GL·iNet



User Manual

GL-AR300M16 / Shadow

Wireless Mini Router

Firmware Version 4.3.27

About This Manual

This manual is your go-to resource for getting started with your device, covering basic product information, hardware connections, web management interface login, initial setup, and detailed instructions for all software features in the web admin panel.

With this guide, you will be able to:

- Understand key product details
- Choose a suitable location for the device
- Complete hardware connections via step-by-step guidance
- Log into the web management interface with ease
- Configure initial settings and master all software features in the web admin panel

Format Conventions

These symbols/colors help you follow steps faster.

Convention	What It Means
Underlined teal text	Clickable link which can open a web page or a specific section
Bold text	Emphasize or mark some key information in this document, such as titles, hyperlinks, and exact menu/item names on the device's web interface
>	The path to load the corresponding page (e.g., System > Firmware)
Note	Key information for setup, operations, and safety. Ignoring this might result in setup failure, device malfunction or damage
Tips	Advice to help you use your device better

Note:

- Device features may vary by model and firmware version.
- Product availability is subject to regional differences or ISP specifications.
- All images, procedures, and descriptions in this guide are for illustrative purposes only and may differ from your actual usage experience.

Need More Help or Info?

- Firmware Update: GL.iNet Firmware Download Center | Router
- Community: Discuss our products and share insights at GL.iNet Community Forum
- Technical Support: Contact our Technical Support at Contact page

Copyright © 2026 GL.iNet Technology (HK) Ltd. All rights reserved.
No part of this manual may be reproduced, transcribed, translated, or distributed in any form or by any means, without the prior written permission of GL.iNet Technology (HK) Ltd. GL.iNet is a registered trademark of GL.iNet Technology (Hong Kong) Ltd. in China and/or other countries and regions. All other brand and product names mentioned herein are trademarks or registered trademarks of their respective owners.
The content of this document is subject to change without notice due to product version upgrades or other reasons. Unless otherwise agreed, this document is provided for informational purposes only, and all statements, information, and recommendations contained herein do not constitute any form of warranty.

GL Tech (HK) Ltd: #601, 5W, Hong Kong Science Park, N.T. Hong Kong
GL Intelligence, Inc.: 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Contents

Chapter 1 Get To Know Your Router 8

1.1 Product Overview 9

1.1.1 Appearance 9

1.1.2 Interface and Button 10

1.1.3 LED 11

1.2 Specifications 11

1.3 Package Contents 12

Chapter 2 Hardware Connection 14

2.1 Choosing a Location 15

2.2 Connecting the Router 15

Chapter 3 Log In To Your Router 16

Chapter 4 Set Up Internet Connection 18

4.1 Connect to the Internet via Ethernet Cable 20

4.1.1 Basic Setup 20

4.1.2 Protocol 21

4.2 Connect to the Internet via an Existing Wi-Fi 23

4.2.1 Basic Setup 24

4.2.2 Repeater Options 27

4.3 Connect to the Internet via USB Tethering 28

4.3.1 iPhone Tethering 28

4.3.2 Android Tethering 30

4.3.3 Troubleshooting 31

4.4 Connect to the Internet via USB Modem 32

Chapter 5 Wireless 34

Chapter 6 Clients 37

6.1 Device Details 39

6.2 Action 40

6.3 Remove Clients 42

6.4 Sort 43

Chapter 7 Get To Know VPN 44

7.1 Introduction 45

7.2 Application Scenarios 46

Chapter 8 VPN Dashboard 48
8.1 VPN Client 49
8.1.1 Client Options 50
8.1.2 Policy Mode 52
8.1.3 Global Options 53
8.2 VPN Server 55
8.2.1 Server Options 56
8.2.2 Server Route Rule 57
8.2.3 Global Options 58
Chapter 9 Set Up VPN Server 59
9.1 Set Up OpenVPN Server 60
9.1.1 Preparation 60
9.1.2 Setup Steps 61
9.1.3 Troubleshooting 63
9.2 Set Up WireGuard Server 64
9.2.1 Preparation 64
9.2.2 Setup Steps 65
9.2.3 Troubleshooting 68
Chapter 10 Set Up VPN Client 69
10.1 Set Up OpenVPN Client 70
10.1.1 Preparation 70
10.1.2 Set Up NordVPN 70
10.1.3 Set Up OpenVPN Client Manually (for other providers) 76
10.2 Set Up WireGuard Client 79
10.2.1 Preparation 79
10.2.2 Set Up AzireVPN 80
10.2.3 Set Up Mullvad 83
10.2.4 Set Up WireGuard Client Manually (for other providers) 87
Chapter 11 Applications 91
11.1 Plug-ins 92
11.2 Dynamic DNS 93
11.2.1 Enable DDNS 93
11.2.2 Check if DDNS Works 95
11.2.3 HTTP Remote Access 97

11.2.4 HTTPS Remote Access 98
11.2.5 SSH Remote Access 100
11.3 GoodCloud 101
11.3.1 Enable GoodCloud 102
11.3.2 Manage Your Router 106
11.3.3 Unbind Device 111
Chapter 12 Network 112
12.1 Firewall 113
12.1.1 Port Forwards 113
12.1.2 Open Ports on Router 115
12.1.3 DMZ 116
12.2 Multi-WAN 117
12.2.1 Interface Status Track 117
12.2.2 Multi-WAN Mode 120
12.3 LAN 123
12.3.1 Private Network 123
12.3.2 Guest Network 125
12.3.3 Address Reservation 127
12.4 DNS 129
12.4.1 General Settings 129
12.4.2 DNS Server Settings 130
12.4.3 Edit Hosts 132
12.5 Network Mode 134
12.6 IPv6 136
12.6.1 IPv6 Mode 136
12.6.2 DNS Acquisition Method 137
12.7 MAC Address 138
12.8 Drop-in Gateway 140
12.9 IGMP Snooping 142
Chapter 13 System 143
13.1 Overview 144
13.2 Upgrade 145
13.2.1 Online Upgrade 145
13.2.2 Local Upgrade 146

13.3 Scheduled Tasks 147
13.3.1 LED Display Schedule 147
13.3.2 Schedule Reboot 148
13.3.3 2.4GHz Wi-Fi Schedule 149
13.4 Admin Password 151
13.5 Time Zone 152
13.6 Toggle Button Settings 153
13.7 Log 154
13.8 Reset Firmware 155
13.9 Advanced Settings 156

Chapter 1

Get To Know Your Router

This chapter covers the router overview, specifications, and package contents.

1.1 Product Overview

Shadow (GL-AR300M16) is a pocket-size mini router, designed to be Portable and Travel-Friendly, supporting up to 300Mbps wireless transmission rate. Shadow offers advanced security features, including support for OpenVPN, WireGuard®, and a DNS server. It not only allows you to convert a public network to a private Wi-Fi for secure surfing, but also allows you to upload vpn configuration files from over 30 VPN service providers, set it as vpn client, providing an added layer of privacy and security to create an encrypted traffic between your device and the VPN server.

1.1.1 Appearance

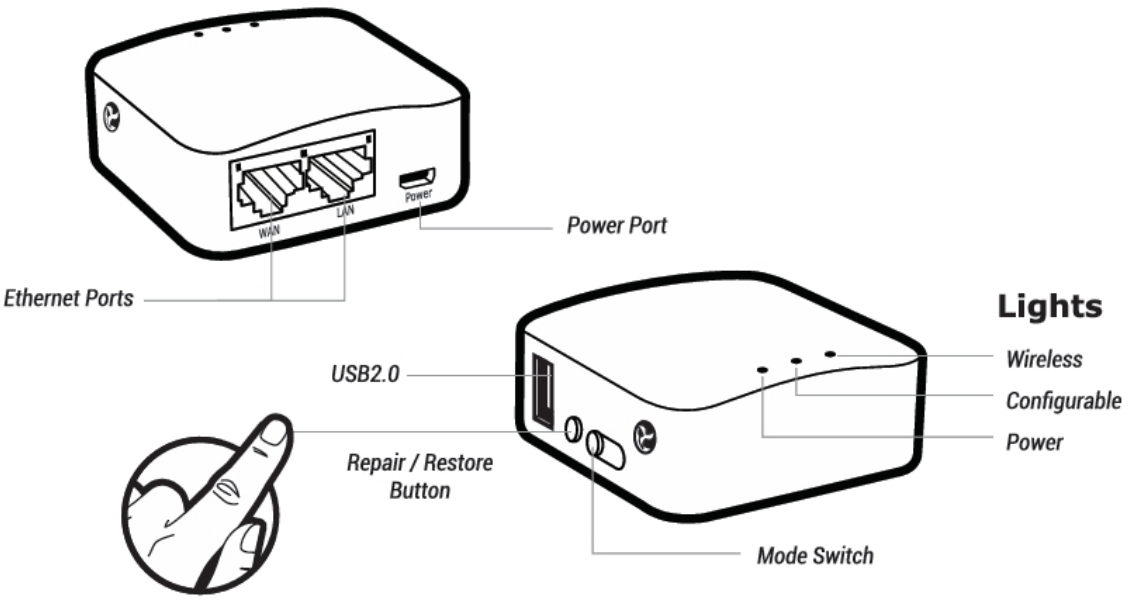








1.1.2 Interface and Button



Item	Description
Power Port	Connects to the power adapter.
WAN Ethernet Port	Connects to a modem or an Ethernet outlet for Internet.
LAN Etherne Port	Connects to wired devices if needed.
USB 2.0	For USB storage devices, phone USB-tethering, and compatible cellular dongles.
Mode Switch	A physical switch that toggles selected router settings with a flip. You can configure it in the web Admin Panel to enable one-click switching of specific features.
Repair/Restore Button	Press and hold for **4 seconds** to repair your network; Press and hold for **10 seconds** and then release to reset the router to factory default.

1.1.3 LED

LED Indicator	Indication
Power LED	On: Power on Off: Power off
Middle LED (Configurable)	On: This LED has been customized Off: This LED has not been customized (default mode)
Wireless LED	On: 2.4G Wi-Fi is connected Off: 2.4G Wi-Fi is disconnected

1.2 Specifications

Interface	1 x WAN Ethernet port 1 x LAN Ethernet port 3 x LEDs 1 x USB 2.0 port 1 x Micro USB power port 1 x Reset button 1 x Toggle button
CPU	QCA9531, @650MHz SoC
Memory / Storage	DDR2 128MB / NOR Flash 16MB
Protocol	IEEE 802.11/b/g/n
Wi-Fi Speed	300Mbps (2.4GHz)
Ethernet Speed	10/100Mbps
Power Input	Micro USB, 5V/2A
LEDs	Power / Wi-Fi
Power Consumption	< 2W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)

Dimension / Weight	58 x 58 x 25mm / 40g
Other Tools	Datasheet / Firmware / App

*Actual wireless speed and range may vary depending on environmental obstacles, network congestion, and client device capabilities.

1.3 Package Contents

Please note that the adapter within the package depends on your shipping country.

The package includes:

- 1 x Shadow (GL-AR300M16)
- 1 x User Manual
- 1 x Thank You Card
- 1 x Ethernet Cable
- 1 x USB Cable



1 x User manual



1 x Shadow (GL-AR300M16)



1 x Thank you card



1 x Ethernet cable



1 x USB cable

(GL-AR300M16-Ext)



1 x User manual



1 x Shadow (GL-AR300M16)



1 x Thank you card



1 x Ethernet cable



1 x USB cable

(GL-AR300M16)

Chapter 2

Hardware Connection

This chapter covers router location selection and connection steps.

2.1 Choosing a Location

Follow these tips to choose a location for best performance.

- **Avoid moisture and hea**t: Do not place the router in areas exposed to water, humidity, or high temperatures (e.g., sinks, radiators).
- **Ventilation and cooling**: Place the router in a cool, well- ventilated area for proper heat dissipation.
- **Central placement**: Position the router where it can connect to power and multiple devices easily (e.g., living room central zone).
- **Cable convenience**: Route cables and the power cord safely to prevent tripping hazards.
- **Stable surface**: Place the router on a horizontal, flat surface (shelf, desktop) for stability.
- **EMI avoidance**: Keep the router away from electromagnetic interference sources (Bluetooth devices, microwaves) to minimize signal interference.

2.2 Connecting the Router

1. **Power on**

   Put the two-piece power adapter together. Connect it to the router and plug it into an outlet. It will start up automatically.

2. **Connect a device to the router**

   Connect a device (e.g., laptop or smartphone) to the router via Wi-Fi or an Ethernet cable.

   - **Wi-Fi**: On your device, go to Settings > WLAN, locate the router's Wi-Fi network name in the available networks list and enter the password. You can find the default network name and password printed on your router's label.
   - **Ethernet**: Connect your device to the router's LAN port via an Ethernet cable.

3. **Log in to the router**

   The Internet is unavailable when connecting to the router for the first time. Please log in to the router as instructed in Chapter 3 to complete the initial setup before accessing the Internet.

Chapter 3

Log In To Your Router

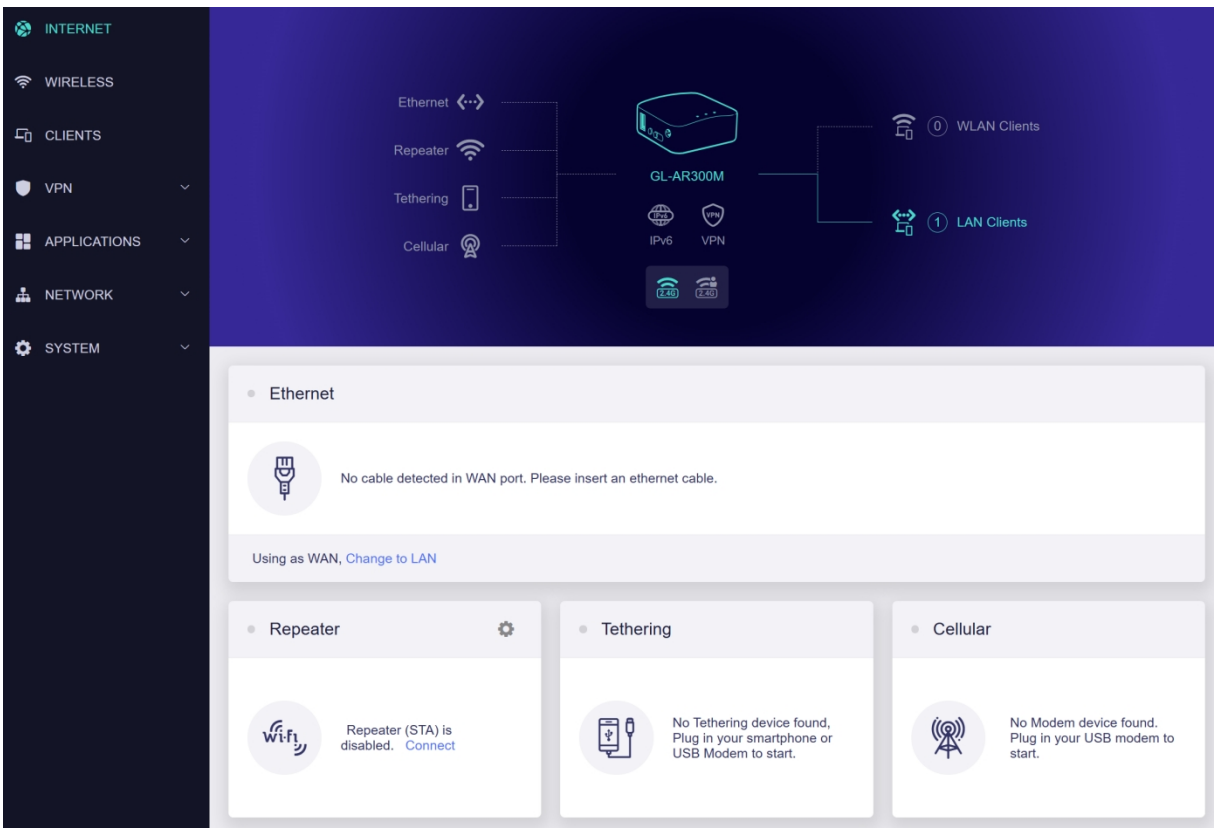
This chapter guides you to log in to your router via web admin panel.

Configure and manage your router through a web-based management interface, which can be accessed on any Windows, Mac OS or Linux OS with a web browser, such as Microsoft Edge, Google Chrome, Mozilla Firefox or Apple Safari.

Note: If you prefer using the GL.iNet app instead of the web admin panel, download the app and follow the on-screen prompts.

Follow the steps below to log in to your router via the web admin panel.

1. Connect a device (e.g., a computer or laptop) to the router via Wi-Fi or an Ethernet cable.
2. Open a web browser (Chrome and Edge are recommended) and visit http://192.168.8.1. You will be directed to the login page of the web admin panel. If you fail to access the web admin panel, see here for troubleshooting.
3. Set up your admin password. A strong password is recommended for security. Then click **Next** to continue.
4. You will then enter the router's web admin panel.



Chapter 4

Set Up Internet Connection

This chapter introduces multiple Internet connection methods for the router to adapt to diverse network environments.

Shadow supports four internet connection methods: Ethernet, Repeater, USB Tethering, and USB Modem. Choose the appropriate method based on your usage needs.

1. **Ethernet**: Connect the router to a broadband network using an Ethernet cable plugged into the WAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.

2. **Repeater**: This mode enables the router to connect to an existing Wi-Fi network to extend the Wi-Fi signal and create a separate, secure local network. Note that transmission speeds may be reduced to some extent. It is ideal for Wi-Fi dead zones that require signal extension, or public locations where enhanced network security is needed.

3. **USB Tethering**: Connect a smartphone or other compatible device to the router via a USB cable to share the device's mobile data connection (e.g., 4G/5G) with the router. This is a convenient solution for temporary internet access, especially when outdoors or in areas without fixed broadband.

4. **USB Modem**: Insert a USB cellular modem with a pre-installed SIM card into the router. The router will then connect to the internet via 4G/5G mobile networks, providing connectivity independent of fixed-line broadband. This method offers high mobility and is suitable for scenarios such as in-vehicle use or outdoor activities.

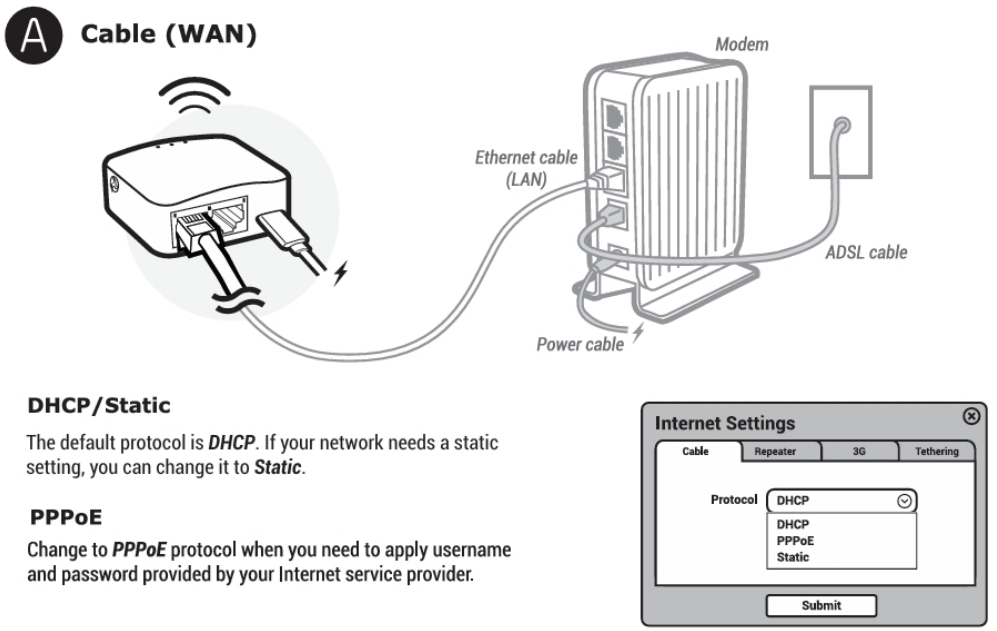
4.1 Connect to the Internet via Ethernet Cable

Connect the router to a broadband network using an Ethernet cable plugged into the WAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.

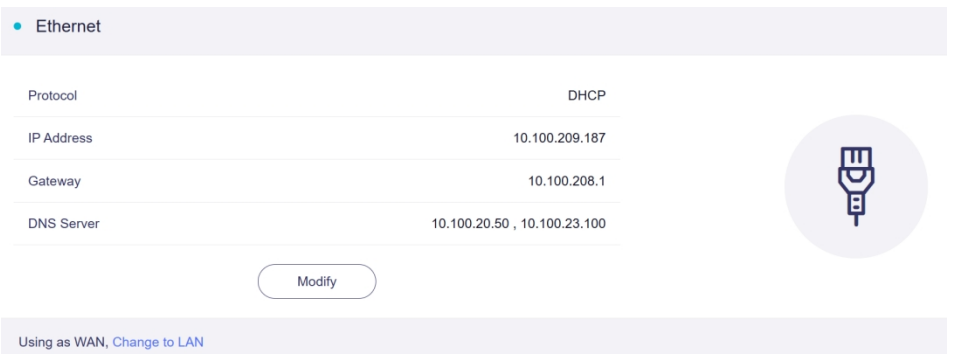
4.1.1 Basic Setup

Follow the steps below to connect your router to the Internet via an Ethernet cable.

1. Connect the **WAN** port of your router to the upstream device (e.g., an ISP modem, primary router, network switch or an Ethernet jack) via an Ethernet cable.

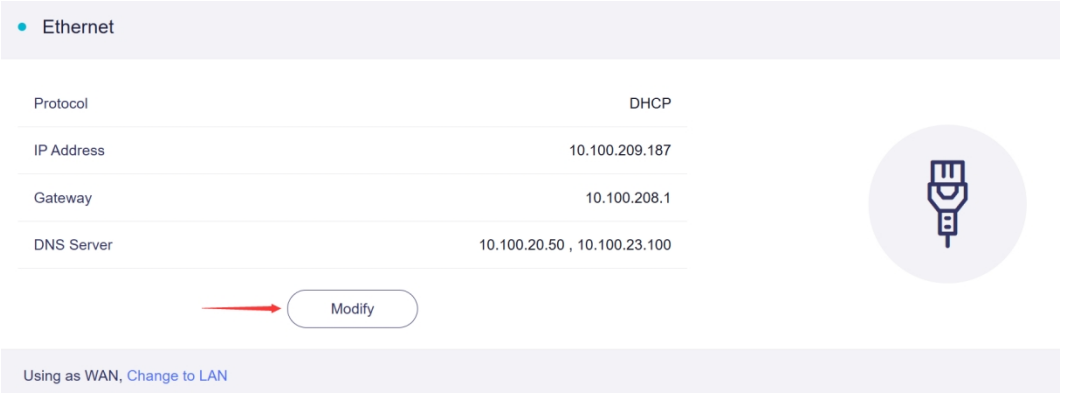


2. Log in to the router's web admin panel and navigate to **INTERNET** > **Ethernet**. If the connection is successful, the Ethernet section will display network details, including Protocol, IP Address, Gateway, and DNS Server.



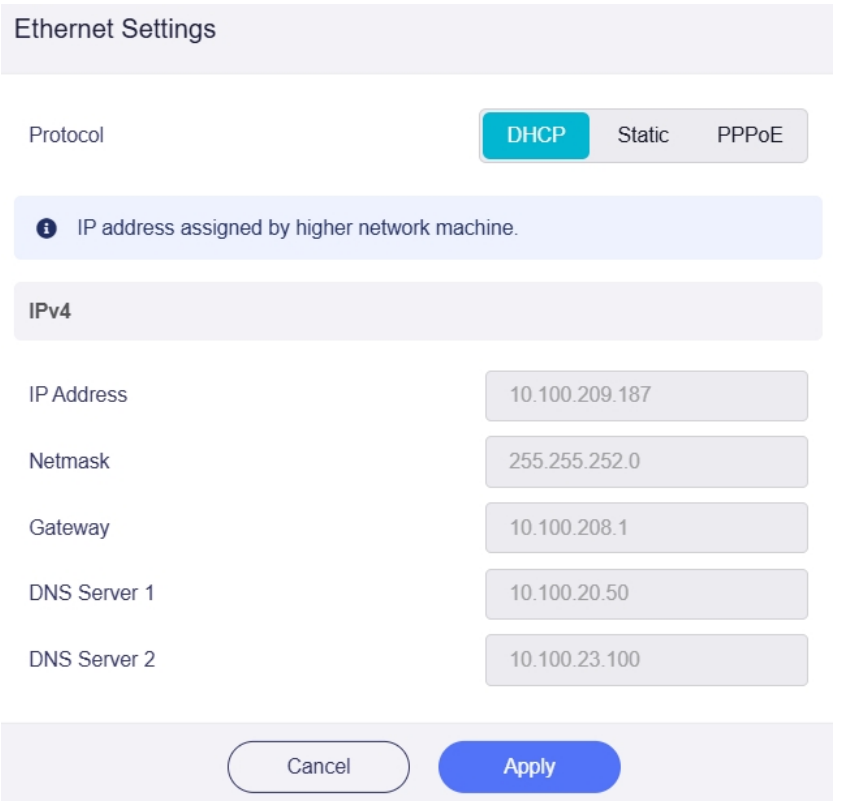
4.1.2 Protocol

There are three types of protocols: DHCP, Static and PPPoE. Click **Modify** to change.



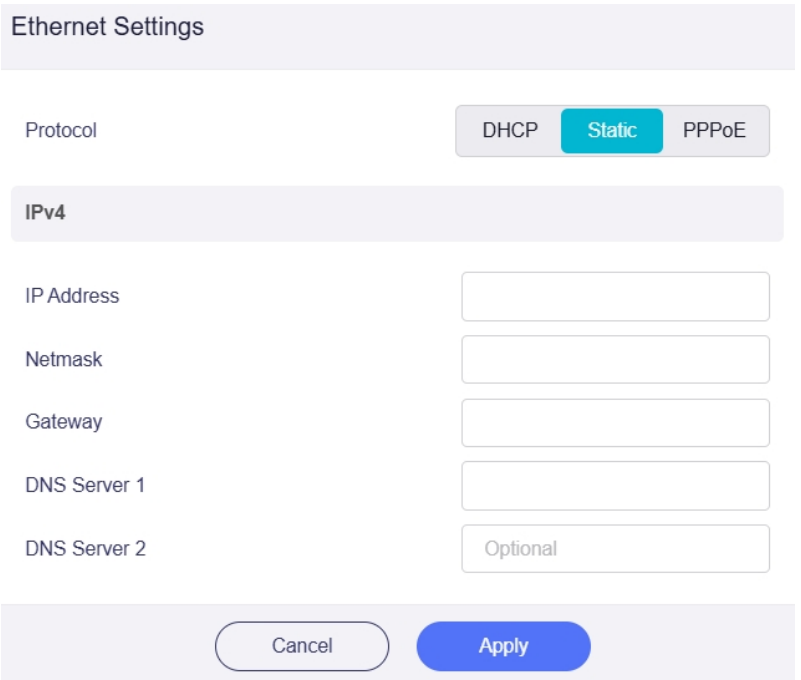
- **DHCP**

  DHCP is the default and most common network protocol, which automatically assigns IP addresses and other network configuration parameters to devices on an IP network via a client-server model.



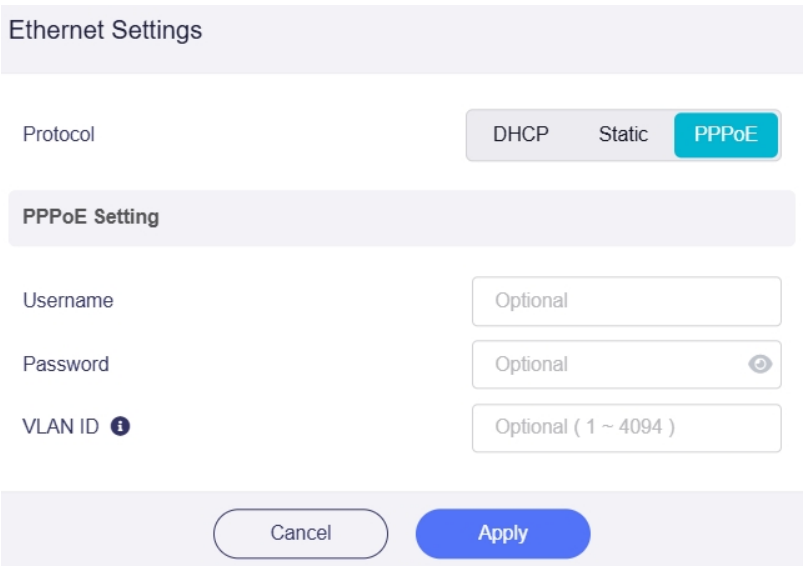
- **Static**

A static IP address is required if your ISP (Internet Service Provider) assigns a fixed public IP address, or if you need to manually configure network parameters (e.g., IP address, gateway, subnet mask).



- **PPPoE**

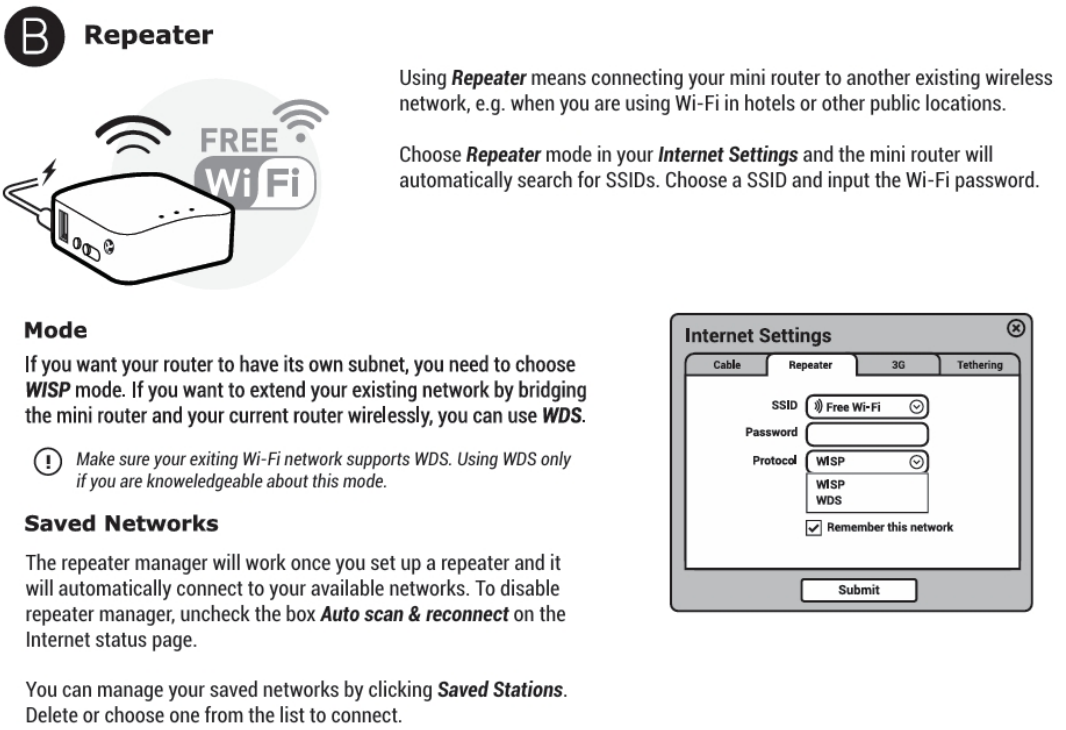
  PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol widely used by ISPs. Typically, they will provide a modem along with a unique username and password, which are required to set up an internet connection.



  You can configure a **VLAN ID** if your service provider requires the interface to use a specific tagged VLAN ID.

4.2 Connect to the Internet via an Existing Wi-Fi

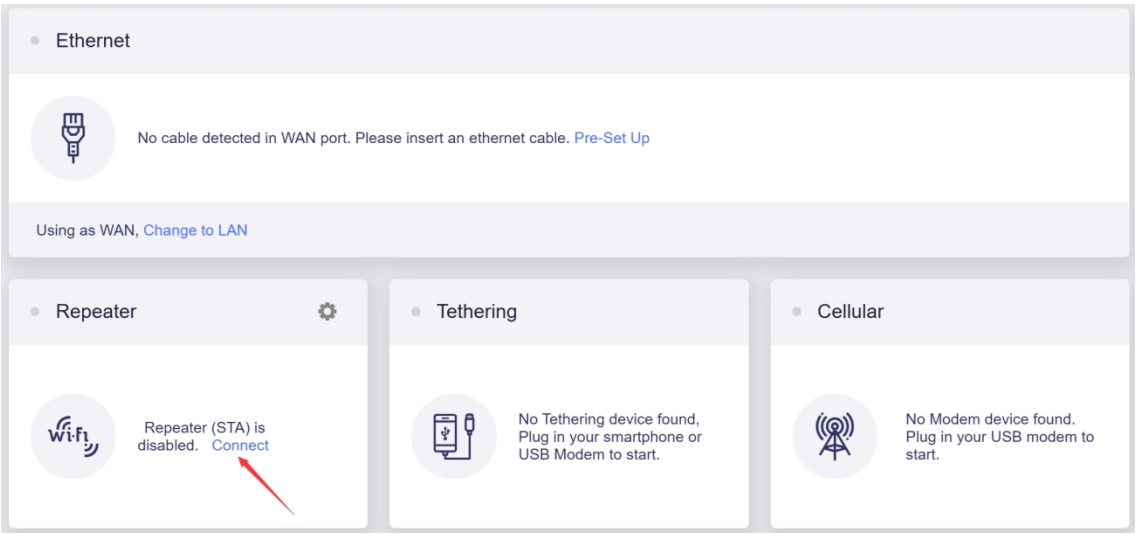
Connect the router as a repeater to the existing wireless network to boost Wi-Fi signals and create a local network isolated from the primary network. When in hotels or cafes with free public hotspots, using a repeater not only strengthens Wi-Fi signals, but also provides wired and wireless access for multiple devices, and safeguards your network security.



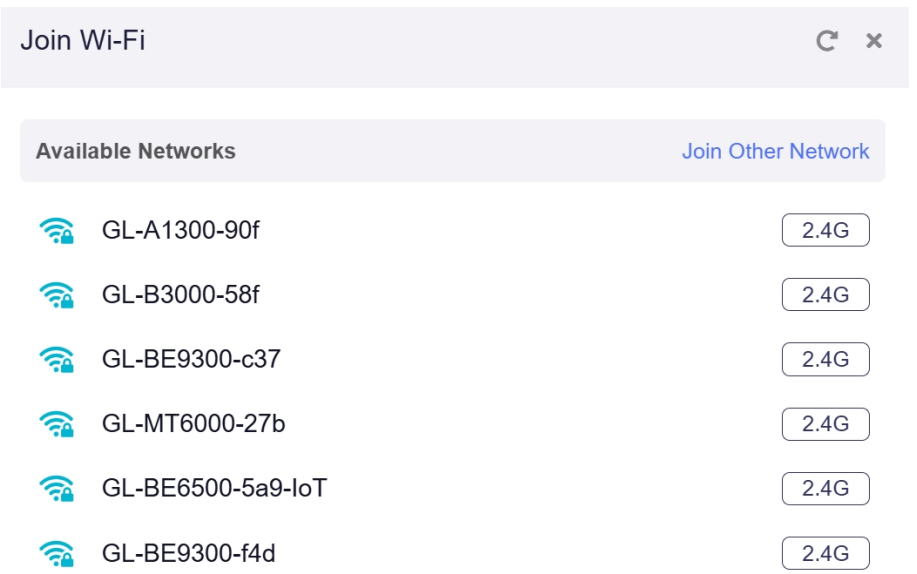
GL.iNet repeater feature works in WISP (Wireless Internet Service Provider) mode by default, which means that the router will create its own subnet and act as a firewall to protect you from the public network.

4.2.1 Basic Setup

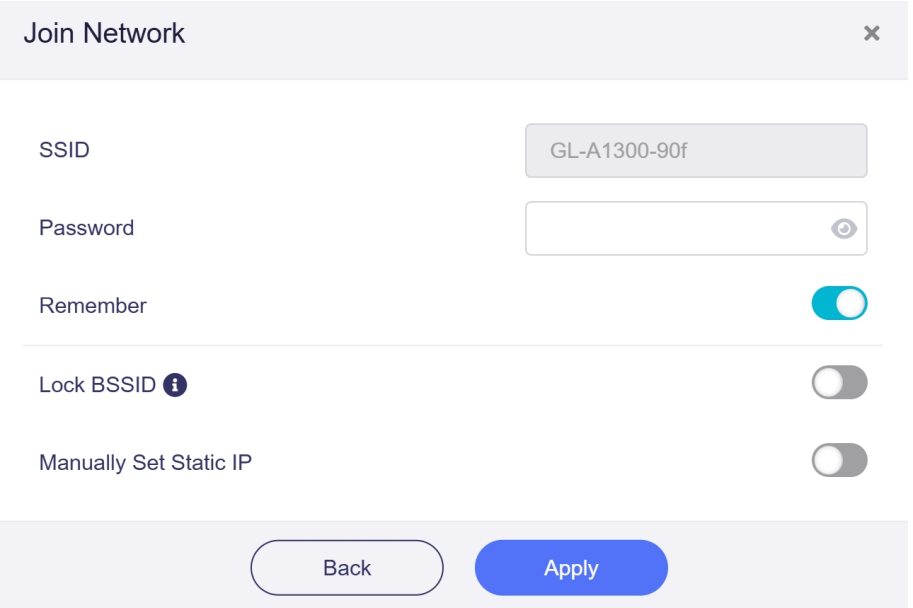
1. Log in to the router's web admin panel and navigate to **INTERNET** > **Repeater**. Click **Connect**.



2. In the pop-up window, choose the Wi-Fi network you want to connect from the available network list.

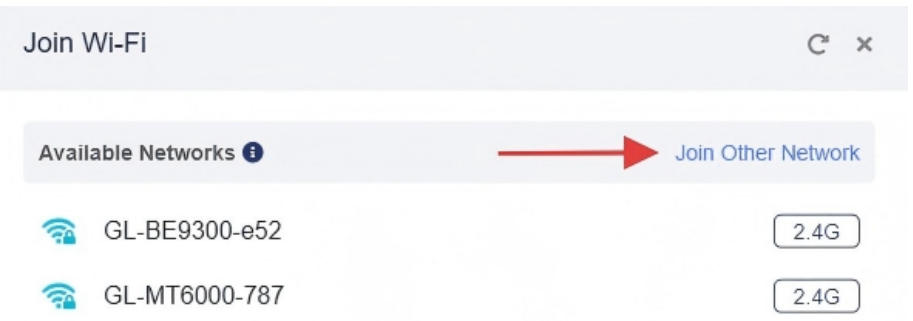


3. Enter the correct Wi-Fi password and click **Apply**.

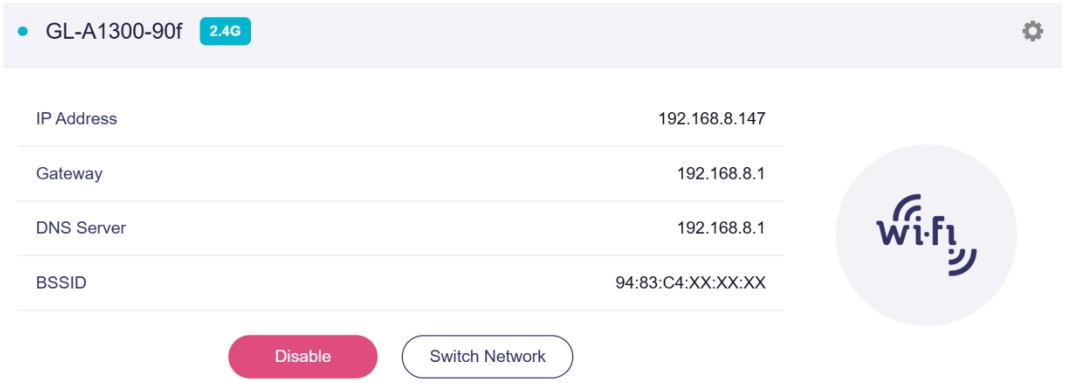


- **Remember**: Enable this to remember the current repeated Wi-Fi network.
- **Lock BSSID**: When enabled, the router will connect only to the specific access point (AP) corresponding to the selected BSSID, even when other APs share the same SSID.
- **Manually Set Static IP**: If enabled, you may manually configure IP address, subnet mask, gateway and DNS servers, instead of obtaining IP settings automatically via DHCP.

4. If the target Wi-Fi SSID is not in the Available Network list, click **Join Other Network** in the top right corner, manually input the Wi-Fi SSID and other info required, and click **Apply**.

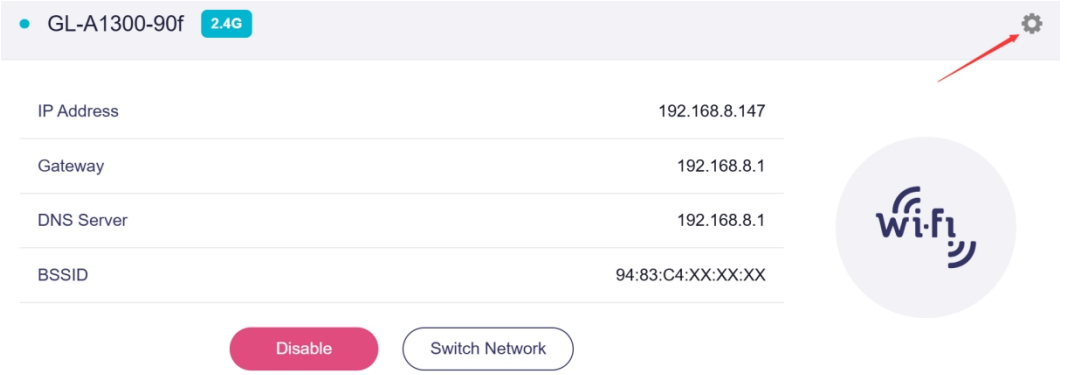


5. Wait a minute for the router to connect. Once connected, the page displays as below.

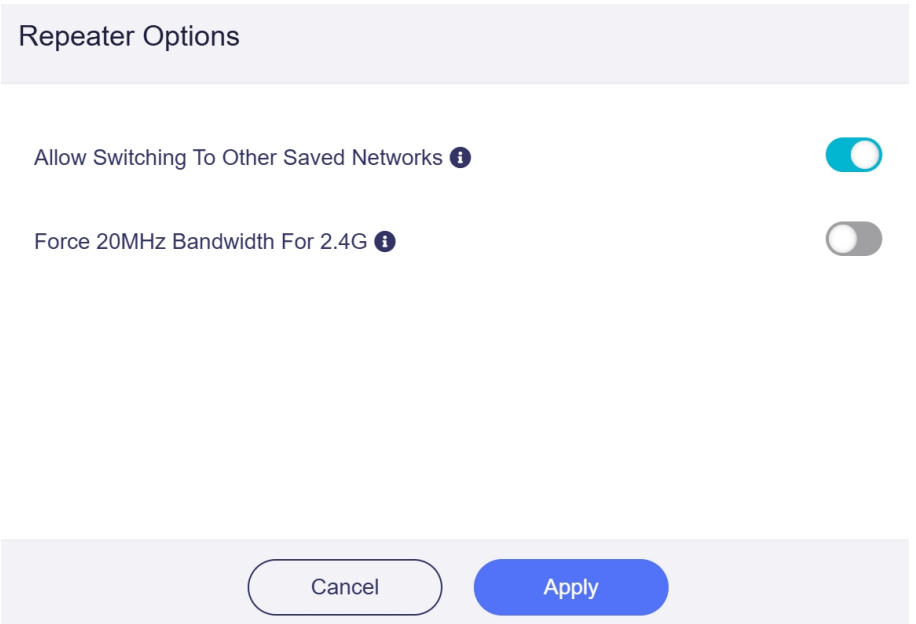

GL-A1300-90f
2.4G
IP Address
192.168.8.147
Gateway
192.168.8.1
DNS Server
192.168.8.1
BSSID
94:83:C4:XX:XX:XX
Disable
Switch Network

4.2.2 Repeater Options

Click the gear icon in the upper-right corner to configure Repeater options.



The page may vary due to different firmware versions.

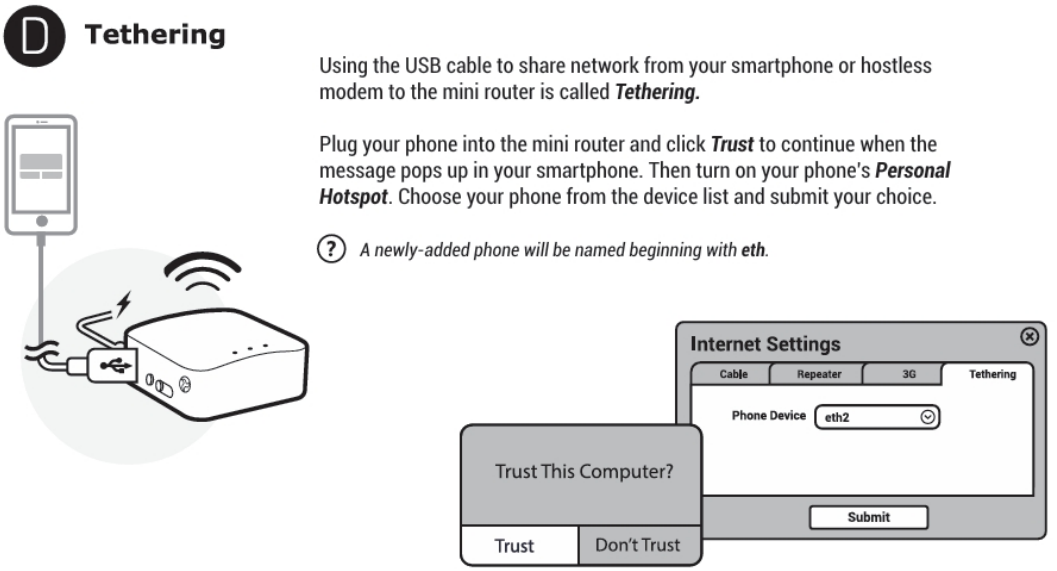


- **Allow Switching to Other Saved Networks**: If the option is enabled, the router will automatically connect to other saved networks when it is unable to connect to the current Wi-Fi network.
- **Force 20MHz Bandwidth for 2.4G**: If this option is enabled, the device will improve the stability of the connection by reducing the connection rate.

  Note: It only works when repeating 2.4G Wi-Fi.

4.3 Connect to the Internet via USB Tethering

Connecting a smartphone to the router through a USB cable is called Tethering, which can share the device's mobile data network (e.g., 4G/5G) with the router. This is a convenient method for temporary internet access, especially when outdoors or in areas without fixed broadband.

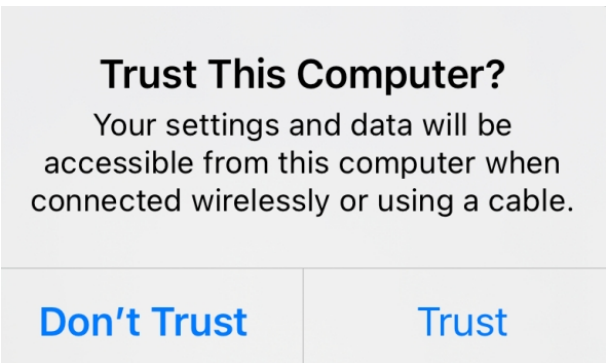


Host-less modem works in Tethering as well during the setup of the modem.

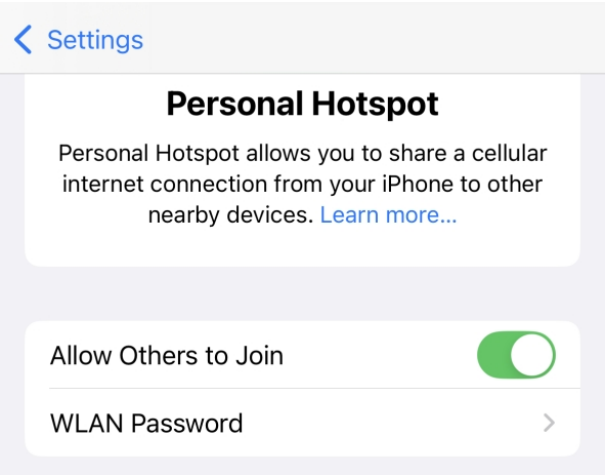
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

4.3.1 iPhone Tethering

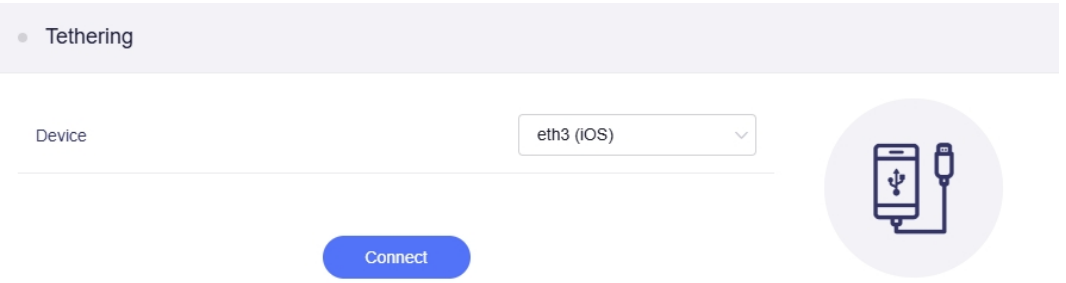
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



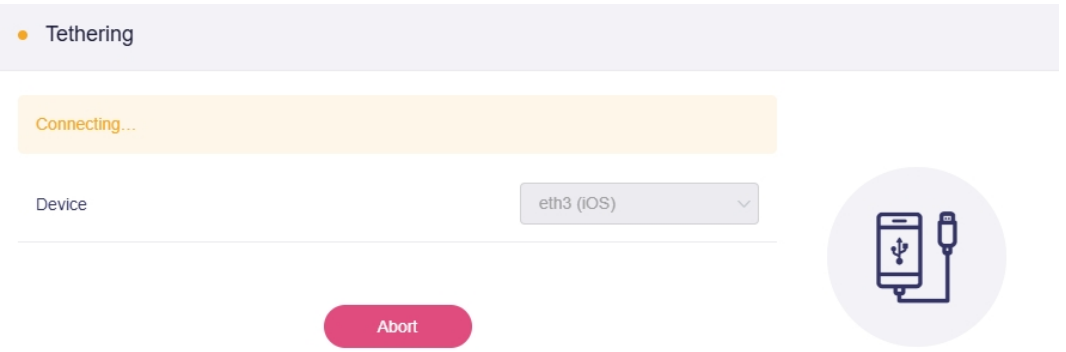
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



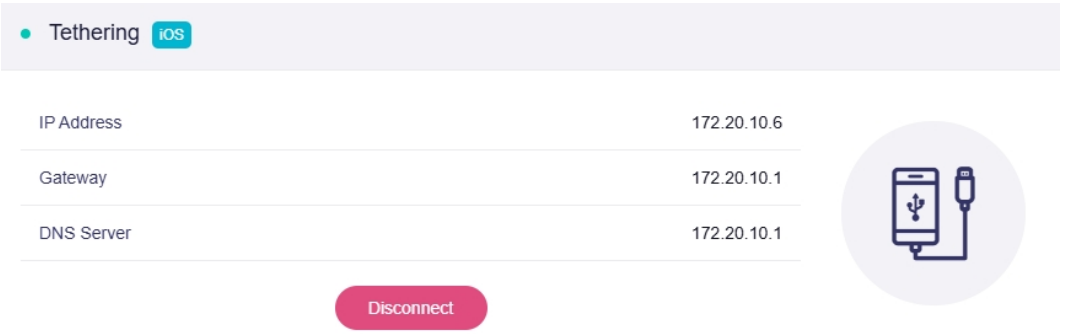
3. Connect a computer or another phone to the router. Log in to the router's web admin panel and navigate to **INTERNET** > **Tethering**, then click **Connect**.



4. It will start connecting.

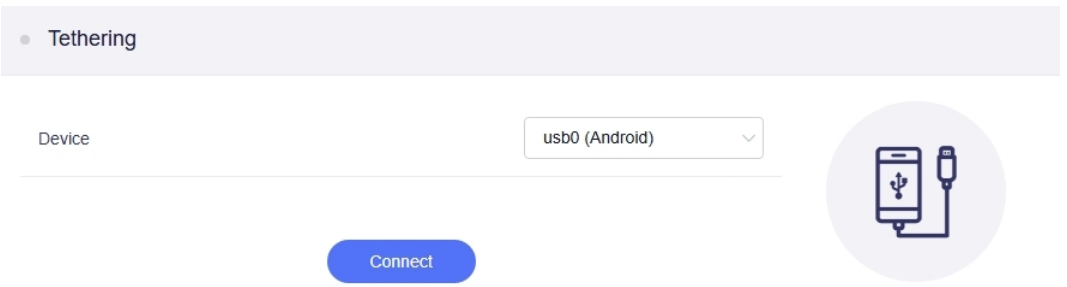


Once connected, this page will display the Tethering connection details.

