



User Manual

GL-MT5000 / Brume 3

Security Gateway

Firmware Version 4.9.0

About This Manual

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

With this guide, you will be able to:

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

Format Conventions

These symbols/colors help you follow steps faster.

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

Note:

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

Need More Help or Info?

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

Copyright © 2026 GL.iNet Technology (HK) Ltd. All rights reserved.

No part of this manual may be reproduced, transcribed, translated, or distributed in any form or by any means, without the prior written permission of GL.iNet Technology (HK) Ltd. GL.iNet is a registered trademark of GL.iNet Technology (Hong Kong) Ltd. in China and/or other countries and regions. All other brand and product names mentioned herein are trademarks or registered trademarks of their respective owners.

The content of this document is subject to change without notice due to product version upgrades or other reasons. Unless otherwise agreed, this document is provided for informational purposes only, and all statements, information, and recommendations contained herein do not constitute any form of warranty.

GL Tech (HK) Ltd: #601, 5W, Hong Kong Science Park, N.T. Hong Kong

GL Intelligence, Inc.: 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Contents

Chapter 1	Get To Know Your Router	6
1.1	Product Overview	7
1.1.1	Appearance	7
1.1.2	Interface and Button	8
1.1.3	LED	9
1.2	Specifications	9
1.3	Package Contents	10
Chapter 2	Hardware Connection	11
2.1	Choosing a Location	12
2.2	Connecting the Router	12
Chapter 3	Log In To Your Router	13
Chapter 4	Set Up Internet Connection	15
4.1	Use Quick Setup Wizard	16
4.2	Manually Set Up Internet Connection	17
4.2.1	Connect to the Internet via Ethernet Cable	18
4.2.2	Connect to the Internet via USB Tethering	22
4.2.3	Connect to the Internet via USB Modem	27
Chapter 5	Clients	29
5.1	Device Details	31
5.2	Action	33
5.3	Remove Clients	36
5.4	Sort	37
Chapter 6	Cloud Services	38
6.1	GoodCloud	39
6.1.1	Enable GoodCloud	40
6.1.2	Manage Your Router	42
6.1.3	Unbind Device	47
6.1.4	Disable GoodCloud	47
6.2	AstroWarp	48
6.2.1	Quick Setup	48
6.2.2	Test Connectivity	52
6.2.3	Upgrade Plan	53

Chapter 7 Get To Know VPN	54
7.1 Introduction	55
7.2 Application Scenarios	56
Chapter 8 VPN Dashboard	58
8.1 Upload VPN Profile	59
8.2 Add VPN Tunnel	62
8.2.1 General Steps	62
8.2.2 Case Reference	64
8.3 Kill Switch	80
8.4 All Other Traffic	81
8.5 Tunnel Options	82
8.6 Tunnel Priority	84
Chapter 9 Set Up VPN Server	86
9.1 Set Up OpenVPN Server	87
9.1.1 Preparation	87
9.1.2 Setup Steps	88
9.1.3 Troubleshooting	90
9.2 Set Up WireGuard Server	91
9.2.1 Preparation	91
9.2.2 Setup Steps	92
9.2.3 Troubleshooting	95
Chapter 10 Set Up VPN Client	96
10.1 Set Up OpenVPN Client	97
10.1.1 Preparation	97
10.1.2 Set Up NordVPN	97
10.1.3 Set Up OpenVPN Client Manually (for other providers)	103
10.2 Set Up WireGuard Client	106
10.2.1 Preparation	106
10.2.2 Set Up AzireVPN	107
10.2.3 Set Up Hide.me	111
10.2.4 Set Up IPVanish	114
10.2.5 Set Up Mullvad	118
10.2.6 Set Up NordVPN	122
10.2.7 Set Up PIA (Private Internet Access)	127

10.2.8 Set Up PureVPN	131
10.2.9 Set Up Surfshark	134
10.2.10 Set Up Windscribe	138
10.2.11 Set Up WireGuard Client Manually (for other providers)	143
Chapter 11 Network	148
11.1 Multi-WAN	149
11.1.1 Interface Status Track	149
11.1.2 Multi-WAN Mode	152
11.2 LAN	155
11.2.1 Basic Settings	155
11.2.2 DHCP Server	156
11.2.3 Address Reservation	158
11.3 DNS	159
11.3.1 DNS Server Settings	160
11.3.2 Edit Hosts	162
11.4 Ethernet Port	164
11.5 IPv6	165
11.5.1 IPv6 Mode	166
11.5.2 DNS acquisition method	166
11.6 IGMP Snooping	167
11.7 Network Mode	168
11.8 Drop-in Gateway	170
11.9 Network Acceleration	172
Chapter 12 Flow Control	174
12.1 DPI Engine	175
12.2 Data Statistics	177
12.2.1 Quick Setup	177
12.2.2 Data Storage Rules	179
12.2.3 Switch Time Range	179
12.2.4 Clear Statistics	180
12.3 Content Filter	181
12.4 QoS	183
12.5 SQM	185
12.6 Parental Control	187

Chapter 13 Security.....	193
13.1 Port Forwarding	194
13.1.1 DMZ	194
13.1.2 Port Forwarding	195
13.2 ACL	197
13.3 Admin Access	199
13.3.1 Access Control	199
13.3.2 Remote Access Control	201
13.3.3 Open Ports on Router	202
13.4 NAT Mode	203
Chapter 14 Applications.....	204
14.1 Plug-ins	205
14.2 Dynamic DNS	206
14.2.1 Enable DDNS	206
14.2.2 Check if DDNS Works	209
14.2.3 HTTPS Remote Access	211
14.2.4 SSH Remote Access	214
14.3 Network Storage	216
14.3.1 Connect Storage	216
14.3.2 Set Up Samba	217
14.3.3 Set Up WebDAV	220
14.3.4 Set Up DLNA	223
14.4 AdGuard Home	224
14.5 Tailscale	226
14.5.1 Set Up Tailscale	227
14.5.2 Allow Remote Access WAN	230
14.5.3 Allow Remote Access LAN	230
14.5.4 Custom Exit Nodes	231
14.5.5 Run Exit Node	232
14.6 ZeroTier	238
14.6.1 Set Up ZeroTier	239
14.6.2 Allow Remote Access WAN	243
14.6.3 Allow Remote Access LAN	244
14.7 Tor	245

Chapter 15 System	246
15.1 Overview	247
15.2 Admin Password	248
15.3 Upgrade	249
15.3.1 Online Upgrade	249
15.3.2 Local Upgrade	250
15.4 Scheduled Tasks	251
15.4.1 LED Display Schedule	251
15.4.2 Schedule Reboot	252
15.5 Time Zone	253
15.6 Reset Firmware	254
15.7 Log	255
15.8 Advanced Settings	257
Regulatory and Legal	259

Chapter 1

Get To Know Your Router

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

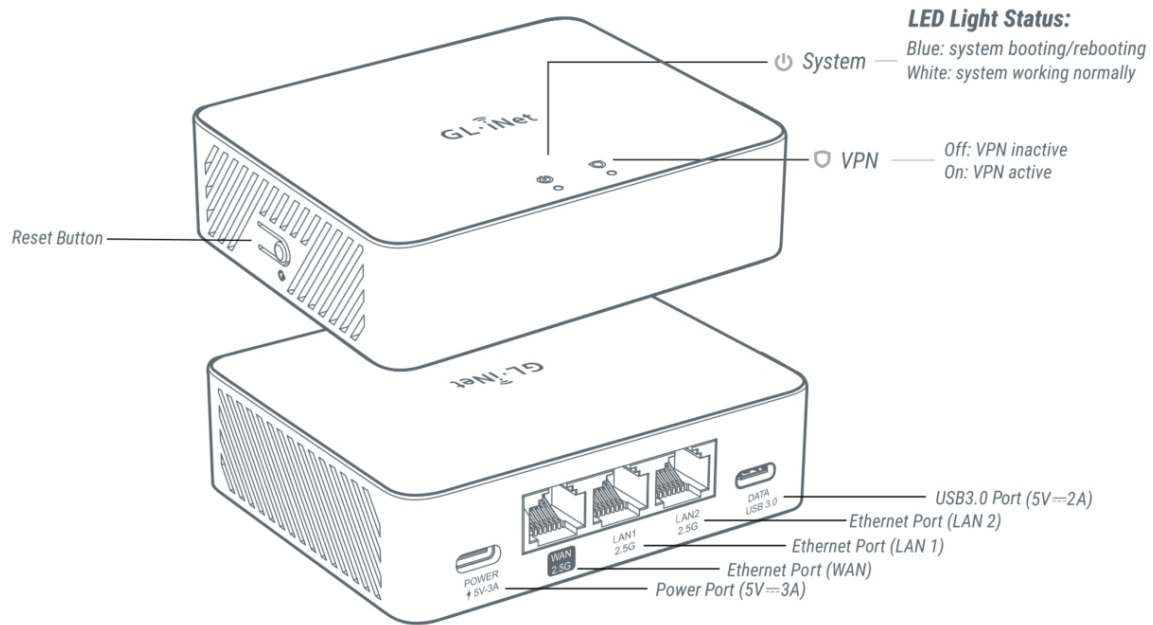
1.1 Product Overview

Brume 3 (GL-MT5000) is a high-performance security gateway, equipped with a MediaTek Quad-core CPU, 1GB RAM, and 8GB eMMC storage. It features a compact design, ideal for space-constrained deployments, and supports home VPN hosting as well as over 30 VPN services. What's more, it comes with GL.iNet's DPI feature, Parental Control and AdGuard Home, meeting the diverse needs of tech enthusiasts and business users.

1.1.1 Appearance



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.
2.5G 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 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 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, Quad-core @2.0GHz
Memory / Storage	DDR4 1GB / eMMC 8GB
Ethernet Speed	10/100/1000/2500Mbps
Power Input	Type-C, 5V/3A
Power Consumption	< 5W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	75 x 92 x 25mm / 148g
Other Tools	Datesheet / Firmware / App / Unboxing / Tutorials

1.3 Package Contents

The package includes:

- 1 x Brume 3 (GL-MT5000)
- 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 heat:** 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 3 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 3'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

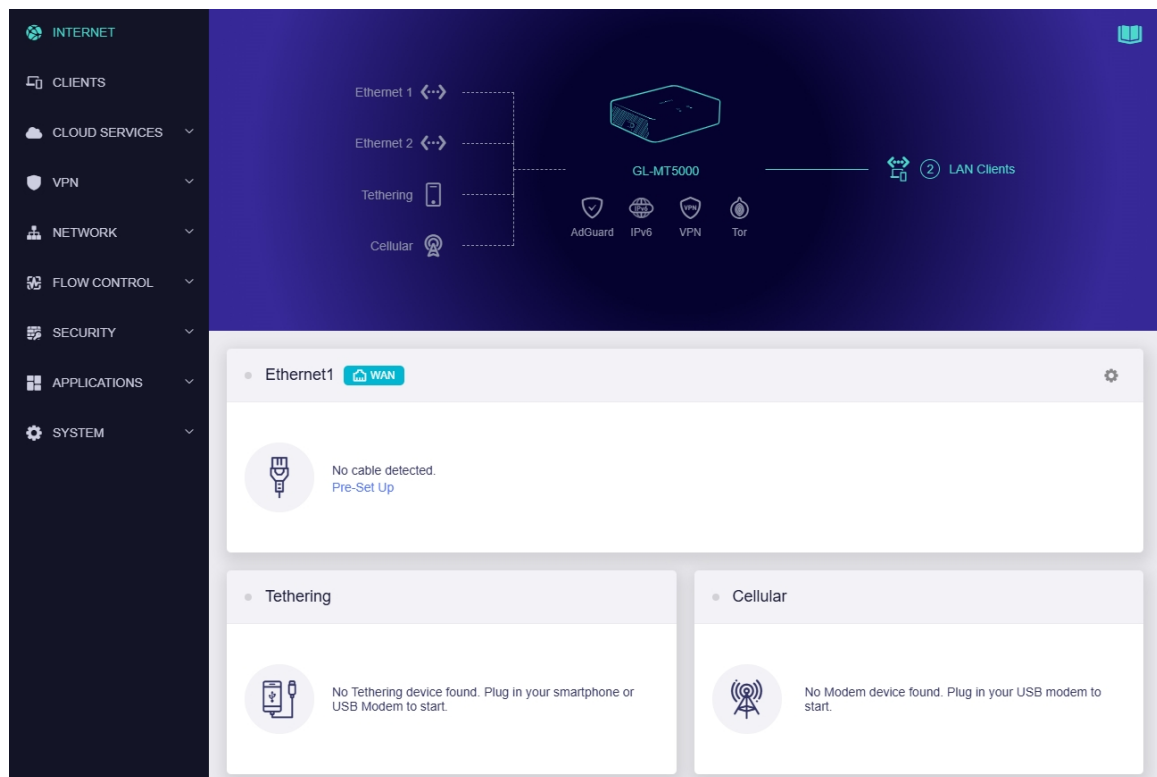
Log In To Your Router

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 3'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 3'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

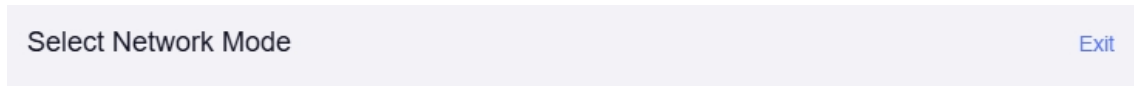
The Web-based Setup Wizard will guide you through the router network configuration.

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.



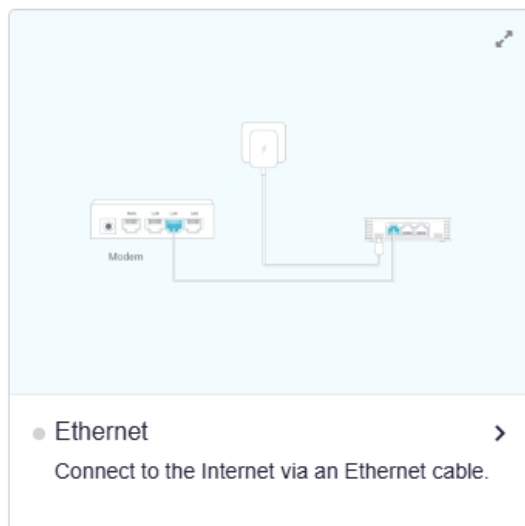
3. Follow the Setup Wizard to configure your router and establish an internet connection.



Network Guide

The Network Guide helps you configure your router network for fast Internet access in no time.

Suggest



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 3 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.

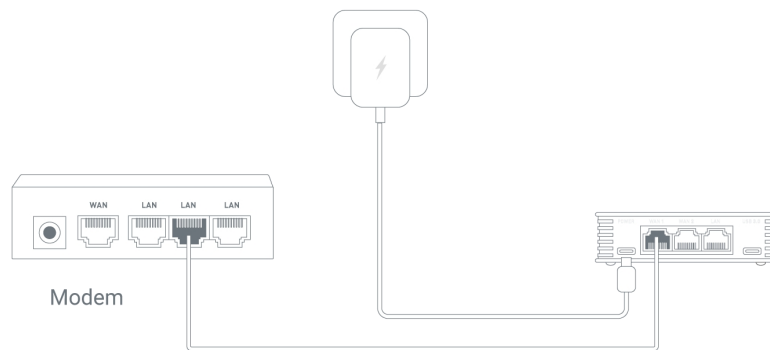
4.2.1 Connect to the Internet via Ethernet Cable

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.

Ethernet 1

WAN

Protocol	DHCP
IP Address	192.168.11.163
Gateway	192.168.11.1
DNS Server	192.168.11.1

Modify

Protocol

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

Ethernet 1 WAN ⚙️

Protocol	DHCP
IP Address	192.168.11.163
Gateway	192.168.11.1
DNS Server	192.168.11.1

Modify

- **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.

Ethernet Settings

Protocol DHCP Static PPPoE

ℹ️ IP address is assigned by higher network machine.

IPv4

IP Address	192.168.116.215
Netmask	255.255.255.0
Gateway	192.168.116.254
DNS Server 1	223.5.5.5
DNS Server 2	223.6.6.6

Cancel Apply

- **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).

Ethernet Settings

Protocol

DHCP
Static
PPPoE

IPv4

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2

VLAN ID ⓘ

Cancel
Apply

- **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.

Ethernet Settings

Protocol

DHCP
Static
PPPoE

PPPoE Setting

Username

Password
 ⓘ

VLAN ID ⓘ

TTL ⓘ

HL ⓘ

MTU ⓘ

Cancel
Apply

Advanced Settings

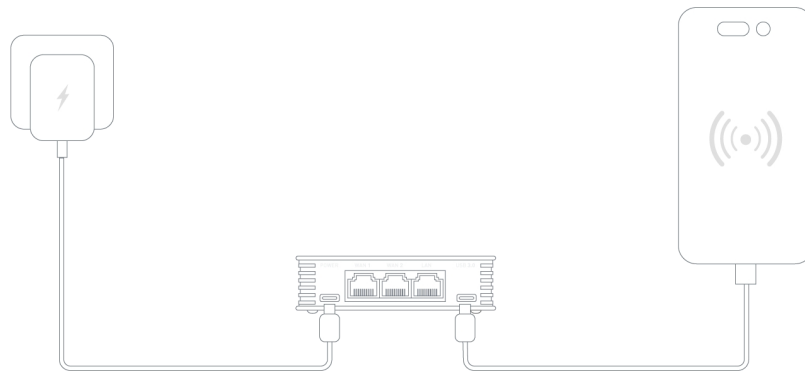
In addition to the essential settings, there are also some optional advanced settings for the above three protocols.

The screenshot shows the 'Ethernet Settings' window. Under the 'IPv4' tab, the following fields are visible: IP Address (192.168.116.221), Netmask (255.255.255.0), Gateway (192.168.116.254), DNS Server 1 (223.5.5.5), and DNS Server 2 (223.6.6.6). Below these, a red box highlights the 'Advanced Settings' section, which includes: VLAN ID (Optional (1 ~ 4094)), TTL (Optional), HL (Optional), and MTU (1500). At the bottom of the window are 'Cancel' and 'Apply' buttons.

- **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.

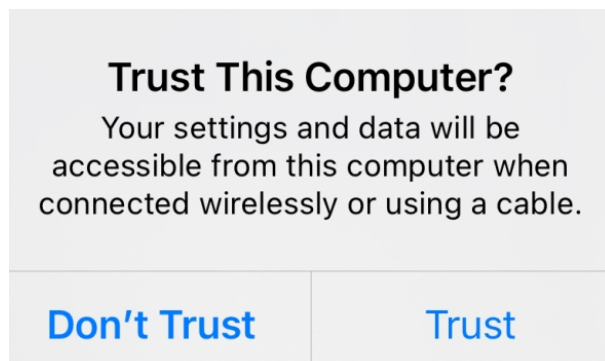


Host-less modem works in Tethering as well during the setup of the modem.

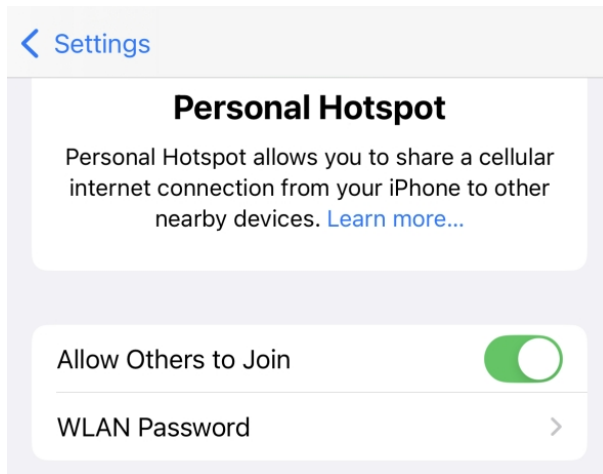
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

iPhone Tethering

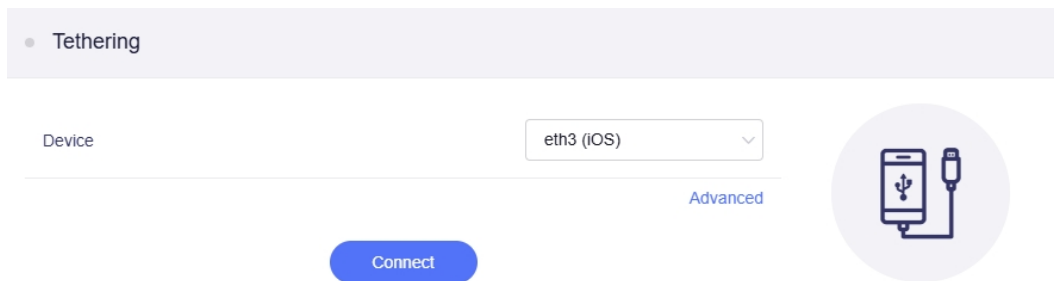
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



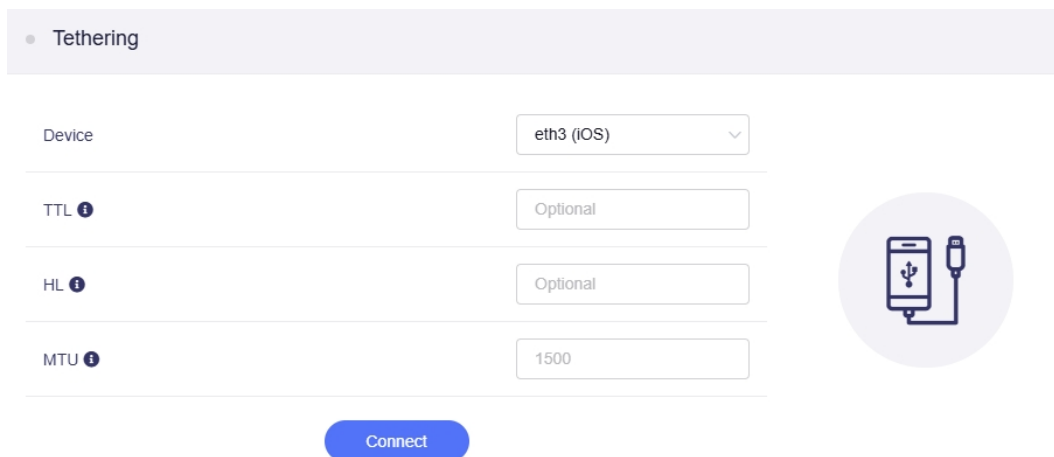
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



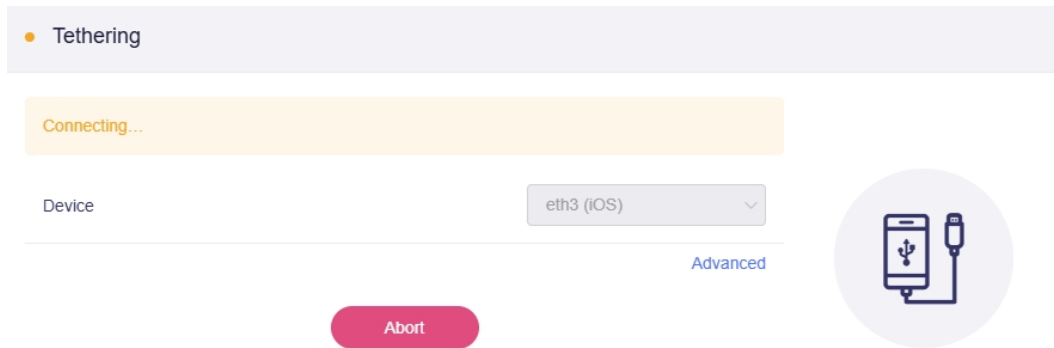
3. Connect a computer or another phone to the router. Log in to the router's web admin panel and navigate to **INTERNET > Tethering**, then click **Connect**.



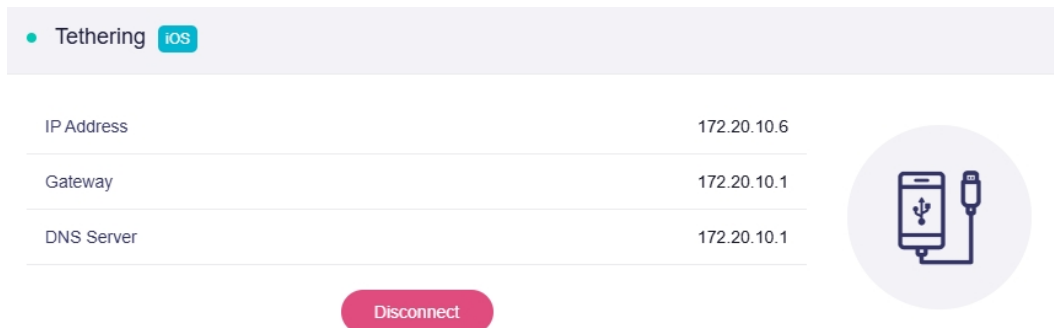
If you need to set advanced settings, such as TTL, HL, and MTU, click **Advanced** to customize these settings before clicking **Connect**.



4. It will start connecting.

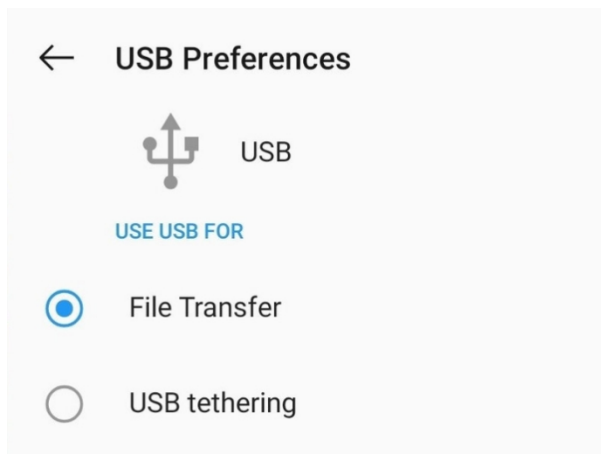


Once connected, this page will display the Tethering connection details.

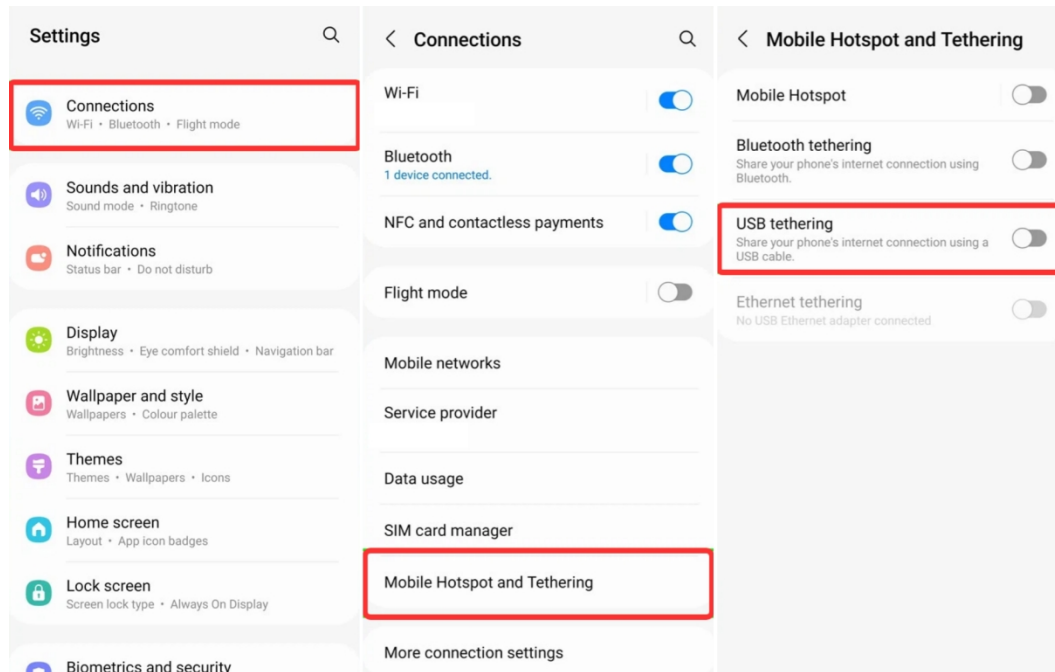


Android Tethering

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.

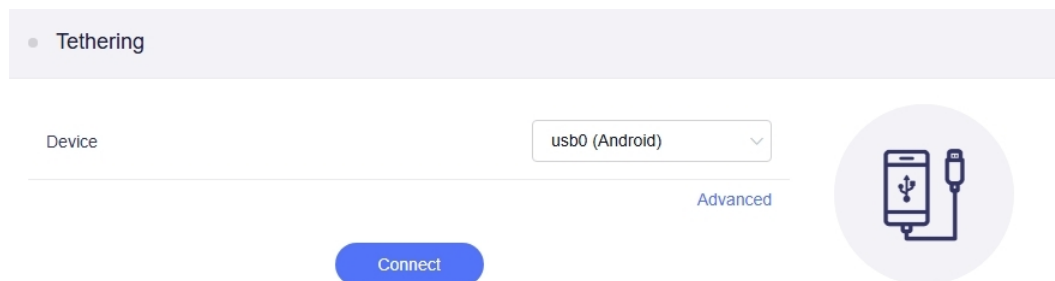


2. Go to your phone's **Settings > Network & Internet > Personal Hotspot**. Enable **Personal Hotspot** or **USB Tethering**.



(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**.

Tethering

Device

usb0 (Android)

TTL ⓘ

Optional

HL ⓘ

Optional

MTU ⓘ

1500

Connect



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

Tethering **Android**

IP Address

192.168.11.9

Gateway

192.168.11.1

DNS Server

192.168.11.1

Disconnect



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.

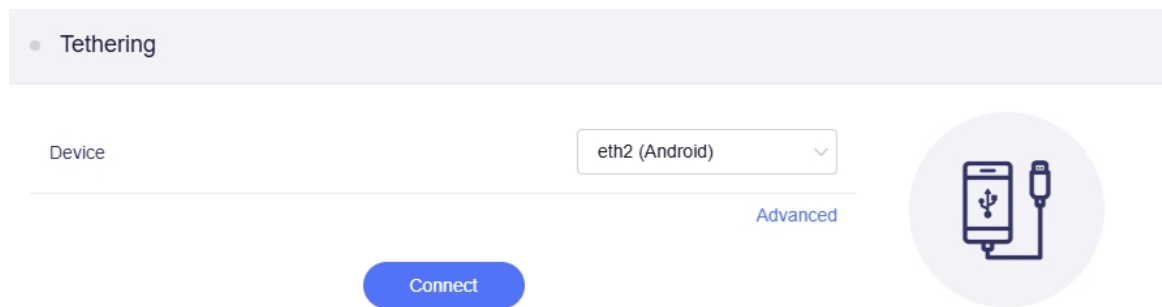
4.2.3 Connect to the Internet via USB Modem

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.

For Brume 3, an additional **USB-C to USB-A adapter** is required to connect a USB modem.

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**.



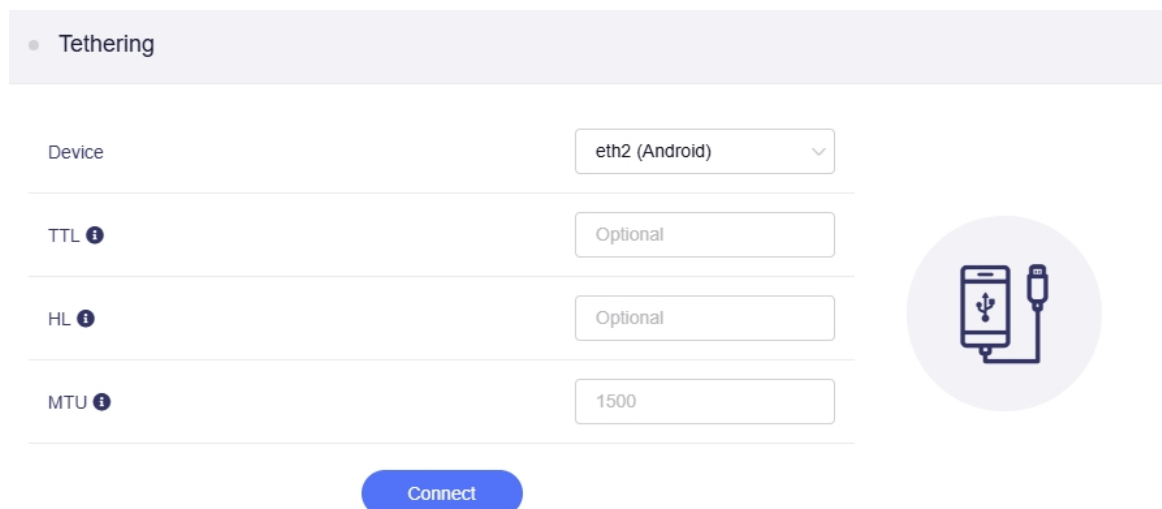
• Tethering

Device eth2 (Android) ▾

[Advanced](#)

Connect

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



• Tethering

Device eth2 (Android) ▾

TTL ⓘ Optional

HL ⓘ Optional

MTU ⓘ 1500

Connect

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

Tethering
Android

IP Address	192.168.1.100
Gateway	192.168.1.1
DNS Server	192.168.1.1, 192.168.1.1



Disconnect

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.

Tethering



Connecting...

No Tethering device found. Plug in your smartphone or USB Modem to start.

Abort

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.

Clients Access Control: [Blocklist](#) 

Sort by Default 

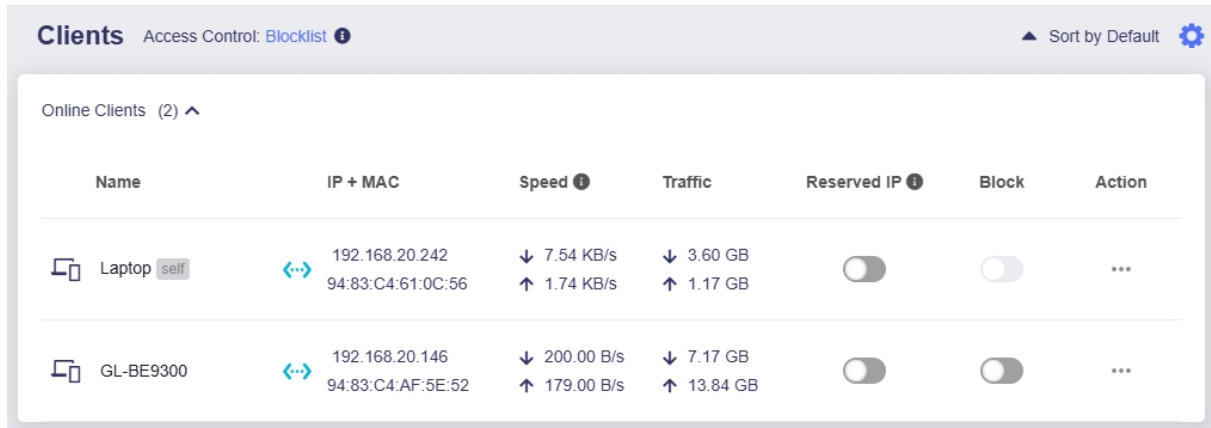
Online Clients (2) 

Name	IP + MAC	Speed 	Traffic	Reserved IP 	Block	Action
 Laptop self	 192.168.20.242 94:83:C4:61:0C:56	↓ 58.54 KB/s ↑ 2.52 KB/s	↓ 3.40 GB ↑ 1.14 GB	☐	☐	...
 GL-BE9300	 192.168.20.146 94:83:C4:AF:5E:52	↓ 103.00 B/s ↑ 111.00 B/s	↓ 6.88 GB ↑ 12.99 GB	☐	☐	...

Offline Clients (1) 

Name	IP + MAC	Speed	Traffic	Reserved IP 	Block	Action
 GL-E5800	 192.168.20.110 00:E0:4C:36:1B:41	↓ 0.00 B/s ↑ 0.00 B/s	↓ 2.52 KB ↑ 3.39 KB	☐	☐	...

5.1 Device Details



Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
 Laptop self	 192.168.20.242 94:83:C4:61:0C:56	↓ 7.54 KB/s ↑ 1.74 KB/s	↓ 3.60 GB ↑ 1.17 GB	☐	☐	...
 GL-BE9300	 192.168.20.146 94:83:C4:AF:5E:52	↓ 200.00 B/s ↑ 179.00 B/s	↓ 7.17 GB ↑ 13.84 GB	☐	☐	...

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. Reserve IP

In the fifth column, you can reserve IP address for connected device with one click. When you specify a reserved IP address for a client within the local area network, it will always receive the same IP address each time it connects to the router.

6. Blocklist

In the sixth column, you can block specific connected devices with one click.

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

Clients Access Control: **Blocklist** Sort by Default ⚙️

Online Clients (2) ^

Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
Laptop Self	↔️ 192.168.20.242 94:83:C4:61:0C:56	↓ 6.70 KB/s ↑ 2.09 KB/s	↓ 3.37 GB ↑ 1.14 GB	☐	☐	...
GL-BE9300	↔️ 192.168.20.146 94:83:C4:AF:5E:52	↓ 109.00 B/s ↑ 112.00 B/s	↓ 6.88 GB ↑ 12.99 GB	☐	☐	...

Access Control

Mode Blocklist ^

Blocklist

Self MAC

1 e.g. 11:22:33:44:55:66

- **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.

Clients Access Control: [Blocklist](#)  Sort by Default 

Online Clients (2) 

Name	IP + MAC	Speed 	Traffic	Reserved IP 	Block	Action
 Laptop self	 192.168.20.242 94:83:C4:61:0C:56	↓ 52.29 KB/s ↑ 5.27 KB/s	↓ 3.42 GB ↑ 1.14 GB	☐	☐	...
 GL-BE9300	 192.168.20.146 94:83:C4:AF:5E:52	↓ 144.96 KB/s ↑ 101.17 KB/s	↓ 7.00 GB ↑ 13.03 GB	☐	☐	 View Details  Modify  Limit Speed

Clients / **Client Details**

 Laptop self

Hostname	GL-AXT1800
Connection Method	 Ethernet
MAC	94:83:C4:61:0C:56
Speed 	↓ 5.58 KB/s ↑ 1.24 KB/s
Traffic	↓ 3.42 GB ↑ 1.14 GB
Reserved IP 	OFF
Block	OFF
IP Address	192.168.20.242

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.

The screenshot displays the 'Clients' management interface. At the top, there's a header with 'Clients', 'Access Control: Blocklist', and a 'Sort by Default' button. Below this, a section titled 'Online Clients (2)' contains a table with the following columns: Name, IP + MAC, Speed, Traffic, Reserved IP, Block, and Action.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
Laptop self	192.168.20.242 94:83:C4:61:0C:56	↓ 5.48 KB/s ↑ 1.14 KB/s	↓ 3.42 GB ↑ 1.14 GB	☐	☐	⋮
GL-BE9300	192.168.20.146 94:83:C4:AF:5E:52	↓ 17.39 KB/s ↑ 13.84 KB/s	↓ 7.03 GB ↑ 13.07 GB	☐	☐	⋮

A dropdown menu is open for the 'GL-BE9300' client, showing options: 'View Details', 'Modify' (highlighted with a red box), and 'Limit Speed'.

Below the table, a 'Modify Client Device' dialog box is shown. It has two input fields: 'Name' (containing 'Auto') and 'Device Type' (containing 'Optional'). A dropdown menu for 'Device Type' is open, listing options: Desktop, Phone, Tablet PC, Camera, Wearable device, Laptop, and Printer. At the bottom of the dialog, there are 'Cancel' and 'OK' buttons.

3. Limit Speed

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

The screenshot shows the 'Clients' interface with 'Access Control: Blocklist'. It lists two online clients: 'Laptop' and 'GL-BE9300'. For each client, it shows IP + MAC, Speed (download and upload), Traffic (download and upload), Reserved IP, and Block status. The 'Action' column for 'GL-BE9300' is open, showing options: 'View Details', 'Modify', and 'Limit Speed' (highlighted with a red box).

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
Laptop	192.168.20.242 94:83:C4:61:0C:56	↓ 80.17 KB/s ↑ 2.72 KB/s	↓ 3.44 GB ↑ 1.15 GB	☐	☐	...
GL-BE9300	192.168.20.146 94:83:C4:AF:5E:52	↓ 5.05 KB/s ↑ 12.38 KB/s	↓ 7.03 GB ↑ 13.10 GB	☐	☐	View Details Modify Limit Speed

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

The 'Limit Speed Settings' dialog shows input fields for 'Download' and 'Upload' speeds, both currently set to 'Unlimited' KB/s. At the bottom are 'Cancel' and 'Apply' buttons.

↓ Download KB/s

↑ Upload KB/s

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

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
Laptop	192.168.20.242 94:83:C4:61:0C:56	↓ 8.73 KB/s ↑ 3.92 KB/s	↓ 3.44 GB ↑ 1.15 GB	☐	☐	...
GL-BE9300	192.168.20.146 94:83:C4:AF:5E:52	↓ 5.04 KB/s ↑ 20.27 KB/s	↓ 7.03 GB ↑ 13.10 GB	☐	☐	...

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.

Offline Clients (3) ^

[Delete All](#)

Name	IP + MAC	Speed	Traffic	Reserved IP ⓘ	Block	Action
 GL-BE9300	 192.168.20.146 94:83:C4:AF:5E:52	↓ 0.00 B/s ↑ 0.00 B/s	↓ 7.09 GB ↑ 13.18 GB	☐	☐	...
 GL-E5800	 192.168.20.110 00:E0:4C:36:1B:41	↓ 0.00 B/s ↑ 0.00 B/s	↓ 2.52 KB ↑ 3.39 KB	☐	☐	...
 glkvm	 192.168.20.209 94:83:C4:BB:A4:FF	↓ 0.00 B/s ↑ 0.00 B/s	↓ 5.49 KB ↑ 6.40 KB	☐	☐	...

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.

Offline Clients (3) ^

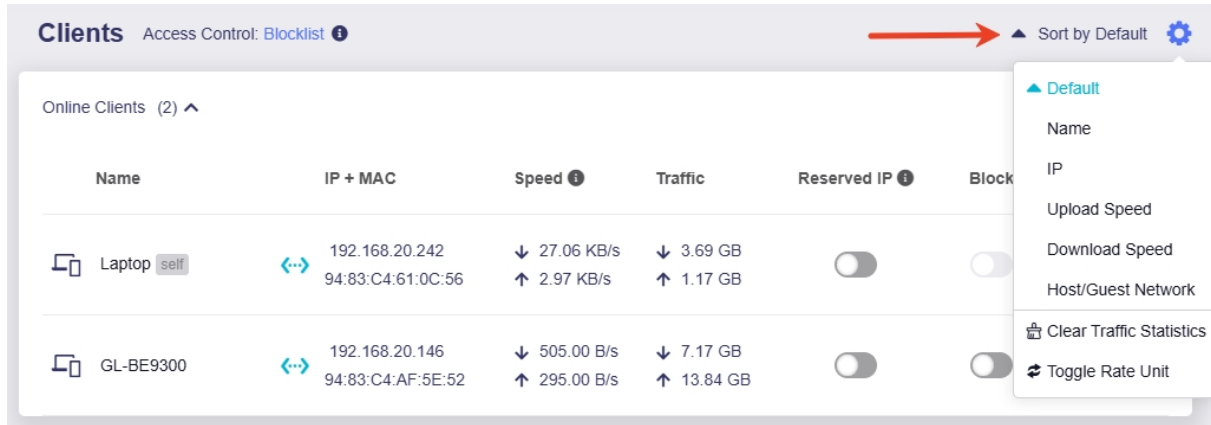
[Delete All](#)

Name	IP + MAC	Speed	Traffic	Reserved IP ⓘ	Block	Action
 GL-BE9300	 192.168.20.146 94:83:C4:AF:5E:52	↓ 0.00 B/s ↑ 0.00 B/s	↓ 7.09 GB ↑ 13.18 GB	☐	☐	...
 GL-E5800	 192.168.20.110 00:E0:4C:36:1B:41	↓ 0.00 B/s ↑ 0.00 B/s	↓ 2.52 KB ↑ 3.39 KB	☐	☐	...
 glkvm	 192.168.20.209 94:83:C4:BB:A4:FF	↓ 0.00 B/s ↑ 0.00 B/s	↓ 5.49 KB ↑ 6.40 KB	☐	☐	...

[View Details](#)
[Modify](#)
[Limit Speed](#)
[Remove Client](#)

5.4 Sort

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



The screenshot shows the 'Clients' page with a header bar containing 'Clients' and 'Access Control: Blocklist'. A red arrow points to the 'Sort by Default' button in the top right corner. Below the header, there is a section for 'Online Clients (2)' with a table listing two devices. A dropdown menu is open, showing sorting options: Default, Name, IP, Upload Speed, Download Speed, Host/Guest Network, Clear Traffic Statistics, and Toggle Rate Unit.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block
Laptop self	192.168.20.242 94:83:C4:61:0C:56	↓ 27.06 KB/s ↑ 2.97 KB/s	↓ 3.69 GB ↑ 1.17 GB	☐	☐
GL-BE9300	192.168.20.146 94:83:C4:AF:5E:52	↓ 505.00 B/s ↑ 295.00 B/s	↓ 7.17 GB ↑ 13.84 GB	☐	☐

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.

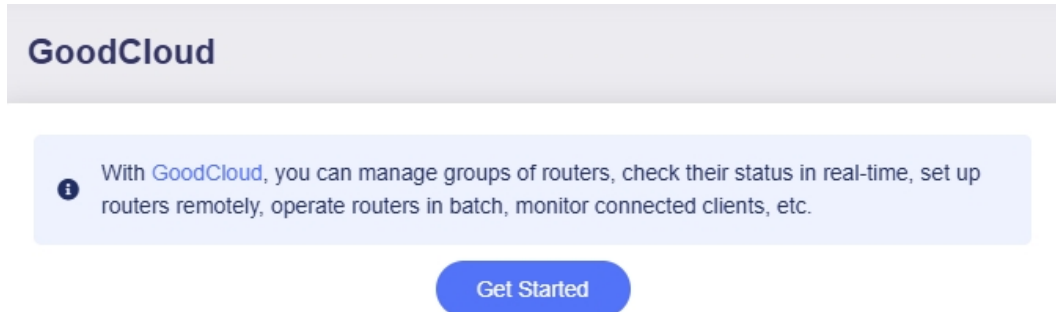
With GoodCloud, you can:

- 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

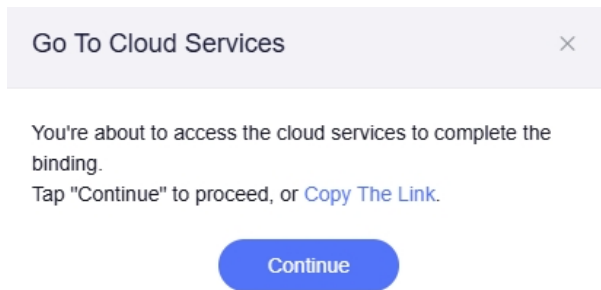
Some features are available in Enterprise Plan and VAR (Value Added Reseller) Plan. See [here](#) for details.

6.1.1 Enable GoodCloud

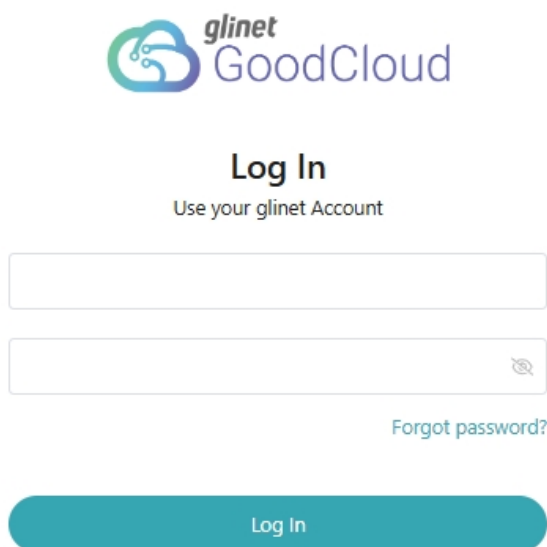
1. Log in to your router's web admin panel, navigate to **CLOUD SERVICE > GoodCloud**, and click **Get Started**.



2. In the pop-up window, click **Continue**.



3. You will be redirected to the GoodCloud login page. Log in with your GL.iNet account. If you don't have an account, click **Sign Up** to register and log in. Once logged in, confirm the device info and bind it to your account.

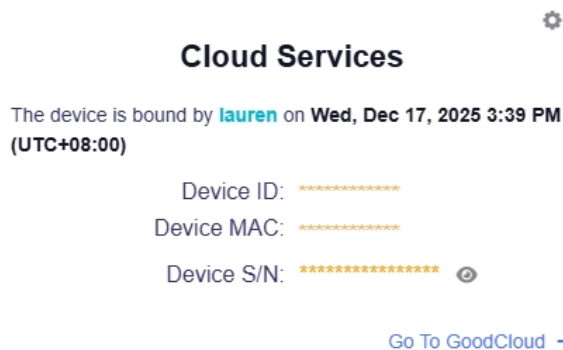


Tips:

- 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.



Cloud Services

The device is bound by **lauren** on **Wed, Dec 17, 2025 3:39 PM (UTC+08:00)**

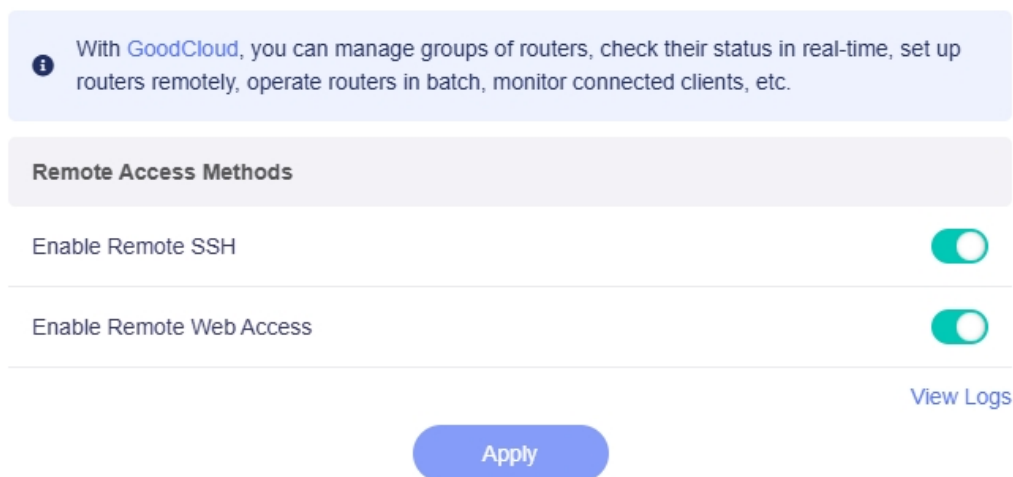
Device ID: *****

Device MAC: *****

Device S/N: *****

[Go To GoodCloud](#) →

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.



With GoodCloud, you can manage groups of routers, check their status in real-time, set up routers remotely, operate routers in batch, monitor connected clients, etc.

Remote Access Methods

Enable Remote SSH ☒

Enable Remote Web Access ☒

[View Logs](#)

Apply

- **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.

Q

Name / MAC / IP / SN / IMEI

Filter

☐	Name	Status	Model	Version	MAC	IP
☐	MT5000-Laure...	Online	MT5000	4.8.4	94:83:C4:C5:BA:FD	113.116.58.214

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.

MT5000-Lauren-ow5bafd

Remote GUI

Remote SSH

Reboot Device

Basic Info

Update Time: 01-14 09:53:52

Status

Online

Type

Router

Model

MT5000

Firmware

4.8.4

MAC Address

IP Address

113.116.58.214

SN

8731*****4905

Compile Time

2025-12-24 12:21:34

Statistical Data

Update Time: 01-14 09:54:06

Network Latency

Retest

232.03 ms

2.26 ms

0 %

Latency

Jitter

Packet Loss

Memory Usage

29%

Up Time

1

days

:

0

hrs

:

4

mins

OVERVIEW

TRAFFIC ANALYSIS

CLIENTS LIST

TIMELINE

SHARE

Ethernet1

Update Time: 01-14 09:52:55

Network Condition

Online

Status

Connected

Ethernet2

Update Time: 01-14 09:54:00

Network Condition

Offline

Status

Disconnected

Tethering

Update Time: 01-14 09:52:55

Status

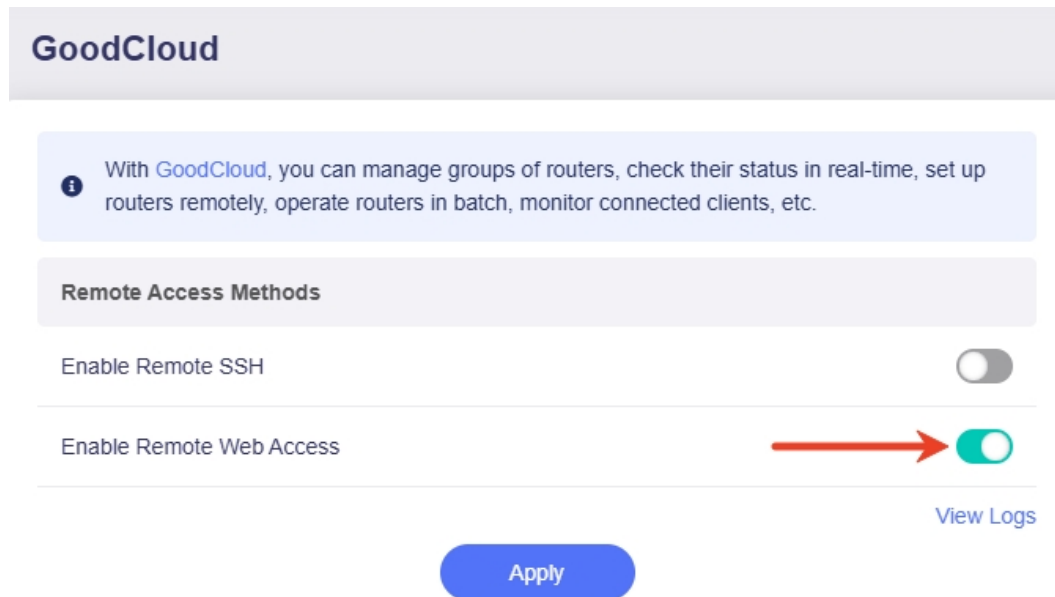
Disconnected

Device List

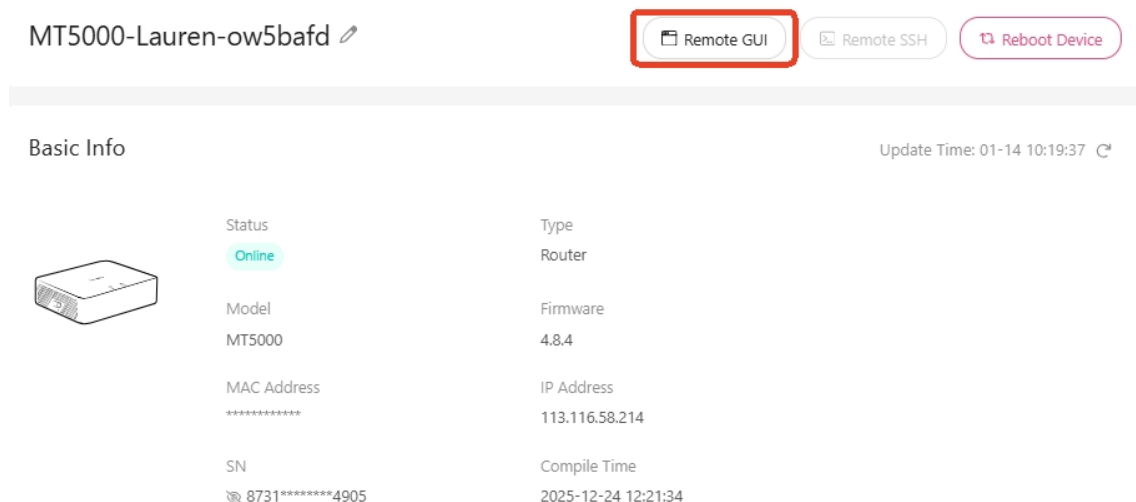
Details

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**.

Remote GUI

☒ HTTP ☐ HTTPS

* Port

80

Cancel

Apply

Remote GUI

☐ HTTP ☒ HTTPS

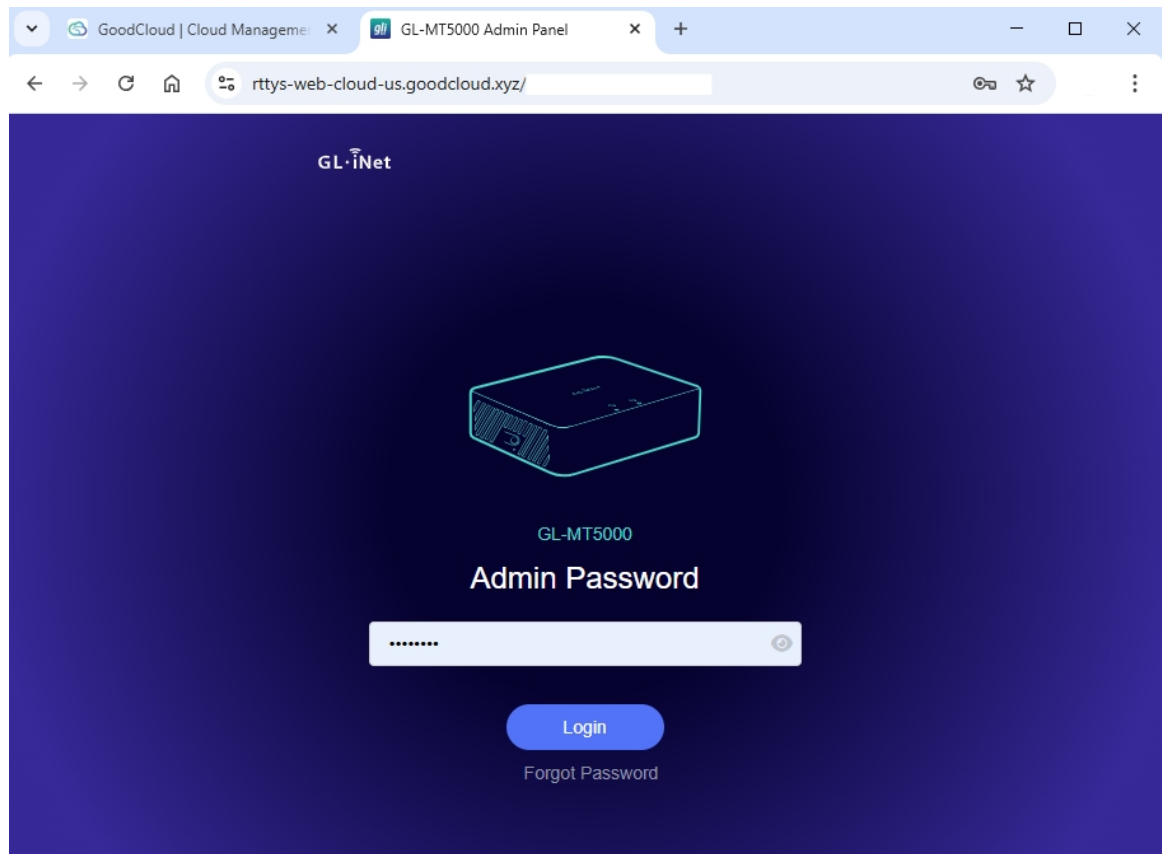
* Port

443

Cancel

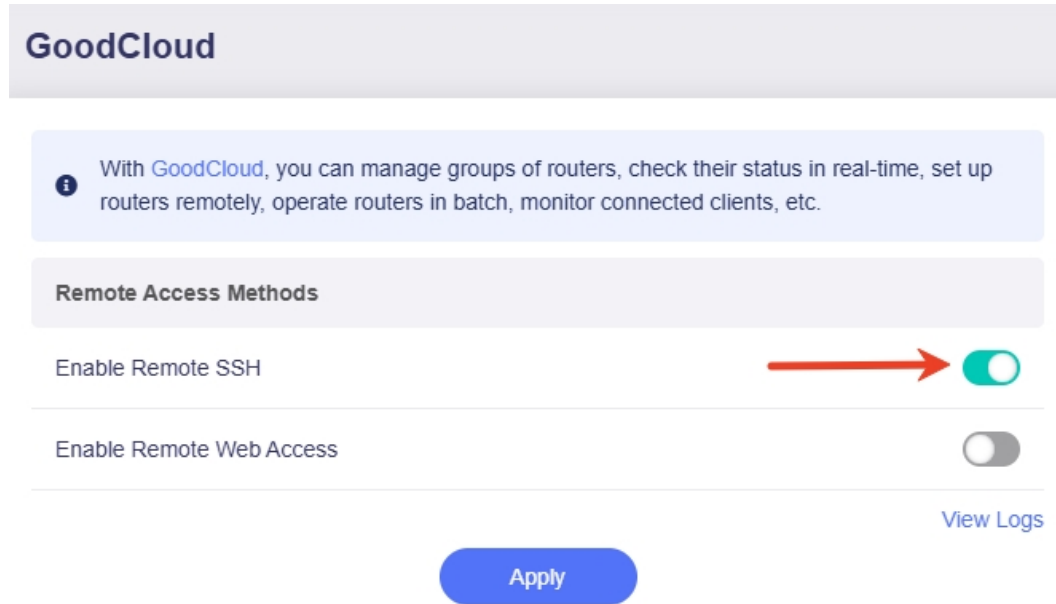
Apply

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.

