



User Manual

GL-BE14000 / Flint 4

Tri-Band Wi-Fi 7 Home Router

Firmware Version 4.9.1

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	Touchscreen	9
1.2	Specifications	11
1.3	Package Contents	12
Chapter 2	Hardware Connection	13
2.1	Choosing a Location	14
2.2	Connecting the Router	14
Chapter 3	Log In To Your Router	15
Chapter 4	Set Up Internet Connection	17
4.1	Quick Setup Wizard	18
4.2	Manually Set Up Internet Connection	19
4.2.1	Connect to the Internet via SFP+ Module	20
4.2.2	Connect to the Internet via Ethernet Cable	24
4.2.3	Connect to the Internet via an Existing Wi-Fi	28
4.2.4	Connect to the Internet via USB Tethering	33
4.2.5	Connect to the Internet via USB Modem	38
Chapter 5	Wireless	40
5.1	Wi-Fi Status Display	41
5.2	Wireless Settings	42
5.2.1	MLO Wi-Fi	42
5.2.2	Main Network	44
5.2.3	Guest Network	45
5.2.4	IoT Network	47
Chapter 6	Clients	49
6.1	Device Details	51
6.2	Action	53
6.3	Sort	56
6.4	Settings	57
Chapter 7	Cloud Services	58

7.1 GoodCloud	59
7.1.1 Enable GoodCloud	59
7.1.2 Manage Your Router	62
7.1.3 Unbind Device	66
7.1.4 Disable GoodCloud	66
7.2 AstroWarp	67
7.2.1 Quick Setup	67
7.2.2 Test Connectivity	71
Chapter 8 Get To Know VPN	72
8.1 Introduction	73
8.2 Application Scenarios	74
Chapter 9 VPN Dashboard	76
9.1 Upload VPN Profile	77
9.2 Add VPN Tunnel	80
9.2.1 General Steps	80
9.2.2 Case Reference	82
9.3 Kill Switch	98
9.4 All Other Traffic	99
9.5 Tunnel Options	100
9.6 Tunnel Priority	102
Chapter 10 Set Up VPN Server	104
10.1 Set Up OpenVPN Server	105
10.1.1 Preparation	105
10.1.2 Setup Steps	106
10.1.3 Troubleshooting	108
10.2 Set Up WireGuard Server	109
10.2.1 Preparation	109
10.2.2 Setup Steps	110
10.2.3 Troubleshooting	113
Chapter 11 Set Up VPN Client	114
11.1 Set Up OpenVPN Client	115
11.1.1 Preparation	115
11.1.2 Set Up NordVPN	115
11.1.3 Set Up OpenVPN Client Manually (for other providers)	121

11.2 Set Up WireGuard Client	124
11.2.1 Preparation	124
11.2.2 Set Up AzireVPN	125
11.2.3 Set Up Hide.me	129
11.2.4 Set Up IPVanish	132
11.2.5 Set Up Mullvad	136
11.2.6 Set Up NordVPN	140
11.2.7 Set Up PIA (Private Internet Access)	145
11.2.8 Set Up Surfshark	149
11.2.9 Set Up WireGuard Client Manually (for other providers)	153
Chapter 12 Network	158
12.1 Multi-WAN	159
12.1.1 Interface Status Track	159
12.1.2 Multi-WAN Mode	162
12.2 Subnet	165
12.2.1 Main Network	165
12.2.2 Guest Network	171
12.2.3 IoT Network	175
12.2.4 VLAN Networks	179
12.3 Ethernet Port	183
12.3.1 SFP+	184
12.3.2 WAN	186
12.3.3 LAN	187
12.3.4 Dual-Ethernet WAN	189
12.4 DNS	193
12.4.1 DNS Server Settings	194
12.4.2 Edit Hosts	196
12.5 IPv6	198
12.5.1 IPv6 Mode	199
12.5.2 DNS Acquisition Method	199
12.6 IGMP Snooping	200
12.7 Network Mode	201
12.8 Drop-in Gateway	203
12.9 Network Acceleration	205

Chapter 13	Flow Control	206
13.1	DPI Engine	207
13.2	Data Statistics	209
13.2.1	Quick Setup	209
13.2.2	Data Storage Rules	211
13.2.3	Switch Time Range	211
13.2.4	Clear Statistics	212
13.3	Content Filter	213
13.4	QoS	215
13.5	SQM	217
13.6	Parental Control	219
Chapter 14	Security	225
14.1	Port Forwarding	226
14.1.1	DMZ	226
14.1.2	Port Forwarding	227
14.2	ACL	229
14.3	Admin Access	231
14.3.1	Access Control	231
14.3.2	Remote Access Control	233
14.3.3	Open Ports on Router	234
14.4	NAT Mode	235
Chapter 15	Applications	236
15.1	Plug-ins	237
15.2	Dynamic DNS	238
15.2.1	Enable DDNS	238
15.2.2	Check if DDNS Works	241
15.2.3	HTTPS Remote Access	243
15.2.4	SSH Remote Access	245
15.3	Network Storage	247
15.3.1	Connect Storage	247
15.3.2	Set Up Samba	248
15.3.3	Set Up WebDAV	251
15.3.4	Set Up DLNA	254
15.4	AdGuard Home	255

15.5 Bark	257
15.6 Tailscale	259
15.6.1 Set Up Tailscale	260
15.6.2 Advertise WAN Subnets	263
15.4.3 Advertise LAN Subnets	264
15.6.4 Custom Exit Nodes	265
15.6.5 Run Exit Node	266
15.7 ZeroTier	272
15.7.1 Set Up ZeroTier	273
15.7.2 Allow Remote Access WAN	277
15.7.3 Allow Remote Access LAN	278
15.8 Tor	279
Chapter 16 System	280
16.1 Overview	281
16.2 Admin Password	282
16.3 Upgrade	283
16.3.1 Online Upgrade	283
16.3.2 Local Upgrade	284
16.4 Scheduled Tasks	285
16.4.1 LED Display Schedule	285
16.4.2 Schedule Reboot	286
16.4.3 MLO Wi-Fi Schedule	286
16.4.4 6 GHz Wi-Fi Schedule	287
16.4.5 5 GHz Wi-Fi Schedule	289
16.4.6 2.4 GHz Wi-Fi Schedule	291
16.5 Time Zone	294
16.6 Reset Firmware	295
16.7 Log	296
16.8 Advanced Settings	298
Regulatory Statement	300

Chapter 1

Get To Know Your Router

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

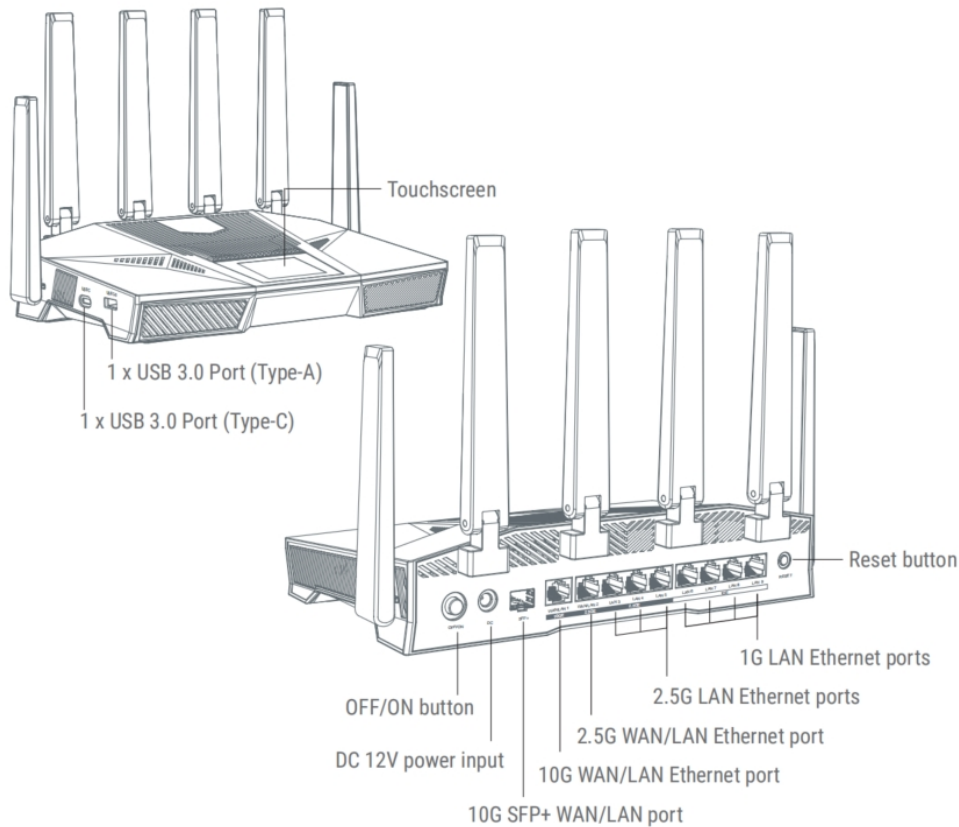
1.1 Product Overview

Flint 4 (GL-BE14000) features tri-band Wi-Fi 7 with MLO, delivering peak rates of 688 Mbps (2.4 GHz) + 4323 Mbps (5 GHz) + 8646 Mbps (6 GHz). For wired connectivity, it comes with a full multi-gig wired backbone, including one 10G SFP+ WAN/LAN port, one 10GE WAN/LAN port, one 2.5GE WAN/LAN port, three 2.5GE LAN ports and four 1GE LAN ports. Supporting high-performance VPN, it achieves throughput up to 1.5 Gbps for both WireGuard® and OpenVPN DCO. A 2.4-inch touchscreen display is also equipped on-board, enabling real-time network-status monitoring and allowing users to view key network metrics directly on the hardware device.

1.1.1 Appearance



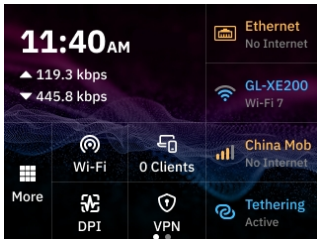
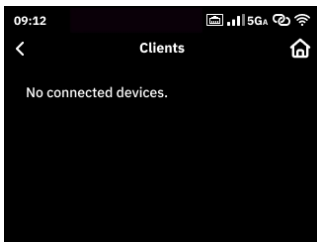
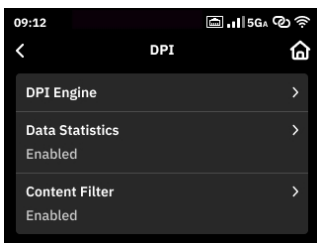
1.1.2 Interface and Button

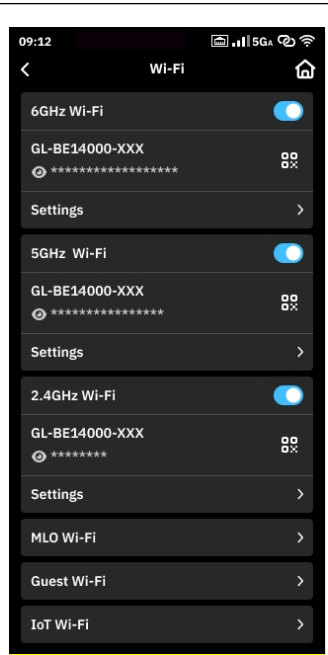
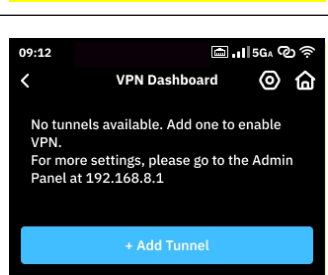
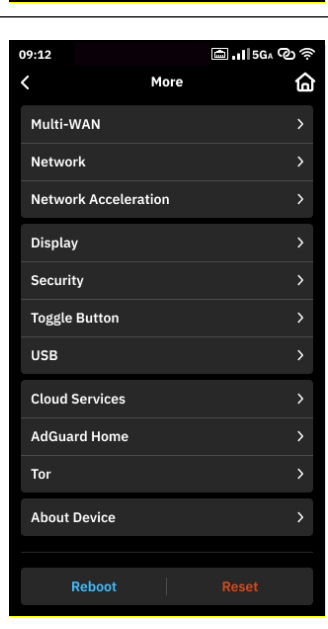


Item	Description
Power Port	Connects to the power adapter.
10G WAN/LAN Ethernet Port	Connects to high-bandwidth wired devices or serves as a high-speed internet uplink.
10G SFP+ WAN/LAN Port	Connects with compatible modules or higher-end wired devices.
2.5G WAN/LAN Ethernet Port	Connects to multi-gig wired devices or serves as a high-speed internet uplink.
2.5G LAN Ethernet Port	Connects to wired devices if needed.
1G LAN Ethernet Port	Connects to wired devices if needed.
USB 3.0 Port(Type-A)	For USB storage devices, phone USB-tethering, and compatible cellular dongles.

USB 3.0 Port(Type-C)	For USB storage devices, phone USB-tethering, and compatible cellular dongles.
Reset Button	Press and hold for 3 seconds and then release to repair your network.
	Press and hold for 10 seconds and then release to reset the router to factory default.
OFF/ON Button	Turns the router on and off.

1.1.3 Touchscreen

Screen Display	Description
	Starting up
	Homepage The homepage displays the status of Ethernet, Repeater, Cellular, Wi-Fi, Clients, DPI, VPN, and other settings. Three colors represent three network connection states: Blue: Active / Connected Yellow: Connecting / abnormal White: Inactive / disconnected
	Clients You can view detailed information of clients connected to your network on this page.
	DPI Tap to configure the DPI Engine, view Data Statistics, and manage Content Filter.

	Wi-Fi details You can configure various Wi-Fi networks, including MLO Wi-Fi, Main Network, Guest Network and IoT Network.
	VPN status It requires initial setup in the web admin panel.
	More settings Tap More on the homepage to access more settings. You can tap each item on the touch screen to access the corresponding settings.

1.2 Specifications

Interface	1 x 10G WAN/LAN Ethernet Port 1 x 10G SFP+ WAN/LAN Port 1 x 2.5G WAN/LAN Ethernet Port 3 x 2.5G LAN Ethernet Ports 4 x 1G LAN Ethernet Ports 1 x USB 3.0 Port (Type-A) 1 x USB 3.0 Port (Type-C) 1 x Reset Button 1 x Power Button
CPU	MediaTek Quad-Core Cortex-A73 @ 1.8GHz
Memory / Storage	DDR4 2GB / eMMC 64GB
Protocol	IEEE 802.11a/b/g/n/ac/ax/be
Wi-Fi Speed	688Mbps (2.4 GHZ), 4323 Mbps (5 GHZ), 8646Mbps (6 GHZ)
Antennas	6 x Foldable External Wi-Fi Antennas
Ethernet Speed	10/100/1000/2500/10000 Mbps
Power Input	12V/4A
Power Consumption	Without USB Load: <25W With USB Load: <45W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	293 x 172 x 76 mm / 1166g
Other Tools	Datasheet / Firmware / App / Unboxing / Tutorials

*Wireless speeds are based on IEEE 802.11 standards (e.g., 802.11be for Wi-Fi 7). Actual throughput and range may be lower due to environmental obstacles (walls, metal), network congestion, or client device capabilities.

*Use of Wi-Fi 7 (802.11be) and its features (OFDMA, MU-MIMO, 4096-QAM, MLO) requires client devices to support the corresponding technologies.

1.3 Package Contents

The package includes:

- 1 x Flint 4 (GL-BE14000)
- 1 x Power Adapter
- 1 x Ethernet Cable
- 1 x User Manual
- 1 x Thank You Card
- 1 x Converter (Based 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.
- **EMI avoidance:** Keep the router away from electromagnetic interference sources (Bluetooth devices, microwaves) to minimize signal interference.

2.2 Connecting the Router

1. Power on

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

2. Connect a device to the router

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

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

3. Log in to the router

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

Chapter 3

Log In To Your Router

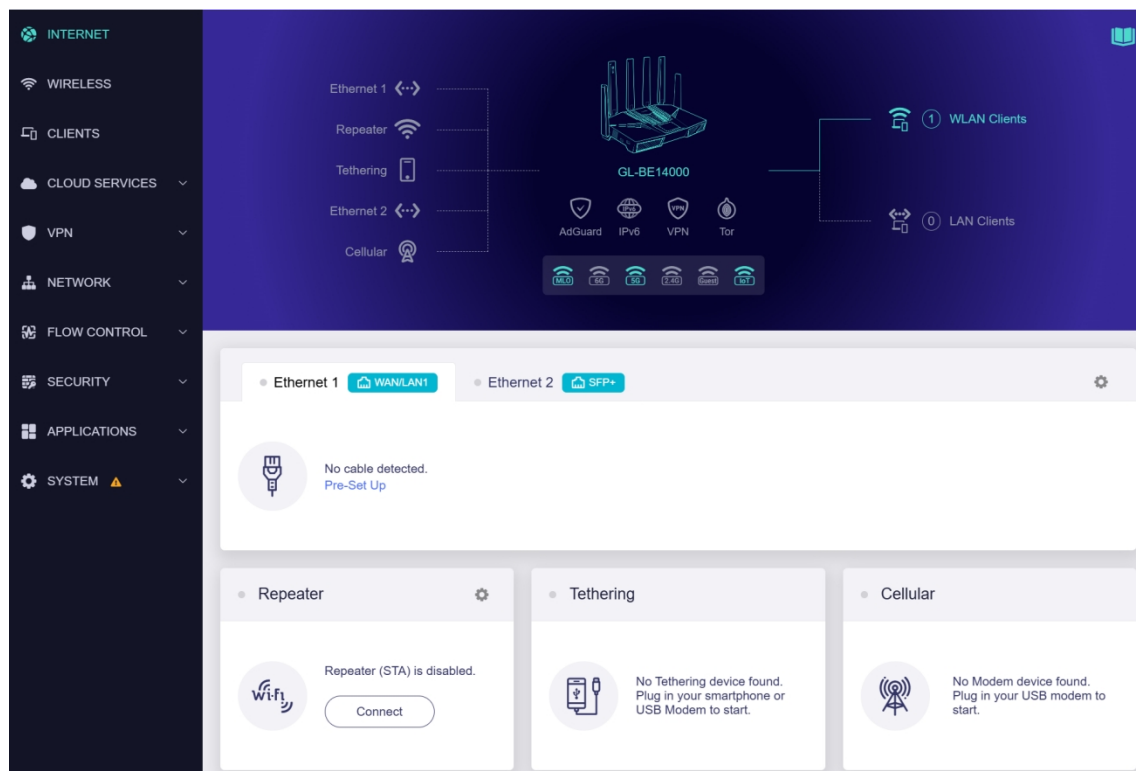
This chapter guides you to log in to your router via web admin panel.

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

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

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

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



Chapter 4

Set Up Internet Connection

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

4.1 Quick Setup Wizard

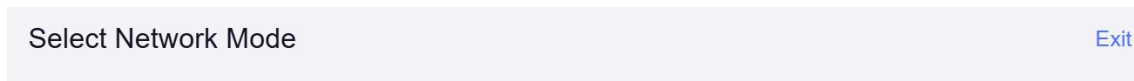
The Web-based Setup Wizard will guide you through the router network configuration.

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.



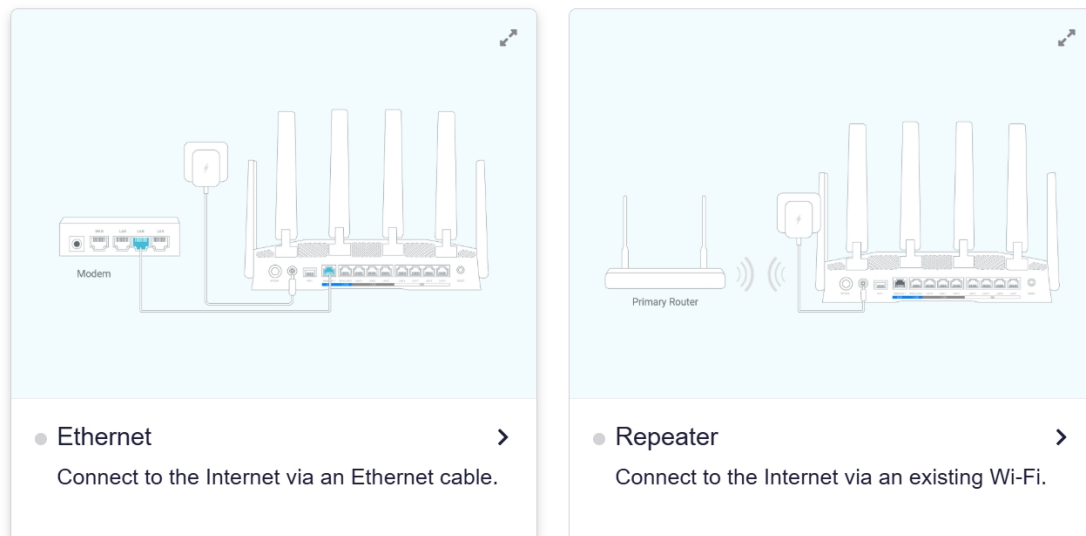
3. Follow the Setup Wizard to configure your router and establish an internet connection.



Network Guide

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

Suggest



If using the [GL.iNet app](#), follow the on-screen prompts to set up internet access.

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 if needed.

Flint 4 supports four internet connection methods: Ethernet, Repeater, USB Tethering, and USB Modem. Choose the appropriate method based on your usage needs.

1. **Ethernet (SFP+)**: Connect the router to a broadband network using a compatible SFP+ module inserted into the SFP+ WAN/LAN port. This method provides the Flint 4 the flexibility to connect with compatible fiber modules or higher-end wired infrastructure where ultra-fast throughput matters most.
2. **Ethernet (RJ45)**: 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.
3. **Repeater**: This mode enables the router to connect to an existing Wi-Fi network to extend the Wi-Fi signal and create a separate, secure local network. Note that transmission speeds may be reduced to some extent. It is ideal for Wi-Fi dead zones that require signal extension, or public locations where enhanced network security is needed.
4. **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.
5. **USB Modem**: Insert a USB cellular modem with a pre-installed SIM card into the router. The router will then connect to the internet via 4G/5G mobile networks, providing connectivity independent of fixed-line broadband. This method offers high mobility and is suitable for scenarios such as in-vehicle use or outdoor activities.

4.2.1 Connect to the Internet via SFP+ Module

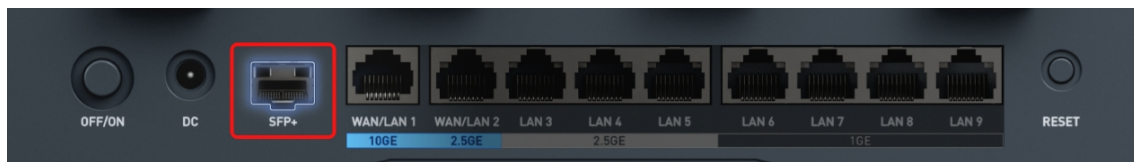
Connect the router to a broadband network using a compatible SFP+ module inserted into the SFP+ WAN/LAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method provides the Flint 4 the flexibility to connect with compatible fiber modules or higher-end wired infrastructure where ultra-fast throughput matters most.

Note: Click [here](#) to view the official GL.iNet Docs for the latest compatibility information and a list of supported models.

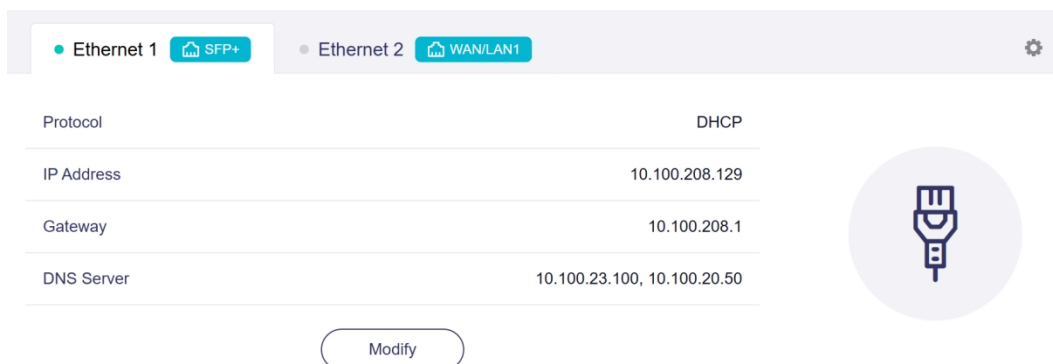
Basic Setup

Follow the steps below to connect your router to the Internet via the SFP+ port, using an SFP+ to RJ45 module (SFP-10G-T) as an example. You may select different modules according to your usage scenario.

1. Insert a compatible 10G SFP+ copper module into Flint 4's **SFP+** port, then connect Flint 4 to an upstream device (e.g., ISP modem, network switch, or wall Ethernet jack) using an Ethernet cable.

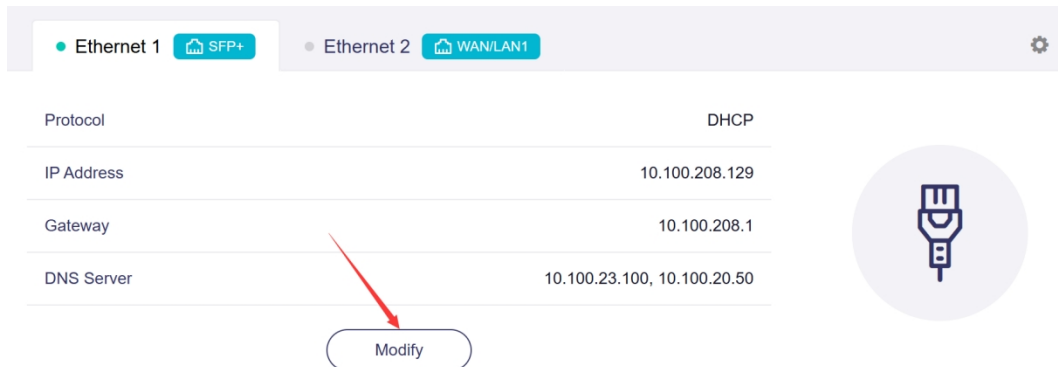


2. Log in to the router's web admin panel and navigate to **INTERNET > Ethernet**. If the connection is successful, the Ethernet section will display network details, including Protocol, IP Address, Gateway, and DNS Server.



Protocol

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



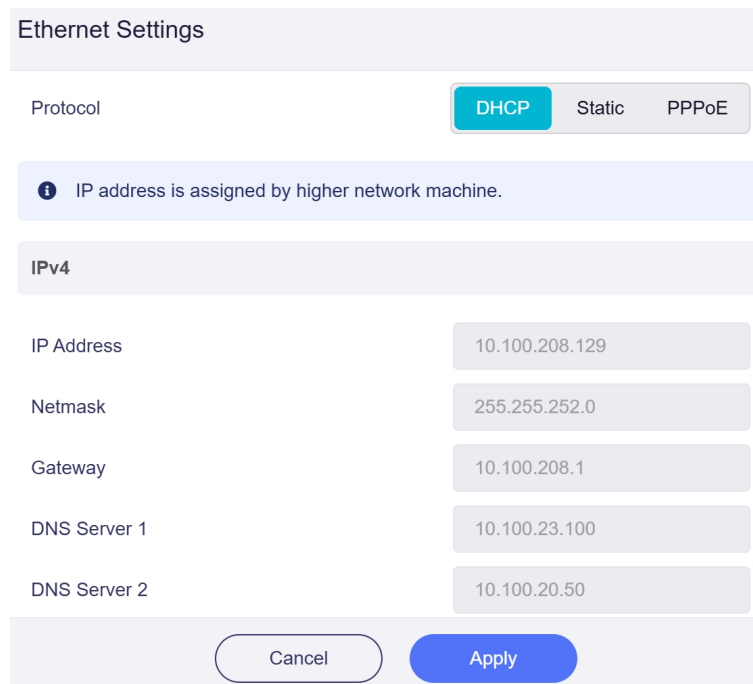
The screenshot shows the configuration page for Ethernet 1 (SFP+). The protocol is set to DHCP. The IP Address is 10.100.208.129, the Gateway is 10.100.208.1, and the DNS Server is 10.100.23.100, 10.100.20.50. A red arrow points to the 'Modify' button. A USB icon is visible on the right side of the page.

Protocol	DHCP
IP Address	10.100.208.129
Gateway	10.100.208.1
DNS Server	10.100.23.100, 10.100.20.50

[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.



The screenshot shows the Ethernet Settings page. The protocol is set to DHCP. A message states: "IP address is assigned by higher network machine." The IPv4 section shows the following configuration:

Field	Value
IP Address	10.100.208.129
Netmask	255.255.252.0
Gateway	10.100.208.1
DNS Server 1	10.100.23.100
DNS Server 2	10.100.20.50

Buttons: [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

When joining the network, there are some optional advanced settings.

Join Network

MAC Mode

Random

MAC Address

52:E2:A5:85:9D:96

Random

Auto Update MAC

Remember

Lock BSSID

Manually Set Static IP

TTL

Optional

HL

Optional

MTU

1500

Back

Apply

- **Remember:** Enable this to remember the current repeated Wi-Fi network. This is available in firmware v4.7 and later.
- **Lock BSSID:** If this option is enabled, the router will only connect to the AP corresponding to the BSSID you selected when switching to a network using this SSID.
- **Manually Set static IP:** This is available in firmware v4.7 and later.
- **TTL:** TTL (Time To Live) sets the maximum time for packets to survive in the network, and is filled in according to the requirements of the operator. By default, the router forwards the TTL of the incoming client device minus one. If you need to camouflage, you can set a fixed value here. the TTL is valid only for IPv4.
- **HL:** In IPv6, the HL (Hop Limit) field is used to limit the number of transmission hops of data packets in the network, which is equivalent to the TTL in IPv4.
- **MTU:** The default value is 1500.

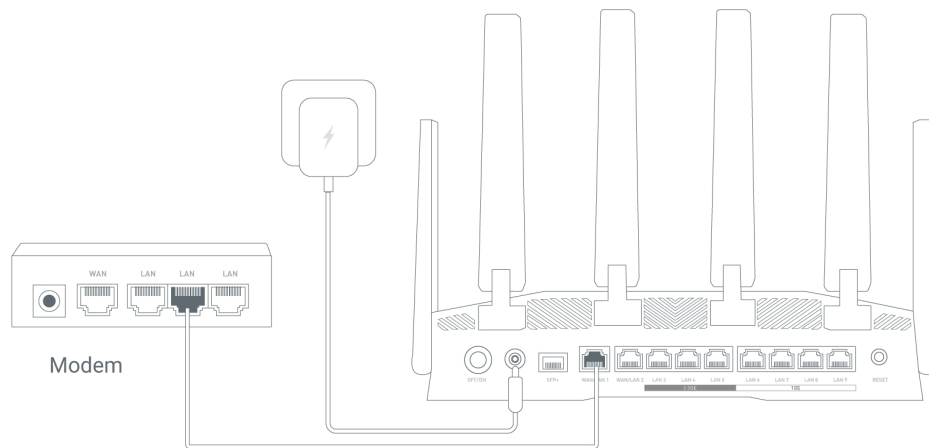
4.2.2 Connect to the Internet via Ethernet Cable

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/LAN1

Ethernet 2

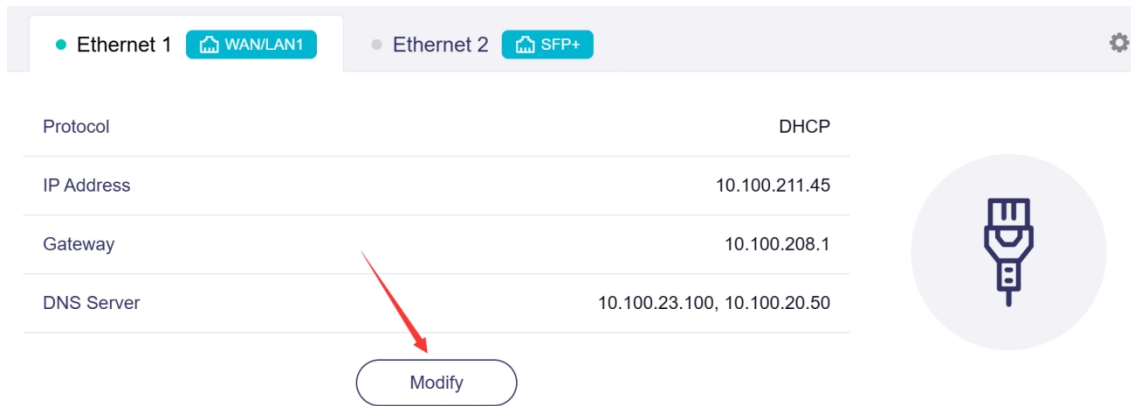
SFP+

Protocol	DHCP
IP Address	10.100.211.45
Gateway	10.100.208.1
DNS Server	10.100.23.100, 10.100.20.50

Modify

Protocol

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



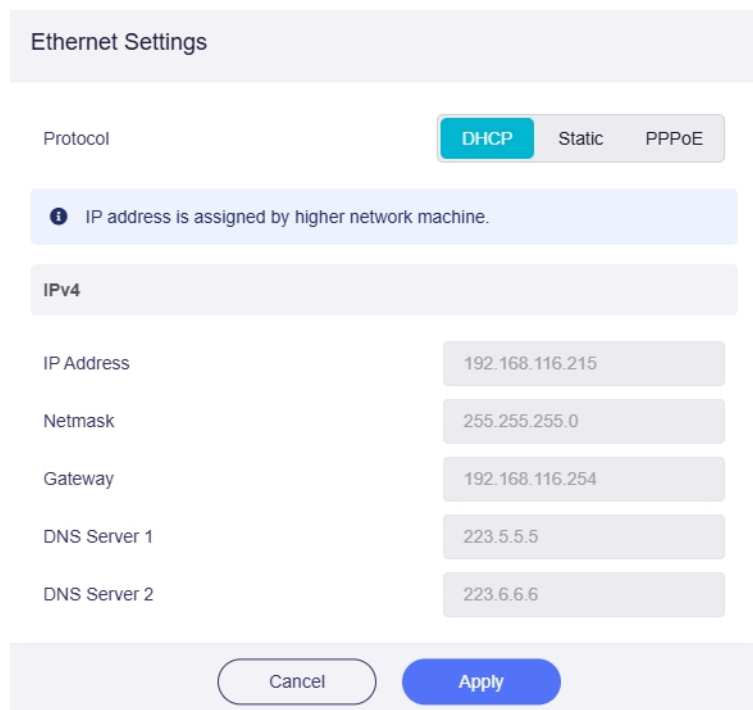
The screenshot shows the 'Ethernet Settings' interface. At the top, there are two tabs: 'Ethernet 1' (selected) and 'Ethernet 2'. Below the tabs is a table with the following data:

Protocol	DHCP
IP Address	10.100.211.45
Gateway	10.100.208.1
DNS Server	10.100.23.100, 10.100.20.50

A red arrow points to a 'Modify' button located below the table. To the right of the table is a circular icon containing a USB symbol.

- **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.



The screenshot shows the 'Ethernet Settings' interface with the 'DHCP' protocol selected. Below the protocol selection, there is a message: 'IP address is assigned by higher network machine.' Below this, there is a section for 'IPv4' configuration with the following fields:

Field	Value
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

At the bottom of the interface are 'Cancel' and 'Apply' buttons.

- **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.

Ethernet Settings

IPv4

IP Address	10.100.208.129
Netmask	255.255.252.0
Gateway	10.100.208.1
DNS Server 1	10.100.23.100
DNS Server 2	10.100.20.50

VLAN ID ⓘ Optional (1 ~ 4094)

TTL ⓘ Optional

HL ⓘ Optional

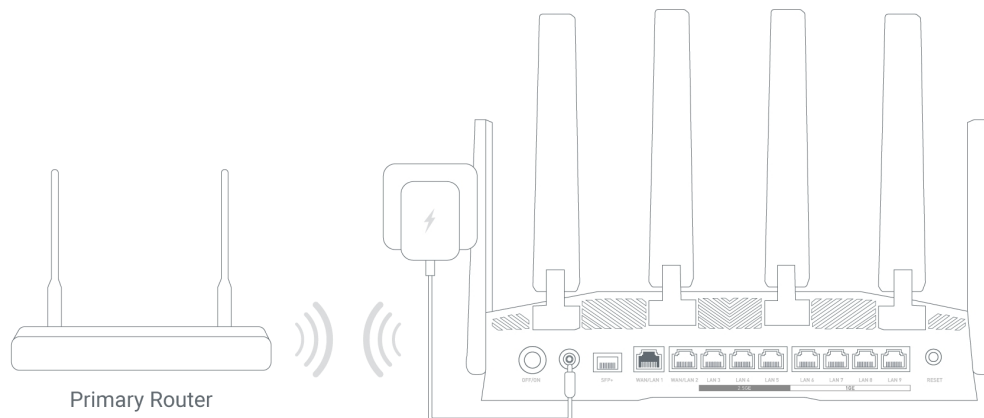
MTU ⓘ 1500

Cancel Apply

- **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.

4.2.3 Connect to the Internet via an Existing Wi-Fi

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

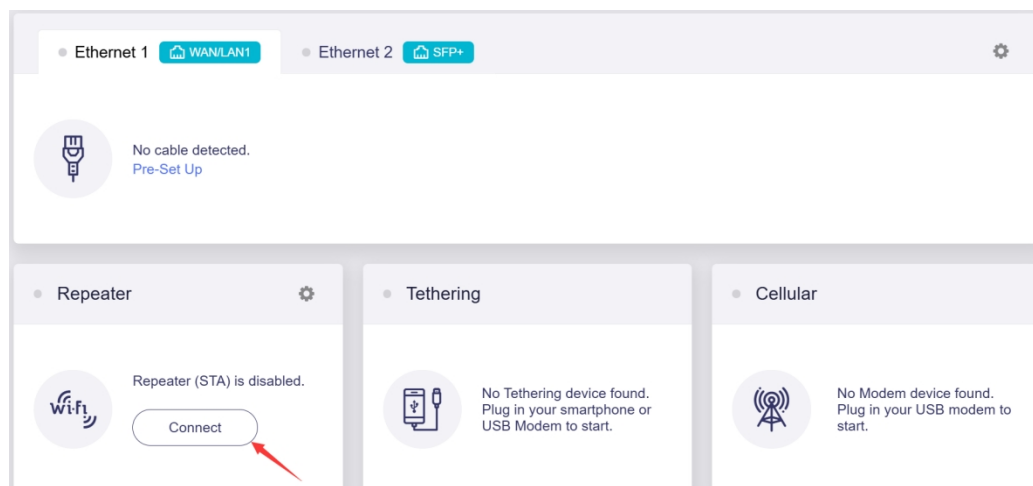


GL.iNet repeater feature works in WISP (Wireless Internet Service Provider) mode by default, which means that the router will create its own subnet and act as a firewall to protect you from the public network.

Basic Setup

Follow the steps below to connect your router to an existing Wi-Fi as a repeater.

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



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

Join Wi-Fi

Exit

The following Wi-Fi channels are supported. Please ensure that the Wi-Fi network you're connecting to uses one of them.

2.4G

 : 1-11;

5G

 : 36-64, 100-144, 149-165;

6G

 : 1-233

Available Networks

Join Other Network

GL-MT6000-6c7

2.4G

GL-MT6000-cc6

2.4G

GL-BE14000-6e2

2.4G

GL-BE14000-6e2-5G

5G

GL-MT6000-f79

2.4G

GL-MT6000-458

2.4G

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

Join Network

SSID

GL-OFFICE-5G

Password

Auto-Enable Login Mode for Public Hotspots

Enable Camouflage

MAC Mode

Random

MAC Address

6E:FD:E3:24:2A:EF [Random](#)

Auto Update MAC

Advanced Settings

Back

Apply

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

Available Networks → [Join Other Network](#)

GL-BE9300-c37
2.4G

GL-MT6000-f47
2.4G

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

GL-OFFICE-5G
5G

⚙️

IP Address	192.168.120.151
Gateway	192.168.120.1
DNS Server	192.168.101.10 , 202.96.134.133
BSSID	10:9F:4F:1E:48:45
MAC Address	📶 9A:39:00:58:34:57

Disable

Switch Network

Modify

Public Hotspot Settings

When connecting the router to a public hotspot with a captive portal, it is recommended to enable the following features to improve the connection success rate.

Join Network Exit

SSID

GL-OFFICE-5G

Password

Auto-Enable Login Mode for Public Hotspots ⓘ

☐

Enable Camouflage ⓘ

☐

MAC Mode

Random

MAC Address

7A:55:9A:AE:2E:20 Random

Auto Update MAC ⓘ

☐

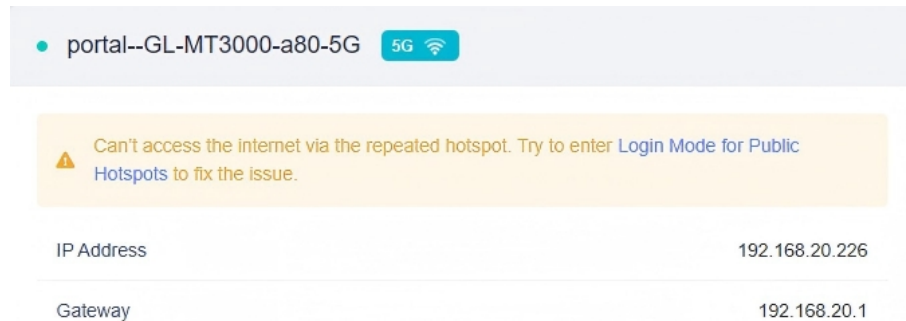
[Advanced Settings](#)

Back

Apply

- **Auto-Enable Login Mode for Public Hotspots**

If enabled, the router automatically enters Public Hotspot Login Mode when it is connected to a hotspot but not the Internet. In this mode, some services will be suspended while DNS mode switches to automatic, which may leak your network activity to the network provider (e.g., hotel, shopping mall). Even if disabled, the router will prompt you to enter this mode if it detects a hotspot captive portal or fails to log in.



- **Enable Camouflage**

If enabled, the router will masquerade as the client device you use to access the admin panel by emulating that device's MAC address.

- **MAC Mode**

Choose which MAC address the router uses to connect to the public hotspot.

Factory: Uses the device's original factory-assigned MAC address.

Clone: Clones a client device's MAC address for connection.

If the desired MAC isn't listed, manually enter the MAC address you want to clone. Note: Many devices use randomized MAC addresses (often called Private Wi-Fi Address or random hardware address) when connecting to Wi-Fi networks. As a result, the MAC address displayed here may not match the device's actual physical MAC.

Random: Automatically generates a random MAC address for connection.

- **Auto Update MAC**

If this option is enabled, the MAC address will be updated automatically.

When saving the network configuration, the MAC Mode, including any cloned or randomized MAC address, will be tied to the specific SSID you save. You can manually change these settings for each SSID at any time.

Advanced Settings

When joining the network, there are some optional advanced settings.

Join Network

MAC Mode

Random

MAC Address

52:E2:A5:85:9D:96

Random

Auto Update MAC

Remember

Lock BSSID

Manually Set Static IP

TTL

Optional

HL

Optional

MTU

1500

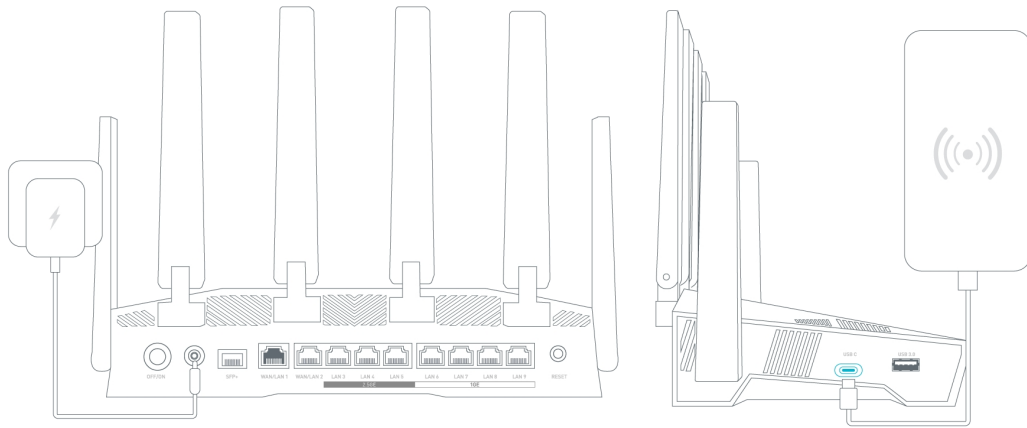
Back

Apply

- **Remember:** Enable this to remember the current repeated Wi-Fi network. This is available in firmware v4.7 and later.
- **Lock BSSID:** If this option is enabled, the router will only connect to the AP corresponding to the BSSID you selected when switching to a network using this SSID.
- **Manually Set static IP:** This is available in firmware v4.7 and later.
- **TTL:** TTL (Time To Live) sets the maximum time for packets to survive in the network, and is filled in according to the requirements of the operator. By default, the router forwards the TTL of the incoming client device minus one. If you need to camouflage, you can set a fixed value here. the TTL is valid only for IPv4.
- **HL:** In IPv6, the HL (Hop Limit) field is used to limit the number of transmission hops of data packets in the network, which is equivalent to the TTL in IPv4.
- **MTU:** The default value is 1500.

4.2.4 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.

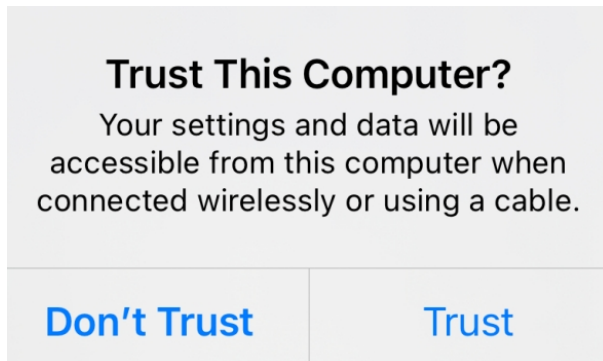


Host-less modem works in Tethering as well during the setup of the modem.

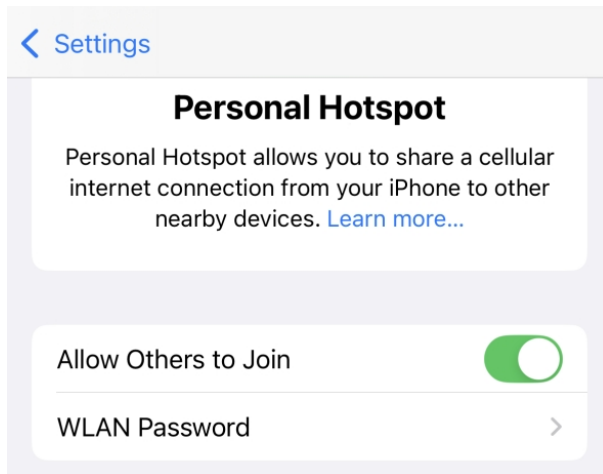
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

iPhone Tethering

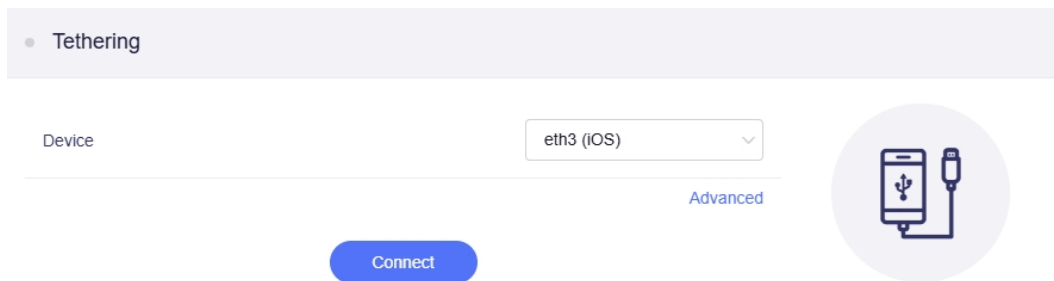
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



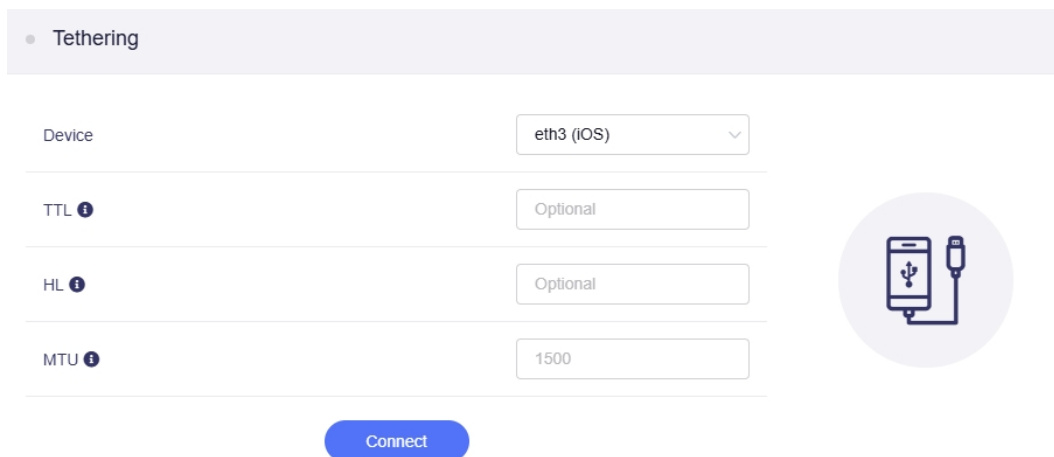
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



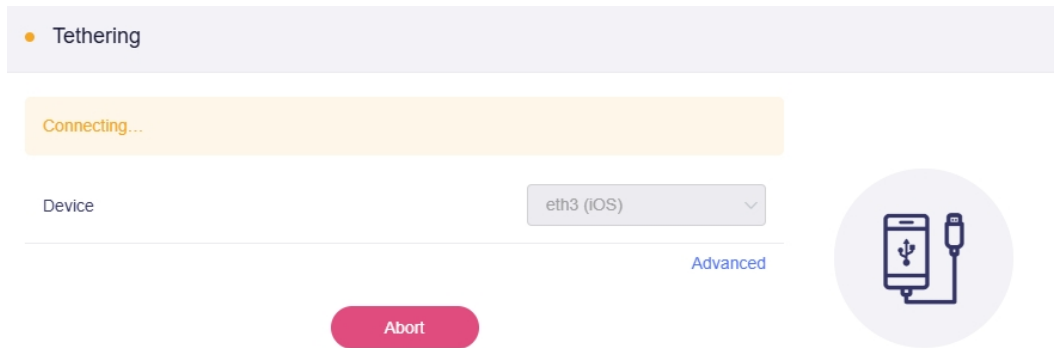
3. Connect a computer or another phone to the router. Log in to the router's web admin panel and navigate to **INTERNET > Tethering**, then click **Connect**.



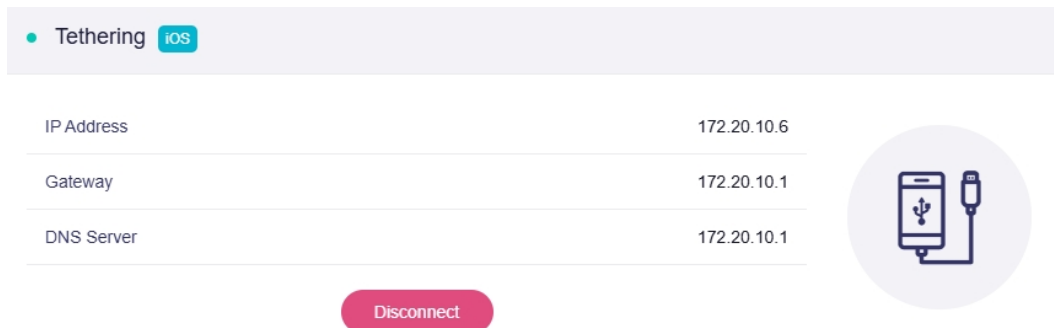
If you need to set advanced settings, such as TTL, HL, and MTU, click **Advanced** to customize these settings before clicking **Connect**.



4. It will start connecting.

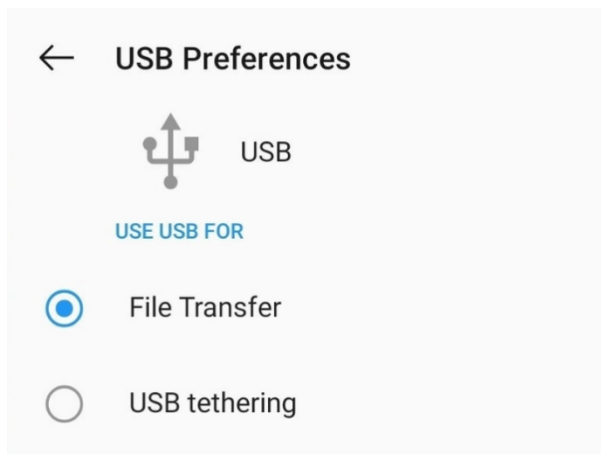


Once connected, this page will display the Tethering connection details.

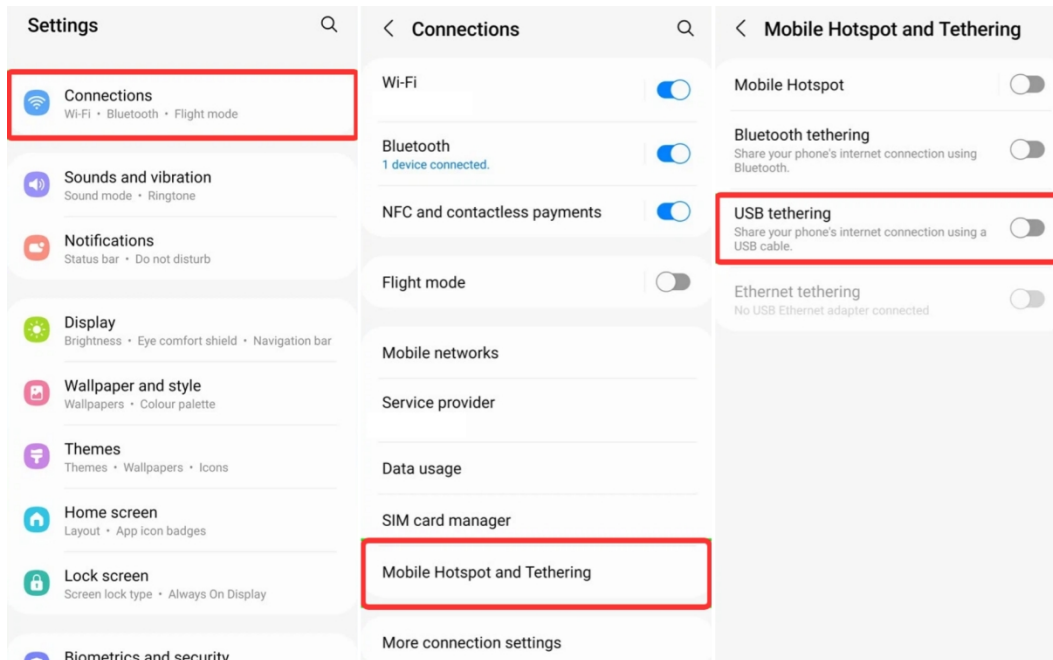


Android Tethering

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.

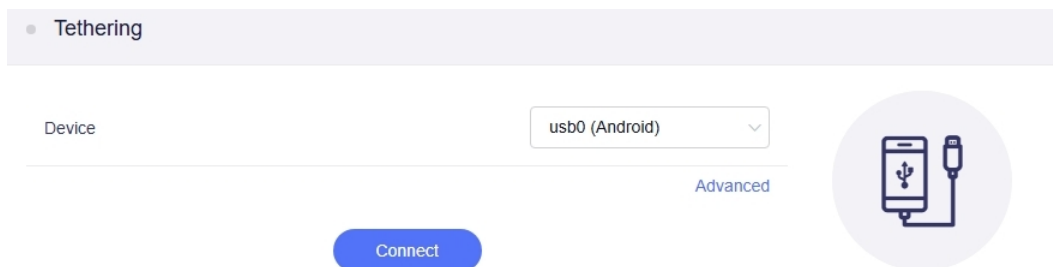


2. Go to your phone's **Settings > Network & Internet > Personal Hotspot**. Enable **Personal Hotspot** or **USB Tethering**.

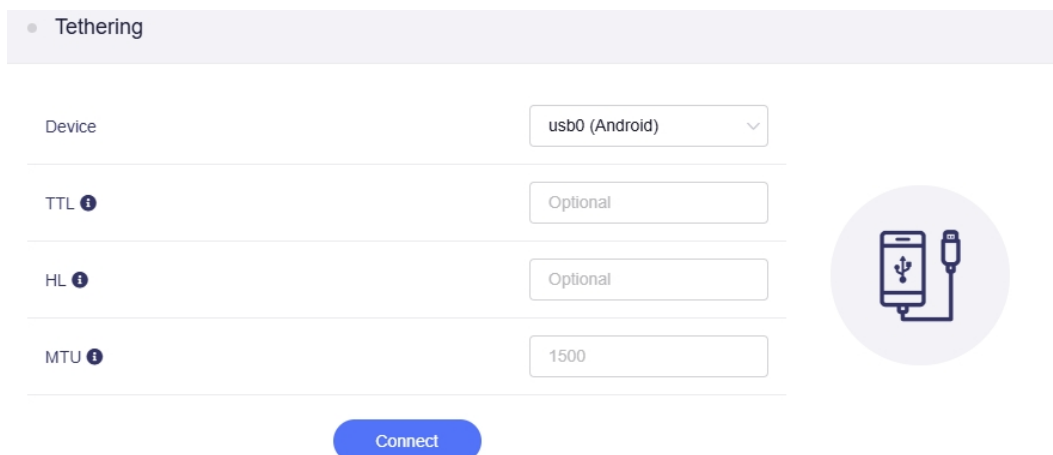


(The steps to enable USB Tethering vary by brand. Check your device's settings for the exact location, and contact your manufacturer's support if needed.)