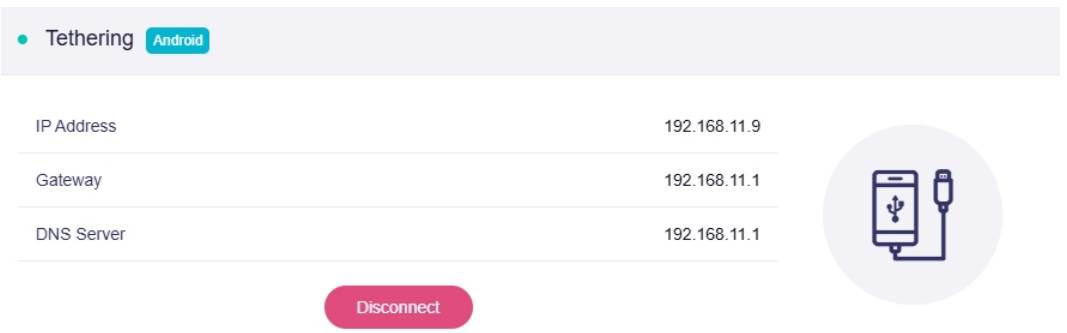


4.3.2 Android Tethering

1. Connect an Android phone to the router's USB port using a USB cable. A system dialog may appear asking USB preferences. Select **USB Tethering** or **File Transfer** if prompted.
2. Go to your phone's **Settings** > **Network & Internet** > **Personal Hotspot**. Enable **Personal Hotspot** or **USB Tethering**.
   (The steps to enable USB Tethering vary by brand. Check your device's settings for the exact location, and contact your manufacturer's support if needed.)
3. Connect a computer or another phone to the router, then log in to the router's web admin panel, navigate to **INTERNET** > **Tethering**. Click **Connect**.



4. Once connected, this page will display the Tethering connection status.



4.3.3 Troubleshooting

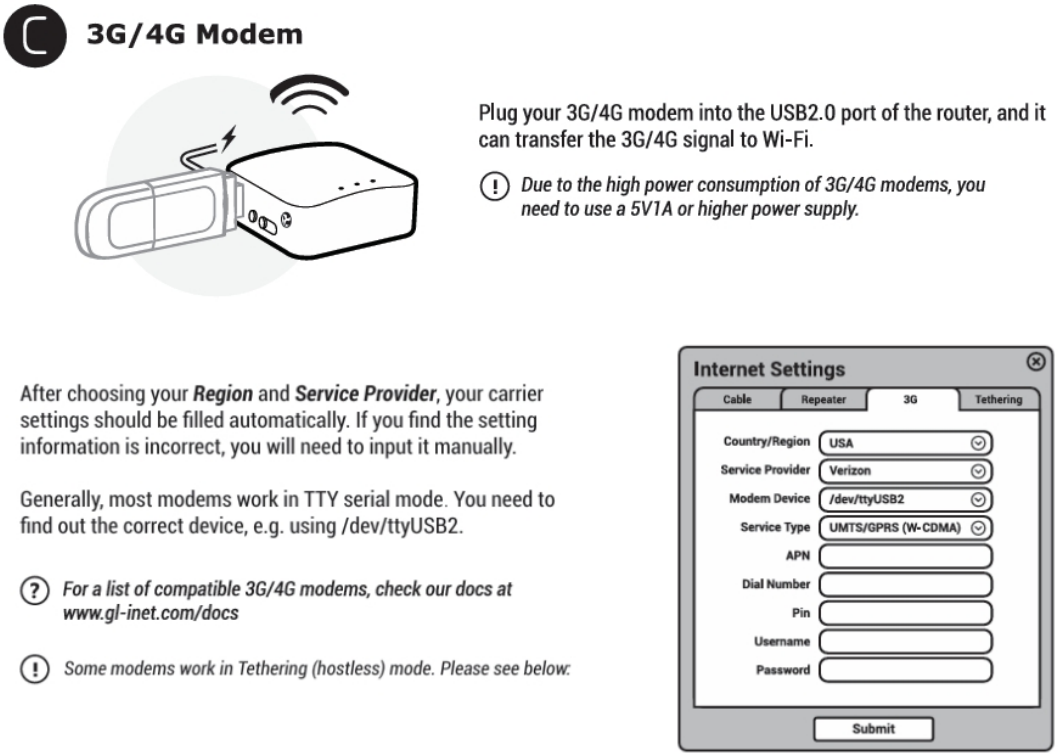
If the Tethering connection fails, try these troubleshooting steps:

- Use the original power supply for the router.
- Unplug and re-plug the USB cable.
- Use another USB cable. Ensure it supports data transfer (not just charging).
- Turn off and turn on "USB Tethering" for a few times (for Android Phone).
- Turn off and turn on "Allow Others to Join" for a few times (for iPhone).
- Restart your smartphone and try again.

If problem persists, contact our technical support at support@gl-inet.com.

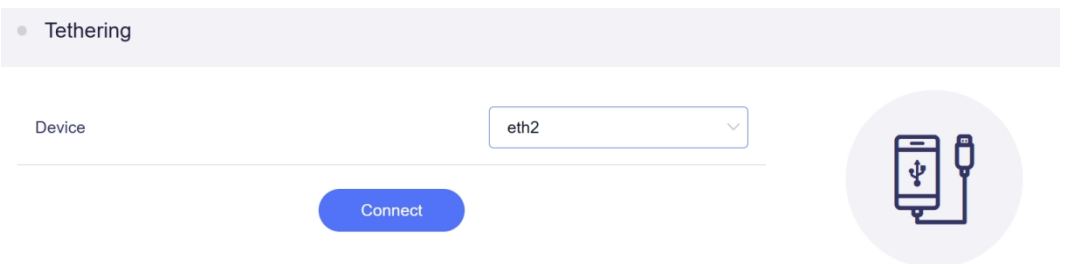
4.4 Connect to the Internet via USB Modem

Connect the router to the internet by inserting a cellular-enabled USB modem into its USB port. This allows the router to connect to the Internet via 3G/4G networks, providing connectivity without relying on fixed-line broadband. It is suitable for in-vehicle use or outdoor activities. Note that this connection is implemented through the router's Tethering or Cellular interface.

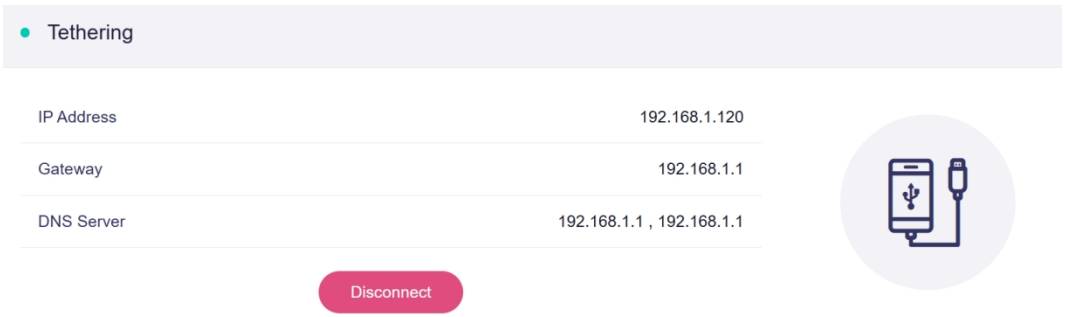


Follow the steps below to connect your router to the Internet via a USB modem.

1. Plug a USB modem with a pre-installed SIM card into the router's USB port before powering it on.
2. Log in to the router's web admin panel and navigate to **INTERNET** > **Tethering**. Click **Connect**.



3. It will start connecting. Once connected, this page will display the network details.



Tip: After initial setup, if you restart the router with the USB modem still connected, or re-insert the modem into the router, the USB modem will be automatically recognized, and a network connection will establish without re-clicking "Connect".

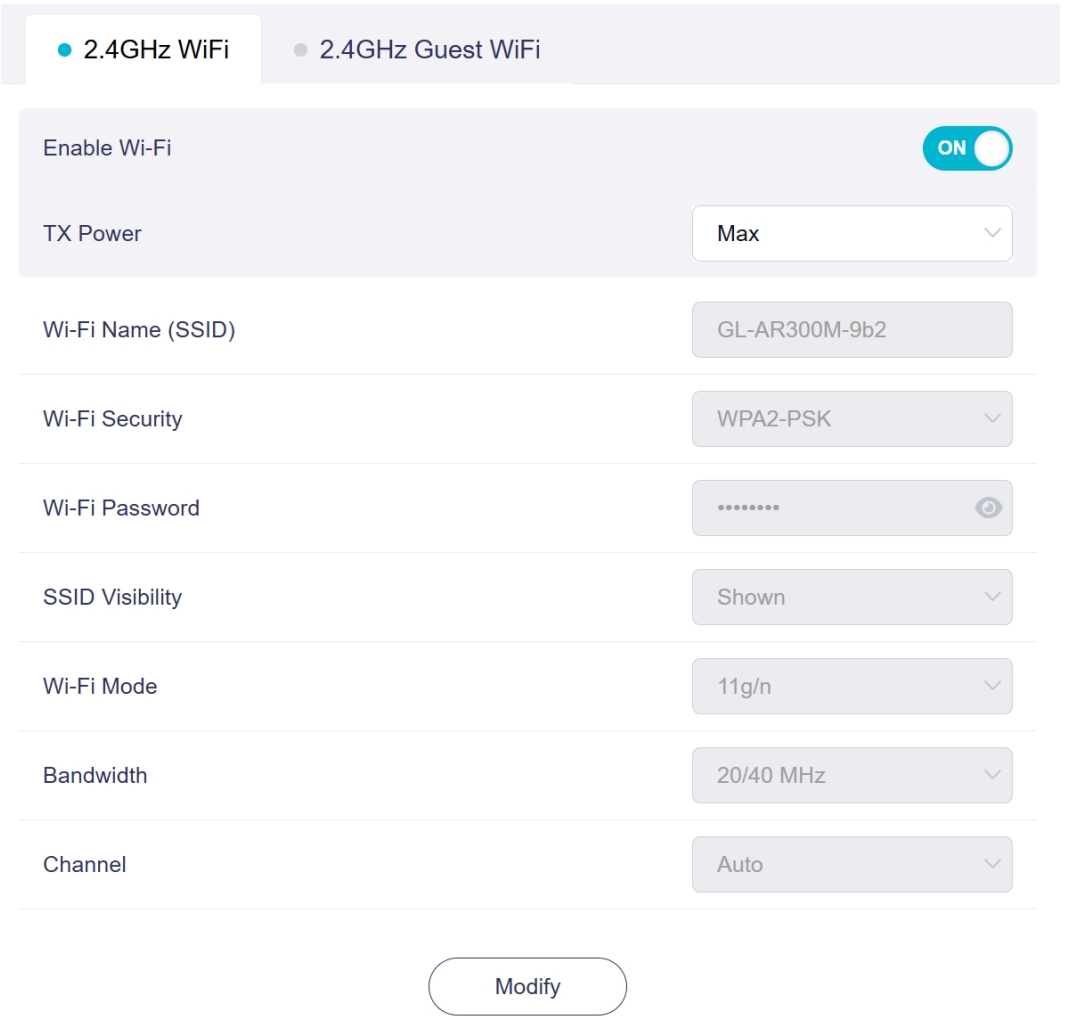
Chapter 5

Wireless

This chapter guides you to check Wi-Fi status and configure wireless settings.

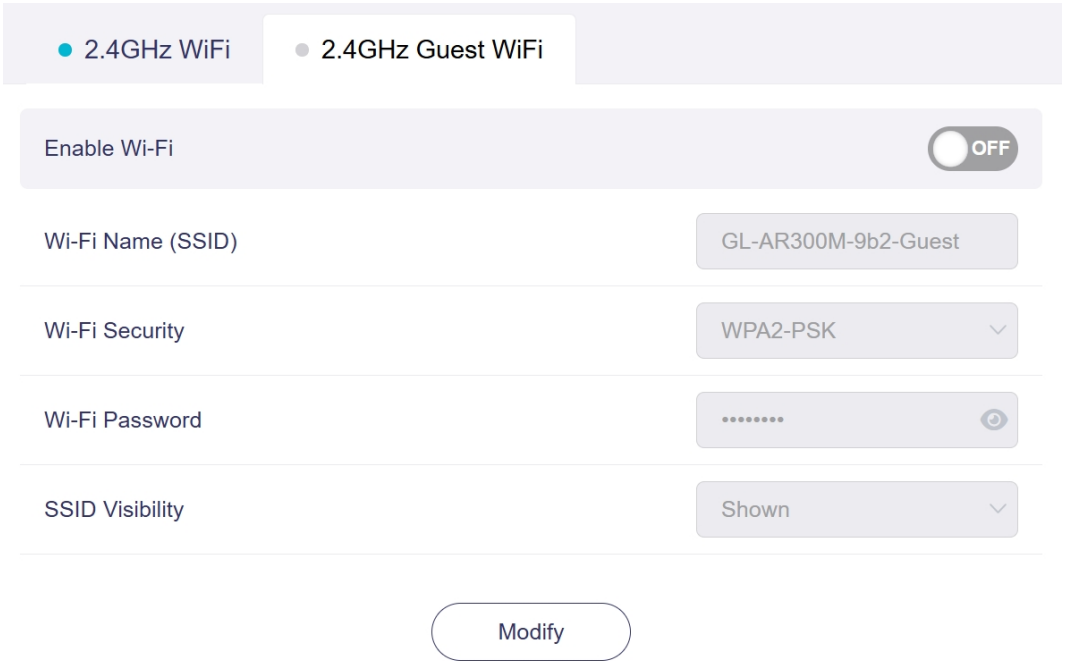
Log in to the router's web admin panel and navigate to **WIRELESS**.
The wireless page displays the router's 2.4 GHz settings, with each further divided into main Wi-Fi and guest Wi-Fi networks for flexible management.

The 2.4 GHz Main Wi-Fi allows you to configure multiple settings, including enabling/disabling Wi-Fi, setting TX power, setting Wi-Fi name (SSID), security, password, SSID visibility, mode, bandwidth, and channel.



Note: The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.

The 2.4 GHz Guest Wi-Fi allows you to configure simplified settings, including enabling/disabling Wi-Fi, setting Wi-Fi name (SSID), security, password, and SSID visibility.


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
OFF
Wi-Fi Name (SSID)
GL-AR300M-9b2-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
••••••••
SSID Visibility
Shown
Modify

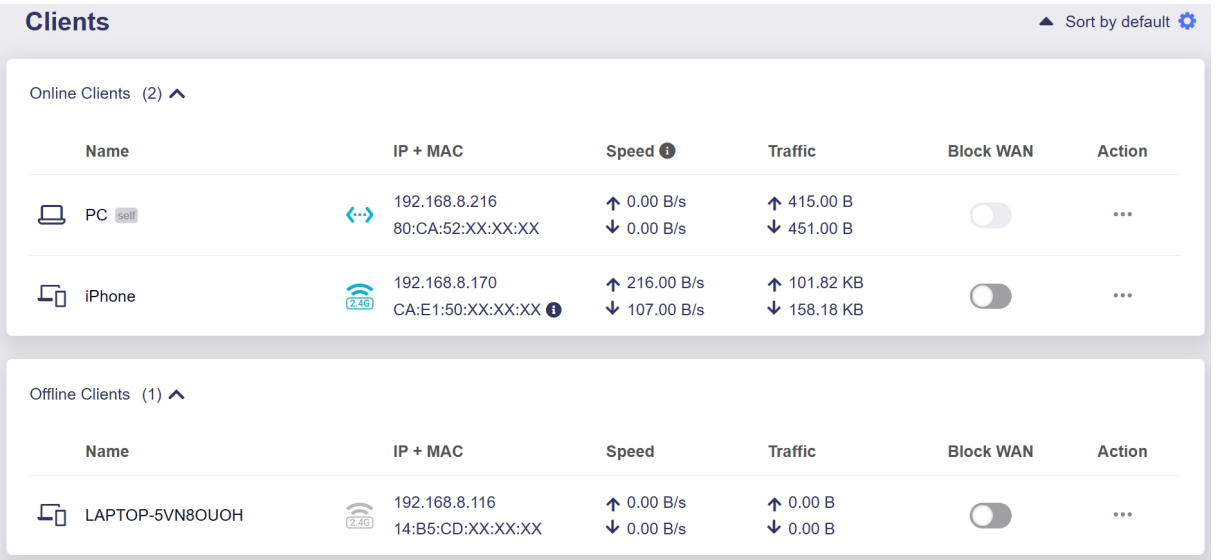
Chapter 6

Clients

This chapter guides you to view details of connected devices and manage their connections.

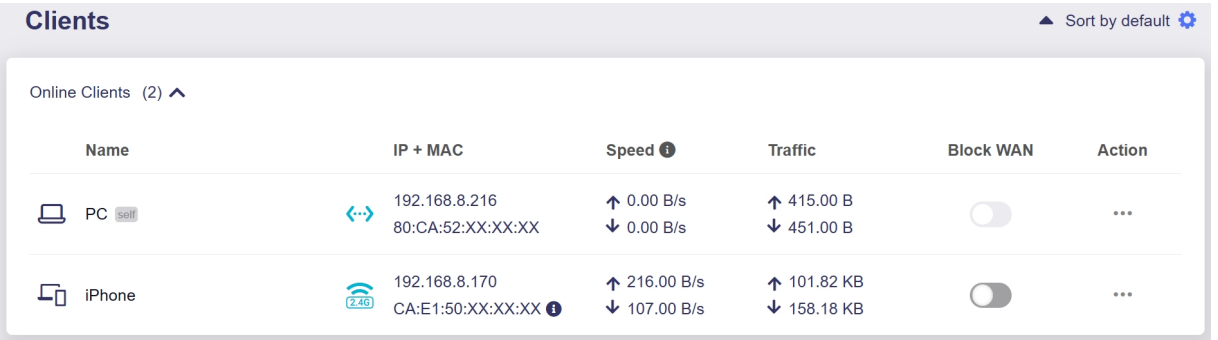
Log in to the router’s web admin panel and navigate to **CLIENTS**.

The Clients page displays information about connected devices, including device name, connection type, IP and MAC address, speed, and traffic, arranged left to right. It also provides quick access to reserve IP, block client or perform other actions.



- **Online Clients**: It refers to devices currently connected to the router's network.
- **Offline Clients**: It refers to devices that have previously connected to the router but are now disconnected from the network.

6.1 Device Details



1. **Device Name**

   The first column displays the device name and type, which depends on the hostname of the device operator. The blue icon next to the device name represents the connection method, indicating that the device is connected to the router via an Ethernet cable.

2. **IP and MAC Address**

   The second column lists the IP and MAC addresses of the connected device. If the connected devices use randomized MAC addresses, a prompt will appear, indicating that this is a randomized MAC address.



   If the second character of the MAC address is 2, 6, A or E (Ignore case), it is considered as a randomized MAC address. However, some devices may use a different rule to generate a randomized MAC address, so this detection method may not be accurate.

3. **Speed**

   The third column displays the internet speed of the connected device. This speed represents the average speed over the past 3 minutes. The system starts calculating the average speed when this page is opened (e.g., if the page has only been open for 10 seconds, the average speed will be based on just 10 seconds of data).

4. **Traffic**: The fourth column displays the internet traffic of the connected device.

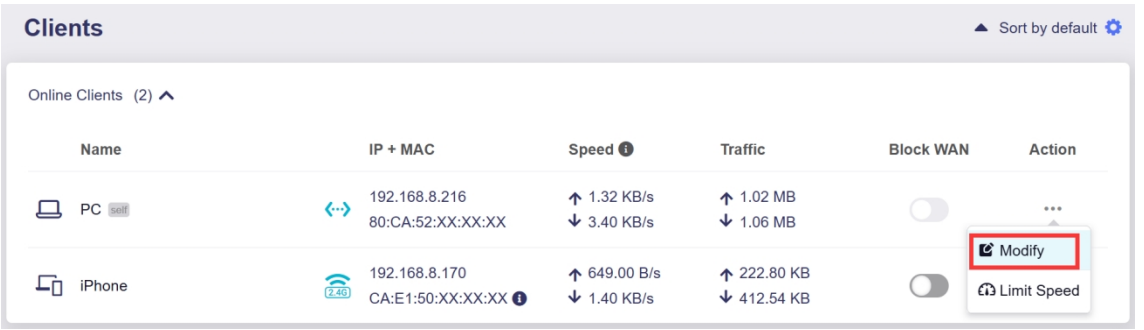
5. **Blocklist**

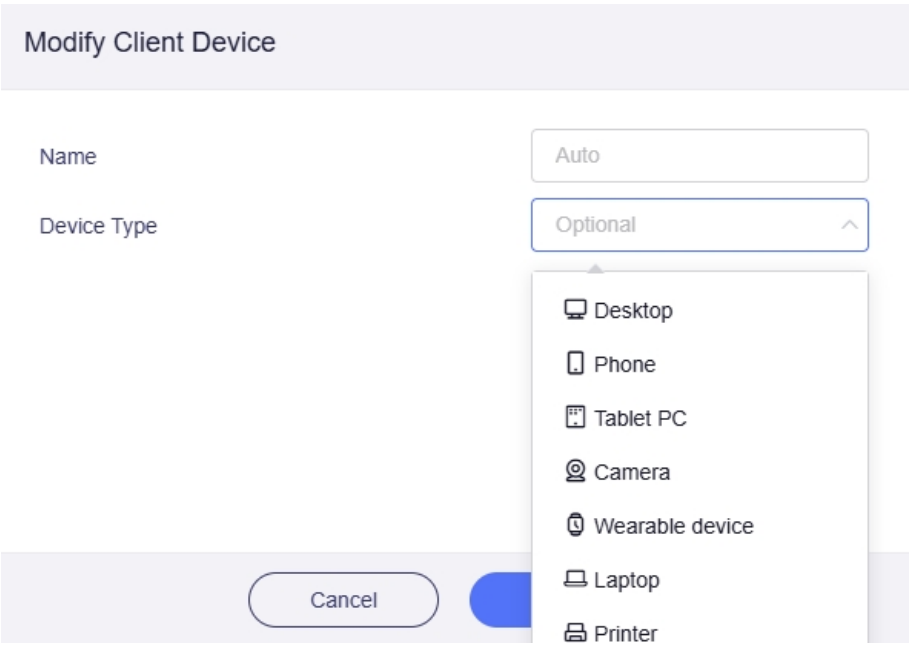
   In the fifth column, you can block specific connected devices with one click. If enabled, devices with MAC addresses in the blacklist are not allowed to connect to this router. Please note that blocking client is based on the MAC address of the device. If the blocked device uses different MAC address next time, it can still be able to connect to router.

6.2 Action

1. **Modify**

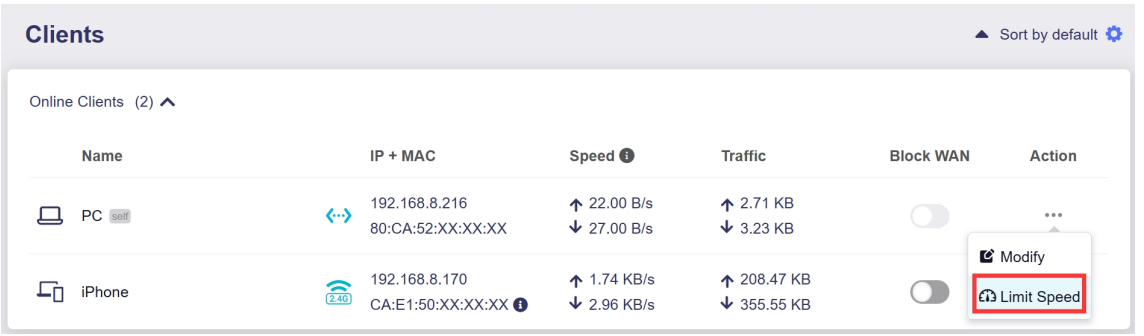
   Click the three-dot icon in the **Action** column, and click **Modify** from the drop-down menu to modify the device name and type.



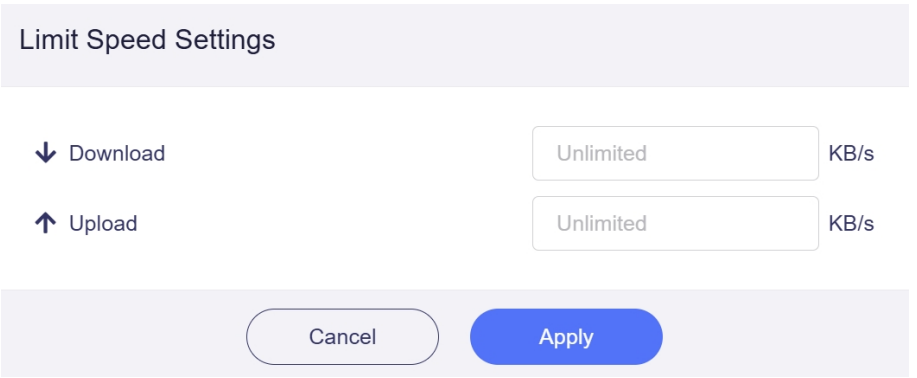


2. **Limit Speed**

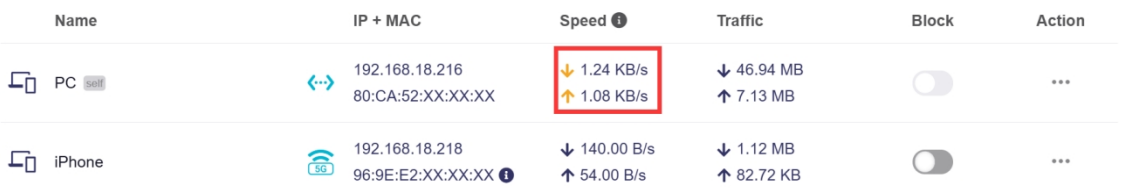
Click the three-dot icon in the **Action** column, and click **Limit Speed** from the drop-down menu.



You will be able to limit the speed of a connected device, with the unit set to KB/s.

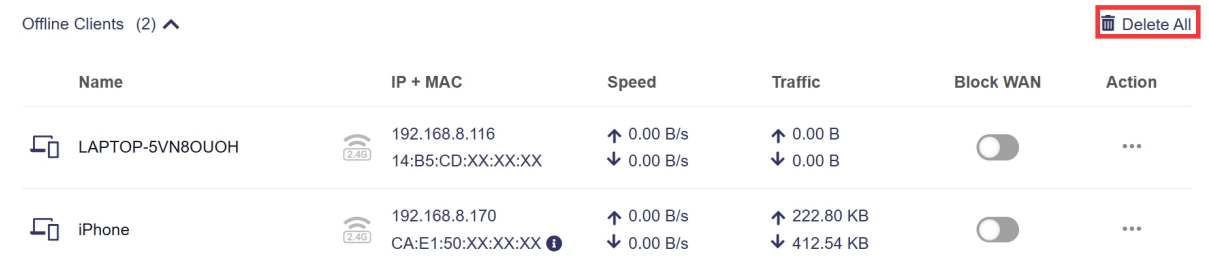


If speed limitation has been applied to a device, the upload/download speed arrows will turn yellow.

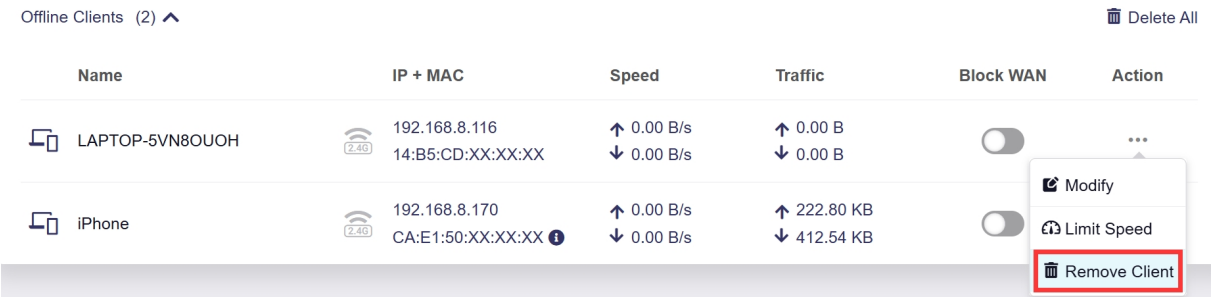


6.3 Remove Clients

In the **Offline Clients** section, you can click **Delete All** in the top right corner to delete all offline clients.

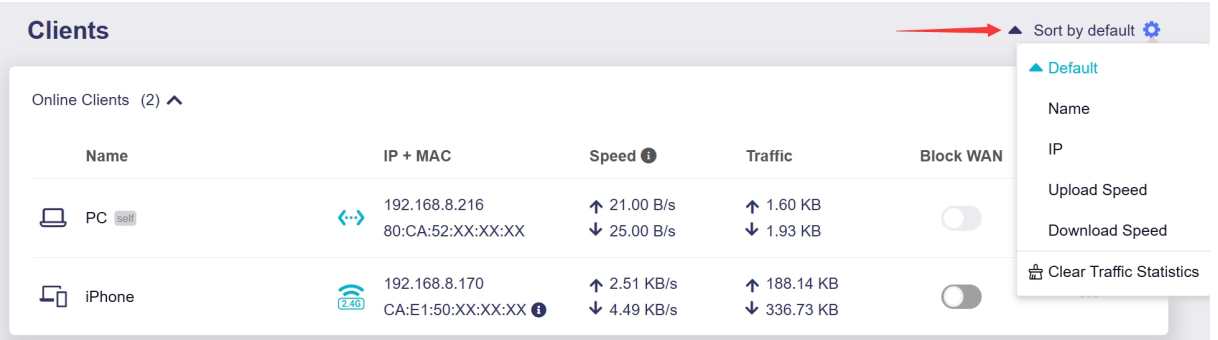


If you want to remove a specific client, click the three-dot icon in the **Action** column, then click **Remove Client** from the drop-down menu.



6.4 Sort

You can set the device sorting rule for the Client page in the top right corner.



The default sorting order is as follows:

- The self-device (i.e., the device you are using to access the router's Admin Panel) always appears at the top.
- In the **Online Clients** section, devices are listed higher if they connected earlier.
- In the **Offline Clients** section, devices are listed higher if they disconnected earlier.

In addition to sorting rules, the dropdown menu also provides the **Clear Traffic Statistics** function. It clears traffic statistics for all online clients with one click. Once applied, the traffic statistics column will be reset to zero and then restart the statistics.



Chapter 7

Get To Know VPN

This chapter introduces VPN concepts and common use scenarios.

7.1 Introduction

VPN

VPN, short for Virtual Private Network, establishes an encrypted and private tunnel between a device and a remote server, protecting data transmission and enabling secure access to private or restricted networks.

VPN Router

A VPN router features preinstalled VPN functionality, protecting all connected devices via VPN. Unlike setting up VPN on individual devices, configuring the router as a VPN client routes all traffic through an encrypted tunnel, with no separate setup needed per device. This secures multiple devices at once, saves time, and ensures consistent VPN configurations, reducing risks from improper individual settings.

GL.iNet routers support over 30 popular commercial OpenVPN and WireGuard VPN services. Upload your VPN configuration files to activate the VPN connection for secure networking. See here for the full list of third-party VPN providers.

OpenVPN

OpenVPN is an open-source VPN protocol using SSL/TLS-based security for point-to-site or site-to-site connections. It supports multiple encryption methods, TCP/UDP, and easy firewall/NAT bypass.

WireGuard

WireGuard is a lightweight, fast VPN protocol simpler and more efficient than OpenVPN. It features modern cryptography for efficiency, a small codebase for easier auditing and security, and state-of-the-art algorithms (ChaCha20/Poly1305) for encryption and data integrity.

7.2 Application Scenarios

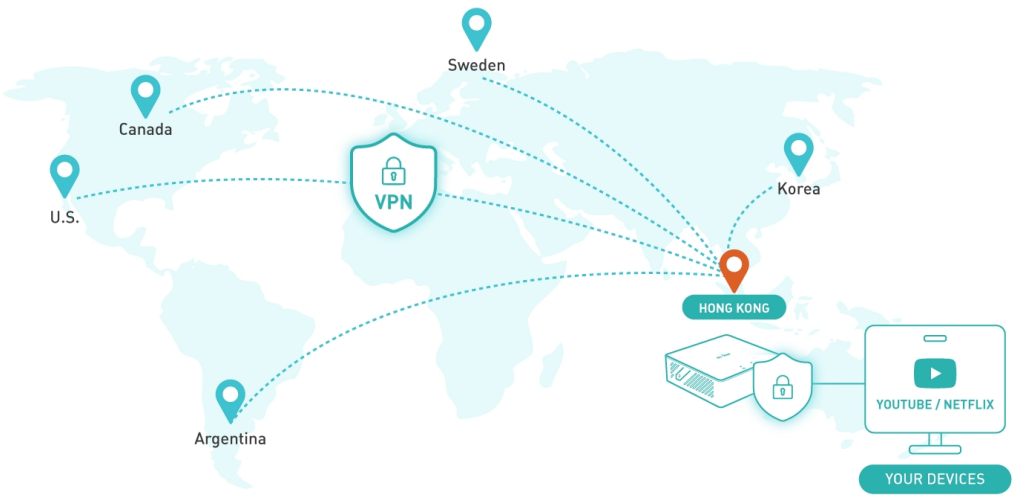
1. Personal Data Privacy

The VPN service is compatible with a wide range of devices via our router, including not just laptops, phones and tablets, but also gaming consoles, TVs, and streaming devices. Your data will be protected whether over wireless or wired connections. You can even customize VPN policies to achieve flexible protection for certain devices.



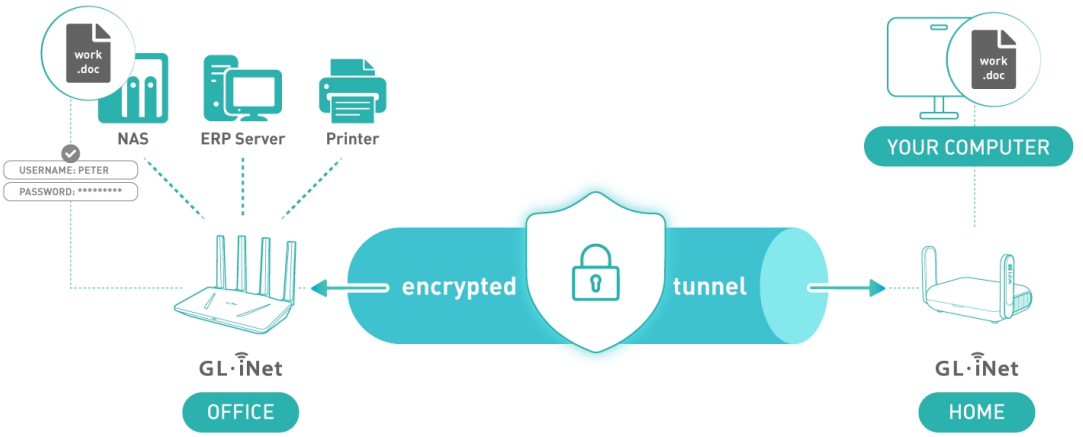
2. Unrestricted Access Worldwide

Accessing some sites may be restricted by location. With VPN enabled, you can unblock any sites when necessary. By connecting to different third-party servers, you will be assigned different IP addresses for surfing or accessing region-blocked sites.



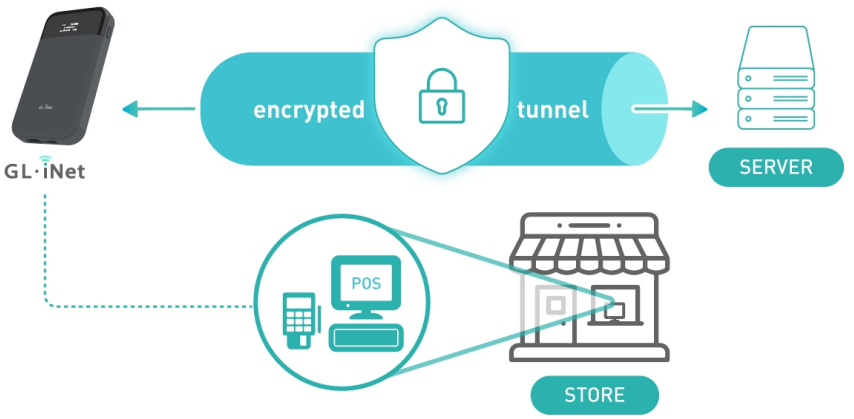
3. Small Business Data Security

Many people work in co-working spaces or cafes and rely on free public Wi- Fi. Such networks are vulnerable to cybercriminal attacks. By configuring your travel router as a VPN client, you can enjoy secure connectivity for work anywhere.



4. Secure Payment Infrastructure

Small retail owners need to handle customers' payment credentials when conducting on-site business. Using a VPN router, their POS machines can upload credit card information via an encrypted VPN tunnel to ensure payment security.



Chapter 8

VPN Dashboard

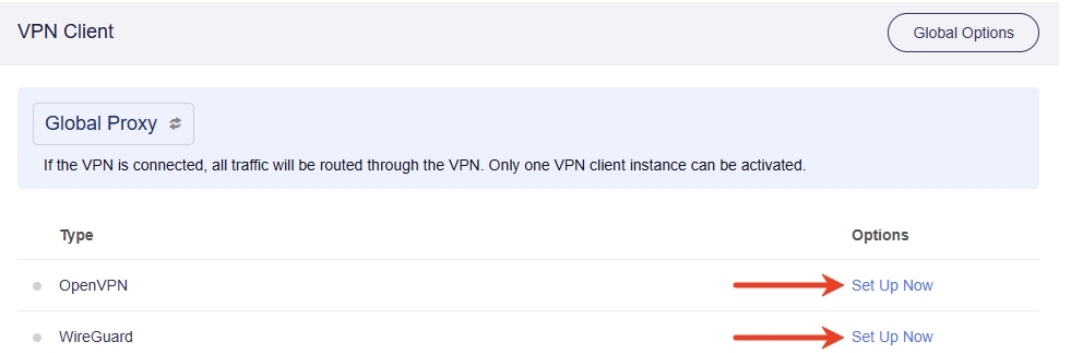
This chapter introduces how to manage VPN connections via the web admin panel.

Log in to the router's web admin panel and navigate to **VPN** > **VPN Dashboard**.

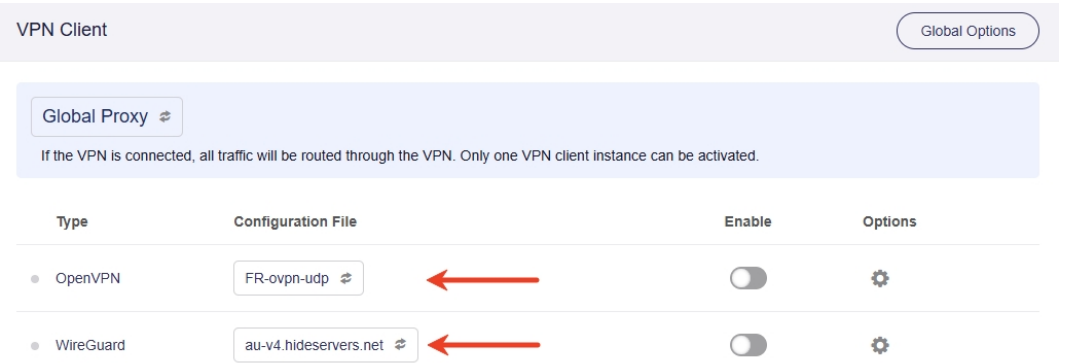
When the router is set as an active VPN client, the VPN dashboard displays VPN connection details, such as server address, traffic statistics, client virtual IP, and connection log. It also allows you to configure advanced settings such as the Block non-VPN traffic, Allow Access WAN, and Services from GL.iNet Use VPN.

8.1 VPN Client

When you enter the **VPN Dashboard** for the first time and no OpenVPN or WireGuard configuration files are available, the page displays as follows. Click **Set Up Now** and you will be directed to the **OpenVPN Client** or **WireGuard Client** page to upload your VPN configuration files.

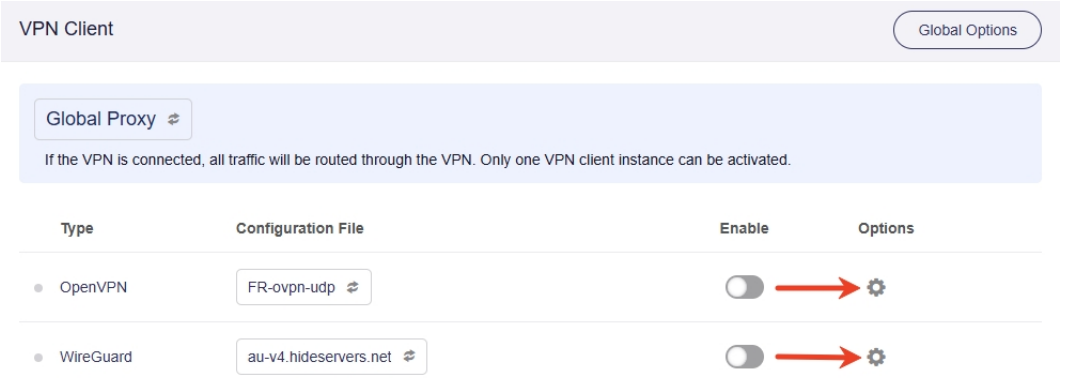


Once uploaded, your configuration will be shown in the **Configuration File** column. If you have multiple configuration files uploaded, you can switch files by clicking on the box.

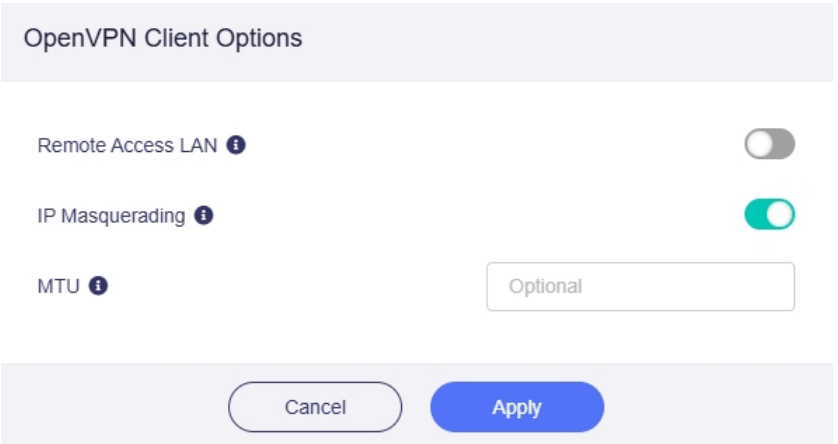


8.1.1 Client Options

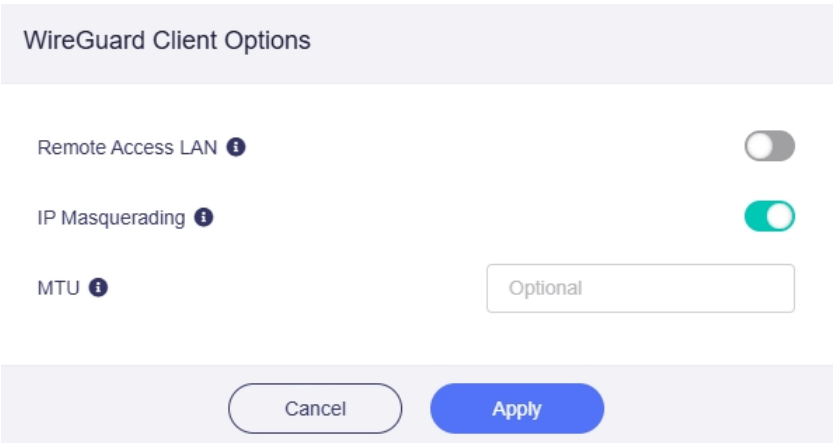
Click the gear icon on the right to access OpenVPN or WireGuard client options.



The OpenVPN Client Options displays as follows.

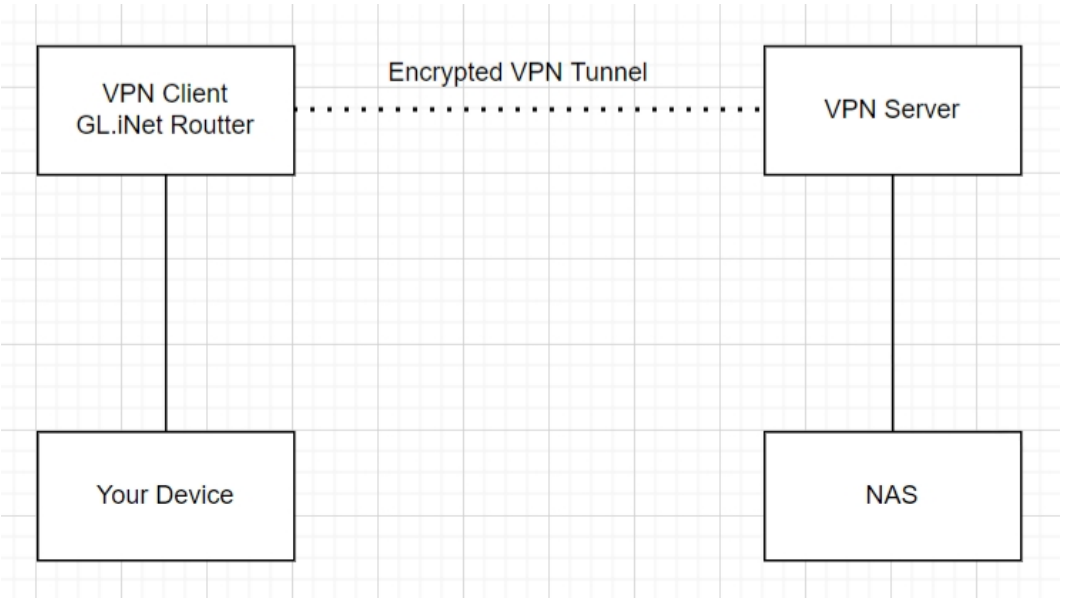


The WireGuard Client Options displays as follows.



- **Remote Access LAN**: If enabled, remote access to this router and its LAN devices via VPN will be allowed. The VPN server must advertise a route to the LAN subnet of this router.

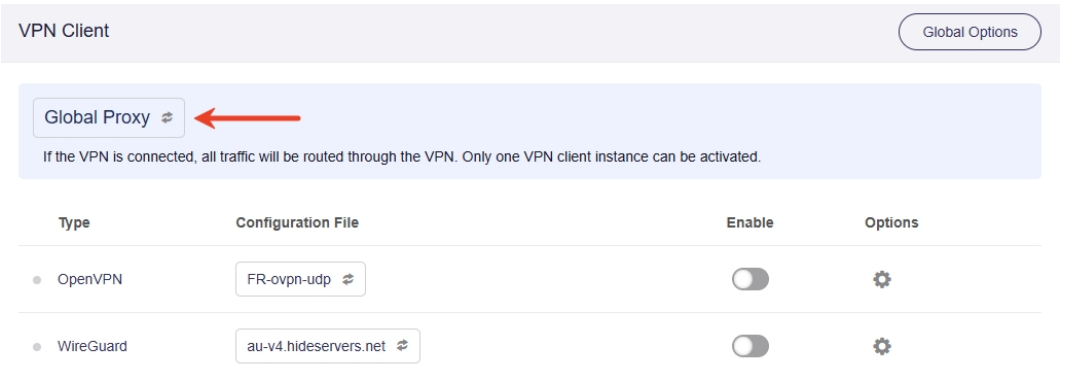
For example, as shown in the diagram below, the GL.iNet router runs as a VPN client and connects to a VPN server over the VPN tunnel. When this option is enabled, both the GL.iNet router and its LAN-side devices can be accessed by devices on the VPN server side (e.g. NAS). This requires you to add a routing rule on the VPN server to reach the LAN subnet of the GL.iNet router.



- **IP Masquerading**: If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU**: Short for Maximum Transmission Unit. This optional setting lets you customize the VPN tunnel MTU, which overrides the value defined in the configuration file.

8.1.2 Policy Mode

The default proxy mode for VPN connection is **Global Proxy**. You can click the box in the upper right to switch to other proxy modes.



Three proxy modes are available: Global Proxy, Policy Mode and Route Mode.

1. **Global Proxy**

   In this mode, all traffic will be routed through the VPN. Only one VPN client instance can be activated.

2. **Policy Mode**

   This mode can be further divided into three policies.

   - **Based on the Target Domain or IP.**

     In this mode, only the traffic of certain websites identified by IP address or domain name will be routed through VPN. Only one VPN client instance can be activated.

   - **Based on the Client Device.**

     In this mode, only the traffic of certain LAN devices identified by MAC addresses will be routed through VPN. Only one VPN client instance can be activated.

   - **Based on the VLAN**.

     In this mode, only the traffic of certain VLAN will be routed through VPN. Only one VPN client instance can be activated.

3. **Route Mode**

   - **Auto Detect**

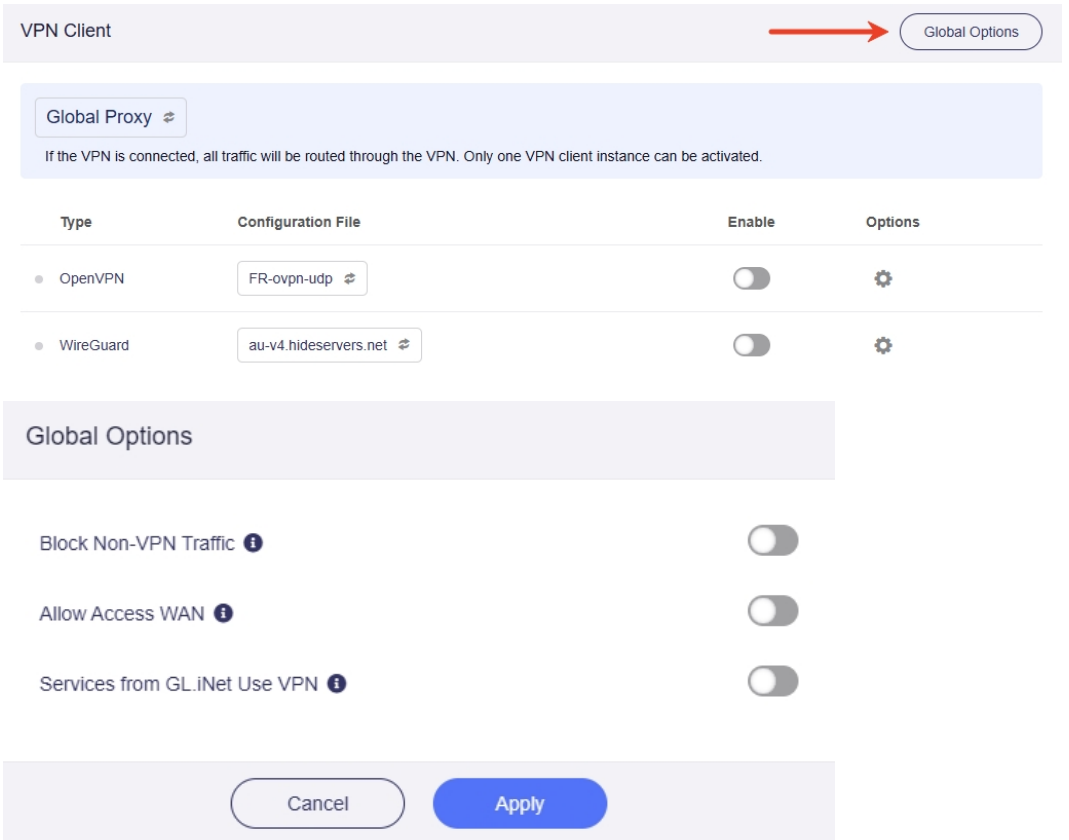
     The routing rules defined in each VPN client configuration file or issued by the VPN server will be used.

   - **Customize Routing Rules**

     You can manually configure routing rules for each VPN client instance.

8.1.3 Global Options

Click **Global Options** in the upper right corner to configure advanced settings for your VPN client.



- **Block Non-VPN Traffic**: If enabled, all internet traffic is forced to pass exclusively through the VPN tunnel and cannot be routed via other interfaces such as the local ISP WAN. If the VPN connection drops unexpectedly, all internet traffic is fully blocked to prevent fallback to the regular WAN. This avoids VPN leaks caused by VPN failures, incorrect client DNS settings, and similar issues.

