



User Manual

GL-X3000 / Spitz AX

Wi-Fi 6 Dual-SIM 4G/5G Cellular Router

Firmware Version 4.8.3

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
- 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	9
1.1	Product Overview	10
1.1.1	Appearance	10
1.1.2	Interface and Button	11
1.1.3	LED	12
1.2	Specifications	13
1.3	Package Contents	14
Chapter 2	Hardware Connection	15
2.1	Choosing a Location	16
2.2	Connecting the Router	16
Chapter 3	Log In To Your Router	17
Chapter 4	Set Up Internet Connection	19
4.1	Quick Setup Wizard	20
4.2	Manually Set Up Internet Connection	21
4.2.1	Connect to the Internet via Ethernet Cable	21
4.2.2	Connect to the Internet via an Existing Wi-Fi	27
4.2.3	Connect to the Internet via USB Tethering	39
4.2.4	Connect to the Internet via Cellular	43
Chapter 5	Wireless	65
5.1	Wi-Fi Status Display	66
5.2	Wireless Settings	67
5.2.1	5GHz Wi-Fi	67
5.2.2	2.4GHz Wi-Fi	69
5.2.3	Randomized BSSID	71
Chapter 6	Clients	73
6.1	Device Details	74
6.2	Action	77
6.3	Remove Clients	80
6.4	Sort	80
Chapter 7	Cloud Services	81
7.1	GoodCloud	82
7.1.1	Enable GoodCloud	83

7.1.2 Manage Your Router	85
7.1.3 Unbind Device	90
7.1.4 Disable GoodCloud	90
7.2 AstroWarp	91
Chapter 8 Get To Know VPN	92
8.1 Introduction	93
8.1.1 VPN	93
8.1.2 VPN Router	93
8.1.3 OpenVPN	93
8.1.4 WireGuard	93
8.2 Application Scenarios	94
Chapter 9 VPN Dashboard	96
9.1 VPN Setup Wizard	97
9.2 VPN Mode	100
9.2.1 Global Mode	101
9.2.2 Policy Mode	102
Chapter 10 Set Up VPN Server	111
10.1 OpenVPN Server	112
10.1.1 Preparation	112
10.1.2 Setup Steps	113
10.1.3 Verify Connection	116
10.1.4 Server Options	117
10.1.5 Client to Client	118
10.2 WireGuard Server	120
10.2.1 Preparation	120
10.2.2 Setup Steps	121
10.2.3 Verify Connection	125
10.2.4 Server Options	126
Chapter 11 Set Up VPN Client	128
11.1 OpenVPN Client	129
11.1.1 Preparation	129
11.1.2 Set Up NordVPN	129
11.1.3 Set Up OpenVPN Client Manually (for other providers)	135
11.2 Set Up WireGuard Client	138

11.2.1 Preparation	138
11.2.2 Set Up AzireVPN	139
11.2.3 Set Up Hide.me	143
11.2.4 Set Up IPVanish	146
11.2.5 Set Up Mullvad	150
11.2.6 Set Up NordVPN	154
11.2.7 Set Up PIA (Private Internet Access)	159
11.2.8 Set Up Surfshark	163
11.2.9 Set Up WireGuard Client Manually (for other providers)	167
Chapter 12 Tor	172
Chapter 13 Applications	174
13.1 Plug-ins	175
13.2 Dynamic DNS	176
13.2.1 Enable DDNS	176
13.2.2 Check if DDNS Works	179
13.2.3 HTTPS Remote Access	181
13.2.4 SSH Remote Access	183
13.3 Network Storage	185
13.3.1 Connect Storage	185
13.3.2 Set Up Samba	186
13.3.3 Set Up WebDAV	189
13.3.4 Set Up DLNA	192
13.4 AdGuard Home	193
13.5 Parental Control	195
13.5.1 Quick Setup	195
13.5.2 Troubleshooting	203
13.6 ZeroTier	204
13.6.1 Set Up ZeroTier	205
13.6.2 Allow Remote Access WAN	209
13.6.3 Allow Remote Access LAN	210
13.7 Tailscale	211
13.7.1 Set Up Tailscale	212
13.7.2 Allow Remote Access WAN	215
13.7.3 Allow Remote Access LAN	216

13.7.4 Custom Exit Nodes	217
13.8 eSIM Management	218
13.8.1 Current eSIM Status	219
13.8.2 eSIM Profile List	220
Chapter 14 Network	227
14.1 Port Forwarding	228
14.1.1 DMZ	228
14.1.2 Port Forwarding	229
14.2 Multi-WAN	231
14.2.1 Interface Status Track	231
14.2.2 Multi-WAN Mode	234
14.3 LAN	237
14.3.1 Basic Settings	237
14.3.2 DHCP Server	238
14.3.3 Address Reservation	240
14.4 Guest Network	241
14.4.1 Basic Settings	241
14.4.2 DHCP Server	242
14.5 DNS	244
14.5.1 General Settings	244
14.5.2 DNS Server Settings	245
14.5.3 Edit Hosts	247
14.6 Ethernet Port	249
14.7 Network Mode	250
14.8 IPv6	252
14.8.1 IPv6 Mode	253
14.8.2 DNS acquisition method	253
14.9 Drop-in Gateway	254
14.10 IGMP Snooping	256
14.11 Network Acceleration	257
14.12 NAT Settings	258
Chapter 15 System	259
15.1 Overview	260
15.2 Upgrade	261

15.2.1 Firmware Online Upgrade	261
15.2.2 Firmware Local Upgrade	262
15.2.3 Modem Online Upgrade	263
15.2.4 Modem Local Upgrade	263
15.3 Scheduled Tasks	264
15.3.1 LED Display Schedule	264
15.3.2 Schedule Reboot	265
15.3.3 5GHz Wi-Fi Schedule	266
15.3.4 2.4GHz Wi-Fi Schedule	268
15.4 Time Zone	270
15.5 Log	271
15.6 Security	273
15.6.1 Admin Password	273
15.6.2 Access Control	274
15.6.3 Remote Access Control	276
15.6.4 Open Ports on Router	277
15.7 Reset Firmware	278
15.8 Advanced Settings	279
Regulatory Statement	281

Chapter 1

Get To Know Your Router

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

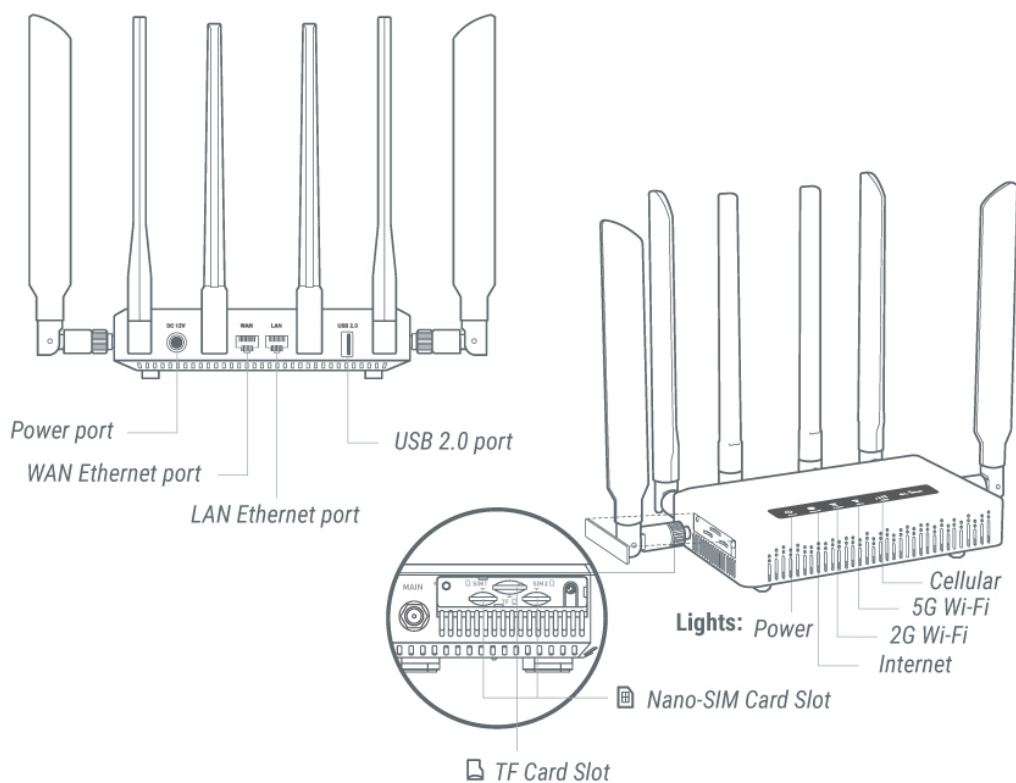
1.1 Product Overview

Spitz AX (GL-X3000) is a dual-SIM Wi-Fi 6 cellular gateway designed to provide fast, reliable connections especially in remote areas and during road trips. It offers four internet access methods: Cellular (SIM cards), ethernet, repeater, and tethering. It supports multi-WAN (failover and load-balancing), VPN (OpenVPN and WireGuard), parental controls, AdGuard Home, port forwarding, Tailscale, and more.

1.1.1 Appearance



1.1.2 Interface and Button



Item	Definition
WAN Ethernet port	Connects the router to an upstream network at 10/100/1000/2500Mbps.
LAN Ethernet port	Connects a wired client to the router at 10/100/1000Mbps.
USB 2.0 port	Connects a supported USB modem, tethering device, or USB storage device.
MicroSD card slot	Accepts a MicroSD card with a maximum capacity of 1 TB.
Nano SIM card slots	Accept two Nano SIM cards. Only one SIM card is active at a time; the other serves as backup.

Item	Definition
Reset button	Press for less than 3 seconds to reset the network, or press for 10 seconds to restore factory settings.
DC5521 power input	Accepts the supplied 12V/2.5A adapter or a 9~36 V DC input.
Cellular antenna connectors	Connect four cellular antennas (SMA, 600 MHz~6 GHz).
Wi-Fi antenna connectors	Connect two Wi-Fi antennas (PR-SMA, 2.4~2.5 GHz and 5.15~5.84 GHz).

1.1.3 LED

Device Status	Power	Internet	2.4GHz	5GHz	Cellular
Internet connected (Cellular active)	Green On	Green On	Green On	Green On	Green On
Internet connected (Cellular inactive)	Green On	Green On	Green On	Green On	Off
No Internet	Green On	Off	Green On	Green On	Off
Firmware updating	Green On	Flashing every 0.5s	Flashing every 0.5s	Flashing every 0.5s	Green On
Network reset (press reset < 3s)	Flashing every 1s	Green On	Green On	Green On	Green On
Factory reset (press reset for 10s)	Flashing every 0.25s	Green On	Green On	Green On	Green On

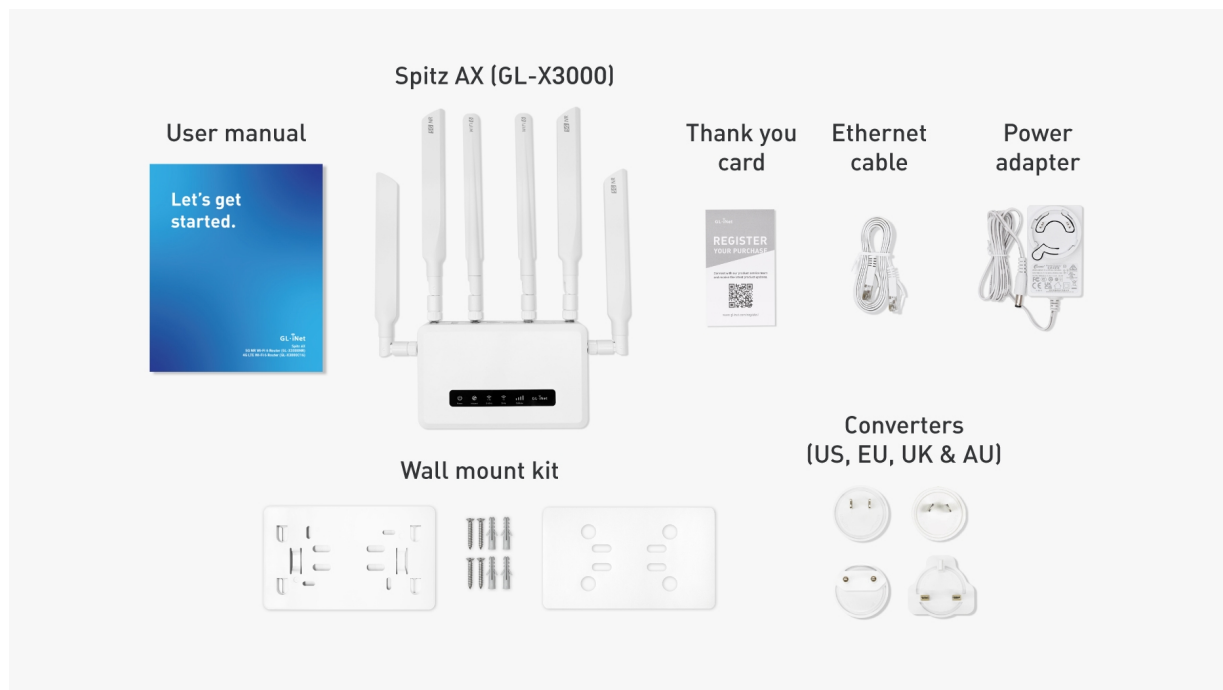
Tips: When connected to the Internet, a flashing 2.4GHz or 5GHz LED means that Wi-Fi devices are connected and actively transmitting data.

1.2 Specifications

Item	Details
Interface	1 x WAN Ethernet port 1 x LAN Ethernet port 1 x USB 2.0 port 1 x MicroSD card slot (Max.1TB) 2 x Nano SIM card slots 1 x Reset button
CPU	MediaTek Dual-core, @1.3GHz
Memory / Storage	DDR4 512 MB / eMMC 8GB
Protocol	IEEE 802.11a/b/g/n/ac/ax
Wi-Fi Speed	574Mbps (2.4GHz), 2402Mbps (5GHz)
Ethernet Speed	WAN Port: 10/100/1000/2500Mbps LAN Port: 10/100/1000Mbps
Antennas	4 x Cellular Antennas (SMA, 600M~6GHz) 2 x Wi-Fi Antennas (PR-SMA, 2.4G~2.5GHz, 5.15~5.84GHz)
LEDs	System / 5G Wi-Fi / 2.4G Wi-Fi / Internet / Cellular Signal Strength
Power Input	DC5521, 12V/2.5A (5.5*2.1mm) [default adapter] / 9~36V
Power Consumption	<14W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	155 x 95 x 36mm / 520g
Other Tools	Datasheet Firmware App Unboxing Tutorials Media Kit

1.3 Package Contents

- 1 x Spitz AX (GL-X3000)
- 1 x User manual
- 1 x Thank you card
- 1 x Ethernet cable
- 1 x Wall mount kit
- 1 x Power adapter
- 4 x Converters



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

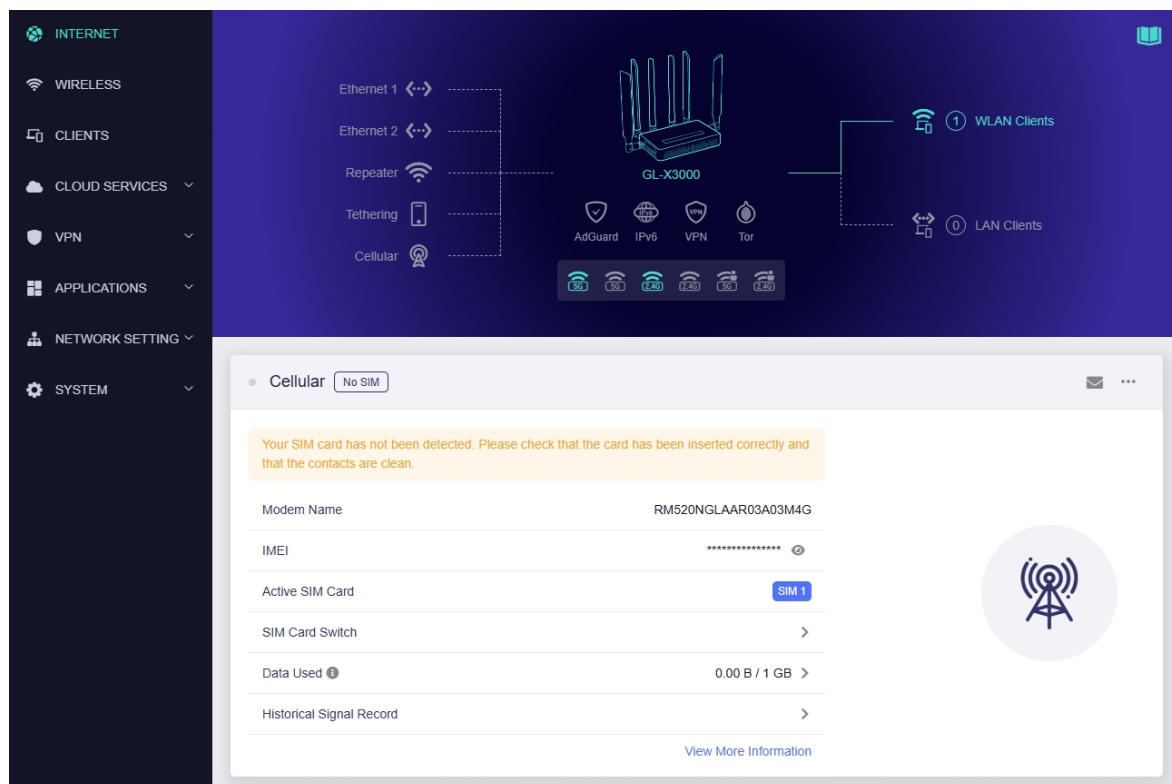
This chapter guides you to log in to your router via web admin panel.

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

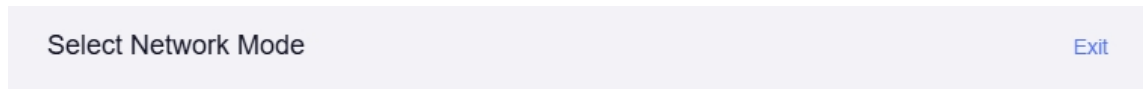
The Web-based Setup Wizard will guide you through the router network configuration.

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.



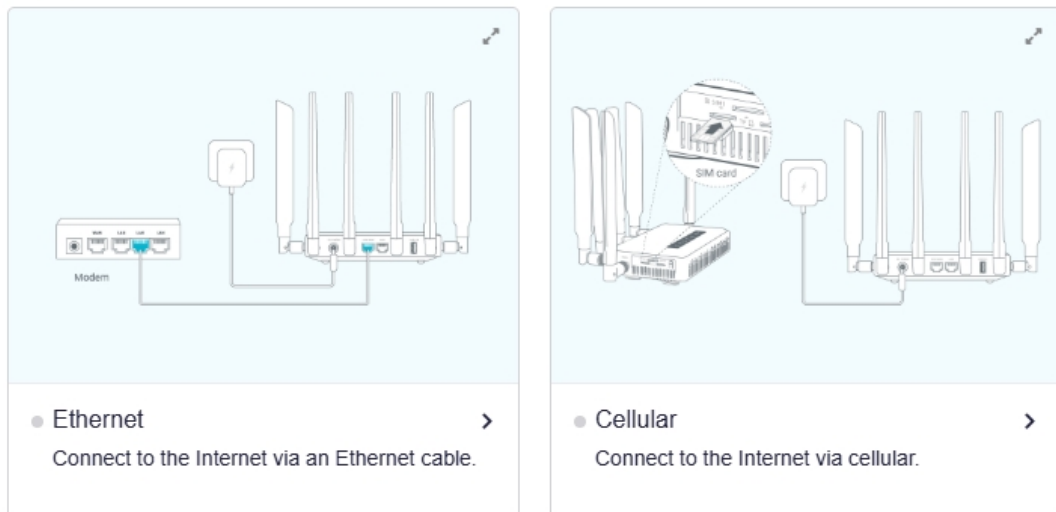
3. Follow the Setup Wizard to configure your router and establish an internet connection.



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 as needed.

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

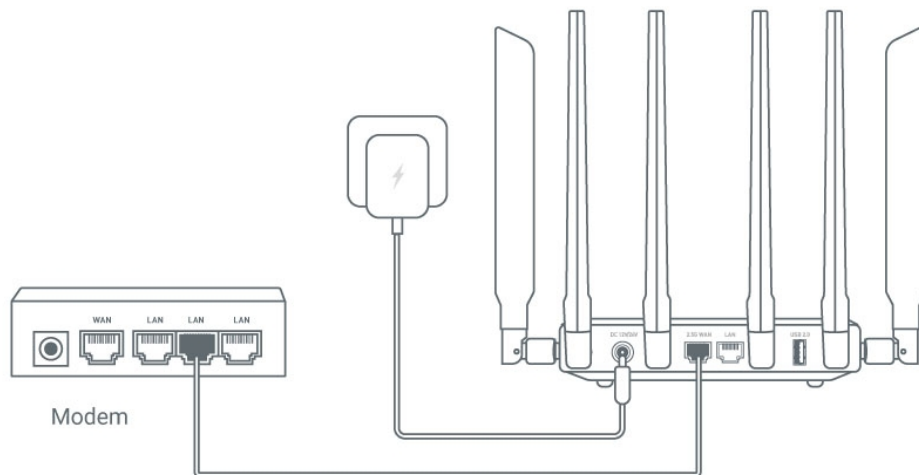
4.2.1 Connect to the Internet via Ethernet Cable

Connect the router to a broadband network via an Ethernet cable plugged into the WAN port. It usually automatically acquires an IP address (DHCP). Users can also configure static IP or PPPoE manually. This method offers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.

4.2.1.1 Basic Steps

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, router, network switch or an Ethernet jack) via an Ethernet cable.



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

Ethernet 1
WAN

Protocol	DHCP
IP Address	192.168.11.163
Gateway	192.168.11.1
DNS Server	192.168.11.1



Modify

Tips: You can switch the WAN port role as a LAN port if needed. That is useful when you are using the router as a repeater since the physical WAN port is idle. You will then have one more LAN port.

4.2.1.2 Protocol

There are 3 types of protocols, DHCP, Static, PPPoE. Click **Modify** to change.

Ethernet 1
WAN

Protocol	DHCP
IP Address	192.168.11.163
Gateway	192.168.11.1
DNS Server	192.168.11.1





Modify

- **DHCP**

DHCP is the default and most common protocol, automatically assigning IP addresses and other communication parameters to network devices via a client-server architecture on IP networks.

Ethernet Settings

Protocol

DHCP
Static
PPPoE

i IP address is assigned by higher network machine.

IPv4

IP Address
192.168.11.163

Netmask
255.255.255.0

Gateway
192.168.11.1

DNS Server 1
192.168.11.1

DNS Server 2

- **Static**

Static is needed if your ISP (Internet Service Provider) provides a fixed IP address, or you want to manually configure network information, such as IP address, Gateway, Netmask.

Ethernet Settings

Protocol

DHCP
Static
PPPoE

IPv4

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2
Optional

- **PPPoE**

PPPoE is a protocol used by most ISPs. Typically, they provide a modem and a username & password, which are needed for Internet setup.

Ethernet Settings

Protocol

DHCP

Static

PPPoE

PPPoE Setting

Username

Optional

Password

Optional



VLAN ID ⓘ

Optional (1 ~ 4094)

TTL ⓘ

Optional

HL ⓘ

Optional

MTU ⓘ

1500

Cancel

Apply

4.2.1.3 Advanced

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

Ethernet Settings

IPv4

IP Address

192.168.116.221

Netmask

255.255.255.0

Gateway

192.168.116.254

DNS Server 1

223.5.5.5

DNS Server 2

223.6.6.6

VLAN ID ⓘ

Optional (1 ~ 4094)

TTL ⓘ

Optional

HL ⓘ

Optional

MTU ⓘ

1500

- **VLAN ID:** This setting entry is required 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. The TTL setting is valid only for IPv4. If you need to override/spoof the TTL, set a fixed value here. For most models, enter the desired effective TTL plus 1 to compensate for the automatic decrement.
- **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.

4.2.1.4 Troubleshooting

If an Ethernet cable is plugged into the WAN port but the Internet is unavailable, a yellow message will be displayed as shown below.

"The interface is connected, but the Internet can't be accessed."

Ethernet 

 The interface is connected, but the Internet can't be accessed.

Protocol	DHCP
IP Address	192.168.8.7
Gateway	192.168.8.1
DNS Server	192.168.8.1

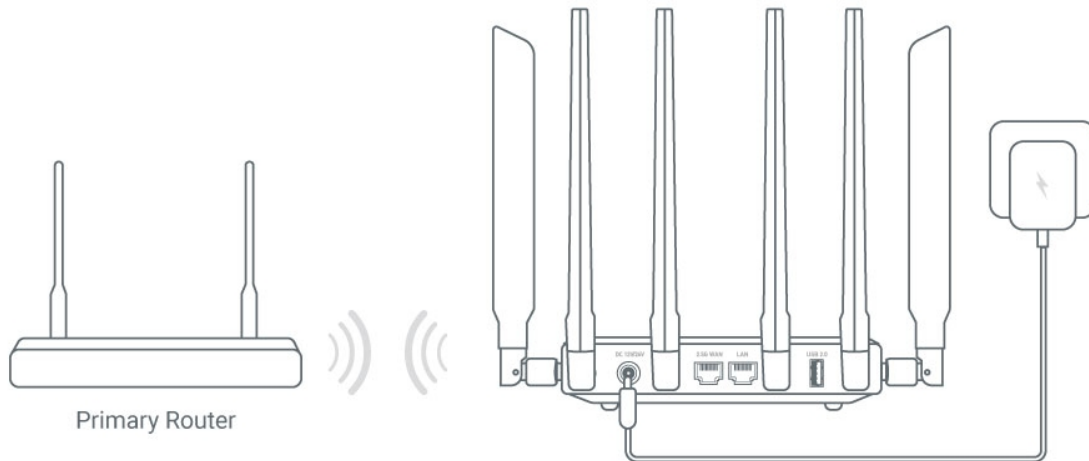
Modify

To fix this issue:

1. Check if the upstream device has Internet access.
2. Go to [Multi-WAN](#) page to check the Ethernet interface status.

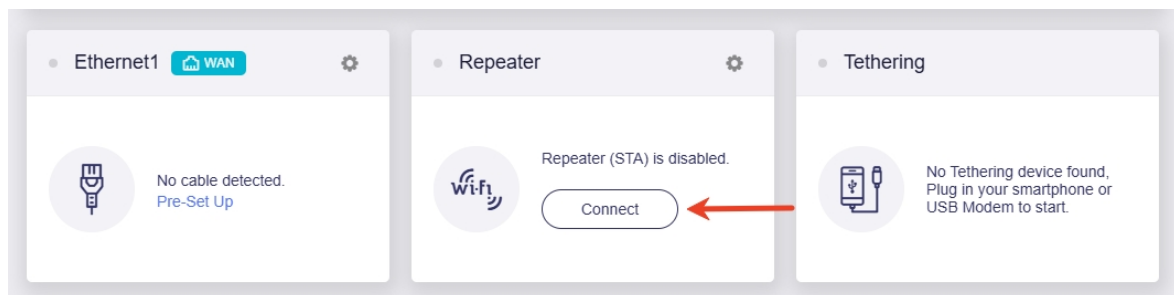
4.2.2 Connect to the Internet via an Existing Wi-Fi

Using Repeater means connecting the router to another existing wireless network, e.g. when you are using free Wi-Fi in a hotel or cafe. It works in WISP (Wireless Internet Service Provider) mode by default, which means that the router will create its own subnet and act as a firewall to protect you from the public network.



4.2.2.1 Basic Steps

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



2. Choose the Wi-Fi network you want to connect to 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

Available Networks

[Join Other Network](#)

	GL-BE9300-c37	2.4G
	GL-B1300-5b8	2.4G
	GL Router-IoT-2.4G	2.4G
	2.4GHZ	2.4G
	GL-BE9300-c37-5G	5G

Note:

1. This page displays the Wi-Fi channels your router supports. Make sure the Wi-Fi network you're trying to connect to uses one of these channels, otherwise it may not be displayed in the available network list.
2. When searching for an iPhone Personal Hotspot, keep the iPhone unlocked to maintain Wi-Fi beacon transmission. Otherwise, the router may fail to detect this hotspot.
3. Enter the correct Wi-Fi password and click **Apply**.

Join Network

[Exit](#)

SSID

@GL-OFFICE

Password

| 

Auto-Enable Login Mode for Public Hotspots 



Enable Camouflage 



MAC Mode

Random



MAC Address

82:53:69:XX:XX:XX [Random](#)

Auto Update MAC 



Back

Apply

Tip: If the Wi-Fi SSID you want to connect to is not in the Available Network list, click **Join Other Network** in the upper-right corner, manually enter the Wi-Fi SSID and other information required before clicking **Apply**.

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

Available Networks

 [Join Other Network](#)


GL-BE9300-c37

2.4G



GL-B1300-5b8

2.4G



GL Router-IoT-2.4G

2.4G

4. After a while, if the password is correct, the connection will be successful.

• @GL-OFFICE   DFS



IP Address	10.100.32.77
Gateway	10.100.32.1
DNS Server	10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID	C0:A9:38:B4:FC:43
MAC Address	 7E:D9:F5:C1:B7:0E

Disable

Switch Network

[Modify](#)

4.2.2.2 For Public Hotspot

When connecting the router to a public hotspot with a captive portal, enabling the following features can help improve the connection success rate.

Join Network

Exit

SSID

LEO-BE6500

Password

Auto-Enable Login Mode for Public Hotspots ⓘ

Enable Camouflage ⓘ

MAC Mode

Random

MAC Address

A6:25:32:69:4D:E6 Random

Auto Update MAC ⓘ

Remember

Lock BSSID ⓘ

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 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.

4.2.2.3 Advanced Settings

When joining the network, there are some additional options.

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

HL

MTU

Back Apply

- **Remember:** Enable this to remember the current repeated Wi-Fi network.
- **Lock BSSID:** When enabled, the router will connect only to the specific access point (AP) corresponding to the selected BSSID, even when other APs share the same SSID.
- **Manually Set Static IP:** When enabled, you can manually configure a fixed IPv4 address, netmask, gateway, and DNS servers for the router's repeater connection, instead of obtaining these settings automatically.
- **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. The TTL is valid only for IPv4. By default, the router forwards the TTL of the incoming client device minus one. If you need to override it, enter the desired effective TTL plus 1 to compensate for the automatic decrement.
- **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.

4.2.2.4 Repeater Options

Click the gear icon in the upper-right corner of the connected Repeater section.

@GL-OFFICE 5G DFS

IP Address	10.100.32.77
Gateway	10.100.32.1
DNS Server	10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID	C0:A9:38:B4:FC:43
MAC Address	7E:D9:F5:C1:B7:0E

Disable

Switch Network

Modify



The Repeater Options are displayed as follows.

Repeater Options

Allow Switching to Other Saved Networks ⓘ

Band Selection ⓘ

Auto

5 GHz

2.4 GHz

Cancel

Apply

- **Allow Switching to Other Saved Networks:** If enabled, the router will automatically connect to other saved networks when the current connected Wi-Fi network is unavailable.
- **Band Selection:** If you manually select a band, the router will only scan and connect to the Wi-Fi networks in this frequency band.

4.2.2.5 Manage Known Network

To manage known networks, click **Switch Network**.

@GL-OFFICE 5G DFS

IP Address	10.100.32.77
Gateway	10.100.32.1
DNS Server	10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID	C0:A9:38:B4:FC:43
MAC Address	7E:D9:F5:C1:B7:0E

Disable

Switch Network

Modify



On the **Known Networks** section, click the trash icon to delete a known network, or the gear icon to configure the network.

Join Wi-Fi

Known Networks

GL-OFFICE-5G

Available Networks ⓘ

Join Other Network

GL-MT300N-V2-184

2.4G

GL-XE300-407

2.4G

GL-MT6000-787-5G

5G

4.2.2.6 Join Other Network

If the SSID is not in the Available Networks list, or if the SSID is hidden, you can click **Join Other Network**.

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

Available Networks

 [Join Other Network](#)

 GL-BE9300-c37

2.4G

 GL-B1300-5b8

2.4G

 GL Router-IoT-2.4G

2.4G

Enter the **SSID**, select the **Security** and enter the password (if required), then click **Apply**.

Join Network

Exit

SSID

Security

None



Auto-Enable Login Mode for Public Hotspots 



Enable Camouflage 



MAC Mode

Random



MAC Address

16:22:D1:XX:XX:XX [Random](#)

Auto Update MAC 



[Advanced Settings](#)

Back

Apply

For **Security** settings, there are two or three options, depending on the model.

- None, which means no password is required.
- WPA/WPA2/WPA3, which is common and supported by nearly all Wi-Fi networks.
- WPA/WPA2/WPA3 Enterprise, which requires Extensible Authentication Protocol (EAP) for authentication. A valid username and password are needed to connect (typically used in business or campus networks).

Join Network

Exit

SSID

Security

WPA/WPA2/WPA3 Enterp

Username

Password

For detailed guidance on repeating EAP networks, please click [here](#).

4.2.2.7 Reconnection

In the following cases, the router will automatically attempt to reconnect to Wi-Fi every once in a while. You can manually disable this if needed. For SSID/password errors, remove the network from Known Networks to resolve it.

1. Incorrect SSID/password entered during Repeater setup.
2. Moved out of range of the upstream router after initial connection.
3. Upstream router changes SSID/password or restricts access post-connection.

The reconnection process has three distinct phases: waiting phase, scanning phase and connecting phase.

1. Waiting Phase: No issues - router waits for reconnection conditions.
2. Scanning Phase: Packet loss may occur on the scanned frequency band. New devices might face connection problems. For models GL-AXT1800/GL-AX1800, Guest Wi-Fi will be temporarily disabled.
3. Connecting Phase: Main Wi-Fi on the target band may drop for a few seconds during re-establishment.

Note: Problems typically arise in the Scanning and Connecting phases.

4.2.2.8 Troubleshooting

When the router is connected to a Wi-Fi network as a repeater, if the Internet is unavailable, a yellow message will be displayed as shown below.

"The interface is connected, but the Internet can't be accessed."

GL-MT6000-787-5G 5G

 The interface is connected, but the Internet can't be accessed.

IP Address	192.168.5.154
Gateway	192.168.5.1
DNS Server	192.168.5.1
BSSID	4E:5D:28:E0:D2:1A
MAC Address	 FA:A9:03:21:A5:C6

Disable Switch Network Modify

To fix this issue:

1. Check if the upstream device (i.e., the Wi-Fi network your router is connected to) has internet access.
2. Go to [Multi-WAN](#) page to check the repeater interface status.

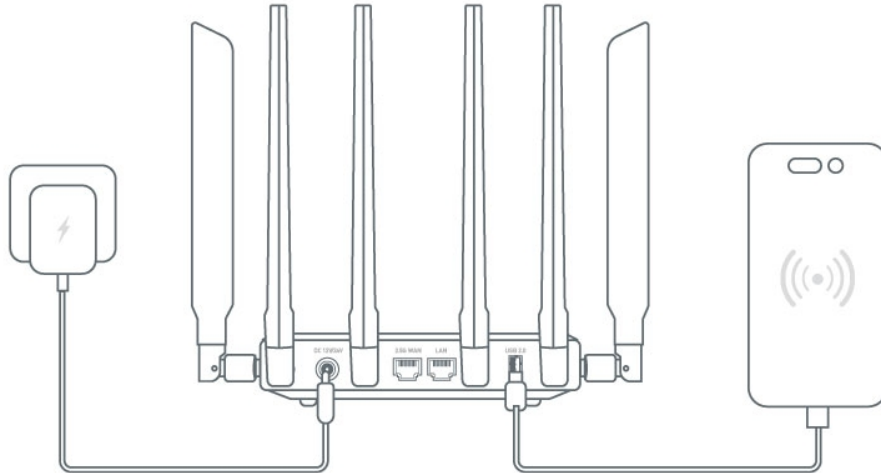
4.2.2.9 DFS

DFS (Dynamic Frequency Selection) is a mechanism that automatically switches Wi-Fi channels to avoid interference with radar signals. When connecting to an upstream 5G Wi-Fi, the router's Wi-Fi will follow the upstream Wi-Fi to use or not use the DFS channel.

- If the upstream Wi-Fi uses a DFS channel and is scannable, the router's 5G Wi-Fi will use the same channel.
- The router's 5G Wi-Fi will switch to the non-DFS channel if the upstream Wi-Fi is not scannable or if the connection fails.

4.2.3 Connect to the Internet via USB Tethering

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

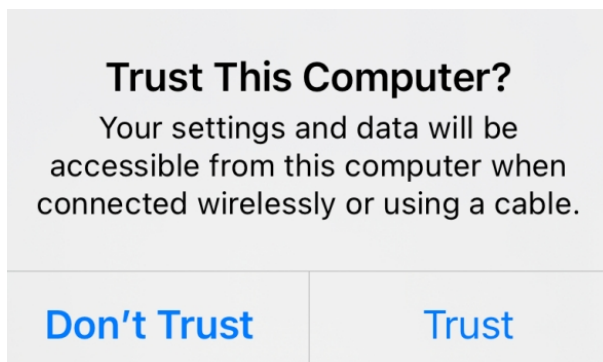


Host-less modem works in Tethering as well during the cellular setup.

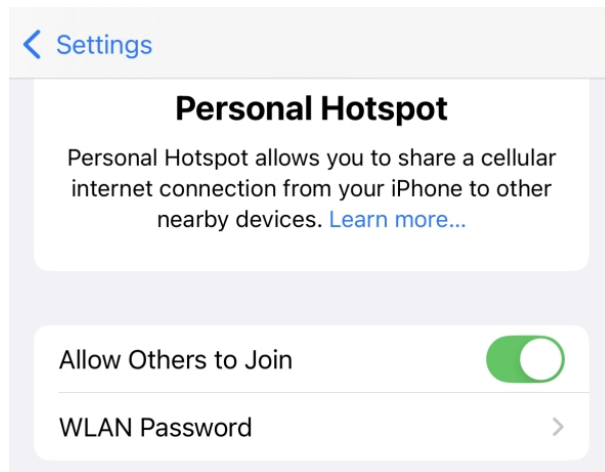
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

4.2.3.1 iPhone

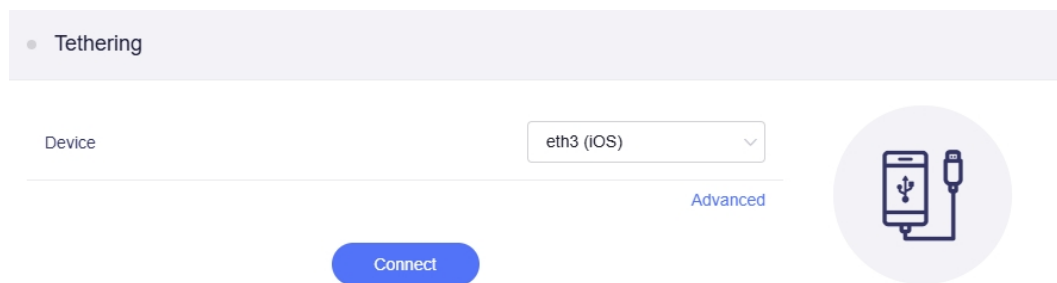
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



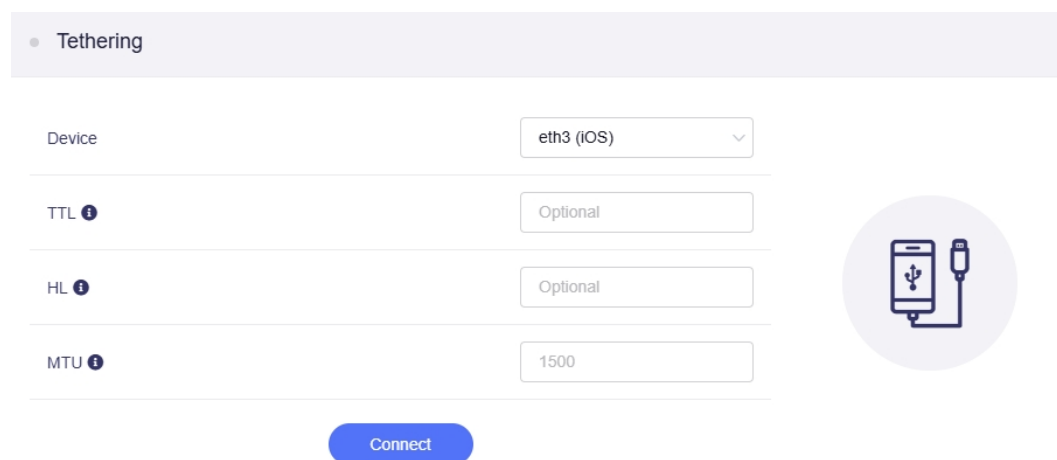
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



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, then click **Connect**.



4. It will start connecting.

● Tethering

Connecting...

Device eth3 (iOS) ▼

[Advanced](#)

[Abort](#)



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

● Tethering iOS

IP Address	172.20.10.6
Gateway	172.20.10.1
DNS Server	172.20.10.1

[Disconnect](#)



4.2.3.2 Android

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**.

● Tethering

Device usb0 (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	usb0 (Android) ▾
TTL ⓘ	Optional
HL ⓘ	Optional
MTU ⓘ	1500

Connect



4. 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



4.2.3.3 Troubleshooting

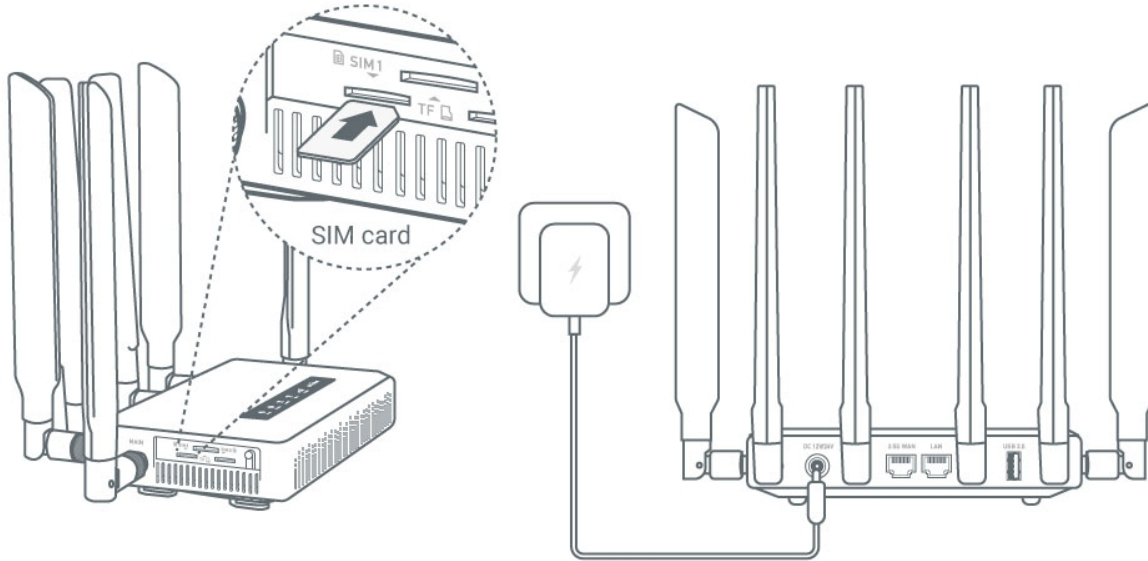
If the connection fails, try these troubleshooting steps:

- 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.

4.2.4 Connect to the Internet via Cellular

Spitz AX (GL-X3000) has a built-in dual-SIM cellular modem. Only one SIM card is active at a time; the other serves as a backup. You can manually switch between the two SIM cards.



4.2.4.1 Auto Setup

We recommend you power off the router first, insert your pre-activated SIM card(s) into the slots, then power it on. If you insert the SIM card after the router has booted up, the web admin panel may not update automatically. In that case, please refresh the page or restart the router.

1. Log in to the router's web admin panel and navigate to **INTERNET > Cellular**.
2. When no SIM card is inserted, the page displays a message "Your SIM card has not been detected".

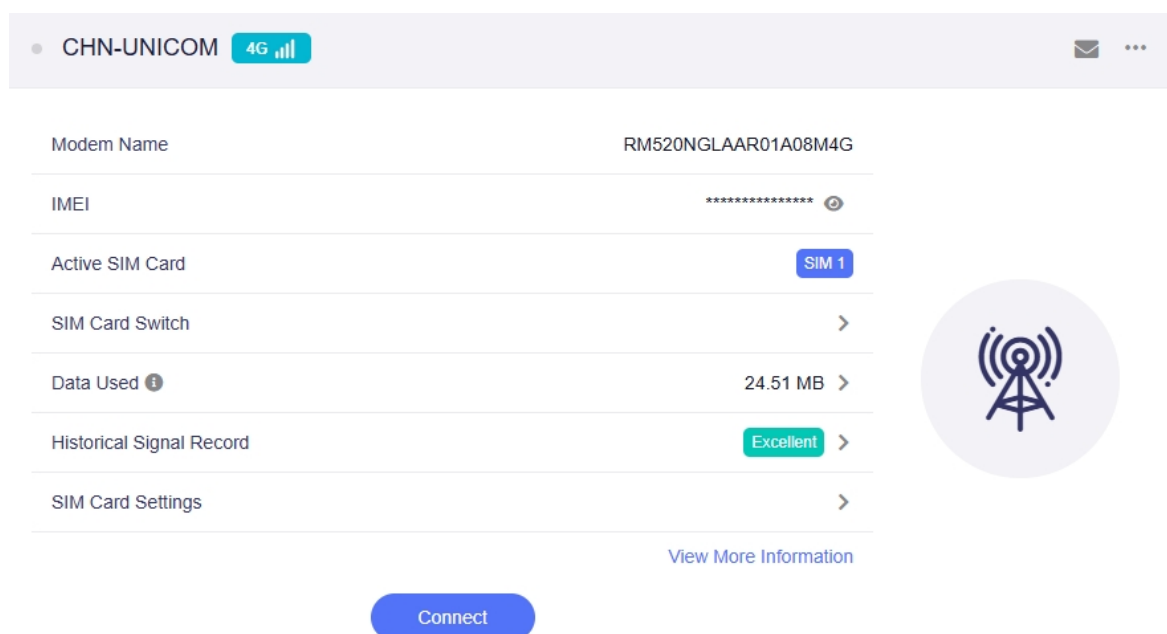
Cellular

No SIM

Your SIM card has not been detected. Please check that the card has been inserted correctly and that the contacts are clean.

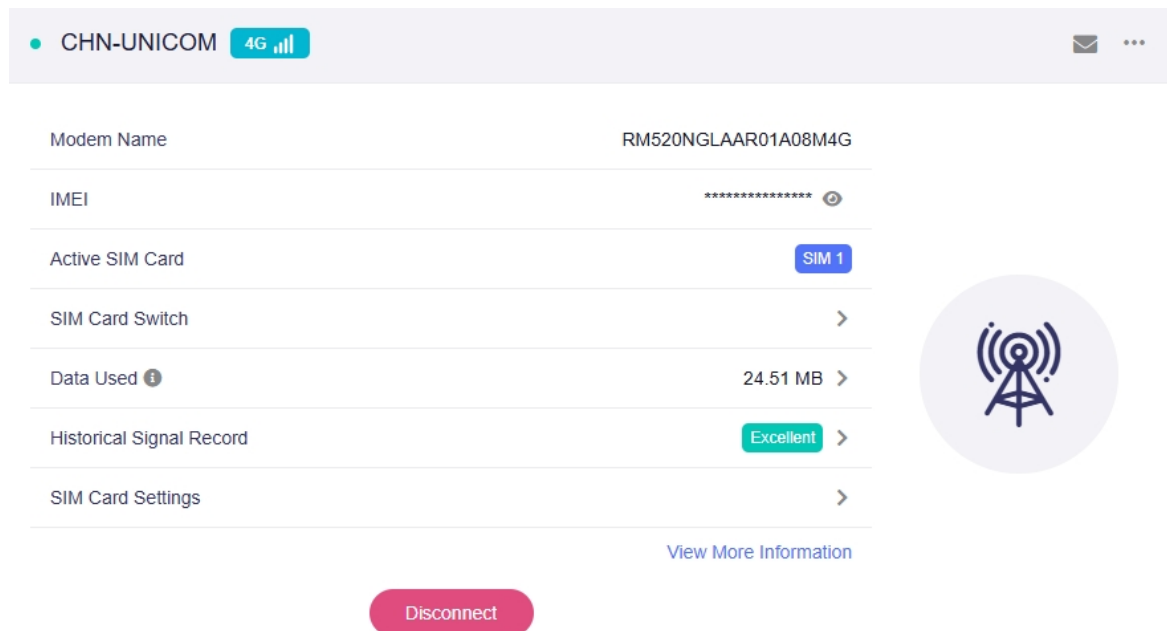
Modem Name	RM520NGLAAR01A07M4G
IMEI	*****
Active SIM Card	SIM 1
SIM Card Switch	>
Data Used	0.00 B >

3. When a SIM card is inserted, the page displays as follows. Click **Connect**.



Tip: If the SIM card is not detected, try restarting the router to see if it can be detected.

4. Once the cellular network is connected, the page displays the network details with a green dot, indicating a successful connection.



5. Click **View More Information** to show more cellular information, including modem details, SIM card details, Internet details, and cellular signal.

● CHN-UNICOM 4G 

 ...

Modem Name	RM520NGLAAR01A08M4G
IMEI	***** 
Active SIM Card	SIM 1
SIM Card Switch	>
Data Used 	24.03 MB >
Historical Signal Record	Excellent >
SIM Card Settings	>



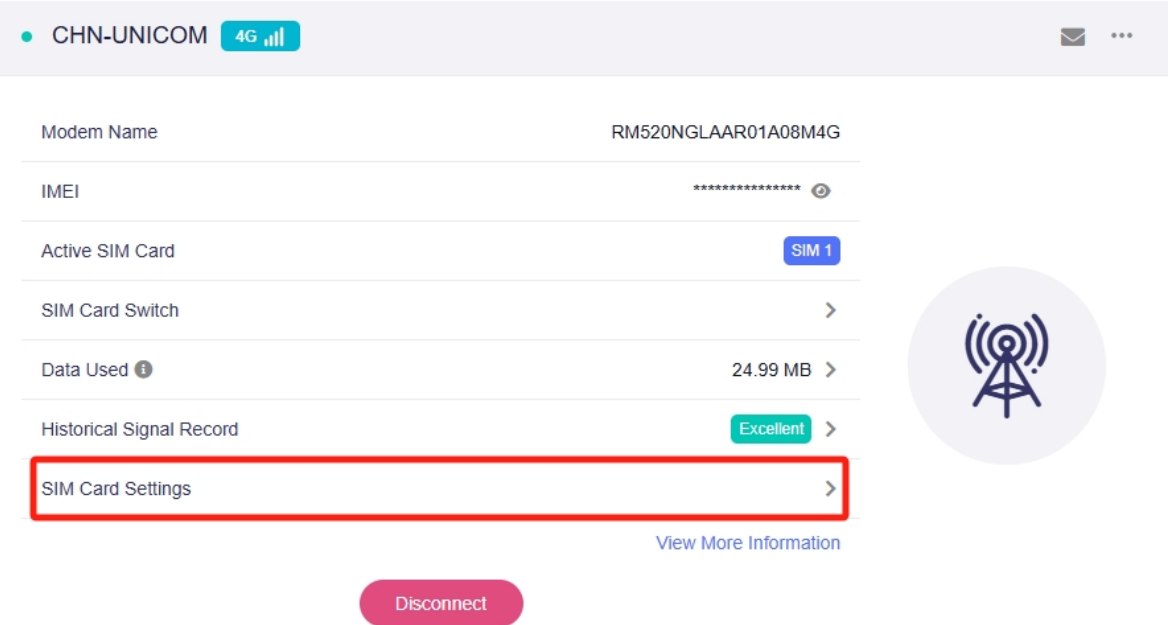
 [View More Information](#)

Disconnect

If Auto Setup fails, please try **Manual Setup**.

4.2.4.2 Manual Setup

1. In the router's web admin panel, navigate to **INTERNET > Cellular**, then click **SIM Card Settings**.



CHN-UNICOM 4G

Modem Name: RM520NGLAAR01A08M4G

IMEI: *****

Active SIM Card: SIM 1

SIM Card Switch: >

Data Used: 24.99 MB >

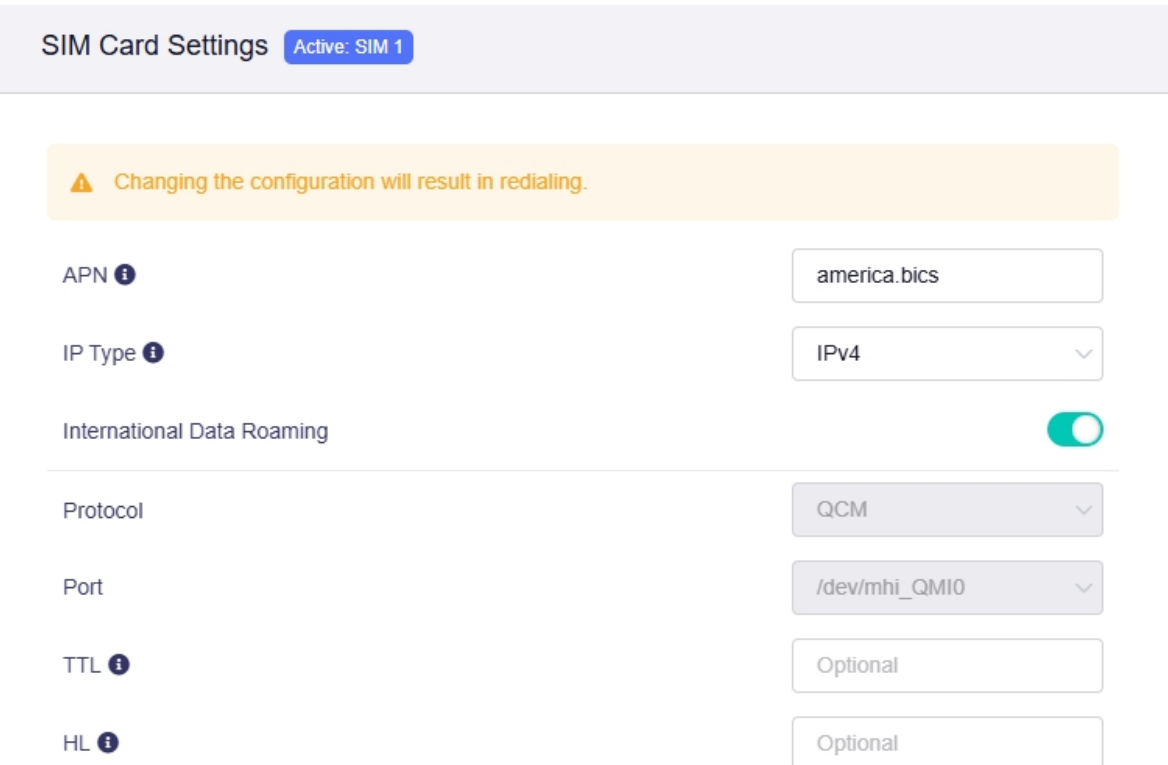
Historical Signal Record: Excellent >

SIM Card Settings >

[View More Information](#)

[Disconnect](#)

2. You can view or modify the cellular settings of the current SIM card. Applying the changes will trigger a reconnection.



SIM Card Settings Active: SIM 1

⚠ Changing the configuration will result in redialing.

APN: america.bics

IP Type: IPv4

International Data Roaming: ☒

Protocol: QCM

Port: /dev/mhi_QM10

TTL: Optional

HL: Optional

The screenshot shows a configuration panel with three settings:

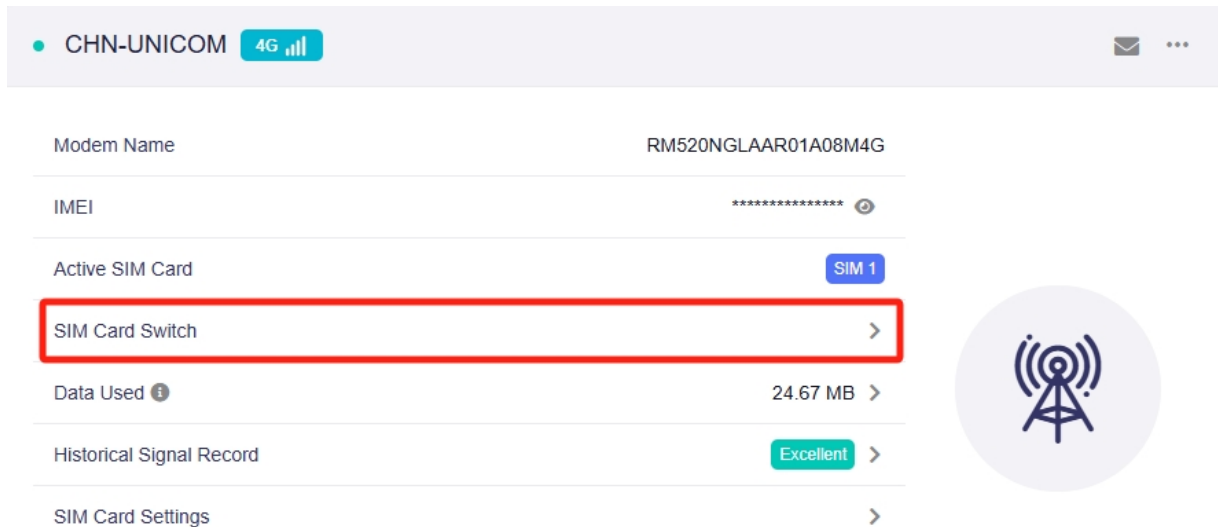
- MTU**: A text input field containing the value "1500".
- Authentication**: A dropdown menu currently showing "NONE".
- Enable Band Masking**: A toggle switch that is currently turned off.

At the bottom of the panel are two buttons: "Cancel" and "Apply".

- **APN**: APN (Access Point Name) is a gateway parameter required for a cellular network connection. It allows the router to connect to the internet provided by your mobile carrier. You can use the default APN or set a custom APN provided by your carrier.
- **Protocol**: The auto-detected cellular communication protocol (e.g., QMI or QCM) based on your modem and carrier.
- **Port**: The auto-detected serial port for communication with the cellular modem.
- **TTL**: TTL (Time To Live) defines the maximum time packets can survive in the network. The TTL setting is valid only for IPv4. By default, the router decrements the TTL of incoming packets from client devices by 1 before forwarding them. If you need to override it, enter the desired effective TTL plus 1 to compensate for the automatic decrement.
- **HL**: In IPv6, HL (Hop Limit) limits the number of transmission hops for data packets in the network and serves as the equivalent of TTL in IPv4.
- **MTU**: The default MTU value is 1500 bytes.
- **Authentication**: Choose the authentication method required by your carrier (e.g., NONE, PAP, CHAP). This is usually set to NONE if no credentials are needed.
- **Band Masking**: You can enable Band Masking if you want the router to block certain bands or use only specific cellular bands. See [4.2.4.6 Band Masking](#) for details.

4.2.4.3 SIM Card Slot Settings

In the router's web admin panel, navigate to **INTERNET > Cellular**, then click **SIM Card Switch**.



