



User Manual

GL-A1300 / Slate Plus

Wi-Fi 5 Travel Router

Firmware Version 4.5.22

About This Manual

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

With this guide, you will be able to:

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

Format Conventions

These symbols/colors help you follow steps faster.

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

Note:

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

Need More Help or Info?

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

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

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

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

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

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

Contents

Chapter 1	Get To Know Your Router	9
1.1	Product Overview	10
1.1.1	Appearance	10
1.1.2	Interface and Button	11
1.1.3	LED	12
1.2	Specifications	12
1.3	Package Contents	13
Chapter 2	Hardware Connection	14
2.1	Choosing a Location	15
2.2	Connecting the Router	15
Chapter 3	Log In To Your Router	16
Chapter 4	Set Up Internet Connection	18
4.1	Connect to the Internet via Ethernet Cable	20
4.1.1	Basic Setup	20
4.1.2	Protocol	21
4.2	Connect to the Internet via an Existing Wi-Fi	24
4.2.1	Basic Setup	24
4.2.2	Repeater Options	27
4.3	Connect to the Internet via USB Tethering	28
4.3.1	iPhone Tethering	28
4.3.2	Android Tethering	30
4.3.3	Troubleshooting	30
4.4	Connect to the Internet via USB Modem	31
Chapter 5	Wireless	33
5.1	5 GHz Wi-Fi	34
5.2	2.4 GHz Wi-Fi	36
Chapter 6	Clients	38
6.1	Device Details	40
6.2	Action	42
6.3	Remove Clients	44
6.4	Sort	45
Chapter 7	Get To Know VPN	46

7.1 Introduction	47
7.2 Application Scenarios	48
Chapter 8 VPN Dashboard	50
8.1 VPN Client	51
8.1.1 Client Options	52
8.1.2 Policy Mode	54
8.1.3 Global Options	55
8.2 VPN Server	57
8.2.1 Server Options	58
8.2.2 Server Route Rule	59
8.2.3 Global Options	60
Chapter 9 Set Up VPN Server	61
9.1 Set Up OpenVPN Server	62
9.1.1 Preparation	62
9.1.2 Setup Steps	63
9.1.3 Troubleshooting	65
9.2 Set Up WireGuard Server	66
9.2.1 Preparation	66
9.2.2 Setup Steps	67
9.2.3 Troubleshooting	70
Chapter 10 Set Up VPN Client	71
10.1 Set Up OpenVPN Client	72
10.1.1 Preparation	72
10.1.2 Set Up NordVPN	72
10.1.3 Set Up OpenVPN Client Manually (for other providers)	78
10.2 Set Up WireGuard Client	81
10.2.1 Preparation	81
10.2.2 Set Up AzureVPN	82
10.2.3 Set Up Mullvad	85
10.2.4 Set Up WireGuard Client Manually (for other providers)	89
Chapter 11 Tor	93
Chapter 12 Applications	95
12.1 Plug-ins	96

12.2 Dynamic DNS	97
12.2.1 Enable DDNS	97
12.2.2 Check if DDNS Works	100
12.2.3 HTTPS Remote Access	102
12.2.4 SSH Remote Access	104
12.3 GoodCloud	106
12.3.1 Enable GoodCloud	107
12.3.2 Manage Your Router	111
12.3.3 Unbind Device	116
12.4 Network Storage	117
12.4.1 Connect Storage	117
12.4.2 Set Up Samba	118
12.4.3 Set Up WebDAV	121
12.4.4 Set Up DLNA	124
12.5 AdGuard Home	125
12.6 Parental Control	127
12.6.1 Quick Setup	127
12.6.2 Troubleshooting	135
12.7 ZeroTier	136
12.7.1 Set Up ZeroTier	137
12.7.2 Allow Remote Access WAN	141
12.7.3 Allow Remote Access LAN	142
12.8 Tailscale	143
12.8.1 Set Up Tailscale	144
12.8.2 Allow Remote Access WAN	147
12.8.3 Allow Remote Access LAN	148
12.8.4 Custom Exit Nodes	149
Chapter 13 Network	150
13.1 Firewall	151
13.1.1 Port Forwards	151
13.1.2 Open Ports on Router	153
13.1.3 DMZ	154
13.2 Multi-WAN	155
13.2.1 Interface Status Track	155

13.2.2 Multi-WAN Mode	158
13.3 LAN	161
13.3.1 Basic Settings	161
13.3.2 DHCP Server	162
13.3.3 Address Reservation	164
13.4 Guest Network	165
13.4.1 Basic Settings	165
13.4.2 DHCP Server	166
13.5 DNS	168
13.5.1 General Settings	168
13.5.2 DNS Server Settings	169
13.5.3 Edit Hosts	171
13.6 Network Mode	173
13.7 IPv6	175
13.7.1 IPv6 Mode	175
13.7.2 DNS Acquisition Method	176
13.8 MAC Address	177
13.9 Drop-in Gateway	179
13.10 IGMP Snooping	181
13.11 NAT Settings	182
Chapter 14 System	183
14.1 Overview	184
14.2 Upgrade	185
14.2.1 Online Upgrade	185
14.2.2 Local Upgrade	186
14.3 Scheduled Tasks	187
14.3.1 LED Display Schedule	187
14.3.2 Schedule Reboot	188
14.3.3 5GHz Wi-Fi Schedule	189
14.3.4 2.4GHz Wi-Fi Schedule	191
14.4 Time Zone	193
14.5 Toggle Button Settings	194
14.6 Log	195
14.7 Security	196

14.7.1 Admin Password	196
14.7.2 Local Access Control	197
14.7.3 Remote Access Control	199
14.8 Reset Firmware	200
14.9 Advanced Settings	201

Chapter 1

Get To Know Your Router

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

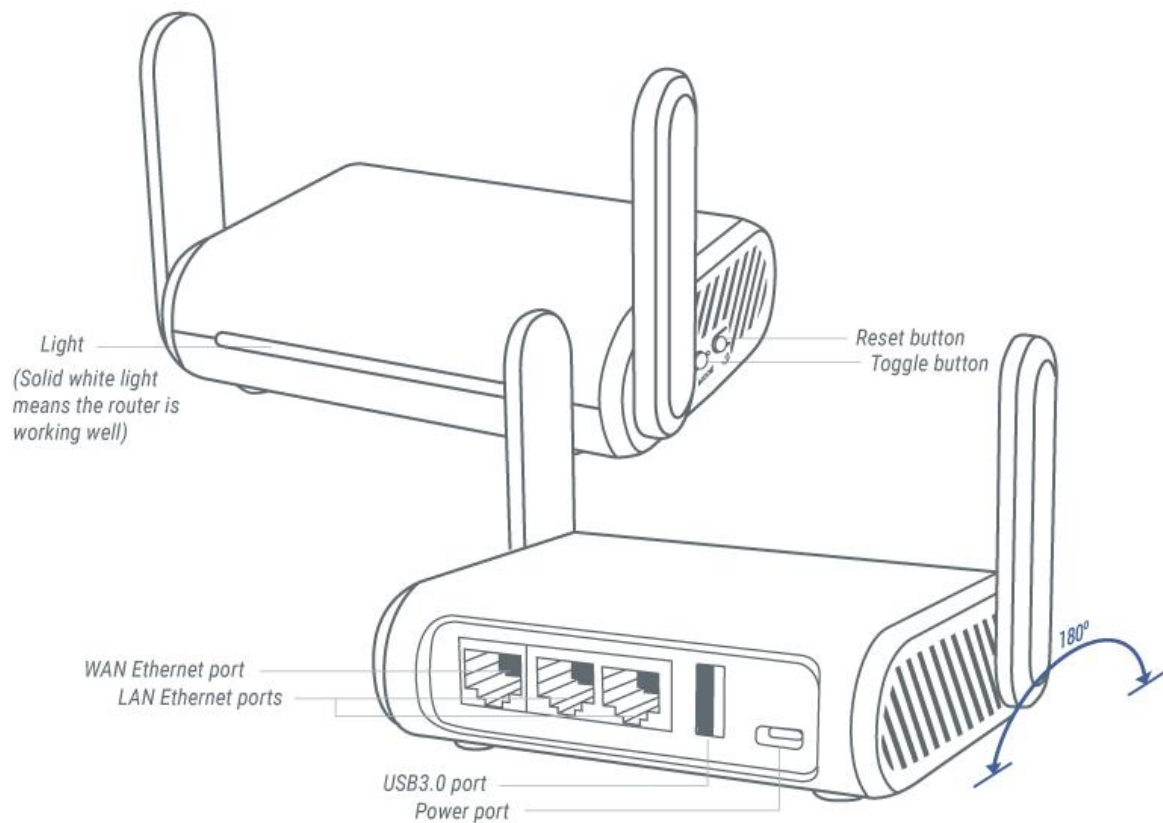
1.1 Product Overview

Slate Plus (GL-A1300) is a pocket-sized travel router with a powerful CPU optimized for network stability and processing VPN encryption efficiently. It includes our latest security features and runs on the latest OpenWrt operating system. It is designed for frequent travelers who have a heavy demand on using VPN networks.

1.1.1 Appearance



1.1.2 Interface and Button



Item	Description
Power Port	Connects to the power adapter.
WAN Ethernet Port	Connects to a modem or an Ethernet outlet for Internet.
LAN Etherne Port	Connects to wired devices if needed.
USB 3.0 Port	For USB storage devices, phone USB-tethering, and compatible cellular dongles.
Reset Button	Press and hold for 4 seconds to repair your network; Press and hold for 10 seconds and then release to reset the router to factory default.
Toggle Button	A physical switch that toggles selected router settings with a flip. You can configure it in the web admin panel to enable one-click switching of specific features.

1.1.3 LED

Status	Indication
Solid Blue	Starting up
Pulsing Blue Slowly	Started but no Internet connection
Solid White	Connected to Internet
Flashing Blue Quickly	Resetting

1.2 Specifications

Interface	1 x WAN Ethernet port 2 x LAN Ethernet ports 1 x USB 3.0 port 1 x Type-C Power port 1 x Reset button 1 x Toggle button
CPU	IPQ4018, Quad Core@717MHz
Memory / Storage	DDR3L 256MB / NOR Flash 4MB + NAND Flash 128MB
Protocol	IEEE 802.11a/b/g/n/ac
Wi-Fi Speed	400Mbps (2.4GHz), 867Mbps (5GHz)
Antennas	2 x undetachable external Wi-Fi antennas
Ethernet Speed	10/100/1000Mbps
Power Input	Type-C, 5V/3A
Power Consumption	< 6.5W
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	118 x 85 x 30mm / 181g
Other Tools	Datasheet / Firmware / App / Unboxing

*Wireless speeds are based on IEEE 802.11 standards (e.g., 802.11ac for Wi-Fi 5). Actual throughput and range may be lower due to environmental obstacles (walls, metal), network congestion, or client device capabilities.

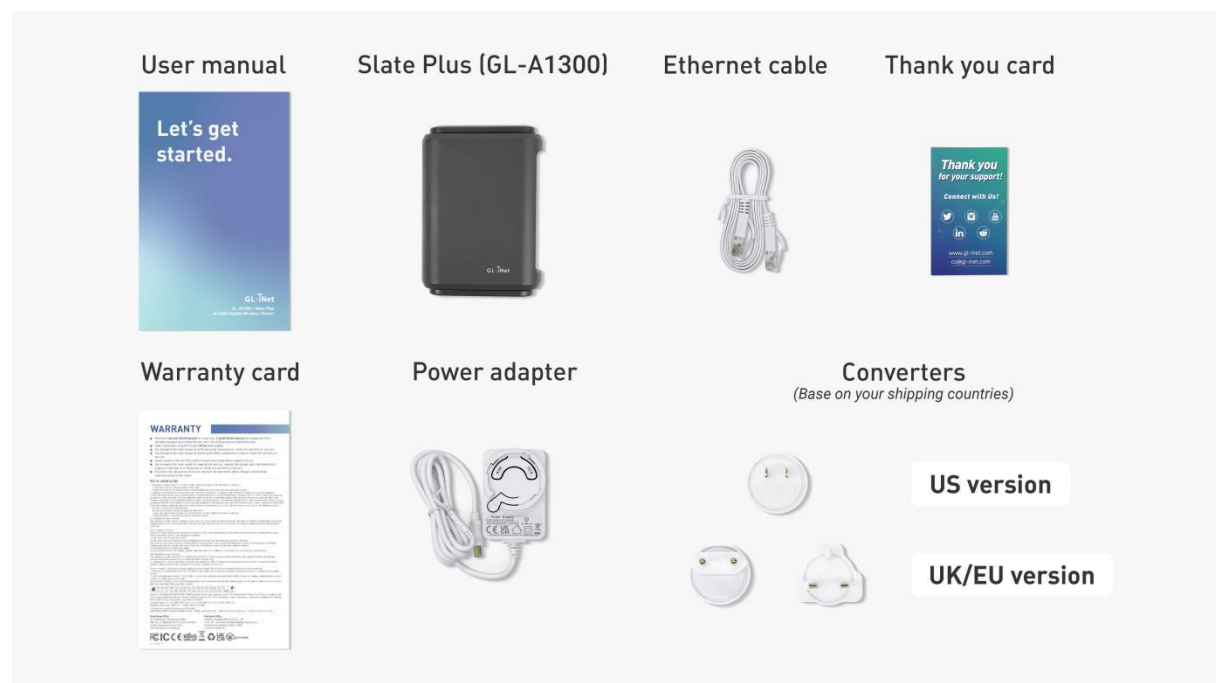
*Use of Wi-Fi 5 (802.11ac) and its features (MU-MIMO, 256-QAM, HT80) requires client devices to support the corresponding technologies.

1.3 Package Contents

Please note that the adapter within the package depends on your shipping country.

The package includes:

- 1 x Slate Plus (GL-A1300)
- 1 x User Manual
- 1 x Ethernet Cable
- 1 x Thank You Card
- 1 x Warranty Card
- 1 x Power Adapter
- 1 x Converter (Depending on your shipping country)



Chapter 2

Hardware Connection

This chapter covers router location selection and connection steps.

2.1 Choosing a Location

Follow these tips to choose a location for best performance.

- **Avoid moisture and heat:** Do not place the router in areas exposed to water, humidity, or high temperatures (e.g., sinks, radiators).
- **Ventilation and cooling:** Place the router in a cool, well-ventilated area for proper heat dissipation.
- **Central placement:** Position the router where it can connect to power and multiple devices easily (e.g., living room central zone).
- **Cable convenience:** Route cables and the power cord safely to prevent tripping hazards.
- **Stable surface:** Place the router on a horizontal, flat surface (shelf, desktop) for stability.
- **EMI avoidance:** Keep the router away from electromagnetic interference sources (Bluetooth devices, microwaves) to minimize signal interference.

2.2 Connecting the Router

1. Power on

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

2. Connect a device to the router

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

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

3. Log in to the router

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

Chapter 3

Log In To Your Router

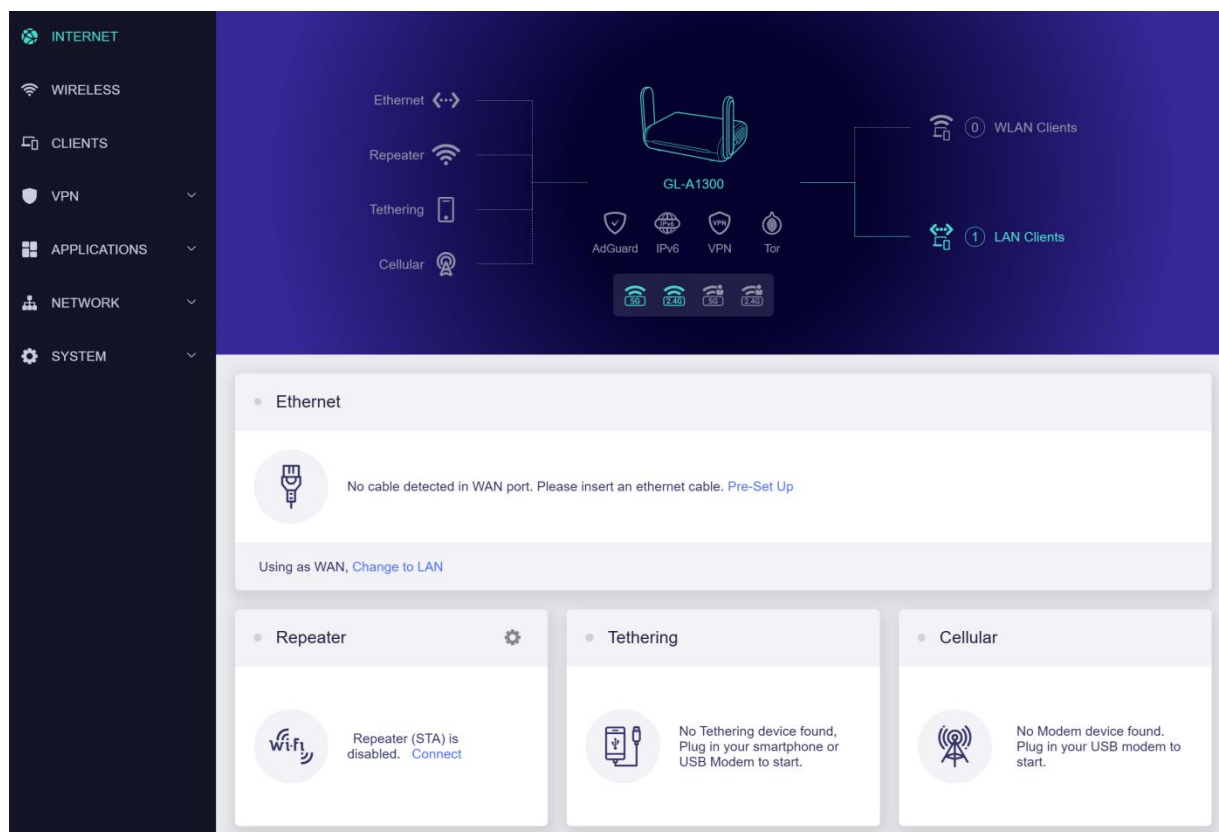
This chapter guides you to log in to your router via web admin panel.

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

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

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

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



Chapter 4

Set Up Internet Connection

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

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

1. **Ethernet:** Connect the router to a broadband network using an Ethernet cable plugged into the WAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.
2. **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.
3. **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. **USB Modem:** Insert a USB cellular modem with a pre-installed SIM card into the router. The router will then connect to the internet via 4G/5G mobile networks, providing connectivity independent of fixed-line broadband. This method offers high mobility and is suitable for scenarios such as in-vehicle use or outdoor activities.

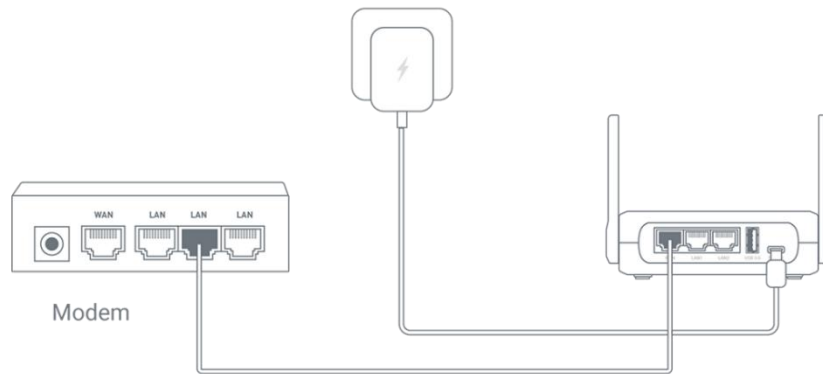
4.1 Connect to the Internet via Ethernet Cable

Connect the router to a broadband network using an Ethernet cable plugged into the WAN port. The router typically obtains an IP address automatically via DHCP. Users can also manually configure a static IP or PPPoE settings. This method delivers high stability and fast speed, making it ideal for home and office environments with fixed broadband access.

4.1.1 Basic Setup

Follow the steps below to connect your router to the Internet via an Ethernet cable.

1. Connect the **WAN** port of your router to the upstream device (e.g., an ISP modem, primary router, network switch or an Ethernet jack) via an Ethernet cable.



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

Ethernet

Protocol	DHCP
IP Address	10.100.211.199
Gateway	10.100.208.1
DNS Server	10.100.20.50 , 10.100.23.100

Modify

Using as WAN, [Change to LAN](#)



4.1.2 Protocol

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

- Ethernet

Protocol	DHCP
IP Address	10.100.211.199
Gateway	10.100.208.1
DNS Server	10.100.20.50 , 10.100.23.100



 Modify

Using as WAN, [Change to LAN](#)

- 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. You can configure a **VLAN ID** if your service provider requires the interface to use a specific tagged VLAN ID.

Ethernet Settings

Protocol **DHCP** Static PPPoE

 IP address assigned by higher network machine.

IPv4

IP Address	10.100.211.199
Netmask	255.255.252.0
Gateway	10.100.208.1
DNS Server 1	10.100.20.50
DNS Server 2	10.100.23.100

VLAN ID 

Cancel Apply

- **Static**

A static IP address is required if your ISP (Internet Service Provider) assigns a fixed public IP address, or if you need to manually configure network parameters (e.g., IP address, gateway, subnet mask). You can configure a **VLAN ID** if your service provider requires the interface to use a specific tagged VLAN ID.

The screenshot shows the 'Ethernet Settings' window. At the top, there's a 'Protocol' section with three buttons: 'DHCP', 'Static' (which is highlighted in blue), and 'PPPoE'. Below this is the 'IPv4' section, which contains five input fields: 'IP Address', 'Netmask', 'Gateway', 'DNS Server 1', and 'DNS Server 2'. The 'DNS Server 2' field has a placeholder text 'Optional'. Below the IPv4 section is a 'VLAN ID' field with an information icon and a placeholder text 'Optional (1 ~ 4094)'. At the bottom of the window are two buttons: 'Cancel' and 'Apply'.

- **PPPoE**

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol widely used by ISPs. Typically, they will provide a modem along with a unique username and password, which are required to set up an internet connection. You can configure a **VLAN ID** if your service provider requires the interface to use a specific tagged VLAN ID.

Ethernet Settings

Protocol

DHCP

Static

PPPoE

PPPoE Setting

Username

Optional

Password

Optional



VLAN ID 

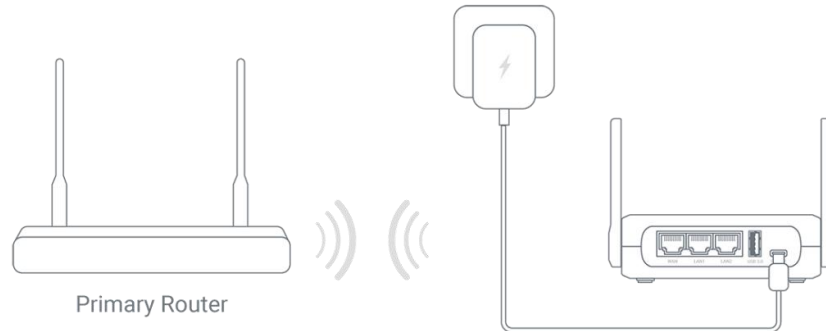
Optional (1 ~ 4094)

Cancel

Apply

4.2 Connect to the Internet via an Existing Wi-Fi

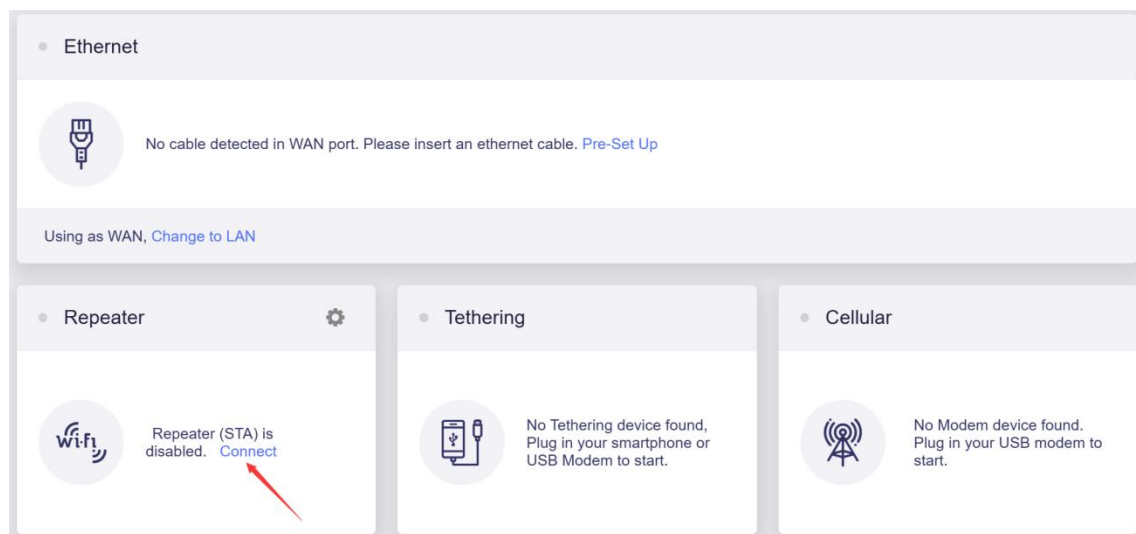
Connect the router as a repeater to the existing wireless network to boost Wi-Fi signals and create a local network isolated from the primary network. When in hotels or cafes with free public hotspots, using a repeater not only strengthens Wi-Fi signals, but also provides wired and wireless access for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

4.2.1 Basic Setup

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



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

Join Wi-Fi

Available Networks ⓘ

Join Other Network

	GL-BE9300-e52	2.4G
	GL-MT6000-787	2.4G
	GL-MT300N-V2-184	2.4G
	GL-MT6000-787-5G	5G
	GL-XE300-407	2.4G
	GL-AX1800-f4e	2.4G
	GL-AX1800-f4e-5G	5G

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

Join Network

SSID

@GL-OFFICE

Password

Remember

Lock BSSID ⓘ

Manually Set Static IP

Back

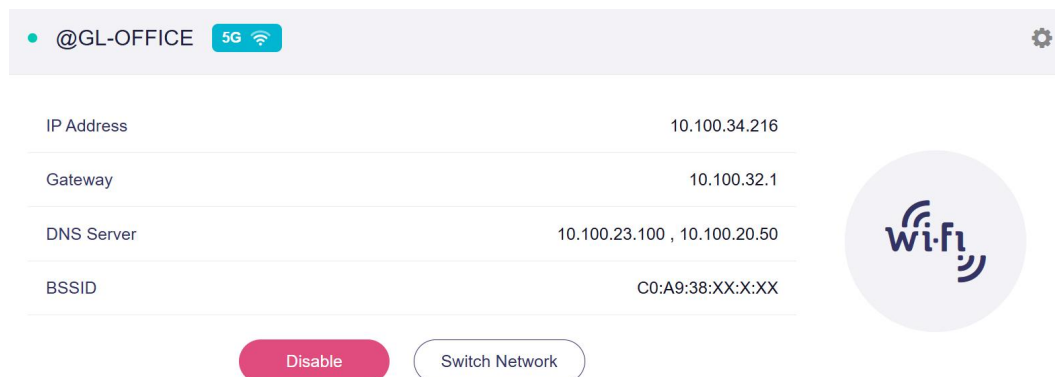
Apply

- **Remember:** Enable this to remember the current repeated Wi-Fi network.

- **Lock BSSID:** When enabled, the router will connect only to the specific access point (AP) corresponding to the selected BSSID, even when other APs share the same SSID.
 - **Manually Set Static IP:** If enabled, you may manually configure IP address, subnet mask, gateway and DNS servers, instead of obtaining IP settings automatically via DHCP.
4. If the target Wi-Fi SSID is not in the Available Network list, click **Join Other Network** in the top right corner, manually input the Wi-Fi SSID and other info required, and click **Apply**.



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



4.2.2 Repeater Options

Click the gear icon in the upper-right corner to configure Repeater options.

@GL-OFFICE 5G

IP Address	10.100.34.216
Gateway	10.100.32.1
DNS Server	10.100.23.100 , 10.100.20.50
BSSID	C0:A9:38:XX:X:XX

Disable

Switch Network

wifi

The page may vary due to different firmware versions.

