GL·iNet

User Manual

GL-E5800 / Mudi 7

5G NR Tri-band Wi-Fi 7 Travel Router

About This Manual

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

With this guide, you will be able to:

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

Format Conventions

These symbols/colors help you follow steps faster.

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

Note:

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

Need More Help or Info?

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

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

Contents

Chapter 1 Get To Know Your Router 6

1.1 Product Overview 7

1.1.1 Appearance 7

1.1.2 Interface and Button 8

1.1.3 Touchscreen 9

1.2 Specifications 10

1.3 Frequency Bands 11

1.4 Package Contents 11

Chapter 2 Router Initialization 12

Chapter 3 Log In To Your Router 14

Chapter 4 Set Up Internet Connection 16

4.1 Quick Setup Wizard 17

4.2 Manually Set Up Internet Connection 18

4.2.1 Connect to the Internet via Cellular 19

4.2.2 Connect to the Internet via Ethernet Cable 23

4.2.3 Connect to the Internet via an Existing Wi-Fi 28

4.2.4 Connect to the Internet via USB Tethering 32

Chapter 5 Wireless 34

5.1 Wi-Fi Status Display 35

5.2 Wireless Settings 36

5.2.1 5GHz/6GHz Wi-Fi 36

5.2.2 2.4GHz Wi-Fi 39

5.2.3 Randomized BSSID 41

Chapter 6 Clients 43

6.1 Device Details 45

6.2 Action 47

6.3 Remove Clients 50

6.4 Sort 51

Chapter 7 Cloud Services 52

7.1 GoodCloud 53

7.1.1 Enable GoodCloud 54

7.1.2 Manage Your Router 56
7.1.3 Unbind Device 61
7.1.4 Disable GoodCloud 61
7.2 AstroWarp 62
Chapter 8 Get To Know VPN 63
8.1 Introduction 64
8.2 Application Scenarios 65
Chapter 9 VPN Dashboard 67
9.1 VPN Setup Wizard 68
9.2 VPN Mode 71
9.2.1 Global Mode 72
9.2.2 Policy Mode 74
Chapter 10 Set Up VPN Server 83
10.1 Set Up OpenVPN Server 84
10.1.1 Preparation 84
10.1.2 Setup Steps 85
10.1.3 Troubleshooting 87
10.2 Set Up WireGuard Server 88
10.2.1 Preparation 88
10.2.2 Setup Steps 89
10.2.3 Troubleshooting 92
Chapter 11 Set Up VPN Client 93
11.1 Set Up OpenVPN Client 94
11.1.1 Preparation 94
11.1.2 Set Up NordVPN 94
11.1.3 Set Up OpenVPN Client Manually (for other providers) 100
11.2 Set Up WireGuard Client 103
11.2.1 Preparation 103
11.2.2 Set Up AzireVPN 104
11.2.3 Set Up Hide.me 108
11.2.4 Set Up IPVanish 111
11.2.5 Set Up Mullvad 115
11.2.6 Set Up NordVPN 119
11.2.7 Set Up PIA (Private Internet Access) 124

11.2.8 Set Up Surfshark 128
11.2.9 Set Up WireGuard Client Manually (for other providers) 132
Chapter 12 Network 137
12.1 Multi-WAN 138
12.2.1 Interface Status Track 138
12.2.2 Multi-WAN Mode 141
12.2 LAN 144
12.2.1 Basic Settings 144
12.2.2 DHCP Server 145
12.2.3 Address Reservation 147
12.3 Guest Network 148
12.3.1 Basic Settings 148
12.3.2 DHCP Server 149
12.4 DNS 151
12.4.1 DNS Server Settings 152
12.4.2 Edit Hosts 154
12.5 Ethernet Port 156
12.6 IPv6 157
12.6.1 IPv6 Mode 158
12.6.2 DNS acquisition method 158
12.7 IGMP Snooping 159
12.8 Network Mode 160
12.9 Drop-in Gateway 162
12.10 Network Acceleration 164
Chapter 13 Flow Control 165
13.1 Parental Control 166
13.1.1 Quick Setup 166
13.1.2 Troubleshooting 174
Chapter 14 Security 175
14.1 Port Forwarding 176
14.1.1 DMZ 176
14.1.2 Port Forwarding 177
14.2 Management Control 179
14.2.1 Access Control 179

14.2.2 Remote Access Control 181
14.2.3 Open Ports on Router 182
14.3 NAT Mode 183
Chapter 15 Applications 184
15.1 Plug-ins 185
15.2 Dynamic DNS 186
15.2.1 Enable DDNS 186
15.2.2 Check if DDNS Works 189
15.2.3 HTTPS Remote Access 191
15.2.4 SSH Remote Access 194
15.3 Network Storage 196
15.3.1 Connect Storage 196
15.3.2 Set Up Samba 197
15.3.3 Set Up WebDAV 200
15.3.4 Set Up DLNA 203
15.4 AdGuard Home 204
15.5 Tailscale 206
15.5.1 Set Up Tailscale 207
15.5.2 Allow Remote Access WAN 210
15.5.3 Allow Remote Access LAN 210
15.5.4 Custom Exit Nodes 211
15.6 ZeroTier 212
15.6.1 Set Up ZeroTier 213
15.6.2 Allow Remote Access WAN 217
15.6.3 Allow Remote Access LAN 218
15.7 Tor 219
Chapter 16 System 220
16.1 Overview 221
16.2 Admin Password 222
16.3 Upgrade 223
16.3.1 Online Upgrade 223
16.3.2 Local Upgrade 224
16.4 Scheduled Tasks 225
16.5 Display Management 226

16.6 USB & Power 227
16.6.1 USB 227
16.6.2 Power 228
16.7 Time Zone 229
16.8 Reset Firmware 230
16.9 Log 231
16.10 Advanced Settings 233
Regulatory and Legal 235

Chapter 1

Get To Know Your Router

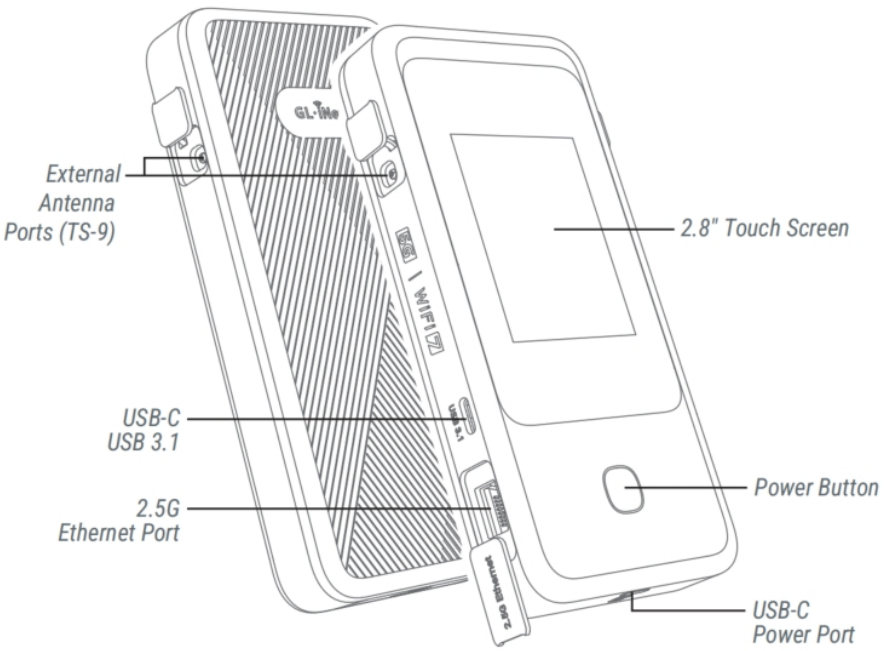
This chapter covers the router overview, specifications, and package contents.

1.1 Product Overview

Mudi 7 (GL-E5800) delivers ultra-fast 5G speeds up to 4.67 Gbps and tri-band Wi-Fi 7 for reliable, secure networking. It supports built-in eSIM and dual-SIM dual standby to ensure seamless connectivity. Boasting a touchscreen, 2.5G Ethernet port, fast charging and long-lasting battery life, Mudi 7 serves as your all-in-one solution for high-performance portable connectivity.

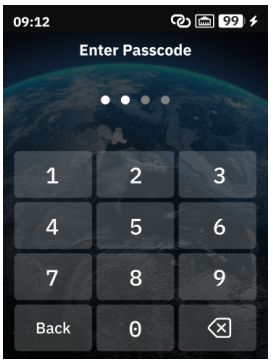
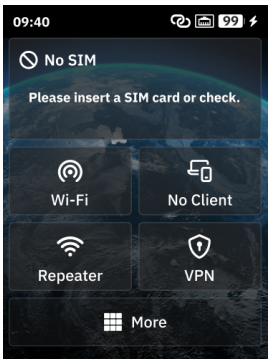
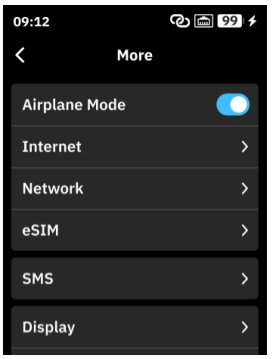
1.1.1 Appearance

1.1.2 Interface and Button



Item	Description
Power Port	For connecting the power adapter.
Power Button	To wake up the screen or return to the homepage.
2.5G Ethernet Port	As WAN: For connecting to a modem or an Ethernet outlet. As LAN: For connecting wired devices to the router.
USB 3.1 Port	For connecting a USB storage device to the router.
2.8" Touchscreen	For real-time status checks and extensive functional control.
External Antenna Ports (TS-9)	For connecting external antennas with the TS-9 interface.

1.1.3 Touchscreen

Screen Display	Description
	Wake Display You can adjust the time and date display style on the wake screen and customize the background image as needed.
	Enter Passcode A 4-digit passcode is required to unlock the screen. You can customize the screen auto-lock time to reduce how often you need to enter the passcode.
	Homepage The homepage displays the status of SIM, Wi-Fi, Clients, Repeater, and VPN, and provides quick access to commonly used functions.
	More Settings Tap More on the homepage to access more settings.

1.2 Specifications

Interface	1 x 2.5G WAN/LAN Ethernet Port 1 x 2.8” Color LCD Touchscreen 2 x Nano SIM Card Slots 1 x Onboard eSIM Chipset 1 x USB Type-C (Power only; power input & output) 1 x USB Type-C (10Gbps; power input & output, USB OTG) 2 x TS-9 Ports 1 x Power Button 1 x Reset Button
5G Platform	Qualcomm Dragonwing MBB Gen 3 (X72)
CPU	Qualcomm, Quad-core @2.2GHz
Memory / Storage	LPDDR4X 2GB / 8GB eMMC
Wi-Fi Speed	688Mbps (2.4GHz), 2882Mbps (5GHz), 5764Mbps (6GHz)
Antennas	8 x Internal Antennas (6 x cellular antennas, 2 x 2.4GHz & 5GHz & 6GHz Wi-Fi antennas)
Ethernet Speed	100/1000/2500Mbps
eSIM	1 x Onboard eSIM
Built-in Battery	3.85V/5380mAh/20.72Wh
Power Input	USB PD/PPS 5-12V, 30W Max.
Power Consumption	<30W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Dimension / Weight	157 x 75 x 22.8mm / 300g
Other Tools	Datasheet / Firmware / App / Unboxing / Tutorials

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

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

1.3 Frequency Bands

	GL-E5800NA	GL-E5800EU
5G NR Connectivity	3GPP Rel-17 NSA/SA operation, Sub-6GHz	
5G NR NSA	n2 / n5 / n7 / n12 / n14 / n25 / n26 / n30 / n38 / n41 / n48 / n66 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
5G NR SA	n2 / n5 / n7 / n12 / n13 / n14 / n25 / n26 / n29 / n30 / n38 / n41 / n48 / n66 / n70 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
LTE Category	Cat 20 (DL) / Cat 18 (UL)	
LTE-FDD	B2 / B4 / B5 / B7 / B12 / B13 / B14 / B17 / B25 / B26 / B29 / B30 / B66 / B71	B1 / B3 / B5 / B7 / B8 / B20 / B28 / B32
LTE-TDD	B38 / B41 / B42 / B43 / B48	B38 / B40 / B41 / B42 / B43
WCDMA		B1 / B5 / B8

1.4 Package Contents

The package includes:

- 1 x Mudi 7 (GL-E5800)
- 1 x Quick Start Guide
- 1 x Battery Pack
- 1 x 10Gbps USB-C Cable
- 1 x Travel Pouch

Chapter 2

Router Initialization

This chapter describes how to finish router initialization and connect your devices.

Follow the steps below to complete router initialization and connect your devices.

1. **Power up**

   Press and hold the Power button for **3 seconds**, or plug in a power adapter. Mudi 7 will start up automatically.

2. **System initialization**

   Follow the on-screen instructions to configure basic settings, including screen passcode, admin password, Wi-Fi name, Wi-Fi password and frequency bands.

   Tip: The default admin password is the last 9 characters of the device's S/N, followed by a # character. You may use the default password or set a custom one.

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

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

   - **Wi-Fi**: On your device, go to Settings -> WLAN, locate the Mudi 7’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 Mudi 7’s screen. Alternatively, scan the QR code on the screen, then click "Join" to connect.
   - **Ethernet**: Connect your device to the Mudi 7’s Ethernet port (defaults to LAN) via an Ethernet cable.
   - **USB**: Connect your device to the USB-C port of Mudi 7 via a USB cable. The USB-C port is OTG-enabled, allowing you to access the Mudi 7 in the next step.

4. **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

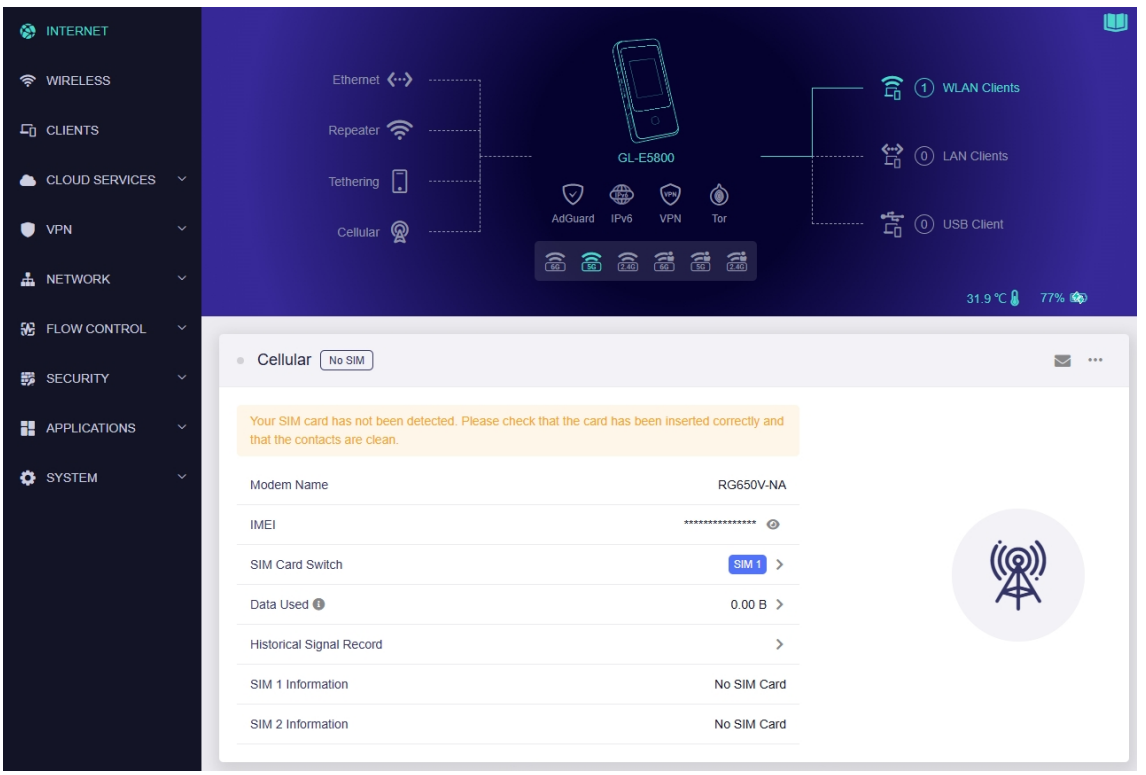
This chapter guides you to log in to your router via web admin panel.

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 your admin password. A strong password is recommended for security. Then click **Next** to continue. If you have already set an admin password, log in directly.
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.

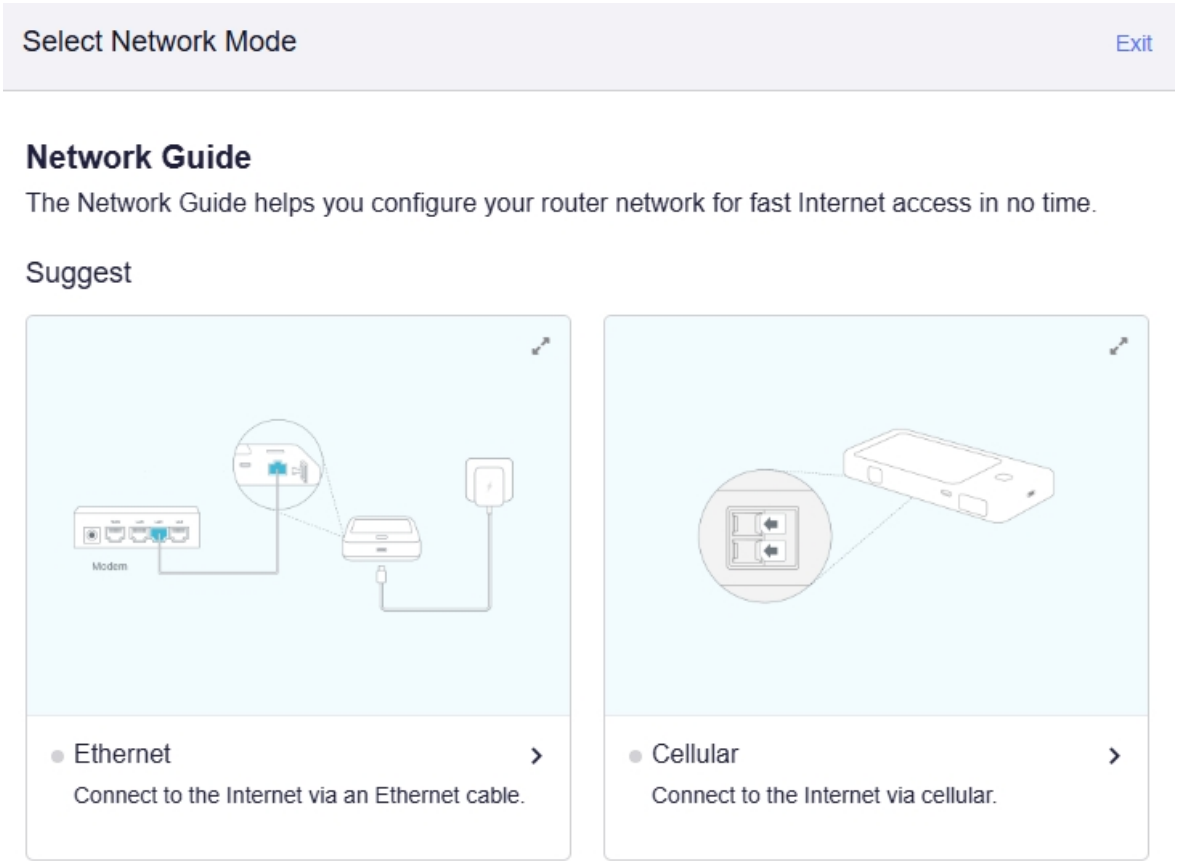
4.1 Quick Setup Wizard

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.



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.

Mudi 7 supports four internet connection methods: Ethernet, Repeater, USB Tethering, and Cellular. Choose the appropriate method based on your usage needs.

1. **Cellular**: Insert a SIM card into the router or enable the onboard eSIM. The router will then connect to the internet via a 4G or 5G cellular network, depending on your carrier's network and supported frequency bands. This method offers great flexibility and is ideal for scenarios such as in-vehicle use or outdoor activities.

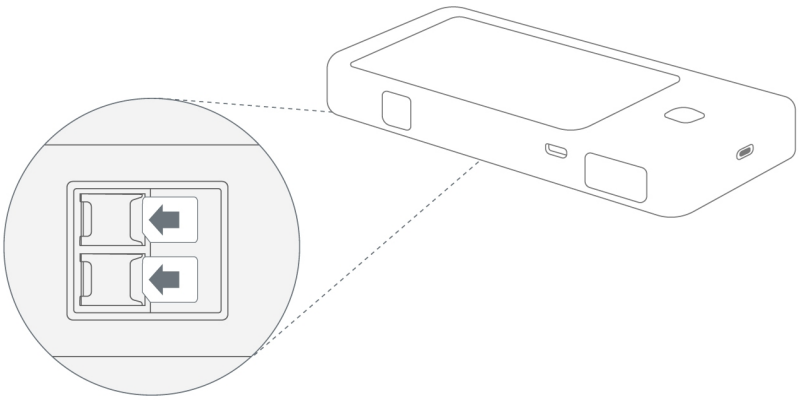
2. **Ethernet**: Connect the router to a broadband network using an Ethernet cable plugged into the WAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.
   In addition, Mudi 7 is equipped with an OTG-enabled USB-C port, allowing you to add a second Ethernet port for Dual-Ethernet WAN. This requires a separately sold USB-C to Ethernet adapter.

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

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

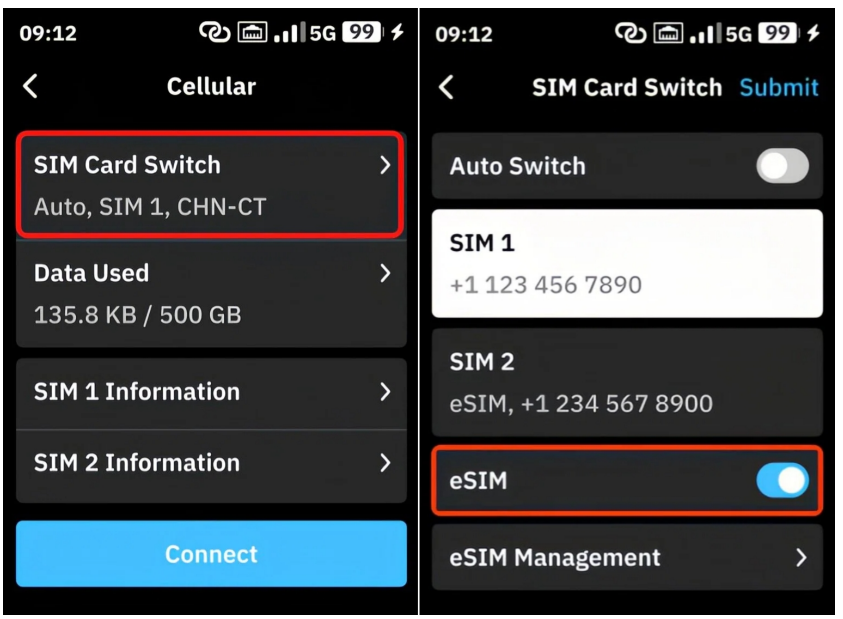
4.2.1 Connect to the Internet via Cellular

Mudi 7 comes with a built-in eSIM and dual Nano-SIM slots. You can connect to the Internet by purchasing an eSIM package (no physical SIM card required), or insert your Nano-SIM cards to access the 5G mobile network.

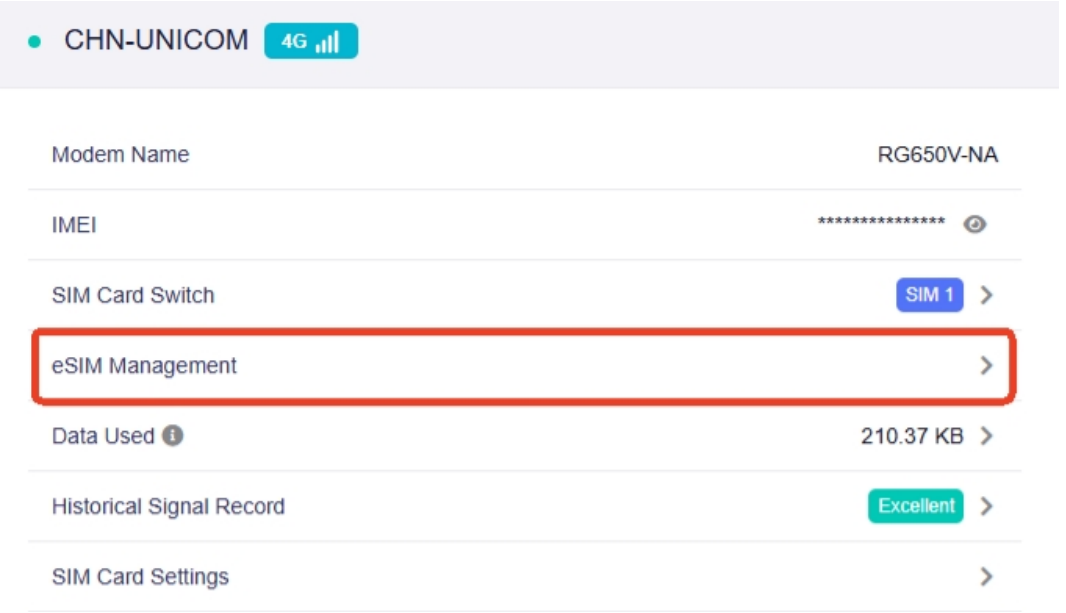


Set up eSIM

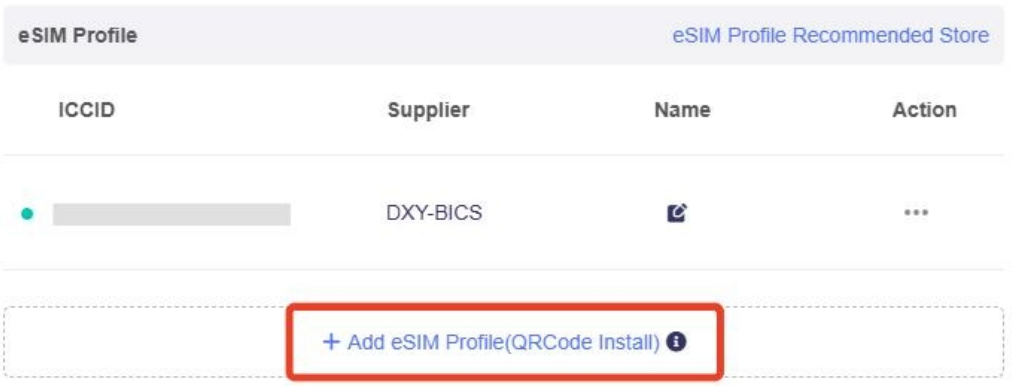
1. On the touchscreen, go to **Cellular** > **SIM Card Switch**, toggle the switch to enable eSIM.



2. Log in to the router's web admin panel and go to **INTERNET** > **Cellular** > **eSIM Management**.

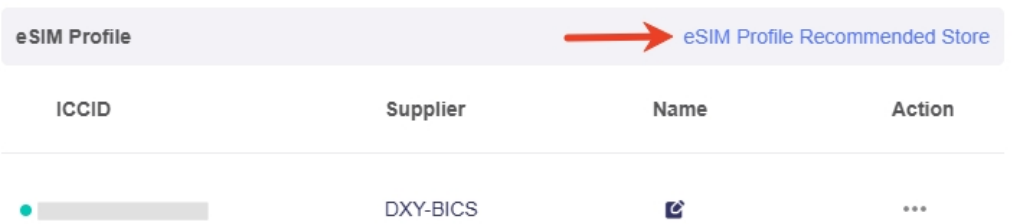


3. In the pop-up window, click **Add eSIM Profile** at the bottom.

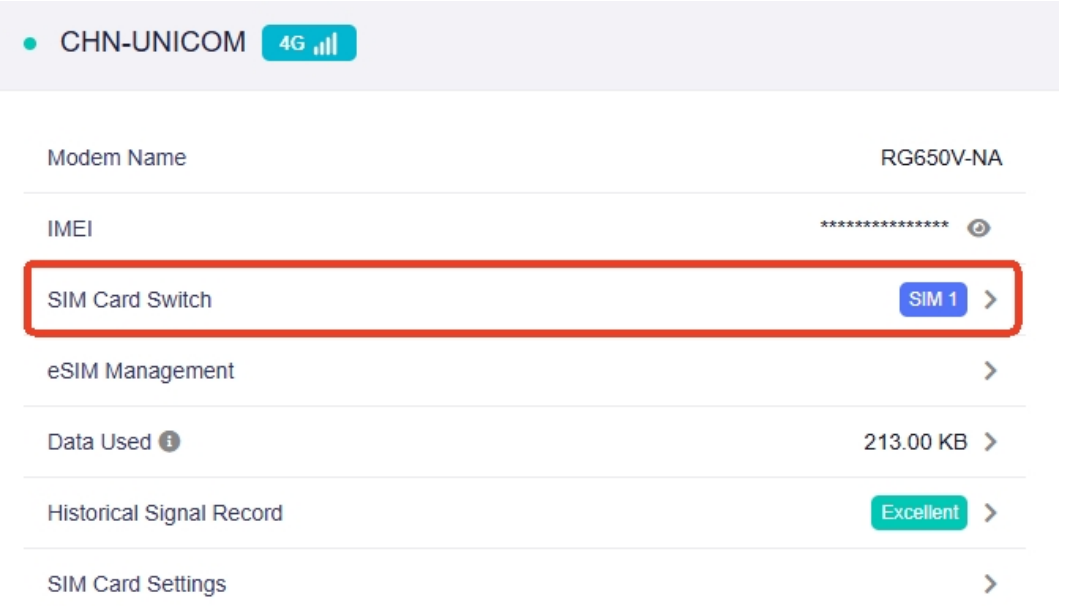


Upload your eSIM profile via a QR code or activation code, and click **Install**. Note that most eSIM profiles can only be downloaded and added once.

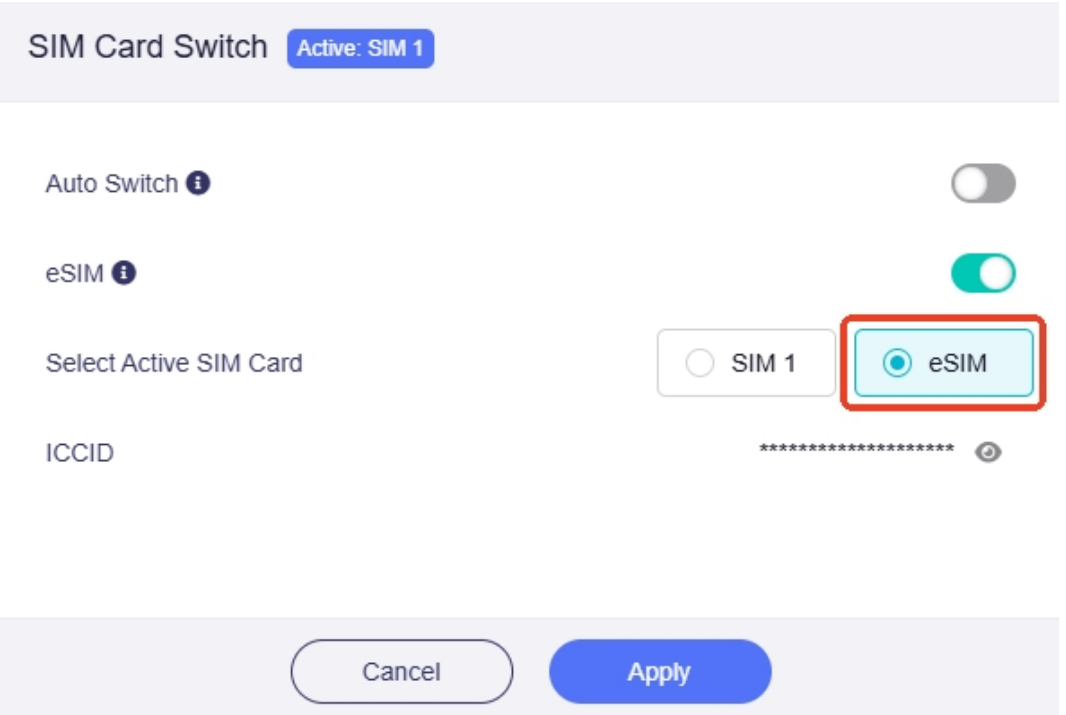
Tip: If you haven't purchased any eSIM profile, you may purchase one in the **eSIM Profile Recommended Store**.



4. Once uploaded, go to **Cellular** and click **SIM Card Switch**.



In the pop-up window, select **eSIM** as the active SIM card, then click **Apply**.



5. The router will start connecting via this eSIM profile. Please wait and check if the connection is successful.

Set up Nano-SIM

1. Use the small notch at the bottom-right corner of the device's back cover as a leverage point. Pry along the seam to create a gap, then open the back cover and remove the Mudi 7 battery.
2. Insert the Nano-SIM card(s). If using only one card, prioritize SIM 1. Then put the battery and the cover back.
3. The router will start connecting automatically the Nano-SIM card. Please wait and check if the connection is successful. Once successfully connected, the signal bars and cellular status will appear in the top right corner of the touchscreen. You can also check the connection details in the web admin panel.

Note:

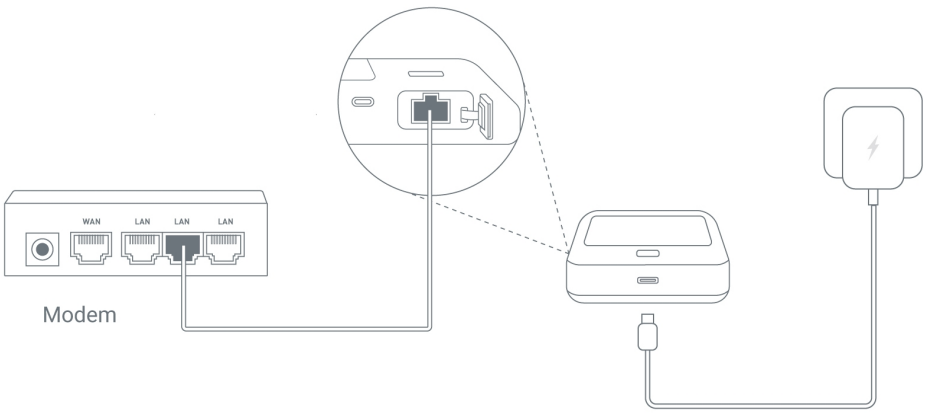
1. The built-in eSIM and SIM 2 are mutually exclusive and cannot be activated at the same time. The eSIM is disabled by default. If you enable the eSIM, SIM 2 will not work even if a SIM card is inserted.
2. Since Mudi 7 comes with a built-in eSIM, a SIMPoYo eSIM physical card will be recognized as a regular SIM card without eSIM functionality on Mudi 7.

4.2.2 Connect to the Internet via Ethernet Cable

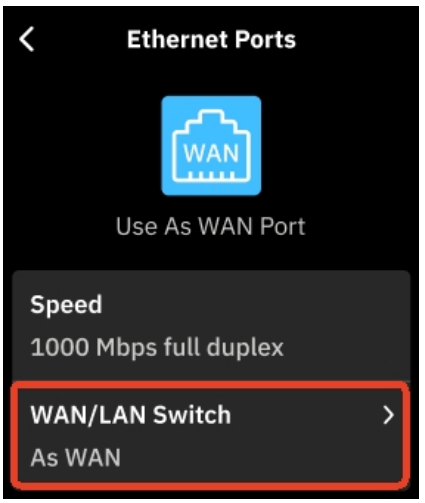
Connect the router to a broadband network using an Ethernet cable. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.

Basic Setup

1. Connect the Mudi 7's Ethernet port to the upstream device (e.g., an ISP modem, primary router, network switch or an Ethernet jack) via an Ethernet cable.



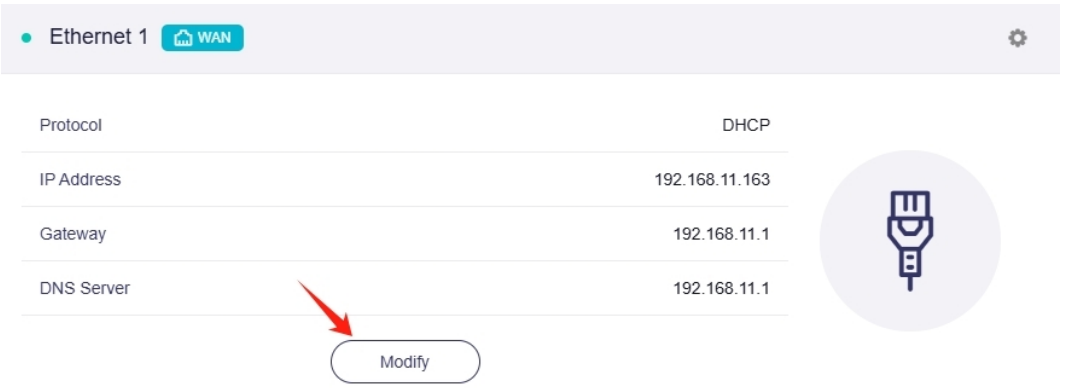
2. On the touchscreen or web admin panel, go to **Network** > **Ethernet Ports**, set the port role to **WAN**, and click **Apply**.



3. The router will start connecting automatically. Once successfully connected, an Ethernet port icon will appear in the top right corner of the touchscreen. You can also check the connection details and configure advanced settings in the web admin panel.

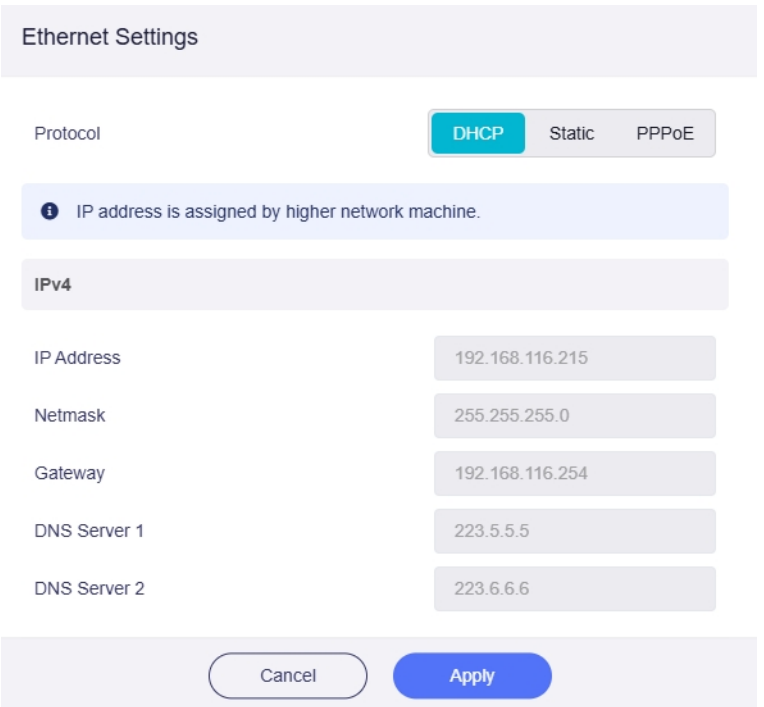
Protocol

There are three types of protocols for Ethernet connection: DHCP, Static and PPPoE. Click **Modify** to change if needed.



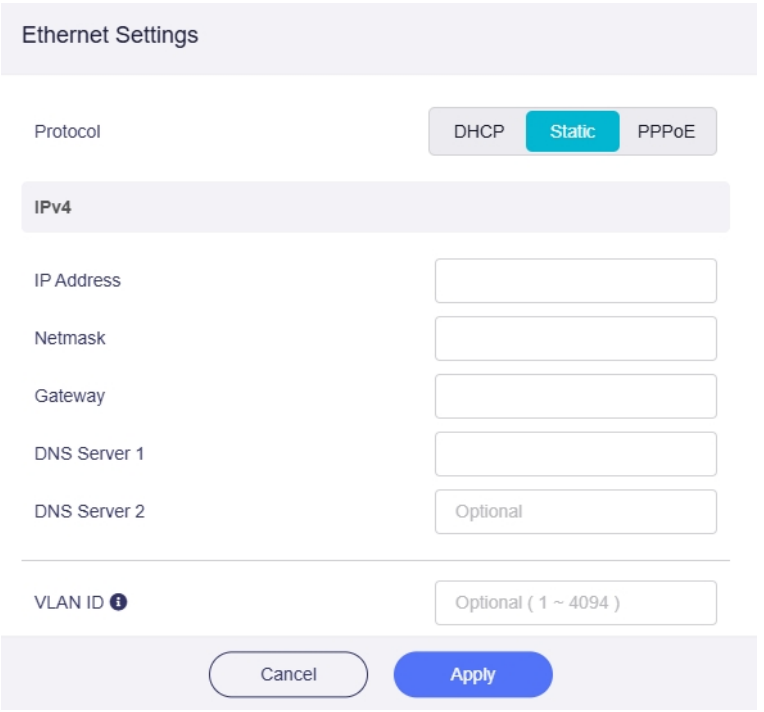
- **DHCP**

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



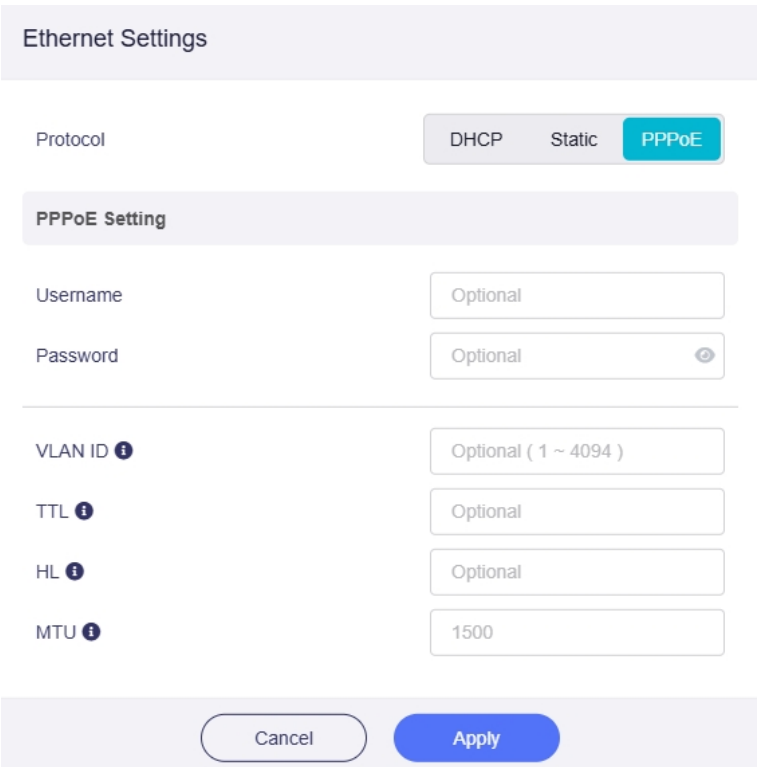
- **Static**

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



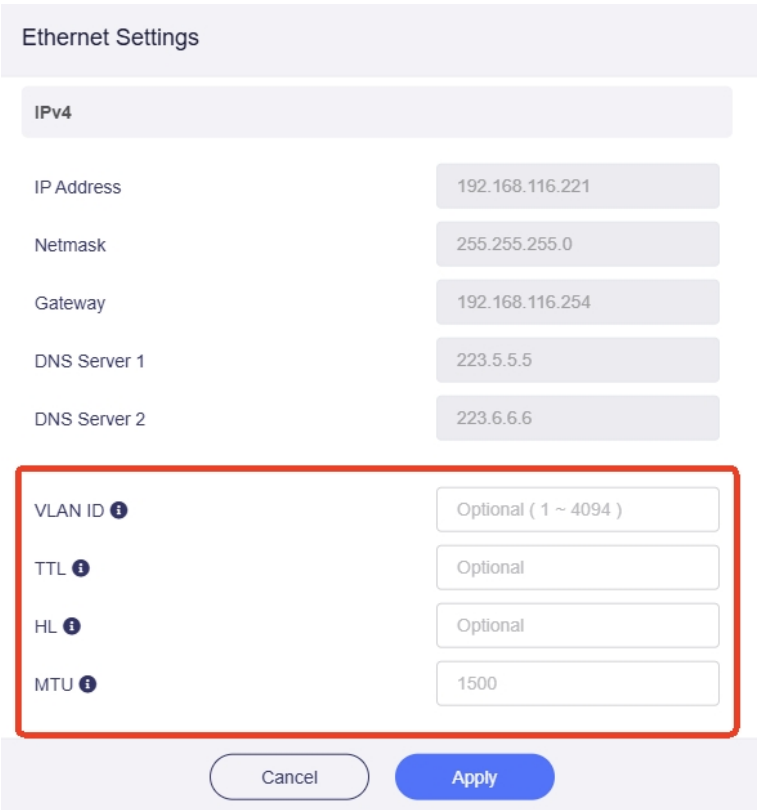
- **PPPoE**

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



Advanced Settings

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



- **VLAN ID**

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

- **TTL**

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

- **HL**

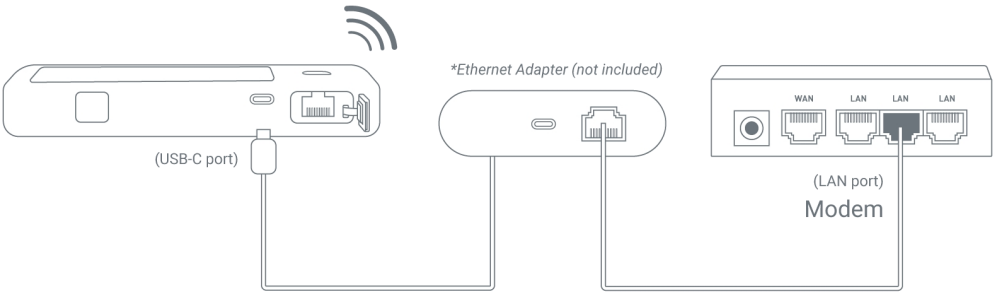
  In IPv6, the HL (Hop Limit) field limits the number of transmission hops for data packets in the network, serving as the equivalent of TTL in IPv4.

- **MTU**

  The default MTU value is 1500 bytes.

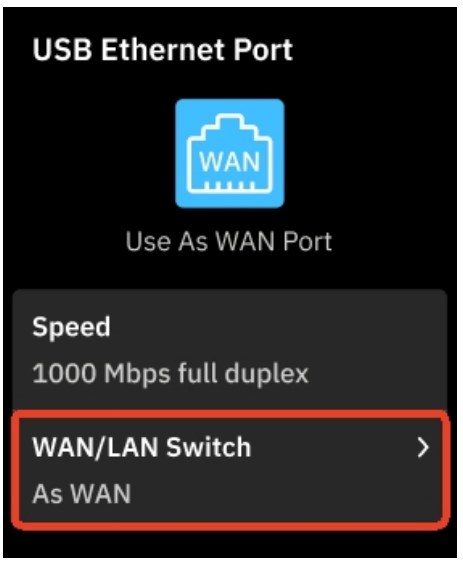
USB Ethernet

Mudi 7 is equipped with an **OTG-enabled** USB-C port, allowing you to add a second Ethernet port for Dual-Ethernet WAN. **This requires a separately sold USB-C to Ethernet adapter**.



Follow the steps below to connect your router to the internet via USB Ethernet.

1. Connect an upstream network source (e.g., ISP modem, network switch, or Ethernet jack on the wall) to Mudi 7's USB-C port via a USB-C to Ethernet adapter.
2. On the touchscreen or web admin panel, go to **Network** > **Ethernet Ports** > **USB Ethernet Port**, set the port role to **WAN**, and click **Apply**.



3. Mudi 7 will then automatically connect to your device. If it does not connect, repeat the above steps, or log in to the web admin panel to check the USB Ethernet connection.
4. Once successfully connected to the internet, a USB icon and an Ethernet port icon will appear in the top right corner of the touchscreen. You can also check the connection details in the web admin panel.

4.2.3 Connect to the Internet via an Existing Wi-Fi

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

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

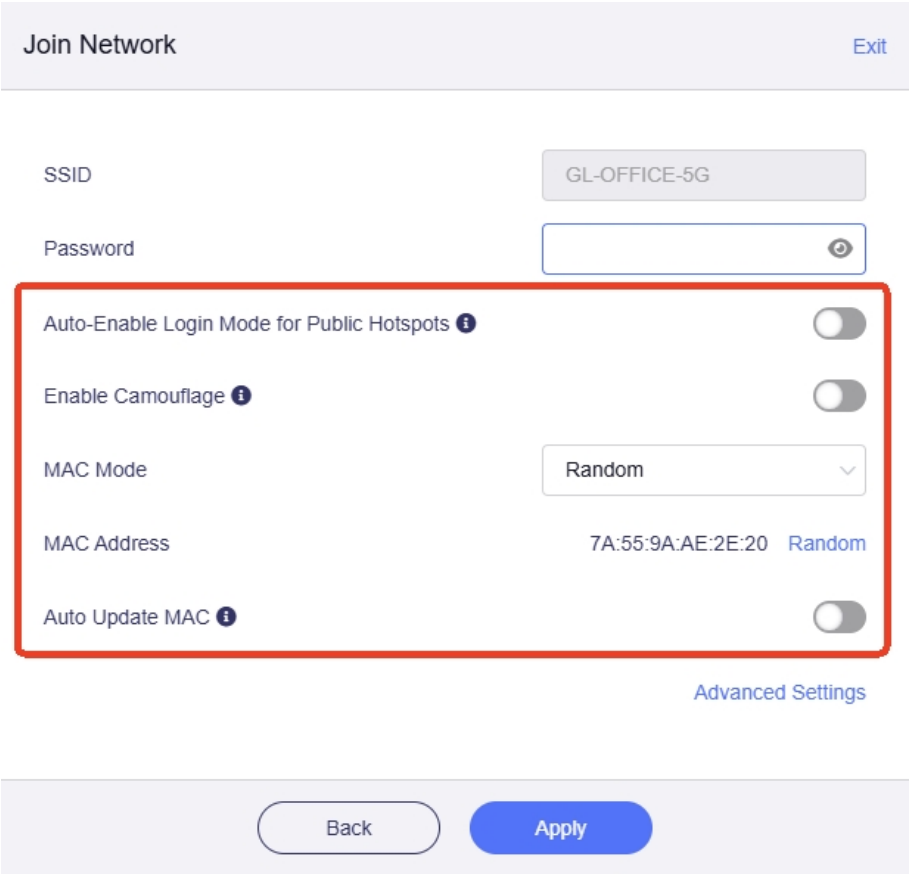
Basic Setup

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

1. On the touchscreen or web admin panel, go to **Internet** > **Repeater** and click **Connect**. Mudi 7 will start scanning for available Wi-Fi networks.
2. Select the Wi-Fi network you want Mudi 7 to extend.
3. Enter the password and click **Apply**.
4. Once successfully connected, a Wi-Fi icon will appear in the top right corner of the touchscreen. You can also check the connection details and configure advanced settings in the web admin panel.

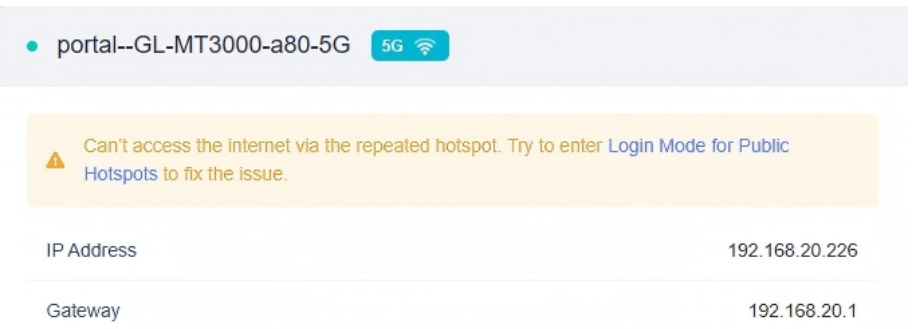
Public Hotspot Settings

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



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

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



- **Enable Camouflage**

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

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

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

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

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

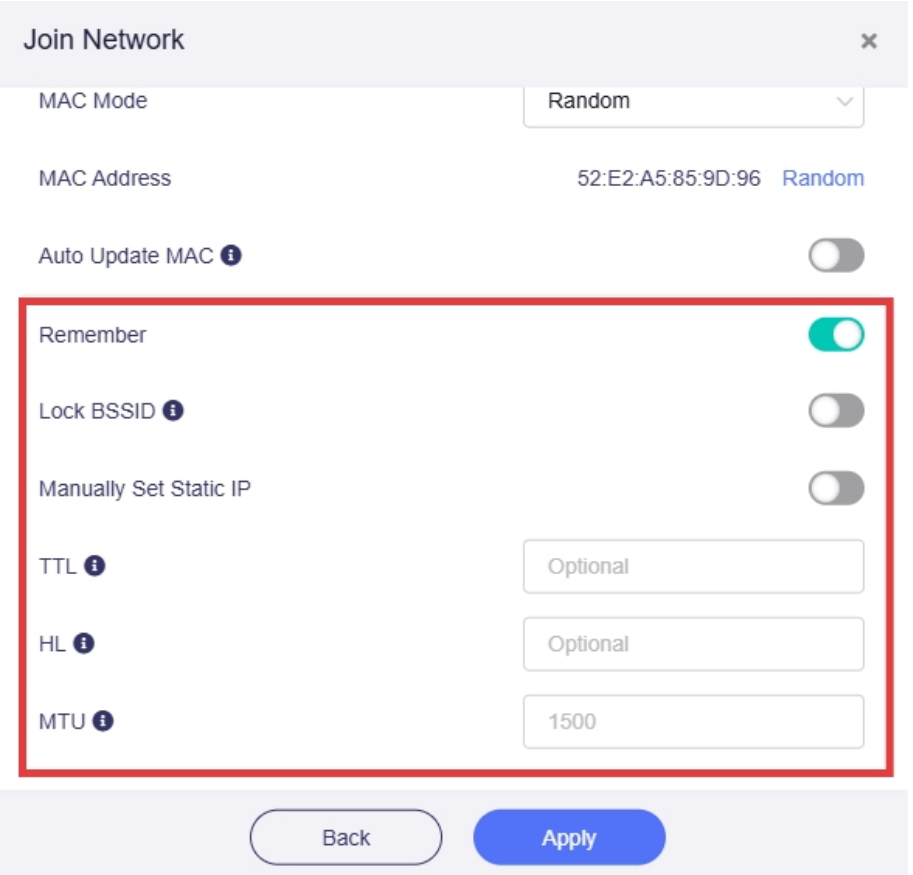
  Random: Automatically generates a random MAC address for connection.
- **Auto Update MAC**

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

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

Advanced Settings

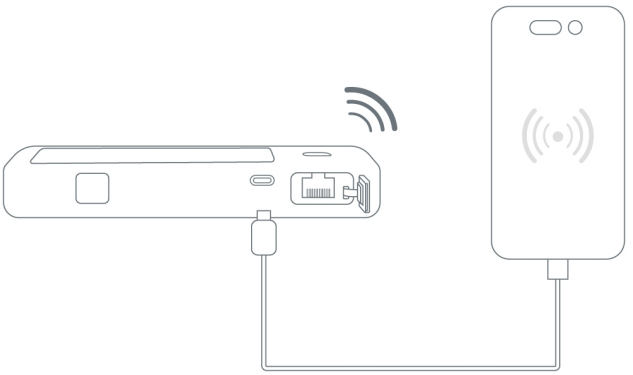
When joining the network, there are some optional advanced settings.



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

4.2.4 Connect to the Internet via USB Tethering

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



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

Basic Setup

1. Connect your mobile device (e.g., smartphone or USB dongle) to Mudi 7's USB-C port via a USB cable.
2. On your mobile device, go to Settings and enable **USB Tethering**. If you use iPhone, tap **Trust This Device** if prompted.
3. Mudi 7 will then automatically connect to your device. If it does not connect, repeat the above steps, or log in to the web admin panel to check the Tethering connection.
4. Once successfully connected, a chain link icon will appear in the top right corner of the touchscreen. You can also check the connection details in the web admin panel.

Troubleshooting

If the Tethering connection fails, try these troubleshooting steps:

- Use the original power supply for the router.
- Unplug and re-plug the USB cable.

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

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

Chapter 5

Wireless

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

5.1 Wi-Fi Status Display

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

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

Note:

1. Due to hardware limitations, the 5GHz and 6GHz Wi-Fi on Mudi 7 cannot be enabled simultaneously. 5GHz Wi-Fi is enabled by default for broader compatibility.
2. When Mudi 7 connects to an upstream Wi-Fi network as a repeater, the band used by the upstream Wi-Fi will be disabled on Mudi 7.
3. When Mudi 7 connects to an upstream Wi-Fi network as a repeater, the Guest Wi-Fi is unavailable.
4. As required by regulations, Wi-Fi must switch to "Outdoor" mode when Mudi 7 is used outdoors. This may reduce coverage range.

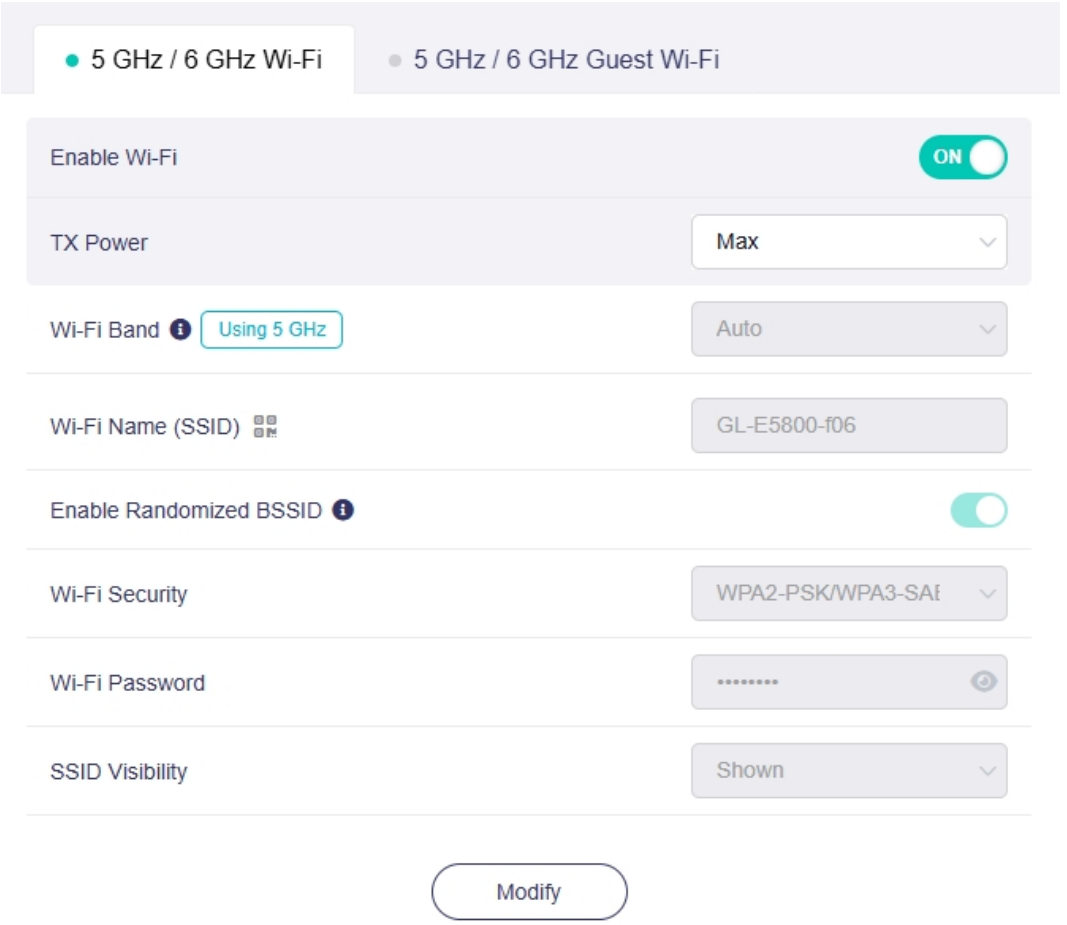
5.2 Wireless Settings

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

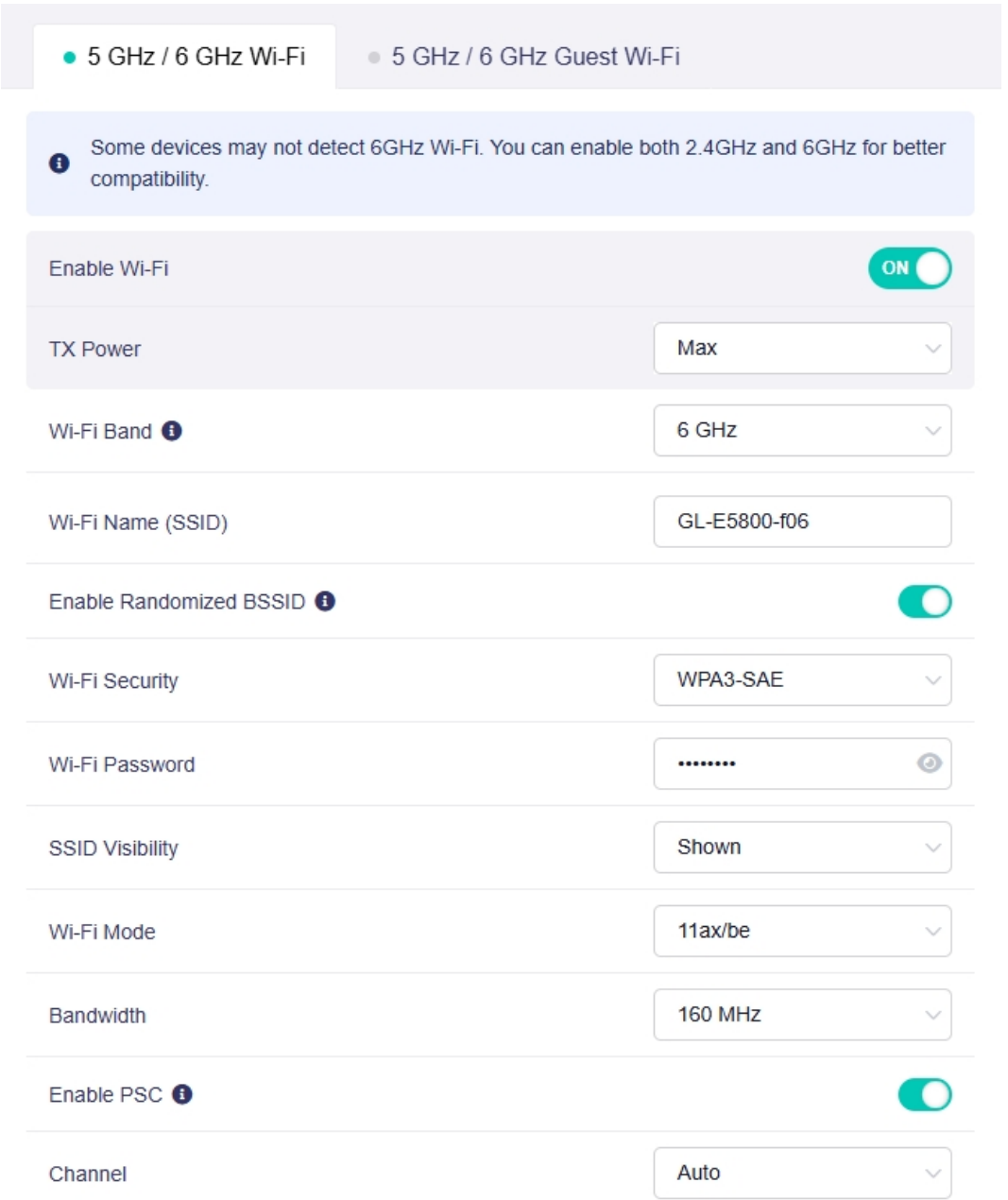
The wireless page displays the router's 2.4GHz, 5GHz, and 6GHz Wi-Fi settings.

5.2.1 5GHz/6GHz Wi-Fi

Due to hardware limitations, the 5 GHz and 6 GHz Wi-Fi bands on Mudi 7 cannot be enabled simultaneously. For simplified setup, these two bands are merged into one unified Wi-Fi network on the Wireless page – the Wi-Fi band is set to **Auto** by default, which dynamically switches between 5 GHz and 6 GHz, with the 5 GHz band prioritized for broader compatibility. This page lets you enable or disable Wi-Fi, adjust TX power, enable or disable randomized BSSID, set Wi-Fi name (SSID), security, password, and SSID visibility. Note that channel and bandwidth can not be manually configured when the Wi-Fi band is set to Auto.



Click **Modify** and switch the Wi-Fi band to 5 GHz only or 6 GHz only if needed. Once the band is fixed, you will be able to customize Wi-Fi channel, bandwidth, and other related parameters, apart from the basic settings.

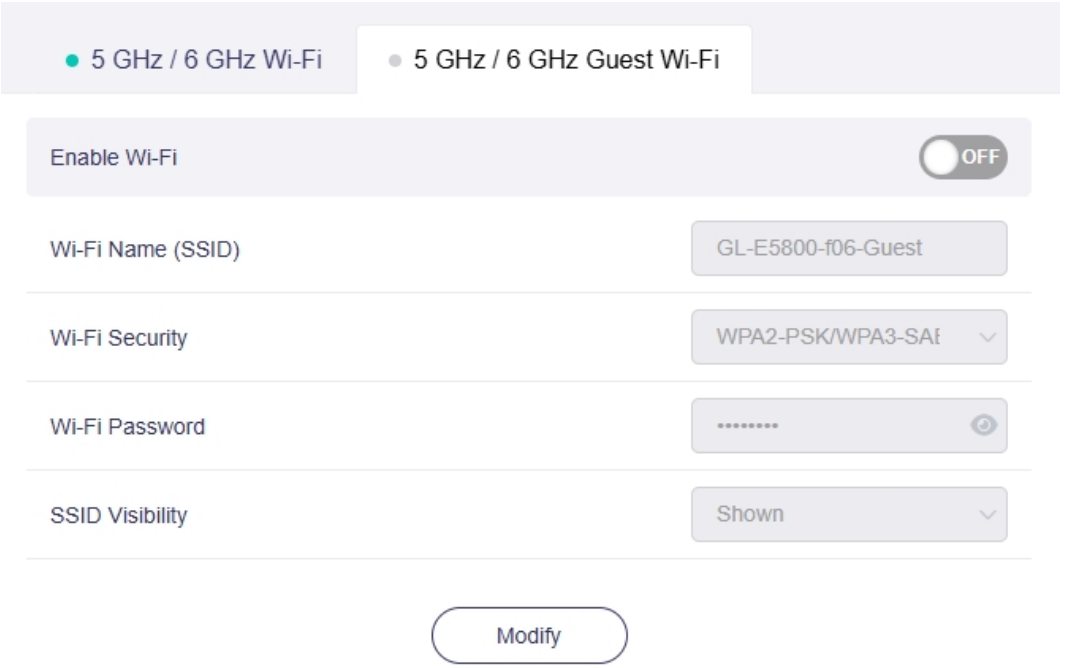


Note:

1. Some devices may not support 6GHz Wi-Fi. You can enable both the 2.4GHz and 6GHz bands for broader compatibility.

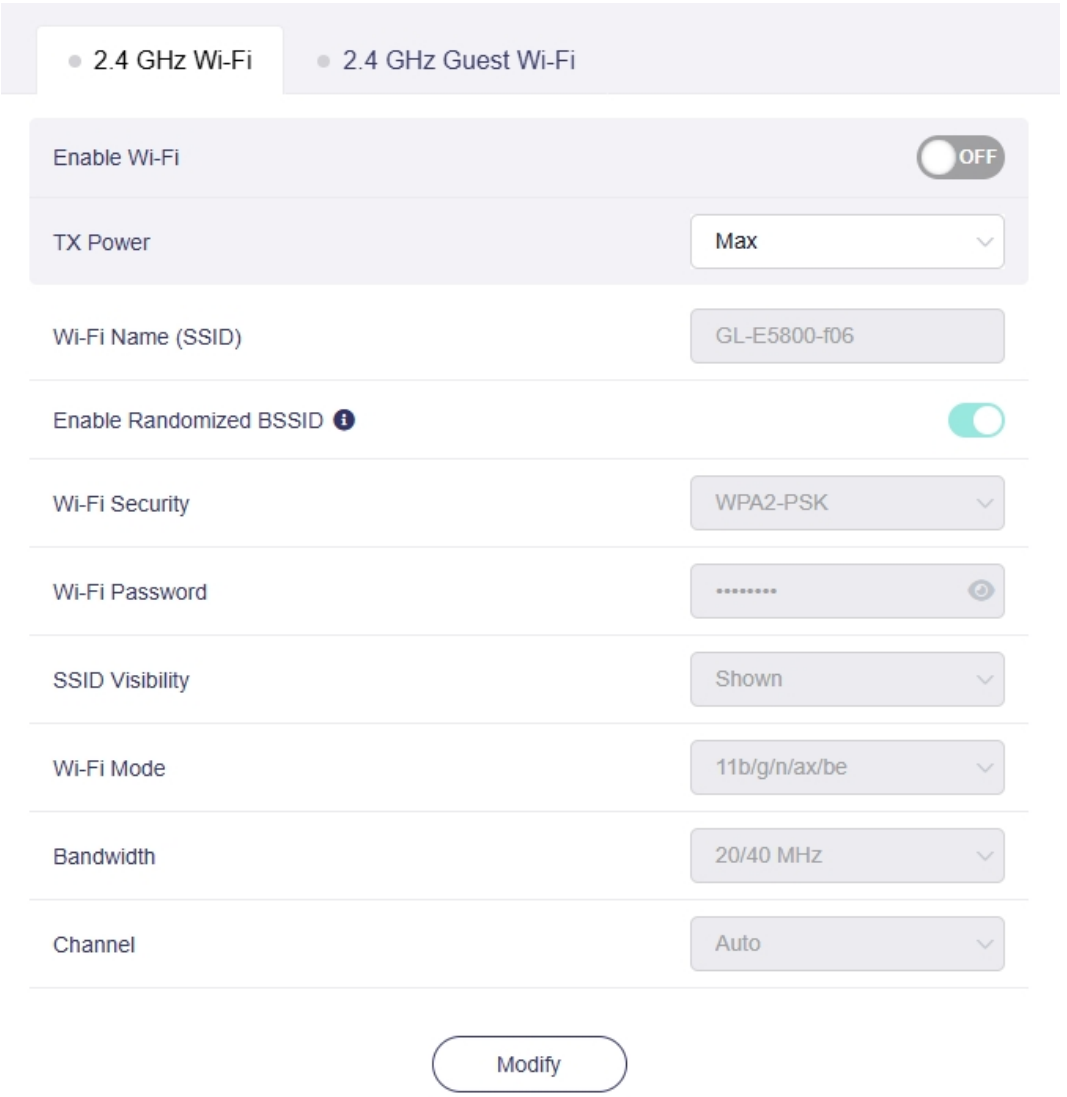
2. **Randomized BSSID** is enabled by default. It aims to prevent the client vendors from collecting nearby Wi-Fi BSSIDs and client devices' GPS coordinates to their servers.
3. The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.
4. When the 5GHz Wi-Fi band is enabled, if the **Bandwidth** is set to **160 MHz**, the Wi-Fi will operate on a DFS channel by default, even if you manually select a non-DFS channel or set the channel to Auto.
5. When the 6GHz Wi-Fi band is enabled, **PSC** (Preferred Scanning Channel) is enabled by default to reserve high-quality channels and guarantee stable connections for 6 GHz devices.

The 5GHz/6GHz Guest Wi-Fi allows you to configure simplified settings, including enabling or disabling Wi-Fi, setting Wi-Fi name (SSID), security, password, and SSID visibility.



5.2.2 2.4GHz Wi-Fi

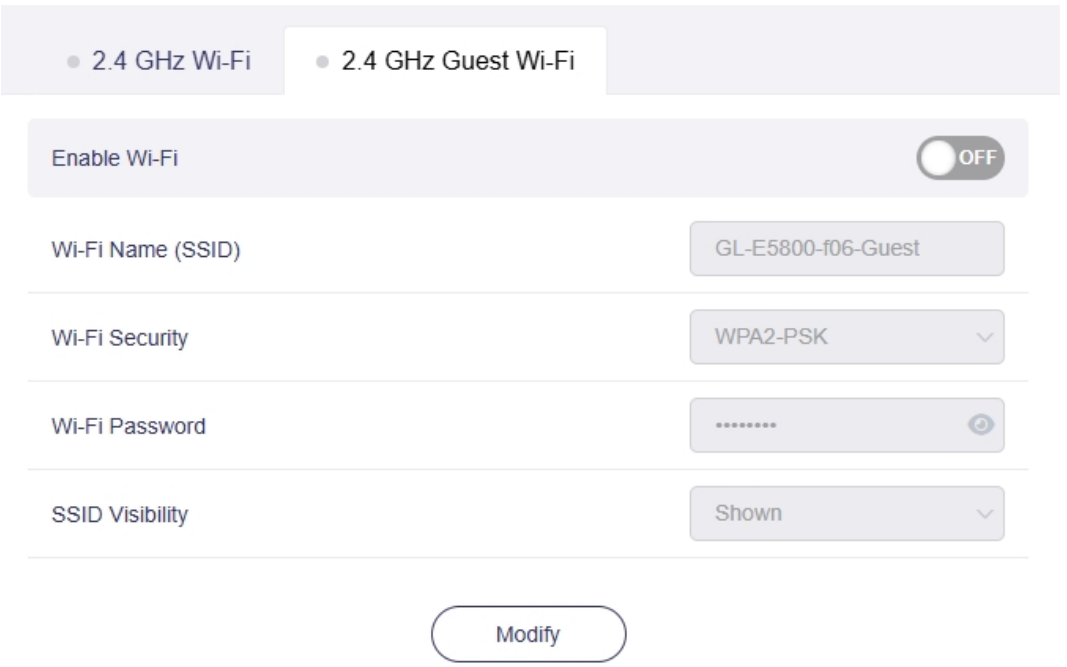
The 2.4GHz Main Wi-Fi allows you to enable or disable Wi-Fi, set TX power, enable or disable randomized BSSID, set Wi-Fi name (SSID), security, password, SSID visibility, Wi-Fi mode (standard), bandwidth, and channel.



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.

The 2.4GHz Guest Wi-Fi allows you to enable or disable Wi-Fi, set Wi-Fi name (SSID), security, password, and SSID visibility.



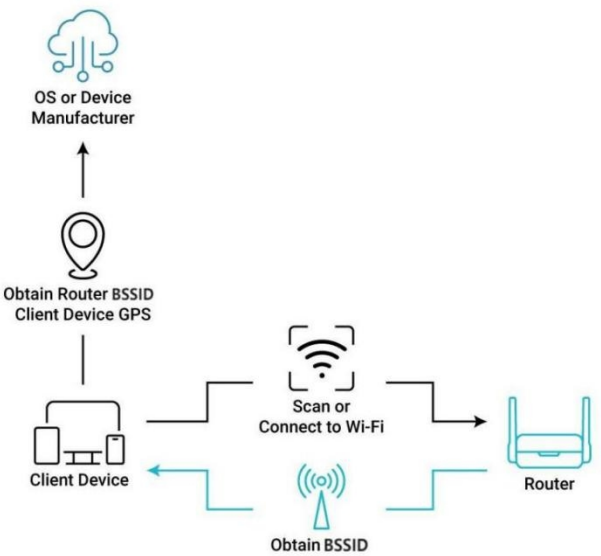
5.2.3 Randomized BSSID

Randomized BSSID feature has been available since firmware v4.6. It 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/6GHz Wi-Fi** or **2.4GHz Wi-Fi**, the Randomized BSSID 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.

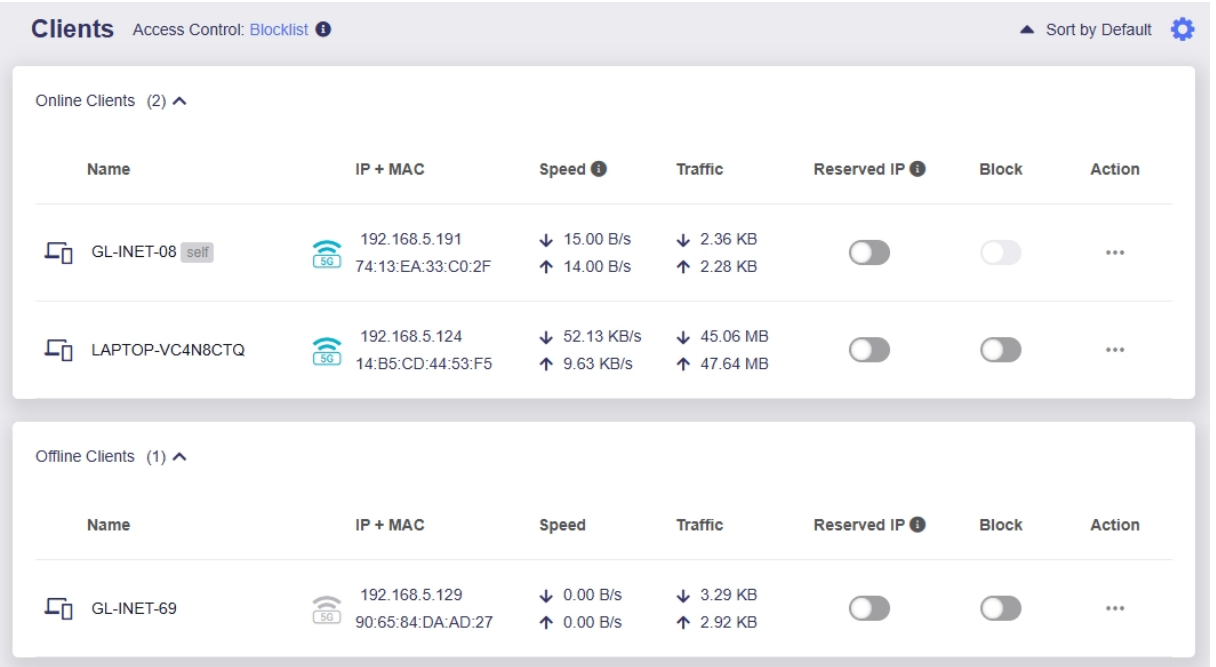
Chapter 6

Clients

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

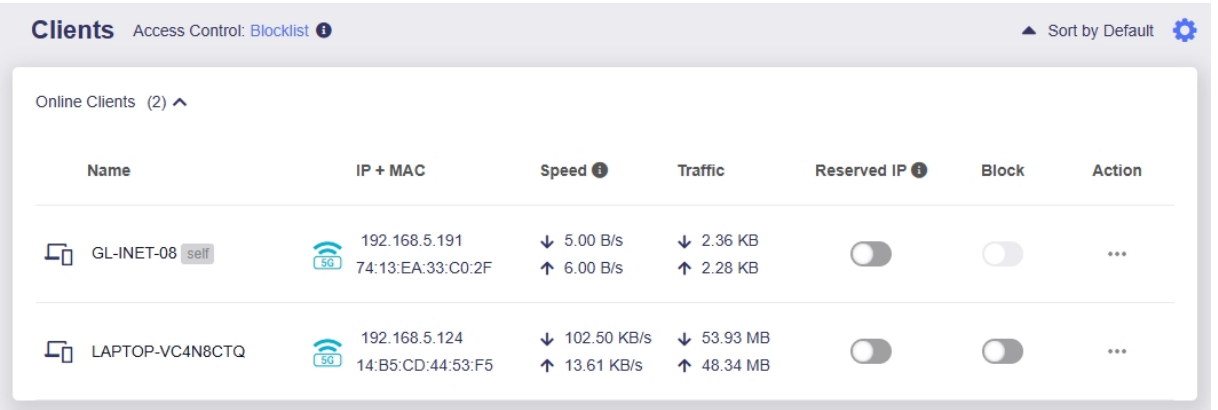
Log in to the router’s web admin panel and navigate to **CLIENTS**.

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



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

6.1 Device Details



1. **Device Name**

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

2. **IP and MAC Address**

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

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

3. **Speed**

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

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

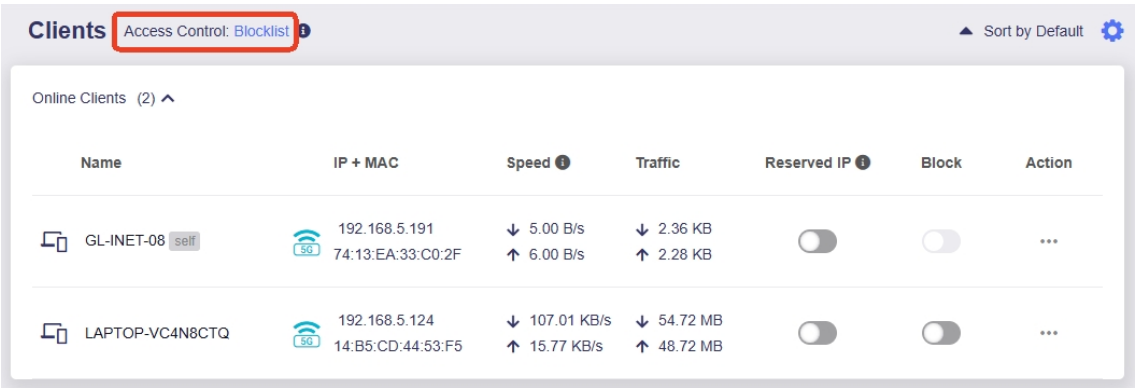
5. **Reserve IP**

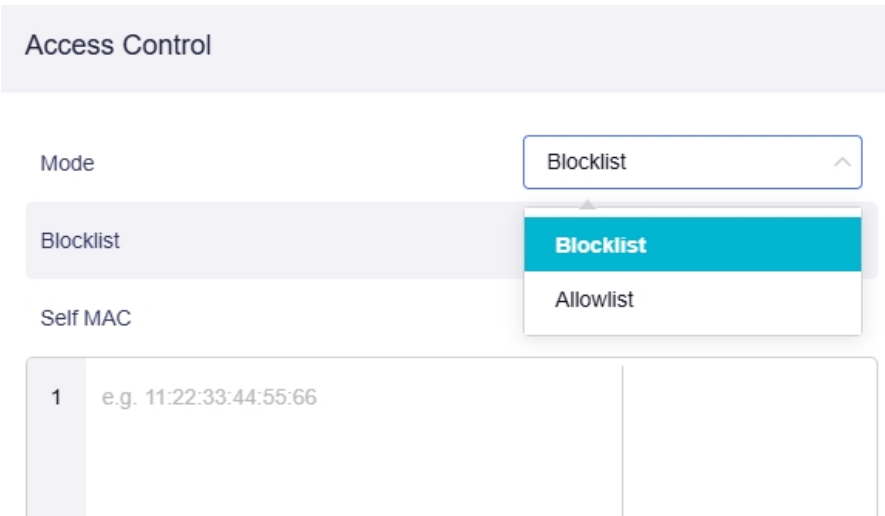
   In the fifth column, you can reserve IP address for connected device with one click. When you specify a reserved IP address for a client within the local area network, it will always receive the same IP address each time it connects to the router.