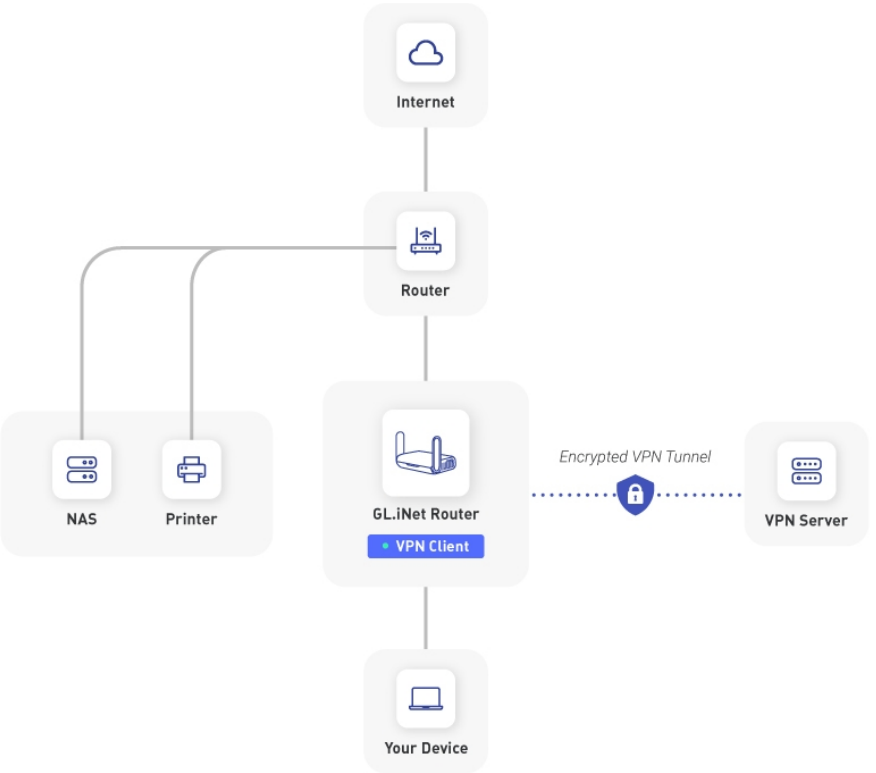
  This feature is also known as VPN Kill Switch. It prevents user data from being exposed online. A typical Kill Switch automatically cuts off internet access when the VPN connection fails. The Block Non-VPN Traffic feature on GL.iNet routers provides broader leak protection and covers the following scenarios:

  a. DNS Leak
  b. IPv6 Leak
  c. WebRTC Leak
  d. VPN Connection Drop

e. Applications Launched Before VPN Establishment

f. Per-Application Traffic Leaks

- **Allow Access WAN**: If enabled, local client devices can still access WAN-side services (e.g., printers, NAS and other devices in the upstream subnet) while the VPN is active.



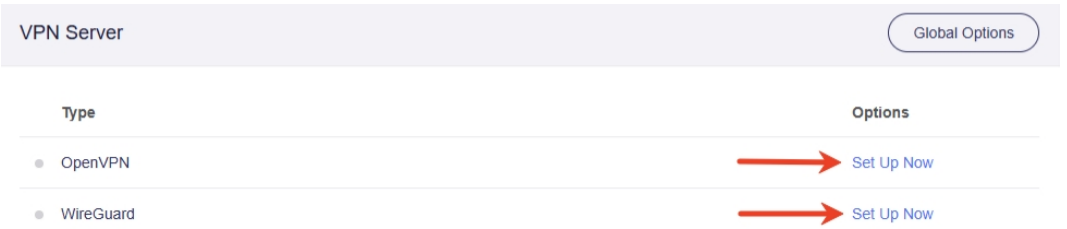
As shown in the diagram above, enabling this feature allows your local devices to reach hosts on the upstream subnet, such as printers and NAS.

This option is primarily designed to let clients access devices within the upstream subnet. However, the router cannot distinguish upstream subnet traffic from regular Internet traffic. If client devices access resources directly via public IPs, there is a potential traffic leakage risk. For this reason, **Allow Access WAN** and **Block Non-VPN Traffic** are mutually exclusive and cannot be enabled simultaneously.

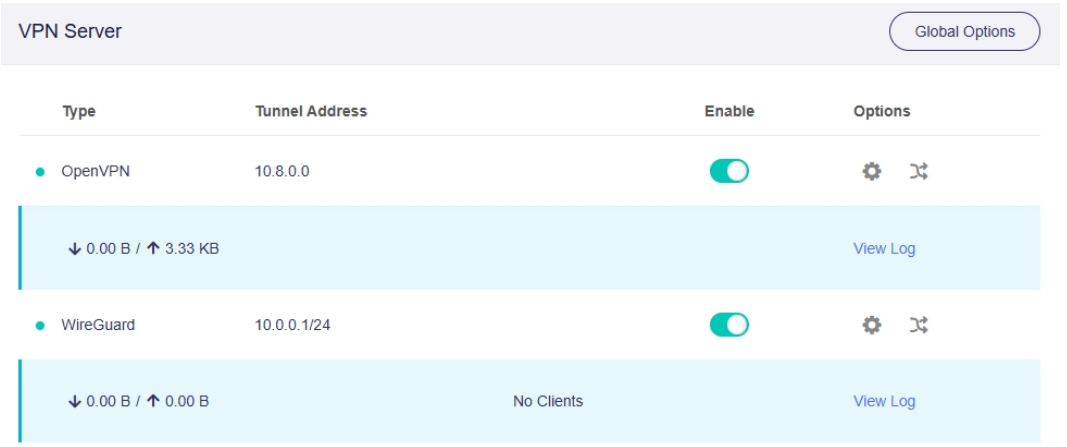
- **Services From GL.iNet Use VPN**: If enabled, GoodCloud, DDNS, and rtty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.

8.2 VPN Server

If the router has never been configured as an OpenVPN or WireGuard server, the page will appear as shown below. Click **Set Up Now** and you will be directed to the **OpenVPN Server** or **WireGuard Server** page to initialize your VPN server.

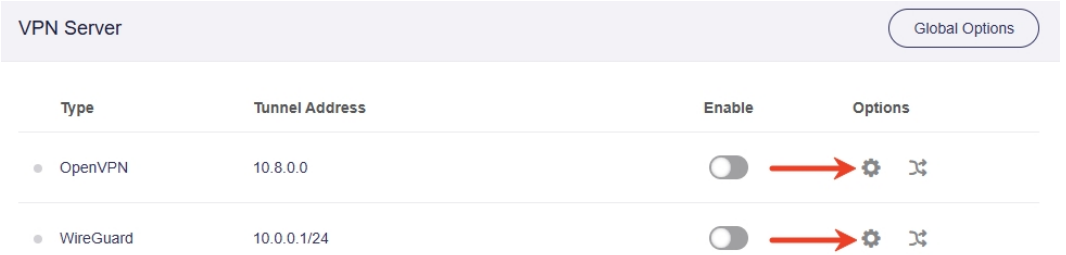


After the OpenVPN Server or WireGuard Server is enabled, the page will display the server status as follows.

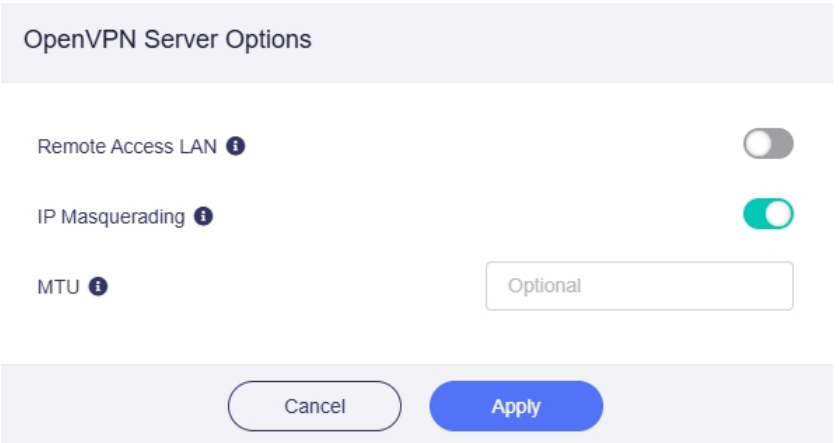


8.2.1 Server Options

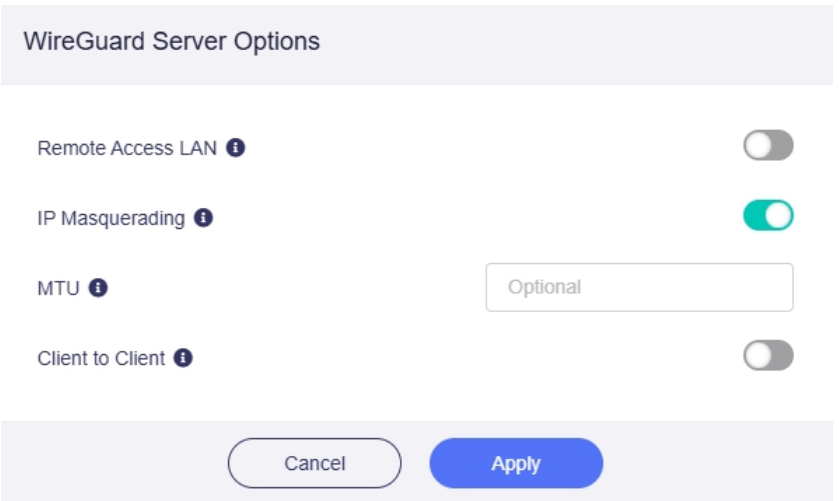
Click the gear icon on the right to access OpenVPN or WireGuard server options.



The OpenVPN Server Options displays as follows.



The WireGuard Server Options displays as follows.

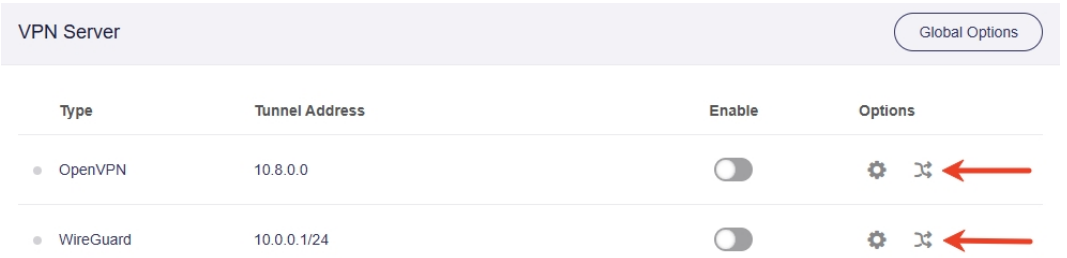


- **Remote Access LAN**: If enabled, resources inside the server's LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading**: If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.

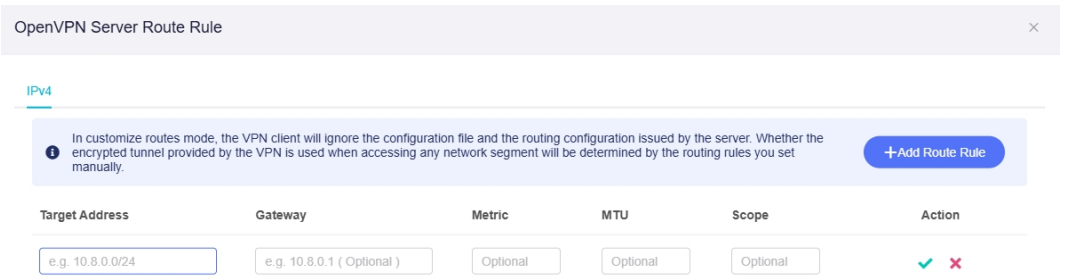
- **MTU**: Short for Maximum Transmission Unit. The MTU value you set for the tunnel will override the MTU settings in the configuration file.
- **Client to Client**: If enabled, VPN clients connected to this server can access each other via their VPN tunnel IPs. If you want to allow clients to also access one another's LAN subnets, you need to add routing rules on the VPN server to advertise those remote LAN subnets.

8.2.2 Server Route Rule

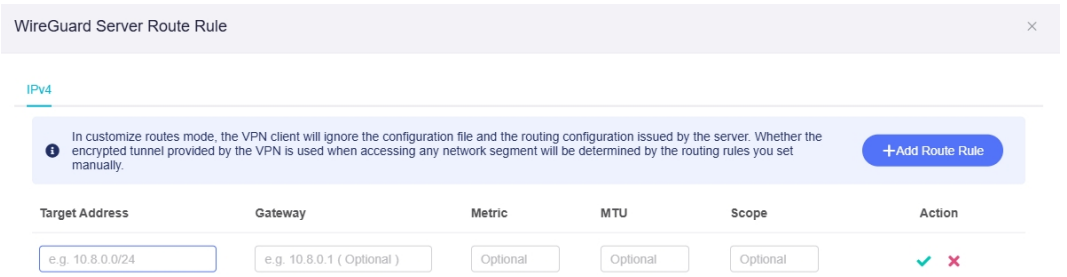
Click the route icon on the right to customize OpenVPN or WireGuard route rules as needed.



The OpenVPN Server Route Rule displays as follows. Click **Add Route Rule**, enter the **Target Address** and **Gateway**, then click the green check icon to apply.



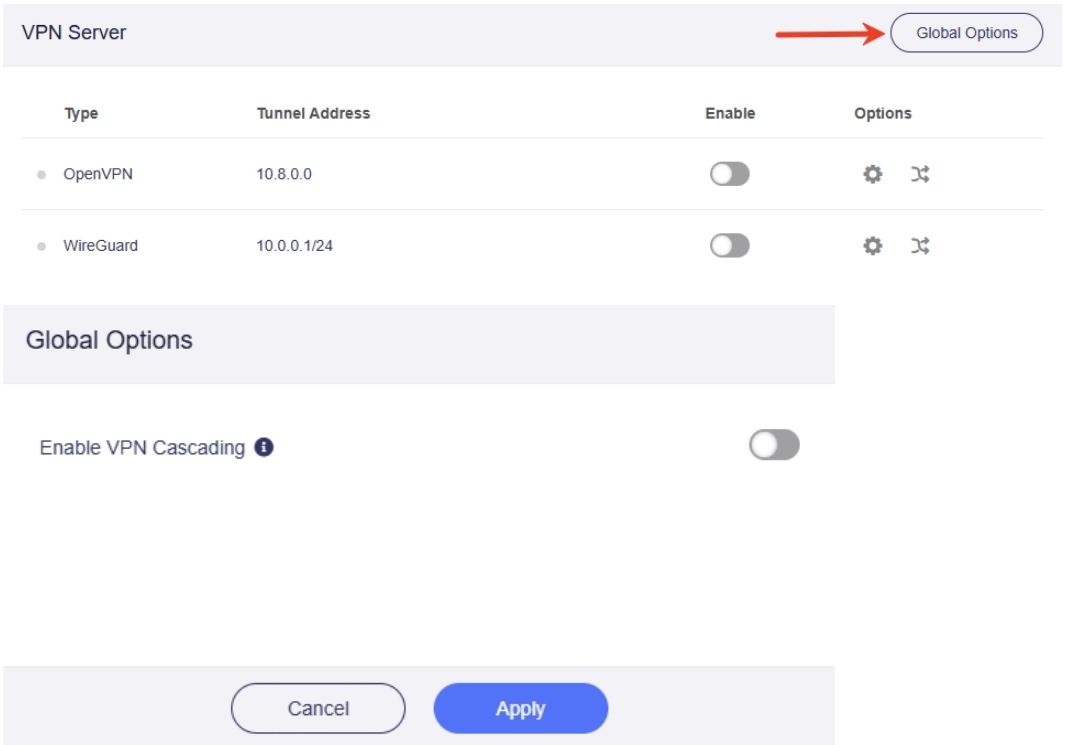
The WireGuard Server Route Rule displays as follows. Click **Add Route Rule**, enter the **Target Address** and **Gateway**, then click the green check icon to apply.



Note: In customize routes mode, the VPN client will ignore the configuration file and the routing configuration issued by the server. Whether to use the VPN encrypted tunnel when accessing any network segment is determined by the routing rules you manually set.

8.2.3 Global Options

Click **Global Options** in the upper right corner to configure advanced settings for your VPN server.



If **VPN Cascading** is enabled, when this router acts as a VPN server and a VPN client simultaneously, remote VPN clients connected to this router's VPN server will have their traffic routed through the upstream VPN tunnel that this router is using as a VPN client. Learn more about VPN Cascading.

Chapter 9

Set Up VPN Server

This chapter introduces how to set up a GL.iNet router as OpenVPN or WireGuard server.

9.1 Set Up OpenVPN Server

OpenVPN is an open-source VPN protocol that utilizes SSL/TLS encryption for secure point-to-point and site-to-site connections. To set up OpenVPN server on a GL.iNet router, watch this video or refer to the steps below.

9.1.1 Preparation

1. **Make sure you have a public IP address**

   Click here to verify if your Internet Service Provider (ISP) assigns you a public IP address. If not, your router cannot be set as an OpenVPN server.

   Alternative methods:

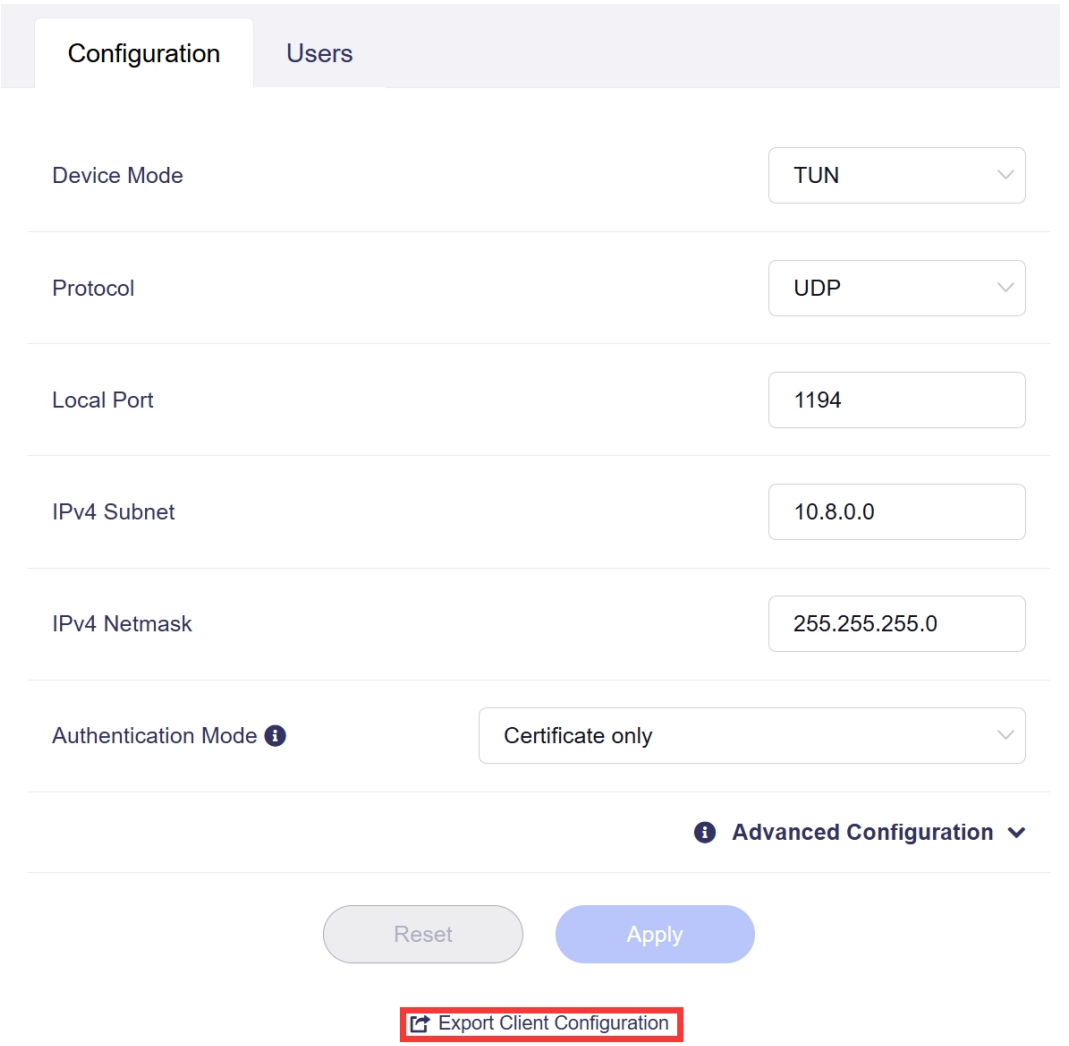
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.

2. **Confirm if Port Forwarding is required**

   - If your GL.iNet router is the primary router in your network, no port forwarding setup is required. Proceed to the next step.
   - If a primary router is already in use and your GL.iNet router is configured as a secondary router, you will need to configure port forwarding on the primary router.
   - If your GL.iNet router is multiple levels downstream from the primary router, configure port forwarding on each intermediate device.

9.1.2 Setup Steps

1. Log in to the router's web admin panel, navigate to **VPN** > **OpenVPN Server**, then click **Generate Configuration** (for VPN server initial setup only).
2. Apply the configuration.
   The default configuration works for most cases. Click **Export Client Configuration** at the bottom and proceed to step 3. If you have modified the configuration, click **Apply** before exporting it.



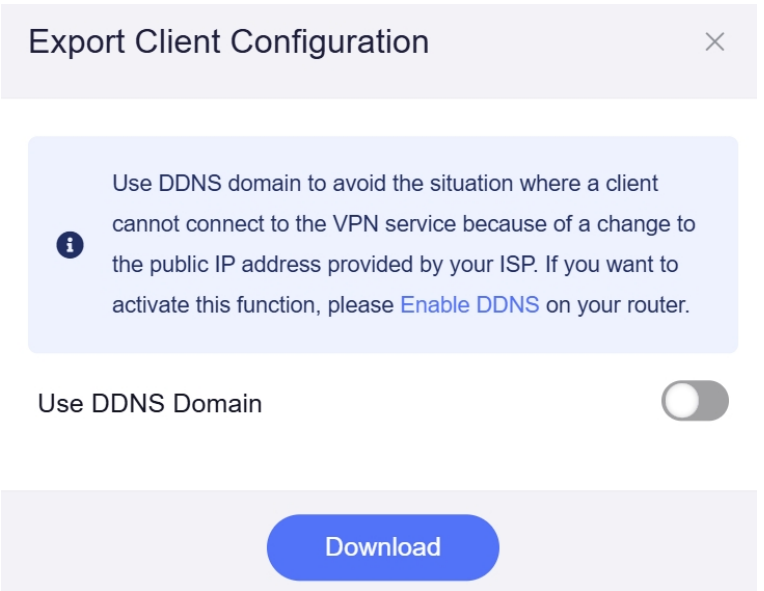
- **Device Mode**: TAP-S2S or Tun. See here for the differences.
- **Protocol**: UDP or TCP. See here for the differences.
- **Authentication Mode**: This determines the authentication method used when the client connects to the server. There are three options:

- **Certificate Only**: If selected, the router will automatically generate a server and client certificate keys and embed them in the configuration file. When you upload the configuration to the client, no additional credentials are required.
- **Username/Password Only**: If selected, the router will generate client configuration without certificate keys. You need to first add a username and password in the **Users** tab before exporting the client configuration. When uploading the configuration to the client, enter these credentials for authentication.
- **Username/Password and Certificate**: If selected, you need to first add a username and password in the **Users** tab before exporting the client configuration; second, the router will automatically generate server and client certificate keys and embed them in the configuration file. When uploading the configuration to the client, the certificate-key will be verified first, followed by username/password authentication for 2FA security.

- **Advanced Configuration**: Customize more server settings if needed.

3. Export Client Configuration.

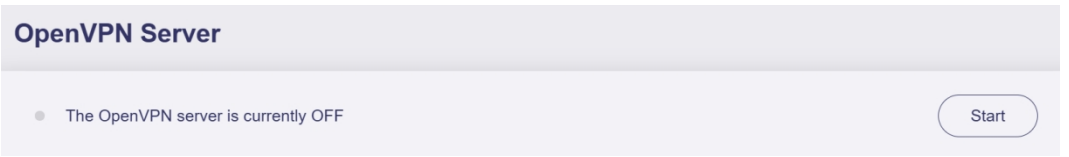
   After clicking **Export Client Configuration** at the bottom of the Configuration tab (or applying the modified configuration), a window will pop up as follows. Click **Download** to export the configuration.



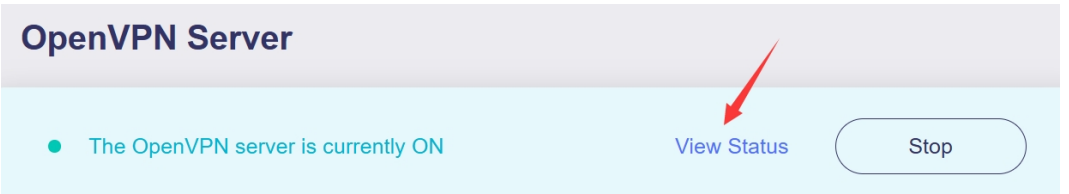
   Tip: If your public IP address changes frequently, go to **APPLICATIONS** > **Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.

4. Start OpenVPN server.

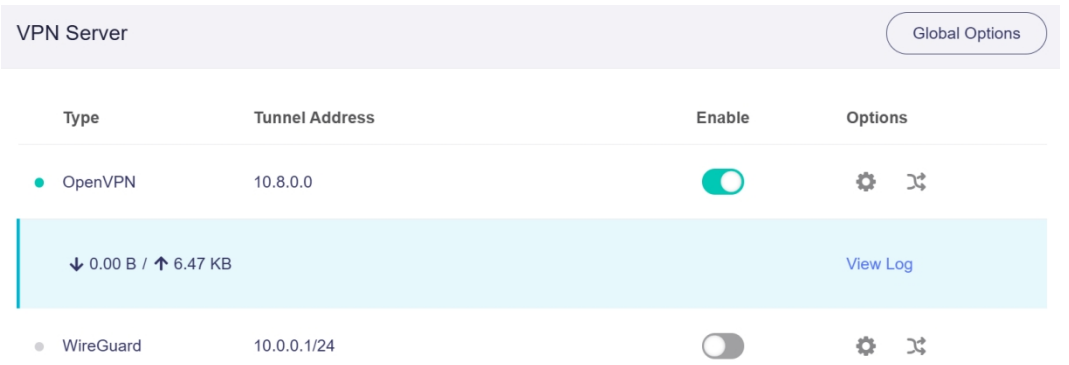
On the **OpenVPN Server** page, click the **Start** button in the upper right corner to start the server.



If you want to view the server connection status, click **View Status**.



You will be redirected to the VPN Dashboard. If theupload and download traffic statistics are displayed in this page, the OpenVPN server is running.



9.1.3 Troubleshooting

If the connection fails, there are several common reasons:

- The VPN server does not have a public IP address. See here for troubleshooting.
- You may need to set up port forwarding. See here for troubleshooting.
- The port used for the OpenVPN Server is blocked by your Internet Service Provider. Change to another port, or contact your ISP for assistance.
- The VPN connection may be blocked in certain countries or regions.

9.2 Set Up WireGuard Server

WireGuard® is a simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. To set up WireGuard server on a GL.iNet router, watch this video or refer to the steps below.

9.2.1 Preparation

1. **Make sure you have a public IP address**

   Click here to verify if your Internet Service Provider assigns you a public IP address. If not, your router cannot be set as a WireGuard Server.

   Alternative methods:

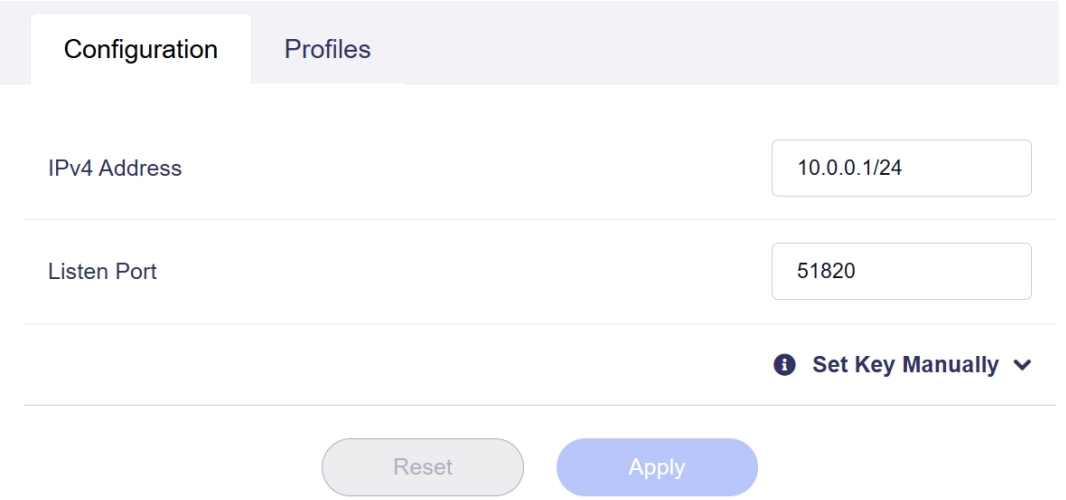
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.

2. **Confirm if Port Forwarding is required**

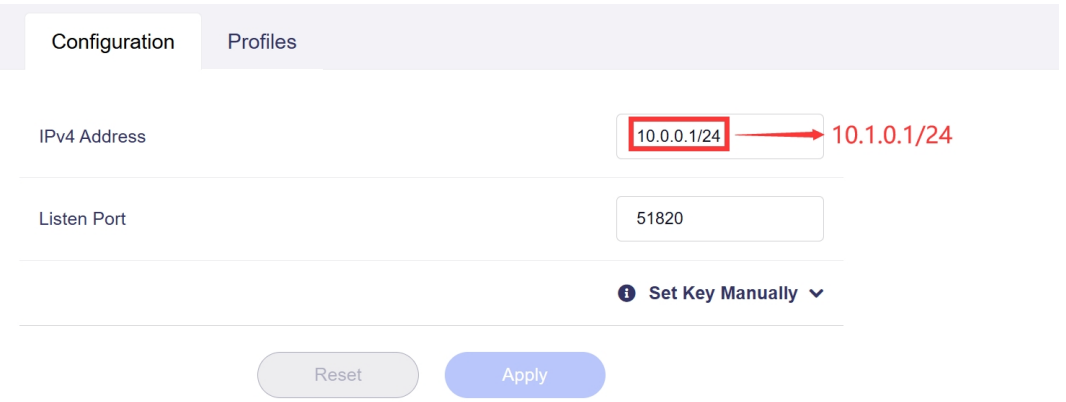
   - If your GL.iNet router is the primary router in your network, no port forwarding setup is required. Proceed to the next step.
   - If a primary router is already in use and your GL.iNet router is configured as a secondary router, you will need to configure port forwarding on the primary router.
   - If your GL.iNet router is multiple levels downstream from the primary router, configure port forwarding on each intermediate device.

9.2.2 Setup Steps

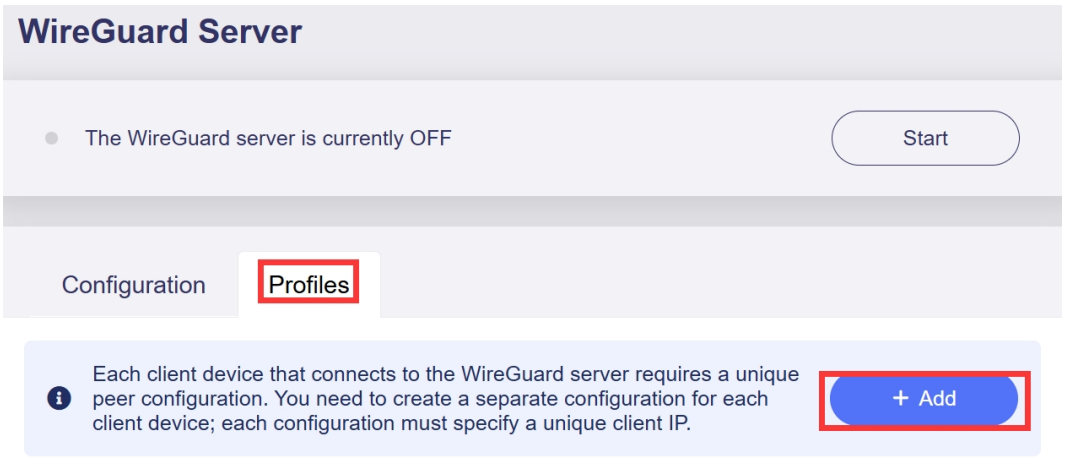
1. Log in to the router's web admin panel, navigate to **VPN** > **WireGuard Server**, then click **Generate Configuration** (for VPN server initial setup only).
2. Apply the configuration.
   The default configuration works for most cases. No need to modify the IPv4 address unless it conflicts with your upstream router's gateway.



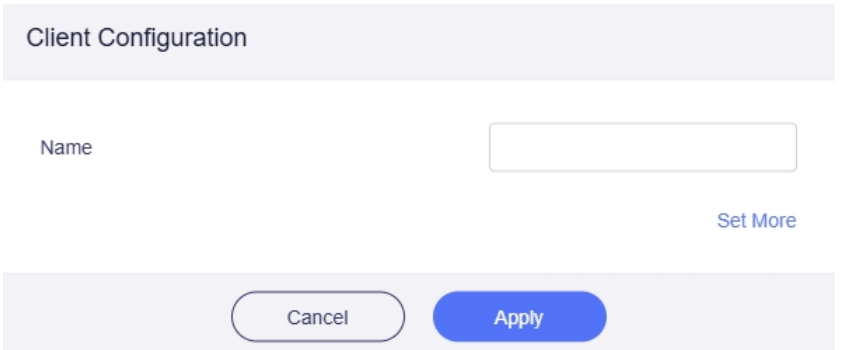
   If the IPv4 address conflicts with your upstream router's gateway, modify the IPv4 address to another one (e.g., **10.1.0.1/24**) and click **Apply**. Ensure the "/24" CIDR notation is included to avoid connectivity issues.



3. Add a profile.
   Switch to **Profiles** tab, click the **Add** button to generate a profile for your device.



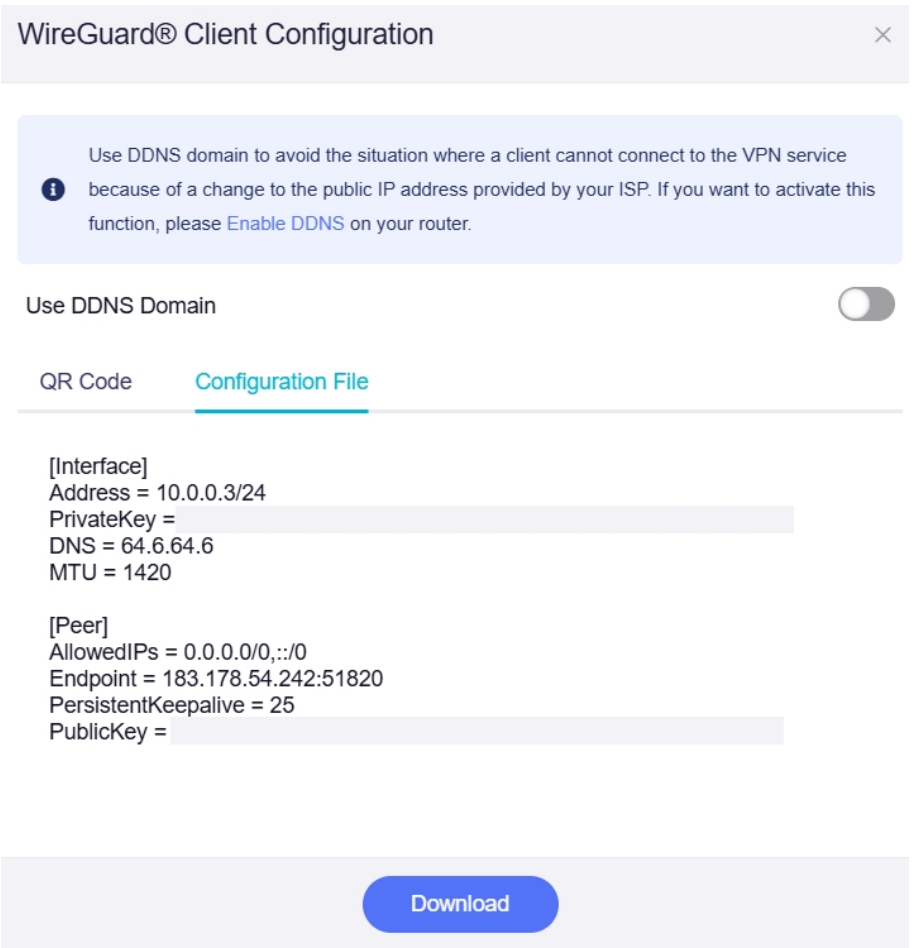
Set a descriptive name and click **Apply** to continue.



4. Download configuration.

   After adding a profile, the router will generate a configuration file in three formats: QR code, plain text, and .conf file. Choose your preferred method to obtain the configuration file.

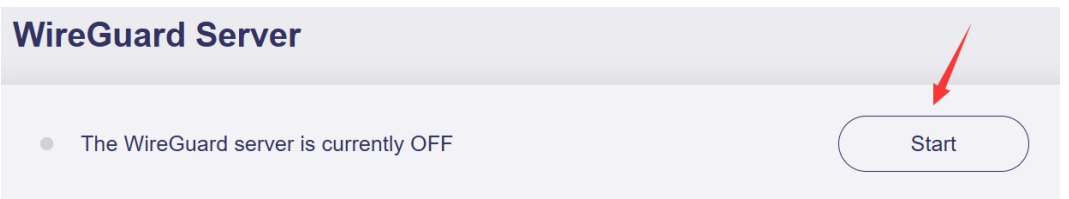
   - **QR code**: Suitable for devices (e.g., smartphones, tablets, laptops) with the WireGuard App installed. If you want to set a specific device as a WireGuard client, simply open the WireGuard App and scan the QR code to import a configuration file.
   - **Plain text**: In plain text format, you can review configuration details and conveniently copy-paste them elsewhere for manual configuration, such as the WireGuard App or a GL.iNet router.
   - **.conf file**: Click the **Download** button to save the .conf file to your local device. It is also convenient and can be directly uploaded to the WireGuard app or a GL.iNet router.



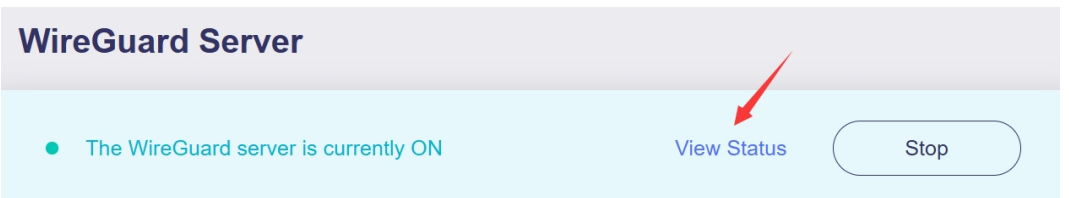
Tip: If your public IP address changes frequently, go to **APPLICATIONS** > **Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.

5. Start WireGuard server.

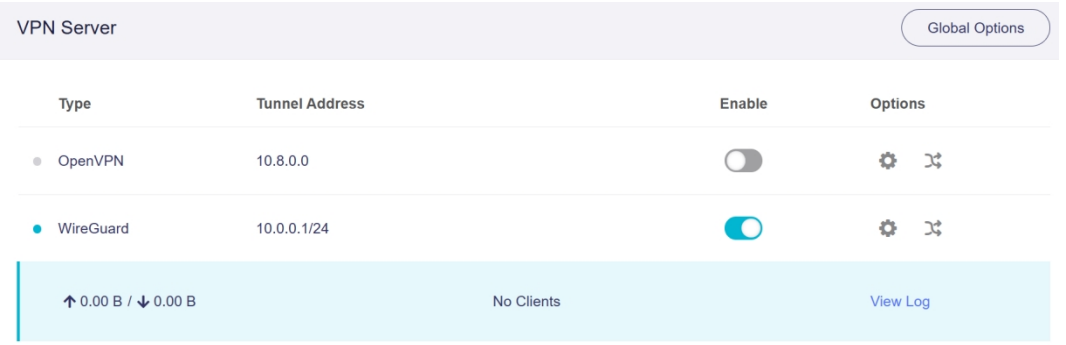
   On the **WireGuard Server** page, click the **Start** button in the upper right corner to start the server.



If you want to view the server connection status, click **View Status**.



You will be redirected to the VPN Dashboard. If theupload and download traffic statistics are displayed in this page, the OpenVPN server is running.



9.2.3 Troubleshooting

If the connection fails, there are several common reasons:

- The VPN server does not have a public IP address. See here for troubleshooting.
- You may need to set up port forwarding. See here for troubleshooting.
- The port used for the WireGuard Server is blocked by your Internet Service Provider. Change to another port, or contact your ISP for assistance.
- The VPN connection may be blocked in certain countries or regions.

Chapter 10

Set Up VPN Client

This chapter introduces how to set up a GL.iNet router as OpenVPN or WireGuard client.

10.1 Set Up OpenVPN Client

10.1.1 Preparation

First, ensure you have an active subscription with a VPN service provider that supports manual OpenVPN configuration. See here for the OpenVPN providers compatible with GL.iNet.

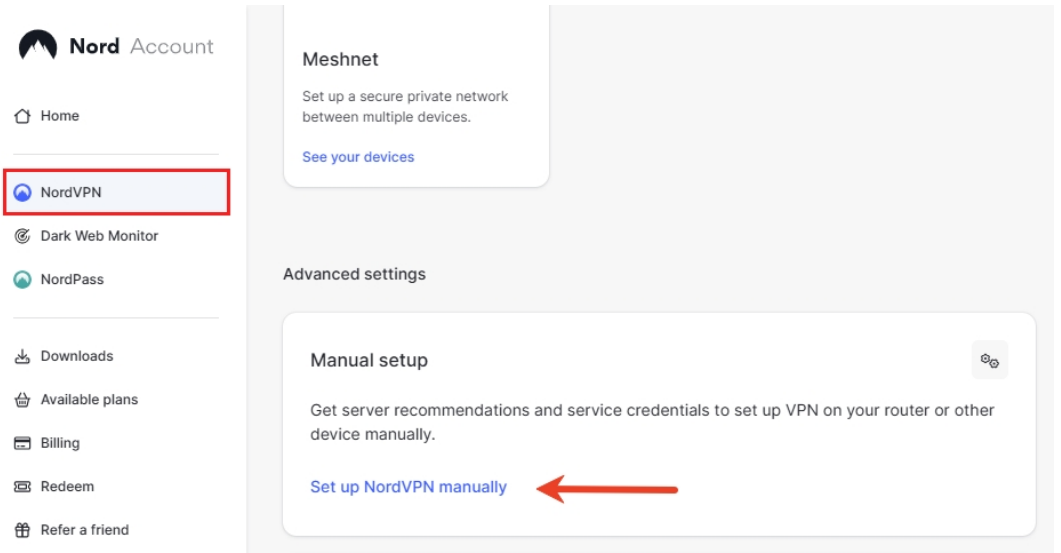
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to this link or contact their support.

10.1.2 Set Up NordVPN

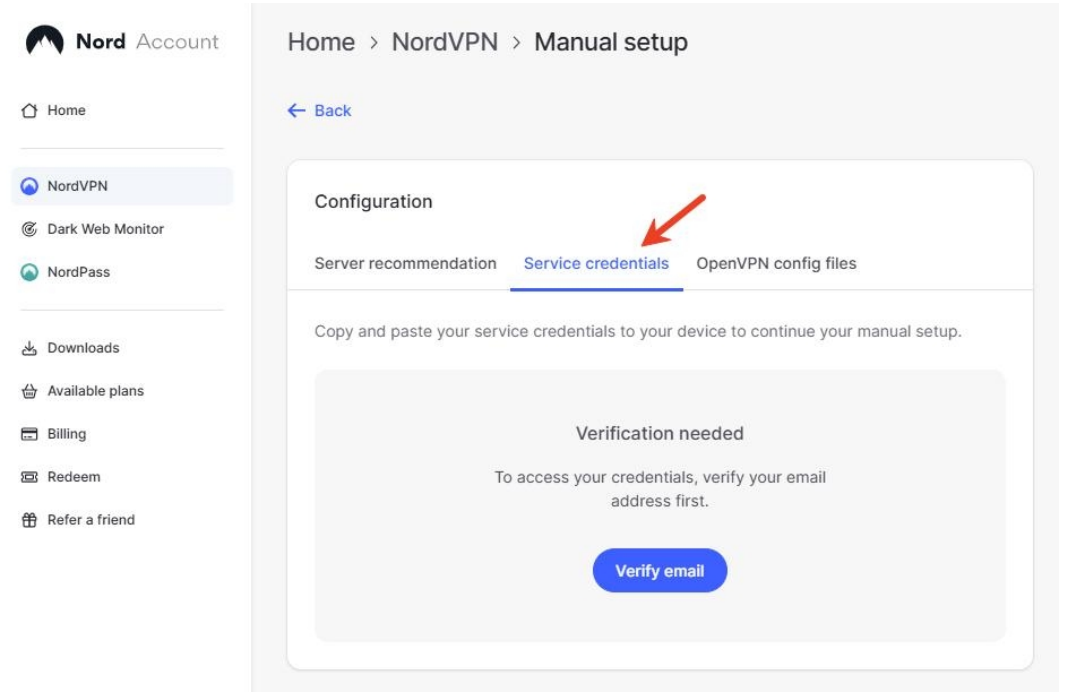
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

Follow the steps below to set your router as a NordVPN client.

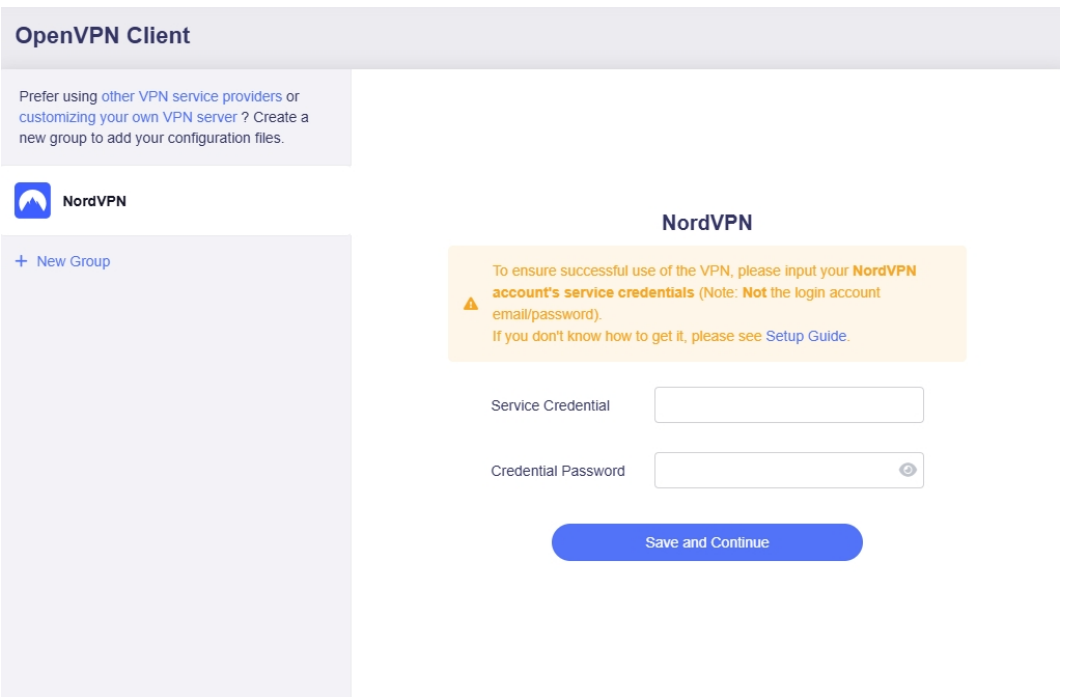
1. Log in to your NordVPN web account here.
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



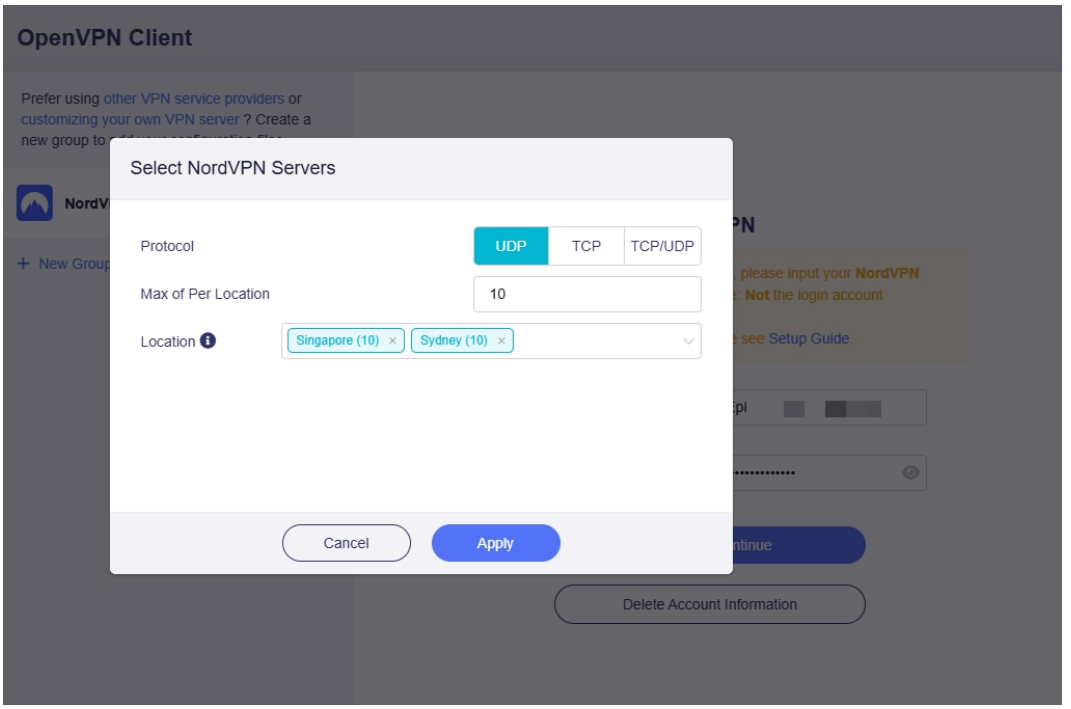
You will find the **service credentials**. Copy them for later use.



