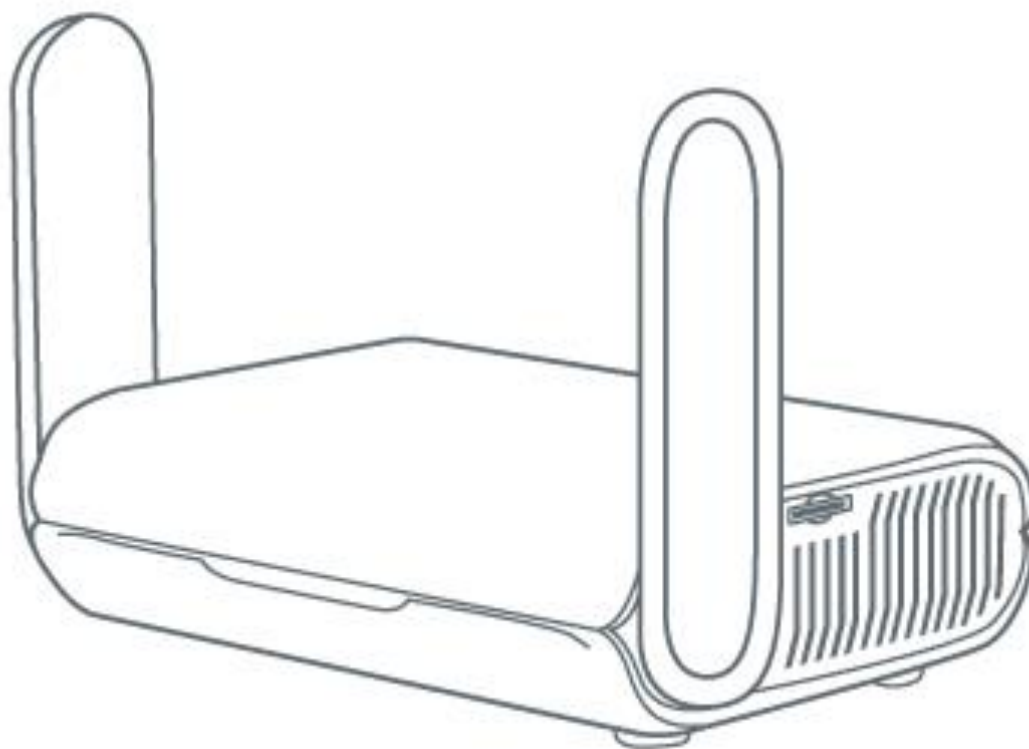


GL·iNet



Beryl AX

(GL-MT3000)

USER MANUAL

Table of Contents

1. Hardware info	1
1.1. Specification	2
1.2. PCB Pinout	3
2. First time setup	4
2.1 Connect to the Internet via an ethernet cable.....	8
Protocol.....	8
2.2 Connect to the Internet via an existing Wi-Fi by Repeater	11
Basic steps	11
Join network advanced setting.....	14
Repeater options	15
Manage known network.....	16
Join other network	18
Reconnection.....	18
2.3 Connect to the Internet via usb tethering	19
2.4 Connect to the Internet via cellular.....	22
3. Wireless.....	27
Main WiFi.....	27
Guest WiFi.....	29
4. CLIENTS	30
Blocking client.....	30
Limiting speed	30
Remove offline clients.....	31
5. Firmware Upgrade	32
Online Upgrade	32
Local Upgrade.....	32
6. FIREWALL.....	35
Port Forwards.....	35
Open Ports on Router.....	37
DMZ	38
7. VPN.....	39
7.1 VPN Dashboard	39

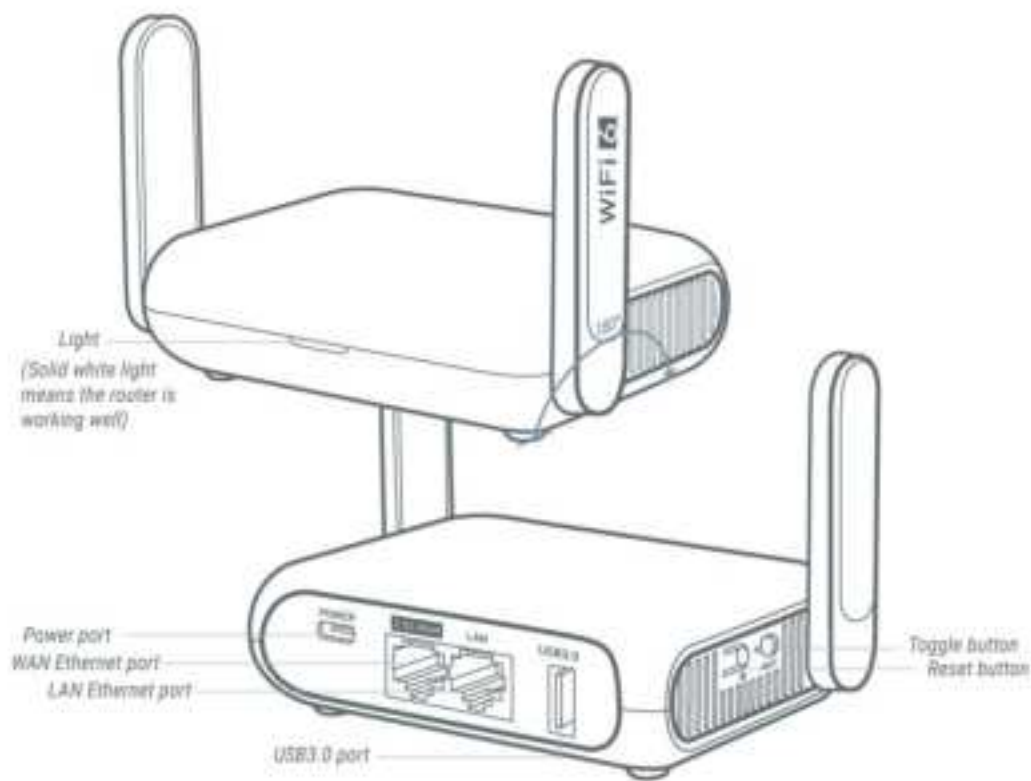
VPN Client.....	40
VPN Client Options.....	41
Proxy mode	44
Global Options.....	45
VPN Server	46
OpenVPN Server Options	46
OpenVPN Server Route Rule	47
WireGuard Server Options.....	47
WireGuard Server Route Rule.....	48
Global Options of Server	48
Global Options of VPN Server¶.....	48
OpenVPN.....	50
7.2 How to Setup OpenVPN Client on GL.iNet router	50
Setup NordVPN.....	50
Setup OpenVPN client	55
Setup OpenVPN server on GL.iNet router	58
Get configuration files from OpenVPN service providers¶.....	58
7.3 Setup OpenVPN Server on GL.iNet router	59
Make sure Internet Service Provider assigns you a public IP address	59
Network Topology	59
Setup OpenVPN Server.....	60
To check if OpenVPN Server is working properly	63
Advanced Configuration	65
OpenVPN Client App.....	66
WireGuard	66
7.4 How to Setup WireGaurd Client on GL.iNet router	66
Setup AzireVPN	66
Setup Mullvad.....	69
Setup WireGuard client.....	73
Setup WireGuard server on GL.iNet router	79
Get configuration files from WireGuard service providers.....	79
7.5 Setup WireGuard Server on GL.iNet router.....	80
Make sure Internet Service Provider assigns you a public IP address¶.....	80

Network Topology	80
Setup WireGuard Server.....	80
WireGuard Client App.....	86
VPN Cascading.....	88
1. APPLICATIONS.....	95
8.1 Plug-ins.....	95
8.2 Dynamic DNS.....	96
Enable DDNS.....	96
Check if DDNS is in effect	97
HTTP Remote Access.....	98
HTTPS Remote Access.....	99
SSH Remote Access.....	103
8.3 GL.iNet GoodCloud.....	105
Contents	105
Introduction	106
Setup	107
Manage your devices	114
Site to Site	122
Batch Setting	131
Template Management.....	134
Task List	138
GoodCloud and VPN.....	139
Turn off cloud	140
8.5 Network Storage.....	144
Contents	144
Introduction	144
Insert storage device.....	144
Set up Samba	145
Set up WebDAV.....	149
Set up DLNA.....	153
Samba Client.....	154
WebDAV Client.....	159
8.6 Log.....	161

2. MORE SETTINGS.....	162
9.1 Admin Password.....	162
9.2 LAN	163
Private Network	163
Reserve an IP for a client.....	165
Guest Network	165
9.3 Time Zone	168
9.4 DNS	169
DNS Server Settings.....	169
Edit Hosts.....	172
9.5 Network Mode.....	173
9.6 IPv6	174
9.7 Toggle Button Settings.....	176
9.8 Reset Firmware.....	177
9.9 Advanced Settings	178

