GL·iNet

User Manual

GL-MT2500 / Brume 2

Security Gateway

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

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

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

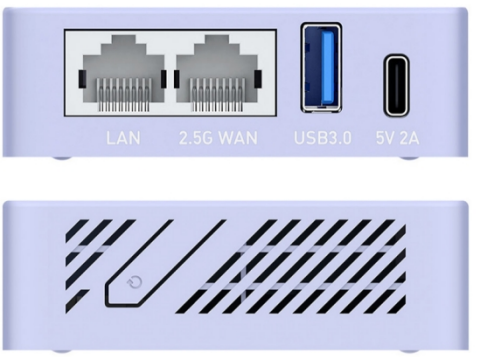
1.1 Product Overview

Brume 2 (GL-MT2500/GL-MT2500A) is a lightweight and powerful VPN gateway that runs on OpenWrt v21.02 operating system. It is compactly designed to host a VPN server at home, or run SD-WAN (Site-to-Site) for small and medium-sized enterprises. It comes in two variants: GL-MT2500 with a plastic casing and GL-MT2500A with an aluminum casing.

1.1.1 Appearance

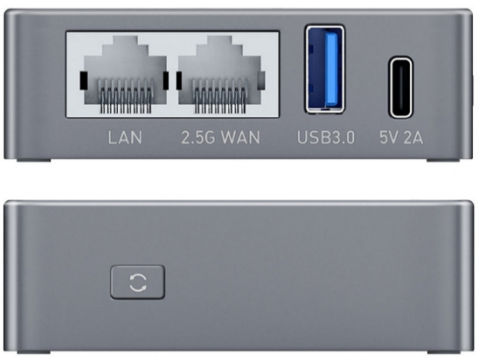
GL-MT2500

GL-MT2500

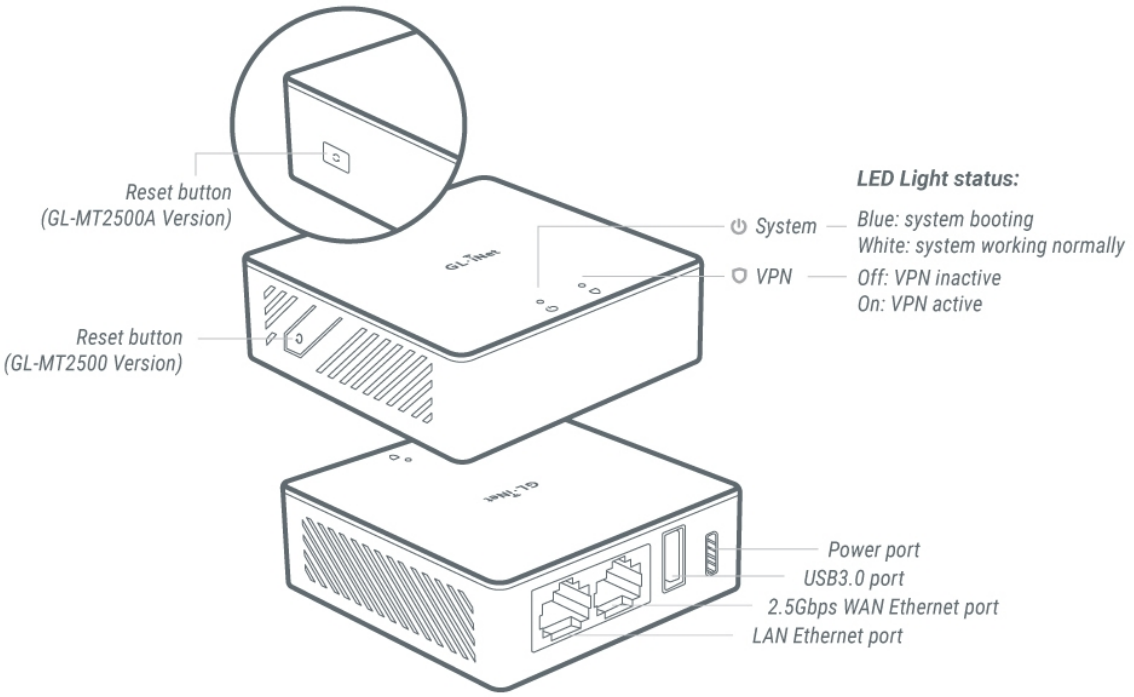


GL-MT2500A

GL-MT2500A



1.1.2 Interface and Button



Item	Description
Power Port	For connecting the power adapter.
2.5G WAN Port	For connecting to a modem or an Ethernet outlet.
LAN Port	For connecting wired devices to the router.
USB 3.0 Port	For connecting a USB storage device to the router.
Reset Button	Press and hold for **4 seconds** and then release to repair your network. The system LED will turn blue and flash slowly until your network is restored.
	Press and hold for **10 seconds** and then release to reset the router to factory defaults. The system LED will turn blue and flash rapidly. All data will be cleared when the LED becomes solid blue.

1.1.3 LED

LED	Status
System	Blue: System booting
	White: Connected to Internet
VPN	Off: VPN inactive
	On: VPN active

1.2 Specifications

Interface	1 x 2.5G WAN Ethernet port 2 x 2.5G LAN Ethernet ports 1 x USB 3.0 Type-C port 1 x Type-C power port 1 x Reset button
CPU	MediaTek MT7981B Dual-core, @1.3GHz
Memory / Storage	DDR4 1GB / eMMC 8GB
Ethernet Speed	WAN Port: 10/100/1000/2500Mbps LAN Port: 10/100/1000 Mbps
Power Input	Type-C, 5V/2A
Power Consumption	< 2.6W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	GL-MT2500: 70 x 70 x 22 mm / 60g GL-MT2500A: 70 x 70 x 22 mm / 157g
Other Tools	Datesheet / Firmware / App / Unboxing / Tutorials

1.3 Package Contents

The package includes:

- 1 x Brume 2 (GL-MT2500/GL-MT2500A)
- 1 x Quick Start Guide
- 1 x Ethernet Cable
- 1 x Thank You Card
- 1 x Power Adapter
- 1 x Converter (Depending on your shipping country)

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.

2.2 Connecting the Router

1. **Power on**

   Put the two-piece power adapter together. Connect it to your Brume 2 and plug it into an outlet. It will start up automatically.
2. **Connect a device to the router**

   Connect a wired device (e.g., a computer or laptop) to the Brume 2’s LAN port with an Ethernet cable.
3. **Log in to the router**

   The Internet will be 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

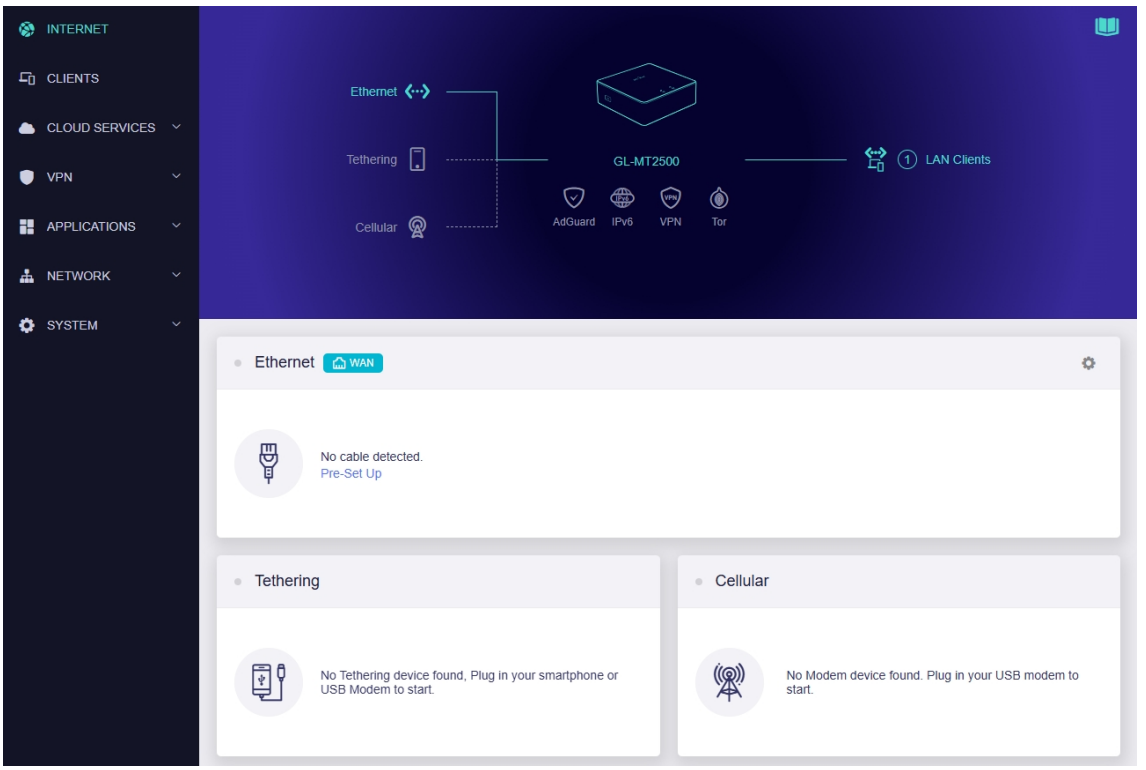
Log In To Your Router

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.

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 Brume 2's LAN port with 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 Brume 2's web admin panel.



Chapter 4

Set Up Internet Connection

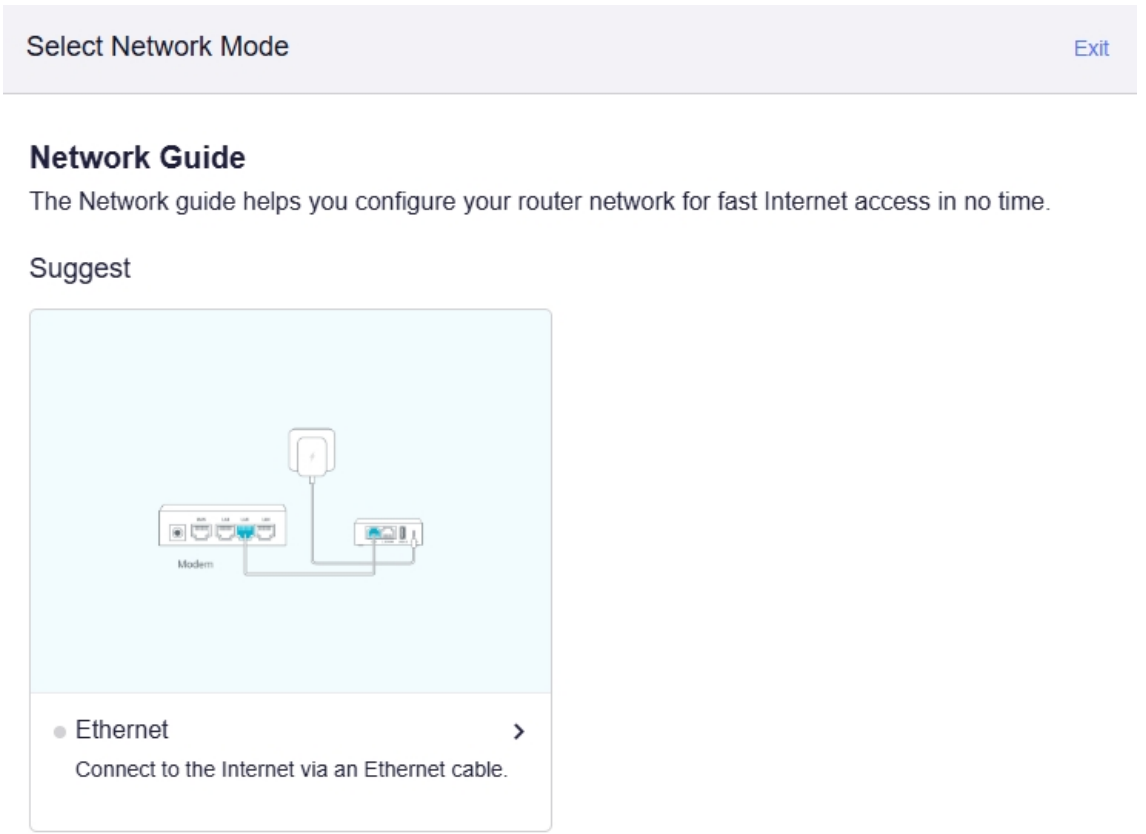
This chapter introduces multiple Internet connection methods for the router to adapt to diverse network environments.

4.1 Use Quick Setup Wizard

The Web-based Setup Wizard will guide you through the router network configuration. Follow the steps below to start the wizard.

1. Log in to the router's web admin panel as instructed in Chapter 3.
2. On the homepage, click the book icon in the top right corner.

3. Follow the Setup Wizard to configure your router and establish an internet connection.



4.2 Manually Set Up Internet Connection

While the Setup Wizard is convenient for quick network setup, manual setup allows you to adjust advanced network settings for specific requirements, and check or modify existing connections as needed.

Brume 2 supports three internet connection methods: Ethernet, USB Tethering, and USB Modem/Cellular. 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. **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.

3. **USB Modem/Cellular**: 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.

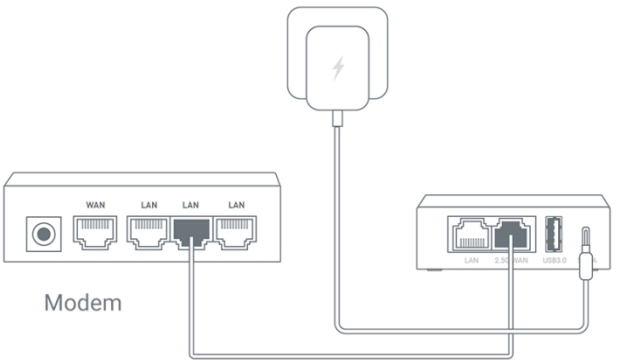
4.2.1 Connect to the Internet via Ethernet Cable

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.

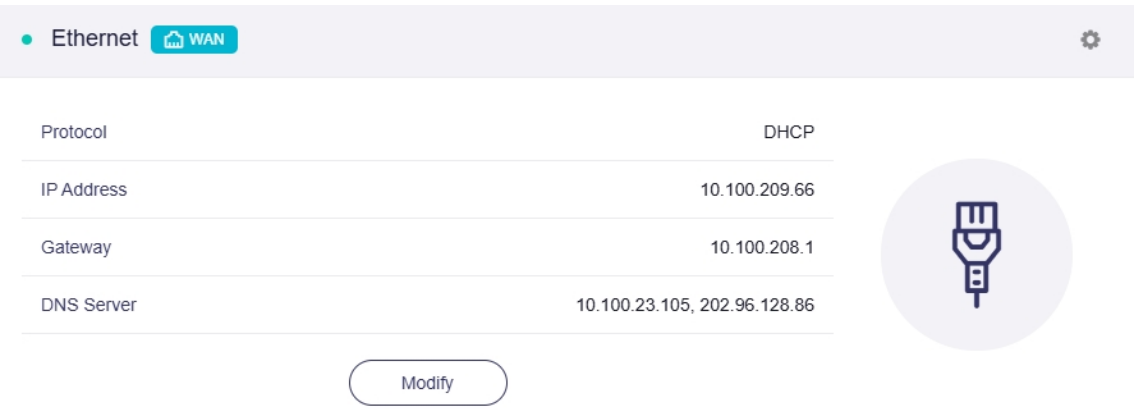
Basic Setup

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.

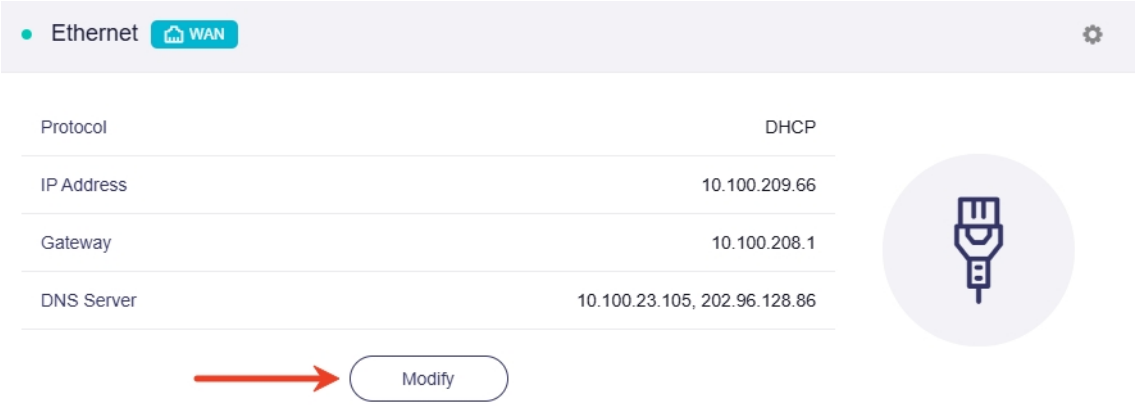


2. Log in to the router's web admin panel and navigate to **INTERNET** > **Ethernet**. If the connection is successful, the Ethernet section will display network details, including Protocol, IP Address, Gateway, and DNS Server.



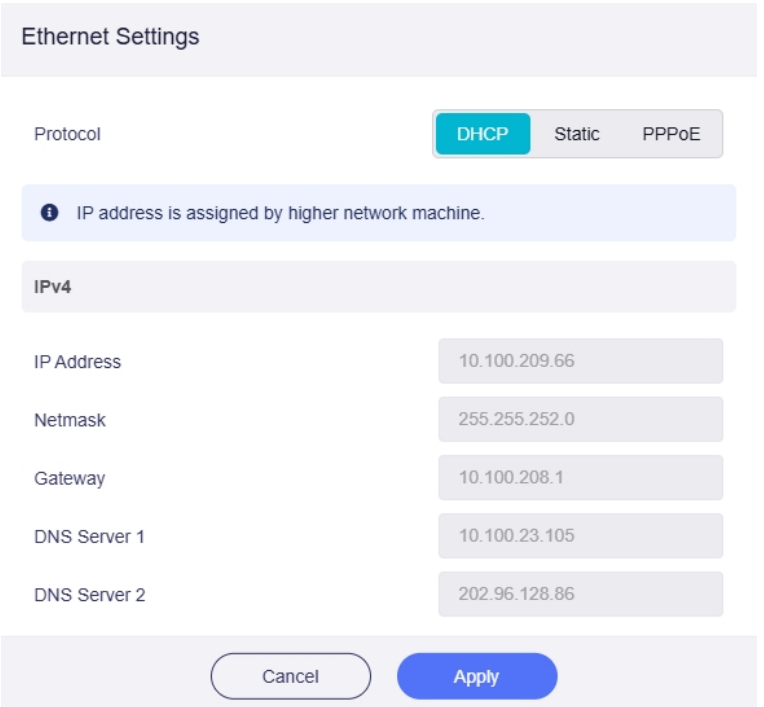
Protocol

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



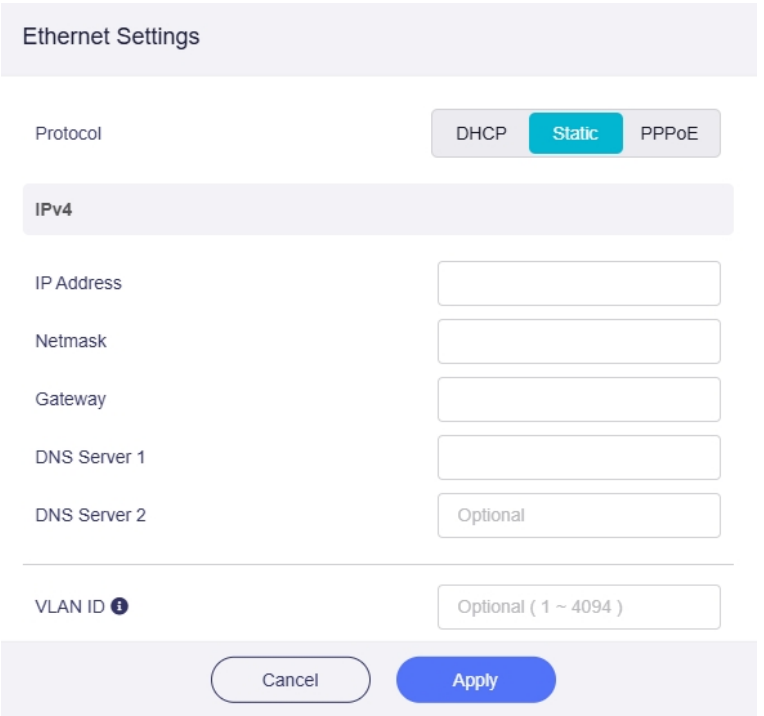
- **DHCP**

  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.



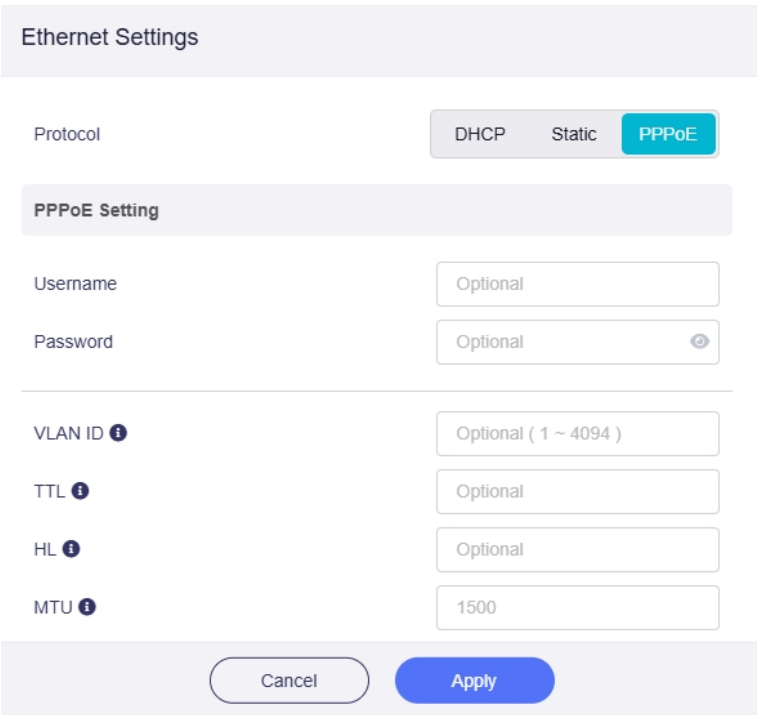
- **Static**

  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).



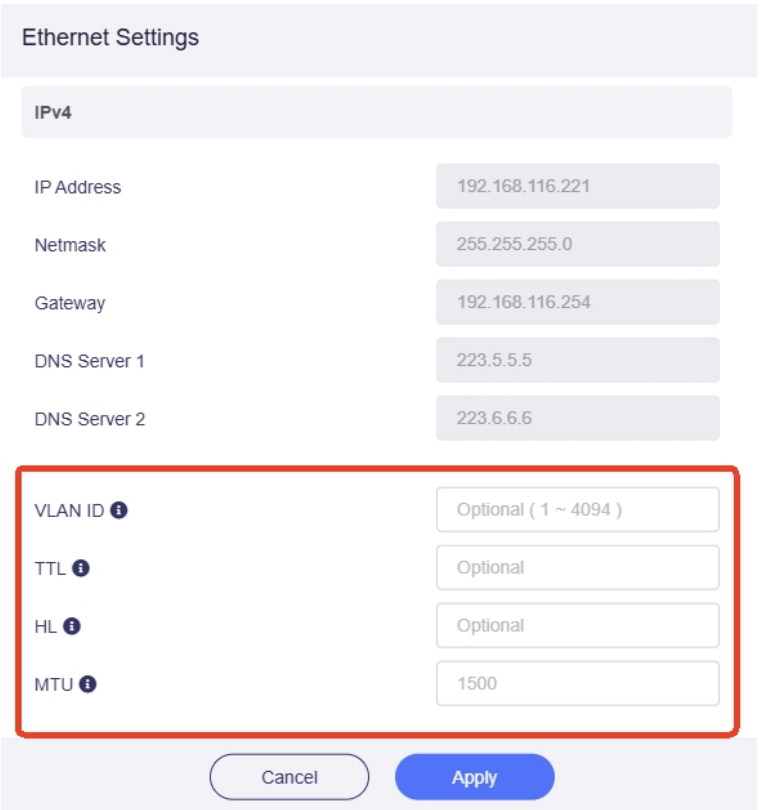
- **PPPoE**

  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.



Advanced Settings

In addition to the essential settings, there are also some optional advanced settings for the above three protocols.



- **VLAN ID**

  This setting is needed only if the provider's server requires the interface to use a specific tagged VLAN ID.

- **TTL**

  TTL (Time To Live) defines the maximum time packets can survive in the network. By default, the router decrements the TTL of incoming packets from client devices by 1 before forwarding them. If you need to override it, you can set a fixed value here. The TTL setting is valid only for IPv4.

- **HL**

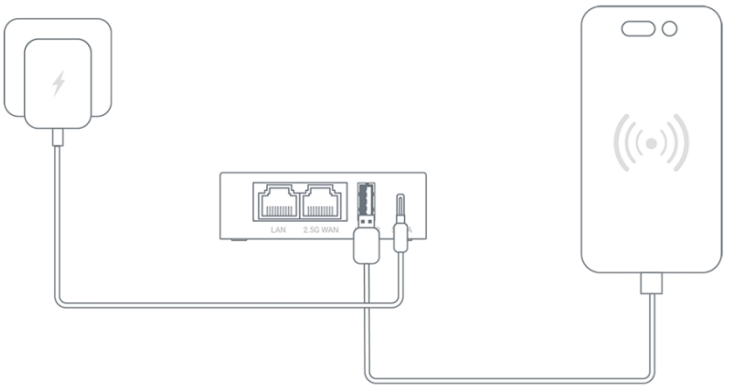
  In IPv6, the HL (Hop Limit) field limits the number of transmission hops for data packets in the network, serving as the equivalent of TTL in IPv4.

- **MTU**

  The default MTU value is 1500 bytes.

4.2.2 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.

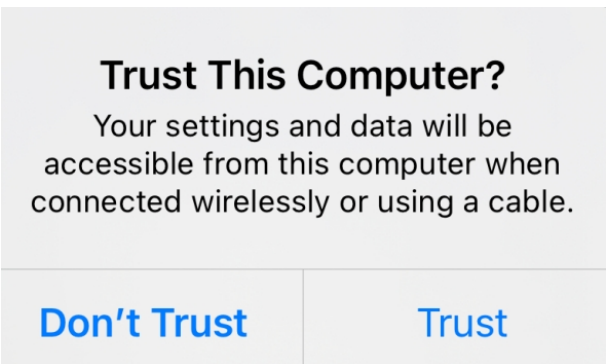


Host-less modem works in Tethering as well during the setup of the modem.

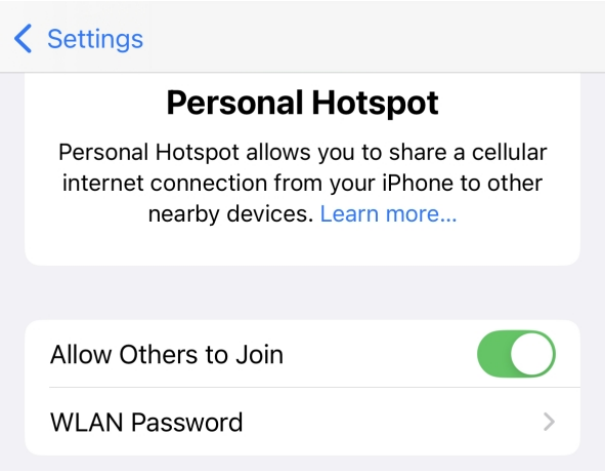
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

iPhone Tethering

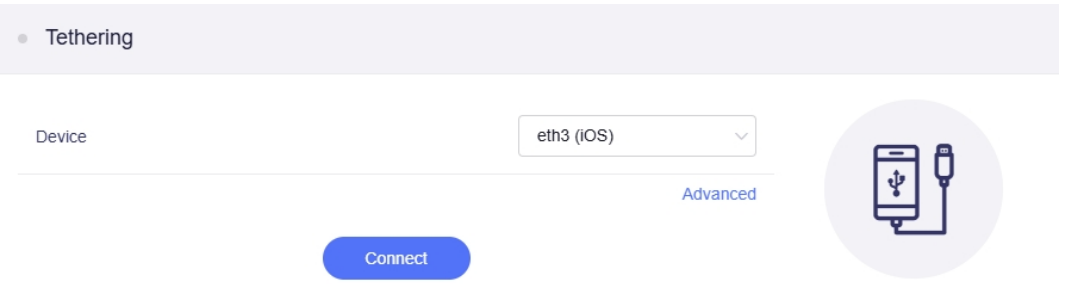
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



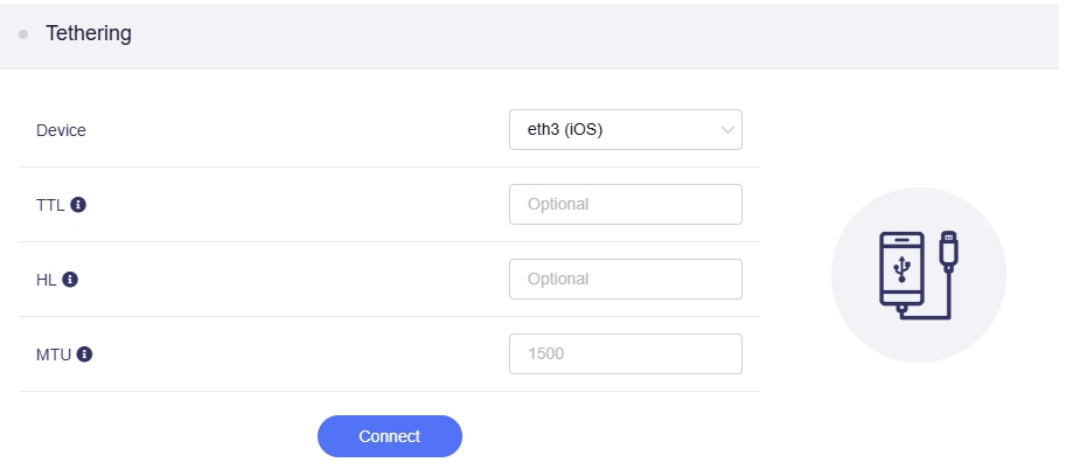
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



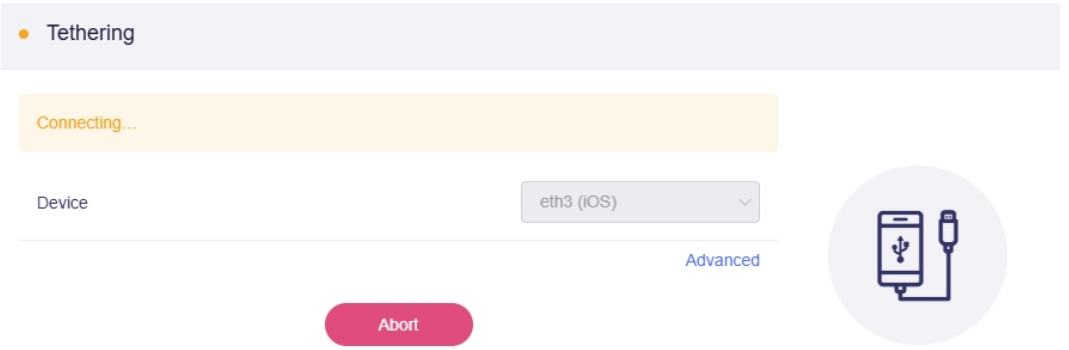
3. Connect a computer or another phone to the router. Log in to the router's web admin panel and navigate to **INTERNET** > **Tethering**, then click **Connect**.



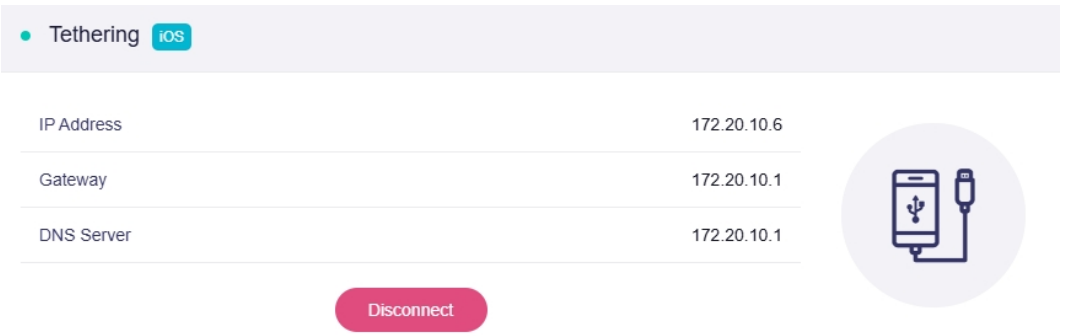
If you need to set advanced settings, such as TTL, HL, and MTU, click **Advanced** to customize these settings before clicking **Connect**.



4. It will start connecting.

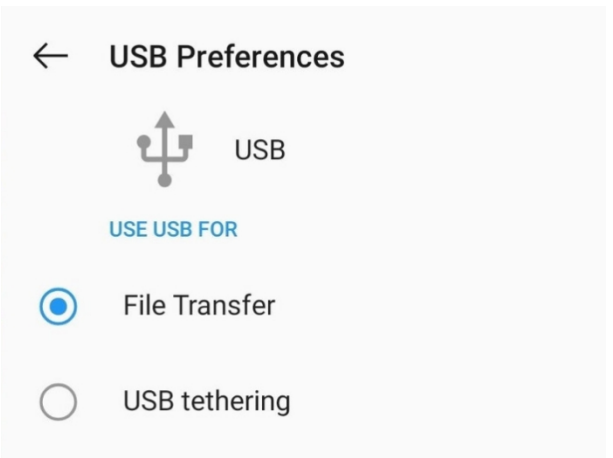


Once connected, this page will display the Tethering connection details.

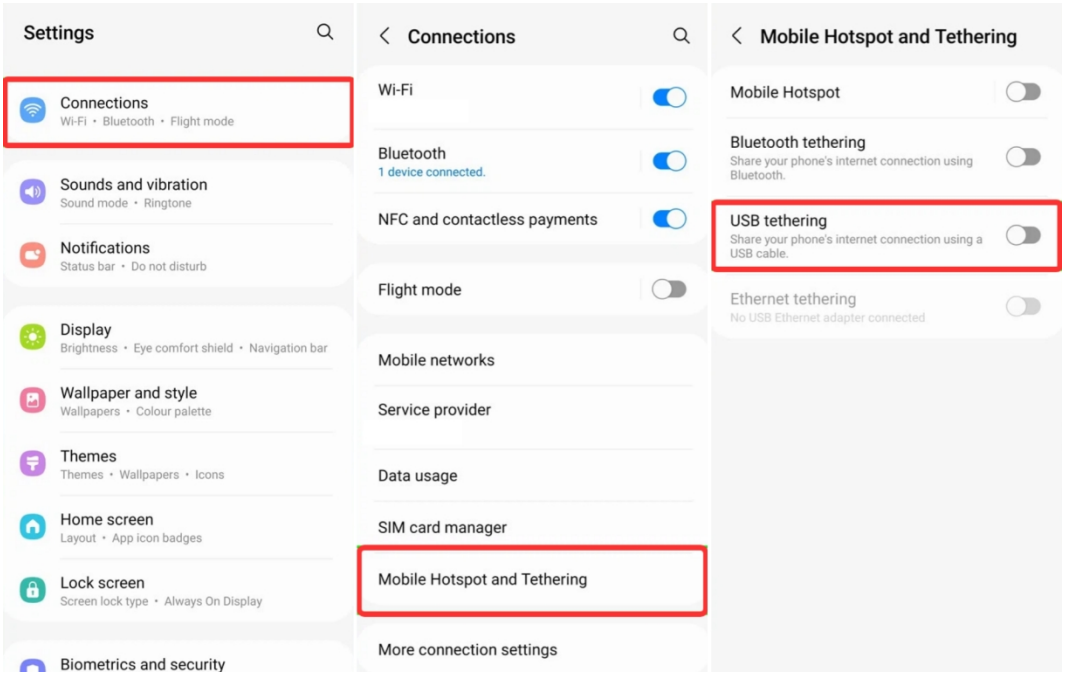


Android Tethering

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.

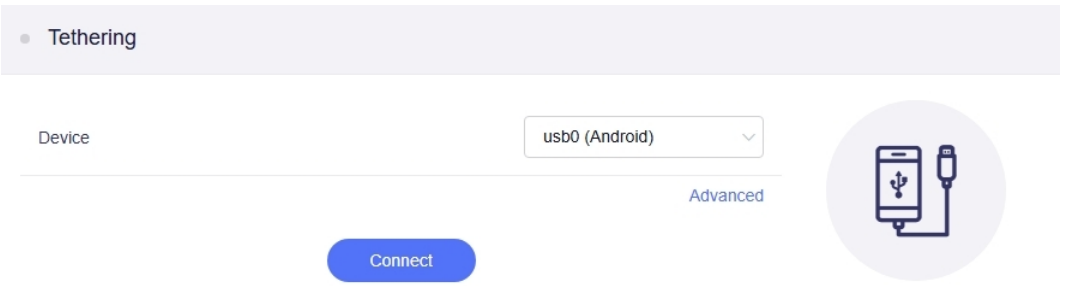


2. Go to your phone's **Settings** > **Network & Internet** > **Personal Hotspot**. Enable **Personal Hotspot** or **USB Tethering**.

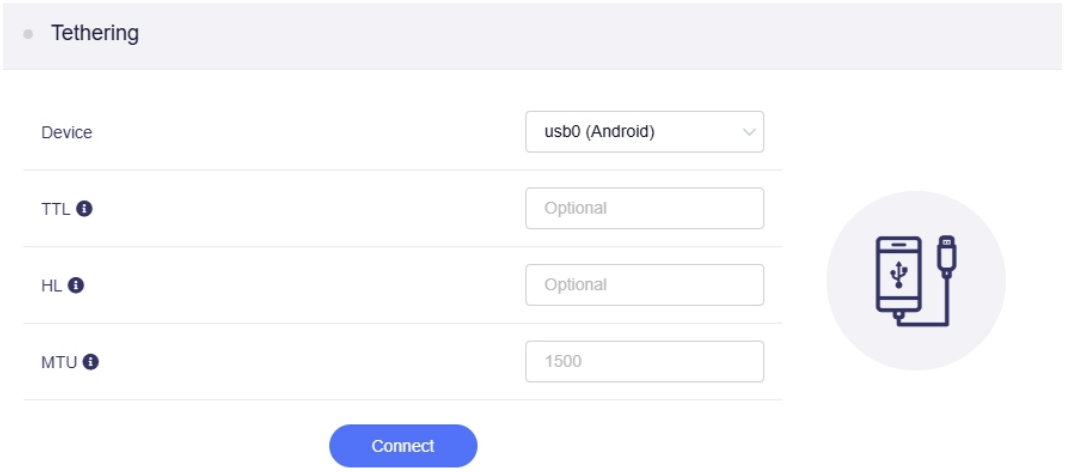


(The steps to enable USB Tethering vary by brand. Check your device's settings for the exact location, and contact your manufacturer's support if necessary.)

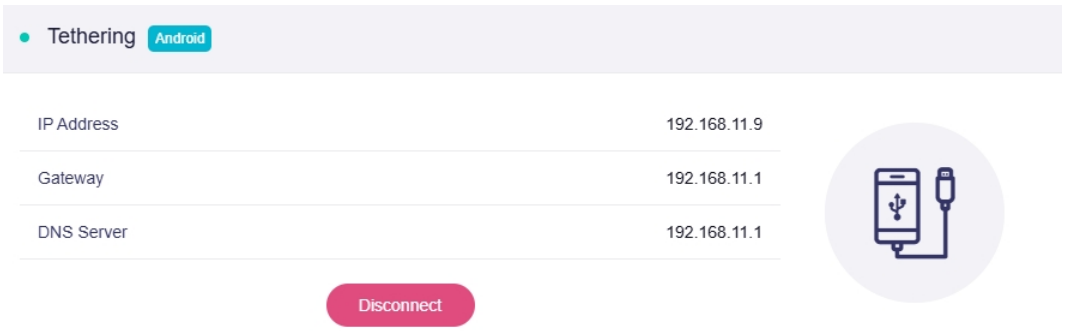
3. Connect a computer or another phone to the router, then log in to the router's web admin panel, navigate to **INTERNET** > **Tethering**. Click **Connect**.



If you need to set advanced settings such as TTL, HL, and MTU, click **Advanced** to customize these settings before clicking **Connect**.



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



Troubleshooting

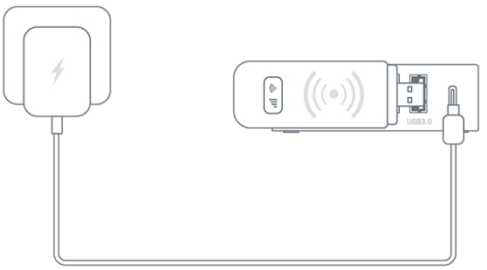
If the Tethering connection fails, try these troubleshooting steps:

- 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.

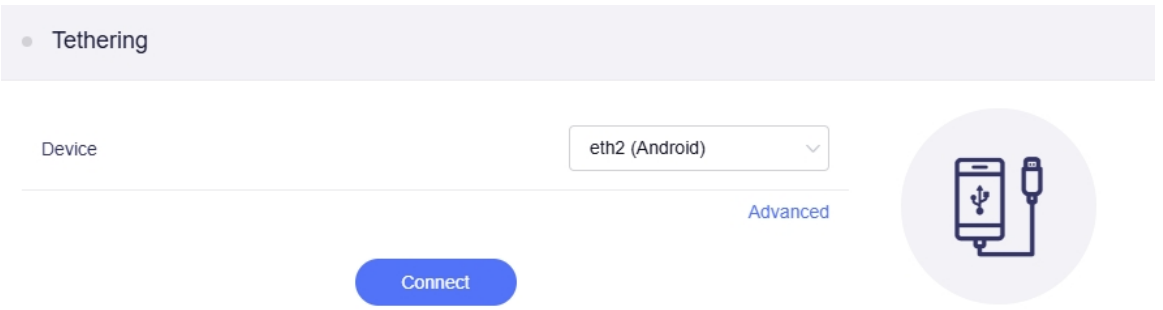
4.2.3 Connect to the Internet via USB Modem

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 4G/5G 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.

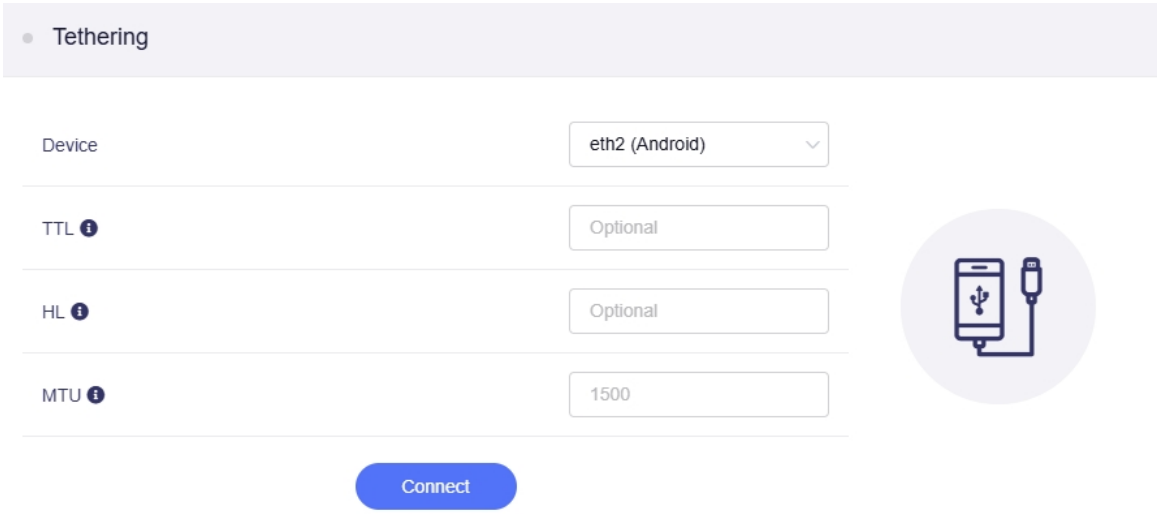


Follow the steps below to connect your router to the Internet via a USB modem.

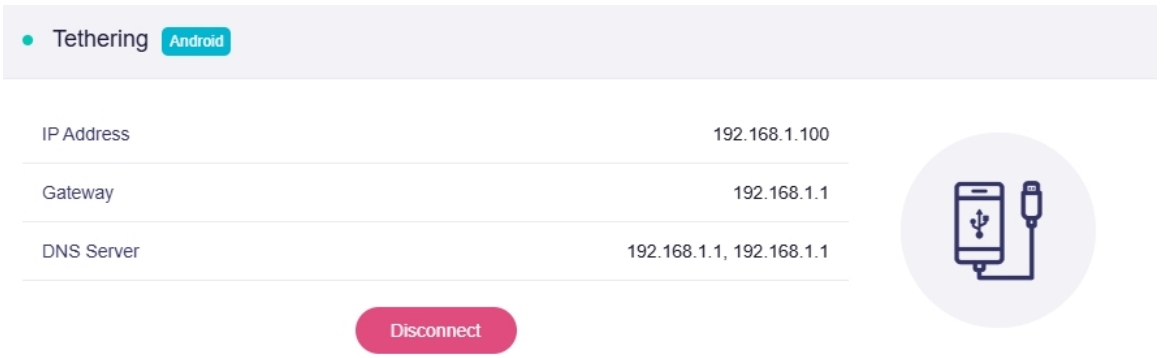
1. Plug a USB modem with a pre-installed SIM card into the router's USB port before powering it on.
2. Log in to the router's web admin panel, navigate to **INTERNET** > **Tethering**, then click **Connect**.



If you need to set advanced settings, such as TTL, HL, and MTU, click **Advanced** to customize these settings, then click **Connect**.

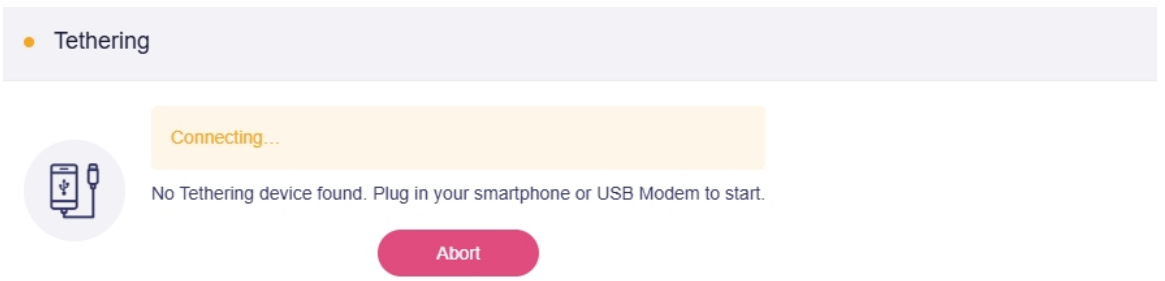


3. It will start connecting. Once connected, this page will display the network details.



Tips:

1. 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".
2. If you unplug the USB modem, the page will display the status shown below, indicating “No Tethering device found”, while the Tethering interface will remain in the “Connecting” state.



Chapter 5

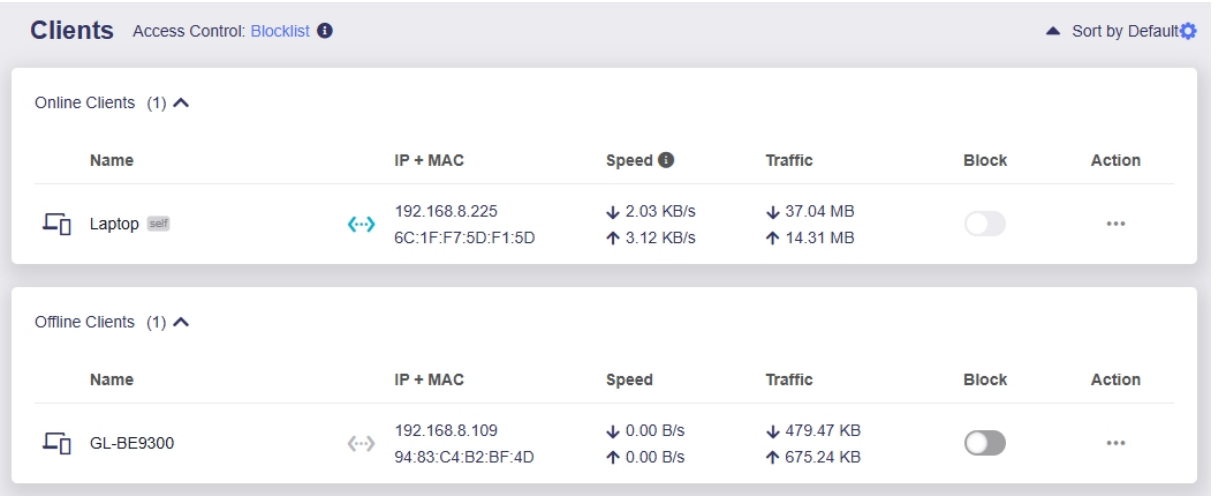
Clients

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.

5.1 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.

3. **Speed**

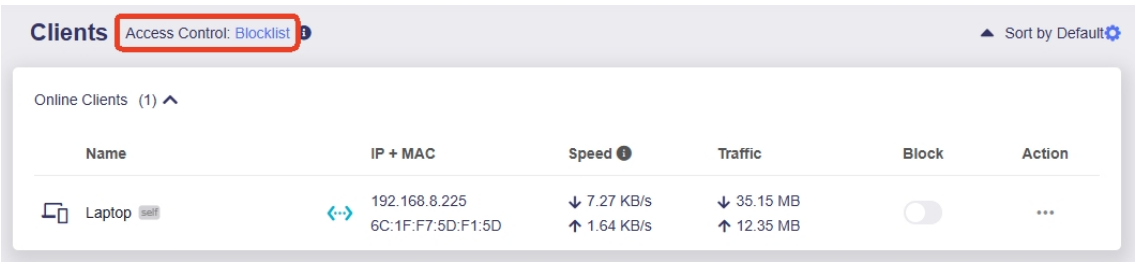
   The third column displays the internet speed of the connected device. This speed represents the average speed over the past 3 minutes. The system starts calculating the average speed when this page is opened (e.g., if the page has only been open for 10 seconds, the average speed will be based on just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

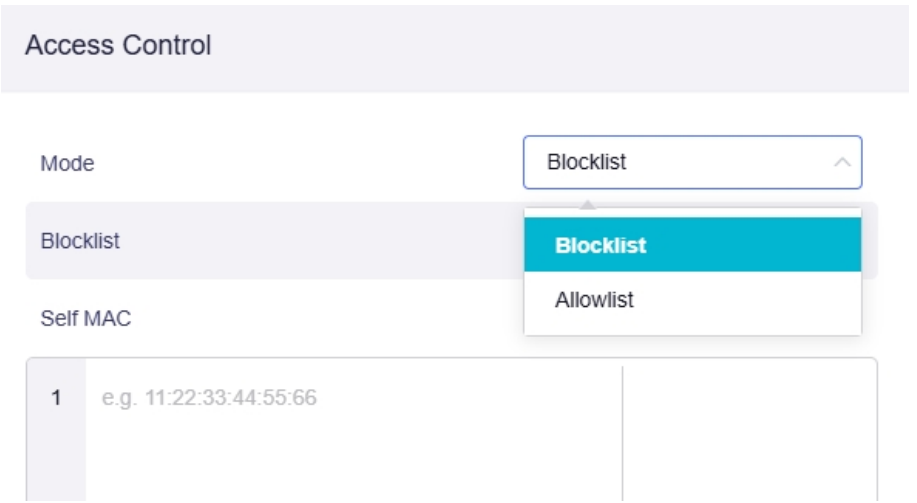
4. **Traffic**: The fourth column displays the internet traffic of the connected device.

5. **Block**

   In the fifth column, you can block specific connected device with one click.

   The Access Control rule is Blocklist by default, and you can switch it to Allowlist from the top as needed.



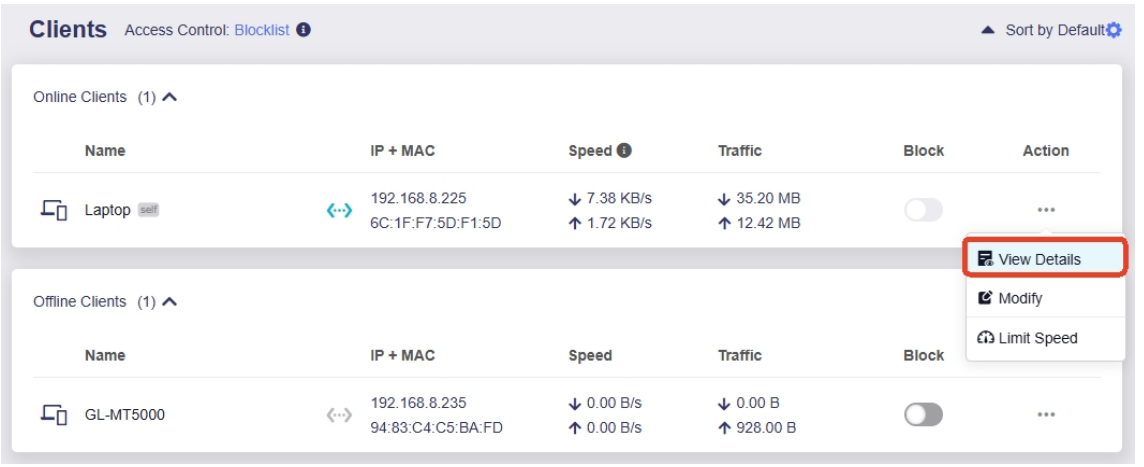


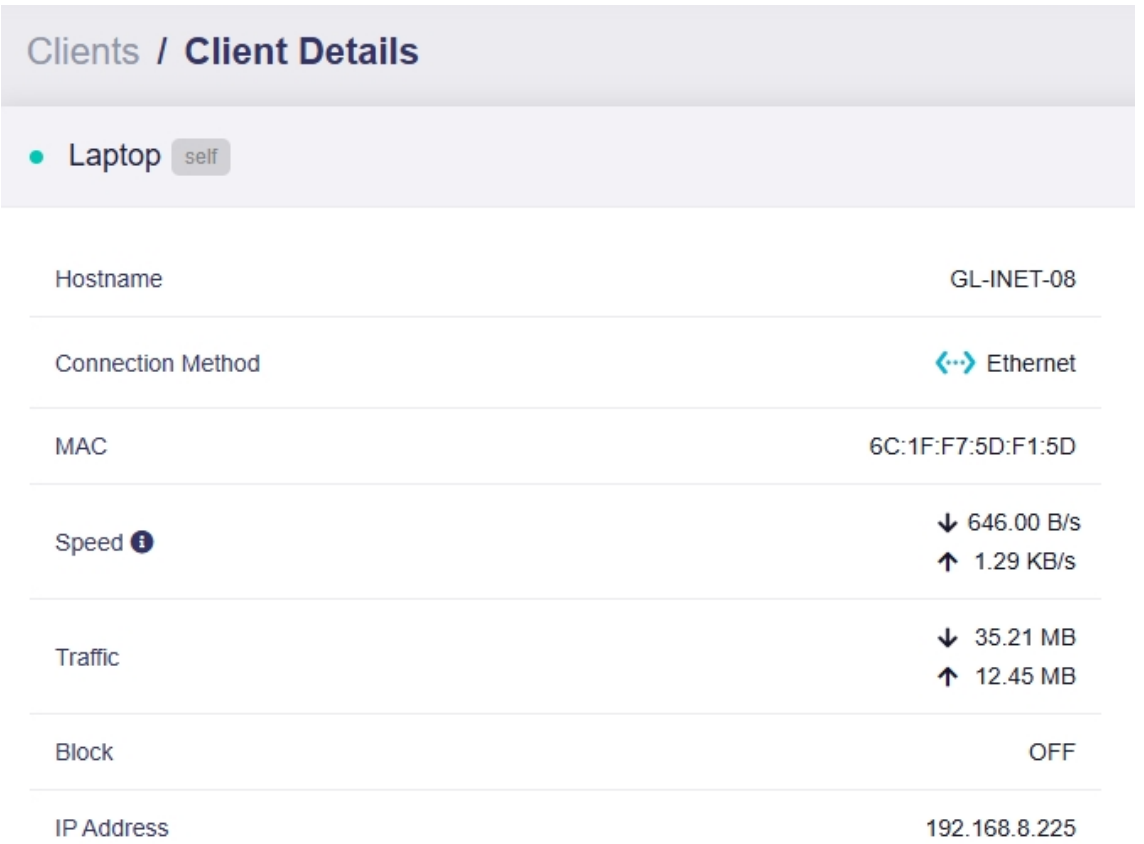
- **Blacklist**: Devices with MAC addresses in the blacklist are not allowed to connect to this router. Please note that blocking client is based on the MAC address of the device. If the blocked device uses different MAC address next time, it can still be able to connect to router.
- **Allowlist**: Only devices with specific MAC addresses are allowed to connect to this router, suitable for IoT devices and enterprise network management.

5.2 Action

1. **View Details**

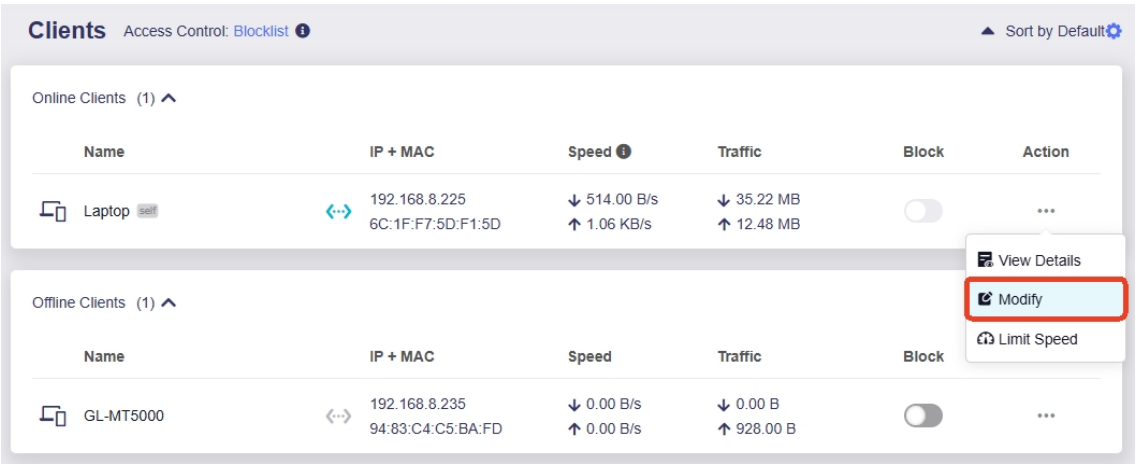
   Click the three-dot icon in the **Action** column, and click **View Details** from the drop-down menu to view the device details on a single page.

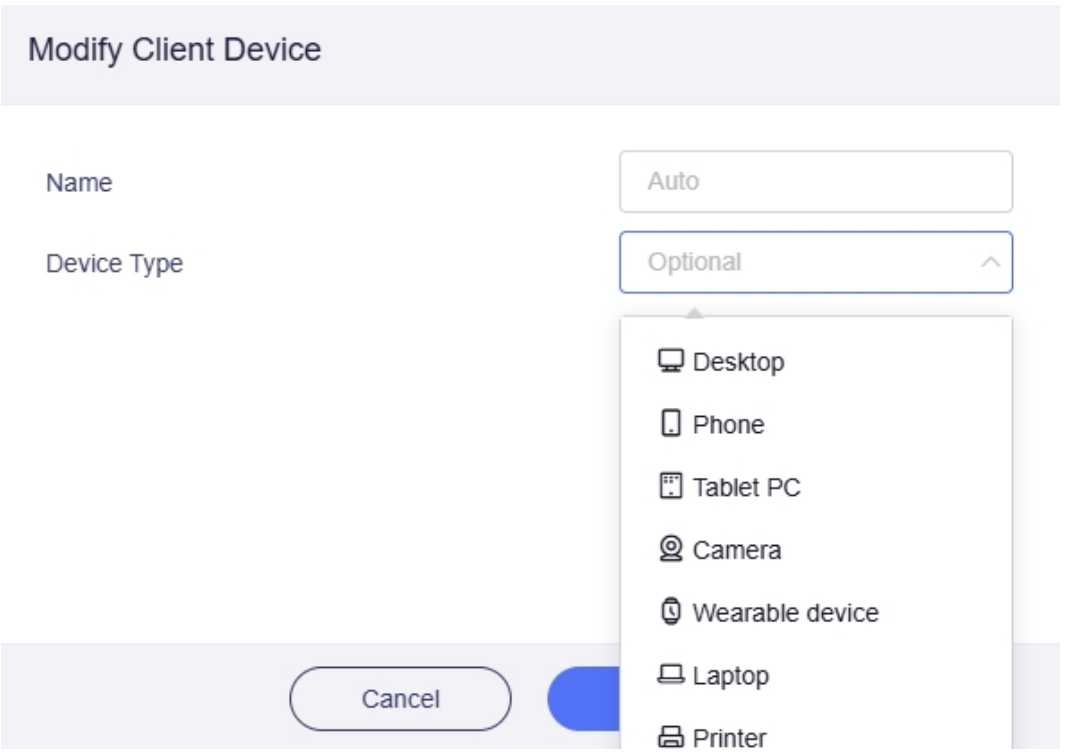




2. **Modify**

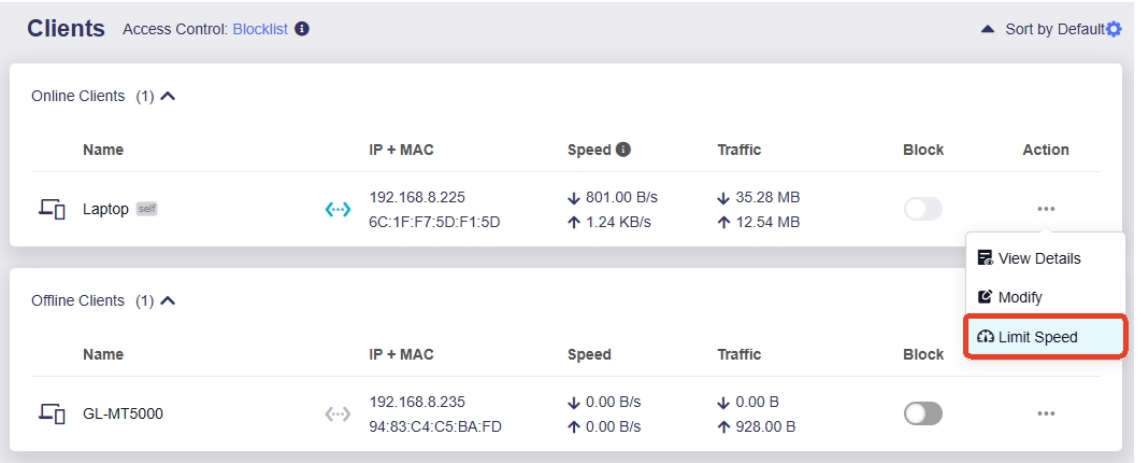
Click the three-dot icon in the **Action** column, and click **Modify** from the drop-down menu to modify the device name and type.



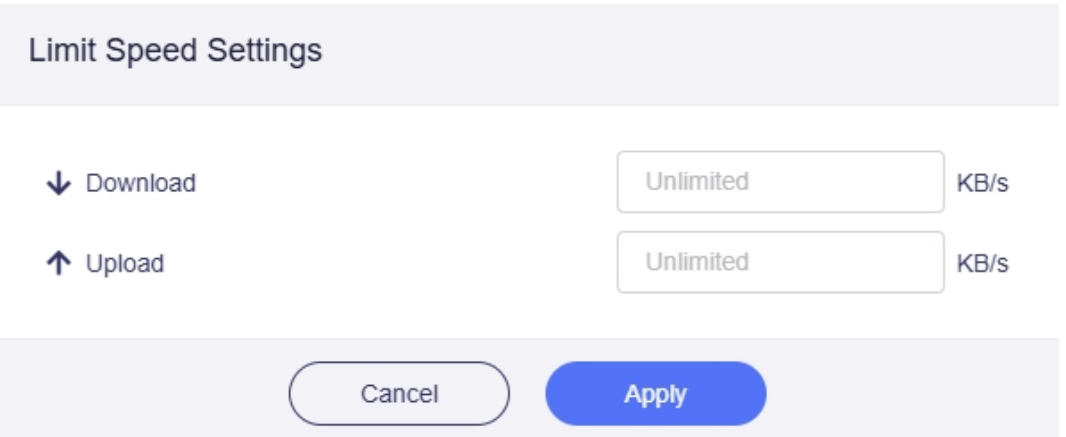


3. **Limit Speed**

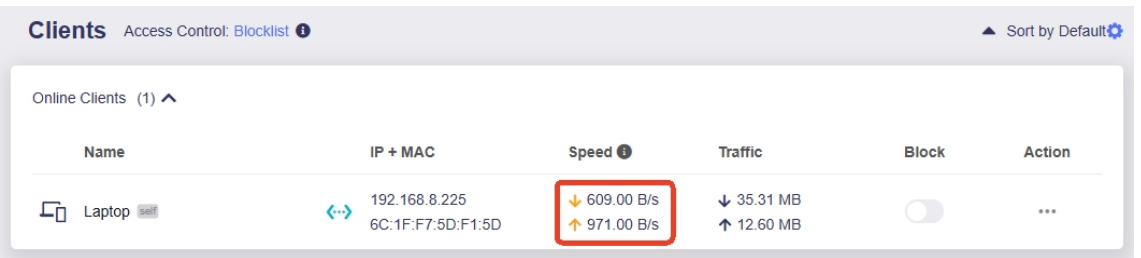
Click the three-dot icon in the **Action** column, and click **Limit Speed** from the drop-down menu.



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



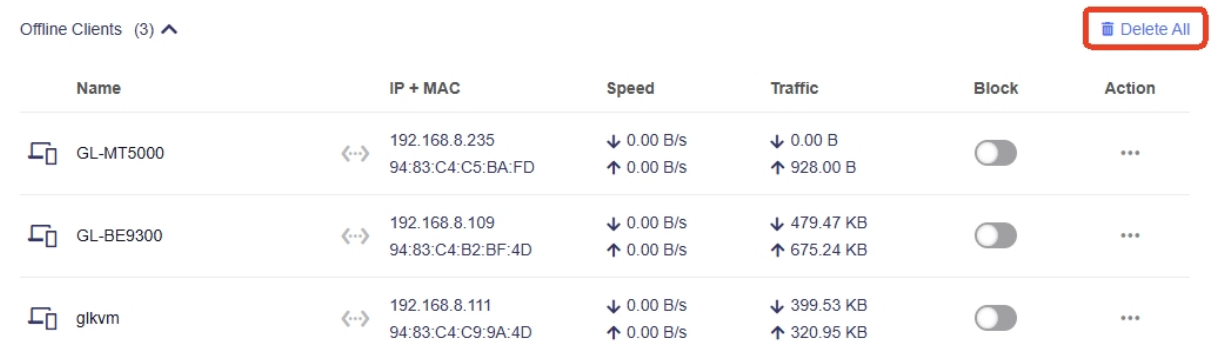
If speed limitation has been applied to a device, the upload/download speed arrows will turn yellow.



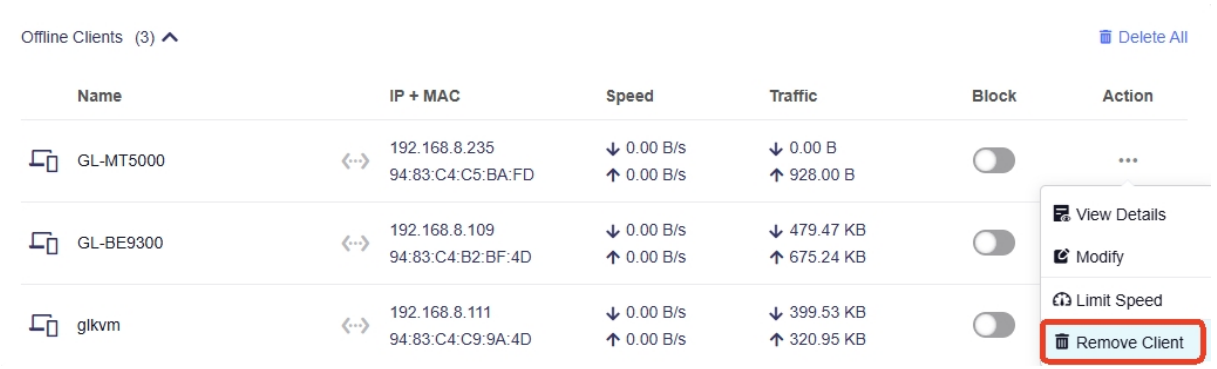
Tip: If the Limit Speed option is not visible, go to **NETWORK** > **Network Acceleration** and disable it. The Limit Speed option will then become available.

5.3 Remove Clients

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

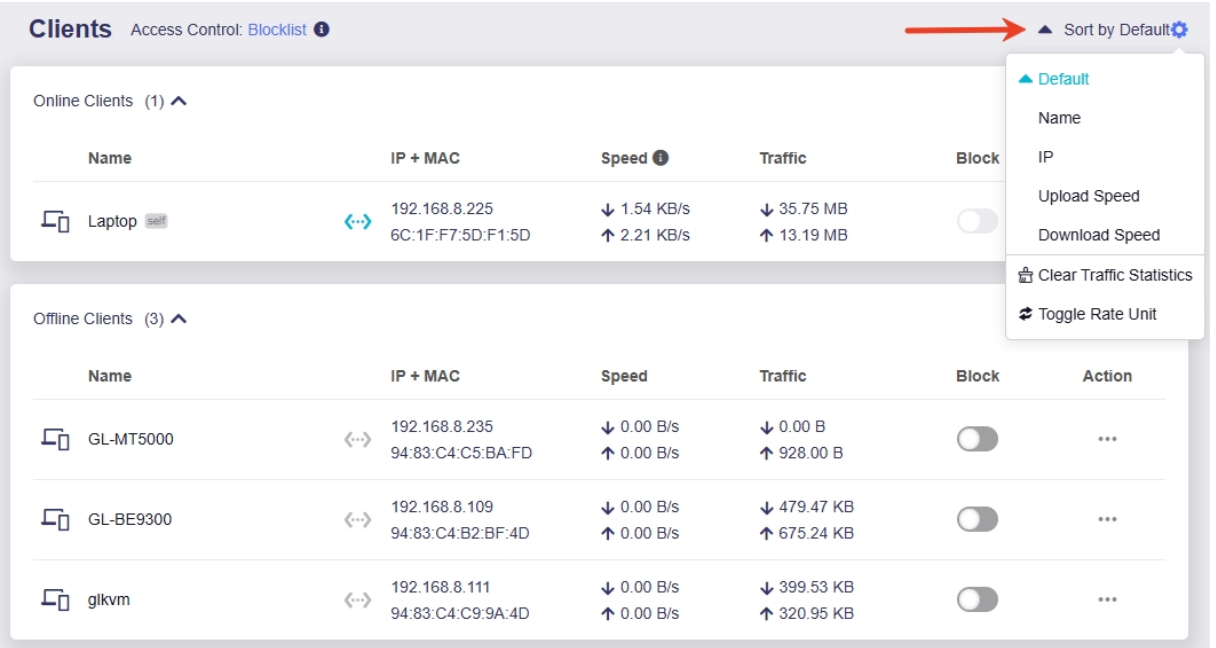


If you want to remove a specific client, click the three-dot icon in the **Action** column, then click **Remove Client** from the drop-down menu.



5.4 Sort

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



The default sorting rules are as follows:

- The self device (i.e., the device used to access the router's web admin panel) is always listed first.
- 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.

Chapter 6

Cloud Services

This chapter introduces two cloud services: GoodCloud and AstroWarp.

6.1 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.

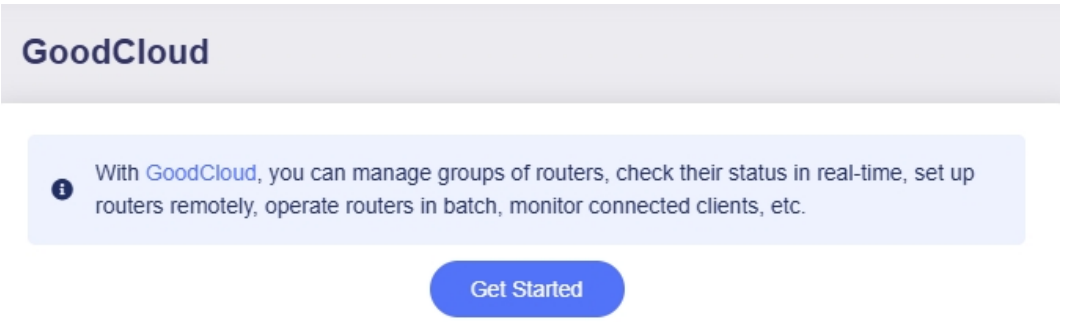
With GoodCloud, you can:

- 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

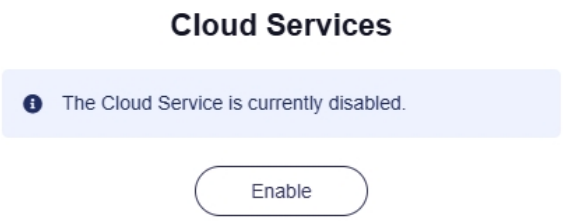
Some features are available in Enterprise Plan and VAR (Value Added Reseller) Plan. See here for details.

6.1.1 Enable GoodCloud

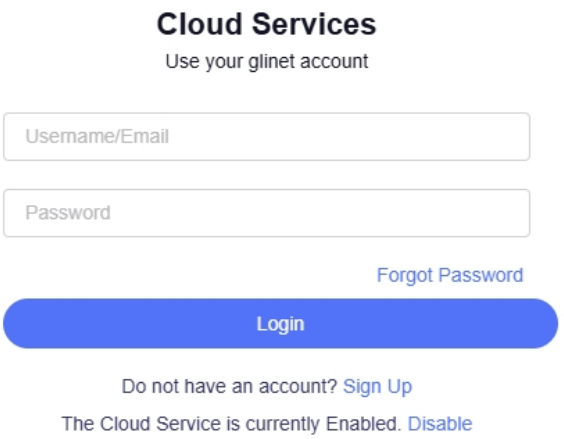
1. Log in to your router's web admin panel, navigate to **CLOUD SERVICE** > **GoodCloud**, and click **Get Started.**



2. A drop-down window will appear in the upper right corner. Click **Enable**.



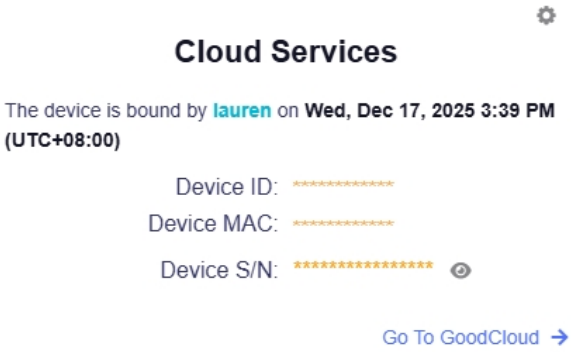
3. Log in with your GL.iNet Cloud account. If you don't have an account, sign up for one and log in. Once logged in, the router will be bound to your account automatically.



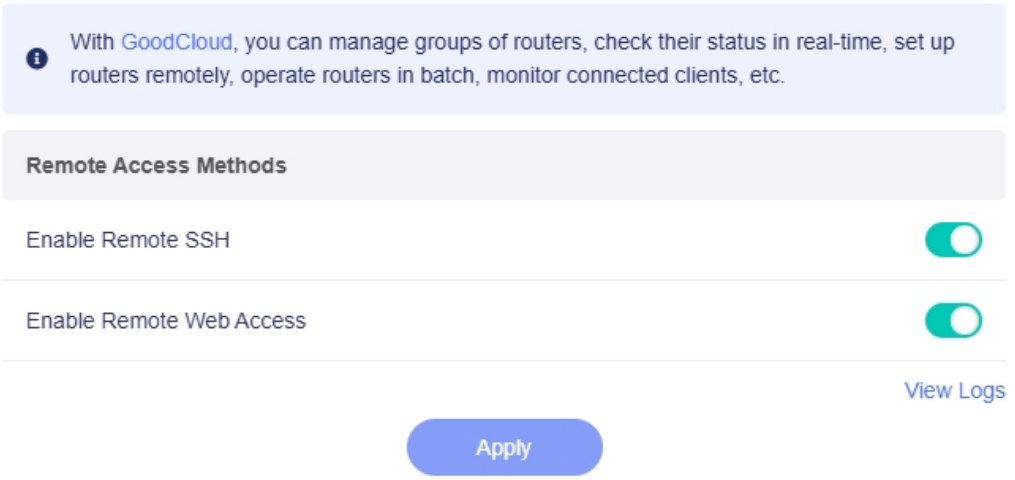
Tips:

- 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.

4. After binding successfully, click the **Cloud icon** in the upper right corner of the web admin panel. You will then see the bound device details, including the bound account, binding date, Device ID, Device MAC, and Device S/N.



5. Navigate to **CLOUD SERVICES** > **GoodCloud** and enable remote access. GoodCloud enables remote access to the bound router's web admin panel and terminal. This is particularly useful for remote management, network configuration, and troubleshooting.You can enable or disable the remote access for your router here.