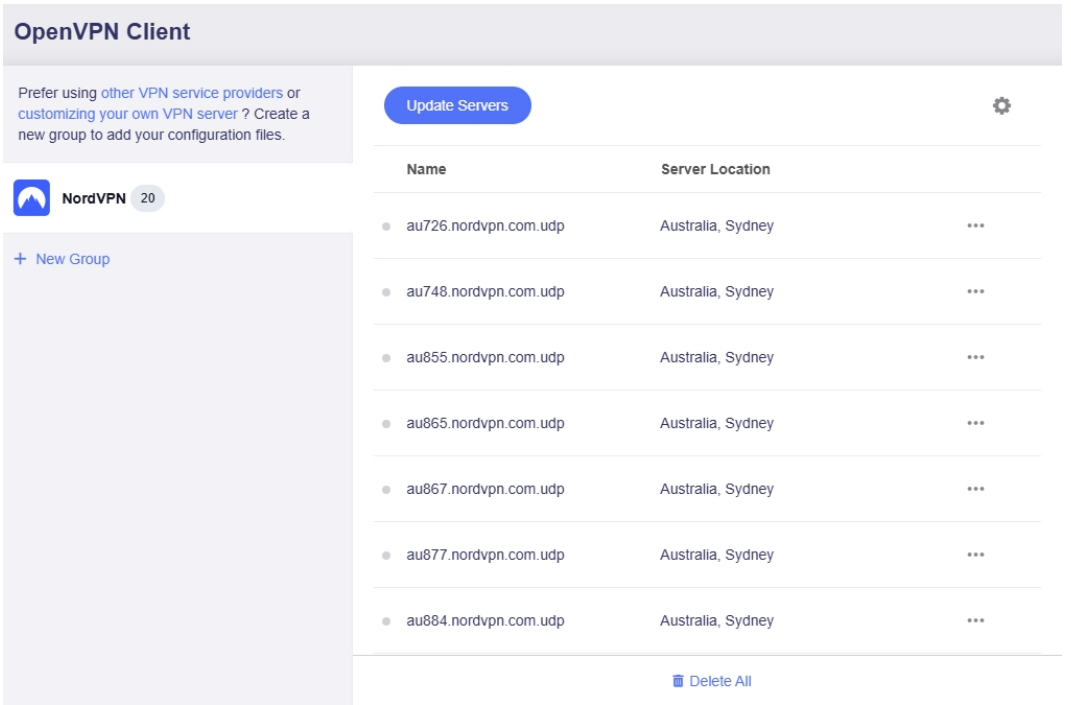
3. Log in to your router's web admin panel and navigate to **VPN** > **OpenVPN Client** > **NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



4. Select protocol, max server count of each location and locations, then click **Apply**.

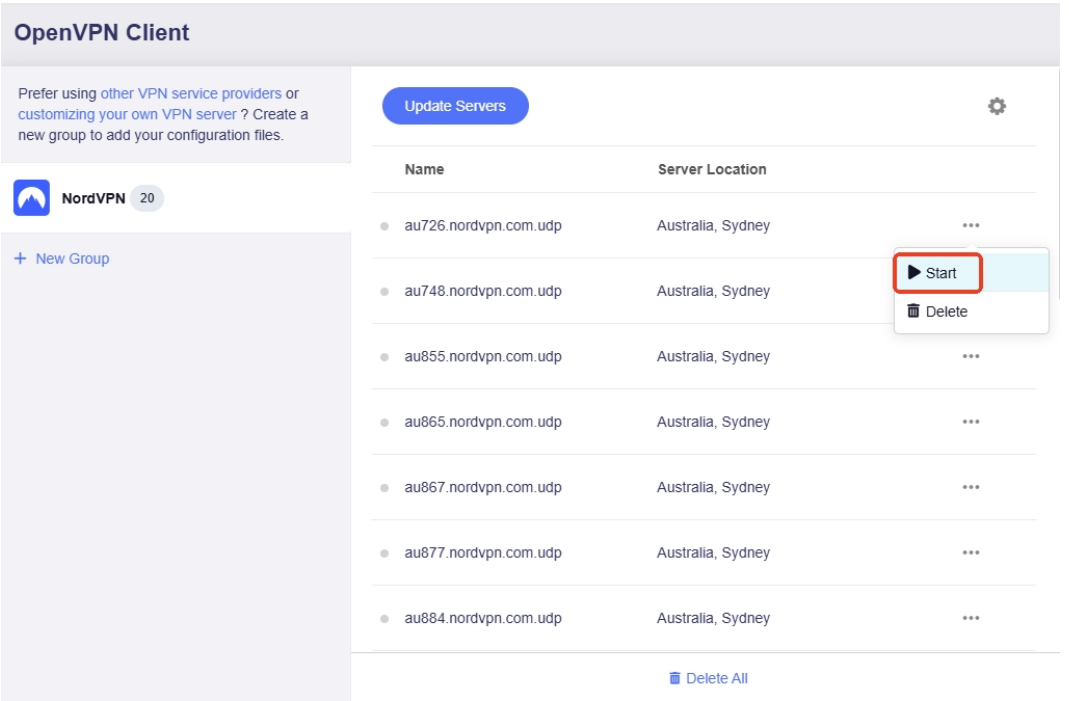


It will download configuration files.

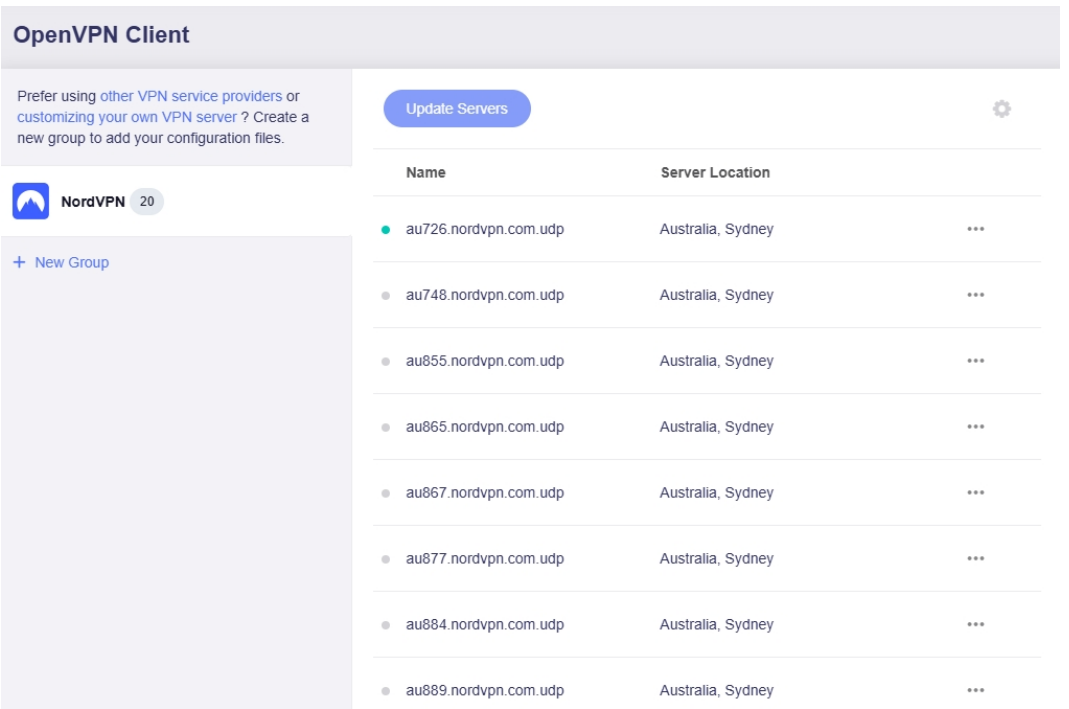


5. Start a connection.

   Select a server, and click the three-dot icon on the right to start a connection.



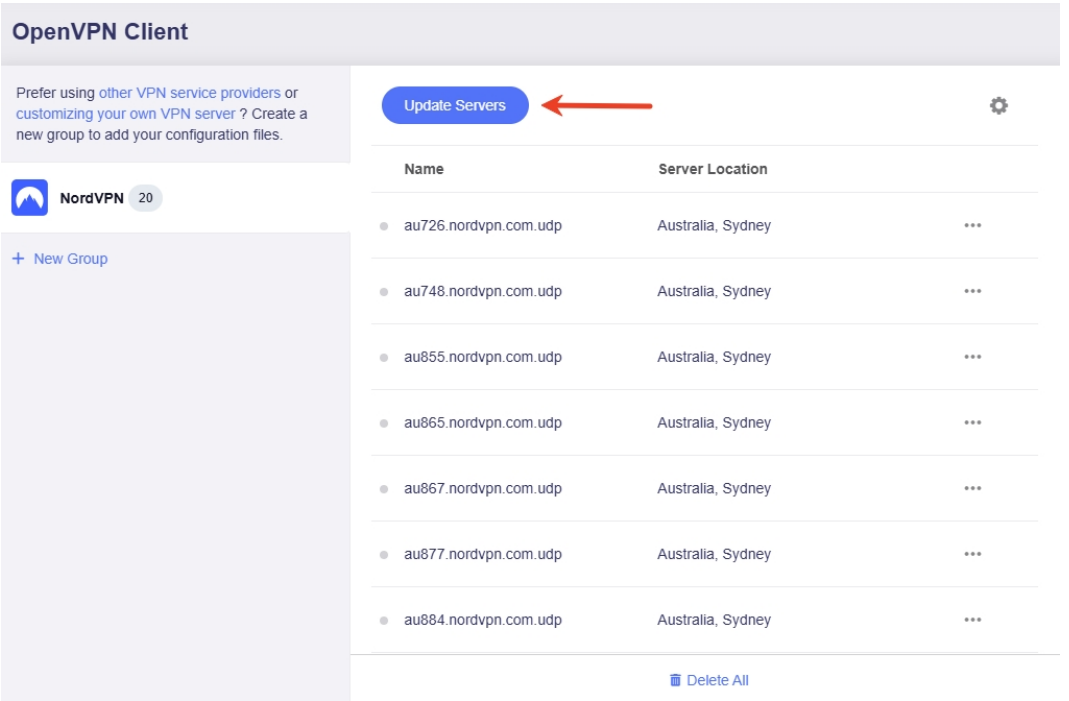
6. Once connected, a green dot will appear next to the configuration file.



You can also check the VPN connection details on the **VPN Dashboard**.

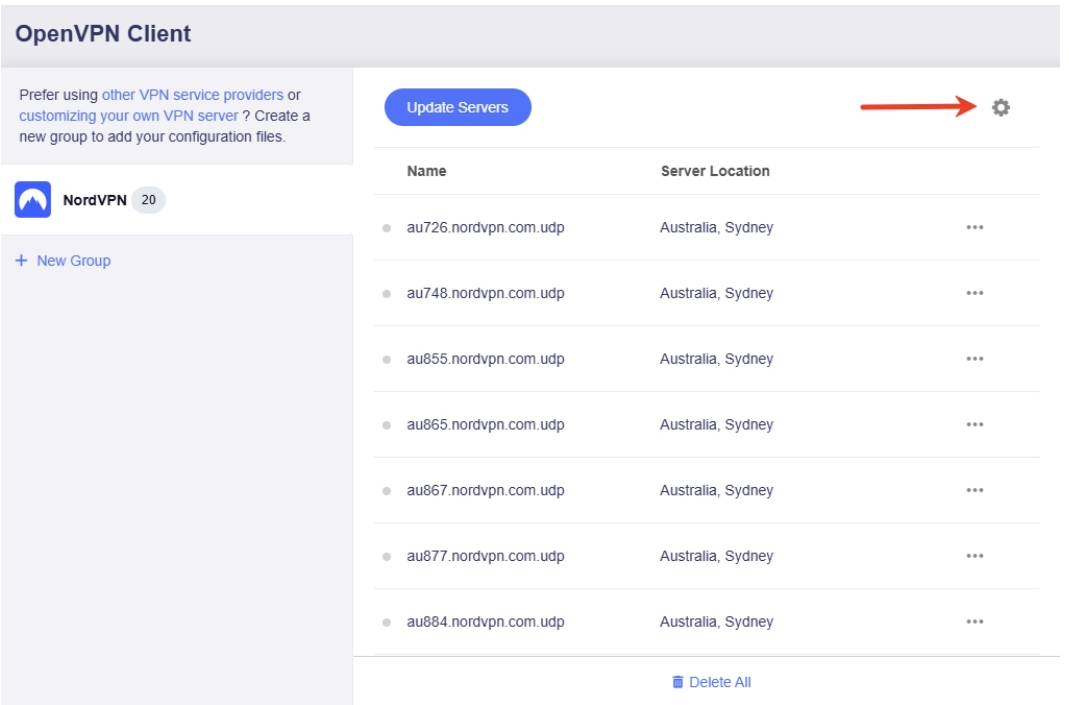
7. Update servers.

   You can click **Update Servers** to obtain the latest available server list, avoiding connection failures caused by server maintenance or shutdown.



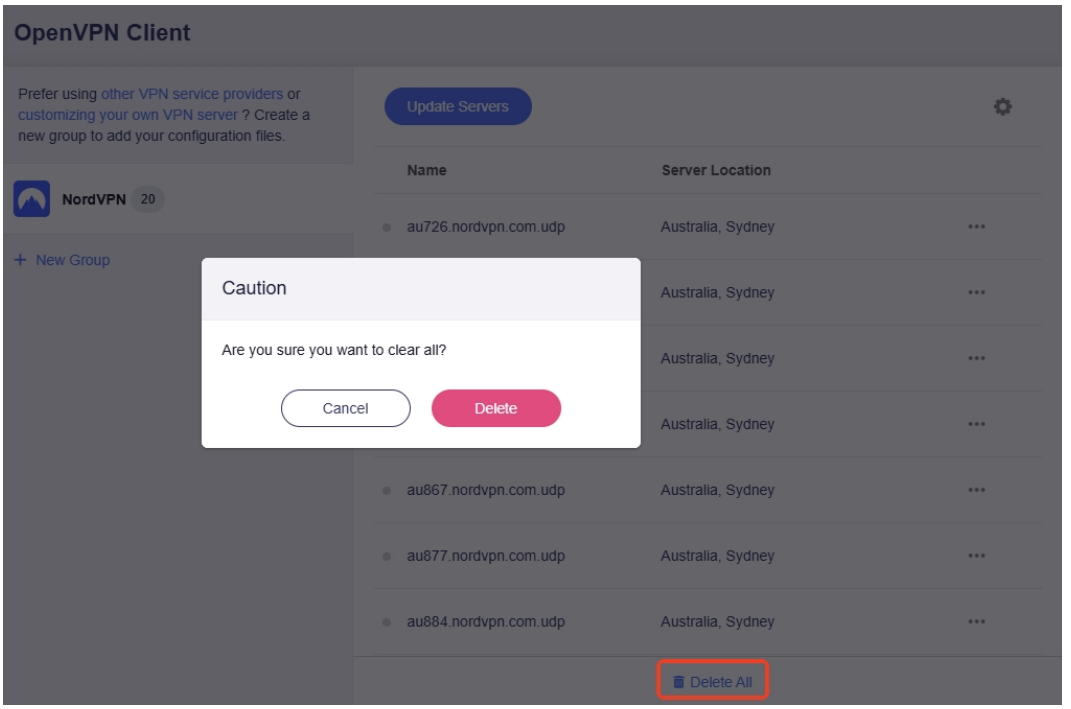
8. Edit credentials.

   Click the gear icon to edit your login credentials.



9. Delete all files.

   You can click **Delete All** to delete all configuration files with one click.

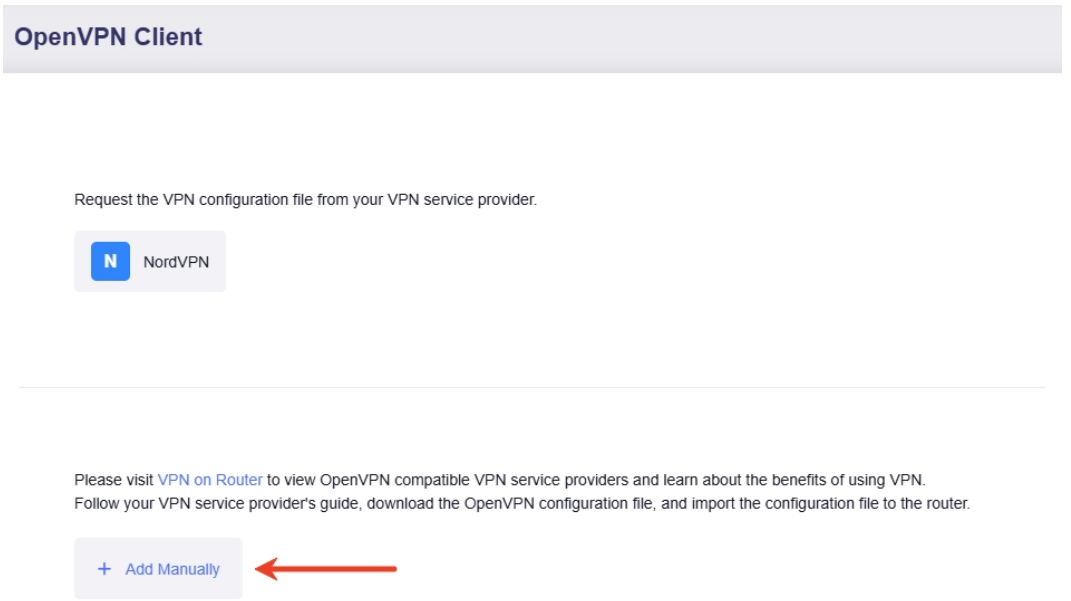

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp
Australia, Sydney
au877.nordvpn.com.udp
Australia, Sydney
au884.nordvpn.com.udp
Australia, Sydney
Delete All
Caution
Are you sure you want to clear all?
Cancel
Delete

10.1.3 Set Up OpenVPN Client Manually (for other providers)

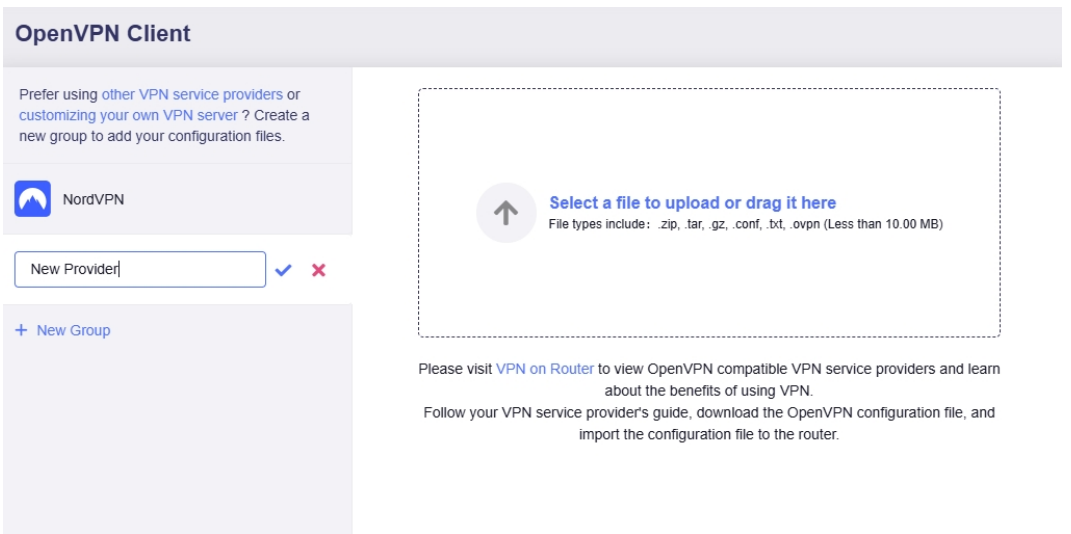
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

In the following steps, we will use PIA (Private Internet Access) as an example.

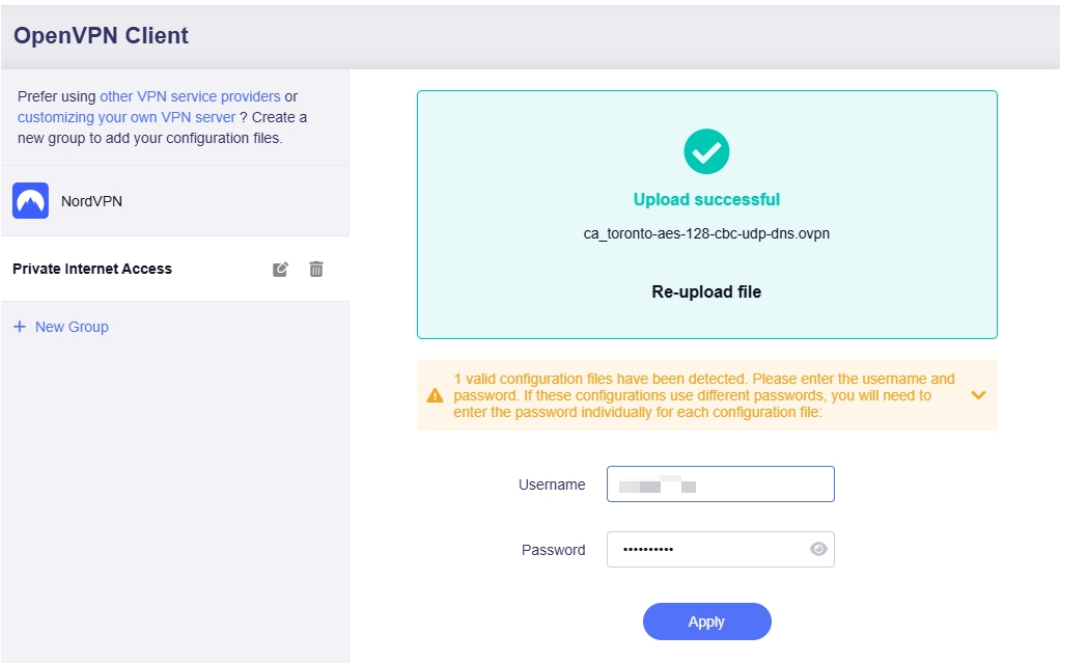
1. Download a configuration file from Private Internet Access official website.
2. Log in to your router's web admin panel, navigate to **VPN** > **OpenVPN Client**, and click **Add Manually**.



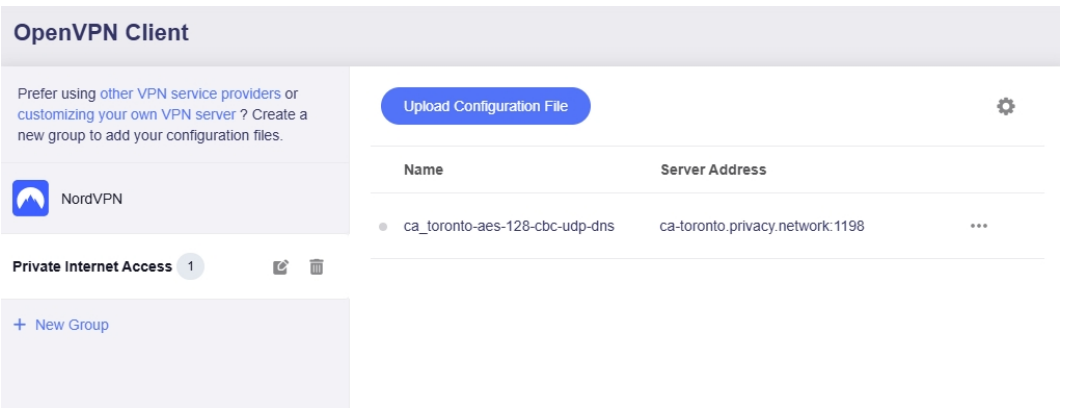
3. It will create a group on the left sidebar. Set a descriptive name for the group.



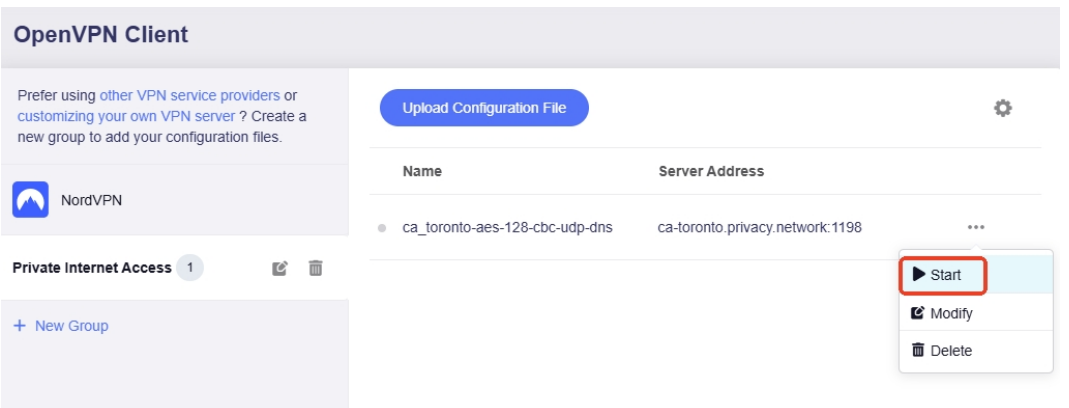
4. Upload your OpenVPN configuration file. Input the credentials if required, then click **Apply**.



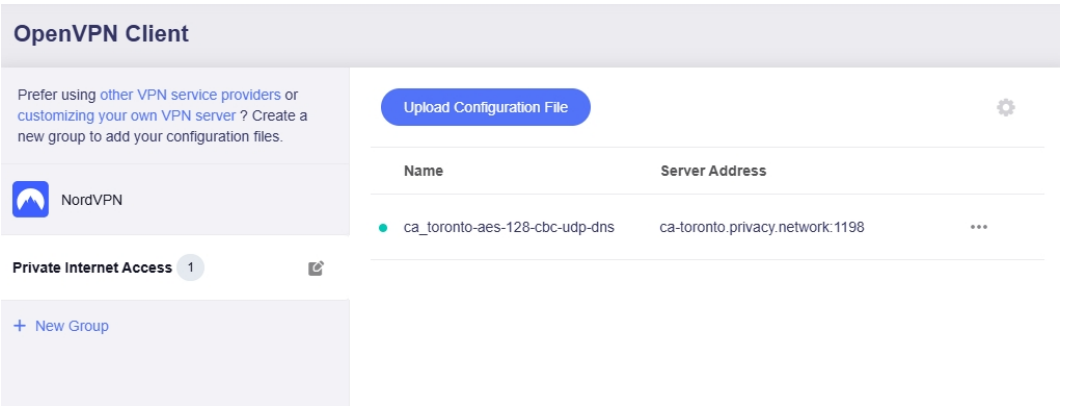
You will see the configuration file uploaded.



5. Click the three-dot icon on the right to start a connection.



6. Once connected, a green dot will appear next to the configuration file.



You can also check the VPN connection details on the **VPN Dashboard**.

10.2 Set Up WireGuard Client

You can set up WireGuard Client via the GL.iNet mobile app or the web admin panel.

- The mobile app integrates some WireGuard service providers, such as AzireVPN, Mullvad VPN, OVPN, StrongVPN, PIA VPN. You can set it up easily by entering the login credentials of the WireGuard service you subscribed to. Open the app and follow the on-screen instructions to set up.
- The web admin panel not only integrates some WireGuard service providers, but also provides an entry for manual configuration. You can either enter the credentials of your subscribed WireGuard service for quick setup, or manually upload a configuration file to complete the setup.

10.2.1 Preparation

First, ensure you have an active subscription with a VPN service provider that supports manual WireGuard configuration. See here for the WireGuard providers compatible with GL.iNet.

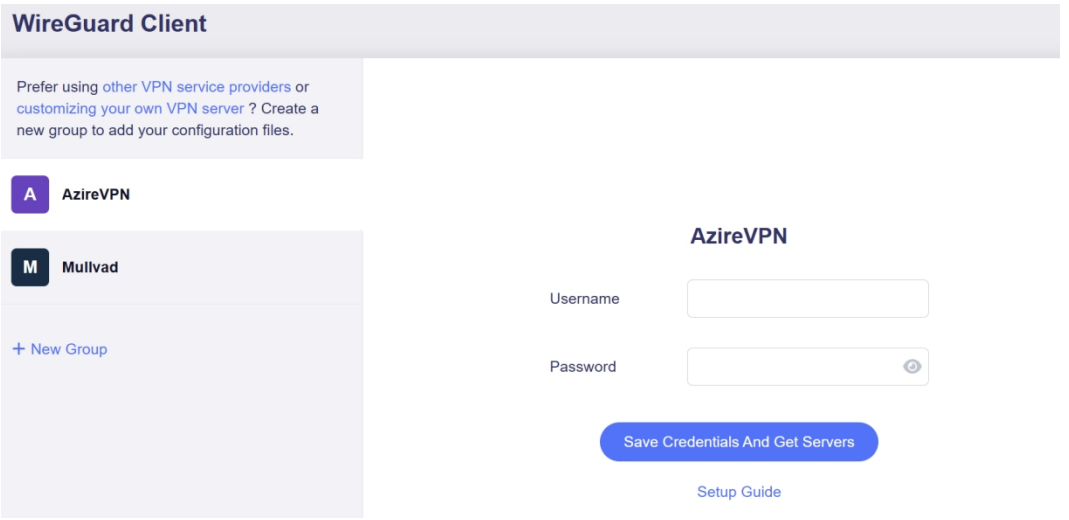
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

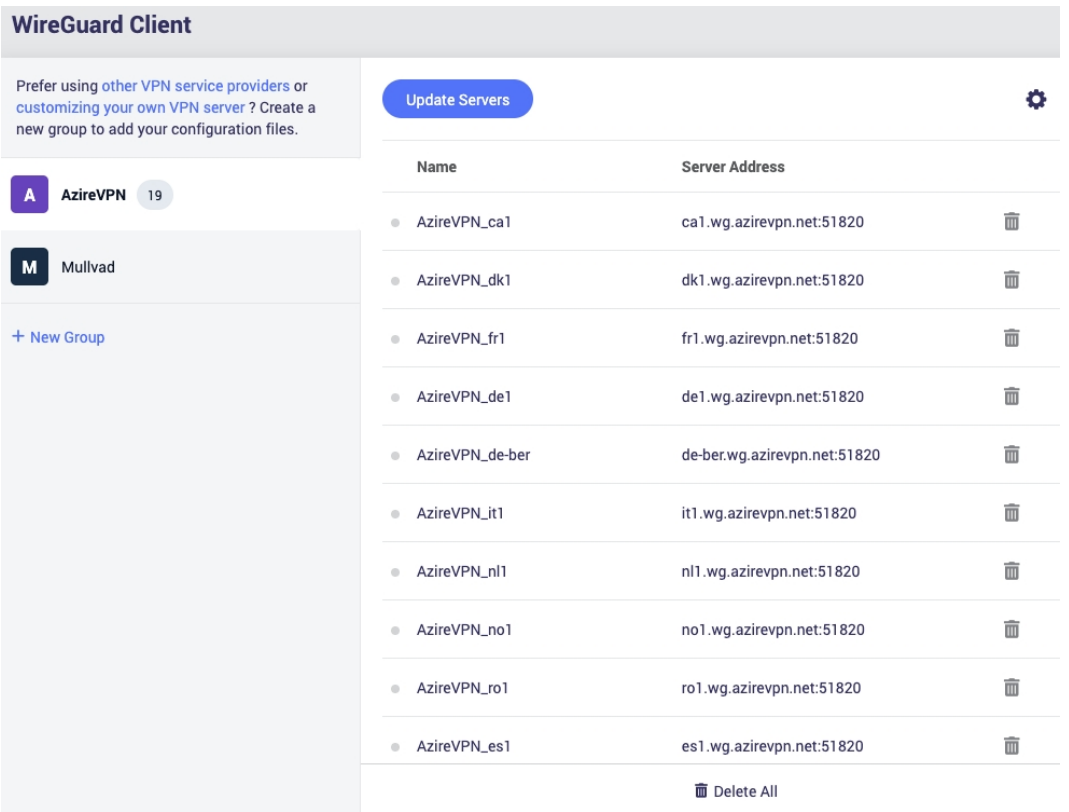
- Set Up AzireVPN
- Set Up Mullvad
- Set Up WireGuard Client Manually (for other providers)

10.2.2 Set Up AzireVPN

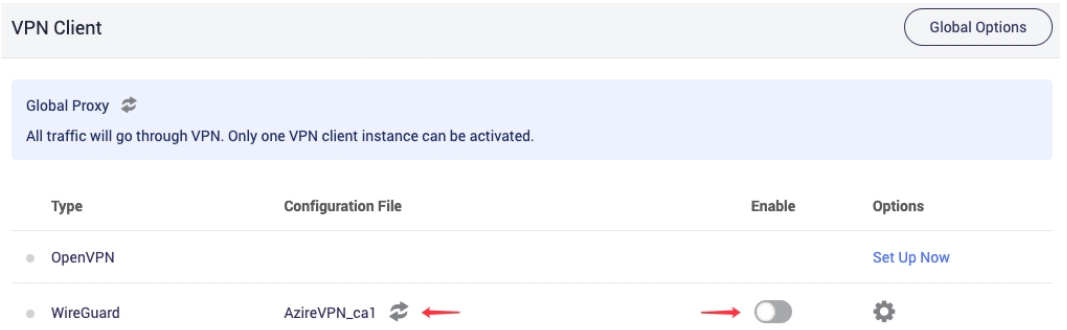
Follow the steps below to set your router as an AzireVPN client.

1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **AzireVPN**.
2. Input Username and Password, then click **Save Credentials And Get Servers**. It will generate configuration files for each servers.

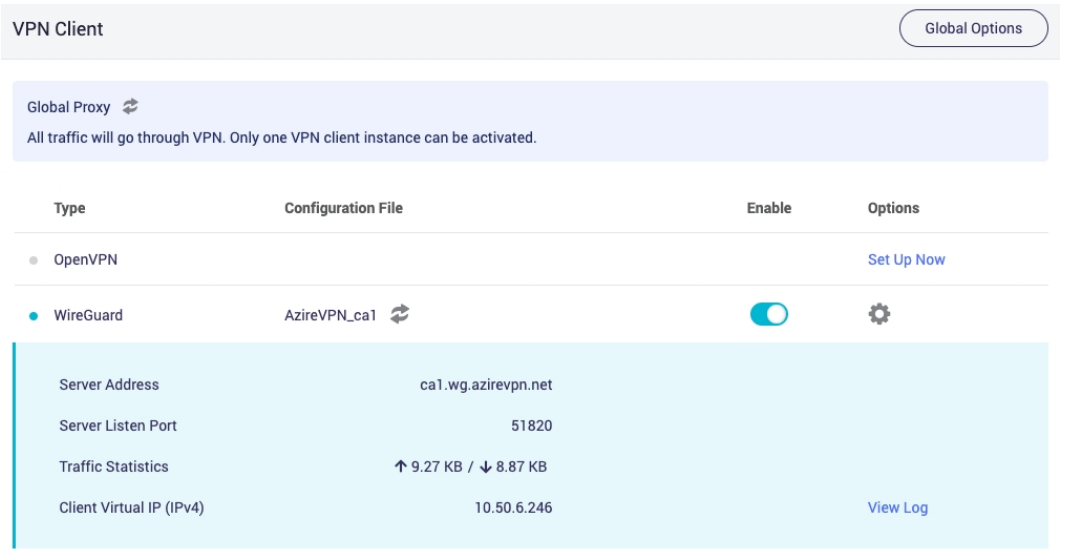




3. Go to VPN Dashboard to enable the connection.

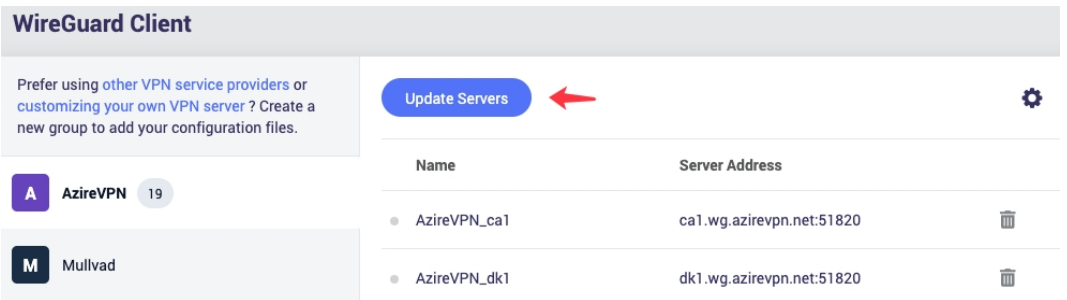


Once connected, you should see your user IP address and the number of Bytes send/received.



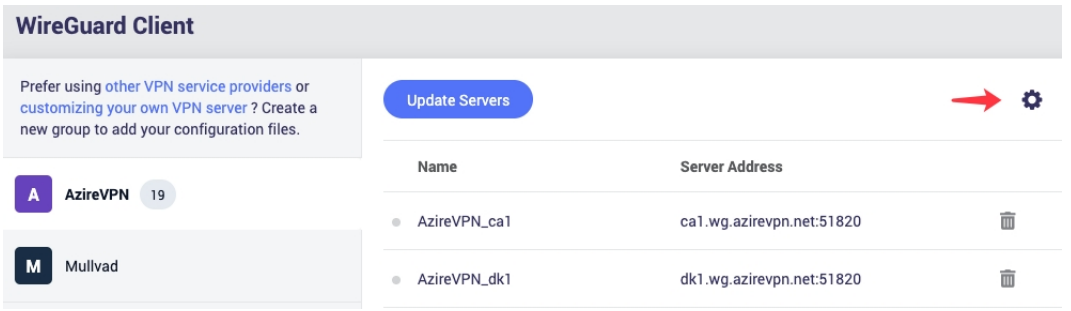
4. Update servers.

   AzireVPN may maintain or shutdown some servers, it will make the connection failed, you can **Update Servers** to get the latest available servers.



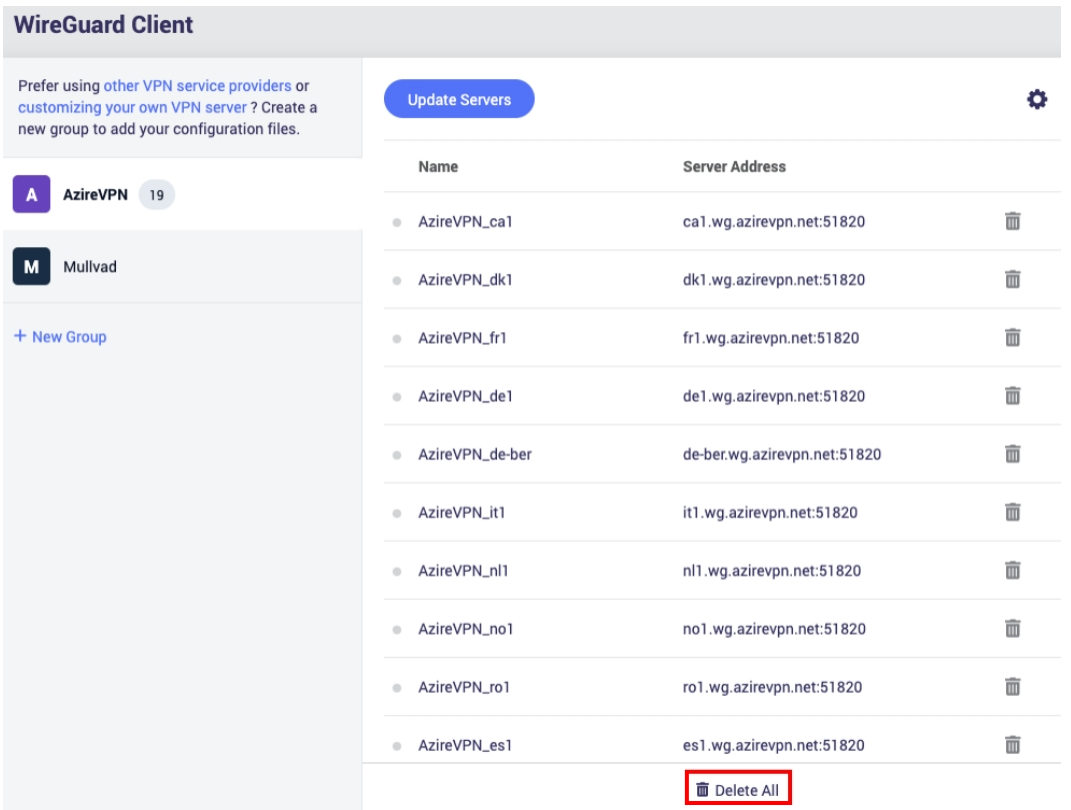
5. Edit credentials.

   Click the cog icon to edit the credential.



6. Delete all files.

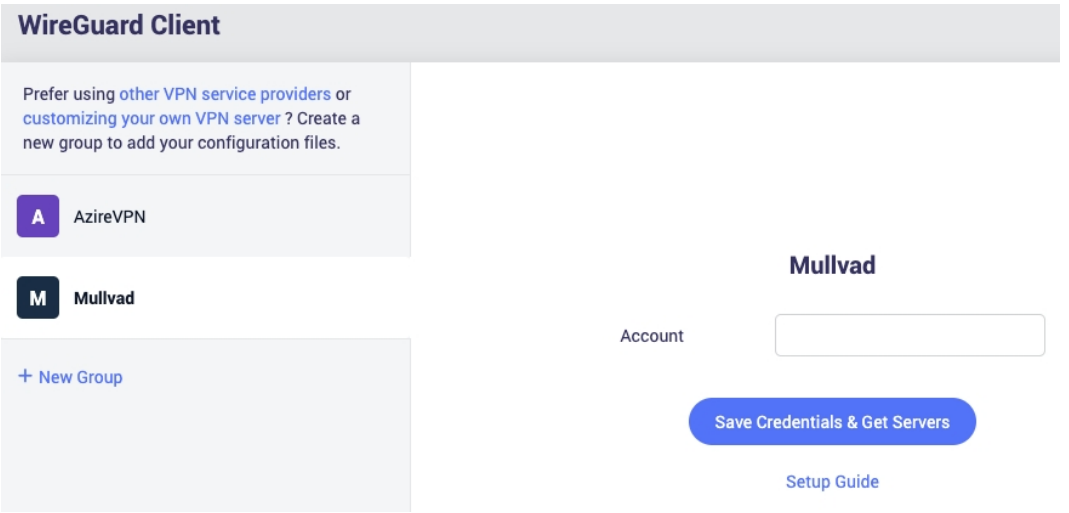
   You can click **Delete All** to delete all configuration files with one click.



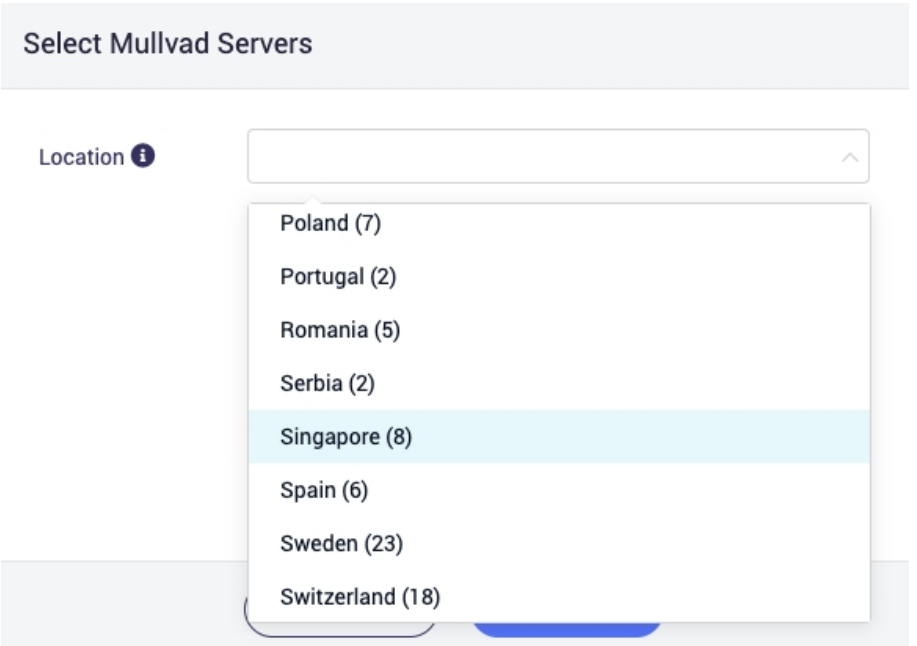
10.2.3 Set Up Mullvad

Follow the steps below to set your router as a Mullvad client.

1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Mullvad**.
2. Enter your Mullvad Account (16-digit number), then click **Save Credentials & Get Servers**.

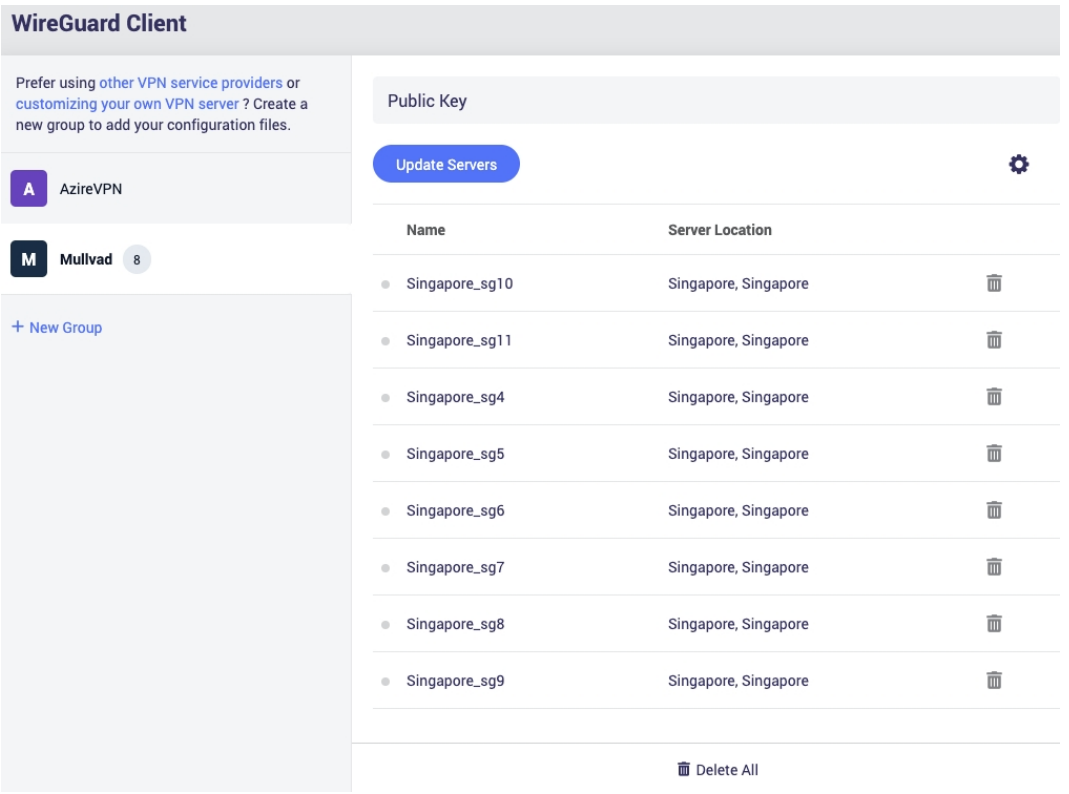


It will pop up a dialog to select a location.

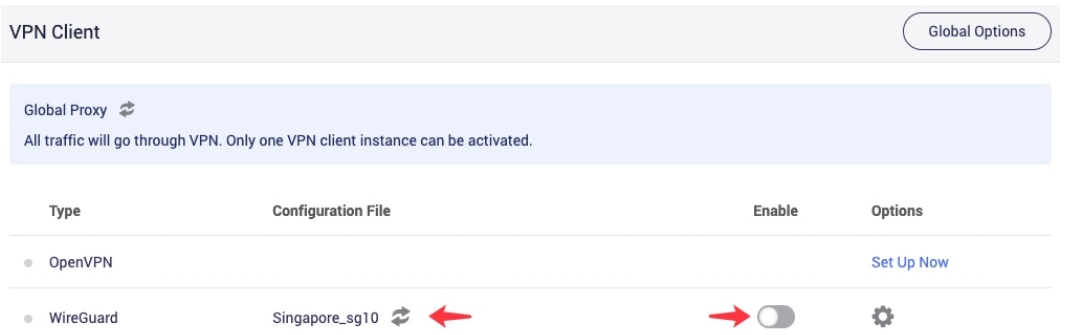


Then it will generate the configuration files of the selected location server.

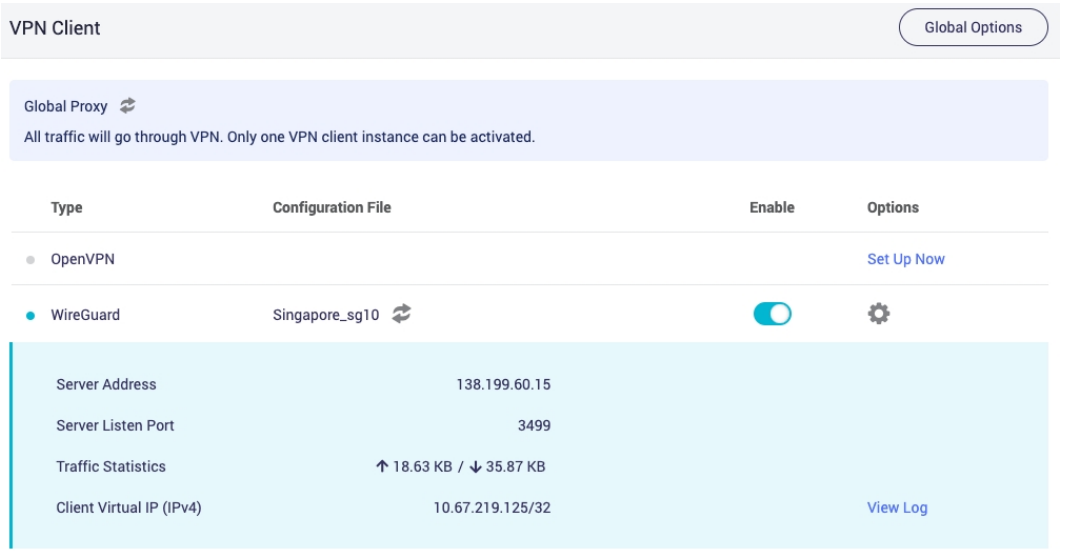
The **Public Key** is the WireGuard public key to send to Mullvad server. You can have up to five keys at the same time, and manage WireGuard keys on your Mullvad account page.



3. Go to VPN Dashboard to enable the connection.

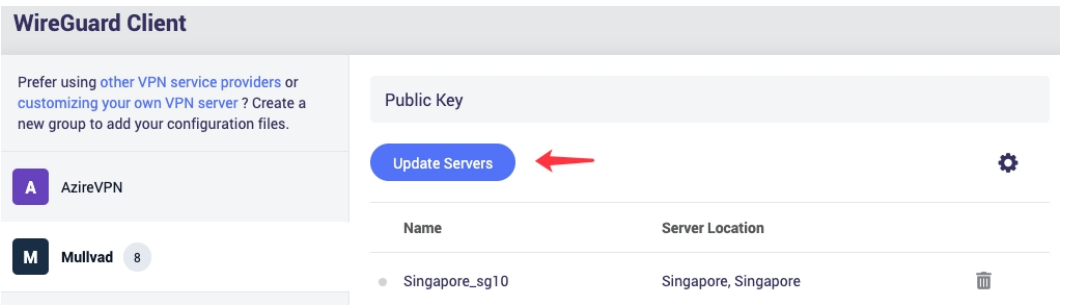


Once connected, you should see your user IP address and the number of Bytes send/received.



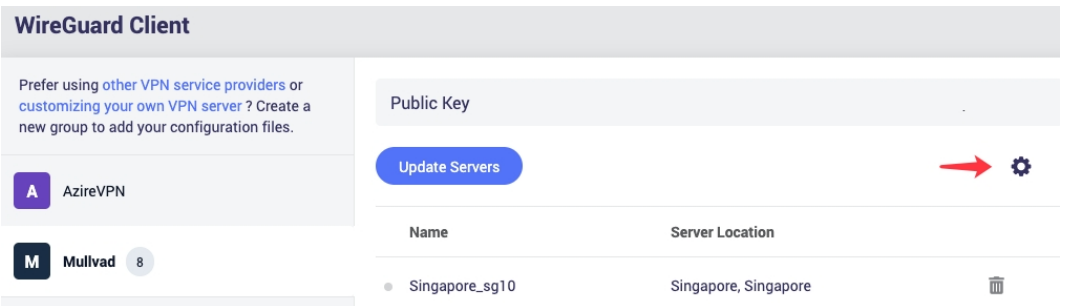
4. Update servers.

   Mullvad may maintain or shutdown some servers, it will make the connection failed, you can **Update Servers** to get the latest available servers.



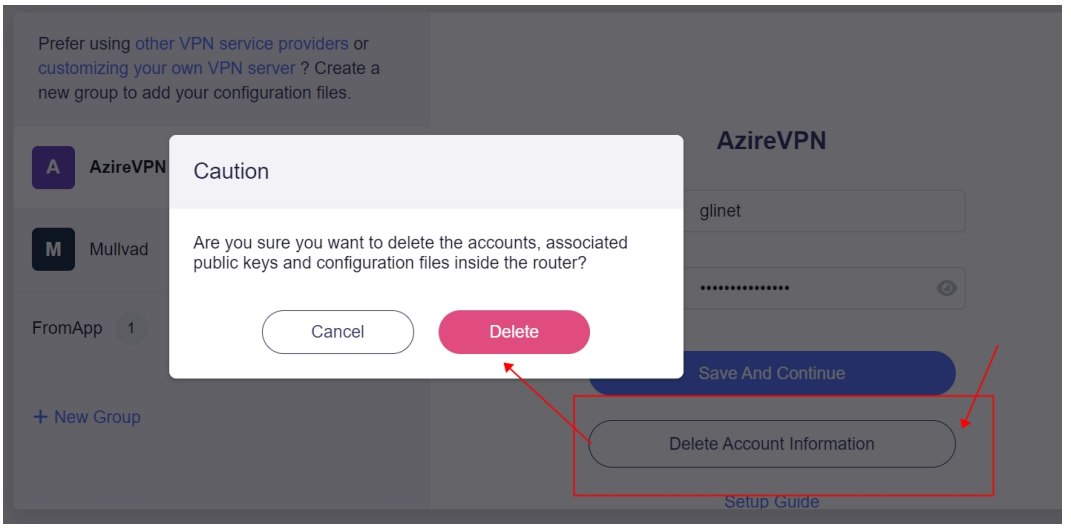
5. Edit credentials

   Click the gear icon to edit your login credentials.