6. **Blocklist**

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

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



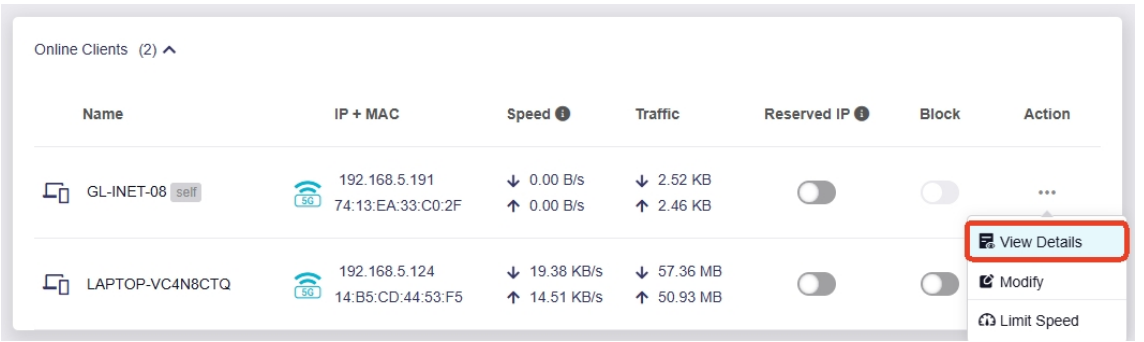


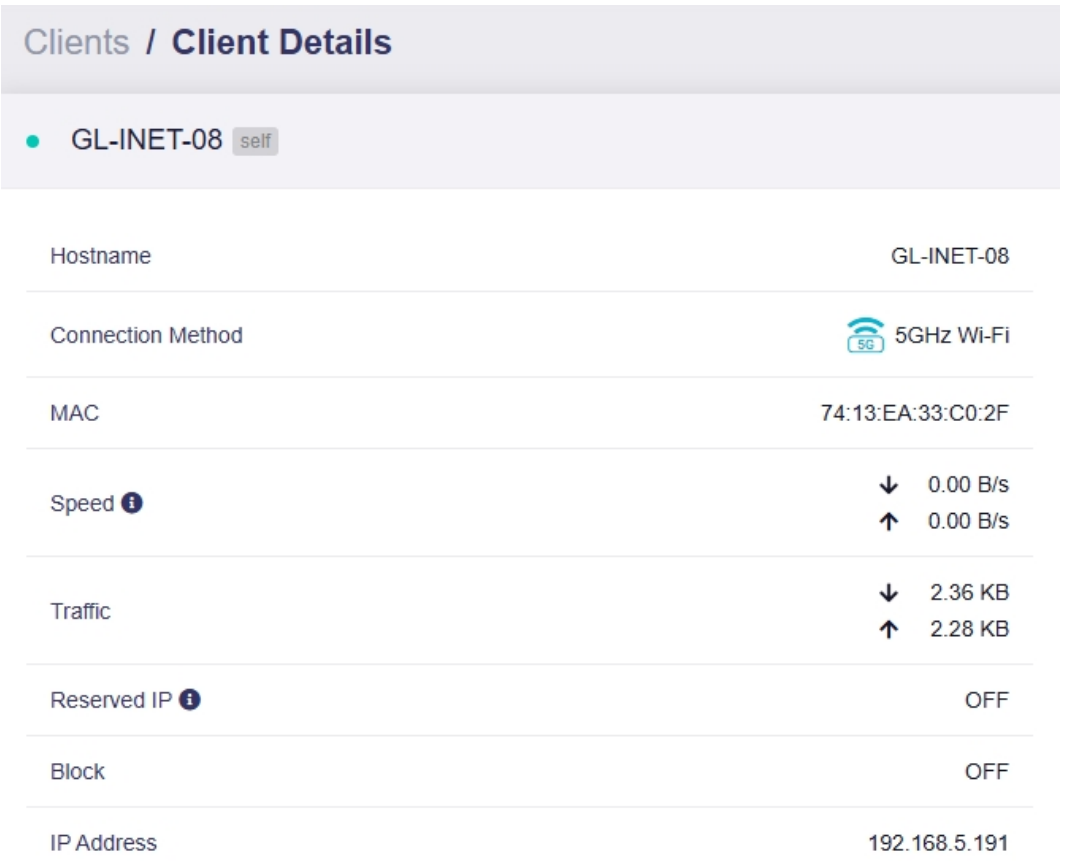
- **Blacklist**: Devices with MAC addresses in the blacklist are not allowed to connect to this router. Please note that blocking client is based on the MAC address of the device. If the blocked device uses different MAC address next time, it can still be able to connect to router.
- **Allowlist**: Only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

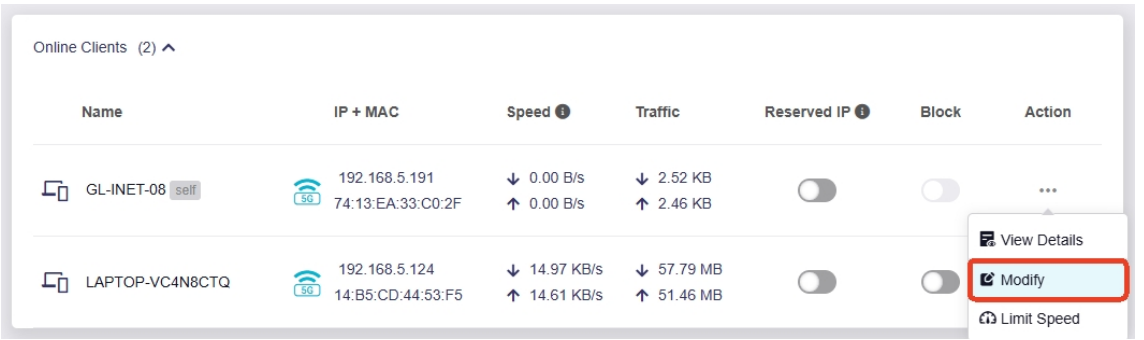
   Click the three-dot icon in the **Action** column, and click **View Details** from the drop-down menu to view the device details on a single page.

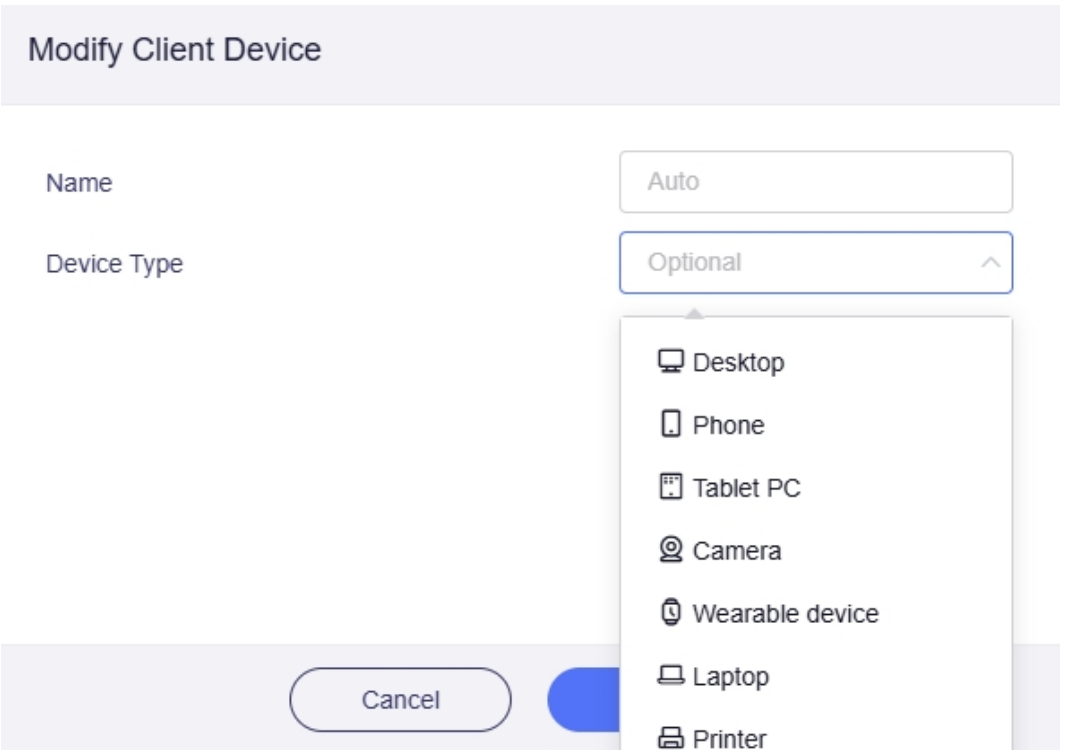




2. **Modify**

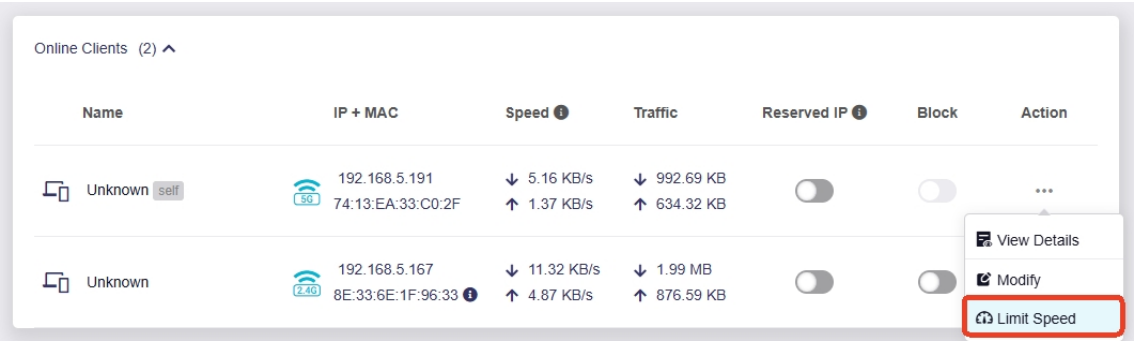
Click the three-dot icon in the **Action** column, and click **Modify** from the drop-down menu to modify the device name and type.



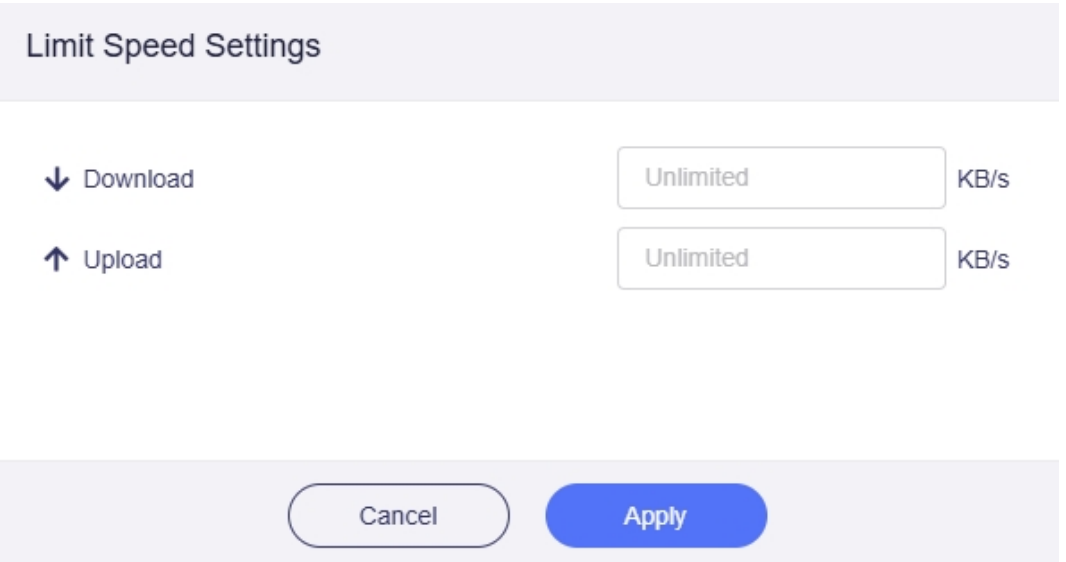


3. **Limit Speed**

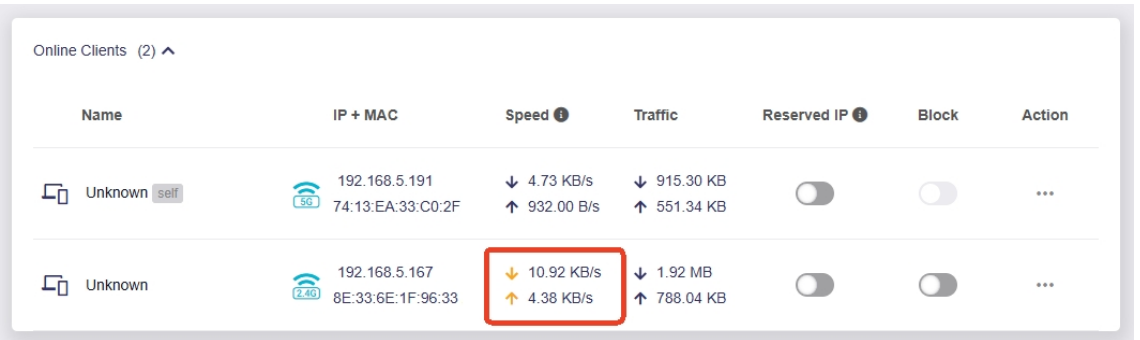
Click the three-dot icon in the **Action** column, and click **Limit Speed** from the drop-down menu.



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



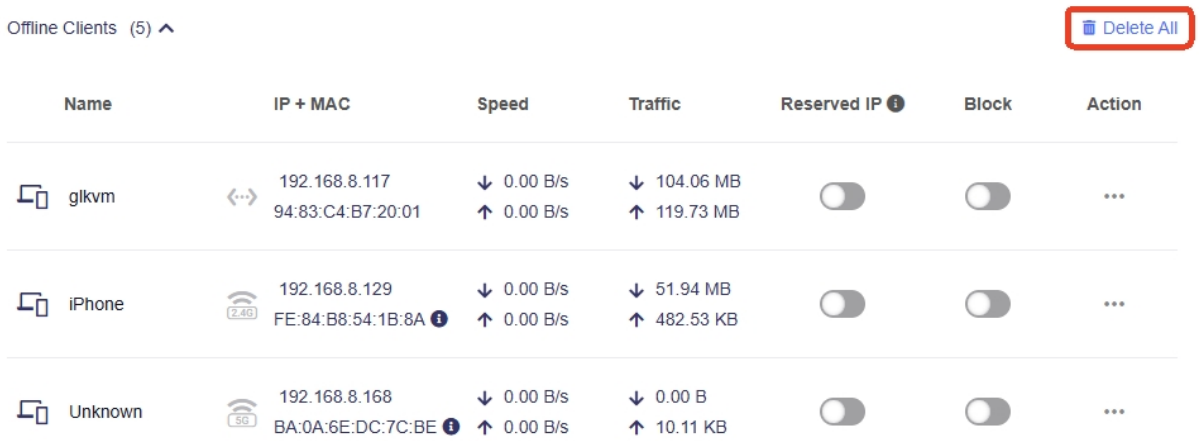
If speed limitation has been applied to a device, the upload/download speed arrows will turn yellow.



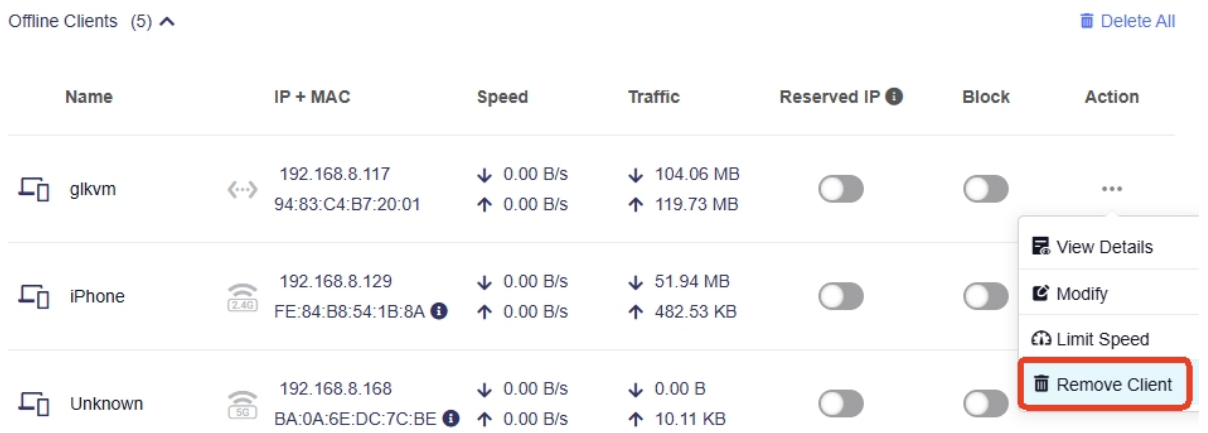
Tip: If the Limit Speed option is not visible, go to **NETWORK** > **Network Acceleration** and disable it. The Limit Speed option will then become available.

6.3 Remove Clients

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

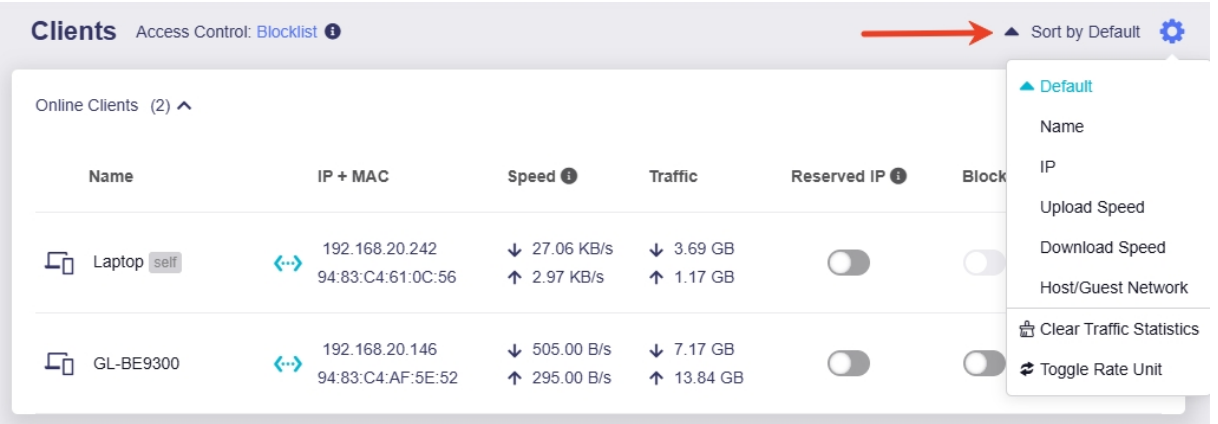


If you want to remove a specific client, click the three-dot icon in the **Action** column, then click **Remove Client** from the drop-down menu.



6.4 Sort

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



The default sorting 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.

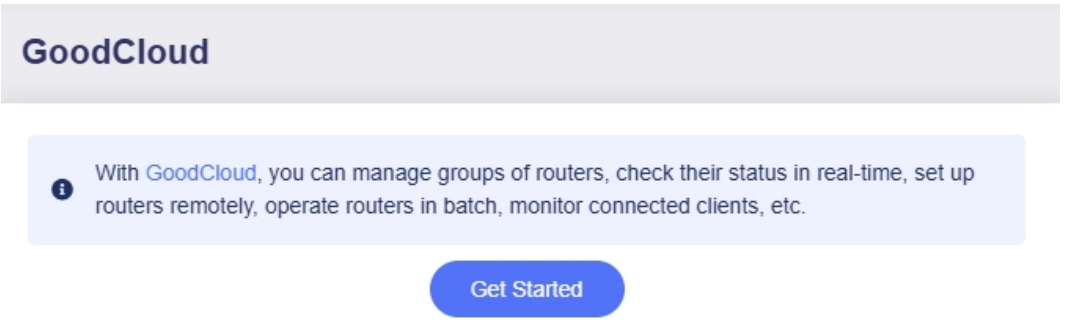
With GoodCloud, you can:

- 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

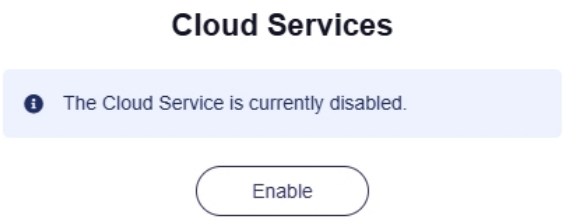
Some features are available in Enterprise Plan and VAR (Value Added Reseller) Plan. See here for details.

7.1.1 Enable GoodCloud

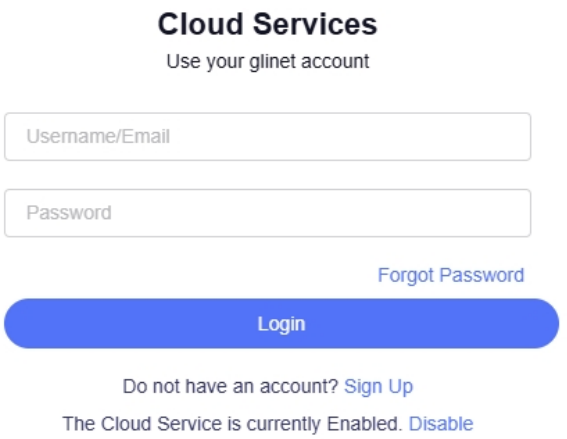
1. Log in to your router's web admin panel, navigate to **CLOUD SERVICE** > **GoodCloud**, and click **Get Started.**



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



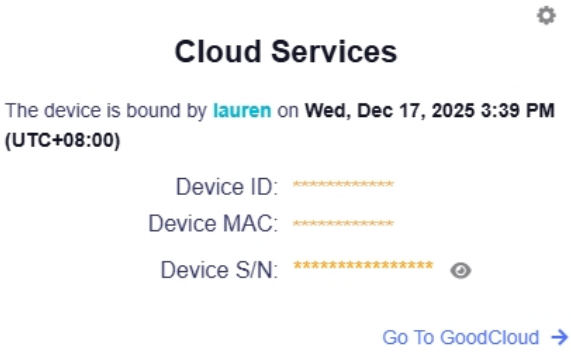
3. Log in with your GL.iNet Cloud account. If you don't have an account, sign up for one and log in. Once logged in, the router will be bound to your account automatically.



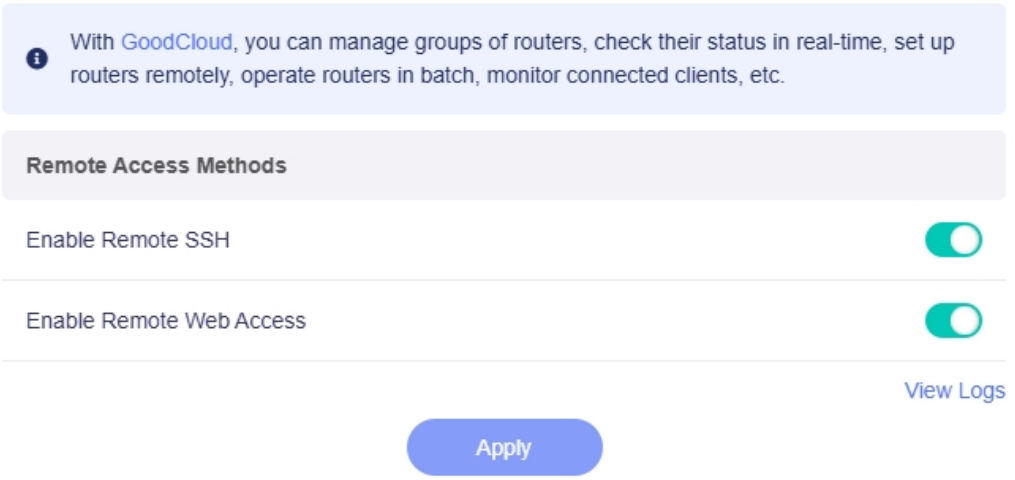
Tips:

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

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



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

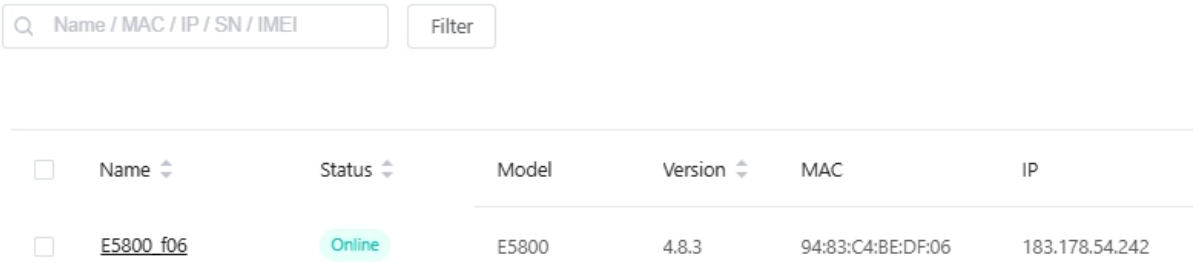


- **Remote SSH**: Remotely access the router's terminal from GoodCloud using SSH.
- **Remote Web Access**: Remotely access to the router's web admin panel from GoodCloud via HTTP/HTTPS.
- **View Logs**: Redirect to the Log page and display Cloud log.

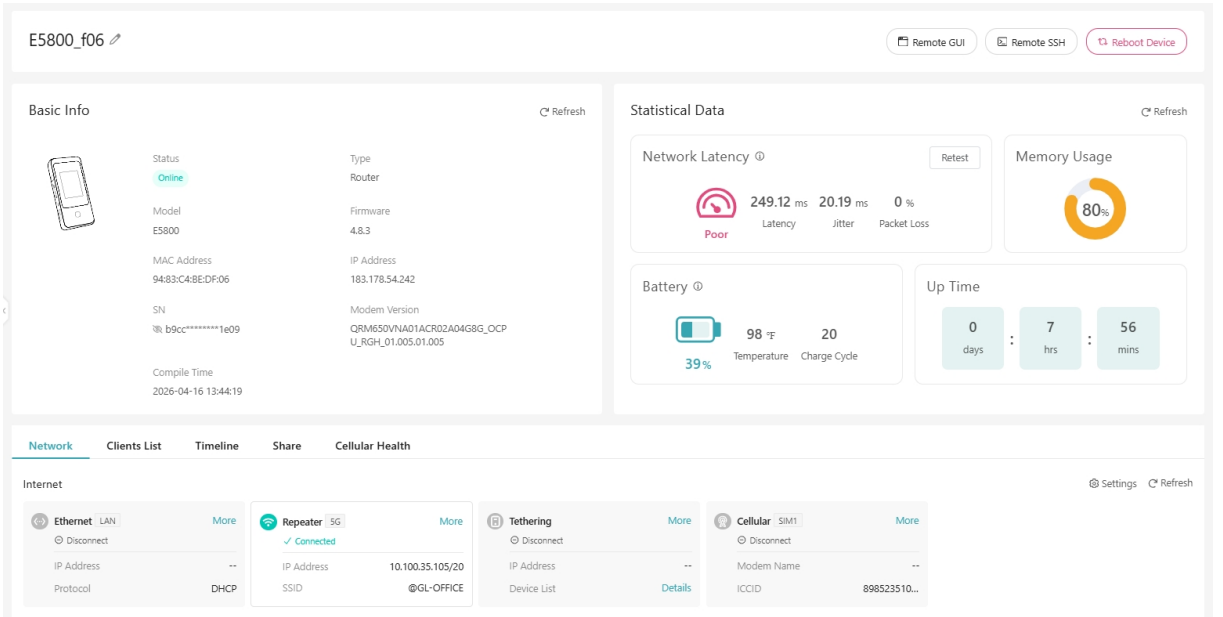
7.1.2 Manage Your Router

Check Device Details

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

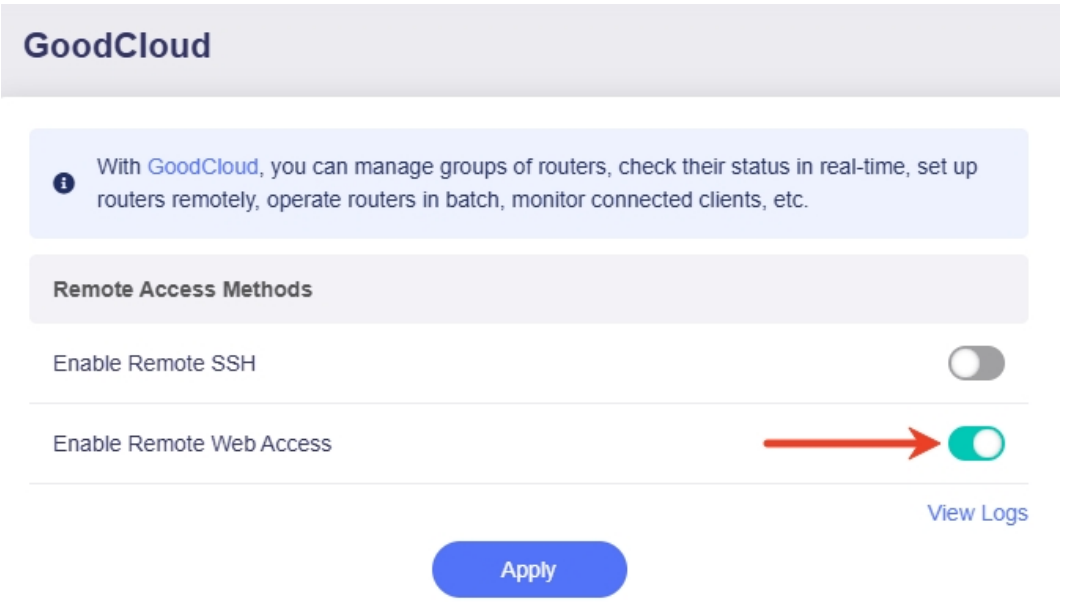


Click the device name to enter the device details page, which displays basic information, statistical data, network overview, client list, and timeline. You can also perform advanced operations, such as remotely accessing the router, and rebooting the device.

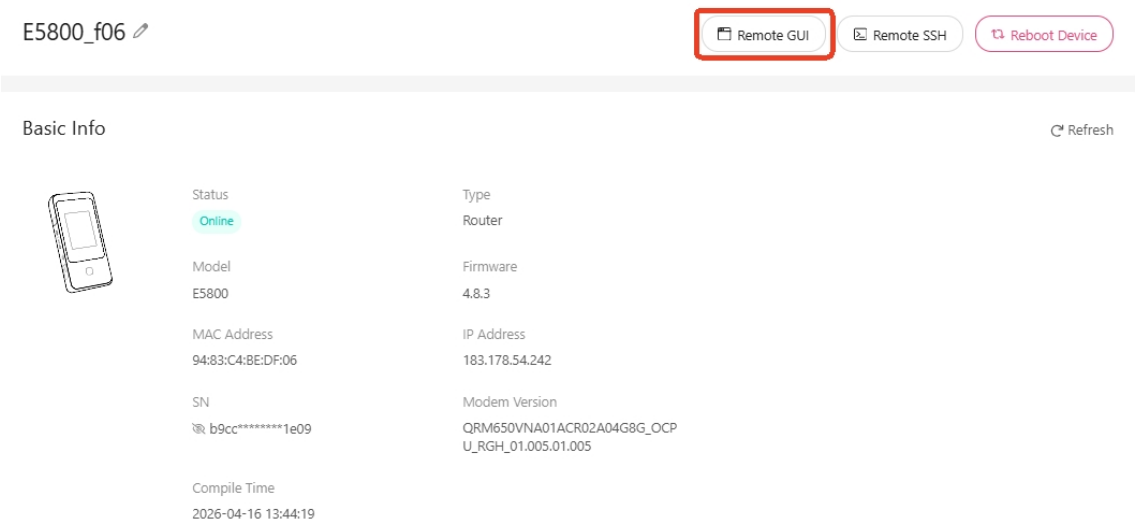


Remote Access Web

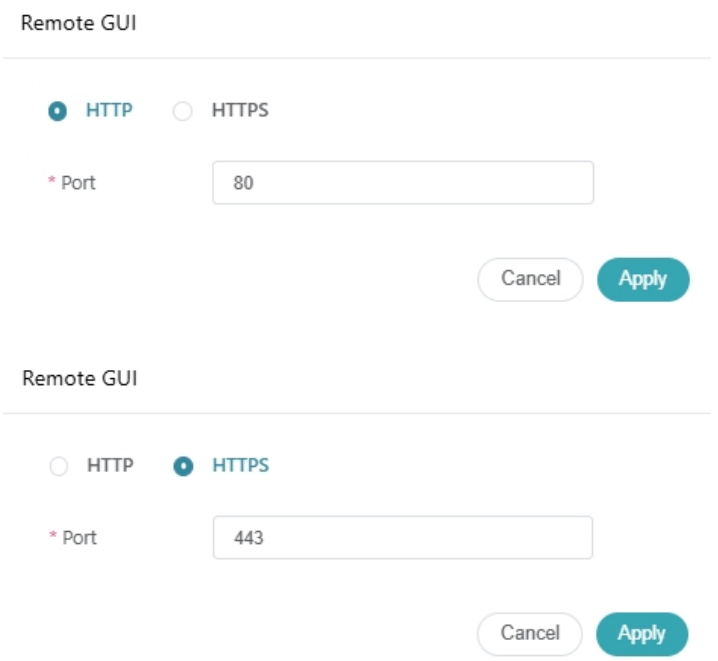
1. Log in to the router's web admin panel, navigate to **CLOUD SERVICES** > **GoodCloud**, enable **Remote Web Access**, then click **Apply**.



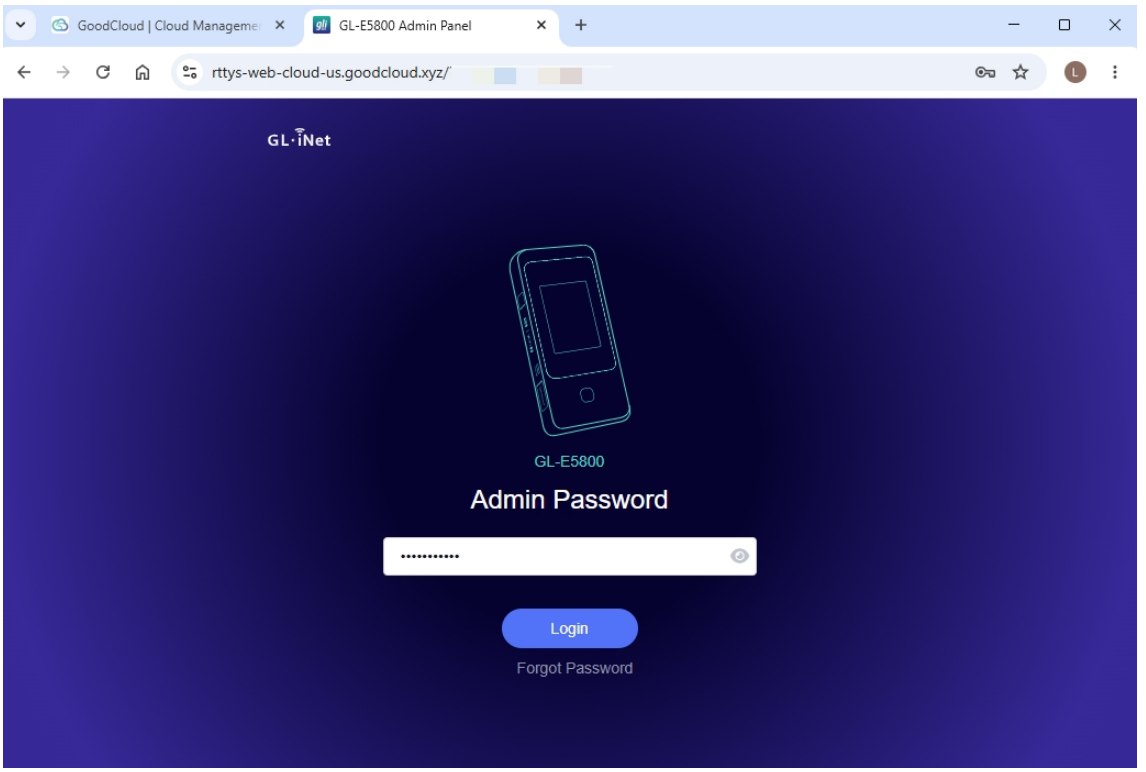
2. Log in to the GoodCloud platform and navigate to **Device** > **Bound Devices**. Click the device you want to access, and you will enter the device details page.
3. On the device details page, click the **Remote GUI** button in the upper right corner.



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

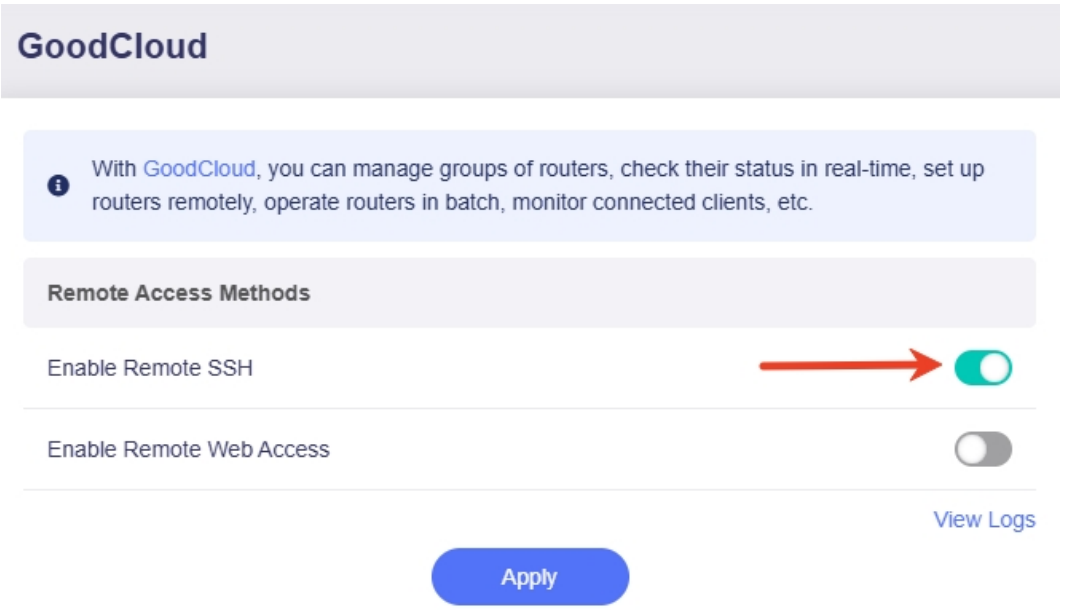


5. You will be re-directed to the router's login page. Enter the admin password to remotely access the router's web admin panel.

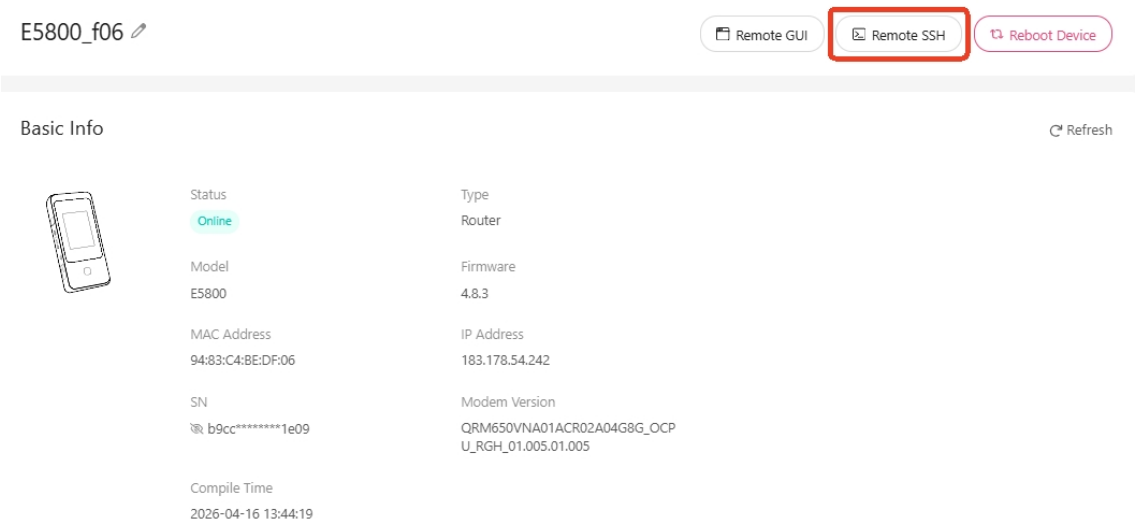


Remote Access Terminal

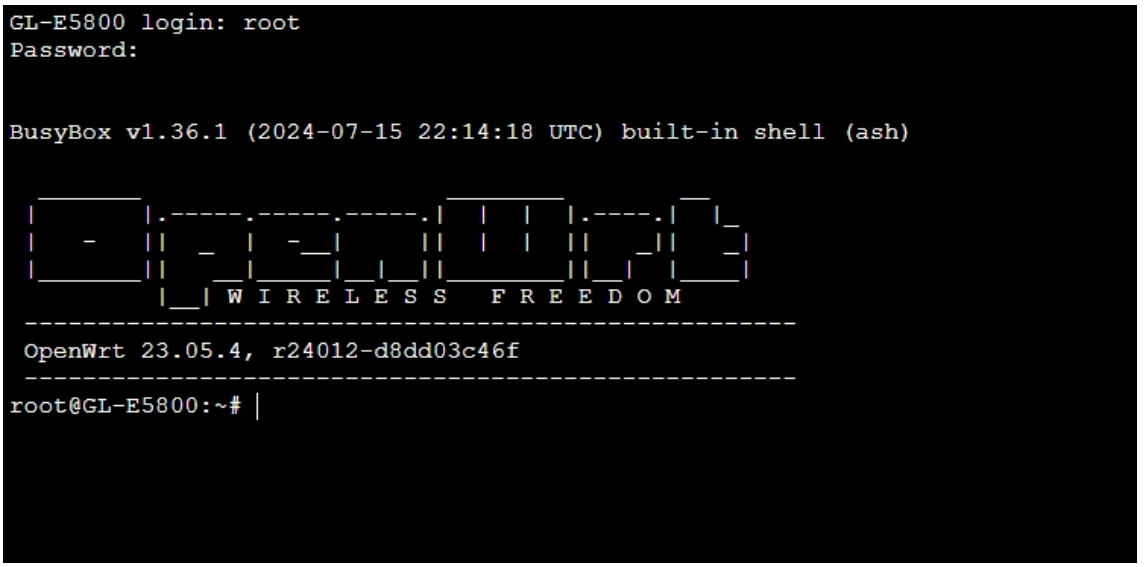
1. Log in to the router's web admin panel, navigate to **CLOUD SERVICES** > **GoodCloud**, enable **Remote SSH**, then click **Apply**.



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

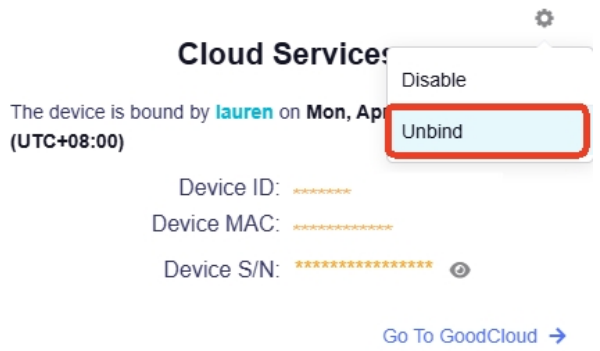


4. Log in as **root** and input the password to access the terminal of your router.

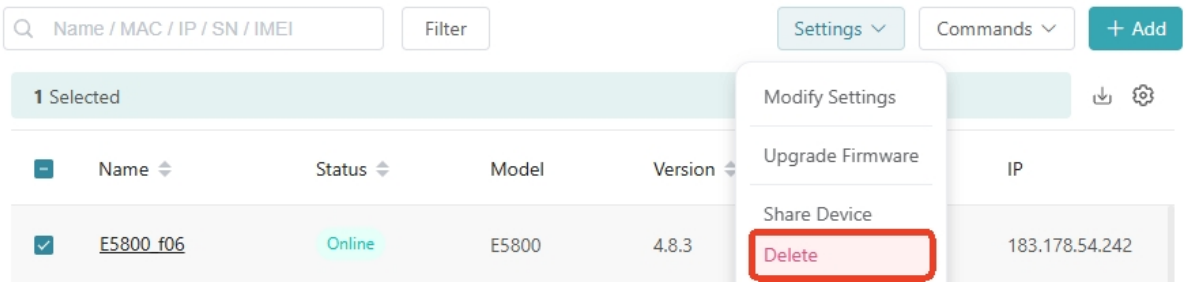

GL-E5800 login: root
Password:
BusyBox v1.36.1 (2024-07-15 22:14:18 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 23.05.4, r24012-d8dd03c46f
root@GL-E5800:~#

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.

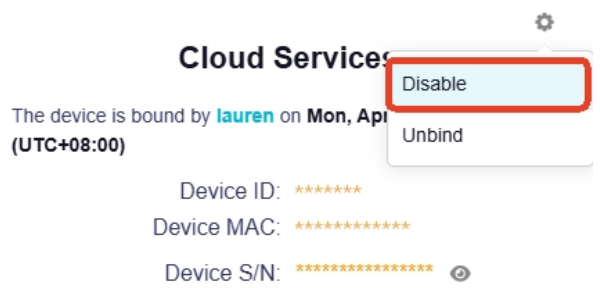


Alternatively, log in to the Cloud platform and navigate to **Device** > **Bound Devices**. Select the device you want to unbind, click **Settings** in the upper right corner, then select **Delete**. Your device will then be unbound from your GoodCloud account.



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 provide seamless remote networking and remote device management.

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

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

Refer to astrowarp.net for more information.

Chapter 8

Get To Know VPN

This chapter introduces VPN concepts and common use scenarios.

8.1 Introduction

VPN

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

VPN Router

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

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

OpenVPN

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

WireGuard

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

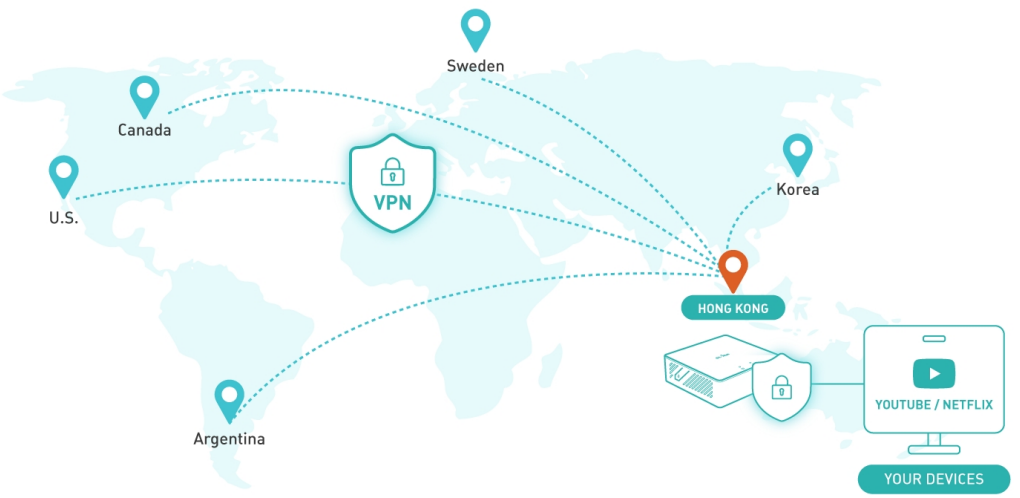
8.2 Application Scenarios

1. Personal Data Privacy

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

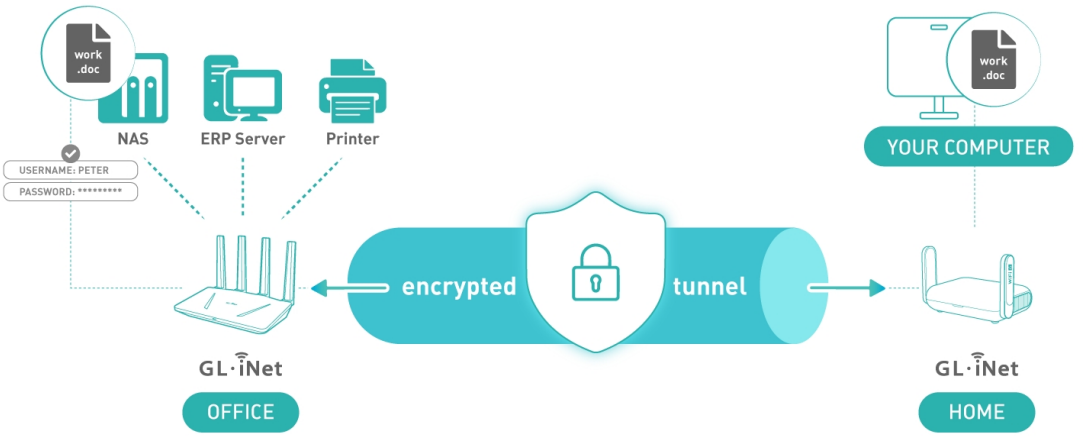
2. Unrestricted Access Worldwide

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



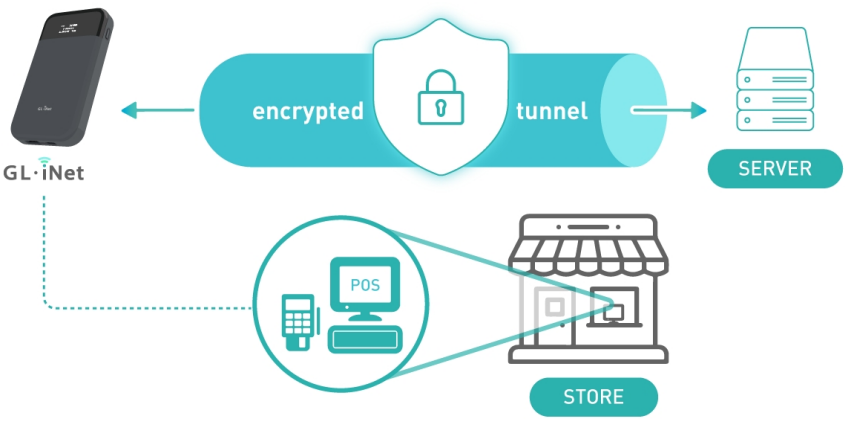
3. Small Business Data Security

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



4. Secure Payment Infrastructure

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



Chapter 9

VPN Dashboard

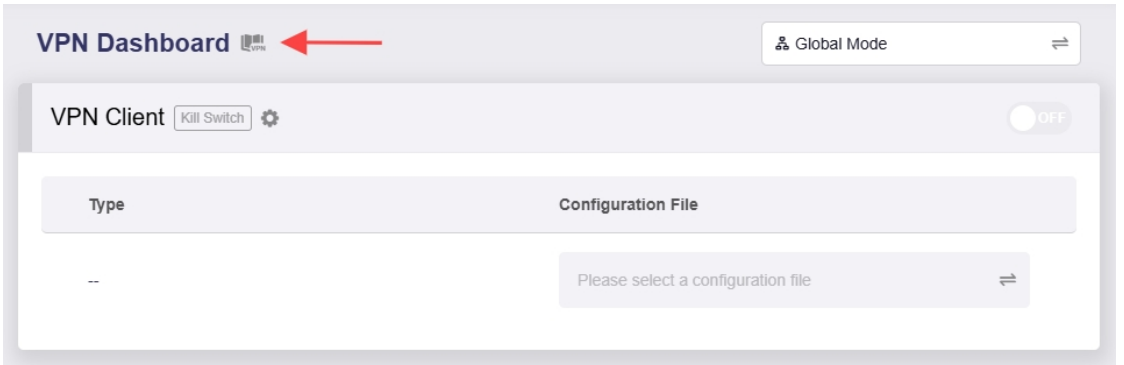
This chapter introduces how to manage VPN connections via the web admin panel.

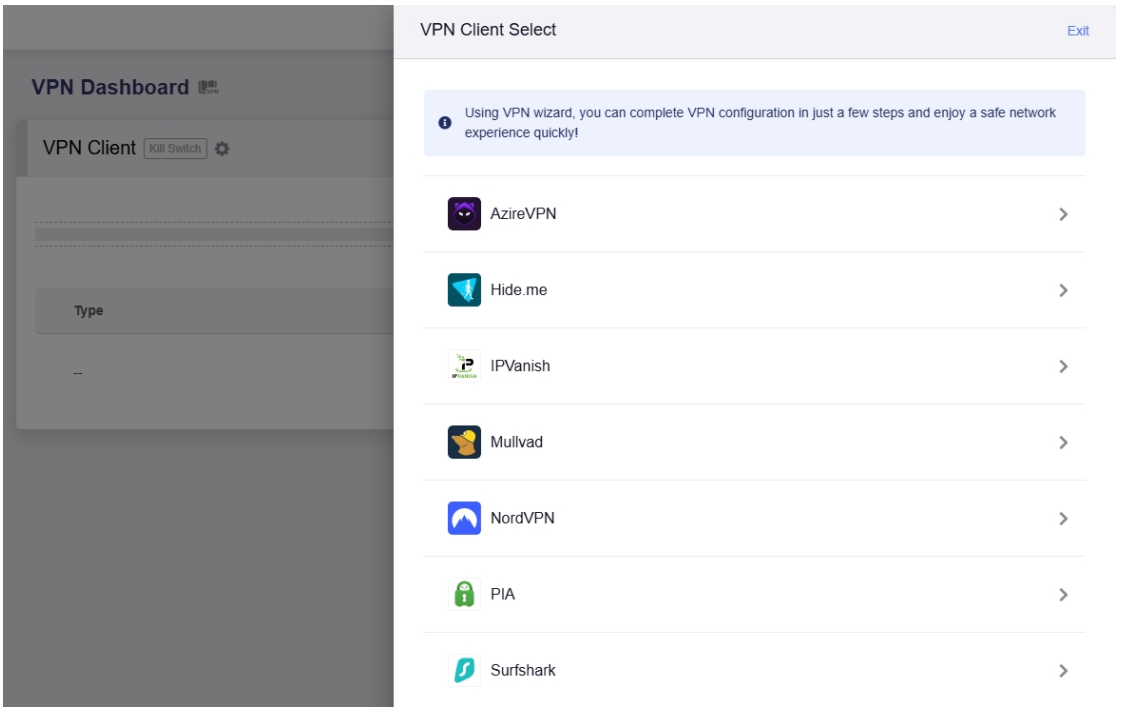
Log in to the router's web admin panel and navigate to **VPN** > **VPN Dashboard**.

The VPN dashboard displays VPN connection details, such as 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.

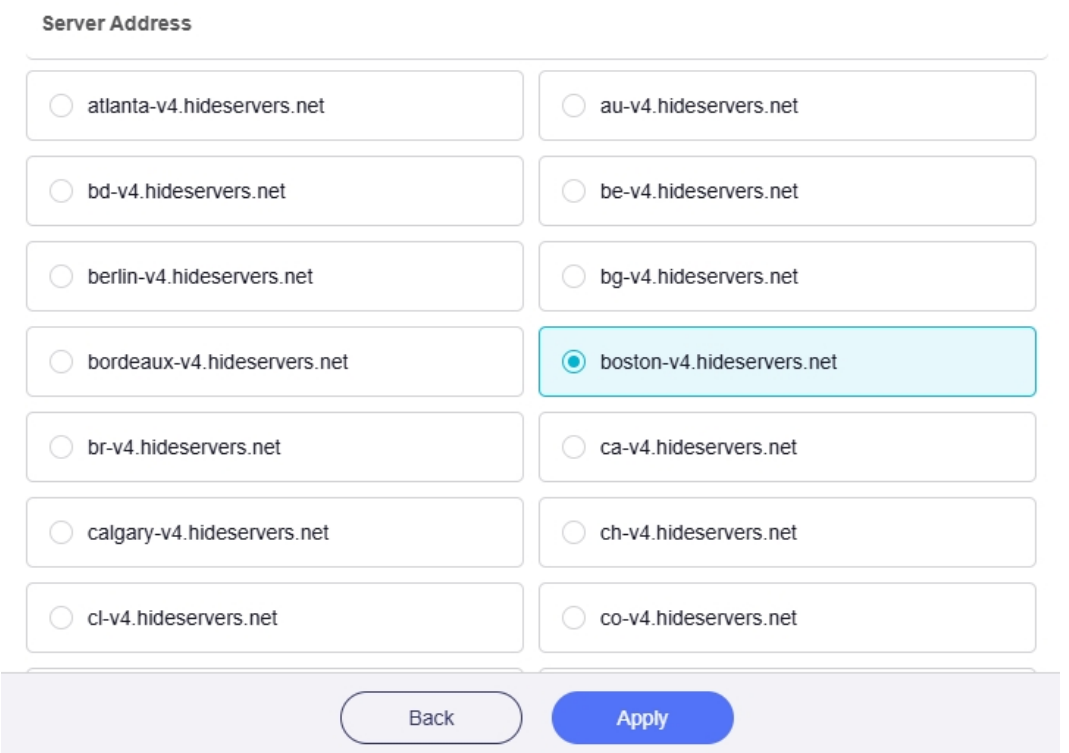




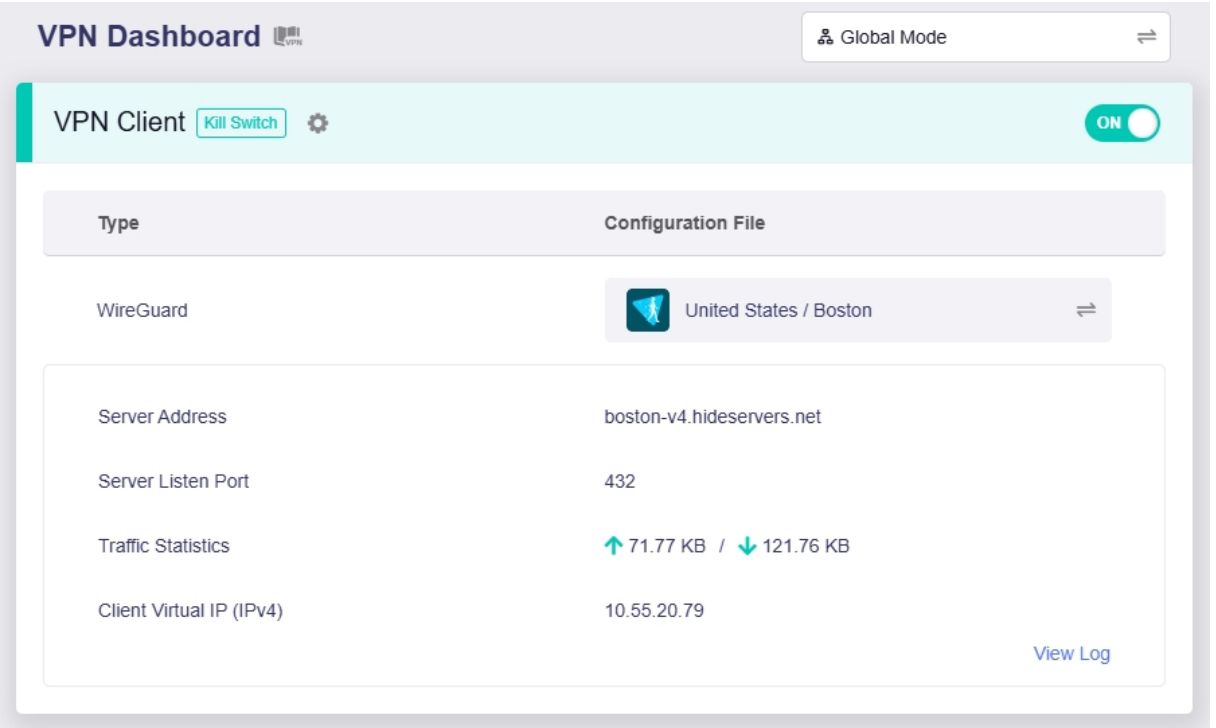
Note: The VPN Setup Wizard is only for the integrated VPN services, including AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA and Surfshark. For other VPN providers, skip the wizard and go to **VPN** > **OpenVPN Client** or **WireGuard Client** to set up VPN manually.

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

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.

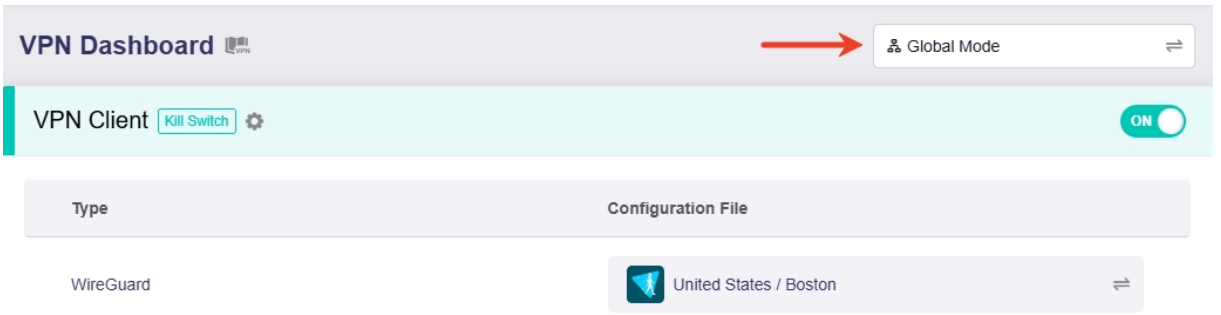


It will connect automatically. Once connected, go to the **VPN Dashboard**. You will see that a VPN tunnel has been enabled, displaying details including the VPN protocol (e.g., WireGuard), configuration file, server address, server listen port, traffic statistics, and the client virtual IP address.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

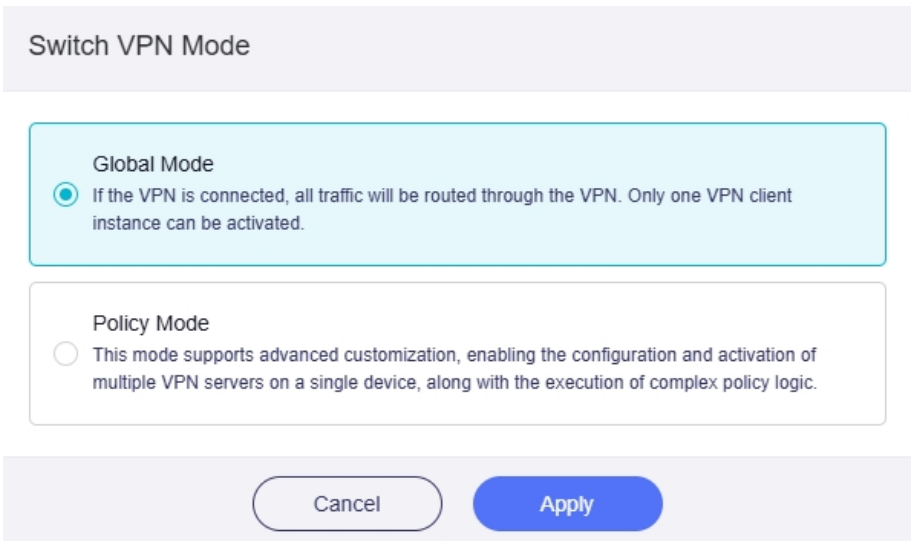


9.2 VPN Mode

On the VPN Dashboard, click the button in the upper right corner to switch VPN modes as needed.



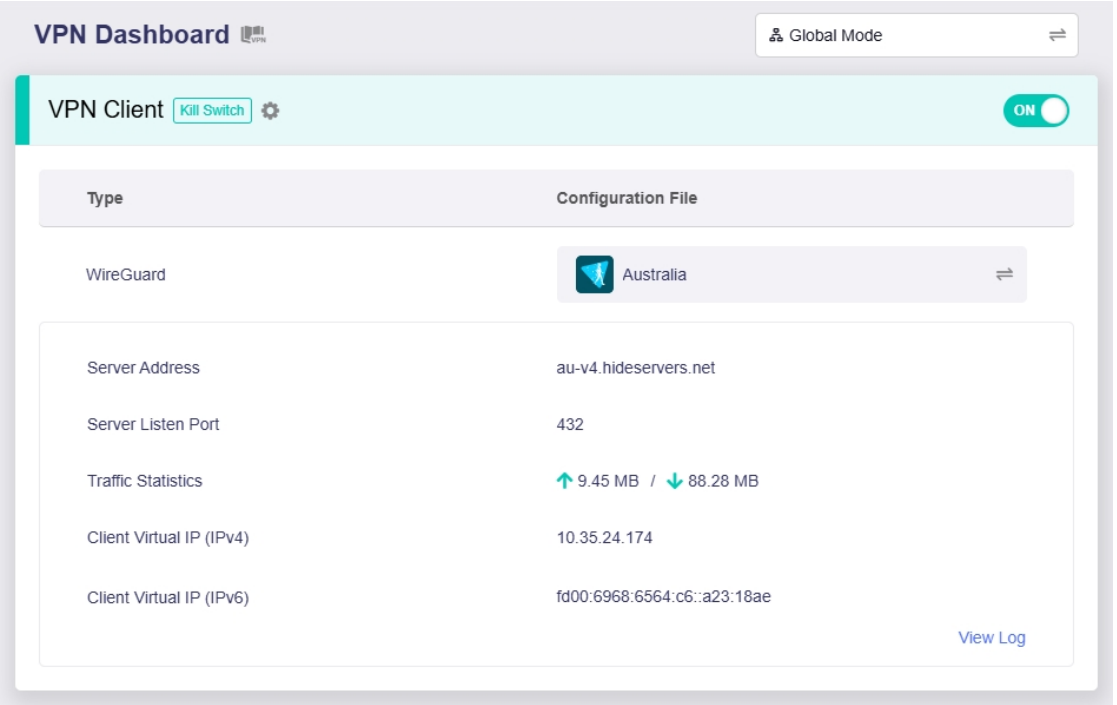
Two modes are available: **Global Mode** and **Policy Mode**.



9.2.1 Global Mode

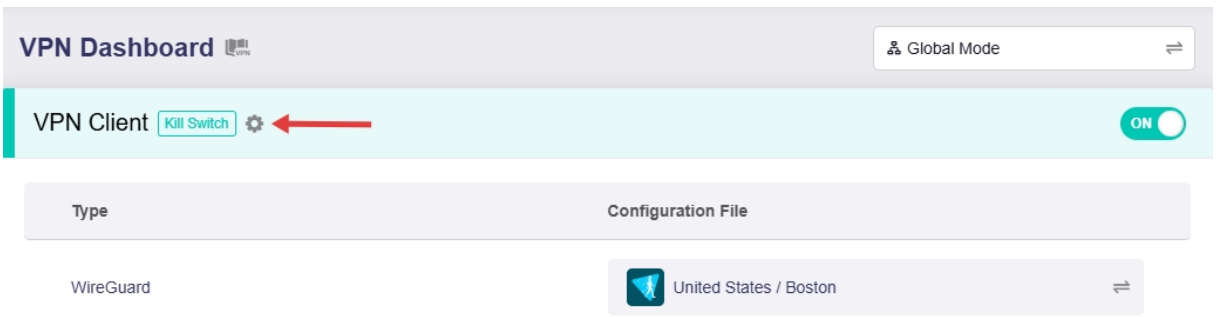
In this mode, all traffic will be routed through the VPN tunnel, and only one VPN client instance can be activated. It is ideal for scenarios requiring all device traffic to pass through a single VPN server, such as unified network security or region-specific content access.

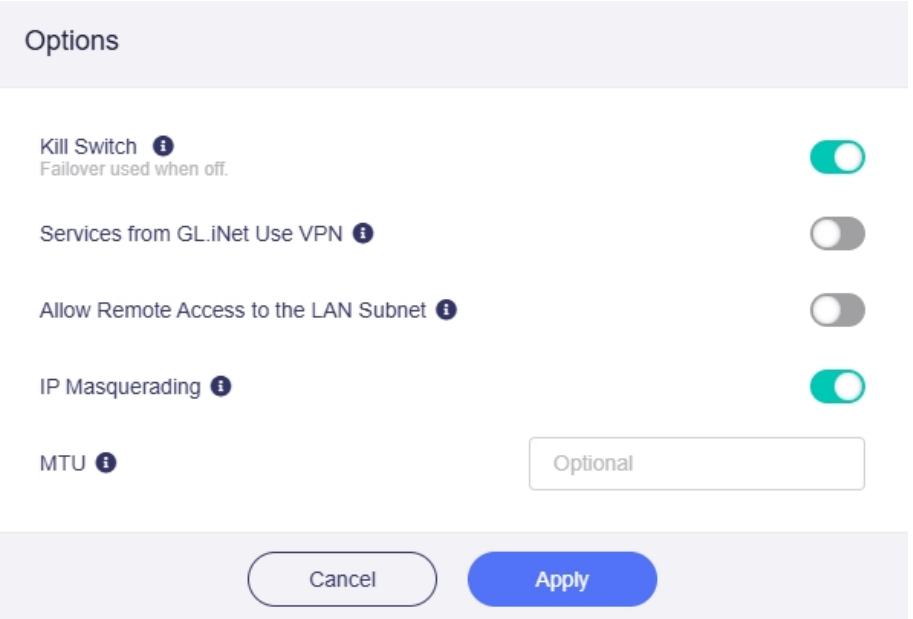
In the following example, the router connects to an Australian server using the WireGuard protocol. All traffic from connected clients will be routed through this VPN tunnel.



Tunnel Options

You can configure advanced settings for your VPN tunnel, such as the VPN Kill Switch, IP Masquerading, and MTU. Click the gear icon in the upper right corner.



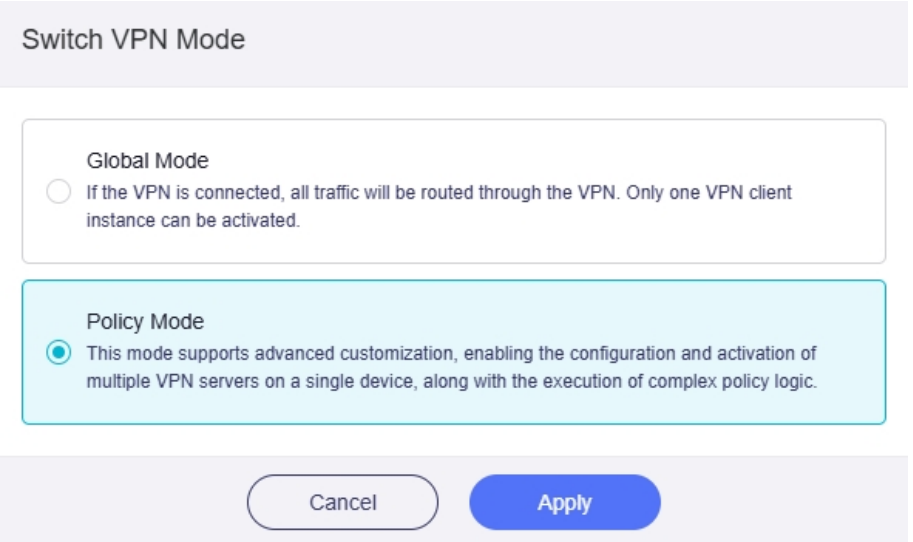


- **Kill Switch**: If enabled, any traffic routed through this VPN tunnel will be automatically blocked when the VPN connection fails. If disabled, traffic will fall back to the local WAN and access the internet without going through the VPN tunnel.
- **Services from GL.iNet Use VPN**: If enabled, GoodCloud, DDNS, and rtty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.
- **Allow Remote Access the LAN Subnet**: If enabled, remote access to this router and its LAN devices via VPN will be allowed. The VPN server must advertise a route to the LAN subnet of this router.
- **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 value defined in the configuration file.

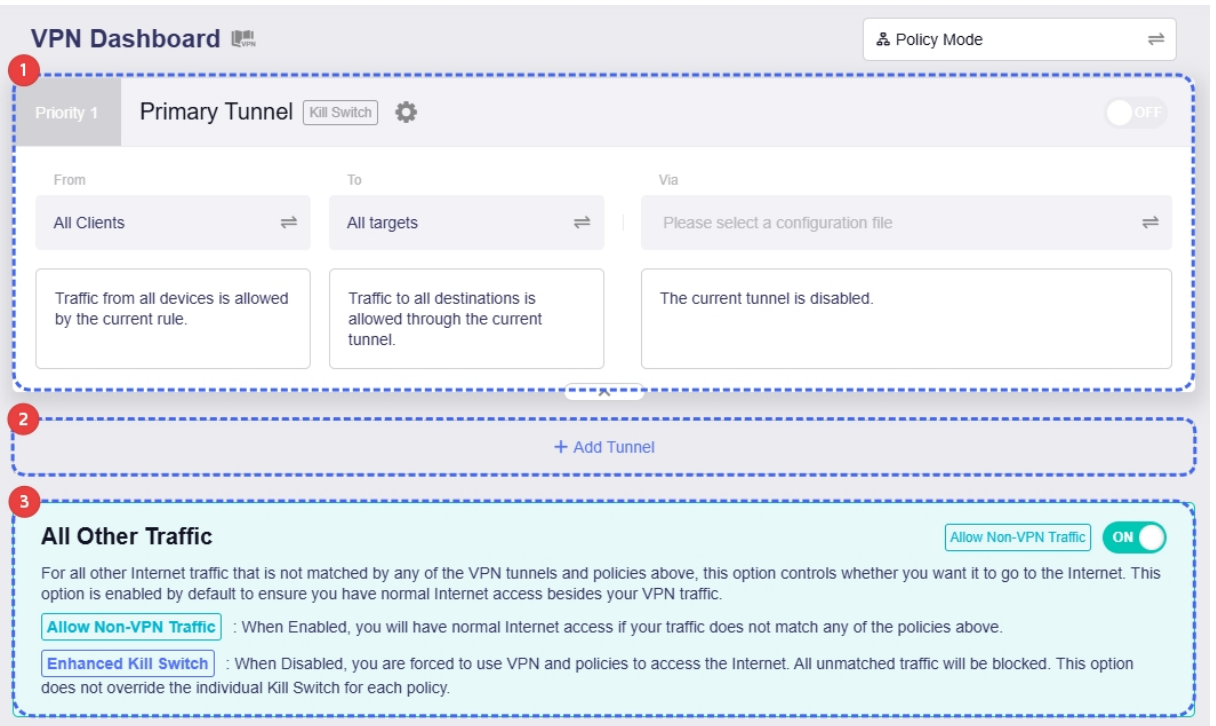
9.2.2 Policy Mode

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**.



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

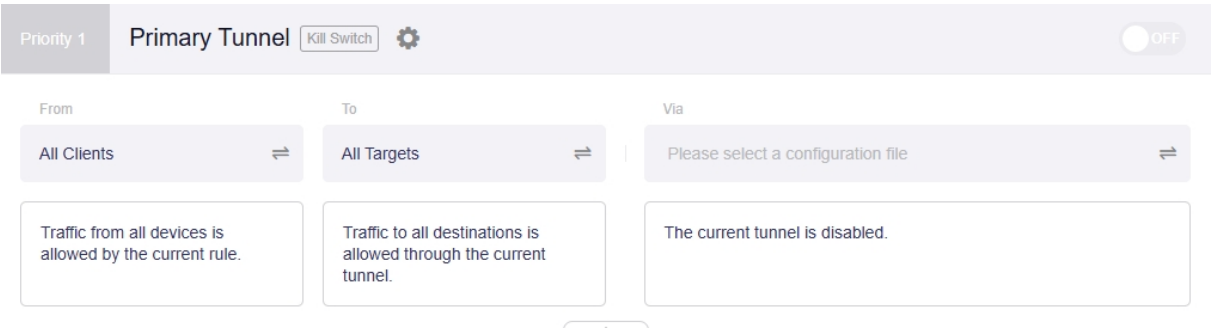


Primary Tunnel

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.

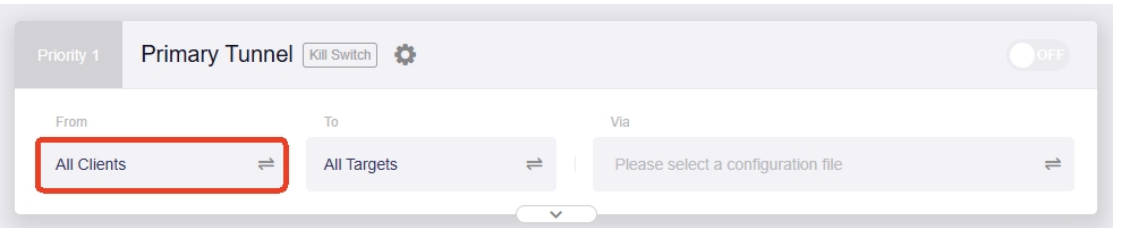
In this tunnel, you can customize the tunnel rule by setting three factors:

- **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.

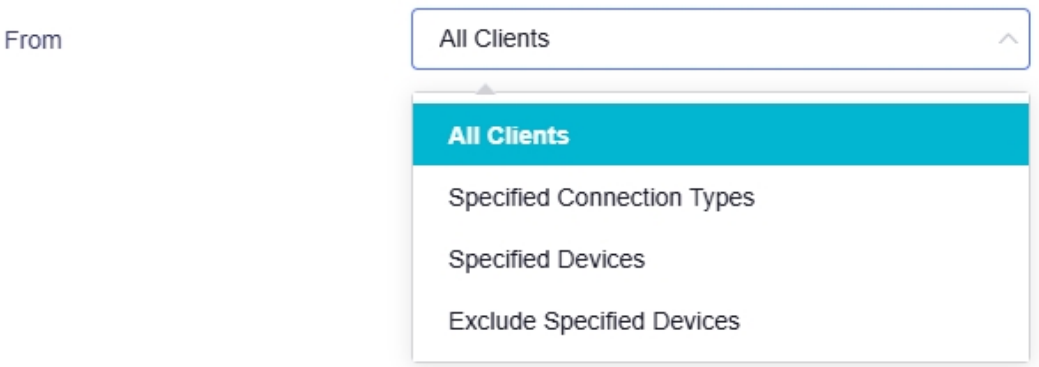


Follow the steps below to configure your tunnel rule.

1. Click the left grayed-out box.



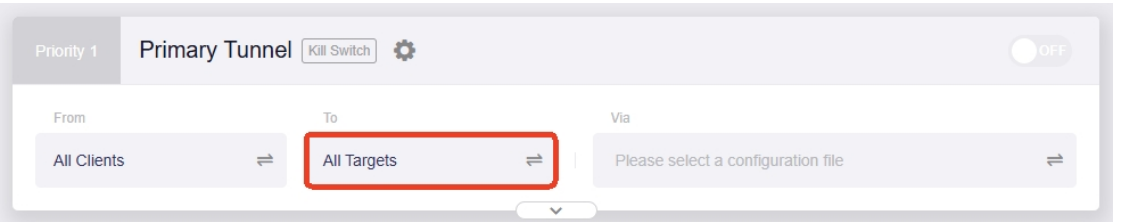
2. Select the device that you want to match this rule, and click **Apply**.



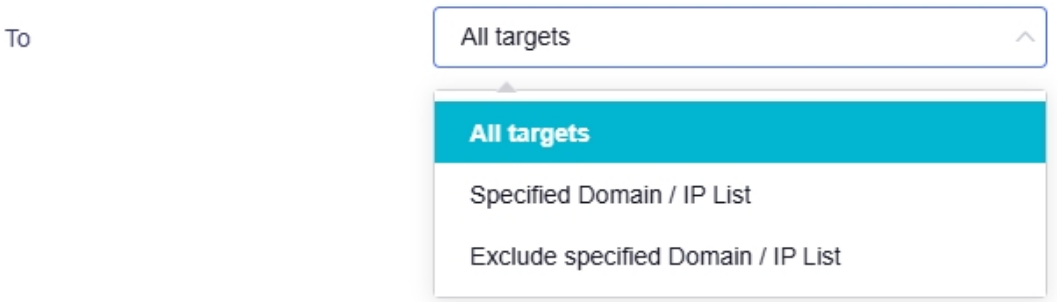
- **All Clients**: If selected, traffic from all devices will match this rule.

- **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.



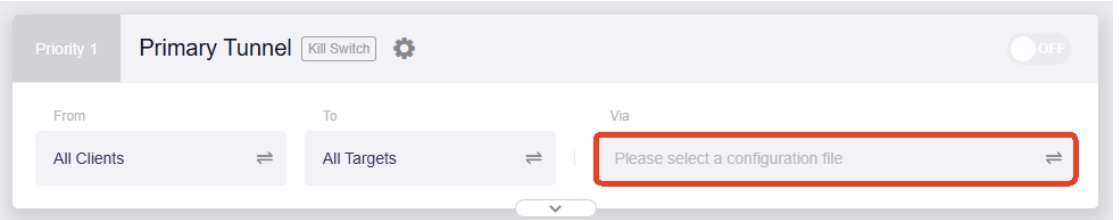
4. Select the destination to which the traffic will be routed via this tunnel, and click **Apply**.



- **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.

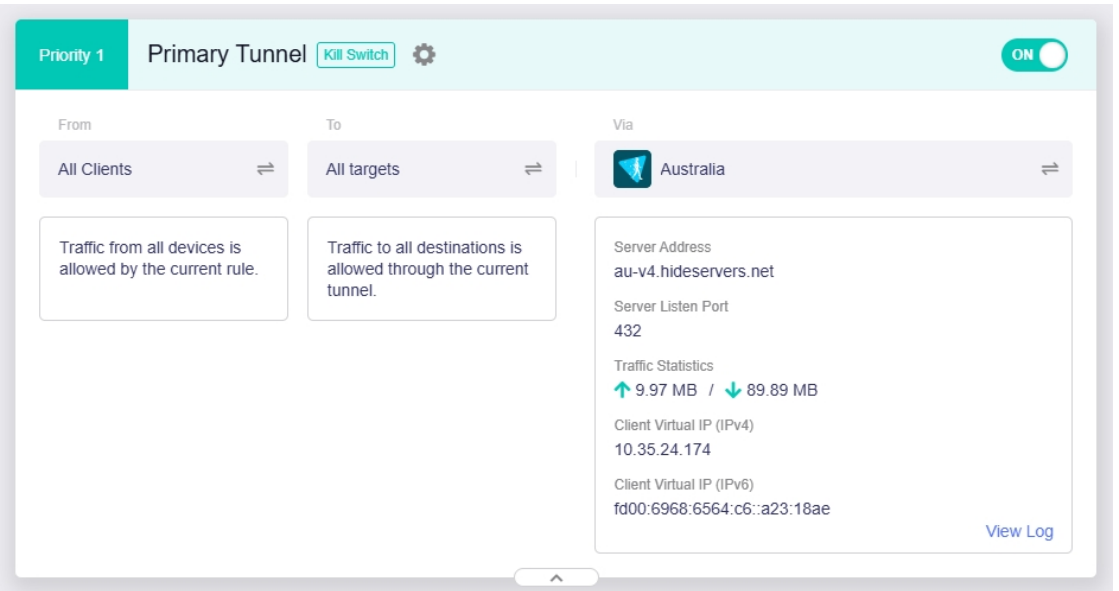
5. Click the right grayed-out box.



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.

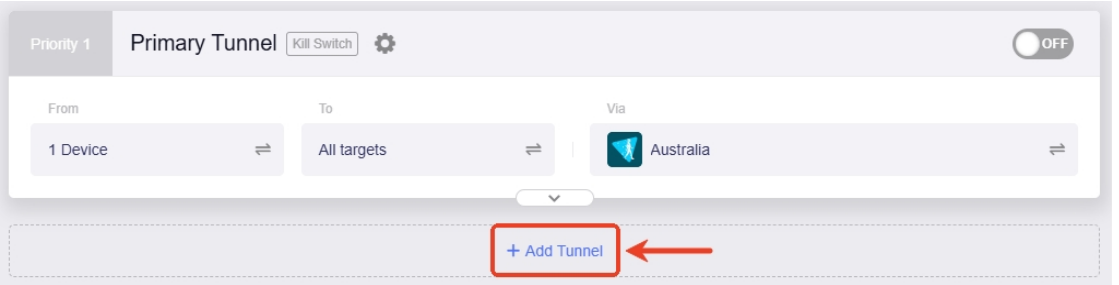


Note: For security, go to All Other Traffic and Tunnel Options to check other settings before enabling this tunnel.

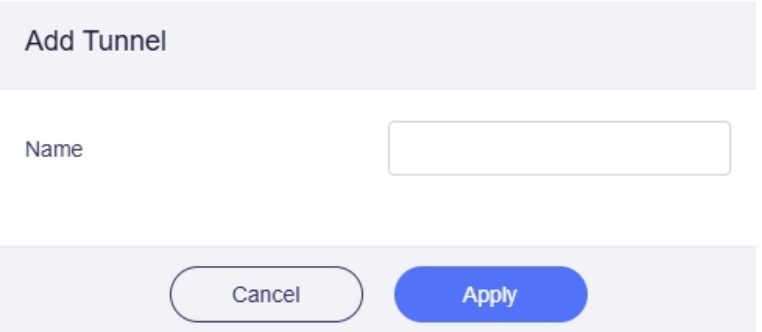
Add Tunnel

Add tunnels if you need to route traffic from different devices to different destinations. Follow the steps below to add a tunnel.