CHN-UNICOM 4G 

Modem Name RM520NGLAAR01A08M4G

IMEI ***** 

Active SIM Card SIM 1

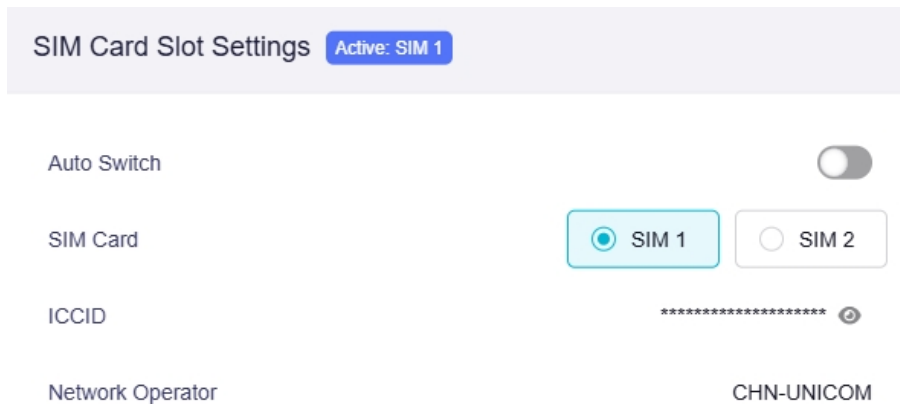
SIM Card Switch >

Data Used  24.67 MB >

Historical Signal Record Excellent >

SIM Card Settings >

It will display the auto switch button, the active SIM card, the ICCID and Network Operator.



SIM Card Slot Settings Active: SIM 1

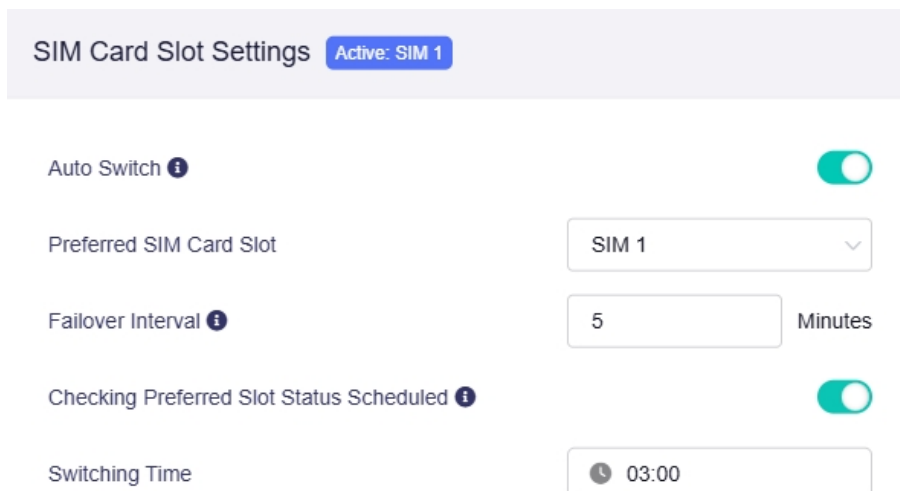
Auto Switch 

SIM Card ☒ SIM 1 ☐ SIM 2

ICCID ***** 

Network Operator CHN-UNICOM

If two SIM cards are inserted, you can enable **Auto Switch**.



SIM Card Slot Settings Active: SIM 1

Auto Switch  

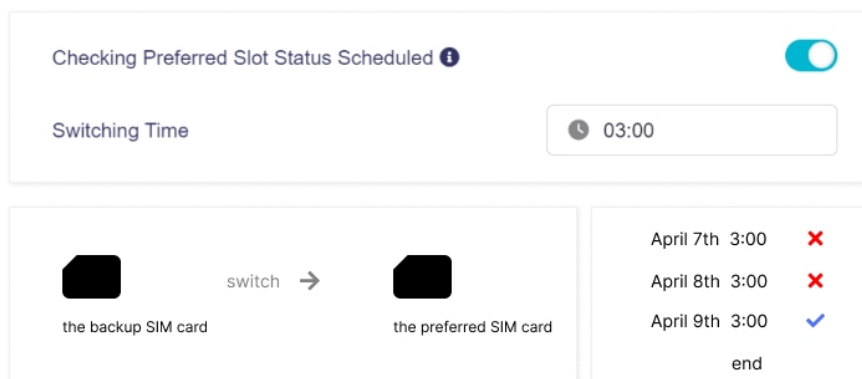
Preferred SIM Card Slot SIM 1 

Failover Interval  5 Minutes

Checking Preferred Slot Status Scheduled  

Switching Time  03:00

- **Auto Switch:** Enables automatic switching between SIM 1 and SIM 2. The network detection method for SIM Auto Switch is the same as the one configured on the Multi-WAN page.
- **Preferred SIM Card Slot:** Please set the preferred SIM card to SIM 1 or SIM 2.
- **Failover Interval:** Available values range from 5 minutes to 24 hours.
If the internet connection is still unavailable after a failover, the device will switch back to the preferred SIM slot and wait for this interval before retrying failover.
This option applies when both the preferred SIM card and the backup SIM card have no signal. The device will switch between SIM cards until one of them obtains a valid signal.
- **Checking Preferred Slot Status Scheduled**
When enabled, the device will check the preferred SIM slot daily at the configured time and attempt to switch back if the preferred SIM regains internet access.
This prevents the backup SIM from consuming excessive data. If the preferred SIM still has no signal, the device will continue using the backup SIM.



Note: The Auto Switch feature does not switch to another SIM card immediately. First, the device needs time to confirm that the current SIM cannot access the internet. Second, the other SIM is not in standby mode and requires time to activate.

4.2.4.4 Traffic Statistics

In the router's web admin panel, navigate to **INTERNET > Cellular**, then click **Data Used**.

● CHN-UNICOM 4G

...

Modem Name	RM520NGLAAR01A08M4G
IMEI	*****
Active SIM Card	SIM 1
SIM Card Switch	>
Data Used	24.75 MB >
Historical Signal Record	Excellent >
SIM Card Settings	>

[View More Information](#)

Disconnect

You will enter the **Traffic Statistics** page. It displays the used data of SIM card(s), and provides data limit settings.

Traffic Statistics

SIM 1 Data Used

23.89 MB [Modify](#)

SIM 2 Data Used

0.00 B [Modify](#)

Save data when power off

☐

SIM 1 Limit Settings

If you need to lock the SIM card based on data usage, turn on the "Save data when power off" switch.

SIM 2 Limit Settings

If you need to lock the SIM card based on data usage, turn on the "Save data when power off" switch.

If the Data Used exceeds the Data Cap Amount, please modify the **Data Cap Amount** or the **Data Used** manually. Otherwise, the network may be disconnected, or the SIM card may Auto Switch (for Dual-SIM models).

- **Modify the Data Used**

Click **Modify** on the right side of SIM 1/2 Data Used.

Traffic Statistics

SIM 1 Data Used ⓘ	23.89 MB	Modify
SIM 2 Data Used ⓘ	0.00 B	Modify
Save data when power off ⓘ	☐	

Then you can modify or reset the data used.

Modify SIM 1 Data

ⓘ The data statistics are for information only. Actual traffic is determined by your network operator and will appear on the bill provided by your network operator.

Data Used

24	MB	▼
----	----	---

[Cancel](#) [Save](#)

- **Set SIM data limit**

If you want to set the SIM data limit, enable **Save data when power off** first. It means the data can be saved even after the device is powered off.

Traffic Statistics

SIM 1 Data Used ⓘ	23.89 MB	Modify
SIM 2 Data Used ⓘ	0.00 B	Modify
Save data when power off ⓘ	☒	

Then enable the SIM 1 or SIM 2 Limit Settings.

Traffic Statistics

Save data when power off ⓘ

SIM 1 Limit Settings ⓘ

⚠ The SIM will switch when data cap is reached.

Enable

Data Cap Amount

GB

▼

Data Reset Period

Month

▼

Start Day ⓘ

Day 1

▼

Start Hour

00:00

▼

SIM 2 Limit Settings ⓘ

Enable

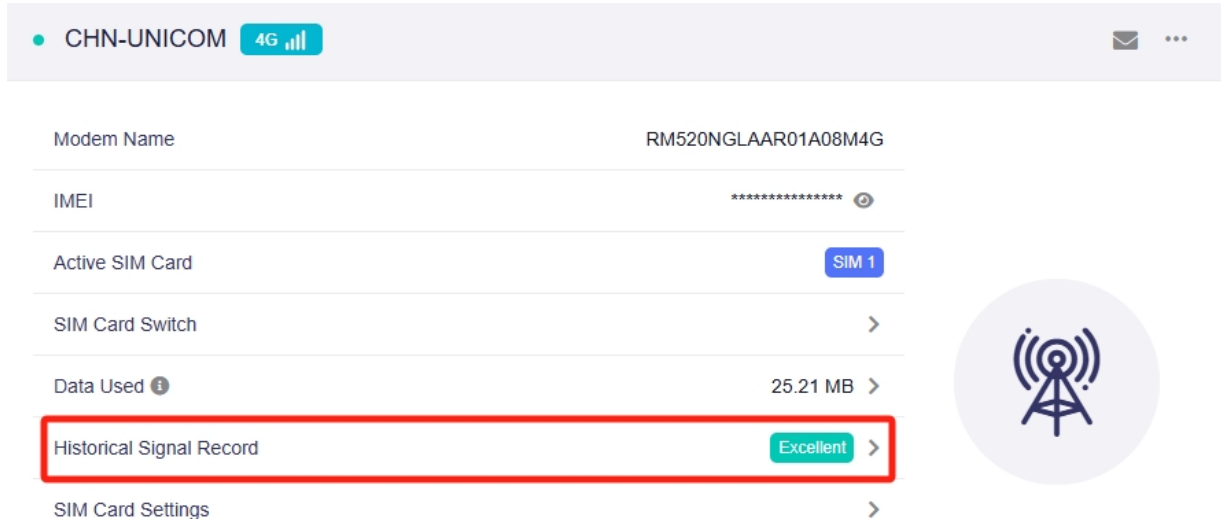
Cancel

Apply

For Dual-SIM models, we suggest enabling the **SIM Card Slot Auto Switch** at the same time. If the SIM 1 Data Cap Amount is set and the SIM Card Slot Auto Switch is enabled, SIM 1 will automatically switch to SIM 2 when it's data exceeds the Data Cap Amount and SIM 1 will be disabled.

4.2.4.5 Historical Signal Record

In the router's web admin panel, navigate to **INTERNET > Cellular**, then click **Historical Signal Record**.



CHN-UNICOM 4G

Modem Name: RM520NGLAAR01A08M4G

IMEI: *****

Active SIM Card: SIM 1

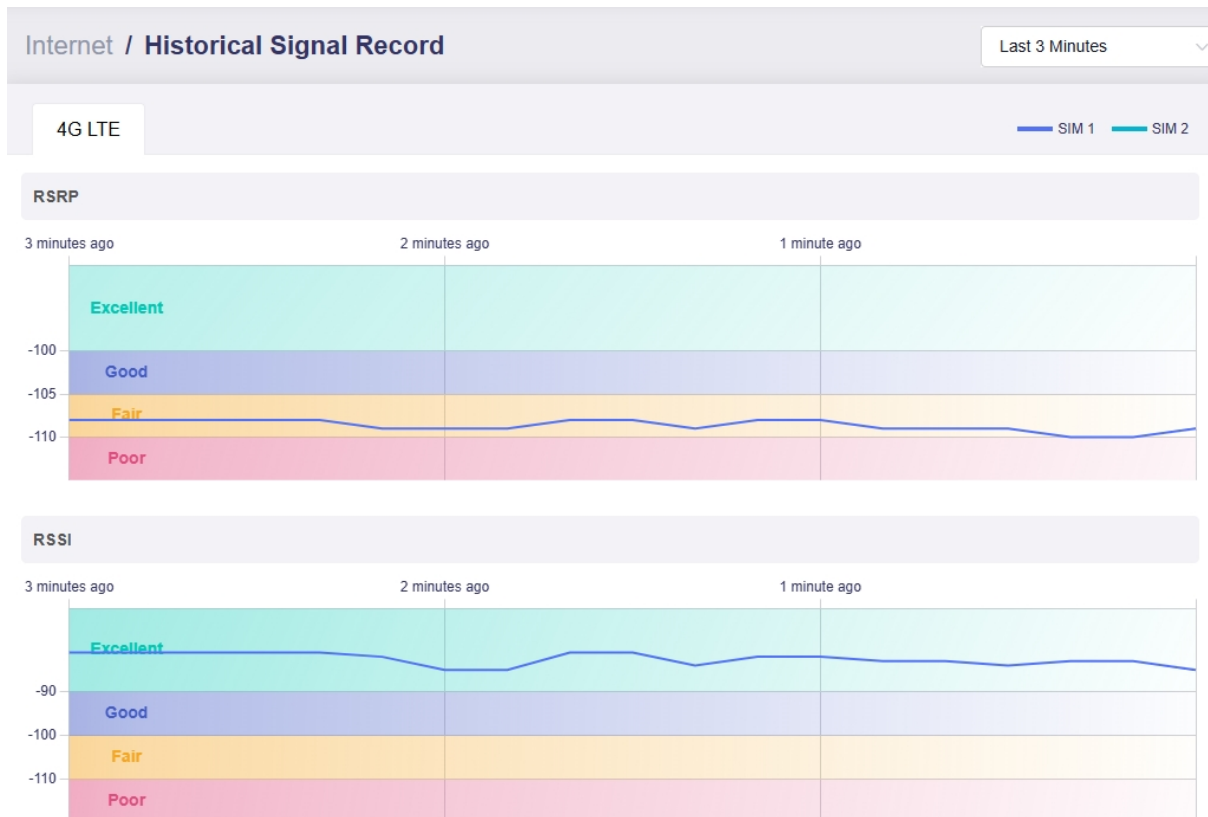
SIM Card Switch: >

Data Used: 25.21 MB >

Historical Signal Record Excellent >

SIM Card Settings: >

You can check the quality of your cellular connection here. If the signal is weak, try switching towers for a better signal.



View the signal strength history by selecting different time frames in the upper-right corner.

Internet / Historical Signal Record

Last 3 Minutes

4G LTE

RSRP

Last 3 Minutes

Last 10 Minutes

Last 30 Minutes

3 minutes ago

2 minutes ago

1 minute ago



4.2.4.6 Band Masking

Band Masking allows you to block specific bands or use only preferred cellular bands to improve weak cellular signal.

In the router's web admin panel, navigate to **INTERNET > Cellular > SIM Card Settings**, toggle on **Enable Band Masking**.

The screenshot displays the 'SIM Card Settings' page. At the top, there's a header 'SIM Card Settings'. Below it, several configuration fields are listed: Protocol (set to QCM), Port (set to /dev/cdc-wdm0), TTL (Optional), HL (Optional), MTU (1500), and Authentication (NONE). A red rectangular box highlights the 'Enable Band Masking' section. This section contains a toggle switch that is turned on, a 'Masking Mode' selector with 'Block' selected and 'Open' as an alternative, and three 'Select' buttons for 'LTE Bands', '5G NSA Bands', and '5G SA Bands'. At the bottom of the page, there are 'Cancel' and 'Apply' buttons.

Select the **Masking Mode** (Block or Open), then select the LTE Bands, 5G NSA Bands, and 5G SA Bands.

4.2.4.7 SMS & SMS Forwarding

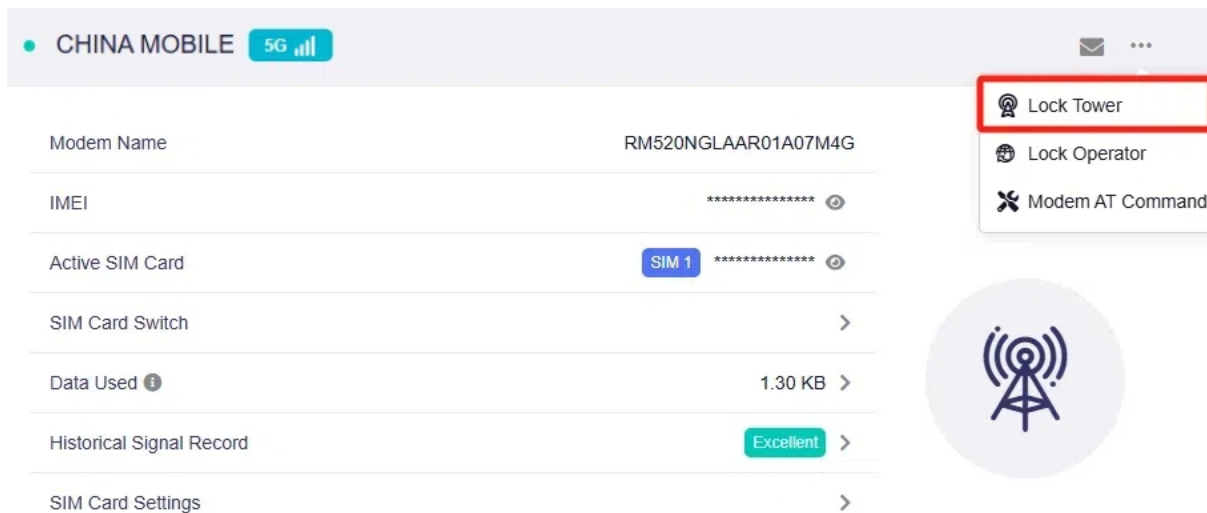
Please refer to [SMS](#) and SMS [Forwarding](#).

4.2.4.8 Lock Tower

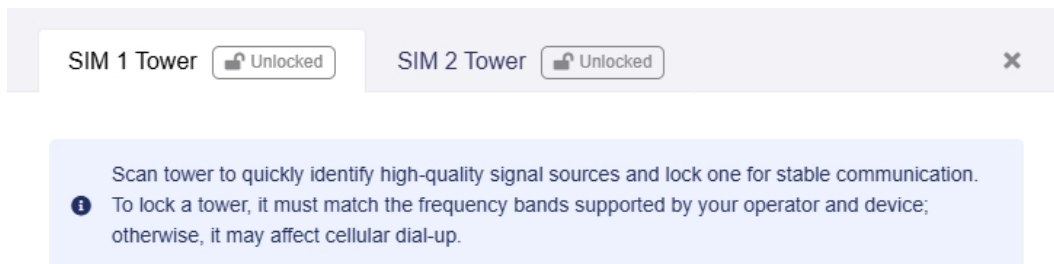
If you want to receive a high-quality signal and ensure a stable cellular connection, you can try locking tower.

Note: The locked tower must match the frequency bands supported by your carrier and device; otherwise, the connection may fail.

In the router's web admin panel, navigate to **INTERNET > Cellular**. Click the three-dot icon in the upper right, then select **Lock Tower**.



Click **Scan** to start scanning the cellular signal towers. It will take a few minutes. Do not refresh the page when scanning.



It will display the available towers.

SIM 1 Tower

Unlocked

SIM 2 Tower

Unlocked

×

Scan tower to quickly identify high-quality signal sources and lock one for stable communication.

i To lock a tower, it must match the frequency bands supported by your operator and device; otherwise, it may affect cellular dial-up.

Available Towers			Scan
	China Telecom 7602244D0 n1 106		NR5G
	China Unicom 7602244D0 n1 106		NR5G
	China Telecom 761BDA603 n5 79		NR5G
	China Mobile C1F6D0001 n41 273		NR5G
	China Broadnet C1F6D0001 n41 273		NR5G
	China Mobile C1EA6B005 n28 160		NR5G
	China Broadnet C1EA6B023 n28 160		NR5G
	China Telecom 424E290		LTE

Click a tower to view the details and lock onto it.

Network Type

NR5G

Network Operator

China Unicom

Cell ID

7602244D0

Band

n1

Bandwidth

106

SCS

15

TAC

76011A

PCI

952

RSRP

-62

Back

Lock

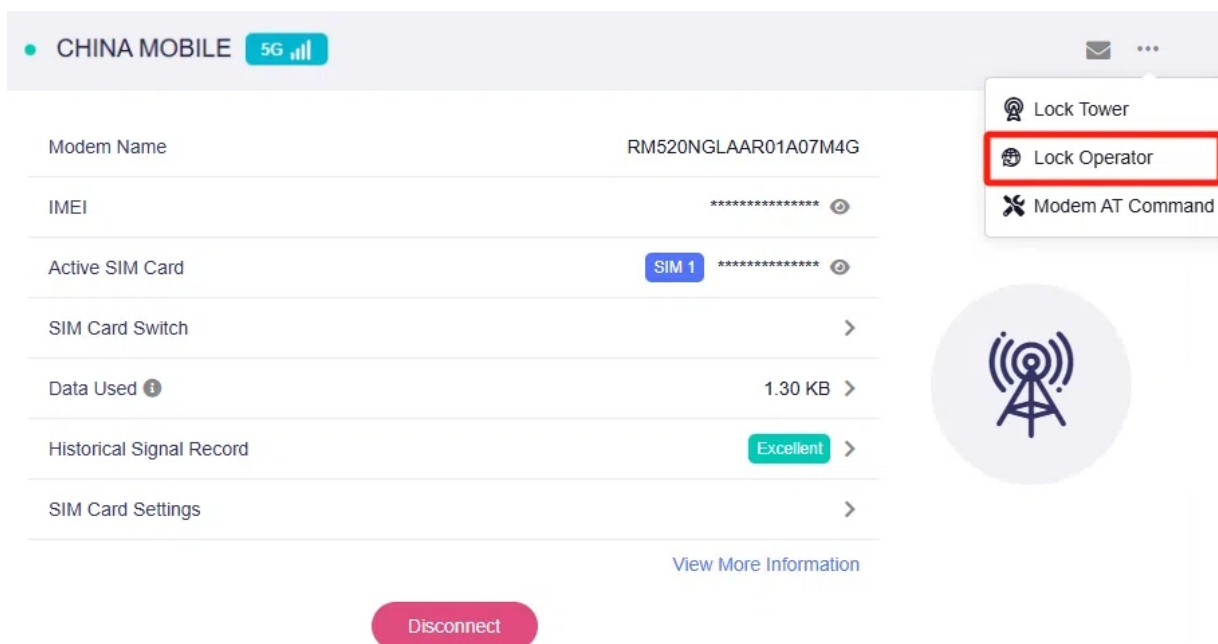
Note:

1. The device may not be able to scan all towers when the Cellular interface is enabled.
2. If the locked tower does not match the band masking or APN parameters in your cellular settings, the router will not be able to connect to the cellular network.
3. After locking a cell tower, if you move the router to another location, it will still attempt to reconnect to the locked tower after rebooting. This may prevent the router from connecting to the cellular network automatically at the new location. In this case, you need to either unlock the current cell tower, or manually lock it to a new tower.

4.2.4.9 Lock Operator

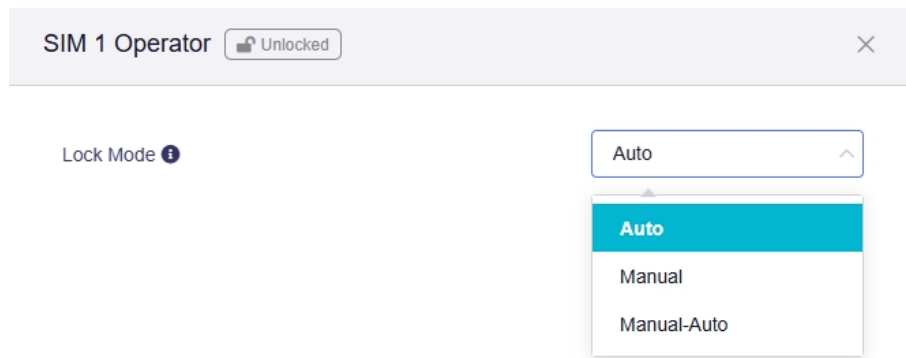
By locking to a specific mobile operator, the router will only use that operator's network, ensuring a stable connection and avoiding unintended roaming charges, especially in border areas where the device may otherwise connect to foreign networks.

In the router's web admin panel, navigate to **INTERNET > Cellular**. Click the three-dot icon in the upper right, then select **Lock Operator**.



There are three locking modes:

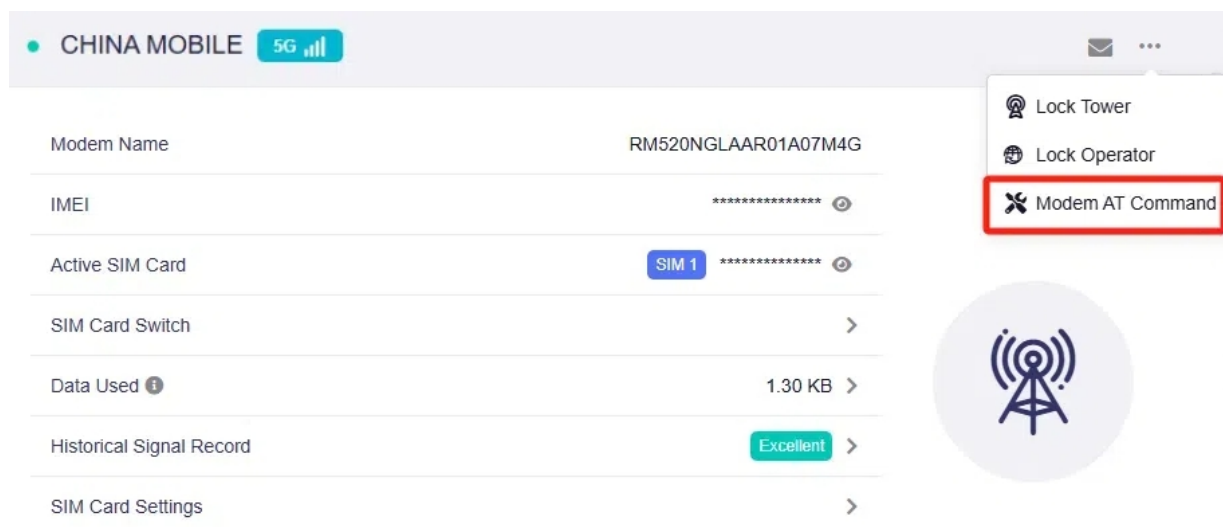
- **Auto:** Automatically connect to an available operator network.
- **Manual:** Manually lock onto a specific operator.
- **Manual-Auto:** Automatically switch to an available operator network if the manual lock fails.



4.2.4.10 Modem AT Command

Modem AT commands are standard instructions used to communicate with the cellular modem. With this feature, you can send commands and check the modem status.

In the router's web admin panel, navigate to **INTERNET > Cellular**. Click the three-dot icon in the upper right, then select **Modem AT Command**.



You will enter the AT Command page.

- **Manual command**

When Shortcut is set to Manual command, you can type your desired command in the AT Command field, and the results will be returned at the bottom gray box.

- **Preset command**

You can also click the Shortcut box and select a preset command from the drop-down list, such as Request IMEI, Check Signal Quality, Reset Modem, etc.

AT Command

Port

/dev/mhi_DUN

Shortcut

Manual command

AT Command

Manual command

Request IMEI

Request QCCID

Request IMSI

Check Signal Quality

Reset modem

Send

Export Debug Info

For example, select the shortcut "Request IMEI" and click "Send", then you will get the result as shown below.

AT Command

Port

/dev/mhi_DUN

Shortcut

Request IMEI

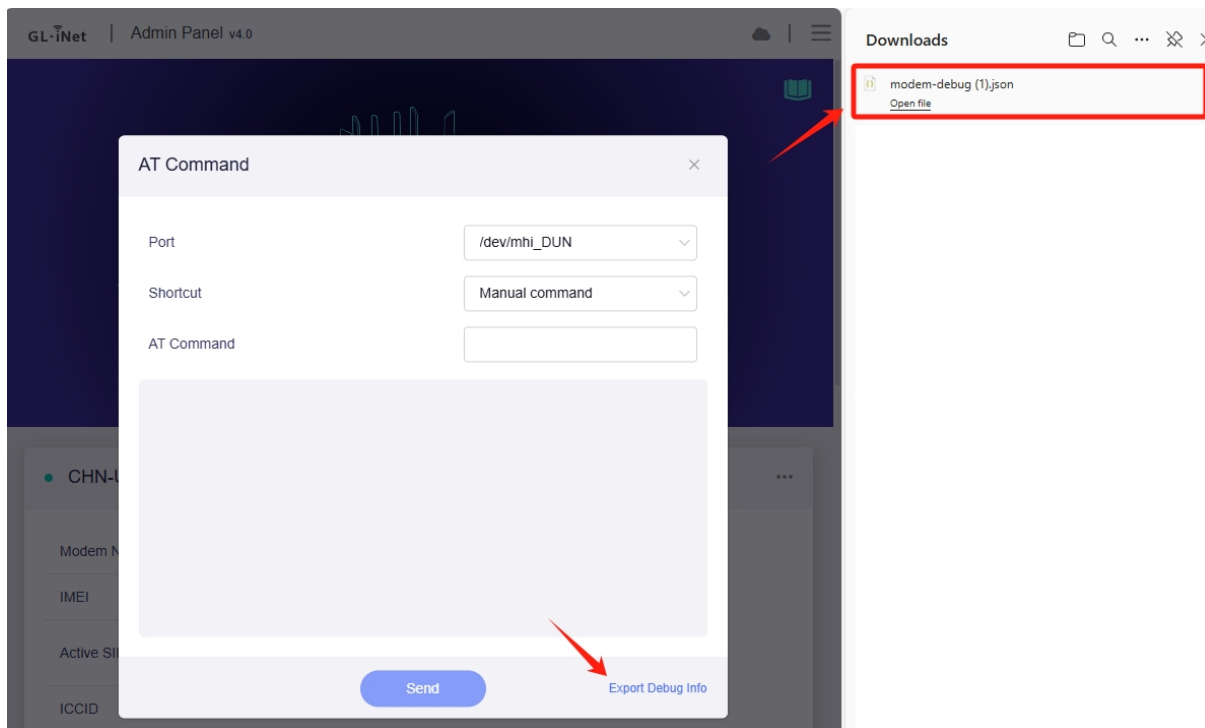
AT Command

AT+GSN

016442006183053

OK

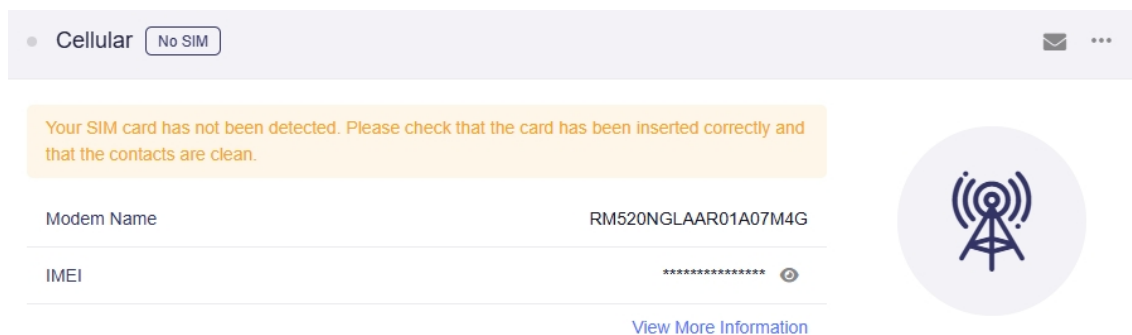
In the bottom right corner, you can click **Export Debug Info** to download a .json file.



4.2.4.11 Troubleshooting

If you fail to establish a cellular connection, choose the corresponding solution based on the following error message.

- **No SIM / Your SIM card has not been detected.**



Here are some suggestions.

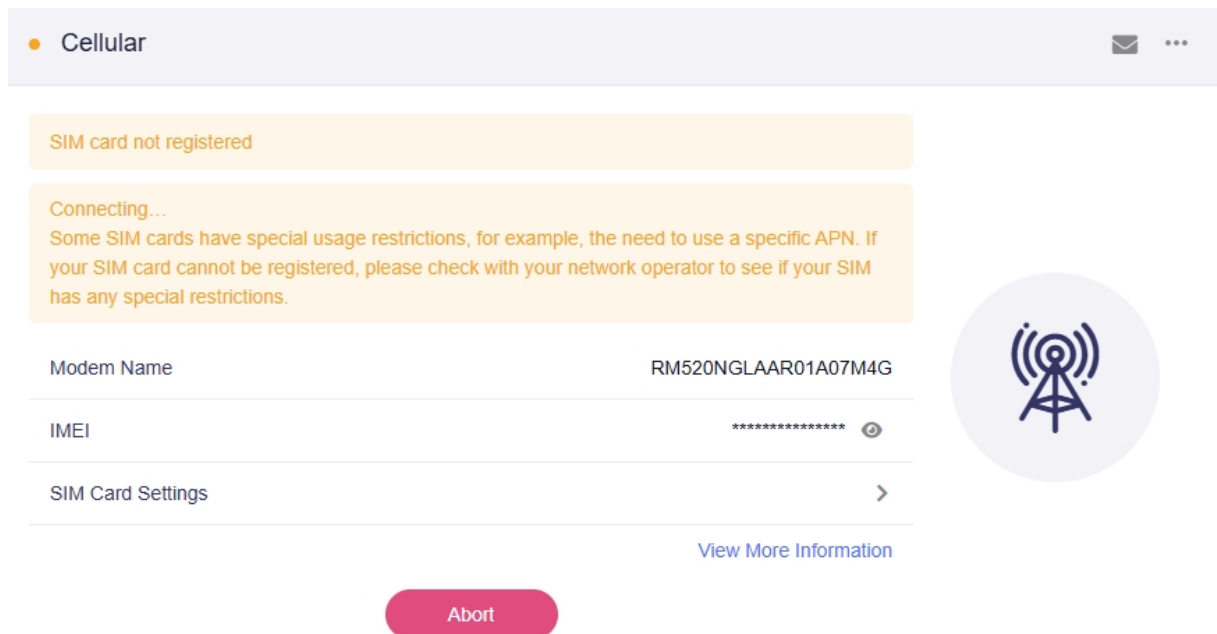
1. Refresh the page and wait a few minutes to check if the SIM card can be detected.
2. Ensure the SIM card is installed correctly. Align the notch on the SIM card with the corresponding mark on the card slot to confirm proper insertion orientation.
3. Power off the router, remove and reinsert the SIM card, then power the router back on.
4. Try using another SIM card if available.

If the issue persists, download the logs and send them to support@gl-inet.com.

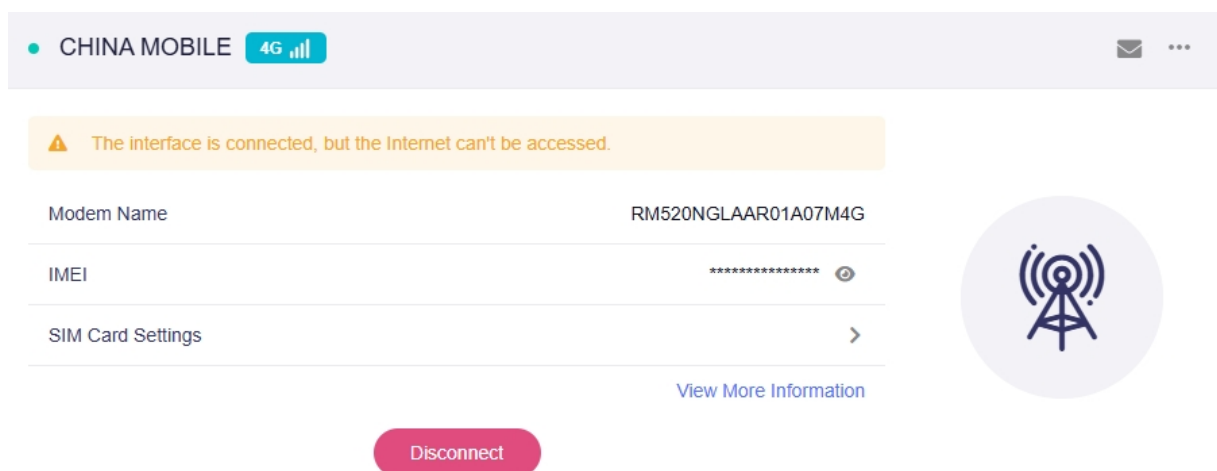
- **SIM card not registered / The Interface is connected, but the Internet can't be accessed.**

This issue has two types of error messages:

(1) SIM card not registered.



(2) The interface is connected, but the Internet can't be accessed.



Here are some suggestions.

1. Refresh the page and wait a few minutes to check if the error disappears.
2. Click **Disconnect/Abort**, then click **Connect** to try reconnecting.
3. Restart the router.

4. Verify the SIM card status and ensure it is activated. Test the SIM card by inserting it into a smartphone to confirm it can access the internet normally with an active mobile data plan, or contact your network carrier for verification.
5. Some network carriers may require a 3G protocol for network connection. Please go to **SIM Card Settings > Protocol**, select **3G**, then click **Apply**.

SIM Card Settings

⚠ Changing the configuration will result in redialing.

APN ⓘ

wbdata

IP Type ⓘ

IPv4

International Data Roaming

☒

Protocol

3G

Port ⓘ

3G

TTL ⓘ

QMI

HL ⓘ

QCM

Optional

MTU ⓘ

1500

Service

LTE/UMTS/GPRS

Dial number

Authentication

NONE

Enable Band Masking

☐

Cancel

Apply

The device will reconnect automatically. Wait a few minutes to check if the connection is successful.

6. Some SIM cards may have special usage restrictions (e.g., requiring a specific APN). If your SIM card fails to register, contact your carrier to check for any restrictions. If necessary, go to **SIM Card Settings > APN**, configure the correct APN on the router, then click **Apply**.

SIM Card Settings

APN ⓘ

wbdata

IP Type ⓘ

IPv4

International Data Roaming

☒

Protocol

QCM

Port ⓘ

/dev/cdc-wdm0

TTL ⓘ

Optional

HL ⓘ

Optional

MTU ⓘ

1500

Authentication

NONE

Enable Band Masking

☐

Cancel

Apply

7. Click **View More Information** to check the cellular signal strength. If the signal is weak, ensure the antenna is installed correctly. Move the router to an open and unobstructed location for better signal reception.
8. Check if **Band Masking** or **Lock Tower** is enabled. If so, disable them and try reconnecting.

If the issue persists, download the logs and send them to support@gl-inet.com.

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 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 displays the router's 2.4GHz and 5GHz Wi-Fi settings, with each further divided into main Wi-Fi and guest Wi-Fi networks for flexible management.

5.2.1 5GHz Wi-Fi

The 5GHz Main Wi-Fi allows you to configure multiple settings, including enabling/disabling Wi-Fi, setting TX power, enabling/disabling randomized BSSID, setting Wi-Fi name (SSID), security, password, SSID visibility, mode, bandwidth, and channel.

● 5 GHz Wi-Fi

● 5 GHz Guest Wi-Fi

Enable Wi-Fi

ON

TX Power

Max

Wi-Fi Name (SSID)

GL-X3000-a0b-5G

Enable Randomized BSSID ⓘ

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Wi-Fi Mode

11a/n/ac/ax

Bandwidth

80 MHz

Channel ⓘ

Auto

The 5GHz Guest Wi-Fi allows you to configure simplified settings, including enabling/disabling Wi-Fi, setting Wi-Fi name (SSID), security, password, and SSID visibility.

● 5 GHz Wi-Fi

● 5 GHz Guest Wi-Fi

Enable Wi-Fi OFF

Wi-Fi Name (SSID)	GL-X3000-a0b-5G-Guest
Wi-Fi Security	WPA2-PSK
Wi-Fi Password	
SSID Visibility	Shown

Note:

1. **Randomized BSSID** is enabled by default. It aims to prevent the client vendors from collecting nearby Wi-Fi BSSIDs and client devices' GPS coordinates to their servers.
2. The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.
3. When **Channel** is set to **Auto**, the router's Wi-Fi will not automatically switch to the DFS channel.
4. When the **Bandwidth** is set to **160 MHz** (Only available on some models), the Wi-Fi will always use the DFS channel, even if you select a non-DFS channel or set it to Auto.

5.2.2 2.4GHz Wi-Fi

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

● 2.4 GHz Wi-Fi

● 2.4 GHz Guest Wi-Fi

Enable Wi-Fi

ON

TX Power

Max

Wi-Fi Name (SSID)

GL-X3000-a0b

Enable Randomized BSSID ⓘ

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Wi-Fi Mode

11g/n/ax

Bandwidth

20/40 MHz

Channel

Auto

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

● 2.4 GHz Wi-Fi

● 2.4 GHz Guest Wi-Fi

Enable Wi-Fi OFF

Wi-Fi Name (SSID)	GL-X3000-a0b-Guest
Wi-Fi Security	WPA2-PSK
Wi-Fi Password	
SSID Visibility	Shown

Note:

1. **Randomized BSSID** is enabled by default. It aims to prevent the client vendors from collecting nearby Wi-Fi BSSIDs and client devices' GPS coordinates to their servers.
2. The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.
3. When **Channel** is set to **Auto**, the router's Wi-Fi will not automatically switch to the DFS channel.

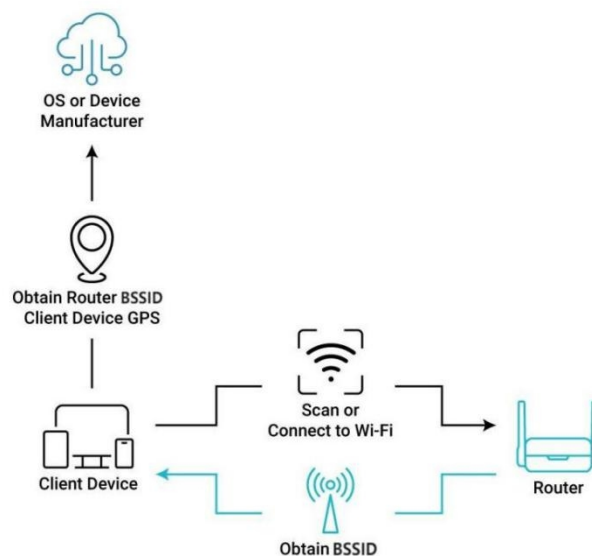
5.2.3 Randomized BSSID

Randomized BSSID aims to prevent the client vendors from collecting nearby Wi-Fi BSSIDs and client devices' GPS coordinates to their servers.

How Client Vendors Collect Location Data

Client vendors usually collect the geographical location data of Wi-Fi access points by leveraging their unique BSSIDs to locate devices. When client devices (e.g., mobile phones, computers) scan or connect to a router:

- If other devices are within the router's Wi-Fi signal coverage, their location and movement trajectories may be exposed.
- If a device uses GPS for positioning, it periodically uploads nearby Wi-Fi BSSIDs and corresponding GPS coordinates to the vendor's server.



Security Risks of Crowdsourced Tracking

Even devices without GPS (or with GPS disabled) can estimate their location by querying visible BSSID info. However, this crowd-sourced location tracking system has security vulnerabilities. Attackers can use it to accumulate a global database of Wi-Fi access point locations and continuously track the movement trajectories of devices, posing a threat to user privacy and security.

How Randomized BSSID Protects Your Privacy

To address these vulnerabilities, GL.iNet routers implement the Randomized BSSID feature as a privacy safeguard.

In the router's web admin panel, go to **WIRELESS** -> **5GHz Wi-Fi** or **2.4GHz Wi-Fi**, the BSSID option is enabled by default. With this setting, the device uses a randomly generated BSSID and renews it each time it boots. If you disable the random BSSID, the router reverts to using the real MAC address.

Note: For Guest Wi-Fi, the BSSID remains consistent with the Main Wi-Fi BSSID within the same frequency band.

Chapter 6

Clients

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

6.1 Device Details

Log in to your router's web admin panel and go to **CLIENTS**.

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

Clients

Access Control: [Blocklist](#) ⓘ

Sort by Default ⚙

Online Clients (2) ^

Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
 GL-INET-08 self	 192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 62.95 KB/s ↑ 4.30 KB/s	↓ 22.65 MB ↑ 3.58 MB	☐	☐	...
 iPhone	 192.168.8.147 3A:2C:39:XX:XX:XX ⓘ	↓ 72.16 KB/s ↑ 8.70 KB/s	↓ 23.49 MB ↑ 3.13 MB	☐	☐	...

Offline Clients (1) ^

Name	IP + MAC	Speed	Traffic	Reserved IP ⓘ	Block	Action
 GL-INET-08	 192.168.8.191 74:13:EA:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 0.00 B ↑ 418.00 B	☐	☐	...

Tip: Online Clients refer to devices currently connected to the router's network. Offline Clients refer to devices that have previously connected to the router but are now disconnected from the network.

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.

Clients

Access Control: Blocklist

Sort by Default

Online Clients (2)

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 9.16 KB/s ↑ 2.05 KB/s	↓ 10.00 MB ↑ 1.22 MB			...
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX	↓ 97.00 B/s ↑ 52.00 B/s	↓ 89.68 KB ↑ 66.34 KB			...

Access Control

Mode

Blocklist

Blocklist

Blocklist

Allowlist

Self MAC

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

Cancel

Apply

- **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' management interface. At the top, there's a header 'Clients' with a sub-header 'Access Control: Blocklist' and a 'Sort by Default' button. 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 'iPhone'. The 'GL-INET-08' client's 'Action' column has a dropdown menu open, showing options: 'View Details' (highlighted with a red box), 'Modify', and 'Limit Speed'.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08 self	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 11.12 KB/s ↑ 3.12 KB/s	↓ 10.38 MB ↑ 1.43 MB	☐	☐	...
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 89.68 KB ↑ 66.34 KB	☐	☐	...

Clients / Client Details

● GL-INET-08 self

Hostname	Unknown
Connection Method	Ethernet
MAC	6C:1F:F7:XX:XX:XX
Speed	↓ 960.00 B/s ↑ 1.05 KB/s
Traffic	↓ 10.55 MB ↑ 1.62 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 a 'Sort by Default' button. Below this is a section for 'Online Clients (2)'. A table lists two clients: 'GL-INET-08' and 'iPhone'. The table columns are Name, IP + MAC, Speed, Traffic, Reserved IP, Block, and Action. The 'Action' column for the 'iPhone' client shows a three-dot menu with options: 'View Details', 'Modify' (highlighted with a red box), and 'Limit Speed'.

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

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 2.57 KB/s ↑ 1.52 KB/s	↓ 10.40 MB ↑ 1.45 MB	☐	☐	...
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 89.68 KB ↑ 66.34 KB	☐	☐	View Details Modify Limit Speed

Modify Client Device

Name: Auto

Device Type: Optional

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

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 the 'Access Control: Blocklist' tab selected. Under 'Online Clients (2)', there are two entries: 'GL-INET-08' and 'iPhone'. The 'iPhone' entry is selected, and its 'Action' column dropdown menu is open, showing options: 'View Details', 'Modify', and 'Limit Speed' (which is highlighted with a red box).

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 2.38 KB/s ↑ 1.30 KB/s	↓ 10.42 MB ↑ 1.45 MB	☐	☐	...
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 89.68 KB ↑ 66.34 KB	☐	☐	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 is shown. It has two sections: 'Download' and 'Upload'. Each section has a text input field set to 'Unlimited' and a unit dropdown menu set to 'KB/s'. At the bottom, there are 'Cancel' and 'Apply' buttons.

Download: Unlimited KB/s

Upload: Unlimited KB/s

Buttons: Cancel, Apply

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

The screenshot shows the 'Clients' interface after applying the speed limit. The 'iPhone' entry now shows yellow arrows in the 'Speed' column, indicating the limit is applied. The 'Limit Speed' option is highlighted with a red box.

Name	IP + MAC	Speed	Traffic	Reserved IP	Block	Action
GL-INET-08	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 2.32 KB/s ↑ 3.51 KB/s	↓ 11.03 MB ↑ 2.27 MB	☐	☐	...
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX	↓ 42.03 KB/s ↑ 2.97 KB/s	↓ 7.97 MB ↑ 975.65 KB	☐	☐	...

6.3 Remove Clients

In the **Offline Clients** section, you can click **Delete All** in the top right corner to delete all offline clients. If you want to remove a specific client, click the three-dot icon in the **Action** column, then click **Remove Client** from the drop-down menu.

Offline Clients (3) ^

[Delete All](#)

Name	IP + MAC	Speed	Traffic	Reserved IP ⓘ	Block	Action
GL	192.168.8.218 	↓ 0.00 B/s ↑ 0.00 B/s	↓ 22.48 KB ↑ 19.77 KB			...
Unknown	192.168.8.176 	↓ 0.00 B/s ↑ 0.00 B/s	↓ 160.97 KB ↑ 187.30 KB			View Details Modify Limit Speed Remove Client
iPhone	192.168.8.223 	↓ 0.00 B/s ↑ 0.00 B/s	↓ 215.60 MB ↑ 17.04 MB			

6.4 Sort

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

Clients Access Control: Blocklist ⓘ

Sort by Default

Online Clients (2) ^

Name	IP + MAC	Speed ⓘ	Traffic	Reserved IP ⓘ	Block	Action
GL-INET-08	192.168.8.225 6C:1F:F7:XX:XX:XX	↓ 1.26 KB/s ↑ 1.32 KB/s	↓ 11.26 MB ↑ 2.52 MB			
iPhone	192.168.8.147 3A:2C:39:XX:XX:XX ⓘ	↓ 0.00 B/s ↑ 0.00 B/s	↓ 7.97 MB ↑ 975.65 KB			Default Name IP Upload Speed Download Speed Host/Guest Network Clear Traffic Statistics Toggle Rate Unit

The default sorting rules are as follows:

- The self device (i.e., the device used to access the router's web admin panel) is always listed first.
- In the **Online Clients** section, devices are listed higher if they connected earlier.
- In the **Offline Clients** section, devices are listed higher if they disconnected earlier.

Chapter 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.

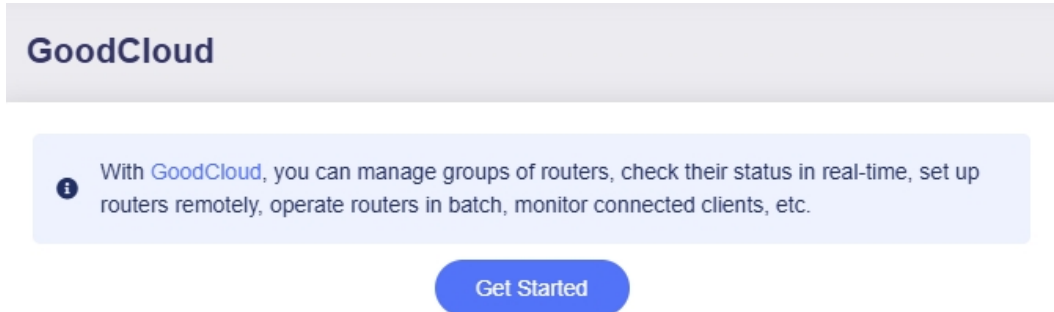
With GoodCloud, you can:

- 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

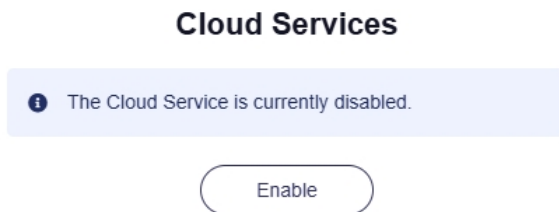
Some features are available in Enterprise Plan and VAR (Value Added Reseller) Plan. See [here](#) for details.

7.1.1 Enable GoodCloud

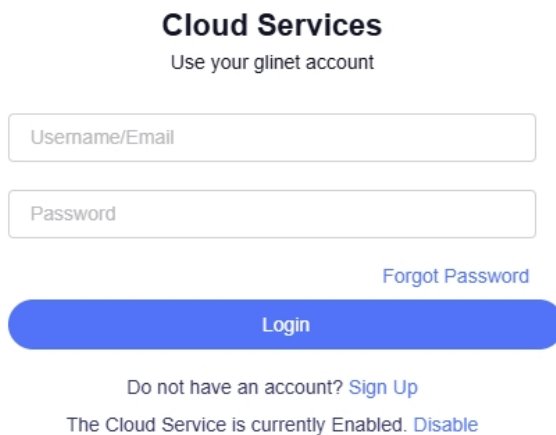
1. Log in to your router's web admin panel, go to **CLOUD SERVICE > GoodCloud**, and click **Get Started**.



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



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



Tips:

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

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



Cloud Services

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

Device ID: *****

Device MAC: *****

Device S/N: ***** 

[Go To GoodCloud](#) →

5. Navigate to **CLOUD SERVICES > GoodCloud** and enable remote access. GoodCloud provides remote access to the bound router's web admin panel and terminal. You can enable or disable the remote access for your router here.

 With Cloud Service, 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 the router's web admin panel from GoodCloud via HTTP/HTTPS.
- **View Logs:** Redirect to the Log page and display Cloud log.

7.1.2 Manage Your Router

7.1.2.1 Check Device Details

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

Q

Name / MAC / IP / SN / IMEI

Filter

Name ▾

Status ▾

Model

Version ▾

MAC

IP

x3000 a0b

Online

X3000

4.8.3

94:83:C4:XX:XX:XX

183.178.10.100

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.

Bound Devices / Edit Device

x3000_a0b Online

Basic Info



X3000

Network Mode
Router

MAC Address
94:83:C4:XX:XX:XX

SN
a71e*****5662

Compile Time
2025-11-06 12:14:12

Version
4.8.3

IP
183.178.10.100

Memory Usage
49%

Up Time
0 days 8 hrs 41 mins

Statistical Data

Network Latency ⓘ

 **Poor**

231.05 ms

0.27 ms

0 %

Latency

Jitter

Packet Loss

Device Status History [More](#)



09/24/2026 00:00 09/24/2026 18:56

Online Offline

Network Clients List Share Cellular Health

Internet

Ethernet1 WAN [More](#)

✓ Connected

IP Address 10.100.209.213

Protocol DHCP

Repeater [More](#)

✓ Connected

IP Address 192.168.0.169/24

SSID GL-BE9300-b3...