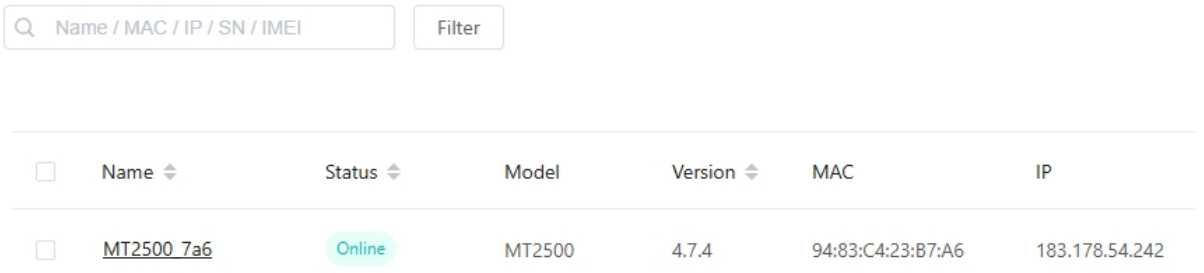


- **Remote SSH**: Remotely access the router's terminal from GoodCloud using SSH.
- **Remote Web Access**: Remotely access to the router's web admin panel from GoodCloud via HTTP/HTTPS.
- **View Logs**: Redirect to the Log page and display Cloud log.

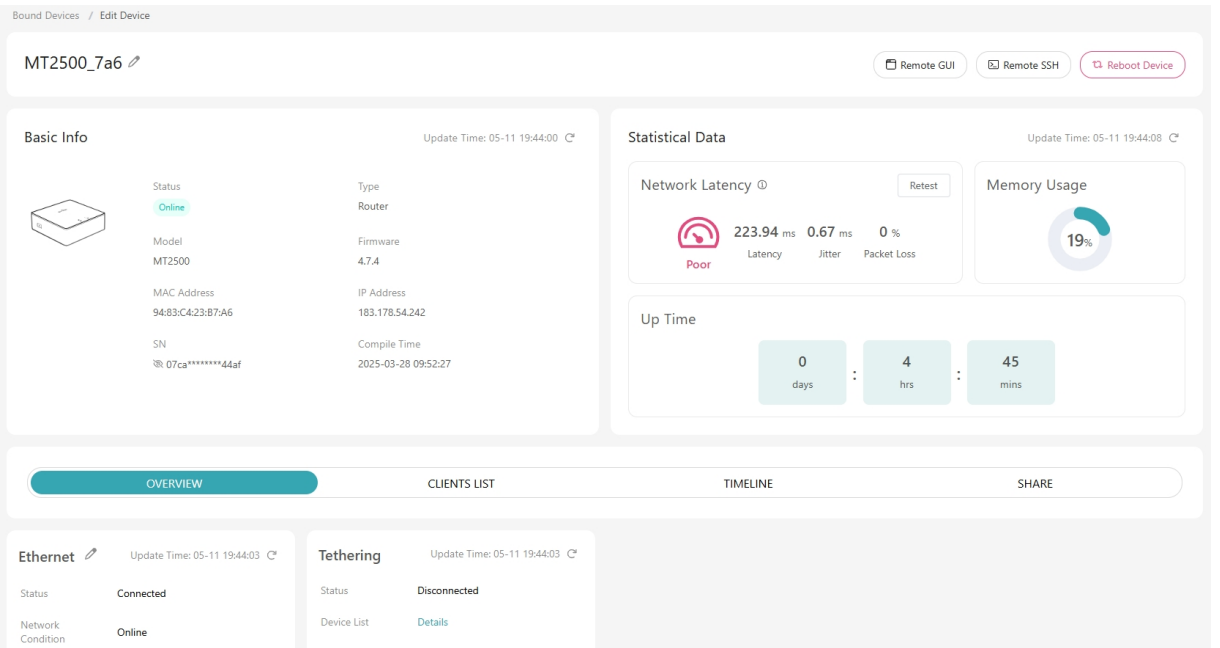
6.1.2 Manage Your Router

Check Device Details

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

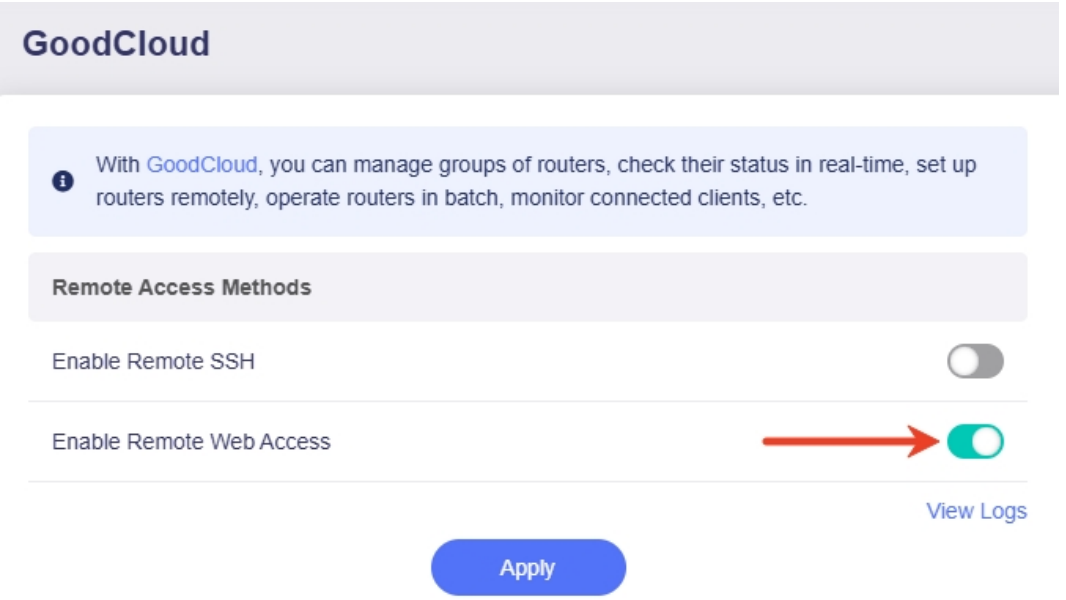


Click the device name to enter the device details page, which displays basic information, statistical data, network overview, client list, and timeline. You can also perform advanced operations, such as remotely accessing the router, and rebooting the device.

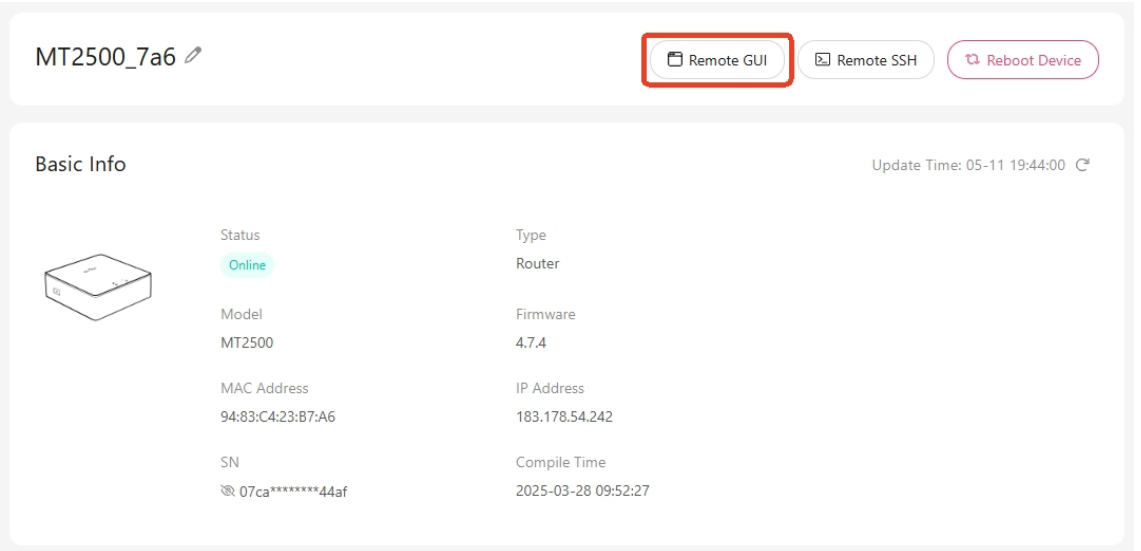


Remote Access Web

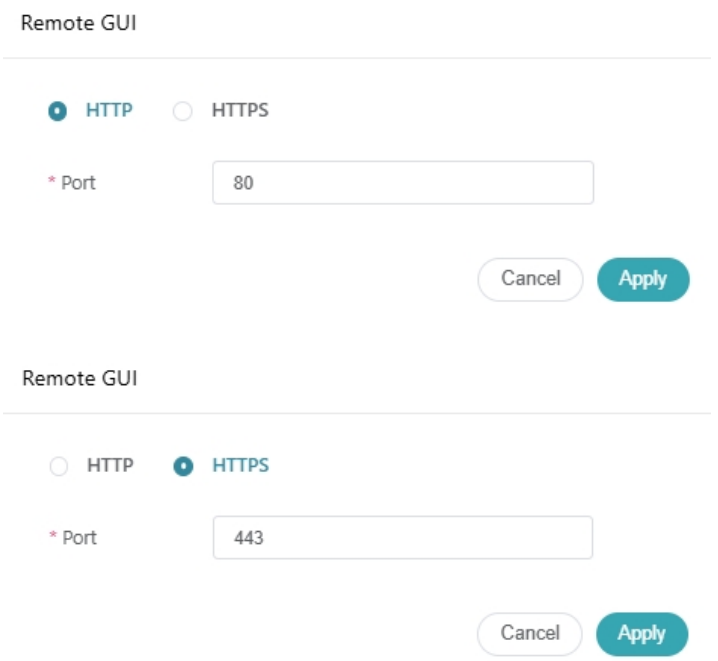
1. Log in to the router's web admin panel, navigate to **CLOUD SERVICES** > **GoodCloud**, enable **Remote Web Access**, then click **Apply**.



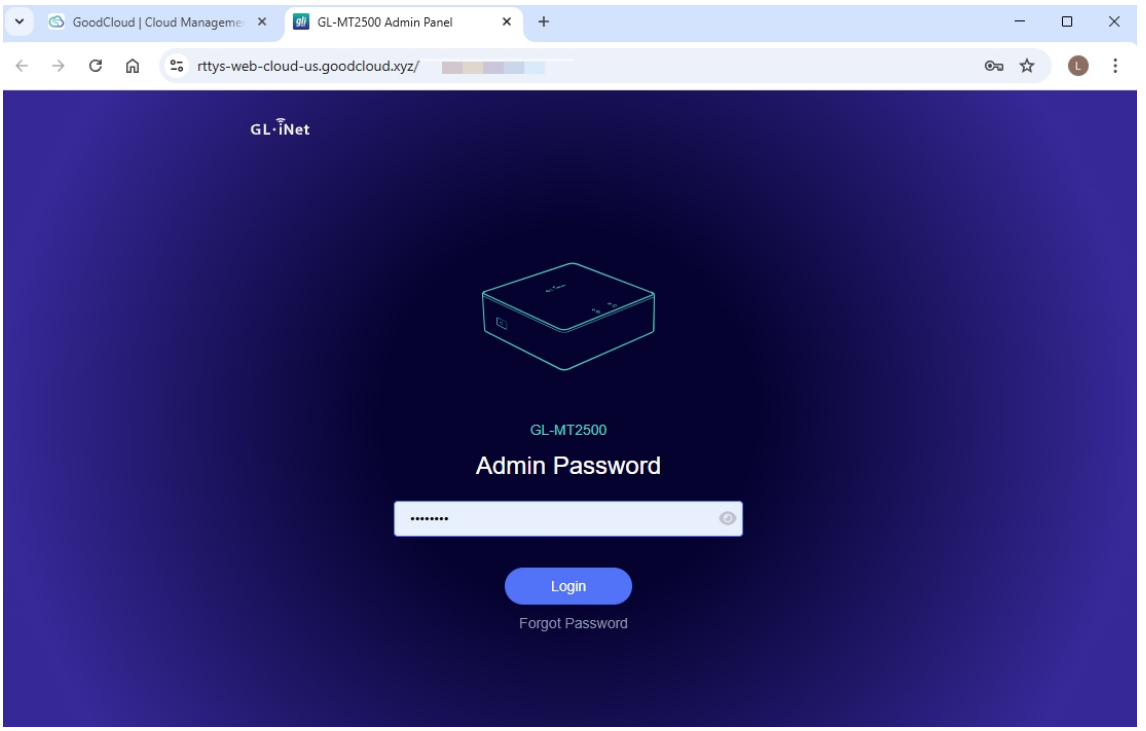
2. Log in to the GoodCloud platform and navigate to **Device** > **Bound Devices**. Click the device you want to access, and you will enter the device details page.
3. On the device details page, click the **Remote GUI** button in the upper right corner.



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

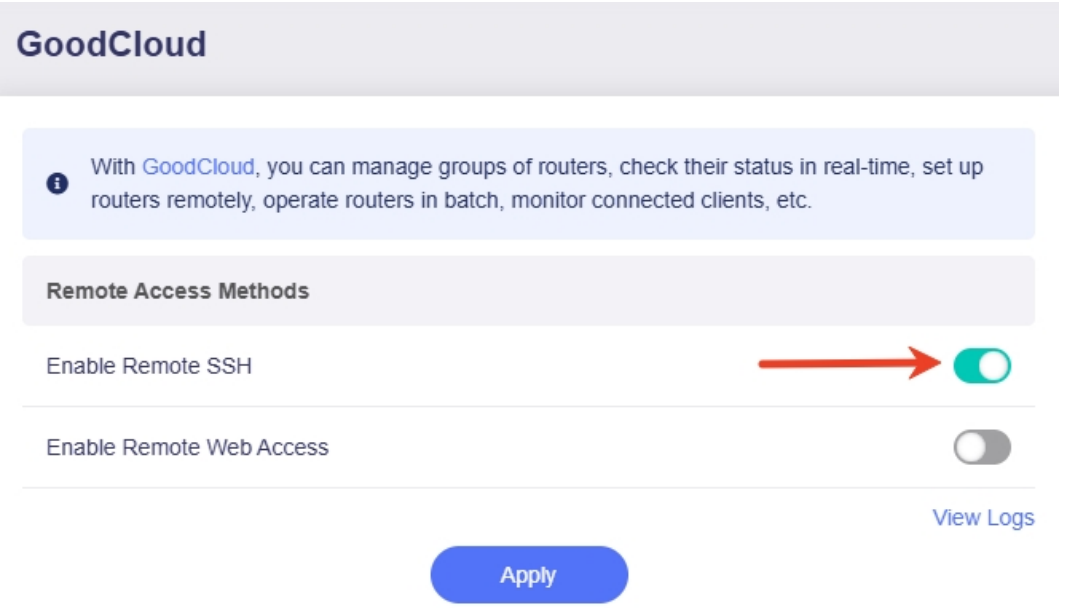


5. You will be re-directed to the router's login page. Enter the admin password to remotely access the router's web admin panel.

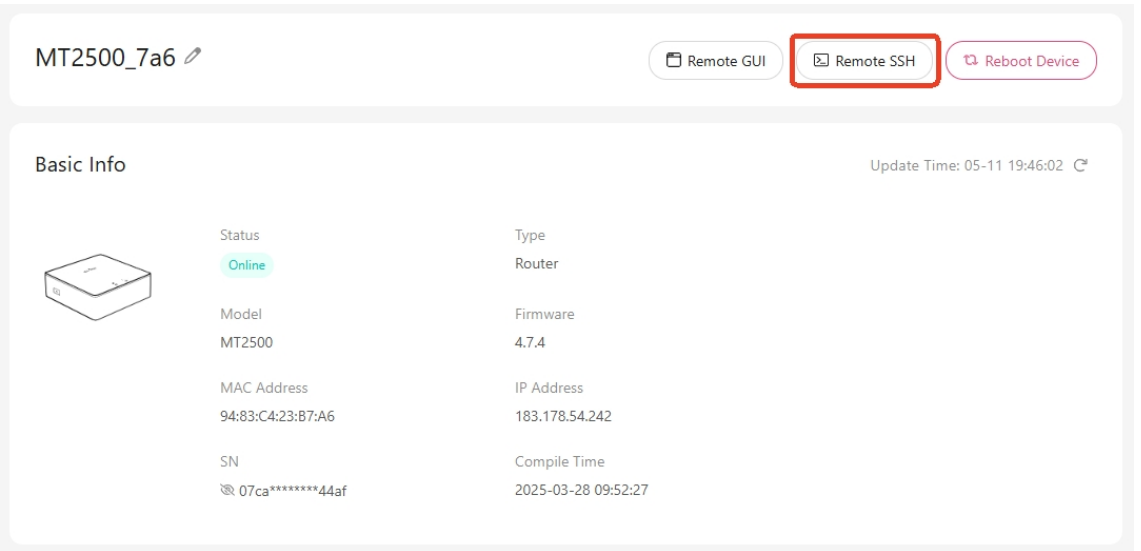


Remote Access Terminal

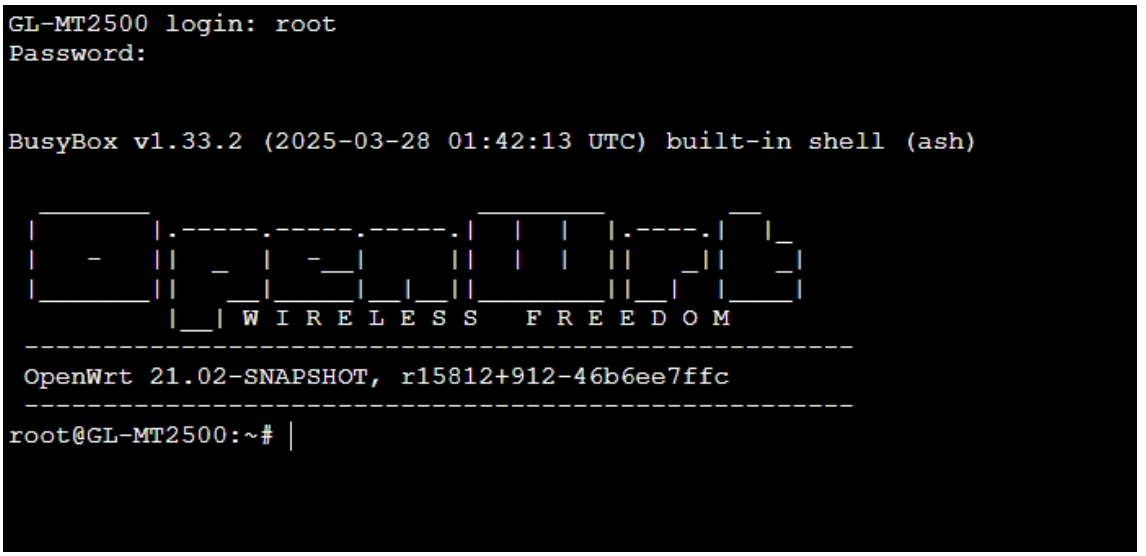
1. Log in to the router's web admin panel, navigate to **CLOUD SERVICES** > **GoodCloud**, enable **Remote SSH**, then click **Apply**.



2. Log in to the GoodCloud platform and navigate to **Device** > **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.

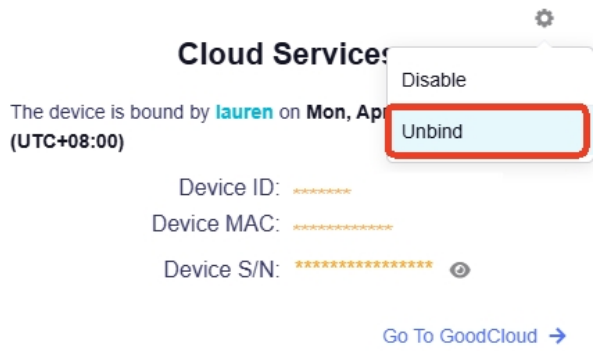


4. Log in as **root** and input the password to access the terminal of your router.

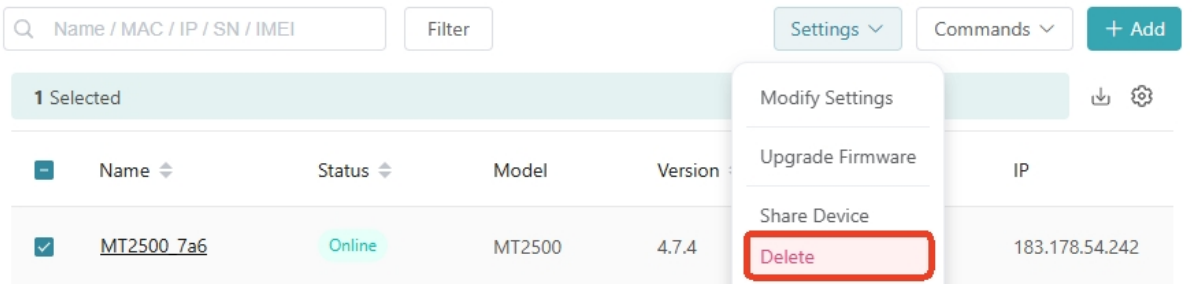

GL-MT2500 login: root
Password:
BusyBox v1.33.2 (2025-03-28 01:42:13 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT, r15812+912-46b6ee7ffc
root@GL-MT2500:~#

6.1.3 Unbind Device

In the router's web admin panel, click the Cloud icon in the upper right corner. In the drop-down menu, click the gear icon and select **Unbind**. Your device will then be unbound from your GoodCloud account.

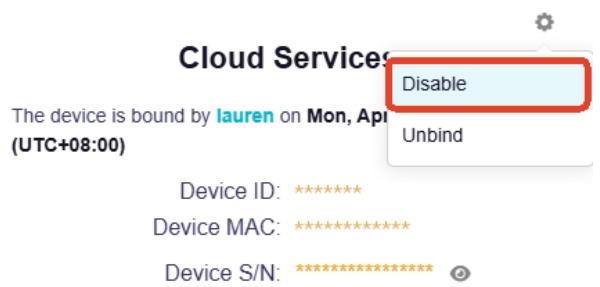


Alternatively, log in to the Cloud platform and navigate to **Device** > **Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



6.1.4 Disable GoodCloud

If you no longer want the device connected to the Cloud, click the Cloud icon in the upper right corner. In the drop-down menu, click the gear icon and select **Disable**. The Cloud service will then be disabled.



6.2 AstroWarp

AstroWarp is an advanced networking platform designed to provide seamless remote networking and remote device management.

Built specifically for GL.iNet router integration, AstroWarp supports comprehensive device management across entire networks, enabling both upper and lower device control.

With a focus on network-wide management and future support for hardware-level control, AstroWarp offers a more robust and dependable solution for managing devices and maintaining secure, stable networks.

Refer to astrowarp.net for more information.

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.

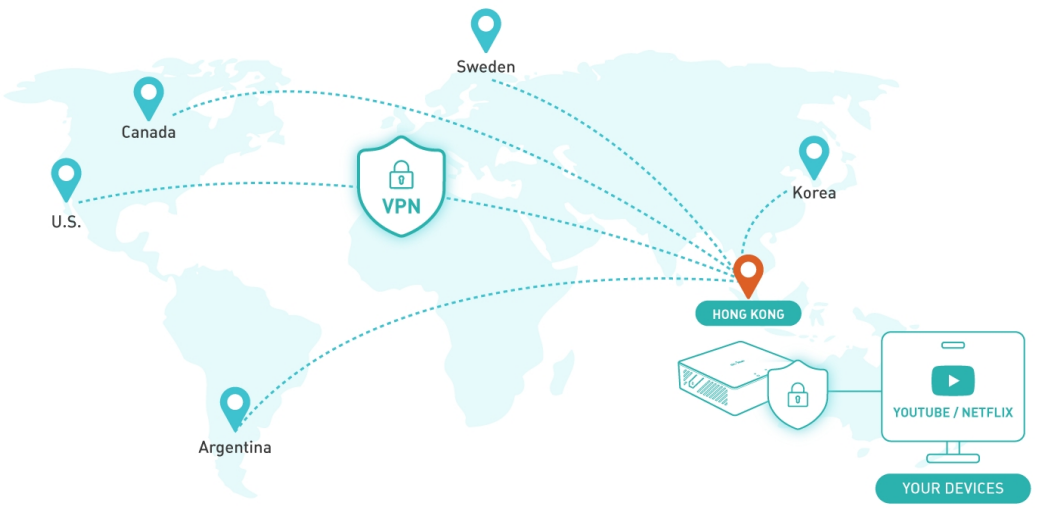
7.2 Application Scenarios

1. **Personal Data Privacy**

   The VPN service on this router works with a full range of wired devices, including desktops, laptops, gaming consoles, smart TVs, and streaming devices. All your data transmitted over wired connections is protected by the VPN. You can also customize VPN policies to enable flexible protection for specific devices.

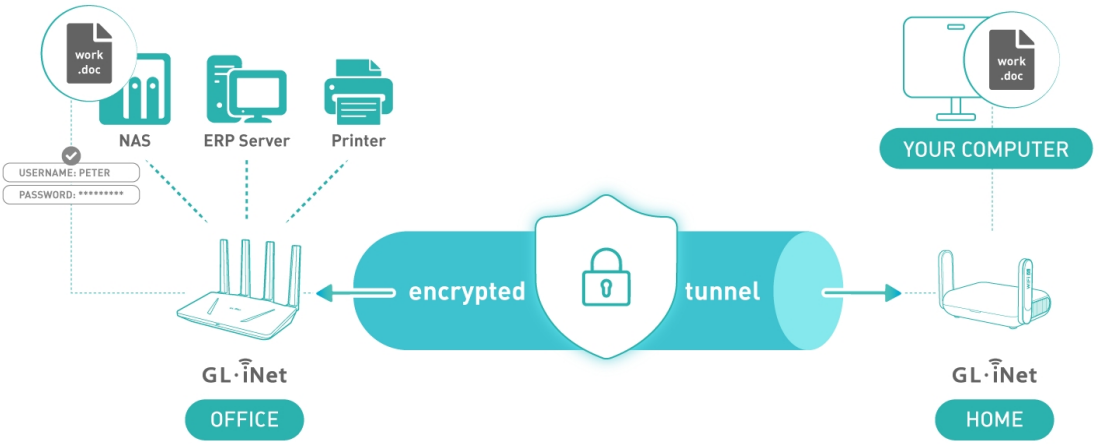
2. **Unrestricted Access Worldwide**

   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.



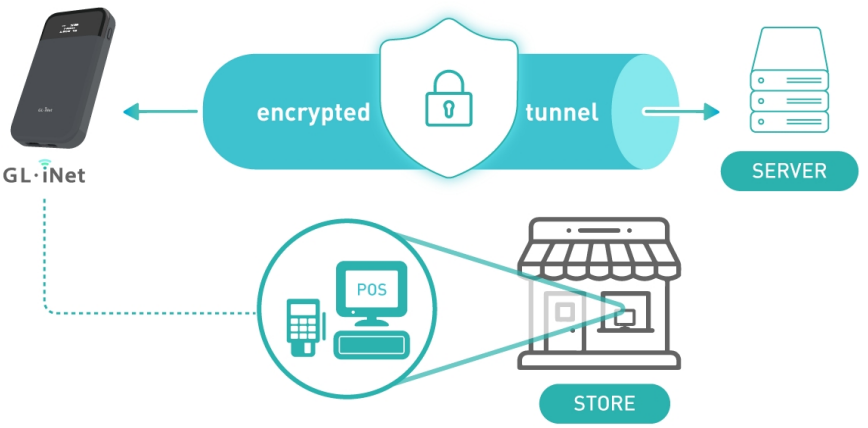
3. Small Business Data Security

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

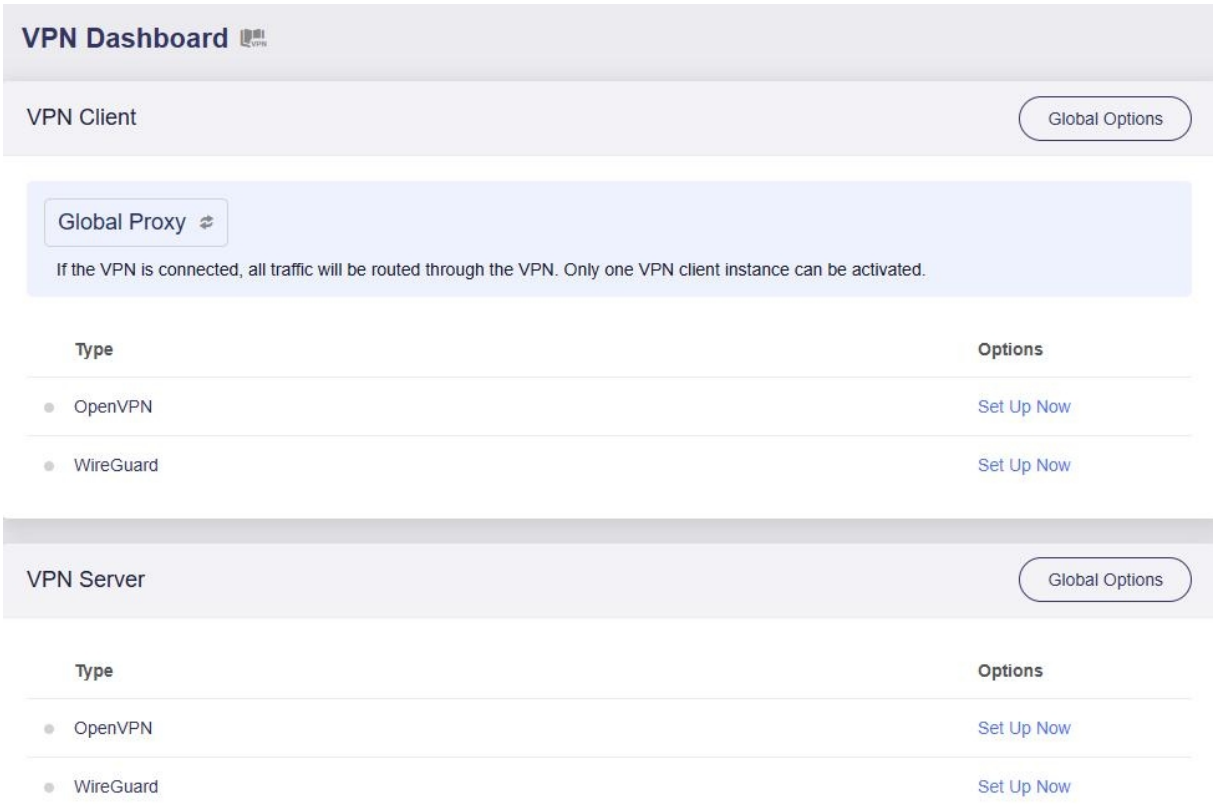
VPN Dashboard

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**.

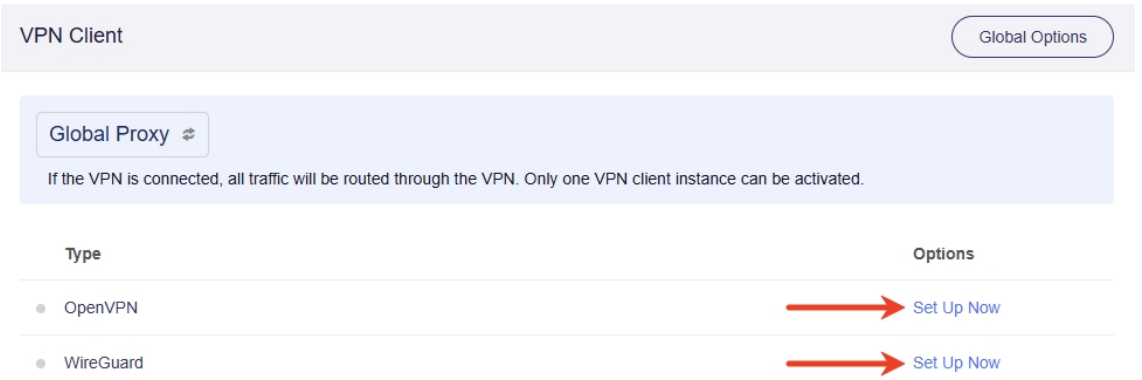
The VPN dashboard displays VPN connection details, such as server address, traffic statistics, client virtual IP, and connection log. It also allows users to configure advanced settings such as the VPN Kill Switch, VPN policy, IP Masquerading, MTU, and VPN Cascading.

This page is divided into two sections: **VPN Client** and **VPN Server**.

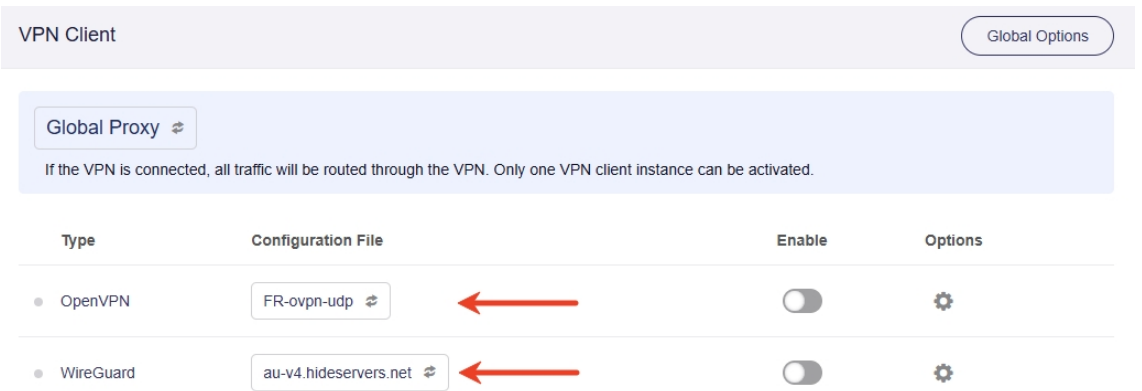


8.1 VPN Client

When entering this page for the first time, if there is no configuration file available for OpenVPN and WireGuard, the page displays as follows. Click **Set Up Now** and you will be redirected to the OpenVPN Client or WireGuard Client to upload your VPN configuration file.

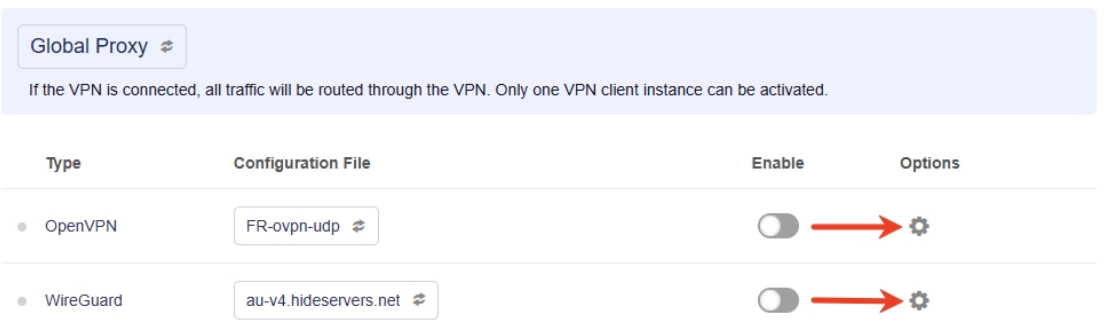


Once uploaded, your configuration will be shown in the Configuration File column. If you have multiple configuration files uploaded, you can switch files by clicking on the box.

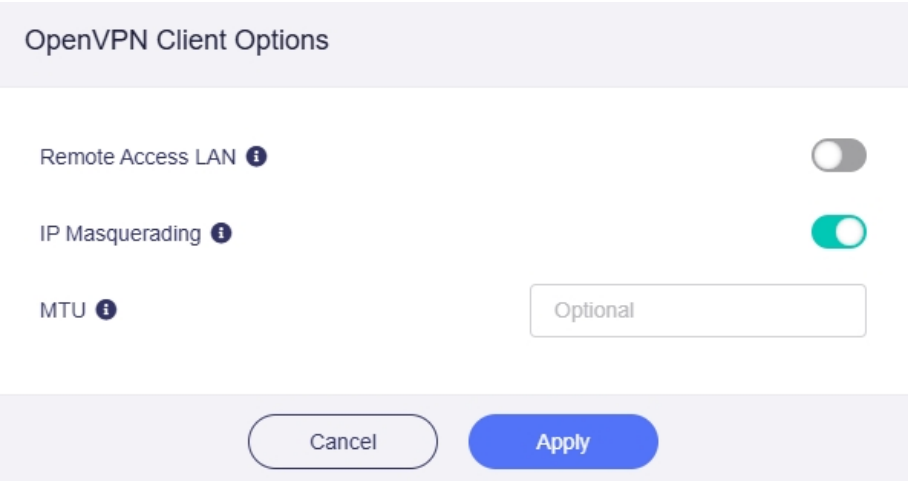


8.1.1 Client Options

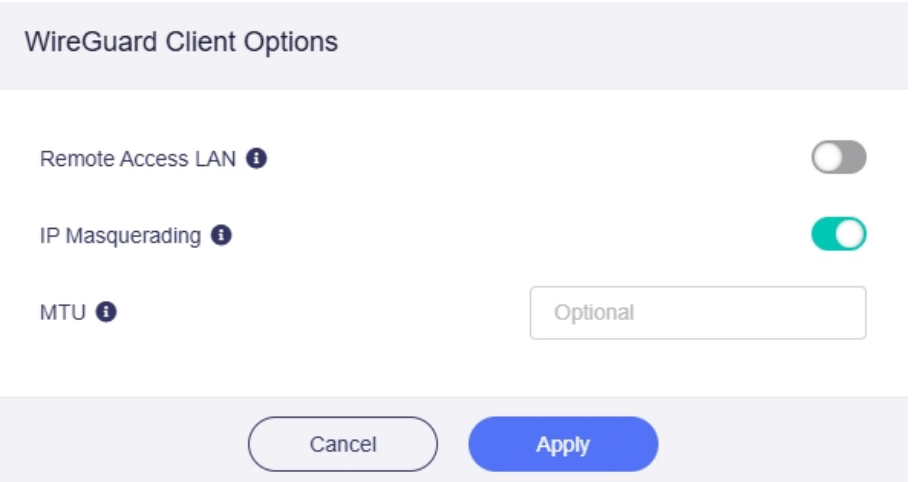
Click the gear icon on the right to access OpenVPN or WireGuard client options.



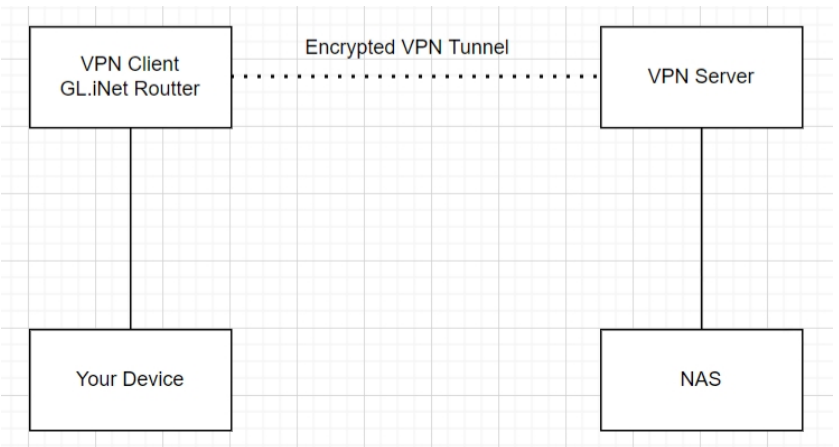
The OpenVPN Client Options displays as follows.



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.

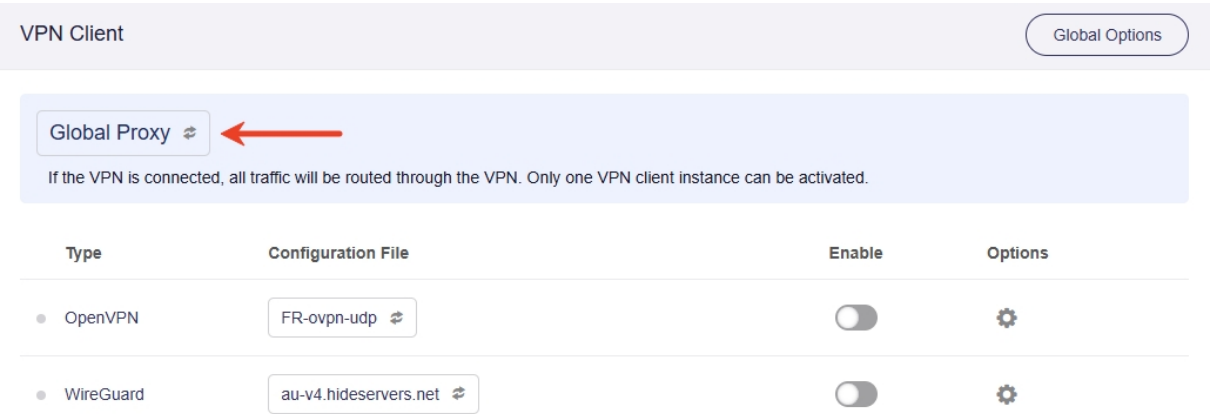


For example, as shown in the diagram above, the GL.iNet router runs as a VPN client and connects to a VPN server over the VPN tunnel. When this option is enabled, both the GL.iNet router and its LAN-side devices can be accessed by devices on the VPN server side (e.g. NAS). This requires you to add a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

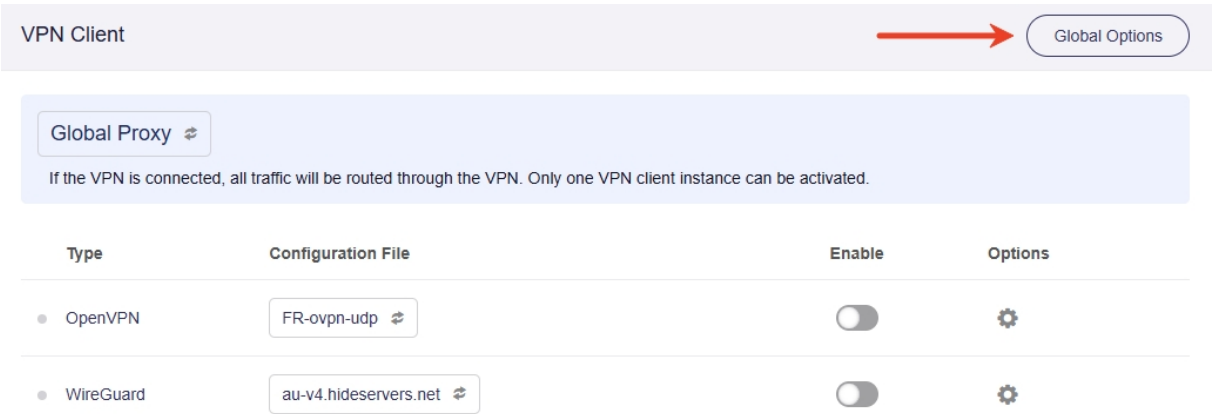
   - **Based on the Target Domain or IP**: In this mode, only the traffic of certain websites identified by IP address or domain name will be routed through VPN. Only one VPN client instance can be activated.

- **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.

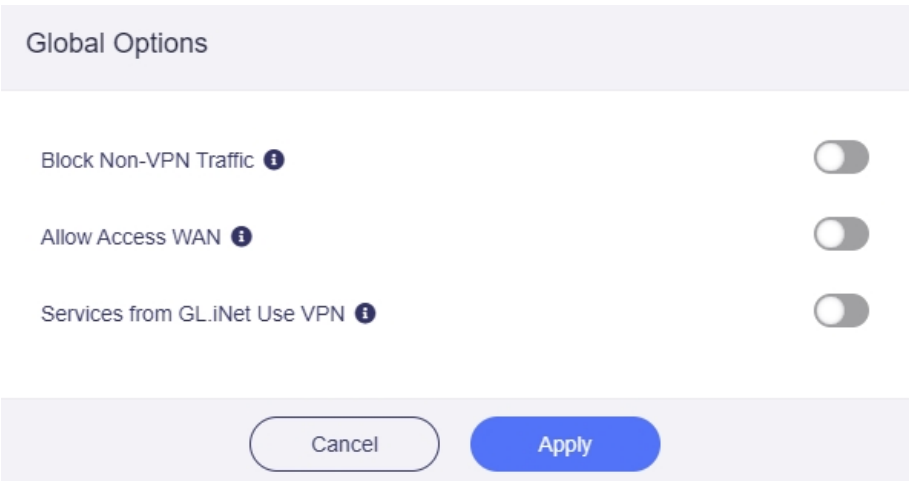
3. **Route Mode**
   - **Auto Detect**: The routing rules defined in each VPN client configuration file or issued by the VPN server will be used.
   - **Customize Routing Rules**: You can manually configure routing rules for each VPN client instance.

8.1.3 Global Options

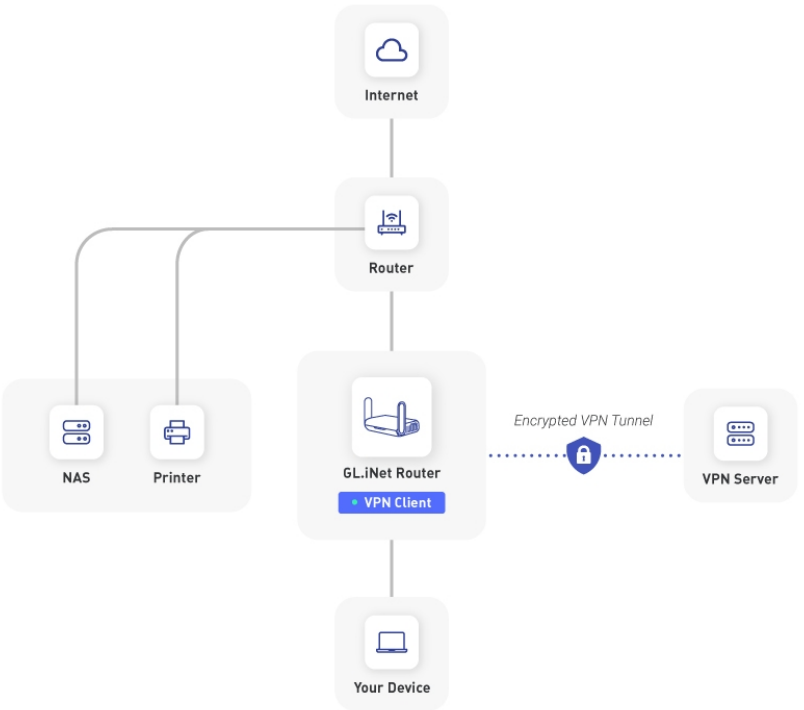
Click **Global Options** in the upper right corner to configure settings for your VPN client.



A pop-up window will appear as shown below.



- **Block Non-VPN Traffic**: It is also known as **VPN Kill Switch**. 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.
- **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.



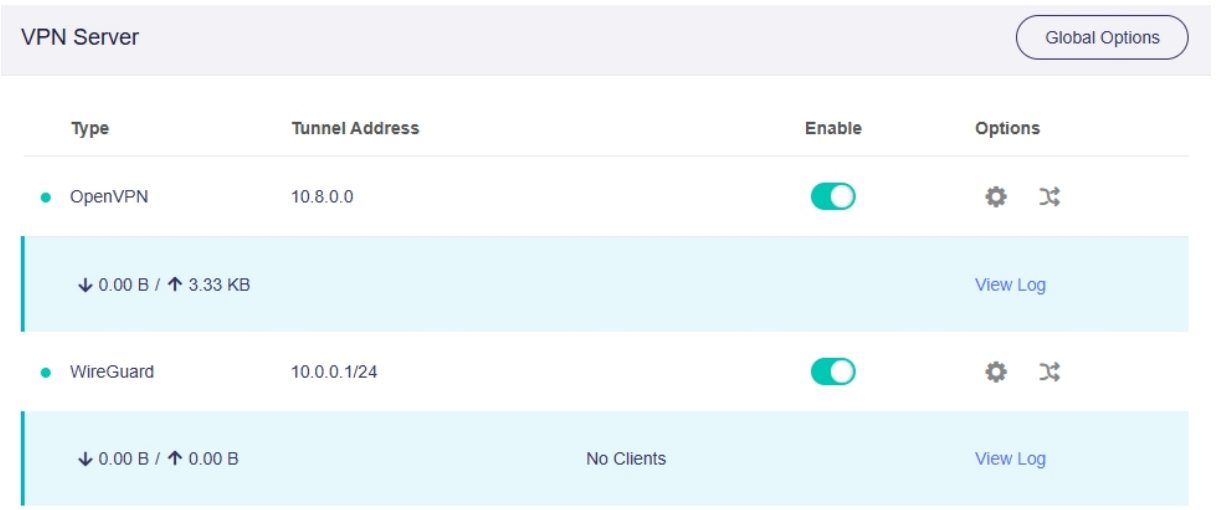
As shown in the diagram above, enabling this feature allows your local devices to reach hosts on the upstream subnet, such as printers and NAS.
This option is primarily designed to let clients access devices within the upstream subnet. However, the router cannot distinguish upstream subnet traffic from 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

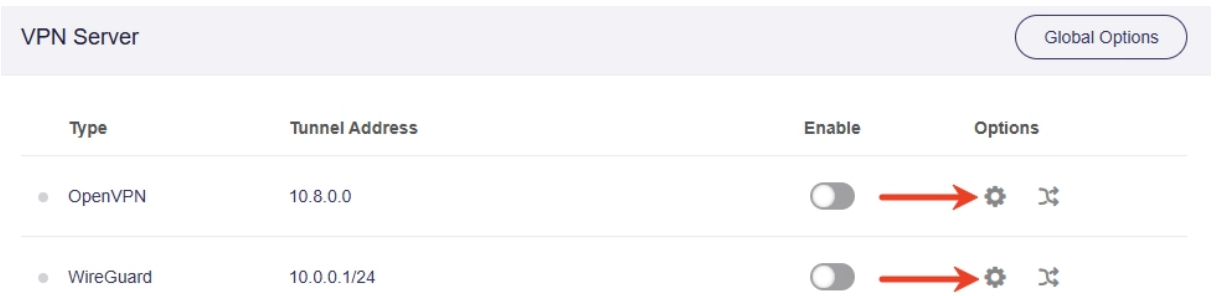
If the router has never been configured as an OpenVPN or WireGuard server, the page will appear as shown below. Click **Set Up Now** and you will be redirected to the OpenVPN Server or WireGuard Server page to initialize your VPN server.

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

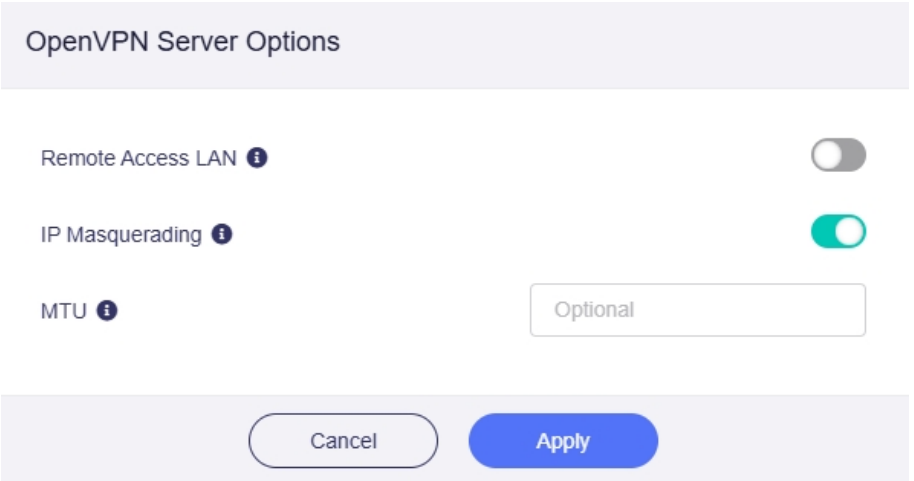


8.2.1 Server Options

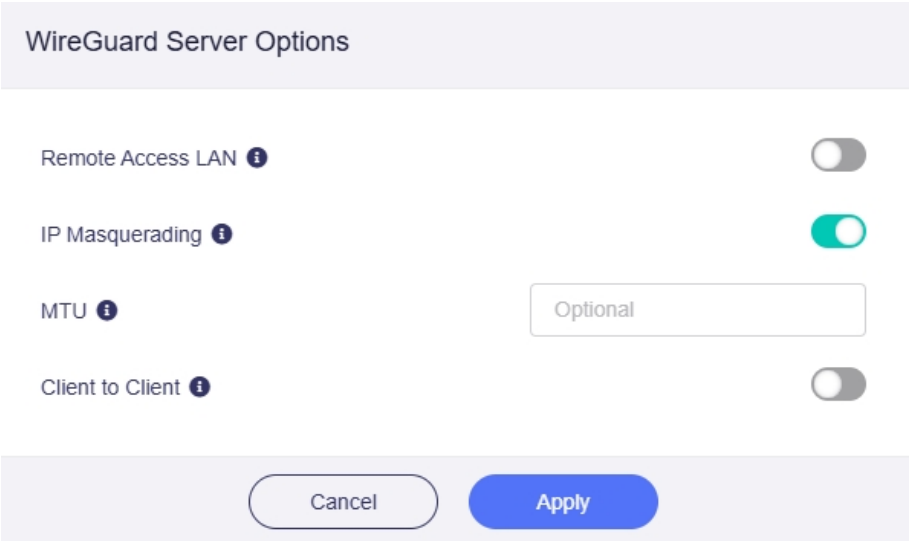
Click the gear icon on the right to access OpenVPN or WireGuard server options.



The OpenVPN Server Options displays as follows.



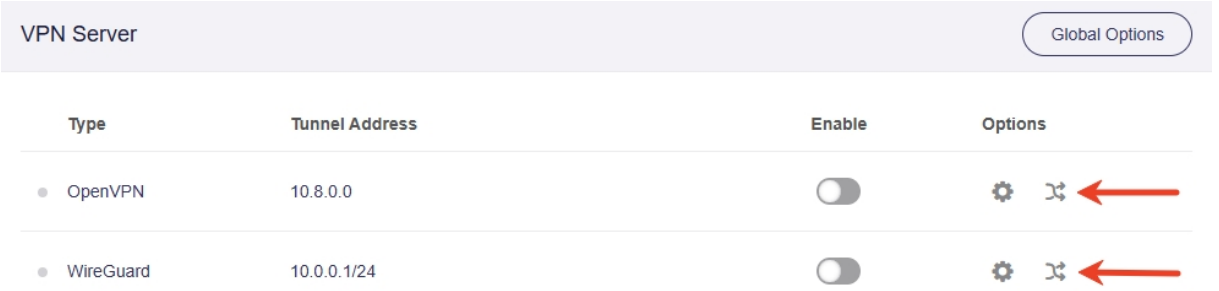
The WireGuard Server Options displays as follows.



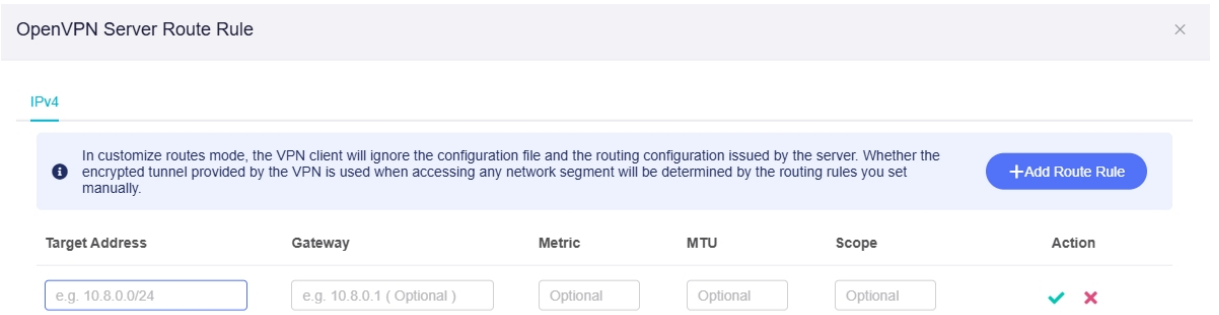
- **Remote Access LAN**: If enabled, resources inside the server's LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading**: If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer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

8.2.2 Server Route Rule

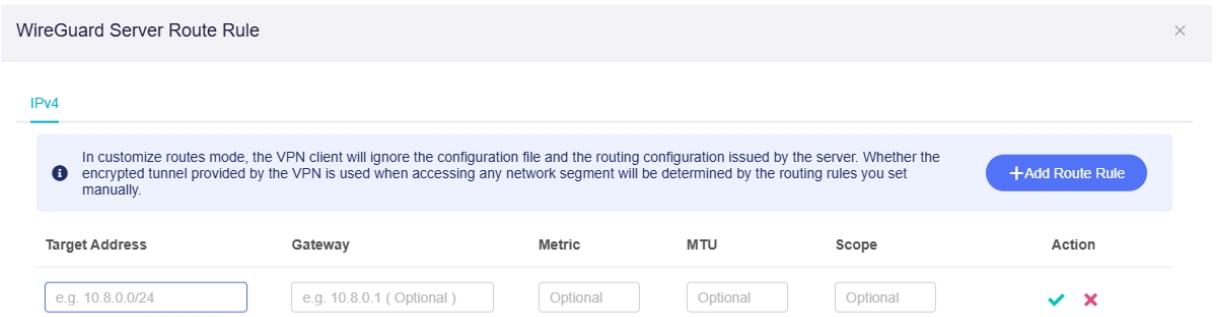
Click the route icon on the right to customize OpenVPN or WireGuard route rules as needed.



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.

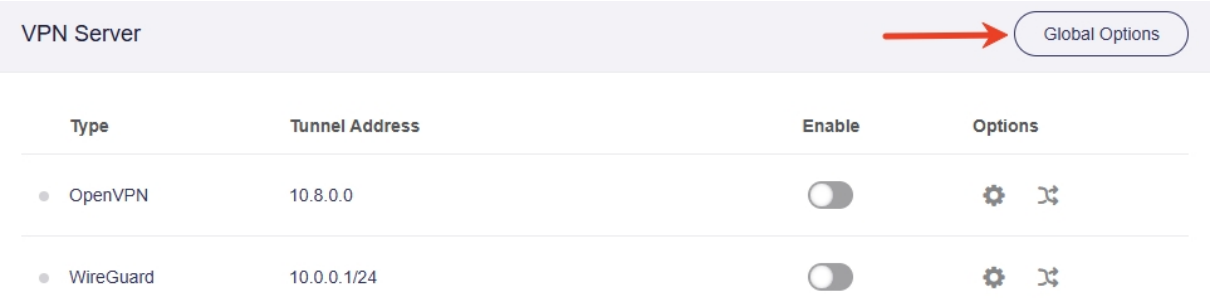


The WireGuard Server Route Rule displays as follows. Click **Add Route Rule**, enter the **Target Address** and **Gateway**, then click the green check icon to apply.

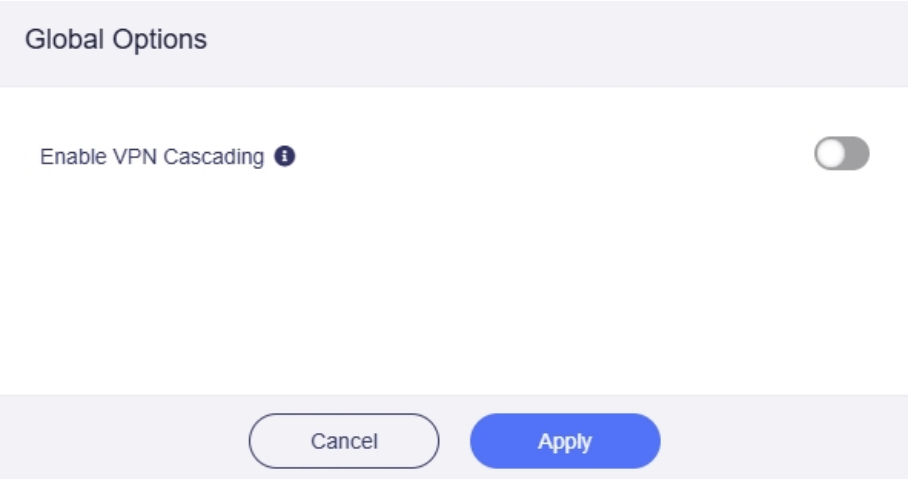


8.2.3 Global Options

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



A pop-up window will appear as shown below.



- **VPN Cascading**: If 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. See here for more details.

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:

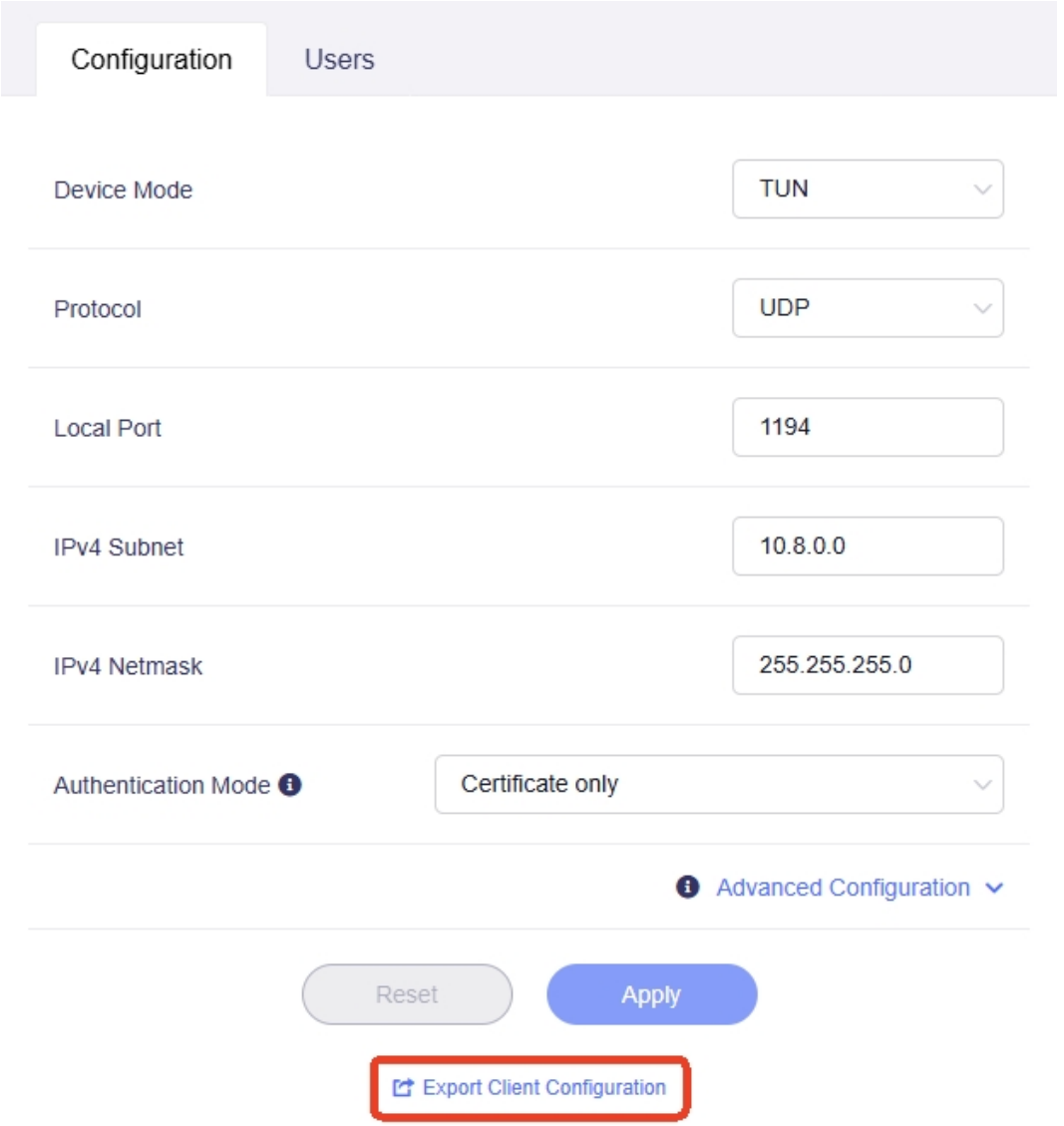
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.
   - If the above two methods don't work (e.g., if your network is behind CGNAT), you may try our SD-WAN solution AstroWarp.

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.

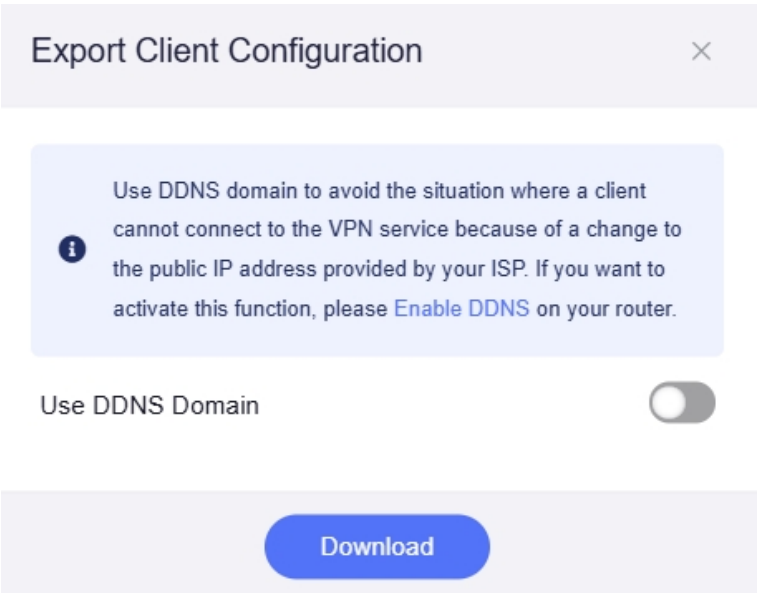


- **Device Mode**: TAP-S2S or Tun. See here for the differences.
- **Protocol**: UDP or TCP. See here for the differences.
- **Authentication Mode**: This determines the authentication method used when the client connects to the server. There are three options:

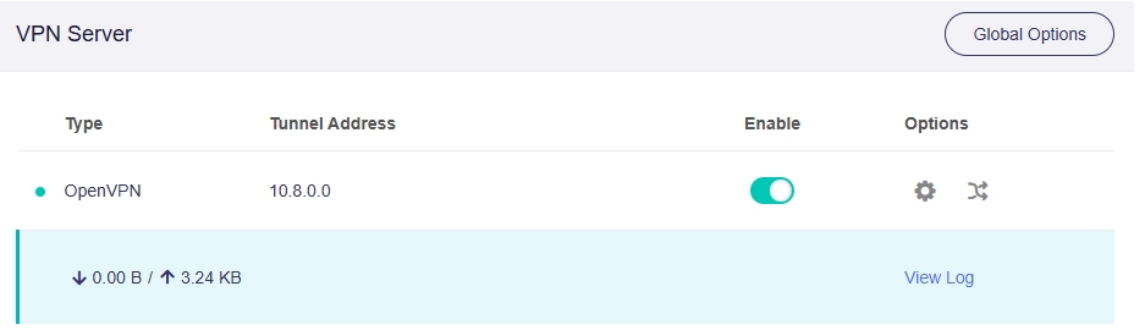
- **Certificate Only**: If selected, the router will automatically generate a server and client certificate keys and embed them in the configuration file. When you upload the configuration to the client, no additional credentials are required.
- **Username/Password Only**: If selected, the router will 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 as needed.

3. 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. **Note**: If your public IP changes frequently, enable DDNS before clicking Download. You can then use the DDNS domain as your server address.



4. Enable OpenVPN server.
   Go to the **VPN Dashboard**, toggle the switch to enable the OpenVPN server. It will start running as shown below.



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:

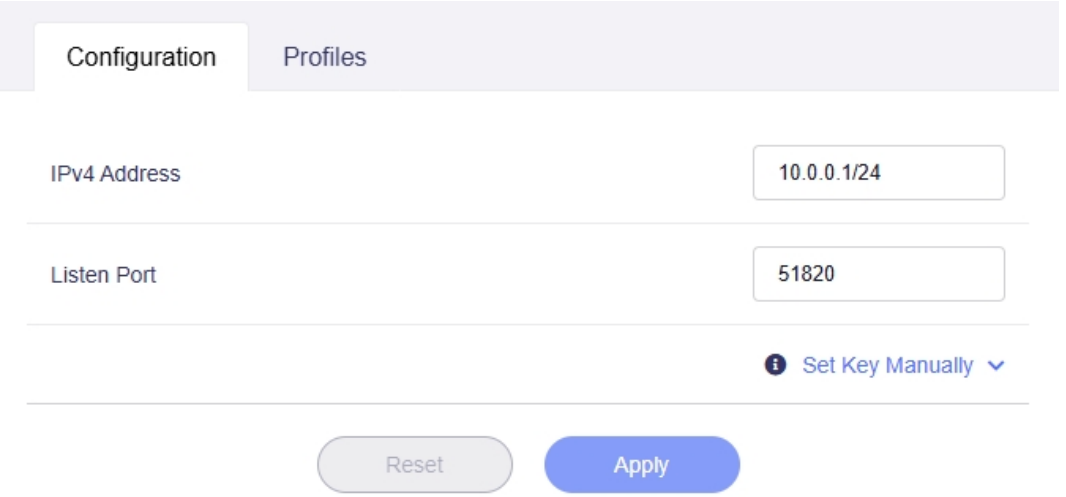
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.
   - If the above two methods don't work (e.g., if your network is behind CGNAT), you may try our SD-WAN solution AstroWarp.

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

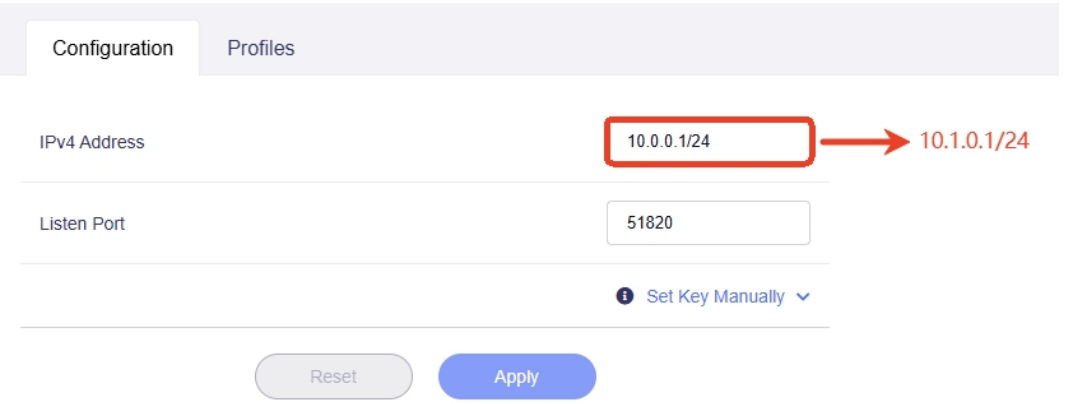
   - If your GL.iNet router is the primary router in your network, no port forwarding setup is required. Proceed to the next step.
   - If a primary router is already in use and your GL.iNet router is configured as a secondary router, you will need to configure port forwarding on the primary router.
  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

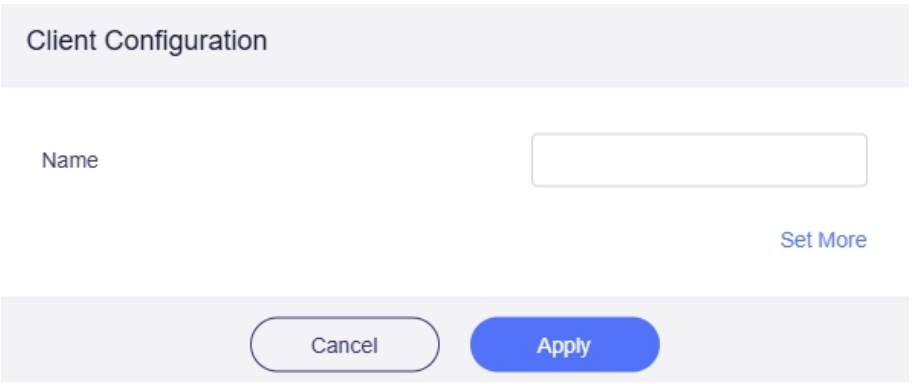


   If the IPv4 address conflicts with your upstream router's gateway, modify the IPv4 address to another one (e.g., **10.1.0.1/24**) and click **Apply**. Ensure the "/24" CIDR notation is included to avoid connectivity issues.



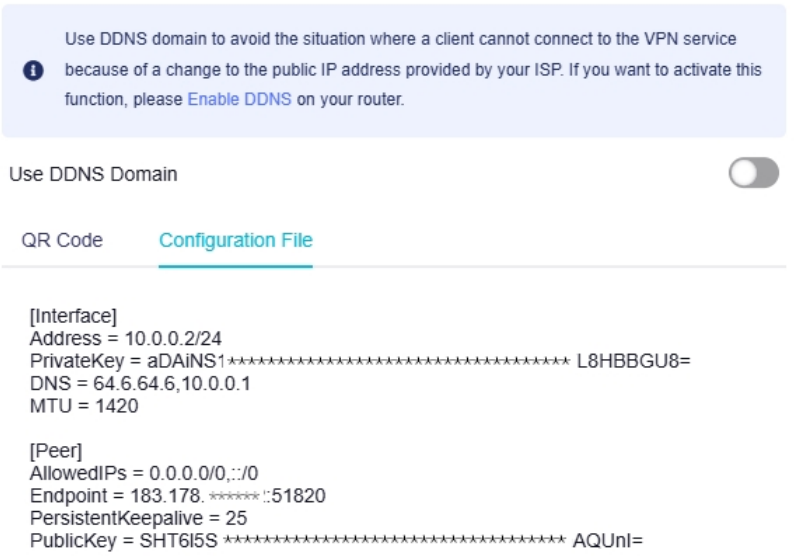
3. Add a profile.
   Switch to **Profiles** tab, click the **Add** button to generate a profile for your device.

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



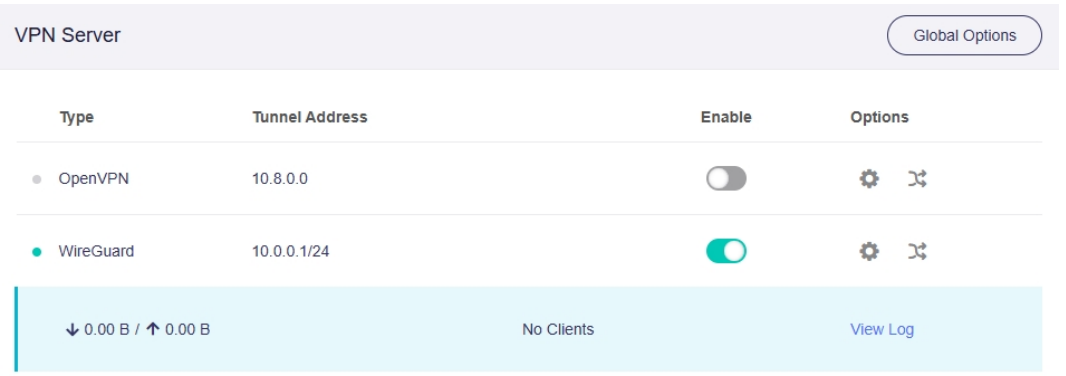
4. After adding a profile, the router will generate a configuration file in three formats: QR code, .conf file, and plain text. Choose your preferred format. **Note**: If your public IP address changes frequently, enable DDNS before downloading the file.
   - **QR code**: Suitable for devices (e.g., 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.
   - **.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.

- **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.



5. Enable WireGuard server.

   Go to the **VPN Dashboard**, toggle the switch to enable your WireGuard server. It will start running as shown below.



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.

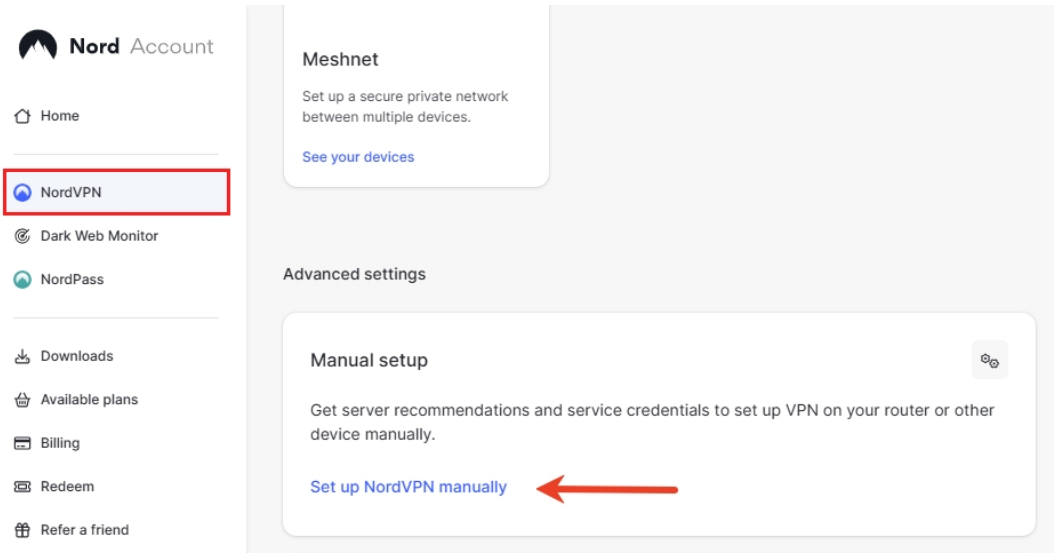
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to this link or contact their support.