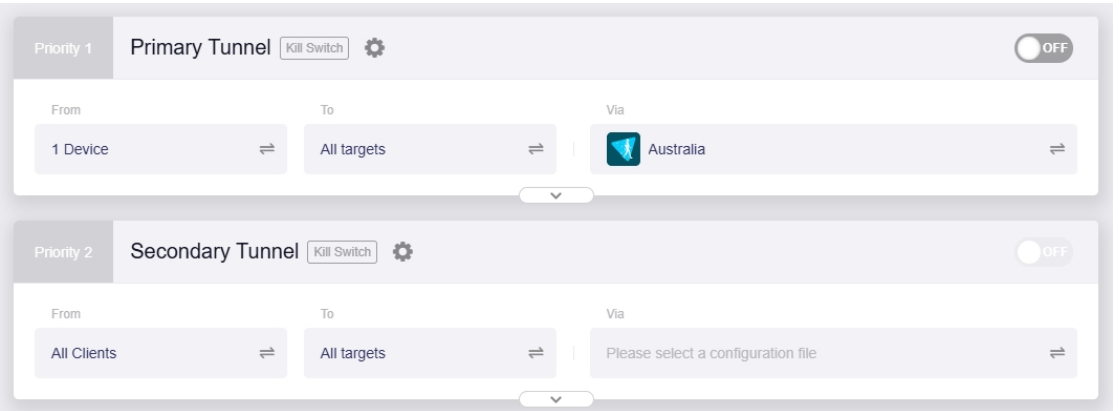
1. Click **Add Tunnel** beneath the Primary Tunnel.



2. Name the tunnel.



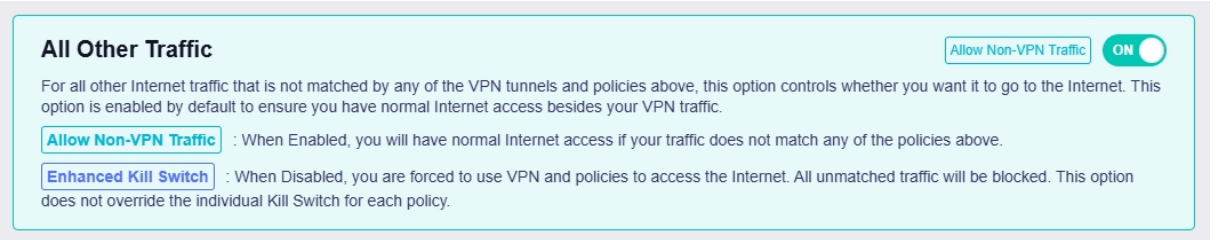
3. You will get one more tunnel on the VPN Dashboard. Up to 5 tunnels can be created (including the preset primary tunnel).



4. Configure tunnel rules by setting the traffic source, destinations and routing method. Once finished, verify other settings in All Other Traffic and Tunnel Options for security before enabling the tunnels.

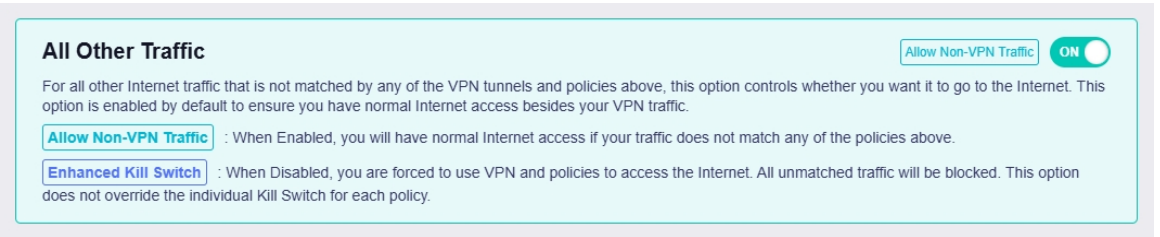
All Other Traffic

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

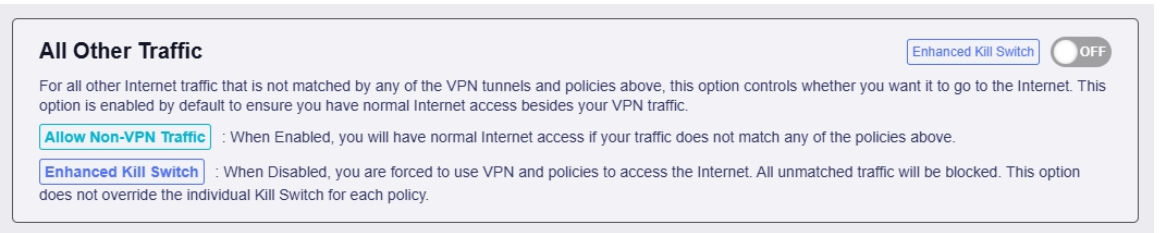


This tunnel controls whether traffic that does not match any of the above VPN tunnel groups can access the Internet. It is enabled by default to ensure normal Internet access for traffic not routed via VPN.

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



- 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.

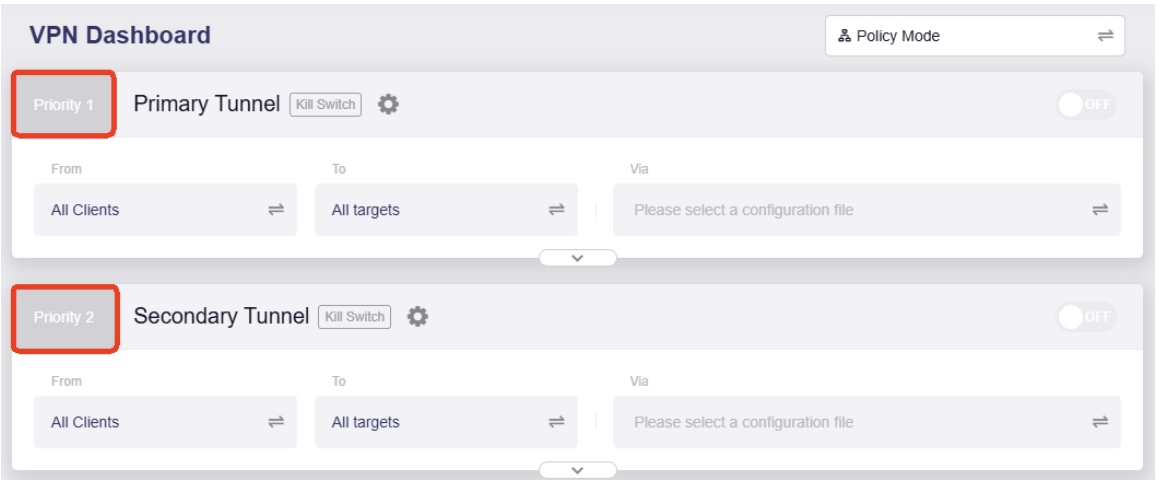


Tunnel Priority

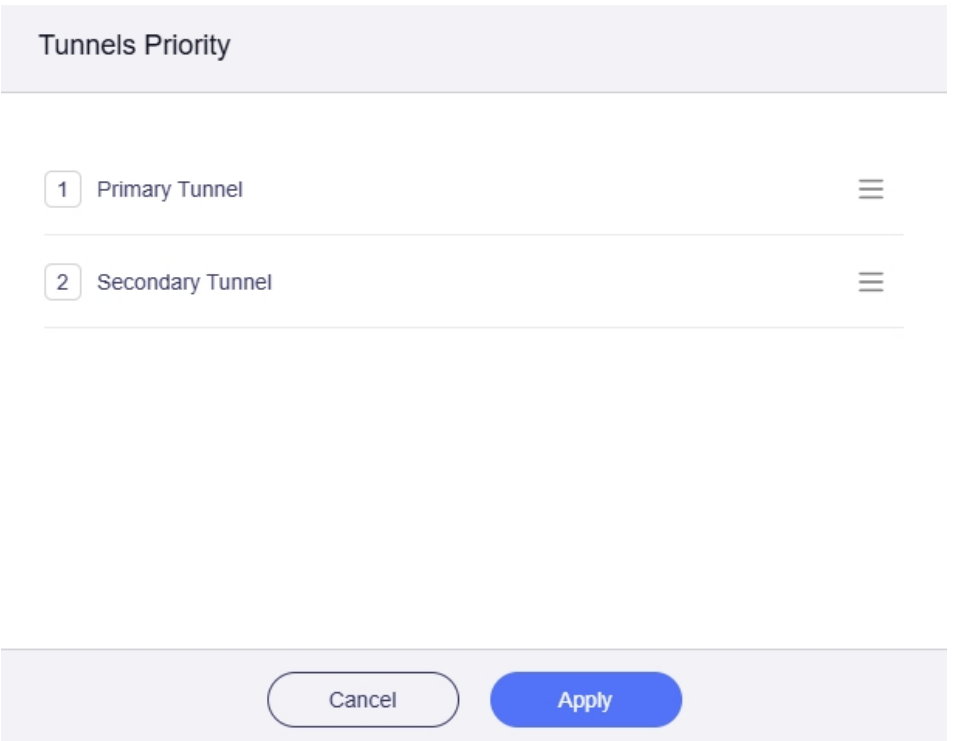
By default, the preset Primary Tunnel has the highest priority, followed by other manual-added tunnel (if any), then the preset All Other Traffic tunnel to ensure network connectivity via local ISP (WAN) network.

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**.

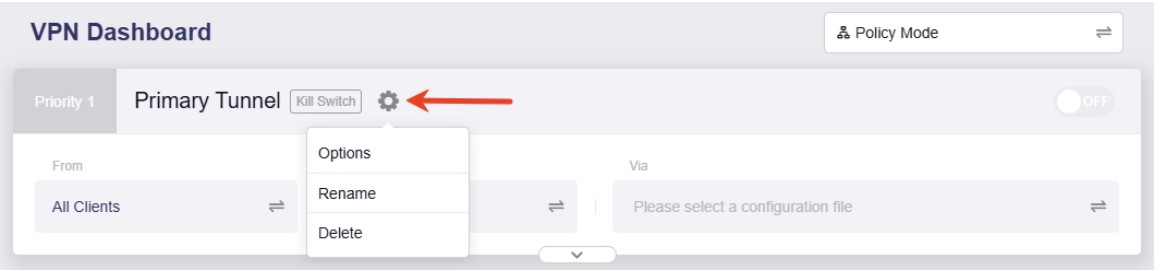


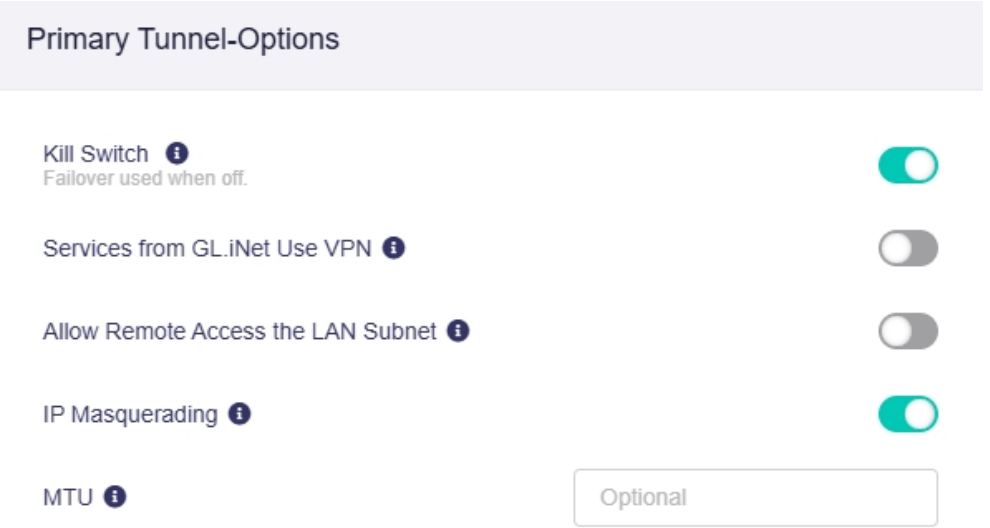
When multiple tunnels are enabled, the router will route traffic in the following order:

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.

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.





- **Kill Switch**: If enabled, any traffic routed through this VPN tunnel will be automatically blocked if the VPN connection fails. If disabled, traffic will fail over to the next priority tunnel or the local WAN.
- **Services from GL.iNet Use VPN**: If enabled, GoodCloud, DDNS, and rtty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.
- **Allow Remote Access the LAN Subnet**: If enabled, remote access to this router and its LAN devices via VPN will be allowed. The VPN server must advertise a route to the LAN subnet of this router.
- **IP Masquerading**: If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU**: The MTU you set for the tunnel will overwrite the value in the configuration file.

Chapter 10

Set Up VPN Server

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

10.1 Set Up OpenVPN Server

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

10.1.1 Preparation

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

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

   Alternative methods:

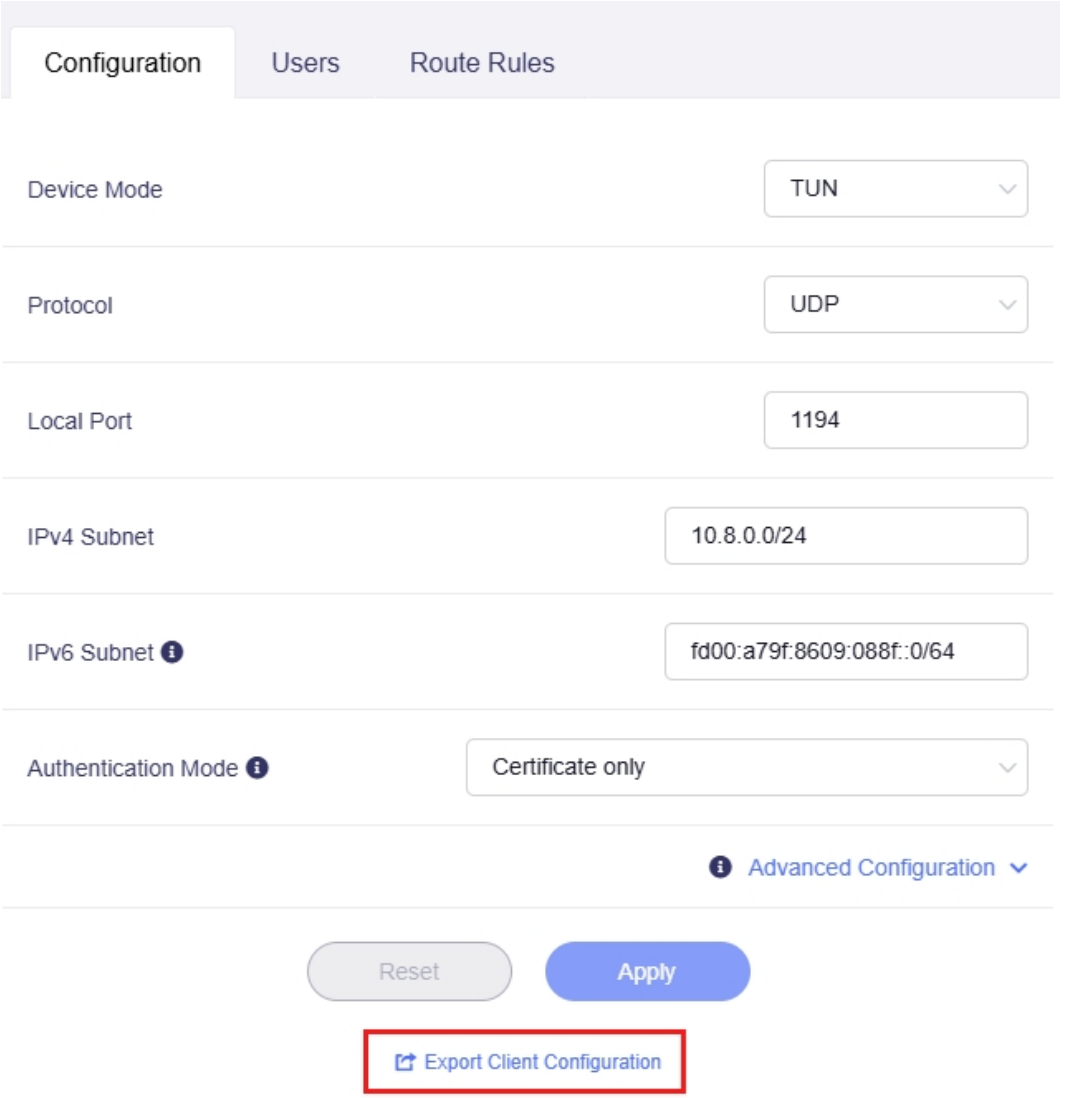
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.
   - If the above two methods don't work (e.g., if your network is behind CGNAT), you may try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

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

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

10.1.2 Setup Steps

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



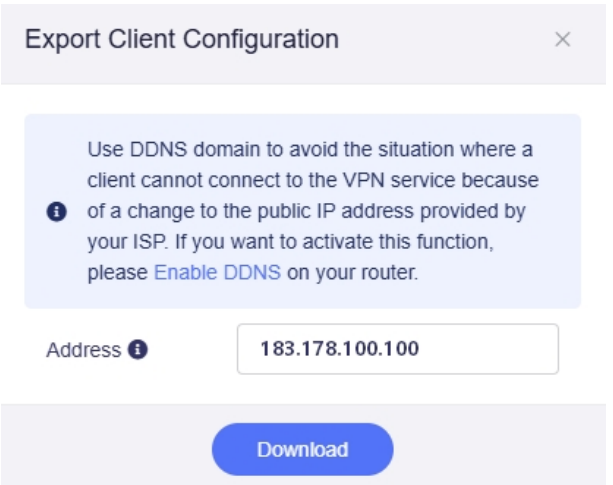
- **Device Mode**: TAP-S2S or Tun. See here for the differences.
- **Protocol**: UDP or TCP. See here for the differences.
- **Authentication Mode**: This determines the authentication method used when the client connects to the server. There are three options:

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

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

3. Export Client Configuration.

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



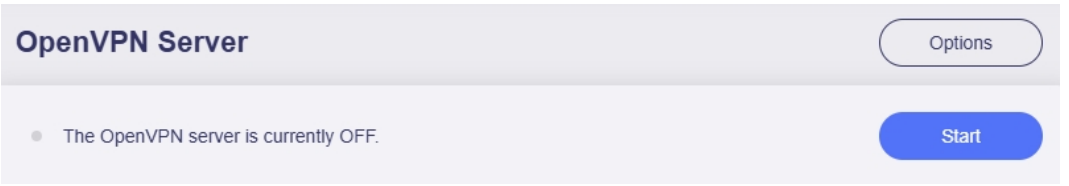
Tips:

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

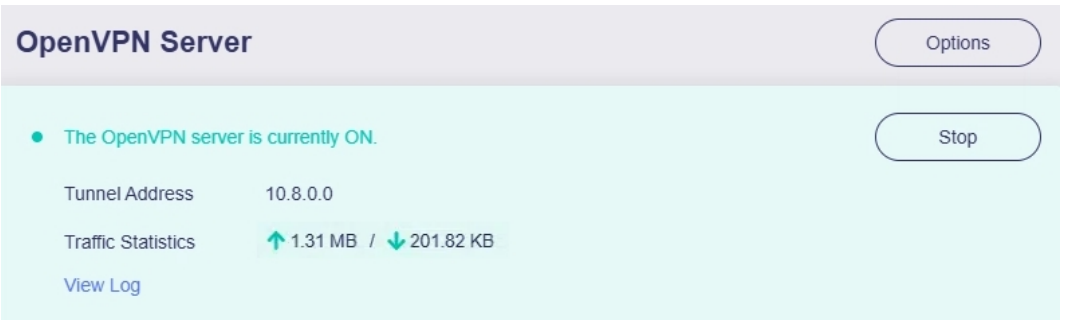
address. Once selected, the server address in the configuration file will be updated automatically. Re-download the configuration file if the server address is changed.

4. Start OpenVPN server.

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



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



10.1.3 Troubleshooting

If the connection fails, there are several common reasons:

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

10.2 Set Up WireGuard Server

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

10.2.1 Preparation

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

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

   Alternative methods:

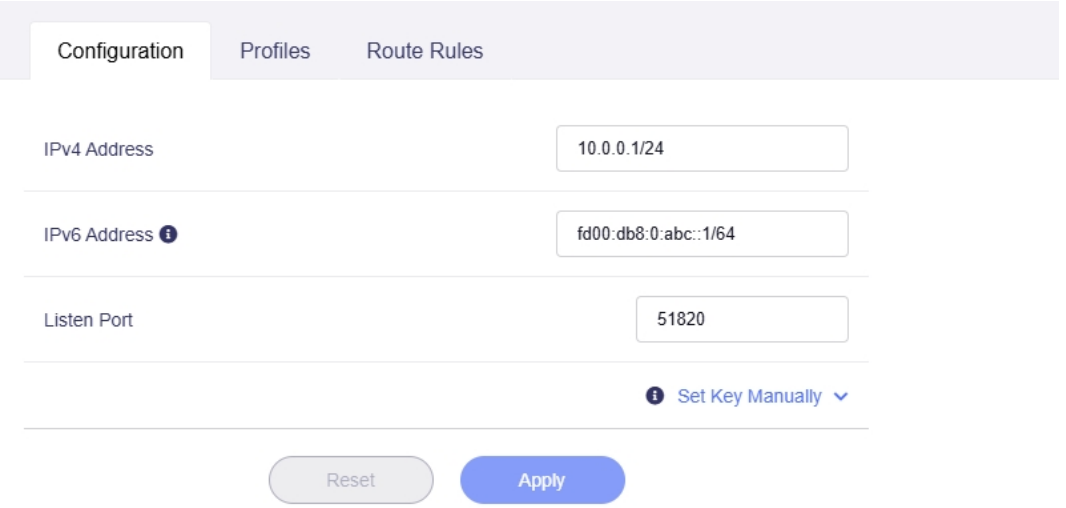
   - If you have a primary router upstream of your GL.iNet router, log in to it and verify it has a public IP address assigned by your ISP.
   - Ask your ISP for a public IP address. This may incur an extra fee.
   - If the above two methods don't work (e.g., if your network is behind CGNAT), you may try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

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

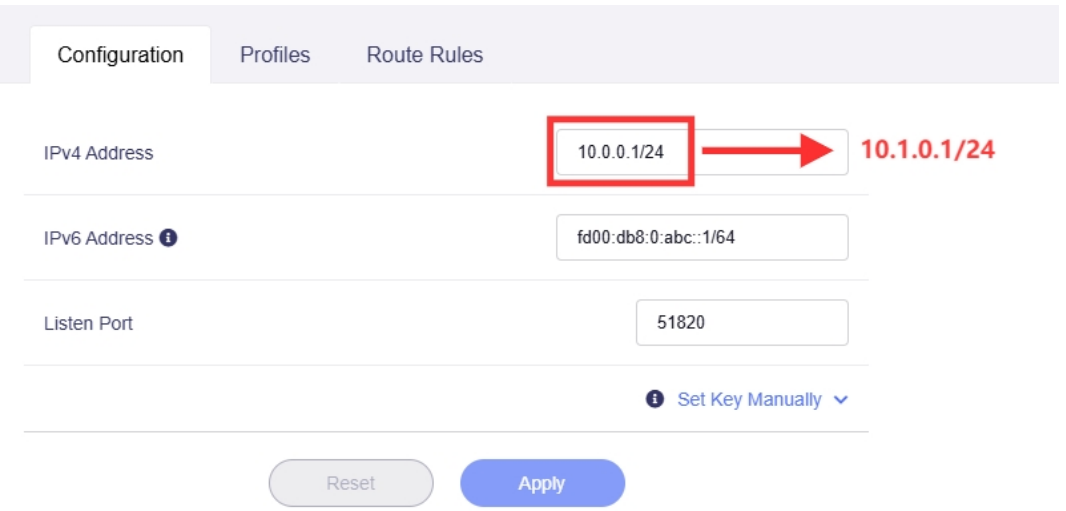
   - If your GL.iNet router is the primary router in your network, no port forwarding setup is required. Proceed to the next step.
   - If a primary router is already in use and your GL.iNet router is configured as a secondary router, you will need to configure port forwarding on the primary router.
  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

10.2.2 Setup Steps

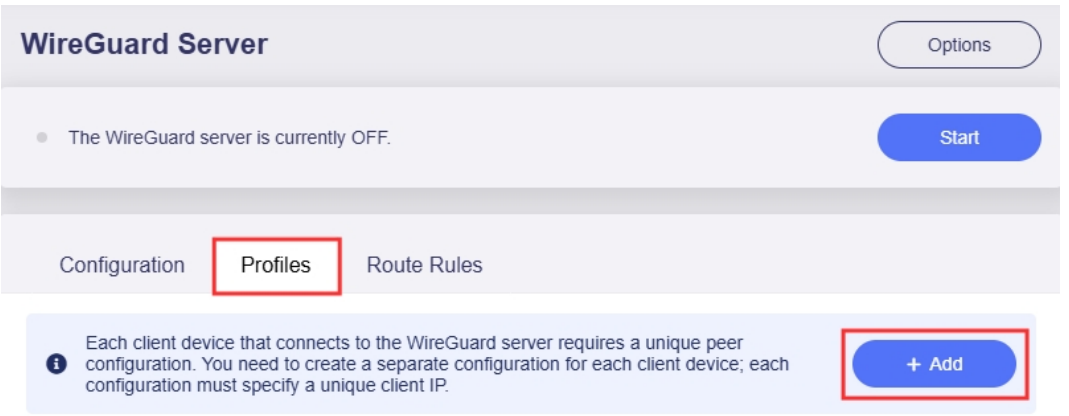
1. Log in to the router's web admin panel, navigate to **VPN** > **WireGuard Server**, then click **Generate Configuration** (for VPN server initial setup only).
2. Apply the configuration.
   The default configuration works for most cases. No need to modify the IPv4 address unless it conflicts with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



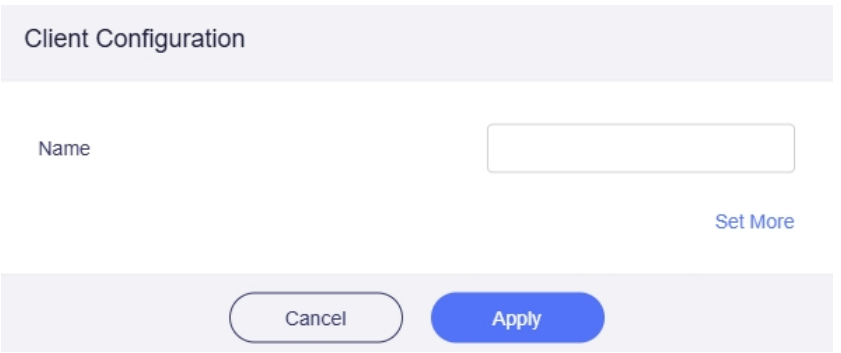
   If the IPv4 address conflicts with your upstream router's gateway, modify the IPv4 address to another one (e.g., **10.1.0.1/24**) and click **Apply**. Ensure the "/24" CIDR notation is included to avoid connectivity issues.



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



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

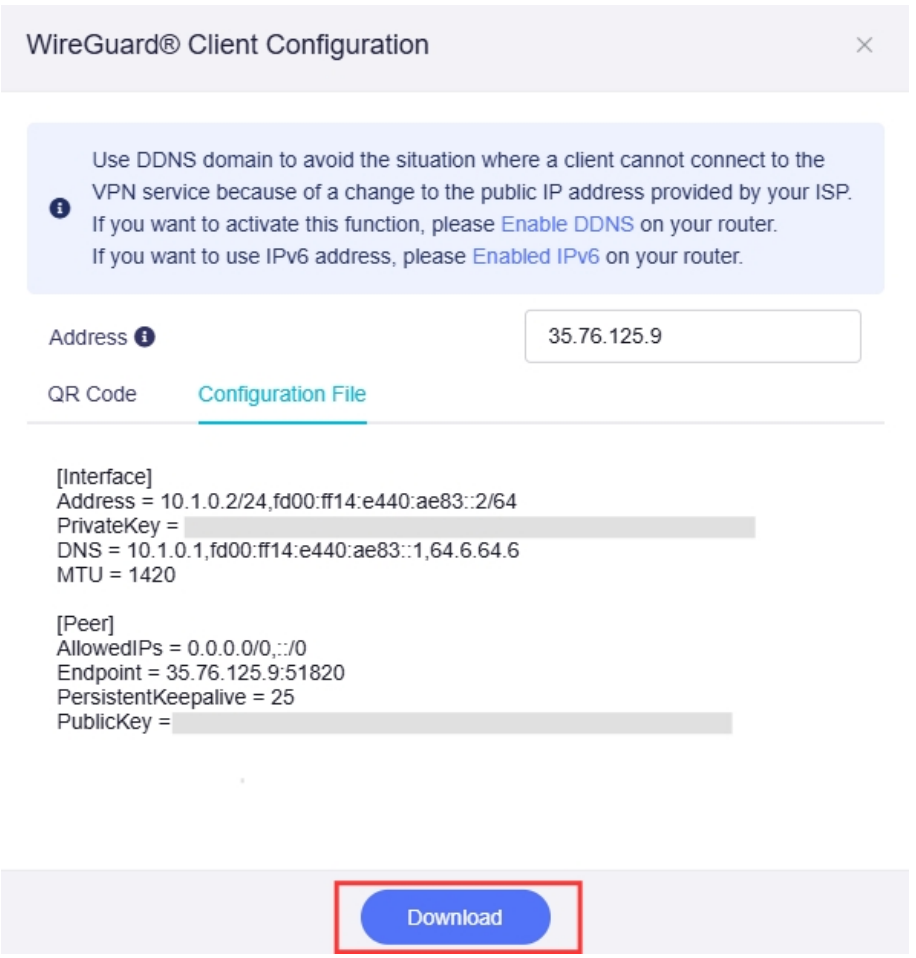


Tip: If you want to access the WireGuard client's LAN devices from your WireGuard server, switch to the **Route Rules** tab to configure route rules. See here for details.

4. Download configuration.

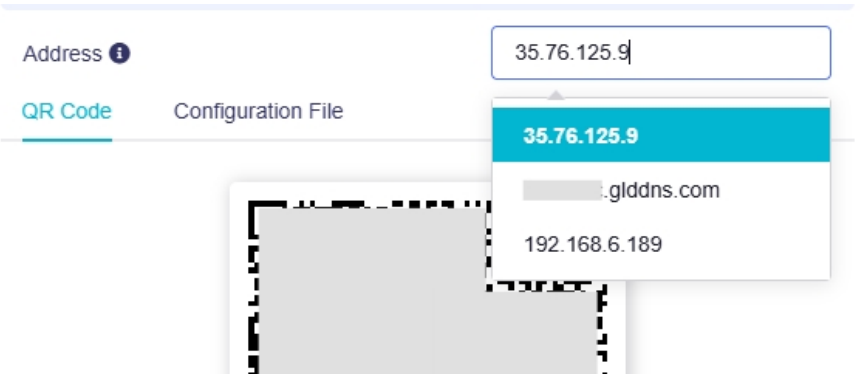
   After adding a profile, the router will generate a configuration file in three formats: QR code, plain text, and .conf file. Choose your preferred method to obtain the configuration file.

   - **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.



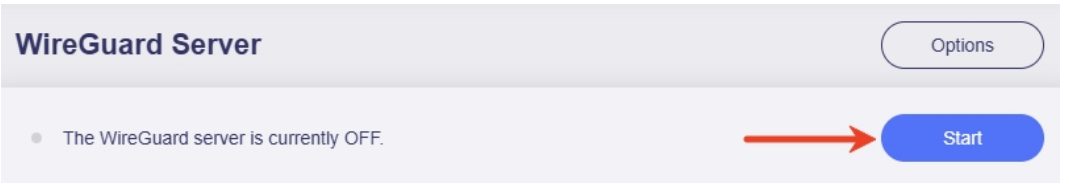
Tips:

- 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.

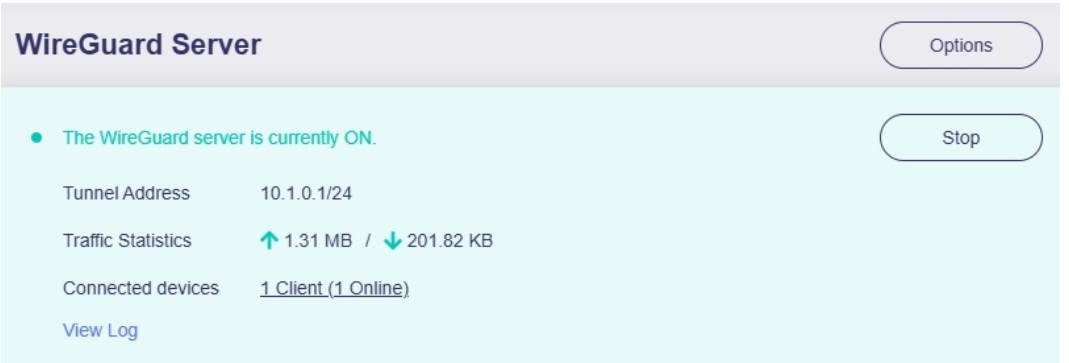


5. Start WireGuard server.

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



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



10.2.3 Troubleshooting

If the connection fails, there are several common reasons:

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

Chapter 11

Set Up VPN Client

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

11.1 Set Up OpenVPN Client

11.1.1 Preparation

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

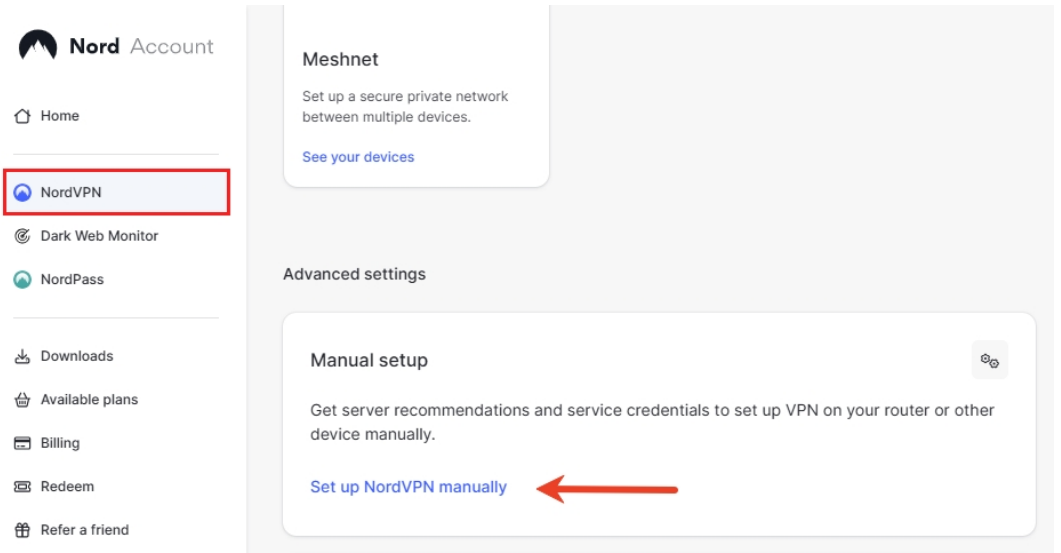
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to this link or contact their support.

11.1.2 Set Up NordVPN

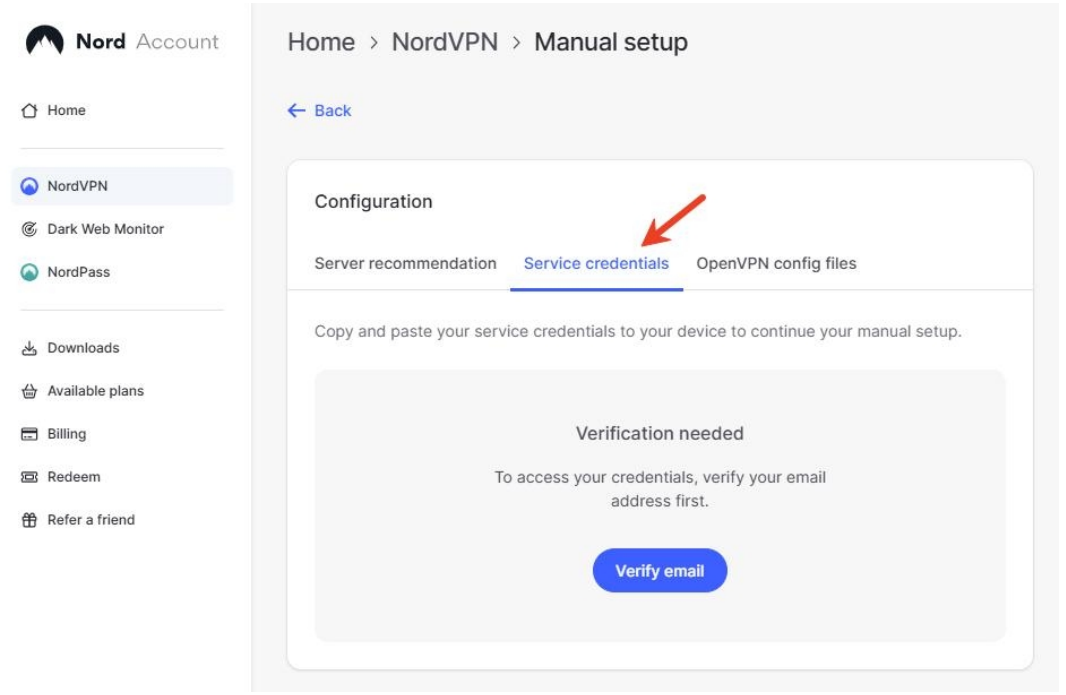
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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

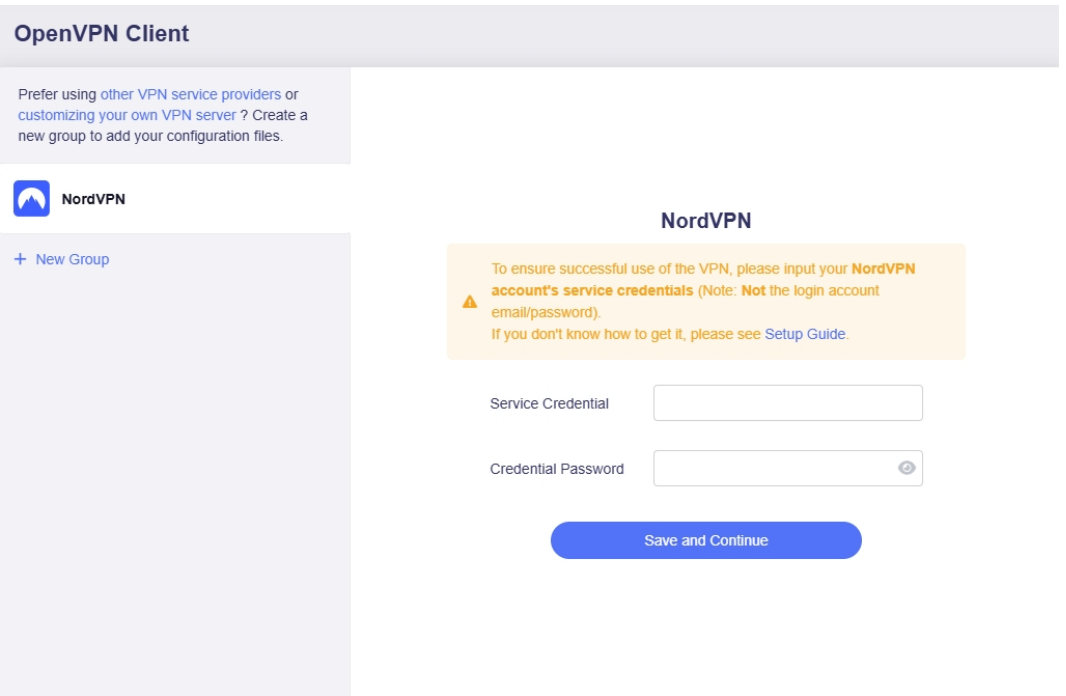
1. Log in to your NordVPN web account here.
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



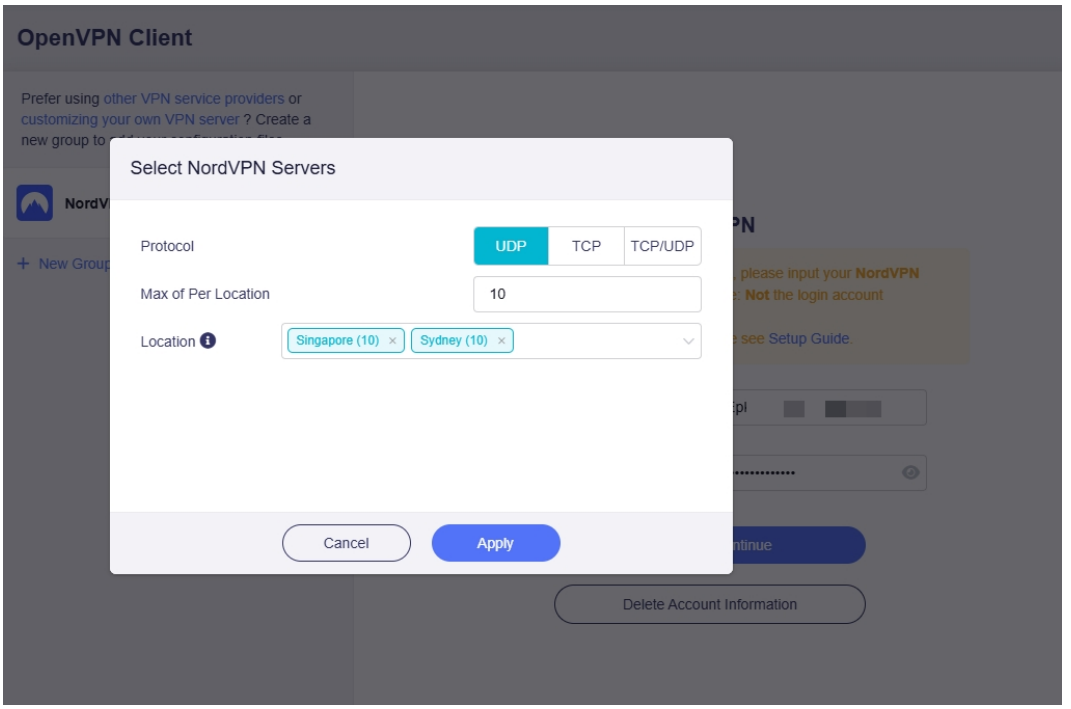
You will find the **service credentials**. Copy them for later use.



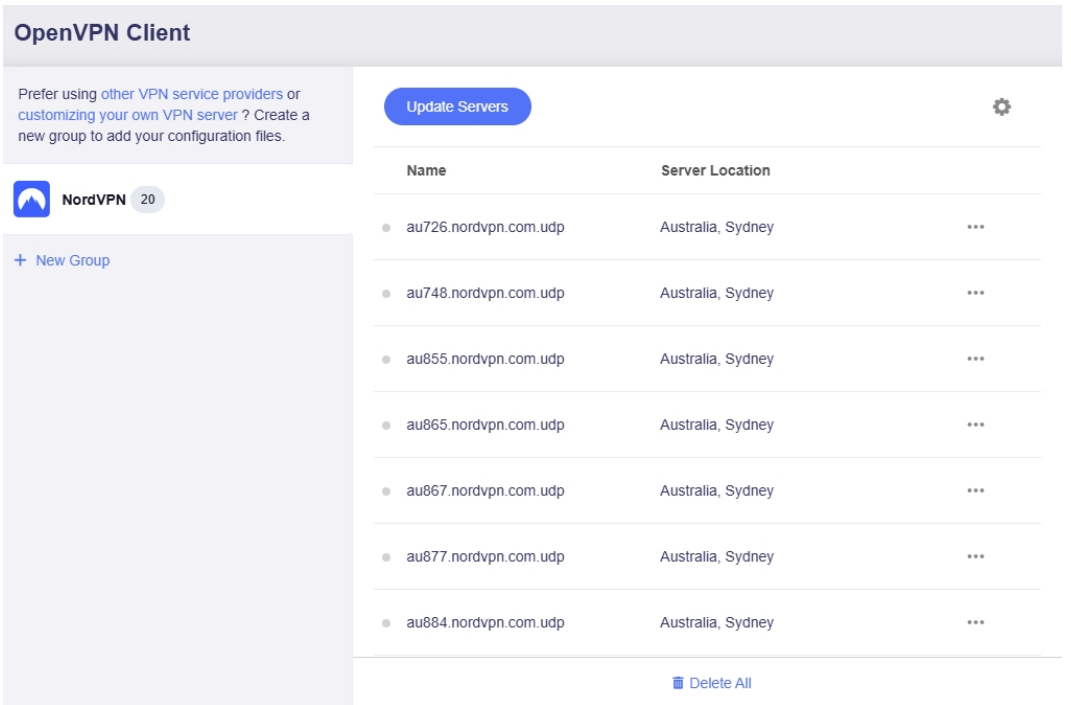
3. Log in to your router's web admin panel and navigate to **VPN** > **OpenVPN Client** > **NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



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

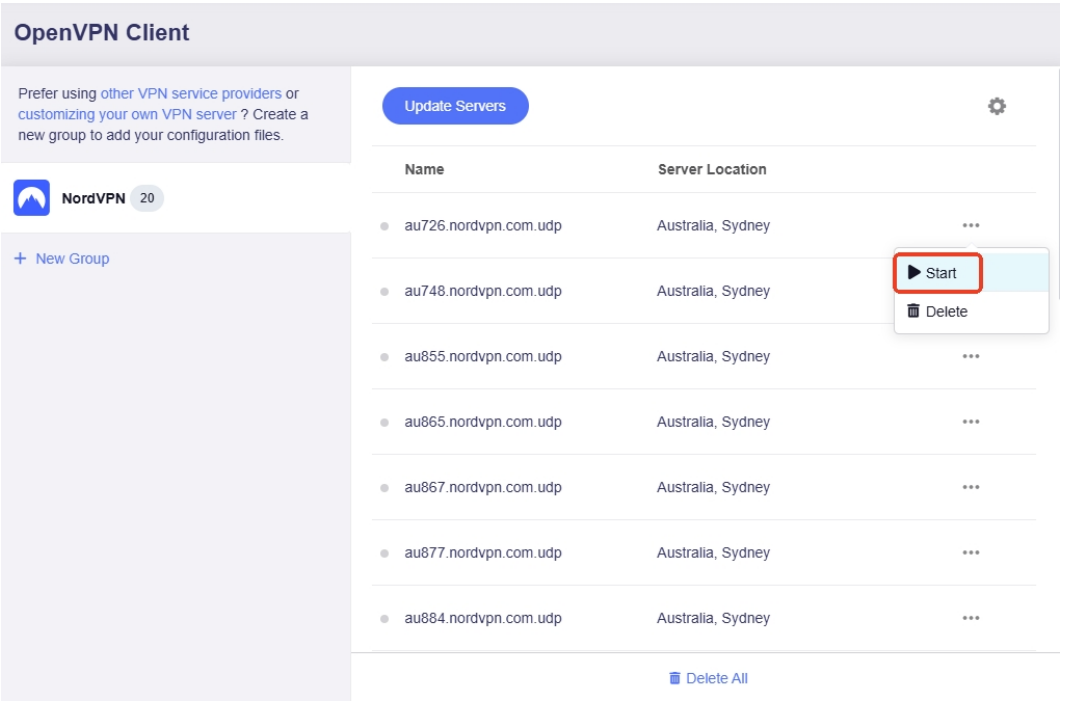


It will download configuration files.

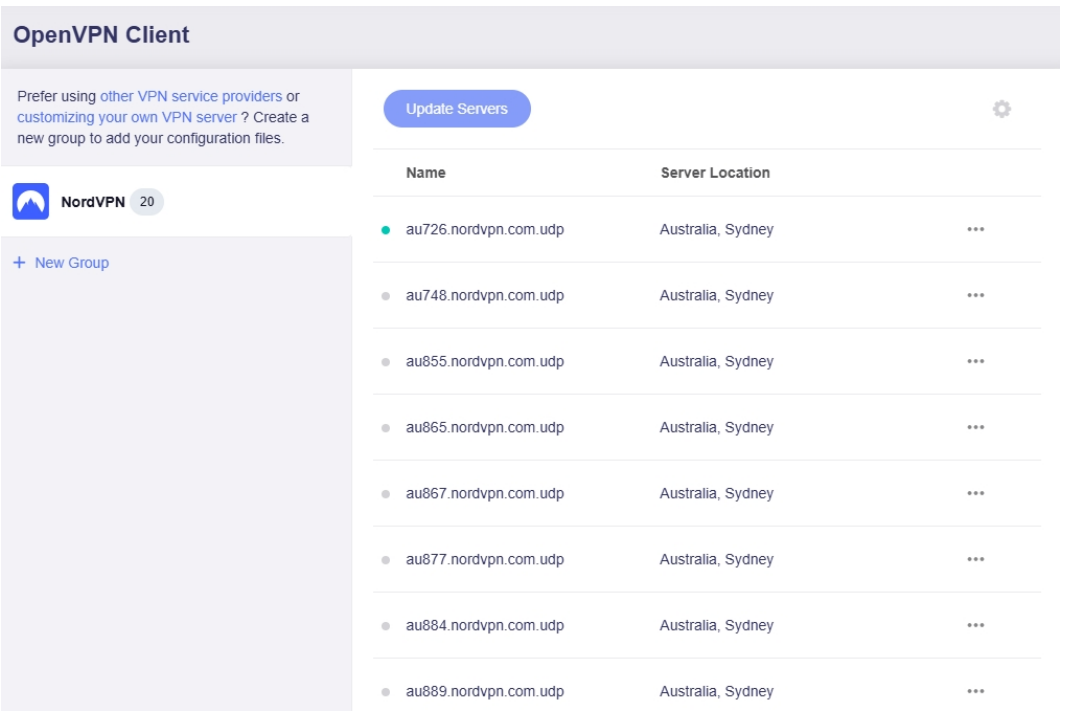


5. Start a connection.

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



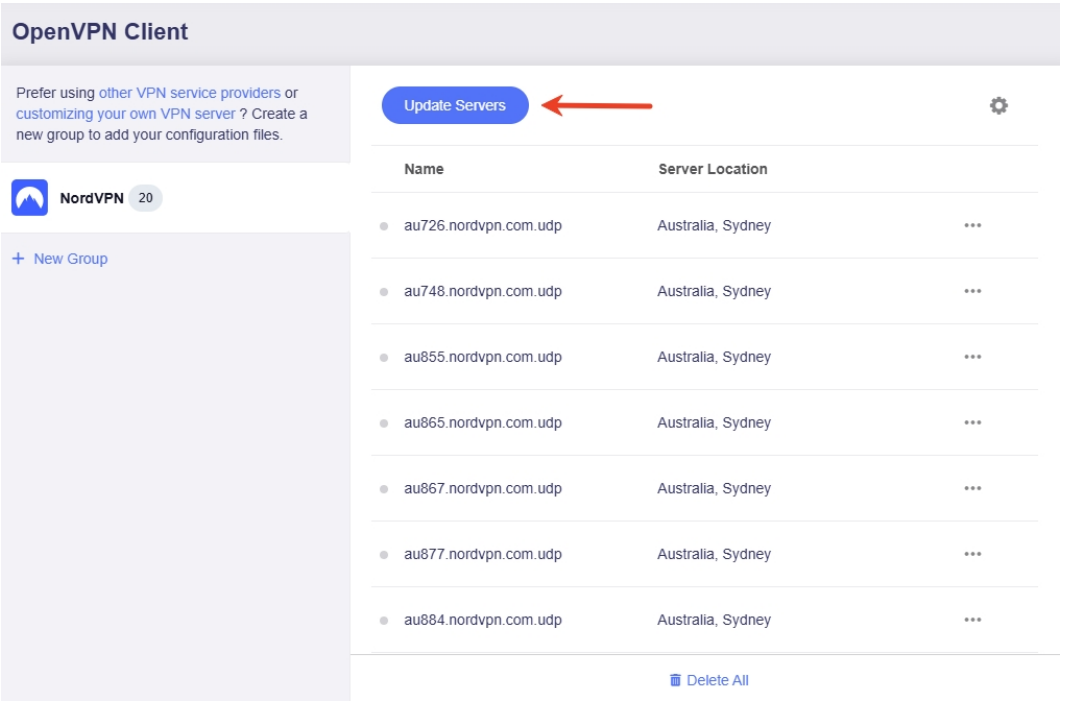
6. Once connected, a green dot will appear next to the configuration file.



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

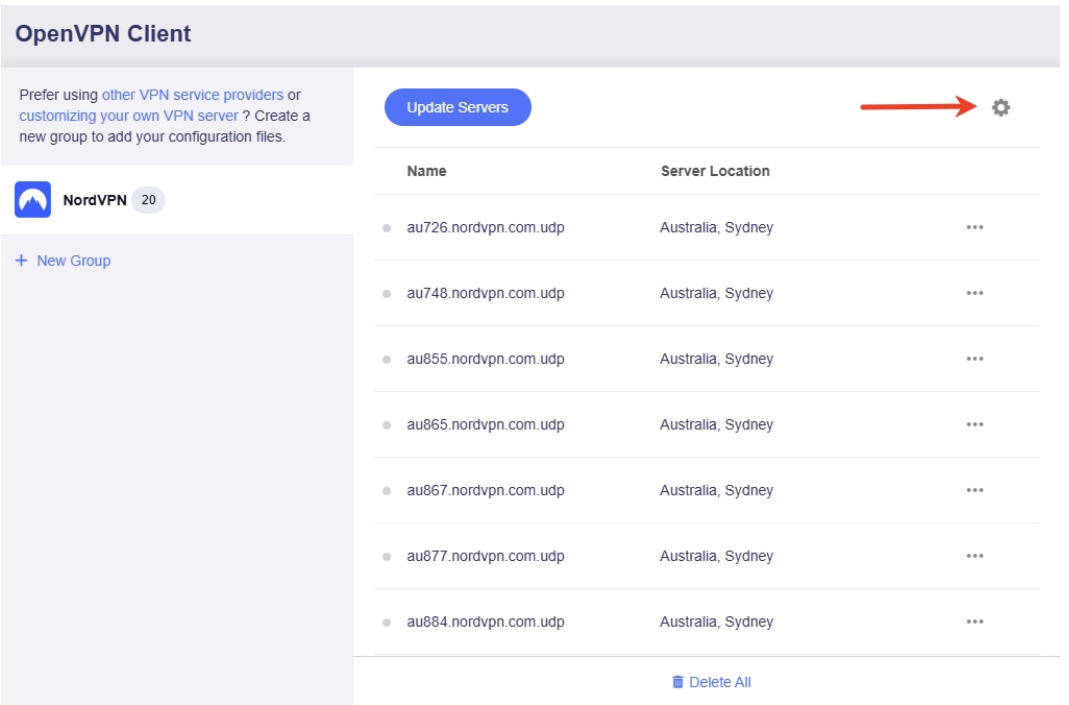
7. Update servers.

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



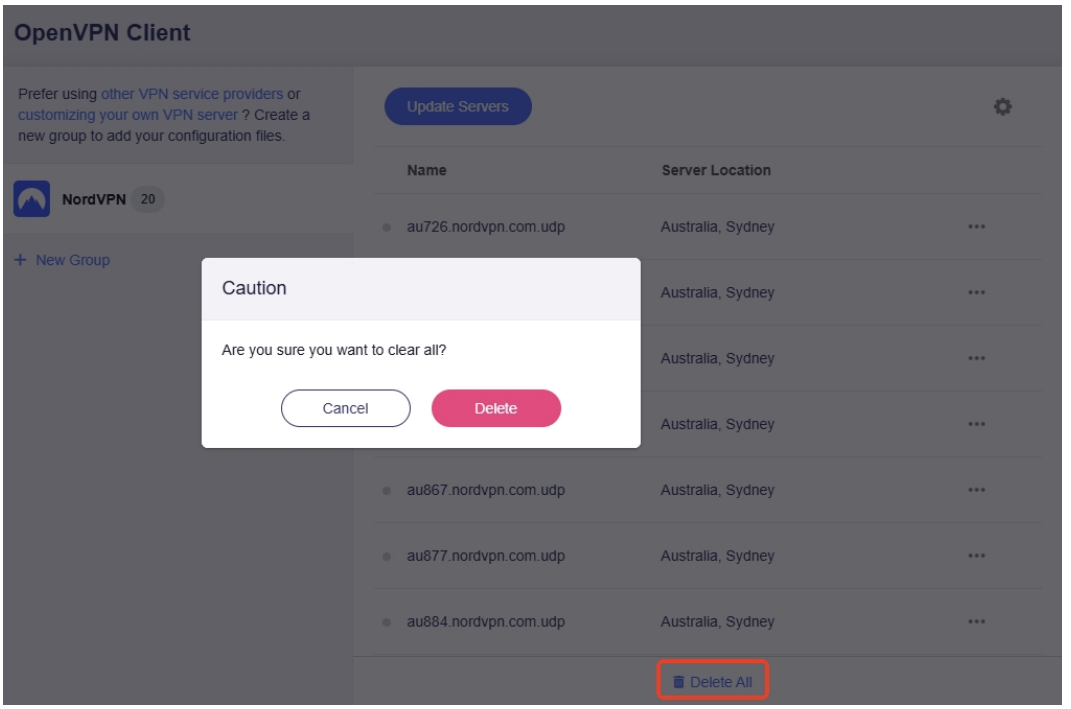
8. Edit credentials.

   Click the gear icon to edit your login credentials.



9. Delete all files.

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

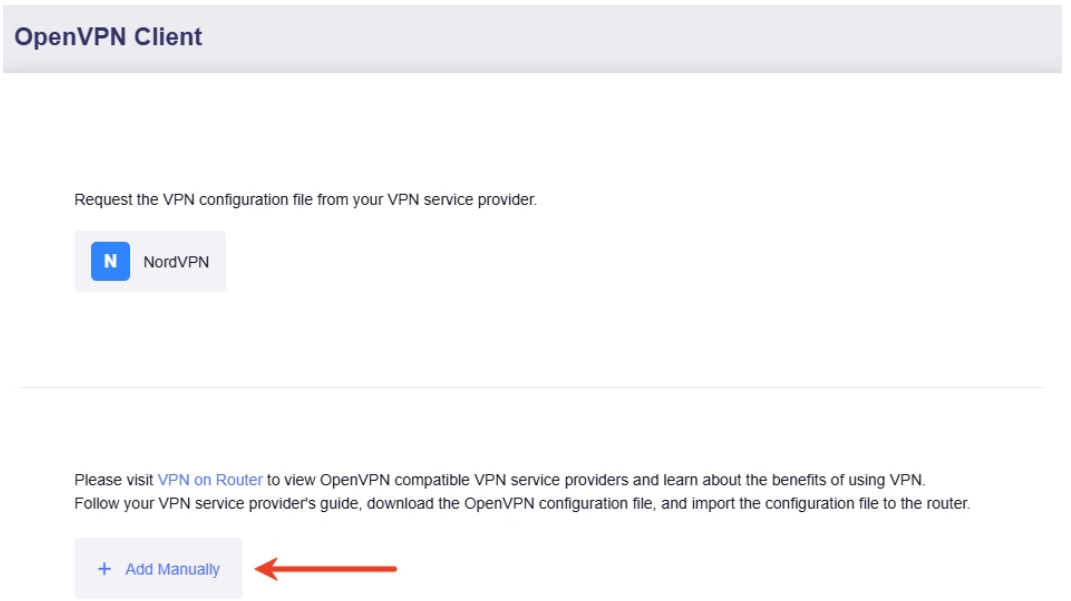

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

11.1.3 Set Up OpenVPN Client Manually (for other providers)

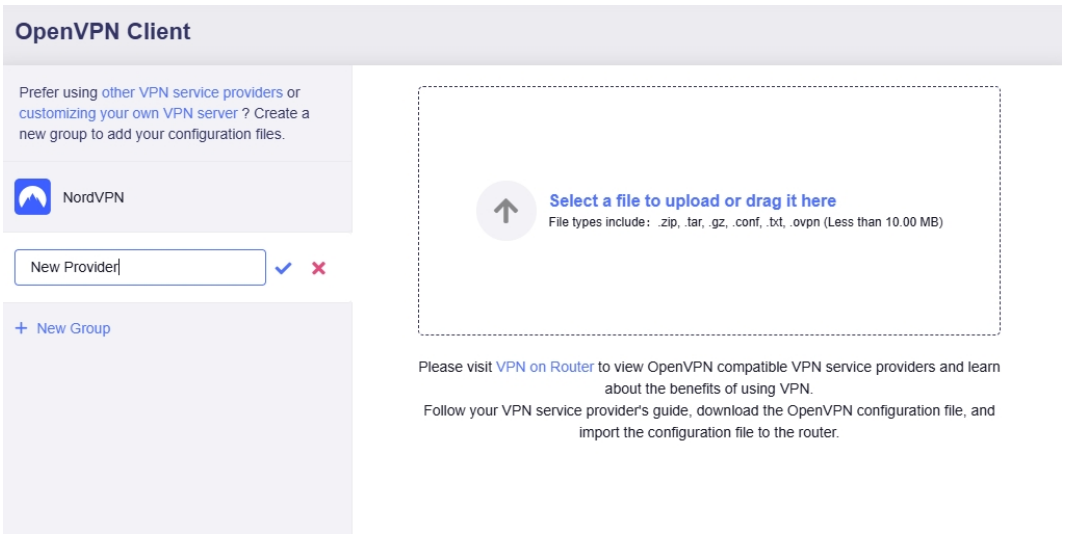
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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

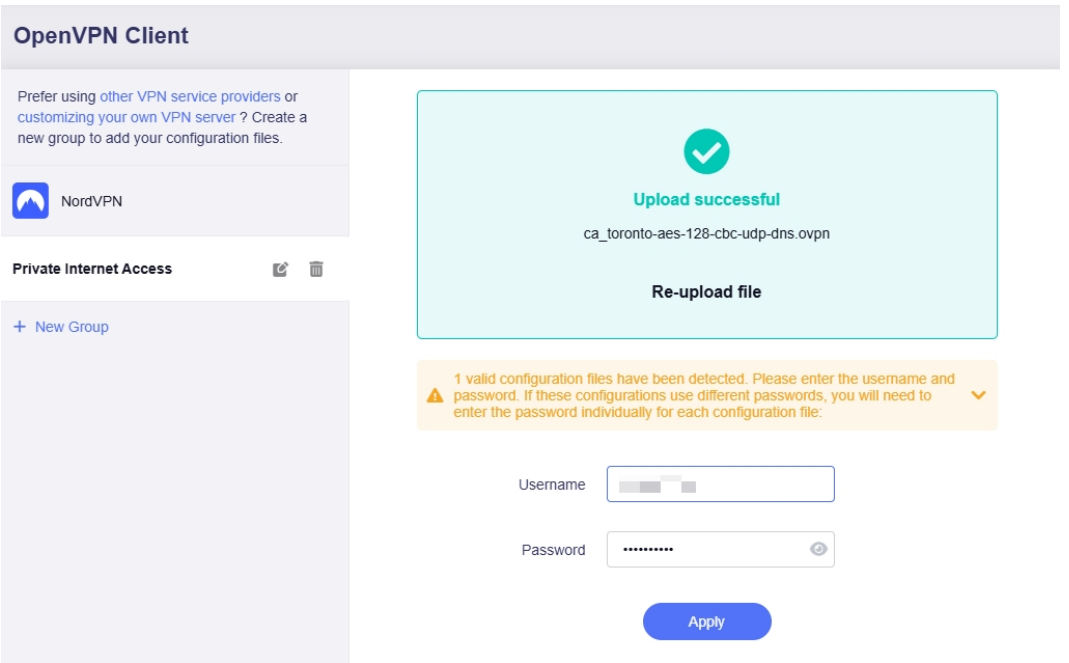
1. Download a configuration file from Private Internet Access official website.
2. Log in to your router's web admin panel, navigate to **VPN** > **OpenVPN Client**, and click **Add Manually**.



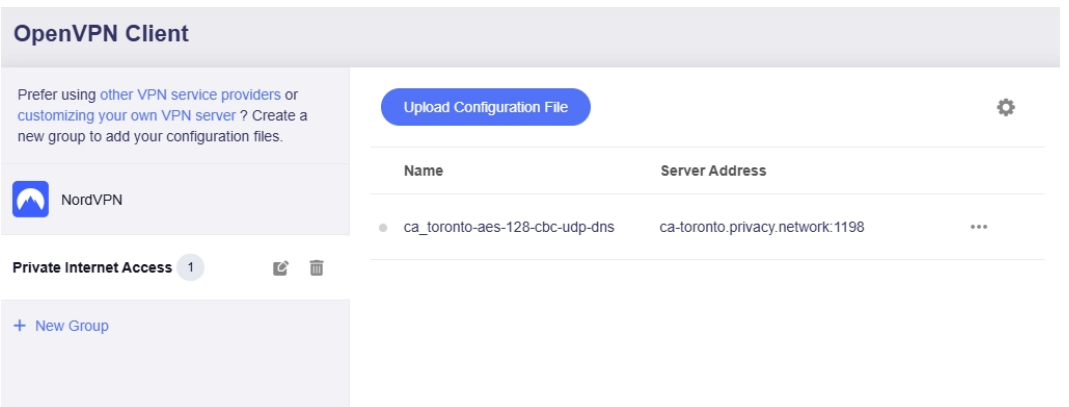
3. It will create a group on the left sidebar. Set a descriptive name for the group.



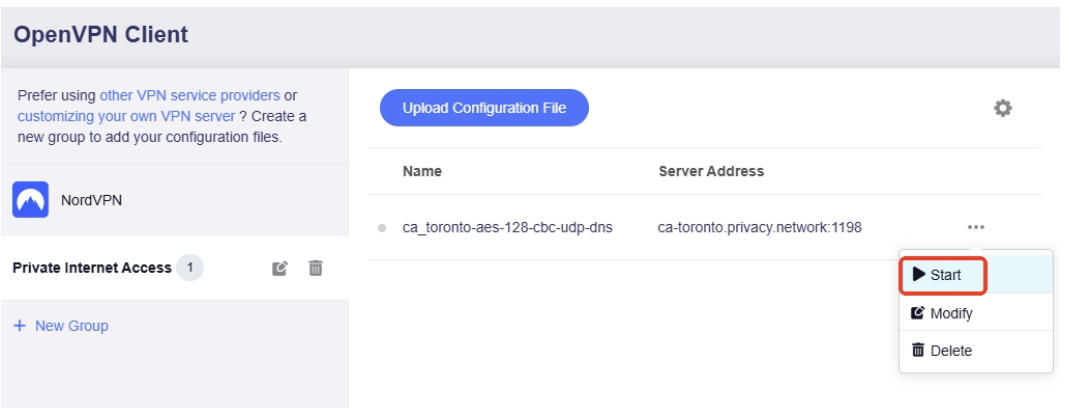
4. Upload your OpenVPN configuration file. Input the credentials if required, then click **Apply**.



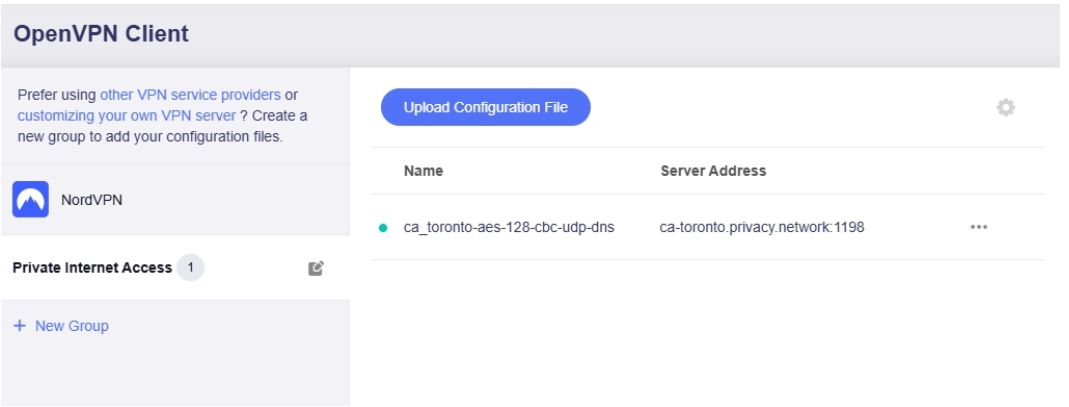
You will see the configuration file uploaded.



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



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



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

11.2 Set Up WireGuard Client

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

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

11.2.1 Preparation

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

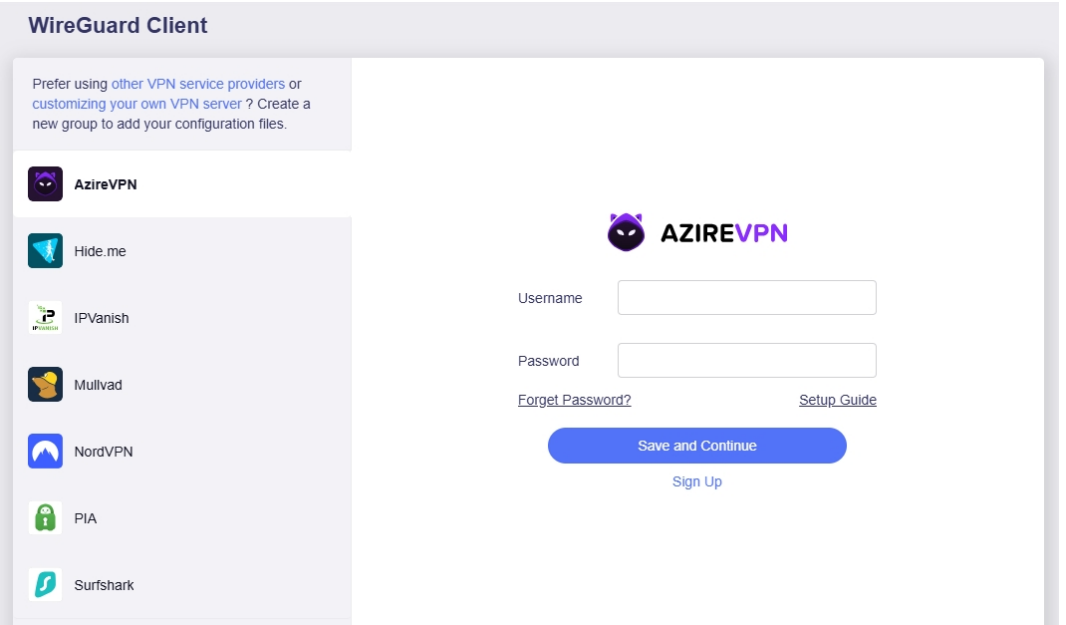
Next, select the corresponding WireGuard service provider below to quickly locate the step-by-step instructions.

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

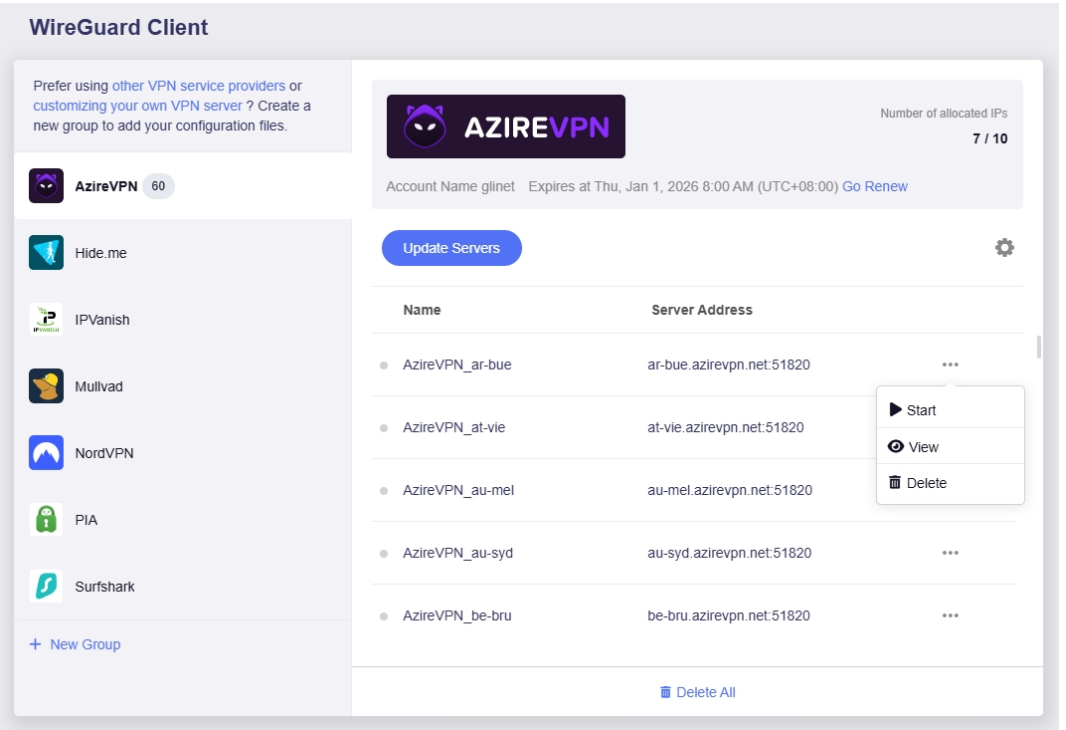
11.2.2 Set Up AzireVPN

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

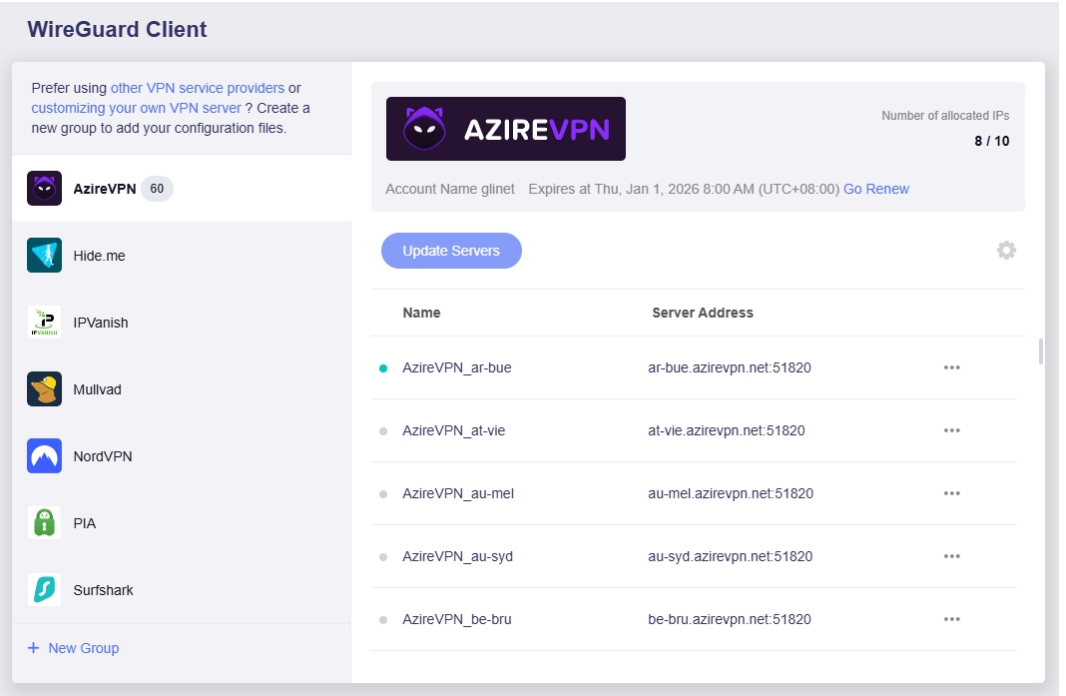
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **AzireVPN**.
2. Input Username and Password, then click **Save and Continue**. It will generate configuration files for each server.



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



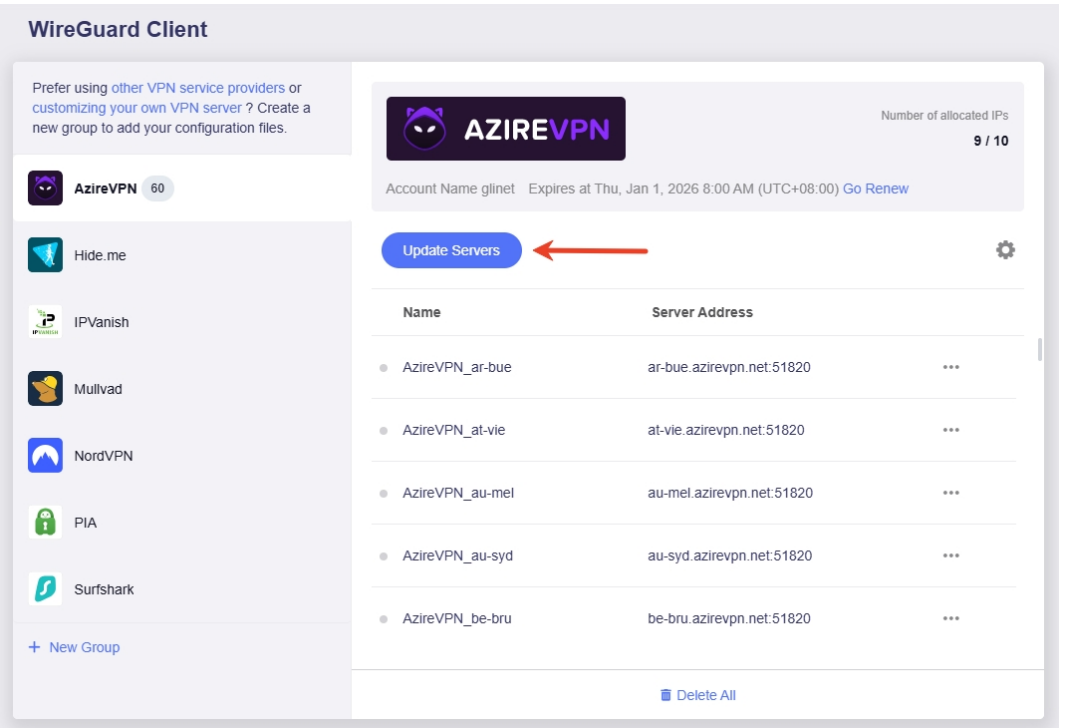
4. Once connected, a green dot will appear next to the configuration file.



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

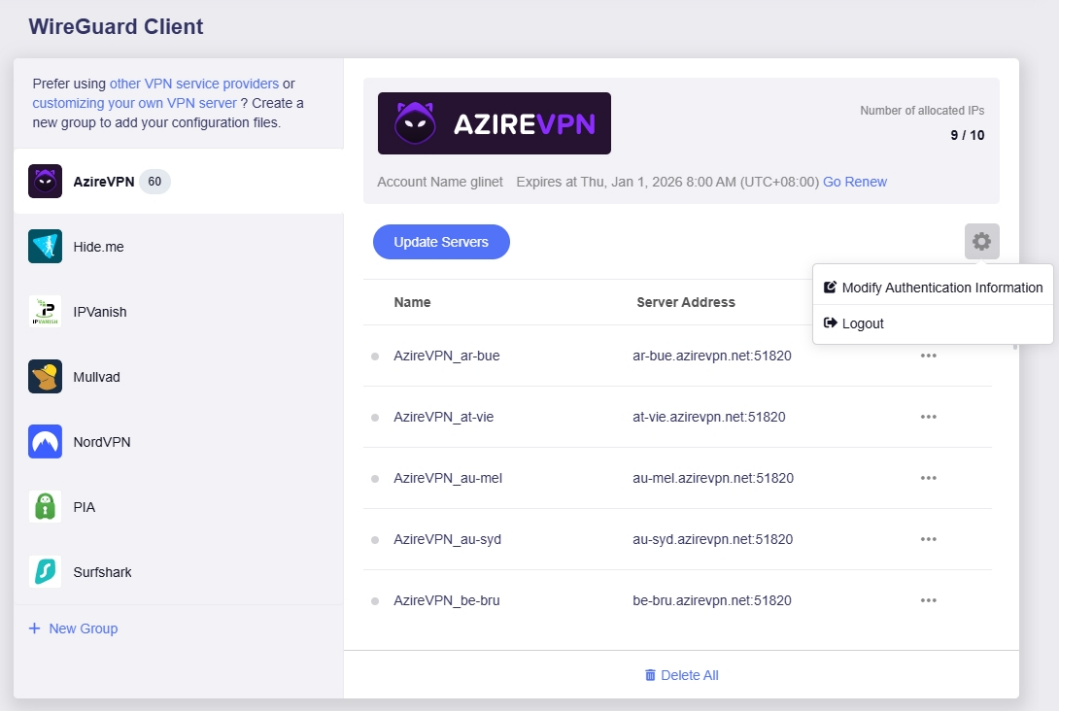
5. Update servers.

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



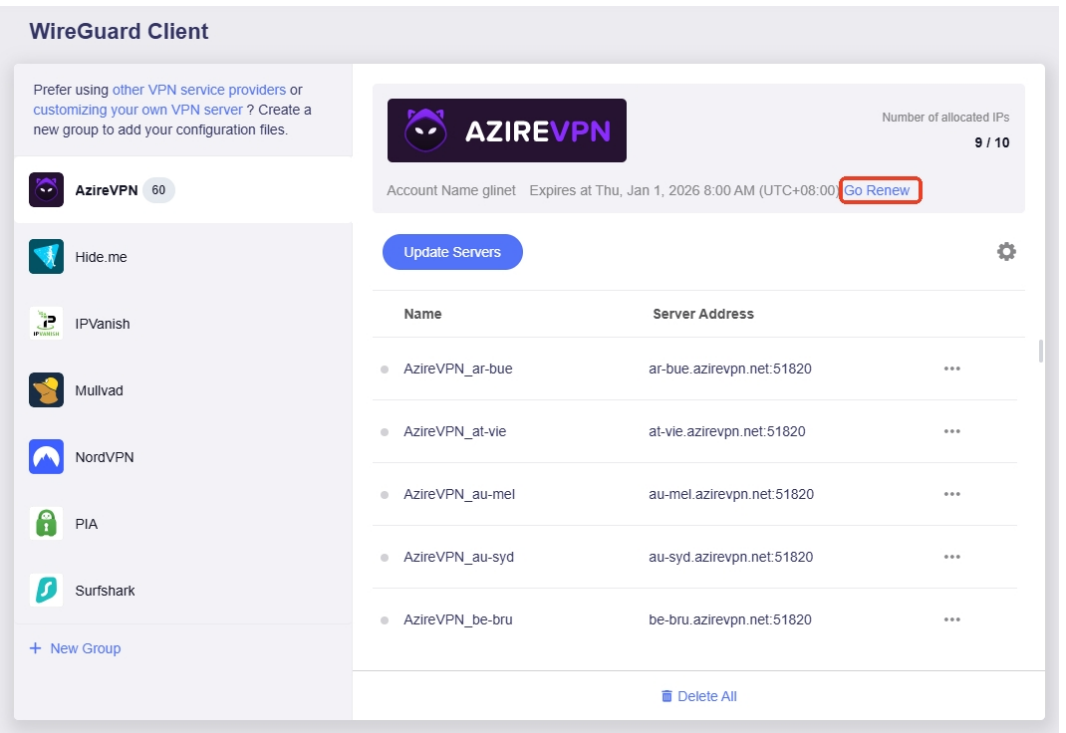
6. Edit credentials or logout.