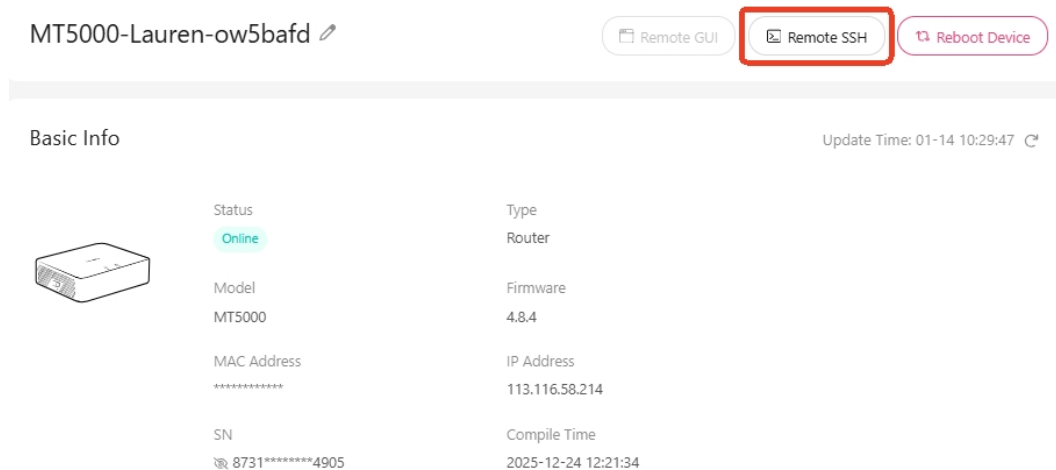


Remote Access Terminal

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-MT5000 login: root
Password:
```

```
BusyBox v1.33.2 (2025-12-24 12:15:29 UTC) built-in shell (ash)
```

```

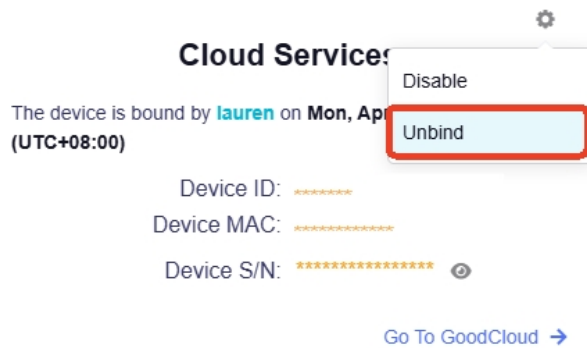
|_| .----- .----- .----- | | | | .----- |_|
|_| - || - | - | || | | | || - || - |
|_| W I R E L E S S F R E E D O M
-----
```

```
OpenWrt 21.02-SNAPSHOT,
-----
```

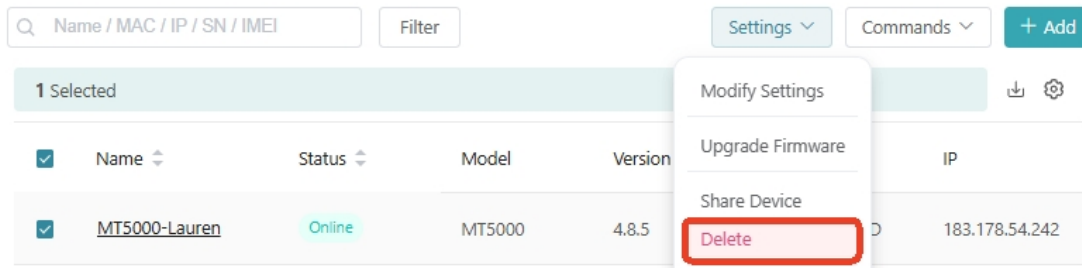
```
root@GL-MT5000:~# |
```

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.

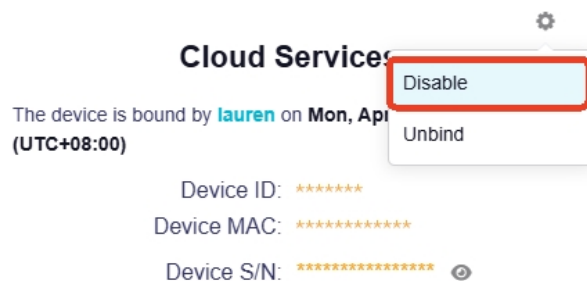


Alternatively, log in to the Cloud platform and navigate to **Device > Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



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 feature designed for GL.iNet routers to provide seamless remote networking and device management. Integrated into the GL.iNet router SDK, it adopts the AmneziaWG protocol with built-in traffic obfuscation, delivering stable and secure connections for reliable remote access anytime, anywhere.

This feature enables seamless remote access to your home network. You can directly set up and pair devices via a dynamic access code in the web Admin Panel, quickly establishing a secure connection between your travel router and home network in just seconds, with no registration or login required.

Note:

1. It is not recommended to use AstroWarp with any of the following features at the same time, as this may cause routing conflicts: GoodCloud Site to Site, ZeroTier, Tailscale, Tor.
2. When AstroWarp is enabled, the Network Mode cannot be used.

6.2.1 Quick Setup

In the following example, two routers will be used to set up an AstroWarp network: Brume 3 will act as the home router, while a GL.iNet travel router will route network traffic back to Brume 3 for Internet access. We suggest setting up the AstroWarp network before departure.

Tip: Each GL.iNet router comes with **10 GB free data per month** for AstroWarp networking. Devices in an AstroWarp network will use the home router's data to access the Internet. You can upgrade to the AstroWarp+ plan for unlimited data if needed.

1. Configure Brume 3 for Internet.
Log in to the Brume 3's web admin panel and navigate to the INTERNET page. Connect it to the Internet using one of the supported internet connection methods: Ethernet, Tethering, and Cellular.
2. In the Brume 3's web admin panel, navigate to **CLOUD SERVICES > AstroWarp**. Click **Use At Home**.



Welcome to AstroWarp!

Bring your home network with you.

AstroWarp utilizes the AmneziaWG protocol with built-in traffic obfuscation to ensure your connection stays steady and undetected. By securely extending your home network globally, you can browse using your home IP with total privacy—as seamlessly as if you were at home.

Select the usage for this router

 Use At Home → Use this router as a fixed home router to access the home network for other devices to connect.	 Use While Traveling → Use this router to connect to your home network remotely when away from home.
---	---

It will generate an **Access Code**. Copy this code for later use.

 Usage of This Router: **Use At Home** Reset

Generate Access Code

M B E A 4 W B X
[Copy](#)

This access code will expire in **09:57**.

Please enter this access code in the **Travel Router**.

After verification, your devices will be able to access the internet through your home network.

3. Configure the travel router for Internet.
Log in to the travel router's web admin panel, and navigate to the INTERNET page. Connect it to the Internet using one of the supported internet connection methods: Ethernet, Repeater, Tethering, and Cellular.
4. Enter Access Code.
In the travel router's web admin panel, navigate to **CLOUD SERVICES > AstroWarp**. Click **Use While Traveling**.



Welcome to AstroWarp!

Bring your home network with you.

AstroWarp utilizes the AmneziaWG protocol with built-in traffic obfuscation to ensure your connection stays steady and undetected. By securely extending your home network globally, you can browse using your home IP with total privacy—as seamlessly as if you were at home.

Select the usage for this router

 **Use At Home** →
Use this router as a fixed home router to access the home network for other devices to connect.

 **Use While Traveling** →
Use this router to connect to your home network remotely when away from home.

Enter the Access Code obtained in Step 2, and wait for the verification to complete.

Usage of This Router: **Use While Traveling** Reset

Enter Access Code

Please enter the access code generated by your home router.
After verification, this router and the devices connected to it will be able to access the internet through your home network.

M B E A 4 W B X

Verifying, please wait a moment...

It will then connect to the Brume 3 successfully. Now you can browse the Internet through your home network securely.

Usage of This Router: **Use While Traveling** Reset

✓ Successfully Connected! You are now browsing the internet through your home network.


Tap to disconnect

Current Session
3 Minutes

5. In the Brume 3's web admin panel, it also displays the connection status as follows.

Usage of This Router: **Use At Home**

Reset

Upgrade Plan

✓ You have successfully established a connection.



Tap to disable connection

Connected/Authorized

1 / 1

Monthly Free Data Usage

0 / 10 GB

Connection Management (1)

Add Device

Device Name	Status	Activity	Action
 BE3600	Connected	Connected for: 2 Minutes	...

6.2.2 Test Connectivity

1. Connect a laptop or smartphone to the travel router's Wi-Fi.
2. Open a browser and visit ipcheck.ing or any other IP address lookup website. It will show the public IP address of Brume 3, indicating that the travel router is accessing the Internet through the Brume 3.

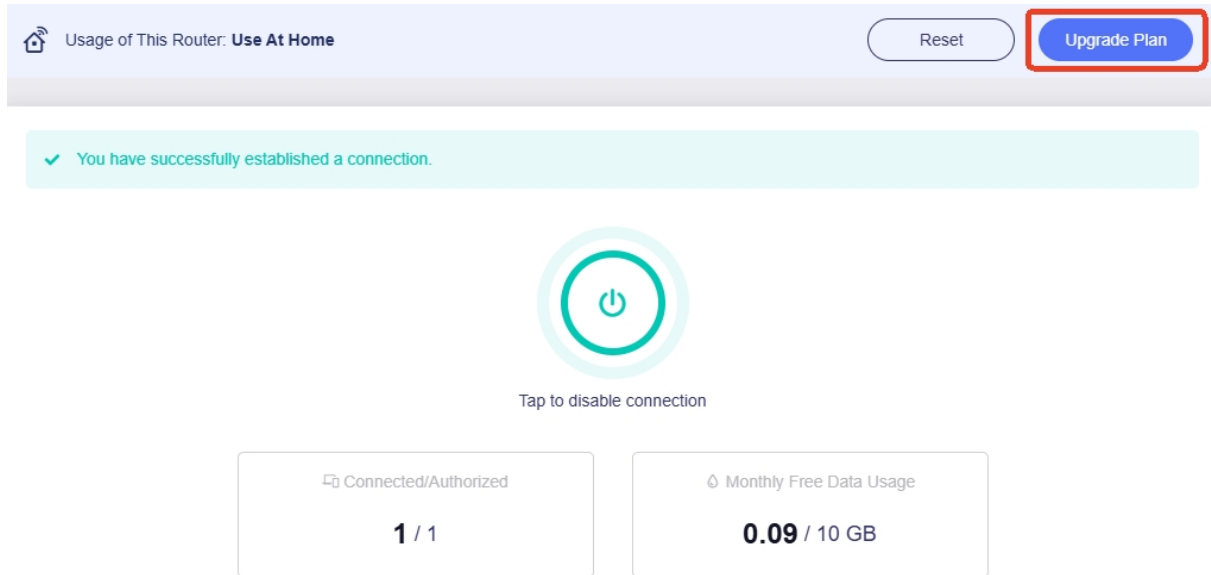


3. Disconnect the AstroWarp connection on the travel router, then refresh the webpage to resubmit the IP query request. It will show the travel router's local public IP address, indicating that it is accessing the Internet through its local network.



6.2.3 Upgrade Plan

Each GL.iNet router comes with **10 GB free data per month** for AstroWarp networking. Devices in an AstroWarp network will use the home router's data to access the Internet. You can upgrade to the **AstroWarp+** plan for unlimited data if needed.



Click [here](#) to view more details and FAQs about AstroWarp.

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

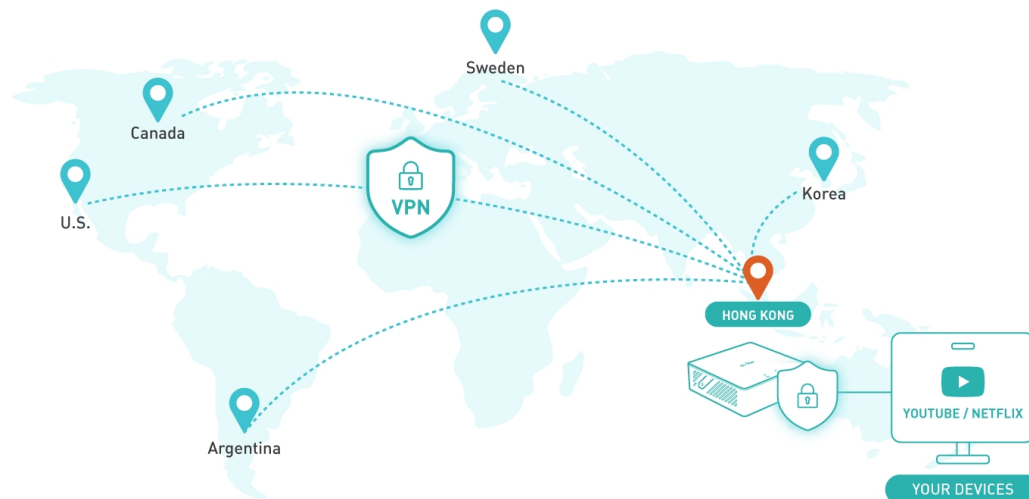
1. Personal Data Privacy

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.



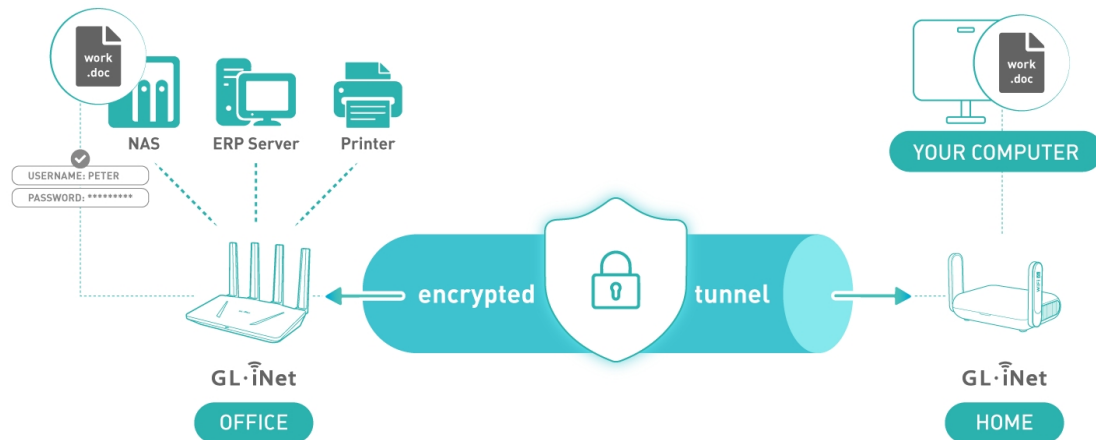
2. Unrestricted Access Worldwide

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.



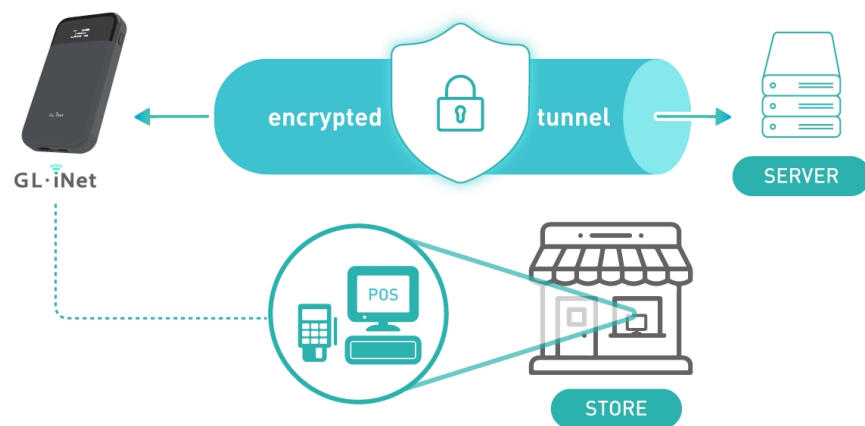
3. Small Business Data Security

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

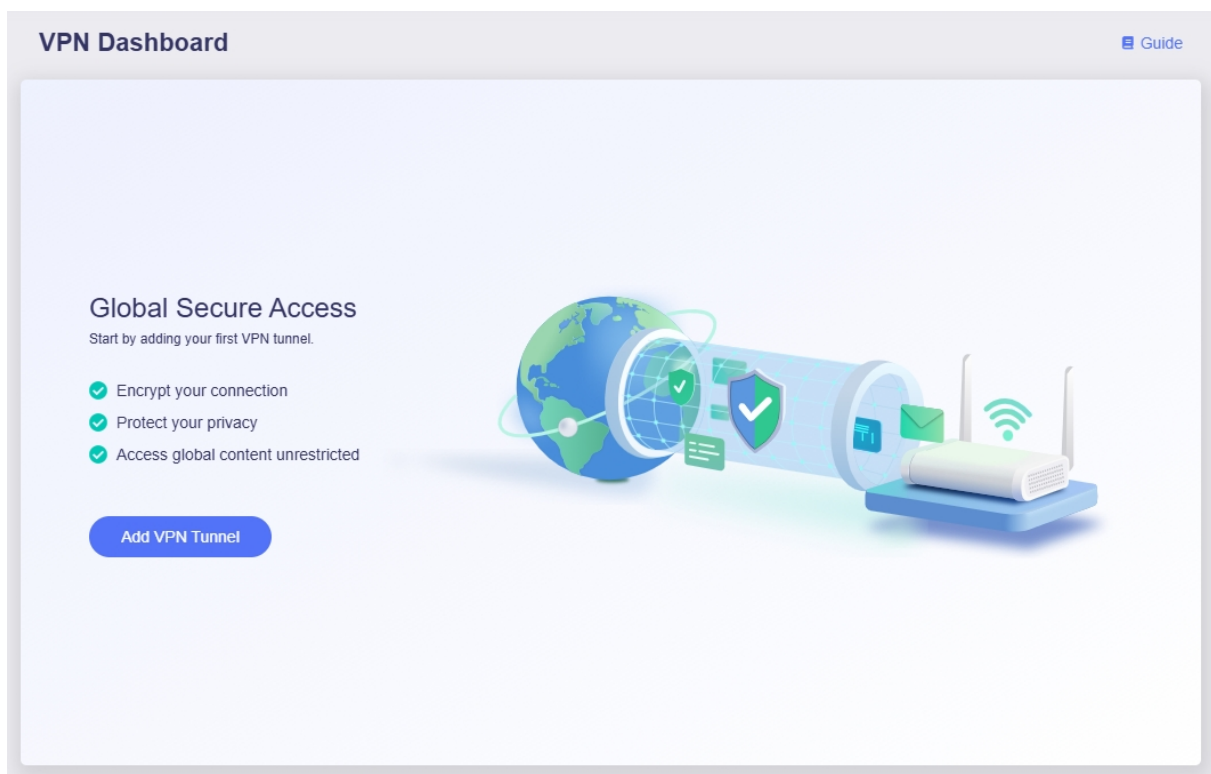
This chapter introduces how to manage VPN connections via the web admin panel.

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

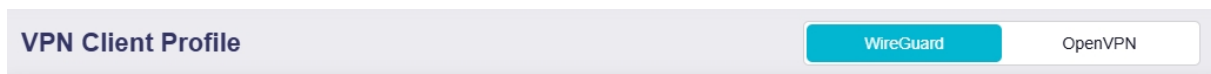
The VPN dashboard displays VPN connection details, such as routing rules, connected server, traffic statistics, client virtual IP, and connection log, and allows users to configure advanced settings such as the VPN Kill Switch, IP Masquerading, and MTU.

8.1 Upload VPN Profile

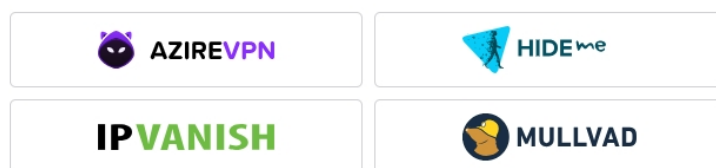
When entering this page for the first time, if no tunnels have been created, the page appears as follows. Click **Add VPN Tunnel** to get started.

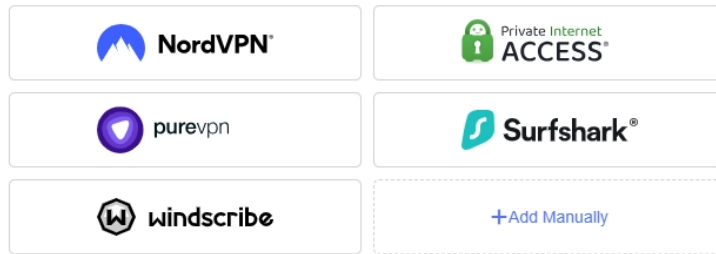


You will be directed to the **VPN Client Profile** page. Select a VPN provider and log in.



Request the VPN configuration file from your VPN service provider.





Please visit [VPN on Router](#) to view WireGuard compatible VPN service providers and learn about the benefits of using VPN. Follow your VPN service provider's guide, download the WireGuard configuration file, and import the configuration file to the router.

Tips:

1. The VPN providers listed are integrated into the GL.iNet router web Admin Panel. With an active subscription, users simply enter their credentials to log in instantly and obtain configuration files for VPN connections.
2. If you have subscribed to other VPN providers, or if you want to upload your personal VPN configurations, click **Add Manually** and upload your configurations.

Take [PureVPN](#) as an example. Click PureVPN and log in with valid credentials.

VPN Client Profile

WireGuardOpenVPN

Prefer using [other VPN service providers](#) or customizing your own VPN server ? Create a new group to add your configuration files.

PureVPN

+ Add Provider | Manual Group

purevpn

Username

Password

[Setup Guide](#)

Save and Continue

You will obtain a list of VPN profiles, as shown below. Click **Go to Dashboard** at the bottom, then you will be directed to the VPN Dashboard to set up your VPN tunnel and VPN policy.

VPN Client Profile

WireGuardOpenVPN

Prefer using [other VPN service providers](#) or customizing your own VPN server ? Create a new group to add your configuration files.

 **PureVPN** 93 

[+ Add Provider](#) | [Manual Group](#)

Update Servers

Name	Server Location	
● sx0112601-ikev.dnsdialer.com	United States	...
● sx0225252-ikev.dnsdialer.com	United Kingdom	...
● sx032111-ikev.dnsdialer.com	Canada	...
● sx041051-ikev.dnsdialer.com	Germany	...
● sx0517119-ikev.dnsdialer.com	Netherlands	...
● sx060289-ikev.dnsdialer.com	Sweden	...
● sx070682-ikev.dnsdialer.com	Romania	...
● sx080801-ikev.dnsdialer.com	Switzerland	...

 [Go to Dashboard](#)

You're signed in to PureVPN. Go to the VPN Dashboard to create and manage VPN tunnels.

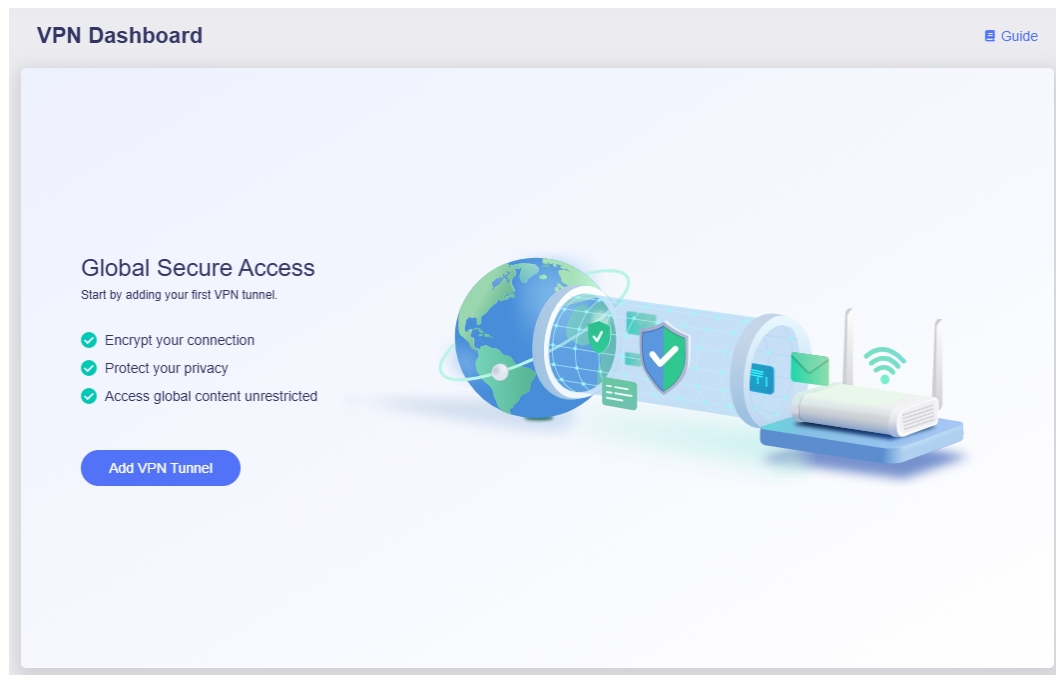
Tip: For some VPN service providers, you may need to select a VPN protocol or preferred servers/cities before the list of profiles appears.

8.2 Add VPN Tunnel

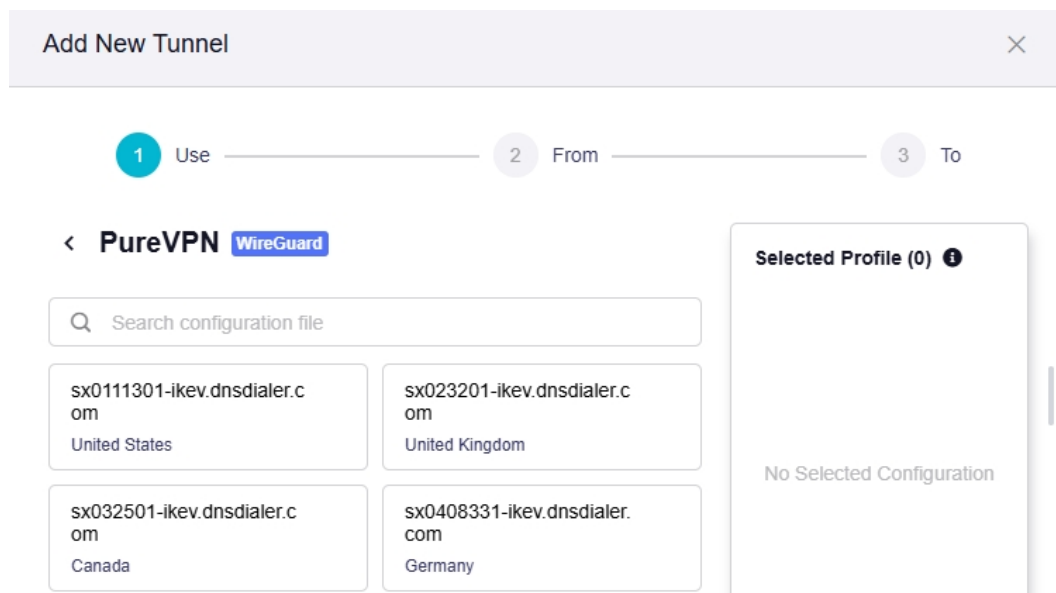
8.2.1 General Steps

Follow the steps below to add your VPN tunnel and configure VPN policies. See [Case Reference](#) if necessary.

1. On the VPN Dashboard, click **Add VPN Tunnel**. A setup wizard will appear on the right.



2. Select one or multiple profiles, and adjust their priority on the right if needed, then click **Next**.



sx0517119-ikev.dnsdialer.com Netherlands	sx060289-ikev.dnsdialer.com Sweden
sx070682-ikev.dnsdialer.com Romania	sx080619-ikev.dnsdialer.com Switzerland
sx090449-ikev.dnsdialer.com Panama	sx1000401-ikev.dnsdialer.com Cyprus

Note: When multiple profiles are selected, the tunnel will attempt to connect using each profile in priority order until a connection is successfully established. If all profiles within a single tunnel fail to connect, the system will determine whether to switch to the router's local network (WAN) based on the status of the Kill Switch in the [Tunnel Options](#) and [All Other Traffic](#) settings.

3. Select client source, then click **Next**. There are four options:
 - **All Clients:** If selected, traffic from all devices will match this rule.
 - **Specified Connection Types:** If selected, traffic from specified connection types (e.g., LAN subnet, Drop-in Gateway, Guest Network) will match this rule.
 - **Specified Devices:** If selected, traffic from specified devices (identified by MAC address) will match this rule.
 - **Exclude Specified Devices:** If selected, traffic from specified devices (identified by MAC address) will not match this rule.
4. Select target destination, then click **Apply**. There are three options:
 - **All Targets:** If selected, traffic matching this rule will be routed to all targets.
 - **Specified Domain / IP List:** If selected, traffic matching this rule will be routed to specified domains or IP addresses. You need to enter them manually.
 - **Exclude specified Domain / IP List:** If selected, traffic matching this rule will not be routed to specified domains or IP addresses. You need to enter them manually.
5. A VPN tunnel is added successfully. You will be directed to the **VPN Dashboard**. Add more VPN tunnels if needed. For security, please go to [All Other Traffic](#) and [Tunnel Options](#) to check **Kill Switch** status before enabling your VPN tunnel.

8.2.2 Case Reference

Here are two typical VPN policy configuration cases with step-by-step instructions for your reference.

Case 1: Route only specified devices over VPN

Requirements:

1. Only specific devices connected to this router access the Internet through the VPN. All other devices access the Internet through the local WAN.
2. The selected devices must use the VPN connection only. If the VPN disconnects unexpectedly, Internet access for these devices will be blocked to prevent DNS leaks and IP tracking.

Configuration Steps:

1. Select VPN profile.

If you have logged in with any integrated VPN service credentials or uploaded a configuration file, the available profiles will be listed here. Otherwise, go to **VPN Client Profile** to log in with your credentials or upload a configuration file manually.

Take [PureVPN](#) as an example. Select one or multiple profiles, and adjust their priority on the right if needed.

Add New Tunnel

1 Use

2 From

3 To

< PureVPN WireGuard

Q Search configuration file

sx0111301-ikev.dnsdialer.com
United States

sx023201-ikev.dnsdialer.com
United Kingdom ✓

sx032501-ikev.dnsdialer.com
Canada

sx0408331-ikev.dnsdialer.com
Germany ✓

sx0517119-ikev.dnsdialer.com
Netherlands

sx060289-ikev.dnsdialer.com
Sweden ✓

Selected Profile (3) ⓘ

sx023201-ikev.dn...
United Kingdom

sx0408331-ikev.d...
Germany

sx060289-ikev.dn...
Sweden

64

sx070682-ikev.dnsdialer.com Romania	sx080619-ikev.dnsdialer.com Switzerland
sx090449-ikev.dnsdialer.com Panama	sx1000401-ikev.dnsdialer.com Cyprus

Cancel
Next

2. Select client source.

Click the **Specified Devices** tab, select devices that will use the VPN, then click **Next**.

Add New Tunnel

Use
2
From
3
To

Select Client Source

All Clients
Specified Connection Types
Specified Devices
Exclude Specified Devices

Only route traffic from explicitly selected devices. All other devices will bypass this VPN tunnel.

Add DeviceSelected 0 / Total 4

GL-INET-08
MAC: self

iPhone
MAC:

glkvm
MAC:

DESKTOP-3PJ8KUD
MAC:

Back
Next

3. Select target destination.

Click the **All Targets** tab, set it as the traffic destination, then click **Apply**.

Add New Tunnel

Use
From
3
To

Select Target Destination ⓘ

All Targets

Specified Domain / IP List

Exclude Specified Domain / IP List

ⓘ Route all traffic from the selected source(s) through this VPN tunnel.



Back

Apply

- You will be directed to the VPN Dashboard. Now a VPN tunnel has been added successfully, as shown below.

VPN Dashboard

[Guide](#)

ⓘ Allow Non-VPN Traffic
Unmatched traffic uses standard internet.

Priority 1 Kill Switch ⚙️

Tunnel 1



Disconnected

From

2 Devices

To

All Targets

 United Kingdom
sx023201-ikev dnsdialer.com

Client Virtual IP (IPv4)

Server Address

Server Listen Port

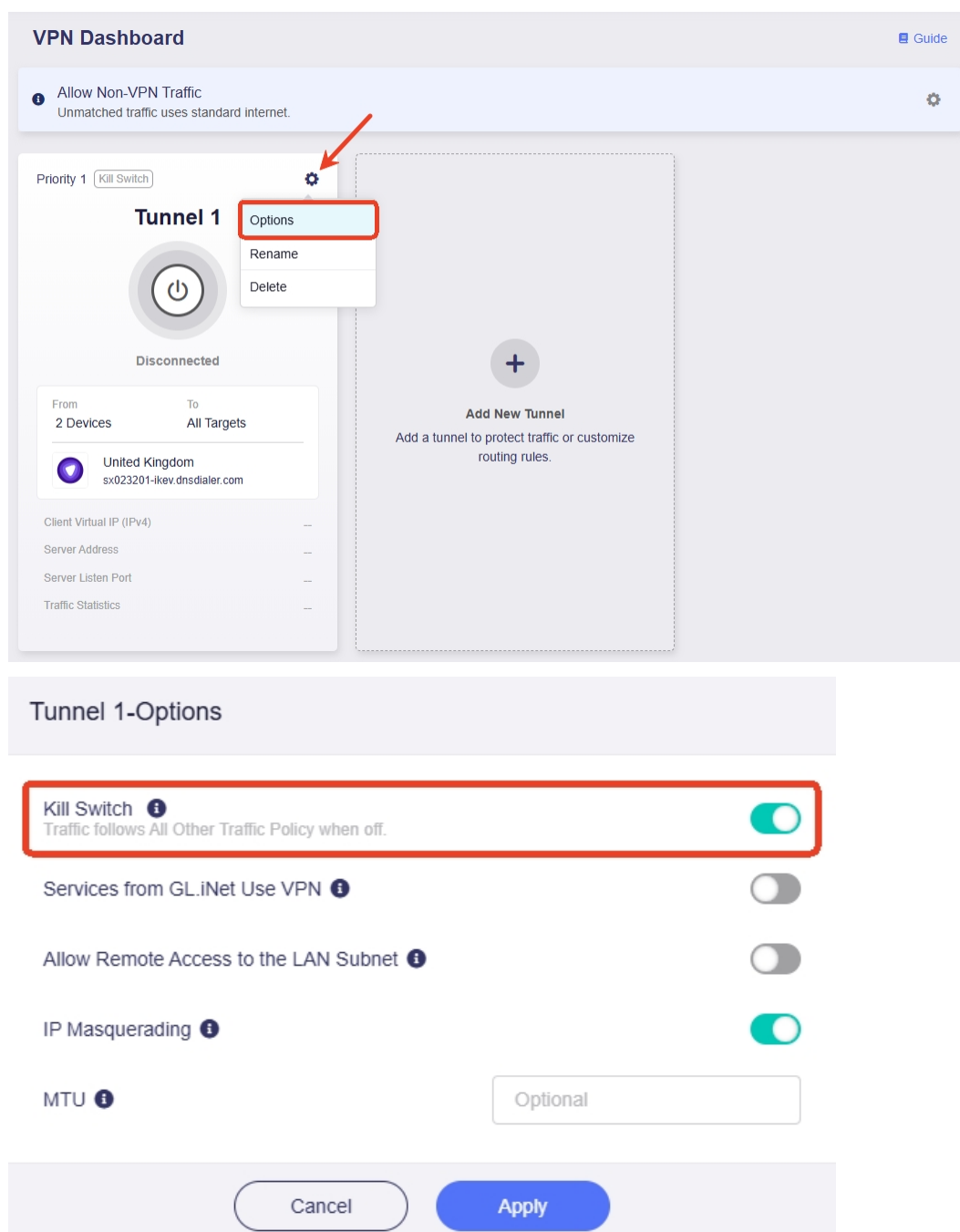
Traffic Statistics



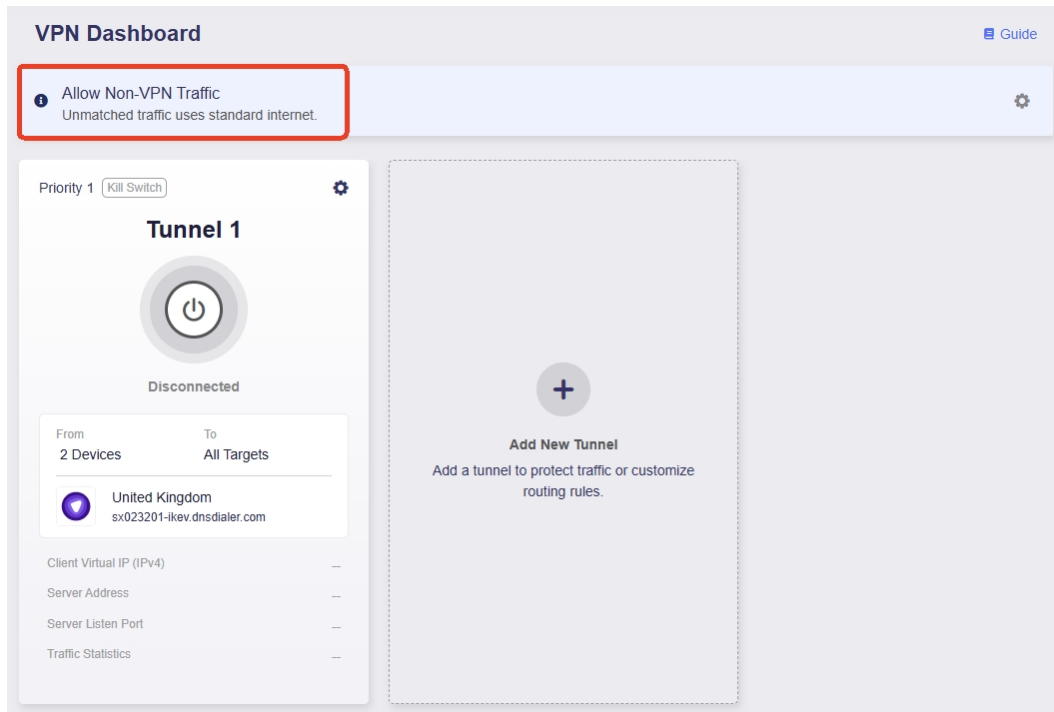
Add New Tunnel

Add a tunnel to protect traffic or customize routing rules.

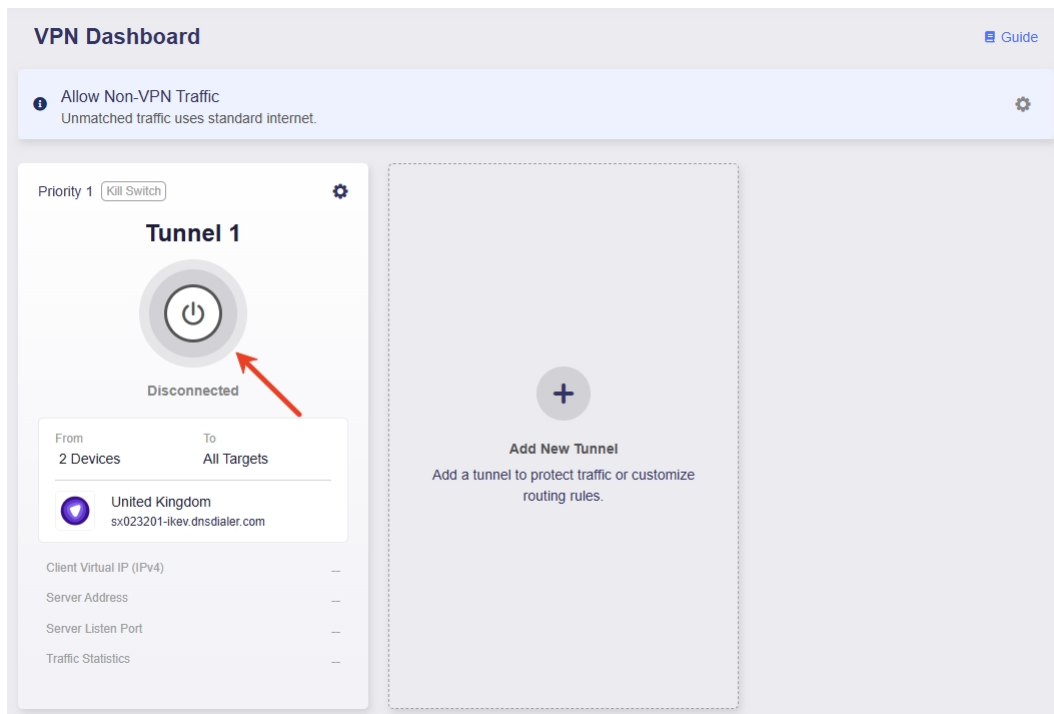
5. Make sure the **Kill Switch** for this tunnel is enabled. If the VPN disconnects unexpectedly, Internet access for traffic matching this tunnel will be blocked to prevent DNS leaks and IP tracking.



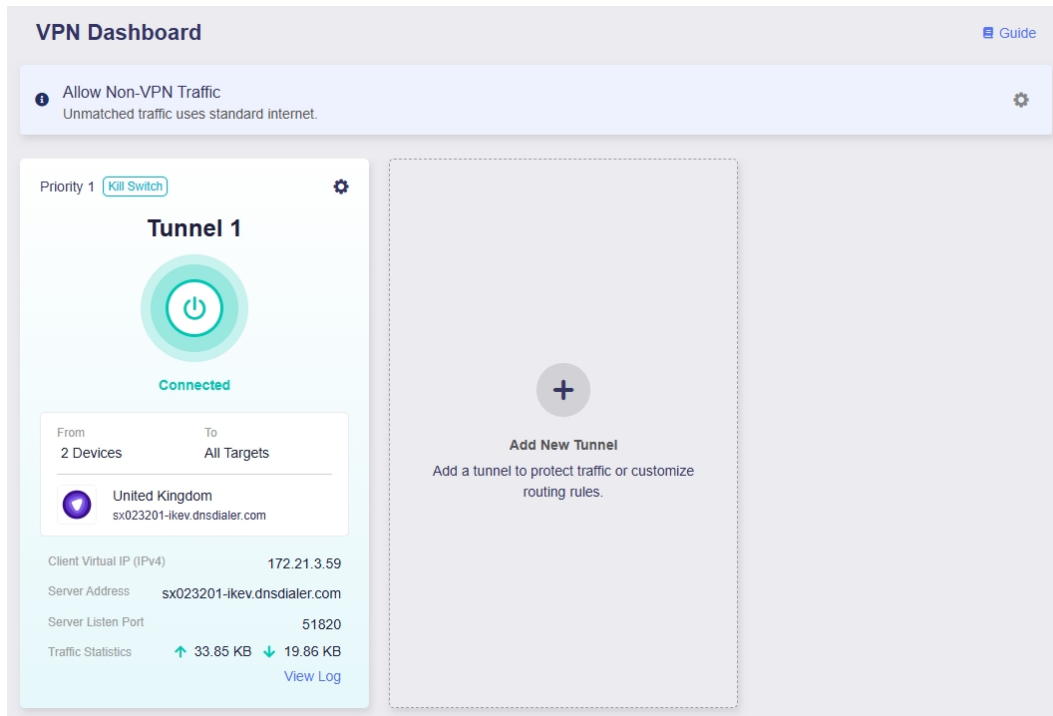
6. Make sure the **Allow Non-VPN Traffic** is enabled. This is enabled by default to ensure that traffic not matching the VPN tunnel can still access the Internet through the local WAN.



7. Click the middle button to activate this tunnel.



8. Once connected, the page will display the VPN connection details, including VPN policy, traffic statistics, server address, listen port, and virtual IP address.



Now, only two specified devices access the Internet through VPN. If the VPN disconnects unexpectedly, Internet access for these devices will be blocked to prevent DNS leaks and IP tracking. All other devices will access the Internet through the local WAN instead.

Case 2: Route all devices over VPN 1 for specific websites, and route all remaining traffic over VPN 2.

Requirements:

1. All devices use VPN Tunnel 1 when accessing domains of specific social media and streaming services, and use VPN Tunnel 2 for all other Internet access.
2. If the VPN tunnels disconnect unexpectedly, Internet access for all devices will be blocked to prevent DNS leaks and IP tracking.

Configuration Steps:

1. Select the VPN profile for Tunnel 1.

If you have logged in with any integrated VPN service credentials or uploaded a configuration file, the available profiles will be listed here. Otherwise, go to **VPN Client Profile** to log in with your credentials or upload a configuration file manually.

Take [PureVPN](#) as an example. Select one or multiple profiles, and adjust their priority on the right if needed, then click **Next**.

Add New Tunnel

1 Use
2 From
3 To

<
PureVPN
WireGuard

Search configuration file

sx0111301-ikev.dnsdialer.com
United States

sx023201-ikev.dnsdialer.com
United Kingdom

sx032501-ikev.dnsdialer.com
Canada

sx0408331-ikev.dnsdialer.com
Germany

sx0517119-ikev.dnsdialer.com
Netherlands

sx060289-ikev.dnsdialer.com
Sweden

sx070682-ikev.dnsdialer.com
Romania

sx080619-ikev.dnsdialer.com
Switzerland

sx090449-ikev.dnsdialer.com
Panama

sx1000401-ikev.dnsdialer.com
Cyprus

Selected Profile (2)

sx0517119-ikev.d...
Netherlands

sx032501-ikev.dn...
Canada

Cancel
Next

2. Select client source.

Click the **All Clients** tab, set it as the client source for Tunnel 1, then click **Next**.

Add New Tunnel

Use
From
To

Select Client Source

All Clients
Specified Connection Types
Specified Devices
Exclude Specified Devices

Route all traffic from every connected device through this VPN tunnel. Ideal for complete network privacy.

70

3. Select target destination.

Click the **Specified Domain / IP List** tab, enter domains of some common social media and streaming services, as shown below, then click **Apply**.

Add New Tunnel

Use

From

3 To

Select Target Destination

All Targets

Specified Domain / IP List

Exclude Specified Domain / IP List

Only route traffic destined for the listed domains or IP addresses through this VPN tunnel. Traffic to other destinations will bypass this tunnel.

Mode

Manual

Subscription URL

Total 15

1 facebook.com

2 instagram.com

3 x.com

4 youtube.com

5 tiktok.com

6 linkedin.com

7 pinterest.com

8 snapchat.com

9 whatsapp.com

10 telegram.org

11 reddit.com

12 netflix.com

13 disneyplus.com

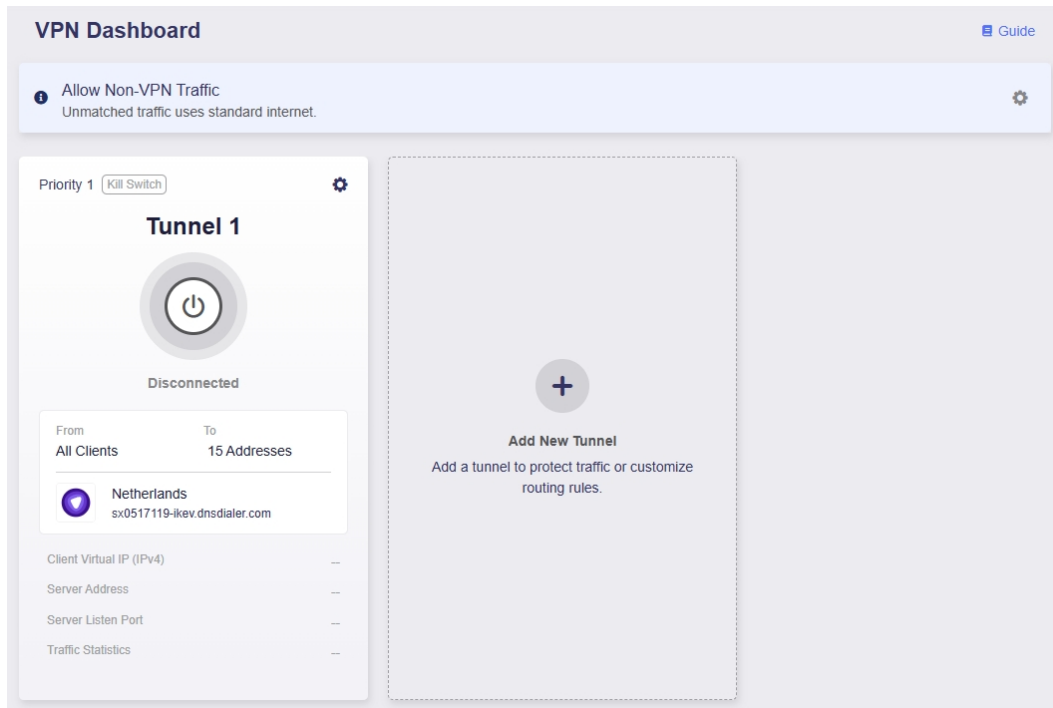
14 hulu.com

15 spotify.com

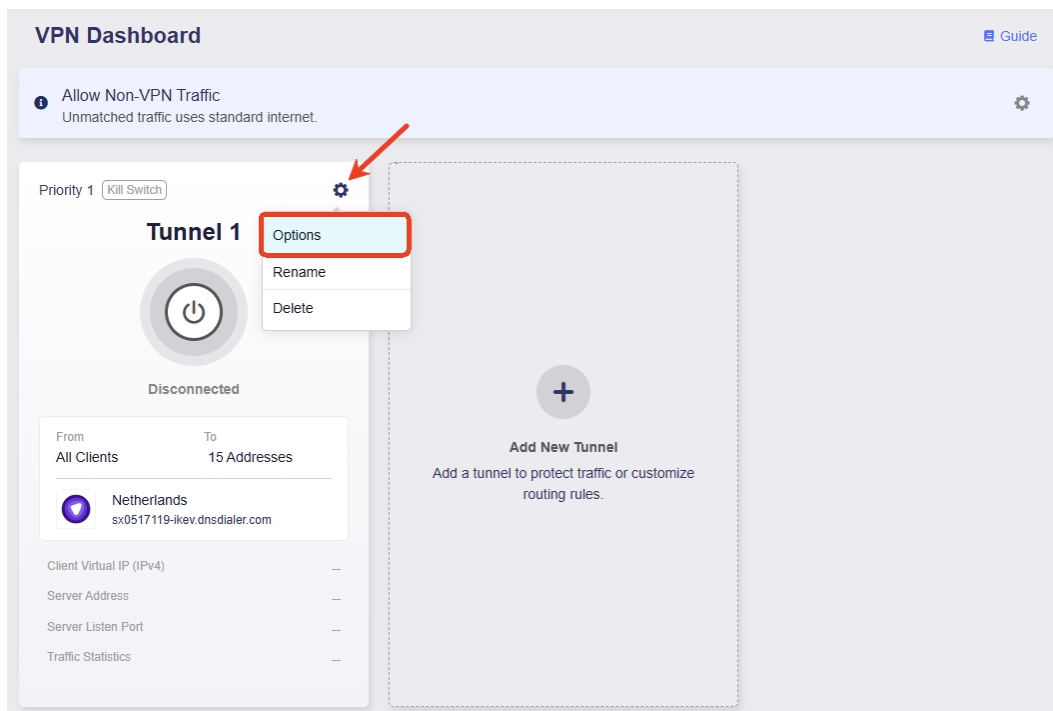
Back

Apply

4. You will be directed to the VPN Dashboard. Now the VPN tunnel 1 has been added successfully.



5. Make sure the **Kill Switch** for Tunnel 1 is enabled. If the VPN disconnects unexpectedly, Internet access for traffic matching this tunnel will be blocked to prevent DNS leaks and IP tracking.



Tunnel 1-Options

Kill Switch ⓘ
Traffic follows All Other Traffic Policy when off.

☒

Services from GL.iNet Use VPN ⓘ

☐

Allow Remote Access to the LAN Subnet ⓘ

☐

IP Masquerading ⓘ

☒

MTU ⓘ

Optional

Cancel

Apply

6. Click **Add New Tunnel** to add Tunnel 2.

VPN Dashboard

Allow Non-VPN Traffic
Unmatched traffic uses standard internet.

Priority 1 Kill Switch ⚙️

Tunnel 1

Disconnected

From

All Clients

To

15 Addresses

Netherlands
sx0517119-ikev.dnsdialer.com

Client Virtual IP (IPv4)

Server Address

Server Listen Port

Traffic Statistics

+

Add New Tunnel

Add a tunnel to protect traffic or customize routing rules.

7. Select VPN profile for Tunnel 2.
Select one or multiple profiles, and adjust their priority on the right if needed. Then click **Next**.

73

Add New Tunnel
×

1
Use
2
From
3
To

<
PureVPN
WireGuard

Search configuration file

sx0111301-ikev.dnsdialer.com
United States

sx023201-ikev.dnsdialer.com
United Kingdom

sx032501-ikev.dnsdialer.com
Canada

sx0408331-ikev.dnsdialer.com
Germany

sx0517119-ikev.dnsdialer.com
Netherlands

sx060289-ikev.dnsdialer.com
Sweden

sx070682-ikev.dnsdialer.com
Romania

sx080619-ikev.dnsdialer.com
Switzerland

sx090449-ikev.dnsdialer.com
Panama

sx1000401-ikev.dnsdialer.com
Cyprus

Selected Profile (2)

sx0408331-ikev.d...
Germany

sx023201-ikev.dn...
United Kingdom

Cancel

Next

8. Select client source.

Click the **All Clients** tab, set it as the client source for Tunnel 2, then click **Next**.

Add New Tunnel
×

✓ Use
2 From
3 To

Select Client Source

All Clients
Specified Connection Types
Specified Devices
Exclude Specified Devices

Route all traffic from every connected device through this VPN tunnel. Ideal for complete network privacy.

74



Back

Next

9. Select target destination.

Click the **All Targets** tab, set it as the traffic destination for Tunnel 2, then click **Apply**.

Add New Tunnel



Use



From



To

Select Target Destination ⓘ

All Targets

Specified Domain / IP List

Exclude Specified Domain / IP List

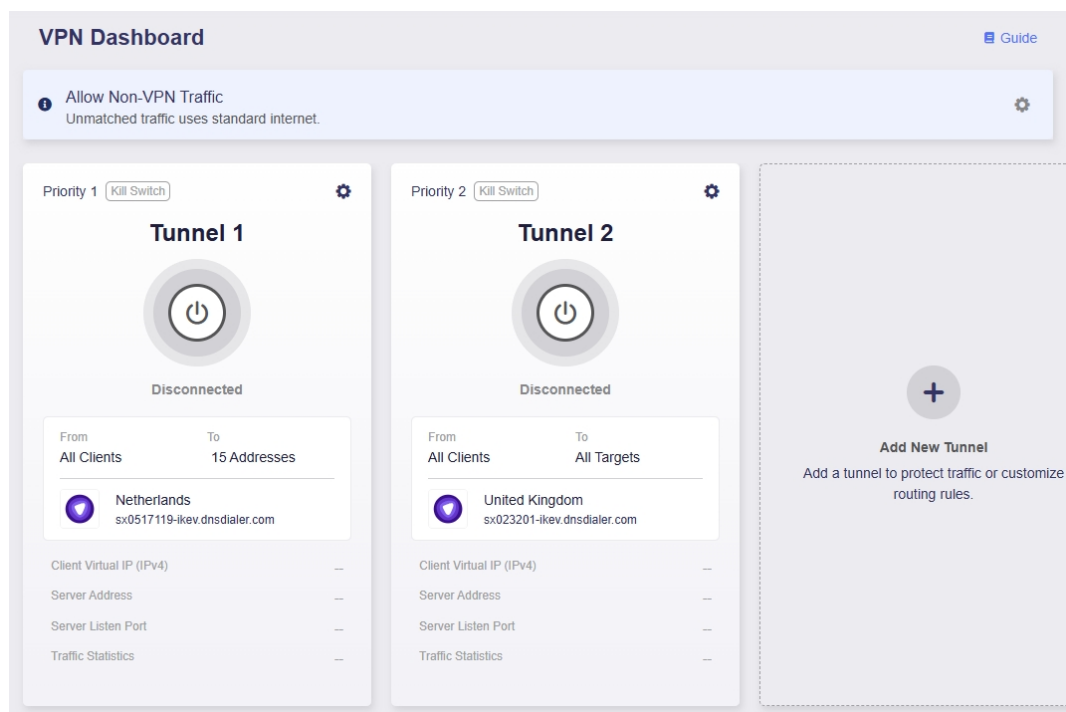
ⓘ Route all traffic from the selected source(s) through this VPN tunnel.



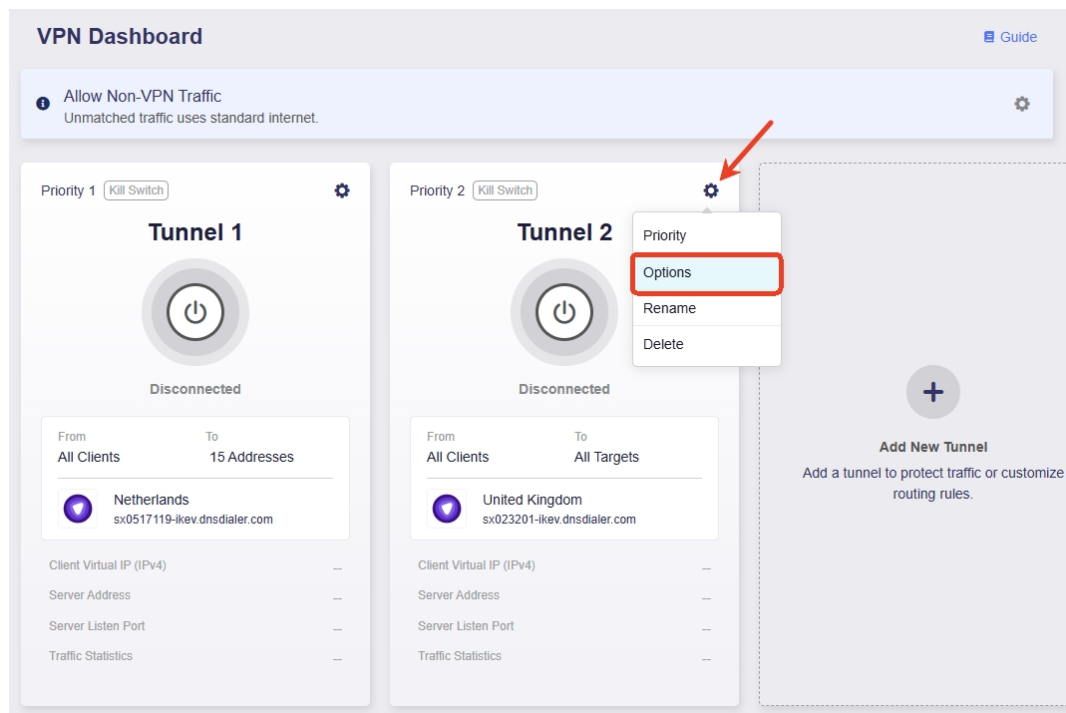
Back

Apply

10. You will be directed to the VPN Dashboard. Now the VPN tunnel 2 has been added successfully.



11. Make sure the **Kill Switch** for Tunnel 2 is enabled. If the VPN disconnects unexpectedly, Internet access for traffic matching this tunnel will be blocked to prevent DNS leaks and IP tracking.



Tunnel 2-Options

Kill Switch ⓘ
Traffic follows All Other Traffic Policy when off.

☒

Services from GL.iNet Use VPN ⓘ

☐

Allow Remote Access to the LAN Subnet ⓘ

☐

IP Masquerading ⓘ

☒

MTU ⓘ

Optional

Cancel

Apply

- Click the gear icon at the upper right to enable **Enhanced Kill Switch**. This ensures that all traffic must access Internet via the VPN.

VPN Dashboard
[Guide](#)

Allow Non-VPN Traffic
Unmatched traffic uses standard internet.

Priority 1 Kill Switch ⓘ

Tunnel 1

☒

Disconnected

From To
All Clients 15 Addresses

Netherlands
sx0517119-ikev.dnsdialer.com

Client Virtual IP (IPv4) —
Server Address —
Server Listen Port —
Traffic Statistics —

Priority 2 Kill Switch ⓘ

Tunnel 2

☒

Disconnected

From To
All Clients All Targets

United Kingdom
sx023201-ikev.dnsdialer.com

Client Virtual IP (IPv4) —
Server Address —
Server Listen Port —
Traffic Statistics —

+

Add New Tunnel
Add a tunnel to protect traffic or customize routing rules.

77

All Other Traffic Policy

This setting controls whether traffic not matched to any enabled VPN tunnel can access the internet.

"Allow Non-VPN Traffic" is enabled by default to ensure normal internet access for non-VPN traffic.

☐ Allow Non-VPN Traffic
Unmatched traffic will access the internet using your standard connection.

☒ Enhanced Kill Switch
Force all devices to use a VPN to access the internet. Any traffic that does not match a VPN tunnel will be blocked.

Note: This global setting does not override the Kill Switch configured for individual VPN tunnels.

Cancel

Apply

- Click the middle button to activate Tunnel 1 and Tunnel 2.

VPN Dashboard

Allow Non-VPN Traffic

Unmatched traffic uses standard internet.

Priority 1 Kill Switch

Tunnel 1

Disconnected

From

All Clients

To

15 Addresses

Netherlands

sx0517119-ikev.dnsdialer.com

Client Virtual IP (IPv4)

Server Address

Server Listen Port

Traffic Statistics

Priority 2 Kill Switch

Tunnel 2

Disconnected

From

All Clients

To

All Targets

United Kingdom

sx023201-ikev.dnsdialer.com

Client Virtual IP (IPv4)

Server Address

Server Listen Port

Traffic Statistics

+

Add New Tunnel

Add a tunnel to protect traffic or customize routing rules.

- Once connected, the page will display the VPN connection details, including VPN policy, traffic statistics, server address, listen port, and virtual IP address.

VPN Dashboard

Guide

1

Allow Non-VPN Traffic

Unmatched traffic uses standard internet.

⚙

Priority 1

Kill Switch

⚙

Tunnel 1



Connected

From

All Clients

To

15 Addresses



Canada

sx032401-ikev.dnsdialer.com

Client Virtual IP (IPv4)

172.21.8.97

Server Address

sx032401-ikev.dnsdialer.com

Server Listen Port

51820

Traffic Statistics

↑ 360.00 B

↓ 184.00 B

[View Log](#)

Priority 2

Kill Switch

⚙

Tunnel 2



Connected

From

All Clients

To

All Targets



United Kingdom

sx0216116-ikev.dnsdialer.com

Client Virtual IP (IPv4)

172.21.9.0

Server Address

sx0216116-ikev.dnsdialer.com

Server Listen Port

51820

Traffic Statistics

↑ 13.91 KB

↓ 9.10 KB

[View Log](#)

+

Add New Tunnel

Add a tunnel to protect traffic or customize routing rules.

Now, all devices will use VPN Tunnel 1 when accessing specified domains, and use VPN Tunnel 2 for all other Internet access. If the VPN tunnels disconnect unexpectedly, Internet access for all devices will be blocked to prevent DNS leaks and IP tracking.

8.3 Kill Switch

Kill Switch is a security feature for VPN connections. It automatically cuts off all internet access for your local network if the VPN connection drops unexpectedly, preventing your real IP address and online data from being exposed and ensuring continuous privacy and security. This feature is particularly useful for maintaining secure, anonymous internet access, such as when using public networks, processing sensitive data, or hiding your real IP address.

When enabled, it blocks any client traffic that attempts to bypass the VPN tunnel, effectively stopping VPN leaks caused by DNS configuration issues, unexpected disconnections, direct IP requests, and other similar scenarios.

Since firmware v4.8, GL.iNet routers supports Kill Switch configuration for the global VPN connection, as well as for each individual VPN tunnel.

- To set up Kill Switch for the global VPN connection, refer to [All Other Traffic](#).
- To set up Kill Switch for each individual VPN tunnel, refer to [Tunnel Options](#).

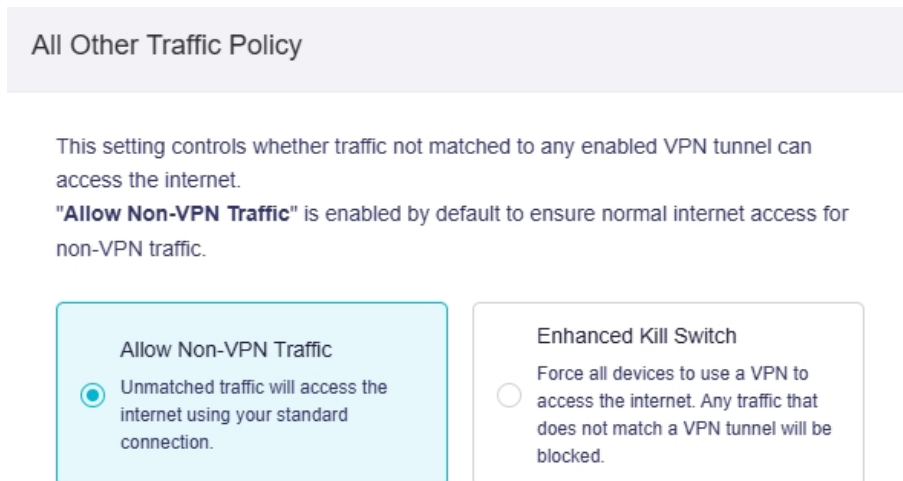
8.4 All Other Traffic

Click the gear icon at the upper right to set up policy for traffic not matching VPN tunnel.

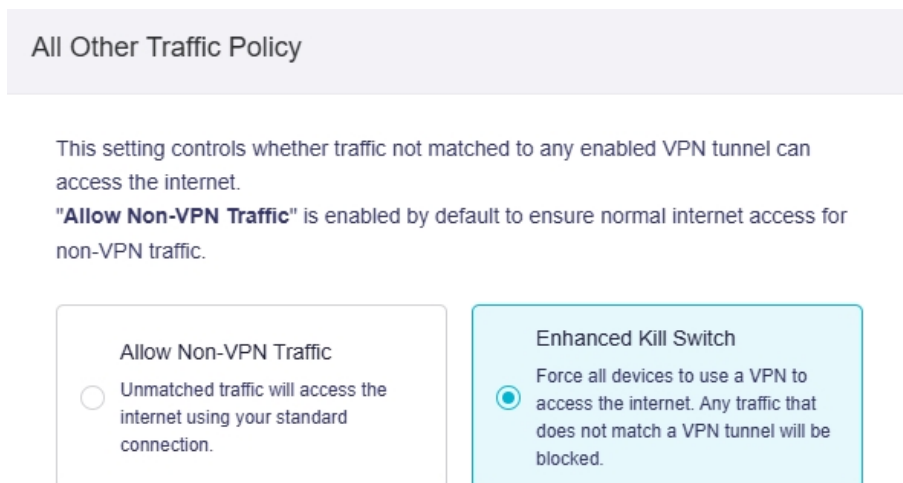


This policy controls whether traffic that does not match any of your VPN tunnel groups can access the Internet or not. It has two options:

- **Allow Non-VPN Traffic:** Enabled by default to ensure normal internet access for non-VPN traffic.



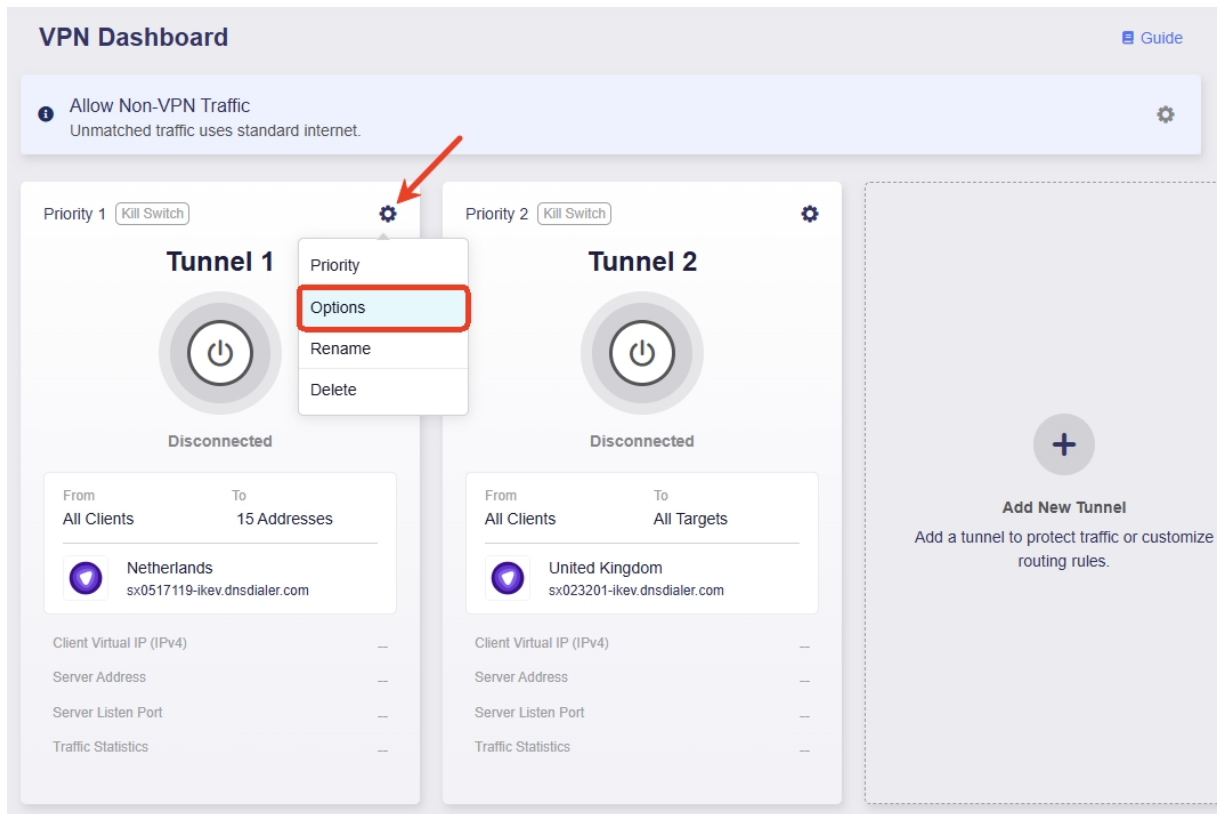
- **Enhanced Kill Switch:** Forces all devices to access the Internet through a VPN. Any traffic that does not match a VPN tunnel will be blocked. This global setting does not override the Kill Switch configured for individual VPN tunnels.



8.5 Tunnel Options

You can configure advanced settings for each VPN tunnel, such as the VPN Kill Switch, IP Masquerading, and MTU.

Click the gear icon in a tunnel group, and select **Options**.



Tunnel 1-Options

Kill Switch ⓘ ☒ Traffic follows All Other Traffic Policy when off.

Services from GL.iNet Use VPN ⓘ ☐

Allow Remote Access to the LAN Subnet ⓘ ☐

IP Masquerading ⓘ ☒

MTU ⓘ

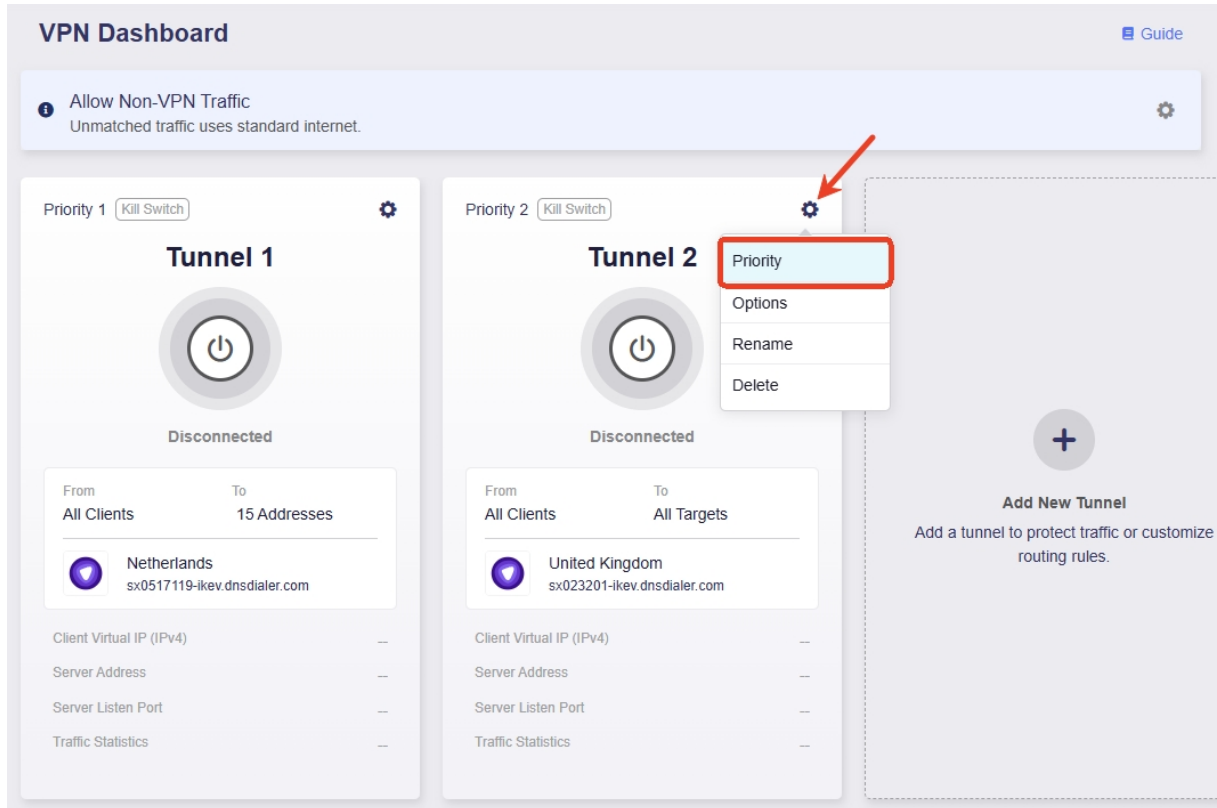
Cancel

Apply

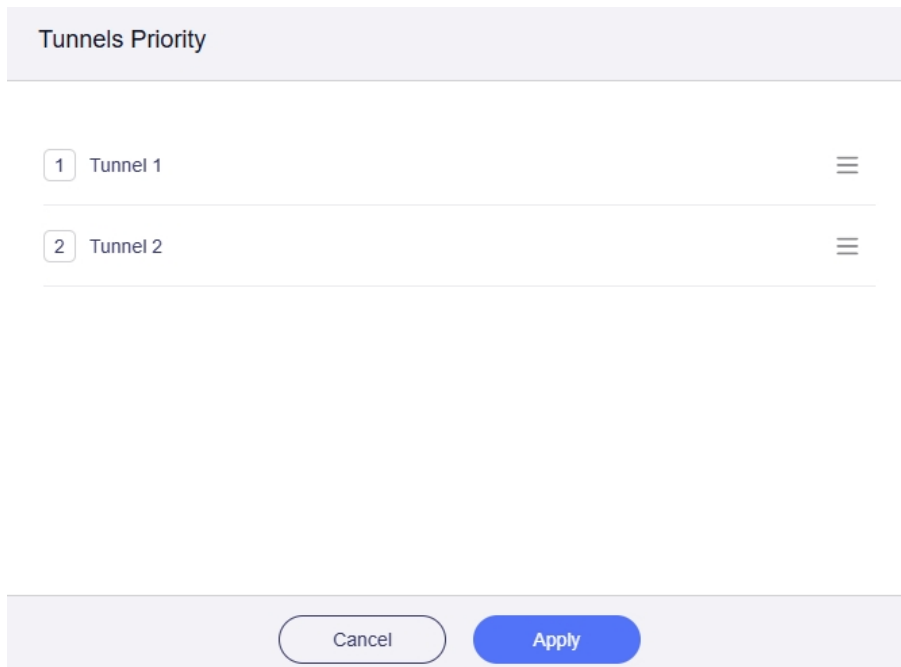
- **Kill Switch:** If enabled, traffic matching this VPN tunnel will be blocked if the VPN connection fails unexpectedly. If disabled, such traffic will fail over to the All Other Traffic tunnel.
- **Services from GL.iNet Use VPN:** If enabled, GoodCloud, DDNS, and rtty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.
- **Allow Remote Access to the LAN Subnet:** If enabled, remote access to this router and its LAN devices through the VPN will be allowed. It requires the VPN server to advertise a route back to its LAN subnet.
- **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:** The MTU value you set for the tunnel will override the MTU settings in the configuration file.

8.6 Tunnel Priority

To adjust tunnel priority, click the gear icon in a tunnel group and select **Priority**.



Click and hold the three-line icon on the right to reorder the tunnels, then click **Apply**.



When multiple tunnels are enabled, the router routes traffic according to the following rules:

1. Traffic will first attempt to match the highest-priority tunnel rule. If matched, it will be routed through that tunnel; otherwise, it will try the next priority tunnel, and so on.
2. Each tunnel group operates independently. Once traffic matches a tunnel rule, it will be routed through that tunnel and will not fail over between tunnel groups.
3. Multiple profiles can be selected within each tunnel group to enable intra-tunnel failover. When the highest-priority profile in a tunnel group goes down, the tunnel will automatically connect using the second-highest priority profile, and so on.
4. If a VPN tunnel disconnects unexpectedly, the system will determine whether to fail over the traffic to the All Other Traffic tunnel based on whether this tunnel's **Kill Switch** is enabled.
 - If the Kill Switch is enabled, traffic will be blocked and will not fail over to the All Other Traffic tunnel.
 - If the Kill Switch is disabled, traffic will fail over to the All Other Traffic tunnel.
5. In the **All Other Traffic** tunnel, different modes determine whether the traffic that does not match the VPN tunnel can access the Internet.
 - **Allow Non-VPN Traffic:** It is enabled by default to ensure that traffic not matching the VPN tunnels can still access the Internet via local WAN.
 - **Enhanced Kill Switch:** It forces all devices to access the Internet through a VPN. Any traffic that does not match a VPN tunnel will be blocked. This global setting does not override the Kill Switch configured for individual VPN tunnels. In short, it strengthens the Kill Switch and blocks regular Internet access to prevent IP leaks.

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.

Configuration Users Route Rules

Device Mode TUN

Protocol UDP

Local Port 1194

IPv4 Subnet 10.8.0.0/24

IPv6 Subnet *i* fd00:a79f:8609:088f::0/64

Authentication Mode *i* Certificate only

i Advanced Configuration *v*

Reset Apply

u Export Client Configuration

- **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. Export Client Configuration.

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

Export Client Configuration

Use DDNS domain to avoid the situation where a client cannot connect to the VPN service because of a change to the public IP address provided by your ISP. If you want to activate this function, please [Enable DDNS](#) on your router.

Address

183.178.100.100

Download

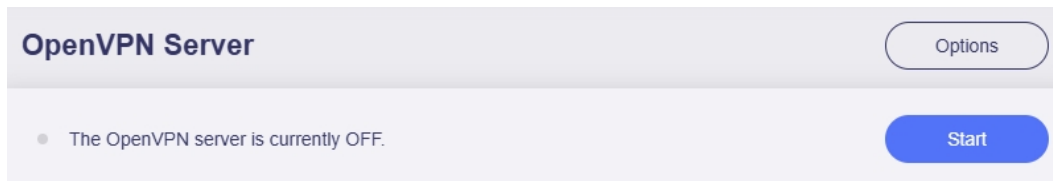
Tips:

- If your public IP address changes frequently, go to **APPLICATIONS > Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.
- Since firmware v4.8, you can select the server address from a drop-down list before exporting the configuration file: Public IP, DDNS domain, and current WAN IP

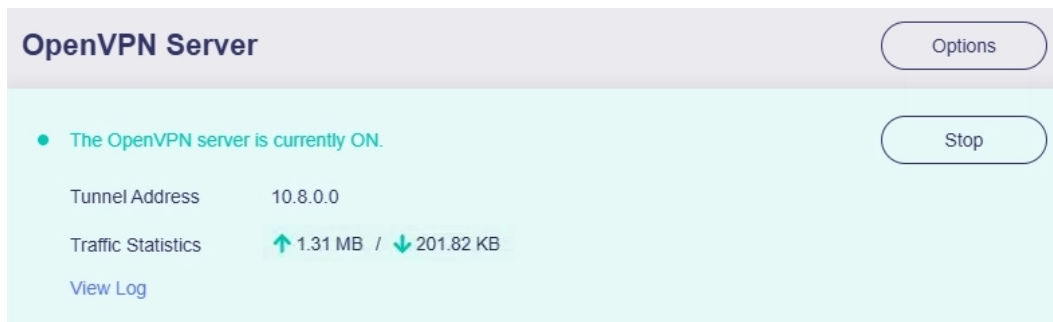
address. Once selected, the server address in the configuration file will be updated automatically. Re-download the configuration file if the server address is changed.

4. Start OpenVPN server.

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



The server connection status is displayed at the top. If it shows upload and download traffic statistics, it means the OpenVPN server is running.



9.1.3 Troubleshooting

If the connection fails, there are several common reasons:

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

9.2 Set Up WireGuard Server

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

9.2.1 Preparation

1. Make sure you have a public IP address

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

Alternative methods:

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

The screenshot shows the 'Configuration' tab of the WireGuard Server setup. It includes three input fields: 'IPv4 Address' with the value '10.0.0.1/24', 'IPv6 Address' with the value 'fd00:db8:0:abc::1/64', and 'Listen Port' with the value '51820'. Below these fields is a link 'Set Key Manually' with a dropdown arrow. At the bottom are 'Reset' and 'Apply' buttons.

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.

This screenshot is similar to the previous one but highlights a modification. The 'IPv4 Address' field, which originally contained '10.0.0.1/24', is now shown with a red box around the text and a red arrow pointing to the new value '10.1.0.1/24'. The other fields and buttons remain the same.

3. Add a profile.

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

WireGuard Server Options

● The WireGuard server is currently OFF. Start

Configuration **Profiles** Route Rules

i Each client device that connects to the WireGuard server requires a unique peer configuration. You need to create a separate configuration for each client device; each configuration must specify a unique client IP. **+ Add**

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

Client Configuration

Name

[Set More](#)

Cancel Apply

Tip: If you want to access the WireGuard client's LAN devices from your WireGuard server, switch to the **Route Rules** tab to configure route rules. See [here](#) for details.

4. Download configuration.

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

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

WireGuard® Client Configuration

Use DDNS domain to avoid the situation where a client cannot connect to the VPN service because of a change to the public IP address provided by your ISP.
If you want to activate this function, please [Enable DDNS](#) on your router.
If you want to use IPv6 address, please [Enabled IPv6](#) on your router.

Address ⓘ 35.76.125.9

QR Code Configuration File