10.1.2 Set Up NordVPN

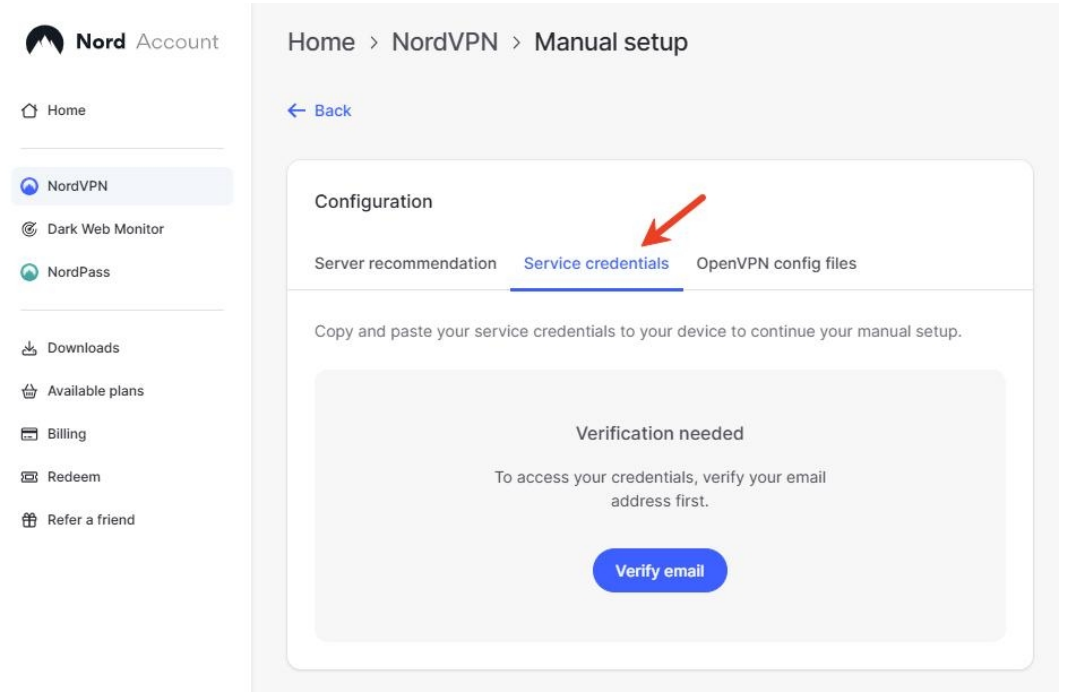
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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

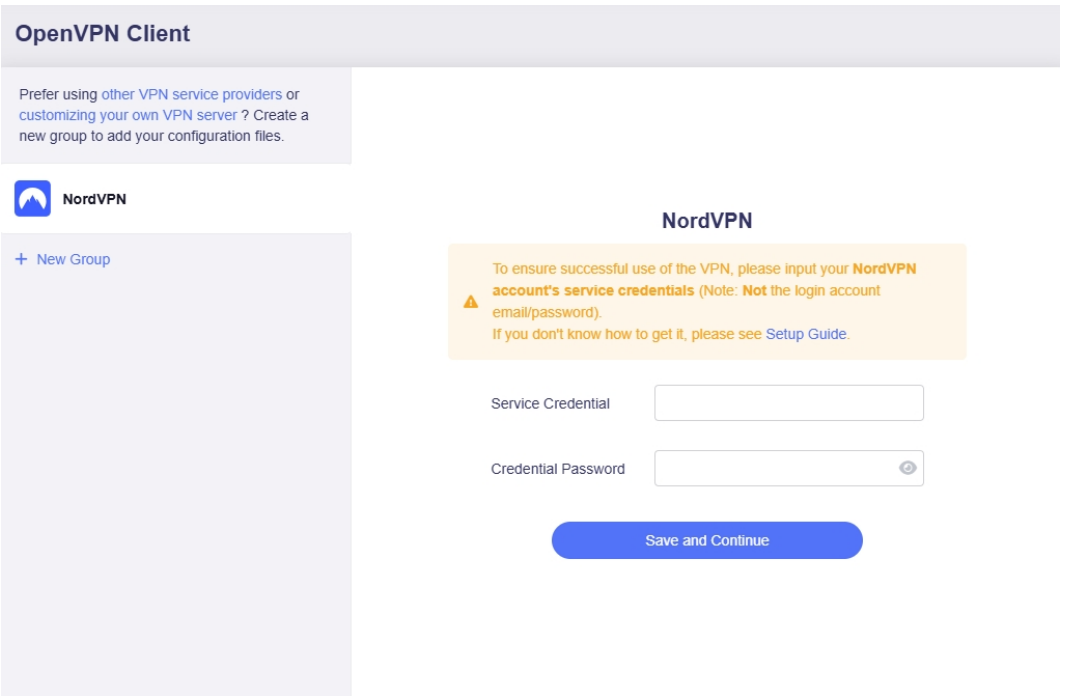
1. Log in to your NordVPN web account here.
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



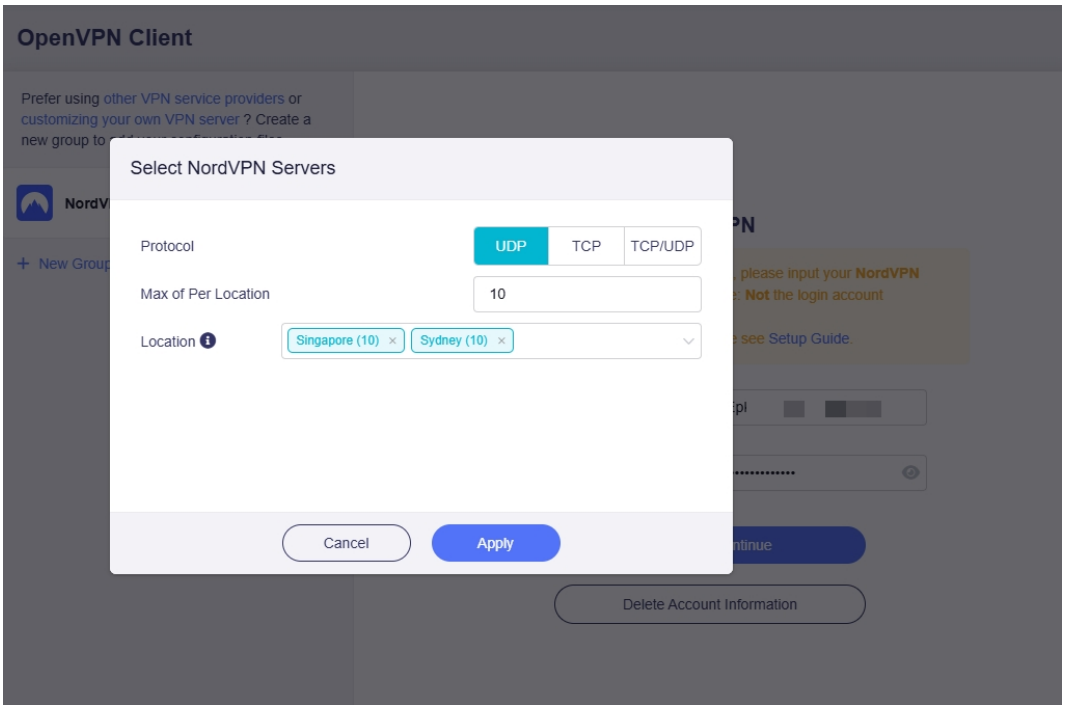
You will find the **service credentials**. Copy them for later use.



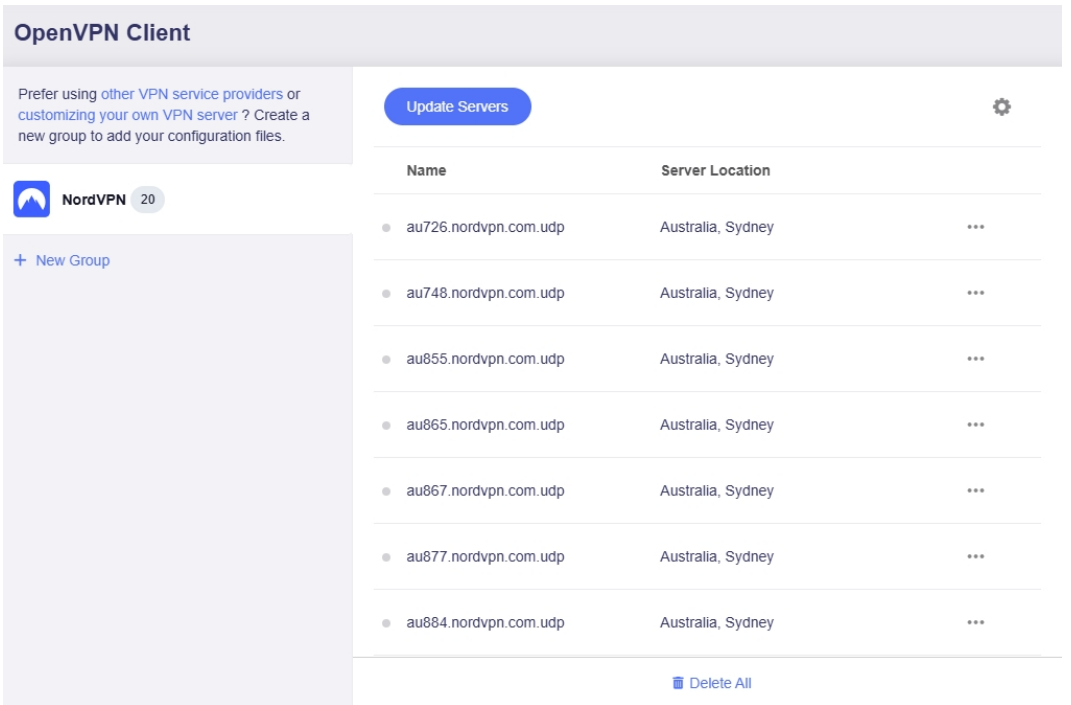
3. Log in to your router's web admin panel and navigate to **VPN** > **OpenVPN Client** > **NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



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

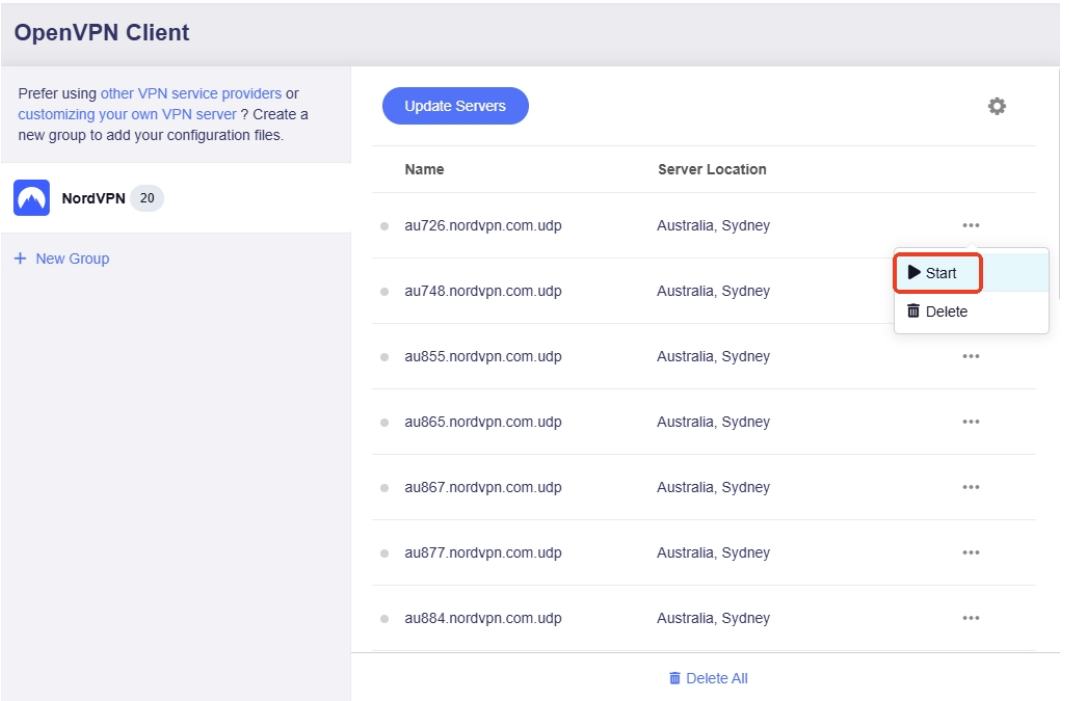


It will download configuration files.

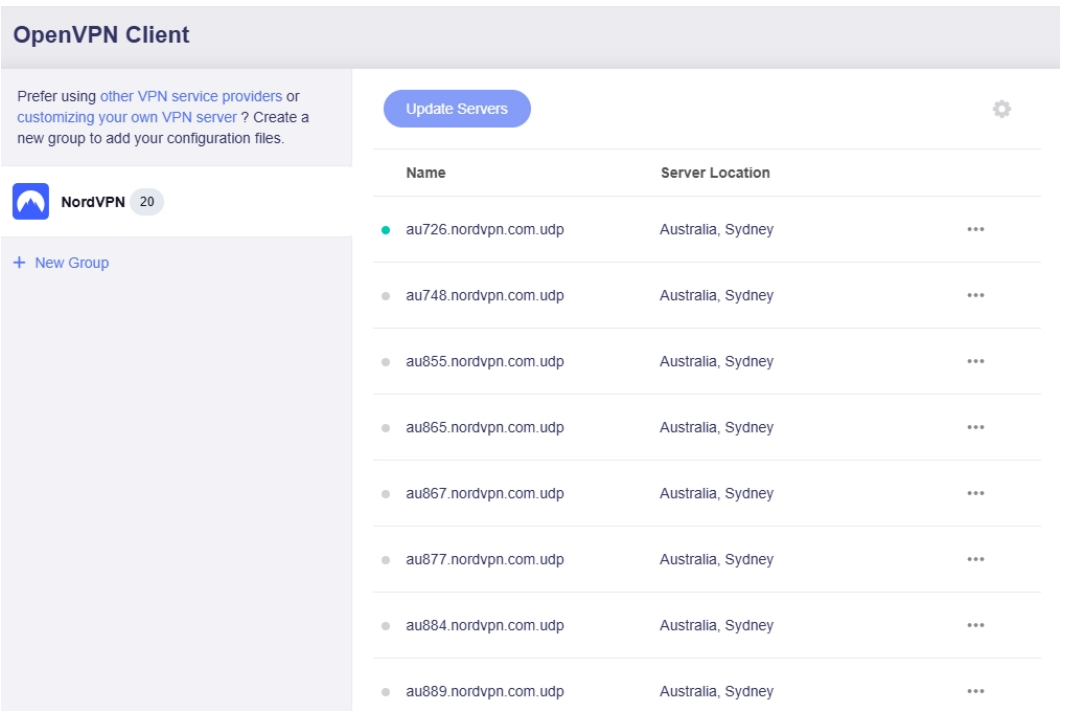


5. Start a connection.

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



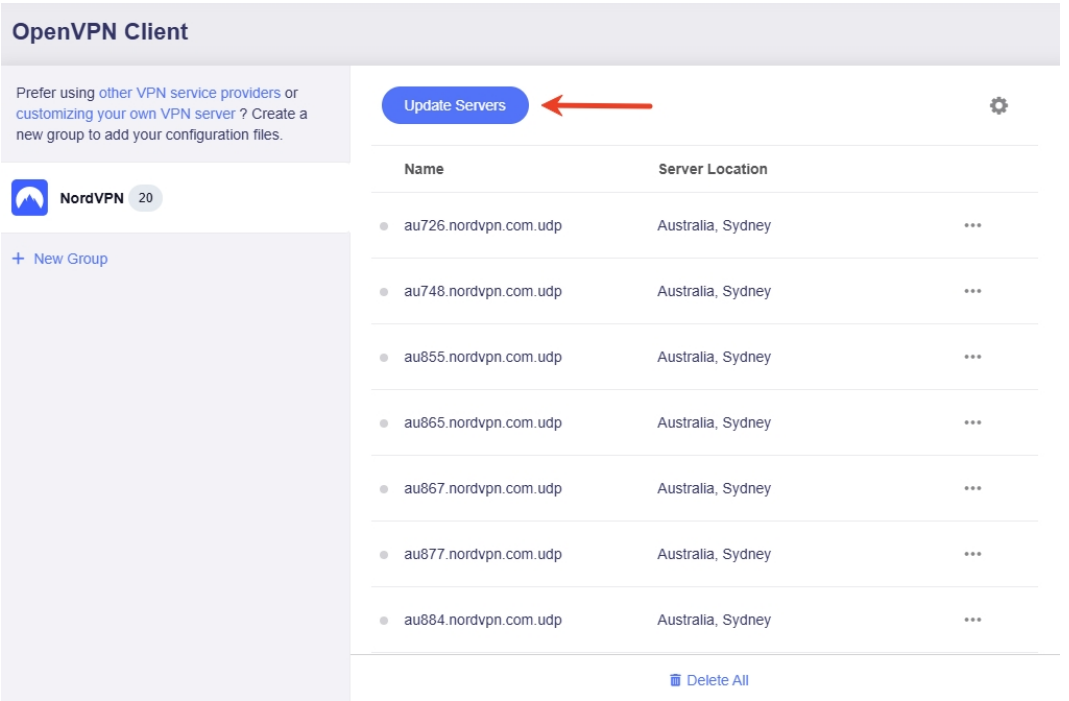
6. Once connected, a green dot will appear next to the configuration file.



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

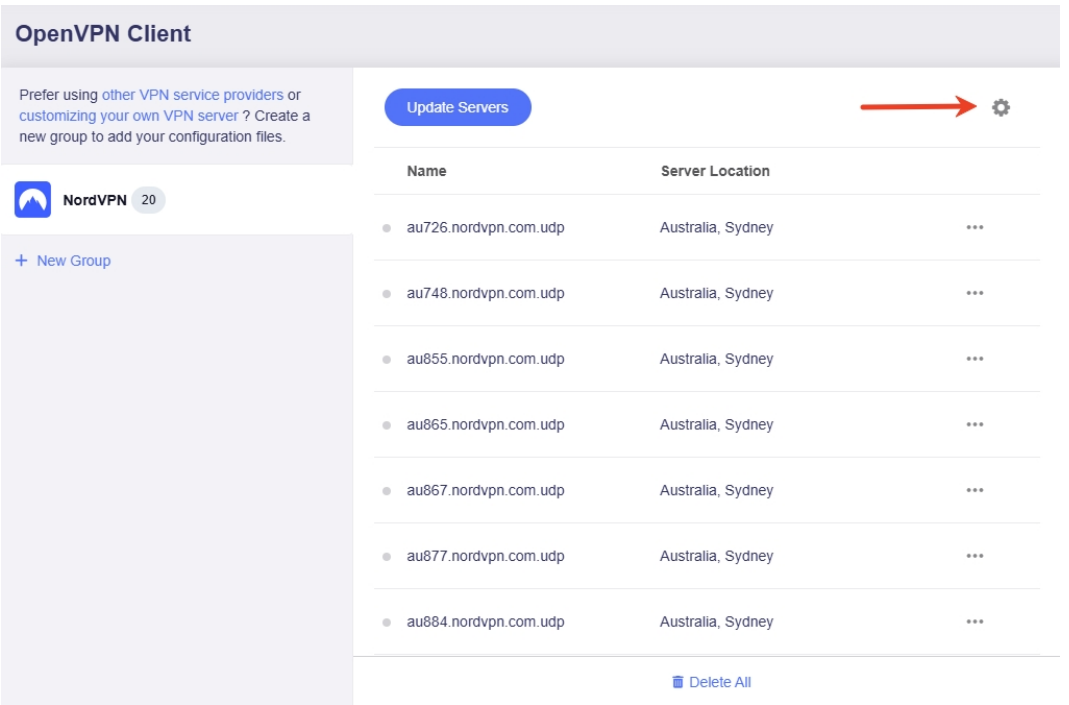
7. Update servers.

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



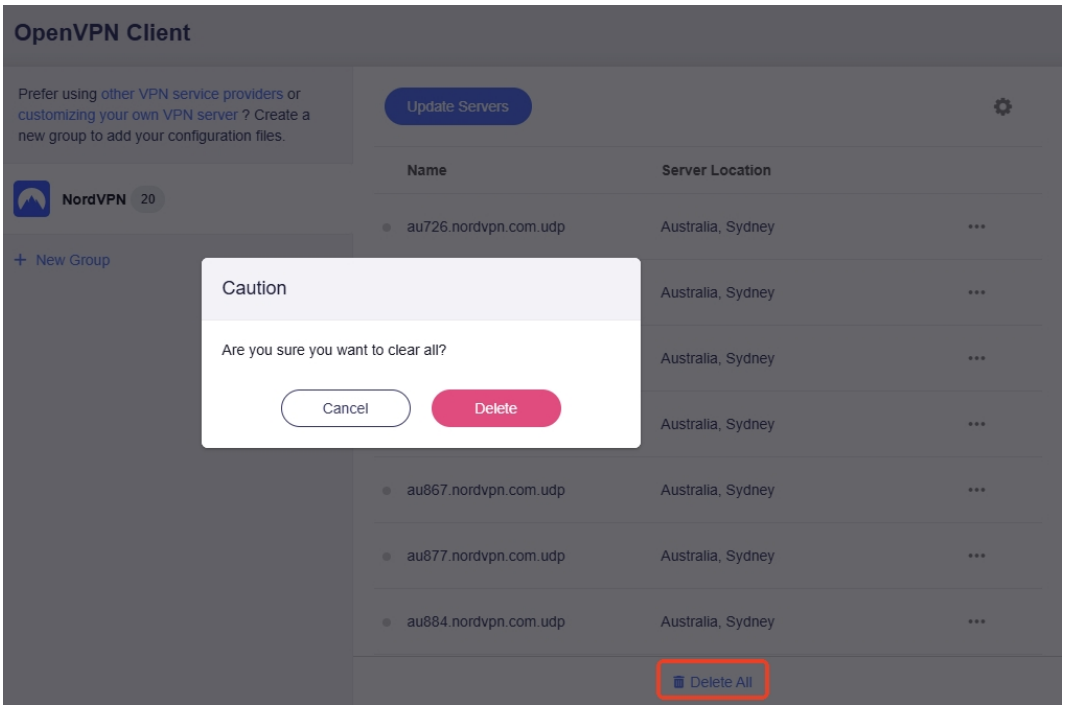
8. Edit credentials.

   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.

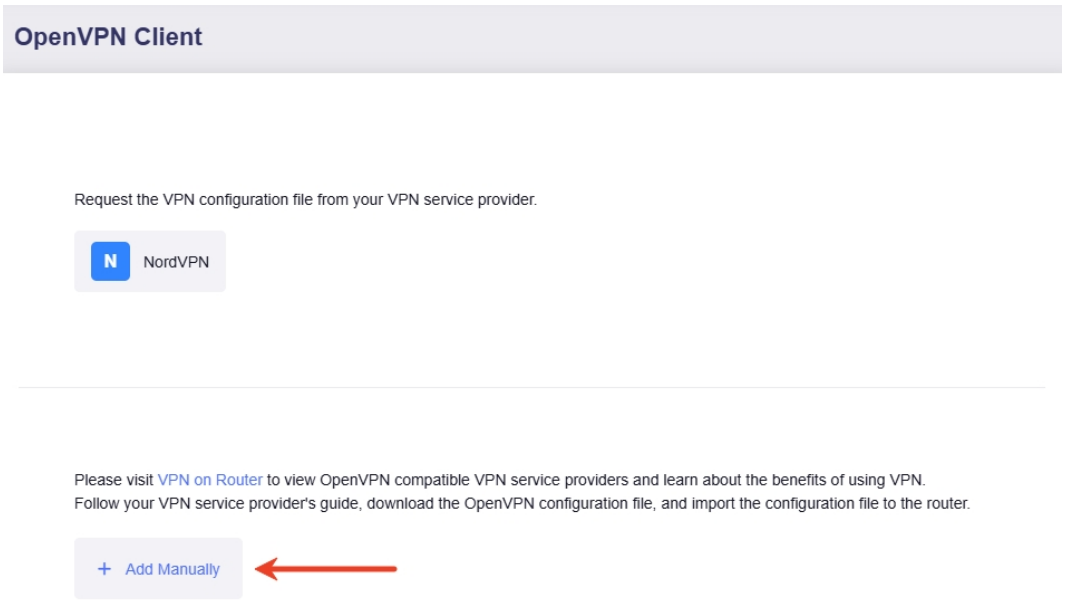

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp
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)

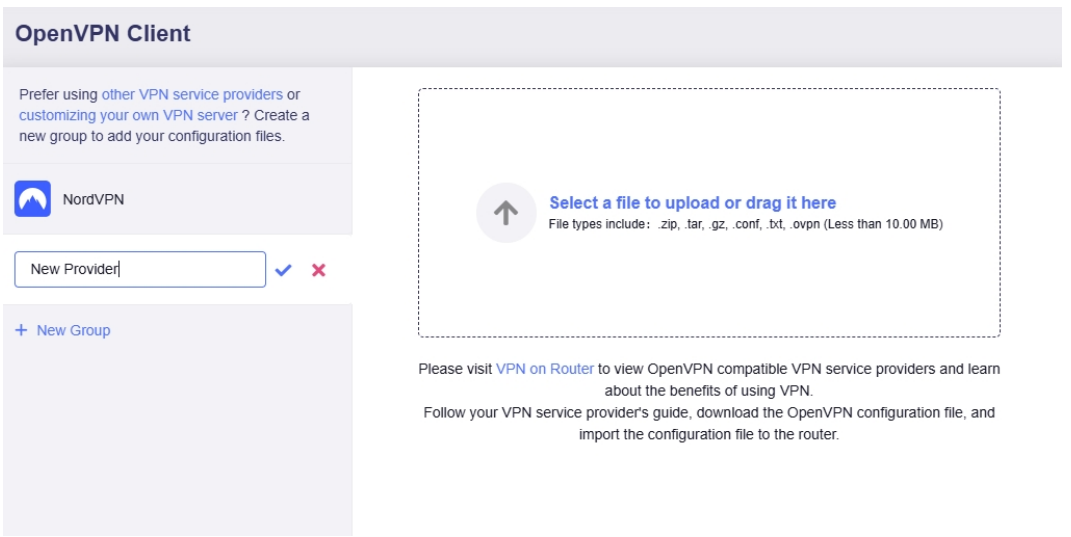
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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

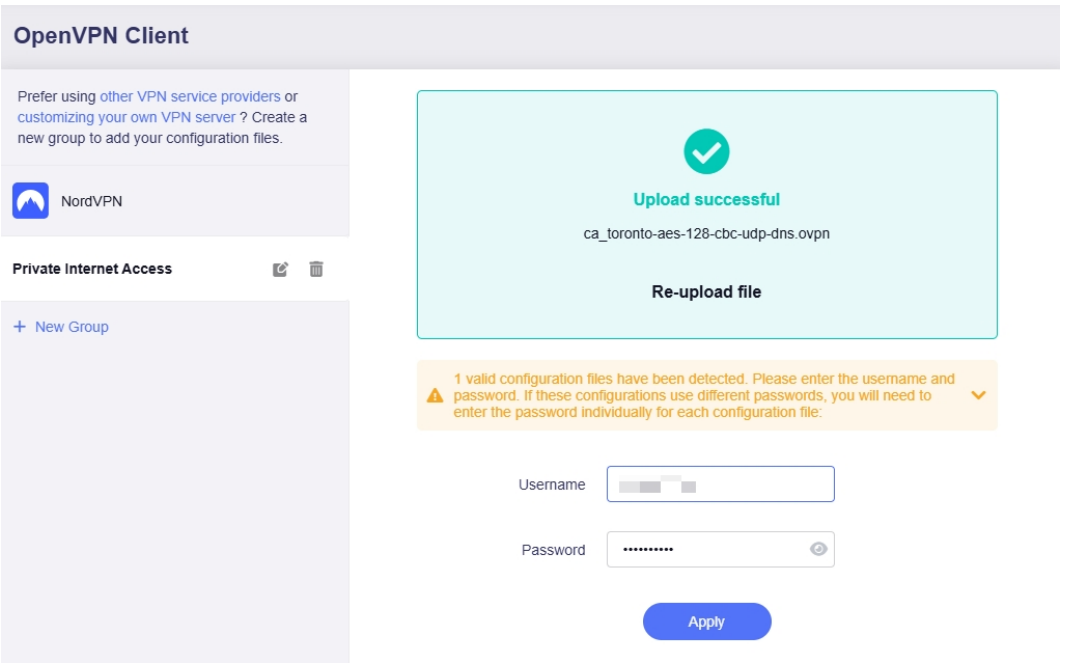
1. Download a configuration file from Private Internet Access official website.
2. Log in to your router's web admin panel, navigate to **VPN** > **OpenVPN Client**, and click **Add Manually**.



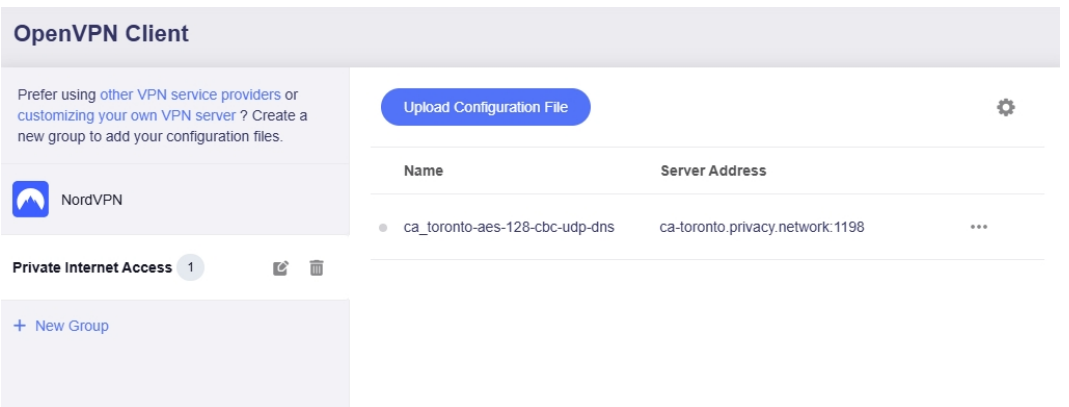
3. It will create a group on the left sidebar. Set a descriptive name for the group.



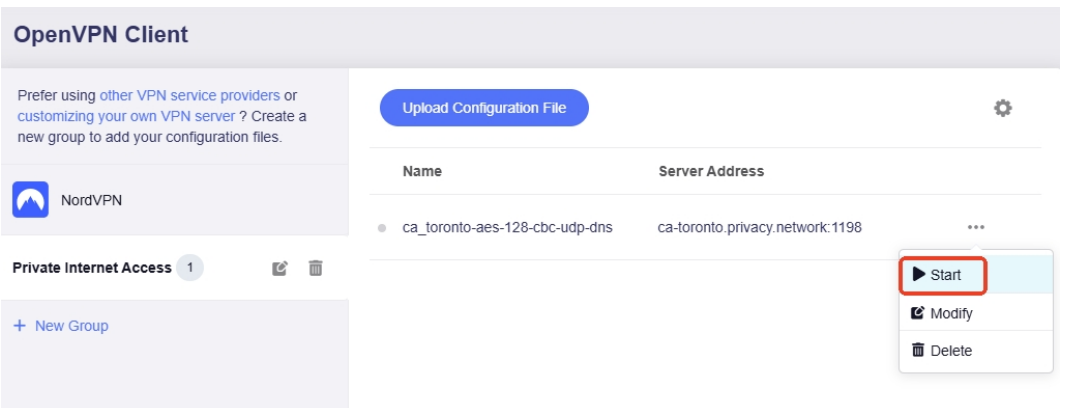
4. Upload your OpenVPN configuration file. Input the credentials if required, then click **Apply**.



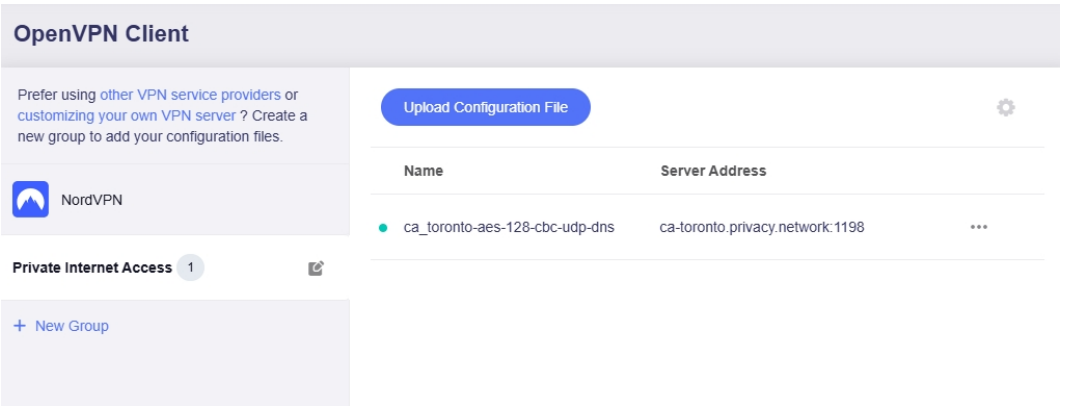
You will see the configuration file uploaded.



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.

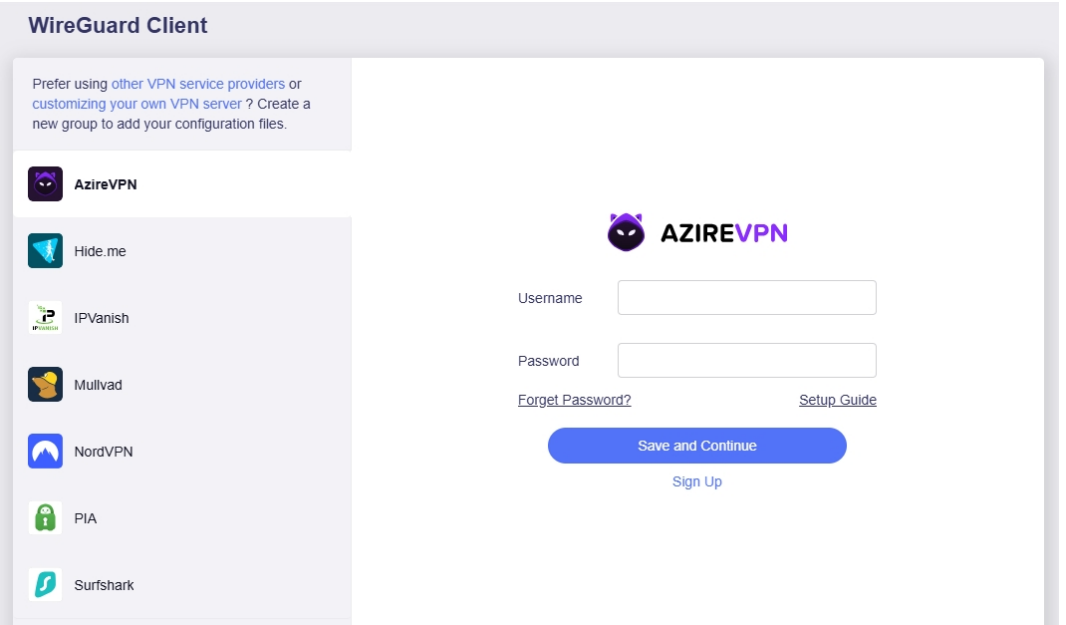
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

- Set Up AzireVPN
- Set Up Hide.me
- Set Up IPVanish
- Set Up Mullvad
- Set Up NordVPN
- Set Up PIA (Private Internet Access)
- Set Up Surfshark
- Set Up WireGuard Client Manually (for other providers)

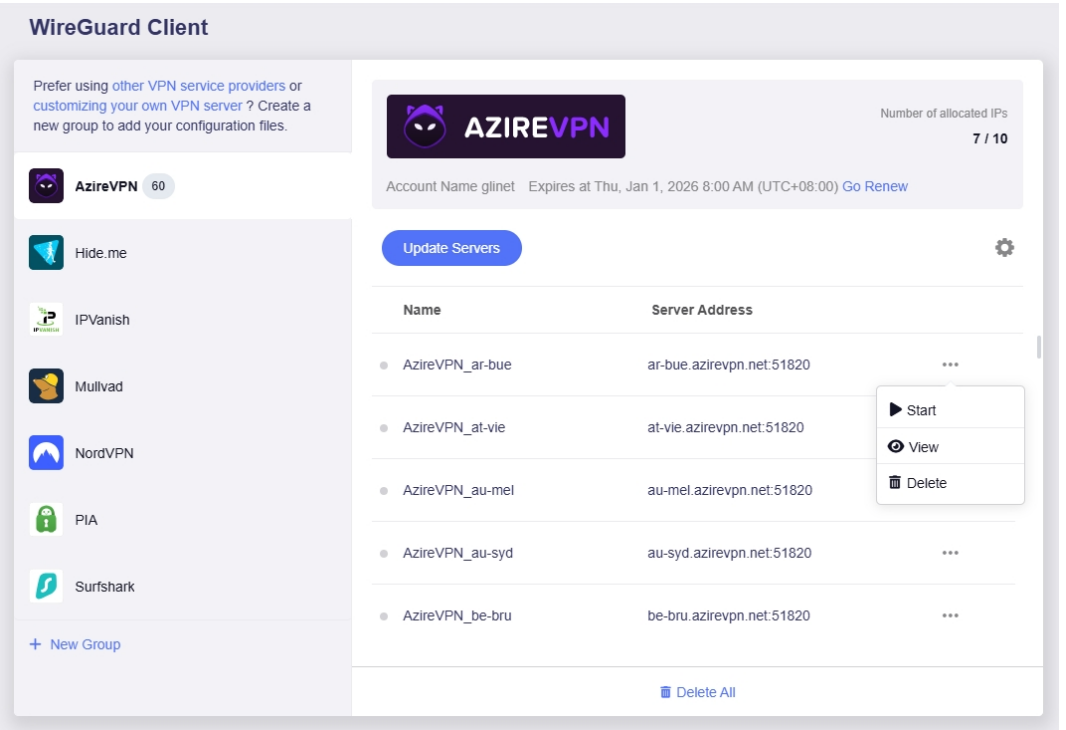
10.2.2 Set Up AzireVPN

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

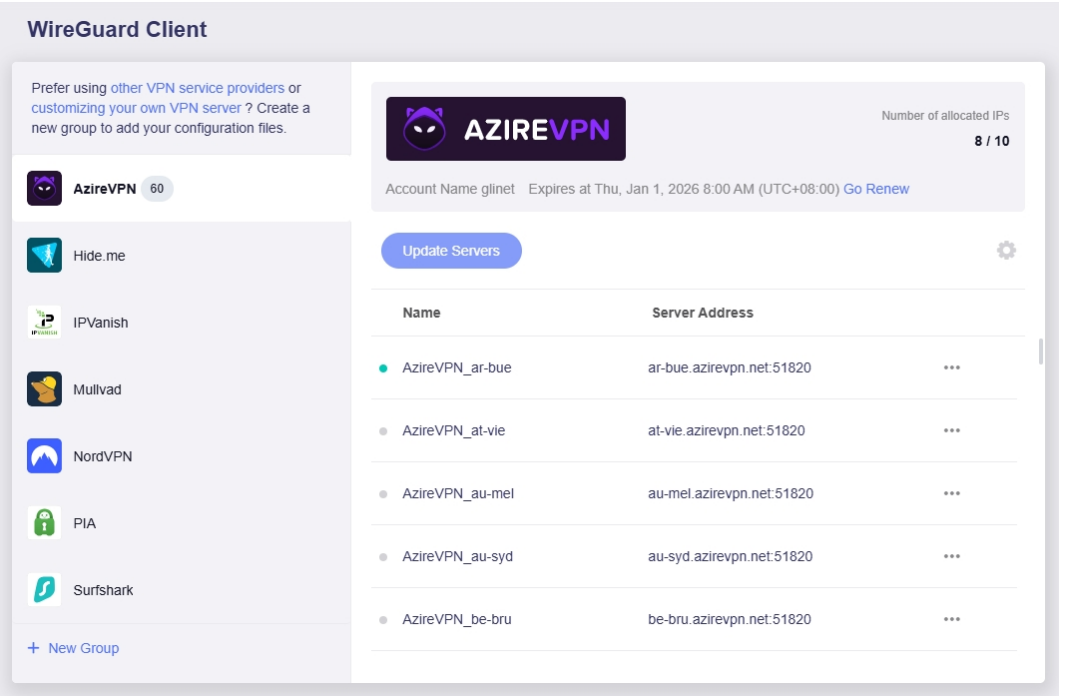
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **AzireVPN**.
2. Input Username and Password, then click **Save and Continue**. It will generate configuration files for each server.



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



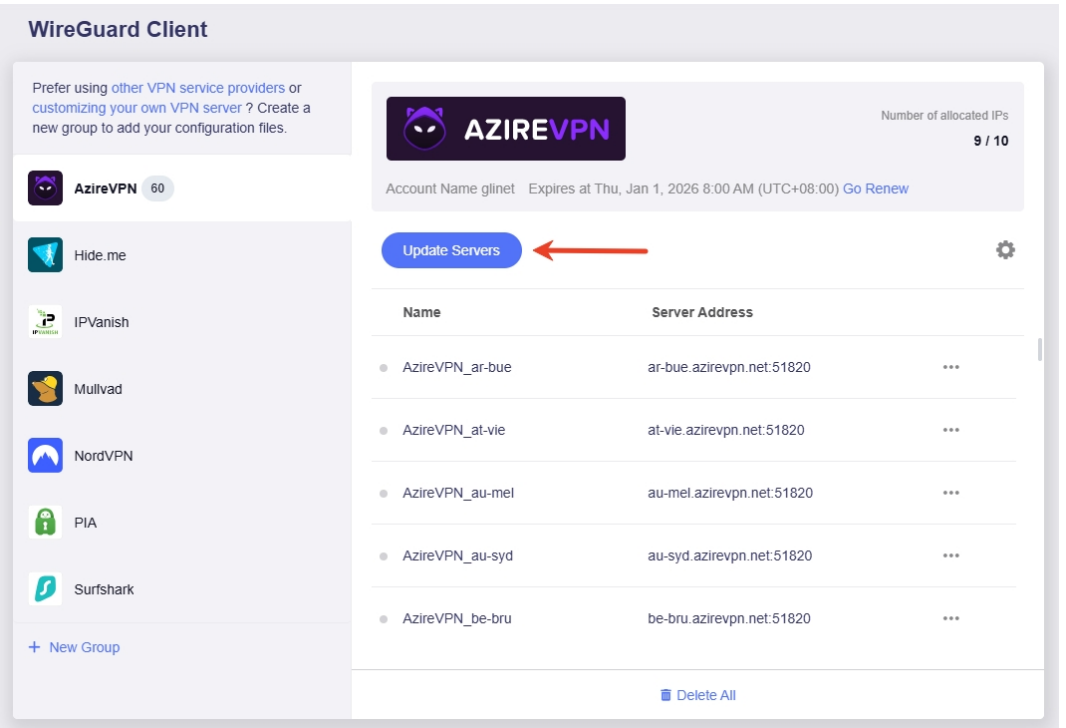
4. Once connected, a green dot will appear next to the configuration file.



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

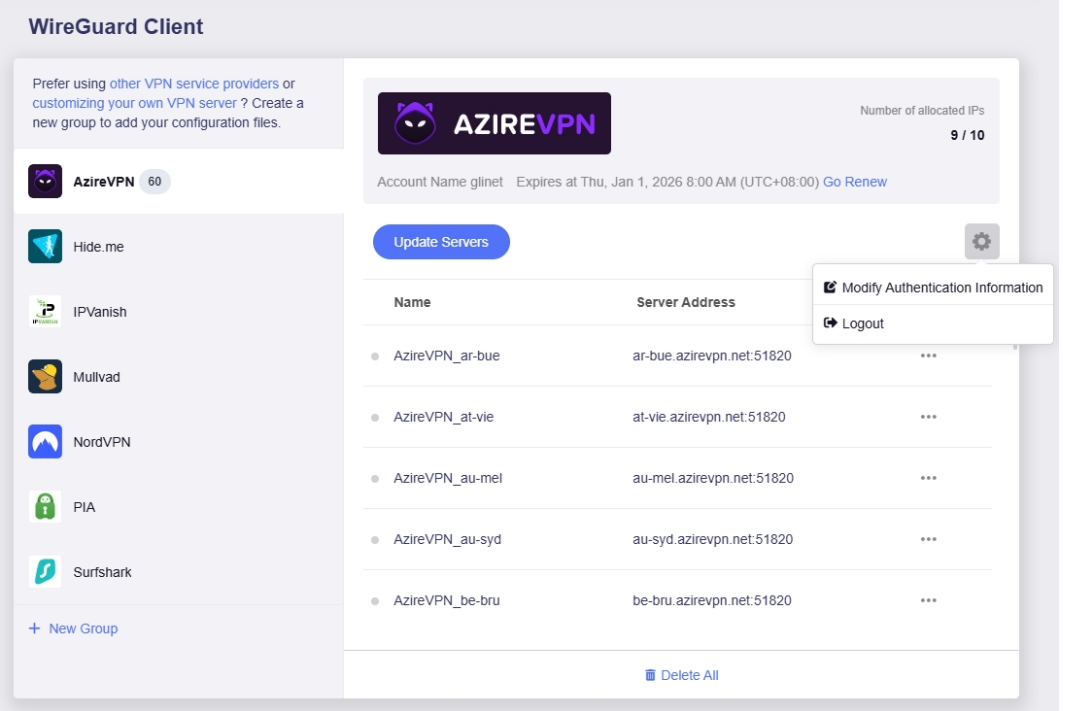
5. Update servers.

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



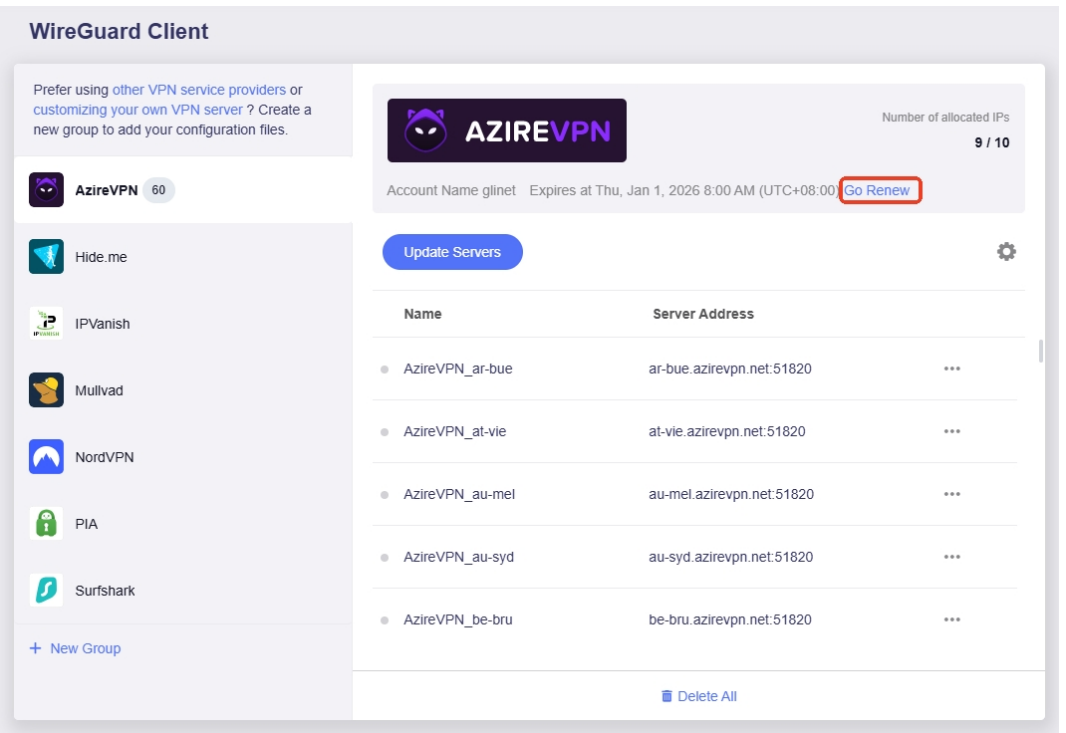
6. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



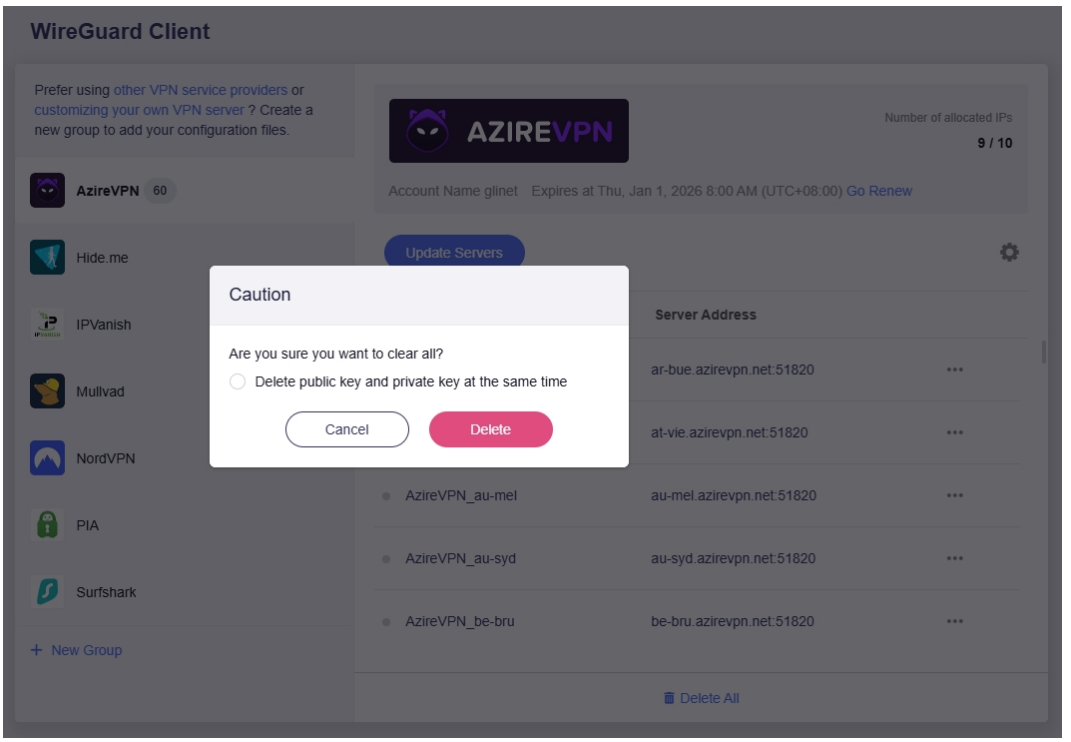
7. Go renew.

   If you click **Go Renew**, you will be re-directed to the official website to renew your subscription.



8. Delete all files.

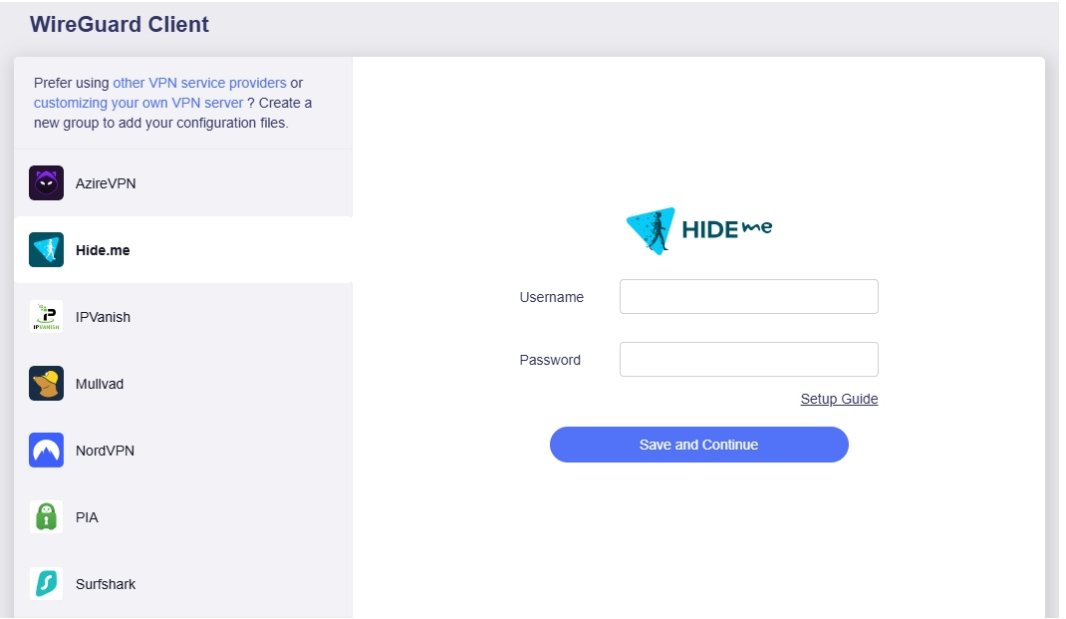
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



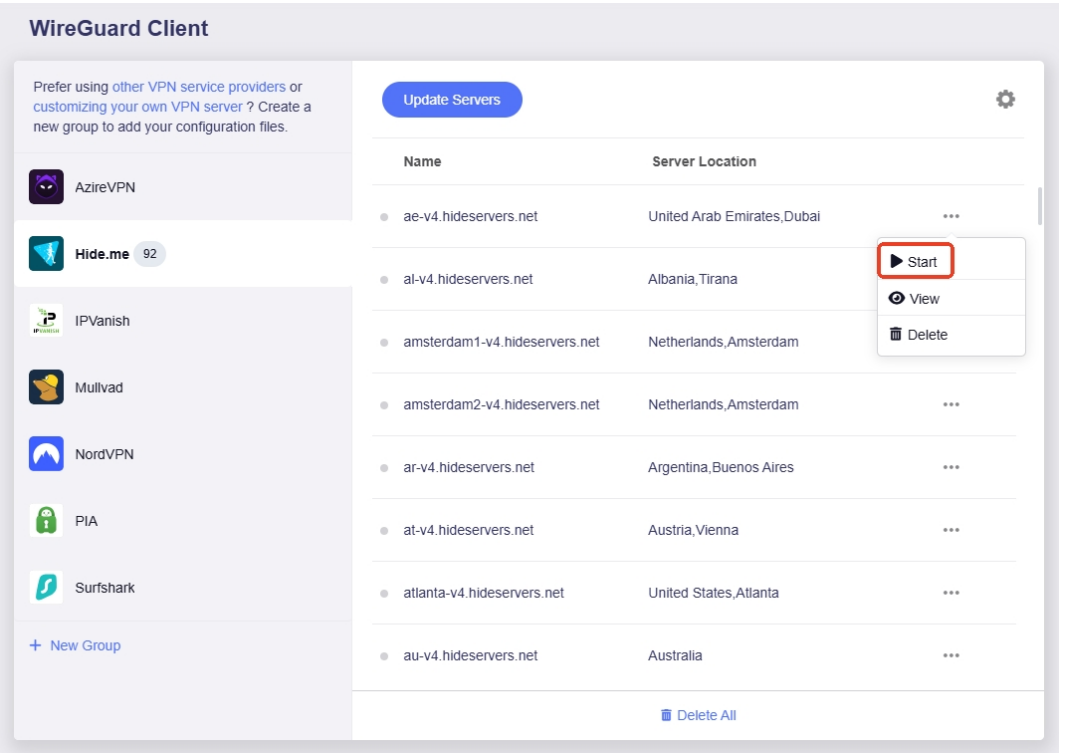
10.2.3 Set Up Hide.me

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

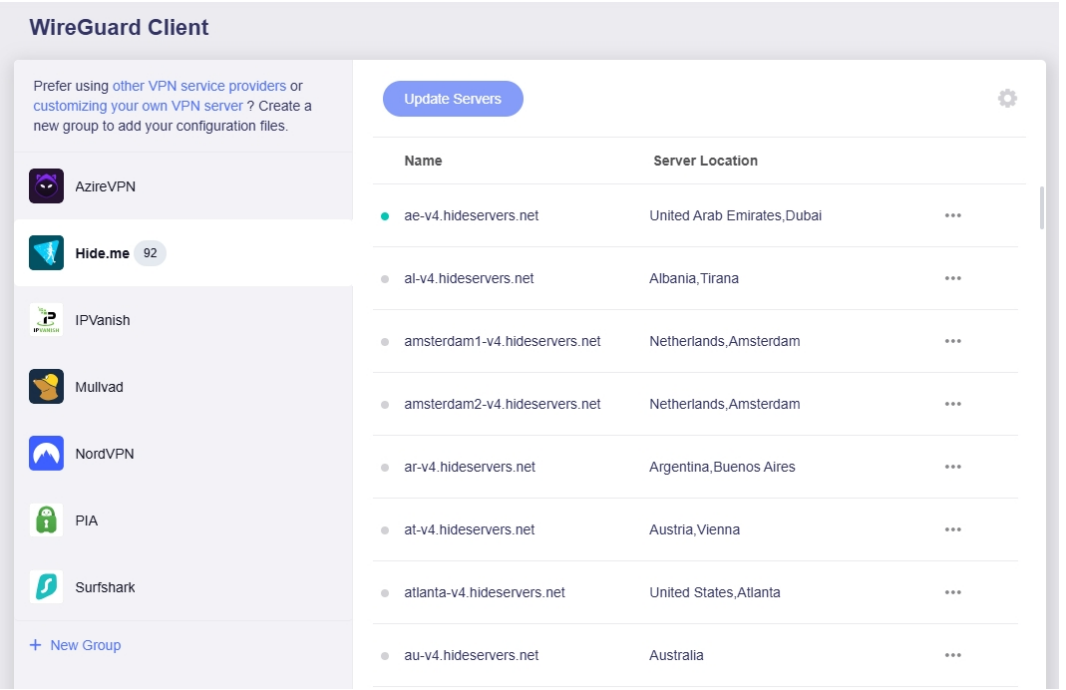
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Hide.me**.
2. Input Username and Password, then click **Save and Continue**. It will generate configuration files for each server.



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



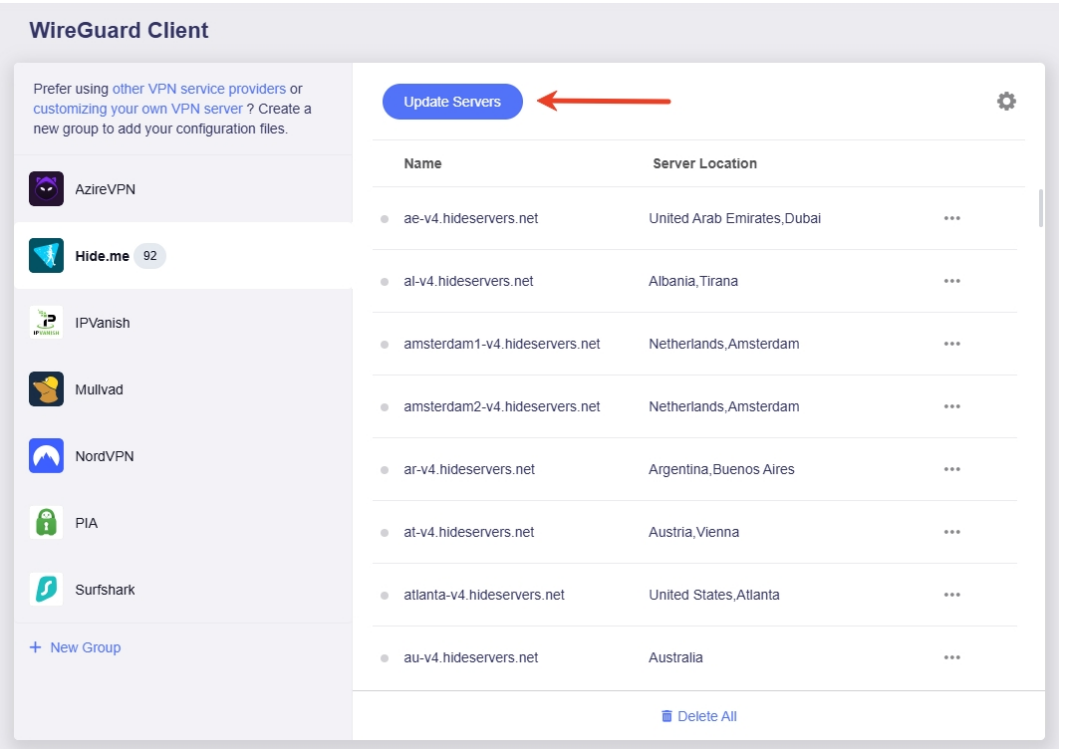
4. Once connected, a green dot will appear next to the configuration file.



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

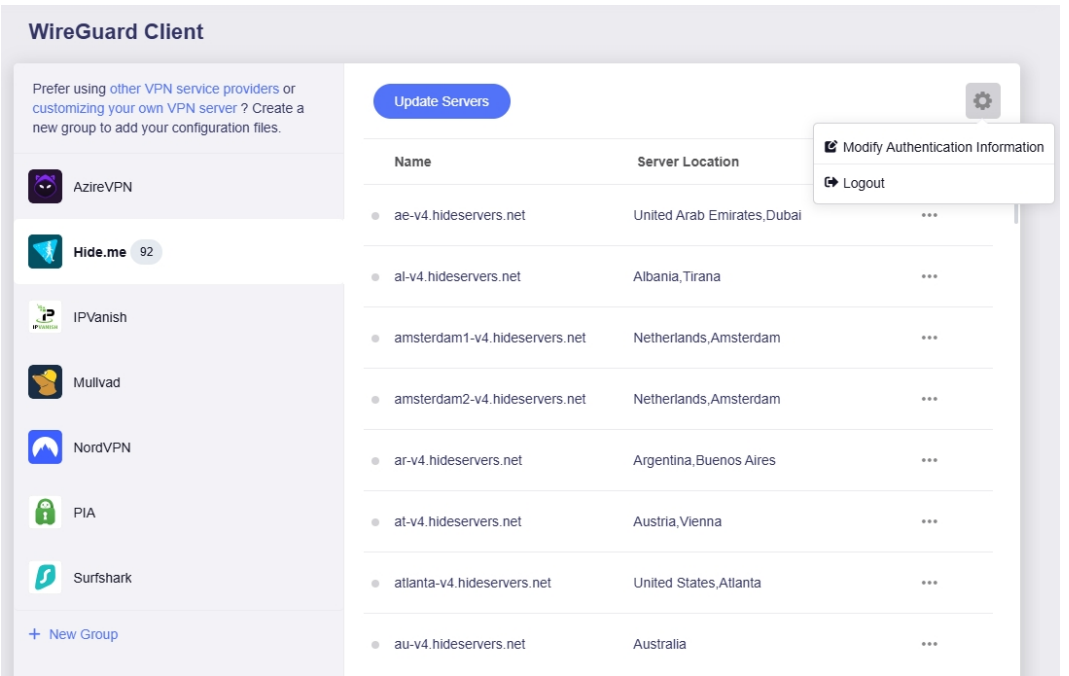
5. Update servers.

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



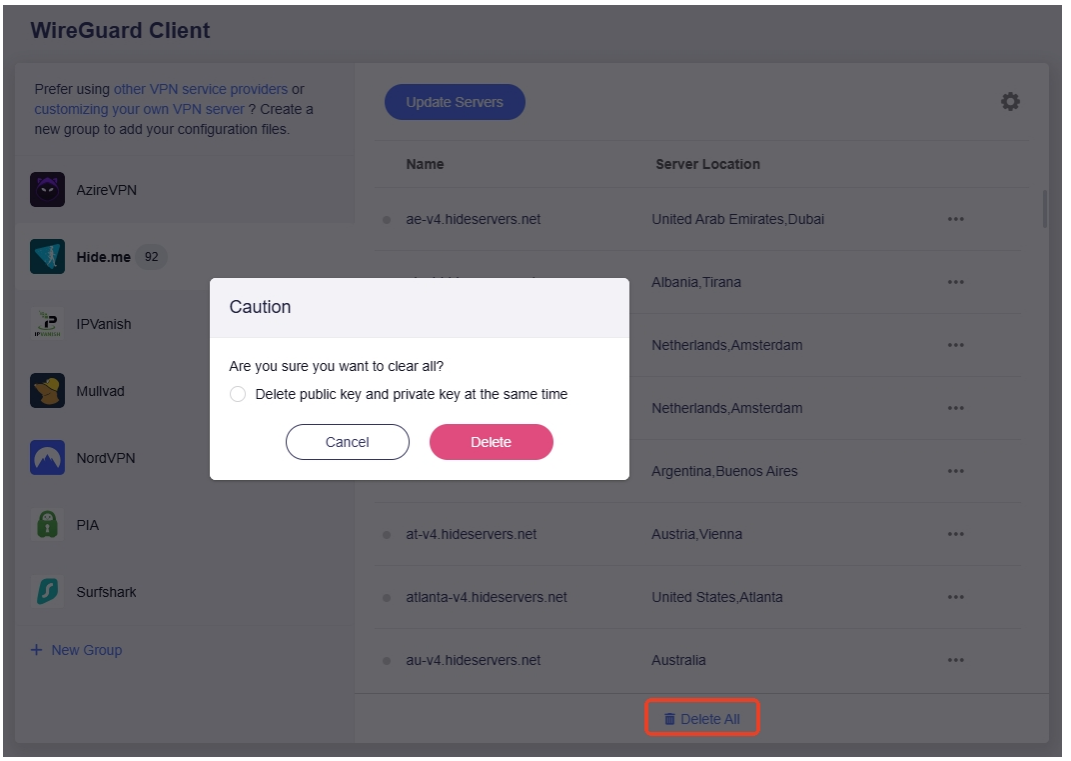
6. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



7. Delete all files.

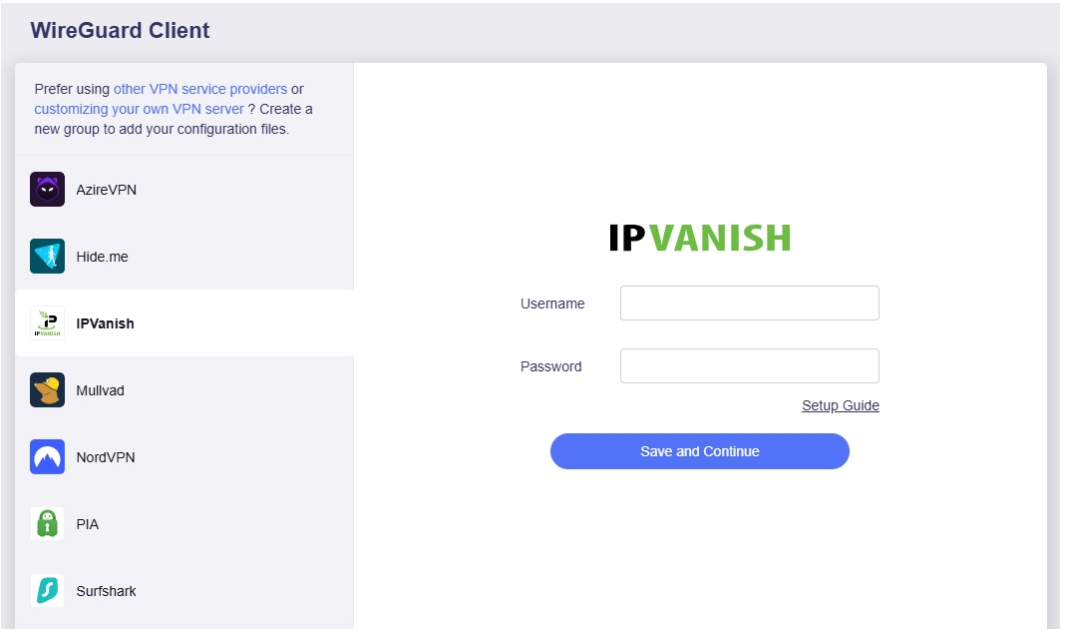
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



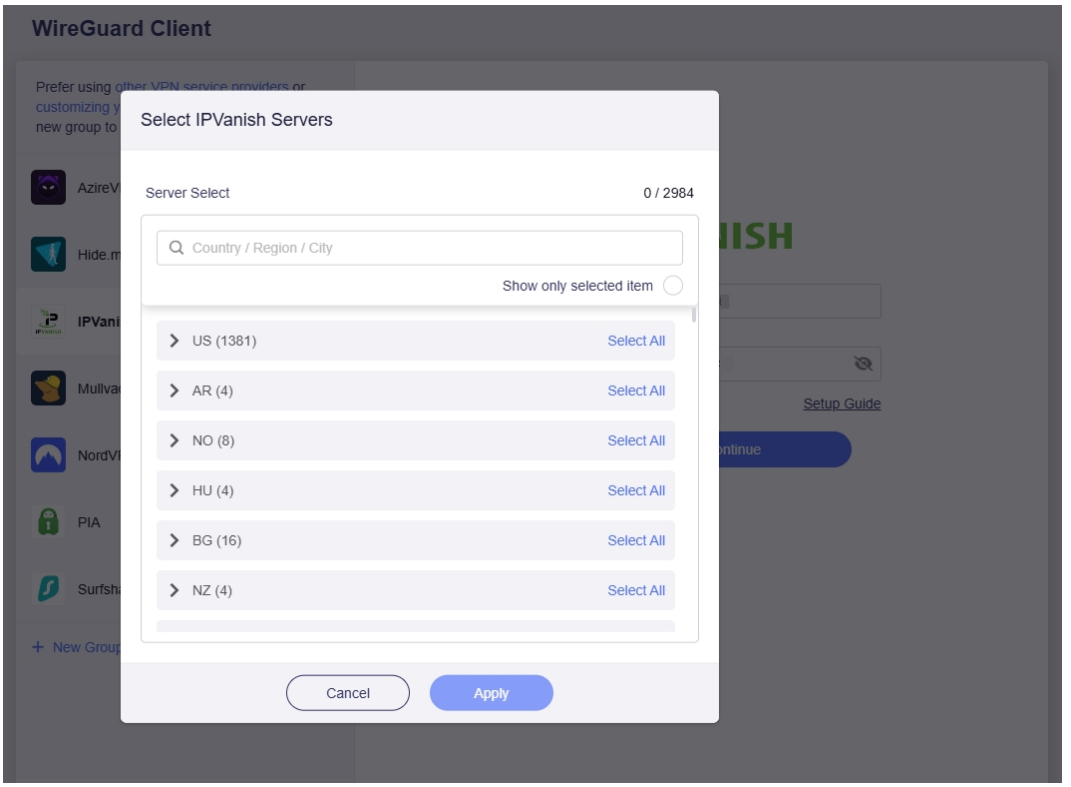
10.2.4 Set Up IPVanish

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

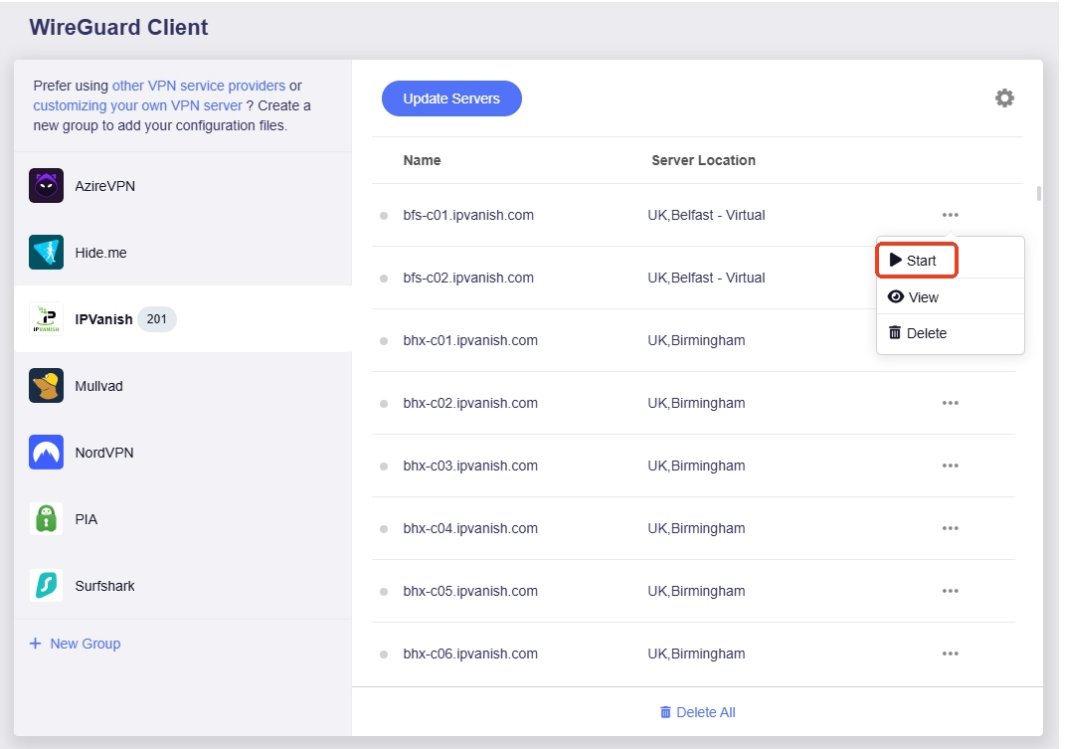
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **IPVanish**.
2. Input Username and Password, then click **Save and Continue**.



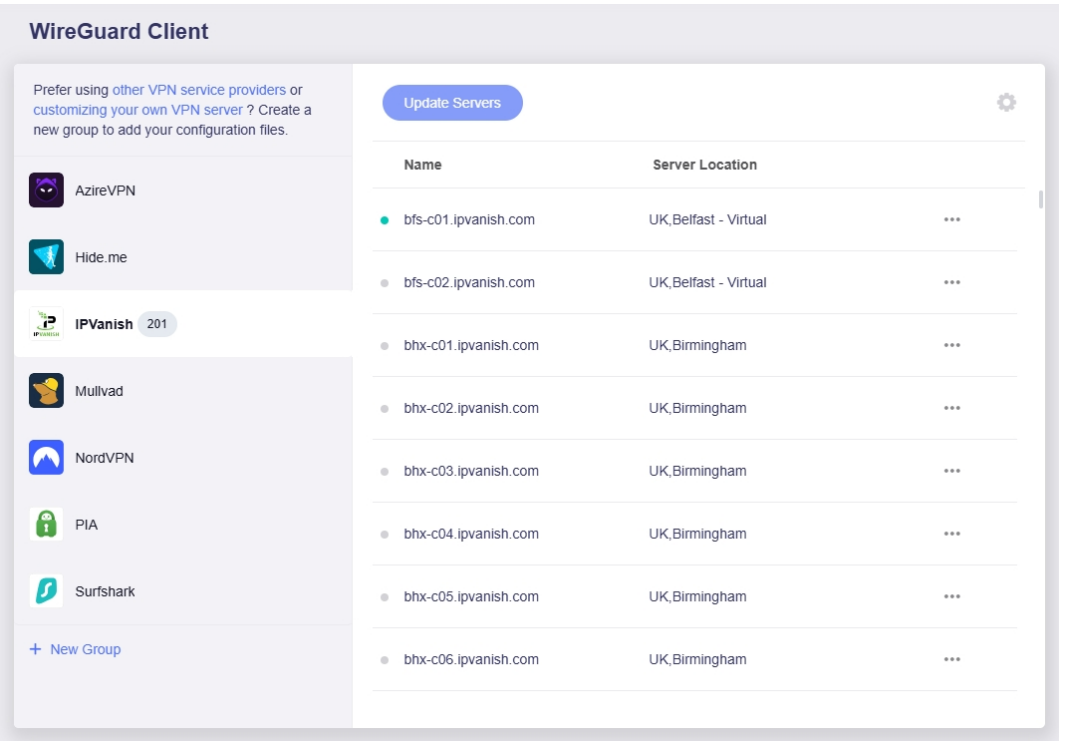
3. Select the server(s) you want to connect to, and click **Apply**.



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



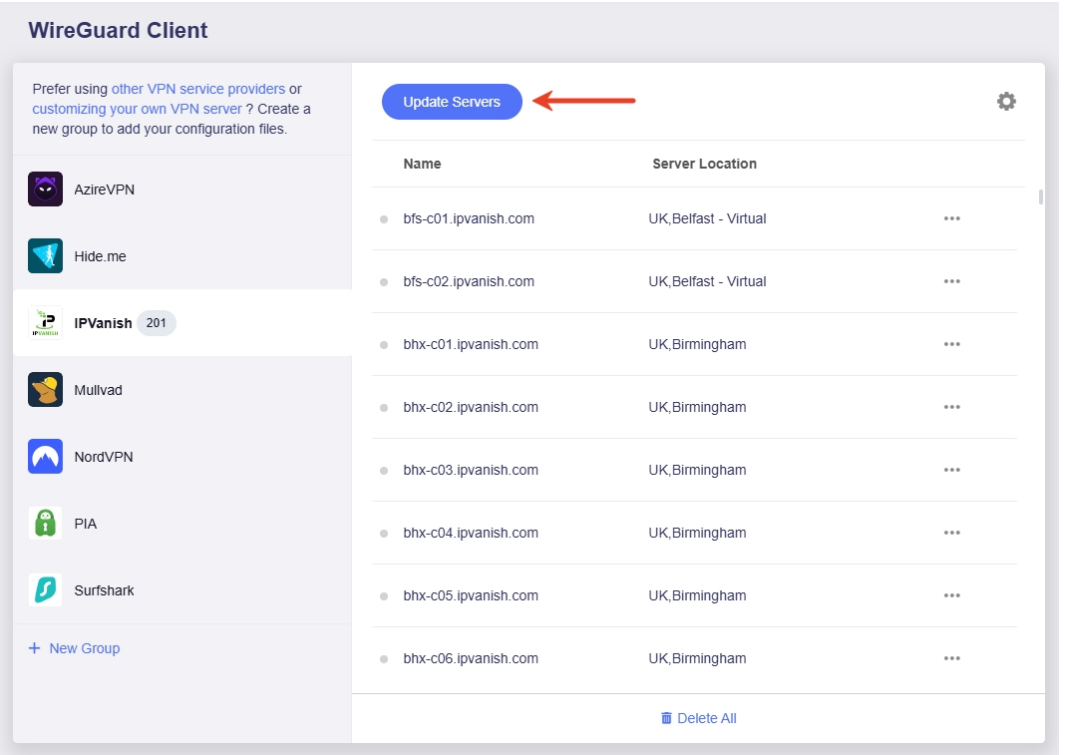
5. Once connected, a green dot will appear next to the configuration file.