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



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



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

Tethering

Android

IP Address	192.168.11.9
Gateway	192.168.11.1
DNS Server	192.168.11.1

Disconnect



Troubleshooting

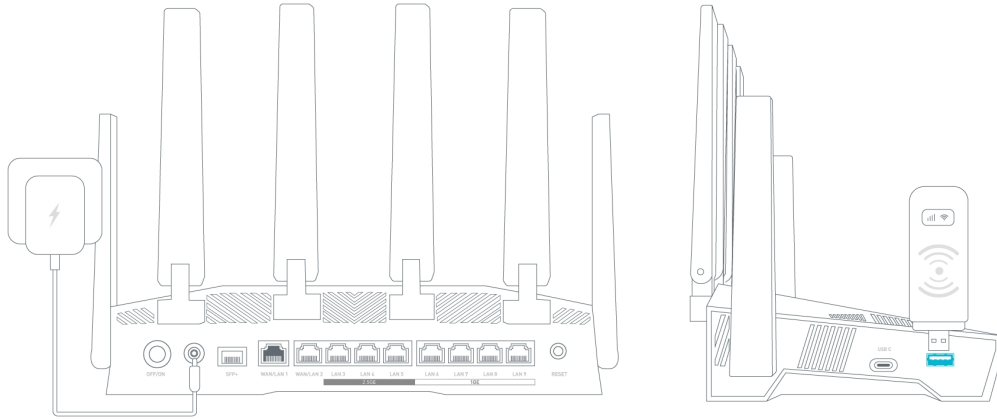
If the Tethering connection fails, try these troubleshooting steps:

- 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.

4.2.5 Connect to the Internet via USB Modem

Connect the router to the internet by inserting a cellular-enabled USB modem into its USB port. This allows the router to connect to the Internet via 4G/5G networks, providing connectivity without relying on fixed-line broadband. It is suitable for in-vehicle use or outdoor activities. Note that this connection is implemented through the router's Tethering or Cellular interface.



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

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

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



- 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:

- 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".
- 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

Wireless

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

5.1 Wi-Fi Status Display

The router's Wi-Fi networks are enabled by default, and the corresponding Wi-Fi icon will light up below the device model image on the INTERNET page.



If the cursor hovers over the enabled Wi-Fi icon, a Wi-Fi QR code will be displayed as follows. You can scan the Wi-Fi QR code to quickly connect to the corresponding Wi-Fi.



5.2 Wireless Settings

Log in to the router's web admin panel and navigate to **WIRELESS**.

The Wireless page lets you configure various Wi-Fi networks, including MLO Wi-Fi (available on selected models), Main Network, Guest Network and IoT Network. The supported Wi-Fi bands vary by model.

5.2.1 MLO Wi-Fi

MLO (Multi-Link Operation) is one of the core features of Wi-Fi 7 (802.11be), designed to improve network performance, significantly reduce latency, and enhance connection stability by utilizing multiple frequency bands simultaneously such as 2.4 GHz, 5 GHz, and 6 GHz.

To create an MLO Wi-Fi network, click the **Add** button on the right.

Multi-Link Operation (MLO)



Wi-Fi 7 clients are recommended to connect with MLO Wi-Fi, which can greatly improve the network transmission rate and reliability through multi-band connection.

+ Add



Select at least two Wi-Fi bands, configure Wi-Fi details, then click **Apply**.

Note: The available Wi-Fi bands vary by model.

Add Multi-Link Operation (MLO)



Wi-Fi Band

2.4 GHz



5 GHz



6 GHz



Wi-Fi Name (SSID)

GL-BE14000-6e2-MLO

Wi-Fi Security

WPA3-SAE



Wi-Fi Password

.....



SSID Visibility

Shown

Enable Randomized BSSID ⓘ

Cancel

Apply

- **Wi-Fi Band:** Select at least two radio bands. The available Wi-Fi bands vary by model.
- **Wi-Fi Security:** Set the Wi-Fi security mode to OPEN, WPA2-PSK, WPA/WPA2-PSK, WPA3-SAE, or WPA2-PSK/WPA3-SAE.
- **Enable Randomized BSSID:** If this option is enabled, the device uses a randomly generated BSSID and renews it at each reboot.

Once enabled, the page appears as shown below.

Multi-Link Operation (MLO)

Wi-Fi 7 clients are recommended to connect with MLO Wi-Fi, which can greatly improve the network transmission rate and reliability through multi-band connection.

2.4 GHz + 5 GHz + 6 GHz

GL-BE14000-6e2-MLO

Show

WPA3-SAE

43

5.2.2 Main Network

The Main Network is your primary Wi-Fi network, supporting simultaneous broadcasts across different radio bands, all enabled by default.

Click the gear icon on the right to view or modify Wi-Fi settings for each band, such as Wi-Fi SSID, security, password, randomized BSSID, TX power, bandwidth, and Wi-Fi channel.

Note: The available Wi-Fi bands vary by model.

Main Network

 6 GHz





GL-BE14000-6e2-6G

 *****



 Shown

 WPA3-SAE

 Channel: 53

 5 GHz





GL-BE14000-6e2-5G

 *****



 Shown

 WPA2-PSK/WPA3-SAE

 Channel: 52

 2.4 GHz





GL-BE14000-6e2

 *****



 Shown

 WPA2-PSK

 Channel: 2

5.2.3 Guest Network

The Guest Network is a dedicated Wi-Fi network for visitors, with all bands disabled by default. You can enable and configure basic network settings for each band, such as the Wi-Fi SSID, security mode, password, and enable randomized BSSID.

To create a Guest Wi-Fi network, click the **Add** button on the right.

Guest Network

Provide dedicated networks for visitors to ensure convenient and secure Internet access.

+ Add

Select a Wi-Fi band, configure Wi-Fi details, then click **Apply**.

Note: The available Wi-Fi bands vary by model.

Add Guest Network

Wi-Fi Band

☒ 2.4 GHz

☐ 5 GHz

☐ 6 GHz

Wi-Fi Name (SSID)

GL-BE14000-6e2-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Enable Randomized BSSID

☒

BSSID

Cancel

Apply

Once enabled, the page appears as shown below.

Guest Network

Provide dedicated networks for visitors to ensure convenient and secure Internet access.

 6 GHz

GL-BE14000-6e2-6G-Guest

Ⓜ

Ⓜ

Shown

WPA3-SAE



 5 GHz

GL-BE14000-6e2-5G-Guest

Ⓜ

Ⓜ

Shown

WPA2-PSK/WPA3-SAE



 2.4 GHz

GL-BE14000-6e2-Guest

Ⓜ

Ⓜ

Shown

WPA2-PSK



5.2.4 IoT Network

The IoT Network is a dedicated Wi-Fi network for smart devices, with all bands disabled by default. You can enable and configure basic network settings for each band, such as the Wi-Fi SSID, security mode, password, and enable randomized BSSID.

To create an IoT Wi-Fi network, click the **Add** button on the right.

IoT Network

 Provide dedicated networks for IoT devices. It is recommended to connect IoT devices to the 2.4 GHz band for better compatibility.

+ Add

Select a Wi-Fi band, configure Wi-Fi details, then click **Apply**.

Note: IoT network does not include the 6 GHz band, and the available Wi-Fi bands vary by model.

Add IoT Network

Wi-Fi Band

☒ 2.4 GHz

☐ 5 GHz

Wi-Fi Name (SSID)

GL-BE14000-6e2-IoT

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Enable Randomized BSSID



☒

BSSID

Cancel

Apply

Once enabled, the page appears as shown below.

IoT Network

5 GHz

GL-BE14000-6e2-5G-IoT

Show

WPA2-PSK



2.4 GHz

GL-BE14000-6e2-IoT

Show

WPA2-PSK



48

Chapter 6

Clients

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

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

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

Clients Access Control: Blocklist ⓘ Sort by Default ⚙ Settings						
Online Clients (2) ^						
Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
 GL-INET-08 self	 192.168.8.225 	↓ 10.56 KB/s ↑ 6.75 KB/s	↓ 2.41 GB ↑ 278.46 MB	☐	☐	...
 GL-INET-08	 192.168.8.191 	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	...
Offline Clients (1) ^						
Name	IP + MAC	Speed	Traffic	Reserved IP ⓘ	Block	Action
 iPhone	 192.168.8.214 ⓘ	↓ 0.00 B/s ↑ 0.00 B/s	↓ 290.43 MB ↑ 5.19 MB	☐	☐	...

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

6.1 Device Details

Clients Access Control: Blocklist ⓘ Sort by Default ⚙ Settings						
Online Clients (2) ^						
Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
 GL-INET-08 self	 192.168.8.225	↓ 75.85 KB/s ↑ 14.98 KB/s	↓ 2.41 GB ↑ 274.83 MB	☐	☐	...
 GL-INET-08	 192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	...

1. Device Name

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

2. IP and MAC Address

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



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

3. Speed

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

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

5. 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 if needed.

The screenshot shows the Mikrotik WinBox interface. At the top, the 'Clients' tab is active, and the 'Access Control: Blocklist' dropdown is highlighted with a red box. Below this, a table lists online clients. The 'Access Control' dropdown menu is open, showing 'Blocklist' (selected) and 'Allowlist' options.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225	↓ 75.85 KB/s ↑ 14.98 KB/s	↓ 2.41 GB ↑ 274.83 MB	☐	☐	...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	...

Access Control

Mode: Blocklist

Blocklist

Self MAC

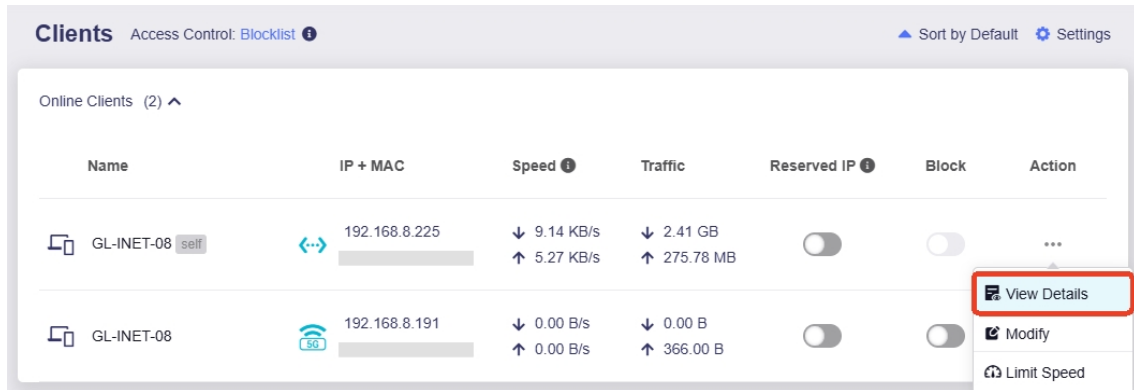
1	e.g. 11:22:33:44:55:66

- **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.

6.2 Action

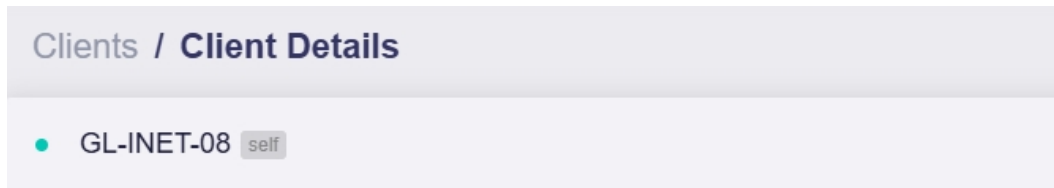
1. View Details

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.



The screenshot shows the 'Clients' page with a table of online clients. The table has columns: Name, IP + MAC, Speed, Traffic, Reserved IP, Block, and Action. The first client is GL-INET-08 with IP 192.168.8.225. The 'Action' column for this client is highlighted, showing a dropdown menu with 'View Details', 'Modify', and 'Limit Speed' options. The 'View Details' option is highlighted with a red box.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08	192.168.8.225	9.14 KB/s 5.27 KB/s	2.41 GB 275.78 MB	☐	☐	...
GL-INET-08	192.168.8.191	0.00 B/s 0.00 B/s	0.00 B 366.00 B	☐	☐	...



The screenshot shows the 'Client Details' page for GL-INET-08. The page has a header 'Clients / Client Details' and a sub-header 'GL-INET-08'. The details are as follows:

Property	Value
Hostname	GL-INET-08
Connection Method	Ethernet
MAC	
Speed	5.01 KB/s 3.80 KB/s
Traffic	2.41 GB 275.79 MB
Reserved IP	OFF
Block	OFF
IP Address	192.168.8.225

Hostname	GL-INET-08
Connection Method	Ethernet
MAC	
Speed	5.01 KB/s 3.80 KB/s
Traffic	2.41 GB 275.79 MB
Reserved IP	OFF
Block	OFF
IP Address	192.168.8.225

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 options for 'Sort by Default' and 'Settings'. Below this, a section titled 'Online Clients (2)' contains a table with columns: Name, IP + MAC, Speed, Traffic, Reserved IP, Block, and Action. Two clients are listed: 'GL-INET-08 self' and 'GL-INET-08'. The 'Action' column for the second client shows a three-dot menu with options: 'View Details', 'Modify' (highlighted with a red box), and 'Limit Speed'.

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

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225	↓ 4.81 KB/s ↑ 3.09 KB/s	↓ 2.41 GB ↑ 275.82 MB	☐	☐	...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	View Details Modify Limit Speed

Modify Client Device

Name: Auto

Device Type: Optional

- Desktop
- Phone
- Tablet PC
- Camera
- Wearable device
- Laptop
- Printer

Buttons: Cancel, OK

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 a table of online clients. The table has columns: Name, IP + MAC, Speed, Traffic, Reserved IP, Block, and Action. Two clients are listed: GL-INET-08 (self) and GL-INET-08. The 'Limit Speed' option is highlighted in the action menu for the second client.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225	↓ 797.00 B/s ↑ 1.56 KB/s	↓ 2.41 GB ↑ 275.83 MB	☐	☐	...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	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 box shows input fields for Download and Upload speeds, both currently set to 'Unlimited' KB/s. At the bottom are 'Cancel' and 'Apply' buttons.

Limit Speed Settings

↓ Download KB/s

↑ Upload KB/s

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

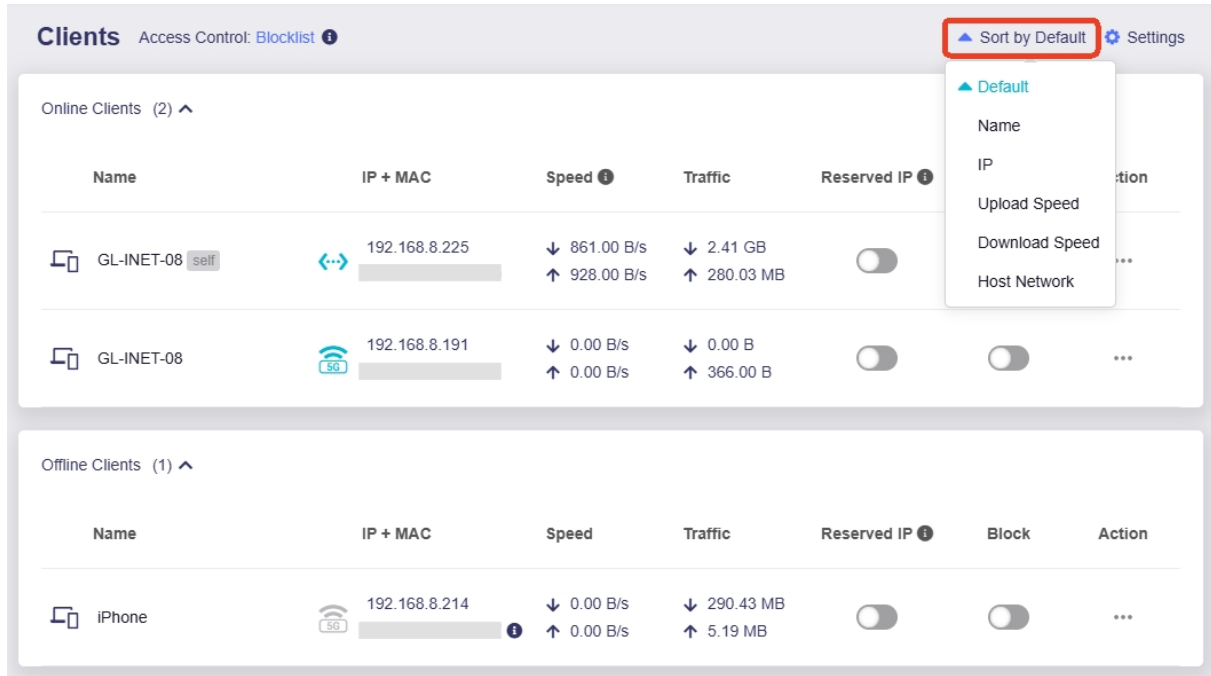
The screenshot shows the 'Clients' interface with the same table as before. The speed arrows for the first client (GL-INET-08 self) are now yellow, indicating that speed limitation has been applied.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225	↓ 3.82 KB/s ↑ 1.50 KB/s	↓ 2.41 GB ↑ 276.03 MB	☐	☐	...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	...

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.

6.3 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 'Sort by Default' dropdown menu open. The menu options are: Default, Name, IP, Upload Speed, Download Speed, and Host Network. The 'Sort by Default' option is highlighted with a red box.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225	↓ 861.00 B/s ↑ 928.00 B/s	↓ 2.41 GB ↑ 280.03 MB	☐		...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 366.00 B	☐	☐	...

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
iPhone	192.168.8.214	↓ 0.00 B/s ↑ 0.00 B/s	↓ 290.43 MB ↑ 5.19 MB	☐	☐	...

The default sorting order is as follows:

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

6.4 Settings

Click the **Settings** button in the upper right corner for further operations.

The screenshot shows the 'Clients' interface with 'Access Control: Blocklist'. The 'Settings' button is highlighted with a red box. The 'Settings' menu is open, showing options: 'Clear Traffic Statistics', 'Toggle Rate Unit', and 'Auto Remove Offline Clients' (which is currently turned off). The table below shows one online client.

Name	IP + MAC	Speed	Traffic	Reserved IP
GL-INET-08 self	192.168.8.225	↓ 71.15 KB/s ↑ 4.13 KB/s	↓ 981.93 MB ↑ 110.14 MB	☐

- **Clear Traffic Statistics:** Clear traffic statistics for all online clients with one click. Once applied, the traffic statistics column will be reset to zero and then restart the statistics.

Name	IP + MAC	Speed ⓘ	Traffic
GL-INET-08 self	192.168.8.225	↓ 43.12 KB/s ↑ 2.40 KB/s	↓ 0.00 B ↑ 0.00 B

- **Toggle Rate Unit:** Switch the rate unit for the speed column between **KB/s** and **Kbps**.
- **Auto Remove Offline Clients:** This feature was introduced in firmware v4.9. Once enabled, all offline clients will be cleared immediately and will not display in the Offline Clients section.

The screenshot shows the 'Clients' interface with 'Access Control: Blocklist'. A green banner indicates 'Auto Remove Offline Clients is currently ON'. The 'Settings' button is highlighted with a red box. The table below shows two online clients and zero offline clients.

Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
GL-INET-08 self	192.168.8.225	↓ 53.10 KB/s ↑ 9.37 KB/s	↓ 12.70 MB ↑ 2.06 MB	☐	☐	...
GL-INET-08	192.168.8.191	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 0.00 B	☐	☐	...

Offline Clients (0) ^

Chapter 7

Cloud Services

This chapter introduces two cloud services: GoodCloud and AstroWarp.

7.1 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.

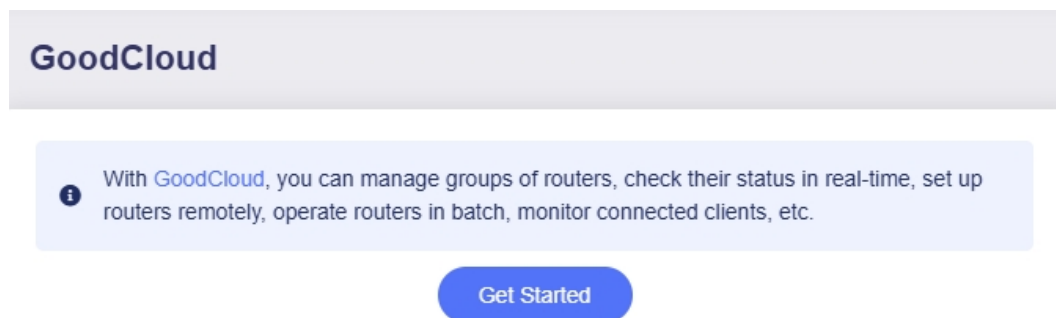
With GoodCloud, you can:

- 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 and VAR (Value Added Reseller) Plan. See [here](#) for details.

7.1.1 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**.

Go To Cloud Services ×

You're about to access the cloud services to complete the binding.
Tap "Continue" to proceed, or [Copy The Link](#).

Continue

- Log in with your GL.iNet account. If you don't have an account, sign up for one and log in.



Log In

Use your GL.iNet account

👁

[Forgot password?](#)

Log In

- Confirm your account and device information in the next step, then click **Bind**. You will then be redirected to the GoodCloud platform, where you can verify that your router has been bound to your account.

☐	Name ▾	Status ▾	Model	Version ▾	MAC	IP
☐	BE14000-6e2	Online	BE14000	4.9.1		

Tips:

- The GoodCloud binding steps differ by firmware version.
 - If you do not receive the verification email during sign-up, check your spam folder or try again later. For further assistance, contact us at support@gl-inet.com.
- After binding successfully, click the **Cloud icon** in the upper right corner of the web admin panel. You will 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](#)

6. In the router's web admin panel, navigate to **CLOUD SERVICES > GoodCloud** and enable remote access to the bound router's web admin panel and terminal. This is particularly useful for remote management and troubleshooting.

GoodCloud

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.

61

7.1.2 Manage Your Router

Check Device Details

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

Name / MAC / IP / SN / IMEI

Filter

Name ▾

Status ▾

Model

Version ▾

MAC

IP

BE14000-6e2

Online

BE14000

4.9.1

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.

BE14000-6e2 Online

[Remote GUI](#) [Remote SSH](#) [Reboot Device](#)

Basic Info



BE14000

Network Mode
Router

Version
4.9.1

MAC Address
[redacted]

IP
[redacted]

SN
[redacted]

Memory Usage
54%

Compile Time
2026-07-22 13:55:32

Up Time
2 days 3 hrs 1 mins

[Refresh](#)

Statistical Data

Interfaces

Ethernet Ports



Network Latency

233.26 ms 1.67 ms 0 %

Latency Jitter Packet Loss

[Retest](#)

Device Status History



[More](#)

Network Traffic Analysis Clients List VPN Server Share

Internet

Ethernet1 WAN

✓ Connected

IP Address 10.100.211.45

Protocol DHCP

[More](#)

Ethernet2 WAN

⊗ Not Physically Connected

IP Address --

Protocol DHCP

[More](#)

Repeater 5G

✓ Connected

IP Address 10.100.46.211/20

SSID @GL-OFFICE

[More](#)

Tethering

⊗ Disconnect

IP Address --

Device List

[Details](#)

Wi-Fi

MLO Wi-Fi Main

GL-BE14000-6e2-MLO

0 Online Clients

[More](#)

6GHz Wi-Fi Main

GL-BE14000-6e2-6G

0 Online Clients

[More](#)

5GHz Wi-Fi Main

GL-BE14000-6e2-5G

2 Online Clients

[More](#)

2.4GHz Wi-Fi Main

GL-BE14000-6e2

0 Online Clients

[More](#)

6GHz Wi-Fi Guest

GL-BE14000-6e2-6G-Guest

0 Online Clients

[More](#)

5GHz Wi-Fi Guest

GL-BE14000-6e2-5G-Guest

0 Online Clients

[More](#)

2.4GHz Wi-Fi Guest

GL-BE14000-6e2-Guest

0 Online Clients

[More](#)

5GHz IOT Wi-Fi IOT

GL-BE14000-6e2-5G-IoT

0 Online Clients

[More](#)

2.4GHz IOT Wi-Fi IOT

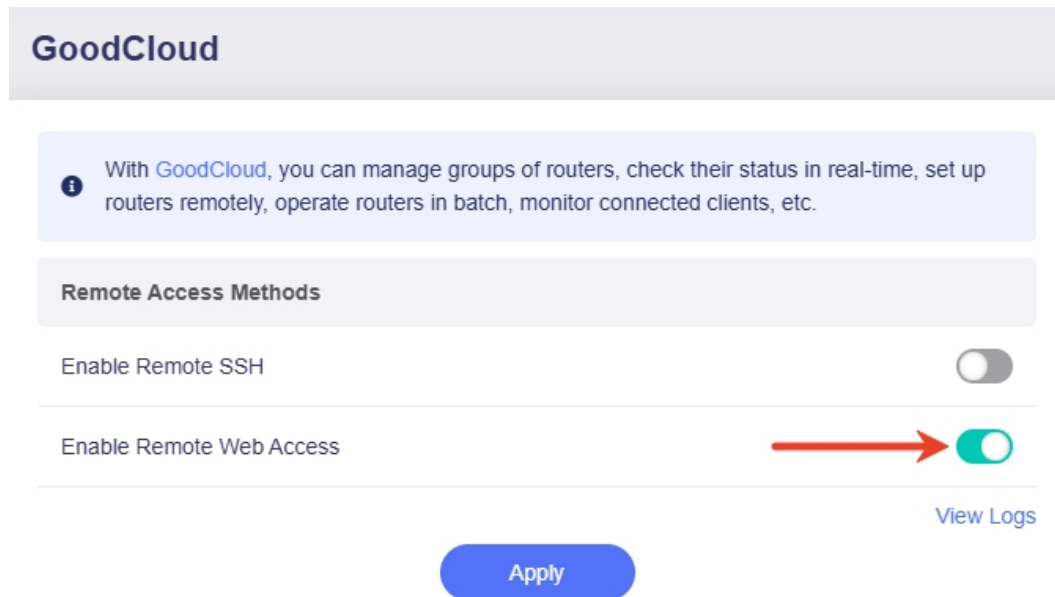
GL-BE14000-6e2-IoT

0 Online Clients

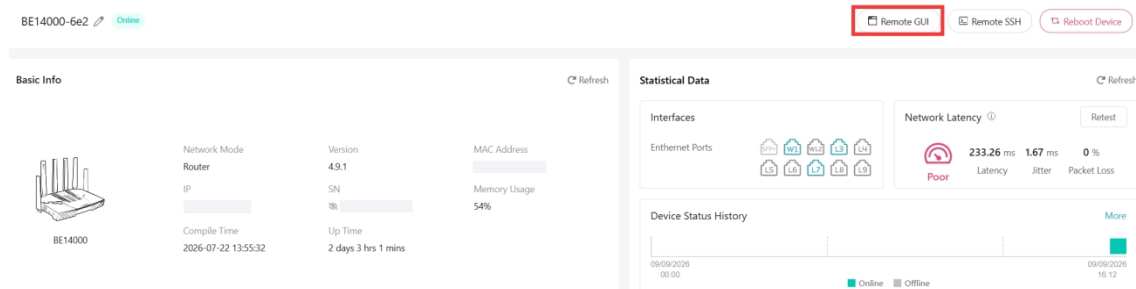
[More](#)

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 if needed, and the port will automatically change to 443. Then click **Apply**.

Remote GUI

☒ HTTP ☐ HTTPS

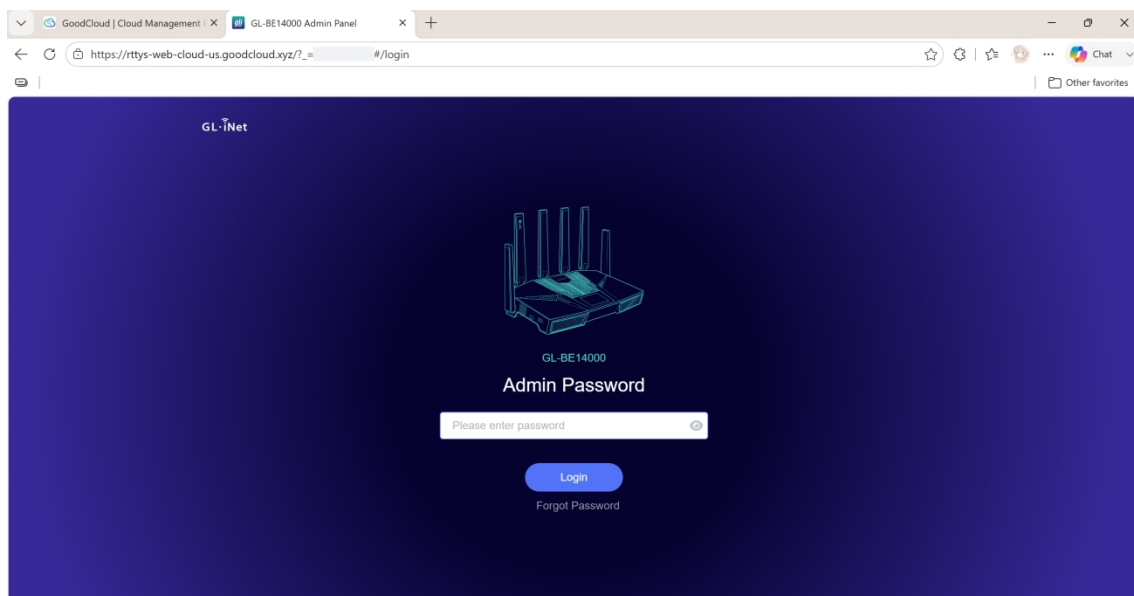
* Port

80

Cancel

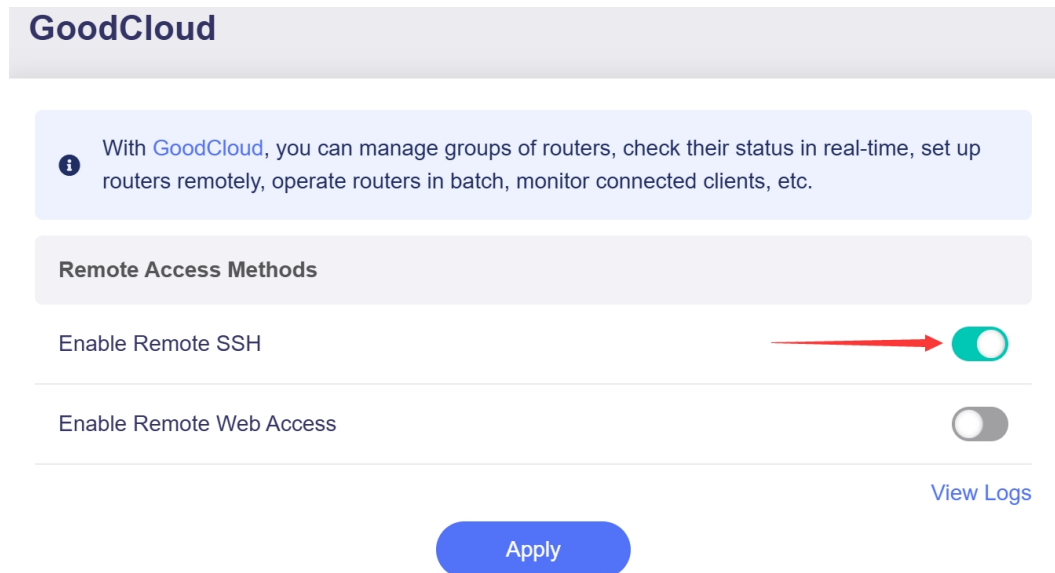
Apply

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.

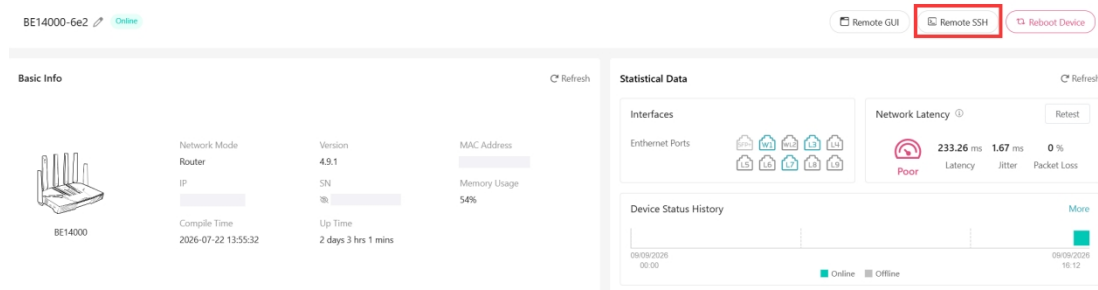


Remote Access Terminal

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



- Log in to the [GoodCloud](#) platform and navigate to **Devices** > **Bound Devices**. Click the device you want to access, and you will enter the device details page.
- 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.

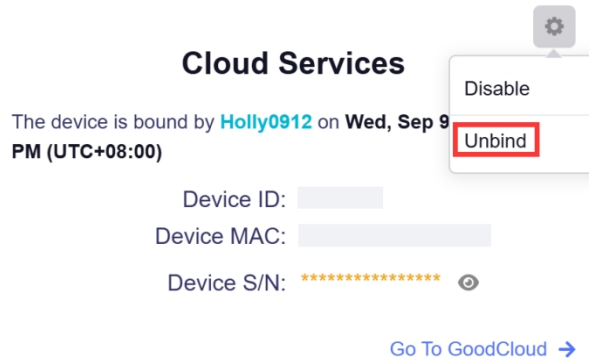
```
GL-BE14000 login: root
Password:

BusyBox v1.33.2 (2025-10-10 07:14:26 UTC) built-in shell (ash)

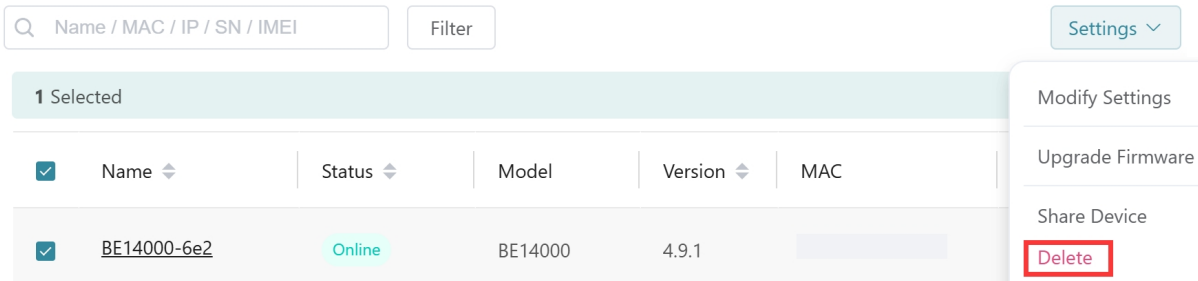
|_| .----- .----- .----- | |_| | | | .----- | |_| | | | | | | | |
|_| - || | | - || | | | | | | | | | | |
|_| | | | | | | | | | | | | | | | |
|_| | | W I R E L E S S F R E E D O M
-----
OpenWrt 21.02-SNAPSHOT,
-----
root@GL-BE14000:~# |
```

7.1.3 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.

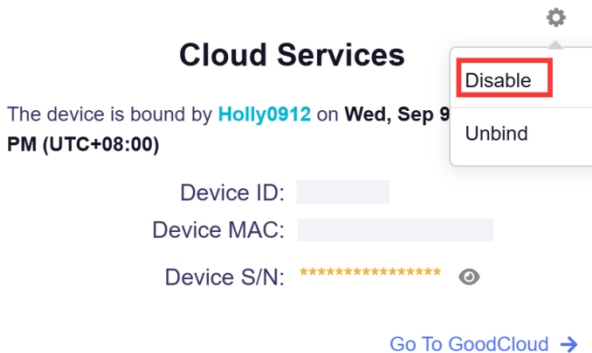


Alternatively, log in to the Cloud platform and navigate to **Devices > Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



7.1.4 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.

7.2 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.

7.2.1 Quick Setup

Below is an example of using Flint 4 (GL-BE14000) and Beryl 7(GL-MT3600BE) to set up an AstroWarp network. Flint 4 is the home router, while Beryl 7 is the travel router that routes network traffic back to Flint 4 for Internet access.

1. Configure Flint 4 for Internet.
Log in to the Flint 4'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.
2. In the Flint 4'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

QADXNSCB
[Copy](#)

This access code will expire in **09:59**.

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 Beryl 7 for Internet.

Log in to the Beryl 7'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 Beryl 7'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.

Q

A

D

X

N

S

C

B

Verifying, please wait a moment...

It will then connect to the Flint 4 home router 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

< 1 Minute

5. In the Flint 4's web admin panel, it also displays the connection status, as shown below.

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
 MT3600BE	Connected	Connected for: 1 Minute	...

7.2.2 Test Connectivity

1. Connect a laptop or smartphone to the Wi-Fi of the Beryl 7 travel router.
2. Open a browser and visit ipcheck.ing or any other IP address lookup website. It will show the public IP address of Flint 4, indicating that Beryl 7 is accessing the Internet through your Flint 4 home router.

1 IP Probe: IPCheck.ing IPv4

183.178.10.100 

 Region	 State	 City
 Hong Kong SAR 	Kwai Tsing District	Kwai Chung 
 Time Zone	 ISP	
Asia/Hong_Kong +08:00	Hong Kong Broadband Network Limited	

3. Disconnect the AstroWarp connection on Beryl 7, then refresh the webpage to resubmit the IP query request. It will show the public IP address of Beryl 7, indicating that Beryl 7 is accessing the Internet through its local network.

1 IP Probe: IPCheck.ing IPv4

112.97.10.100 

 Region	 State	 City
 China 	Guangdong	Shenzhen 
 Time Zone	 ISP	
Asia/Shanghai +08:00	China Unicom CHINA169 Guangdong Province Network	

Chapter 8

Get To Know VPN

This chapter introduces VPN concepts and common use scenarios.

8.1 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.

8.2 Application Scenarios

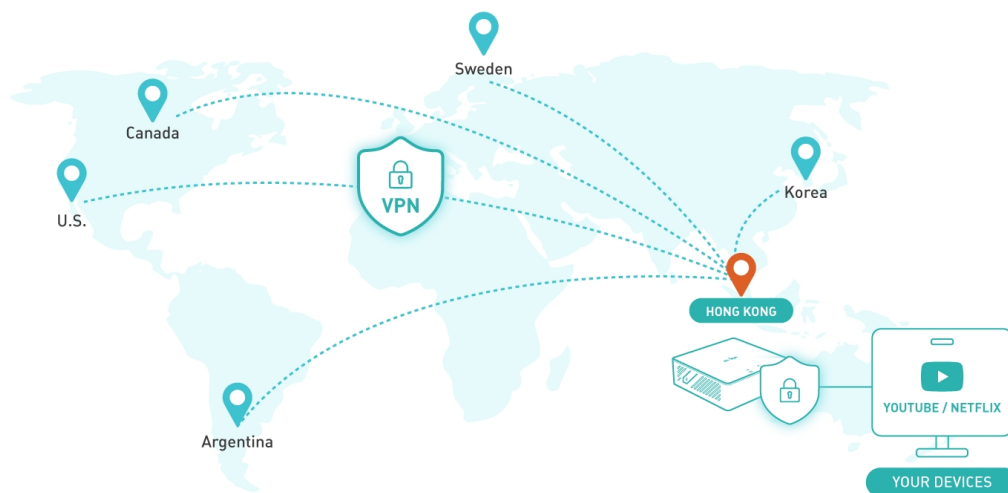
1. Personal Data Privacy

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



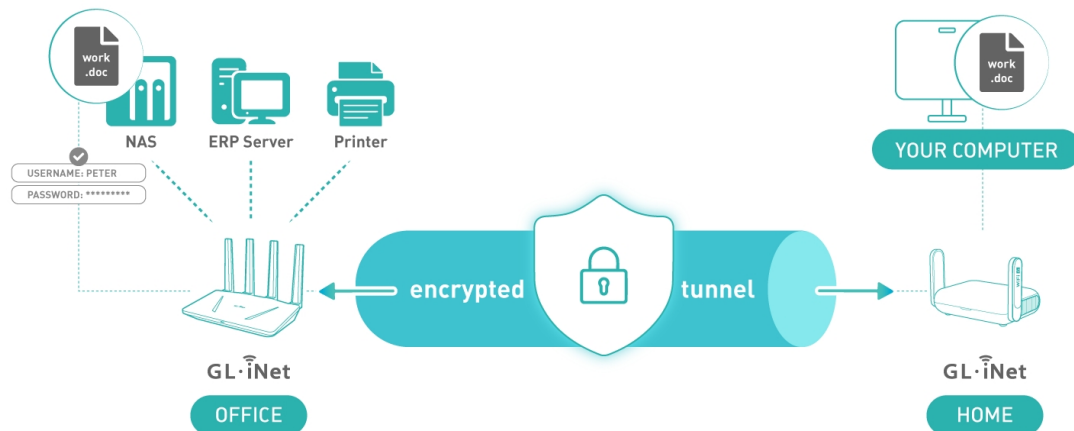
2. Unrestricted Access Worldwide

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



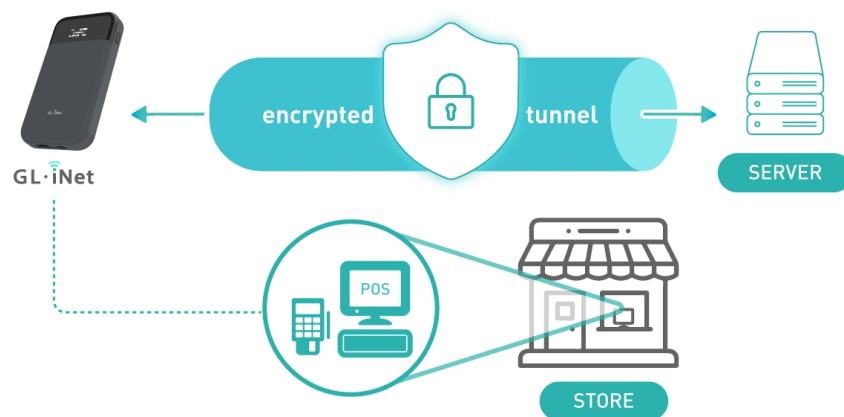
3. Small Business Data Security

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



4. Secure Payment Infrastructure

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



Chapter 9

VPN Dashboard

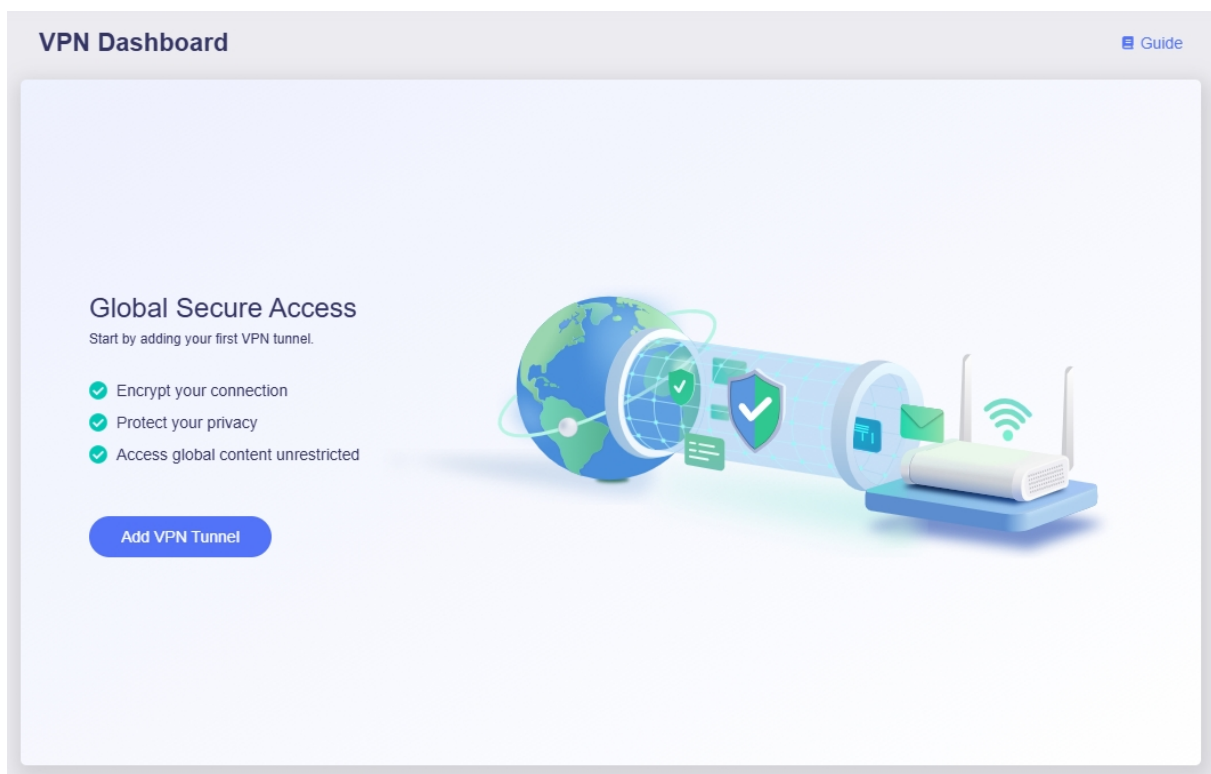
This chapter introduces how to manage VPN connections via the web admin panel.

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

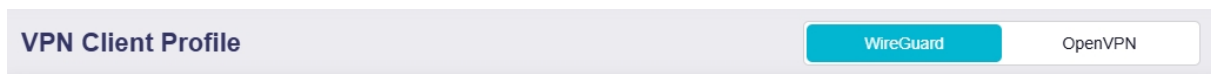
The VPN dashboard displays VPN connection details, such as routing rules, connected server, traffic statistics, client virtual IP, and connection log, and allows users to configure advanced settings such as the VPN Kill Switch, IP Masquerading, and MTU.

9.1 Upload VPN Profile

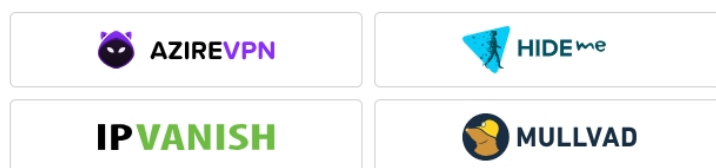
When entering this page for the first time, if no tunnels have been created, the page appears as follows. Click **Add VPN Tunnel** to get started.

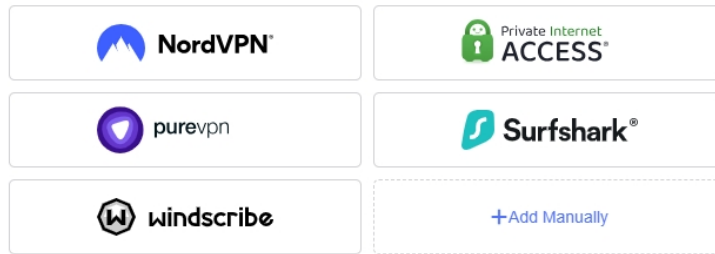


You will be directed to the **VPN Client Profile** page. Select a VPN provider and log in.



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.

PureVPN93

+ 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.

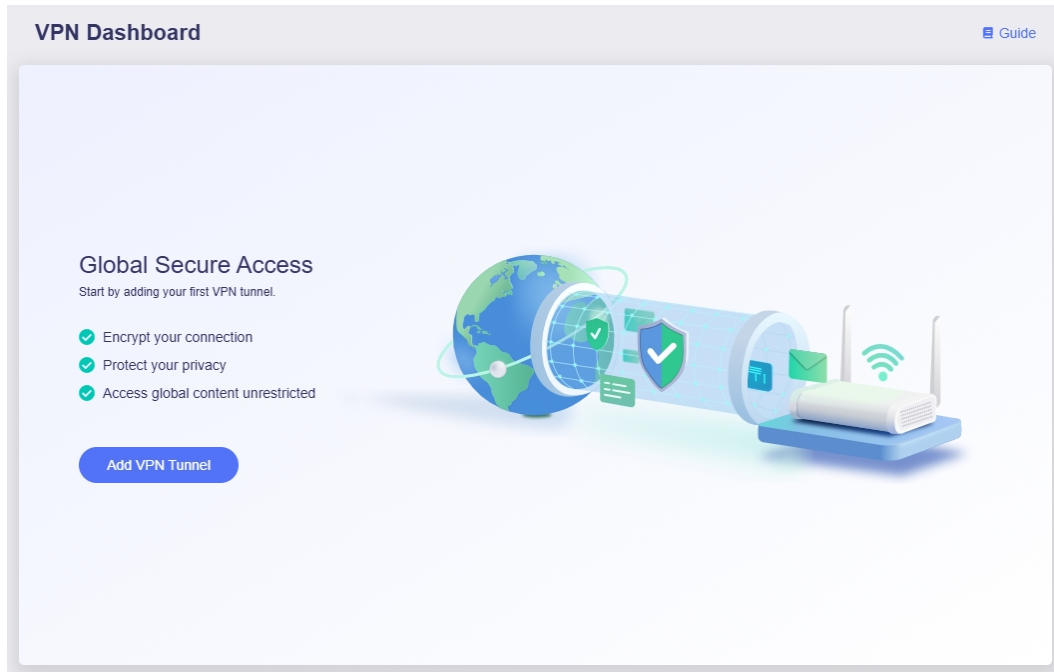
Tip: For some VPN service providers, you may need to select a VPN protocol or preferred servers/cities before the list of profiles appears.

9.2 Add VPN Tunnel

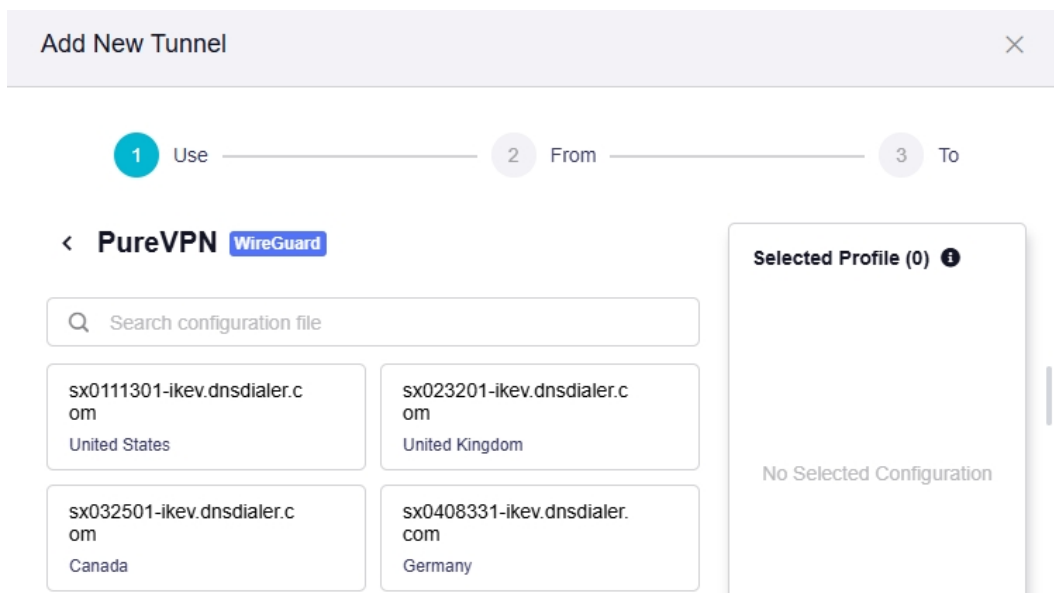
9.2.1 General Steps

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	

Cancel
Next

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.

9.2.2 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

82

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	To
2 Devices	All Targets

 United Kingdom
sx023201-ikev dnsdialer.com

Client Virtual IP (IPv4) —

Server Address —

Server Listen Port —

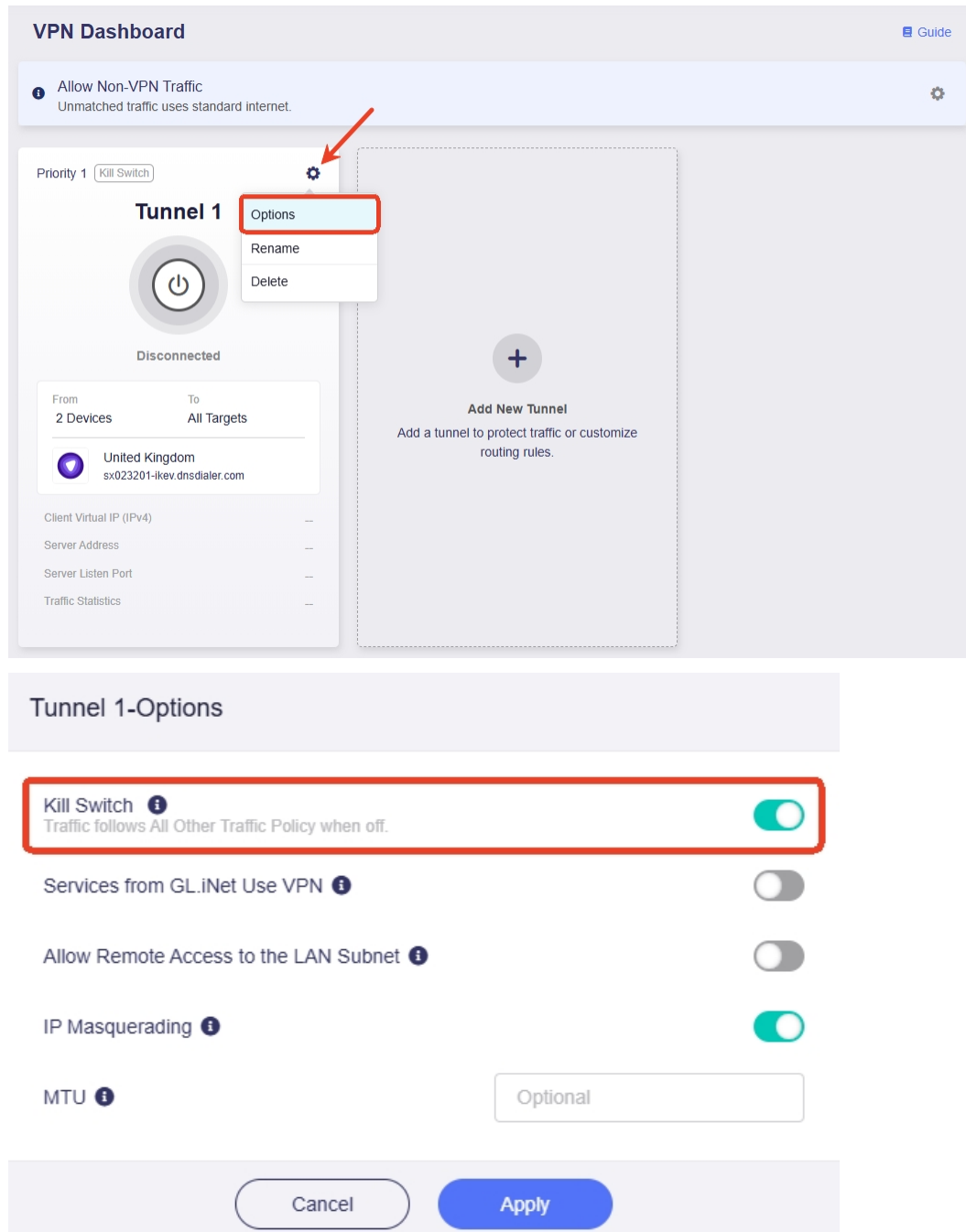
Traffic Statistics —



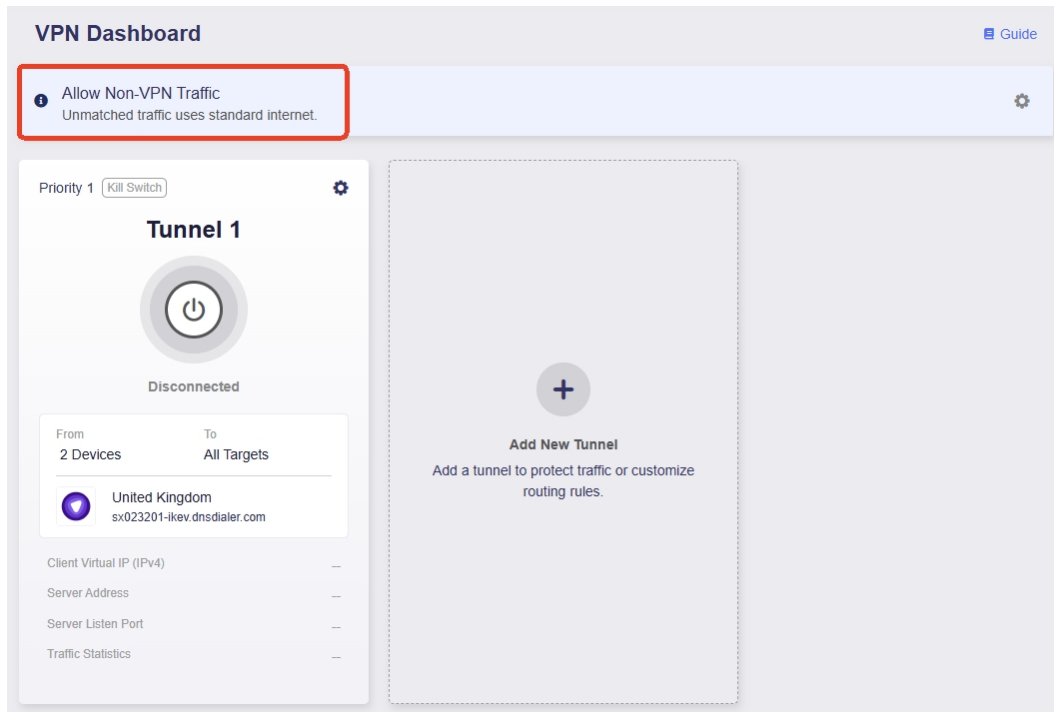
Add New Tunnel

Add a tunnel to protect traffic or customize routing rules.