Tethering [More](#)

⊙ Disconnect

IP Address --

Device List [Details](#)

Cellular SIM2 [More](#)

⊙ Disconnect

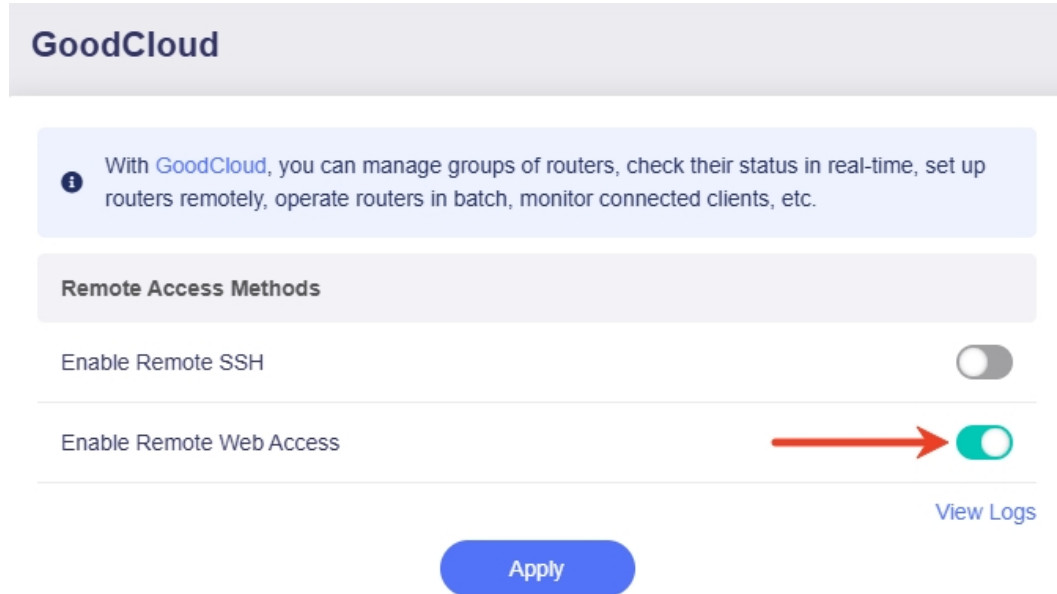
Operator --

ICCID --

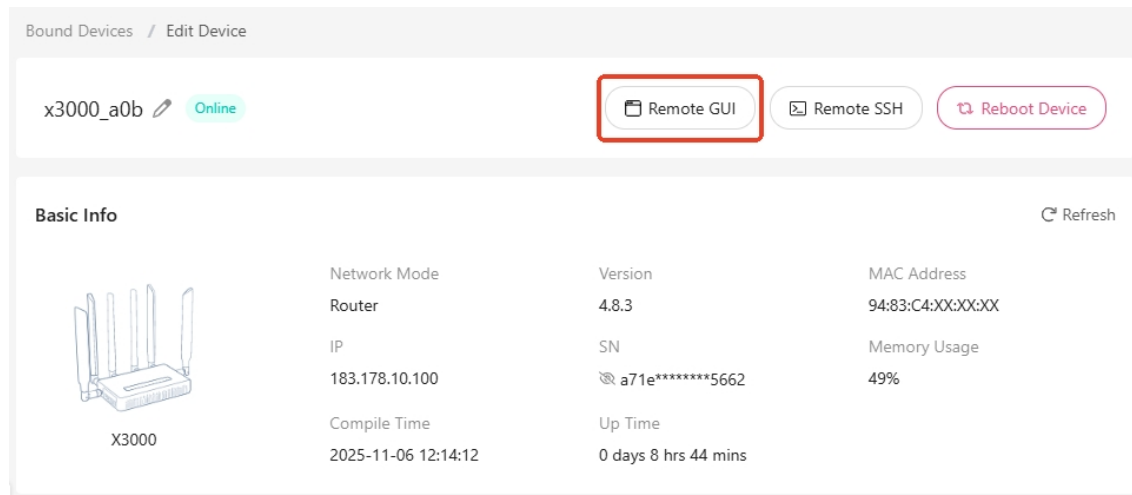
85

7.1.2.2 Remote Web Access

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

Remote GUI

☒ HTTP ☐ HTTPS

* Port

80

Cancel

Apply

Remote GUI

☐ HTTP ☒ HTTPS

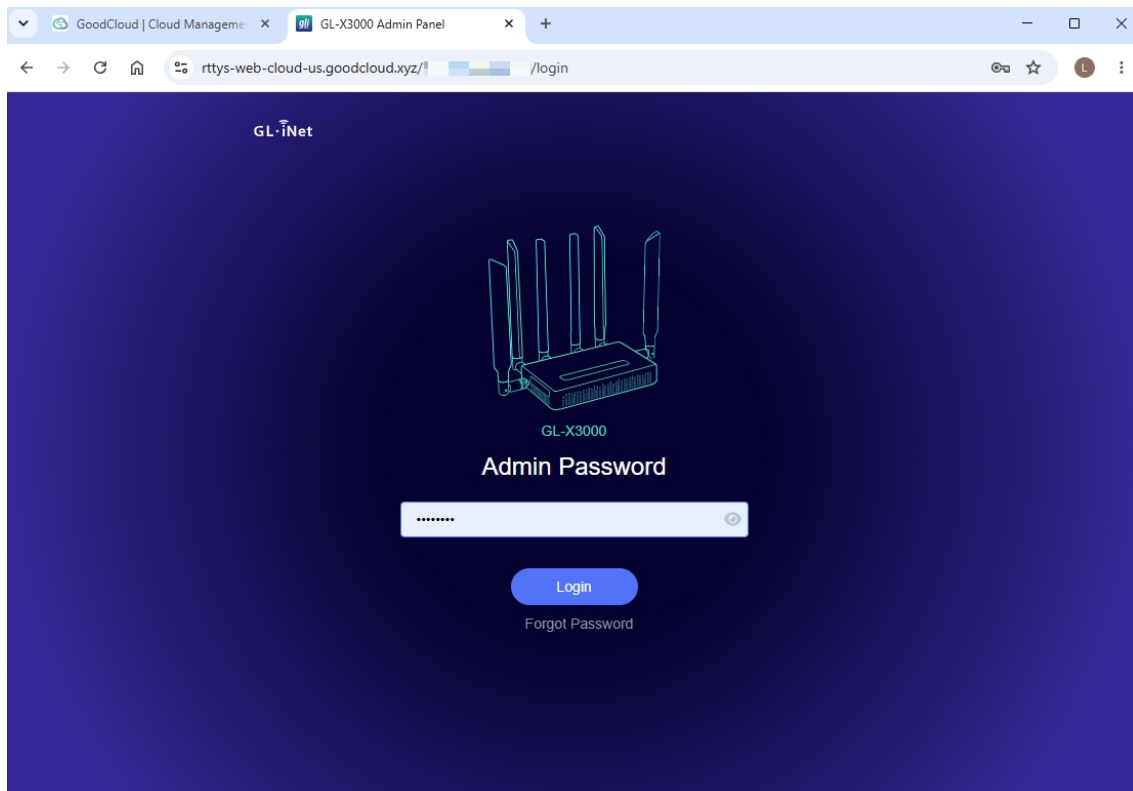
* Port

443

Cancel

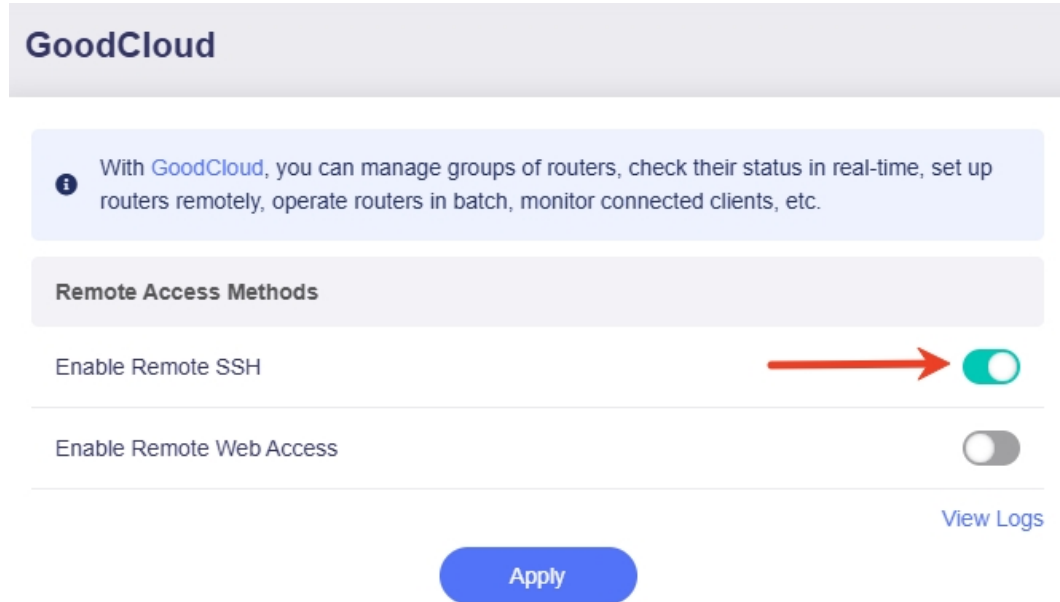
Apply

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

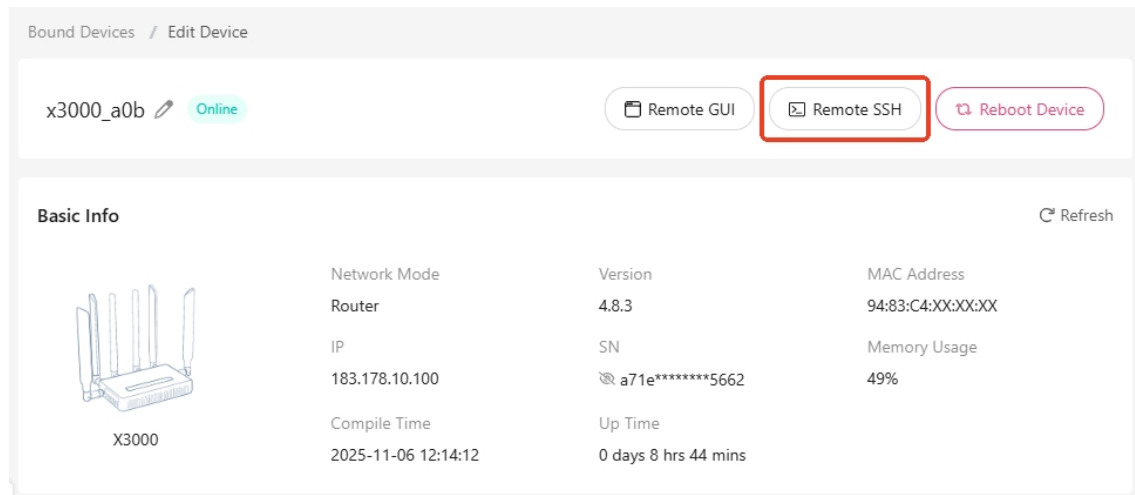


7.1.2.3 Remote SSH

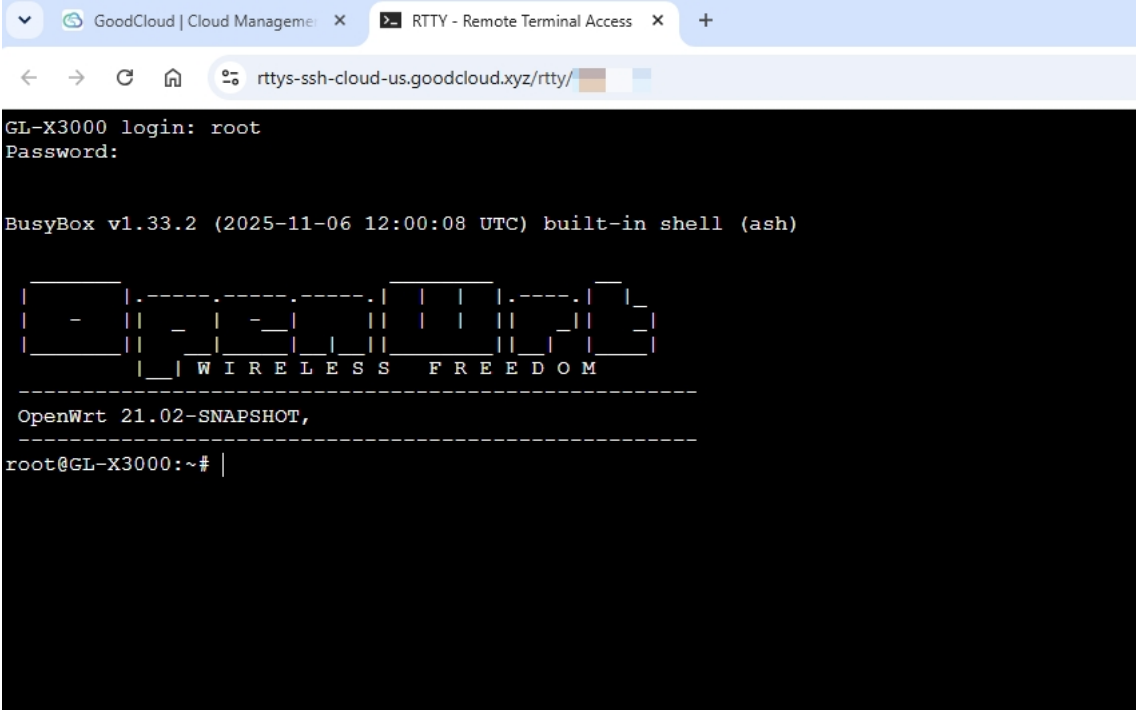
1. Log in to the router's web admin panel, navigate to **CLOUD SERVICES > GoodCloud**, enable **Remote SSH**, then click **Apply**.



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

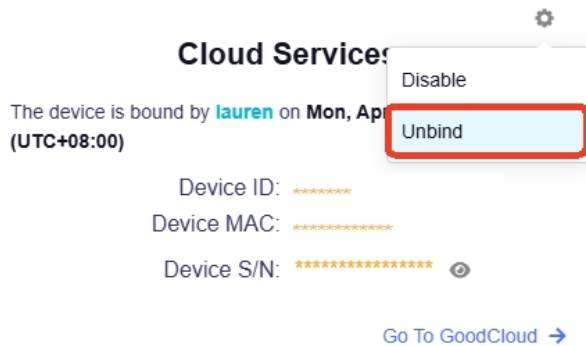


4. Log in as **root** and input the password to access the terminal of your router.

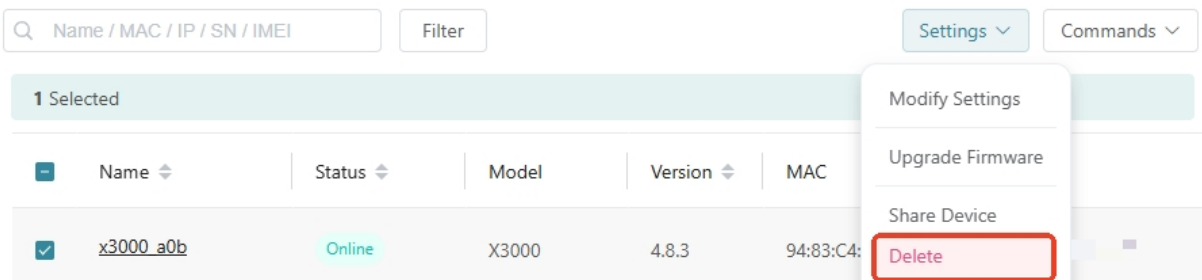


7.1.3 Unbind Device

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.

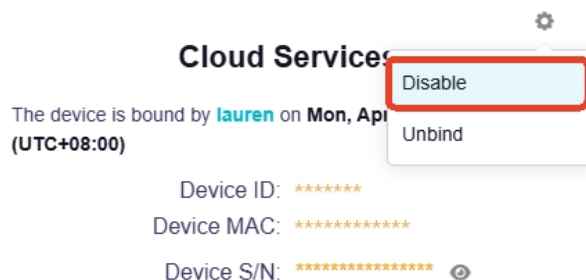


Alternatively, log in to the Cloud platform and navigate to **Device > Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



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 platform designed to seamlessly connect multiple GL.iNet routers into a unified network, enabling effortless remote access. With flexible networking capabilities, user-friendly configuration and robust privacy protection, AstroWarp delivers secure and reliable connectivity at all times. Whether for remote work or secure access to internal corporate resources across multiple sites, AstroWarp is your ideal solution for high-performance, protected networking.

Log in to your router's web admin panel, go to **CLOUD SERVICE > AstroWarp** and click **Get Started**. Then follow the instructions to set up your network. Please refer to astrowarp.net for details.

AstroWarp

i When AstroWarp is enabled, functions such as Tor, ZeroTier, Tailscale, Network Mode cannot be used.



Get started for Work From Home that you can access internet and servers using this router as internet exit with its WAN IP wherever you are.

1. Download AstroWarp app on your mobile phone or PC.
2. Click the button to set this router as your internet exit node.
3. Use app to scan or enter the code at the exit node page.
4. You're connected!

Get Started

Install the app to get started



MacOS



Windows



iOS



Android

Chapter 8

Get To Know VPN

This chapter introduces VPN concepts and common use scenarios.

8.1 Introduction

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 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.

*WireGuard® is a registered trademark of Jason A. Donenfeld.

8.2 Application Scenarios

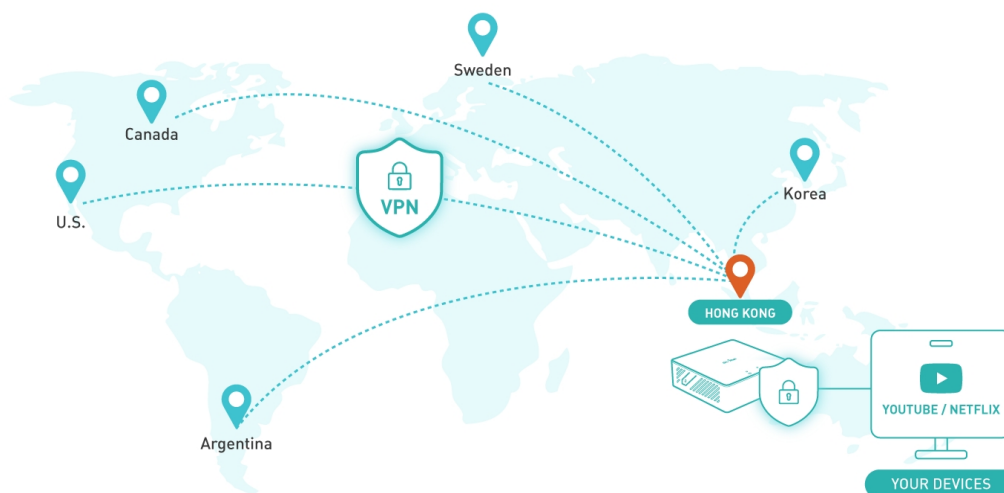
1. Personal Data Privacy

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.



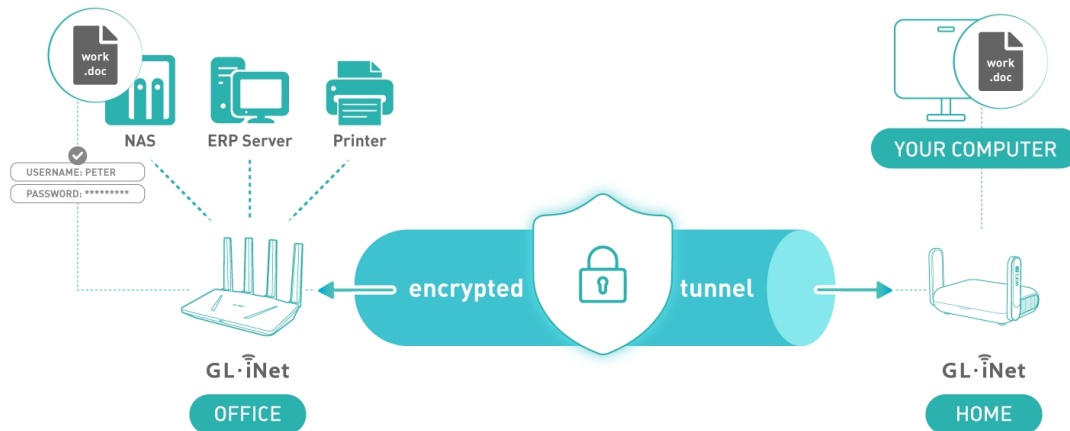
2. Unrestricted Access Worldwide

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.



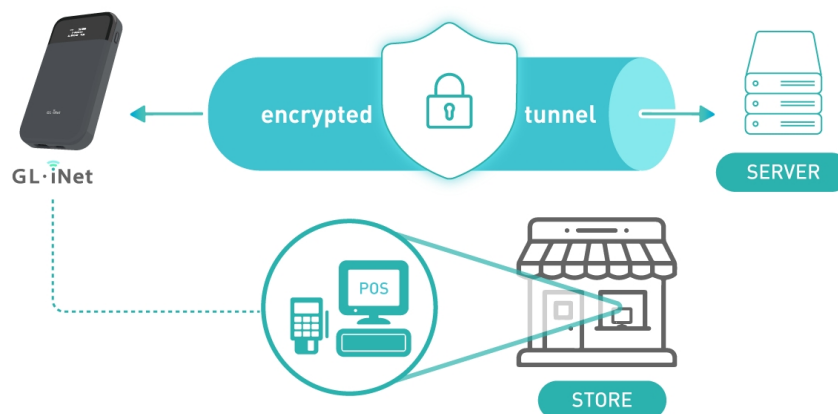
3. Small Business Data Security

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

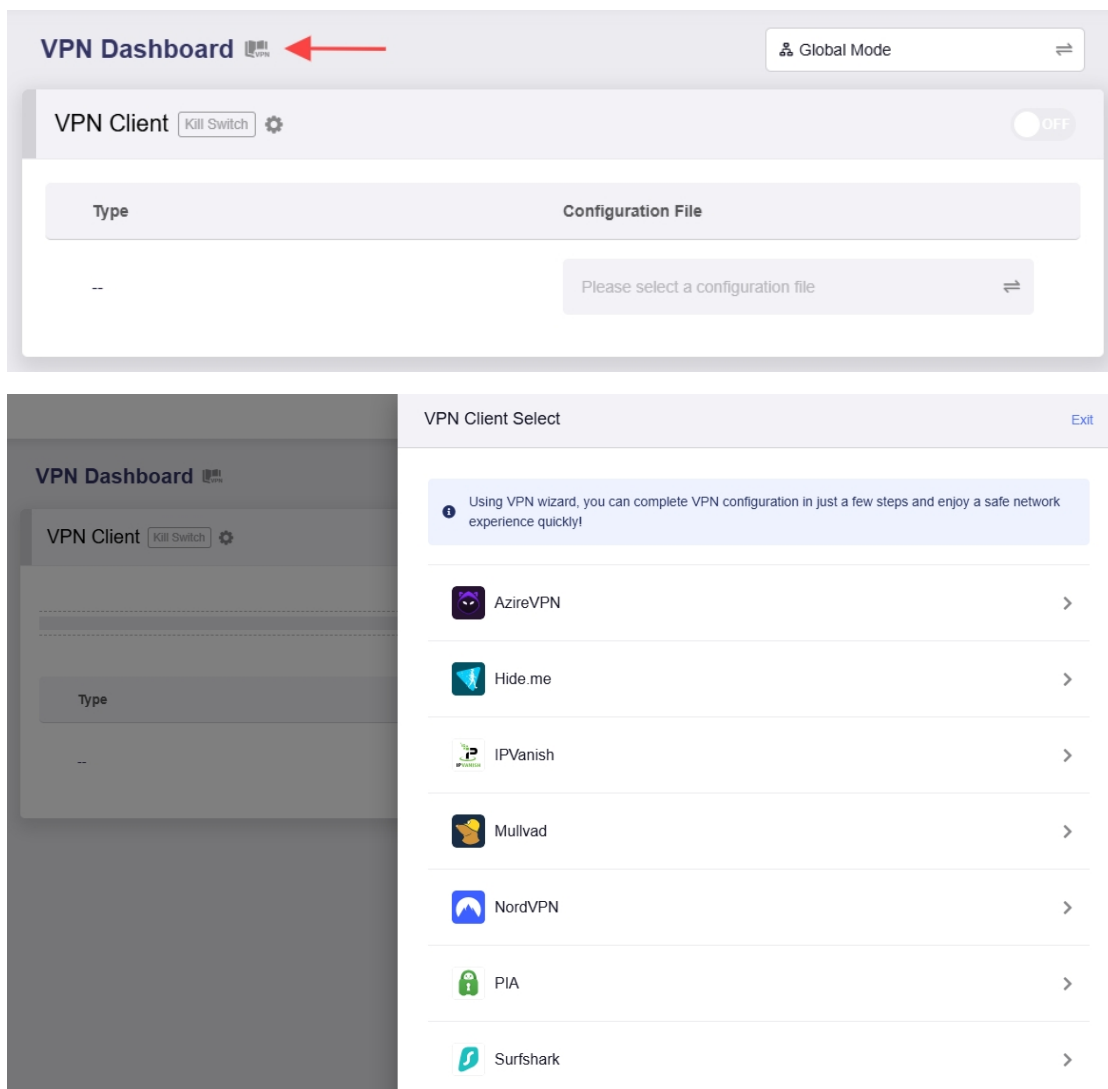
This chapter introduces how to manage VPN connections via the web admin panel.

Log in to your router's web admin panel, and go to **VPN > VPN Dashboard**.

The VPN dashboard displays VPN connection details, such as tunnel rules, server address, 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. You can also activate multiple VPN connections for multi-tunnel scenarios.

9.1 VPN Setup Wizard

To begin with, click the book icon in the upper left corner and follow the VPN Setup Wizard to complete the VPN configuration quickly.



Note: The VPN Setup Wizard is only for the integrated VPN services, including AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA and Surfshark. For other VPN providers, skip the wizard and go to **VPN > OpenVPN Client** or **WireGuard Client** to set up VPN manually.

Here's an example with **Hide.me**. Log in with Hide.me credentials.



Username

Password

Select a VPN server and click **Apply**. This is the server you will connect to, and your public IP address will appear to be from the selected server's location.

Server Address

☐ atlanta-v4.hideservers.net	☐ au-v4.hideservers.net
☐ bd-v4.hideservers.net	☐ be-v4.hideservers.net
☐ berlin-v4.hideservers.net	☐ bg-v4.hideservers.net
☐ bordeaux-v4.hideservers.net	☒ boston-v4.hideservers.net
☐ br-v4.hideservers.net	☐ ca-v4.hideservers.net
☐ calgary-v4.hideservers.net	☐ ch-v4.hideservers.net
☐ cl-v4.hideservers.net	☐ co-v4.hideservers.net

It will connect automatically. Once connected, go to the **VPN Dashboard**. You will see that a VPN tunnel has been enabled, displaying details including the VPN protocol (e.g., WireGuard), configuration file, server address, server listen port, traffic statistics, and the client virtual IP address. You can also view the connection logs in the lower right corner.

VPN Dashboard

Global Mode

VPN Client

Kill Switch

ON

Type	Configuration File
WireGuard	United States / Boston

Server Address

boston-v4.hideservers.net

Server Listen Port

432

Traffic Statistics

↑ 71.77 KB / ↓ 121.76 KB

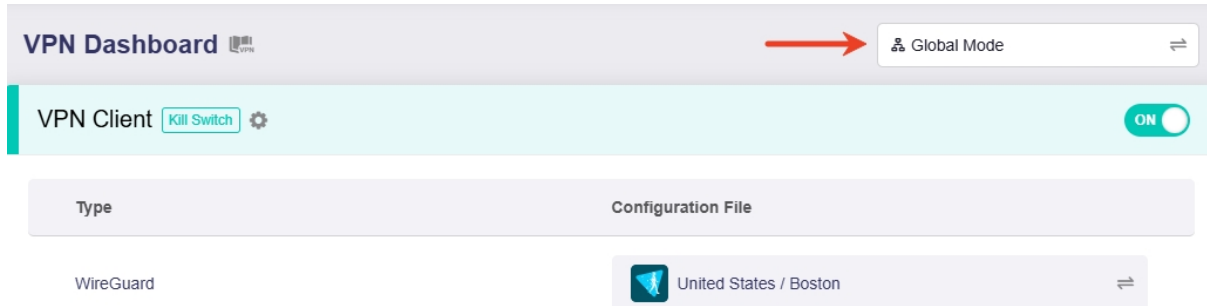
Client Virtual IP (IPv4)

10.55.20.79

View Log

9.2 VPN Mode

On the VPN Dashboard, click the button in the upper right corner to switch VPN modes if required.



Two modes are available: **Global Mode** and **Policy Mode**.

Switch VPN Mode

☒ **Global Mode**
If the VPN is connected, all traffic will be routed through the VPN. Only one VPN client instance can be activated.

☐ **Policy Mode**
This mode supports advanced customization, enabling the configuration and activation of multiple VPN servers on a single device, along with the execution of complex policy logic.

Cancel

Apply

9.2.1 Global Mode

In this mode, all traffic will be routed through the VPN tunnel, and only one VPN client instance can be activated. It is ideal for scenarios requiring all device traffic to pass through a single VPN server, such as unified network security or region-specific content access.

In the following example, the router connects to an Australian server using the WireGuard protocol. All traffic from connected clients will be routed through this VPN tunnel.

The screenshot displays the 'VPN Dashboard' interface. At the top right, a dropdown menu is set to 'Global Mode'. Below this, a 'VPN Client' section features a 'Kill Switch' button and a status toggle set to 'ON'. The main content area is divided into two columns: 'Type' and 'Configuration File'. Under 'Type', 'WireGuard' is listed. The 'Configuration File' column shows a selection of 'Australia' with a swap icon. Below these columns, a detailed configuration box lists the following information:

Server Address	au-v4.hideservers.net
Server Listen Port	432
Traffic Statistics	↑ 9.45 MB / ↓ 88.28 MB
Client Virtual IP (IPv4)	10.35.24.174
Client Virtual IP (IPv6)	fd00:6968:6564:c6::a23:18ae

A 'View Log' link is located at the bottom right of the configuration box.

9.2.2 Policy Mode

In this mode, you can connect a single router to multiple VPN servers and customize VPN rules. It is suitable for cases needing flexible traffic management, such as routing different traffic to different destinations through multiple VPN servers.

Switch the VPN Mode to **Policy Mode**, and click **Apply**.

Switch VPN Mode

Global Mode

☐ If the VPN is connected, all traffic will be routed through the VPN. Only one VPN client instance can be activated.

Policy Mode

☒ This mode supports advanced customization, enabling the configuration and activation of multiple VPN servers on a single device, along with the execution of complex policy logic.

Cancel

Apply

After switching, if the VPN is not enabled, the page displays as below, including three sections: **Primary Tunnel**, **Add Tunnel** and **All Other Traffic**.

VPN Dashboard

Policy Mode

1

Priority 1

Primary Tunnel

Kill Switch

OFF

From

To

Via

All Clients

All targets

Please select a configuration file

Traffic from all devices is allowed by the current rule.

Traffic to all destinations is allowed through the current tunnel.

The current tunnel is disabled.

2

+ Add Tunnel

3

All Other Traffic

Allow Non-VPN Traffic

ON

For all other Internet traffic that is not matched by any of the VPN tunnels and policies above, this option controls whether you want it to go to the Internet. This option is enabled by default to ensure you have normal Internet access besides your VPN traffic.

Allow Non-VPN Traffic : When Enabled, you will have normal Internet access if your traffic does not match any of the policies above.

Enhanced Kill Switch : When Disabled, you are forced to use VPN and policies to access the Internet. All unmatched traffic will be blocked. This option does not override the individual Kill Switch for each policy.

9.2.2.1 Primary Tunnel

The primary tunnel is a preset tunnel in Policy Mode. It has the highest priority by default, and you can adjust its priority when multiple tunnels are configured.

In this tunnel, you can customize the tunnel rule by setting three factors:

- **From:** It refers to the traffic source, i.e., the traffic that should be routed via this tunnel.
- **To:** It refers to the traffic destination, to which the traffic is routed through this tunnel.
- **Via:** It refers to the traffic routing method, i.e., whether to use VPN.

Priority 1 Primary Tunnel Kill Switch OFF

From: All Clients Traffic from all devices is allowed by the current rule.

To: All Targets Traffic to all destinations is allowed through the current tunnel.

Via: Please select a configuration file The current tunnel is disabled.

Follow the steps below to configure your tunnel rule.

1. Click the left grayed-out box.

Priority 1 Primary Tunnel Kill Switch OFF

From: All Clients To: All Targets Via: Please select a configuration file

2. Select the device that you want to match this rule, and click **Apply**.

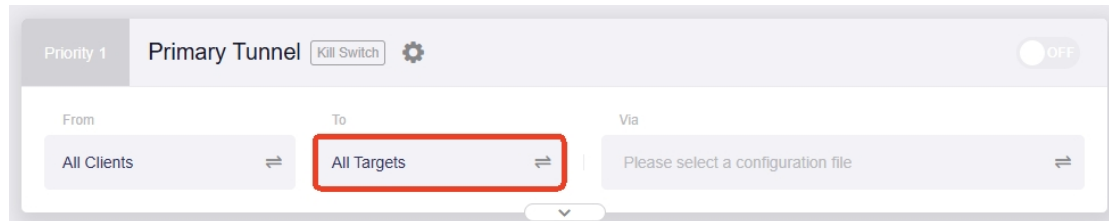
From: All Clients

- All Clients
- Specified Connection Types
- Specified Devices
- Exclude Specified Devices

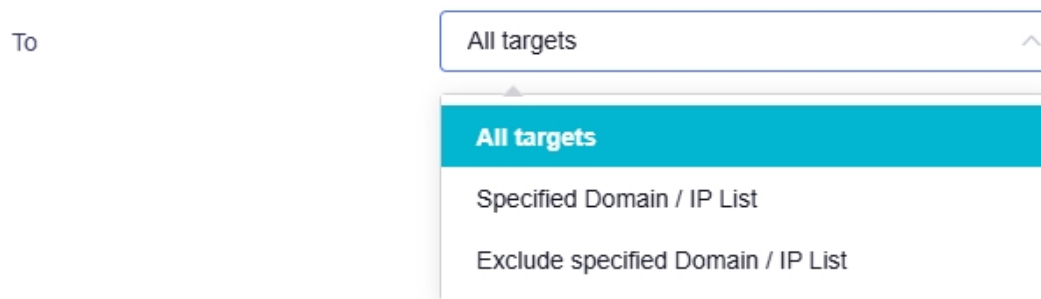
- **All Clients:** If selected, traffic from all devices will match this rule.

- **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.

3. Click the middle grayed-out box.



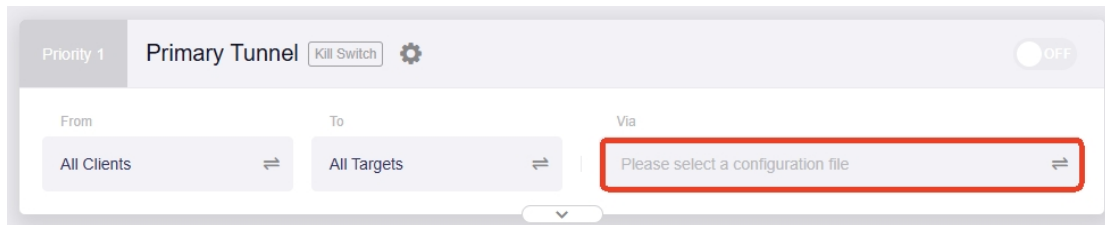
4. Select the destination to which the traffic will be routed via this tunnel, and click **Apply**.



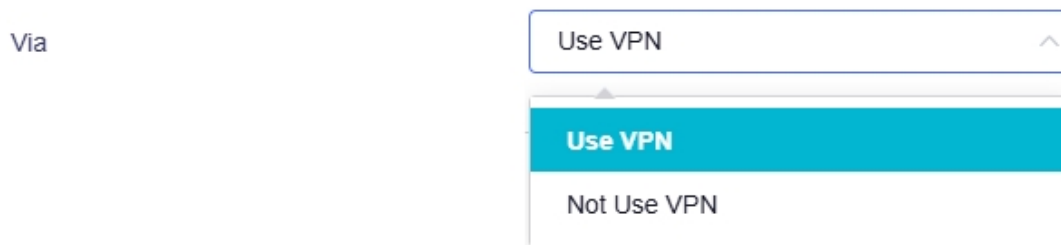
- **All Targets:** If selected, traffic matching this rule will be routed to all destinations.
- **Specified Domain / IP List:** If selected, traffic matching this rule will be routed to specified Domain / IP. You need to enter the specified Domain / IP manually, or enter the Subscription URL link. Specifying a root domain will cover all its subdomains.
- **Exclude specified Domain / IP List:** If selected, traffic matching this rule will **NOT** be routed to specified Domain / IP. You need to enter the specified Domain / IP manually, or enter the Subscription URL link. Specifying a root domain will cover all its subdomains.

Note: If you select Subscribe URL, the domain name or IP address in the URL will be automatically updated every day. Make sure to enter the correct URL. The URL detection will verify the validity of the domain name or IP address.

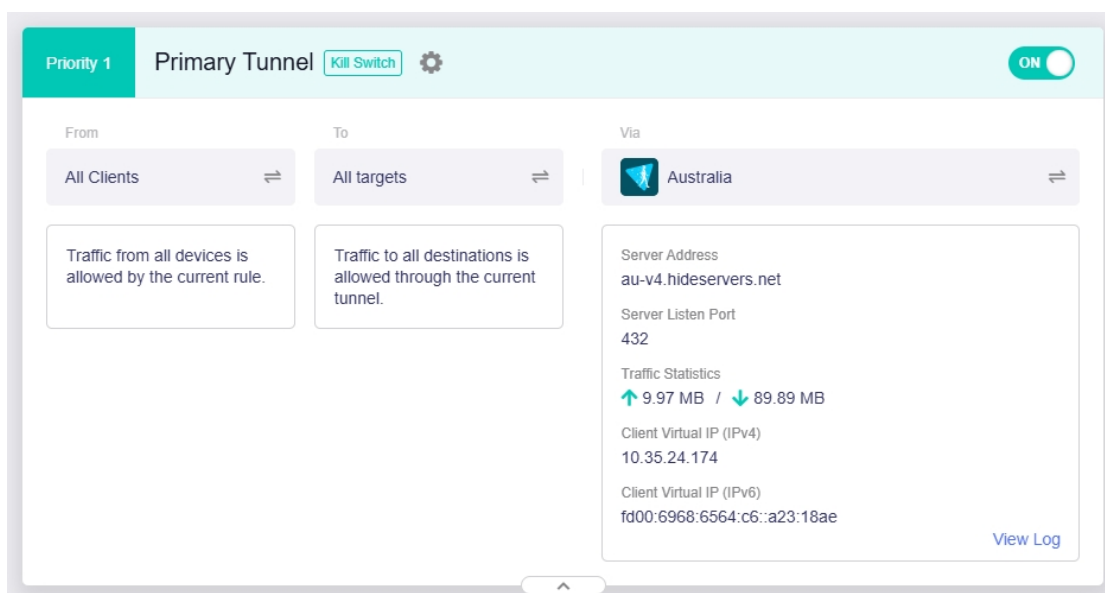
5. Click the right grayed-out box.



6. Select the routing method for this tunnel: **Use VPN** or **Not Use VPN**.



- **Use VPN:** If selected, traffic matching this rule will be routed to the selected destinations via VPN tunnel. You need to select a VPN configuration file for this rule.
 - **Not Use VPN:** If selected, traffic matching this rule will be routed to the selected destinations via local WAN network instead of VPN.
7. After configuring the traffic source, destination, and routing method, the primary tunnel rule setup is complete. In the following example, the tunnel rule is: All clients connected to this router will access the Internet via VPN; Their traffic will be routed through this VPN tunnel to the Australia server and eventually exit from this server to the Internet.



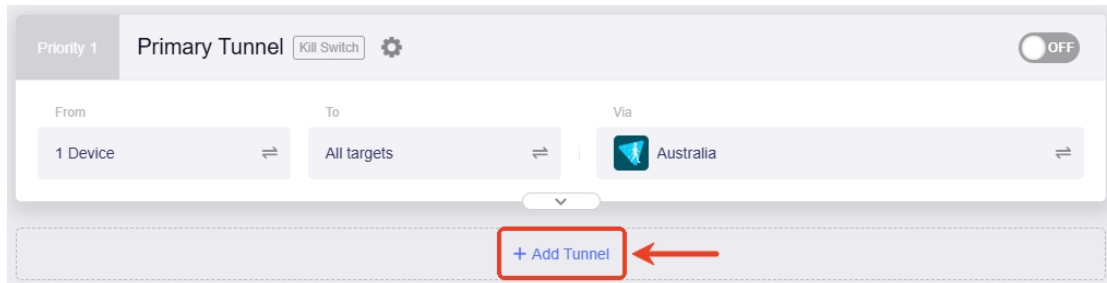
Note: For security, go to [9.2.2.3 All Other Traffic](#) and [9.2.2.4 Tunnel Options](#) to check other settings before enabling this tunnel.

9.2.2.2 Add Tunnel

Add tunnels if you need to route traffic from different devices to different destinations.

Follow the steps below to add a tunnel.

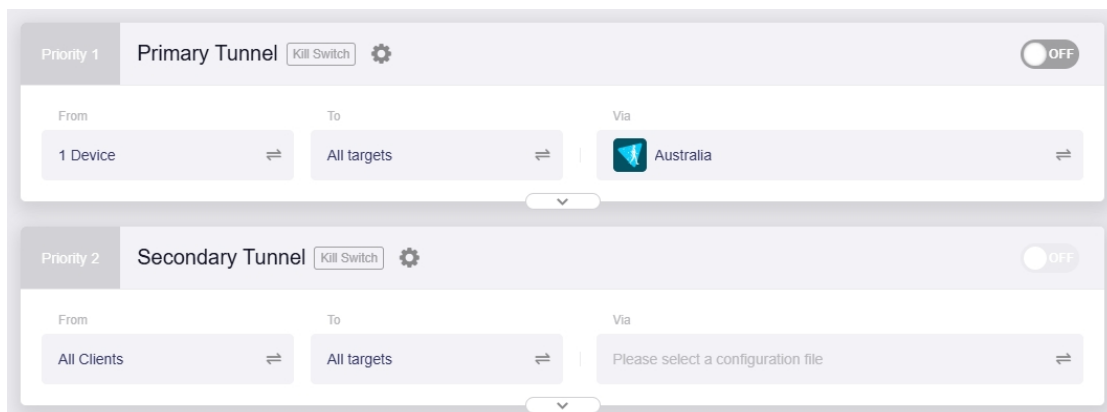
1. Click **Add Tunnel** beneath the Primary Tunnel.



2. Name the tunnel.

A screenshot of a dialog box titled 'Add Tunnel'. It has a light gray background. At the top, the title 'Add Tunnel' is displayed. Below the title is a text input field with the placeholder text 'Name'. At the bottom of the dialog, there are two buttons: a 'Cancel' button and an 'Apply' button.

3. You will get one more tunnel on the VPN Dashboard. Up to 5 tunnels can be created (including the preset primary tunnel).



4. Configure tunnel rules by setting the traffic source, destinations and routing method. Once finished, go to [9.2.2.3 All Other Traffic](#) and [9.2.2.4 Tunnel Options](#) to check other settings before enabling this tunnel.

9.2.2.3 All Other Traffic

In Policy Mode, a pre-enabled default tunnel is shown at the bottom of the VPN Dashboard.

All Other Traffic

Allow Non-VPN Traffic ☒

For all other Internet traffic that is not matched by any of the VPN tunnels and policies above, this option controls whether you want it to go to the Internet. This option is enabled by default to ensure you have normal Internet access besides your VPN traffic.

Allow Non-VPN Traffic : When Enabled, you will have normal Internet access if your traffic does not match any of the policies above.

Enhanced Kill Switch : When Disabled, you are forced to use VPN and policies to access the Internet. All unmatched traffic will be blocked. This option does not override the individual Kill Switch for each policy.

This tunnel controls whether traffic that does not match any of the above VPN tunnel groups can access the Internet. It is enabled by default to ensure normal Internet access for traffic not routed via VPN.

- When enabled, unmatched traffic can still access the Internet.

All Other Traffic

Allow Non-VPN Traffic ☒

For all other Internet traffic that is not matched by any of the VPN tunnels and policies above, this option controls whether you want it to go to the Internet. This option is enabled by default to ensure you have normal Internet access besides your VPN traffic.

Allow Non-VPN Traffic : When Enabled, you will have normal Internet access if your traffic does not match any of the policies above.

Enhanced Kill Switch : When Disabled, you are forced to use VPN and policies to access the Internet. All unmatched traffic will be blocked. This option does not override the individual Kill Switch for each policy.

- When disabled, only traffic routed via VPN is allowed to access the Internet. All non-VPN traffic and traffic that fails over from VPN connections will be blocked. This option does not override the individual Kill Switch for each VPN tunnel.

All Other Traffic

Enhanced Kill Switch ☐

For all other Internet traffic that is not matched by any of the VPN tunnels and policies above, this option controls whether you want it to go to the Internet. This option is enabled by default to ensure you have normal Internet access besides your VPN traffic.

Allow Non-VPN Traffic : When Enabled, you will have normal Internet access if your traffic does not match any of the policies above.

Enhanced Kill Switch : When Disabled, you are forced to use VPN and policies to access the Internet. All unmatched traffic will be blocked. This option does not override the individual Kill Switch for each policy.

9.2.2.4 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 next to a tunnel name.

The screenshot shows the 'VPN Dashboard' with a 'Policy Mode' dropdown. Under 'Priority 1', the 'Primary Tunnel' is selected. A red arrow points to the gear icon next to the 'Kill Switch' label. A context menu is open, showing 'Options', 'Rename', and 'Delete'. Below the dashboard, the 'Primary Tunnel-Options' section is visible, containing several settings with toggle switches and an MTU input field.

Primary Tunnel-Options

- Kill Switch** ⓘ ☒ Failover used when off.
- Services from GL.iNet Use VPN** ⓘ ☐
- Allow Remote Access the LAN Subnet** ⓘ ☐
- IP Masquerading** ⓘ ☒
- MTU** ⓘ

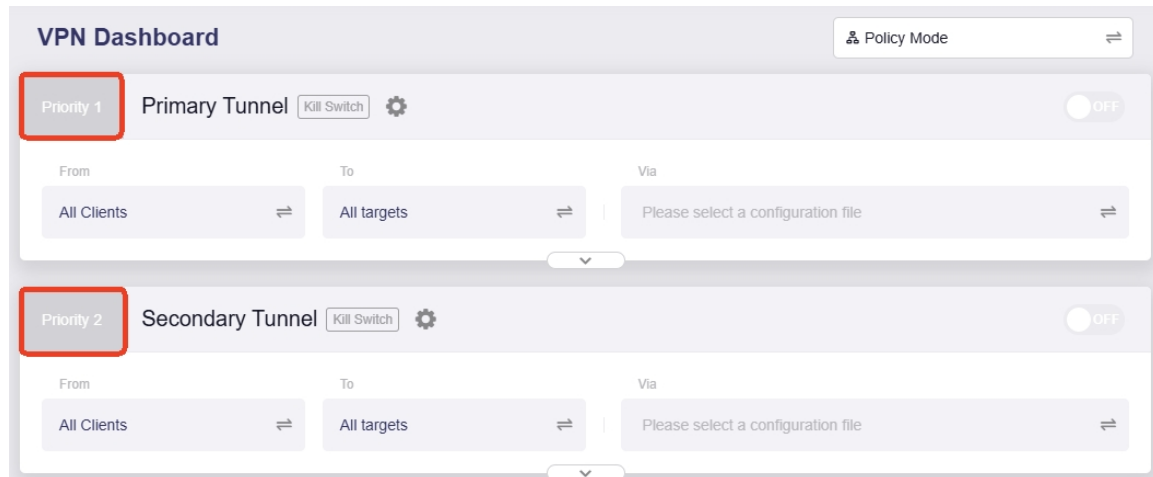
- **Kill Switch:** If enabled, traffic matching this VPN tunnel will be blocked when the connection fails unexpectedly; otherwise, it will fail over to next priority tunnels or WAN.
- **Services from GL.iNet Use VPN:** If enabled, GoodCloud, DDNS, and rty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.
- **Allow Remote Access the LAN Subnet:** If enabled, remote access to this router (tunnel IP) and LAN devices through the VPN will be allowed. It requires the VPN server to advertise a route back to this router's LAN subnet.
- **IP Masquerading:** If enabled, the LAN client source IPs will be rewritten to the router's VPN tunnel IP. Disabled only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU:** The MTU you set for the tunnel will overwrite the MTU item in the configuration file.

9.2.2.5 Tunnel Priority

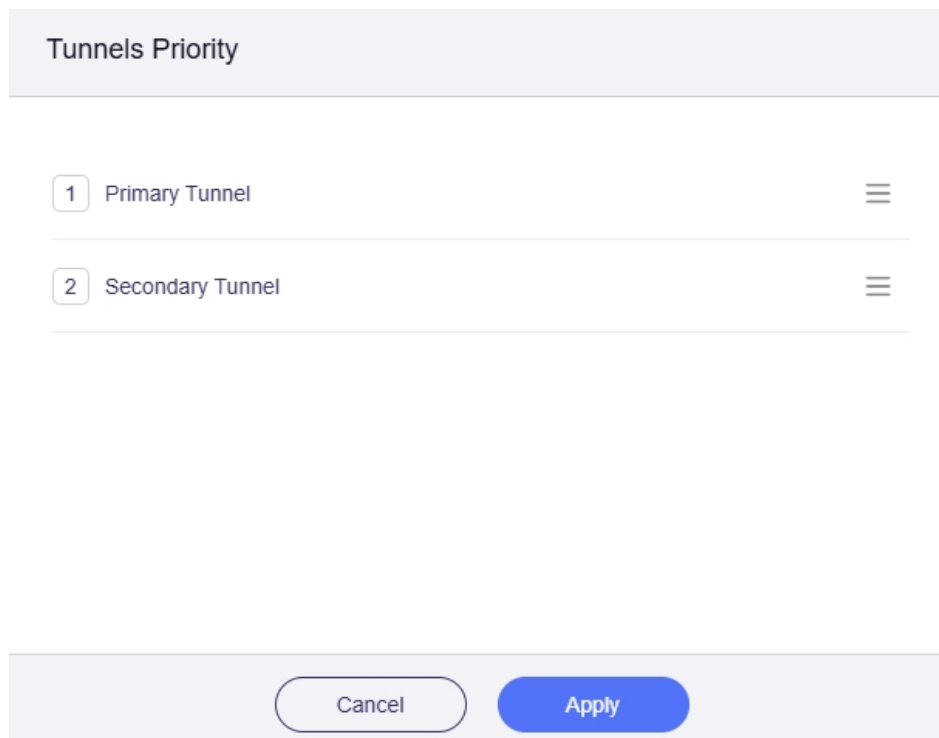
By default, the preset Primary Tunnel has the highest priority, followed by other manual-added tunnel (if any), then the preset All Other Traffic tunnel to ensure network connectivity via local ISP (WAN) network.

If you need to modify tunnel priority, follow the steps below.

1. Click the priority label in the upper left corner of any tunnel (e.g., Priority 1 / Priority 2).



2. In the pop-up window, click and hold the three-line icon on the right to reorder the tunnel, then click **Apply**.



When multiple tunnels are enabled, the router will route traffic in the following order:

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, until it matches the "All Other Traffic" tunnel.
2. If a VPN tunnel disconnects unexpectedly, the system will determine whether to fail over the traffic to the next priority tunnel based on whether this tunnel's **Kill Switch** is enabled.
 - When the Kill Switch is enabled, traffic will be blocked and will not fail over to the next priority tunnel.
 - When the Kill Switch is disabled, traffic will fail over to the next priority tunnel and attempt to match its tunnel rules.
3. The **All Other Traffic** tunnel is enabled by default to ensure that traffic not matching the VPN tunnels can still access the Internet.
 - If enabled, it routes unmatched or failover traffic through the local WAN.
 - If disabled, 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 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 contains several configuration fields:

- Device Mode:** A dropdown menu set to 'TUN'.
- Protocol:** A dropdown menu set to 'UDP'.
- Local Port:** A text input field containing '1194'.
- IPv4 Subnet:** A text input field containing '10.8.0.0/24'.
- IPv6 Subnet:** A text input field containing 'fd00:a79f:8609:088f::0/64'.
- Authentication Mode:** A dropdown menu set to 'Certificate only'.

Below these fields is a link for 'Advanced Configuration'. At the bottom, there are 'Reset' and 'Apply' buttons. A red rectangular box highlights the 'Export Client Configuration' link, 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:

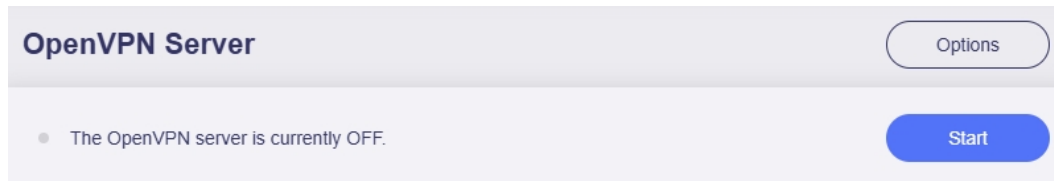
- If your public IP address changes frequently, go to **APPLICATIONS > Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.
- Since firmware v4.8, you can select the server address from a drop-down list before exporting the configuration file: Public IP, DDNS domain,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

Once selected, the server address in the configuration file will be updated automatically.

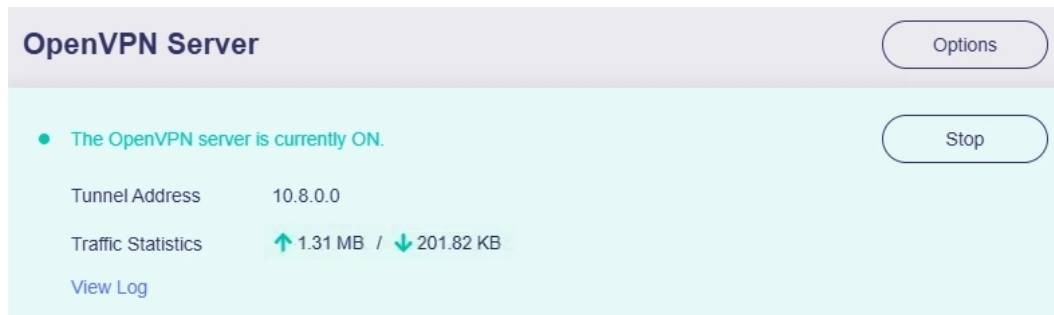
Re-download the configuration file if the server address is changed.

4. Start OpenVPN server.

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



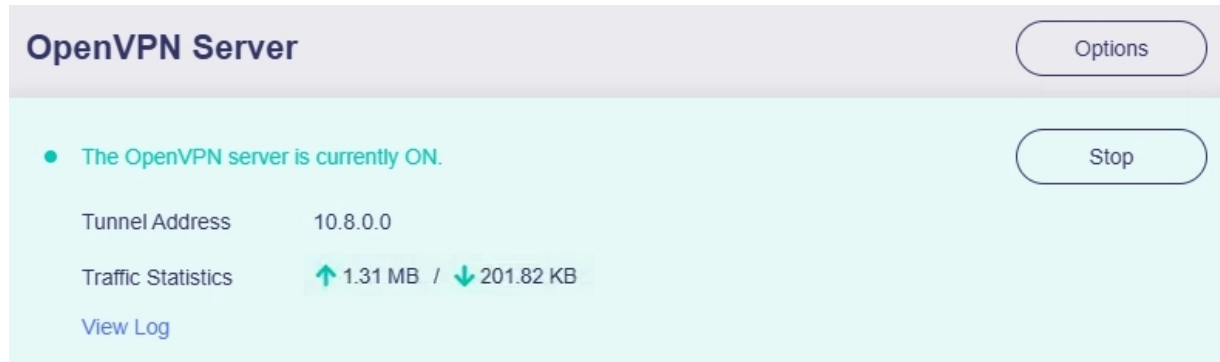
The server connection status is displayed at the top. If it shows upload and download traffic statistics, it means the OpenVPN server is running.



10.1.3 Verify Connection

Method 1. Verify Server Status

In firmware v4.8, you can check the server connection status on the **OpenVPN Server** page. If it shows upload/download traffic statistics, it means the OpenVPN server is running.



Method 2. Verify Client's IP

Import the previously-exported OpenVPN configuration to a device on a different network (not the same local network as the server). Then open a web browser, search for your IP address and location. If they match the VPN server's IP (instead of your Internet service provider's IP) and location, the VPN connection is successful.

Here's an example to use a smartphone with the official [OpenVPN App](#) installed to verify.

1. First, disable the smartphone's Wi-Fi and enable the cellular data (4G/5G) exclusively.
2. Next, open the OpenVPN app, import the configuration file, and initiate the connection.
3. Check if the smartphone can access the internet and if its IP address matches the OpenVPN Server's IP.

Tip: When importing the configuration file into the OpenVPN app, a reminder may appear as shown below. Click **CONTINUE** to proceed, as the certificate is already embedded in the configuration file.

Select Certificate

This profile doesn't include a client certificate. Continue connecting without a certificate or select one from the Android keychain?

CONTINUE **SELECT CERTIFICATE**

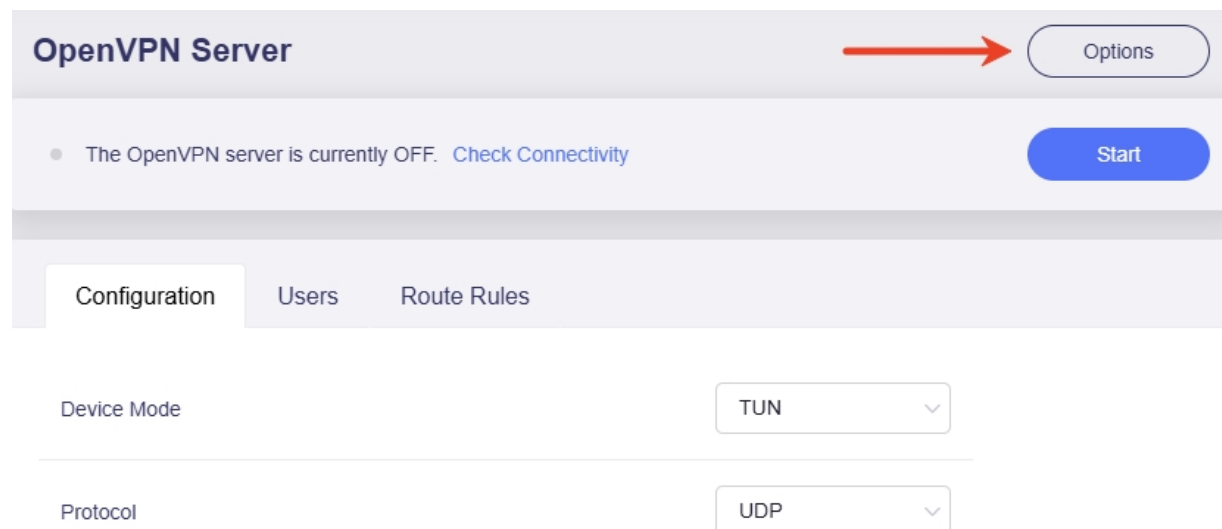
If the connection fails, there are several common reasons:

- The VPN server does not have a public IP address. See [10.1.1 Preparation](#) for details.
- You may need to set up port forwarding. See [10.1.1 Preparation](#) for details.
- 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.

10.1.4 Server Options

Server Options include some advanced settings on the server side, such as remote access server's LAN, IP Masquerading, etc. Configure these settings according to your needs.

On the **OpenVPN Server** page, click **Options** in the upper-right corner.



OpenVPN Server Options

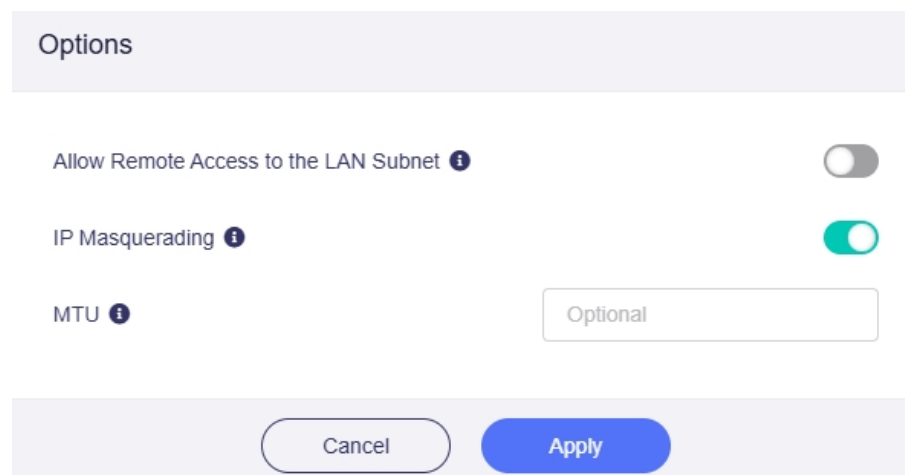
• The OpenVPN server is currently OFF. [Check Connectivity](#) Start

Configuration Users Route Rules

Device Mode TUN

Protocol UDP

In the pop-up window, you will see the following features.



Options

Allow Remote Access to the LAN Subnet i ☐

IP Masquerading i ☒

MTU i Optional

Cancel Apply

- **Allow Remote Access to the LAN Subnet:** If enabled, resources inside the server's LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading:** If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU:** Short for Maximum Transmission Unit. The MTU value you set for the tunnel will override the MTU settings in the configuration file.

10.1.5 Client to Client

Client-to-Client is a server-side VPN feature. Once enabled, connected VPN clients can communicate with one another using their respective VPN tunnel IP addresses.

Follow the steps below to enable Client to Client on your OpenVPN server if needed.

1. On the **OpenVPN Server** page, click **Advanced Configuration** in the bottom-right.

The screenshot shows the OpenVPN Server Configuration interface. At the top, there are three tabs: 'Configuration', 'Users', and 'Route Rules'. The 'Configuration' tab is selected. Below the tabs, there are several configuration fields:

- Device Mode:** A dropdown menu set to 'TUN'.
- Protocol:** A dropdown menu set to 'UDP'.
- Local Port:** A text input field containing '1194'.
- IPv4 Subnet:** A text input field containing '10.8.0.0/24'.
- IPv6 Subnet:** A text input field containing 'fd00:a19a:42c1:0283::0/64'.
- Authentication Mode:** A dropdown menu set to 'Certificate only'.

At the bottom of the configuration area, there is a link labeled 'Advanced Configuration' with an information icon (i) and a dropdown arrow (v). A red arrow points to this link, and it is enclosed in a red rectangular box. Below the configuration area, there are two buttons: 'Reset' and 'Apply'.

2. Enable **Client to Client** and click **Apply**. Then export a new configuration and upload it to your OpenVPN clients.

The screenshot shows a configuration interface for a VPN. At the top, there is a toggle switch for "Enable TLS Authentication" which is currently turned off. Below this, there is a section for "Client to Client" with a toggle switch that is turned on; a red arrow labeled with a circled "1" points to this toggle. Underneath, the "Verbosity Level" is set to "3" in a dropdown menu. To the right of the dropdown is a link labeled "Advanced Configuration" with an information icon and an upward arrow. Below these elements are two buttons: "Reset" and "Apply". A red arrow labeled with a circled "2" points to the "Apply" button. At the bottom, there is a link labeled "Export Client Configuration" with a document icon. A red arrow labeled with a circled "3" points to this link.

Tip: Client-to-Client only advertises each client's tunnel IP address. It does not automatically expose the local LAN subnets behind each VPN client. If you need to grant clients access to each other's LAN subnets, please add routing rules on the VPN server to advertise those remote LAN subnets.

10.2 WireGuard Server

WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN.

*WireGuard® is a registered trademark of Jason A. Donenfeld.

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:

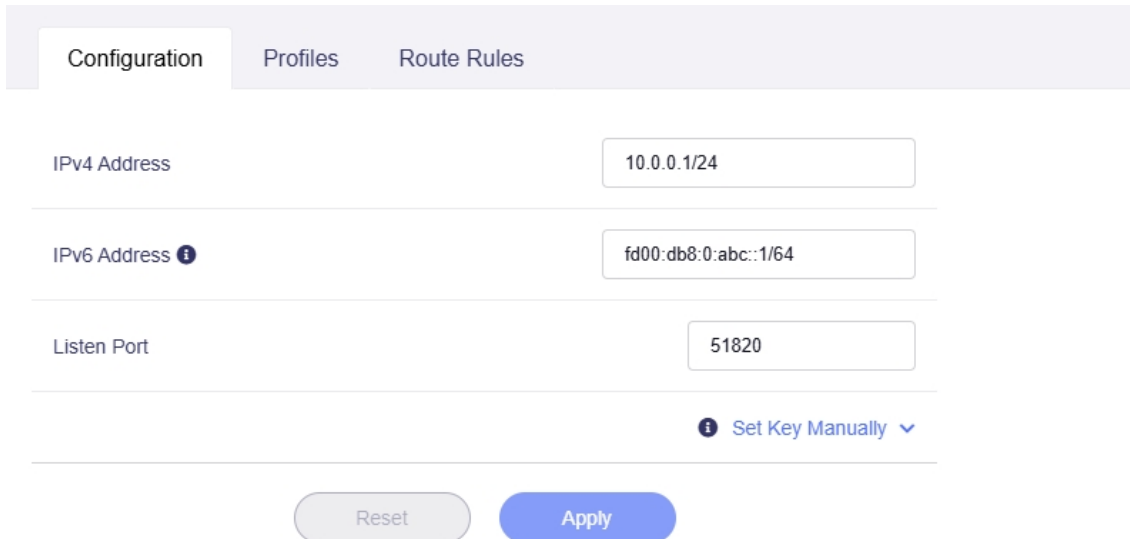
- If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
- Ask your ISP for a public IP address. This may incur an extra fee.
- If the above two methods don't work (e.g., if your network is behind CGNAT), you may try our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

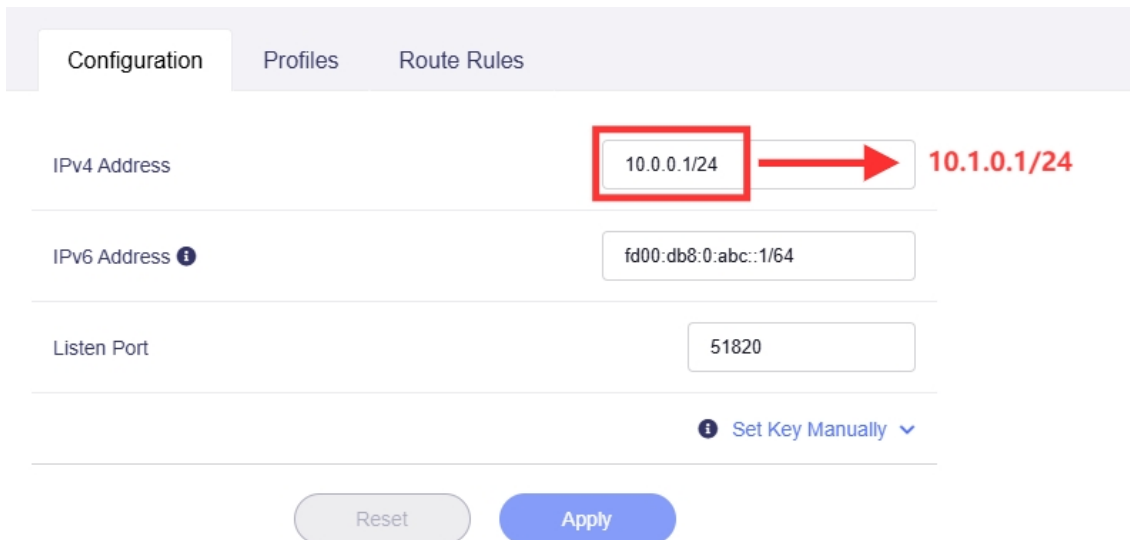
10.2.2 Setup Steps

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 features 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 an information icon and a dropdown arrow. At the bottom are two buttons: 'Reset' and 'Apply'.