1. Hardware info

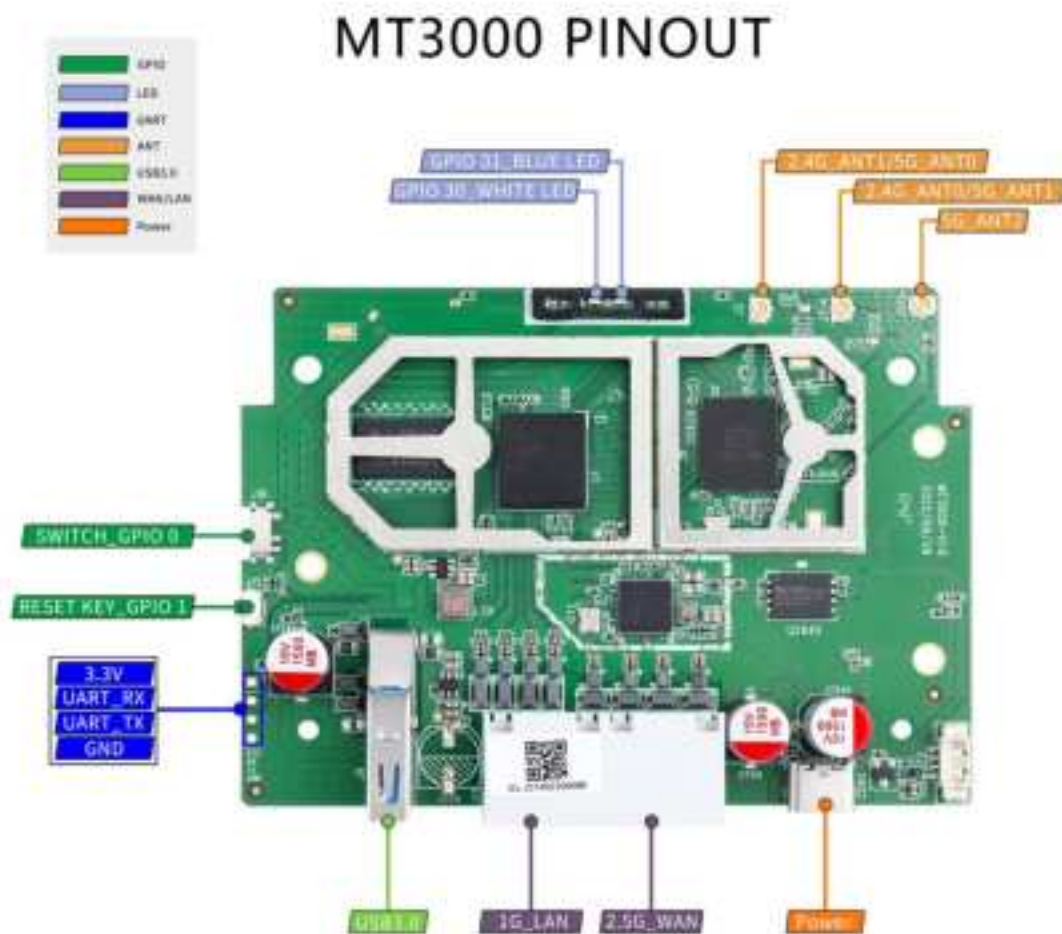
Beryl AX (GL-MT3000) is an AX3000 pocket-sized travel router that uses the Wi-Fi 6 protocol. It is an upgraded version of Beryl (GL-MT1300), it runs on MT7981B 1.3GHz dual-core processor, offering more than double the total Wi-Fi speed. It is designed to support families with heavy Wi-Fi usage, and it's also compactly designed for travel use.



1.1. Specification

Interface	1 x WAN Ethernet port 1 x LAN Ethernet port 1 x USB 3.0 port 1 x Type-C Power Input 1 x Reset button 1 x Toggle button
CPU	MT7981B Dual-core Processor @1.3GHz
Memory / Storage	DDR4 512MB / NAND Flash 256MB
Protocol	IEEE 802.11a/b/g/n/ac/ax
Wi-Fi Speed	574Mbps (2.4GHz), 2402Mbps (5GHz)
Antennas	2 x retractable external Wi-Fi antennas
Ethernet Speed	WAN Port: 10/100/1000/2500Mbps LAN Port: 10/100/1000 Mbps
Power Input	Type-C, 5V/3A
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	106 x 83 x 33mm

1.2. PCB Pinout



2. First time setup

Please prepare the following items that included in the package.

GL-MT3000, power adapter, ethernet cable.

Here is a video guide, which used GL-AXT1800(Slate AX) as a setup example:

<https://youtu.be/f7DYULL6ZSI>

Power on

Plug one end of the power adapter into the router and the other end into an outlet. It will automatically power on.

Connect to the router

You can connect to router via an ethernet cable or via Wi-Fi.

- Connect via cable

Connect your computer to the LAN port of the router via Ethernet cable.

- Connect via Wi-Fi

The SSID was printed on the bottom label of the router with the following formats:

GL-MT3000-XXX or GL-MT3000-XXX-5G

Search for the SSID of the router in your computer/phone/tablet and input the WiFi password. Please find the WiFi password on the label on the back of the router. Some models if you can't find the WiFi password on the label, please try the default password **goodlife**.

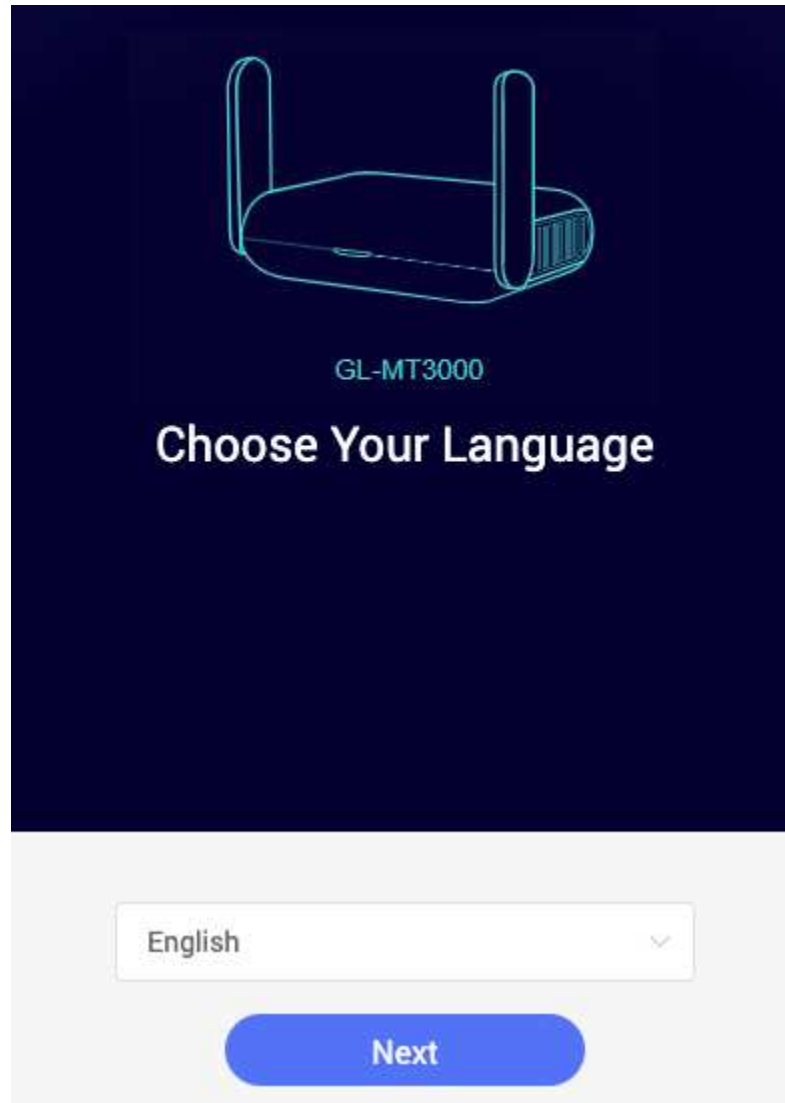
Tip: The QR code on the label on the back of the GL-MT3000 is with wifi connection information and can be quickly connected using your phone's QR code scanning tool.

Note: At this time, you cannot access the Internet after connecting to the WiFi, you need to set up the admin password in the next step before you can access the Internet.