```
[Interface]
Address = 10.1.0.2/24,fd00:ff14:e440:ae83::2/64
PrivateKey = 
DNS = 10.1.0.1,fd00:ff14:e440:ae83::1,64.6.64.6
MTU = 1420

[Peer]
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = 35.76.125.9:51820
PersistentKeepalive = 25
PublicKey = 
```

Download

Tips:

- If your public IP address changes frequently, go to **APPLICATIONS > Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.
- Since firmware v4.8, you can select the server address from a drop-down list before exporting the configuration file: Public IP, DDNS domain, and current WAN IP address. Once selected, the server address in the configuration file will be updated automatically. Re-download the configuration file if the server address is changed.

Address ⓘ 35.76.125.9

QR Code Configuration File

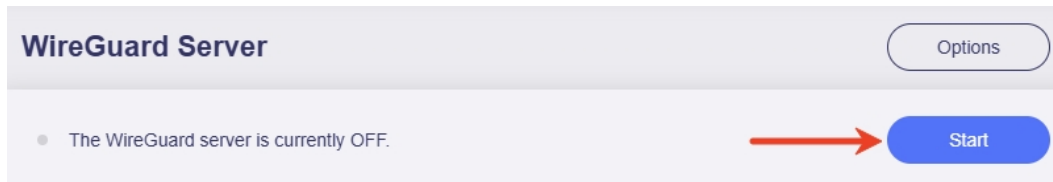
35.76.125.9

.glddns.com

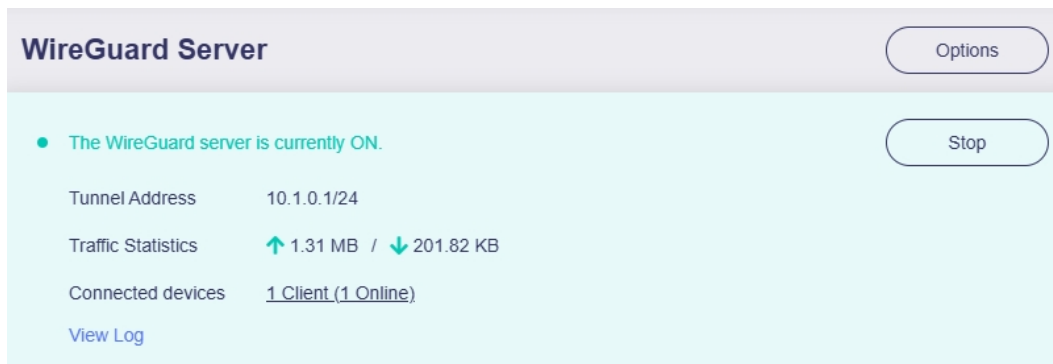
192.168.6.189

5. Start WireGuard server.

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



The server connection status is displayed at the top. If it shows upload, download traffic statistics, and online connected devices, it means the WireGuard server is running.



9.2.3 Troubleshooting

If the connection fails, there are several common reasons:

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

Chapter 10

Set Up VPN Client

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

10.1 Set Up OpenVPN Client

10.1.1 Preparation

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

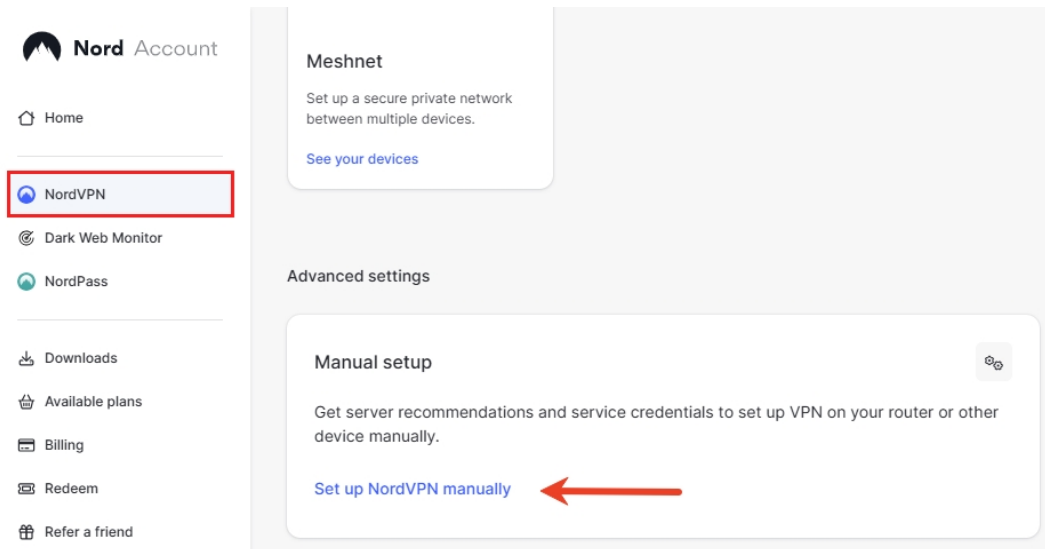
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to [this link](#) or contact their support.

10.1.2 Set Up NordVPN

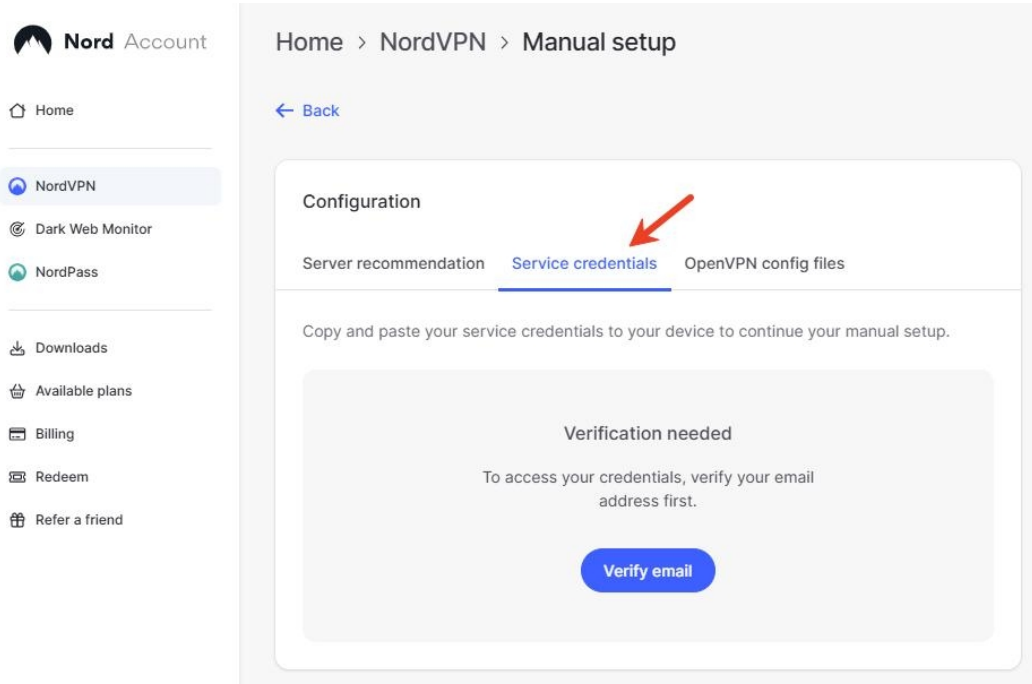
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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

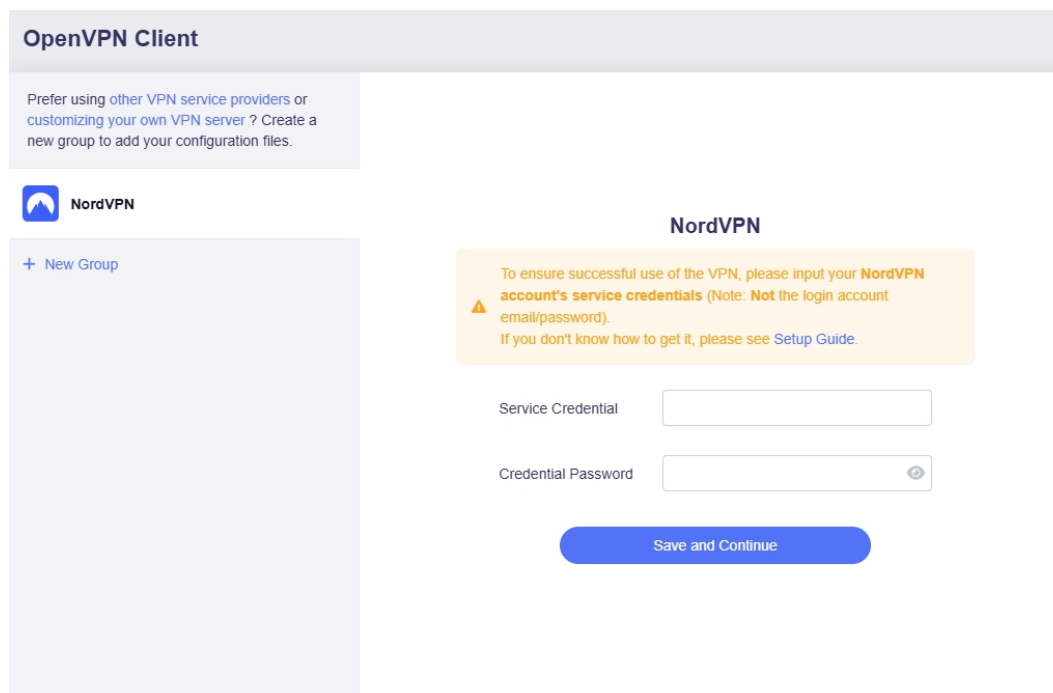
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



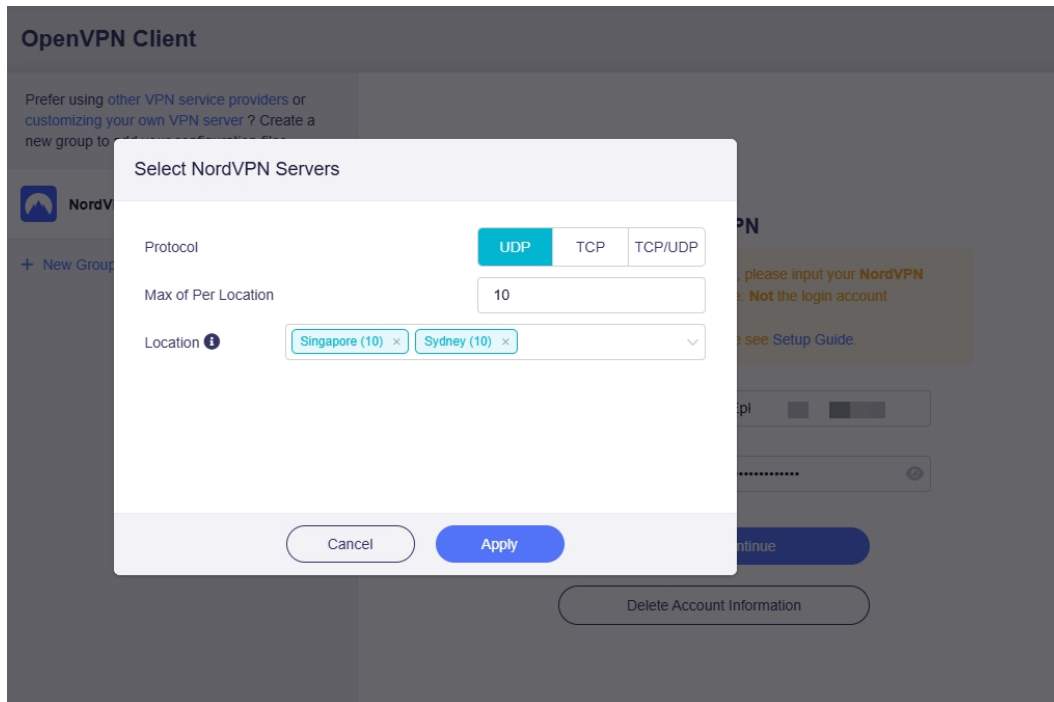
You will find the **service credentials**. Copy them for later use.



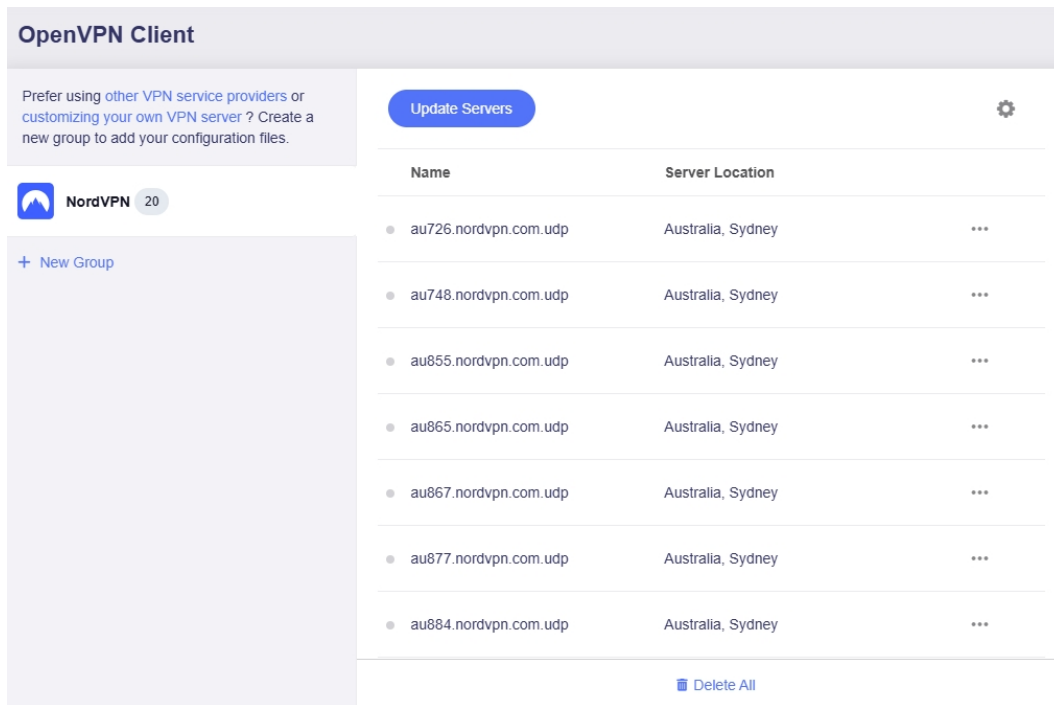
3. Log in to your router's web admin panel and navigate to **VPN > OpenVPN Client > NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



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

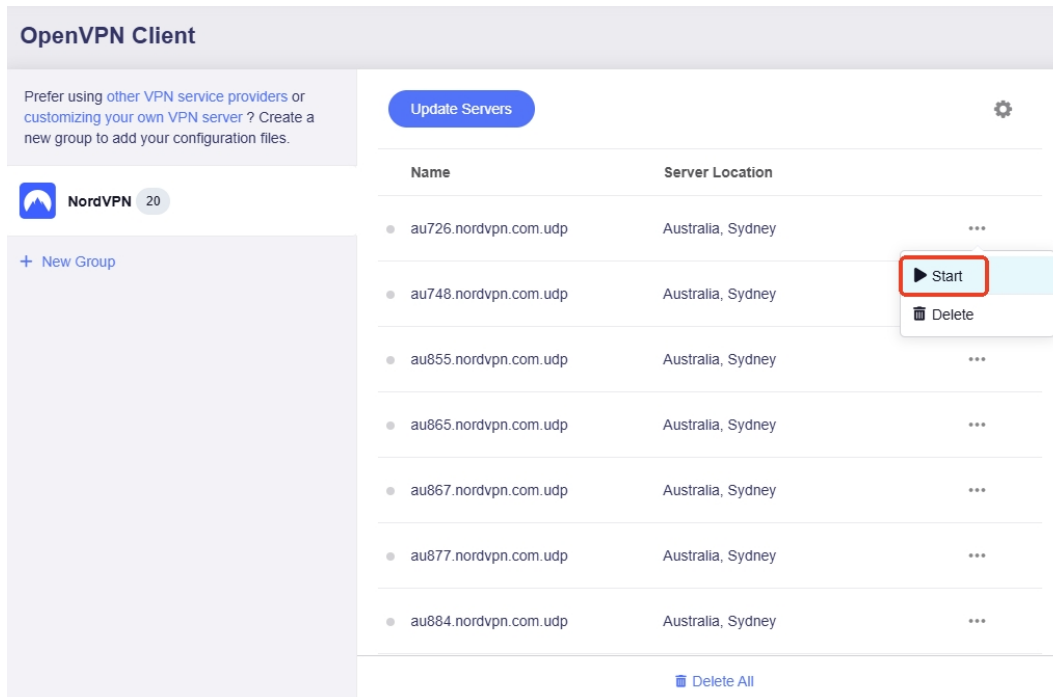


It will download configuration files.

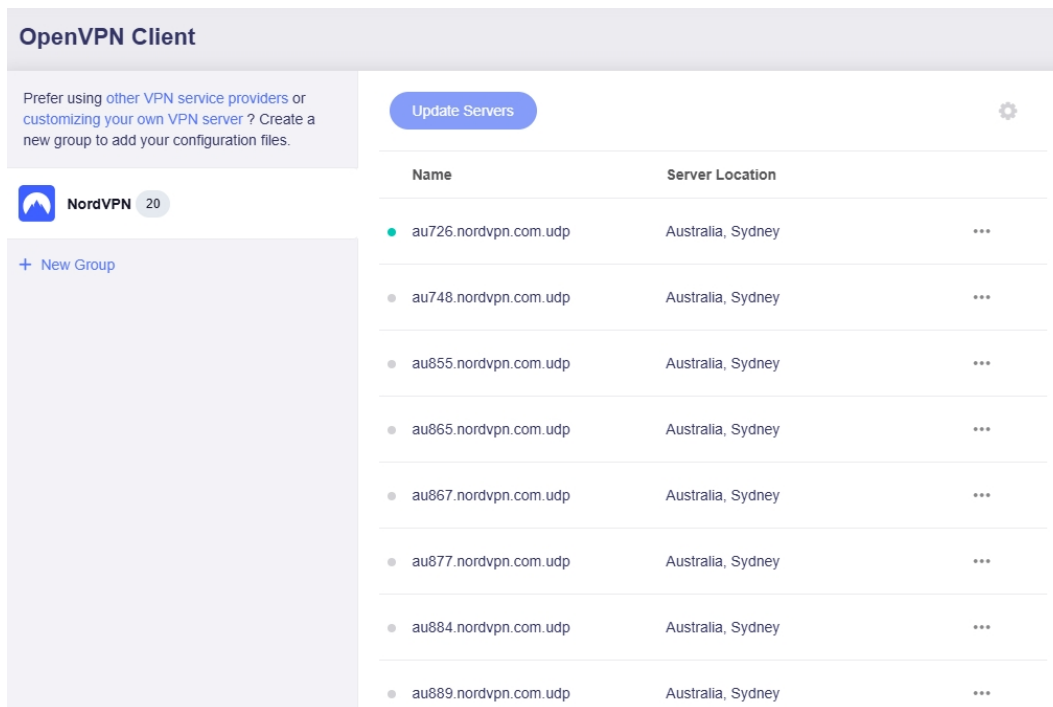


5. Start a connection.

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



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



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

- Update servers.

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

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	...
• au748.nordvpn.com.udp	Australia, Sydney	...
• au855.nordvpn.com.udp	Australia, Sydney	...
• au865.nordvpn.com.udp	Australia, Sydney	...
• au867.nordvpn.com.udp	Australia, Sydney	...
• au877.nordvpn.com.udp	Australia, Sydney	...
• au884.nordvpn.com.udp	Australia, Sydney	...

[Delete All](#)

8. Edit credentials.

Click the gear icon to edit your login credentials.

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	...
• au748.nordvpn.com.udp	Australia, Sydney	...
• au855.nordvpn.com.udp	Australia, Sydney	...
• au865.nordvpn.com.udp	Australia, Sydney	...
• au867.nordvpn.com.udp	Australia, Sydney	...
• au877.nordvpn.com.udp	Australia, Sydney	...
• au884.nordvpn.com.udp	Australia, Sydney	...

[Delete All](#)

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

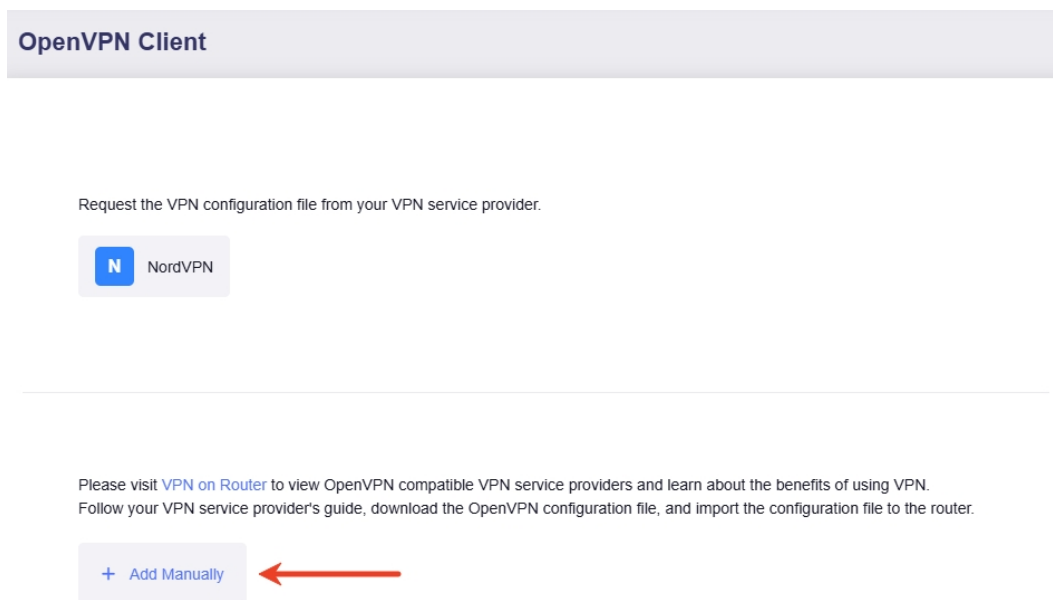
Delete

10.1.3 Set Up OpenVPN Client Manually (for other providers)

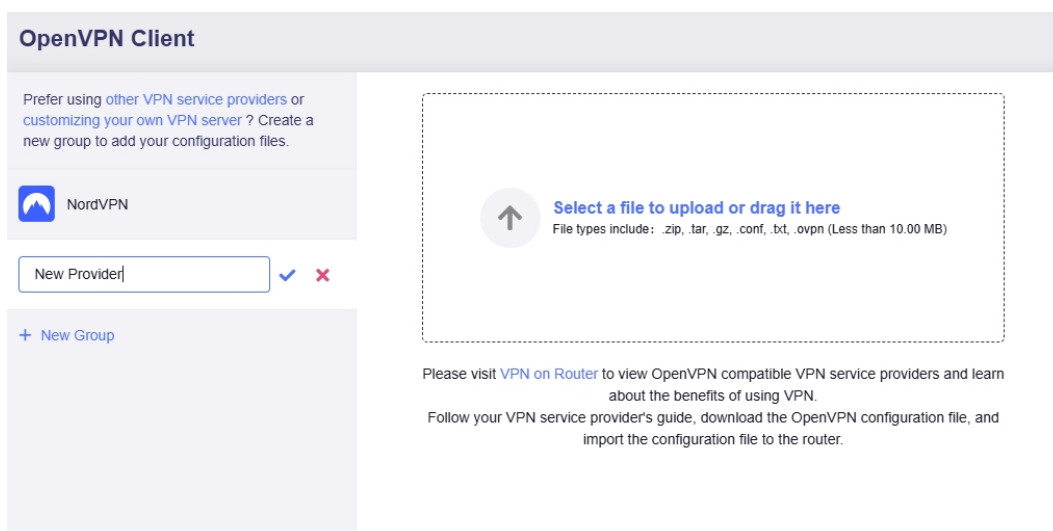
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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**.

OpenVPN Client

Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.

NordVPN

Private Internet Access

+ New Group

Upload successful
ca_toronto-aes-128-cbc-udp-dns.ovpn
Re-upload file

1 valid configuration files have been detected. Please enter the username and password. If these configurations use different passwords, you will need to enter the password individually for each configuration file:

Username

Password

Apply

You will see the configuration file uploaded.

OpenVPN Client

Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.

NordVPN

Private Internet Access **1**

+ New Group

Upload Configuration File

Name	Server Address	
ca_toronto-aes-128-cbc-udp-dns	ca-toronto.privacy.network:1198	...

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

OpenVPN Client

Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.

NordVPN

Private Internet Access **1**

+ New Group

Upload Configuration File

Name	Server Address	
ca_toronto-aes-128-cbc-udp-dns	ca-toronto.privacy.network:1198	...

Start
 Modify
 Delete

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

OpenVPN Client

Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.

 NordVPN

Private Internet Access 1

+ New Group

Upload Configuration File

Name	Server Address	
ca_toronto-aes-128-cbc-udp-dns	ca-toronto.privacy.network:1198	...

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.

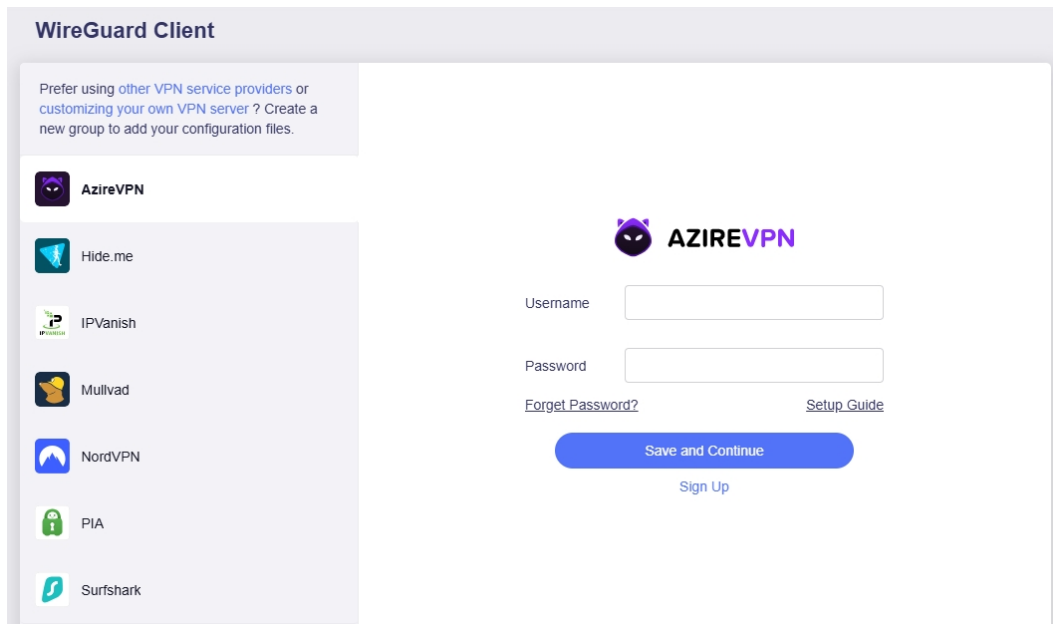
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

- [Set Up AzireVPN](#)
- [Set Up Hide.me](#)
- [Set Up IPVanish](#)
- [Set Up Mullvad](#)
- [Set Up NordVPN](#)
- [Set Up PIA \(Private Internet Access\)](#)
- [Set Up PureVPN](#)
- [Set Up Surfshark](#)
- [Set Up Windscribe](#)
- [Set Up WireGuard Client Manually \(for other providers\)](#)

10.2.2 Set Up AzireVPN

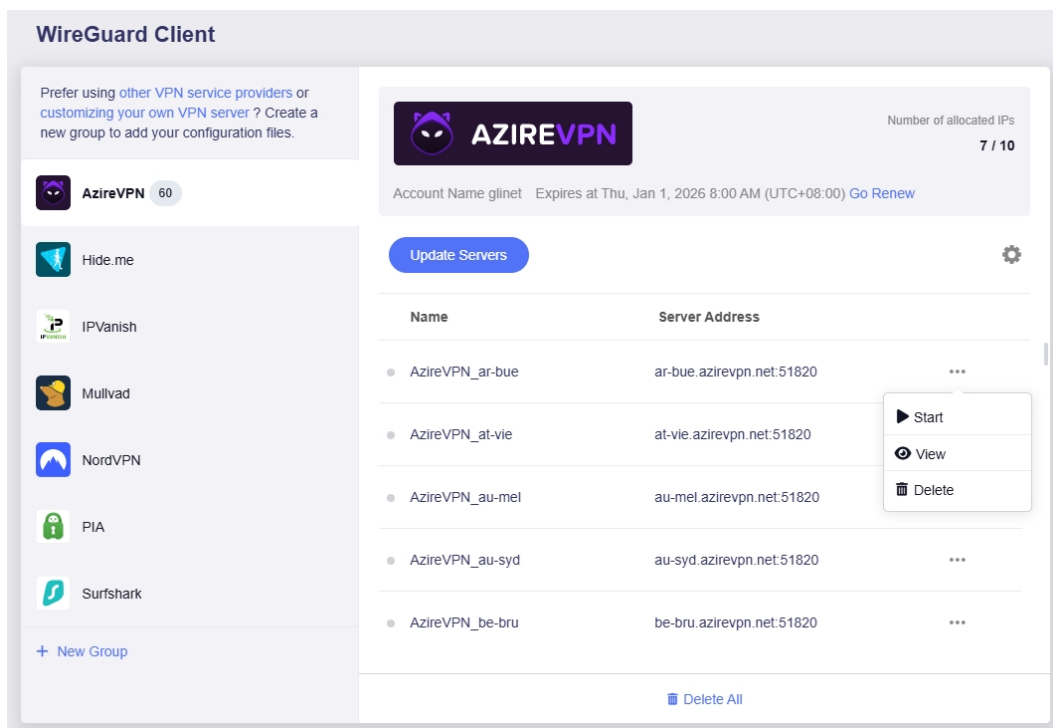
Follow the steps below to set your router as an AzireVPN client.

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.



The screenshot shows the 'WireGuard Client' interface. On the left, a sidebar lists various VPN providers: AzireVPN (selected), Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The main area displays the 'AZIREVPN' login form. It includes a 'Username' field, a 'Password' field, and a 'Save and Continue' button. Below the password field are links for 'Forgot Password?' and 'Setup Guide'. A 'Sign Up' link is located at the bottom of the form.

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

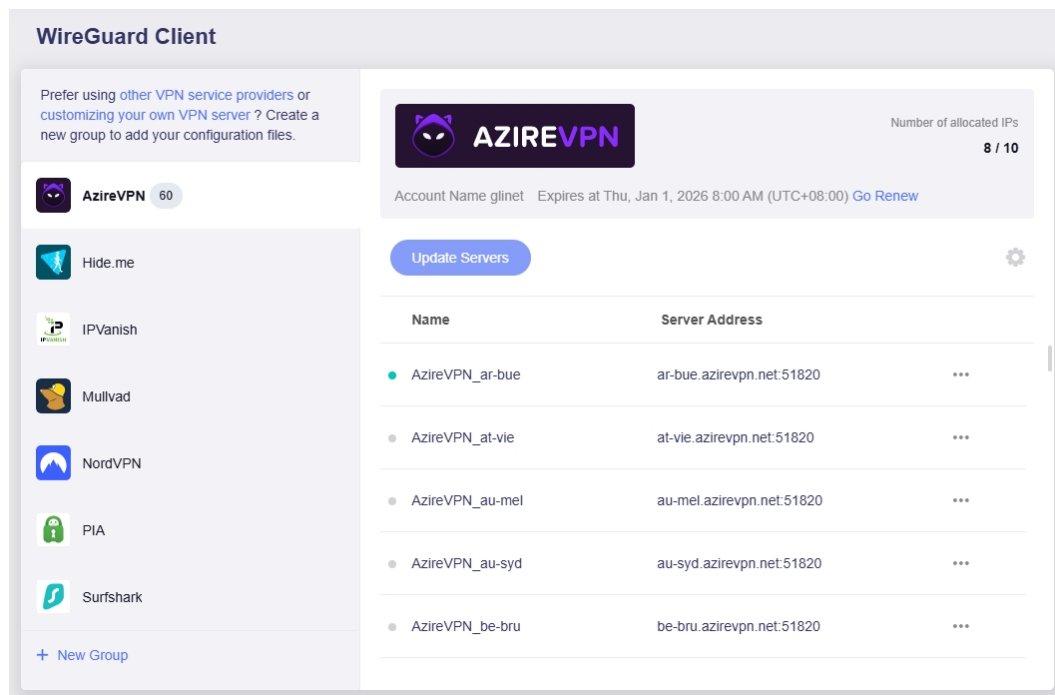


The screenshot shows the 'WireGuard Client' interface after logging in. The sidebar on the left remains the same. The main area now displays the 'AZIREVPN' account details, including the account name 'glinet', the expiration date 'Expires at Thu, Jan 1, 2026 8:00 AM (UTC+08:00)', and a 'Go Renew' link. Below this is an 'Update Servers' button. A table lists the available servers:

Name	Server Address	
AzireVPN_ar-bue	ar-bue.azirevpn.net:51820	...
AzireVPN_at-vie	at-vie.azirevpn.net:51820	
AzireVPN_au-mel	au-mel.azirevpn.net:51820	
AzireVPN_au-syd	au-syd.azirevpn.net:51820	...
AzireVPN_be-bru	be-bru.azirevpn.net:51820	...

A context menu is open for the first server, showing options: 'Start', 'View', and 'Delete'. At the bottom of the table is a 'Delete All' button.

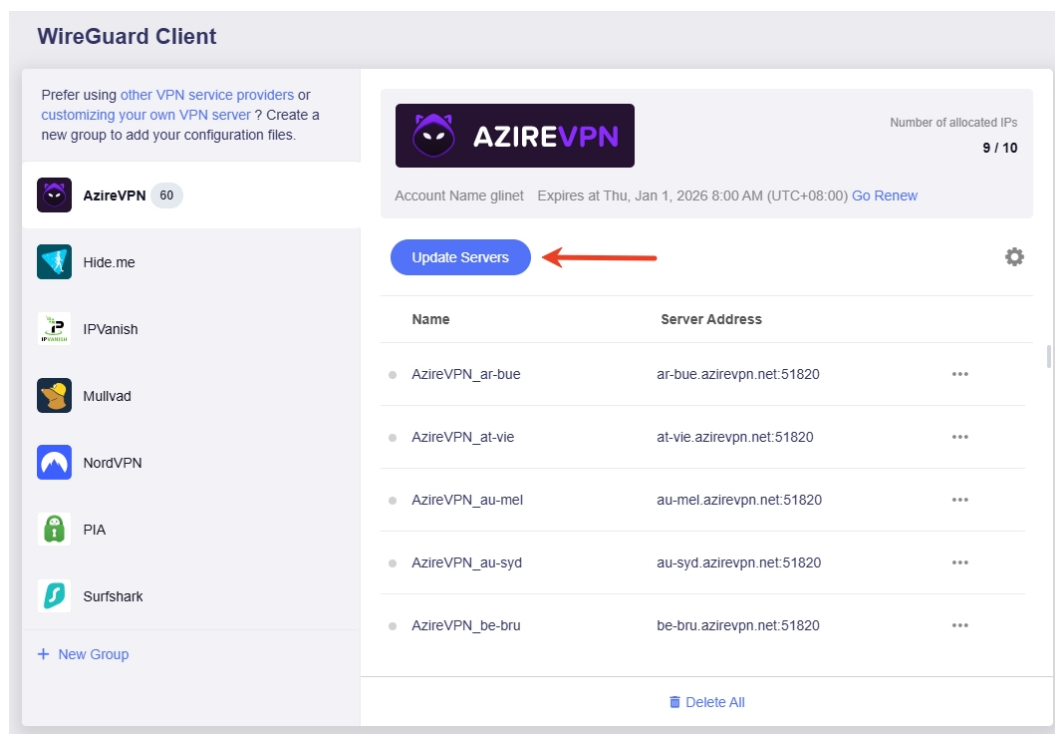
- Once connected, a green dot will appear next to the configuration file.



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

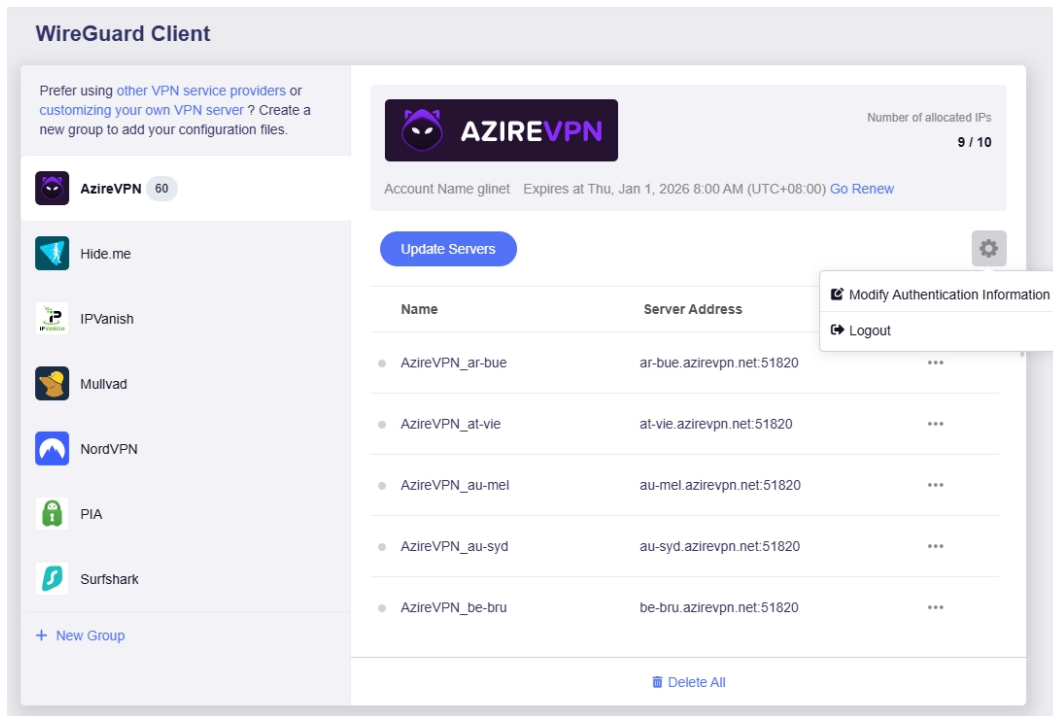
- Update servers.

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



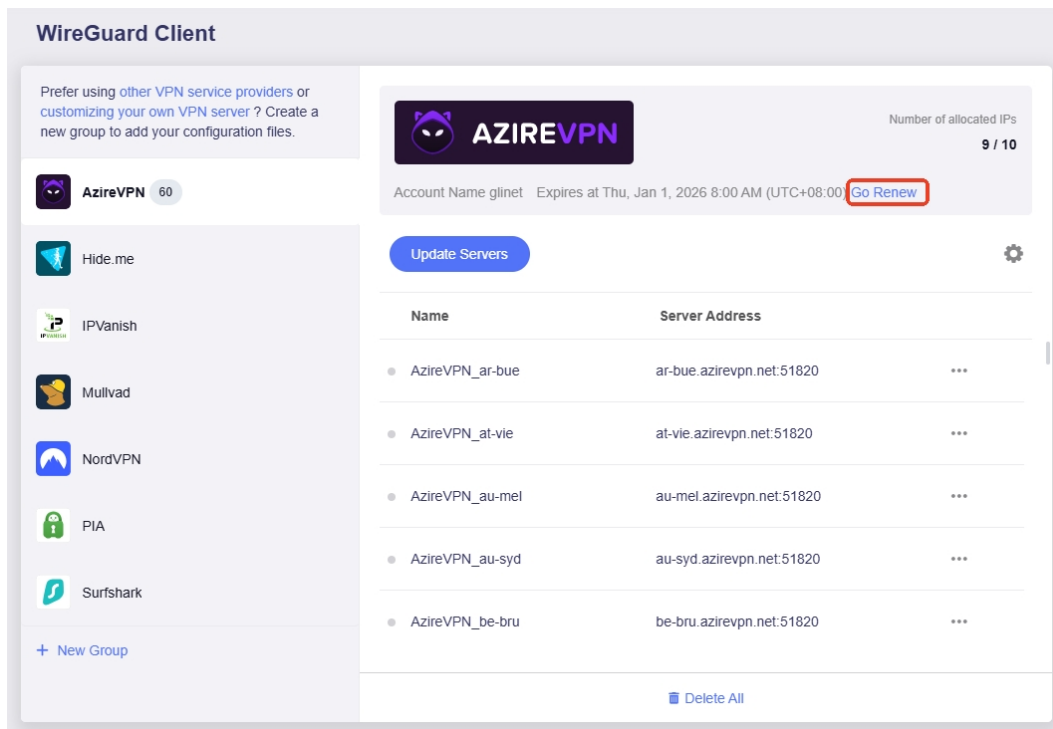
6. Edit credentials or logout.

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



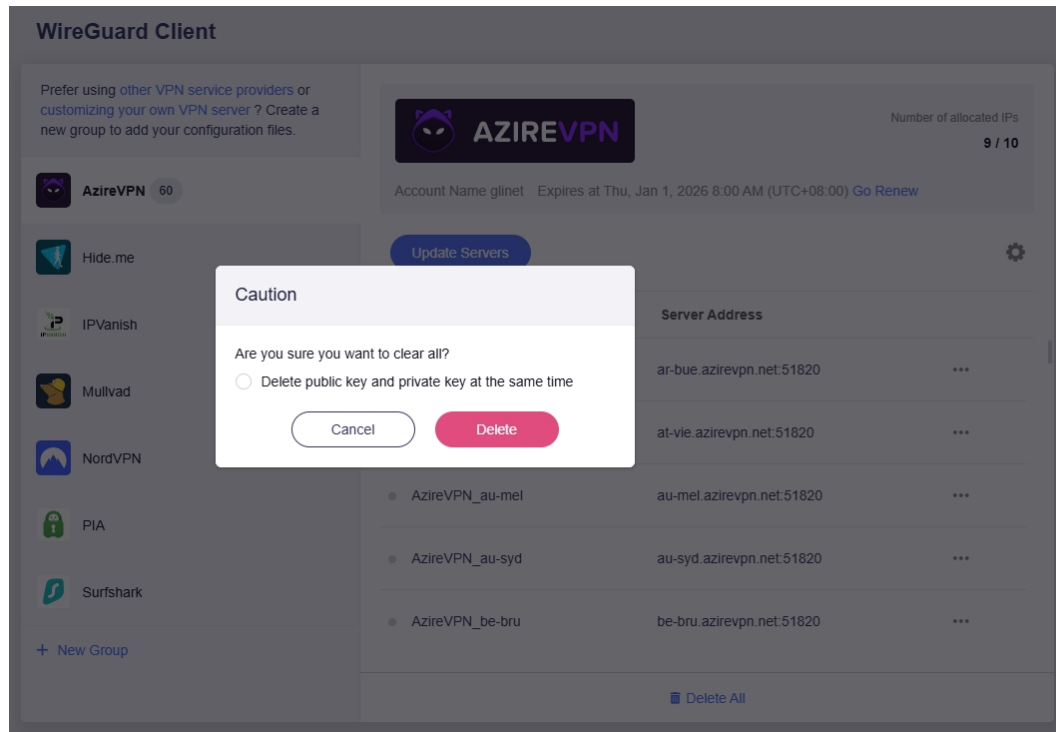
7. Go renew.

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



8. Delete all files.

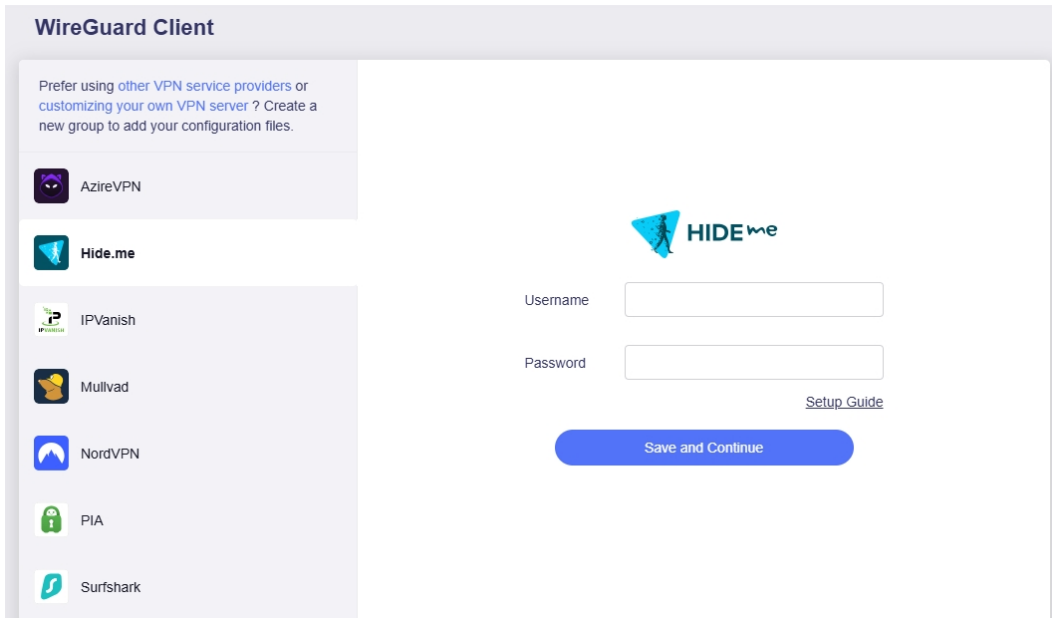
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.3 Set Up Hide.me

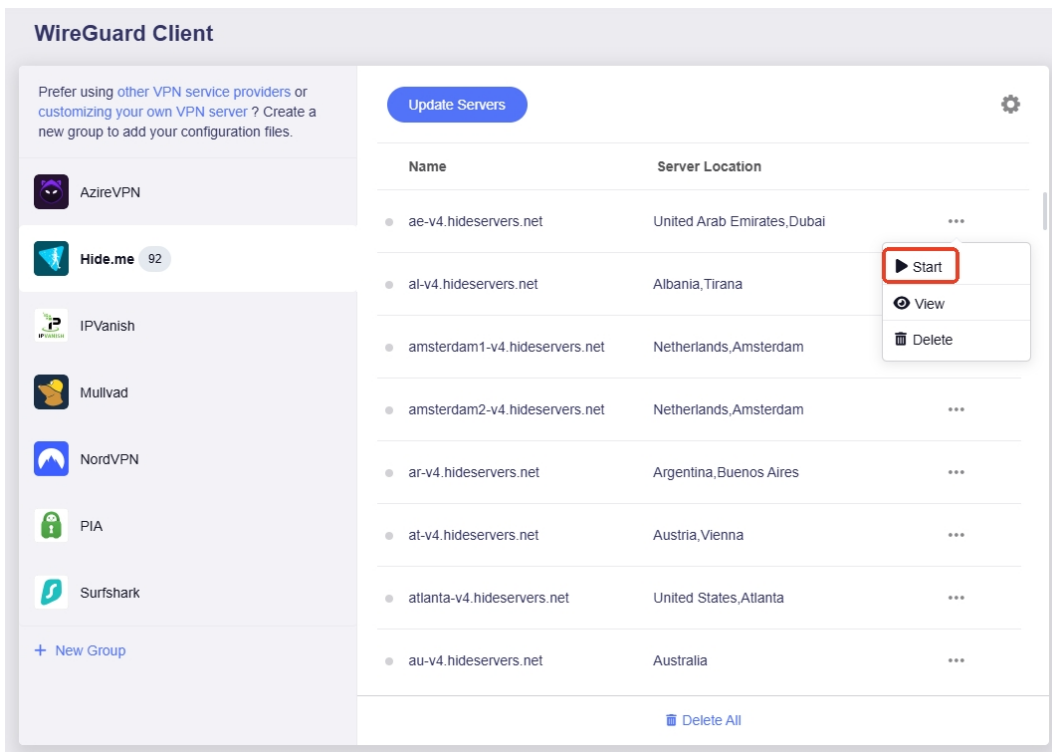
Follow the steps below to set your router as a Hide.me client.

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.



The screenshot shows the 'WireGuard Client' configuration page. On the left, a sidebar lists various VPN providers: AzureVPN, Hide.me (selected), IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The main area features the Hide.me logo, a 'Username' input field, a 'Password' input field, a 'Setup Guide' link, and a blue 'Save and Continue' button. A note at the top left suggests using other VPN service providers or customizing one's own server.

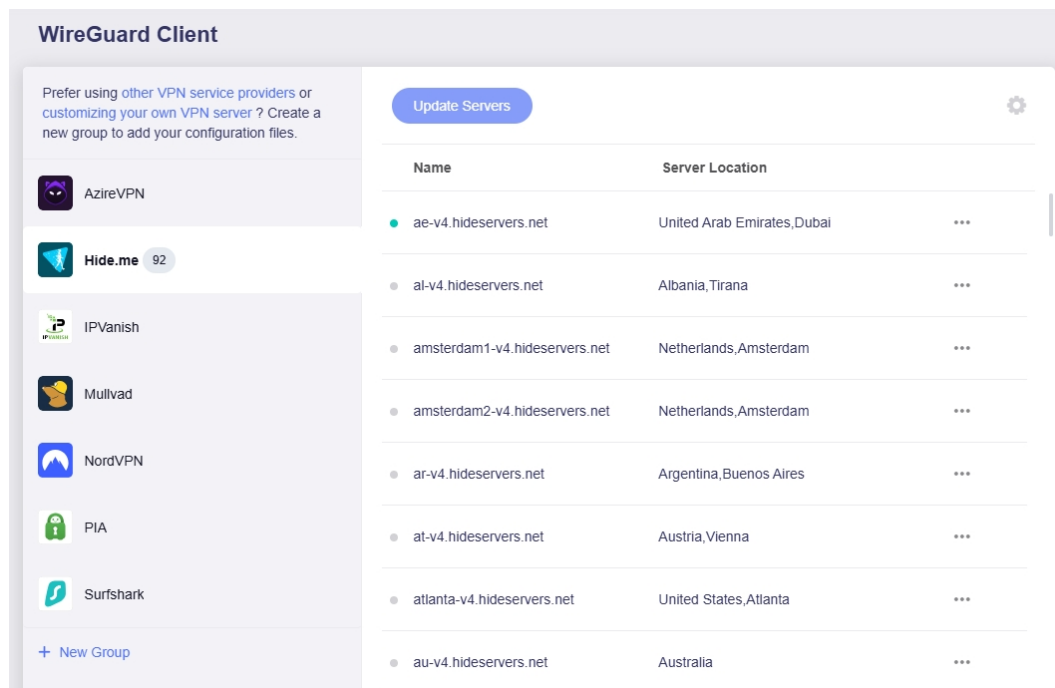
3. Select a preferred server, and click the three-dot icon on the right to start a connection.



The screenshot shows the 'WireGuard Client' server selection page. The left sidebar is identical to the previous screen, with 'Hide.me' selected. The main area has an 'Update Servers' button and a table of available servers. A context menu is open for the first server, showing 'Start', 'View', and 'Delete' options. The table lists servers with their names and locations.

Name	Server Location
ae-v4.hideservers.net	United Arab Emirates,Dubai
al-v4.hideservers.net	Albania,Tirana
amsterdam1-v4.hideservers.net	Netherlands,Amsterdam
amsterdam2-v4.hideservers.net	Netherlands,Amsterdam
ar-v4.hideservers.net	Argentina,Buenos Aires
at-v4.hideservers.net	Austria,Vienna
atlanta-v4.hideservers.net	United States,Atlanta
au-v4.hideservers.net	Australia

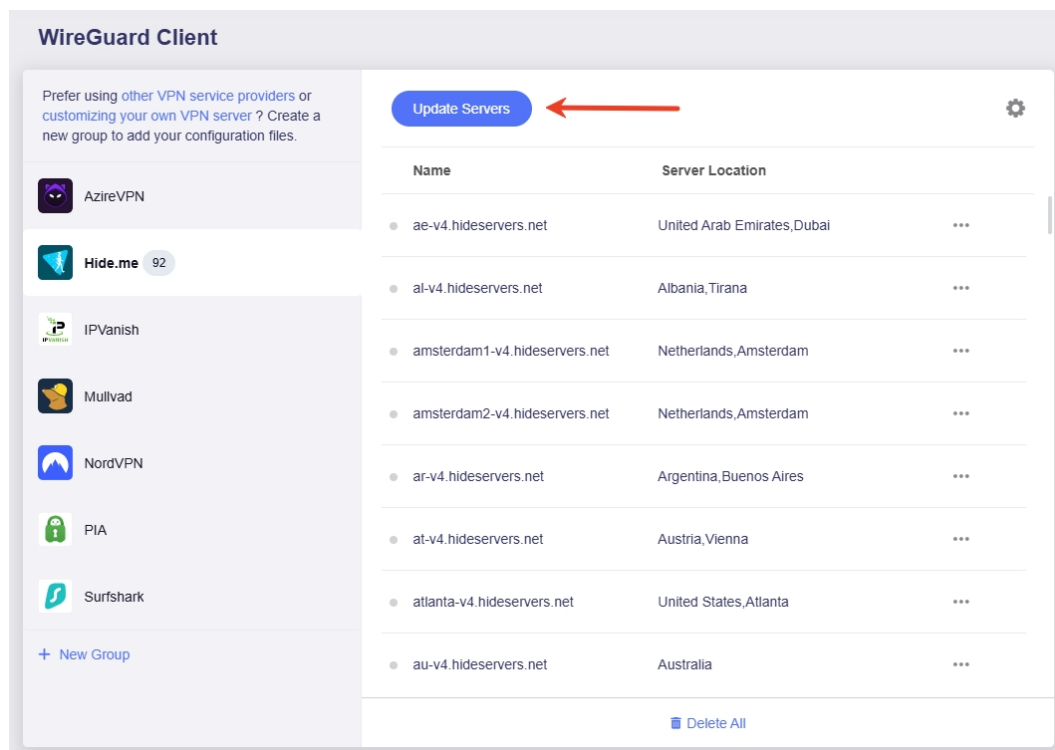
4. Once connected, a green dot will appear next to the configuration file.



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

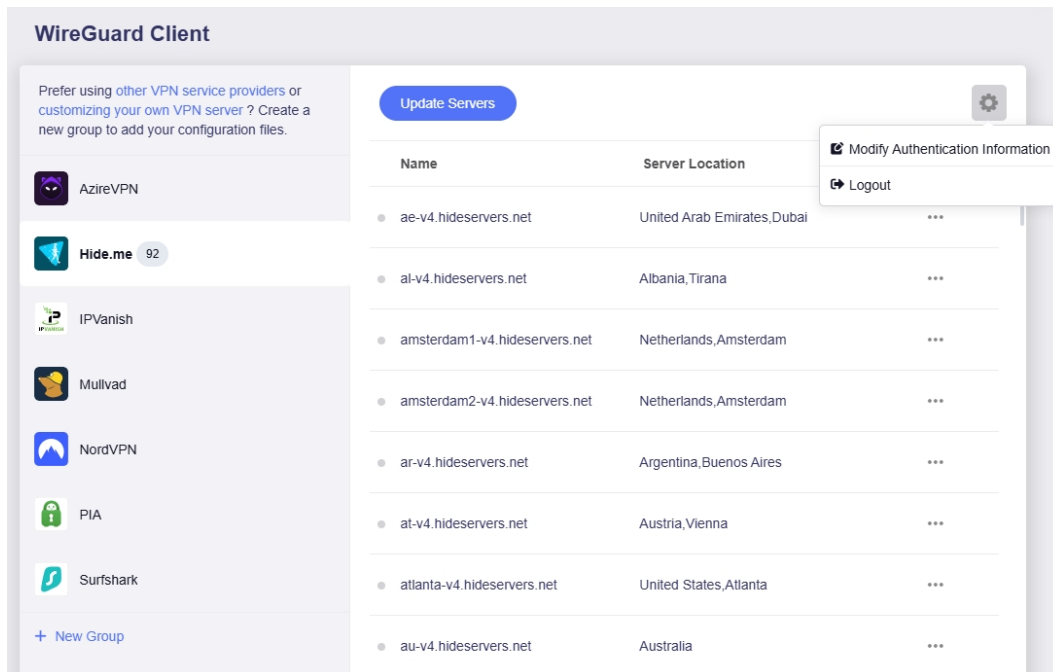
5. Update servers.

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



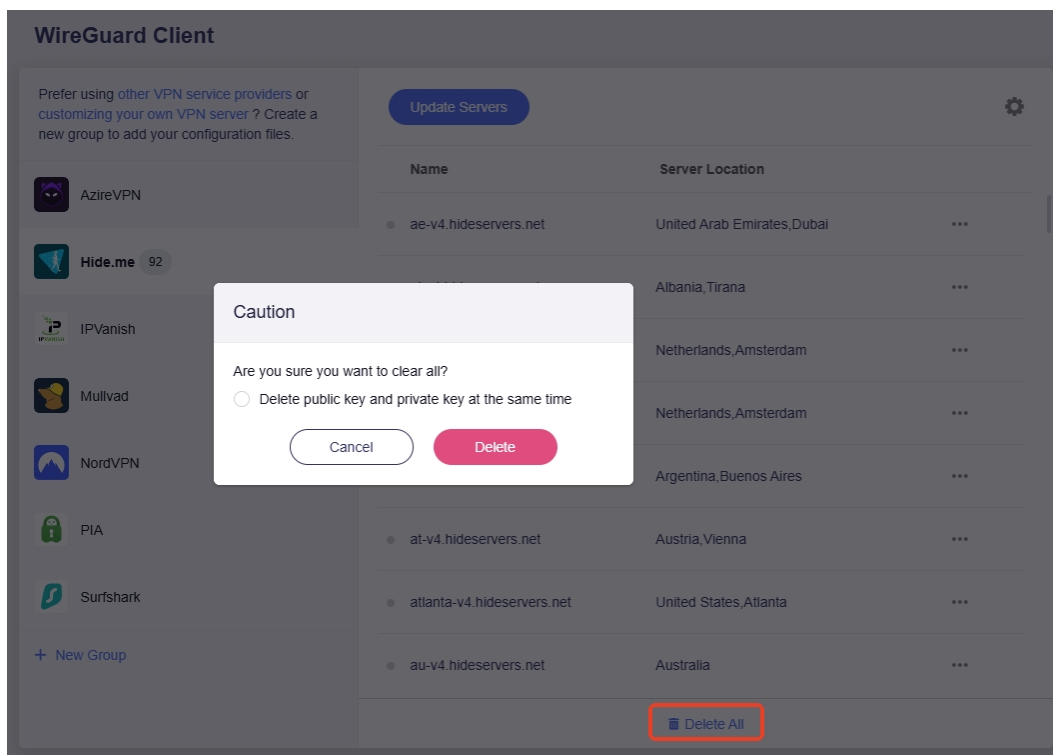
6. Edit credentials or logout.

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



7. Delete all files.

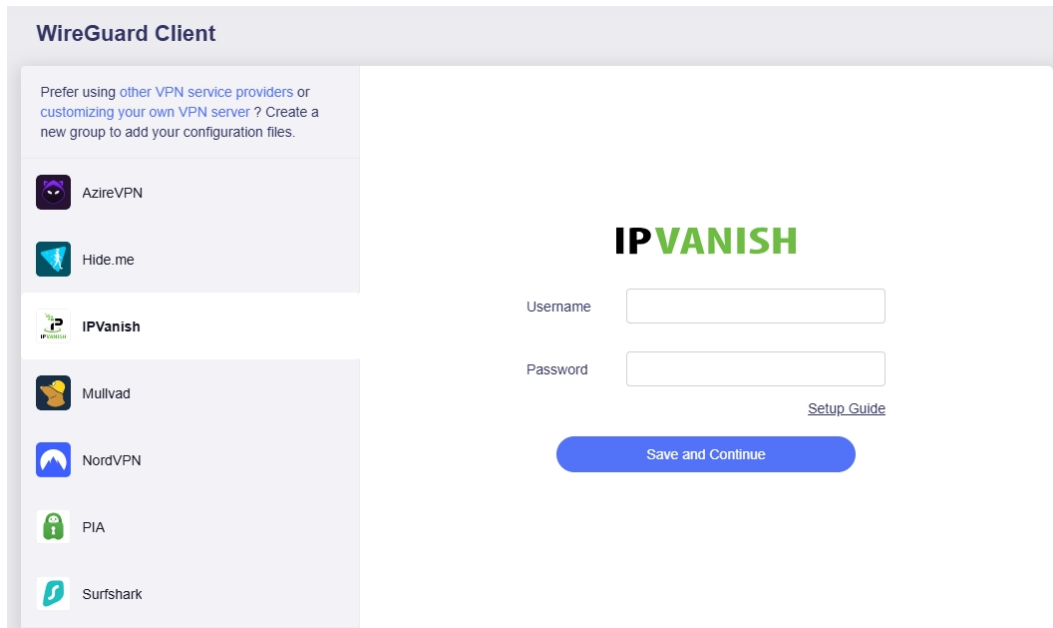
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.4 Set Up IPVanish

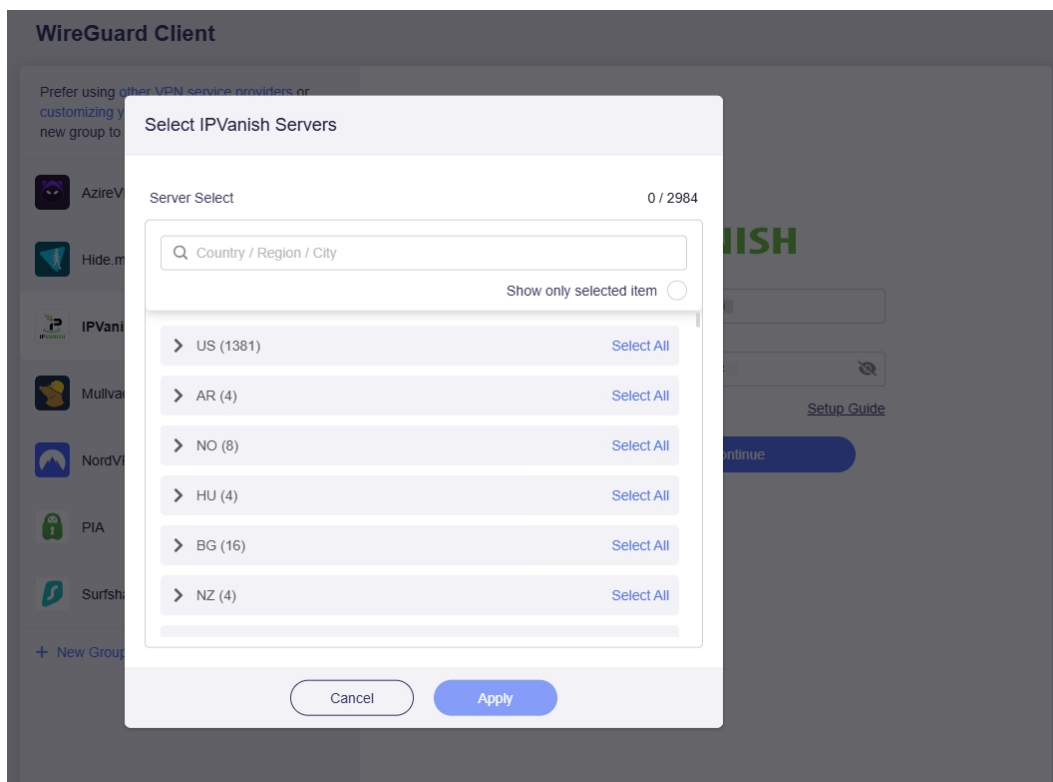
Follow the steps below to set your router as an IPVanish client.

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**.



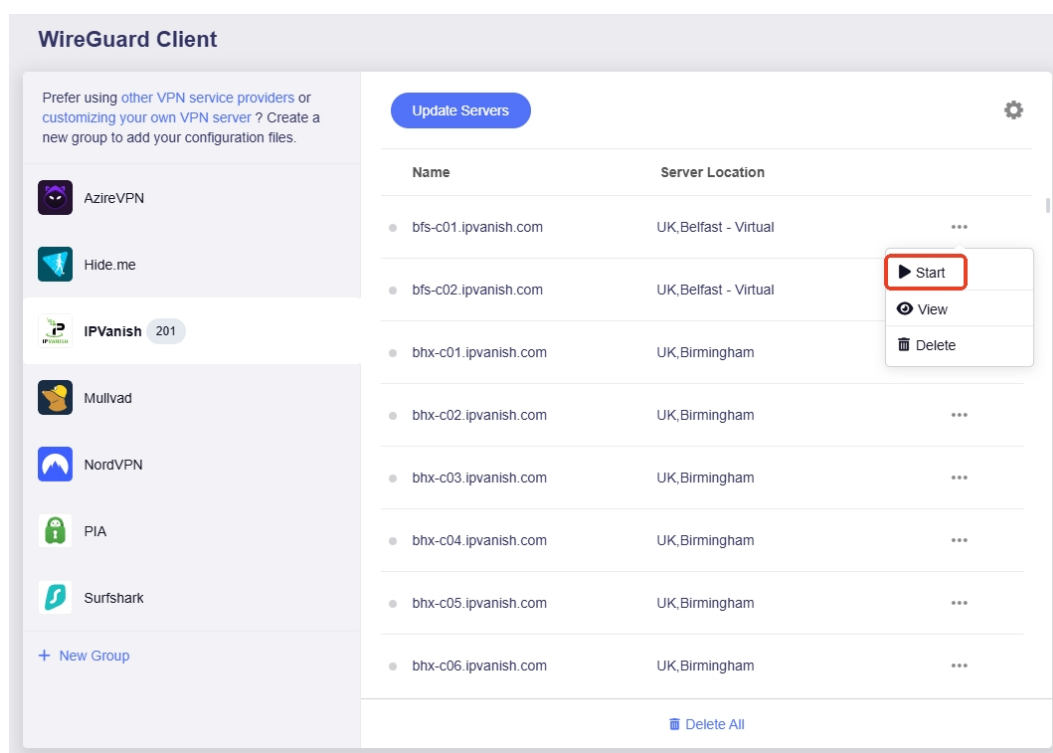
The screenshot shows the 'WireGuard Client' configuration page. On the left, there is a list of VPN providers: AzireVPN, Hide.me, IPVanish (highlighted), Mullvad, NordVPN, PIA, and Surfshark. On the right, the 'IPVANISH' logo is displayed above two input fields for 'Username' and 'Password'. Below these fields is a 'Setup Guide' link and a blue 'Save and Continue' button.

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

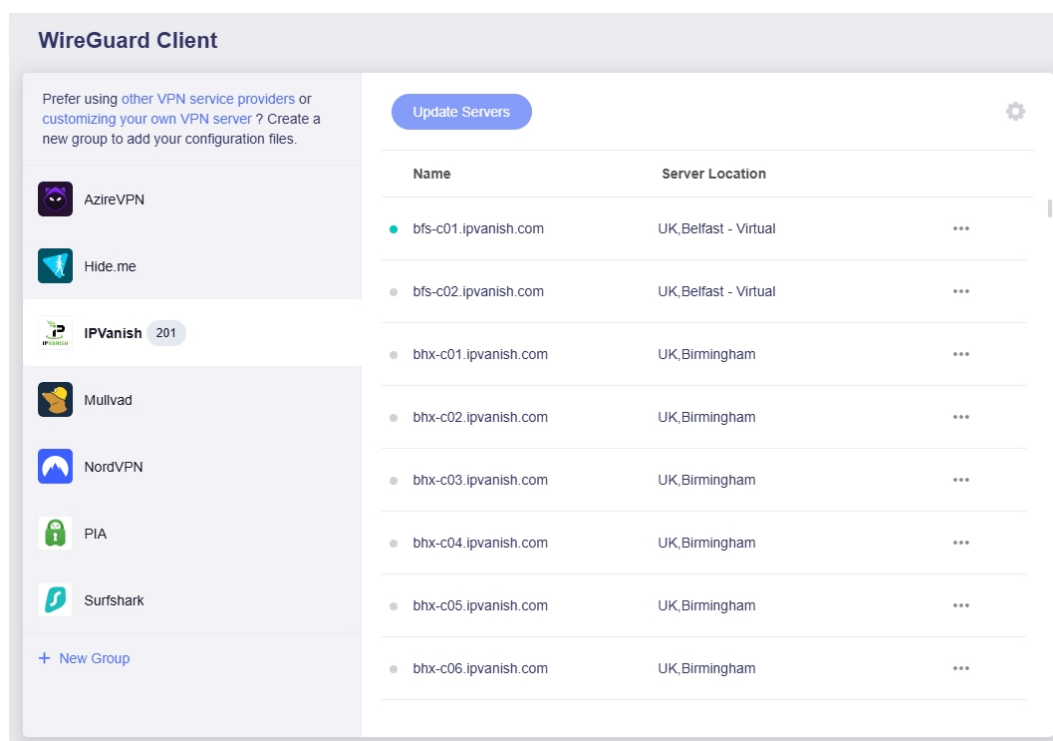


This screenshot shows the same 'WireGuard Client' setup page as before, but with a modal window open for selecting IPVanish servers. The modal is titled 'Select IPVanish Servers' and shows a 'Server Select' list with 0 / 2984 servers. The list includes search filters for 'Country / Region / City' and a 'Show only selected item' toggle. The list contains several entries with expandable arrows and 'Select All' links: US (1381), AR (4), NO (8), HU (4), BG (16), and NZ (4). At the bottom of the modal are 'Cancel' and 'Apply' buttons.

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



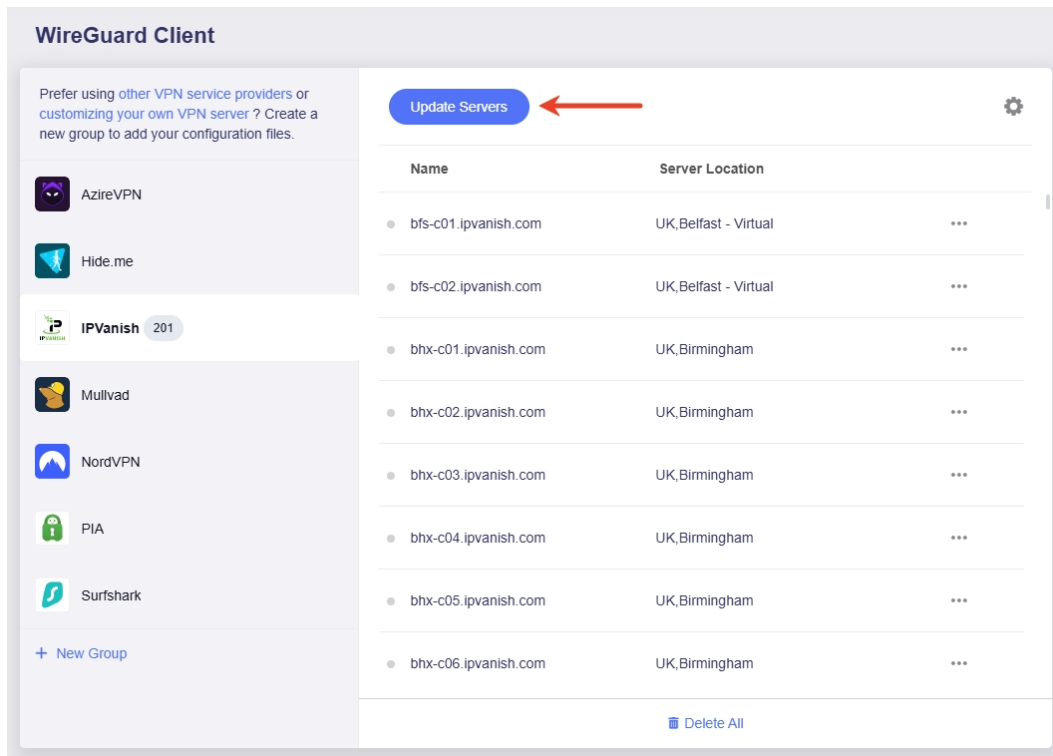
5. Once connected, a green dot will appear next to the configuration file.



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

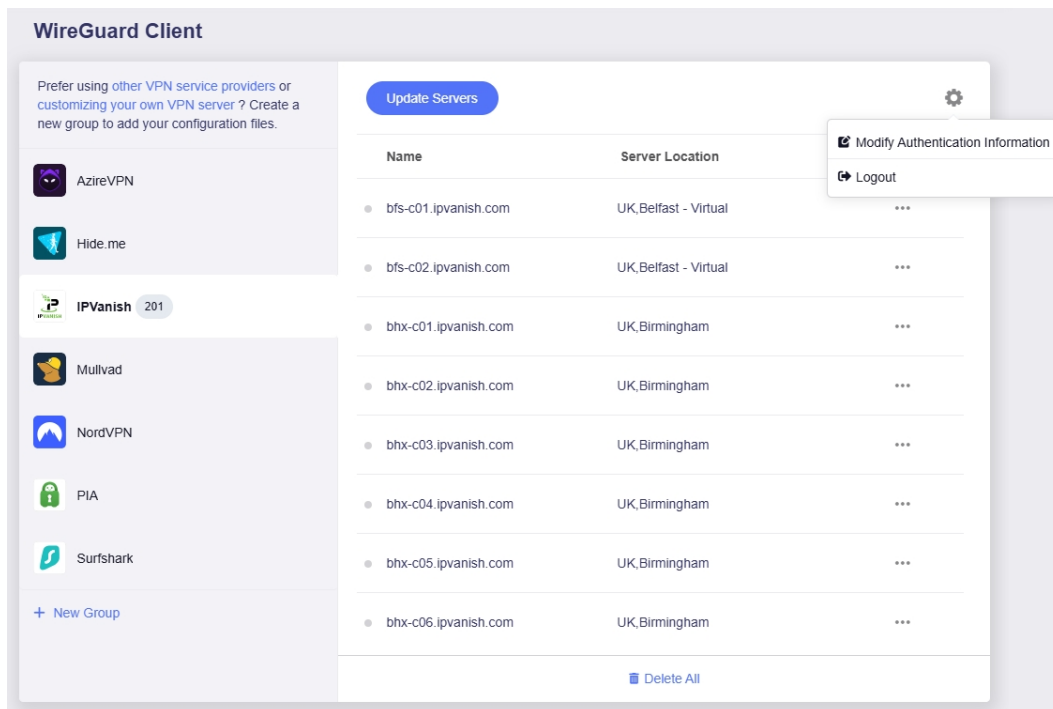
6. Update servers.

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



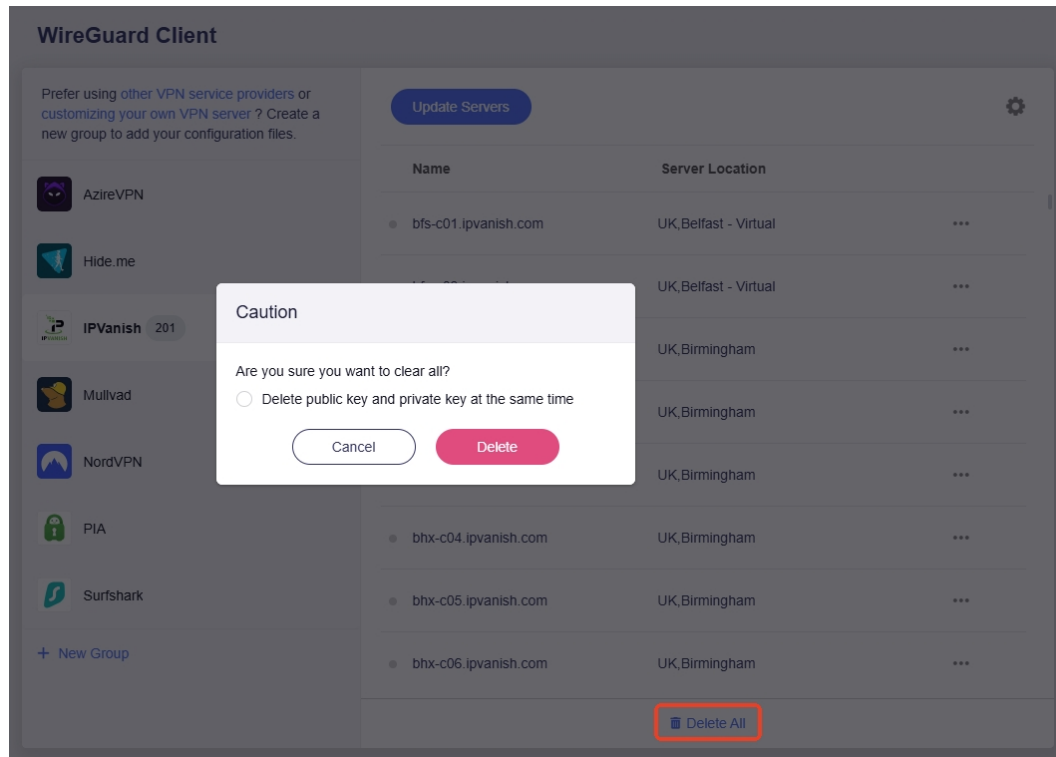
7. Edit credentials or logout.

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



8. Delete all files.

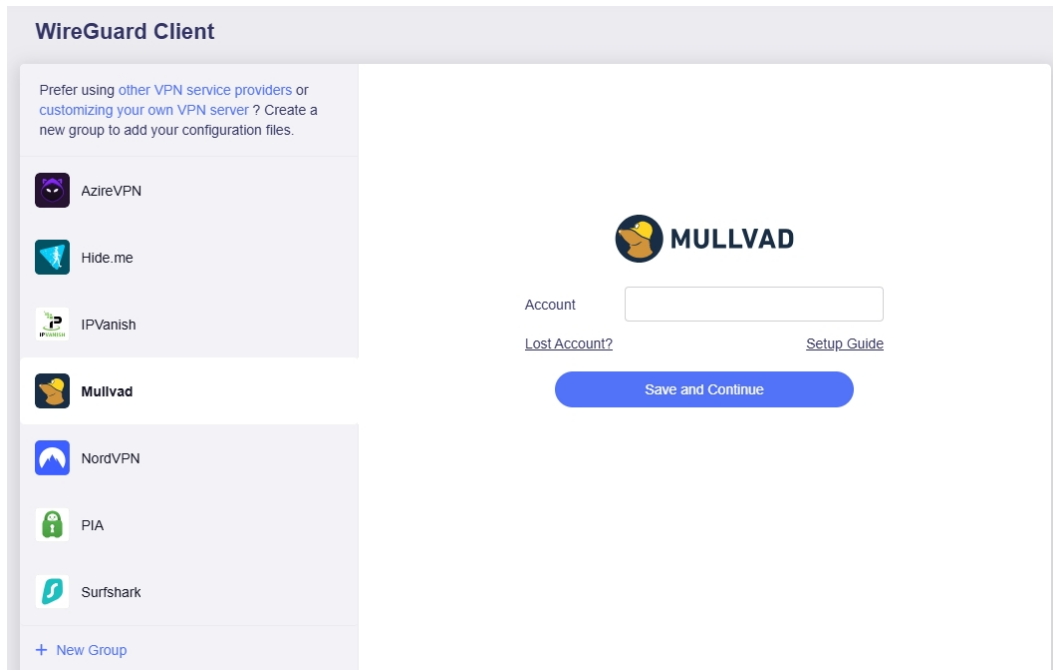
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



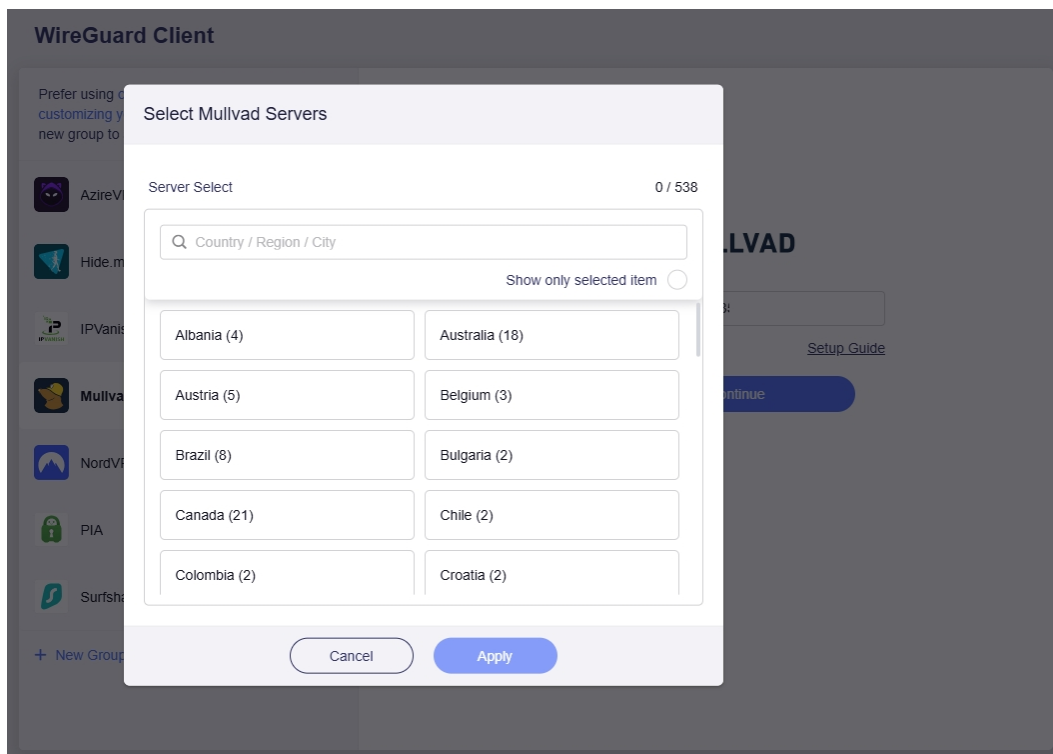
10.2.5 Set Up Mullvad

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

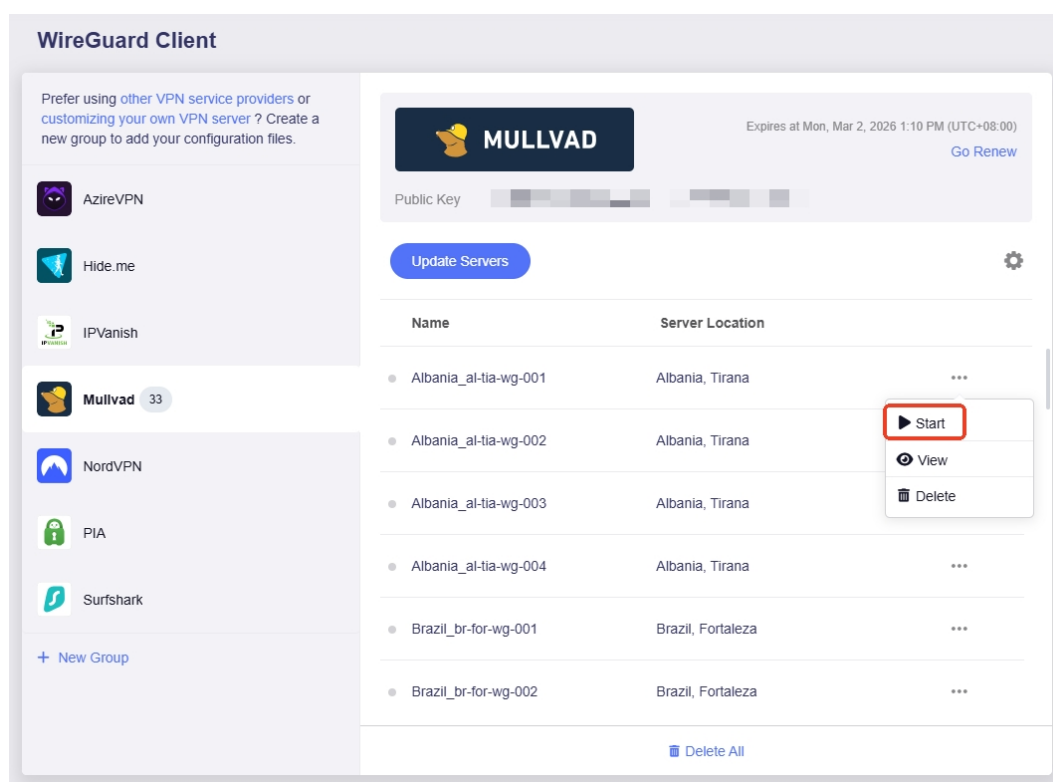
1. Log in to your router's web admin panel and go to **VPN > WireGuard Client > Mullvad**.
2. Input Username and Password, then click **Save and Continue**.



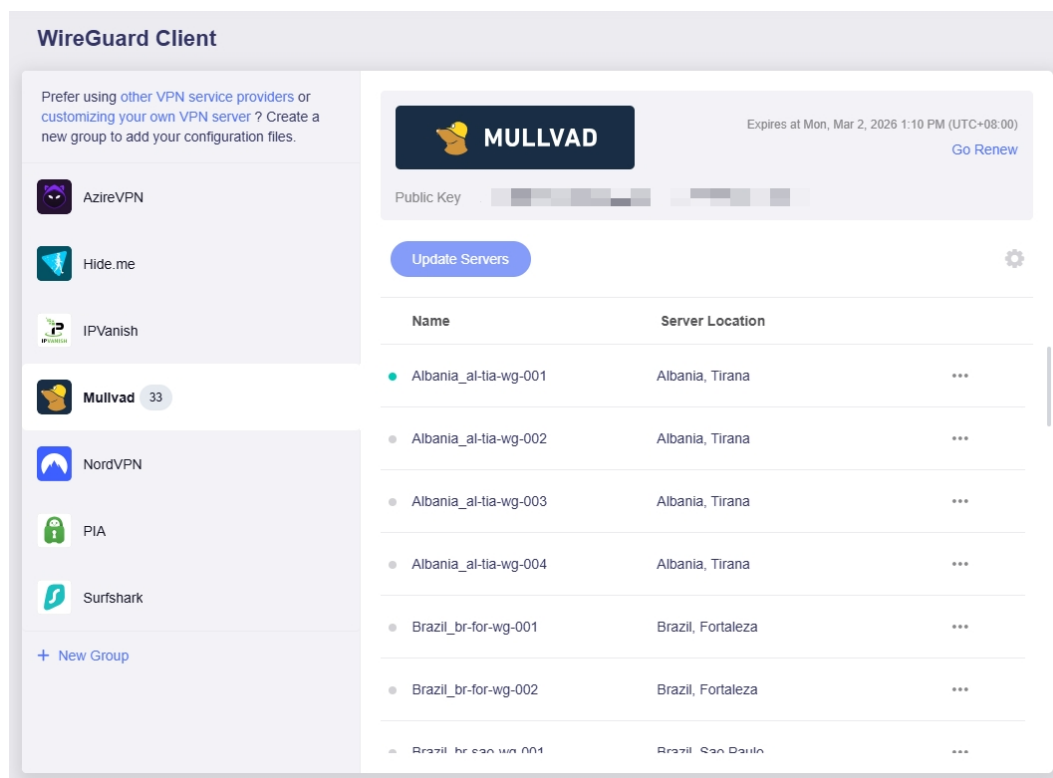
3. Select the server(s) you want to connect to, and click **Apply**.



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



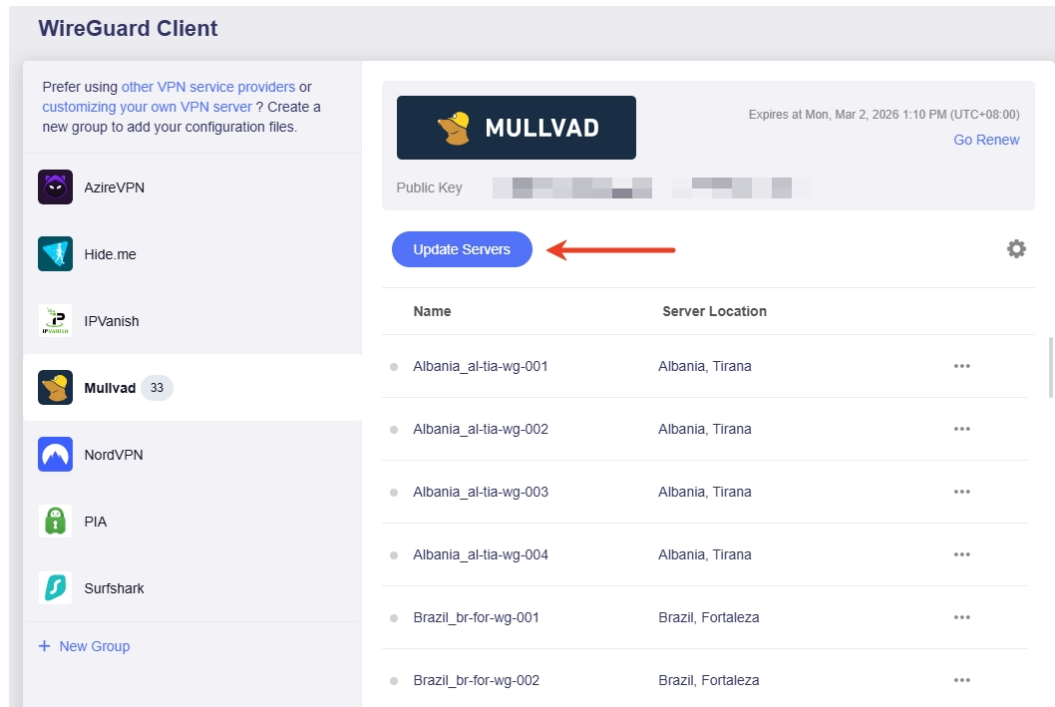
5. Once connected, a green dot will appear next to the configuration file.



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

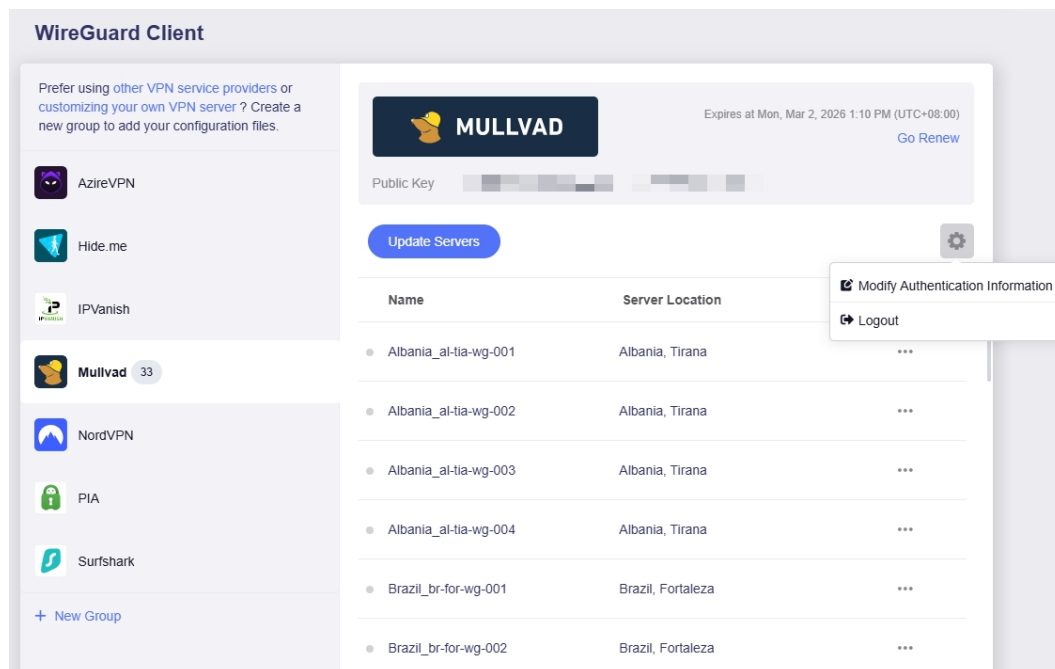
6. Update servers.

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



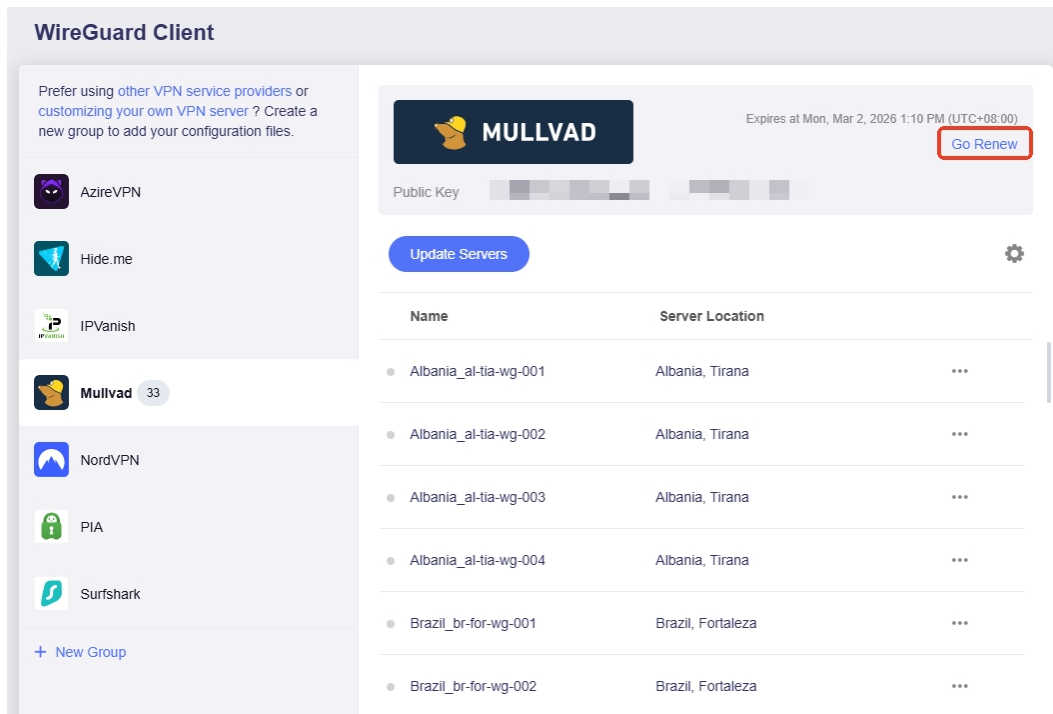
7. Edit credentials or logout.

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



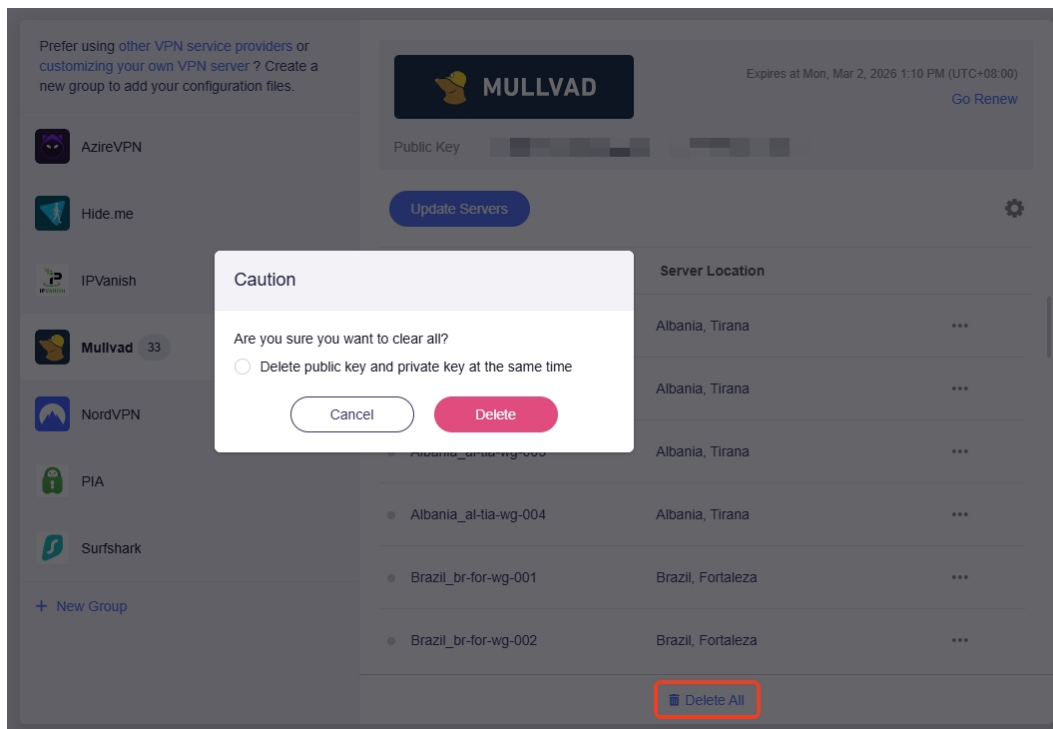
8. Go renew.

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



9. Delete all files.

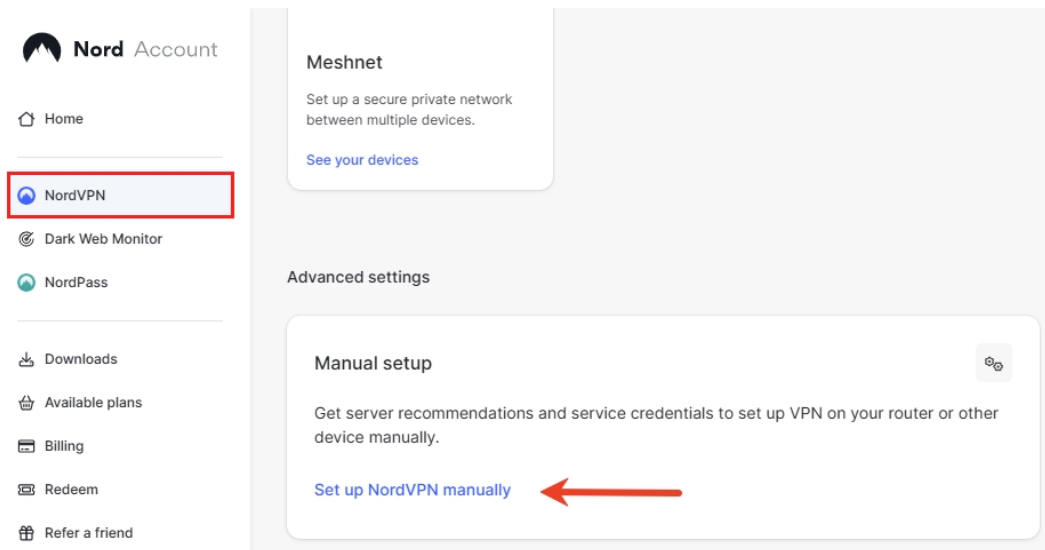
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



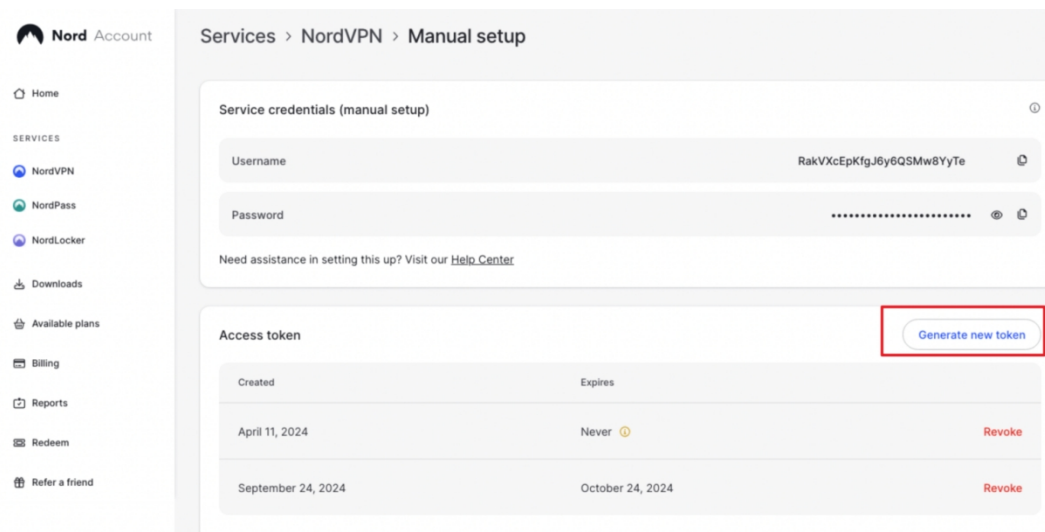
10.2.6 Set Up NordVPN

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

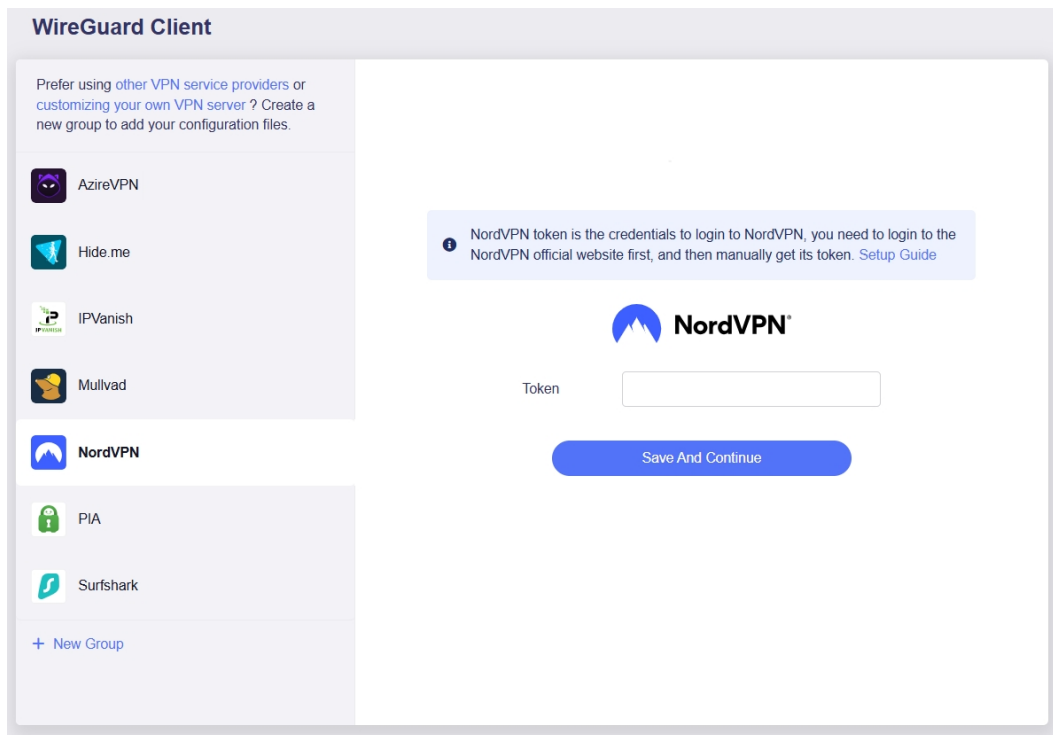
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



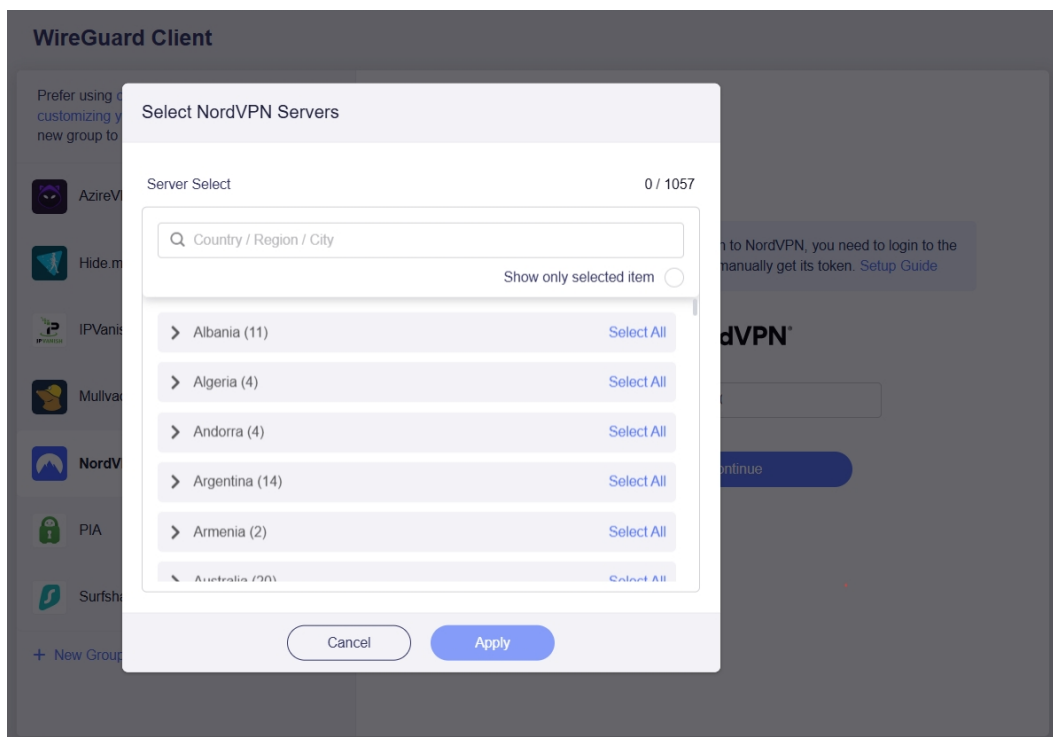
You will find the **Access Token**. Create an access token and copy for later use.



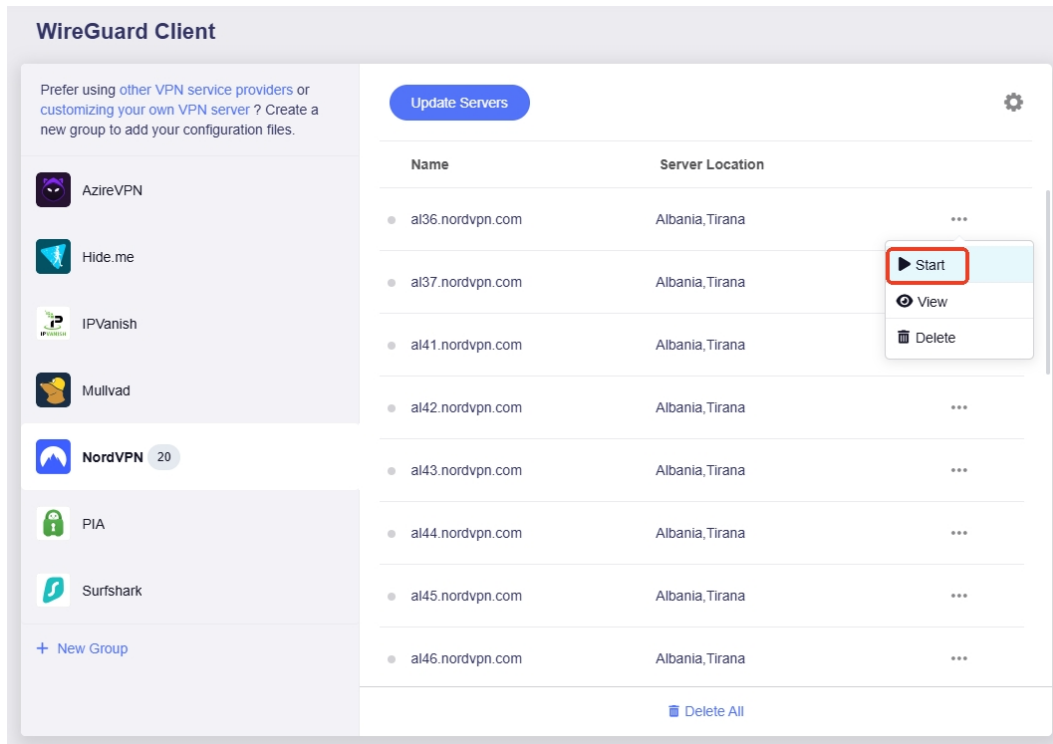
3. Log in to your router's web admin panel and go to **VPN > WireGuard Client > NordVPN**.
4. Input token, and click **Save and Continue**.



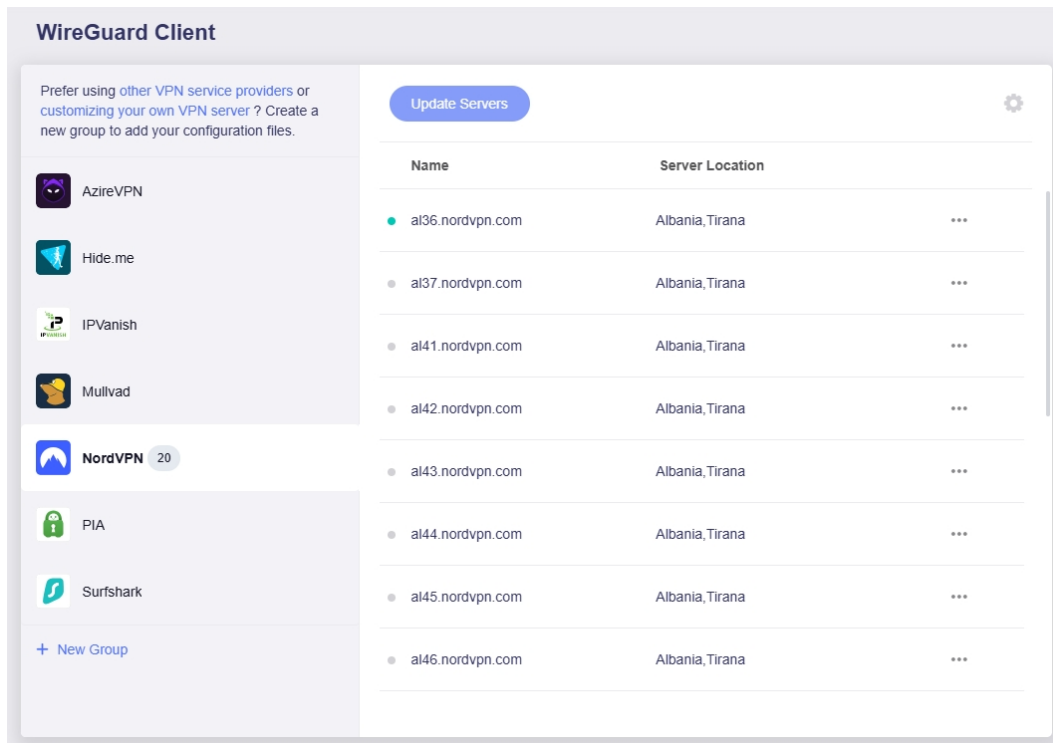
5. Select the server(s) you want to connect to, and click **Apply**.



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



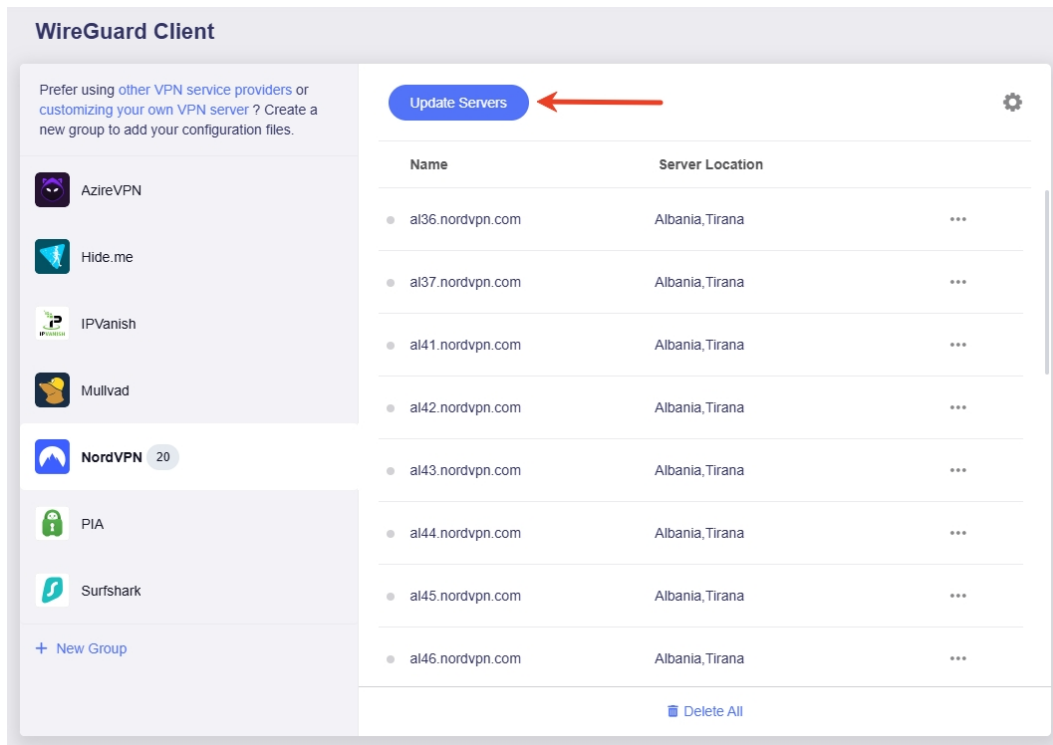
7. Once connected, a green dot will appear next to the configuration file.



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

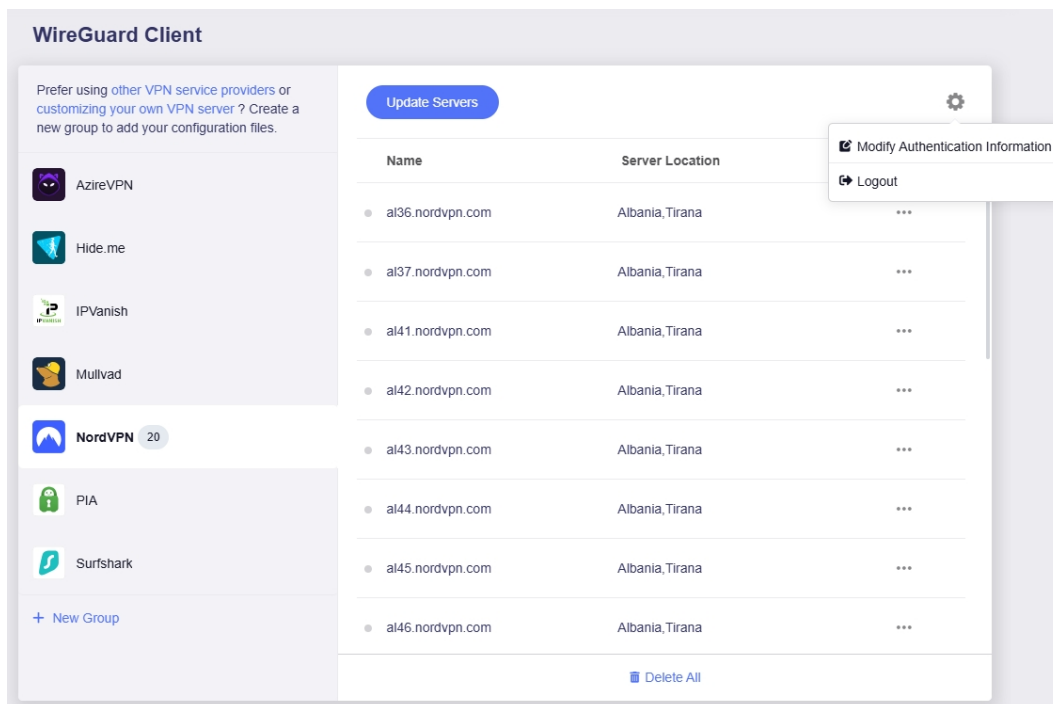
8. Update servers.

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



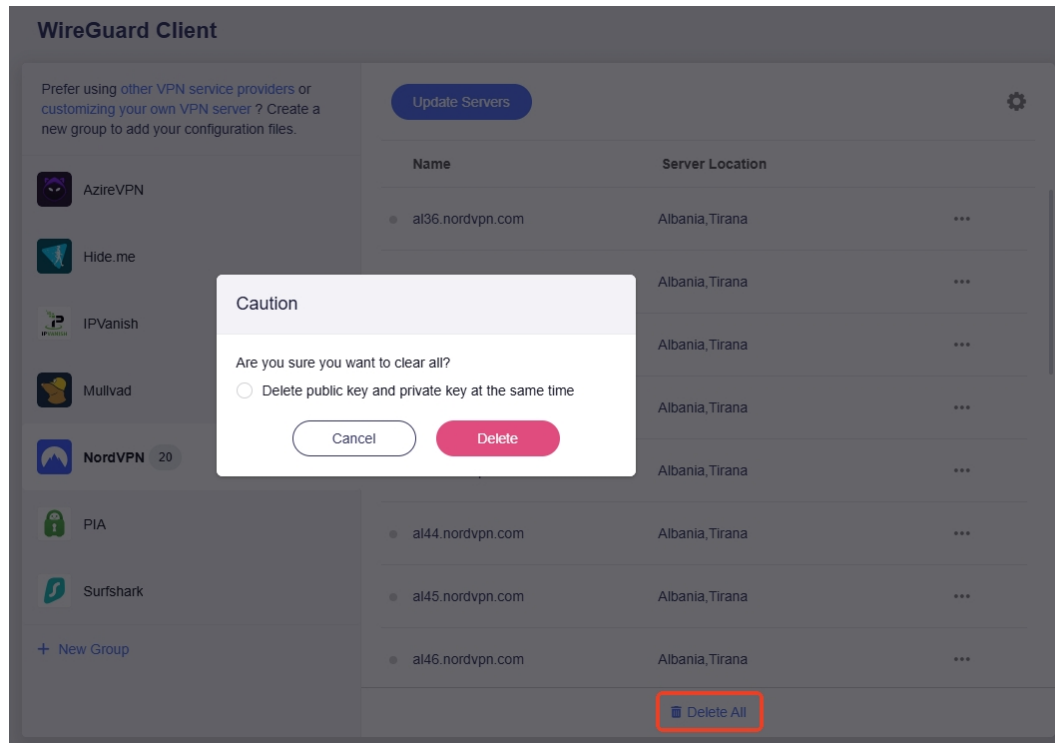
9. Edit credentials or logout.

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



10. Delete all files.

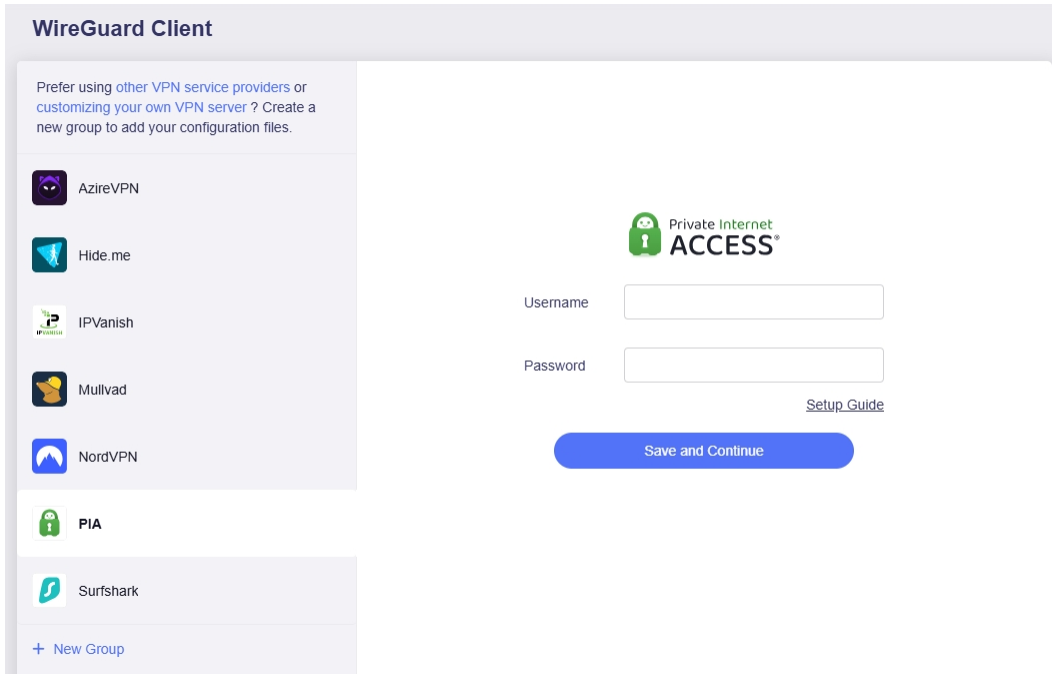
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.7 Set Up PIA (Private Internet Access)

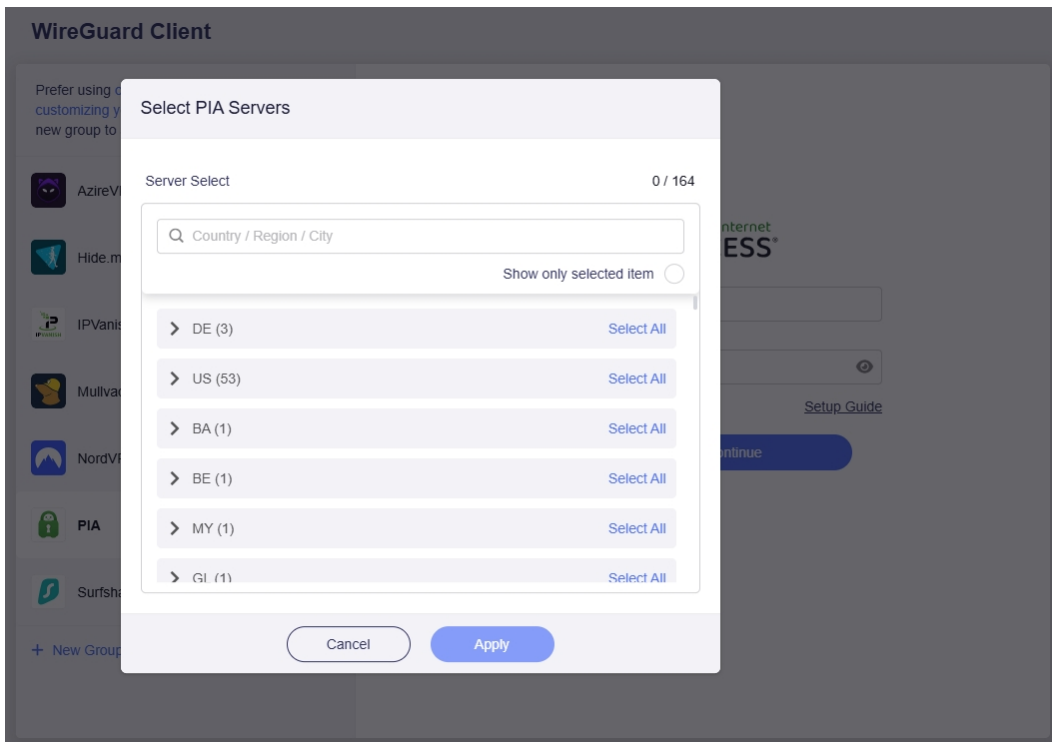
Follow the steps below to set your router as a PIA client.

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**.



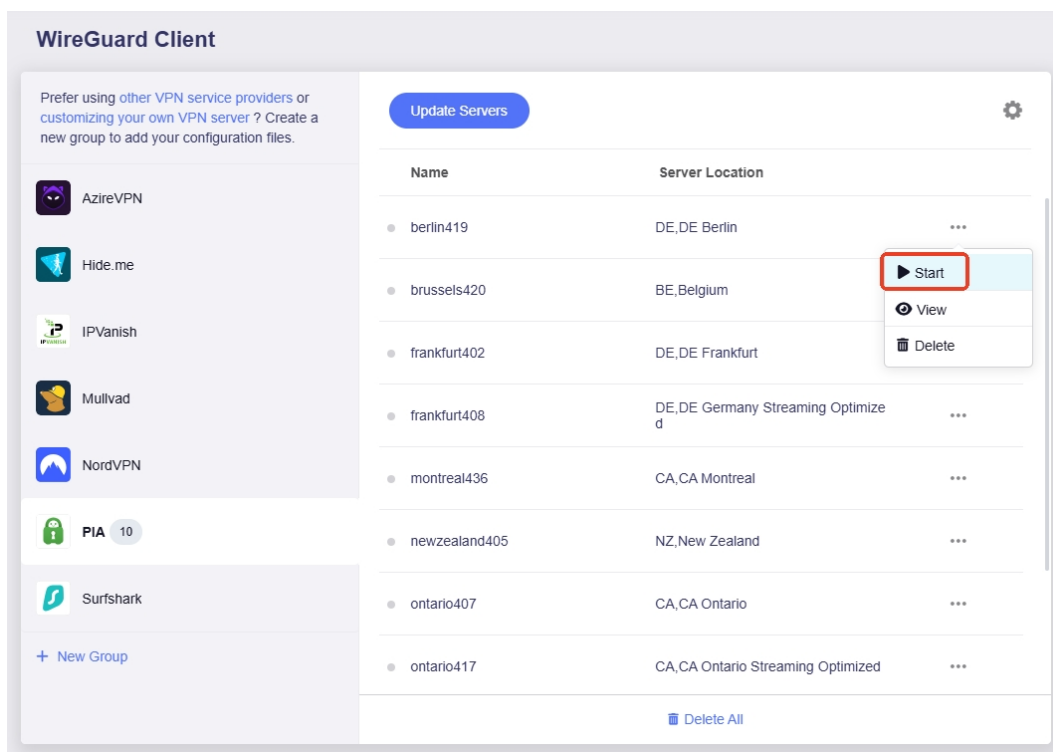
The screenshot shows the 'WireGuard Client' configuration page. On the left, there is a list of VPN providers: AzureVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA (highlighted), and Surfshark, with a '+ New Group' option at the bottom. The main area on the right is for PIA configuration, featuring the PIA logo, 'Username' and 'Password' input fields, a 'Setup Guide' link, and a blue 'Save and Continue' button.

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

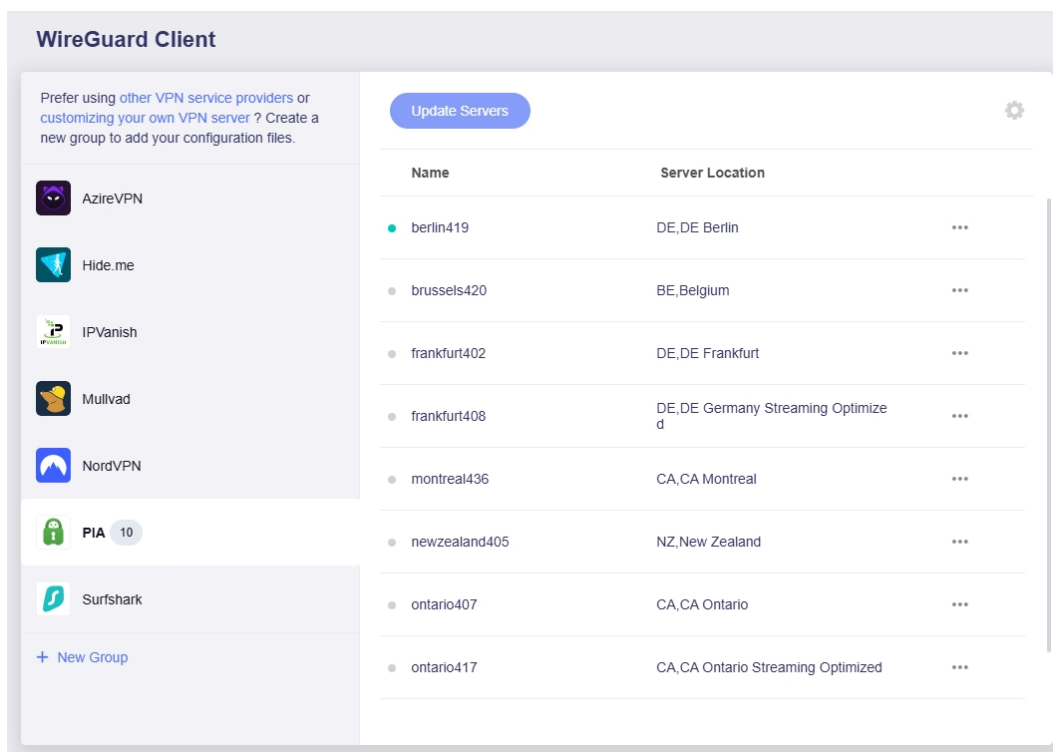


The screenshot shows the 'WireGuard Client' page with a 'Select PIA Servers' modal dialog open. The dialog has a search bar labeled 'Country / Region / City' and a 'Show only selected item' toggle. Below the search bar is a list of regions with their respective server counts and a 'Select All' link for each: DE (3), US (53), BA (1), BE (1), MY (1), and GL (1). At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

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



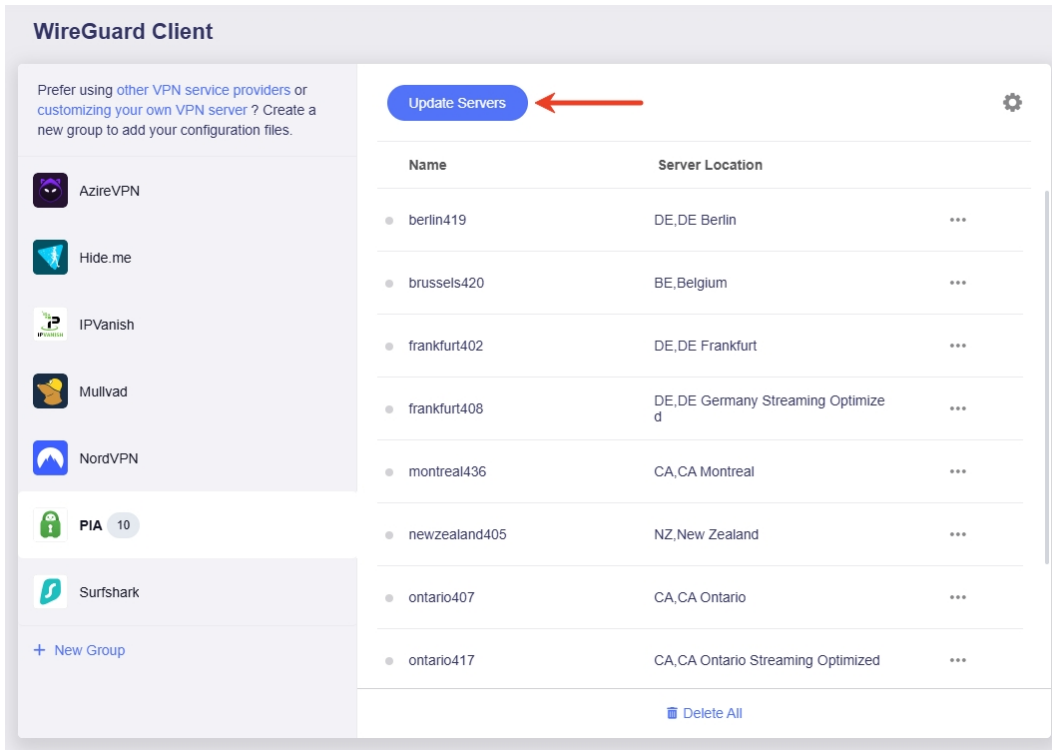
5. Once connected, a green dot will appear next to the configuration file.



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.

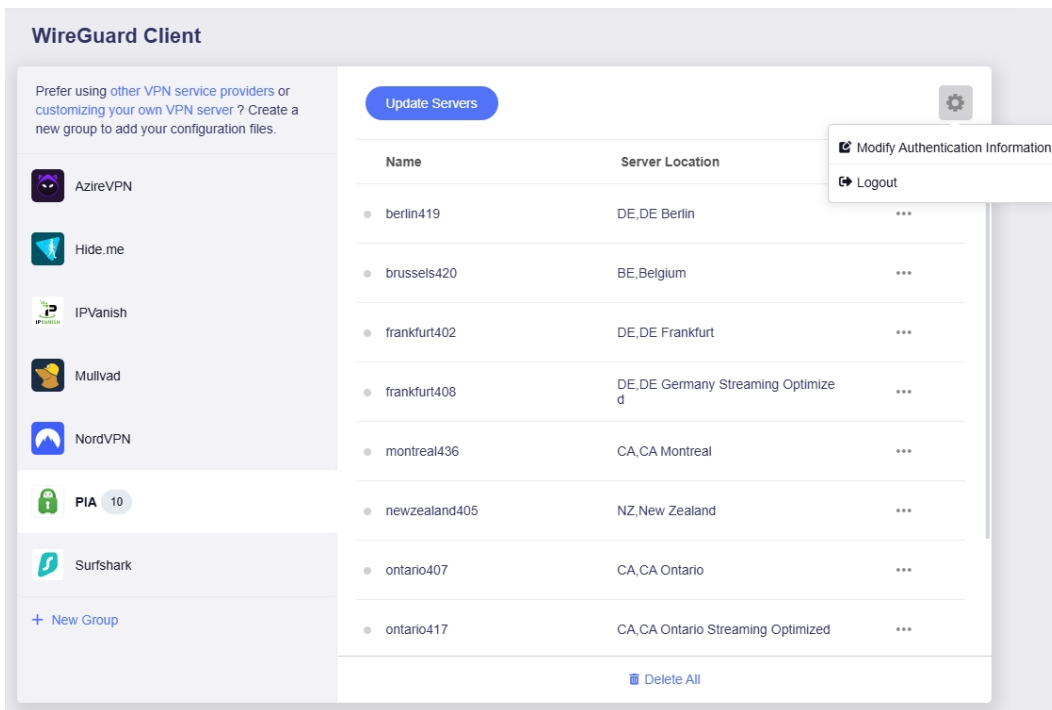


The screenshot shows the WireGuard Client interface. On the left, there's a sidebar with various VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA (with a '10' badge), and Surfshark. Below these is a '+ New Group' button. The main area has a header with a blue 'Update Servers' button, which is pointed to by a red arrow. Below the button is a table of servers. At the bottom right of the table is a 'Delete All' button.