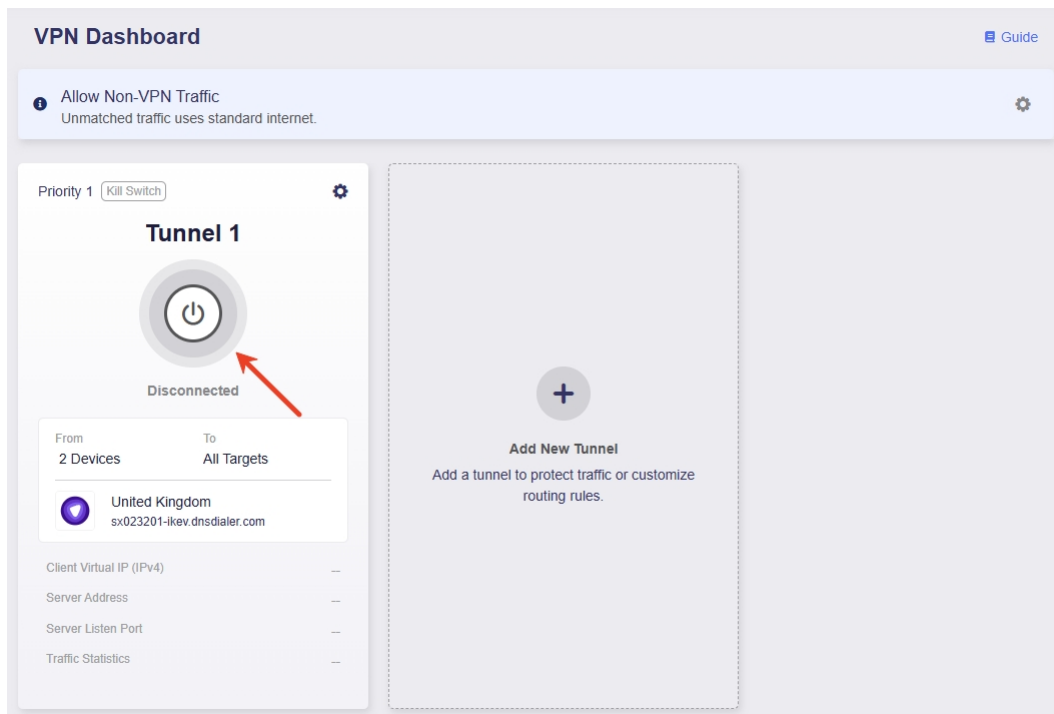
5. Make sure the **Kill Switch** for this tunnel is enabled. If the VPN disconnects unexpectedly, Internet access for traffic matching this tunnel will be blocked to prevent DNS leaks and IP tracking.



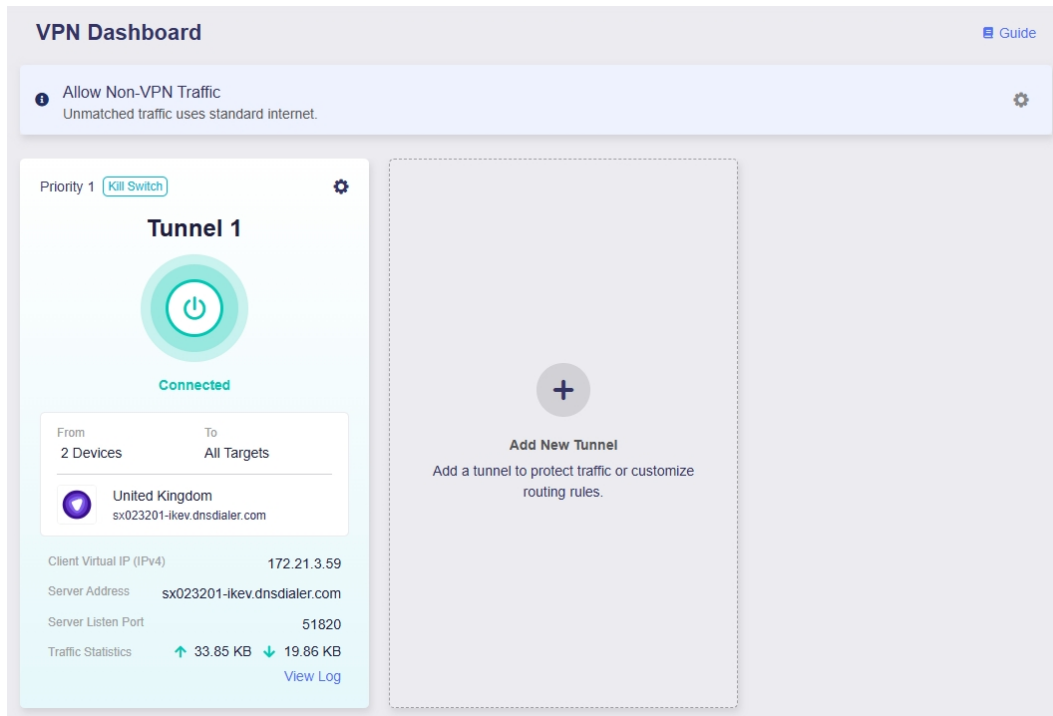
6. Make sure the **Allow Non-VPN Traffic** is enabled. This is enabled by default to ensure that traffic not matching the VPN tunnel can still access the Internet through the local WAN.



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

1 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.

88

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

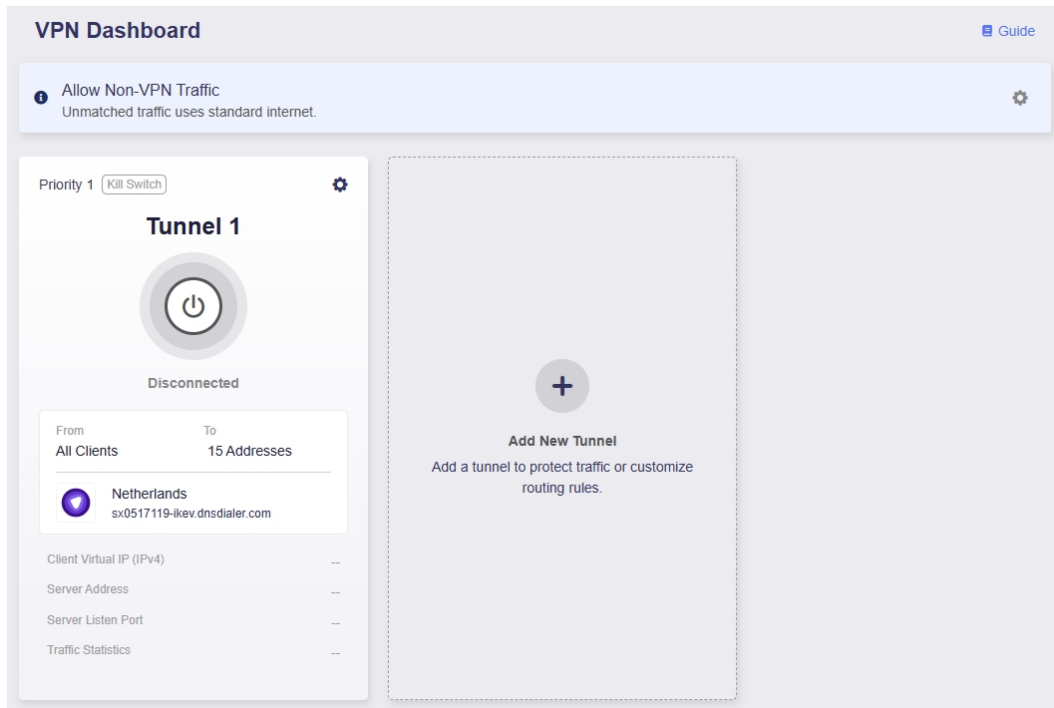
14 hulu.com

15 spotify.com

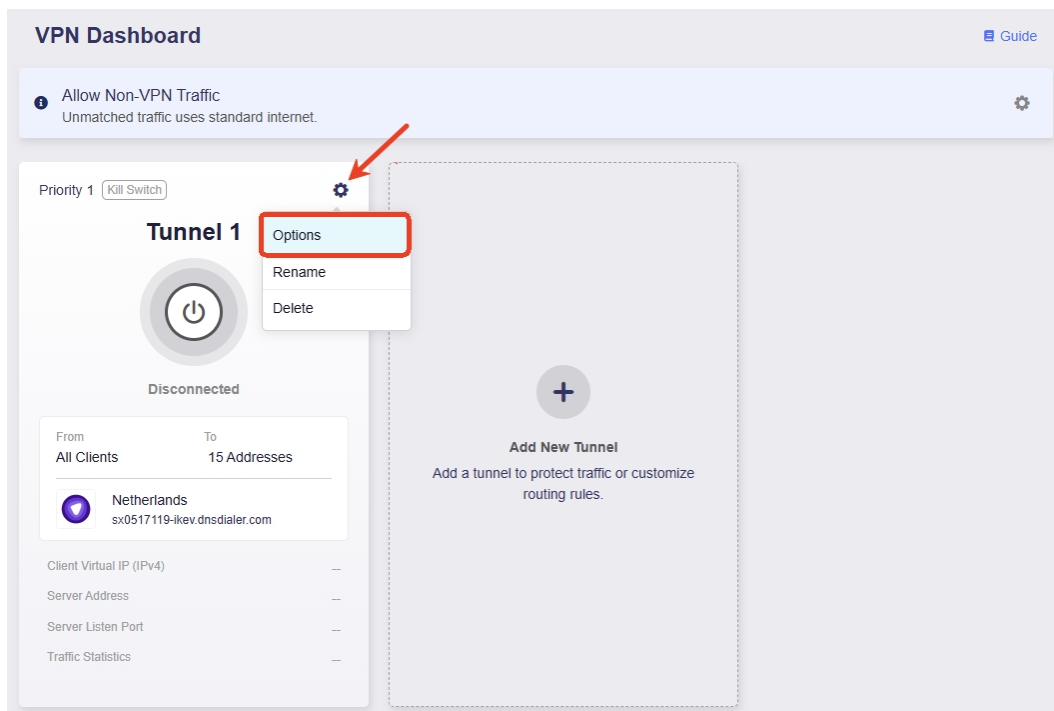
Back

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

- 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.

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

91

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.



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

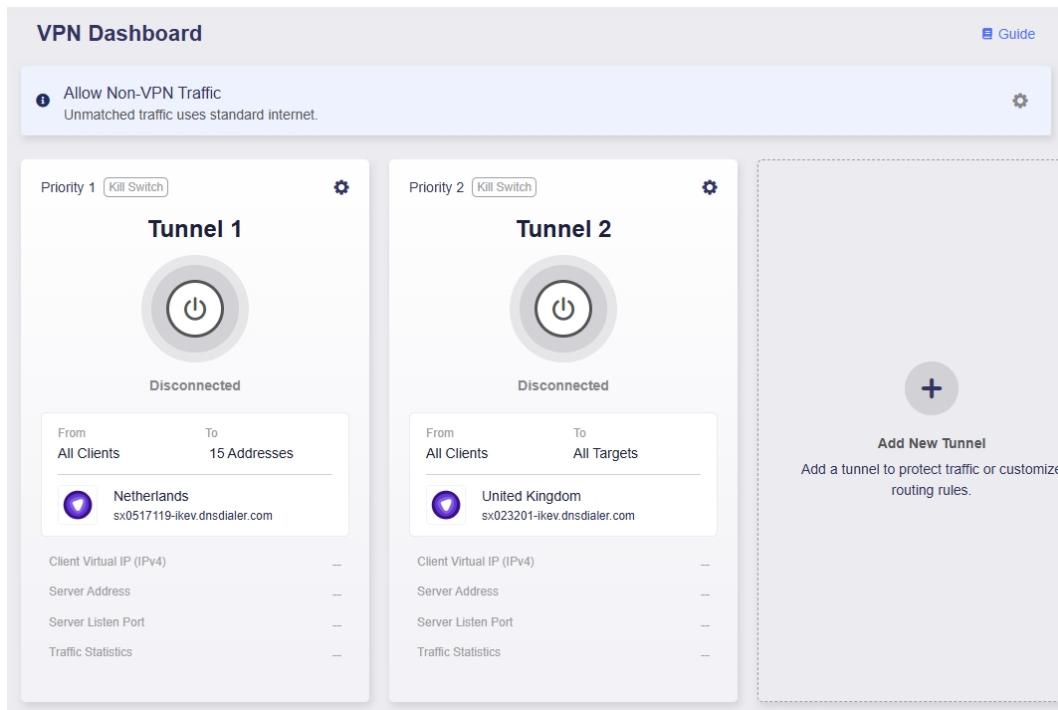
ⓘ Route all traffic from the selected source(s) through this VPN tunnel.



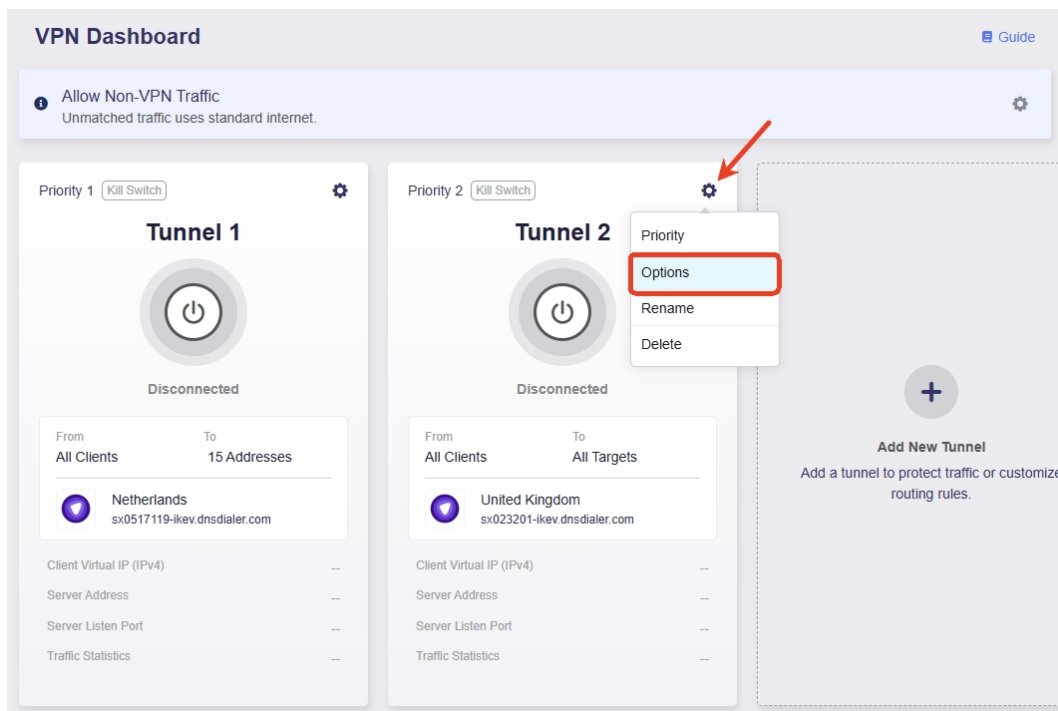
Back

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

12. 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.

95

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.

96

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.

9.3 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](#).

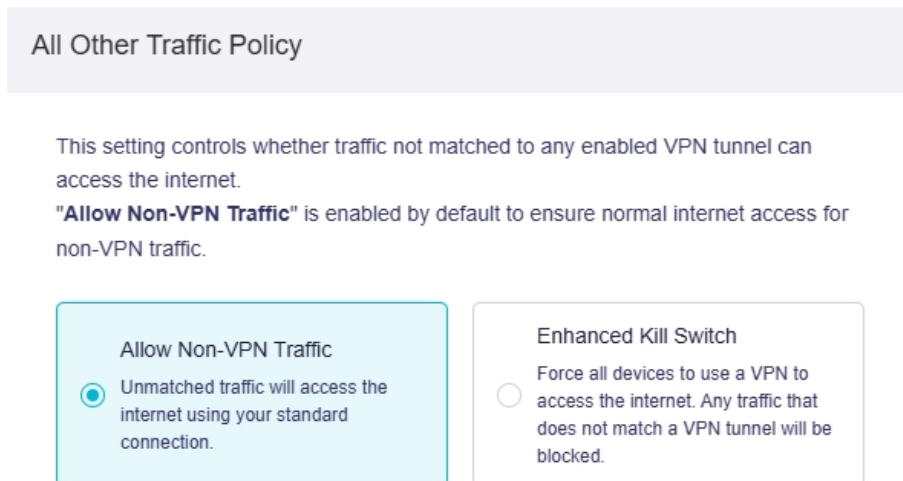
9.4 All Other Traffic

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

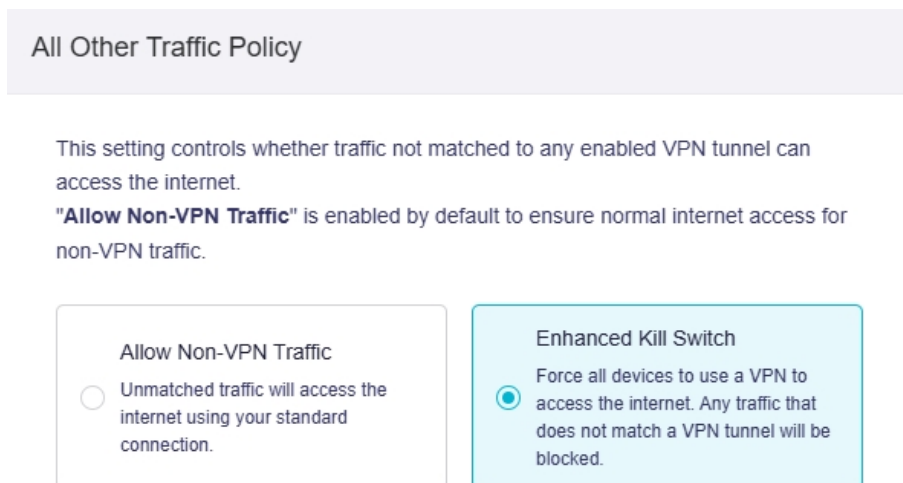


This policy controls whether traffic that does not match any of your VPN tunnel groups can access the Internet or not. It has two options:

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



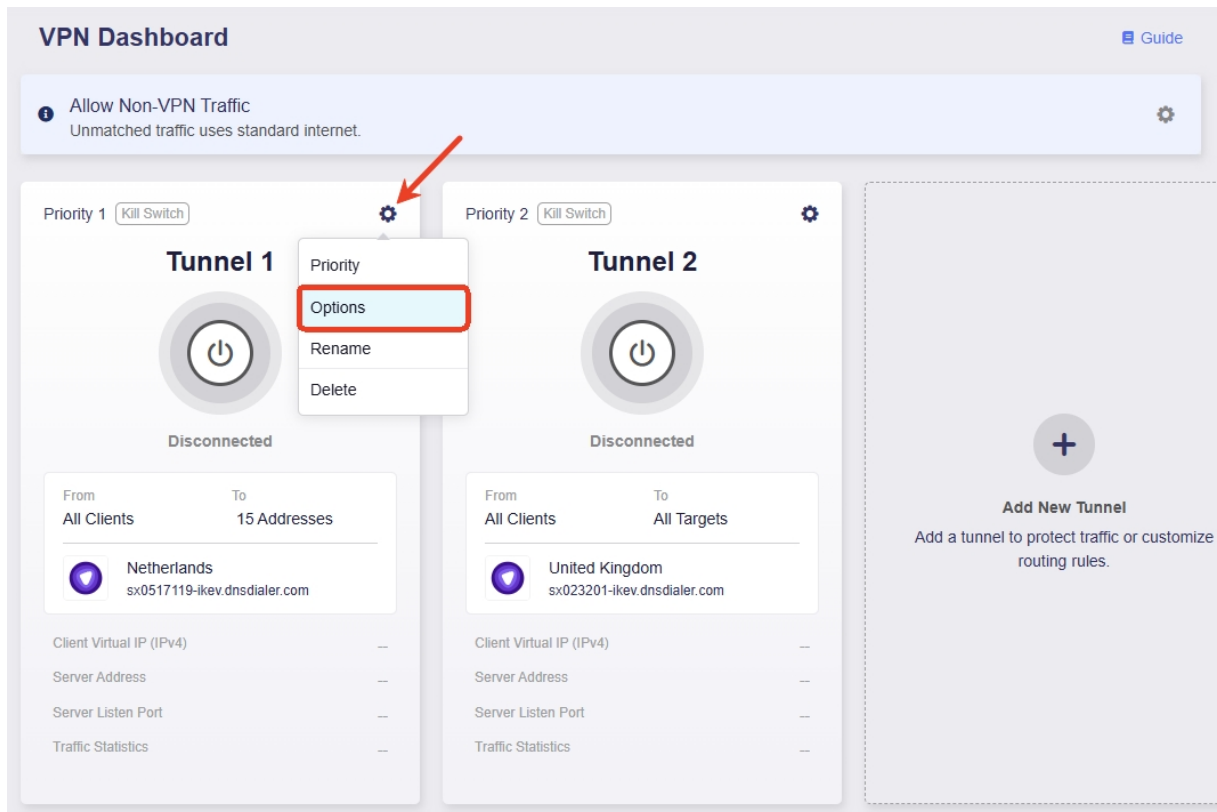
- **Enhanced Kill Switch:** Forces all devices to access the Internet through a VPN. Any traffic that does not match a VPN tunnel will be blocked. This global setting does not override the Kill Switch configured for individual VPN tunnels.



9.5 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 ⓘ

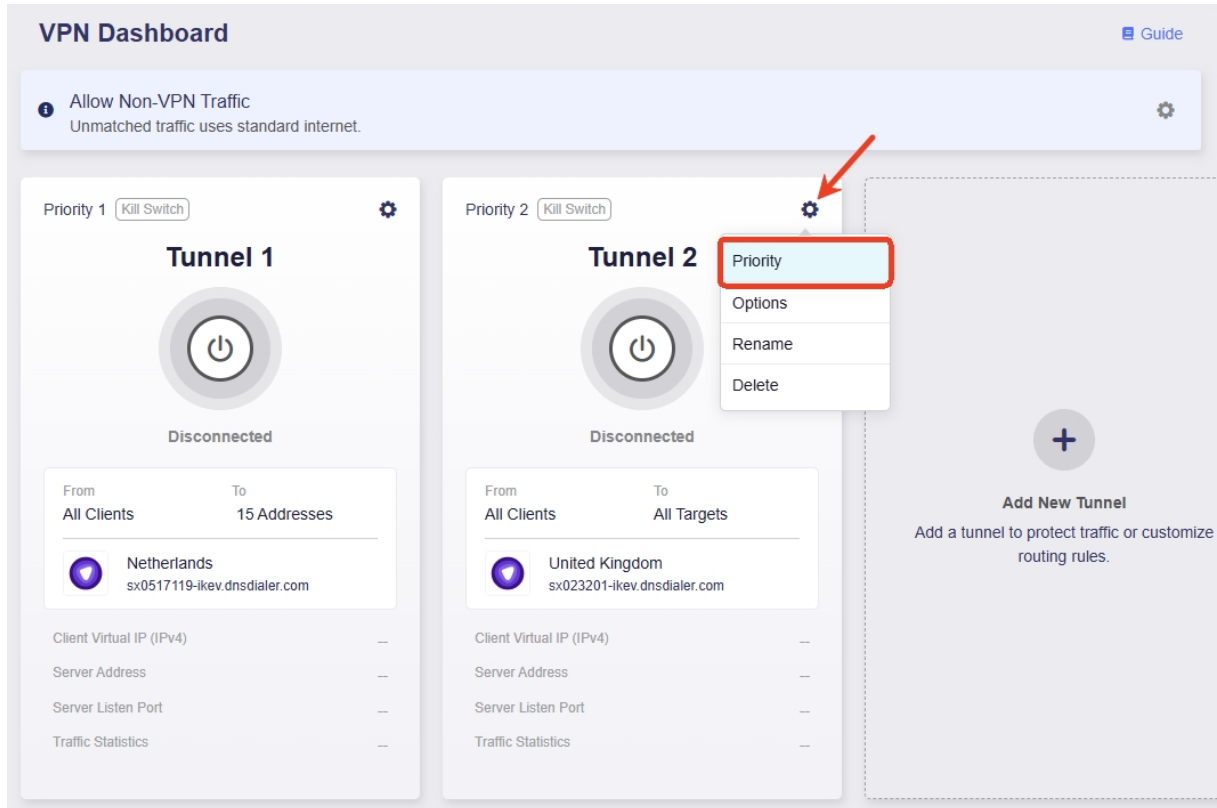
Cancel

Apply

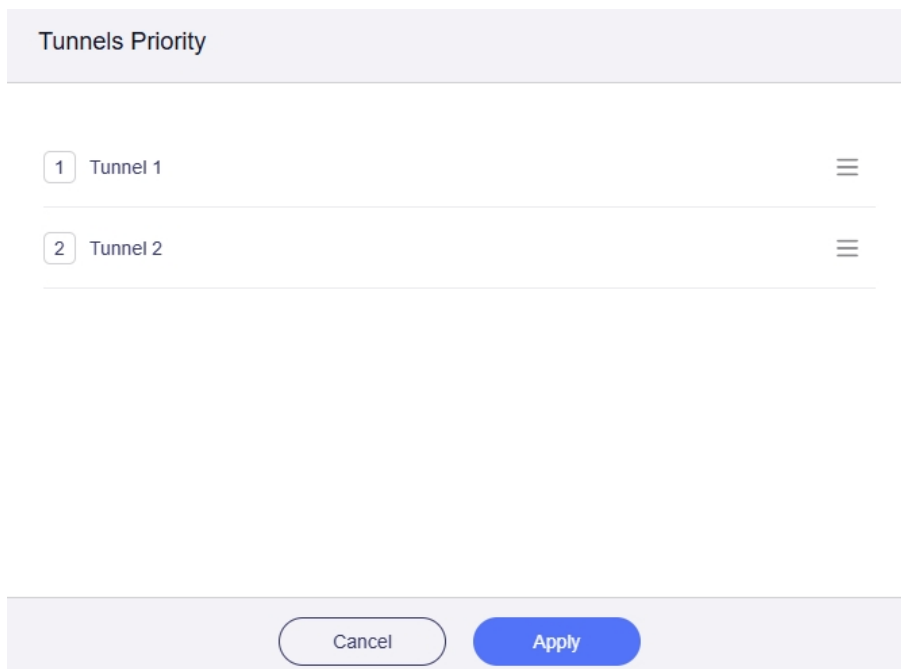
- **Kill Switch:** If enabled, traffic matching this VPN tunnel will be blocked if the VPN connection fails unexpectedly. If disabled, such traffic will fail over to the All Other Traffic tunnel.
- **Services from GL.iNet Use VPN:** If enabled, GoodCloud, DDNS, and rtty services will transmit packets 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.

9.6 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 10

Set Up VPN Server

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

10.1 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.

10.1.1 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.

10.1.2 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.

The screenshot shows the 'Configuration' tab of the OpenVPN Server settings. It includes the following fields and options:

- Device Mode:** TUN (dropdown)
- Protocol:** UDP (dropdown)
- Local Port:** 1194 (text input)
- IPv4 Subnet:** 10.8.0.0/24 (text input)
- IPv6 Subnet:** fd00:a79f:8609:088f::0/64 (text input)
- Authentication Mode:** Certificate only (dropdown)

At the bottom of the configuration area, there is a link for **Advanced Configuration**. Below the configuration fields are two buttons: **Reset** and **Apply**. A red rectangular box highlights the **Export Client Configuration** button, which is located below the 'Apply' button.

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

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

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

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

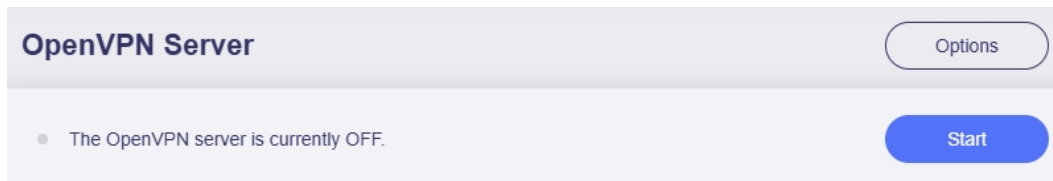
Tips:

- 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

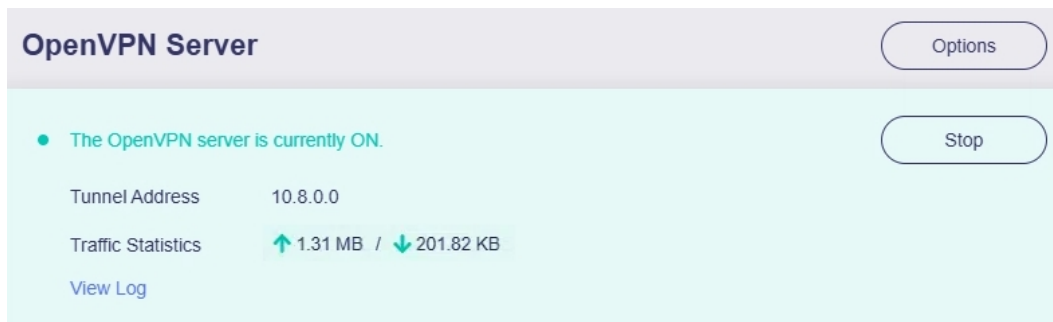
address. Once selected, the server address in the configuration file will be updated automatically. Re-download the configuration file if the server address is changed.

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.



10.1.3 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.

10.2 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.

10.2.1 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.

10.2.2 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.

The screenshot shows the 'WireGuard Server' interface. At the top, there's a status bar indicating 'The WireGuard server is currently OFF.' with a 'Start' button. Below this is a tabbed interface with 'Configuration', 'Profiles', and 'Route Rules'. The 'Profiles' tab is selected and highlighted with a red box. A message box below the tabs states: '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.' To the right of this message is a blue '+ Add' button, also highlighted with a red box.

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

The screenshot shows the 'Client Configuration' form. It has a 'Name' label followed by a text input field. Below the input field is a 'Set More' link. At the bottom of the form are two buttons: 'Cancel' and '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.

i 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 **i**

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 **i**

35.76.125.9

QR Code

Configuration File

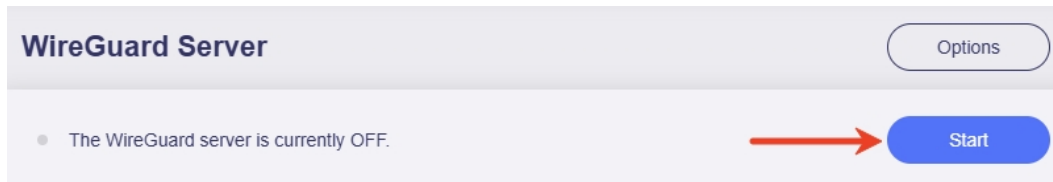
35.76.125.9

.glddns.com

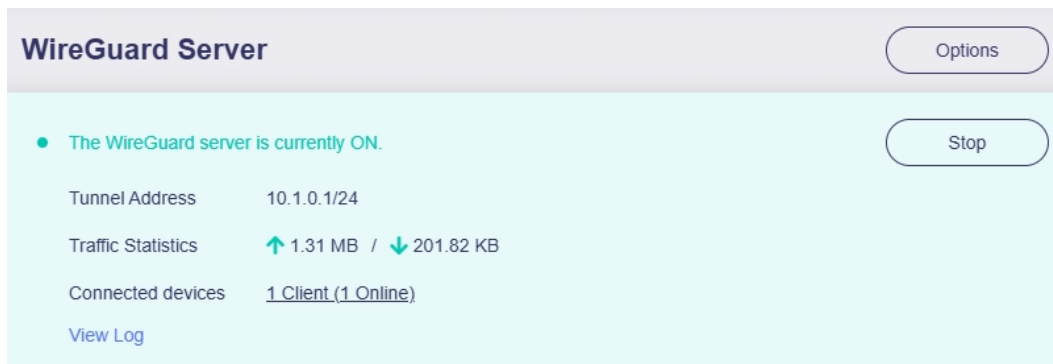
192.168.6.189

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.



10.2.3 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 11

Set Up VPN Client

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

11.1 Set Up OpenVPN Client

11.1.1 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.

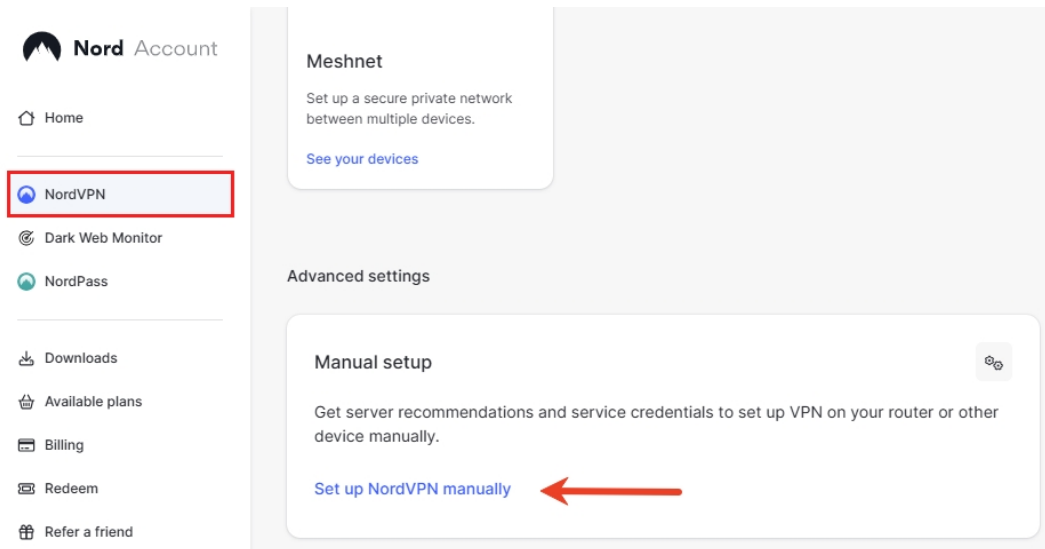
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to [this link](#) or contact their support.

11.1.2 Set Up NordVPN

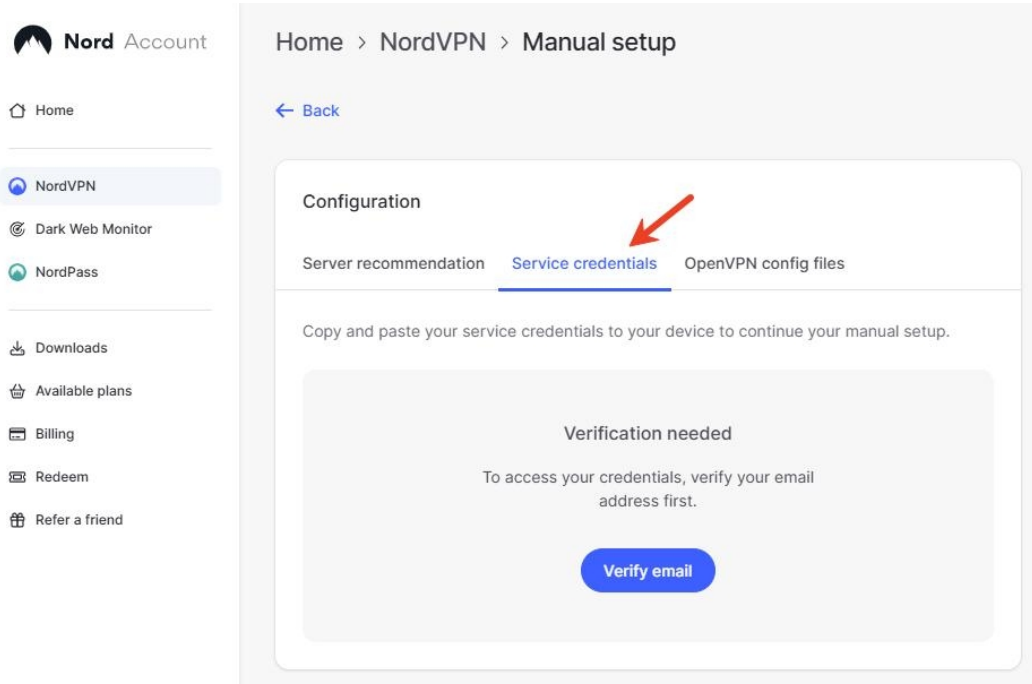
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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

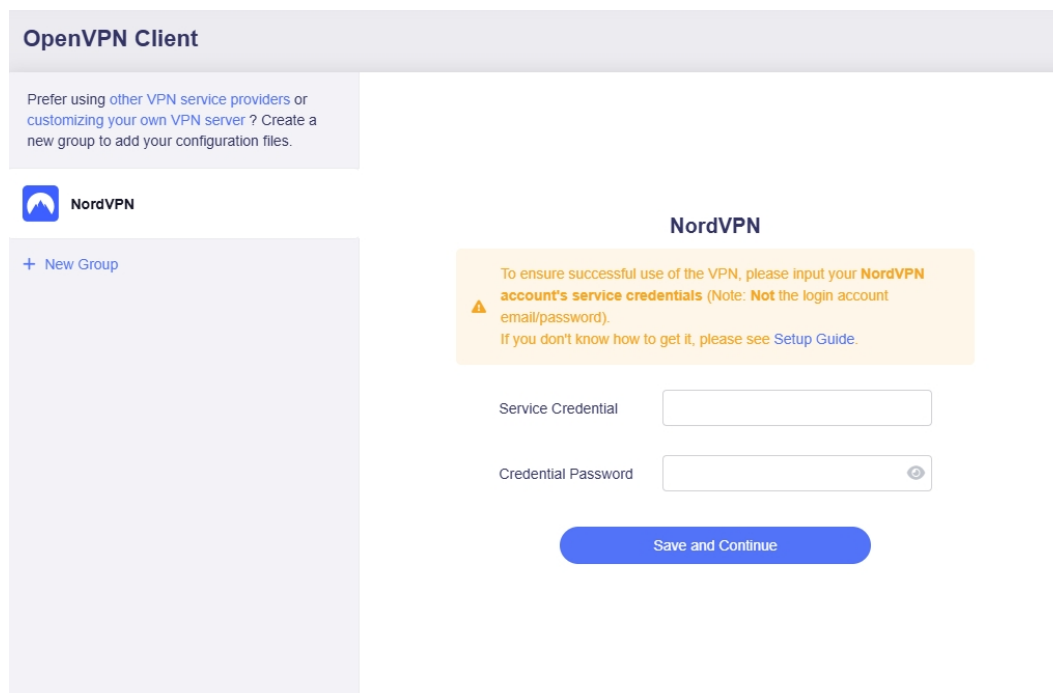
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



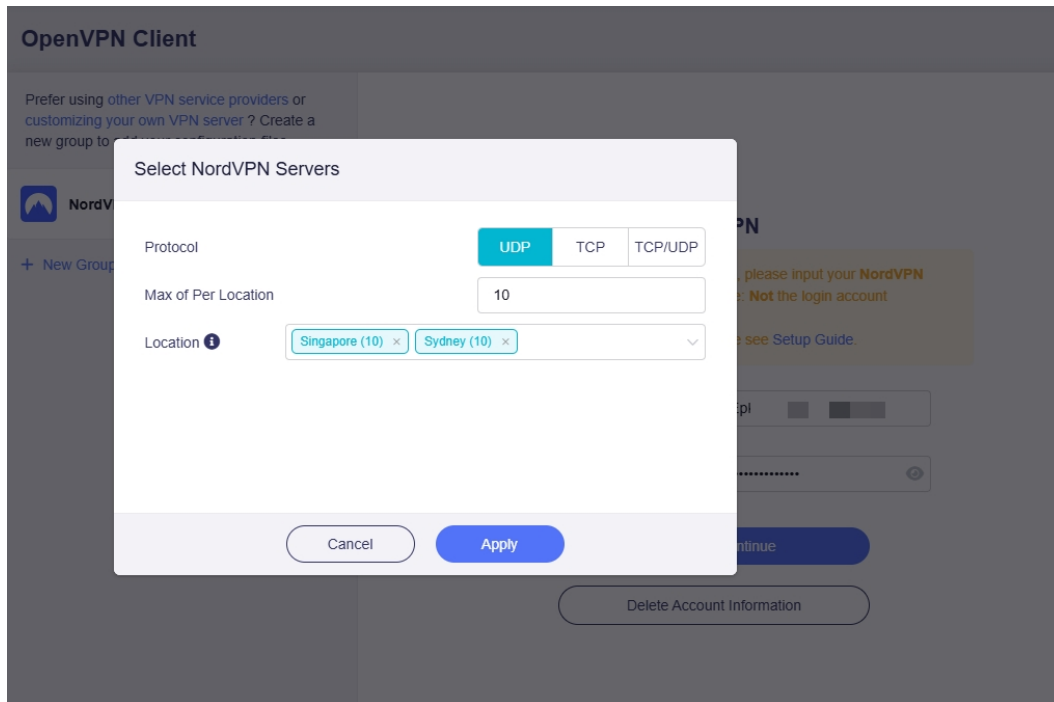
You will find the **service credentials**. Copy them for later use.



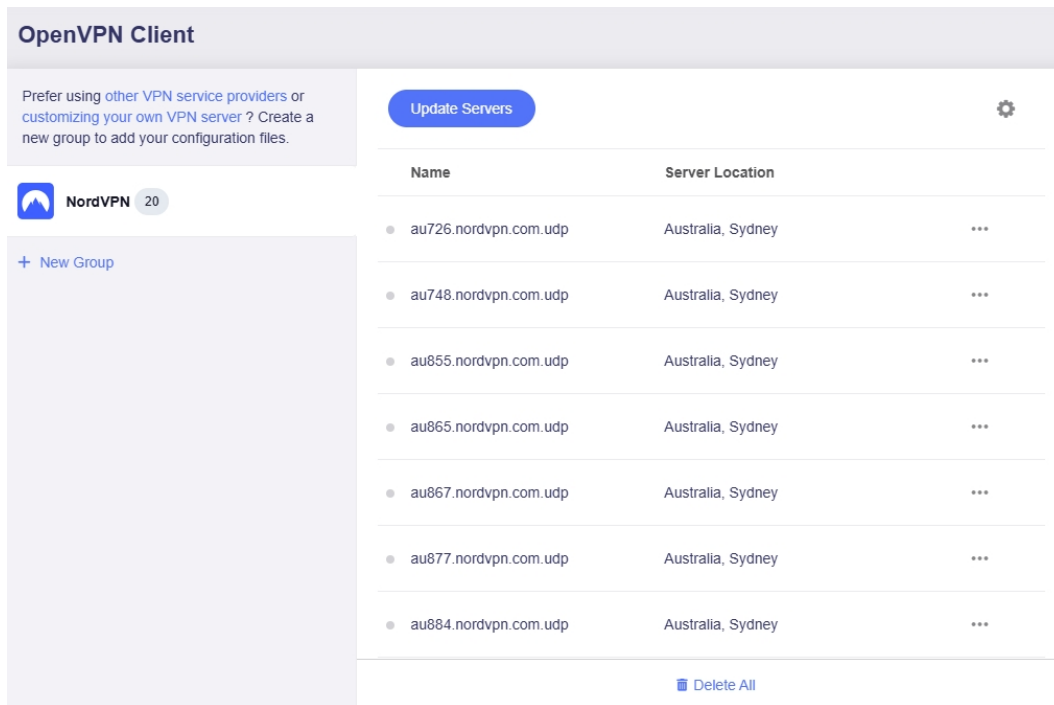
- Log in to your router's web admin panel and navigate to **VPN > OpenVPN Client > NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



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

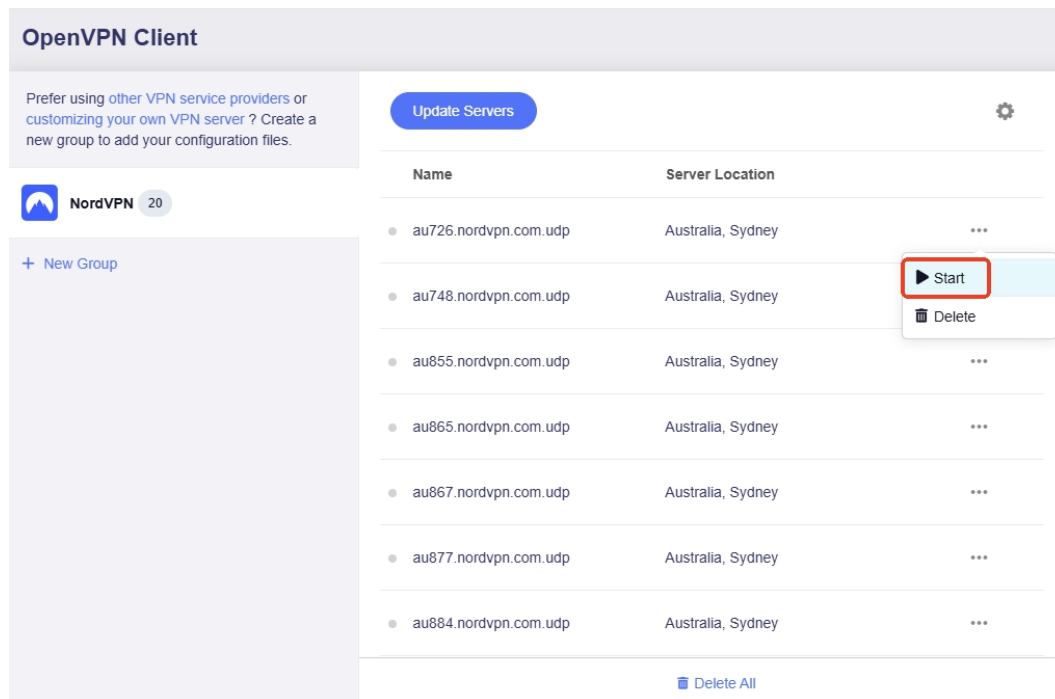


It will download configuration files.

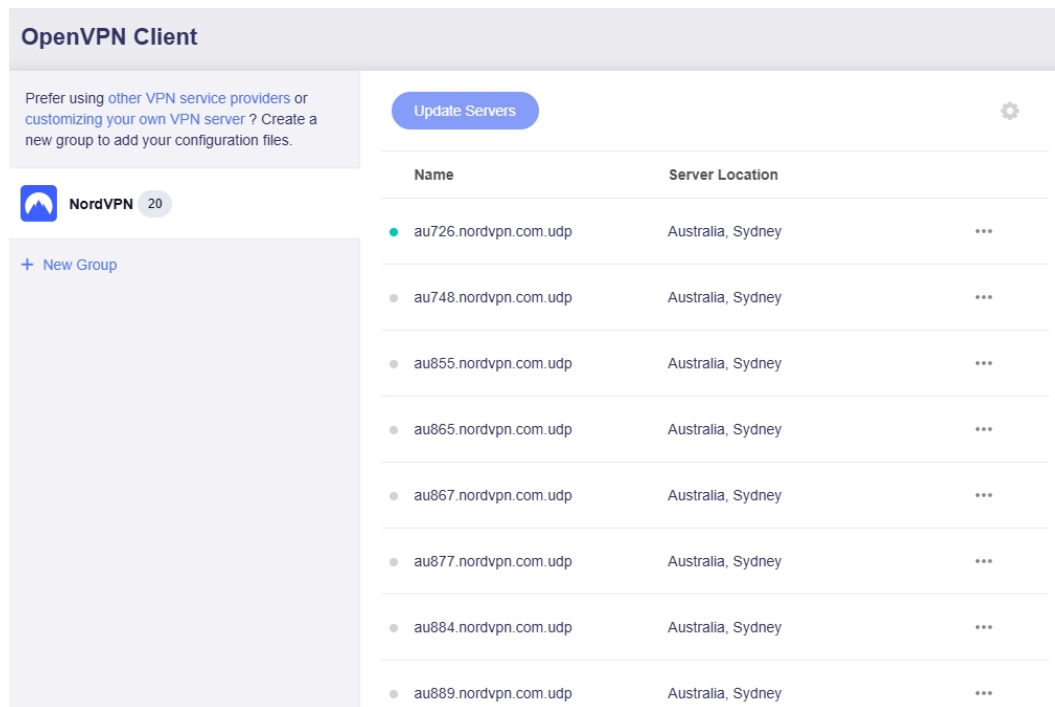


5. Start a connection.

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

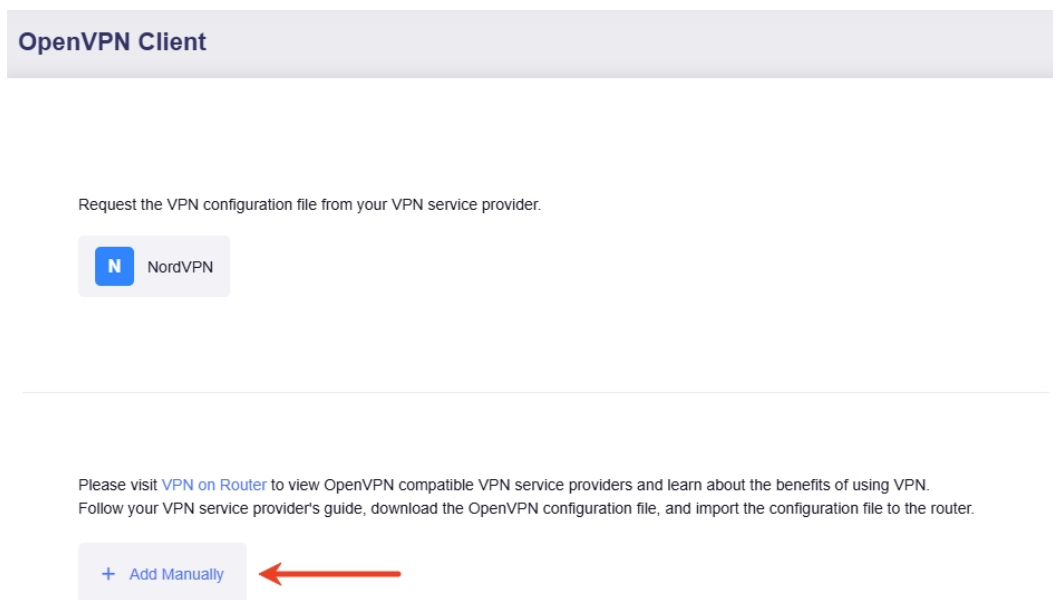
Delete

11.1.3 Set Up OpenVPN Client Manually (for other providers)

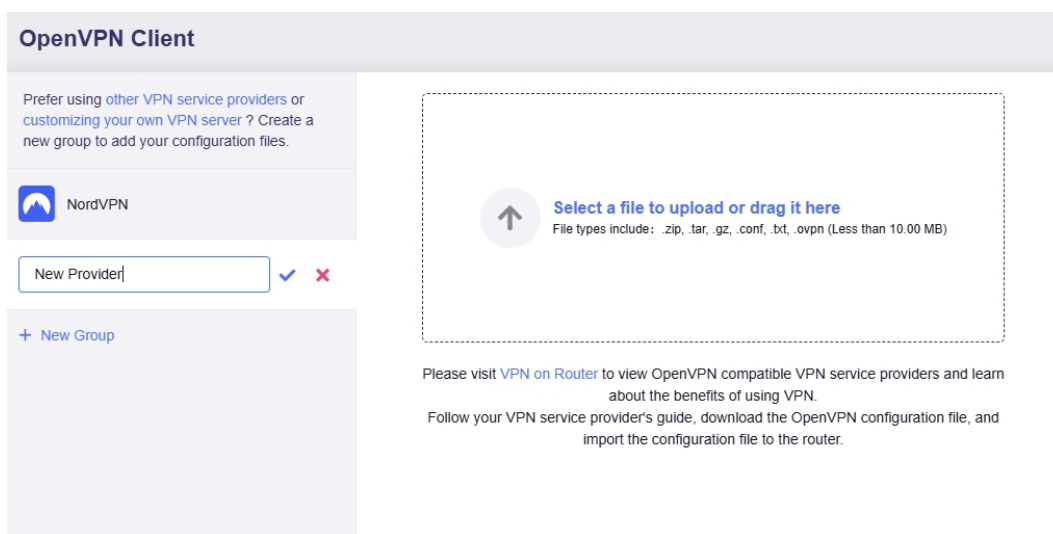
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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**.

11.2 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.

11.2.1 Preparation

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

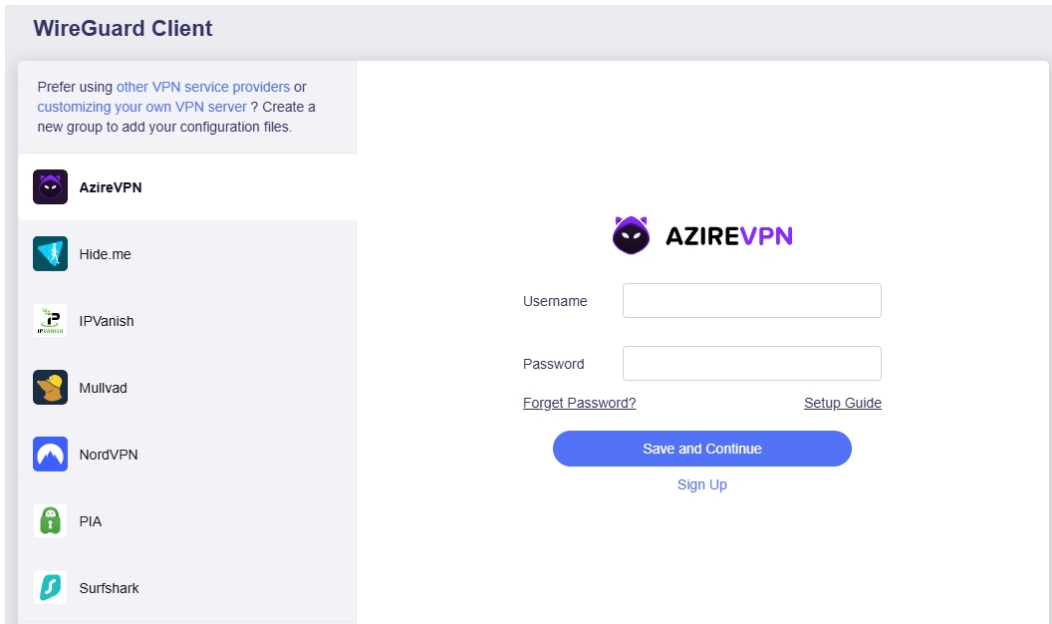
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

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

11.2.2 Set Up AzireVPN

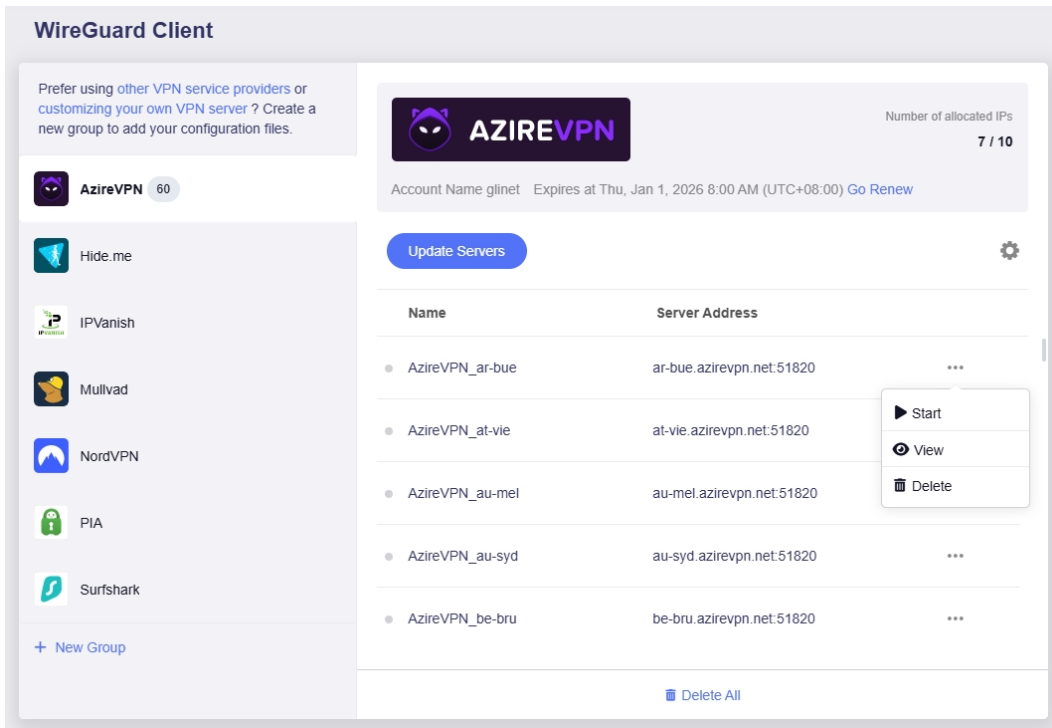
Follow the steps below to set your router as an AzireVPN client.

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, there's a sidebar with a list of VPN providers: AzireVPN (selected), Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The main area displays the 'AZIREVPN' login form. It includes a note about using other VPN services, a 'Username' field, a 'Password' field, and links for 'Forgot Password?' and 'Setup Guide'. A blue 'Save and Continue' button is prominent, with a 'Sign Up' link below it.