Repeater Options

Allow Switching To Other Saved Networks ⓘ

Band Selection ⓘ

Auto

5GHz

2.4GHz

Force 20MHz Bandwidth For 2.4G ⓘ

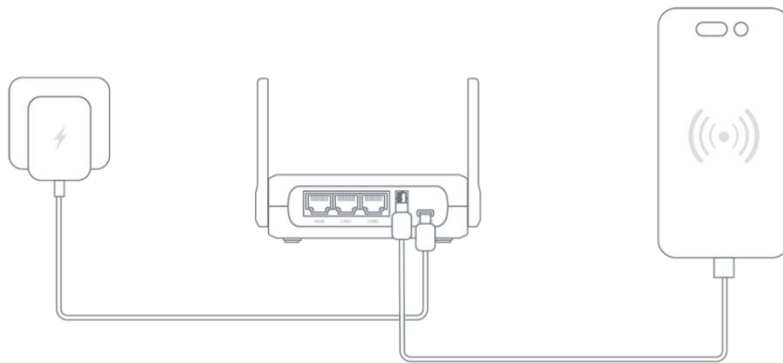
Cancel

Apply

- **Allow Switching to Other Saved Networks:** If the option is enabled, the router will automatically connect to other saved networks when it is unable to connect to the current Wi-Fi network.
- **Band Selection:** If you manually select a band, the router will not scan or connect to any Wi-Fi that is using another band.
- **Force 20MHz Bandwidth for 2.4G:** If this option is enabled, the device will improve the stability of the connection by reducing the connection rate.
Note: It only works when repeating 2.4G Wi-Fi.

4.3 Connect to the Internet via USB Tethering

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

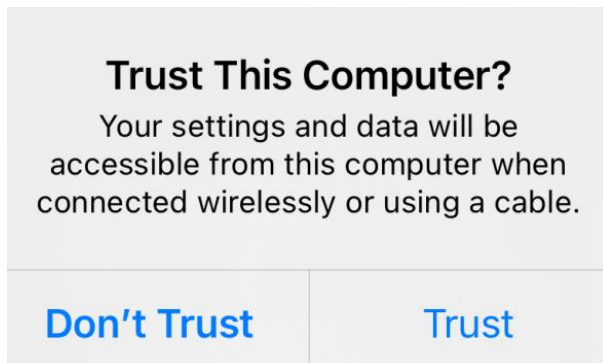


Host-less modem works in Tethering as well during the setup of the modem.

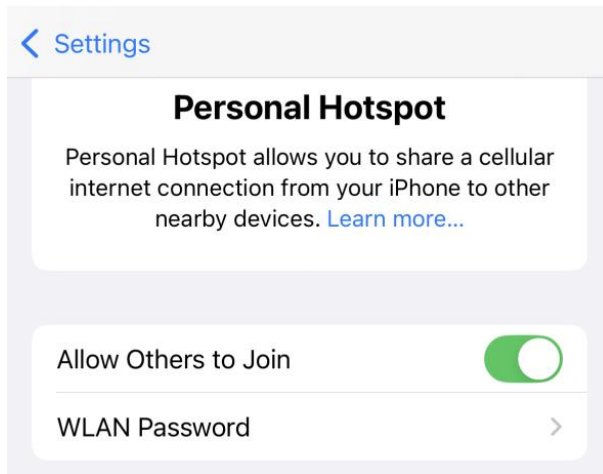
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

4.3.1 iPhone Tethering

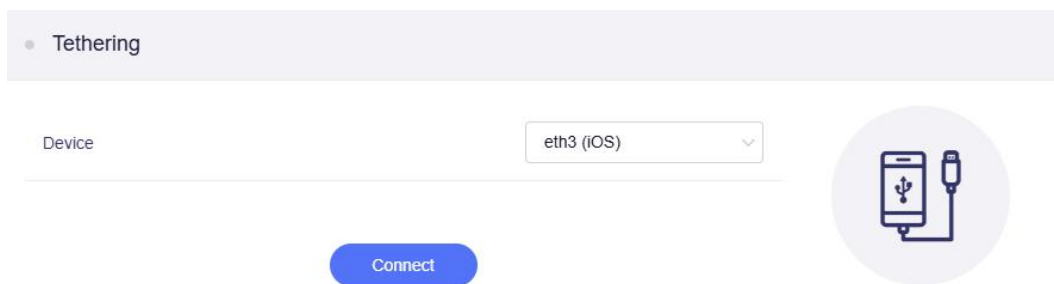
1. Connect an iPhone to the router's USB port using a USB cable. A system dialog will appear asking whether to trust the device. Tap **Trust** to proceed.



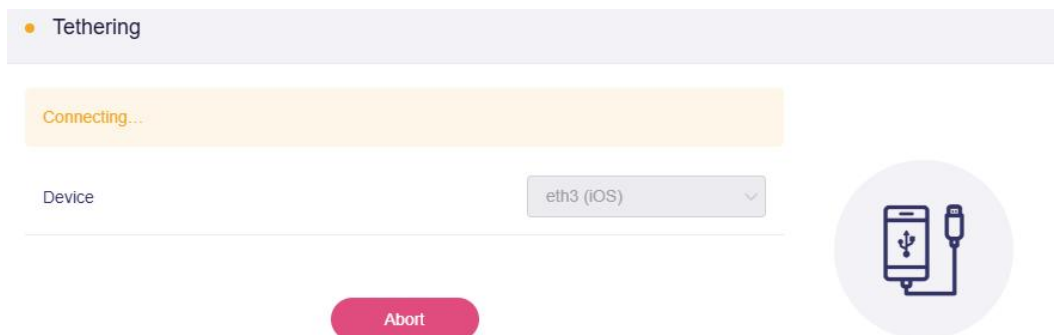
2. Go to iPhone **Settings** > **Personal Hotspot**. Enable **Allow Others to Join**.



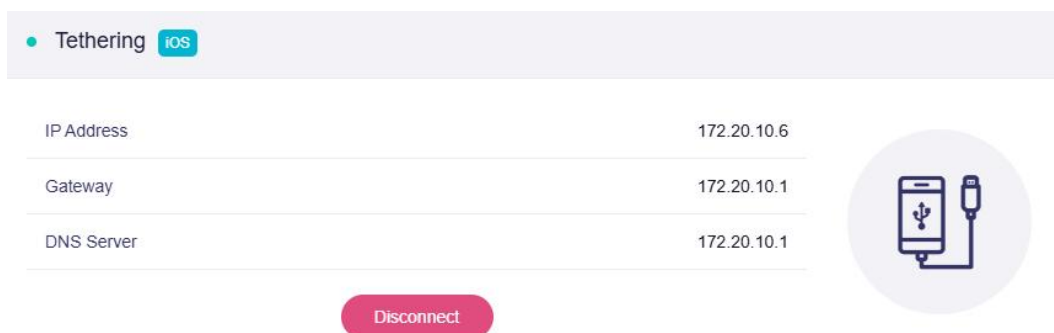
3. Connect a computer or another phone to the router. Log in to the router's web admin panel and navigate to **INTERNET > Tethering**, then click **Connect**.



4. It will start connecting.

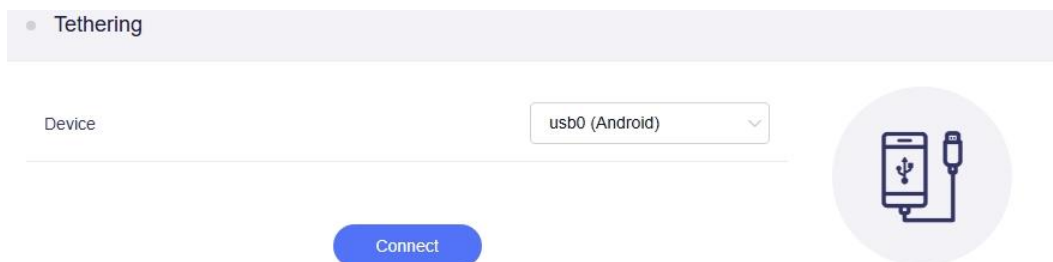


Once connected, this page will display the Tethering connection details.

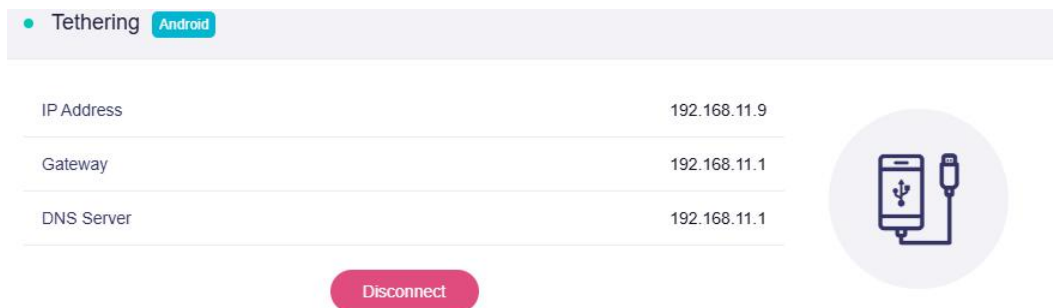


4.3.2 Android Tethering

1. Connect an Android phone to the router's USB port using a USB cable. A system dialog may appear asking USB preferences. Select **USB Tethering** or **File Transfer** if prompted.
2. Go to your phone's **Settings > Network & Internet > Personal Hotspot**. Enable **Personal Hotspot** or **USB Tethering**.
(The steps to enable USB Tethering vary by brand. Check your device's settings for the exact location, and contact your manufacturer's support if needed.)
3. Connect a computer or another phone to the router, then log in to the router's web admin panel, navigate to **INTERNET > Tethering**. Click **Connect**.



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



4.3.3 Troubleshooting

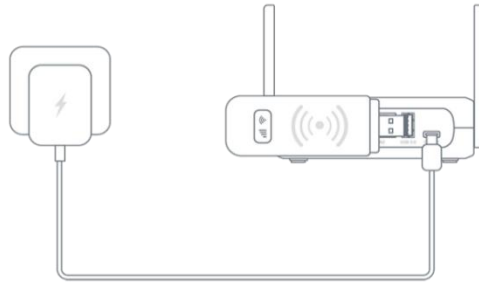
If the Tethering connection fails, try these troubleshooting steps:

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

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

4.4 Connect to the Internet via USB Modem

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



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

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

Tethering

Device

eth2

Connect



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

Tethering

IP Address	192.168.1.120
Gateway	192.168.1.1
DNS Server	192.168.1.1 , 192.168.1.1

Disconnect



Tip: After initial setup, if you restart the router with the USB modem still connected, or re-insert the modem into the router, the USB modem will be automatically recognized, and a network connection will establish without re-clicking "Connect".

Chapter 5

Wireless

This chapter guides you to check and configure wireless settings.

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

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

5.1 5 GHz Wi-Fi

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

● 5GHz WiFi

● 5GHz Guest WiFi

Enable Wi-Fi

ON

TX Power

Max

Wi-Fi Name (SSID)

GL-A1300-90f-5G

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Wi-Fi Mode

11a/n/ac

Bandwidth

80 MHz

Channel

Auto

Modify

Note:

1. The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.
2. When **Channel** is set to **Auto**, the router's Wi-Fi will not automatically switch to the DFS channel.

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

● 5GHz WiFi

● 5GHz Guest WiFi

Enable Wi-Fi

OFF

Wi-Fi Name (SSID)

GL-A1300-90f-5G-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

5.2 2.4 GHz Wi-Fi

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

● 2.4GHz WiFi

● 2.4GHz Guest WiFi

Enable Wi-Fi

ON

TX Power

Max

Wi-Fi Name (SSID)

GL-A1300-90f

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Wi-Fi Mode

11g/n

Bandwidth

20/40 MHz

Channel

11

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

● 2.4GHz WiFi

● 2.4GHz Guest WiFi

Enable Wi-Fi

OFF

Wi-Fi Name (SSID)

GL-A1300-90f-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

.....

SSID Visibility

Shown

Note: The **Bandwidth** and **Channel** cannot be modified when the router is configured as a repeater, as they follow that of the repeated network.

Chapter 6

Clients

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

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

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

Clients Access Control: Blocklist ⓘ						Sort by default ⚙
Online Clients (2) ^						
Name	IP + MAC	Speed ⓘ	Traffic	Block	Action	
 PC Self	 192.168.18.216 80:CA:52:XX:XX:XX	↓ 825.00 B/s ↑ 1004.00 B/s	↓ 46.53 MB ↑ 6.82 MB	☐	...	
 iPhone	 192.168.18.218 96:9E:E2:XX:XX:XX ⓘ	↓ 5.94 KB/s ↑ 240.00 B/s	↓ 1.09 MB ↑ 68.99 KB	☐	...	
Offline Clients (1) ^						
Name	IP + MAC	Speed	Traffic	Block	Action	
 LAPTOP-O15BJHA8	 192.168.8.138 80:CA:52:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 401.10 KB ↑ 311.97 KB	☐	...	

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

6.1 Device Details

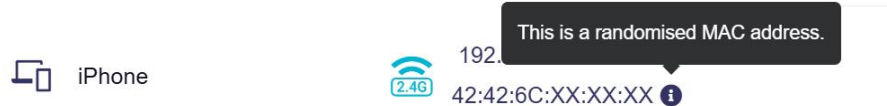
Clients Access Control: Blocklist ⓘ Sort by default ⚙					
Online Clients (2) ^					
Name	IP + MAC	Speed ⓘ	Traffic	Block	Action
 PC Self	 192.168.18.216 80:CA:52:XX:XX:XX	↓ 825.00 B/s ↑ 1004.00 B/s	↓ 46.53 MB ↑ 6.82 MB	☐	...
 iPhone	 192.168.18.218 96:9E:E2:XX:XX:XX ⓘ	↓ 5.94 KB/s ↑ 240.00 B/s	↓ 1.09 MB ↑ 68.99 KB	☐	...

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. Blocklist

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

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

Clients

Access Control: Blocklist

Sort by default

Online Clients (2)					
Name	IP + MAC	Speed	Traffic	Block	Action
PC	192.168.18.216 80:CA:52:XX:XX:XX	↓ 825.00 B/s ↑ 1004.00 B/s	↓ 46.53 MB ↑ 6.82 MB	☐	...
iPhone	192.168.18.218 96:9E:E2:XX:XX:XX	↓ 5.94 KB/s ↑ 240.00 B/s	↓ 1.09 MB ↑ 68.99 KB	☐	...

Access Control

Mode

Blocklist

Blocklist

Self MAC

1

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

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

6.2 Action

1. 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.

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

Online Clients (2) ▲

Name	IP + MAC	Speed !	Traffic	Block	Action
 PC Self	 192.168.18.216 80:CA:52:XX:XX:XX	↓ 1.88 KB/s ↑ 1.10 KB/s	↓ 46.87 MB ↑ 7.02 MB	☐	⋮ Modify Limit Speed
 iPhone	 192.168.18.218 96:9E:E2:XX:XX:XX !	↓ 101.00 B/s ↑ 45.00 B/s	↓ 1.11 MB ↑ 79.23 KB	☐	

Modify Client Device

Name

Auto

Device Type

Optional ▲

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

Cancel

2. Limit Speed

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

The screenshot shows the 'Clients' interface with a table of online clients. The 'Action' column for the 'iPhone' client has a dropdown menu open, with 'Limit Speed' highlighted in a red box.

Name	IP + MAC	Speed	Traffic	Block	Action
PC	192.168.18.216 80:CA:52:XX:XX:XX	↓ 1.91 KB/s ↑ 1012.00 B/s	↓ 46.89 MB ↑ 7.03 MB	☐	...
iPhone	192.168.18.218 96:9E:E2:XX:XX:XX	↓ 146.00 B/s ↑ 64.00 B/s	↓ 1.12 MB ↑ 82.72 KB	☐	Modify Limit Speed

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

Limit Speed Settings

↓ Download KB/s

↑ Upload KB/s

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

Name	IP + MAC	Speed	Traffic	Block	Action
PC	192.168.18.216 80:CA:52:XX:XX:XX	↓ 1.24 KB/s ↑ 1.08 KB/s	↓ 46.94 MB ↑ 7.13 MB	☐	...
iPhone	192.168.18.218 96:9E:E2:XX:XX:XX	↓ 140.00 B/s ↑ 54.00 B/s	↓ 1.12 MB ↑ 82.72 KB	☐	...

6.3 Remove Clients

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

Offline Clients (2)

Delete All

Name	IP + MAC	Speed	Traffic	Block	Action
LAPTOP-O15BJHA8	192.168.8.138 80:CA:52:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 401.10 KB ↑ 311.97 KB		...
iPhone	192.168.18.218 96:9E:E2:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 1.12 MB ↑ 82.72 KB		...

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

Offline Clients (2)

Delete All

Name	IP + MAC	Speed	Traffic	Block	Action
LAPTOP-O15BJHA8	192.168.8.138 80:CA:52:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 401.10 KB ↑ 311.97 KB		...
iPhone	192.168.18.218 96:9E:E2:XX:XX:XX	↓ 0.00 B/s ↑ 0.00 B/s	↓ 1.12 MB ↑ 82.72 KB		Modify Limit Speed Remove Client

6.4 Sort

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

The screenshot shows the 'Clients' page with the 'Access Control: Blocklist' tab selected. A red arrow points to the 'Sort by default' dropdown menu in the top right corner. The menu is open, showing options: 'Default', 'Name', 'IP', 'Upload Speed', 'Download Speed', 'Clear Traffic Statistics', and 'Toggle Rate Unit'. Below the menu, a table lists online clients.

Name	IP + MAC	Speed	Traffic	Block
PC-20260821AATR Self	192.168.8.216 80:CA:52:XX:XX:XX	↓ 2.02 Kbps ↑ 816.00 bps	↓ 996.88 MB ↑ 154.11 MB	☐
iPhone	192.168.8.218 96:9E:E2:XX:XX:XX	↓ 7.62 Kbps ↑ 2.42 Kbps	↓ 45.64 KB ↑ 17.90 KB	☐

The default sorting order is as follows:

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

In addition to sorting rules, the dropdown menu also provides the following functions:

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

Name	IP + MAC	Speed	Traffic
PC-20260821AATR Self	192.168.8.216 80:CA:52:XX:XX:XX	↓ 3.18 Kbps ↑ 4.94 Kbps	↓ 0.00 B ↑ 0.00 B

- **Toggle Rate Unit:** Switch the rate unit for the speed column between **KB/s** and **Kbps**.

Chapter 7

Get To Know VPN

This chapter introduces VPN concepts and common use scenarios.

7.1 Introduction

VPN

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

VPN Router

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

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

OpenVPN

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

WireGuard

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

7.2 Application Scenarios

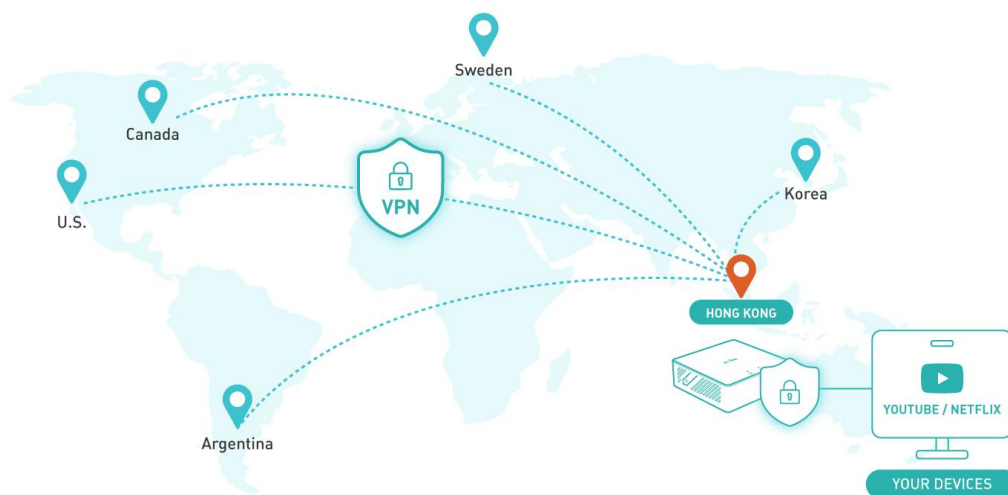
1. Personal Data Privacy

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



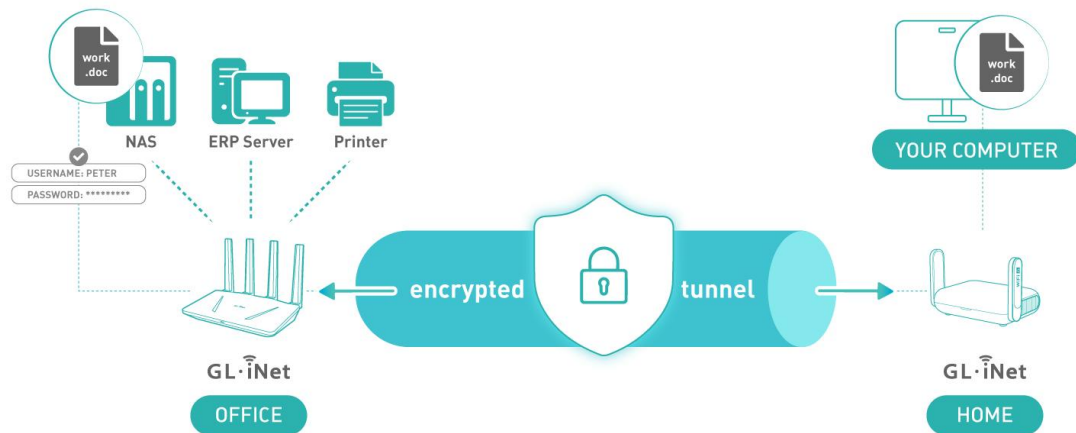
2. Unrestricted Access Worldwide

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



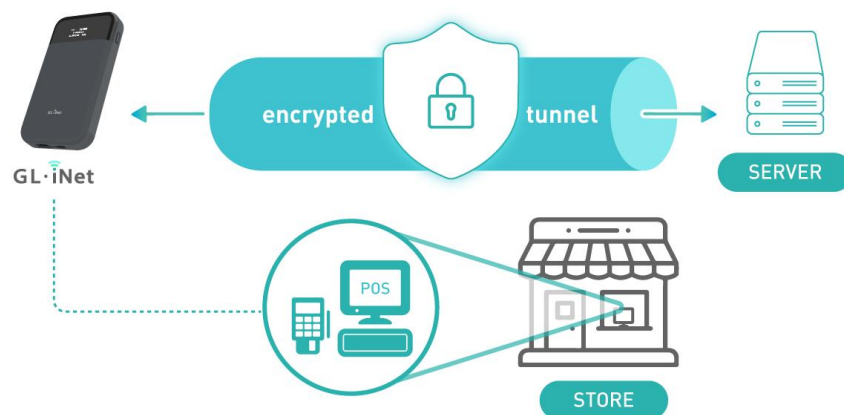
3. Small Business Data Security

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



4. Secure Payment Infrastructure

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



Chapter 8

VPN Dashboard

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

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

When the router is set as an active VPN client, the VPN dashboard displays VPN connection details, such as server address, traffic statistics, client virtual IP, and connection log. It also allows you to configure advanced settings such as the Block non-VPN traffic, Allow Access WAN, and Services from GL.iNet Use VPN.

8.1 VPN Client

When you enter the **VPN Dashboard** for the first time and no OpenVPN or WireGuard configuration files are available, the page displays as follows. Click **Set Up Now** and you will be directed to the **OpenVPN Client** or **WireGuard Client** page to upload your VPN configuration files.

VPN Client Global Options

Global Proxy

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

Type	Options
☐ OpenVPN	Set Up Now
☐ WireGuard	Set Up Now

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

VPN Client Global Options

Global Proxy

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

Type	Configuration File	Enable	Options
☐ OpenVPN	FR-ovpn-udp		
☐ WireGuard	au-v4.hideservers.net		

8.1.1 Client Options

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

VPN Client

Global Options

Global Proxy

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

Type	Configuration File	Enable	Options
☐ OpenVPN	FR-ovpn-udp	☐	
☐ WireGuard	au-v4.hideservers.net	☐	

The OpenVPN Client Options displays as follows.

OpenVPN Client Options

Remote Access LAN

☐

IP Masquerading

☒

MTU

Optional

Cancel

Apply

The WireGuard Client Options displays as follows.

WireGuard Client Options

Remote Access LAN

☐

IP Masquerading

☒

MTU

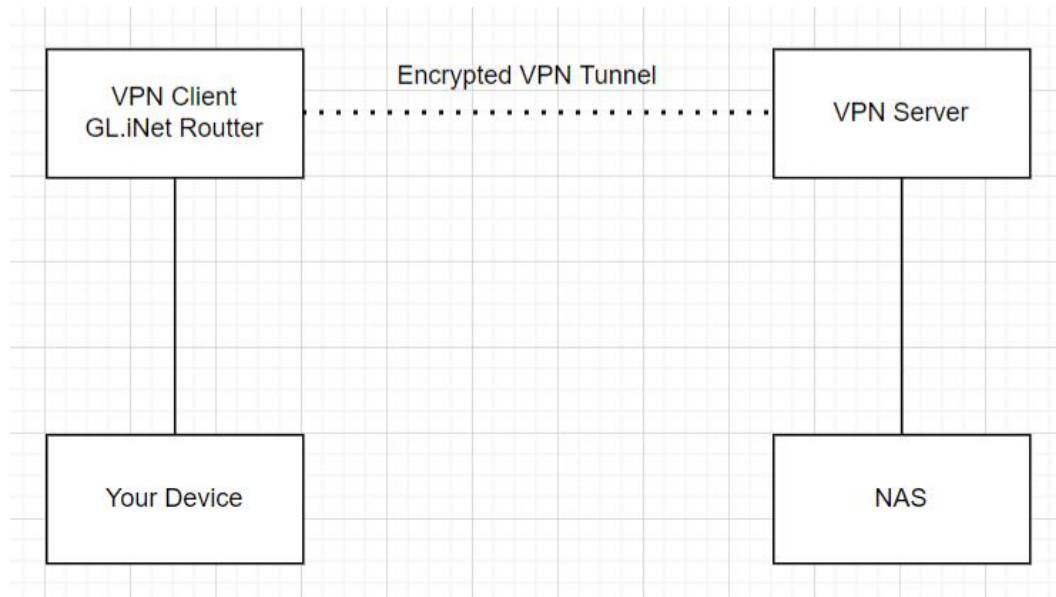
Optional

Cancel

Apply

- **Remote Access LAN:** If enabled, remote access to this router and its LAN devices via VPN will be allowed. The VPN server must advertise a route to the LAN subnet of this router.

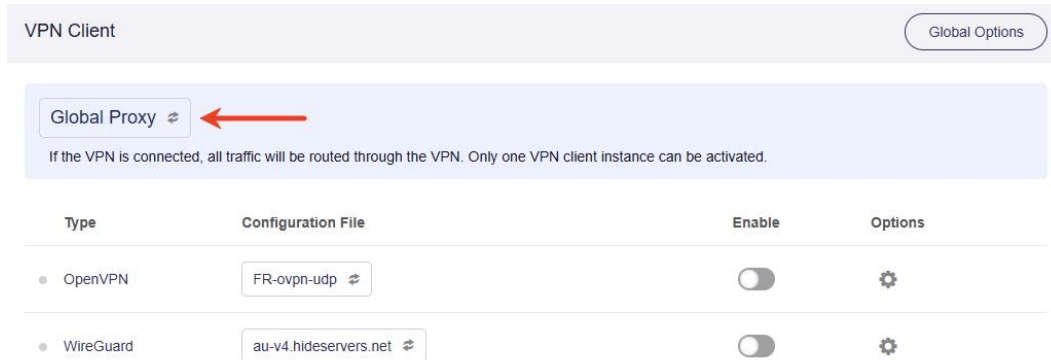
For example, as shown in the diagram below, the GL.iNet router runs as a VPN client and connects to a VPN server over the VPN tunnel. When this option is enabled, both the GL.iNet router and its LAN-side devices can be accessed by devices on the VPN server side (e.g. NAS). This requires you to add a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



- **IP Masquerading:** If enabled, the source IP addresses of LAN clients will be rewritten to the router's VPN tunnel IP. Disable this only for Site-to-Site setups where the remote peer knows your LAN subnets.
- **MTU:** Short for Maximum Transmission Unit. This optional setting lets you customize the VPN tunnel MTU, which overrides the value defined in the configuration file.