Name	Server Location	
berlin419	DE,DE Berlin	...
brussels420	BE,Belgium	...
frankfurt402	DE,DE Frankfurt	...
frankfurt408	DE,DE Germany Streaming Optimized	...
montreal436	CA,CA Montreal	...
newzealand405	NZ,New Zealand	...
ontario407	CA,CA Ontario	...
ontario417	CA,CA Ontario Streaming Optimized	...

7. Edit credentials or logout.

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

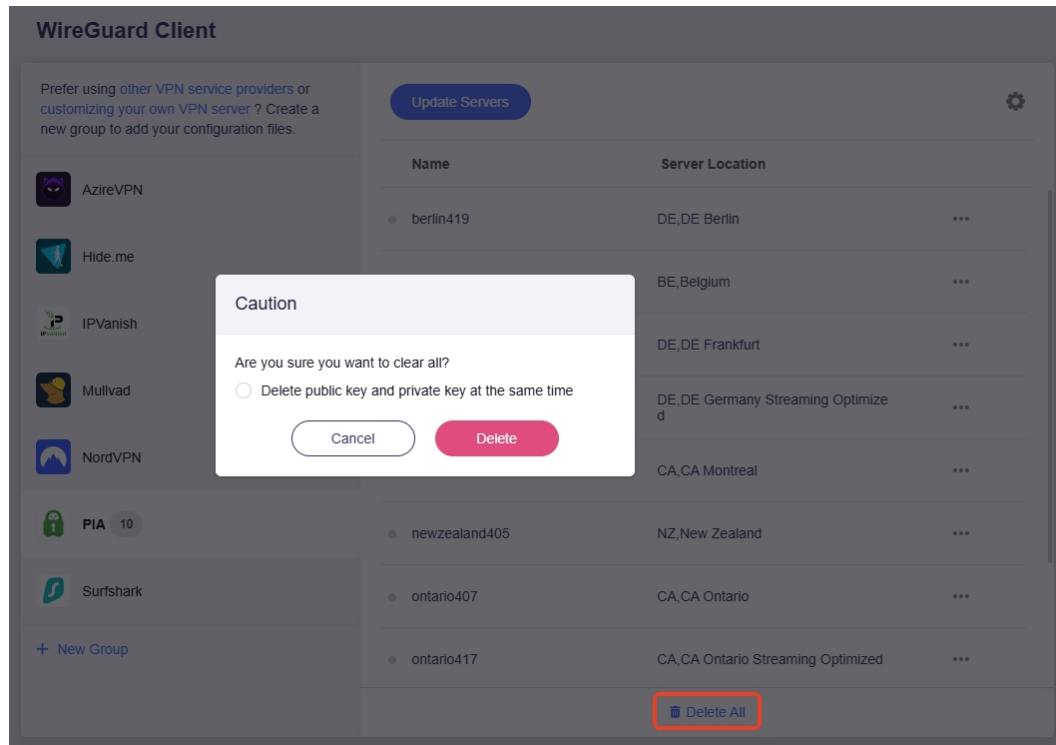


This screenshot shows the same WireGuard Client interface as the previous one, but with the settings menu open. The menu is accessed via a gear icon in the top right corner of the main area. It contains two options: 'Modify Authentication Information' and 'Logout'. The 'Update Servers' button and the server table are still visible in the background.

Name	Server Location	
berlin419	DE,DE Berlin	...
brussels420	BE,Belgium	...
frankfurt402	DE,DE Frankfurt	...
frankfurt408	DE,DE Germany Streaming Optimized	...
montreal436	CA,CA Montreal	...
newzealand405	NZ,New Zealand	...
ontario407	CA,CA Ontario	...
ontario417	CA,CA Ontario Streaming Optimized	...

8. Delete all files.

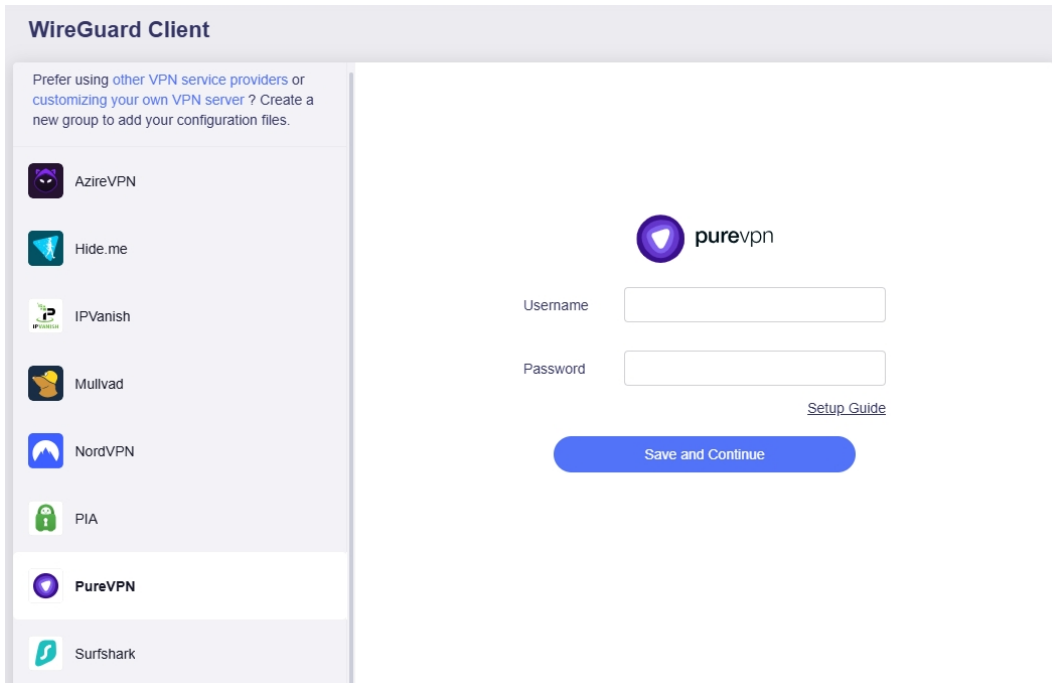
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.8 Set Up PureVPN

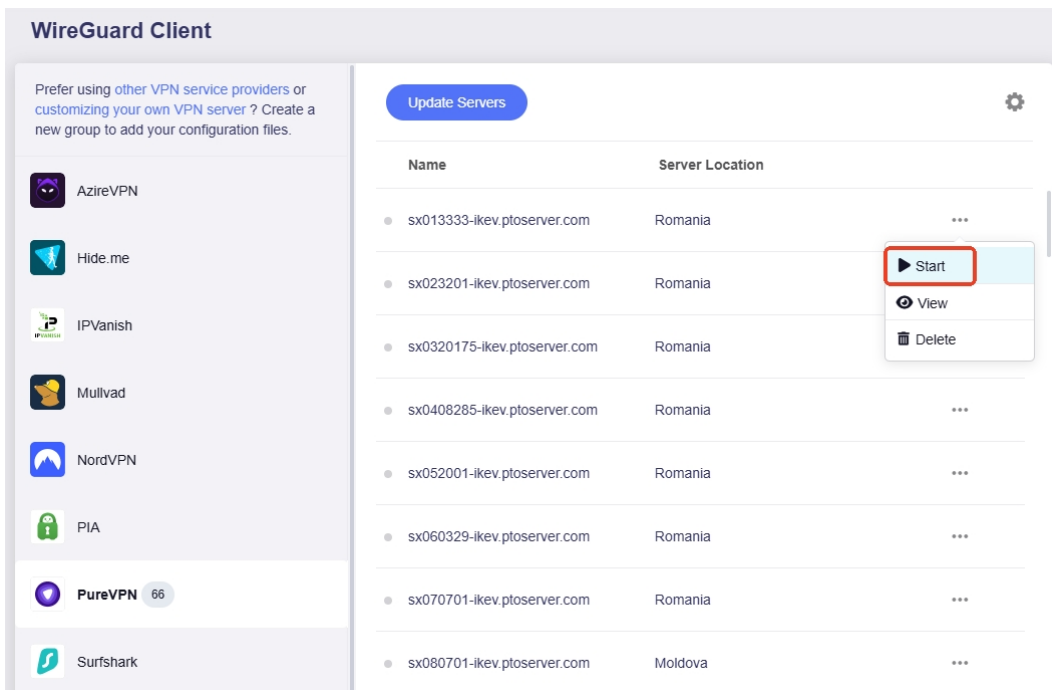
Follow the steps below to set your router as a PureVPN client.

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



The screenshot shows the 'WireGuard Client' configuration page. On the left, a sidebar lists various VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA, PureVPN (selected), and Surfshark. The main area features the PureVPN logo, input fields for 'Username' and 'Password', a 'Setup Guide' link, and a blue 'Save and Continue' button. A note at the top left suggests using other VPN providers or customizing a server.

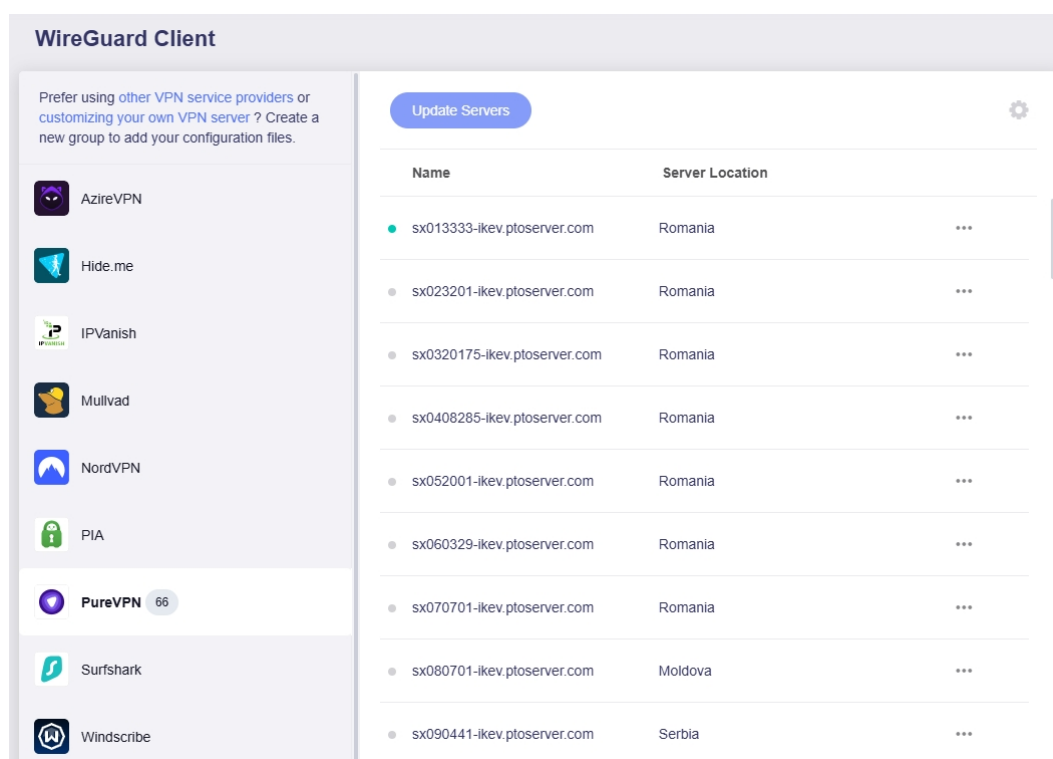
3. Select your preferred server, and click the three-dot icon on the right to start a connection.



The screenshot shows the 'WireGuard Client' server selection page. The left sidebar is identical to the previous screen, with 'PureVPN' selected. The main area has an 'Update Servers' button and a table of available servers. A context menu is open for the first server, showing 'Start', 'View', and 'Delete' options.

Name	Server Location	
● sx013333-ikev.ptoserver.com	Romania	...
● sx023201-ikev.ptoserver.com	Romania	...
● sx0320175-ikev.ptoserver.com	Romania	...
● sx0408285-ikev.ptoserver.com	Romania	...
● sx052001-ikev.ptoserver.com	Romania	...
● sx060329-ikev.ptoserver.com	Romania	...
● sx070701-ikev.ptoserver.com	Romania	...
● sx080701-ikev.ptoserver.com	Moldova	...

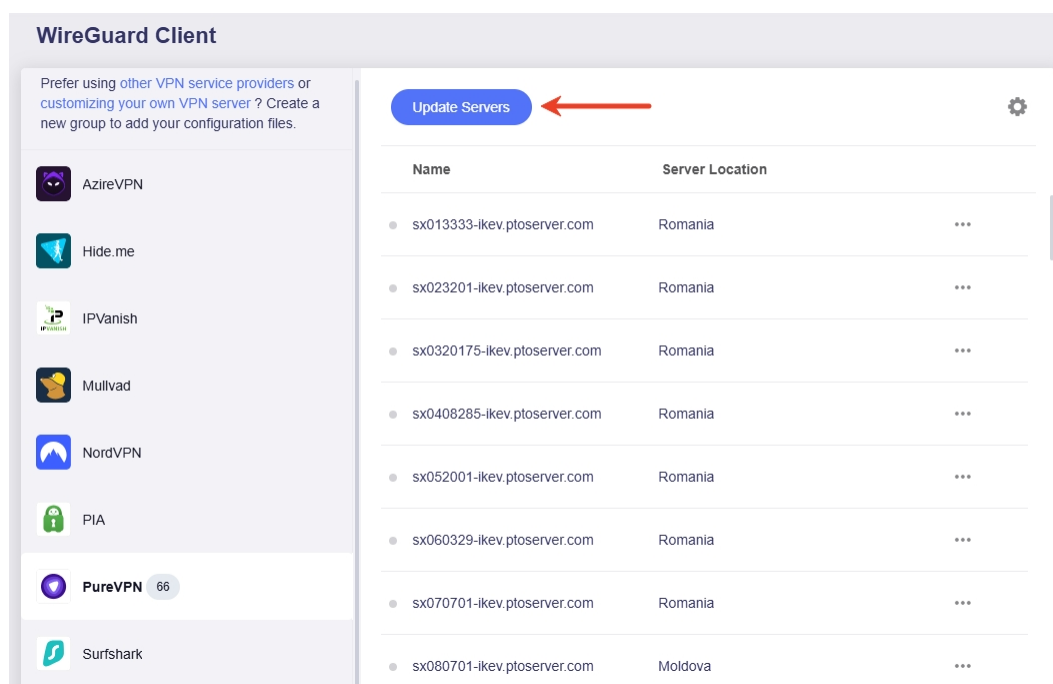
- Once connected, a green dot will appear next to the configuration file.



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

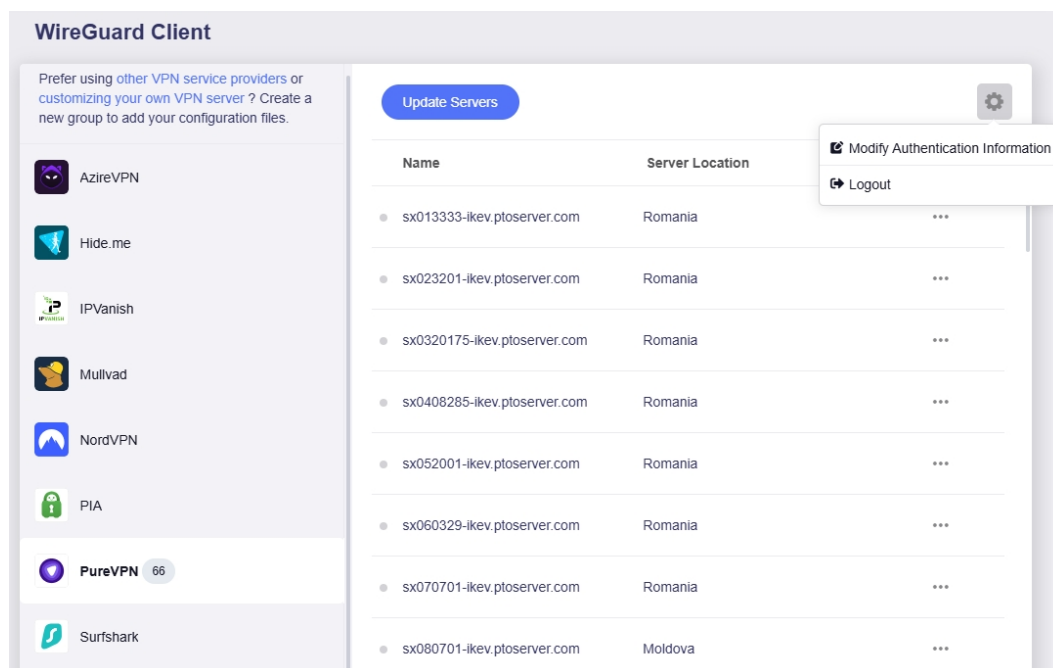
- Update servers.

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



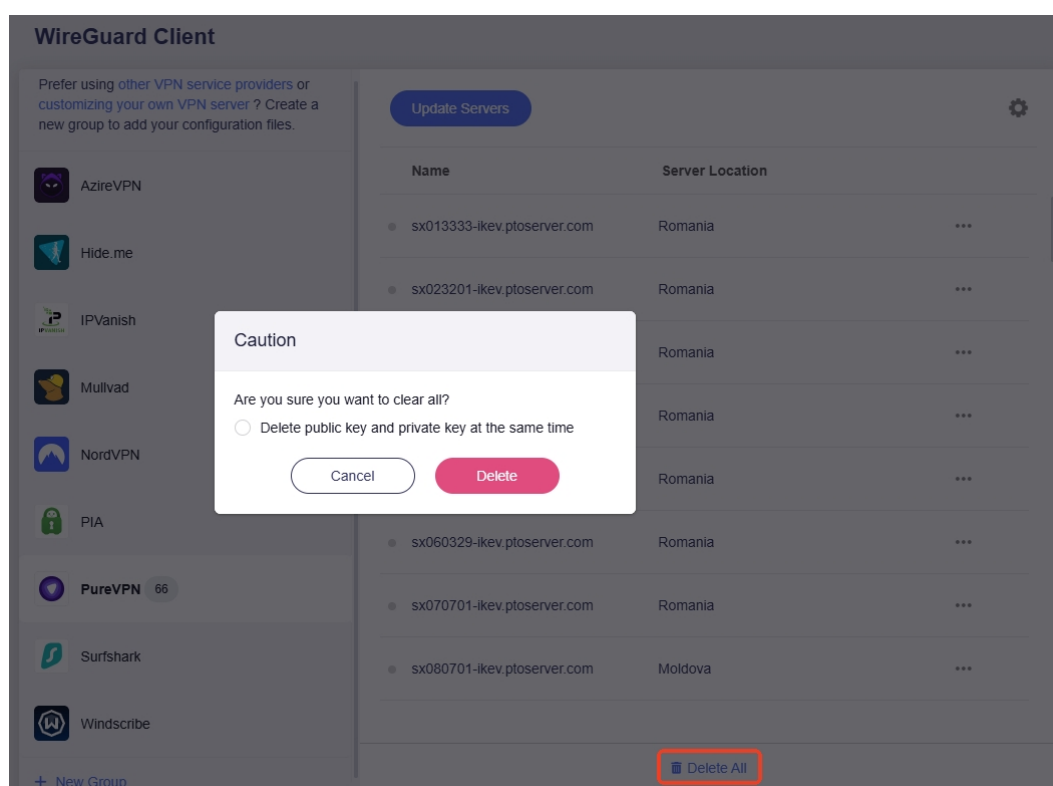
6. Edit credentials or logout.

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



7. Delete all files.

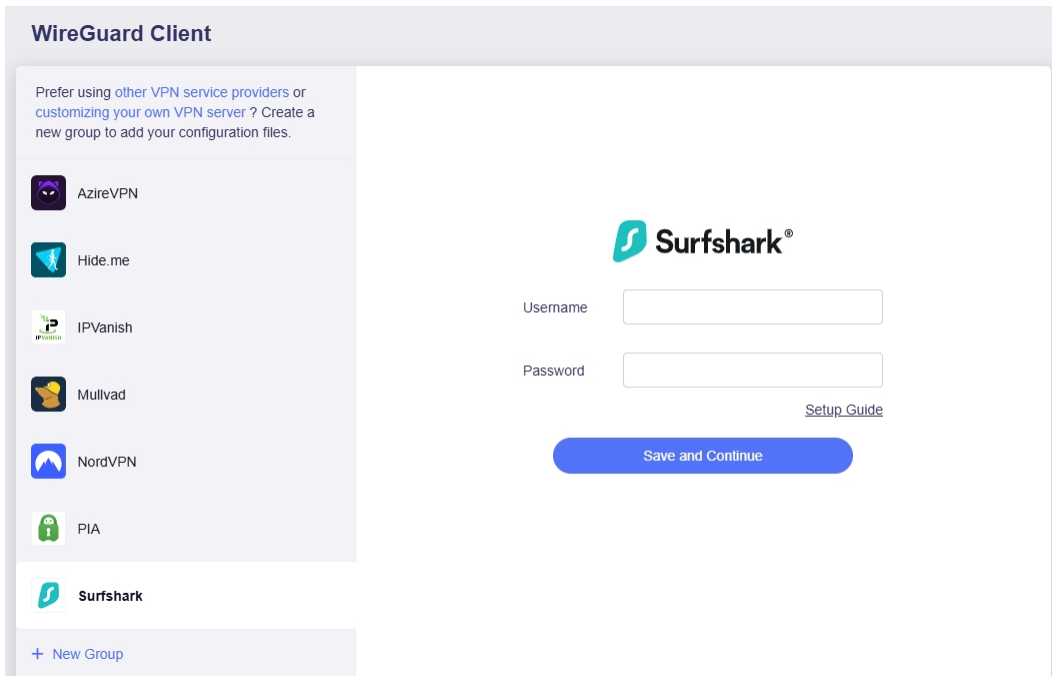
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.9 Set Up Surfshark

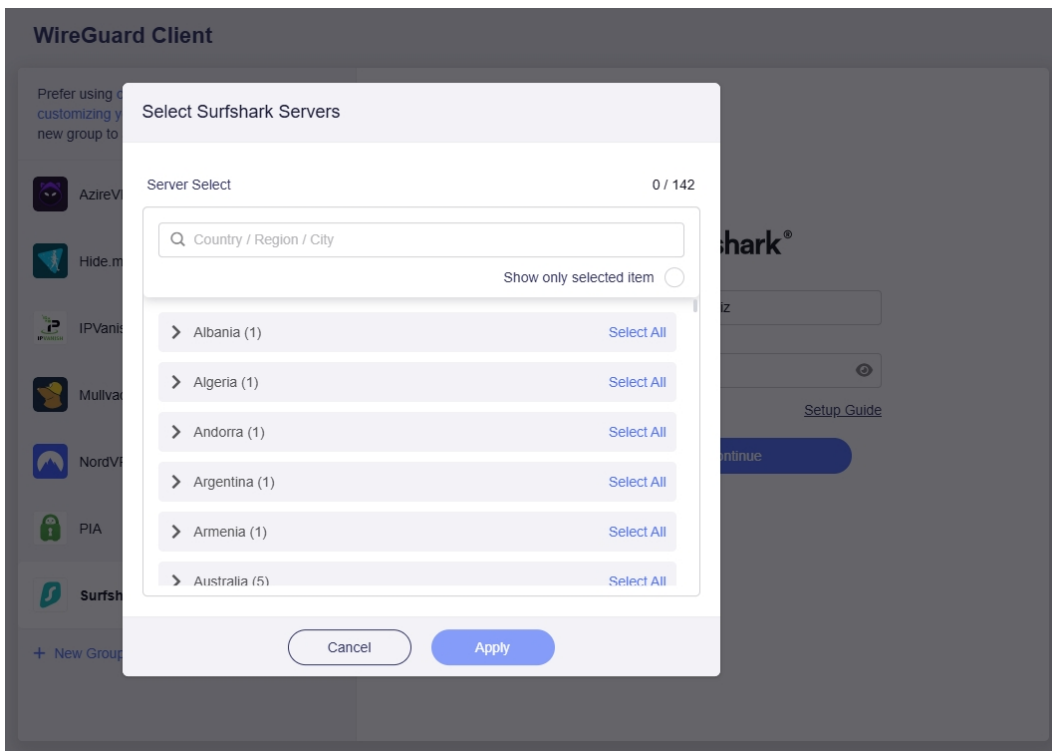
Follow the steps below to set your router as a Surfshark client.

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**.



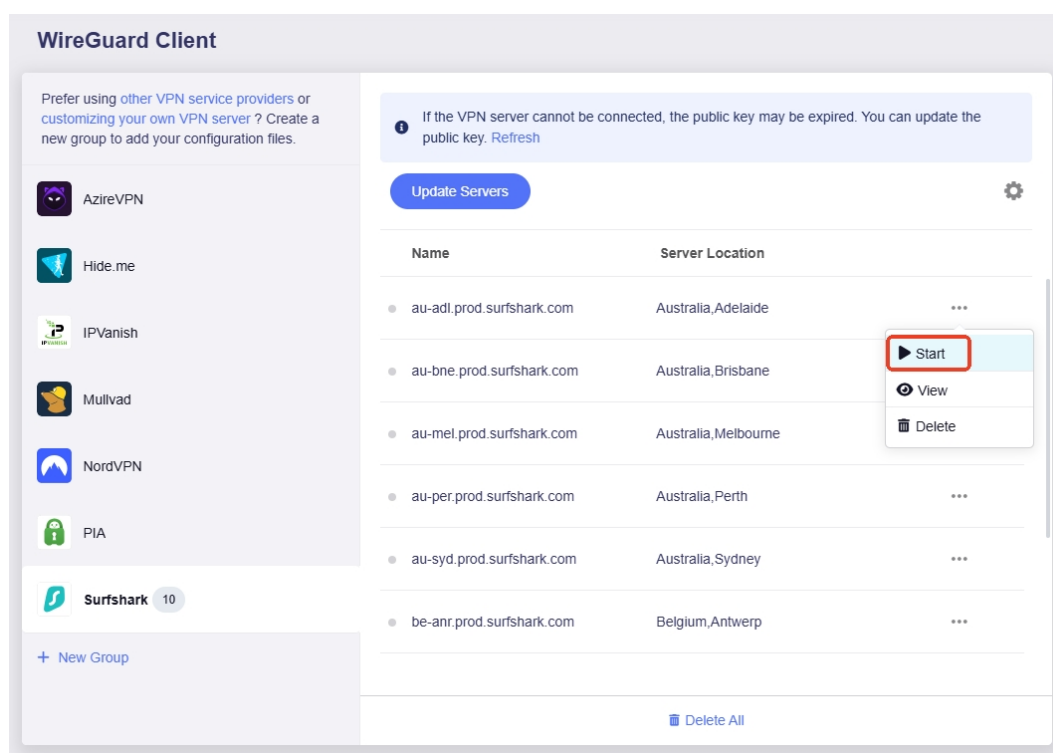
The screenshot shows the 'WireGuard Client' configuration page. On the left, there is a list of VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. Below this list is a '+ New Group' button. The main area on the right is for the Surfshark configuration. It features the Surfshark logo at the top, followed by 'Username' and 'Password' input fields. A 'Setup Guide' link is located below the password field. At the bottom of this section is a blue 'Save and Continue' button.

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

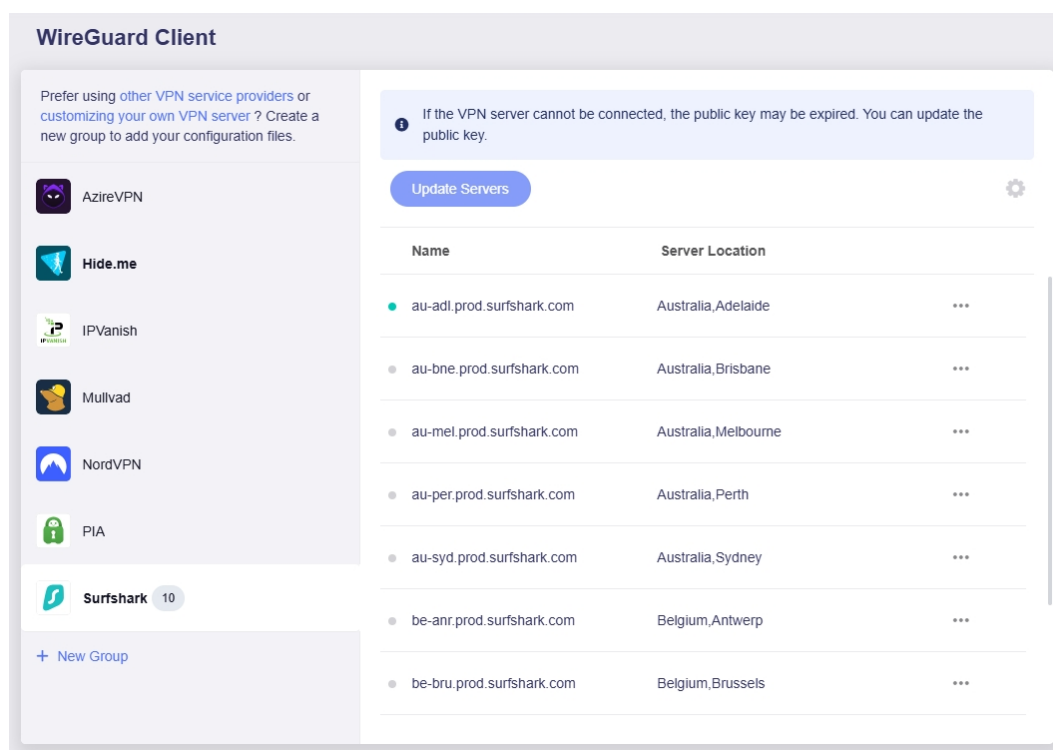


The screenshot shows a 'Select Surfshark Servers' dialog box overlaid on the configuration page. The dialog has a title bar and a search bar labeled 'Country / Region / City'. Below the search bar is a toggle for 'Show only selected item'. A list of countries with their respective server counts is displayed: Albania (1), Algeria (1), Andorra (1), Argentina (1), Armenia (1), and Australia (5). Each country entry has a 'Select All' link to its right. At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

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



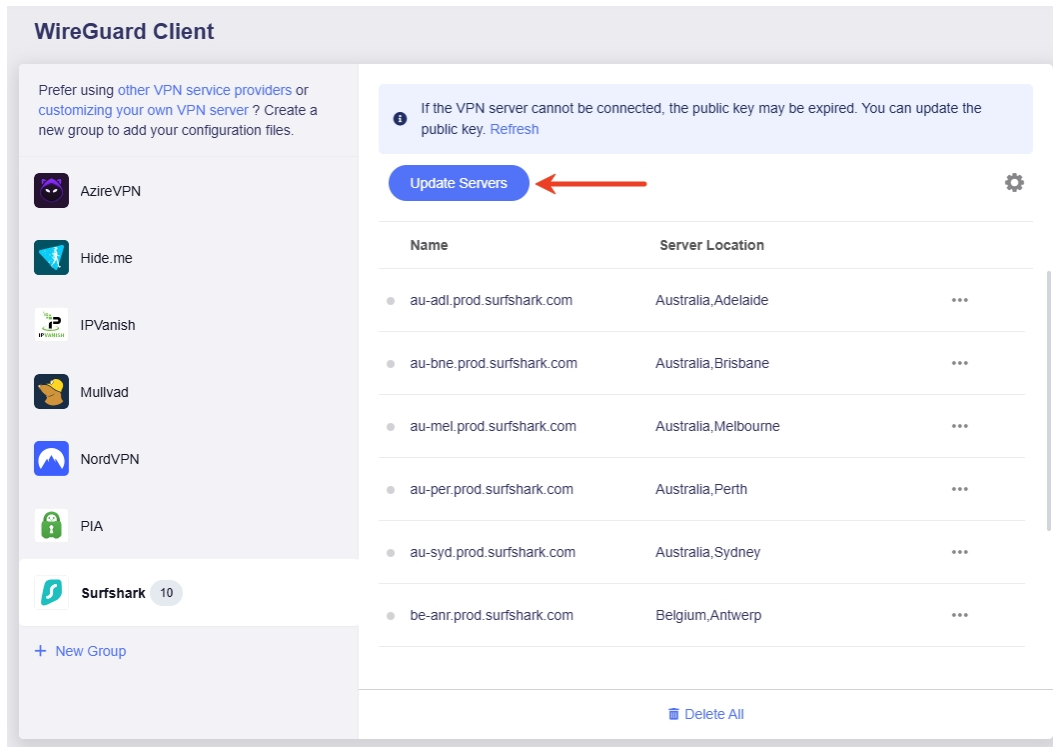
5. Once connected, a green dot will appear next to the configuration file.



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

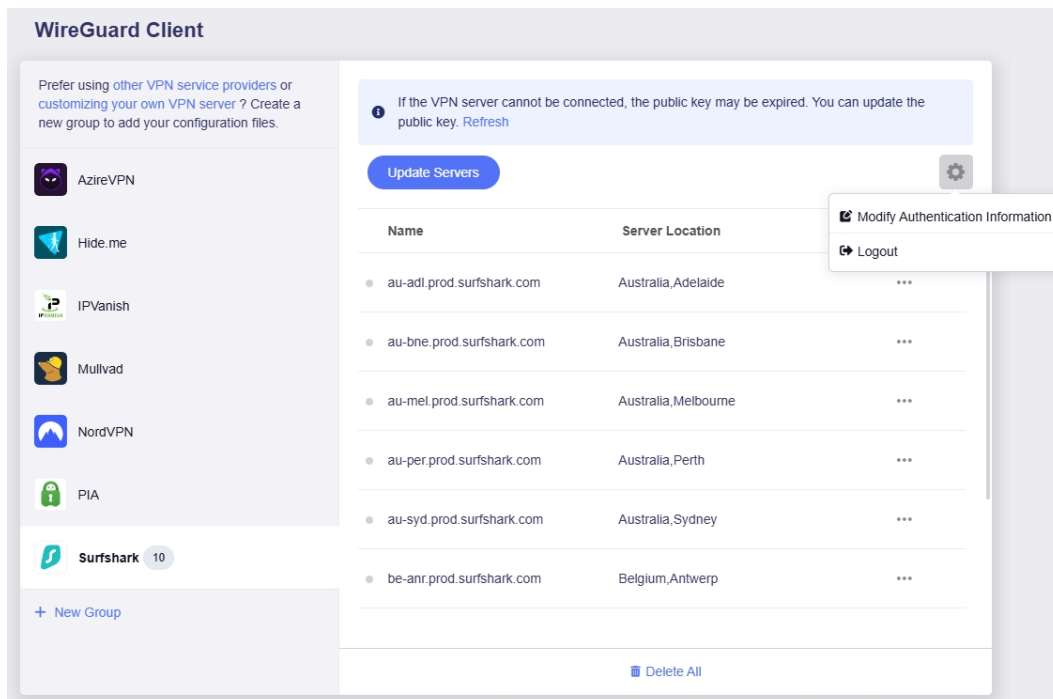
6. Update servers.

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



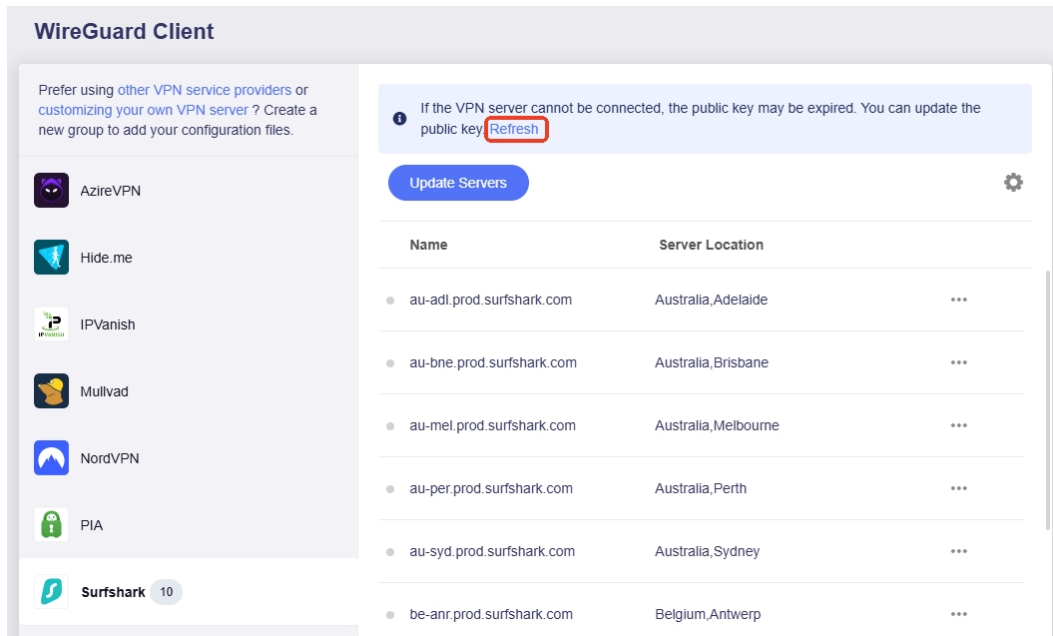
7. Edit credentials or logout.

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



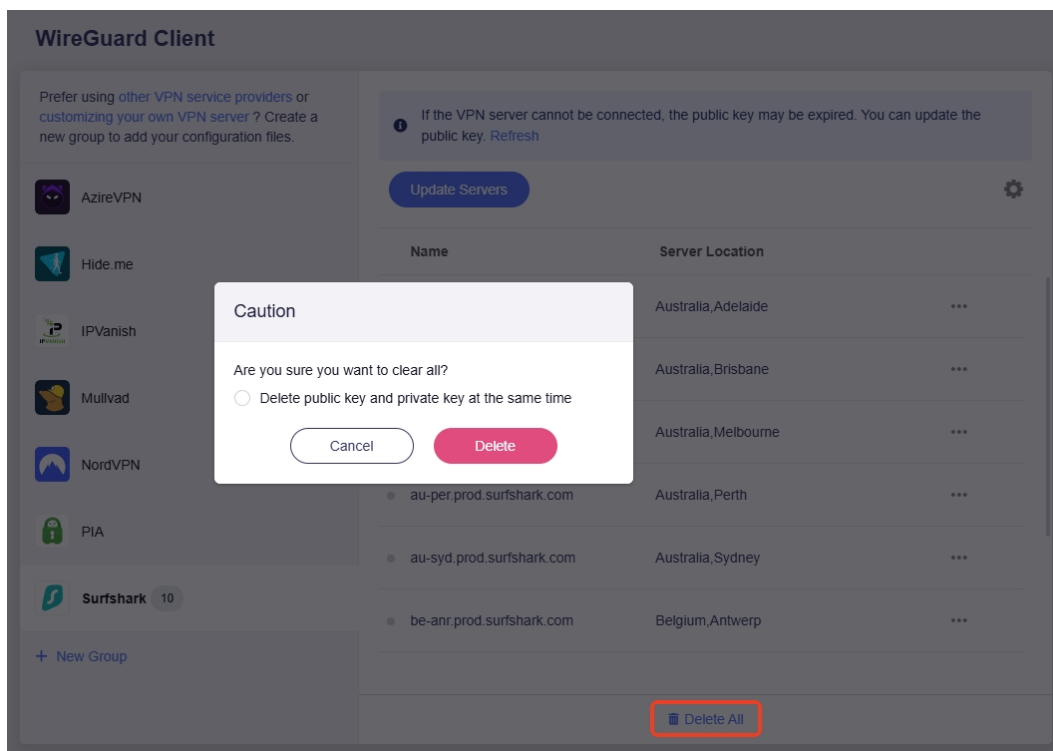
8. Refresh.

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



9. Delete all files.

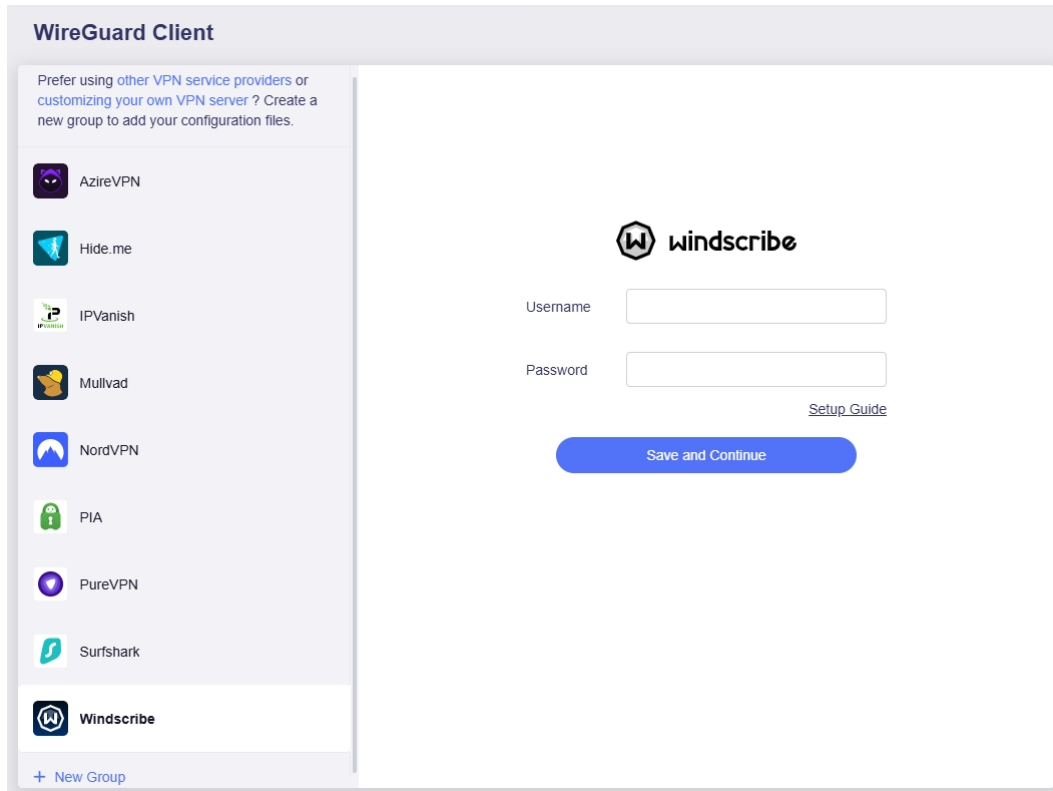
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



10.2.10 Set Up Windscribe

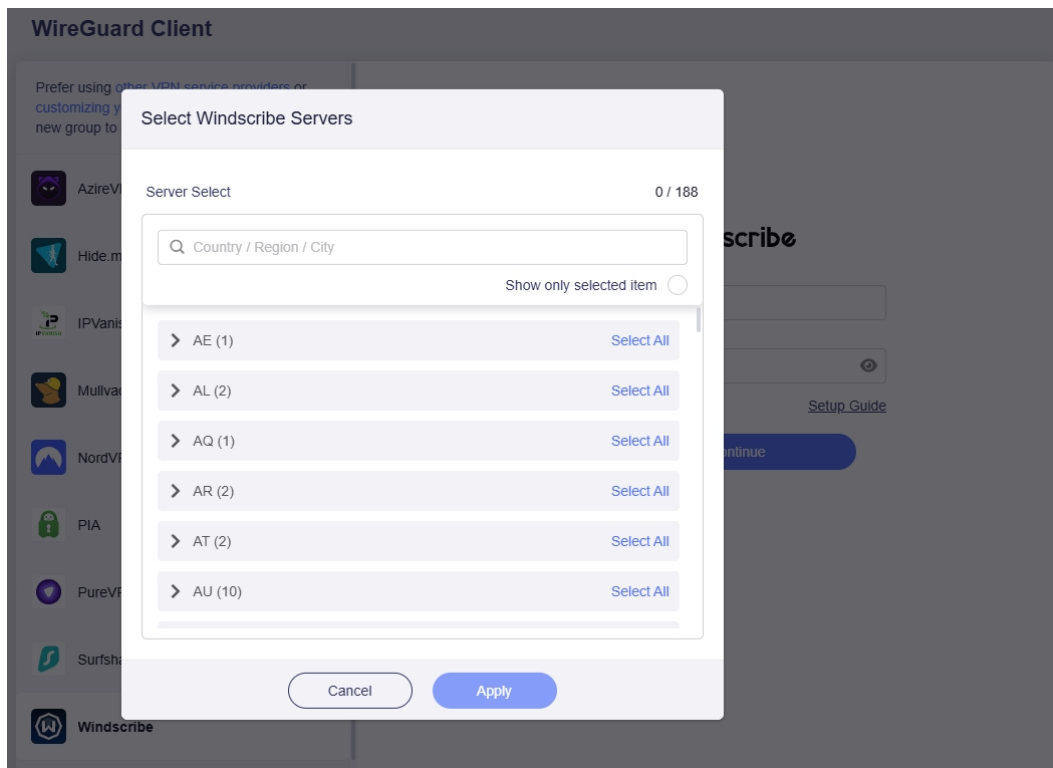
Follow the steps below to set your router as a Windscribe client.

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

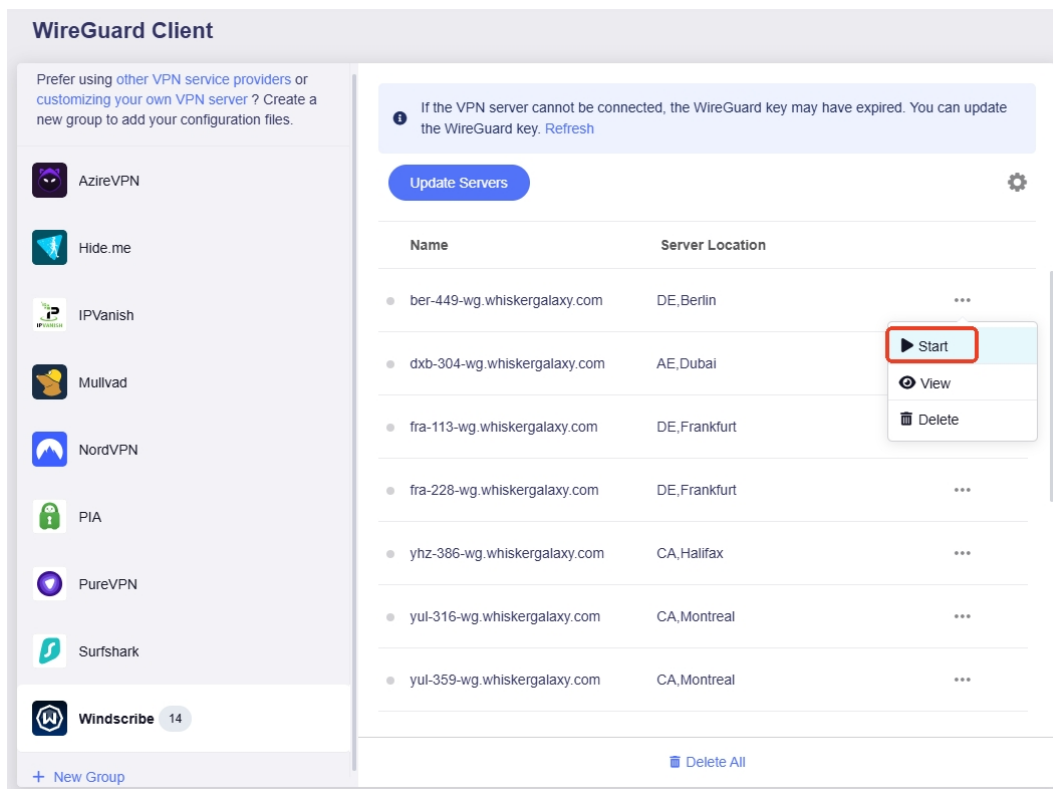


The screenshot shows the 'WireGuard Client' web interface. On the left, there is a sidebar with a list of VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA, PureVPN, Surfshark, and Windscribe. The 'Windscribe' option is highlighted. Above this list, a text prompt asks if the user prefers using other VPN service providers or customizing their own VPN server, suggesting to create a new group to add configuration files. On the right, the 'windscribe' logo is displayed above two input fields for 'Username' and 'Password'. A 'Setup Guide' link is located below the password field. At the bottom of the right panel is a blue button labeled 'Save and Continue'.

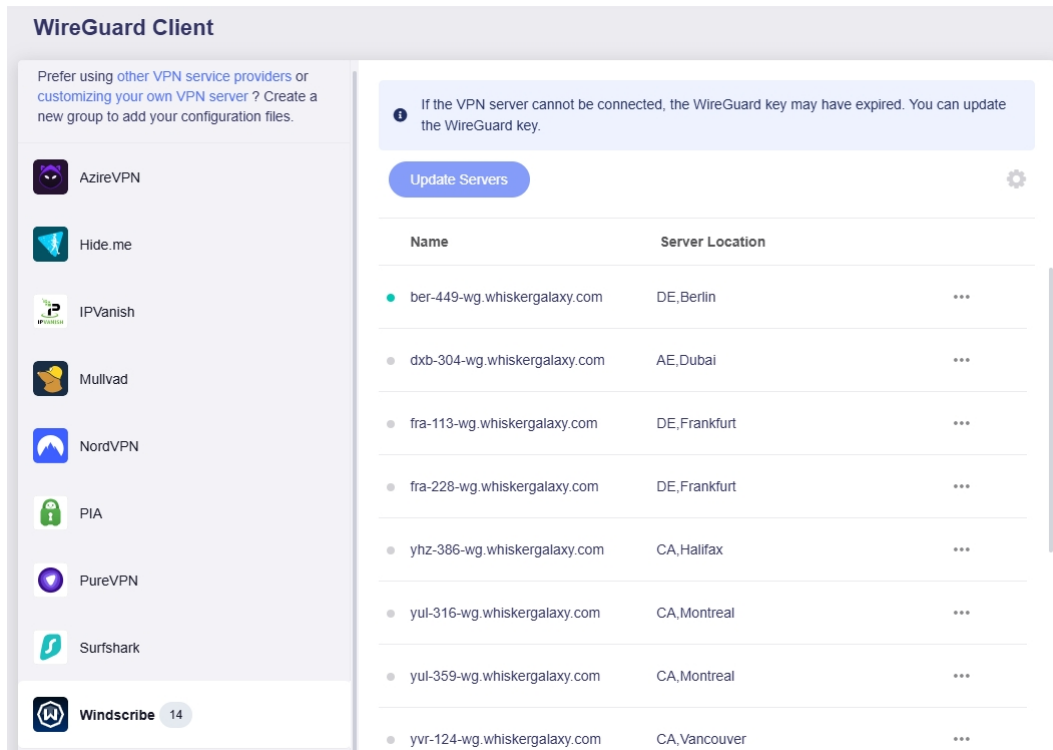
3. Select the server(s) you want to connect to, and click **Apply**.



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



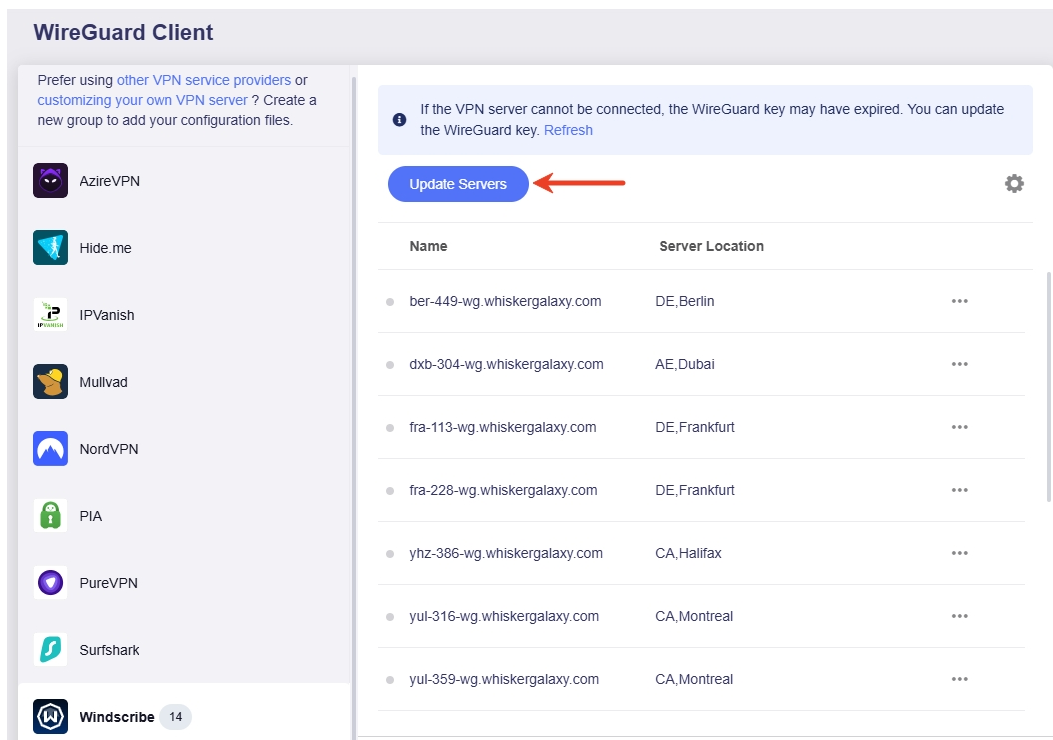
5. Once connected, a green dot will appear next to the configuration file.



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

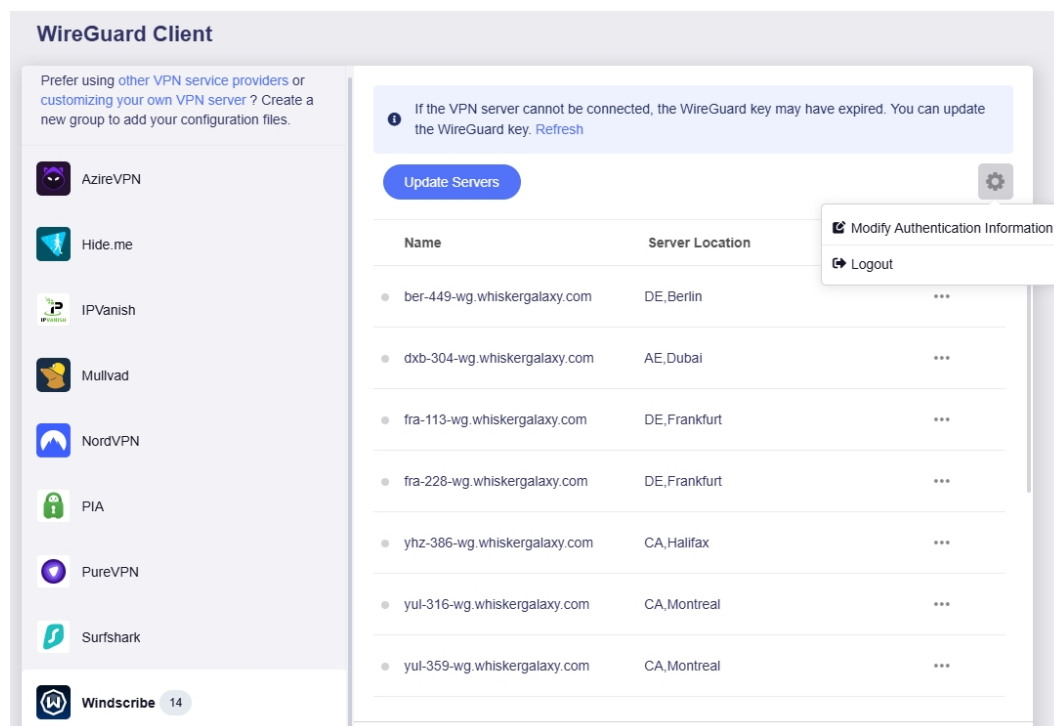
6. Update servers.

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



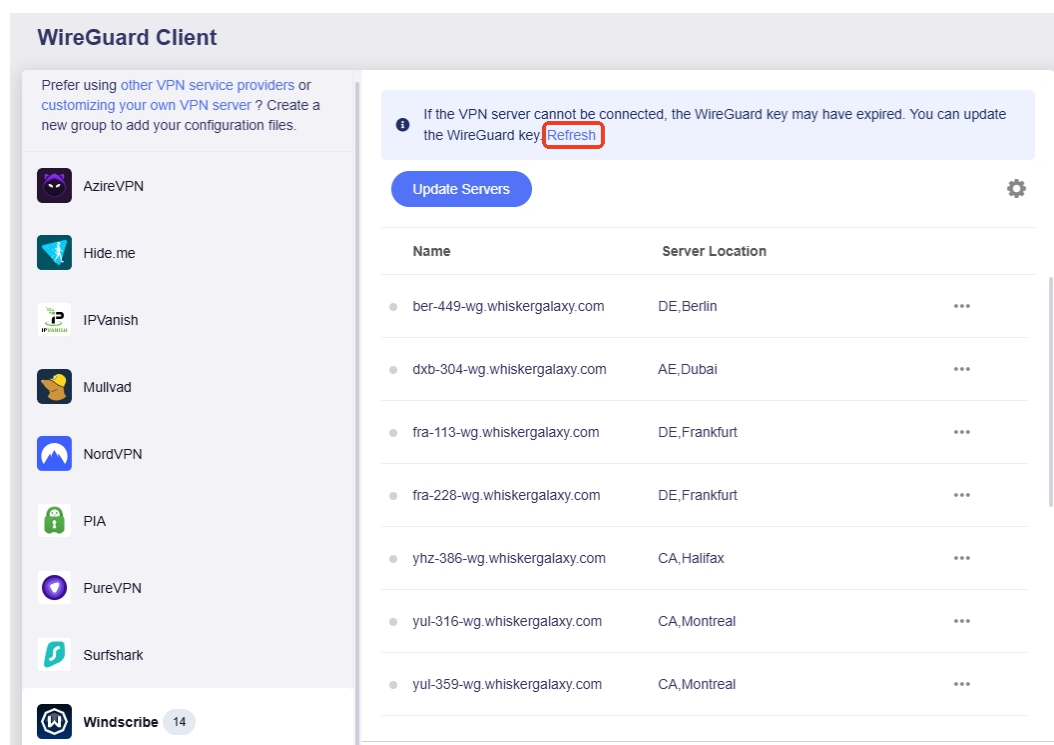
7. Edit credentials or logout.

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



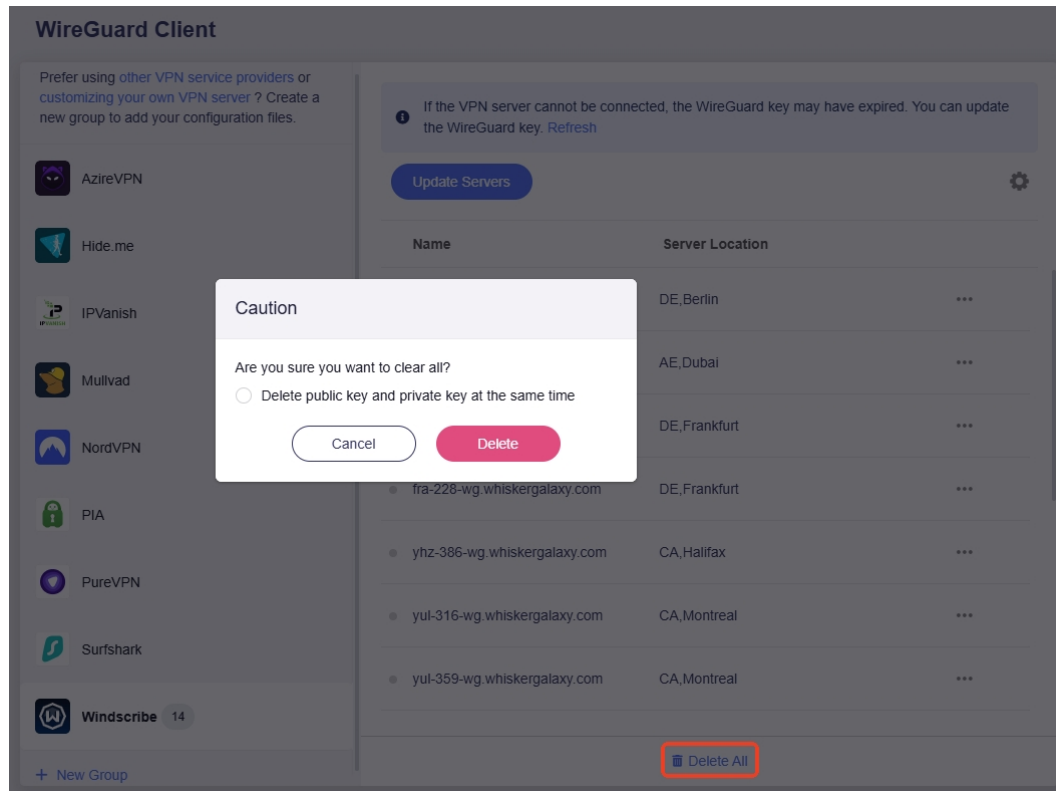
8. Refresh.

You can click **Refresh** to update the public key when the VPN 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.

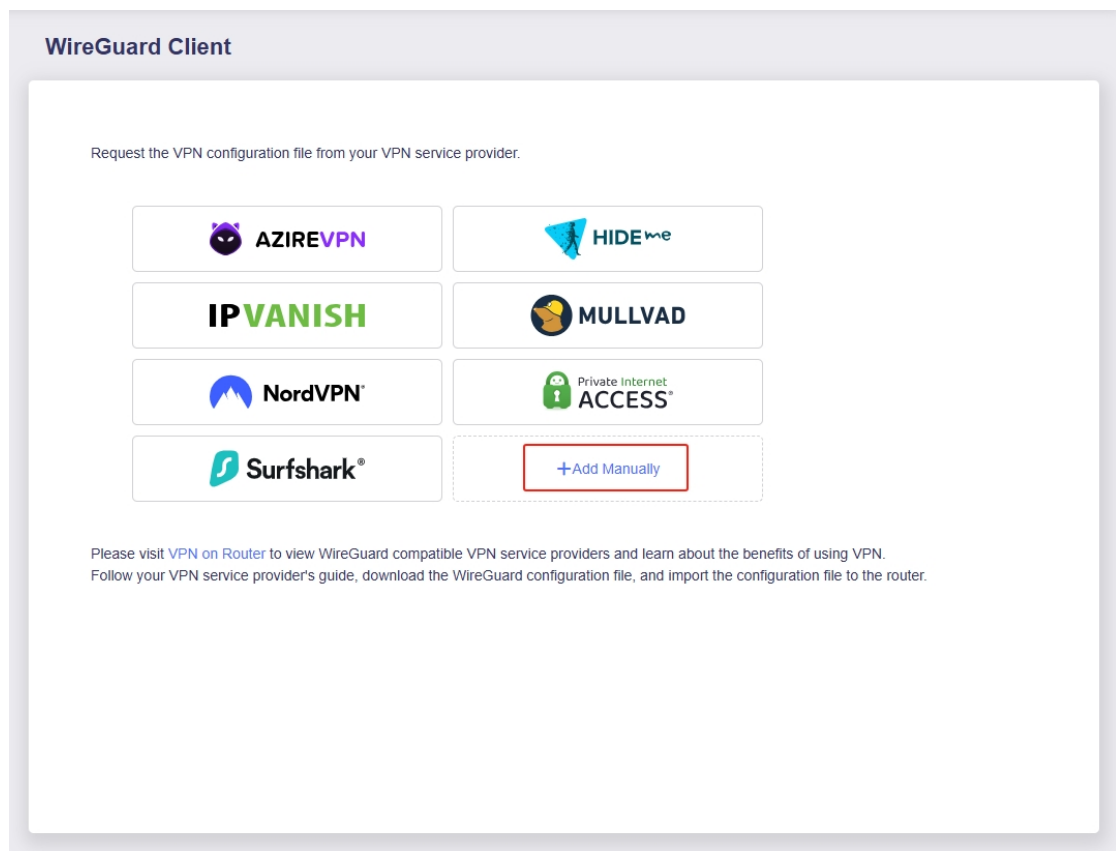


10.2.11 Set Up WireGuard Client Manually (for other providers)

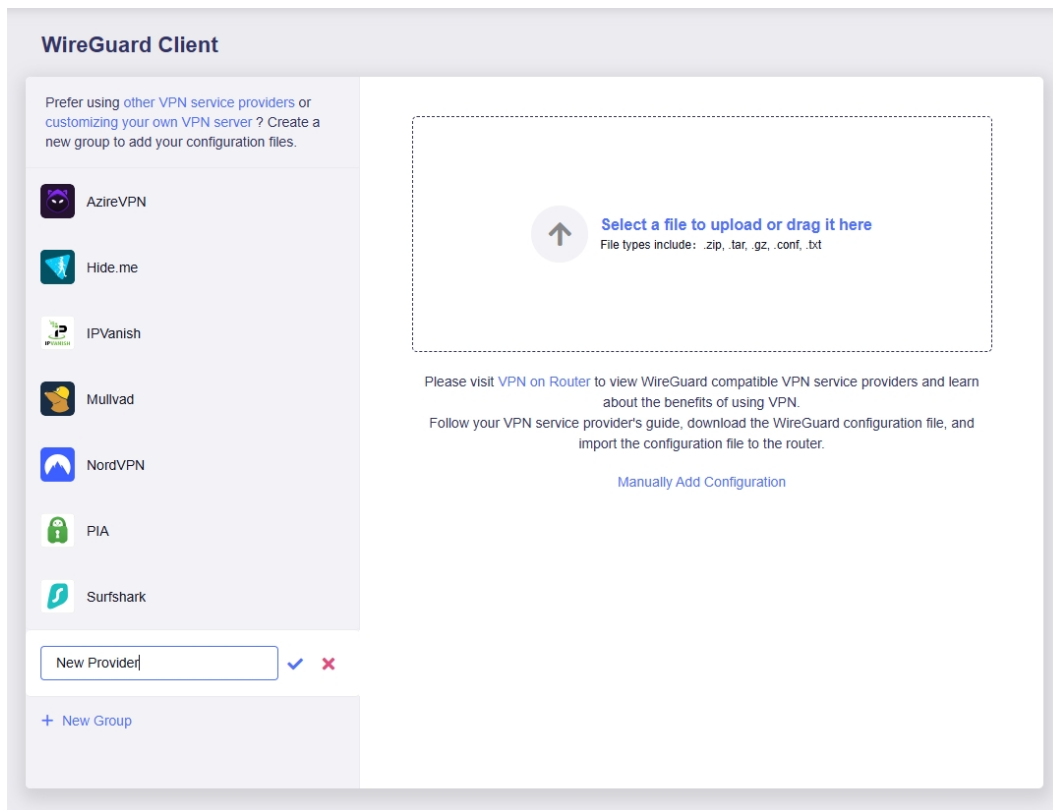
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see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

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

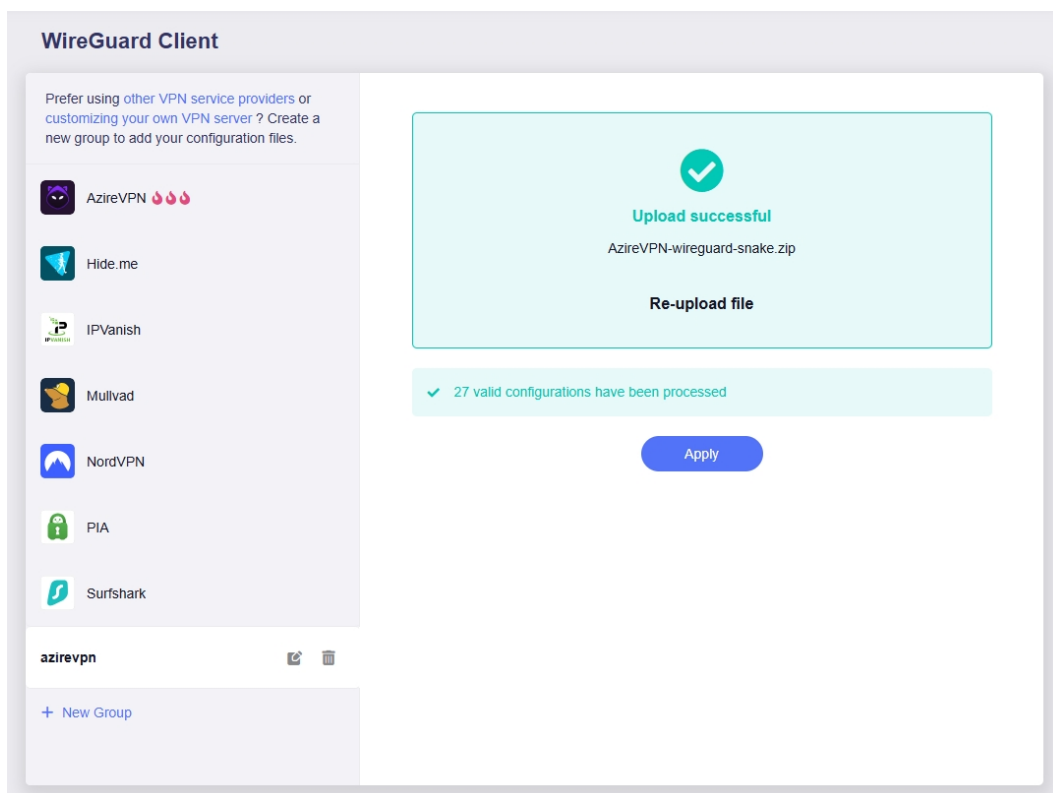
1. Log in to your router's web admin panel and navigate to **VPN > WireGuard Client > Add Manually**.



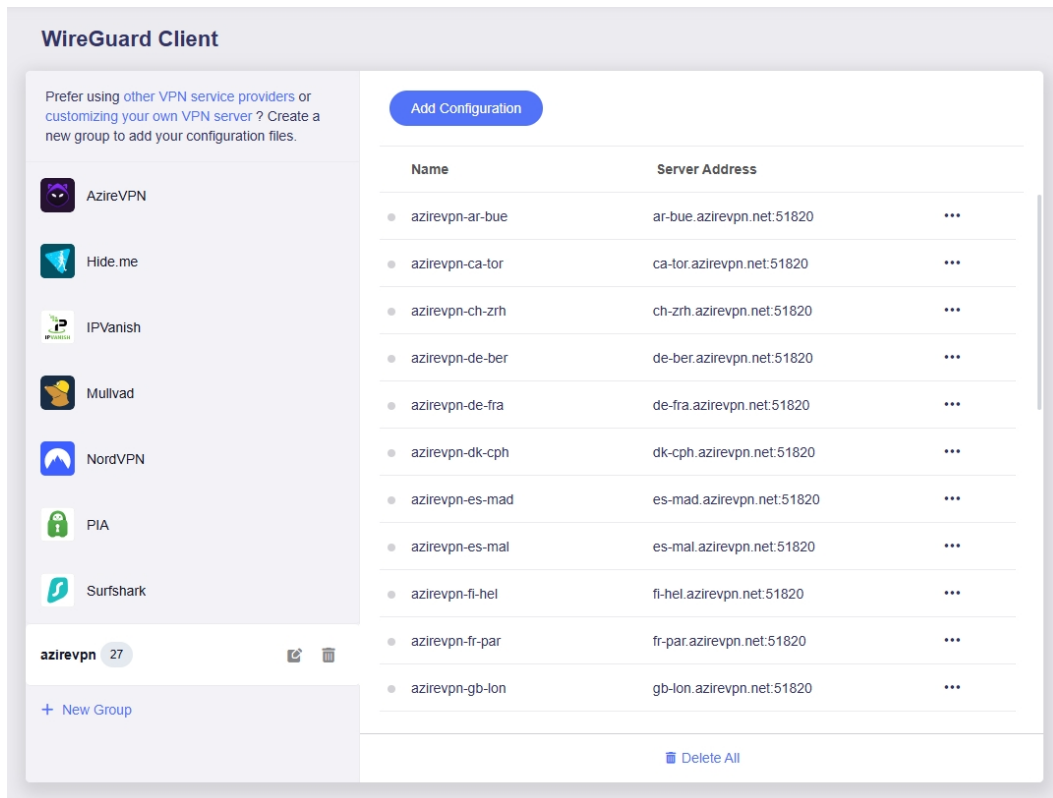
2. It will create a group on the left sidebar. Set a descriptive name for the group.



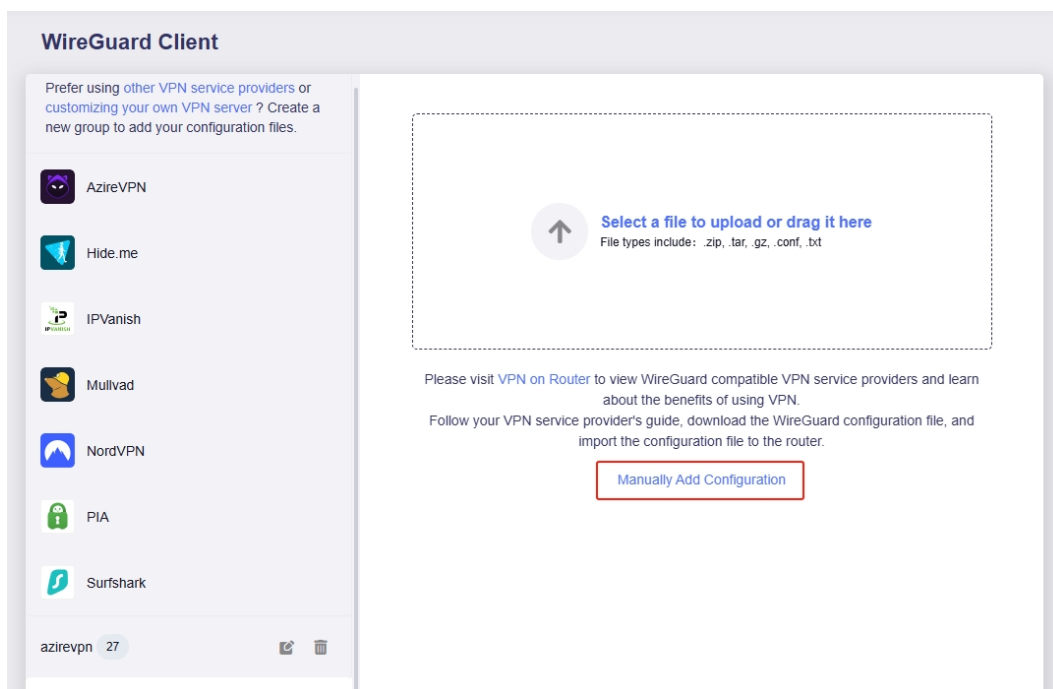
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.

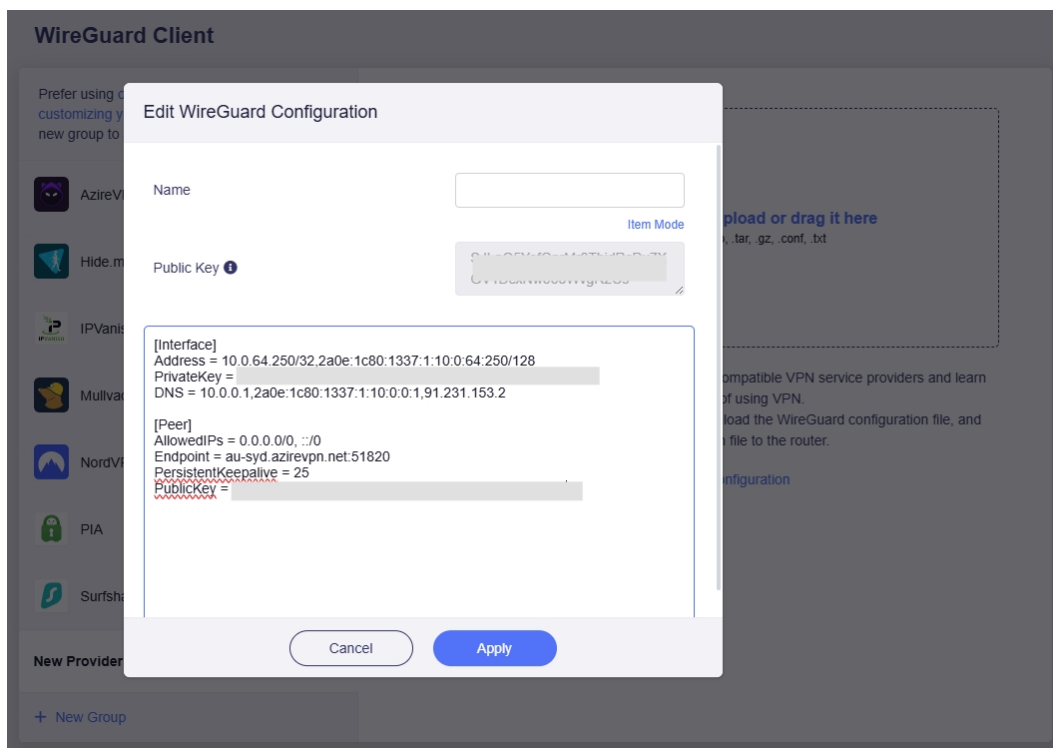


If you upload a compressed file containing multiple configuration files, it will be decompressed automatically, as shown below.

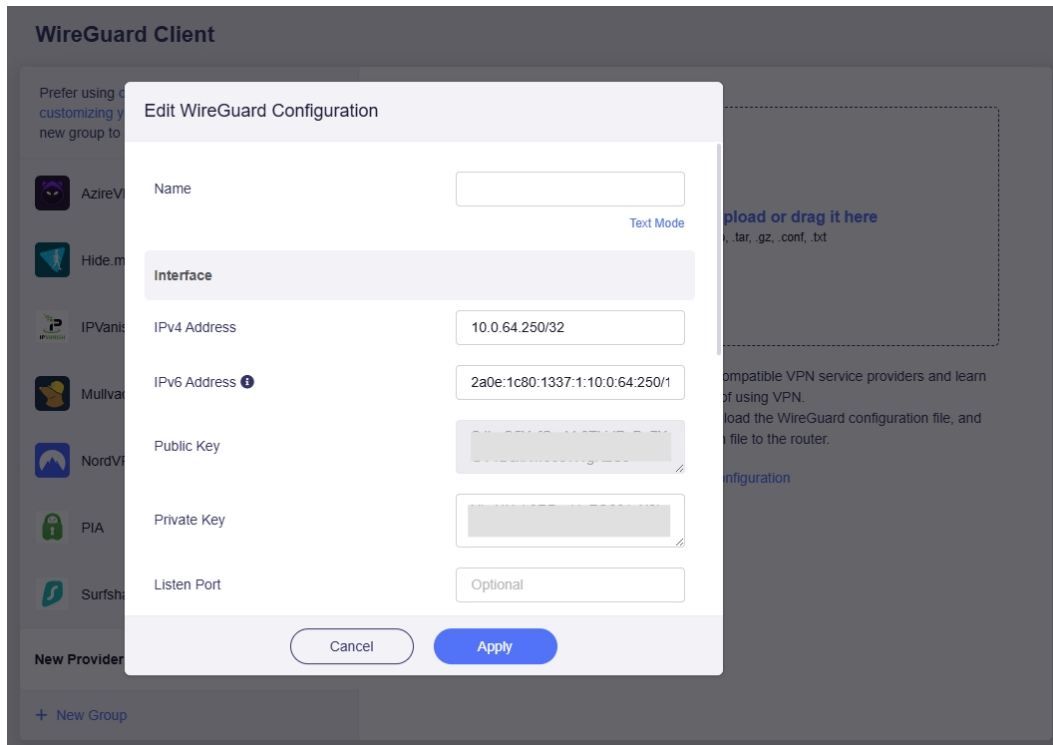


Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

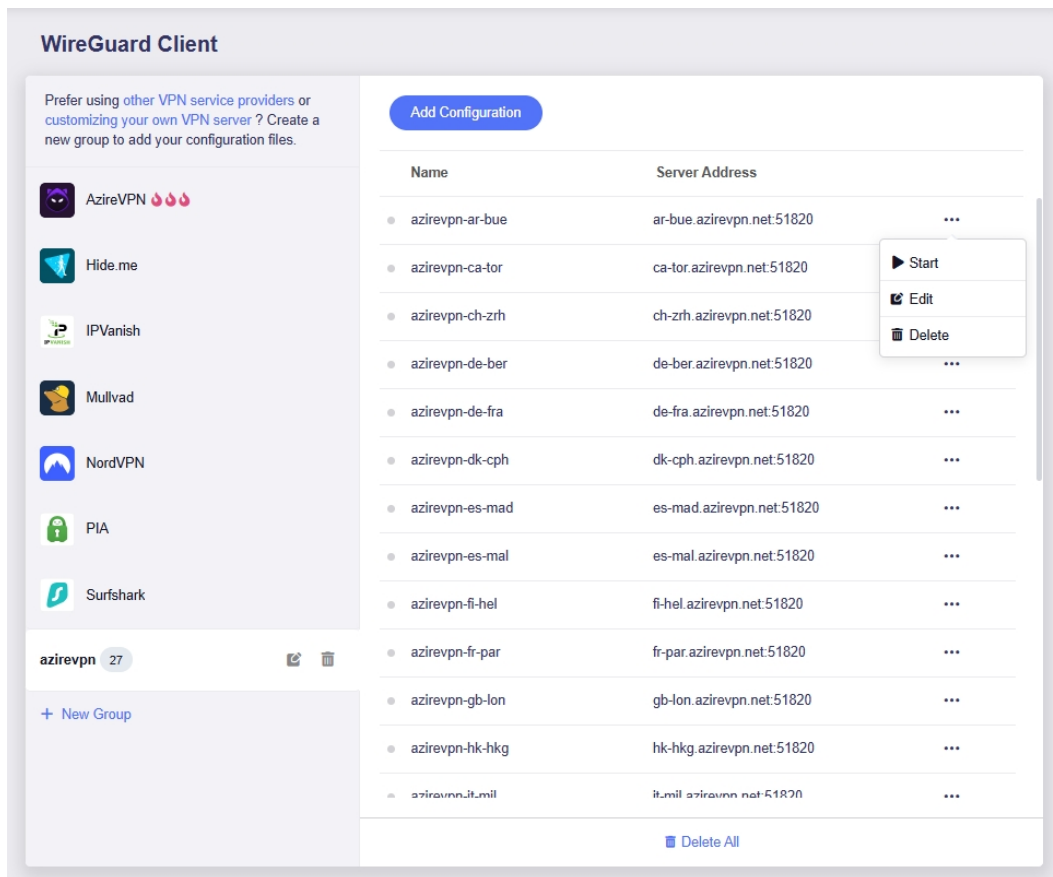




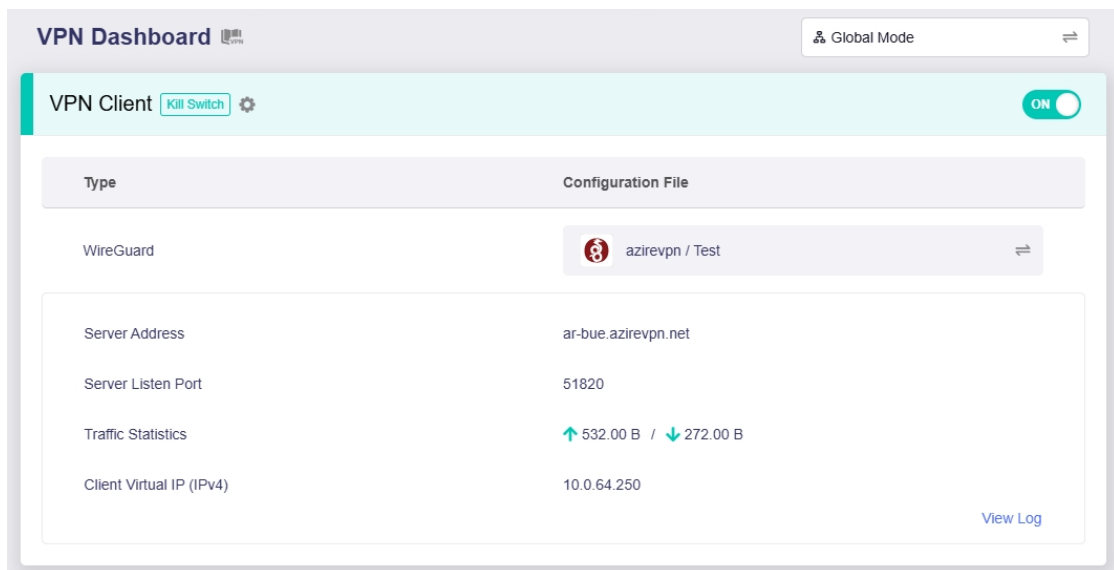
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



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



- 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

Network

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

11.1 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:

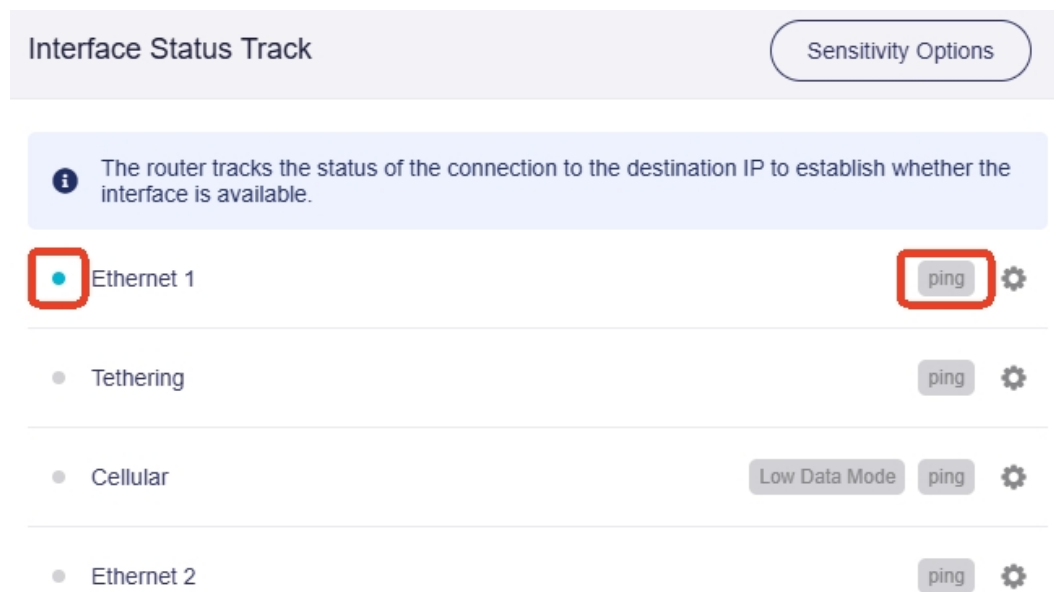
- **Failover:** Automatically switches to an alternate connection within a short time if the primary connection fails, ensuring uninterrupted network access.
- **Load Balance:** Distributes network traffic across all available connections at a set ratio for concurrent multi-connection usage, optimizing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

Brume 3 supports three types of internet connection methods, including Ethernet, Tethering, and Cellular, each serving a distinct network function in software-defined configurations.

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.

11.1.1 Interface Status Track

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



In the **Interface Status Track** section, click the gear icon on the right to access the status tracking settings for each network interface.

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

Ethernet 1 Status Track

Enable Interface Status Track ⓘ



Detection Mode ⓘ

Normal ▼

Track Command

ping ▼

IPv4 Track IP

1.1.1.1

8.8.8.8

208.67.222.222

208.67.220.220

Cancel

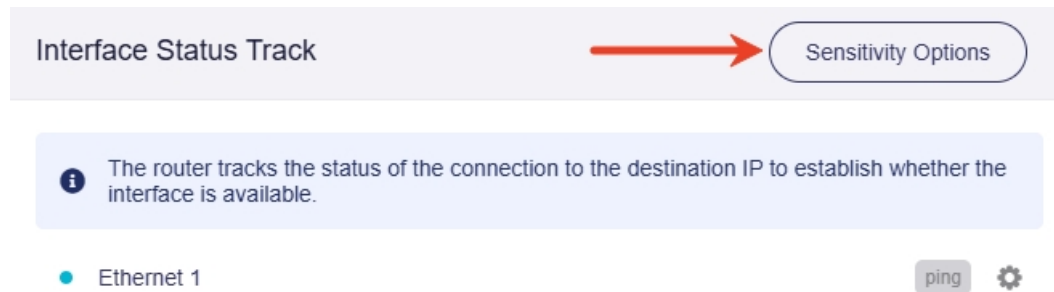
Apply

- **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

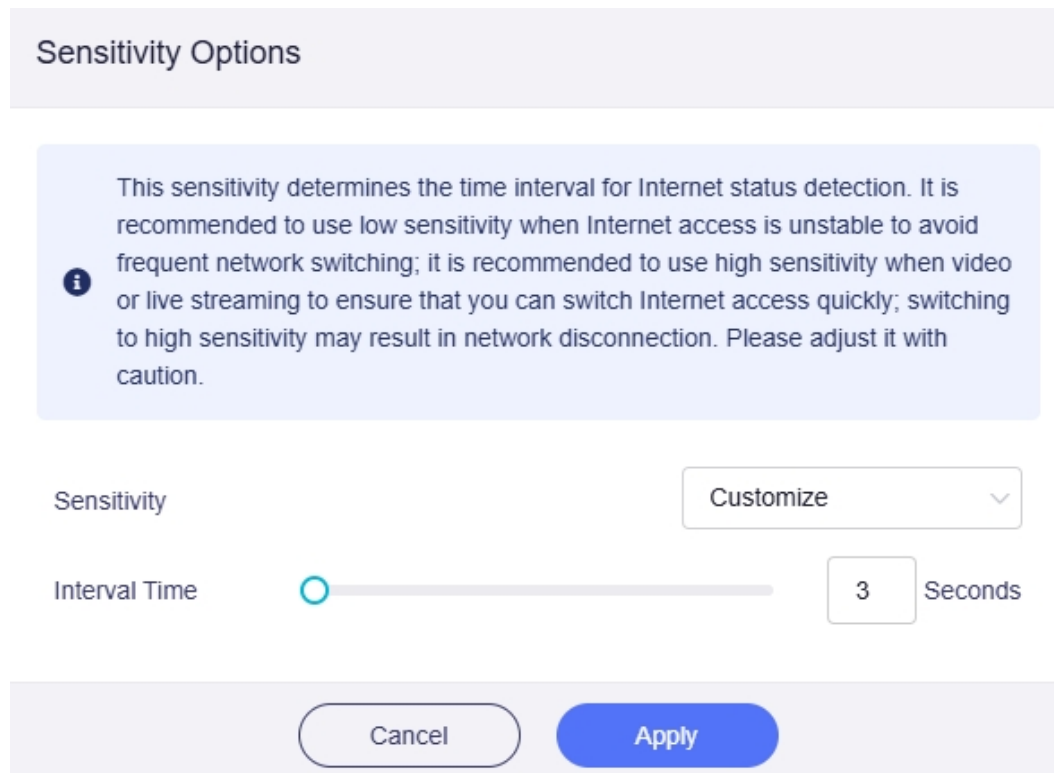
a disconnection may be slightly slower than in Normal Mode, and it is enabled by default only for cellular interface.

- **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.

11.1.2 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.

Mode ⓘ

Failover

Load Balance

Interface Priority

1	Ethernet 1	≡
2	Ethernet 2	≡
3	Tethering	≡
4	Cellular	≡

Apply

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 four networks (e.g., Ethernet 1, Tethering, Cellular, and Ethernet 2) simultaneously and all four interfaces are available for Internet access, enabling Load Balance and setting a 1:1:1:1 ratio means the four interfaces will share network bandwidth equally. The system will distribute new connections across these four interfaces according to the configured 1:1:1:1 load ratio.

Mode ⓘ

Failover Load Balance

Load Ratio

Ethernet 1	1 ▼
Tethering	1 ▼
Cellular	1 ▼
Ethernet 2	1 ▼

Apply

Customize the load ratio as needed. For example, if Ethernet 1 has a bandwidth of 100 Mbps, Ethernet 2 has 200 Mbps, and no Tethering or Cellular connections are active, set the load ratios to 1 for Ethernet 1, 2 for Ethernet 2, and 0 for Tethering and Cellular. The system will then distribute new connections across these interfaces according to the configured 1:2 ratio, meaning Ethernet 1 will handle half as many connections as Ethernet 2. 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.

11.2 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.

11.2.1 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

LAN

 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 

192.168.8.1

Netmask

255.255.255.0

Apply

- **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.

11.2.2 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.

DHCP Server

The DHCP server automatically assigns IP addresses and other communication parameters to client devices. If the DHCP server is disabled, client device network settings will need to be configured manually. [Learn More](#)

Enable ☒

Start IP Address

End IP Address

[Advanced](#)

[Apply](#)

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

Start IP Address

End IP Address

[Advanced](#)

[Apply](#)

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

Lease Time	720	Minutes
Gateway	Optional	
DNS Server 1	Optional	
DNS Server 2	Optional	
LPR Server ⓘ	Optional	
+ Add		

- **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.

11.2.3 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**.

Add a New Reservation Entry

MAC

IP

192.168.8.223

Description

Lauren-iPhone

Cancel

Submit

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

Address Reservation

When you specify a reserved IP address for a LAN client, the client will always receive the same IP address when it requests an IP address from router's DHCP server. You can assign reserved IP addresses to computers or servers that require permanent IP settings.
Note: Configured clients have to reconnect the router to activate.

Add

MAC	IP	Description	Action
	192.168.8.223	Lauren-iPhone	...

158

11.3 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

 When you set custom DNS servers, any DNS queries will be resolved through them (instead of the DNS servers obtained through network interface). Otherwise, you will use the DNS settings configured for each interface.

DNS Rebinding Attack Protection 



Override DNS Settings of All Clients 



Allow Custom DNS to Override VPN DNS 



DNS Server Settings

Mode

Automatic



DNS from Repeater

192.168.18.1

Apply

- **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.

11.3.1 DNS Server Settings

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

The screenshot shows the 'DNS Server Settings' section. The 'Mode' dropdown menu is open, displaying four options: 'Automatic' (highlighted in blue), 'Encrypted DNS', 'Manual DNS', and 'DNS Proxy'. Below the dropdown is a blue 'Apply' button. The 'DNS from Repeater' field is currently empty.

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

This screenshot shows the 'DNS Server Settings' section after the 'Automatic' mode has been selected. The 'Mode' dropdown is now closed and shows 'Automatic'. The 'DNS from Repeater' field now contains the IP address '192.168.18.1'.

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.

The screenshot shows the 'DNS Server Settings' section. The 'Mode' is set to 'Encrypted DNS'. The 'Encryption Type' dropdown menu is open, showing four options: 'DNS over TLS' (highlighted), 'DNSCrypt-Proxy', 'DNS over HTTPS', and 'Oblivious DNS over HTTPS'. There is an 'Apply' button at the bottom.

- 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.

The screenshot shows the 'DNS Server Settings' section with the 'Mode' set to 'Manual DNS'. There are four input fields for DNS servers: 'DNS Server 1' (empty), 'DNS Server 2' (Optional), 'DNS Server 3' (Optional), and 'DNS Server 4' (Optional).

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.

DNS Server Settings ⓘ

Mode

DNS Proxy ▼

Proxy Server Address

8.8.8.8#53

11.3.2 Edit Hosts

You can define static DNS resolution rules as needed.

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

DNS  **Edit Hosts**

ⓘ When you set custom DNS servers, any DNS queries will be resolved through them (instead of the DNS servers obtained through network interface). Otherwise, you will use the DNS settings configured for each interface.

DNS Rebinding Attack Protection ⓘ

☐

Override DNS Settings of All Clients ⓘ

☐

Allow Custom DNS to Override VPN DNS ⓘ

☒

DNS Server Settings

Mode

Automatic ▼

DNS from Repeater

192.168.18.1

Apply

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

11.4 Ethernet Port

Log in to your router's web admin panel and navigate to **NETWORK > Ethernet Port**. 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 screenshot shows the WAN configuration page. At the top, there are three tabs: WAN, LAN1, and LAN2. The WAN tab is active, showing 'As WAN Port'. Below the tabs, there is a 'WAN/LAN' dropdown menu set to 'Ethernet1'. To the right of this are two buttons: 'WAN' (highlighted in blue) and 'LAN'. Below these is a 'MAC Mode' dropdown menu set to 'Factory'. Underneath is the 'MAC Address' field, which contains the value '94:83:C4:C5:BA:FD'. At the bottom, there is a section titled 'Negotiated Network Port Rate' with a 'Speed' field displaying '2500 Mbps full duplex'.