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

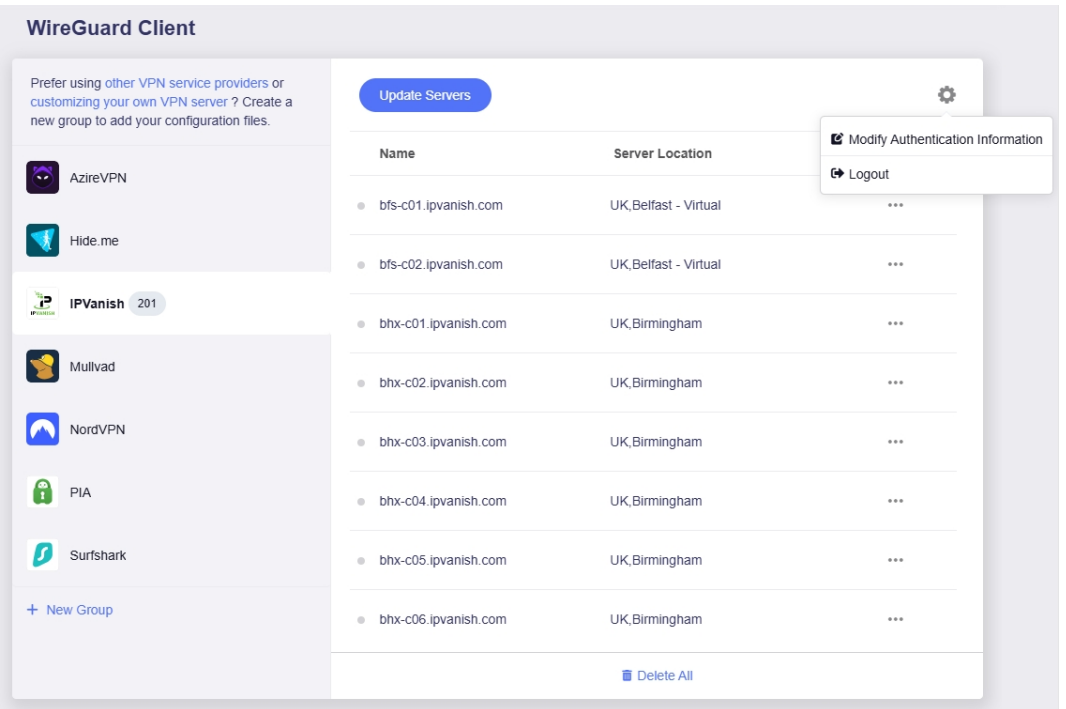
6. Update servers.

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



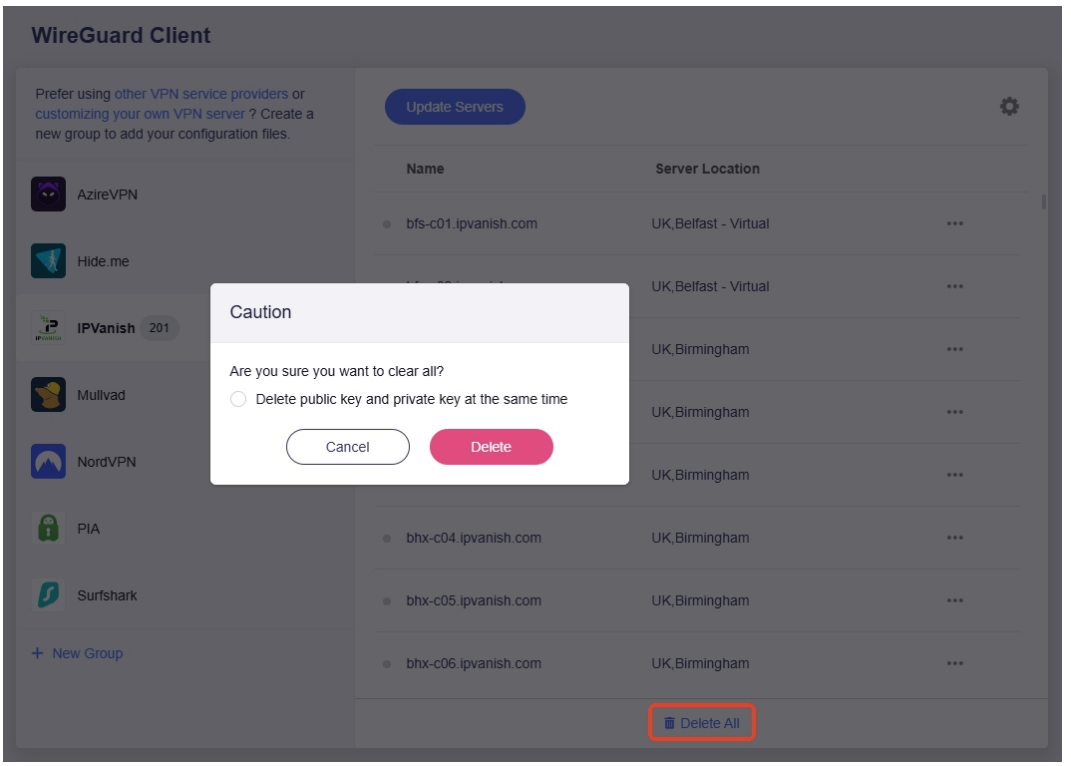
7. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



8. Delete all files.

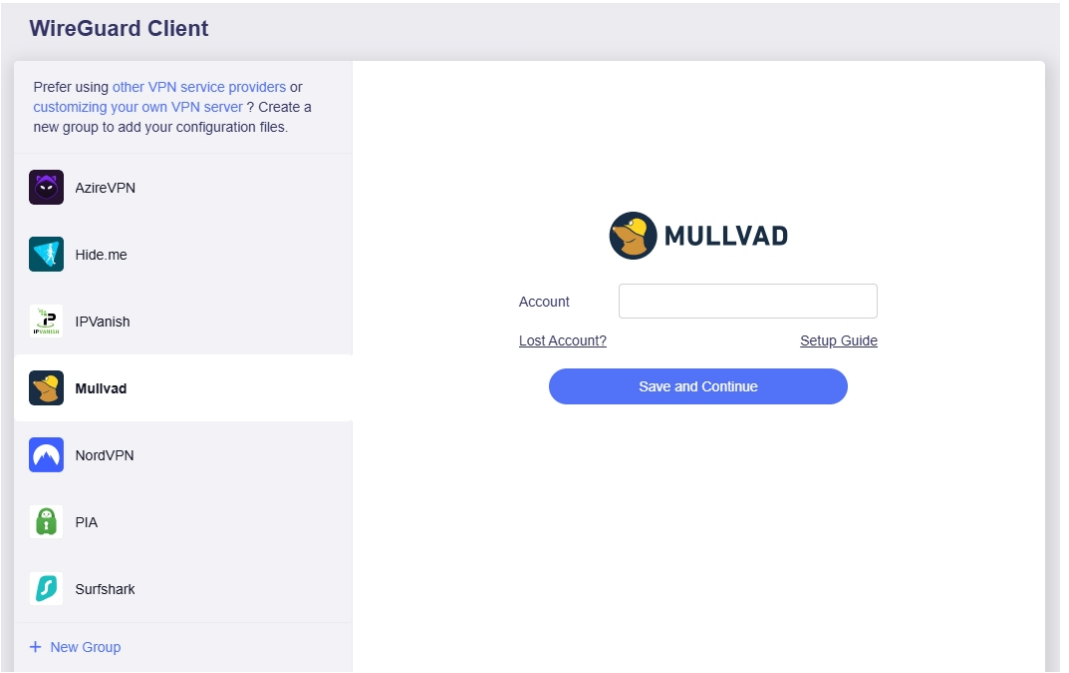
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



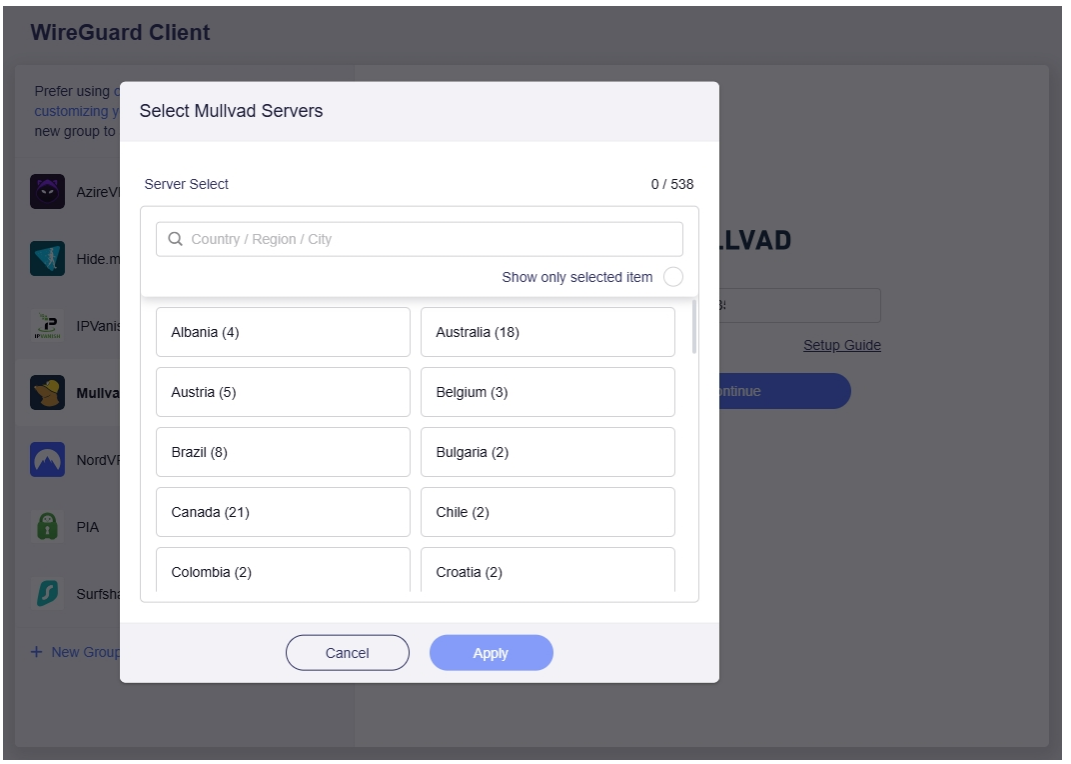
10.2.5 Set Up Mullvad

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

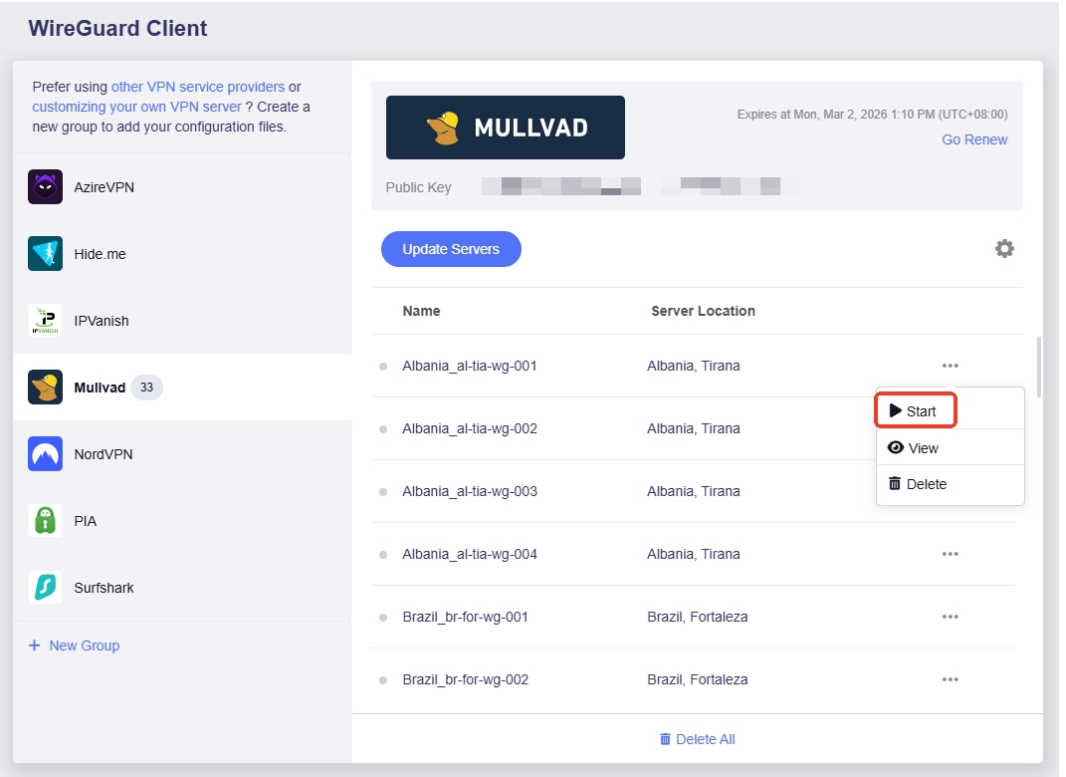
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Mullvad**.
2. Input Username and Password, then click **Save and Continue**.



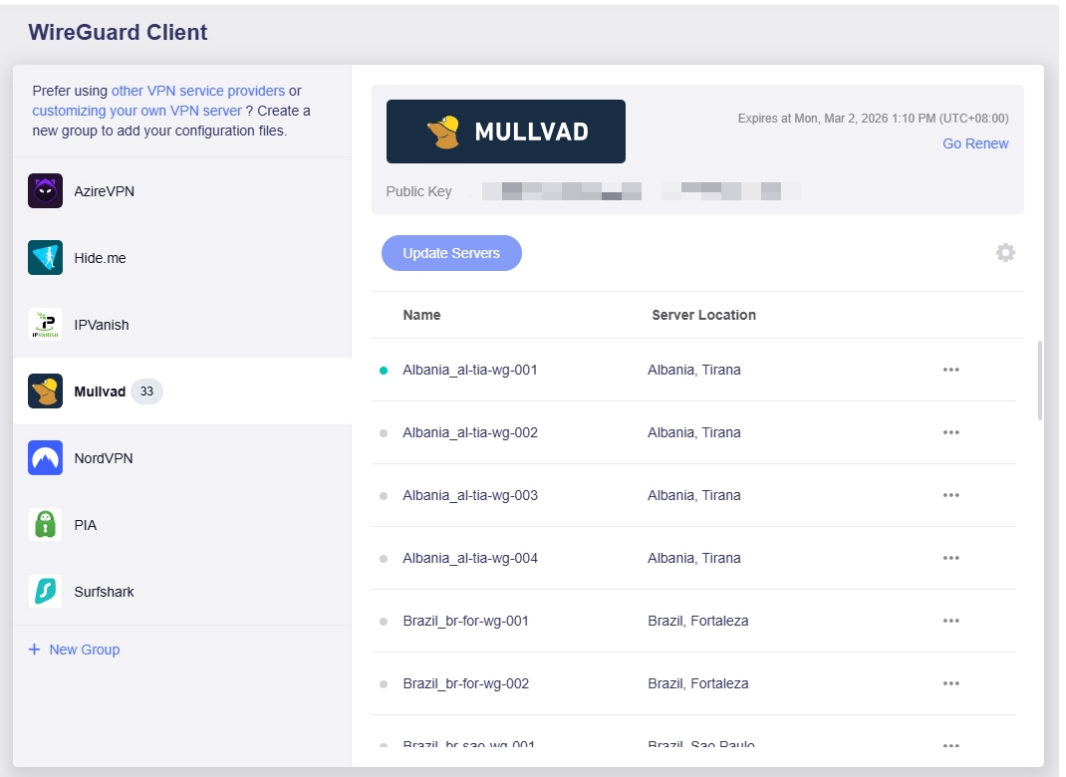
3. Select the server(s) you want to connect to, and click **Apply**.



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



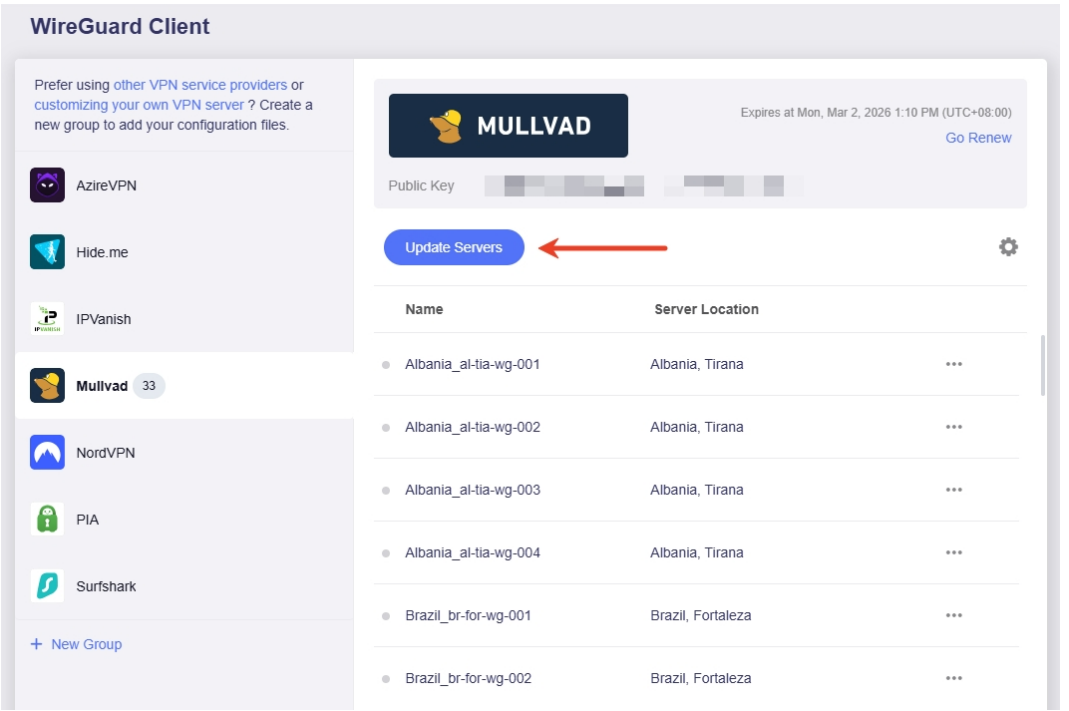
5. Once connected, a green dot will appear next to the configuration file.



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

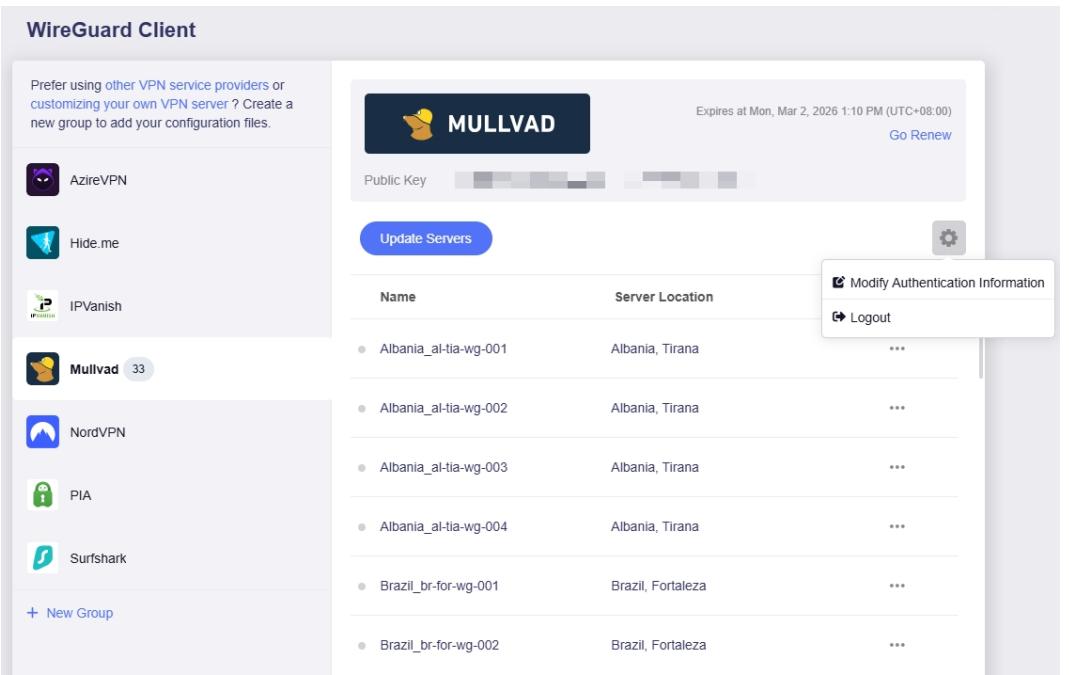
6. Update servers.

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



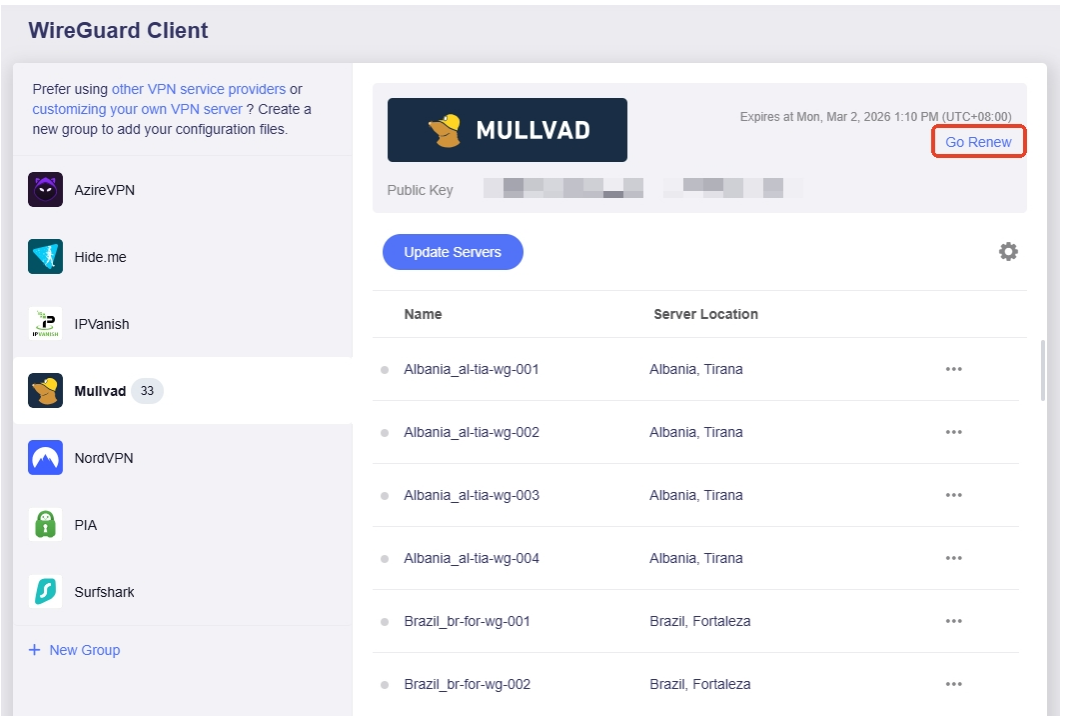
7. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



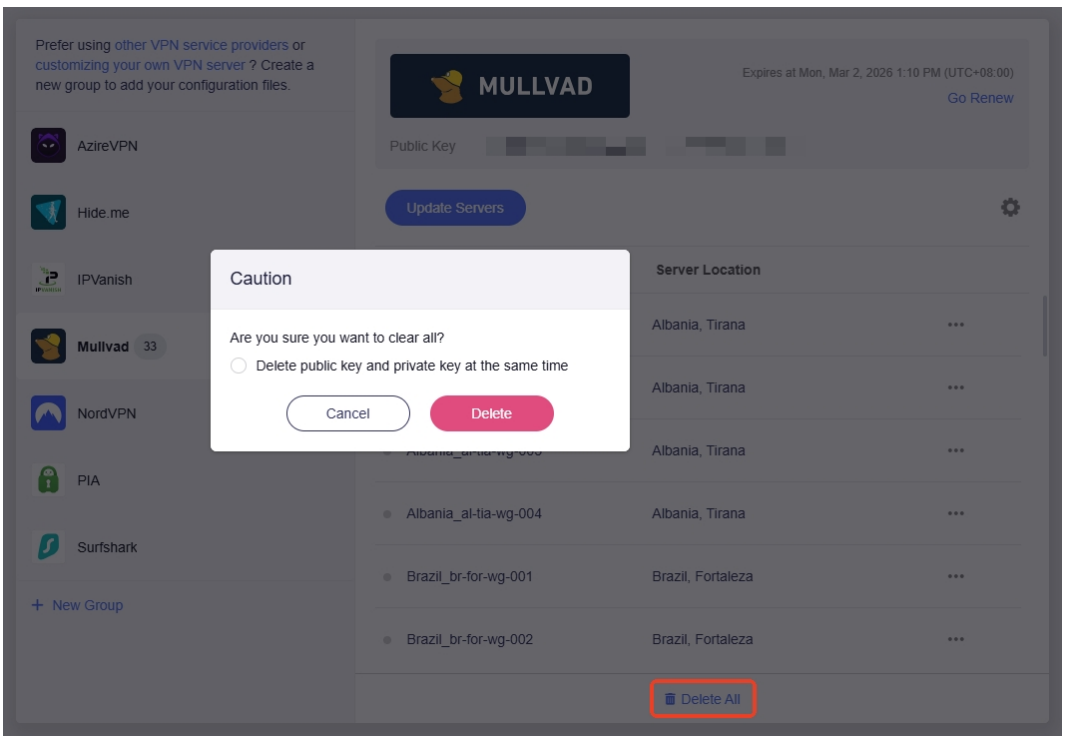
8. Go renew.

If you click **Go Renew**, you will be re-directed to the official website to renew your subscription.



9. Delete all files.

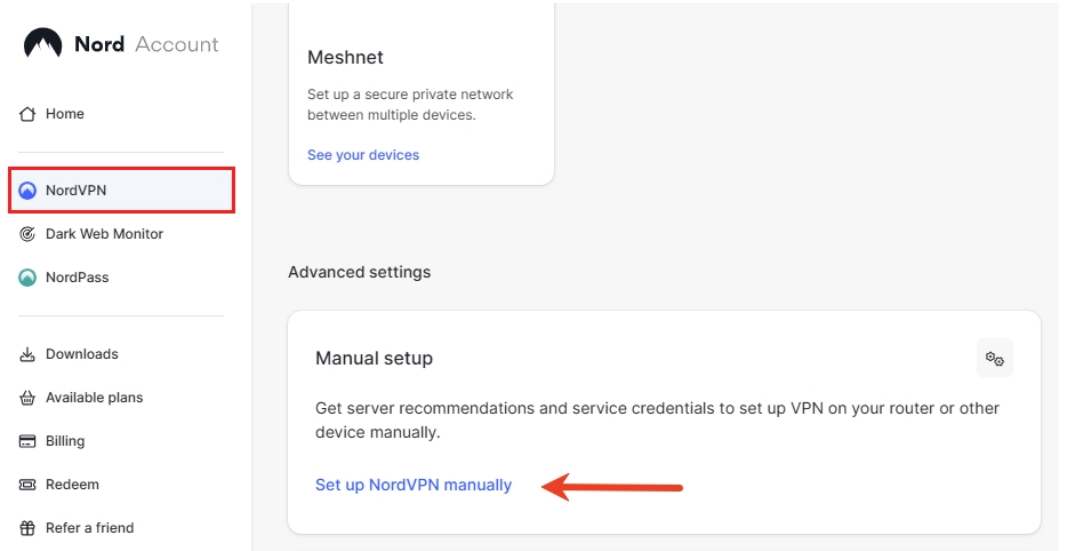
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



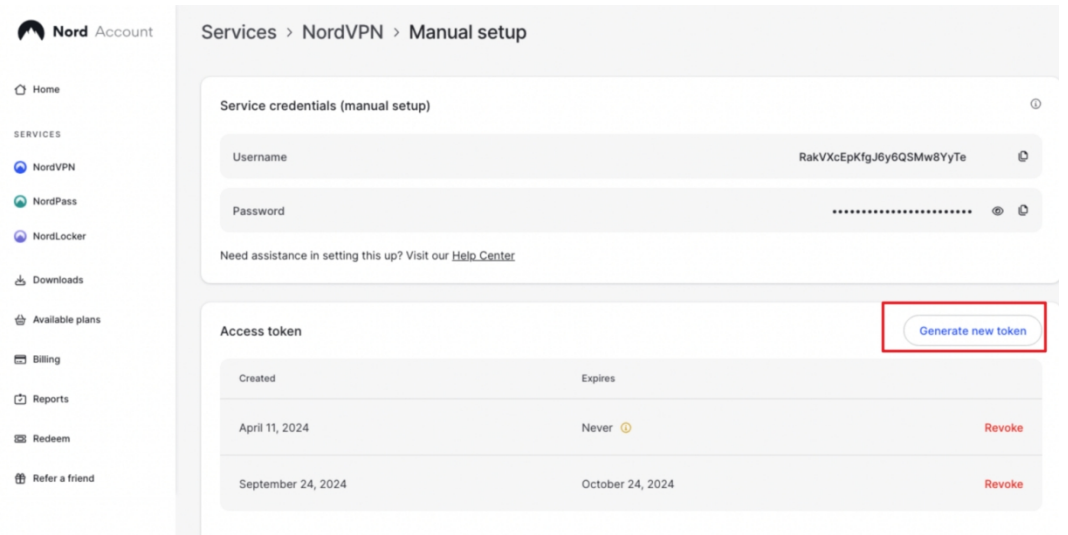
10.2.6 Set Up NordVPN

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

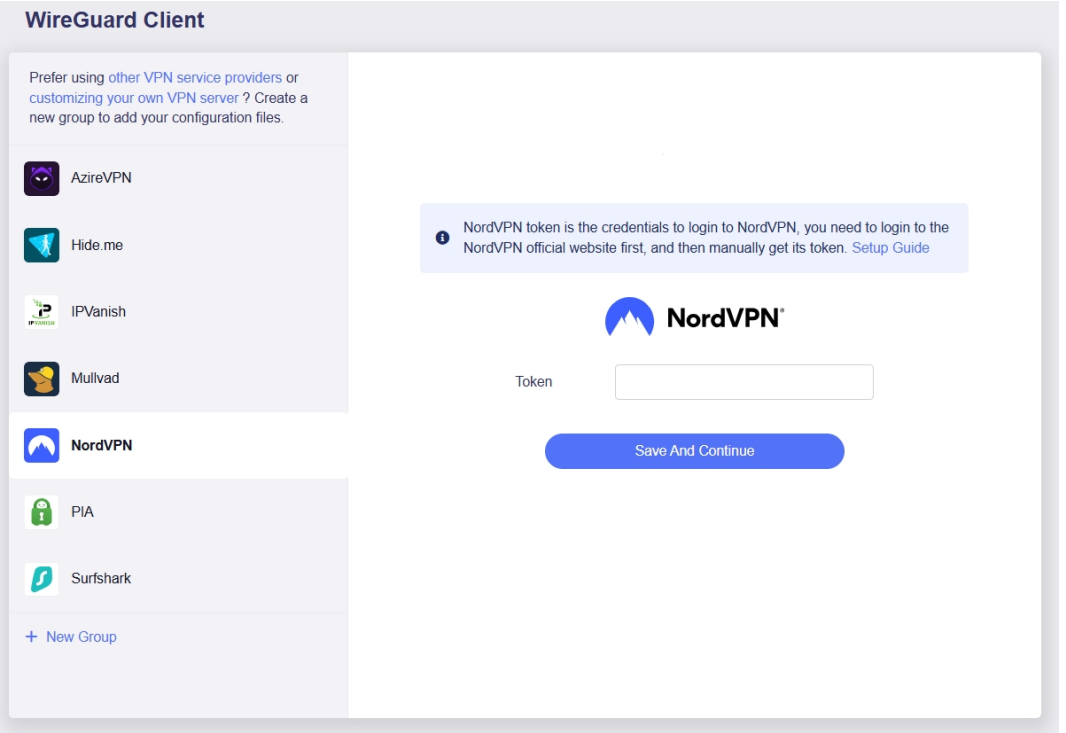
1. Log in to your NordVPN web account here.
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



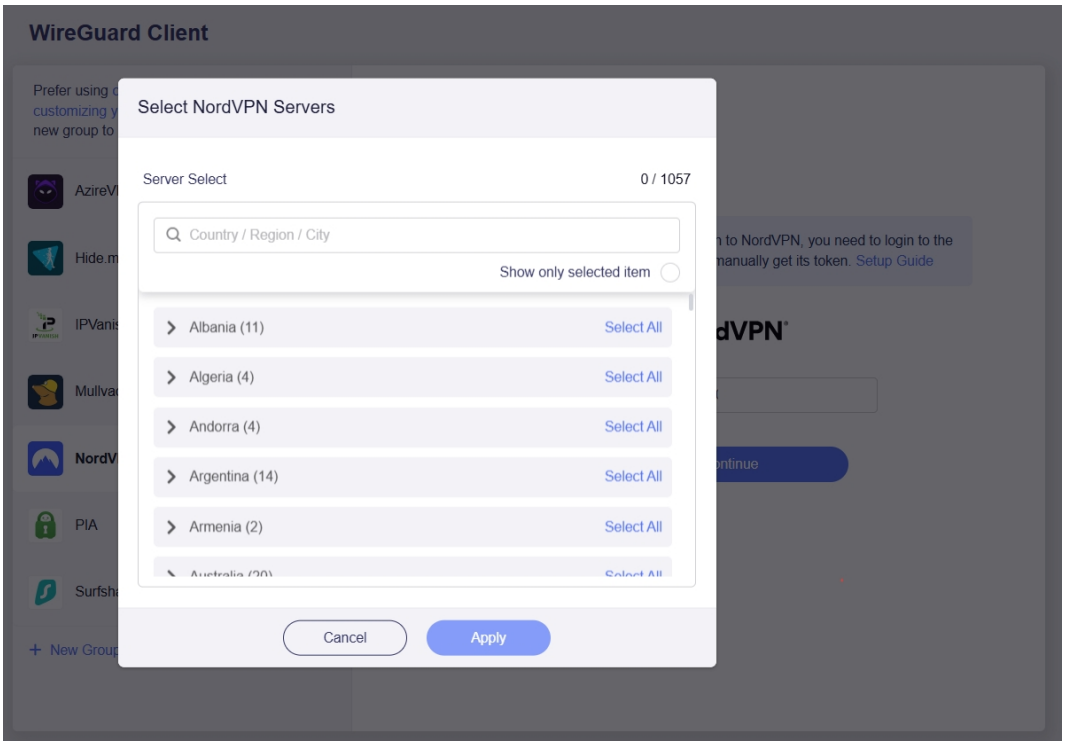
You will find the **Access Token**. Create an access token and copy for later use.



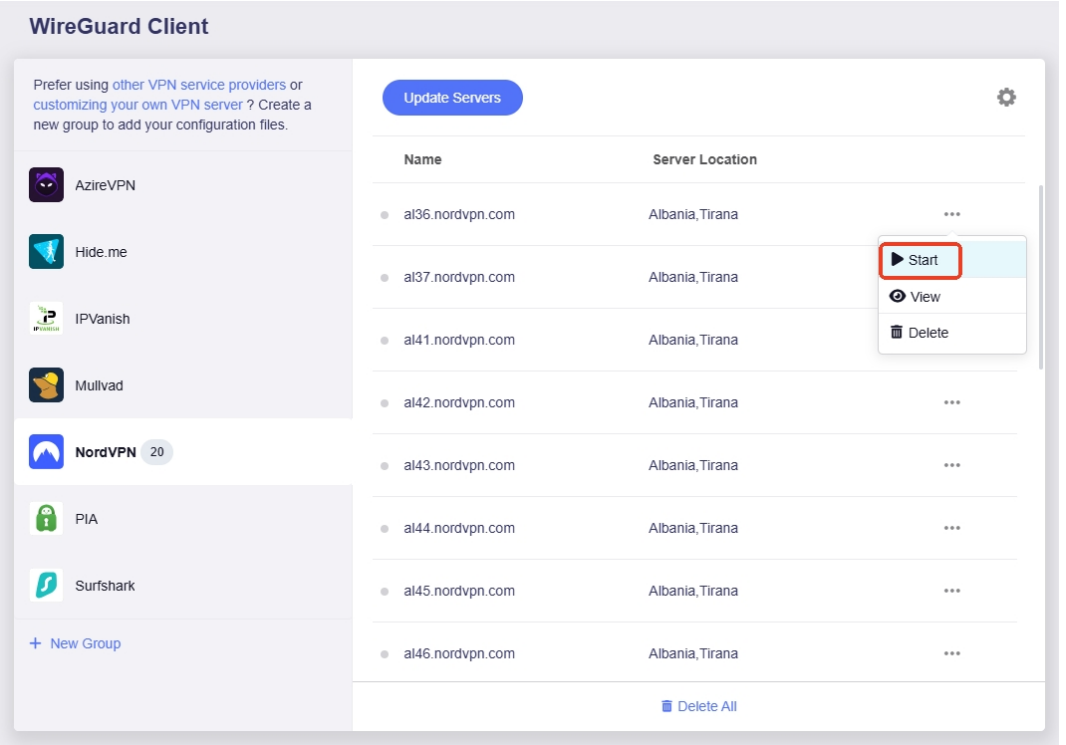
3. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **NordVPN**.
4. Input token, and click **Save and Continue**.



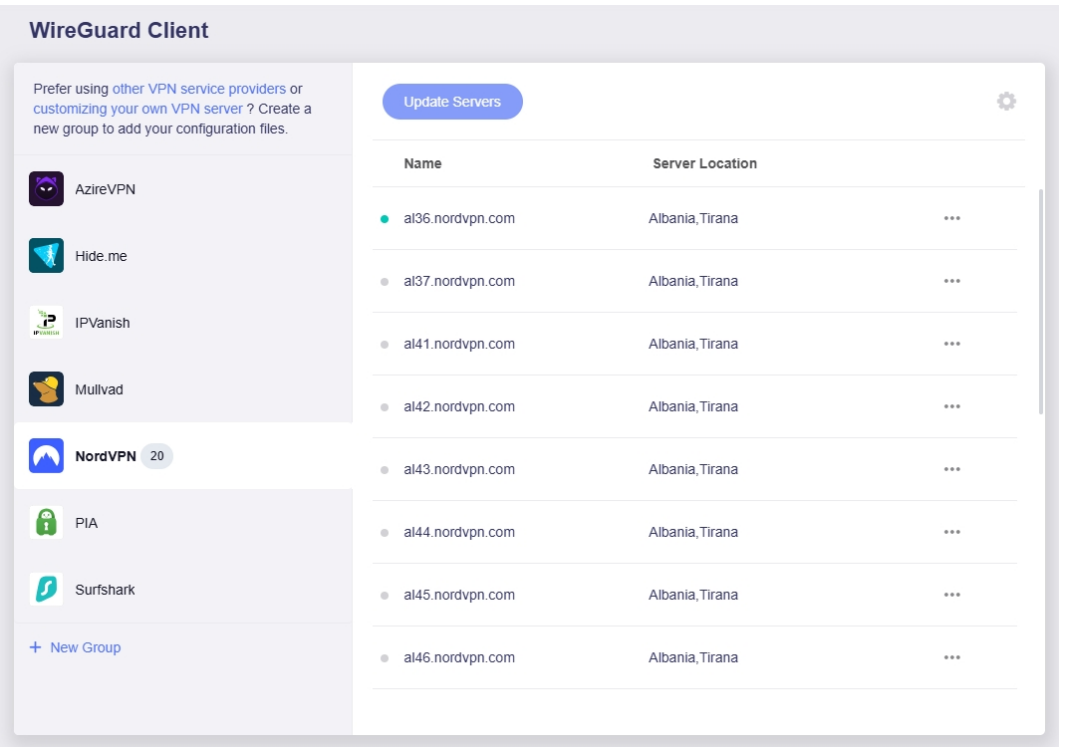
5. Select the server(s) you want to connect to, and click **Apply**.



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



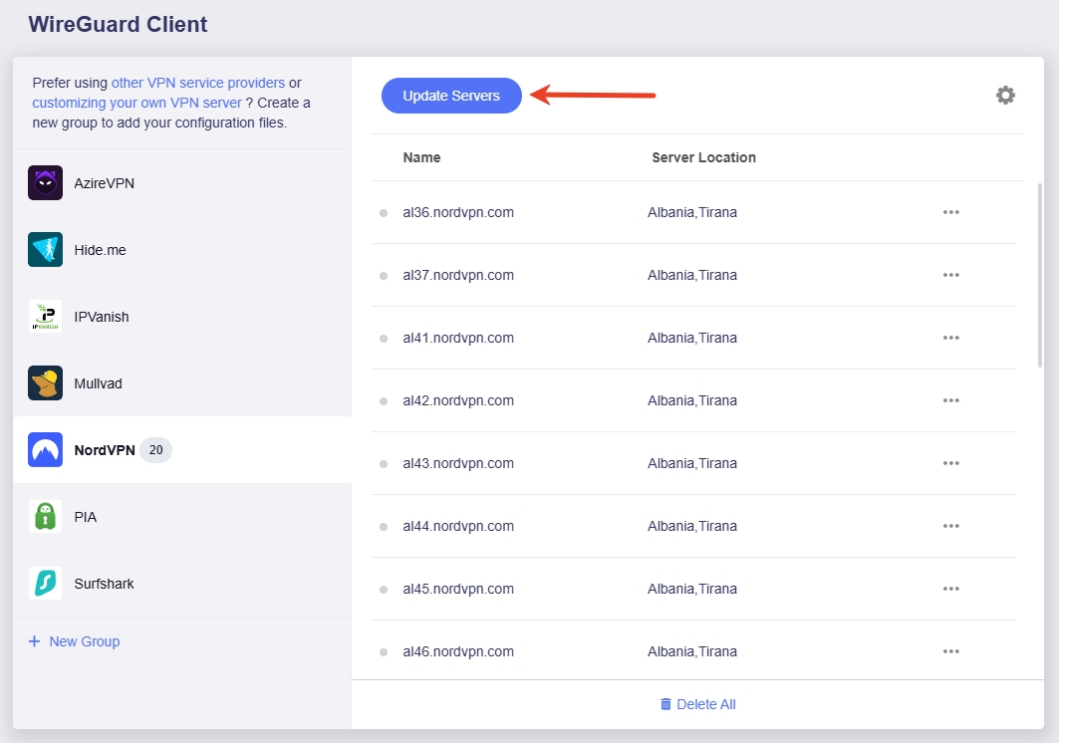
7. Once connected, a green dot will appear next to the configuration file.



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

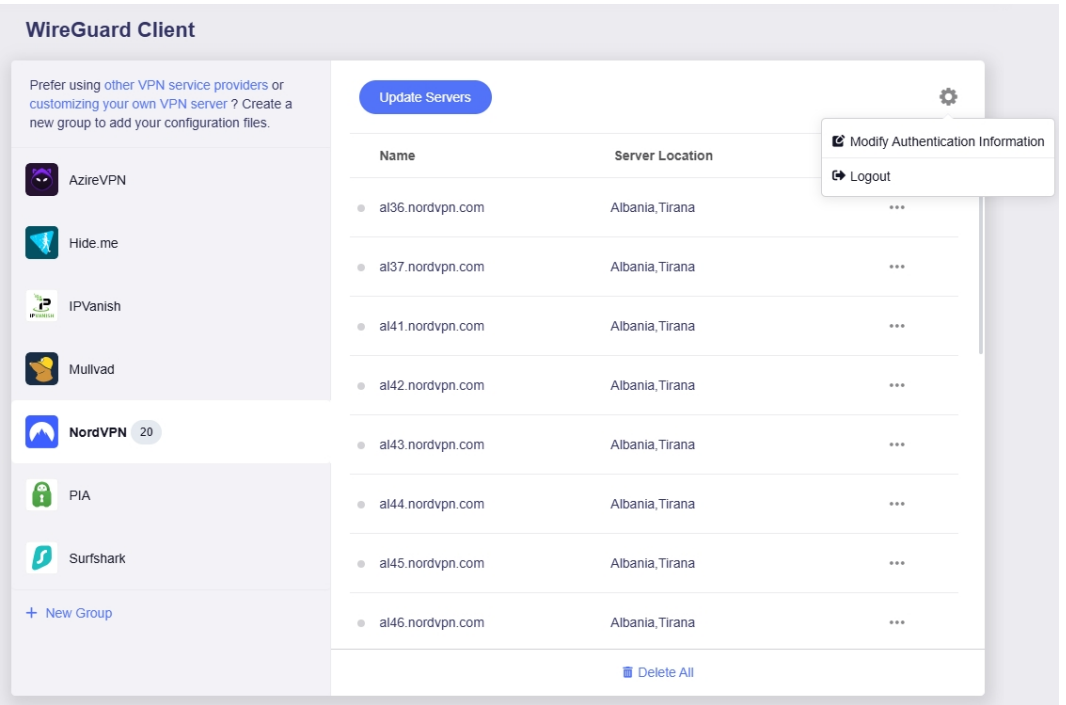
8. Update servers.

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



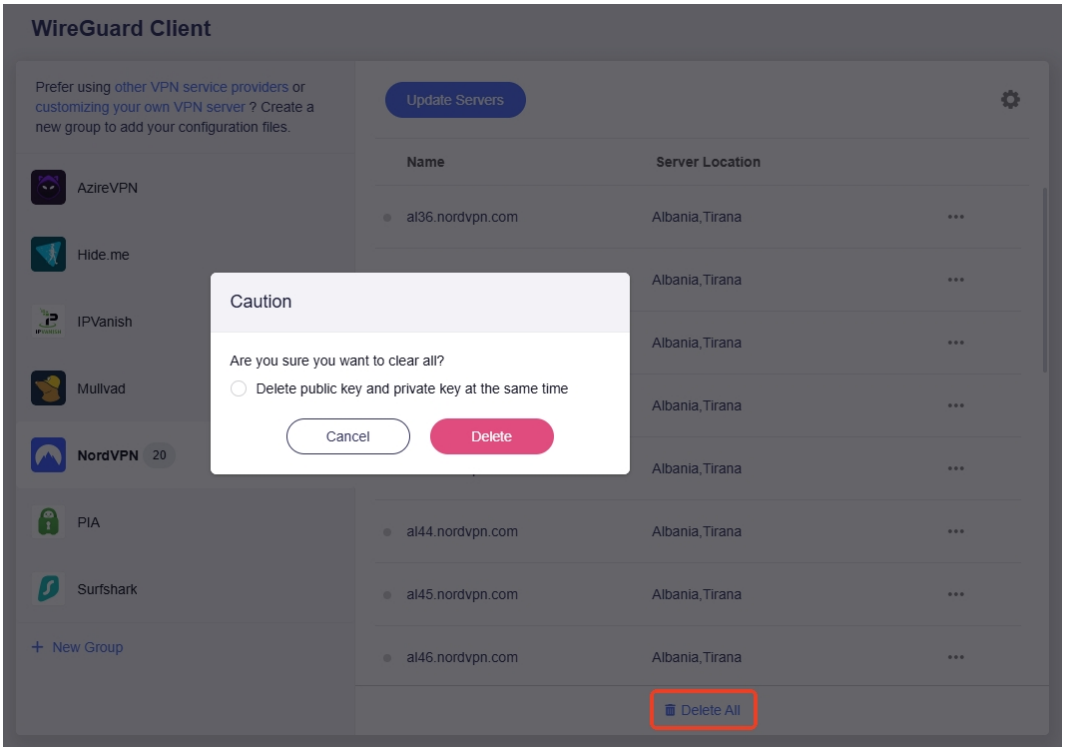
9. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



10. Delete all files.

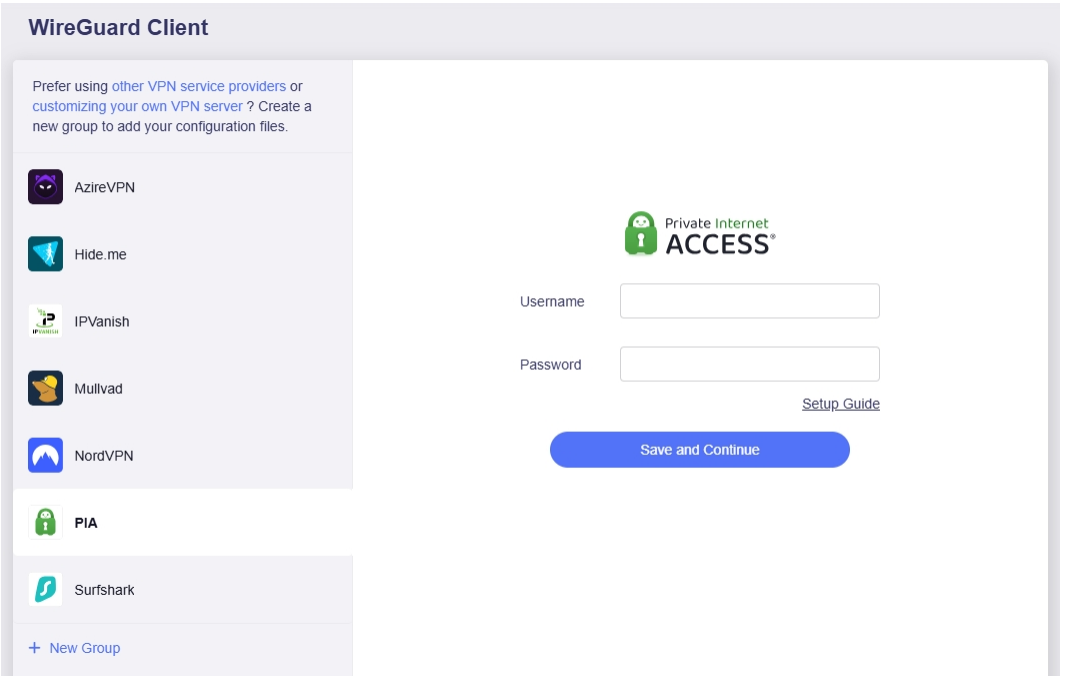
    You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



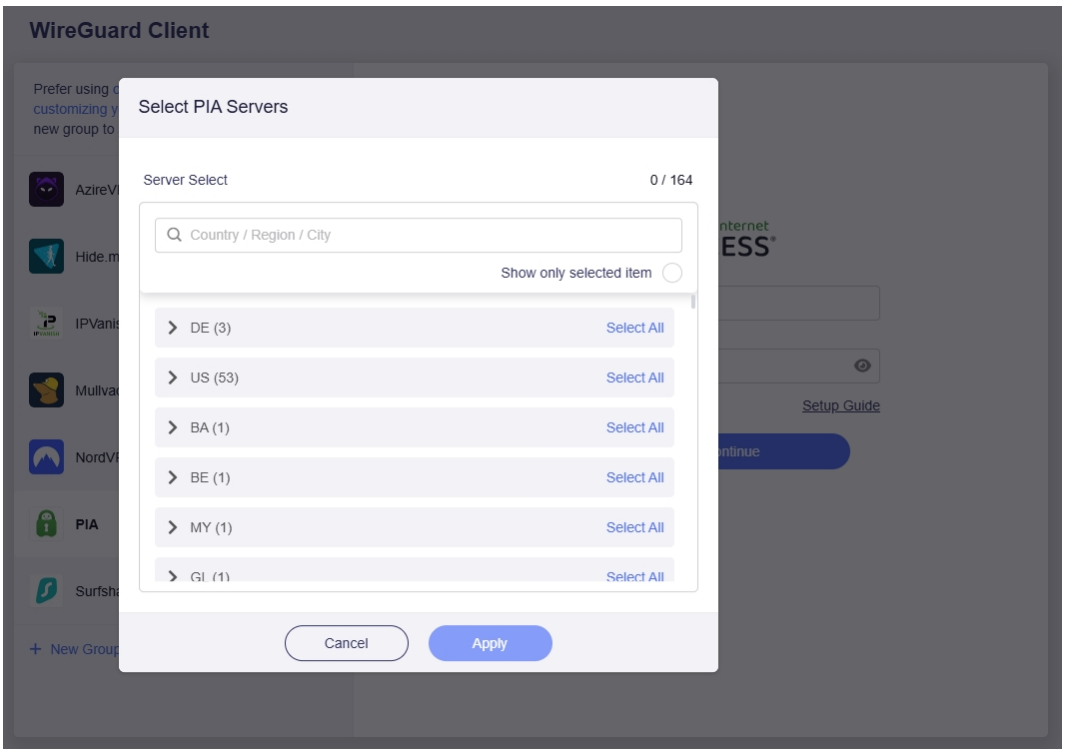
10.2.7 Set Up PIA (Private Internet Access)

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

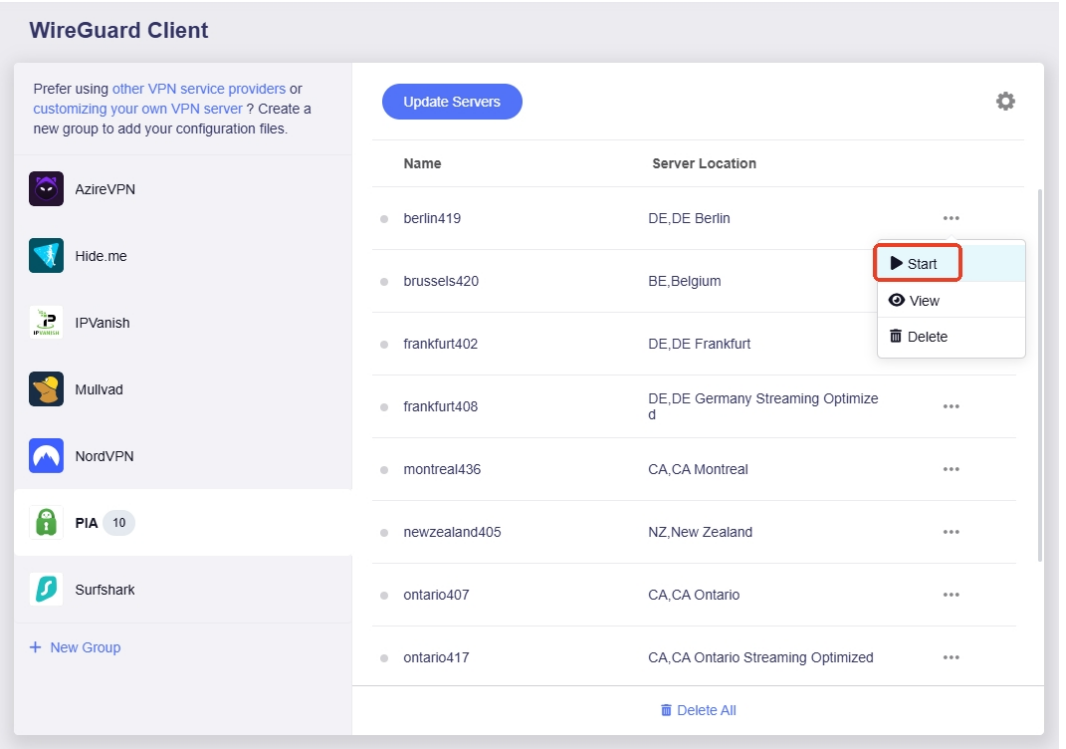
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **PIA**.
2. Input Username and Password, then click **Save and Continue**.



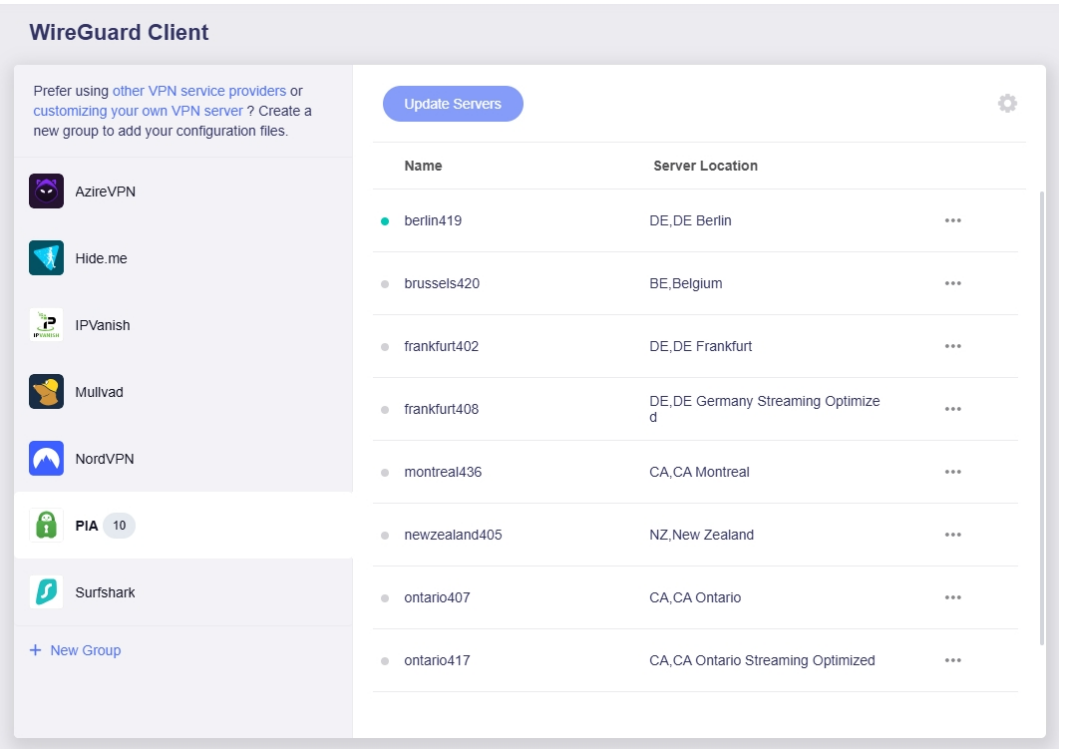
3. Select the server(s) you want to connect to, and click **Apply**.



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



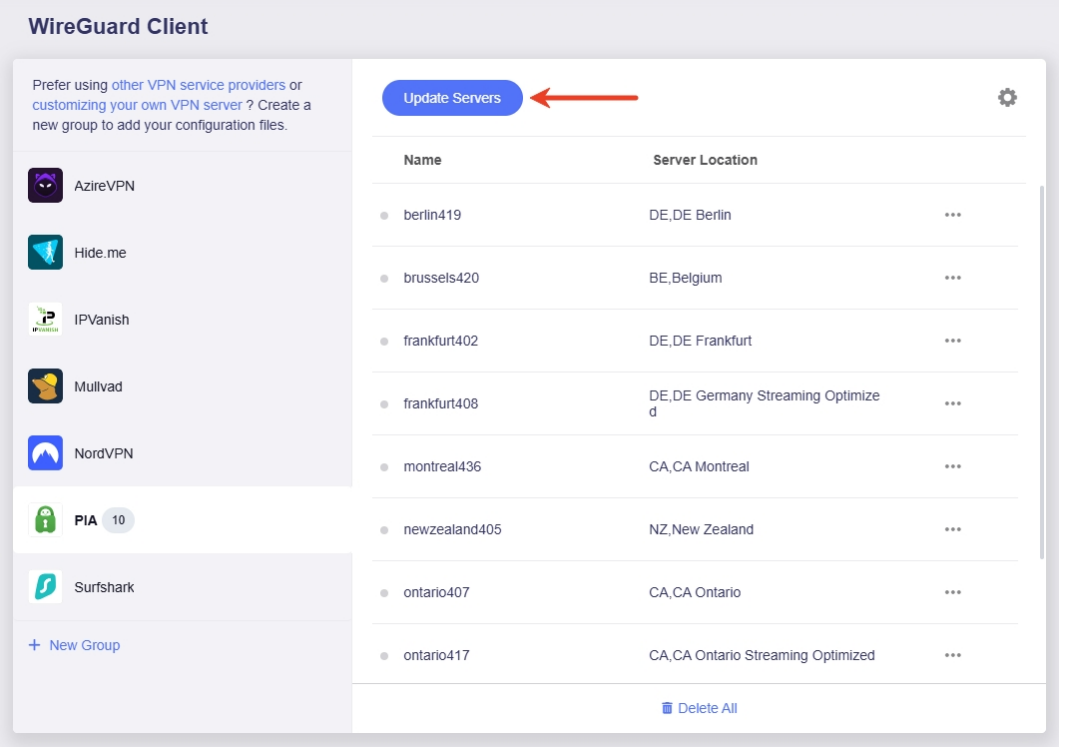
5. Once connected, a green dot will appear next to the configuration file.



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

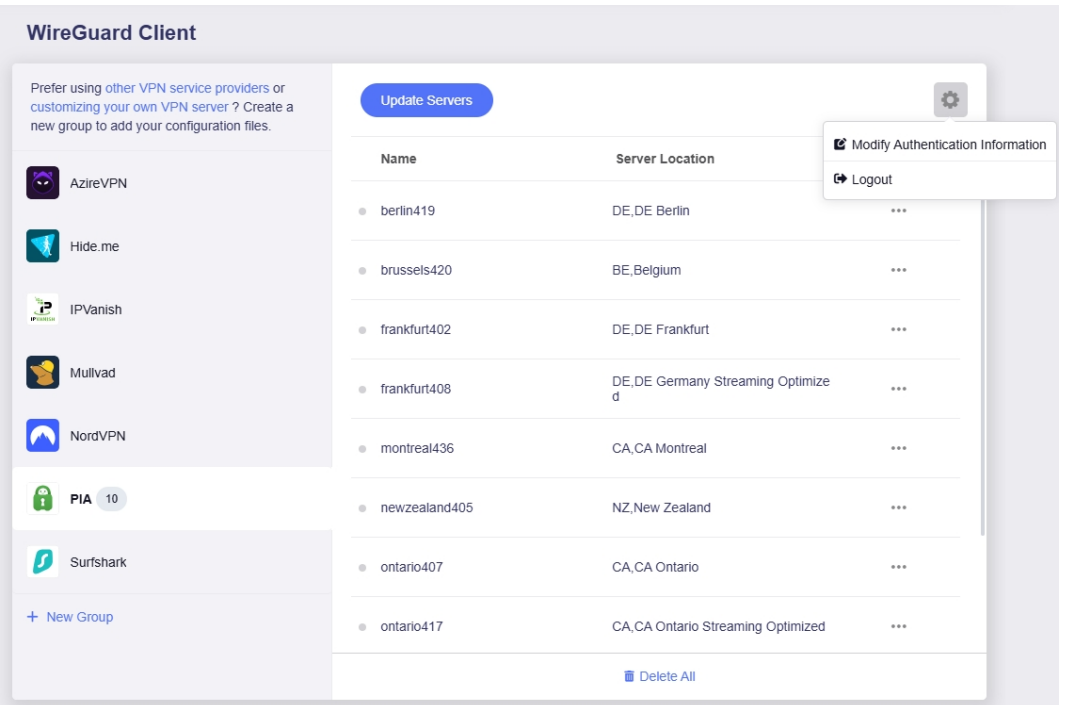
6. Update servers.

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



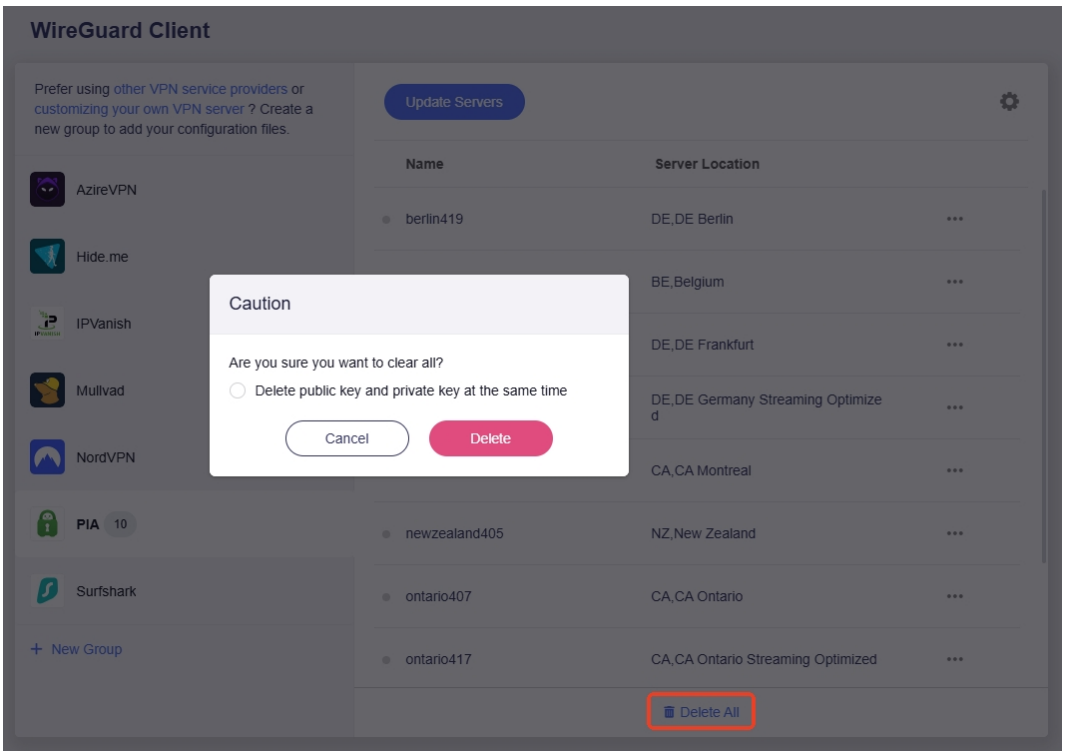
7. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



8. Delete all files.

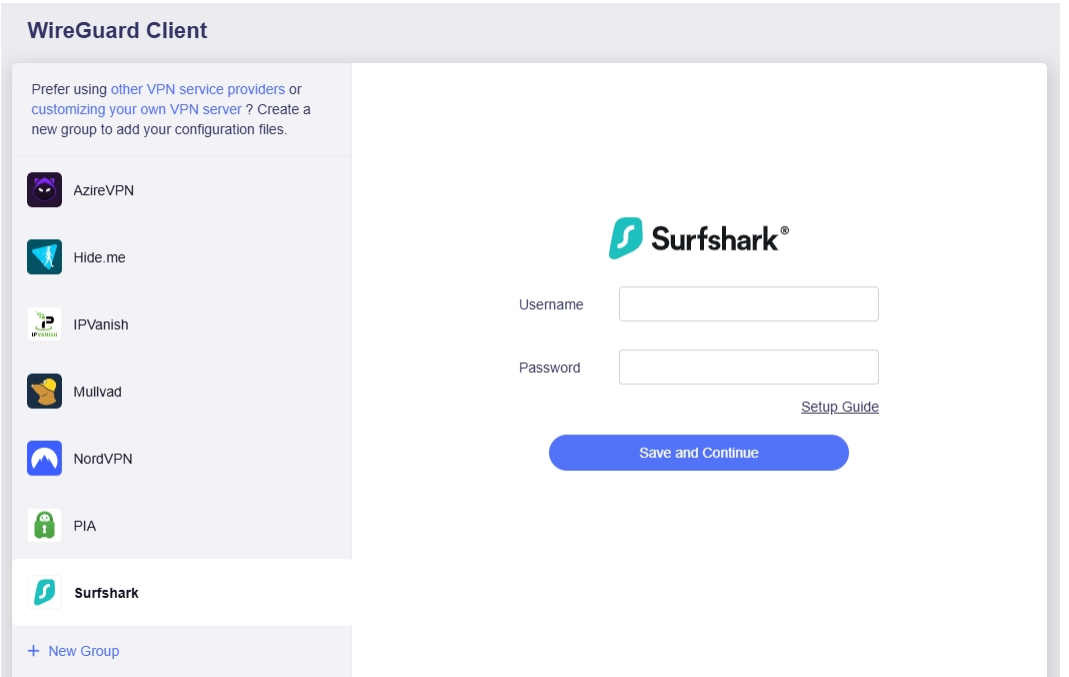
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



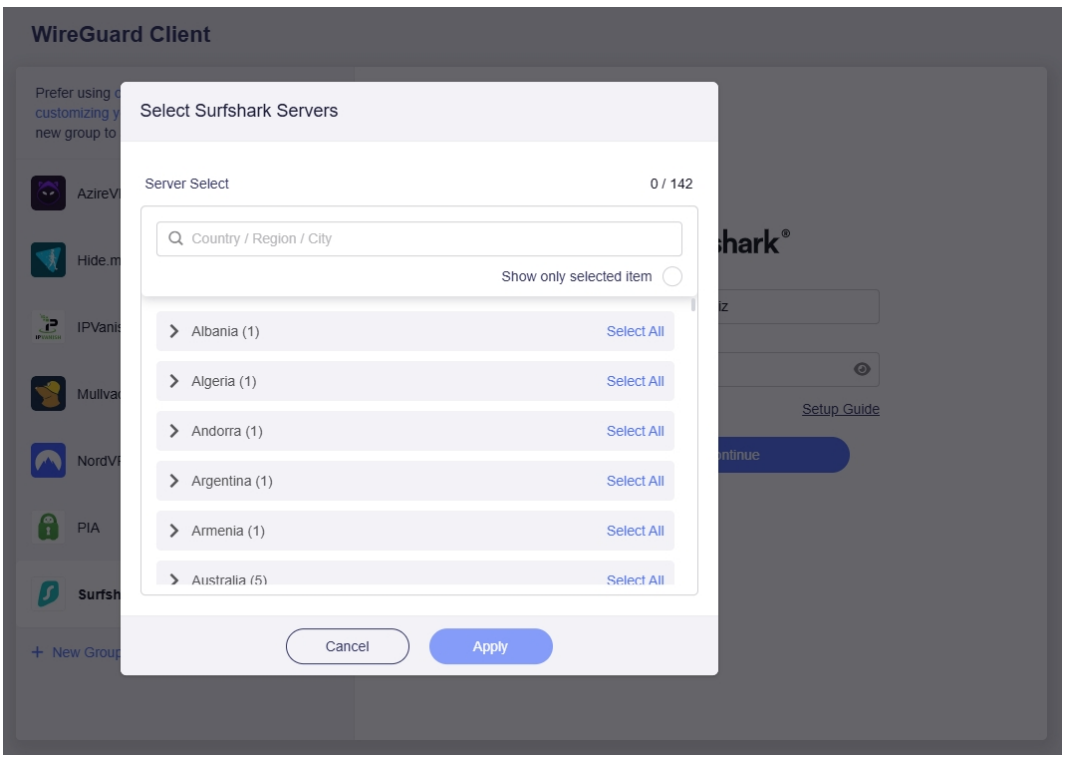
10.2.8 Set Up Surfshark

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

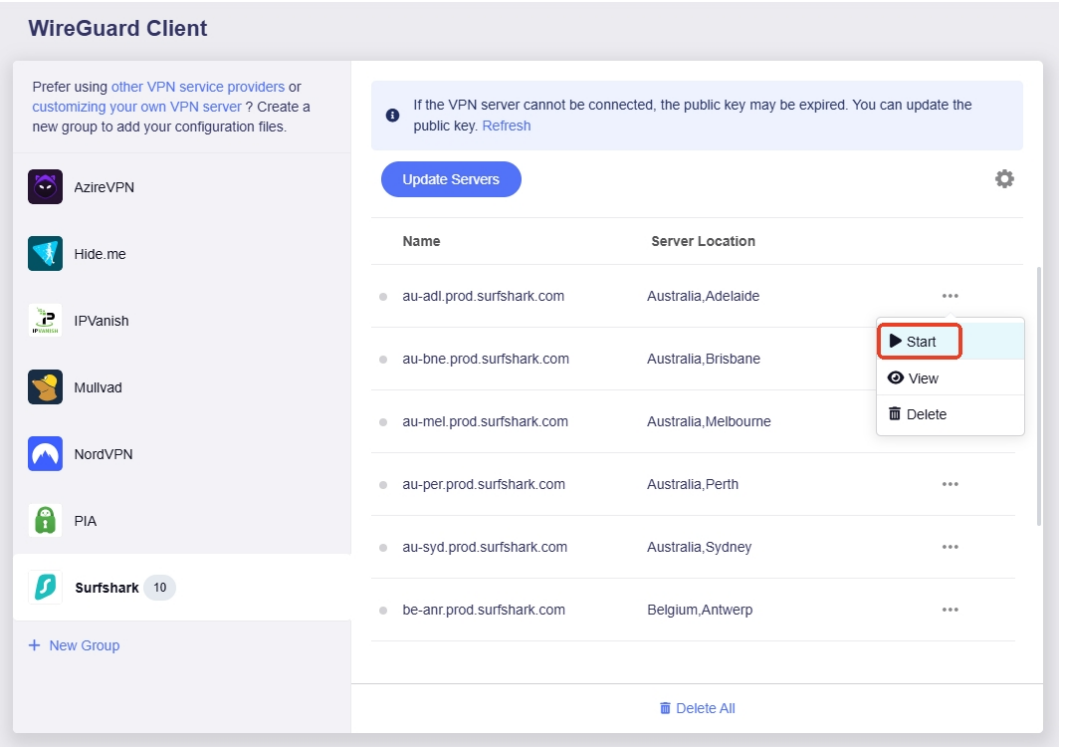
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Surfshark**.
2. Input Username and Password, then click **Save and Continue**.



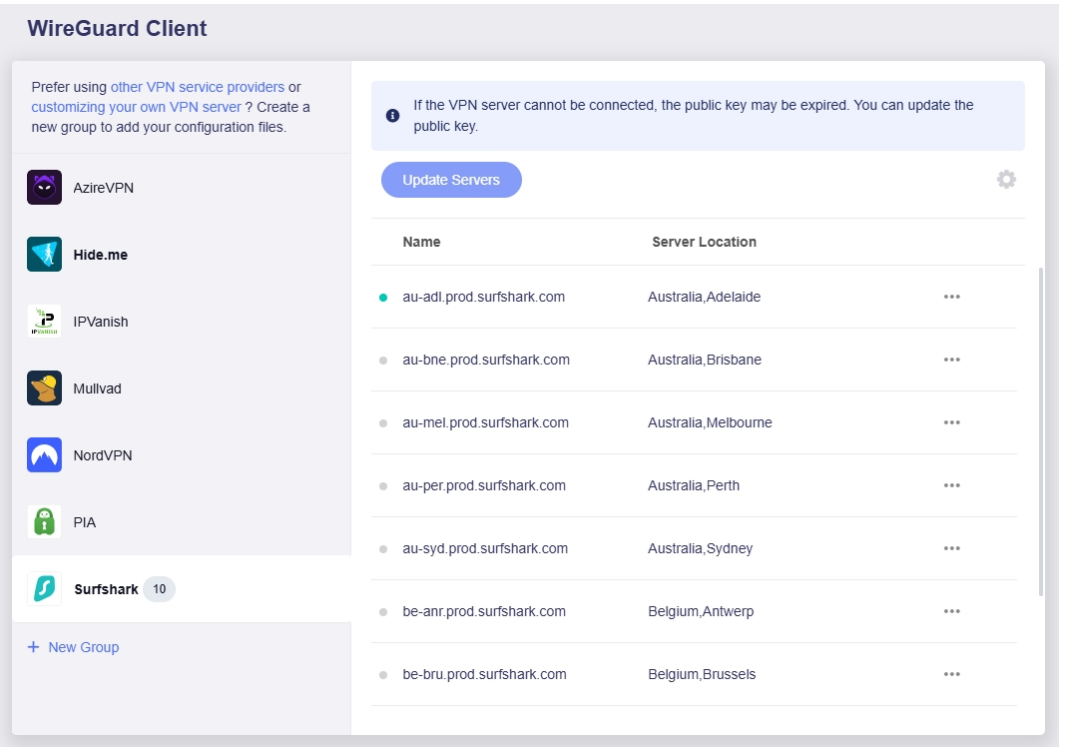
3. Select the server(s) you want to connect to, and click **Apply**.



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



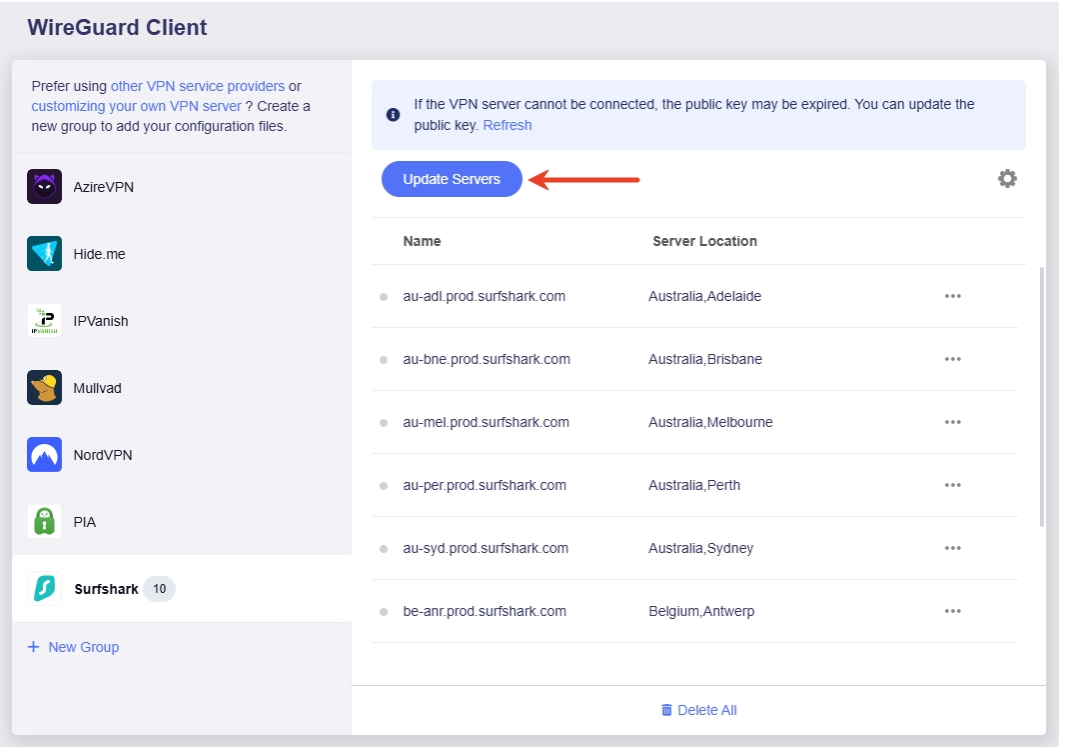
5. Once connected, a green dot will appear next to the configuration file.



