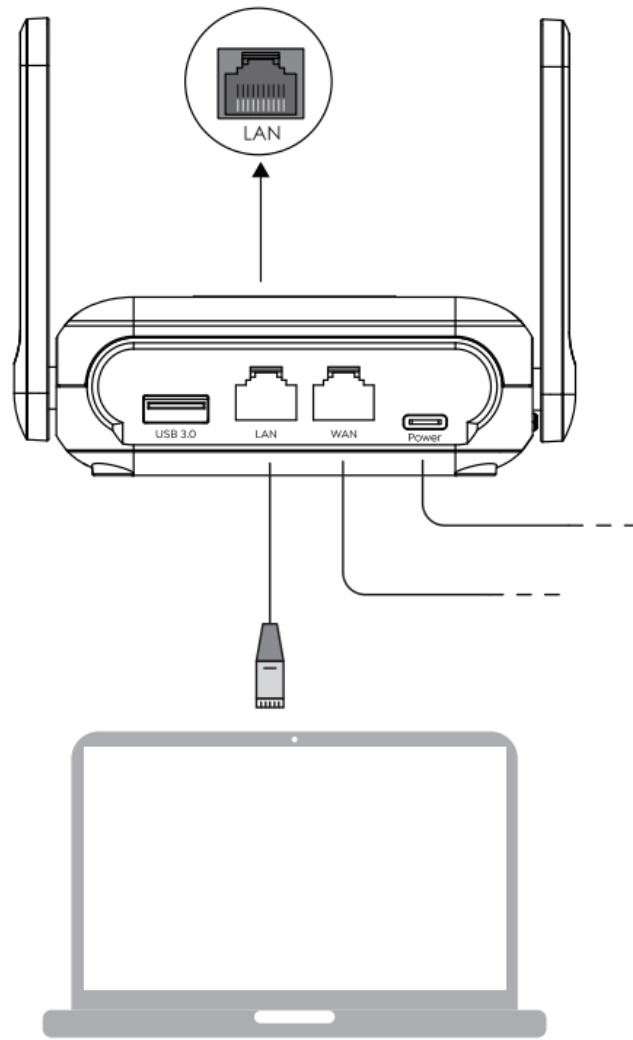
1. Connect the USB-C power adapter to the Router, then wait for the router to finish booting up.



2. Connect the WAN port to DSL/Cable Modem or the Ethernet wall outlet.



3. Connect to the device via Wireless or Wired connection (1) Wireless Connection Connect to the router's WiFi SSID(on the bottom of the router). (2) Wired Connection Disconnect or Turn Off WiFi on your computer to prevent conflicts in network processing order, then connect it to router's LAN port via an Ethernet cable.



4. Open a browser and enter 192.168.20.1 or <http://wavlogin.link> in the address bar, click **Start Configuration**.

Welcome to WAVLINK

[Start Configuration](#)



[Click here to download the
WavRouter APP](#)

Chapter 3 Initial Setup

This chapter contains the following sections:

- [Setup Guide](#)

Setup Guide

1. Select the **Country/Region** and **Time Zone**, then set the **WiFi name** and **password**, and you can keep the device management password same as the wireless password, after the above configuration, click **Save**.

The screenshot shows a web-based configuration interface for a WavRouter. It is divided into three main sections: 'Country code/time zone', 'Wi-Fi settings', and 'Device management password'. In the 'Country code/time zone' section, there are two dropdown menus: 'Country/Region' and 'Time Zone'. The 'Wi-Fi settings' section includes a 'Dual-band convergence' toggle switch (which is turned on), a 'Wi-Fi name' text field containing 'WAVLINK_5858', and a 'Wi-Fi Password' text field with a placeholder 'Between 8~63 characters' and a strength indicator bar below it. The 'Device management password' section has a toggle switch labeled 'Same as the wireless password' (which is turned on). At the bottom, there is a blue 'Save' button, which is highlighted with a red rounded rectangle.

Country code/time zone

Country/Region

Time Zone

Wi-Fi settings

Dual-band convergence ☒

Wi-Fi name

Same name for 2.4G and 5G Wi-Fi

Wi-Fi Password

Device management password

Same as the wireless password ☒


Save

2. Wait for the process bar to be 100%, then you can connect to the WiFi using your new WiFi password. Scan the QR Code using your phone to download WavRouter APP.

The setting is successful, please wait for the setting to be completed, and then use the new Wi-Fi password to connect to the Wi-Fi

Wi-Fi name : WAVLINK_5858

Wi-Fi Password : *****




Scan the QR code to download the WavRouter APP for easier router management

1%,Please wait...

Refresh

3. Customize network settings according to your needs.


see the world


Home

Wireless

Network

Terminal

More Settings



2.4G

2.4G SSID: WAVLINK_5858

5G

5G SSID: WAVLINK_5858

2.4G

2.4G Guest SSID: Disabled

5G

5G Guest SSID: Disabled

Ethernet

Disconnected

WAN mode

DHCP

Gateway

0.0.0.0

IP Address

0.0.0.0

Subnet Mask

0.0.0.0

DNS1

0.0.0.0

DNS2

0.0.0.0

Settings >

Repeater

Disconnected

Settings >

Multi-WAN

Settings >

Multi-WAN mode

Failure recovery

In use

WAN

Use Time

4m 28s

VPN

Settings >

VPN server

Off

VPN Client

Off

USB Status

Settings >

USB Status

Disconnected

Client List

Guest List

Connection Type	Device Information	IP Address	MAC Address
PC-	20190307WVDD	192.168.20.171	80:3F:5D:0D:20:B4

Chapter 4 Network Management

This chapter contains the following sections :

- [Network Setting](#)
- [LAN Setting](#)
- [Setting IPv6](#)
- [Setting Static IP](#)
- [Setting Dynamic DNS](#)
- [Mode Selection](#)
- [Wireless Repeater](#)
- [Setting Multi-WAN](#)
- [URL Filter](#)

Network Setting

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

- 1 . Access **Network** setting or **More>Network>Internet**.
- 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.

Internet

WAN Type

DHCP



Advanced

Custom MTU



MAC Clone



Custom DNS



Internet VLAN ID



SAVE

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.

Internet

WAN Type

PPPoE



Username

Password

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 specified 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.

Internet

WAN Type

Static IP



IP

Subnet Mask

Gateway

DNS1

DNS2

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 occasion 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**.

Internet

WAN Type

PPPoE Dual Access



Username

Password

Second WAN

DHCP



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**.