8.1.2 Policy Mode

The default proxy mode for VPN connection is **Global Proxy**. You can click the box in the upper right to switch to other proxy modes.



The screenshot shows the 'VPN Client' interface. At the top right is a 'Global Options' button. Below it, a light blue box contains the 'Global Proxy' mode, which is selected and highlighted with a red arrow. Below this box is a note: 'If the VPN is connected, all traffic will be routed through the VPN. Only one VPN client instance can be activated.' Below the note is a table with columns: Type, Configuration File, Enable, and Options.

Type	Configuration File	Enable	Options
• OpenVPN	FR-ovpn-udp	☐	
• WireGuard	au-v4.hideservers.net	☐	

Three proxy modes are available: Global Proxy, Policy Mode and Route Mode.

1. Global Proxy

In this mode, all traffic will be routed through the VPN. Only one VPN client instance can be activated.

2. Policy Mode

This mode can be further divided into three policies.

- **Based on the Target Domain or IP**

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

- **Based on the Client Device**

In this mode, only the traffic of certain LAN devices identified by MAC addresses will be routed through VPN. Only one VPN client instance can be activated.

- **Based on the VLAN**

In this mode, only the traffic of certain VLAN will be routed through VPN. Only one VPN client instance can be activated.

3. Route Mode

- **Auto Detect**

The routing rules defined in each VPN client configuration file or issued by the VPN server will be used.

- **Customize Routing Rules**

You can manually configure routing rules for each VPN client instance.

8.1.3 Global Options

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

The screenshot shows the 'VPN Client' configuration page. At the top right, there is a 'Global Options' button with a red arrow pointing to it. Below this, a 'Global Proxy' section contains a note: 'If the VPN is connected, all traffic will be routed through the VPN. Only one VPN client instance can be activated.' Below the note is a table with columns: Type, Configuration File, Enable, and Options.

Type	Configuration File	Enable	Options
• OpenVPN	FR-ovpn-udp	☐	
• WireGuard	au-v4.hideservers.net	☐	

Below the table is the 'Global Options' section with three toggle switches, all currently turned off:

- Block Non-VPN Traffic
- Allow Access WAN
- Services from GL.iNet Use VPN

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

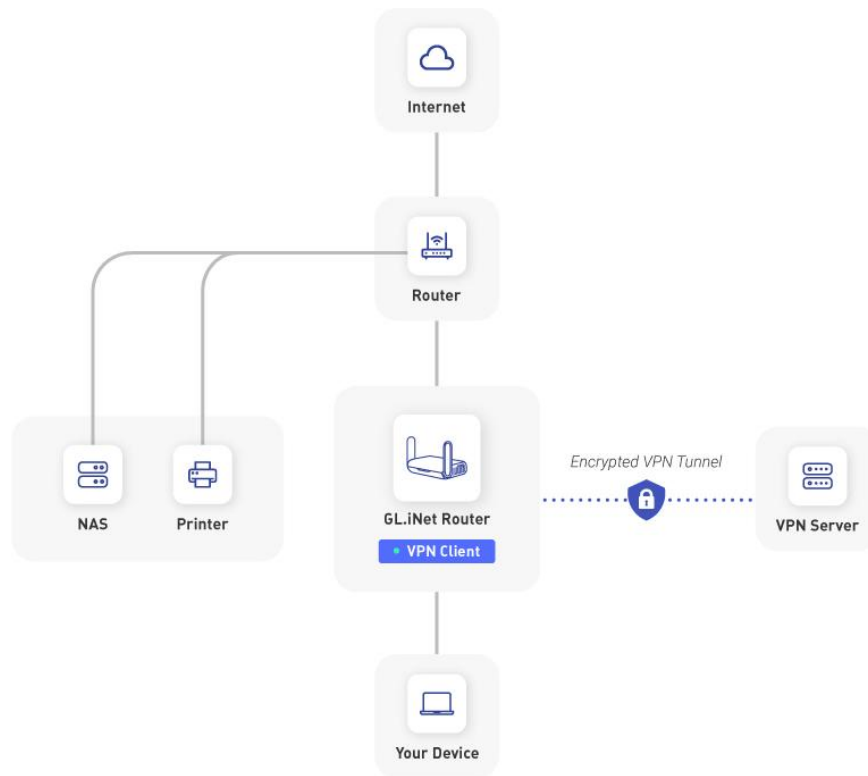
- **Block Non-VPN Traffic:** If enabled, all internet traffic is forced to pass exclusively through the VPN tunnel and cannot be routed via other interfaces such as the local ISP WAN. If the VPN connection drops unexpectedly, all internet traffic is fully blocked to prevent fallback to the regular WAN. This avoids VPN leaks caused by VPN failures, incorrect client DNS settings, and similar issues.

This feature is also known as [VPN Kill Switch](#). It prevents user data from being exposed online. A typical Kill Switch automatically cuts off internet access when the VPN connection fails. The Block Non-VPN Traffic feature on GL.iNet routers provides broader leak protection and covers the following scenarios:

- DNS Leak
- IPv6 Leak
- WebRTC Leak
- VPN Connection Drop

- e. Applications Launched Before VPN Establishment
- f. Per-Application Traffic Leaks

- **Allow Access WAN:** If enabled, local client devices can still access WAN-side services (e.g., printers, NAS and other devices in the upstream subnet) while the VPN is active.



As shown in the diagram above, enabling this feature allows your local devices to reach hosts on the upstream subnet, such as printers and NAS.

This option is primarily designed to let clients access devices within the upstream subnet. However, the router cannot distinguish upstream subnet traffic from regular Internet traffic. If client devices access resources directly via public IPs, there is a potential traffic leakage risk. For this reason, **Allow Access WAN** and **Block Non-VPN Traffic** are mutually exclusive and cannot be enabled simultaneously.

- **Services From GL.iNet Use VPN:** If enabled, GoodCloud, DDNS, and rty services will transmit packets through VPN tunnels. This option is disabled by default, as these services normally require the device's real IP address to work properly.

8.2 VPN Server

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

VPN Server		Global Options
Type	Options	
☐ OpenVPN		Set Up Now
☐ WireGuard		Set Up Now

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

VPN Server

Global Options

Type	Tunnel Address	Enable	Options
OpenVPN	10.8.0.0		
0.00 B / 3.33 KB			View Log
WireGuard	10.0.0.1/24		
0.00 B / 0.00 B		No Clients	View Log

8.2.1 Server Options

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

VPN Server				Global Options
Type	Tunnel Address	Enable	Options	
• OpenVPN	10.8.0.0	☐		 
• WireGuard	10.0.0.1/24	☐		 

The OpenVPN Server Options displays as follows.

OpenVPN Server Options

Remote Access LAN ⓘ

☐

IP Masquerading ⓘ

☒

MTU ⓘ

Cancel

Apply

The WireGuard Server Options displays as follows.

WireGuard Server Options

Remote Access LAN ⓘ

☐

IP Masquerading ⓘ

☒

MTU ⓘ

Client to Client ⓘ

☐

Cancel

Apply

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

- **MTU:** Short for Maximum Transmission Unit. The MTU value you set for the tunnel will override the MTU settings in the configuration file.
- **Client to Client:** If enabled, VPN clients connected to this server can access each other via their VPN tunnel IPs. If you want to allow clients to also access one another's LAN subnets, you need to add routing rules on the VPN server to advertise those remote LAN subnets.

8.2.2 Server Route Rule

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

VPN Server				Global Options
Type	Tunnel Address	Enable	Options	
● OpenVPN	10.8.0.0	☐	 	
● WireGuard	10.0.0.1/24	☐	 	

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

OpenVPN Server Route Rule ×

IPv4

 In customize routes mode, the VPN client will ignore the configuration file and the routing configuration issued by the server. Whether the encrypted tunnel provided by the VPN is used when accessing any network segment will be determined by the routing rules you set manually.

[+Add Route Rule](#)

Target Address	Gateway	Metric	MTU	Scope	Action
e.g. 10.8.0.0/24	e.g. 10.8.0.1 (Optional)	Optional	Optional	Optional	 

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

WireGuard Server Route Rule ×

IPv4

 In customize routes mode, the VPN client will ignore the configuration file and the routing configuration issued by the server. Whether to use the VPN encrypted tunnel when accessing any network segment is determined by the routing rules you manually set.

[+Add Route Rule](#)

Target Address	Gateway	Metric	MTU	Scope	Action
e.g. 10.8.0.0/24	e.g. 10.8.0.1 (Optional)	Optional	Optional	Optional	 

Note: In customize routes mode, the VPN client will ignore the configuration file and the routing configuration issued by the server. Whether to use the VPN encrypted tunnel when accessing any network segment is determined by the routing rules you manually set.

8.2.3 Global Options

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

VPN Server

Global Options

Type	Tunnel Address	Enable	Options
● OpenVPN	10.8.0.0	☐	 
● WireGuard	10.0.0.1/24	☐	 

Global Options

Enable VPN Cascading 

☐

Cancel

Apply

If **VPN Cascading** is enabled, when this router acts as a VPN server and a VPN client simultaneously, remote VPN clients connected to this router's VPN server will have their traffic routed through the upstream VPN tunnel that this router is using as a VPN client. [Learn more about VPN Cascading.](#)

Chapter 9

Set Up VPN Server

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

9.1 Set Up OpenVPN Server

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

9.1.1 Preparation

1. Make sure you have a public IP address

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

Alternative methods:

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

2. Confirm if Port Forwarding is required

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

9.1.2 Setup Steps

1. Log in to the router's web admin panel, navigate to **VPN > OpenVPN Server**, then click **Generate Configuration** (for VPN server initial setup only).

2. Apply the configuration.

The default configuration works for most cases. Click **Export Client Configuration** at the bottom and proceed to step 3. If you have modified the configuration, click **Apply** before exporting it.

Configuration

Users

Device Mode

TUN

Protocol

UDP

Local Port

1194

IPv4 Subnet

10.8.0.0

IPv4 Netmask

255.255.255.0

Authentication Mode ⓘ

Certificate only

ⓘ Advanced Configuration

Export Client Configuration

- **Device Mode:** TAP-S2S or Tun. See [here](#) for the differences.
- **Protocol:** UDP or TCP. See [here](#) for the differences.
- **Authentication Mode:** This determines the authentication method used when the client connects to the server. There are three options:
 - **Certificate Only:** If selected, the router will automatically generate a server and client certificate keys and embed them in the configuration file. When you upload the configuration to the client, no additional credentials are required.

- **Username/Password Only:** If selected, the router will generate client configuration without certificate keys. You need to first add a username and password in the **Users** tab before exporting the client configuration. When uploading the configuration to the client, enter these credentials for authentication.
 - **Username/Password and Certificate:** If selected, you need to first add a username and password in the **Users** tab before exporting the client configuration; second, the router will automatically generate server and client certificate keys and embed them in the configuration file. When uploading the configuration to the client, the certificate-key will be verified first, followed by username/password authentication for 2FA security.
 - **Advanced Configuration:** Customize more server settings if needed.
3. Export Client Configuration.
- After clicking **Export Client Configuration** at the bottom of the Configuration tab (or applying the modified configuration), a window will pop up as follows. Click **Download** to export the configuration.

Export Client Configuration

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

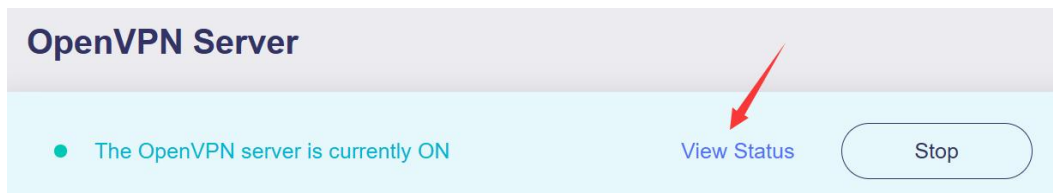
Use DDNS Domain

Download

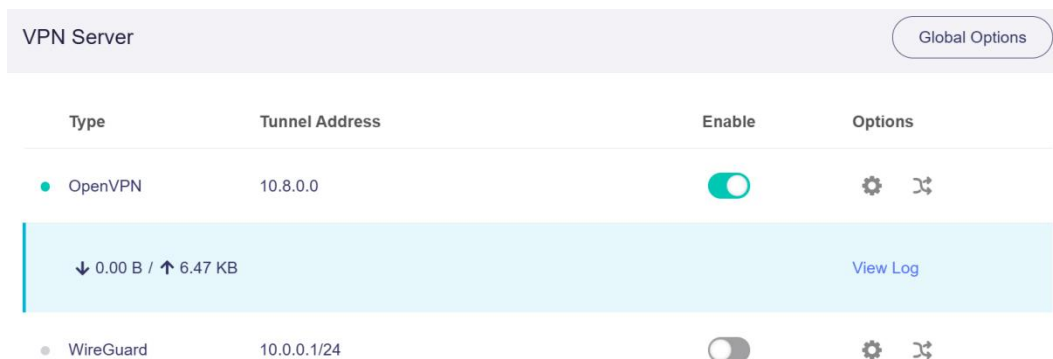
- Tip:** If your public IP address changes frequently, go to **APPLICATIONS > Dynamic DNS** and enable DDNS. You can then use the DDNS domain as your server address.
4. Start OpenVPN server.
- On the **OpenVPN Server** page, click the **Start** button in the upper right corner to start the server.



If you want to view the server connection status, click **View Status**.



You will be redirected to the VPN Dashboard. If the upload and download traffic statistics are displayed in this page, the OpenVPN server is running.



9.1.3 Troubleshooting

If the connection fails, there are several common reasons:

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

9.2 Set Up WireGuard Server

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

9.2.1 Preparation

1. Make sure you have a public IP address

Click [here](#) to verify if your Internet Service Provider assigns you a public IP address.

If not, your router cannot be set as a WireGuard Server.

Alternative methods:

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

2. Confirm if Port Forwarding is required

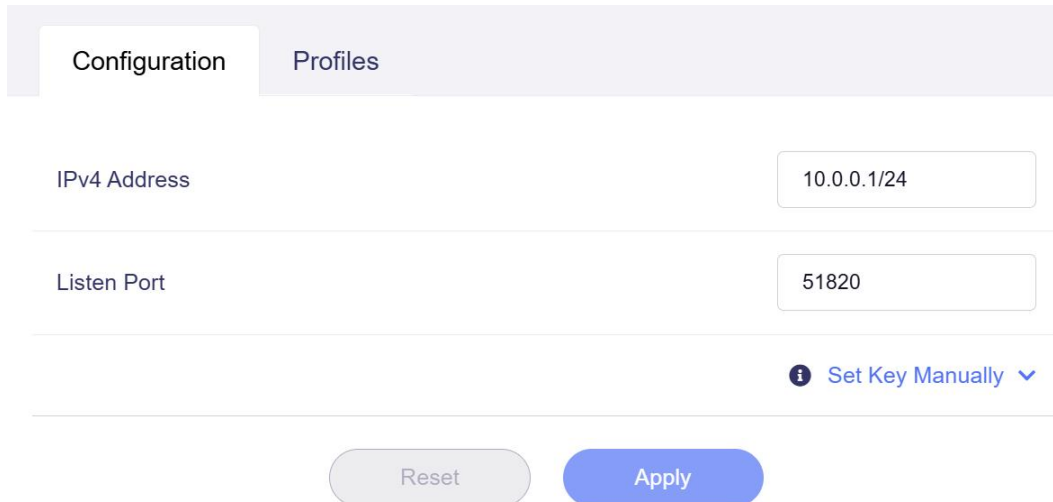
- If your GL.iNet router is the primary router in your network, no port forwarding setup is required. Proceed to the next step.
- If a primary router is already in use and your GL.iNet router is configured as a secondary router, you will need to configure port forwarding on the primary router.
- If your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

9.2.2 Setup Steps

1. Log in to the router's web admin panel, navigate to **VPN > WireGuard Server**, then click **Generate Configuration** (for VPN server initial setup only).

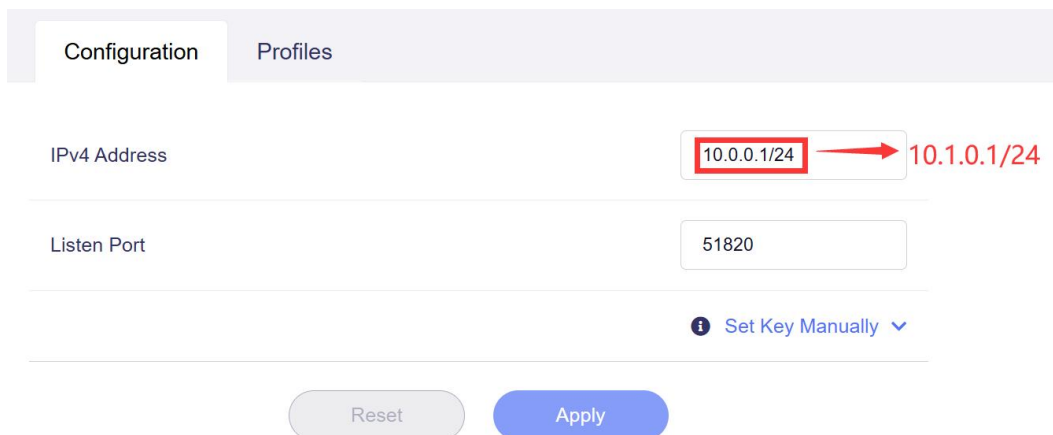
2. Apply the configuration.

The default configuration works for most cases. No need to modify the IPv4 address unless it conflicts with your upstream router's gateway.



The screenshot shows the 'Configuration' tab of the WireGuard Server setup. It features two input fields: 'IPv4 Address' with the value '10.0.0.1/24' and 'Listen Port' with the value '51820'. Below these fields is a link 'Set Key Manually' with an information icon and a dropdown arrow. At the bottom are two buttons: 'Reset' and 'Apply'.

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



This screenshot is similar to the previous one but shows a modification to the 'IPv4 Address' field. The original value '10.0.0.1/24' is highlighted with a red box, and a red arrow points to the new value '10.1.0.1/24'. The 'Listen Port' remains '51820'. The 'Set Key Manually' link and 'Reset'/'Apply' buttons are also present.

3. Add a profile.

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

The screenshot shows the 'WireGuard Server' interface. At the top, there's a status indicator: 'The WireGuard server is currently OFF' with a 'Start' button. Below this, there are two tabs: 'Configuration' and 'Profiles'. The 'Profiles' tab is selected and highlighted with a red box. Under the 'Profiles' tab, there is an information icon and a text block stating: 'Each client device that connects to the WireGuard server requires a unique peer configuration. You need to create a separate configuration for each client device; each configuration must specify a unique client IP.' To the right of this text is a blue button with a white plus sign and the text '+ Add', which is also highlighted with a red box.

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

The screenshot shows the 'Client Configuration' form. It has a header 'Client Configuration'. Below it, there is a 'Name' label followed by an empty text input field. To the right of the input field is a blue link that says 'Set More'. At the bottom of the form, there are two buttons: a 'Cancel' button and an 'Apply' button.

4. Download configuration.

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

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

WireGuard® Client Configuration

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

Use DDNS Domain ☐

QR Code [Configuration File](#)

```
[Interface]
Address = 10.0.0.3/24
PrivateKey = 
DNS = 64.6.64.6
MTU = 1420

[Peer]
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = 183.178.54.242:51820
PersistentKeepalive = 25
PublicKey = 
```

Download

Tip: 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.

5. Start WireGuard server.

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

WireGuard Server

The WireGuard server is currently OFF

Start

If you want to view the server connection status, click **View Status**.

WireGuard Server

The WireGuard server is currently ON

View Status

Stop

You will be redirected to the VPN Dashboard. If the upload and download traffic statistics are displayed in this page, the OpenVPN server is running.

VPN Server				Global Options
Type	Tunnel Address	Enable	Options	
● OpenVPN	10.8.0.0	☐		
● WireGuard	10.0.0.1/24	☒		
↑ 0.00 B / ↓ 0.00 B		No Clients		View Log

9.2.3 Troubleshooting

If the connection fails, there are several common reasons:

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

Chapter 10

Set Up VPN Client

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

10.1 Set Up OpenVPN Client

10.1.1 Preparation

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

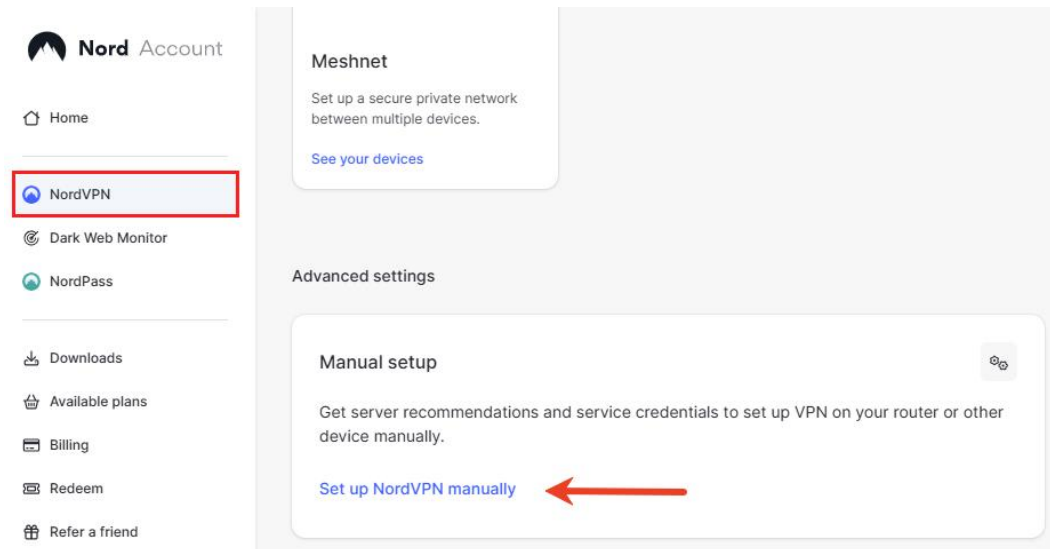
Next, visit the official website of the VPN service provider you subscribed and obtain service credentials or configuration file. If you don't know how to get the configuration file, refer to [this link](#) or contact their support.

10.1.2 Set Up NordVPN

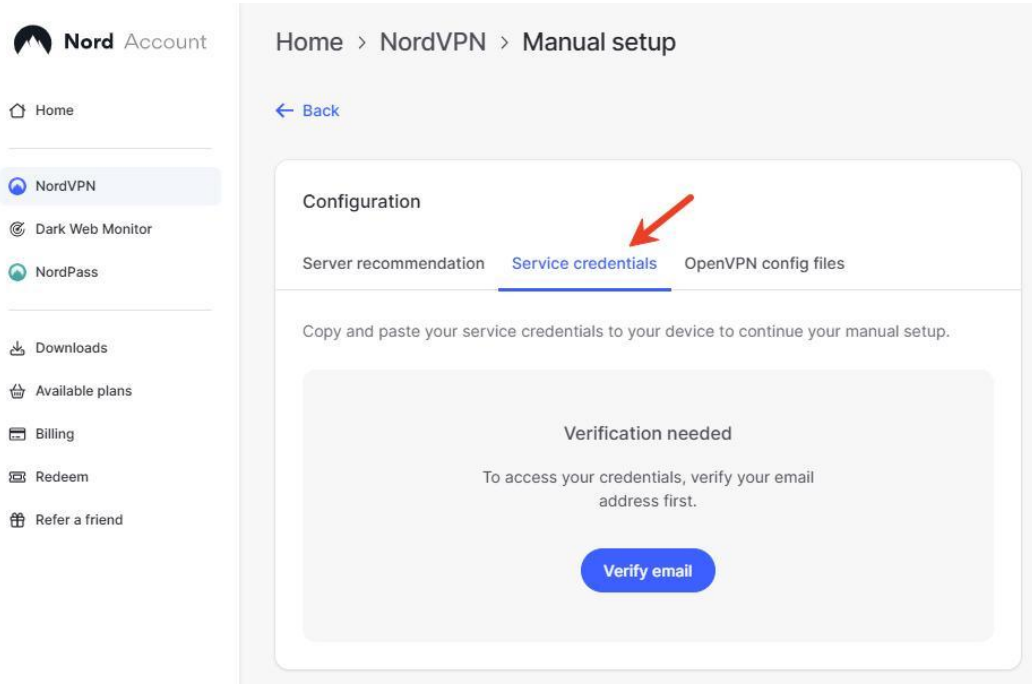
NordVPN is integrated into the GL.iNet web admin panel. You can acquire configuration files for all NordVPN servers by entering your account credentials (obtained from the NordVPN Dashboard) in the router's web admin panel or GL.iNet mobile app, eliminating the need for manual file uploads.

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

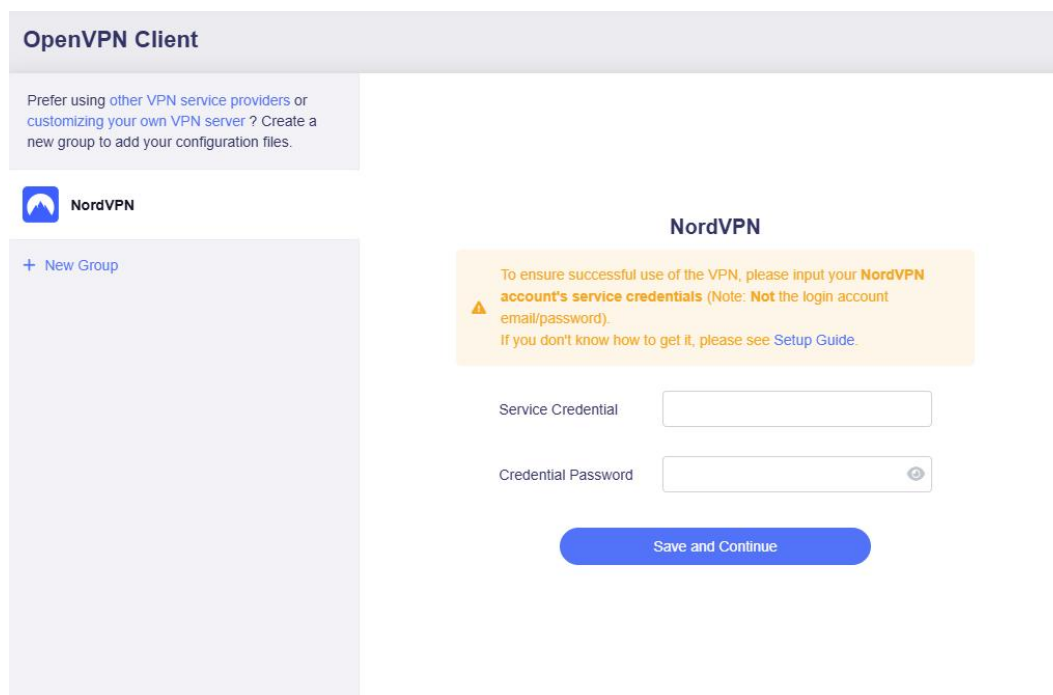
1. Log in to your NordVPN web account [here](#).
2. On the Nord Dashboard, click **NordVPN**, then click **Set up NordVPN manually**.