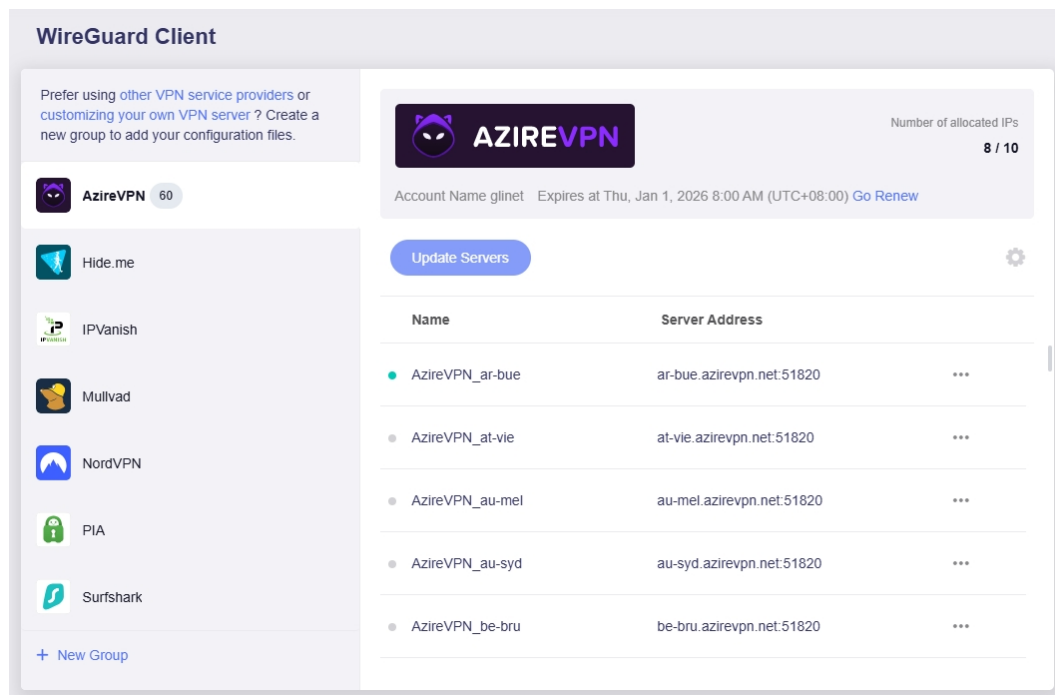
3. Select a preferred server, and click the three-dot icon on the right to start a connection.



The screenshot shows the 'WireGuard Client' interface after login. The sidebar remains the same. The main area now displays the 'AZIREVPN' account details: 'Account Name glinet', 'Expires at Thu, Jan 1, 2026 8:00 AM (UTC+08:00)', and 'Go Renew'. Below this is an 'Update Servers' button and a table of available servers. A context menu is open over the first server, showing 'Start', 'View', and 'Delete' options.

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	...

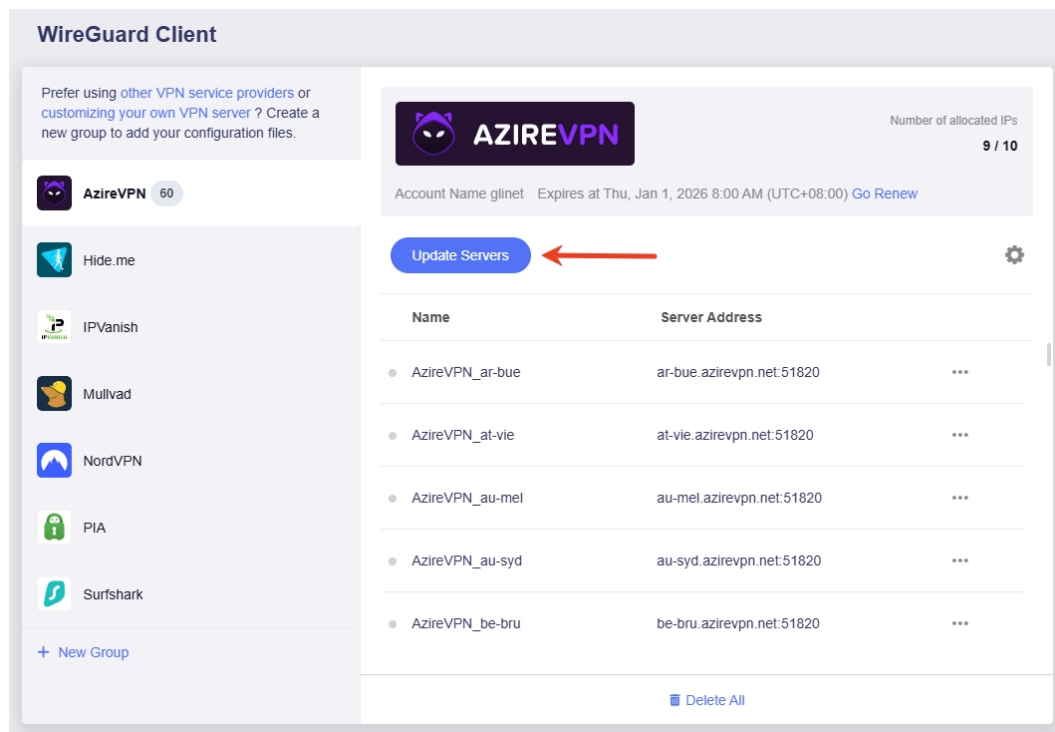
- Once connected, a green dot will appear next to the configuration file.



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

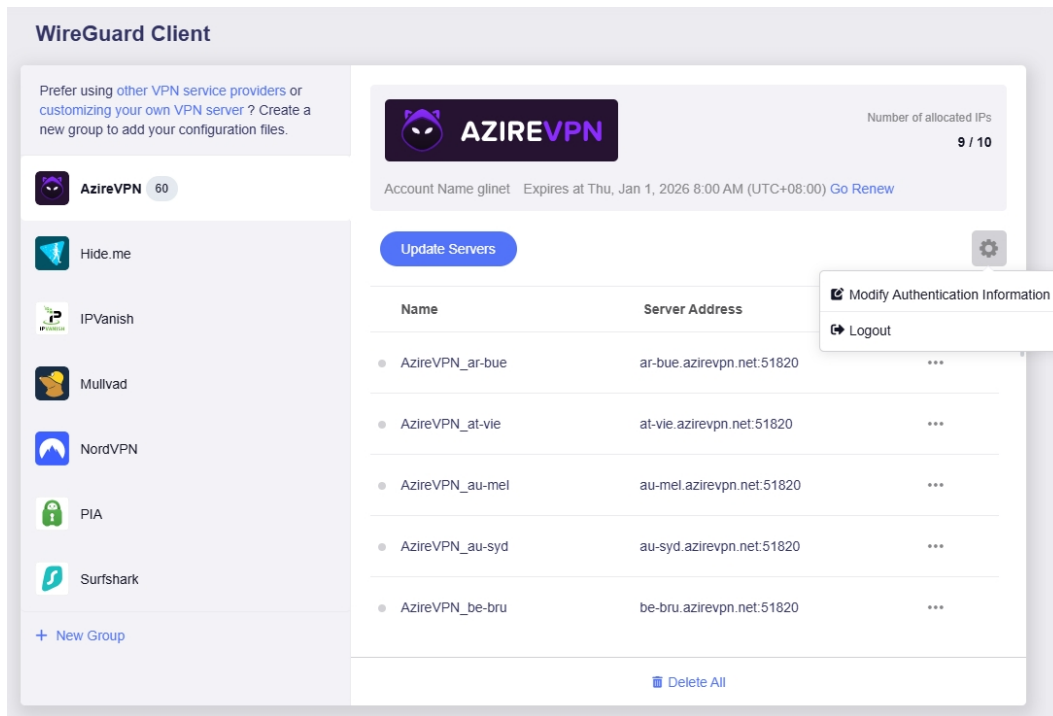
- Update servers.

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



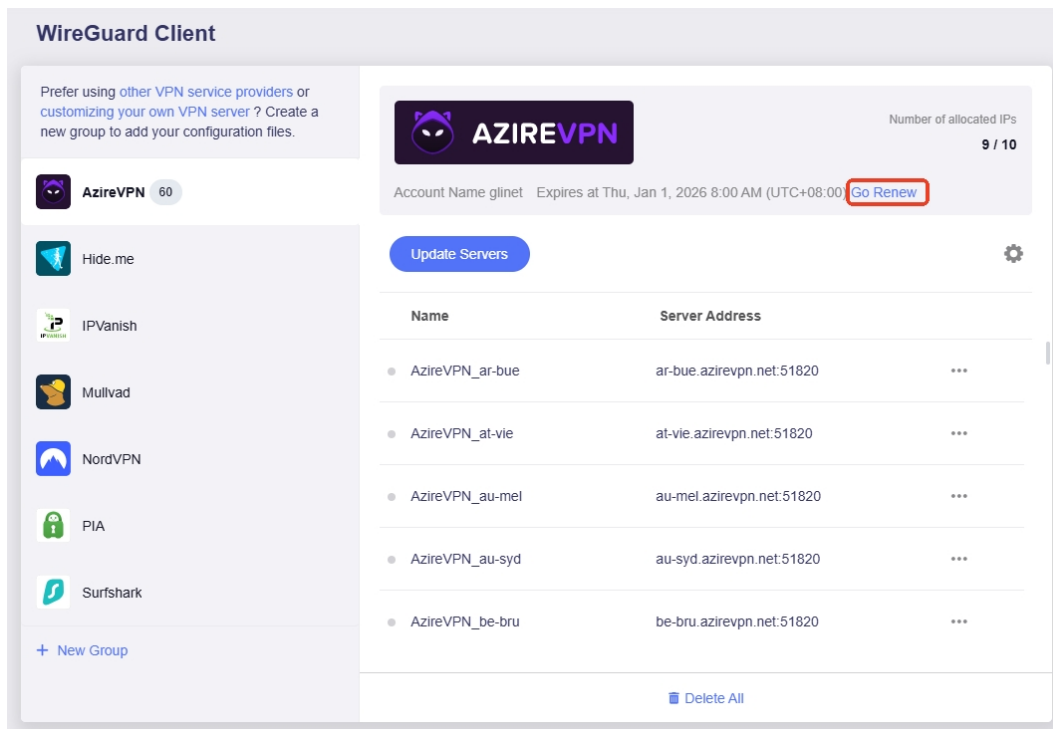
6. Edit credentials or logout.

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



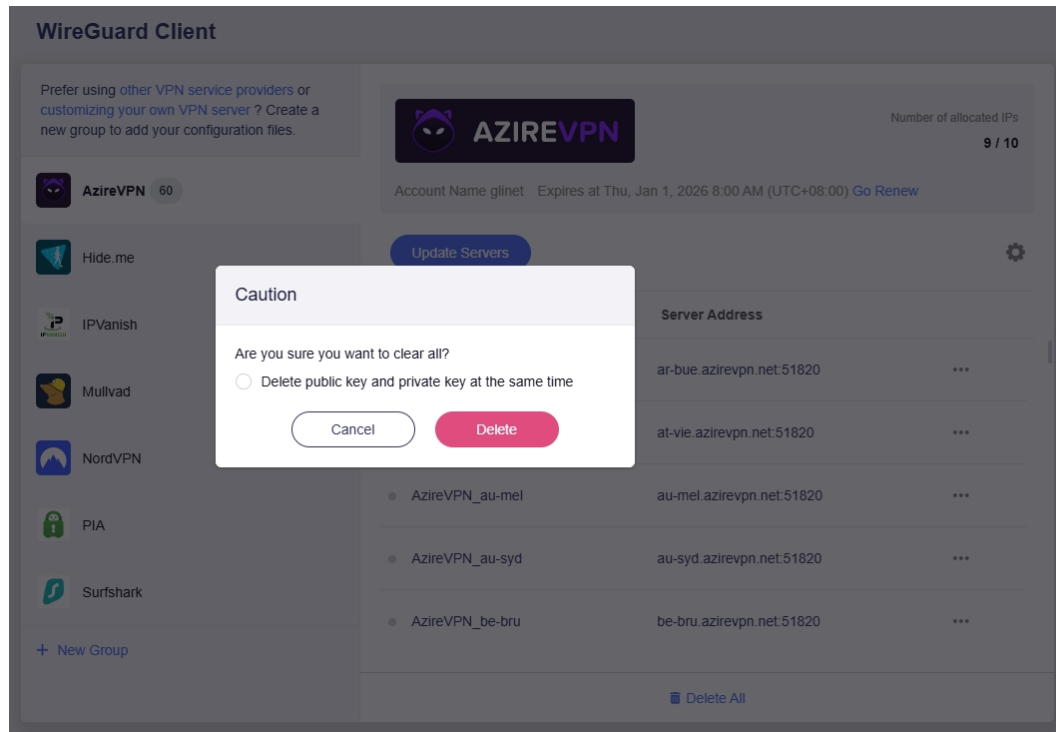
7. Go renew.

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



8. Delete all files.

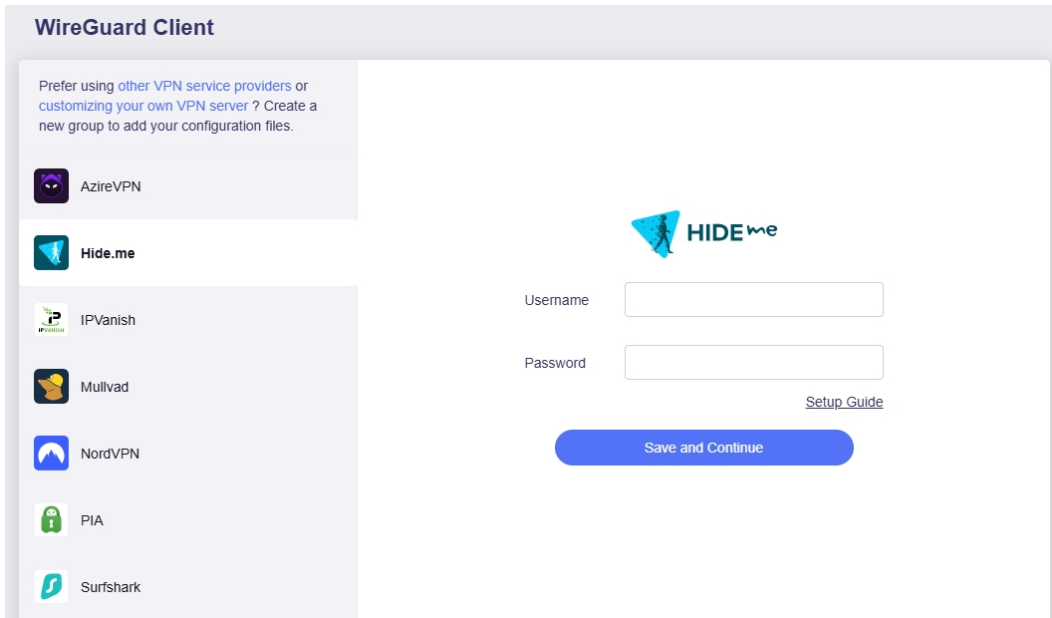
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.3 Set Up Hide.me

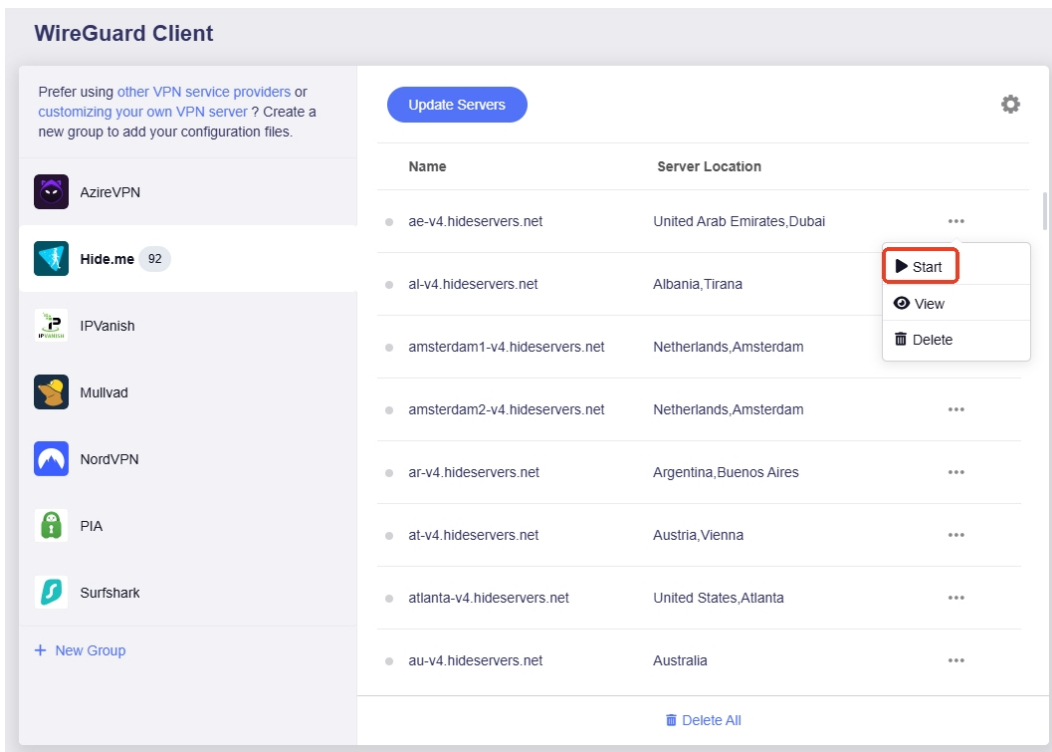
Follow the steps below to set your router as a Hide.me client.

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 a own VPN server.

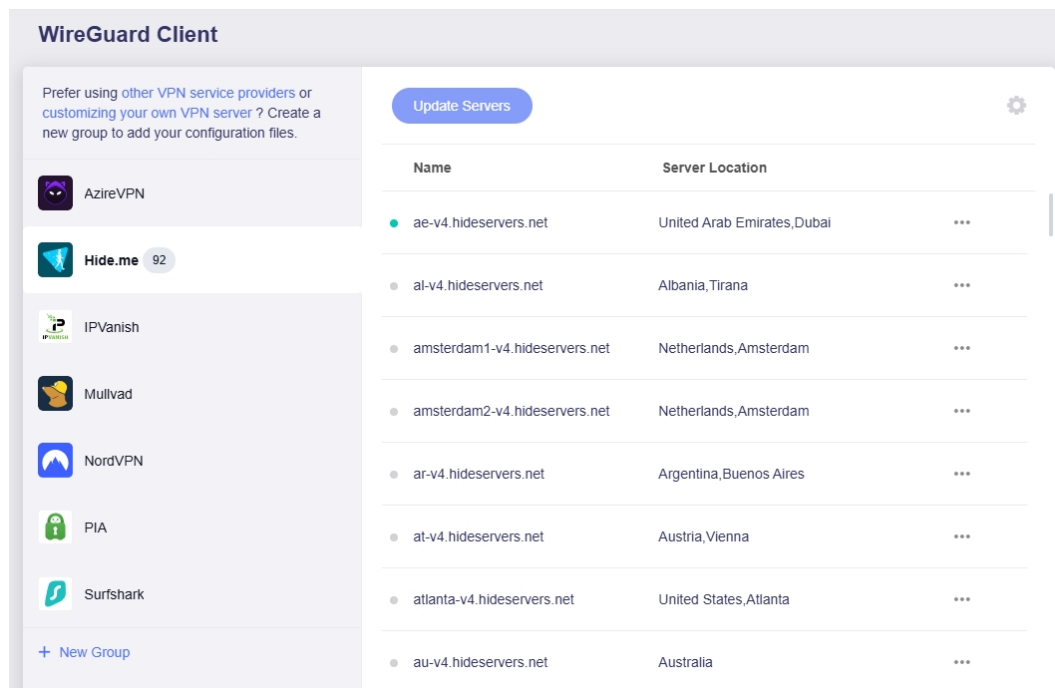
3. Select a preferred server, and click the three-dot icon on the right to start a connection.



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

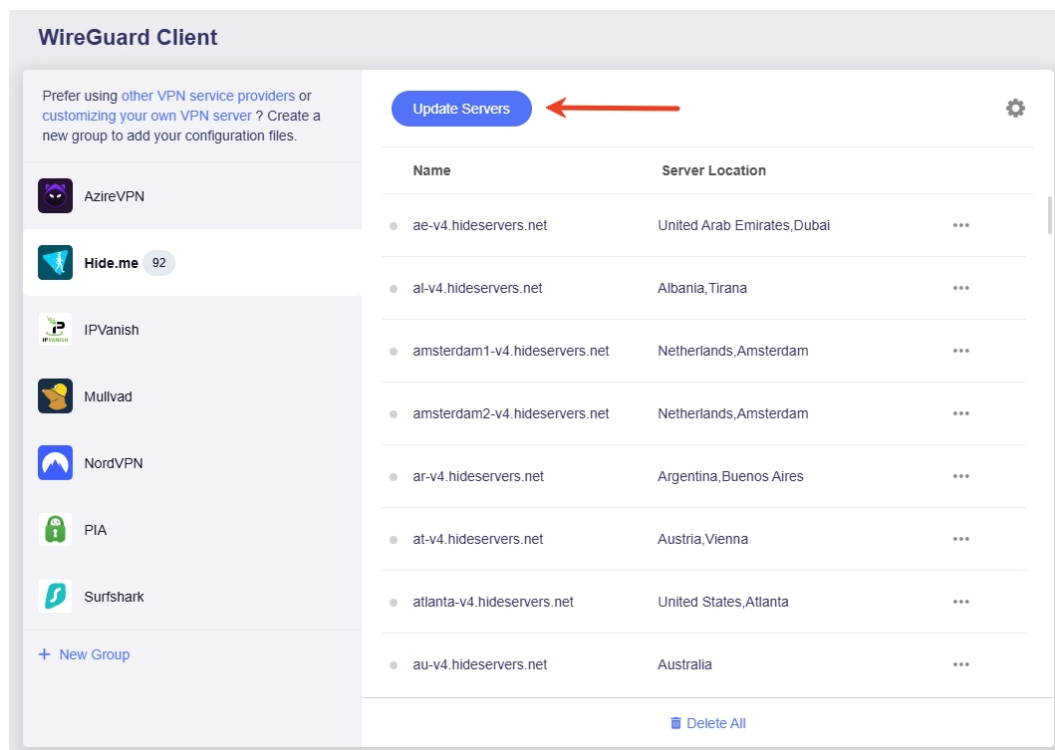
4. Once connected, a green dot will appear next to the configuration file.



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

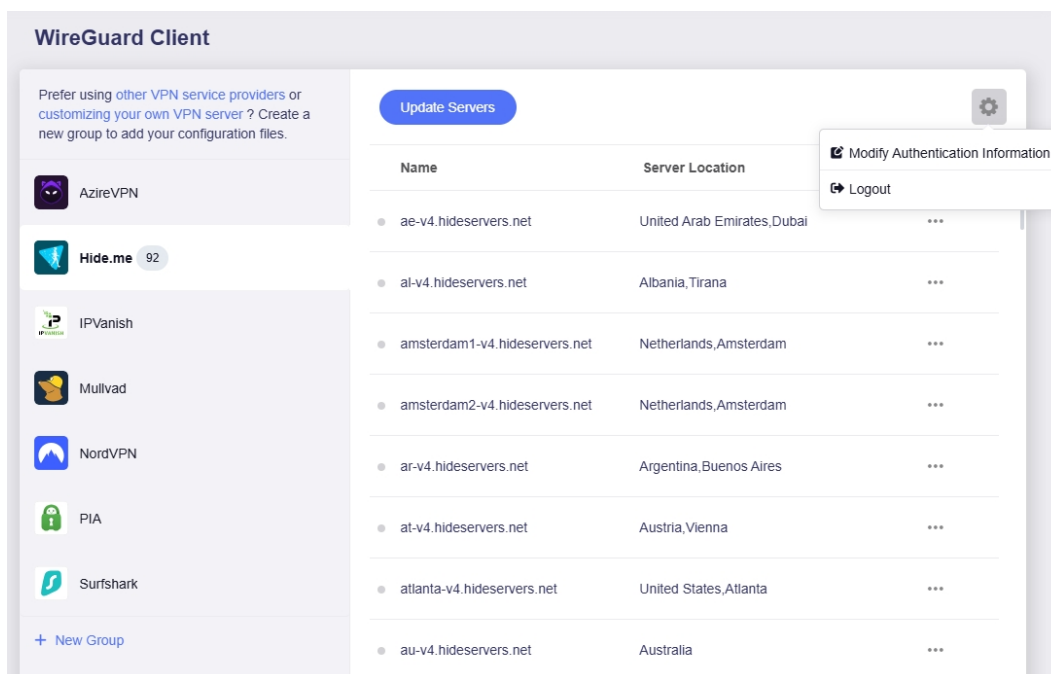
5. Update servers.

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



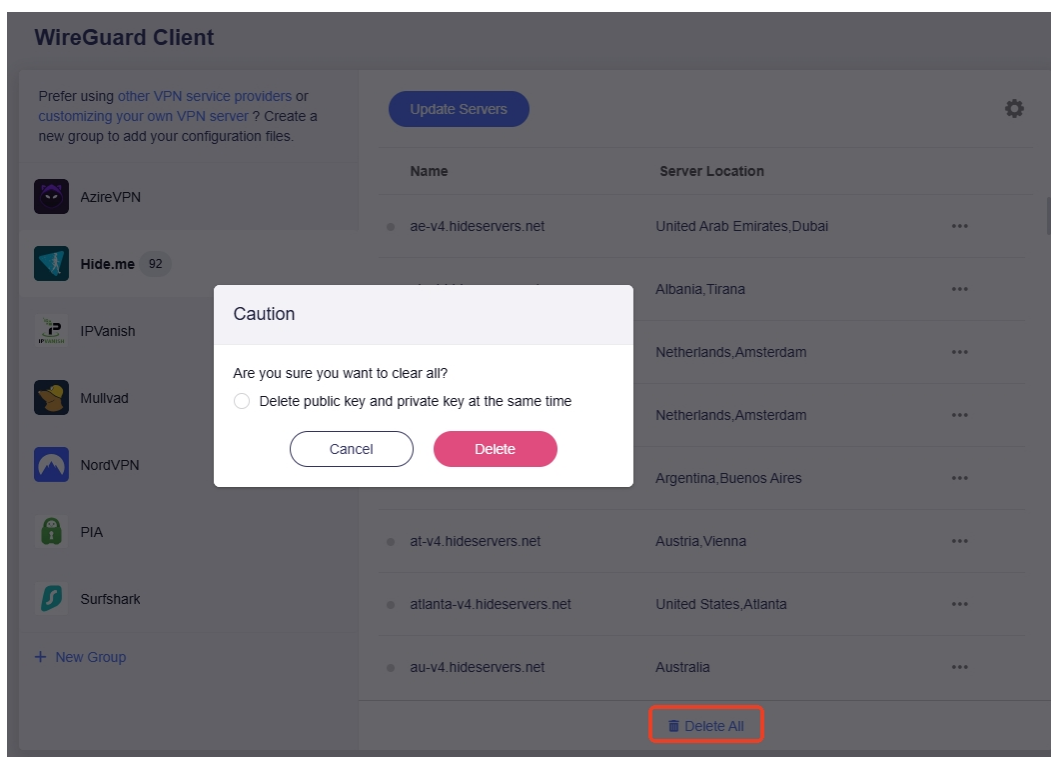
6. Edit credentials or logout.

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



7. Delete all files.

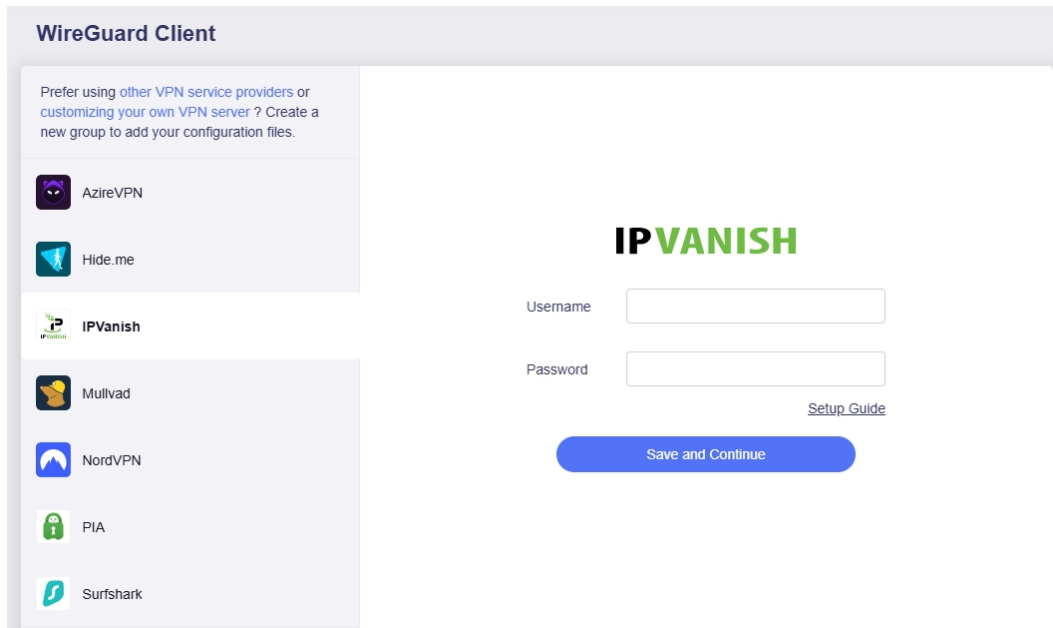
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.4 Set Up IPVanish

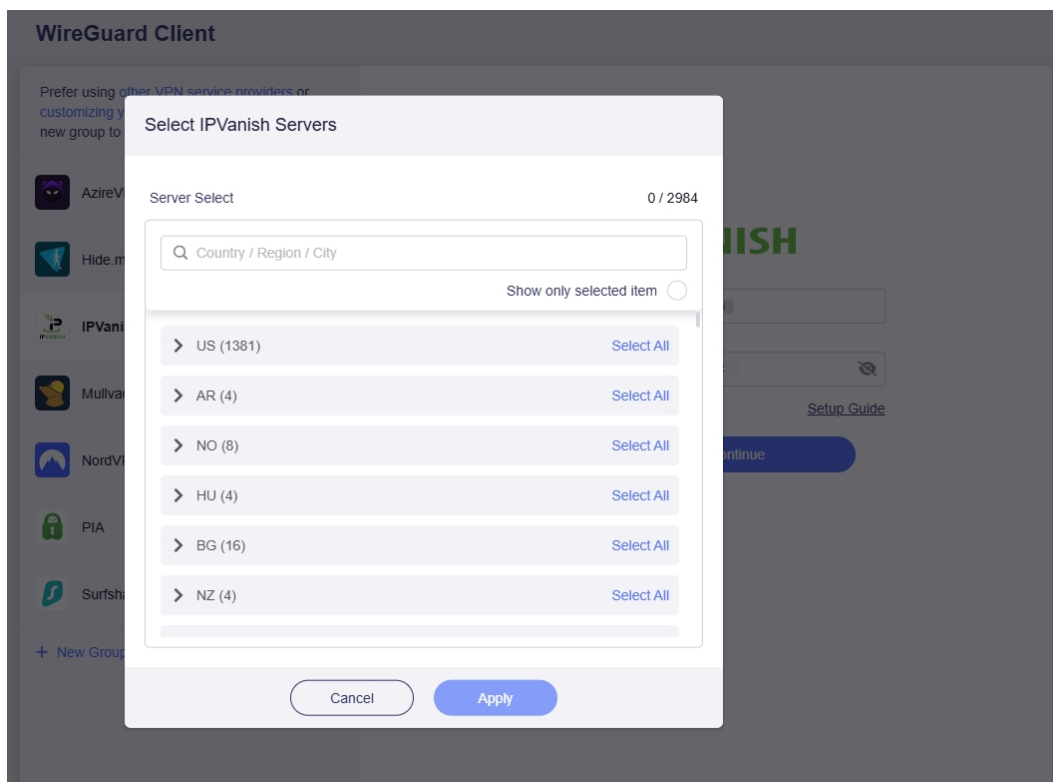
Follow the steps below to set your router as an IPVanish client.

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**.



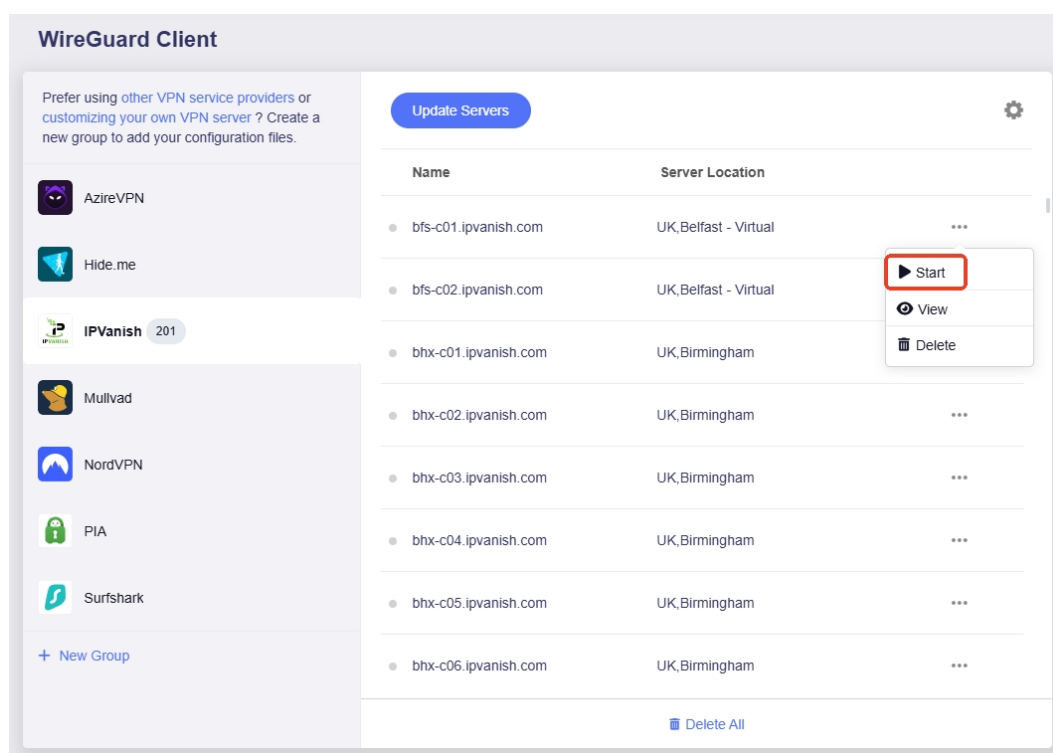
The screenshot shows the 'WireGuard Client' configuration page. On the left, there is a list of VPN providers: AzureVPN, Hide.me, IPVanish (highlighted), Mullvad, NordVPN, PIA, and Surfshark. On the right, the 'IPVANISH' logo is displayed above two input fields for 'Username' and 'Password'. Below these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

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

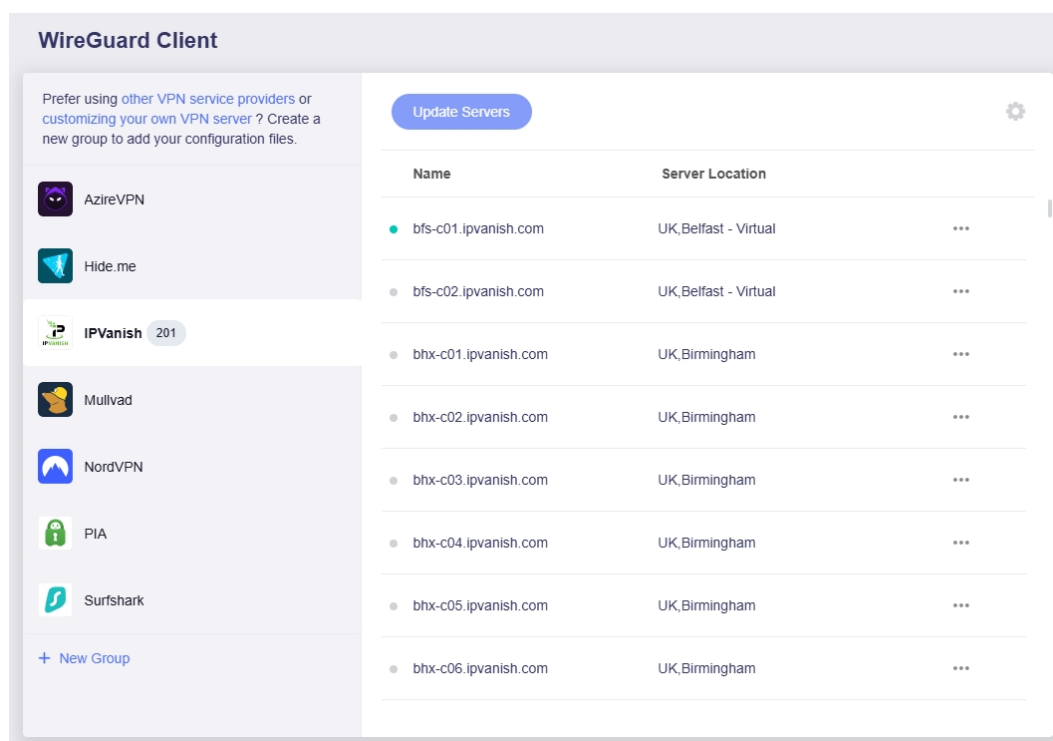


This screenshot shows the same 'WireGuard Client' setup page as before, but with a modal window open for selecting IPVanish servers. The modal is titled 'Select IPVanish Servers' and shows a list of server groups with their respective counts: US (1381), AR (4), NO (8), HU (4), BG (16), and NZ (4). Each group has a 'Select All' link to its right. At the bottom of the modal are 'Cancel' and 'Apply' buttons. The background setup page is dimmed.

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



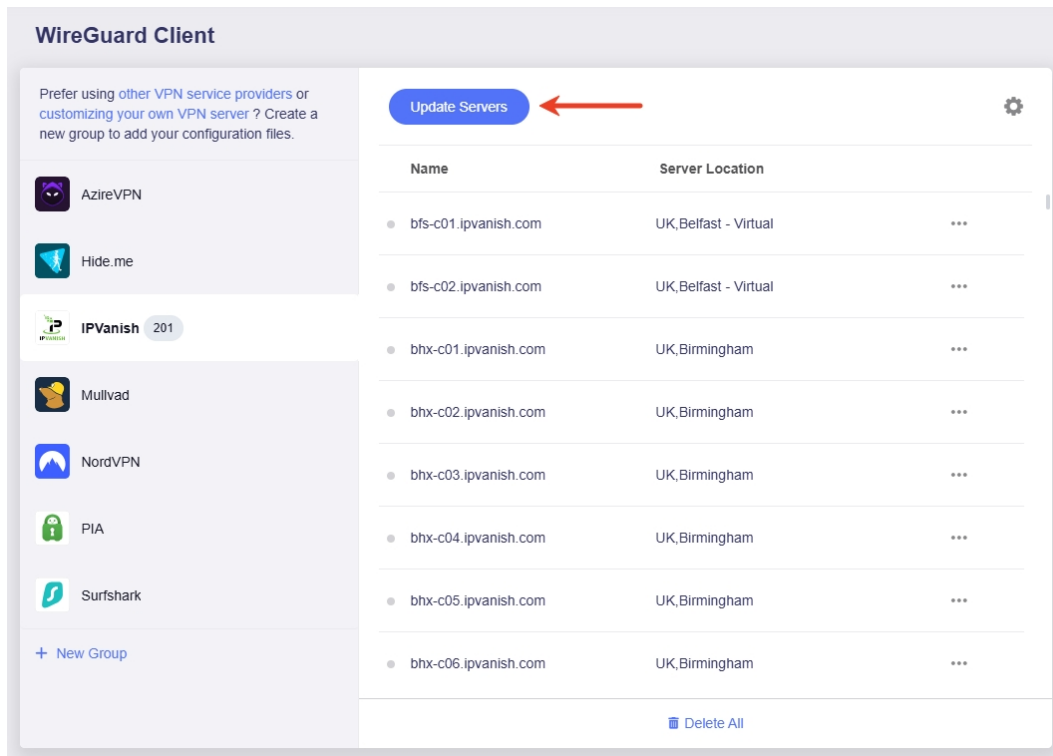
5. Once connected, a green dot will appear next to the configuration file.



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

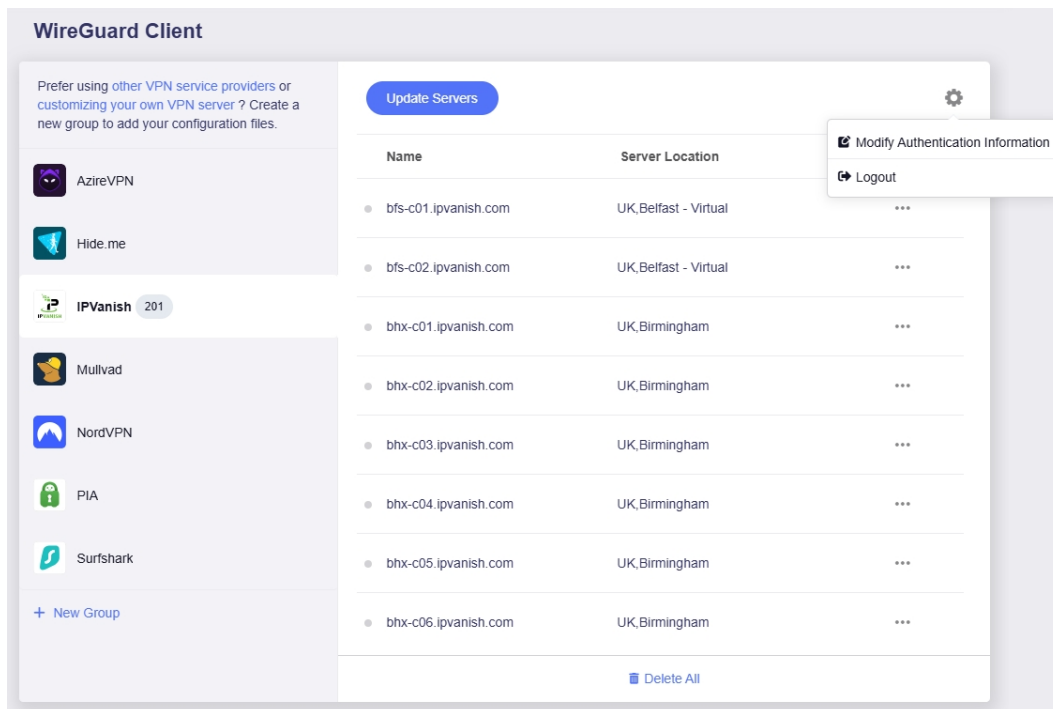
6. Update servers.

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



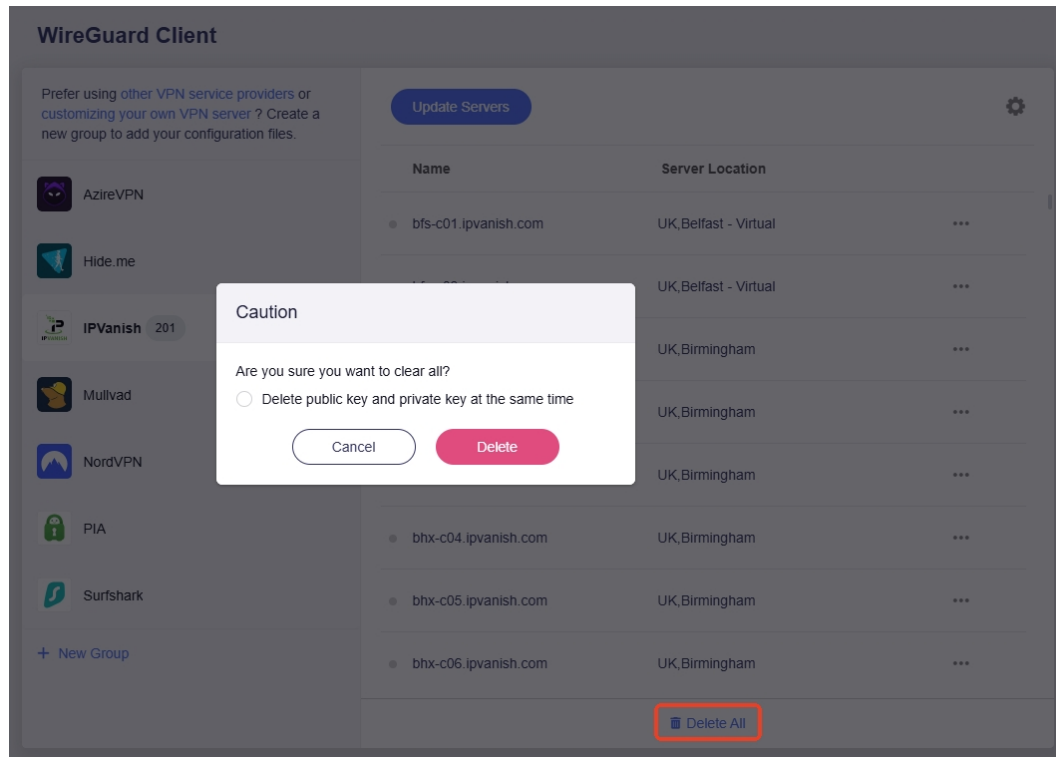
7. Edit credentials or logout.

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



8. Delete all files.

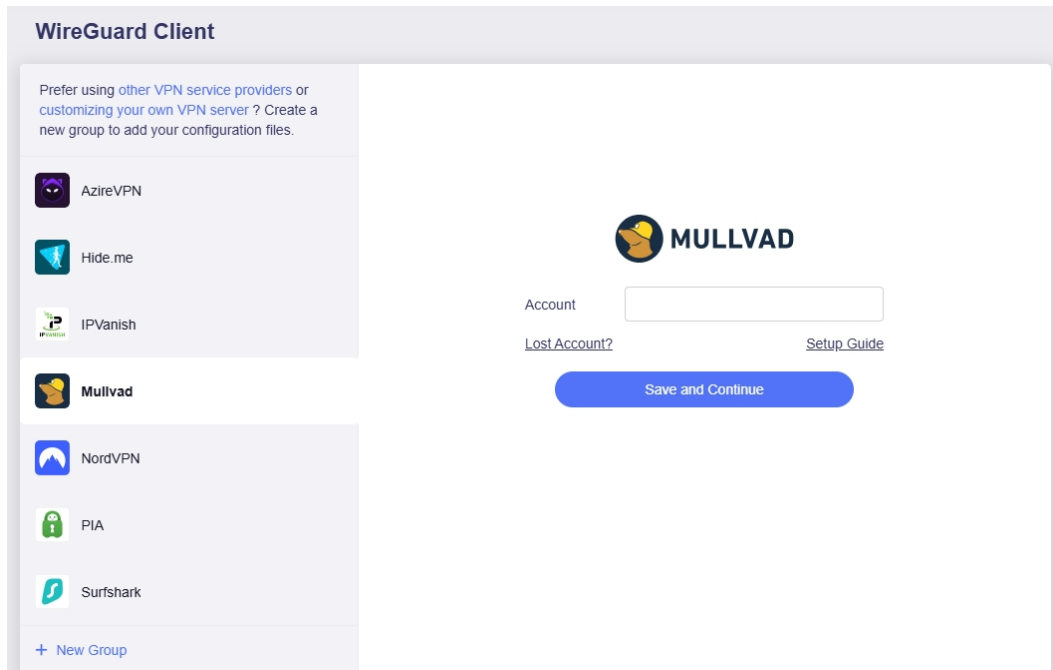
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



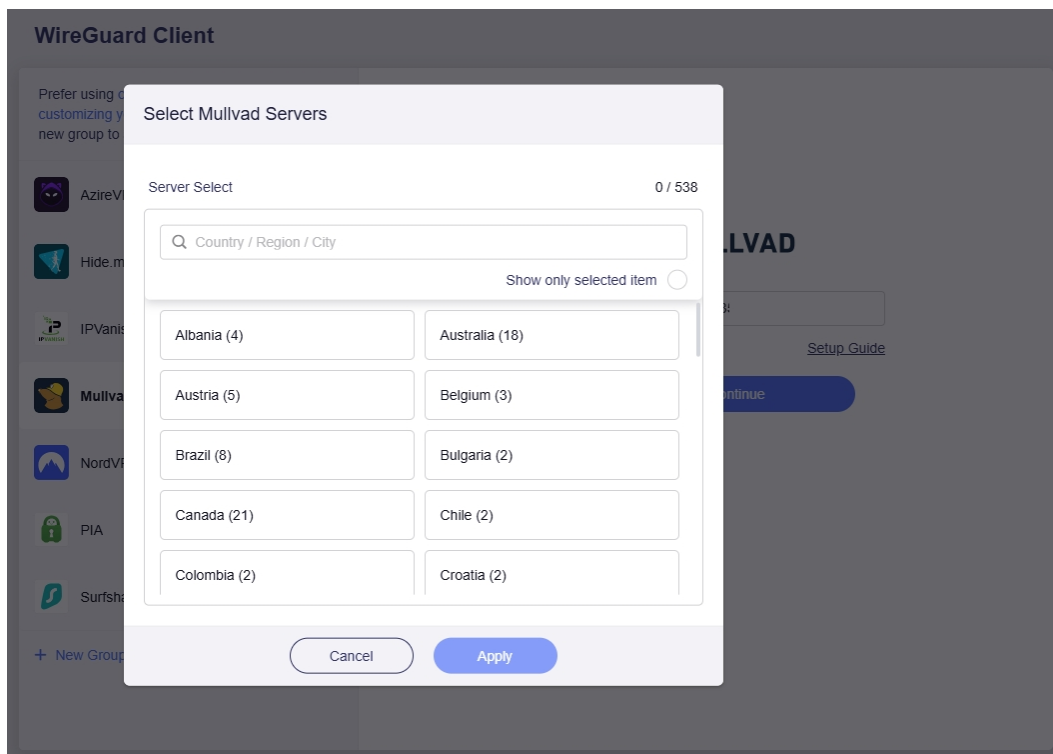
11.2.5 Set Up Mullvad

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

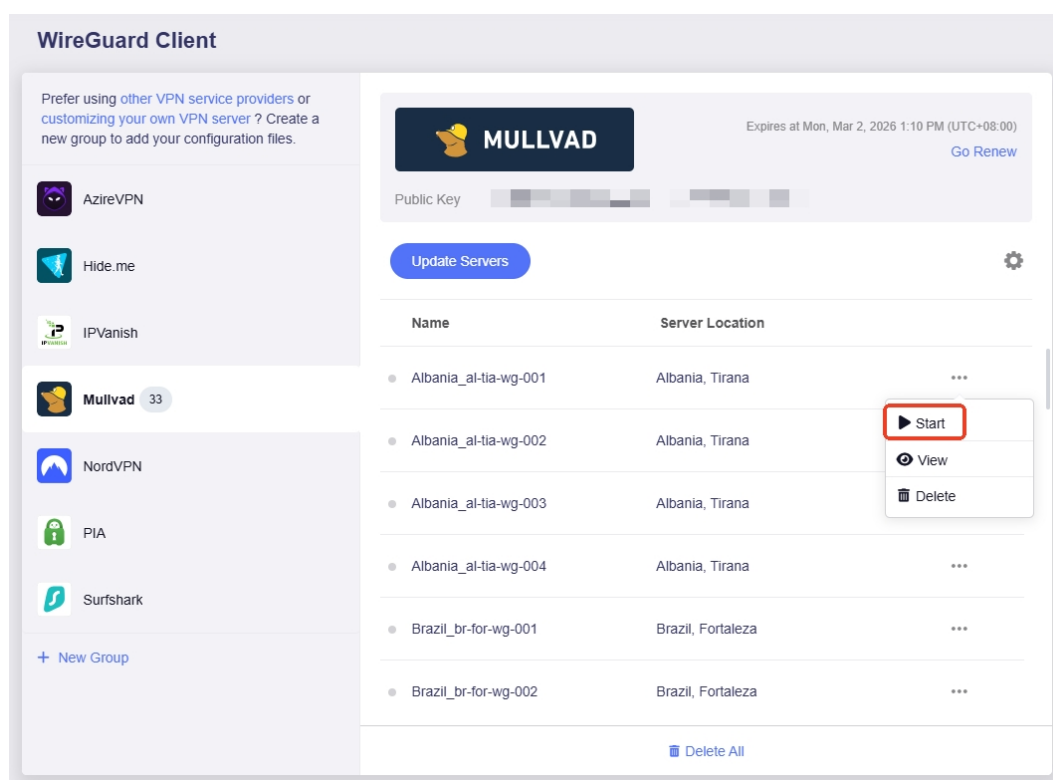
1. Log in to your router's web admin panel and go to **VPN > WireGuard Client > Mullvad**.
2. Input Username and Password, then click **Save and Continue**.



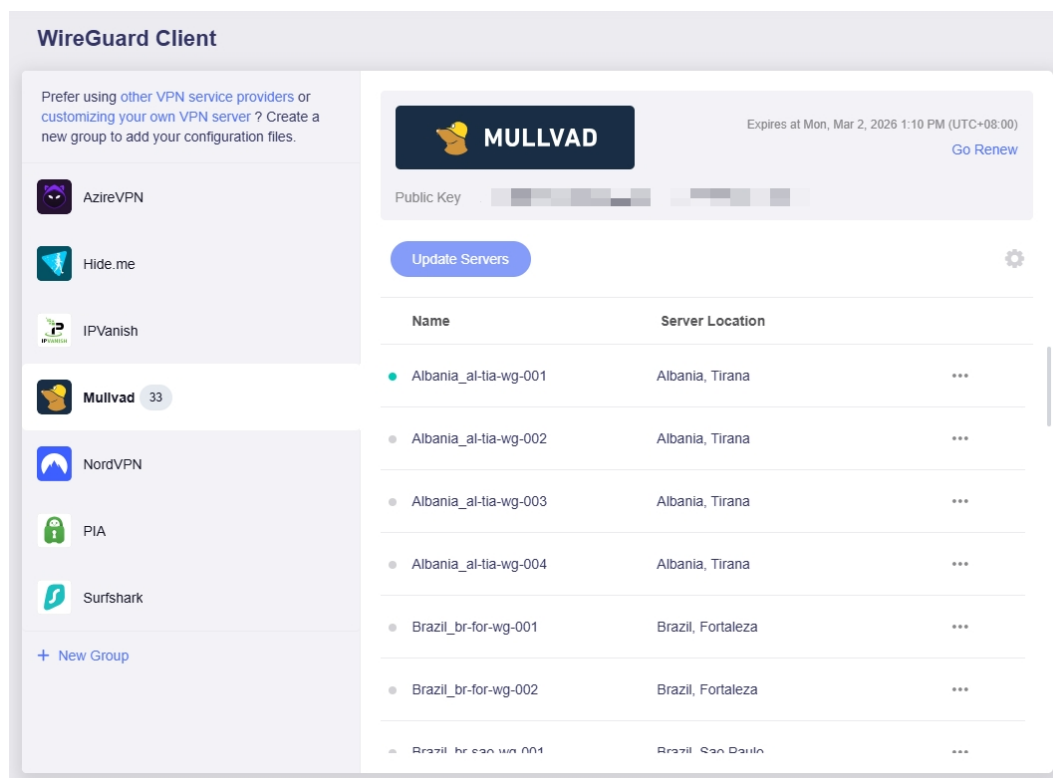
3. Select the server(s) you want to connect to, and click **Apply**.



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



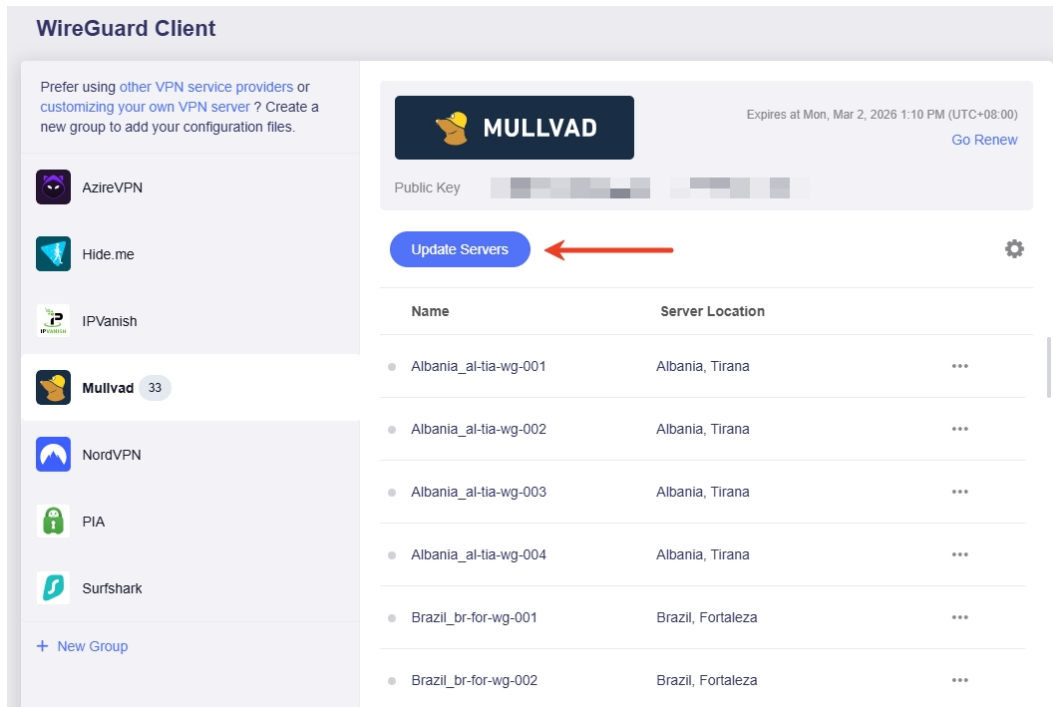
5. Once connected, a green dot will appear next to the configuration file.