Internet

WAN Type

PPTP Dual Access



Username

Password

Server URL

Second WAN

DHCP



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**.

Internet

WAN Type

L2TP Dual Access



Username

Password

Server URL

Second WAN

DHCP



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

Advanced

Custom MTU



MAC Clone



Custom DNS



Internet VLAN ID



SAVE

- **Custom MTU(MaximumTransmission 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 appear as the original device, 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.

4 . 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**.

LAN

DHCP



IP

192.168.20.1

Subnet Mask

255.255.255.0

Start IP

192.168.20.100

End IP

192.168.20.249

Lease Time

1 Day



DNS Rebinding Protection

ON



SAVE

- **IP**: 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.
- **Start IP and End IP**: 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 IP and End IP.
- **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.
- **DNS Rebinding Protection**: Discard response messages from upstream domain name servers with private IP address ranges.

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

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.

IPv6

IPv6

IPv6 WAN Settings

Method Of Obtaining

Automatic Detection

IPv6 LAN Settings

IPv6 Address Assignment

Automatic Allocation

IPv6 Prefix

fd00:7c28:2a96::

/48

IPv6

fd00:7c28:2a96::/48

SAVE

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

IPv6

IPv6 WAN Settings

Method of Obtaining

Automatic Detection

IPv6

IPv6 WAN Settings

Method of Obtaining

IPv4+IPv6 PPPoE



IPv6 WAN Settings

Method of Obtaining

Static IPv6 Address

IPv6 Address

IPv6 Gateway

Preferred DNS

Alternative DNS

- 3.1 Select corresponding **Method Of Obtaining** from the list, then input corresponding information:
 - Automatic Detection**: 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 Address**: Manually input **IPv6 Address**, **IPv6 Gateway**, **Preferred DNS** and **Alternative DNS**.

4 . IPv6 LAN Settings.

IPv6 LAN Settings

IPv6 Address Assignment

Automatic Allocation

IPv6 Address Prefix

Automatic Allocation

SLAAC

IPv6 Address

fd00:7c28:aac0::/48

- 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.

Setting Static IP

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.

⊕ Add New Rule

IP Address	MAC Address	Operate
<input type="text" value="192.168.20.249"/>	<input type="text" value="4C:77:CB:DA:24:97"/>	<div><div>Bind</div><div>Cancel</div></div>

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

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.

Dynamic DNS

Dynamic DNS



Connection Status

Disconnected

Service Provider

oray.com



Username

user_ddns

Password



Host Name

www.domain.com

SAVE

- 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 inputted.

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**, **AP Mode** or **Repeater Mode**.

Router Mode

- In router mode, the router converts Wi-Fi signals to wireless Internet access for devices by connecting to the network operator's wired network, and provides wired Internet access for devices through a wired port.

Mode Selection

Mode Selection

Router Mode

WAN Type

DHCP

Internet VLAN ID



ID Number

0

Cloud App



WAN Status

Connected

SAVE

- **WAN Type: DHCP, PPPoE or Static IP**, inputting the corresponding parameters is required for PPPoE or Static IP.
- **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.

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.

Mode Selection

Mode Selection

AP Mode

Smart DHCP Service



WAN Status

Connected

SAVE

- **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.

Mode Selection

Repeater Mode

Connection Type

Bridge(Recommend)

Next

- 1) Select **Bridge(Recommend)** or **WISP** from the **Connection Type** list, then click **NEXT** to rescan the Wi-Fi signal.

Mode Selection

☒ Select Wi-Fi

☐ Manual Input



Scanning ...

RESCAN

- 2) **Select** the wireless signal to be relayed.
- 3) If the network to be added is not found, click **RESCAN** to rediscover the network. Or select **Manual Input** to set it up.










Mode Selection

☒ Select Wi-Fi

☐ Manual Input

Please select the wireless network to be relayed

New Wi-Fi networks

	17F_model_test_586A5G	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>
	zh_h_debug_5G	<input type="radio"/>
	WAVLINK_AP_5G	<input type="radio"/>
	WAVLINK-Mesh_761F	<input type="radio"/>
	tpwifi-z-555	<input type="radio"/>
	GL-SFT1200-88b-5G	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>

RESCAN

- 4) Enter the password of the superior wireless network, and click **SAVE** to complete the setup.

Mode Selection

Superior wireless network information

Superior Network Name

17F_model_test_586A5G

Password



SAVE

Wireless Repeater

By enabling repeater mode, you can provide a new way of connecting for Multi-WAN mode. In repeater mode, you can use wireless relay to provide network access for this device and its clients. If the Wi-Fi you choose to relay is a public Wi-Fi and requires

authentication, please do the following in advance or after successful relaying: 1) Disable DNS rebinding protection in LAN settings within network settings. 2) In network guardian, turn off Secure DNS AdGuard Home.

Repeater Mode

Repeater Mode



SCAN



Auto Reconnect



Auto Switch



Saved Wi-Fi networks

	WAVLINK-Mesh_8E3E	
---	-------------------	---

1. Access to **More > Network > Wireless Repeater**.
2. Click once to enable **Repeater Mode**, then click **SCAN** to scan the Wi-Fi signal.

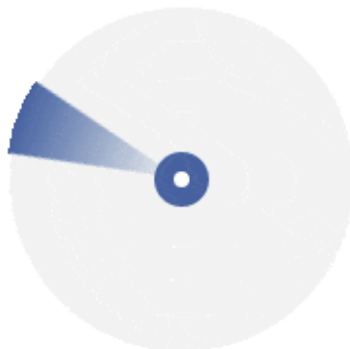
Repeater Mode

Repeater Mode



☒ **Select Wi-Fi**

☐ **Manual Input**



Scanning

RESCAN

3. **Select** the wireless signal to be relayed.
4. If the network to be added is not found, click **RESCAN** to rediscover the network. Or select **Manual Input** to set it up.

Repeater Mode

Repeater Mode












☒ **Select Wi-Fi**

☐ **Manual Input**

Please select the wireless network to be relayed

New Wi-Fi networks

	17F_model_test_586A5G	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>
	zh_h_debug_5G	<input type="radio"/>
	WAVLINK_AP_5G	<input type="radio"/>
	WAVLINK-Mesh_761F	<input type="radio"/>
	tpwifi-z-555	<input type="radio"/>
	GL-SFT1200-88b-5G	<input type="radio"/>
	WAVLINK_Touch	<input type="radio"/>

RESCAN

5. Enter the password of the superior wireless network, and click **SAVE** to complete the setup.

Repeater Mode

Repeater Mode



Superior wireless network information

Superior Network Name

17F_model_test_586A5G

Password

A password input field with a blue eye icon on the right side to toggle visibility.