Access the web Admin Panel

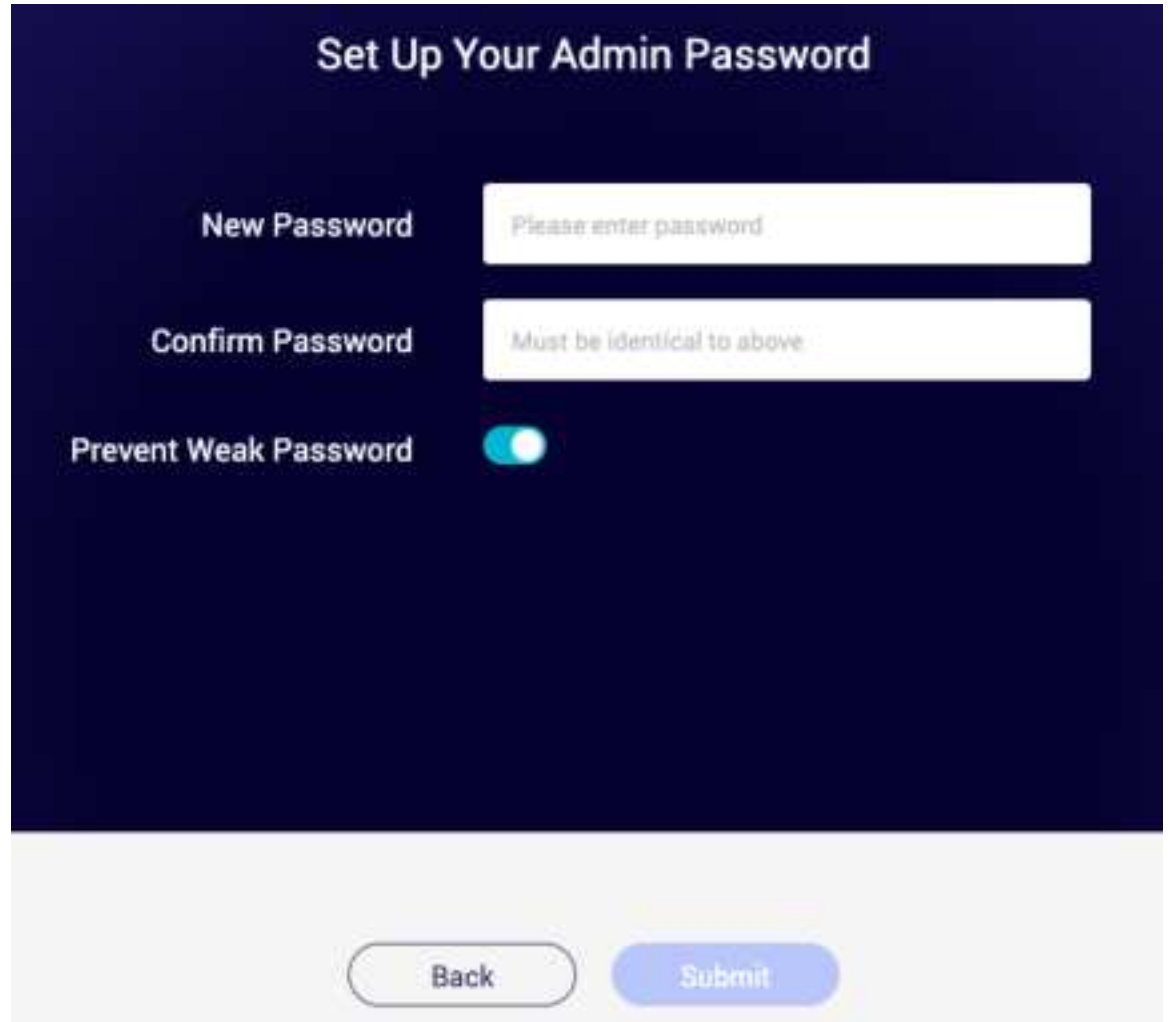
Open a web browser (we recommend Chrome, Edge, Safari) and visit <http://192.168.8.1>. You will be directed to the initial setup of the web Admin Panel.

Choose a language, and click **Next** to continue.



Set up admin password, we recommend using a strong password.
Click **Submit** to continue.

Note: Wi-Fi may turn off during the initialization, please make sure to reconnect to the router.

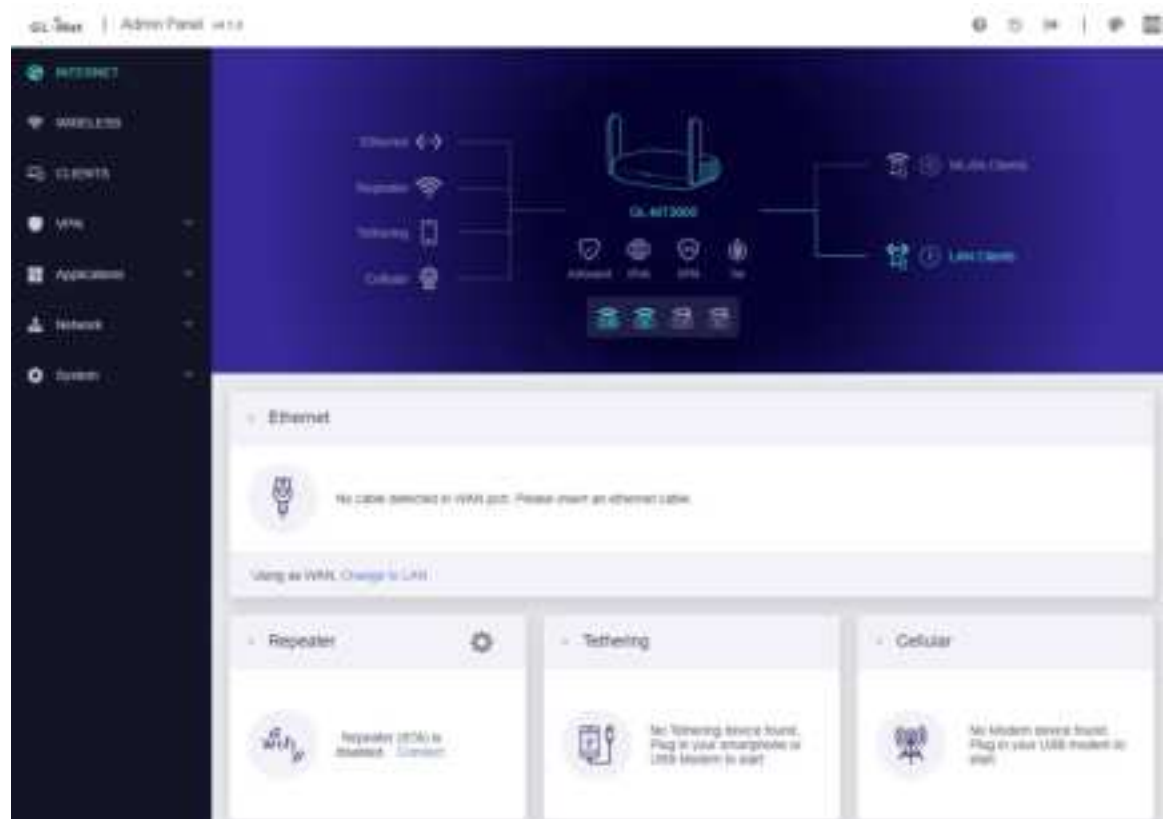


The image shows a web interface for setting an admin password. The title is "Set Up Your Admin Password". There are three main sections: "New Password" with a text input field containing the placeholder "Please enter password"; "Confirm Password" with a text input field containing the placeholder "Must be identical to above"; and "Prevent Weak Password" with a toggle switch that is currently turned on. At the bottom, there are two buttons: "Back" and "Submit".

Field	Value / State
New Password	Please enter password
Confirm Password	Must be identical to above
Prevent Weak Password	On

Buttons: Back, Submit

After the initial setup, you will enter the web Admin Panel of the router.

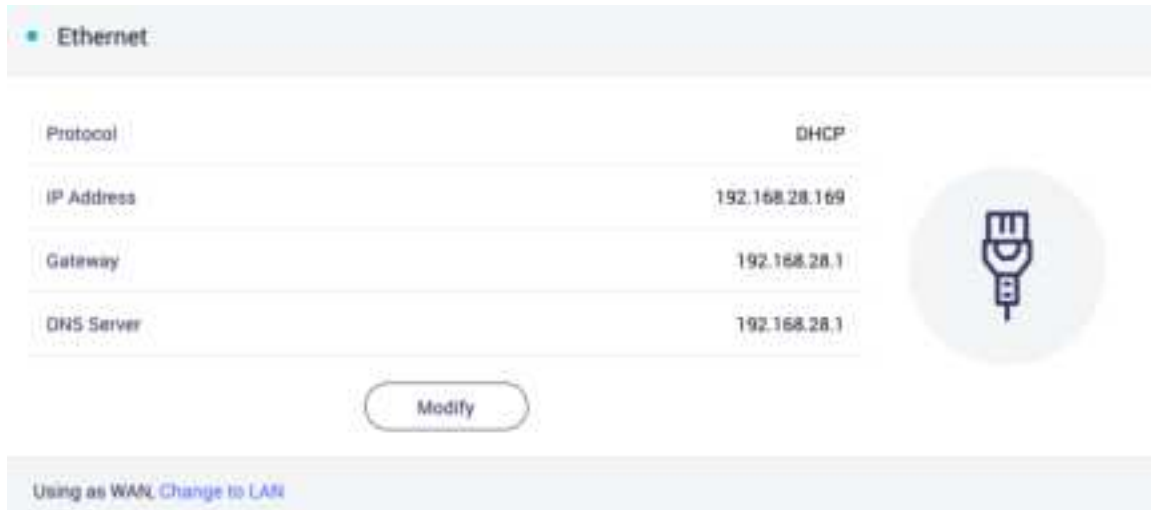


Connect to the Internet

2.1 Connect to the Internet via an ethernet cable

To access the Internet, it can connect the WAN port of router to the modem or the LAN port of other router via an ethernet cable.