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

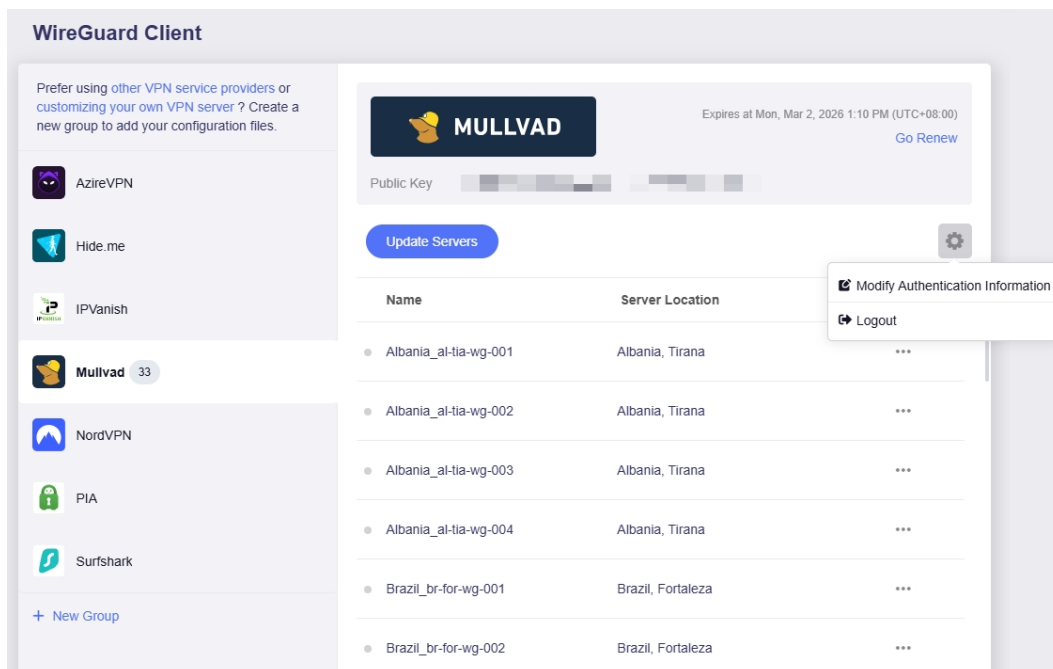
6. Update servers.

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



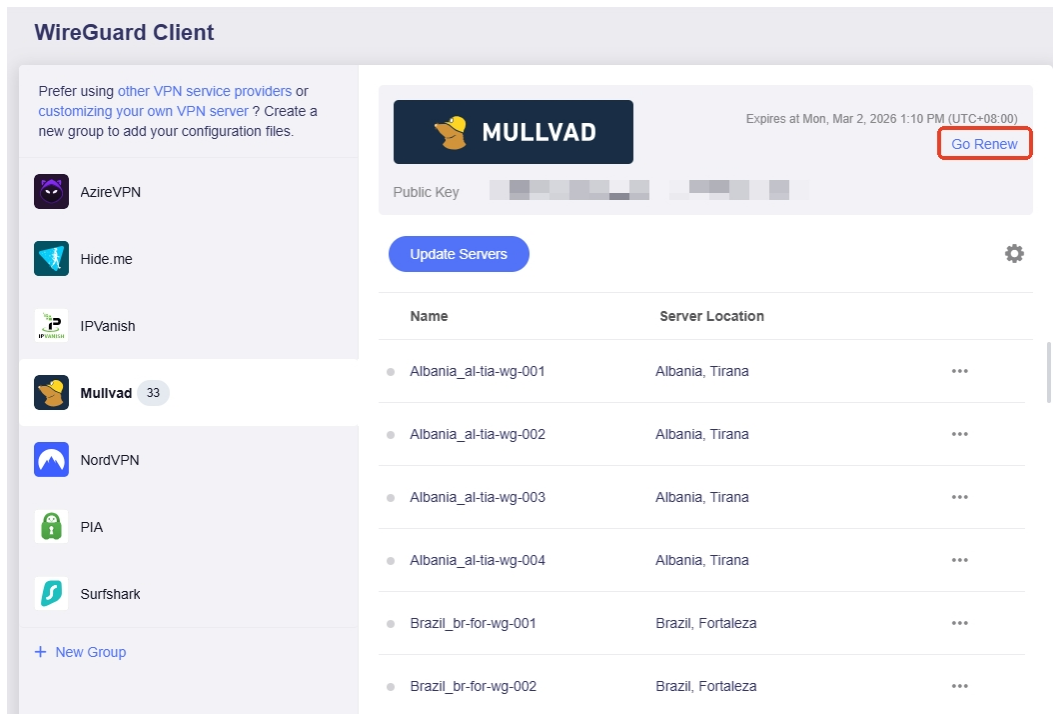
7. Edit credentials or logout.

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



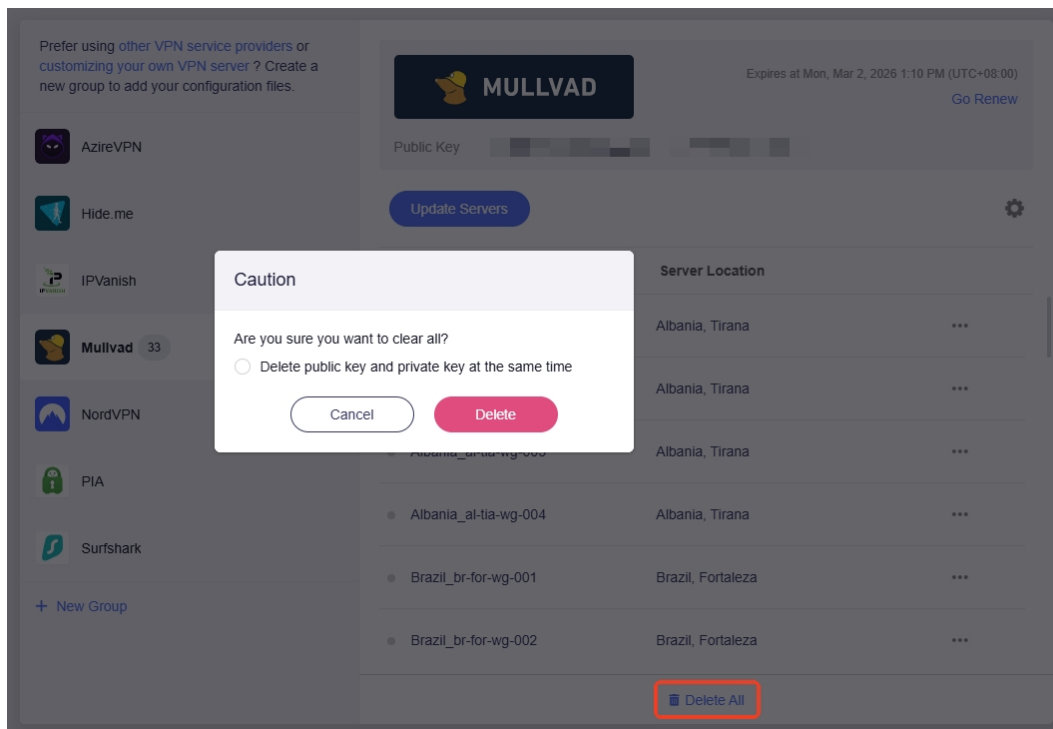
8. Go renew.

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



9. Delete all files.

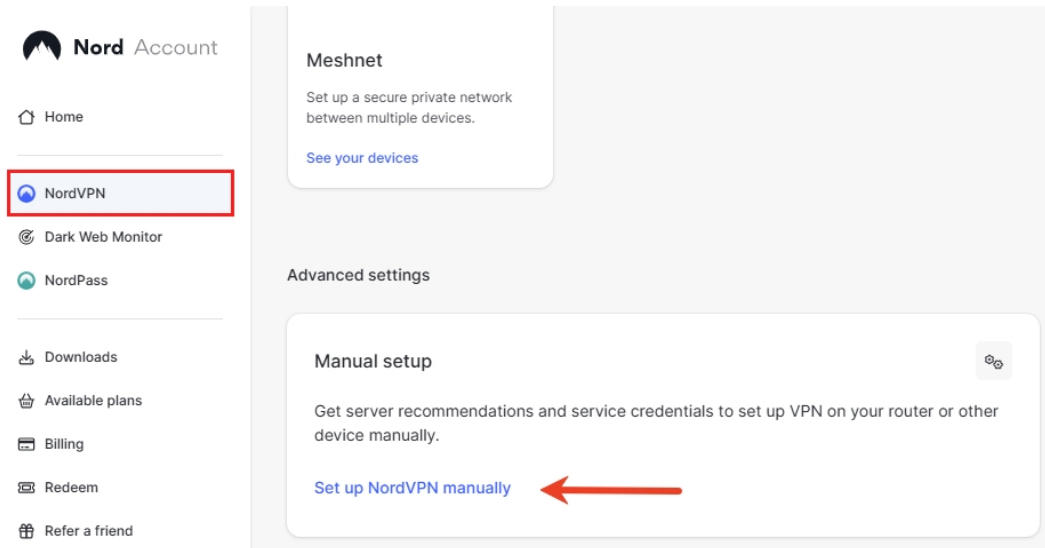
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



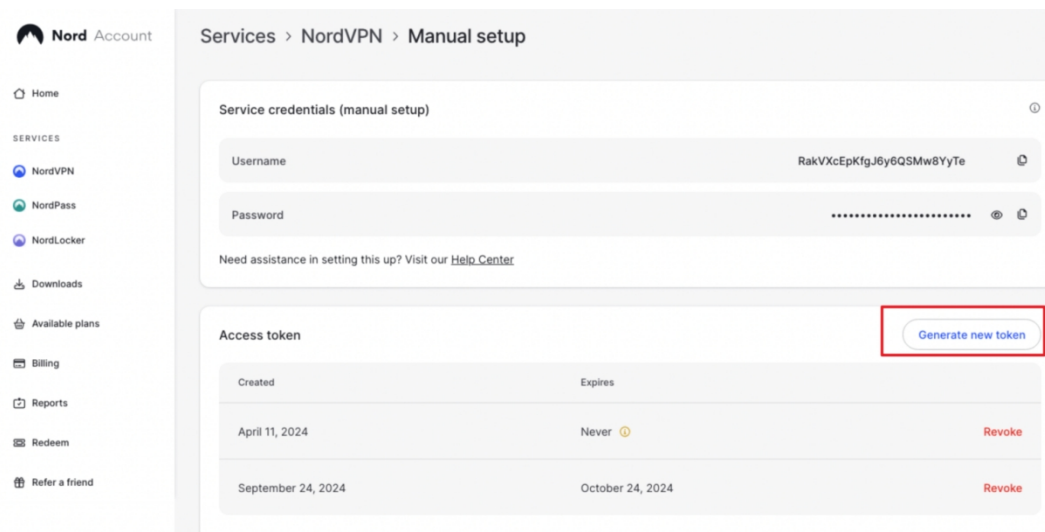
11.2.6 Set Up NordVPN

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

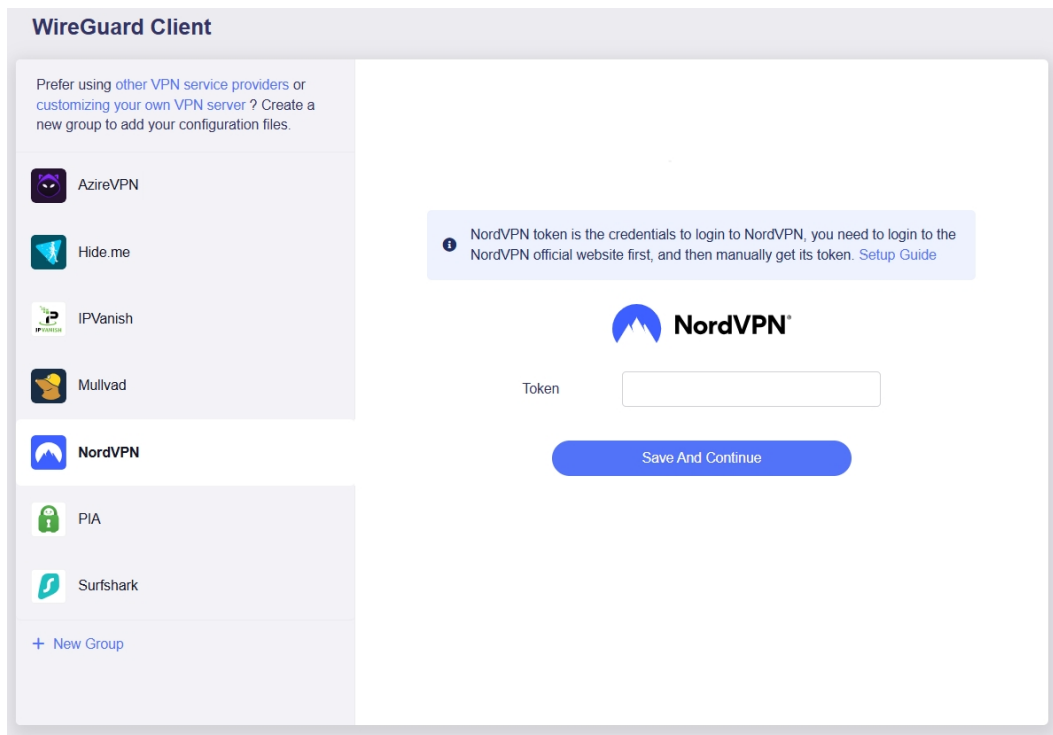
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



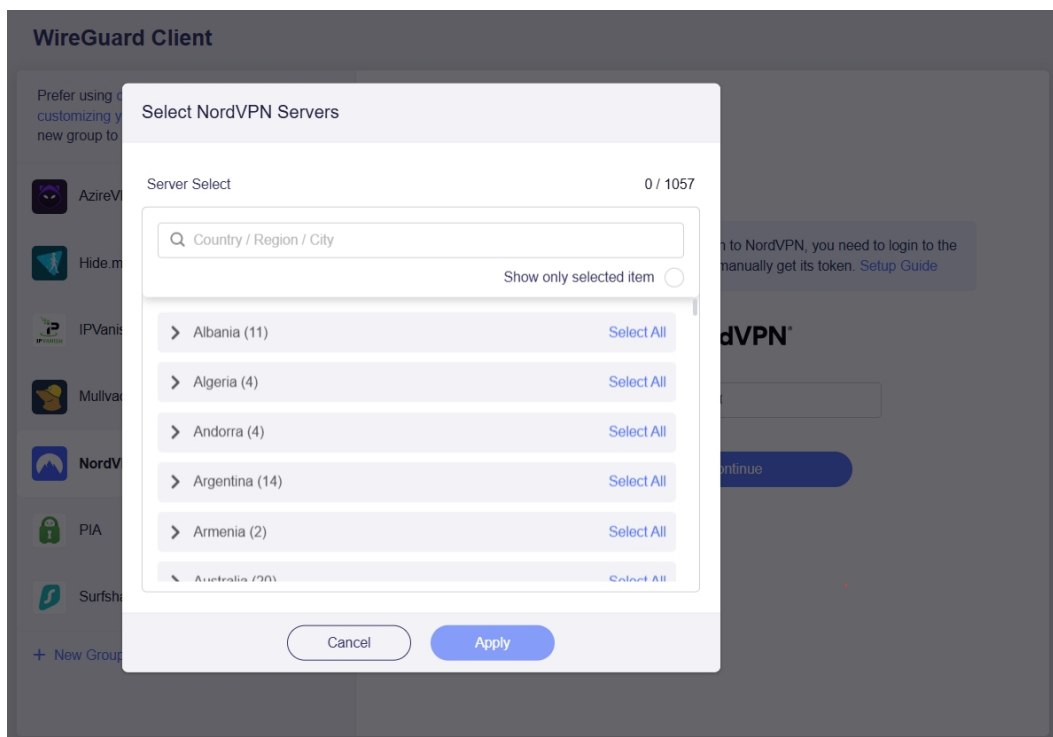
You will find the **Access Token**. Create an access token and copy for later use.



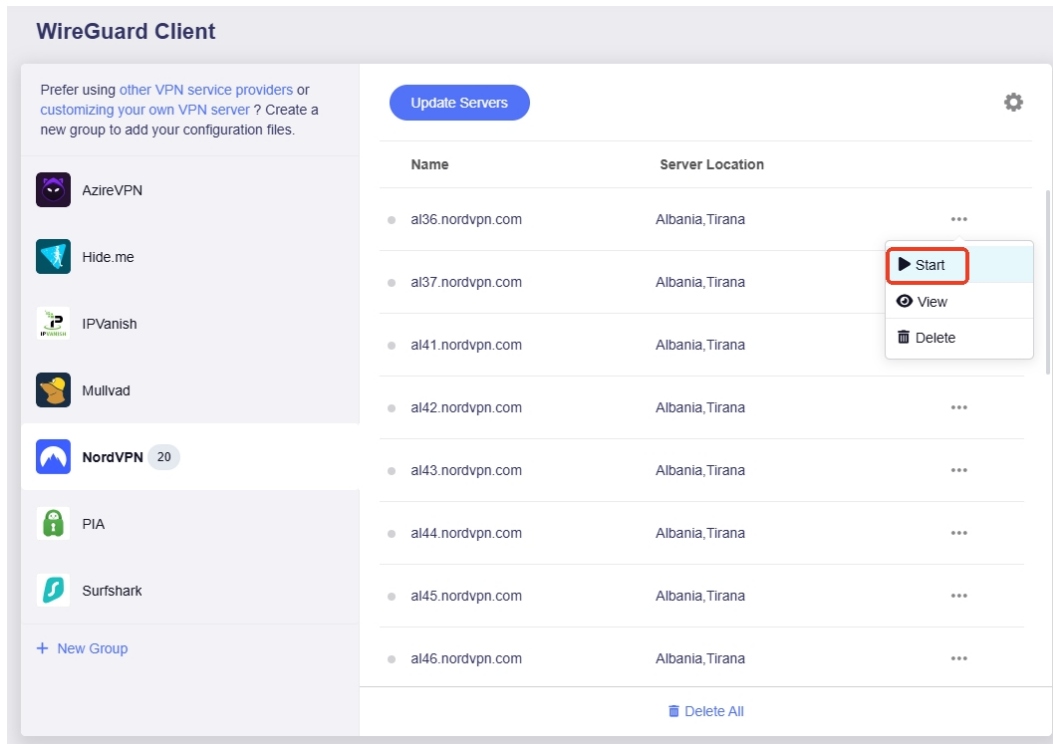
3. Log in to your router's web admin panel and go to **VPN > WireGuard Client > NordVPN**.
4. Input token, and click **Save and Continue**.



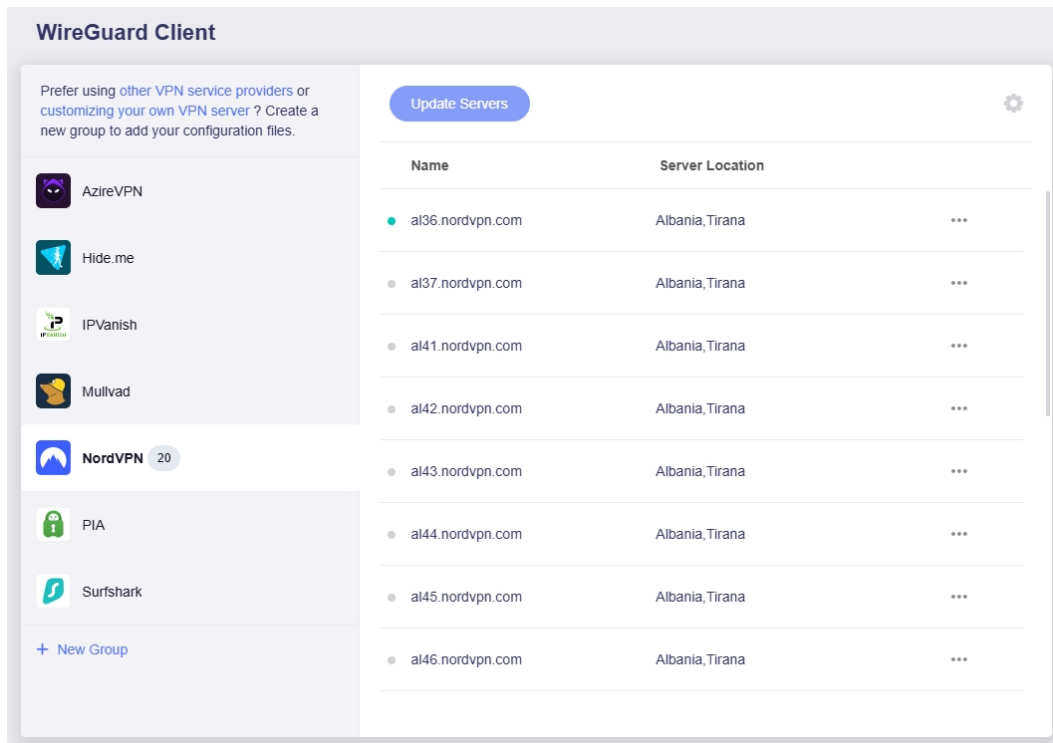
5. Select the server(s) you want to connect to, and click **Apply**.



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



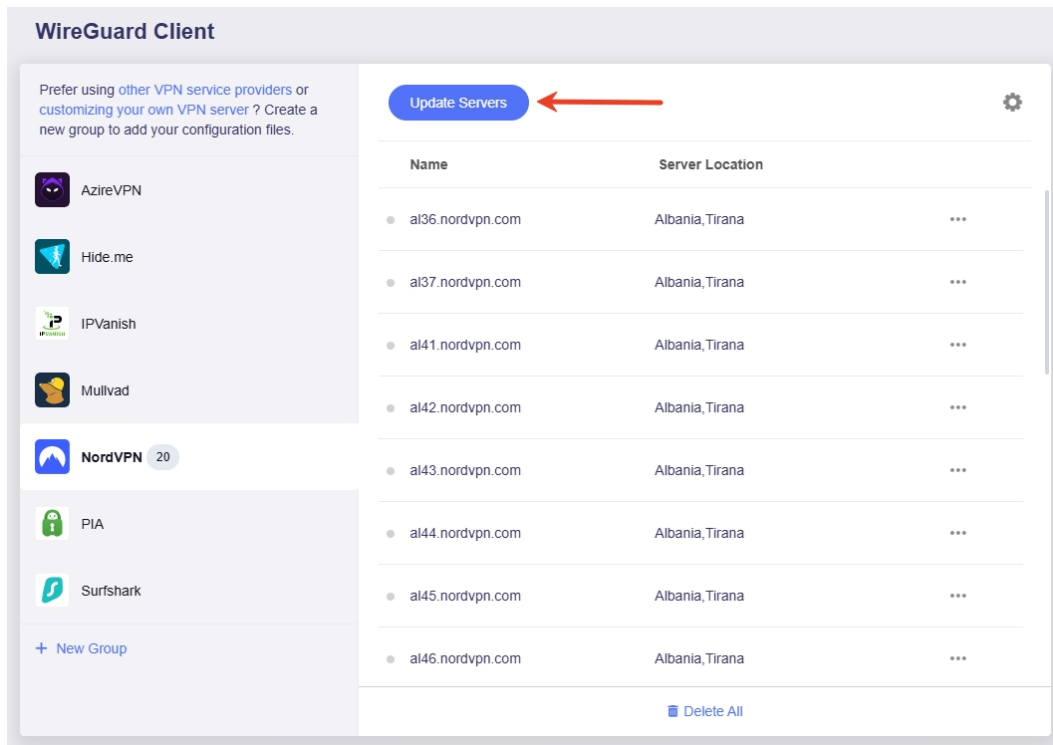
- Once connected, a green dot will appear next to the configuration file.



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

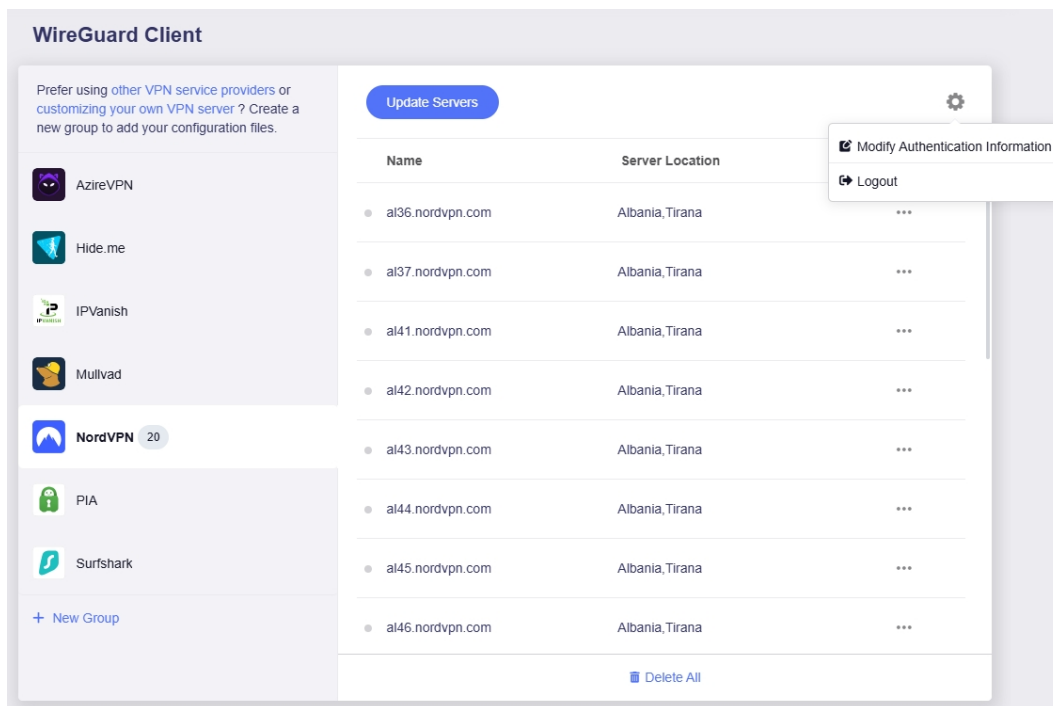
- Update servers.

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



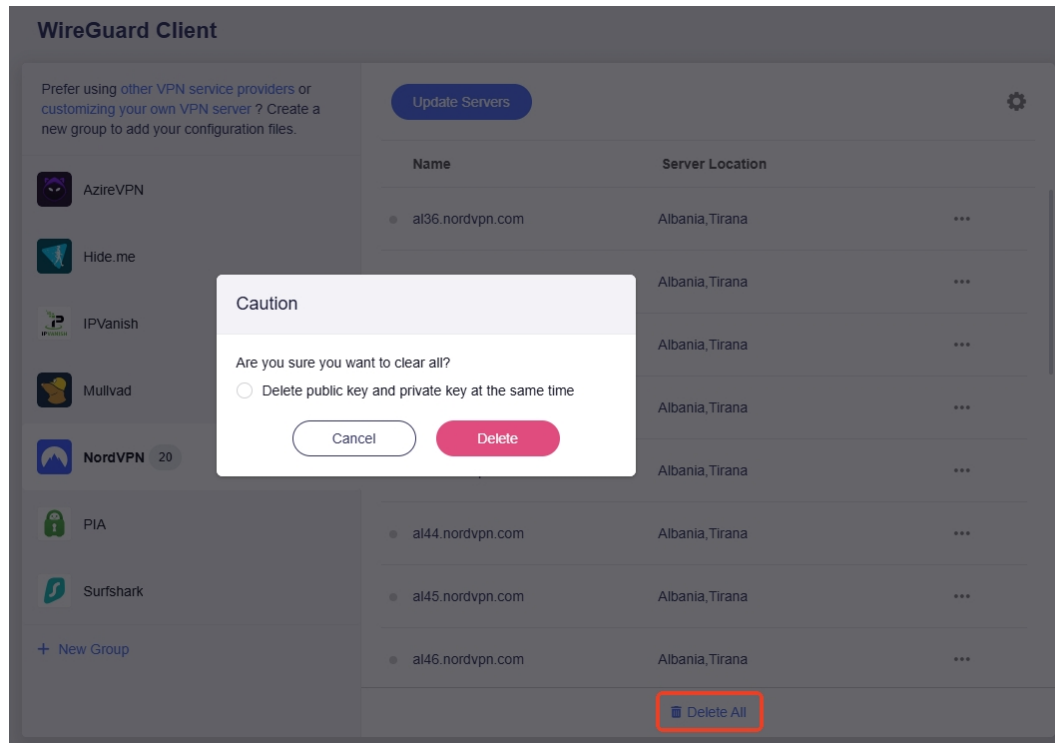
9. Edit credentials or logout.

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



10. Delete all files.

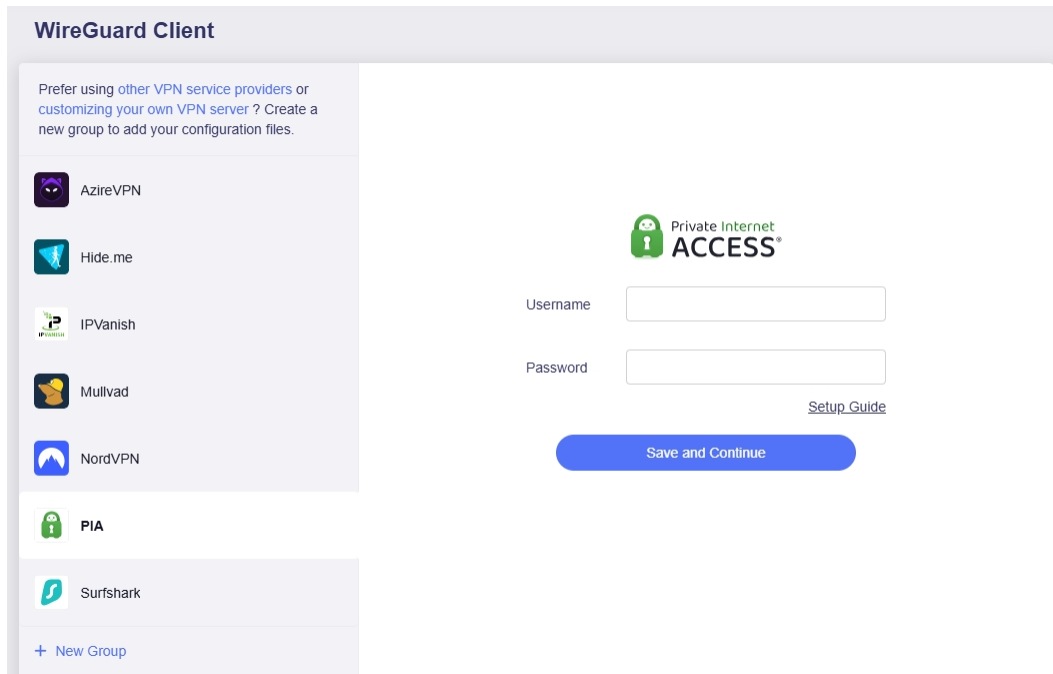
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.7 Set Up PIA (Private Internet Access)

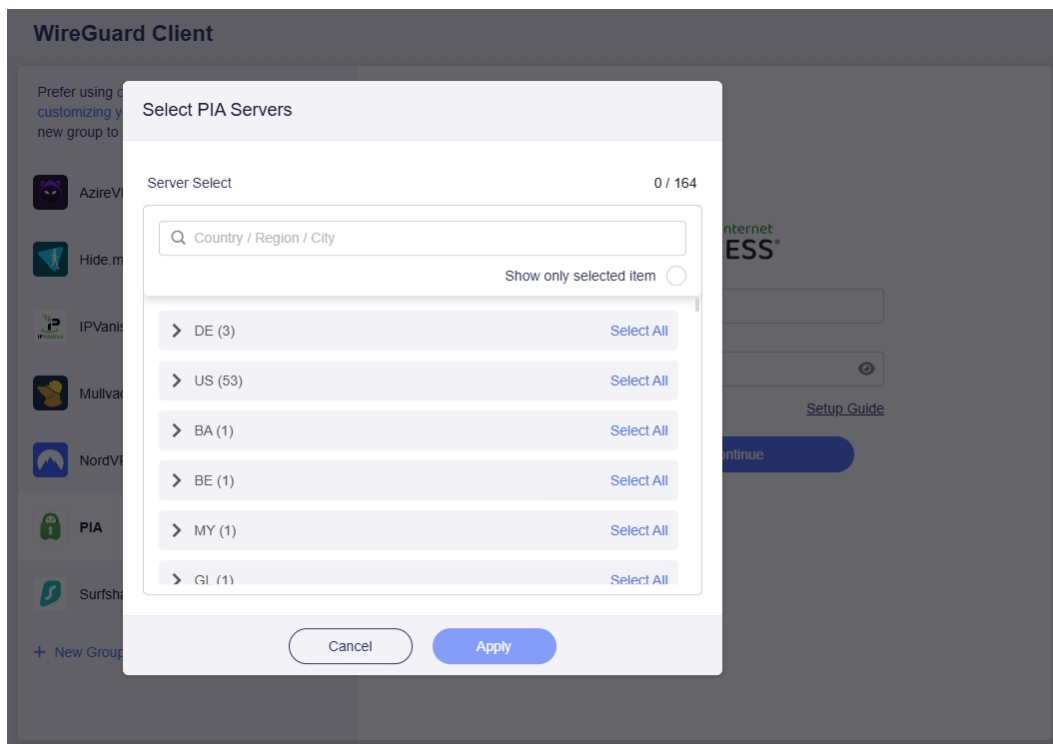
Follow the steps below to set your router as a PIA client.

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**.



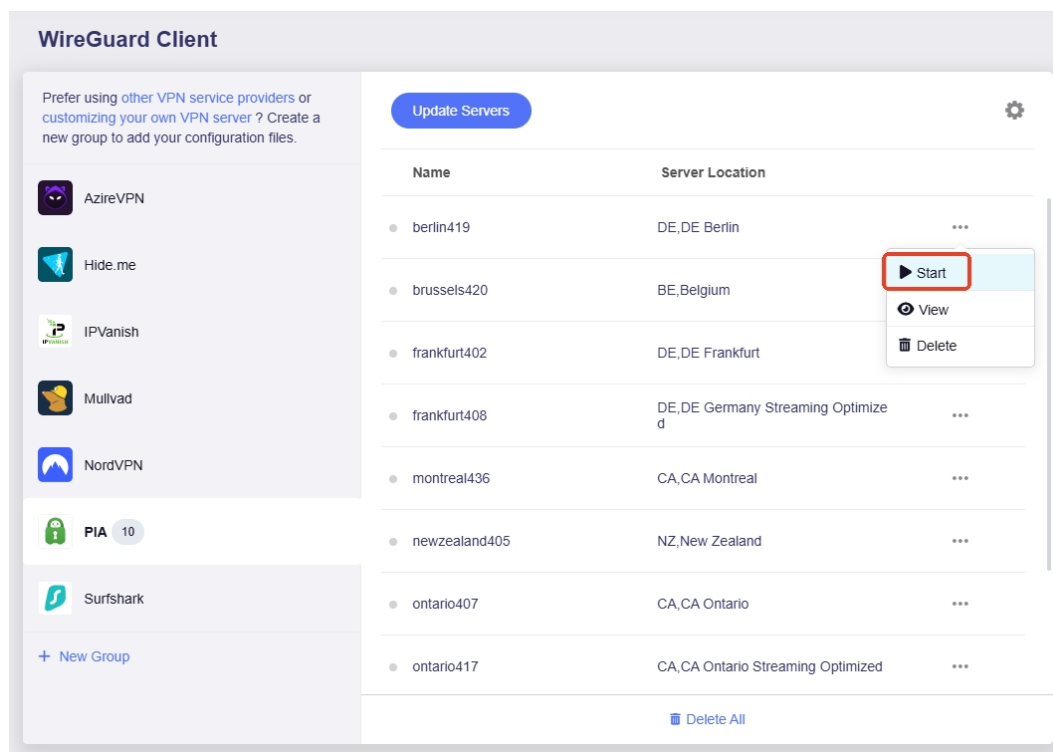
The screenshot shows the 'WireGuard Client' configuration page. On the left, there is a list of VPN providers: AzureVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA (highlighted), and Surfshark, with a '+ New Group' option at the bottom. The main area on the right is for PIA configuration, featuring the 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**.

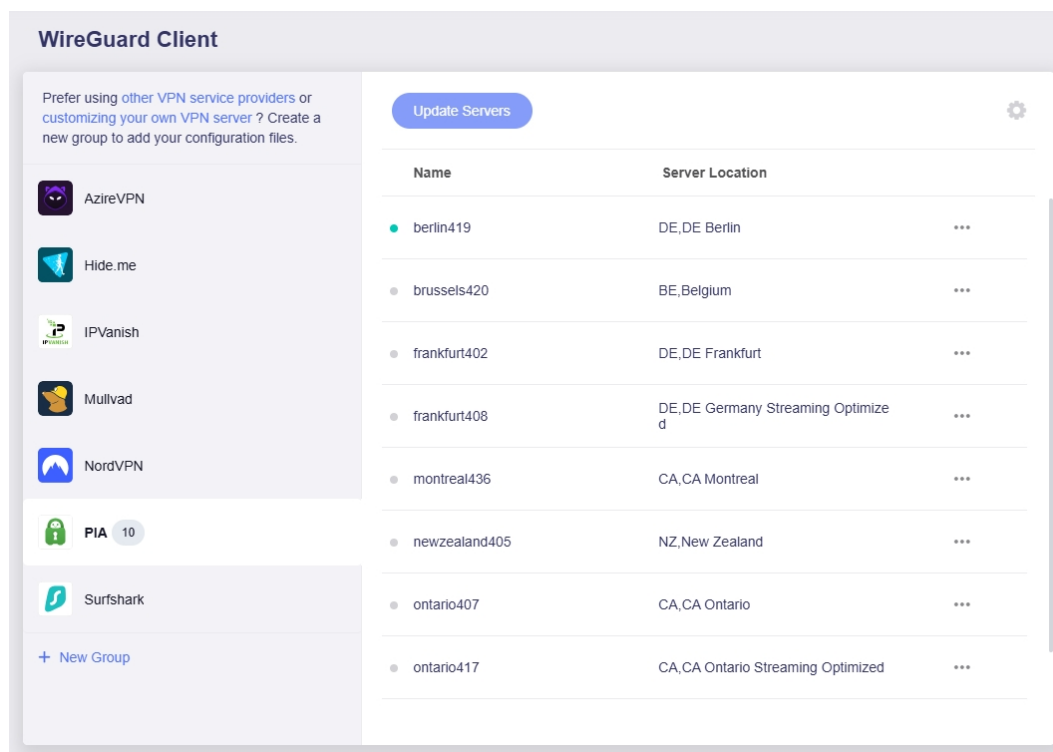


The screenshot shows the 'WireGuard Client' page with a 'Select PIA Servers' modal dialog open. The dialog has a search bar labeled 'Country / Region / City' and a 'Show only selected item' toggle. Below the search bar, a list of regions is displayed: DE (3), US (53), BA (1), BE (1), MY (1), and GL (1). Each region 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.



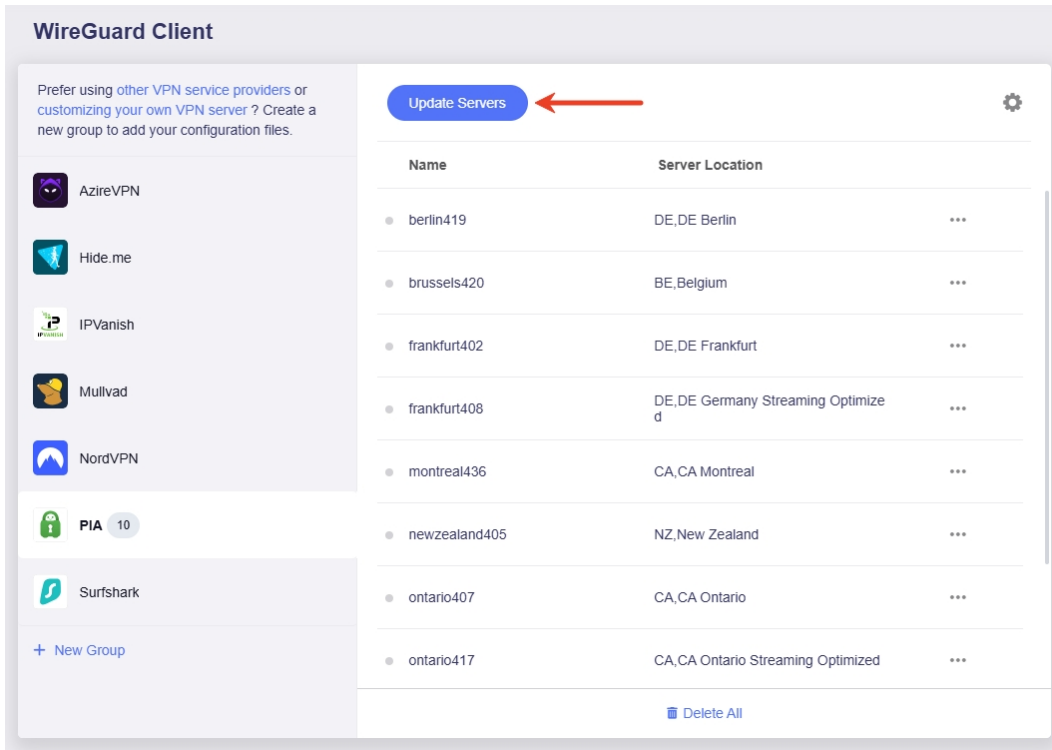
5. Once connected, a green dot will appear next to the configuration file.



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.

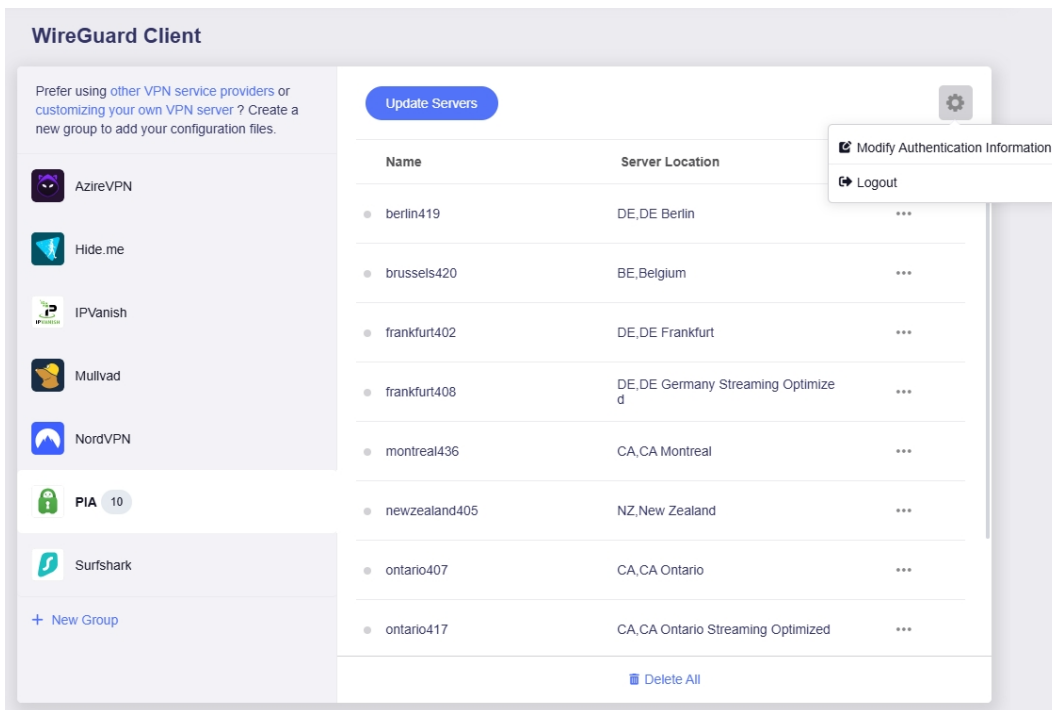


The screenshot shows the WireGuard Client interface. On the left, there's a sidebar with various VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA (with a '10' badge), and Surfshark. Below these is a '+ New Group' button. The main area features a blue 'Update Servers' button at the top, which is highlighted by a red arrow. Below this button is a table of available 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.

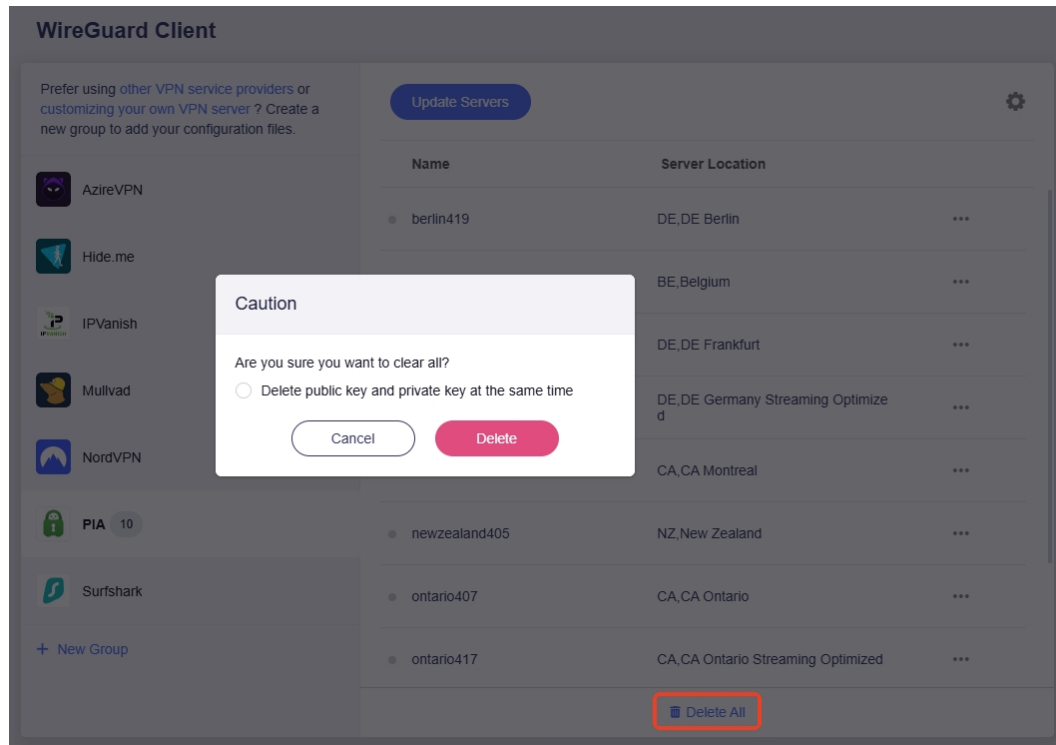
Click the gear icon to edit your login credentials or log out.



This screenshot shows the same WireGuard Client interface as before, but with the settings menu open. The menu is accessed by clicking the 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 list remain visible in the background.

8. Delete all files.

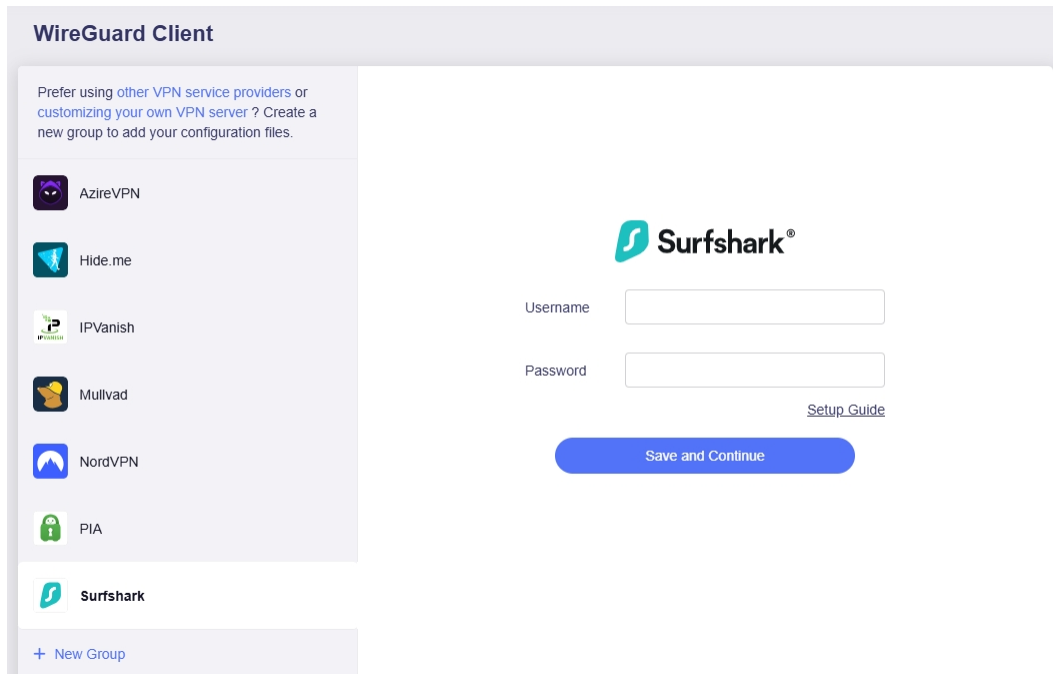
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.8 Set Up Surfshark

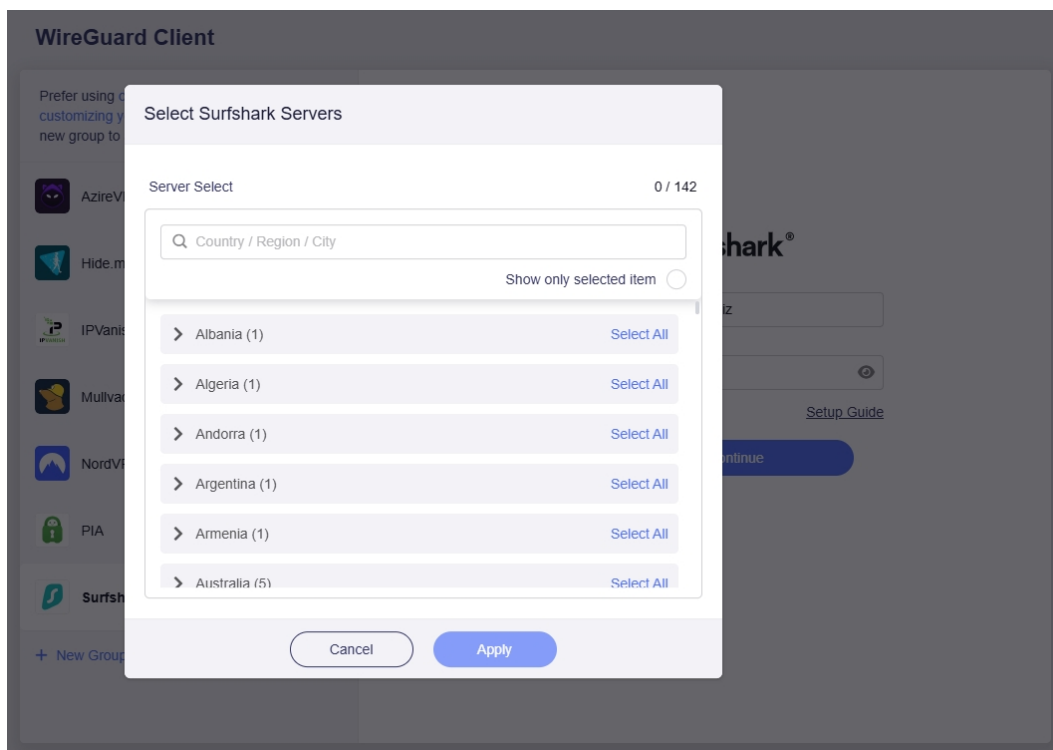
Follow the steps below to set your router as a Surfshark client.

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



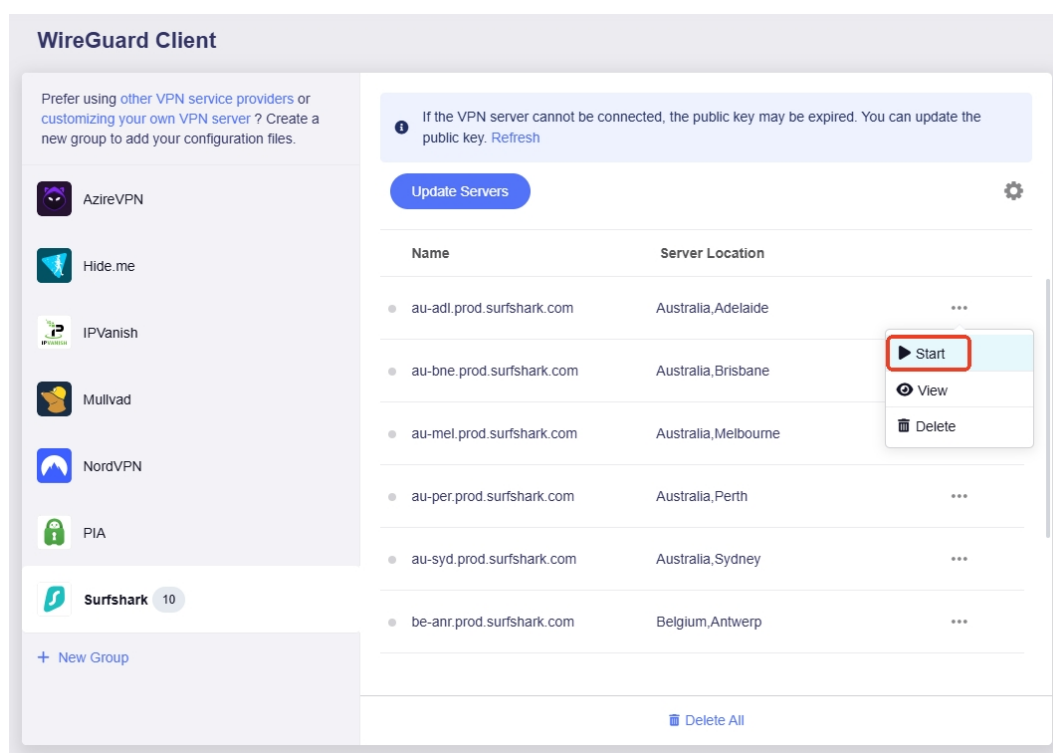
The image shows the 'WireGuard Client' configuration page in a router's web admin panel. On the left, there is a list of VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. Below this list is a '+ New Group' button. The main area on the right is for the Surfshark configuration. 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**.

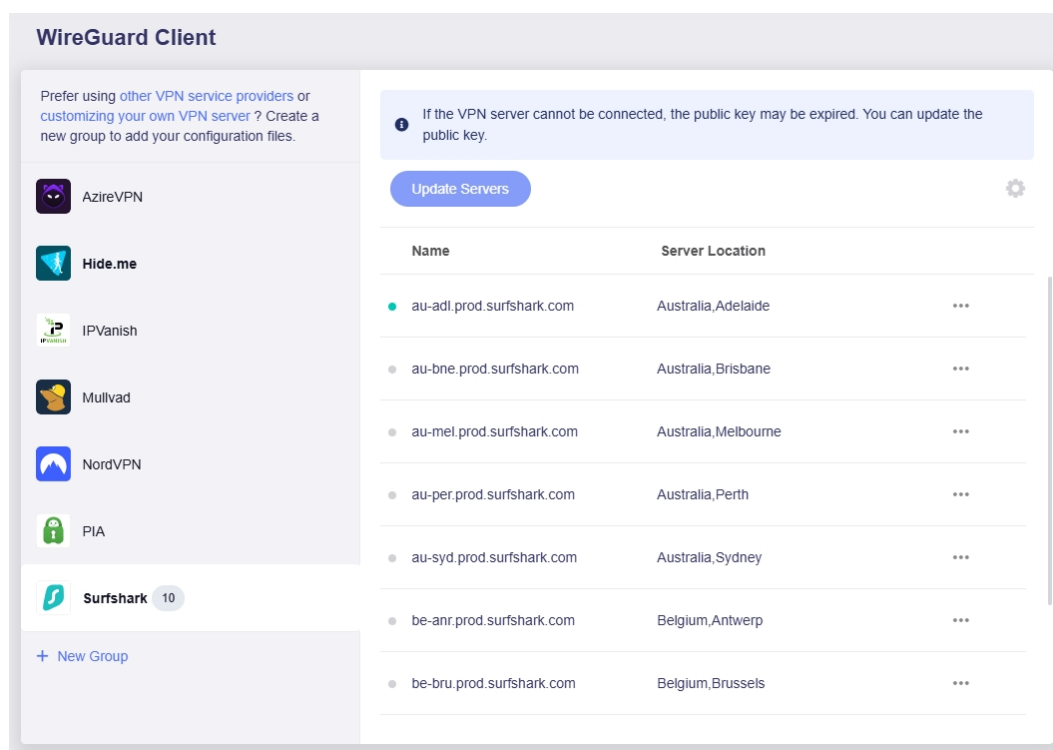


The image shows a 'Select Surfshark Servers' dialog box overlaid on the configuration page. The dialog has a title bar and a search bar labeled 'Country / Region / City'. Below the search bar is a toggle for 'Show only selected item'. A list of countries with their respective server counts is displayed: 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.



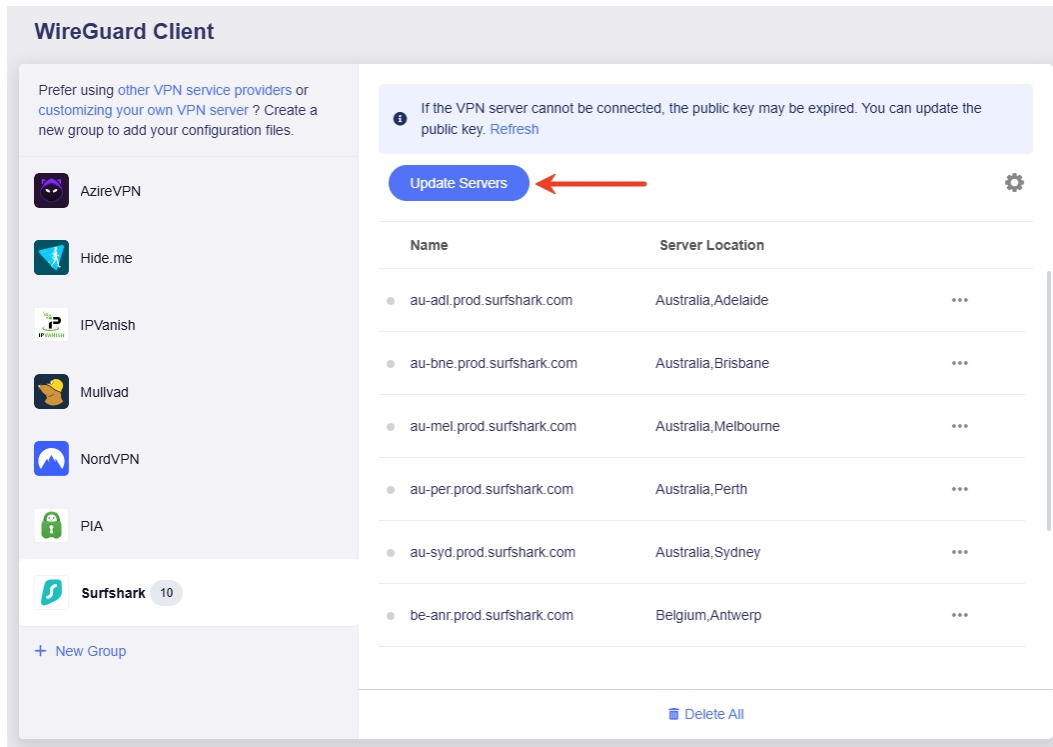
5. Once connected, a green dot will appear next to the configuration file.