SAVE

Auto Reconnect



Auto Switch



Setting Multi-WAN

Multi-WAN is an advanced networking technology that combines wired, wireless, and USB tethering methods to deliver exceptional network stability and performance.

Multi-WAN

Ethernet	SETTINGS
Repeater	SETTINGS
Hotpot Sharing	SETTINGS
Mode	Failover

Interface Priority

1	Ethernet	⬆️⬆️
2	Repeater	⬆️⬆️
3	Hotpot Sharing	⬆️⬆️

SAVE

1. Navigate to **More > Network > Multi-WAN**.
2. Click the **SETTINGS** button next to the mode (Ethernet/Repeater/Hotpot Sharing) for which you want to configure interface detection.

Interface Detection Mode

×

Enable Monitoring

☒

Detection Command

ping

▼

Detection Interval (Seconds)

3

▼

Become Faulty

Failure

3

times

Become Available

Success

4

times

Detection IP

8.8.8.8

208.67.222.222

208.67.220.220

1.1.1.1

CANCEL

APPLY

3. In the pop-up **Interface Detection Mode** panel:

- Ensure “Enable Monitoring” is toggled **ON**.
- Select a “Detection Command” (e.g., keep default **ping**).
- Choose a “Detection Interval (Seconds)” (e.g., keep default **3**).
- Set “Become Faulty” (failure threshold, e.g., **3** times) and “Become Available” (success threshold, e.g., **4** times).
- Enter “Detection IP” addresses (e.g., **8.8.8.8**, **208.67.222.222**, etc.).

4. After confirming all settings, click **APPLY** to save the interface detection configuration. If you want to discard changes, click **CANCEL**.

Failover Mode Setup

In failover mode, you can set interface priorities to determine the source priority for internet access. If a high-priority interface fails, it switches to a lower-priority interface.

Meanwhile, the system scans in the background and switches back to the highest priority interface once the issue is resolved.

Mode

Failover

Interface Priority

1

Ethernet

⬆️⬆️

2

Repeater

⬆️⬆️

3

Hotpot Sharing

⬆️⬆️

SAVE

1. Navigate to **More > Network > Multi-WAN**.
2. Locate the **Mode** dropdown and select **Failover**.
3. In the **Interface Priority** section, drag the interface rows up or down to change their priority order (e.g., **Ethernet** → 1st, **Repeater** → 2nd, **Hotpot Sharing** → 3rd).
4. Click **SAVE** to apply Failover mode settings.

Load Balancing Mode Setup

In load balancing mode, you can adjust the bandwidth distribution between different interfaces in overall network usage by adjusting the load ratio of the interfaces.

Mode Load Balancing

Load Ratio

Ethernet 3

Repeater 3

Hotpot Sharing 3

SAVE

1. Navigate to **More > Network > Multi-WAN**.
2. Locate the **Mode** dropdown and select **Load Balancing**.
3. In the **Load Ratio** section, adjust the load distribution for each interface:
 - For **Ethernet**, **Repeater**, and **Hotpot Sharing**, use the dropdowns to set a load ratio (e.g., default **3**, or choose from **0-10**).
 - The ratio determines how bandwidth is distributed across interfaces during overall network usage.
4. Click **SAVE** to apply Load Balancing mode settings.

URL Filter

You can set up URL filtering for each device connected to this router. You can block devices from accessing specific websites using keywords or full domain names.

URL Filter

Device Information	MAC	URL Filter
DESKTOP-BQQJDROP	00:E0:4C:36:00:C1	+

1. Access to **More > Network > URL Filter**.
2. Click the "+" icon to add filter rules.

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

3. Enter the Keywords or Domain Names that needs to be blocked.(Example: baidu, google, youtube)
4. Click **SAVE** to complete the settings.
5. To remove existing restricted items, find them in the "**Restricted Keywords Or Domain Names**" box and click **DELETE**.

Chapter 5 Managing Wireless Network

This chapter contains the following sections:

- [Wireless](#)
- [Guest Wi-Fi](#)
- [Parental Wi-Fi](#)

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**.

Wireless

Dual Frequency Selection



Wi-Fi

SSID

WAVLINK_2AAA

Encryption Method

WPA2-PSK (Recommended)



Password

.....



[Advanced >](#)

[Schedule >](#)

SAVE

Configuring Wireless Network

1) Dual Frequency Selection

Enabling Dual Frequency Selection combines the 2.4GHz and 5GHz Wi-Fi bands into a single network to provide a better overall network experience. Disabling this feature

allows for separate configuration of the 2.4G and 5G networks.

1. Navigate to **Wireless** or go to **More > Wireless > Wireless**.
2. Click to enable/disable **Dual Frequency Selection**.

2) Setting Wi-Fi SSID and Password

1. Navigate to **Wireless** or go to **More > Wireless > Wireless**.
2. Set a new wireless network name in the **SSID**.
3. In the **Encryption Method**, select an encryption method from the dropdown list.(It is recommended to choose **WPA3-SAE** or **WPA2-PSK**)
4. Set a new password for your wireless network in the **Password**.

Note: After setting up the new network, you will need to reconnect to the WiFi network using the new password.

Advanced Settings

Advanced

2.4G Wi-Fi Settings

Enable Wi-Fi



Channel

Automatic



Bandwidth

20/40MHz



Hide SSID



TWT



MU-OFDMA



5G Wi-Fi Settings

Enable Wi-Fi



Channel

Automatic



Bandwidth

20/80/160MHz



Hide SSID



DFS



TWT



MU-OFDMA



[Schedule >](#)

SAVE

1) Setting Channel and Bandwidth

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. From the **Channel** dropdown list, select the operating channel for your wireless network. (If you are unsure about which channel to choose, it is recommended to select **Automatic**, so the device can automatically select the optimal channel based on the surrounding environment for your better network experience.)
3. From the **Bandwidth** dropdown list, select the bandwidth for the router's wireless data transmission.

2) Setting Hide SSID

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **Hide SSID**. After enabling this, the wireless signal for the corresponding network will be hidden.

3) Setting DFS

After enabling this, the device will automatically avoid channels that are restricted in your region.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **DFS**.

4) Setting TWT

After enabling this feature, the router will automatically optimize resource scheduling between devices, negotiate target wake time to reduce contention, increase device sleep time, and ultimately extend the lifespan of the router.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **TWT**.