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

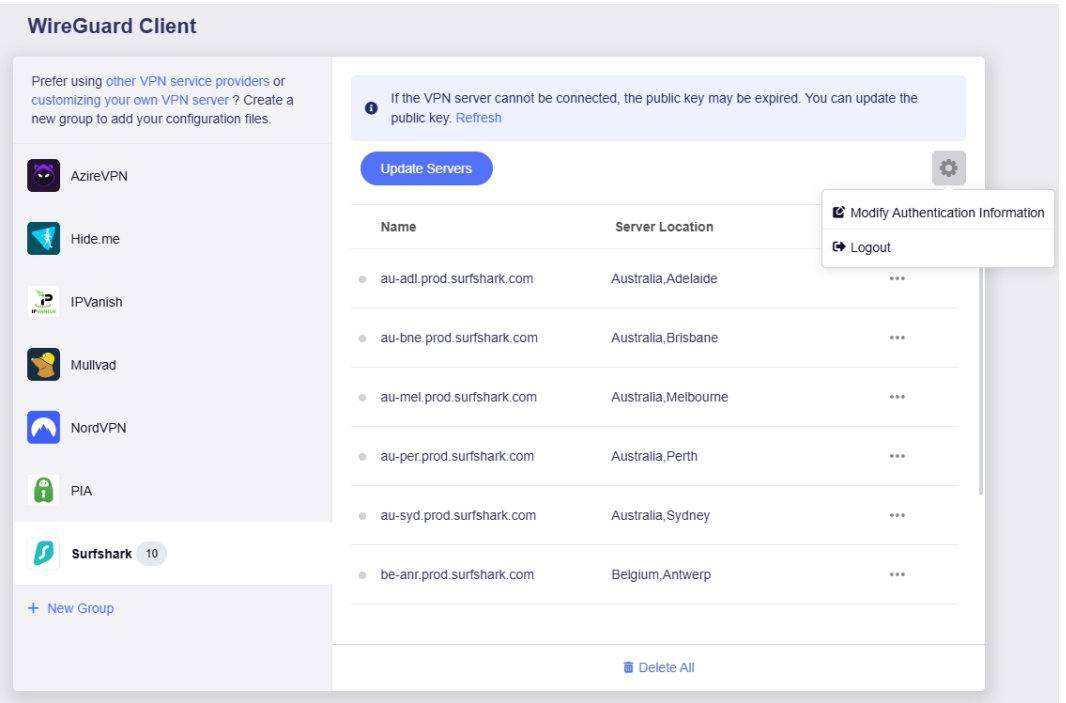
6. Update servers.

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



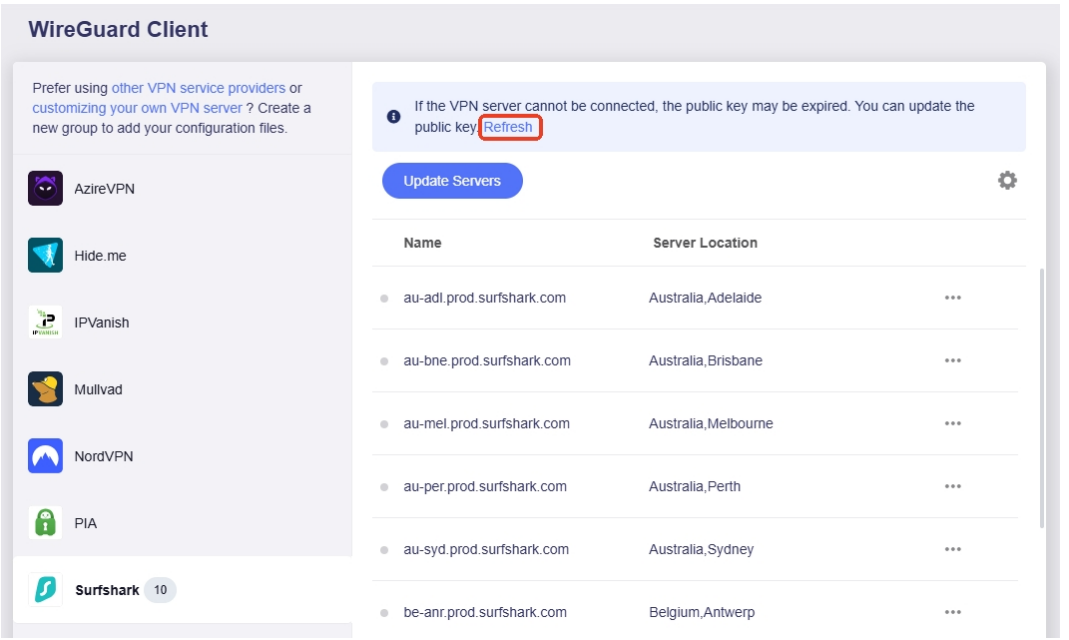
7. Edit credentials or logout.

   Click the gear icon to edit your login credentials or log out.



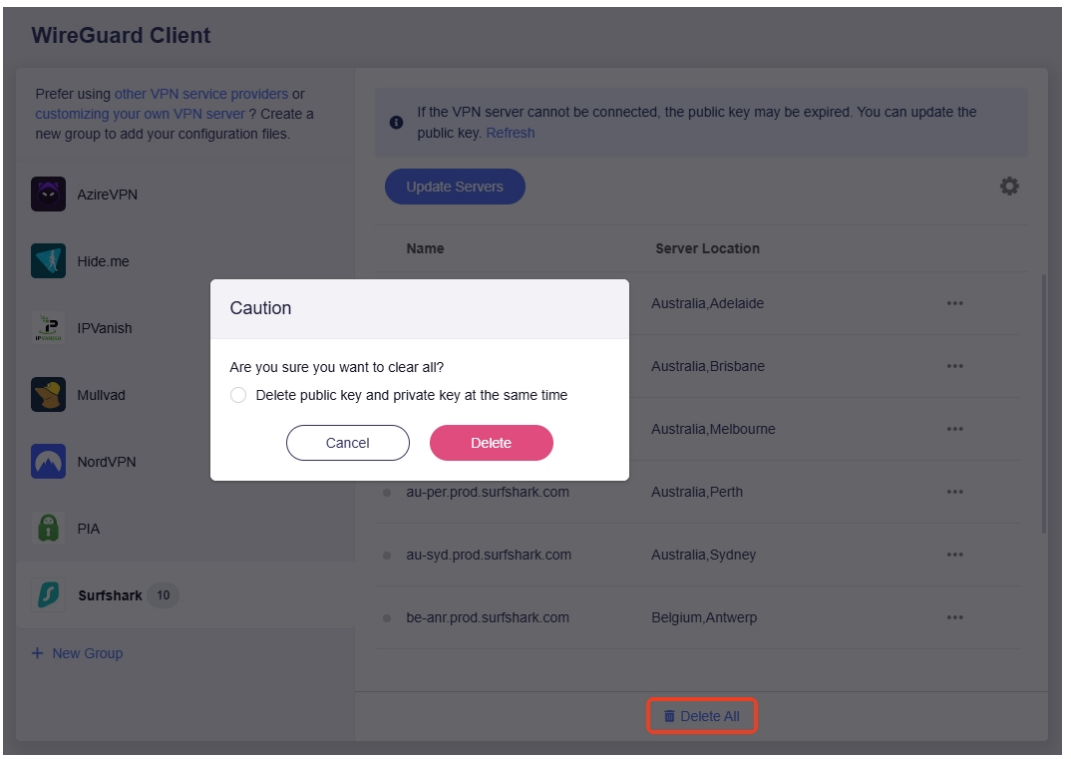
8. Refresh.

   You can click **Refresh** to update the public key when the VPN server cannot be connected.



9. Delete all files.

   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.

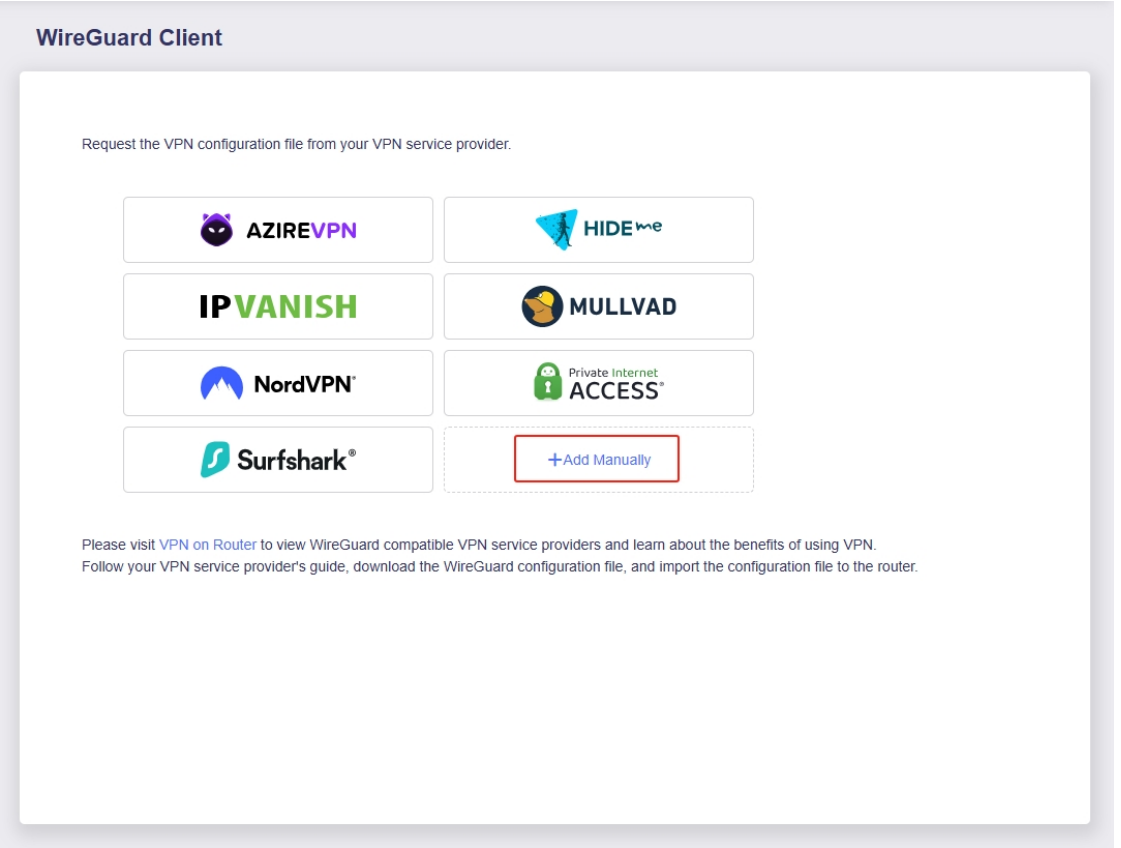


10.2.9 Set Up WireGuard Client Manually (for other providers)

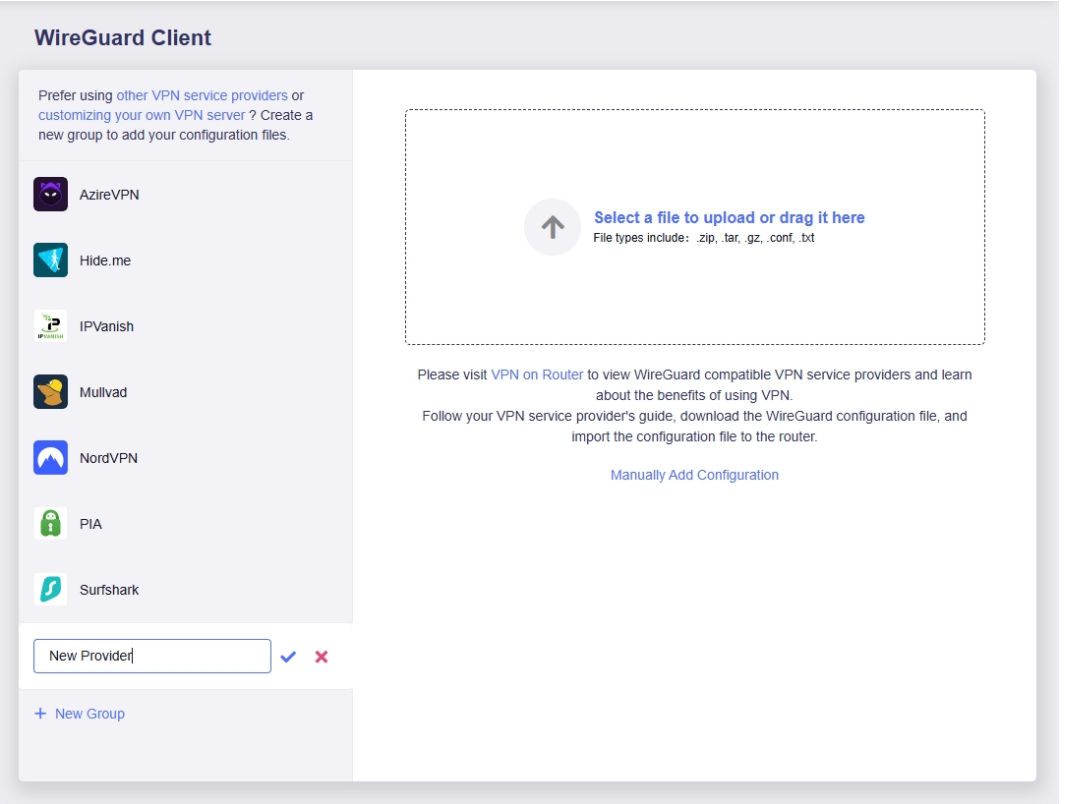
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see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

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

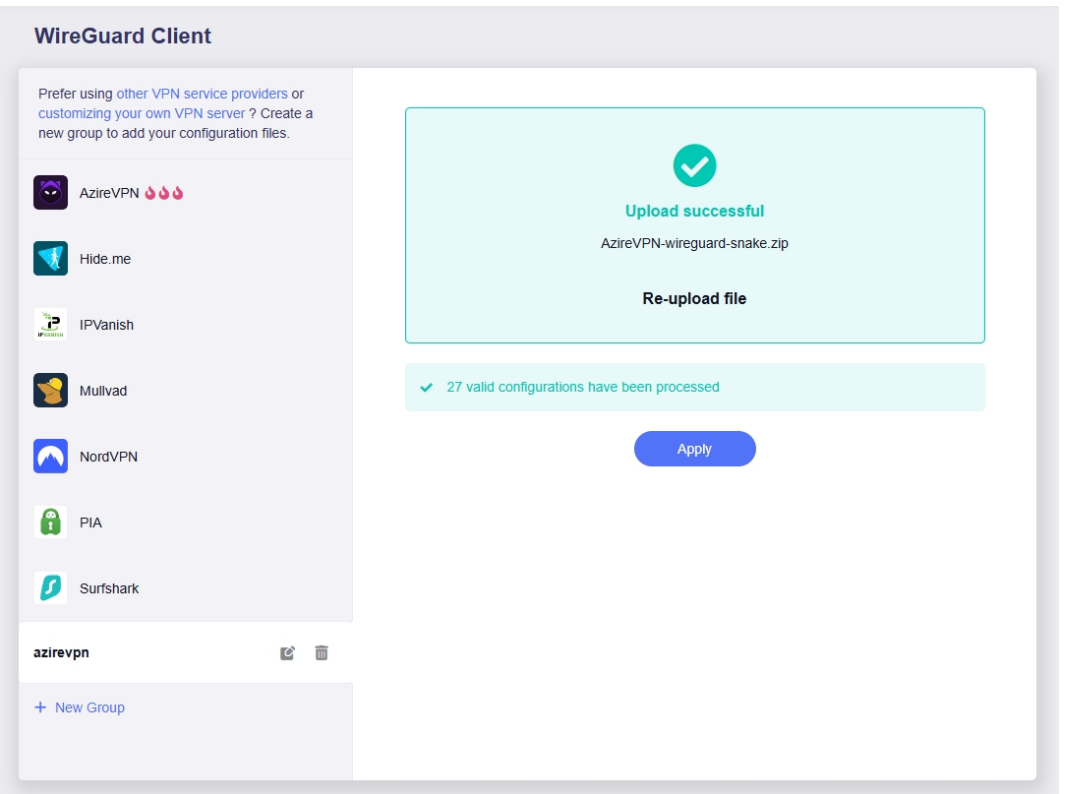
1. Log in to your router's web admin panel and navigate to **VPN** > **WireGuard Client** > **Add Manually**.



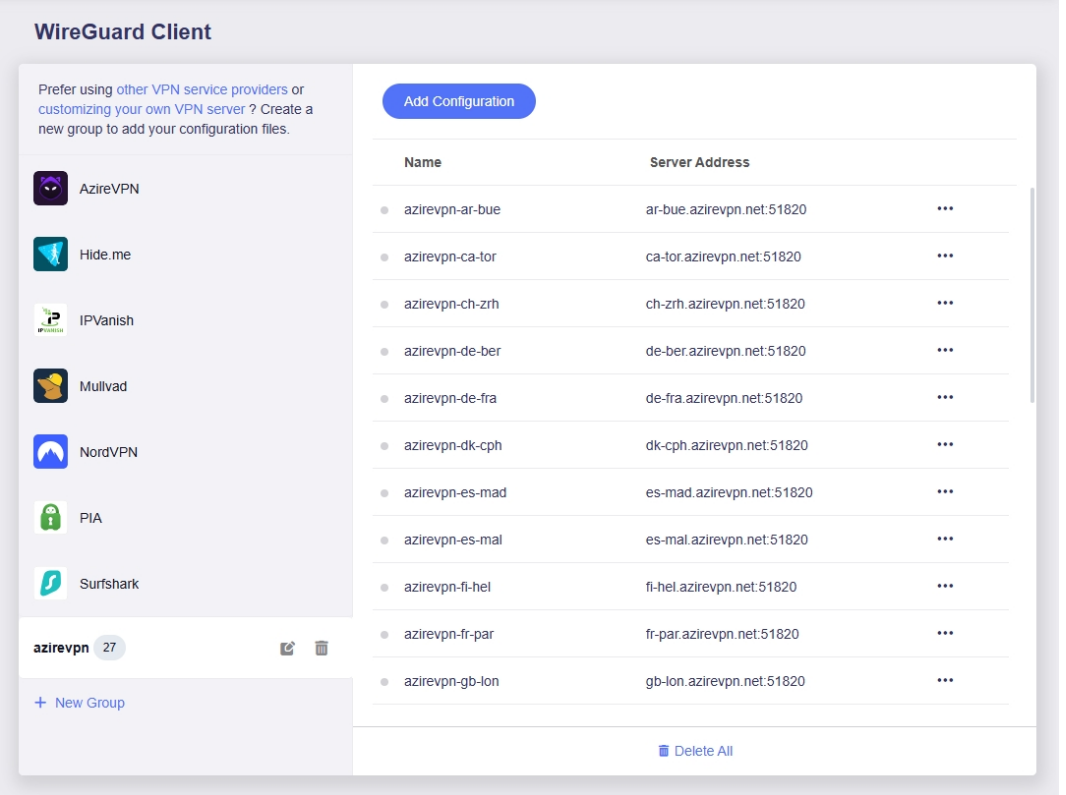
2. It will create a group on the left sidebar. Set a descriptive name for the group.



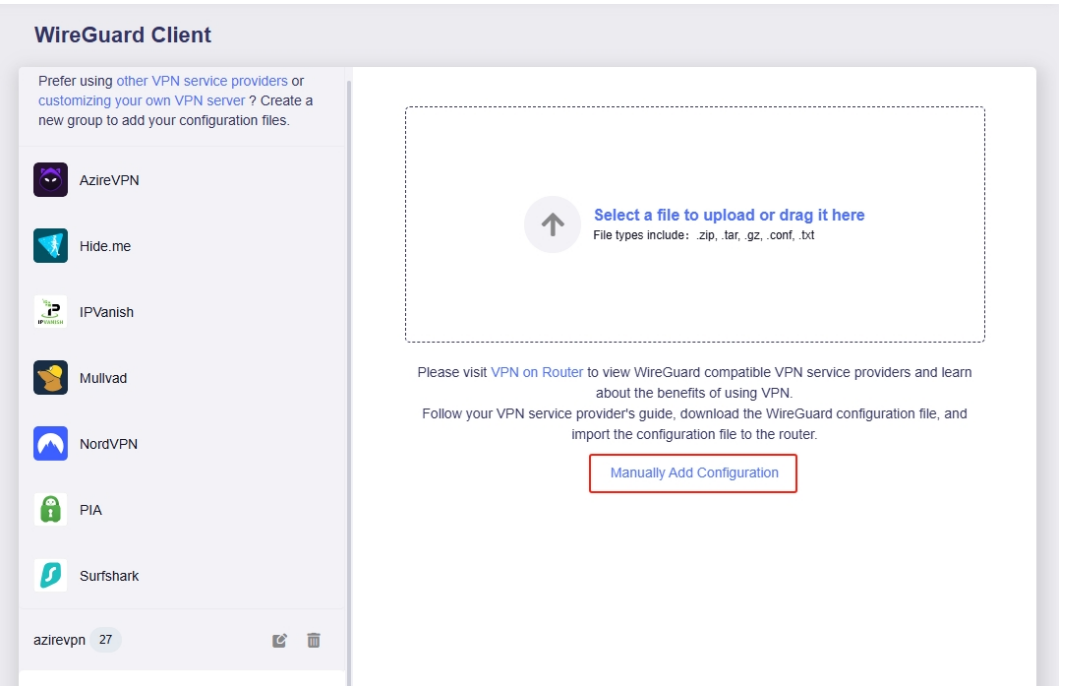
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.

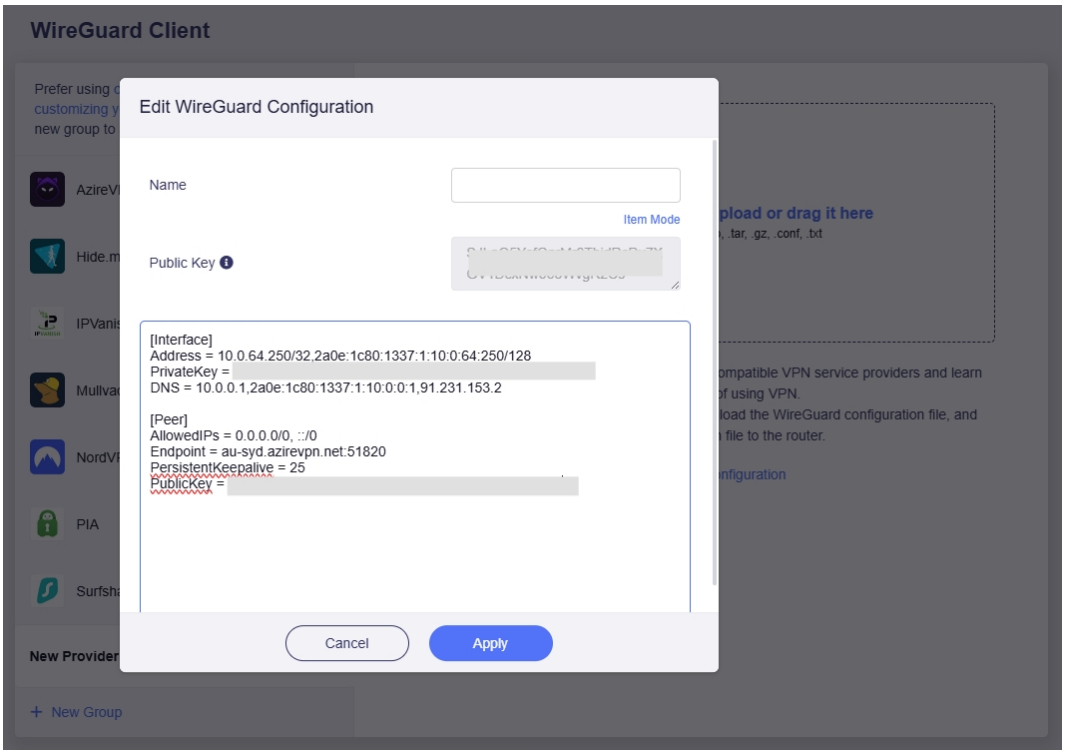


If you upload a compressed file containing multiple configuration files, it will be decompressed automatically, as shown below.

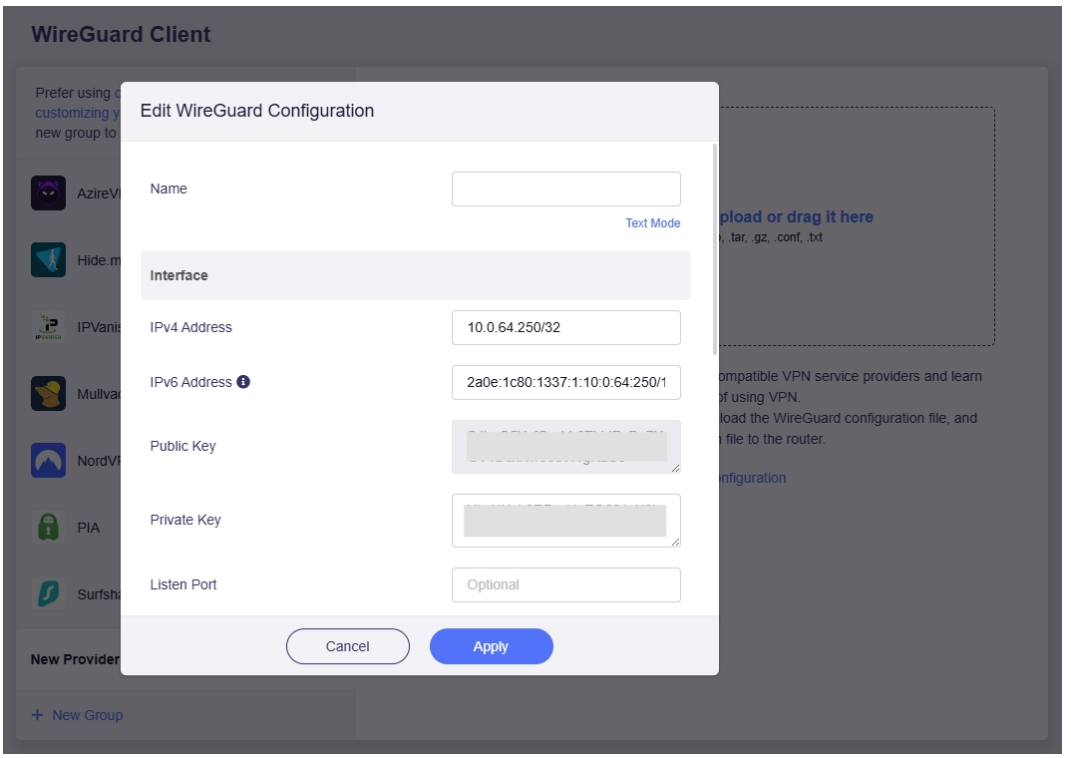


Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

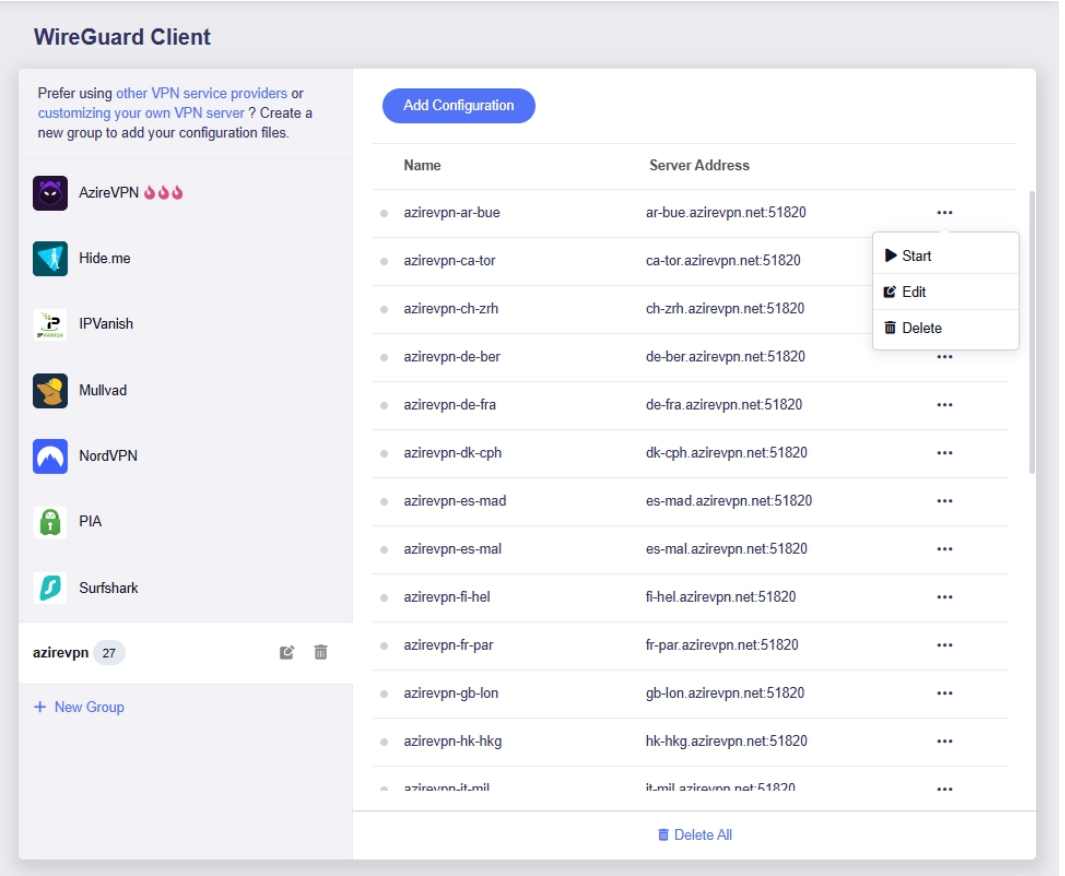




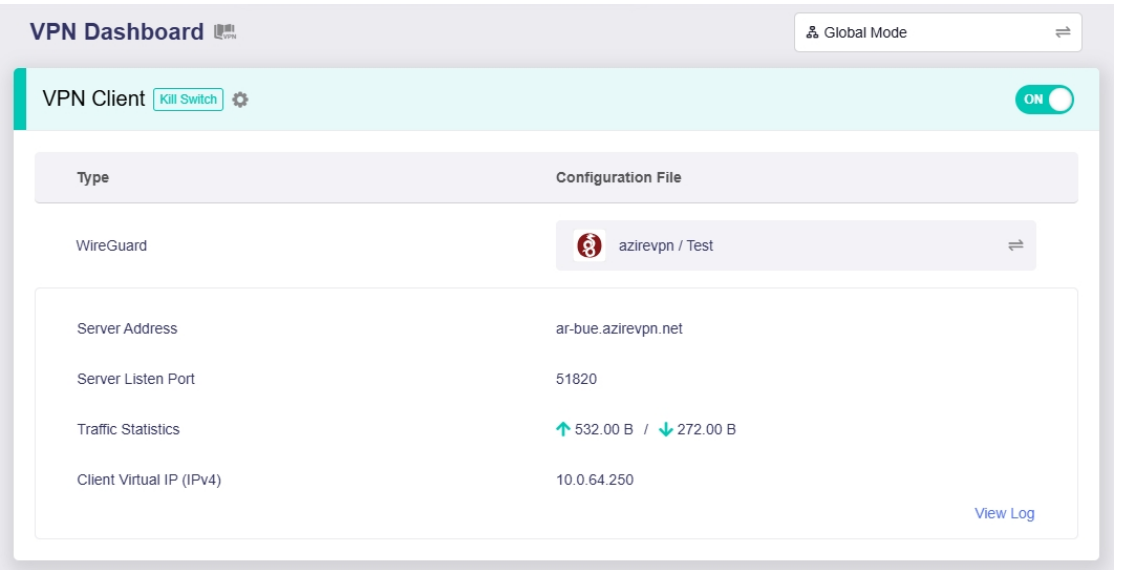
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



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

Tor

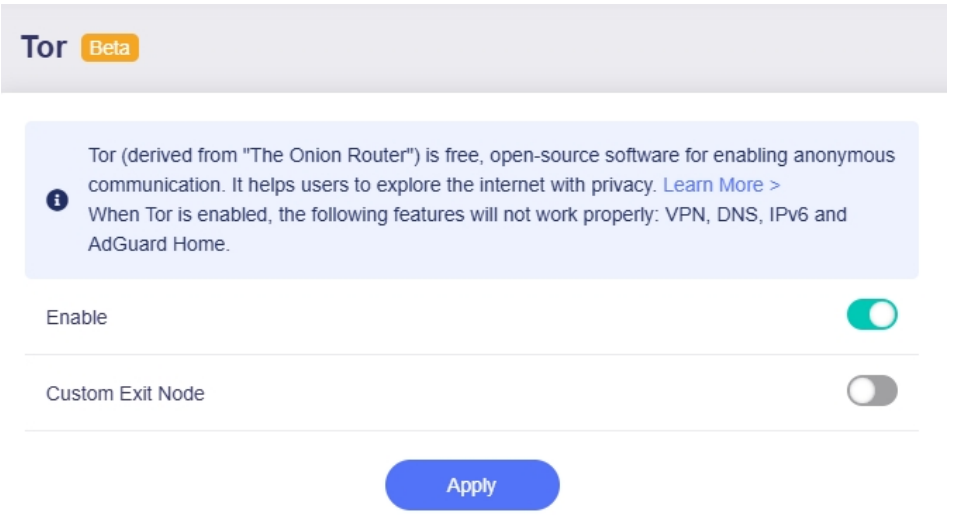
This chapter provides a brief introduction to Tor (The Onion Router), a free and open-source software for enabling anonymous communication.

Tor (derived from **The Onion Router**) is a free and open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Note that this feature is currently in beta, and may have some bugs.

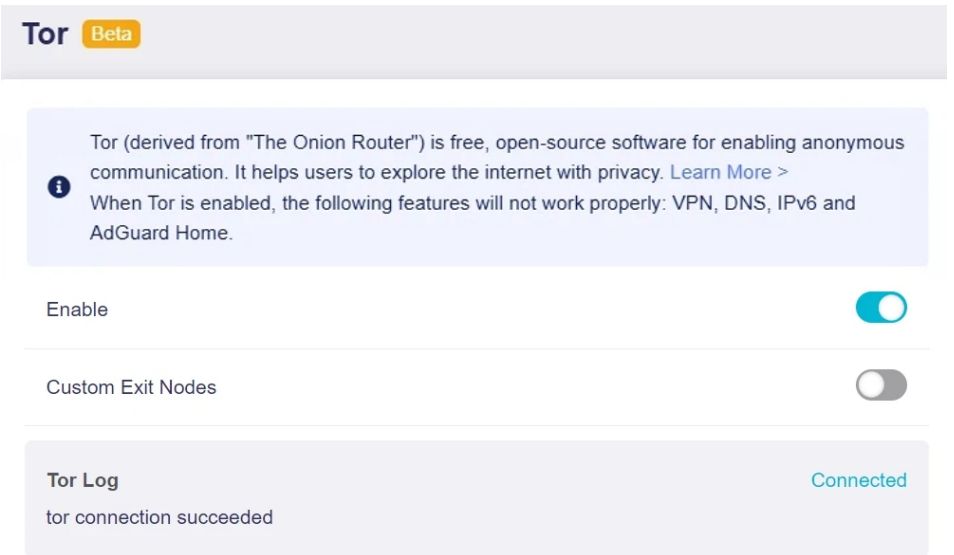
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6, and AdGuard Home.

Follow the steps below to set up Tor as needed.

1. Log in to your router's web admin panel and navigate to **VPN** > **Tor**. Toggle the switch to enable it, enable Custom Exit Nodes as needed, and click **Apply**.



2. It will start connecting. If your network meets the requirements, it will show connected.



Chapter 12

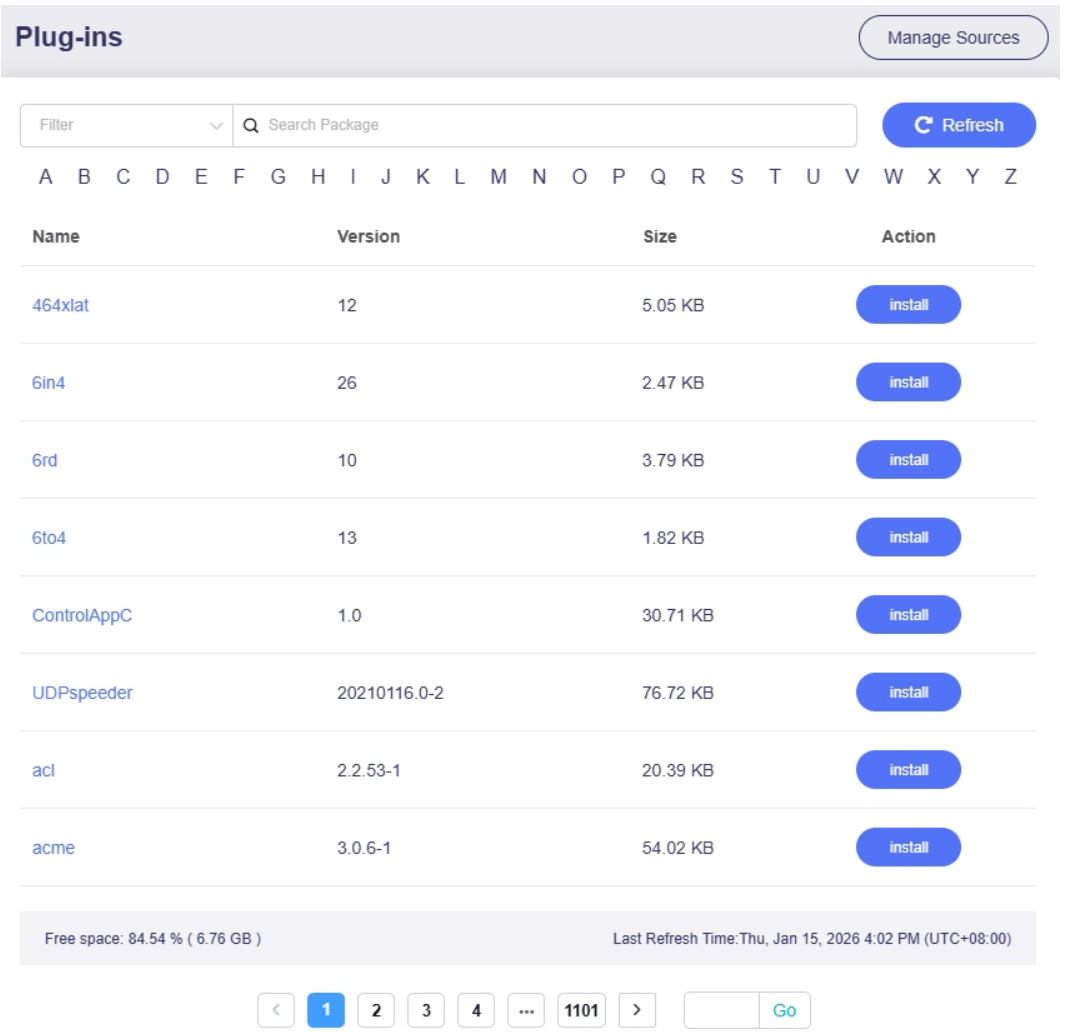
Applications

This chapter introduces some applications in GL.iNet routers, e.g., Plug-ins, Dynamic DNS, Network Storage, AdGuard Home, Parental Control, ZeroTier, and Tailscale.

12.1 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:

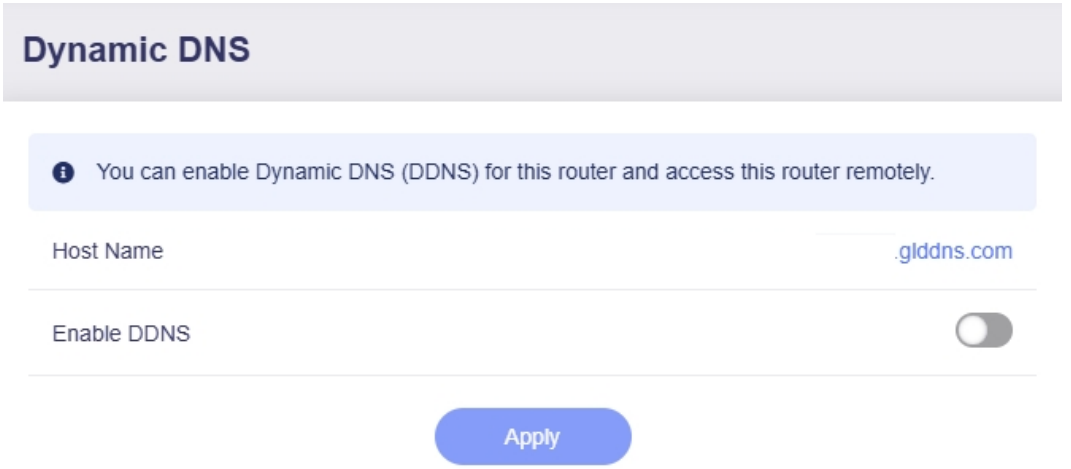
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

12.2 Dynamic DNS

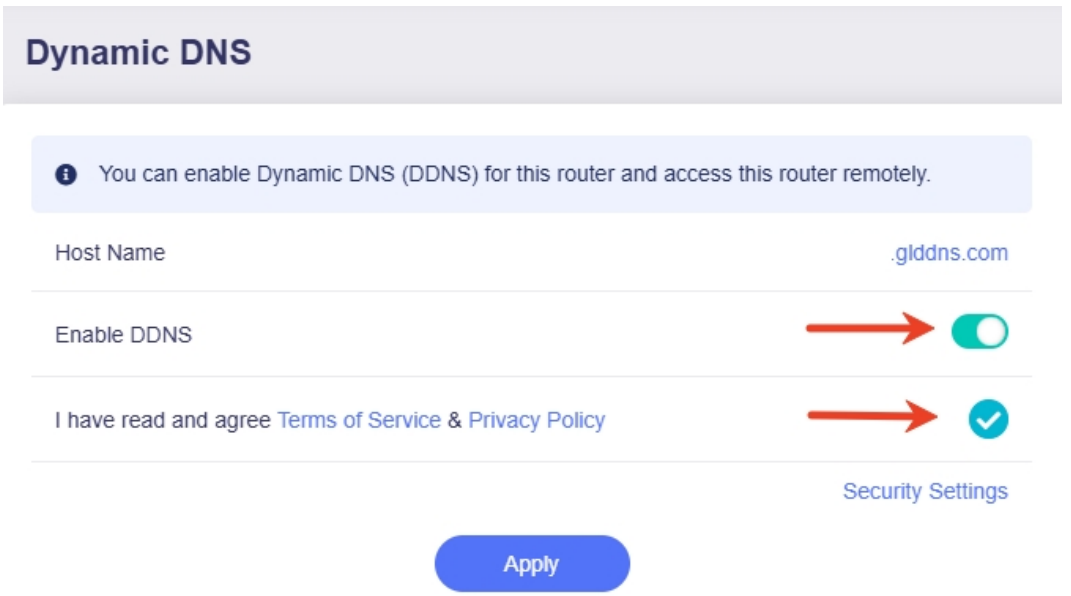
Dynamic Domain Name Service (DDNS, or Dynamic DNS) is a service used to map a domain name to the dynamic IP address of a network device. With Dynamic DNS, you can access your router remotely. A public IP address is required for this functionality.

12.2.1 Enable DDNS

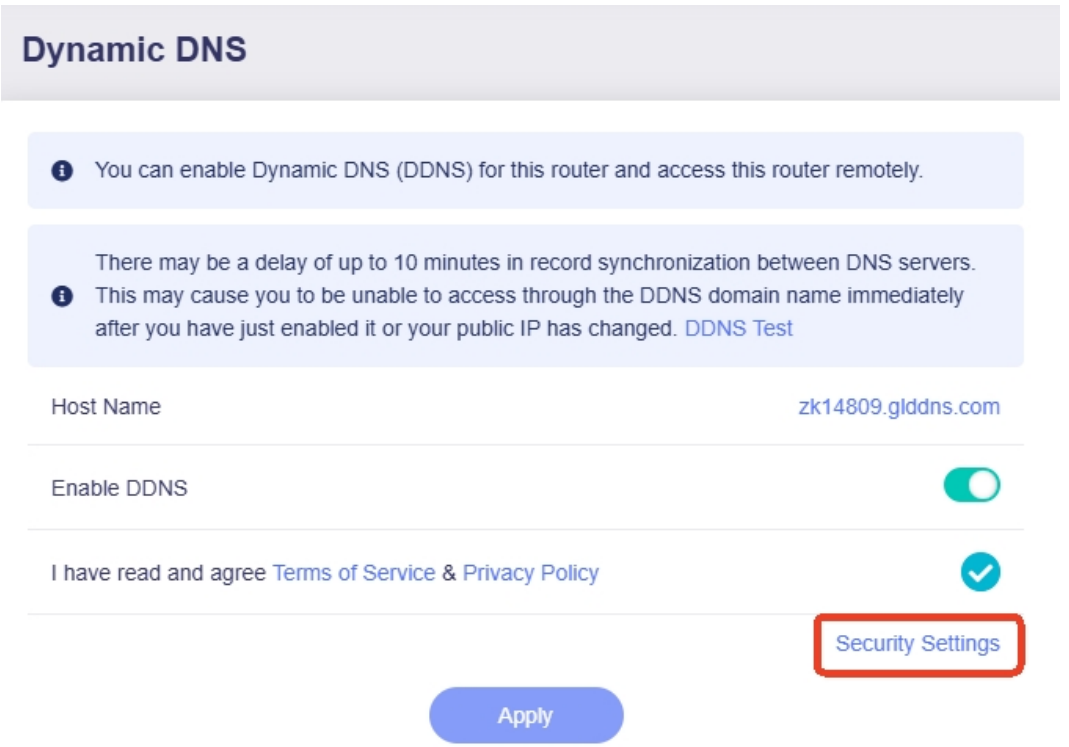
1. Log in to your router's web admin panel, navigate to **APPLICATIONS** > **Dynamic DNS**, the page is displayed as below.



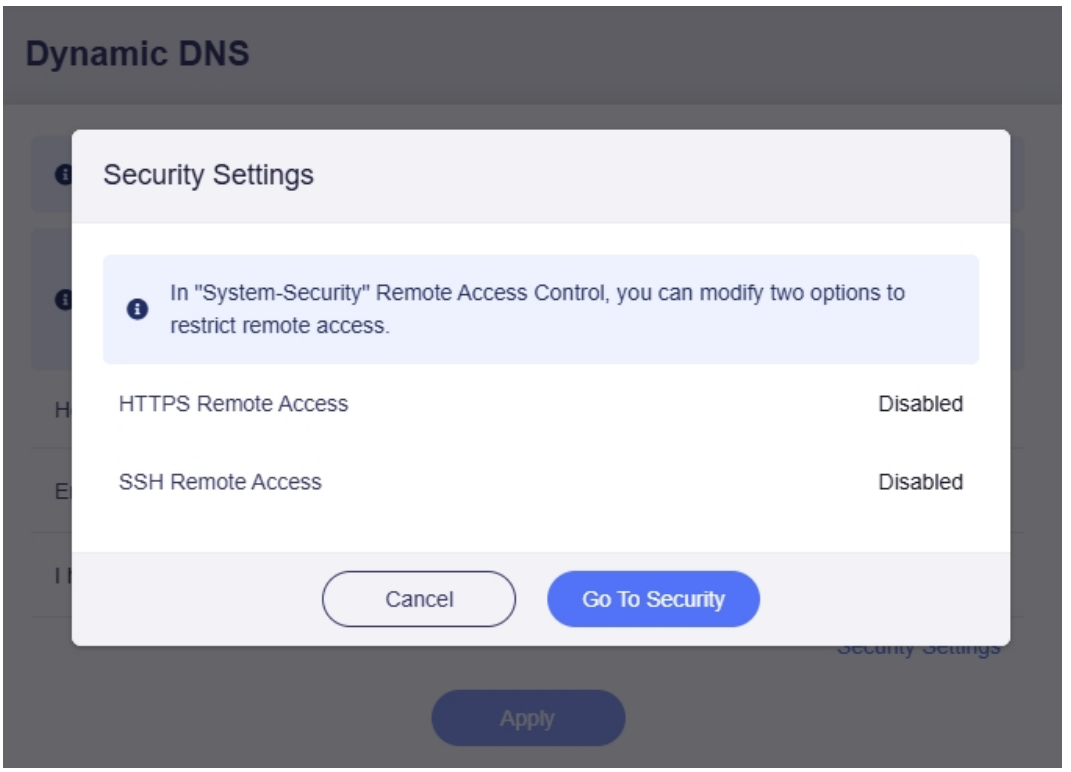
2. Toggle on **Enable DDNS**, read and agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



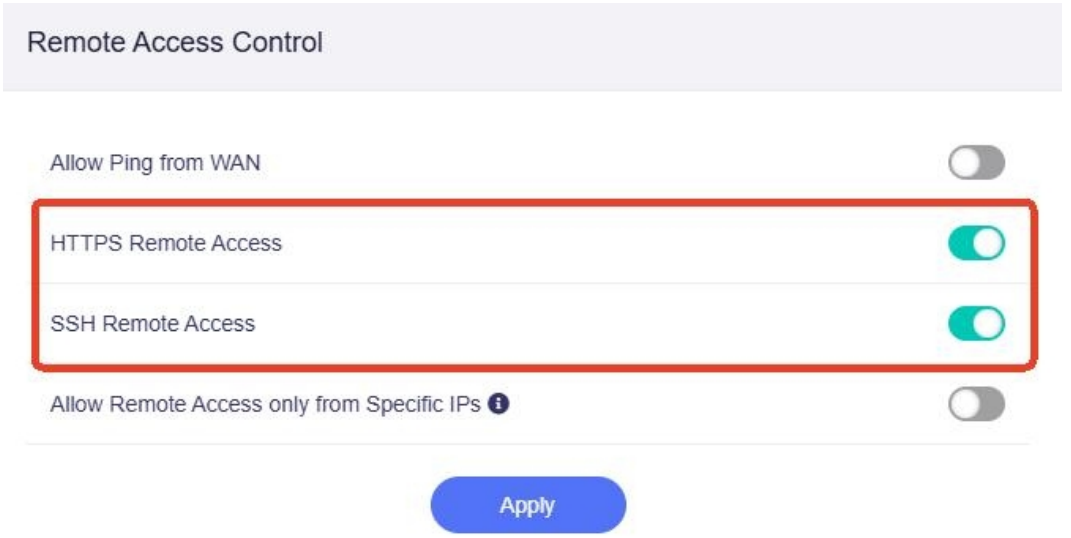
3. Click **Security Settings** in the bottom right corner.



4. In the pop-up window, check if the remote access you want to use is enabled.



If not, go to **Security** > **Management Control** > **Remote Access Control** to enable it, and click **Apply**.



Note:

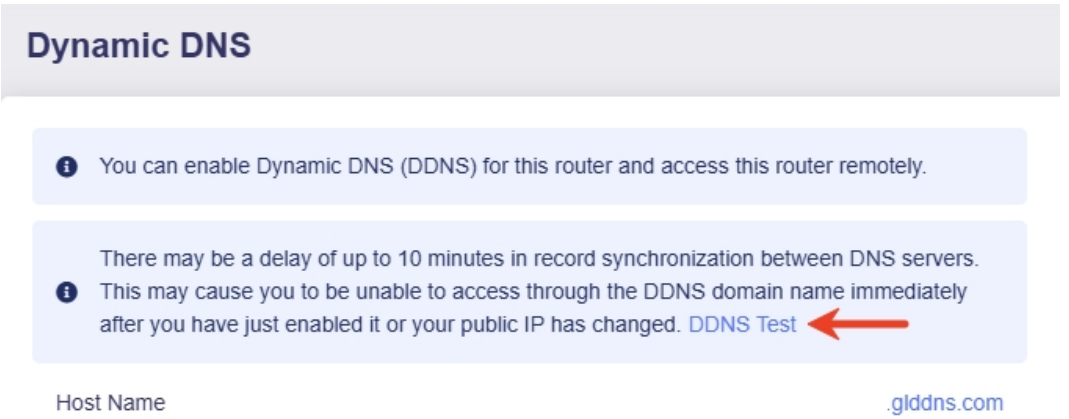
1. There may be a delay of up to 10 minutes in record synchronization between DNS servers. This may prevent you from accessing through the DDNS domain name immediately after enabling it or when your public IP changes.
2. If you enable DDNS and VPN Client at the same time, ensure that Services From GL.iNet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

12.2.2 Check if DDNS Works

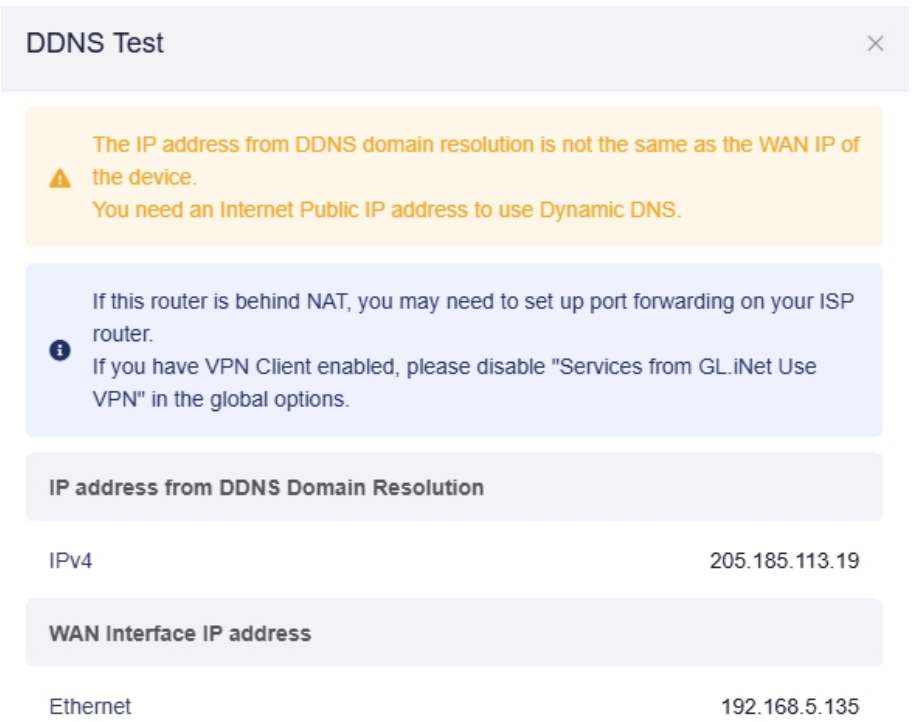
You can check if DDNS works using the DDNS test tool or manually via commands.

Method 1. Use DDNS Test tool

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

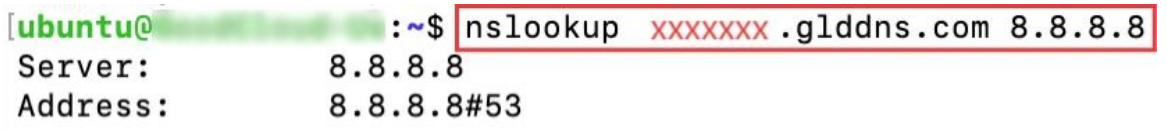


2. Make sure the IP address from DDNS domain resolution matches the router's WAN IP. If not, a yellow prompt will appear at the top, indicating that the router might be behind NAT, and you need to set up port forwarding on the upstream router.



Method 2. Use commands

1. Use **nslookup** command 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. You can use it or replace it with other DNS, then press Enter.

2. If you get a public IP address as an output, such as “103.81.180.10” in the image below, it indicates that your DDNS domain has been successfully mapped to a public IP address.

3. On a device connected to the router, search for “what is my ip address” in a browser, or visit a website like What Is My IP Address. You will get your public IP address. Compare the two IP addresses obtained from Step 1 and 2. If they are the same, the DDNS is in effect, otherwise it is not.

4. If you get a message “server can’t find xxxxxxx.glddns.com: NXDOMAIN”, as shown below, it indicates that domain resolution failed, and your DDNS domain has not been successfully mapped to a public IP address.

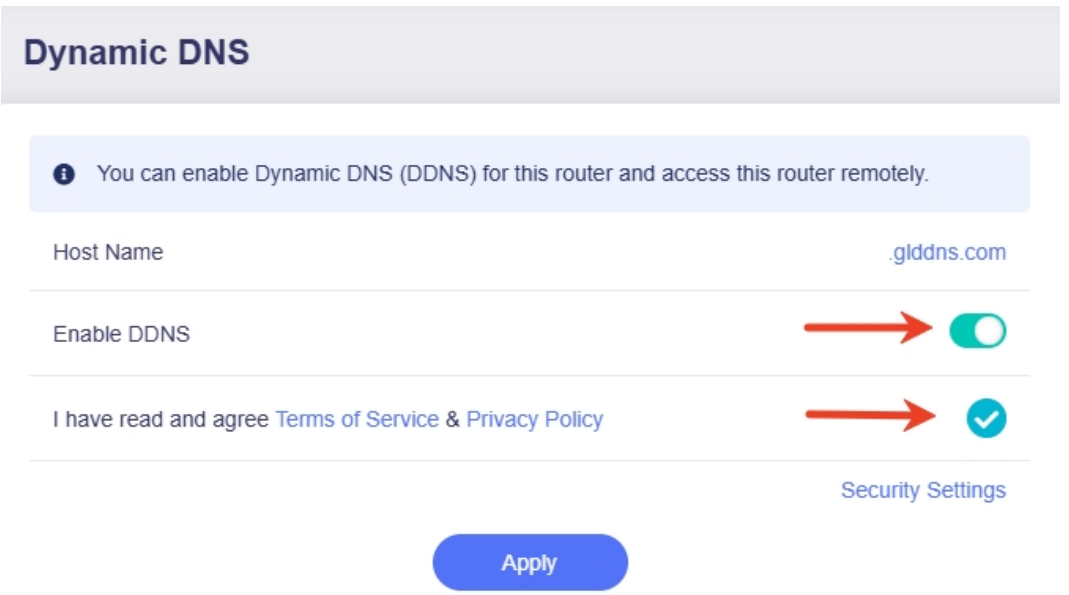
12.2.3 HTTPS Remote Access

A **Public IP address** is required for HTTPS remote access. See here to verify whether your ISP assigns you a public IP address.

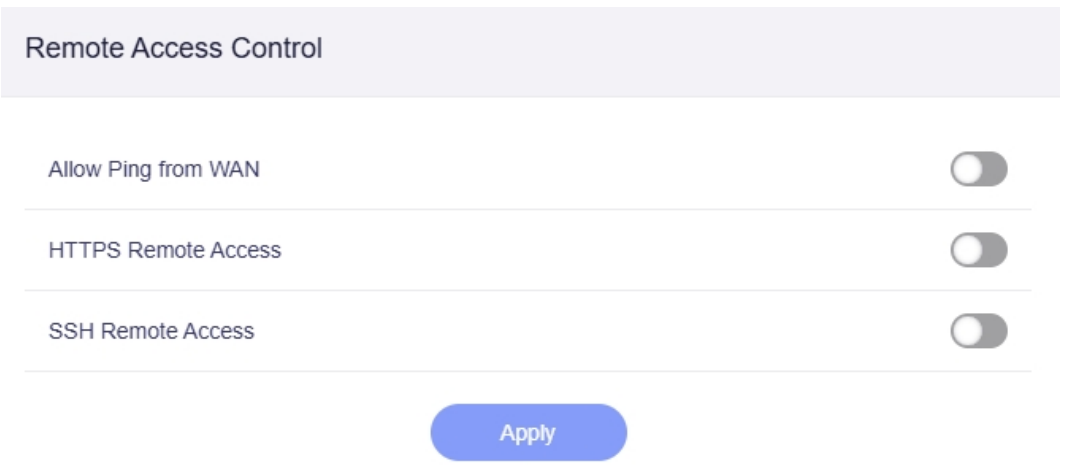
If your router is behind NAT, configure port forwarding (**port 443**) on the upstream router for HTTPS access.

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

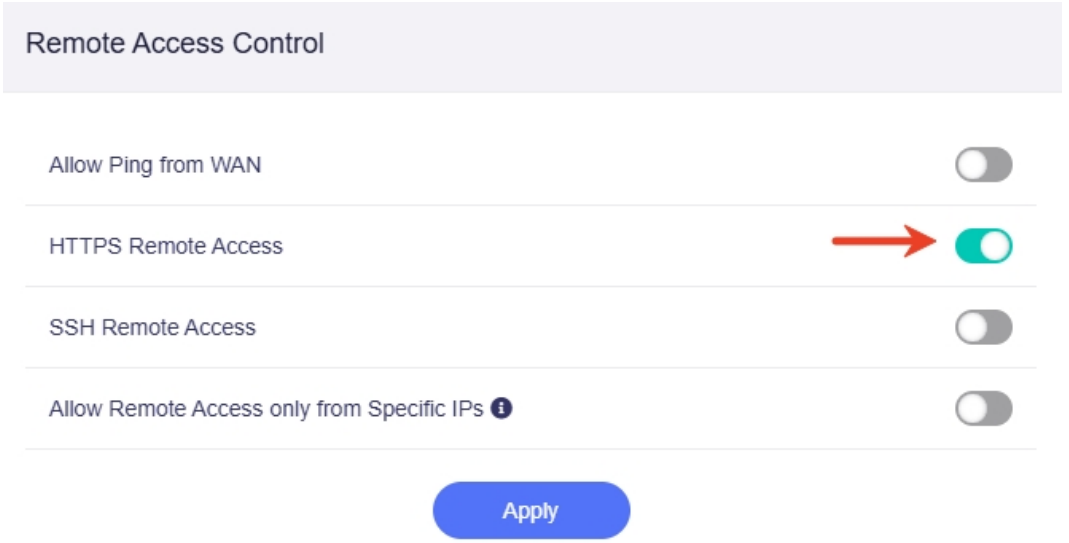
1. On the Dynamic DNS page, toggle on **Enable DDNS**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



2. In the web admin panel, go to **SYSTEM** > **Security** > **Remote Access Control**.

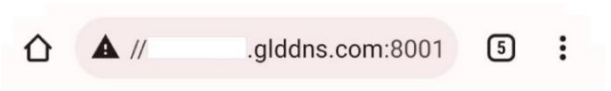


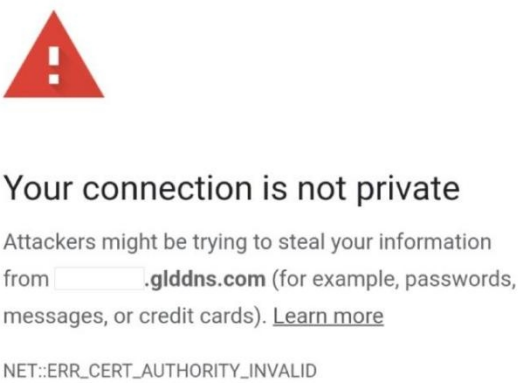
3. Enable **HTTPS Remote Access**, and click **Apply**.



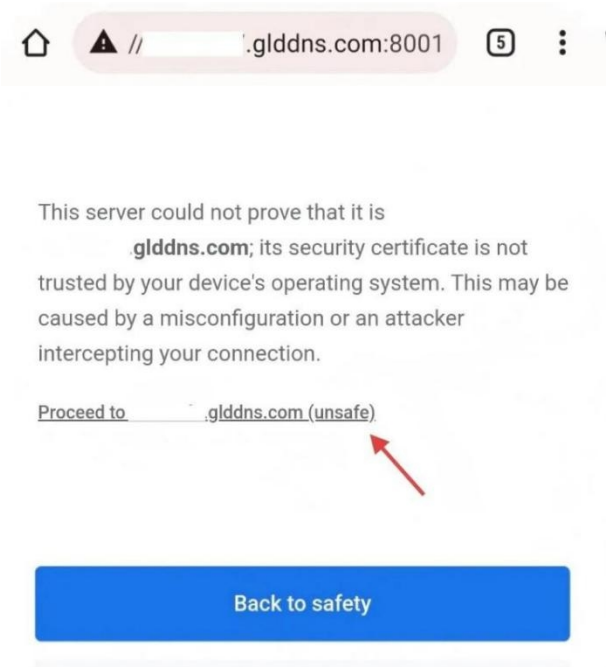
Once enabled, you can access the router's admin panel from anywhere using the DDNS host name over HTTPS, e.g., **https://xxxxxxx.glddns.com**. If port forwarding is configured, access it as **https://xxxxxxx.glddns.com:external_port** (replace the external_port with your actual port number).

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, as shown below (port 8001 is used as an example).





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**.

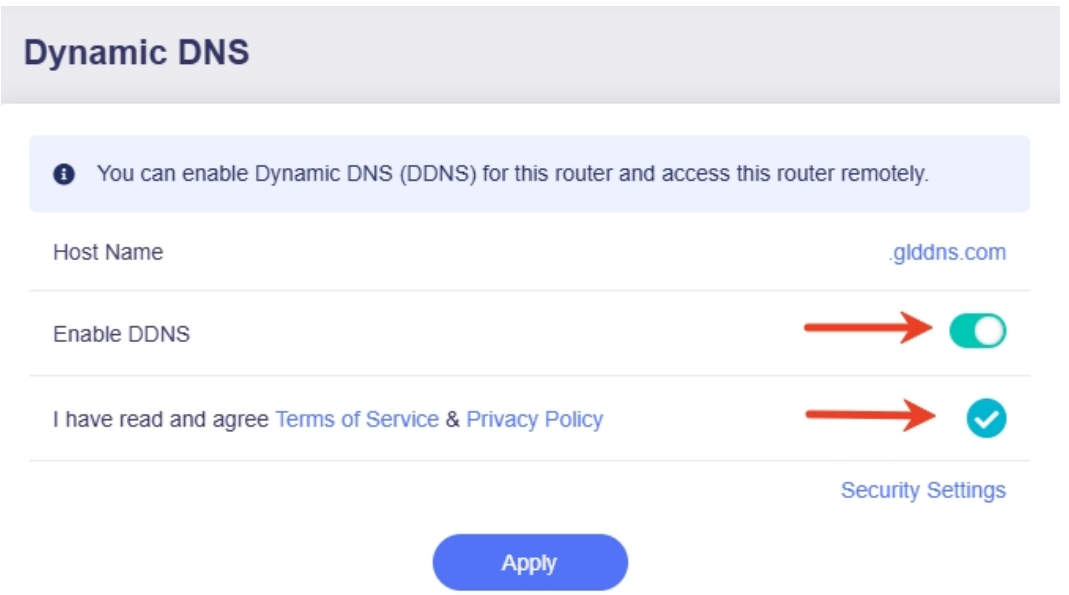
12.2.4 SSH Remote Access

A **Public IP address** is required for SSH remote access. See here to verify whether your ISP assigns you a public IP address.

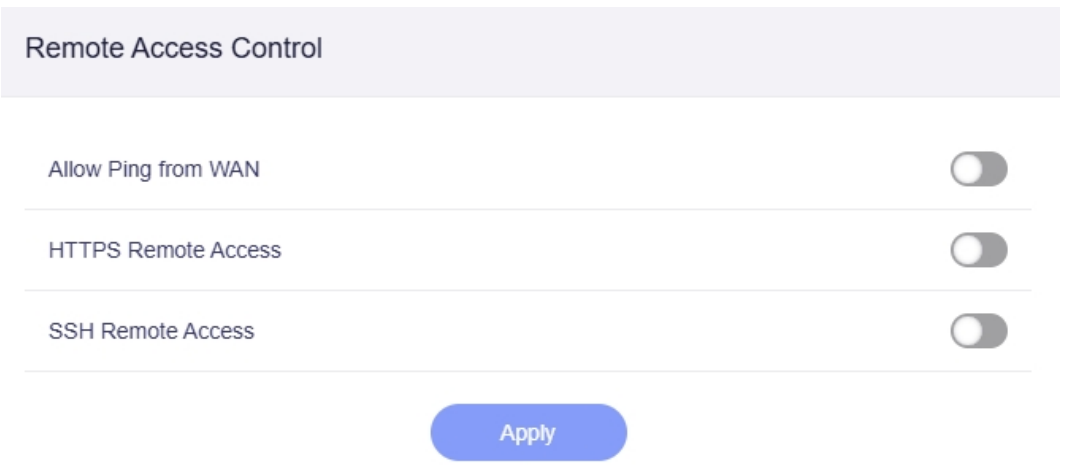
If your router is behind NAT, configure port forwarding (**port 22**) on the upstream router for SSH remote access.

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

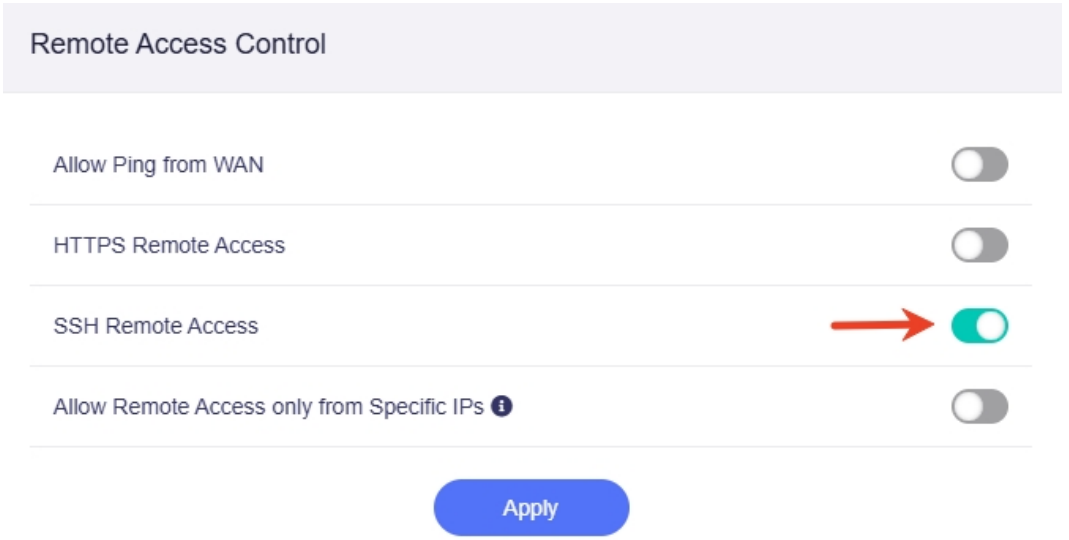
1. On the Dynamic DNS page, toggle on **Enable DDNS**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



2. In the web admin panel, go to **SYSTEM** > **Security** > **Remote Access Control**.



3. Enable **SSH Remote Access**, and 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).

12.3 Network Storage

Network storage enables file sharing across devices by connecting a USB drive or SD card to your router. The router converts the storage device into a shared network drive, accessible to all connected devices.

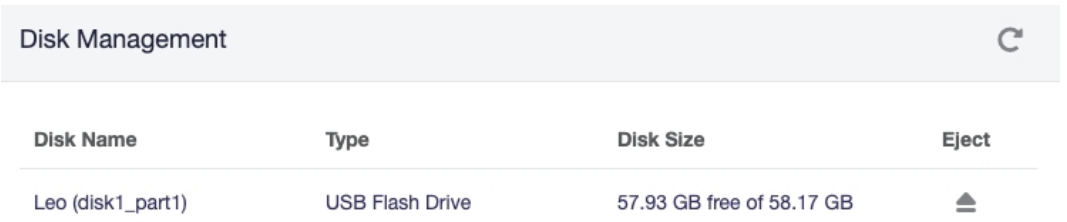
Among GL.iNet models, some support MicroSD (TF) cards, while others feature a USB port, compatible with USB flash drives and portable external hard drives. You can configure Samba, WebDAV, or DLNA for these storage devices, which support common formats such as NTFS, FAT32, and EXT4.

Note:

1. The power consumption of USB hard drive is quite high. Use it with an external power supply, otherwise it may cause malfunction.
2. Some models have USB Port or MicroSD slot but have limited storage space and do not support network storage.

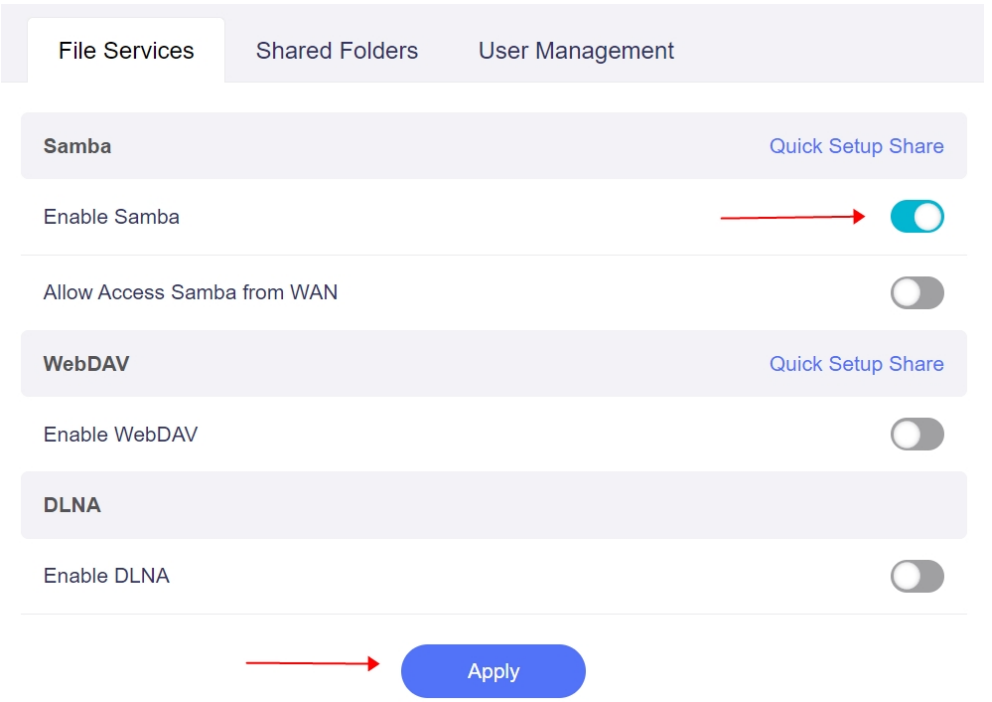
12.3.1 Connect Storage

1. Connect your storage device to the router.
   - For a TF card: Power off the router, insert the TF card, then power it on.
   - For a USB drive: Plug it directly into the USB port.
   - For an external hard drive: Connect it to a separate power supply (if required), then plug it into the router.
2. Log in to your router's web admin panel, navigate to **APPLICATIONS** > **Network Storage**. You can enable file transfer services, and manage the shared folder here.
3. If the storage device is detected, the **Disk Management** will be displayed as follows.



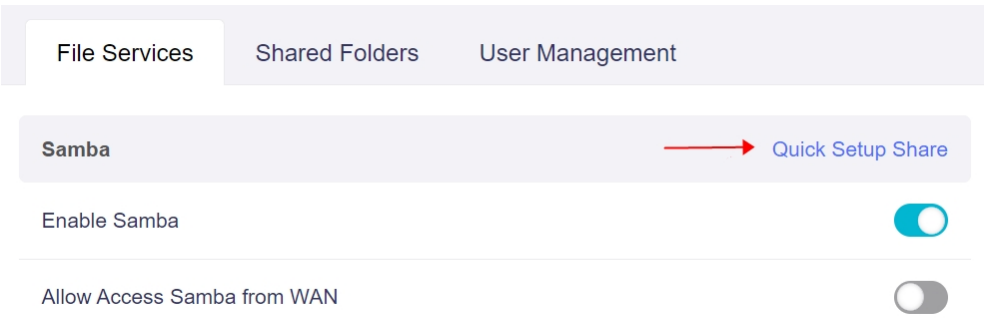
12.3.2 Set Up Samba

1. In the **File Services** section, toggle on **Enable Samba**, and click **Apply**.

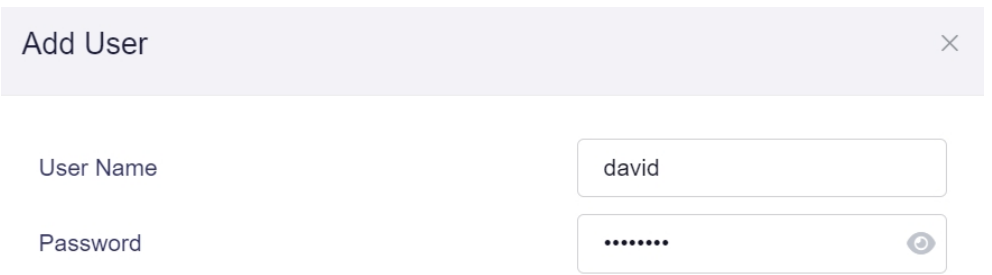


   - **Allow Access Samba from WAN**: Enable it if you want upstream devices to access the Samba service.

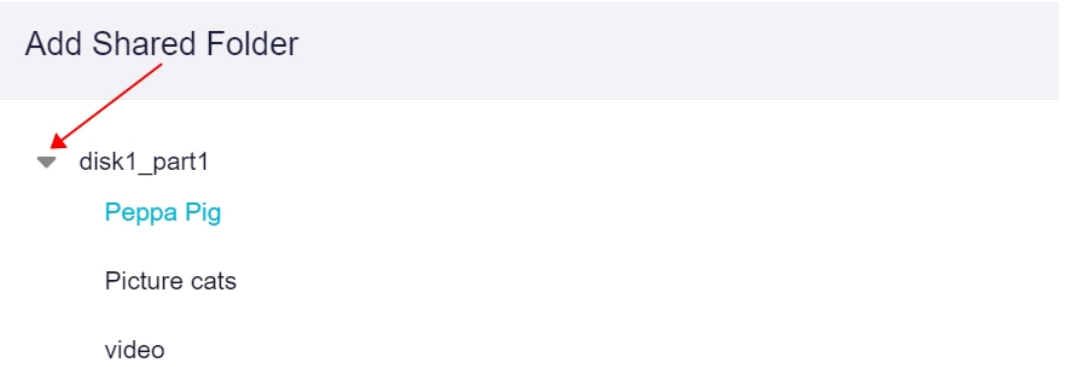
2. Click **Quick Setup Share** to set the shared link.