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



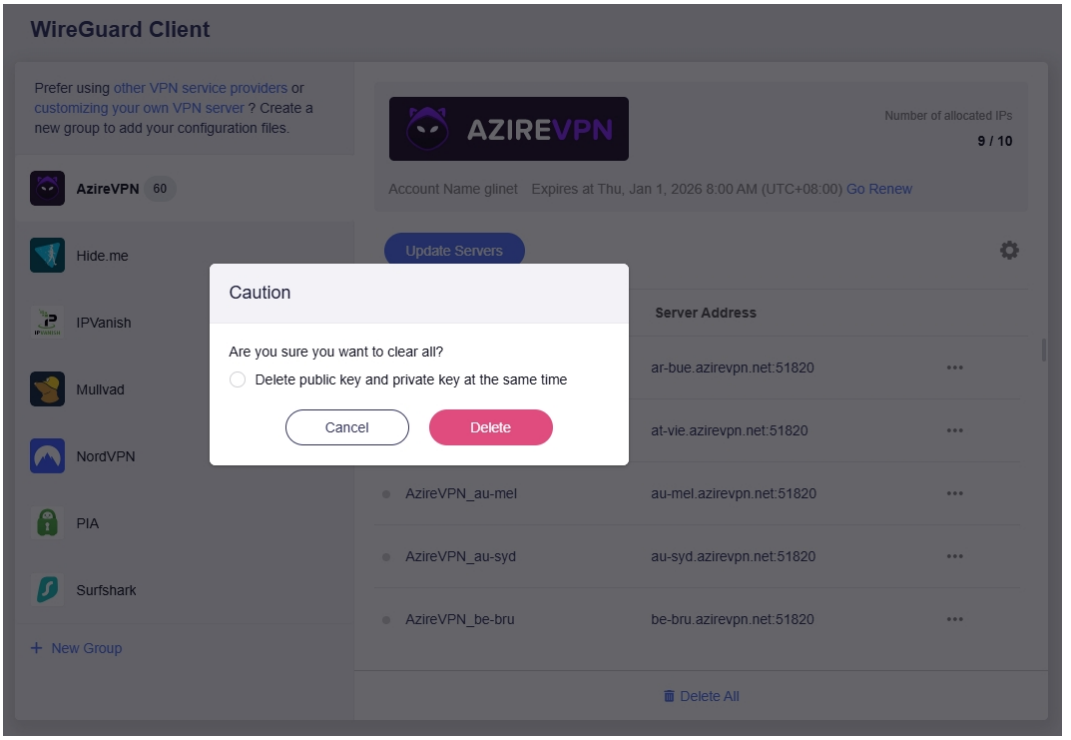
7. Go renew.

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



8. Delete all files.

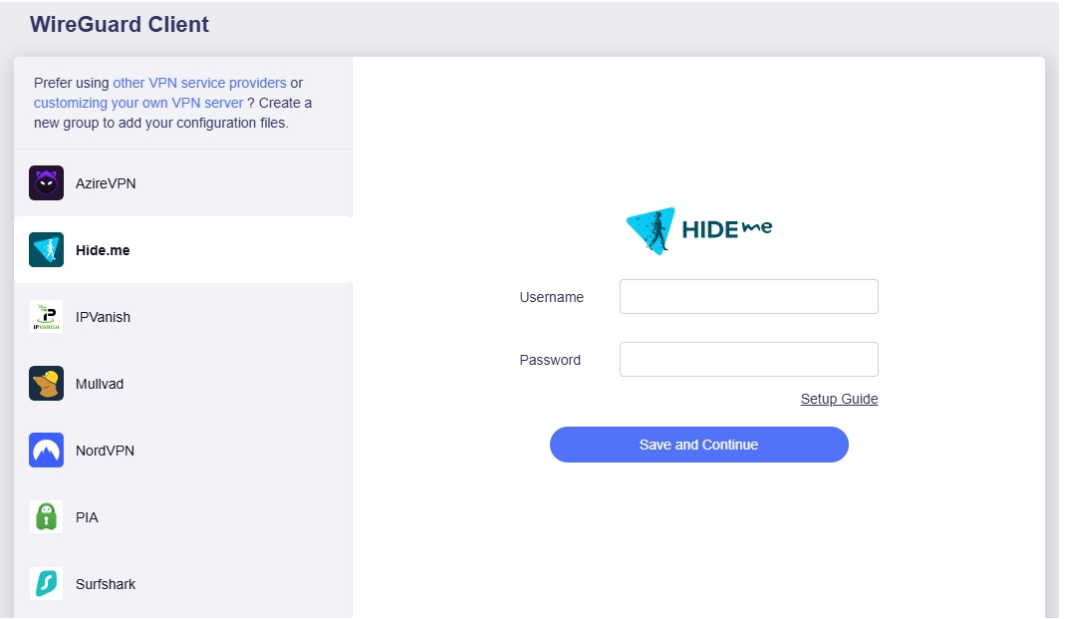
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



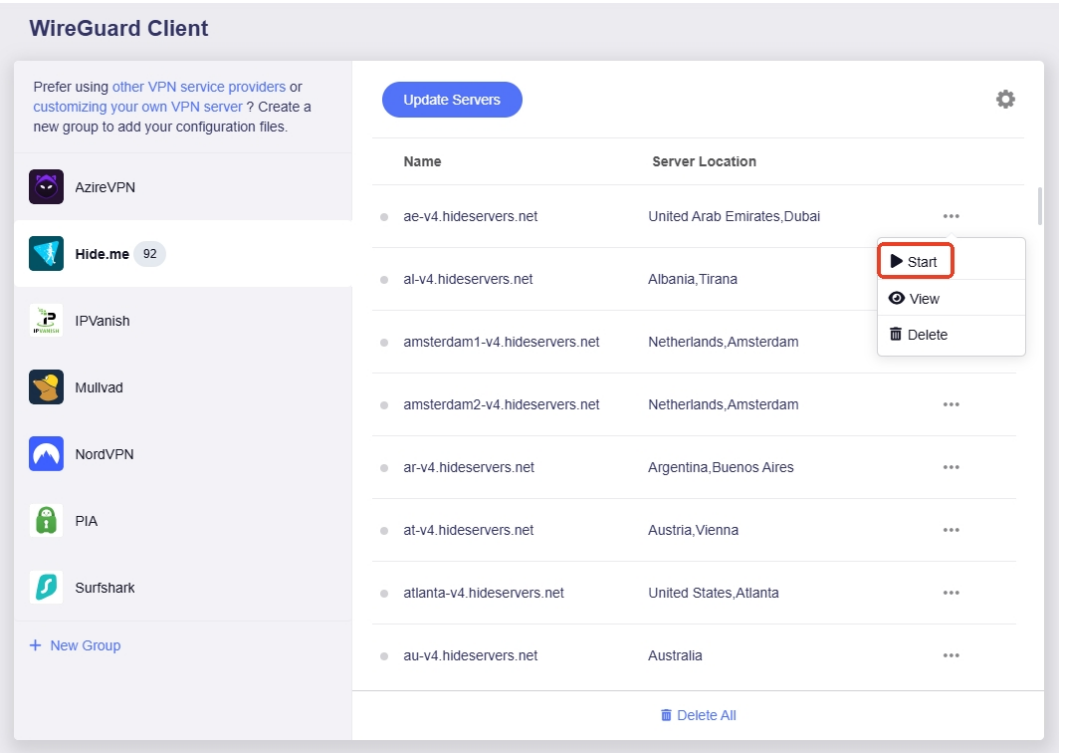
11.2.3 Set Up Hide.me

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

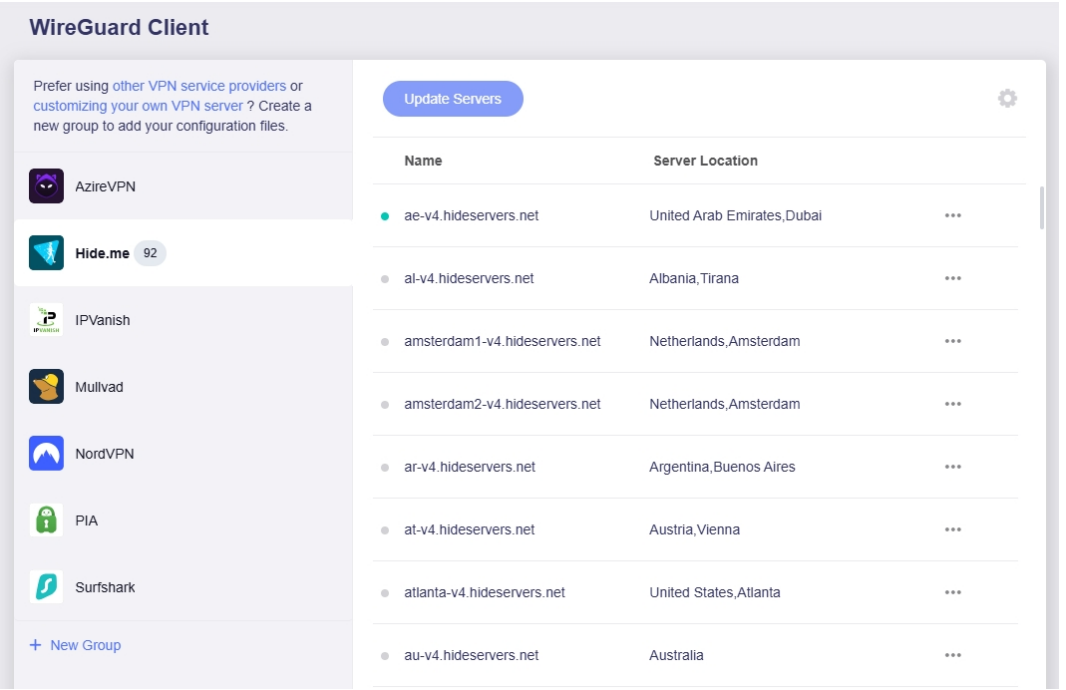
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Hide.me**.
2. Input Username and Password, then click **Save and Continue**. It will generate configuration files for each server.



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



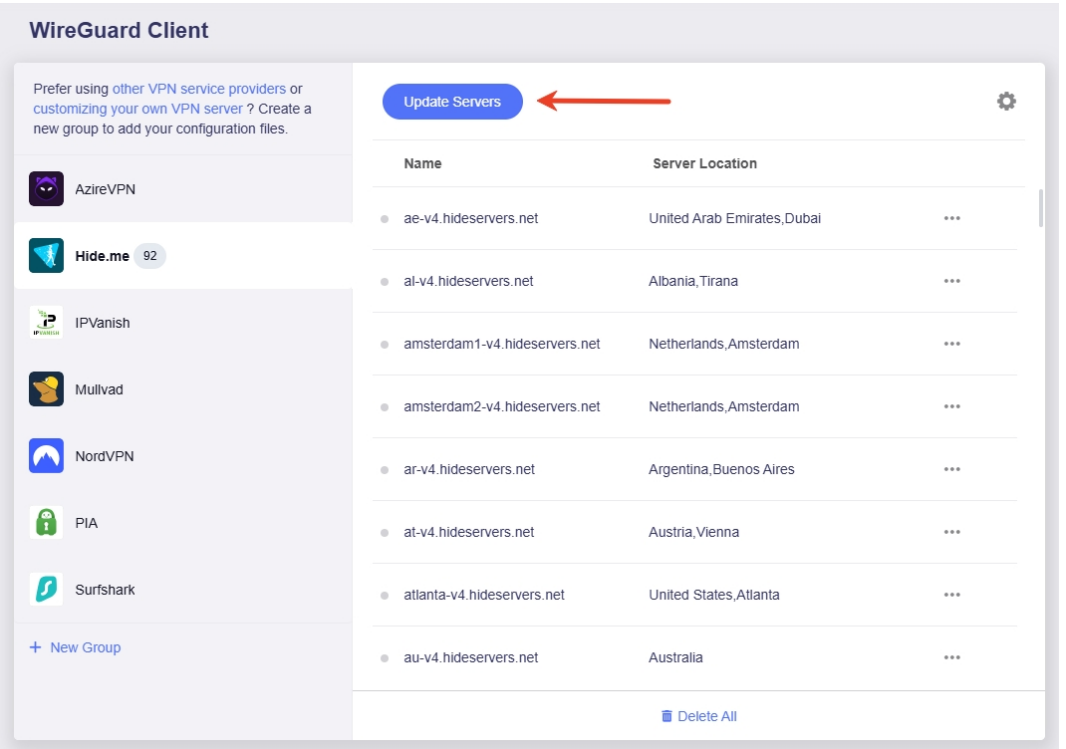
4. Once connected, a green dot will appear next to the configuration file.



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

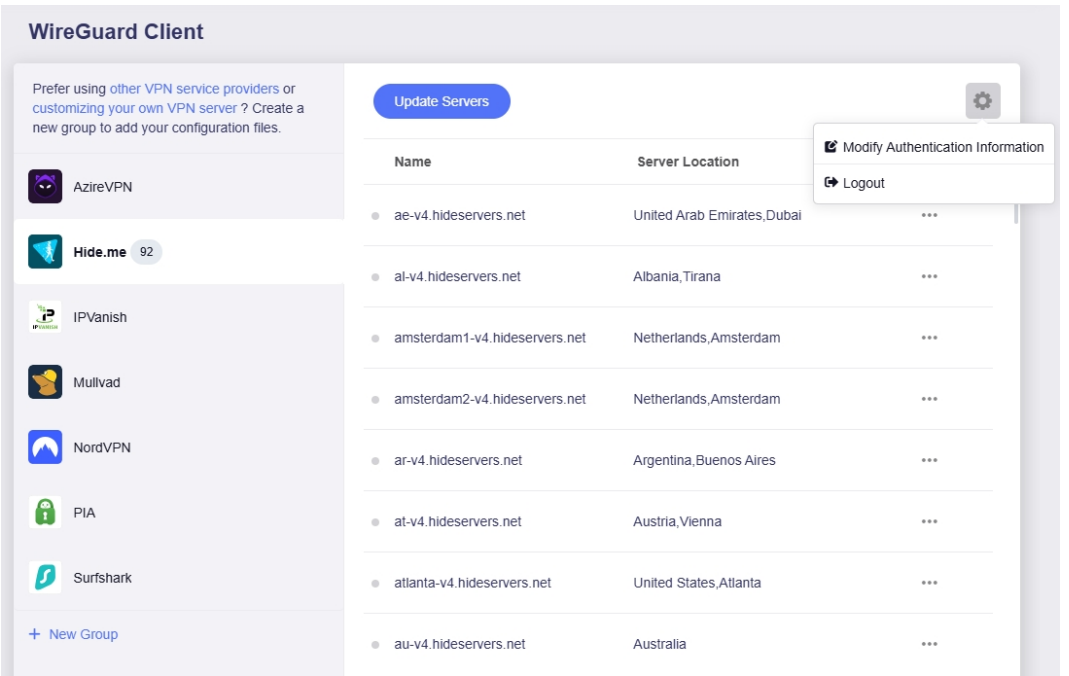
5. Update servers.

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



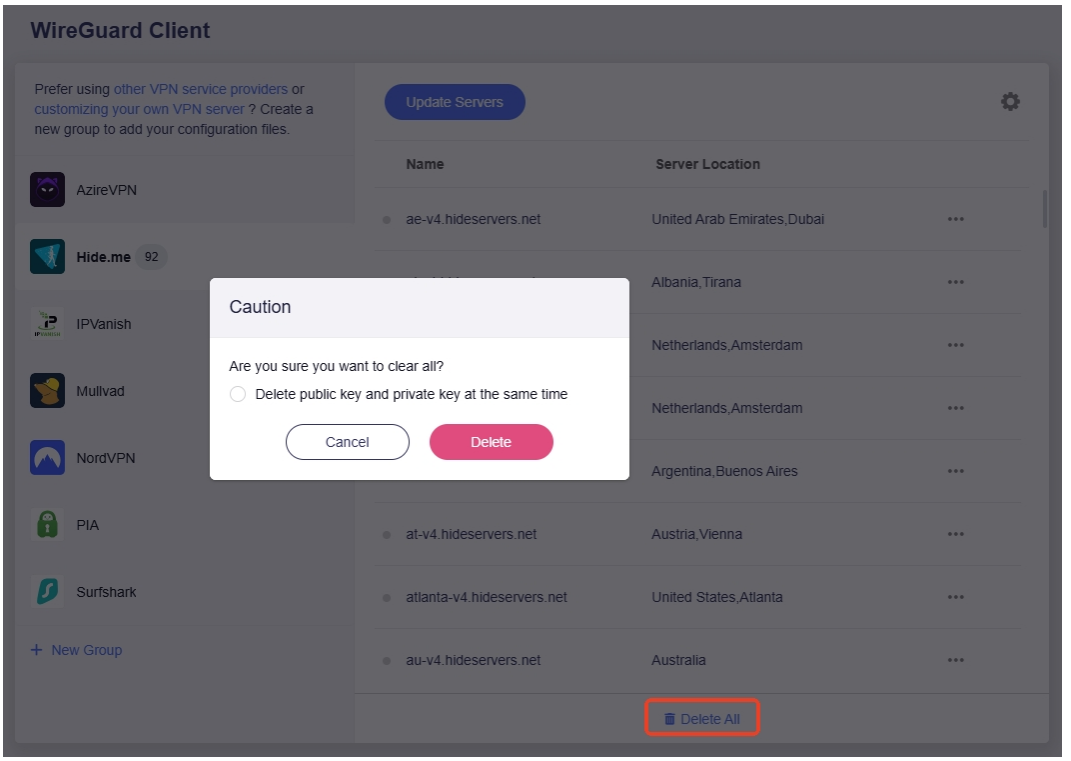
6. Edit credentials or logout.

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



7. Delete all files.

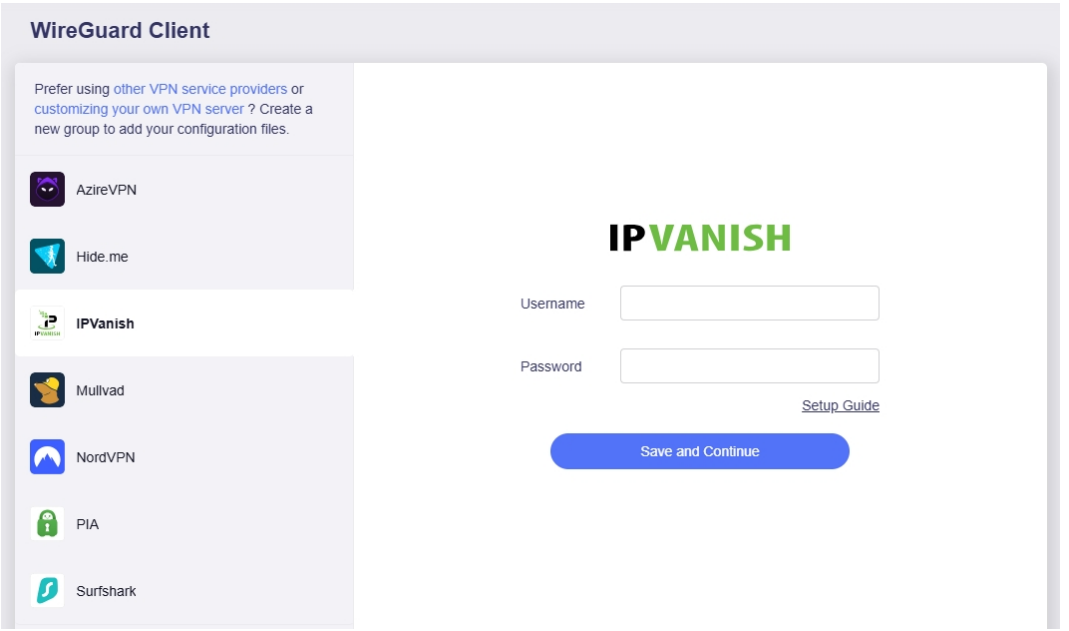
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



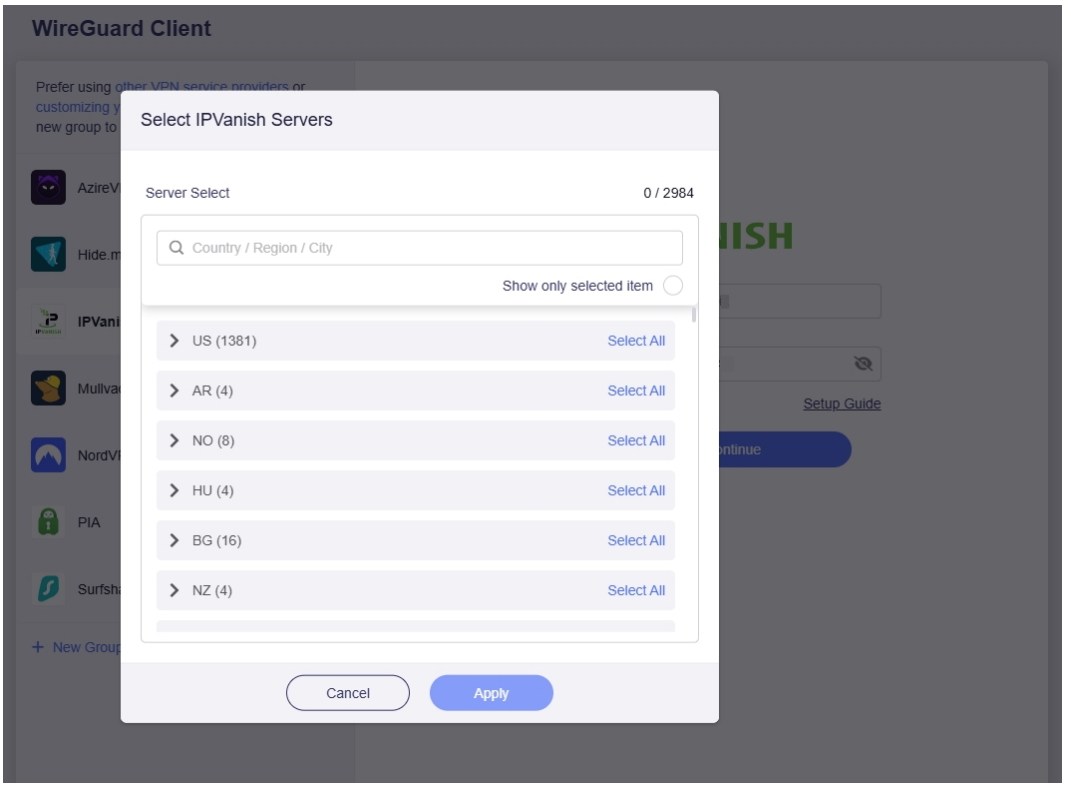
11.2.4 Set Up IPVanish

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

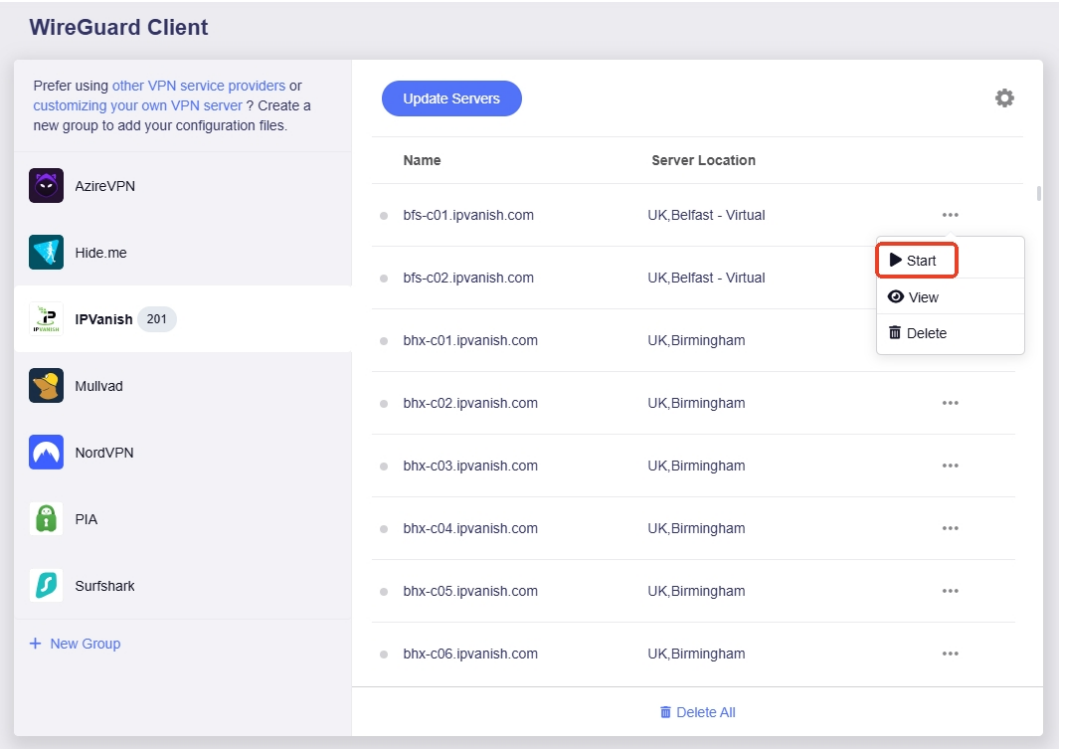
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **IPVanish**.
2. Input Username and Password, then click **Save and Continue**.



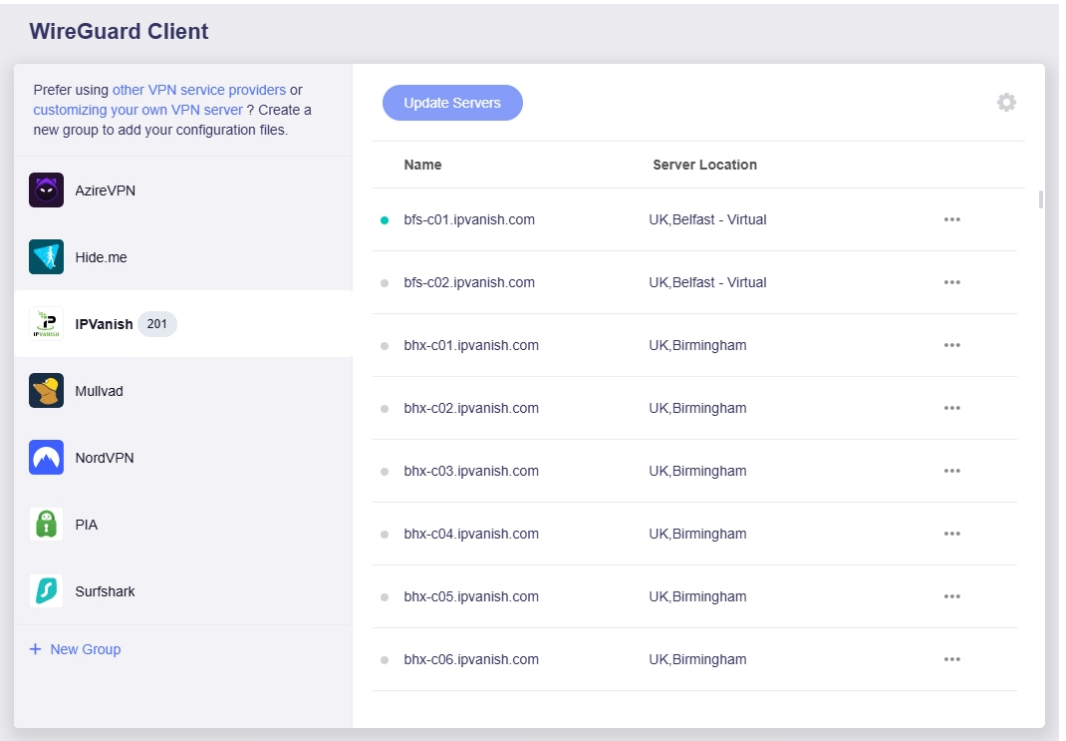
3. Select the server(s) you want to connect to, and click **Apply**.



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



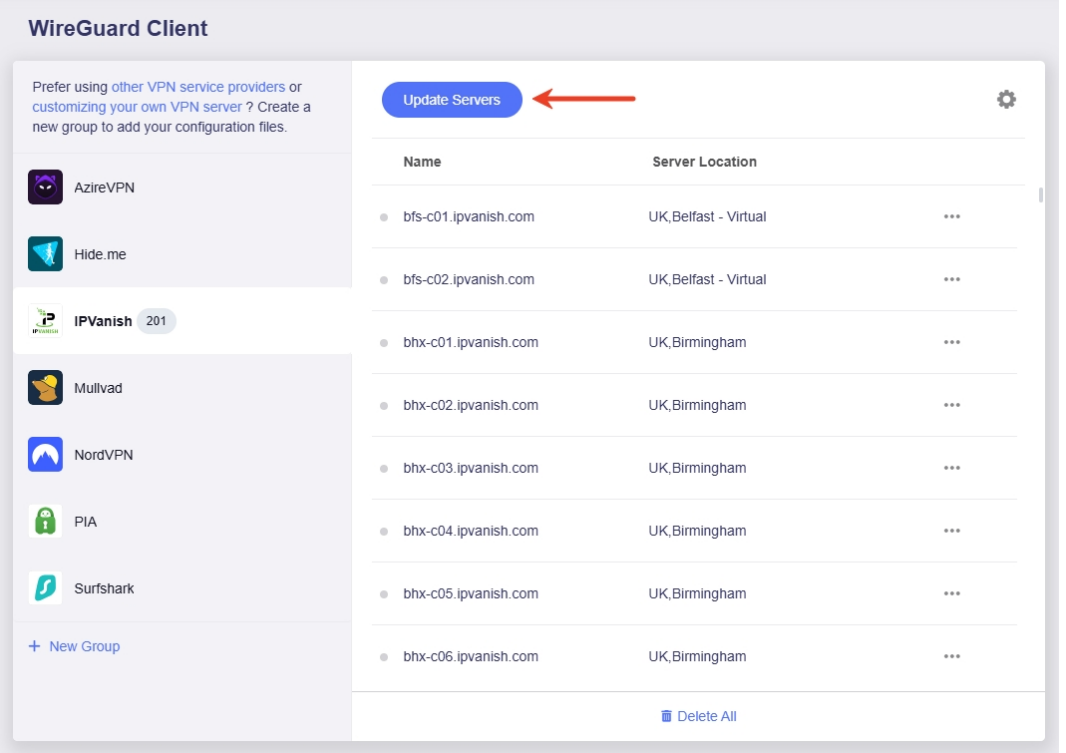
5. Once connected, a green dot will appear next to the configuration file.



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

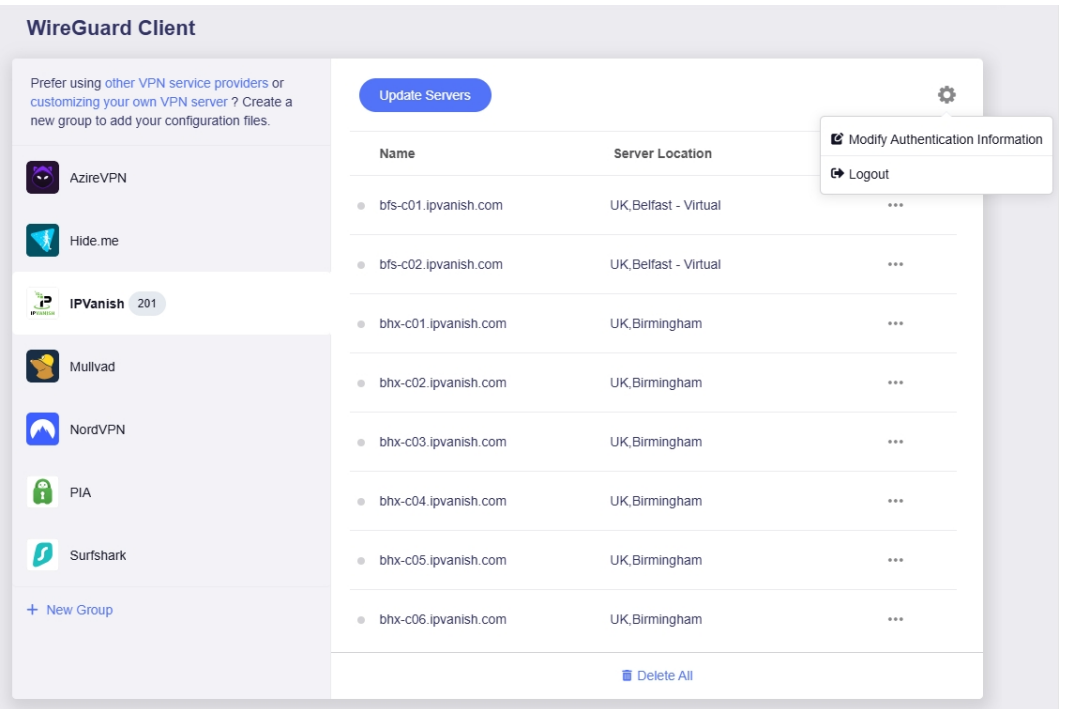
6. Update servers.

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



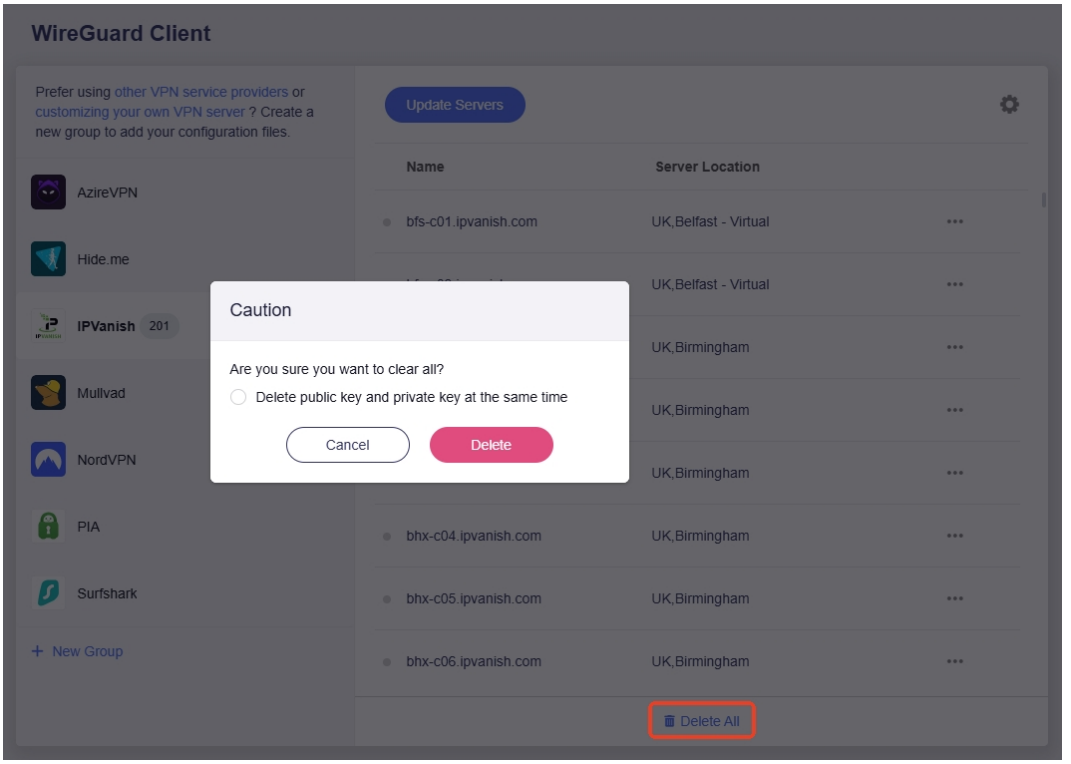
7. Edit credentials or logout.

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



8. Delete all files.

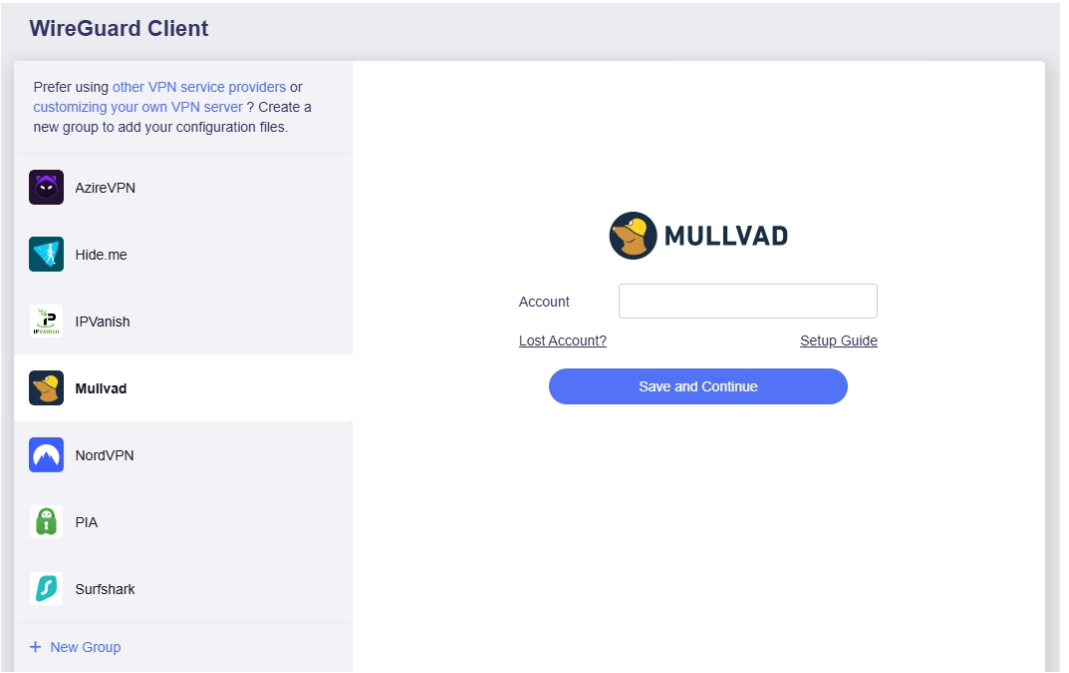
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



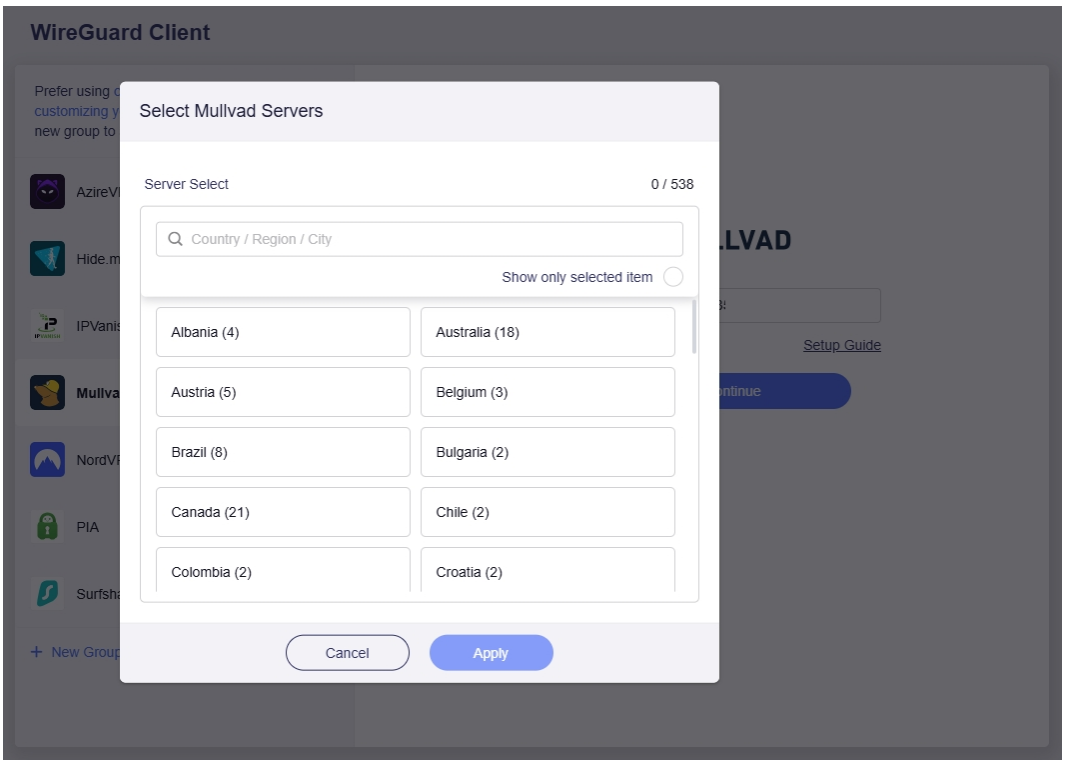
11.2.5 Set Up Mullvad

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

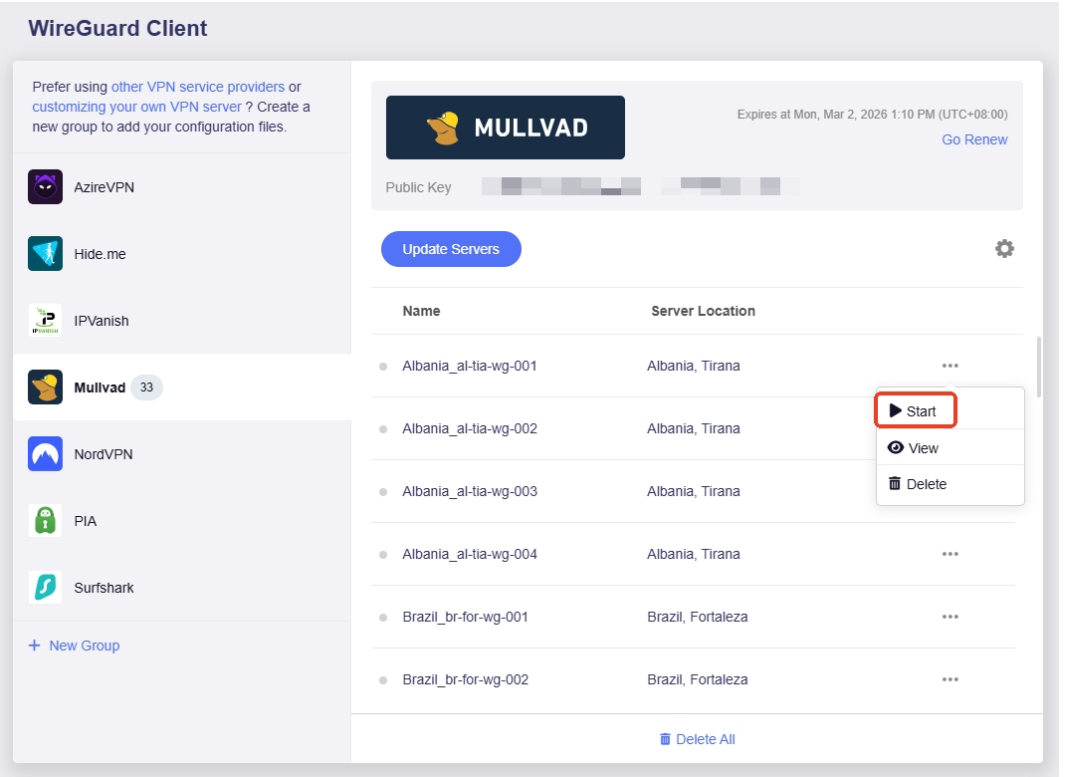
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Mullvad**.
2. Input Username and Password, then click **Save and Continue**.



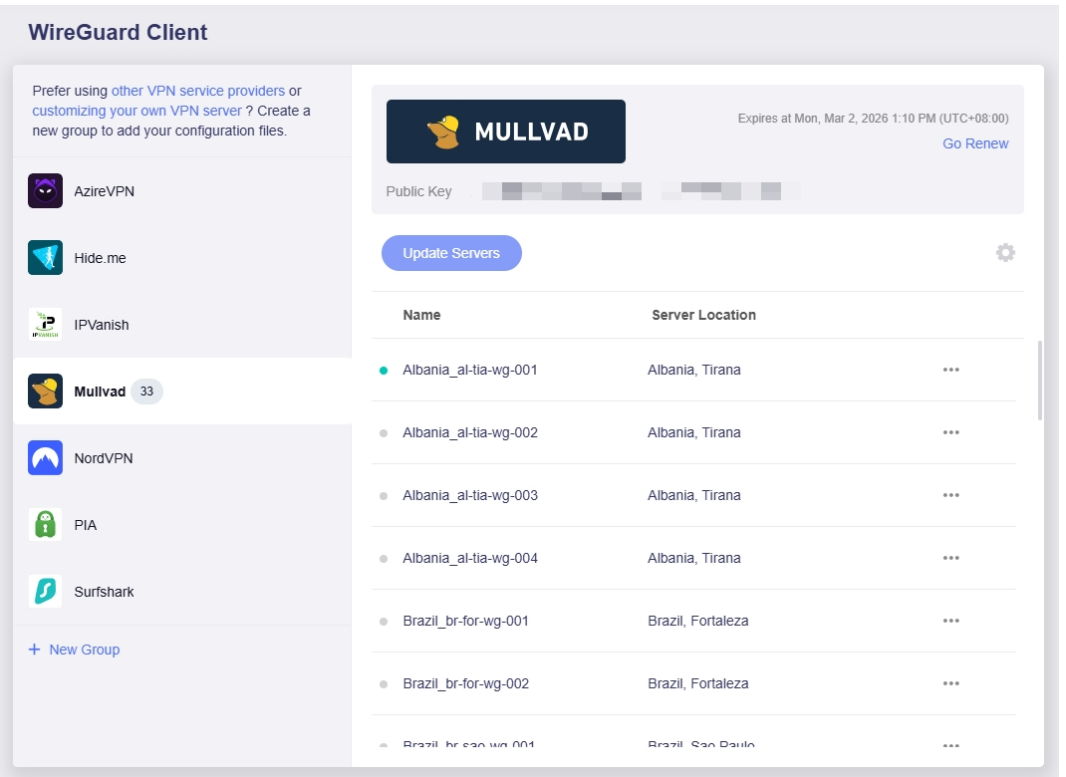
3. Select the server(s) you want to connect to, and click **Apply**.



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



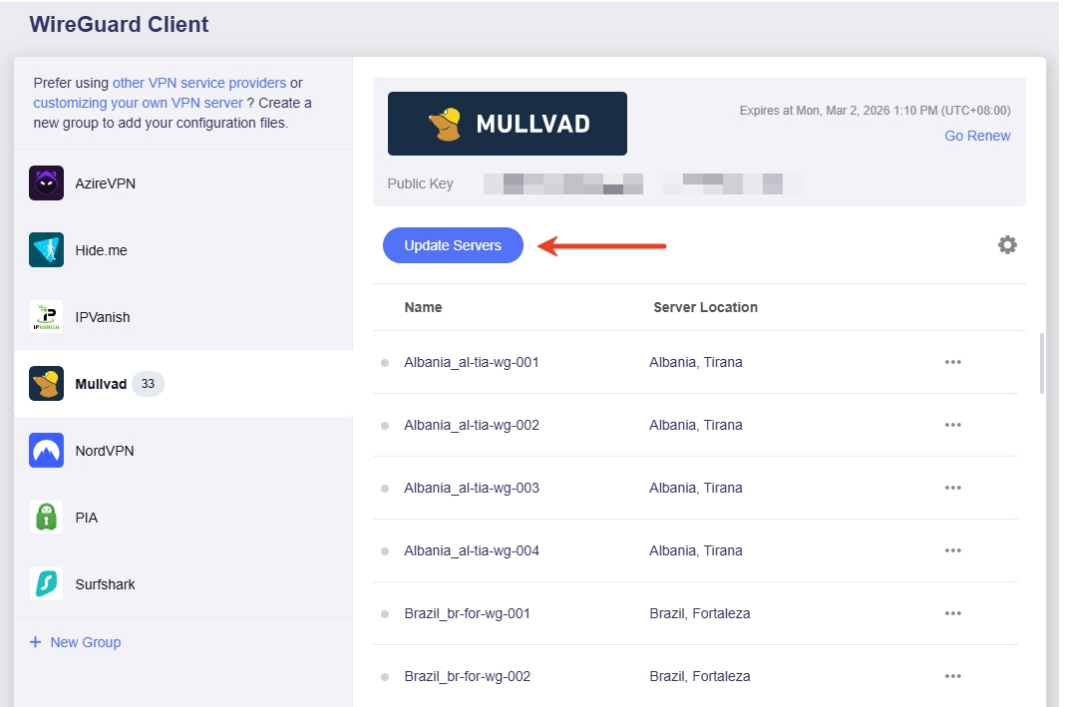
5. Once connected, a green dot will appear next to the configuration file.



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

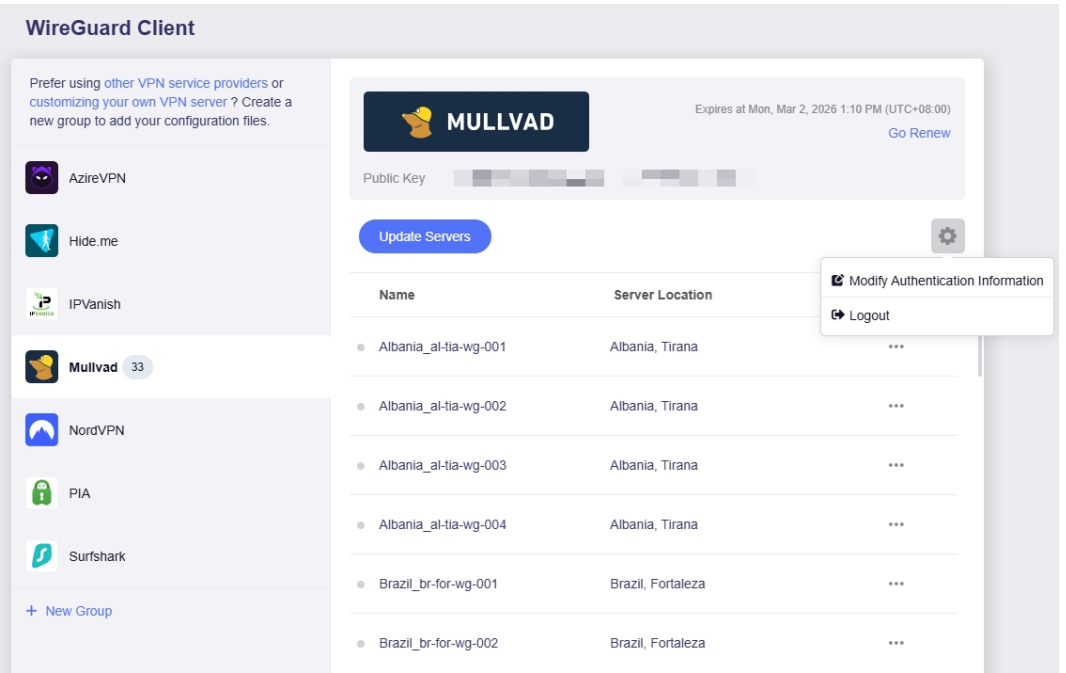
6. Update servers.

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



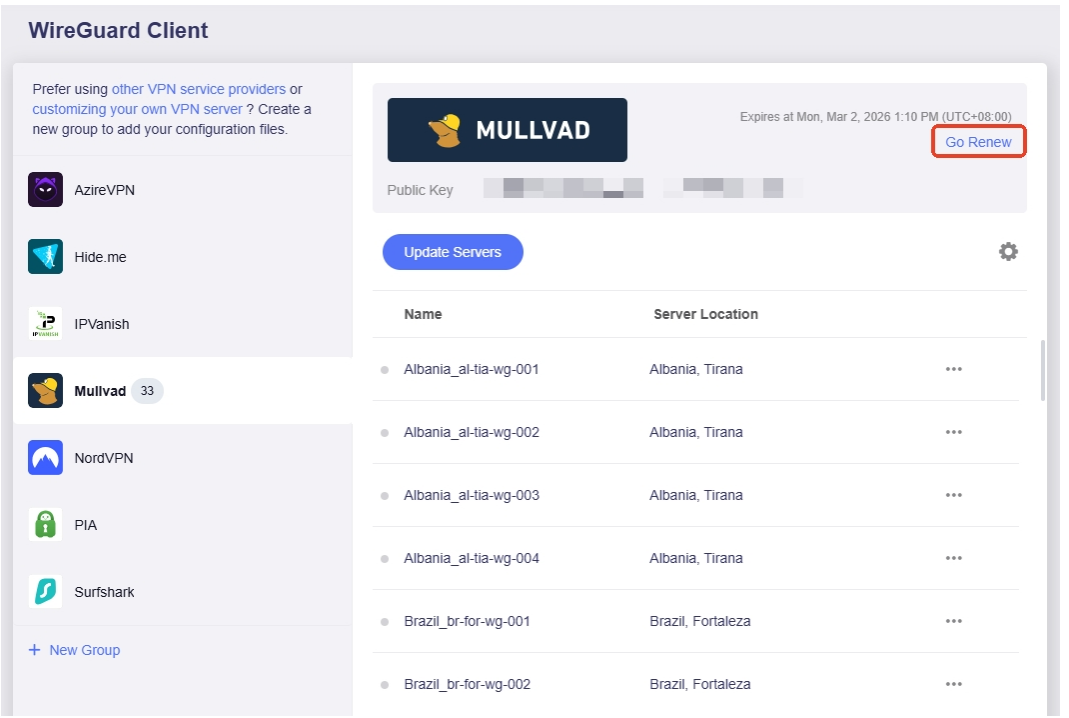
7. Edit credentials or logout.

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



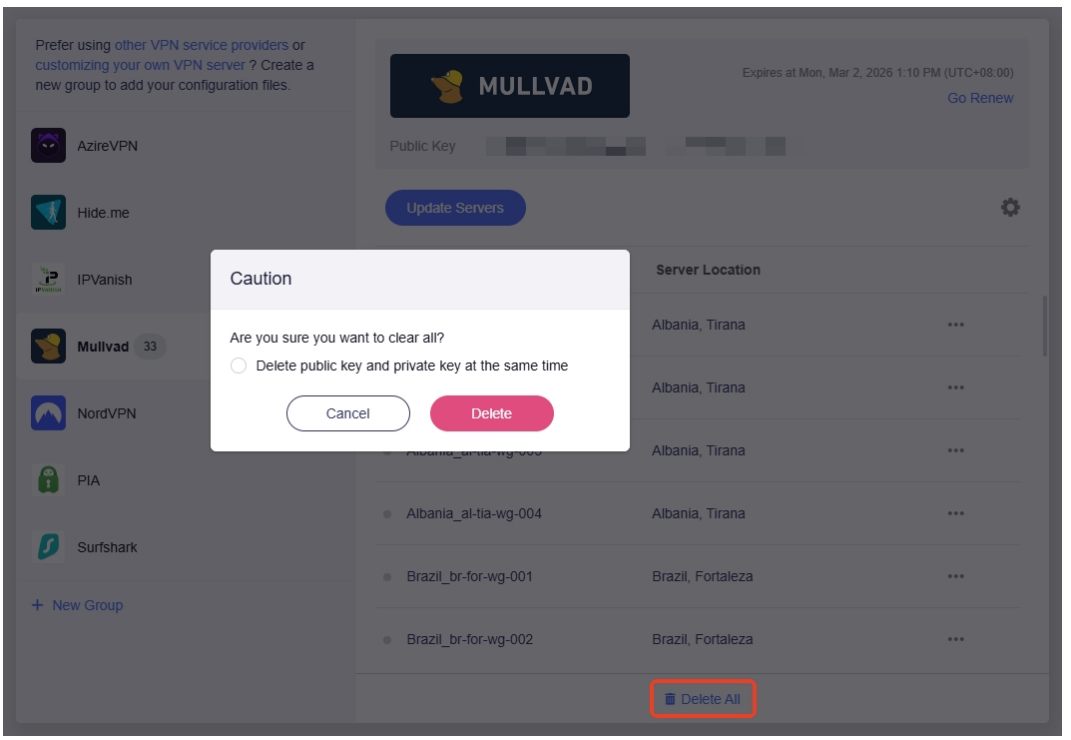
8. Go renew.

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



9. Delete all files.

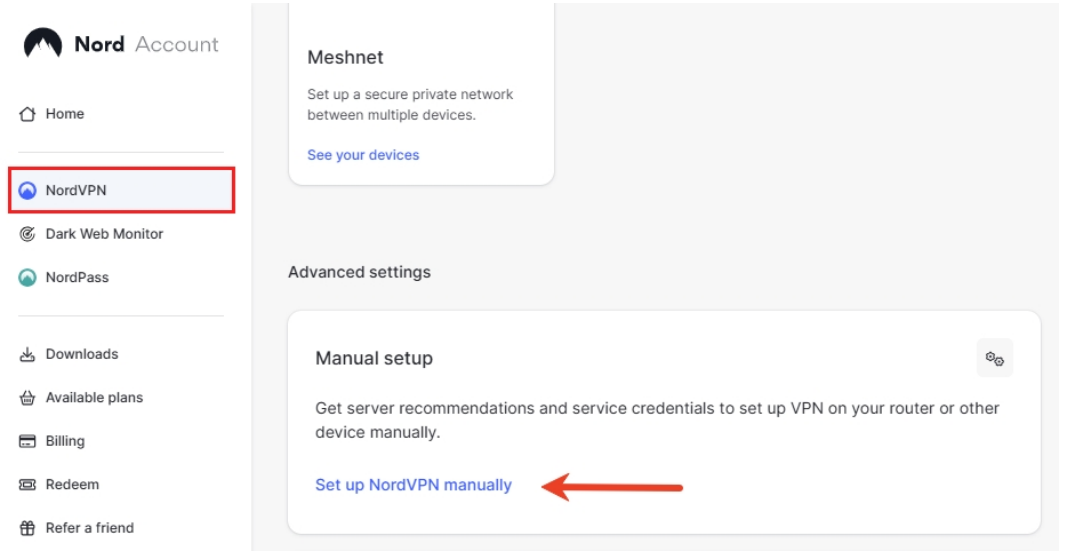
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



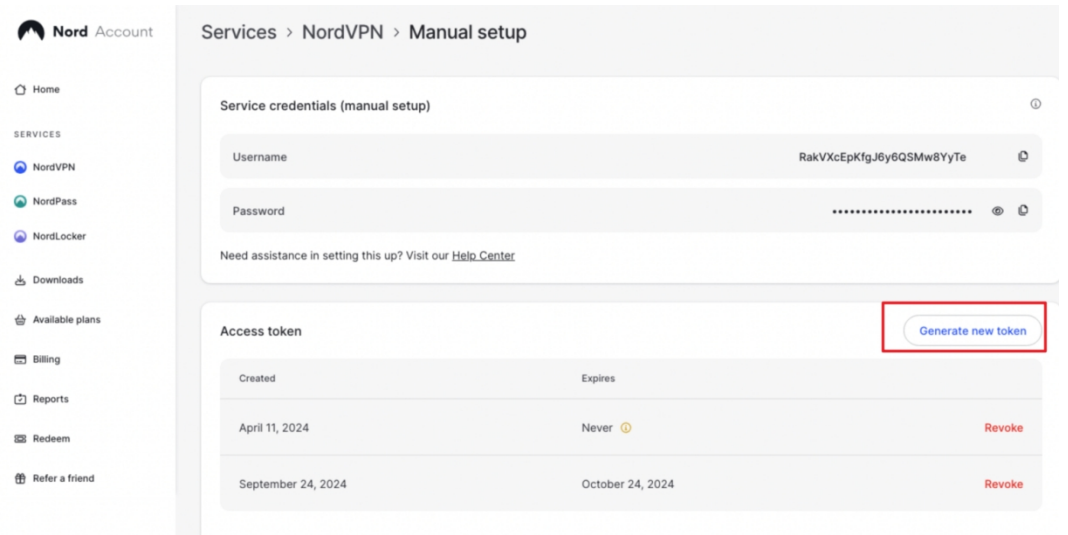
11.2.6 Set Up NordVPN

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

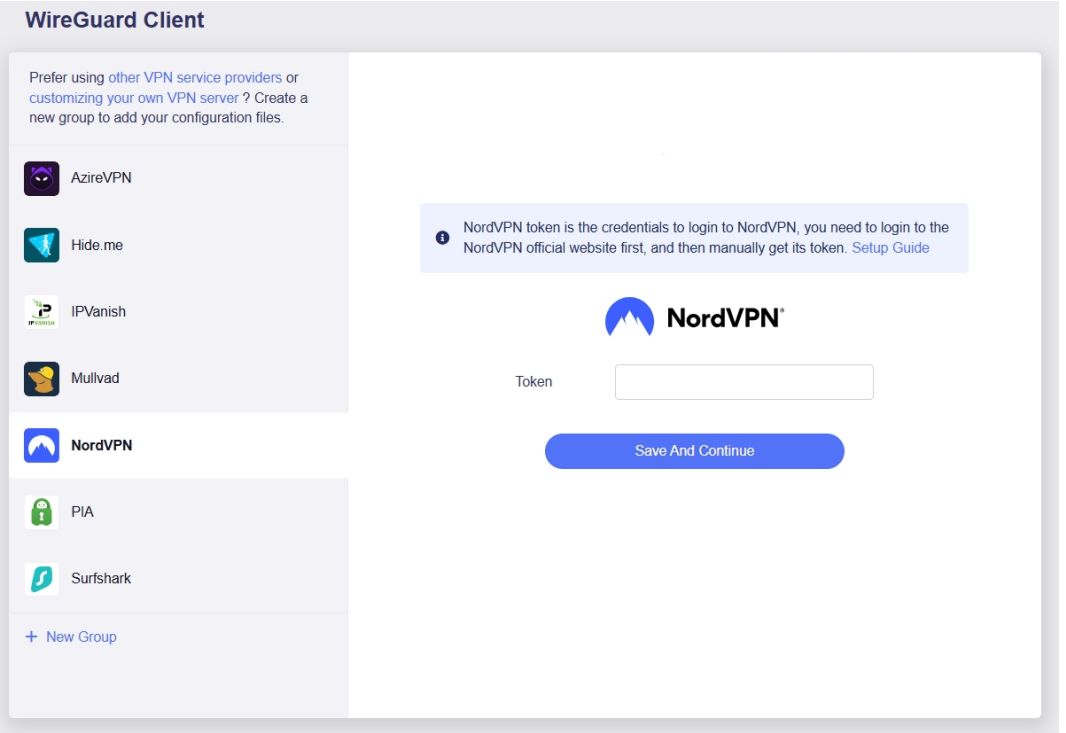
1. Log in to your NordVPN web account here.
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



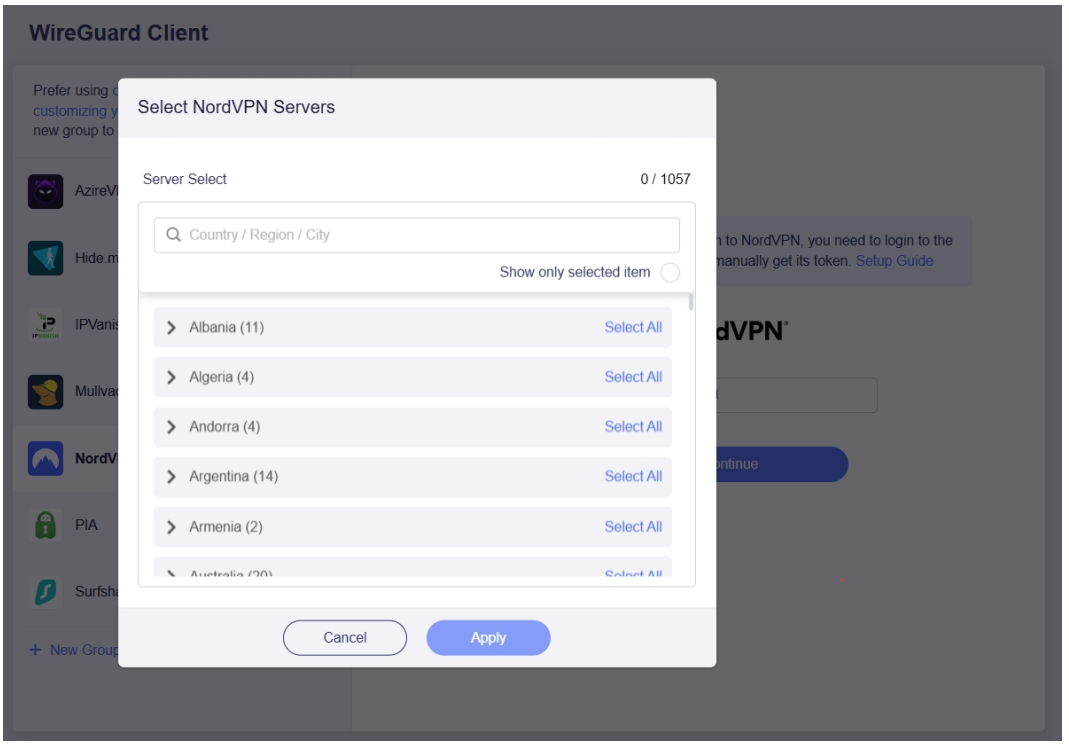
You will find the **Access Token**. Create an access token and copy for later use.



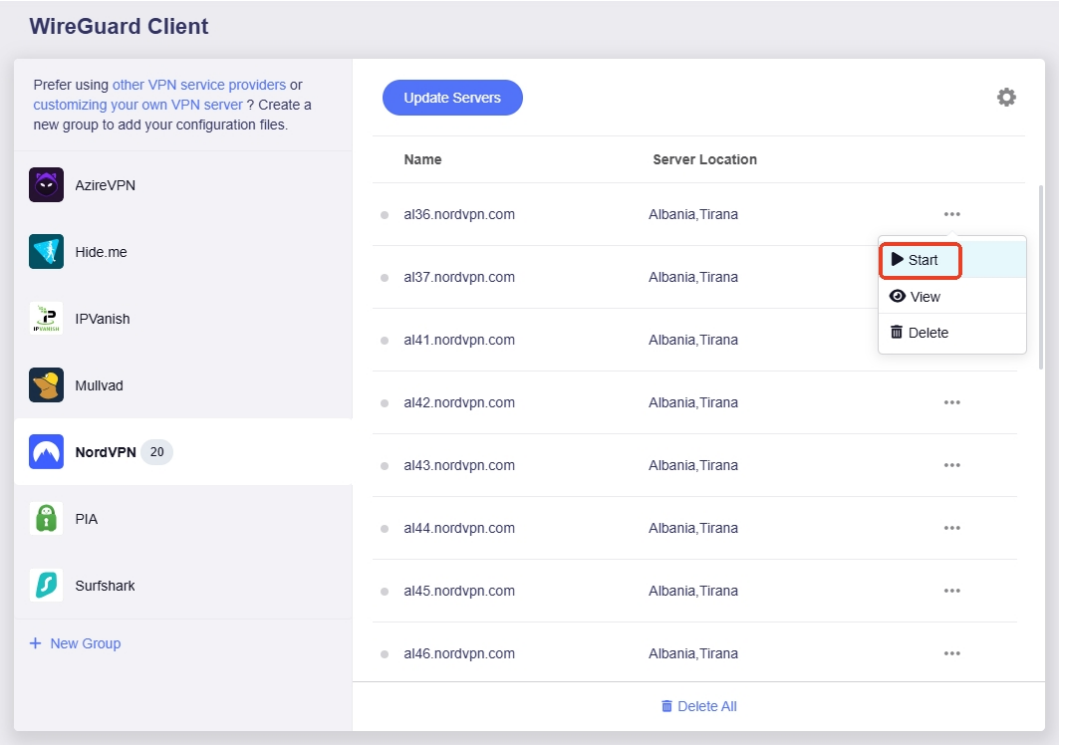
3. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **NordVPN**.
4. Input token, and click **Save and Continue**.



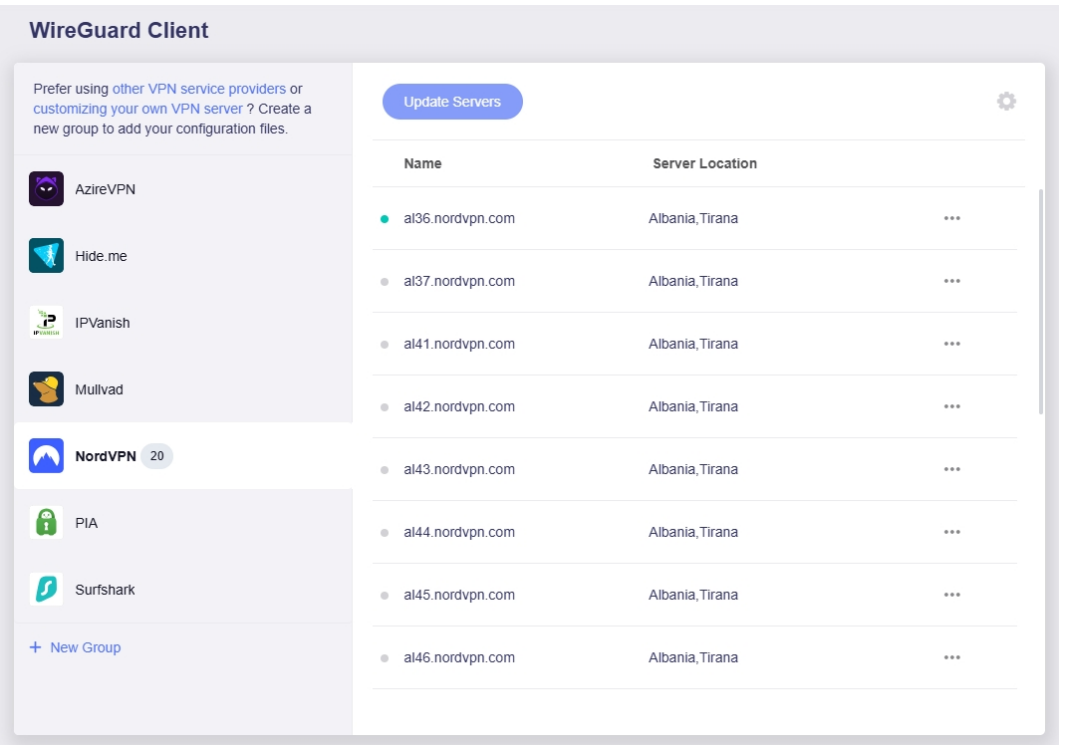
5. Select the server(s) you want to connect to, and click **Apply**.



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



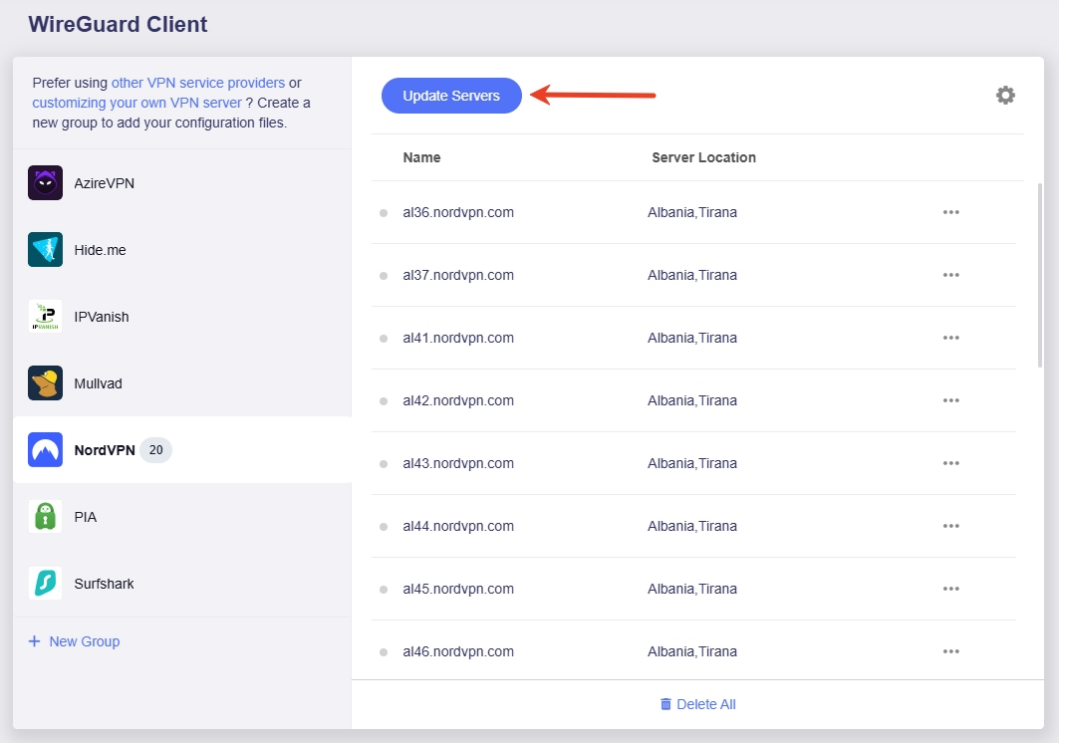
7. Once connected, a green dot will appear next to the configuration file.



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

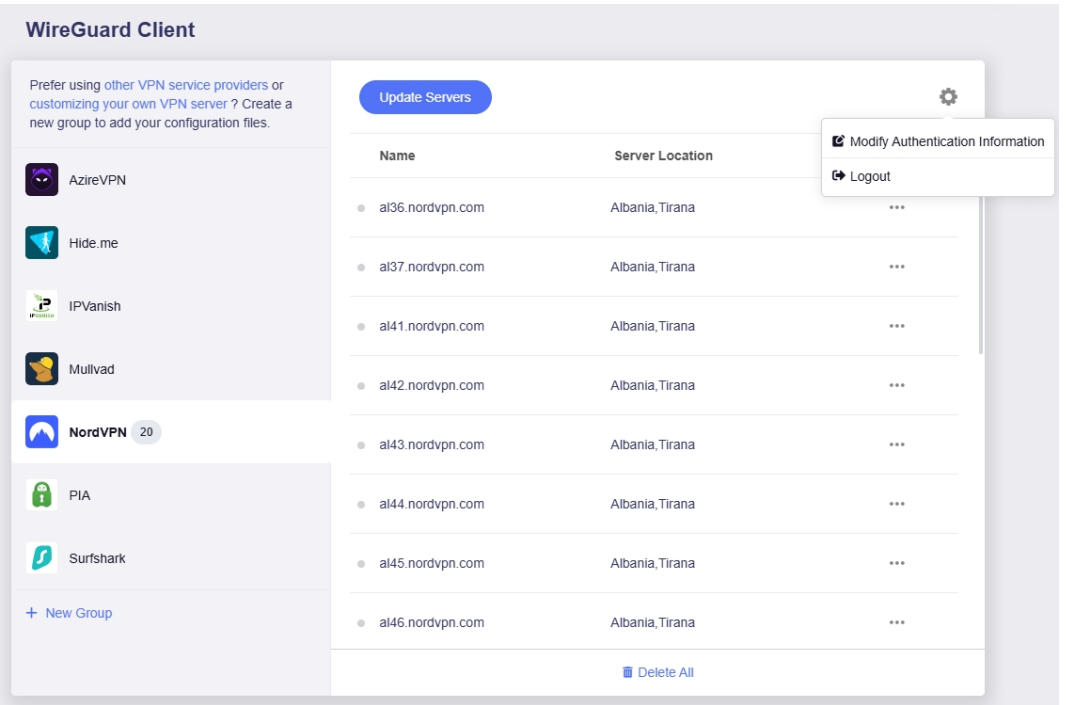
8. Update servers.

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



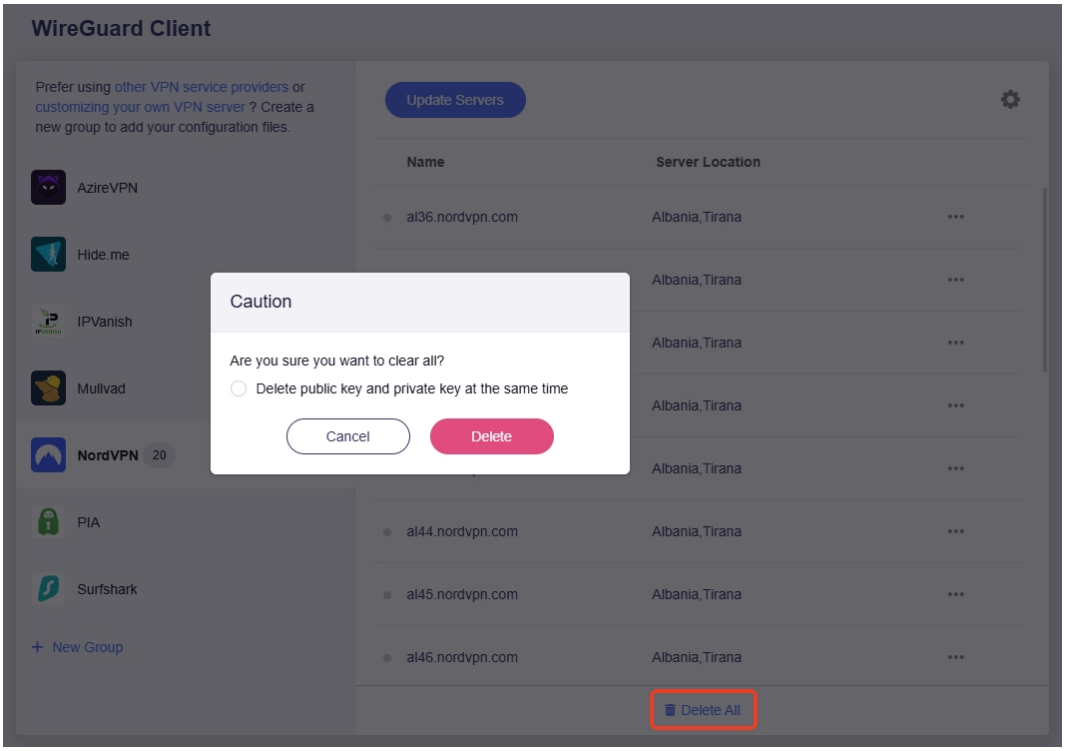
9. Edit credentials or logout.

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



10. Delete all files.

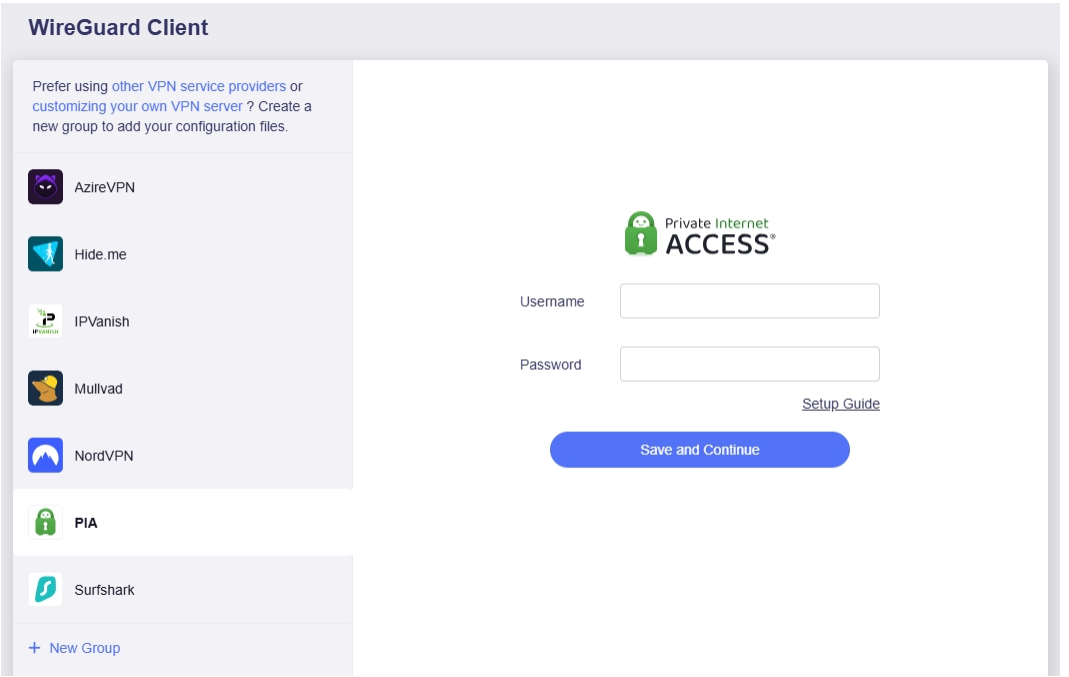
    You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



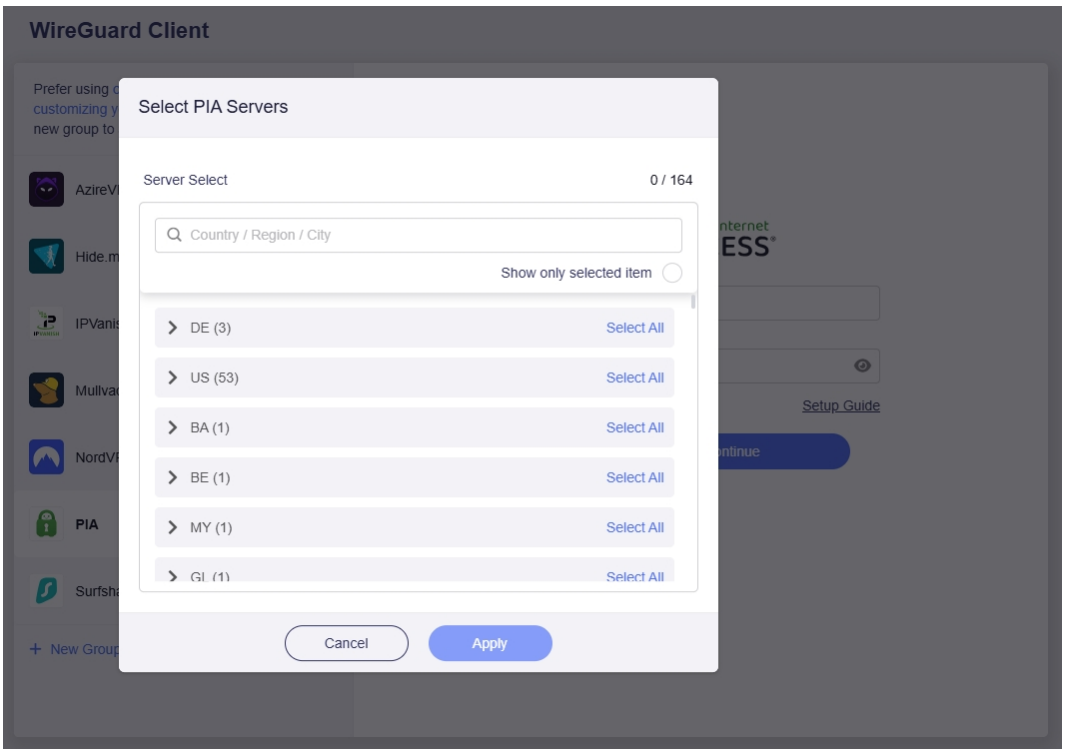
11.2.7 Set Up PIA (Private Internet Access)

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

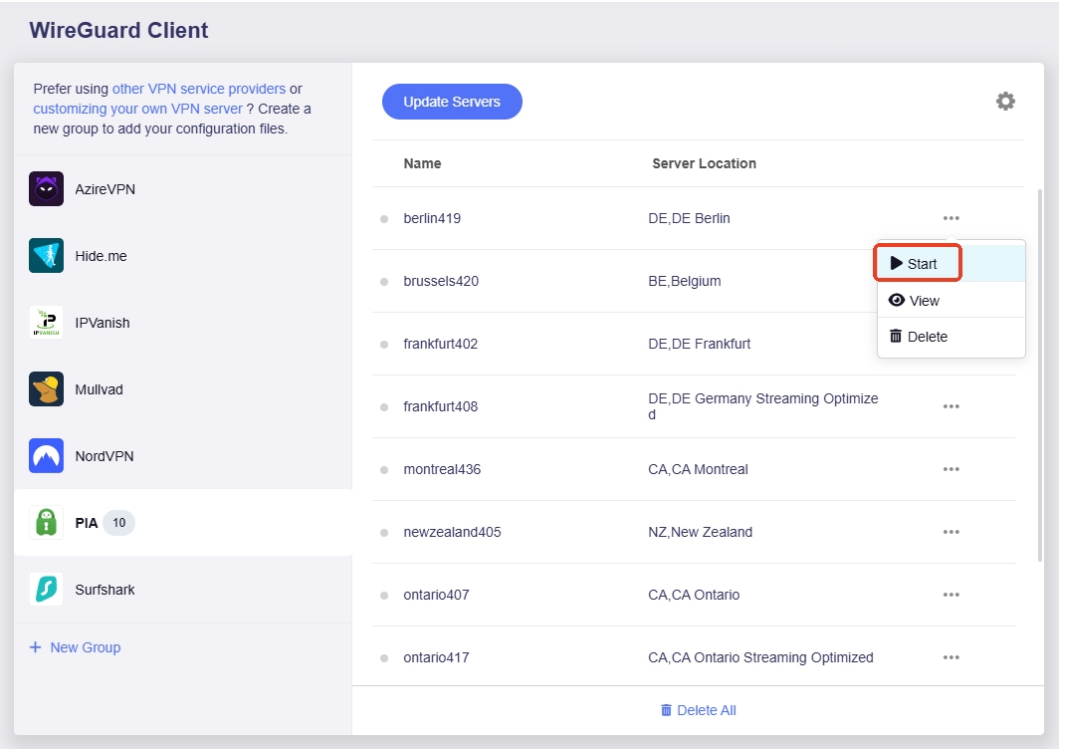
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **PIA**.
2. Input Username and Password, then click **Save and Continue**.