Note: This feature requires terminal devices that support Wi-Fi 6. If the terminal device is inactive for a long time, it may disconnect from the router.

5) Setting MU-OFDMA

After enabling this feature, the router will multiplex multiple users to improve transmission efficiency and reduce network latency in multi-user internet environments.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **MU-OFDMA**.

Schedule (Wireless Timer Switch)

The schedule function allows you to customize event rules to control the wireless network switch, with up to two 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.

Schedule

2.4G Wi-Fi

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	<input type="text" value="00"/>	<input type="text" value="00"/>	~	<input type="text" value="00"/>			
Internet Blocking Day	<input type="text" value="Sun"/>	<input type="text" value="Mon"/>	<input type="text" value="Tues"/>	<input type="text" value="Wed"/>	<input type="text" value="Thu"/>	<input type="text" value="Fri"/>	<input type="text" value="Sat"/>

Rule 2



5G Wi-Fi

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	<input type="text" value="00"/>	<input type="text" value="00"/>	~	<input type="text" value="00"/>			
Internet Blocking Day	<input type="text" value="Sun"/>	<input type="text" value="Mon"/>	<input type="text" value="Tues"/>	<input type="text" value="Wed"/>	<input type="text" value="Thu"/>	<input type="text" value="Fri"/>	<input type="text" value="Sat"/>

Rule 2



SAVE

1. Navigate to **Wireless > Schedule** or go to **More > Wireless > Wireless > Schedule**.
2. Click on **Rule 1/2** 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

This feature allows you to provide Wi-Fi to guests without exposing your main network. When you have visitors at your home, apartment, or workplace, you can create a guest Wi-Fi for them. Additionally, you can customize guest Wi-Fi settings to ensure security and privacy.

Guest Wi-Fi

Guest Wi-Fi 

Dual Frequency Selection 

Wi-Fi

SSID

Guest Wi-Fi Mode

Device Isolation

Schedule

Rule 1 

	Blocking Start Time		Blocking End Time	
Internet Blocking Period	<input type="text" value="00"/>	<input type="text" value="00"/>	~	<input type="text" value="00"/>
Internet Blocking Day	<input type="text" value="Sun"/>	<input type="text" value="Mon"/>	<input type="text" value="Tues"/>	<input type="text" value="Wed"/>
	<input type="text" value="Thu"/>	<input type="text" value="Fri"/>	<input type="text" value="Sat"/>	

Rule 2 

SAVE

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.
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 timing rules in the **Schedule**.
7. Click **SAVE** to complete the settings.

Parental Wi-Fi

The parental Wi-Fi feature creates a separate wireless network with a unique name and password for your child. You can customize internet access times for this network to control when it is available.

Parental Wi-Fi

Enable



SSID

Parental-Wi-Fi

Encryption Method

WPA2-PSK (Recommended)



Password

.....



Schedule

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	00 ▾	:	00 ▾	~ 00 ▾ : 00 ▾			
Internet Blocking Day	Sun	Mon	Tues	Wed	Thu	Fri	Sat

Rule 2



SAVE

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

Chapter 6 Net Guardian

This chapter contains the following sections:

- [Secure DNS](#)
- [AdGuard Home](#)

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.

Secure DNS

Secure DNS



DNS Protocol

DNS over HTTPS



Server Provider

Cloudflare



SAVE

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 plugins on each device.

Initial Settings

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

2 . Open **AdGuard Home**.

AdGuard Home



AdGuard Home Manage Page

192.168.20.1:3000

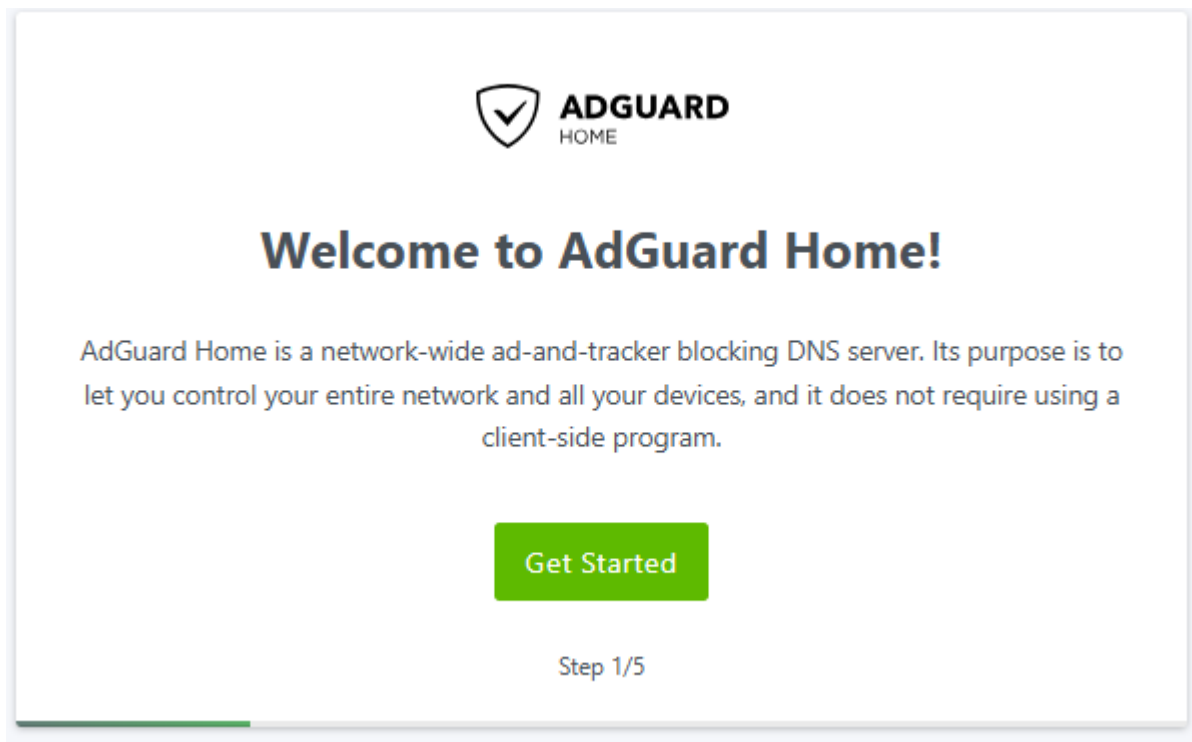
Save

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.