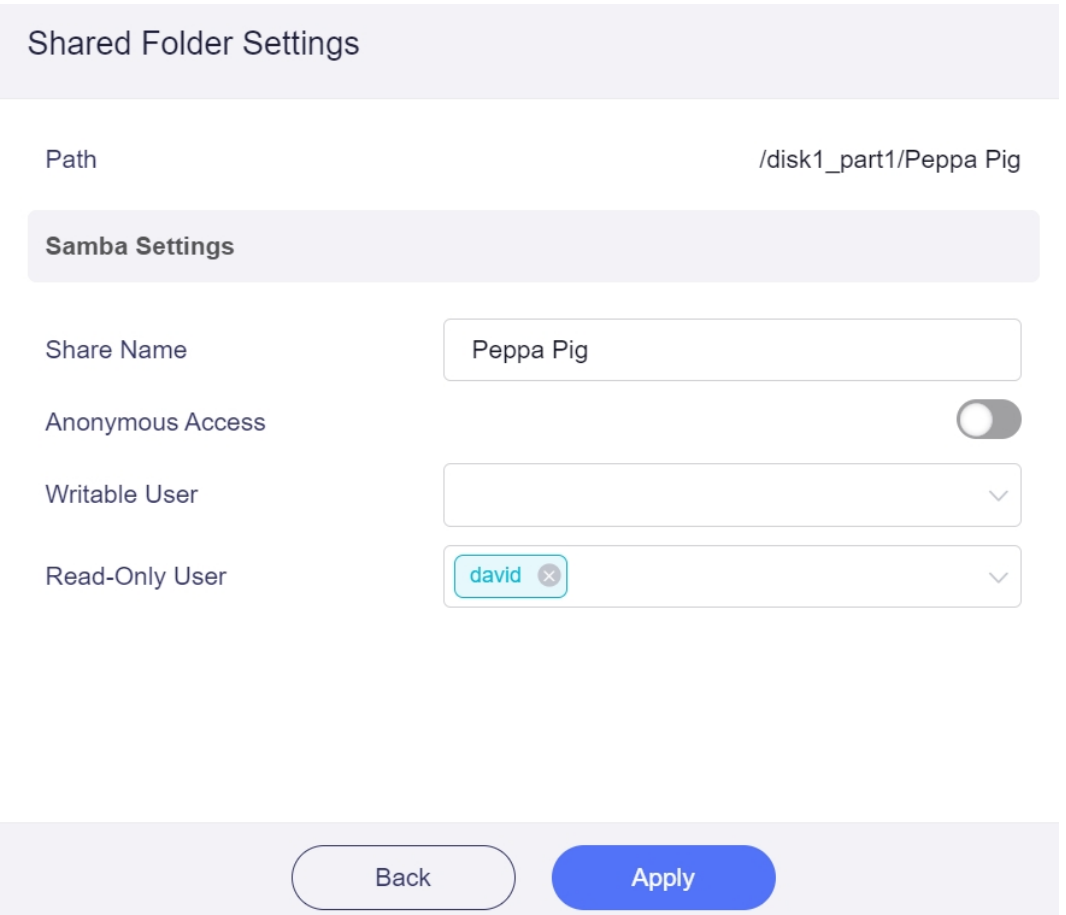
3. Add a user and click **Next**. This step will be skipped if you already have an account.



4. Click the triangle icon to show all folders. Select a folder for sharing, or click the disk name (e.g., disk1_part1) if you want to share the whole disk. Then click **Next**.

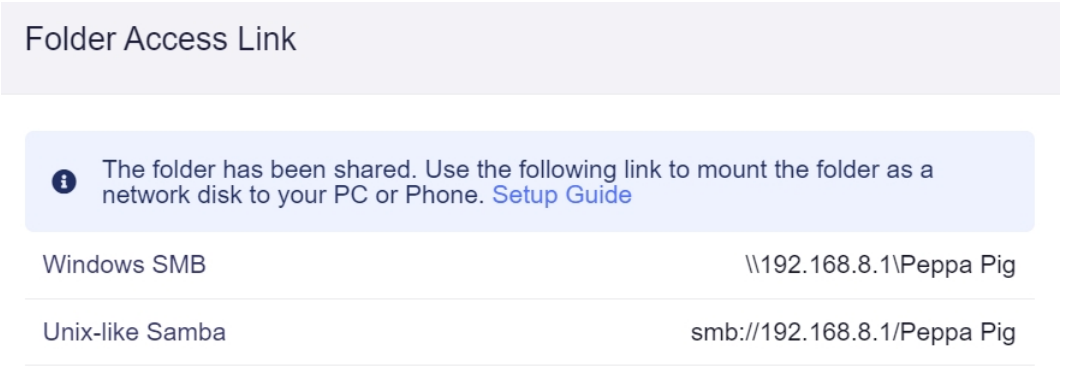


5. Set up the shared folder.
   For security reasons, it is not recommend to enable Anonymous Access.
   The user created in the previous step will be added to **Read-Only User** by default. If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Writable User**, then click **Apply**.



6. Obtain the folder access link.

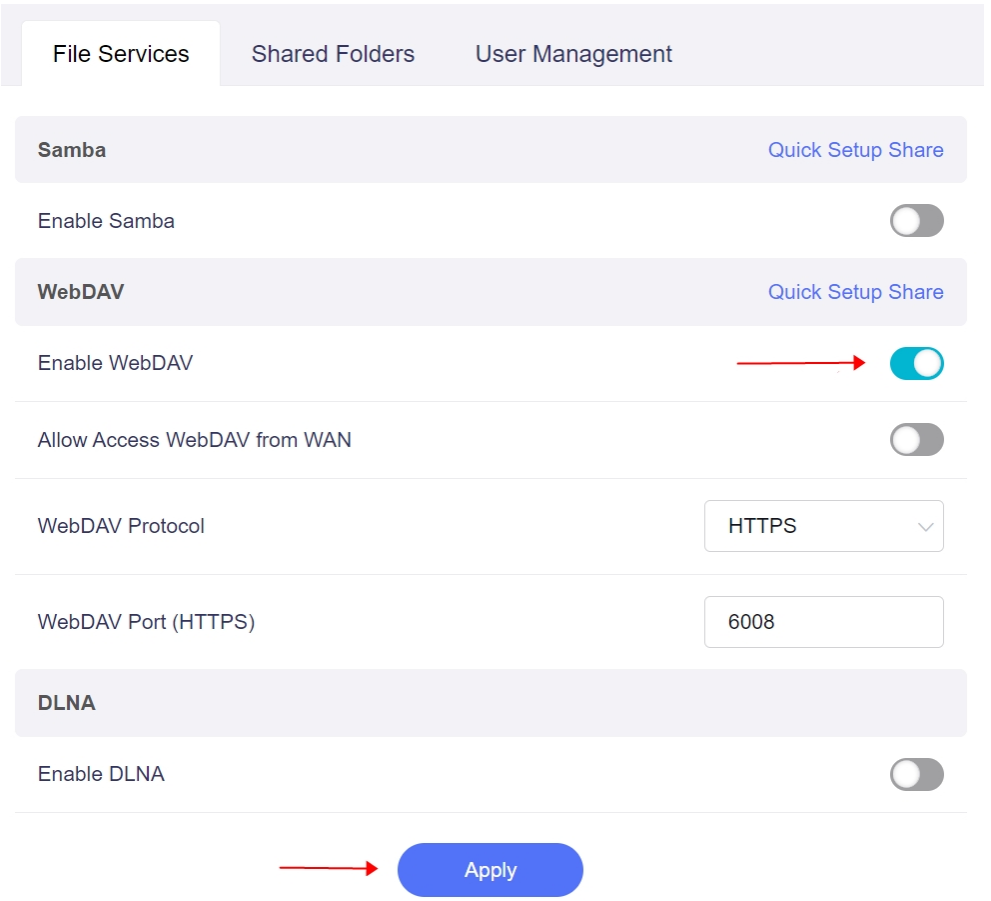
   The page will display the links for Windows and Unix-like OS. The Unix-like system includes Android, iOS, macOS, Ubuntu, etc. Now you can access your shared folder over Samba service via these links.



Note: If you enable **Allow Access Samba from WAN** and access the shared folder from upstream network, replace the router IP (default: 192.168.8.1) in the access link with your router's WAN IP, which can be found on the INTERNET page of the web admin panel.

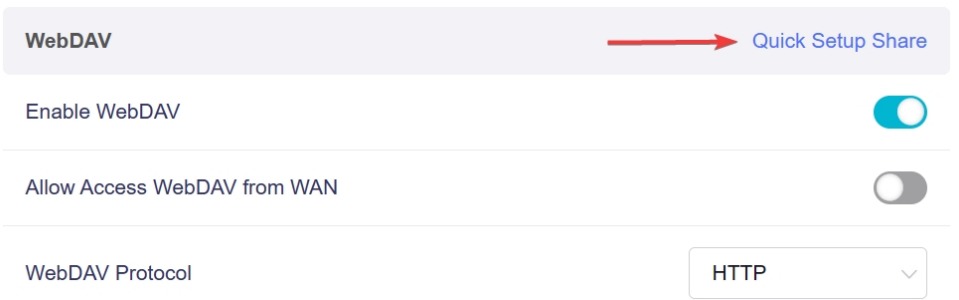
12.3.3 Set Up WebDAV

1. In the **File Services** section, toggle on **Enable WebDAV**, and click **Apply**.

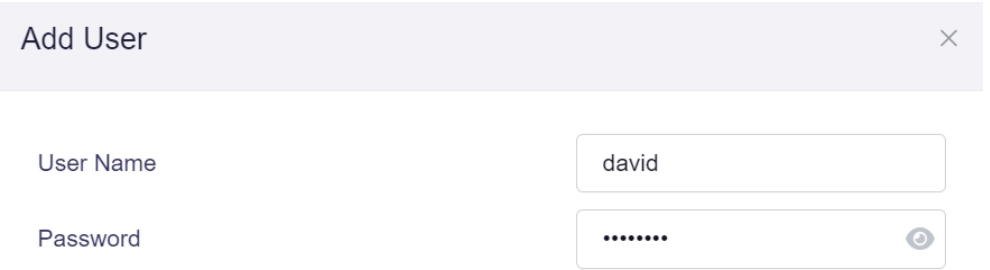


- **Allow Access WebDAV from WAN**: Enable it if you want the upstream devices to access the WebDAV service.
- **WebDAV Protocol**: HTTP is unencrypted; use it at your own risk. HTTPS is encrypted and it uses self-signed certificate.
- **WebDAV Port**: No need to modify the port number unless there's a conflict. The recommended port number range is 1024 - 65535.

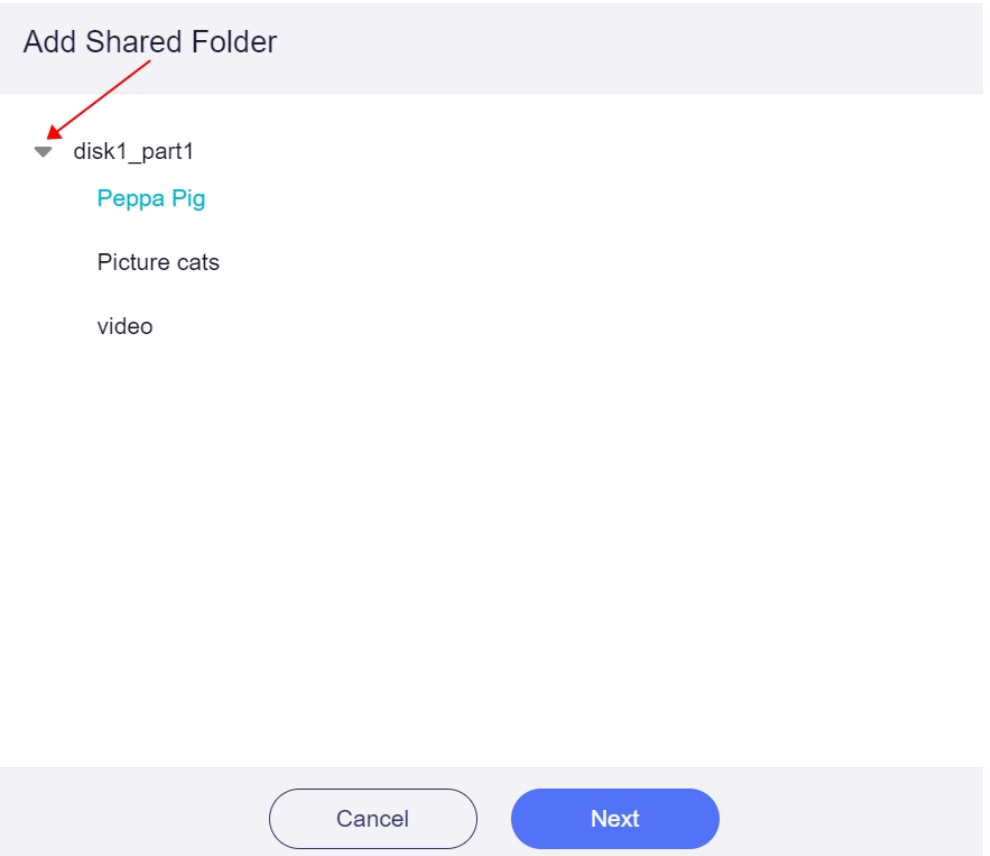
2. Click **Quick Setup Share** to set the shared link.



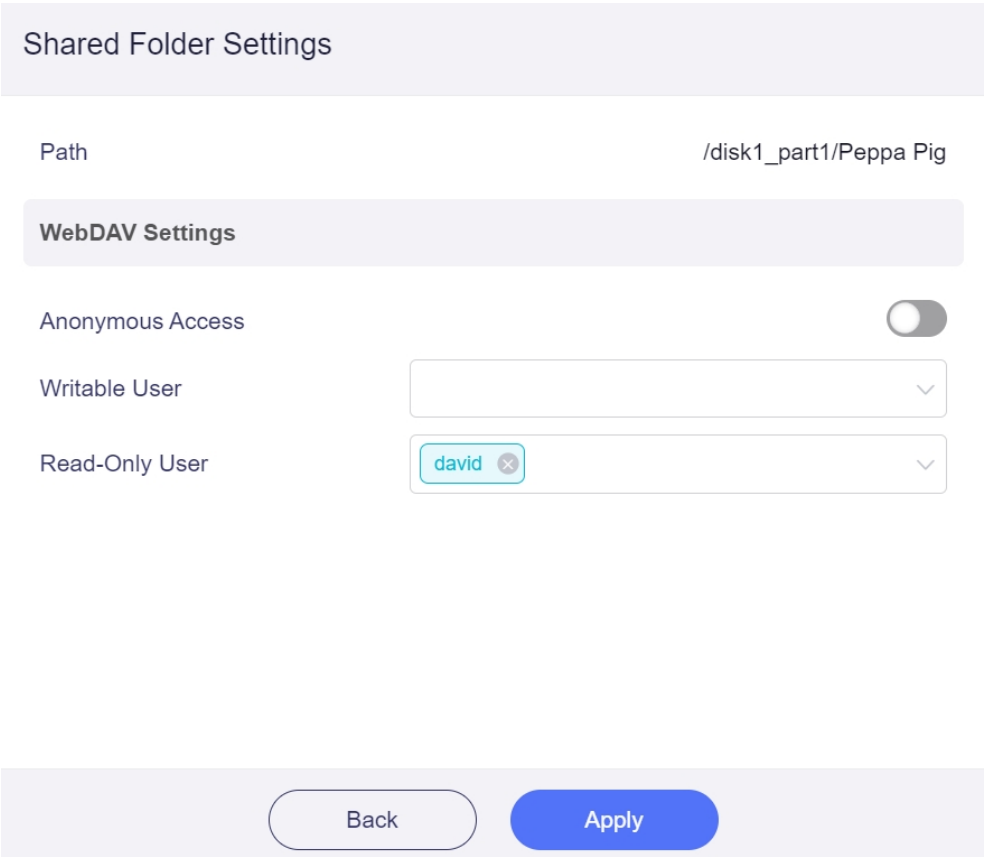
3. Add a user and click **Next**. This step will be skipped if you already have an account.



4. Click the triangle icon to show all folders. Select a folder for sharing, or click the disk name (e.g., disk1_part1) if you want to share the whole disk. Then click **Next**.

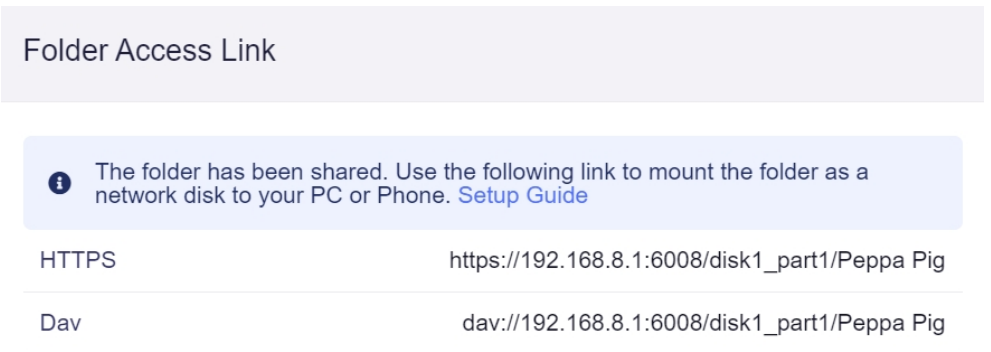


5. Set up the shared folder.
   For security reasons, it is not recommend to enable Anonymous Access.
   The user created in the previous step will be added to **Read-Only User** by default.
   If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Writable User**, then click **Apply**.



6. Obtain the folder access link.

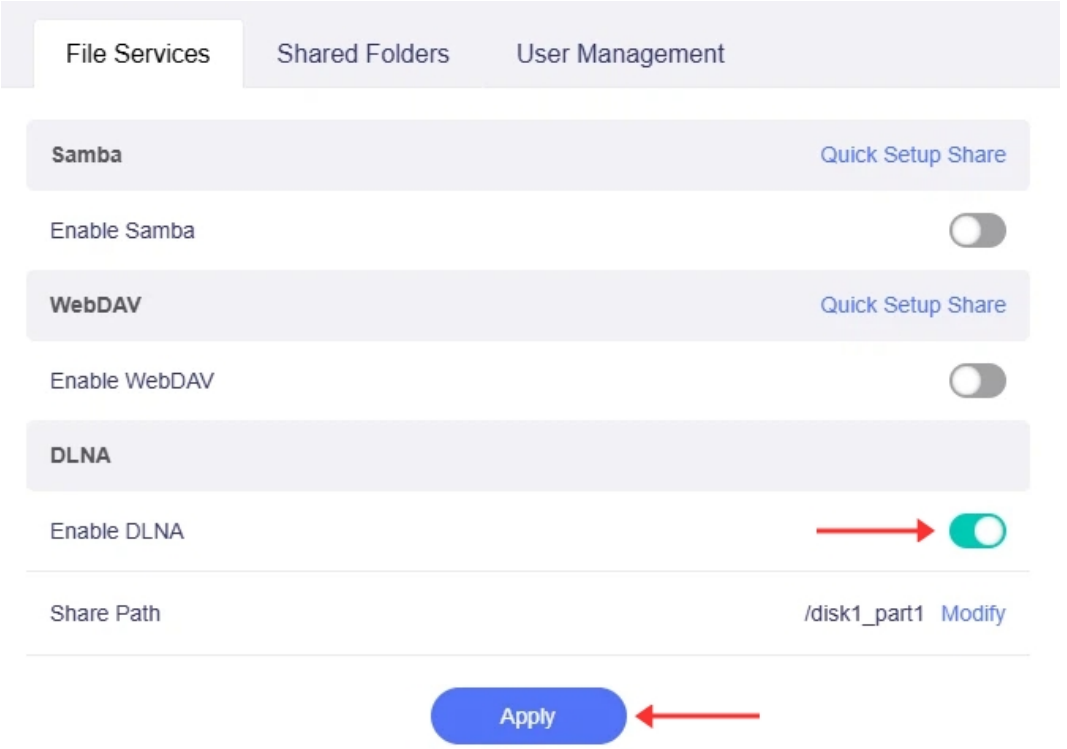
   The page will display the links for Windows and Unix-like OS. The Unix-like systems includes Android, iOS, macOS, Ubuntu, etc. Now you can access your shared folder over WebDAV service via these links.



Note: If you enable **Allow Access WebDAV from WAN** and access the shared folder from upstream network, replace the router IP (default: 192.168.8.1) in the access link with your router's WAN IP, which can be found on the INTERNET page of the web admin panel.

12.3.4 Set Up DLNA

1. In the **File Services** section, toggle on **Enable DLNA**, and click **Apply**.



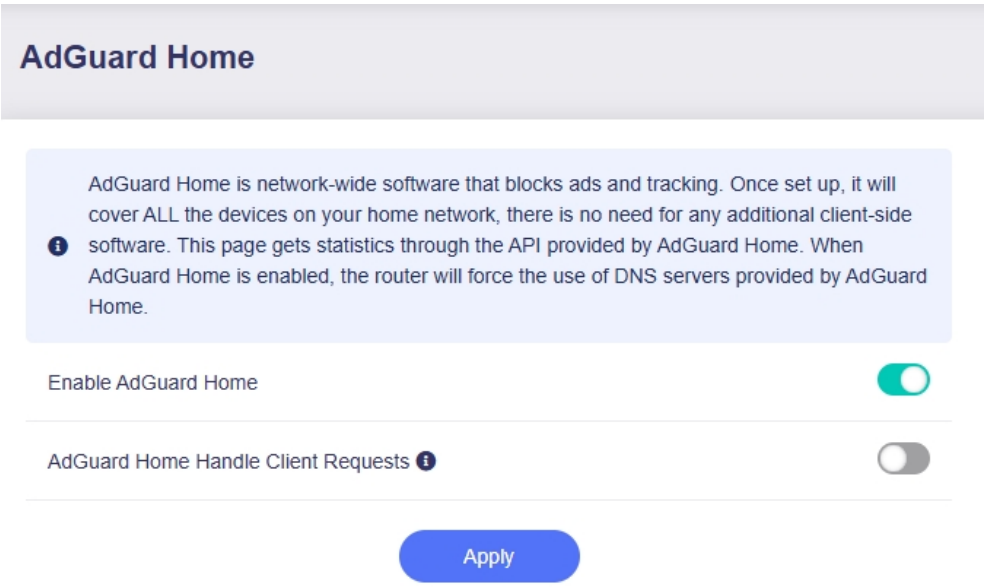
2. Connect your smart TV to the router, and it will find the DLNA Server.

12.4 AdGuard Home

AdGuard Home is a network-wide ad-blocking and tracking-prevention software. Once set up, it will cover all client devices with no additional client-side software required.

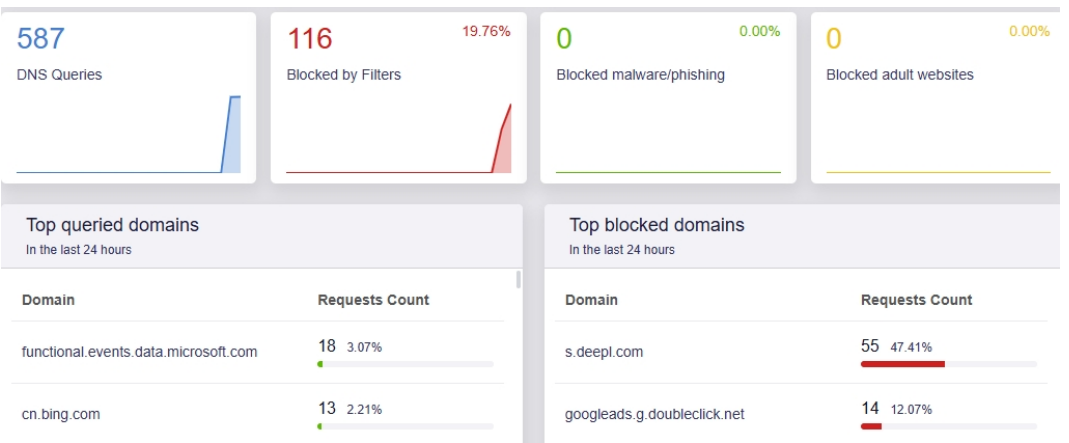
Follow these steps to set up AdGuard Home.

1. Log in to the router's web admin panel, navigate to **APPLICATIONS** > **AdGuard Home**. Toggle on **Enable AdGuard Home** and click **Apply**.

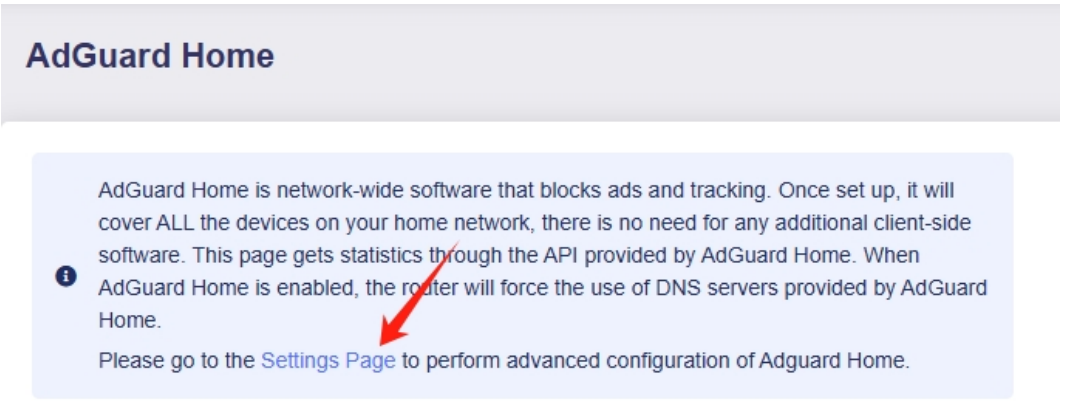


   - **AdGuard Home Handles Client Requests**: If enabled, DNS queries from client devices will be handled directly by AdGuard Home, but this will cause VPN policies based on domains to fail.

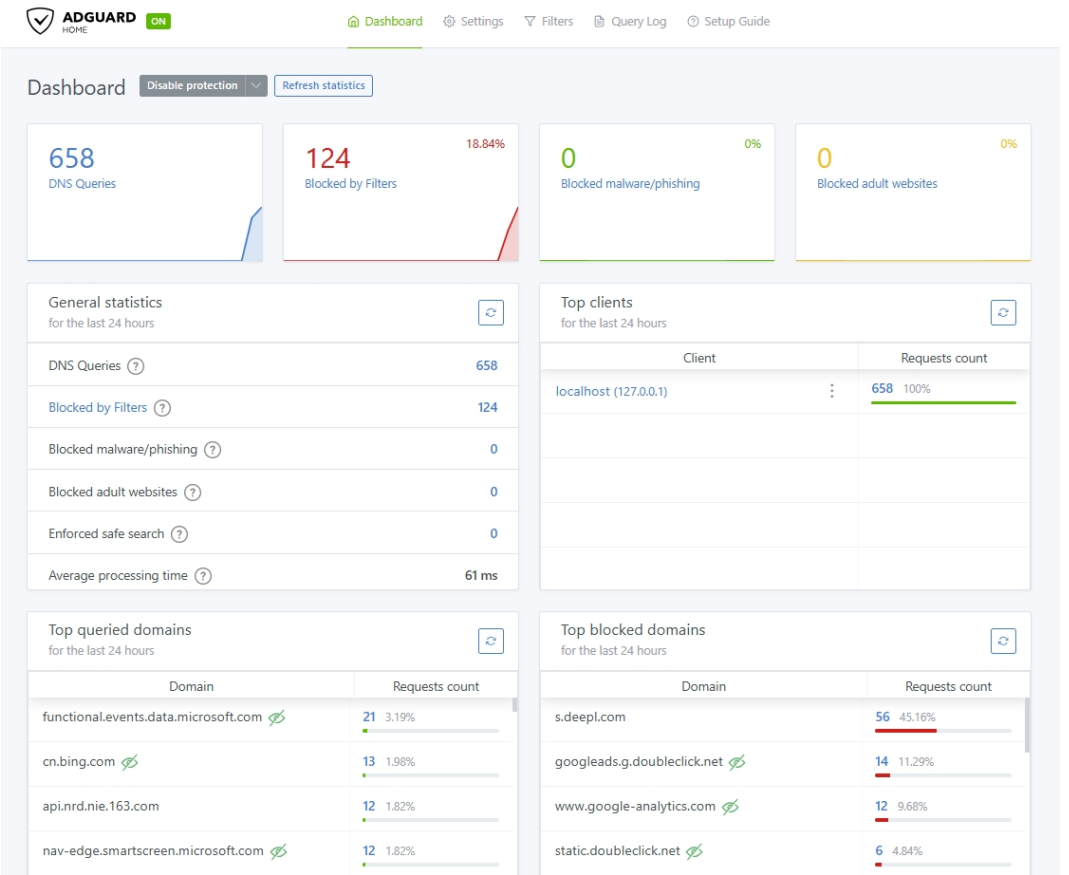
2. The page will automatically load DNS statistics (queries, blocked domains, etc.) via the API provided by AdGuard Home.



3. Click **Settings Page** to configure advanced settings for AdGuard Home.



4. You will be redirected to AdGuard Home's settings page. Please visit the [AdGuard Home Support Center] for assistance.



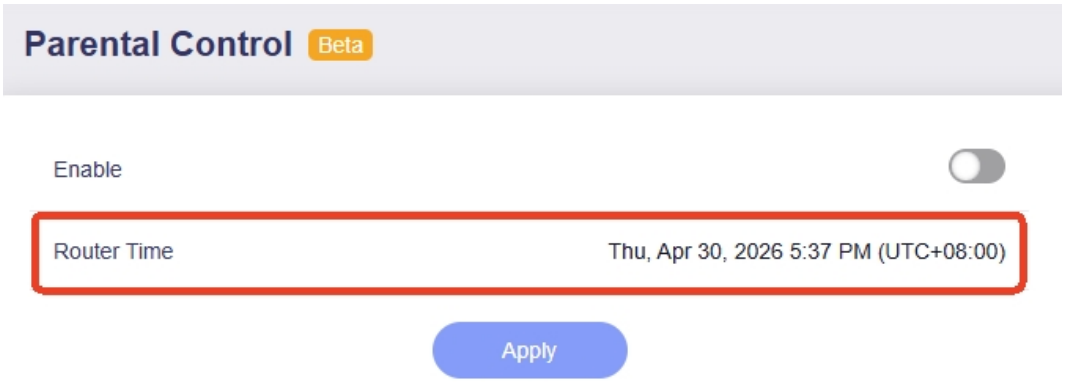
12.5 Parental Control

Parental control is a way to keep children safe online by blocking inappropriate websites and limiting how long they use devices. It helps prevent access to harmful content, manage screen time, and ensure children use the internet responsibly.

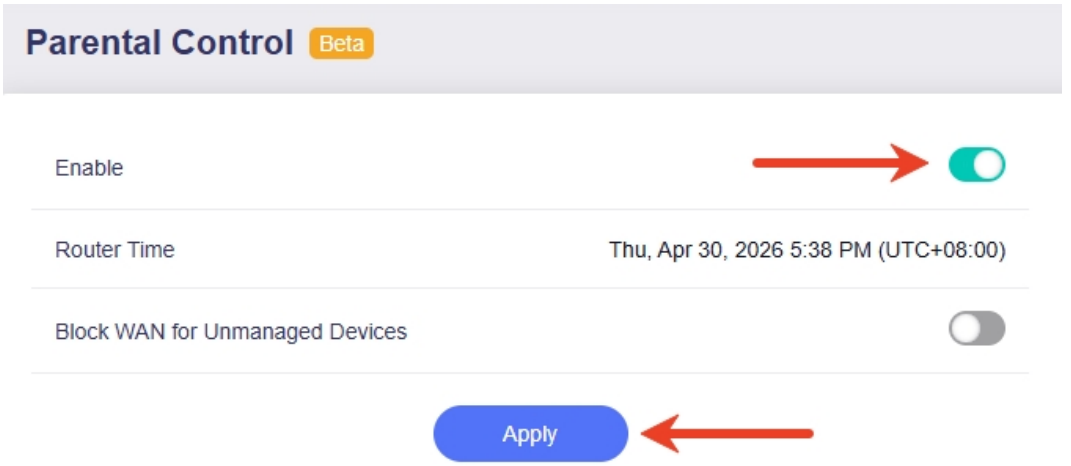
12.5.1 Quick Setup

Follow these steps to set up Parental Control on GL.iNet routers.

1. Log in to the router's web admin panel and go to **APPLICATIONS** > **Parental Control.** Ensure the router time is accurate. If not, go to **SYSTEM** > **Time Zone** to synchronize it first.



2. Enable Parental Control and click **Apply**. Then follow the setup wizard to set up Parental Control. You can also watch the setup video here.



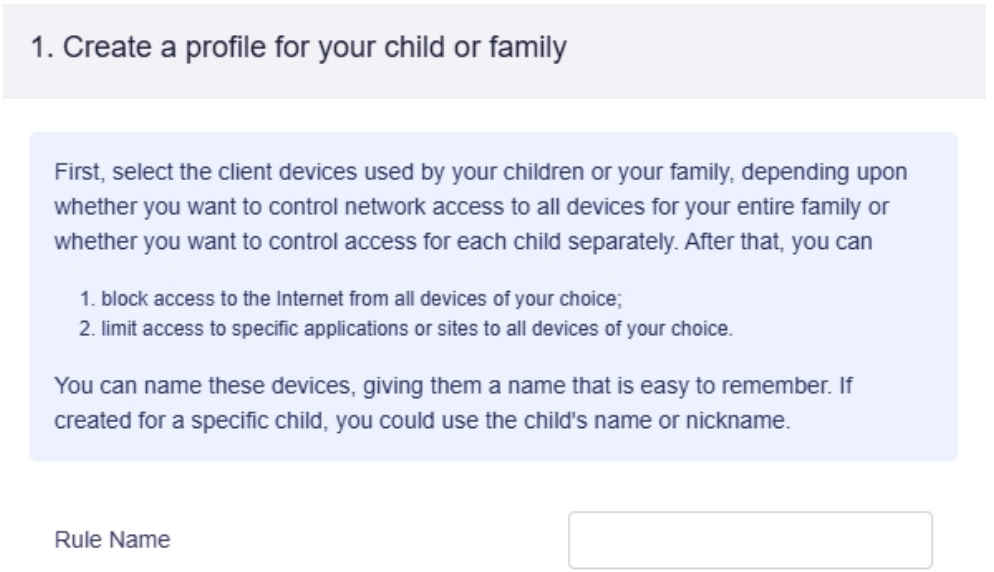
- **Block WAN for Unmanaged Devices**: Blocks internet access for all devices that are not on the Parental Control list.

Here is a use case for your reference.

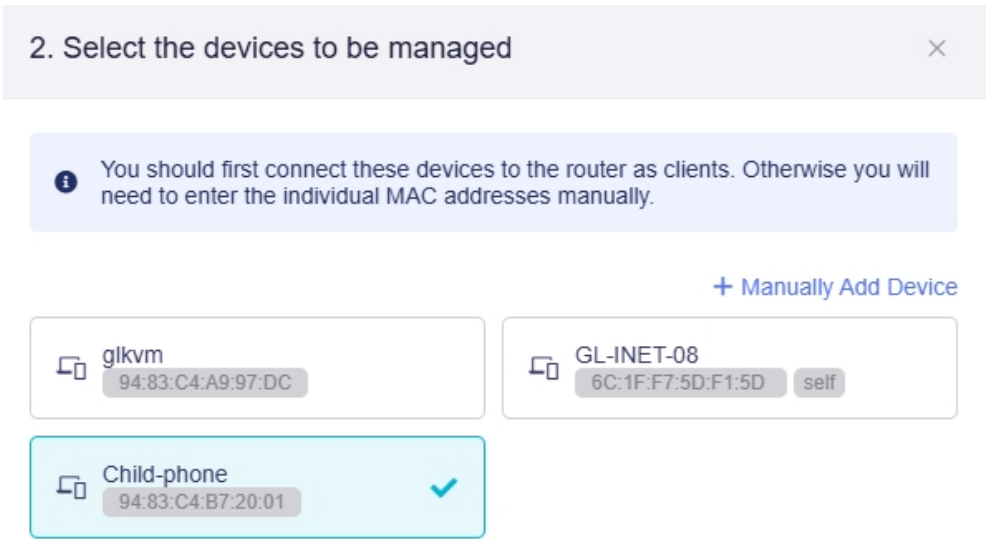
Scenario: Devices in this profile are only allowed to access the Internet for study from 8 AM to 11 AM on weekdays, and for gaming from 6 PM to 8 PM on weekends. Internet access is blocked by default at all other times.

Setup Steps:

1. Create a profile and customize a name.



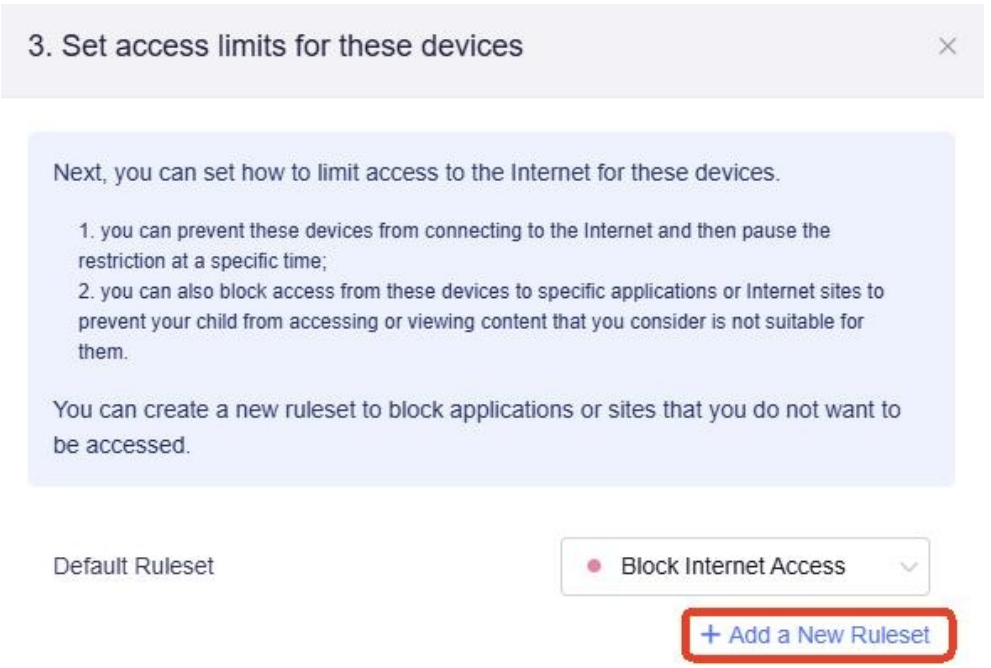
2. Select the devices you want to manage. Connect them to the router first. If they have not been connected to the router, add them manually by entering their MAC addresses.



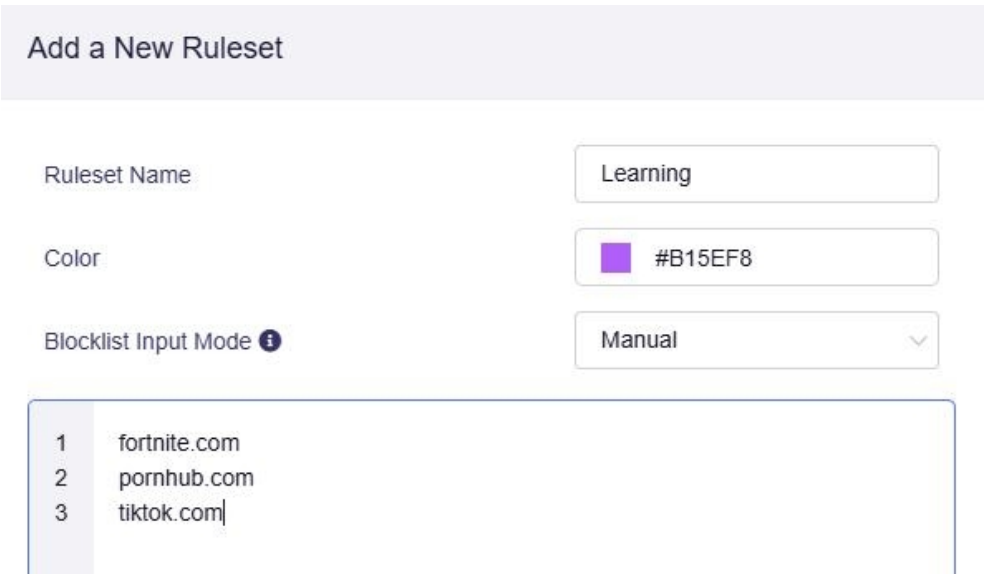
3. Set access limit.

   There are two default rulesets: **Block Internet Access** and **No Limit**.

Click **Add a New Ruleset** to create two more rulesets for later use: **Learning** and **Play**.

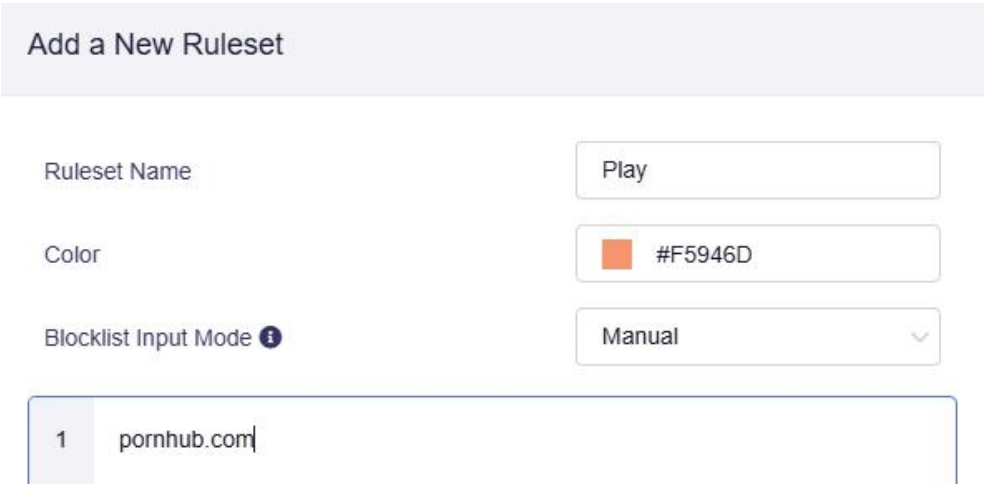


Specify the ruleset name (e.g., Learning) and color, enter the websites to block, then click **Apply**.

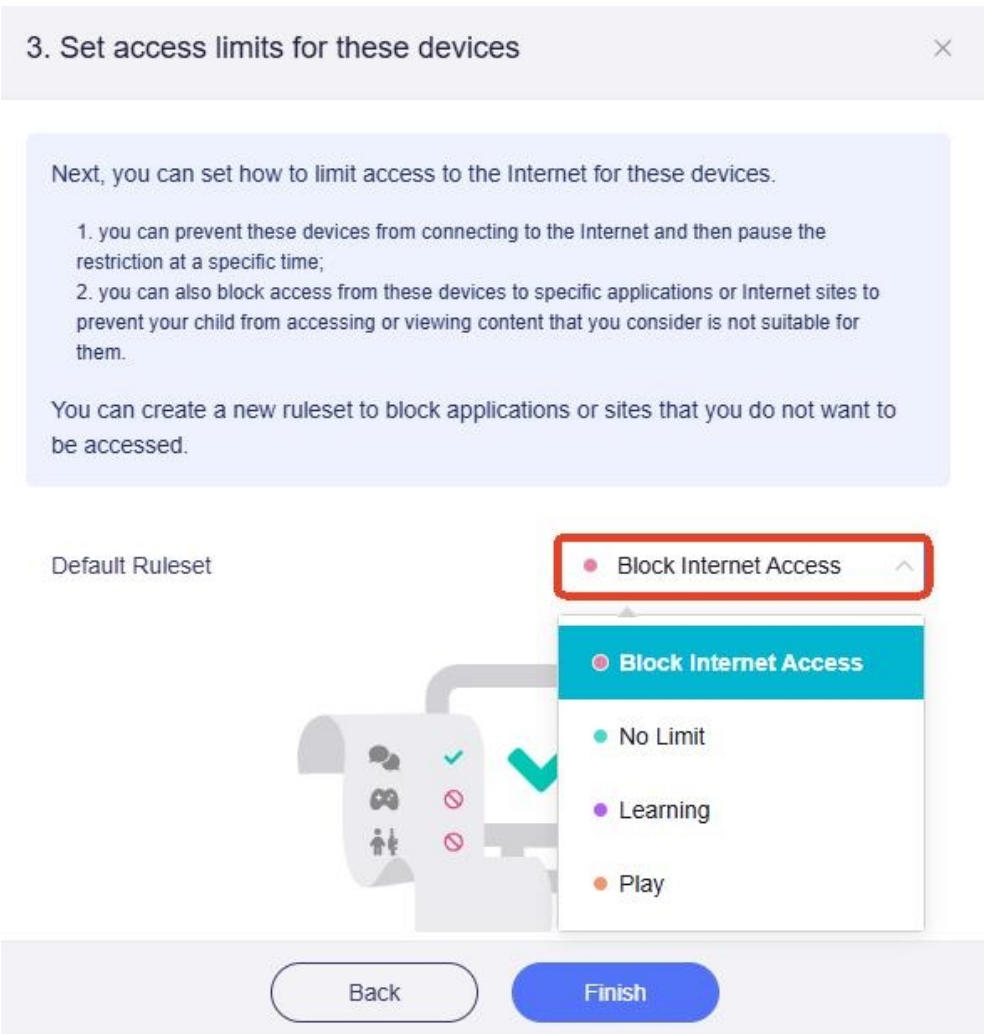


Note: The domain names entered in the blocklist should include their subdomains. For example, if "example.com" is entered, it also includes any subdomain, such as "subdomain.example.com".

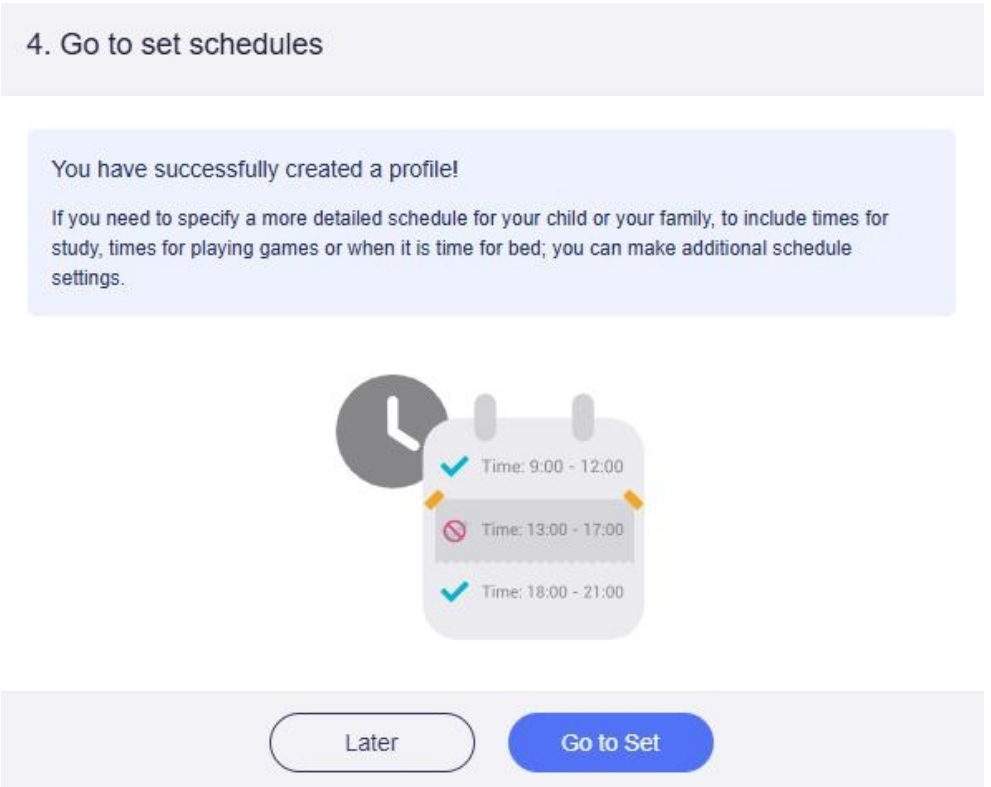
Similarly, create another ruleset. Specify the ruleset name (e.g., Play) and color, enter the websites to block, then click **Apply**.



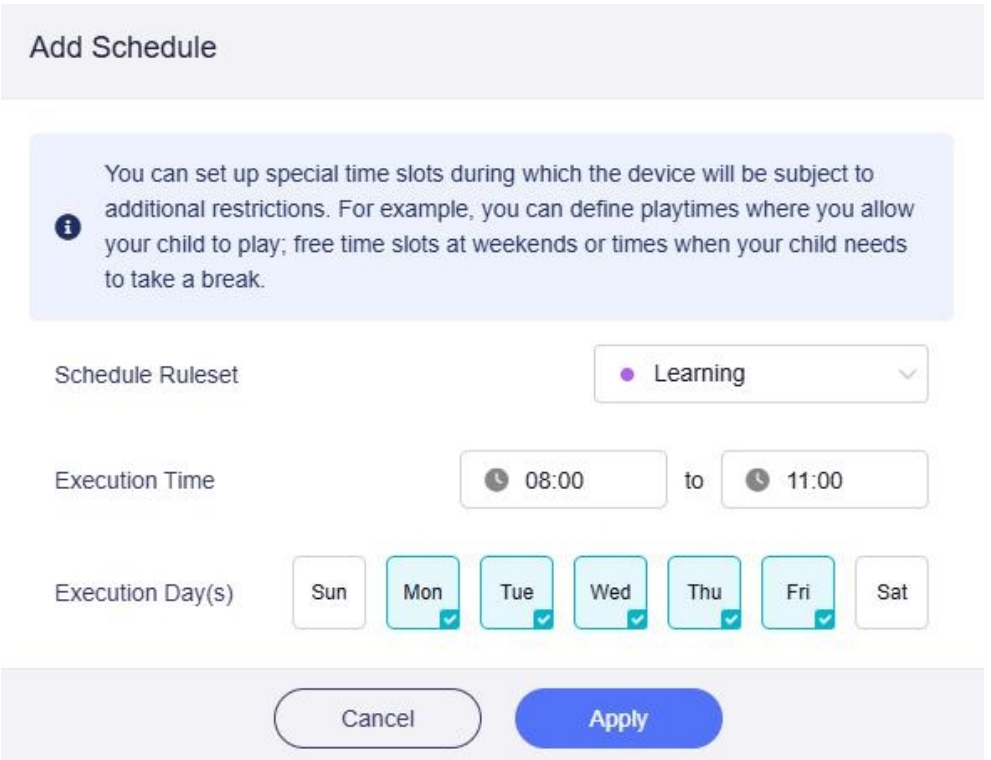
Upon applied, there will be a total of four rulesets. Select **Block Internet Access** as the **Default Ruleset**, and click **Finish**.



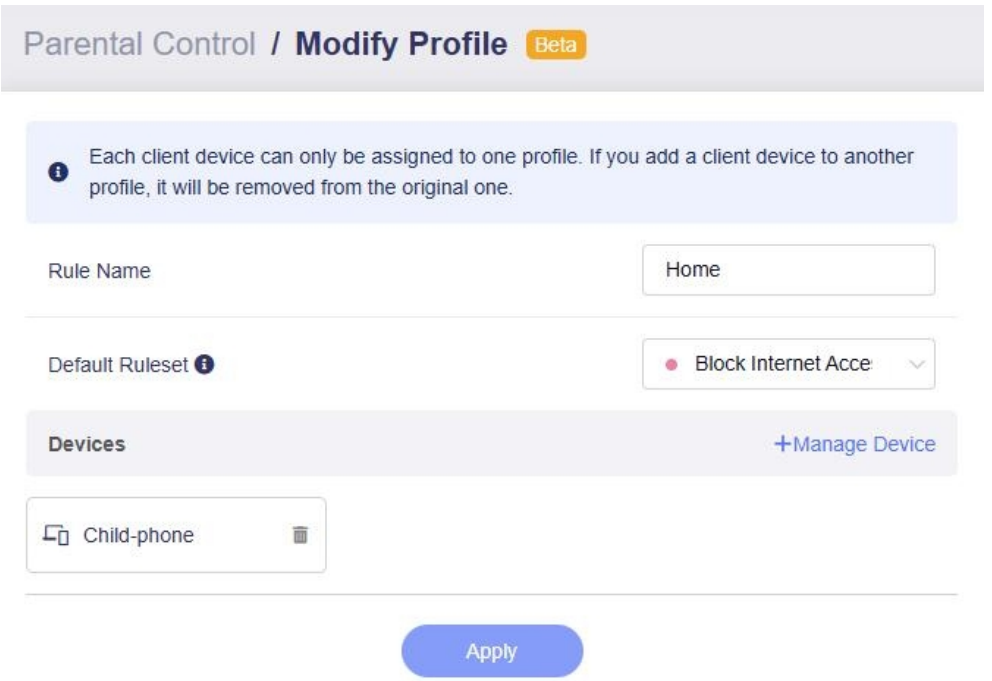
4. Next, set schedule for your profile. Click **Go to Set**.



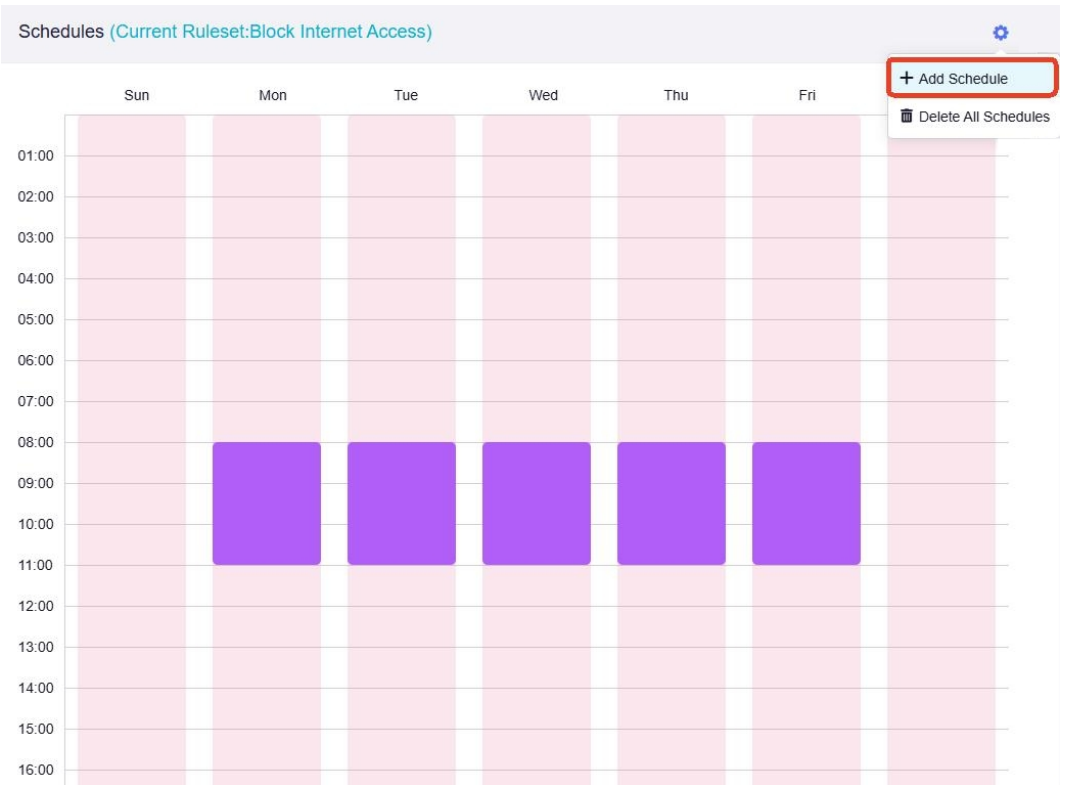
Add the **Learning** ruleset to the schedule. Set the **Execution Time** from 8 AM to 11 AM on weekdays, then click **Apply**.



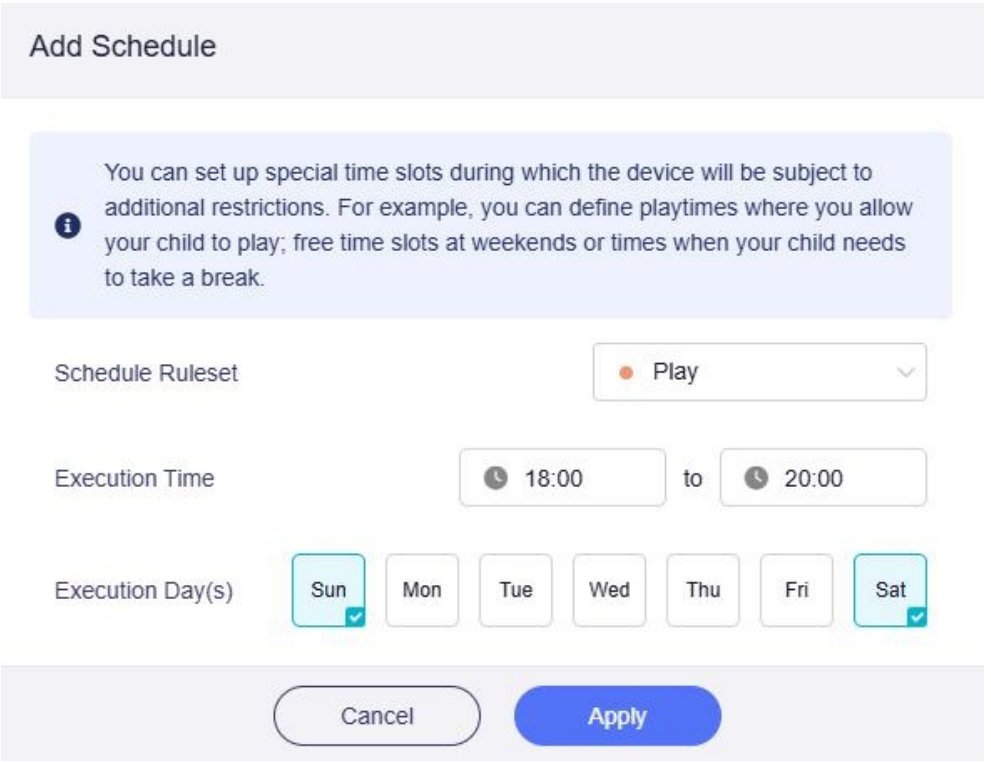
5. You will be redirected to the edit page of the created profile.



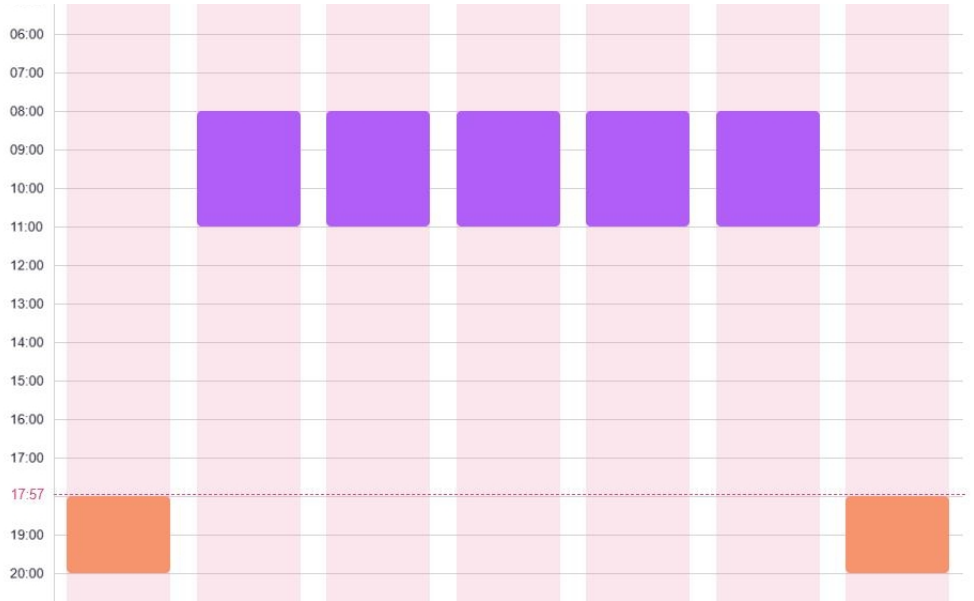
Move to the bottom, and you will see that a schedule has been created. Click the gear icon in the upper right and select **Add Schedule**.



6. Add another ruleset **Play** to the schedule. Set the **Execution Time** from 6 PM to 8 PM on weekends, then click **Apply**.



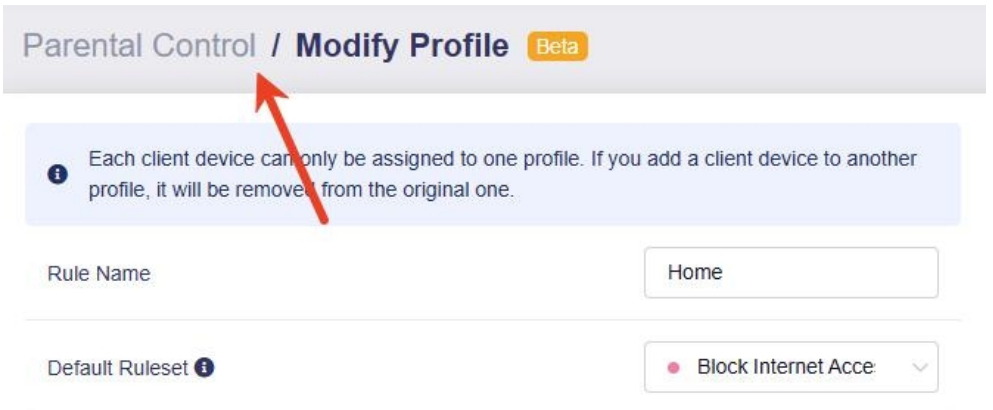
The Play ruleset will then be added into the schedule.



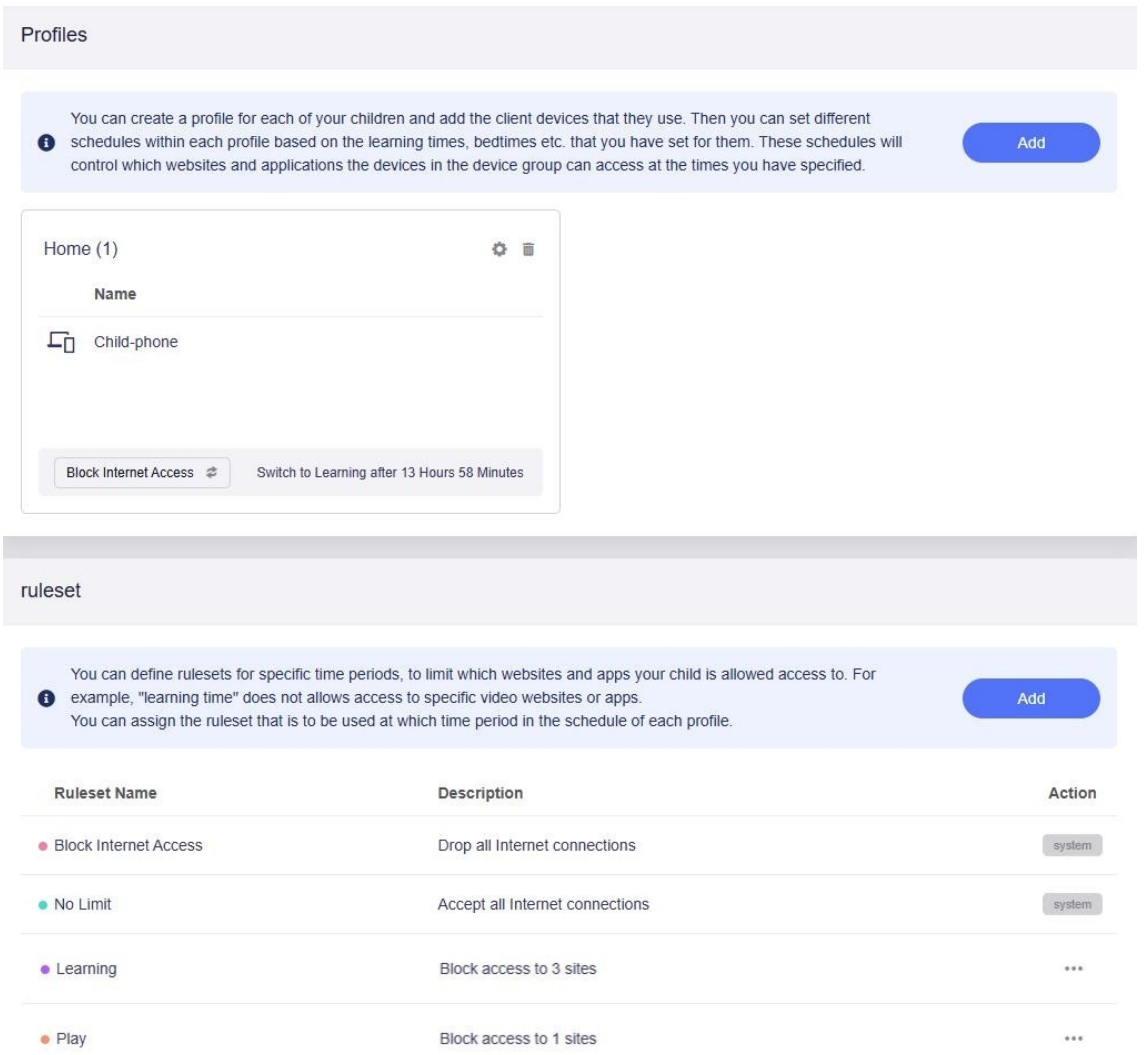
Tips:

- The red dashed line indicates the current time.
- You can modify the execution time by clicking on a certain ruleset in the schedule.

7. Click **Parental Control** at the top to return to the Parental Control page.



You will see the final configuration. Parental Control is now taking effect as per the schedule. You can modify existing profiles and rulesets, or add new ones as needed.



12.5.2 Troubleshooting

If your configured settings fail to take effect, check the following possible causes.

1. DNS cache issue.
   Browsers and operating systems maintain DNS caches, which may delay the application of configuration changes. Clear the DNS cache to apply changes immediately.
2. The profile schedule has not yet started.
3. The entered domain name may be incorrect.
   While a website's public domain is easy to find, the API domains used by apps are often not publicly available. To locate the correct domain, use a packet capture tool such as Wireshark or look up the relevant domain information.
   For example, when blocking "www.google.com", entering "google.com" delivers better results than "www.google.com".
4. The target device uses a randomized MAC address for each network connection, which prevents access rules from taking effect. Disable random MAC address on the target device, then re-add the device to your profile.

12.6 ZeroTier

ZeroTier is a software-defined VPN that enables secure encrypted communication between devices over the internet. It creates a private virtual network, allowing devices to communicate as if on the same LAN regardless of physical location or network topology. ZeroTier features simple setup and ease of use, along with end-to-end encryption, network segmentation, and network bridging.

The ZeroTier feature on GL.iNet routers allows the router to join a ZeroTier virtual network, enabling remote access to the router itself, as well as its WAN and LAN-side resources.

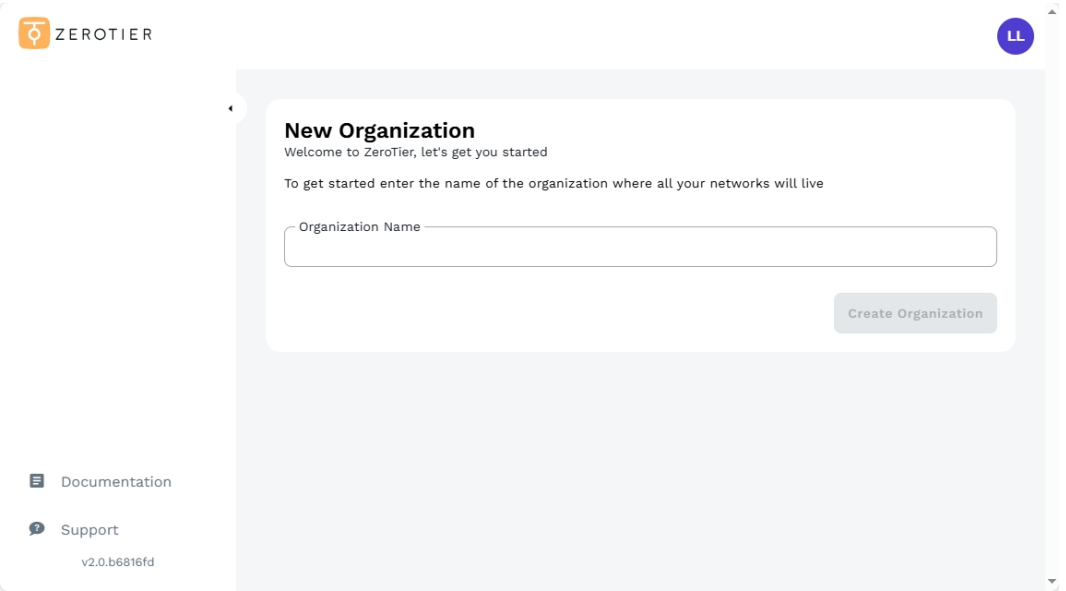
Note:

1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale, and AstroWarp.
2. This feature is currently in beta, and may have some bugs.

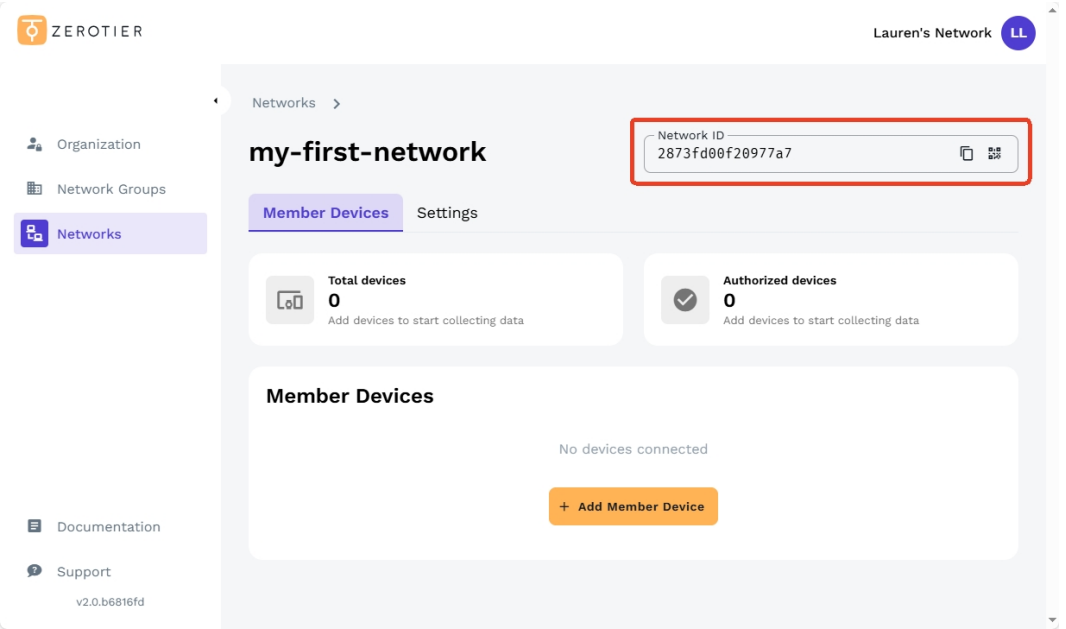
12.6.1 Set Up ZeroTier

Two versions of ZeroTier Central are available: New Central and Legacy Central.
The following steps use New Central as an example.

1. Visit ZeroTier official website and sign in with your account.
2. Create an organization.

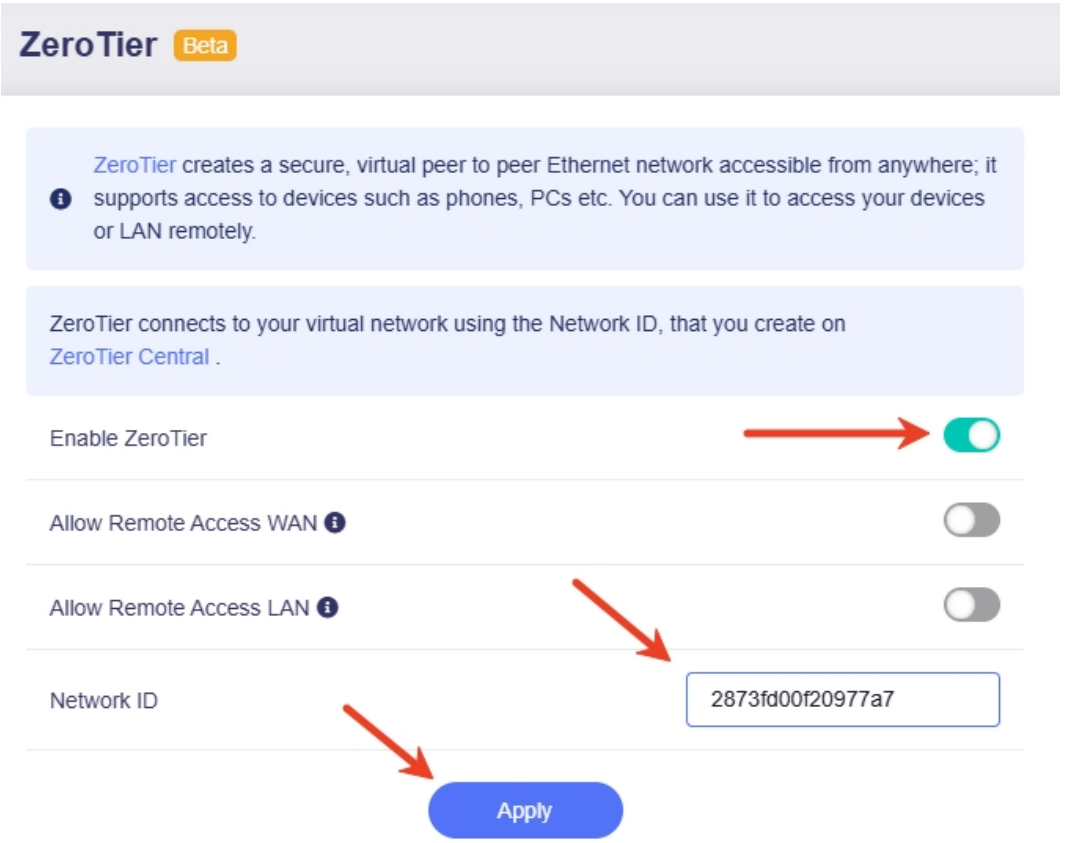


3. Select a plan. Here we choose **Personal plan** as an example, which includes 10 devices, 1 network admin, and 1 network. If you need to create more networks, add more devices, or add custom routes and DNS, choose other paid plan.
4. Now your ZeroTier network has been created.

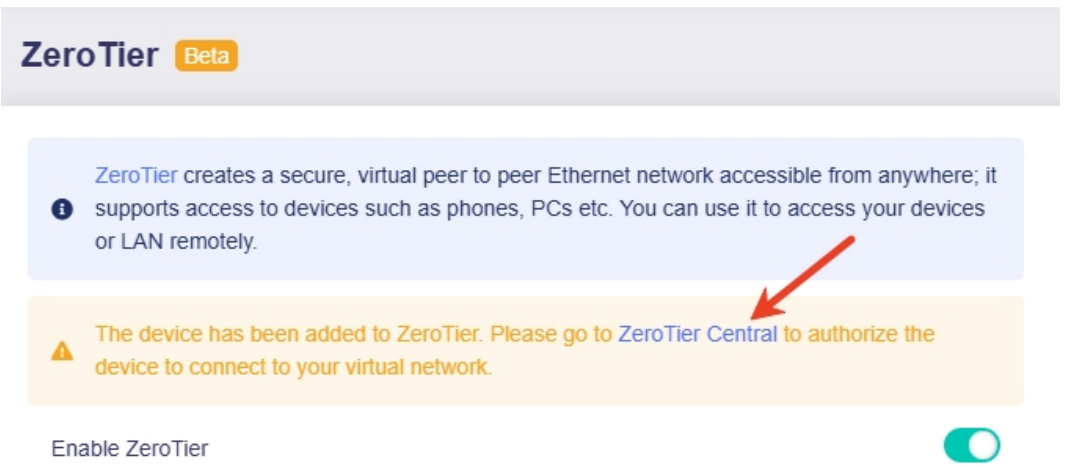


Take note of the **Network ID**, which is a 16-character alphanumeric combination in the upper right corner, as it will be required when connecting other devices later.

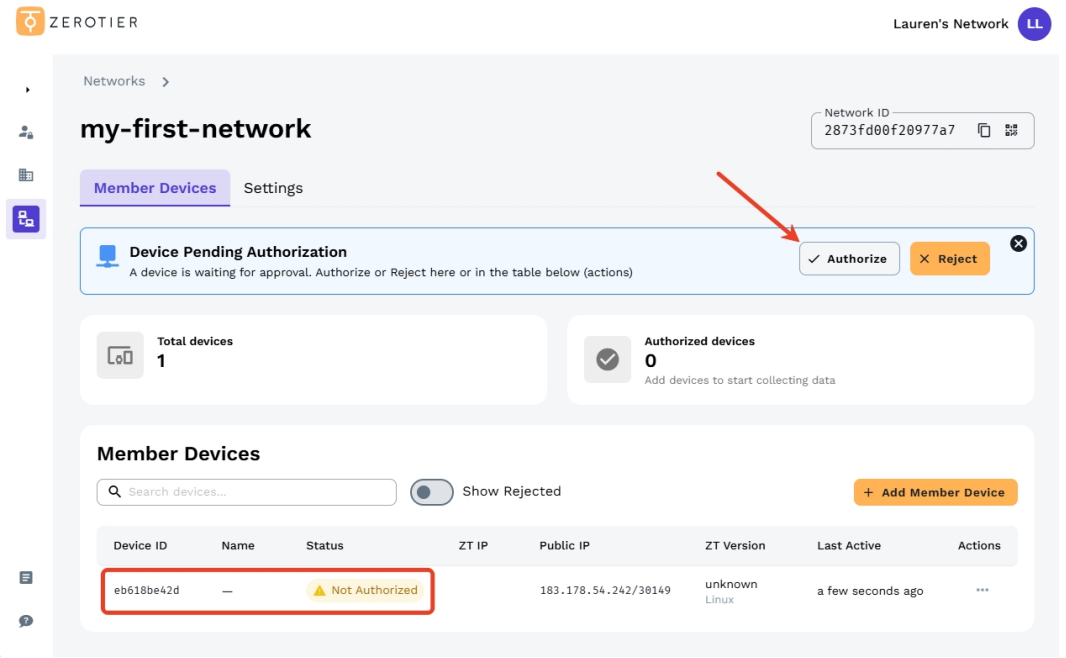
5. Log in to your router's web Admin Panel and navigate to **APPLICATIONS** -> **ZeroTier**. Enable ZeroTier, enter the **Network ID**, then click **Apply**.