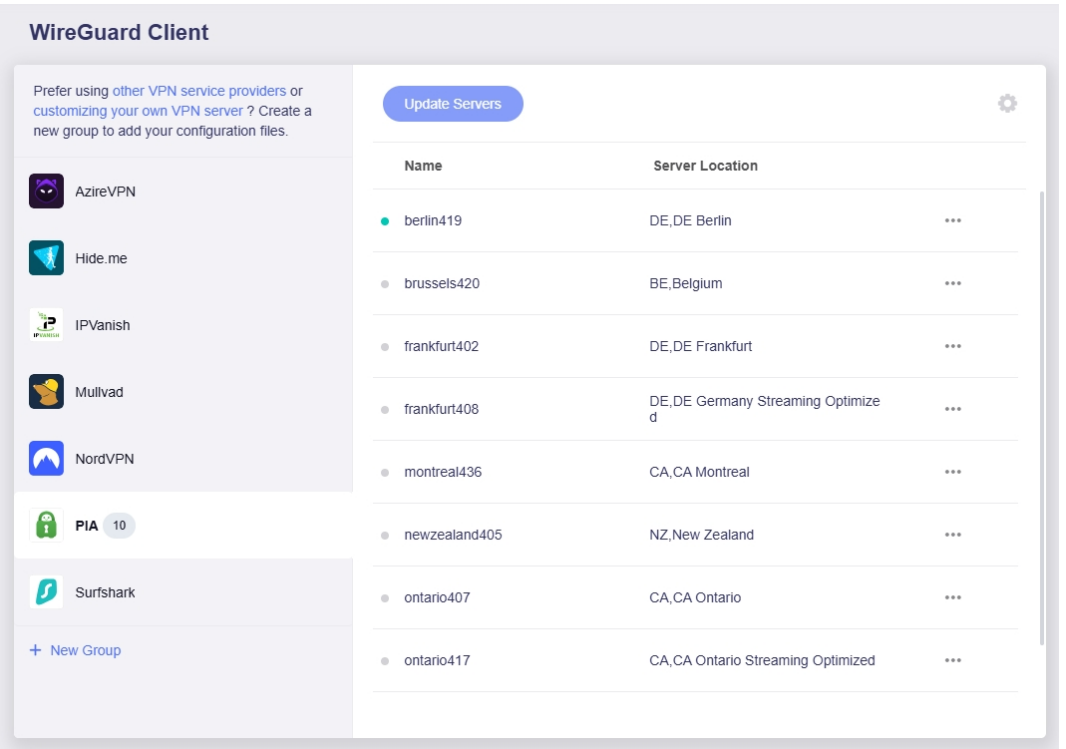
3. Select the server(s) you want to connect to, and click **Apply**.



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



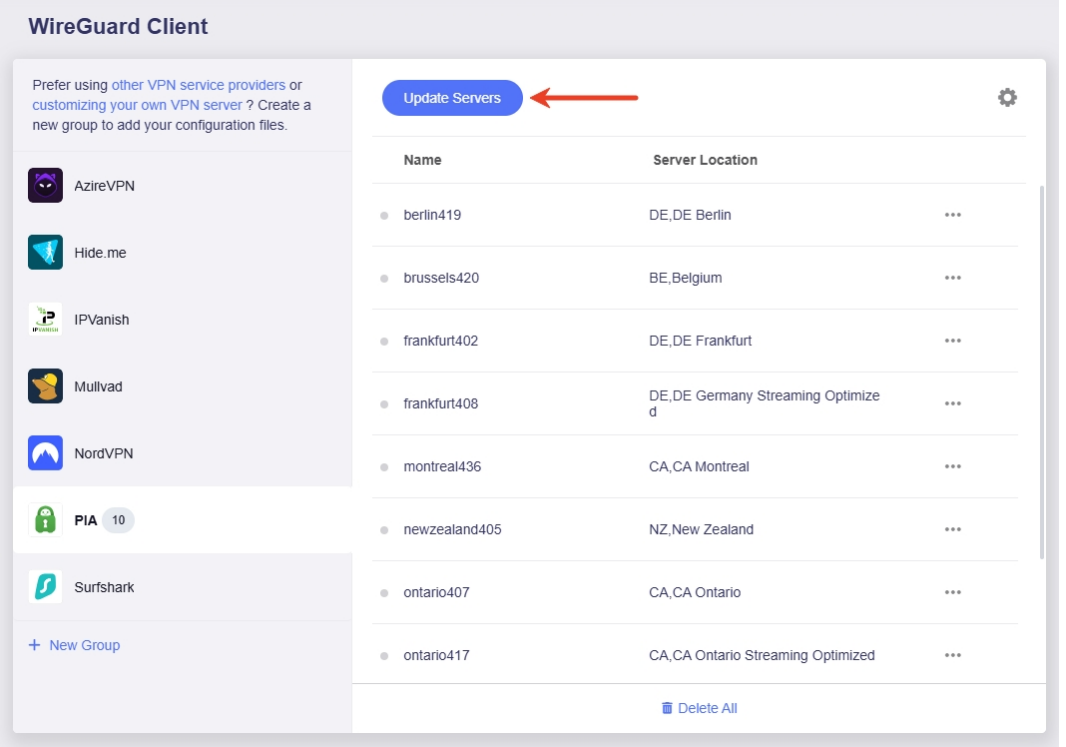
5. Once connected, a green dot will appear next to the configuration file.



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

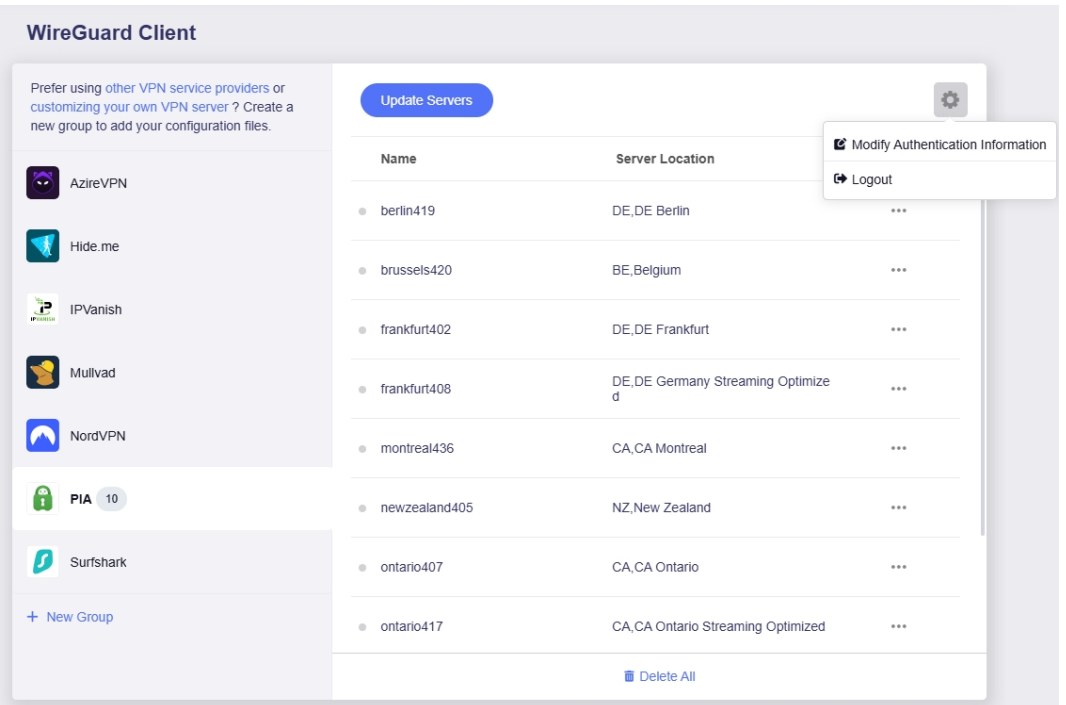
6. Update servers.

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



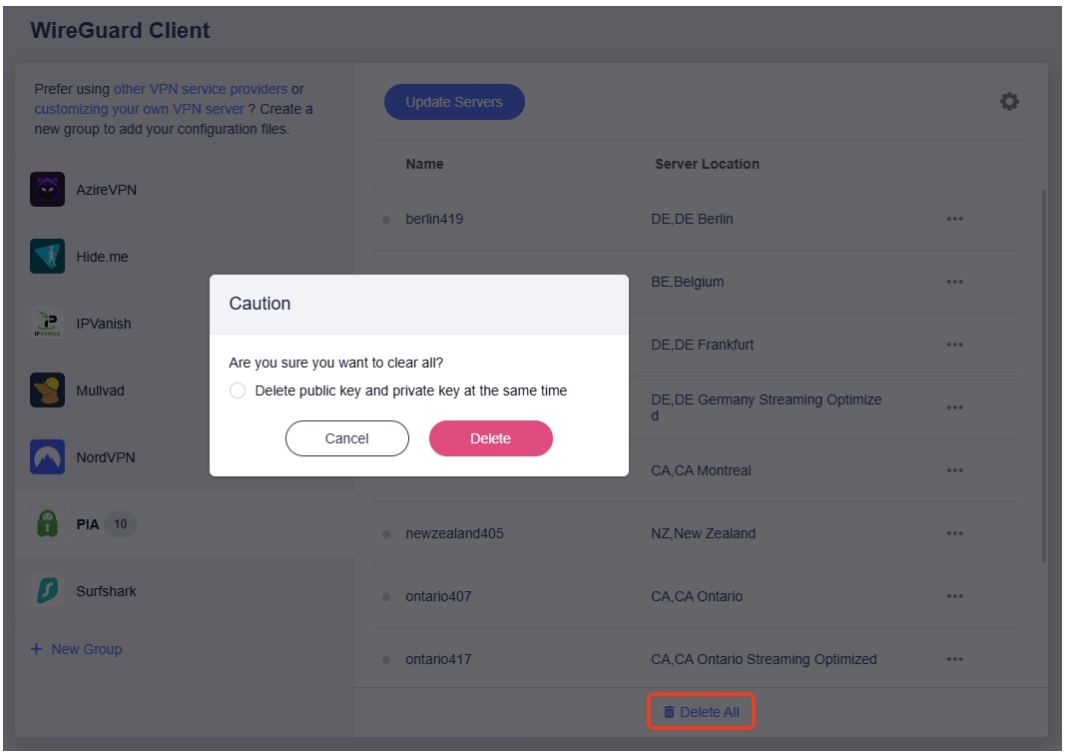
7. Edit credentials or logout.

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



8. Delete all files.

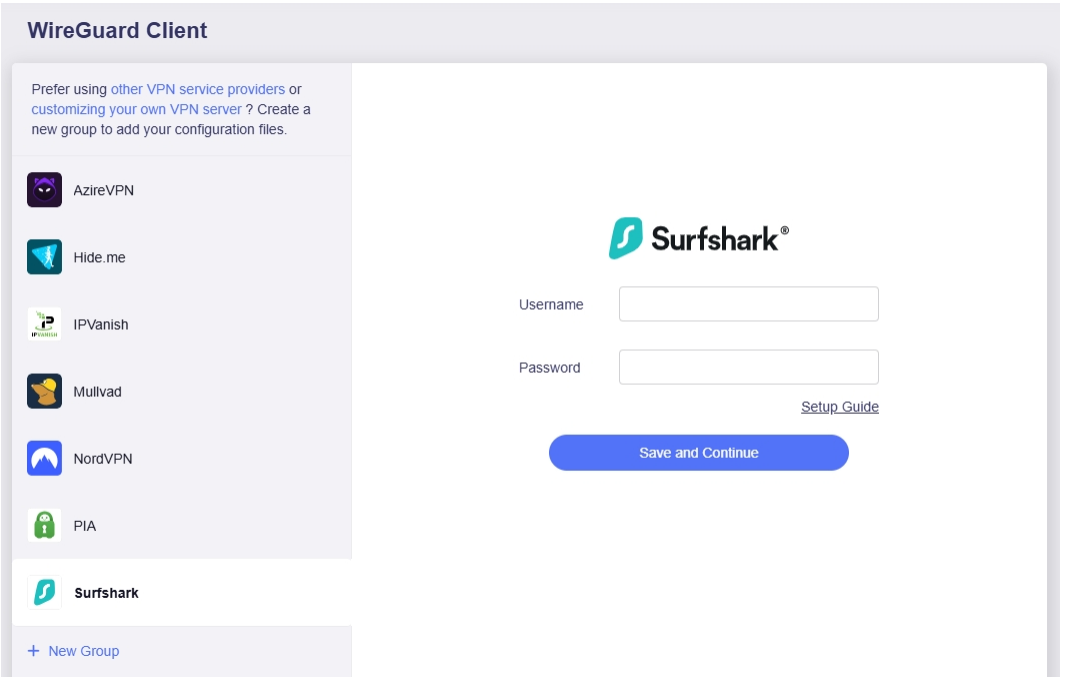
   You can click **Delete All** to delete all configuration files with one click, and choose whether to delete the private and public keys simultaneously.



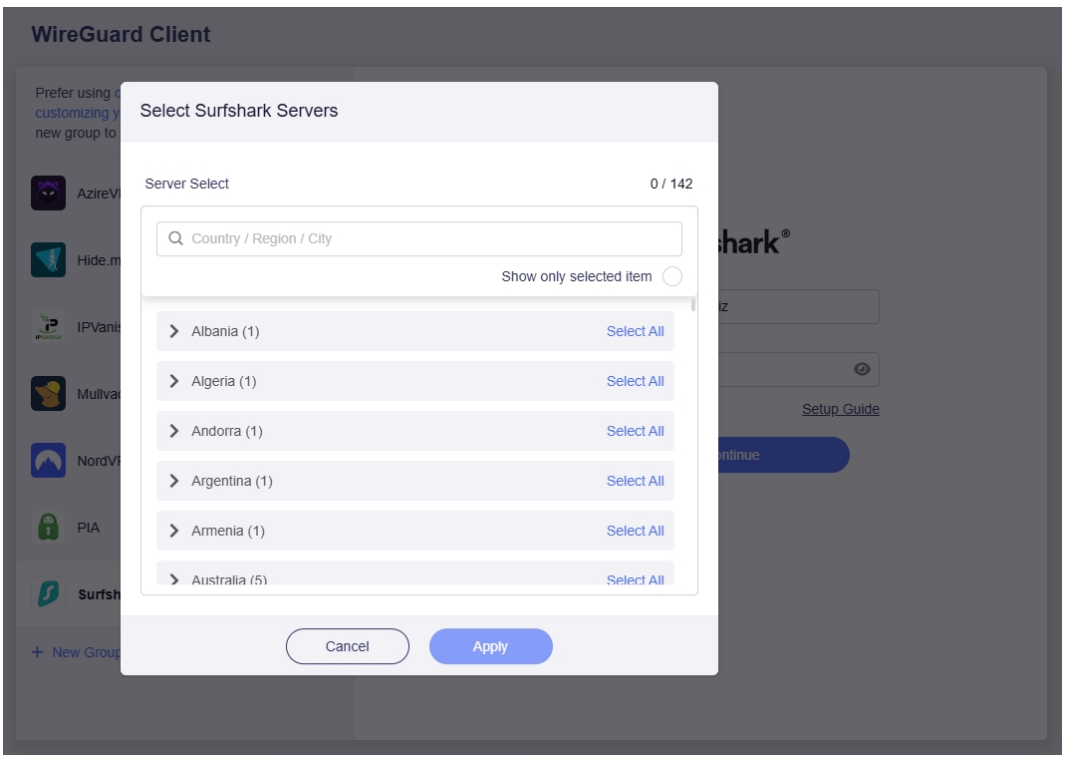
11.2.8 Set Up Surfshark

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

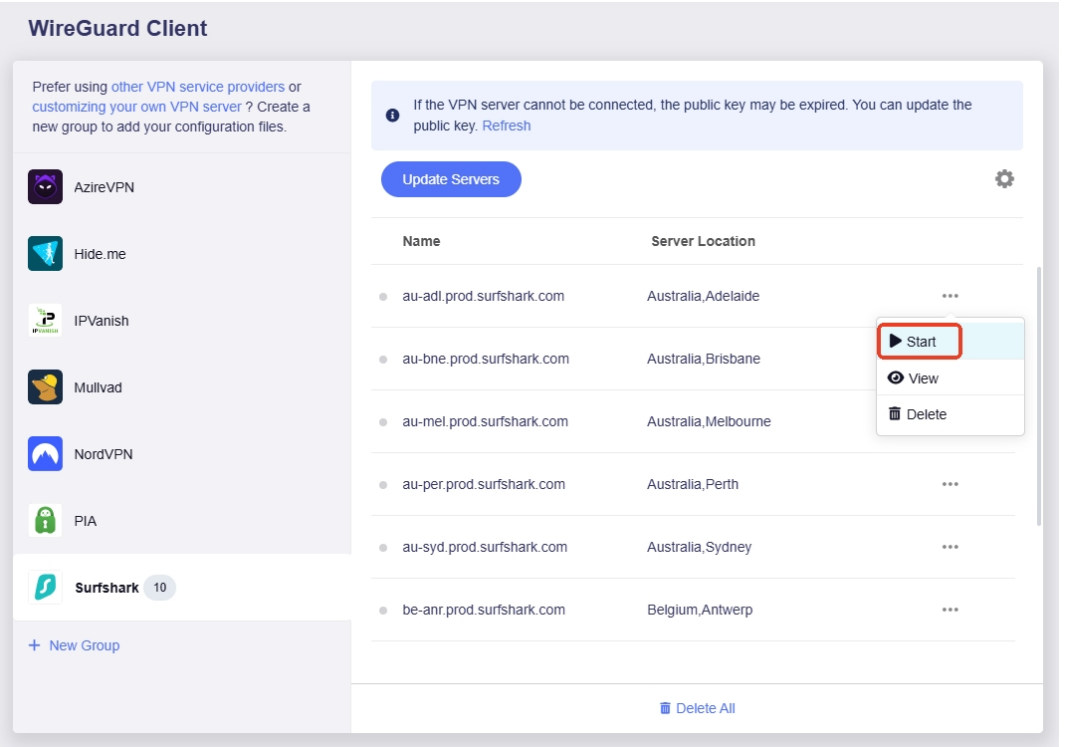
1. Log in to your router's web admin panel and go to **VPN** > **WireGuard Client** > **Surfshark**.
2. Input Username and Password, then click **Save and Continue**.



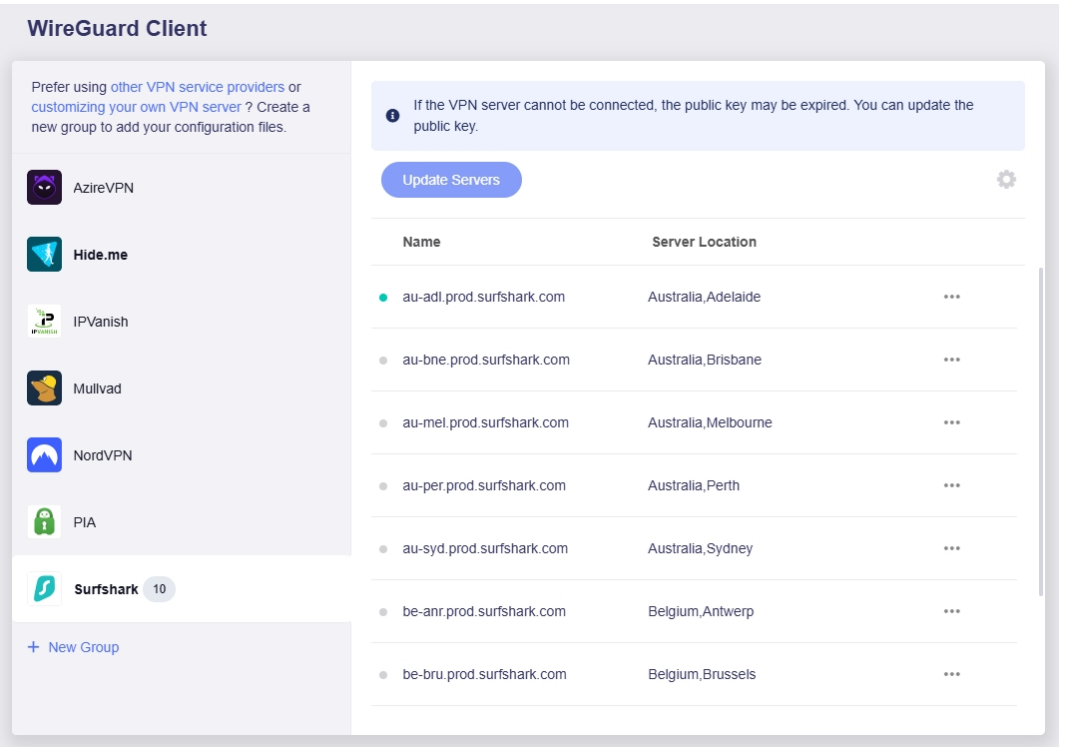
3. Select the server(s) you want to connect to, and click **Apply**.



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



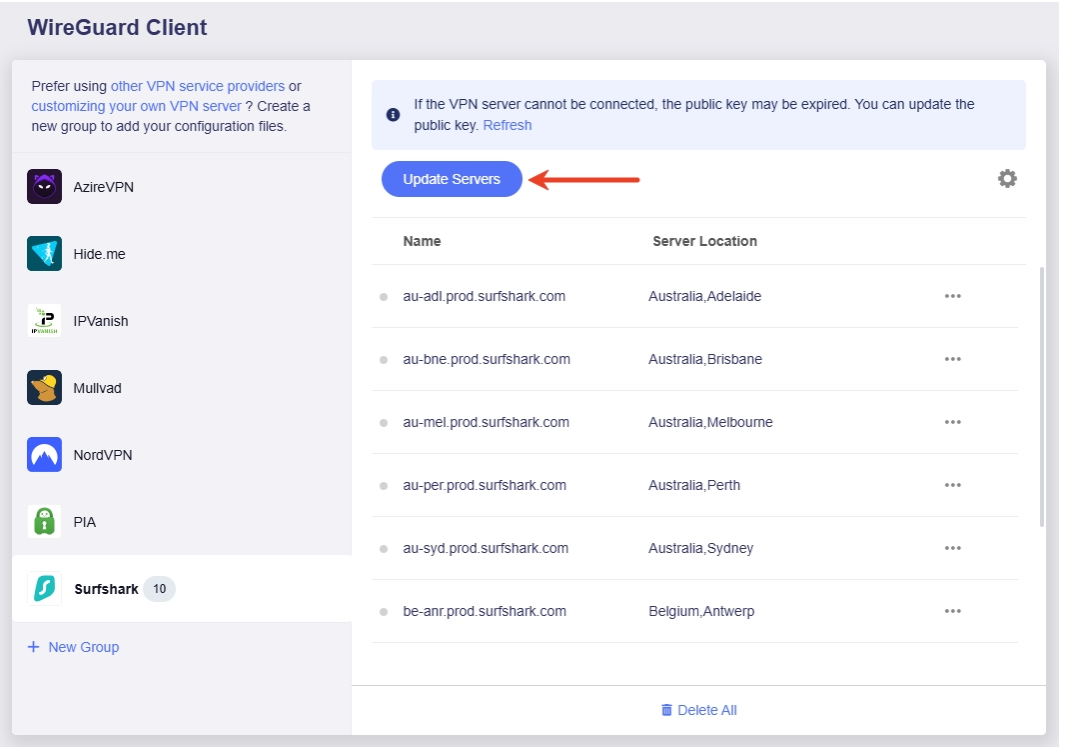
5. Once connected, a green dot will appear next to the configuration file.



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

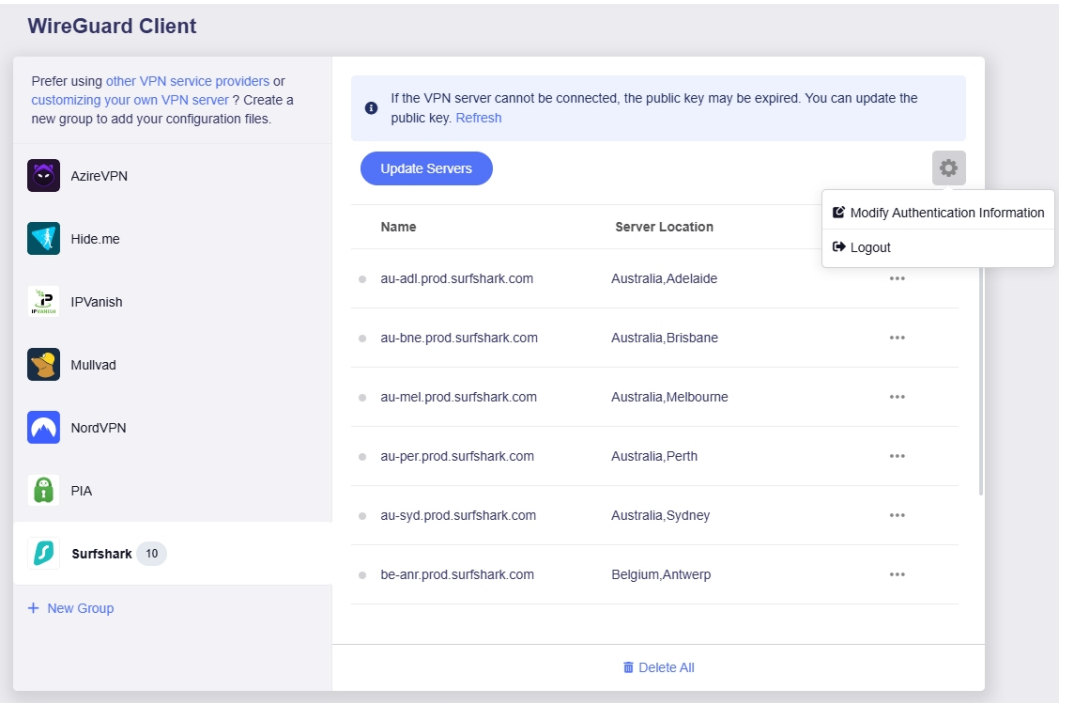
6. Update servers.

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



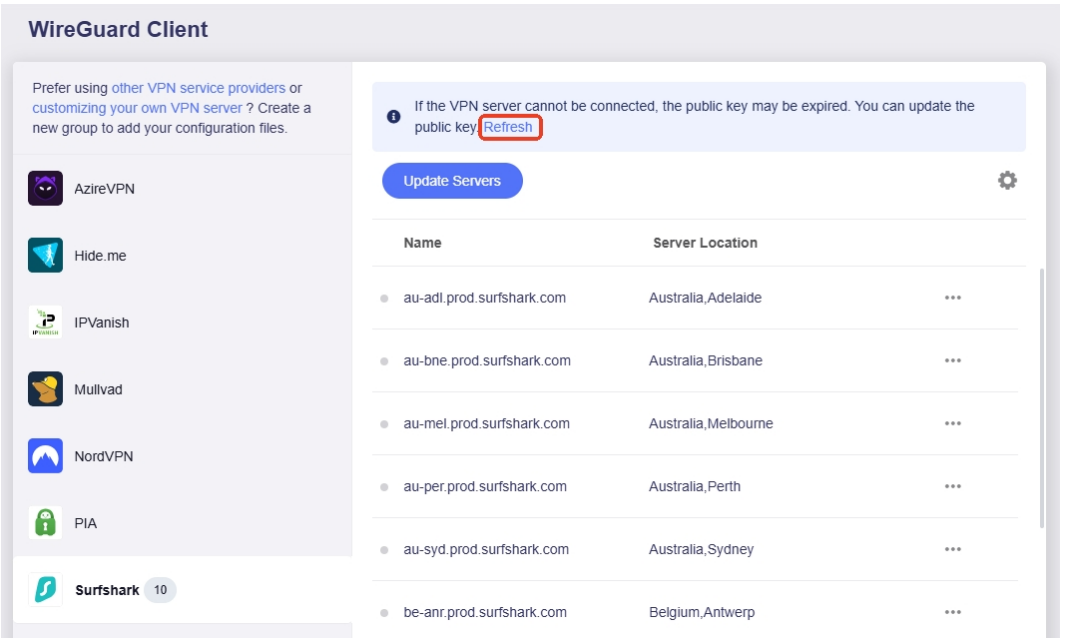
7. Edit credentials or logout.

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



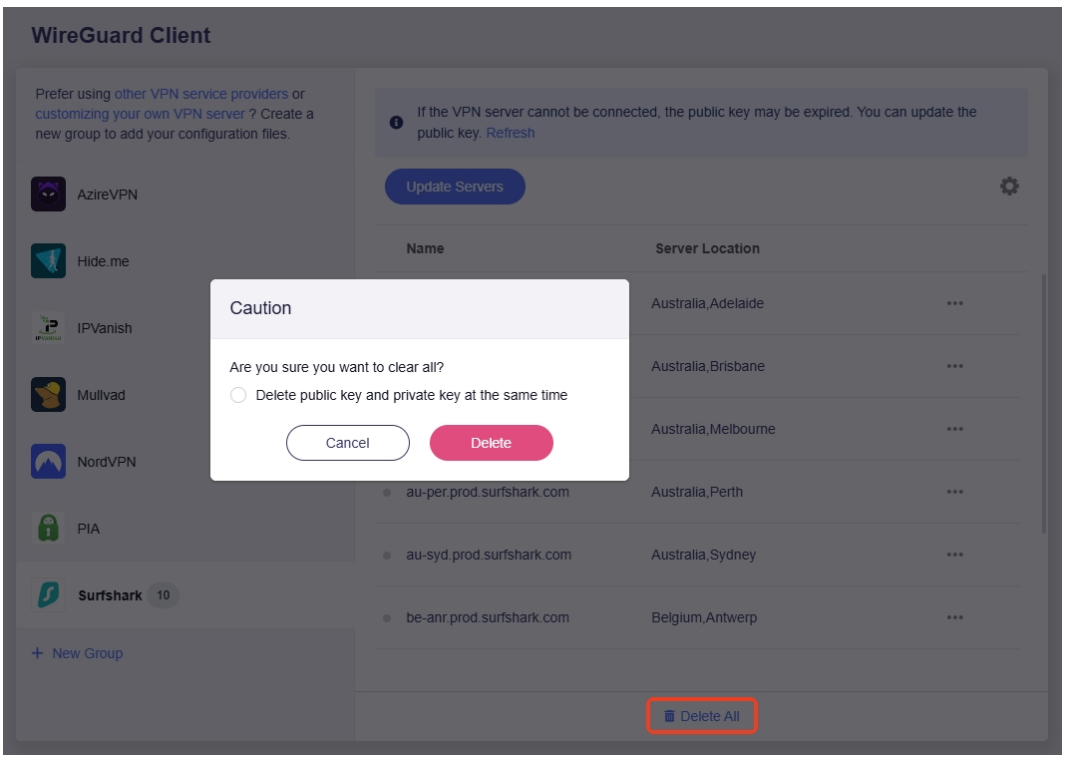
8. Refresh.

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



9. Delete all files.

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

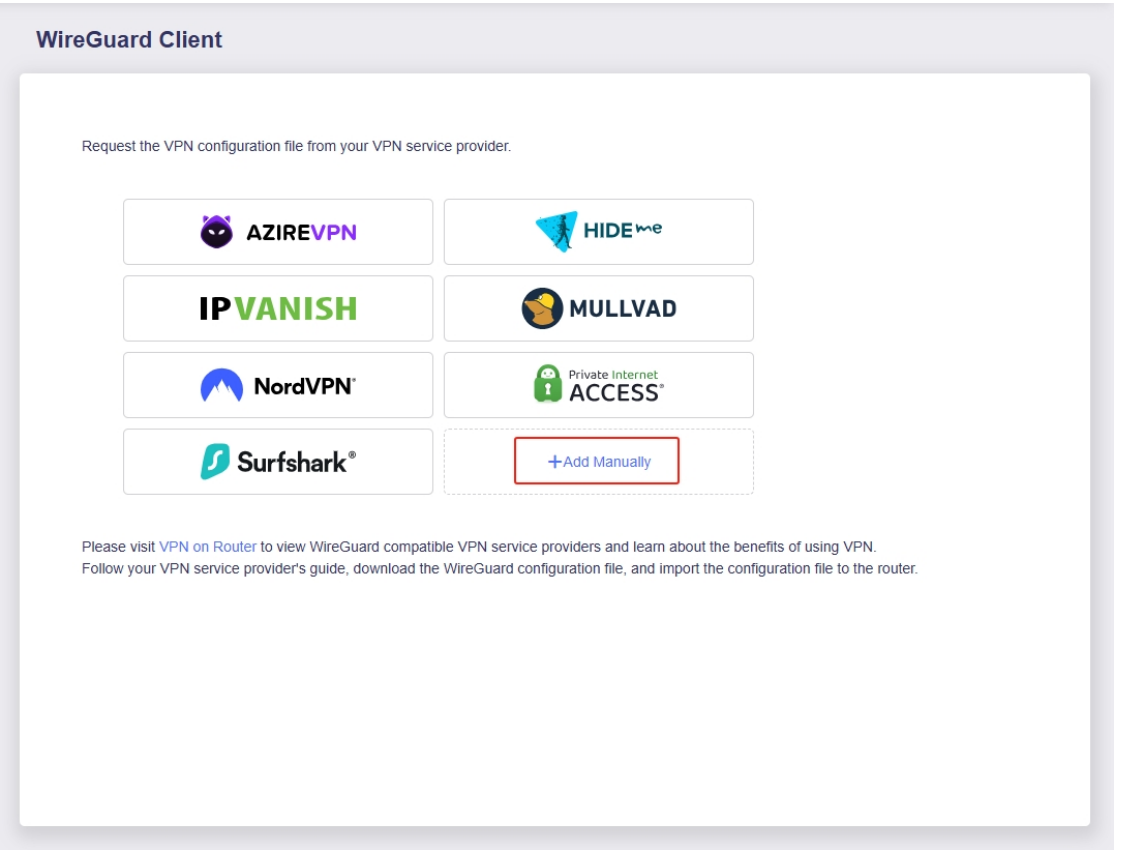


11.2.9 Set Up WireGuard Client Manually (for other providers)

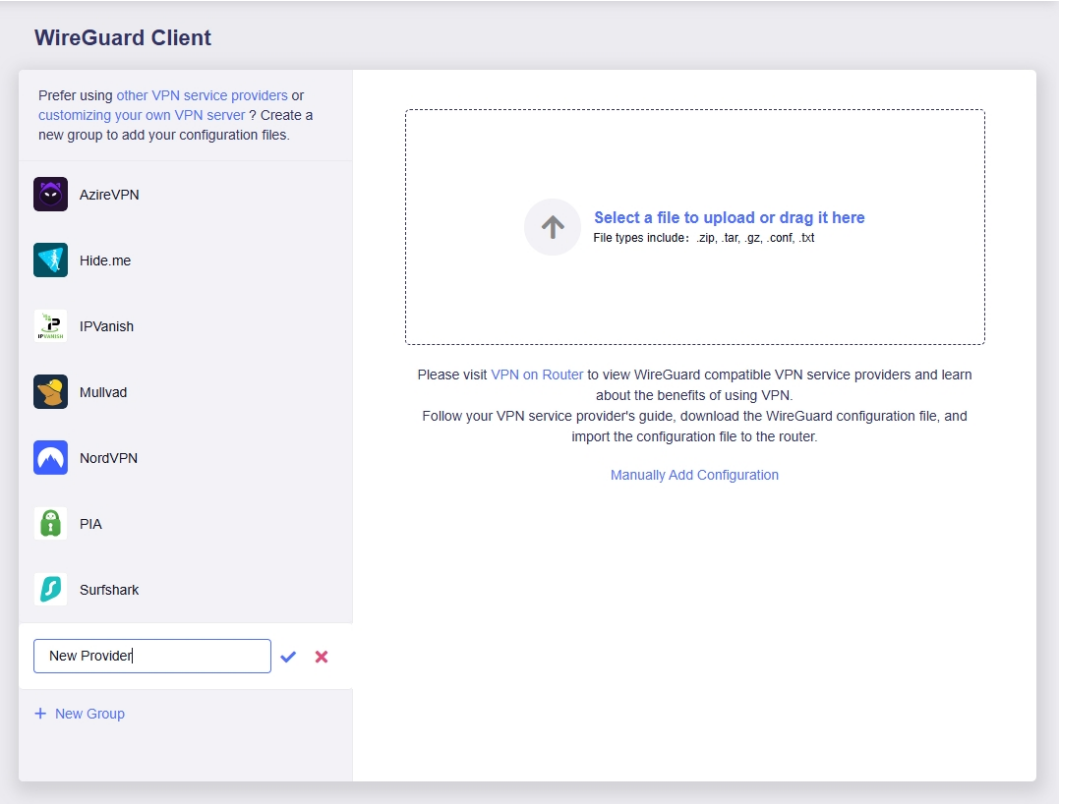
If your WireGuard service provider is not integrated into the web admin panel, visit the official website of your subscribed service provider first to obtain the configuration file. Then upload it to the router to set up a WireGuard client. If you don't know how to download the configuration files, see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

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

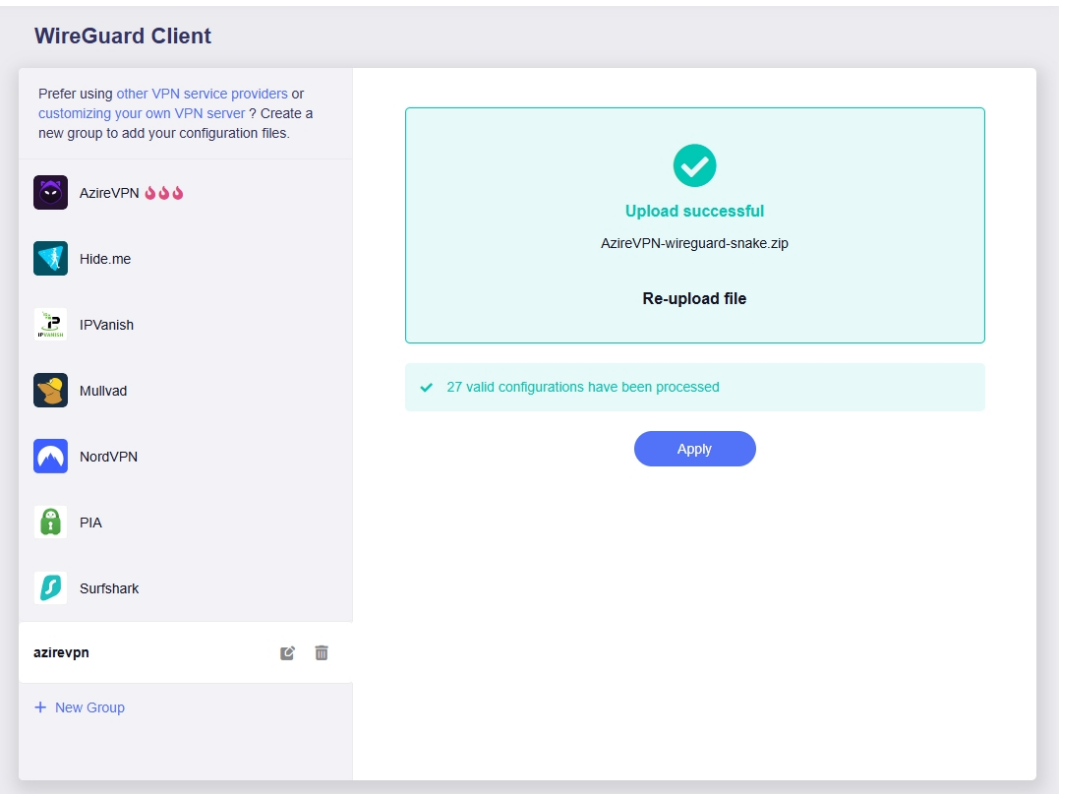
1. Log in to your router's web admin panel and navigate to **VPN** > **WireGuard Client** > **Add Manually**.



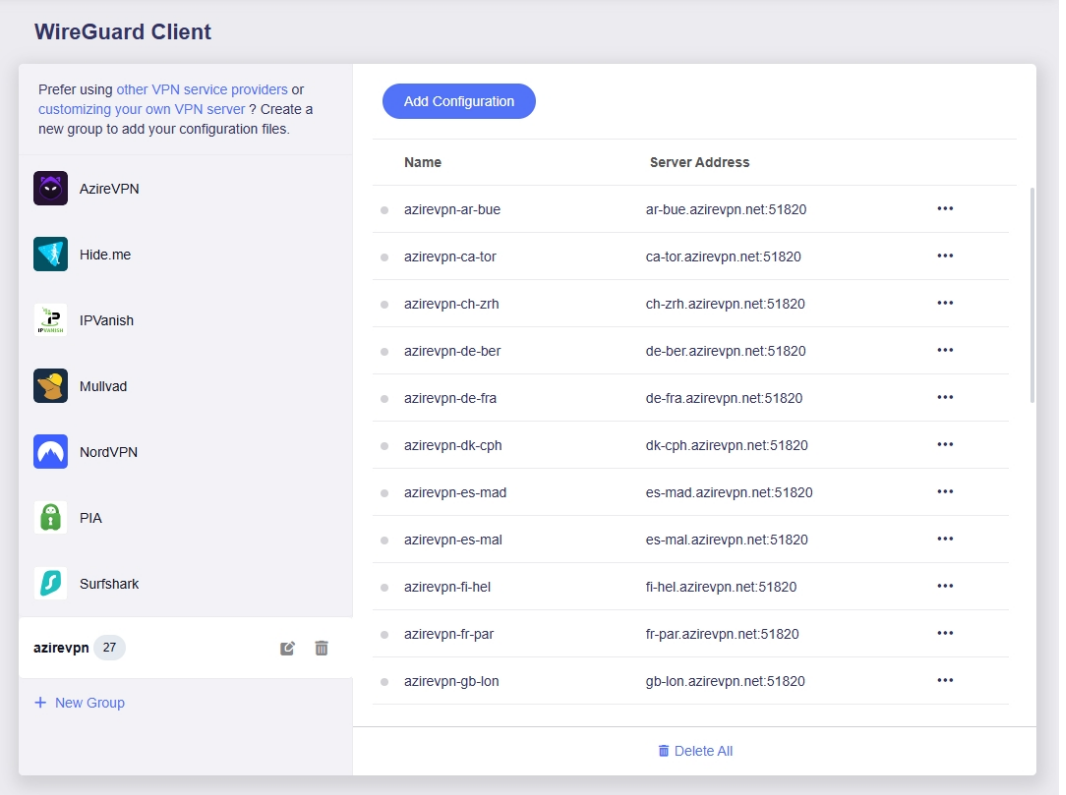
2. It will create a group on the left sidebar. Set a descriptive name for the group.



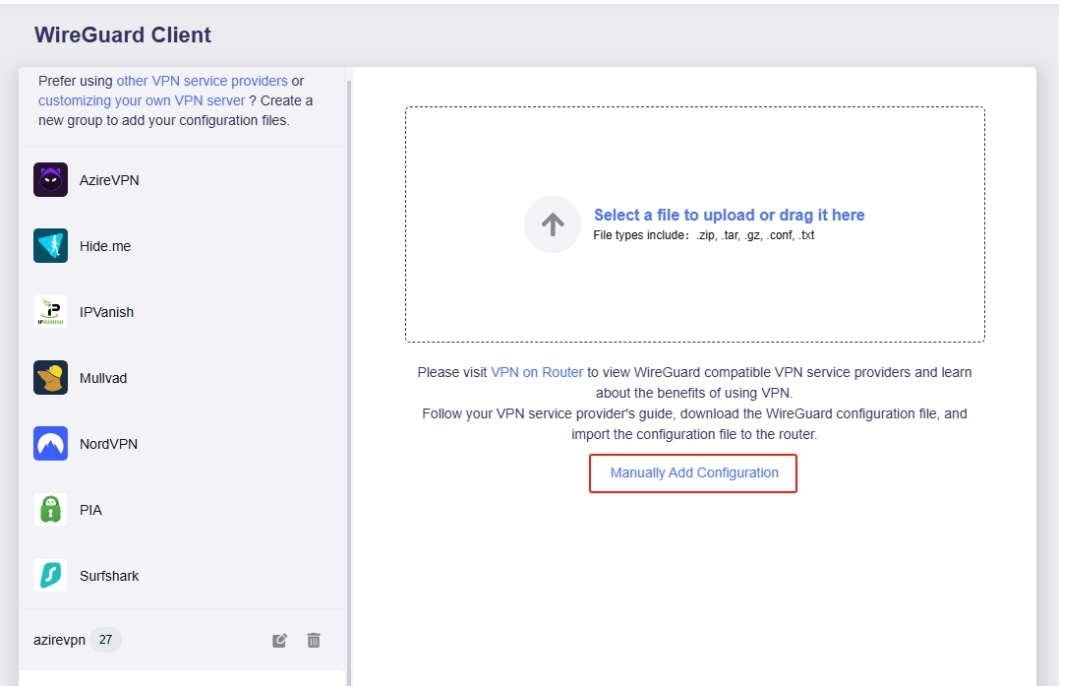
3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.

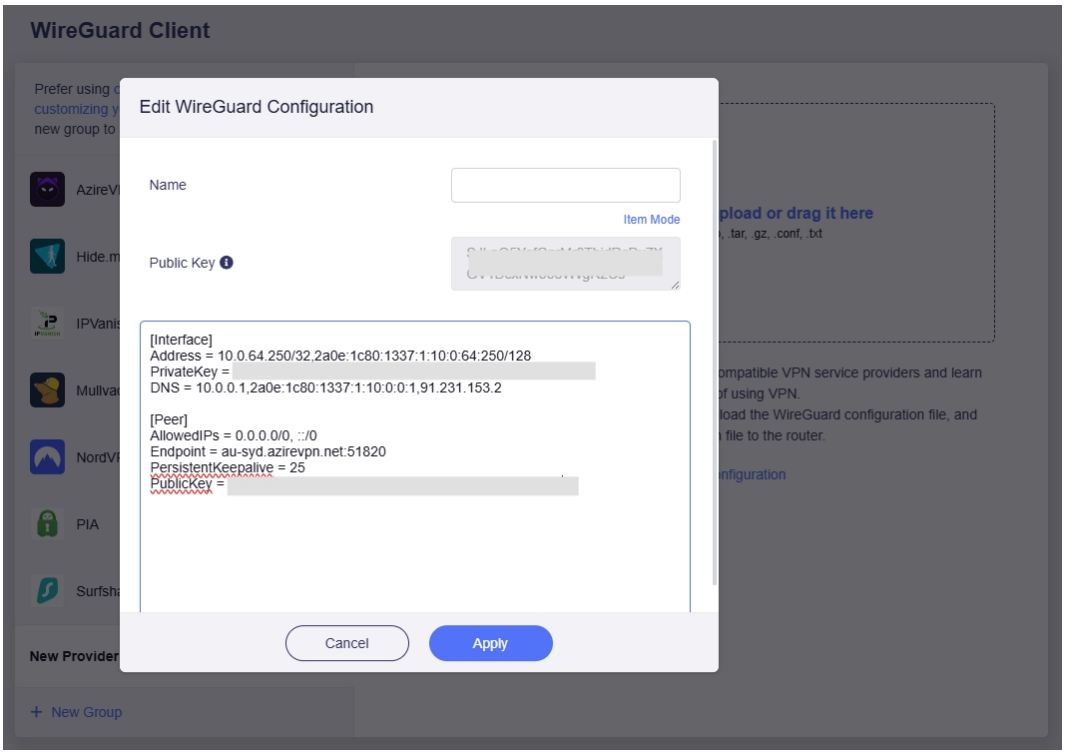


If you upload a compressed file containing multiple configuration files, it will be decompressed automatically, as shown below.

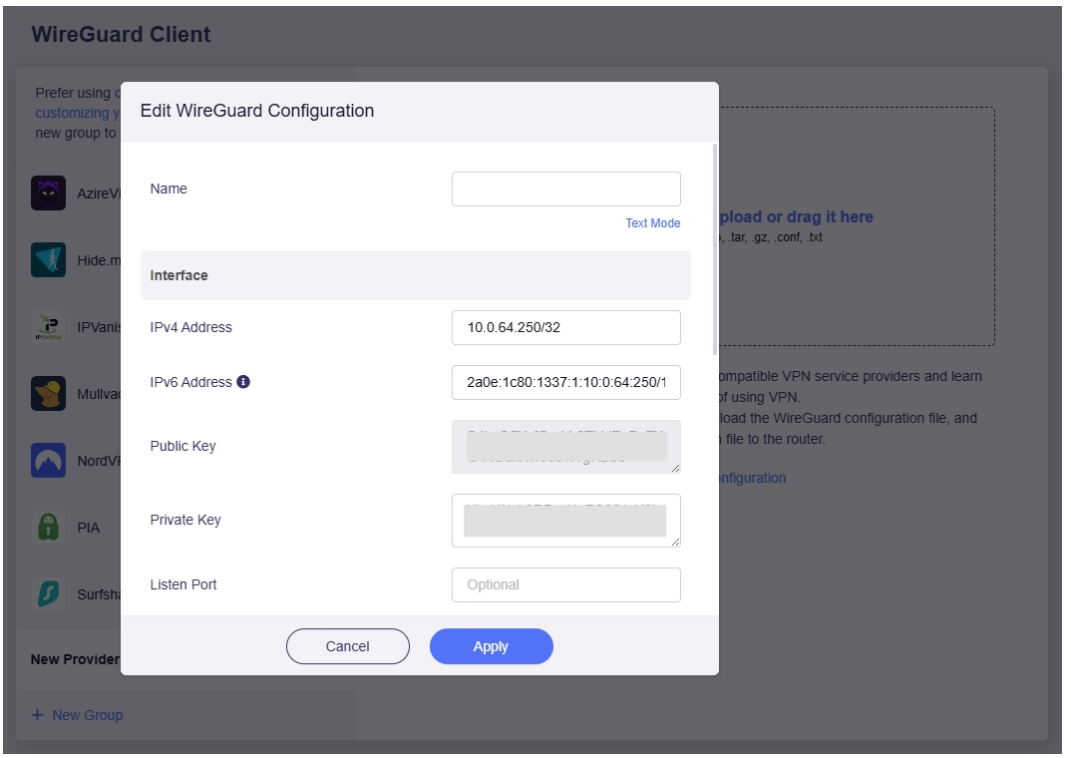


Alternatively, you can click **Manually Add Configuration** at the bottom of the upload area, add configuration details in text form and click **Apply**.

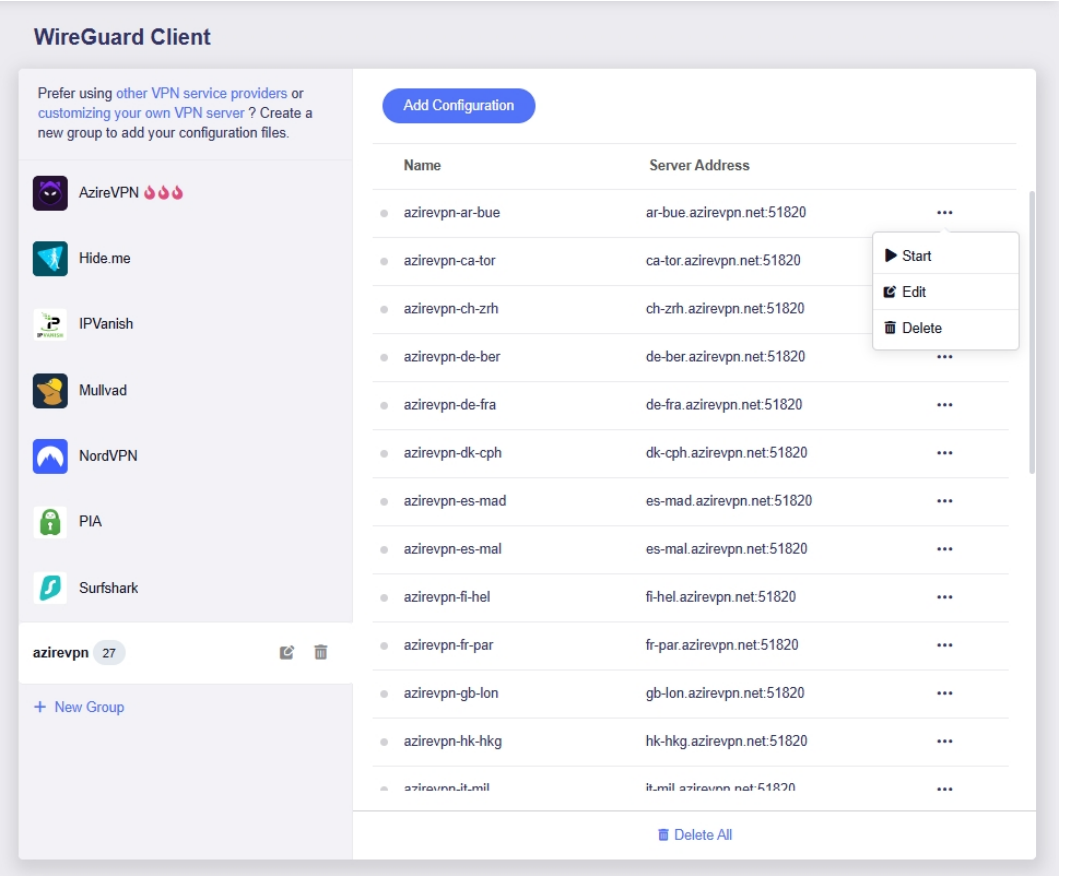




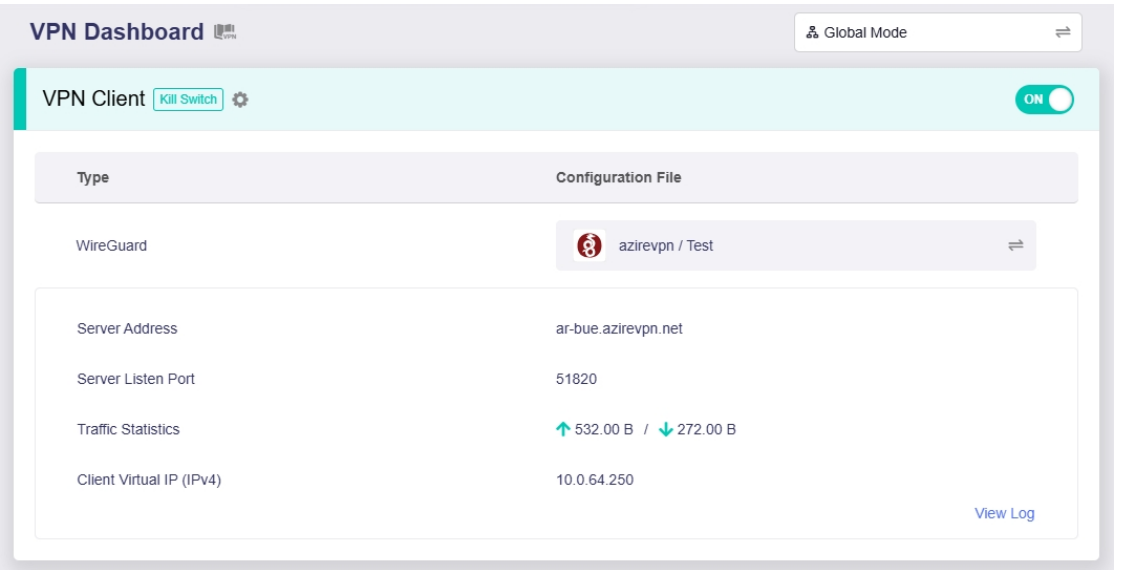
If you want to verify each item, you can switch to the Item mode and check the configuration details, then click **Apply**.



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



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



Chapter 12

Network

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

12.1 Multi-WAN

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

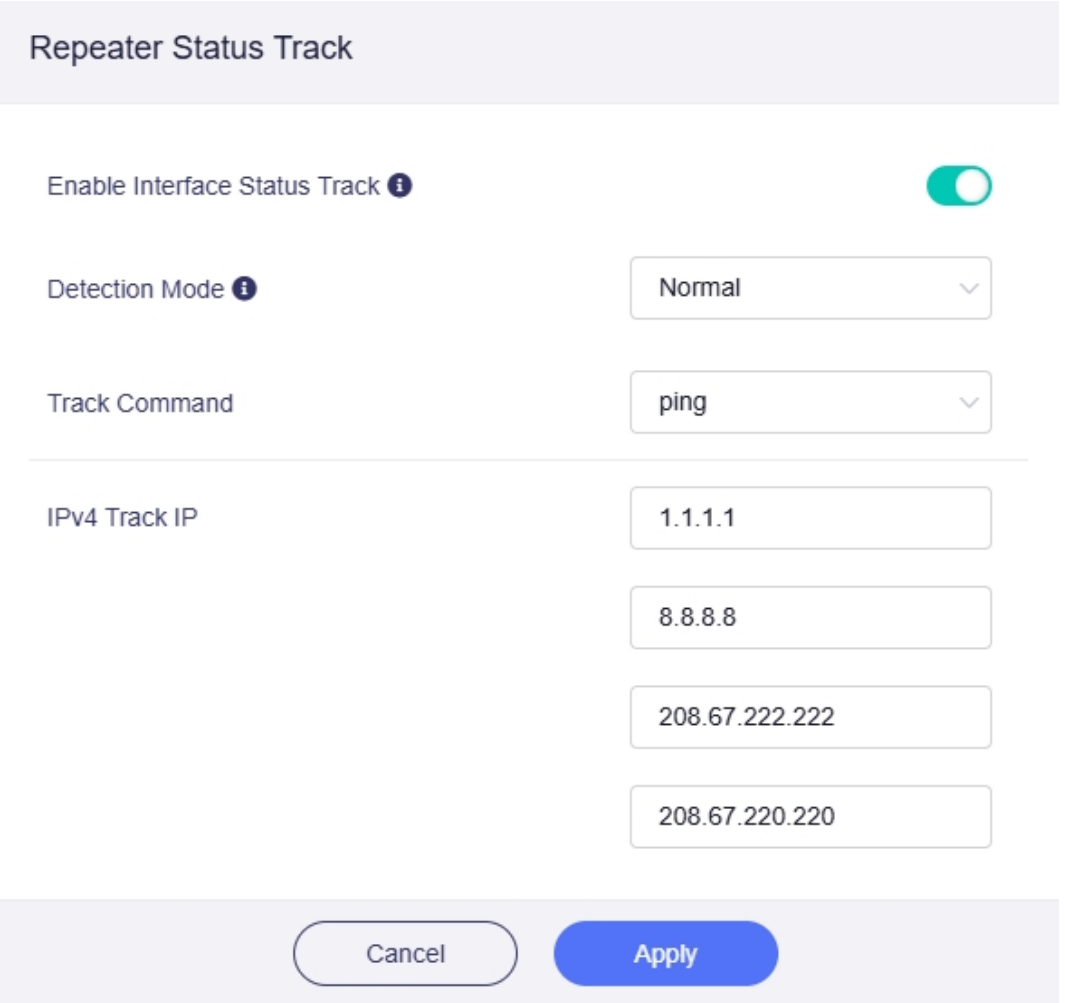
- **Failover**: Automatically switches to an alternate connection within a short time if the primary connection fails, ensuring uninterrupted network access.
- **Load Balance**: Distributes network traffic across all available connections at a set ratio for concurrent multi-connection usage, optimizing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

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

12.2.1 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.

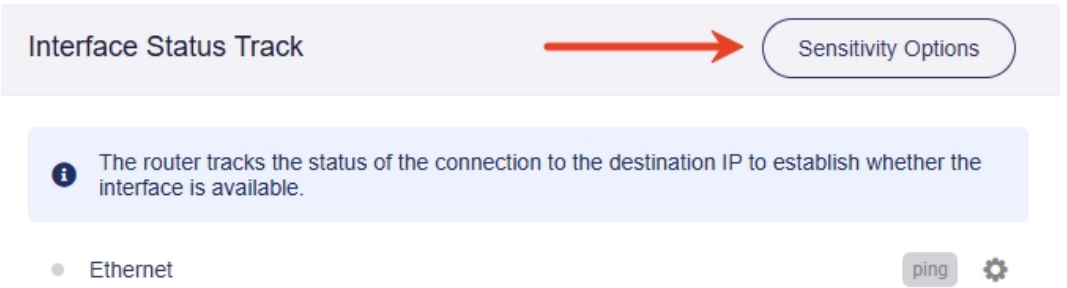
In the **Interface Status Track** section, click the gear icon on the right to access the status tracking settings for each network interface. Below are the status tracking settings for the Repeater interface. The same configuration logic applies to other interfaces.



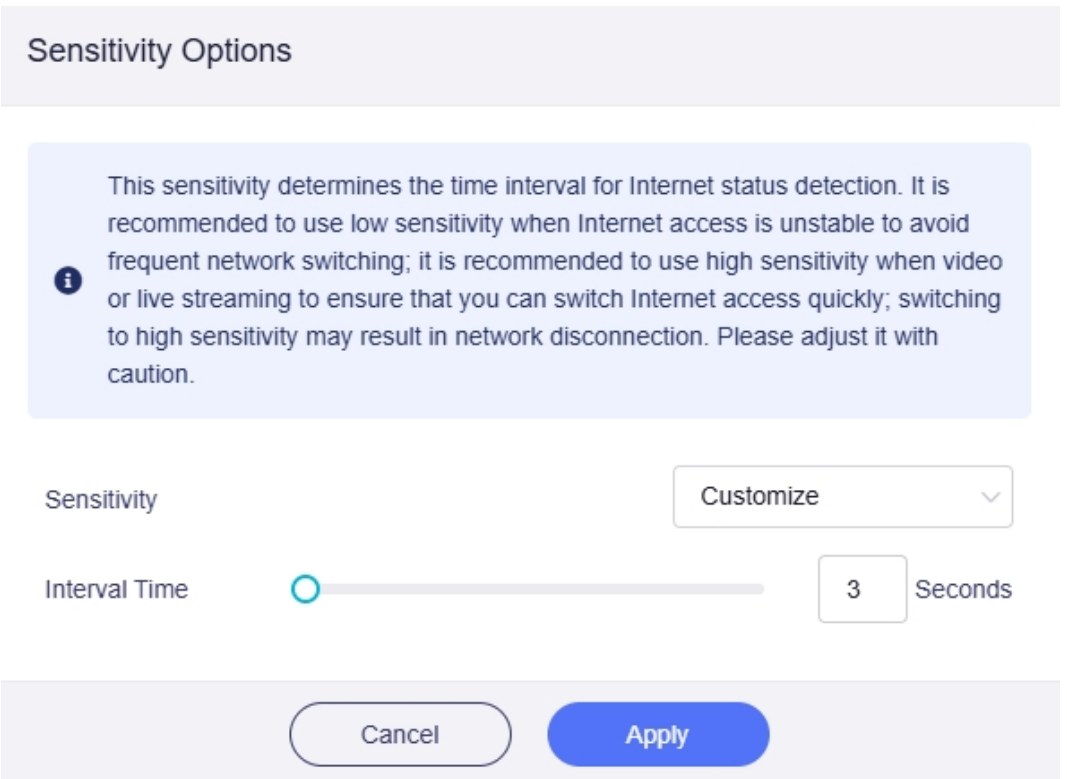
- **Enable Interface Status Track**: It is enabled by default. If disabled, the device will assume that it is connected to the Internet when the interface is connected (e.g. if a cable is plugged in and an IP address is acquired).
- **Detection Mode**: This feature was introduced as Low Data Mode in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

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

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



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



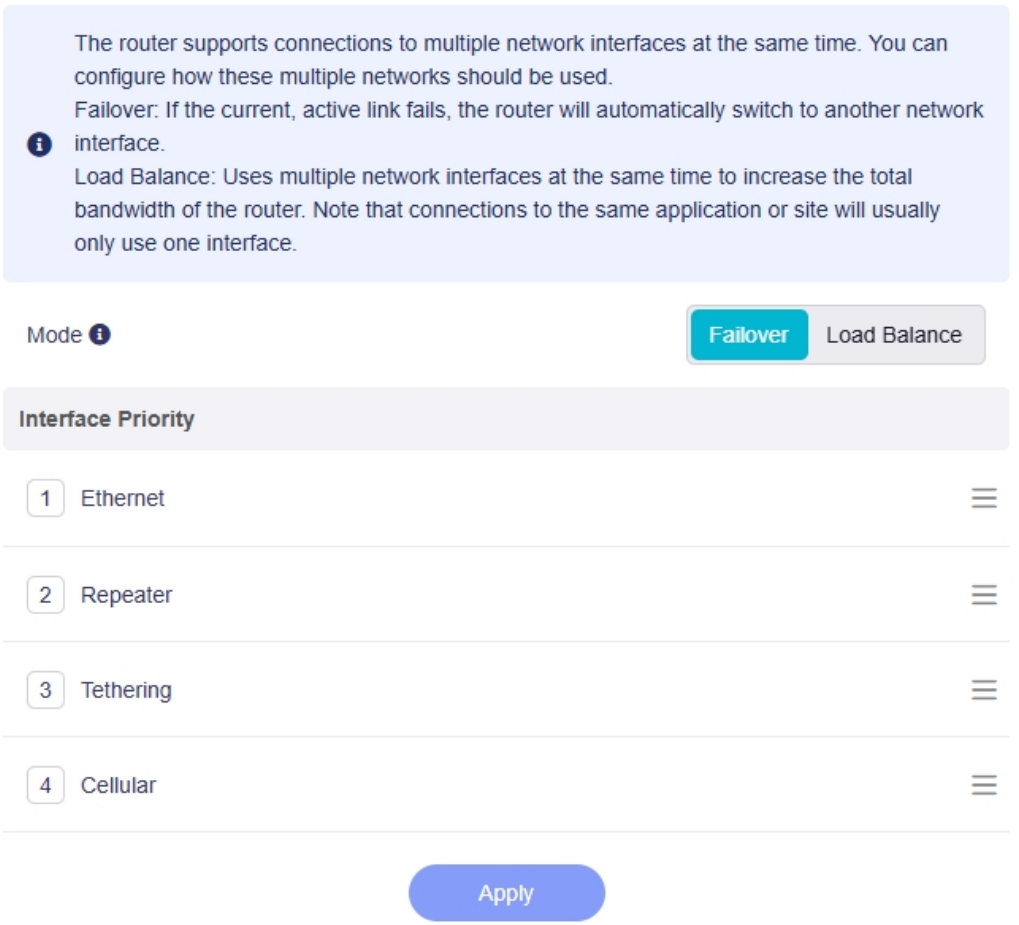
12.2.2 Multi-WAN Mode

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

Failover

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

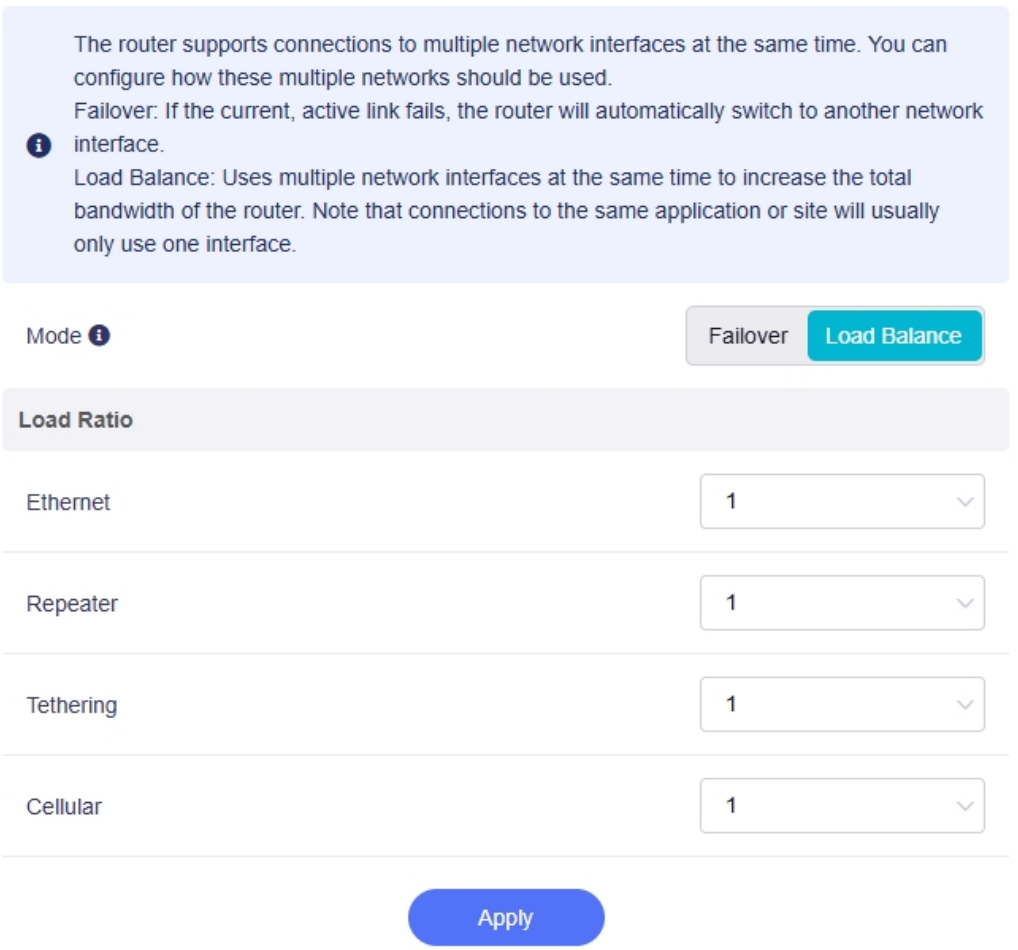
You can set priority levels for each interface: when the currently used interface fails, the router switches to the next available interface with the highest priority. Once a higher-priority connection is restored, the router will automatically switch back to it.



Load Balance

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

The load ratio refers to the proportion between each network interface. The system will assign interfaces to handle new connections based on this configured ratio. For example, if the router is connected to four networks simultaneously (e.g., Ethernet, Repeater, Tethering, and Cellular) and all 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 interfaces according to the configured load ratio.



You can also customize the load ratio as needed. For example, if Ethernet has a bandwidth of 100 Mbps, Repeater has 200 Mbps, and no other 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.

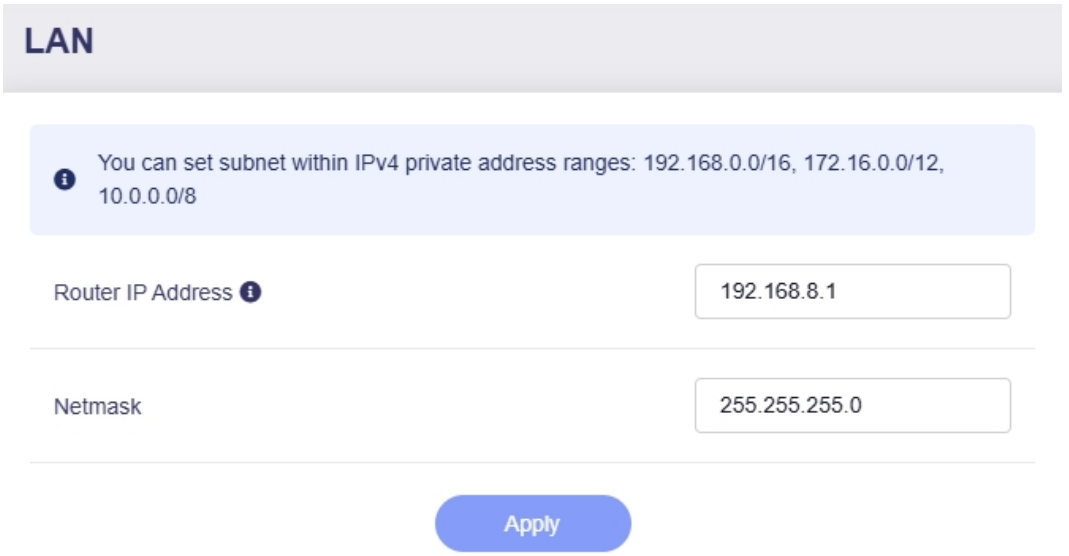
12.2 LAN

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

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

12.2.1 Basic Settings

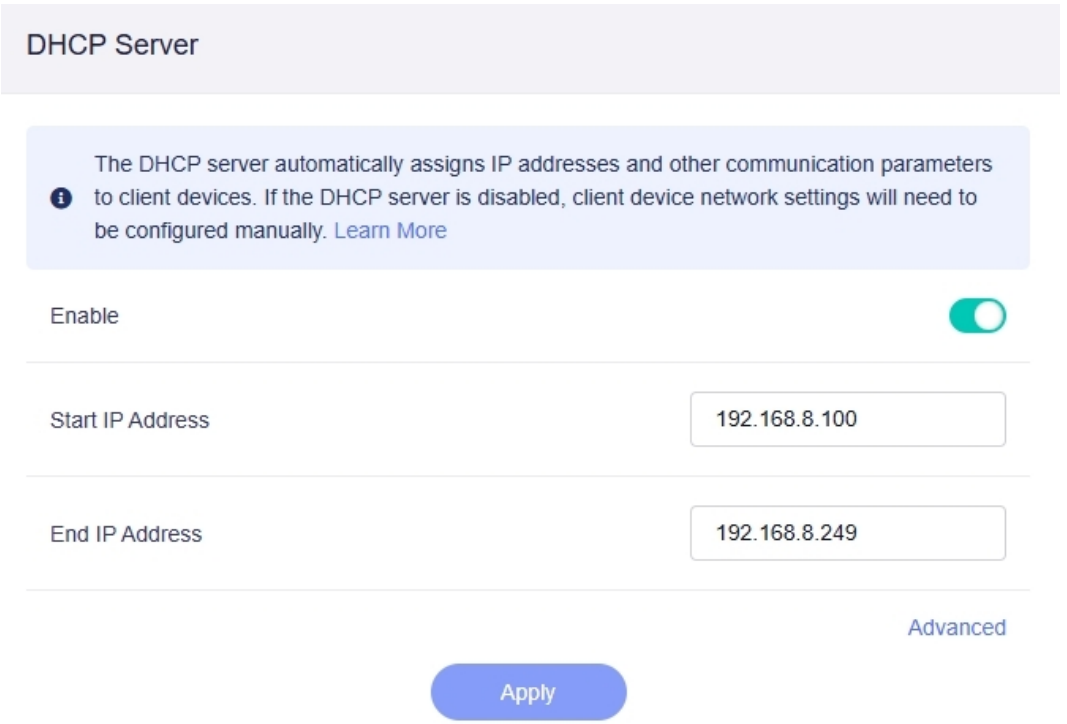
The basic settings include Router IP address and Netmask. You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



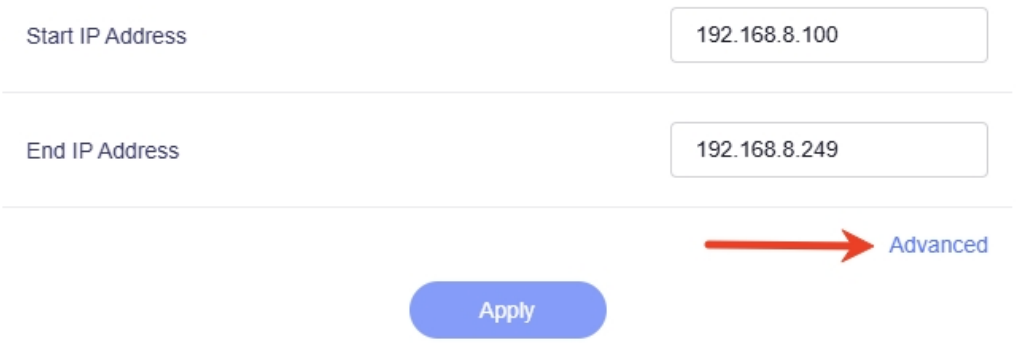
- **Router IP Address**: This is the address entered into a browser's address bar to access the router's admin panel. It is 192.168.8.1 by default and can be changed if it conflicts with the upstream network.
- **Netmask**: Two options are available: 255.255.255.0 and 255.255.0.0.

12.2.2 DHCP Server

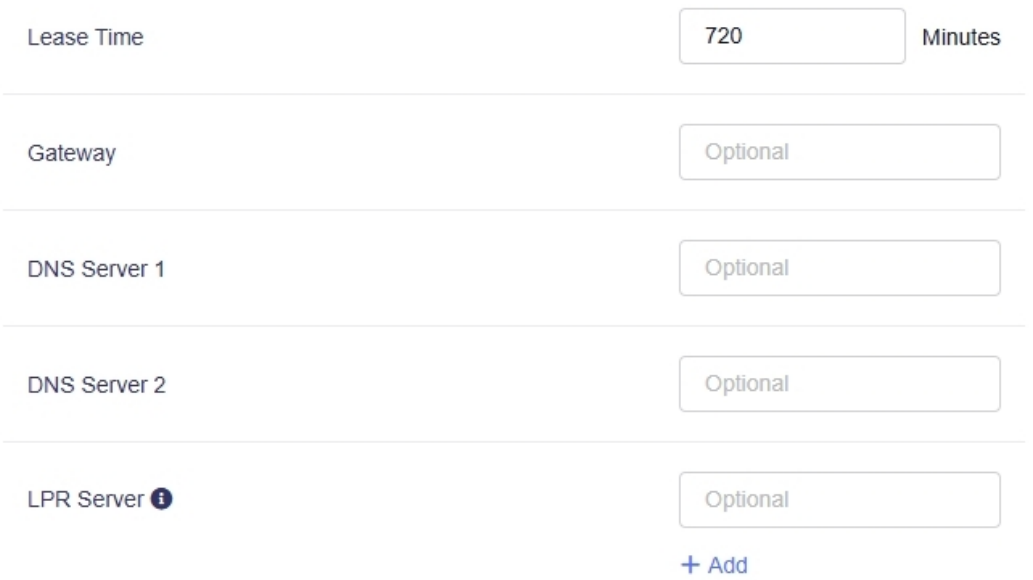
The DHCP server automatically assigns IP addresses and other communication parameters to each connected client. GL.iNet router's DHCP server is enabled by default, and the DHCP server's IP address pool ranges from 192.168.8.100 to 192.168.8.249. You can customize the address range as needed.



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



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



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

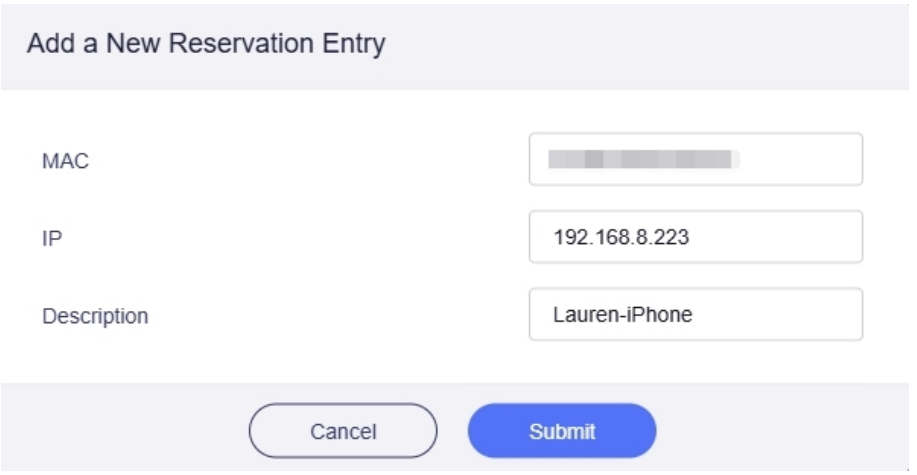
Note: If DHCP server is disabled, you need to configure static IP and other communication parameters manually for each clients. See here for details.

12.2.3 Address Reservation

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

Follow the steps below to configure address reservation as needed.

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



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

12.3 Guest Network

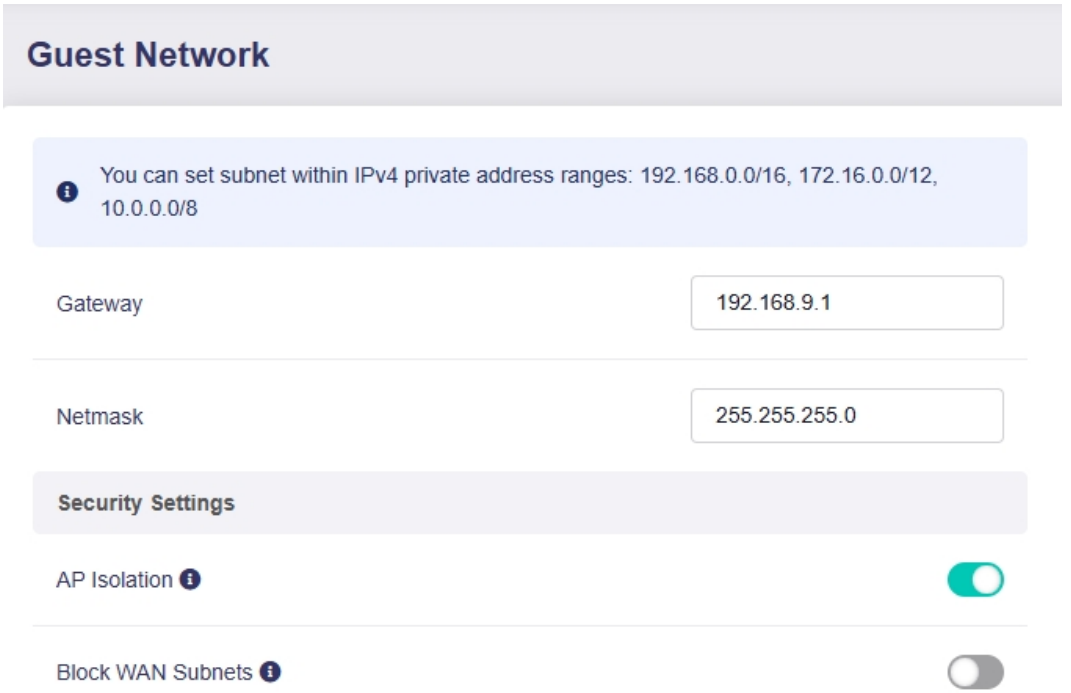
Guest Network refers to a dedicated network for visitors to connect to, isolating them from your main LAN to protect your private network security.

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.

Note: The Guest Wi-Fi is unavailable when Mudi 7 acts as a repeater.