Admin Web Interface

Listen interface

Port

All interfaces ▼

8080

Your AdGuard Home admin web interface will be available on the following addresses:

- <http://127.0.0.1:8080>
- <http://172.16.2.111:8080>
- <http://192.168.20.1:8080>
- <http://197.131.179.1:8080>
- [http://\[::1\]:8080](http://[::1]:8080)
- [http://\[fd00:7c28:acc8::1\]:8080](http://[fd00:7c28:acc8::1]:8080)

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

DNS server

Listen interface

Port

All interfaces ▼

5353

You will need to configure your devices or router to use the DNS server on the following addresses:

- 127.0.0.1:5353
- 172.16.2.111:5353
- 192.168.20.1:5353
- 197.131.179.1:5353
- [::1]:5353
- [fd00:7c28:acc8::1]:5353

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



Authentication

Password authentication to your AdGuard Home admin web interface must be configured. Even if AdGuard Home is accessible only in your local network, it is still important to protect it from unrestricted access.

Username

Password

Confirm password

[Back](#)[Next](#)

Step 3/5

5) Click **Open Dashboard**.



Congratulations!

The setup procedure is complete and you're now ready to start using AdGuard Home.

[Open Dashboard](#)

Step 5/5

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



Username

Test

Password

.....

Sign in

[Forgot password?](#)

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

Dashboard

Disable protection

Refresh statistics

0

DNS Queries

0

0%

Blocked by Filters

0

0%

Blocked malware/phishing

0

0%

Blocked adult websites

General statistics

for the last 24 hours



DNS Queries (?)

0

Blocked by Filters (?)

0

Blocked malware/phishing (?)

0

Blocked adult websites (?)

0

Enforced safe search (?)

0

Average processing time (?)

0

Top clients

for the last 24 hours



Client

Requests count

No clients found

Top queried domains

for the last 24 hours



Domain

Requests count

No domains found

Top blocked domains

for the last 24 hours



Domain

Requests count

No domains found

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

DNS settings

Upstream DNS servers

Enter one server address per line. [Learn more](#) about configuring upstream DNS servers. Here is a [list of known DNS providers](#) to choose from.

```
114.114.114.114
119.29.29.29
```

☒ Load-balancing

Query one upstream server at a time. AdGuard Home uses its weighted random algorithm to pick the server so that the fastest server is used more often.

☐ Parallel requests

Use parallel queries to speed up resolving by querying all upstream servers simultaneously.

☐ Fastest IP address

Query all DNS servers and return the fastest IP address among all responses. This slows down DNS queries as AdGuard Home has to wait for responses from all DNS servers, but improves the overall connectivity.

Examples:

1. `94.140.14.140` ; regular DNS (over UDP);
2. `tls://dns-unfiltered.adguard.com` ;encrypted DNS-over-TLS;
3. `https://dns-unfiltered.adguard.com/dns-query` ;encrypted DNS-over-HTTPS;
4. `quic://dns-unfiltered.adguard.com:784` ;encrypted DNS-over-QUIC (experimental);
5. `tcp://94.140.14.140` ; regular DNS (over TCP);
6. `sdns://...` ;DNS Stamps for DNSCrypt or DNS-over-HTTPS resolvers;
7. `[/example.local/]94.140.14.140` ;an upstream for specific domains;
8. `# comment` ;a comment.

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

DNS blocklists

AdGuard Home will block domains matching the blocklists.

AdGuard Home understands basic adblock rules and hosts files syntax.

Enabled	Name	List URL	Rules count	Last time updated	Actions
<input checked="" type="checkbox"/>	AdGuard DNS filter	https://adguardteam.github.io/Ad...	0	–	Edit Delete
<input type="checkbox"/>	AdAway Default Blocklist	https://adaway.org/hosts.txt	0	–	Edit Delete

Previous

Page 1 / 1

10 rows ▼

Next

Add blocklist

Check for updates

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

New blocklist

Choose from the list

Add a custom list

Cancel

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

New blocklist

Enter name

Enter a URL or an absolute path of the list

Enter a valid URL to the blocklist.

Cancel

Save

Chapter 7 NAT Forwarding

This chapter contains the following sections:

- [UPnP Settings](#)
- [Port Forwarding](#)
- [DMZ Host](#)
- [Hardware NAT](#)

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.

UPnP



[Connection List >](#)

Number of connections: 0

Save

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.

Port Forwarding

+

ADD

Server IP	External Port	Internal Port	Protocol	Operation
192.168.20.111	88	8888	TCP	<div>EDIT</div> <div>DELETE</div>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<div>TCP</div> <div></div>	<div>BIND</div> <div>CANCEL</div>

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

DMZ Host

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.

DMZ

DMZ Host



DMZ Host IP

SAVE

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. Set the computer to a Static IP such as 192.168.20.215.
2. Access **More>NAT Forwarding>DMZ Host**.
3. Open **DMZ Host**.
4. Enter the **IP address** of the corresponding computer (192.168.20.215).
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.

Hardware NAT

Hardware NAT



SAVE

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](#)

Firewall

Firewall

Block Ping



Port Scan Blocking



Block DDoS Attacks



SAVE

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.

Chapter 9 VPN Server and Client

This chapter contains the following sections:

- [VPN Server Configuration](#)
- [VPN Client Configuration](#)

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.

OpenVPN Server



Device IP

172.16.4.196

The current WAN port IP is a private network address (10. x.x.x, 172.16. x.x, or 192.168. x.x)

Interface Type

tun



OpenVPN Protocol

tcp



IP Address

10.8.0.0

Subnet Mask

255.255.255.0

OpenVPN port

1194

Encryption

AES-128-GCM



authentication

SHA256



Login with username and password



Allow access to LAN



Save

- 1 . Access **More>VPN>OpenVPN Server**.
- 2 . Open **OpenVPN Server**.
- 3 . Select **Interface Type**.
- 4 . Select **OpenVPN Protocol**.
- 5 . In **IP** and **Subnet Mask**, enter the range of IP addresses the OpenVPN server can lease to devices.
- 6 . Enter **OpenVPN Port**. 1024~65535 is recommended.
- 7 . Select **Encryption** and **Authentication** methods.
- 8 . Open **Login With Username And Password** to customize username and password. If turned off, you can connect without a username and password.
- 9 . Set whether to enable **Allow LAN Access**.
- 10 . Click **SAVE**.

virtual address	Physical address	Receive Bytes	Send Bytes	Connection Time
-----------------	------------------	---------------	------------	-----------------

Save

[Export Configuration File](#)

[Export Log File](#)

11 . Click **Export Configuration File** to save it. VPN client device will establish VPN connection by using the file.