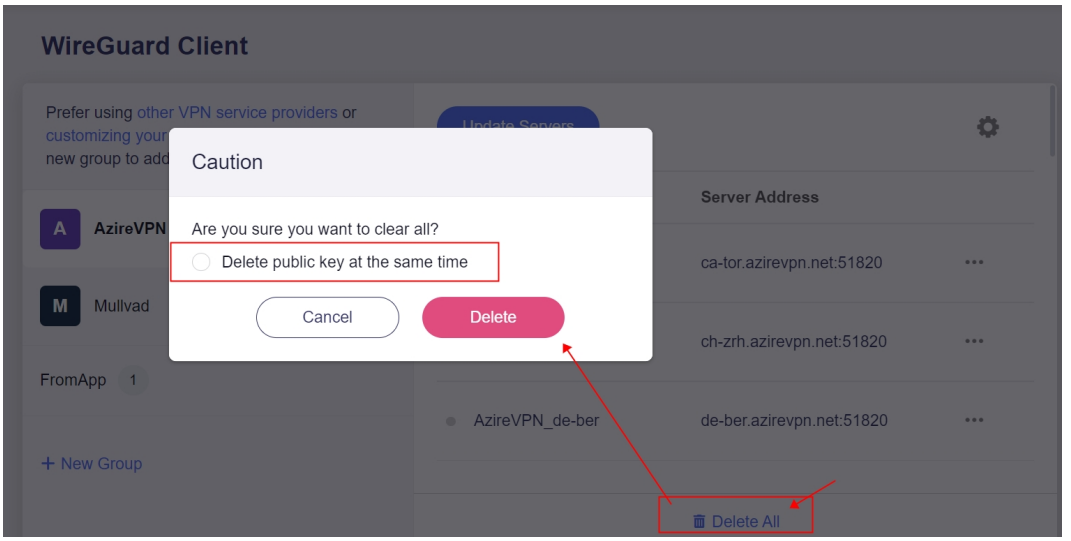
6. Delete account information

   If you click **Delete**, it will delete the account credential, private key, public key and configuration files **in the router**.



7. Delete

   Allow deleting all configuration files with one click and provide a prompt to also delete private key and public key.

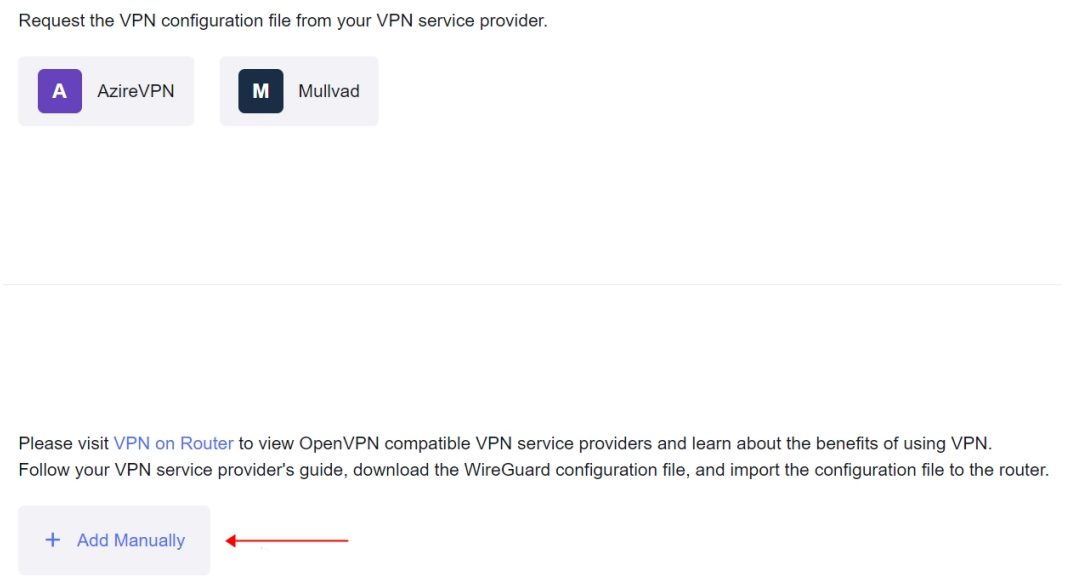


10.2.4 Set Up WireGuard Client Manually (for other providers)

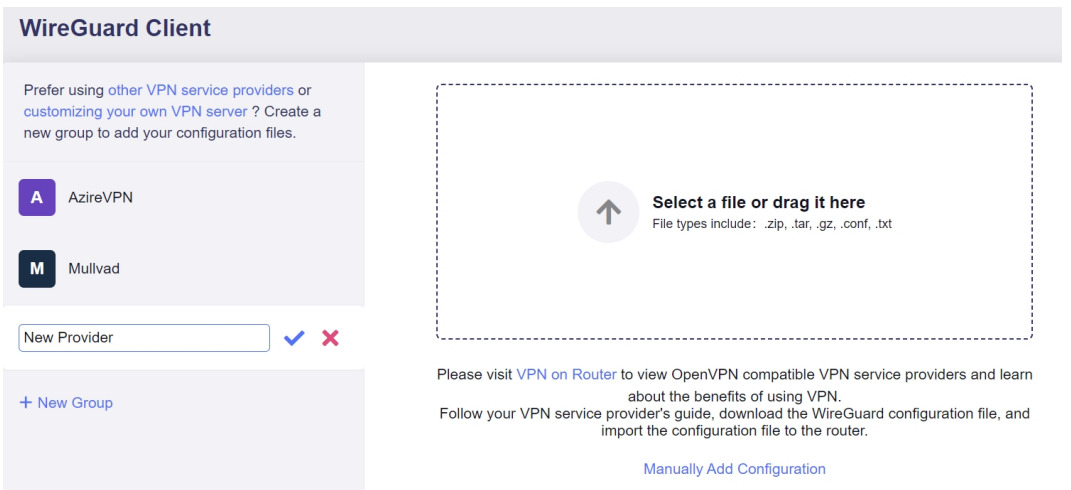
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see this guide or contact their support.

Below are steps to upload the configuration file to the router to set up a WireGuard client.

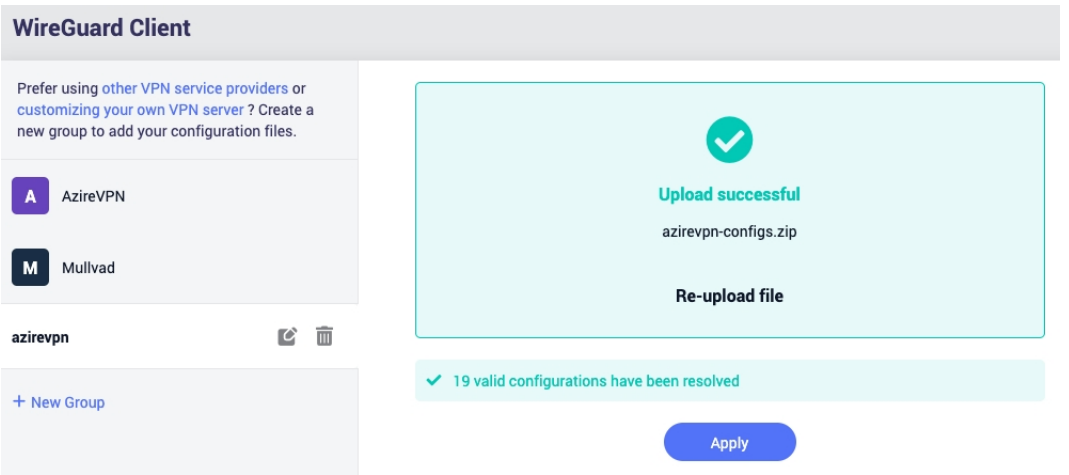
1. Log in to your router's web admin panel and navigate to **VPN** > **WireGuard Client** > **Add Manually**.



2. It will create a group on the left sidebar. Set a descriptive name for the group.

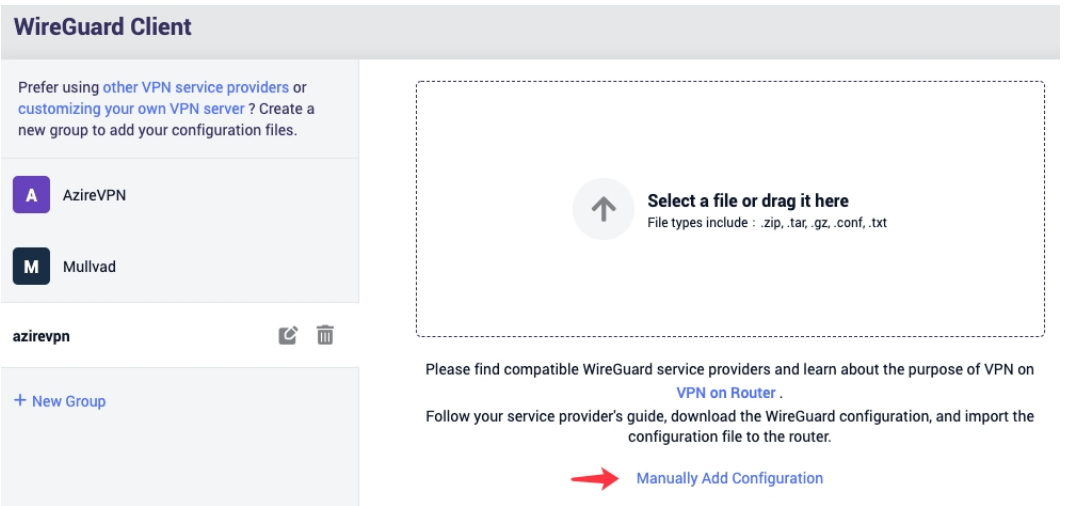


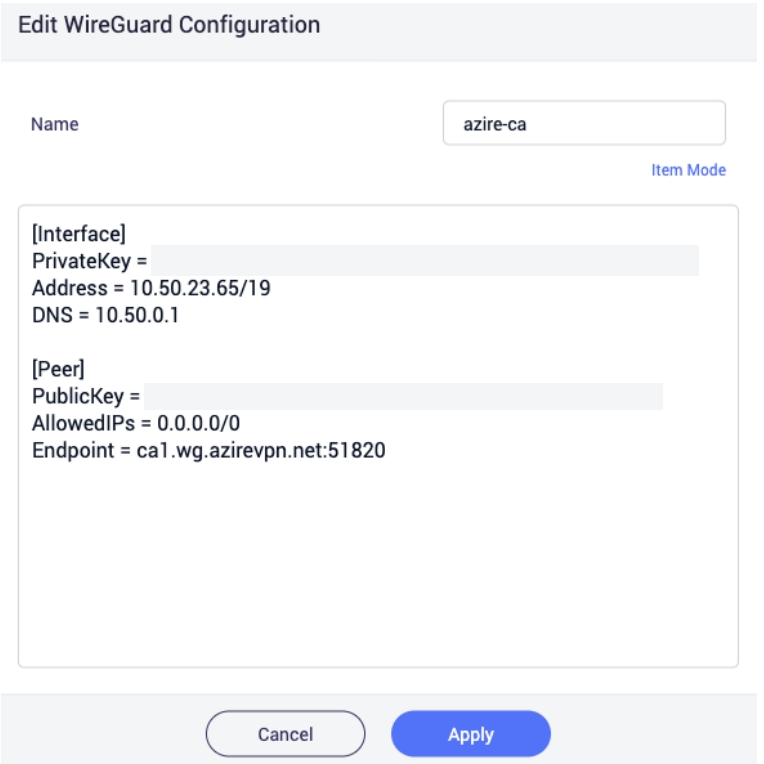
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.



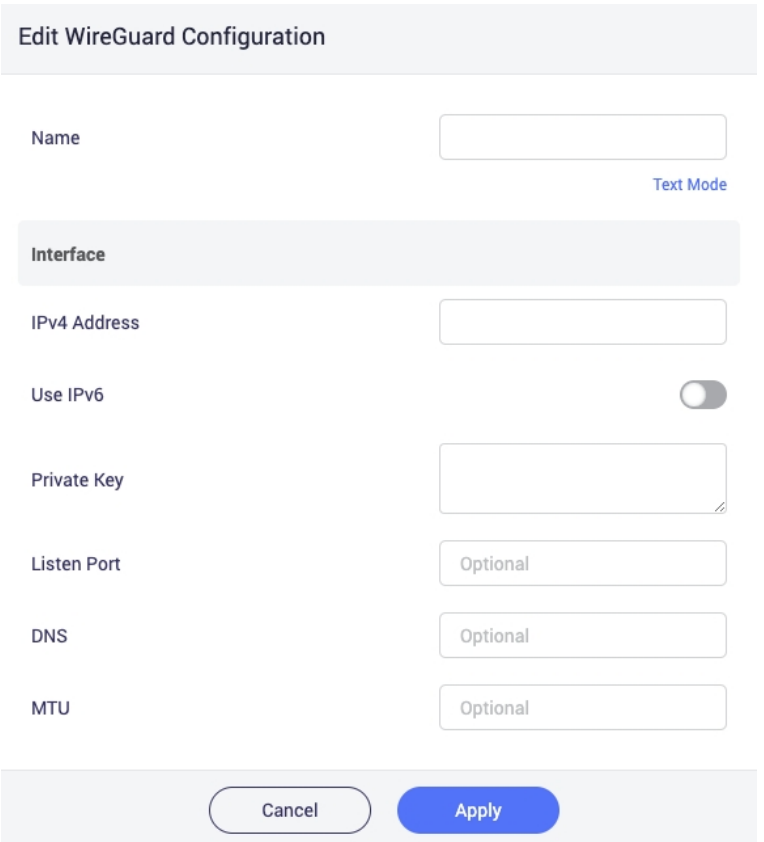
If you upload a compressed file containing multiple configuration files, it will be decompressed automatically.

Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

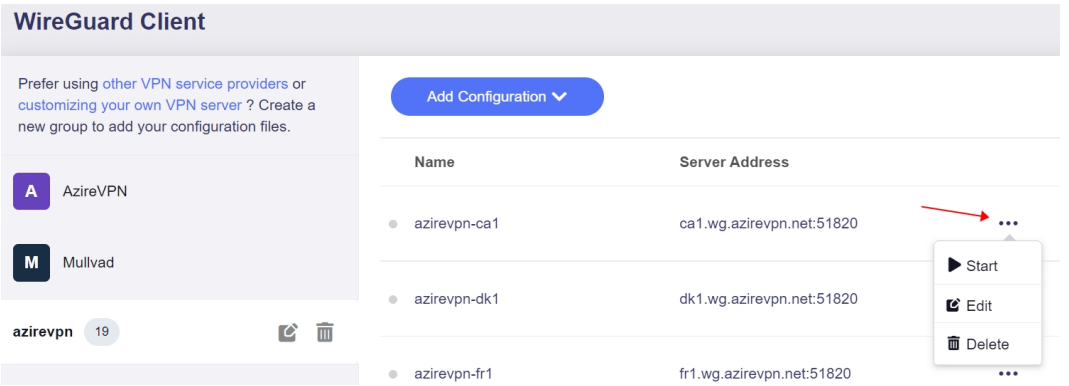




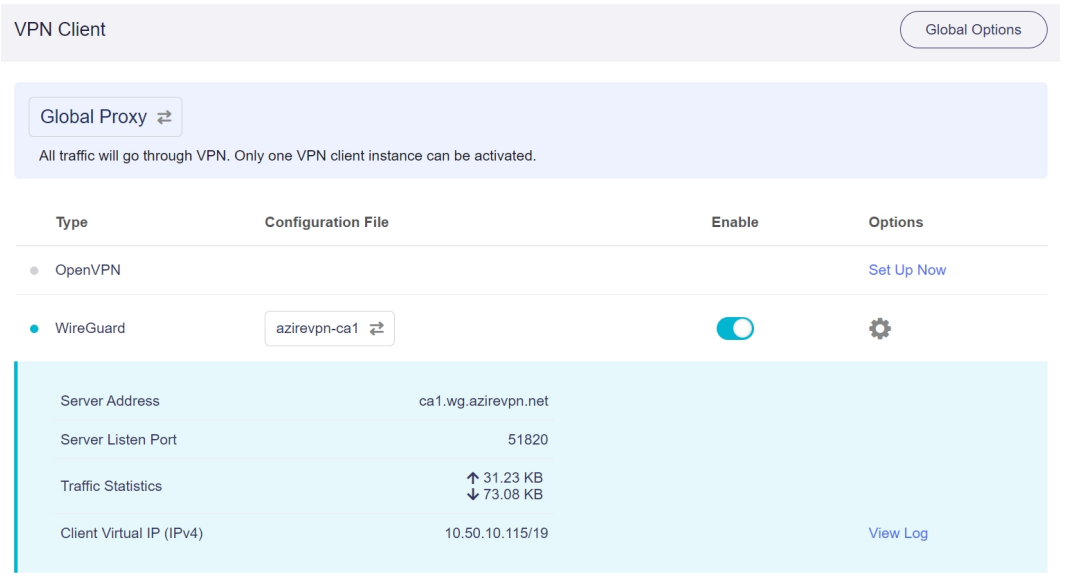
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



4. Click the three-dot icon on the right side to start the connection.



5. Once connected, a green dot will appear next to the configuration file. You can check the VPN connection details on the **VPN Dashboard**.



Chapter 11

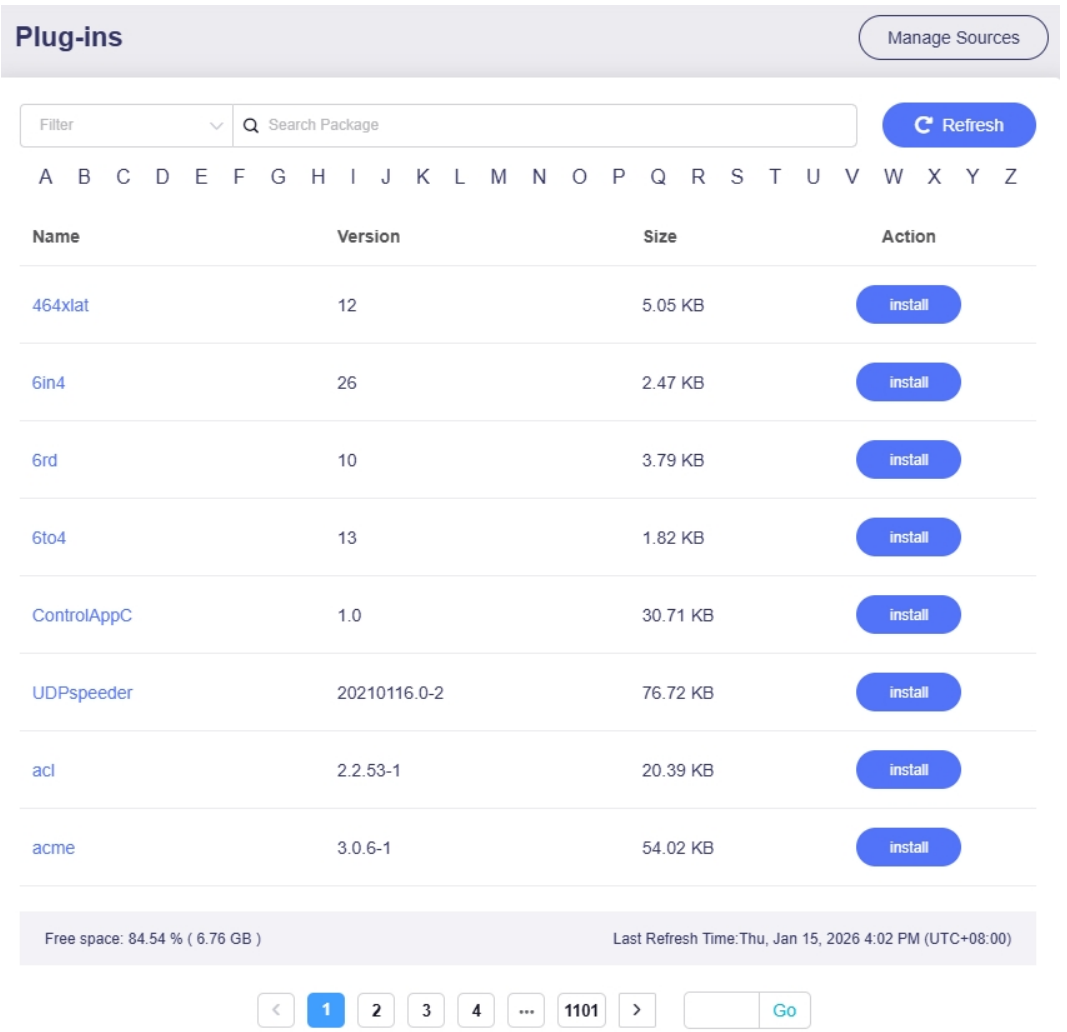
Applications

This chapter introduces some applications in GL.iNet routers, e.g., Plug-ins, Dynamic DNS, and GoodCloud.

11.1 Plug-ins

The Plug-ins page allows you to manage OpenWrt packages.

Log in to your router's web admin panel, navigate to **APPLICATIONS** > **Plug-ins.** You can install or remove any package available in the repository. Click the **Refresh** button to update the package list before installing plug-ins.



Note:

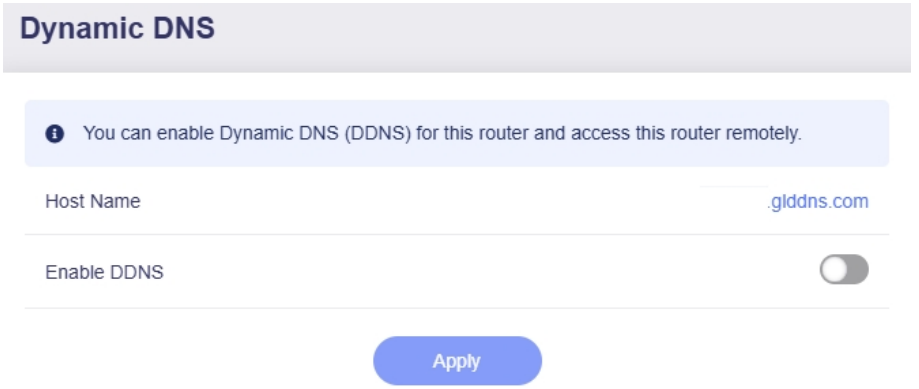
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please contact the respective third-party plugin authors.

11.2 Dynamic DNS

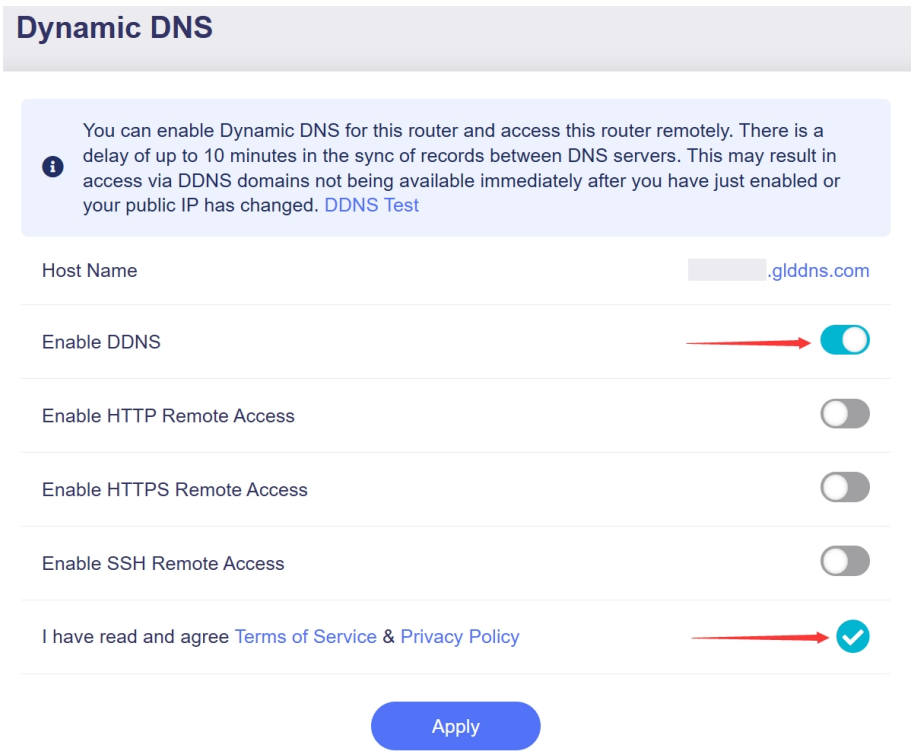
Dynamic Domain Name Service (DDNS, or Dynamic DNS) is a service used to map a domain name to the dynamic IP address of a network device. With Dynamic DNS, you can access your router remotely. A public IP address is required for this functionality.

11.2.1 Enable DDNS

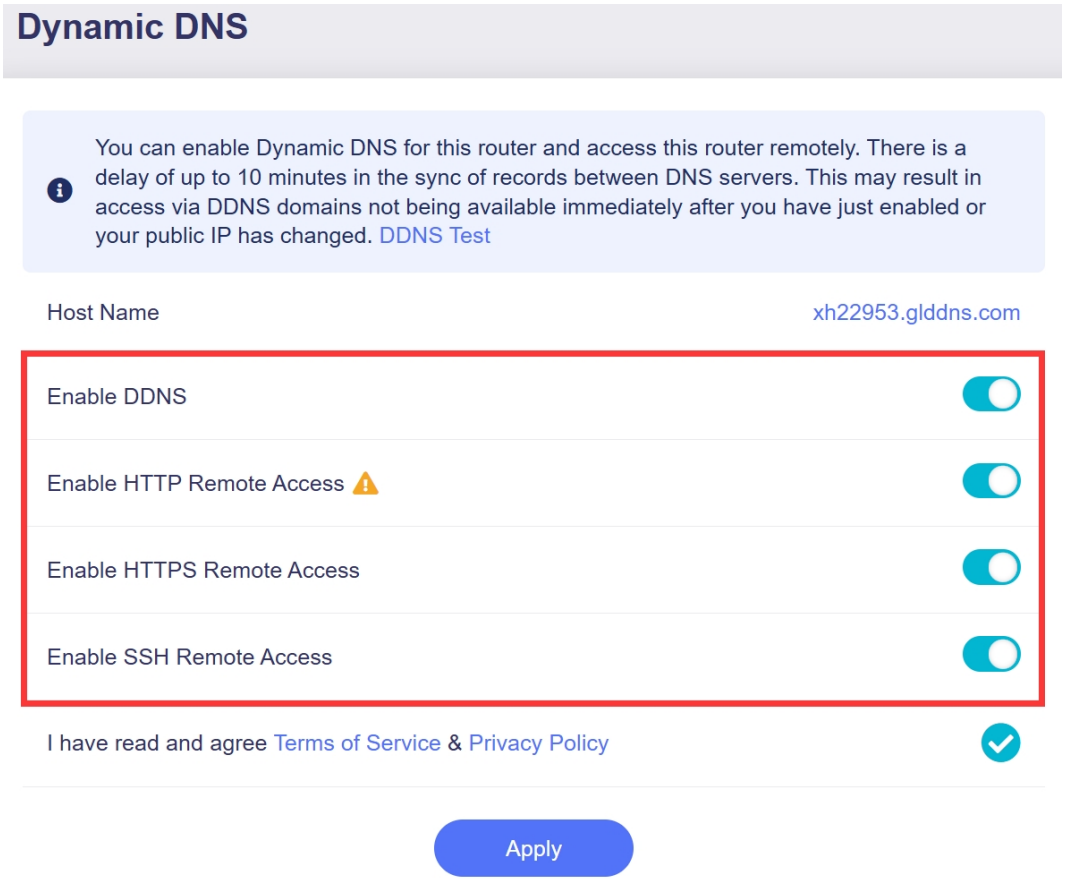
1. Log in to your router's web admin panel, navigate to **APPLICATIONS** > **Dynamic DNS**, the page is displayed as below.



2. Toggle on **Enable DDNS**, read and agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



3. If you need remote access, enable the required services on this page, including **HTTP**, **HTTPS**, and **SSH**.



Note:

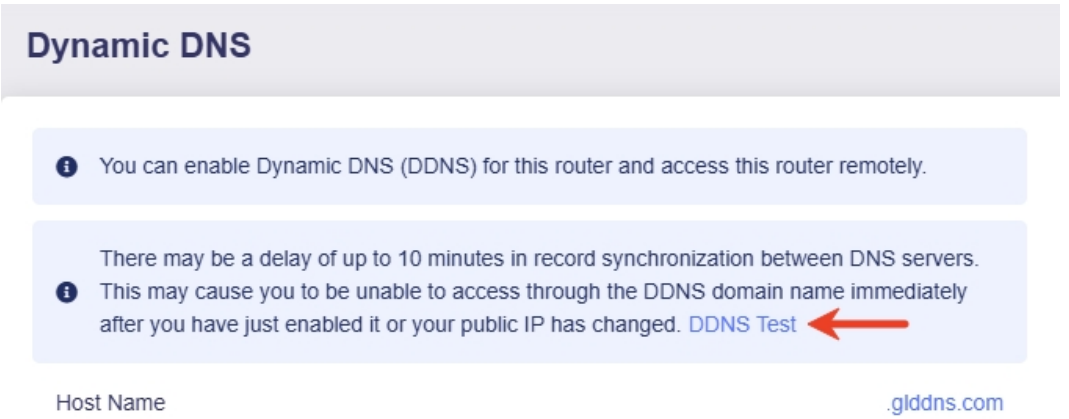
1. There may be a delay of up to 10 minutes in record synchronization between DNS servers. This may prevent you from accessing through the DDNS domain name immediately after enabling it or when your public IP changes.
2. If you enable DDNS and VPN Client at the same time, ensure that Services From GL.iNet Use VPN is disabled.

11.2.2 Check if DDNS Works

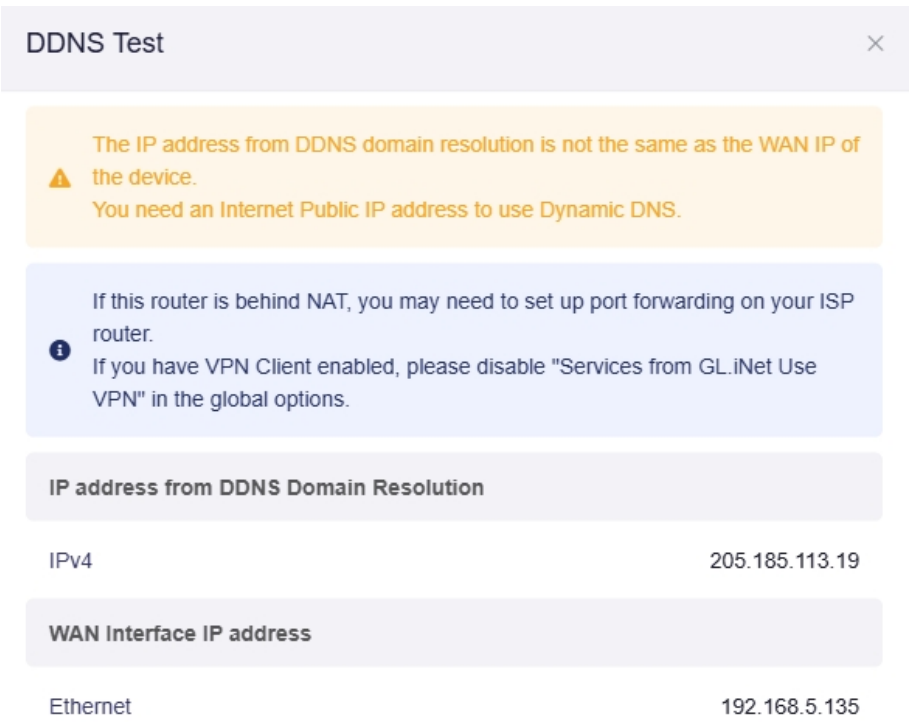
You can check if DDNS works using the DDNS test tool or manually via commands.

Method 1. Use DDNS Test tool

1. In the Dynamic DNS page, click the **DDNS Test**.



2. Make sure the IP address from DDNS domain resolution matches the router's WAN IP. If not, a yellow prompt will appear at the top, indicating that the router might be behind NAT, and you need to set up port forwarding on the upstream router.



Method 2. Use commands

1. Use nslookup command *nslookup xxxxxxx.glddns.com 8.8.8.8* to obtain the mapping between domain name and IP address, as shown below.



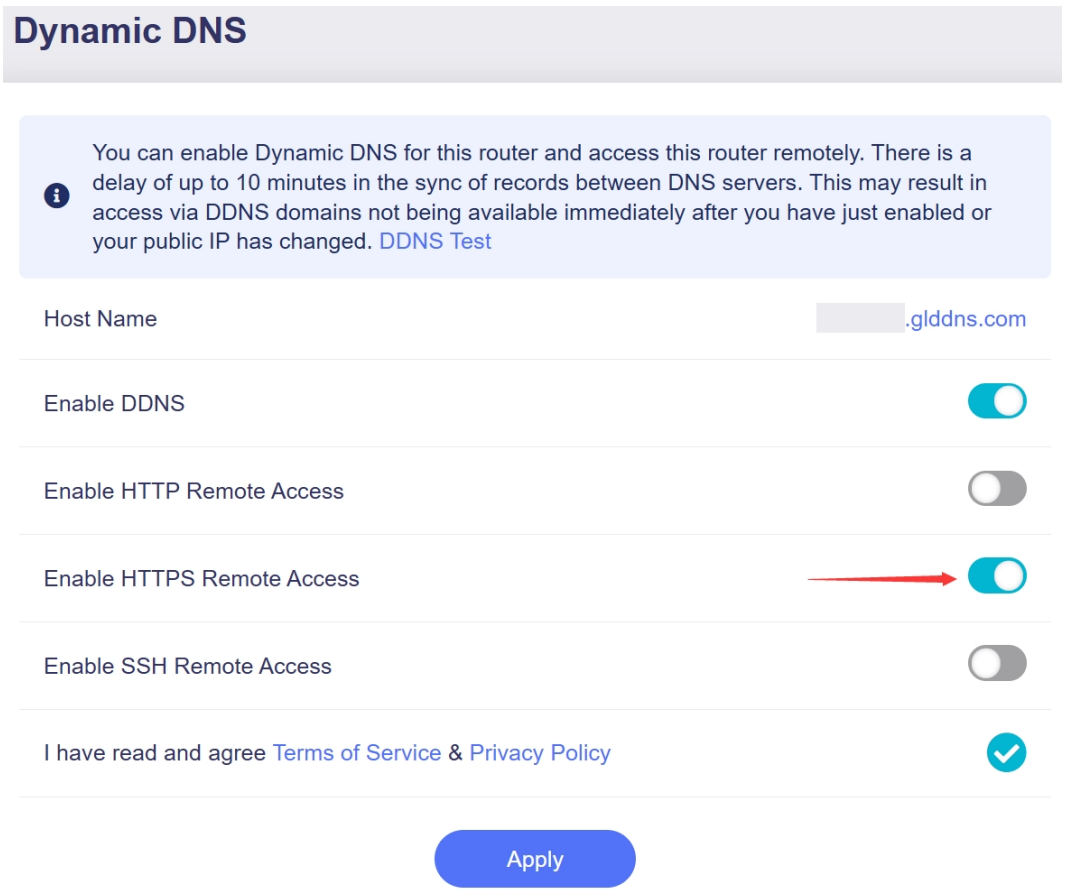
   - Replace “xxxxxxx.glddns.com” in the image above with your Host Name.
   - The “8.8.8.8” is the Google DNS. Use it or replace it with others, then press Enter.
2. If you get a public IP address such as “183.178.10.100” in the image above, it indicates that your DDNS domain has been successfully mapped to a public IP address. If you get a message like “server can’t find xxxxxxx.glddns.com”, it may indicate that domain resolution failed, and your DDNS domain has not been successfully mapped to a public IP address. Proceed to the next step to verify.
3. Log in to your router’s web admin panel and navigate to **INTERNET**. Find your router’s WAN IP address in the current active interface. Compare this IP address with the public IP address obtained above. If they are the same, the DDNS is in effect, otherwise it is not.

11.2.3 HTTP Remote Access

A **Public IP address** is required for HTTP remote access. See here to verify whether your ISP assigns you a public IP address. If your router is behind NAT, configure port forwarding (**port 80**) on the upstream router for HTTP access.

Follow the steps below to enable HTTP remote access for your router.

1. On the Dynamic DNS page, toggle on **Enable DDNS** and **HTTP Remote Access**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



2. Once enabled, you can access the router's admin panel from anywhere using the DDNS host name over HTTP, e.g., **http://xxxxxxx.glddns.com**. If port forwarding is configured, access it as **http://xxxxxxx.glddns.com:external_port** (replace the external_port with your actual port number).

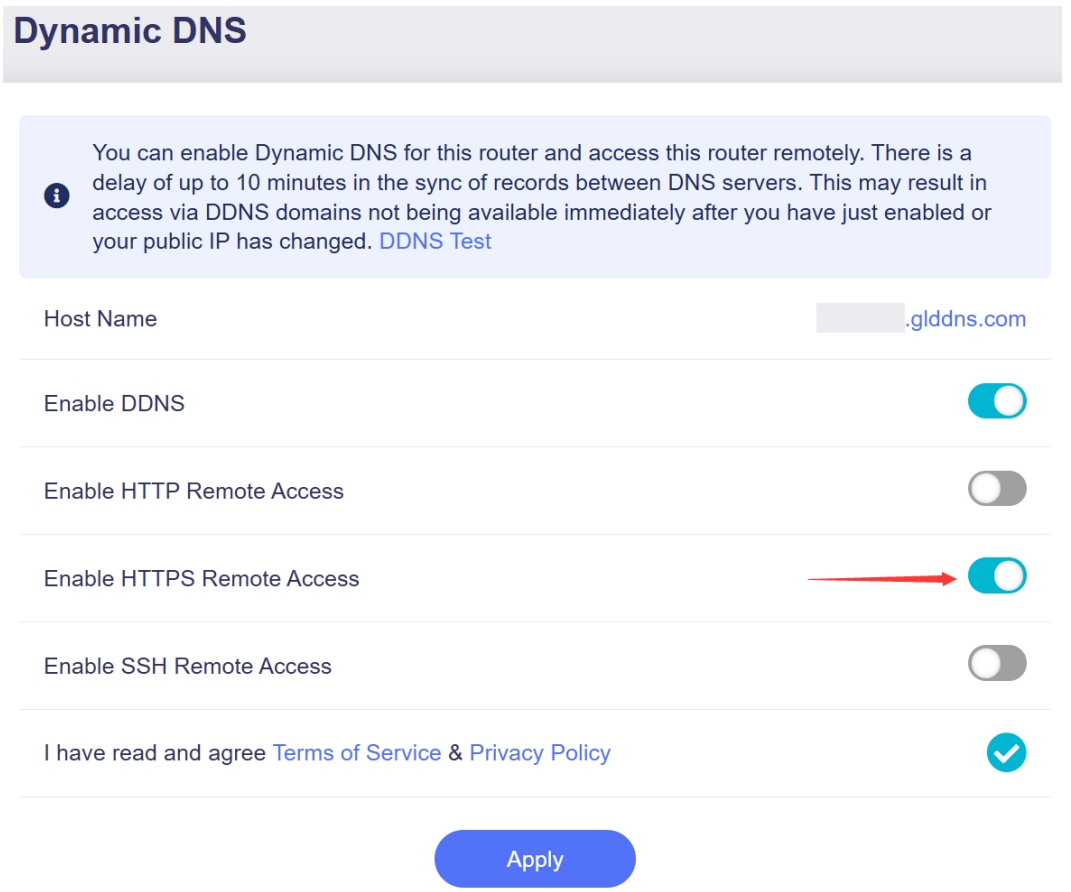
Note: HTTP is a non-encrypted protocol. All transmitted data including login credentials are sent in plaintext, which poses security risks. You should use HTTP remote access with caution.

11.2.4 HTTPS Remote Access

A **Public IP address** is required for HTTPS remote access. See here to verify whether your ISP assigns you a public IP address. If your router is behind NAT, configure port forwarding (**port 443**) on the upstream router for HTTPS access.

Follow the steps below to enable HTTPS remote access for your router.

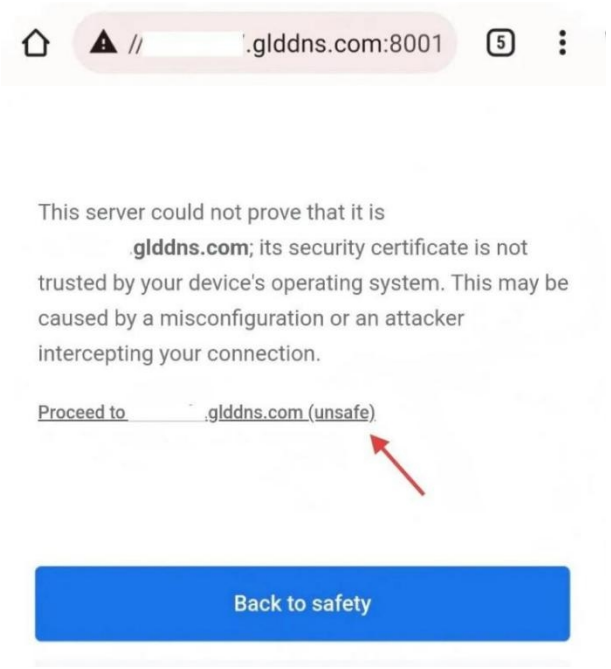
1. On the Dynamic DNS page, toggle on **Enable DDNS** and **HTTPS Remote Access**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



2. Once enabled, you can access the router's admin panel from anywhere using the DDNS host name over HTTPS, e.g., **https://xxxxxxx.glddns.com**. If port forwarding is configured, access it as **https://xxxxxxx.glddns.com:external_port** (replace the external_port with your actual port number).

Note: This function uses self-signed certificates; therefore, browsers will indicate "Your connection is not private" when accessing the router's admin panel via the DDNS host name

over HTTPS. To proceed the HTTPS remote access, click **Advanced** at the bottom, then click **Proceed to xxxxxxx.glddns.com** to continue.



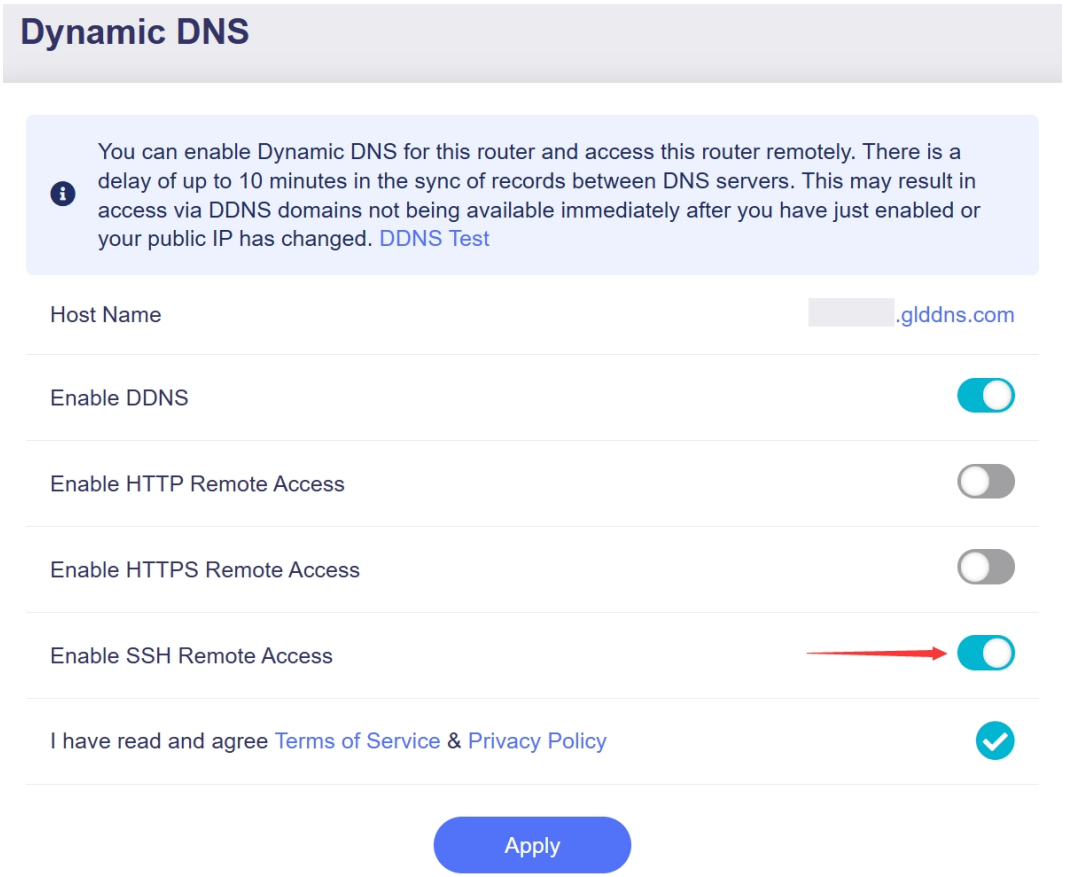
You will then be able to access the router's web admin panel using the DDNS host name over **HTTPS**.

11.2.5 SSH Remote Access

A **Public IP address** is required for SSH remote access. See here to verify whether your ISP assigns you a public IP address. If your router is behind NAT, configure port forwarding (**port 22**) on the upstream router for SSH remote access.

Follow the steps below to enable SSH remote access for your router.

1. On the Dynamic DNS page, toggle on **Enable DDNS** and **SSH Remote Access**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



Once enabled, you can access the router's admin panel from anywhere using the DDNS host name over SSH, e.g., **ssh root@xxxxxxx.glddns.com**. If port forwarding is configured, access it as **ssh root@xxxxxxx.glddns.com:external_port** (replace the external_port with your actual port number).

11.3 GoodCloud

GL.iNet GoodCloud is a platform designed to simplify the remote deployment and management of connected devices. It provides an easy way to remotely access and manage GL.iNet routers. By centralizing network devices on the cloud, users can efficiently perform batch management tasks, such as deploying network configurations and performing software upgrades. They can also remotely access the router's web admin panel or connect to the router's terminal via SSH, achieving cross-regional and end-to-end network device management.

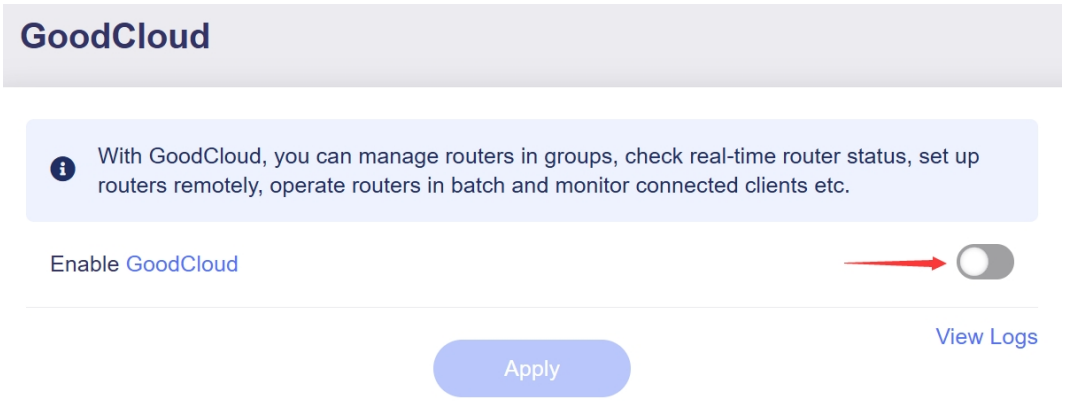
With GoodCloud, you can:

- Check your router’s status in real-time
- Manage groups of routers
- Set up routers remotely
- Monitor connected clients
- Operate routers in batch
- Establish Site-to-Site connection

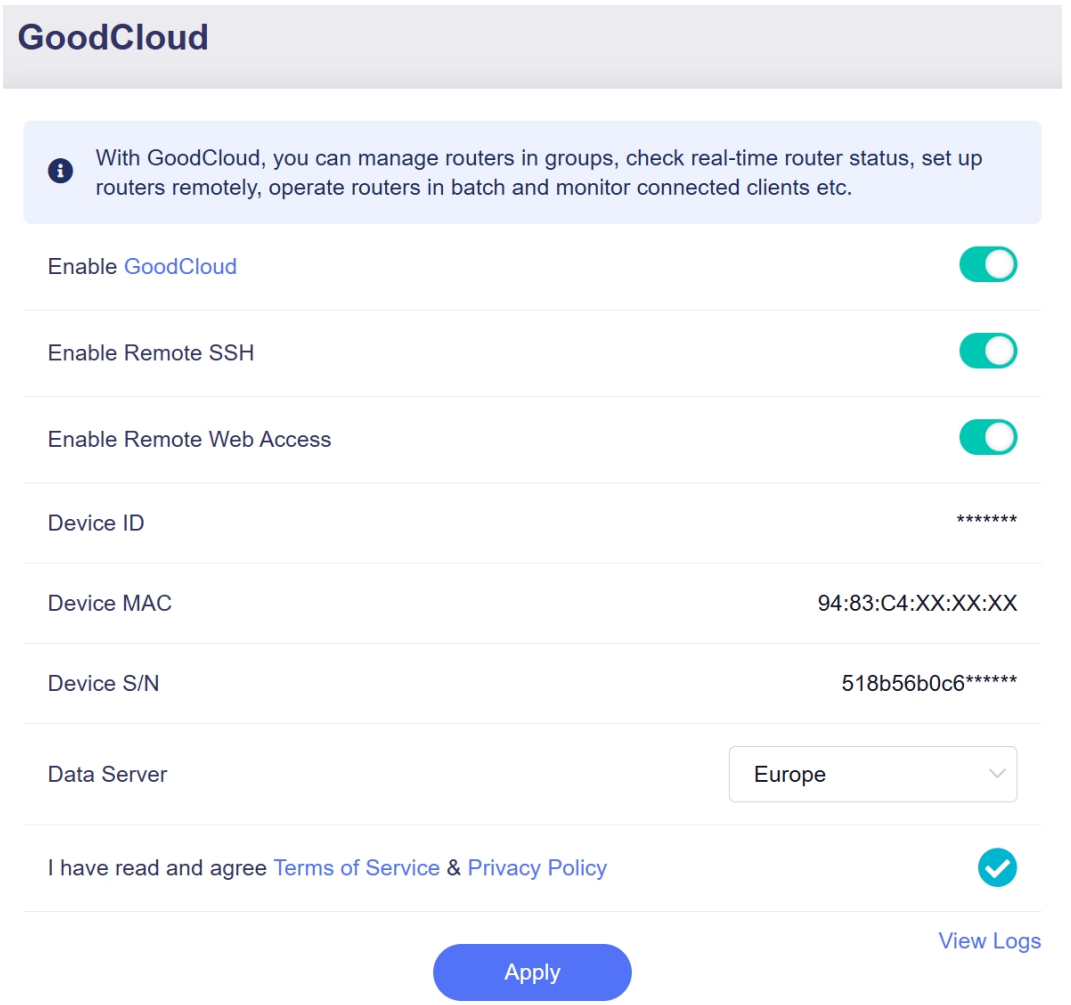
Some features are available in Enterprise Plan and VAR (Value Added Reseller) Plan. See here for details.

11.3.1 Enable GoodCloud

1. Log in to your router's web Admin Panel and navigate to **APPLICATIONS** > **GoodCloud**. Toggle the switch to enable GoodCloud.