The **LAN 1** section allows you to switch LAN 1 to WAN. You can switch the port role and check the negotiated rate here.

The screenshot shows the LAN 1 configuration page. At the top, there are three tabs: WAN, LAN1, and LAN2. The LAN1 tab is active, showing 'As LAN Port'. Below the tabs, there is a 'WAN/LAN' dropdown menu. To the right of this are two buttons: 'WAN' and 'LAN' (highlighted in blue). Below these is a section titled 'Negotiated Network Port Rate' with a 'Speed' field displaying '1000 Mbps full duplex'.

The **LAN 2** section displays the LAN port negotiated rate.

The screenshot shows the LAN 2 configuration page. At the top, there are three tabs: WAN, LAN1, and LAN2. The LAN2 tab is active, showing 'As LAN Port'. Below the tabs, there is a section titled 'Negotiated Network Port Rate' with a 'Speed' field displaying '1000 Mbps full duplex'.

Note: The negotiated rate for WAN and LAN ports is displayed only when an Ethernet cable is connected.

11.5 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**.

IPv6



When IPv6 is enabled, WAN interfaces such as Ethernet will get their IPv6 addresses via DHCPv6. You can also modify the IPv6 address manually in the Ethernet settings page. Some features (Firewall, GoodCloud, OpenVPN DCO) do not yet support IPv6.

Enable IPv6



LAN

Mode ⓘ

Native



DNS acquisition method

Automatic



Apply

11.5.1 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.

11.5.2 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.

11.6 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.

IGMP Snooping

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

IGMPv3 is compatible with v1 and v2. Use v3 by default, and switch if you experience a problem.

Enable



Version

3



Apply

11.7 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 3 supports two modes: Router and Bridge mode.

Network Mode

When you change the router's network mode, you may need to reconnect all of your client devices.

i When you use Bridge, you will not be able to connect to this UI again. You can press and hold the reset button for 4 seconds to revert to router mode. [Learn More](#)

☒ Router
Create your own private network. The router will act as a NAT, firewall and DHCP server.

☐ Bridge
Connect to a wired network.

Apply

- **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:

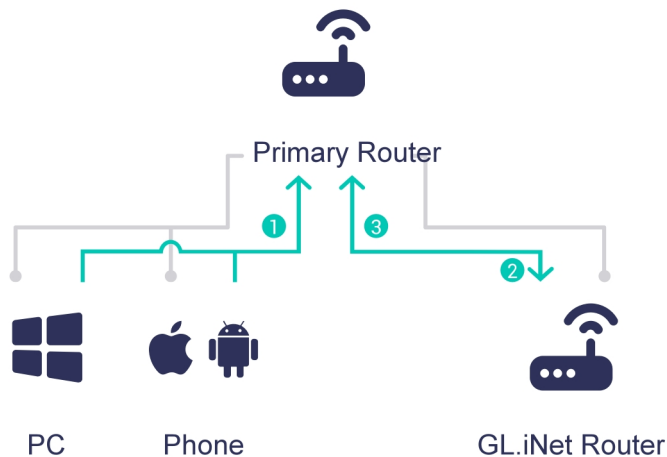
1. When the network mode is changed, devices need to reconnect to the router to ensure a stable connection.
2. **In Bridge mode, you will not be able to access the web admin panel using the original IP address.** Instead, you need to log in to the upstream router to find the IP address it has assigned 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, AdGuard Home, Parental Control, ZeroTier, Tailscale, Port Forwarding, Multi-WAN, DHCP Server, Address Reservation, DNS, Ethernet Port, IPv6, Drop-in Gateway, IGMP Snooping, Network Acceleration, NAT Settings.

11.8 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. Please refer to [this link](#) for more instructions.

11.9 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.

Network Acceleration

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

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

Enable



Mode

Auto

Apply

- **Auto:** Automatically switch between the two acceleration modes based on actual usage.
- **Hardware Acceleration:** This mode usually works on Ethernet and Repeater (the latter is unavailable on Brume 3). 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, 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:** This mode works on Cellular. It relies on a router's general CPU paired with optimized kernels or drivers (e.g., SWNAT). It works on Cellular (4G/5G) access, 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 DPI, 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.

Chapter 12

Flow Control

This chapter introduces flow control features, providing dedicated tools for network traffic and content management.

12.1 DPI Engine

DPI (Deep Packet Inspection) is a core technology for intelligent network management. Unlike traditional routers that only identify source and destination addresses, DPI performs in-depth analysis of packet payloads and accurately identifies applications and websites using a feature-matching library, enabling fine-grained traffic classification and control.

GL.iNet DPI Engine runs locally on your router to deliver intelligent network management with complete privacy. It provides full access to traffic statistics, content filtering, and QoS for comprehensive traffic control. Integrated with [Netify](#), a lightweight embedded DPI agent for intelligent network management, GL.iNet DPI utilizes Netify's automatically updated online signature database to deliver reliable, accurate and efficient network control.

Note:

1. When the router is in Drop-in Gateway mode, DPI features (including Data Statistics, Content Filter and QoS) and SQM will not take effect.
2. When DPI is enabled, the Network Acceleration will be disabled automatically to ensure stable performance.

Log in to the router's web admin panel and navigate to **FLOW CONTROL > DPI Engine**. Click **Enable DPI Engine**.

DPI Engine Beta

About DPI Engine

The DPI Engine function of GL.iNet provides intelligent network management exclusively on your local router. Enjoy complete privacy with full access to Data Statistics, Content Filter and QoS.

[Enable DPI Engine](#)

What Features Are Included?



Data Statistics

Provides a clear dashboard that identifies network usage by applications and protocols, allows viewing traffic history for 1 hour, 1 day, or 7 days, shows detailed usage rankings, monitors per-device traffic, and lets you block unwanted apps with one click.



Content Filter

An intelligent online safety feature powered by DPI classification that automatically blocks harmful or malicious websites, keeps your network clean and secure, and supports custom rules to block specific apps, domains, or IP addresses.



QoS

Intelligently optimizes bandwidth during network congestion by prioritizing critical application traffic—such as video calls and gaming—reducing latency under limited bandwidth conditions and improving overall network responsiveness.

In the pop-up window, read and agree Terms of Service & Privacy Policy, then click **Apply**. The router will then start DPI initialization. It will disable Network Acceleration, while enabling **Data Statistics** and **Content Filter**.

Activate DPI



Checking and disabling Network Acceleration...

- ✓ Checking device availability
- ✓ Updating configuration and license
- ✓ Checking and disabling Network Acceleration
- ⌚ Enabling Data Statistics and Content Filter

Once activated, you will be directed to the **DPI Engine Version Center**, where you can view the DPI Program version and Database version. You may update the database here when a newer database version is available.

DPI Engine Beta



DPI Engine Version Center Core Services Ready

This page shows only core system status indicators. Traffic processing will start once the relevant features are enabled. DPI Engine is ready. Data Statistics, Content Filter, and QoS work only when enabled in their own pages.

 DPI Program Version
v1.0.2 ✓ Up-to-date

 Database Version
v20260226_01 ✓ Up-to-date

Note: This page displays core system status indicators only. Traffic processing will start once the relevant features are enabled.

12.2 Data Statistics

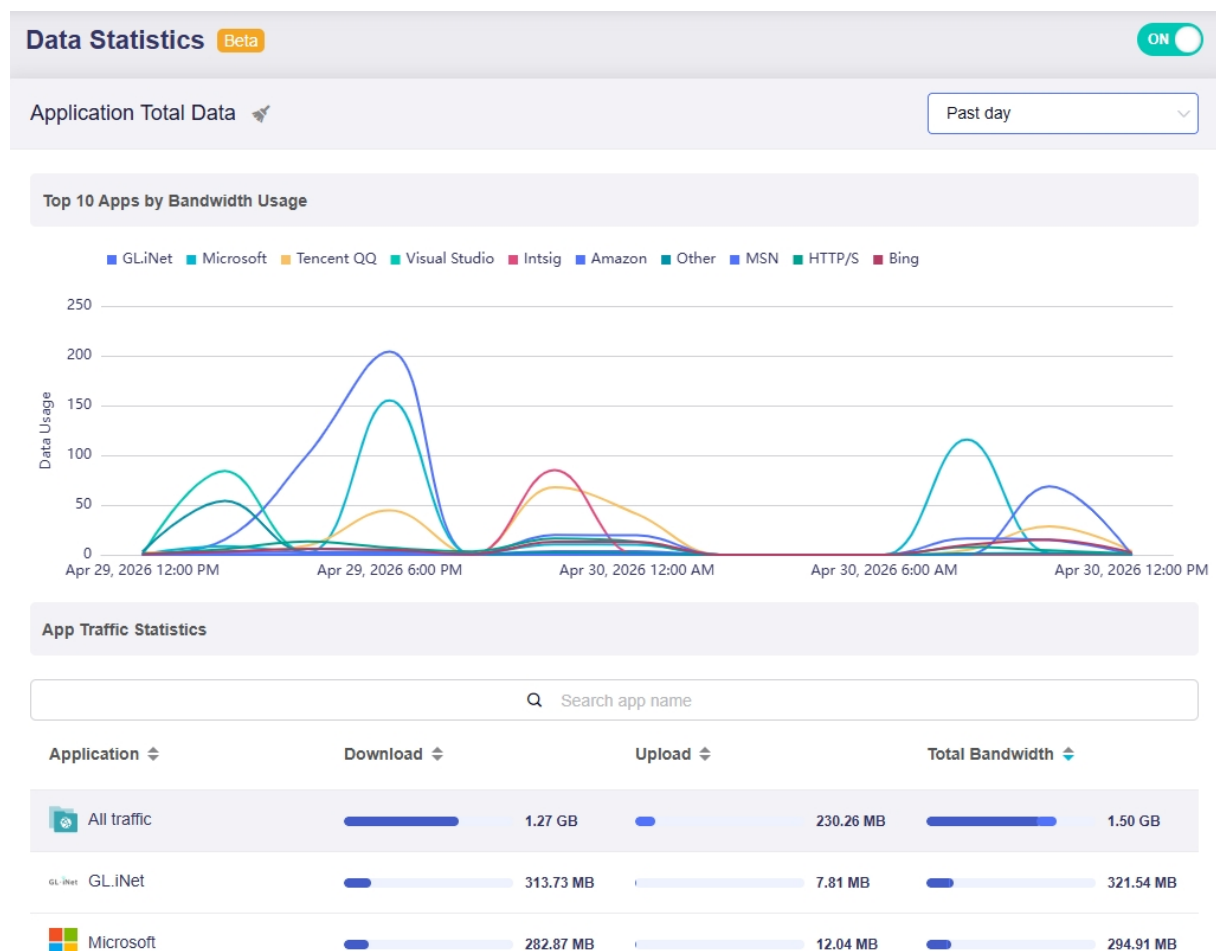
Data Statistics provides an intuitive traffic dashboard that identifies network usage by application and protocol. It supports viewing 1-hour, 1-day, and 7-day historical trends, displays usage rankings, monitors per-device traffic, and allows one-click blocking of unwanted apps.

Note:

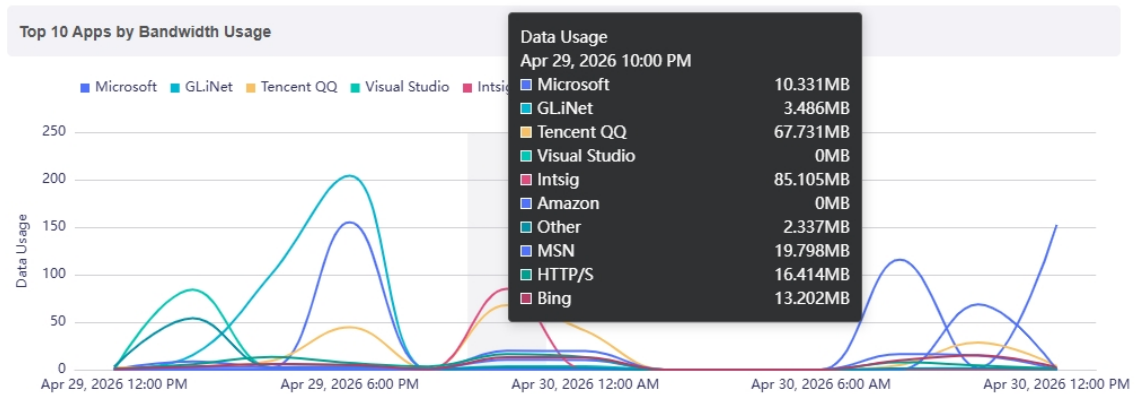
1. Data Statistics will not take effect when the router is in Drop-in Gateway mode.
2. Data Statistics cannot work with Network Acceleration. Enabling Data Statistics will automatically disable Network Acceleration to ensure stable performance.

12.2.1 Quick Setup

Log in to the router's web admin panel and navigate to **FLOW CONTROL > Data Statistics**. Toggle the switch in the upper right to view the **Application Total Data**.



- **Top 10 Apps by Bandwidth Usage:** It presents a time-based trend chart (e.g., for the past day) to show the bandwidth consumption of the top 10 applications over the selected period. Hover your mouse over the chart to view data usage of the top 10 bandwidth consuming apps at a specific time.



- **App Traffic Statistics:** It displays detailed traffic metrics for each application, including Download, Upload, and Total Bandwidth data. Search for specific apps in the search bar if needed. You can click the sort arrow next to the column header to sort the list in ascending or descending order.

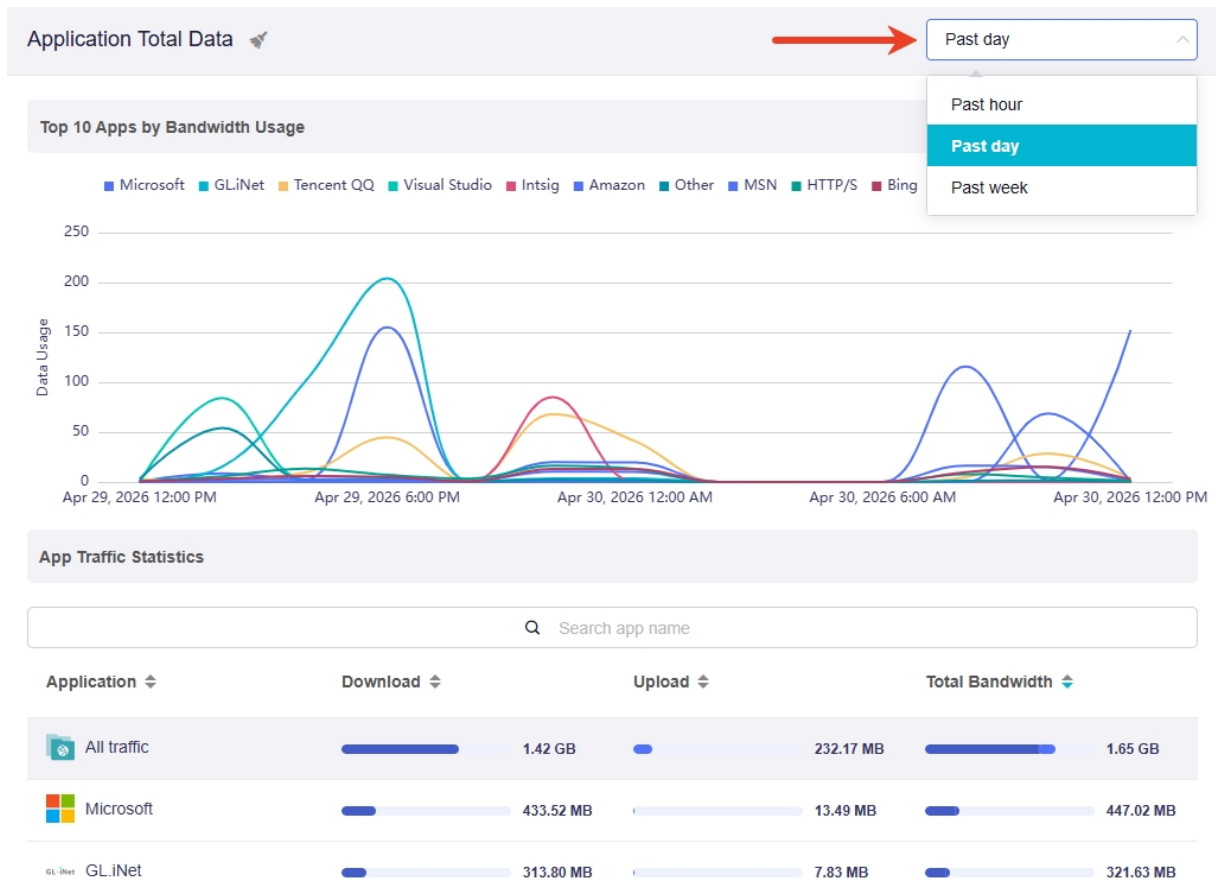
App Traffic Statistics					
Search app name					
Application	Download	Upload	Total Bandwidth		
All traffic	1.42 GB	232.01 MB	1.65 GB		
Microsoft	433.52 MB	13.49 MB	447.01 MB		
GLiNet	313.73 MB	7.82 MB	321.55 MB		
Tencent QQ	155.76 MB	6.57 MB	162.32 MB		
Visual Studio	83.95 MB	4.01 MB	87.96 MB		
Intsig	13.59 MB	71.51 MB	85.11 MB		
Amazon	60.63 MB	8.15 MB	68.78 MB		

12.2.2 Data Storage Rules

1. Traffic statistics are saved to RAM every 15 seconds and stored in flash every 1 hour. Frequent flash writes are avoided to protect flash memory lifespan.
2. A soft reboot will not cause data loss. The system first writes data from RAM to flash before restarting.
3. A hard reboot (unplugging and replugging the power) or a firmware upgrade (retaining settings) may result in data loss of up to the most recent hour.

12.2.3 Switch Time Range

You can switch the time range between Past hour, Past day, and Past week if needed.



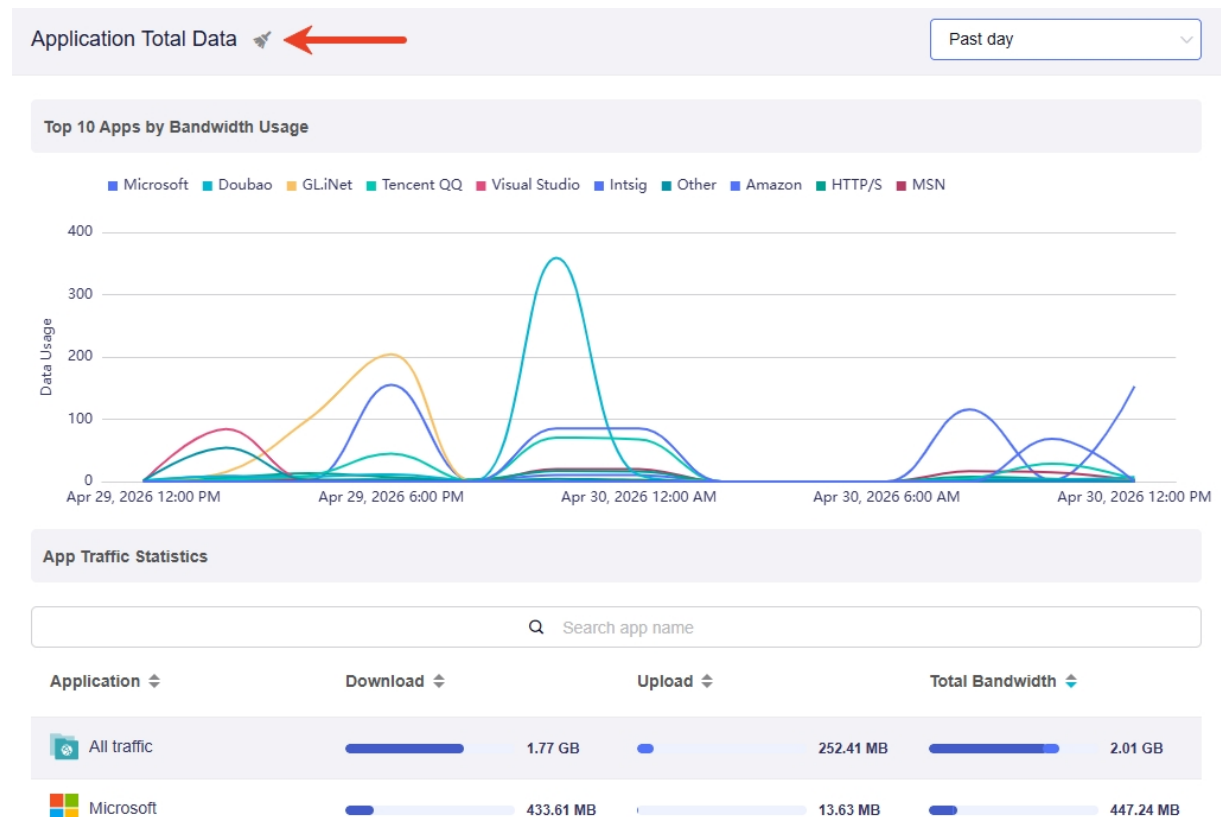
The time range you choose determines how the data is displayed:

- **For a closer look (e.g., Past Hour):** The chart shows fine-grained, real-time fluctuations. Peaks are taller and drops are steeper, making it easy to spot sudden spikes in bandwidth usage.

- **For a broad overview (e.g., Past Day or Past Week):** The chart condenses the data into a longer timeline. The curves become smoother, showing the general traffic trend rather than every small change.

12.2.4 Clear Statistics

Click the broom icon in the upper left corner to clear statistics if needed.



After clearing, the page will display no data. Wait a moment for new statistics to populate.

12.3 Content Filter

Content Filter is an intelligent online safety feature powered by DPI classification. It blocks harmful and malicious websites automatically to keep your network clean and secure, and also supports custom rules to block specific apps, domains, or IP addresses.

Note:

1. Content Filter will not take effect when the router is in Drop-in Gateway mode.
2. Content Filter cannot work with Network Acceleration. Enabling Content Filter will automatically disable Network Acceleration to ensure stable performance.

Log in to the router's web admin panel and navigate to **FLOW CONTROL > Content Filter**. Toggle the switch in the upper right corner, customize blocked content, then click **Apply**.

Content Filter Beta

 When enabled, your router automatically blocks adult, gambling, and malware, creating a clean, safe online environment for your family.

Enable



BLOCKED TOTAL

0

BLOCKED TODAY

0

Blocked Apps List (3)

[Edit App](#)



Gambling



Adult



Malware



App recognition incorrect ? [Submit feedback](#)

Blocked Domain / IP List (0)

1

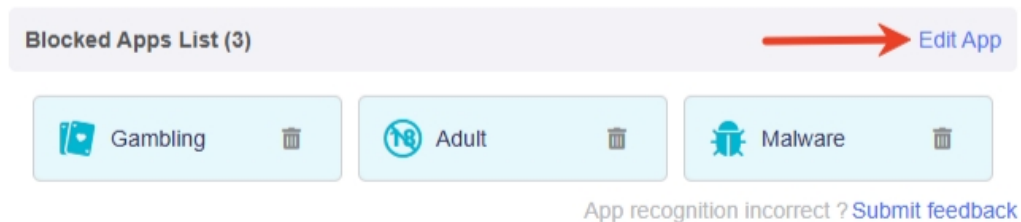
e.g. google.com

e.g. 192.168.8.0/24

e.g. 192.168.10.10

This page consists of two parts:

- **Blocked Apps List:** This section includes three pre-selected categories: Gambling, Adult, and Malware. When enabled, any websites, services or apps related to these three categories will be blocked. You can click **Edit App** to add other categories (e.g., Game, Social Media, Shopping) if needed.



- **Blocked Domain / IP List:** This section allows you to manually enter specific domains (e.g., google.com), CIDR range (e.g., 192.168.8.0/24), or IP addresses (e.g., 192.168.10.10) to block access to them. The list supports up to 10000 entries. Enter the domains or IP addresses you want to block, then click **Apply**.

The screenshot shows the 'Blocked Domain / IP List (0)' section. It has a header bar with the title 'Blocked Domain / IP List (0)'. Below the header is a large text input area. On the left side of the input area, there is a vertical list of numbers, with '1' currently selected. Inside the input area, there are example entries: 'e.g. google.com', 'e.g. 192.168.8.0/24', and 'e.g. 192.168.10.10'. At the bottom right of the input area, there is a character count '0/10000'. Below the input area is a blue 'Apply' button.

12.4 QoS

QoS (Quality of Service) optimizes bandwidth allocation by prioritizing latency-sensitive traffic such as video calls and gaming during network congestion, reducing latency and enhancing overall network performance.

Note:

1. This feature only affects traffic passing through the router when it operates as a gateway, including local client traffic and VPN client traffic. It does not apply to inbound traffic when the router acts as a VPN server.
2. QoS will not take effect when the router is in Drop-in Gateway mode.
3. QoS and SQM cannot be enabled simultaneously.
4. QoS cannot work with Network Acceleration. Enabling QoS will automatically disable Network Acceleration to ensure stable performance.

Log in to the router's web admin panel, go to **FLOW CONTROL > QoS** and enable it. Set your maximum upload and download speeds (input range: 1-10000) for traffic scheduling. Match them to your actual internet bandwidth for the best results.

Quality of Service

When enabled, your router prioritizes bandwidth for critical applications (e.g., video calls, online classes, gaming) during network congestion, ensuring smooth performance even during peak network usage.

This applies to local client traffic and traffic routed through VPN Client tunnels, but does not apply to traffic received when the router is acting as a VPN Server.

Enable



Upload ⓘ

62.5MB/s ≈

500

Mbps

Download ⓘ

125MB/s ≈

1000

Mbps

Tip: Values entered in the input field are in **Mbps** (megabits per second). The equivalent MB/s (megabytes per second) is displayed for your reference.

Then set priorities for different applications. The router will allocate bandwidth accordingly.

Upload ⓘ

62.5MB/s ≈

500

Mbps

Download ⓘ

125MB/s ≈

1000

Mbps

Allocate bandwidth based on application priority.

☒ Meeting Priority
Prioritize video conferences for a smooth and uninterrupted experience.

☐ Gaming Priority
Prioritize online games to avoid lag and packet loss.

☐ Web Browsing Priority
Prioritize web browsing for faster and smoother loading.

☐ Video Streaming Priority
Prioritize video streaming for buffer-free playback and HD quality.

☐ Customize
Customize application priority.

Pre-Set Up

Apply

12.5 SQM

SQM (Smart Queue Management) intelligently manages your router's network traffic to minimize latency and "bufferbloat", ensuring smoother gaming and voice calls.

Note:

1. This feature only affects traffic passing through the router when it operates as a gateway, including local client traffic and VPN client traffic. It does not apply to inbound traffic when the router acts as a VPN server.
2. Since SQM is resource-intensive, it works best for low-bandwidth or congested networks. Enabling it on high-speed connections may reduce peak throughput.