12.3.1 Basic Settings

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

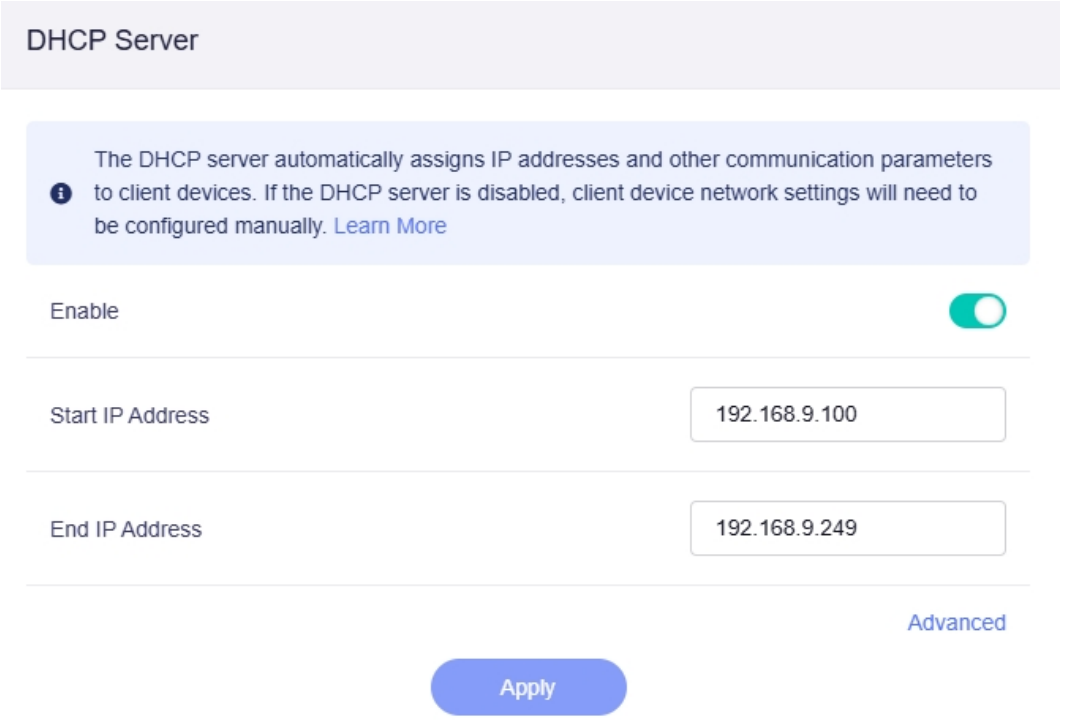


- **Gateway**: It is 192.168.9.1 by default and can be changed as needed, but it must not conflict with the gateway of the main network.
- **Netmask**: Two options are available: 255.255.255.0 and 255.255.0.0.
- **AP Isolation**: It is used to isolate guest network clients into separate segments so they 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.

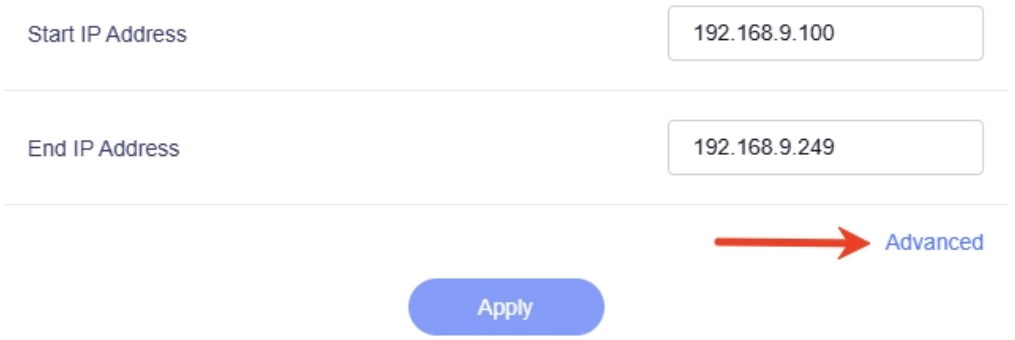
12.3.2 DHCP Server

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

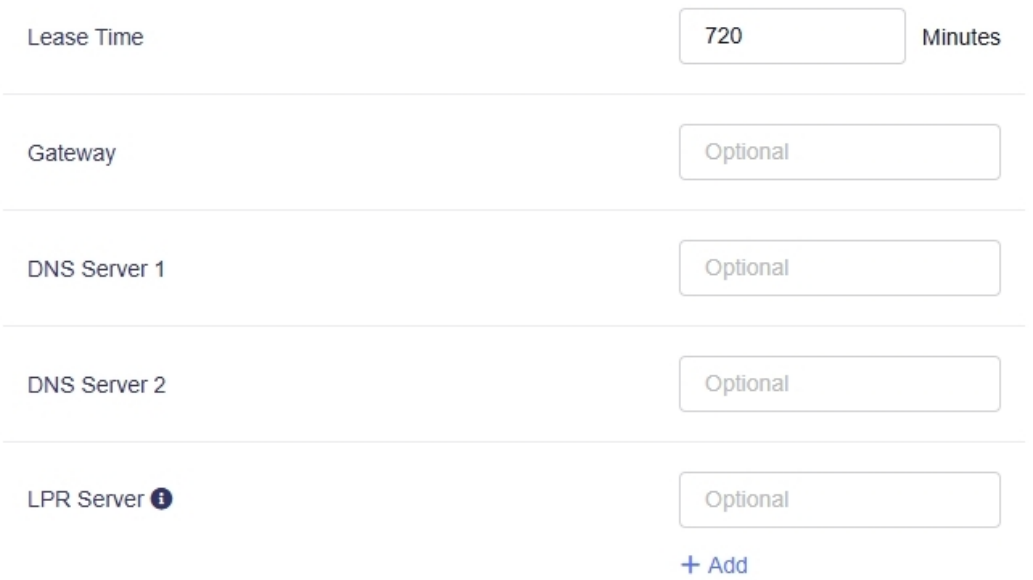
When enabled, the DHCP server automatically assigns IP addresses and other communication parameters to each connected client. The DHCP server's IP address pool for the Guest network ranges from 192.168.9.100 to 192.168.9.249. You can customize the address range as needed.



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



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



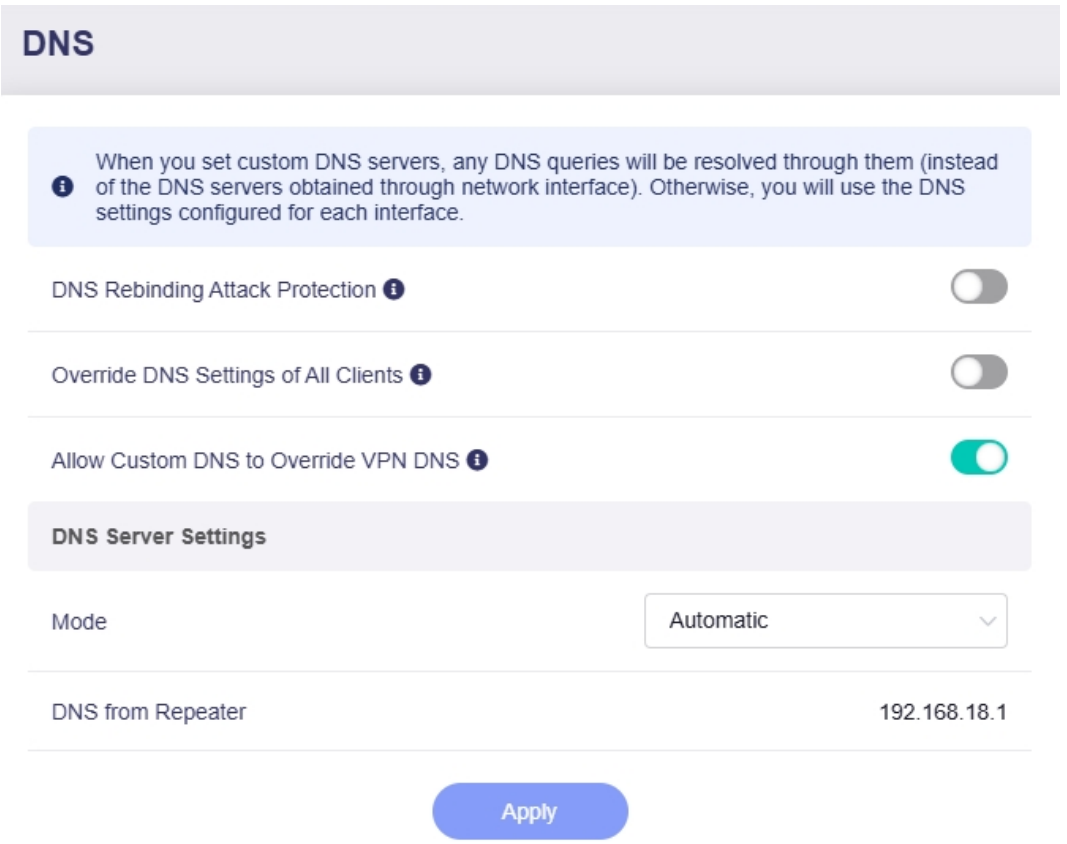
- **Lease Time**: The duration for which a device can use an IP address assigned via the Guest network's DHCP.
- **Gateway**: The router component that routes traffic between the guest network and external networks (e.g., the internet).
- **DNS Server 1**: The primary server responsible for translating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

12.4 DNS

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

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

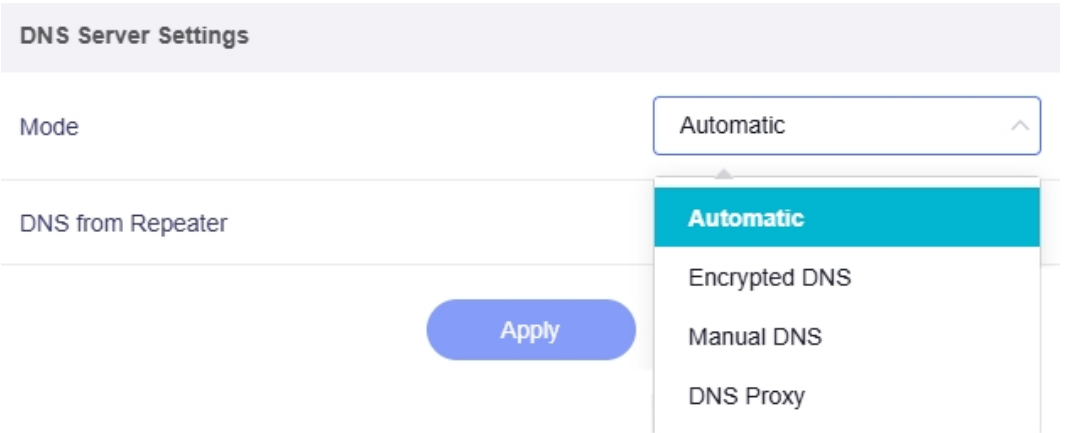
Log in to your router's web admin panel and navigate to **NETWORK** > **DNS**. This page allows you to configure DNS related settings, including security options, server modes, and DNS priority rules for different network scenarios.



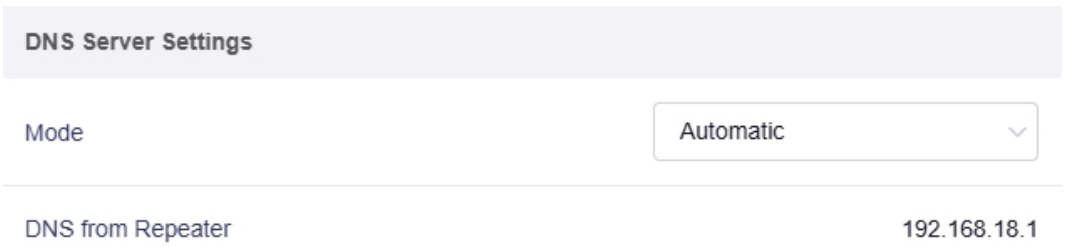
- **DNS Rebinding Attack Protection**: Protects against DNS rebinding attacks by blocking malicious DNS resolution attempts. Note that enabling it may cause private DNS lookup failure; disable if your network uses a captive portal (e.g., public Wi-Fi login pages).
- **Override DNS Settings of All Clients**: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

12.4.1 DNS Server Settings

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

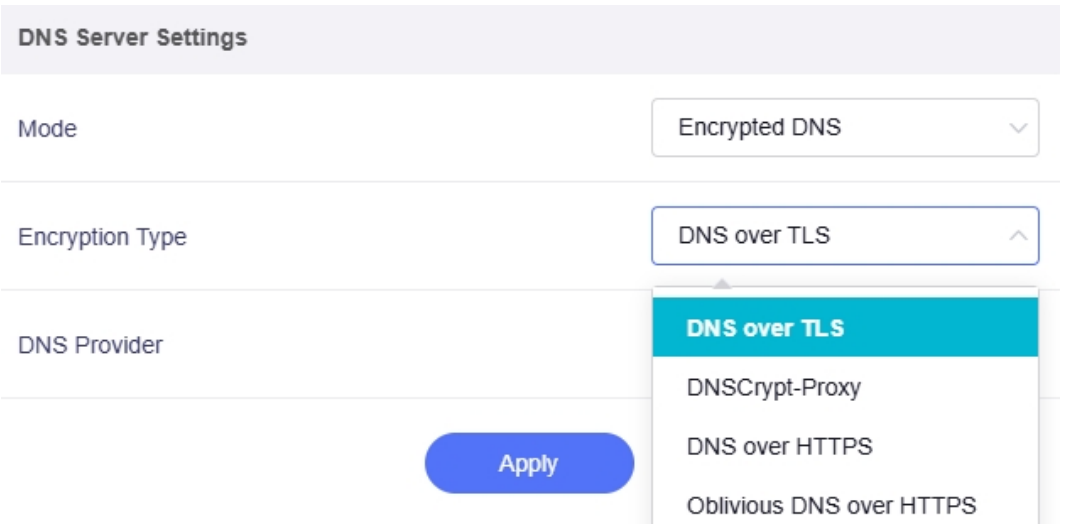


1. **Automatic**: When selected, the router will automatically obtain DNS server addresses from the upstream network and apply them to all connected devices.



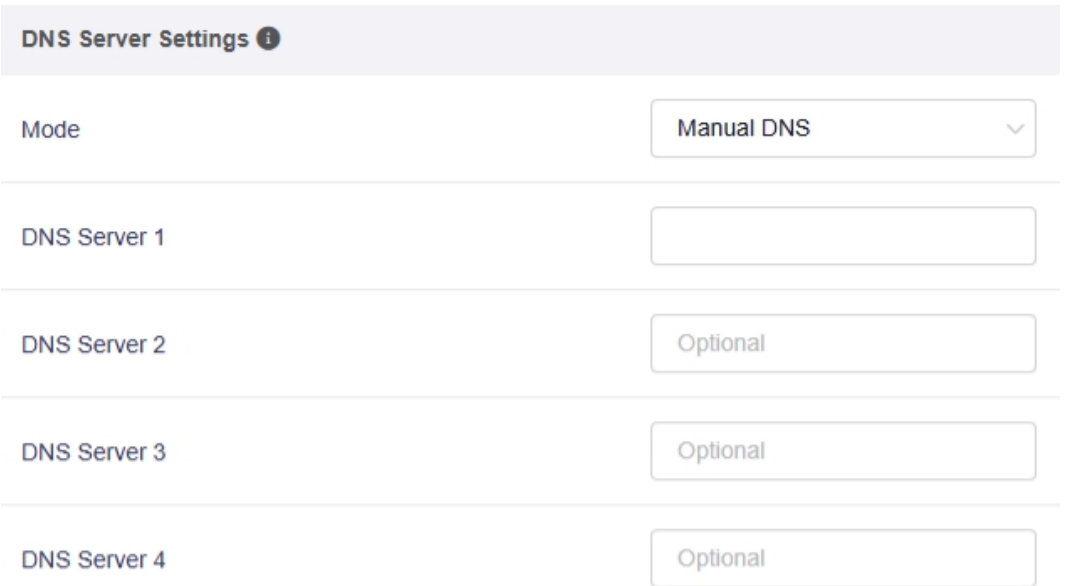
2. **Encrypted DNS**: When selected, the router will use encrypted protocols to process DNS queries, securing resolution data against eavesdropping or tampering.

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



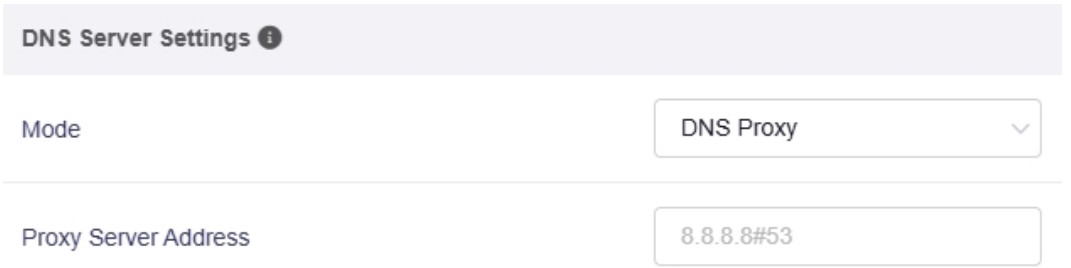
- For DNS over TLS, select a DNS provider among Control D, NextDNS, and Cloudflare.
- For the other three (i.e., DNSCrypt-Proxy, DNS over HTTPS, and Oblivious DNS over HTTPS), select at least one DNS server from the repository. Up to 8 servers can be selected. When multiple servers are selected, the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

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



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

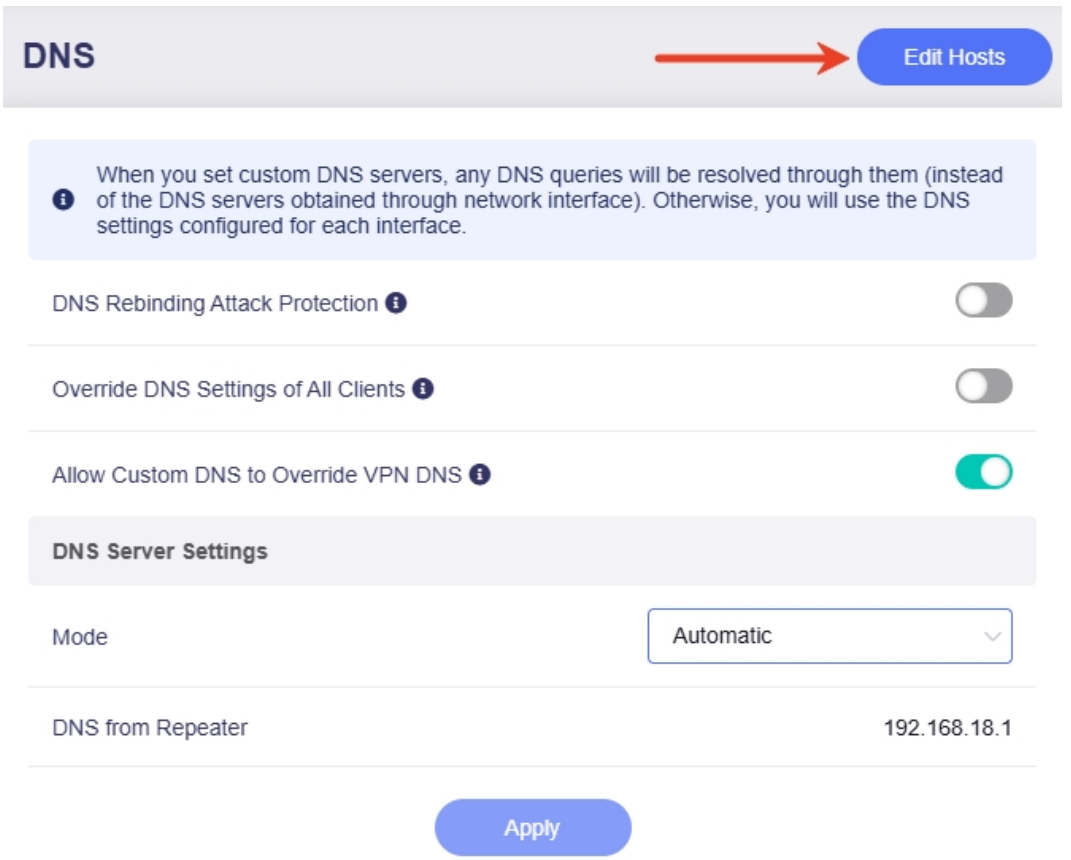
4. **DNS Proxy**: When selected, the router forwards all DNS queries through a proxy server, allowing resolution via the proxy's network environment for specific access needs.



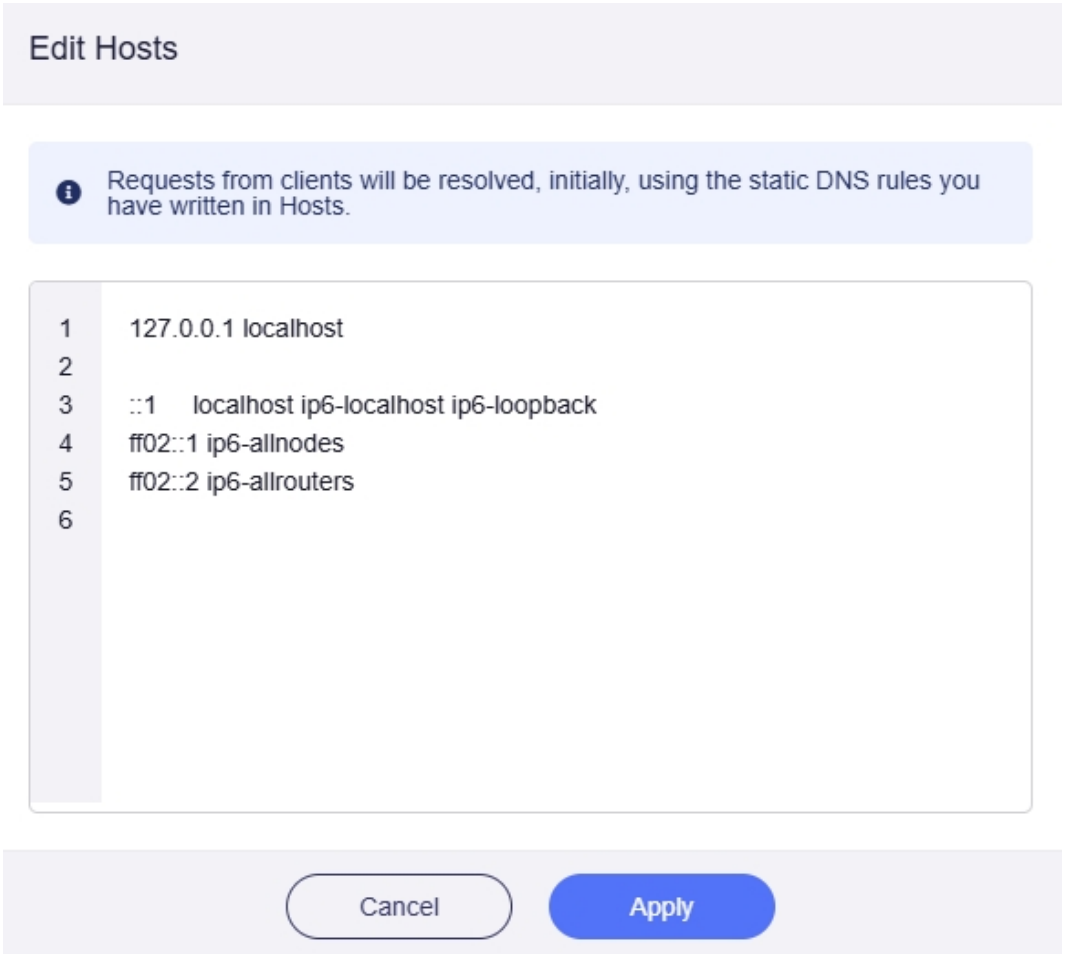
12.4.2 Edit Hosts

You can define static DNS resolution rules as needed.

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



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

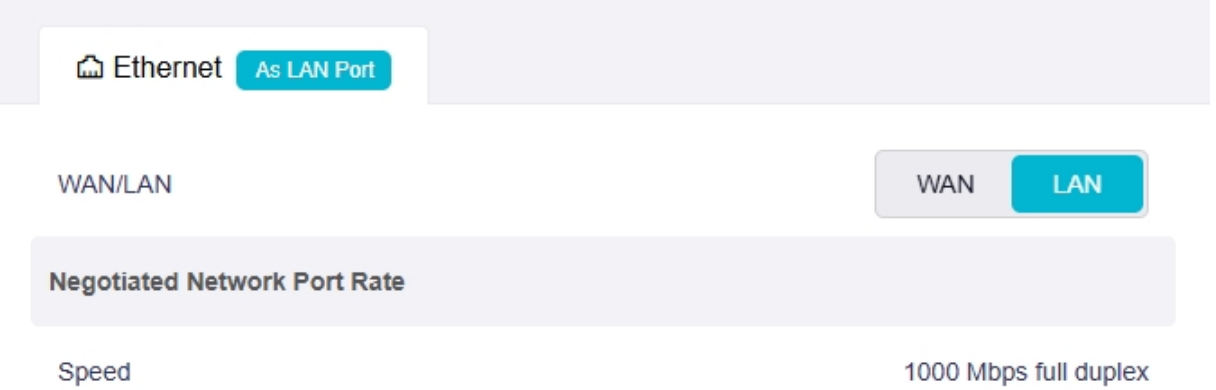

Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 Ethernet Port

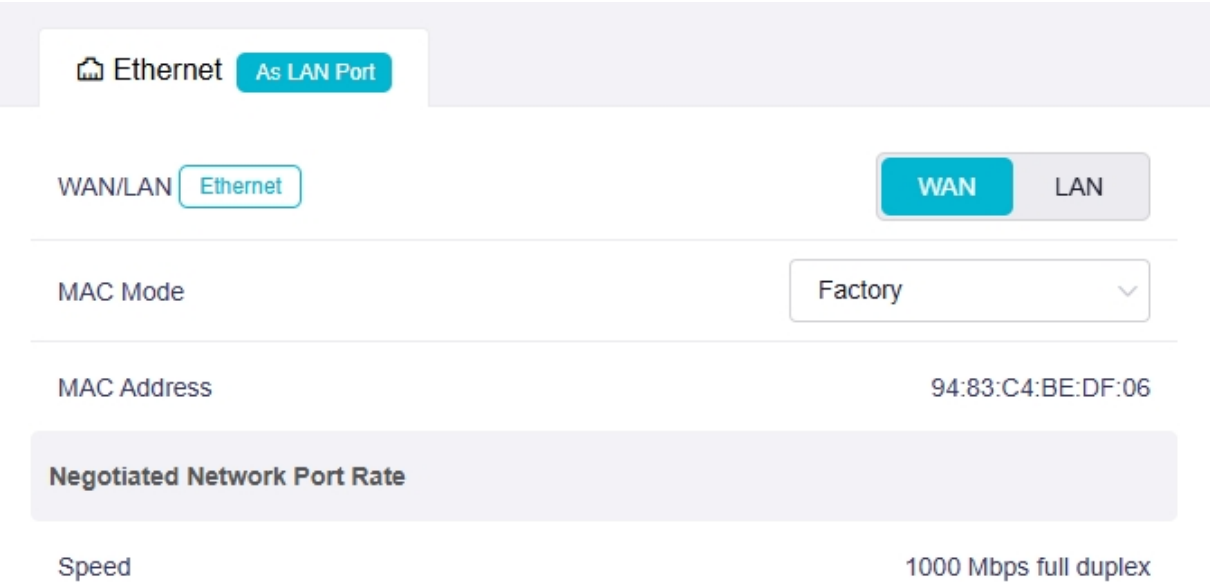
Log in to your router's web admin panel and navigate to **NETWORK** > **Ethernet Port**. This page allows you to manage the router's Ethernet ports.

Mudi 7 is equipped with an Ethernet port. This Ethernet port defaults to LAN, and you can adjust its port role between WAN and LAN port.

When acting as **LAN**, the page displays the port role and the negotiated rate.



When acting as **WAN**, the page displays the port role, MAC mode, MAC address, and the negotiated rate.



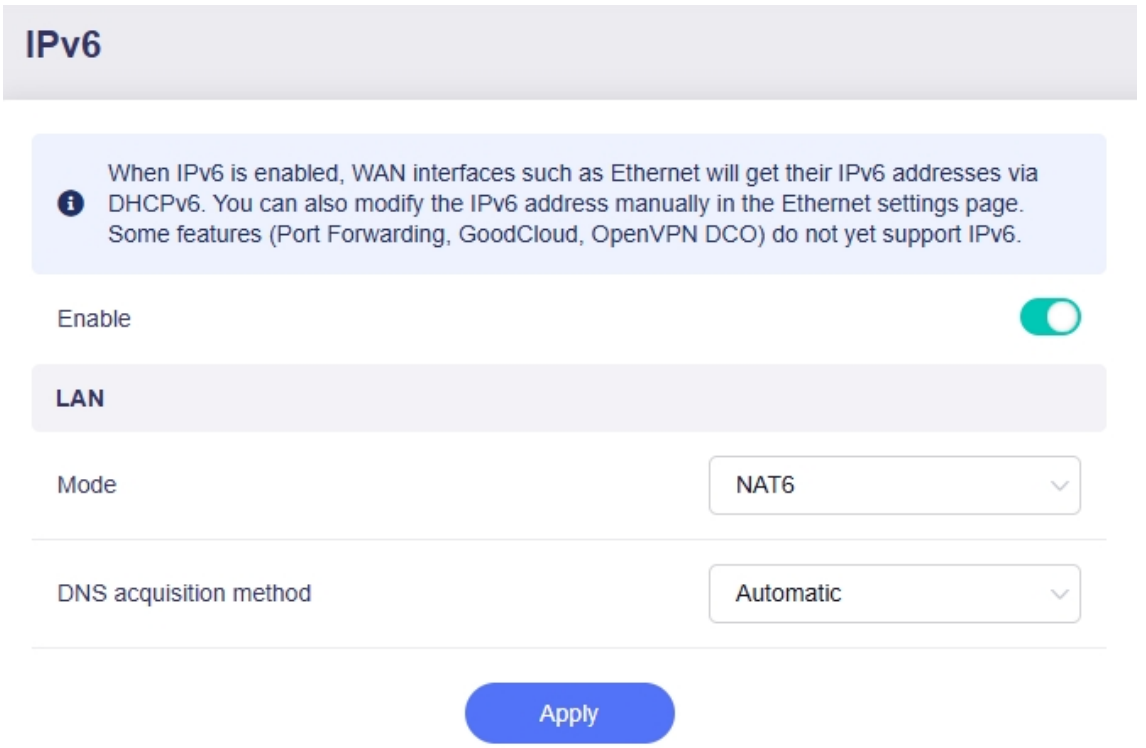
Note: The negotiated rate is displayed only when an Ethernet cable is connected. It depends on both the Ethernet port and the Ethernet cable.

12.6 IPv6

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

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

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



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

12.6.1 IPv6 Mode

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

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

12.6.2 DNS acquisition method

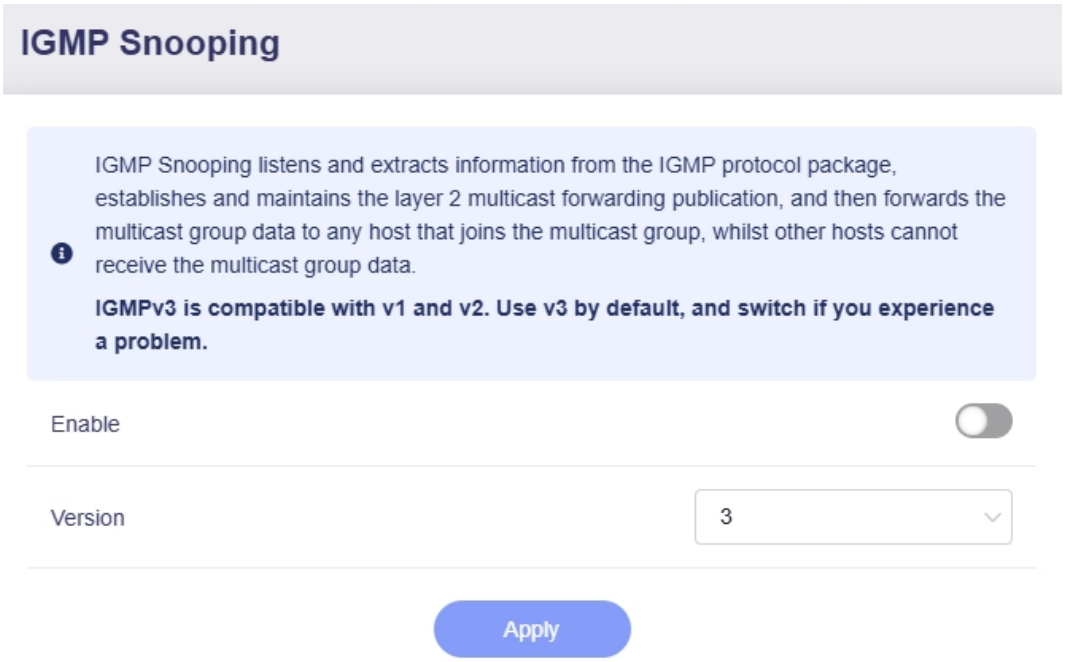
It determines how the router obtains IPv6 DNS server addresses. There are two options: Automatic and Manual.

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

12.7 IGMP Snooping

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

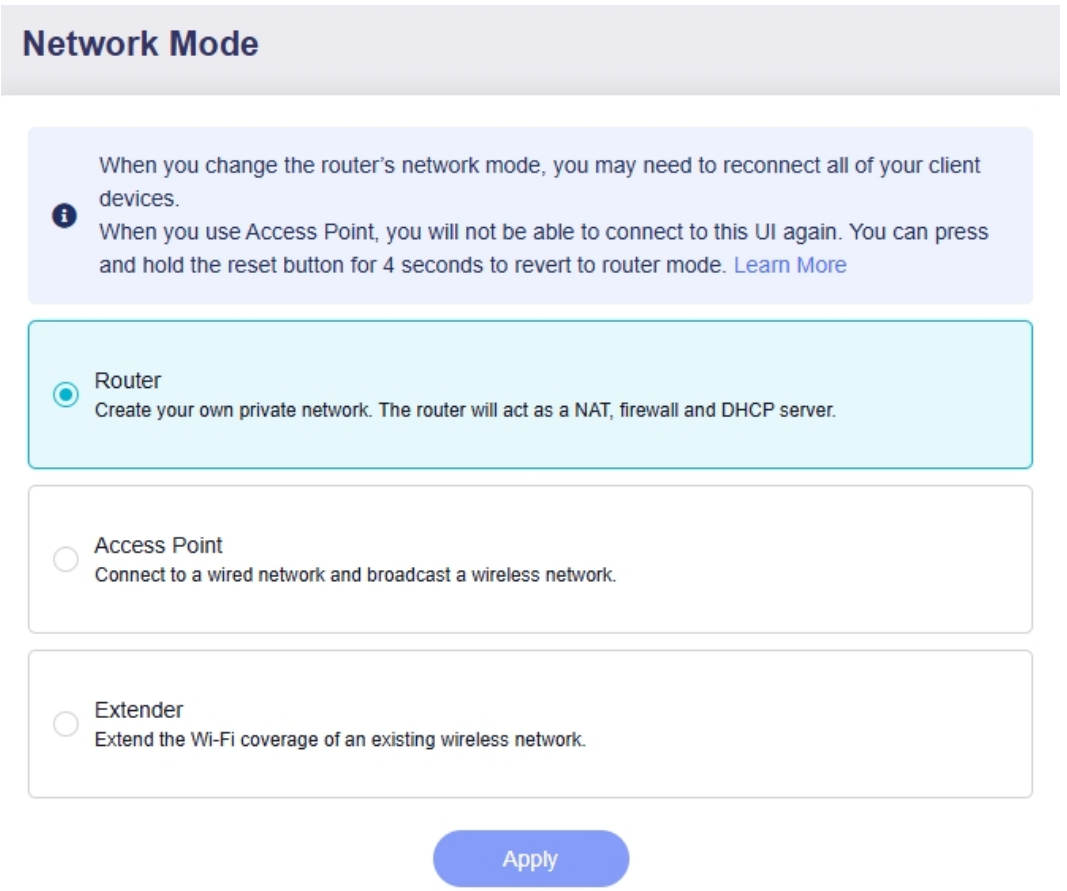
Log in to your router's web admin panel and navigate to **NETWORK** > **IGMP Snooping**. You can enable it to use the multicast function on your router as needed.



12.8 Network Mode

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

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



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

functions, operating purely as a wireless signal transmitter and switch rather than a standalone gateway.

- **Extender**: This mode is designed to extend the Wi-Fi coverage of an existing wireless network and eliminate signal dead zones in areas with poor connectivity. It enables the router to wirelessly receive signals from the main router, amplify them, and retransmit the boosted signal. Unlike Access Point mode, it requires no wired connection to the main router, but it may lead to bandwidth halving, as the device has to handle simultaneous signal reception and transmission.

Note:

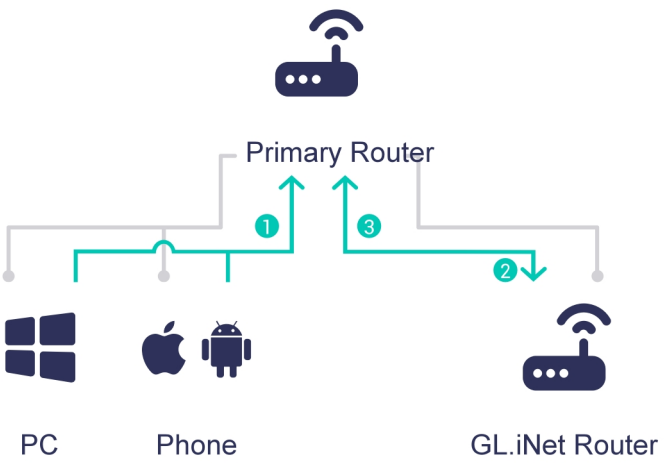
1. When the network mode is changed, all client devices shall reconnect to the router for stable network connectivity.
2. **In Access Point mode, you will not be able to access the web admin panel using the original IP address**. Instead, you need to log in to the upstream router to find the IP address 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 mode, the following features will be unavailable**: Access Control (Allowlist and Blocklist), AstroWarp, VPN, AdGuard Home, Parental Control, ZeroTier, Tailscale, Port Forwarding, Multi-WAN, DHCP Server, Address Reservation, Guest Network, DNS, Ethernet Port, IPv6, Drop-in Gateway, IGMP Snooping, Network Acceleration, NAT Settings.

12.9 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 as needed.



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

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

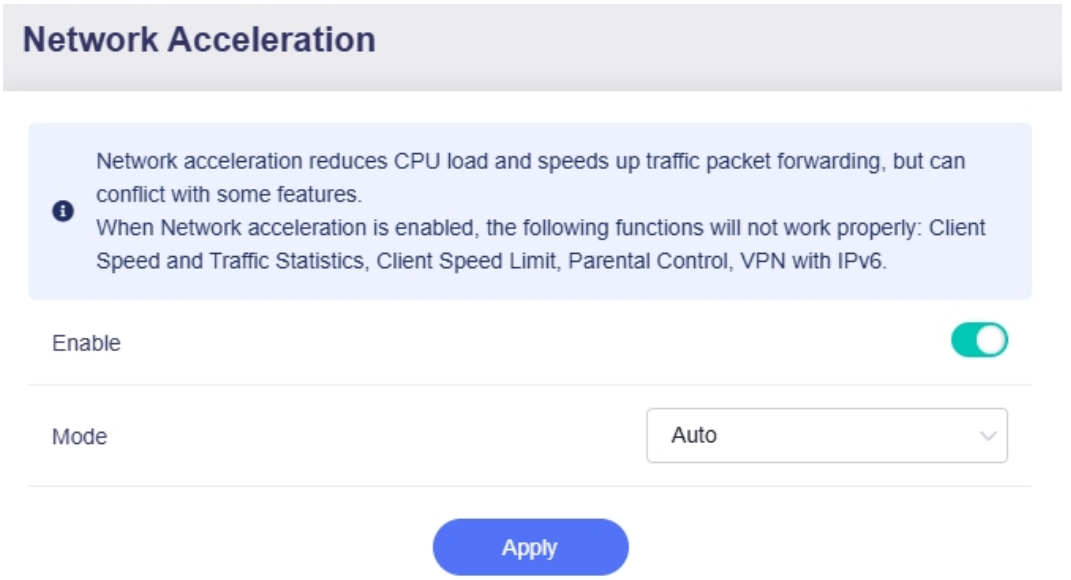
- **Green lines** depict the sequential data transmission path when Drop-in Gateway is active, with the numbered arrows indicating the traffic flow order:
    1. Traffic from client devices is first routed to the primary router;
    2. The primary router forwards the traffic to the GL.iNet router for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

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

12.10 Network Acceleration

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

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



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

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

Chapter 13

Flow Control

This chapter introduces a flow control feature: Parental Control.

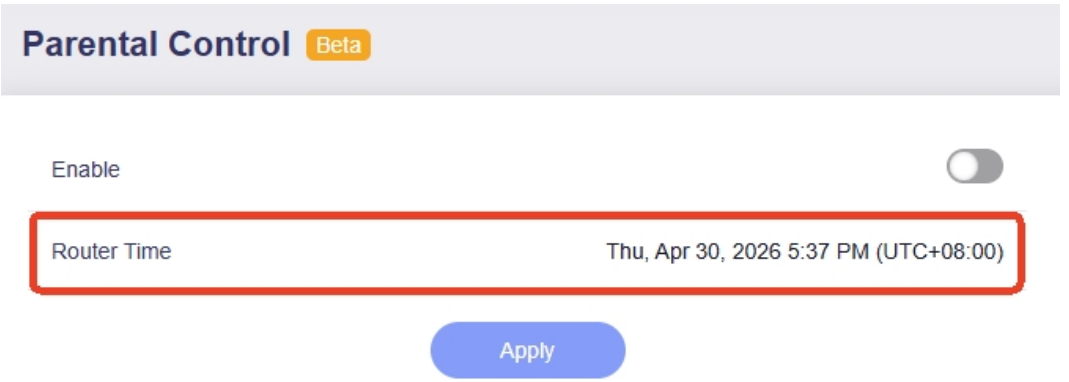
13.1 Parental Control

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.

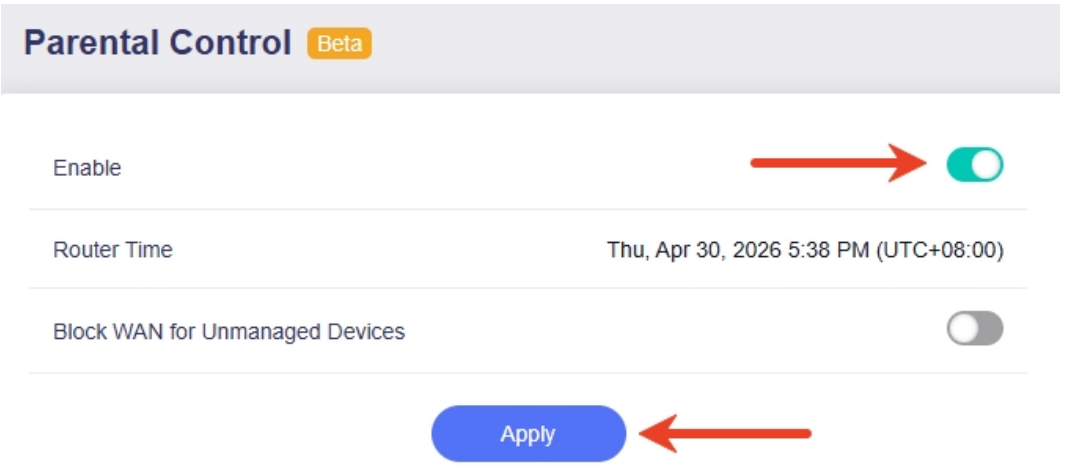
13.1.1 Quick Setup

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



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



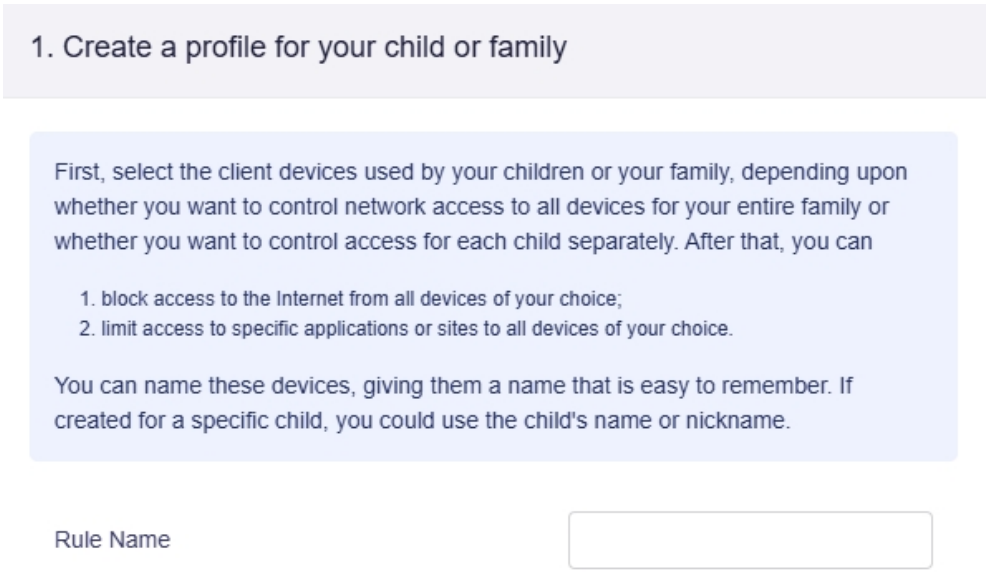
- **Block WAN for Unmanaged Devices**: Blocks internet access for all devices that are not on the Parental Control list.

Here is a use case for your reference.

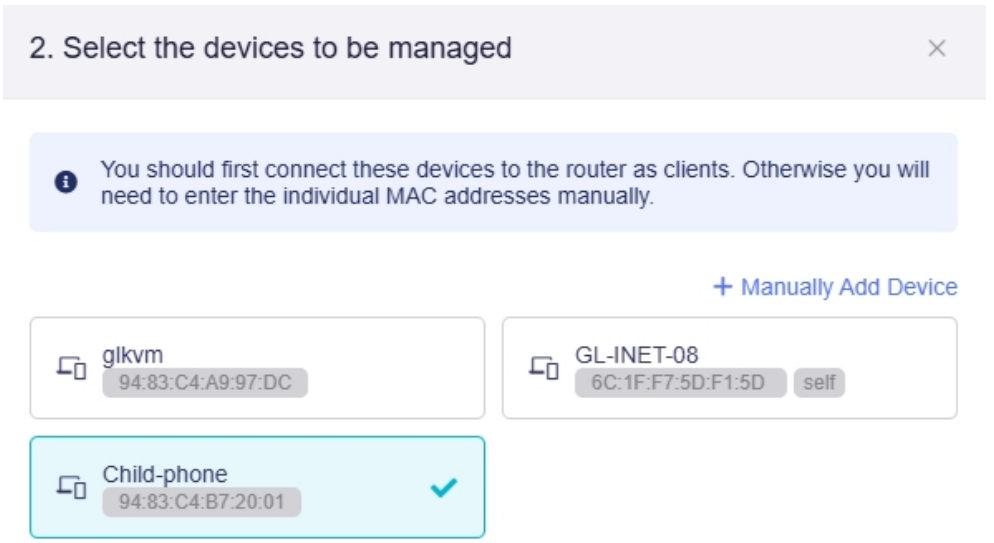
Scenario: Devices in this profile are only allowed to access the Internet for study from 8 AM to 11 AM on weekdays, and for gaming from 6 PM to 8 PM on weekends. Internet access is blocked by default at all other times.

Setup Steps:

1. Create a profile and customize a name.



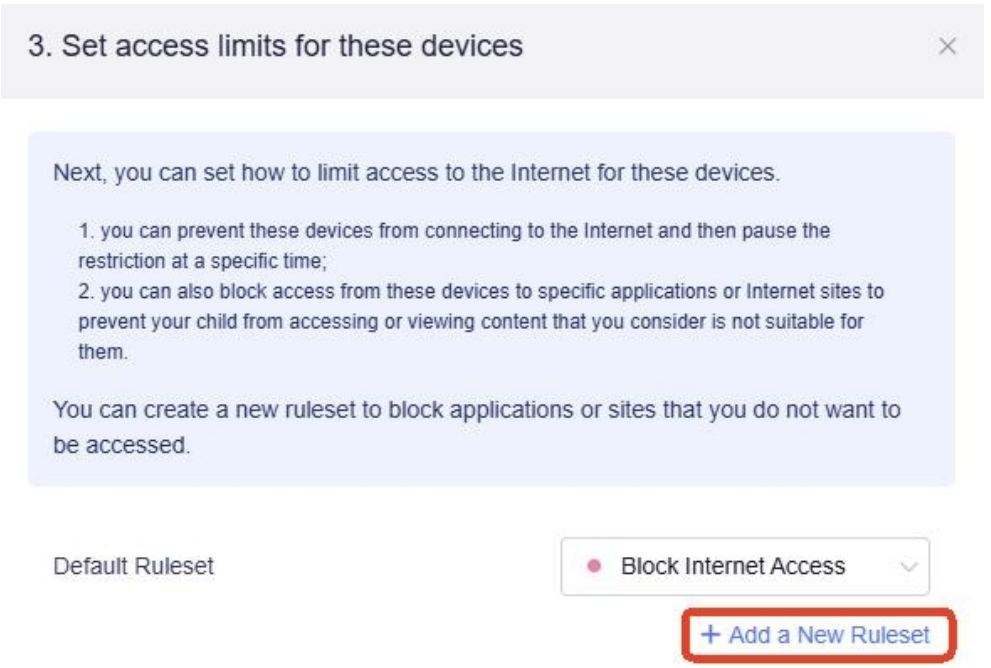
2. Select the devices you want to manage. Connect them to the router first. If they have not been connected to the router, add them manually by entering their MAC addresses.



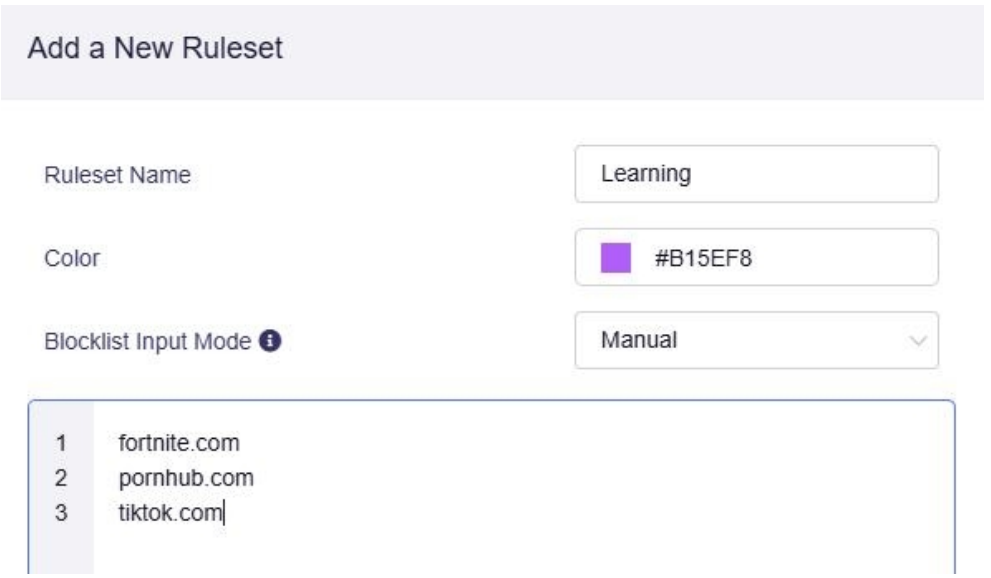
3. Set access limit.

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

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

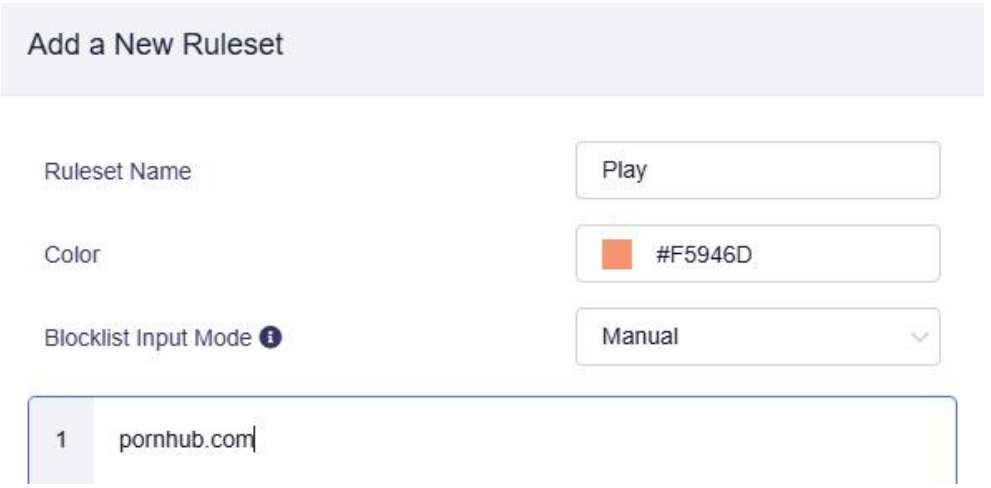


Specify the ruleset name (e.g., Learning) and color, enter the websites to block, then click **Apply**.

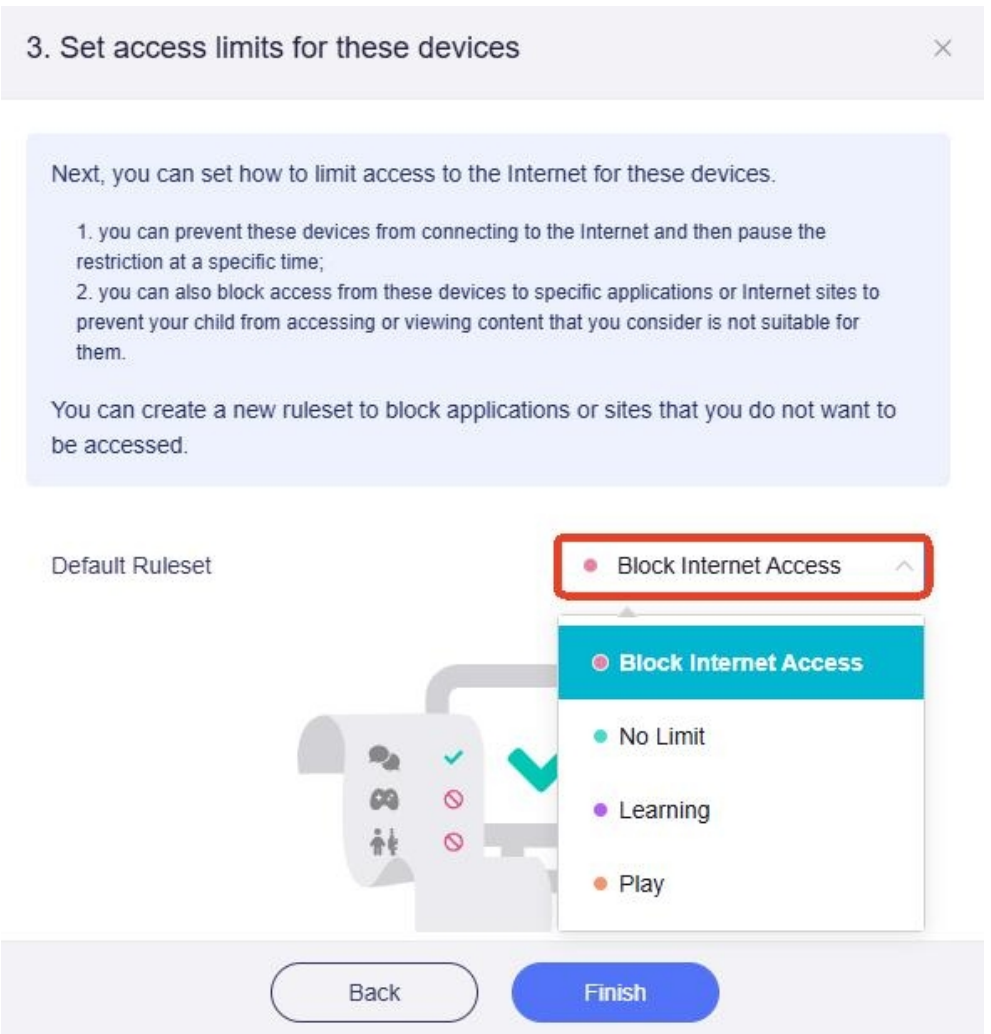


Note: The domain names entered in the blocklist should include their subdomains. For example, if "example.com" is entered, it also includes any subdomain, such as "subdomain.example.com".

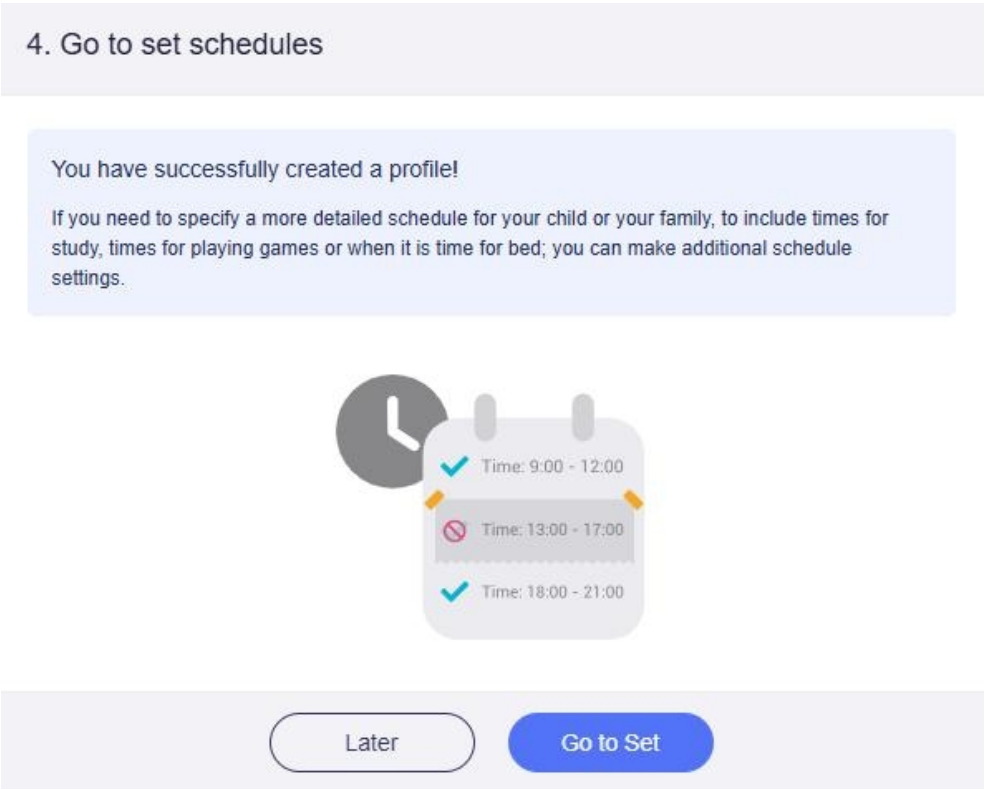
Similarly, create another ruleset. Specify the ruleset name (e.g., Play) and color, enter the websites to block, then click **Apply**.



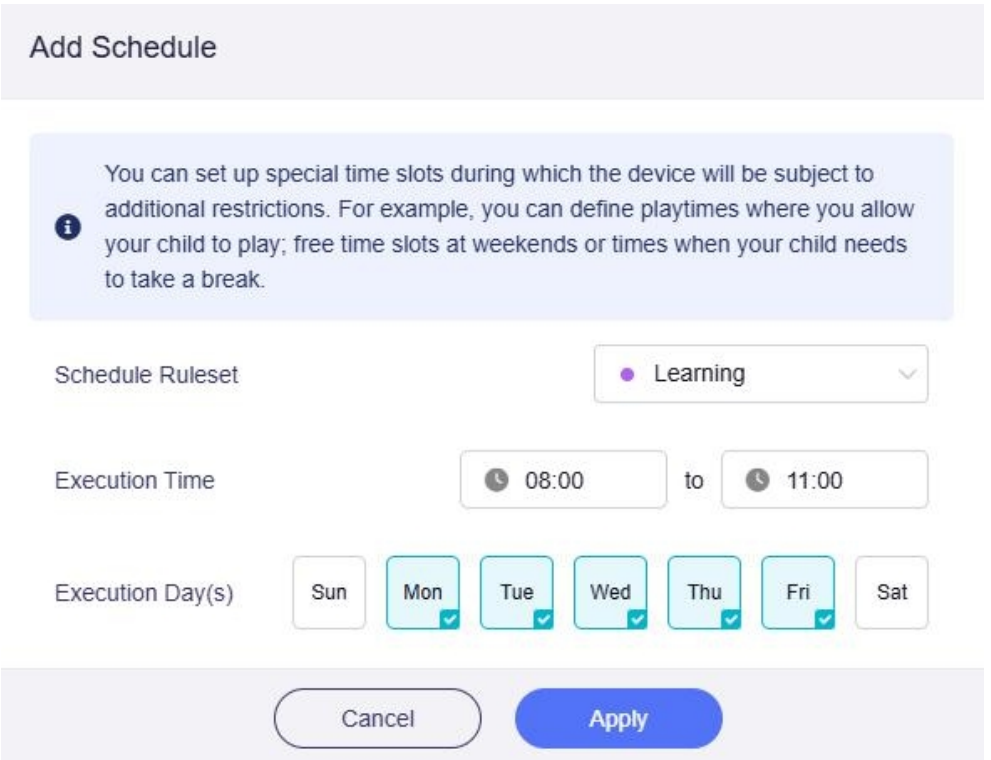
Upon applied, there will be a total of four rulesets. Select **Block Internet Access** as the **Default Ruleset**, and click **Finish**.



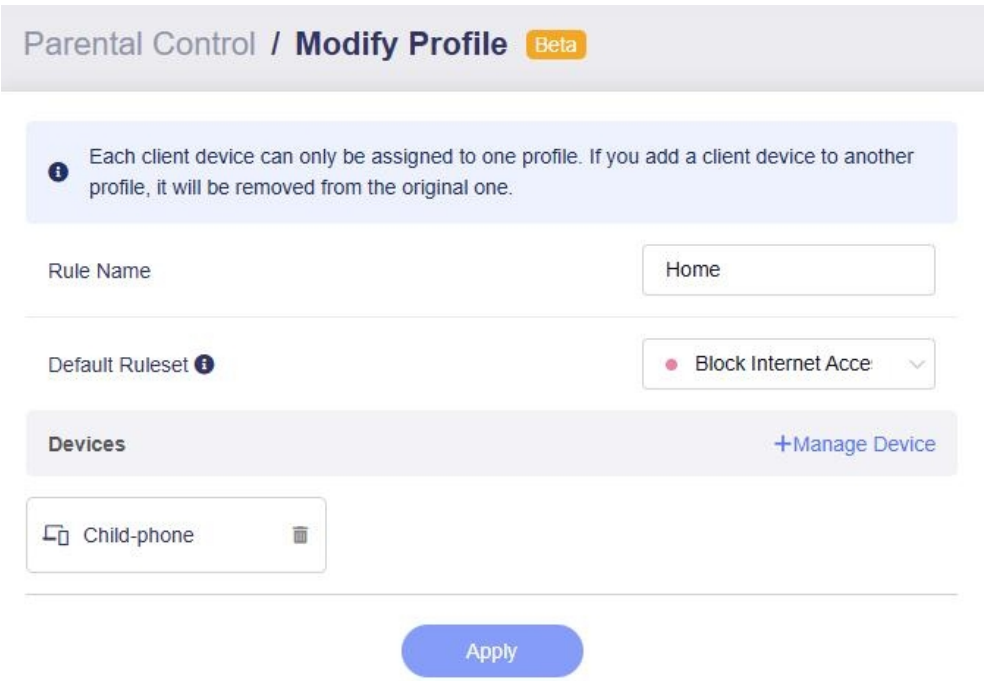
4. Next, set schedule for your profile. Click **Go to Set**.



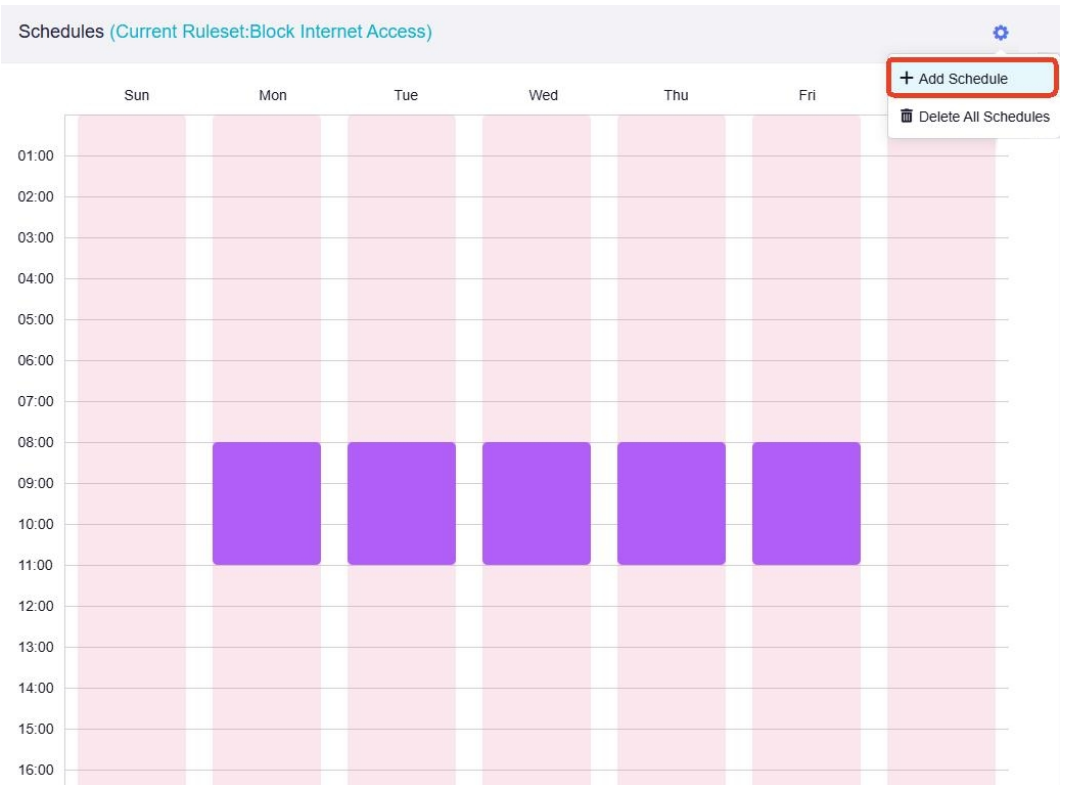
Add the **Learning** ruleset to the schedule. Set the **Execution Time** from 8 AM to 11 AM on weekdays, then click **Apply**.



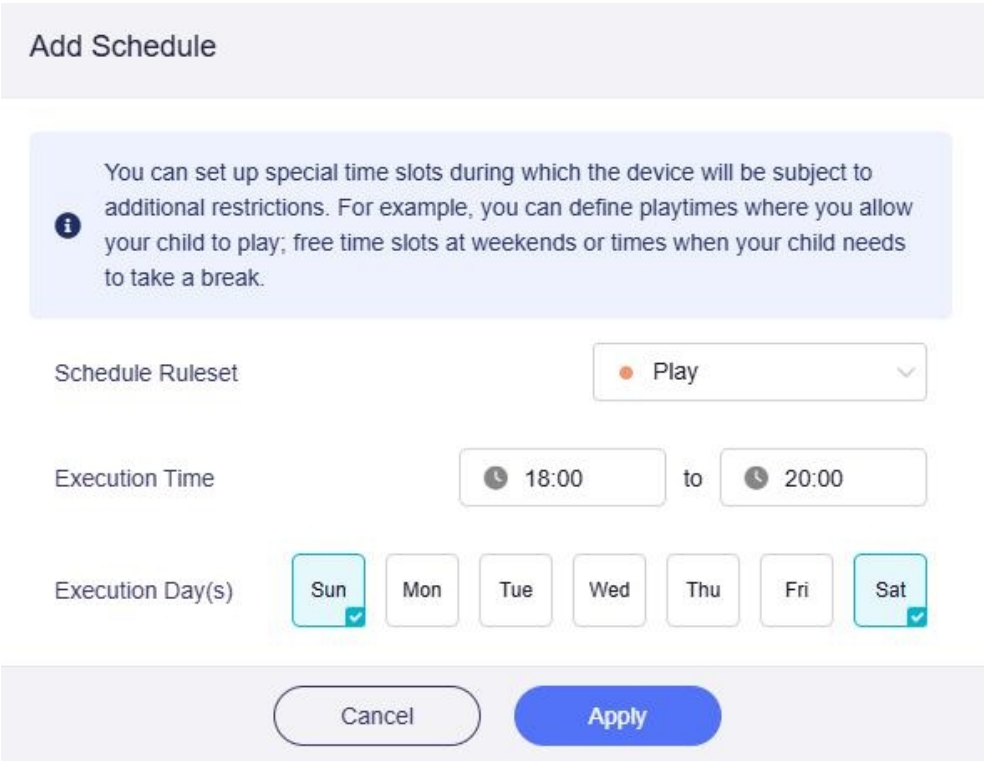
5. You will be redirected to the edit page of the created profile.



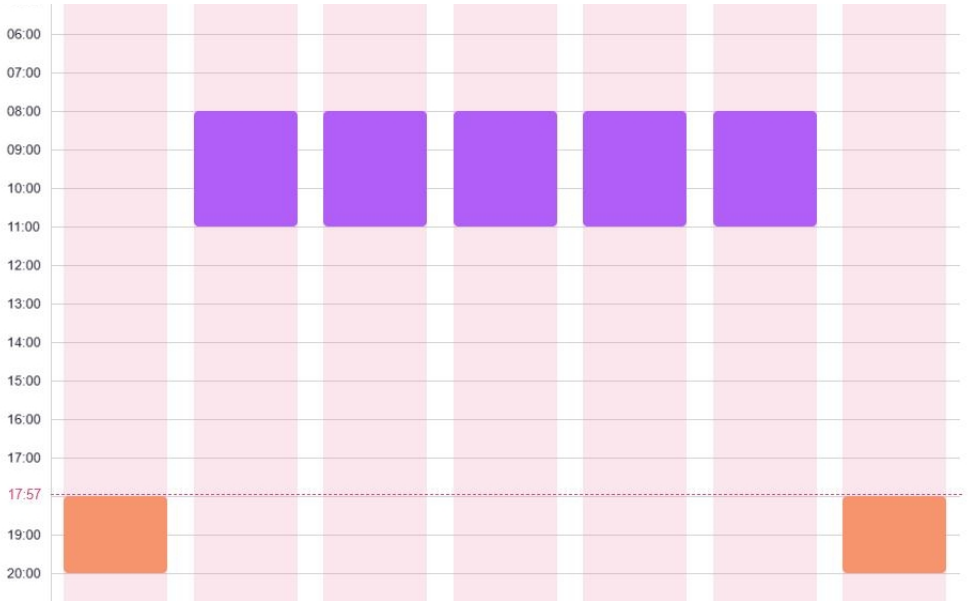
Move to the bottom, and you will see that a schedule has been created. Click the gear icon in the upper right and select **Add Schedule**.



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



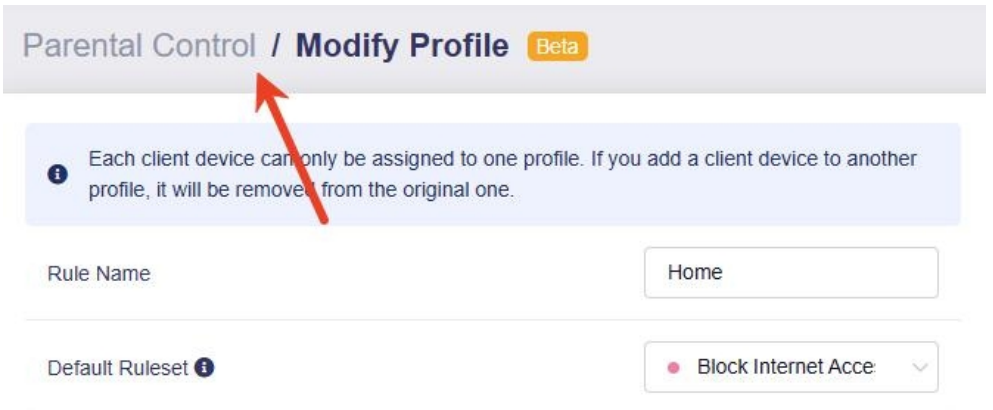
The Play ruleset will then be added into the schedule.



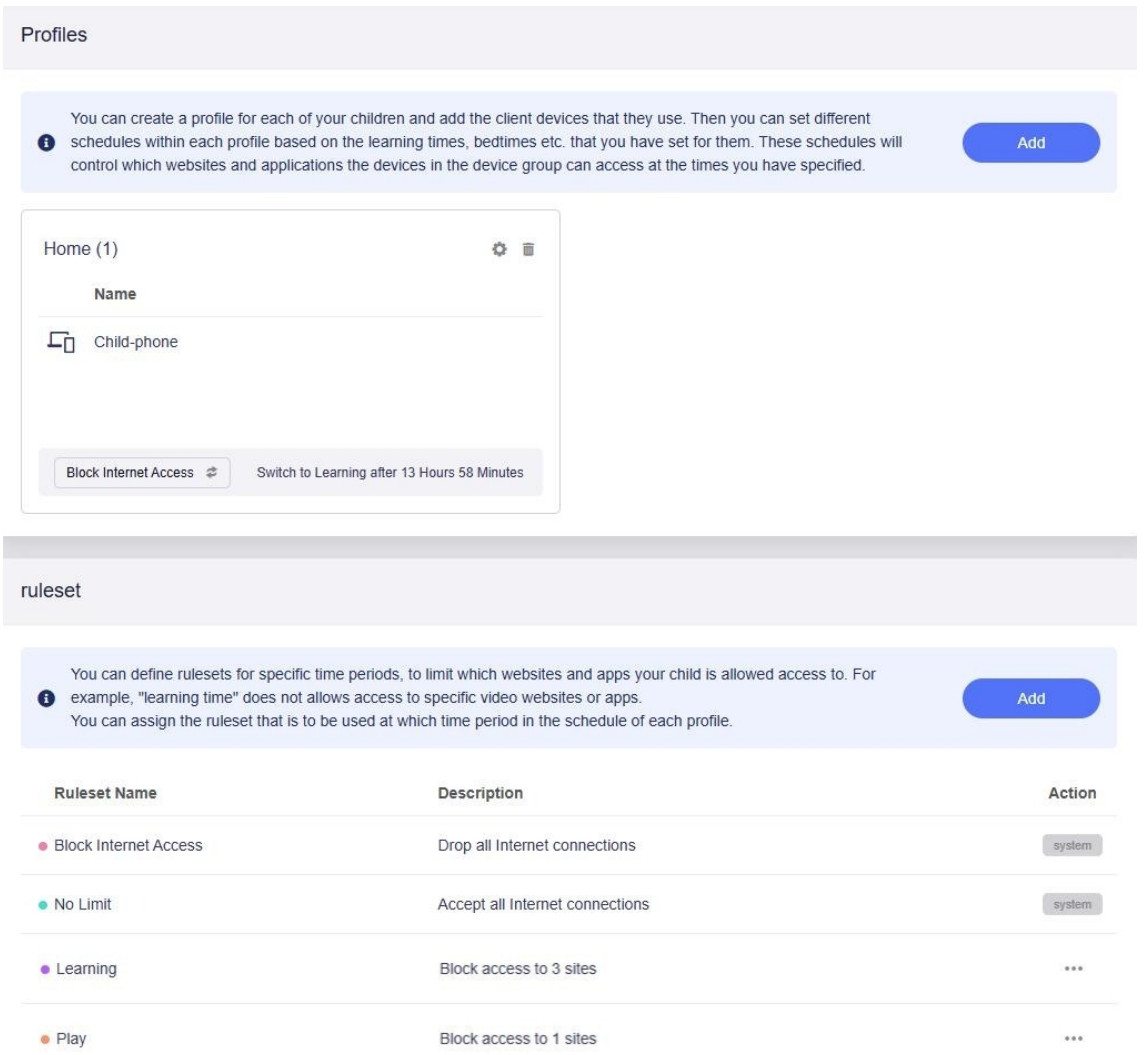
Tips:

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

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



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



13.1.2 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.

Chapter 14

Security

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

14.1 Port Forwarding

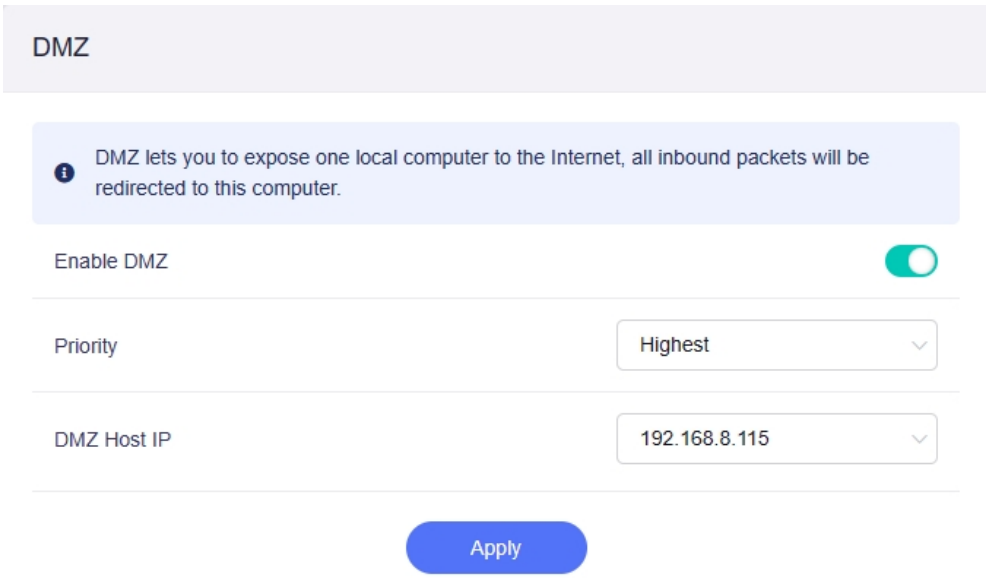
Port forwarding is a network feature that routes external requests to specific devices on your local network. The Port Forwarding page includes two key functions: **DMZ** (for direct full access to a single device) and **Port Forwarding** (for targeted access to specific ports of devices).

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 as needed.

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



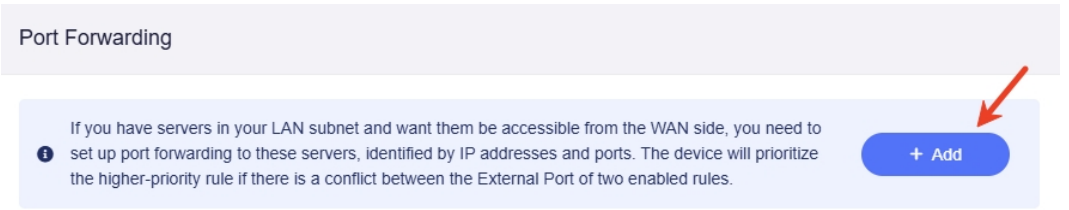
- **Priority**: Set it as Highest or Lowest. If the priority of the DMZ is higher than the port forwarding rules, all port forwarding rules will be invalidated. Otherwise, requests will be forwarded to the DMZ client device only if the accessed port has no corresponding port forwarding rule.
- **DMZ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

14.1.2 Port Forwarding

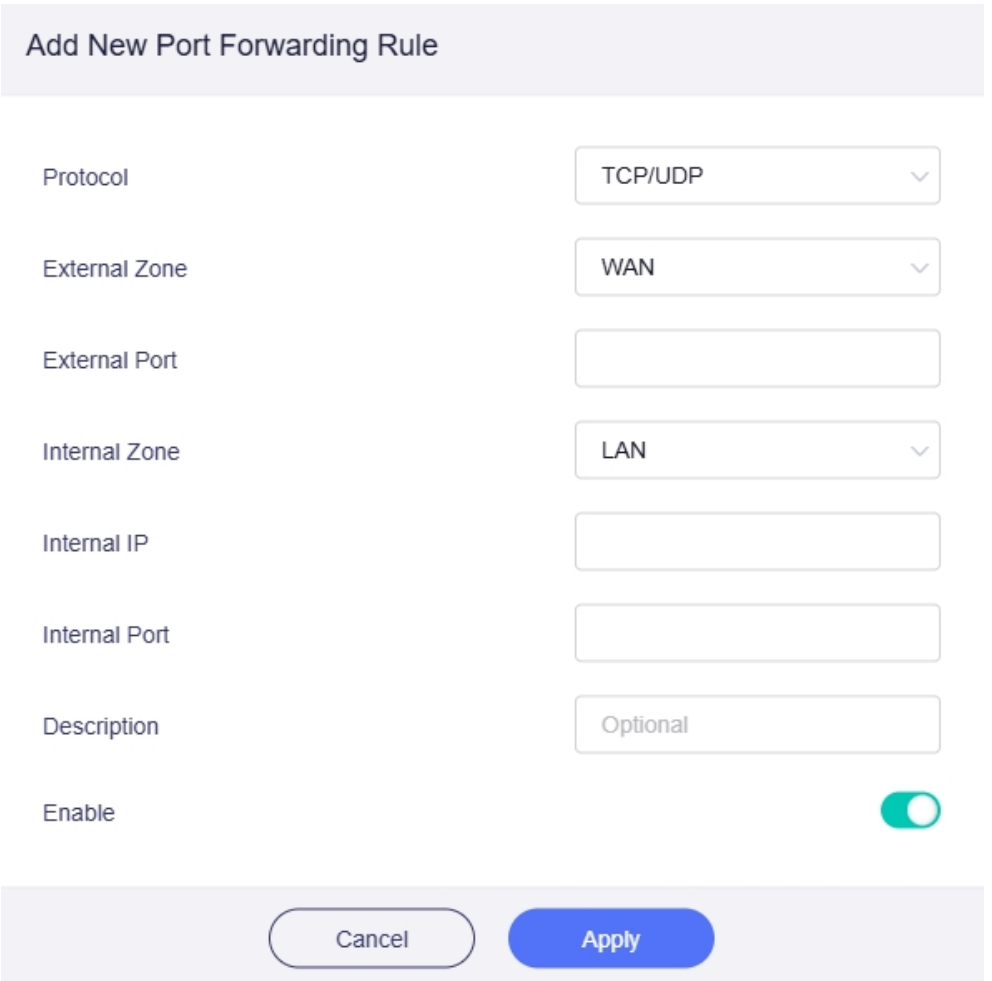
Port Forwarding enables remote computers to connect to a local computer or server behind the LAN firewall (e.g., web servers, FTP servers).