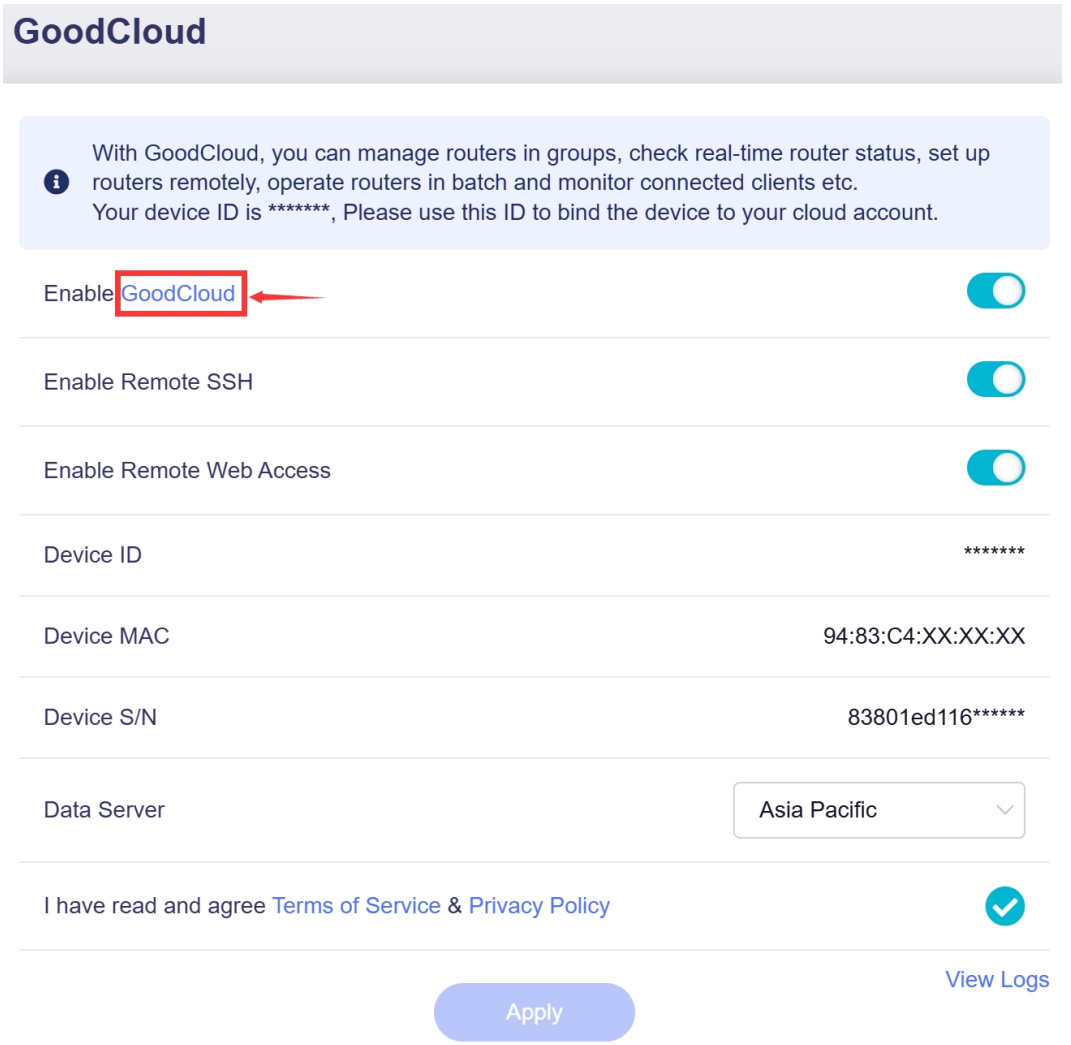


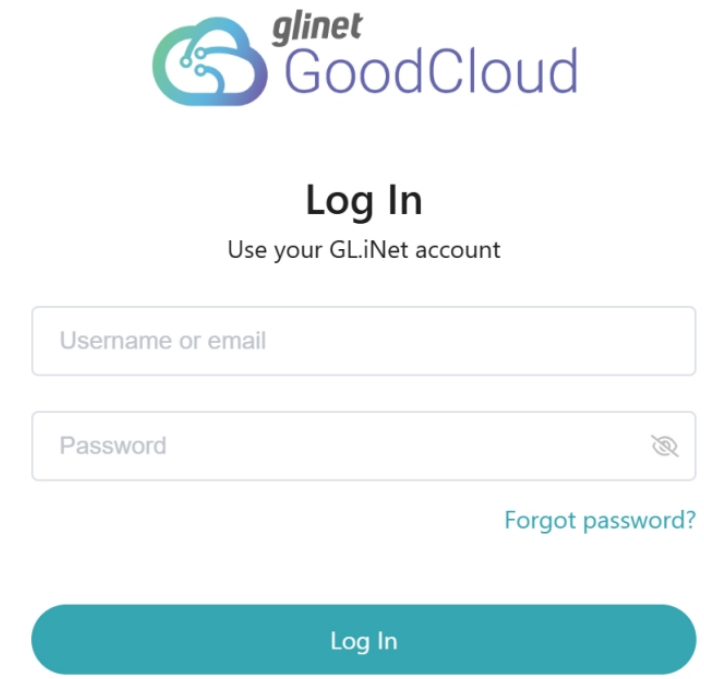
Enable **Remote SSH** and **Remote Web Access** if needed, select the nearest server, read and agree the **Terms of Service & Privacy Policy**, then click **Apply**.



- **Remote SSH**: For remotely accessing the router's terminal over SSH from GoodCloud platform.
- **Remote Web Access**: For remotely accessing the router's web Admin Panel over HTTP/HTTPS from GoodCloud platform.
- **Data Server**: Please choose the server nearest to your device's location. There are three options: Asia Pacific (Japan), America (Oregon), and Europe (Ireland).
- **View Logs**: Redirect to the Log page and display Cloud log.

2. Click GoodCloud to go to the login page, and log in with your GL.iNet Cloud account. If you don't have an account, sign up for one and log in. Once logged in, the router will be bound to your account automatically.

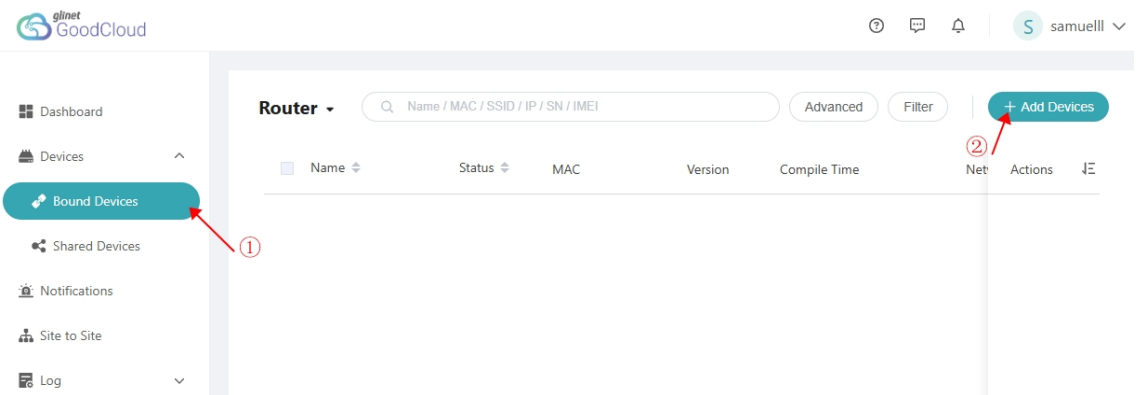




Tips:

- The GoodCloud binding steps differ by firmware version.
- If you fail to receive the verification email, check your spam folder or try again later. For further assistance, contact us at support@gl-inet.com.

3. On the Cloud platform, navigate to **Devices** > **Bound Devices** > **Add Devices**.



There are three methods to bind device to your GoodCloud account: Auto Discover, Manually Add, and Bulk Import. Click here for more details.

4. After successful binding, return to the router's web Admin Panel and navigate to **APPLICATIONS** > **GoodCloud**. This page displays the binding details, including username and binding time.

GoodCloud

With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by **Holly0912** on **2026-10-10 17:26**,Unbind

Enable GoodCloud	
Enable Remote SSH	
Enable Remote Web Access	
Device ID	*******
Device MAC	94:83:C4:XX:XX:XX
Device S/N	518b56b0c6******
Data Server	Europe
I have read and agree Terms of Service & Privacy Policy	

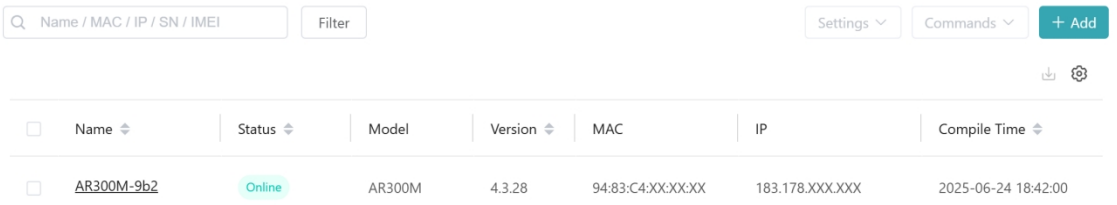
View Logs

Apply

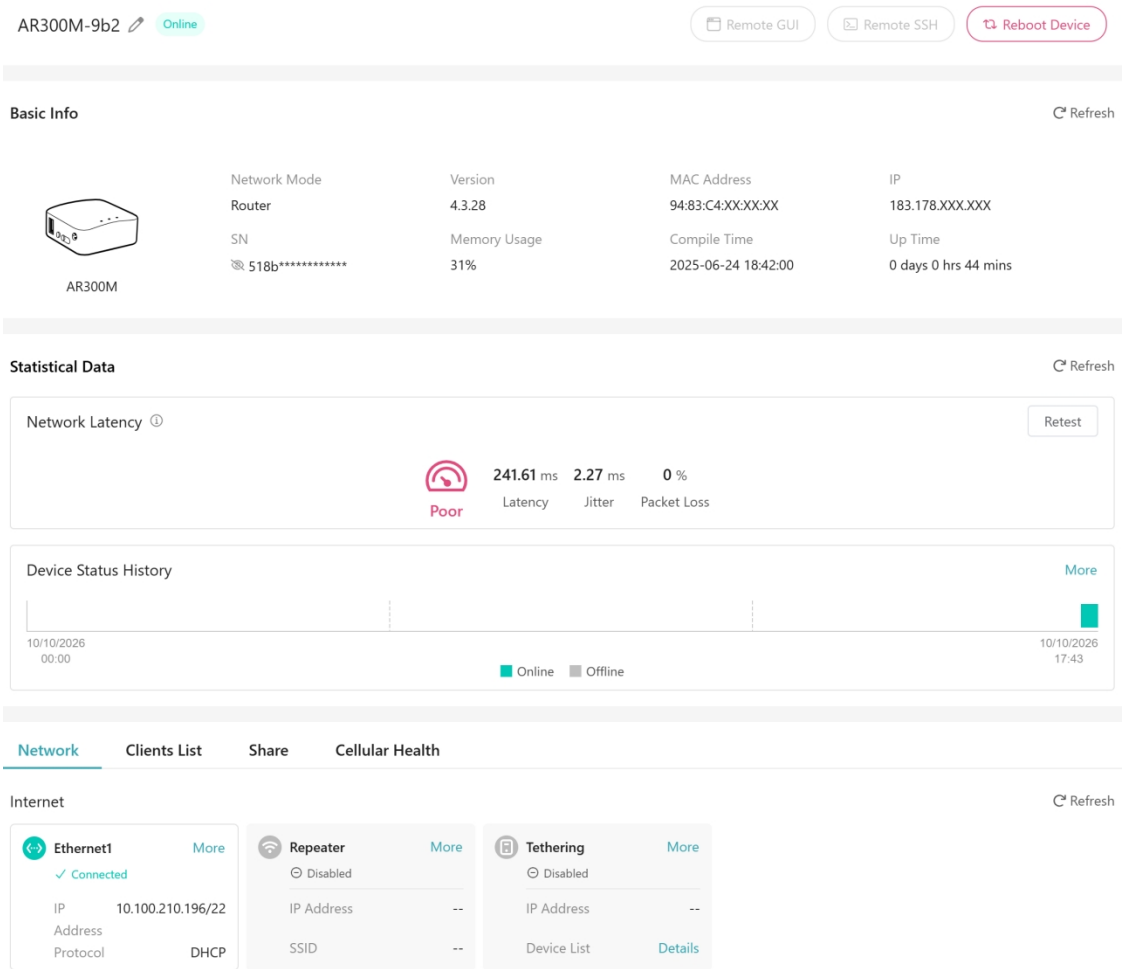
11.3.2 Manage Your Router

Check Device Details

Log in to the GoodCloud platform and navigate to **Devices** > **Bound Devices**. You can view the device's basic information, such as host name, status (online/offline), model, firmware version, and MAC address.

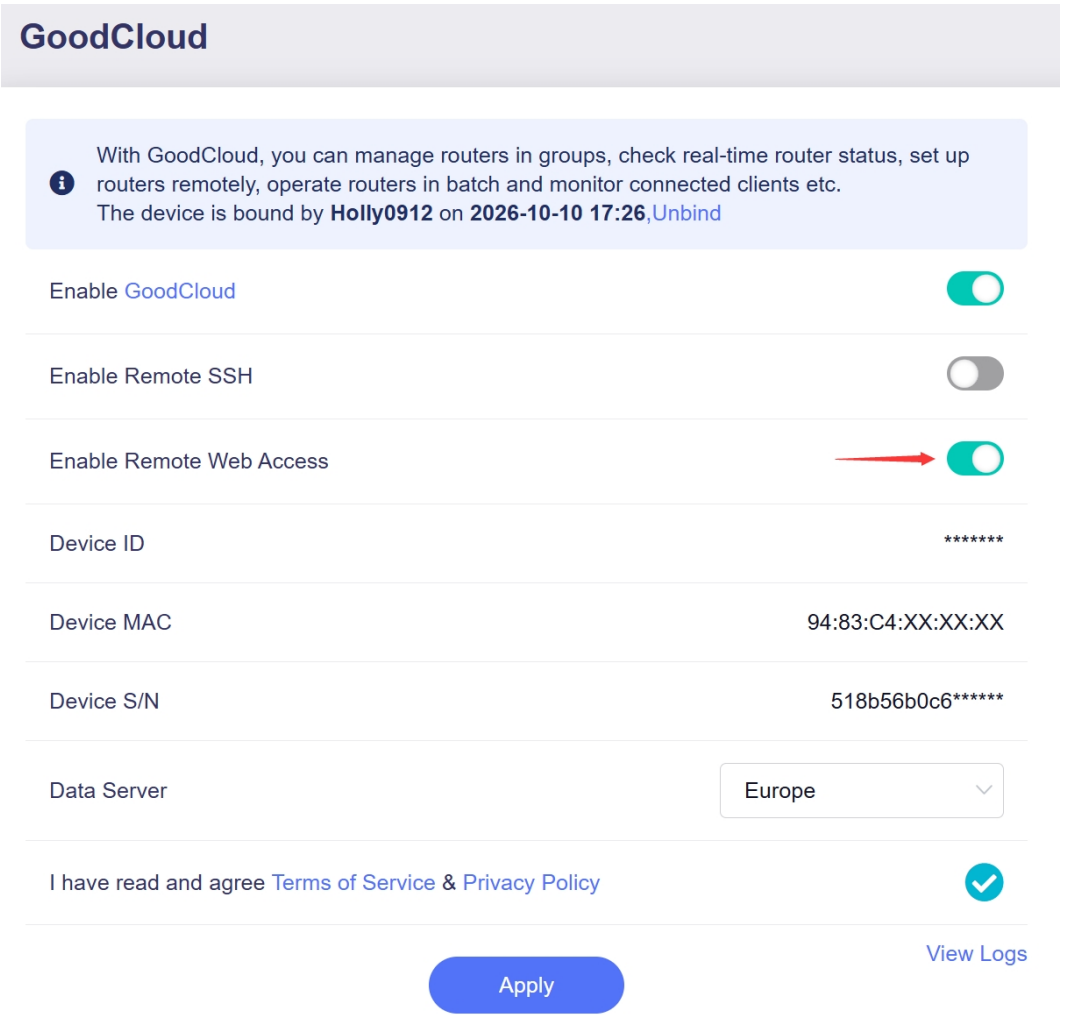


Click the device name to enter the device details page, which displays basic information, statistical data, network overview, client list, and timeline. You can also perform advanced operations, such as remotely accessing the router, and rebooting the device.

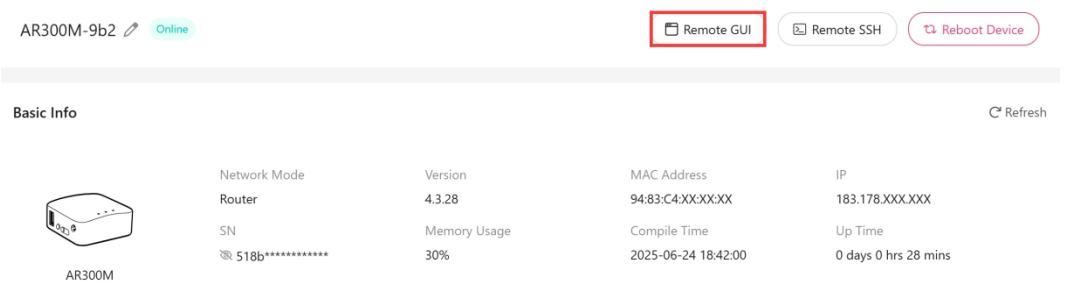


Remote Web Access

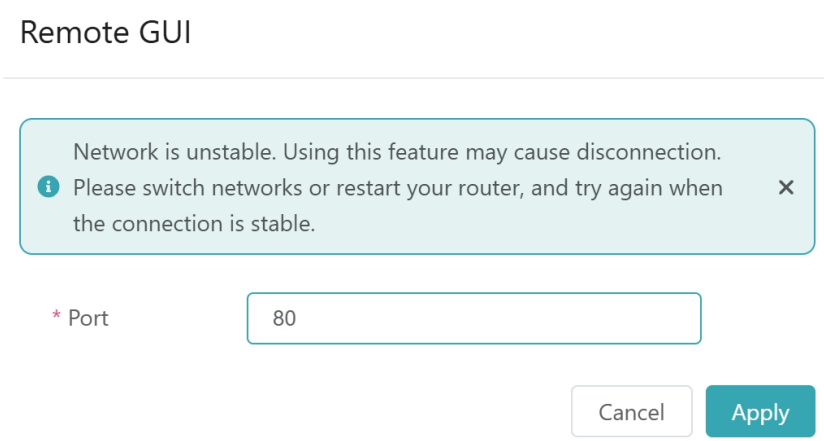
1. Log in to the router's web admin panel, navigate to **APPLICATIONS** > **GoodCloud**, enable **Remote Web Access**, then click **Apply**.



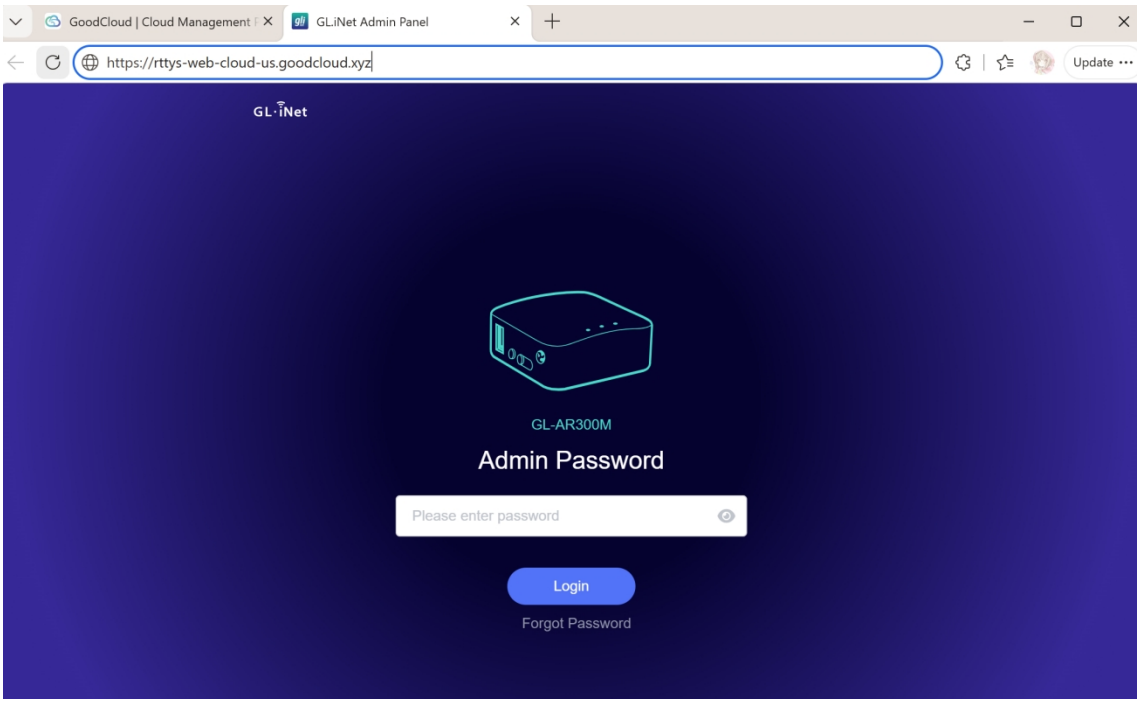
2. Log in to the GoodCloud platform and navigate to **Devices** > **Bound Devices**. Click the device you want to access, and you will enter the device details page.
3. On the device details page, click the **Remote GUI** button in the upper right corner.



4. Select the transfer protocol and port. The defaults are **HTTP** and Port **80**. You can switch the protocol to HTTPS if required, and the port will automatically change to 443. Then click **Apply**.

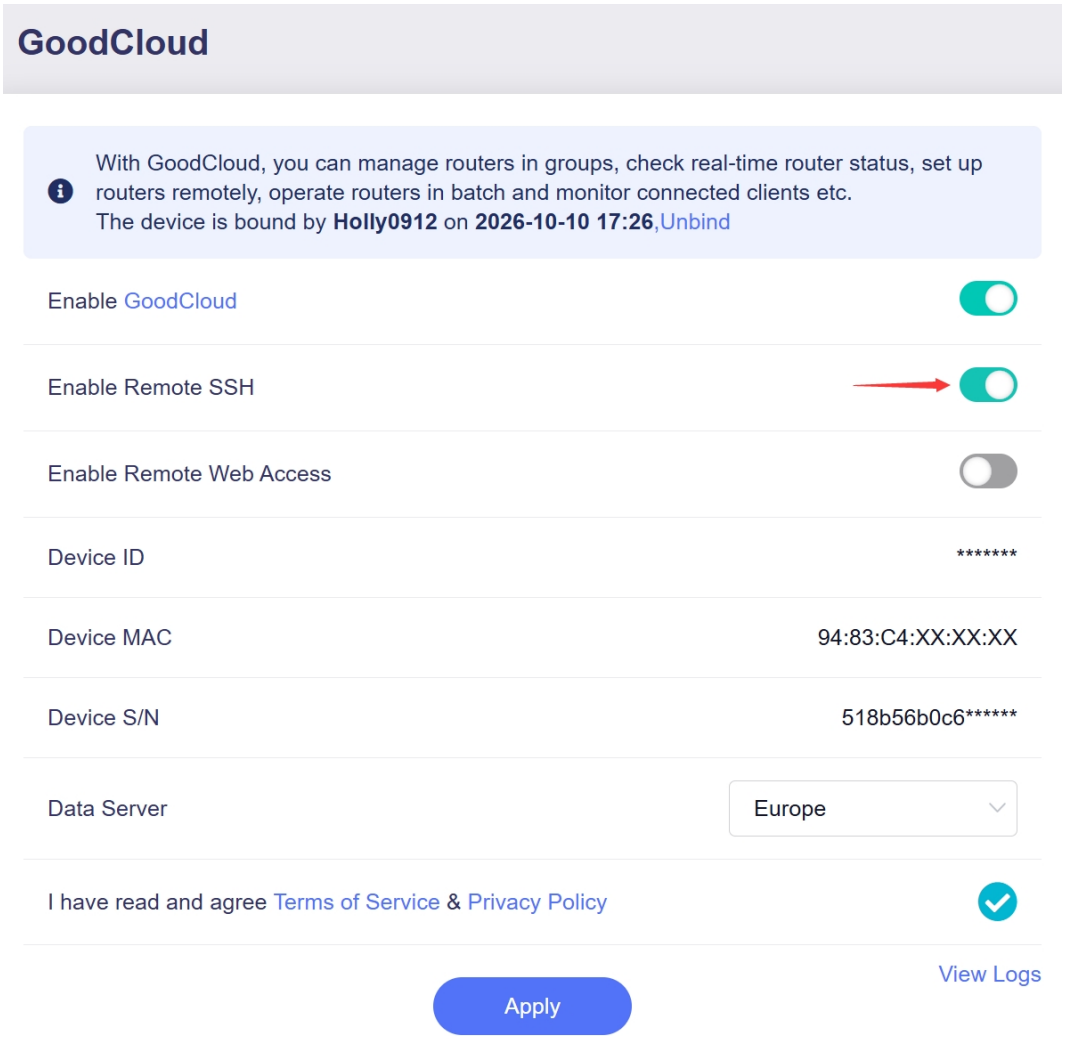


5. You will be re-directed to the router's login page. Enter the admin password to remotely access the router's web admin panel.

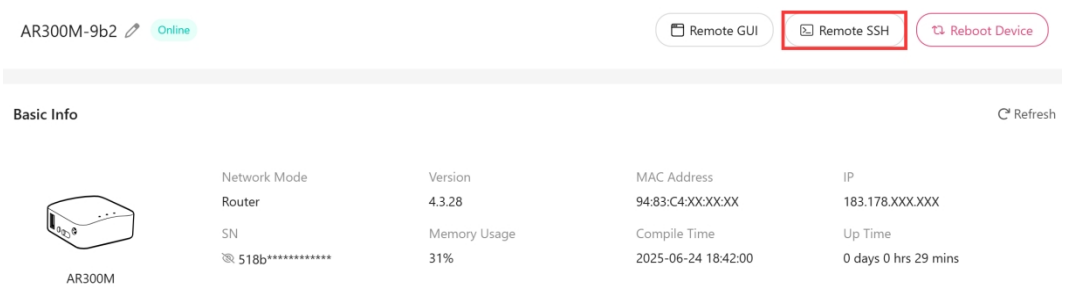


Remote SSH

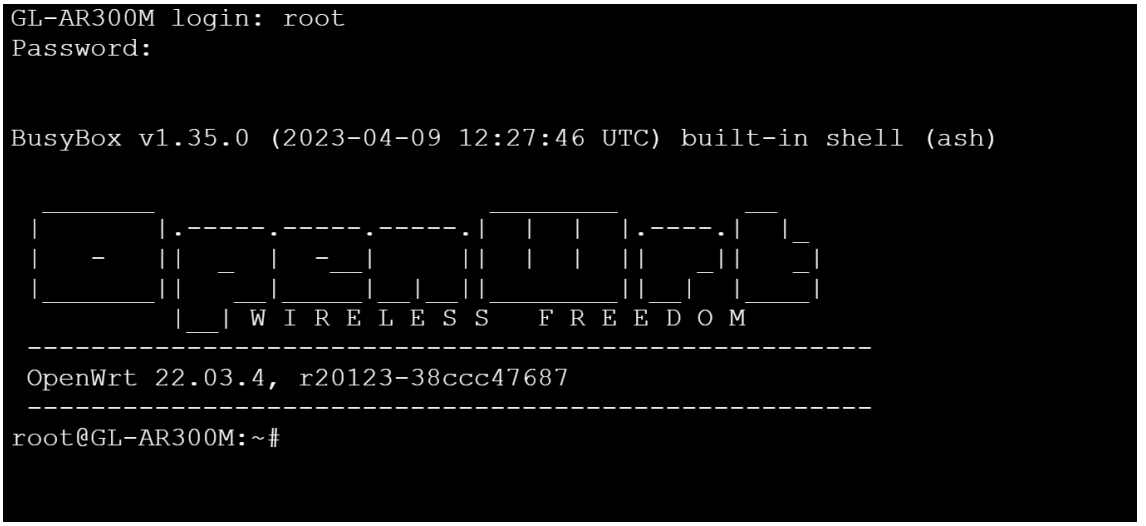
1. Log in to the router's web admin panel, navigate to **APPLICATIONS** > **GoodCloud**, enable **Remote SSH**, then click **Apply**.



2. Log in to the GoodCloud platform and navigate to **Devices** > **Bound Devices**. Click the device you want to access, and you will enter the device details page.
3. On the device details page, click the **Remote SSH** button in the upper right corner.

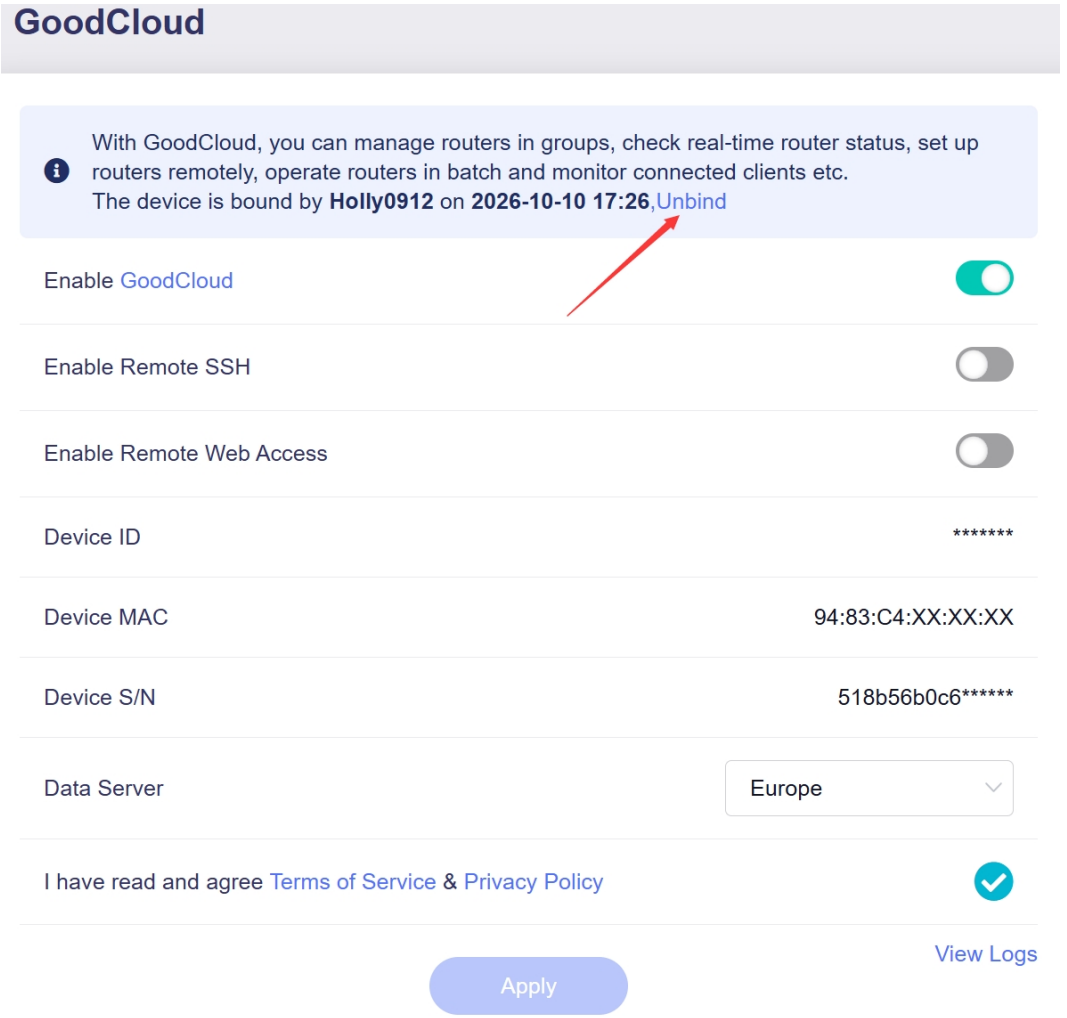


4. Log in as **root** and input the password to access the terminal of your router.

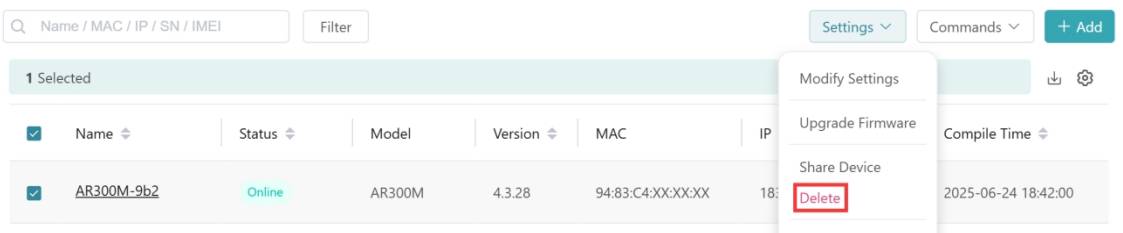


11.3.3 Unbind Device

In the router's web admin panel, click **Unbind**. Your device will then be unbound from your GoodCloud account.



Alternatively, log in to the Cloud platform and navigate to **Devices** > **Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



Chapter 12

Network

This chapter introduces network-related settings for configuration and management, such as LAN, DNS, and IPv6.

12.1 Firewall

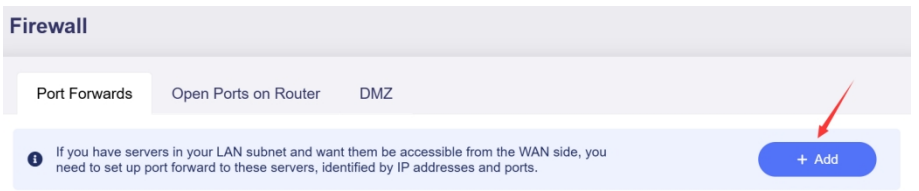
Firewall is a network feature that routes external requests to specific devices on your local network. The Firewall page includesthree key functions: **Port Forwards** (for targeted access to specific ports of devices), **Open Ports on Router** (for access to services running on the router itself) and **DMZ** (for direct full access to a single device).

12.1.1 Port Forwards

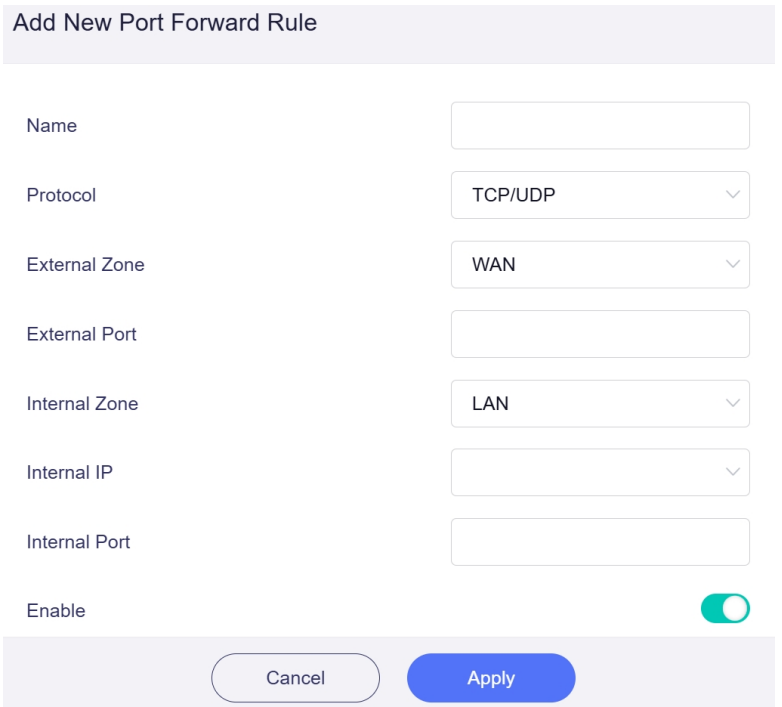
Port Forwards enables remote computers to connect to a local computer or server behind the LAN firewall (e.g., web servers, FTP servers).

If you need to set up port forwards, follow the steps below.

1. Log in to your router's web admin panel, go to **NETWORK** > **Firewall** > **Port Forwards** section, and click **Add**.



2. In the pop-up window, enter or select the required parameters from the drop-down list to add a port forward rule, then click **Apply**.

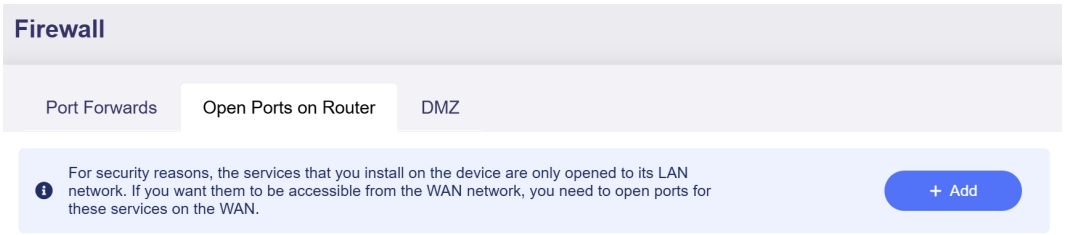


- **Name**: The name of the rule which can be specified by the user.
- **Protocol**: The protocol used. You can choose TCP, UDP, or both TCP and UDP.
- **External Zone**: Available options are WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN, and Guest.
- **External Port**: The number(s) of external ports. Enter a specific port number here. The port range is 1–65535. You can set a single port or a port range by concatenating the first and last port numbers with a hyphen (e.g., 501-510).
- **Internal Zone**: Available options are LAN, Guest, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, and WAN.
- **Internal IP**: The IP address assigned by the router to the device that needs remote access. If you set a single port in External Port, set a single port here. If you set a port range in External Port, set the corresponding port range here.
- **Internal Port**: The internal port number of the device. Enter a specific port number. Leave it blank if it matches the external port.
- **Enable**: Enable or disable this rule.

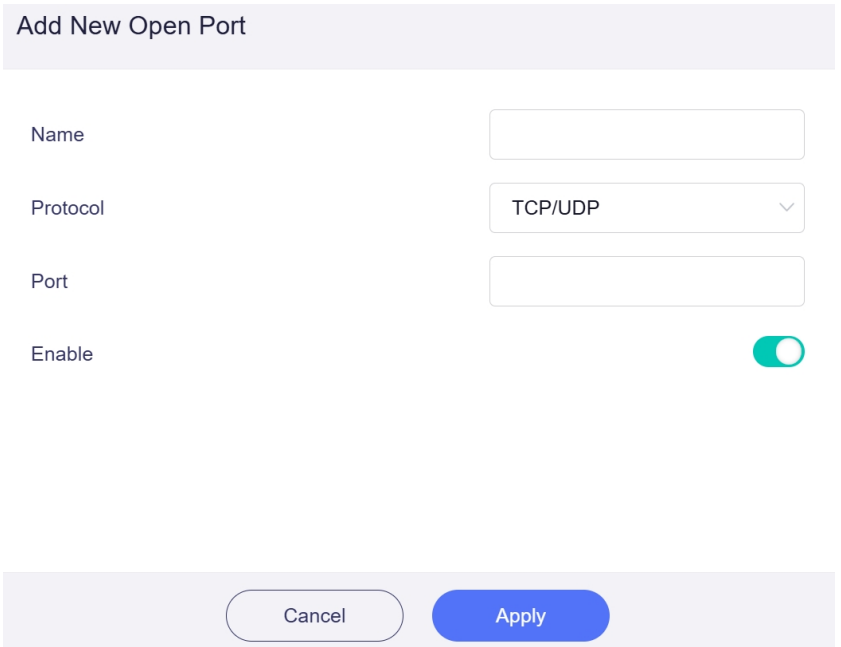
12.1.2 Open Ports on Router

The router's services, such as web and FTP, requires their respective ports to be opened on the router in order to be publicly reachable.

To open a port, switch to the Open Ports on Router tab, then click Add.



In the pop-up window, open a new port and click Apply.



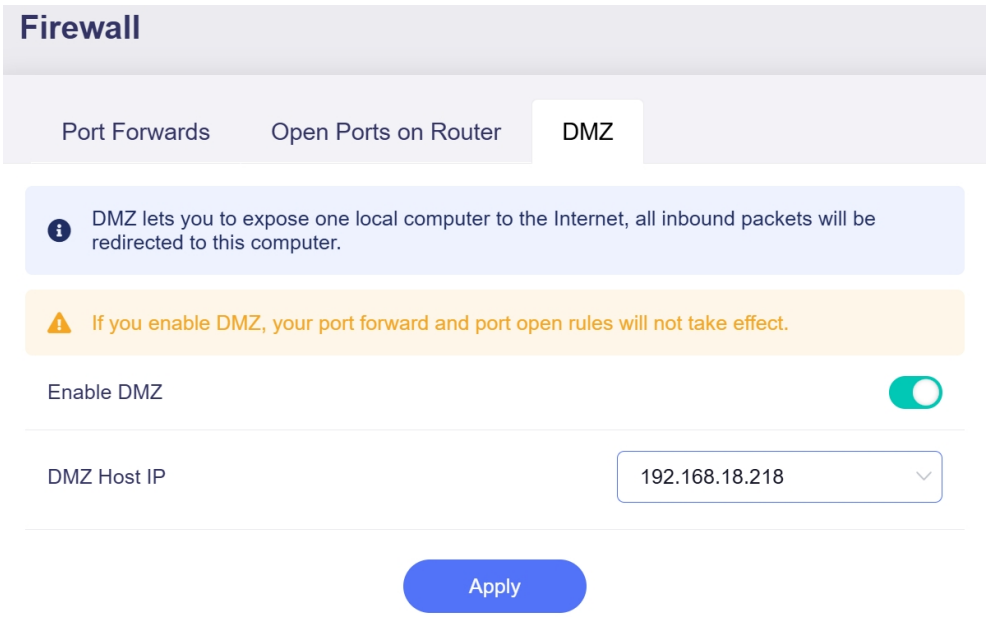
- **Name**: The name of the rule which can be specified by the user.
- **Protocol**: The protocol used, you can choose TCP, UDP, or both TCP and UDP.
- **Port**: The port number that you want to open.
- **Enable**: Enable or disable this rule.

12.1.3 DMZ

DMZ allows you to expose one computer to the Internet, so all inbound packets will be redirected to this computer.

Follow the steps below to enable DMZ if needed.

1. Log in to your router's web admin panel and navigate to **NETWORK** > **Firewall** > **DMZ** section.
2. Toggle on **Enable DMZ**, then select the **DMZ Host IP** from the drop-down list. The selected device receives all inbound packets. Click **Apply** to save the settings.



12.2 Multi-WAN

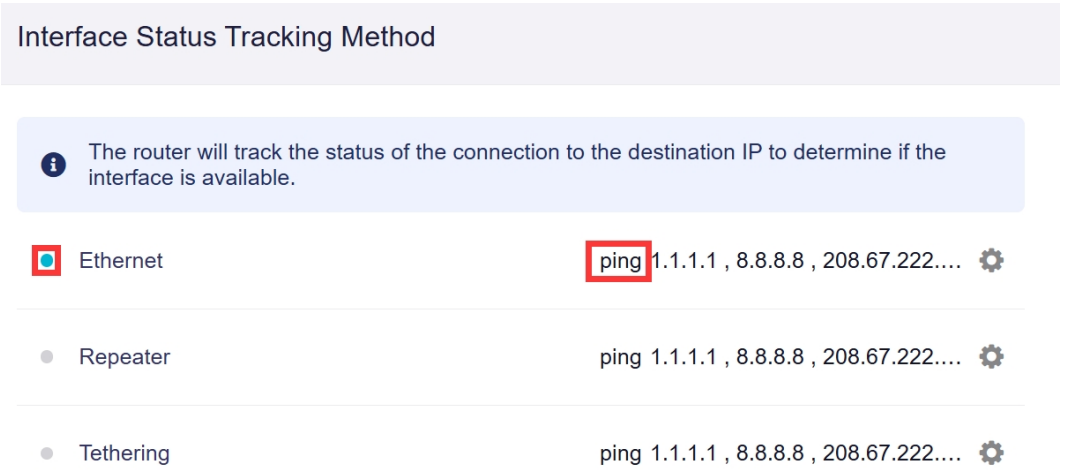
Multi-WAN enables simultaneous use of multiple Internet access methods, allowing configuration of diverse connectivity options on the router. It offers two working modes:

- **Failover**: Automatically switches to an alternate connection within a short time if the primary connection fails, ensuring uninterrupted network access.
- **Load Balance**: Distributes network traffic across all available connections at a set ratio for concurrent multi-connection usage, optimizing bandwidth utilization.

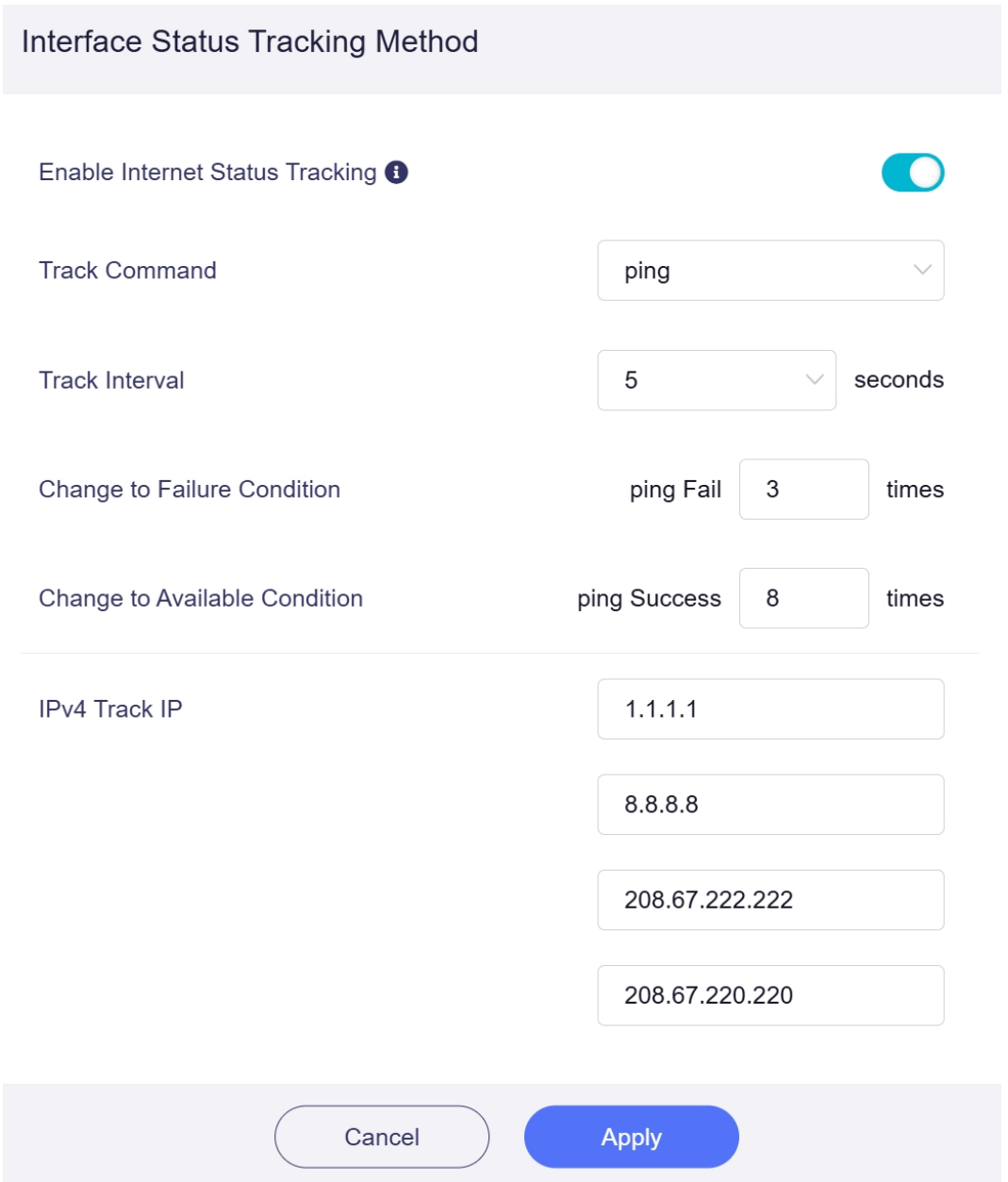
Log in to your router's web admin panel and navigate to **NETWORK** > **Multi-WAN**. This page includes two sections: Interface Status Track and Multi-WAN Mode.

12.2.1 Interface Status Track

GL.iNet routers use the **ping** command to monitor the connection status to the destination IP and determine if the interface is available. If the interface is available, a green dot will be displayed on the left; otherwise it will be gray.



In the **Interface Status Track** section, click the gear icon on the right to access the status tracking settings for each network interface. Below are the status tracking settings for the Ethernet interface. The same configuration logic applies to other interfaces.



- **Enable Interface Status Track**: It is enabled by default. If disabled, the router will determine the interface status based on physical conditions (e.g., whether the Ethernet cable is plugged in).
- **Track Command**: The ping command is used to monitor connection status to the destination IP and verify interface availability.
- **Track Interval**: Set how often the router executes the track command. The unit is seconds.
- **Change to Failure Condition**: The router will mark this interface as disconnected after the specified number of consecutive ping failures.

- **Change to Available Condition**: The router will restore the interface to connected status after the specified number of consecutive ping successes.
- **IPv4 Track IP**: Customize the IPv4 Track IP addresses if needed.

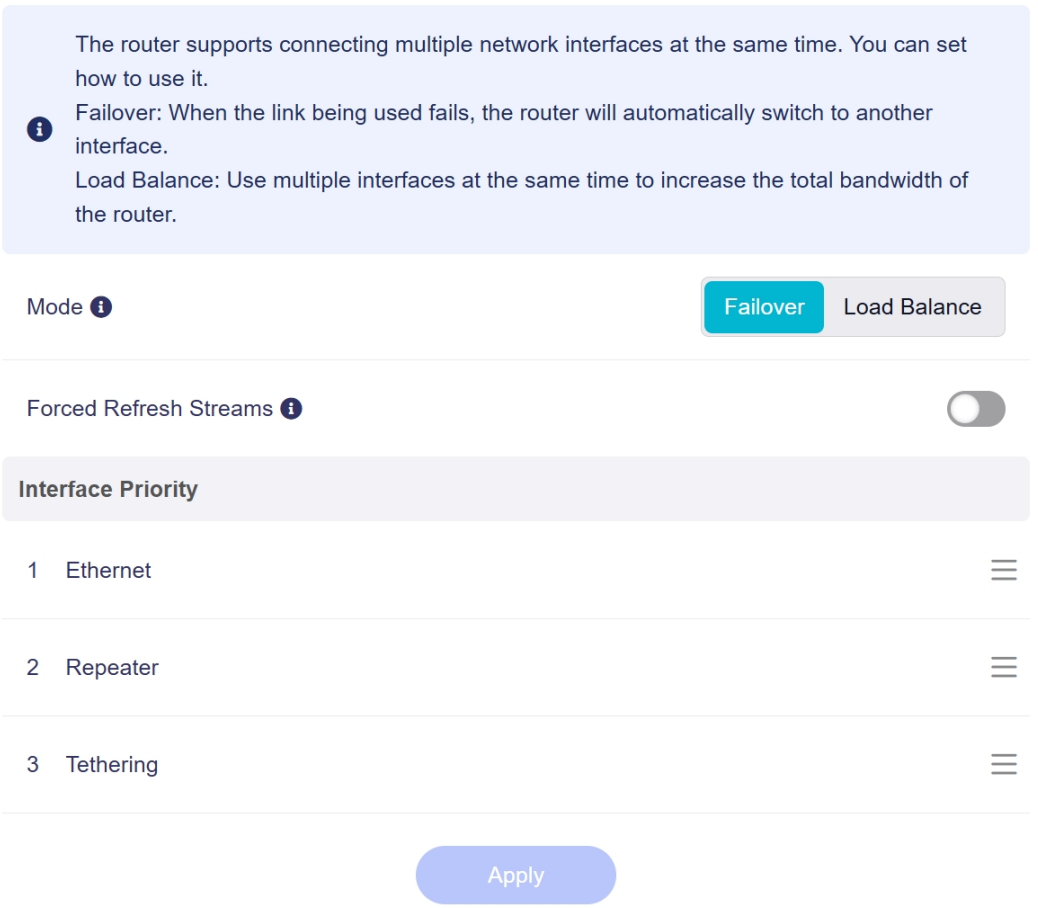
12.2.2 Multi-WAN Mode

Two modes are available for Multi-WAN: **Failover** and **Load Balance**. Note that these modes are mutually exclusive.

Failover

Failover is the default mode when multiple connections are configured. If the active link fails, the router will automatically switch to another network interface for Internet access.

You can set priority levels for each interface: when the currently used interface fails, the router switches to the next available interface with the highest priority. Once a higher-priority connection is restored, the router will automatically switch back to it.