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 identical to the previous one, but with an annotation. A red rectangle highlights the '10.0.0.1/24' text in the 'IPv4 Address' field. A red arrow points from this box to the new address '10.1.0.1/24' written in red text to the right of the field.

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

WireGuard Server Options

● The WireGuard server is currently OFF. Start

Configuration **Profiles** Route Rules

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

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

Client Configuration

Name

[Set More](#)

Cancel Apply

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

4. Download configuration.

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

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

WireGuard® Client Configuration

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

Address ⓘ

35.76.125.9

QR Code

Configuration File

[Interface]

Address = 10.1.0.2/24,fd00:ff14:e440:ae83::2/64

PrivateKey =

DNS = 10.1.0.1,fd00:ff14:e440:ae83::1,64.6.64.6

MTU = 1420

[Peer]

AllowedIPs = 0.0.0.0/0,::/0

Endpoint = 35.76.125.9:51820

PersistentKeepalive = 25

PublicKey =

Download

Tips:

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

Address ⓘ

35.76.125.9

QR Code

Configuration File

35.76.125.9

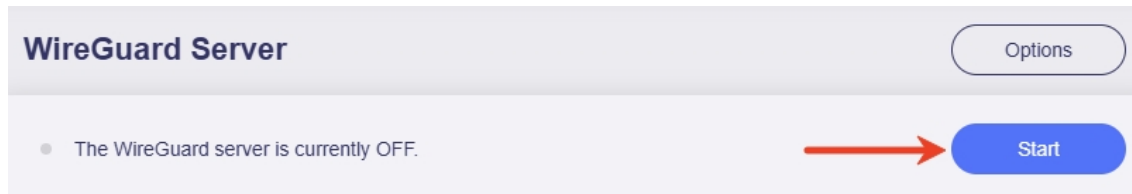
.glddns.com

192.168.6.189

123

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 Verify Connection

Method 1. Verify Server Status

In firmware v4.8, you can check the server connection status on the **WireGuard Server** page. If it shows upload/download traffic statistics and online connected devices, it means the WireGuard server is running and there are WireGuard clients connected to it.



The screenshot shows the 'WireGuard Server' interface. At the top, there's a title 'WireGuard Server' and an 'Options' button. Below, a green status message says 'The WireGuard server is currently ON.' with a 'Stop' button. The 'Tunnel Address' is '10.1.0.1/24'. 'Traffic Statistics' shows '↑ 1.31 MB / ↓ 201.82 KB'. 'Connected devices' shows '1 Client (1 Online)'. A 'View Log' link is at the bottom.

Property	Value
Tunnel Address	10.1.0.1/24
Traffic Statistics	↑ 1.31 MB / ↓ 201.82 KB
Connected devices	1 Client (1 Online)

If it shows 0 traffic and 0 client, it means that there's no WireGuard client connected.



The screenshot shows the 'WireGuard Server' interface with zero activity. The status message is 'The WireGuard server is currently ON.' with a 'Stop' button. The 'Tunnel Address' is '10.0.0.1/24'. The 'Traffic Statistics' and 'Connected devices' sections are highlighted with a red box, showing '↑ 0.00 B / ↓ 0.00 B' and 'No Clients' respectively. A 'View Log' link is at the bottom.

Property	Value
Tunnel Address	10.0.0.1/24
Traffic Statistics	↑ 0.00 B / ↓ 0.00 B
Connected devices	No Clients

Method 2. Verify Client's IP

Import the previously-exported WireGuard configuration to a device on a different network (not the same local network as the server). Then open a web browser, search for your IP address and location. If they match the VPN server's IP (instead of your Internet service provider's IP) and location, the VPN connection is successful.

Here's an example to use a smartphone with the official [WireGuard App](#) installed to verify.

1. First, disable the smartphone's Wi-Fi and enable the cellular data (4G/5G) exclusively.
2. Next, open the WireGuard App, import the configuration file, and initiate the connection.

3. Check if the smartphone can access the internet and if its IP address matches the WireGuard Server's IP.

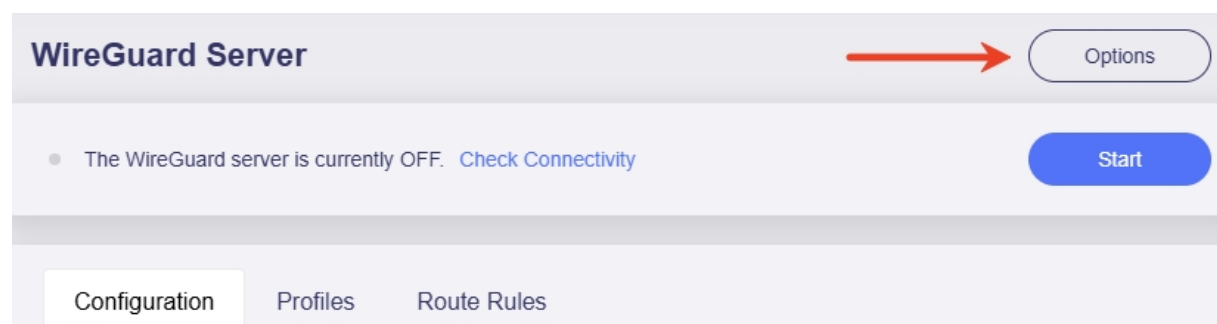
If the connection fails, there are several common reasons:

- The VPN server does not have a public IP address. See [10.2.1 Preparation](#) for details.
- You may need to set up port forwarding. See [10.2.1 Preparation](#) for details.
- 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.

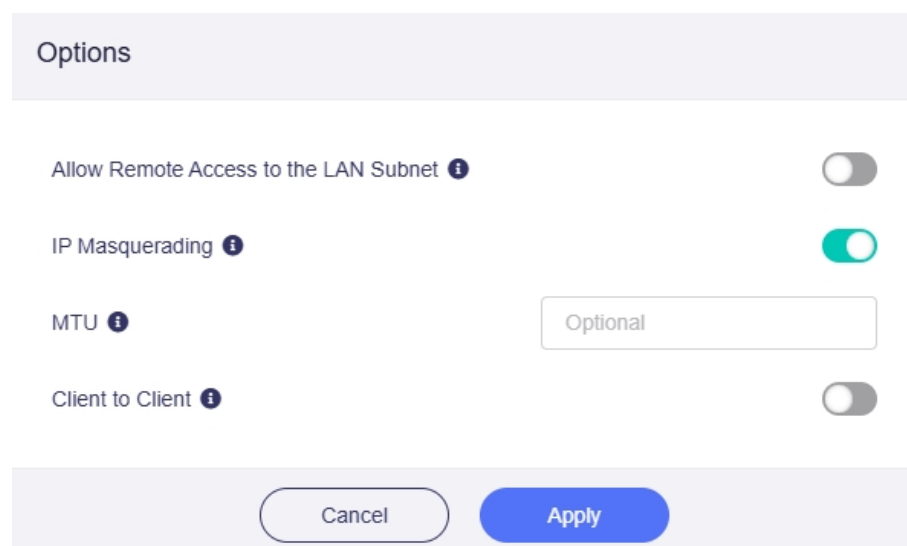
10.2.4 Server Options

Server Options include some advanced settings on the server side, such as remote access server's LAN, IP Masquerading, etc. Configure these settings according to your needs.

On the **WireGuard Server** page, click **Options** in the upper-right corner.



In the pop-up window, you will see the following features.



- **Allow Remote Access to the LAN Subnet:** If enabled, resources inside the server's LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading:** If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU:** Short for Maximum Transmission Unit. The MTU value you set for the tunnel will override the MTU settings in the configuration file.
- **Client to Client:** If enabled, VPN clients connected to this server can access each other via their respective VPN tunnel IPs.

Note that Client-to-Client only advertises each client's tunnel IP address. It does not automatically expose the local LAN subnets behind each VPN client. If you need to grant clients access to each other's LAN subnets, please add routing rules on the VPN server to advertise those remote LAN subnets.

Chapter 11

Set Up VPN Client

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

11.1 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.

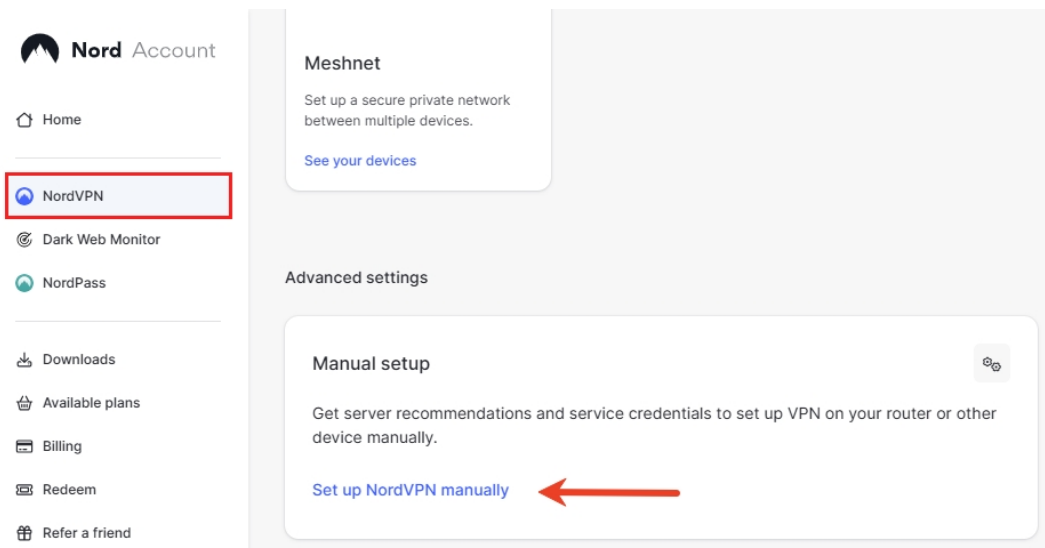
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to [this link](#) or contact their support.

11.1.2 Set Up NordVPN

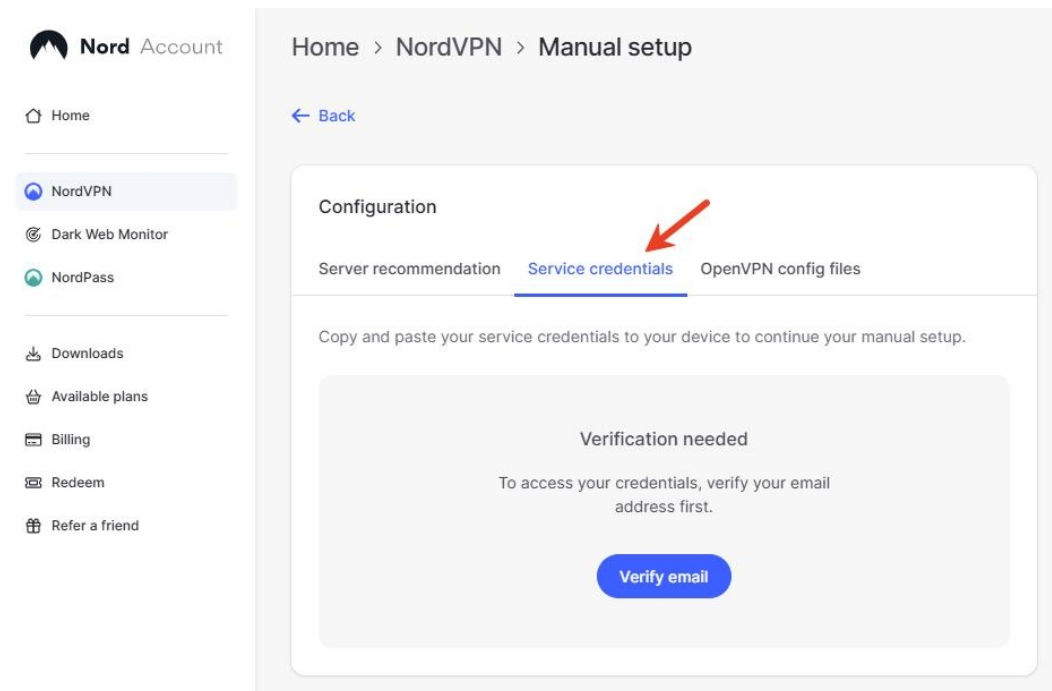
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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**.



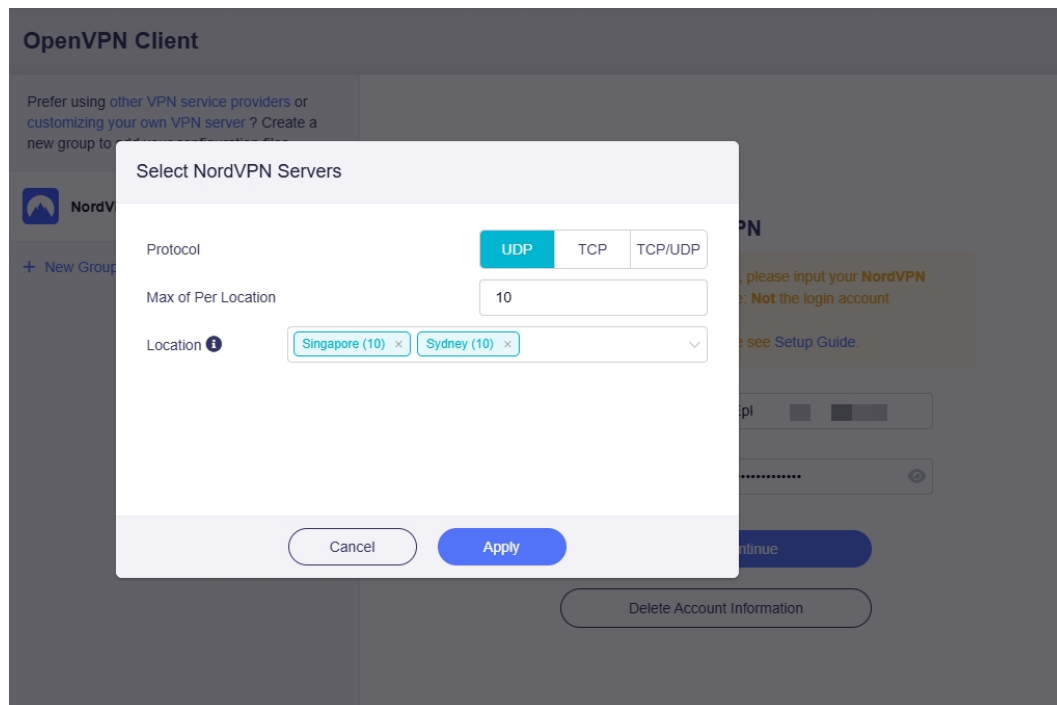
You will find the **service credentials**. Copy them for later use.



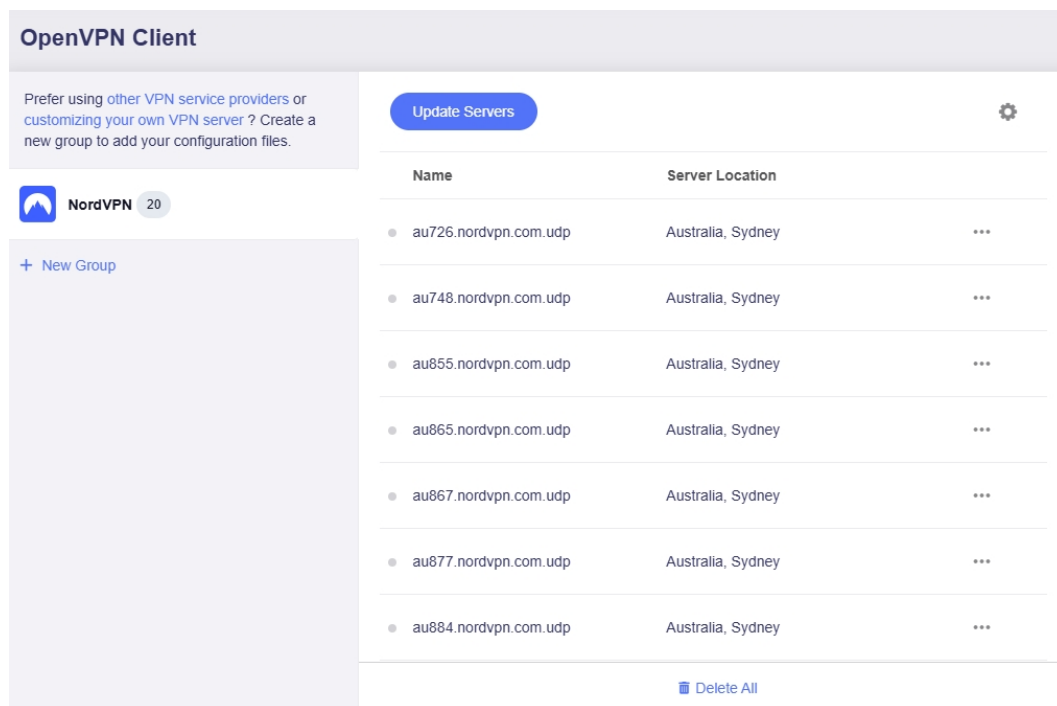
3. Log in to your router's web admin panel and navigate to **VPN > OpenVPN Client > NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.

The screenshot shows the 'OpenVPN Client' configuration page. On the left, there is a sidebar with a 'New Group' button. The main content area is titled 'NordVPN'. Below the title, there is a yellow warning box with a triangle icon and the text: 'To ensure successful use of the VPN, please input your NordVPN account's service credentials (Note: Not the login account email/password). If you don't know how to get it, please see Setup Guide.' Below the warning box are two input fields: 'Service Credential' and 'Credential Password'. Below these fields is a blue button labeled 'Save and Continue'.

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

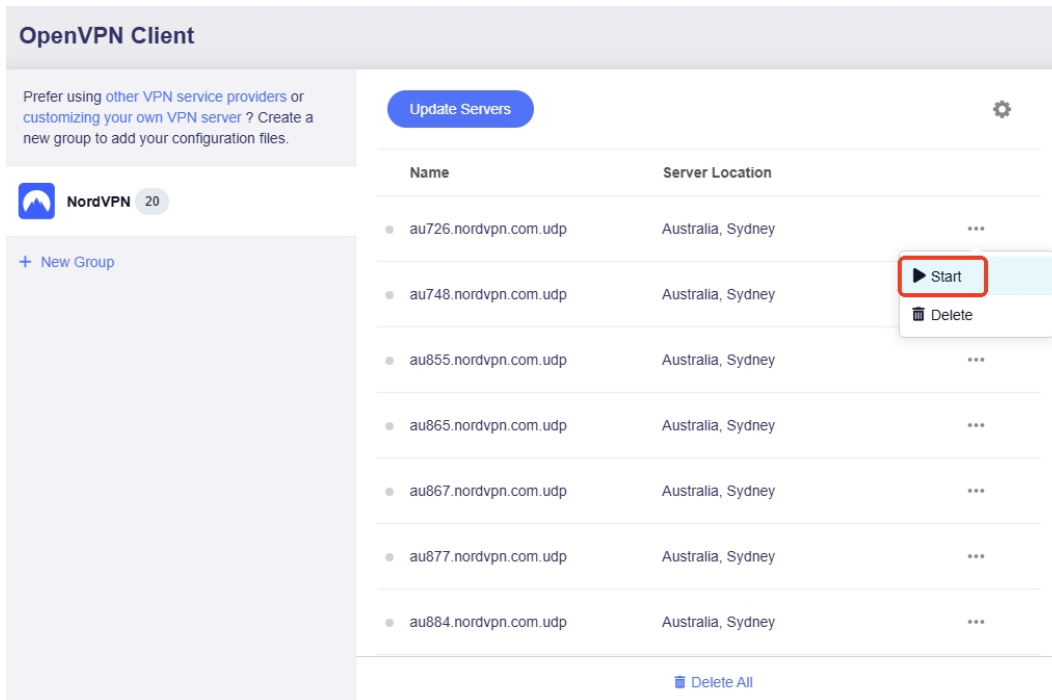


It will download configuration files.

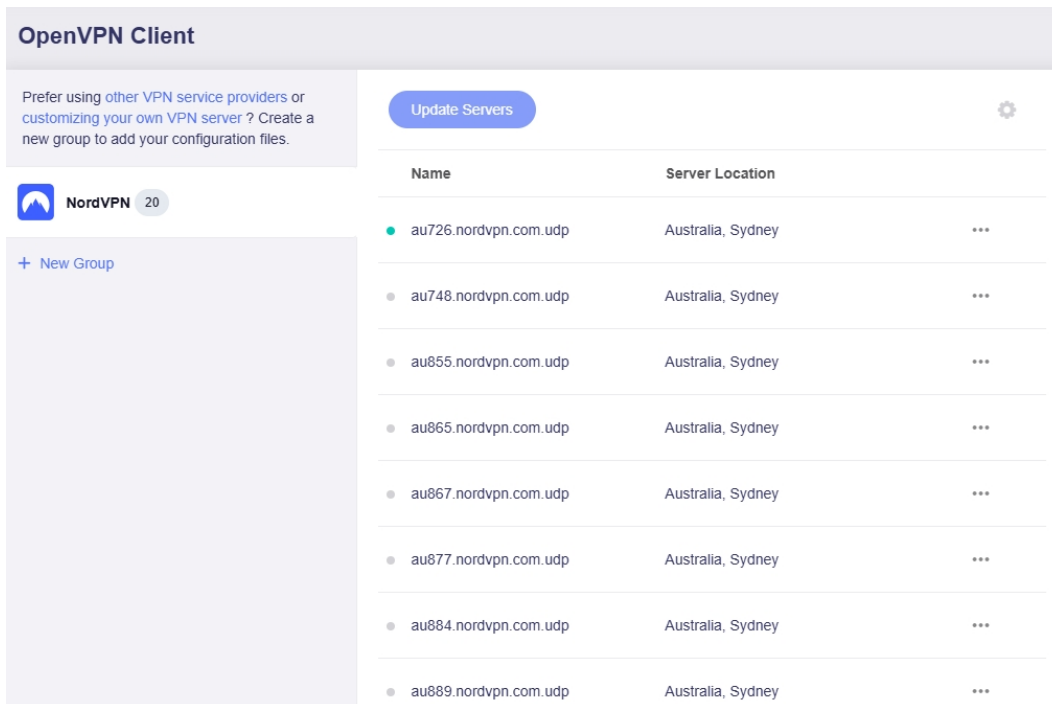


5. Start a connection.

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



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



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

- Update servers.

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

OpenVPN Client

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

NordVPN 20

+ New Group

Update Servers

Name	Server Location	
● au726.nordvpn.com.udp	Australia, Sydney	...
● au748.nordvpn.com.udp	Australia, Sydney	...
● au855.nordvpn.com.udp	Australia, Sydney	...
● au865.nordvpn.com.udp	Australia, Sydney	...
● au867.nordvpn.com.udp	Australia, Sydney	...
● au877.nordvpn.com.udp	Australia, Sydney	...
● au884.nordvpn.com.udp	Australia, Sydney	...

[Delete All](#)

8. Edit credentials.

Click the gear icon to edit your login credentials.

OpenVPN Client

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

NordVPN 20

+ New Group

Update Servers

Name	Server Location	
● au726.nordvpn.com.udp	Australia, Sydney	...
● au748.nordvpn.com.udp	Australia, Sydney	...
● au855.nordvpn.com.udp	Australia, Sydney	...
● au865.nordvpn.com.udp	Australia, Sydney	...
● au867.nordvpn.com.udp	Australia, Sydney	...
● au877.nordvpn.com.udp	Australia, Sydney	...
● au884.nordvpn.com.udp	Australia, Sydney	...

[Delete All](#)

9. Delete all files.

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

OpenVPN Client

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

**NordVPN** 20

+ New Group

Update Servers

Name	Server Location	
• au726.nordvpn.com.udp	Australia, Sydney	...
	Australia, Sydney	...
	Australia, Sydney	...
	Australia, Sydney	...
• au867.nordvpn.com.udp	Australia, Sydney	...
• au877.nordvpn.com.udp	Australia, Sydney	...
• au884.nordvpn.com.udp	Australia, Sydney	...

Delete All

Caution

Are you sure you want to clear all?

Cancel

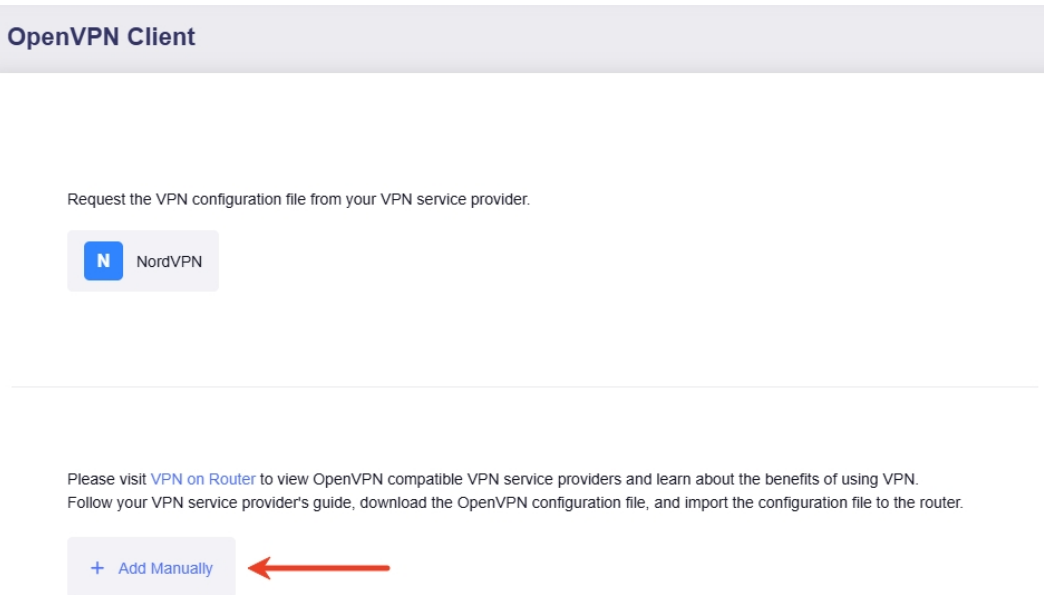
Delete

11.1.3 Set Up OpenVPN Client Manually (for other providers)

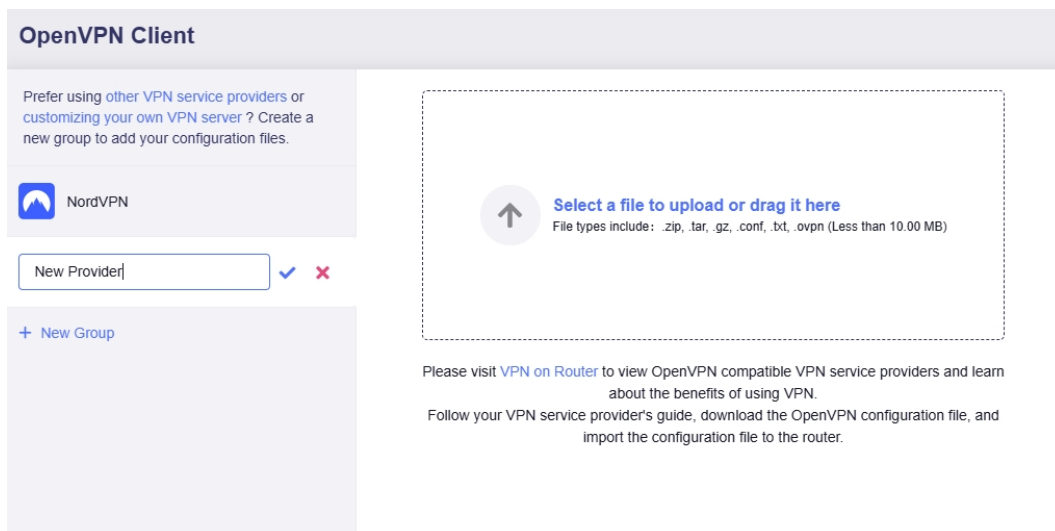
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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**.

The screenshot shows the 'OpenVPN Client' interface. On the left, there's a sidebar with a NordVPN logo and a 'Private Internet Access' section with a '+ New Group' button. The main area displays a large green checkmark icon with the text 'Upload successful' and 'ca_toronto-aes-128-cbc-udp-dns.ovpn'. Below this is a 'Re-upload file' button. A yellow warning box states: '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:'. Below the warning are input fields for 'Username' and 'Password', followed by an 'Apply' button.

You will see the configuration file uploaded.

The screenshot shows the 'OpenVPN Client' interface after the upload. The sidebar is the same. The main area now has an 'Upload Configuration File' button and a table with two columns: 'Name' and 'Server Address'. The table contains one entry: 'ca_toronto-aes-128-cbc-udp-dns' with the server address 'ca-toronto.privacy.network:1198'. A three-dot menu icon is visible to the right of the table entry.

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

The screenshot shows the 'OpenVPN Client' interface with the context menu open for the configuration file. The menu has three options: 'Start' (highlighted with a red box), 'Modify', and '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.

*WireGuard® is a registered trademark of Jason A. Donenfeld.

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.

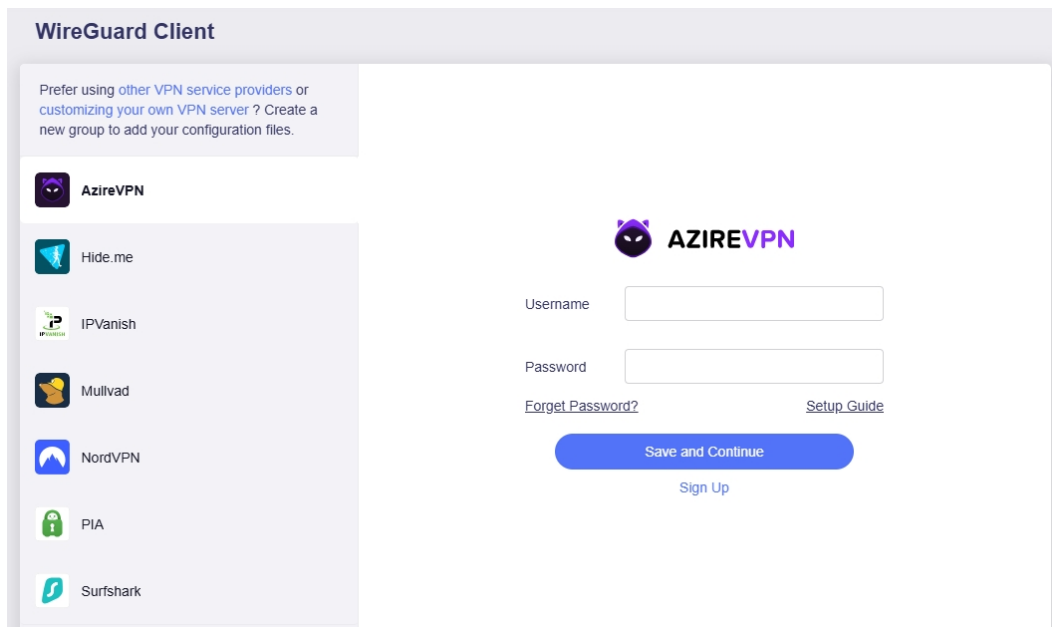
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

- [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

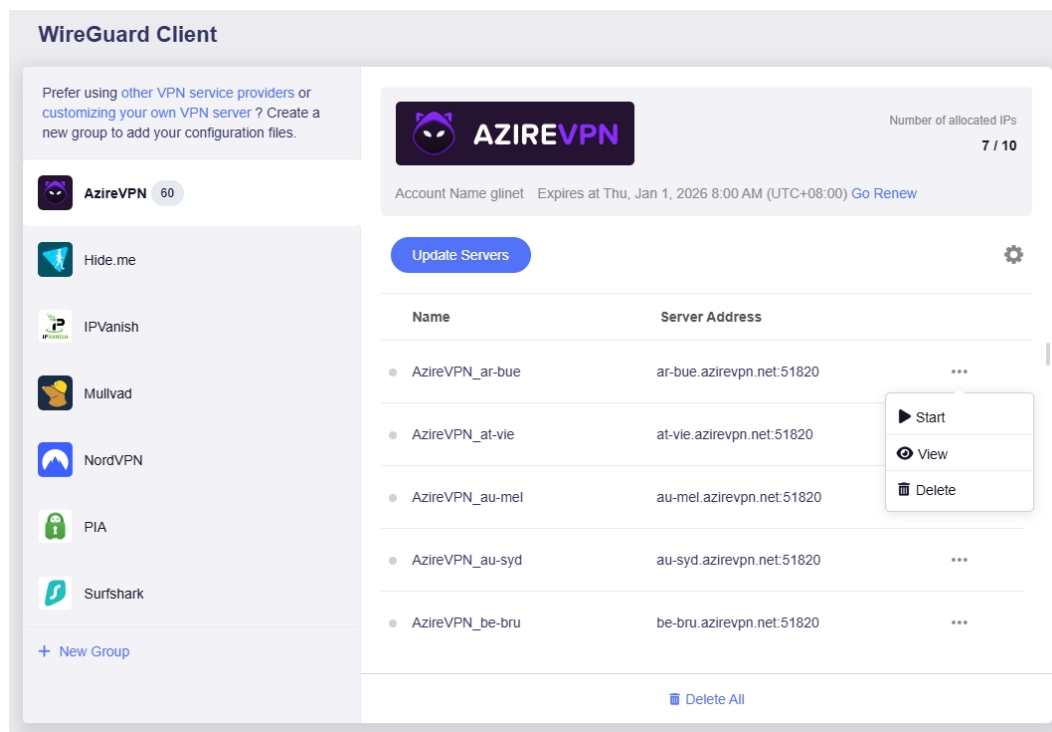
Follow the steps below to set your router as an AzireVPN client.

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 logo and a login form with fields for 'Username' and 'Password'. Below the password field are links for 'Forgot Password?' and 'Setup Guide'. A blue 'Save and Continue' button is prominently displayed, with a 'Sign Up' link below it. A note at the top left suggests using other VPN providers or customizing a server.

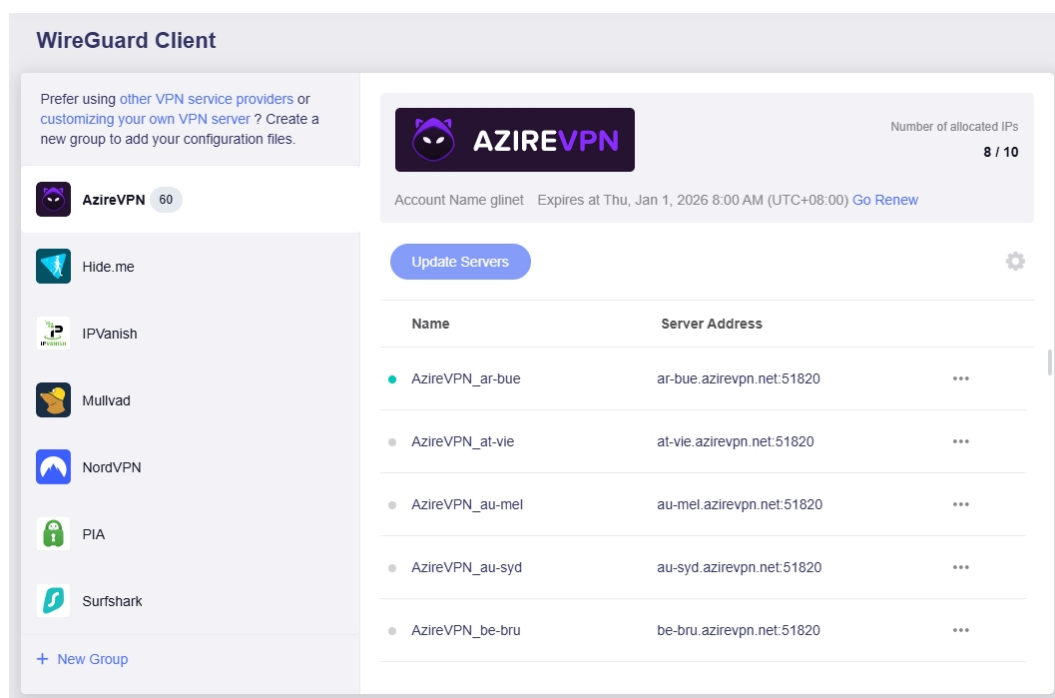
3. Select a preferred server, and click the three-dot icon on the right to start a connection.



The screenshot shows the 'WireGuard Client' 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. A table lists available servers with columns for 'Name' and 'Server Address'. A context menu is open over the first server, showing 'Start', 'View', and 'Delete' options. The table also shows the number of allocated IPs (7 / 10) and a 'Delete All' button at the bottom.

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

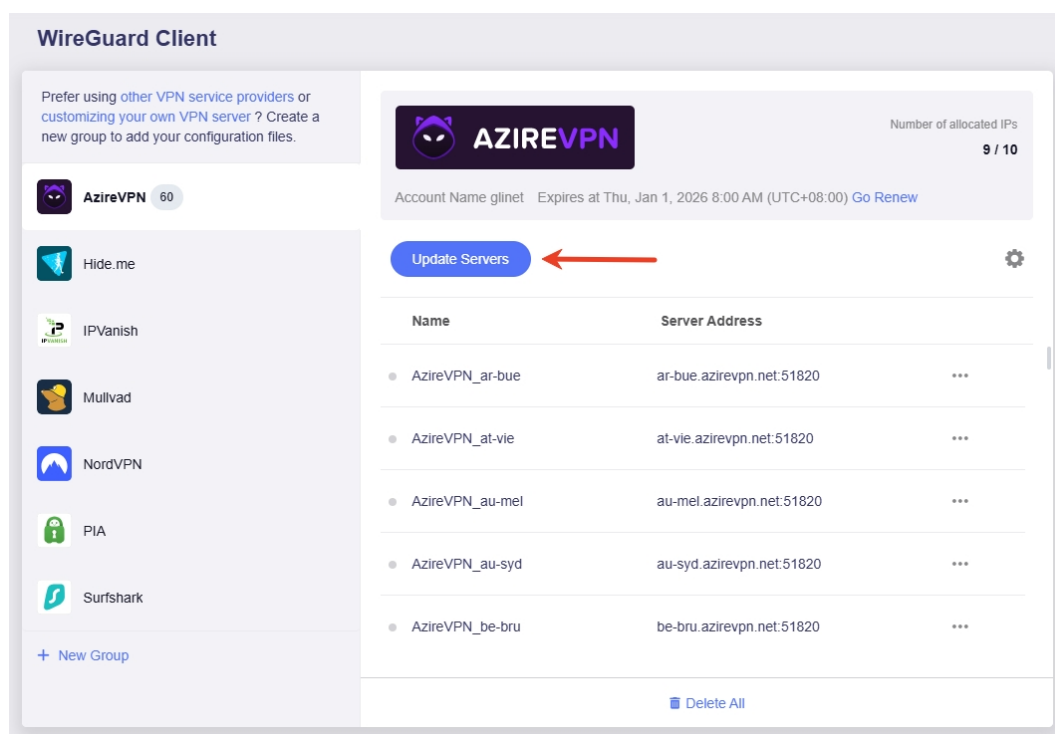
- Once connected, a green dot will appear next to the configuration file.



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.

The screenshot shows the WireGuard Client interface for an AzireVPN account. On the left, there's a sidebar with various VPN providers like Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The main area displays the AzireVPN account information, including the account name 'glinet', expiration date 'Thu, Jan 1, 2026 8:00 AM (UTC+08:00)', and a 'Go Renew' link. Below this is a table of servers with columns for Name, Server Address, and a menu icon. A dropdown menu is open, showing 'Modify Authentication Information' and 'Logout' options. The 'Go Renew' link is highlighted with a red box.

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	...

7. Go renew.

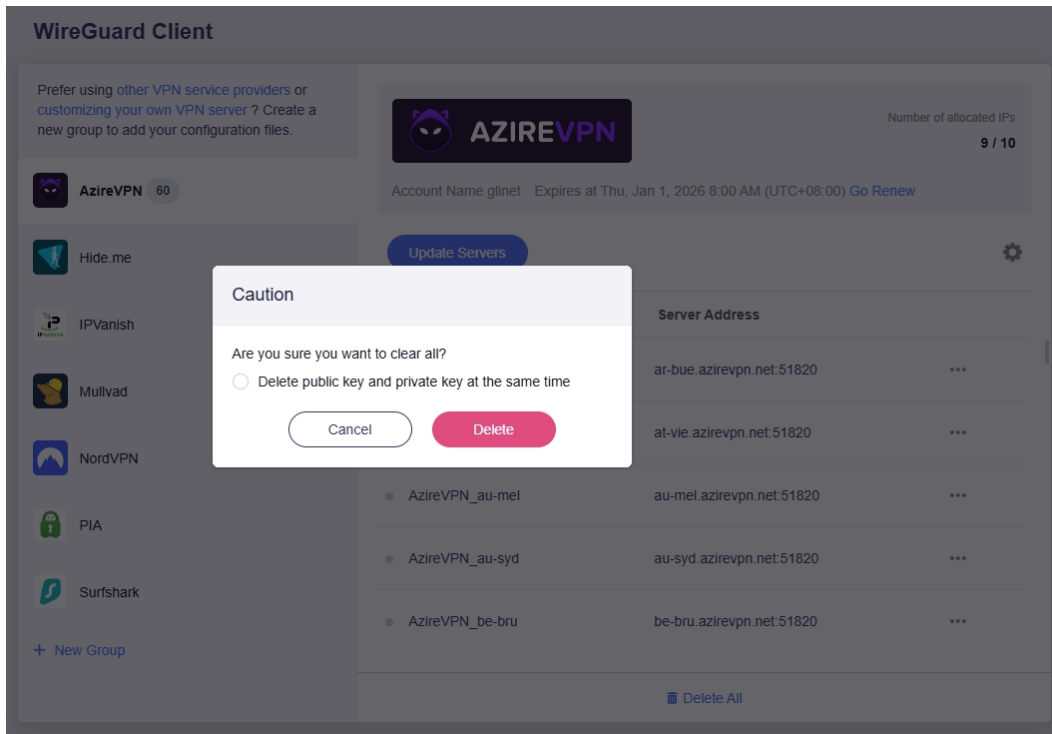
If you click **Go Renew**, you will be re-directed to the official website to renew your subscription.

This screenshot is identical to the one above, showing the WireGuard Client interface for an AzireVPN account. The 'Go Renew' link is highlighted with a red box.

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	...

8. Delete all files.

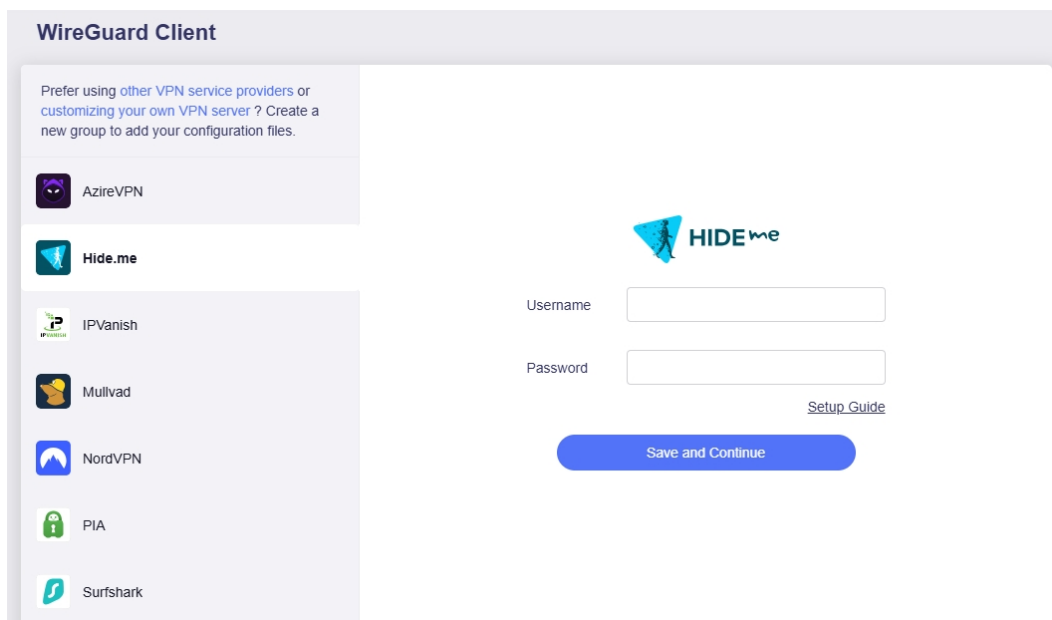
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.3 Set Up Hide.me

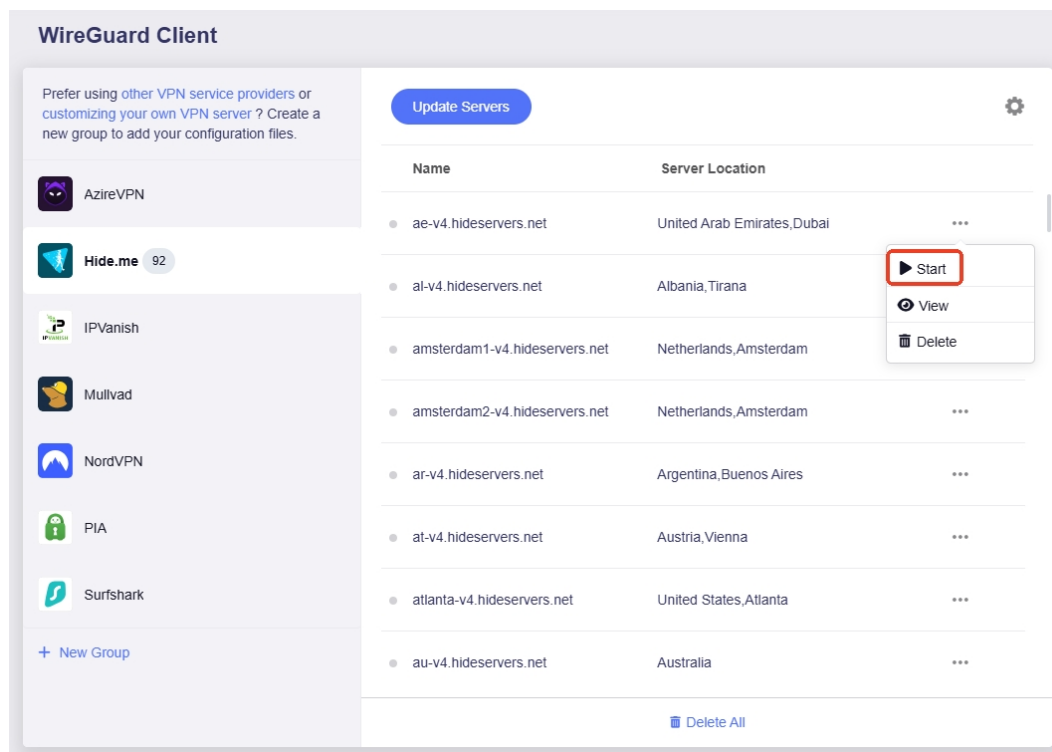
Follow the steps below to set your router as a Hide.me client.

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' interface. On the left, a sidebar lists VPN providers: AzireVPN, Hide.me (selected), IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The main area displays the Hide.me logo, a 'Username' input field, a 'Password' input field, a 'Setup Guide' link, and a blue 'Save and Continue' button.

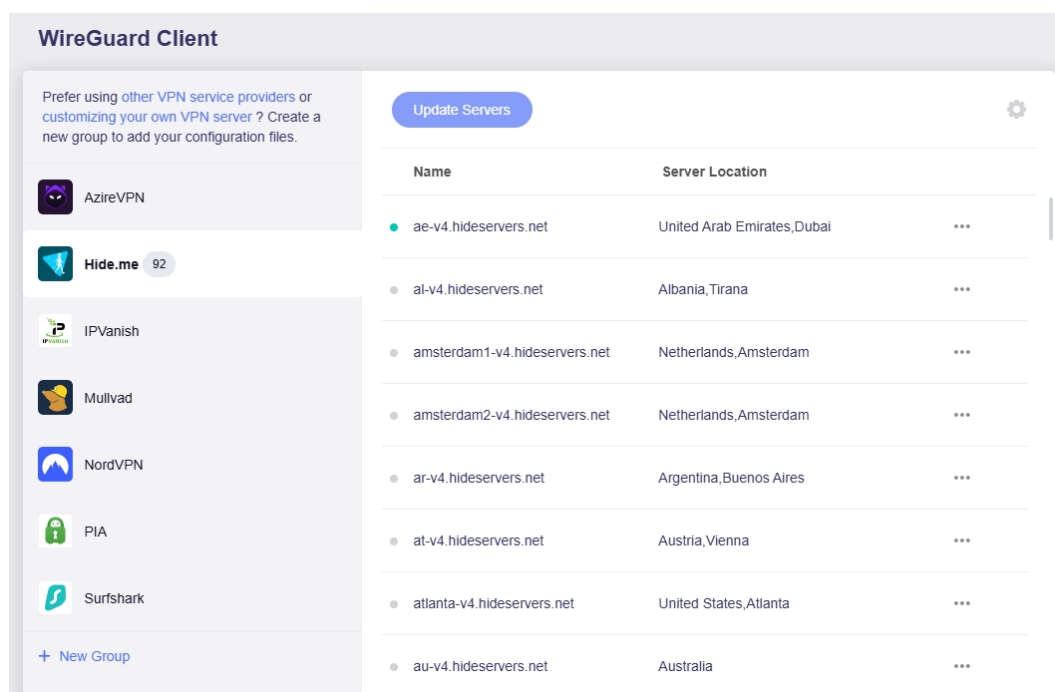
3. Select a preferred server, and click the three-dot icon on the right to start a connection.



The screenshot shows the 'WireGuard Client' interface with a list of servers. The 'Hide.me' group is selected in the sidebar. The server list has columns for 'Name' and 'Server Location'. A context menu is open for the first server, showing 'Start', 'View', and 'Delete' options. The 'Start' option is highlighted with a red box.

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

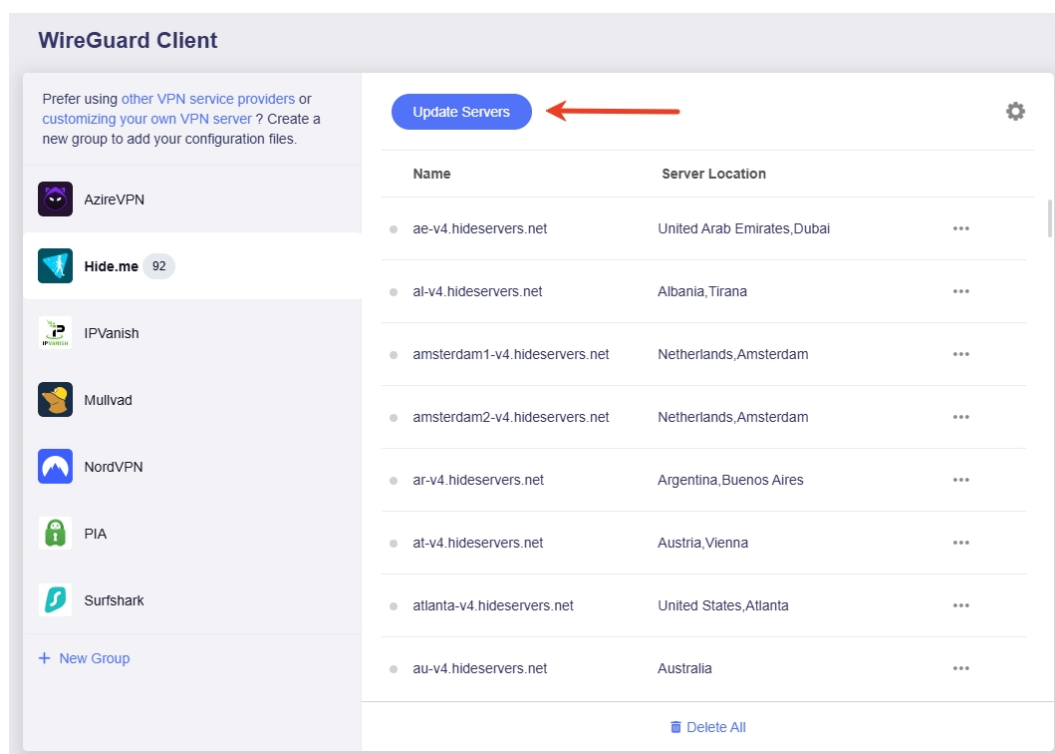
4. Once connected, a green dot will appear next to the configuration file.



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

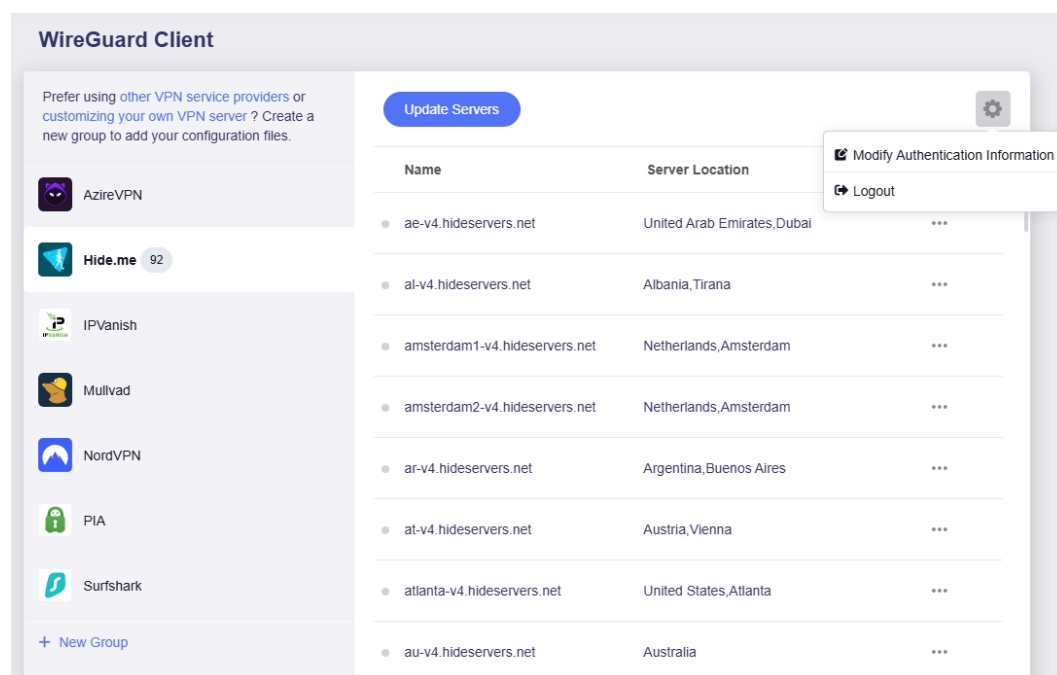
5. Update servers.

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



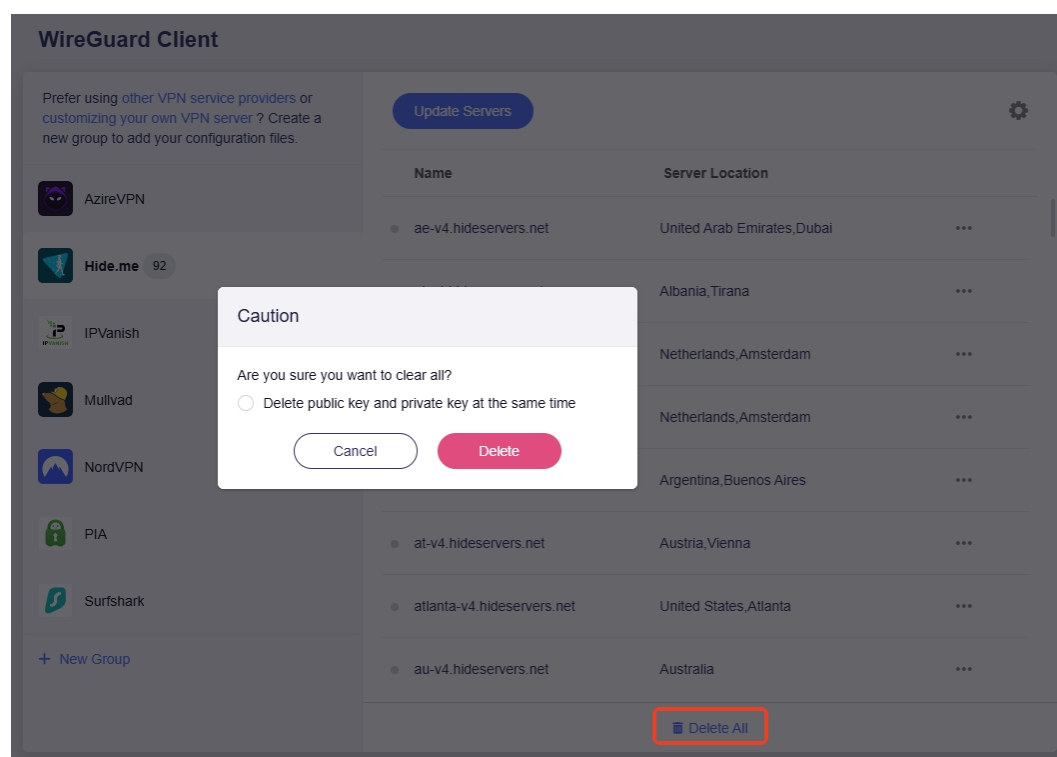
6. Edit credentials or logout.