On the left side of web Admin Panel -> INTERNET, Ethernet sector.



Protocol	DHCP
IP Address	192.168.28.169
Gateway	192.168.28.1
DNS Server	192.168.28.1

Modify

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

Note: Before plugging the Ethernet cable into the WAN port of the router, you can click **Change to LAN** to [set the WAN port as a LAN port](#). That is useful when you are using the router as a [repeater](#). As a result, you can have one more LAN port.

Protocol

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

- DHCP

DHCP is the default and most common protocol. It is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture.

- Static

Static is required if your Internet Service Provider (ISP) has provided a fixed IP address for you or you want to configure the

network information such as IP address, Gateway, Netmask manually.

Ethernet Settings

Protocol

DHCPStaticPPPoE

IPv4

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2

Optional

Cancel

Apply

- PPPoE
PPPoE is required by many Internet Service Providers (ISP). Generally, your ISP will give you a modem and provide you a username & password that you needed when you are creating the Internet connection.

Ethernet Settings

Protocol

DHCP

Static

PPPoE

PPPoE Setting

User Name

Password

Cancel

Apply

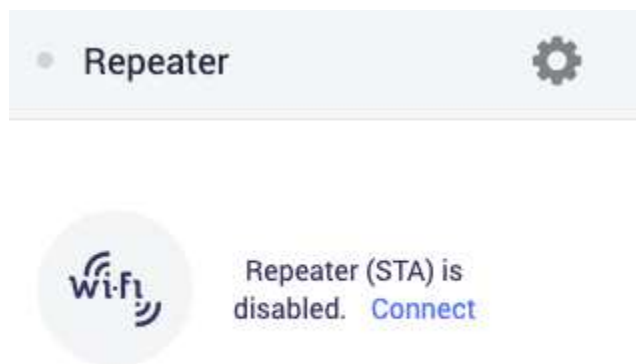
2.2 Connect to the Internet via an existing Wi-Fi by Repeater

Using Repeater means connecting the router to another existing wireless network, e.g. when you are using free Wi-Fi in a hotel or cafe.

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

On the left side of web Admin Panel -> INTERNET, Repeater sector.

Basic steps



Click **Connect** in the image above.

Join WLAN

Available Networks

Join Other Network

 GL-Office	Mixed
 Fish	2.4G
 GL-AR750S-07c	2.4G
 TBBT	2.4G
 GL-MT300N-V2-ea8	2.4G
 TBBT-5G	5G

Choose a SSID from the drop-down list and enter its password. If the SSID you want to connect to is not in the list, click [Join Other Network](#) in the image above.

Join Network

SSID

GL-Office

Password

.....

Remember

Advanced Settings

Back

Apply

For [Advanced Settings](#).

Wait a moment, if the password is correct, the connection will be successful.

GL-Office





IP Address	192.168.111.172
Gateway	192.168.111.1
DNS Server	192.168.111.1
BSSID	94:83:C4:08:3B:88




Disable

Switch Network

Join network advanced setting

When joining the network, there are two additional options.


Join Network




SSID


GL-Office


Password




Remember



Lock BSSID 



Manually Set Static IP





Back

Apply


- **Lock BSSID.** If this option is enabled, the router will only connect to the AP corresponding to the BSSID you selected when switching to a network using this SSID.
- **Manually set static IP.**

Repeater options

Click the cog icon for Repeater options.

GL-Office



IP Address	192.168.111.172
Gateway	192.168.111.1
DNS Server	192.168.111.1
BSSID	94:83:C4:08:3B:88



Disable
Switch Network

Repeater Options

Allow Switching To Other Saved Networks ⓘ
☒

Band Selection ⓘ

Auto
5GHz
2.4GHz

Allow Repeat DFS Channels ⓘ
☐

Force 20MHz Bandwidth For 2.4G ⓘ
☐

Cancel
Apply

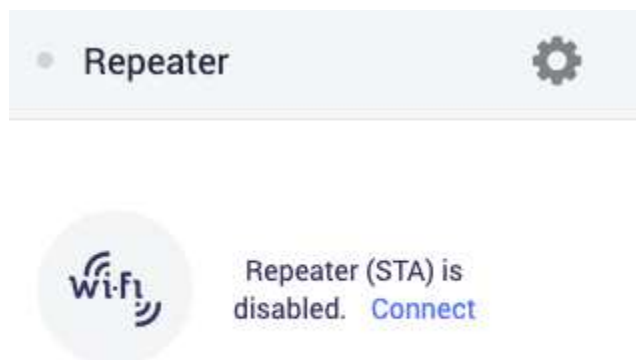
- **Allow Switching To Other Saved Network.** If the option is enabled, the router will automatically connect to other saved networks when it is unable to connect to the current Wi-Fi network.
- **Band Selection.** If you manually select a band, the router will not scan or connect to any Wi-Fi with another band.
- **Force 20MHz Bandwidth For 2.4G.** If the option is enabled, The device will prompting the stability of the connection in exchange of reducing the connection speed. It only works when repeating 2.4G Wi-Fi.

Manage known network

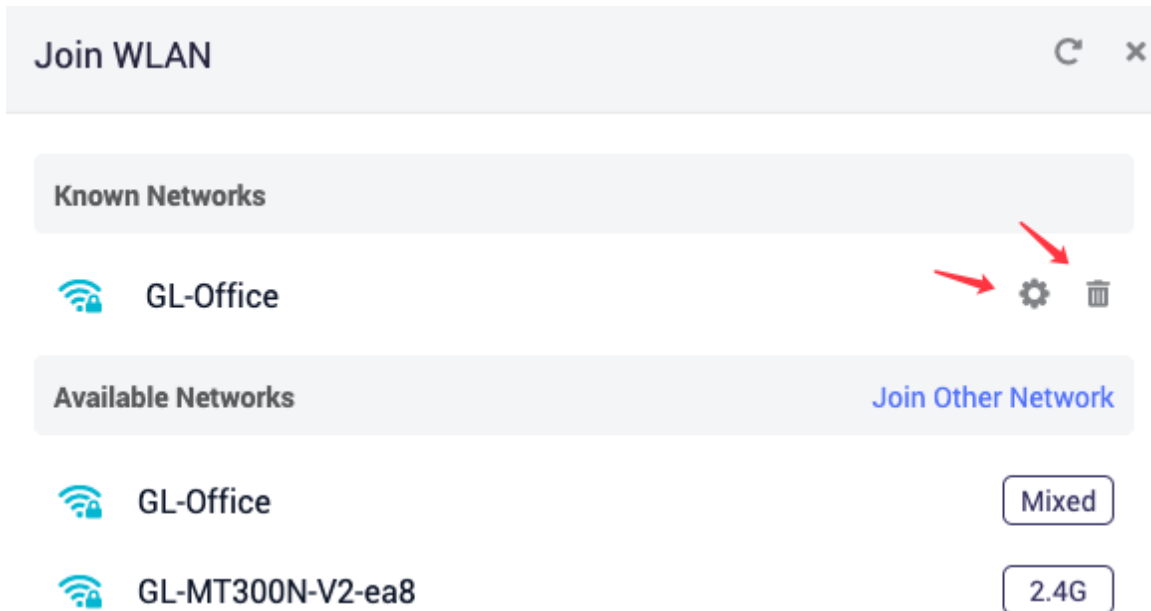
To delete known network, click **Switch Network**.



Or click **Connect**.



On the **Known Network** sector, click trash icon to delete a known network, click cog icon to config the network.



Join other network

Join Network

SSID

Security

None

Remember

Manually Set Static IP

Back

Apply

Reconnection

In the following cases, the router's Repeater will try to connect to WiFi every once in a while. You can turn off the reconnection manually, and for ssid/password errors, please delete it in Known Network.

1. The wrong SSID/password was entered during the process of Repeater, after the first failed connection.
2. After connecting to the WiFi of the upstream router, the router moves out of the signal range of the upstream router.

3. After connecting to the WiFi of the upstream router, the upstream router changed the SSID/password, or restricted the connection.

It can be divided into three phases, the waiting phase, the scanning phase, and the connecting phase.

Note: There are some problems during the scanning phase and the connection phase.