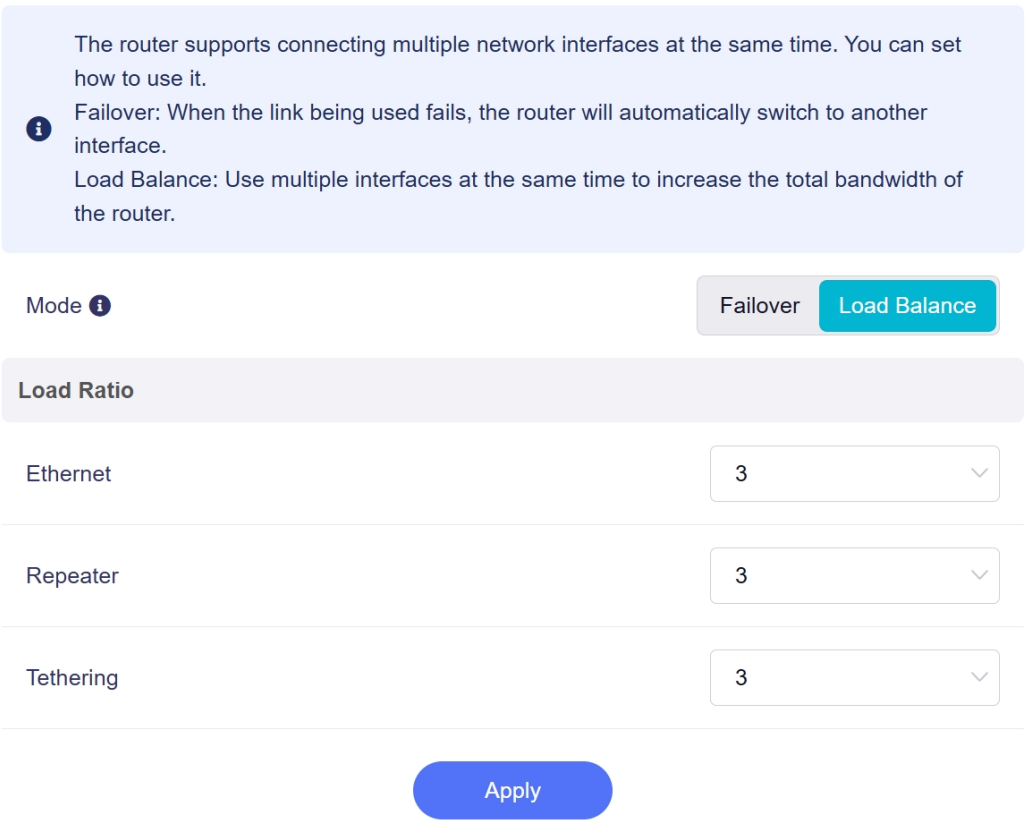


Load Balance

Load Balance mode uses multiple network interfaces simultaneously to increase the router's total bandwidth, with the system distributing new connections across interfaces according to a configured load ratio. Note that connections to the same application or website will typically use only one interface.

The load ratio refers to the proportion between each network interface. The system will assign interfaces to handle new connections based on this configured ratio.

For example, if the router is connected to three networks (e.g., Ethernet, Repeater, and Tethering) simultaneously and all interfaces are available for Internet access, enabling Load Balance and setting a 1:1:1 ratio means the three interfaces will share network bandwidth equally. The system will distribute new connections across these interfaces according to the configured 1:1:1 load ratio.



You can also customize the load ratio if needed. For example, if Ethernet has a bandwidth of 100 Mbps, Repeater has 200 Mbps, and no Tethering connection are active, set the load ratios to 1 for Ethernet, 2 for Repeater, and 0 for Tethering. The system will then distribute

new connections across these interfaces according to the configured 1:2 ratio, meaning Ethernet will handle half as many connections as Repeater. Unlike Failover mode, this mode optimizes overall throughput efficiency by balancing traffic load across all available interfaces.

Note: Existing connections or traffic are not guaranteed to align with the load ratio. The actual distribution will gradually approach the configured ratio with prolonged use.

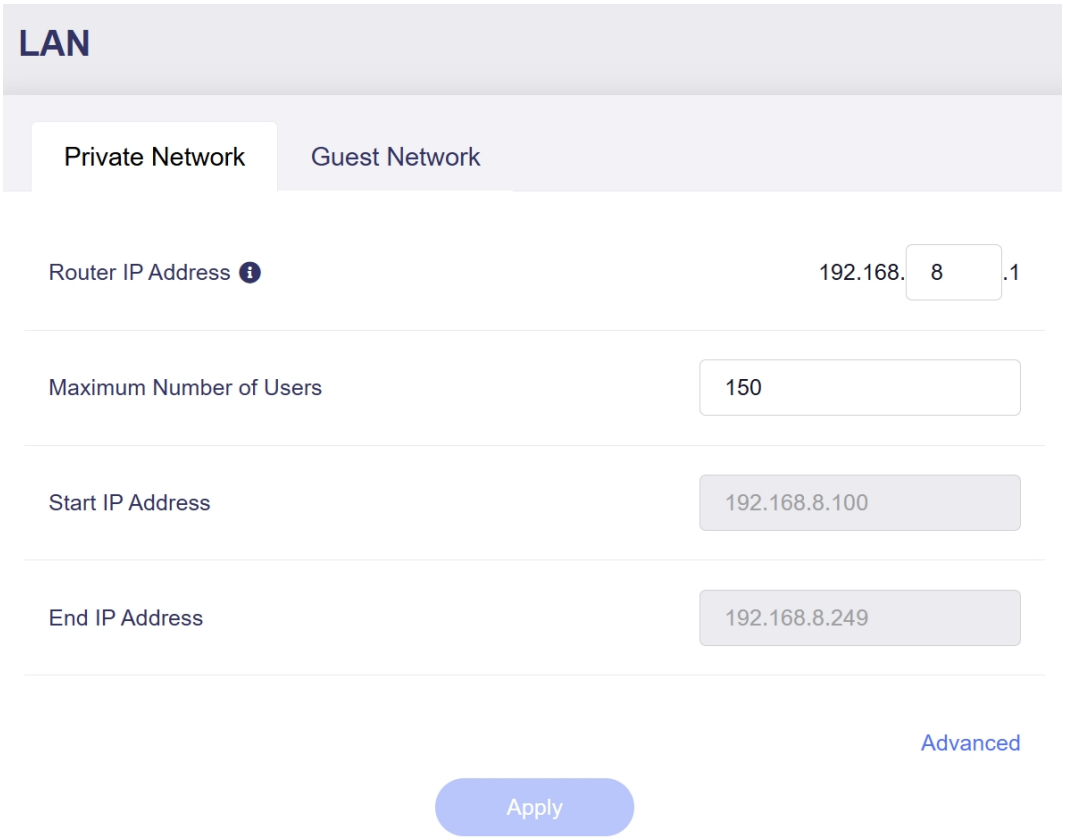
12.3 LAN

LAN (Local Area Network) refers to the private local network, to which your devices connect via Ethernet cables.

Log in to your router's web admin panel and navigate to **NETWORK** > **LAN** . Here you can configure LAN settings, including Private Network and Guest Network.

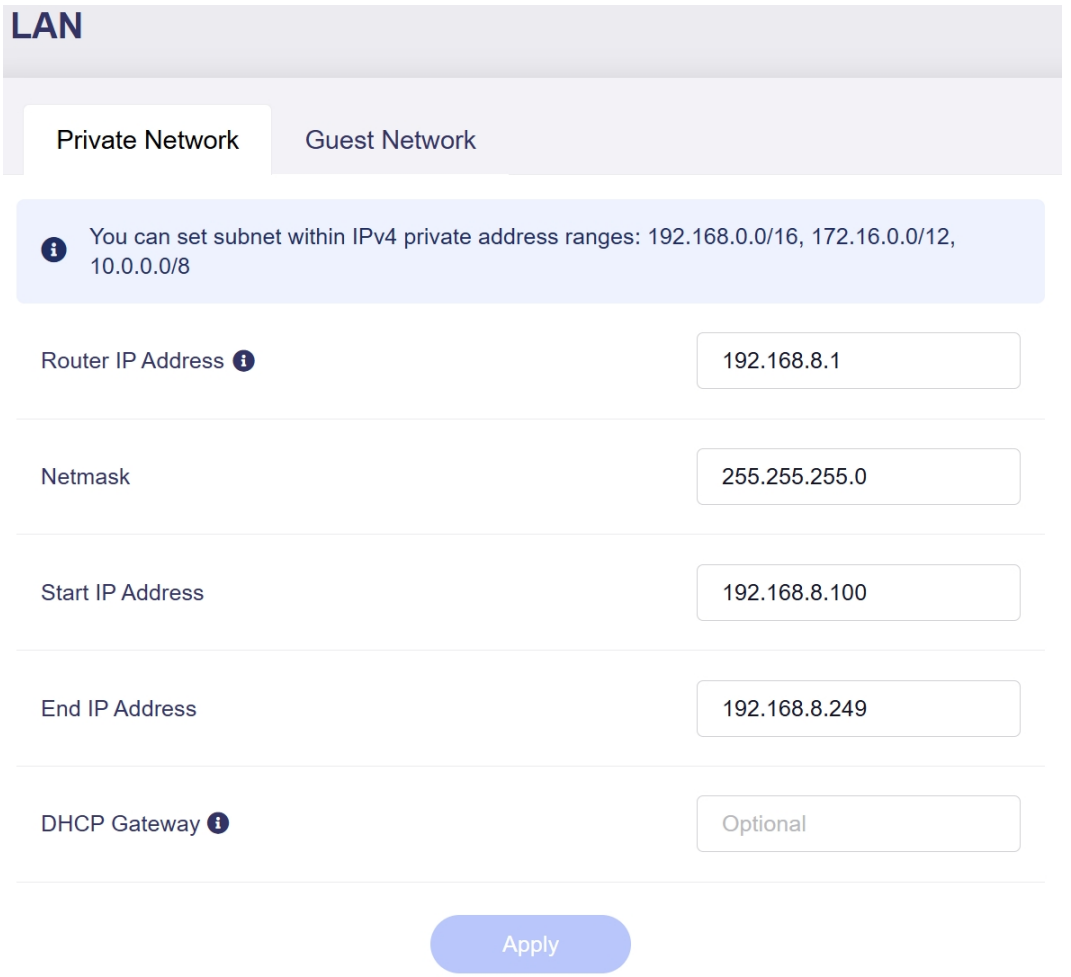
12.3.1 Private Network

The Private Network is the main local network for your connected devices. You can configure the router IP address, DHCP address range, and maximum number of connected clients.



- **Router IP Address**: This is the address entered into a browser's address bar to access the router's admin panel. It is 192.168.8.1 by default and can be changed if it conflicts with the upstream network.
- **Maximum Number of Users**: Set the maximum number of clients allowed to connect to the guest network.

Click **Advanced** to modify advanced settings, including Default Gateway, Netmask, Start IP Address, End IP Address and DHCP Gateway.

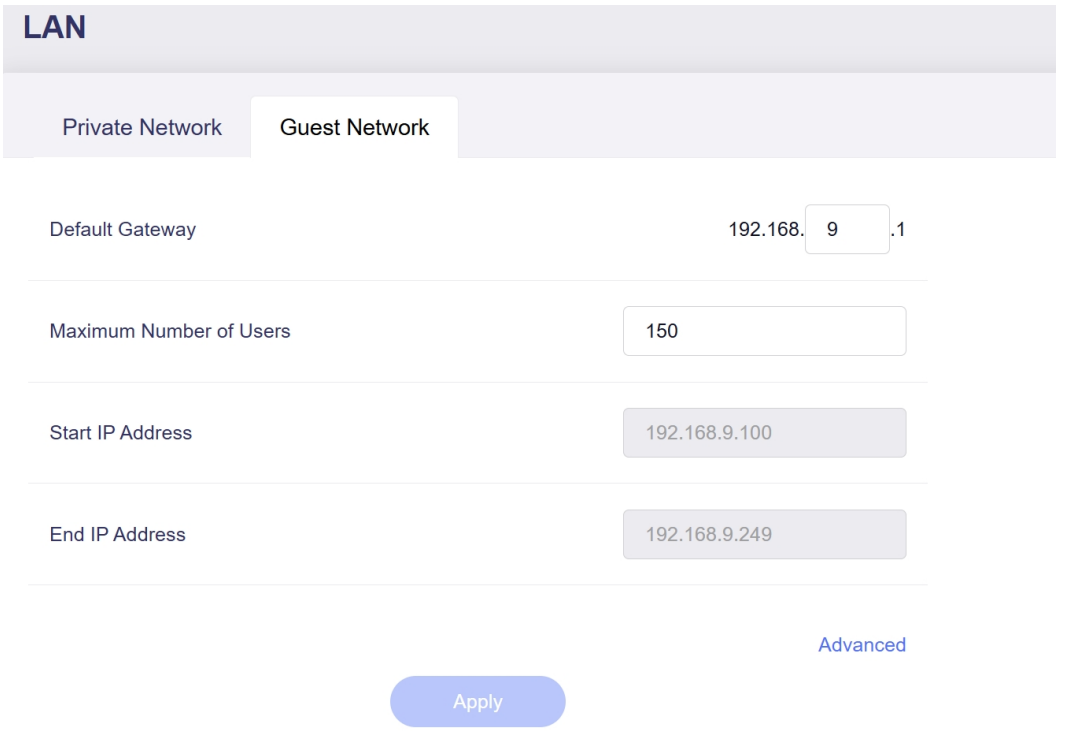


- **DHCP Gateway**: The default gateway address assigned to clients by the DHCP server. It routes traffic from the local network to external networks, such as the Internet.
- **Netmask**: The subnet mask for the Private Network. The default value is 255.255.255.0.

12.3.2 Guest Network

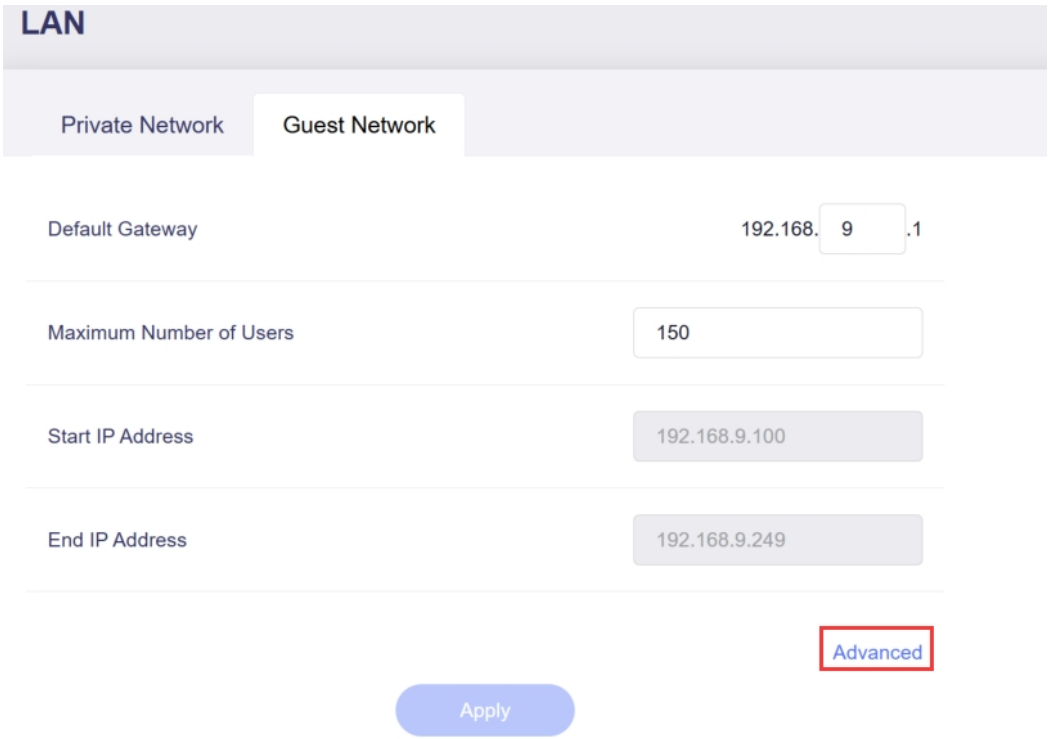
Guest Network refers to a dedicated network for visitors to connect to, isolating them from your main LAN to protect your private network security.

Log in to your router's web admin panel and go to **NETWORK** > **LAN** > **Guest Network**. This page allows you to configure Guest Network settings.

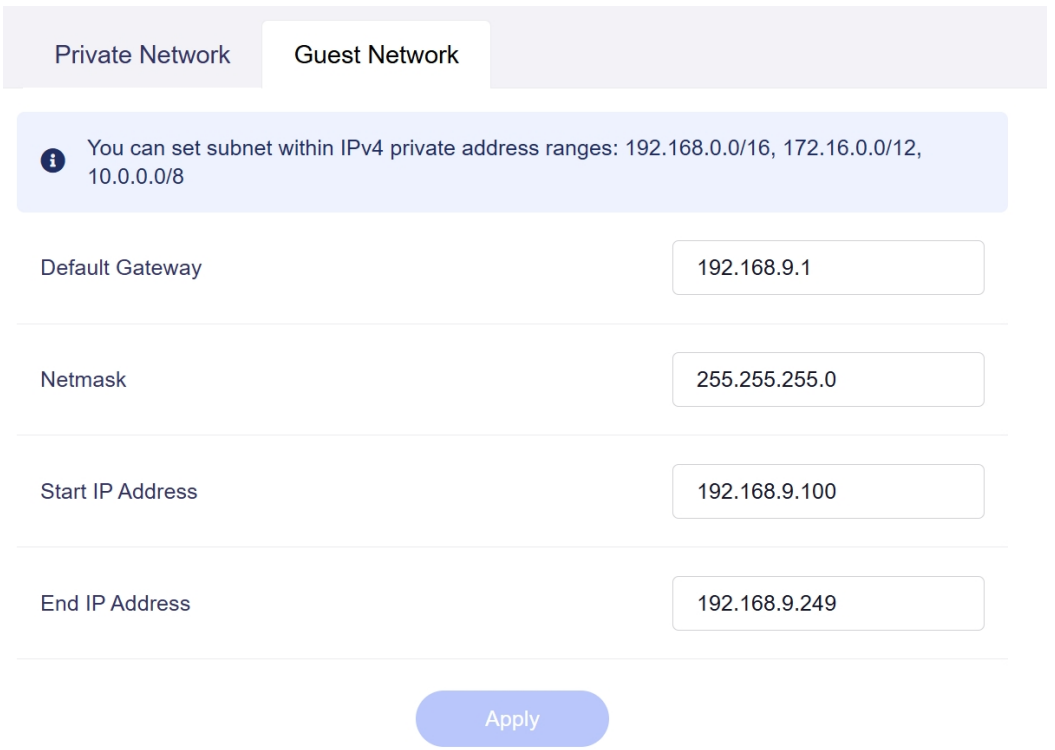


- **Default Gateway**: It is 192.168.9.1 by default and can be changed if needed, but it must not conflict with the gateway of the main network.
- **Maximum Number of Users**: Set the maximum number of clients allowed to connect to the guest network.

Click **Advanced** in the bottom right corner.



You will be able to configure advanced settings, including Default Gateway, Netmask, Start IP Address and End IP Address.



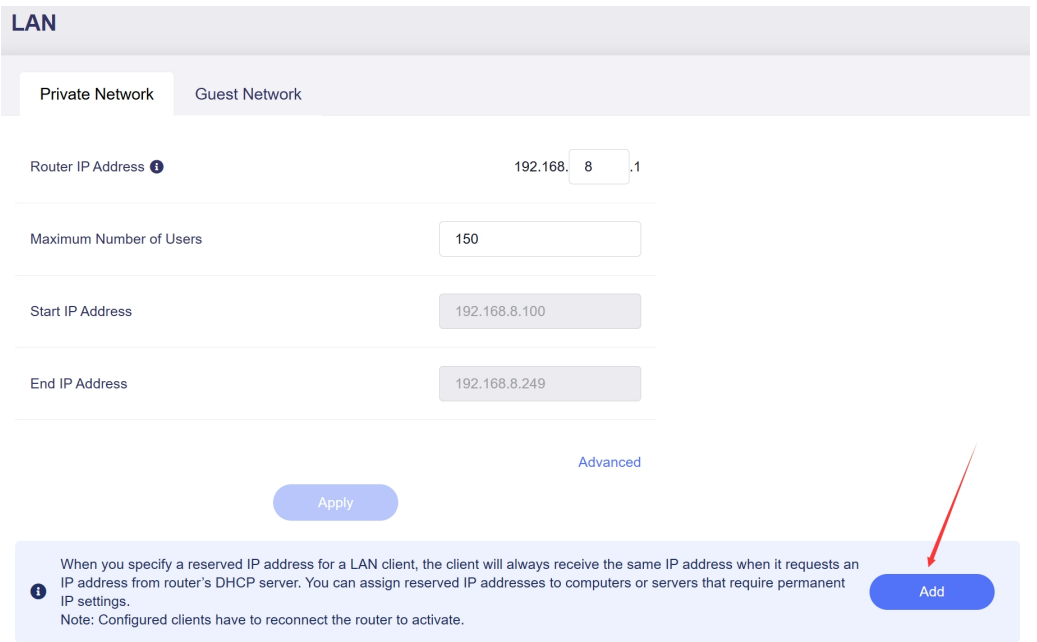
The **Netmask** defaults to 255.255.255.0. You can also select 255.255.0.0 if you need a larger subnet with more IP addresses.

12.3.3 Address Reservation

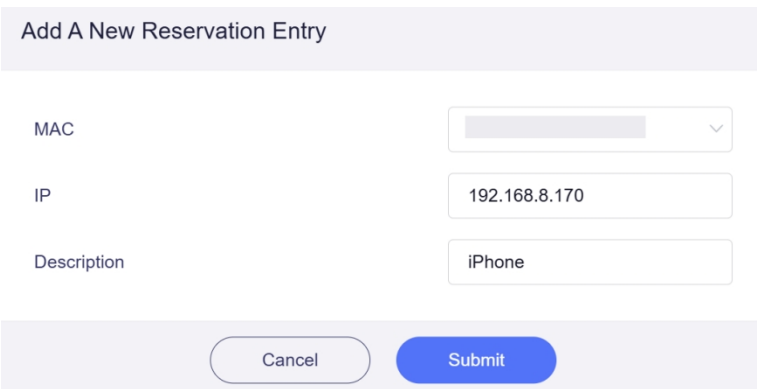
Address reservation allows you to specify a fixed IP address for a LAN client, so that the client will always receive the same IP address each time it accesses the router's DHCP server. You can assign reserved IP addresses to computers or servers that require permanent IP settings. Note that clients with address reservation configured must reconnect to the router to activate the setting.

Follow the steps below to configure address reservation if needed.

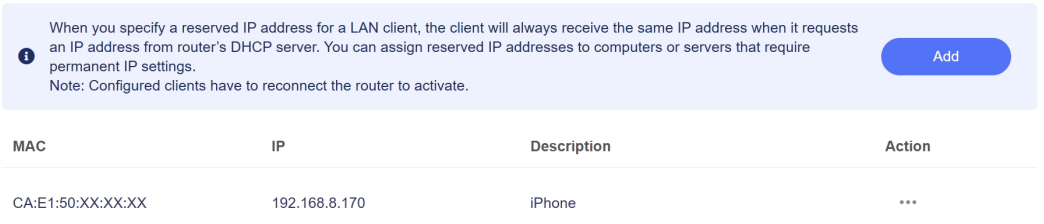
1. Log in to your router's web admin panel, navigate to **NETWORK** > **LAN** > **Address Reservation**, and click **Add**.



2. In the pop-up window, select the MAC address from the drop-down list, then the corresponding IP address for the selected MAC will be auto-filled. Enter a descriptive name and click **Submit**.



3. After adding a new IP address reservation, the page will display the reserved entry, as shown below.



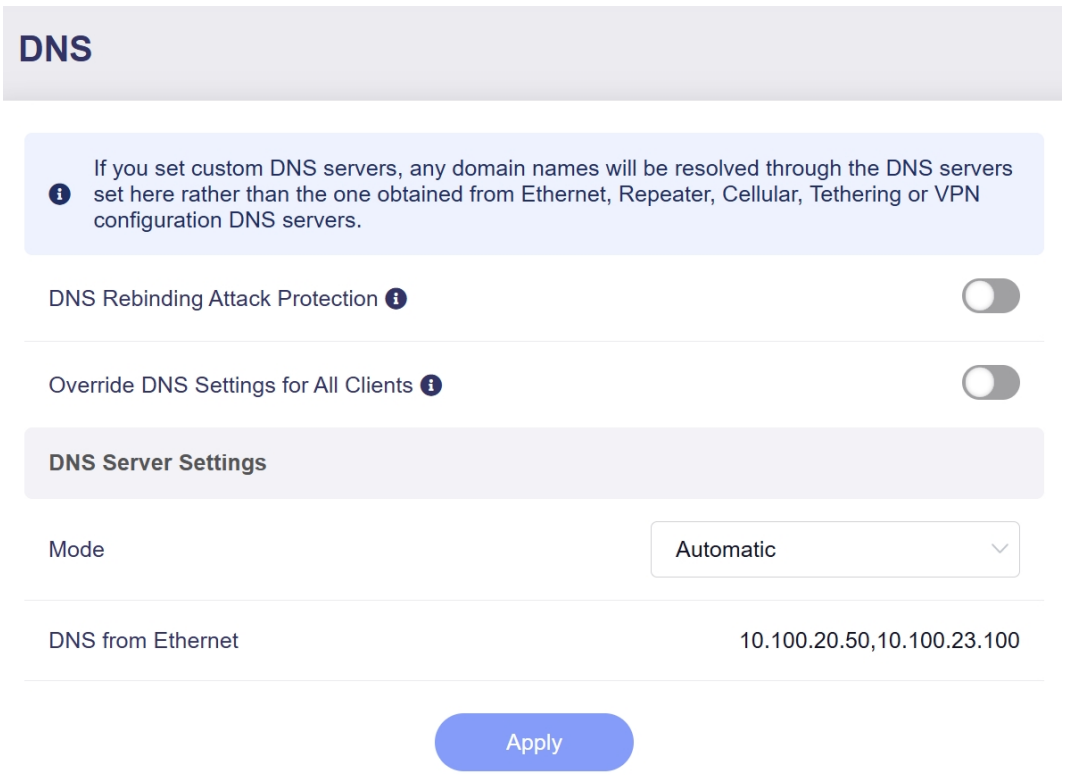
12.4 DNS

DNS (Domain Name System) is a service that translates human-readable domain names, such as www.google.com, into IP addresses so that devices can locate and connect to websites and online services.

On a router, DNS settings usually determine which DNS servers are used by connected devices. In most cases, the router either obtains DNS server addresses automatically from the ISP or upstream network, or allows users to manually specify public DNS servers, such as 8.8.8.8, in the web management interface. Once configured, these DNS settings are typically distributed to connected devices automatically, so there is no need to configure DNS separately on each device.

Log in to your router's web admin panel and navigate to **NETWORK** > **DNS**. This page allows you to configure DNS related settings.

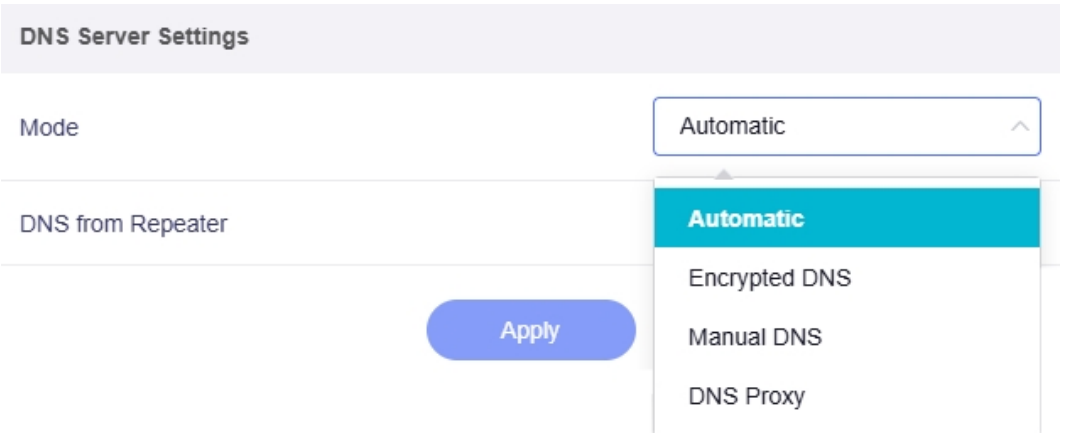
12.4.1 General Settings



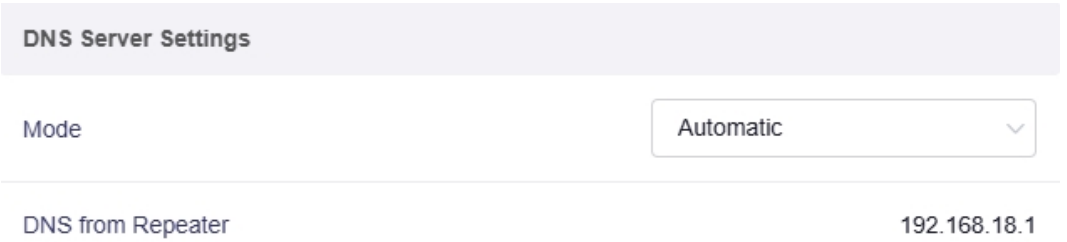
- **DNS Rebinding Attack Protection**: Protects against DNS rebinding attacks by blocking malicious DNS resolution attempts. Note that enabling it may cause private DNS lookup failure; disable if your network uses a captive portal (e.g., public Wi-Fi login pages).
- **Override DNS Settings of All Clients**: If enabled, all connected devices will be forced to use the DNS servers configured on the router, ignoring their own original DNS settings. It enables unified DNS configuration for all devices.

12.4.2 DNS Server Settings

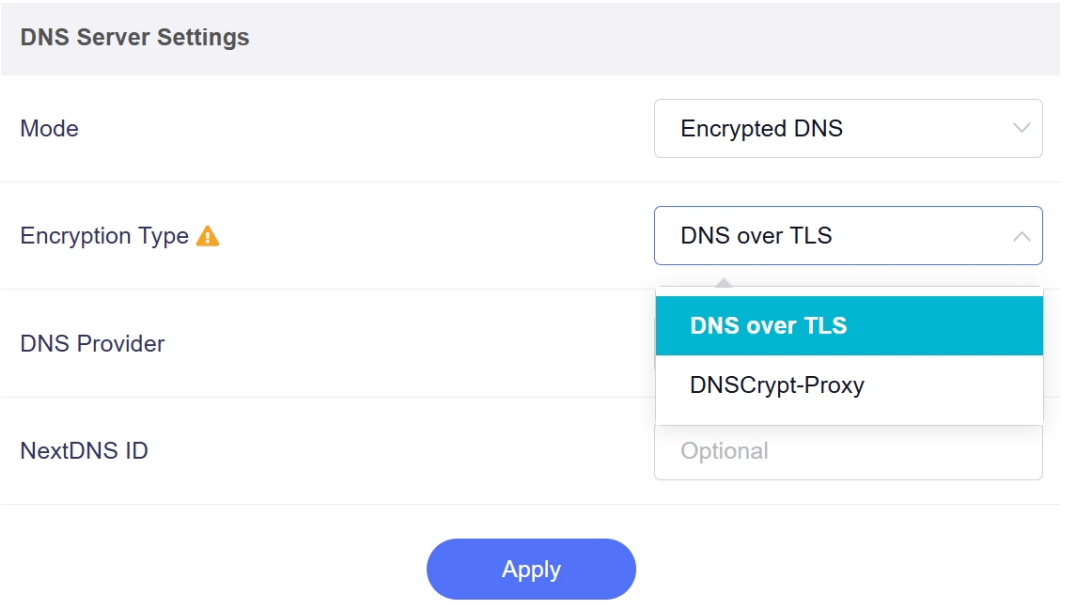
There are four modes for the DNS server: Automatic, Encrypted DNS, Manual DNS, and DNS Proxy.



1. **Automatic**: When selected, the router will automatically obtain DNS server addresses from the upstream network and apply them to all connected devices.

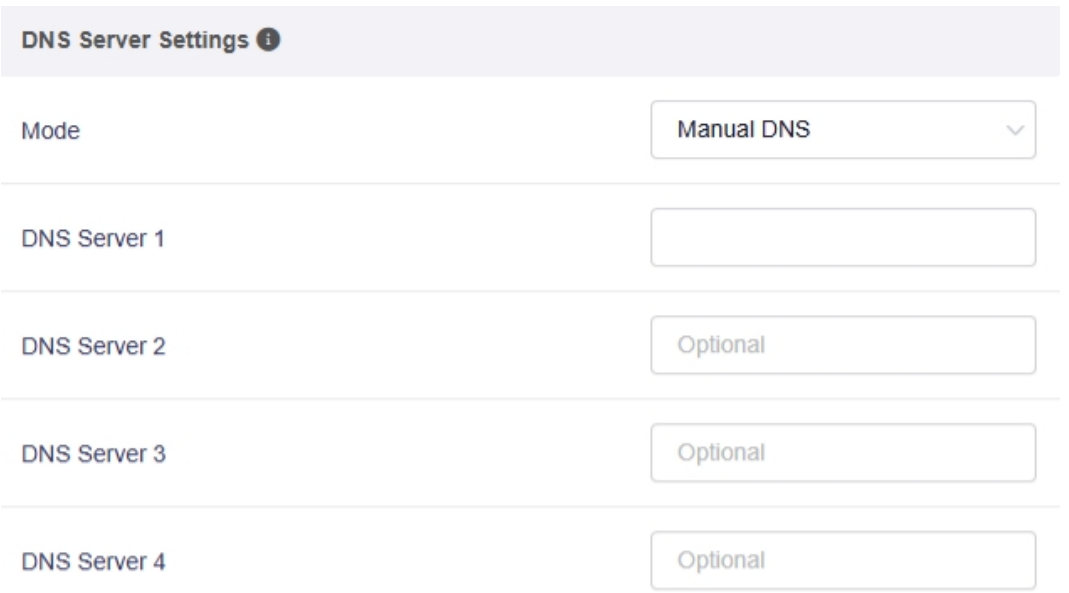


2. **Encrypted DNS**: When selected, the router will use encrypted protocols to process DNS queries, securing resolution data against eavesdropping or tampering.
   It has two encryption types: DNS over TLS, and DNSCrypt-Proxy.



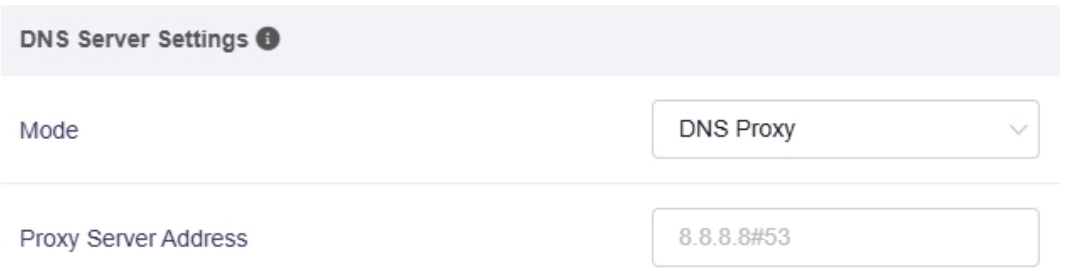
- For DNS over TLS, select a DNS provider among Control D, NextDNS, and Cloudflare.
- For DNSCrypt-Proxy, select at least one DNS server from the repository. Up to 8 servers can be selected. When multiple servers are selected, the router will use the fastest one automatically.

3. **Manual DNS**: When selected, you can customize your router's DNS servers. Click DNS Server 1 and choose a DNS server from the drop-down list. The remaining DNS fields will update automatically.



Note: If you need to use IPv6 addresses for manual DNS, enable IPv6 on your router first.

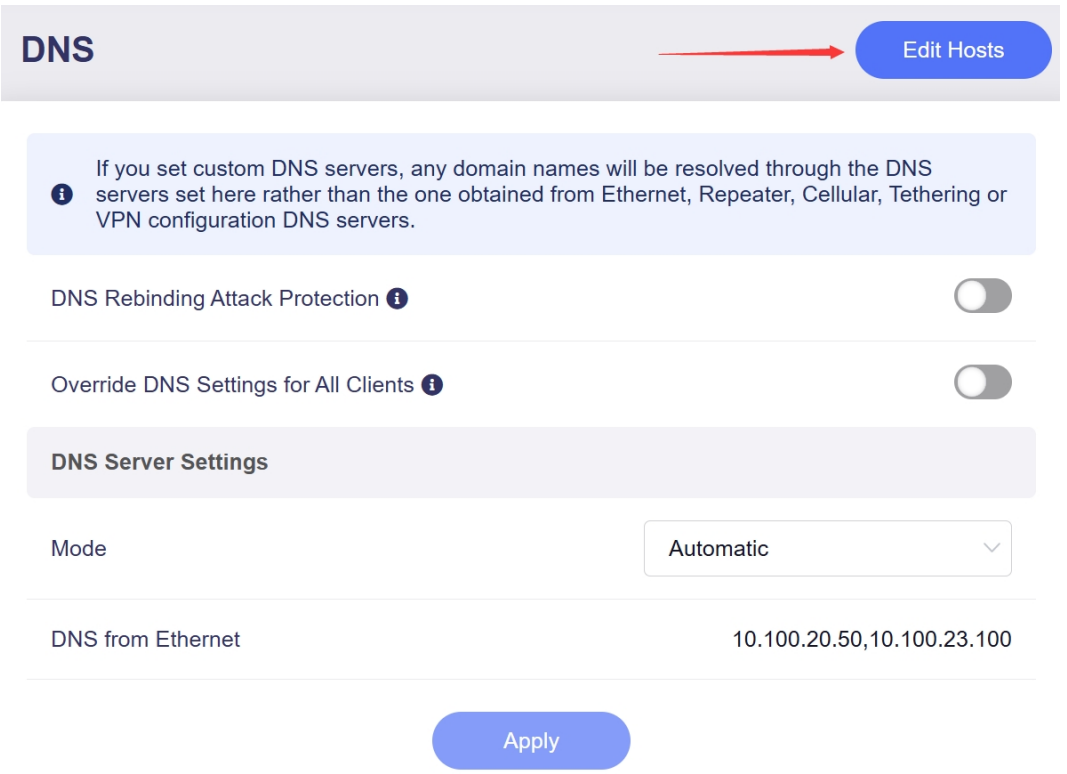
4. **DNS Proxy**: When selected, the router forwards all DNS queries through a proxy server, allowing resolution via the proxy's network environment for specific access needs.



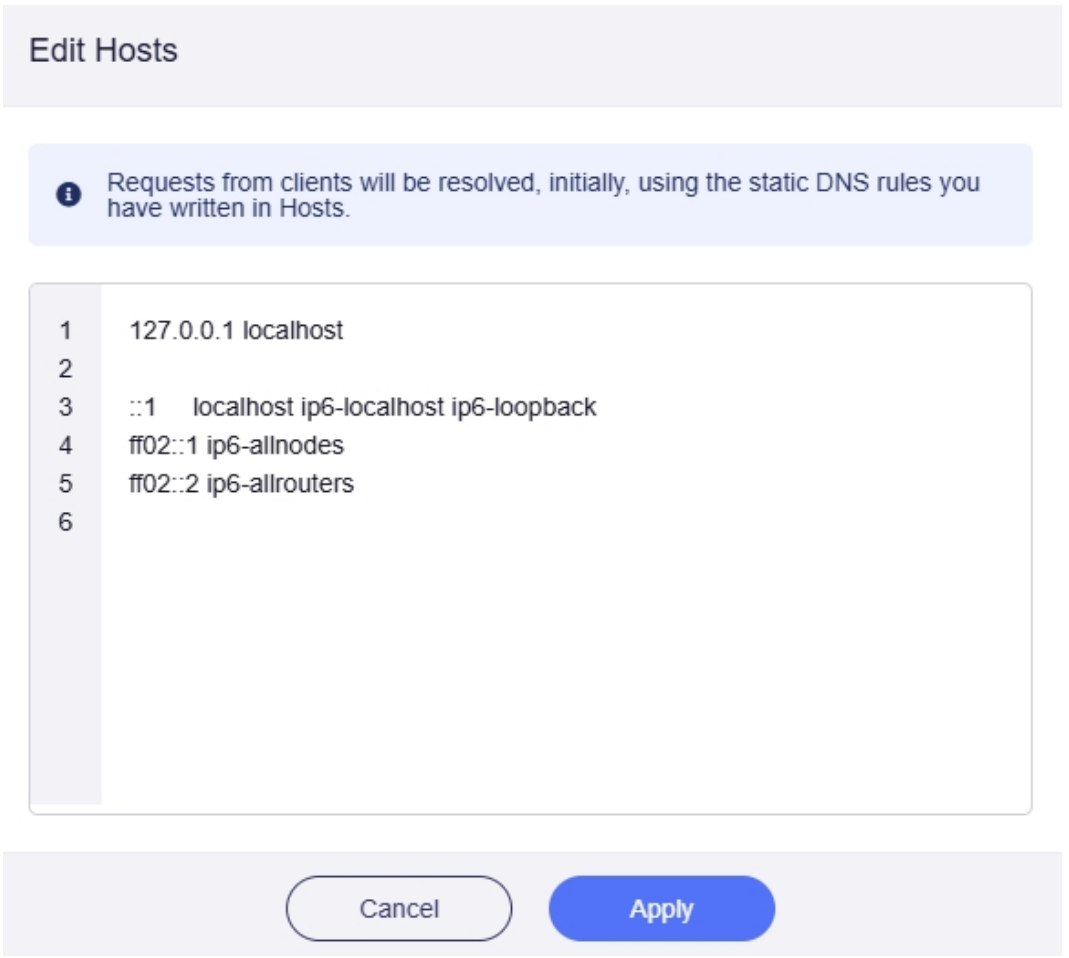
12.4.3 Edit Hosts

You can define static DNS resolution rules if needed.

On the DNS page, click **Edit Hosts** in the top right corner.



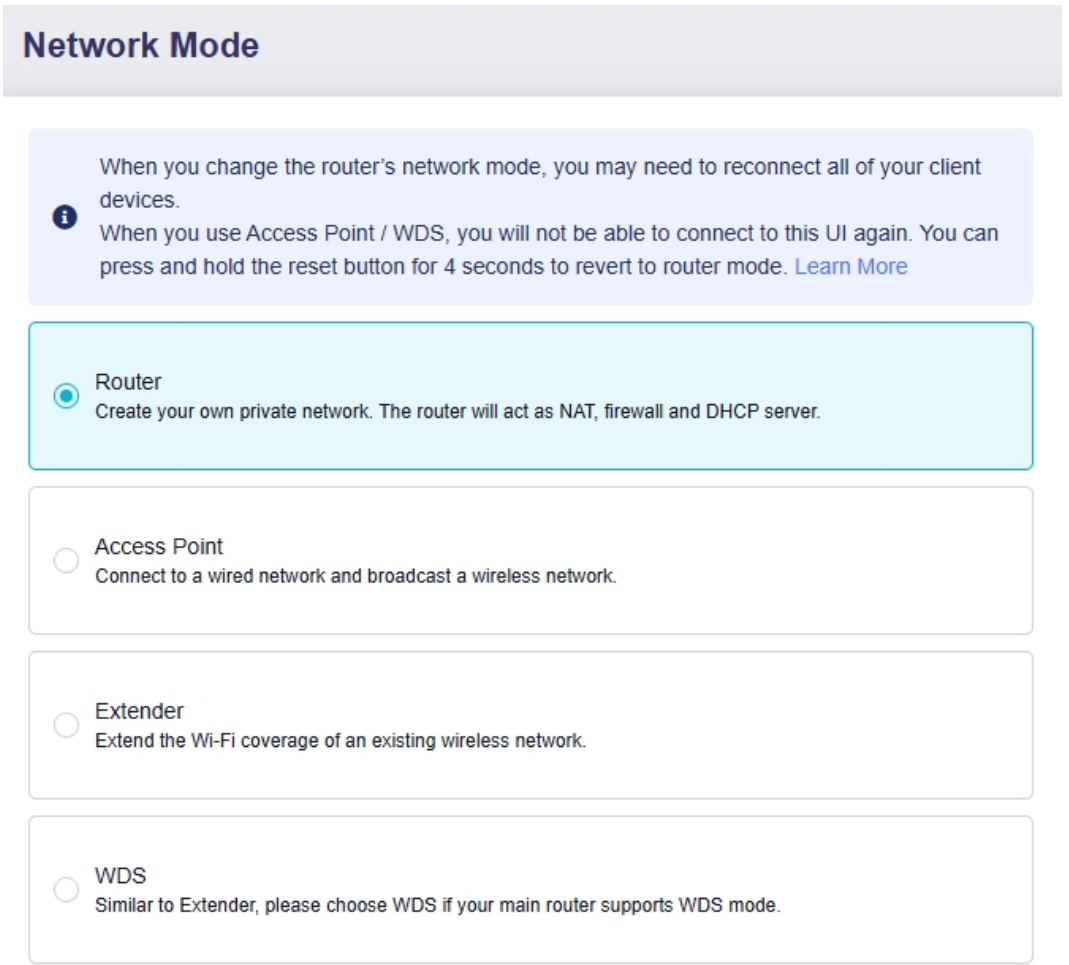
Requests from clients will be resolved preferentially using the static DNS rules written here, allowing you to manually map IP addresses to hostnames (e.g., the default entries like 127.0.0.1 localhost for local loopback) for customized domain name resolution control.


Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 Network Mode

Network mode refers to the different operational roles and functions a router can assume to meet various network deployment needs.

Log in to your router's web admin panel and navigate to **NETWORK** > **Network Mode**. You can change the network mode of your router.



- **Router**: This is the default operational mode for most home and small office routers, designed to create a private local area network (LAN) and act as a dedicated gateway between the public internet and connected devices. In this mode, the router enables core functions including NAT, DHCP, and a built-in firewall. It connects to an upstream line such as broadband fiber, automatically assigns private IP addresses to connected devices, and provides network security for the entire private network.
- **Access Point**: This mode enables a router to connect to a wired network via a LAN cable and broadcast wireless signals, expanding Wi-Fi coverage in large spaces to allow more

devices to access the network. In this mode, the router disables its NAT and DHCP functions, operating purely as a wireless signal transmitter and switch rather than a standalone gateway.

- **Extender**: This mode is designed to extend the Wi-Fi coverage of an existing wireless network and eliminate signal dead zones in areas with poor connectivity. It enables the router to wirelessly receive signals from the main router, amplify them, and retransmit the boosted signal. Unlike Access Point mode, it requires no wired connection to the main router, but it may lead to bandwidth halving, as the device has to handle simultaneous signal reception and transmission.
- **WDS**: Wireless Distribution System (WDS) mode is similar to Extender mode as it extends Wi-Fi coverage wirelessly, but it supports wireless bridging between multiple compatible routers. It is recommended for wireless network expansion when the upstream router has WDS functionality.

  This mode is ideal for scenarios like covering multi-story buildings or small office campuses where multiple routers need to work together to form a unified wireless network. Unlike Extender mode, which only transmits signals from one main router to a single extender, WDS mode allows interconnected routers to both send and receive signals, enabling seamless coverage across larger areas with multiple signal nodes.

Note:

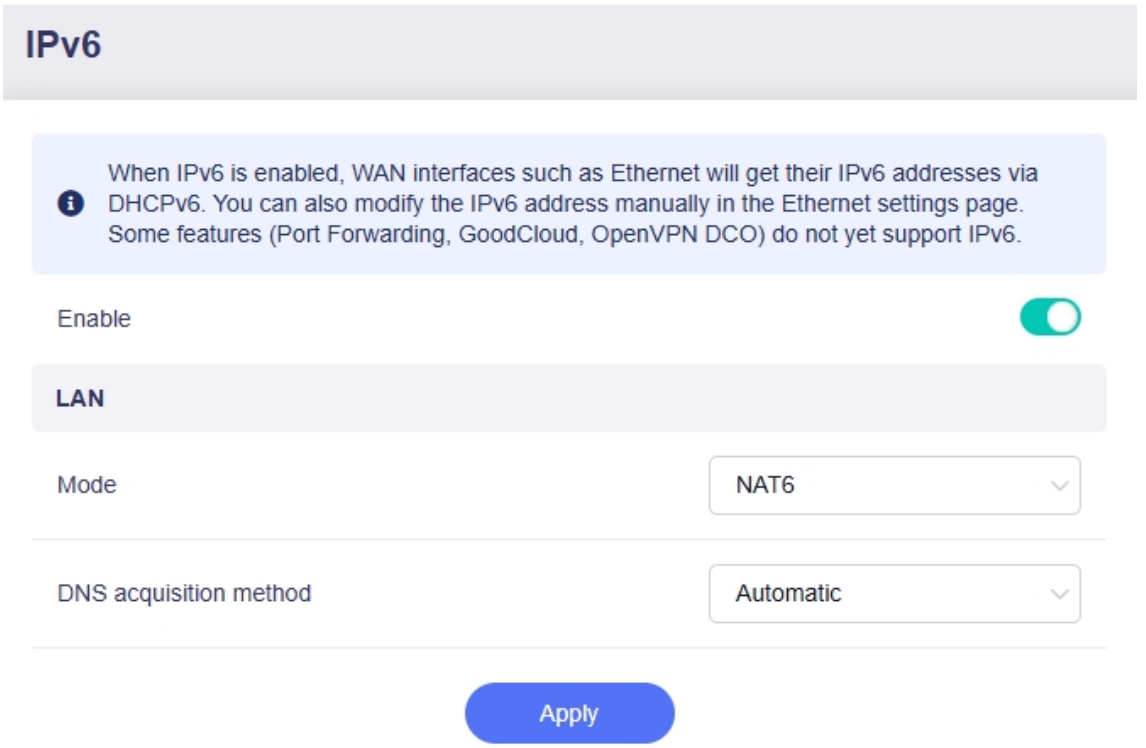
1. When the network mode is changed, all client devices shall reconnect to the router for stable network connectivity.
2. **In Access Point / WDS mode, you will not be able to access the web admin panel using the original IP address**. Instead, you need to log in to the upstream router to find the IP address it has assigned to this router, then use this IP address to access the web admin panel. If you do not have access to the upstream router, press and hold the reset button for 4 seconds to revert it to the default Router mode.
3. **In Access Point / Extender / WDS mode, the following features will be unavailable**: Access Control (Allowlist and Blocklist), VPN, Firewall, Multi-WAN, DHCP Server, Address Reservation, Guest Network, DNS, IPv6, Drop-in Gateway, IGMP Snooping.

12.6 IPv6

IPv6 (Internet Protocol version 6) is the latest Internet Protocol designed to replace IPv4. It offers a larger pool of unique IPs, solving the address exhaustion issue of IPv4 and supporting the growing number of connected devices globally.

Log in to your router's web admin panel and navigate to **NETWORK** > **IPv6**. This page allows you to enable and configure IPv6 on your router. When IPv6 is enabled, WAN interfaces such as Ethernet will get their IPv6 addresses via DHCPv6.

Toggle on **Enable**, select the mode for your main network and DNS acquisition method, then click **Apply.**



Note: Some features (e.g., firewall, GoodCloud) do not yet support IPv6. If you enable these features and IPv6 at the same time, it's likely to cause connectivity issues.

12.6.1 IPv6 Mode

Four modes are available: Native, Passthrough, NAT6 and Static IPv6.

- **Native**: This mode is applicable when the router directly obtains a public IPv6 address, and the router automatically assigns IPv6 addresses to online devices. This mode can meet the IPv6 access needs of most users.
- **Passthrough**: This mode is applicable when IPv6 packets need to be directly passed through without any processing or conversion. For example, some specific applications or services may require the complete preservation of IPv6 packet content for further processing or analysis. This mode is used by technical personnel for network debugging or security analysis.
- **NAT6**: This mode is suitable for scenarios where a router is used as a gateway to assign dynamic internal IPv6 addresses to each device on the network. In this mode, terminal devices connect through a Optical Network Terminal and obtain a local area network IPv6 address.
- **Static IPv6**: This mode is suitable for devices or services that require a fixed IPv6 address, such as servers or network printers. This mode ensures that the device always uses the same IPv6 address, facilitating management and access.

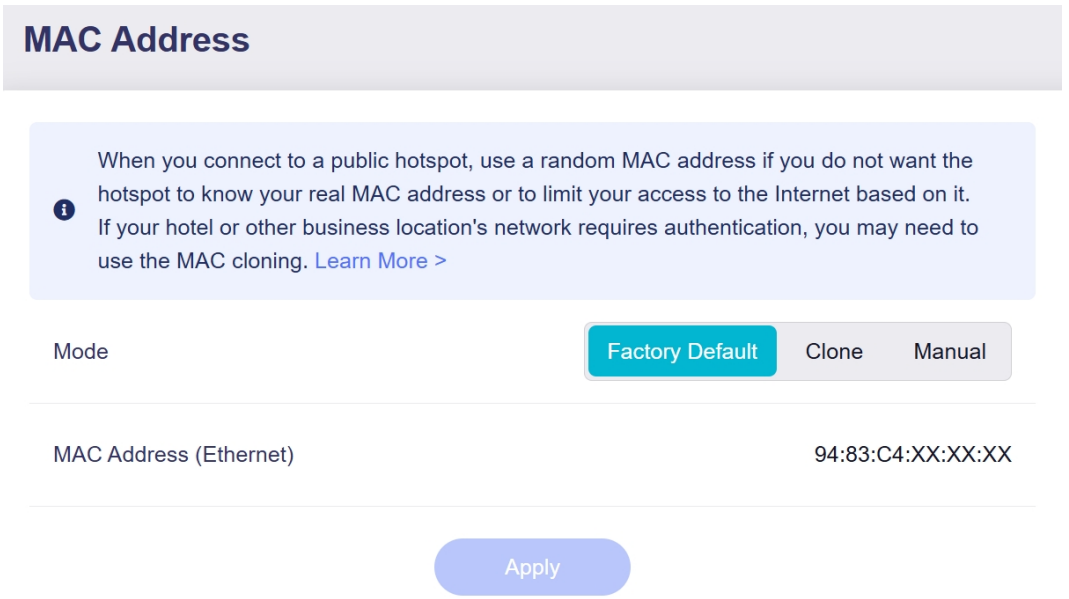
12.6.2 DNS Acquisition Method

It determines how the router obtains IPv6 DNS server addresses. There are two options: Automatic and Manual.