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

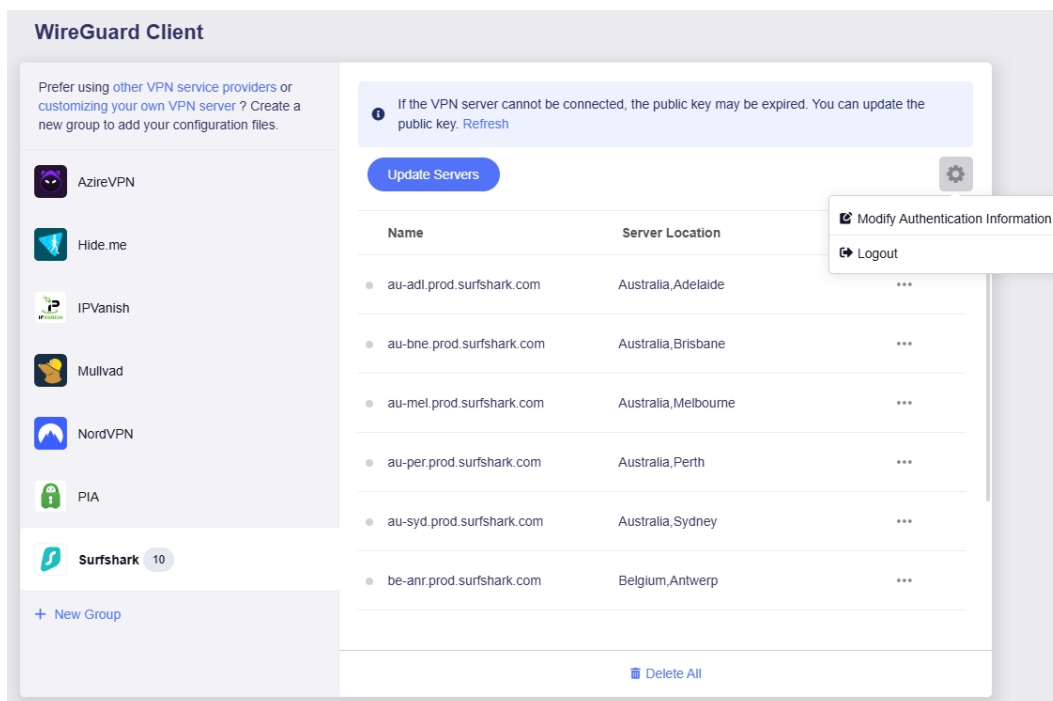
6. Update servers.

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



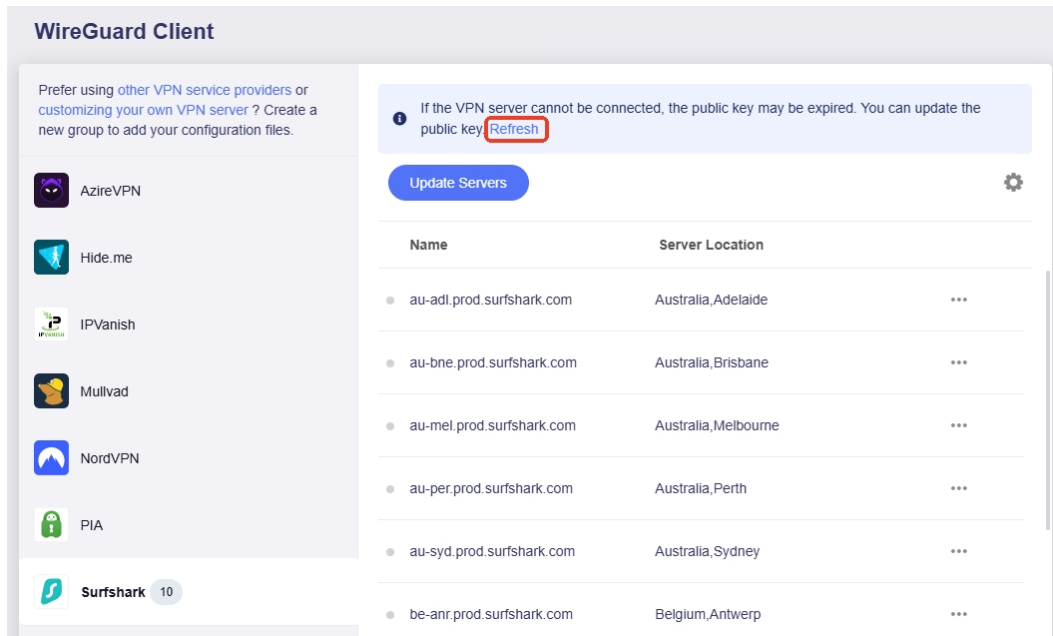
7. Edit credentials or logout.

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



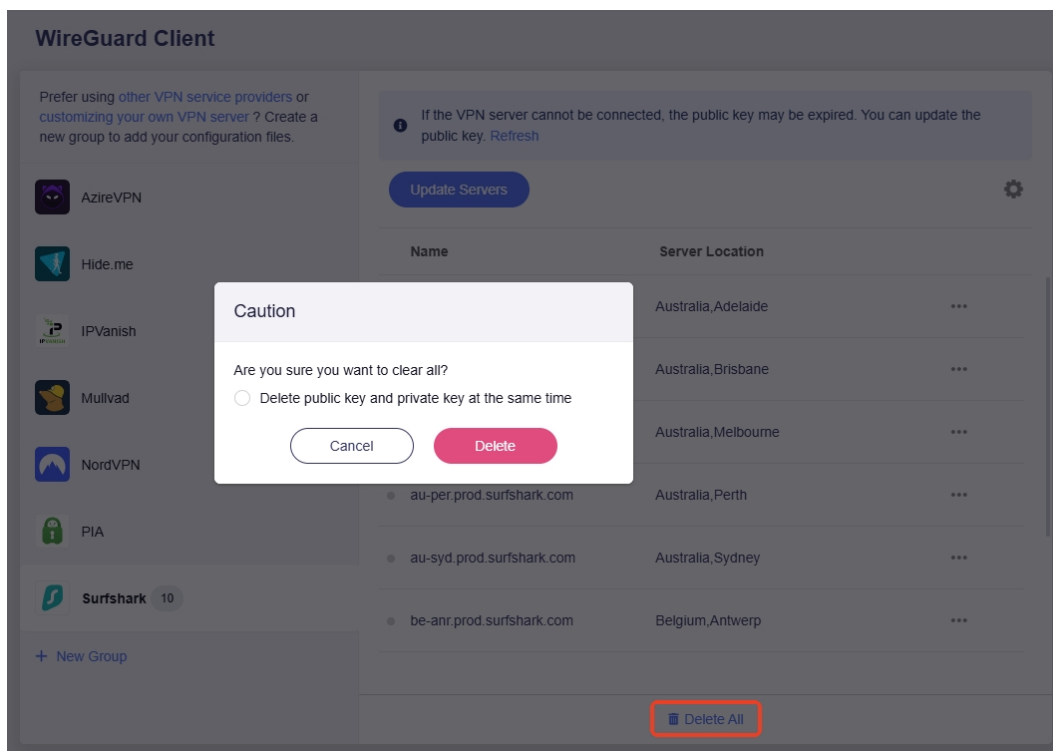
8. Refresh.

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.

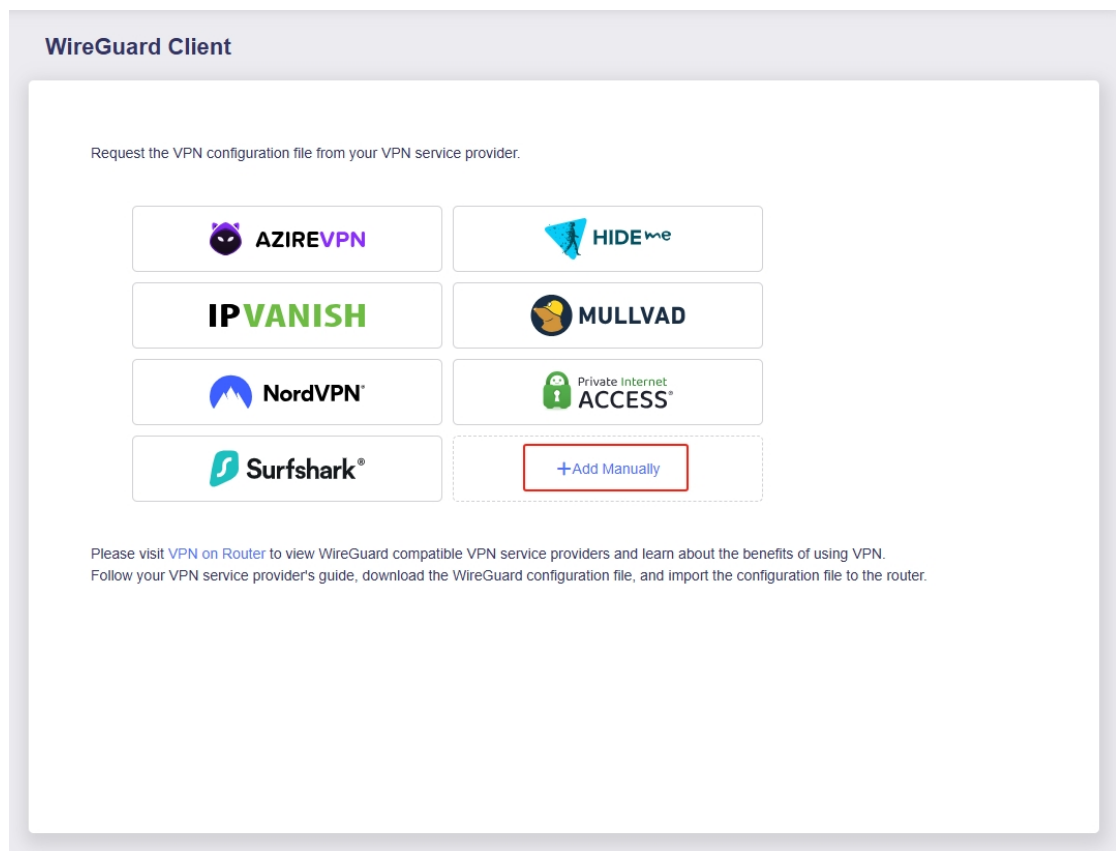


11.2.9 Set Up WireGuard Client Manually (for other providers)

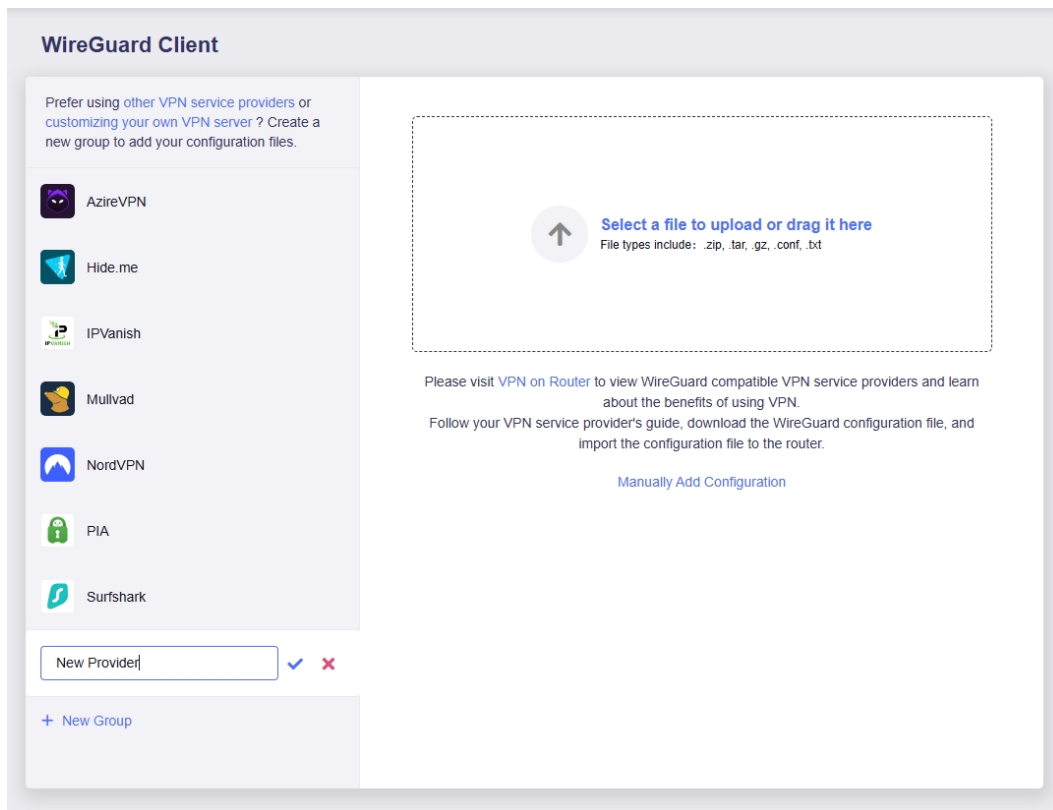
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see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

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

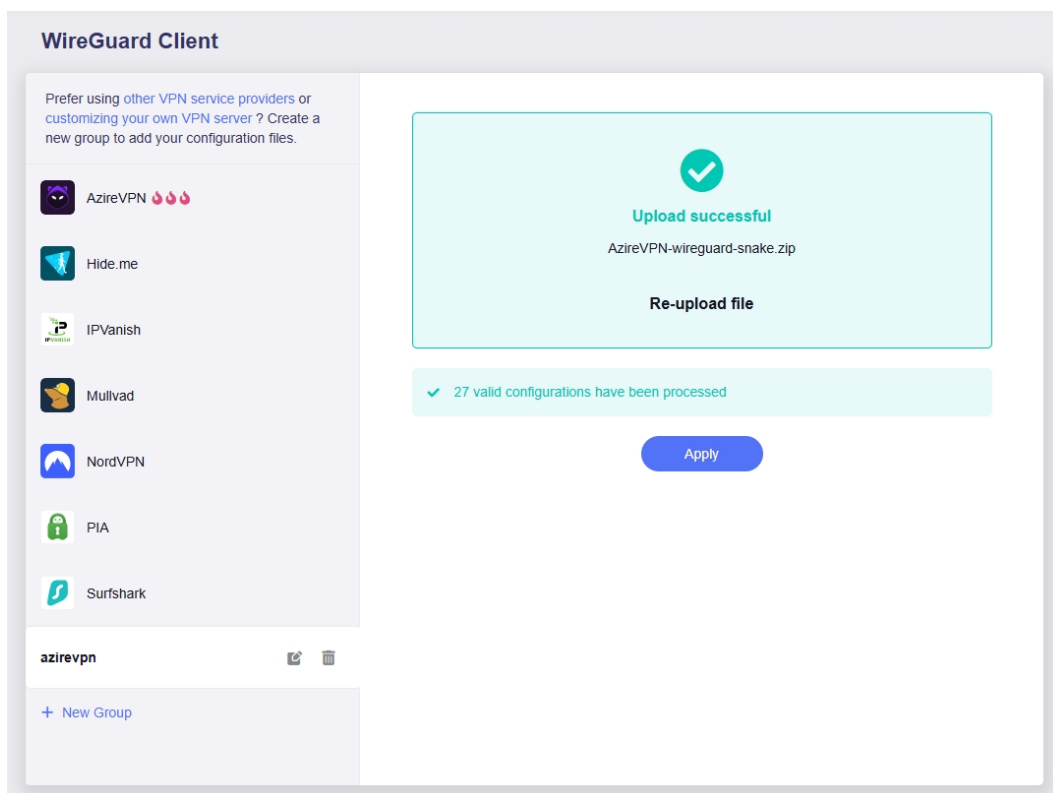
1. Log in to your router's web admin panel and navigate to **VPN > WireGuard Client > Add Manually**.



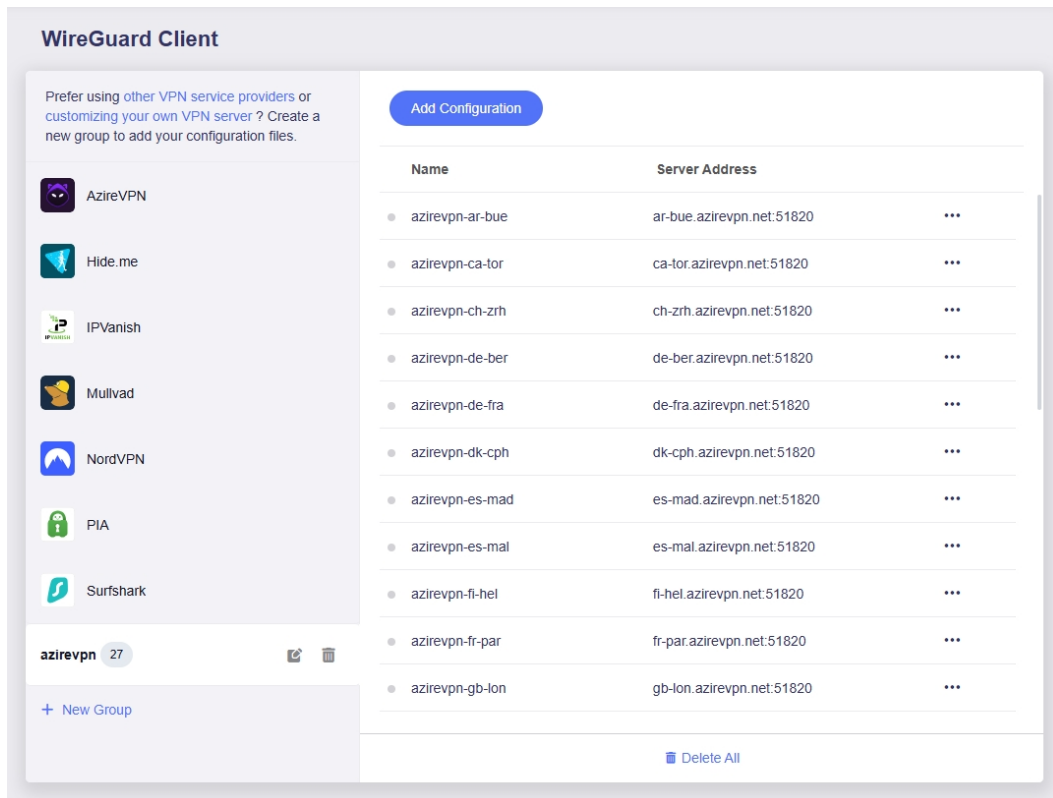
2. It will create a group on the left sidebar. Set a descriptive name for the group.



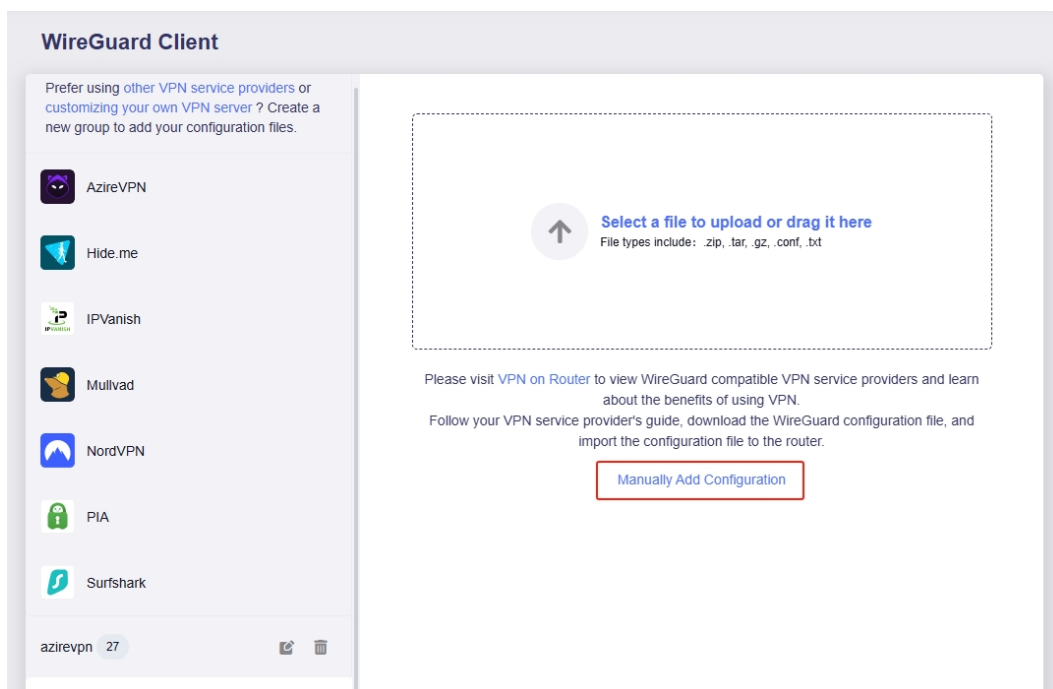
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.

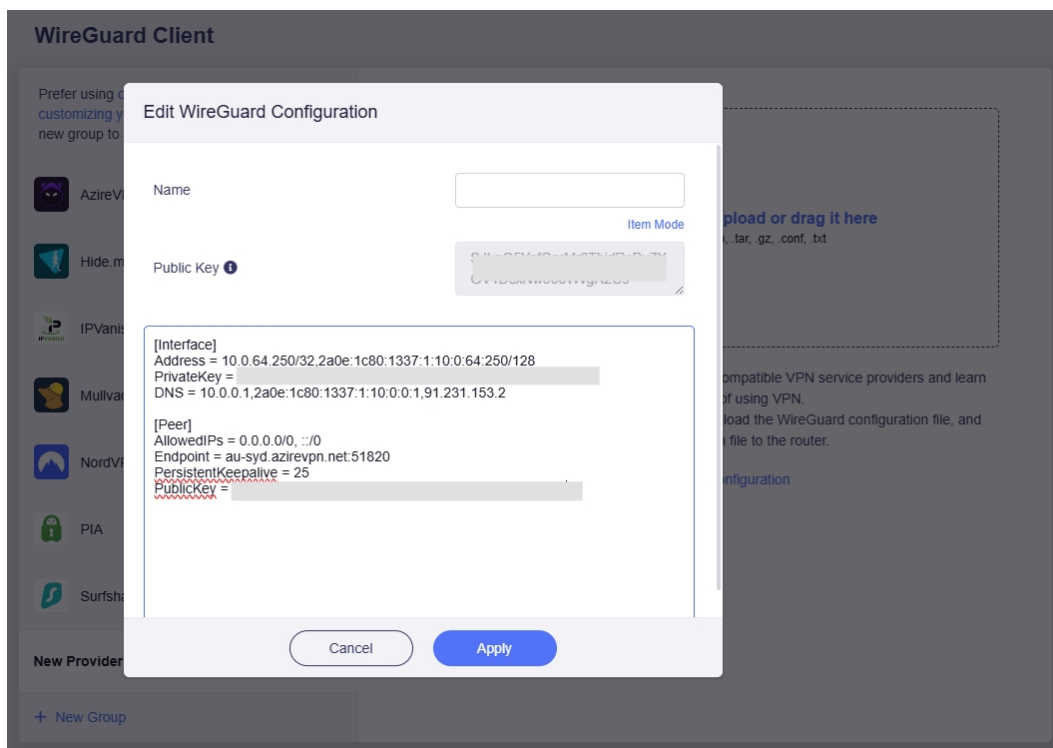


If you upload a compressed file containing multiple configuration files, it will be decompressed automatically, as shown below.

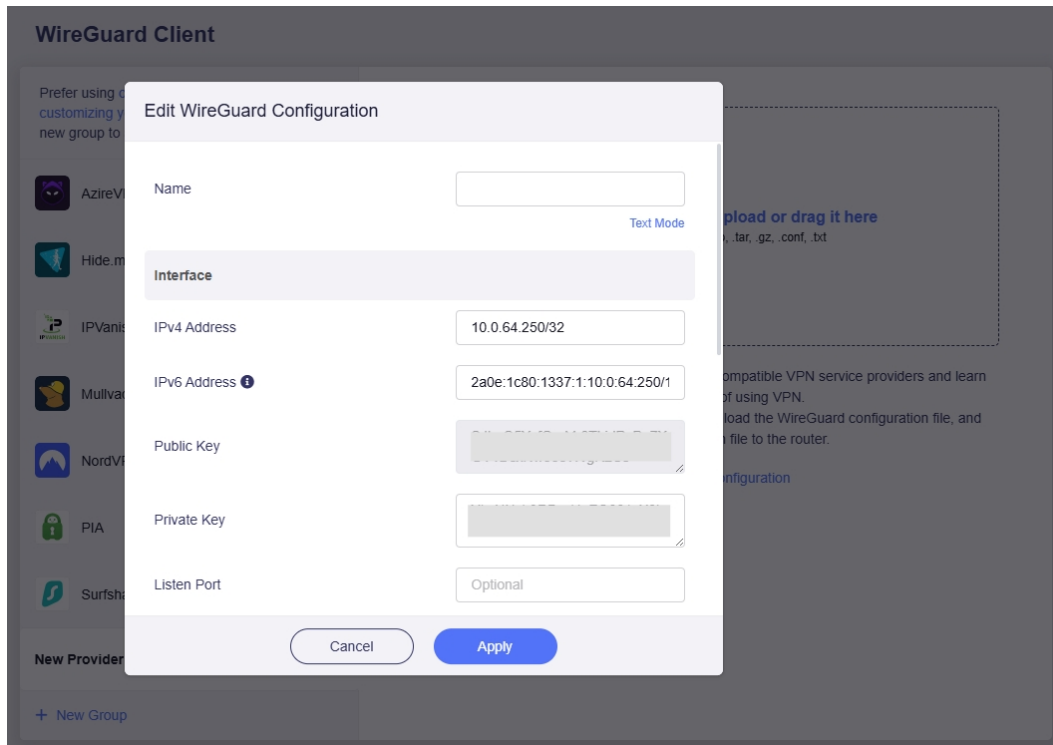


Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

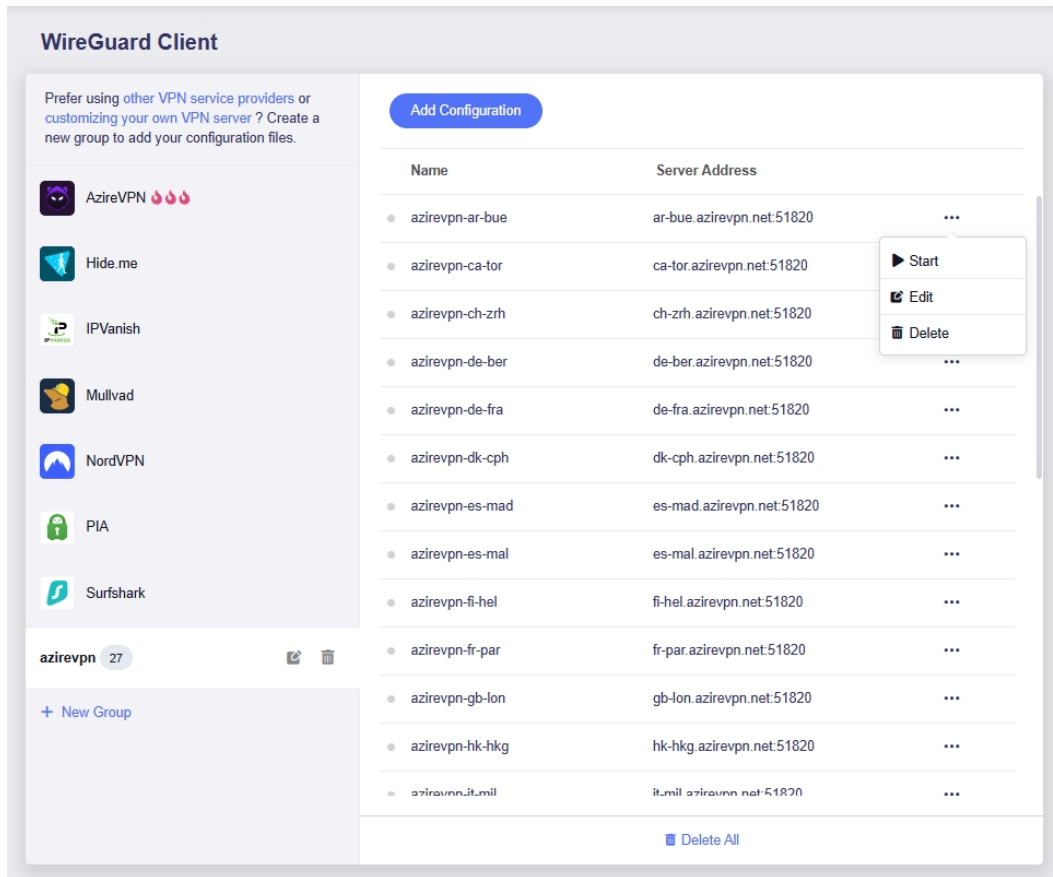




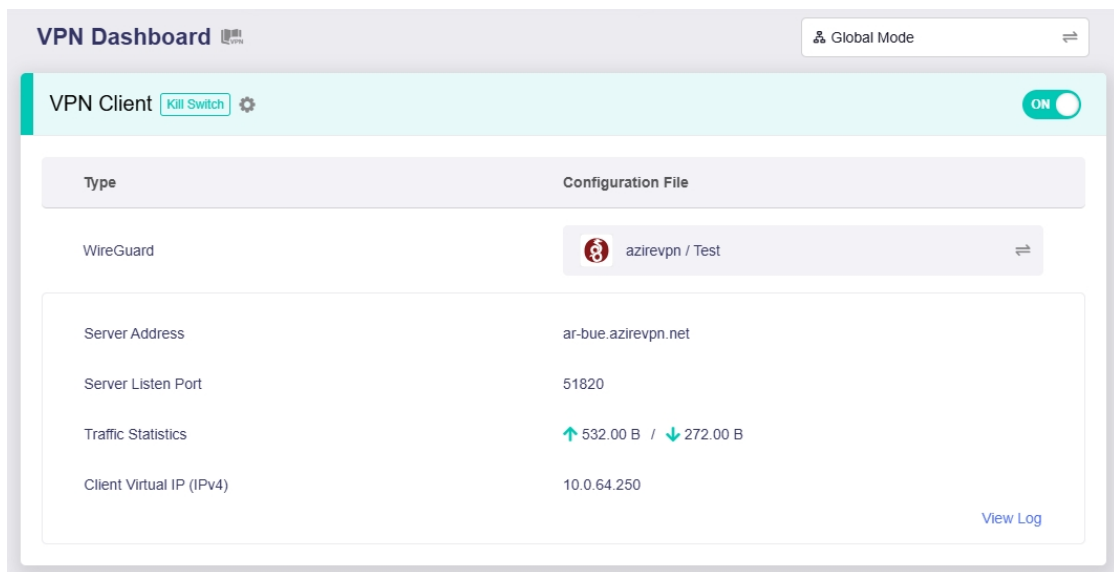
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



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



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



Chapter 12

Network

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

12.1 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.

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

12.1.1 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.

Interface Status Track

 The router tracks the status of the connection to the destination IP to establish whether the interface is available.

 Ethernet 1	 
 Repeater	 
 Tethering	 
 Ethernet 2	 

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

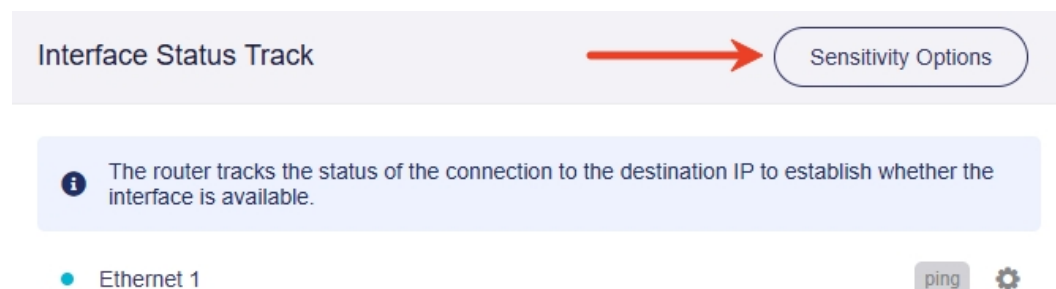
Cancel

Apply

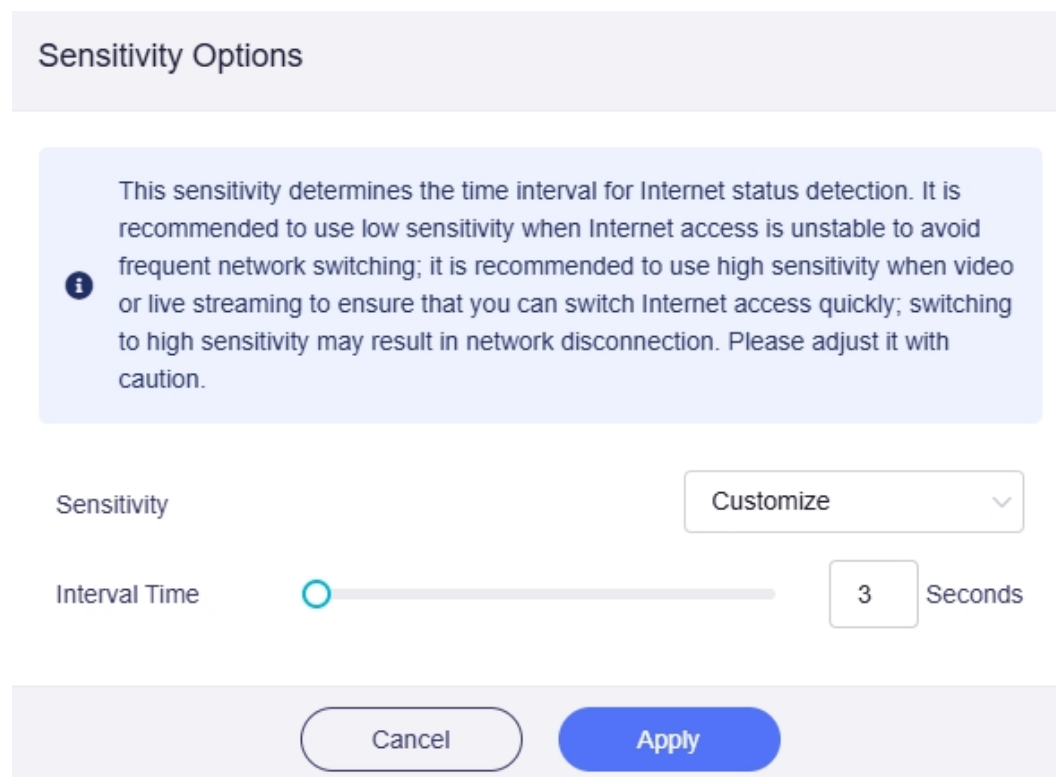
- **Enable Interface Status Track:** It is enabled by default. If disabled, the router will determine the interface status based on physical conditions (e.g., whether the Ethernet cable is plugged in).
- **Detection Mode:** This feature was introduced as Low Data Mode in firmware v4.5, then renamed Detection 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 if 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.



12.1.2 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.

The router supports connections to multiple network interfaces at the same time. You can configure how these multiple networks should be used.

i Failover: If the current, active link fails, the router will automatically switch to another network interface.

Load Balance: Uses multiple network interfaces at the same time to increase the total bandwidth of the router. Note that connections to the same application or site will usually only use one interface.

Mode **i**

Failover

Load Balance

Interface Priority

1	Ethernet 1	≡
2	Ethernet 2	≡
3	Repeater	≡
4	Tethering	≡

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

The router supports connections to multiple network interfaces at the same time. You can configure how these multiple networks should be used.



Failover: If the current, active link fails, the router will automatically switch to another network interface.

Load Balance: Uses multiple network interfaces at the same time to increase the total bandwidth of the router. Note that connections to the same application or site will usually only use one interface.

Mode

Failover

Load Balance

Load Ratio

Ethernet 1

1

Repeater

1

Tethering

1

Ethernet 2

1

Apply

You can also customize the load ratio if needed. For example, if Ethernet 1 has a bandwidth of 100 Mbps, Repeater has 200 Mbps, and no other connections are active, set the load ratios to 1 for Ethernet 1, 2 for Repeater, and 0 for Tethering, Cellular and Ethernet 2. 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 Repeater. Unlike Failover mode, this mode optimizes overall throughput efficiency by balancing traffic load across all available interfaces.

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

12.2 Subnet

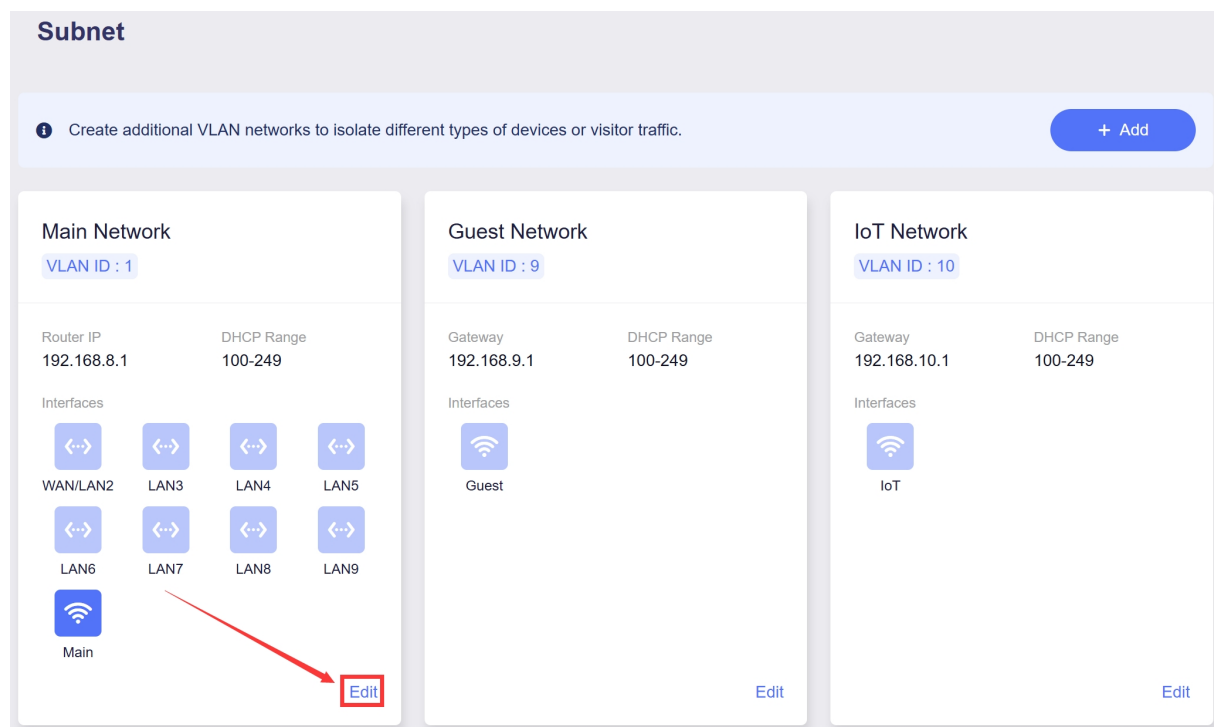
Subnet refers to a logical subdivision of a network, used to organize and isolate devices within different network segments.

Log in to your router's web Admin Panel and navigate to **NETWORK > Subnet**. Here you can configure Main Network, Guest Network, IoT Network, and custom VLAN Networks.

12.2.1 Main Network

The Main Network refers to the connection established via your primary Wi-Fi or Ethernet. It provides visibility into all interface statuses, VLAN ID, router IP address, and DHCP Range.

Click **Edit** in the lower-right corner to configure the Main Network.



The configuration page includes Basic settings, DHCP server settings and Address Reservation.

Basic Settings

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

Main Network ✕

LAN

i 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 i

192.168.8.1

Netmask

255.255.255.0

VLAN ID

1

Security Settings

AP Isolation i



- **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.
- **VLAN ID:** The Main Network's default VLAN ID is 1, which cannot be modified.
- **AP Isolation:** You can isolate client devices into a separate network segment. These devices will not be able to communicate with other devices on the same network.

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 if 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](#)

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

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](#)

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.

Address Reservation

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

Follow the steps below to configure address reservation if needed.

1. Log in to your router's web Admin Panel, navigate to **Subnet > Main Network > Address Reservation**, and click **Add**.

Address Reservation

i 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 the 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

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 Hostname and a custom Name for easy identification. Then click **Submit**.

Add a New Reservation Entry

MAC Address	
IP Address	192.168.8.155
Hostname	iPhone
Name	Holly-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 the 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 Address ▾	IP Address ▾	Hostname ▾	Name ▴▾	Action
	192.168.8.155	iPhone	Holly-iPhone	...

12.2.2 Guest Network

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

Log in to your router's web Admin Panel and go to **NETWORK > Subnet > Guest Network** section. This page allows you to configure Guest Network settings, including basic settings and DHCP server.

Click **Edit** in the lower-right corner to configure the Guest Network.

The screenshot displays the 'Subnet' configuration page. At the top, there is a header 'Subnet' and a blue bar with a tip: 'Create additional VLAN networks to isolate different types of devices or visitor traffic.' and a '+ Add' button. Below this, there are three network configuration cards:

- Main Network** (VLAN ID : 1): Shows Router IP 192.168.8.1, DHCP Range 100-249, and a list of interfaces (WAN/LAN2, LAN3, LAN4, LAN5, LAN6, LAN7, LAN8, LAN9, and Main) with status icons. An 'Edit' button is at the bottom right.
- Guest Network** (VLAN ID : 9): Shows Gateway 192.168.9.1, DHCP Range 100-249, and a single 'Guest' interface with a Wi-Fi icon. A red arrow points from the text above to the 'Edit' button at the bottom right.
- IoT Network** (VLAN ID : 10): Shows Gateway 192.168.10.1, DHCP Range 100-249, and a single 'IoT' interface with a Wi-Fi icon. An 'Edit' button is at the bottom right.

Basic Settings

The basic settings include Gateway, Netmask, AP Isolation, VLAN ID and WAN Access Control.

Guest Network

You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

Gateway

192.168.9.1

Netmask

255.255.255.0

VLAN ID

9

Security Settings

AP Isolation

WAN Access Control

Unrestricted

- **Gateway:** It is 192.168.9.1 by default and can be changed if needed, but it must not conflict with the gateway of the main network.
- **Netmask:** Two options are available: 255.255.255.0 and 255.255.0.0.
- **VAN ID:** The Guest Network's default VLAN ID is 9, which can be modified as required.
- **AP Isolation:** It is used to isolate guest network clients into separate segments so they cannot communicate with other devices on the same network.
- **WAN Access Control:** WAN Access Control manages local subnet access to WAN-side networks, including the internet and other WAN subnets.

Three WAN access control modes are available:

- **Unrestricted:** Allows this subnet to access the internet and other WAN-side subnets without restrictions.
- **Block WAN Subnet:** Blocks access to other WAN-side subnets. Internet access remains available.
- **Block Internet Access:** Blocks all outbound access, including the internet and WAN-side subnets.

DHCP Server

Since the Guest network is disabled by default, its DHCP server is disabled and hidden until it is manually enabled.

When enabled, the DHCP server automatically assigns IP addresses and other communication parameters to each connected client. The DHCP server's IP address pool for the Guest network ranges from 192.168.9.100 to 192.168.9.249. You can customize the address range if 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

192.168.9.100

End IP Address

192.168.9.249

[Advanced](#)

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

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

192.168.9.100

End IP Address

192.168.9.249

[Advanced](#)

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 the Guest network's DHCP.
- **Gateway:** The router component that routes traffic between the guest 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.

12.2.3 IoT Network

IoT Network creates a dedicated Wi-Fi network for IoT devices. Isolated from the primary network, it delivers better compatibility and improved security. You can directly view the interface status, VLAN ID, Gateway, and DHCP Range.

Log in to your router's web Admin Panel and go to **NETWORK > Subnet > IoT Network** section. This page allows you to configure IoT Network settings, including basic settings and DHCP server.

Click **Edit** in the lower-right corner to configure the Guest Network.

Subnet

Create additional VLAN networks to isolate different types of devices or visitor traffic. [+ Add](#)

Network Type	VLAN ID	Router IP / Gateway	DHCP Range	Interfaces	Action
Main Network	VLAN ID : 1	192.168.8.1	100-249	WAN/LAN2, LAN3, LAN4, LAN5, LAN6, LAN7, LAN8, LAN9, Main	Edit
Guest Network	VLAN ID : 9	192.168.9.1	100-249	Guest	Edit
IoT Network	VLAN ID : 10	192.168.10.1	100-249	IoT	Edit

Basic Settings

The basic settings include Gateway, Netmask, AP Isolation, VLAN ID and WAN Access Control.

IoT Network

You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

Gateway

192.168.10.1

Netmask

255.255.255.0

VLAN ID

10

Security Settings

AP Isolation

WAN Access Control

Unrestricted

- **Gateway:** It is 192.168.10.1 by default and can be changed if needed, but it must not conflict with the gateway of the main network.
- **Netmask:** Two options are available: 255.255.255.0 and 255.255.0.0.
- **VAN ID:** The Guest Network's default VLAN ID is 10, which can be modified as required.
- **AP Isolation:** It is used to isolate guest network clients into separate segments so they cannot communicate with other devices on the same network.
- **WAN Access Control:** WAN Access Control manages local subnet access to WAN-side networks, including the internet and other WAN subnets.

Three WAN access control modes are available:

- **Unrestricted:** Allows this subnet to access the internet and other WAN-side subnets without restrictions.
- **Block WAN Subnet:** Blocks access to other WAN-side subnets. Internet access remains available.
- **Block Internet Access:** Blocks all outbound access, including the internet and WAN-side subnets.

DHCP Server

Since the IoT network is disabled by default, its DHCP server is disabled and hidden until it is manually enabled.

When enabled, the DHCP server automatically assigns IP addresses and other communication parameters to each connected client. The DHCP server's IP address pool for the IoT network ranges from 192.168.10.100 to 192.168.10.249. You can customize the address range if 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](#)

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

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](#)

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 the Guest network's DHCP.
- **Gateway:** The router component that routes traffic between the guest 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.

12.2.4 VLAN Networks

VLAN Networks enables the creation of additional VLAN networks to isolate different device types or visitor traffic as needed.

Click the **+ Add** button on the right side of the page to configure a new network.

Subnet

Create additional VLAN networks to isolate different types of devices or visitor traffic.

+ Add

Network Name	VLAN ID	Router IP	DHCP Range	Interfaces
Main Network	VLAN ID : 1	192.168.8.1	100-249	WAN/LAN2, LAN3, LAN4, LAN5, LAN6, LAN7, LAN8, LAN9, Main
Guest Network	VLAN ID : 9	192.168.9.1	100-249	Guest
IoT Network	VLAN ID : 10	192.168.10.1	100-249	IoT

This page allows you to configure VLAN Networks settings, including basic settings and DHCP server.

Basic Settings

You can configure the basic VLAN Networks information on this page.

Add A New Network



You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

Name

Enter network name

Gateway

Netmask

VLAN ID

9 - 4000

Security Settings

AP Isolation



WAN Access Control

Unrestricted



- **Name:** Customize a name for your newly created subnet for identification.
- **Gateway:** It is 192.168.10.1 by default and can be changed if needed, but it must not conflict with the gateway of the main network.
- **Netmask:** Two options are available: 255.255.255.0 and 255.255.0.0.
- **VAN ID:** When creating a subnet, you must assign a VLAN ID between 9 and 4000. Avoid using an already occupied VLAN ID to prevent network conflicts.
- **AP Isolation:** It is used to isolate guest network clients into separate segments so they cannot communicate with other devices on the same network.
- **WAN Access Control:** WAN Access Control manages local subnet access to WAN-side networks, including the internet and other WAN subnets.

Three WAN access control modes are available:

- **Unrestricted:** Allows this subnet to access the internet and other WAN-side subnets without restrictions.

- **Block WAN Subnet:** Blocks access to other WAN-side subnets. Internet access remains available.
- **Block Internet Access:** Blocks all outbound access, including the internet and WAN-side subnets.

DHCP Server

When enabled, the DHCP server automatically assigns IP addresses and other communication parameters to each connected client. You can customize the address range if 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

Click **Advanced** for further configuration if 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

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 the Guest network's DHCP.
- **Gateway:** The router component that routes traffic between the guest 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.

Once configured, you can see the new VLAN network appear on the current page, showing the subnet information.

12.3 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.

Ethernet Port page displays all router interfaces. You can view the connection status of each interface, manage Ethernet port roles (WAN or LAN), and view port details such as MAC address, negotiated speed, and current link status. Additionally, you can assign physical interfaces to any subnets you have created.

	PORT 01 SFP+	PORT 02 WAN/LAN1	PORT 03 WAN/LAN2	PORT 04 LAN3	PORT 05 LAN4	PORT 06 LAN5	PORT 07 LAN6	PORT 08 LAN7	PORT 09 LAN8	PORT 10 LAN9
Speed	-	-	-	-	-	-	-	-	-	-
MAC			-	-	-	-	-	-	-	-
VLAN Mode	-	-	Standard							
Native Network	-	-	main (1)							
Allowed VLANs	-	-	-							
Settings	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙

- **Link up:** When the port icon is highlighted in blue, the physical link is active.
- **Link Down:** When the port icon is gray, the physical link is inactive.
- **No Module:** When the SFP+ port icon is light gray, no SFP+ module is detected in the SFP+ slot.
- **Speed:** Negotiated transmission rate of the Ethernet port.
- **MAC:** MAC address of the port.
- **VLAN ID:** The working mode of LAN ports can be set to either Standard or Multiple VLANs mode.
- **Native Network:** Default untagged subnet assigned to the LAN port.

- **Allowed VLANs:** Specifies tagged VLANs permitted to pass through this port under Multiple VLANs mode.
- **Settings:** Click to access the configuration page for each individual port.

12.3.1 SFP+

Flint 4 has a 10G SFP+ port that can operate in either WAN or LAN mode. The port supports multiple types of SFP+ modules and cables for fiber-optic and copper Ethernet connections, including long-distance fiber links, conventional twisted-pair cabling, and advanced PON fiber termination. You can choose optical modules or cables based on your networking requirements.

1. **Optical Transceiver + Fiber Cable**

This solution is intended for long-distance, reliable 10G Ethernet connections. Typical uses include:

- Connecting to an ISP's 10G fiber Ethernet uplink for high-speed residential or commercial broadband access.
- Deploying long-distance indoor or outdoor network links, such as connecting Flint 4 to a remote 10G switch, cabling between floors in a home, or deploying a small-office backbone network.

2. **SFP+ to RJ45 Module (SFP-10G-T)**

The SFP-10G-T module converts the SFP+ slot into a standard RJ45 twisted-pair interface, making it suitable for short-distance 10G networks that use conventional Ethernet cables. Typical applications include connecting Flint 4 to a nearby 10G switch or NAS, adding a 10G RJ45 port without installing fiber, and building a high-speed home or SOHO LAN with existing twisted-pair cabling. This option is suitable for users who need 10G Ethernet but do not have fiber cabling.

3. **PON-ONU SFP+ Stick**

The PON-ONU SFP+ stick provides the functions of an ONU optical modem, allowing Flint 4's SFP+ port to terminate traditional GPON/XGS-PON residential fiber lines directly. This option eliminates the need for a separate external optical modem by combining fiber access and routing in one device. It is intended for advanced, enthusiast-level

deployments, particularly for users who want to reduce the number of devices in their home network and connect the router directly to an ISP's PON fiber line.

Note: For more information about the Flint 4 SFP+ port's connections, please click [here](#).

The **SFP+** section displays the port role (WAN or LAN), Module Status, MAC mode, MAC address, and Connection status.

Port 1: SFP+ Configuration

Module Status

● Not Inserted

Port Mode ⓘ

WAN

LAN

MAC Mode

Factory

MAC Address

Connection status

Link down

Cancel

Apply

- **Module Status:** Indicates SFP+ module detection status with two states: Inserted and Not Inserted.
- **Port Mode:** The current operating mode of the physical WAN port. You can set it to LAN as needed.
- **MAC Mode:** Defaults to Factory Mode. You can switch it to Clone Mode or Random Mode.
- **MAC Address:** The MAC address of the WAN interface.
- **Connection status:** Displays the connection status of the SFP+ module.

12.3.2 WAN

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

Port 2: WAN/LAN1 Configuration ✕

Port Mode ⓘ

WAN

LAN

MAC Mode

Factory ▾

MAC Address

Negotiated Network Port Rate

--

Cancel

Apply

- **Port Mode:** The current operating mode of the physical WAN port. You can set it to LAN as needed.
- **MAC Mode:** Defaults to Factory Mode. You can switch it to Clone Mode or Random Mode.
- **MAC Address:** The MAC address of the WAN interface.
- **Negotiated Network Port Rate:** The negotiated link speed of the WAN interface, displayed only when a valid link is detected.

12.3.3 LAN

The **LAN** section displays the LAN port configuration, including the Ethernet Mode (Standard or Multiple VLANs) for the LAN port, and the negotiated link rate.

1. Standard Mode

Standard Mode allows only one VLAN (Untagged), used for connecting end devices.

Port 4: LAN3 Configuration

Negotiated Network Port Rate

--

Ethernet Mode i

Standard

Multiple VLANs

Access Network

main (1)

▼

Cancel

Apply

- **Negotiated Network Port Rate:** The negotiated link speed of the LAN interface, displayed only when a valid link is detected.
- **Ethernet Mode:** Defaults to Standard Mode.
- **Access Network:** The Access Network allows you to achieve network isolation by assigning LAN ports to different subnets.

2. Multiple VLANs Mode

Multiple VLANs mode allows multiple VLANs (Tagged) on one port, typically for connecting APs or other switches.

Port 4: LAN3 Configuration ✕

Negotiated Network Port Rate --

VLAN Mode ⓘ

Standard

Multiple VLANs

Untagged Traffic Handling ⓘ

main (1) ▼

Allowed Tagged Networks

Select networks ▼

Cancel

Apply

- **Negotiated Network Port Rate:** The negotiated link speed of the LAN interface, displayed only when a valid link is detected.
- **VLAN Mode:** : To switch to Multiple VLANs mode, click the Multiple VLANs tab.
- **Untagged Traffic Handling:** Configure untagged packet handling for the port. You can select to either drop such packets directly or forward them to another subnet as the native PVID network.
- **Allowed Tagged Networks:** Specifies the VLANs allowed to pass through this port in tagged mode. You can select VLAN networks from the list, and only matching traffic will be forwarded.

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

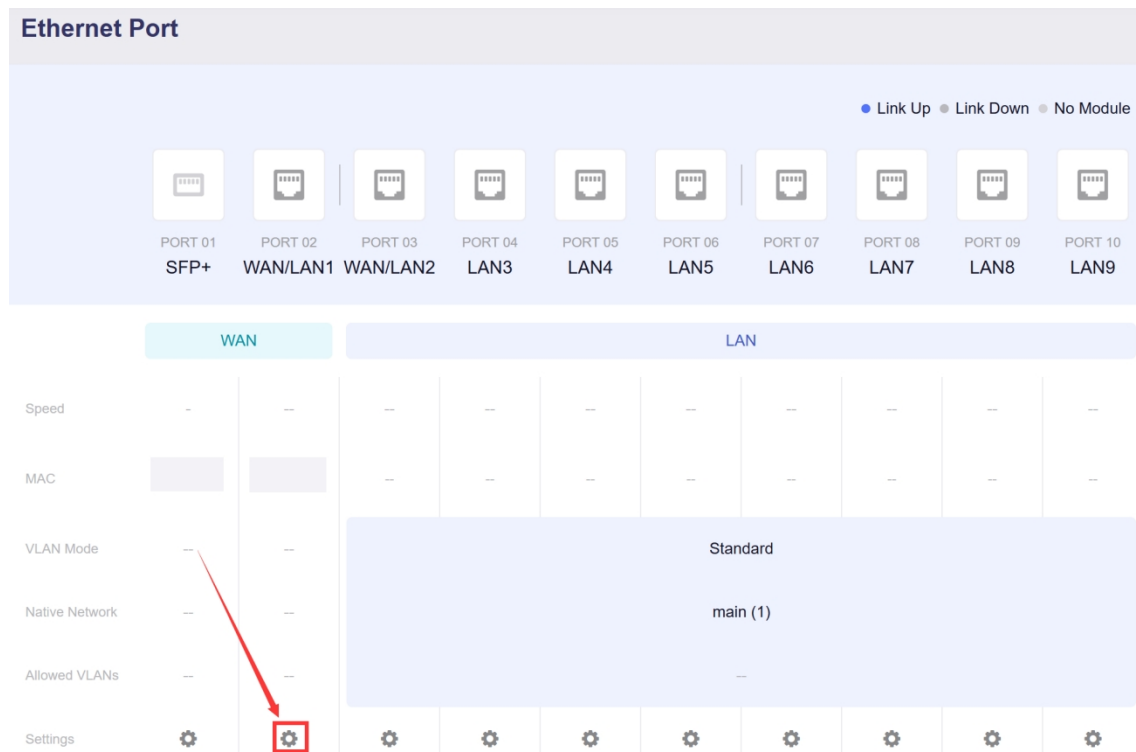
12.3.4 Dual-Ethernet WAN

The Dual-Ethernet WAN feature lets you switch a default LAN Ethernet port to a secondary WAN port for dual Ethernet internet access. It also lets you connect to two independent networks (e.g., work and personal) simultaneously, enhancing flexibility without extra hardware.