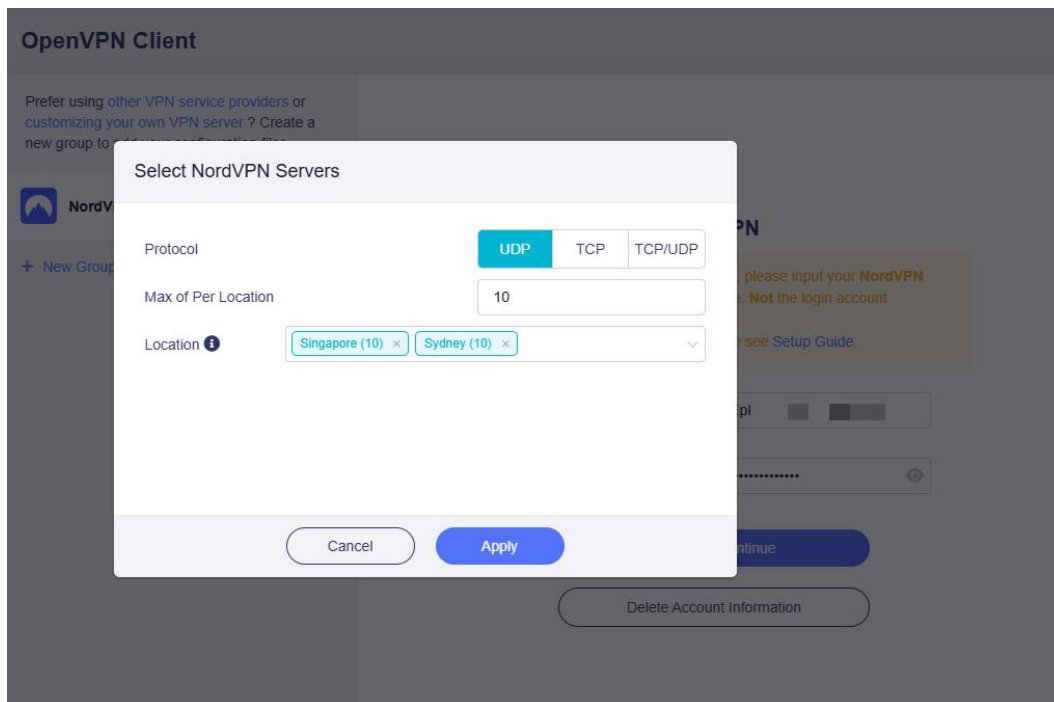
You will find the **service credentials**. Copy them for later use.



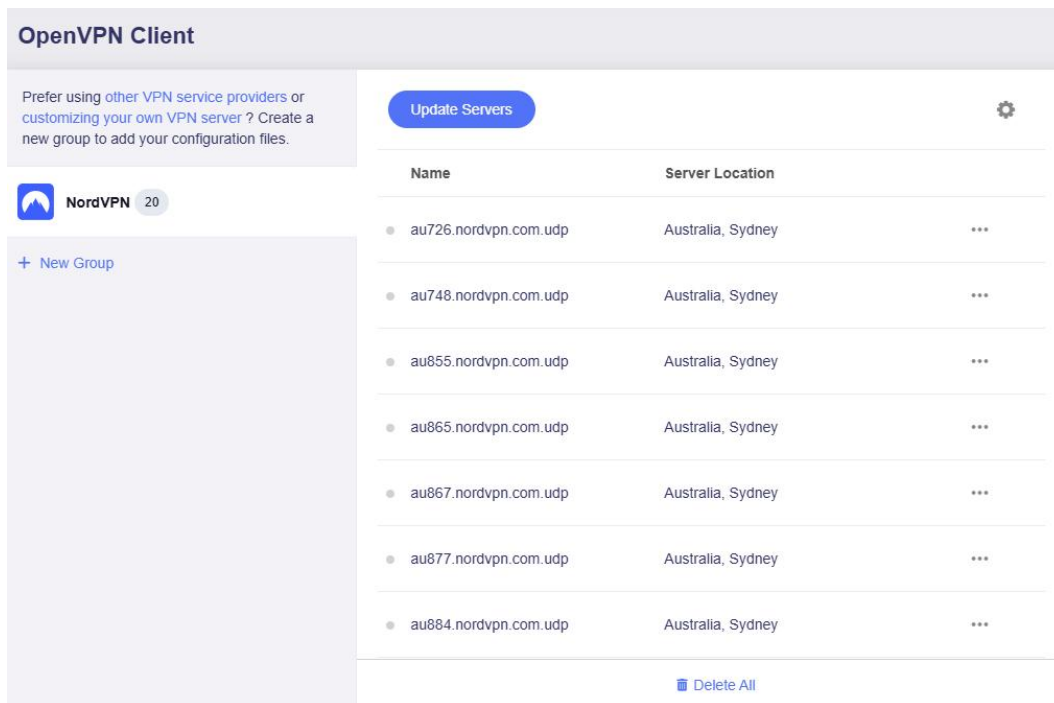
3. Log in to your router's web admin panel and navigate to **VPN > OpenVPN Client > NordVPN**. Input the service credentials (Note: It is NOT the login account email/password), then click **Save and Continue**.



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

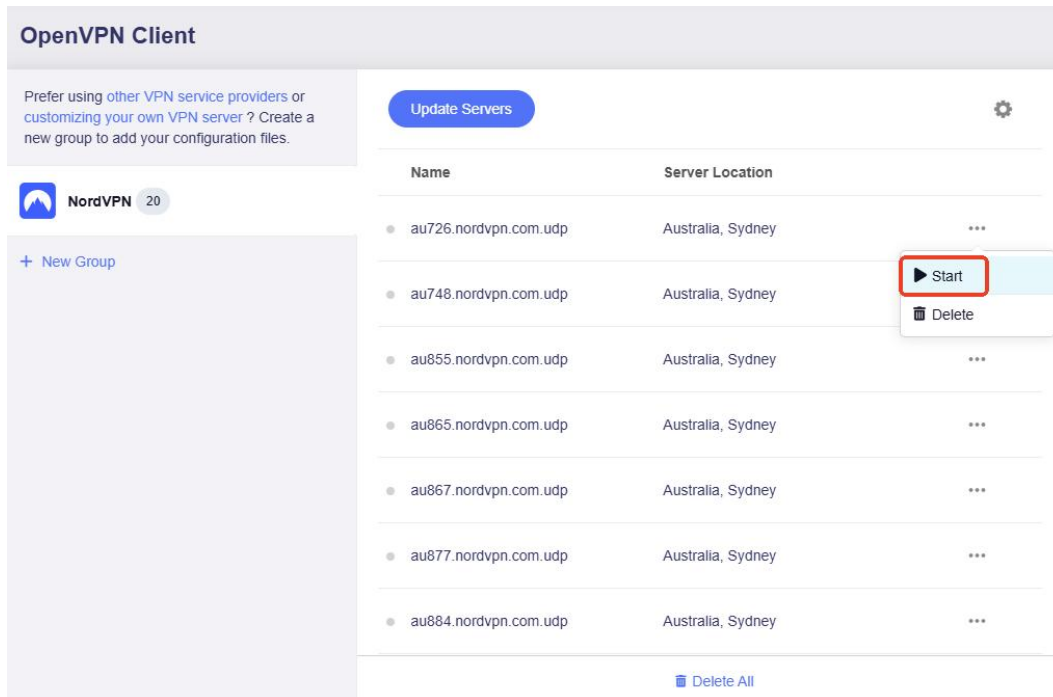


It will download configuration files.

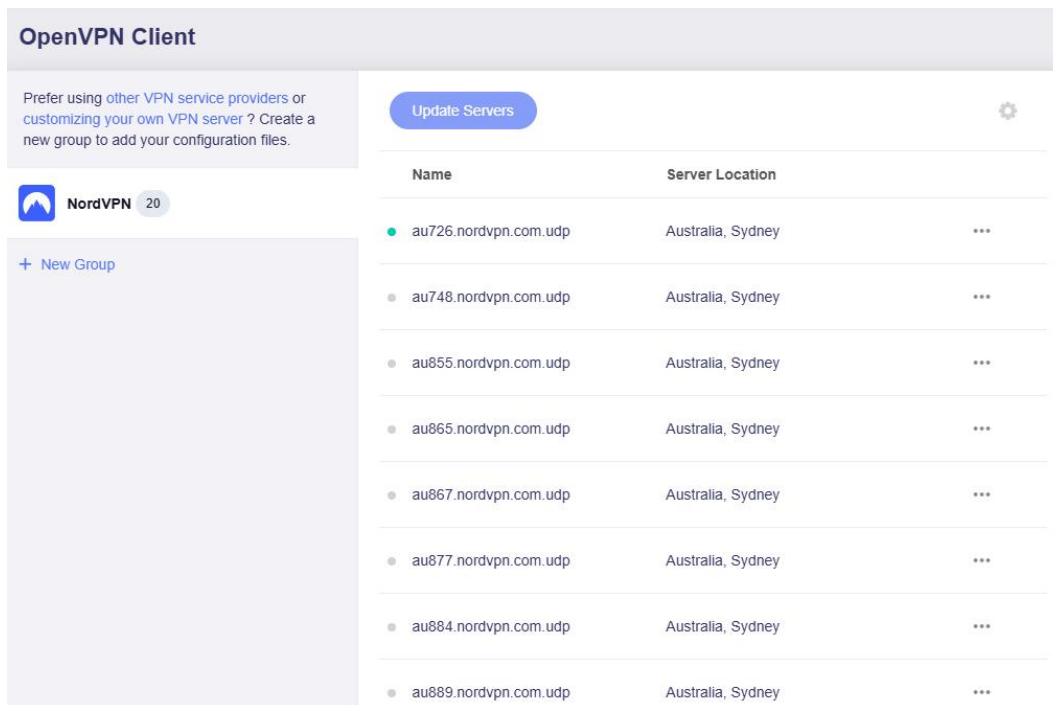


5. Start a connection.

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



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



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

- Update servers.

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

OpenVPN Client

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

NordVPN 20

+ New Group

Update Servers

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

[Delete All](#)

8. Edit credentials.

Click the gear icon to edit your login credentials.

OpenVPN Client

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

NordVPN 20

+ New Group

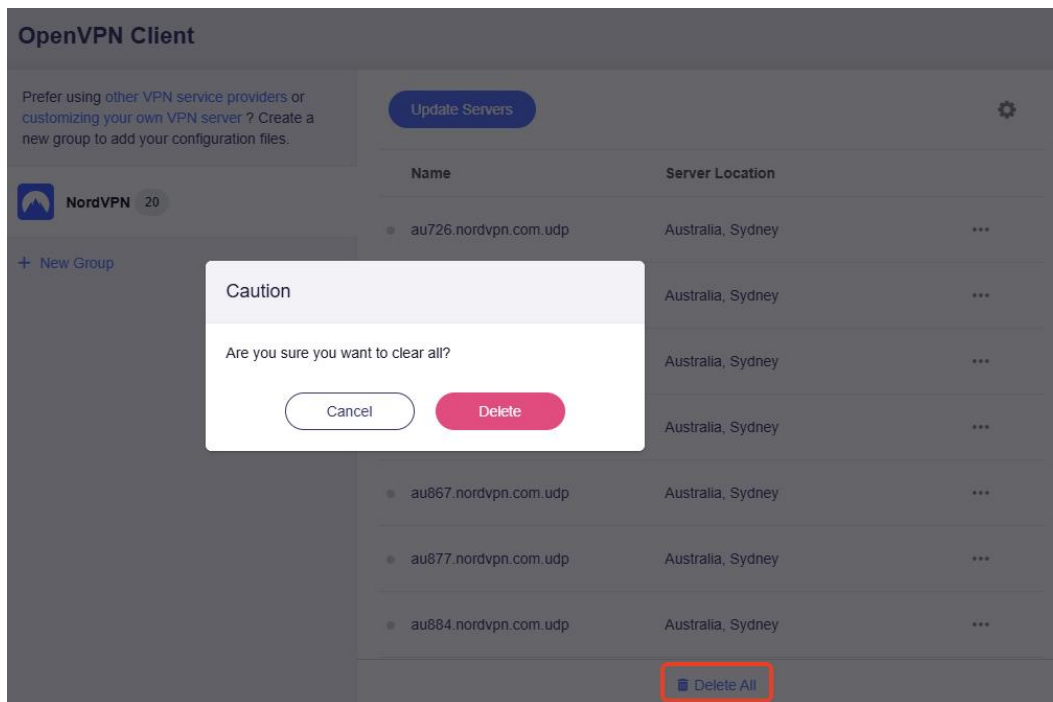
Update Servers

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

[Delete All](#)

9. Delete all files.

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

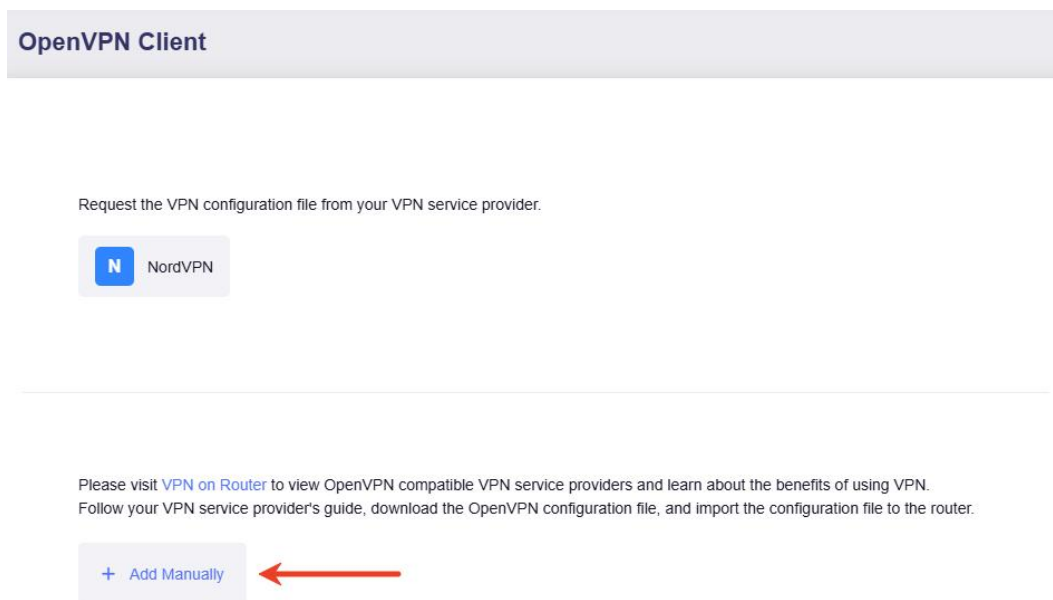


10.1.3 Set Up OpenVPN Client Manually (for other providers)

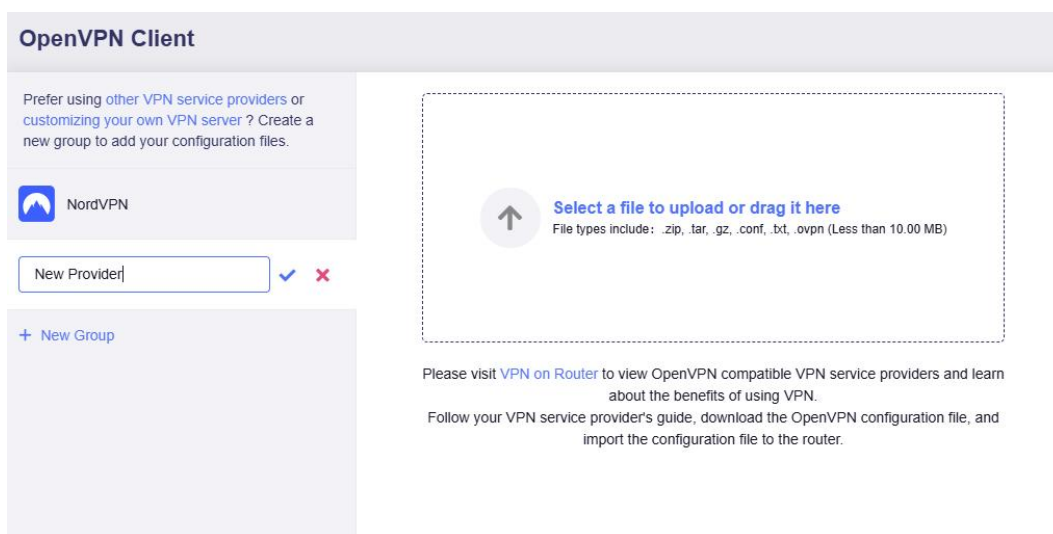
If your OpenVPN service provider is not integrated into our admin panel, please first visit the official website of your subscribed service provider to obtain the configuration file. Then upload it to the router to set up an OpenVPN client.

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

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



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



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

OpenVPN Client

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

NordVPN

Private Internet Access

+ New Group

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

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

Username

Password

Apply

You will see the configuration file uploaded.

OpenVPN Client

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

NordVPN

Private Internet Access 1

+ New Group

Upload Configuration File

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

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

OpenVPN Client

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

NordVPN

Private Internet Access 1

+ New Group

Upload Configuration File

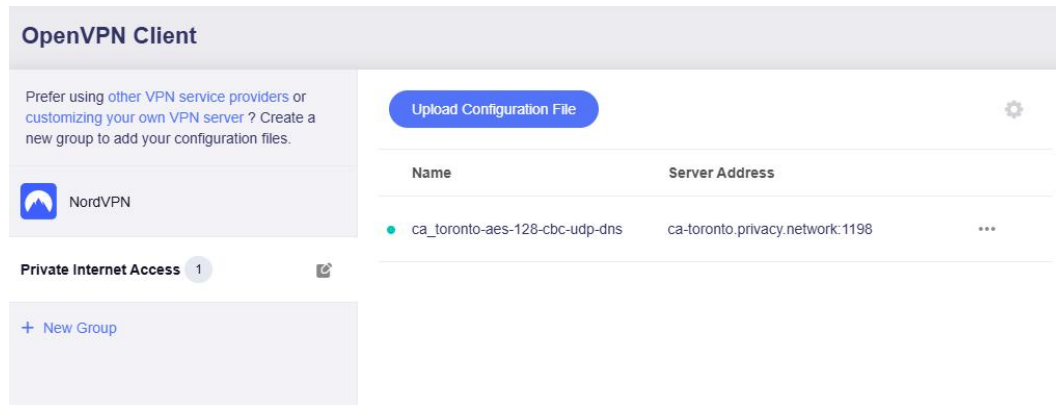
Name	Server Address	
ca_toronto-aes-128-cbc-udp-dns	ca-toronto.privacy.network:1198	...

▶ Start

Modify

Delete

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



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

10.2 Set Up WireGuard Client

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

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

10.2.1 Preparation

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

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

- [Set Up AzireVPN](#)
- [Set Up Mullvad](#)
- [Set Up WireGuard Client Manually \(for other providers\)](#)

10.2.2 Set Up AzireVPN

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

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

WireGuard Client

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

A AzireVPN

M Mullvad

+ New Group

AzireVPN

Username

Password

Save Credentials And Get Servers

[Setup Guide](#)

WireGuard Client

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

A AzireVPN 19

M Mullvad

+ New Group

Update Servers

Name	Server Address	
AzireVPN_ca1	ca1.wg.azirevpn.net:51820	
AzireVPN_dk1	dk1.wg.azirevpn.net:51820	
AzireVPN_fr1	fr1.wg.azirevpn.net:51820	
AzireVPN_de1	de1.wg.azirevpn.net:51820	
AzireVPN_de-ber	de-ber.wg.azirevpn.net:51820	
AzireVPN_it1	it1.wg.azirevpn.net:51820	
AzireVPN_nl1	nl1.wg.azirevpn.net:51820	
AzireVPN_no1	no1.wg.azirevpn.net:51820	
AzireVPN_ro1	ro1.wg.azirevpn.net:51820	
AzireVPN_es1	es1.wg.azirevpn.net:51820	

Delete All

3. Go to VPN Dashboard to enable the connection.

VPN Client Global Options

Global Proxy

All traffic will go through VPN. Only one VPN client instance can be activated.

Type	Configuration File	Enable	Options
• OpenVPN			Set Up Now
• WireGuard	AzureVPN_ca1		

Once connected, you should see your user IP address and the number of Bytes send/received.

VPN Client Global Options

Global Proxy

All traffic will go through VPN. Only one VPN client instance can be activated.

Type	Configuration File	Enable	Options
• OpenVPN			Set Up Now
• WireGuard	AzureVPN_ca1		

Server Address ca1.wg.azurevpn.net

Server Listen Port 51820

Traffic Statistics 9.27 KB / 8.87 KB

Client Virtual IP (IPv4) 10.50.6.246 [View Log](#)

4. Update servers.

AzureVPN may maintain or shutdown some servers, it will make the connection failed, you can **Update Servers** to get the latest available servers.

WireGuard Client

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

AzureVPN 19

Mullvad

[Update Servers](#)

Name	Server Address	
• AzureVPN_ca1	ca1.wg.azurevpn.net:51820	
• AzureVPN_dk1	dk1.wg.azurevpn.net:51820	

5. Edit credentials.

Click the cog icon to edit the credential.

WireGuard Client

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

A

AzureVPN

19

M

Mullvad

+ New Group

Update Servers

→ ⚙️

Name	Server Address	
AzureVPN_ca1	ca1.wg.azurevpn.net:51820	🗑️
AzureVPN_dk1	dk1.wg.azurevpn.net:51820	🗑️

6. Delete all files.

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

WireGuard Client

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

A

AzureVPN

19

M

Mullvad

+ New Group

Update Servers

⚙️

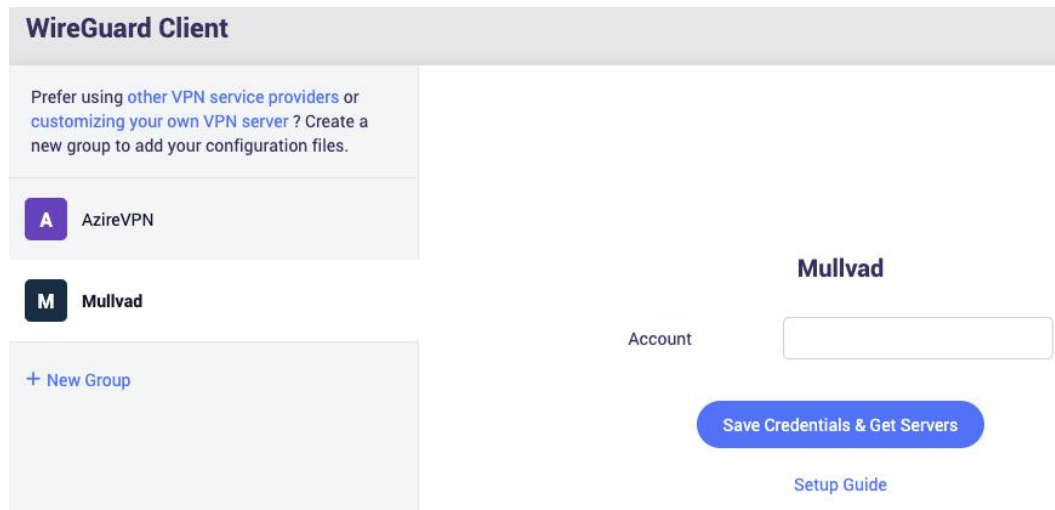
Name	Server Address	
AzureVPN_ca1	ca1.wg.azurevpn.net:51820	🗑️
AzureVPN_dk1	dk1.wg.azurevpn.net:51820	🗑️
AzureVPN_fr1	fr1.wg.azurevpn.net:51820	🗑️
AzureVPN_de1	de1.wg.azurevpn.net:51820	🗑️
AzureVPN_de-ber	de-ber.wg.azurevpn.net:51820	🗑️
AzureVPN_it1	it1.wg.azurevpn.net:51820	🗑️
AzureVPN_nl1	nl1.wg.azurevpn.net:51820	🗑️
AzureVPN_no1	no1.wg.azurevpn.net:51820	🗑️
AzureVPN_ro1	ro1.wg.azurevpn.net:51820	🗑️
AzureVPN_es1	es1.wg.azurevpn.net:51820	🗑️

🗑️ Delete All

10.2.3 Set Up Mullvad

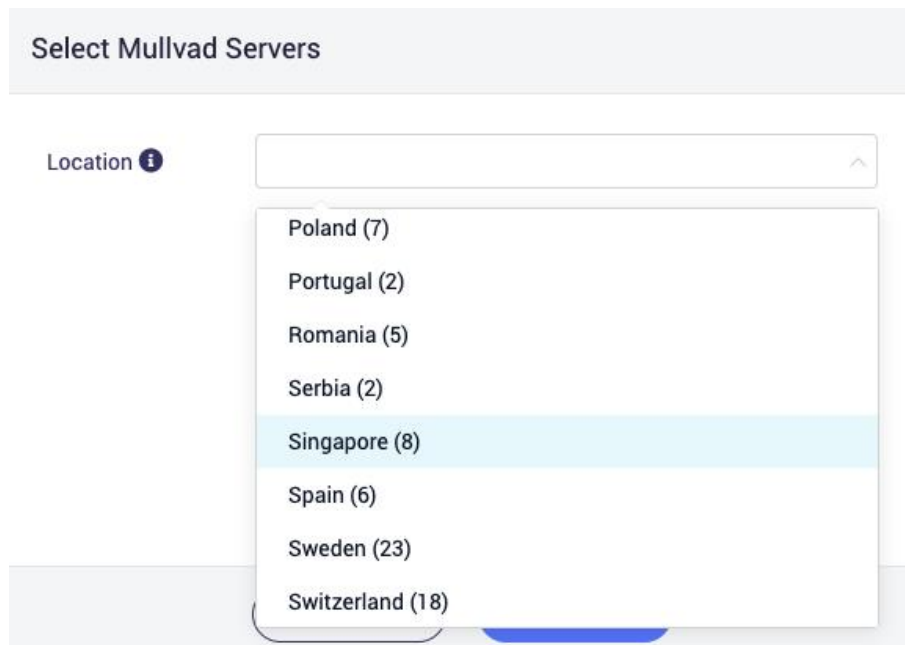
Follow the steps below to set your router as a Mullvad client.

1. Log in to your router's web admin panel and go to **VPN > WireGuard Client > Mullvad**.
2. Enter your Mullvad Account (16-digit number), then click **Save Credentials & Get Servers**.



The screenshot shows the 'WireGuard Client' interface. On the left, there's a sidebar with a link to 'Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.' Below this are two group cards: 'AzureVPN' with a purple 'A' icon and 'Mullvad' with a black 'M' icon. A '+ New Group' link is at the bottom. The main area is titled 'Mullvad' and contains an 'Account' input field, a blue 'Save Credentials & Get Servers' button, and a 'Setup Guide' link.

It will pop up a dialog to select a location.



The screenshot shows a 'Select Mullvad Servers' dialog. It has a 'Location' label with an information icon and a search input field. A dropdown menu is open, listing locations with the number of servers in parentheses: Poland (7), Portugal (2), Romania (5), Serbia (2), Singapore (8) (highlighted), Spain (6), Sweden (23), and Switzerland (18).

Then it will generate the configuration files of the selected location server.

The **Public Key** is the WireGuard public key to send to Mullvad server. You can have up to five keys at the same time, and manage WireGuard keys on your [Mullvad account page](#).

WireGuard Client

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

A

AzureVPN

M

Mullvad

8

+ New Group

Public Key

Update Servers

Name	Server Location	
Singapore_sg10	Singapore, Singapore	
Singapore_sg11	Singapore, Singapore	
Singapore_sg4	Singapore, Singapore	
Singapore_sg5	Singapore, Singapore	
Singapore_sg6	Singapore, Singapore	
Singapore_sg7	Singapore, Singapore	
Singapore_sg8	Singapore, Singapore	
Singapore_sg9	Singapore, Singapore	

Delete All

- Go to VPN Dashboard to enable the connection.

VPN Client

Global Options

Global Proxy

All traffic will go through VPN. Only one VPN client instance can be activated.

Type	Configuration File	Enable	Options
OpenVPN			Set Up Now
WireGuard	Singapore_sg10		

Once connected, you should see your user IP address and the number of Bytes send/received.

VPN Client
Global Options

Global Proxy
All traffic will go through VPN. Only one VPN client instance can be activated.

Type	Configuration File	Enable	Options
OpenVPN			Set Up Now
WireGuard	Singapore_sg10	☒	Server Address 138.199.60.15 Server Listen Port 3499 Traffic Statistics ↑ 18.63 KB / ↓ 35.87 KB Client Virtual IP (IPv4) 10.67.219.125/32 View Log

4. Update servers

Mullvad may maintain or shutdown some servers, it will make the connection failed, you can **Update Servers** to get the latest available servers.