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



7. Delete all files.

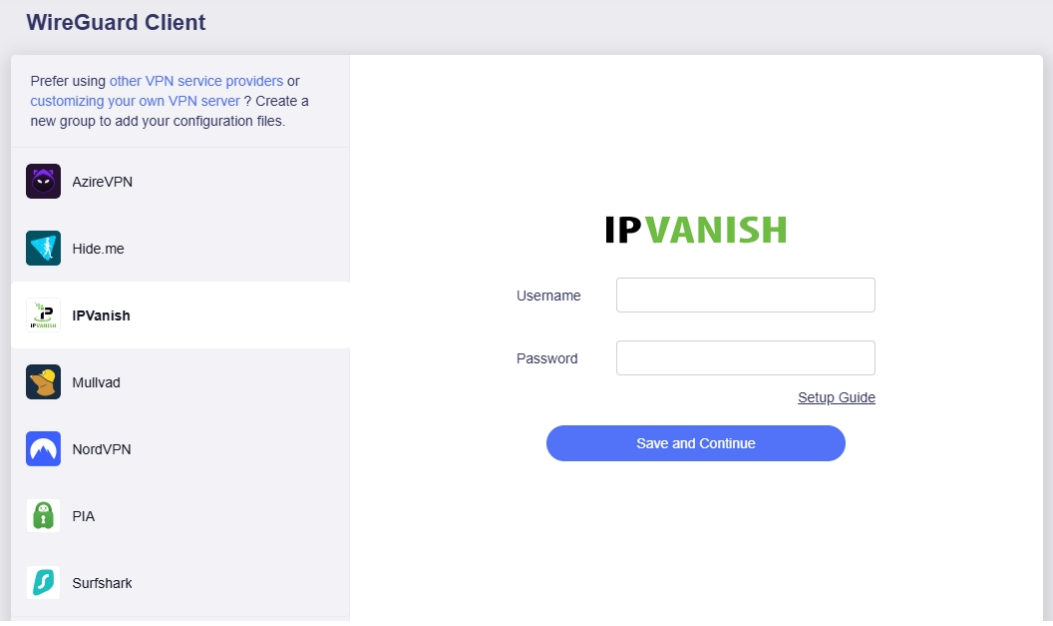
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.4 Set Up IPVanish

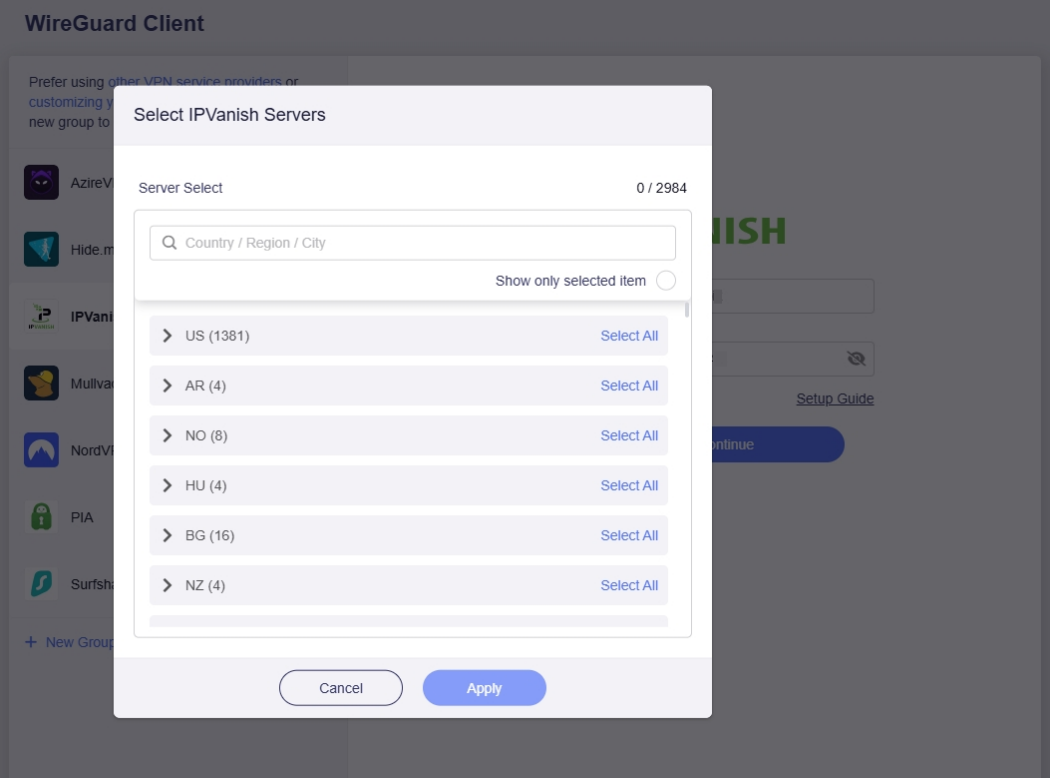
Follow the steps below to set your router as an IPVanish client.

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: AzireVPN, Hide.me, IPVanish (highlighted), Mullvad, NordVPN, PIA, and Surfshark. The main area is titled 'IPVANISH' in green. It contains two input fields: 'Username' and 'Password'. Below the password field is a link for 'Setup Guide'. At the bottom right is a blue button labeled 'Save and Continue'.

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

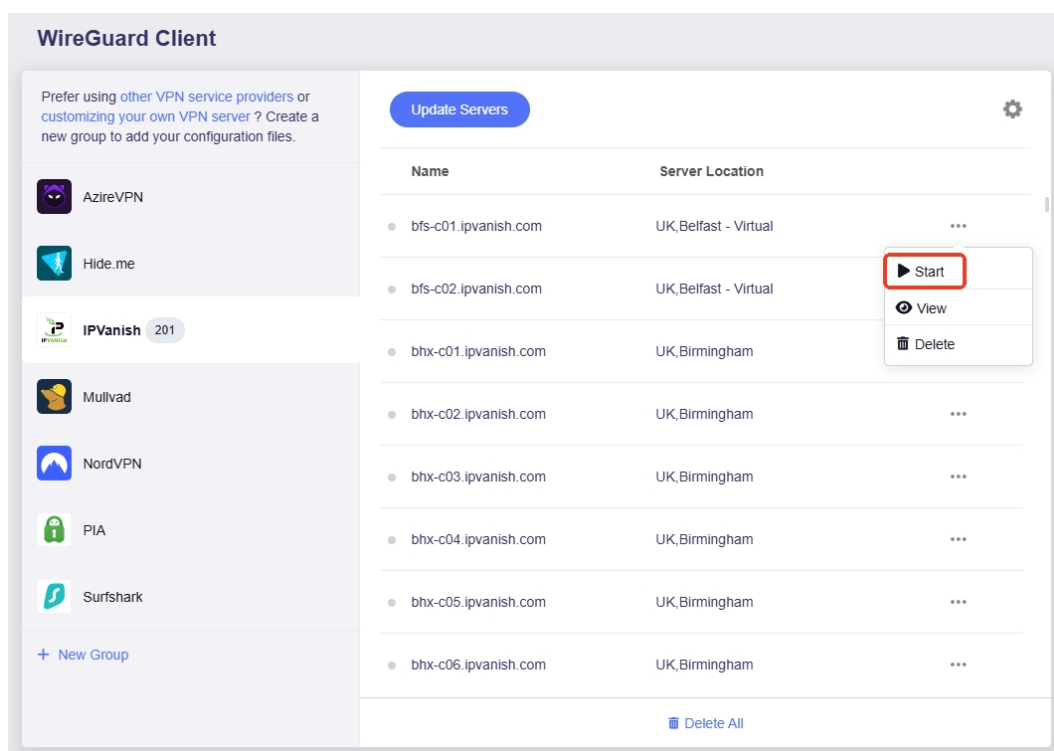


The screenshot shows a 'Select IPVanish Servers' dialog box overlaid on the main configuration page. The dialog has a search bar labeled 'Country / Region / City' and a 'Show only selected item' toggle. Below the search bar is a list of server groups with expandable arrows and 'Select All' links:

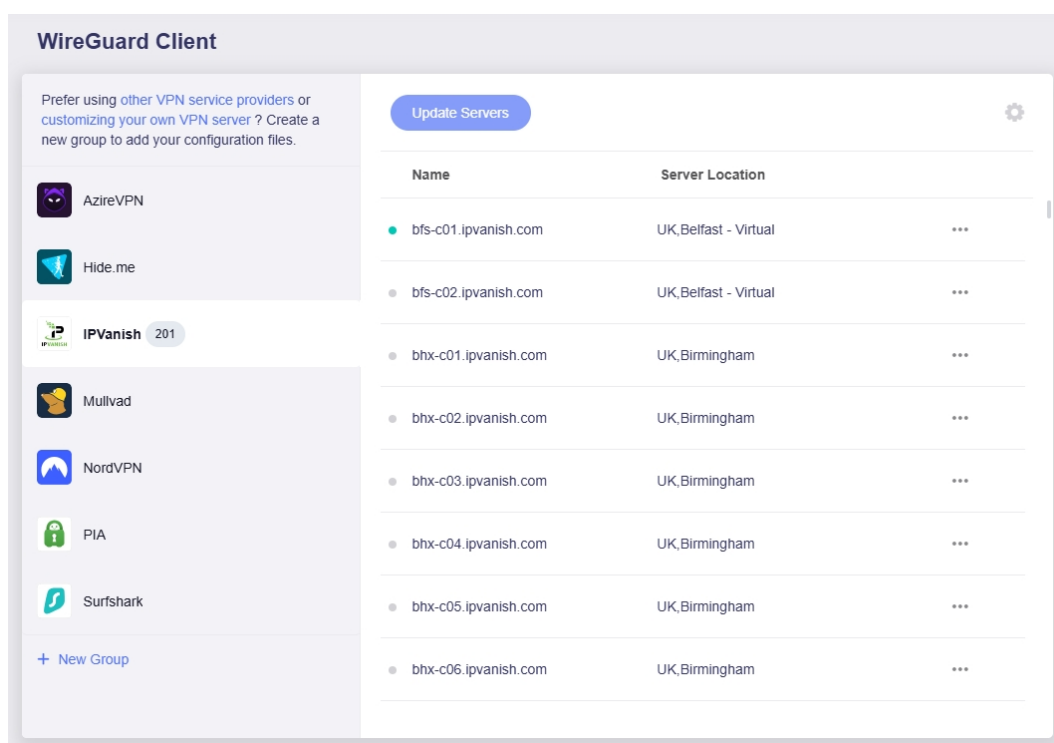
- > US (1381) [Select All](#)
- > AR (4) [Select All](#)
- > NO (8) [Select All](#)
- > HU (4) [Select All](#)
- > BG (16) [Select All](#)
- > NZ (4) [Select All](#)

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.



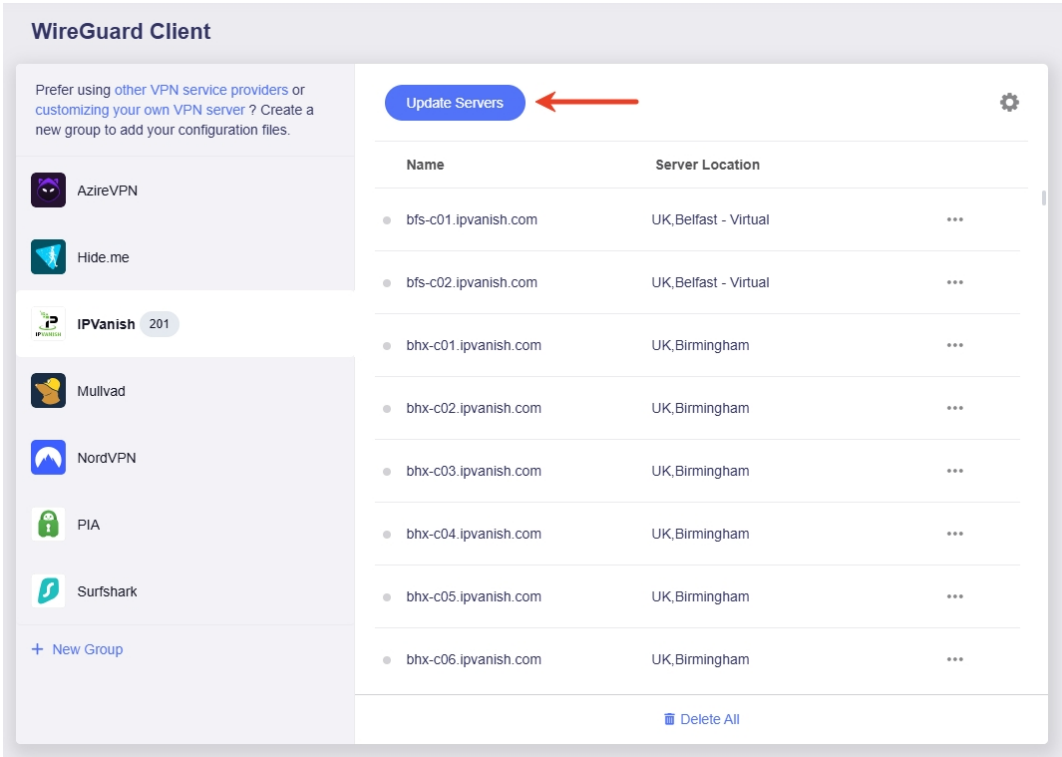
5. Once connected, a green dot will appear next to the configuration file.



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

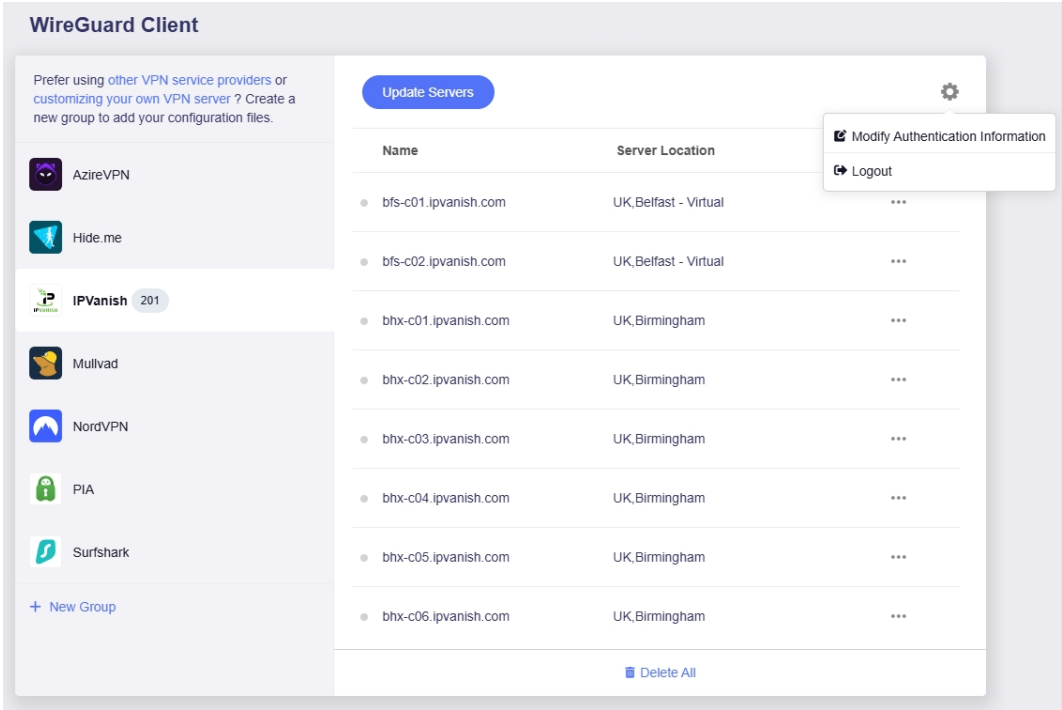
6. Update servers.

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



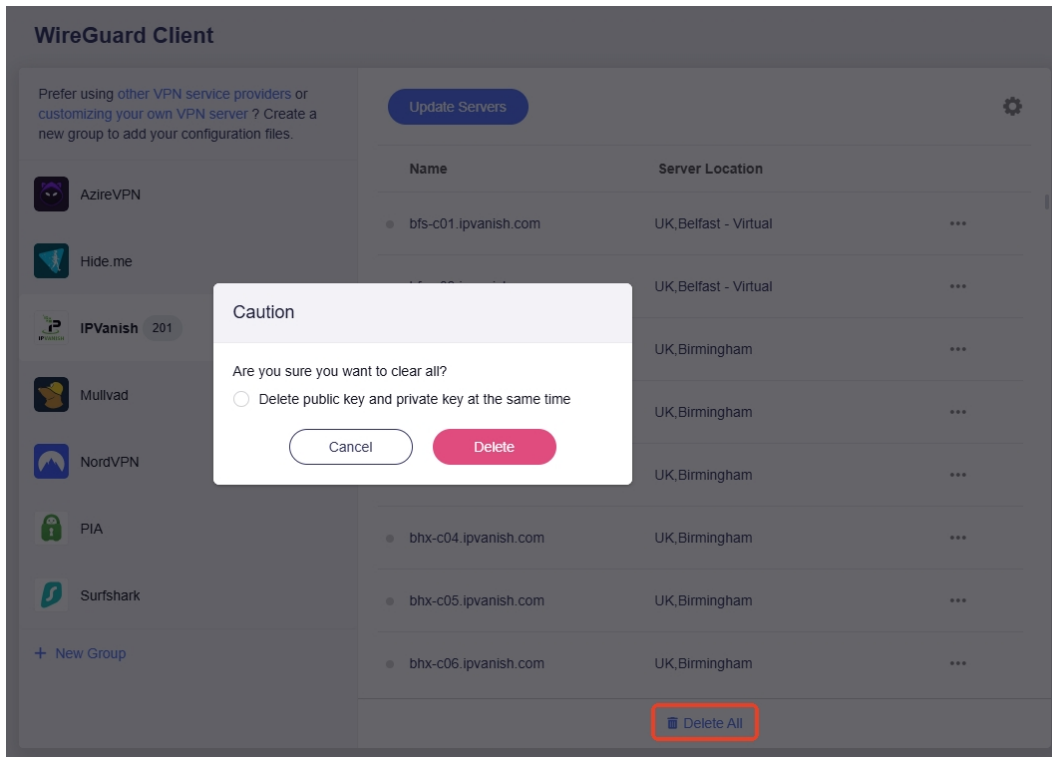
7. Edit credentials or logout.

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



8. Delete all files.

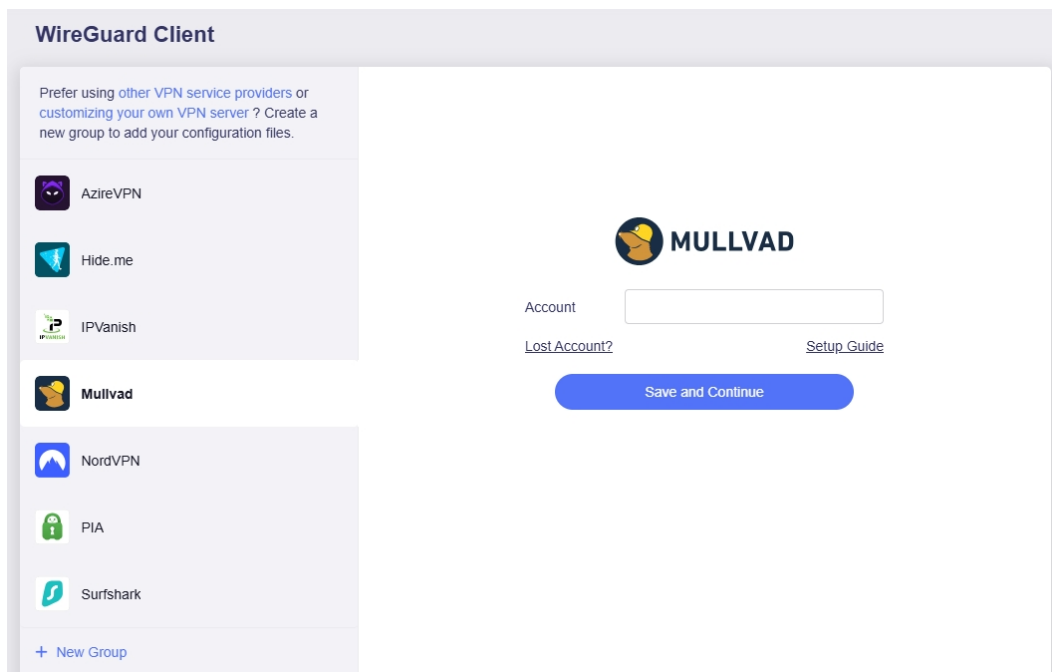
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.5 Set Up Mullvad

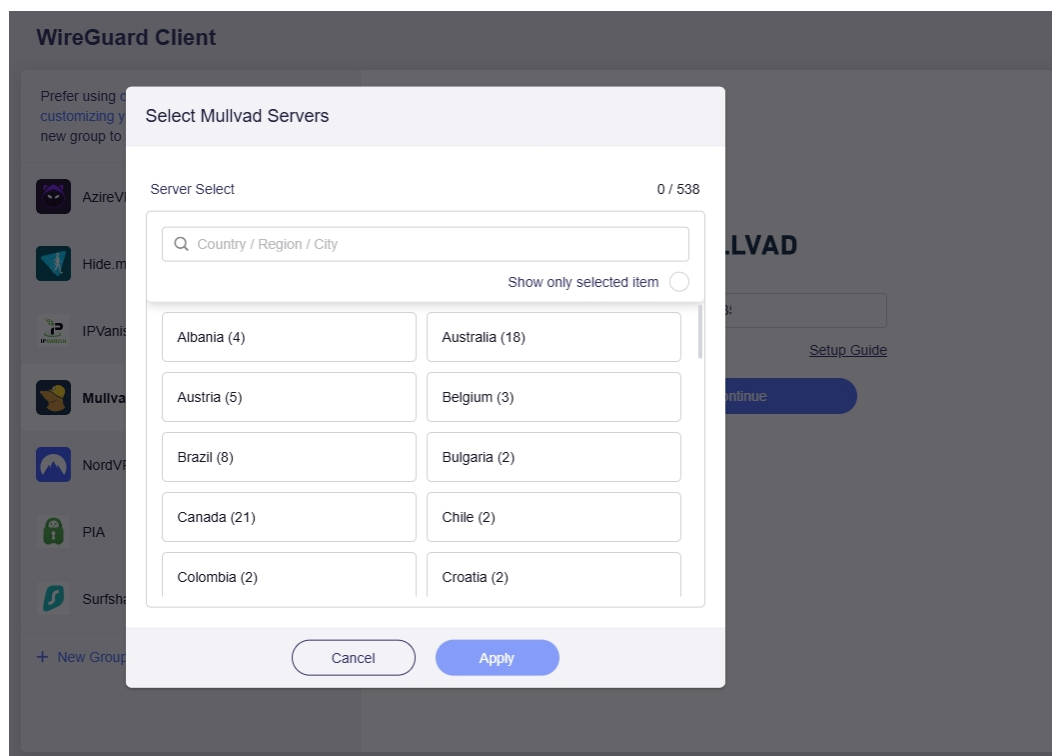
Follow the steps below to set your router as a Mullvad client.

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**.



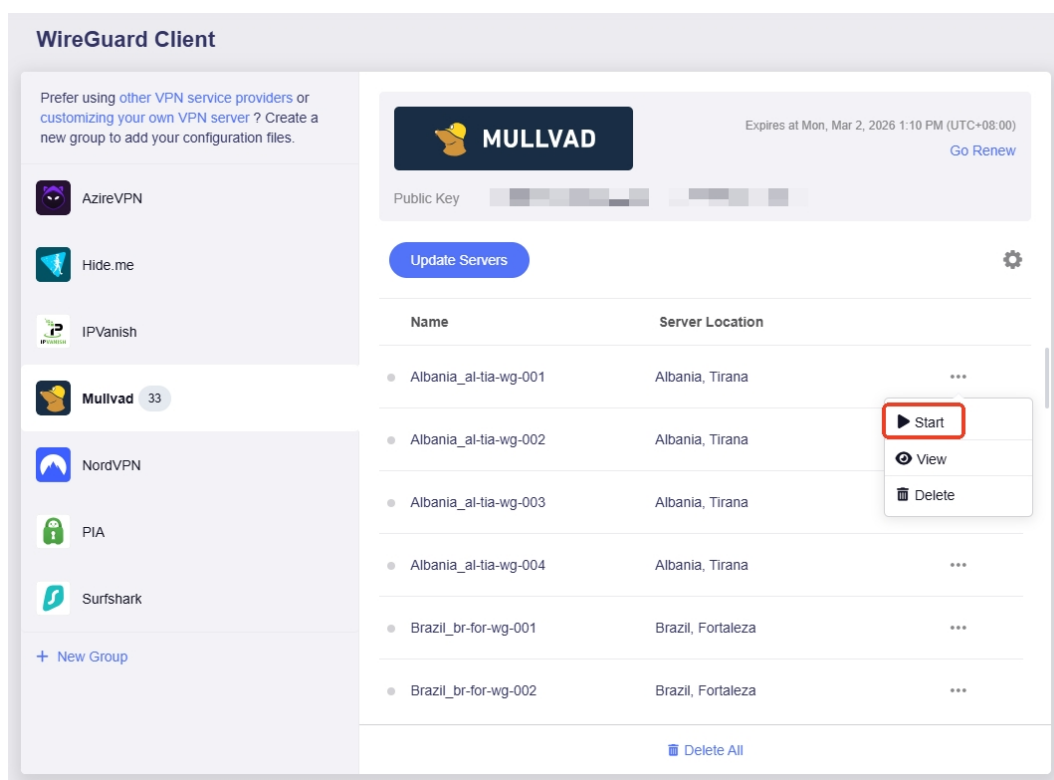
The screenshot shows the 'WireGuard Client' configuration page for Mullvad. On the left, there is a list of VPN providers: AzureVPN, Hide.me, IPVanish, Mullvad (selected), NordVPN, PIA, and Surfshark. Below this list is a '+ New Group' link. The main area on the right features the Mullvad logo, an 'Account' input field, a 'Lost Account?' link, and a 'Setup Guide' link. At the bottom of this section is a blue 'Save and Continue' button.

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

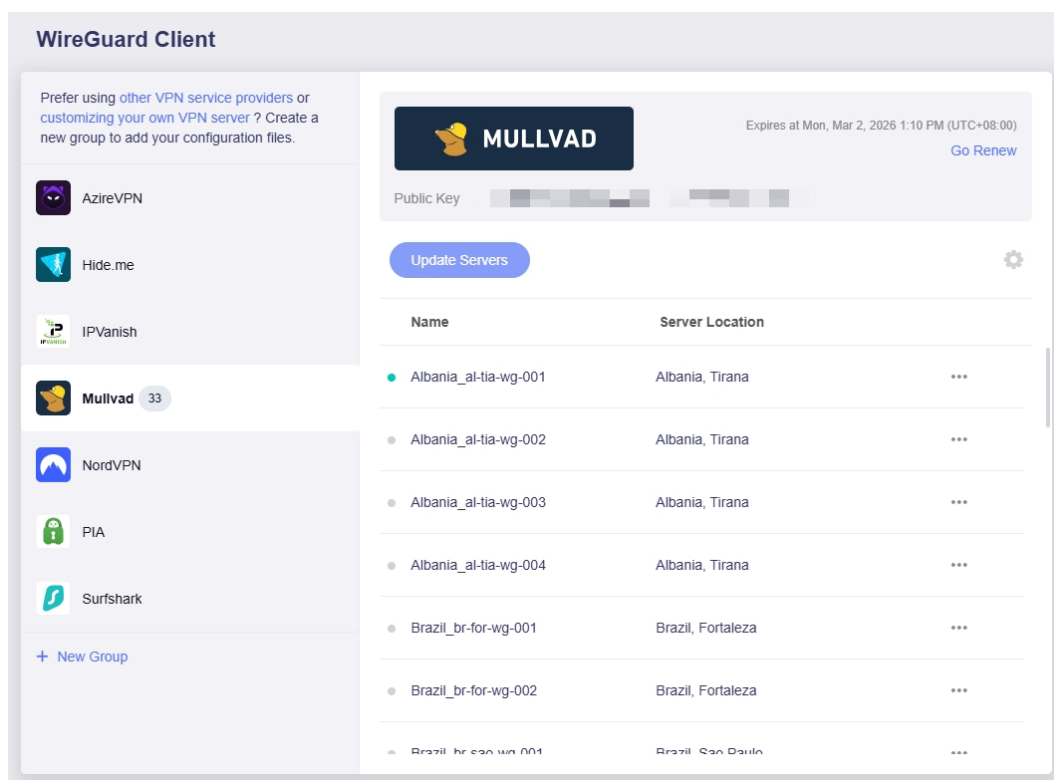


The screenshot shows a 'Select Mullvad Servers' dialog box overlaid on the WireGuard Client page. The dialog has a title bar 'Select Mullvad Servers' and a 'Server Select' header with a count '0 / 538'. Below the header is a search bar with the placeholder text 'Country / Region / City'. To the right of the search bar is a toggle switch labeled 'Show only selected item'. The main area of the dialog contains a grid of buttons representing different countries and the number of servers available in each: Albania (4), Australia (18), Austria (5), Belgium (3), Brazil (8), Bulgaria (2), Canada (21), Chile (2), Colombia (2), and Croatia (2). 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.



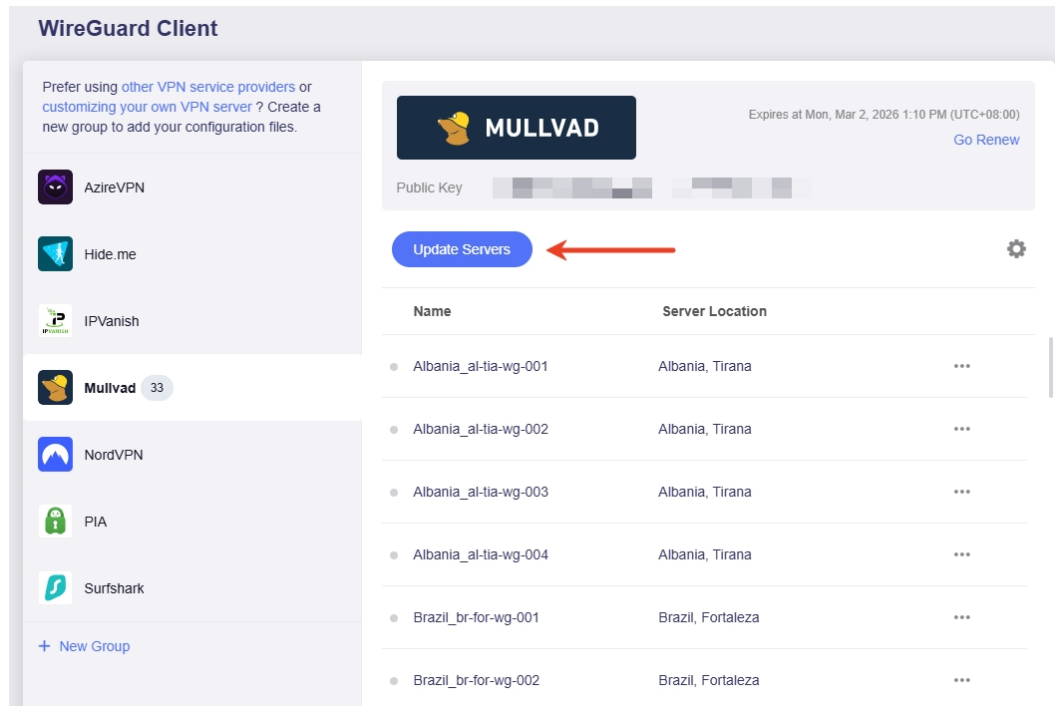
5. Once connected, a green dot will appear next to the configuration file.



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

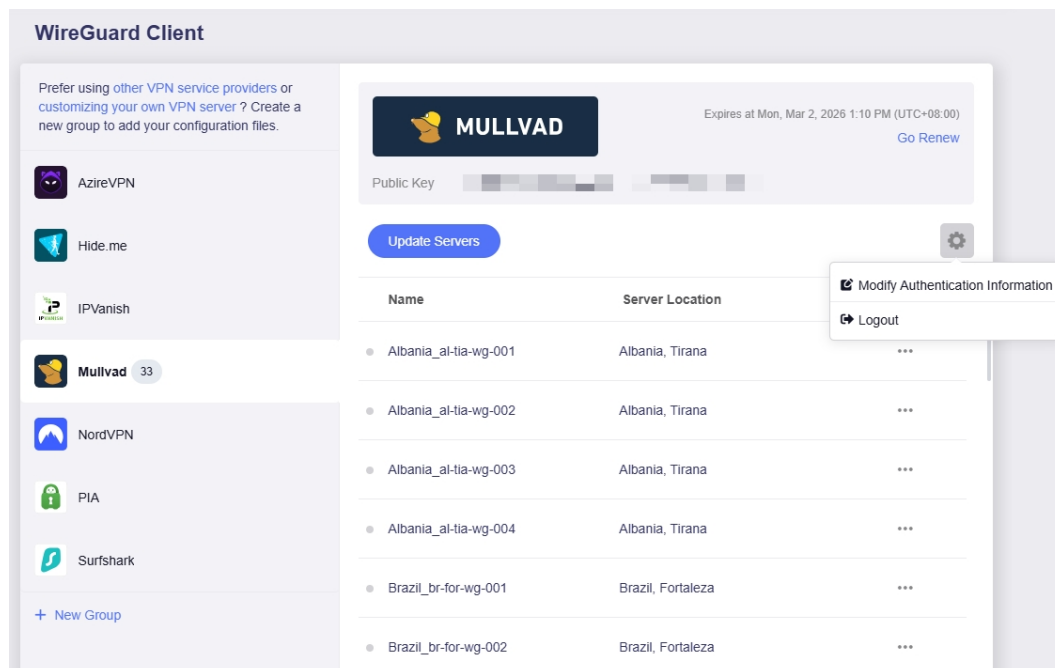
6. Update servers.

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



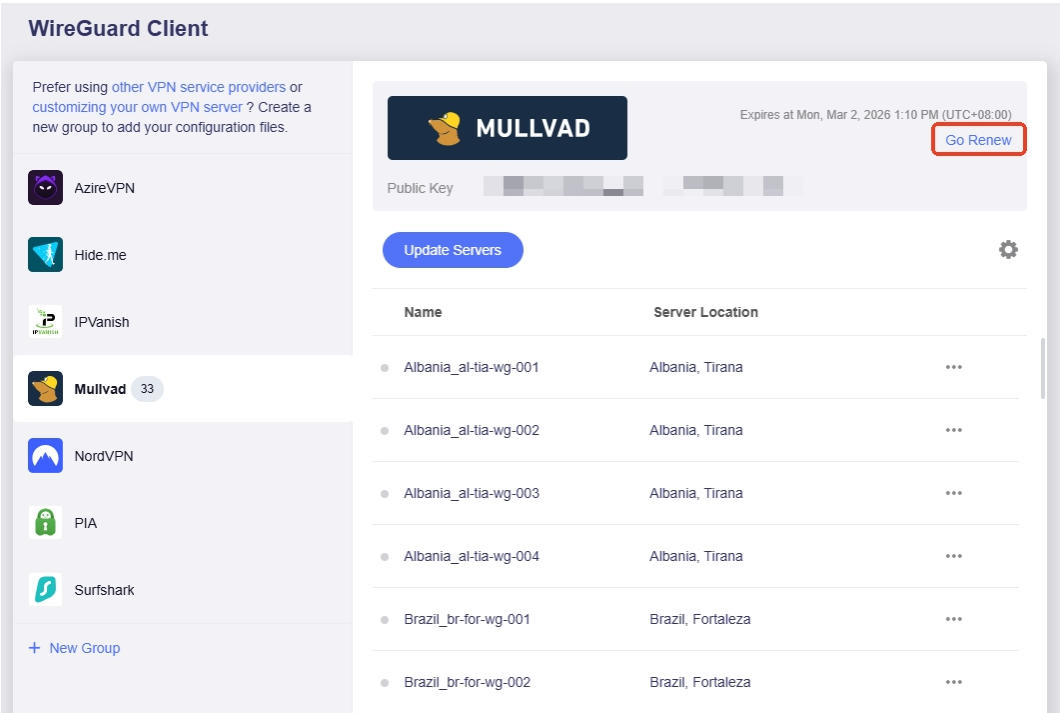
7. Edit credentials or logout.

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



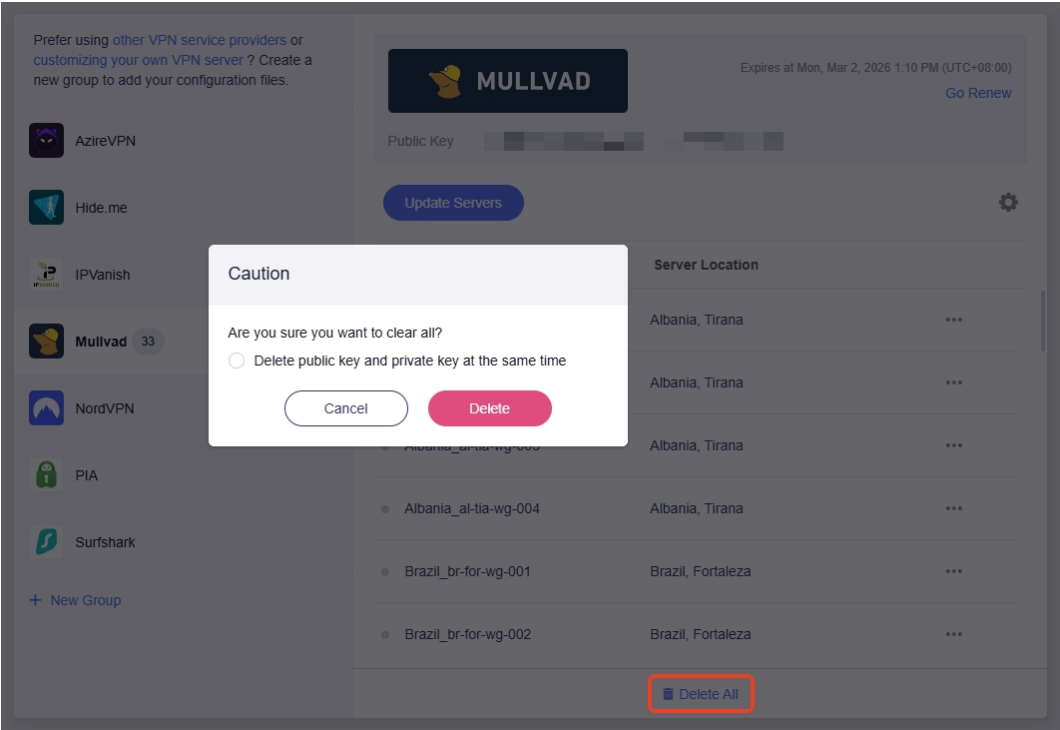
8. Go renew.

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



9. Delete all files.

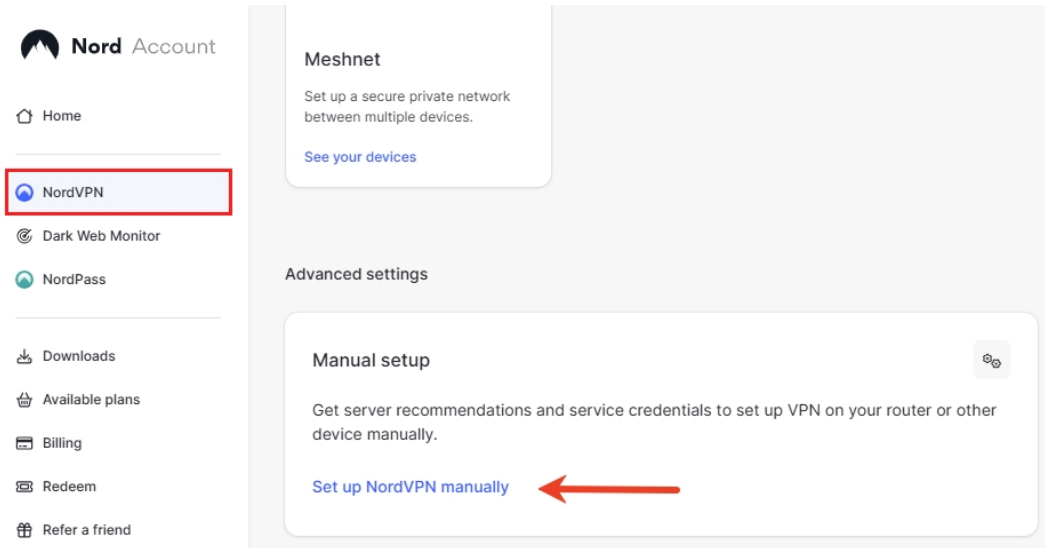
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



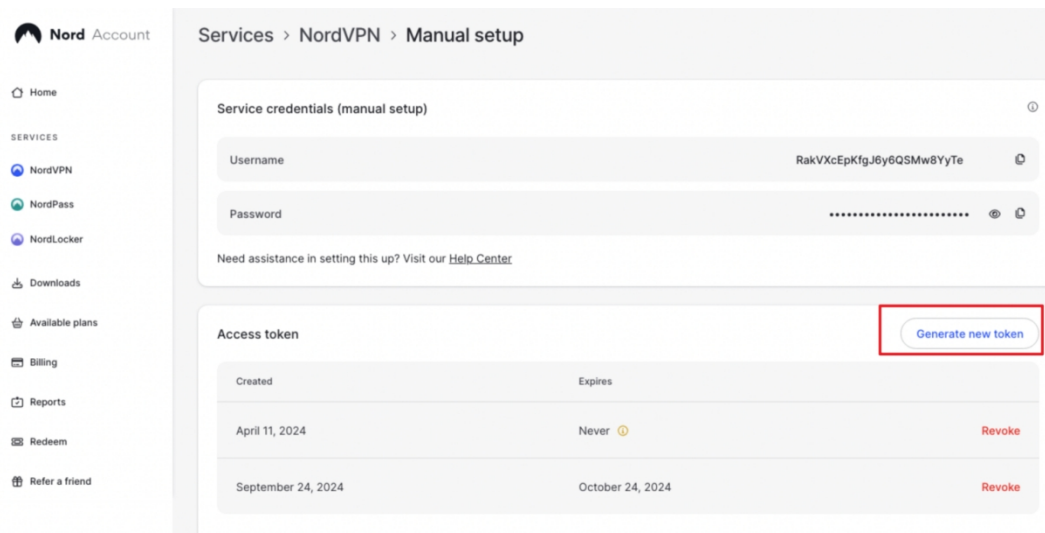
11.2.6 Set Up NordVPN

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

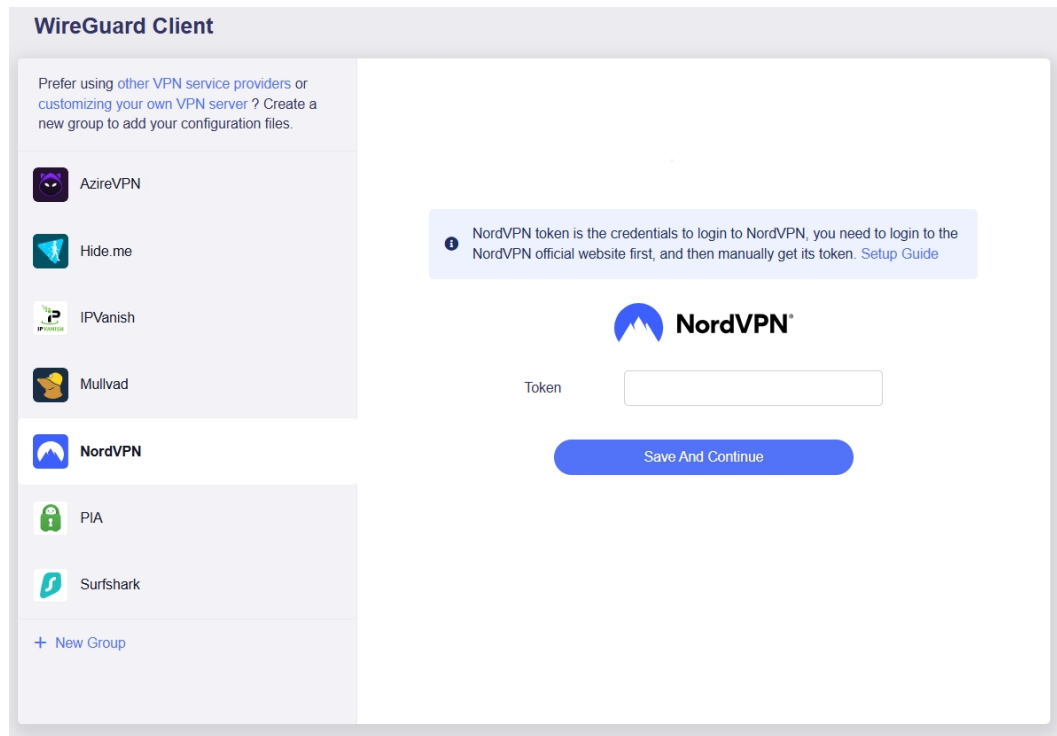
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



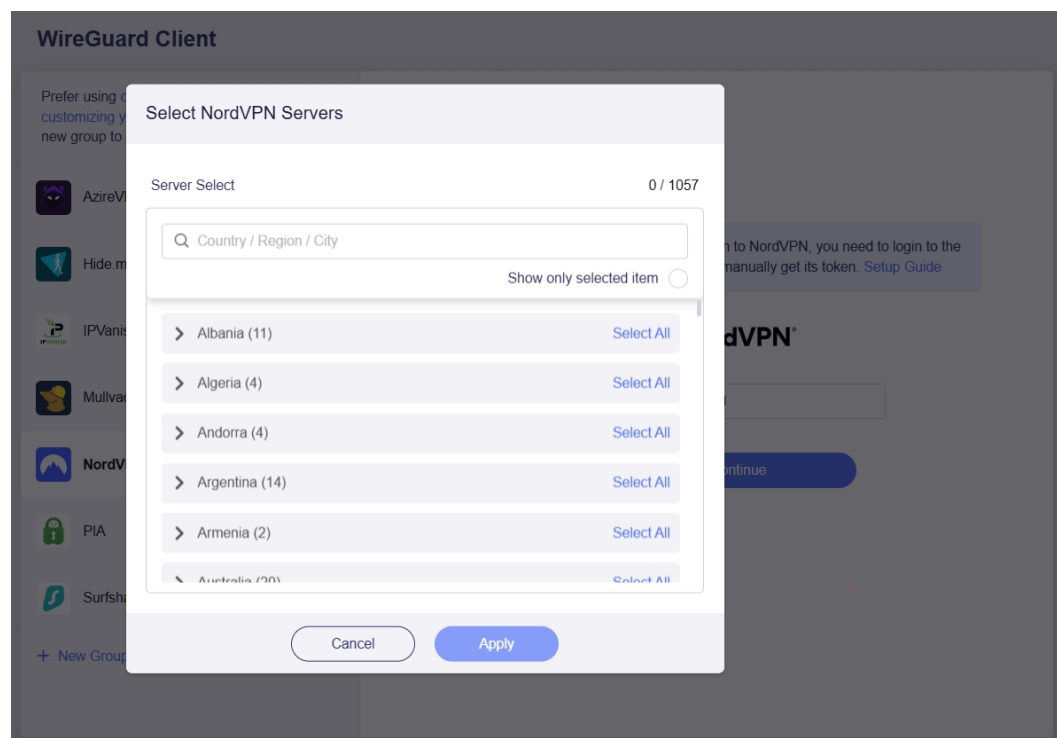
You will find the **Access Token**. Create an access token and copy for later use.



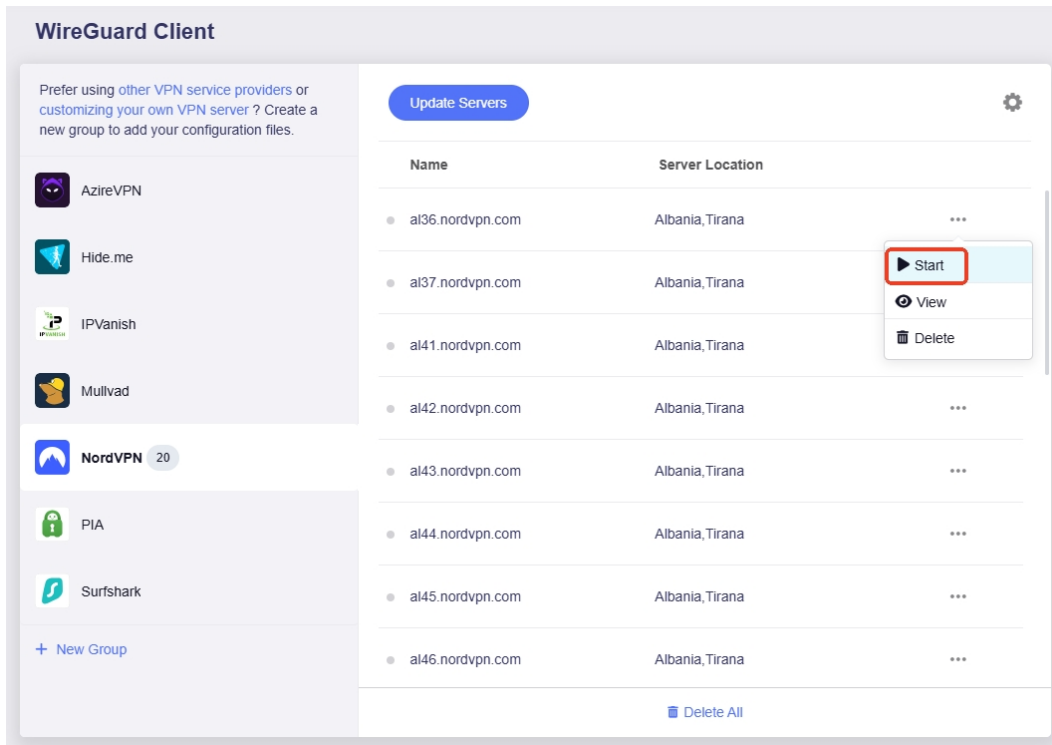
3. Log in to your router's web admin panel and go to **VPN > WireGuard Client > NordVPN**.
4. Input token, and click **Save and Continue**.



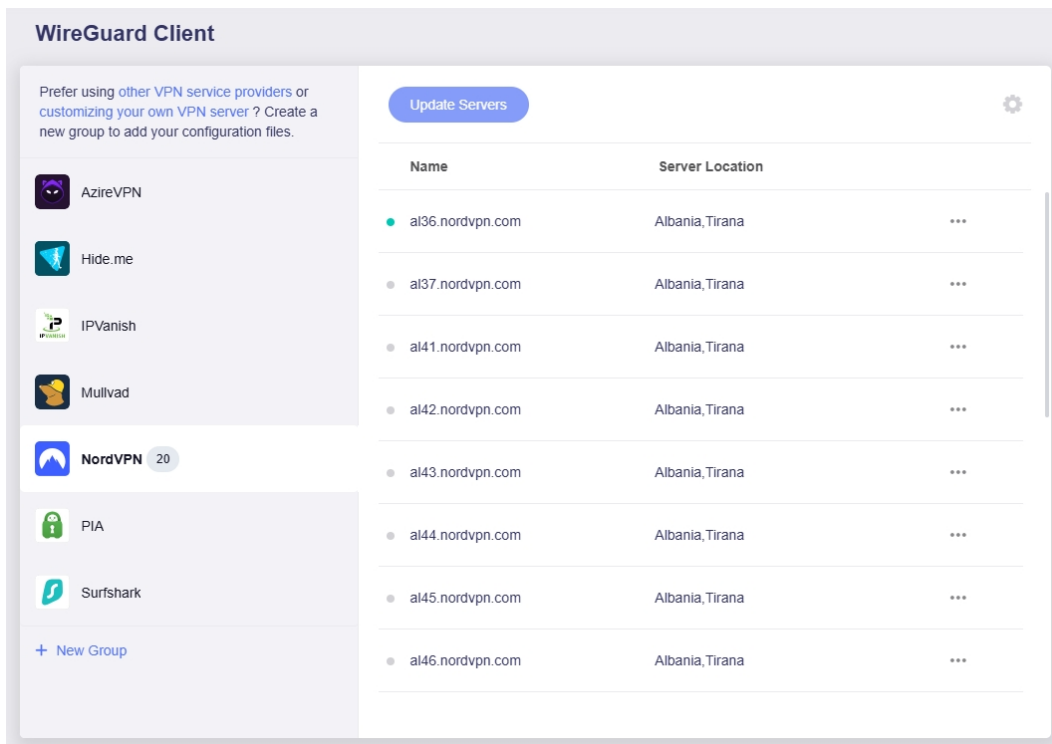
5. Select the server(s) you want to connect to, and click **Apply**.



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



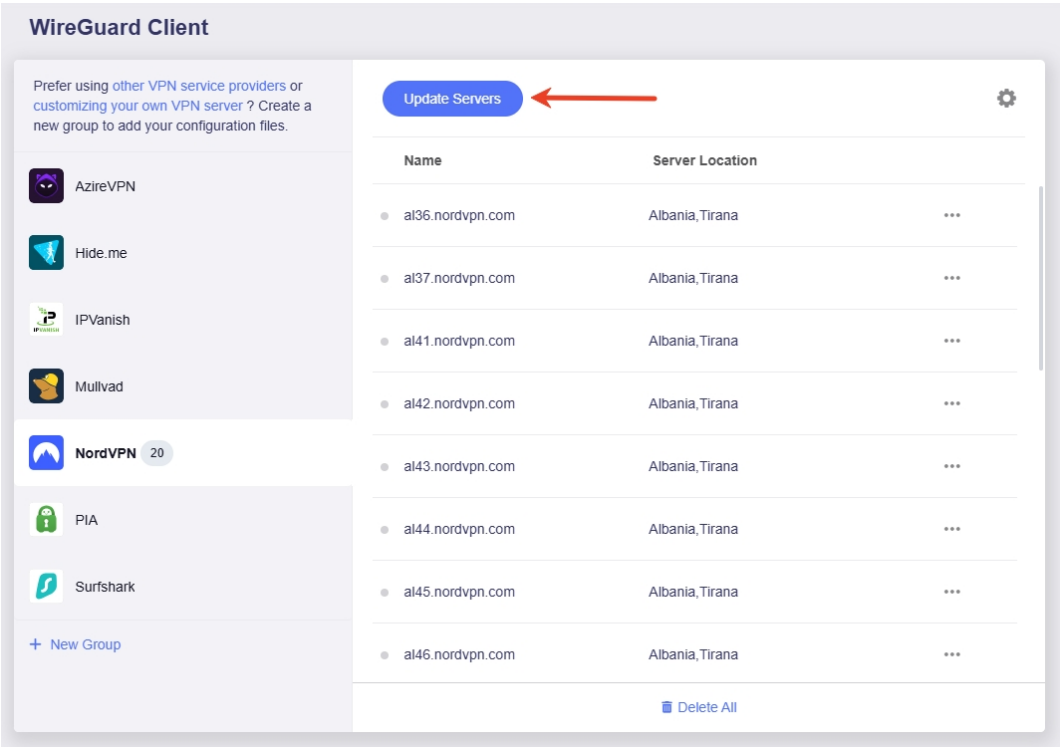
- Once connected, a green dot will appear next to the configuration file.



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

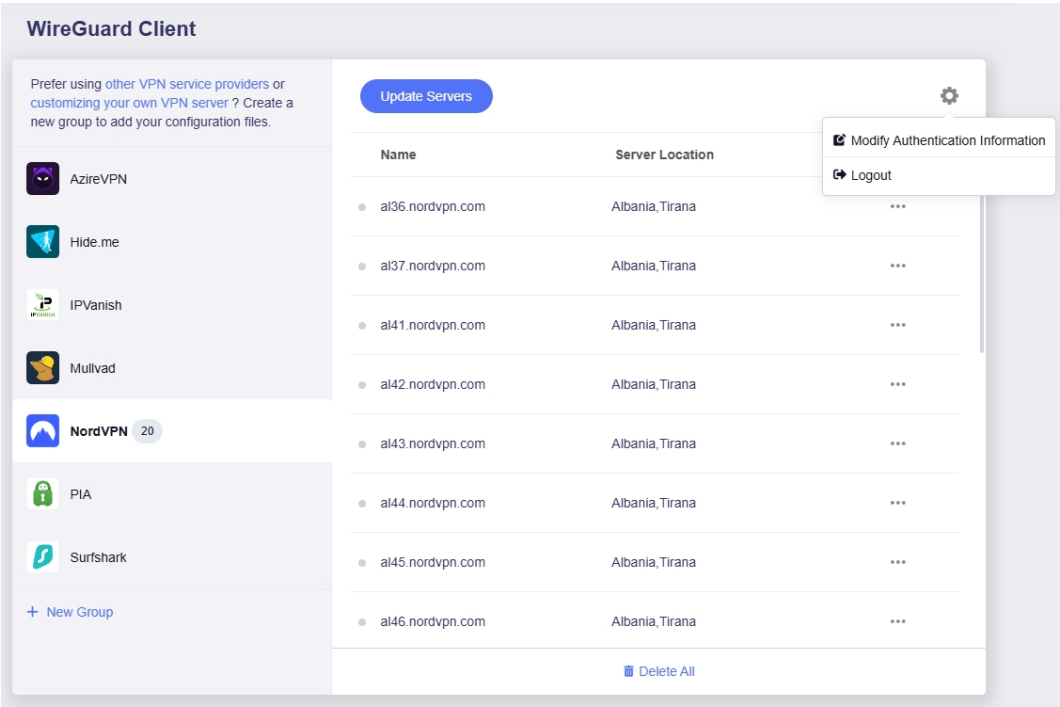
- Update servers.

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



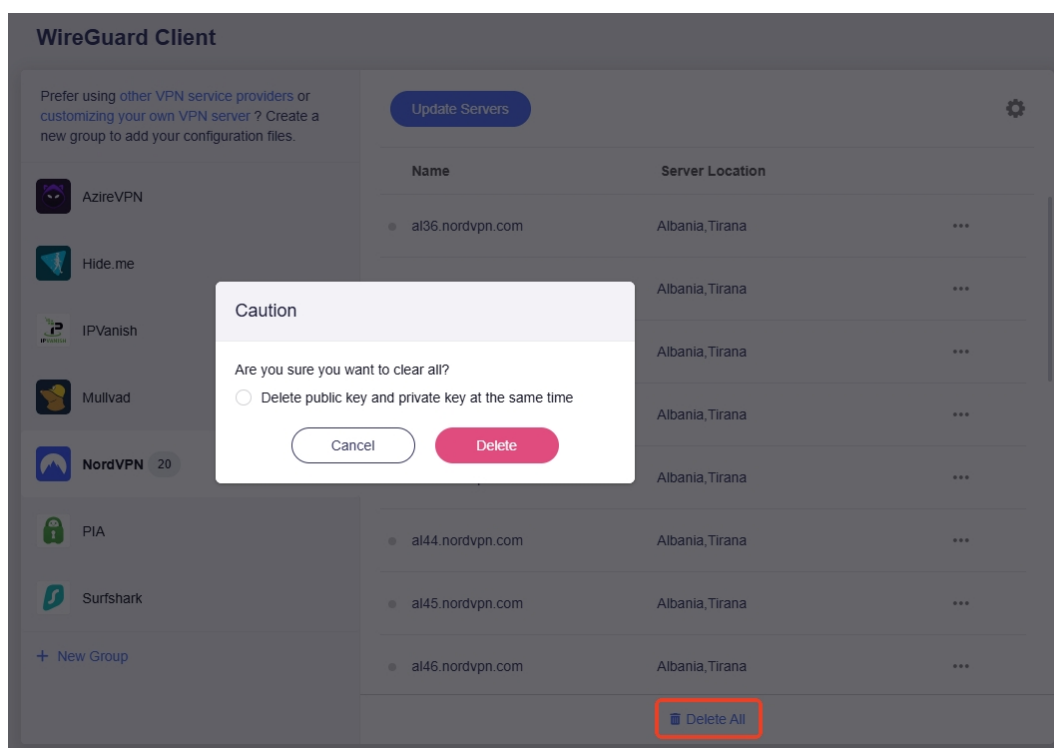
9. Edit credentials or logout.