The SFP+ port, WAN/LAN1 and WAN/LAN2 of the Flint 4 all support WAN/LAN port role switching. By default, the SFP+ port and WAN/LAN1 are configured as WAN ports. To adjust port roles for dual Ethernet WAN connections, you must first reconfigure one of the default WAN ports as a LAN port.

The following steps demonstrate changing WAN/LAN1 to a LAN port and then setting the WAN/LAN2 as a WAN port, as an example.

1. Switch the WAN/LAN1 to a LAN port. On the Ethernet Port page, click the WAN/LAN1 settings to enter the configuration page.



Ethernet Port

● Link Up ● Link Down ● No Module

PORT 01	PORT 02	PORT 03	PORT 04	PORT 05	PORT 06	PORT 07	PORT 08	PORT 09	PORT 10
SFP+	WAN/LAN1	WAN/LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	LAN8	LAN9
WAN		LAN							
Speed	-	-	-	-	-	-	-	-	-
MAC			-	-	-	-	-	-	-
VLAN Mode	-	-	Standard						
Native Network	-	-	main (1)						
Allowed VLANs	-	-	-						
Settings	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️	⚙️

Switch the port role to LAN and click **Apply**.

Port 2: WAN/LAN1 Configuration

Port Mode

WAN
LAN

Negotiated Network Port Rate
--

Ethernet Mode

Standard
Multiple VLANs

Access Network

main (1)

Cancel

Apply

Return to the Ethernet Port page to verify that the port role has switched to LAN, and the WAN/LAN1 port will then operate as a LAN port.

Ethernet Port

Link Up
Link Down
No Module

PORT 01
SFP+

PORT 02
WAN/LAN1

PORT 03
WAN/LAN2

PORT 04
LAN3

PORT 05
LAN4

PORT 06
LAN5

PORT 07
LAN6

PORT 08
LAN7

PORT 09
LAN8

PORT 10
LAN9

WAN
LAN

Speed	-	--	--	--	--	--	--	--	--	--
MAC		--	--	--	--	--	--	--	--	--
VLAN Mode	--	Standard								
Native Network	--	main (1)								
Allowed VLANs	--	-								
Settings	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙

- Configure the WAN/LAN2 as a WAN. On the Ethernet Port page, click the WAN/LAN2 settings to enter the configuration page.

Ethernet Port

● Link Up ● Link Down ● No Module

PORT 01	PORT 02	PORT 03	PORT 04	PORT 05	PORT 06	PORT 07	PORT 08	PORT 09	PORT 10
SFP+	WAN/LAN1	WAN/LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	LAN8	LAN9
WAN LAN									
Speed	-	-	-	-	-	-	-	-	-
MAC			-	-	-	-	-	-	-
VLAN Mode	-	-	Standard						
Native Network	-	-	main (1)						
Allowed VLANs	-	-	-						
Settings	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙	⚙

Switch the port role to WAN and click **Apply**.

Port 3: WAN/LAN2 Configuration ✕

Port Mode ⓘ WAN LAN

MAC Mode Factory ▾

MAC Address

Negotiated Network Port Rate --

Cancel Apply

- After configuring, return to the Ethernet Port page. You will see that WAN/LAN2 has switched to WAN, and this port will operate as a WAN port.

Ethernet Port

Link Up

Link Down

No Module

PORT 01

SFP+

PORT 02

WAN/LAN1

PORT 03

WAN/LAN2

PORT 04

LAN3

PORT 05

LAN4

PORT 06

LAN5

PORT 07

LAN6

PORT 08

LAN7

PORT 09

LAN8

PORT 10

LAN9

WAN

LAN

WAN

LAN

Speed	-	--	--	--	--	--	--	--	--	--
MAC		--		--	--	--	--	--	--	--
VLAN Mode	--	Standard	--	Standard						
Native Network	--	main (1)	--	main (1)						
Allowed VLANs	--	--	--	--						
Settings										

12.4 DNS

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

Router DNS Server refers to the DNS service built into the router, which provides domain name-to-IP translation for all connected devices. It typically works in two ways: first, it automatically obtains DNS addresses from the upstream network to provide default translation services; second, users can manually configure custom public DNS addresses (e.g., 8.8.8.8) in 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 Ethernet

10.100.23.100
10.100.20.50

DNS from Repeater

10.100.23.100
10.100.20.50

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; disable if your network uses a captive portal (e.g., public Wi-Fi login pages).
- **Override DNS Settings of All Clients:** If enabled, all connected devices will be forced to use the DNS servers configured on the router, ignoring their own original DNS settings. It enables unified DNS configuration for all devices.
- **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.

12.4.1 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 with the 'Mode' dropdown set to '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 in blue), 'DNSCrypt-Proxy', 'DNS over HTTPS', and 'Oblivious DNS over HTTPS'. The 'DNS Provider' field is empty. An 'Apply' button is visible at the bottom of the settings area.

- 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

12.4.2 Edit Hosts

You can define static DNS resolution rules if 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 Ethernet

10.100.23.100
10.100.20.50

DNS from Repeater

10.100.23.100
10.100.20.50

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

12.5 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.

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

IPv6

i 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 (Port Forwarding, GoodCloud, OpenVPN DCO) do not yet support IPv6.

Enable



LAN

Mode	NAT6
DNS acquisition method	Automatic

Apply

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.

12.5.1 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.

12.5.2 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.

12.6 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 if 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

12.7 Network Mode

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

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

Network Mode

 When you change the router's network mode, you may need to reconnect all of your client devices.
When you use Access Point / WDS, 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 NAT, firewall and DHCP server.

☐ **Access Point**
Connect to a wired network and broadcast a wireless network.

☐ **Extender**
Extend the Wi-Fi coverage of an existing wireless network.

☐ **WDS**
Similar to Extender, please choose WDS if your main router supports WDS mode.

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

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

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

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

Note:

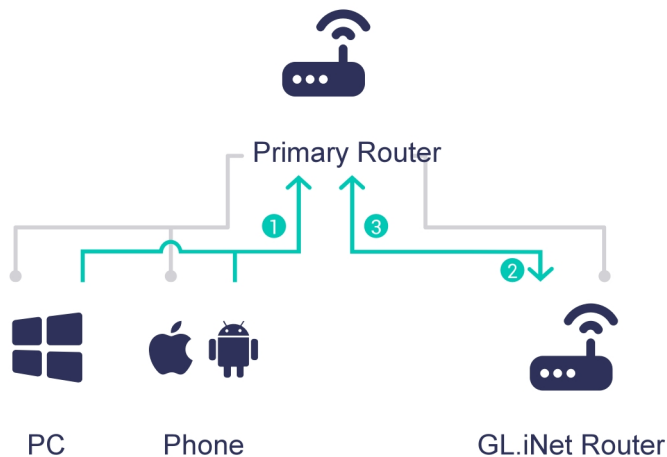
1. When the network mode is changed, all client devices shall reconnect to the router for stable network connectivity.
2. **In Access Point / WDS mode, you will not be able to access the web admin panel using the original IP address.** Instead, you need to log in to the upstream router to find the IP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

12.8 Drop-in Gateway

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

- 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 if needed.



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

- **Gray lines** illustrate the physical connection topology: client devices (e.g., computer, laptop) connect to the primary router, and the primary router's LAN port links to the WAN port of the GL.iNet router (with Drop-in Gateway enabled) via an Ethernet cable.

- **Green lines** depict the sequential data transmission path when Drop-in Gateway is active, with the numbered arrows indicating the traffic flow order:
 1. Traffic from client devices is first routed to the primary router;
 2. The primary router forwards the traffic to the GL.iNet router for processing (e.g., ad filtering, VPN encryption);
 3. After processing, the traffic is sent back to the primary router, which then either delivers the final data to the original client devices or routes it out to the Internet.

You can enable Drop-in Gateway for all or specific devices connected to your primary router. See [this link](#) for more details.

12.9 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 mode between Hardware Acceleration and Software Acceleration.

Network Acceleration

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

i 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

Hardware Acceleration



Apply

- **Hardware Acceleration:** It offloads high-frequency network tasks (e.g., NAT, packet forwarding, checksum verification) to dedicated hardware like NPUs or HWNAT chips. It specifically works on Ethernet 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:** 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.

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

Chapter 13

Flow Control

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

13.1 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.

13.2 Data Statistics

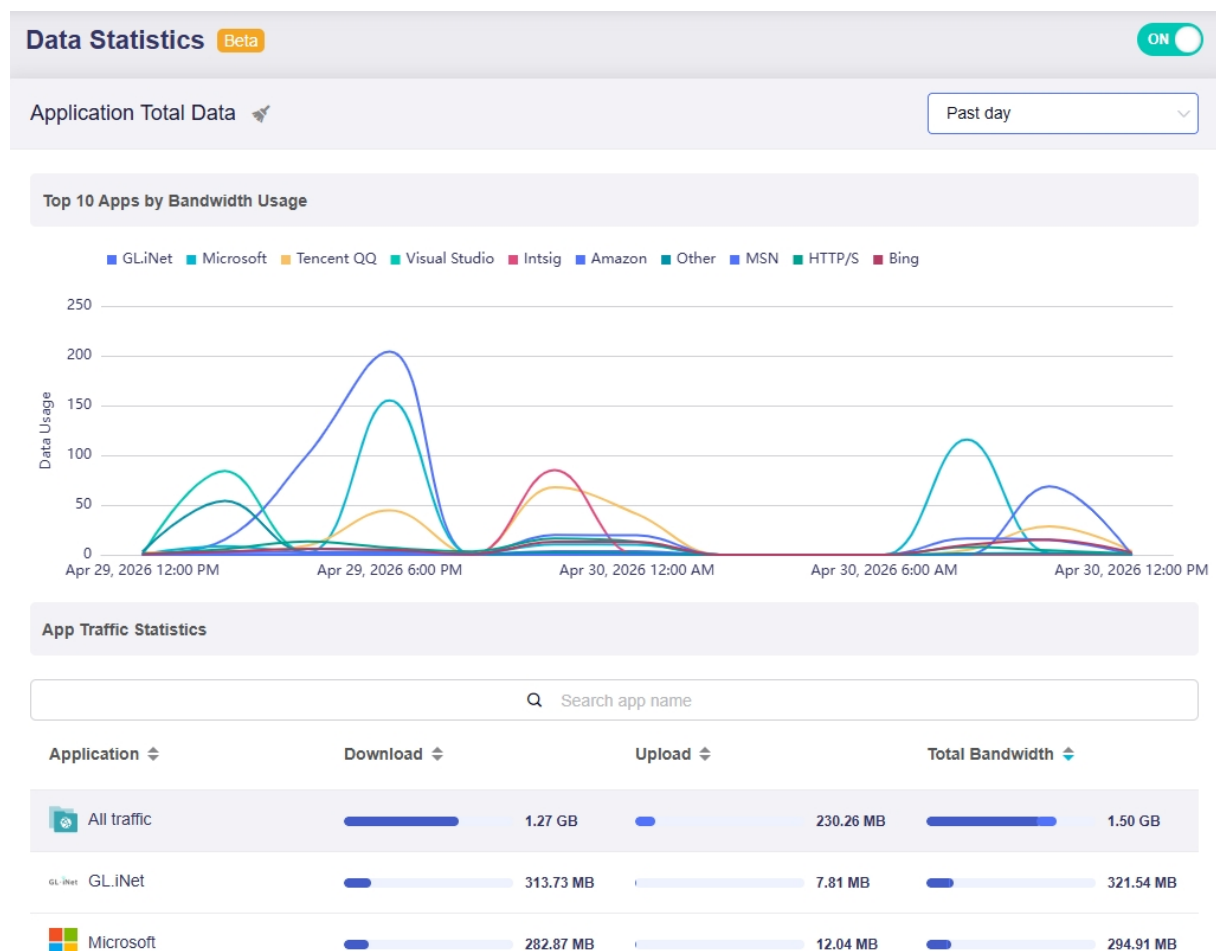
Data Statistics provides an intuitive traffic dashboard that identifies network usage by application and protocol. It supports viewing 1-hour, 1-day, and 7-day historical trends, displays usage rankings, monitors per-device traffic, and allows one-click blocking of unwanted apps.

Note:

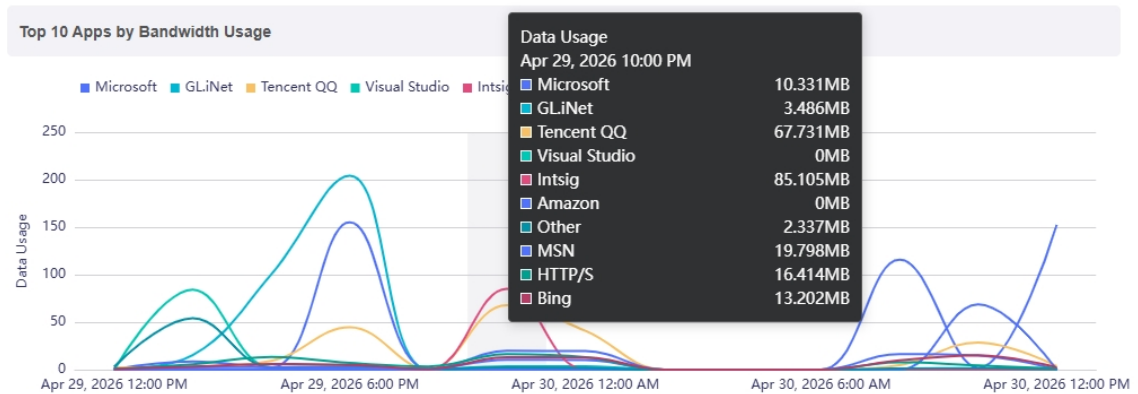
1. Data Statistics will not take effect when the router is in Drop-in Gateway mode.
2. Data Statistics cannot work with Network Acceleration. Enabling Data Statistics will automatically disable Network Acceleration to ensure stable performance.

13.2.1 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.

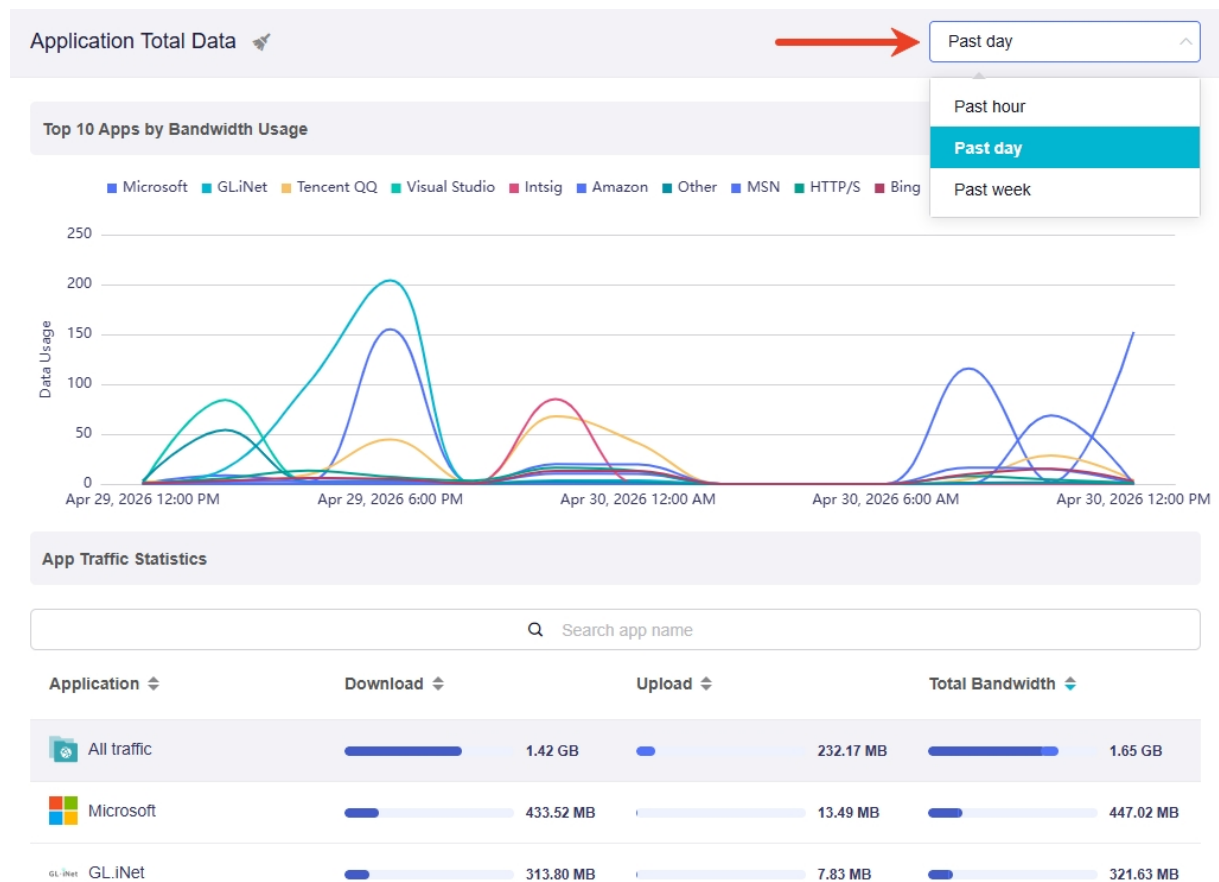
App Traffic Statistics					
Search app name					
Application	Download	Upload	Total Bandwidth		
All traffic	1.42 GB	232.01 MB	1.65 GB		
Microsoft	433.52 MB	13.49 MB	447.01 MB		
GLiNet	313.73 MB	7.82 MB	321.55 MB		
Tencent QQ	155.76 MB	6.57 MB	162.32 MB		
Visual Studio	83.95 MB	4.01 MB	87.96 MB		
Intsig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

13.2.2 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.

13.2.3 Switch Time Range

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



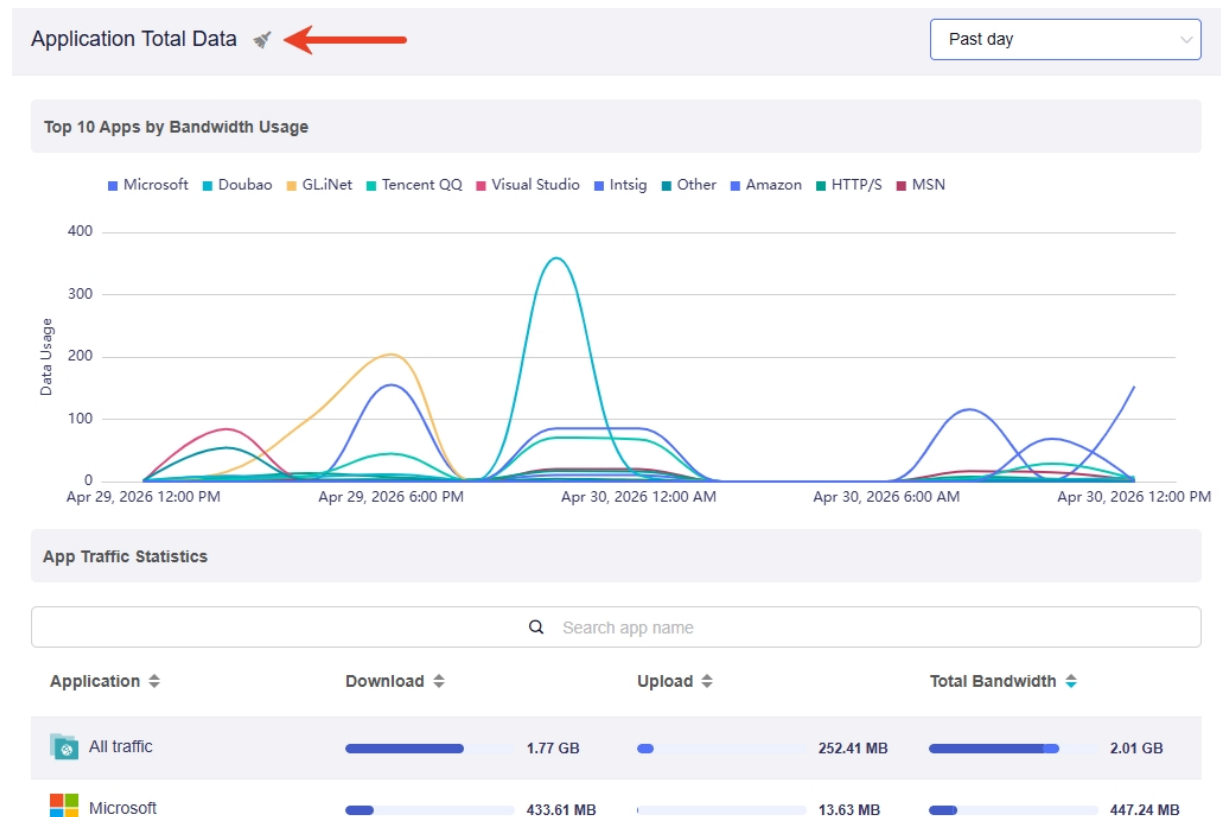
The time range you choose determines how the data is displayed:

- **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.

13.2.4 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.

13.3 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

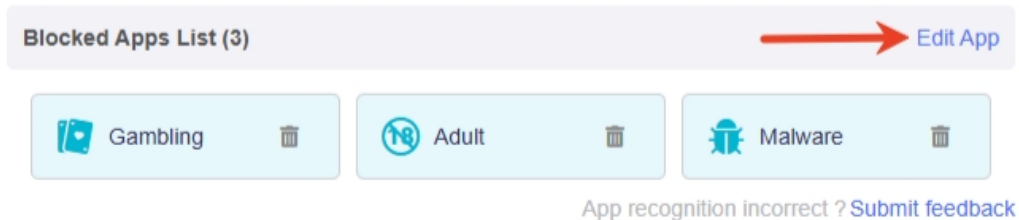
e.g. google.com

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. At the top, there is a header bar with the text 'Blocked Domain / IP List (0)'. Below the header, there is a large text input area. On the left side of the input area, there is a vertical list of numbers, with '1' being the first and most prominent. Inside the input area, there are three lines of placeholder text: '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 text '0/10000'. Below the input area, there is a blue button with the text 'Apply'.

13.4 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

13.5 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.

13.6 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)

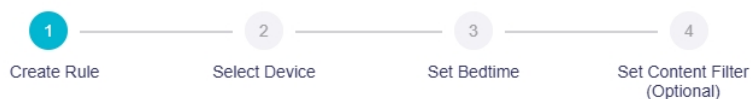
Apply

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.

☐ 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 14

Security

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

14.1 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).

14.1.1 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 if 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

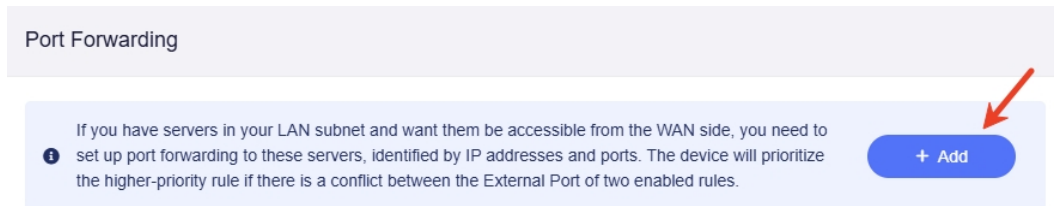
- **Priority:** Set it as Highest or Lowest. If the priority of the DMZ is higher than the port forwarding rules, all port forwarding rules will be invalidated. Otherwise, requests will be forwarded to the DMZ client device only if the accessed port has no corresponding port forwarding rule.
- **DMZ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

14.1.2 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).

Follow the steps below to set up port forwarding if needed.

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	☒

CancelApply

- **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.

14.2 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.

14.3 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.

14.3.1 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

Please install LuCI on the [Advanced Settings](#) before setting the access control for it.

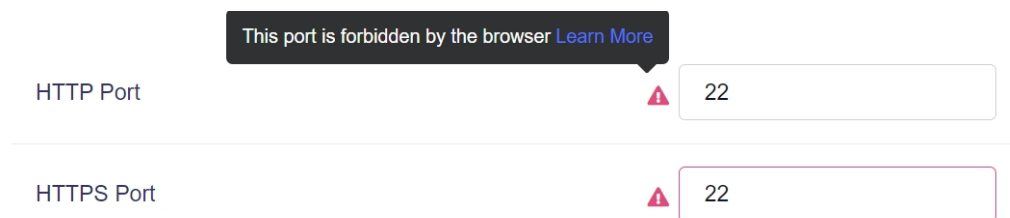
- **HTTP Port:** Defaults to 8080, for unencrypted HTTP access to the LuCI interface.
- **HTTPS Port:** Defaults to 8443, for secure HTTPS access to the LuCI interface.
- **Force HTTPS:** When enabled, access to the LuCI interface is enforced to use a secure HTTPS connection.

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 configuration interface with two input fields. The first field is labeled 'HTTP Port' and contains the value '22'. The second field is labeled 'HTTPS Port' and also contains the value '22'. A dark grey tooltip with a red triangle icon is positioned above the '22' in the 'HTTP Port' field, containing the text 'This port is forbidden by the browser' and a blue link 'Learn More'. The 'HTTPS Port' field also has a red triangle icon to its left.

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.

14.3.2 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

...

14.3.3 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.

14.4 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 15

Applications

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

15.1 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:

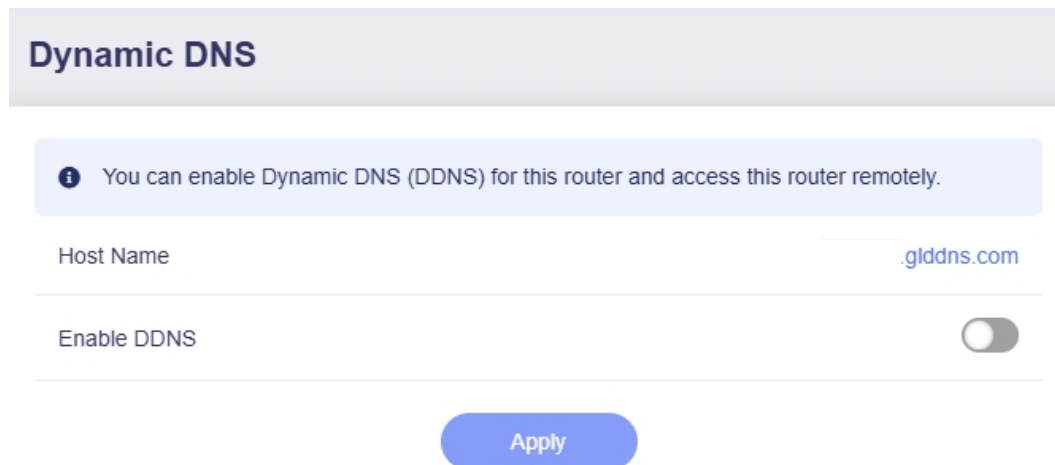
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

15.2 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.

15.2.1 Enable DDNS

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



Dynamic DNS

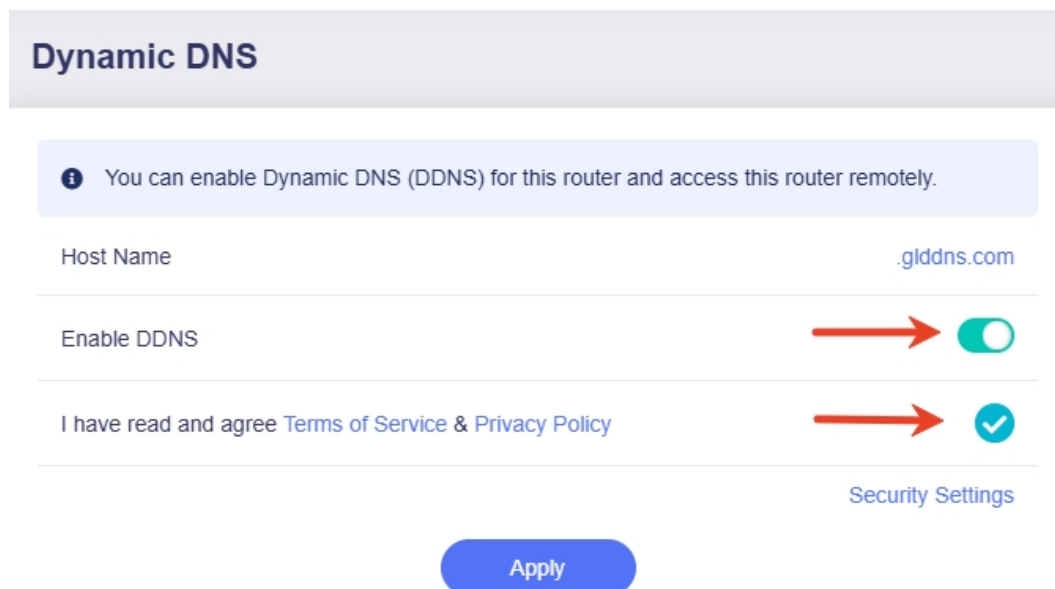
i You can enable Dynamic DNS (DDNS) for this router and access this router remotely.

Host Name .glddns.com

Enable DDNS ☐

Apply

2. Toggle on **Enable DDNS**, read and 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

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](#)

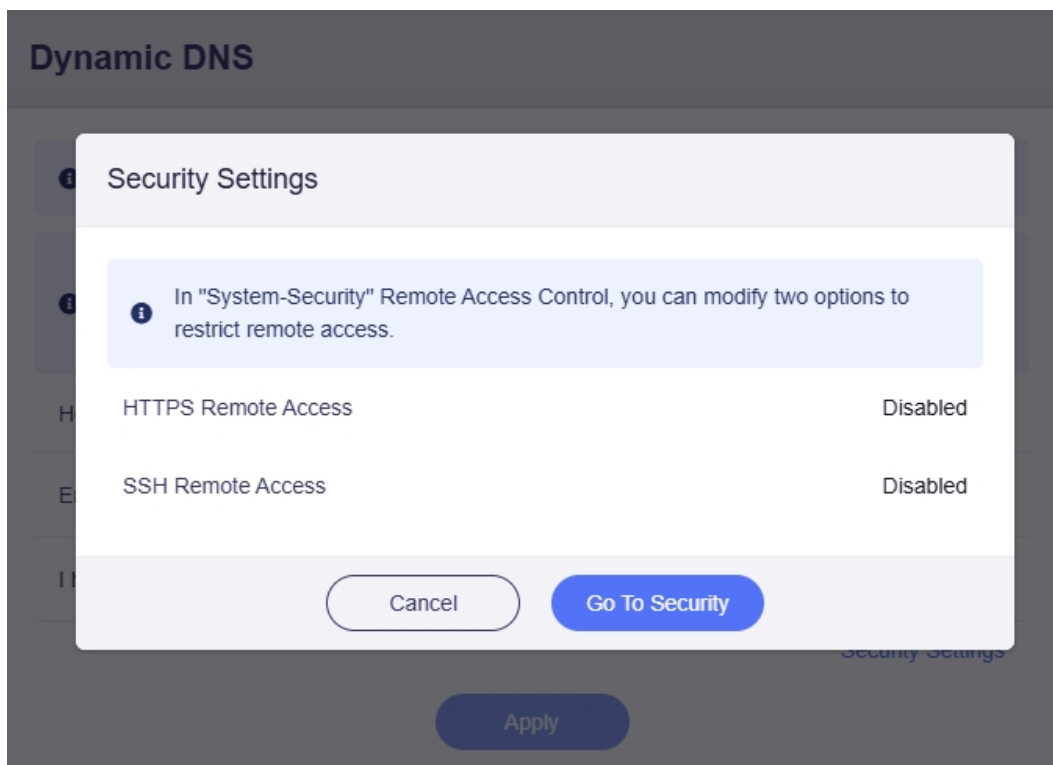
Enable DDNS ☒

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 > Admin Access > 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.

15.2.2 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.

15.2.3 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

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 **SECURITY > Admin Access > Remote Access Control**. Enable **HTTPS Remote Access**, and click **Apply**.

Remote Access Control

Allow Ping from WAN ☐

HTTPS Remote Access  ☒

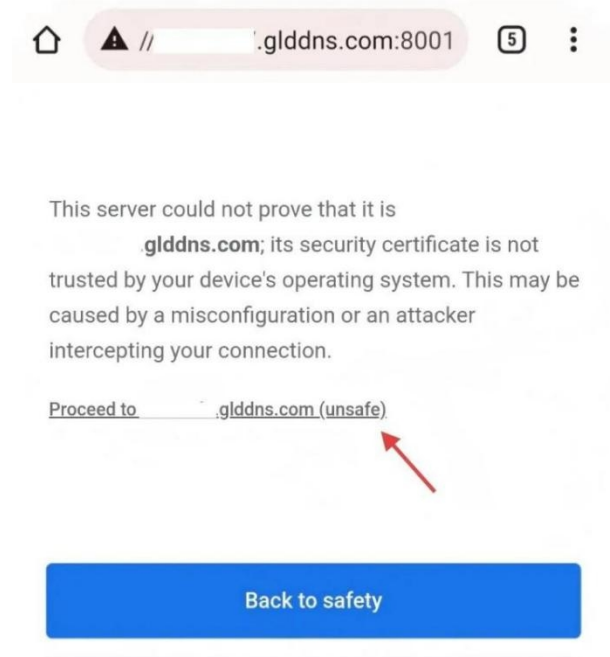
SSH Remote Access ☐

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



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

15.2.4 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

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 **SECURITY > Admin Access > Remote Access Control**. 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).

15.3 Network Storage

Network storage enables wireless 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 Wi-Fi-connected devices.

Flint 4 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 with 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.

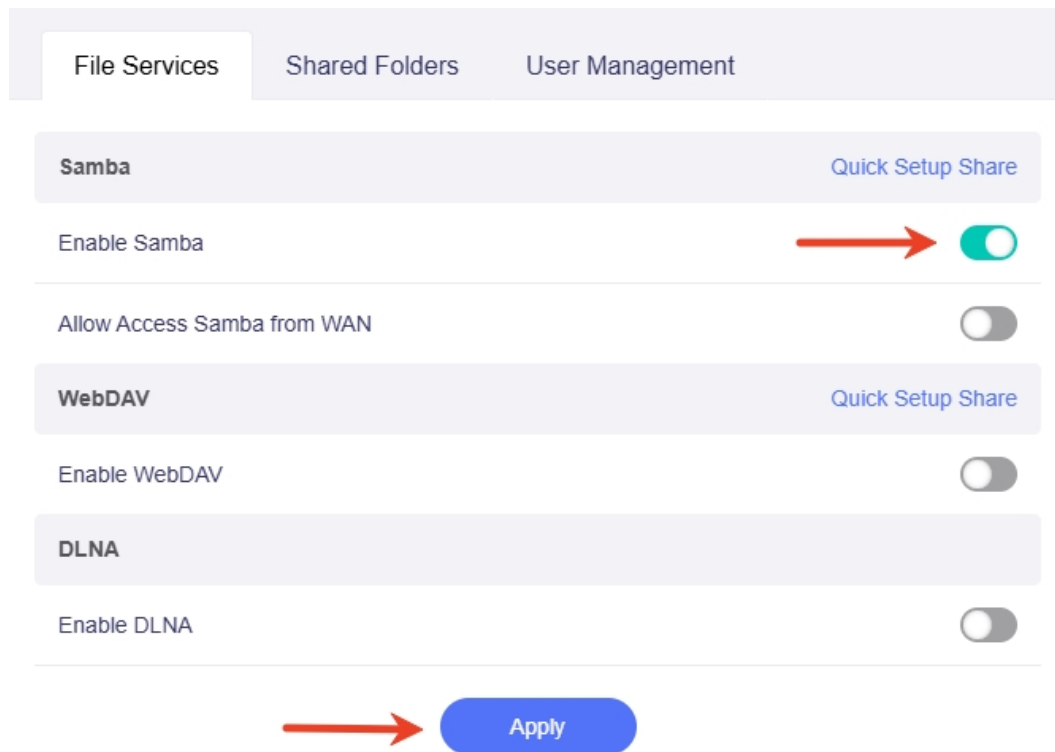
15.3.1 Connect Storage

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	

15.3.2 Set Up Samba

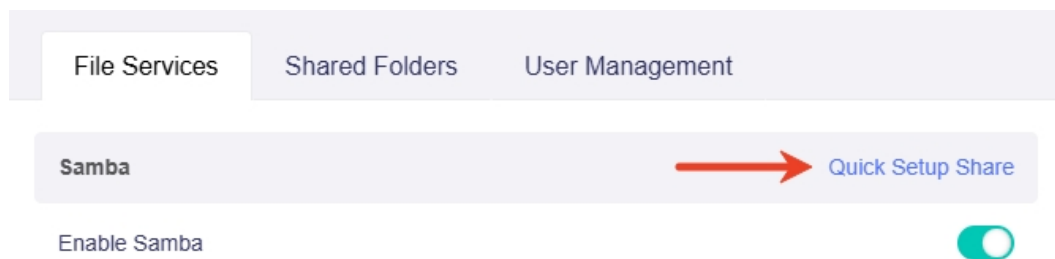
1. In the **File Services** section, toggle on **Enable Samba**, and click **Apply**.



The screenshot shows the 'File Services' tab in a configuration interface. It contains three sections: Samba, WebDAV, and DLNA. Each section has a 'Quick Setup Share' link. The 'Enable Samba' toggle is turned on, indicated by a red arrow. The 'Allow Access Samba from WAN' toggle is turned off. The 'Apply' button at the bottom is highlighted with a red arrow.

File Services	Shared Folders	User Management
Samba Quick Setup Share		
Enable Samba 		
Allow Access Samba from WAN 		
WebDAV Quick Setup Share		
Enable WebDAV 		
DLNA		
Enable DLNA 		
 Apply		

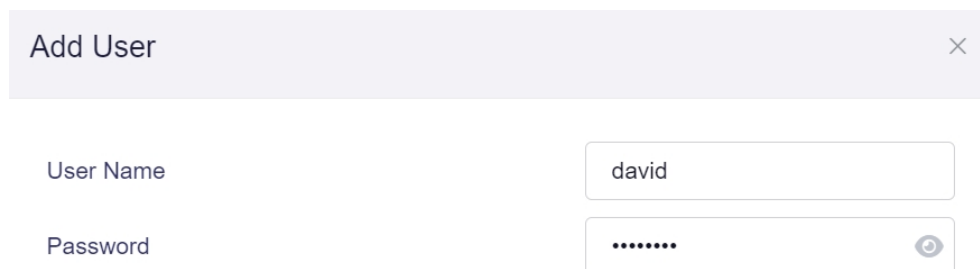
- **Allow Access Samba from WAN:** Enable it if you want upstream devices to access the Samba service.
2. Click **Quick Setup Share** to set the shared link.



The screenshot shows the 'File Services' tab. The 'Samba' section is highlighted, and the 'Quick Setup Share' link is pointed to by a red arrow. The 'Enable Samba' toggle is turned on.

File Services	Shared Folders	User Management
Samba  Quick Setup Share		
Enable Samba 		

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 a close button. Below the title bar, there are two input fields: 'User Name' with the value 'david' and 'Password' with a masked password '.....' and a toggle to show/hide the password.

Add User 	
User Name	david
Password	 

- 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

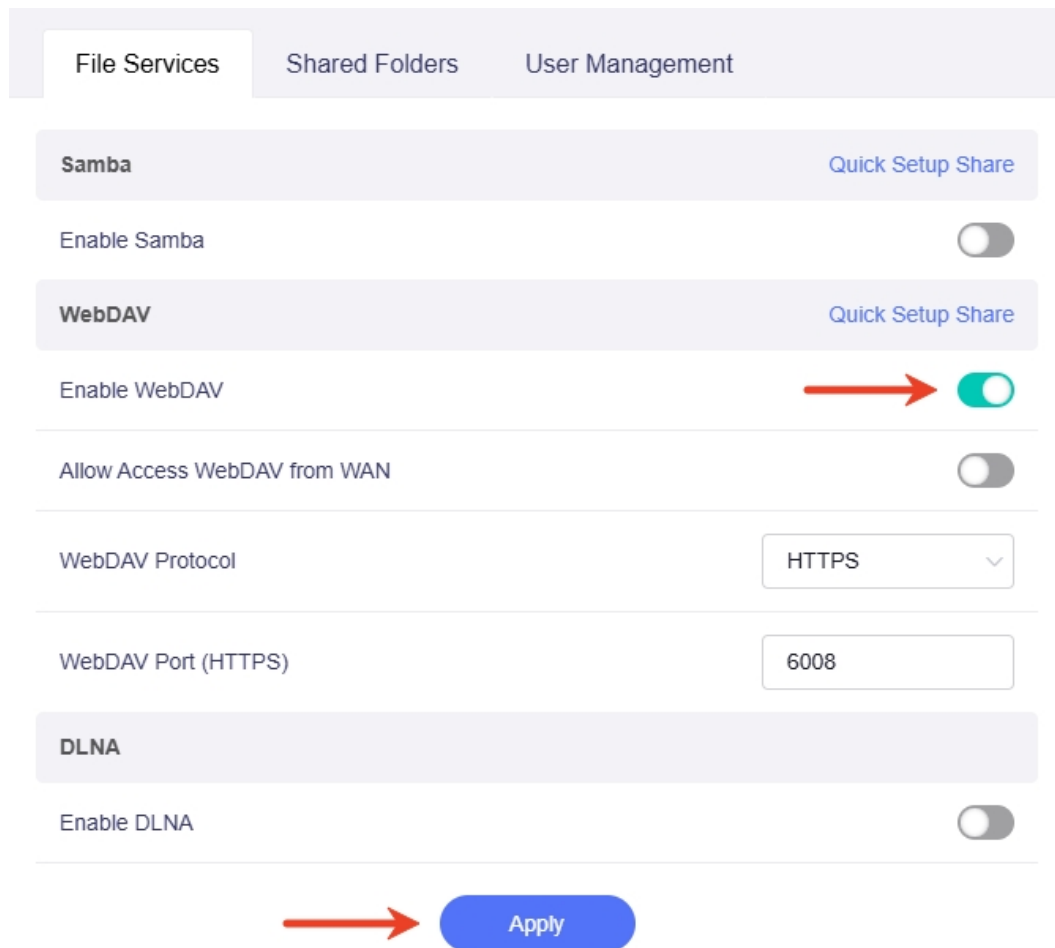
Unix-like Samba

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.

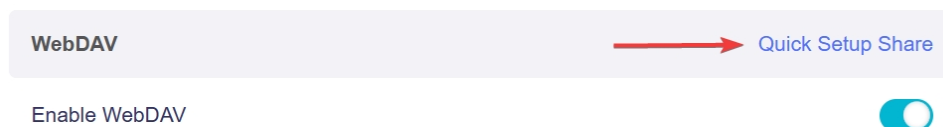
15.3.3 Set Up WebDAV

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' (selected), 'Shared Folders', and 'User Management'. Below the tabs, there are three main sections: Samba, WebDAV, and DLNA. The Samba section has a toggle for 'Enable Samba' which is currently off. The WebDAV section has a toggle for 'Enable WebDAV' which is currently on, with a red arrow pointing to it. Below this toggle is a toggle for 'Allow Access WebDAV from WAN' which is currently off. Further down, there is a dropdown menu for 'WebDAV Protocol' set to 'HTTPS' and a text input field for 'WebDAV Port (HTTPS)' set to '6008'. The DLNA section has a toggle for 'Enable DLNA' which is currently off. At the bottom of the page, 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 blue 'Quick Setup Share' button with a red arrow pointing to it. Below the button, there is a toggle for 'Enable WebDAV' which is currently 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

.....

4. 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

5. 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.

15.3.4 Set Up DLNA

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

The screenshot shows the 'File Services' tab selected in a navigation bar. Below the navigation bar, there are three sections: Samba, WebDAV, and DLNA. Each section has a 'Quick Setup Share' link. The 'Enable Samba' and 'Enable WebDAV' toggles are turned off. 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, a blue 'Apply' button is highlighted with a red arrow.

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

This is a close-up of the DLNA settings section. It shows the 'DLNA' header, the 'Enable DLNA' toggle which is turned on, and the 'Share Path' set to '/disk1_part1' with a 'Modify' link highlighted by a red box.

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

15.4 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

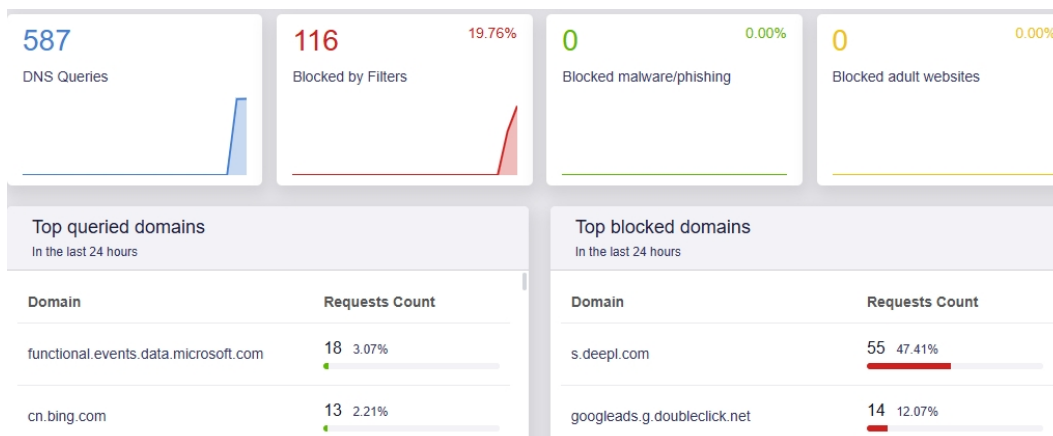
AdGuard Home is network-wide software that blocks ads and tracking. Once set up, it will cover ALL the devices on your home network, there is no need for any additional client-side software. This page gets statistics through the API provided by AdGuard Home. When AdGuard Home is enabled, the router will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

Enable AdGuard Home ☒

AdGuard Home Handle Client Requests ☐

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.



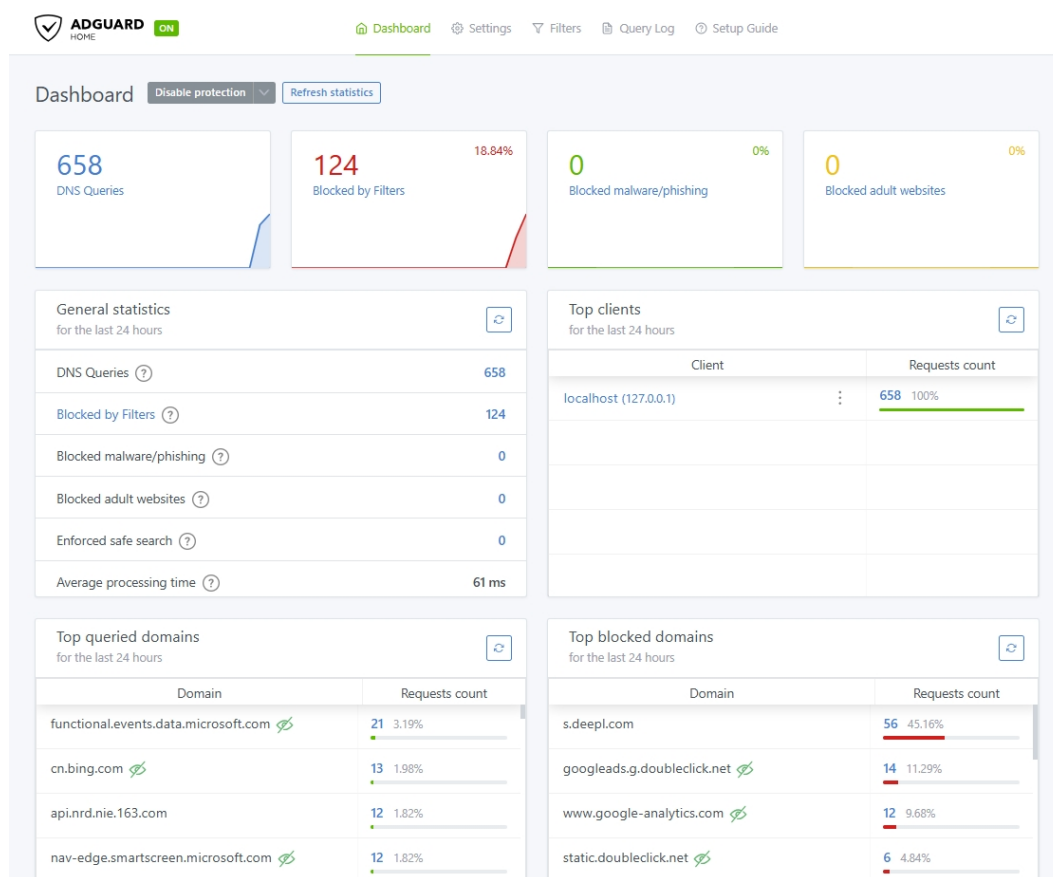
3. Click **Settings Page** to configure advanced settings for AdGuard Home.

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.



15.5 Bark

The [Bark](#) service can help protect your child's digital world and provide comprehensive online protection. It typically requires a paid subscription. However, as part of our partnership with Bark, GL.iNet offers the Bark Home plan for free **on select router models including Flint 4**, providing advanced monitoring and alerts at no extra cost.

Note:

1. The Bark service is available **only in the United States, Australia, and South Africa**. Click [here](#) for details.
2. Bark and GL.iNet Parental Control cannot be enabled simultaneously, as this may trigger conflicts.

Follow these steps to use Bark service if needed.

1. Log in to the router's web admin panel and navigate to **APPLICATIONS > Bark**. Toggle the switch to enable Bark, then click **Apply**.

Bark

Bark's award-winning service can help protect your child's digital world and provide comprehensive online protection. Depending on the subscription you choose (Bark or BarkJr), you'll be able to:

- Set parental controls on all of the internet-connected devices in your home.
- Set daily bedtimes and school times on all your child's devices to limit online distractions
- Choose which websites and apps are allowed/blocked on all devices

Visit [bark.us](#) to learn more and free to use forever.

Please note: Bark's service may not be available in certain countries. As GL.iNet is not the provider of this service, should you encounter any issues using Bark kindly reach out directly to [Bark's Technical Support](#) for assistance.

Enable



Enable IPv6



Apply

- Next, pair your device with your Bark account. Click **Device Pairing Link** to pair this router with your Bark account.

Bark

Bark's award-winning service can help protect your child's digital world and provide comprehensive online protection. Depending on the subscription you choose (Bark or BarkJr), you'll be able to:

- Set parental controls on all of the internet-connected devices in your home.
- Set daily bedtimes and school times on all your child's devices to limit online distractions
- Choose which websites and apps are allowed/blocked on all devices

Visit [bark.us](#) to learn more and free to use forever.

Please note: Bark's service may not be available in certain countries. As GL.iNet is not the provider of this service, should you encounter any issues using Bark kindly reach out directly to [Bark's Technical Support](#) for assistance.

The Bark service is enabled, but this device is not yet paired with any account. Please use the [Device Pairing Link](#) to pair this device with your Bark account.

Enable



- You will be redirected to the Bark website. Follow the on-screen instructions to log in, pair your device, create a profile and finish the initial setup.
- Once your device connects to Bark Cloud services and is paired with your account, the router's web Admin Panel will show a hyperlink. Click **Go to Bark** to log in to the Bark dashboard and set up your parental control rules.

The device is connected to Bark Cloud Services and paired with an account. Please [Go to Bark](#) and log in to the paired account to control access.

Enable



Enable IPv6



Pairing Code

93

[Re-pair](#)

Note: Since GL.iNet is not the provider of this service, should you encounter any issues while using Bark, kindly reach out directly to [Bark's Technical Support](#) for assistance.

15.6 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.

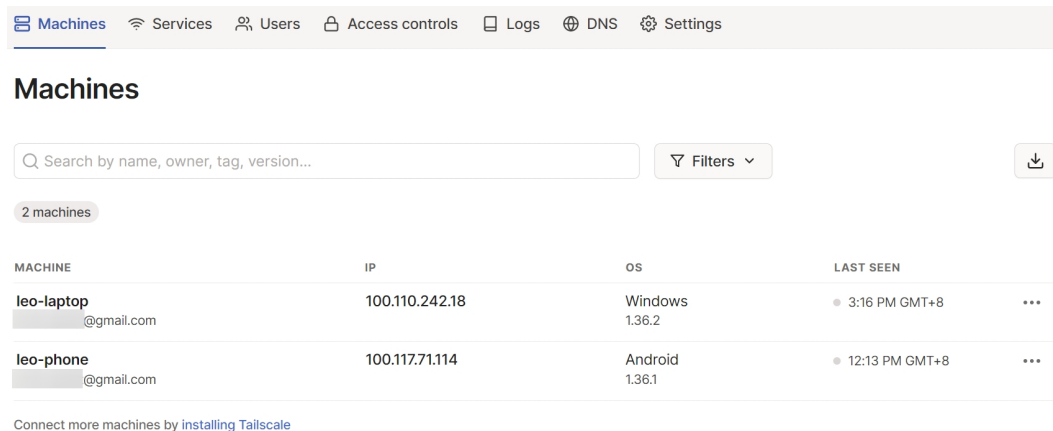
Note:

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.

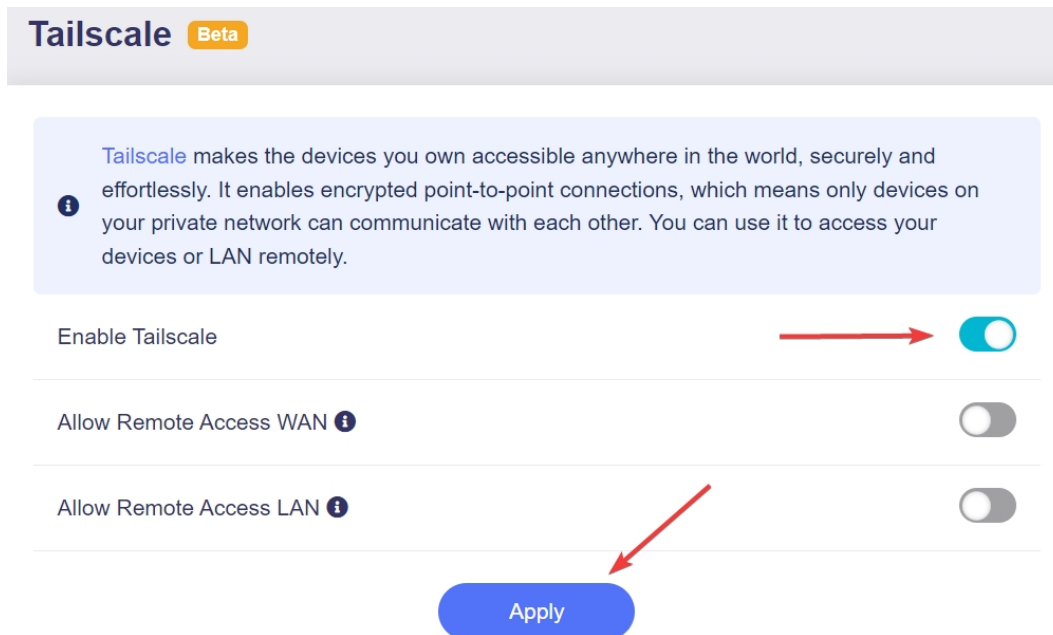
15.6.1 Set Up Tailscale

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

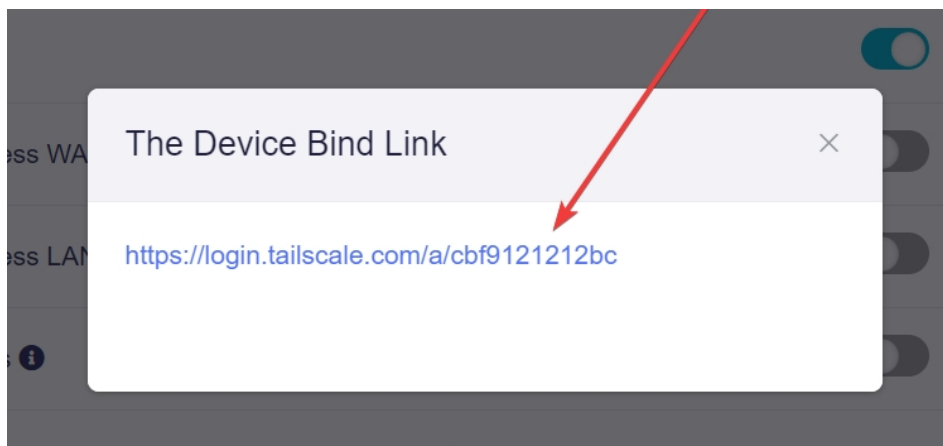
i Tailscale makes the devices you own accessible anywhere in the world, securely and effortlessly. It enables encrypted point-to-point connections, which means only devices on your private network can communicate with each other. You can use it to access your devices or LAN remotely.

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**.



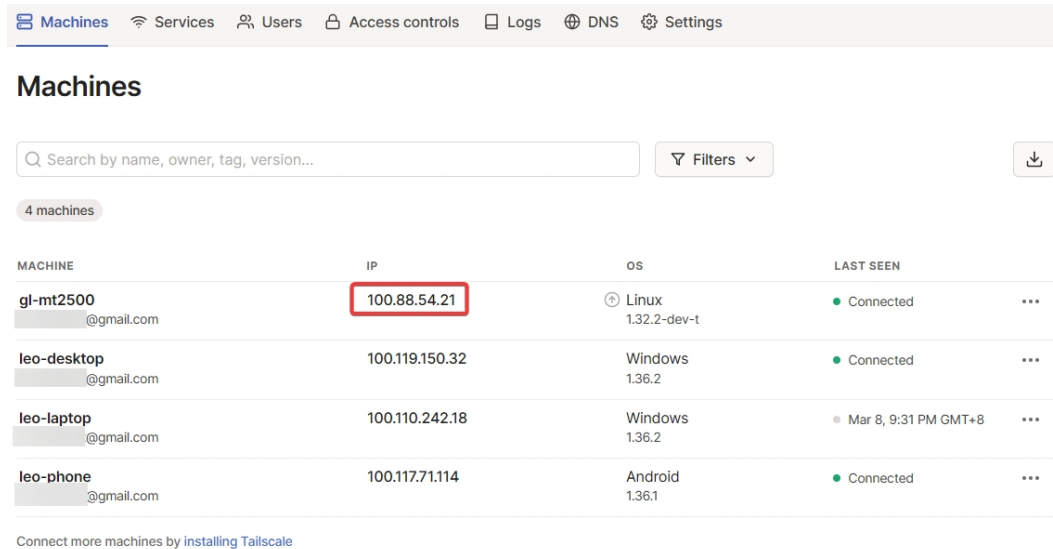
Connect device

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

- 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](#)

- 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.