1. In the waiting phase, everything is OK.
2. In the scanning phase, data packet may loss in the scanned band, possible connection problems for new devices. For GL-MT3000 and GL-MT3000, the Guest Wi-Fi will be temporarily turned off.
3. In the connecting phase, the Main Wi-Fi on the corresponding band may be disconnected.

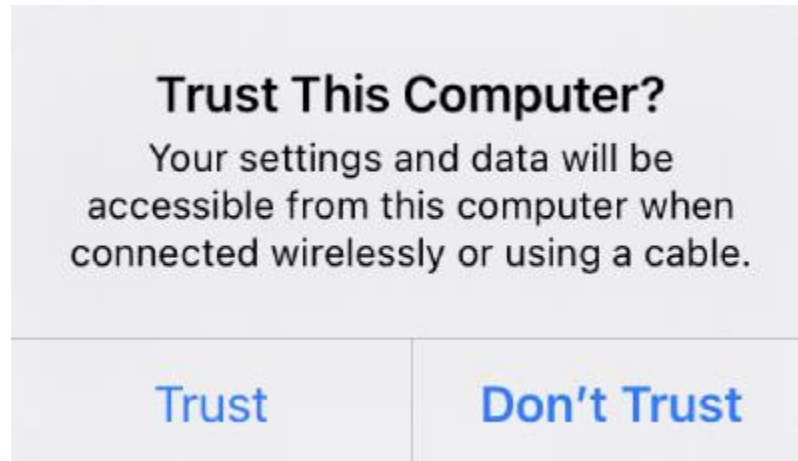
2.3 Connect to the Internet via usb tethering

Using a USB cable to share network from your smartphone to the router is called Tethering. Host-less modem works in Tethering during the setup of the modem as well.

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

iPhone

1. Connect iPhone to the USB port of the router. It will pop up a message asking to trust this computer? Click "Trust" to continue. Because we are connecting the iPhone to the router, so here is to TRUST the router.



2. Go to iPhone -> Settings -> Personal Hotspot -> Turn on Allow Others to Join.



3. Go to web Admin Panel, on the left side bar, choose "INTERNET" and click "Connect" in the middle of the page.



4. It will show connected information on the top of your phone screen and the web Admin Panel once you connect successfully.



Tethering connected.



If the connection fails, please turn off and turn on **Allow Others to Join** for a few times.

2.4 Connect to the Internet via cellular

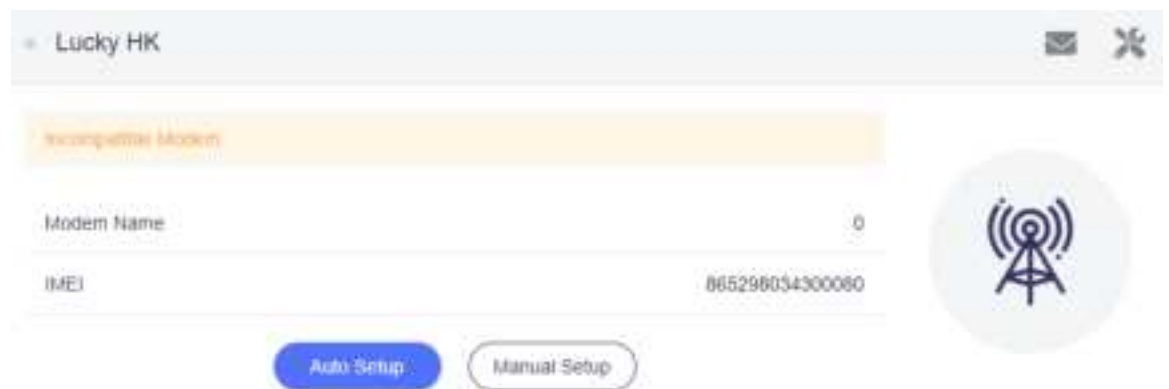
The router can be used to access the Internet through cellular. There are two cases, some models have a built-in 3G/4G model; some models have a usb port and can be plugged into a usb 3G/4G modem.

On the left side of web Admin Panel -> INTERNET, Cellular sector.

Note: Some SIM cards may need to be activated the first time you use them, so please activate them in your phone before using them in your router.

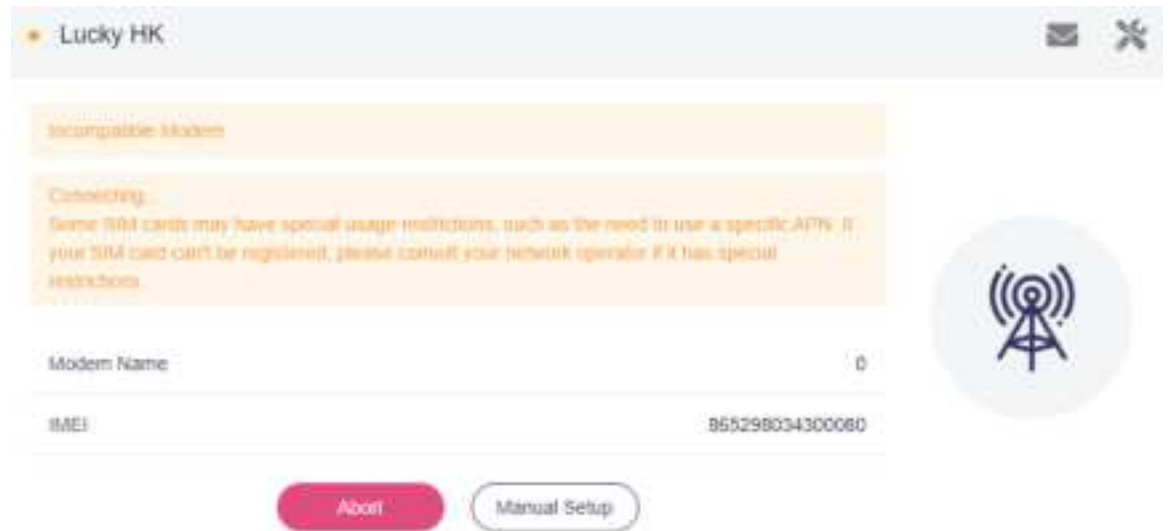
1. We recommend to turn off the router first, insert your SIM card into the USB modem then plug the USB modem into the USB port of the router, and then turn it on again. If you insert a usb modem at power on, the page may be no change, please refresh the page.
2. Please access the web Admin Panel -> INTERNET, Cellular sector. The first time, it may not connect automatically, but it has read the name of your carrier in the upper left corner and the IMEI, then please click **Auto Setup**.

Please ignore the warning of *Incompatible Modem*



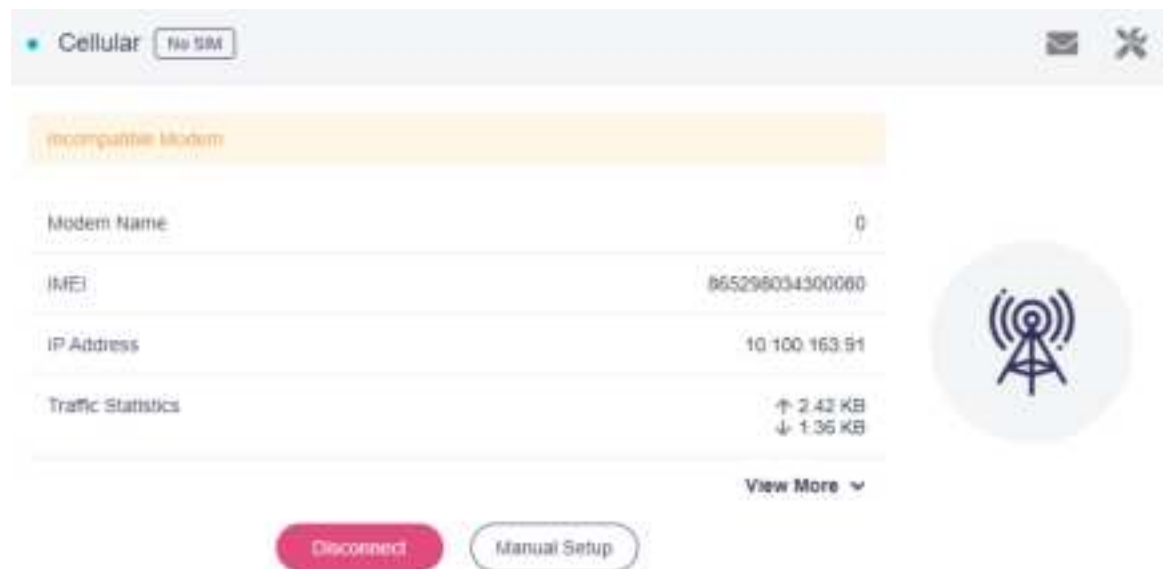
3. Connecting.

Note: Some SIM cards may have special usage restrictions, such as the need to use a special APN. If your SIM card can't be registered, please consult your network operator if it has special restrictions.