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

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



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



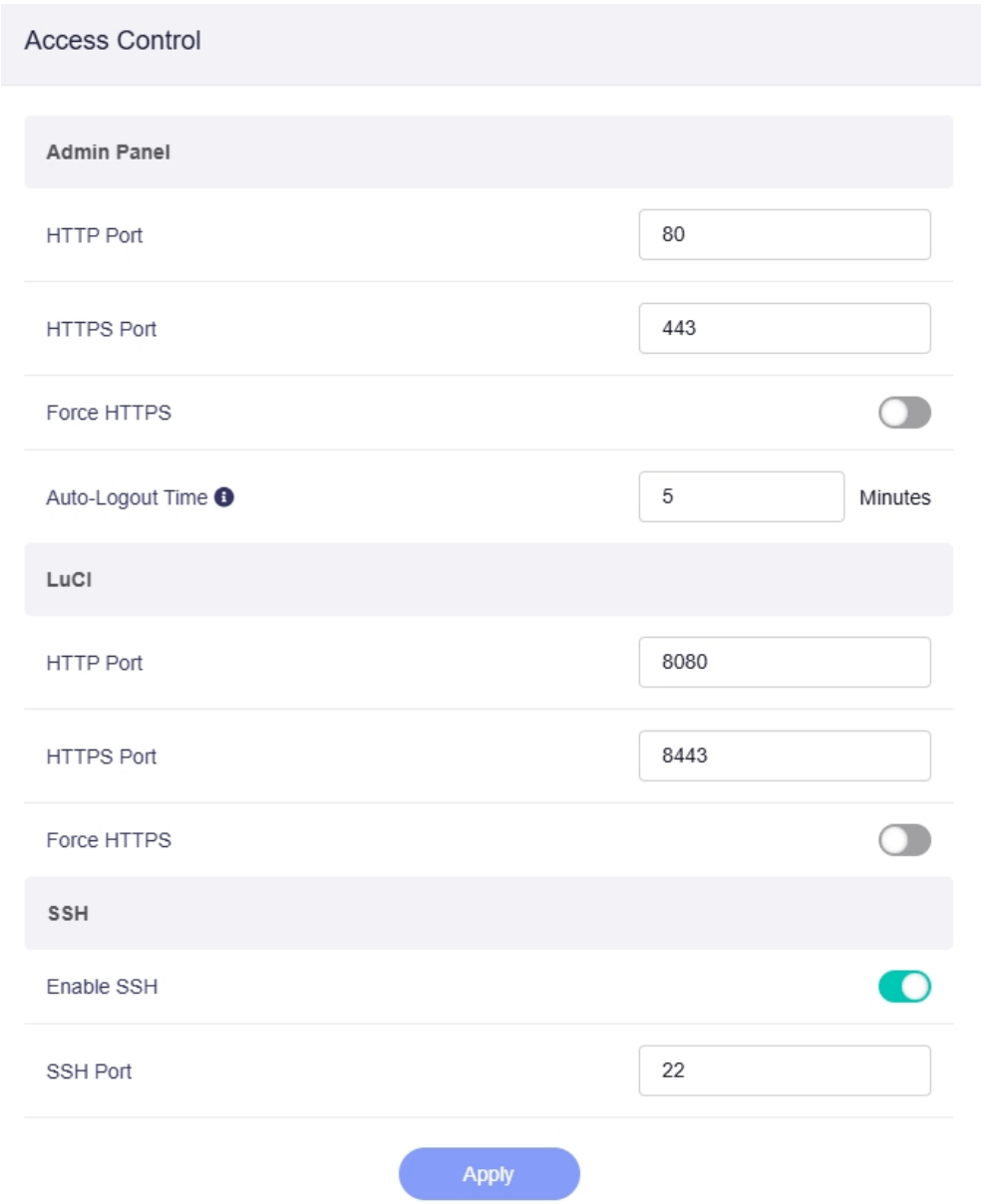
- **Protocol**: The protocol used. You can choose TCP, UDP, or both TCP and UDP.
- **External Zone**: Available options are WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, and LAN.
- **External Port**: The number(s) of external ports. Enter a specific port number here. The port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

14.2 Management Control

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

14.2.1 Access Control

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



Admin Panel

- **HTTP Port**: Defaults to 80, used for unencrypted HTTP access to the web admin panel.
- **HTTPS Port**: Defaults to 443, used for secure HTTPS access to the web admin panel.
- **Force HTTPS**: When enabled, access to the web admin panel is enforced to use a secure HTTPS connection.
- **Auto-Logout Time**: Set to 5 minutes by default, it automatically logs out idle admin sessions after this duration for security. You can customize the auto-logout time, ranging from 1 minute to 3 hours.

LuCI

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

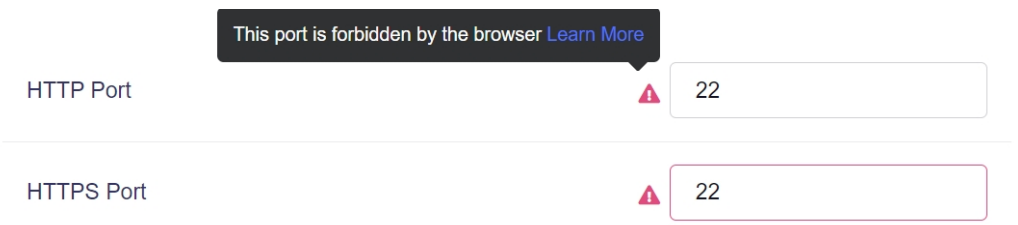
- **HTTP Port**: Defaults to 8080, for unencrypted HTTP access to the LuCI interface.
- **HTTPS Port**: Defaults to 8443, for secure HTTPS access to the LuCI interface.
- **Force HTTPS**: When enabled, access to the LuCI interface is enforced to use a secure HTTPS connection.

SSH

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

Note:

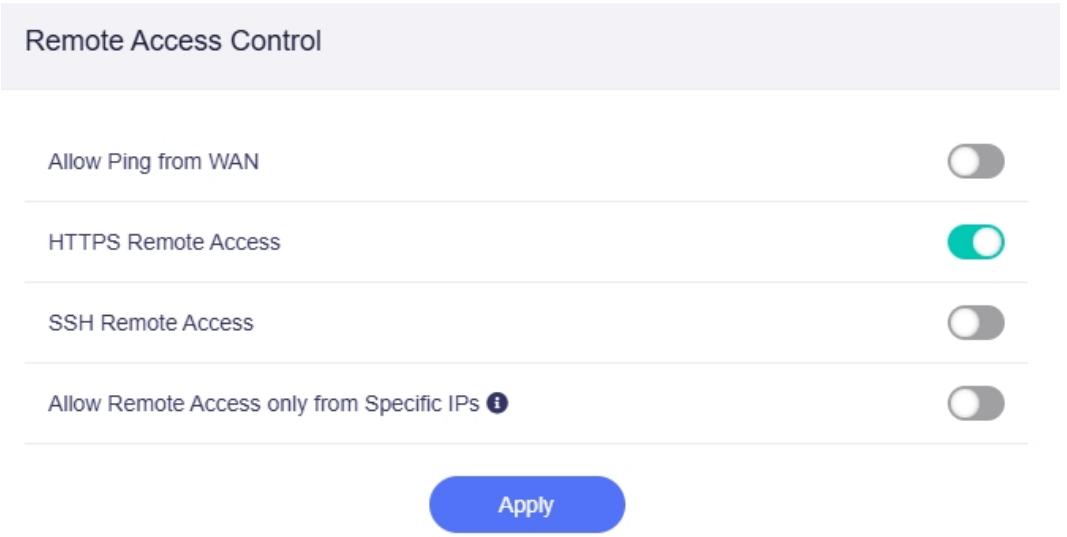
1. If you assign a port number that conflicts with a reserved port (or one reserved for specific services by browsers/network conventions), a prompt will appear stating "This port is forbidden by the browser".



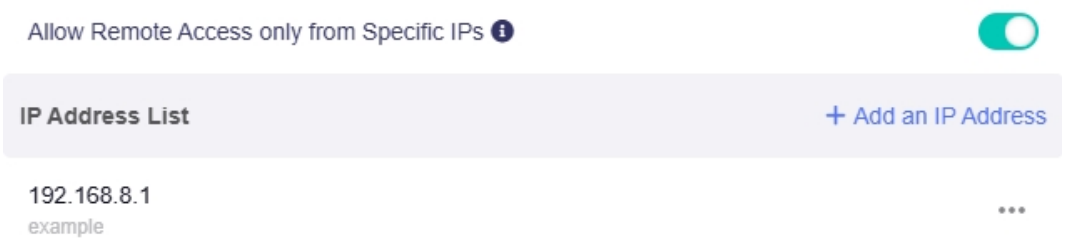
2. If the port number is modified in the firmware, you need to enter the correct port number to access the admin panel. If you forgot the port number, please reset the router to restore the default port number.

14.2.2 Remote Access Control

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

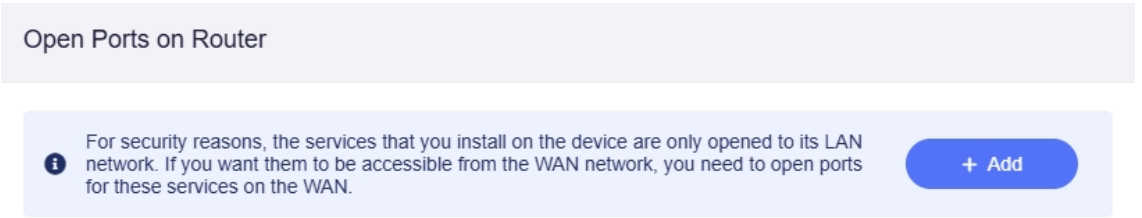


- **Allow Ping from WAN**: Allowing Ping from the router's WAN side can help users check whether the router is reachable over the WAN when there is a network issue, as well as determine network latency and packet loss.
- **HTTPS Remote Access**: HTTPS Remote Access enables secure remote access to the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

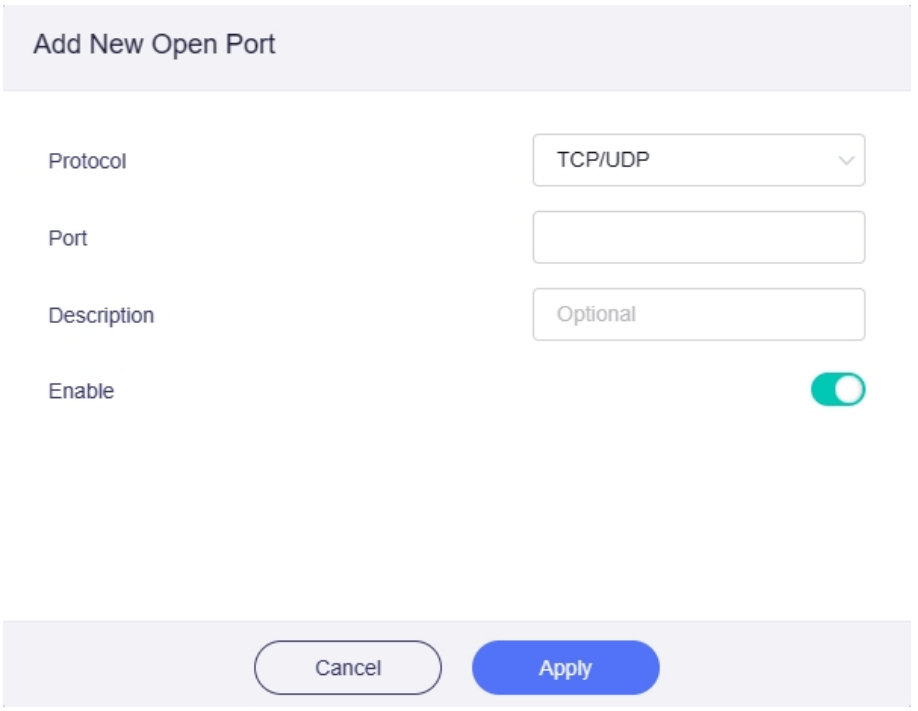


14.2.3 Open Ports on Router

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



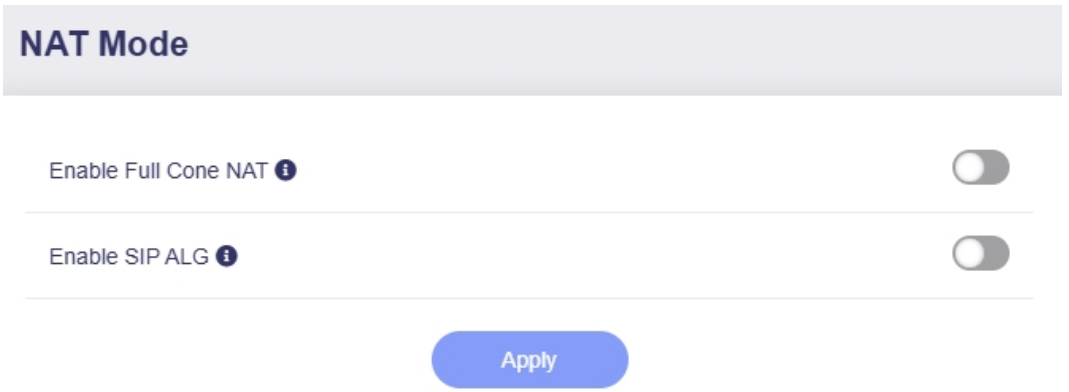
To open a port, click **Add**, and enter the required information in the pop-up window.



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

14.3 NAT Mode

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



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

Chapter 15

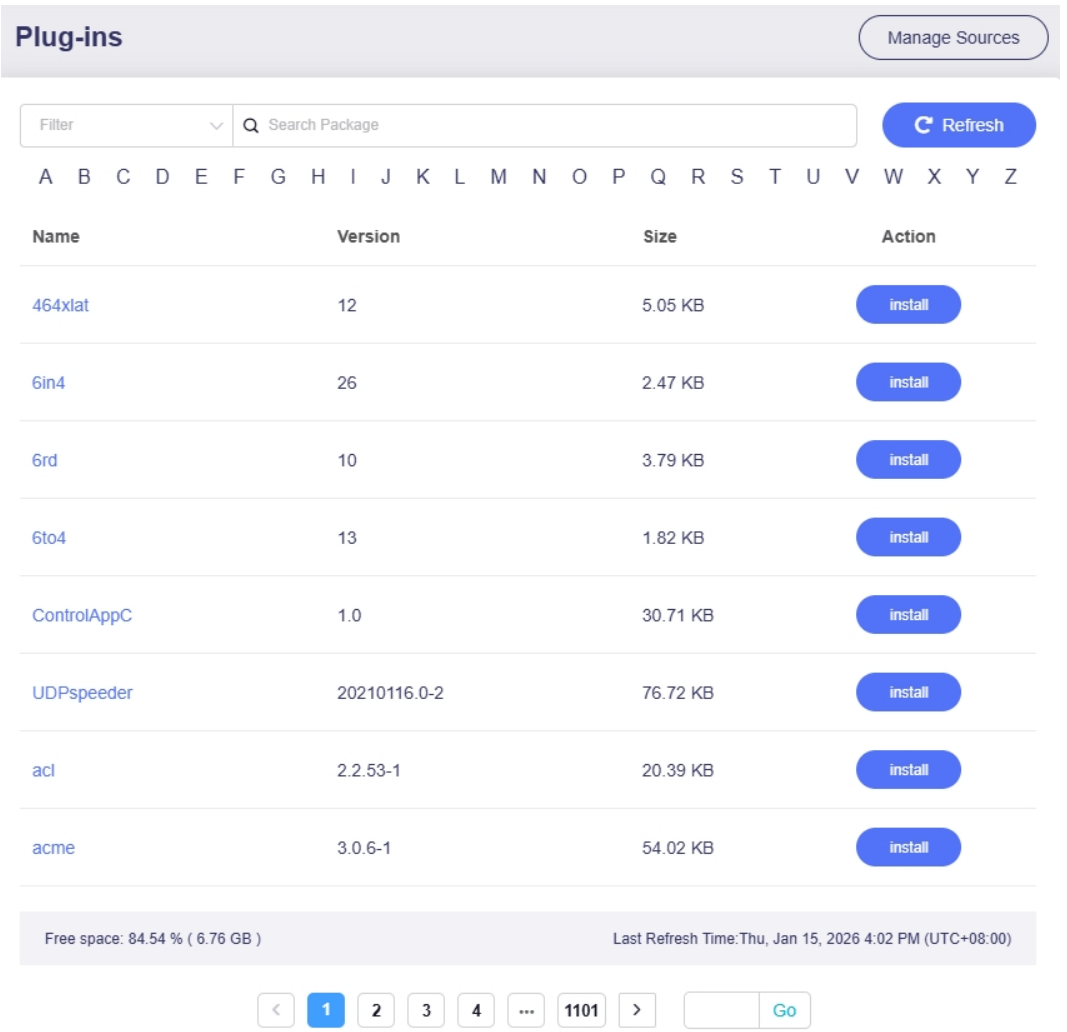
Applications

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

15.1 Plug-ins

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

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



Note:

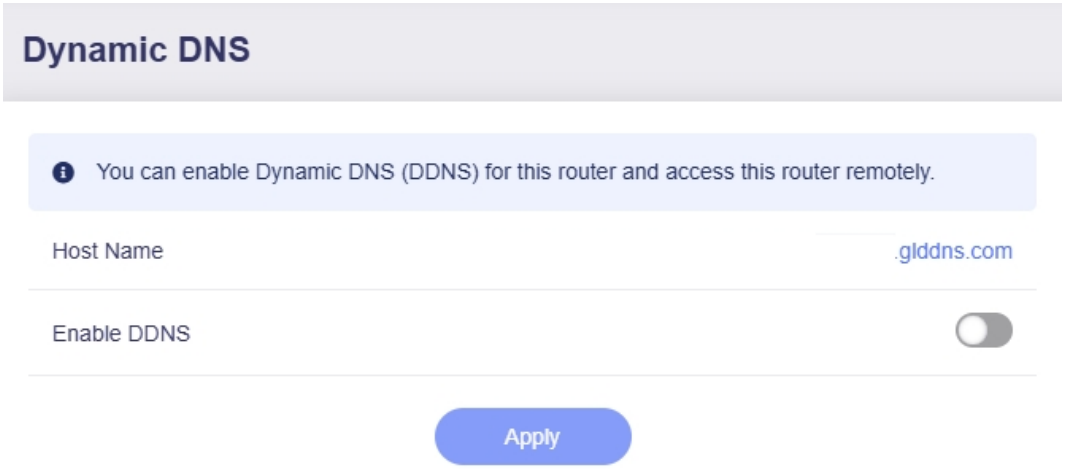
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

15.2 Dynamic DNS

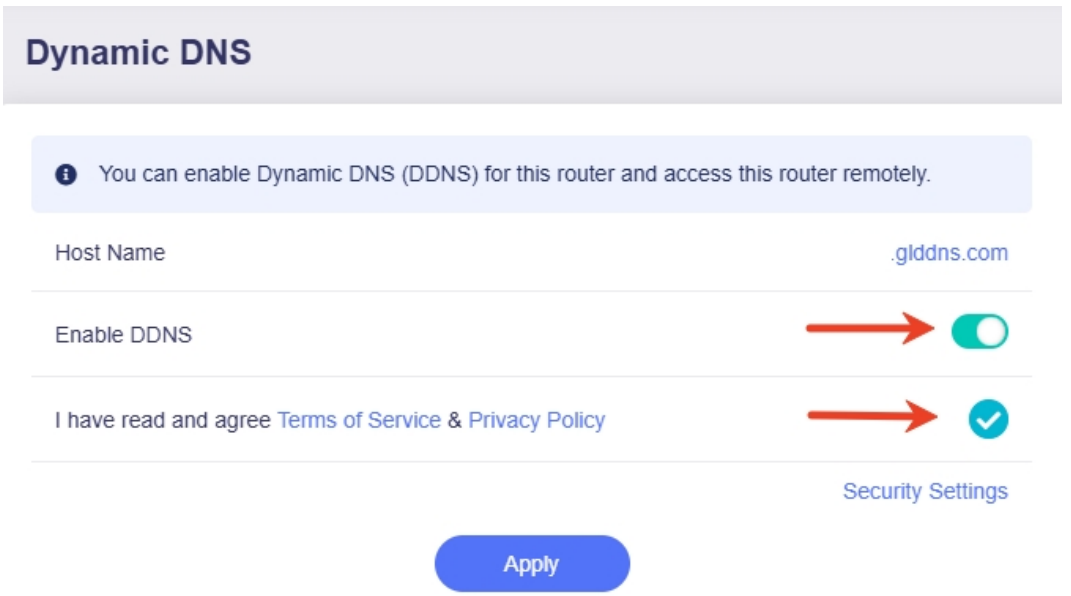
Dynamic Domain Name Service (DDNS, or Dynamic DNS) is a service used to map a domain name to the dynamic IP address of a network device. With Dynamic DNS, you can access your router remotely. A public IP address is required for this functionality.

15.2.1 Enable DDNS

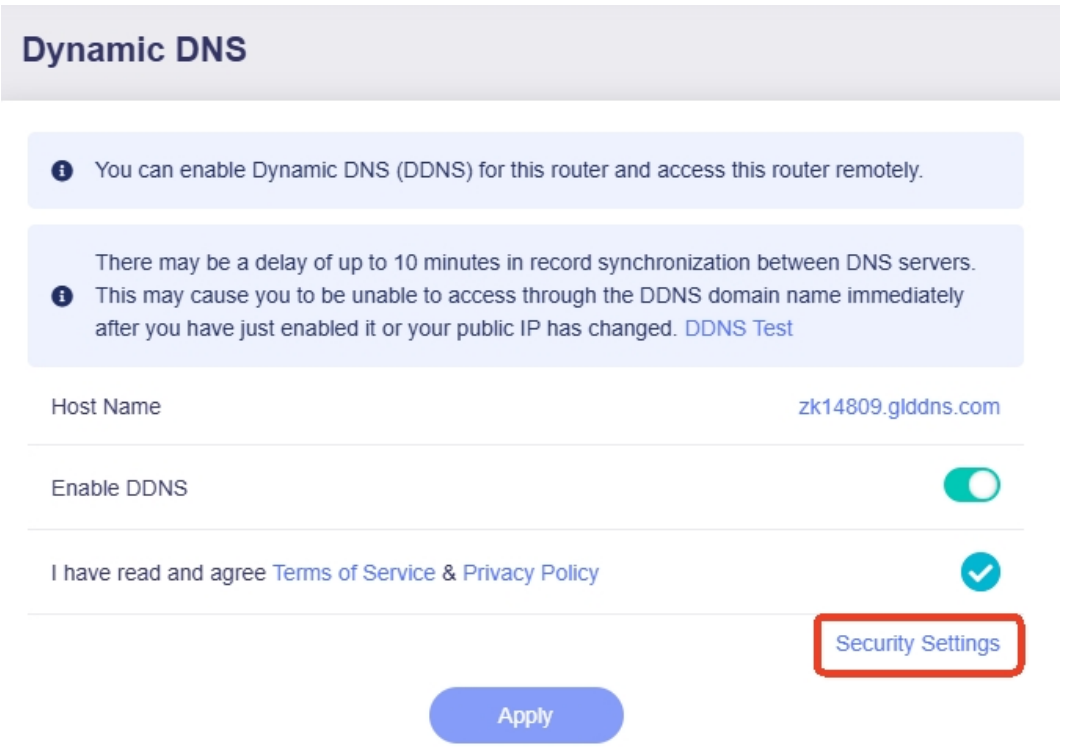
1. Log in to your router's web admin panel, navigate to **APPLICATIONS** > **Dynamic DNS**, the page is displayed as below.



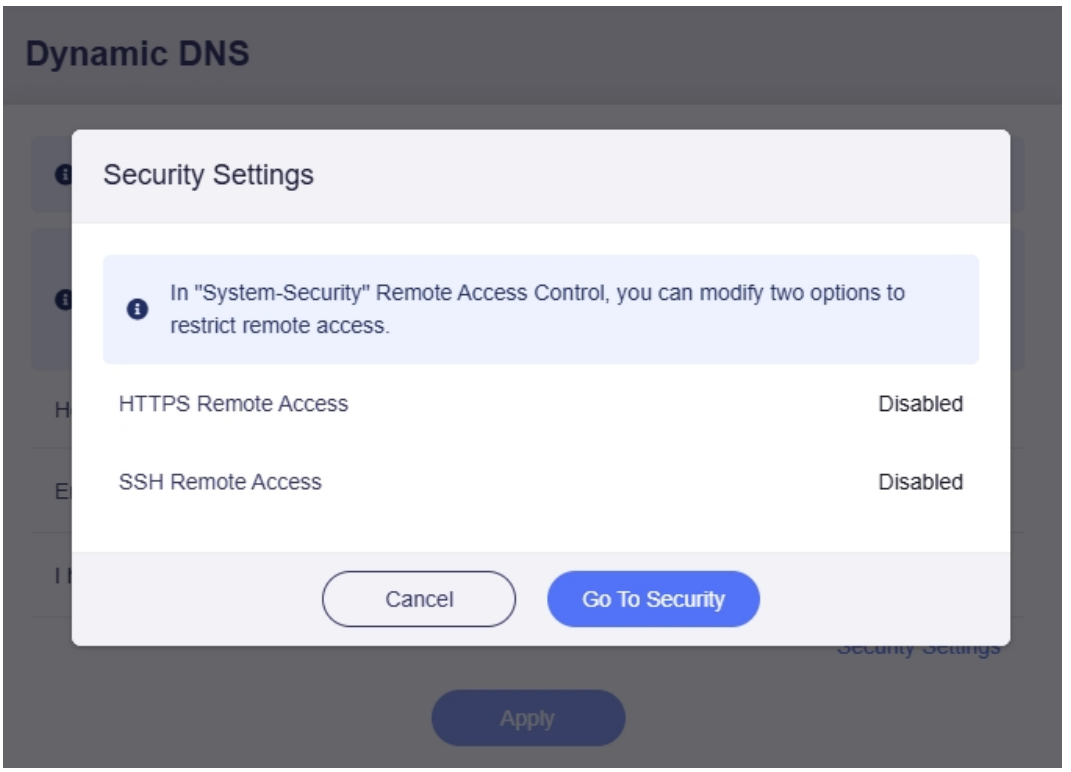
2. Toggle on **Enable DDNS**, read and agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



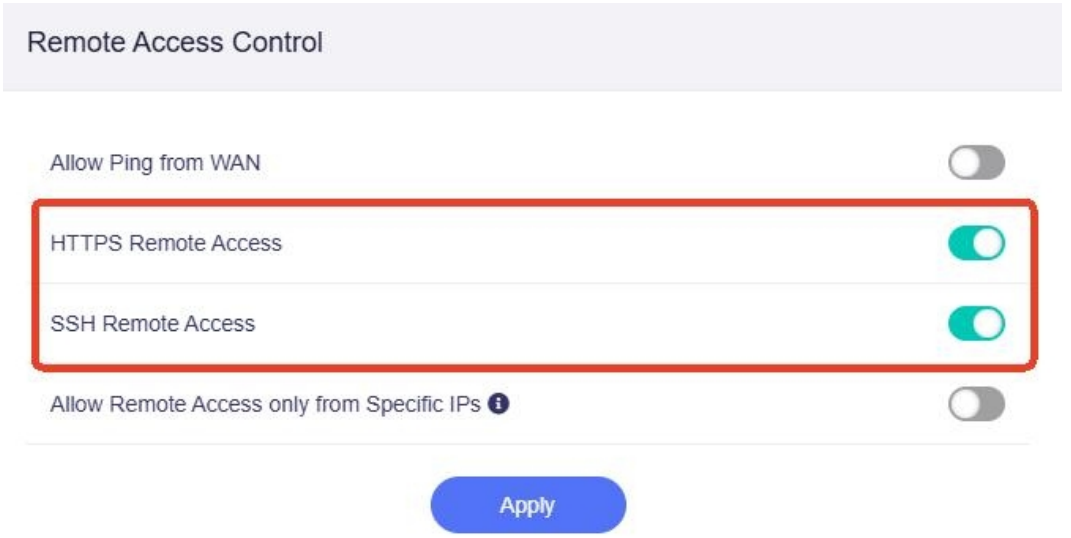
3. Click **Security Settings** in the bottom right corner.



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



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



Note:

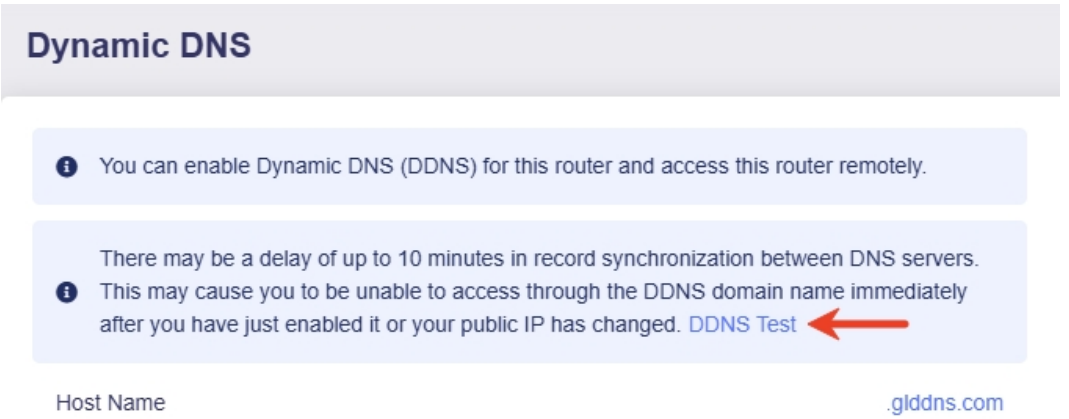
1. There may be a delay of up to 10 minutes in record synchronization between DNS servers. This may prevent you from accessing through the DDNS domain name immediately after enabling it or when your public IP changes.
2. If you enable DDNS and VPN Client at the same time, ensure that Services From GL.iNet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

15.2.2 Check if DDNS Works

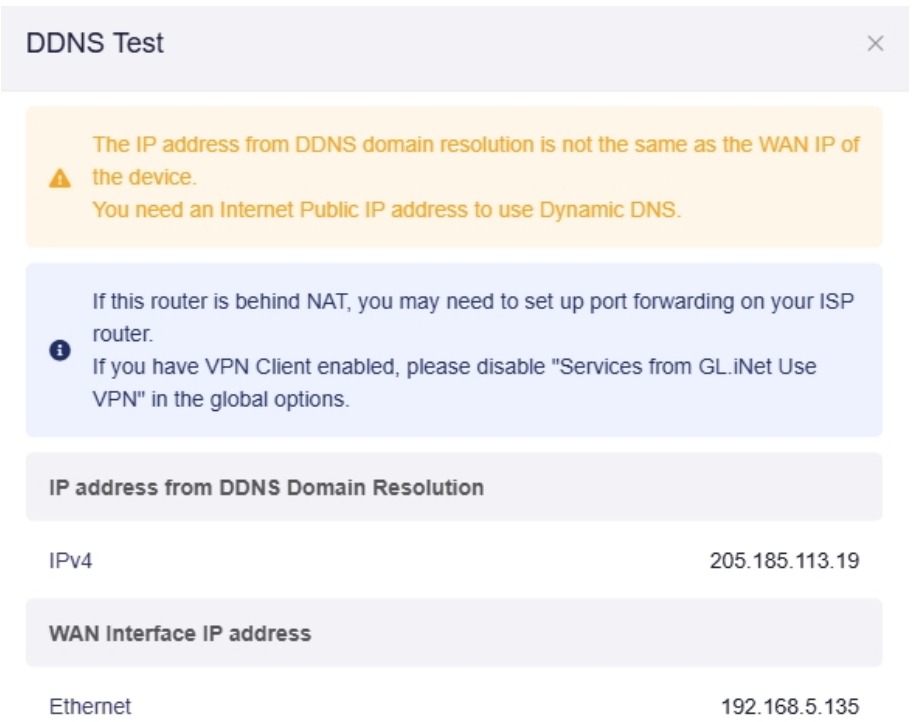
You can check if DDNS works using the DDNS test tool or manually via commands.

Method 1. Use DDNS Test tool

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

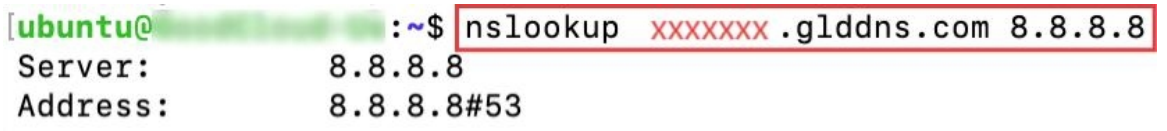


2. Make sure the IP address from DDNS domain resolution matches the router's WAN IP. If not, a yellow prompt will appear at the top, indicating that the router might be behind NAT, and you need to set up port forwarding on the upstream router.



Method 2. Use commands

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



   - Replace “xxxxxxx.glddns.com” in the image above with your Host Name.
   - The “8.8.8.8” is the Google DNS. You can use it or replace it with other DNS, then press Enter.

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

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

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

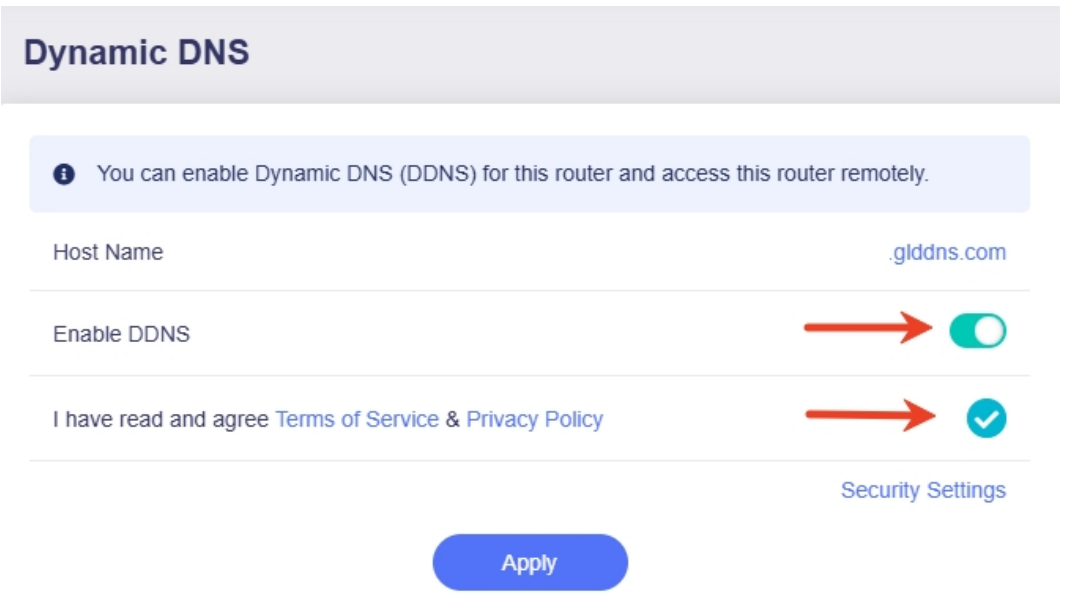
15.2.3 HTTPS Remote Access

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

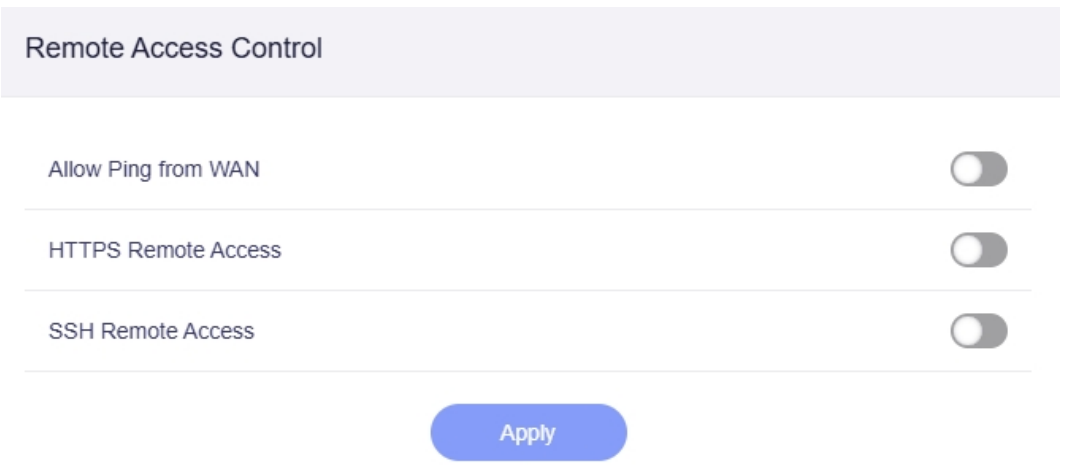
If your router is behind NAT, configure port forwarding (**port 443**) on the upstream router for HTTPS access.

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

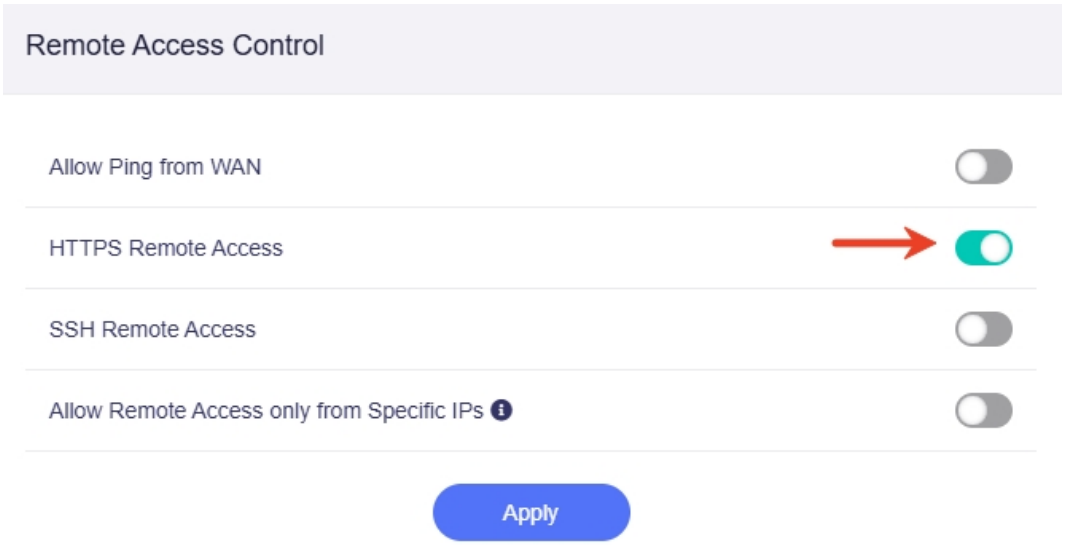
1. On the Dynamic DNS page, toggle on **Enable DDNS**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



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

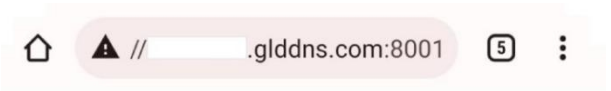


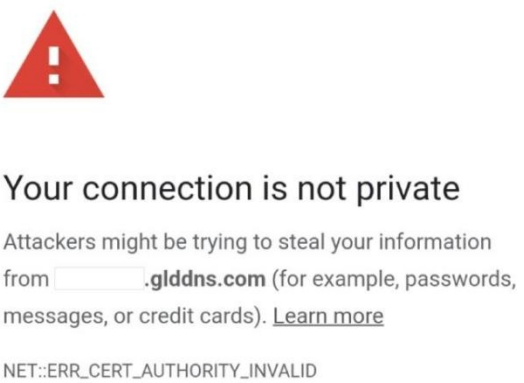
3. Enable **HTTPS Remote Access**, and click **Apply**.



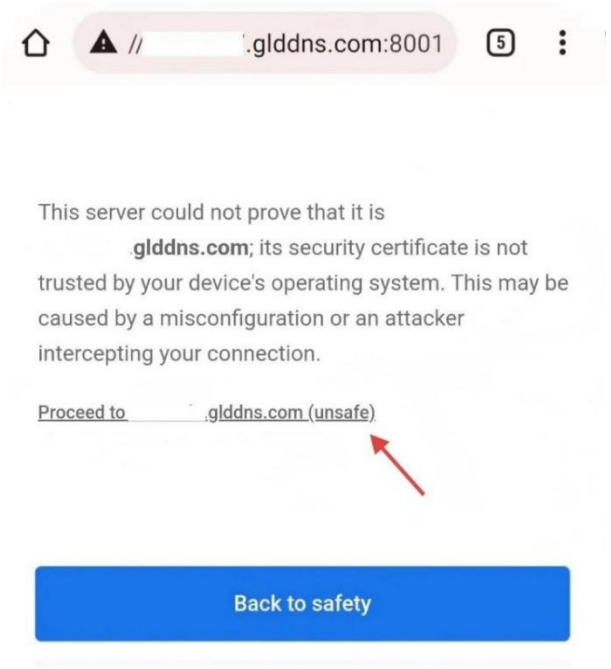
Once enabled, you can access the router's admin panel from anywhere using the DDNS host name over HTTPS, e.g., **https://xxxxxxx.glddns.com**. If port forwarding is configured, access it as **https://xxxxxxx.glddns.com:external_port** (replace the external_port with your actual port number).

Note: This function uses self-signed certificates; therefore, browsers will indicate "Your connection is not private" when accessing the router's admin panel via the DDNS host name over HTTPS, as shown below (port 8001 is used as an example).





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



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

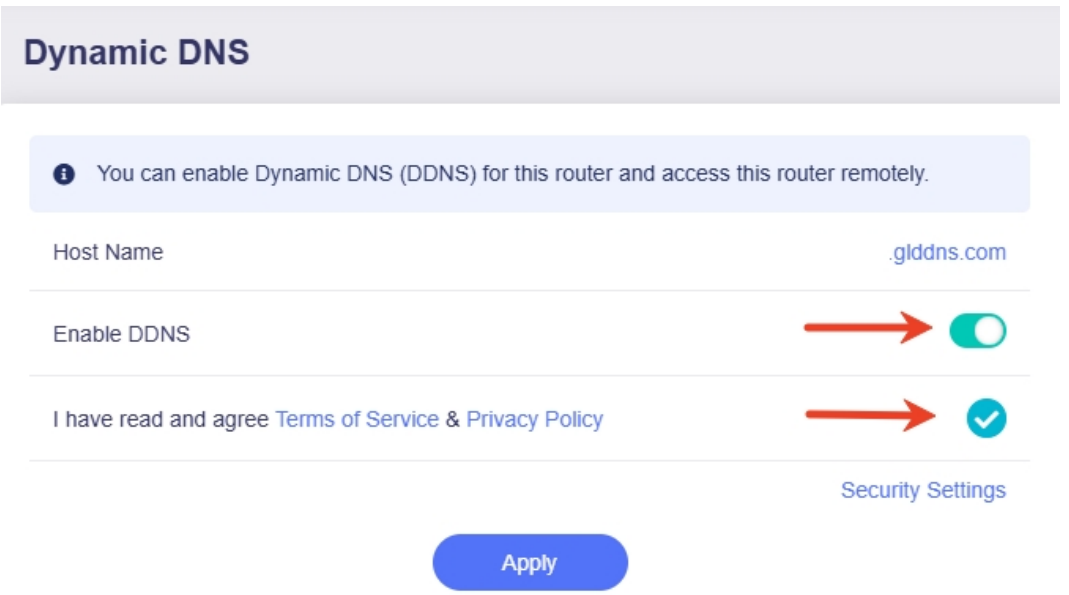
15.2.4 SSH Remote Access

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

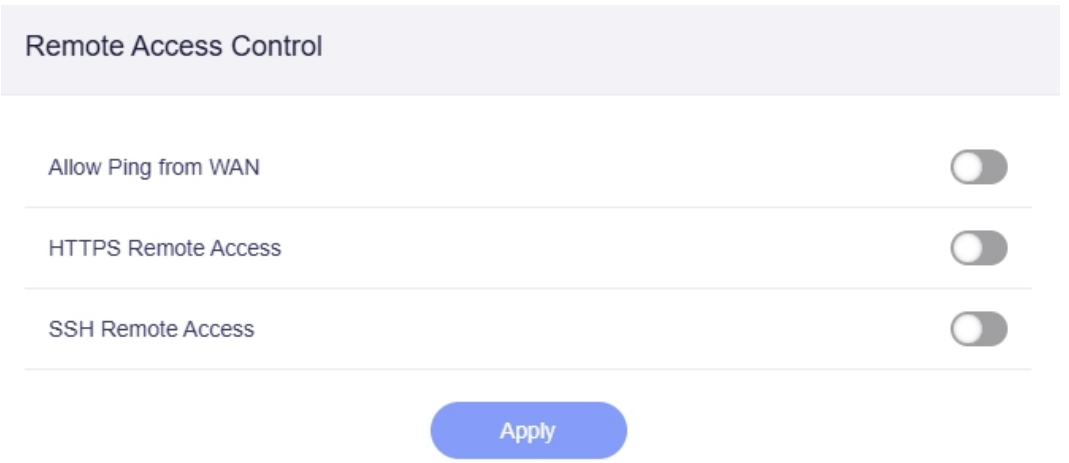
If your router is behind NAT, configure port forwarding (**port 22**) on the upstream router for SSH remote access.

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

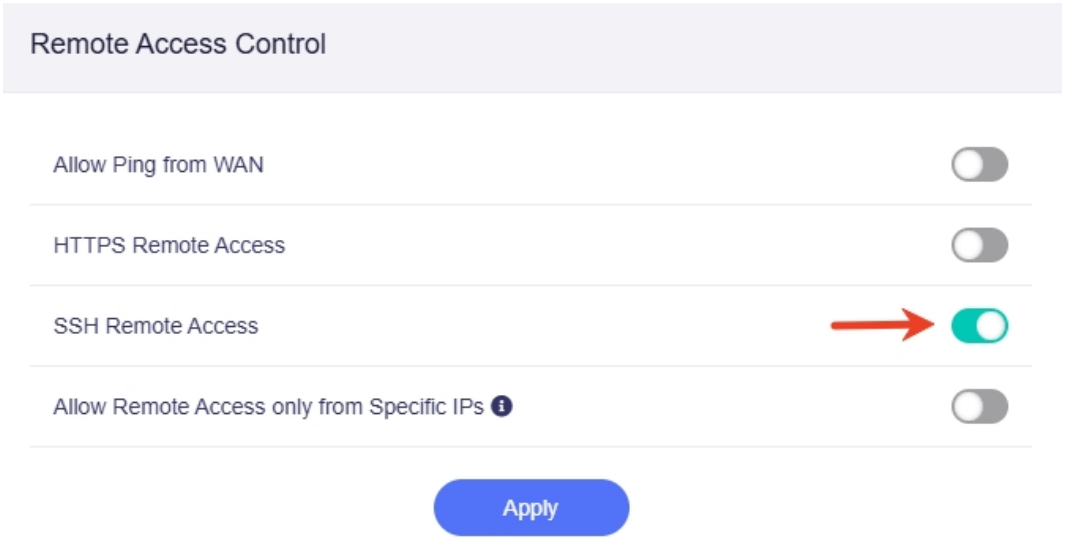
1. On the Dynamic DNS page, toggle on **Enable DDNS**, agree to the **Terms of Services & Privacy Policy**, then click **Apply**.



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



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



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

15.3 Network Storage

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

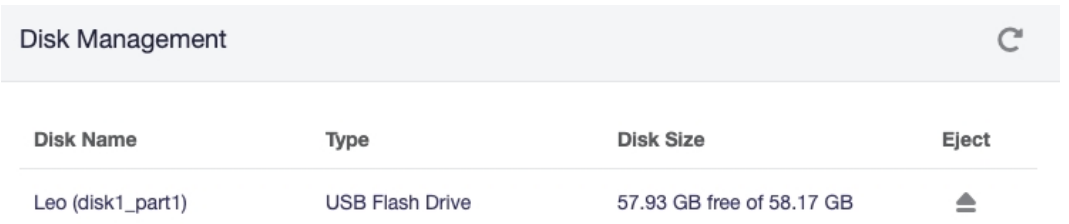
Among GL.iNet models, some support MicroSD (TF) cards, while others feature a USB port, compatible with USB flash drives and portable external hard drives. You can configure Samba, WebDAV, or DLNA for these storage devices, which support common formats such as NTFS, FAT32, and EXT4.

Note:

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

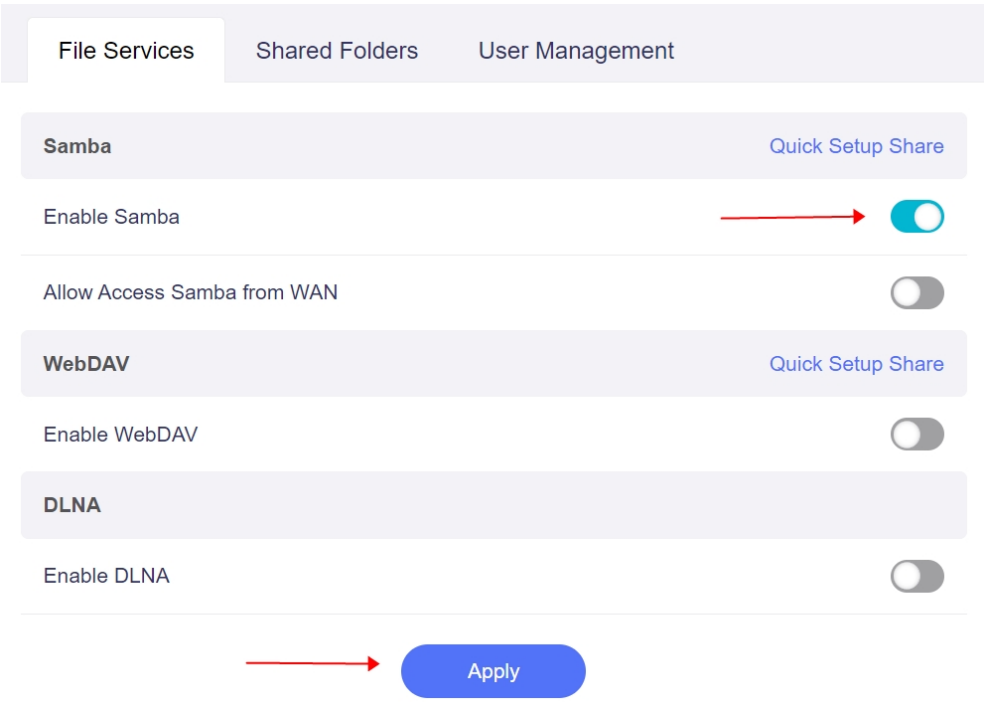
15.3.1 Connect Storage

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



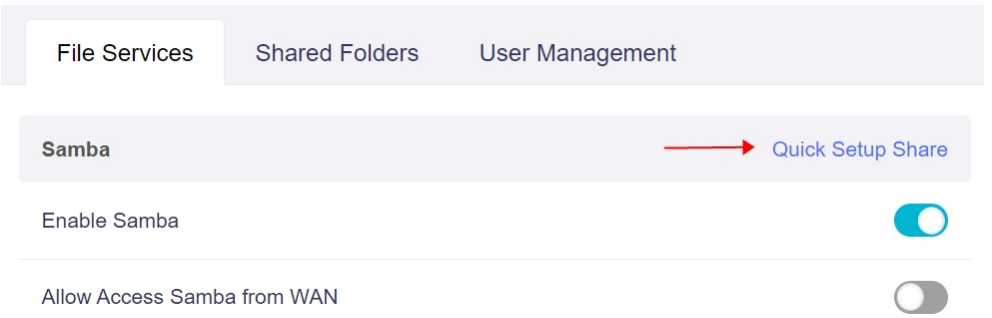
15.3.2 Set Up Samba

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

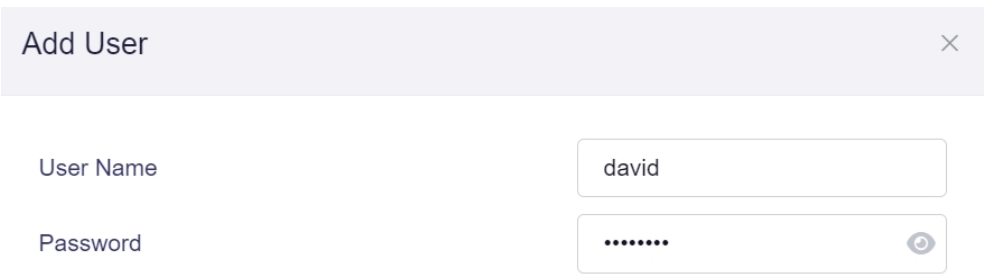


   - **Allow Access Samba from WAN**: Enable it if you want upstream devices to access the Samba service.

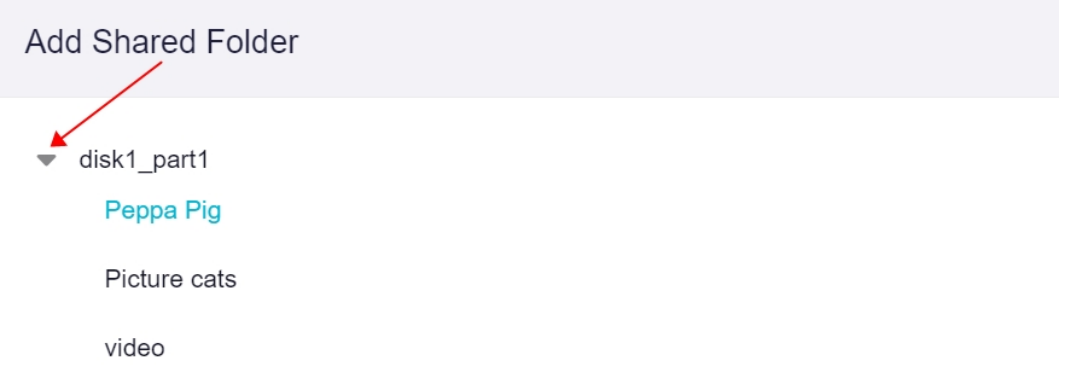
2. Click **Quick Setup Share** to set the shared link.



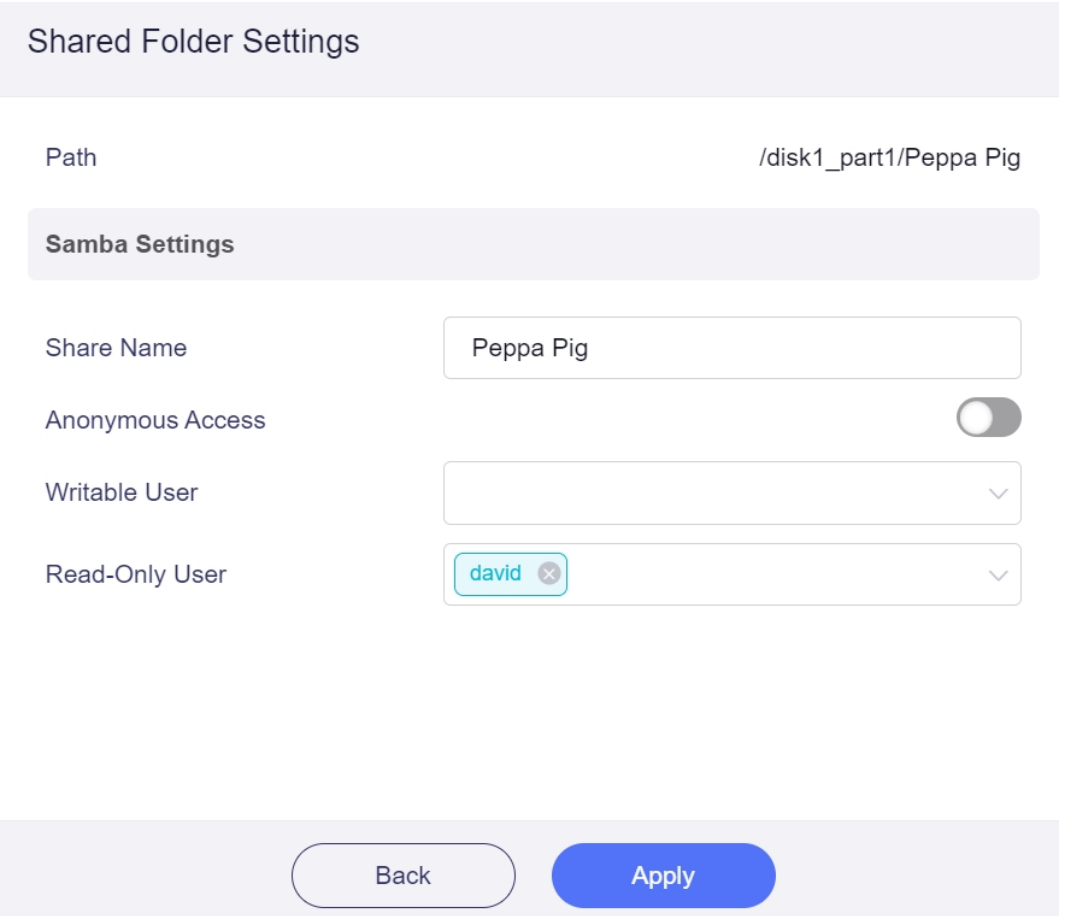
3. Add a user and click **Next**. This step will be skipped if you already have an account.



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

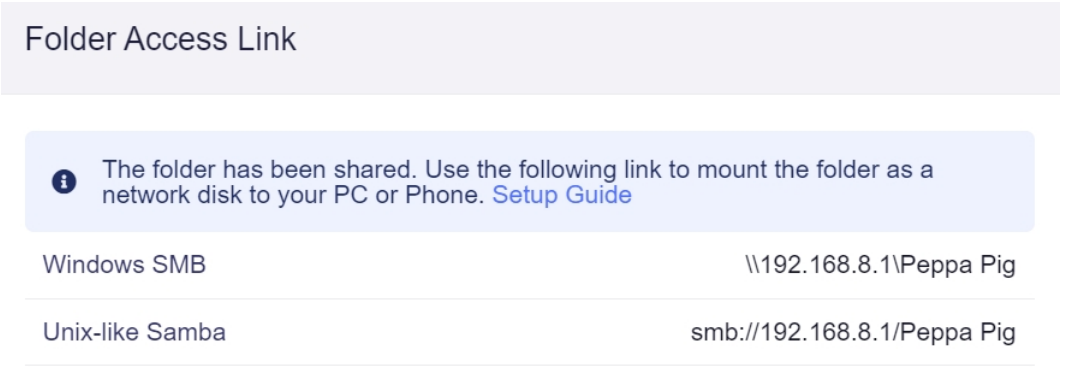


5. Set up the shared folder.
   For security reasons, it is not recommend to enable Anonymous Access.
   The user created in the previous step will be added to **Read-Only User** by default. If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Writable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



6. Obtain the folder access link.

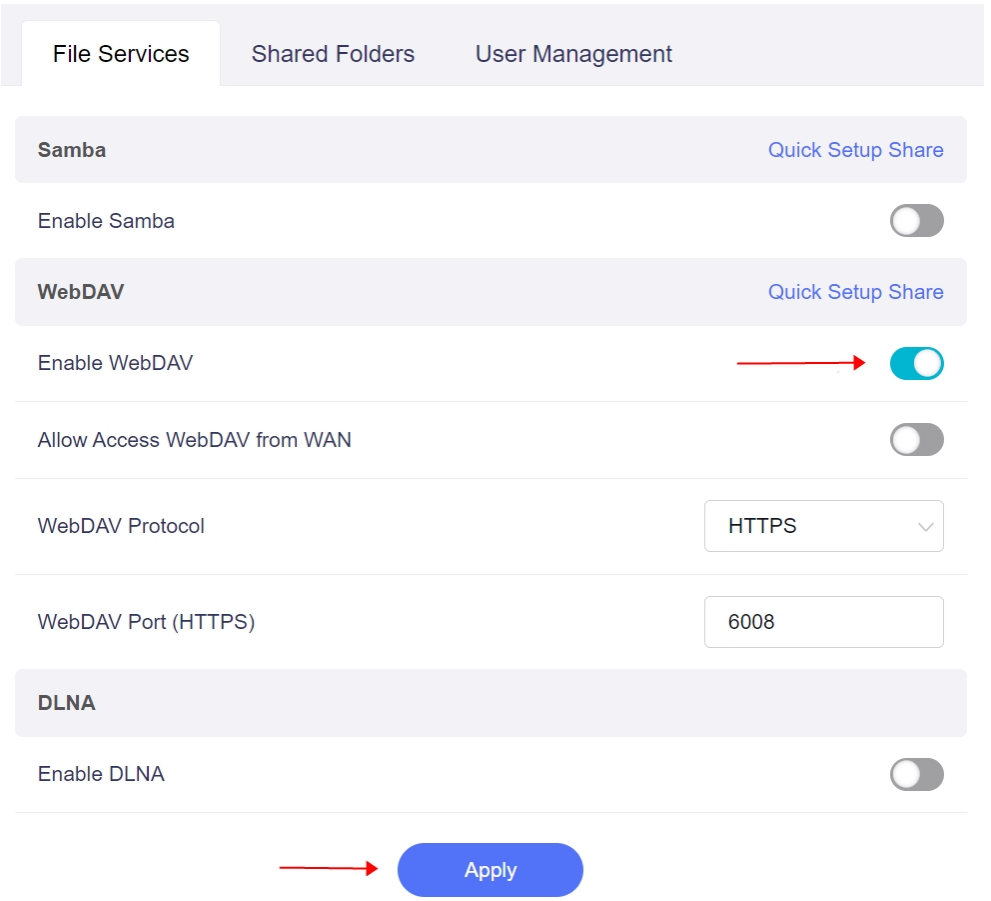
   The page will display the links for Windows and Unix-like OS. The Unix-like system includes Android, iOS, macOS, Ubuntu, etc. Now you can access your shared folder over Samba service via these links.



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

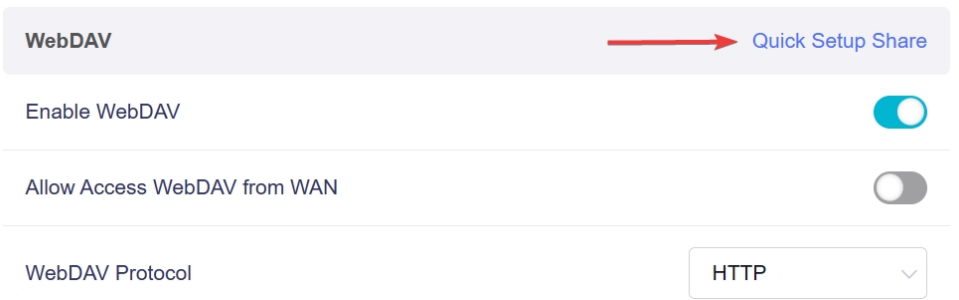
15.3.3 Set Up WebDAV

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

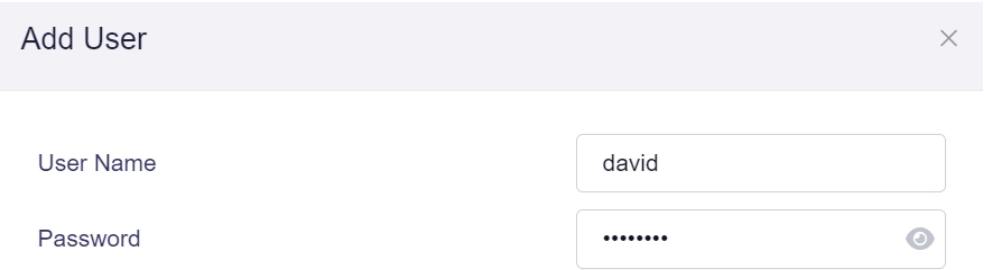


- **Allow Access WebDAV from WAN**: Enable it if you want the upstream devices to access the WebDAV service.
- **WebDAV Protocol**: HTTP is unencrypted; use it at your own risk. HTTPS is encrypted and it uses self-signed certificate.
- **WebDAV Port**: No need to modify the port number unless there's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

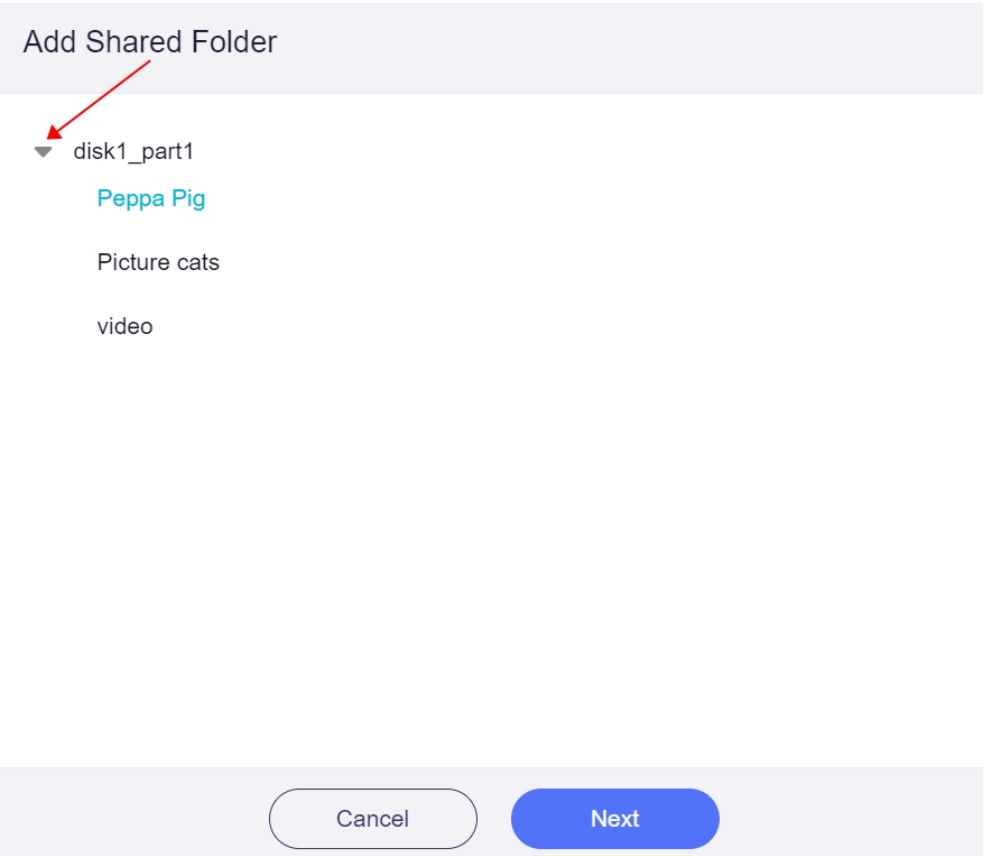
2. Click **Quick Setup Share** to set the shared link.



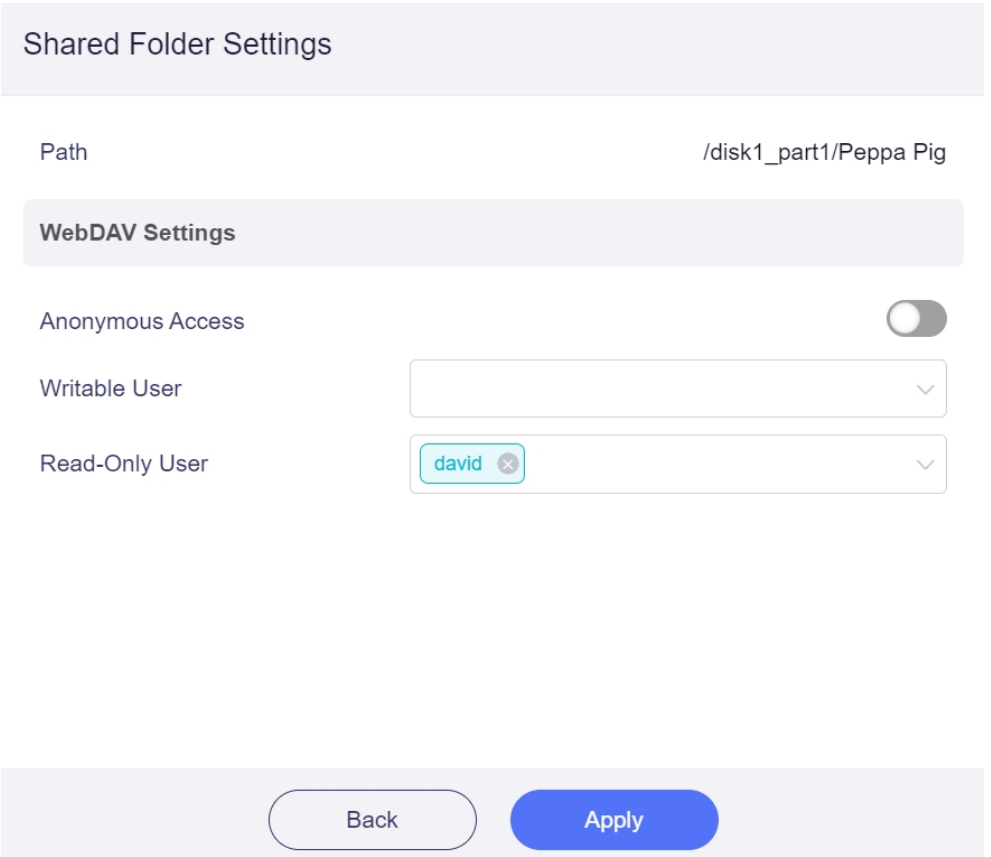
3. Add a user and click **Next**. This step will be skipped if you already have an account.



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

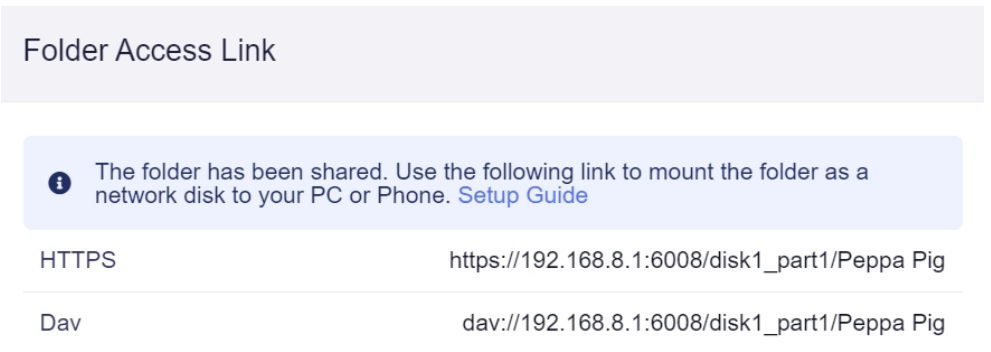


5. Set up the shared folder.
   For security reasons, it is not recommend to enable Anonymous Access.
   The user created in the previous step will be added to **Read-Only User** by default.
   If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Writable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



6. Obtain the folder access link.

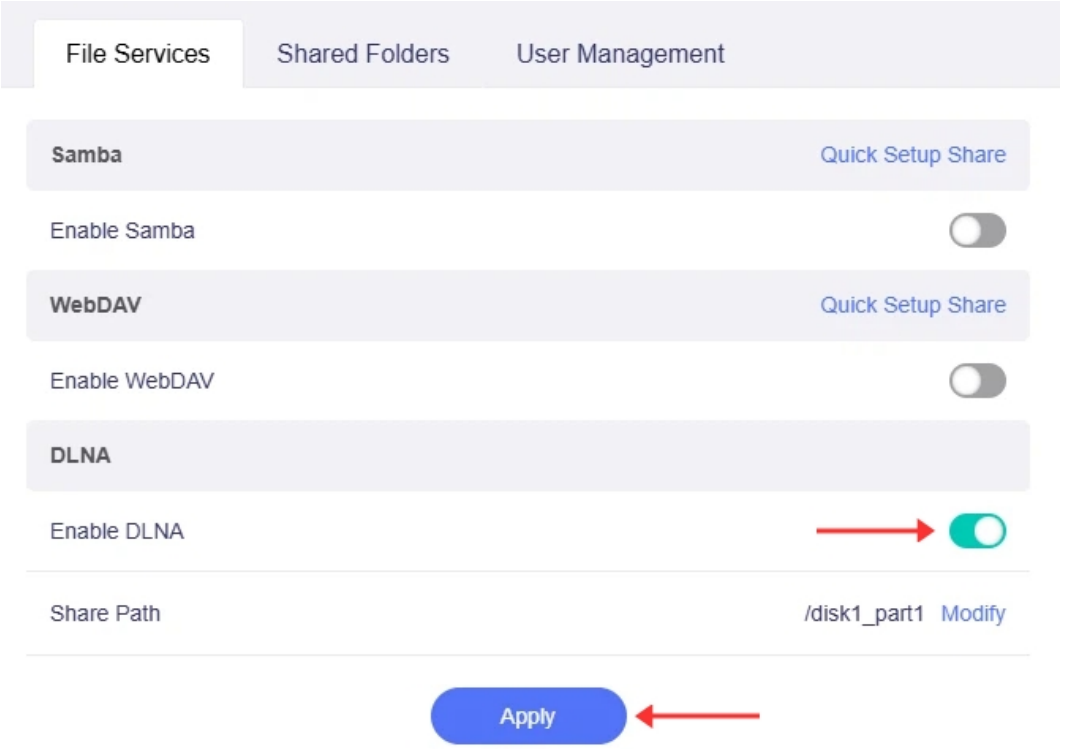
   The page will display the links for Windows and Unix-like OS. The Unix-like systems includes Android, iOS, macOS, Ubuntu, etc. Now you can access your shared folder over WebDAV service via these links.



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

15.3.4 Set Up DLNA

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



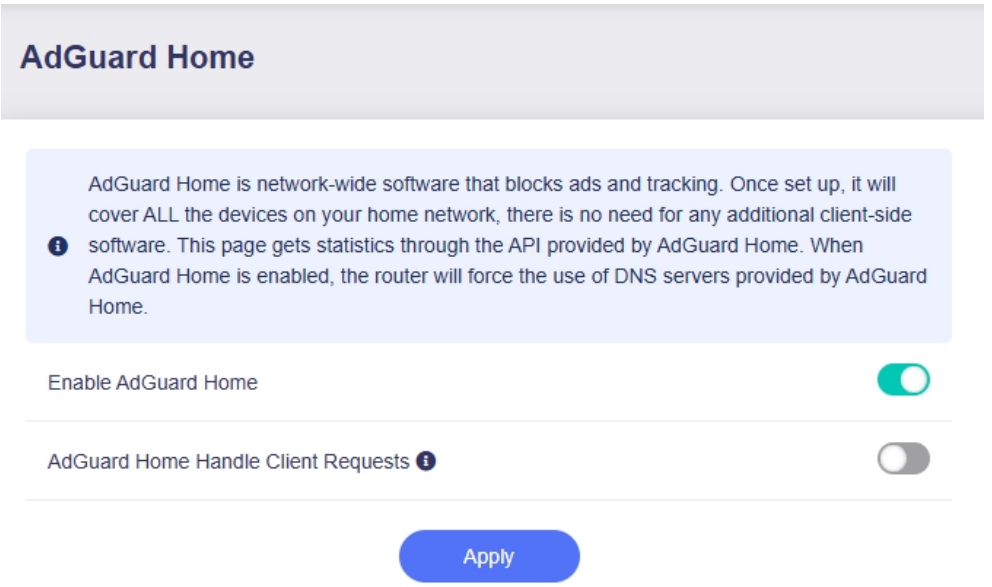
2. Connect your smart TV to the router, and it will find the DLNA Server.

15.4 AdGuard Home

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

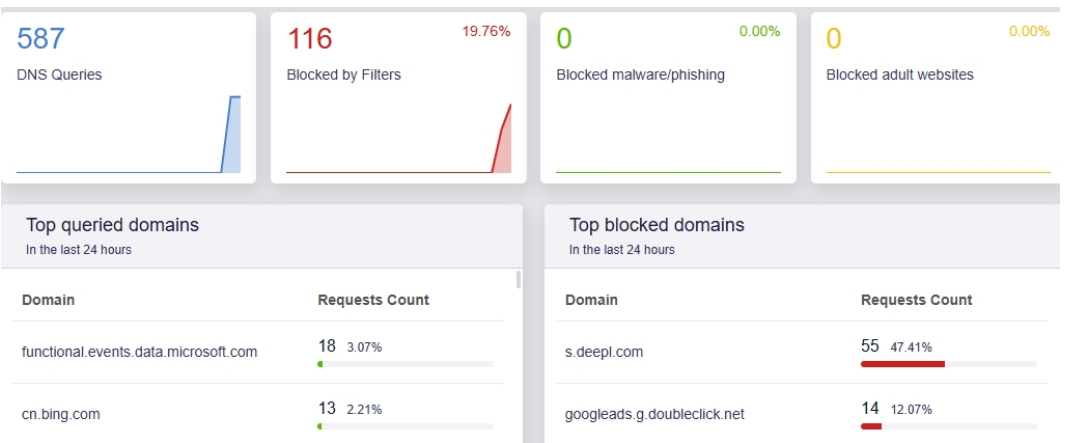
Follow these steps to set up AdGuard Home.

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

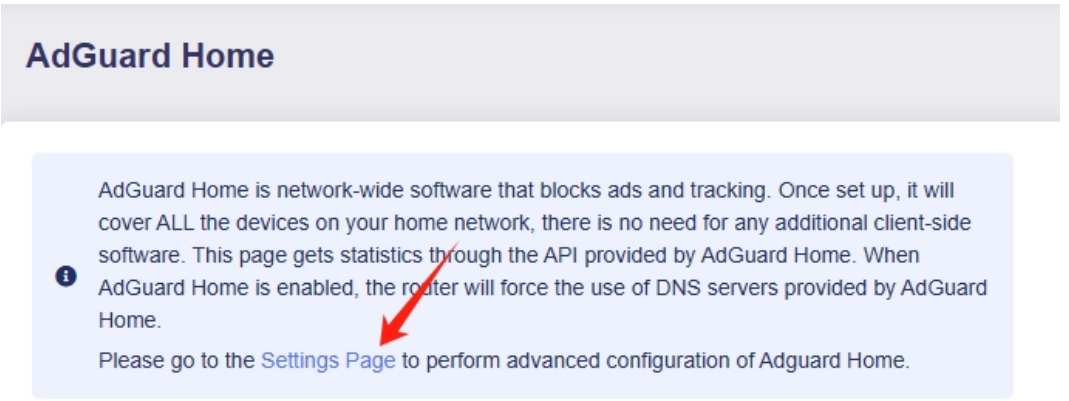


   - **AdGuard Home Handles Client Requests**: If enabled, DNS queries from client devices will be handled directly by AdGuard Home, but this will cause VPN policies based on domains to fail.

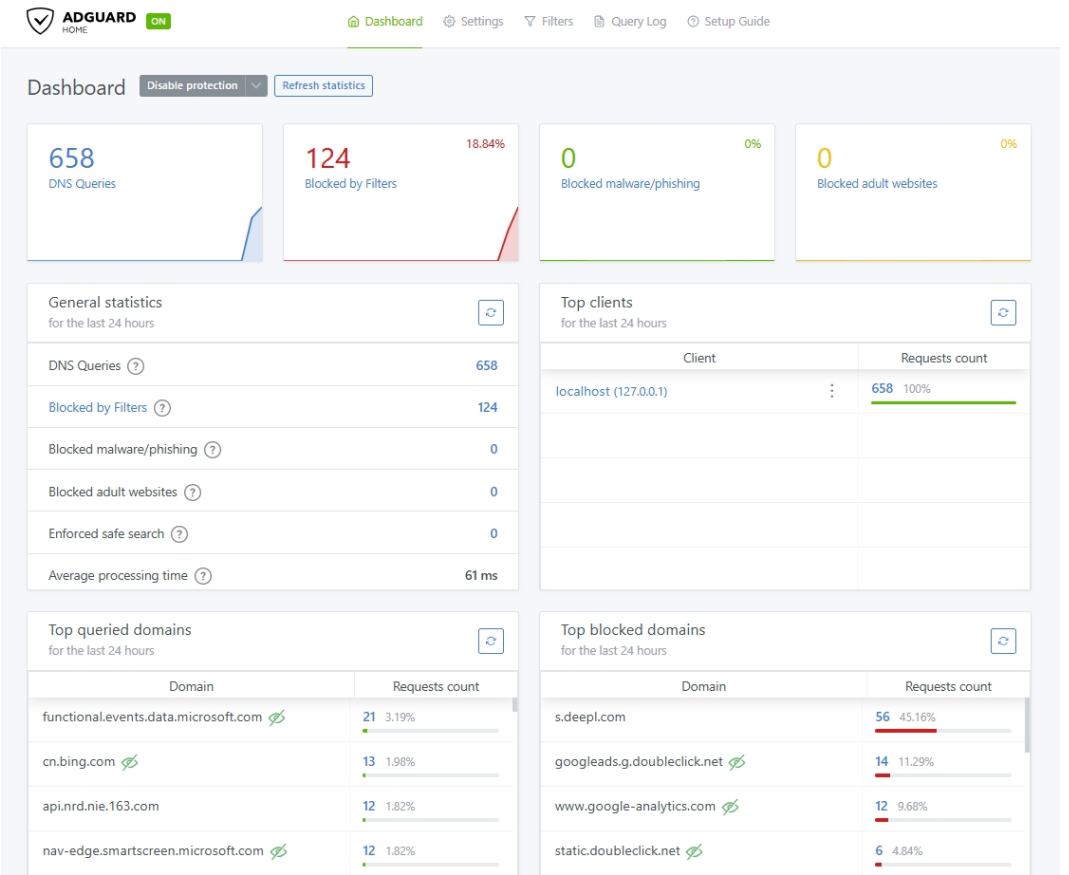
2. The page will automatically load DNS statistics (queries, blocked domains, etc.) via the API provided by AdGuard Home.



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



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



15.5 Tailscale

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

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

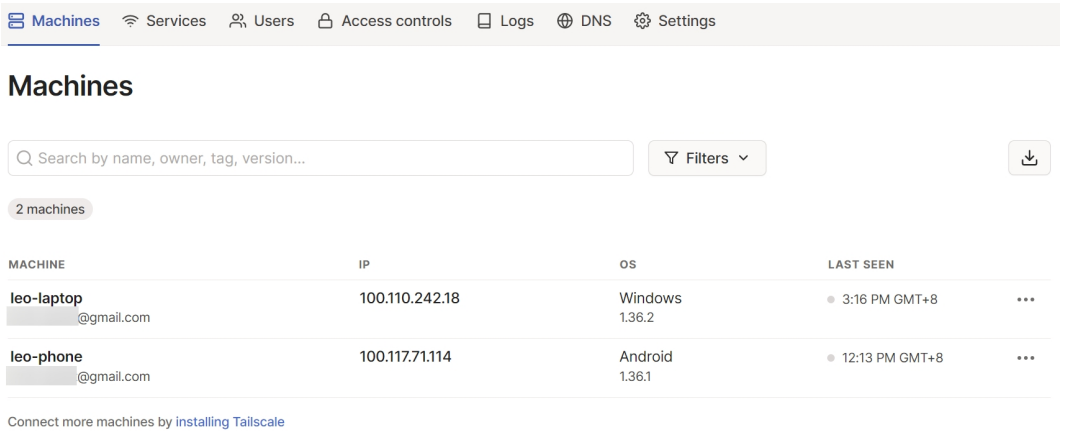
Note:

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

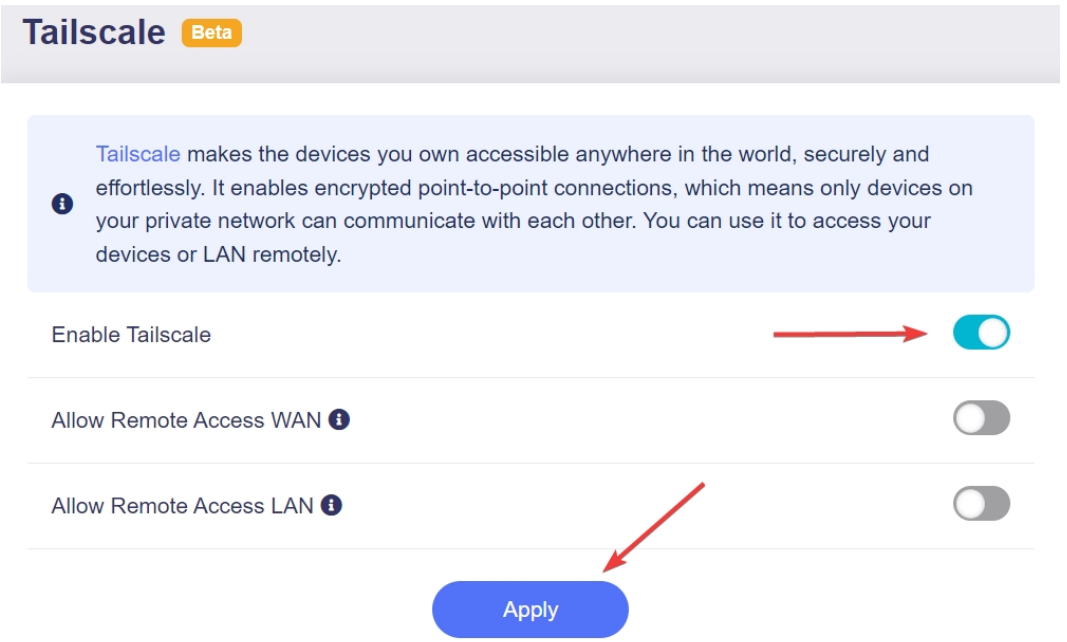
15.5.1 Set Up Tailscale

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

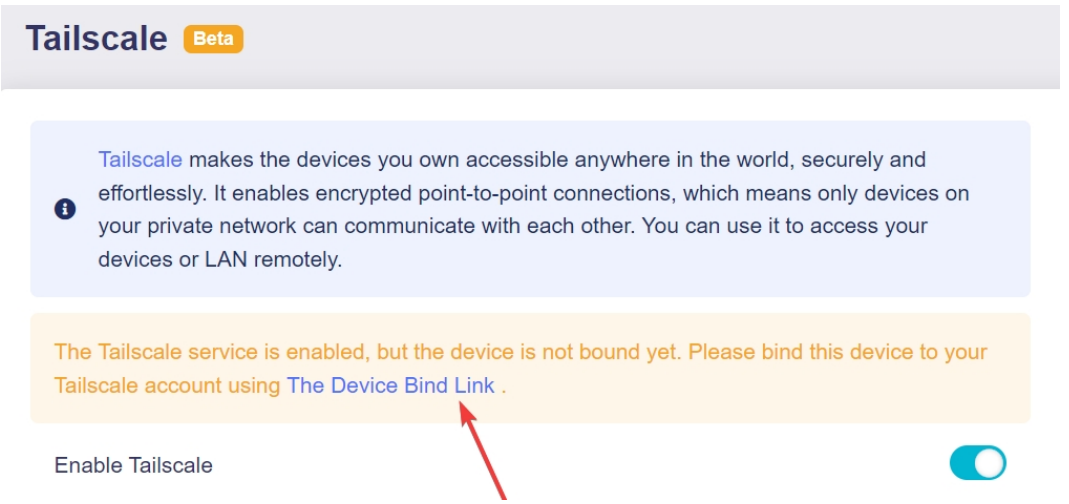
1. Register a Tailscale account first and bind one or two devices to your Tailscale account for testing purposes. After binding, you will see your devices in the Tailscale Console.