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



10. Delete all files.

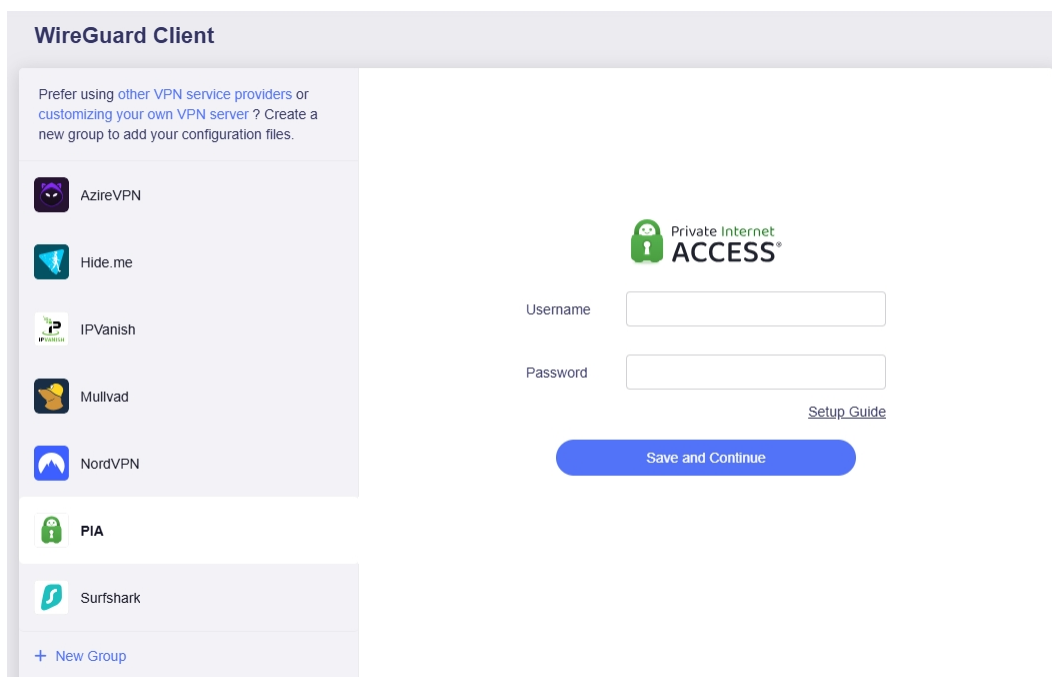
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.7 Set Up PIA (Private Internet Access)

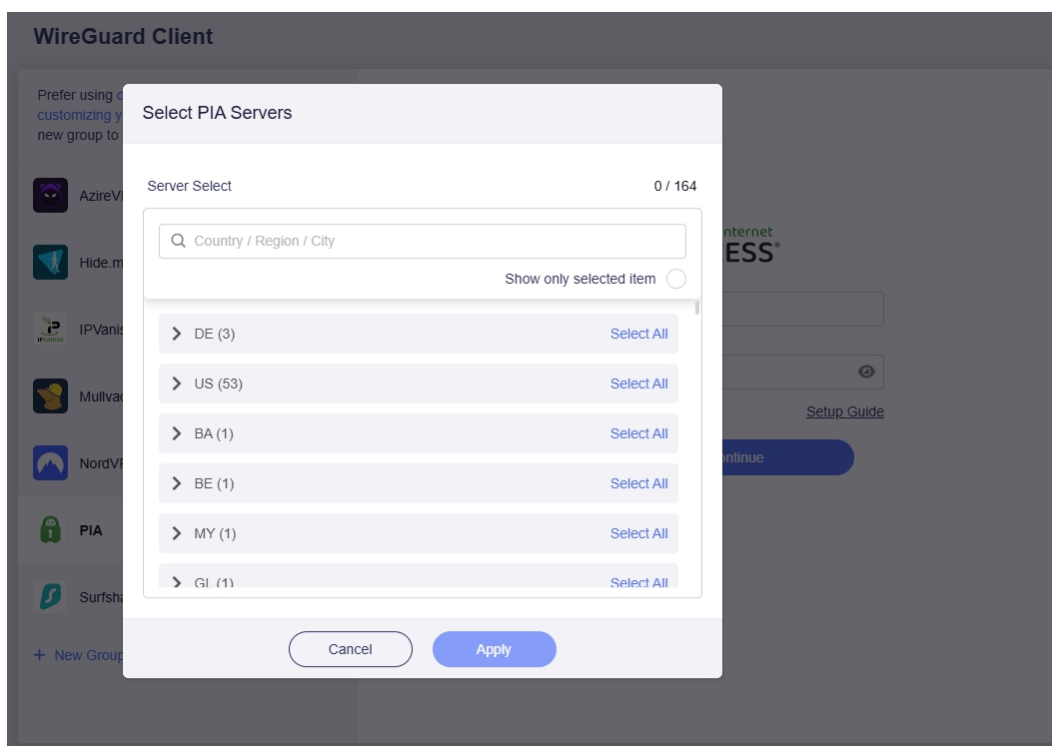
Follow the steps below to set your router as a PIA client.

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**.



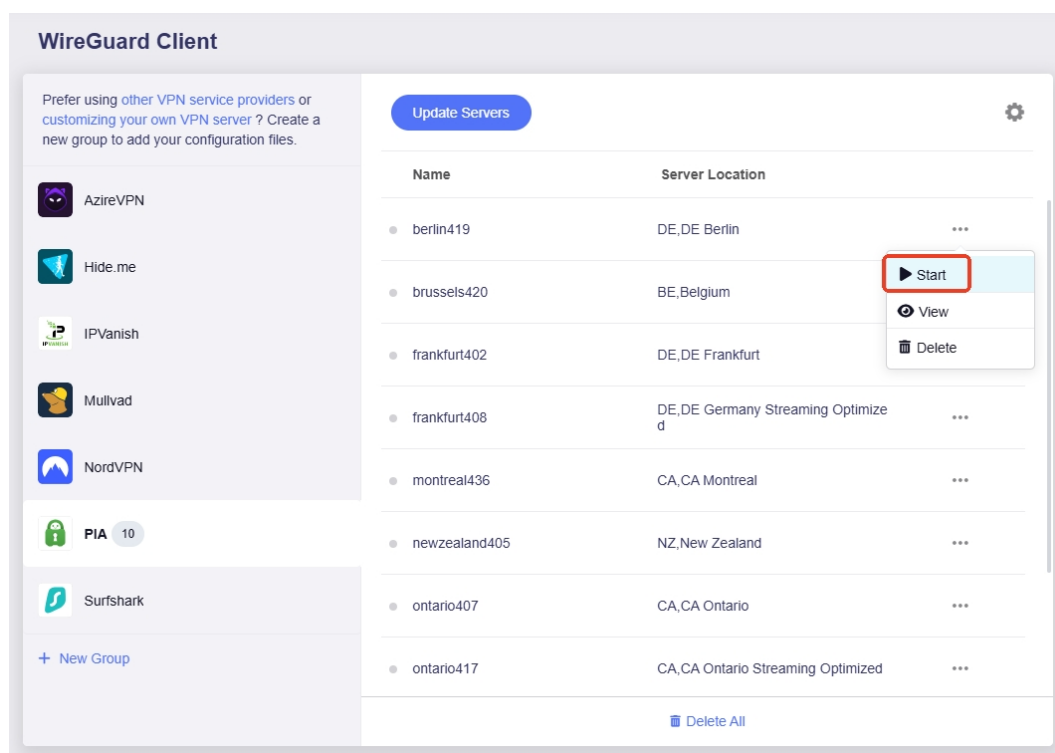
The screenshot shows the 'WireGuard Client' configuration page in a router's web interface. On the left, there is a list of VPN providers: AzureVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA (highlighted), and Surfshark, with a '+ New Group' option at the bottom. The main area on the right is for PIA configuration, featuring the PIA logo and the text 'Private Internet ACCESS'. Below the logo are input fields for 'Username' and 'Password'. A 'Setup Guide' link is located below the password field. At the bottom right of the main area is a blue 'Save and Continue' button.

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

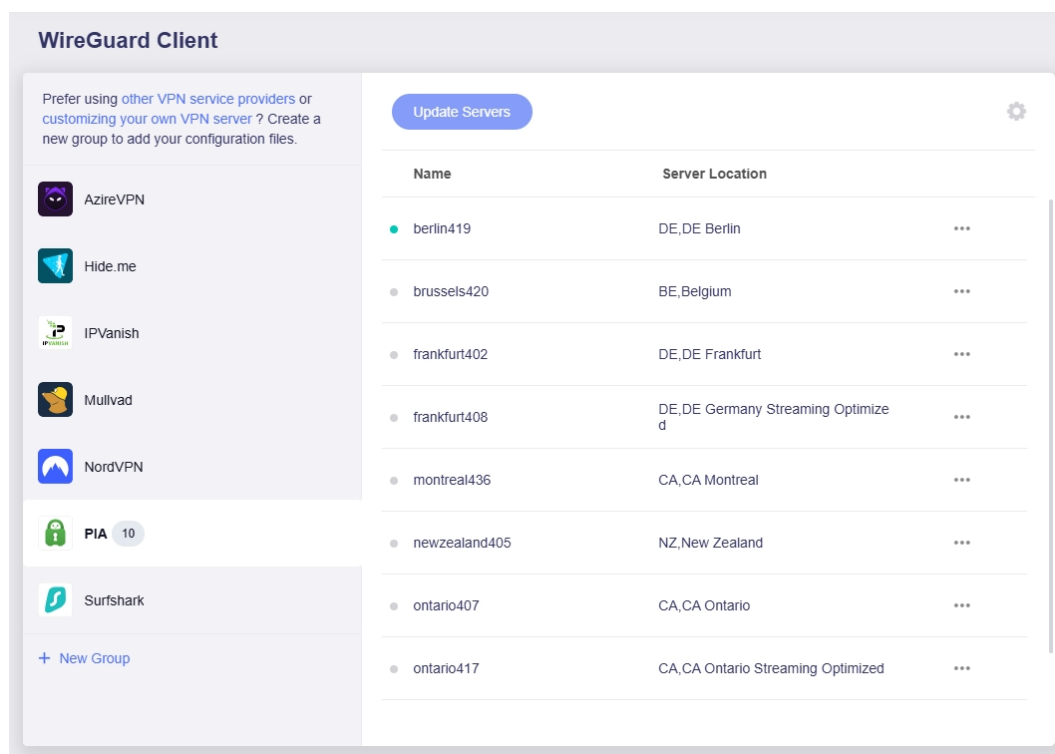


The screenshot shows the 'WireGuard Client' page with a 'Select PIA Servers' modal dialog open. The dialog has a title bar 'Select PIA Servers' and a subtitle 'Server Select' with a counter '0 / 164'. It features a search bar with the placeholder 'Country / Region / City' and a 'Show only selected item' toggle. Below the search bar is a list of regions with expandable arrows and counts: 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.



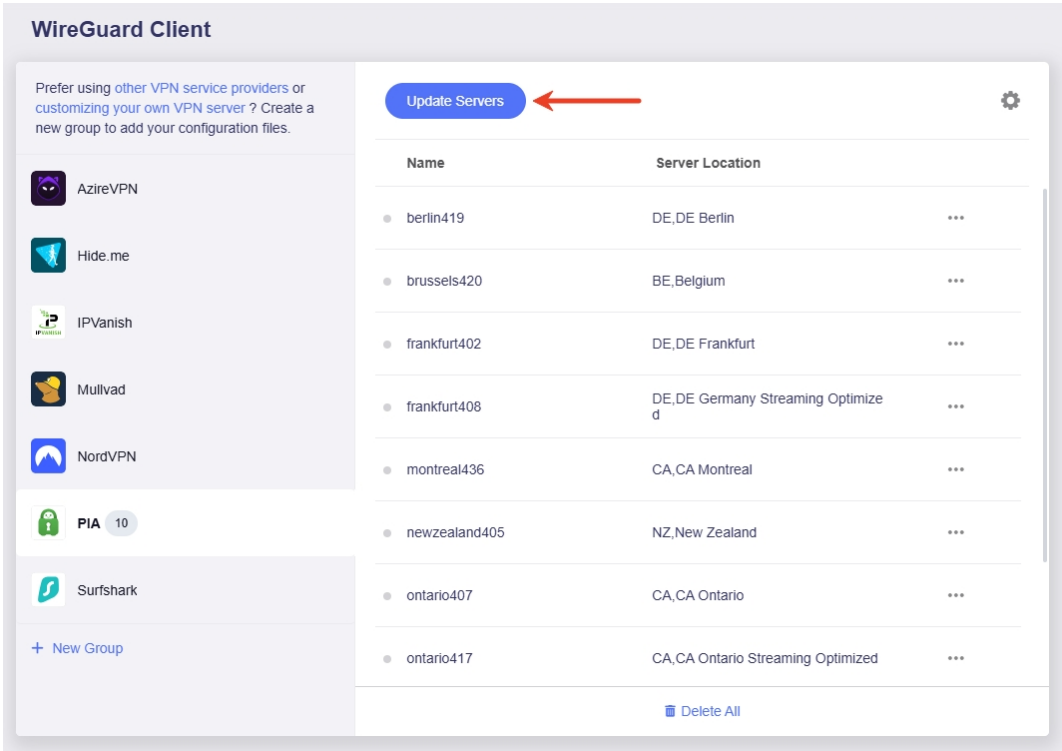
5. Once connected, a green dot will appear next to the configuration file.



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

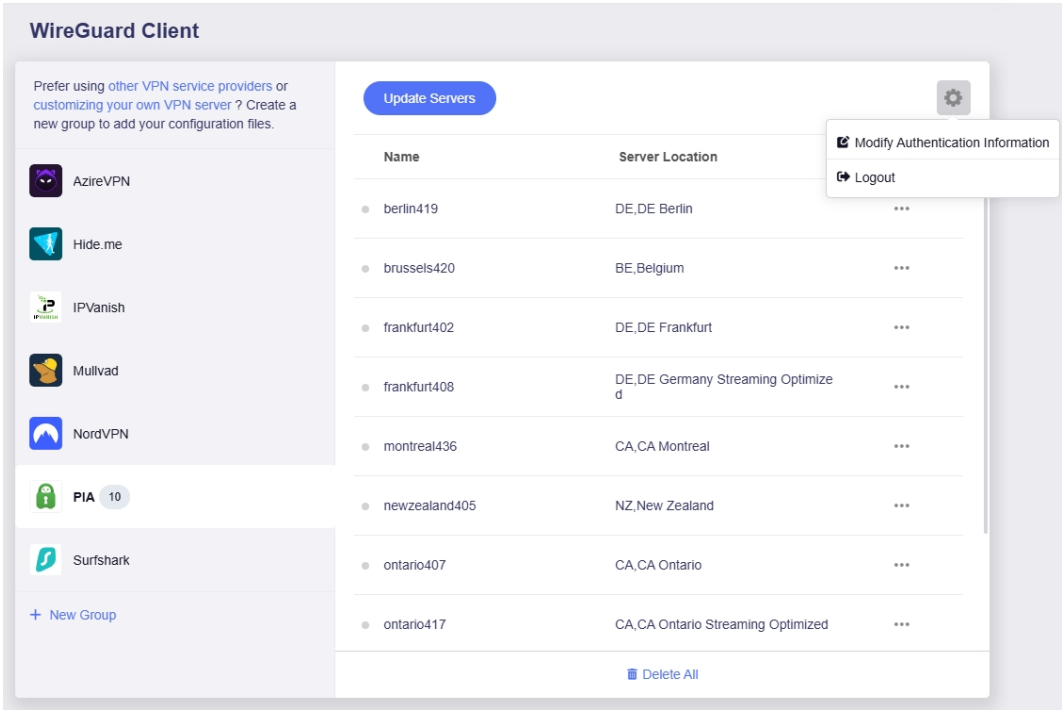
6. Update servers.

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



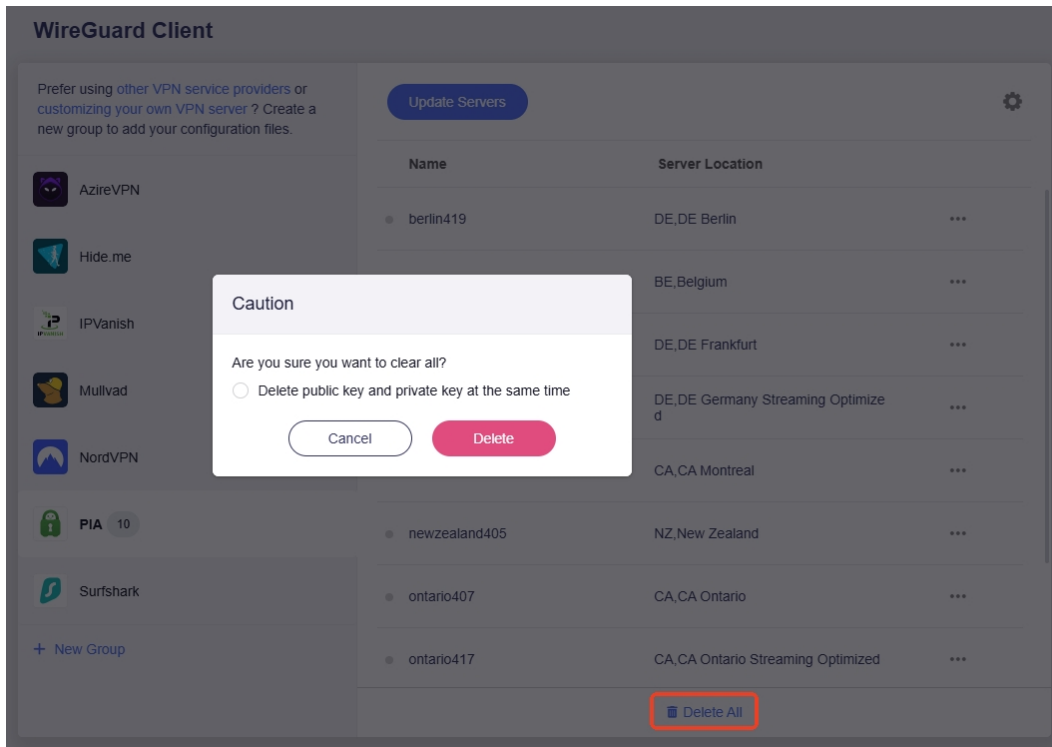
7. Edit credentials or logout.

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



8. Delete all files.

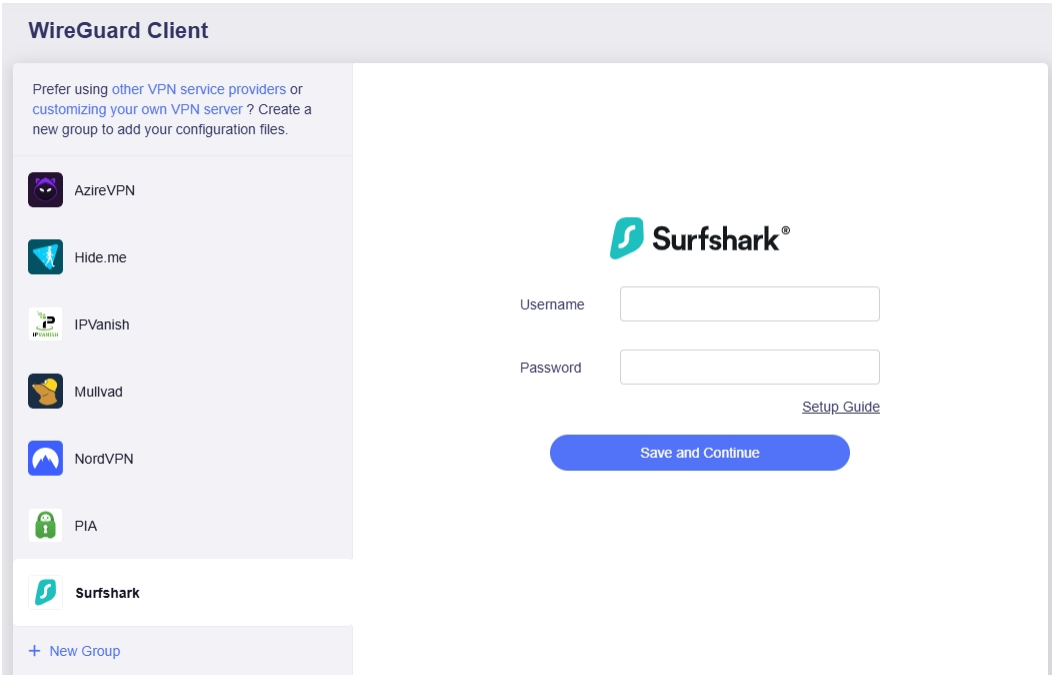
You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



11.2.8 Set Up Surfshark

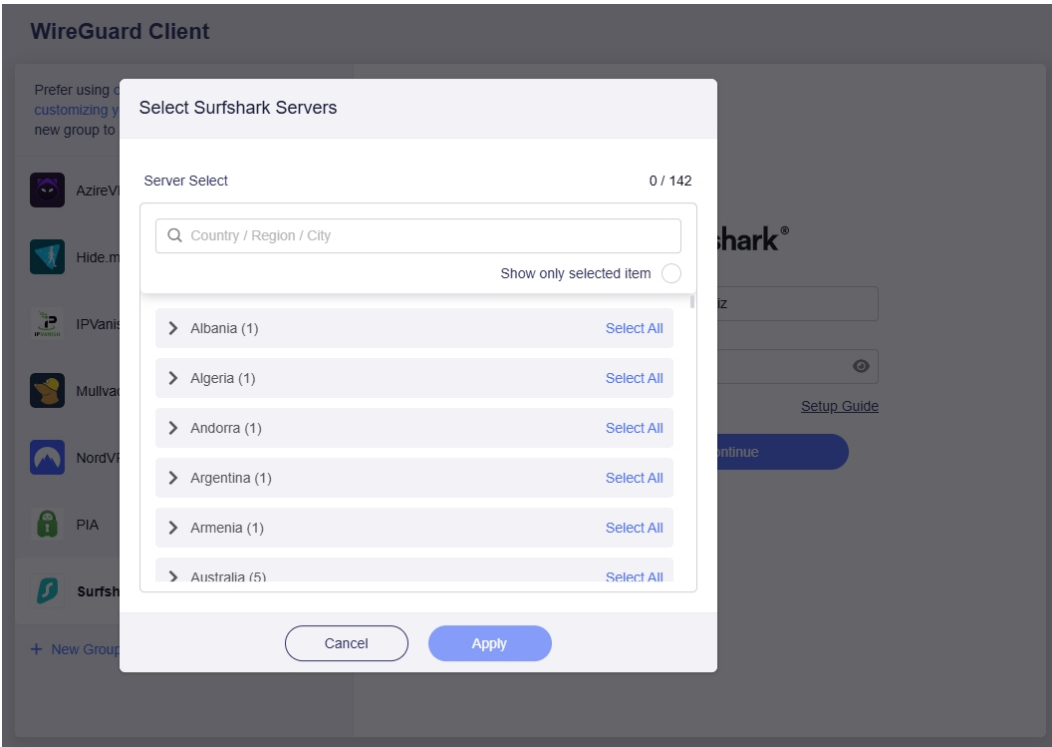
Follow the steps below to set your router as a Surfshark client.

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**.



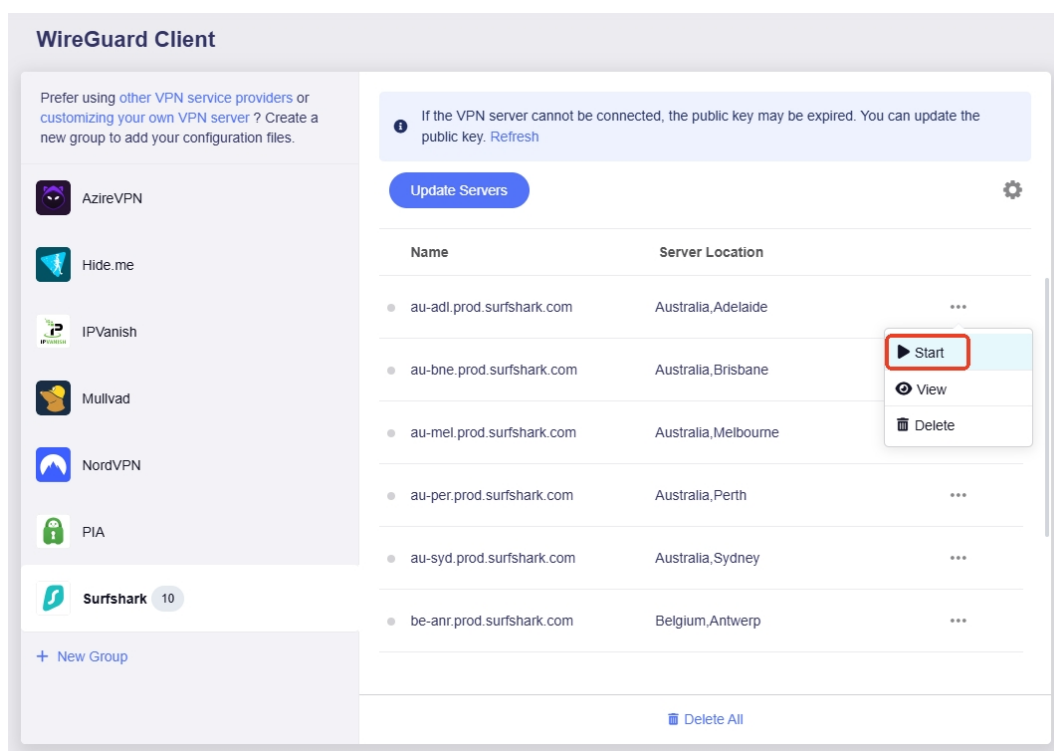
The screenshot shows the 'WireGuard Client' configuration page in a router's web interface. On the left, there is a list of VPN providers: AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA, and Surfshark. The 'Surfshark' option is selected. On the right, the 'Surfshark' logo is displayed above two input fields for 'Username' and 'Password'. Below these fields is a blue button labeled 'Save and Continue'. A link for 'Setup Guide' is also visible.

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

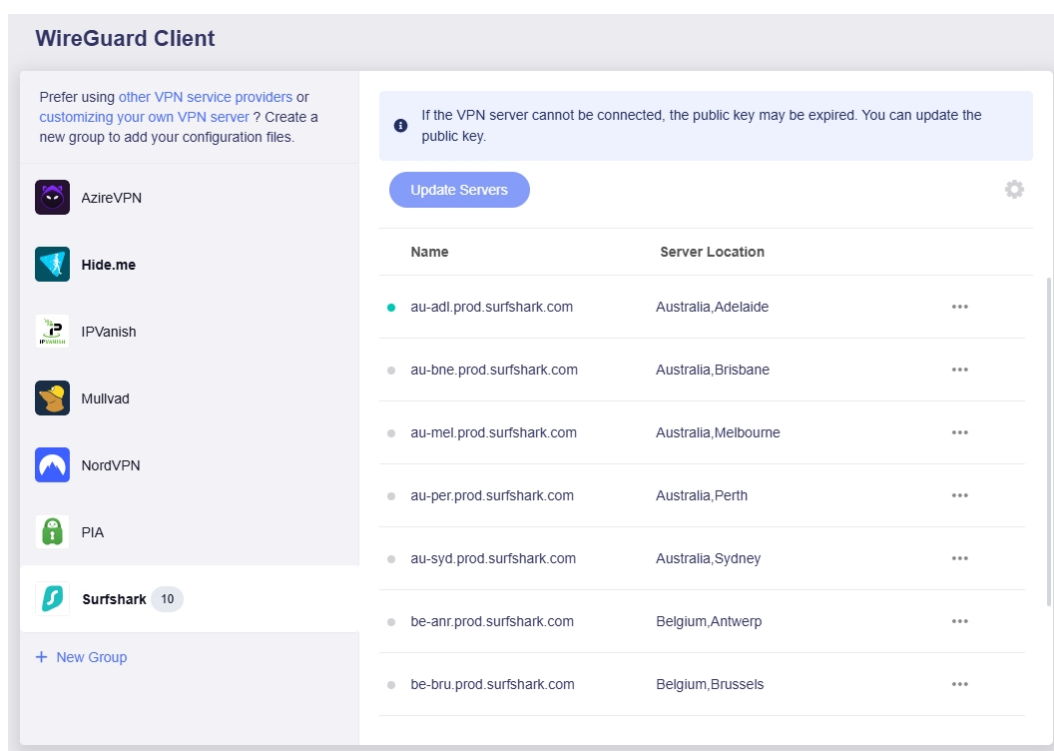


The screenshot shows a 'Select Surfshark Servers' dialog box overlaid on the configuration page. The dialog has a search bar labeled 'Country / Region / City' and a 'Show only selected item' toggle. Below the search bar, a list of countries with their respective server counts is shown: Albania (1), Algeria (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.



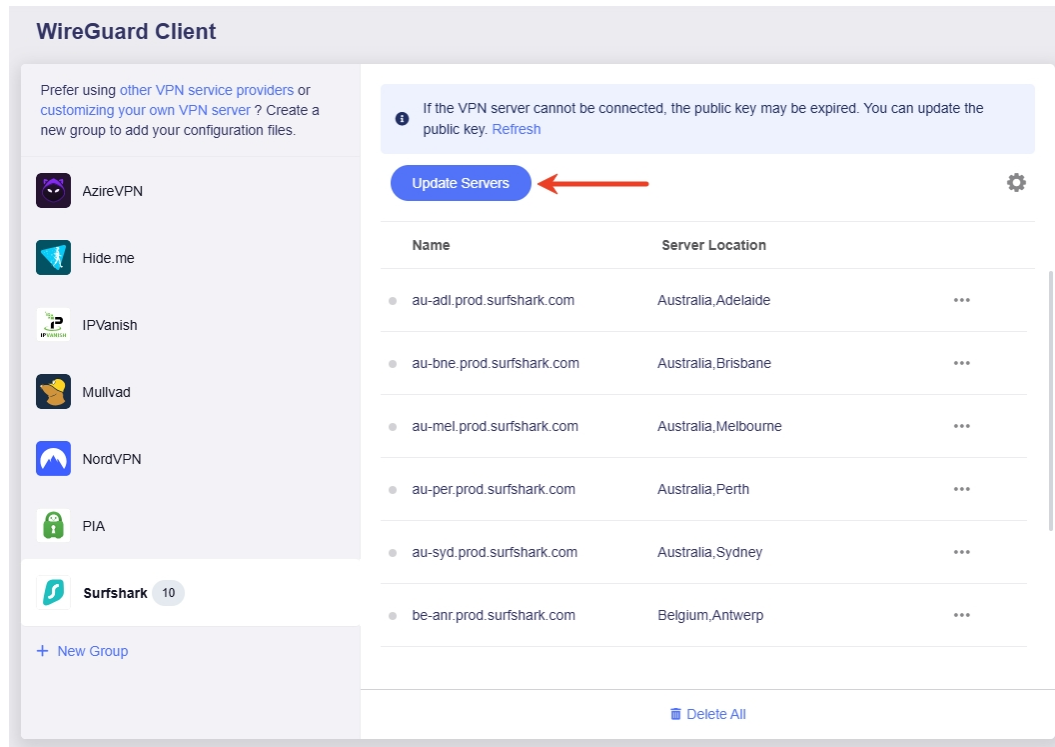
5. Once connected, a green dot will appear next to the configuration file.



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

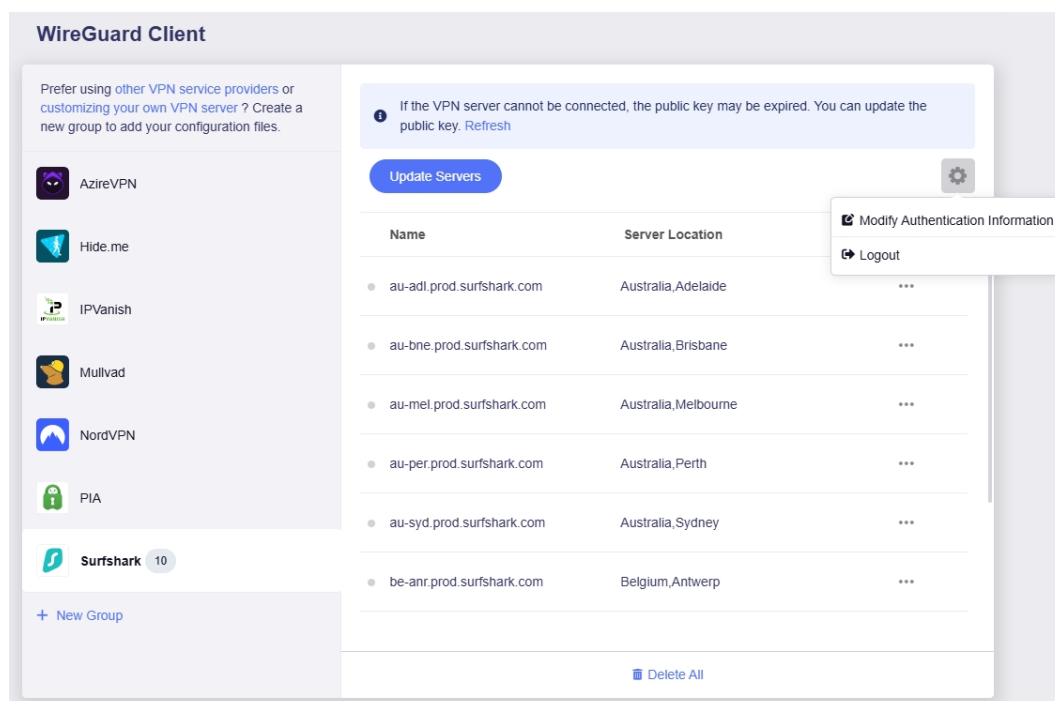
6. Update servers.

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



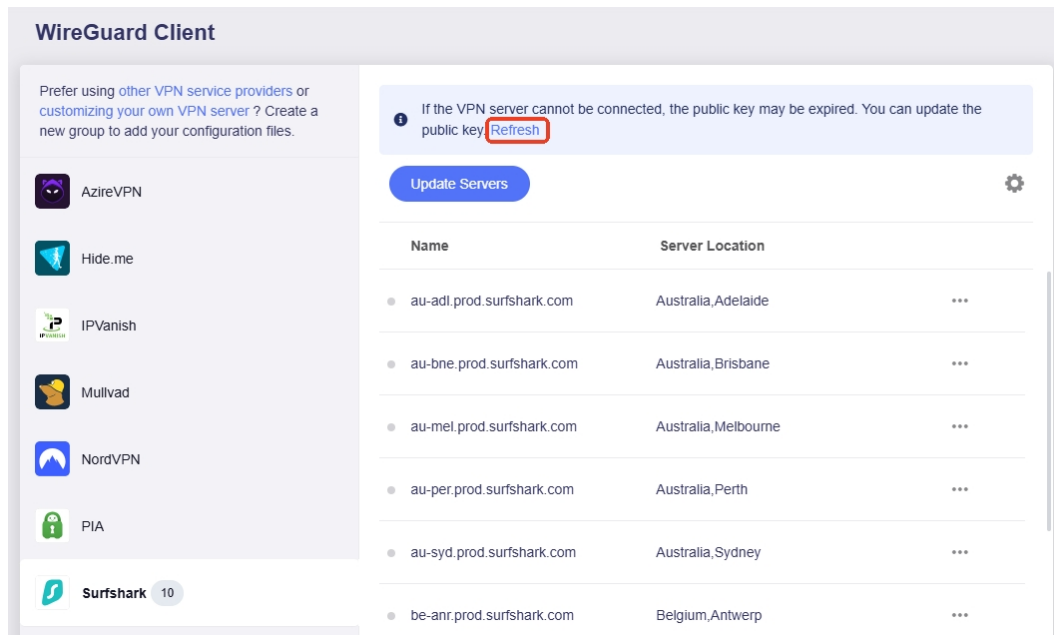
7. Edit credentials or logout.

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



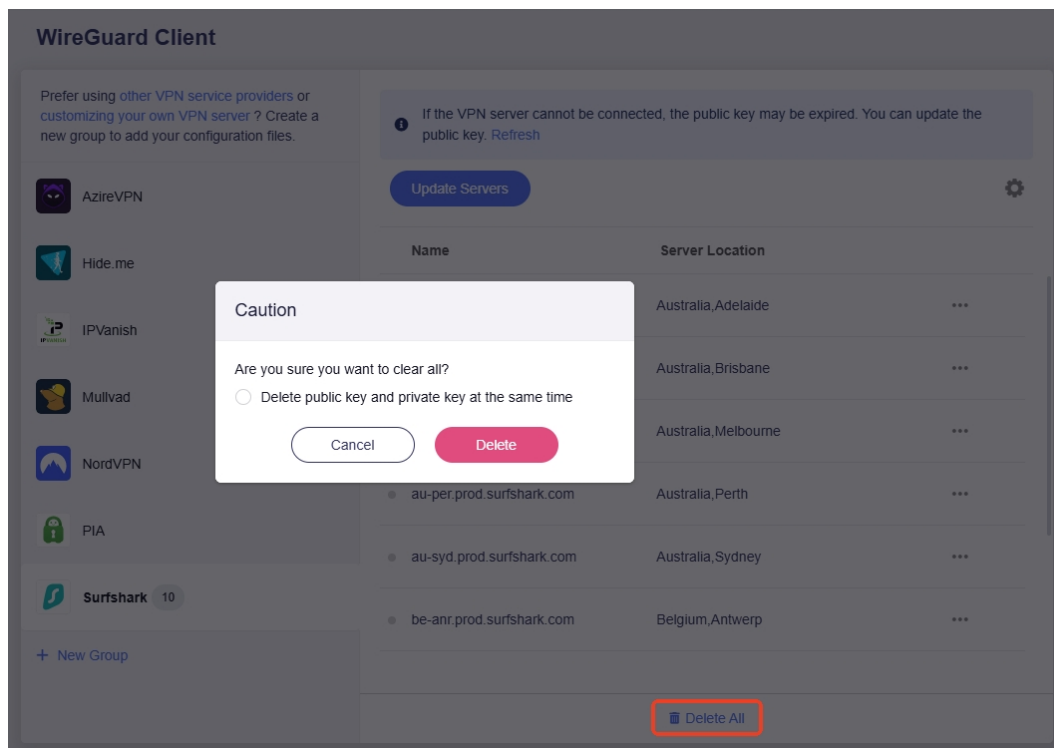
8. Refresh.

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.

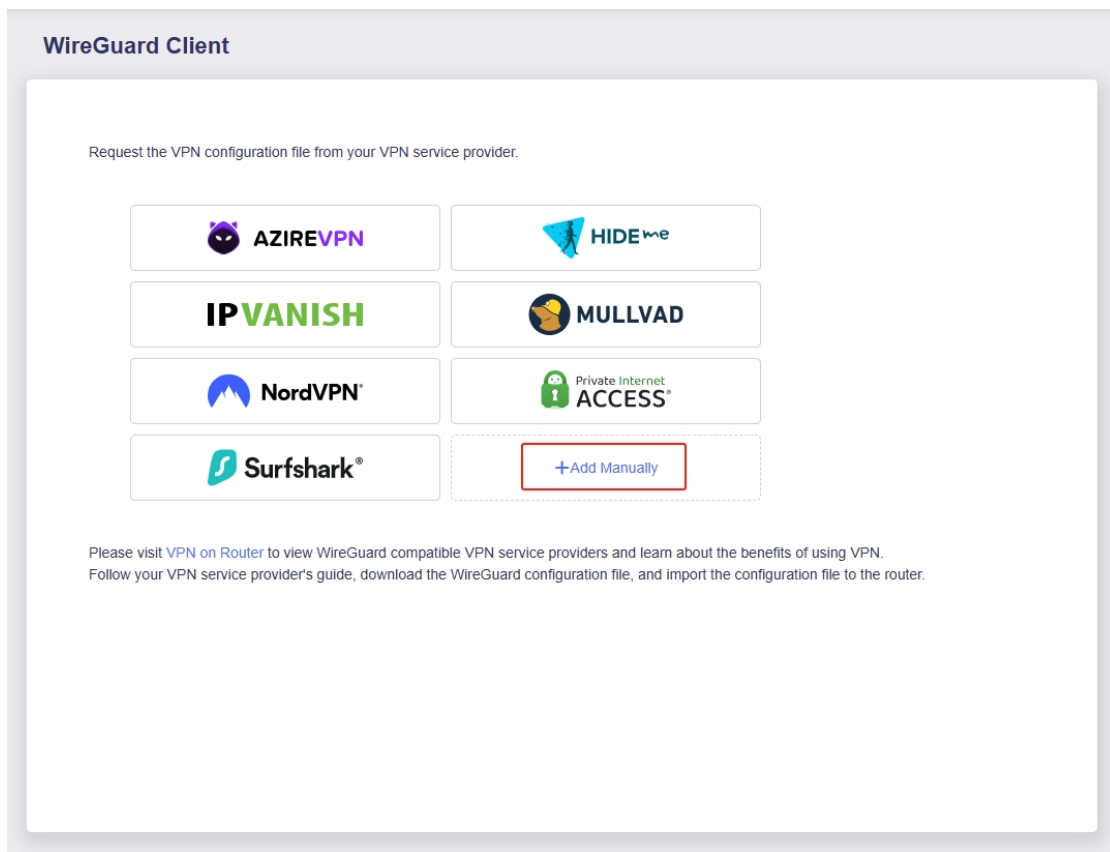


11.2.9 Set Up WireGuard Client Manually (for other providers)

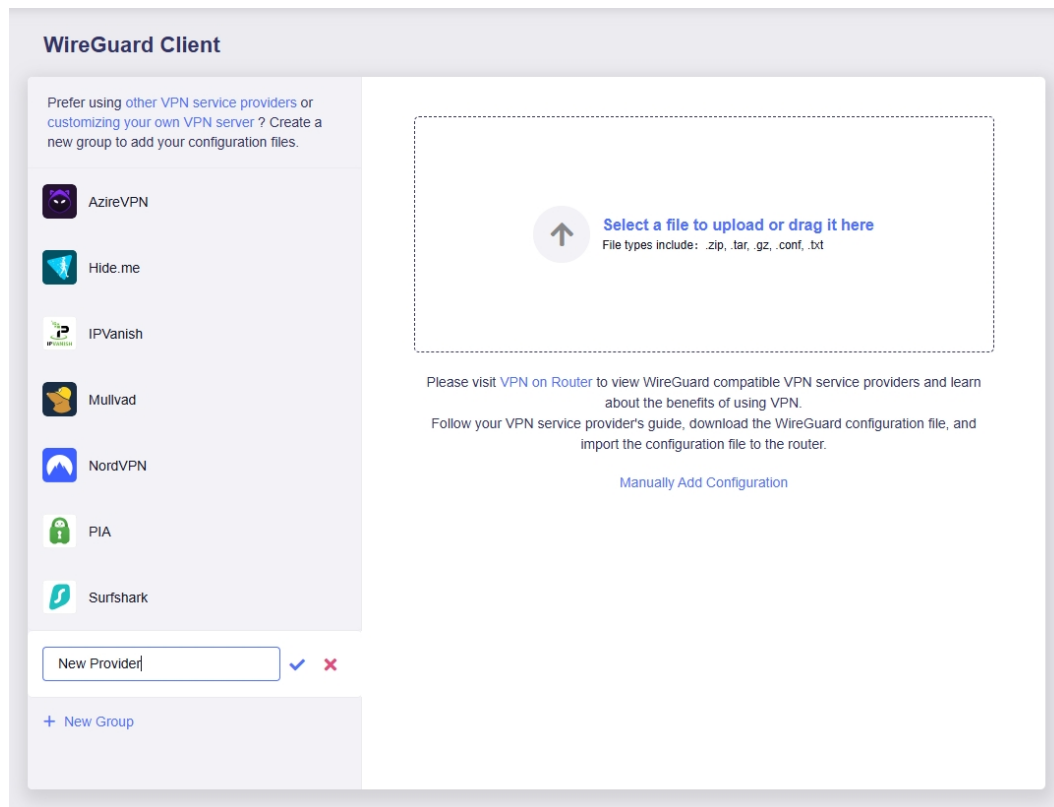
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see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

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

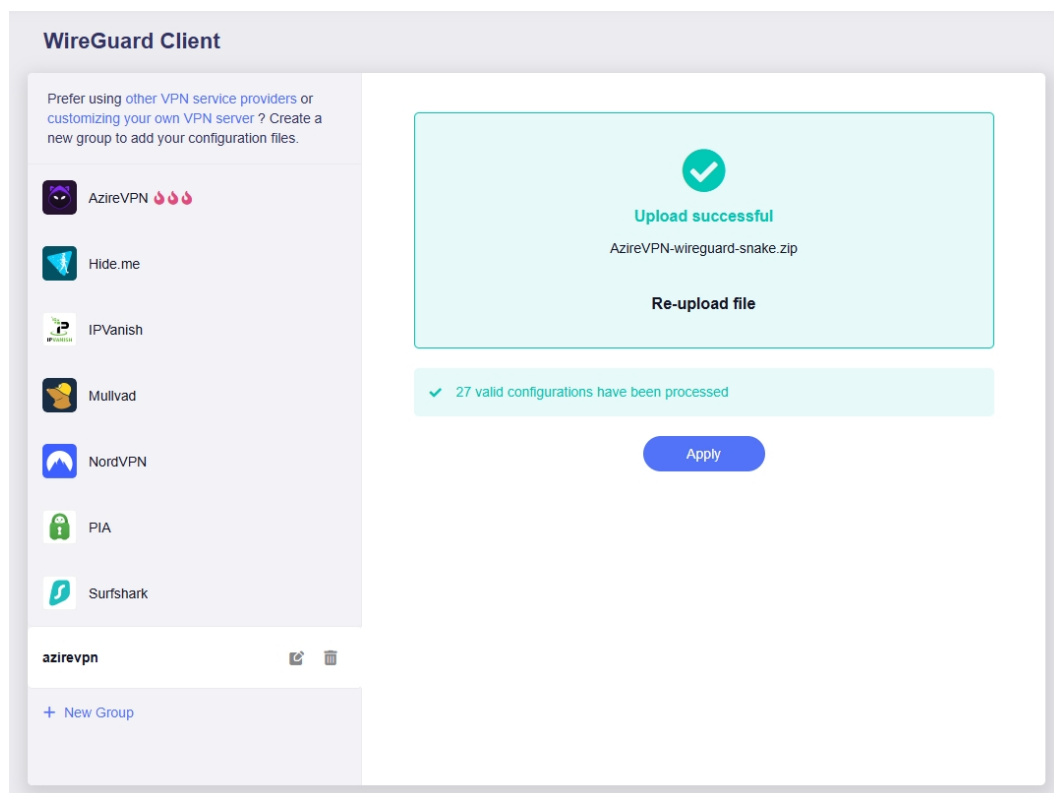
1. Log in to your router's web admin panel and navigate to **VPN > WireGuard Client > Add Manually**.



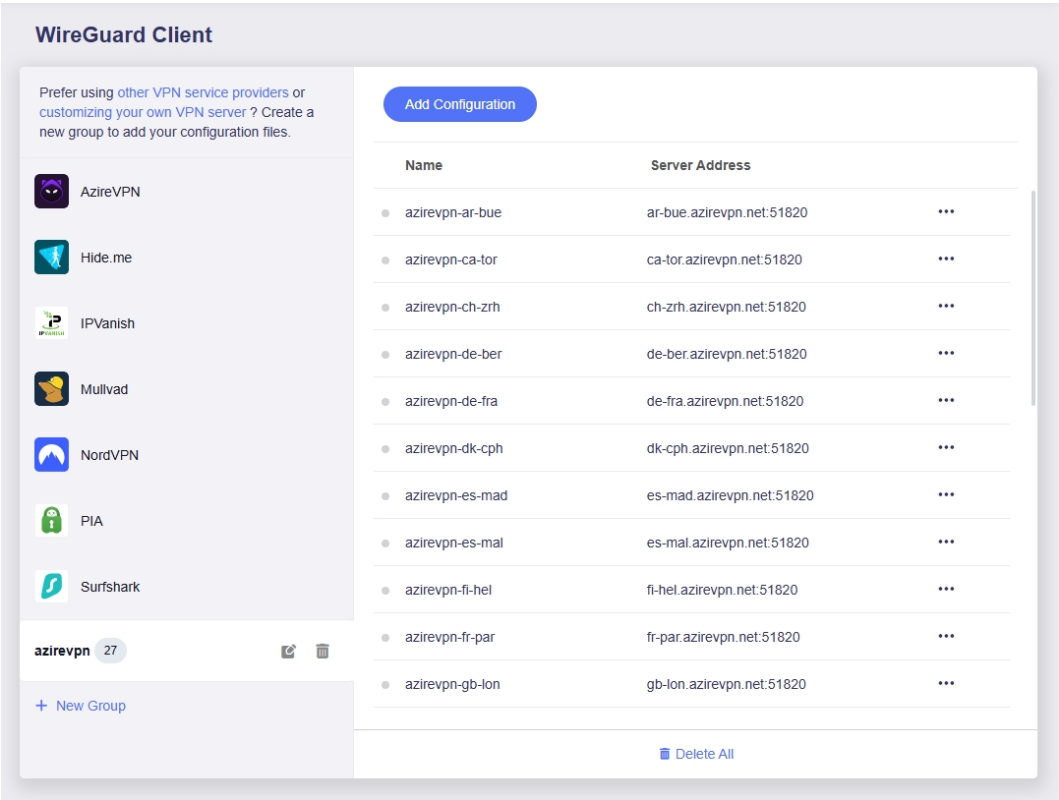
2. It will create a group on the left sidebar. Set a descriptive name for the group.



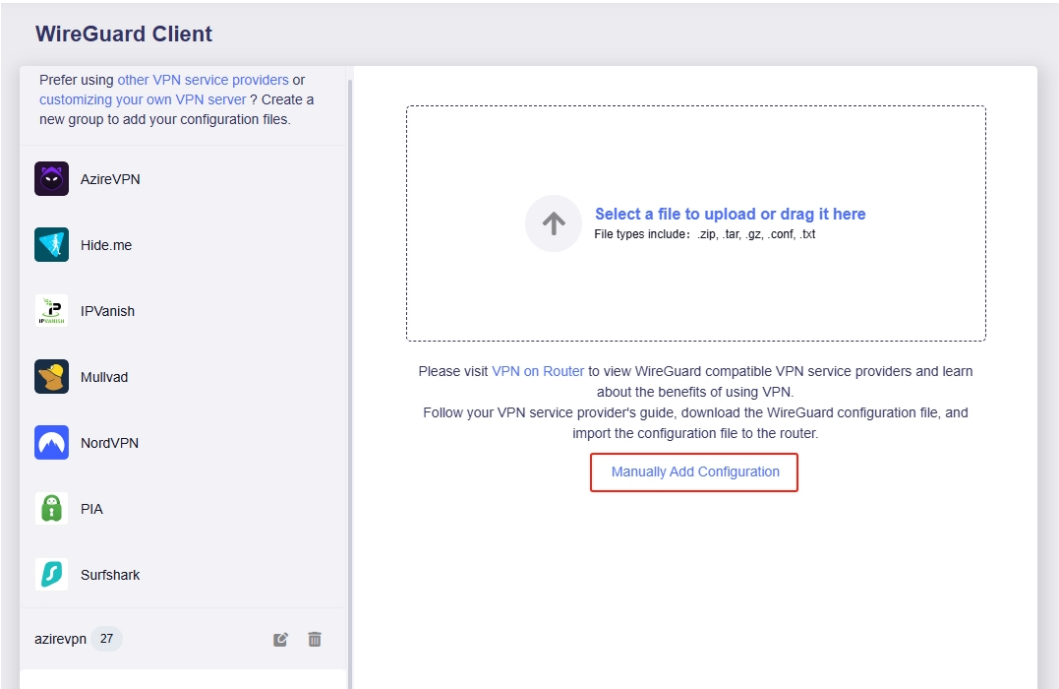
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.

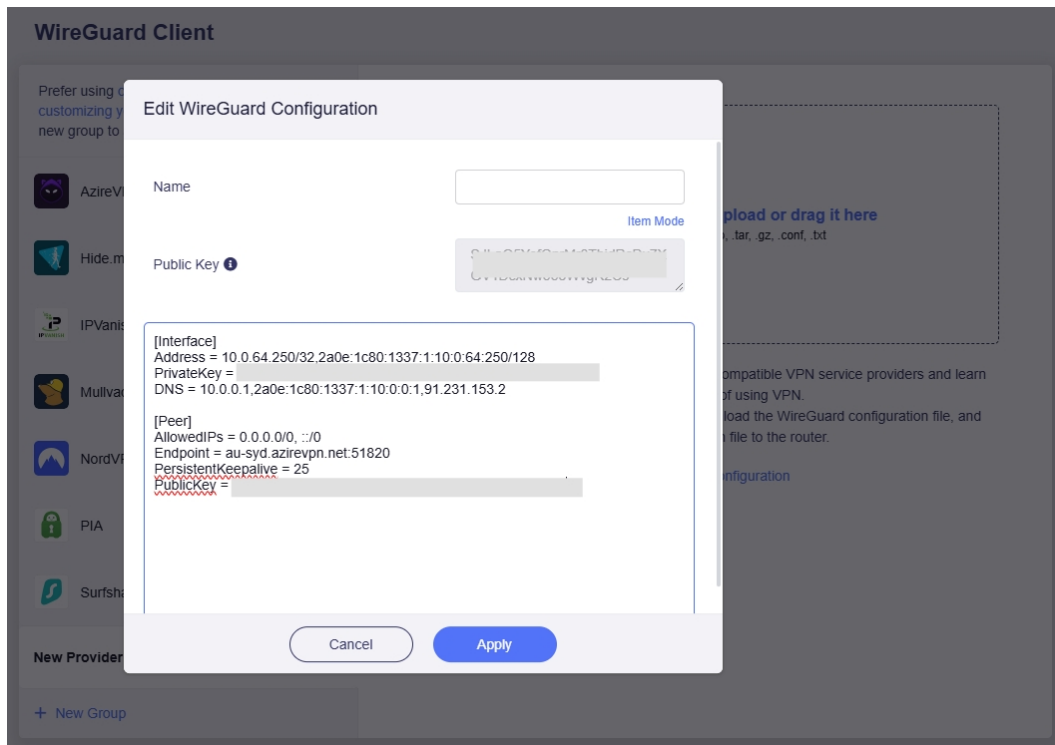


If you upload a compressed file containing multiple configuration files, it will be decompressed automatically, as shown below.

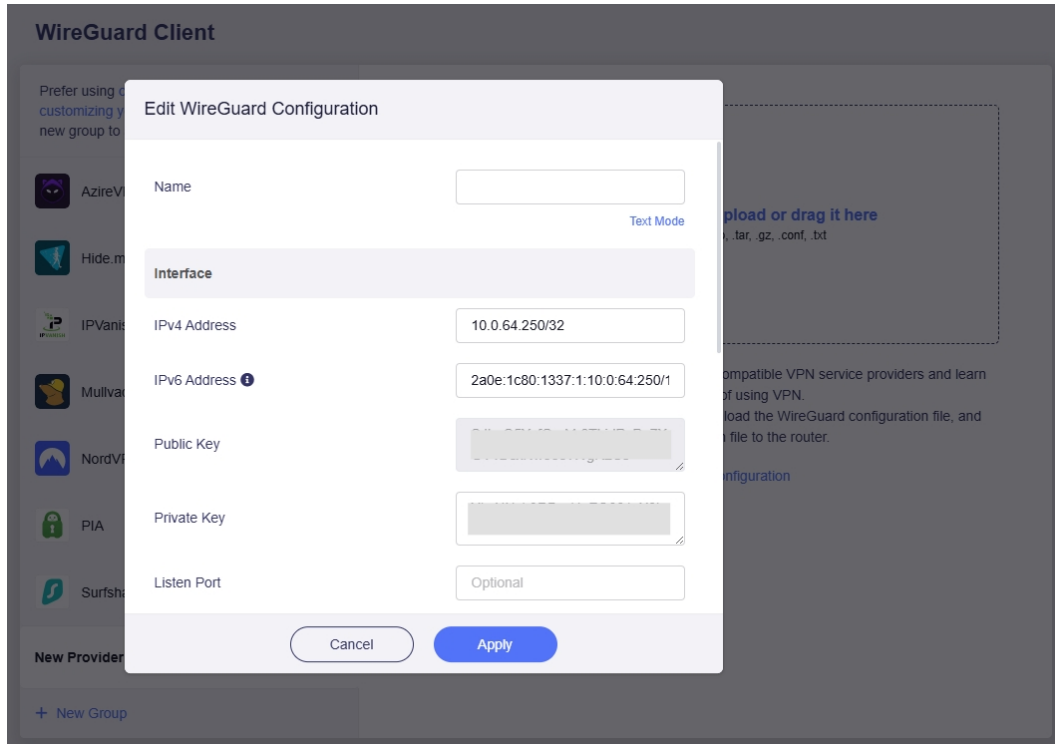


Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

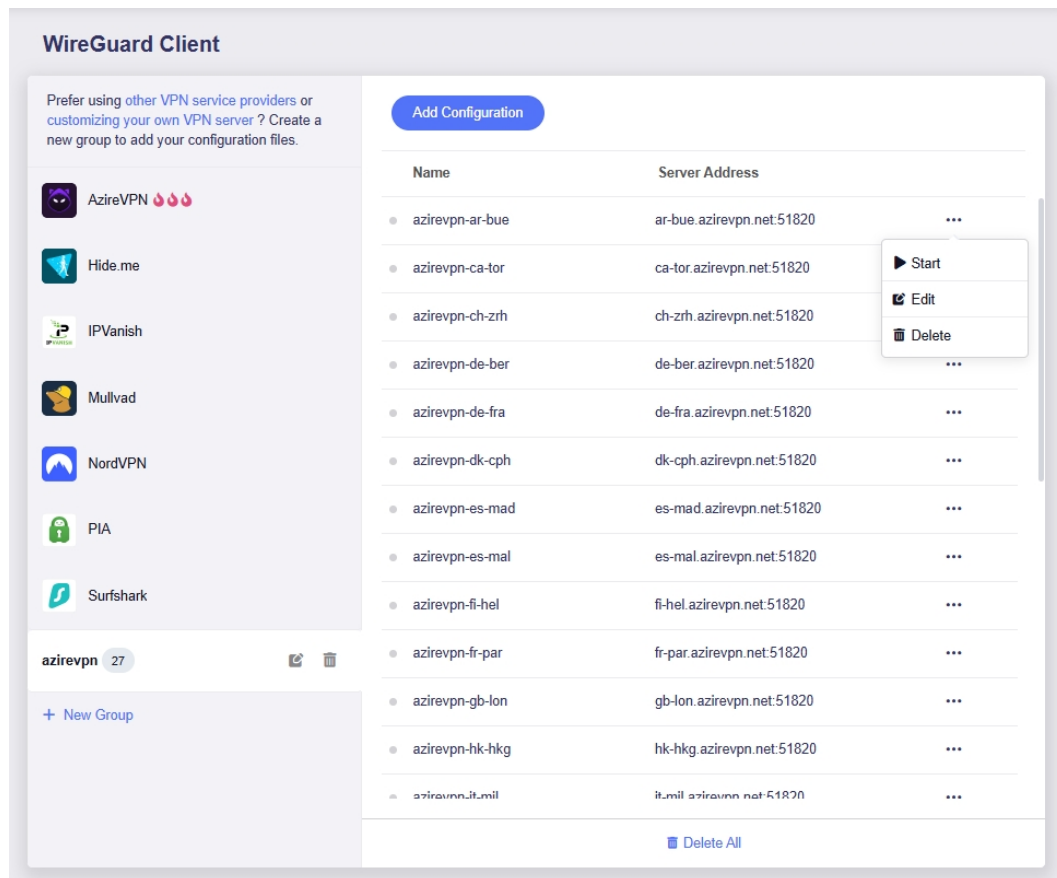




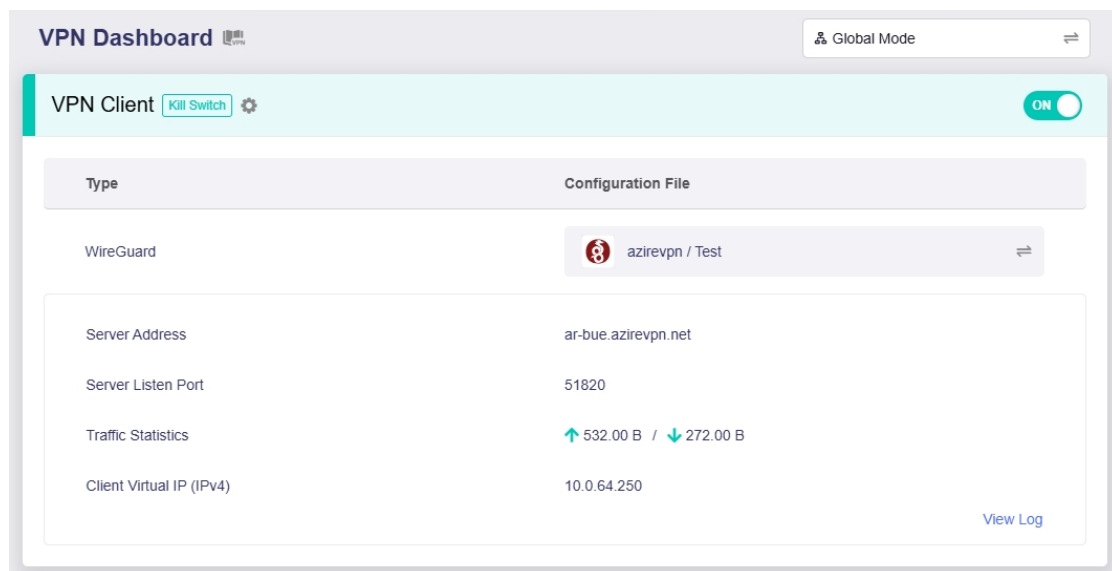
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



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

Tor

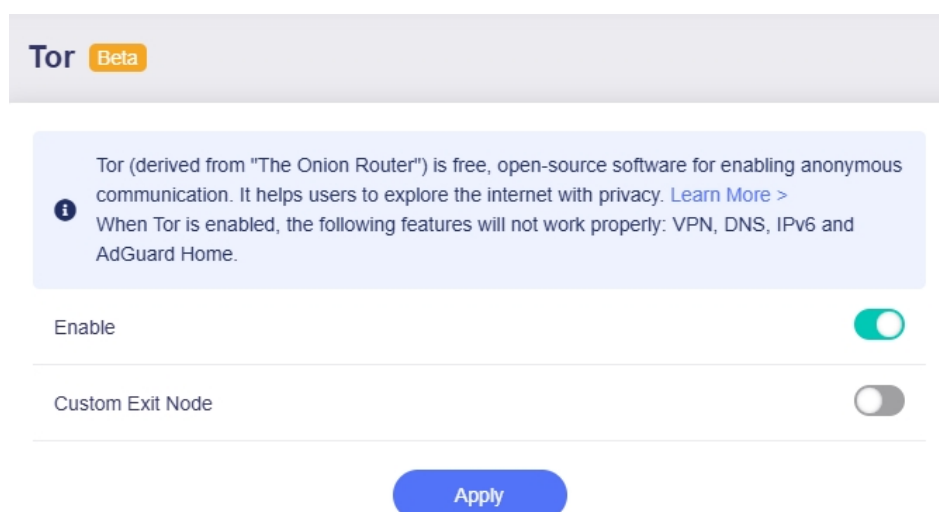
This chapter provides a brief introduction to Tor (The Onion Router), a free and open-source software for enabling anonymous communication.