Use WireGuard VPN Server

WireGuard is a concise, efficient, and secure VPN protocol with advanced encryption algorithms, low latency, high throughput, simple and easy-to-use configuration, and cross-platform support.

WireGuard server

IP Address

10.0.0.1

Local Port

51820

Save

- 1 . Access **More>VPN>WireGuard Server**.
- 2 . Enable **WireGuard Server**.
- 3 . Enter **IP Address** and **Local Port**.
- 4 . Click **SAVE**, then click **Refresh**.

Save

100%,Please refresh...

Refresh

5 . Enter **Password** again to access router manage page. Access **More>VPN>WireGuard Server**.

6 . Click **Add User**. Set **Username** and click **APPLY**.

WireGuard server ☒

IP Address

Local Port

⊕ Add User

Username	IP Address	Configuration file	Operate
<input type="text" value="Test"/>			Apply Cancel

7 . Click **download icon** to export the configuration file. VPN client device will establish VPN connection by using the file.

Username	IP Address	Configuration file	Operate
Test	10.0.0.2/32		Delete

8 . If the client connects successfully. You can view this client in the **connection list**.

Connection List

Username	IP	Receive Bytes	Send Bytes	Last Connection
Test	10.0.0.2/32	188.62KiB	200.36KiB	1m 34s ago

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.

VPN Client

Client On/Off



Internet Access Method

PPTP

Server

Server Address

Server Address

172.16.2.216

Username

Password

Connection Status

Disconnected

SAVE

1. Access **More>VPN>VPN Client**.
2. Open **VPN Client**.
3. Select **Internet Access Method**.
4. Select **Server Address** or **Server Domain Name** in **Server** and then enter the corresponding information in **Server Address** or **Server Domain Name**.
5. Enter **Username** and **Password**.
6. Click **SAVE** to finish the configuration.

OpenVPN Client Configuration

OpenVPN Client

OpenVPN Client

Login With Username And Password

Username

Test

Password

.....

Status

Connecting...

Upload Ovpn File

master.ovpn

📁

UPLOAD

SAVE

1. Access **More>VPN>OpenVPN Client**.
2. Open **OpenVPN Client**.
3. If your VPN supplier requires **Login With Username And Password**, open it and enter VPN **Username** and **Password**.
4. Click **file icon** to import **“.ovpn file”**, then click **UPLOAD**.
5. Click **SAVE** to finish the configuration.

WireGuard Client Configuration

1. Access **More>VPN>WireGuard Client**.
2. Open **WireGuard Client**.
3. Import the WireGuard Configuration File supplied by the VPN supplier, then click **UPLOAD**. Or click **Manual Input** to enter the parameters of WireGuard VPN.

WireGuard Client

WireGuard Client



Receive

0 B

Sent

0 B

[Upload](#) [Manual Input](#)

WireGuard Configuration File

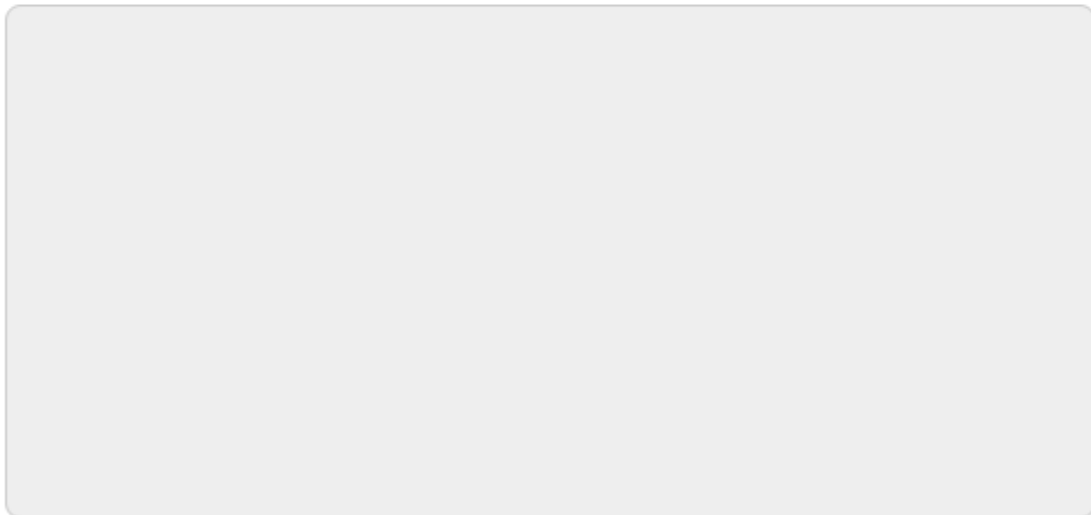
Test.conf



UPLOAD

SAVE

Configuration File

A large, empty, light gray rectangular area intended for pasting or editing the configuration file content.

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

ZeroTier Configuration

ZeroTier provides a simple, secure, and efficient way for users to create virtual networks between devices in different geographical locations. It connects dispersed devices together through the use of encryption and tunneling technology, making them communicate as if they were in the same local area network. It is suitable for various scenarios such as remote office, IoT device management, cross-regional connected connectivity, etc.

ZeroTier

ZeroTier



Connection Status

Disconnected

Network ID

8056c2e21c000001

SAVE

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 USB Setting

This chapter introduces USB server and USB tethering.

It contains the following sections:

- [Storage Server](#)
- [USB Tethering](#)

Storage Server


Please plug your USB storage device into the router's USB port, then you can access the stored file locally and remotely.


Storage Server

Username

usbuser

Password

..... 

IP	MAC	USB Status
192.168.20.1	8*:~*:~*:~*:AC:CA	

SAVE

1. Plug the USB storage device into the router's USB port.
2. Windows PC: Input the IP address (for example:\192.168.20.1) in the address bar of the file explorer and press Enter. MAC PC: Enter the connection server, and input IP address(for example:\192.168.20.1).

NOTE

Only FAT32, and NTFS file format are supported.

3. Use the username and password you set before to access it. If you need to change your password, please click **More>USB>Storage Server**.

USB Tethering

You can connect your phone to this router via the USB port to enable the USB network tethering feature, which allows network communication between other devices and this router.