WireGuard Client

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

A
AzireVPN

M
Mullvad
8

Public Key

Update Servers

Name

Server Location

Singapore_sg10

Singapore, Singapore

5. Edit credentials

Click the gear icon to edit your login credentials.

WireGuard Client

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

A
AzireVPN

M
Mullvad
8

Public Key

Update Servers

Name

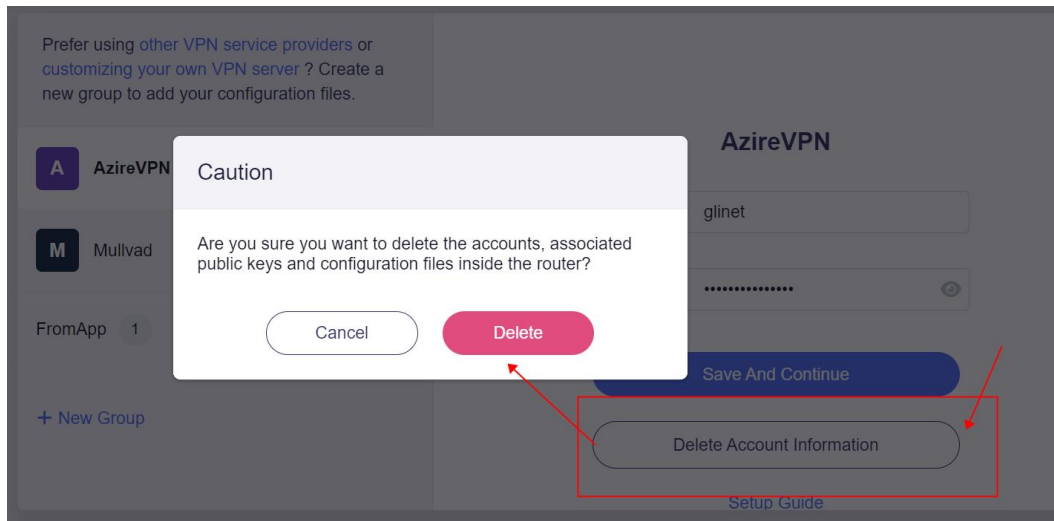
Server Location

Singapore_sg10

Singapore, Singapore

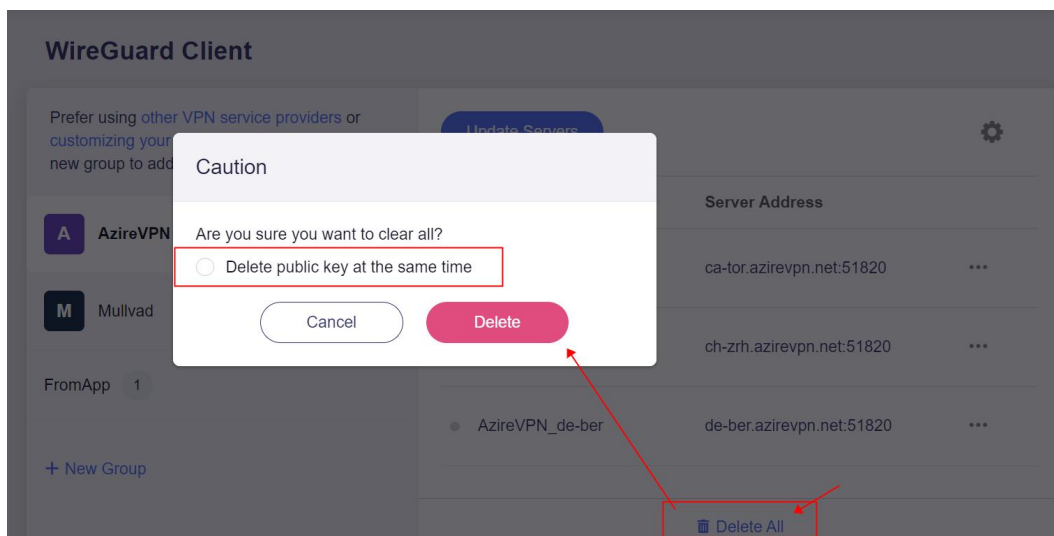
6. Delete account information

If you click **Delete**, it will delete the account credential, private key, public key and configuration files **in the router**.



7. Delete

Allow deleting all configuration files with one click and provide a prompt to also delete private key and public key.



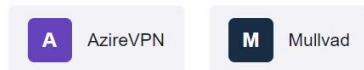
10.2.4 Set Up WireGuard Client Manually (for other providers)

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.

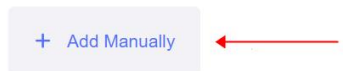
Below are steps to upload the configuration file to the router to set up a WireGuard client.

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

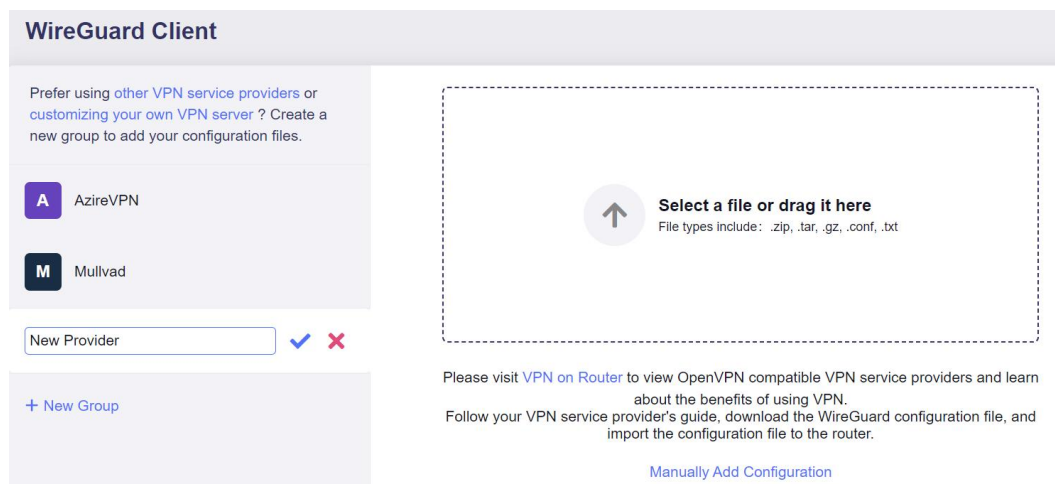
Request the VPN configuration file from your VPN service provider.



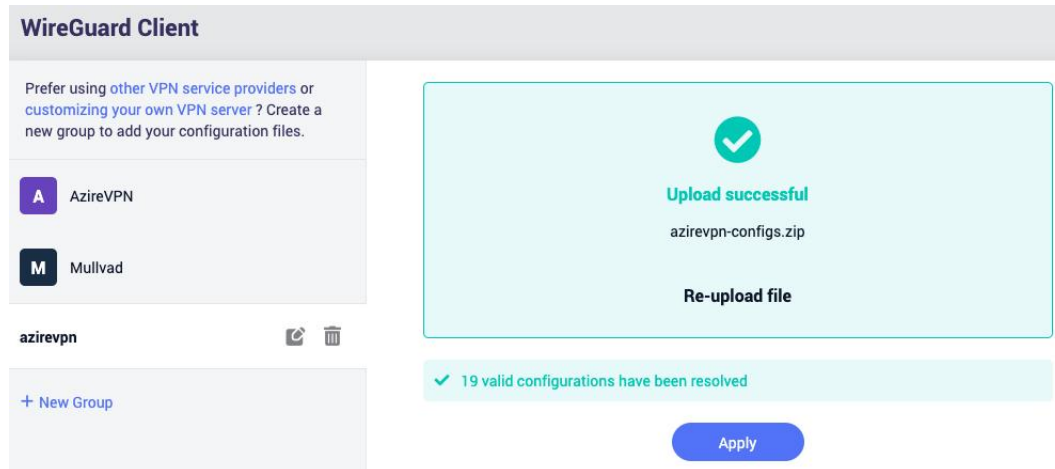
Please visit [VPN on Router](#) to view OpenVPN compatible VPN service providers and learn about the benefits of using VPN. Follow your VPN service provider's guide, download the WireGuard configuration file, and import the configuration file to the router.



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

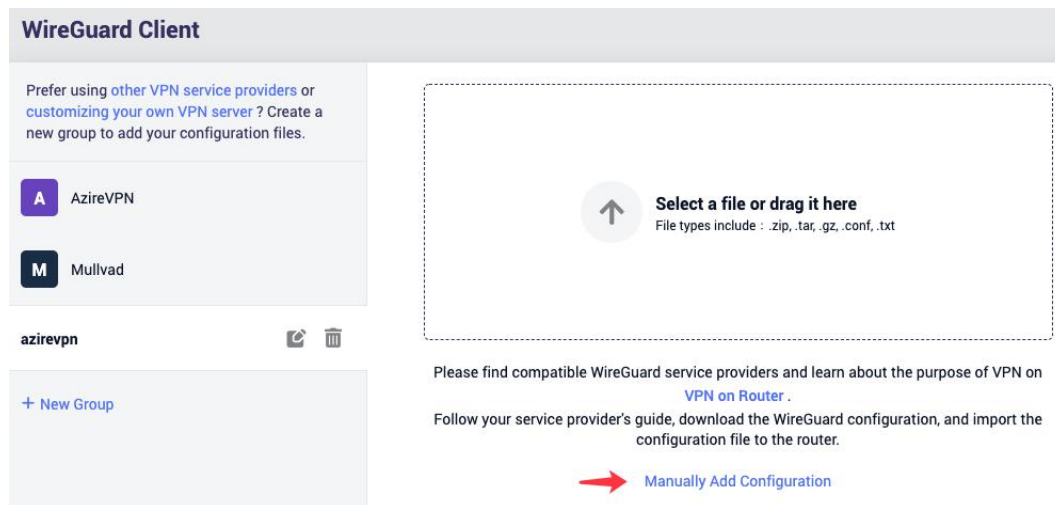


3. Click the upload area to upload your WireGuard configuration file (supported formats: zip, tar, gz, conf, txt), and click **Apply**.



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

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



Edit WireGuard Configuration

Name

azure-ca

Item Mode

[Interface]
PrivateKey =
Address = 10.50.23.65/19
DNS = 10.50.0.1

[Peer]
PublicKey =
AllowedIPs = 0.0.0.0/0
Endpoint = ca1.wg.azurevpn.net:51820

Cancel

Apply

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

Edit WireGuard Configuration

Name

Text Mode

Interface

IPv4 Address

Use IPv6

Private Key

Listen Port

DNS

MTU

Optional

Optional

Optional

Cancel

Apply

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

WireGuard Client

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

A

AzureVPN

M

Mullvad

azurevpn 19

Add Configuration

Name	Server Address	
● azurevpn-ca1	ca1.wg.azurevpn.net:51820	⋮
● azurevpn-dk1	dk1.wg.azurevpn.net:51820	
● azurevpn-fr1	fr1.wg.azurevpn.net:51820	⋮

▶ Start

✎ Edit

🗑 Delete

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

VPN Client

Global Options

Global Proxy

All traffic will go through VPN. Only one VPN client instance can be activated.

Type	Configuration File	Enable	Options
● OpenVPN			Set Up Now
● WireGuard	azurevpn-ca1	☒	⚙

Server Address

ca1.wg.azurevpn.net

Server Listen Port

51820

Traffic Statistics

↑ 31.23 KB

↓ 73.08 KB

Client Virtual IP (IPv4)

10.50.10.115/19

[View Log](#)

Chapter 11

Tor

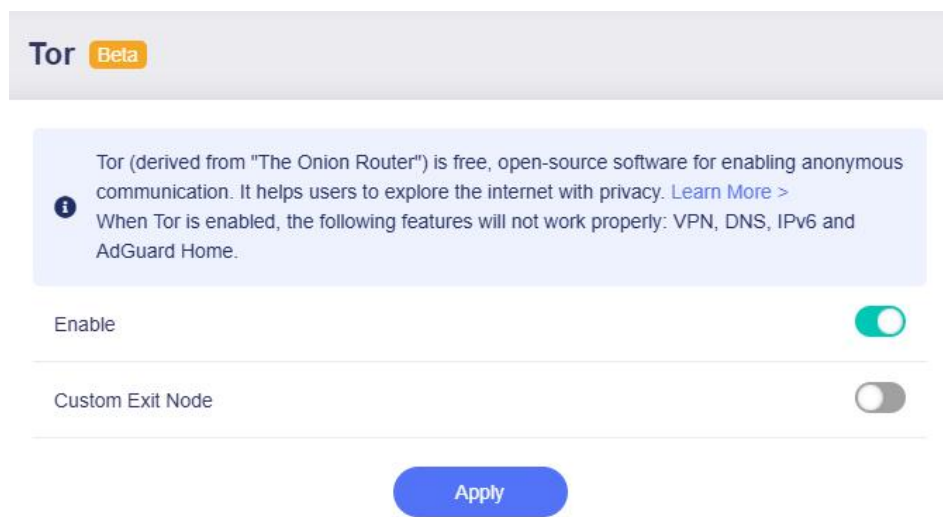
This chapter provides a brief introduction to Tor (The Onion Router), a free and open-source software for enabling anonymous communication.

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

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

Follow the steps below to set up Tor if needed.

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



Tor Beta

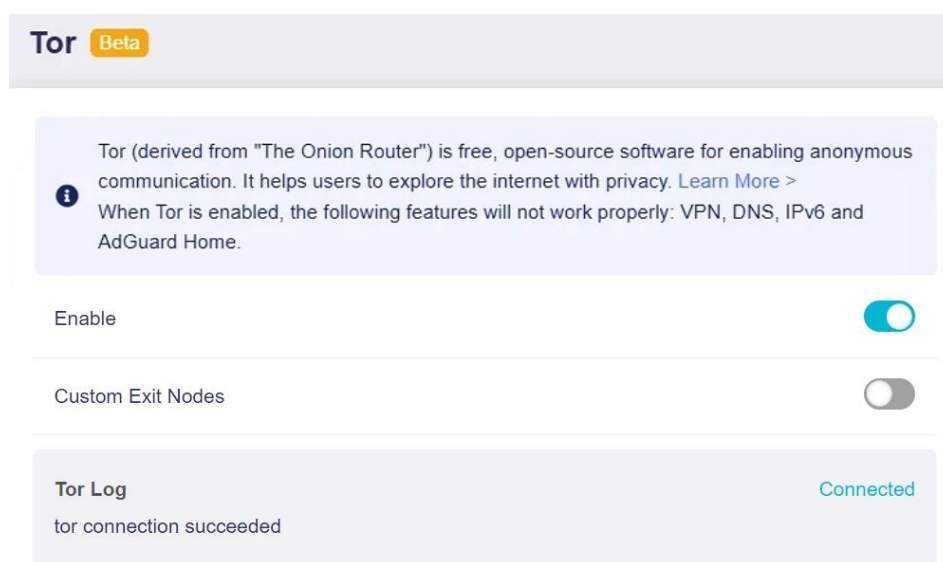
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.

Enable ☒

Custom Exit Node ☐

Apply

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



Tor Beta

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

Enable ☒

Custom Exit Nodes ☐

Tor Log Connected
tor connection succeeded

Chapter 12

Applications

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

12.1 Plug-ins

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

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

Plug-insManage Sources

Filter

Q Search Package

Refresh

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

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

Free space: 84.54 % (6.76 GB)

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

< 1 2 3 4 ... 1101 >

Go

Note:

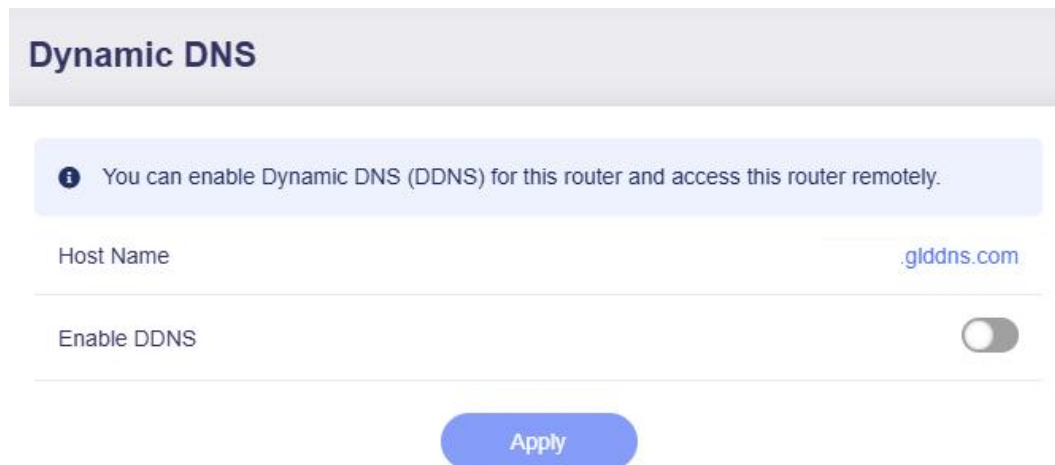
1. It is not recommended to update pre-installed plug-ins in GL.iNet official firmware, such as nginx, adguard home, tailscale, etc.
2. Third-party plugins manually installed by users can be updated; however, GL.iNet is not liable for any security issues from third-party plugins. For inquiries, please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

12.2 Dynamic DNS

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

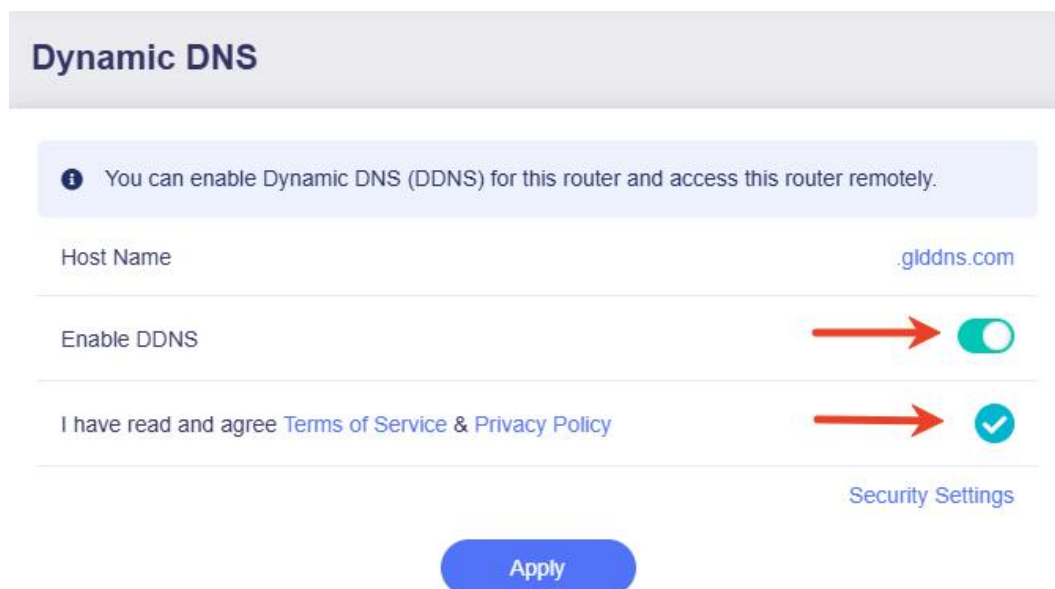
12.2.1 Enable DDNS

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



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

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



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

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

Dynamic DNS

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

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

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

Host Name [.glddns.com](#)

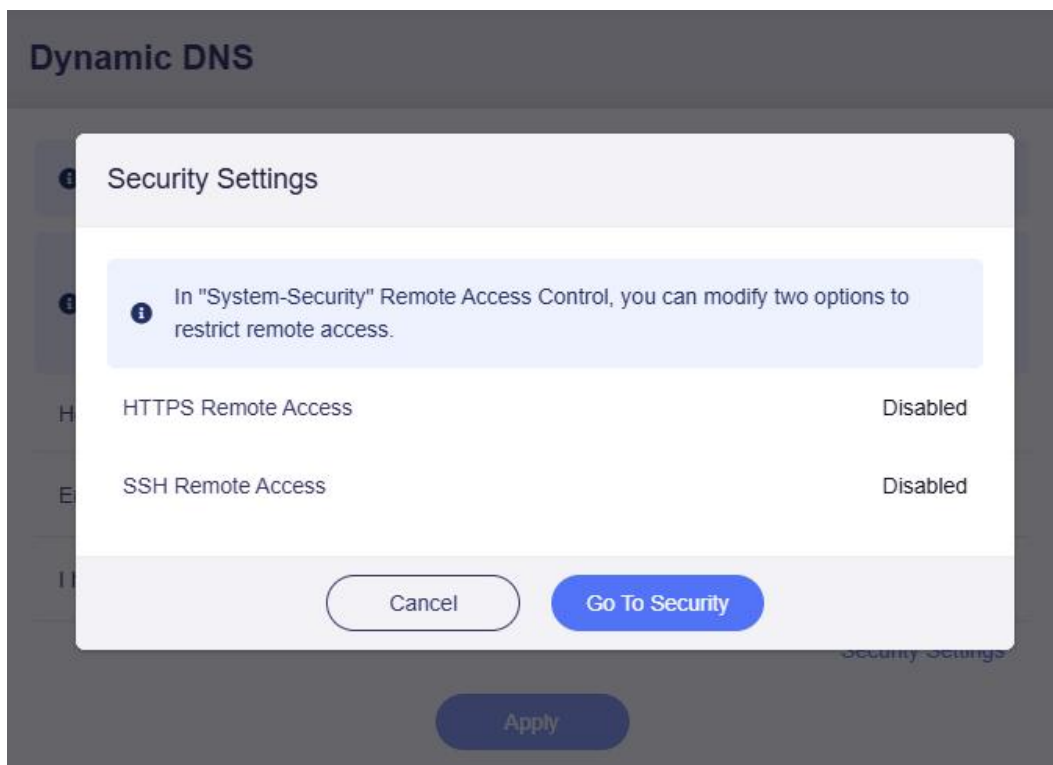
Enable DDNS ☒

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

[Security Settings](#)

Apply

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



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

Remote Access Control

Allow Ping from WAN

HTTPS Remote Access

SSH Remote Access

Allow Remote Access only from Specific IPs ⓘ

Apply

Note:

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

12.2.2 Check if DDNS Works

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

Method 1. Use DDNS Test tool

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

Dynamic DNS

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

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

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

Host Name [.glddns.com](#)

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

DDNS Test

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

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

IP address from DDNS Domain Resolution	
IPv4	205.185.113.19

WAN Interface IP address	
Ethernet	192.168.5.135

Method 2. Use commands

1. Use nslookup command *nslookup xxxxxxx.glddns.com 8.8.8.8* to obtain the mapping between domain name and IP address, as shown below.

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

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

12.2.3 HTTPS Remote Access

A **Public IP address** is required for HTTPS remote access. See [here](#) to verify whether your ISP assigns you a public IP address. If your router is behind NAT, configure port forwarding (**port 443**) on the upstream router for HTTPS access.

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

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

Dynamic DNS

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

Host Name [.glddns.com](#)

Enable DDNS  ☒

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

[Security Settings](#)

Apply

2. In the web admin panel, go to **SYSTEM > Security > Remote Access Control**. Enable **HTTPS Remote Access**, and click **Apply**.

Remote Access Control

Allow Ping from WAN ☐

HTTPS Remote Access  ☒

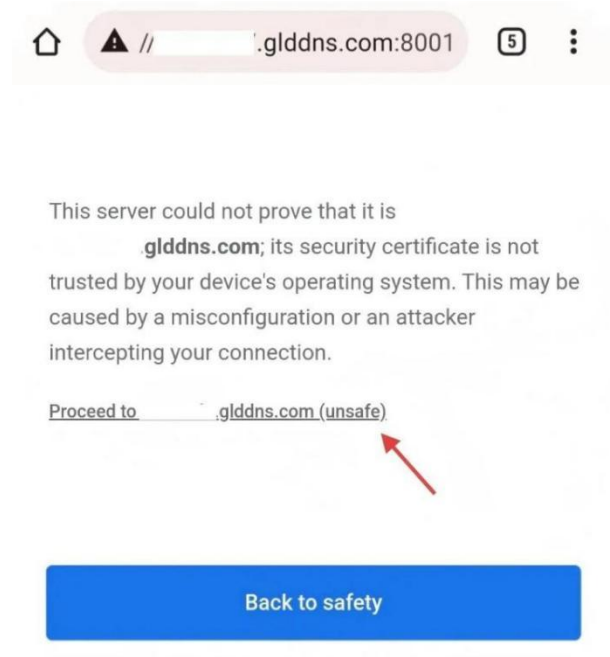
SSH Remote Access ☐

Allow Remote Access only from Specific IPs  ☐

Apply

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

Note: This function uses self-signed certificates; therefore, browsers will indicate "Your connection is not private" when accessing the router's admin panel via the DDNS host name over HTTPS. To proceed the HTTPS remote access, click **Advanced** at the bottom, then click **Proceed to xxxxxxx.glddns.com** to continue.



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

12.2.4 SSH Remote Access

A **Public IP address** is required for SSH remote access. See [here](#) to verify whether your ISP assigns you a public IP address. If your router is behind NAT, configure port forwarding (**port 22**) on the upstream router for SSH remote access.

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

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

Dynamic DNS

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

Host Name [.glddns.com](#)

Enable DDNS  ☒

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

[Security Settings](#)

Apply

2. In the web admin panel, go to **SYSTEM > Security > Remote Access Control**. Enable **SSH Remote Access**, and click **Apply**.

Remote Access Control

Allow Ping from WAN ☐

HTTPS Remote Access ☐

SSH Remote Access  ☒

Allow Remote Access only from Specific IPs  ☐

Apply

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

12.3 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.

12.3.1 Enable GoodCloud

1. Log in to your router's web Admin Panel and navigate to **APPLICATIONS > GoodCloud**. Toggle the switch to enable GoodCloud.

GoodCloud

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

Enable [GoodCloud](#) 

[View Logs](#)

[Apply](#)

Enable **Remote SSH** and **Remote Web Access** if needed, select the nearest server, read and agree the **Terms of Service & Privacy Policy**, then click **Apply**.

GoodCloud

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

Enable [GoodCloud](#) 

Enable Remote SSH 

Enable Remote Web Access 

Device ID *****

Device MAC 94:83:C4:XX:XX:XX

Device S/N b5e3968666*****

Data Server

Europe 

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

[View Logs](#)

[Apply](#)

- **Remote SSH:** For remotely accessing the router's terminal over SSH from GoodCloud platform.
 - **Remote Web Access:** For remotely accessing the router's web Admin Panel over HTTP/HTTPS from GoodCloud platform.
 - **Data Server:** Please choose the server nearest to your device's location. There are three options: Asia Pacific (Japan), America (Oregon), and Europe (Ireland).
 - **View Logs:** Redirect to the Log page and display Cloud log.
2. Click [GoodCloud](#) to go to the login page, and 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.

GoodCloud

 With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is *****, Please use this ID to bind the device to your cloud account.

Enable [GoodCloud](#)



Enable Remote SSH



Enable Remote Web Access



Device ID

Device MAC

94:83:C4:XX:XX:XX

Device S/N

83801ed116*****

Data Server

Asia Pacific



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



Apply

[View Logs](#)



Log In

Use your GL.iNet account

[Forgot password?](#)

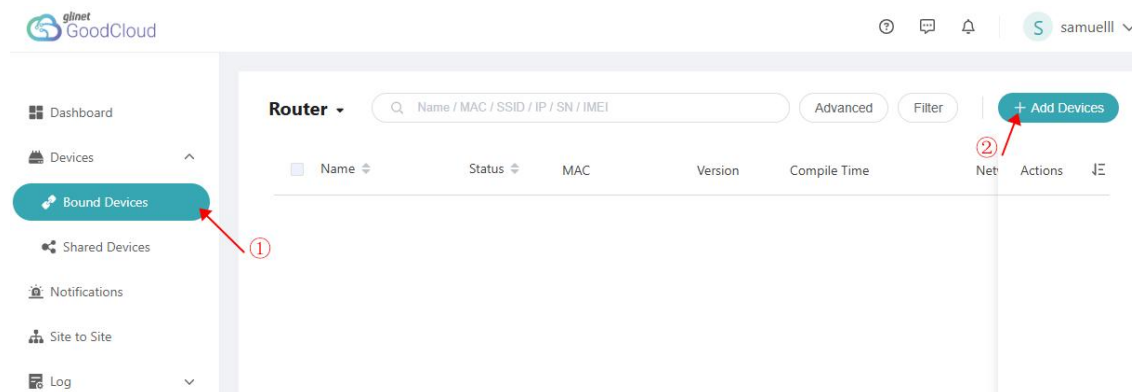
Log In

Tips:

- The GoodCloud binding steps differ by firmware version.
- If you fail to receive the verification email, check your spam folder or try again later.