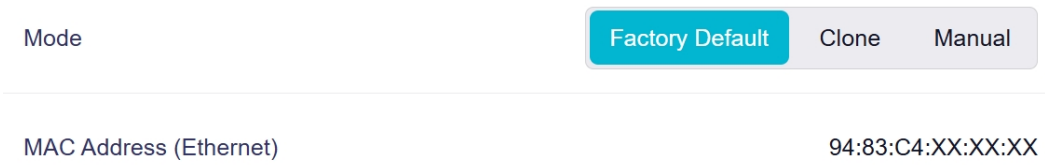
- **Automatic**: The router will obtain IPv6 DNS server addresses dynamically (e.g., via DHCPv6).
- **Manual**: Input custom IPv6 DNS server addresses. However, since DNS is used to resolve domain names to their corresponding IP addresses, manual DNS server configuration may result in DNS lookup failures. Please use it with caution.

12.7 MAC Address

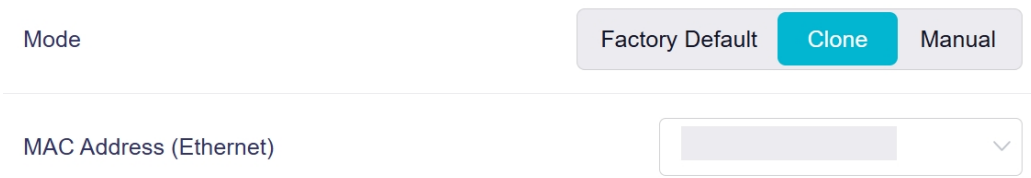
The MAC Address page displays the router's default MAC address, clone a client's MAC address, enter a MAC address manually, or generate a random MAC address. If the device supports setting multiple Ethernet ports to be used as WAN ports, you can set the MAC address for each port separately. Note that the MAC address setting is only valid when the Ethernet port is used as a WAN port.



- **The factory default MAC address.**

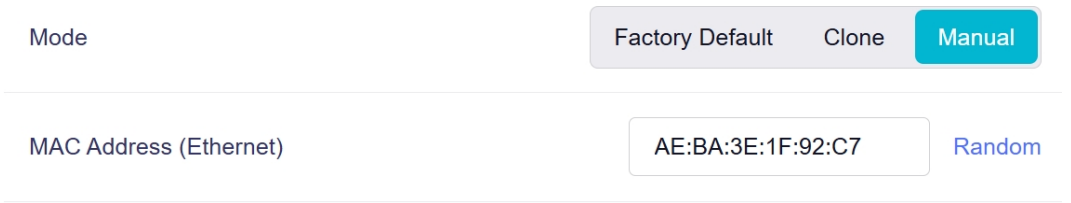


- **Clone a client's MAC address.**



Note: Many new devices now use a different random MAC address to connect to different Wi-Fi, so the MAC address shown here may not be the actual MAC address of the user's device. The randomized MAC may also be called a Private Wi-Fi Address or a random hardware address on different devices.

- **Manual input or generate a random MAC address.**

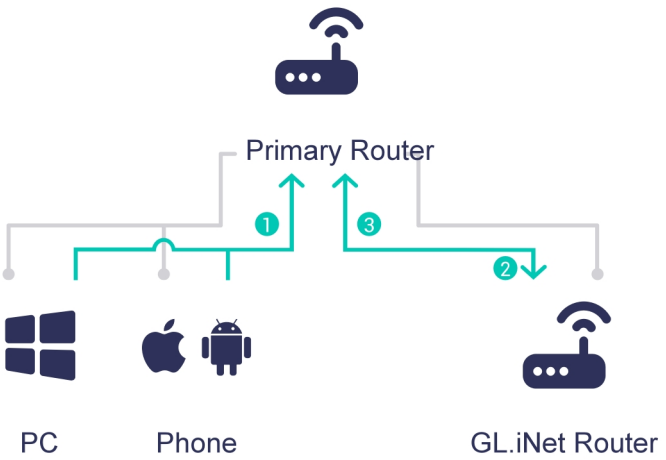


12.8 Drop-in Gateway

Drop-in Gateway is an extension function that enables capability expansion for an existing primary router without replacing or re-configuring it. By connecting the GL.iNet router to the primary router via an Ethernet cable, users can add advanced features onto the existing network infrastructure, for example:

- Enable VPN client
- Use encrypted DNS

Drop-in Gateway operates as an intermediate network system, routing data traffic from client devices through the GL.iNet router for processing before transmitting it via the primary router. During this process, it not only preserves existing network settings to ensure uninterrupted connectivity for all connected devices, but also allows you to manage network traffic for all or specific client devices if needed.



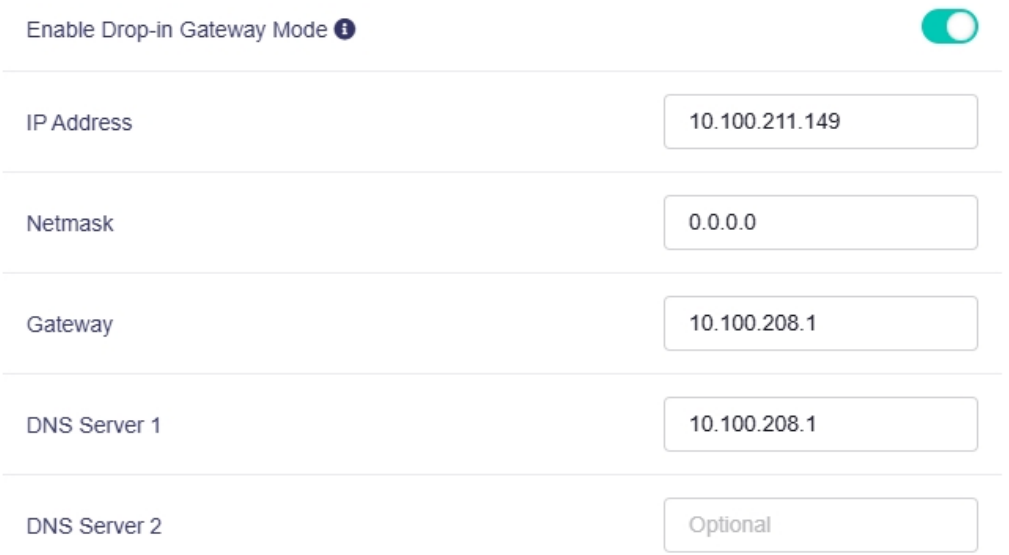
The diagram above consists of two types of lines: gray lines, and green lines marked with three arrows, each labeled with a corresponding number.

- **Gray lines** illustrate the physical connection topology: client devices (e.g., computer, laptop) connect to the primary router, and the primary router's LAN port links to the WAN port of the GL.iNet router (with Drop-in Gateway enabled) via an Ethernet cable.
- **Green lines** depict the sequential data transmission path when Drop-in Gateway is active, with the numbered arrows indicating the traffic flow order:

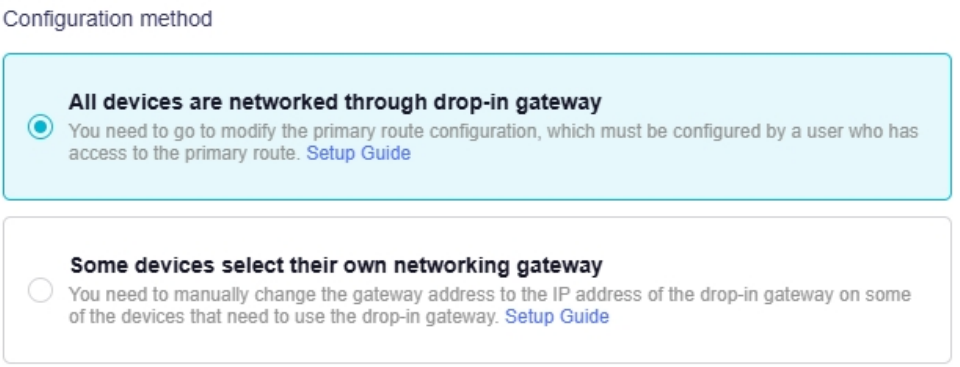
1. Traffic from client devices is first routed to the primary router;
2. The primary router forwards the traffic to the GL.iNet router for processing (e.g., ad filtering, VPN encryption);
3. After processing, the traffic is sent back to the primary router, which then either delivers the final data to the original client devices or routes it out to the Internet.

Follow the steps below to enable Drop-in Gateway if needed.

1. Log in to your router's web admin panel and navigate to **NETWORK** > **Drop-in Gateway**. Toggle on **Enable Drop-in Gateway Mode**, and confirm the network parameters.



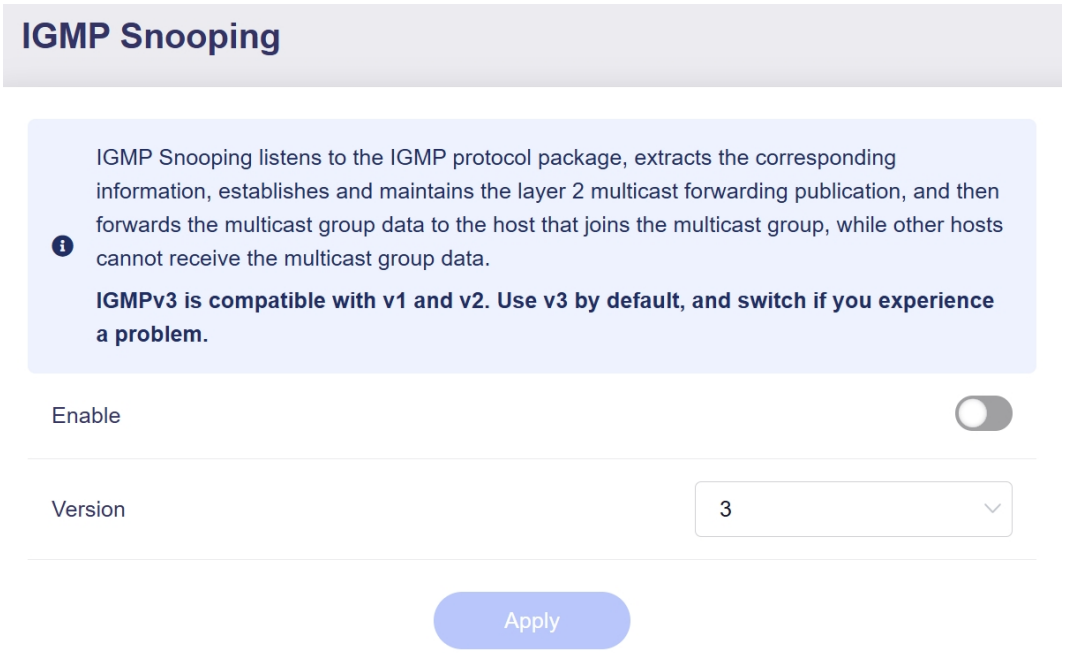
2. Select the configuration method, then click **Apply**. Please refer to this tutorial for details.



12.9 IGMP Snooping

IGMP Snooping listens to the IGMP protocol package, extracts the corresponding information, establishes and maintains the layer 2 multicast forwarding table, and then forwards the multicast group data to the host that joins the multicast group, while other hosts cannot receive the multicast group data.

Log in to your router's web admin panel and navigate to **NETWORK** > **IGMP Snooping**. You can enable it to use the multicast function on your router if needed.



Chapter 13

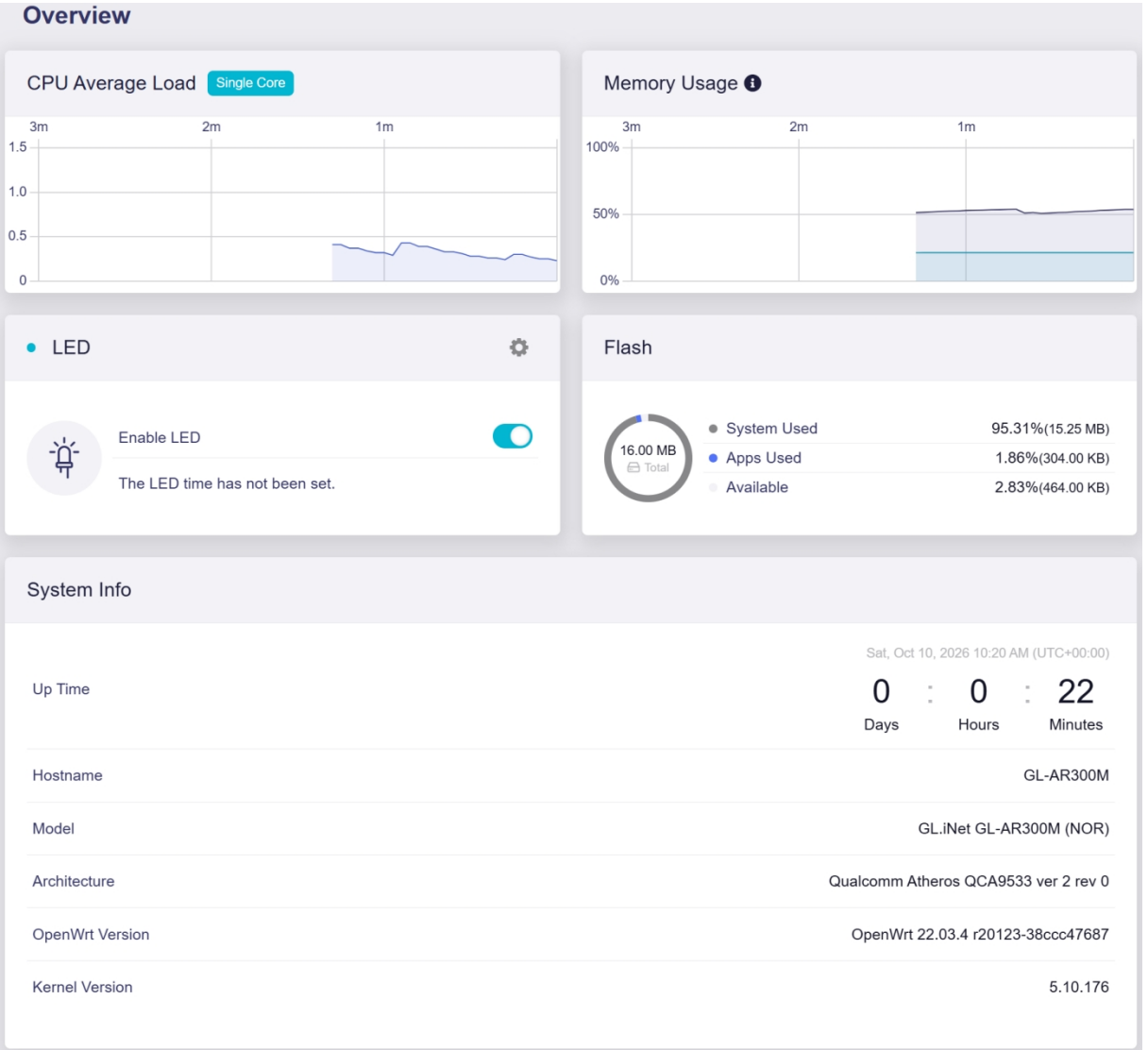
System

This chapter covers system management tools for the device, such as system overview, upgrade, scheduled tasks, time zone, log, firmware reset, and advanced settings.

13.1 Overview

Log in to your router's web admin panel and navigate to **SYSTEM** > **Overview**. This page displays hardware status and supports some simple controls, including:

- CPU, Memory, and Flash Status
- LED Control
- Device Information

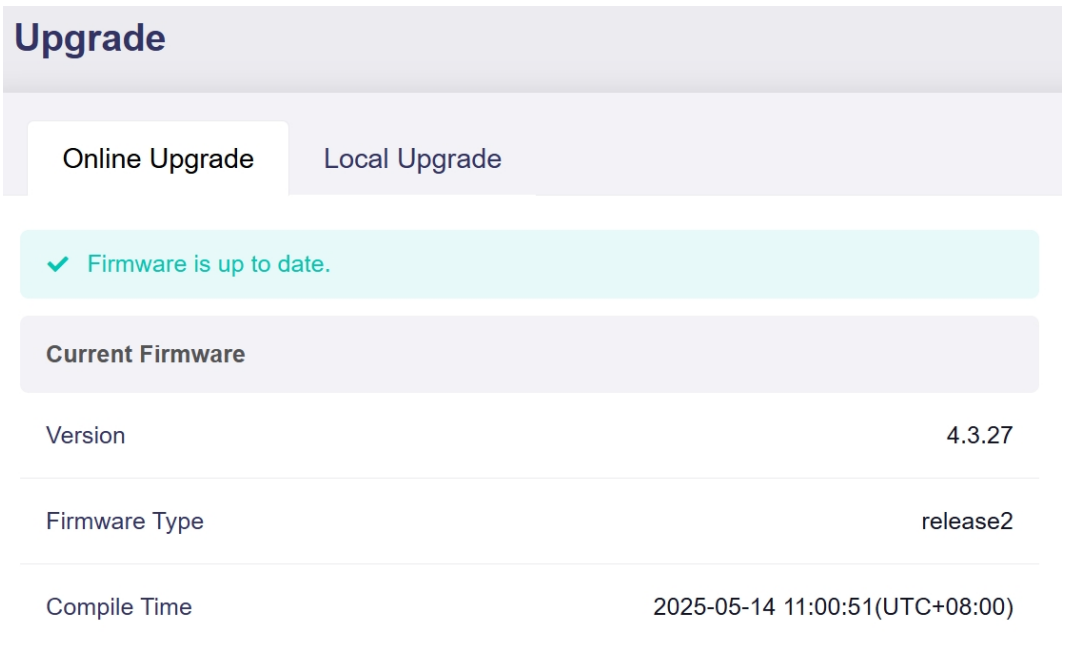


13.2 Upgrade

Log in to your router's web admin panel and navigate to **SYSTEM** > **Upgrade**. You can upgrade the router's firmware version by online upgrade or local upgrade.

13.2.1 Online Upgrade

You can find the current firmware details here, including firmware version, firmware type (e.g., release, beta), and update time. If your router is connected to the Internet, it will check for the newer firmware version available for download.

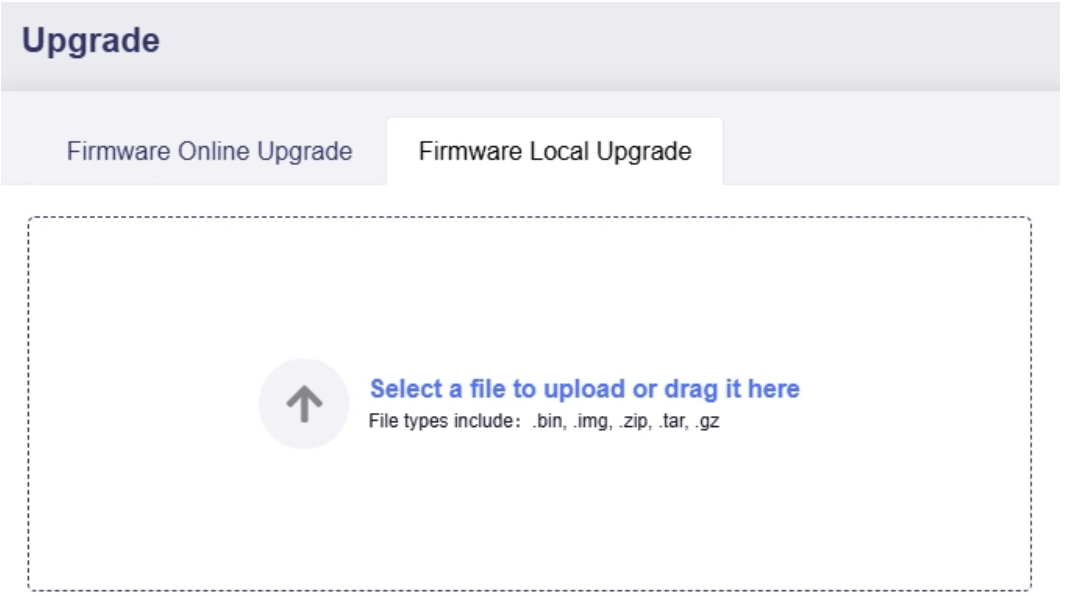


Tip: When trying to perform an online upgrade, if it displays **Download Failed**, please navigate to **SYSTEM** > **Time Zone**, and fix the time zone error (sync to browser).

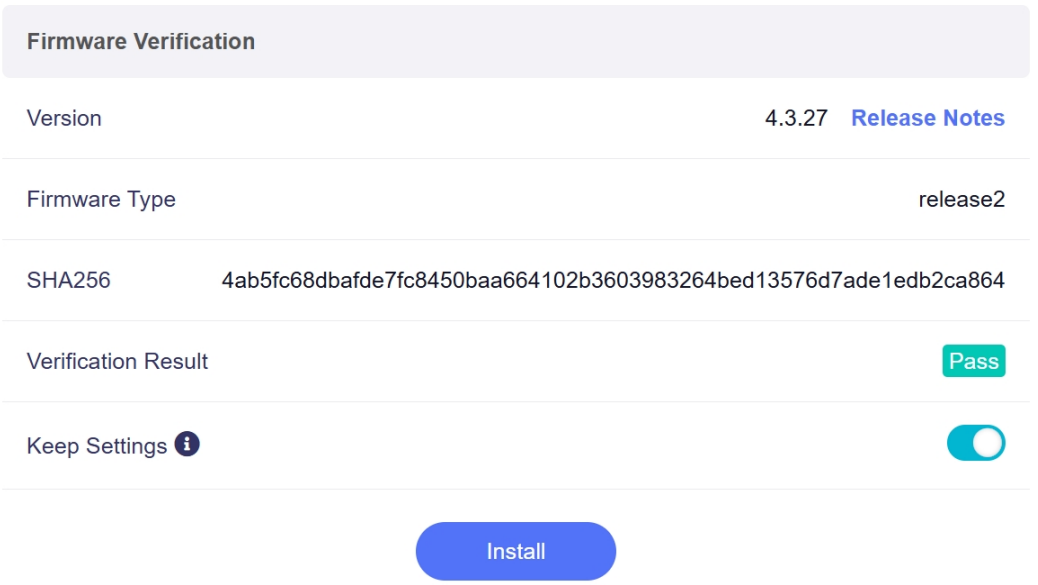
13.2.2 Local Upgrade

Local upgrade does not rely on an Internet connection for the router.

Download the correct firmware package (matching your router model) from the official Download Center to your local device. Then log in to the router's web admin panel, navigate to **SYSTEM** > **Upgrade** > **Local Upgrade** section, and upload the firmware package.



The page will display the firmware details. Verify these details before clicking **Install**.



If **Keep Settings** is enabled, current settings are retained. However, any manually installed packages must be reinstalled after the upgrade completes. Do not enable this option when downgrading the firmware.

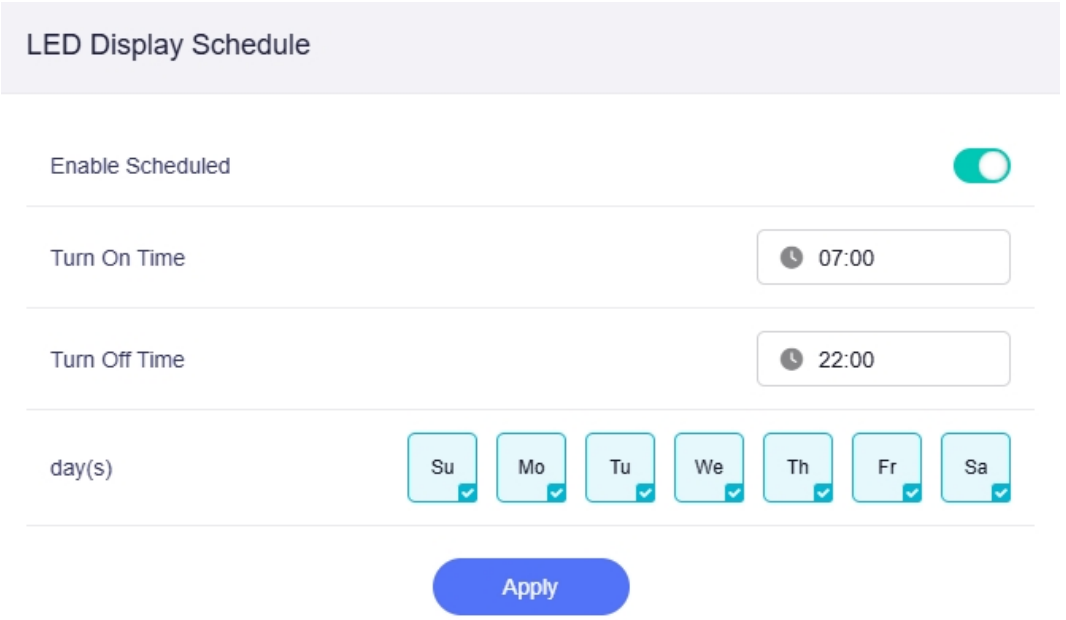
13.3 Scheduled Tasks

Log in to your router's web admin panel and navigate to **SYSTEM** > **Scheduled Tasks**. This page allows you to set up a daily schedule for some basic actions, including switching LED light on and off, and restarting the router.

Note: Please synchronize the time in the Time Zone before using this function. If the device is shut down at the scheduled time, the task will not be executed.

13.3.1 LED Display Schedule

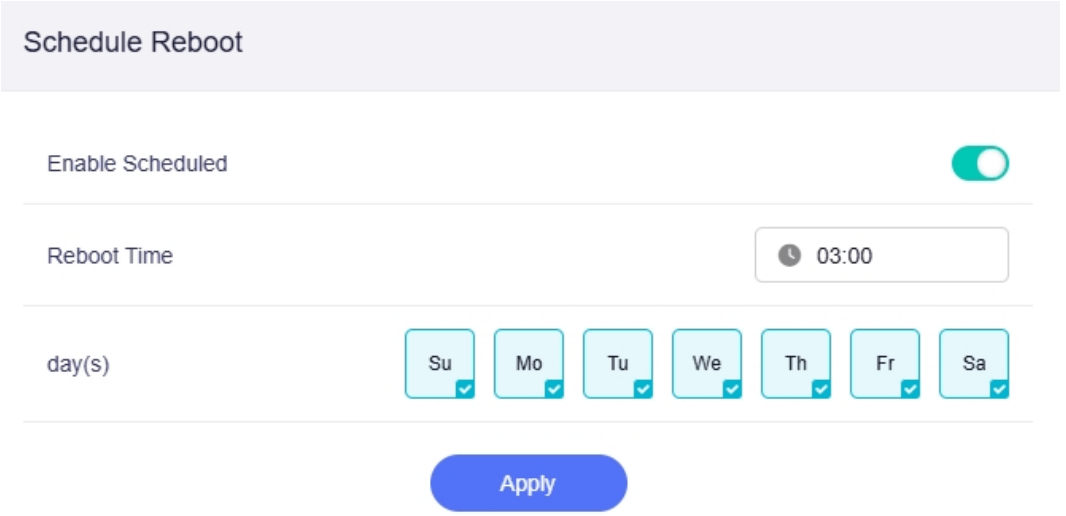
Set a schedule for your router's LED light if needed, then click **Apply**.



- **Enable Scheduled**: Toggle this switch to enable the LED display schedule.
- **Turn On Time**: Set the time (e.g., 07:00) when the LED light will turn on.
- **Turn Off Time**: Set the time (e.g., 22:00) when the LED light will turn off.
- **day(s)**: Select the effective days of the week for these settings.

13.3.2 Schedule Reboot

Set a schedule for automatically restarting your router if needed, then click **Apply**.



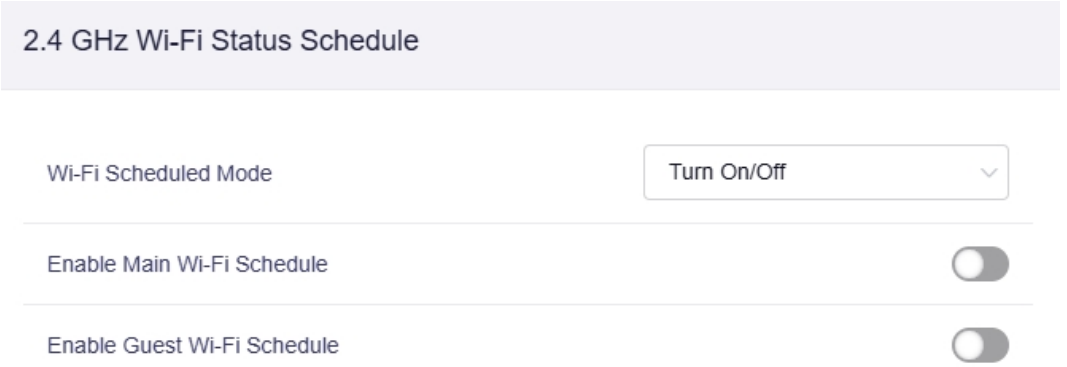
- **Enable Scheduled**: Toggle this switch to enable the scheduled reboot.
- **Reboot Time**: Set the specific time (e.g., 03:00) when the router will restart.
- **day(s)**: Select the effective days of the week for these settings.

13.3.3 2.4GHz Wi-Fi Schedule

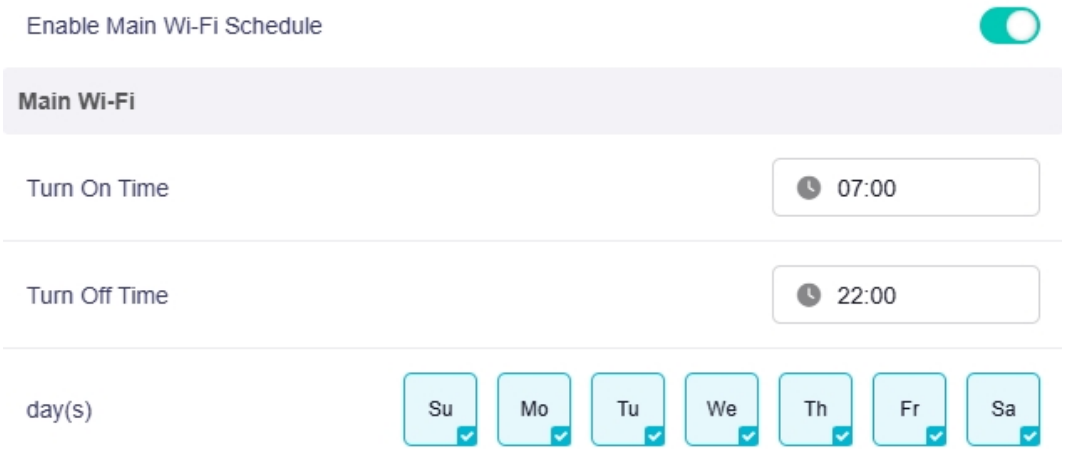
This function allows you to set a schedule for your 2.4GHz Wi-Fi. There are two modes: Turn On/Off, and Switch TX Power.

Mode 1: Turn On/Off

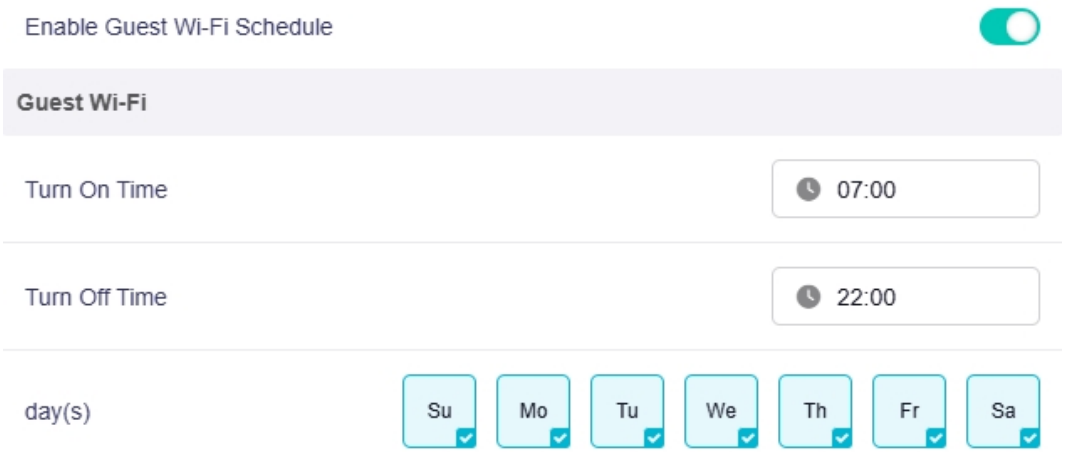
You can enable the on/off schedule for both the 2.4GHz Main Wi-Fi and Guest Wi-Fi.



- **Main Wi-Fi Schedule**: When enabled, set the on and off times for your 2.4GHz Main Wi-Fi, and select an effective date for the week.

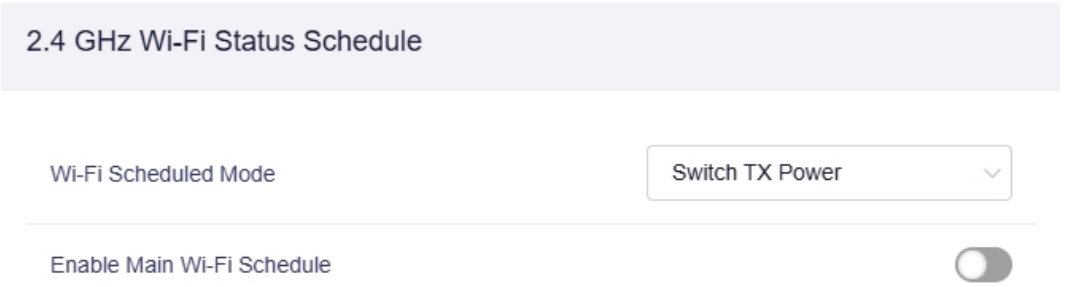


- **Guest Wi-Fi Schedule**: When enabled, set the on and off times for your 2.4GHz Guest Wi-Fi, and select an effective date for the week.

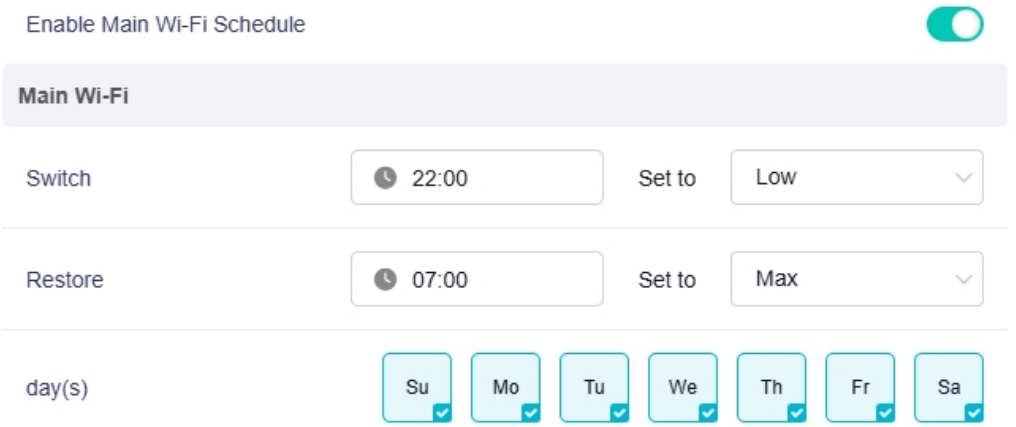


Mode 2: Switch TX Power

You can enable the TX power switching schedule for the 2.4GHz Main Wi-Fi.



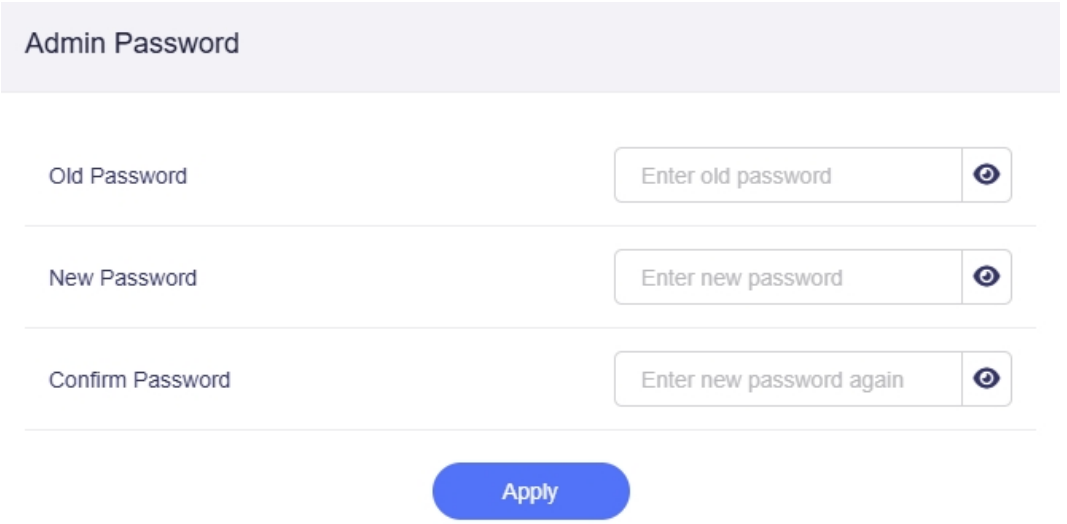
When enabled, set two timed actions for your 2.4GHz Main Wi-Fi to switch TX power, and select an effective date for the week.



- **Switch**: Set TX Power to a certain level (e.g., Low) at a specific time (e.g., 22:00).
- **Restore**: Restore TX Power to another level (e.g., Max) at another time (e.g., 07:00).
- **days**: Select the effective days of the week for these settings.

13.4 Admin Password

Log in to your router's web admin panel and navigate to **SYSTEM** > **Admin Password**. On this page, you can change the login password of the web admin panel.

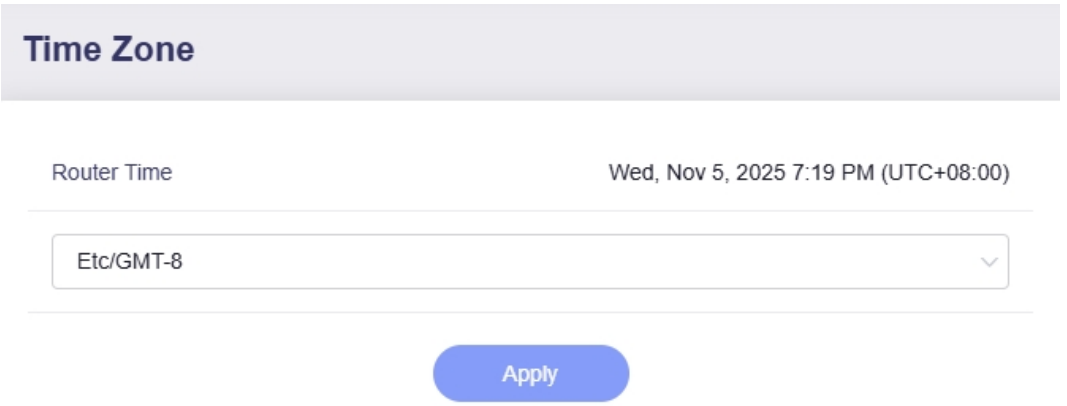


The requirements for the admin password are as follows:

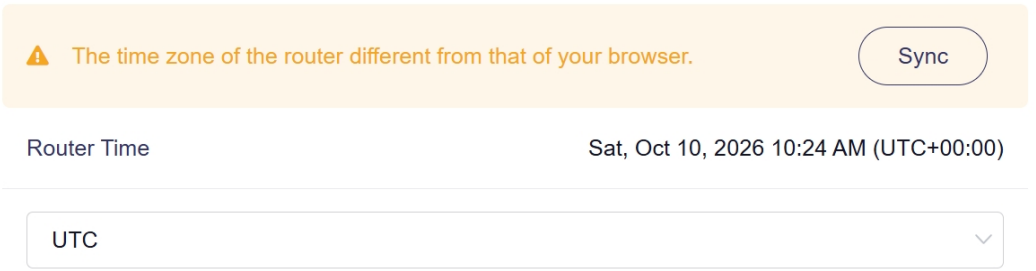
1. Minimum 10 characters and maximum 63 characters in length.
2. Letters (case sensitive), numbers and symbols (e.g., ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) are allowed.
3. At least two types (uppercase letters, lowercase letters, numbers, and symbols) are required.

13.5 Time Zone

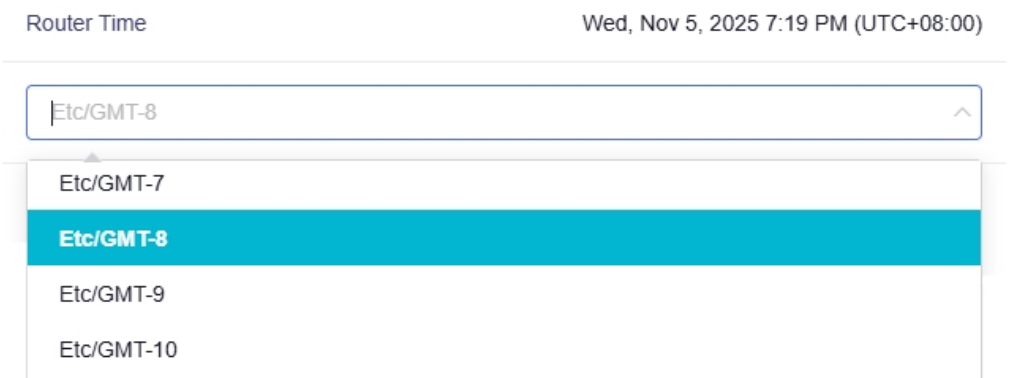
Log in to your router's web admin panel and navigate to **SYSTEM** > **Time Zone**. This page displays your router's system time, indicating the date, time, and corresponding time zone offset.



Some functions rely on the router's system time to take effect. Please ensure the correct time zone is properly synchronized. If the router's time zone is different from that of your browser, a prompt will be displayed as follows. Click the **Sync** button to synchronize the time zone.

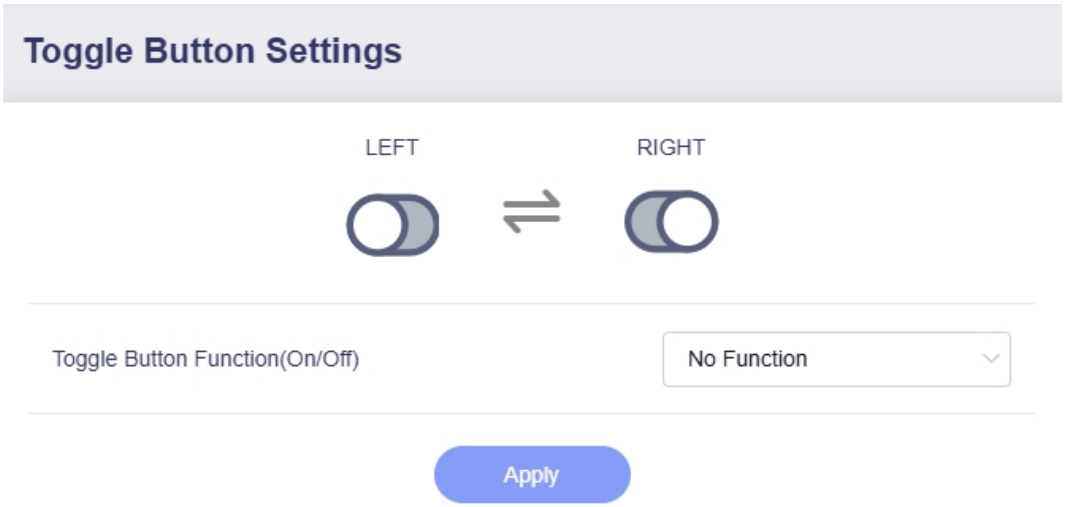


To switch time zone, select the appropriate time zone from the list to ensure the router's system time matches your local time.

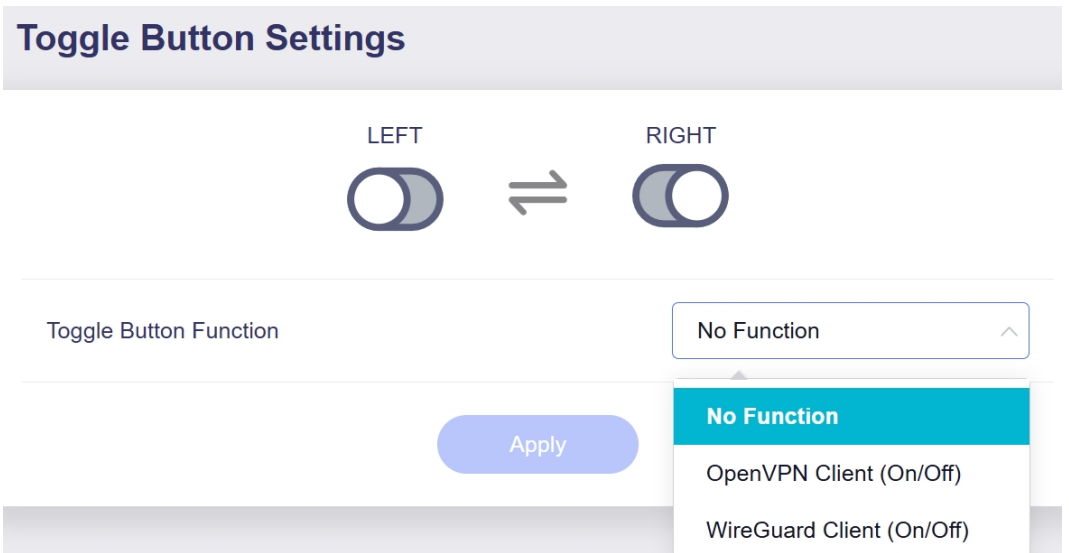


13.6 Toggle Button Settings

Log in to your router's web admin panel and navigate to **SYSTEM** > **Toggle Button Settings**. This page allows you to customize the function of the router's physical toggle switch (located on the side) for easier use.

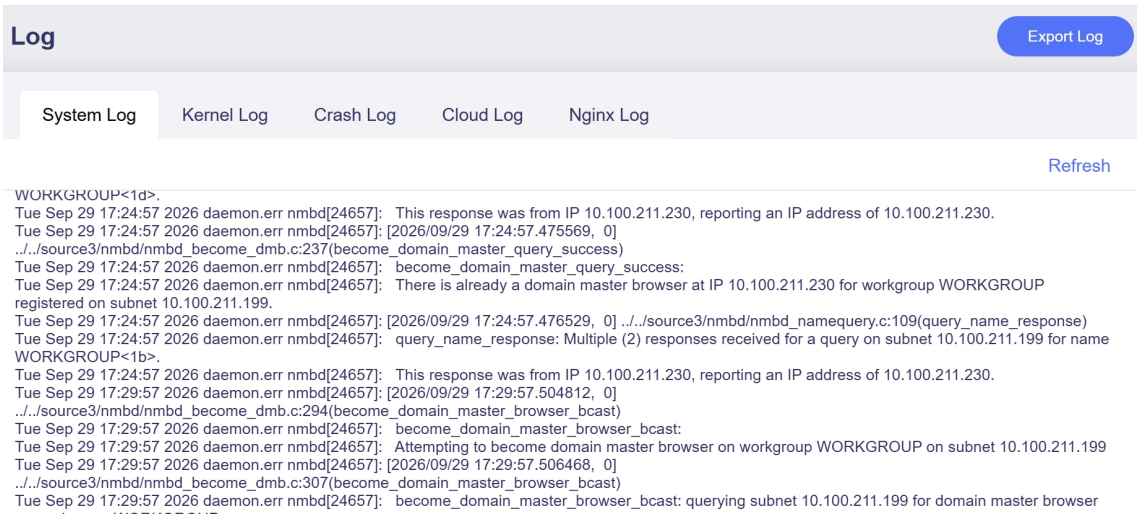


By default, the toggle switch is not assigned any functions. You can customize it if needed to turn specific functions on or off with a single flip.



13.7 Log

Log in to your router's web admin panel and navigate to **SYSTEM** > **Log**. This page allows you to view logs of System, Kernel, Crash, Cloud and Nginx for analysis and troubleshooting.

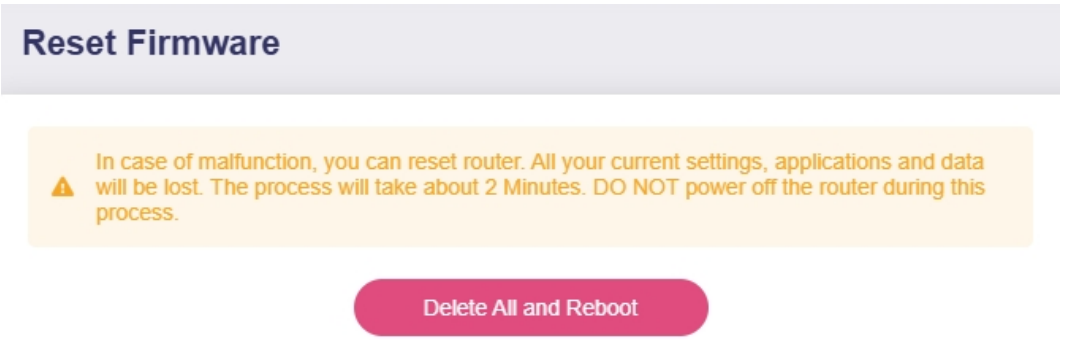


- **Refresh**: Click this button to refresh logs.
- **Export Log**: Click this button to export debug info along with the logs.

13.8 Reset Firmware

If the router malfunctions, you can try resolving the issue by resetting the firmware.

Log in to your router's web admin panel and navigate to **SYSTEM** > **Reset Firmware**. Click **Delete All and Reboot** to reset the firmware if needed.



Note: All your current settings, applications and data will be cleared. The process will take about 2 minutes. Do not power off the router during this process.

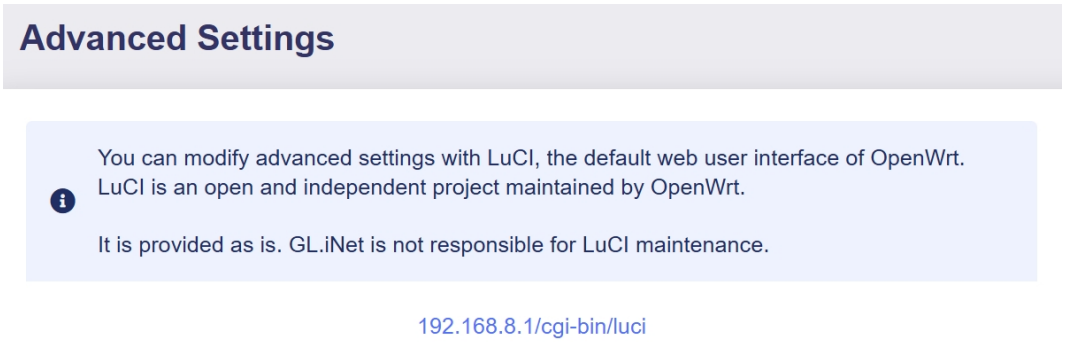
If you fail to access the router's web admin panel, try resetting your router using the physical reset button on the side.

13.9 Advanced Settings

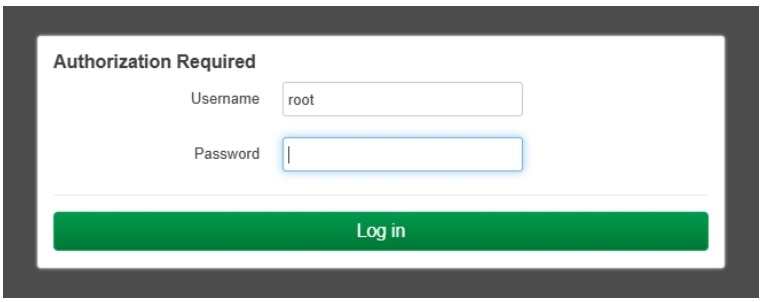
Log in to your router's web admin panel and navigate to **SYSTEM** > **Advanced Settings**. This page allows you to modify advanced settings in LuCI, which is the default web user interface of OpenWrt. As an open and independent project maintained by OpenWrt, LuCI is provided as-is. GL.iNet is not responsible for LuCI maintenance.

Follow the steps below to log in to the LuCI interface.

1. Click the access link, and you will be re-directed to the LuCI login page.



2. Enter the login password, which is the same as the password of the web admin panel.



You will then log in to the LuCI interface.