3. SQM will not take effect when the router is in Drop-in Gateway mode.
4. SQM and QoS cannot be enabled simultaneously.
5. SQM cannot work with Network Acceleration. Enabling SQM will automatically disable Network Acceleration to ensure stable performance.

Log in to the router's web admin panel, go to **FLOW CONTROL > SQM** and enable it. Set your maximum upload and download speeds first (input range: 1-10000) for traffic scheduling. Match them to your actual internet bandwidth for the best results.

Smart Queue Management



When enabled, your router intelligently manages traffic to minimize latency and "bufferbloat" for smoother gaming and calls. Since SQM is resource-intensive, it is best suited for low-bandwidth or congested networks; on high-speed connections, enabling this may lead to a reduction in peak throughput performance.

SQM affects traffic passing through the router as a gateway, including VPN Client traffic, but does not affect incoming traffic when the router is operating as a VPN Server.

Enable



Upload

1-10000

Mbps

Download

1-10000

Mbps

Queue Rule

cake



For **Queue Rule**, two options are available:

- **cake**: Smart, automatic traffic shaping with superior overall latency control (recommended).
- **fq_codel**: Simple, efficient fair queueing with basic latency reduction.

Tip: A difference between QoS and SQM settings is that the QoS allows you set the application priorities, with the router allocating bandwidth accordingly; while the SQM allows you to select a queue rule.

12.6 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.

Follow the steps below to set up your Parental Control.

1. Log in to the router's web Admin Panel and go to **FLOW CONTROL -> Parental Control**. Ensure the router time is accurate.

Parental Control

Through Parental Control, you can set exclusive internet-blocking time periods for your child's commonly used devices (e.g., smartphones and tablets), block inappropriate apps and websites, and fully safeguard your child's sleep quality and healthy online environment. You can also use the third-party service [Bark](#) for more diverse internet management.

Enable ☐

Router Time

Mon, Jun 1, 2026 2:24 PM (UTC+08:00)

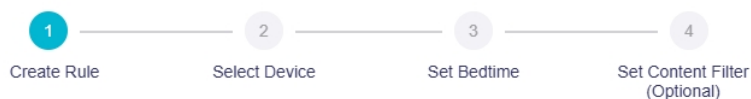
Apply

If not, go to **SYSTEM -> Time Zone** to synchronize it first.

2. Enable Parental Control and click **Apply**.
3. You will see a rule list as follows. Click **Add a New Rule**.

Rules					
Rule Name	Device	Bedtime	Content Filter	Enable	Action
No Data					
+ Add a New Rule					

4. In the pop-up window, create a rule and set a custom name, then click **Next**.



Create a rule for your child

Rule Name
Child's name recommended

5. Select your child's device, then click **Next**.
Devices will only appear on this page if they are connected to the router via Wi-Fi or Ethernet. Cyan indicates online status, while grey indicates offline status.



Select your child's device

Selected 2 / Total 6

iPhone MAC:	Samsung MAC:
LAPTOP-Carry MAC:	GL-INET-08 MAC: self
Watch MAC:	Anna's Tablet MAC:

Back

Next

Tip: If you want to distinguish the connected devices, go to **CLIENTS** page and customize device names.

- Set bedtime for your child's device, then click **Next**. The internet on the selected device(s) will be unavailable during this period. The bedtime is the same for every day by default.



Set bedtime for your child's device

i You can set internet-blocking time periods according to your child's schedule. During this period, the internet on the child's devices will be automatically disconnected to protect their peaceful sleep.

Enable Bedtime Schedule ☒

Day Every Day

Every Day 🕒 22:00 to 🕒 07:00 Next Day

Back Next

If you want to set different bedtimes for each day of the week, select **Customize Days** and set different bedtimes, then click **Next**.

- Select content filter.

Three categories have been selected by default: **Gambling**, **Malicious Content**, and **Sexual Content**. You may select other categories if needed, such as **Games**, **Shopping**, **Social Media**, **Entertainment**, etc.



Set content filter for your child's device

Selected 3 / 422

i Block inappropriate apps, harmful website content, and reduce distractions. It is suitable for various scenarios such as online education and entertainment.

☐ Show selected item only

Gambling ✓

Malicious Content ✓

Sexual Content ✓

> Games (79)

Select All

> Shopping (57)

Select All

> Social Media / Entertainment (283)

Select All

Advance Settings ▾

Back

Finish

If a certain app you want to block is hard to find out, you may search it on the top.

✓

✓

✓

4

Create Rule

Select Device

Set Bedtime

Set Content Filter (Optional)

Set content filter for your child's device

Selected 3 / 422

Block inappropriate apps, harmful website content, and reduce distractions. It is suitable for various scenarios such as online education and entertainment.

☐ Show selected item only

> Shopping (1)

Select All

SnapAV

> Social Media / Entertainment (3)

Select All

Snapchat

Snaptube

TeamSnap

- If you need to block certain domains, click **Advanced Settings** at the bottom right.



Set content filter for your child's device

Selected 3 / 422

i Block inappropriate apps, harmful website content, and reduce distractions. It is suitable for various scenarios such as online education and entertainment.

Search Content or App Name

☐ Show selected item only

Gambling



Malicious Content



Sexual Content



> **Games (79)**

Select All

> **Shopping (57)**

Select All

> **Social Media / Entertainment (283)**

Select All

[Advance Settings](#) ▾

Back

Finish

Enter domains manually, then click **Finish**.

Manually Block Domain (0)

1 e.g. [tcp;;443;weibo;;]
e.g. www.4399.com

0/10000

Back

Finish

9. The rule is now added. The list shows the rule name, connected device count, bedtime schedule, filtered content and rule status (enabled/disabled).

Rules					
Rule Name	Device	Bedtime	Content Filter	Enable	Action
Anna 	2 Devices	Every Day 22:00 - 07:00	Blocked 82 items		...
+ Add a New Rule					

Chapter 13

Security

This chapter manages network security, such as port forwarding, admin access settings, and NAT mode.

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 **SECURITY > Port Forwarding > DMZ** section.
2. Toggle on **Enable DMZ**. Select the Priority and DMZ Host IP from the drop-down list, and click **Apply**.

DMZ

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

Enable DMZ

☒

Priority

Highest

▼

DMZ Host IP

192.168.8.115

▼

Apply

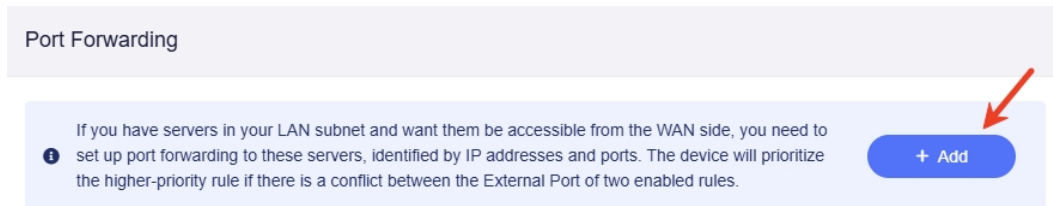
- **Priority:** Set it as Highest or Lowest. If the priority of the DMZ is higher than the port forwarding rules, all port forwarding rules will be invalidated. Otherwise, requests will be forwarded to the DMZ client device only if the accessed port has no corresponding port forwarding rule.
- **DMZ 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 **SECURITY > 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**.

Add New Port Forwarding Rule

Protocol	TCP/UDP
External Zone	WAN
External Port	
Internal Zone	LAN
Internal IP	
Internal Port	
Description	Optional
Enable	☒

Cancel

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 ACL

ACL, short for Access Control List, lets you create rules to manage network traffic based on connection protocols, device addresses and ports. It controls whether to allow or block network access. If multiple ACL rules conflict, the system applies the one with higher priority.

Different from Port Forwarding, ACL mainly allows or blocks network access for security purposes, while Port Forwarding redirects external traffic to specific devices on your local network to enable remote access to local services.

Follow the steps below to set up Access Control List if needed.

1. Log in to your router's web admin panel and go to **SECURITY > ACL**. Click the **Add Rule** button on the right.

ACL

 ACL can control network traffic based on rules such as protocol, destination IP address, source IP address, and port number. If there is a conflict between two enabled ACL rules, the device will prioritize the higher-priority rule.

+ Add Rule

2. Create your ACL rule in the pop-up window, then click **Apply**.

Add an ACL rule

Name	
Protocol	Any
IP Type	IPv4 & IPv6
Source Zone	LAN
Source Address	Optional
Destination Zone	WAN
Destination Address	Optional
Action	Accept Block

Enable



Cancel

Apply

- **Name:** Enter a custom name for the rule.
- **Protocol:** Specify which type of network traffic the rule applies to. Select a connection protocol from Any, TCP, UDP, TCP+UDP, and ICMP.
- **IP Type:** Define the IP address format for network traffic. Select the IP type from IPv4 & IPv6, IPv4, and IPv6.
- **Source Zone:** Select the network zone where traffic originates. Available options: LAN, Guest, IoT, and WAN.
- **Source Address:** (Optional) Restrict the rule to specific source devices or IP addresses. You may select a source address from the drop-down list.
- **Destination Zone:** This is where the network traffic is heading to. Select the target network zone. Available options: LAN, Guest, IoT, and WAN.
- **Destination Address:** (Optional) Restrict the rule to specific destination devices or IP addresses. You may select a destination address from the drop-down list.
- **Action:** Choose to Accept or Block network traffic matching this rule.
- **Enable:** Toggle to enable or disable this rule.

13.3 Admin Access

Log in to your router's web admin panel and navigate to **SECURITY > Admin Access**. This page allows you to configure router local access, remote HTTPS/SSH access, and manage open ports on the router, protecting your router and network from unauthorized access.

13.3.1 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.

Access Control

Admin Panel

HTTP Port

HTTPS Port

Force HTTPS



Auto-Logout Time ⓘ

Minutes

LuCI

HTTP Port

HTTPS Port

Force HTTPS



SSH

Enable SSH



SSH Port

Apply

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.

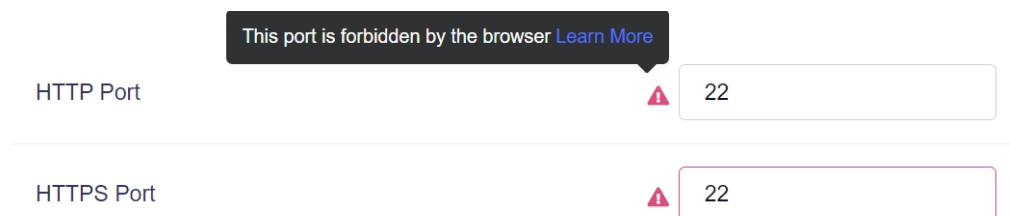
- **HTTP Port:** Defaults to 8080, for unencrypted HTTP access to the LuCI interface.
- **HTTPS Port:** Defaults to 8443, for secure HTTPS access to the LuCI interface.
- **Force HTTPS:** When enabled, access to the LuCI interface is enforced to use a secure HTTPS connection.

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".



The screenshot shows a web interface for configuring ports. There are two input fields: "HTTP Port" and "HTTPS Port". Both fields contain the number "22". Above the "HTTP Port" field, there is a dark grey tooltip with the text "This port is forbidden by the browser" and a blue link "Learn More". To the right of each input field, there is a red warning triangle icon.

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.

13.3.2 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.

Remote Access Control

Allow Ping from WAN

HTTPS Remote Access

SSH Remote Access

Allow Remote Access only from Specific IPs ⓘ

Apply

- **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.

Allow Remote Access only from Specific IPs ⓘ

IP Address List

+ Add an IP Address

192.168.8.1

example

...

13.3.3 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.

Open Ports on Router

 For security reasons, the services that you install on the device are only opened to its LAN network. If you want them to be accessible from the WAN network, you need to open ports for these services on the WAN.

+ Add

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

Add New Open Port

Protocol

TCP/UDP

Port

Description

Optional

Enable

☒

Cancel

Apply

- **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.

13.4 NAT Mode

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

NAT Mode

Enable Full Cone NAT ⓘ

☐

Enable SIP ALG ⓘ

☐

Apply

- **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

Applications

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

14.1 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.

Plug-insManage Sources

Filter

Q Search Package

Refresh

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name	Version	Size	Action
464xlat	12	5.05 KB	install
6in4	26	2.47 KB	install
6rd	10	3.79 KB	install
6to4	13	1.82 KB	install
ControlAppC	1.0	30.71 KB	install
UDPSpeeder	20210116.0-2	76.72 KB	install
acl	2.2.53-1	20.39 KB	install
acme	3.0.6-1	54.02 KB	install

Free space: 84.54 % (6.76 GB)

Last Refresh Time: Thu, Jan 15, 2026 4:02 PM (UTC+08:00)

< 1 2 3 4 ... 1101 >

Go

Note:

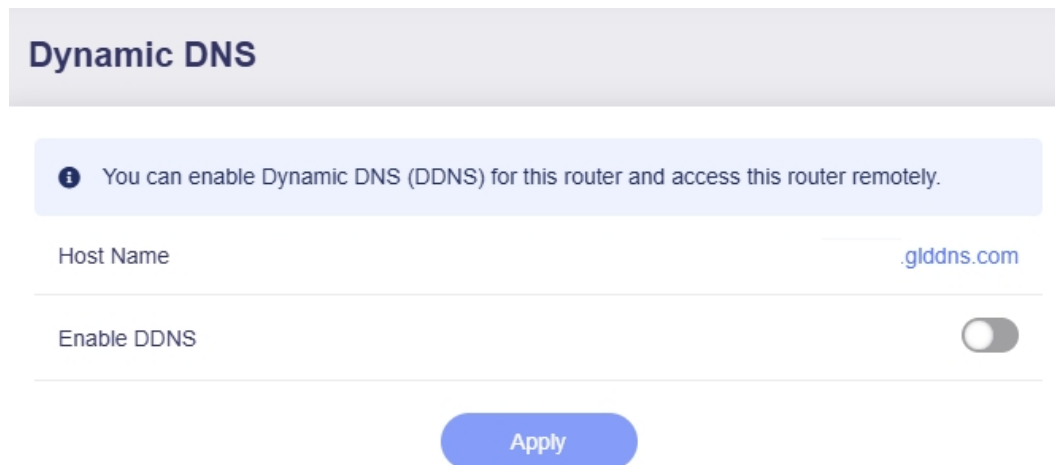
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

14.2 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.

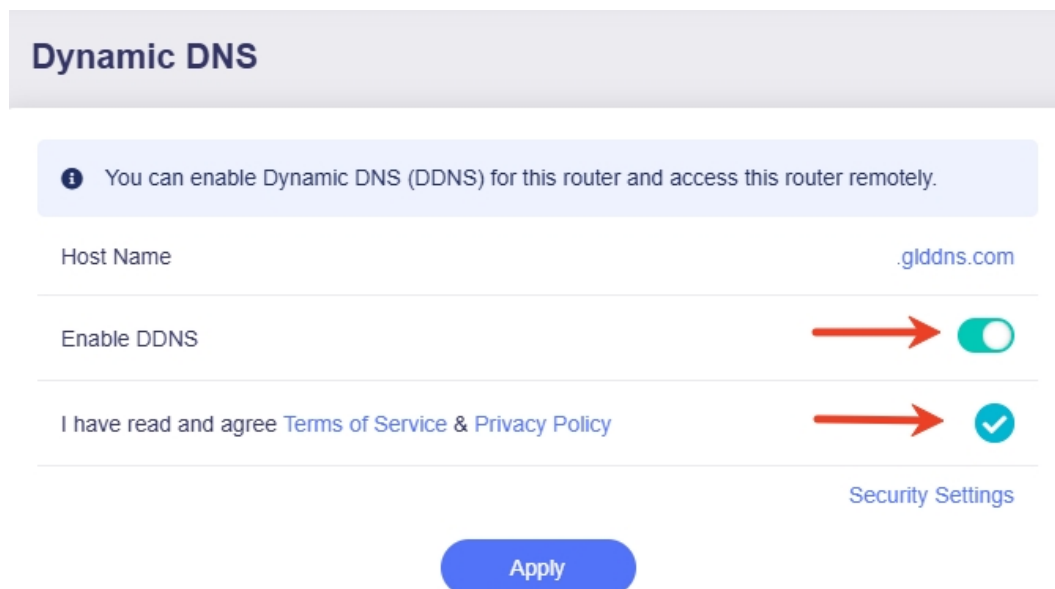
14.2.1 Enable DDNS

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



The screenshot shows the 'Dynamic DNS' configuration page. At the top is a header 'Dynamic DNS'. Below it is an information box stating: 'You can enable Dynamic DNS (DDNS) for this router and access this router remotely.' Underneath, there is a 'Host Name' field containing '.glddns.com'. Below that is a toggle switch for 'Enable DDNS', which is currently turned off. At the bottom center is a blue 'Apply' button.

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



This screenshot shows the 'Dynamic DNS' configuration page after the first step. The 'Host Name' field still contains '.glddns.com'. The 'Enable DDNS' toggle switch is now turned on, indicated by a red arrow pointing to it. Below the toggle, there is a checkbox labeled 'I have read and agree Terms of Service & Privacy Policy', which is also checked, with a red arrow pointing to it. In the bottom right corner, there is a link for 'Security Settings'. At the bottom center is a blue 'Apply' button.

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

Dynamic DNS

i You can enable Dynamic DNS (DDNS) for this router and access this router remotely.

There may be a delay of up to 10 minutes in record synchronization between DNS servers.

i This may cause you to be unable to access through the DDNS domain name immediately after you have just enabled it or your public IP has changed. [DDNS Test](#)

Host Name [.glddns.com](#)

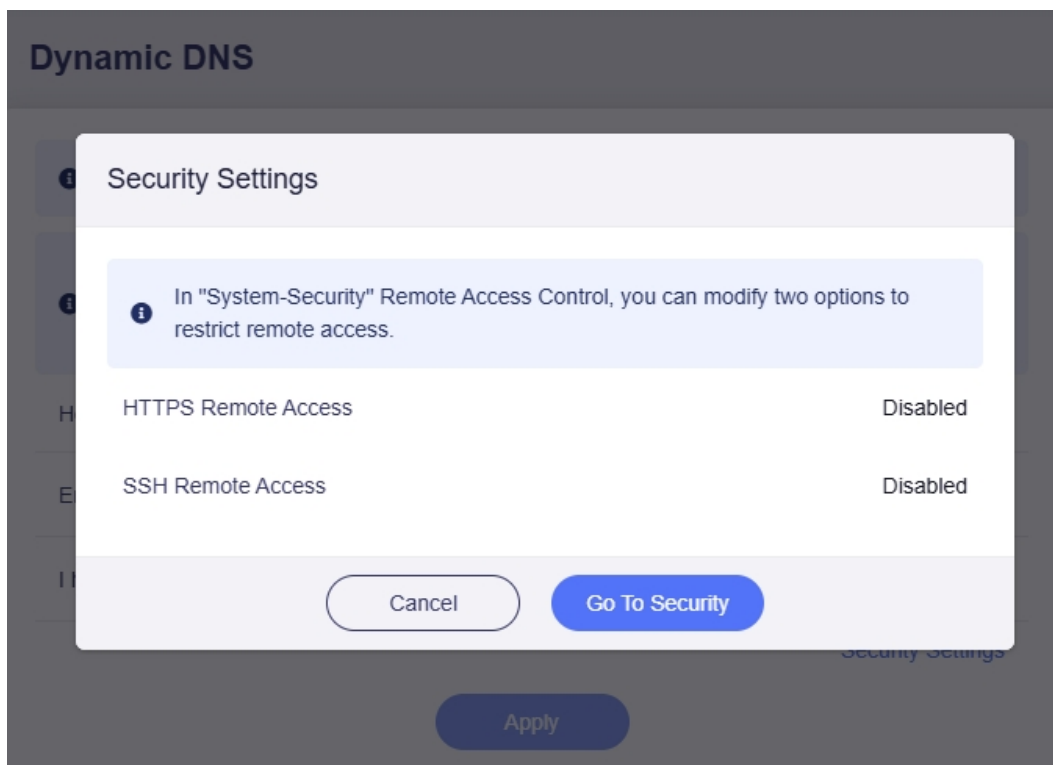
Enable DDNS ☒

I have read and agree [Terms of Service & Privacy Policy](#) ☒

[Security Settings](#)

Apply

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**.

Remote Access Control

Allow Ping from WAN

HTTPS Remote Access

SSH Remote Access

Allow Remote Access only from Specific IPs ⓘ

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.

14.2.2 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**.

Dynamic DNS

i You can enable Dynamic DNS (DDNS) for this router and access this router remotely.

There may be a delay of up to 10 minutes in record synchronization between DNS servers.
i This may cause you to be unable to access through the DDNS domain name immediately after you have just enabled it or your public IP has changed. [DDNS Test](#) 

Host Name

[.glddns.com](#)

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.

DDNS Test

×

⚠ The IP address from DDNS domain resolution is not the same as the WAN IP of the device.
You need an Internet Public IP address to use Dynamic DNS.

i If this router is behind NAT, you may need to set up port forwarding on your ISP router.
If you have VPN Client enabled, please disable "Services from GL.iNet Use VPN" in the global options.

IP address from DDNS Domain Resolution

IPv4	205.185.113.19
------	----------------

WAN Interface IP address

Ethernet	192.168.5.135
----------	---------------

Method 2. Use commands

1. Use nslookup command *nslookup xxxxxxx.glddns.com 8.8.8.8* to obtain the mapping between domain name and IP address. Below is an example of Beryl AX GL-MT3000.