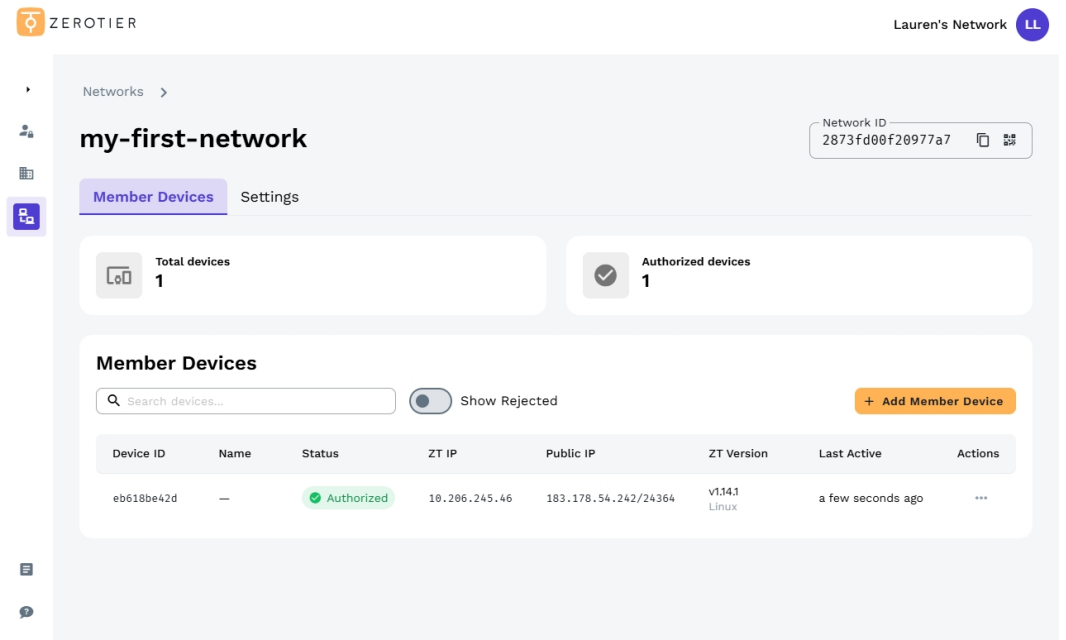
After a short while, the page will indicate that authorization is required. Click the **ZeroTier Central** hyperlink to redirect to the ZeroTier Central.



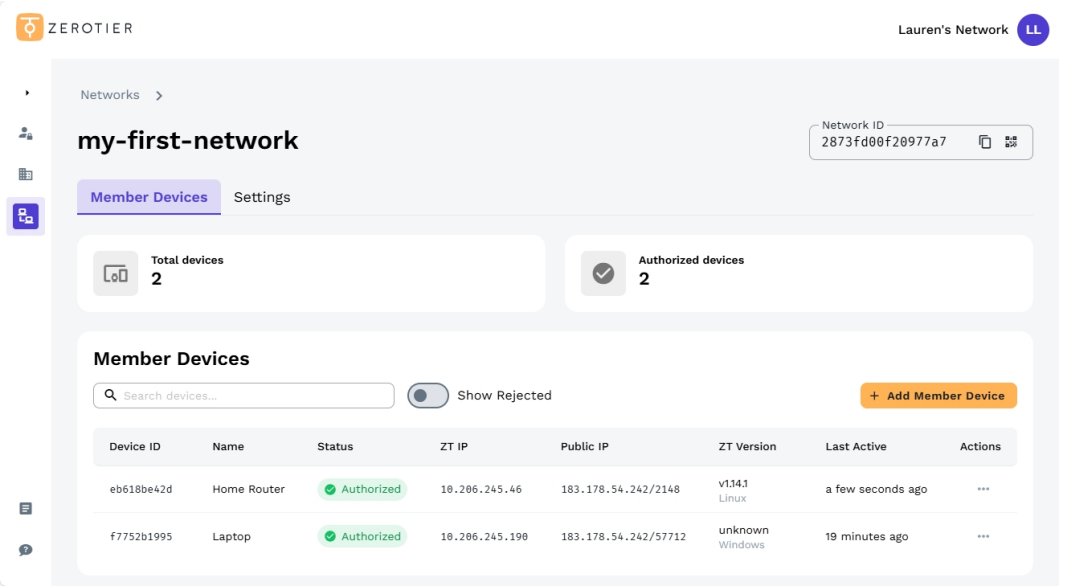
6. On the ZeroTier Central, locate the Pending device and authorize it.



Once authorized, the page displays as follows.

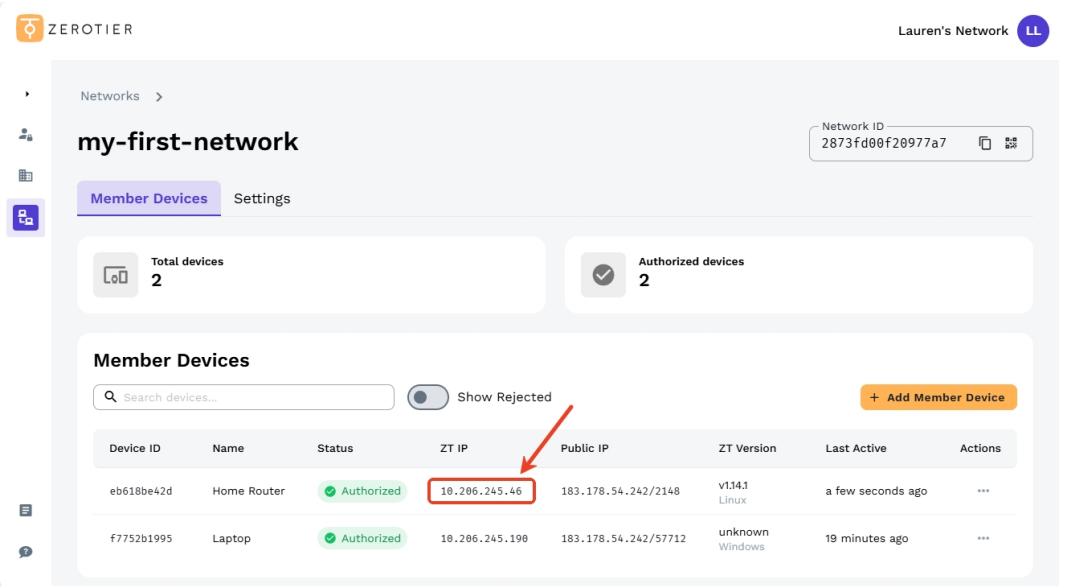


7. Add another device (such as a computer or smartphone) to the same ZeroTier network by following this guide. Once successfully added, the page displays as follows. You will see the details of member devices, such as **Device ID**, **Name**, **Status**, **Managed IP**, and **Public IP**.



Tips: You can click the three-dot icon on the right to edit member device settings, including the device name, Managed IP(s), and advanced settings.

8. Click the router's **Managed IP** to copy it.



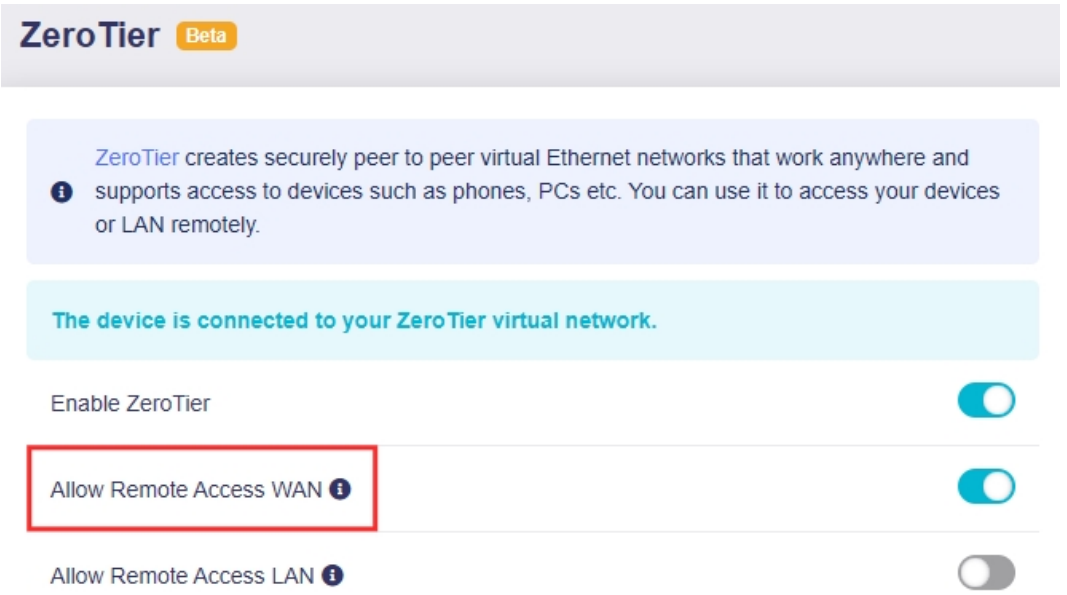
You can then use this Managed IP to access the router from your laptop that is on the same ZeroTier network.

9. Test connectivity.

   On the laptop connected to the same ZeroTier network, open a web browser and enter the router's Managed IP obtained in the previous step. If you can access the router's web Admin Panel, the ZeroTier connection is successful.

12.6.2 Allow Remote Access WAN

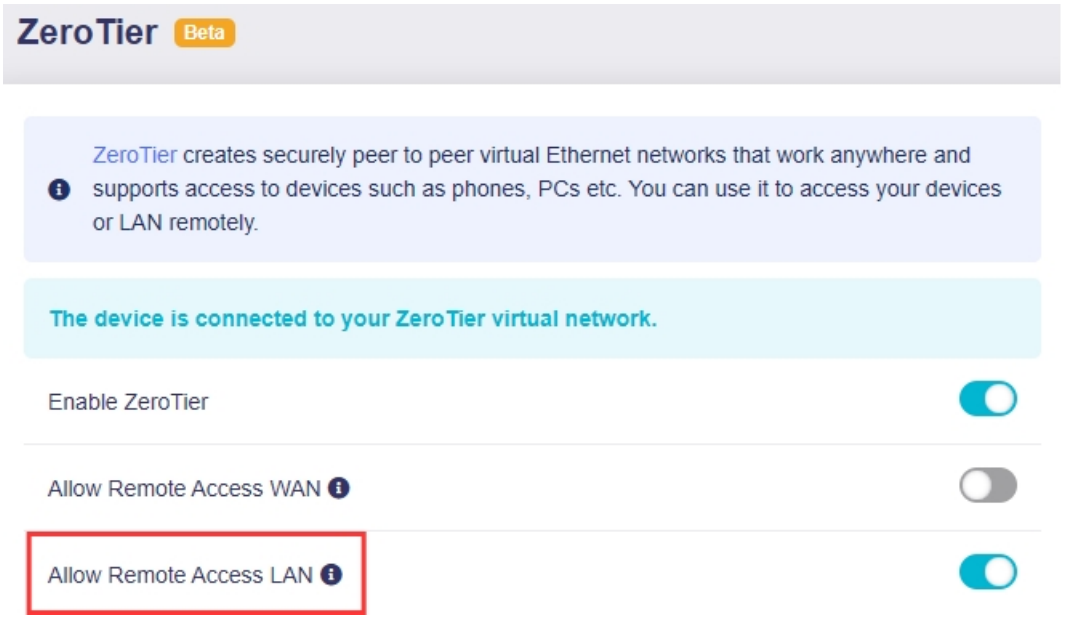
If this option is enabled, resources on the device's WAN side can be accessed through the ZeroTier virtual network. See here for more details.



Note: This feature requires routing rules to be added to the ZeroTier network to take effect. One custom route can be added for free in Legacy Central, while in New Central you can only configure custom routes with an Essential plan or higher. See here for pricing details.

12.6.3 Allow Remote Access LAN

If this option is enabled, resources on the device's LAN side can be accessed through the ZeroTier virtual network. See here for more details.



Note: This feature requires routing rules to be added to the ZeroTier network to take effect. One custom route can be added for free in Legacy Central, while in New Central you can only configure custom routes with an Essential plan or higher. See here for pricing details.

12.7 Tailscale

Tailscale is a VPN service that makes your personal devices and applications accessible worldwide, securely and effortlessly. See here for more details.

The Tailscale feature on GL.iNet routers allows the router to join a Tailscale virtual network, enabling remote access to the router itself, as well as its WAN and LAN-side resources.

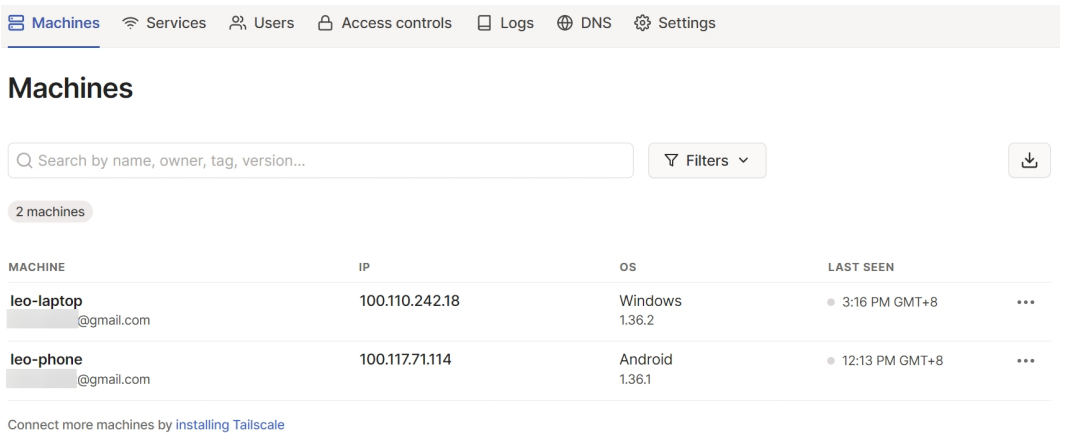
Note:

1. Since Tailscale is based on WireGuard, it is not recommended to use Tailscale with any of the following features or services simultaneously, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier, AstroWarp.
2. This feature is currently in beta, and may have some bugs.
3. GL.iNet routers are not yet available as exit nodes.

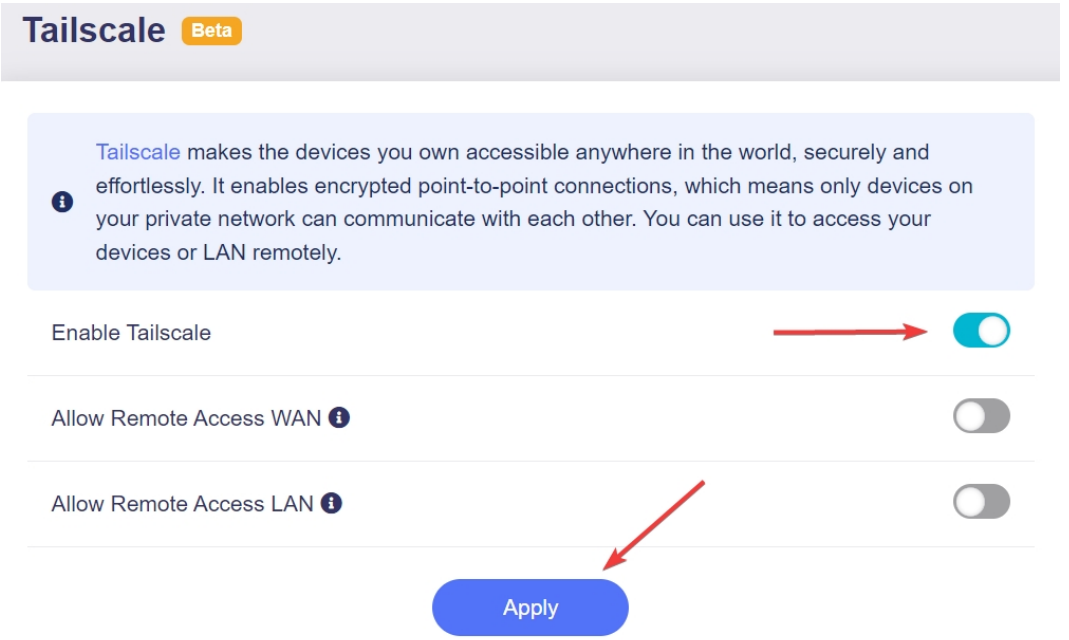
12.7.1 Set Up Tailscale

Here is an example of using GL-MT2500 to set up Tailscale network.

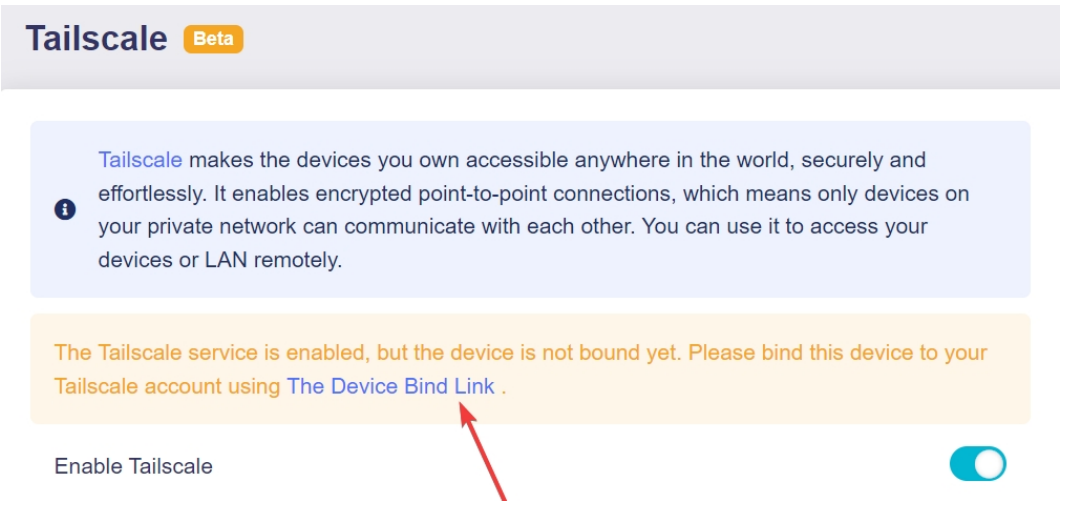
1. Register a Tailscale account first and bind one or two devices to your Tailscale account for testing purposes. After binding, you will see your devices in the Tailscale Console.



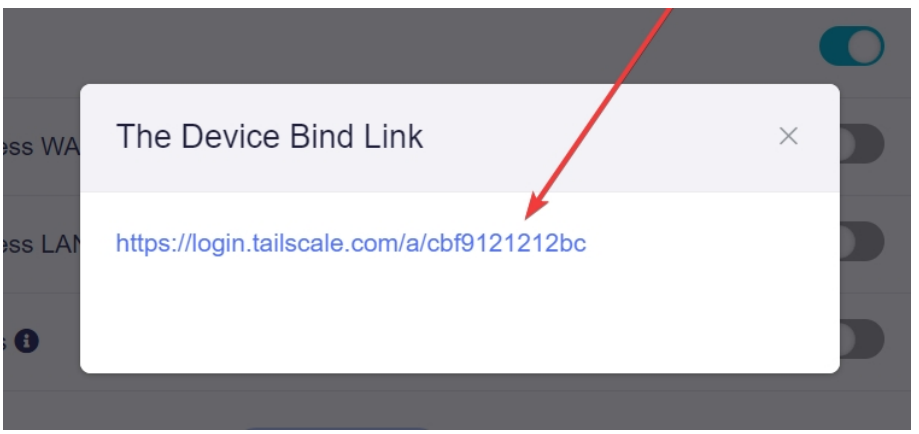
2. Log in to your router's web admin panel and navigate to **APPLICATIONS** > **Tailscale**. Toggle on **Enable Tailscale** and click **Apply**.



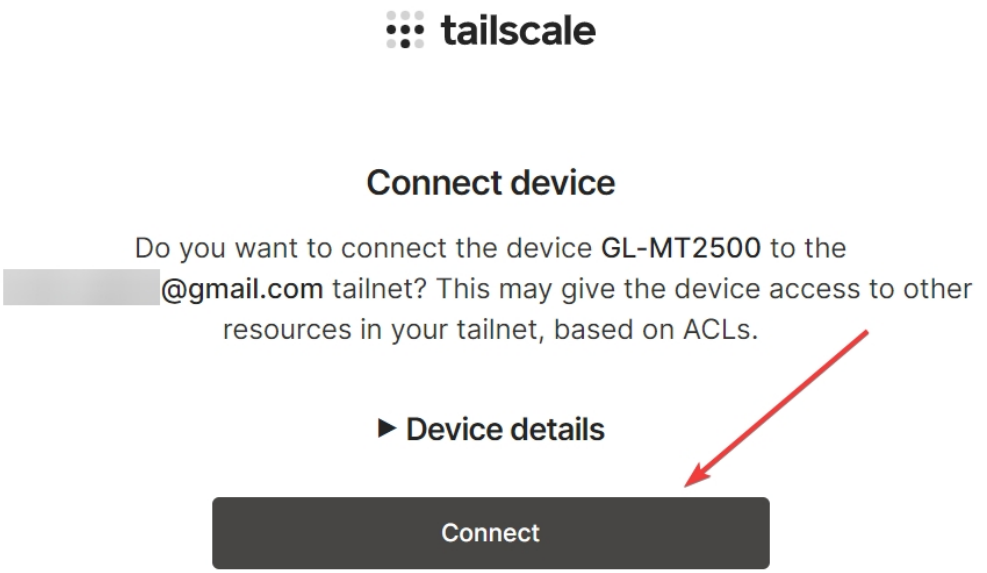
3. The page will prompt you to bind the device. Click **Device Bind Link**.



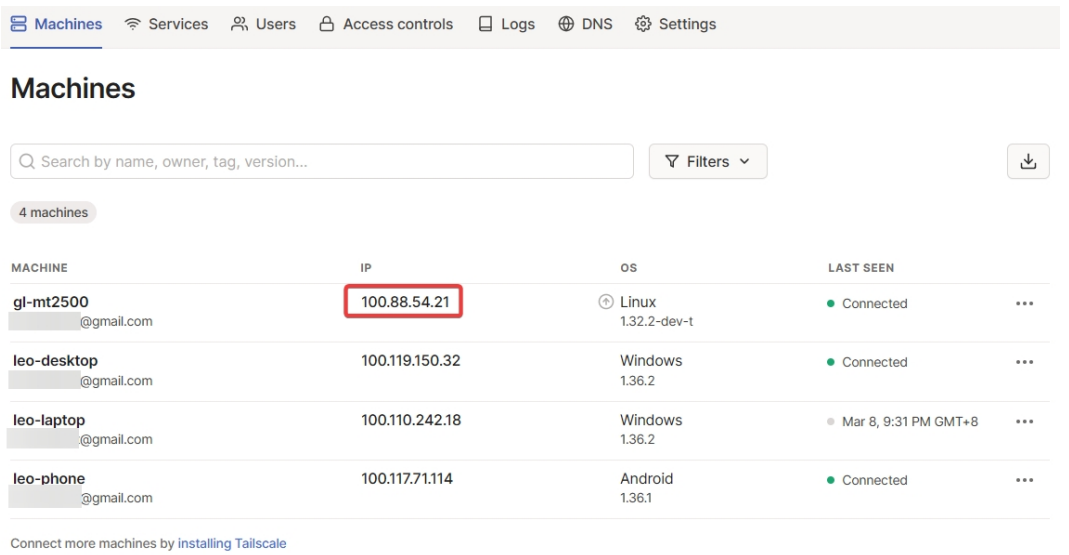
4. In the pop-up window, click the link and log in with your Tailscale account.



5. Once logged in, you will be asked to confirm the device. Click **Connect**.



6. You will then be redirected to the Tailscale admin console. Now the router has been added into the Tailscale virtual network, and it can be accessed remotely by the Tailscale virtual IP 100.88.54.21.

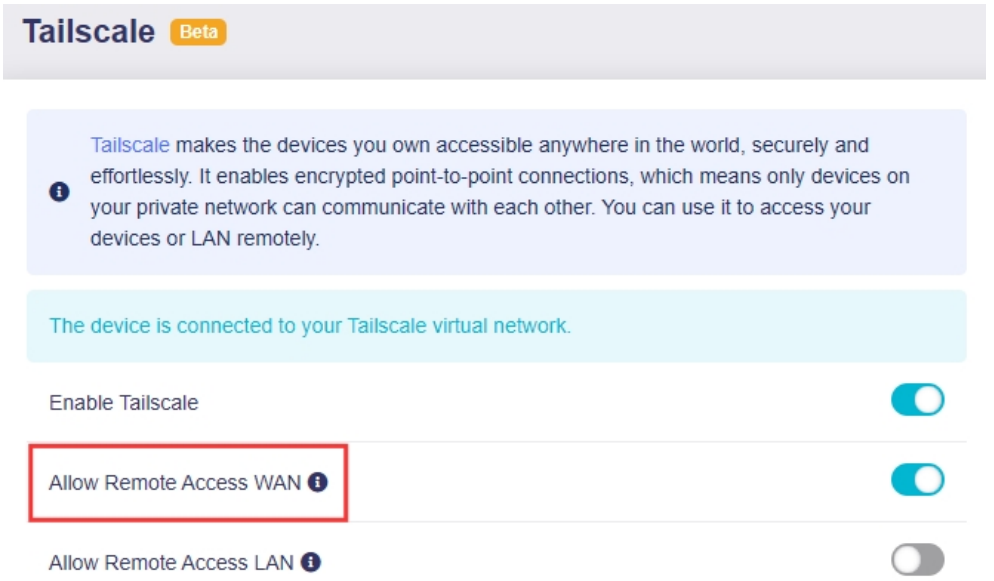


7. Test connectivity.

   On another device connected to the same Tailscale network, open a web browser and enter the router's virtual IP in the address bar. If you can access the router's web admin panel, it means Tailscale is working. You can also use the ping command or SSH log in to the router's terminal by its virtual IP to test connectivity.

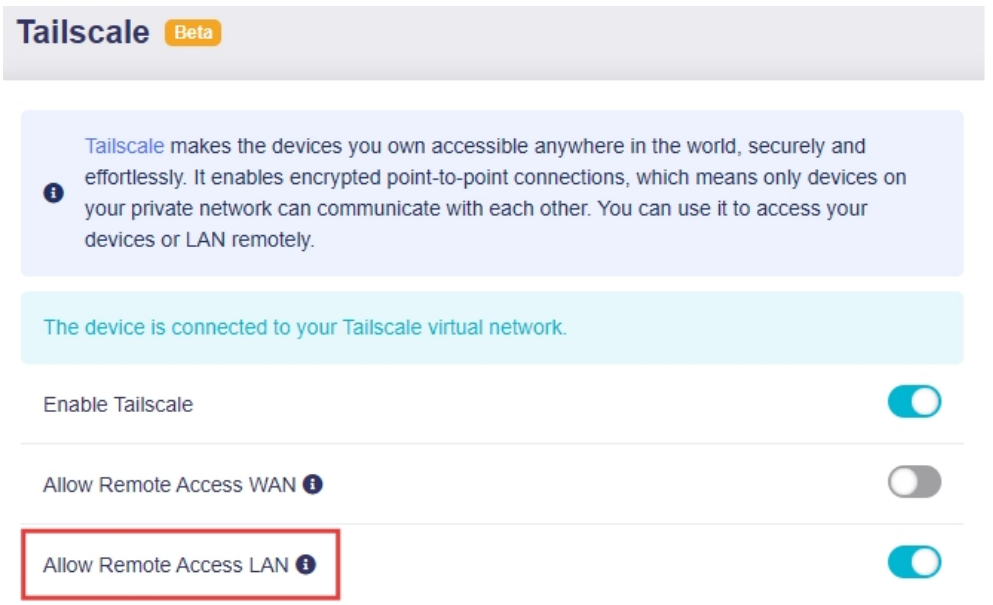
12.7.2 Allow Remote Access WAN

If this option is enabled, resources on the device's WAN side can be accessed through the Tailscale virtual network. See here for more details.



12.7.3 Allow Remote Access LAN

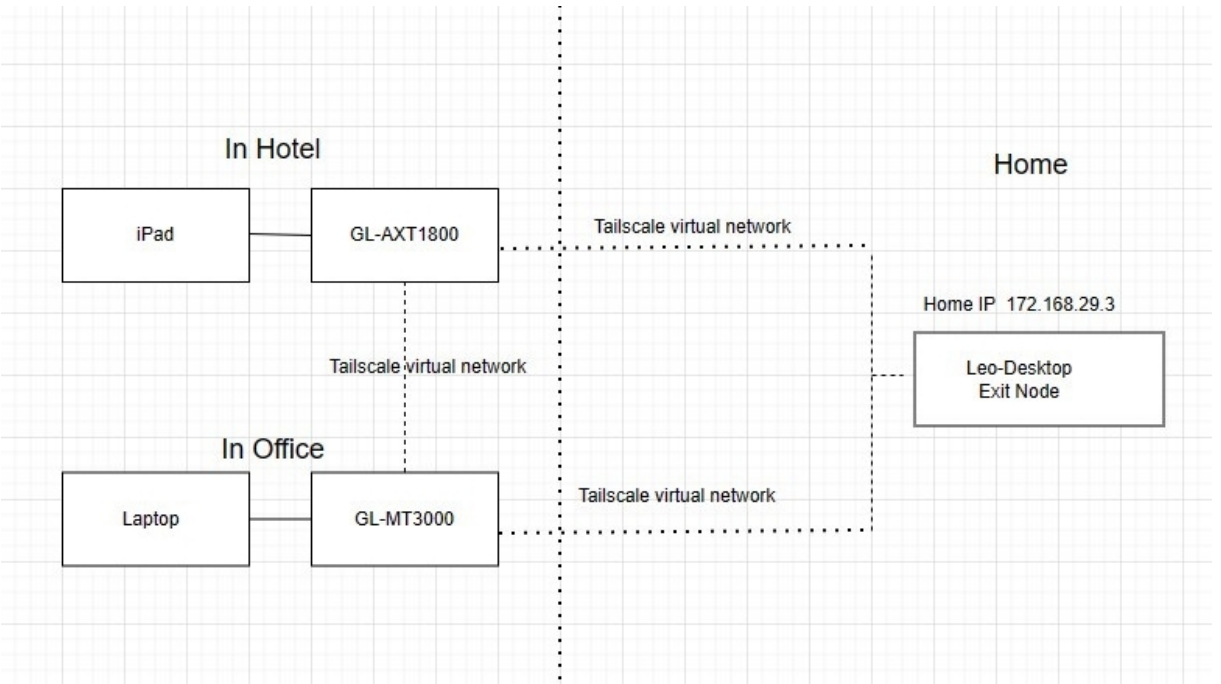
If this option is enabled, resources on the device's LAN side can be accessed through the Tailscale virtual network. See here for more details.



12.7.4 Custom Exit Nodes

By default, Tailscale acts as an overlay network: it only routes traffic between devices running Tailscale, and does not process your public Internet traffic — such as when browsing websites like Google.

However, there might be times when you want Tailscale to route your public Internet traffic. For example, when you are away from home or traveling abroad, if you need to access online services (such as banking) that are only available in your home country, you can set your home desktop with a public IP as an Exit node, and configure other devices on the same Tailnet — such as the GL-AXT1800 and GL-MT3000 in the image below — to send their traffic through it. This enables all your public Internet traffic to be forwarded via the Exit Node.



In summary, an Exit node routes outbound Internet traffic from your Tailnet devices, effectively acting as VPN servers. When connected to an Exit node, all your non-Tailscale Internet traffic appears to originate from its location, helping you access geo-restricted content and enhance your online privacy. The device handling this traffic forwarding is referred to as an "exit node". See here for more details.

Note: If the router's DNS Server is a private IP address that can be accessed only in the local network, you may lose Internet access when running the exit nodes. To avoid this, please set a public DNS server (e.g., 8.8.8.8) manually for your router.

Chapter 13

Network

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

13.1 Port Forwarding

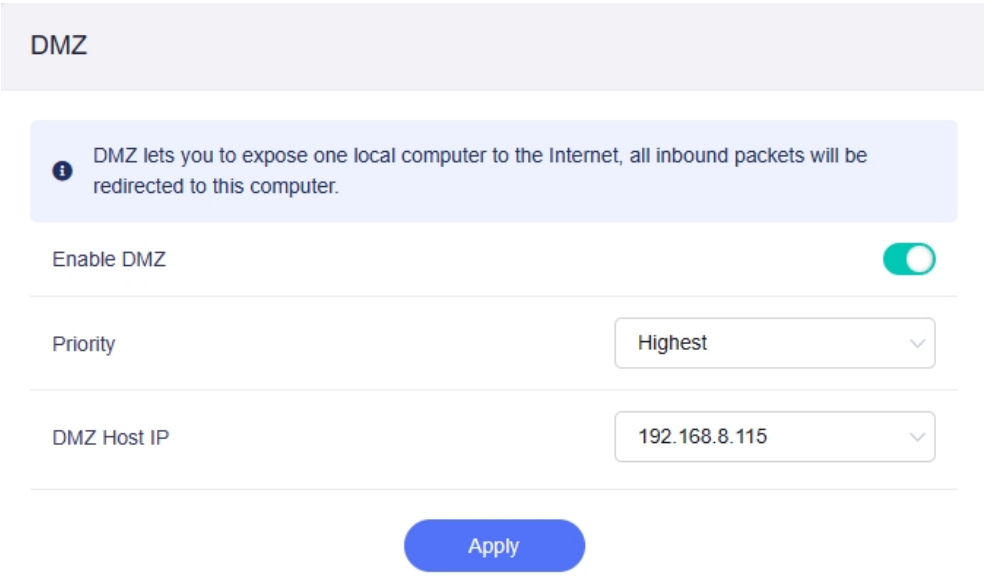
Port forwarding is a network feature that routes external requests to specific devices on your local network. The Port Forwarding page includes two key functions: **DMZ** (for direct full access to a single device) and **Port Forwarding** (for targeted access to specific ports of devices).

13.1.1 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 as needed.

1. Log in to your router's web admin panel and navigate to **NETWORK** > **Port Forwarding** > **DMZ** section.
2. Toggle on **Enable DMZ**. Select the Priority and DMZ Host IP from the drop-down list, and click **Apply**.



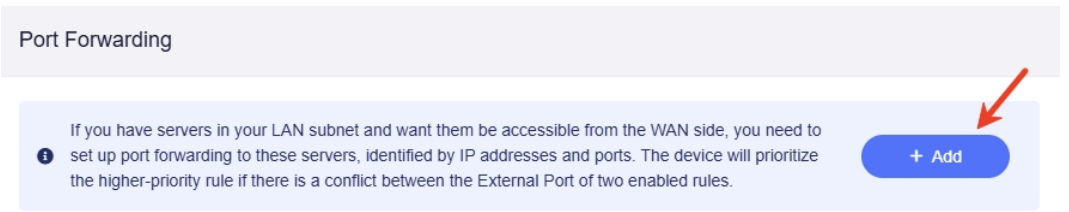
- **Priority**: Set it as Highest or Lowest. If the priority of the DMZ is higher than the port forwarding rules, all port forwarding rules will be invalidated. Otherwise, requests will be forwarded to the DMZ client device only if the accessed port has no corresponding port forwarding rule.
- **DMZ Host IP**: Select the internal IP address of the device that will receive all the inbound packets.

13.1.2 Port Forwarding

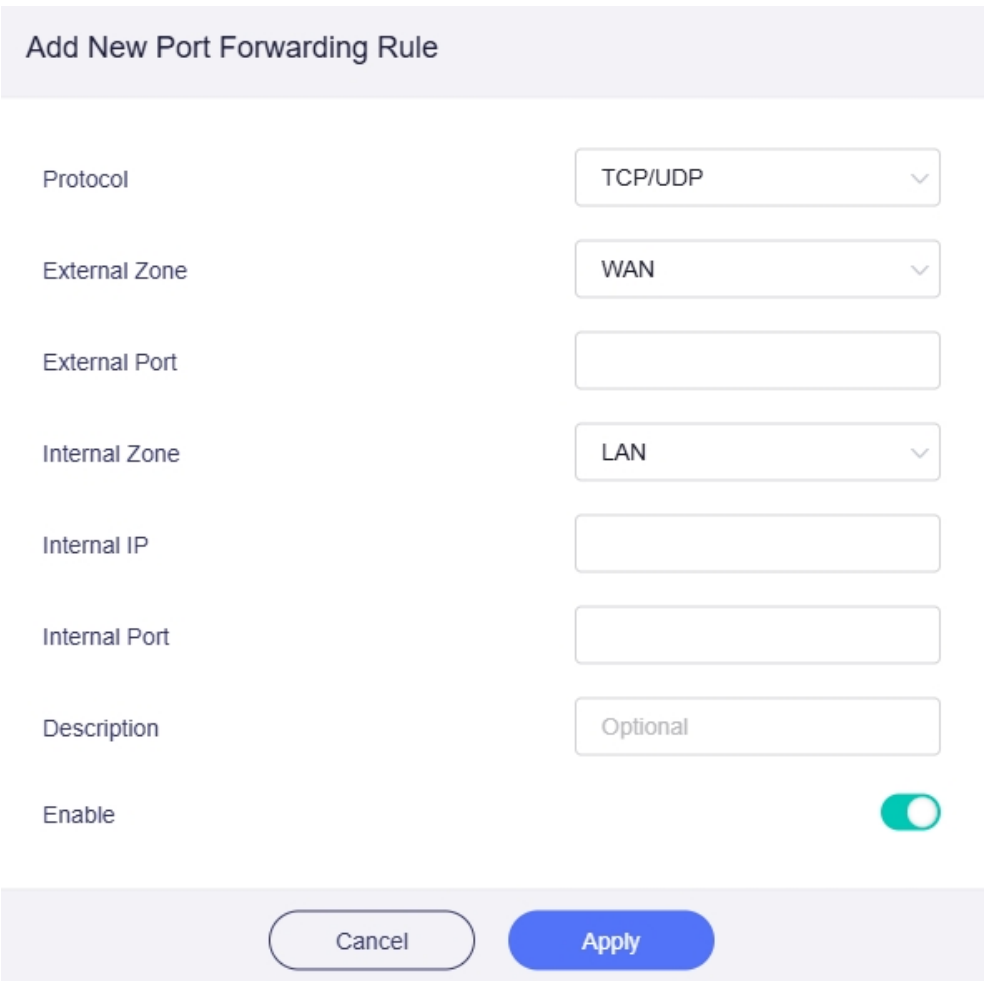
Port Forwarding enables remote computers to connect to a local computer or server behind the LAN firewall (e.g., web servers, FTP servers).

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

1. Log in to your router's web admin panel, go to **NETWORK** > **Port Forwarding** > **Port Forwarding** 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 forwarding rule, then click **Apply**.



- **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, and LAN.
- **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, 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.
- **Description**: Set a name or add a description for the port forwarding rule (optional).
- **Enable**: Enable or disable this rule.

13.2 Multi-WAN

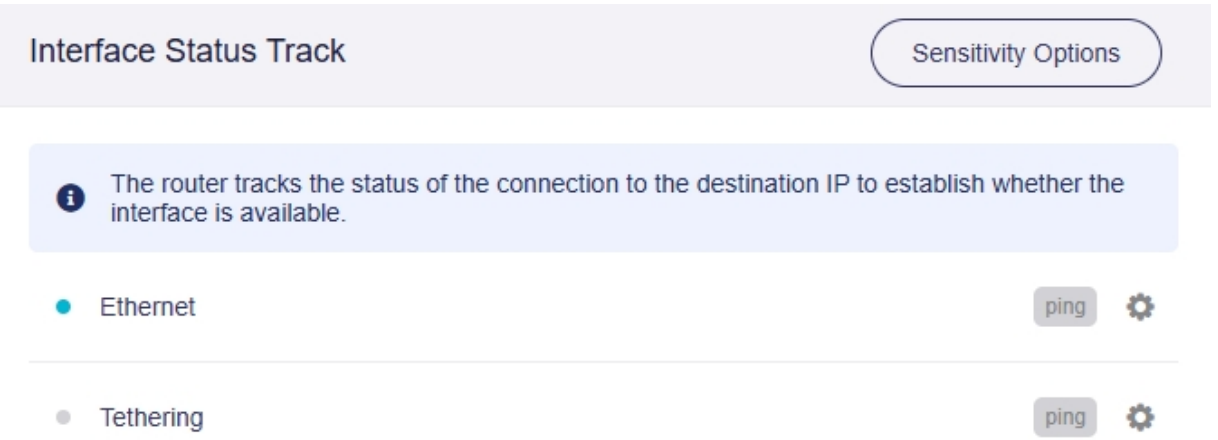
Multi-WAN enables simultaneous use of multiple Internet access methods, allowing configuration of diverse connectivity options on the router. It offers two working modes:

- **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.

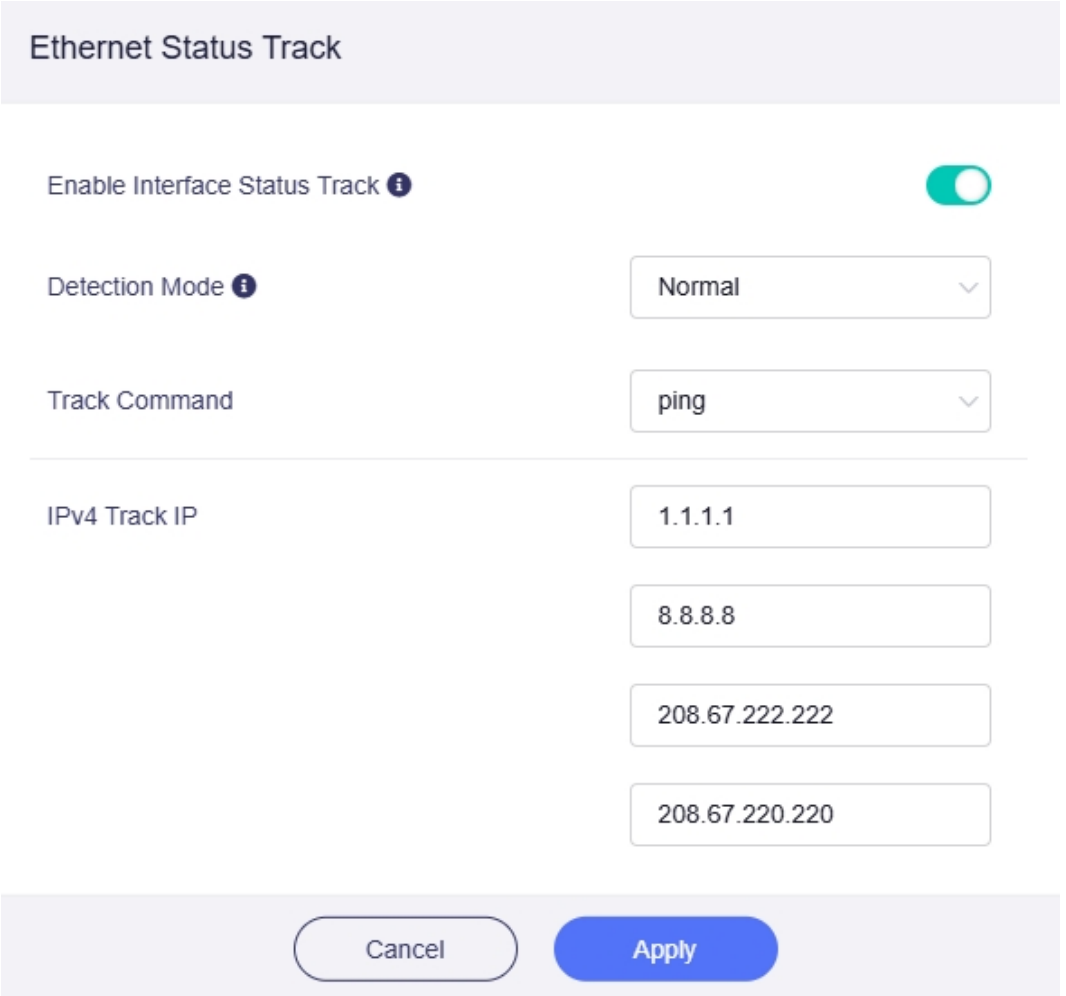
13.2.1 Interface Status Track

Brume 2 has two interfaces for Internet connection: Ethernet and Tethering. It uses 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.

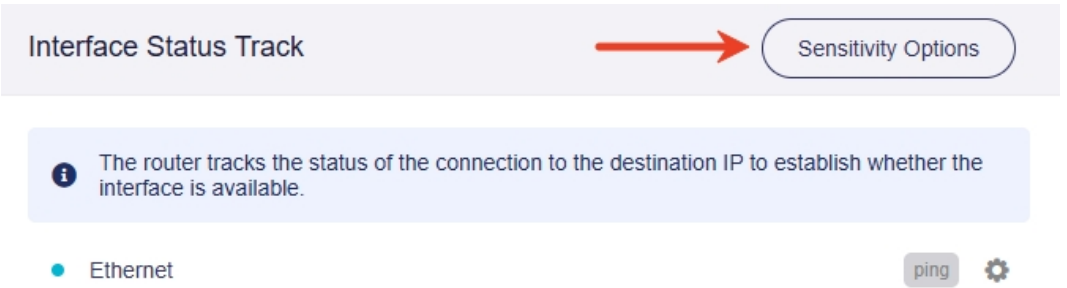
Below are the status tracking settings for the Ethernet interface. The same configuration logic applies to the other interface.



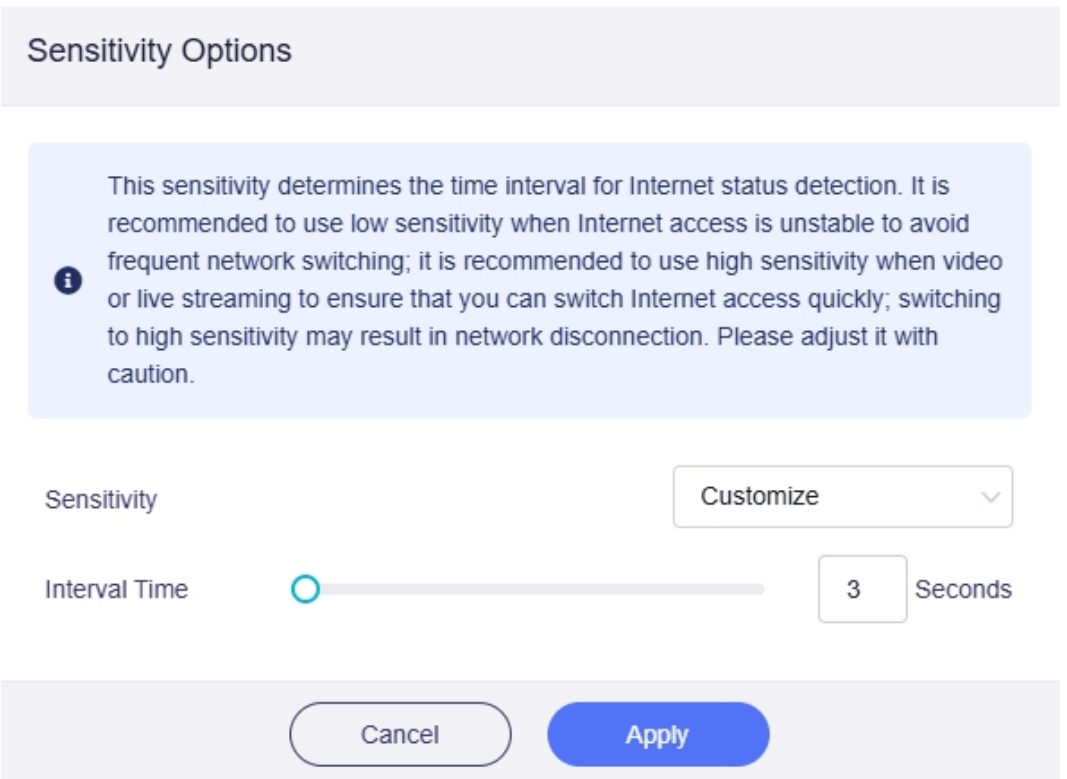
- **Enable Interface Status Track**: It is enabled by default. If disabled, the router will determine the interface status based on physical conditions (e.g., whether the Ethernet cable is plugged in).
- **Detection Mode**: This feature was introduced as Low Data Mode in firmware v4.5, then renamed Detection Mode in firmware v4.7. Three modes are available: Normal Mode, Low Data Mode, and Strict Mode.
  - **Normal Mode**: It is used by default.
  - **Low Data Mode**: It only triggers tracking when a network error occurs on the network interface. Use this mode if you are on a limited data plan. Note that reconnecting after a disconnection may be slightly slower than in Normal Mode, and it is enabled by default only for cellular interface.
  - **Strict Mode**: It determines the interface status exclusively based on the results of a detection command sent to a public IP.

- **Track Command**: The ping command is used to monitor connection status to the destination IP and verify interface availability.
- **IPv4 Track IP**: Customize the IPv4 Track IP addresses as needed.

Click **Sensitivity Options** in the upper right corner.



You can set the time interval for Internet status detection to Low, Medium, High, or customize it. The adjustable interval time ranges from 0.5 seconds to 90 seconds.



Tips: If the network is stable, high sensitivity is recommended for quick switching in case of network disconnection. This is suitable for scenarios such as watching videos, live streaming, or playing games. If the network is unstable, low sensitivity is recommended to avoid frequent

network switching and failed connections. This applies to scenarios such as downloading cached files.

Note: Switching to high sensitivity may cause occasional network disconnections during the process. Please adjust with caution.

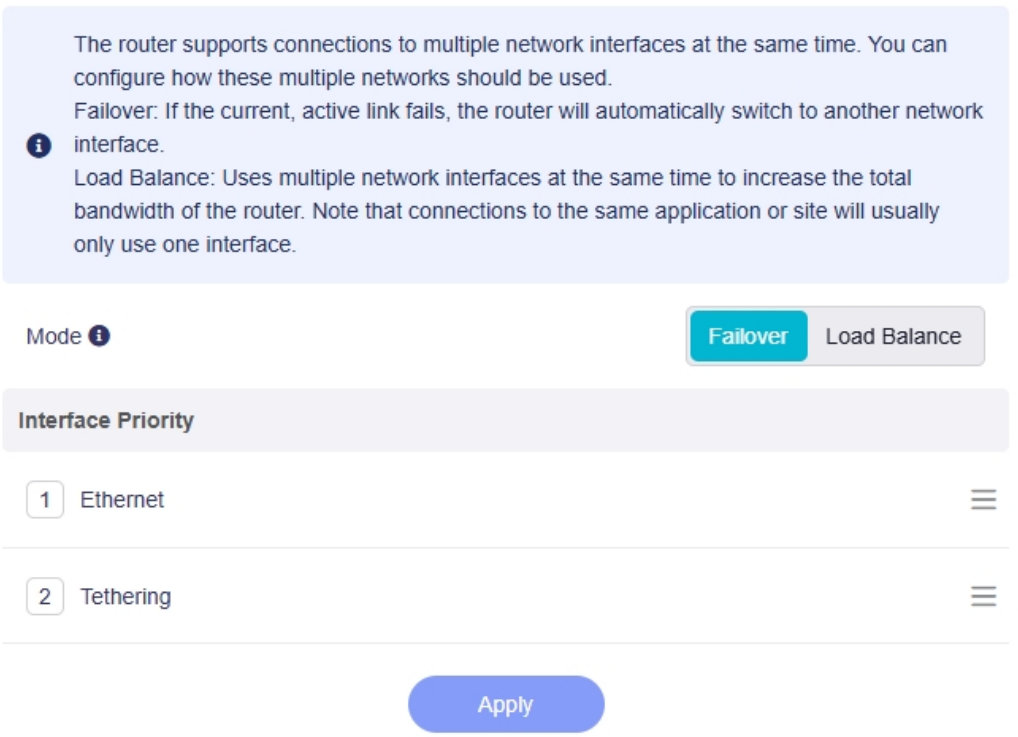
13.2.2 Multi-WAN Mode

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.

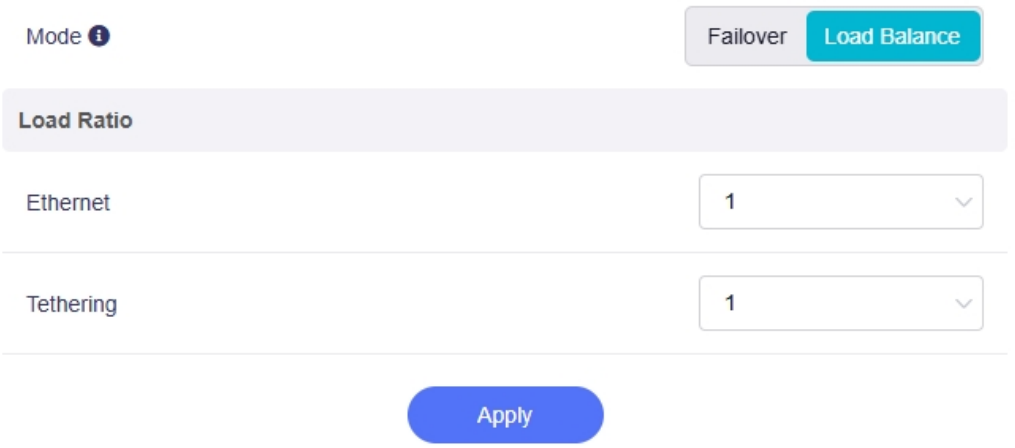
You can set priority levels for each interface: when the currently used interface fails, the router switches to the next available interface with the highest priority. Once a higher-priority connection is restored, the router will automatically switch back to it.



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 two networks (e.g., Ethernet and Tethering) simultaneously and the two interfaces are available for Internet access, enabling Load Balance and setting a 1:1 ratio means the four interfaces will share network bandwidth equally. The system will distribute new connections across these four interfaces according to the configured load ratio.



You can customize the load ratio as needed. For example, if Ethernet has a bandwidth of 100 Mbps, Tethering has 200 Mbps, set the load ratios to 1 for Ethernet, 2 for Tethering. The system will then distribute new connections across the two interfaces according to the configured 1:2 ratio, meaning Ethernet will handle half as many connections as Tethering. 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.

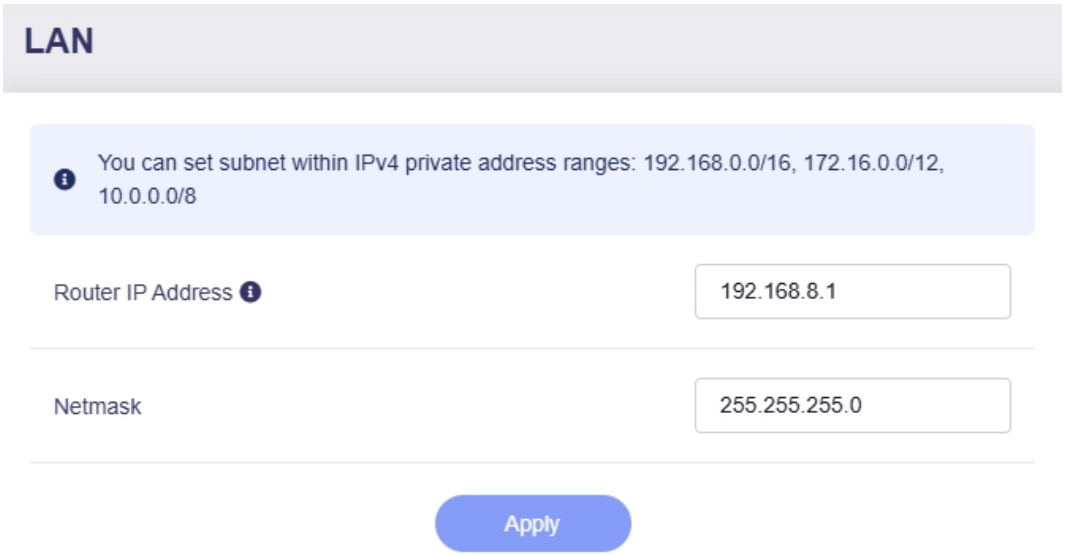
13.3 LAN

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 basic settings, DHCP server, and address reservation.

13.3.1 Basic Settings

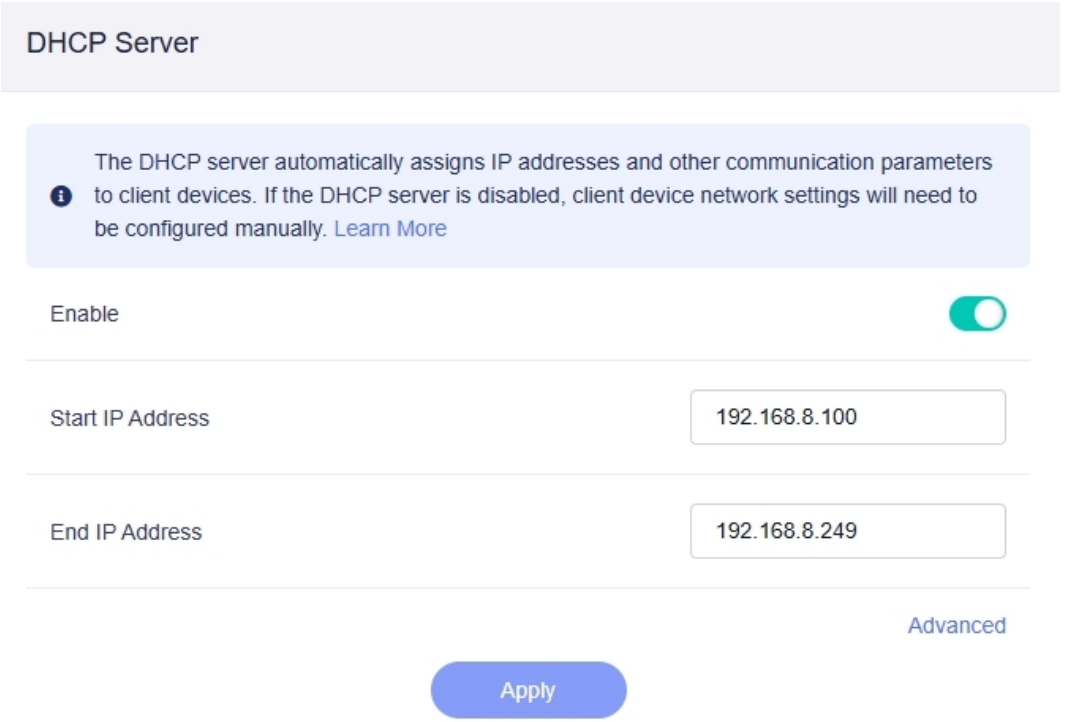
The basic settings include Router IP address and Netmask. You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



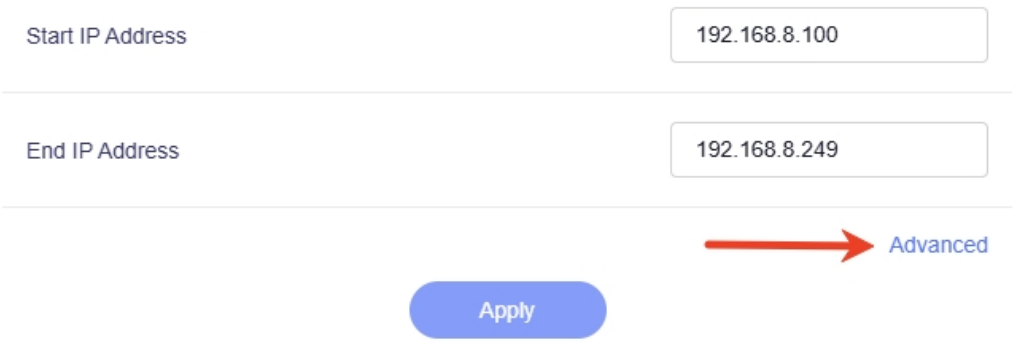
- **Router IP Address**: This is the address entered into a browser's address bar to access the router's admin panel. It is 192.168.8.1 by default and can be changed if it conflicts with the upstream network.
- **Netmask**: Two options are available: 255.255.255.0 and 255.255.0.0.

13.3.2 DHCP Server

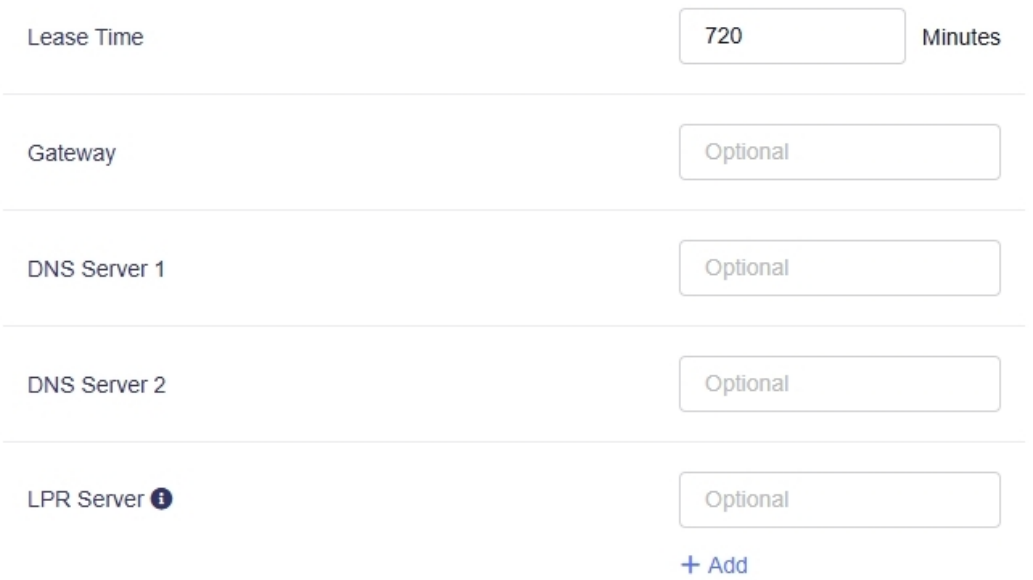
The DHCP server automatically assigns IP addresses and other communication parameters to each connected client. GL.iNet router's DHCP server is enabled by default, and the DHCP server's IP address pool ranges from 192.168.8.100 to 192.168.8.249. You can customize the address range as needed.



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



You will be able to configure advanced settings, including Lease Time, Gateway, DNS Server(s), and LPR Server.



- **Lease Time**: The duration for which a device can use an IP address assigned via DHCP.
- **Gateway**: The router component that routes traffic between the local network and external networks (e.g., the internet).
- **DNS Server 1**: The primary server responsible for translating domain names into IP addresses.
- **DNS Server 2**: A backup server used to resolve domain names if the primary DNS server fails.
- **LPR Server**: (Line Printer Remote Server) A service that manages print jobs and enables networked devices to send print requests to remote printers. Multiple LPR ports for printers can be configured.

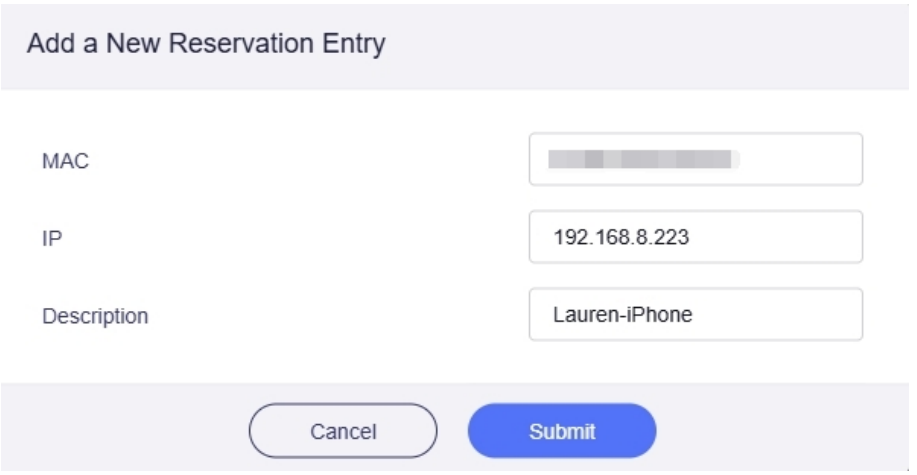
Note: If DHCP server is disabled, you need to configure static IP and other communication parameters manually for each clients. See here for details.

13.3.3 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 as 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**.



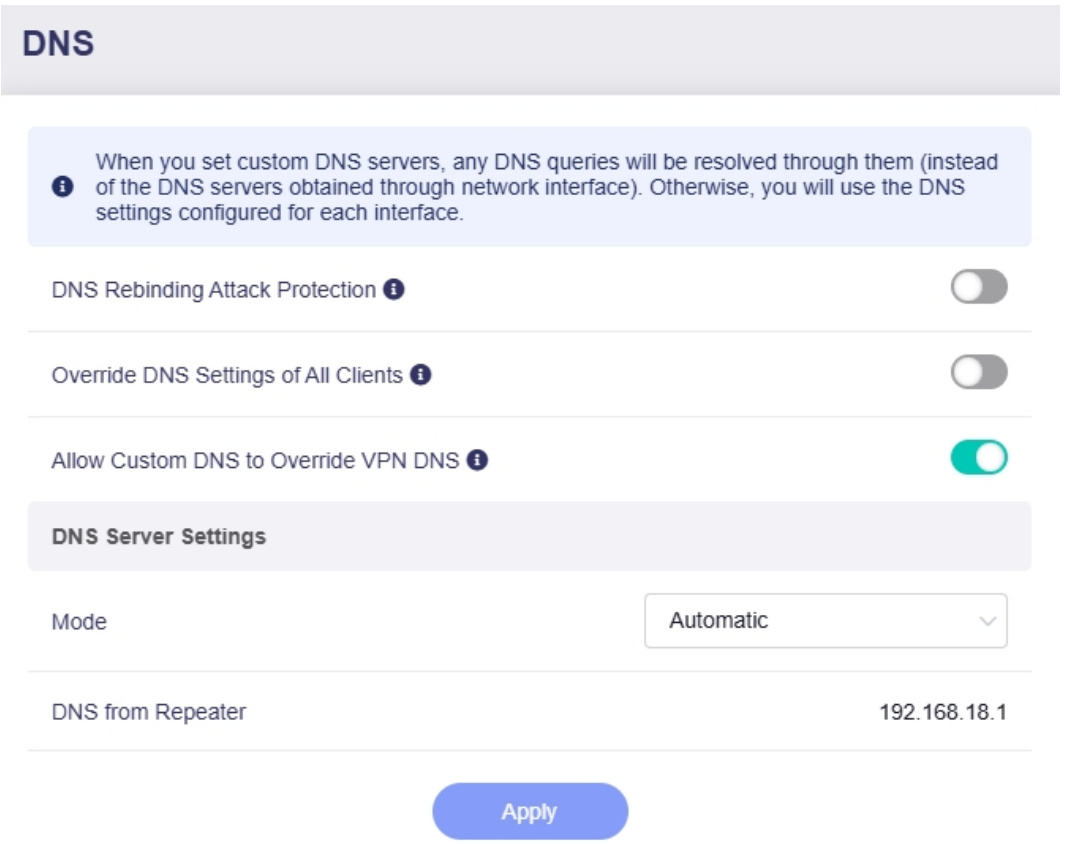
3. After adding a new IP address reservation, the page will display the reserved entry, as shown below.

13.4 DNS

DNS (Domain Name System) is a network service that translates human-readable domain names (e.g., www.google.com) into machine-recognizable IP addresses (e.g., 142.250.185.142), enabling devices to connect to target websites or services.

Router DNS Server refers to the DNS service built into the router, which provides domain name-to-IP translation for all connected devices. It typically works in two ways: first, it automatically obtains DNS addresses from the upstream network to provide default translation services; second, users can manually configure custom public DNS addresses (e.g., 8.8.8.8) on the router's web admin panel to optimize network access or enhance security. Once set up, all connected devices will use this unified DNS server by default, eliminating the need for separate DNS configuration on each device.

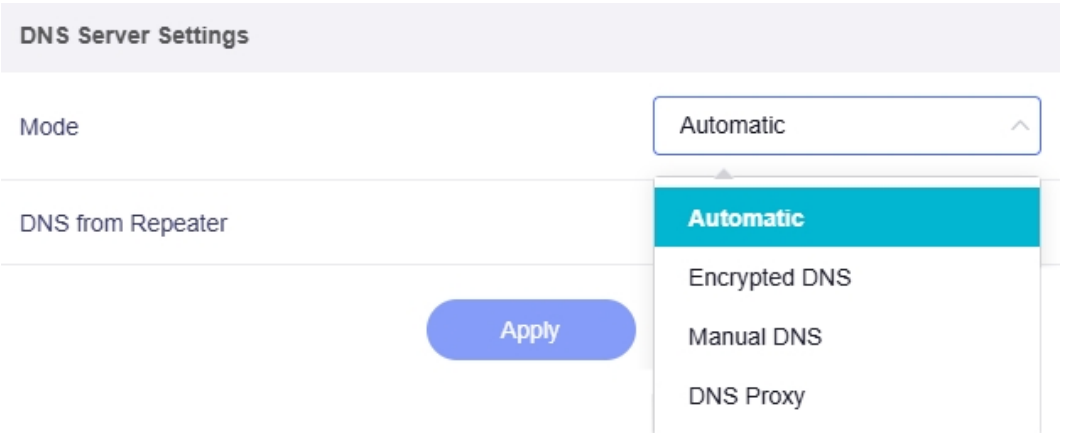
Log in to your router's web admin panel and navigate to **NETWORK** > **DNS**. This page allows you to configure DNS related settings, including security options, server modes, and DNS priority rules for different network scenarios.



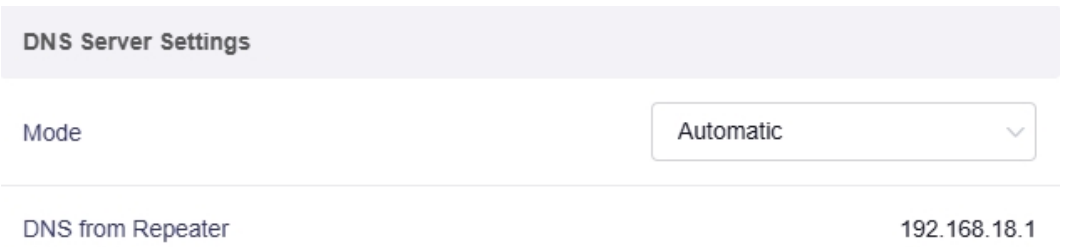
- **DNS Rebinding Attack Protection**: Protects against DNS rebinding attacks by blocking malicious DNS resolution attempts. Note that enabling it may cause private DNS lookup failure.
- **Override DNS Settings of All Clients**: If enabled, all connected devices will be forced to use the DNS servers configured on the router, ignoring their own original DNS settings. It enables unified DNS configuration for all devices.
- **Allow Custom DNS to Override VPN DNS**: When enabled, if you have set custom DNS, packets transmitted through the VPN tunnel will use the custom DNS for resolution, instead of the DNS servers from the VPN connection. This ensures your custom DNS resolution rules apply normally when using VPN.

13.4.1 DNS Server Settings

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

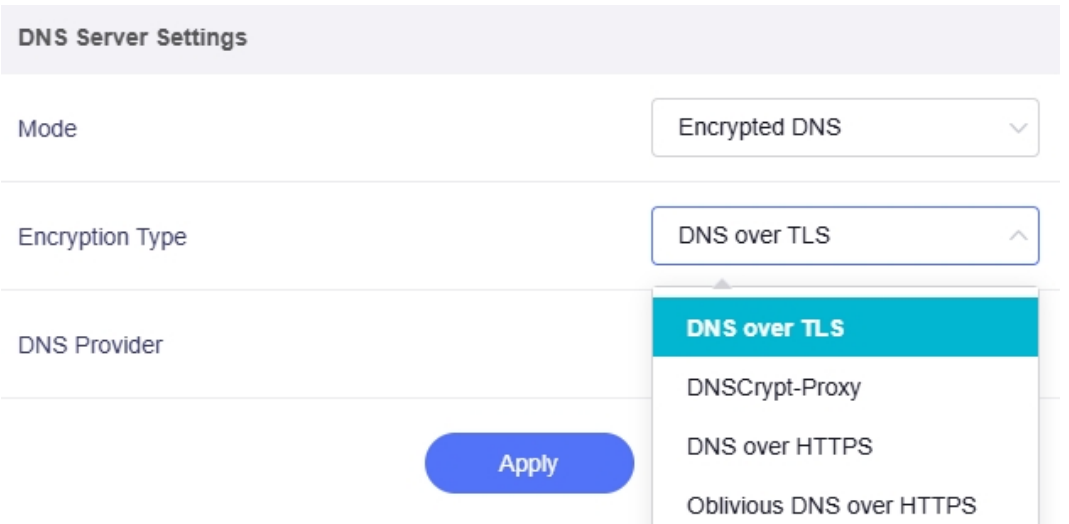


1. **Automatic**: When selected, the router will automatically obtain DNS server addresses from the upstream network and apply them to all connected devices.



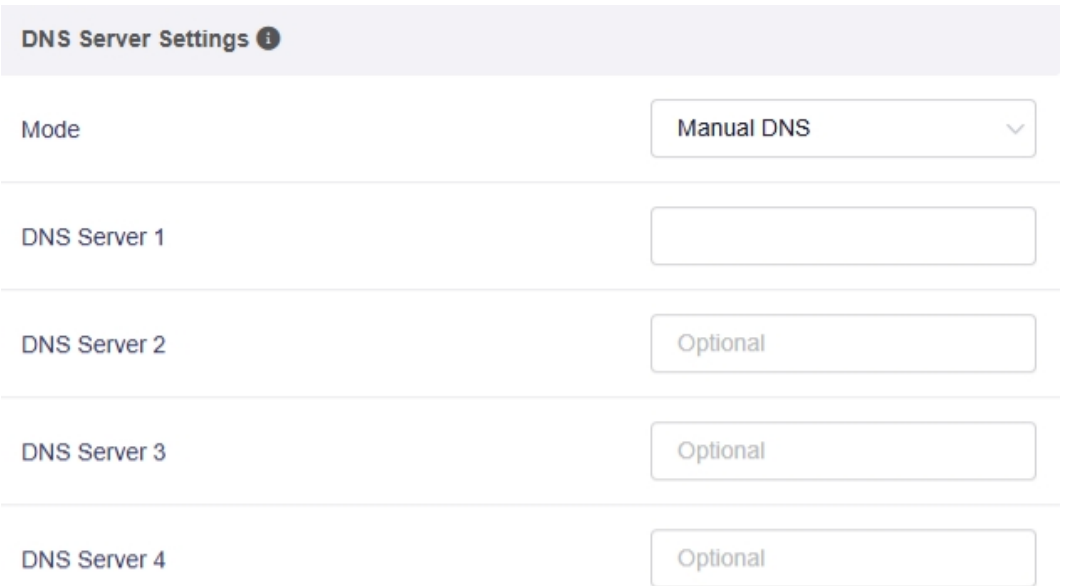
2. **Encrypted DNS**: When selected, the router will use encrypted protocols to process DNS queries, securing resolution data against eavesdropping or tampering.

It has four encryption type: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS, and Oblivious DNS over HTTPS.



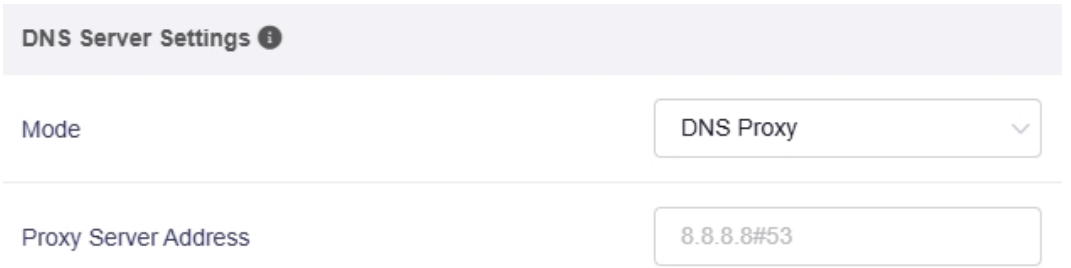
- For DNS over TLS, select a DNS provider among Control D, NextDNS, and Cloudflare.
- For the other three (i.e., DNSCrypt-Proxy, DNS over HTTPS, and Oblivious DNS over HTTPS), select at least one DNS server from the repository. Up to 8 servers can be selected. When multiple servers are selected, the 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.