For further assistance, contact us at support@gl-inet.com.

3. On the Cloud platform, navigate to **Devices > Bound Devices > Add Devices**.



There are three methods to bind device to your GoodCloud account: Auto Discover, Manually Add, and Bulk Import. Click [here](#) for more details.

4. After successful binding, return to the router's web Admin Panel and navigate to **APPLICATIONS > GoodCloud**. This page displays the binding details, including username and binding time.

GoodCloud



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

The device is bound by **Holly0912** on **2026-09-29 12:22**, [Unbind](#)

Enable [GoodCloud](#)



Enable Remote SSH



Enable Remote Web Access



Device ID

Device MAC

94:83:C4:XX:XX:XX

Device S/N

b5e396866*****

Data Server

Europe



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



Apply

[View Logs](#)

12.3.2 Manage Your Router

Check Device Details

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

Filter

Settings

Commands

+ Add

☐	Name	Status	Model	Version	MAC	IP	Compile Time
☐	A1300-90f	Online	A1300	4.5.22	94:83:C4:XX:XX:XX	183.178.xx.xx	2025-04-08 16:48:05

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.

A1300-90f

Online

Remote GUI

Remote SSH

Reboot Device

Basic Info

Refresh



A1300

Network Mode

Router

SN

b5e3*****

Version

4.5.22

Memory Usage

43%

MAC Address

94:83:C4:XX:XX:XX

Compile Time

2025-04-08 16:48:05

IP

183.178.xx.xx

Up Time

0 days 4 hrs 54 mins

Statistical Data

Refresh

Network Latency

Retest



Poor

360.44 ms

2.16 ms

0 %

Latency

Jitter

Packet Loss

Device Status History

More

09/29/2026 00:00

09/29/2026 14:18

Online

Offline

Network

Clients List

Share

Cellular Health

Internet

Refresh



Ethernet1

More

Connected

IP 10.100.211.199/22

Address

Protocol DHCP



Repeater

More

Disabled

IP Address --

SSID --



Tethering

More

Disabled

IP Address --

Device List

Details

111

Remote Web Access

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

GoodCloud

With GoodCloud, you can manage groups of routers, check their status in real-time, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by **Holly0912** on **2026-09-29 14:16**, [Unbind](#)

Enable [GoodCloud](#) ☒

Enable Remote SSH ☐

Enable Remote Web Access ☒

Device ID *****

Device MAC 94:83:C4:XX:XX:XX

Device S/N b5e3968666*****

Data Server Europe

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

[View Logs](#)

[Apply](#)

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

A1300-90f Online Remote GUI Remote SSH Reboot Device

Basic Info



A1300

Network Mode	Router	Version	4.5.22	MAC Address	94:83:C4:XX:XX:XX	IP	183.178.xx.xx
SN	b5e3*****	Memory Usage	43%	Compile Time	2025-04-08 16:48:05	Up Time	0 days 3 hrs 1 mins

[Refresh](#)

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

Remote GUI

Network is unstable. Using this feature may cause disconnection.
Please switch networks or restart your router, and try again when the connection is stable.

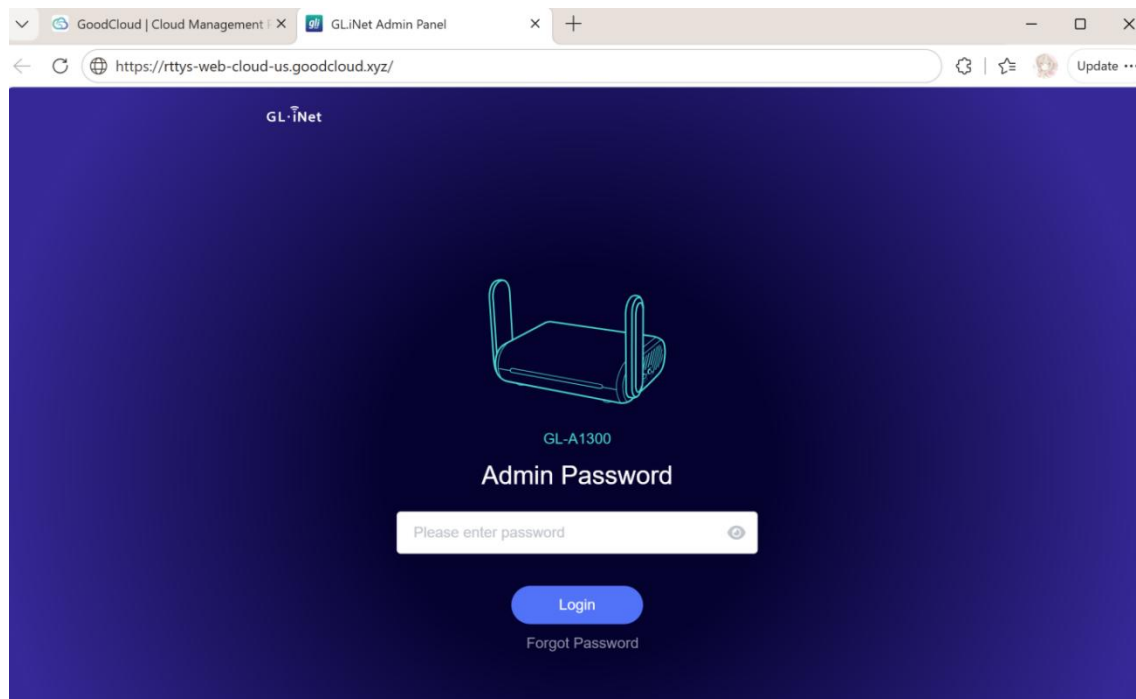
* Port

80

Cancel

Apply

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



Remote SSH

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

GoodCloud

With GoodCloud, you can manage groups of routers, check their status in real-time, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by **Holly0912** on **2026-09-29 14:16**,[Unbind](#)

Enable [GoodCloud](#) ☒

Enable Remote SSH ☒

Enable Remote Web Access ☐

Device ID *****

Device MAC 94:83:C4:XX:XX:XX

Device S/N b5e3968666*****

Data Server

Europe

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

[View Logs](#)

[Apply](#)

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

A1300-90f Online

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

Basic Info



A1300

Network Mode	Version	MAC Address	IP
Router	4.5.22	94:83:C4:XX:XX:XX	183.178.xxxx
SN	Memory Usage	Compile Time	Up Time
b5e3*****	43%	2025-04-08 16:48:05	0 days 3 hrs 4 mins

[Refresh](#)

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

```
GL-A1300 login: root
Password:

BusyBox v1.33.2 (2022-02-16 20:29:10 UTC) built-in shell (ash)

|_| .----- .----- .----- | | | | .----- | | | | | | | | | |
|_| - | | - | | | | | | | | | | | |
|_| | | | | | | | | | | | | | |
|_| | W I R E L E S S F R E E D O M
-----
OpenWrt 21.02.2, r16495-bf0c965af0
-----
root@GL-A1300:~#
```

12.3.3 Unbind Device

In the router's web admin panel, click **Unbind**. Your device will then be unbound from your GoodCloud account.

GoodCloud

With GoodCloud, you can manage groups of routers, check their status in real-time, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by **Holly0912** on **2026-09-29 12:22**, [Unbind](#)

Enable [GoodCloud](#)

Enable Remote SSH

Enable Remote Web Access

Device ID

vxd290f

Device MAC

94:83:C4:XX:XX:XX

Device S/N

b5e396866*****

Data Server

Europe

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

Apply

[View Logs](#)

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

Q

Name / MAC / IP / SN / IMEI

Filter

Settings

Commands

+ Add

1 Selected

☒	Name	Status	Model	Version	MAC	IP		
☒	A1300-90f	Online	A1300	4.5.22	94:83:C4:XX:XX:XX	18:		

Modify Settings

Upgrade Firmware

Share Device

Delete

Compile Time

2025-04-08 16:48:05

12.4 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.

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

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

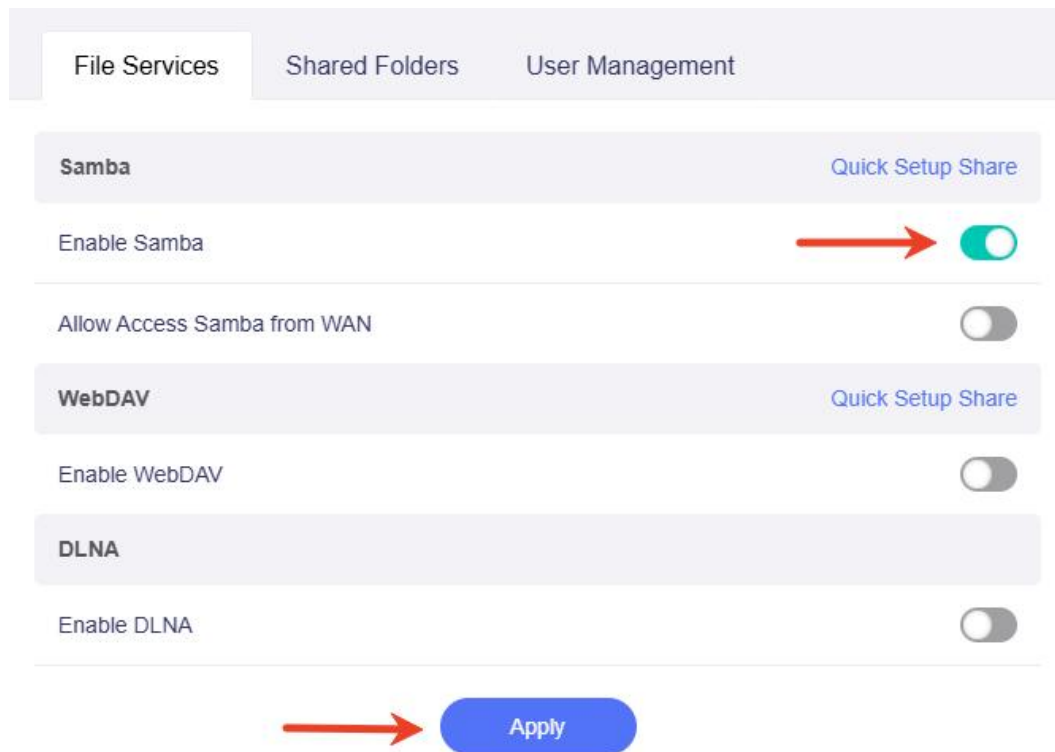
12.4.1 Connect Storage

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

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

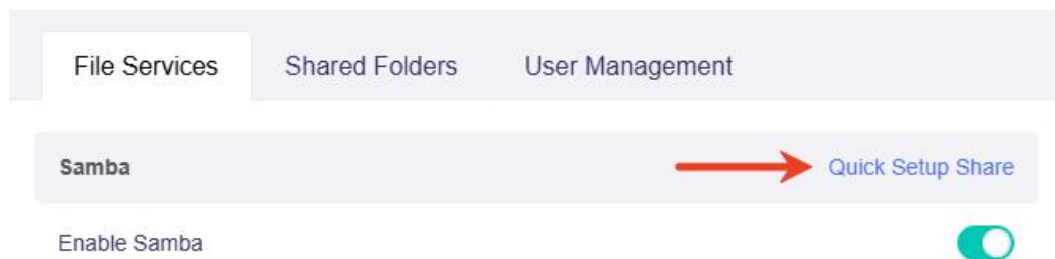
12.4.2 Set Up Samba

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



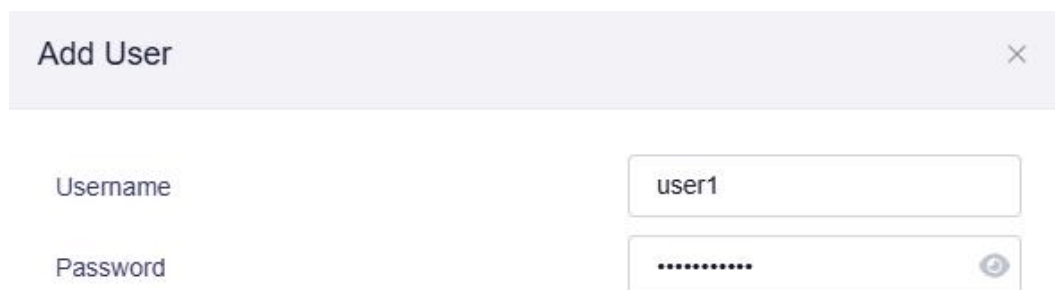
The screenshot shows the 'File Services' configuration page. At the top, there are three tabs: 'File Services', 'Shared Folders', and 'User Management'. Under the 'File Services' tab, there are three sections: 'Samba', 'WebDAV', and 'DLNA'. Each section has a 'Quick Setup Share' link. The 'Samba' section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

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



The screenshot shows the 'File Services' configuration page, specifically the 'Samba' section. The 'Enable Samba' toggle switch is turned on. A red arrow points to the 'Quick Setup Share' link.

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



The screenshot shows the 'Add User' dialog box. It has a title bar with 'Add User' and a close button. There are two input fields: 'Username' with the text 'user1' and 'Password' with a masked password '.....' and an eye icon to toggle visibility.

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

Add Shared Folder

▼ disk1_part1

qlogs_20260709_161408

qlogs_20260709_161458

qlogs_20260709_162031

Cancel

Next

- Set up the shared folder.

The user created in the previous step will be added to **Read-Only User** by default. If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Read-Write User**, then click **Apply**.

Shared Folder Settings

Path

/disk1_part1

Samba Settings

Share Name

disk1_part1

Anonymous Access

☐

Read-Write User

Read-only User

user1 ×

Back

Apply

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

6. Obtain the folder access link.

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

Folder Access Link

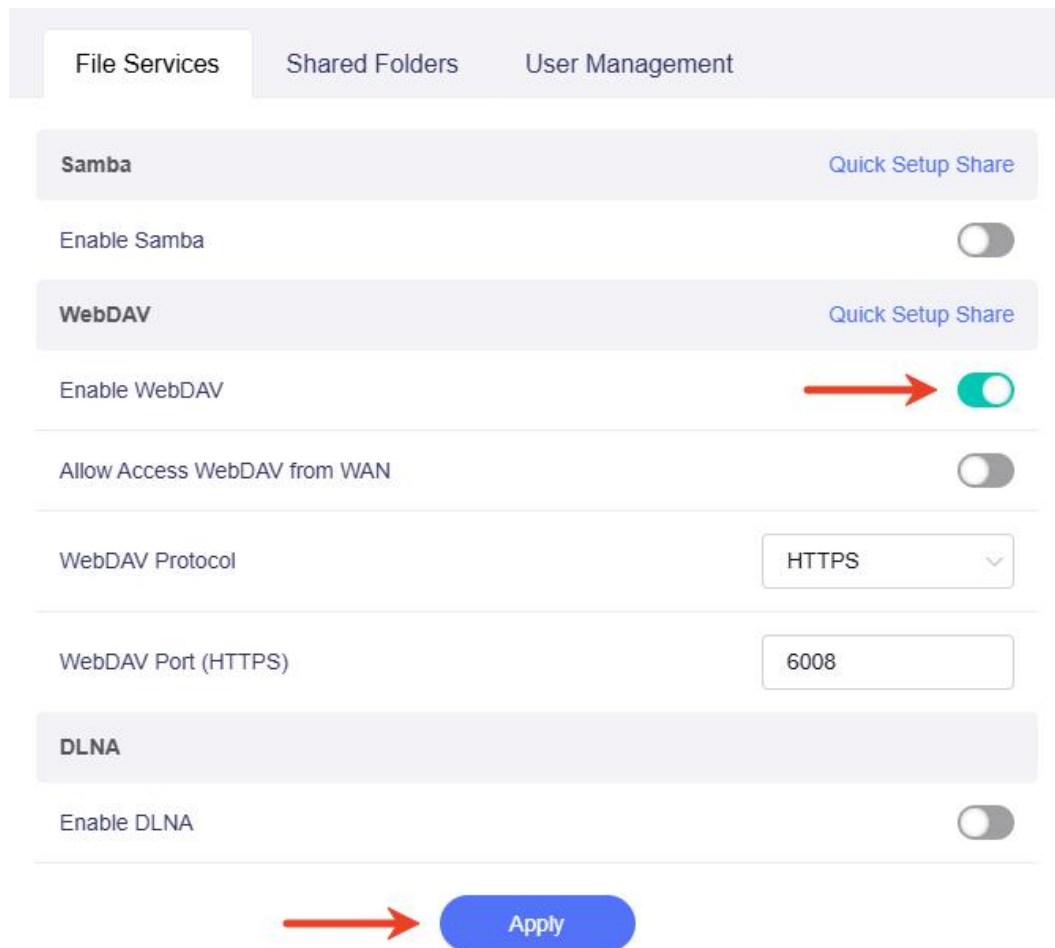
 The folder has been shared. Use the following link to mount the folder as a network disk to your PC or Phone. [Learn More](#)

Windows SMB	\\192.168.8.1\disk1_part1
Unix-like Samba	smb://192.168.8.1/disk1_part1

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

12.4.3 Set Up WebDAV

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



The screenshot shows the 'File Services' tab in a configuration interface. It contains sections for Samba, WebDAV, and DLNA. The WebDAV section is highlighted with a red arrow pointing to the 'Enable WebDAV' toggle, which is turned on. Another red arrow points to the 'Apply' button at the bottom of the page.

File Services Shared Folders User Management

Samba [Quick Setup Share](#)

Enable Samba ☐

WebDAV [Quick Setup Share](#)

Enable WebDAV ☒

Allow Access WebDAV from WAN ☐

WebDAV Protocol HTTPS

WebDAV Port (HTTPS) 6008

DLNA

Enable DLNA ☐

[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.



The screenshot shows the 'WebDAV' section with the 'Enable WebDAV' toggle turned on. A red arrow points to the 'Quick Setup Share' link.

WebDAV [Quick Setup Share](#)

Enable WebDAV ☒

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

Add User

Username

user1

Password

.....

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

Add Shared Folder

▼ disk1_part1

qlogs_20260709_161408

qlogs_20260709_161458

qlogs_20260709_162031

5. Set up the shared folder.

The user created in the previous step will be added to **Read-Only User** by default. If you want this user to be able to write or delete files, remove it from Read-Only User and add it to **Read-Write User**, then click **Apply**.

Shared Folder Settings

Path

/disk1_part1

WebDAV Settings

Anonymous Access

Read-Write User

Read-only User

user1 ×

Back

Apply

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

6. Obtain the folder access link.

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

Folder Access Link



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

HTTPS

https://192.168.8.1:6008/disk1_part1

Dav

dav://192.168.8.1:6008/disk1_part1

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

12.4.4 Set Up DLNA

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

The screenshot shows the 'File Services' tab selected in a navigation bar. Below it are three sections: Samba, WebDAV, and DLNA. Each section has a 'Quick Setup Share' link and an 'Enable' toggle switch. The 'Enable DLNA' toggle is turned on and highlighted with a red arrow. Below the DLNA section, the 'Share Path' is set to '/disk1_part1' with a 'Modify' link. At the bottom of the page, a blue 'Apply' button is highlighted with a red arrow.

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

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

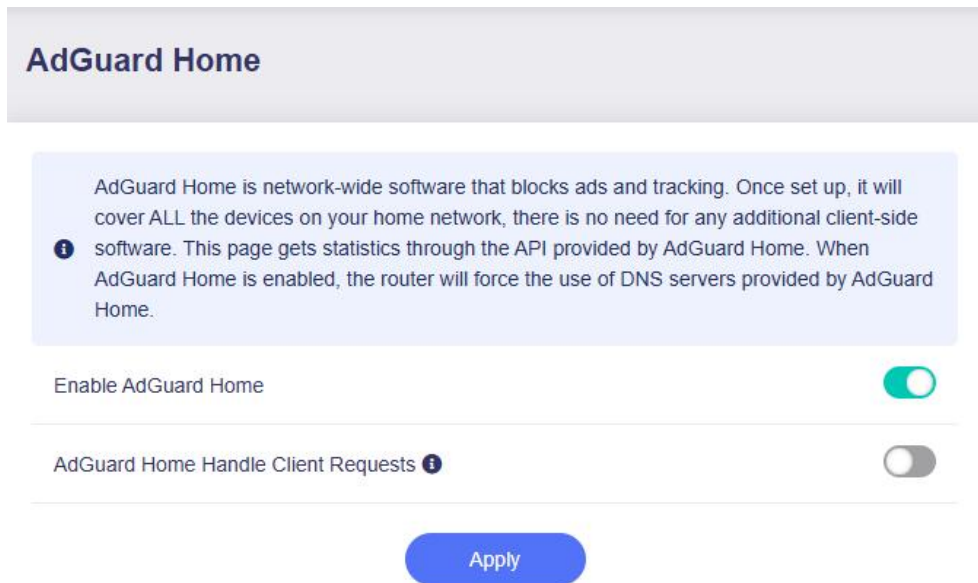
3. Connect your smart TV to the router. It will find the DLNA server automatically.

12.5 AdGuard Home

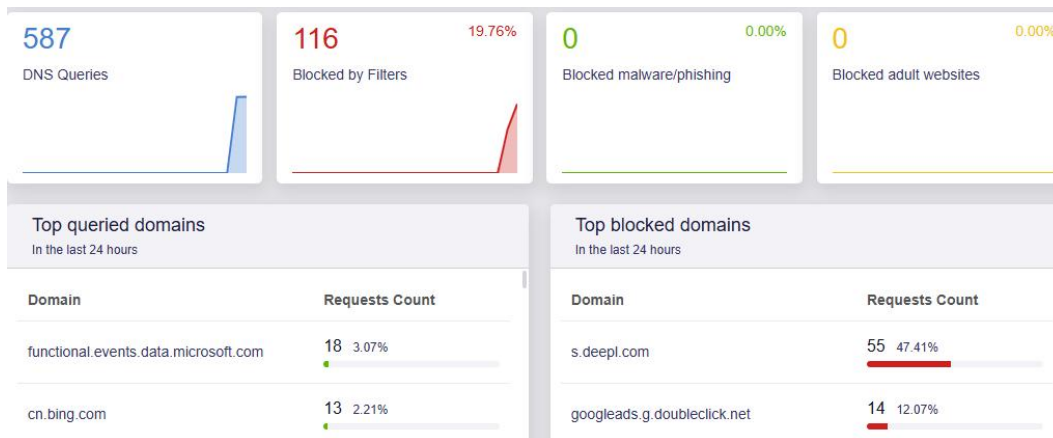
AdGuard Home is a network-wide ad-blocking and tracking-prevention software. Once set up, it will cover all client devices with no additional client-side software required.

Follow these steps to set up AdGuard Home.

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



- **AdGuard Home Handles Client Requests:** If enabled, DNS queries from client devices will be handled directly by AdGuard Home, but this will cause VPN policies based on domains to fail.
2. The page will automatically load DNS statistics (queries, blocked domains, etc.) via the API provided by AdGuard Home.



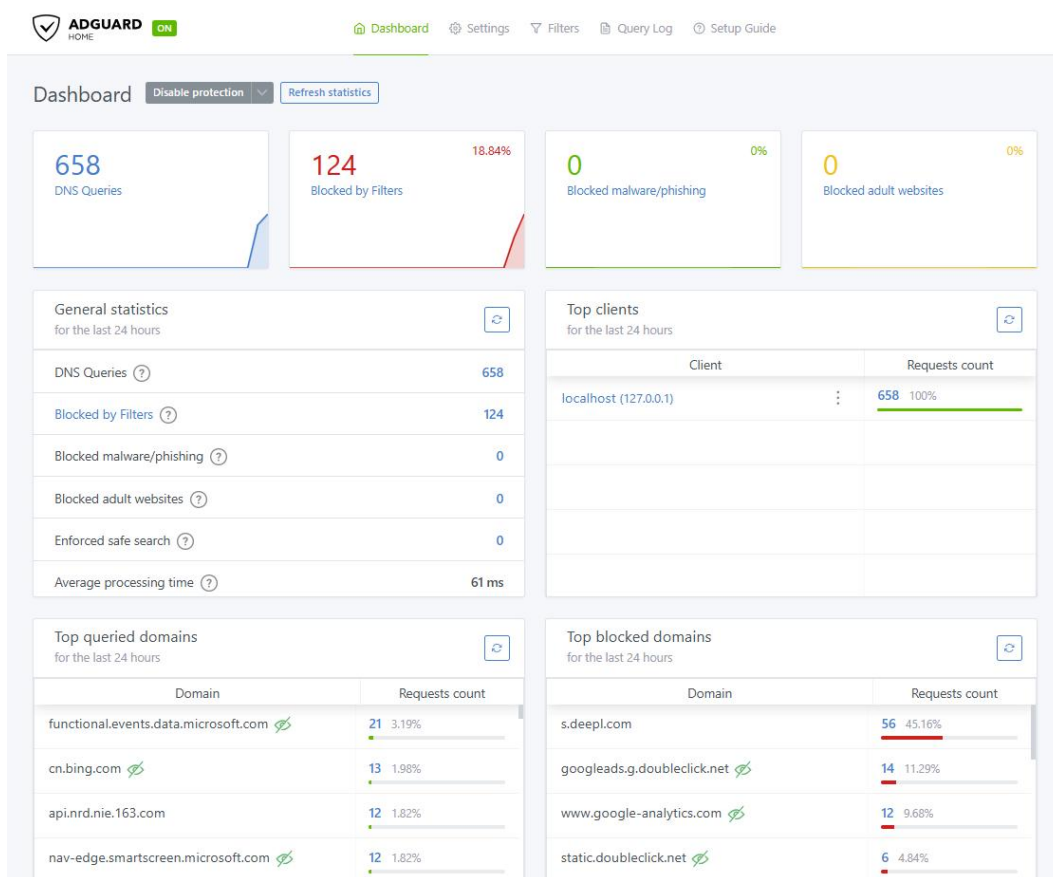
3. Click **Settings Page** to configure advanced settings for AdGuard Home.

AdGuard Home

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

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

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



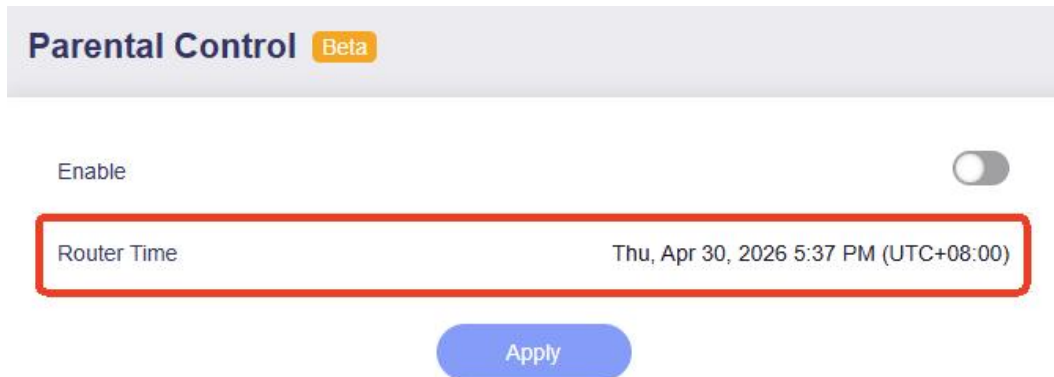
12.6 Parental Control

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

12.6.1 Quick Setup

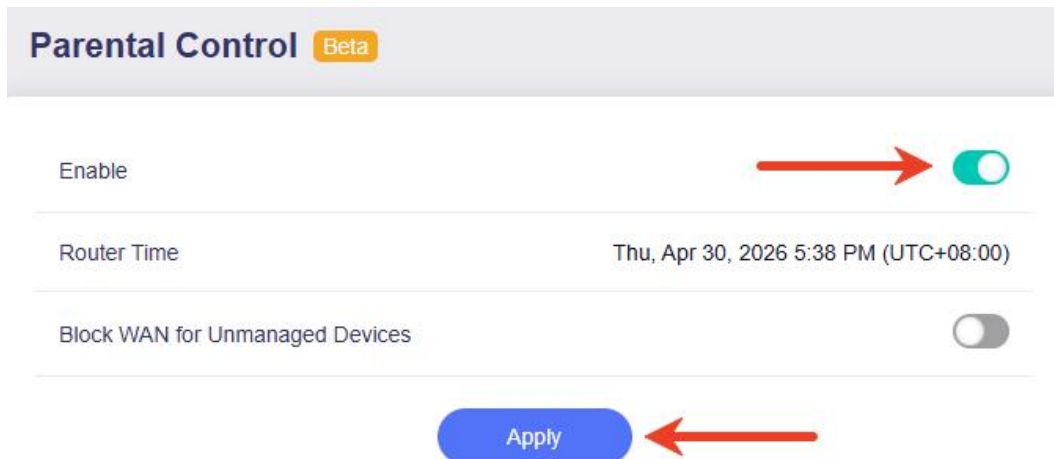
Follow these steps to set up Parental Control on GL.iNet routers.