4. After a while, it will be connected. Otherwise, try [Manual Setup](#).

When the usb modem is plugged into the router the second time it is powered on, it is usually automatically recognized and a connection is established. It may not get the information of signal, modem name and IMEI.



Manual Setup

Sometimes, **Auto Setup** may not work, you can try **Manual Setup**.

Cellular Settings

Protocol

3G

Port ⓘ

/dev/ttyUSB0

APN ⓘ

mobile

PIN

Optional

TTL ⓘ

Optional

Service

LTE/UMTS/GPRS

Dial Number

Authentication

NONE

Cancel

Apply

Compatible Modems

Here is a list of supported modems that we had tested before.

Model	3G/4G	Tested	Tested by	Comments*
Quectel EC20-E, EC20-A, EC20-C	4G	Yes	GL.iNet	

Model	3G/4G	Tested	Tested by	Comments*
Quectel EC25-E, EC25-A, EC25-V, EC25-C	4G	Yes	GL.iNet	
Quectel UC20-E	3G	Yes	GL.iNet	
ZTE ME909s-821	4G	Yes	GL.iNet	
Huawei E1550	3G	Yes	GL.iNet	
Huawei E3276	4G	Yes	GL.iNet	
TP-Link MA260	3G	Yes	GL.iNet	
ZTE M823	4G	Yes	Arnas Risqianto	
ZTE MF190	3G	Yes	Arnas Risqianto	
Huawei E3372	4G	Yes	anonymous	
Pantech UML290VW (Verizon)	4G	Yes	GL.iNet/steven	
Pantech UML295 (Verizon)	4G	Yes	GL.iNet/steven	

Model	3G/4G	Tested	Tested by	Comments*
Novatel USB551L (Verizon)	4G	Yes	GL.iNet/steven	
Verizon U620L (Verizon)	4G	Yes		

QMI: This modem supports QMI mode. Please choose /dev/cdc-wdm0 in the Device list.*

*Host-less: This modem supports tethering mode, please set up by using Tethering but not 3G/4G modem.

You can also refer to <http://ofmodemsandmen.com/modems.html> for a well supported modem list.

You can also search on the [forum](#) or create a post for asking.

3. Wireless

The wireless interface may vary a bit from model to model.

On the left side of web Admin Panel -> WIRELESS

Main WiFi

5GHz WiFi

5GHz Guest WiFi

Enable Wi-Fi

ON

TX Power

Max

Wi-Fi Name (SSID)

GL-AXT1800-cd7-5G

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

••••••••

SSID Visibility

Shown

Wi-Fi Mode

11a/n/ac/ax

Bandwidth

20/40/80 MHz

Channel ⚠

40

Modify

Note: The **Channel** can't be modified when [repeater](#) is enabled.

2.4GHz WiFi

2.4GHz Guest WiFi

Enable Wi-Fi



TX Power

Max

Wi-Fi Name (SSID)

GL-AXT1800-ed7

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

SSID Visibility

Shown

Wi-Fi Mode

11g/n/ax

Bandwidth

20/40 MHz

Channel

auto

Modify

Guest WiFi

● 5GHz WiFi

● 5GHz Guest WiFi

Enable Wi-Fi

OFF

Wi-Fi Name (SSID)

GL-AXT1800-cd7-5G-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

Modify

● 2.4GHz WiFi

● 2.4GHz Guest WiFi

Enable Wi-Fi

OFF

Wi-Fi Name (SSID)

GL-AXT1800-cd7-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Password

Modify

4. CLIENTS

On the left side of web Admin Panel -> CLIENTS

You can manage all connected devices in CLIENTS page.

Blocking client

Enable **Block WAN** so that it cannot access the WAN, only LAN. To put it simple, it will cannot access the Internet.

Online Clients (3) ^					
Name	IP + MAC	Speed	Traffic	Block WAN	Action
 Leo-MBP	192.168.8.149 8C:85:90:8F:42:F5	↑ 89.05 B/s ↓ 131.00 B/s	↑ 136.33 MB ↓ 606.96 MB	<input type="checkbox"/>	...
 GL-AR750S-07r	192.168.8.154 84:95:5E:45:D0:7C	↑ 28.00 B/s ↓ 28.00 B/s	↑ 15.00 KB ↓ 14.68 KB	<input checked="" type="checkbox"/>	...
 Leo-Phone	192.168.8.118 14:16:9E:4D:A1:8D	↑ 0.00 B/s ↓ 0.00 B/s	↑ 110.52 KB ↓ 7.43 MB	<input type="checkbox"/>	...

Offline Clients (1) ^					
Name	IP + MAC	Speed	Traffic	Block WAN	Action
 Unknown	192.168.8.213 06:52:8C:37:27:C5	↑ 0.00 B/s ↓ 0.00 B/s	↑ 779.36 KB ↓ 2.86 MB	<input type="checkbox"/>	...

Limiting speed

Click **Action** to limit speed a client.

Limit Speed Settings

↑ Upload

Unlimited KB/s

↓ Download





Unlimited KB/s

Cancel

Apply

If a client has applied speed limitation, its up arrow and down arrow of speed will turn yellow.

Online Clients (3) ▲

Name	IP + MAC	Speed	Traffic	Block WAN	Action
 Leo-MBP 	192.168.8.149 8C85528F43F3	↑ 2.44 KB/s ↓ 3.17 KB/s	↑ 136.60 MB ↓ 607.46 MB	<input type="checkbox"/>	...
 GL-AR7505-07c	192.168.8.154 E4555E45007C	↑ 28.00 B/s ↓ 28.00 B/s	↑ 23.04 KB ↓ 22.64 KB	<input type="checkbox"/>	...
 Leo-Phone	192.168.8.118 14169E40A1F8	↑ 7.93 KB/s ↓ 55.45 KB/s	↑ 756.23 KB ↓ 7.64 MB	<input type="checkbox"/>	...

Click **Action** to disable limiting.

Remove offline clients

For offline clients, click **Action** can remove this client as well.

5. Firmware Upgrade

On the left side of web Admin Panel -> UPGRADE

Upgrade

Online Upgrade

Local Upgrade

✓ Firmware is up to date.

Current Firmware

Version	4.0.0
Firmware Type	release1
Compile Time	2022-05-25 7:19:16(UTC+08:00)

Online Upgrade


You can find the current firmware version here. If your router is connected to the Internet, it will check for the newer firmware version available for download.

Local Upgrade

Select a firmware file or drag and drop to upgrade. You can download the firmware from our [download site](#).

Online Upgrade

Local Upgrade



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

After uploaded, it will verify the firmware.

Keep Setting: Current settings will be retained. User installed packages will be prompted to re-install after upgrade.

Click **Install** to upgrade.

Note: Please do not disconnect the power during the upgrade.

Online Upgrade

Local Upgrade



Upload successful

Re-upload file

Firmware Verification

Version

4.0.0 [Release Notes](#)

SHA256

517b4222abb754c47ef892f33efaa5d746ce289c2062c816cbfd05a65738a602

Verification Result

Pass

Keep Settings 



Install

6. FIREWALL

GL.iNet's routers include multiple firewall features to ensure a secure connection and complete oversight by users. It lets users configure firewall rules including Port Forwarding, Open Ports, and DMZ. The firewall interface is accessible by clicking [FIREWALL] on the side menu of the router's web Admin Panel

On the left side of web Admin Panel -> FIREWALL

In FIREWALL page, you can set up firewall rules like **Port Forwarding**, **Open Ports on Router** and **DMZ**.

Port Forwards

Port Forwarding lets remote computers to connect to a local computer or server behind the firewall in the LAN network (such as web servers, FTP servers, etc).

To set up port forwarding, on the **Port Forwards** tab click **Add**.



It will pop up **Add New Port Forward Rule** dialog.

Add New Port Forward Rule

Name

Protocol

TCP/UDP



External Zone

WAN



External Port

Internal Zone

LAN



Internal IP

Internal Port

Enable



Cancel

Apply

Name: The name of the rule.

Protocol: The protocol used, you can choose TCP, UDP, or both TCP and UDP.

External Zone: The options for external zone are WAN, wgclient, wgserver, ovpnclient, ovpnserver.

External Port: The numbers of external ports. You can enter a specific port number or a range of service ports (E.g **100-300**).

Internal Zone: The options for external zone are WAN, wgclient, wgserver, ovpnclient, ovpnserver.

Internal IP: The IP address assigned by the router to the device which needs to be accessed remotely.

Internal Port: The internal port number of the device. You can enter a specific port number. Leave it blank if it is same as the external port.

Enable: Enable or disable of the rule.

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, click **Add**.



Add New Open Port

Name	<input type="text"/>
Protocol	<div>TCP/UDP</div>
Port	<input type="text"/>
Enable	<div><div></div></div>

Cancel

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 of the rule.