```
root@GL-MT3000:~#  
root@GL-MT3000:~# nslookup      ***** .glddns.com 8.8.8.8  
Server:                8.8.8.8  
Address:                8.8.8.8#53  
  
Name:                   ***** .glddns.com  
Address 1: 183.178.10.100
```

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

14.2.3 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**.

Dynamic DNS

i You can enable Dynamic DNS (DDNS) for this router and access this router remotely.

Host Name	.glddns.com
Enable DDNS	 ☒
I have read and agree Terms of Service & Privacy Policy	 ☒

[Security Settings](#)

Apply

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

Remote Access Control

Allow Ping from WAN	☐
HTTPS Remote Access	☐
SSH Remote Access	☐

Apply

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

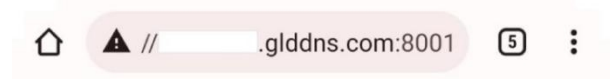
Remote Access Control

Allow Ping from WAN	☐
HTTPS Remote Access	☒
SSH Remote Access	☐
Allow Remote Access only from Specific IPs 	☐

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).

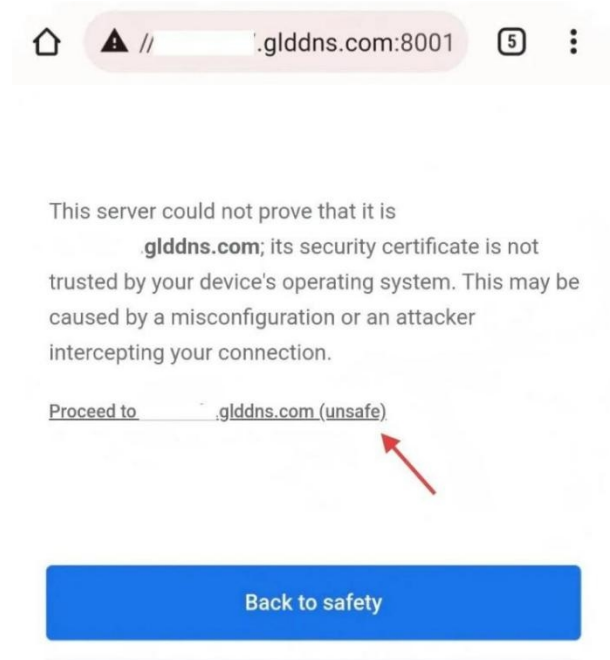


Your connection is not private

Attackers might be trying to steal your information from [redacted].glddns.com (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

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



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

14.2.4 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**.

Dynamic DNS

i You can enable Dynamic DNS (DDNS) for this router and access this router remotely.

Host Name	.glddns.com
Enable DDNS	 ☒
I have read and agree Terms of Service & Privacy Policy	 ☒

[Security Settings](#)

Apply

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

Remote Access Control

Allow Ping from WAN	☐
HTTPS Remote Access	☐
SSH Remote Access	☐

Apply

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

Remote Access Control

Allow Ping from WAN

HTTPS Remote Access

SSH Remote Access

Allow Remote Access only from Specific IPs

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).

14.3 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.

Brume 3 is equipped with 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: The power consumption of USB hard drive is quite high. Use it with an external power supply, otherwise it may cause malfunction.

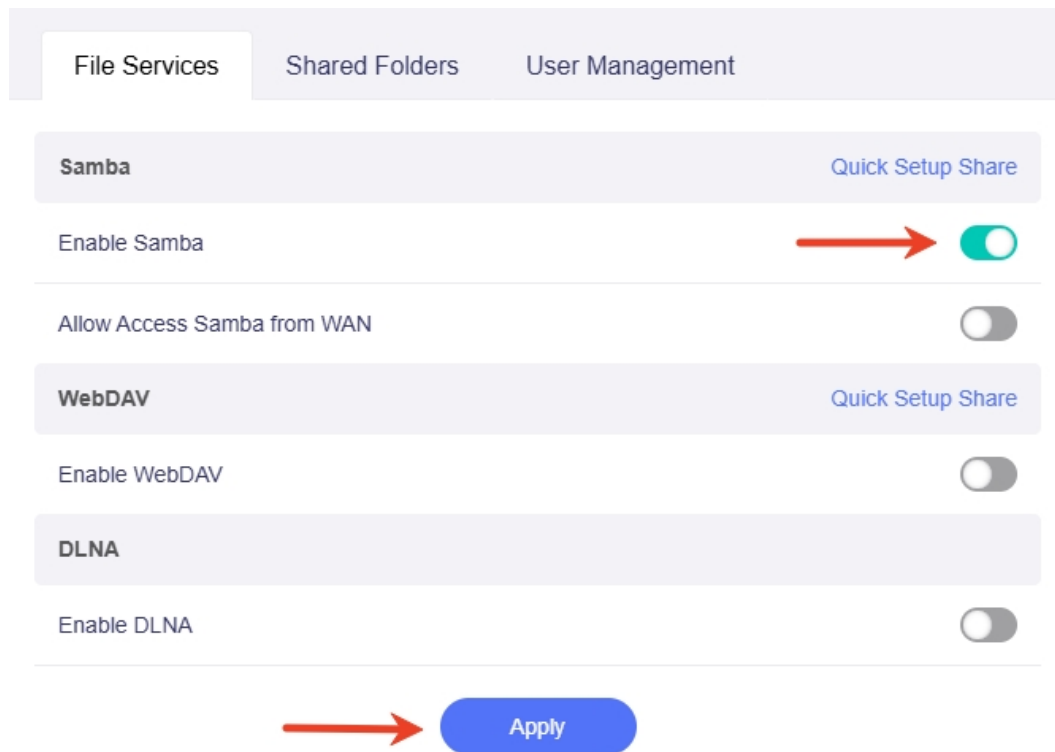
14.3.1 Connect Storage

1. Connect your storage device to the router.
 - 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.

Disk Management 				
Disk Name	Type	Format	Disk Size	Eject
Ventoy (disk1_part1)	USB Flash Drive	EXFAT	7.29 GB free of 14.40 GB	

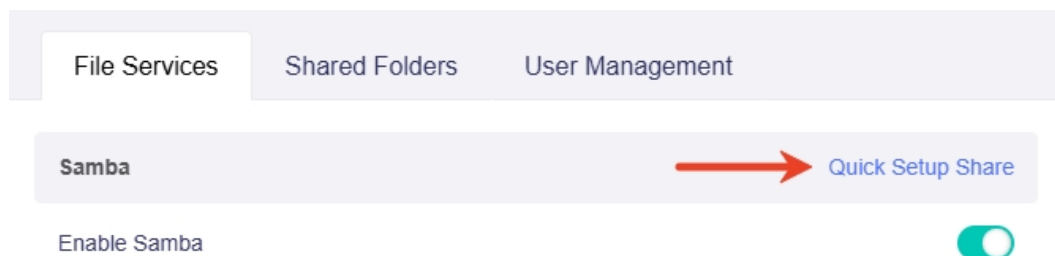
14.3.2 Set Up Samba

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



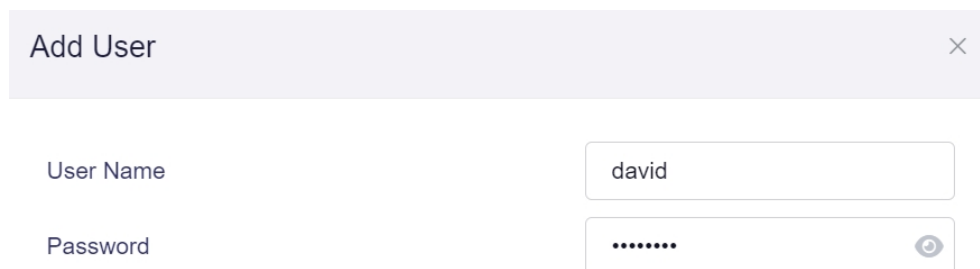
The screenshot shows the 'File Services' tab selected in the top navigation bar. Below it, there are three sections: Samba, WebDAV, and DLNA. Each section has a 'Quick Setup Share' link. The 'Samba' section has a toggle switch for 'Enable Samba' which is turned on, indicated by a red arrow. Below it is a toggle for 'Allow Access Samba from WAN' which is turned off. The 'WebDAV' section has a toggle for 'Enable WebDAV' which is turned off. The 'DLNA' section has a toggle for 'Enable DLNA' which is turned off. At the bottom, there is a blue 'Apply' button with a red arrow pointing to it.

- **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.



The screenshot shows the 'File Services' tab selected. The 'Samba' section is highlighted, and a red arrow points to the 'Quick Setup Share' link. Below it, the 'Enable Samba' toggle switch is shown, which is now turned on.

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



The screenshot shows the 'Add User' dialog box. It has a title bar with 'Add User' and a close button (X). Below the title bar, there are two input fields: 'User Name' with the text 'david' and 'Password' with dots. There is an eye icon next to the password field to toggle visibility.

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

Add Shared Folder

▼ disk1_part1

qlogs_20260709_161408

qlogs_20260709_161458

qlogs_20260709_162031

Cancel

Next

- Set up the shared folder.

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 **Read-Write User**, then click **Apply**.

Shared Folder Settings

Path

/disk1_part1

Samba Settings

Share Name

disk1_part1

Anonymous Access

☐

Read-Write User

Read-only User

user1 ×

Back

Apply

Tip: For security reasons, it is not recommend to enable Anonymous Access.

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.

Folder Access Link



The folder has been shared. Use the following link to mount the folder as a network disk to your PC or Phone. [Learn More](#)

Windows SMB

\\192.168.8.1\disk1_part1

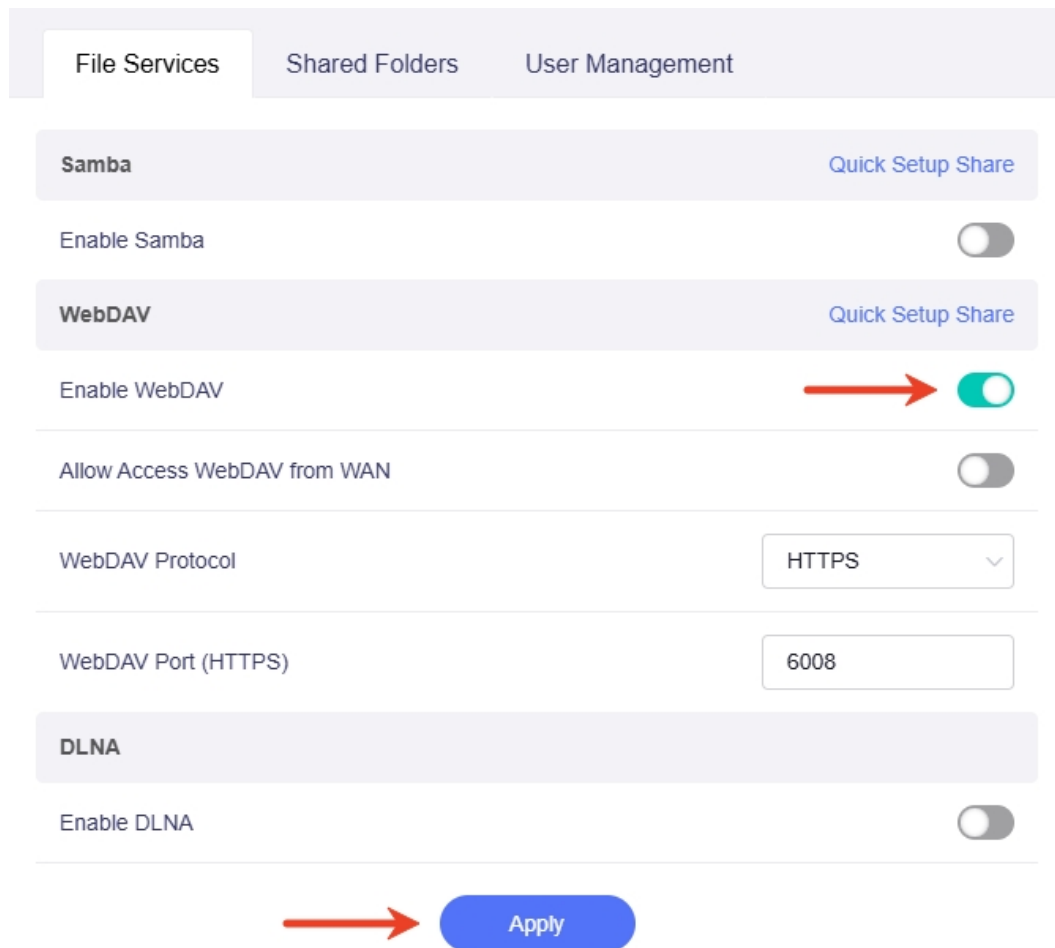
Unix-like Samba

smb://192.168.8.1/disk1_part1

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.

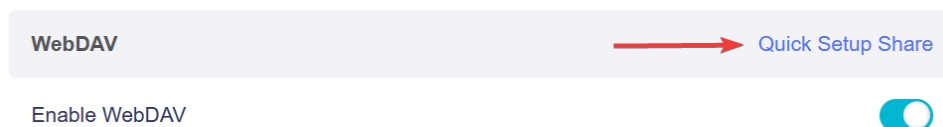
14.3.3 Set Up WebDAV

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



The screenshot shows the 'File Services' configuration page. At the top, there are three tabs: 'File Services', 'Shared Folders', and 'User Management'. The 'File Services' tab is active. Below the tabs, there are three main sections: 'Samba', 'WebDAV', and 'DLNA'. The 'WebDAV' section is highlighted. It contains the following settings: 'Enable WebDAV' (a toggle switch that is turned on, with a red arrow pointing to it), 'Allow Access WebDAV from WAN' (a toggle switch that is turned off), 'WebDAV Protocol' (a dropdown menu set to 'HTTPS'), and 'WebDAV Port (HTTPS)' (a text box containing '6008'). At the bottom of the 'WebDAV' section, there is a blue 'Apply' button with a red arrow pointing to it.

- **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.



The screenshot shows the 'WebDAV Quick Setup Share' dialog. It has a title bar 'WebDAV' and a 'Quick Setup Share' button with a red arrow pointing to it. Below the title bar, there is a toggle switch for 'Enable WebDAV' which is turned on.

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

Add User

User Name

david

Password

.....

- Click the triangle icon to show all folders. Select a folder for sharing. If you want to share the whole disk, click the disk name (e.g., disk1_part1).

Add Shared Folder

▼ disk1_part1

qlogs_20260709_161408

qlogs_20260709_161458

qlogs_20260709_162031

- Set up the shared folder.

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 **Read-Write User**, then click **Apply**.

Shared Folder Settings

Path

/disk1_part1

WebDAV Settings

Anonymous Access

Read-Write User

Read-only User

user1 x

Back

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.

Folder Access Link



The folder has been shared. Use the following link to mount the folder as a network disk to your PC or Phone. [Learn More](#)

HTTPS

https://192.168.8.1:6008/disk1_part1

Dav

dav://192.168.8.1:6008/disk1_part1

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.

14.3.4 Set Up DLNA

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

The screenshot shows the 'File Services' configuration page. It has three tabs: 'File Services', 'Shared Folders', and 'User Management'. Under 'File Services', there are three sections: 'Samba', 'WebDAV', and 'DLNA'. Each section has a 'Quick Setup Share' link and an 'Enable' toggle. The 'Enable DLNA' toggle is turned on, with a red arrow pointing to it. Below the 'DLNA' section, the 'Share Path' is set to '/disk1_part1' with a 'Modify' link. At the bottom of the page, there is a blue 'Apply' button, which is highlighted with a red arrow.

2. Modify the Share Path on the right if needed.

This is a close-up of the 'DLNA' configuration section. It shows the 'Enable DLNA' toggle is turned on. Below it, the 'Share Path' is set to '/disk1_part1', and the 'Modify' link next to it is highlighted with a red rectangle.

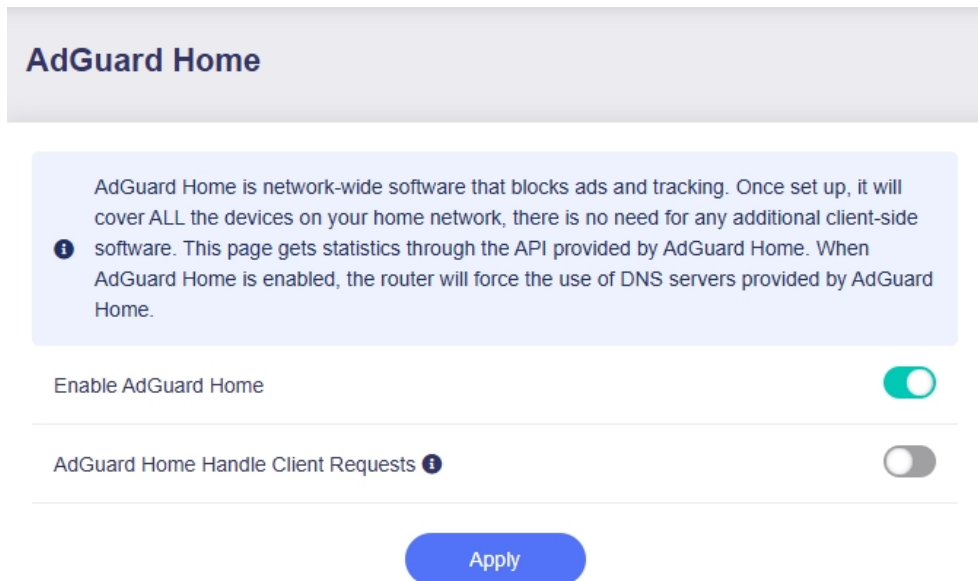
3. Connect your smart TV to the router. It will find the DLNA server automatically.

14.4 AdGuard Home

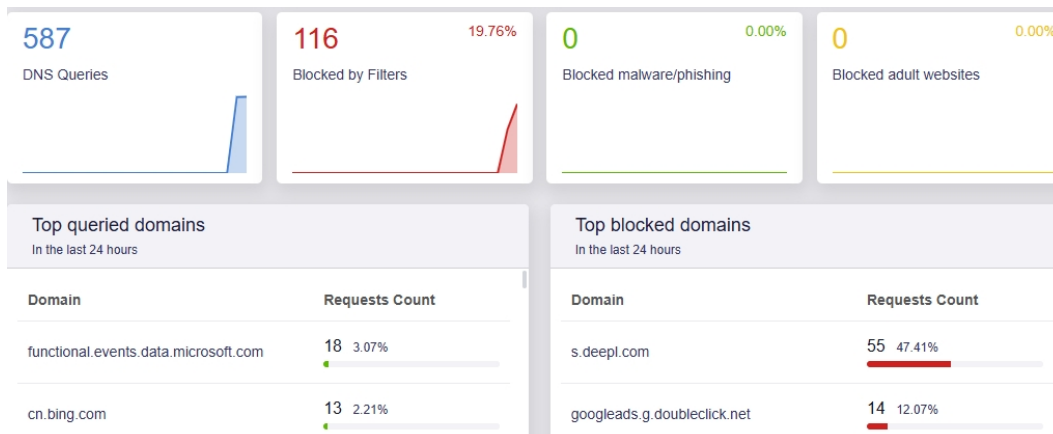
AdGuard Home is a network-wide ad-blocking and tracking-prevention software. Once set up, it will cover all client devices with no additional client-side software required.

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.



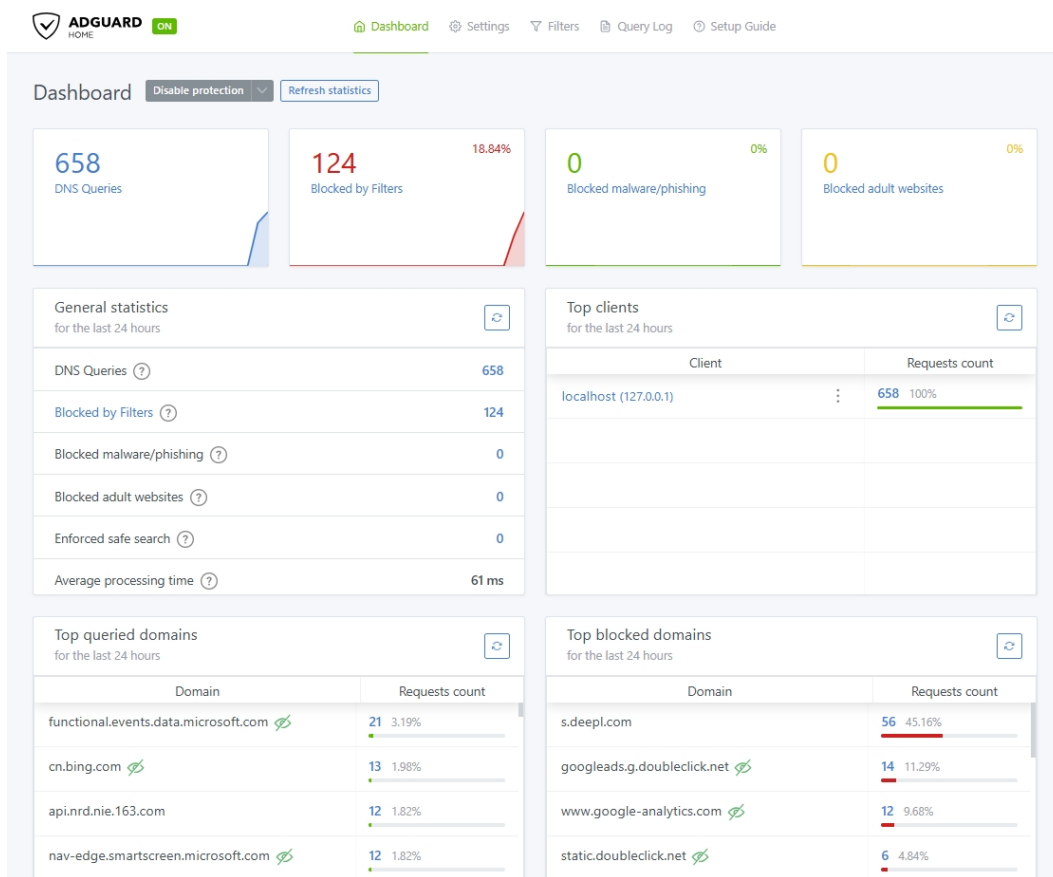
3. Click **Settings Page** to configure advanced settings for AdGuard Home.

AdGuard Home

AdGuard Home is network-wide software that blocks ads and tracking. Once set up, it will cover ALL the devices on your home network, there is no need for any additional client-side software. This page gets statistics through the API provided by AdGuard Home. When AdGuard Home is enabled, the router will force the use of DNS servers provided by AdGuard Home.

Please go to the [Settings Page](#) to perform advanced configuration of Adguard Home.

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



14.5 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.

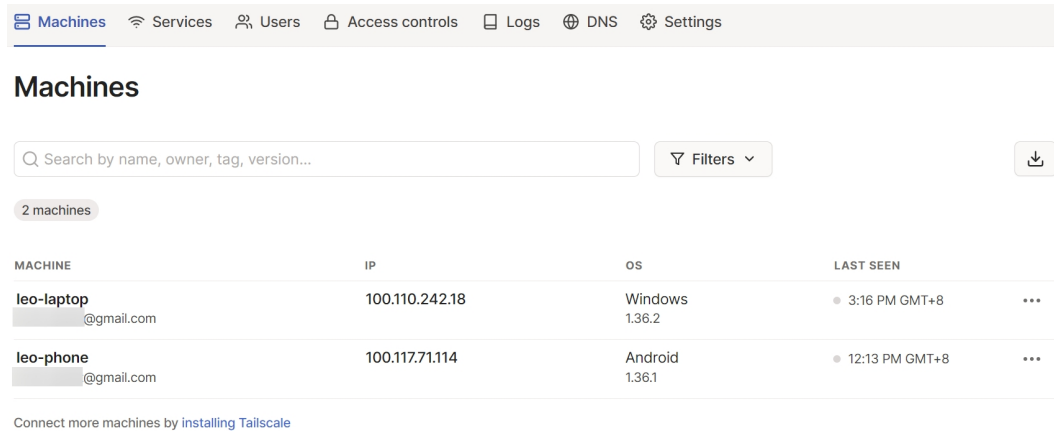
Note:

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.

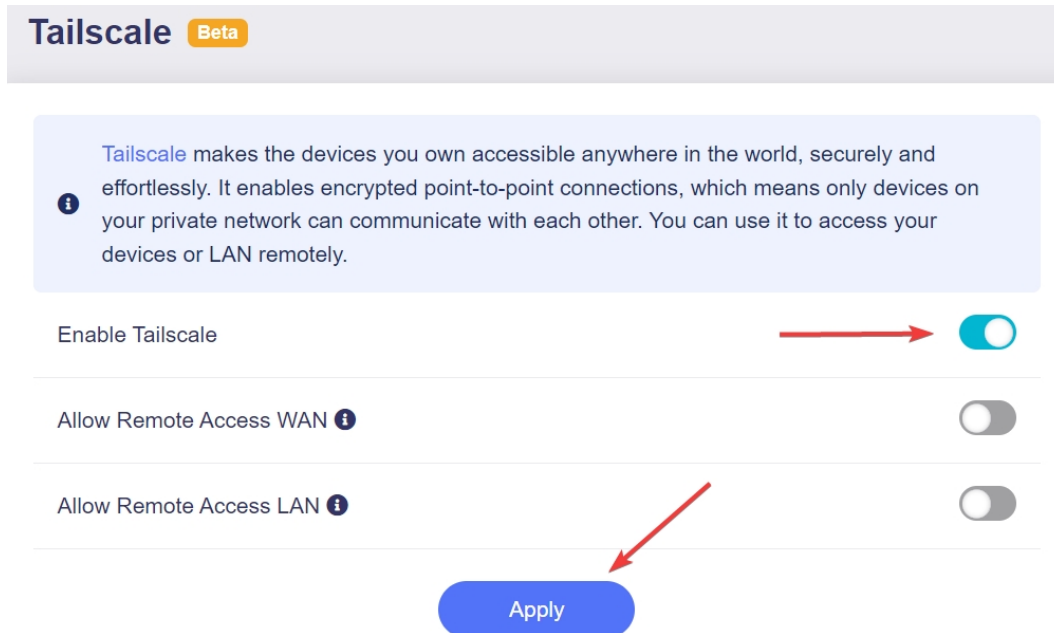
14.5.1 Set Up Tailscale

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**.

Tailscale Beta

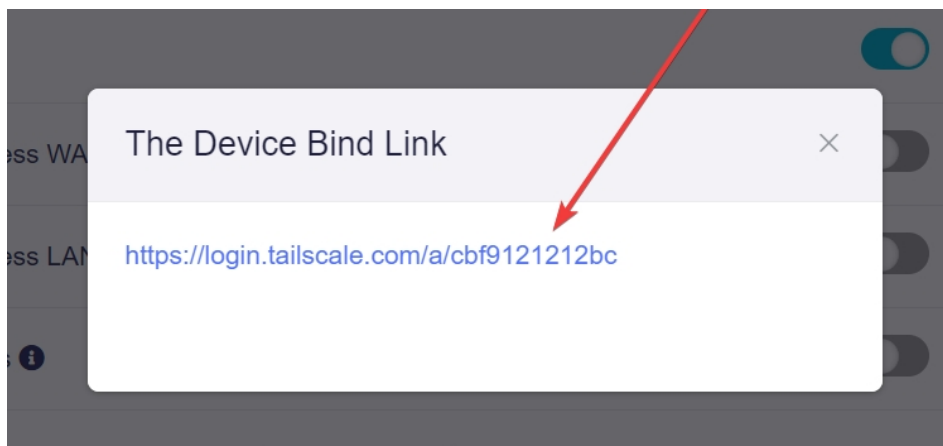
i Tailscale makes the devices you own accessible anywhere in the world, securely and effortlessly. It enables encrypted point-to-point connections, which means only devices on your private network can communicate with each other. You can use it to access your devices or LAN remotely.

The Tailscale service is enabled, but the device is not bound yet. Please bind this device to your Tailscale account using [The Device Bind Link](#).

Enable Tailscale



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**.



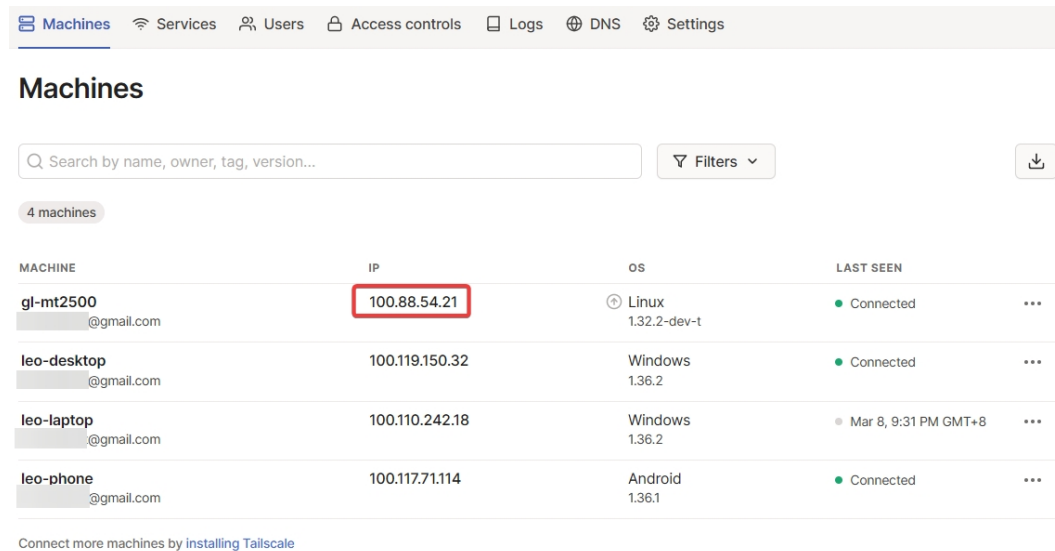
Connect device

Do you want to connect the device GL-MT2500 to the [redacted]@gmail.com tailnet? This may give the device access to other resources in your tailnet, based on ACLs.

► Device details

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.



Machines				
Search by name, owner, tag, version...				
4 machines				
MACHINE	IP	OS	LAST SEEN	
gl-mt2500 @gmail.com	100.88.54.21	Linux 1.32.2-dev-t	Connected	...
leo-desktop @gmail.com	100.119.150.32	Windows 1.36.2	Connected	...
leo-laptop @gmail.com	100.110.242.18	Windows 1.36.2	Mar 8, 9:31 PM GMT+8	...
leo-phone @gmail.com	100.117.71.114	Android 1.36.1	Connected	...

Connect more machines by [installing Tailscale](#)

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.

14.5.2 Allow Remote Access WAN

Note: This feature was renamed to **Advertise WAN Subnets** in firmware v4.9 and later. 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.

Tailscale Beta

i Tailscale makes the devices you own accessible anywhere in the world, securely and effortlessly. It enables encrypted point-to-point connections, which means only devices on your private network can communicate with each other. You can use it to access your devices or LAN remotely.

The device is connected to your Tailscale virtual network.

Enable Tailscale ☒

Allow Remote Access WAN **i** ☒

Allow Remote Access LAN **i** ☐

14.5.3 Allow Remote Access LAN

Note: This feature was renamed to **Advertise LAN Subnets** in firmware v4.9 and later. 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.

Tailscale Beta

i Tailscale makes the devices you own accessible anywhere in the world, securely and effortlessly. It enables encrypted point-to-point connections, which means only devices on your private network can communicate with each other. You can use it to access your devices or LAN remotely.

The device is connected to your Tailscale virtual network.

Enable Tailscale ☒

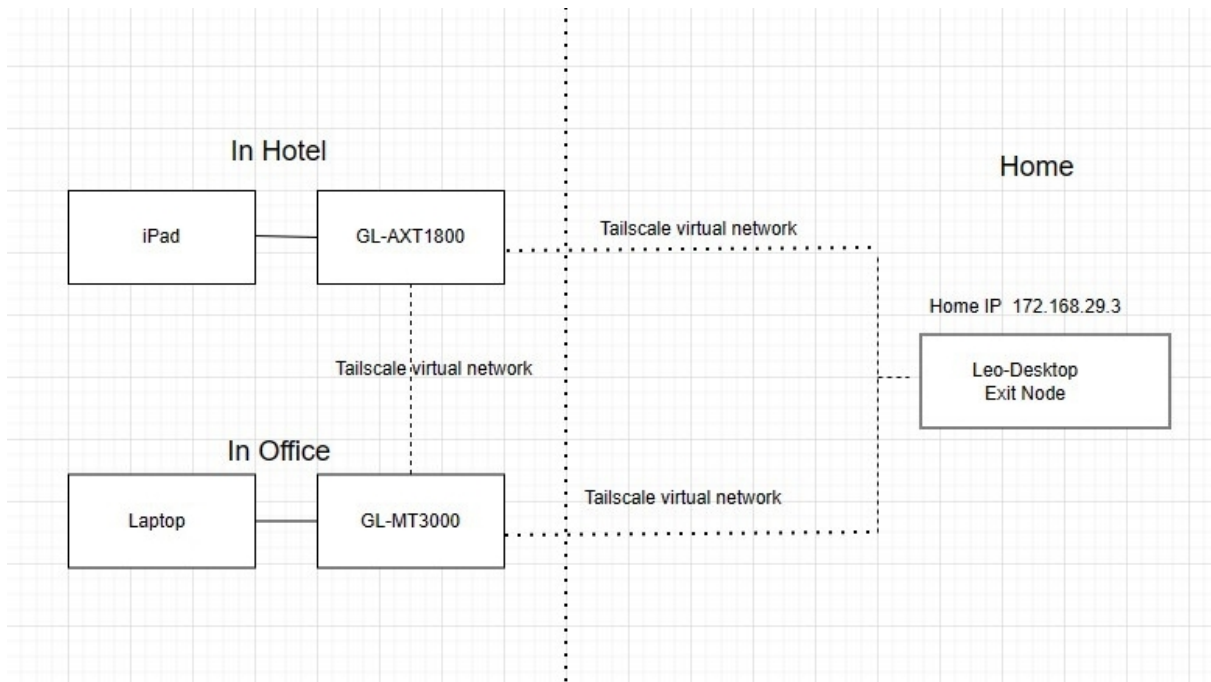
Allow Remote Access WAN **i** ☐

Allow Remote Access LAN **i** ☒

14.5.4 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.



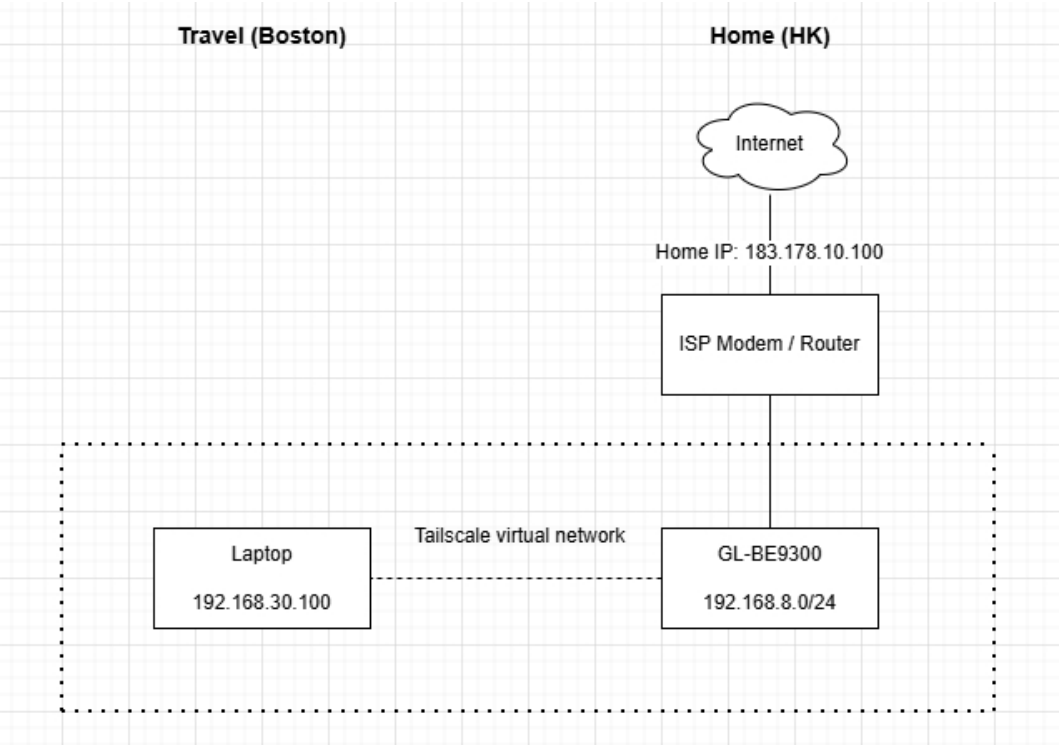
In summary, an Exit node routes outbound Internet traffic from your Tailnet devices, effectively acting as VPN servers. When connected to an Exit node, all your non-Tailscale Internet traffic appears to originate from its location, helping you access geo-restricted content and enhance your online privacy. 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.

14.5.5 Run Exit Node

Running an exit node on your router allows other devices within your tailnet to route all outbound internet traffic via this router's public IP.

In the topology below, a laptop is in Boston, while a router GL-BE9300 is in Hong Kong. Both have been added into the same Tailscale network. If you set the GL-BE9300 as an exit node, all outbound traffic from the laptop will exit through this router to access the internet, and the laptop's public IP will resolve to a Hong Kong IP address instead of a Boston one.



Here is an example of setting up a router GL-BE9300 as an Exit Node.

1. Enroll both GL-BE9300 and travel laptop to the same Tailscale tailnet.

Machines

Manage the devices connected to your tailnet. [Learn more](#)

Search by name, owner, tag, version...

Filters Learn more

2 machines

MACHINE	ADDRESSES	VERSION	LAST SEEN
gl-be9300@gmail.com	100.115.67.77	1.92.5-1 (OpenWrt) Linux 5.4.213	Connected
gl-inet-08@gmail.com	100.78.71.68	1.92.1 Windows 11 25H2	Connected

2. In the GL-BE9300 web Admin Panel, go to APPLICATIONS > Tailscale. enable **Run Exit Node** and click **Apply**.

The screenshot shows the Tailscale web interface. At the top, there's a header with 'Tailscale' and a 'Beta' badge. Below it, a light blue box contains an information icon and text explaining Tailscale's purpose. A light green box below that states 'The device is connected to your Tailscale virtual network.' The main settings area includes an 'Enable' toggle (which is turned on), a 'Bind Account' field with an email address and an 'Unbind' link, a 'Router Virtual IP' field with an information icon and the value '100.115.67.77', and an 'Exit Node' section. In the 'Exit Node' section, there's a 'Custom Exit Node' toggle (turned off) and a 'Run Exit Node' toggle (turned on). A red arrow points to the 'Run Exit Node' toggle.

3. Go to the Tailscale Admin Console, and you will see a tag "Exit Node" under the GL-BE9300.

The screenshot shows the Tailscale Admin Console. At the top, there's a 'Machines' section with a subtitle 'Manage the devices connected to your tailnet. Learn more' and an 'Add device' button. Below this is a search bar and a 'Filters' dropdown. A '2 machines' badge is shown. The main part of the screenshot is a table with columns: MACHINE, ADDRESSES, VERSION, and LAST SEEN. The first row is for 'gl-be9300' with an '@gmail.com' email. Under the 'MACHINE' column, there's a red box highlighting the 'Exit Node' tag. The second row is for 'gl-inet-08' with an '@gmail.com' email.

MACHINE	ADDRESSES	VERSION	LAST SEEN
gl-be9300 @gmail.com Exit Node	100.115.67.77	1.92.5-1 (OpenWrt) Linux 5.4.213	Connected
gl-inet-08 @gmail.com	100.78.71.68	1.92.1 Windows 11 25H2	Connected

4. Click the three-dot icon on the right of GL-BE9300 and select **Edit route settings**.

Machines
Manage the devices connected to your tailnet. [Learn more](#)

Search by name, owner, tag, version... Filters [Learn more](#) Download

2 machines

MACHINE	ADDRESSES	VERSION	LAST SEEN	
gl-be9300 @gmail.com Exit Node	100.115.67.77	1.92.5-1 (OpenWrt) Linux 5.4.213	Connected	Share... ⋮
gl-inet-08 @gmail.com	100.78.71.68	1.92.1 Windows 11 25H2	Connected	

Add devices to your network

- Set up SSH
- Edit machine name...
- Edit machine IPv4...
- Share...
- Disable key expiry
- View recent activity
- Edit route settings...**
- Edit ACL tags...
- Remove...

- In the pop-up window, check **Use as exit node** and click **Save**.

Edit route settings of gl-be9300 ✕

Subnet routes
Connect to devices you can't install Tailscale on by advertising IP ranges as subnet routes. [Learn more](#)

This machine does not expose any routes.

Exit node
Allow your network to route internet traffic through this machine.
[Learn more](#)

☒ Use as exit node

Cancel Save

- Disable key expiry.
As a security feature, users need to periodically re-authenticate on each of their devices. To avoid disconnections when the exit node authentication key expires, we recommend disabling key expiry for your exit node. Click [here](#) for more details about key expiry. Click the three-dot icon on the right of GL-BE9300 and select Disable key expiry.

Machines

Manage the devices connected to your tailnet. [Learn more](#)

Add device

Search by name, owner, tag, version...

Filters Learn more

2 machines

MACHINE	ADDRESSES	VERSION	LAST SEEN	
gl-be9300 @gmail.com Exit Node	100.115.67.77	1.92.5-1 (OpenWrt) Linux 5.4.213	Connected	Share... ⋮
gl-inet-08 @gmail.com	100.78.71.68	1.92.1 Windows 11 25H2	Connected	

Add devices to your network

- Set up SSH
- Edit machine name...
- Edit machine IPv4...
- Share...
- Disable key expiry
- View recent activity
- Edit route settings...
- Edit ACL tags...
- Remove...

Once applied, a tag "Expiry disabled" will appear under the GL-BE9300.

Machines

Manage the devices connected to your tailnet. [Learn more](#)

Add device

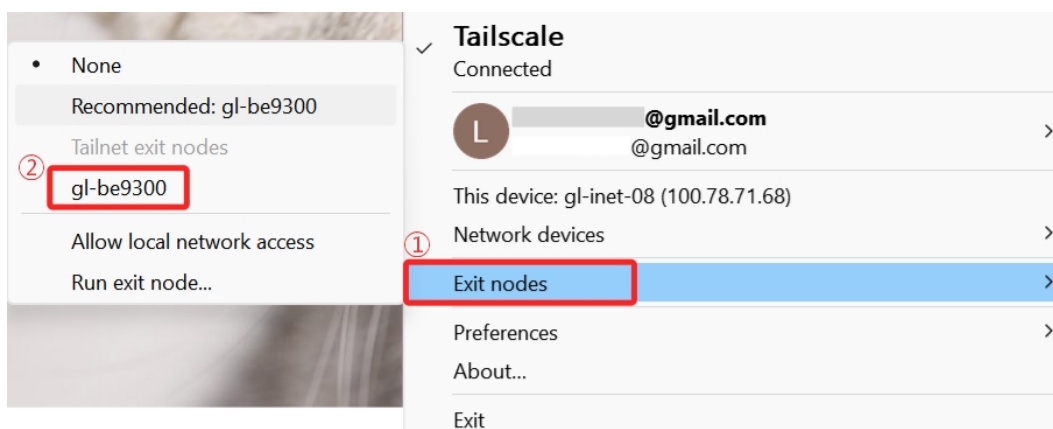
Search by name, owner, tag, version...

Filters Learn more

2 machines

MACHINE	ADDRESSES	VERSION	LAST SEEN	
gl-be9300 @gmail.com Expiry disabled Exit Node	100.115.67.77	1.92.5-1 (OpenWrt) Linux 5.4.213	Connected	...
gl-inet-08 @gmail.com	100.78.71.68	1.92.1 Windows 11 25H2	Connected	...

- Run Tailscale on your travel laptop. The Tailscale icon will appear in the system tray at the bottom right corner. Right-click the icon, click **Exit nodes** and select **gl-be9300**.



Now, all outbound traffic from this travel laptop will exit through GL-BE9300 to access the internet.

- Test connectivity.

(1) On your travel laptop, open a web browser and visit ipcheck.ing or any other IP lookup website. The page will display the public IP address belonging to your Tailscale exit node, confirming the laptop is accessing the internet via the exit node (the GL-BE9300 located in Hong Kong, in this example).

1

IP Source: IPCheck.ing IPv4



183.178.10.100



 Region

 Hong Kong

 State

Kwai Tsing District

 City

Kwai Chung 

 ISP

Hong Kong Broadband Network Limited

 To avoid abuse, sign in to view the following information

 All Type

 Proxy

 ASN-Geo match

 IP Quality

 ASN AS9269



(2) Press *Win+R*, type *cmd* to launch Command Prompt, then run *tracert google.com* to trace the outbound traffic routes. The command output lists all routing hops for your internet traffic. If configured correctly, the first external hop will route through the exit node, as shown below, verifying all outbound internet traffic egresses through this router.