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

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

Follow the steps below to set up Tor if needed.

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



Tor Beta

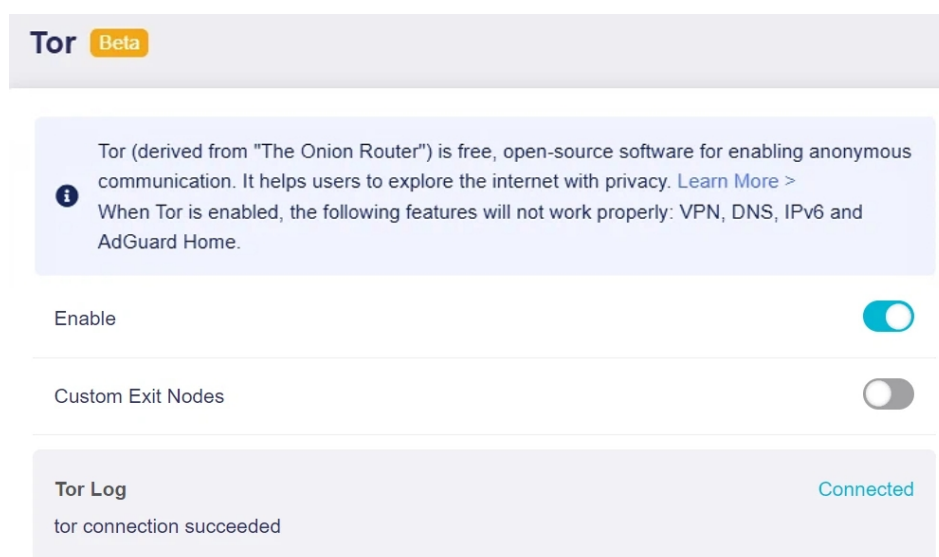
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.

Enable ☒

Custom Exit Node ☐

Apply

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



Tor Beta

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

Enable ☒

Custom Exit Nodes ☐

Tor Log Connected
tor connection succeeded

Chapter 13

Applications

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

13.1 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:

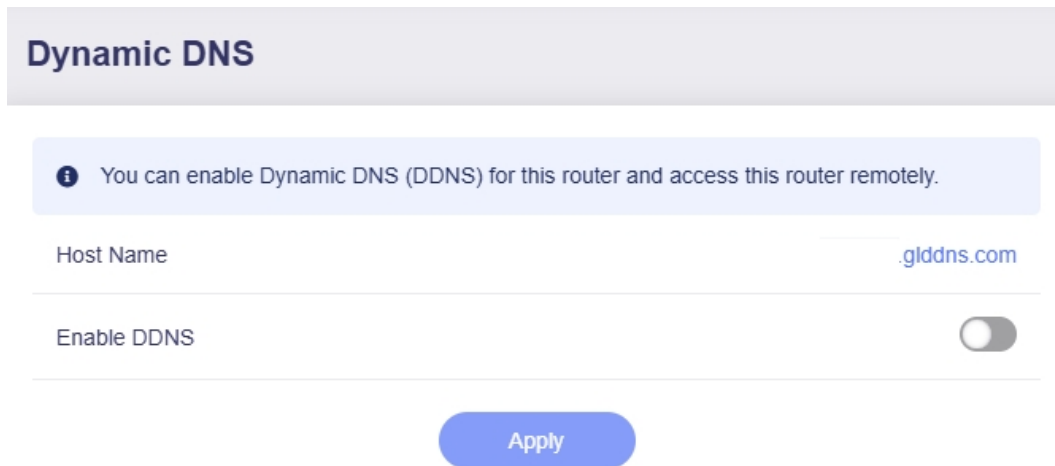
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

13.2 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.

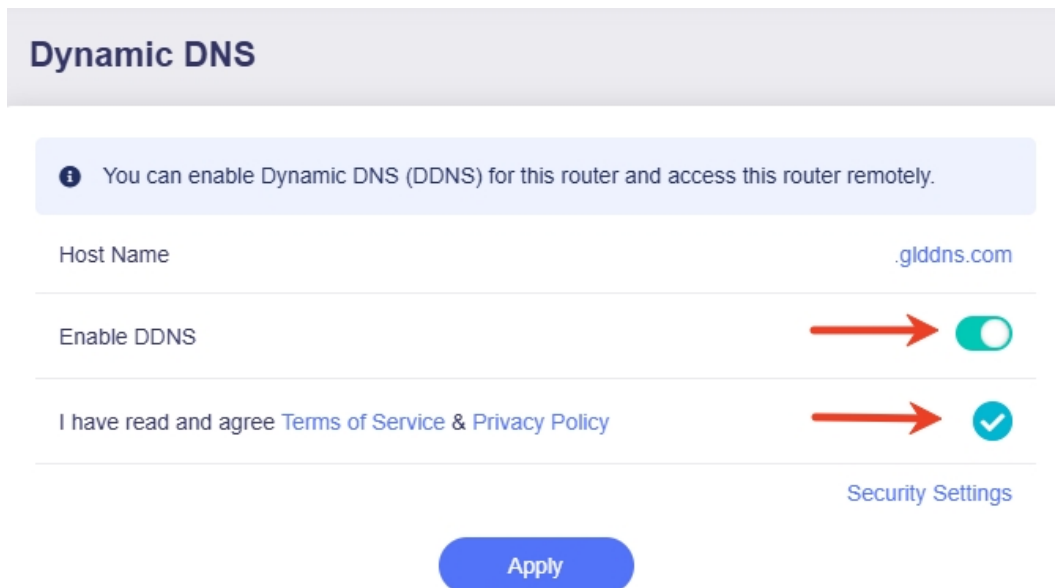
13.2.1 Enable DDNS

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



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

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



This screenshot shows the 'Dynamic DNS' configuration page after the first step. The 'Host Name' field still shows '.glddns.com'. The 'Enable DDNS' row now has a red arrow pointing to a toggle switch that is turned on (green). Below this, there is a row with the text 'I have read and agree' followed by a link 'Terms of Service & Privacy Policy'. A red arrow points to a green checkmark icon. At the bottom right, there is a link 'Security Settings'. At the bottom center, there is a blue 'Apply' button.

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

Dynamic DNS

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

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

Host Name [.gliddns.com](#)

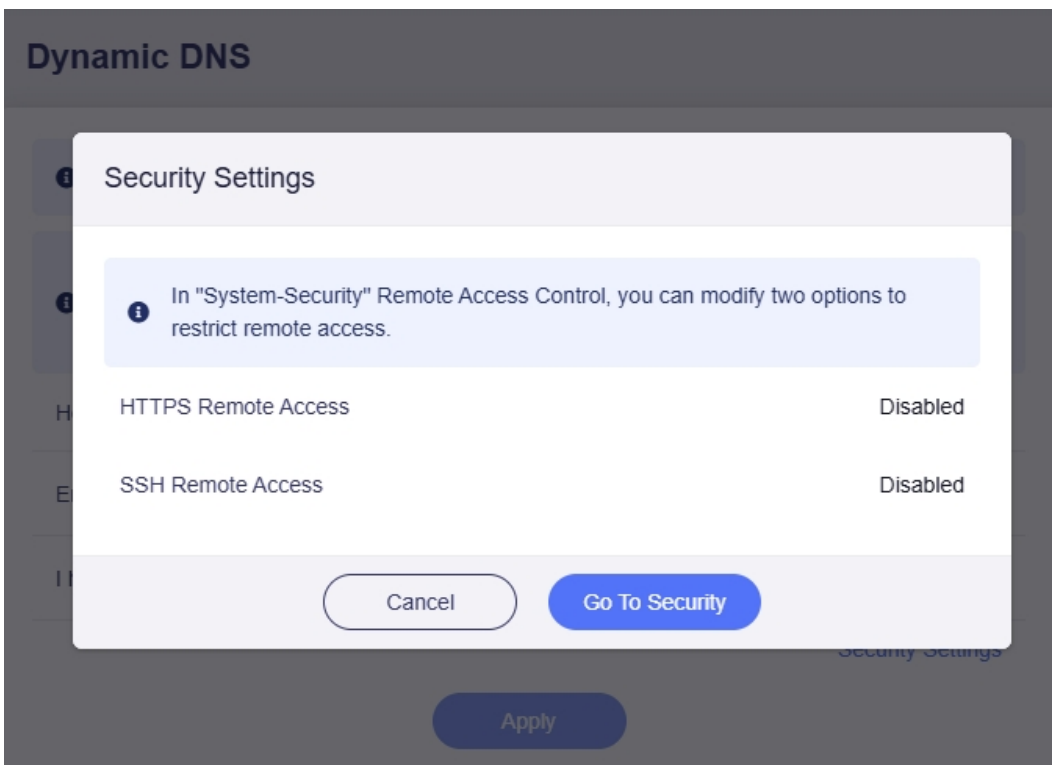
Enable DDNS ☒

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 **SYSTEM > Security > Remote Access Control** to enable it, then 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.

13.2.2 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

 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.
 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.

 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

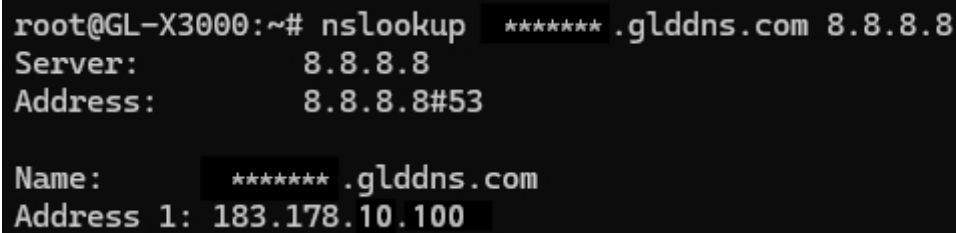
IPv4	205.185.113.19
------	----------------

WAN Interface IP address

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

Method 2. Use commands

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

A terminal window screenshot showing the execution of the nslookup command. The prompt is root@GL-X3000:~#. The command entered is nslookup *****.glddns.com 8.8.8.8. The output shows the server as 8.8.8.8, the address as 8.8.8.8#53, the name as *****.glddns.com, and the first address as 183.178.10.100.

```
root@GL-X3000:~# 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 currently 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.

13.2.3 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 **SYSTEM > Security > Remote Access Control**. Enable **HTTPS Remote Access**, and click **Apply**.

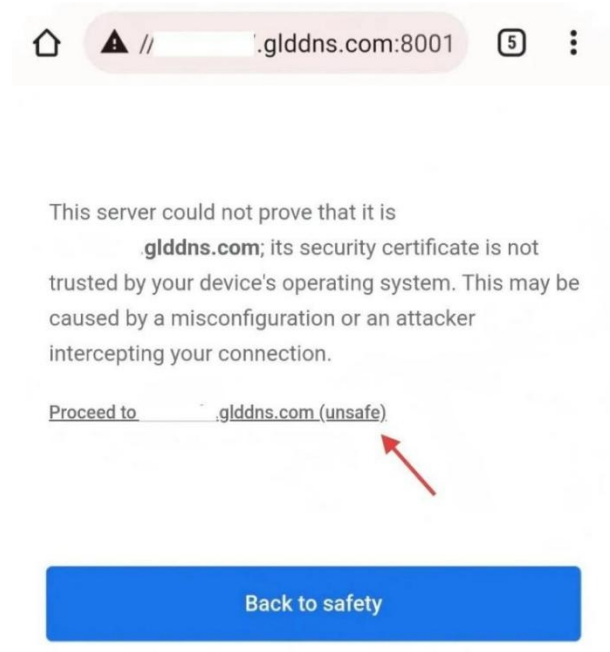
Remote Access Control

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

Apply

3. 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**.

13.2.4 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 [.gliddns.com](#)

Enable DDNS  ☒

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

[Security Settings](#)

Apply

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

13.3 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.

Beryl AX is equipped with a USB port, compatible with USB flash drives and portable external hard drives. You can configure Samba, WebDAV, or DLNA for these storage devices, which support common formats such as NTFS, FAT32, and EXT4.

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

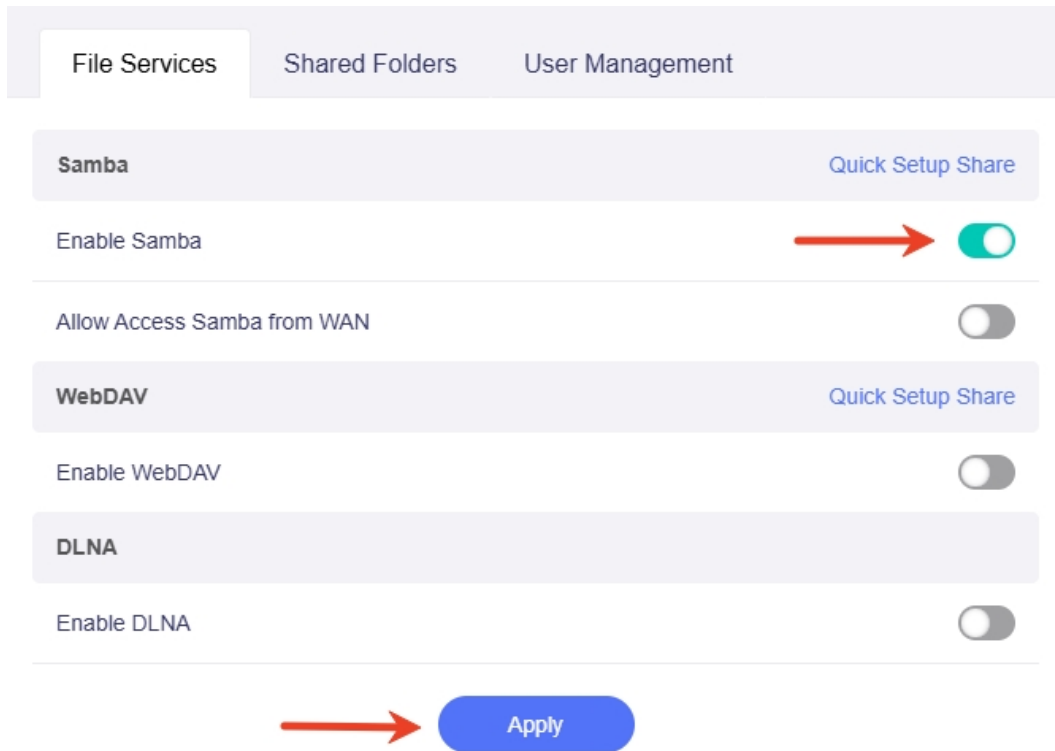
13.3.1 Connect Storage

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	

13.3.2 Set Up Samba

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

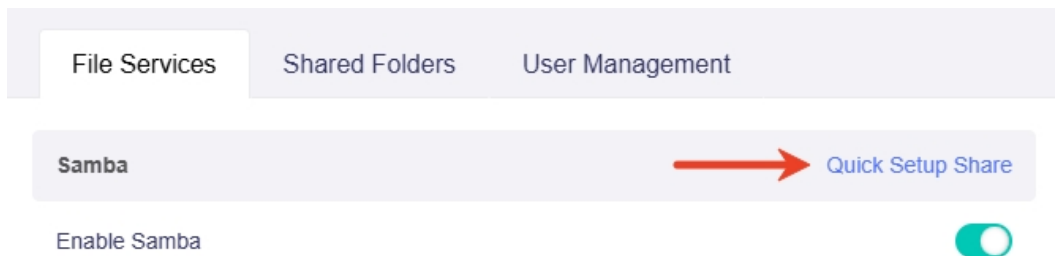


The screenshot shows the 'File Services' tab selected in a configuration interface. It contains three sections: Samba, WebDAV, and DLNA. Each section has a 'Quick Setup Share' link and an 'Enable' toggle switch. A red arrow points to the 'Enable Samba' toggle, which is currently turned on. Another red arrow points to the 'Apply' button at the bottom of the page.

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](#)

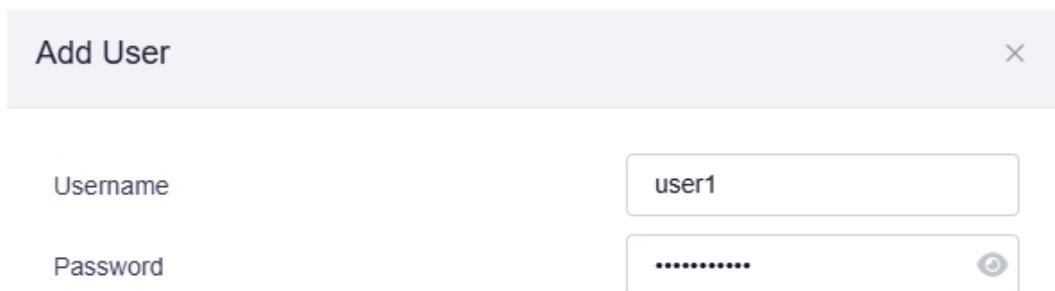
- **Allow Access Samba from WAN:** Enable it if you want upstream devices to access the Samba service.
2. Click **Quick Setup Share** to set the shared link.



This screenshot shows the 'File Services' tab with the 'Samba' section expanded. The 'Quick Setup Share' link is highlighted with a red arrow. The 'Enable Samba' toggle is now 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 'Add User' dialog box is shown with a close button (X) in the top right corner. It contains two input fields: 'Username' with the text 'user1' and 'Password' with masked characters (dots) and an eye icon to toggle visibility.

Add User		X
Username	user1	
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

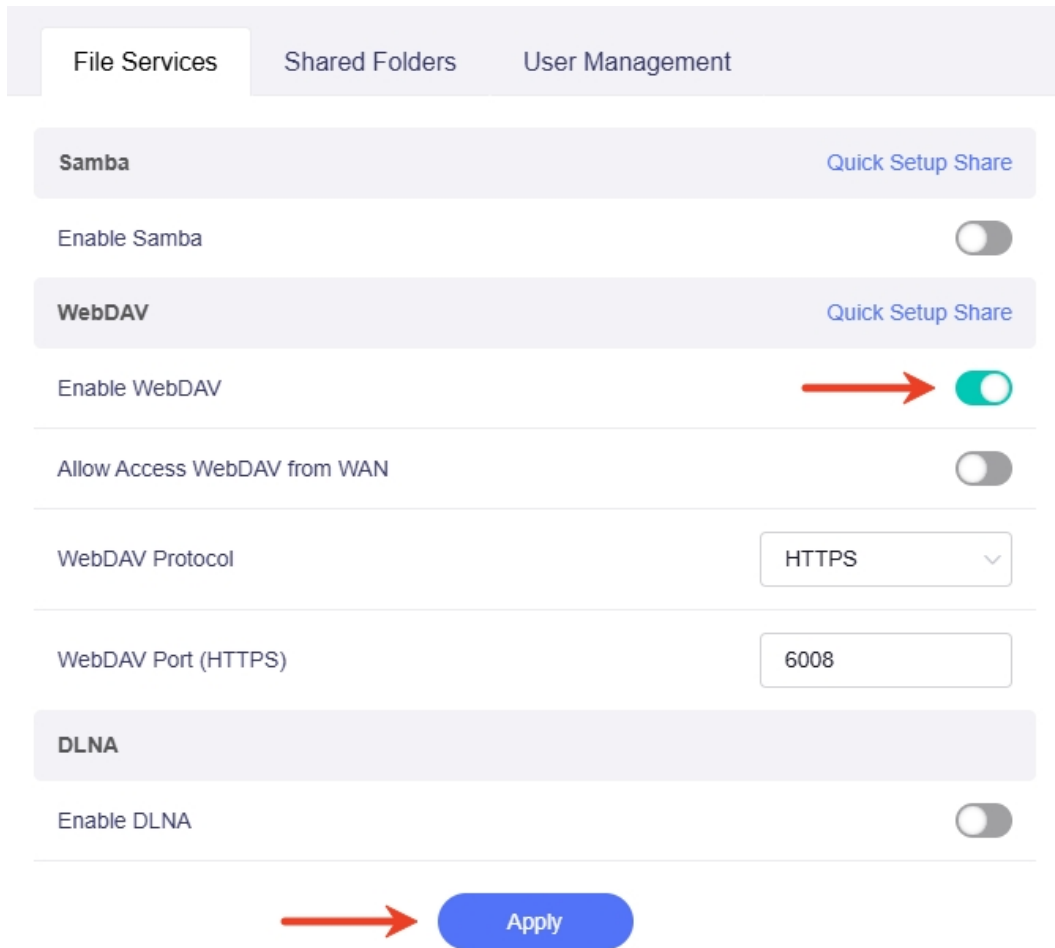
Unix-like Samba

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.

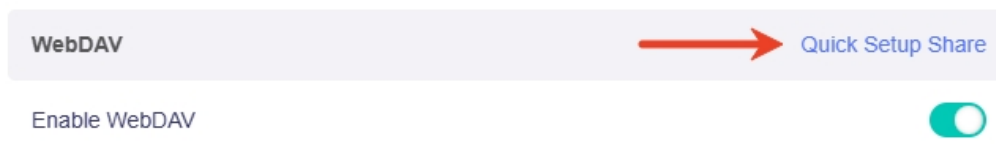
13.3.3 Set Up WebDAV

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



The screenshot shows the 'File Services' configuration page with three tabs: 'File Services', 'Shared Folders', and 'User Management'. The 'File Services' tab is active. It contains three sections: 'Samba', 'WebDAV', and 'DLNA'. The 'WebDAV' section is highlighted with a red arrow pointing to the 'Enable WebDAV' toggle switch, which is currently turned on. Below this, there is a toggle for 'Allow Access WebDAV from WAN' (turned off), a dropdown for 'WebDAV Protocol' (set to 'HTTPS'), and a text input for 'WebDAV Port (HTTPS)' (set to '6008'). At the bottom of the page, a red arrow points to a blue 'Apply' button.

- **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' section of the configuration page. A red arrow points to the 'Quick Setup Share' link. Below it, the 'Enable WebDAV' toggle switch is shown in the 'on' position.

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

Add User

Username

user1

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 ×

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 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.

13.3.4 Set Up DLNA

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

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

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

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

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

13.4 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

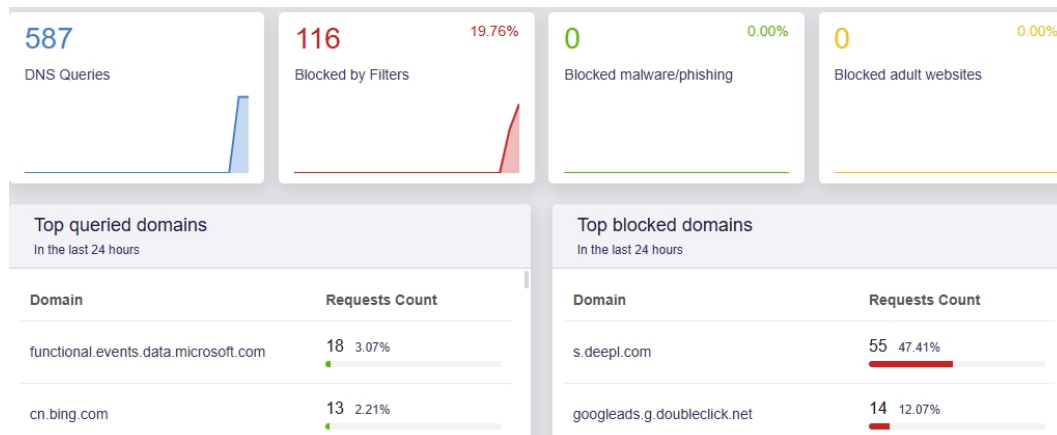
AdGuard Home is network-wide software that blocks ads and tracking. Once set up, it will cover ALL the devices on your home network, there is no need for any additional client-side software. This page gets statistics through the API provided by AdGuard Home. When AdGuard Home is enabled, the router will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



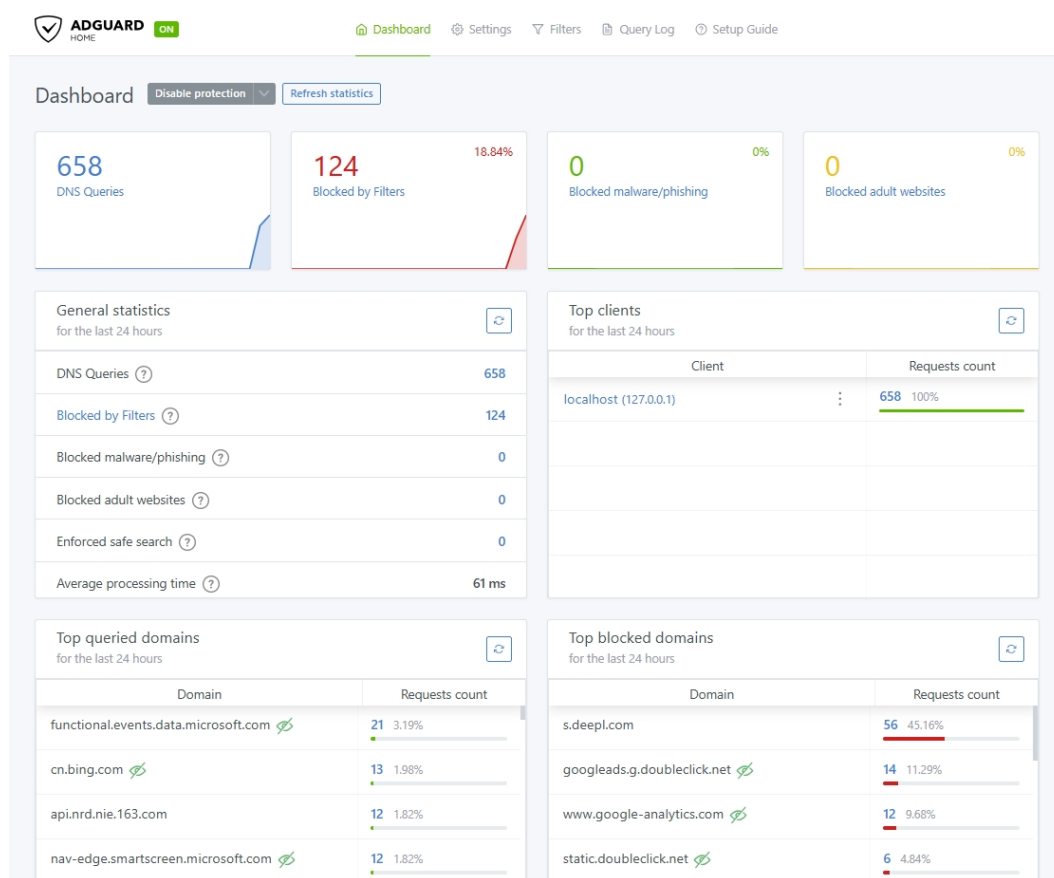
3. Click **Settings Page** to configure advanced settings for AdGuard Home.

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.



13.5 Parental Control

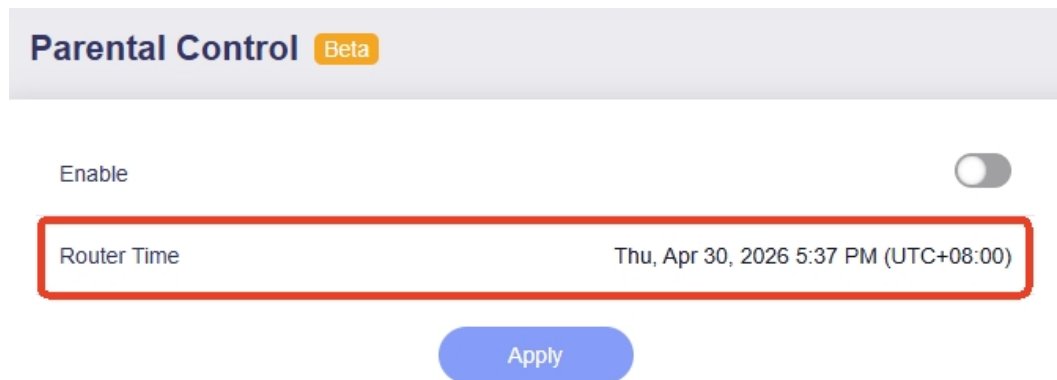
Parental control is a way to keep children safe online by blocking inappropriate websites and limiting how long they use devices. It helps prevent access to harmful content, manage screen time, and ensure children use the internet responsibly.

13.5.1 Quick Setup

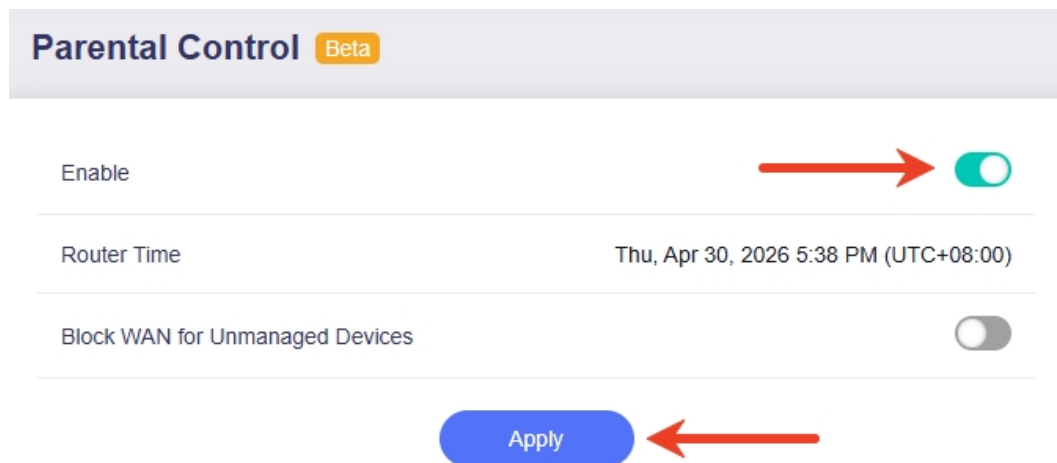
Follow these steps to set up Parental Control on GL.iNet routers.

1. Log in to the router's web admin panel and go to **APPLICATIONS > Parental Control**.

Ensure the router time is accurate. If not, go to **SYSTEM > Time Zone** to synchronize it first.



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



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

Here is a use case for your reference.

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

Setup Steps:

1. Create a profile and customize a name.

1. Create a profile for your child or family

First, select the client devices used by your children or your family, depending upon whether you want to control network access to all devices for your entire family or whether you want to control access for each child separately. After that, you can

1. block access to the Internet from all devices of your choice;
2. limit access to specific applications or sites to all devices of your choice.

You can name these devices, giving them a name that is easy to remember. If created for a specific child, you could use the child's name or nickname.

Rule Name

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

2. Select the devices to be managed



You should first connect these devices to the router as clients. Otherwise you will need to enter the individual MAC addresses manually.

[+ Manually Add Device](#)

glkvm 94:83:C4:A9:97:DC	GL-INET-08 6C:1F:F7:5D:F1:5D self
Child-phone 94:83:C4:B7:20:01	

3. Set access limit.

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

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

3. Set access limits for these devices



Next, you can set how to limit access to the Internet for these devices.

1. you can prevent these devices from connecting to the Internet and then pause the restriction at a specific time;
2. you can also block access from these devices to specific applications or Internet sites to prevent your child from accessing or viewing content that you consider is not suitable for them.

You can create a new ruleset to block applications or sites that you do not want to be accessed.

Default Ruleset

Block Internet Access

+ Add a New Ruleset

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

Add a New Ruleset

Ruleset Name

Learning

Color

#B15EF8

Blocklist Input Mode ⓘ

Manual