1. Choose **More>USB>USB Tethering**.
2. Click to open **USB Tethering**.
3. Click on "**SAVE**" to complete setting.

Chapter 11 Remote Access

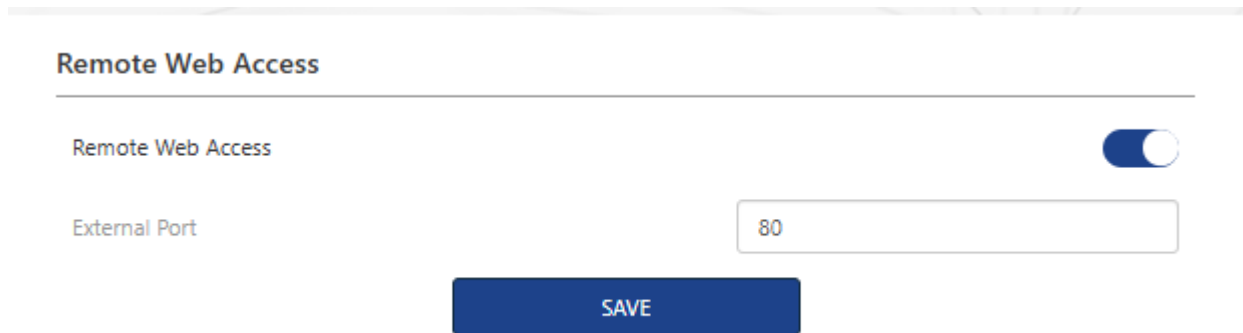
This chapter introduces remote web access and cloud APP.

It contains the following sections:

- [Remote Web Access](#)
- [Cloud App](#)

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.



Remote Web Access

Remote Web Access ☒

External Port

SAVE

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.

Cloud App

Cloud App



Connection Status

Connected

SAVE

Don't have the app? [Click to download](#)

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.

Scan the QR code using your phone to download the app. ✕



Chapter 12 NET Tools

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

It contains the following sections:

- [Diagnostics](#)
- [Wake On LAN](#)

Diagnostics

Diagnostics

Ping Or Route Tracking

Ping

IP Address Or Domain Name

www.biyiing.com

PING

PING www.biyiing.com (202.89.233.100): 56 data bytes

64 bytes from 202.89.233.100: seq=0 ttl=117 time=44.165 ms

64 bytes from 202.89.233.100: seq=1 ttl=117 time=43.364 ms

64 bytes from 202.89.233.100: seq=2 ttl=117 time=43.051 ms

64 bytes from 202.89.233.100: seq=3 ttl=117 time=42.965 ms

www.biyiing.com ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 42.965/43.386/44.165 ms

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 **TRACETOUTE** 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>Remote Wakeup**.

Wake On LAN

<input type="checkbox"/>	Describe	MAC	Hour	Minute	Repeat
--------------------------	----------	-----	------	--------	--------

No Data

ADD

DELETE

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

Wake-up Configuration ×

Describe

Test

MAC

C0 : 25 : A5 : 9F : B5 : 2F

Time setting

12

Hour

00

Minute

Reboot Time

Su

Mo

Tu

We

Th

Fr

Sa

WAKE UP

SAVE

3. Add the **Describe** 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 13 System Setting

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

It contains the following sections:

- [Firmware Update](#)
- [Change Password](#)
- [System Log](#)
- [Time Zone](#)
- [LED Control](#)
- [Restore Factory Settings](#)
- [Scheduled Reboot](#)
- [Mode Switch](#)
- [Router Reboot](#)

Firmware Update

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**.

Current SW Version

M100X3A_V240613

Local Upgrade

Upgrade File

Choose File



Upload

Online Upgrade

Latest Software Version

Status

No New Version

Non-Upgradable

Check New Version

One-Click 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**.
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.

i 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

Change Password

Old Password

New Password

The password should be at least 6 characters

Confirm New Password

The password should be at least 6 characters

SAVE

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 Password** text field.
4. Input the new one on the **Confirm New Password** text field, ensuring the inputted 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.

```
Tue Nov 19 13:36:38 2024 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Tue Nov 19 13:36:57 2024 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 03 07:28:26 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:28:31 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 03 07:28:34 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:28:36 2025 [USER] login successful, ::ffff:192.168.20.215.  
Fri Jan 03 07:29:35 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:29:36 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 3 07:29:42 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.  
Fri Jan 03 07:29:47 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:29:52 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 03 07:29:57 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:30:09 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.  
Fri Jan 3 07:31:23 2025 [USER] login successful, ::ffff:192.168.20.215.  
Fri Jan 03 07:31:57 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:32:02 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 3 07:32:02 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 03 07:32:09 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:32:14 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 03 07:32:19 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:32:24 2025 [USER] login successful, ::ffff:192.168.20.215.  
Fri Jan 3 07:33:03 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.  
Fri Jan 3 07:33:47 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.  
Fri Jan 3 07:34:06 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.  
Fri Jan 3 07:35:34 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.  
Fri Jan 3 07:37:28 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.  
Fri Jan 03 07:38:26 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.  
Fri Jan 3 07:38:31 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.  
Fri Jan 3 07:38:31 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.
```

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.

Time Zone

Current Time

2025/07/04 16:12:40

Time Zone

(UTC+08:00) Beijing, Chongqing, HongKong, Urumqi



Daylight Saving Time (DST)

SAVE

1. Access to **More>System>Time Zone**.
2. Choose the right time zone in the dropdown 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.

Led Control

Led Status



SAVE

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

Restore Factory Settings

If necessary, you can delete the current system setting and reset the router to the default factory settings.

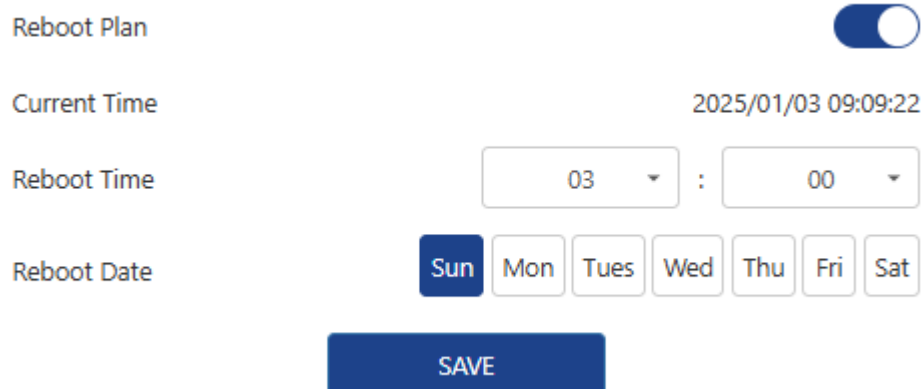
1. Access to **More>System>Restore Factory Settings**.
2. Click on **RESTORE FACTORY SETTINGS** to reset the router.