```
Administrator: C:\WINDOWS\...
Microsoft Windows [Version 10.0.26200.8655]
(c) Microsoft Corporation. All rights reserved.

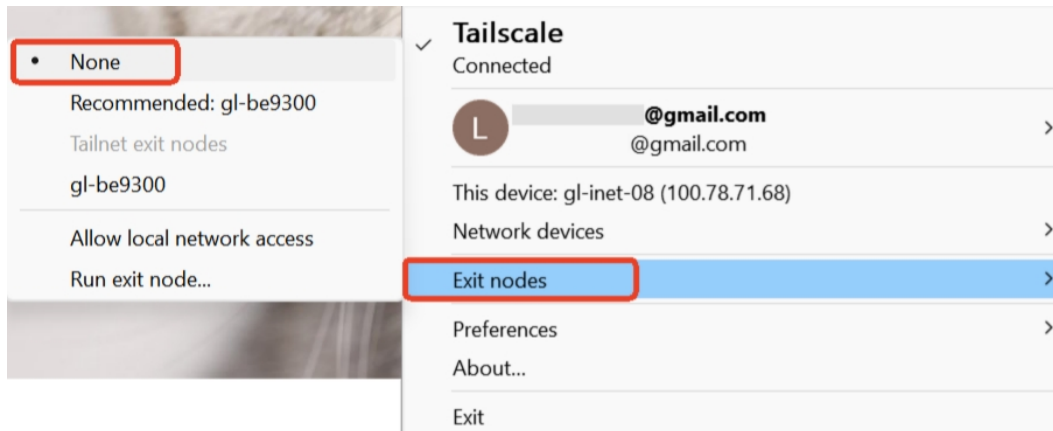
C:\Users\Administrator>tracert google.com

Tracing route to google.com [142.250.197.142]
over a maximum of 30 hops:

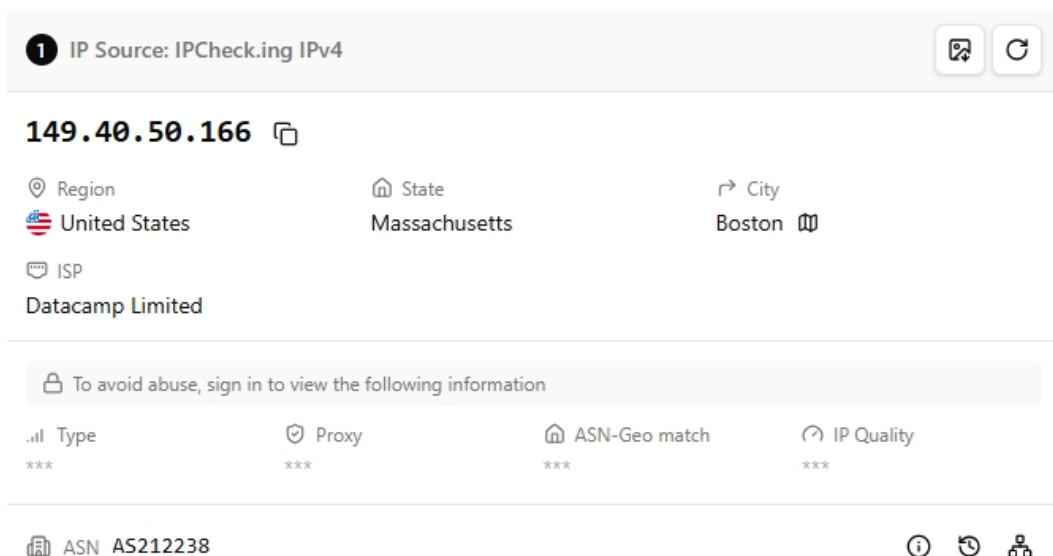
  1  478 ms  478 ms  471 ms  gl-be9300.tail1fd0.ts.net [100.115.67.77]
  2  479 ms  480 ms  473 ms  10.
  3  496 ms  478 ms  655 ms  10.
  4  478 ms  583 ms  532 ms  192
  5  492 ms  481 ms  486 ms  44.
  6  494 ms  517 ms  523 ms  10.
  7  496 ms  499 ms  525 ms  44.
  8  503 ms  522 ms  490 ms  192
  9  502 ms  509 ms  507 ms  183
 10  530 ms  499 ms  504 ms  203
 11  495 ms  498 ms  691 ms  202
 12  517 ms  509 ms  581 ms  061
 13  519 ms  522 ms  503 ms  203
 14  524 ms  544 ms  507 ms  142
 15  506 ms  496 ms  502 ms  142
 16  501 ms  514 ms  515 ms  nch

Trace complete.
```

(3) Disconnect the exit node for a comparative test. Right-click the Tailscale icon in the system tray at the bottom-right corner, click **Exit nodes** then select **None** to stop using the exit node.



(4) Open a new browser tab and visit ipcheck.ing or any IP lookup service. It will now show your laptop's native public IP address, proving the device is using your local internet connection instead (Boston, in this example).



14.6 ZeroTier

ZeroTier is a software-based virtual private network (VPN) that enables secure, encrypted communications between devices over the internet. It creates a private, virtual network that allows devices to communicate as if they were on the same local network, regardless of their physical location or network topology. ZeroTier is designed to be easy to set up and use, and offers features such as end-to-end encryption, network segmentation, and network bridging capabilities.

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:

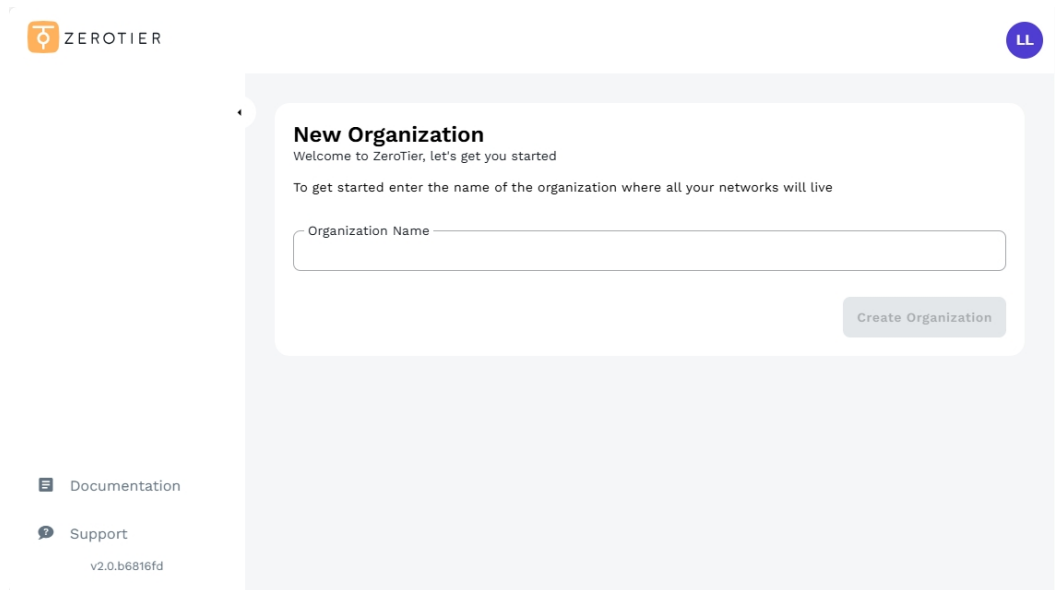
1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale, and AstroWarp.
2. This feature is currently in beta, and may have some bugs.

14.6.1 Set Up ZeroTier

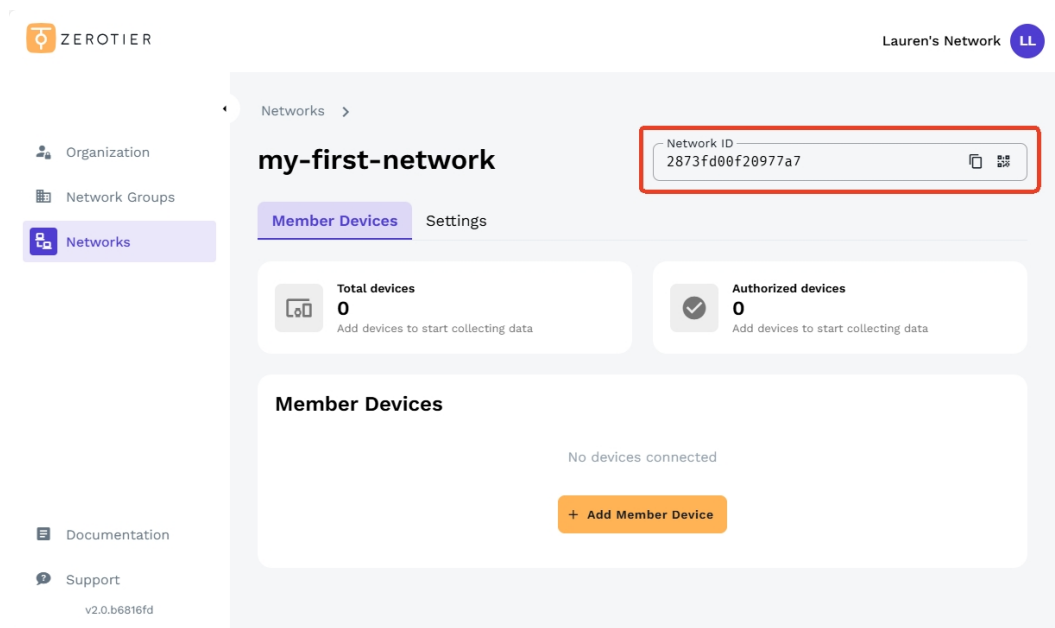
Two versions of ZeroTier Central are available: New Central and Legacy Central.

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**.

The screenshot shows the ZeroTier configuration interface. At the top, there's a header with 'ZeroTier' and a 'Beta' badge. Below it, a light blue box contains an information icon and text explaining that ZeroTier creates a secure, virtual peer-to-peer Ethernet network accessible from anywhere, supporting access to devices like phones and PCs. Another light blue box states that ZeroTier connects to a virtual network using a Network ID created on ZeroTier Central. The configuration options include: 'Enable ZeroTier' (a toggle switch turned on, indicated by a red arrow), 'Allow Remote Access WAN' (a toggle switch turned off), and 'Allow Remote Access LAN' (a toggle switch turned off). Below these is the 'Network ID' field, which contains the value '2873fd00f20977a7' (indicated by a red arrow). At the bottom, there is a blue 'Apply' button (indicated by a red arrow).

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

The screenshot shows the ZeroTier configuration interface after the settings have been applied. The header remains the same. The light blue information box is still present. Below it, a yellow box with a warning icon contains a message: 'The device has been added to ZeroTier. Please go to ZeroTier Central to authorize the device to connect to your virtual network.' A red arrow points to the 'ZeroTier Central' link in this message. The 'Enable ZeroTier' toggle switch is now turned on.

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

The screenshot shows the ZeroTier web interface for a network named "my-first-network". The network ID is 2873fd00f20977a7. Under the "Member Devices" tab, there is a "Device Pending Authorization" section with a blue bar. A red arrow points to the "Authorize" button. Below this, there are two summary boxes: "Total devices 1" and "Authorized devices 0". The "Member Devices" table shows one device with ID "eb618be42d", status "Not Authorized", and a yellow warning icon. The table has columns: Device ID, Name, Status, ZT IP, Public IP, ZT Version, Last Active, and Actions.

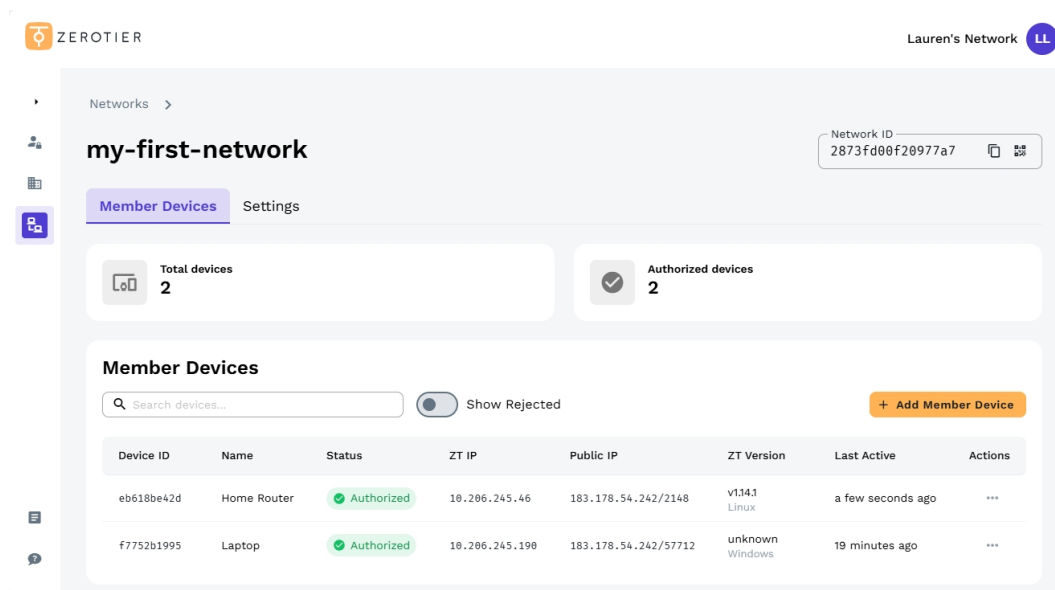
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Not Authorized		183.178.54.242/30149	unknown Linux	a few seconds ago	...

Once authorized, the page displays as follows.

The screenshot shows the ZeroTier web interface after the device has been authorized. The "Authorized devices" summary box now shows "1". The "Member Devices" table shows the device "eb618be42d" with a status of "Authorized" (green checkmark) and a ZT IP of "10.206.245.46". The table has columns: Device ID, Name, Status, ZT IP, Public IP, ZT Version, Last Active, and Actions.

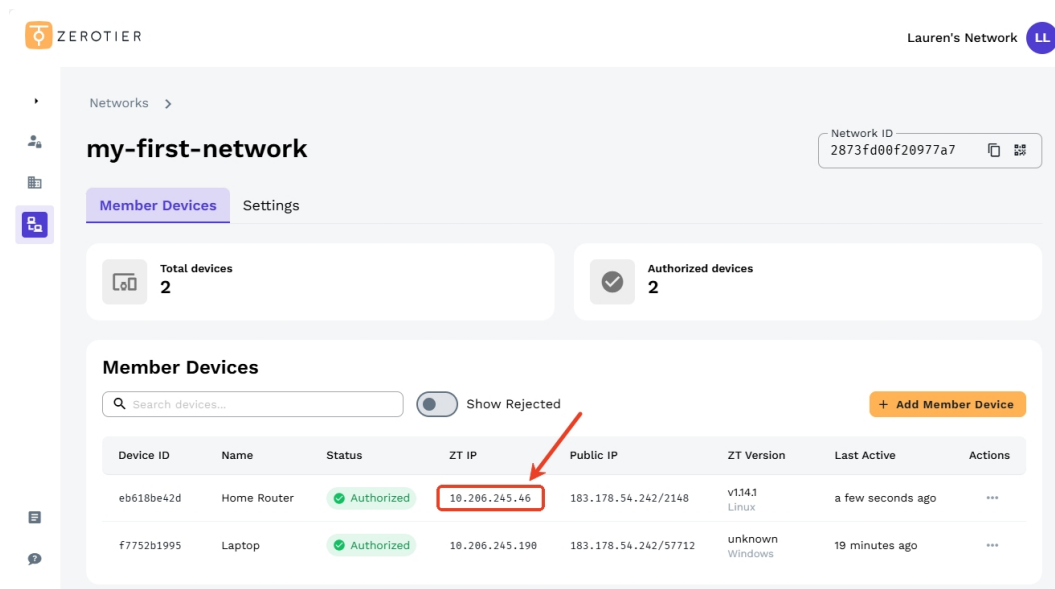
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Authorized	10.206.245.46	183.178.54.242/24364	V1.14.1 Linux	a few seconds ago	...

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.

- 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.

- 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.

14.6.2 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.

14.6.3 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.

ZeroTier Beta

ZeroTier creates securely peer to peer virtual Ethernet networks that work anywhere and supports access to devices such as phones, PCs etc. You can use it to access your devices or LAN remotely.

The device is connected to your ZeroTier virtual network.

Enable ZeroTier

☒

Allow Remote Access WAN ⓘ

☐

Allow Remote Access LAN ⓘ

☒

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.

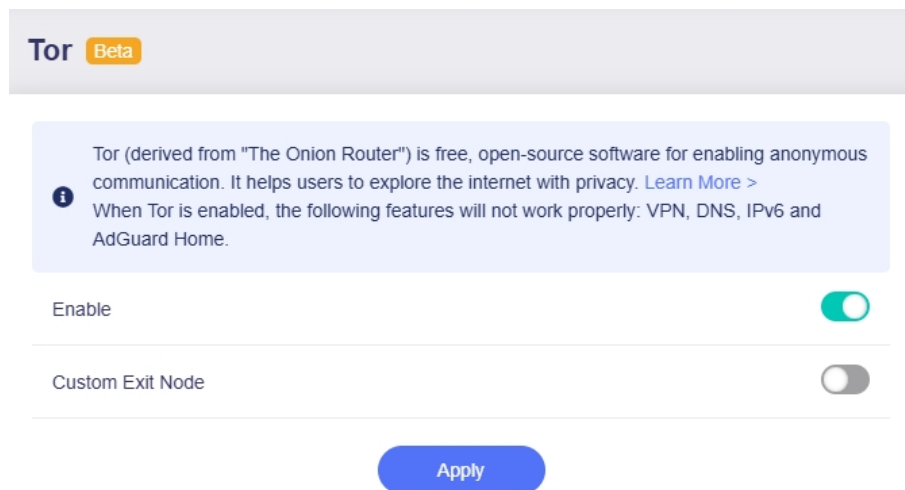
14.7 Tor

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 **APPLICATIONS > Tor**. Toggle the switch to enable it, enable Custom Exit Nodes as needed, and click **Apply**.



Tor Beta

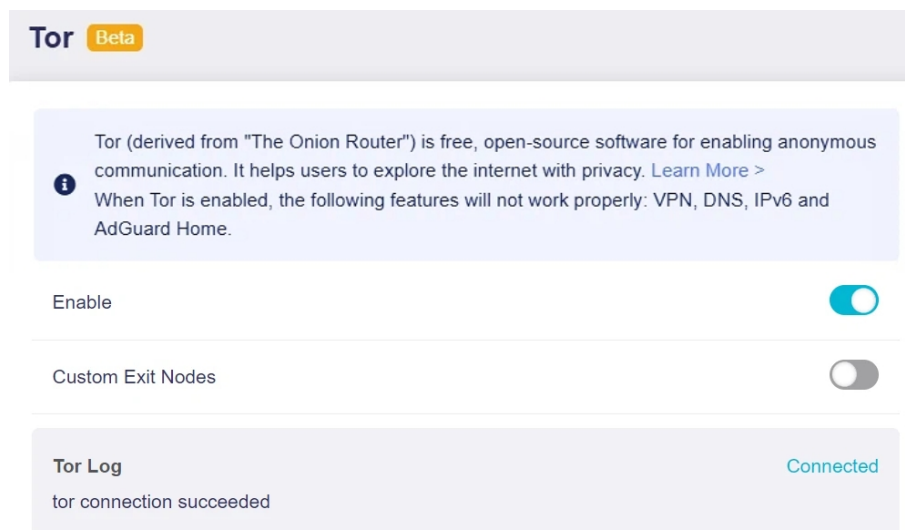
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.

Enable ☒

Custom Exit Node ☐

Apply

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



Tor Beta

Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.

Enable ☒

Custom Exit Nodes ☐

Tor Log Connected
tor connection succeeded

Chapter 15

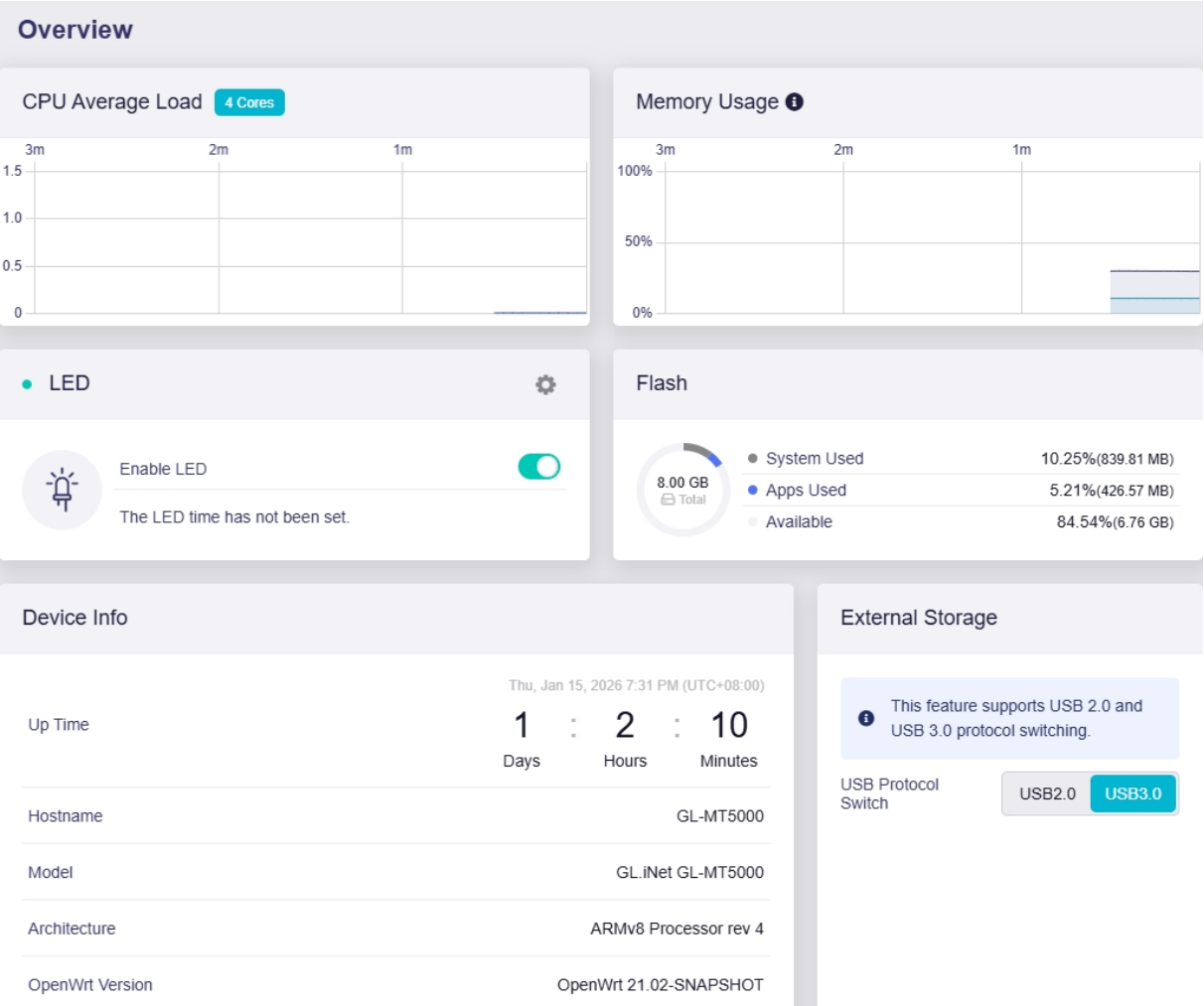
System

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

15.1 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 Status, Memory, Flash, and External Storage devices
- LED Control
- Device information



15.2 Admin Password

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

Admin Password

Old Password

Enter old password

New Password

Enter new password

Confirm Password

Enter new password again

Apply

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.

15.3 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.

15.3.1 Online Upgrade

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

Upgrade

Firmware Online Upgrade

Firmware Local Upgrade

✓ Firmware is up-to-date.

Current Firmware

Version	4.8.4
Firmware Type	release
Update Time	2026-01-08 09:23:25 (UTC+00:00)

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).

15.3.2 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.

Upgrade

Firmware Online Upgrade

Firmware Local Upgrade



Select a file to upload or drag it here
File types include: .bin, .img, .zip, .tar, .gz

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

Firmware Verification

Version	4.8.1 Release Notes
Firmware Type	release8
SHA256	ee038ee0f399c1454cc660dd47811b44697f5304e0f61af145c7dca6817d0e5c
Verification Result	Pass
Keep Settings 	☒

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.

15.4 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.

15.4.1 LED Display Schedule

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

LED Display Schedule

Enable Scheduled



Turn On Time

 07:00

Turn Off Time

 22:00

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

Apply

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

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

15.4.2 Schedule Reboot

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

Schedule Reboot

Enable Scheduled



Reboot Time

 03:00

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

Apply

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

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

15.5 Time Zone

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

Time Zone

Router Time

Wed, Nov 5, 2025 7:19 PM (UTC+08:00)

Etc/GMT-8

Apply

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.

The time zone of the router is different from that of your browser.

Sync

Router Time

Sun, Dec 15, 2024 3:20 PM (UTC+00:00)

UTC

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

Router Time

Wed, Nov 5, 2025 7:19 PM (UTC+08:00)

Etc/GMT-8

Etc/GMT-7

Etc/GMT-8

Etc/GMT-9

Etc/GMT-10

15.6 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.

Reset Firmware

 In case of malfunction, you can reset router. All your current settings, applications and data will be lost. The process will take about 2 Minutes. DO NOT power off the router during this process.

Delete All and Reboot

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.

15.7 Log

Log in to your router's web admin panel and navigate to **SYSTEM > Log**. This page allows you to view logs of System, Kernel, Crash, Cloud and Nginx for analysis and troubleshooting. In addition, some cellular models that supports eSIM also provides eSIM log.

Log

Export LogContact Support

System LogKernel LogCrash LogCloud LogNginx Log

LevelAllModuleAllKey wordSearchRefresh

Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: DNS service limited to local subnets
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: compile time options: IPv6 GNU-getopt no-DBus UBus no-i18n no-IDN DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth cryptohash DNSSEC no-ID loop-detect inotify dumpfile
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: UBus support enabled: connected to system bus
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq-dhcp[14269]: DHCP, IP range 192.168.3.100 -- 192.168.3.200, lease time 30m
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq-dhcp[14269]: IPv6 router advertisement enabled
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain test
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain onion
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain localhost
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain local
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain invalid
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using only locally-known addresses for domain bind
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using nameserver 2001:4860:4860::8844#53
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using nameserver 2001:4860:4860::8888#53
Wed Nov 5 18:17:02 2025 daemon.info dnsmasq[14269]: using nameserver 8.8.4.4#53

- **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.

Your Feedback

Subject

Your Contact Email

Description

0/1000

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](#)

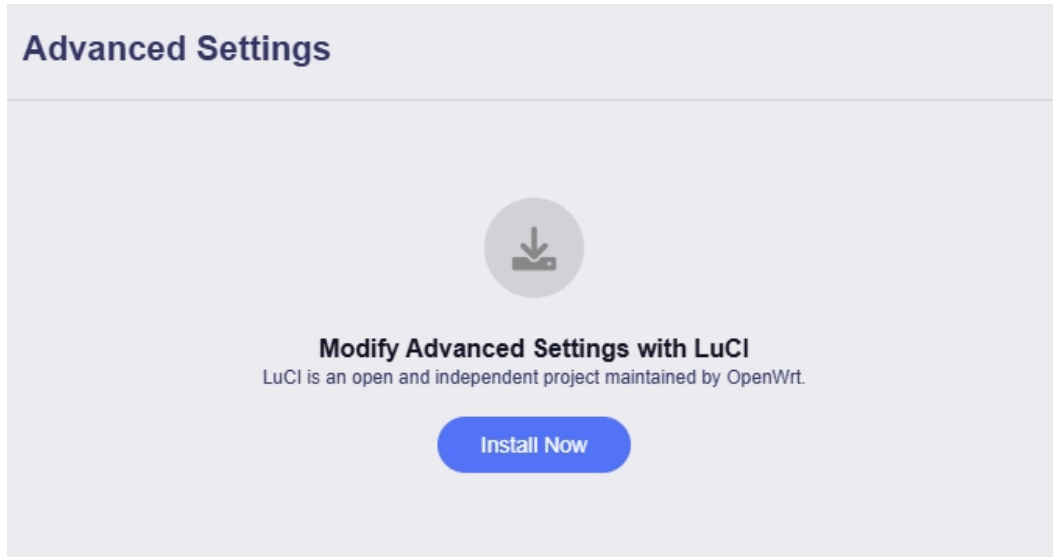
Cancel

Send

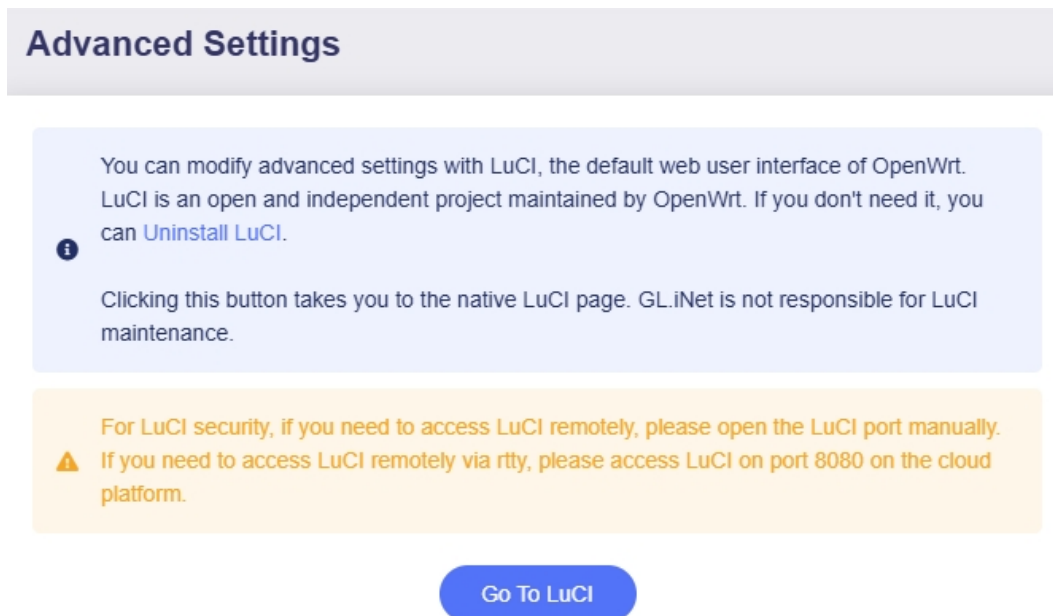
15.8 Advanced Settings

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.

Authorization Required

Username

root

Password

Log in

Then you will be logged into the LuCI page.

GL-MT5000

Status ▾System ▾Network ▾Logout

Status

System

Hostname	GL-MT5000
Model	GL.iNet GL-MT5000
Architecture	ARMv8 Processor rev 4
Target Platform	mediatek/mt7987
Firmware Version	OpenWrt 21.02-SNAPSHOT / LuCI openwrt-21.02 branch git-23.093.57360-e98243e
Kernel Version	5.4.281
Local Time	2026-01-15 19:55:18
Uptime	1d 2h 34m 30s
Load Average	0.00, 0.00, 0.00

Regulatory and Legal

FCC Compliance Statement

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

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help important announcement.

CAN ICES-3(B) NMB-3(B)

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'encombrer le fonctionnement.

Hereby, GL TECHNOLOGIES (HONG KONG) LIMITED declares that this product is in compliance with the essential requirements and other relevant provisions of EMC directive 2014/30/EU, LVD directive 2014/35/EU. A copy of the EC Declaration of Conformity (DoC) is available at <https://www.gl-inet.com/products/certificate>.

Trademarks

- 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.