```
1  fortnite.com
2  pornhub.com
3  tiktok.com|
```

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

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

Add a New Ruleset

Ruleset Name

Play

Color

#F5946D

Blocklist Input Mode ⓘ

Manual

1 pornhub.com

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

3. Set access limits for these devices

Next, you can set how to limit access to the Internet for these devices.

1. you can prevent these devices from connecting to the Internet and then pause the restriction at a specific time;
2. you can also block access from these devices to specific applications or Internet sites to prevent your child from accessing or viewing content that you consider is not suitable for them.

You can create a new ruleset to block applications or sites that you do not want to be accessed.

Default Ruleset

Block Internet Access

Block Internet Access

No Limit

Learning

Play

Back

Finish

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

4. Go to set schedules

You have successfully created a profile!

If you need to specify a more detailed schedule for your child or your family, to include times for study, times for playing games or when it is time for bed; you can make additional schedule settings.



Later

Go to Set

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

Add Schedule



You can set up special time slots during which the device will be subject to additional restrictions. For example, you can define playtimes where you allow your child to play; free time slots at weekends or times when your child needs to take a break.

Schedule Ruleset

Learning

Execution Time

08:00

to

11:00

Execution Day(s)

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Cancel

Apply

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

Parental Control / **Modify Profile** Beta

i Each client device can only be assigned to one profile. If you add a client device to another profile, it will be removed from the original one.

Rule Name

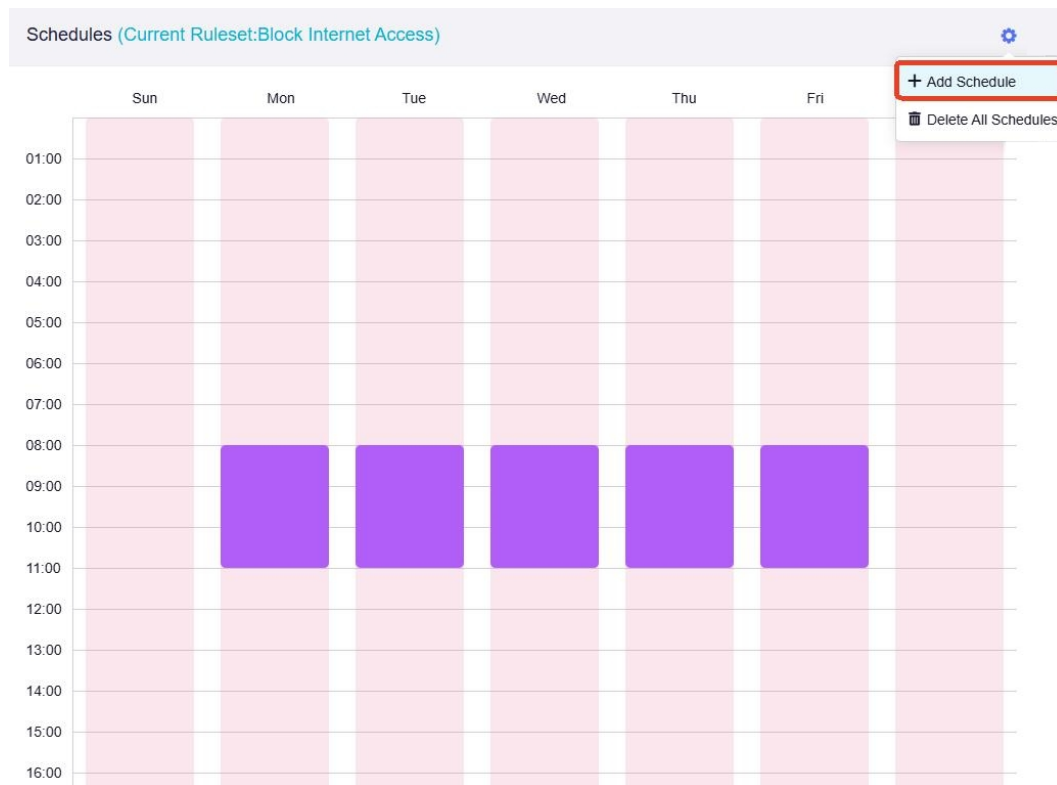
Default Ruleset **i** ● Block Internet Acce ▼

Devices + Manage Device

Child-phone

Apply

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



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

Add Schedule



You can set up special time slots during which the device will be subject to additional restrictions. For example, you can define playtimes where you allow your child to play; free time slots at weekends or times when your child needs to take a break.

Schedule Ruleset

● Play

Execution Time

🕒 18:00

to

🕒 20:00

Execution Day(s)

Sun



Mon

Tue

Wed

Thu

Fri

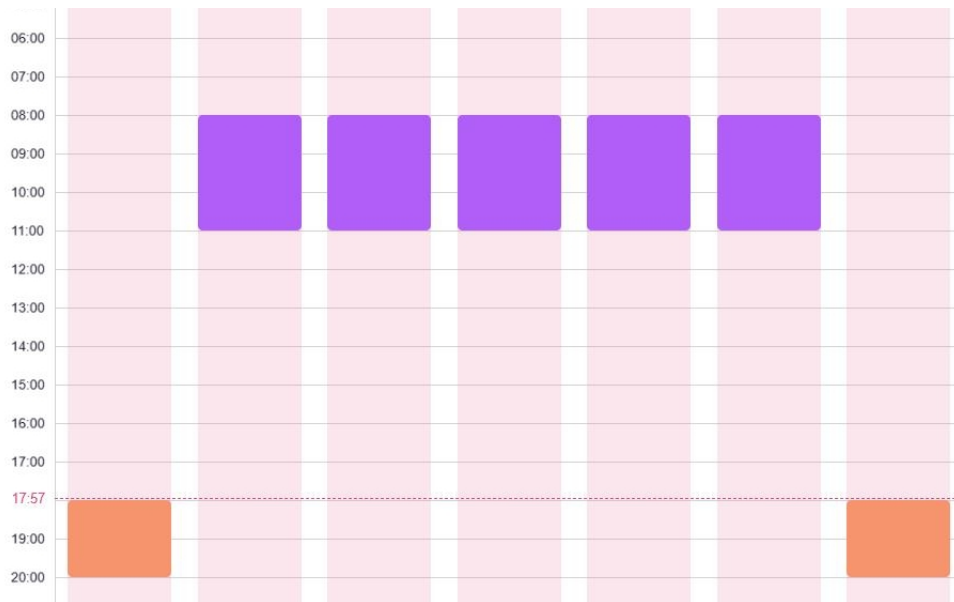
Sat



Cancel

Apply

The Play ruleset will then be added into the schedule.



Tips:

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

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

Parental Control / **Modify Profile** Beta



Each client device can only be assigned to one profile. If you add a client device to another profile, it will be removed from the original one.

Rule Name

Home

Default Ruleset ?

Block Internet Acce



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

Profiles



You can create a profile for each of your children and add the client devices that they use. Then you can set different schedules within each profile based on the learning times, bedtimes etc. that you have set for them. These schedules will control which websites and applications the devices in the device group can access at the times you have specified.

Add

Home (1)



Name



Child-phone

Block Internet Access



Switch to Learning after 13 Hours 58 Minutes

ruleset



You can define rulesets for specific time periods, to limit which websites and apps your child is allowed access to. For example, "learning time" does not allow access to specific video websites or apps. You can assign the ruleset that is to be used at which time period in the schedule of each profile.

Add

Ruleset Name	Description	Action
Block Internet Access	Drop all Internet connections	system
No Limit	Accept all Internet connections	system
Learning	Block access to 3 sites	...
Play	Block access to 1 sites	...

13.5.2 Troubleshooting

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

1. DNS cache issue.

Browsers and operating systems maintain DNS caches, which may delay the application of configuration changes. Clear the DNS cache to apply changes immediately.

2. The profile schedule has not yet started.
3. The entered domain name may be incorrect.

While a website's public domain is easy to find, the API domains used by apps are often not publicly available. To locate the correct domain, use a packet capture tool such as Wireshark or look up the relevant domain information.

For example, when blocking "www.google.com", entering "google.com" delivers better results than "www.google.com".

4. The target device uses a randomized MAC address for each network connection, which prevents access rules from taking effect. Disable random MAC address on the target device, then re-add the device to your profile.

13.6 ZeroTier

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

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

Note:

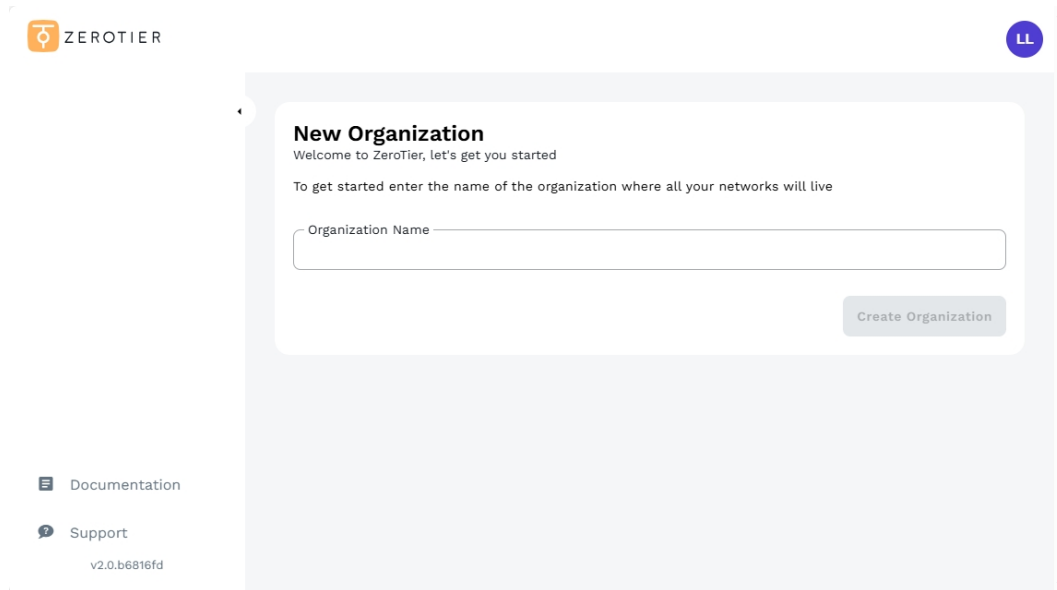
1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale, and AstroWarp.
2. This feature is currently in beta, and may have some bugs.

13.6.1 Set Up ZeroTier

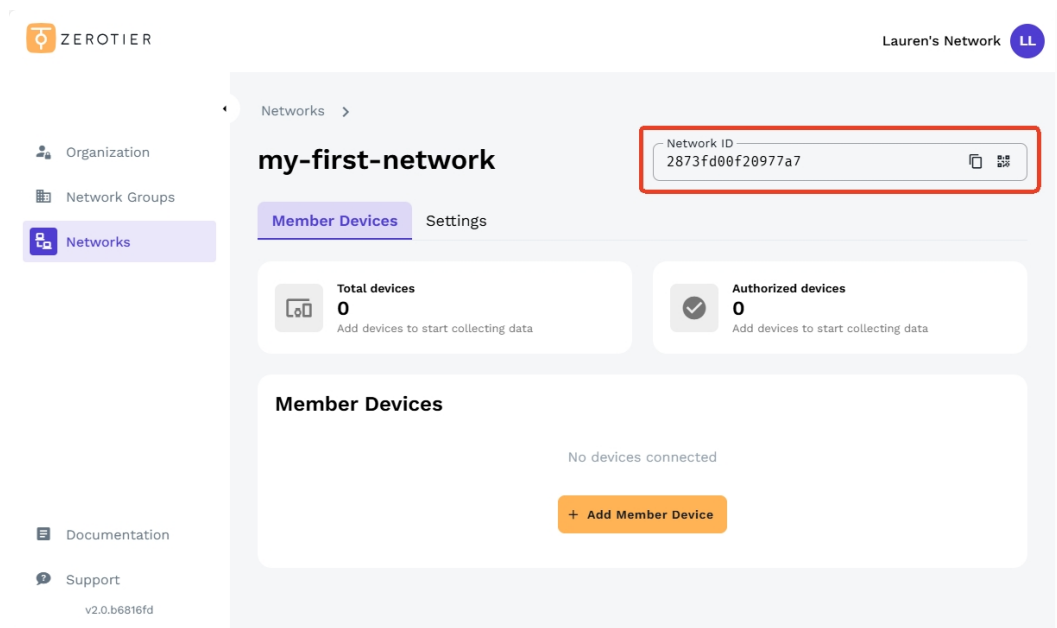
Two versions of ZeroTier Central are available: New Central and Legacy Central.

The following steps use New Central as an example.

1. Visit [ZeroTier official website](#) and sign in with your account.
2. Create an organization.

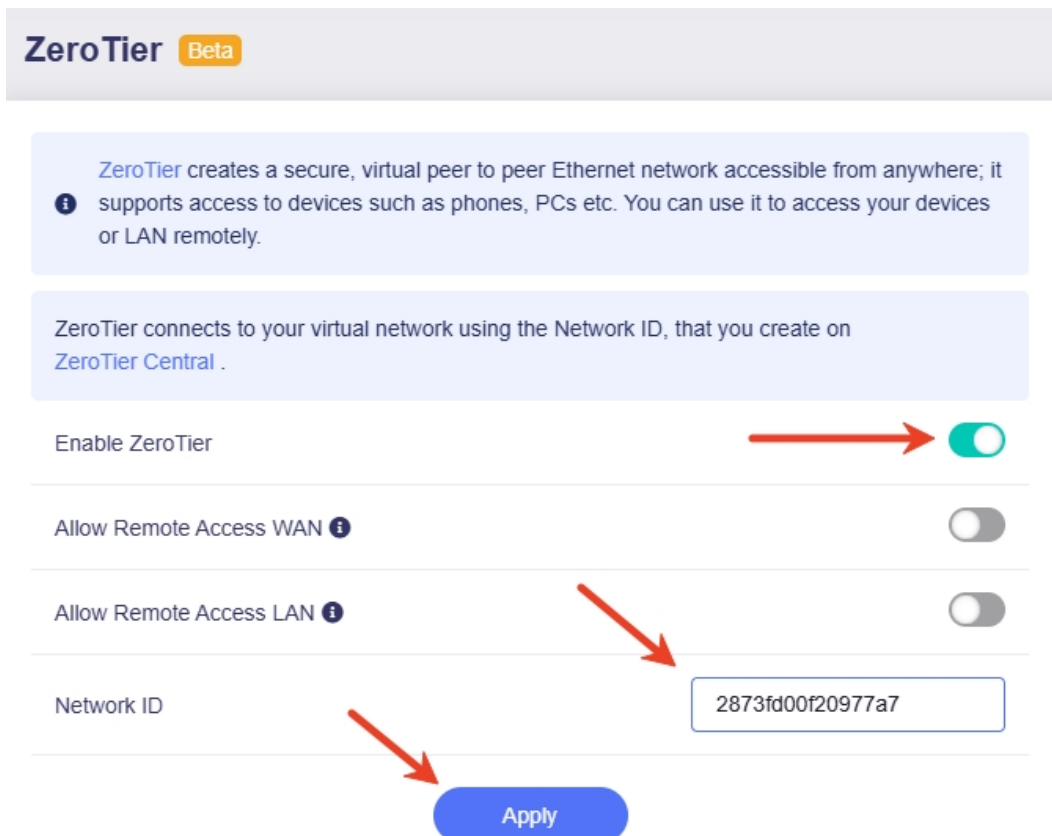


3. Select a plan. Here we choose **Personal plan** as an example, which includes 10 devices, 1 network admin, and 1 network. If you need to create more networks, add more devices, or add custom routes and DNS, choose other paid plan.
4. Now your ZeroTier network has been created.

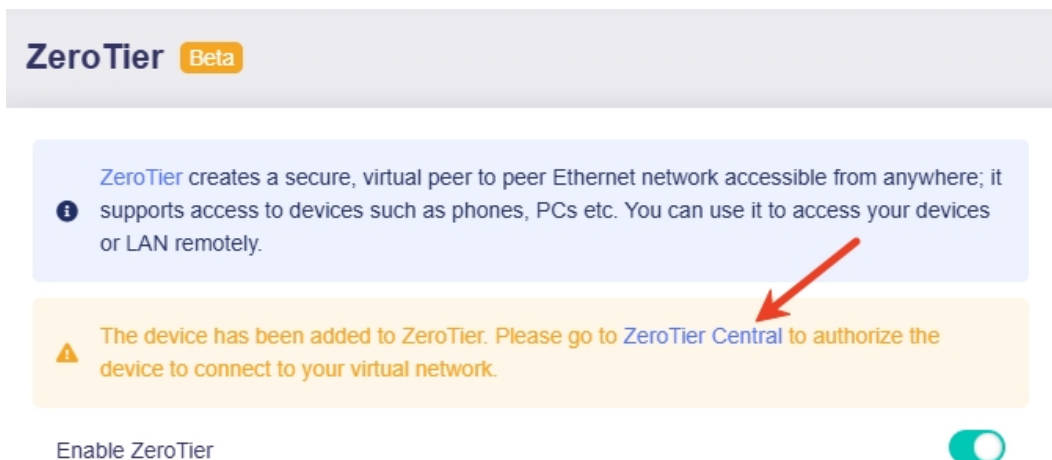


Take note of the **Network ID**, which is a 16-character alphanumeric combination in the upper right corner, as it will be required when connecting other devices later.

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



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



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

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 background. It contains a message: "A device is waiting for approval. Authorize or Reject here or in the table below (actions)". To the right of this message are two buttons: "✓ Authorize" and "✗ Reject". A red arrow points to the "✓ Authorize" button. Below this section, there are two summary cards: "Total devices 1" and "Authorized devices 0". The "Member Devices" table below shows one device with ID "eb618be42d", status "Not Authorized", and other details. The "Status" cell for this device is highlighted with a red box.

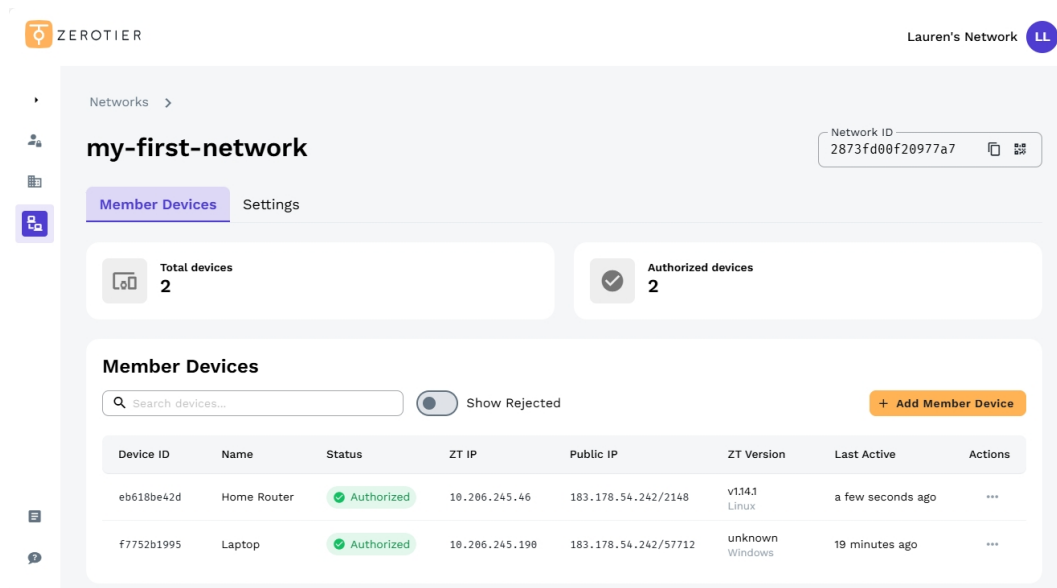
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Not Authorized		183.178.54.242/30149	unknown Linux	a few seconds ago	...

Once authorized, the page displays as follows.

The screenshot shows the ZeroTier web interface after the device has been authorized. The "Device Pending Authorization" section is no longer present. The "Total devices" card now shows "1", and the "Authorized devices" card now shows "1". The "Member Devices" table now shows the device "eb618be42d" with a status of "Authorized" (indicated by a green checkmark icon). The "Status" cell for this device is highlighted with a green box.

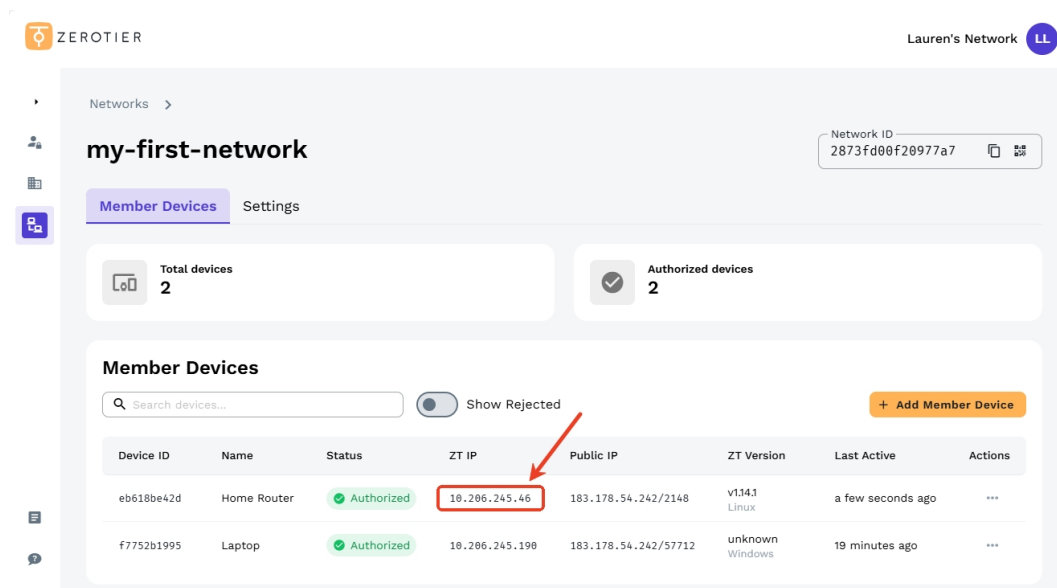
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Authorized	10.206.245.46	183.178.54.242/24364	v1.14.1 Linux	a few seconds ago	...

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.

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



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

9. Test connectivity.

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

13.6.2 Allow Remote Access WAN

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



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

13.6.3 Allow Remote Access LAN

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

ZeroTier Beta

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

The device is connected to your ZeroTier virtual network.

Enable ZeroTier

☒

Allow Remote Access WAN ⓘ

☐

Allow Remote Access LAN ⓘ

☒

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

13.7 Tailscale

[Tailscale](#) is a VPN service that makes your personal devices and applications accessible worldwide, securely and effortlessly.

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

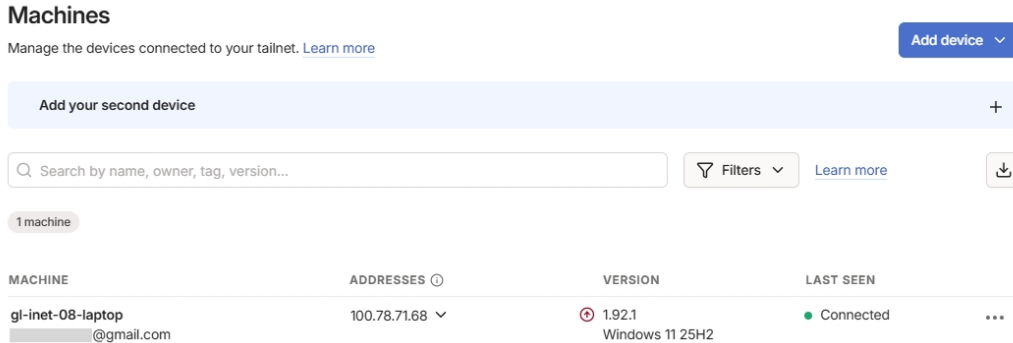
Note:

1. Since Tailscale is based on WireGuard, it is not recommended to use Tailscale with any of the following features or services simultaneously, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier, AstroWarp.
2. This feature is currently in beta, and may have some bugs.
3. GL.iNet routers are not yet available as exit nodes. This feature will be available in firmware v4.9 and later.

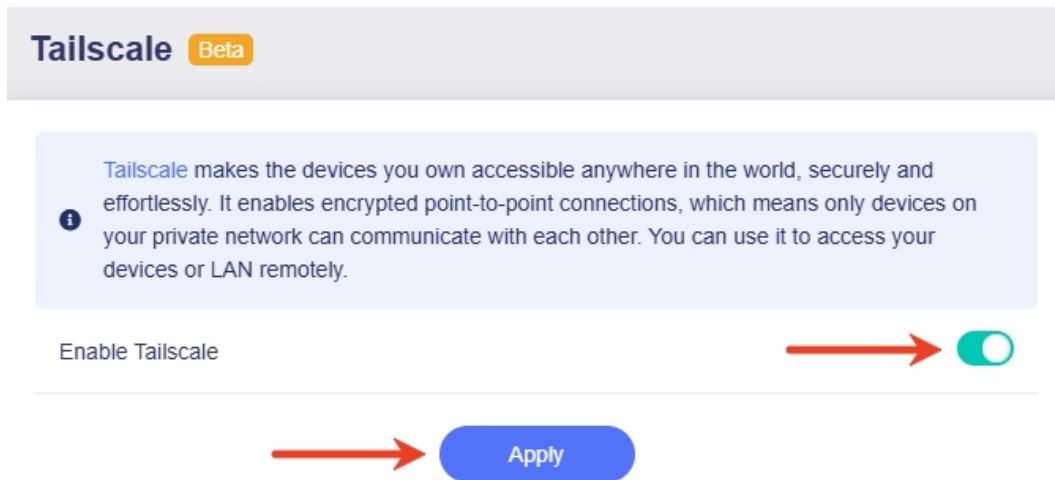
13.7.1 Set Up Tailscale

The following uses a Beryl AX (GL-MT3000) and a laptop as an example.

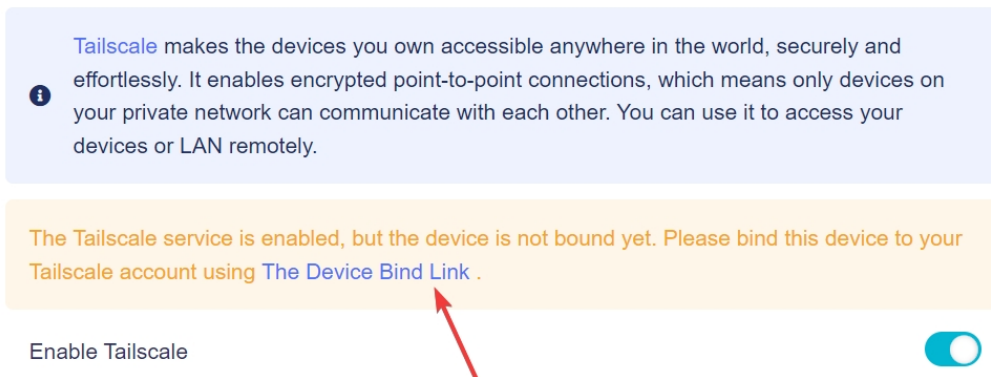
1. Register a Tailscale account first and bind one or two devices to your Tailscale account for testing purposes. After binding, you will see your devices in the Tailscale Console.



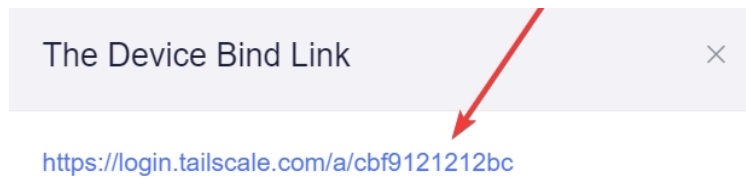
2. Log in to your router's web admin panel and navigate to **APPLICATIONS > Tailscale**. Toggle on **Enable Tailscale** and click **Apply**.



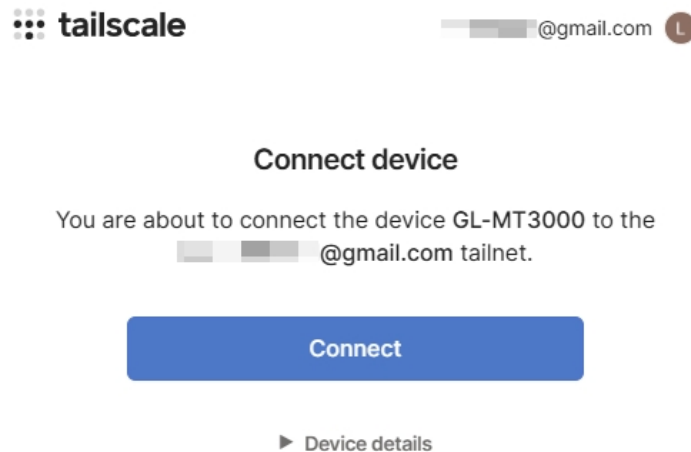
3. The page will prompt you to bind the device. Click **Device Bind Link**.



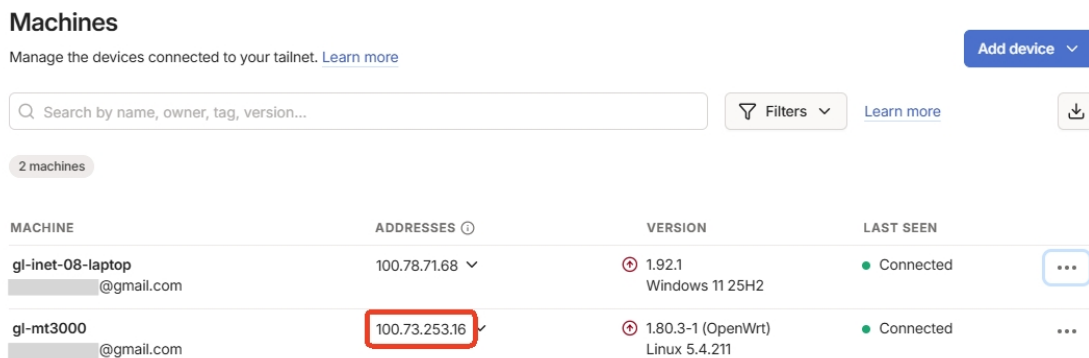
4. In the pop-up window, click the link and log in with your Tailscale account.



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

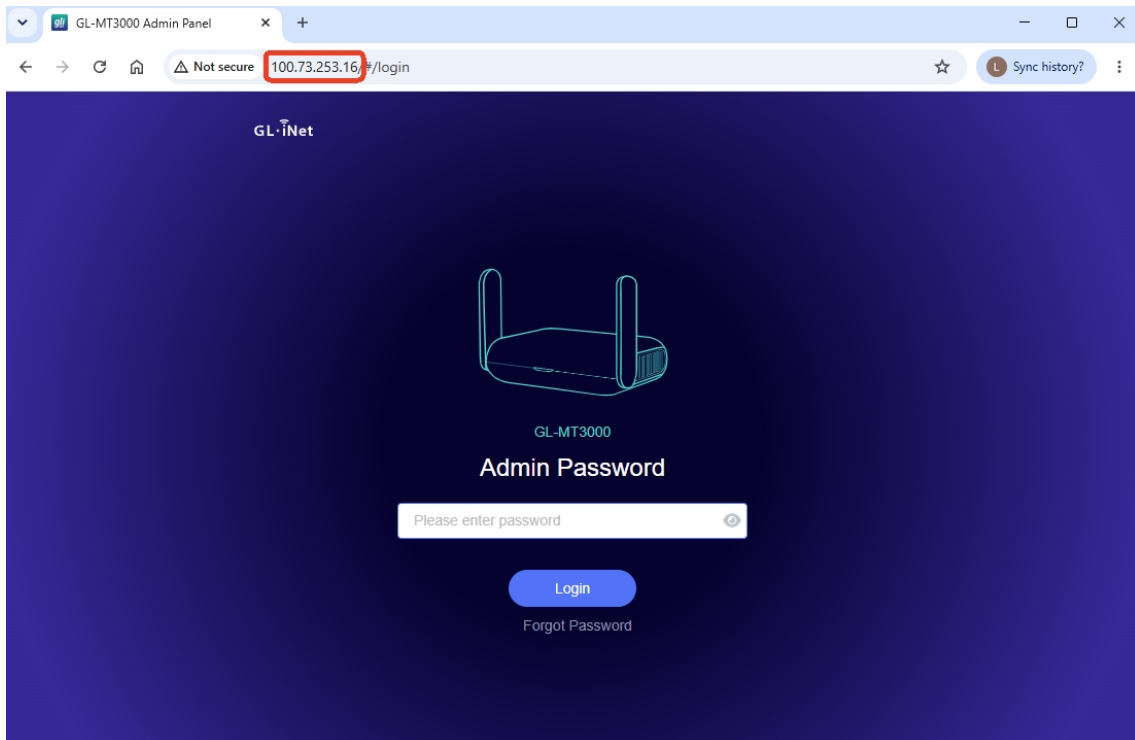


6. You will then be redirected to the Tailscale admin console. Now the router has been added into the Tailscale virtual network, and it can be accessed remotely by the Tailscale virtual IP **100.73.253.16**.



7. Test connectivity.

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



13.7.2 Allow Remote Access WAN

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

Tailscale Beta

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

The device is connected to your Tailscale virtual network.

Enable Tailscale



Bind Account

@gmail.com [Unbind](#)

Router Virtual IP 

100.73.253.16

Custom Exit Node



Allow Remote Access WAN 



Allow Remote Access LAN 



Apply

13.7.3 Allow Remote Access LAN

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

Tailscale Beta

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

The device is connected to your Tailscale virtual network.

Enable Tailscale

☒

Bind Account

@gmail.com [Unbind](#)

Router Virtual IP **i**

100.73.253.16

Custom Exit Node

☐

Allow Remote Access WAN **i**

☐

Allow Remote Access LAN **i**

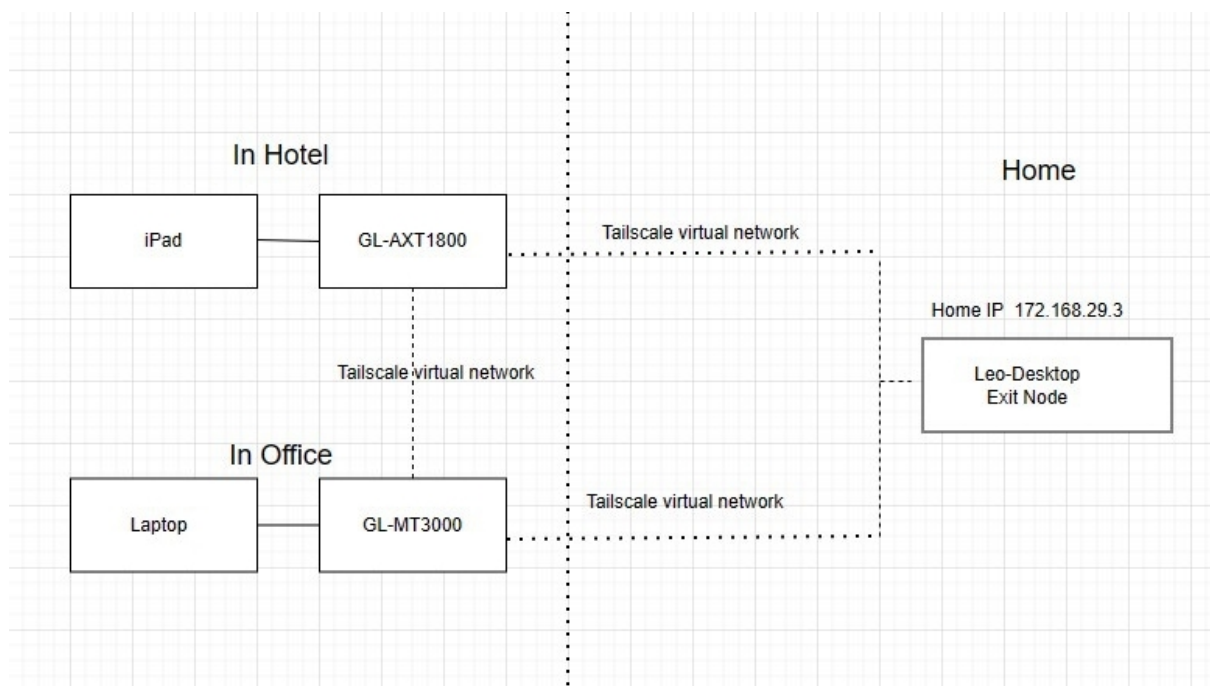
☒

Apply

13.7.4 Custom Exit Nodes

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

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



In summary, an Exit node routes outbound Internet traffic from your Tailnet devices, effectively acting as VPN servers. When connected to an Exit node, all your non-Tailscale Internet traffic appears to originate from its location, helping you access geo-restricted content and enhance your online privacy. The device handling this traffic forwarding is referred to as an "[Exit Node](#)". To configure custom exit node on GL.iNet routers, please refer to this [tutorial](#).

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.

13.8 eSIM Management

Log in to your router's web admin panel and navigate to **APPLICATIONS > eSIM Management**. This page allows you to check eSIM physical card status and manage eSIM profiles. It consists of two parts: **Current eSIM Status** and **eSIM Profile List**.

eSIM Management

Current eSIM Status

EID	6898
ICCID	865F
IMSI	2865
eSIM OS Version	10.34
eSIM Storage(remain/total)	296KB/360KB
eSIM Profile Number ⓘ	1

eSIM Profile List

Export Log For Support

Seed Profile ⓘ

ICCID	Usage(remain/total/expire)	Action
865F	US/EU: 1.00 GB/1.00 GB/Unactivated	Disable Top-up

Normal Profile

eSIM Profile Recommended Store

ICCID	Supplier	Name	Action
No Normal Profile			

+ Add eSIM Profile(QRCode Install) ⓘ

13.8.1 Current eSIM Status

This section displays basic information and details about the currently active eSIM profile.

Current eSIM Status	
EID	6898
ICCID	865F
IMSI	2865
eSIM OS Version	10.34
eSIM Storage(remain/total)	296KB/360KB
eSIM Profile Number ⓘ	1

- **EID:** The globally unique identifier of the eUICC (eSIM chip), used for identification and profile management.
- **ICCID:** The Integrated Circuit Card Identifier of the currently active eSIM profile.
- **IMSI:** The International Mobile Subscriber Identity of the currently active eSIM profile.
- **eSIM OS Version:** The operating system version of the eUICC, which defines its compatibility and supported capabilities.
- **eSIM Storage (remain/total):** Available and total storage capacity on the eUICC for storing eSIM profiles.
- **eSIM Profile Number:** Number of eSIM profiles currently stored on the eUICC. Note that eSIM profiles offered by different carriers vary in size, so the number of profiles that can be stored on the eUICC will also differ.

13.8.2 eSIM Profile List

This section displays information about the eSIM seed profile and normal profiles.

eSIM Profile List

Export Log For Support

Seed Profile ⓘ

ICCID	Usage(remain/total/expire)	Action
 865F	US/EU: 1.00 GB/1.00 GB/Unactivated	Disable Top-up

Normal Profile

eSIM Profile Recommended Store

ICCID	Supplier	Name	Action
No Normal Profile			

+ Add eSIM Profile(QRCode Install) ⓘ

- **Seed Profile:** The seed profile comes preloaded with 1GB of free data for the U.S. and Europe, plus 100MB of global data, valid for 1 year from the date of activation. This data allows you to download other profiles anywhere in the world. You can also monitor usage of the seed profile, including remaining data, total data allowance, and expiration date.
- **Normal Profile:** If you purchase an eSIM profile and upload it via a QR code or activation code, the profile will be displayed here.

13.8.2.1 Top-up Seed Profile

GL.iNet provides a preloaded seed profile with 100MB of global data and 1GB of data valid in Europe and the U.S. for initial setup and eSIM profile activation. This plan is designed for downloading new eSIM profiles when you arrive at a destination with no internet access.

If you have used up the preloaded free data, or if the free data has expired and you wish to continue using the service, you can top up your seed profile.

In the Seed Profile section, click the **Top-up** button on the right.

eSIM Profile List

Export Log For Support

Seed Profile ⓘ

ICCID	Usage(remain/total/expire)	Action
865F	US/EU: 1.00 GB/1.00 GB/Unactivated	Enable Top-up

In the pop-up window, scan the QR code and follow the instructions to complete your top-up.

Scan the QR code to top up



13.8.2.2 Purchase eSIM Profile

You can purchase eSIM profiles from our recommended stores, tested stores, or other third-party eSIM providers.

Option 1: Purchase From Our Recommended Stores.

There are two recommended stores: [EIOTCLUB eSIM Store](#) and [Tuge eSIM Store](#).

In the Normal Profile section, click **eSIM Profile Recommended Store** on the right.

Normal Profile

eSIM Profile Recommended Store

ICCID	Supplier	Name	Action
No Normal Profile			
+ Add eSIM Profile(QRCode Install)			

Scan the QR code or click the links to purchase eSIM profiles.

eSIM Profile Recommended Store ×



EIoTCLUB eSIM Store >



Tuge eSIM Store >

Note: All eSIM profile packages purchased from these two stores are fully compatible with GL.iNet routers. If you have any questions, contact our support team at support@gl-inet.com.

Option 2: Purchase From Tested Stores.

Refer to [this link](#) to view a list of stores tested by GL.iNet.

Note: We cannot guarantee full compatibility with GL.iNet routers for all profiles or packages from these stores. Since GL.iNet does not have partnerships with them, we cannot provide after-sales support or assist with refunds.

Option 3: Purchase From Other Third-Party Esim Providers.

You can also choose to buy eSIM profiles from other third-party providers of your choice.

However, we cannot guarantee full compatibility with GL.iNet routers for eSIM profiles purchased from other third-party providers. Please purchase at your own discretion. GL.iNet is not responsible for any incompatibility issues.

For after-sales support or refunds, please contact the corresponding eSIM provider.

13.8.2.3 Upload eSIM Profile

After purchasing an eSIM profile, you will typically receive a QR code (or an activation code). Save this QR code locally, then follow the steps below to upload your eSIM profile.

1. In the Normal Profile section, click **Add eSIM Profile** at the bottom.

Normal Profile

eSIM Profile Recommended Store

ICCID	Supplier	Name	Action
No Normal Profile			
→ + Add eSIM Profile(QRCode Install) i			

2. Upload your eSIM QR code or enter the activation code, then click **Install**. It will then download and install the eSIM profile onto your router.

Add eSIM Profile(QRCode Install)

Upload QRCode



Select a file to upload or drag it here
File types include: .jpeg, .jpg, .png

Input Activation Code

Activation Code

Confirmation code

Optional

Cancel

Install

Note:

1. Most eSIM profiles can only be downloaded and installed once.

2. A properly formatted QR code will display an activation code that starts with **LPA:**. However, some non-standard QR codes may only provide a raw activation code without the LPA prefix. In this case, manually add LPA: at the beginning of the code before clicking the Install button.

Add eSIM Profile(QRCode Install)

Upload QRCode



Select a file to upload or drag it here

Input Activation Code

Activation Code

LPA:1\$smdp.io\$57-25QC4A-1

Confirmation code

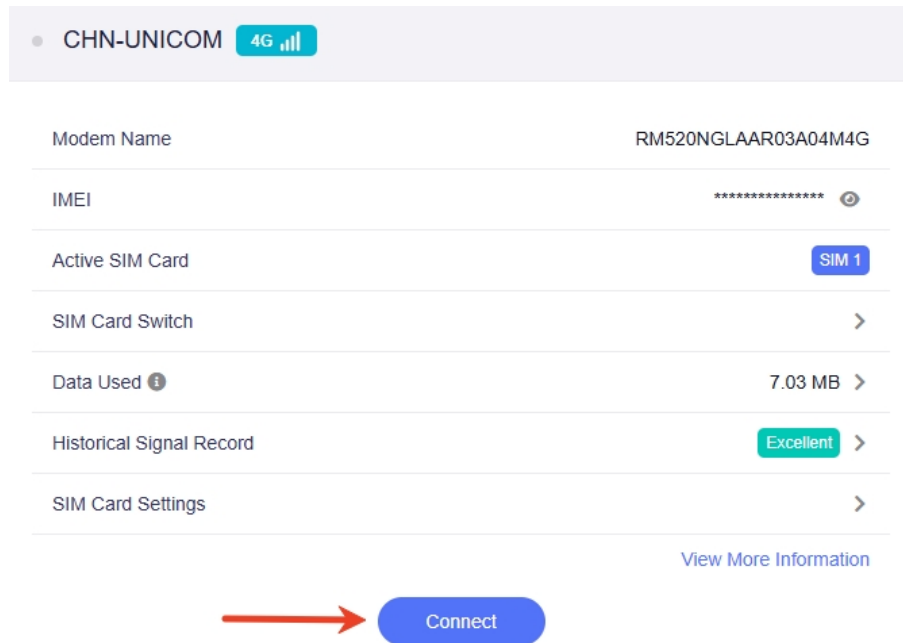
Optional

3. If you haven't purchased any eSIM profile, you may purchase one from the eSIM Profile Recommended Store. Click [here](#) for details.
3. After successful upload, your new eSIM profile will appear in the **Normal Profile** list. Click **Enable** to activate it.

Normal Profile				eSIM Profile Recommended Store	
ICCID	Supplier	Name		Action	
 3181	CITIC Telecom	2025.10.31 12:19		Disable	
 1013	Redtea Mobile	2025.11.19 12:22		Enable	Delete
 7194	CITIC Telecom	2025.10.24 18:09		Enable	Delete
+ Add eSIM Profile(QRCode Install) ⓘ					

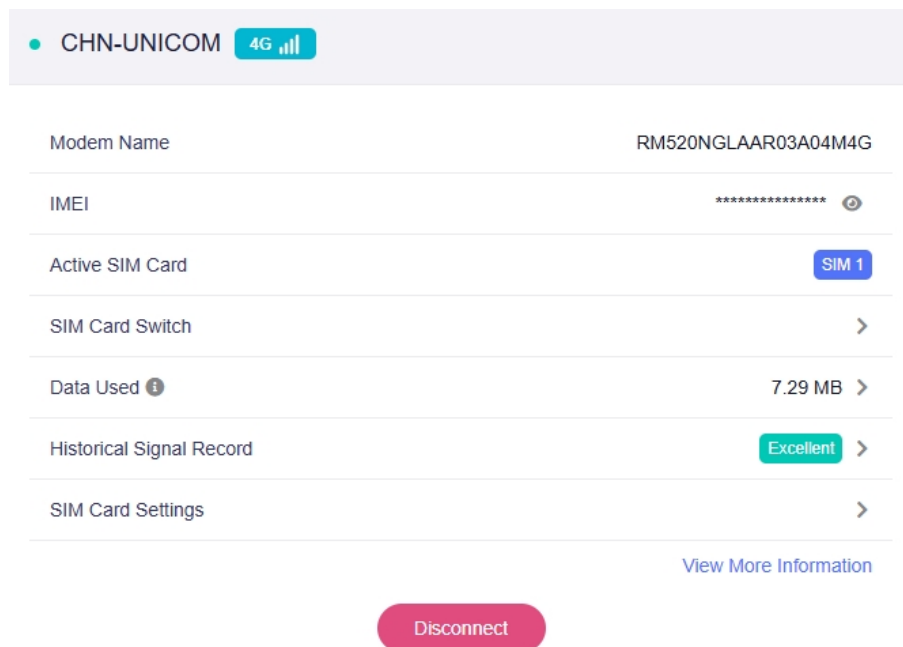
4. Connect to the Internet.

After enabling the eSIM profile, go to **INTERNET > Cellular**. Click **Connect** to establish an internet connection via your eSIM profile.



Note: Some eSIM profiles may require additional configuration, such as APN, PIN, or TTL settings. If needed, click **Manual Setup** or **SIM Card Settings** to adjust these parameters. In some cases, you may need to reboot the device to establish an internet connection.

5. Once the router connects successfully via the eSIM profile, the page will display as follows:



13.8.2.4 Export Log for Support

Click **Export Log for Support** to view all eSIM-related logs.

If you encounter any issues and require technical support, export the eSIM logs and share them with our support team via email at support@gl-inet.com.

eSIM Profile List

Export Log For Support

Seed Profile ⓘ

ICCID	Usage(remain/total/expire)	Action
 865F	US/EU: 1.00 GB/1.00 GB/Unactivated	Disable Top-up

Chapter 14

Network

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

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

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

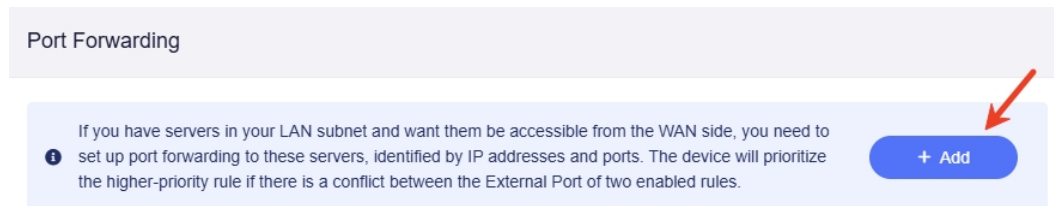
- **Priority:** Set it as Highest or Lowest. If the priority of the DMZ is higher than the port forwarding rules, all port forwarding rules will be invalidated. Otherwise, requests will be forwarded to the DMZ client device only if the accessed port has no corresponding port forwarding rule.
- **DMZ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

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

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



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

Add New Port Forwarding Rule

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

Cancel

Apply

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

14.2 Multi-WAN

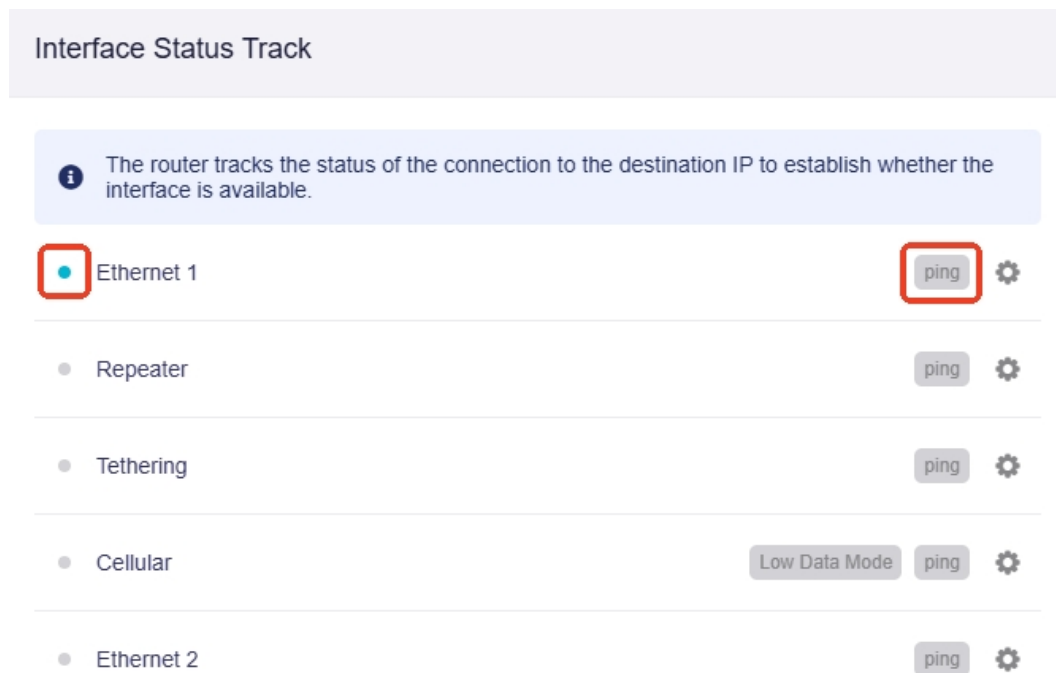
Multi-WAN enables simultaneous use of multiple Internet access methods, allowing configuration of diverse connectivity options on the router. It offers two working modes:

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

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

14.2.1 Interface Status Track

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



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

Ethernet 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

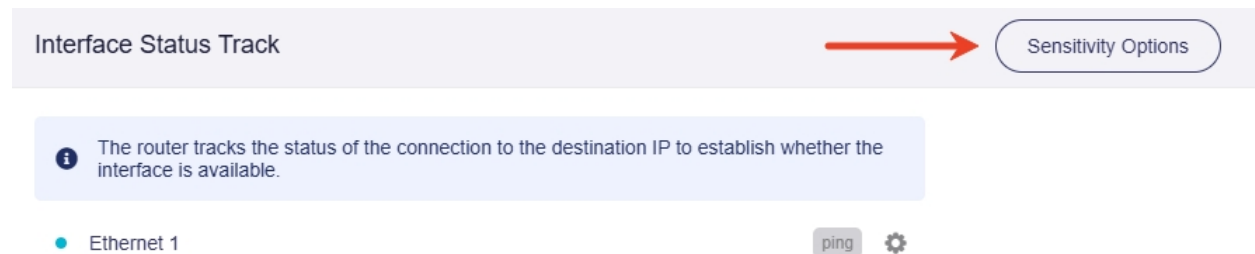
Cancel

Apply

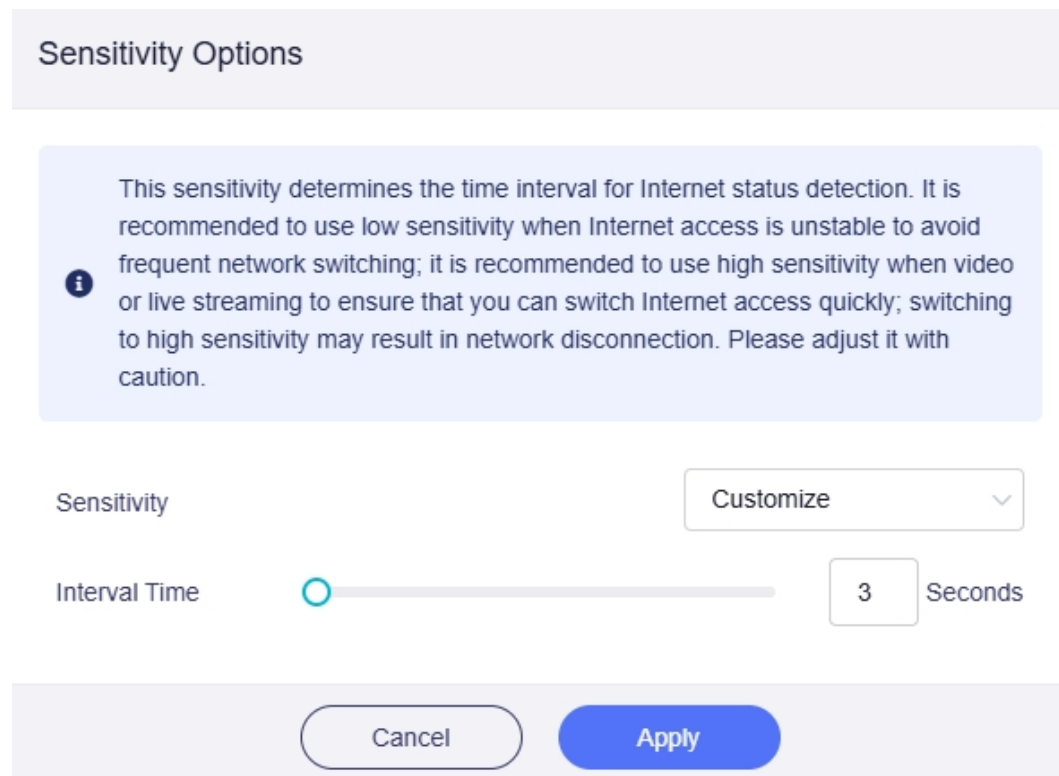
- **Enable Interface Status Track:** It is enabled by default. If disabled, the router will determine the interface status based on physical conditions (e.g., whether the Ethernet cable is plugged in).
- **Detection Mode:** This feature was introduced as Low Data Mode in firmware v4.5, then renamed Detection Mode in firmware v4.7. Three modes are available: Normal Mode, Low Data Mode, and Strict Mode.
 - **Normal:** It is used by default.
 - **Low Data:** 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:** 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.



14.2.2 Multi-WAN Mode

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

Failover

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

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

Interface Priority

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

Apply

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

Load Balance

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

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

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.

i 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

Load Ratio

Ethernet 1	1
Repeater	1
Tethering	1
Cellular	1
Ethernet 2	1

Apply

For example, if the router is connected to four networks (e.g., Ethernet, Repeater, Tethering, and Cellular) simultaneously and all four interfaces are available for Internet access, enabling Load Balance and setting a 1:1:1:1 ratio means the four interfaces will share network bandwidth

equally. The system will distribute new connections across these four interfaces according to the configured 1:1:1:1 load ratio.

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

14.3 LAN

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

Log in to your router's web admin panel and navigate to **NETWORK > LAN**. Here you can configure LAN settings, including basic settings, DHCP server, and address reservation.

14.3.1 Basic Settings

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

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

Security Settings

AP Isolation *i* ☐

Apply

- **Router IP Address:** This is the address entered into a browser's address bar to access the router's admin panel. It is 192.168.8.1 by default and can be changed if it conflicts with the upstream network.
- **Netmask:** Two options are available: 255.255.255.0 and 255.255.0.0.
- **AP Isolation:** You can isolate your network's client devices into a separate network area. These devices cannot communicate with other devices on the network.

14.3.2 DHCP Server

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

[Apply](#)

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

Start IP Address

End IP Address

 [Advanced](#)

[Apply](#)

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

Lease Time	720	Minutes
Gateway	Optional	
DNS Server 1	Optional	
DNS Server 2	Optional	
LPR Server 	Optional	

[+ Add](#)

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

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

14.3.3 Address Reservation

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

Follow the steps below to configure address reservation if needed.

1. Log in to your router's web admin panel, navigate to **NETWORK > LAN > Address Reservation**, and click **Add**.
2. In the pop-up window, select the MAC address from the drop-down list, then the corresponding IP address for the selected MAC will be auto-filled. Enter a descriptive name and click **Submit**.

Add a New Reservation Entry

MAC

IP

192.168.8.223

Description

Lauren-iPhone

Cancel

Submit

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

Address Reservation

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

Add

MAC ▾	IP ▾	Description ▾	Action
	192.168.8.223	Lauren-iPhone	...

14.4 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** -> **Guest Network**. This page allows you to configure Guest Network settings, including basic settings and DHCP server.

14.4.1 Basic Settings

The basic settings include Gateway, Netmask, AP Isolation, and Block WAN Subnets.

Guest Network

Info 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

Security Settings

AP Isolation Info	☒
Block WAN Subnets Info	☐

Apply

- **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.
- **AP Isolation:** It is used to isolate guest network clients into separate segments so they cannot communicate with other devices on the same network.
- **Block WAN Subnets:** If enabled, the guest network will not be able to access the upstream network or its corresponding network segment.

14.4.2 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

Apply

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

Start IP Address

192.168.9.100

End IP Address

192.168.9.249

Advanced

Apply

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

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

[+ Add](#)

- **Lease Time:** The duration for which a device can use an IP address assigned via 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.

14.5 DNS

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

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

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

14.5.1 General Settings

DNS



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

DNS Rebinding Attack Protection 

☐

Override DNS Settings of All Clients 

☐

Allow Custom DNS to Override VPN DNS 

☒

DNS Server Settings

Mode

Automatic 

DNS from Repeater

192.168.18.1

Apply

- **DNS Rebinding Attack Protection:** Protects against DNS rebinding attacks by blocking malicious DNS resolution attempts. Note that enabling it may cause private DNS lookup failure; 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.

14.5.2 DNS Server Settings

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

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

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

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

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

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

DNS Server Settings

Mode

Encrypted DNS

Encryption Type

DNS over TLS

DNS Provider

DNS over TLS

DNSCrypt-Proxy

DNS over HTTPS

Oblivious DNS over HTTPS

Apply

- 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.

DNS Server Settings ⓘ

Mode

Manual DNS

DNS Server 1

DNS Server 2

Optional

DNS Server 3

Optional

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

14.5.3 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 Repeater

192.168.18.1

Apply

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

Edit Hosts

 Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.

```
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
```

Cancel

Apply

14.6 Ethernet Port

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

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

 WAN

As WAN Port

 LAN

As LAN Port

WAN/LAN

Ethernet1

WAN

LAN

MAC Mode

Factory

MAC Address

94:83:C4:XX:XX:XX

Negotiated Network Port Rate

Speed

1000 Mbps full duplex

Apply

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

 WAN

As WAN Port

 LAN

As LAN Port

WAN/LAN

WAN

LAN

Negotiated Network Port Rate

Speed

1000 Mbps full duplex

Apply

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.

14.7 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.

i 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.

14.8 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 IPv6**, 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 (Firewall, GoodCloud, OpenVPN DCO) do not yet support IPv6.

Enable IPv6 

LAN

Mode **i**

Native

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.

14.8.1 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.

14.8.2 DNS acquisition method

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

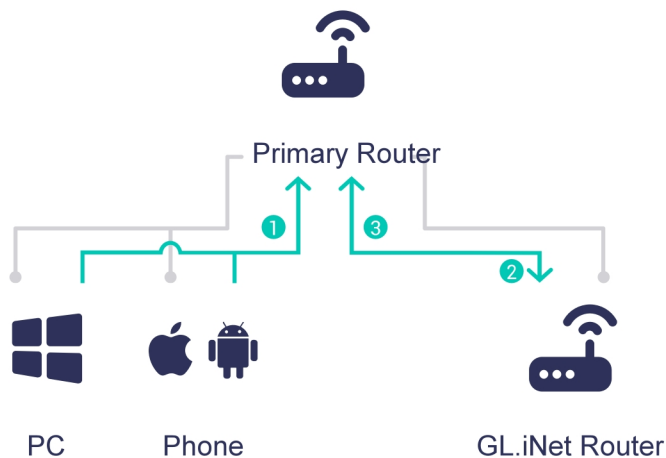
- **Automatic:** The router will obtain IPv6 DNS server addresses dynamically (e.g., via DHCPv6).
- **Manual:** Input custom IPv6 DNS server addresses. However, since DNS is used to resolve domain names to their corresponding IP addresses, manual DNS server configuration may result in DNS lookup failures.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

14.9 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.

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

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

Enable Drop-in Gateway Mode ⓘ 

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2

2. Select the configuration method, then click **Apply**. Please refer to [this tutorial](#) for details.

Configuration method

☒

All devices are networked through drop-in gateway
 You need to go to modify the primary route configuration, which must be configured by a user who has access to the primary route. [Setup Guide](#)

☐

Some devices select their own networking gateway
 You need to manually change the gateway address to the IP address of the drop-in gateway on some of the devices that need to use the drop-in gateway. [Setup Guide](#)

14.10 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

14.11 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 an acceleration mode among Auto, Hardware Acceleration and Software Acceleration.

Network Acceleration

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

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

Auto



Apply

- **Auto:** Automatically switch between the two acceleration modes based on actual usage.
- **Hardware Acceleration:** It offloads high-frequency network tasks (e.g., NAT, packet forwarding, checksum verification) to dedicated hardware like NPUs or HWNAT chips. It specifically works on Ethernet 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.

14.12 NAT Settings

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

NAT Settings

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

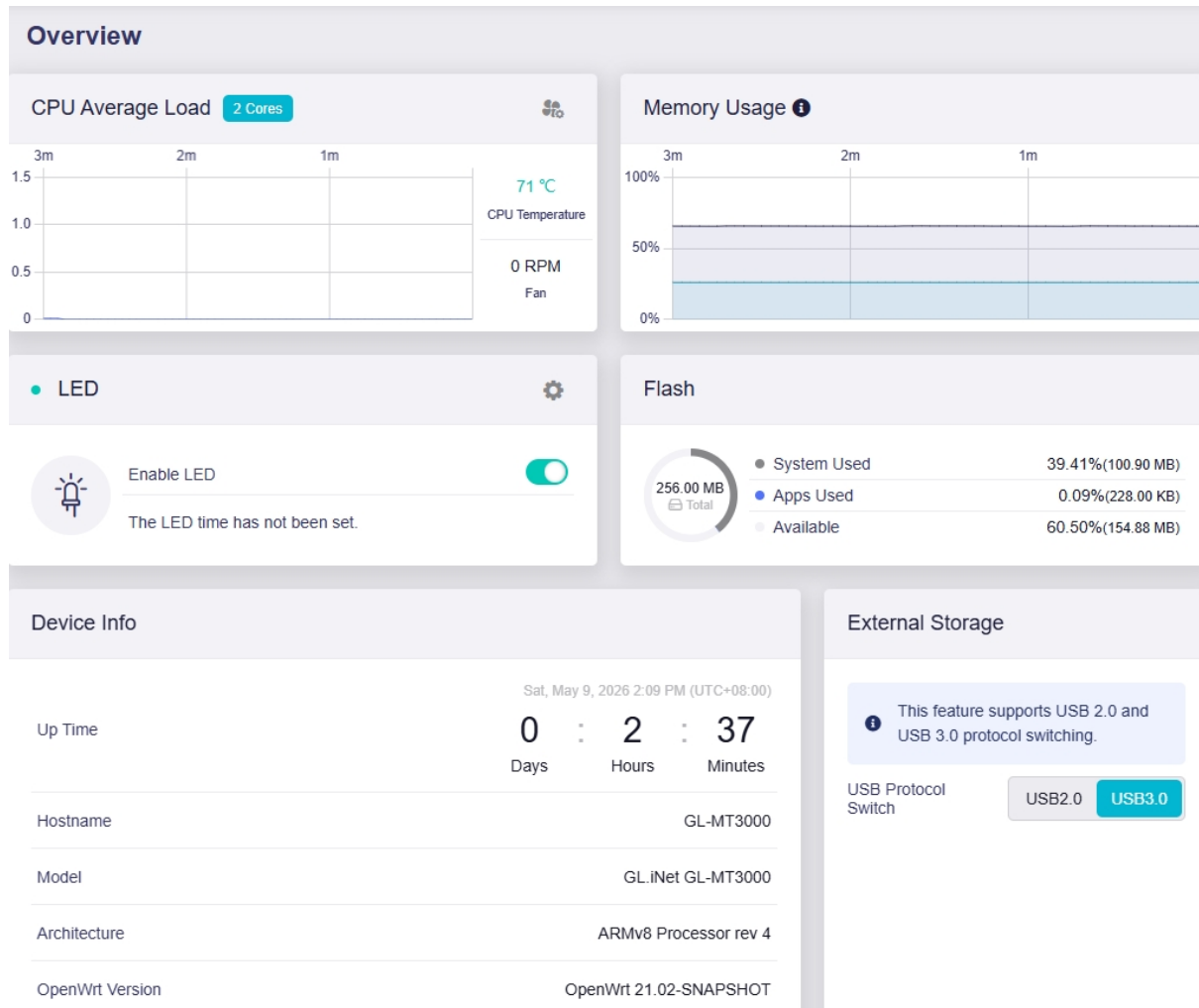
System

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

15.1 Overview

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

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



15.2 Upgrade

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

15.2.1 Firmware Online Upgrade

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

Firmware Online Upgrade

Firmware Local Upgrade

✓ Firmware is up-to-date.

Current Firmware

Version	4.0
Firmware Type	0803release
Update Time	2025-11-06 12:14:12 (UTC+00:00)

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).

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

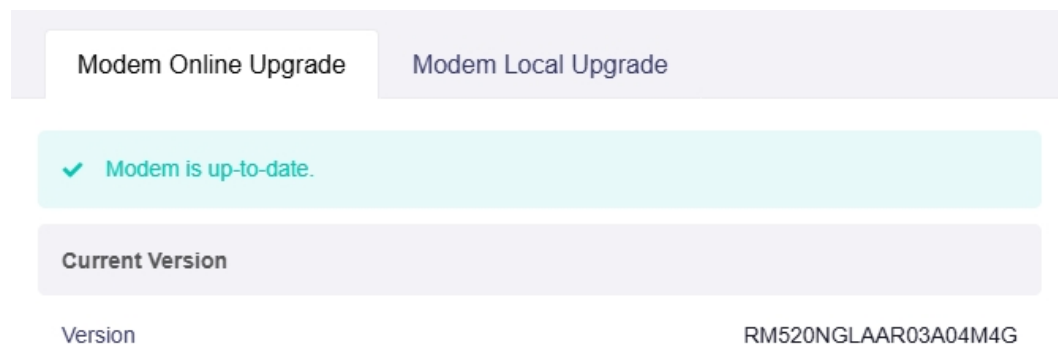
Install

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

15.2.3 Modem Online Upgrade

GL.iNet cellular routers allow users to view and upgrade the cellular modem firmware through the web Admin Panel.

You can find the current cellular modem version here. If your router is connected to the Internet, it will automatically check for the latest cellular modem version from the manufacturer's server, simplifying the update process.

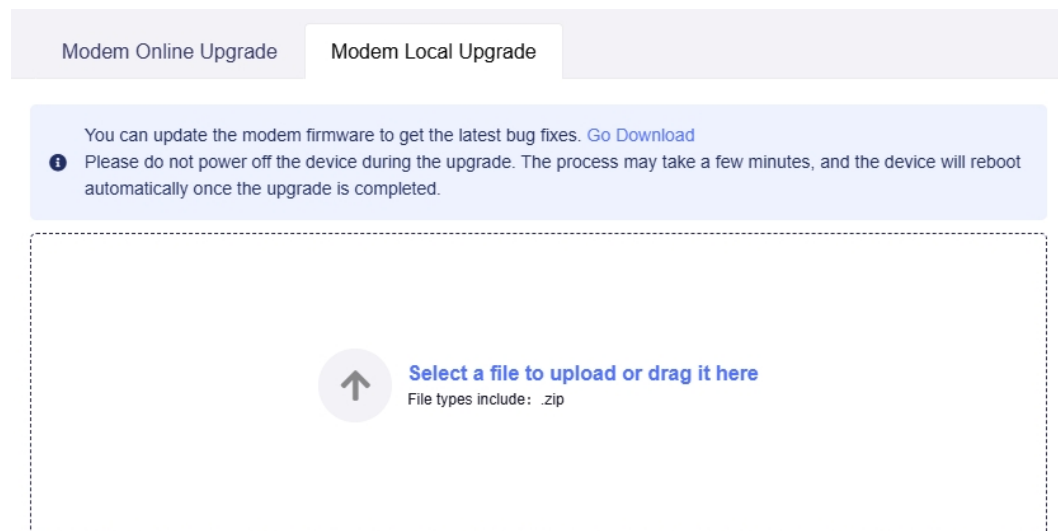


The interface for 'Modem Online Upgrade' features two tabs: 'Modem Online Upgrade' (active) and 'Modem Local Upgrade'. A green success message states 'Modem is up-to-date.' Below this, a section titled 'Current Version' displays the version number 'RM520NGLAAR03A04M4G'.

15.2.4 Modem Local Upgrade

You may try a cellular module upgrade when cellular networking fails or experiences instability. We recommend contacting technical support for troubleshooting before performing the modem upgrade.

Manually upload a modem firmware file to update the cellular modem if needed.



The 'Modem Local Upgrade' interface includes two tabs: 'Modem Online Upgrade' and 'Modem Local Upgrade' (active). A light blue information box contains the text: 'You can update the modem firmware to get the latest bug fixes. [Go Download](#)' followed by a note: 'Please do not power off the device during the upgrade. The process may take a few minutes, and the device will reboot automatically once the upgrade is completed.' Below this is a large dashed box for file upload, containing an upward arrow icon and the text 'Select a file to upload or drag it here' with 'File types include: .zip'.

15.3 Scheduled Tasks

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

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

15.3.1 LED Display Schedule

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

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.

15.3.2 Schedule Reboot

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

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.

15.3.3 5GHz Wi-Fi Schedule

This function allows you to set a schedule for your 5GHz 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 5GHz 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 5GHz 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)

Su

Mo

Tu

We

Th

Fr

Sa

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

Enable Guest Wi-Fi Schedule



Guest Wi-Fi

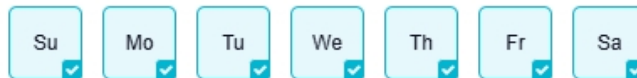
Turn On Time

🕒 07:00

Turn Off Time

🕒 22:00

day(s)



Mode 2: Switch TX Power

You can enable the TX power switching schedule for the 5GHz 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 5GHz 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

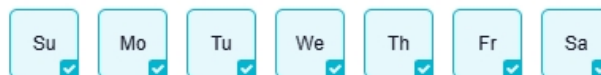
🕒 07:00

Set to

Max



day(s)



- **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.

15.3.4 2.4GHz Wi-Fi Schedule

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

Mode 1: Turn On/Off

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

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 2.4GHz Main Wi-Fi, and select an effective date for the week.

Enable Main Wi-Fi Schedule



Main Wi-Fi

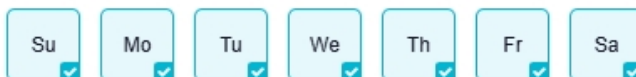
Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Enable Guest Wi-Fi Schedule



Guest Wi-Fi

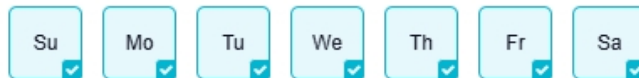
Turn On Time

🕒 07:00

Turn Off Time

🕒 22:00

day(s)



Mode 2: Switch TX Power

You can enable the TX power switching schedule for the 2.4GHz 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 2.4GHz 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

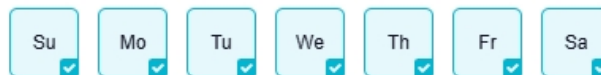
🕒 07:00

Set to

Max



day(s)



- **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.

15.4 Time Zone

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

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

⚠

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

Sync

Router Time

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

UTC

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

Router Time

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

Etc/GMT-8

Etc/GMT-7

Etc/GMT-8

Etc/GMT-9

Etc/GMT-10

15.5 Log

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

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

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

Your Feedback

Subject

Your Contact Email

Description

0/1000

Upload Picture (Optional)



You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.

- ☒ Upload System Log
- ☒ Upload Debug Info
- ☐ I have read and agree [Privacy Policy](#)

Cancel

Send

15.6 Security

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

- Admin password
- Local access for web admin panel, LuCI, and SSH
- Remote HTTPS/SSH access
- Open ports on router

15.6.1 Admin Password

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

Admin Password

Old Password

Enter old password

New Password

Enter new password

Confirm Password

Enter new password again

Apply

The requirements for the admin password are as follows:

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

15.6.2 Access Control

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

Access Control

Admin Panel

HTTP Port

80

HTTPS Port

443

Force HTTPS



Auto-Logout Time ⓘ

5

Minutes

LuCI

HTTP Port

8080

HTTPS Port

8443

Force HTTPS



SSH

Enable SSH



SSH Port

22

Apply

Admin Panel

- **HTTP Port:** Defaults to 80, used for unencrypted HTTP access to the web admin panel.
- **HTTPS Port:** Defaults to 443, used for secure HTTPS access to the web admin panel.

- **Force HTTPS:** When enabled, access to the web admin panel is enforced to use a secure HTTPS connection.
- **Auto-Logout Time:** Set to 5 minutes by default, it automatically logs out idle admin sessions after this duration for security. You can customize the auto-logout time, ranging from 1 minute to 3 hours.

LuCI

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

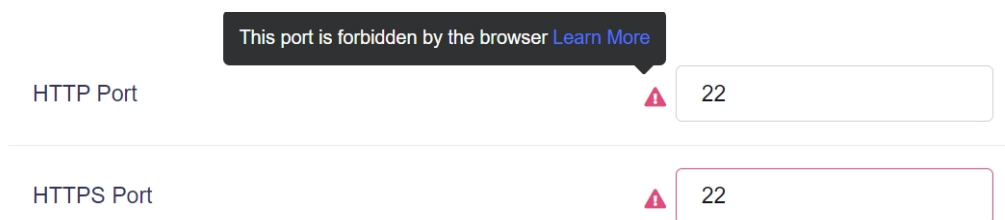
- **HTTP Port:** Defaults to 8080, for unencrypted HTTP access to the LuCI interface.
- **HTTPS Port:** Defaults to 8443, for secure HTTPS access to the LuCI interface.
- **Force HTTPS:** When enabled, access to the LuCI interface is enforced to use a secure HTTPS connection.

SSH

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

Note:

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



The screenshot shows a web form for configuring LuCI settings. At the top, a dark grey tooltip with white text says "This port is forbidden by the browser" followed by a blue link "Learn More". Below this, there are two input fields. The first is labeled "HTTP Port" and contains the value "22". To its right is a red triangle warning icon. The second is labeled "HTTPS Port" and also contains the value "22", with a red triangle warning icon to its right. The form is separated by a horizontal line.

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

15.6.3 Remote Access Control

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

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

...

15.6.4 Open Ports on Router

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

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.

15.7 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.

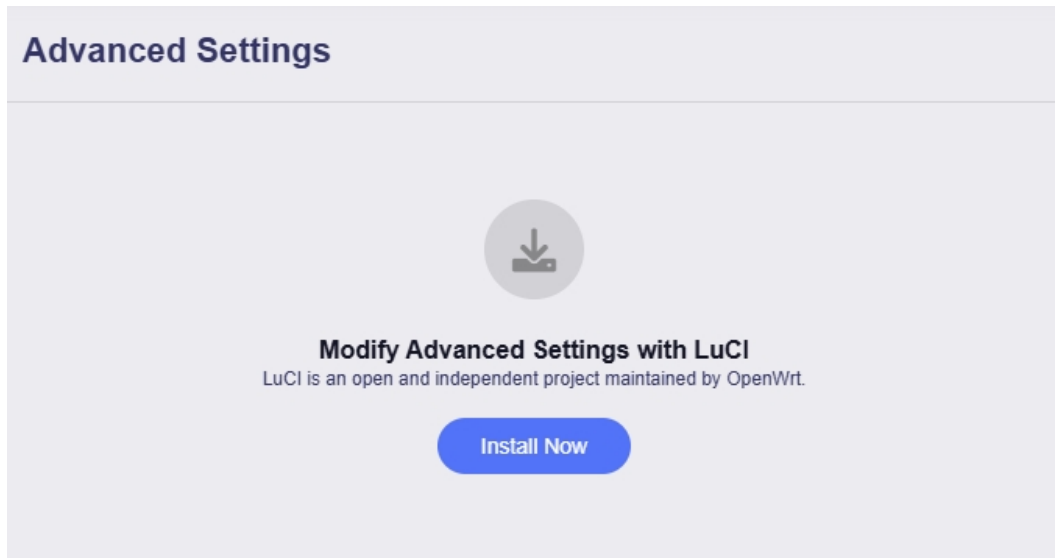
If you fail to access the router's web admin panel, try resetting your router using the physical reset button on the side.

15.8 Advanced Settings

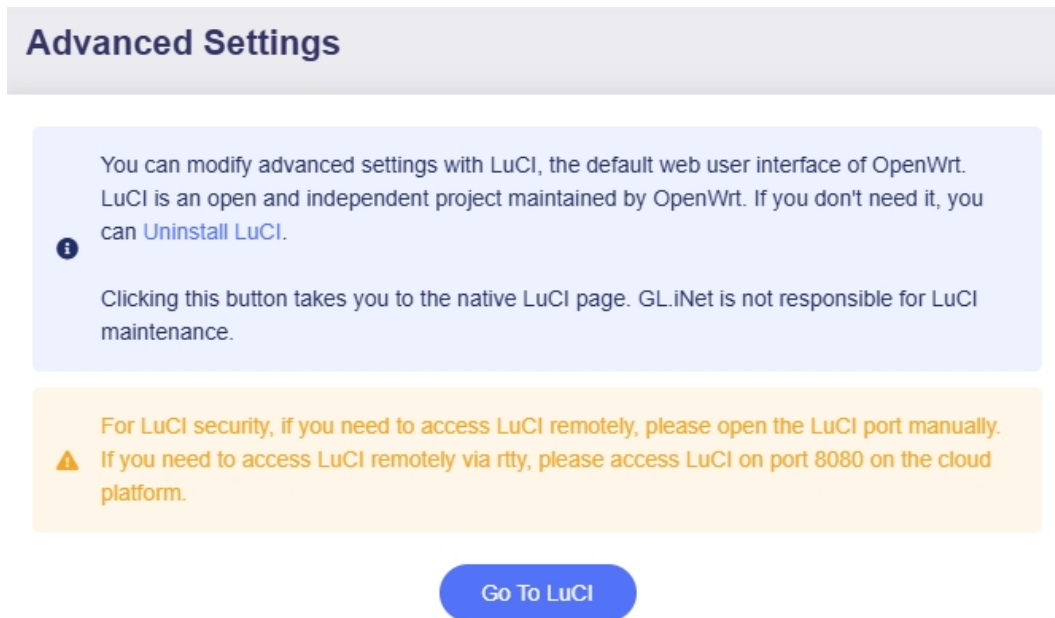
Log in to your router's web admin panel and navigate to **SYSTEM > Advanced Settings**. This page allows you to modify advanced settings in LuCI, which is the default web user interface of OpenWrt. As an open and independent project maintained by OpenWrt, LuCI is provided as-is. GL.iNet is not responsible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

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

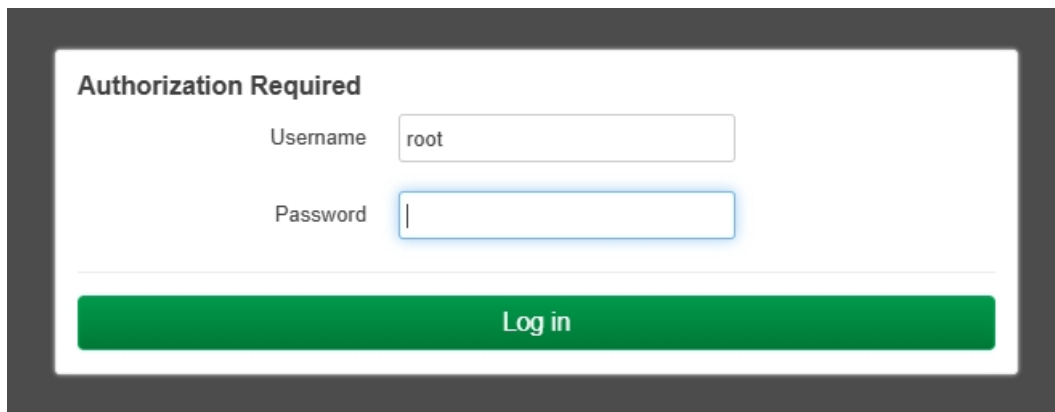
1. Click **Install Now**, and it will be installing LuCI interface.



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.



The image shows a login form titled "Authorization Required". It has two input fields: "Username" with the value "root" and "Password" which is empty. Below the fields is a green "Log in" button.

Authorization Required	
Username	root
Password	
Log in	

You will then log in to the LuCI interface.

GL-X3000		Status ▾	System ▾	Network ▾	Logout
Status					
System					
Hostname	GL-X3000				
Model	GL.iNet GL-X3000				
Architecture	ARMv8 Processor rev 4				
Target Platform	mediatek/mt7981				
Firmware Version	OpenWrt 21.02-SNAPSHOT / LuCI openwrt-21.02 branch git-22.245.77575-63bfee6				
Kernel Version	5.4.211				
Local Time	2026-09-24 20:23:36				
Uptime	10h 8m 39s				
Load Average	0.03, 0.07, 0.08				

Regulatory Statement

FCC ID: 2AFIW-X3000NR | 2AFIW-X3000C16

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
3. Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, and the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help important announcement.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s).

Operation is subject to the following two conditions:

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

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

- (1) L'appareil ne doit pas produire de brouillage;
- (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Cet équipement est conforme aux limites d'exposition aux radiations IC CNR-102 établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

The user manual for LE-LAN devices shall contain instructions related to the restrictions mentioned in the above sections, namely that:

- i. the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- i. le dispositif utilisé dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur afin de réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite dans le même canal;
- ii. for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;

ii. pour les dispositifs à antenne(s) détachable(s), le gain d'antenne maximal autorisé pour les dispositifs dans les bandes 5250-5350 MHz et 5470-5725 MHz doit être tel que l'équipement soit toujours conforme à la norme e.i.r.p. limite;

iii. for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate;

iii. pour les dispositifs à antenne(s) détachable(s), le gain d'antenne maximal autorisé pour les dispositifs de la bande 5725-5850 MHz doit être tel que l'équipement soit toujours conforme à la norme e.i.r.p. les limites, le cas échéant;

The functions of Wireless Access Systems including Radio Local Area Networks(WAS/RLANs) within the band 5150-5350 MHz for this device are restricted to indoor use only within all European Union countries.

Hereby, GL TECHNOLOGIES (HONG KONG) LIMITED declares that the radio equipment type [5G NR Wi-Fi 6 Router, GL-X3000NR / 4G LTE Wi-Fi 6 Router, GL-X3000C16] 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 available at <https://www.glinet.com/products/certificate>.

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);

Power supply: ICP30A-120-2500