15.6.2 Advertise WAN Subnets

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 ☒

Bind Account _____@gmail.com [Unbind](#)

Router Virtual IP **i** 100.113.50.89

Exit Node

Custom Exit Node ☐

Run Exit Node **i** ☐

Subnet Routes

Advertise WAN Subnets **i** ☒

Advertise LAN Subnets **i** ☐

NAT

IP Masquerading **i** ☐

Apply

15.4.3 Advertise LAN Subnets

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



Bind Account

@gmail.com [Unbind](#)

Router Virtual IP **i**

100.113.50.89

Exit Node

Custom Exit Node



Run Exit Node **i**



Subnet Routes

Advertise WAN Subnets **i**



Advertise LAN Subnets **i**



NAT

IP Masquerading **i**

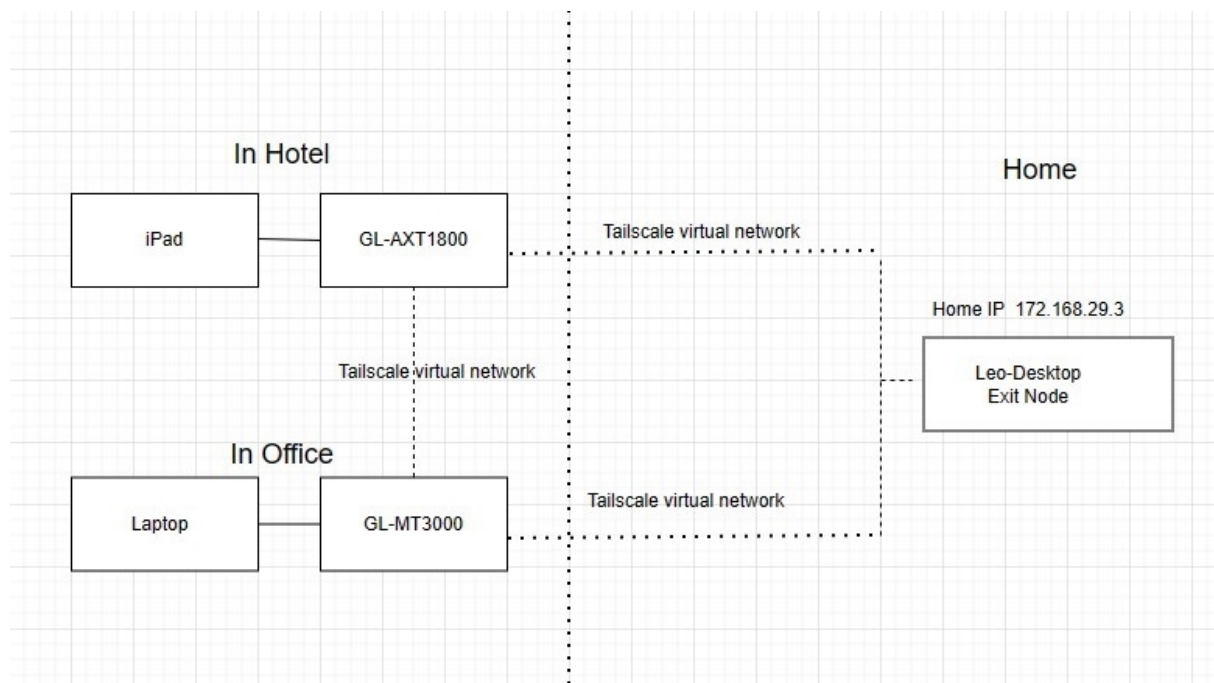


Apply

15.6.4 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.



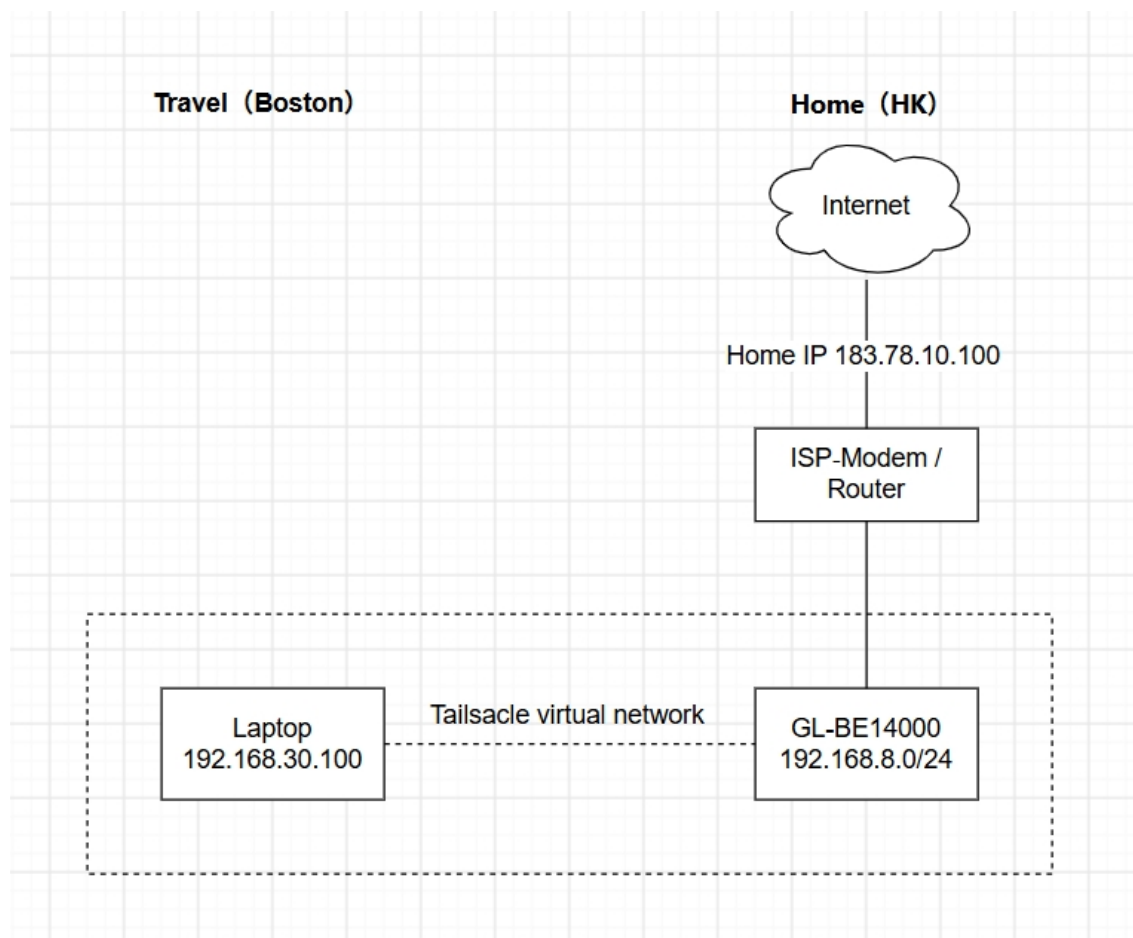
In summary, an Exit node routes outbound Internet traffic from your Tailnet devices, effectively acting as VPN servers. When connected to an Exit node, all your non-Tailscale Internet traffic appears to originate from its location, helping you access geo-restricted content and enhance your online privacy.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

15.6.5 Run Exit Node

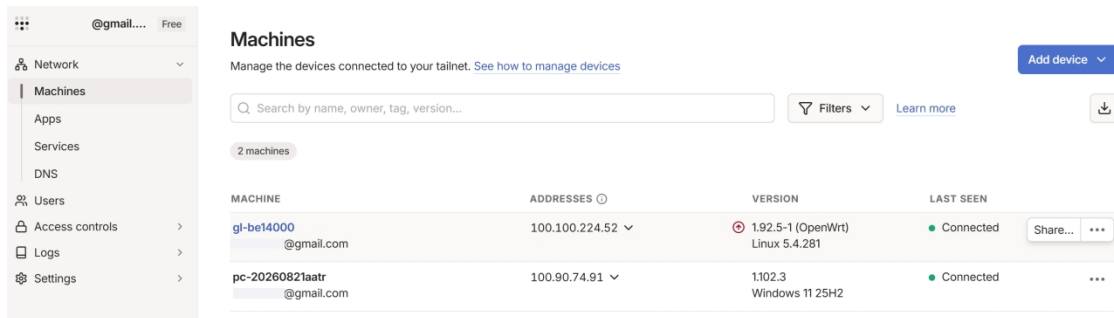
Running an exit node on your router allows other devices within your tailnet to route all outbound internet traffic via this router's public IP.

In the topology below, a laptop is in Boston, while a router GL-BE14000 is in Hong Kong. Both have been added into the same Tailscale network. If you set the GL-BE14000 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.

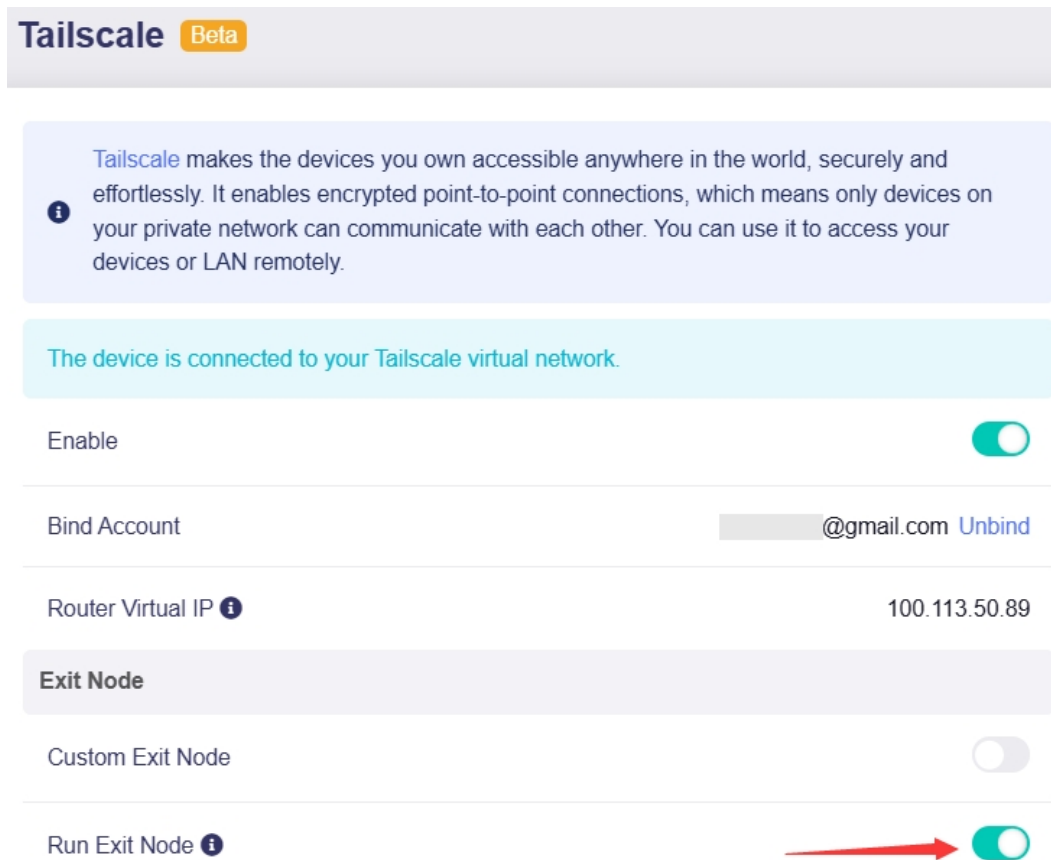


Here are the steps to set the GL-BE14000 as an Exit Node.

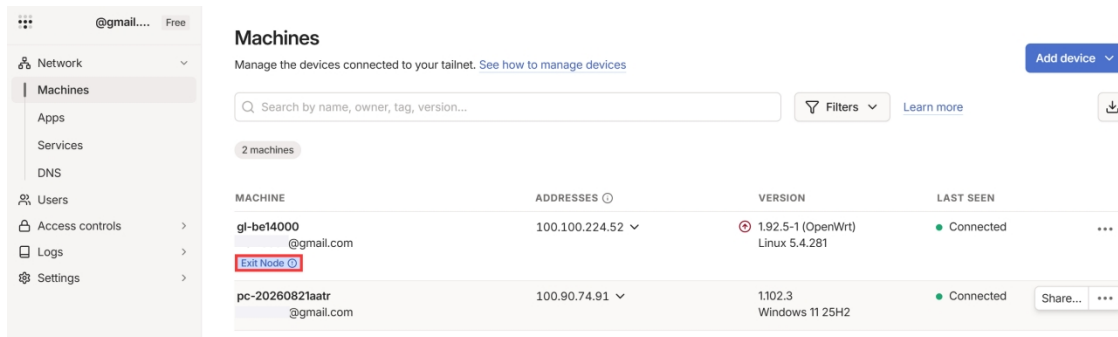
1. Enroll both the router GL-BE14000 and travel laptop to the same Tailscale tailnet.



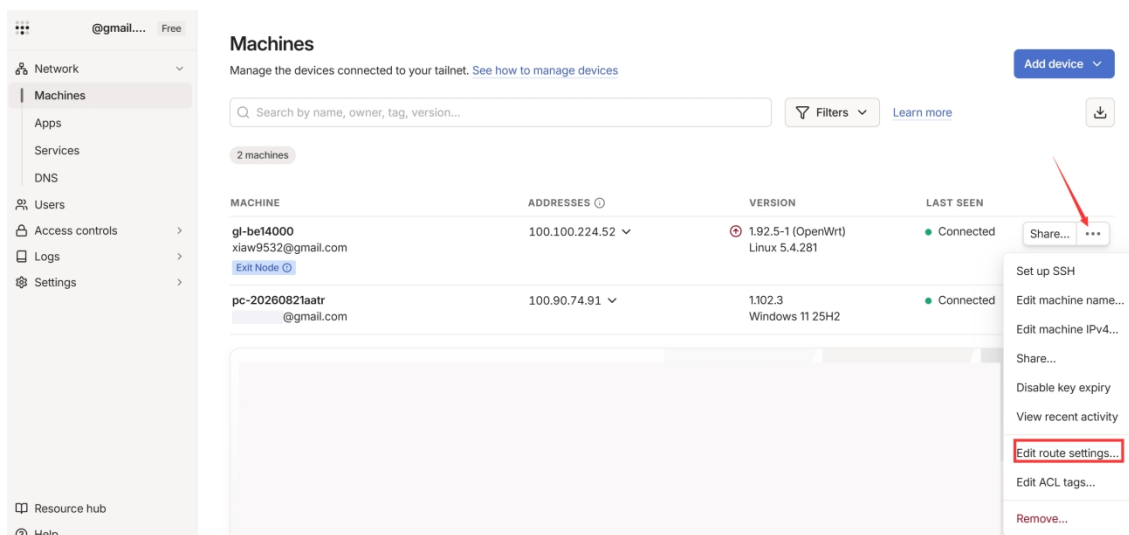
- In the GL-BE14000 web Admin Panel, go to **APPLICATIONS > Tailscale**. enable **Run Exit Node** and click **Apply**.



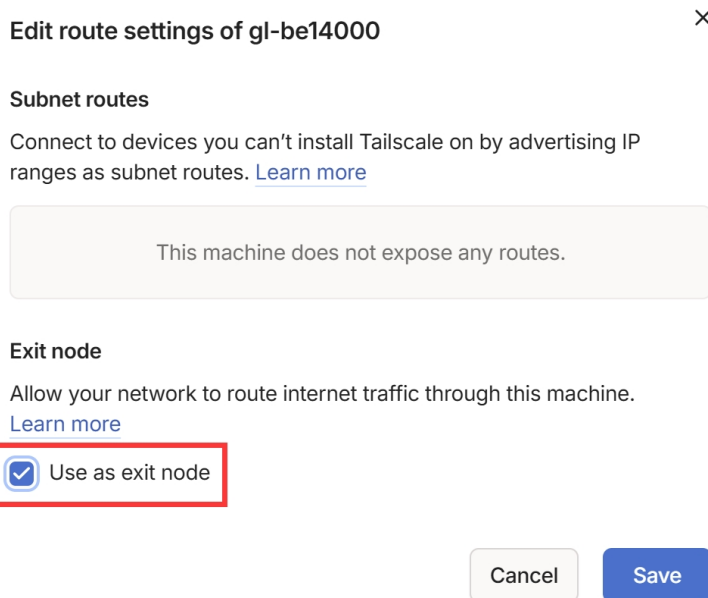
- Go to the Tailscale Admin Console, and you will see a tag "Exit Node" under the GL-BE14000.



- Click the three-dot icon on the right of GL-BE14000 and select **Edit route settings**.

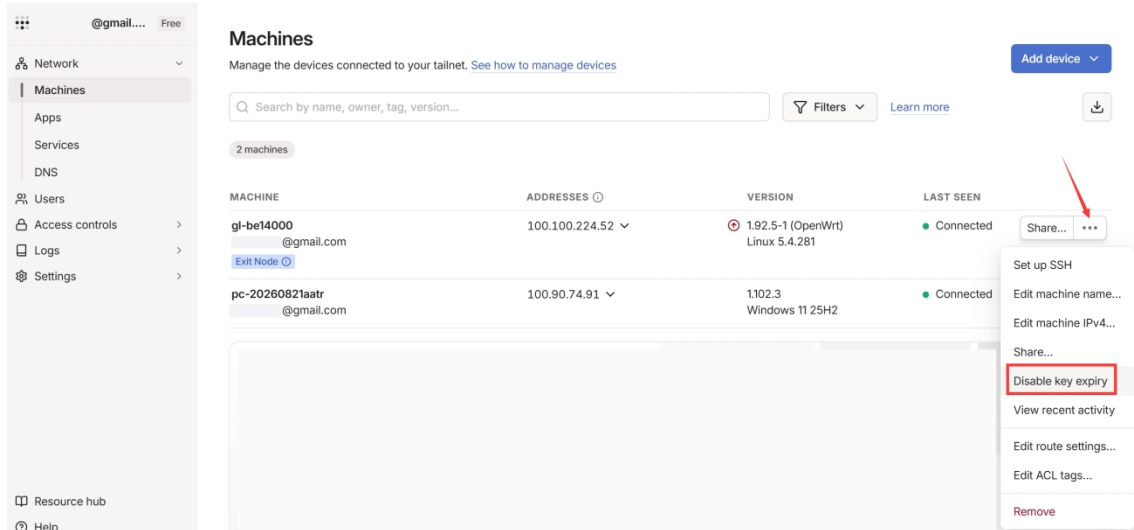


- In the pop-up window, check **Use as exit node** and click **Save**.

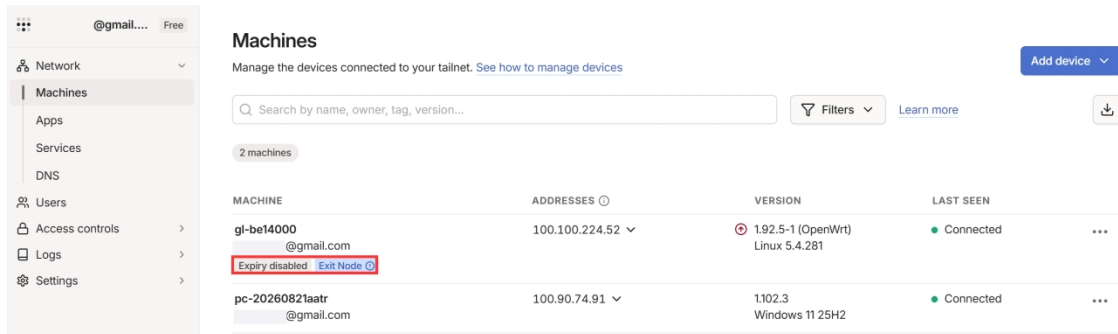


- Disable key expiry.

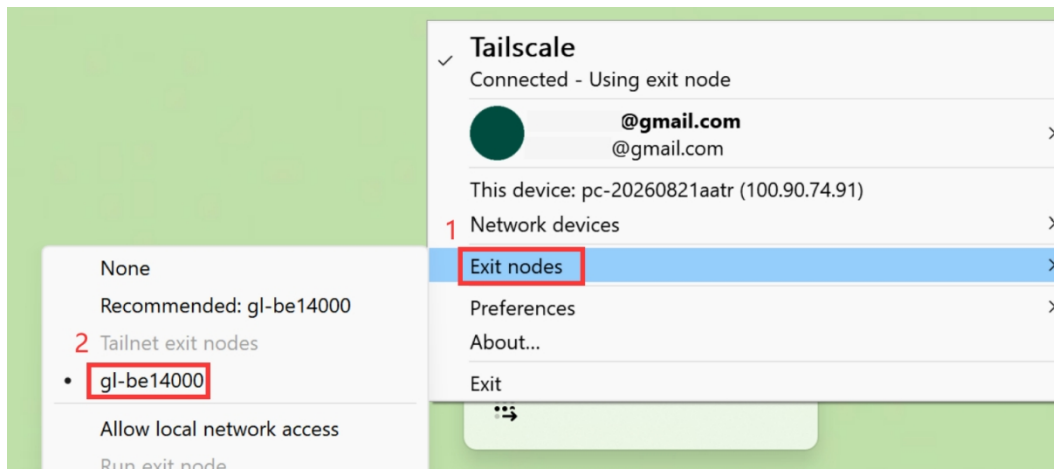
As a security feature, users need to periodically re-authenticate on each of their devices. To avoid disconnections when the exit node authentication key expires, we recommend disabling key expiry for your exit node. Click [here](#) for more details about key expiry. Click the three-dot icon on the right of GL-BE14000 and select Disable key expiry.



Once applied, a tag "Expiry disabled" will appear under the GL-BE14000.



7. 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-be14000**.



Now, all outbound traffic from this travel laptop will exit through GL-BE14000 to access the internet.

8. 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-BE14000 located in Hong Kong, in this example).

1 IP Source: IPCheck.ing IPv4

183.178.10.100

Region

State

City

Hong Kong SAR

Kwai Tsing District

Kwai Chung

Time Zone

ISP

Asia/Hong_Kong +08:00

Hong Kong Broadband Network Limited

To avoid abuse, sign in to view the following information

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\system32\cmd.exe
Microsoft Windows [Version 10.0.26200.9168]
(c) Microsoft Corporation. All rights reserved.

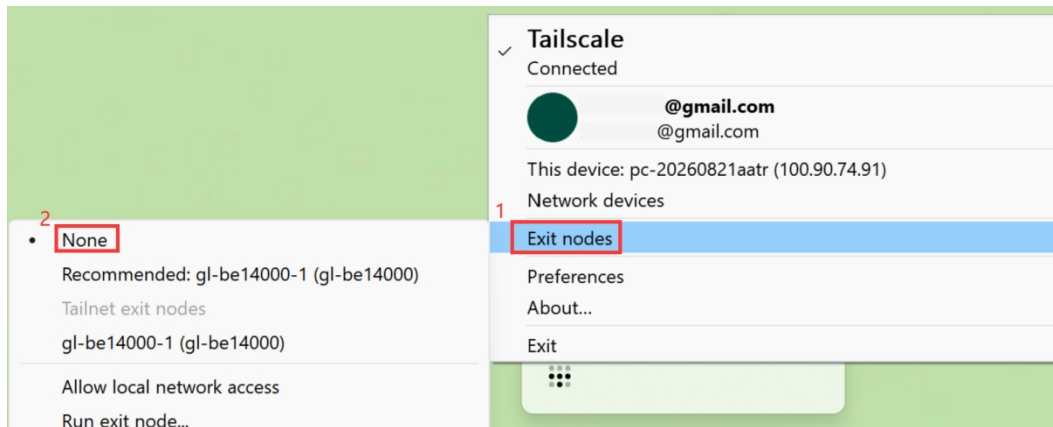
C:\Users\Administrator>tracert google.com

Tracing route to google.com [217.160.0.201]
over a maximum of 30 hops:

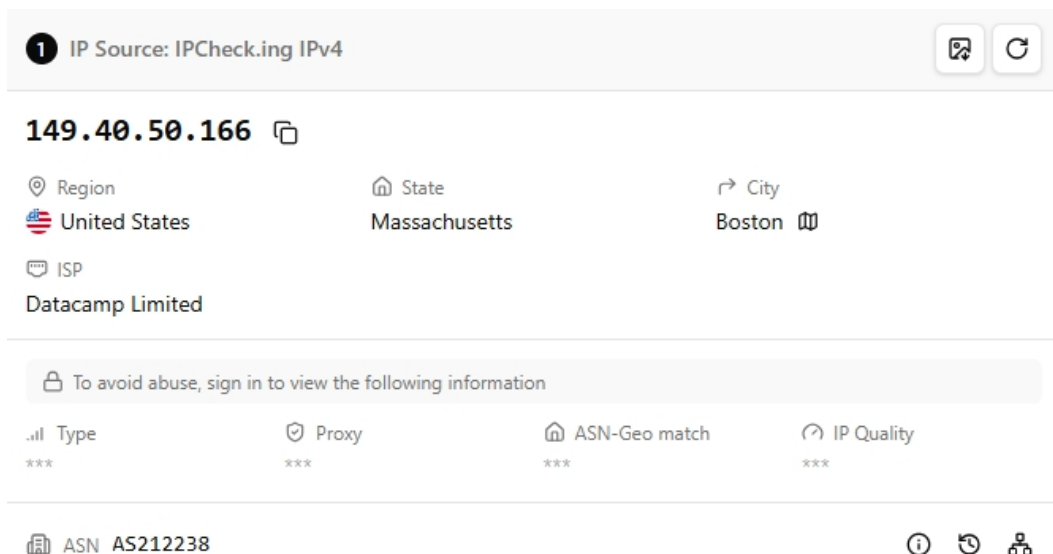
  1  6 ms    3 ms    4 ms    gl-be14000.taile18dc6.ts.net [100.81.20.59]
  2  9 ms    4 ms    3 ms    10
  3  5 ms    6 ms    3 ms    10
  4  6 ms    3 ms    2 ms    19
  5  9 ms    9 ms    8 ms    44
  6  22 ms   14 ms   13 ms   10
  7  21 ms   16 ms   17 ms   44
  8  18 ms   18 ms   21 ms   19
  9  20 ms   21 ms   18 ms   18
 10  43 ms   26 ms   32 ms   20
 11  28 ms   21 ms   22 ms   20
 12  32 ms   20 ms   25 ms   06
 13  213 ms  214 ms  215 ms   li
 14  300 ms  299 ms  298 ms   ae
 15  303 ms  319 ms  322 ms   lo
 16  231 ms  229 ms  233 ms   lo
 17  233 ms  235 ms  233 ms   lo
 18  234 ms  253 ms  235 ms   21

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).



15.7 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:

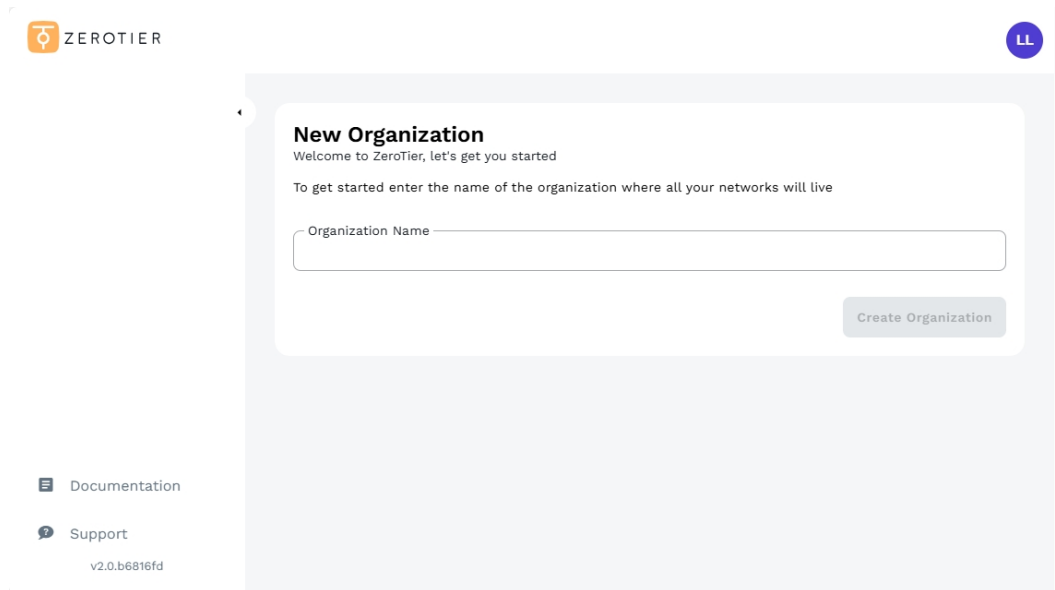
1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale, and AstroWarp.
2. This feature is currently in beta, and may have some bugs.

15.7.1 Set Up ZeroTier

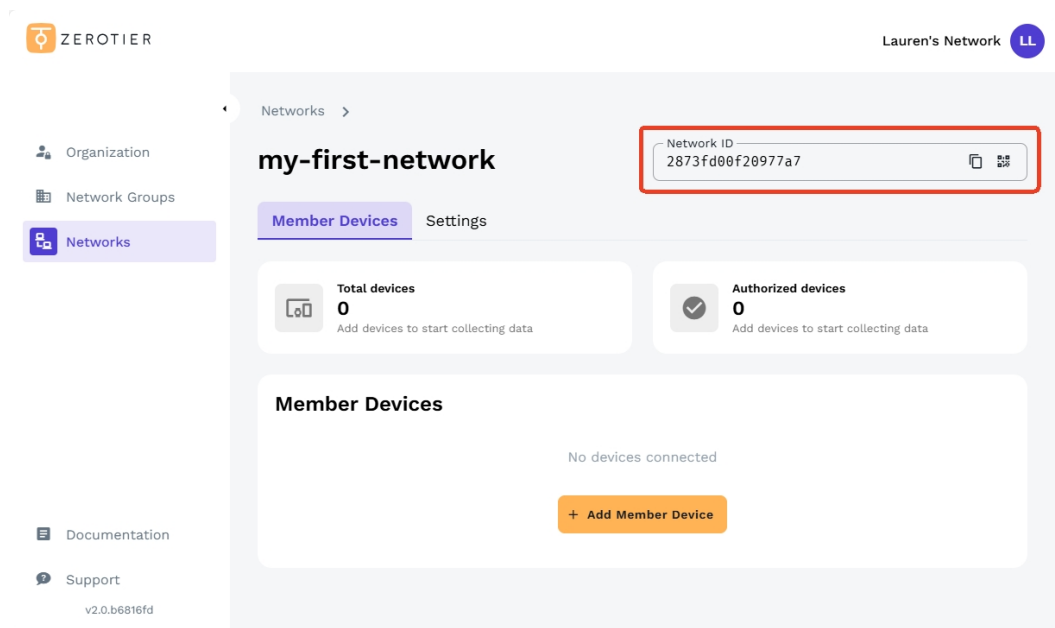
Two versions of ZeroTier Central are available: New Central and Legacy Central.

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: 'ZeroTier creates a secure, virtual peer to peer Ethernet network accessible from anywhere; it supports access to devices such as phones, PCs etc. You can use it to access your devices or LAN remotely.' Another light blue box below explains: 'ZeroTier connects to your virtual network using the Network ID, that you create on ZeroTier Central.' The settings section includes three toggle switches: 'Enable ZeroTier' (turned on, with a red arrow pointing to it), 'Allow Remote Access WAN' (turned off), and 'Allow Remote Access LAN' (turned off). Below these is the 'Network ID' field, which contains the value '2873fd00f20977a7' (with a red arrow pointing to it). At the bottom is a blue 'Apply' button (with a red arrow pointing to it).

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

This screenshot shows the ZeroTier configuration page after the settings have been applied. The 'Enable ZeroTier' toggle is now turned on. A yellow warning box with an exclamation mark icon contains the 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 from this message to the 'ZeroTier Central' link. The 'Network ID' field and the 'Apply' button are still visible at the bottom.

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 and a red arrow pointing to the "Authorize" button. Below this, the "Total devices" is 1 and "Authorized devices" is 0. The "Member Devices" table shows one device with ID "eb618be42d" and status "Not Authorized".

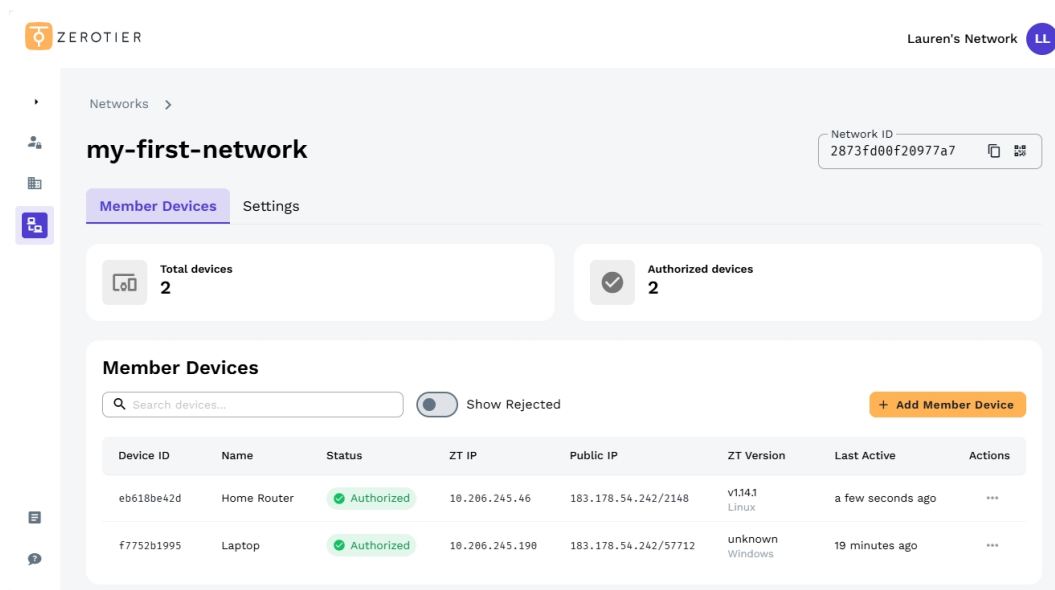
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Not Authorized		183.178.54.242/30149	unknown Linux	a few seconds ago	...

Once authorized, the page displays as follows.

The screenshot shows the ZeroTier web interface after the device has been authorized. The "Authorized devices" count is now 1. The "Member Devices" table shows the device with ID "eb618be42d" and status "Authorized".

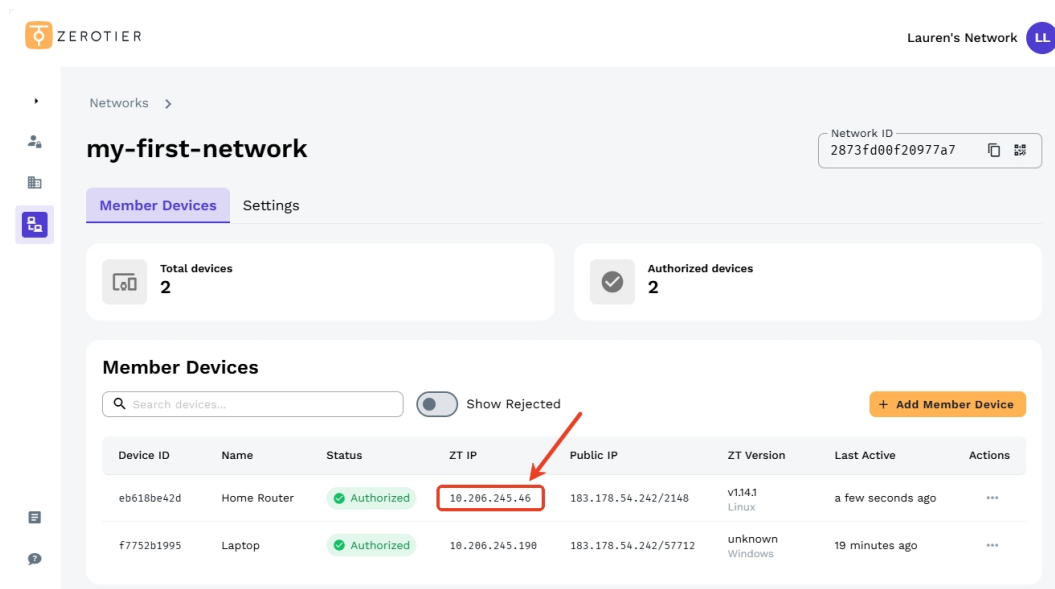
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Authorized	10.206.245.46	183.178.54.242/24364	V1.14.1 Linux	a few seconds ago	...

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**.



Tip: 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.

15.7.2 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.

15.7.3 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 ⓘ



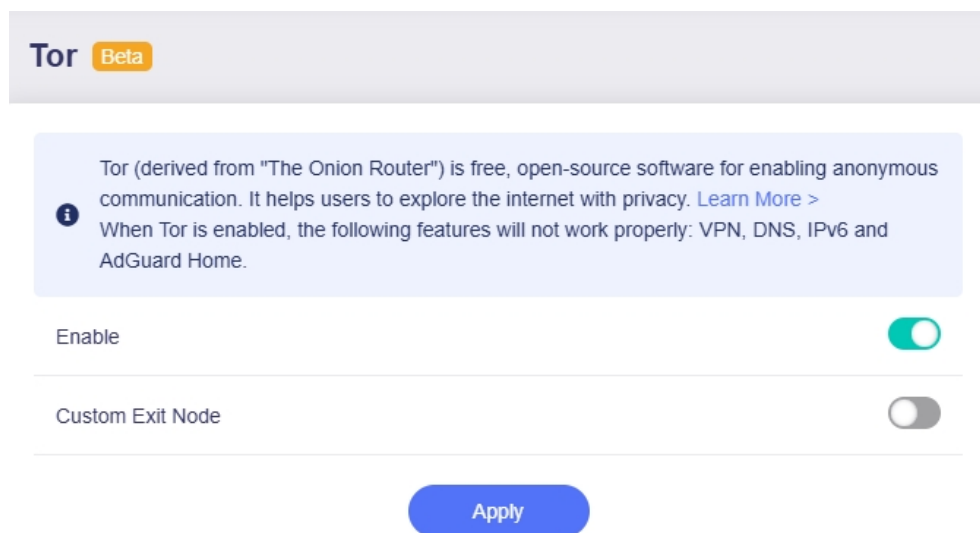
Note: This feature requires routing rules to be added to the ZeroTier network to take effect. One custom route can be added for free in Legacy Central, while in New Central you can only configure custom routes with an Essential plan or higher. See [here](#) for pricing details.

15.8 Tor

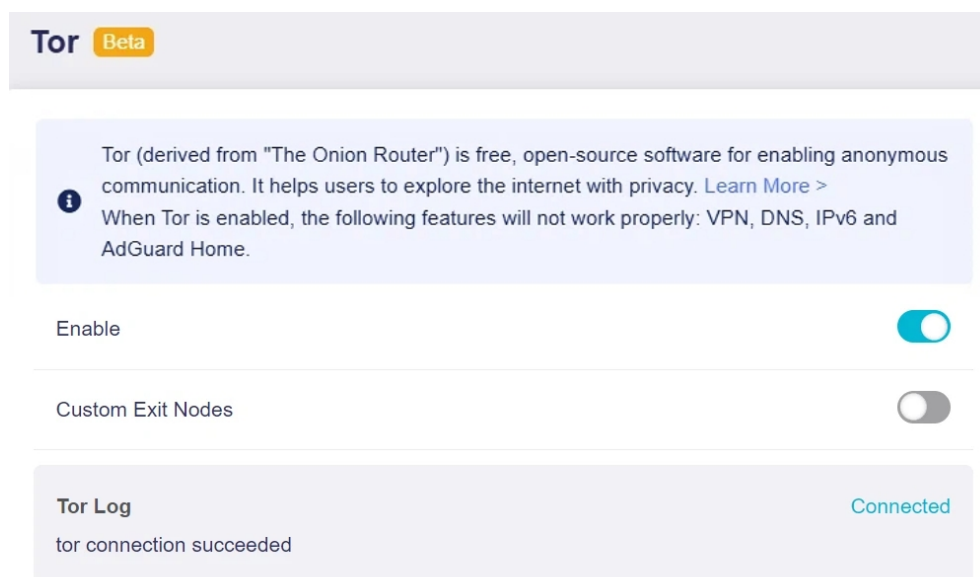
Tor (derived from **The Onion Router**) is a free and open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Note that this feature is currently in beta, and may have some bugs. When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6, and AdGuard Home.

Follow the steps below to set up Tor if 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 if needed, and click **Apply**.



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



Chapter 16

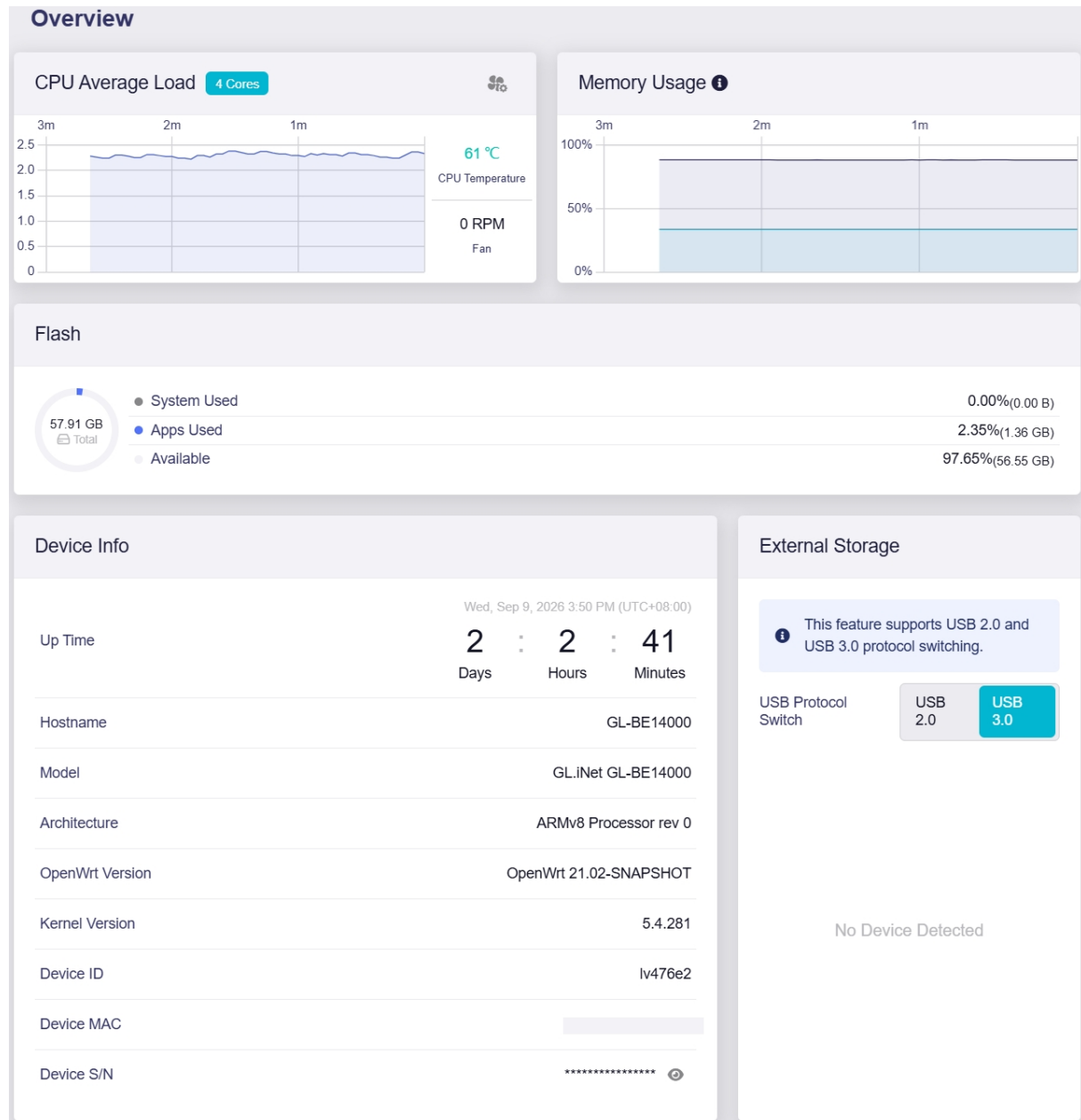
System

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

16.1 Overview

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

- CPU, Memory, and Flash Status
- Device Information
- External Storage Protocol Switch



16.2 Admin Password

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

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.

16.3 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.

16.3.1 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	4.8.3
Firmware Type	release1
Update Time	2026-04-13 07:14:36 (UTC+00:00)

Preview Version

Accept Preview Plan ⓘ ☐

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

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

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

16.3.2 Local Upgrade

Local upgrade does not rely on an Internet connection for the router. Download the correct firmware package (matching your router model) from the official [Download Center](#) to your local device. Then log in to the router's web admin panel, navigate to **SYSTEM > Upgrade > Local Upgrade** section, and upload the firmware package.

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

4.9.1

Release Notes

Firmware Type

release

SHA256

77d314e7bbeaa92b0fc5272be18e630550b062e88b7f5a91a76af2fd1965e460

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.

16.4 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 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.

16.4.1 LED Display Schedule

Set a schedule for your router's LED light if needed.

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.

16.4.2 Schedule Reboot

Set a schedule for automatically restarting your router if needed.

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.

16.4.3 MLO Wi-Fi Schedule

This function allows you to set a schedule for your MLO Wi-Fi. You can enable the on/off schedule for the MLO Main Wi-Fi.

MLO Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off



Enable Main Wi-Fi Schedule



Apply

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

Enable Main Wi-Fi Schedule


Main Wi-Fi

Turn On Time

 07:00

Turn Off Time

 22:00

day(s)

Sun

Mon

Tue

Wed

Thu

Fri

Sat

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

16.4.4 6 GHz Wi-Fi Schedule

This function allows you to set a schedule for your 6 GHZ Wi-Fi. There are two modes: Turn On/Off, and Switch TX Power.

Mode 1: Turn On/Off

You can enable the on/off schedule for both the 6 GHZ Main Wi-Fi and Guest Wi-Fi.

6 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off


Enable Main Wi-Fi Schedule


Enable Guest Wi-Fi Schedule


- **Main Wi-Fi Schedule:** When enabled, set the on and off times for your 6 GHZ Main Wi-Fi, and select an effective date for the week.

Enable Main Wi-Fi Schedule



Main Wi-Fi

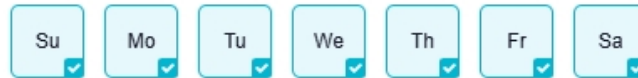
Turn On Time

07:00

Turn Off Time

22:00

day(s)



- **Guest Wi-Fi Schedule:** When enabled, set the on and off times for your 6 GHZ Guest Wi-Fi, and select an effective date for the week.

Enable Guest Wi-Fi Schedule



Guest Wi-Fi

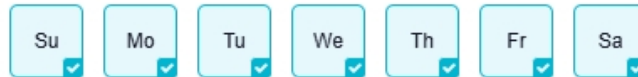
Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Mode 2: Switch TX Power

You can enable the TX power switching schedule for the 6 GHZ Main Wi-Fi.

6 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Switch TX Power



Enable Main Wi-Fi Schedule



When enabled, set two timed actions for your 6 GHZ Main Wi-Fi to switch TX power, and select an effective date for the week.

Enable Main Wi-Fi Schedule 

Main Wi-Fi

Switch

🕒 22:00

Set to

Low

Restore

🕒 07:00

Set to

Max

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

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

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

16.4.5 5 GHz Wi-Fi Schedule

This function allows you to set a schedule for your 5 GHZ Wi-Fi. There are two modes: Turn On/Off, and Switch TX Power.

Mode 1: Turn On/Off

You can enable the on/off schedule for both the 5 GHZ Main Wi-Fi and Guest Wi-Fi.

5 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off

Enable Main Wi-Fi Schedule



Enable Guest Wi-Fi Schedule



- **Main Wi-Fi Schedule:** When enabled, set the on and off times for your 5 GHZ Main Wi-Fi, and select an effective date for the week.

Enable Main Wi-Fi Schedule



Main Wi-Fi

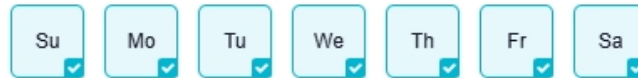
Turn On Time

07:00

Turn Off Time

22:00

day(s)



- **Guest Wi-Fi Schedule:** When enabled, set the on and off times for your 5 GHZ Guest Wi-Fi, and select an effective date for the week.

Enable Guest Wi-Fi Schedule



Guest Wi-Fi

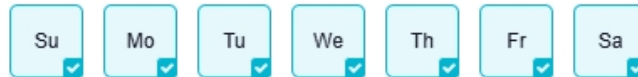
Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Mode 2: Switch TX Power

You can enable the TX power switching schedule for the 5 GHZ Main Wi-Fi.

5 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Switch TX Power



Enable Main Wi-Fi Schedule



When enabled, set two timed actions for your 5 GHZ Main Wi-Fi to switch TX power, and select an effective date for the week.

Enable Main Wi-Fi Schedule


Main Wi-Fi

Switch

 22:00

Set to

Low


Restore

 07:00

Set to

Max


day(s)

Su


Mo


Tu


We


Th


Fr


Sa


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

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

16.4.6 2.4 GHz Wi-Fi Schedule

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

Mode 1: Turn On/Off

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

2.4 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off


Enable Main Wi-Fi Schedule



Enable Guest Wi-Fi Schedule



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

Enable Main Wi-Fi Schedule



Main Wi-Fi

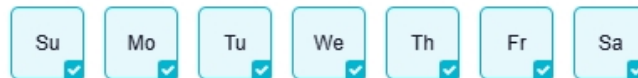
Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Enable Guest Wi-Fi Schedule



Guest Wi-Fi

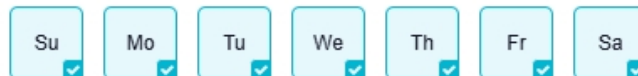
Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Mode 2: Switch TX Power

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

2.4 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Switch TX Power



Enable Main Wi-Fi Schedule



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

Enable Main Wi-Fi Schedule



Main Wi-Fi

Switch

🕒 22:00

Set to

Low



Restore

🕒 07:00

Set to

Max



day(s)

Su	Mo	Tu	We	Th	Fr	Sa
☒	☒	☒	☒	☒	☒	☒

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

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

16.5 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

16.6 Reset Firmware

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

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

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.

16.7 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

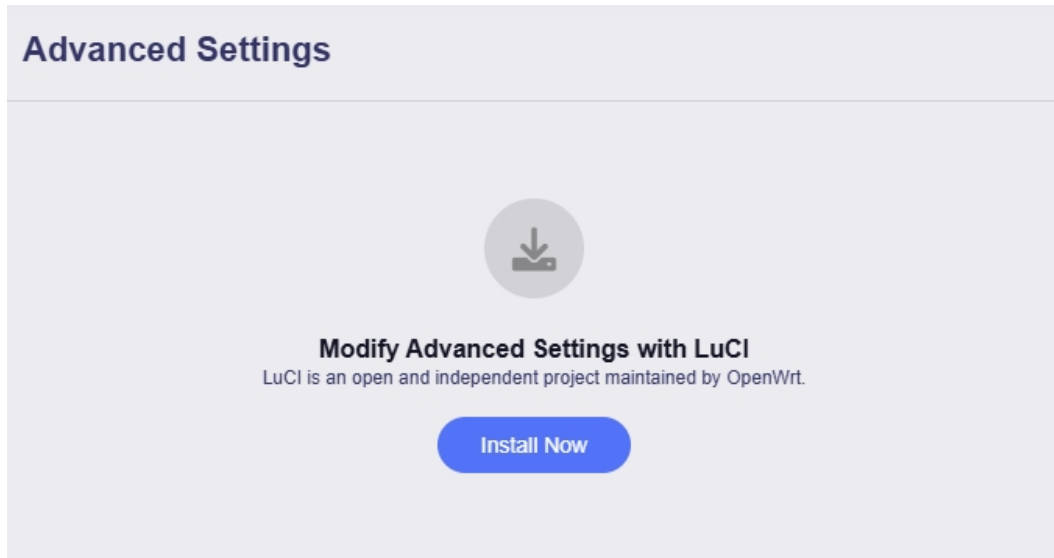
Send

16.8 Advanced Settings

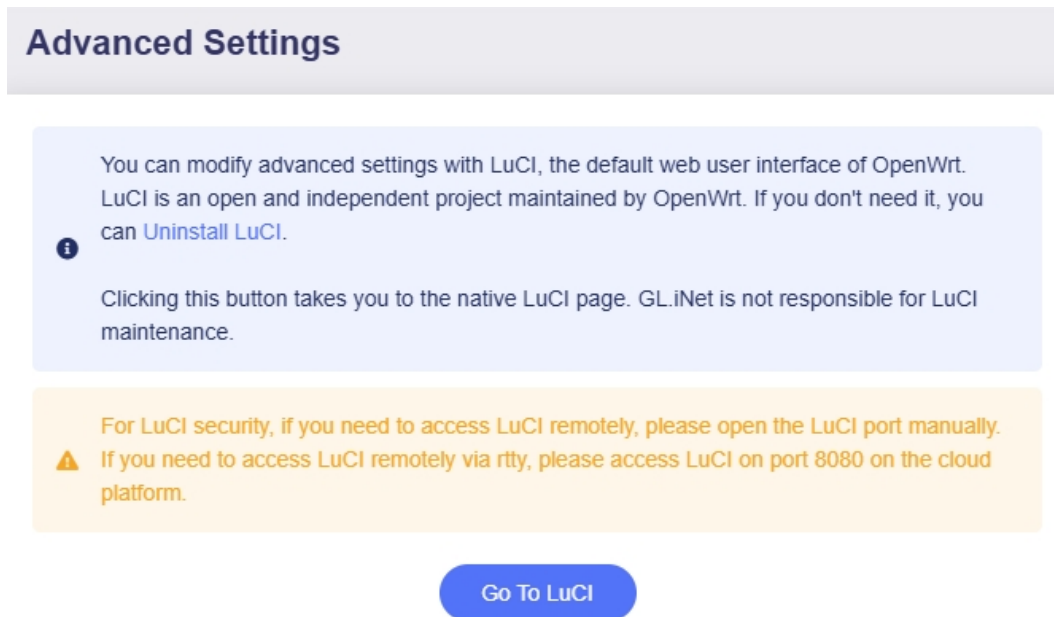
Log in to your router's web admin panel and navigate to **SYSTEM > Advanced Settings**. This page allows you to modify advanced settings in LuCI, which is the default web user interface of OpenWrt. As an open and independent project maintained by OpenWrt, LuCI is provided as-is. GL.iNet is not responsible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

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

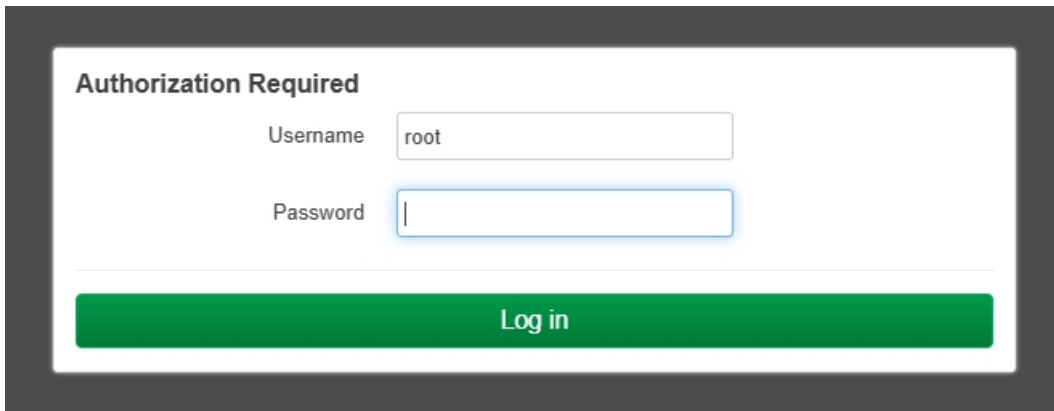
1. Click **Install Now**, and it will be installing LuCI interface.



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



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



Authorization Required

Username

Password

[Log in](#)

You will then log in to the LuCI interface.

GL-BE14000

Status ▾

System ▾

Network ▾

MTK ▾

Logout

Status

System

Hostname	GL-BE14000
Model	GL.iNet GL-BE14000
Architecture	ARMv8 Processor rev 0
Target Platform	mediatek/mt7988
Firmware Version	OpenWrt 21.02-SNAPSHOT / LuCI openwrt-21.02 branch git-23.093.57360-e98243e
Kernel Version	5.4.281
Local Time	2026-09-09 15:59:49
Uptime	2d 2h 50m 6s
Load Average	2.15, 2.25, 2.30

Regulatory Statement

GL TECHNOLOGIES (HONG KONG) LIMITED declares that the radio equipment type [BE14000 Wi-Fi 7 Router, GL-BE14000] is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is <https://www.gl-inet.com/products/certificate>.

For EU:

Maximum output power:

CE: $\leq 20\text{dBm}$ EIRP (2.412GHz~2.472GHz); $\leq 23\text{dBm}$ EIRP (5.15GHz~5.35GHz); $\leq 30\text{dBm}$ EIRP (5.47GHz~5.725GHz); $\leq 13.98\text{dBm}$ (5.725GHz~5.85GHz); $\leq 23\text{dBm}$ EIRP (5.925GHz~6.425GHz)