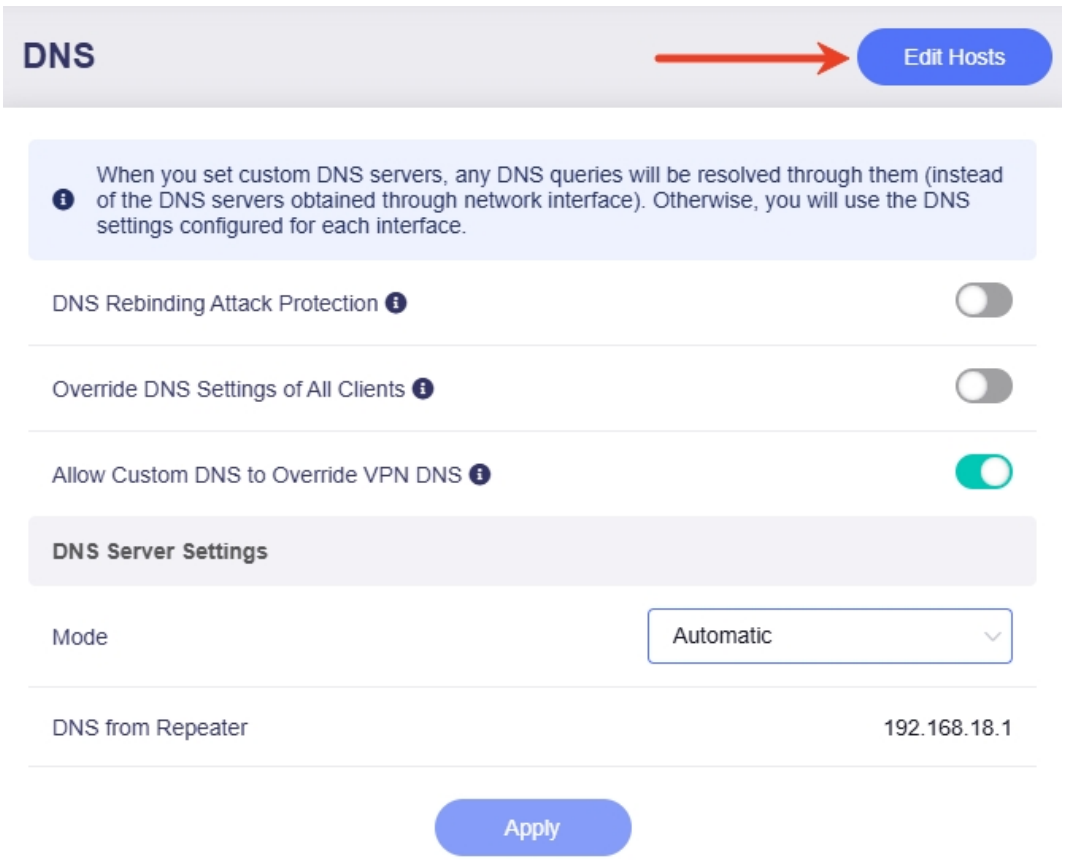
4. **DNS Proxy**: When selected, the router forwards all DNS queries through a proxy server, allowing resolution via the proxy's network environment for specific access needs.



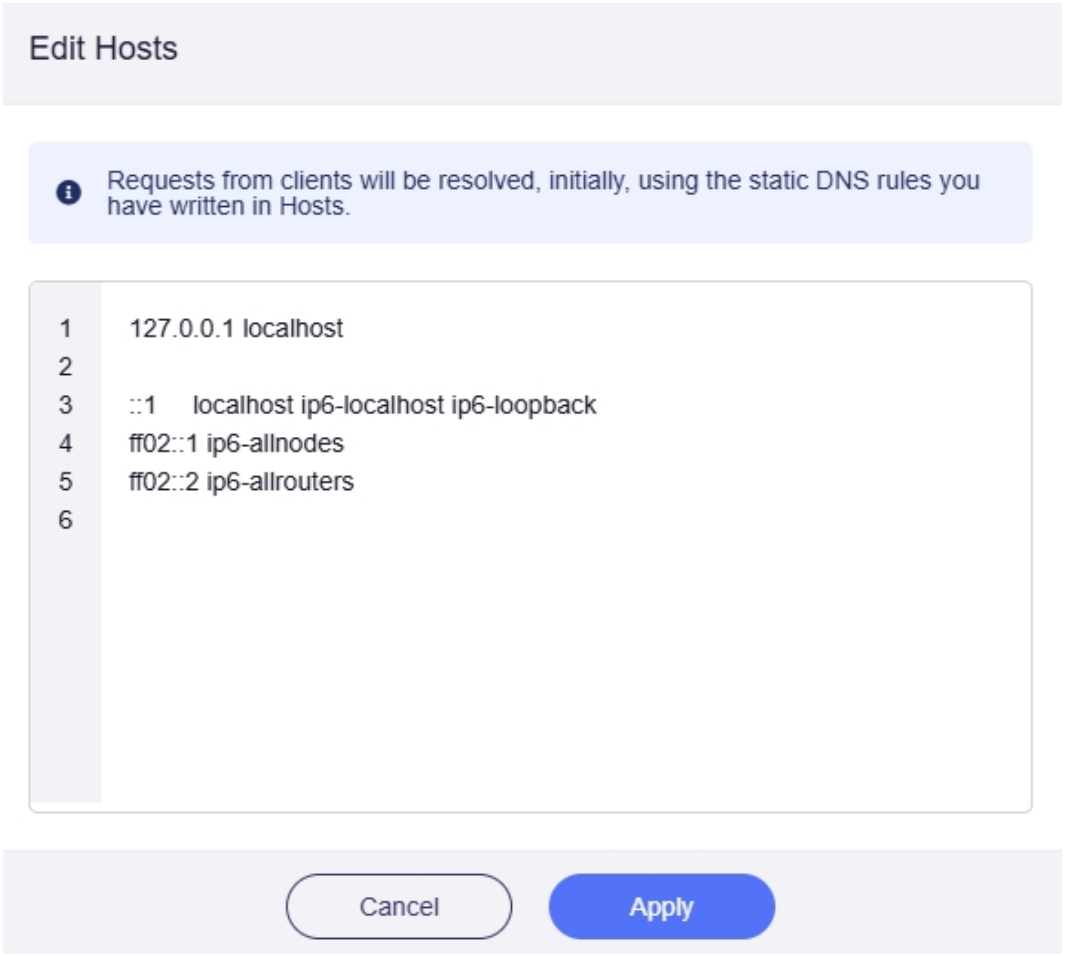
13.4.2 Edit Hosts

You can define static DNS resolution rules as needed.

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



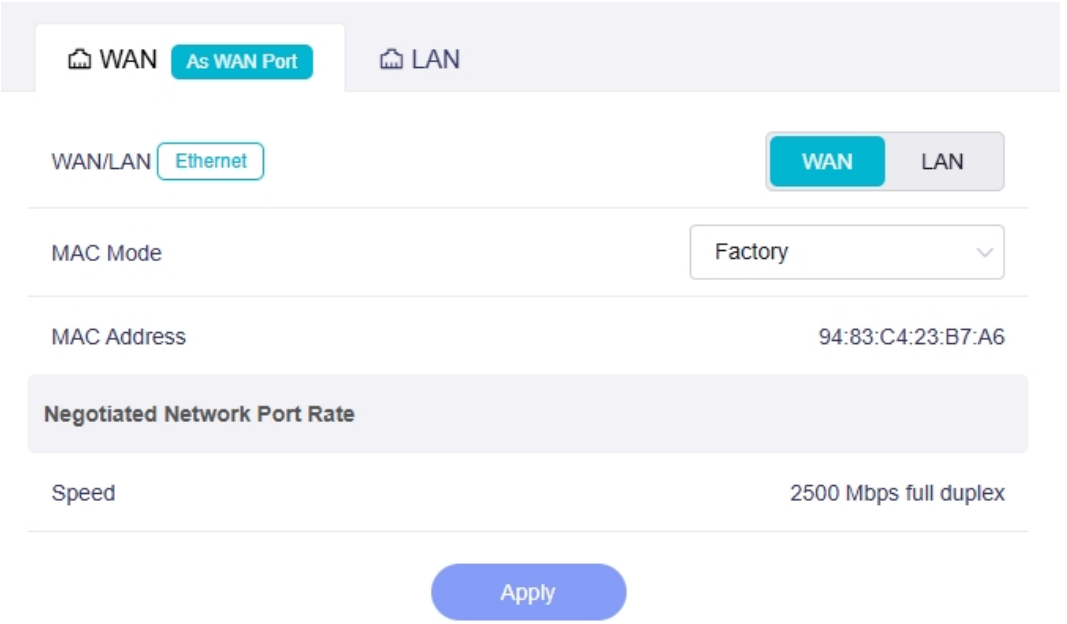
Requests from clients will be resolved preferentially using the static DNS rules written here, allowing you to manually map IP addresses to hostnames (e.g., the default entries like 127.0.0.1 localhost for local loopback) for customized domain name resolution control.


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

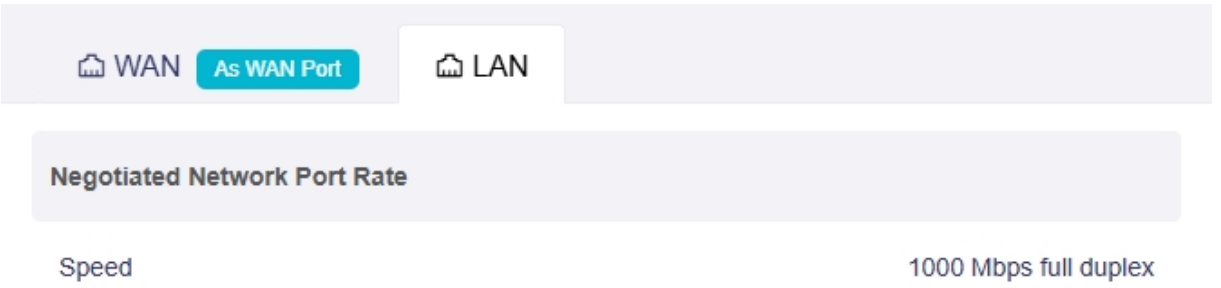
13.5 Port Management

Log in to your router's web admin panel and navigate to **NETWORK** > **Port Management**. This page allows you to manage the router's Ethernet ports.

The **WAN** section displays the port role (WAN or LAN), MAC address, and negotiated rate.



The **LAN** section displays the LAN port negotiated rate.

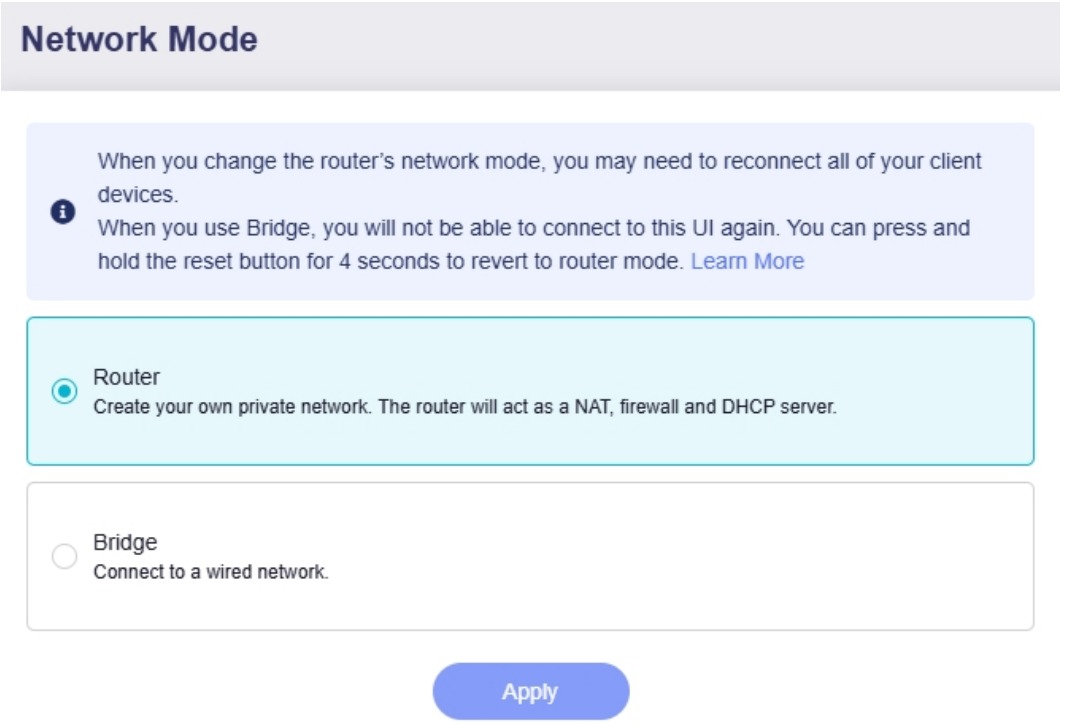


Note: The negotiated rate for WAN and LAN ports is displayed only when an Ethernet cable is connected. It depends on both the Ethernet port and the Ethernet cable.

13.6 Network Mode

Network mode refers to the different operational roles and functionalities 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. Brume 2 supports two modes: Router and Bridge mode.



- **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.
- **Bridge**: Allows the router to connect to a wired network and function as a bridge between network devices. In this mode, the router essentially operates as a switch, forwarding data between connected devices without performing NAT, firewall, or DHCP services. This enables seamless communication between devices on the same network by acting as a simple connection point rather than a network gateway.

Note:

1. When the network mode is changed, devices need to reconnect to the router to ensure a stable connection.
2. **In Bridge 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 Bridge mode, the following features will be unavailable**: Access Control (Allowlist and Blocklist), AstroWarp, VPN, Tor, AdGuard Home, Parental Control, ZeroTier, Tailscale, Port Forwarding, Multi-WAN, DHCP Server, Address Reservation, DNS, Port Management, IPv6, Drop-in Gateway, IGMP Snooping, Network Acceleration, NAT Settings.

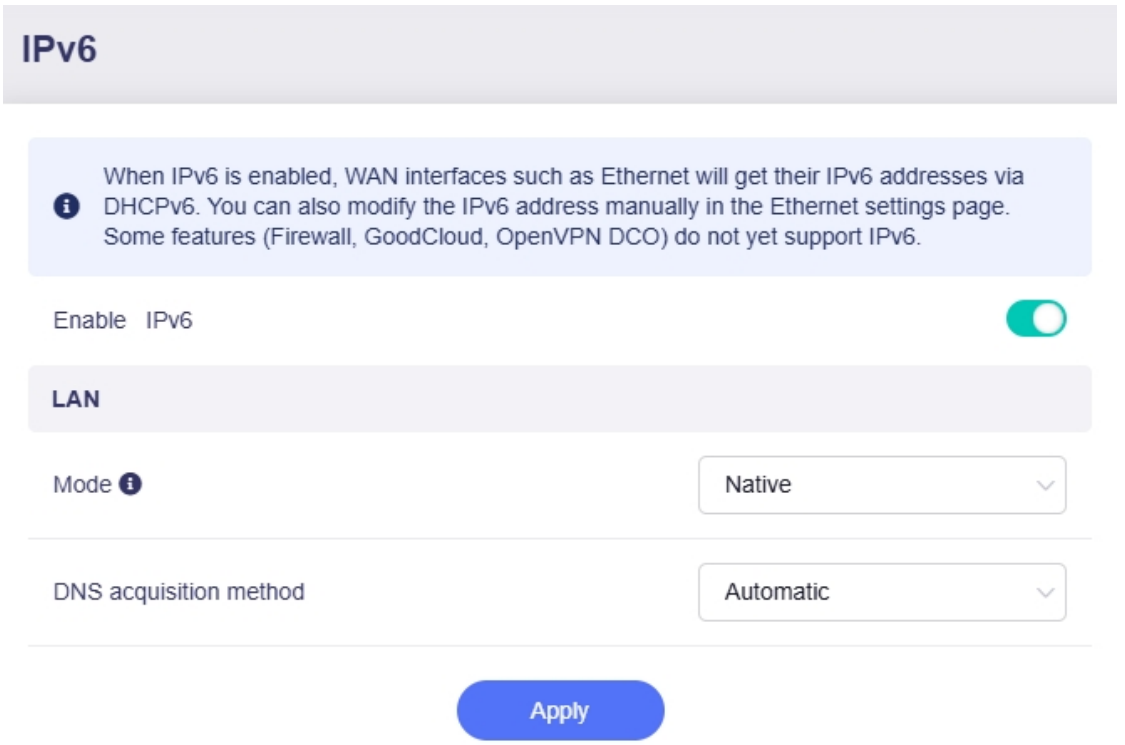
13.7 IPv6

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.

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

Toggle on **Enable IPv6**, select the mode for your main network and DNS acquisition method, then click **Apply.**



13.7.1 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.

13.7.2 DNS acquisition method

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

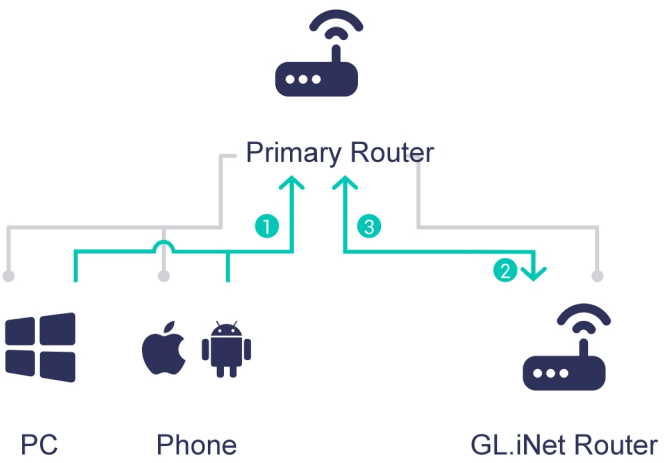
- **Automatic**: The router will obtain IPv6 DNS server addresses dynamically (e.g., via DHCPv6).
- **Manual**: Input custom IPv6 DNS server addresses. However, since DNS is used to resolve domain names to their corresponding IP addresses, manual DNS server configuration may result in DNS lookup failures.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

13.8 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:

- Filter advertisements via AdGuard Home
- 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 as 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.

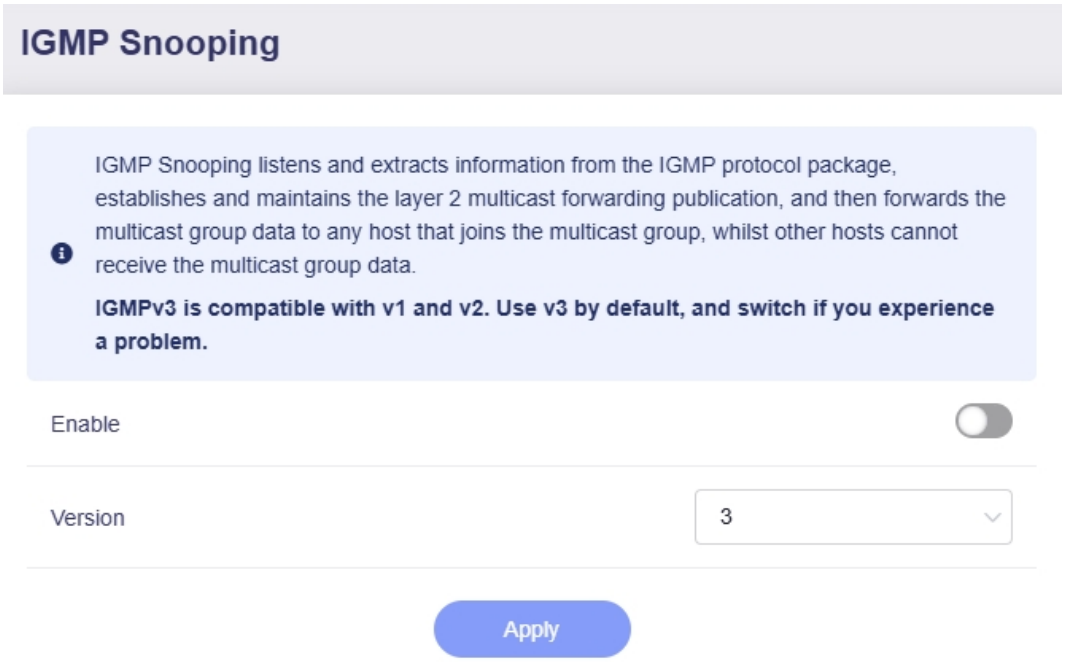
- **Green lines** depict the sequential data transmission path when Drop-in Gateway is active, with the numbered arrows indicating the traffic flow order:
    1. Traffic from client devices is first routed to the primary router;
    2. The primary router forwards the traffic to the GL.iNet router for 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.

You can enable Drop-in Gateway for all or specific devices connected to your primary router. See this link for more instructions.

13.9 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.

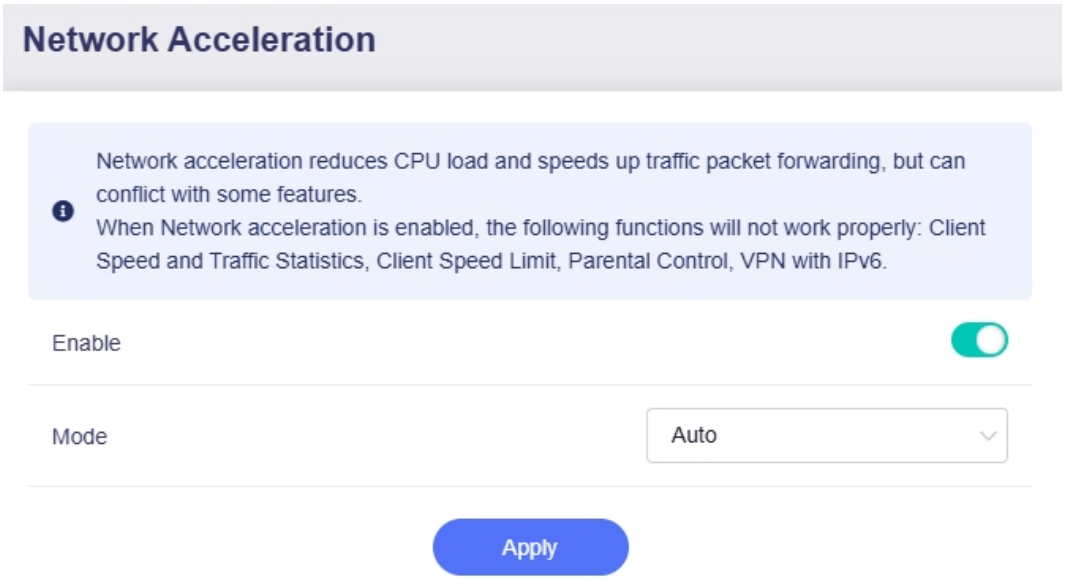
Log in to your router's web admin panel and navigate to **NETWORK** > **IGMP Snooping**. You can enable it to use the multicast function on your router as needed.



13.10 Network Acceleration

Network acceleration reduces CPU load and speeds up traffic packet forwarding, but can conflict with some features.

Log in to your router's web admin panel and navigate to **NETWORK** > **Network Acceleration**. This page allows you to enable network acceleration and select acceleration mode among Auto, Hardware Acceleration and Software Acceleration.

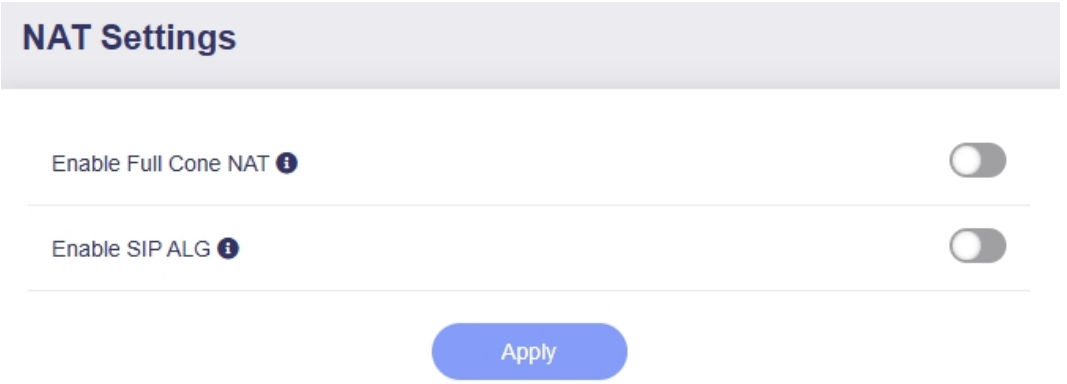


- **Auto**: Automatically switch between the two acceleration modes based on actual usage.
- **Hardware Acceleration**: It offloads high-frequency network tasks (e.g., NAT, packet forwarding, checksum verification) to dedicated hardware like NPUs or HWNAT chips. It specifically works on Ethernet (wired WAN/LAN) and Repeater connections (unavailable on Brume 2), excelling in these scenarios with fixed paths and simple rules to deliver high throughput, low latency, and minimal CPU load for wire-speed data transmission.
- **Software Acceleration**: It relies on a router's general CPU paired with optimized kernels or drivers (e.g., SWNAT). It works on Cellular (4G/5G) connection, typically the primary scenario where hardware acceleration is unavailable, offering strong compatibility and support for complex protocols. While flexible, it may hit CPU bottlenecks under high-bandwidth loads, especially when running advanced features like QoS or port forwarding.

Note: When Network acceleration is enabled, the following functions will not work properly: Client Speed Statistics, Traffic Statistics, Speed Limit, Parental Control, VPN with IPv6, Data Statistics, Content Filter, QoS, and SQM.

13.11 NAT Settings

Log in to your router's web admin panel and navigate to **NETWORK** > **NAT Settings**. This page allows you to configure two key NAT-related features: Full Cone NAT and SIP ALG.



- **Full Cone NAT**: It can be used to reduce game latency, enhancing the responsiveness of online gaming. However, enabling Full Cone NAT may be less secure as it allows unrestricted incoming connections.
- **SIP ALG**: It is intended to mitigate the effects of multiple NATs on SIP (Session Initiation Protocol) traffic. However, in most cases, it will not help and may even affect VoIP calls, causing issues like one-way audio, phones not ringing, unexpected call drops, or calls going directly to voicemail.

Chapter 14

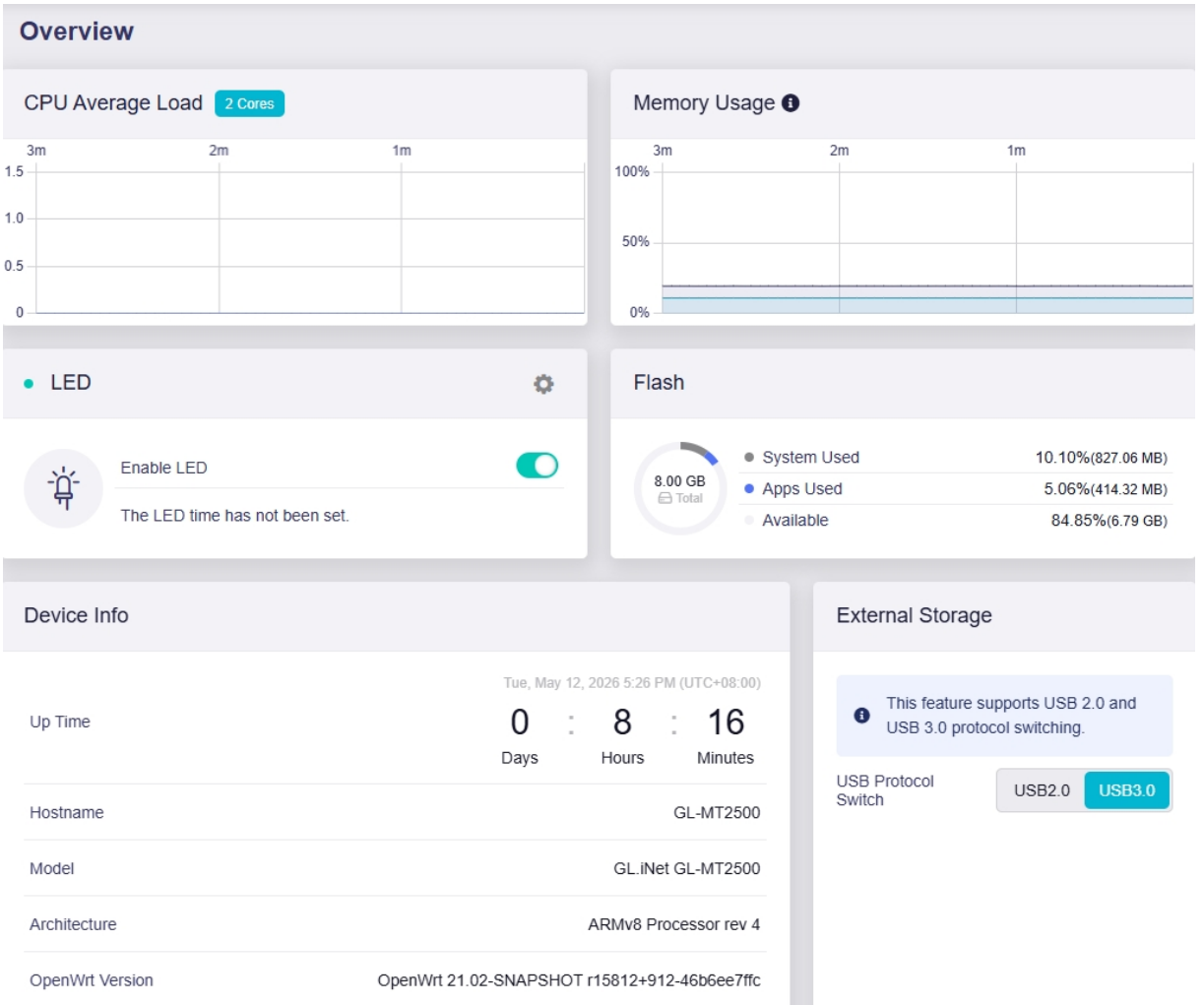
System

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

14.1 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
- External Storage Protocol Switch

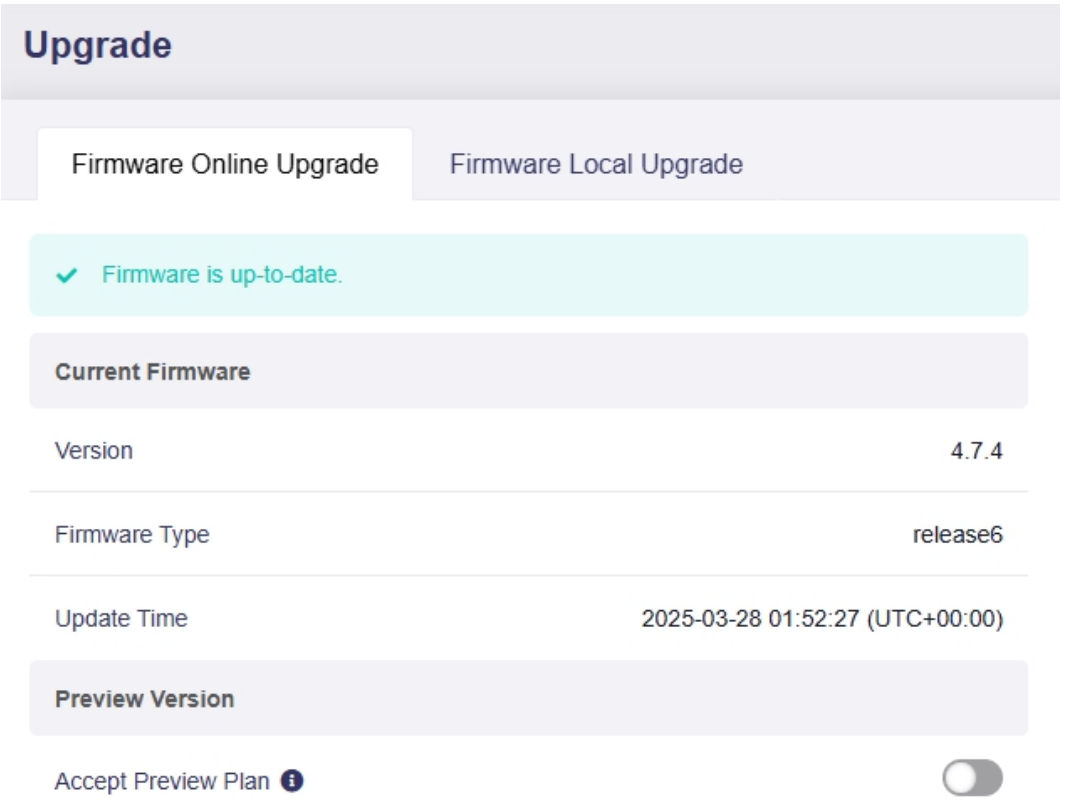


14.2 Upgrade

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.

14.2.1 Online Upgrade

You can find the current firmware details here, including firmware version, firmware type (e.g., release, beta), and update time.



- **Accept Preview Plan**: If this option is enabled, you can try new features before the final version is issued and provide us with feedback. Set it once and it stays on. Note that these upgrades may not be stable.

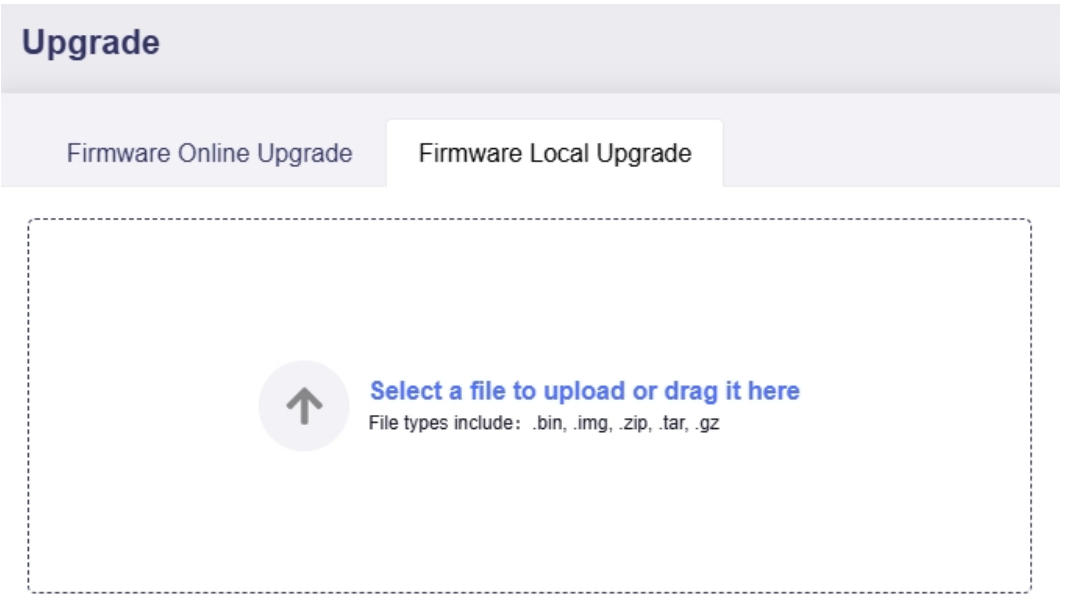
If your router is connected to the Internet, it will check for the newer firmware version available for download.

Tips: 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).

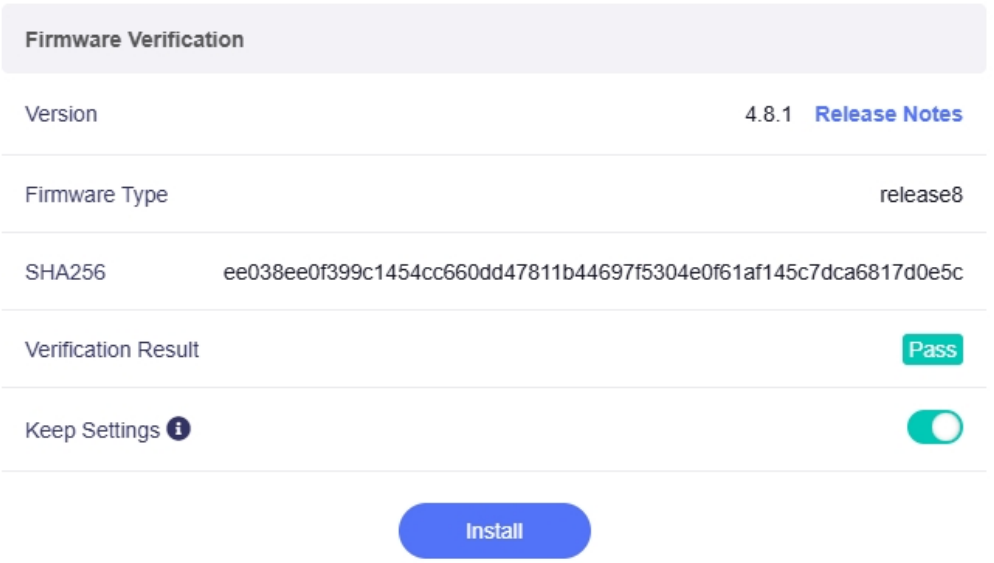
14.2.2 Local Upgrade

This method 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**.



- **Keep Settings**: If 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.

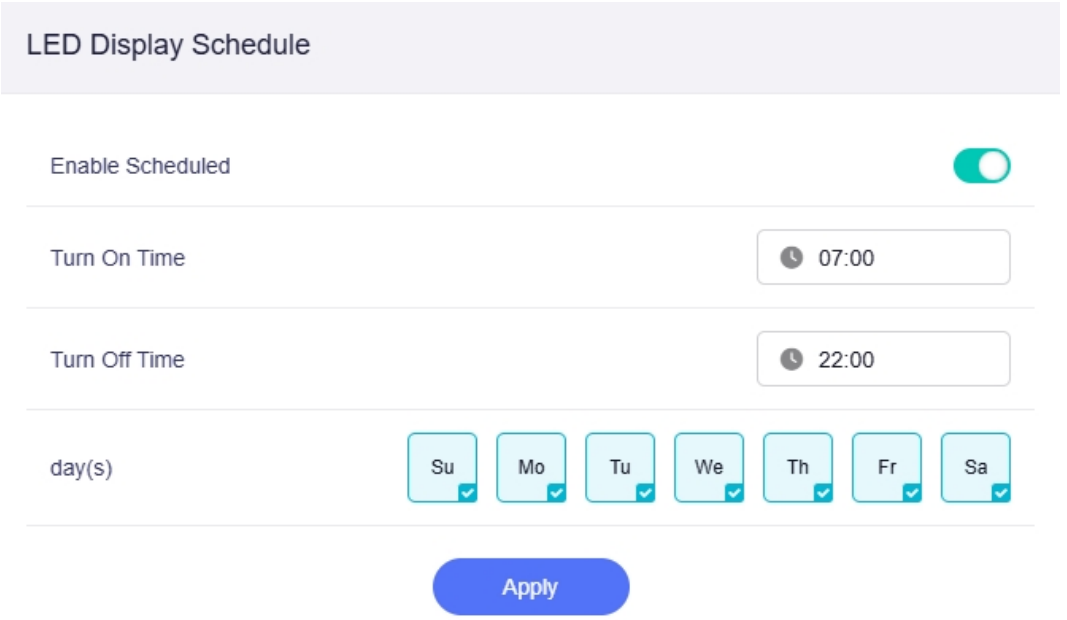
14.3 Scheduled Tasks

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 first 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.

14.3.1 LED Display Schedule

This function allows you to set a schedule for your router's LED light.

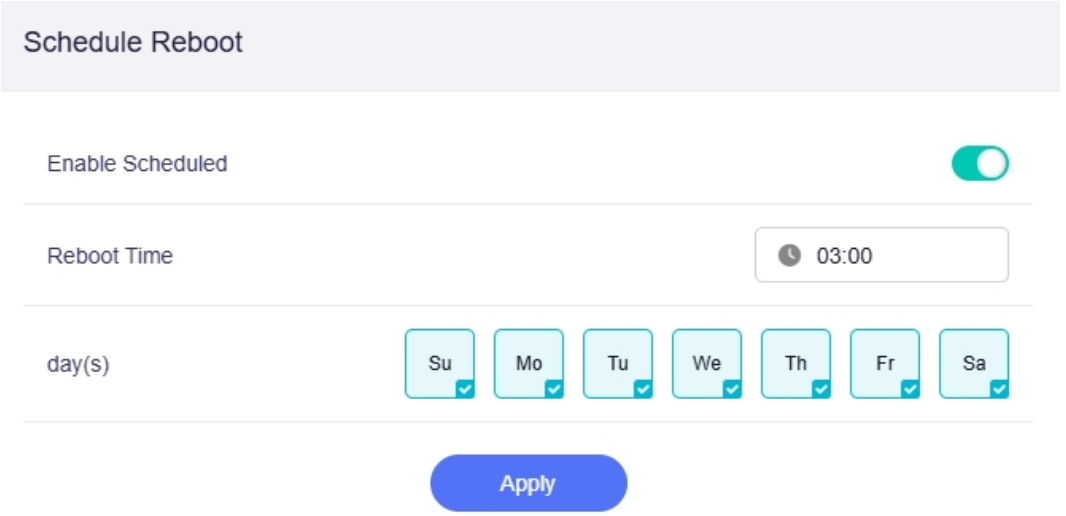


- **Enable Scheduled**: Toggle this switch to enable the LED display schedule.
- **Turn On Time**: Set the time (e.g., 07:00) when the LED light will turn on.
- **Turn Off Time**: Set the time (e.g., 22:00) when the LED light will turn off.
- **day(s)**: Select the effective days of the week for these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

After configuring, click **Apply** to save your settings.

14.3.2 Schedule Reboot

This function allows you to set a schedule for automatically restarting your router.

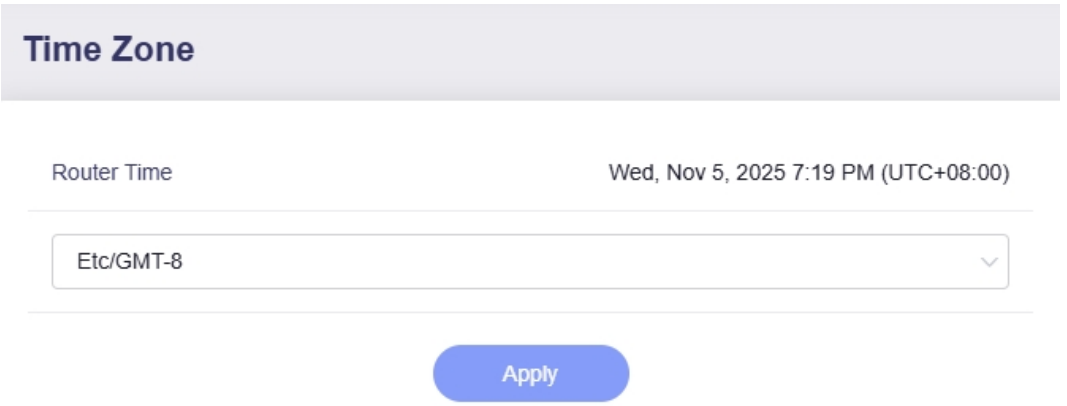


- **Enable Scheduled**: Toggle this switch to enable the scheduled reboot.
- **Reboot Time**: Set the specific time (e.g., 03:00) when the router will restart.
- **day(s)**: Select the effective days of the week for these settings.

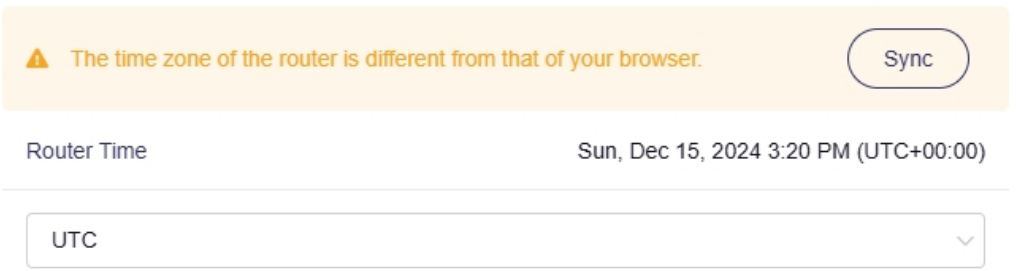
After configuring, click **Apply** to save your settings.

14.4 Time Zone

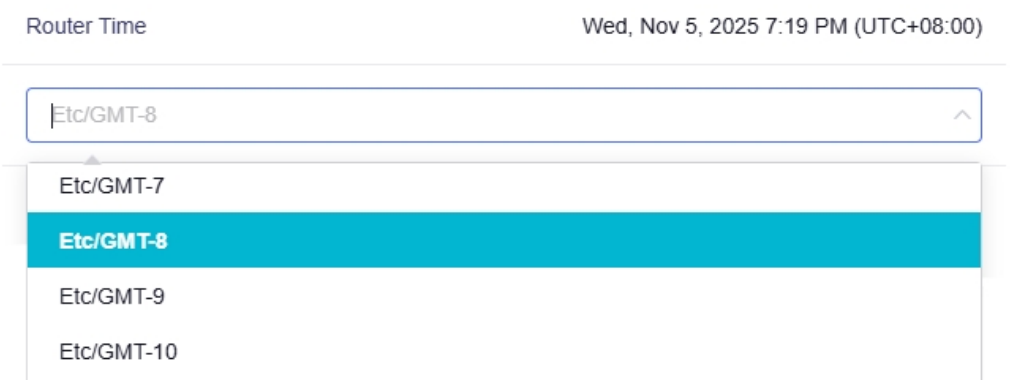
Log in to your router's web admin panel and navigate to **SYSTEM** > **Time Zone**. This page displays your router's system time, indicating the date, time, and corresponding time zone offset.



Some functions rely on the router's system time to take effect. Therefore, 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.

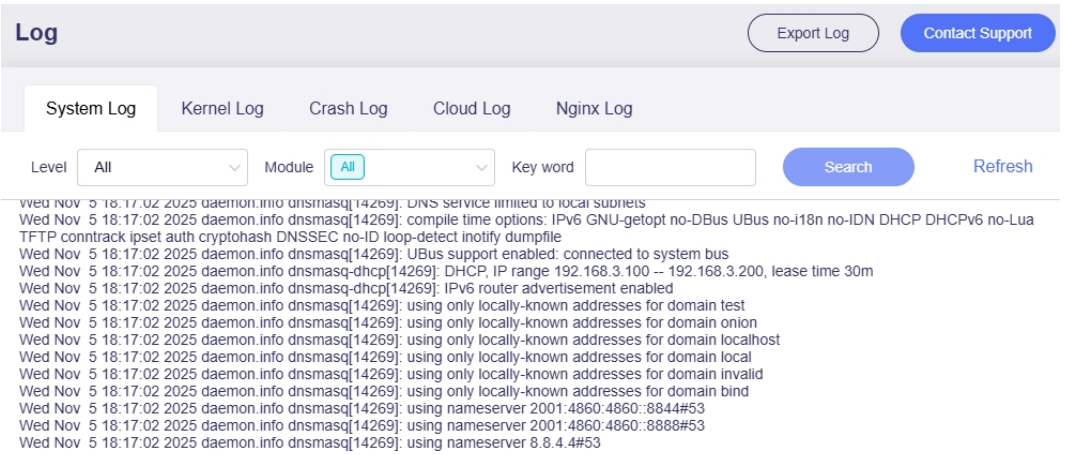


To switch time zone, select the appropriate time zone from the list to ensure the router's system time matches your local time.

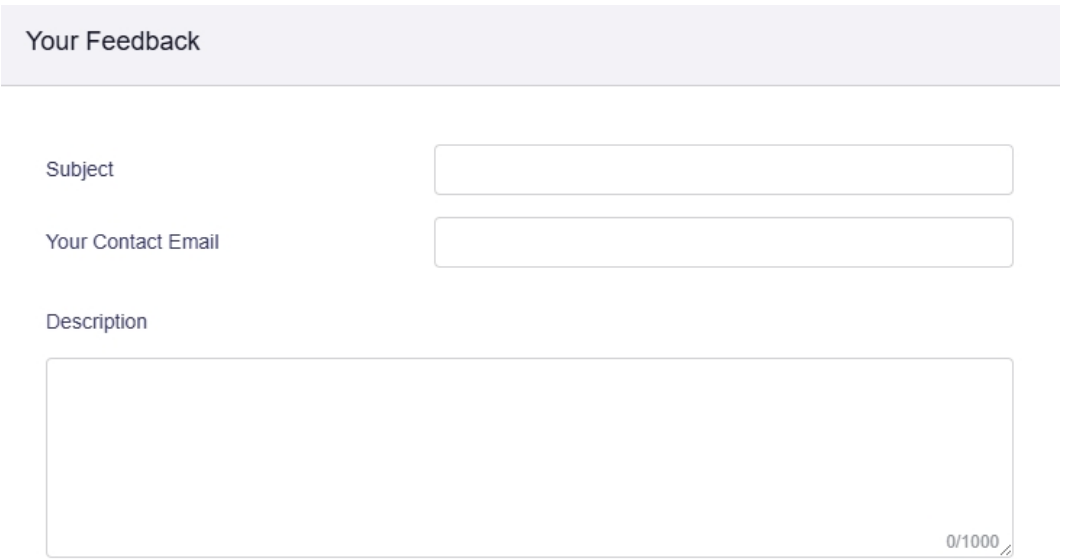


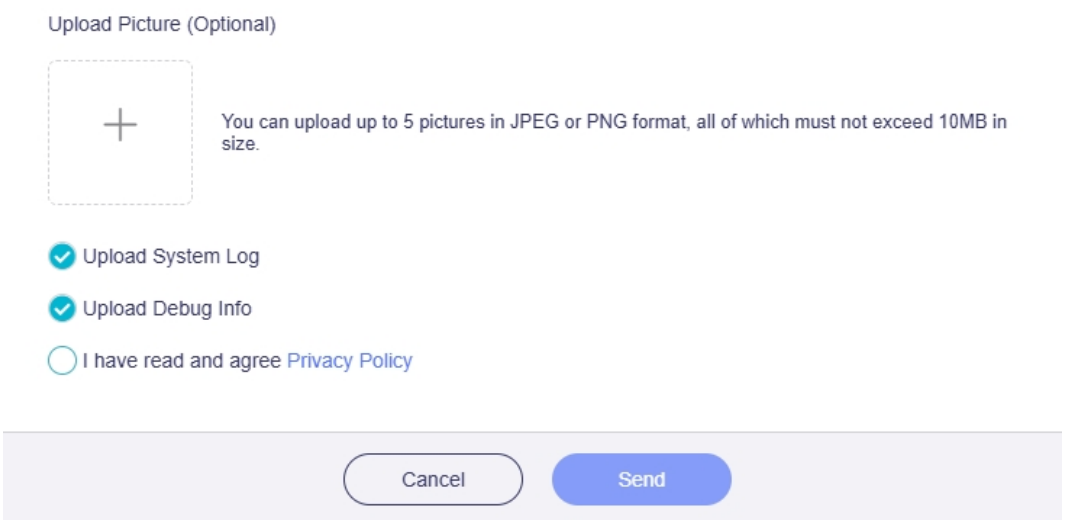
14.5 Log

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. In addition, some cellular models that supports eSIM also provides eSIM log.



- **Search**: The system log page provides filtering for quick search. You can select the log level (e.g., all, info, error) or module (e.g., IPv6, Tethering, Cellular) from the drop-down list, or enter keywords to quickly query logs.
- **Refresh**: Click this button to refresh logs.
- **Export Log**: Click this button to export debug info along with the logs.
- **Contact Support**: Click this button, fill in detailed information in the pop-up window on the right, then click **Send**. Your feedback will be sent directly to GL.iNet Technical Support.




Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

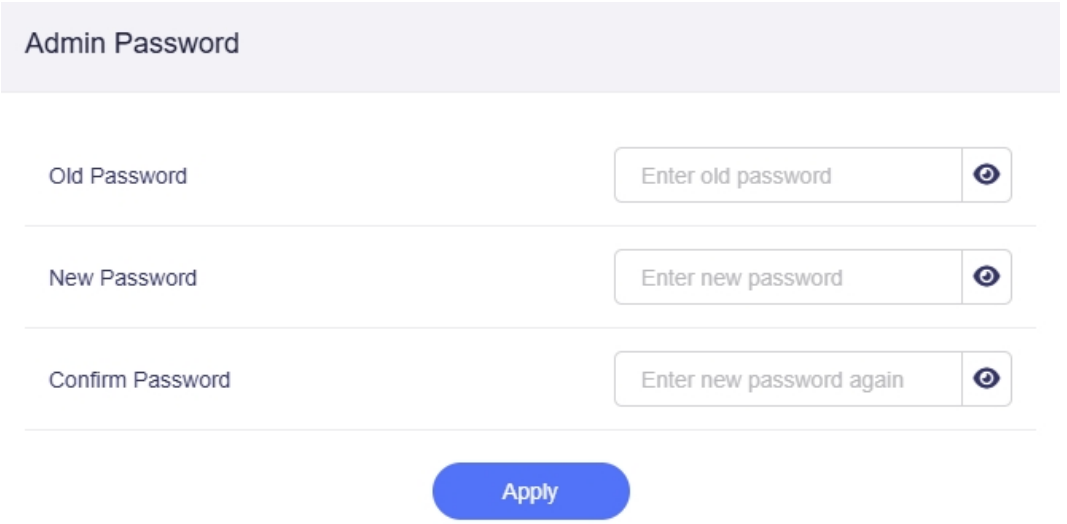
14.6 Security

Log in to your router's web admin panel and navigate to **SYSTEM** > **Security**. This page contains configuration options for the router's local and remote management, including:

- Admin password
- Local access for web admin panel, LuCI, and SSH
- Remote HTTPS/SSH access
- Router open ports management

14.6.1 Admin Password

In this section, you can change the login password of the web admin panel.

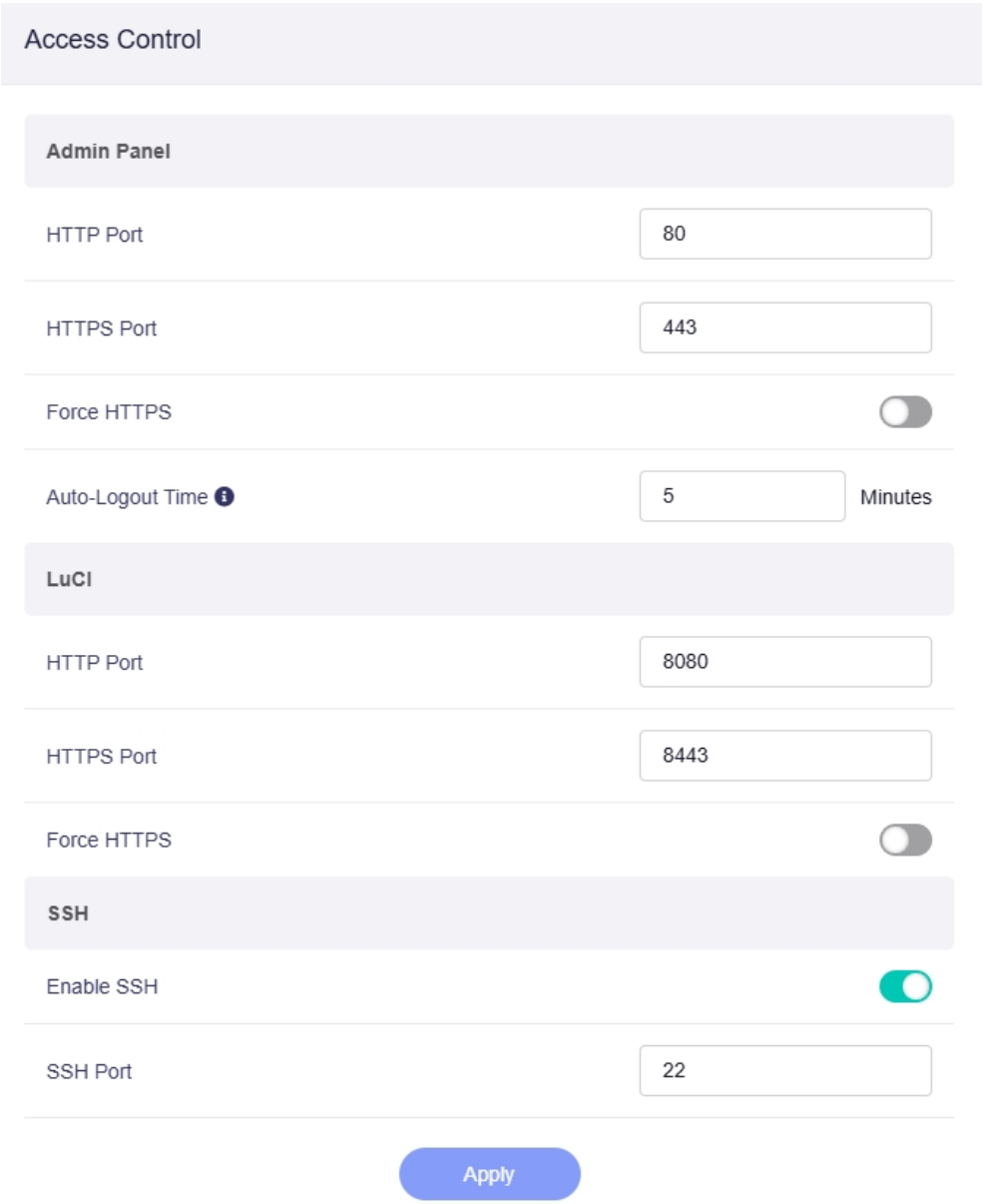


The requirements for the admin password are as follows:

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.

14.6.2 Access Control

This section manages access to the router's multiple interfaces (Admin Panel, LuCI, and SSH). It can prevent scanning and intrusion attempts on the default port and avoid network problems caused by port conflicts.



Admin Panel

- **HTTP Port**: Defaults to 80, used for unencrypted HTTP access to the web admin panel.
- **HTTPS Port**: Defaults to 443, used for secure HTTPS access to the web admin panel.
- **Force HTTPS**: When enabled, access to the web admin panel is enforced to use a secure HTTPS connection.

- **Auto-Logout Time**: Set to 5 minutes by default, it automatically logs out idle admin sessions after this duration for security. You can customize the auto-logout time, ranging from 1 minute to 3 hours.

LuCI

Note: Please install LuCI on the Advanced Settings before setting the access control for it.

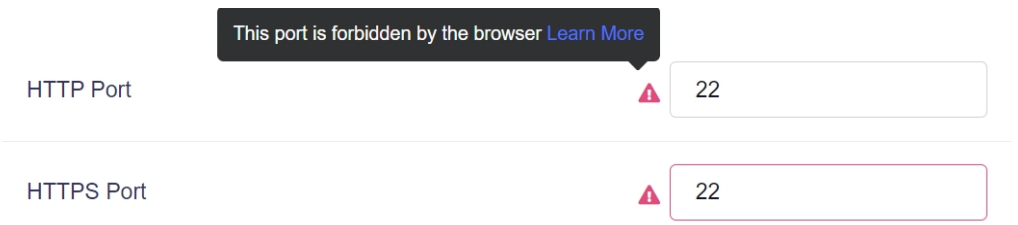
- **HTTP Port**: Defaults to 8080, for unencrypted HTTP access to the LuCI interface.
- **HTTPS Port**: Defaults to 8443, for secure HTTPS access to the LuCI interface.
- **Force HTTPS**: When enabled, access to the LuCI interface is enforced to use a secure HTTPS connection.

SSH

- **Enable SSH**: Enabled by default, it controls whether the SSH access to the router is permitted.
- **SSH Port**: Defaults to 22, the port used for SSH access to the router.

Note:

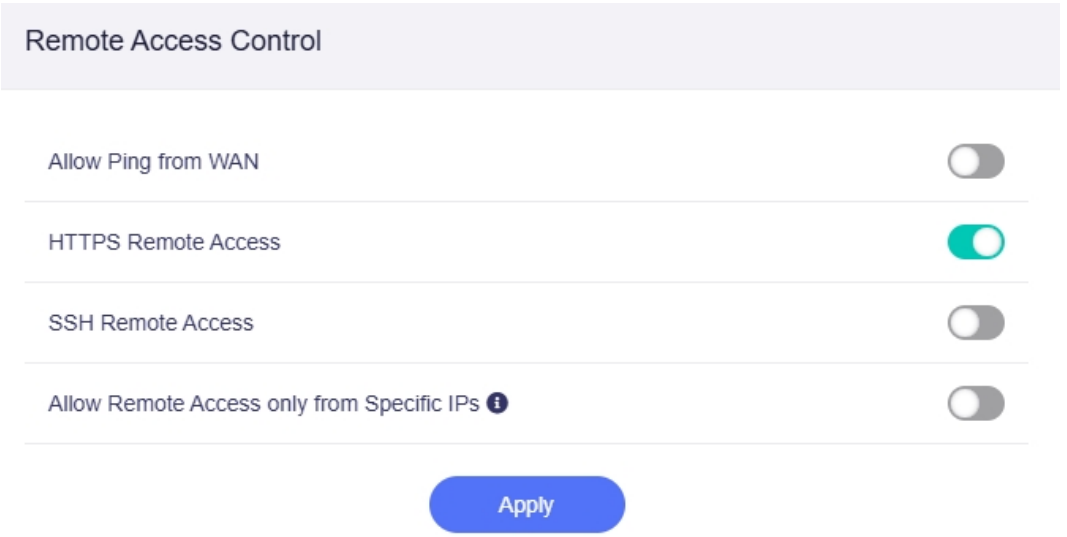
1. If you assign a port number that conflicts with a reserved port (or one reserved for specific services by browsers/network conventions), a prompt will appear stating "This port is forbidden by the browser".



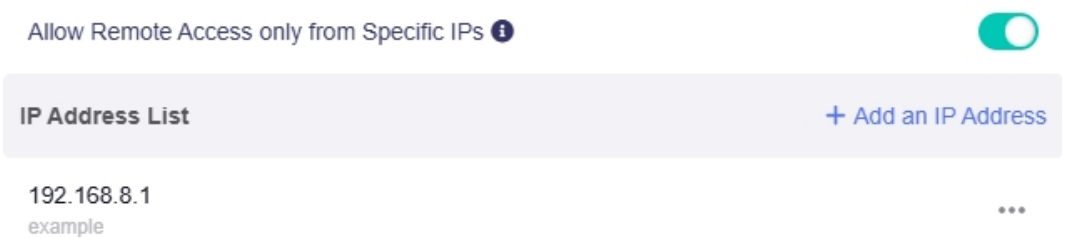
2. If the port number is modified in the firmware, you need to enter the correct port number to access the admin panel. If you forgot the port number, please reset the router to restore the default port number.
3. LuCI access settings are available only after LuCI is installed. If these settings are not visible, go to **SYSTEM** > **Advanced Settings** to install LuCI.

14.6.3 Remote Access Control

This section manages remote access to router interfaces, including HTTPS, SSH and WAN-side ping. It also allows you to restrict access from specific IP addresses, striking a balance between remote accessibility and network security.

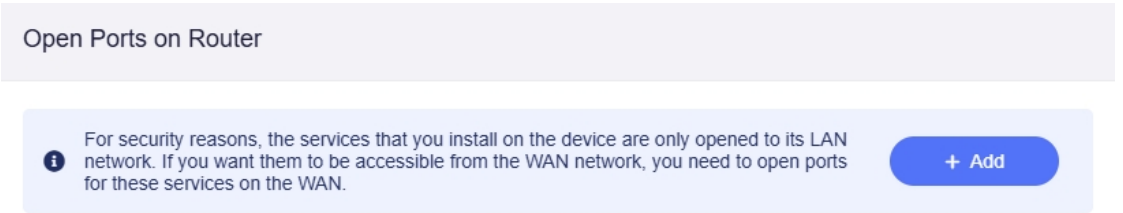


- **Allow Ping from WAN**: Allowing Ping from the router's WAN side can help users check whether the router is reachable over the WAN when there is a network issue, as well as determine network latency and packet loss.
- **HTTPS Remote Access**: HTTPS Remote Access enables secure remote access to the router's web admin panel via the HTTPS protocol. It ensures encrypted data transmission when managing the router remotely through a web browser.
- **SSH Remote Access**: SSH Remote Access enables secure access to the router terminal. It allows users to remotely manage the router via SSH, establishing an encrypted tunnel for tasks.
- **Allow Remote Access from Specific IPs**: This feature is only available when any of the above three features are enabled. You can add multiple specified IP addresses to remotely manage the router only from devices with these IPs.

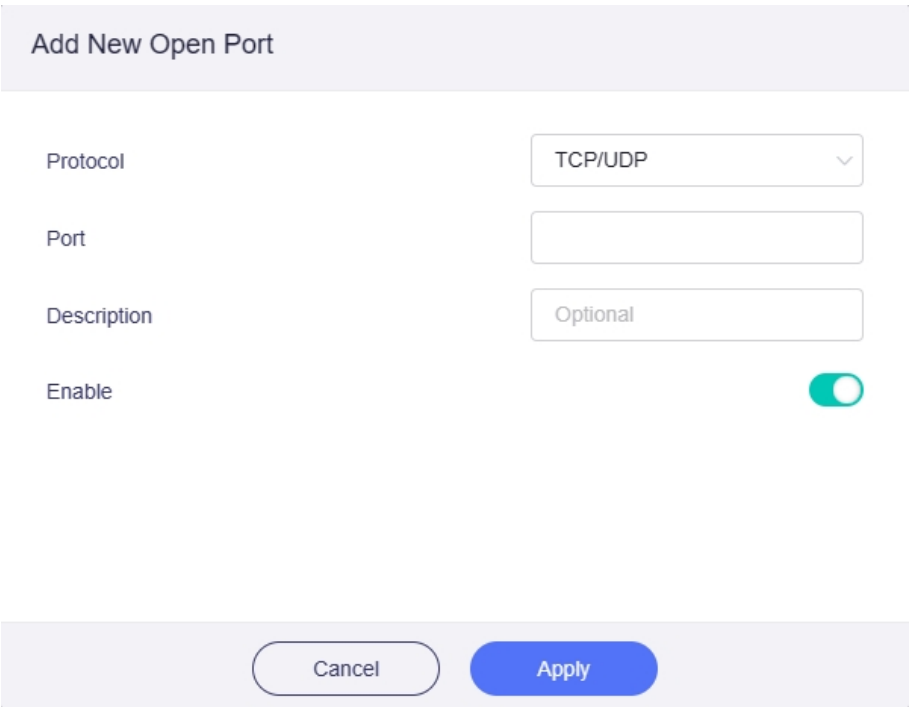


14.6.4 Open Ports on Router

This section manages port forwarding for services on your router. Some services, such as web and FTP, require their respective ports to be opened on the router in order to be publicly reachable from the WAN network. For security reasons, services installed on the device are only accessible within the LAN by default. If you need to enable such WAN access, you can open specific ports here.



To open a port, click **Add**, and enter the required information in the pop-up window.

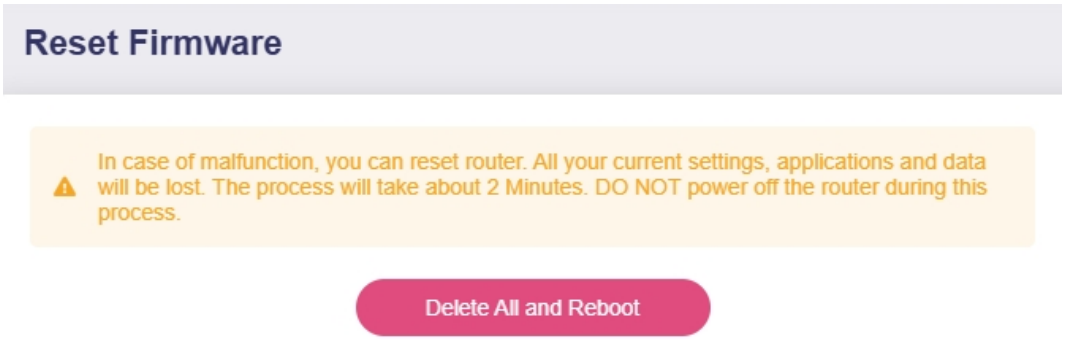


- **Protocol**: Select the network protocol (TCP, UDP, or TCP/UDP) for the port. This determines how data is transmitted for the service associated with the port.
- **Port**: Enter the specific port number you want to open.
- **Description** (Optional): Add a brief note to describe the purpose of this open port (e.g., “Web Server” or “FTP Service”) for easier management.
- **Enable**: Toggle this switch to activate or deactivate the port forwarding rule.

14.7 Reset Firmware

Log in to your router's web admin panel and navigate to **SYSTEM** > **Reset Firmware**. If the router malfunctions, you can try to resolve the issue by resetting the firmware.

Click the **Delete All and Reboot** button to reset the firmware as needed.



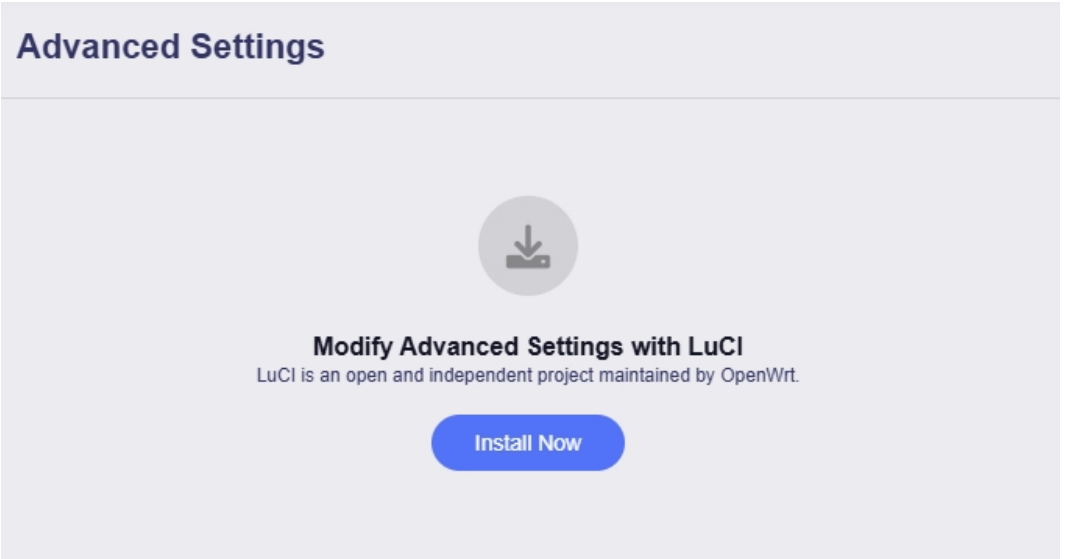
Note: All your current settings, applications and data will be cleared. The process will take about 2 minutes. Do not power off the router during this process.

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

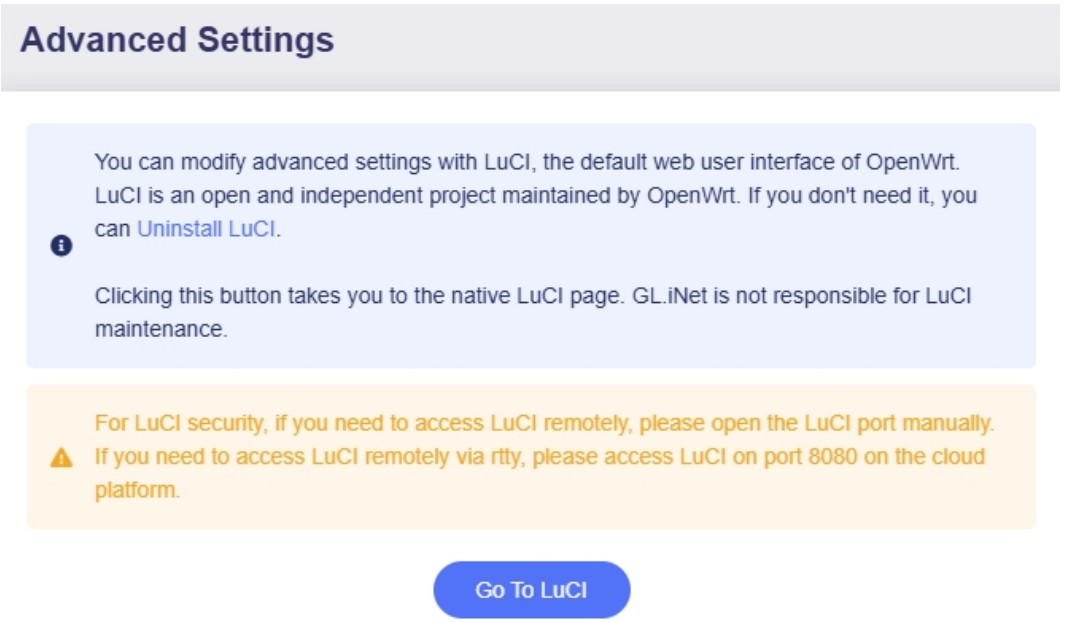
14.8 Advanced Settings

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.

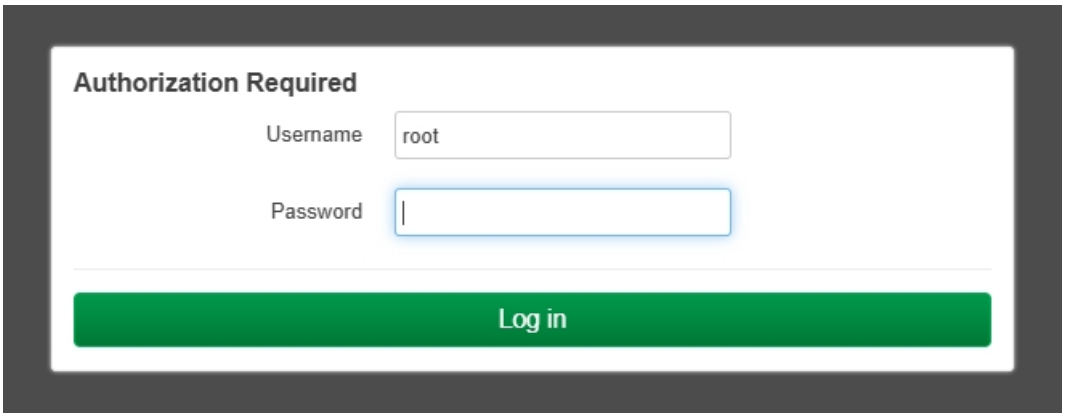
Click the **Install Now** button, and it will be installing LuCI interface.



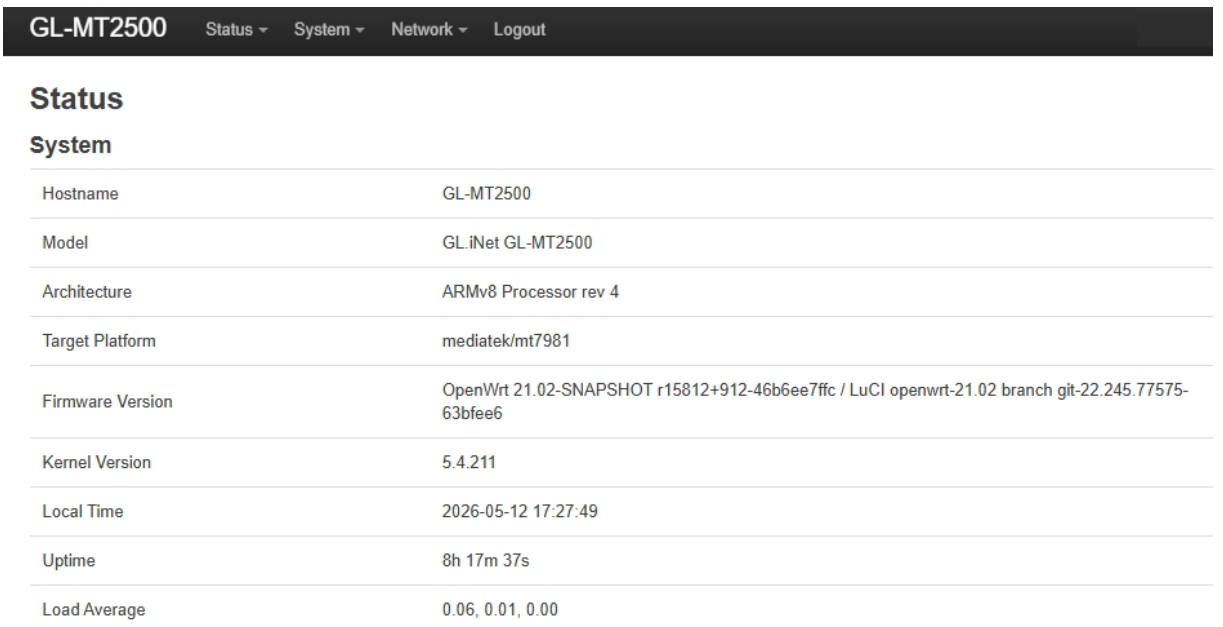
Click the **Go To LuCI** button, and you will be re-directed to the LuCI login page.



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



Then you will be logged into the LuCI page.



Regulatory and Legal

Regulatory Compliance

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

This product complies with the essential requirements and other relevant provisions of Directive 2014/53/EU. A copy of the Declaration of Conformity (DoC) is available at: https://www.gl-inet.com/products/certificate/

RF Exposure Compliance

This equipment complies with FCC/CE RF exposure limits set forth for an uncontrolled environment. To comply with RF exposure requirements, maintain a minimum distance of 20 cm (8 inches) between the device and your body during normal operation.

Trademarks

- Wi-Fi®, Wi-Fi 6™, Wi-Fi CERTIFIED™ are registered trademarks of the Wi-Fi Alliance.
- IEEE® 802.11ax/b/g/n/ac are trademarks of the Institute of Electrical and Electronics Engineers, Inc.
- Other product names, logos, and brands mentioned in this guide are the property of their respective owners.
- GL.iNet and its logo are registered trademarks of GL.iNet Technology (Hong Kong) Ltd.

Limitation of Liability

This product is designed for residential and small office use. GL.iNet shall not be liable for:

- Damages caused by improper installation, misuse, or modification of the device.
- Interference with other electronic equipment due to non-compliance with installation guidelines.
- Loss of data or business interruption resulting from device performance issues, except as required by applicable law.

Software License

The firmware and software included with this device are protected by copyright laws and international treaties. Users are granted a non-exclusive, non-transferable license to use the software solely for operating the device in accordance with this guide. Reverse engineering, decompiling, or modifying the software is prohibited unless permitted by applicable law.

Export Control

This product may be subject to export controls under the laws of the Hong Kong Special Administrative Region of the People's Republic of China (including the Import and Export (Strategic Commodities) Regulations, Chapter 60G of the Laws of Hong Kong), the People's Republic of China (including the Export Control Law of the People's Republic of China and related regulations), and other jurisdictions (e.g., the United States, European Union, Canada, and the United Kingdom). Diversion contrary to applicable laws is prohibited.