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



The screenshot shows the 'Parental Control' settings page. At the top, there is a header 'Parental Control' with a 'Beta' tag. Below it, the 'Enable' toggle is currently turned off. A red rectangular box highlights the 'Router Time' field, which displays 'Thu, Apr 30, 2026 5:37 PM (UTC+08:00)'. Below the time field is a blue 'Apply' button.

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](#).



This screenshot shows the 'Parental Control' settings page with more options visible. The 'Enable' toggle is now turned on, indicated by a red arrow pointing to it. The 'Router Time' field still shows 'Thu, Apr 30, 2026 5:38 PM (UTC+08:00)'. Below it, the 'Block WAN for Unmanaged Devices' toggle is currently turned off. At the bottom, a blue 'Apply' button is highlighted with a red arrow pointing to it.

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

Here is a use case for your reference.

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

Setup Steps:

1. Create a profile and customize a name.

1. Create A Profile For Your Child Or Family

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

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

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

Profile Name

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

2. Select the devices to be managed



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

[+ Manually Add Device](#)



glkvm

94:83:C4:A9:97:DC



GL-INET-08

6C:1F:F7:5D:F1:5D

self



Child-phone

94:83:C4:B7:20:01



3. Set access limit.

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

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

3. Set access limits for these devices

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

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

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

Default Ruleset

Block Internet Access

+ Add a New Ruleset

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

Add a New Ruleset

Ruleset Name

Learning

Color

#B15EF8

Blocklist Input Mode ⓘ

Manual

1

fortnite.com

2

pornhub.com

3

tiktok.com|

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

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

Add a New Ruleset

Ruleset Name

Play

Color

#F5946D

Blocklist Input Mode ⓘ

Manual

1 pornhub.com

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

3. Set access limits for these devices

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

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

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

Default Ruleset

Block Internet Access

Block Internet Access

No Limit

Learning

Play

Back

Finish

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

4. Go to set schedules

You have successfully created a profile!

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



Later

Go to Set

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

Add Schedule



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

Schedule Ruleset

● Learning

Execution Time

08:00

to

11:00

Execution Day(s)

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Cancel

Apply

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

Parental Control / Modify Profile Beta

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

Rule Name

Home

Default Ruleset **i**

Block Internet Acce

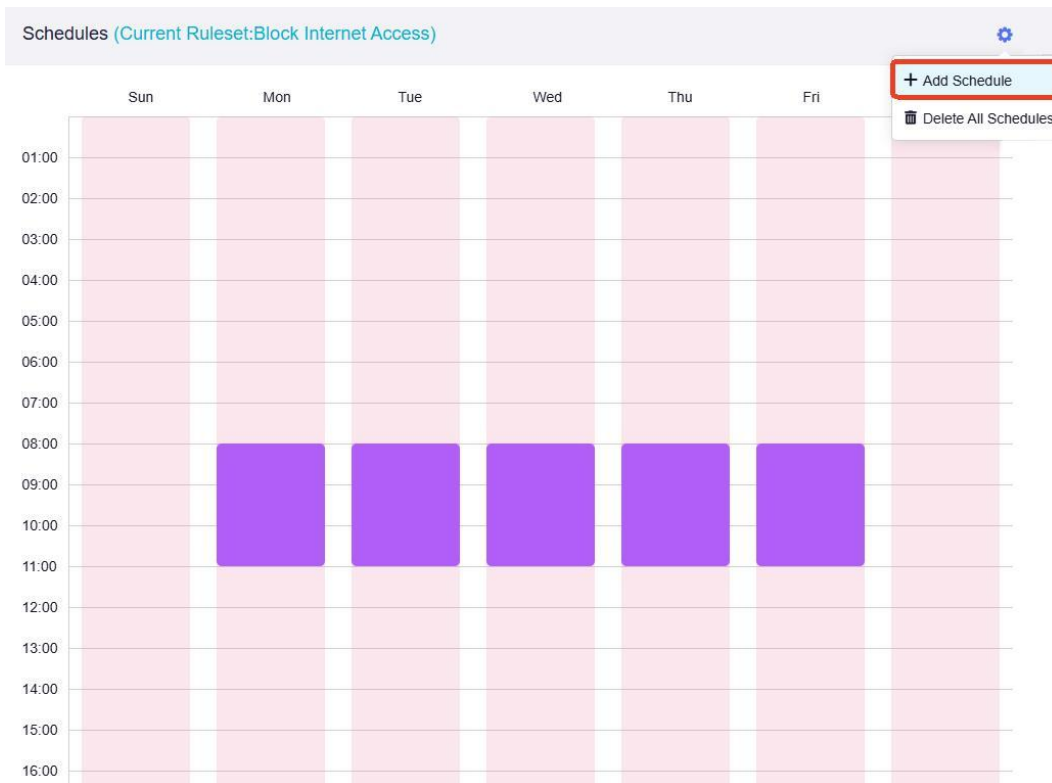
Devices

[+Manage Device](#)

 Child-phone 

Apply

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



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

Add Schedule



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

Schedule Ruleset

● Play

Execution Time

🕒 18:00

to

🕒 20:00

Execution Day(s)

Sun



Mon

Tue

Wed

Thu

Fri

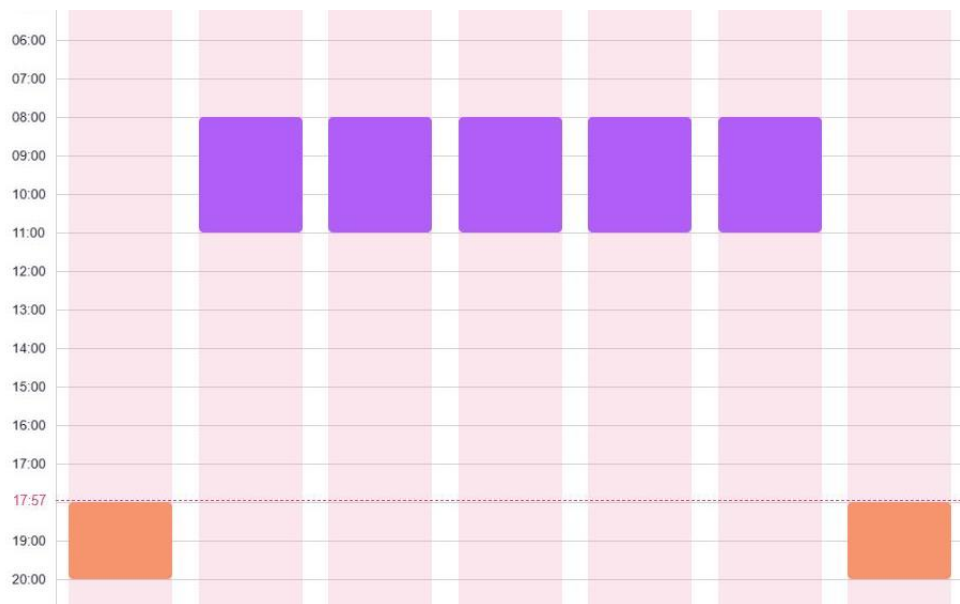
Sat



Cancel

Apply

The Play ruleset will then be added into the schedule.



Tips:

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

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

Parental Control / Modify Profile Beta



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

Rule Name

Home

Default Ruleset

Block Internet Access

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

Profiles



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

Add

Home (1)



Name



Child-phone

Block Internet Access



Switch to Learning after 13 Hours 58 Minutes

ruleset



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

Add

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

12.6.2 Troubleshooting

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

1. DNS cache issue.

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

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

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

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

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

12.7 ZeroTier

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

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

Note:

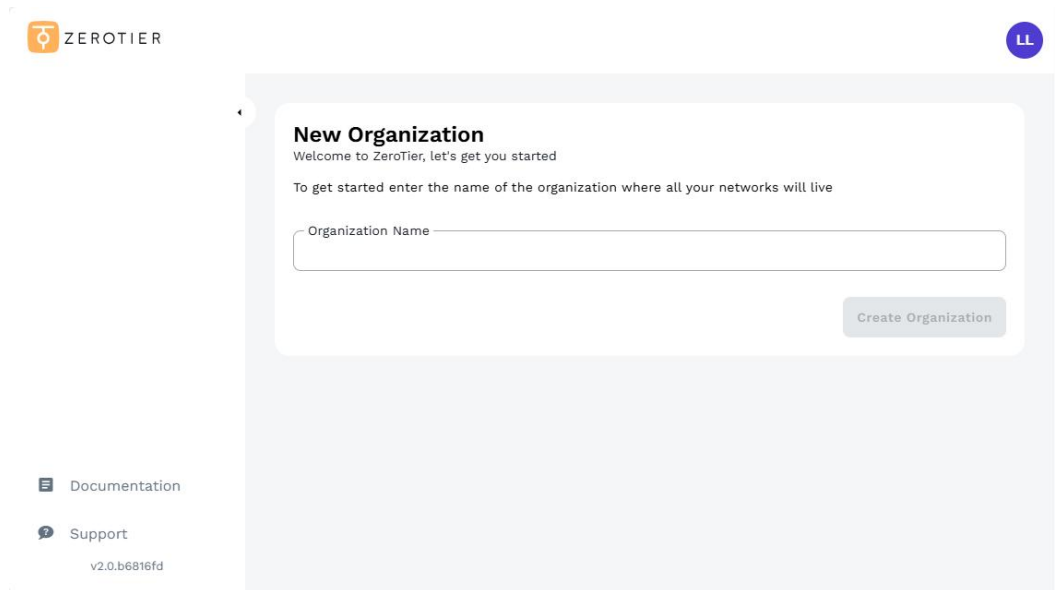
1. It is not recommended to use ZeroTier simultaneously with any of the following features or services, as this may cause routing conflicts: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, and Tailscale.
2. This feature is currently in beta, and may have some bugs.

12.7.1 Set Up ZeroTier

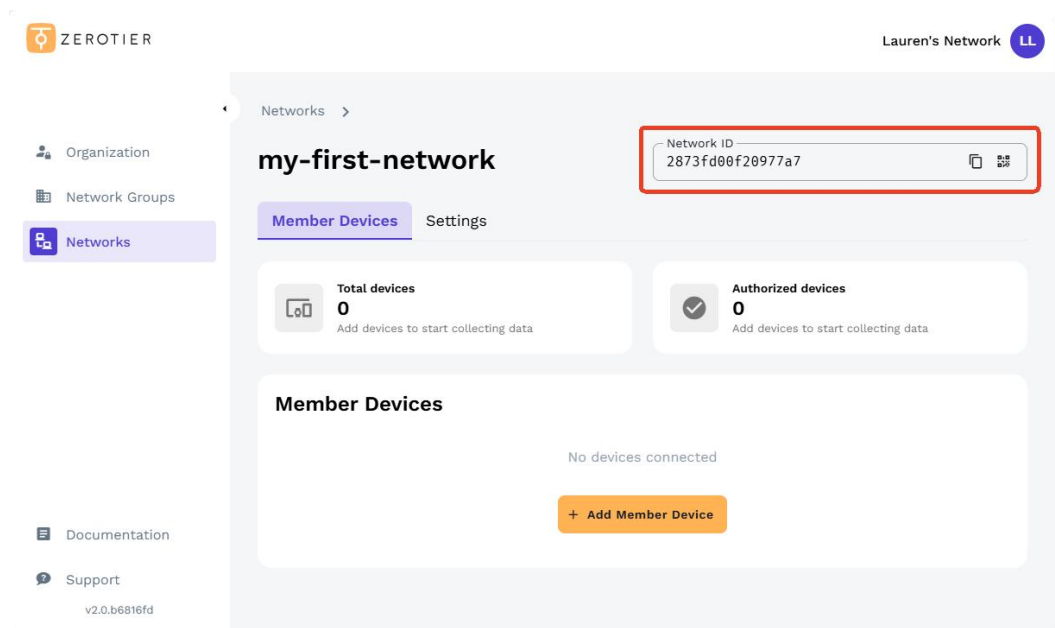
Two versions of ZeroTier Central are available: New Central and Legacy Central.

The following steps use New Central as an example.

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



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



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

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

The screenshot shows the ZeroTier configuration page in a router's admin panel. At the top, there's a header with 'ZeroTier' and a 'Beta' badge. Below this, two informational boxes describe ZeroTier's capabilities. The main configuration area includes three toggle switches: 'Enable ZeroTier' (which is turned on and highlighted with a red arrow), 'Allow Remote Access WAN' (turned off), and 'Allow Remote Access LAN' (turned off). Below these is a 'Network ID' field containing the alphanumeric string '2873fd00f20977a7', with a red arrow pointing to it. At the bottom of the configuration section is a blue 'Apply' button, also highlighted with a red arrow.

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

This screenshot shows the ZeroTier configuration page after the 'Apply' button was clicked. The 'Enable ZeroTier' toggle remains turned on. A new yellow message box with a warning icon appears, stating: 'The device has been added to ZeroTier. Please go to ZeroTier Central to authorize the device to connect to your virtual network.' A red arrow points to the 'ZeroTier Central' link within this message. The 'Network ID' field and the 'Apply' button are no longer visible in this view.

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

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

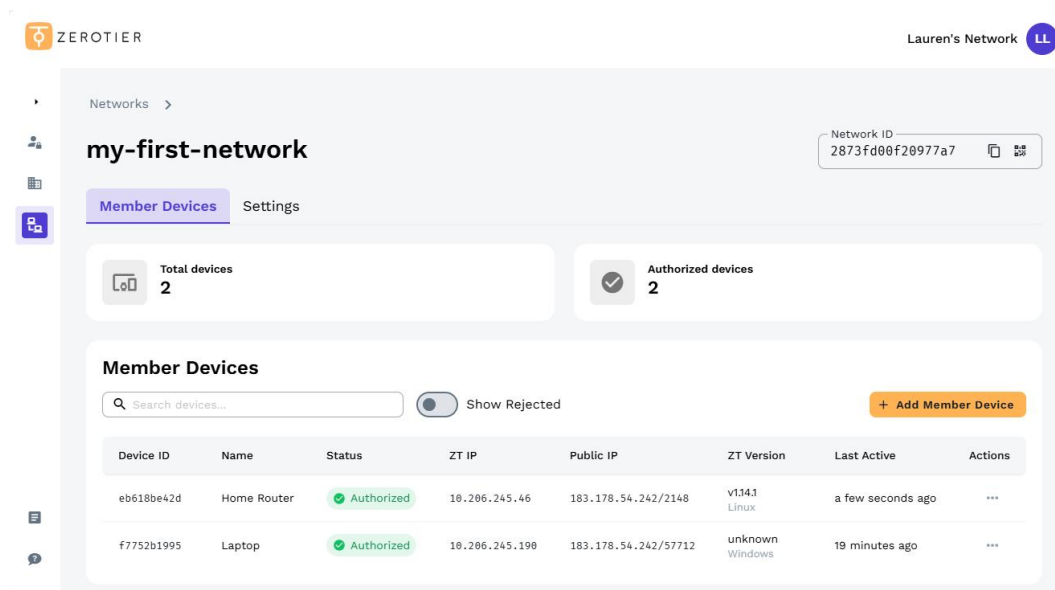
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Not Authorized		183.178.54.242/30149	unknown Linux	a few seconds ago	...

Once authorized, the page displays as follows.

The screenshot shows the ZeroTier web interface after the device has been authorized. The "Authorized devices" summary box now shows "1". The "Member Devices" table shows the device "eb618be42d" with a status of "Authorized" (green checkmark) and a ZT IP of "10.206.245.46".

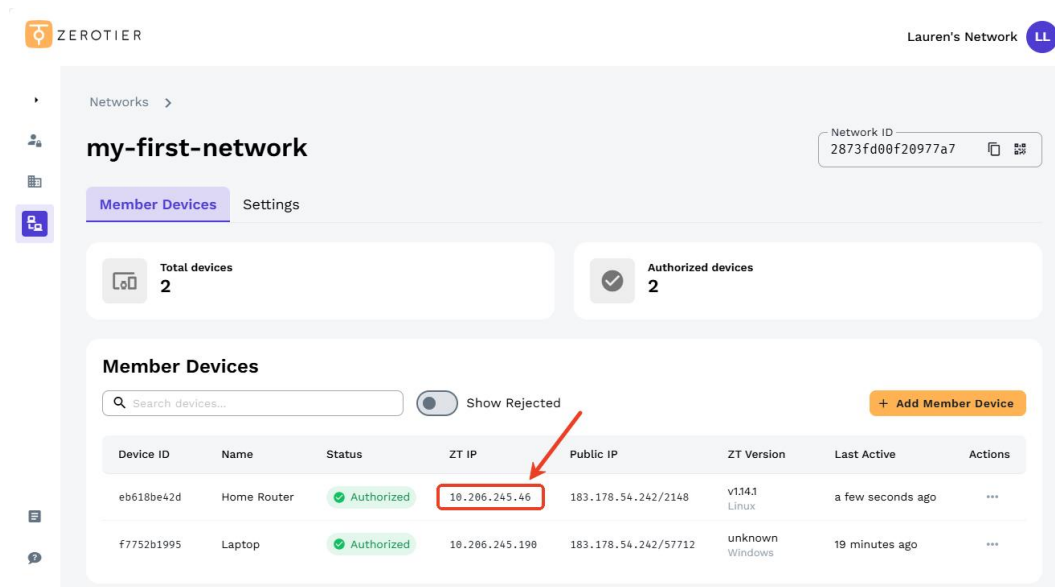
Device ID	Name	Status	ZT IP	Public IP	ZT Version	Last Active	Actions
eb618be42d	—	Authorized	10.206.245.46	183.178.54.242/24364	V134.1 Linux	a few seconds ago	...

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



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

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



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

9. Test connectivity.

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

12.7.2 Allow Remote Access WAN

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



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

12.7.3 Allow Remote Access LAN

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

ZeroTier Beta

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

The device is connected to your ZeroTier virtual network.

Enable ZeroTier

☒

Allow Remote Access WAN ⓘ

☐

Allow Remote Access LAN ⓘ

☒

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

12.8 Tailscale

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

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

Note:

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

12.8.1 Set Up Tailscale

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.

Machines
Manage the devices connected to your tailnet. [See how to manage devices](#) [Add device](#)

Add your second device

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

1 machine

MACHINE	ADDRESSES	VERSION	LAST SEEN	
pc-20260821aatr@gmail.com	100.90.74.91	1.102.3 Windows 11 25H2	Connected	...

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

Tailscale Beta

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

Enable Tailscale

[Apply](#)

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

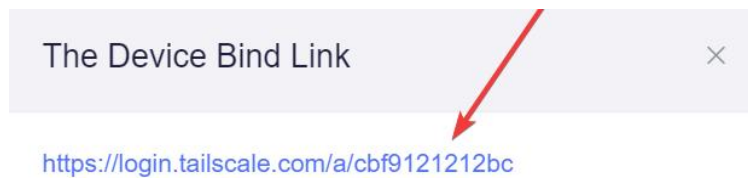
Tailscale Beta

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

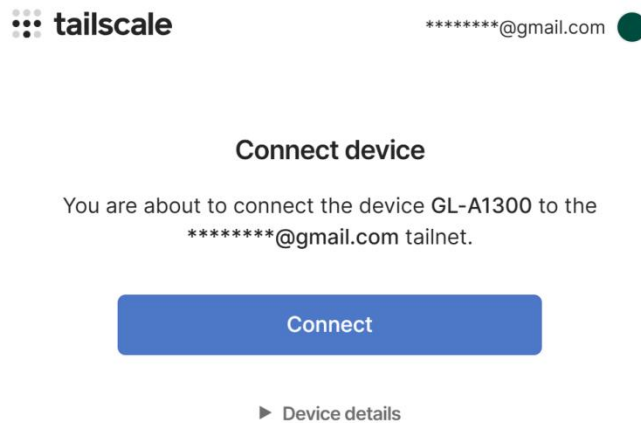
The Tailscale service is enabled, but the device is not bound yet. Please bind this device to your Tailscale account using [The Device Bind Link](#).

Enable Tailscale

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



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



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 **100.112.166.12**.

Machines
Manage the devices connected to your tailnet. [See how to manage devices](#) Add device

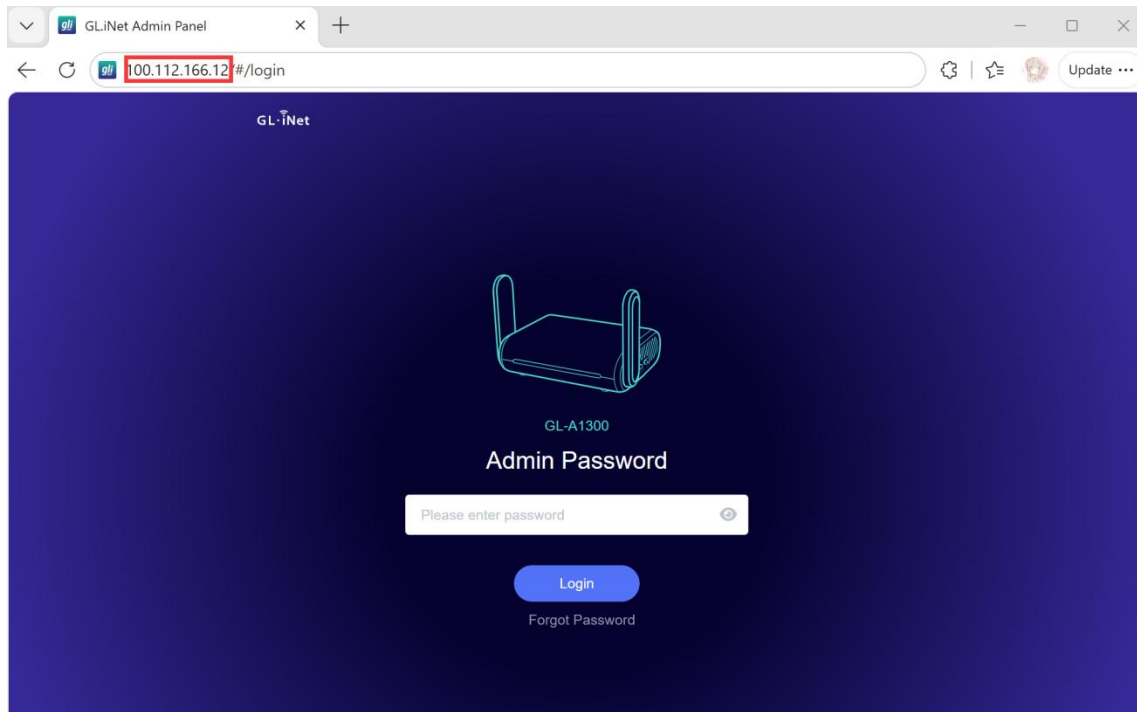
Search by name, owner, tag, version... Filters [Learn more](#) Download

2 machines

MACHINE	ADDRESSES	VERSION	LAST SEEN
gl-a1300 @gmail.com	100.112.166.12 ✓	1.80.3-1 (OpenWrt) Linux 5.4.164	Connected
pc-20260821aatr @gmail.com	100.90.74.91 ✓	1.102.3 Windows 11 25H2	Connected

7. Test connectivity.

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



12.8.2 Allow Remote Access WAN

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

Tailscale Beta

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

The device is connected to your Tailscale virtual network.

Enable Tailscale



Bind Account

@gmail.com [Unbind](#)

Router Virtual IP 

100.73.253.16

Custom Exit Node



Allow Remote Access WAN 



Allow Remote Access LAN 



Apply

12.8.3 Allow Remote Access LAN

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

Tailscale Beta

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

The device is connected to your Tailscale virtual network.

Enable Tailscale

☒

Bind Account

@gmail.com [Unbind](#)

Router Virtual IP **i**

100.73.253.16

Custom Exit Node

☐

Allow Remote Access WAN **i**

☐

Allow Remote Access LAN **i**

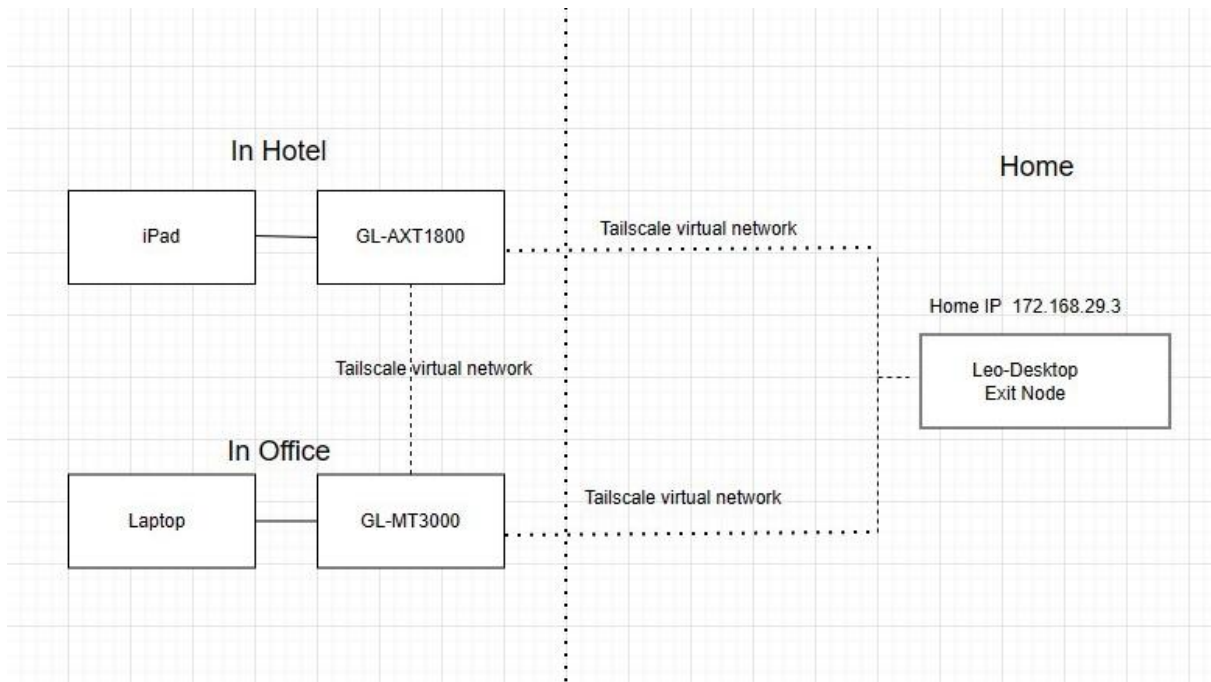
☒

Apply

12.8.4 Custom Exit Nodes

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

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



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

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

Chapter 13

Network

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

13.1 Firewall

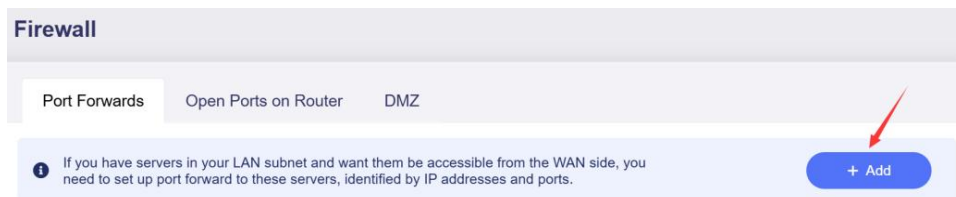
Firewall is a network feature that routes external requests to specific devices on your local network. The Firewall page includes three key functions: **Port Forwards** (for targeted access to specific ports of devices), **Open Ports on Router** (for access to services running on the router itself) and **DMZ** (for direct full access to a single device).