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

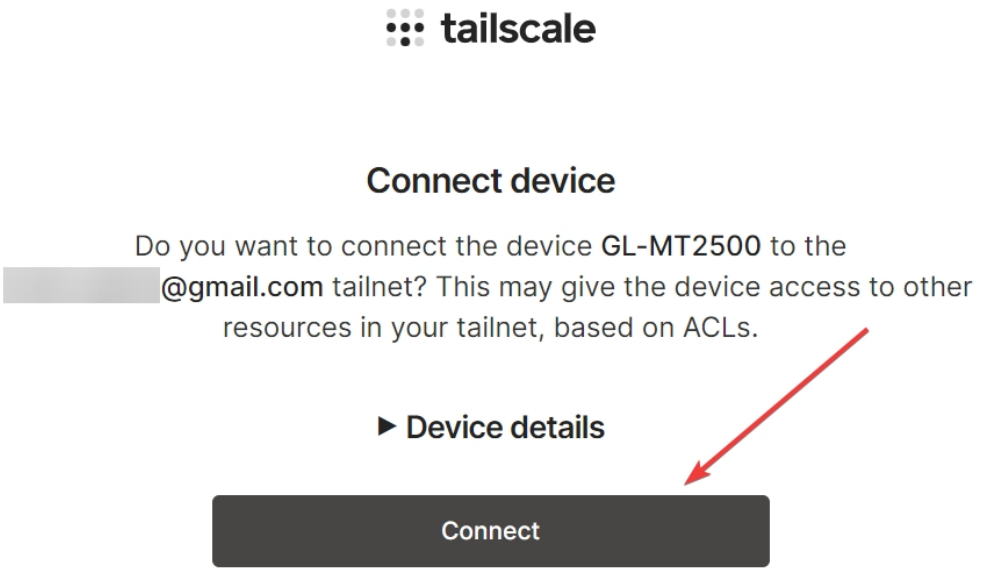


3. The page will prompt you to bind the device. Click **Device Bind Link**.

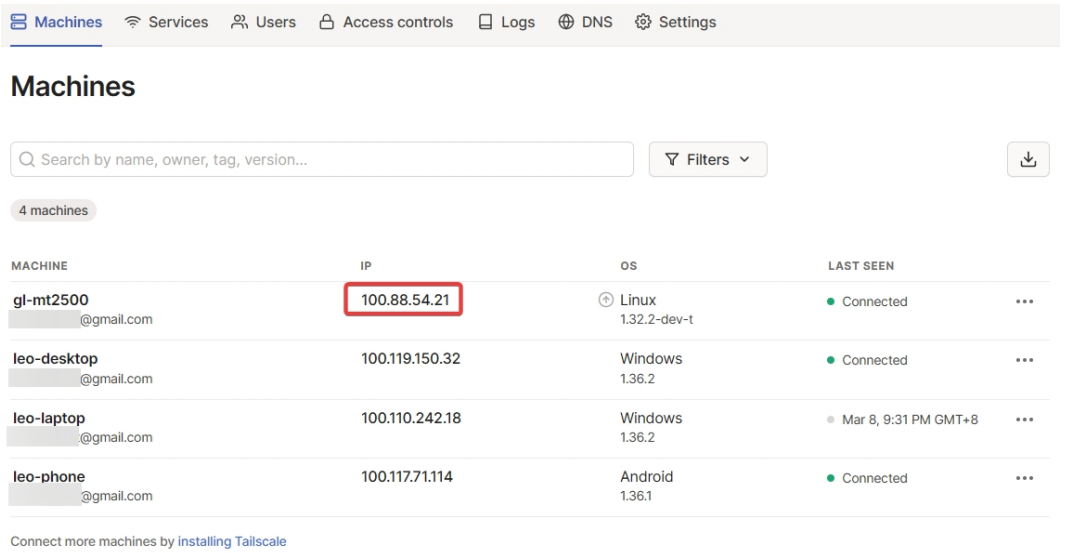


4. In the pop-up window, click the link and log in with your Tailscale account.

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



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

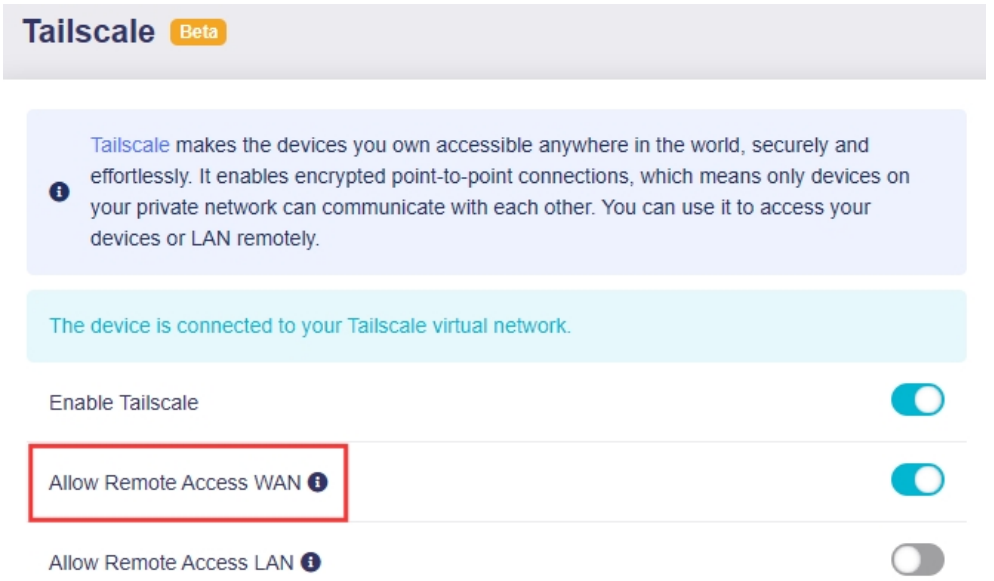


7. Test connectivity.

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

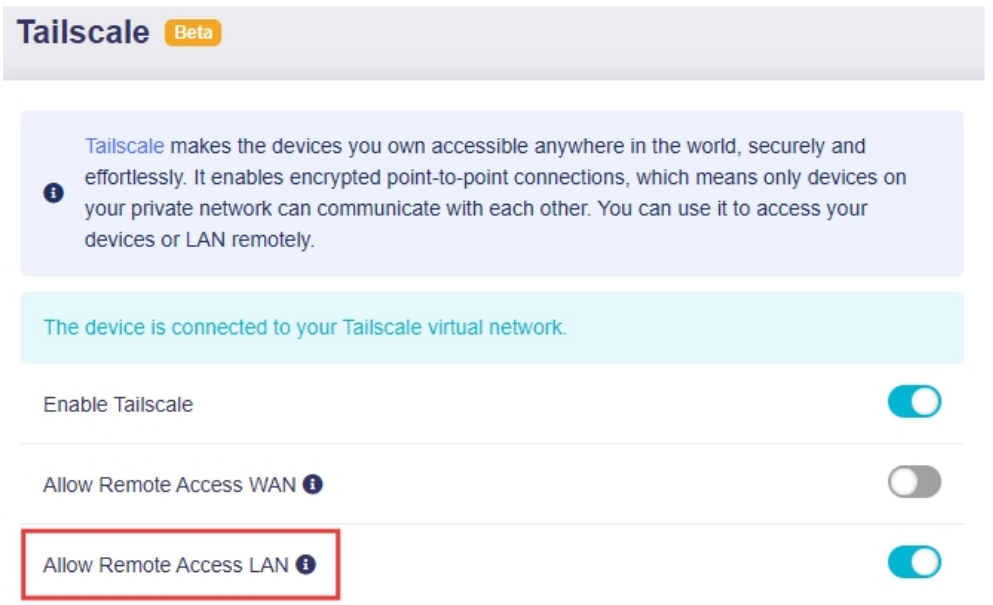
15.5.2 Allow Remote Access WAN

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.



15.5.3 Allow Remote Access LAN

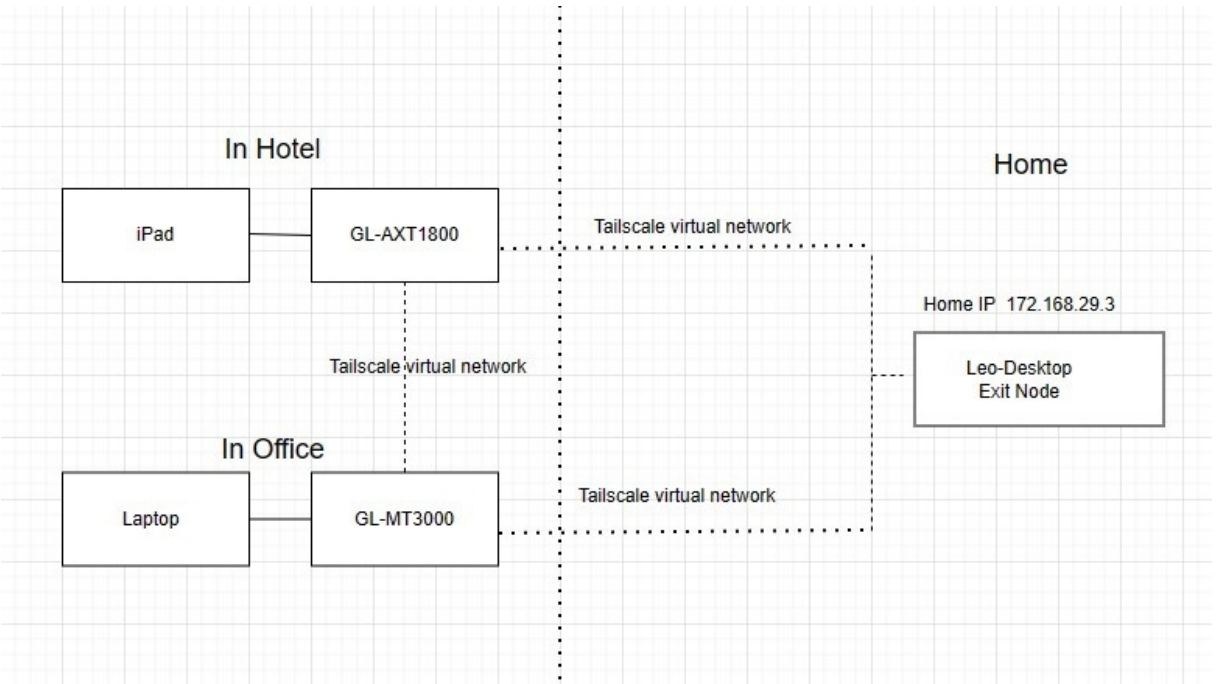
If this option is enabled, resources on the device's LAN side can be accessed through the Tailscale virtual network. See here for more details.



15.5.4 Custom Exit Nodes

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

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



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

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

15.6 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:

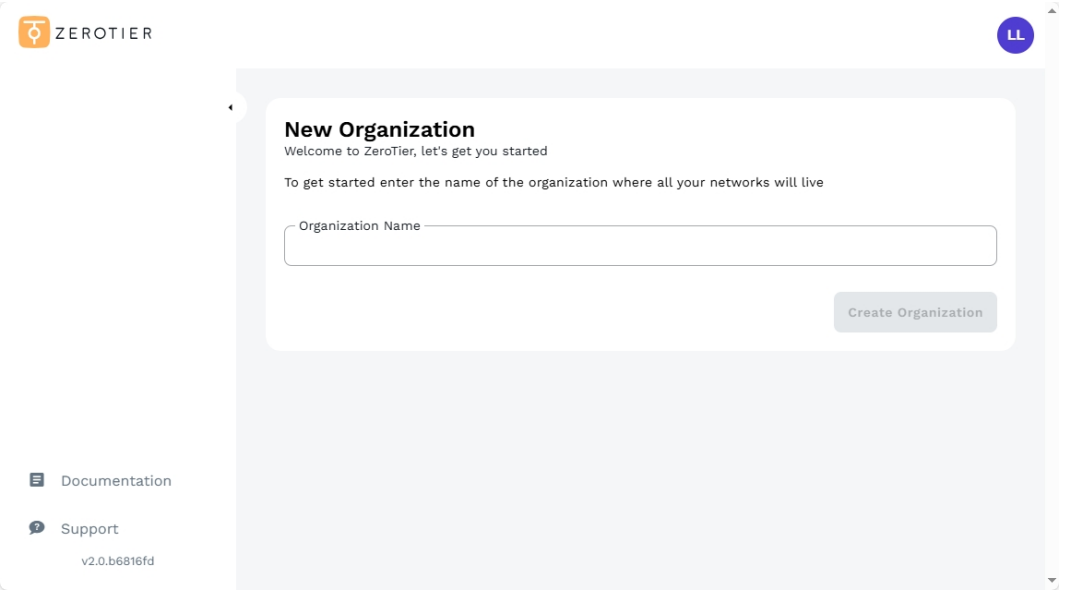
1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale, and AstroWarp.
2. This feature is currently in beta, and may have some bugs.

15.6.1 Set Up ZeroTier

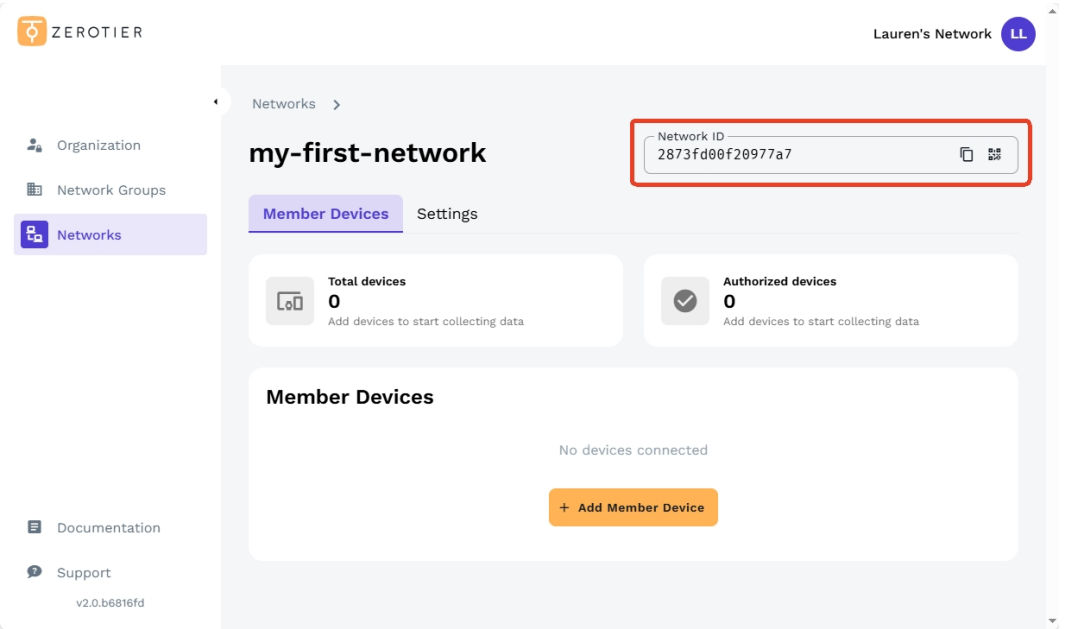
Two versions of ZeroTier Central are available: New Central and Legacy Central.

The following steps use New Central as an example.

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

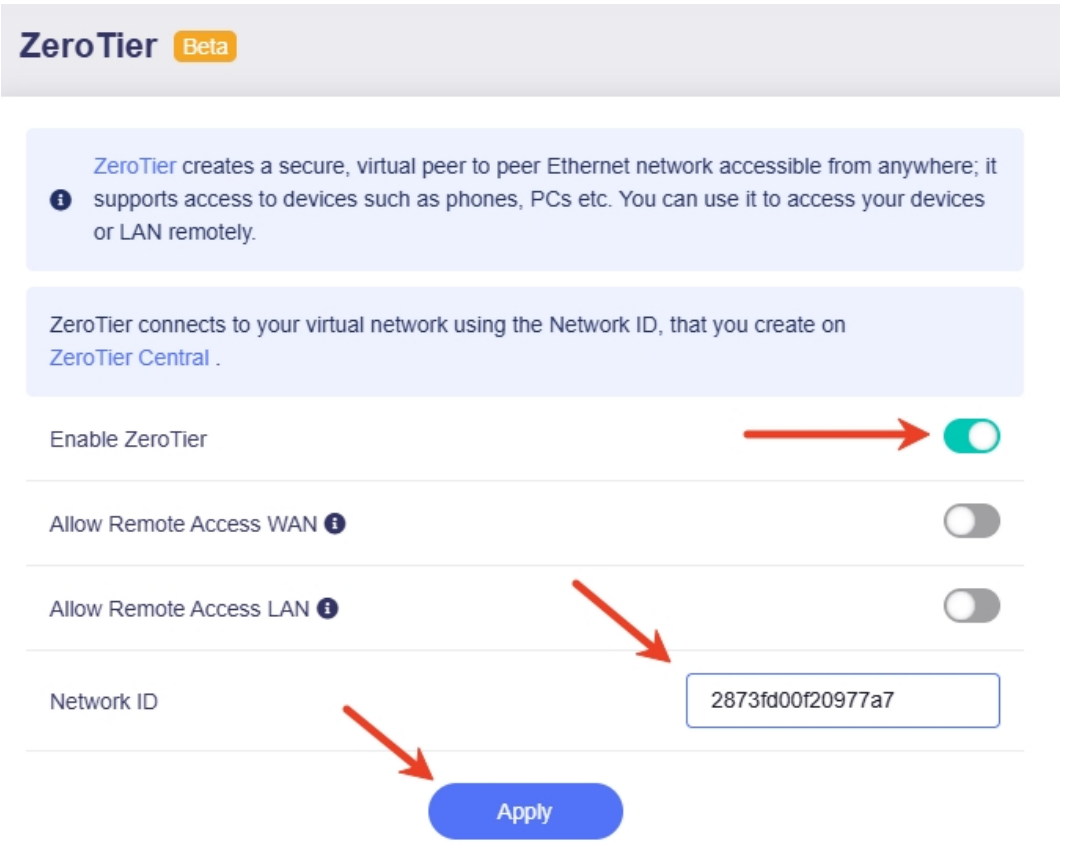


3. Select a plan. Here we choose **Personal plan** as an example, which includes 10 devices, 1 network admin, and 1 network. If you need to create more networks, add more devices, or add custom routes and DNS, choose other paid plan.
4. Now your ZeroTier network has been created.

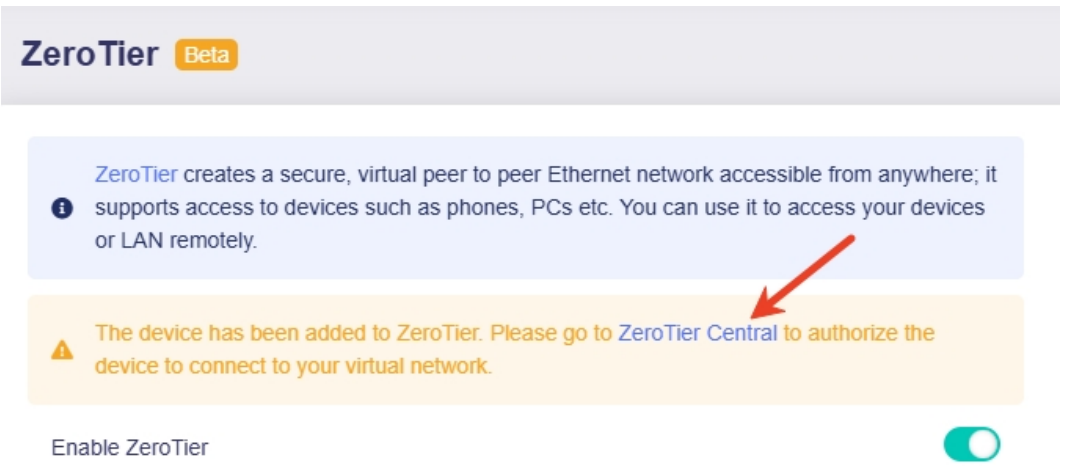


Take note of the **Network ID**, which is a 16-character alphanumeric combination in the upper right corner, as it will be required when connecting other devices later.

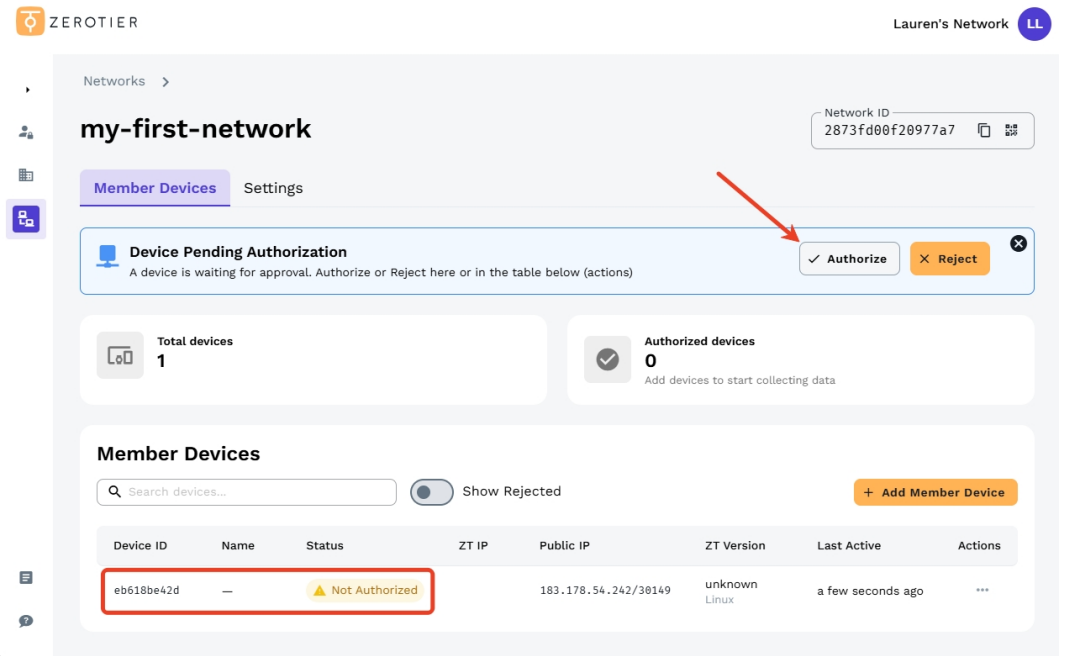
5. Log in to your router's web Admin Panel and navigate to **APPLICATIONS** -> **ZeroTier**. Enable ZeroTier, enter the **Network ID**, then click **Apply**.



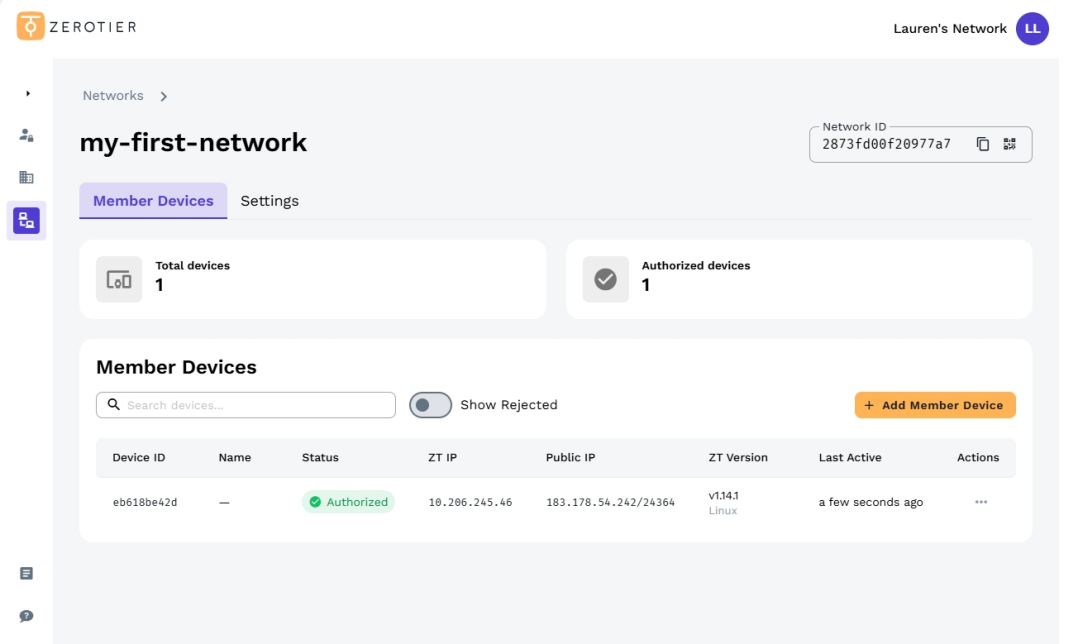
After a short while, the page will indicate that authorization is required. Click the **ZeroTier Central** hyperlink to redirect to the ZeroTier Central.



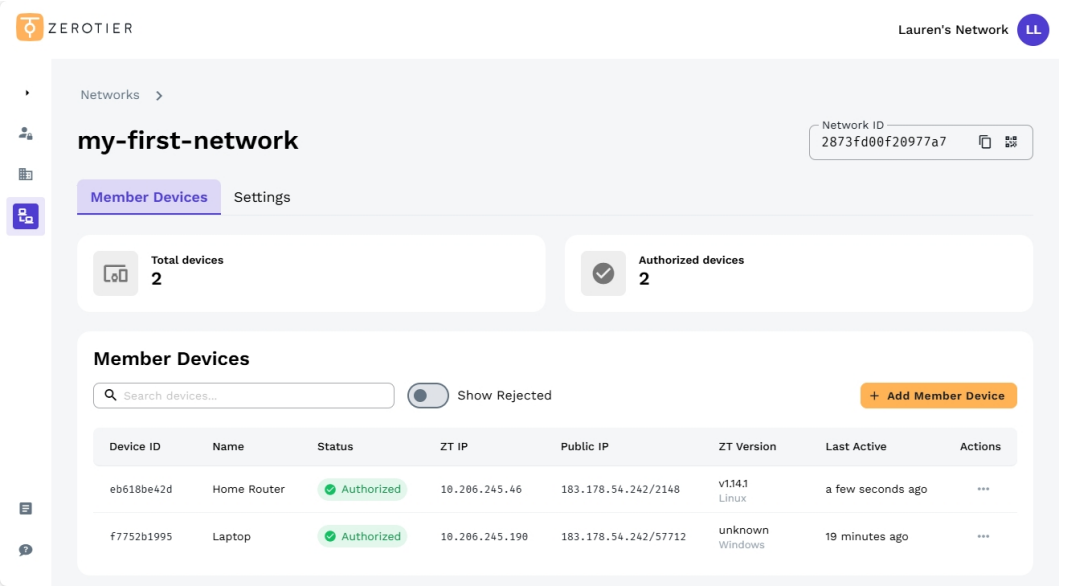
6. On the ZeroTier Central, locate the Pending device and authorize it.



Once authorized, the page displays as follows.

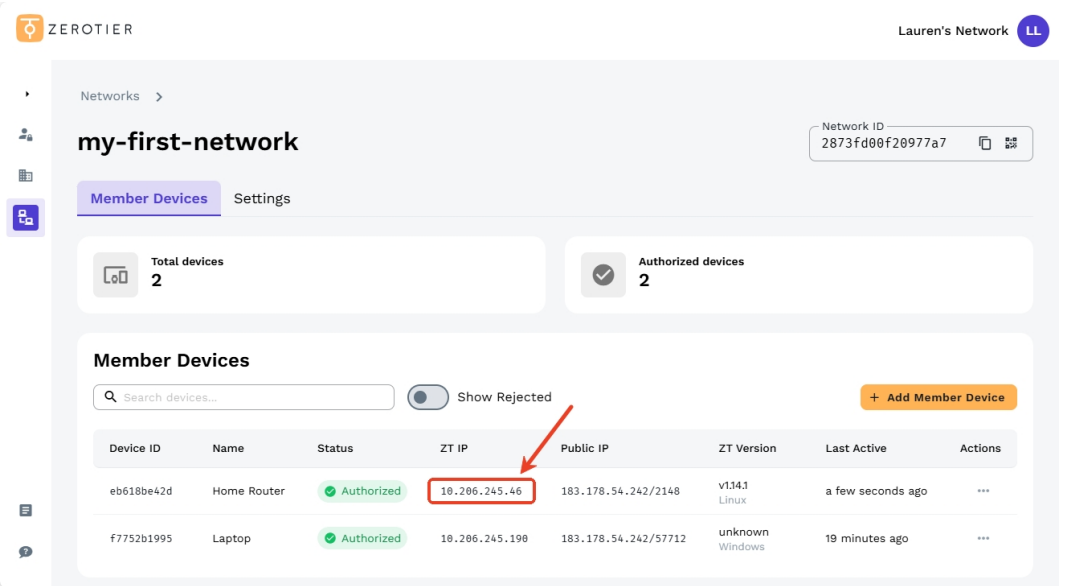


7. Add another device (such as a computer or smartphone) to the same ZeroTier network by following this guide. Once successfully added, the page displays as follows. You will see the details of member devices, such as **Device ID**, **Name**, **Status**, **Managed IP**, and **Public IP**.



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.



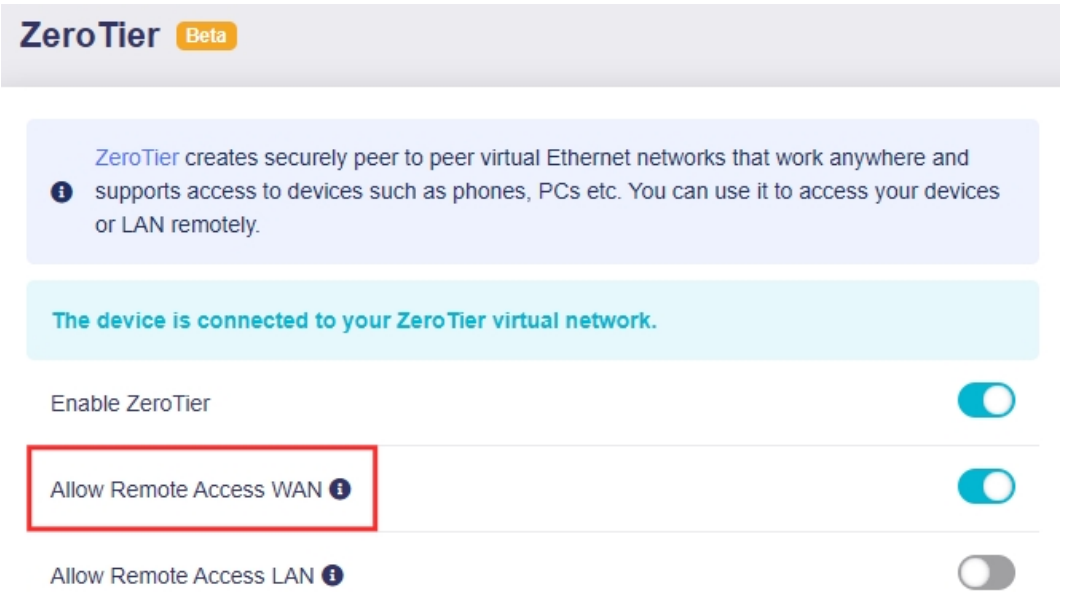
You can then use this Managed IP to access the router from your laptop that is on the same ZeroTier network.

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.

15.6.2 Allow Remote Access WAN

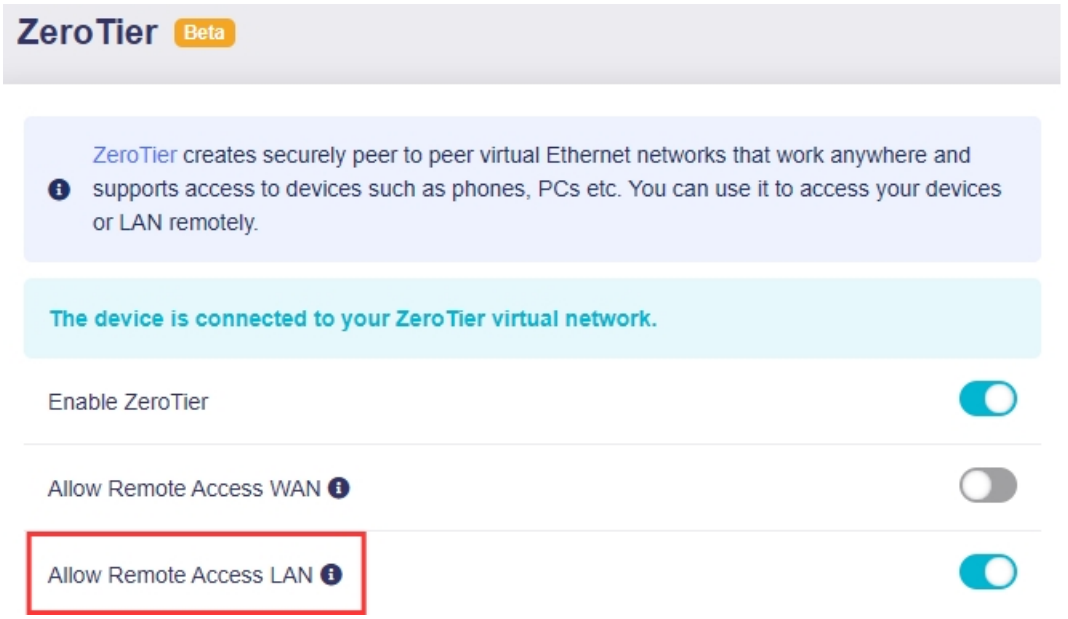
If this option is enabled, resources on the device's WAN side can be accessed through the ZeroTier virtual network. See here for more details.



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

15.6.3 Allow Remote Access LAN

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



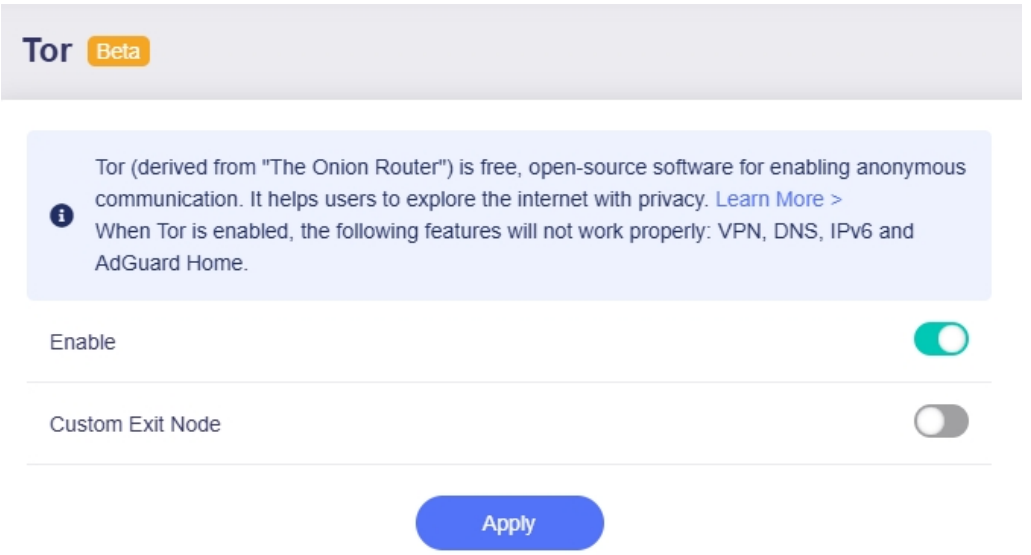
Note: This feature requires routing rules to be added to the ZeroTier network to take effect. One custom route can be added for free in Legacy Central, while in New Central you can only configure custom routes with an Essential plan or higher. See here for pricing details.

15.7 Tor

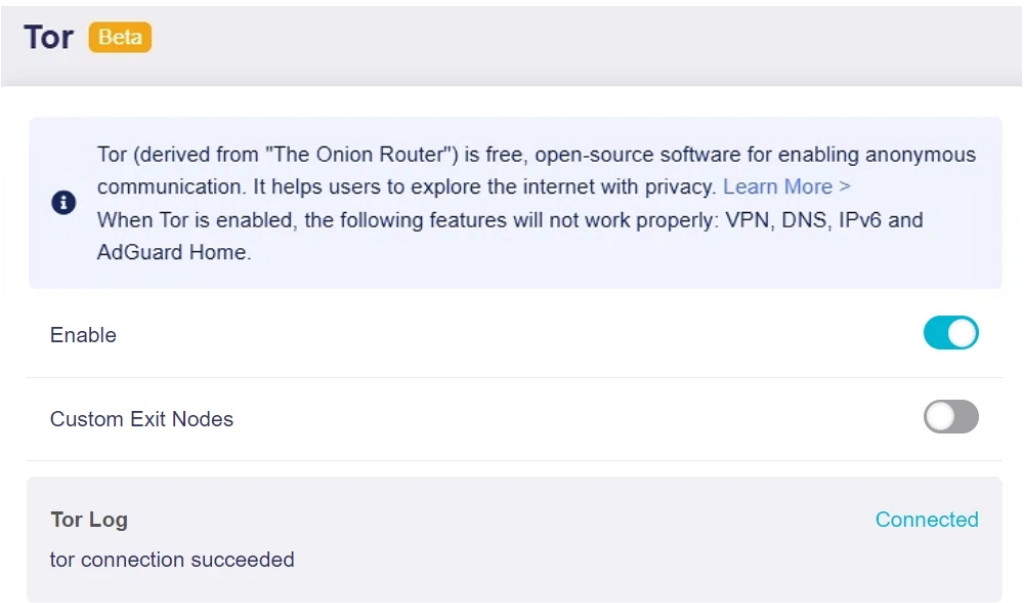
Tor (derived from **The Onion Router**) is a free and open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Note that this feature is currently in beta, and may have some bugs. When Tor is enabled, the following features will not work properly: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

Follow the steps below to set up Tor as needed.

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



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



Chapter 16

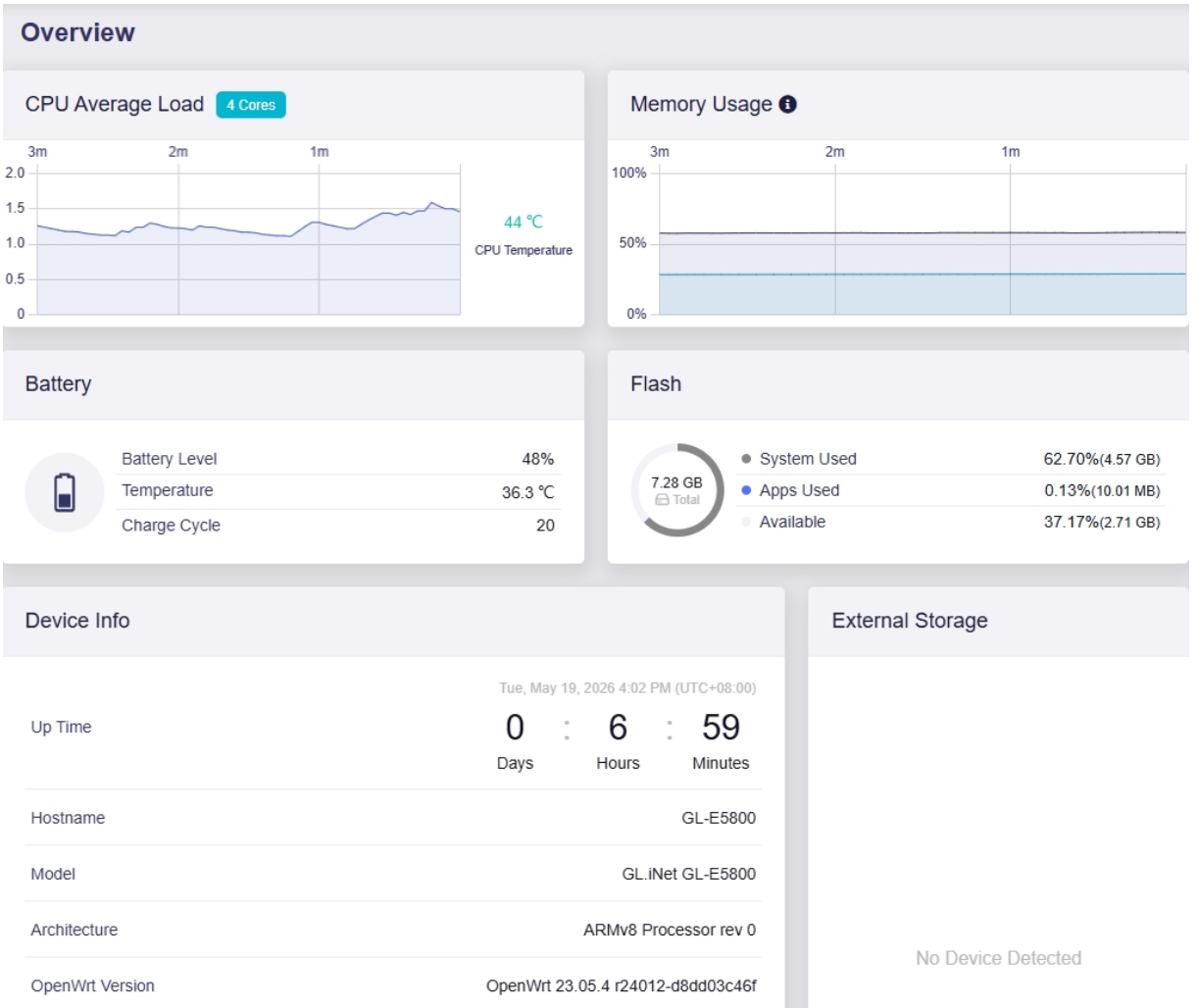
System

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

16.1 Overview

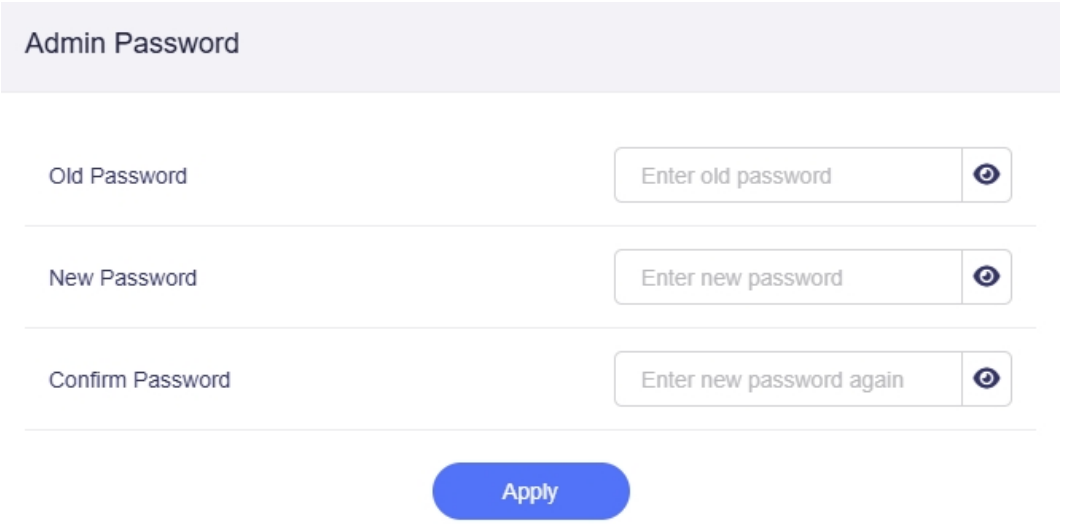
Log in to your router's web admin panel and navigate to **SYSTEM** > **Overview**. This page displays hardware status and supports some simple controls, including:

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



16.2 Admin Password

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



The requirements for the admin password are as follows:

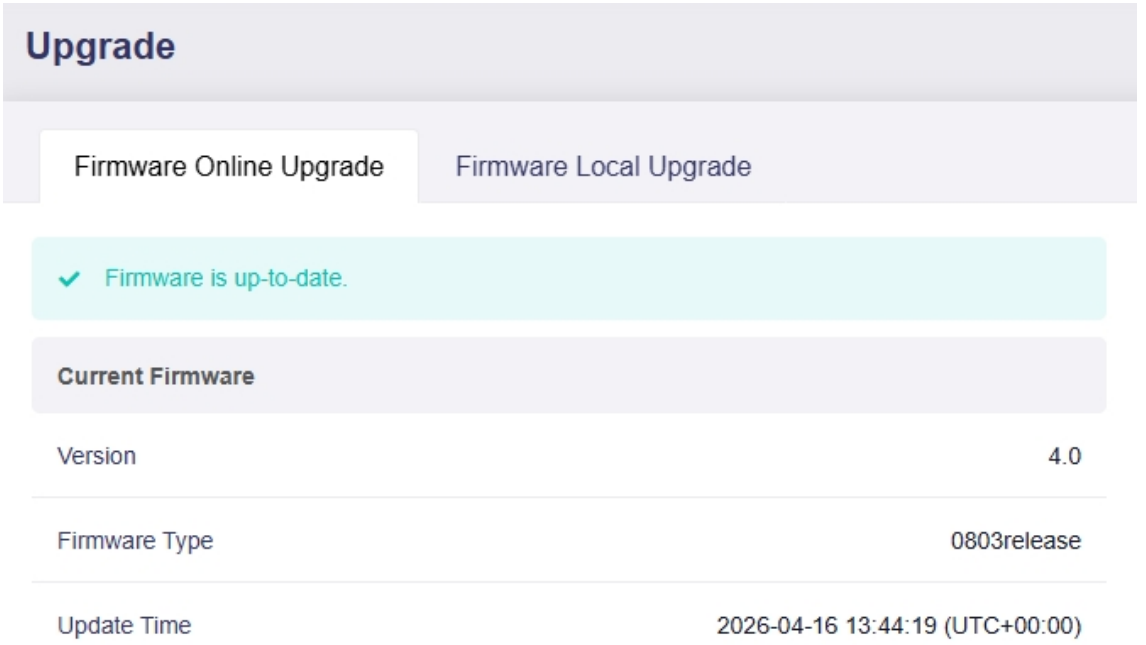
1. Minimum 10 characters and maximum 63 characters in length.
2. Letters (case sensitive), numbers and symbols (e.g., ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) are allowed.
3. At least two types (uppercase letters, lowercase letters, numbers, and symbols) are required.

16.3 Upgrade

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

16.3.1 Online Upgrade

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

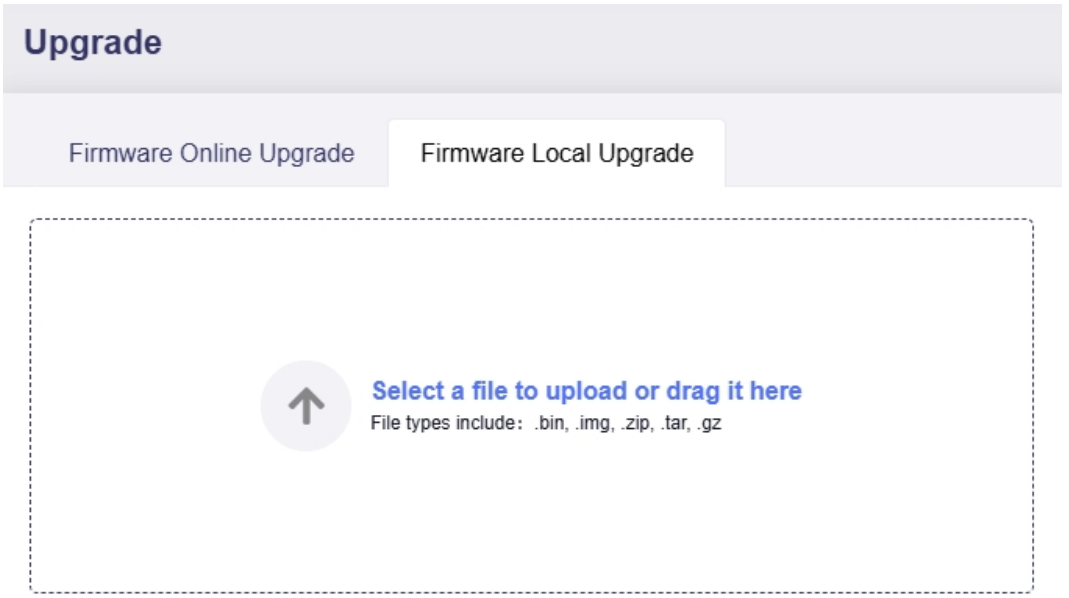


Tip: When trying to perform an online upgrade, if it displays **Download Failed**, please navigate to **SYSTEM** -> **Time Zone**, and fix the time zone error (sync to browser).

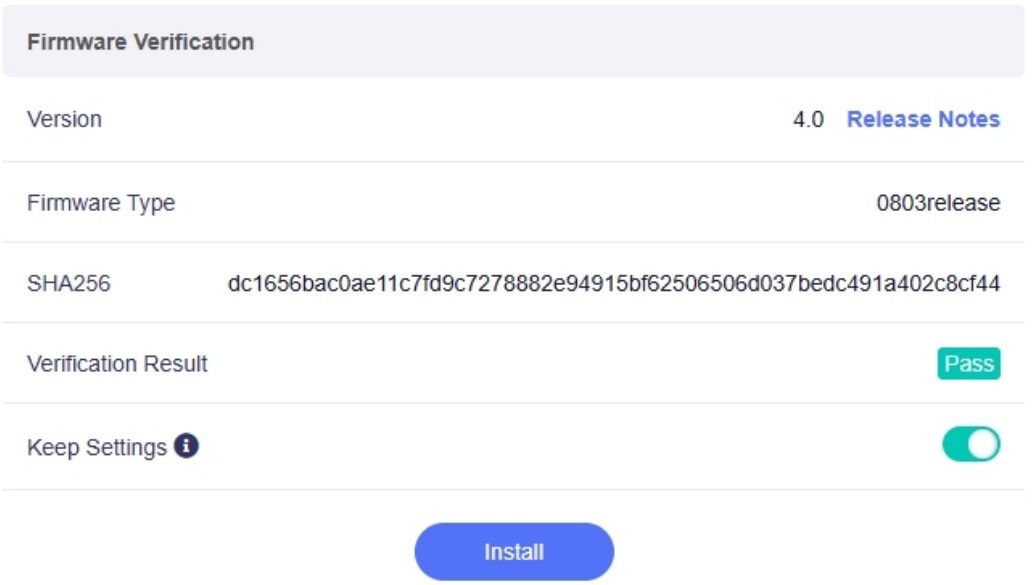
16.3.2 Local Upgrade

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

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



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

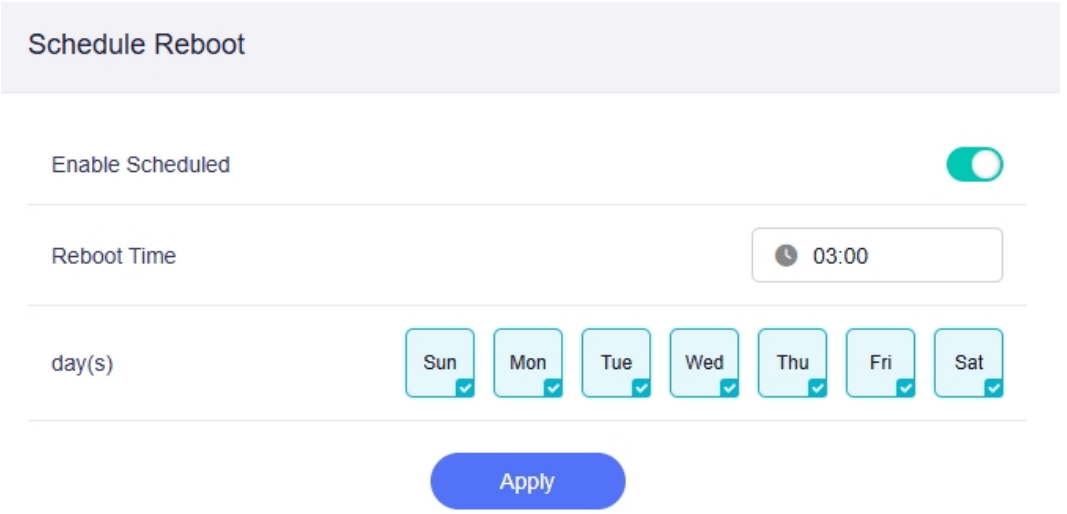


- **Keep Settings**: If enabled, current settings are retained. However, any manually installed packages must be reinstalled after the upgrade completes. Do not enable this option when downgrading the firmware.

16.4 Scheduled Tasks

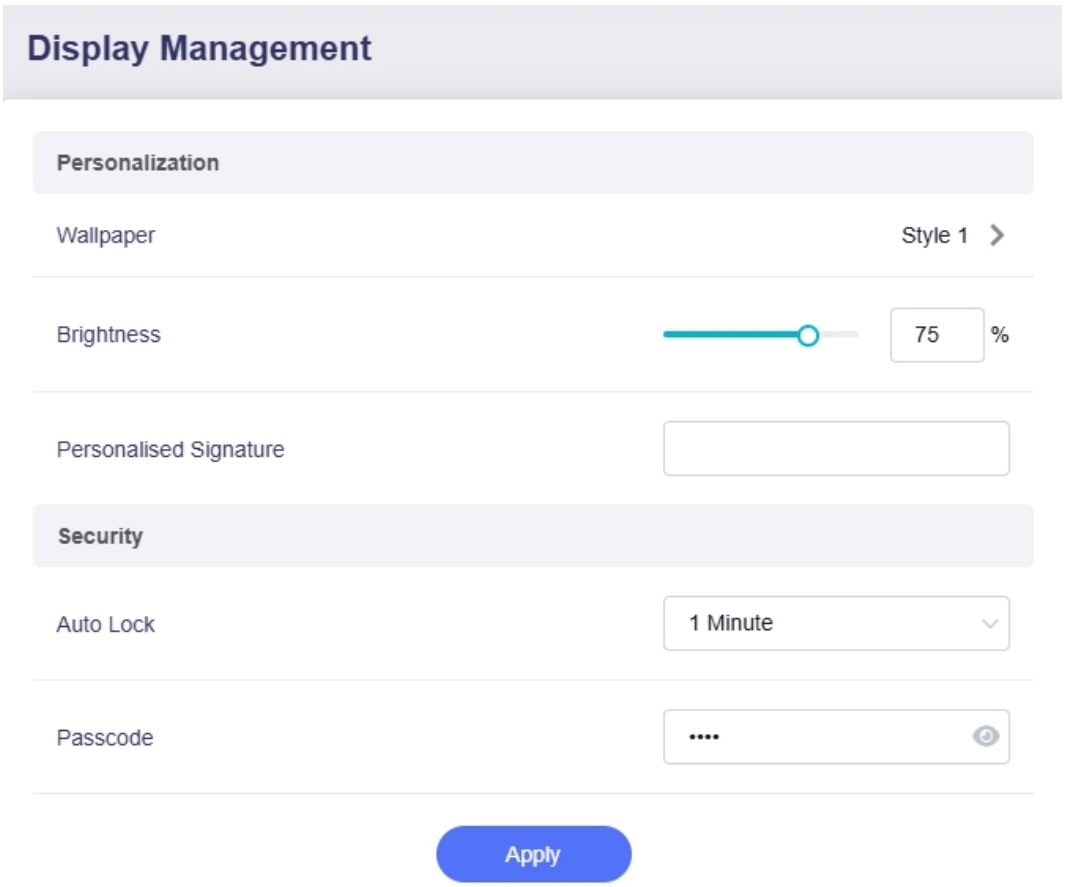
Log in to your router's web admin panel and navigate to **SYSTEM** > **Scheduled Tasks**. This page allows you to set a reboot schedule. Synchronize the time in the Time Zone before using this function. If the device shuts down at the scheduled time, the task will not be executed.

Set a schedule for automatically restarting your router as needed. Once enabled, set the reboot times, select the weekly effective days, then click **Apply**.



16.5 Display Management

Log in to your router's web admin panel and navigate to **SYSTEM** > **Display Management**. This page lets you manage the touchscreen display and its related settings.



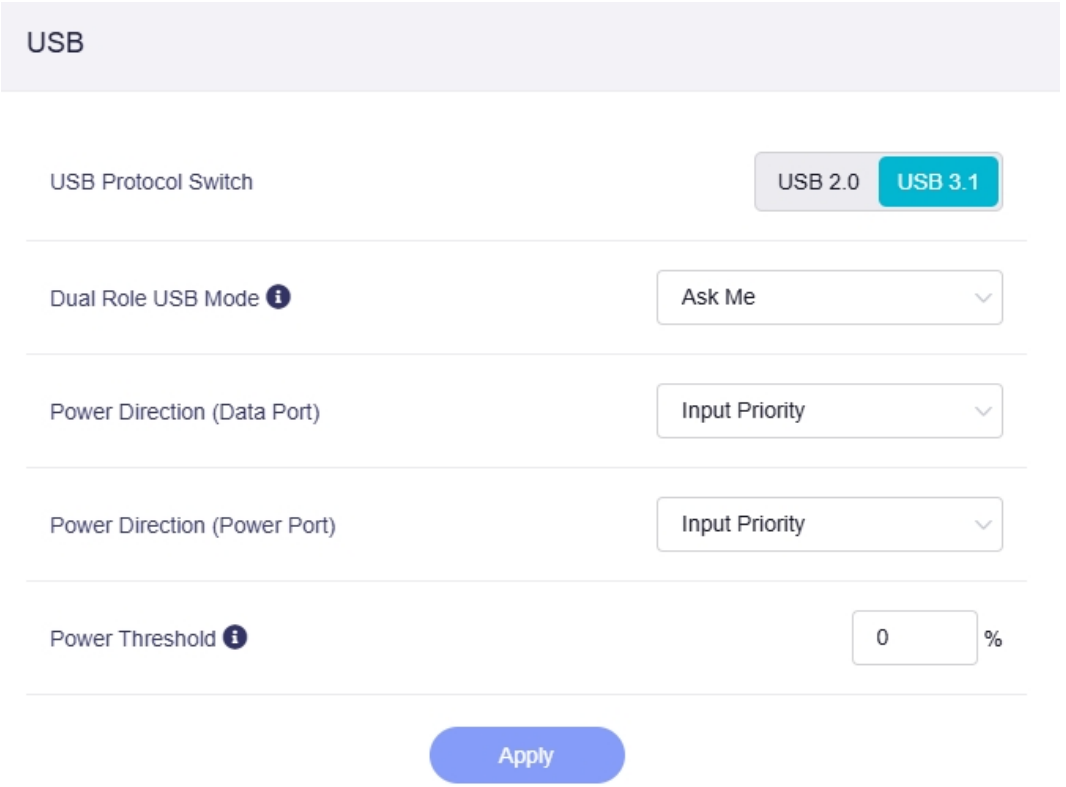
- **Wallpaper**: Customize the wallpaper and wake display style.
- **Brightness**: Adjust the touchscreen brightness. Use the slider or enter a percentage to fit different lighting conditions.
- **Personalised Signature**: Add a custom text to the touchscreen to show your unique style or for quick identification.
- **Auto Lock**: Set the time delay for the screen to auto-lock when there is no activity. The range is 15 seconds to 5 minutes.
- **Passcode**: Set a 4-digit passcode for the touchscreen for an extra layer of security.

16.6 USB & Power

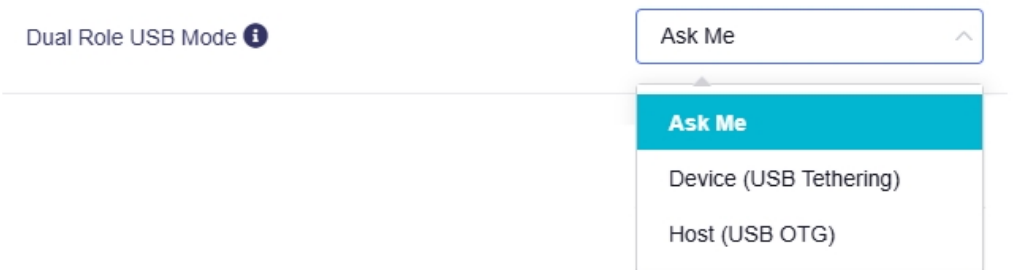
Log in to your router's web admin panel and navigate to **SYSTEM** > **USB & Power**. This page allows you to configure USB-related and power settings for your router, such as USB protocol, power direction, idle timeouts, and standby behavior.

16.6.1 USB

This section lets you customize the behavior of your router's USB ports.



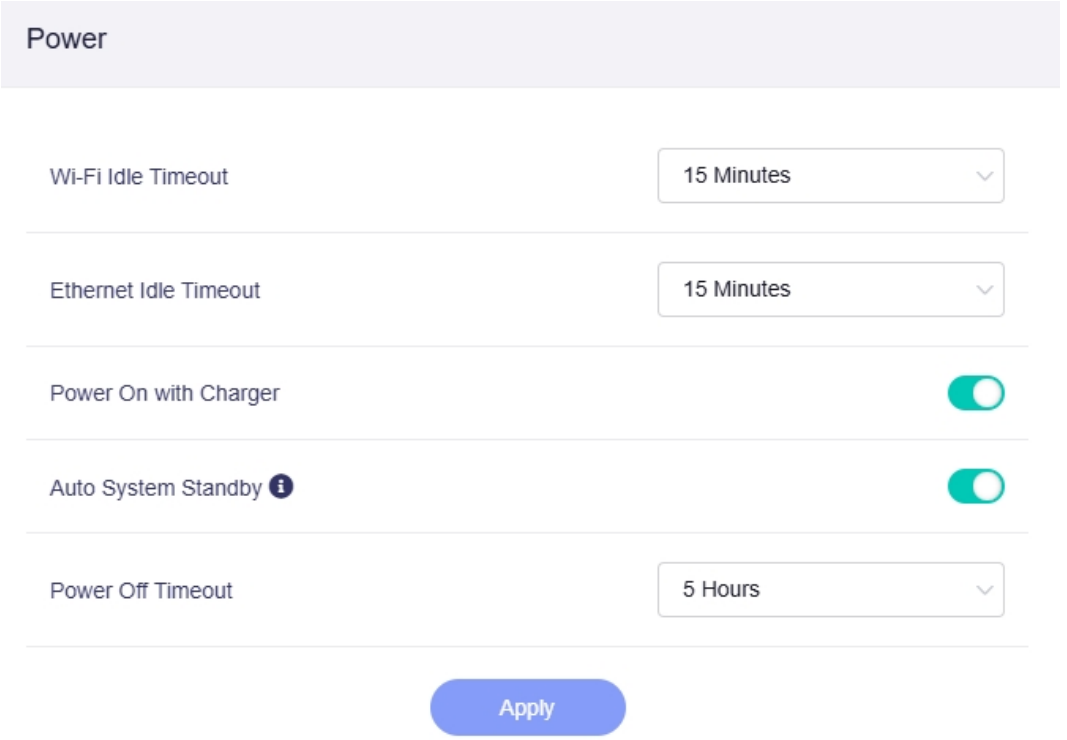
- **USB Protocol Switch**: Switch between USB 2.0 and USB 3.1 protocols for the USB port.
- **Dual Role USB Mode**: Select the USB working mode from the dropdown menu. You can set it as Device or Host.



- **Power Direction**: Choose the power priority for the USB port from the dropdown menu. You can set it as Input Priority or Output Priority.
- **Power Threshold**: Set a specific power threshold percentage for the USB port to control the minimum power level required for USB operations, helping to preserve battery life.

16.6.2 Power

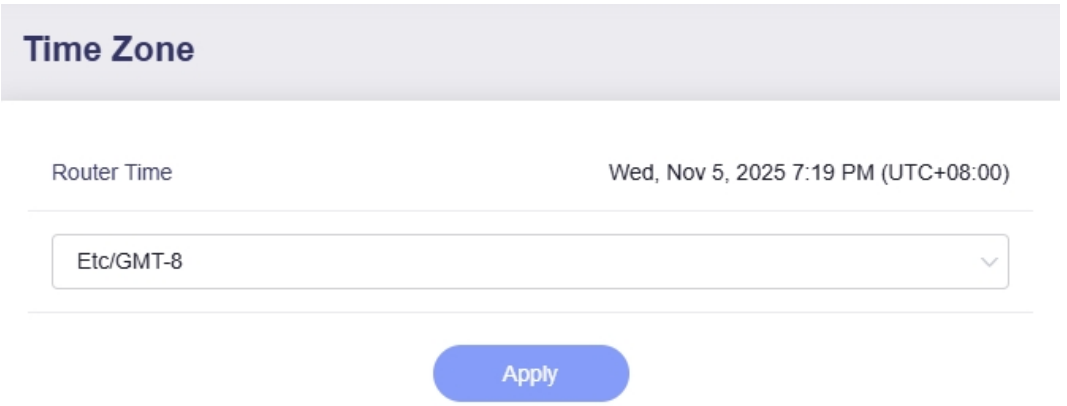
This section enables you to optimize power consumption and device behavior.



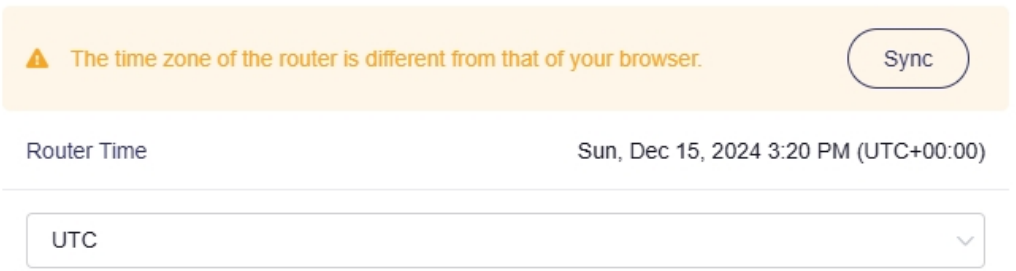
- **Wi-Fi Idle Timeout**: Set the idle duration (range from 10 minutes to 2 hours, or never) after which Wi-Fi will enter standby.
- **Ethernet Idle Timeout**: Set the idle duration (range from 10 minutes to 2 hours, or never) for Ethernet to switch to standby.
- **Power Off Timeout**: Set the time delay (range from 1 hour to 12 hours, or never) until the router automatically powers off when idle.
- **Power On with Charger**: Toggle this switch to enable/disable the router powering on automatically when connected to a charger.
- **Auto Standby**: Toggle this switch to activate/deactivate automatic standby for power saving.

16.7 Time Zone

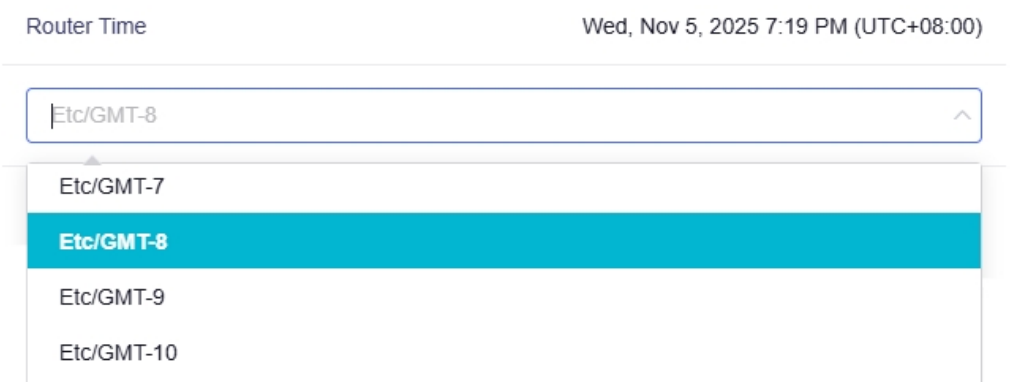
Log in to your router's web admin panel and navigate to **SYSTEM** > **Time Zone**. This page displays your router's system time, indicating the date, time, and corresponding time zone offset.



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



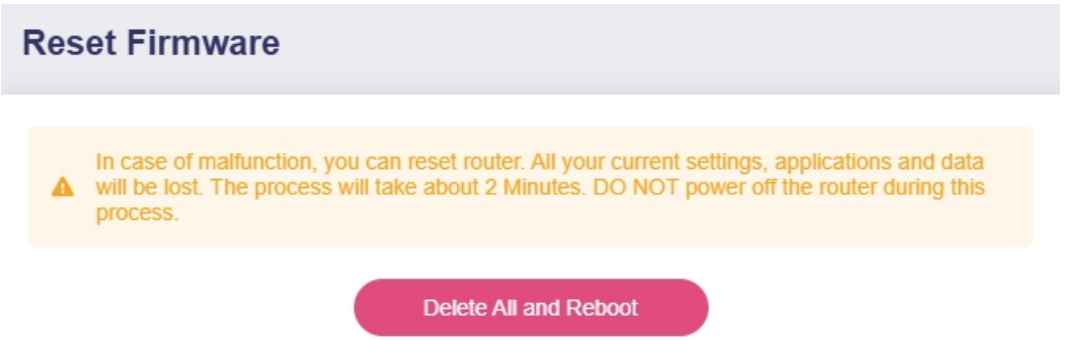
To switch time zone, select the appropriate time zone from the list to ensure the router's system time matches your local time.



16.8 Reset Firmware

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

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

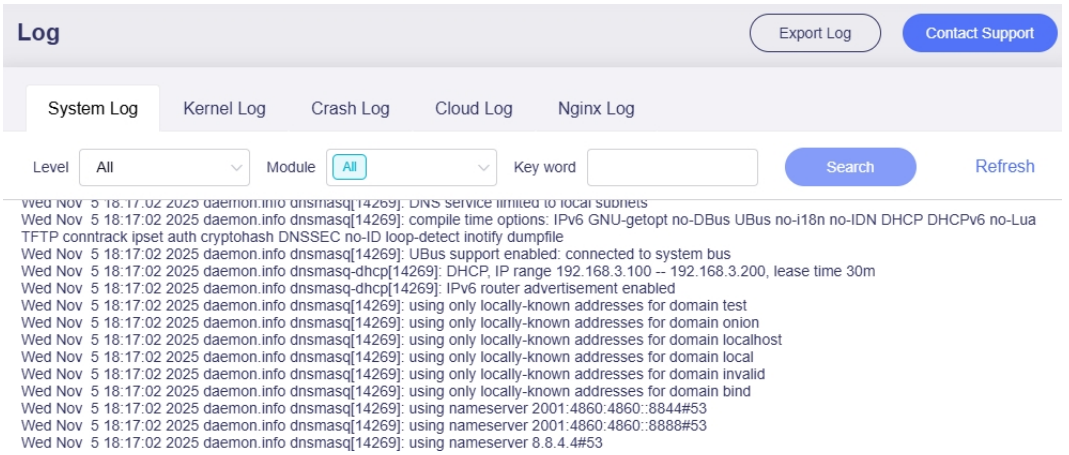


Note: All your current settings, applications and data will be cleared. The process will take about 2 minutes. Do not power off the router during this process.

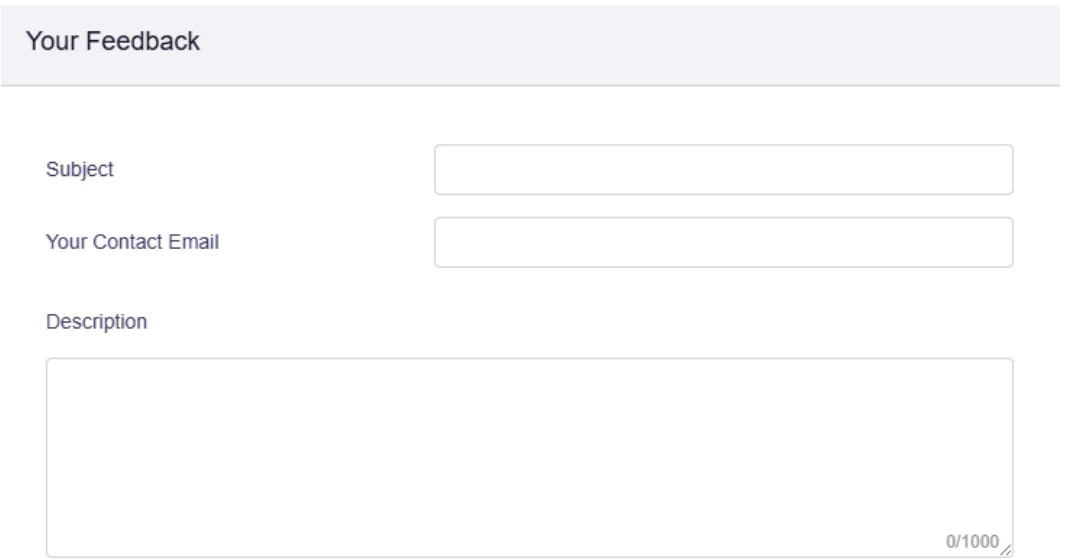
If you fail to access the router's web admin panel, try resetting your router using the physical reset button on the side.

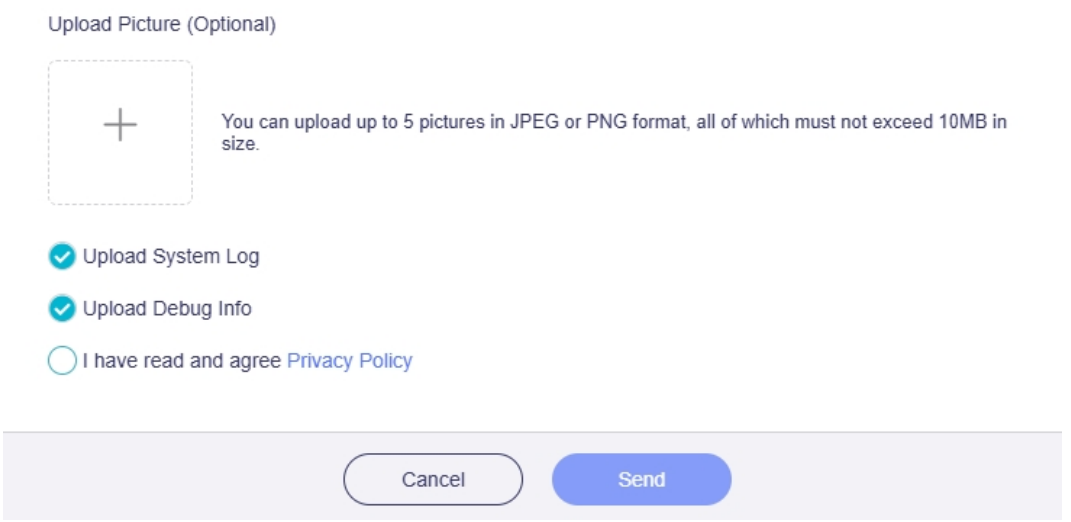
16.9 Log

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



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



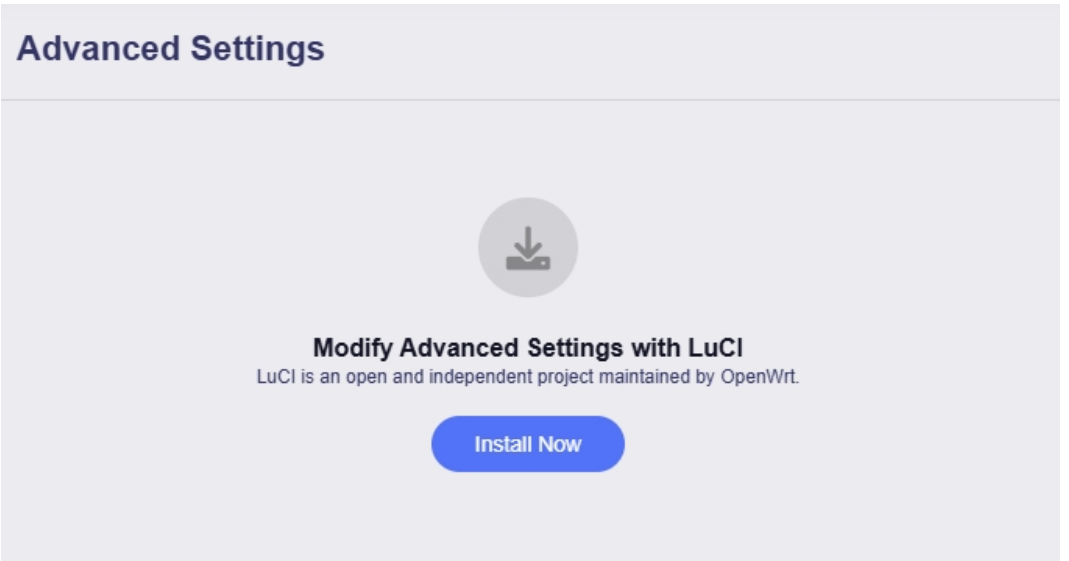

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.10 Advanced Settings

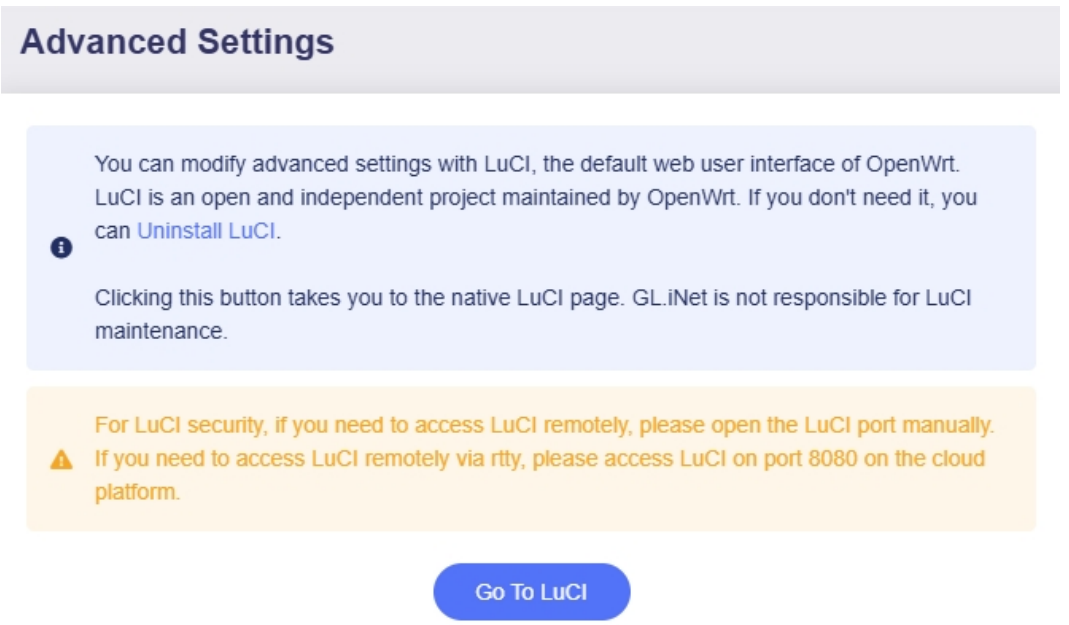
Log in to your router's web admin panel and navigate to **SYSTEM** > **Advanced Settings**. This page allows you to modify advanced settings in LuCI, which is the default web user interface of OpenWrt. As an open and independent project maintained by OpenWrt, LuCI is provided as-is. GL.iNet is not responsible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

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

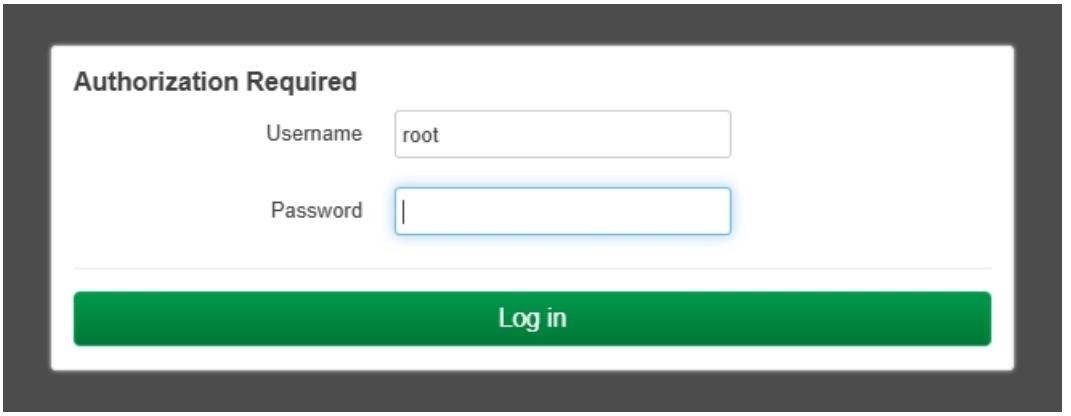
1. Click **Install Now**, and it will be installing LuCI interface.



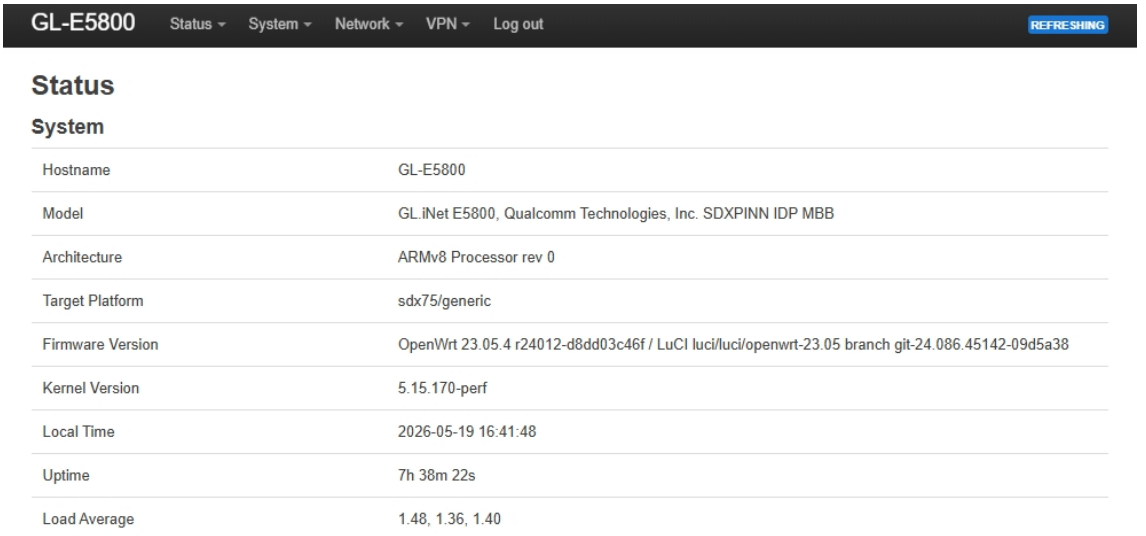
2. Click **Go To LuCI**, and you will be re-directed to the LuCI login page.



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



You will then log in to the LuCI interface.



Regulatory and Legal

Regulatory Compliance

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

(1) This device may not cause harmful interference.

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

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

RF Exposure Compliance

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

Trademarks

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

Limitation of Liability

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

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

Software License

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

Export Control

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