3. Wait a few minutes for the reset and reboot.

Scheduled Reboot

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.



The screenshot shows a configuration interface for the 'Scheduled Reboot' feature. At the top, there is a 'Reboot Plan' toggle switch, which is currently turned on (blue). Below this, the 'Current Time' is displayed as '2025/01/03 09:09:22'. The 'Reboot Time' is set to '03 : 00' using two dropdown menus. The 'Reboot Date' is set to 'Sun' from a row of seven buttons labeled 'Sun', 'Mon', 'Tues', 'Wed', 'Thu', 'Fri', and 'Sat'. At the bottom, there is a blue 'SAVE' button.

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

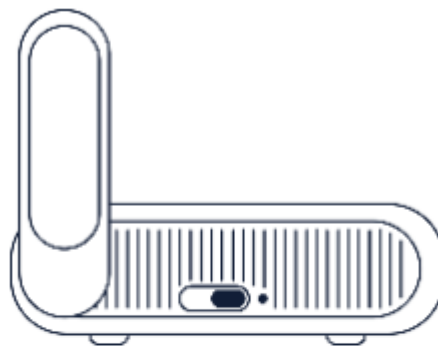
2. Turn on **Reboot Plan**.

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

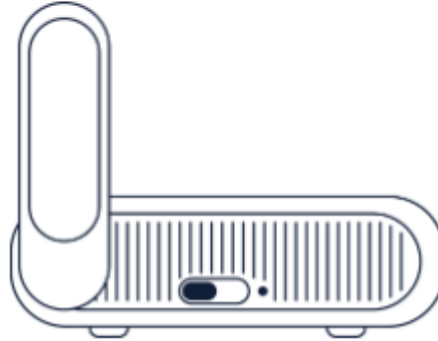
4. Click on **SAVE** to complete the configuration.

Mode Switch

Customize the toggle switch to control functions like LED settings or VPN protocols, including OpenVPN and WireGuard.



Mode Switch Disabled State



1. Access to **More** > **System** > **Mode Switch**.

Mode Switch

Feature Selection

No Specified Function



SAVE

2. Select a function from **Feature Selection** to assign to the toggle switch. (Options: No Specified Function, LED, OpenVPN, WireGuard.)
3. Click **SAVE** to apply the changes and finalize the toggle's function.

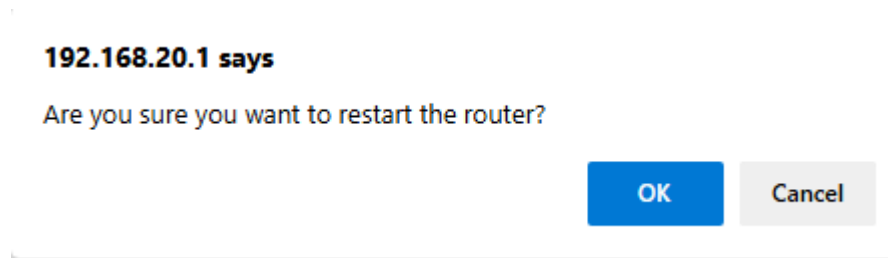
Router Reboot

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>Router 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**.

Chapter 14 Developer Options

This contains the following sections:

- [SSH](#)
- [LUCI](#)

SSH

SSH (Secure Shell) is an encrypted network protocol. When enabled, it allows users to remotely log in to the router via an SSH client application. This feature is primarily intended for users with certain development experience, enabling them to perform tasks like configuration management, debugging, and executing commands on the router's system in a secure manner.

SSH

SSH



SAVE

1. Access to **More>Developer Options>SSH**.
2. Toggle the SSH switch to **ON** (blue indicates enabled).
3. Click **SAVE** to confirm and activate SSH access.

LUCI

LuCI (Lua Configuration Interface) is the default web-based management interface for OpenWrt systems. Accessing LuCI enables you to manage and configure your router via an intuitive web interface.

LUCI

LUCI



192.168.20.1/cgi-bin/luci

1. Access to **More>Developer Options>LUCI**.
2. Toggle the LUCI switch to **ON** (blue indicates enabled).
3. Click the **clickable access link** displayed on the page to open LUCI directly in your default web browser.

Authorization Required

Username

root

Password

Login

4. Log in with your router's password to access and manage settings via the graphical interface.

wsrouter

Status ▾System ▾Network ▾VPN ▾Logout

REFRESHING

Status

System

Hostname	wsrouter
Model	MediaTek MT7981 RFB
Architecture	ARMv8 Processor rev 4
Target Platform	mediatek/mt7981
Firmware Version	OpenWrt 21.02-SNAPSHOT r17214-6cb6a60 / LuCI openwrt-21.02_230804 branch git-22.335.71649-0ecaf74
Kernel Version	5.4.194
Local Time	2025-07-23 06:28:31
Uptime	5h 54m 16s
Load Average	1.31, 1.19, 1.07

Memory

Total Available	317.07 MiB / 480.93 MiB (65%)
Used	181.20 MiB / 480.93 MiB (37%)
Buffered	5.39 MiB / 480.93 MiB (1%)
Cached	20.80 MiB / 480.93 MiB (4%)

5. If you adjust any settings on this page, click **SAVE** to apply and update your changes.

Chapter 15 Logout

Logout

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

Chapter 16 FAQ

This chapter contains the following sections:

- [FAQ](#)
- [GNU General Public License Notice](#)
- [Aftersale Service](#)

FAQ

【暂无，待补充。以下为其他型号格式参考】

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. Try to use 192.168.20.1 to login the management page.

Q2. What should I do if I can't 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. Check the router's web management page:

-Verify Internet IP validity on the Network Map.

-If valid, set DNS1 to 8.8.8.8 and DNS2 to 8.8.4.4 under More>Network>Internet>Custom DNS.

-If invalid, check hardware or contact 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?

Log in the router's web management page at <http://wavlogin.link> and go to Wireless, you can find your Wi-Fi password here.

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 License (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 software and licenses. Please inform us of your contact details (full address) and the product code. We will send you a software package with the software 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>

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 equipment, or returned to the supplier for disposal.

Aftersale Service

Need help?

We're here for you!



Online support: [wavlink.com](https://www.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 - 10:00 pm (UTC-5)

www.wavlink.com



**Thank you for purchasing
WAVLINK product!**

Chapter 17 After Sale Service_CE_FCC

- [Safety and Emission Statement](#)

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 unauthorized 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 AERIAL BayTrek is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following Internet address: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.