DMZ

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

Toggle on **Enable DMZ**. Select the internal IP address of your device which is going to receive all the inbound packets.

Port Forwards

Open Ports on Router

DMZ

DMZ lets you to expose one computer to the Internet, so 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

192.168.8.154

Apply

7. VPN

GL.iNet routers are pre-installed with OpenVPN and WireGuard® supporting 30+ VPN services. It automatically encrypts all network traffic within the connected network, including guest devices and client devices that are not capable of running VPN encryption. Our routers can also act as VPN servers, redirecting traffic from client devices in remote locations to the VPN server via a VPN tunnel before accessing the public internet.

7.1 VPN Dashboard

Access to web Admin Panel, on the left side -> VPN -> VPN Dashboard

VPN Dashboard page is for the status and setting of VPN.

VPN Dashboard

VPN Client

Global Options

Global Proxy

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

Type	Options
<div>OpenVPN</div>	<div>Set Up Now</div>
<div>WireGuard</div>	<div>Set Up Now</div>

VPN Server

Type	Options
<div>OpenVPN</div>	<div>Set Up Now</div>
<div>WireGuard</div>	<div>Set Up Now</div>

VPN Client

In the beginning, there is no configuration available for OpenVPN and WireGuard, you need to click **Set Up Now** to go to the corresponding page to configure.

VPN Client

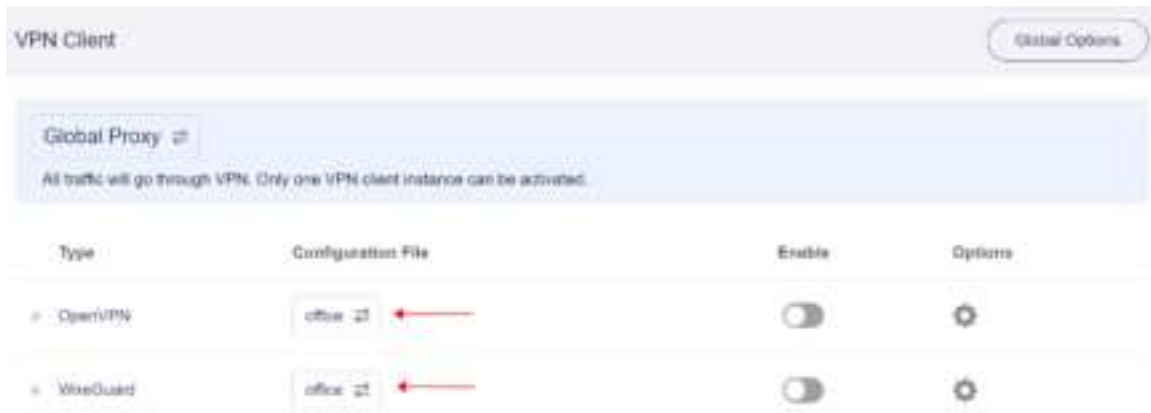
Global Options

Global Proxy

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

Type	Options
<div>OpenVPN</div>	<div>→ Set Up Now</div>
<div>WireGuard</div>	<div>→ Set Up Now</div>

Once the configuration is complete, you can select the configuration file in the Configuration file column.



VPN Client Options

Click the cog icon of OpenVPN or WireGuard.



OpenVPN client options.

OpenVPN Client Options

Allow Remote Access LAN ⓘ



IP Masquerading ⓘ



MTU ⓘ

Cancel

Apply

WireGuard client options.

WireGuard Client Options

Allow Remote Access LAN ⓘ



IP Masquerading ⓘ



MTU ⓘ

1420

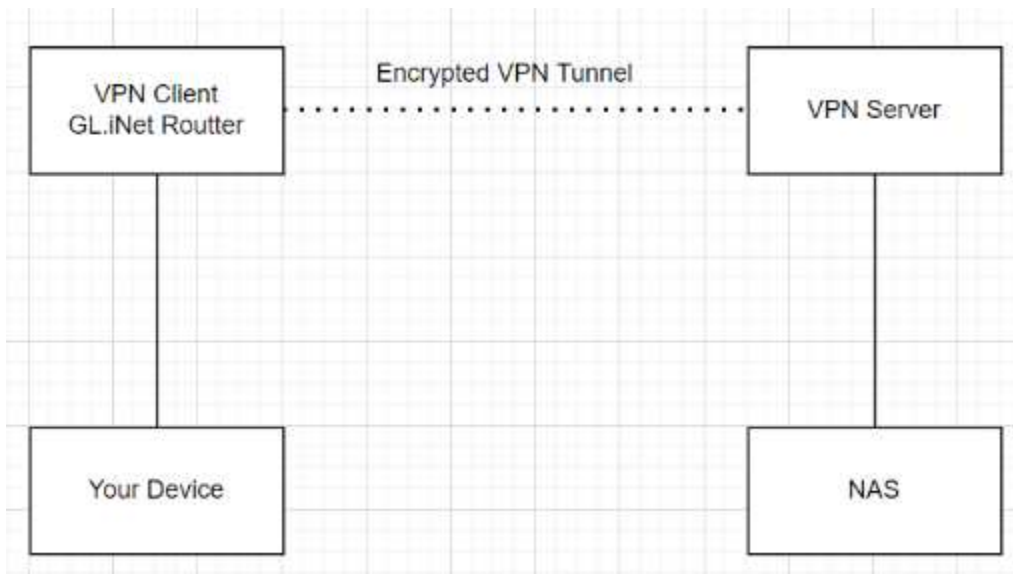
Cancel

Apply

- Allow Remote Access LAN

If this option is enabled, the devices connected under the router is allowed to access the LAN on the VPN Server side, which also requires the appropriate settings on the VPN Server side.

For example, in the image below, if this option is enabled, it means *Your Device* is allowed to access the *NAS*, but still needs the *VPN Server* to allow you to access the *NAS* within its subnet.



- IP Masquerading

If this option is enabled, When clients devices on LAN send their IP packets, the router replaces the source IP address with its own address and then forwards it to the VPN tunnel.

- MTU

Stands for maximum transmission unit. The MTU you set for the instance will overwrite the MTU item in the configuration file.

Proxy mode



1. Global proxy

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

2. Policy mode

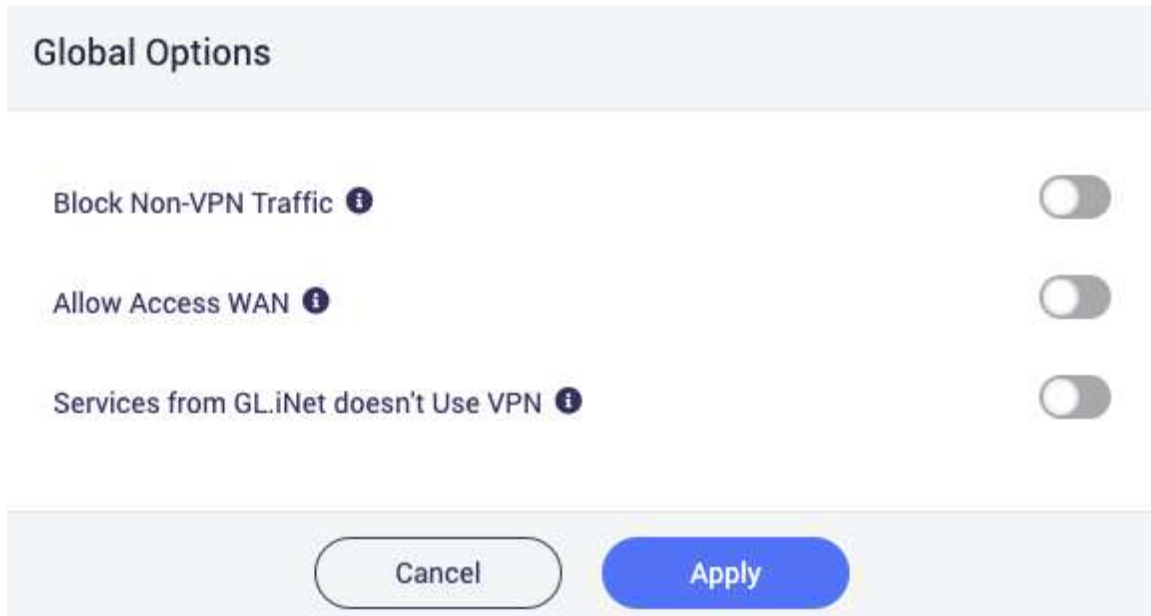
- Based on the target domain or IP.
In this mode, only the traffic of certain websites defined by IP address or domain name will go through VPN. Only one VPN client instance can be activated.
- Based on the client device.
In this mode, only the traffic of certain local client devices defined by MAC address will go through VPN. Only one VPN client instance can be activated.
- Based on the VLAN.
In this mode, only the traffic of certain VLAN can go through the 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.