13.1.1 Port Forwards

Port Forwards 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 forwards, follow the steps below.

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

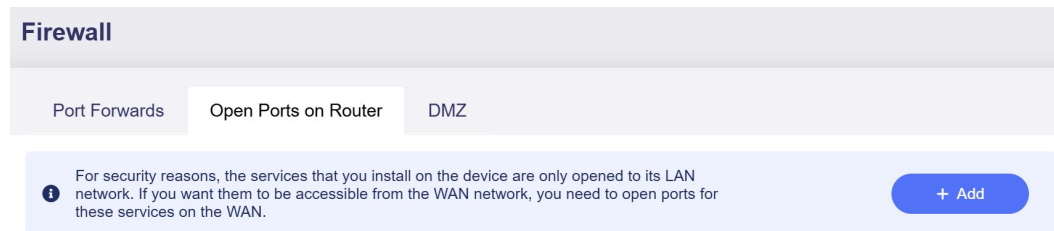
A screenshot of a 'Add New Port Forward Rule' pop-up window. The window has a title bar 'Add New Port Forward Rule'. Inside, there are several form fields: 'Name' (text input), 'Protocol' (dropdown menu showing 'TCP/UDP'), 'External Zone' (dropdown menu showing 'WAN'), 'External Port' (text input), 'Internal Zone' (dropdown menu showing 'LAN'), 'Internal IP' (dropdown menu), 'Internal Port' (text input), and 'Enable' (toggle switch, currently turned on). At the bottom of the window, there are two buttons: 'Cancel' and 'Apply'. The 'Apply' button is highlighted with a blue background.

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

13.1.2 Open Ports on Router

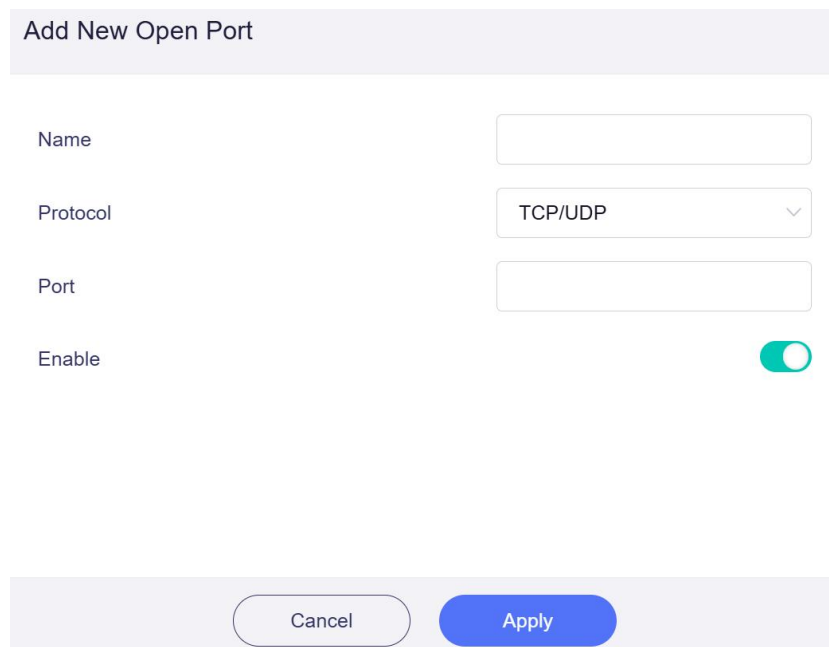
The router's services, such as web and FTP, requires their respective ports to be opened on the router in order to be publicly reachable.

To open a port, switch to the Open Ports on Router tab, then click Add.



The screenshot shows the 'Firewall' configuration page. At the top, there are three tabs: 'Port Forwards', 'Open Ports on Router' (which is selected), and 'DMZ'. Below the tabs, there is a light blue informational box with an information icon and text: 'For security reasons, the services that you install on the device are only opened to its LAN network. If you want them to be accessible from the WAN network, you need to open ports for these services on the WAN.' To the right of this box is a blue button with a white plus sign and the text '+ Add'.

In the pop-up window, open a new port and click Apply.



The screenshot shows the 'Add New Open Port' pop-up window. It has a title bar 'Add New Open Port'. Inside, there are four fields: 'Name' with an empty text input box; 'Protocol' with a dropdown menu showing 'TCP/UDP'; 'Port' with an empty text input box; and 'Enable' with a toggle switch that is currently turned on (green). At the bottom of the window, there are two buttons: 'Cancel' and 'Apply'.

- **Name:** The name of the rule which can be specified by the user.
- **Protocol:** The protocol used, you can choose TCP, UDP, or both TCP and UDP.
- **Port:** The port number that you want to open.
- **Enable:** Enable or disable the rule.

13.1.3 DMZ

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

Follow the steps below to enable DMZ if needed.

1. Log in to your router's web admin panel and navigate to **NETWORK > Firewall > DMZ** section.
2. Toggle on **Enable DMZ**, then select the **DMZ Host IP** from the drop-down list. The selected device receives all inbound packets. Click **Apply** to save the settings.

Firewall

Port ForwardsOpen Ports on RouterDMZ

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

If you enable DMZ, your port forward and port open rules will not take effect.

Enable DMZ

☒

DMZ Host IP

192.168.18.218

Apply

13.2 Multi-WAN

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

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

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

13.2.1 Interface Status Track

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

Interface Status Track



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



Ethernet



Repeater



Tethering



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

Ethernet Status Track

Enable Interface Status Track ⓘ



Low Data Mode ⓘ



Track Command

ping



IPv4 Track IP

1.1.1.1

8.8.8.8

208.67.222.222

208.67.220.220

Cancel

Apply

- **Enable Interface Status Track:** It is enabled by default. If disabled, the router will determine the interface status based on physical conditions (e.g., whether the Ethernet cable is plugged in).
- **Low Data Mode:** Enable the switch to track only when there is an interface network error, and recommend users to use Low Data Mode when you are on a limited data plan.
- **Track Command:** The ping command is used to monitor connection status to the destination IP and verify interface availability.
- **IPv4 Track IP:** Customize the IPv4 Track IP addresses if needed.

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

Interface Status Track



Sensitivity Options



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

• Ethernet

ping



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.

Sensitivity Options



This sensitivity determines the time interval for Internet status detection. It is recommended to use low sensitivity when Internet access is unstable to avoid frequent network switching; it is recommended to use high sensitivity when video or live streaming to ensure that you can switch Internet access quickly; switching to high sensitivity may result in network disconnection. Please adjust it with caution.

Sensitivity

Customize



Interval Time



3

Seconds

Cancel

Apply

13.2.2 Multi-WAN Mode

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

Failover

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

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

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



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

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

Mode ⓘ

Failover

Load Balance

Interface Priority

1

Ethernet



2

Repeater



3

Tethering



Apply

Load Balance

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

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

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

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

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

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

Mode **i**

Failover Load Balance

Load Ratio

Ethernet	1
Repeater	1
Tethering	1

Apply

You can also customize the load ratio if needed. For example, if Ethernet has a bandwidth of 100 Mbps, Repeater has 200 Mbps, and no Tethering connection are active, set the load

ratios to 1 for Ethernet, 2 for Repeater, and 0 for Tethering. 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.

13.3 LAN

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

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

13.3.1 Basic Settings

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

LAN

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

Router IP Address 

192.168.8.1

Netmask

255.255.255.0 

Apply

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

13.3.2 DHCP Server

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

DHCP Server

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

Enable ☒

Start IP Address

End IP Address

[Advanced](#)

[Apply](#)

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

Start IP Address

End IP Address

[Advanced](#)

[Apply](#)

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

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

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

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

13.3.3 Address Reservation

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

Follow the steps below to configure address reservation if needed.

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

Add a New Reservation Entry

MAC

IP

192.168.8.223

Description

Lauren-iPhone

Cancel

Submit

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

Address Reservation

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

Add

MAC	IP	Description	Action
	192.168.8.223	Lauren-iPhone	...

13.4 Guest Network

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

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

13.4.1 Basic Settings

The basic settings include Gateway, Netmask, and AP Isolation.

Guest Network

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

Gateway

192.168.9.1

Netmask

255.255.255.0 

Security Settings

AP Isolation 



Apply

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

13.4.2 DHCP Server

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

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

DHCP Server

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

Enable 

Start IP Address

End IP Address

[Advanced](#)



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

Start IP Address

End IP Address

  [Advanced](#)

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

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

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

13.5 DNS

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

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

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

13.5.1 General Settings

DNS

 If you set custom DNS servers, any domain names will be resolved through the DNS servers set here rather than the one obtained from Ethernet, Repeater, Cellular, Tethering or VPN configuration DNS servers.

DNS Rebinding Attack Protection 



Override DNS Settings for All Clients 



DNS Server Settings

Mode

Automatic



DNS from Ethernet

10.100.20.50,10.100.23.100

Apply

- **DNS Rebinding Attack Protection:** Protects against DNS rebinding attacks by blocking malicious DNS resolution attempts. Note that enabling it may cause private DNS lookup failure; disable if your network uses a captive portal (e.g., public Wi-Fi login pages).
- **Override DNS Settings of All Clients:** If enabled, all connected devices will be forced to use the DNS servers configured on the router, ignoring their own original DNS settings. It enables unified DNS configuration for all devices.

13.5.2 DNS Server Settings

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

The screenshot shows the 'DNS Server Settings' section. The 'Mode' dropdown menu is open, displaying four options: 'Automatic' (highlighted in blue), 'Encrypted DNS', 'Manual DNS', and 'DNS Proxy'. Below the settings, there is an 'Apply' button.

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

The screenshot shows the 'DNS Server Settings' section. The 'Mode' dropdown menu is set to 'Automatic'. Below it, the 'DNS from Repeater' field is set to '192.168.18.1'.

2. **Encrypted DNS:** When selected, the router will use encrypted protocols to process DNS queries, securing resolution data against eavesdropping or tampering. It has four encryption types: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS, and Oblivious DNS over HTTPS.

DNS Server Settings

Mode

Encrypted DNS

Encryption Type

DNS over TLS

DNS Provider

DNS over TLS

DNSCrypt-Proxy

DNS over HTTPS

Oblivious DNS over HTTPS

Apply

- For DNS over TLS, select a DNS provider among Control D, NextDNS, and Cloudflare.
 - For the other three (i.e., DNSCrypt-Proxy, DNS over HTTPS, and Oblivious DNS over HTTPS), select at least one DNS server from the repository. Up to 8 servers can be selected. When multiple servers are selected, the router will use the fastest one automatically.
3. **Manual DNS:** When selected, you can customize your router's DNS servers. Click DNS Server 1 and choose a DNS server from the drop-down list. The remaining DNS fields will update automatically.

DNS Server Settings ⓘ

Mode

Manual DNS

DNS Server 1

DNS Server 2

Optional

DNS Server 3

Optional

DNS Server 4

Optional

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

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

DNS Server Settings ⓘ

Mode

DNS Proxy ▼

Proxy Server Address

8.8.8.8#53

13.5.3 Edit Hosts

You can define static DNS resolution rules if needed.

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

DNS Edit Hosts

ⓘ If you set custom DNS servers, any domain names will be resolved through the DNS servers set here rather than the one obtained from Ethernet, Repeater, Cellular, Tethering or VPN configuration DNS servers.

DNS Rebinding Attack Protection ⓘ

☐

Override DNS Settings for All Clients ⓘ

☐

DNS Server Settings

Mode

Automatic ▼

DNS from Ethernet

10.100.20.50,10.100.23.100

Apply

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

Edit Hosts

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

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

Cancel

Apply

13.6 Network Mode

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

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

Network Mode

 When you change the router's network mode, you may need to reconnect all of your client devices.
When you use Access Point / WDS, you will not be able to connect to this UI again. You can press and hold the reset button for 4 seconds to revert to router mode. [Learn More](#)

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

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

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

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

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

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

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

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

Note:

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

13.7 IPv6

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

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

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

IPv6

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

Enable



LAN

Mode

NAT6

DNS acquisition method

Automatic

Apply

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

13.7.1 IPv6 Mode

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

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

13.7.2 DNS Acquisition Method

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

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

13.8 MAC Address

The MAC Address page displays the router's default MAC address, clone a client's MAC address, enter a MAC address manually, or generate a random MAC address. If the device supports setting multiple Ethernet ports to be used as WAN ports, you can set the MAC address for each port separately. Note that the MAC address setting is only valid when the Ethernet port is used as a WAN port.

MAC Address



When you connect to a public hotspot, use a random MAC address if you do not want the hotspot to know your real MAC address or to limit your access to the Internet based on it. If your hotel or other business location's network requires authentication, you may need to use the MAC cloning. [Learn More >](#)

Mode

Factory Default

Clone

Manual

MAC Address (Ethernet)

94:83:C4:XX:XX:XX

MAC Address (Repeater)

Generated when the interface is enabled

Apply

- **The factory default MAC address.**

Mode

Factory Default

Clone

Manual

MAC Address (Ethernet)

94:83:C4:XX:XX:XX

MAC Address (Repeater)

Generated when the interface is enabled

- **Clone a client's MAC address.**

Mode	Factory Default Clone Manual
MAC Address	
MAC Address (Ethernet)	
MAC Address (Repeater)	

Note: Many new devices now use a different random MAC address to connect to different Wi-Fi, so the MAC address shown here may not be the actual MAC address of the user's device. The randomized MAC may also be called a Private Wi-Fi Address or a random hardware address on different devices.

- **Manual input or generate a random MAC address.**

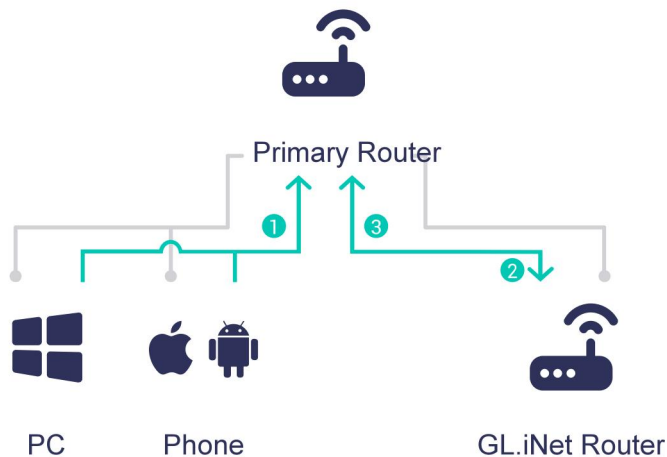
Mode	Factory Default Clone Manual
MAC Address	B6:6C:F7:E3:76:D1 Random
MAC Address (Ethernet)	B6:6C:F7:E3:76:D1
MAC Address (Repeater)	B6:6C:F7:E3:76:D1

13.9 Drop-in Gateway

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

- Filter advertisements via AdGuard Home
- Enable VPN client
- Use encrypted DNS

Drop-in Gateway operates as an intermediate network system, routing data traffic from client devices through the GL.iNet router for processing before transmitting it via the primary router. During this process, it not only preserves existing network settings to ensure uninterrupted connectivity for all connected devices, but also allows you to manage network traffic for all or specific client devices if needed.



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

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

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

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

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

Enable Drop-in Gateway Mode ⓘ 

IP Address	10.100.211.149
Netmask	0.0.0.0
Gateway	10.100.208.1
DNS Server 1	10.100.208.1
DNS Server 2	Optional

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

Configuration method

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

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

13.10 IGMP Snooping

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

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

IGMP Snooping

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

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

Enable



Version

3



Apply

13.11 NAT Settings

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

NAT Settings

Enable Full Cone NAT ⓘ

☐

Enable SIP ALG ⓘ

☐

Apply

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

Chapter 14

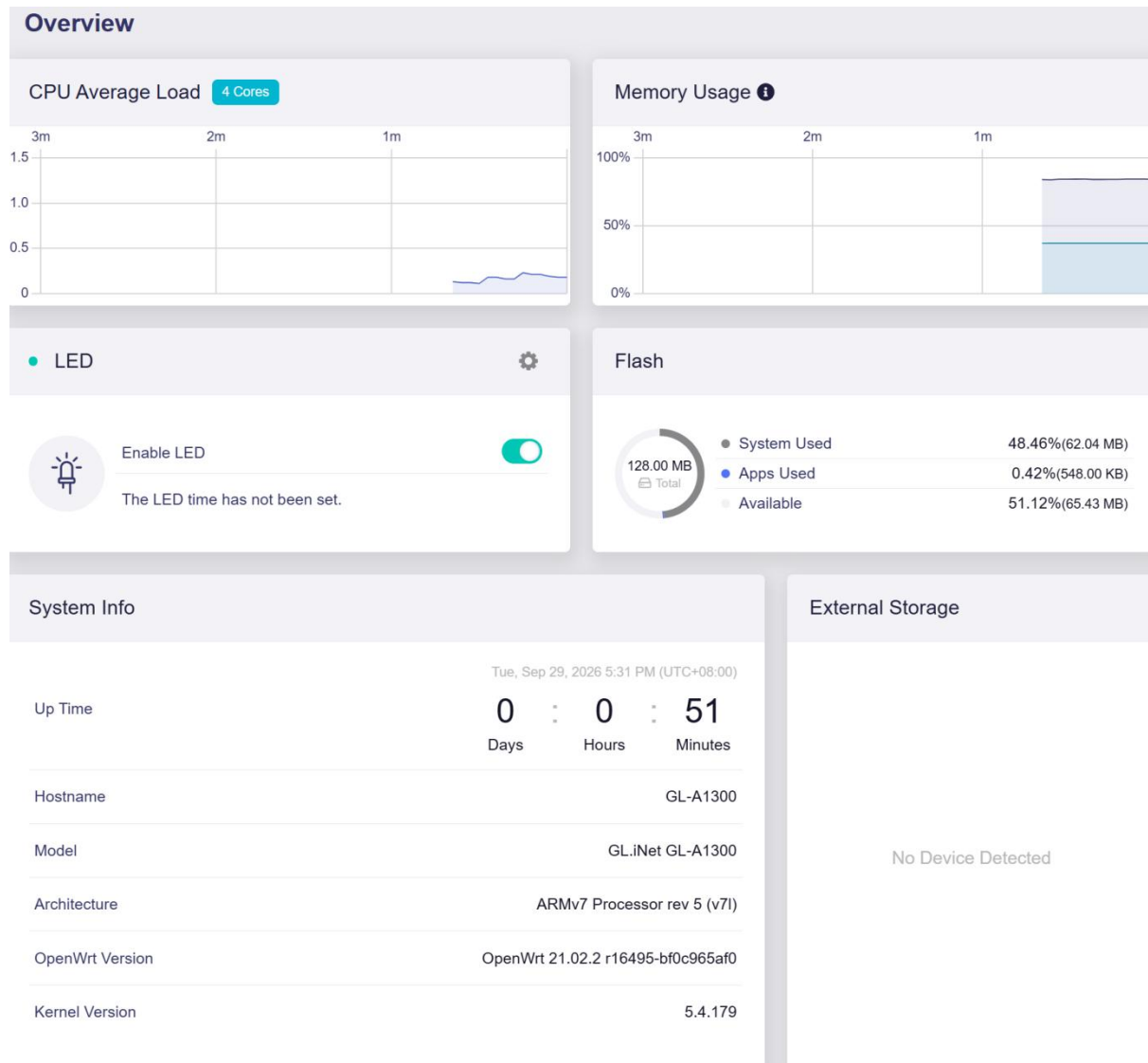
System

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

14.1 Overview

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

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



14.2 Upgrade

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

14.2.1 Online Upgrade

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

Upgrade

Online Upgrade

Local Upgrade

✓ Firmware is up-to-date.

Current Firmware

Version	4.5.22
Firmware Type	release1
Compile Time	2025-04-08 08:48:05 (UTC+00:00)

Preview Version

Accept Preview Plan ⓘ ☐

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

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).

14.2.2 Local Upgrade

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

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

Upgrade

Firmware Online Upgrade

Firmware Local Upgrade



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

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

Firmware Verification

Version	4.5.22 Release Notes
Firmware Type	release1
SHA256	ef25c2803d1b0e727748c3aeeb5c4aa950066fedfa18cb171ca3f4f0180cf5bd
Verification Result	Pass
Keep Settings 	☒

Install

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

14.3 Scheduled Tasks

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

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

14.3.1 LED Display Schedule

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

LED Display Schedule

Enable Scheduled



Turn On Time

 07:00

Turn Off Time

 22:00

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

Apply

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

14.3.2 Schedule Reboot

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

Schedule Reboot

Enable Scheduled



Reboot Time

 03:00

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

Apply

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

14.3.3 5GHz Wi-Fi Schedule

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

Mode 1: Turn On/Off

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

5 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off

Enable Main Wi-Fi Schedule

☐

Enable Guest Wi-Fi Schedule

☐

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

Enable Main Wi-Fi Schedule

☒

Main Wi-Fi

Turn On Time

07:00

Turn Off Time

22:00

day(s)

Su

Mo

Tu

We

Th

Fr

Sa

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

Enable Guest Wi-Fi Schedule 

Guest Wi-Fi

Turn On Time

Turn Off Time

day(s) Su Mo Tu We Th Fr Sa

Mode 2: Switch TX Power

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

5 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Enable Main Wi-Fi Schedule 

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

Enable Main Wi-Fi Schedule 

Main Wi-Fi

Switch Set to

Restore Set to

day(s) Su Mo Tu We Th Fr Sa

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

14.3.4 2.4GHz Wi-Fi Schedule

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

Mode 1: Turn On/Off

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

2.4 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Turn On/Off

Enable Main Wi-Fi Schedule



Enable Guest Wi-Fi Schedule



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

Enable Main Wi-Fi Schedule



Main Wi-Fi

Turn On Time

07:00

Turn Off Time

22:00

day(s)



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

Enable Guest Wi-Fi Schedule 

Guest Wi-Fi

Turn On Time

Turn Off Time

day(s) Su Mo Tu We Th Fr Sa

Mode 2: Switch TX Power

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

2.4 GHz Wi-Fi Status Schedule

Wi-Fi Scheduled Mode

Enable Main Wi-Fi Schedule 

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

Enable Main Wi-Fi Schedule 

Main Wi-Fi

Switch Set to

Restore Set to

day(s) Su Mo Tu We Th Fr Sa

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

14.4 Time Zone

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

Time Zone

Router Time

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

Etc/GMT-8

Apply

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

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

Sync

Router Time

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

UTC

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

Router Time

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

Etc/GMT-8

Etc/GMT-7

Etc/GMT-8

Etc/GMT-9

Etc/GMT-10

14.5 Toggle Button Settings

Log in to your router's web admin panel and navigate to **SYSTEM > Toggle Button Settings**. This page allows you to customize the function of the router's physical toggle switch (located on the side) for easier use.

Toggle Button Settings

LEFT





RIGHT



Toggle Button Function(On/Off)

No Function

Apply

By default, the toggle switch is not assigned any functions. You can customize it if needed to turn specific functions on or off with a single flip.

Toggle Button Settings

LEFT





RIGHT



Toggle Button Function

No Function

Apply

No Function

AdGuard Home (On/Off)

OpenVPN Client (On/Off)

Tor (On/Off)

WireGuard Client (On/Off)

14.6 Log

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

Log

Export Log

System Log

Kernel Log

Crash Log

Cloud Log

Nginx Log

Refresh

WORKGROUP<1d>.

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: This response was from IP 10.100.211.230, reporting an IP address of 10.100.211.230.

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: [2026/09/29 17:24:57.475569, 0]

.././source3/nmbd/nmbd_become_dmb.c:237(become_domain_master_query_success)

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: become_domain_master_query_success:

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: There is already a domain master browser at IP 10.100.211.230 for workgroup WORKGROUP registered on subnet 10.100.211.199.

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: [2026/09/29 17:24:57.476529, 0] .././source3/nmbd/nmbd_namequery.c:109(query_name_response)

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: query_name_response: Multiple (2) responses received for a query on subnet 10.100.211.199 for name WORKGROUP<1b>.

Tue Sep 29 17:24:57 2026 daemon.err nmbd[24657]: This response was from IP 10.100.211.230, reporting an IP address of 10.100.211.230.

Tue Sep 29 17:29:57 2026 daemon.err nmbd[24657]: [2026/09/29 17:29:57.504812, 0]

.././source3/nmbd/nmbd_become_dmb.c:294(become_domain_master_browser_bcast)

Tue Sep 29 17:29:57 2026 daemon.err nmbd[24657]: become_domain_master_browser_bcast:

Tue Sep 29 17:29:57 2026 daemon.err nmbd[24657]: Attempting to become domain master browser on workgroup WORKGROUP on subnet 10.100.211.199

Tue Sep 29 17:29:57 2026 daemon.err nmbd[24657]: [2026/09/29 17:29:57.506468, 0]

.././source3/nmbd/nmbd_become_dmb.c:307(become_domain_master_browser_bcast)

Tue Sep 29 17:29:57 2026 daemon.err nmbd[24657]: become_domain_master_browser_bcast: querying subnet 10.100.211.199 for domain master browser

- **Refresh:** Click this button to refresh logs.
- **Export Log:** Click this button to export debug info along with the logs.

14.7 Security

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

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

14.7.1 Admin Password

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

Admin Password

Old Password

Enter old password

New Password

Enter new password

Confirm Password

Enter new password again

Apply

The requirements for the admin password are as follows:

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

14.7.2 Local Access Control

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

Local Access Control

HTTP Port

80

HTTPS Port

443

Force HTTPS

☐

SSH Port

22

Auto-Logout Time ⓘ

5

Minutes

Apply

Admin Panel

- **HTTP Port:** Defaults to 80, used for unencrypted HTTP access to the web admin panel.
- **HTTPS Port:** Defaults to 443, used for secure HTTPS access to the web admin panel.
- **Force HTTPS:** When enabled, access to the web admin panel is enforced to use a secure HTTPS connection.
- **SSH Port:** Defaults to 22, the port used for SSH access to the router.
- **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.

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".

This port is forbidden by the browser [Learn More](#)

HTTP Port	22
HTTPS Port	22

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.

14.7.3 Remote Access Control

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

Remote Access Control

Allow Ping from WAN

HTTPS Remote Access

SSH Remote Access

Allow Remote Access only from Specific IPs

Apply

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

Allow Remote Access only from Specific IPs

IP Address List

+ Add an IP Address

192.168.8.1

example

...

14.8 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 if needed.

Reset Firmware

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

Delete All and Reboot

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

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

14.9 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 the access link, and you will be re-directed to the LuCI login page.

Advanced Settings



You can modify advanced settings with LuCI, the default web user interface of OpenWrt. LuCI is an open and independent project maintained by OpenWrt.

It is provided as is. GL.iNet is not responsible for LuCI maintenance.

192.168.8.1/cgi-bin/luci

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

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

You will then log in to the LuCI interface.

GL-A1300		Status ▾	System ▾	Network ▾	Logout	REFRESHING
Status						
System						
Hostname	GL-A1300					
Model	GL.iNet GL-A1300					
Architecture	ARMv7 Processor rev 5 (v7l)					
Target Platform	ipq40xx/generic					
Firmware Version	OpenWrt 21.02.2 r16495-bf0c965af0 / LuCI openwrt-21.02 branch git-22.347.45520-d30ab74					
Kernel Version	5.4.179					
Local Time	2026-09-29 17:44:16					
Uptime	1h 4m 22s					
Load Average	0.50, 0.43, 0.37					