Global Options

Click **Global Options** will popup a global options dialog.



Global Options

Block Non-VPN Traffic ⓘ ☐

Allow Access WAN ⓘ ☐

Services from GL.iNet doesn't Use VPN ⓘ ☐

Cancel Apply

1. Block Non-VPN Traffic

If this option is enabled, all traffic from client devices trying to be sent out of the VPN tunnel will be blocked, which will effectively prevent VPN leaks due to client DNS settings, dropped VPN connections, client apps requesting by IP, etc.

2. Allow Access WAN

If this option is enabled, while VPN is connected, client devices will still be able to access WAN, e.g. accessing your printer, NAS etc in upper subnet.

3. Services From GL.iNet Doesn't Use VPN

If this option is enabled, services on routers that usually require the use of a real IP will not use VPN. Including GoodCloud, DDNS, rty.

VPN Server

VPN Server			
Type	Tunnel Address	Enable	Options
• OpenVPN	10.8.0.0	<input type="checkbox"/>	 
• WireGuard	10.0.0.1/24	<input type="checkbox"/>	 

OpenVPN Server Options

Click the cog icon of OpenVPN server.

OpenVPN Server Options

Allow Remote Access LAN ⓘ

☐

IP Masquerading ⓘ

☒

MTU ⓘ

Cancel

Apply

- **Allow Remote Access LAN:** If this option is enabled, resources inside the LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading:** If this option is enabled, when clients devices on LAN send their IP packets, the router replaces the source IP address with its own address and then forwards it to the VPN tunnel.
- **MTU:** The MTU you set for the instance will overwrite the MTU item in the configuration file.

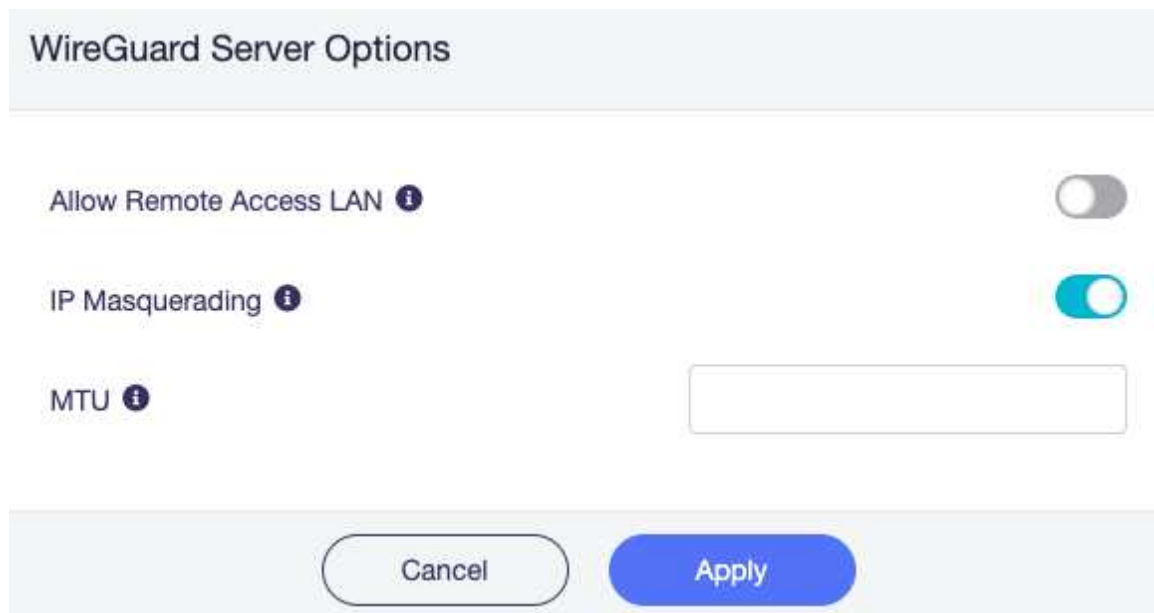
OpenVPN Server Route Rule

Click the network icon of OpenVPN server.

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



WireGuard Server Options



- **Allow Remote Access LAN:** If this option is enabled, resources inside the LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading:** If this option is enabled, when clients devices on LAN send their IP packets, the router replaces the source IP address with its own address and then forwards it to the VPN tunnel.

- **MTU:** The MTU you set for the instance will overwrite the MTU item in the configuration file.

WireGuard Server Route Rule

Click the network icon of WireGuard server.

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



Global Options of Server

Global Options of VPN Server



Global Options

Enable VPN Cascading ⓘ



Cancel

Apply

- **VPN Cascading**, If this option is enabled, when you have both VPN server and VPN Client running on this router, clients connected to the VPN server will further be routed to the VPN client tunnel. [Learn more about VPN Cascading](#).

OpenVPN

Please refer to the following links for a step to step setup guide:

7.2 How to Setup OpenVPN Client on GL.iNet router

OpenVPN is an open-source VPN protocol that makes use of virtual private network (VPN) techniques to establish safe site-to-site or point-to-point connections.

GL.iNet routers have pre-installed OpenVPN Client and Server.

We recommend WireGuard over OpenVPN because it is much faster.

If you have already bought OpenVPN service from a provider, but you don't know how to get the configuration file, please refer to [get configuration files from OpenVPN service providers](#) or ask its support.

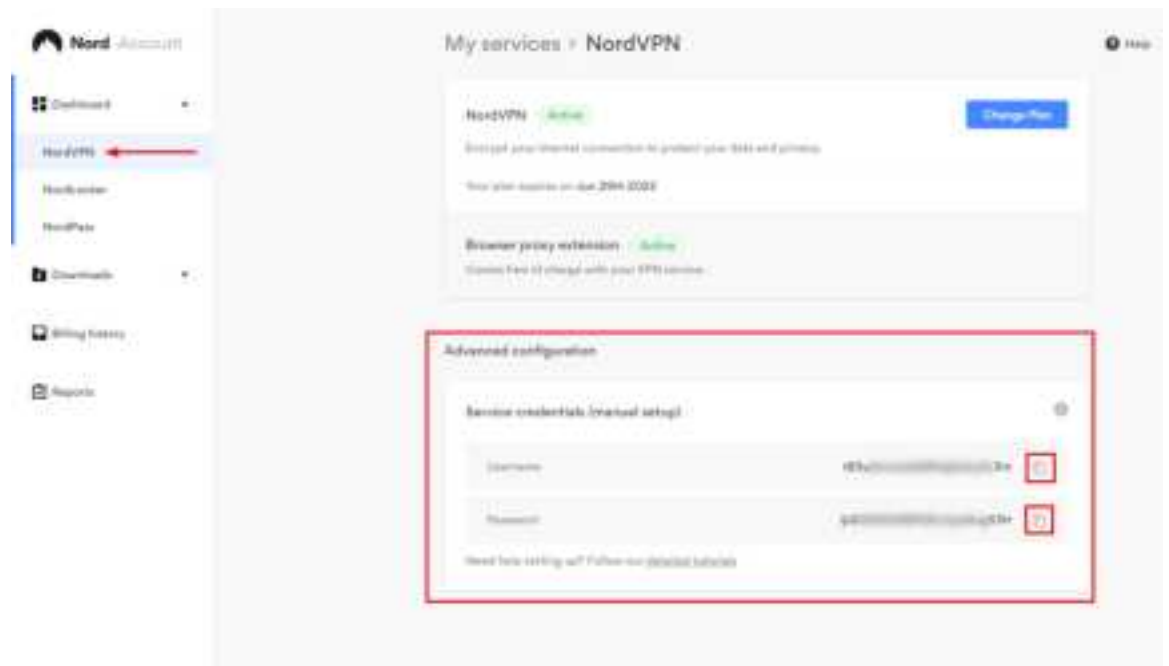
You can setup OpenVPN Client via web Admin Panel and [mobile app](#). For the mobile app, it has already integrated NordVPN.

Setup NordVPN

[NordVPN](#) is the top online VPN service for speed and security.

1. Input your NordVPN account's service credentials, then click **Save Credentials & Get Servers**

Where to find the NordVPN service credentials.



OpenVPN Client

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

N NordVPN

+ New Group

NordVPN

Username

XDSYVQIQ

Password

.....

Save Credentials & Get Servers

[Setup Guide](#)

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

Select NordVPN Servers

Protocol

UDP

TCP


TCP/UDP

Max Of Per Location

2

Location 

Singapore (2) 

Tokyo (2) 



Cancel

Apply

It will download configuration files.

OpenVPN Client

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


Update Servers



 NordVPN 

 New Group


Name	Server Location	
------	-----------------	--

sg494.nordvpn.com.udp	Singapore, Singapore	
-----------------------	----------------------	---



sg492.nordvpn.com.udp	Singapore, Singapore	
-----------------------	----------------------	---



jp531.nordvpn.com.udp	Japan, Tokyo	
-----------------------	--------------	---



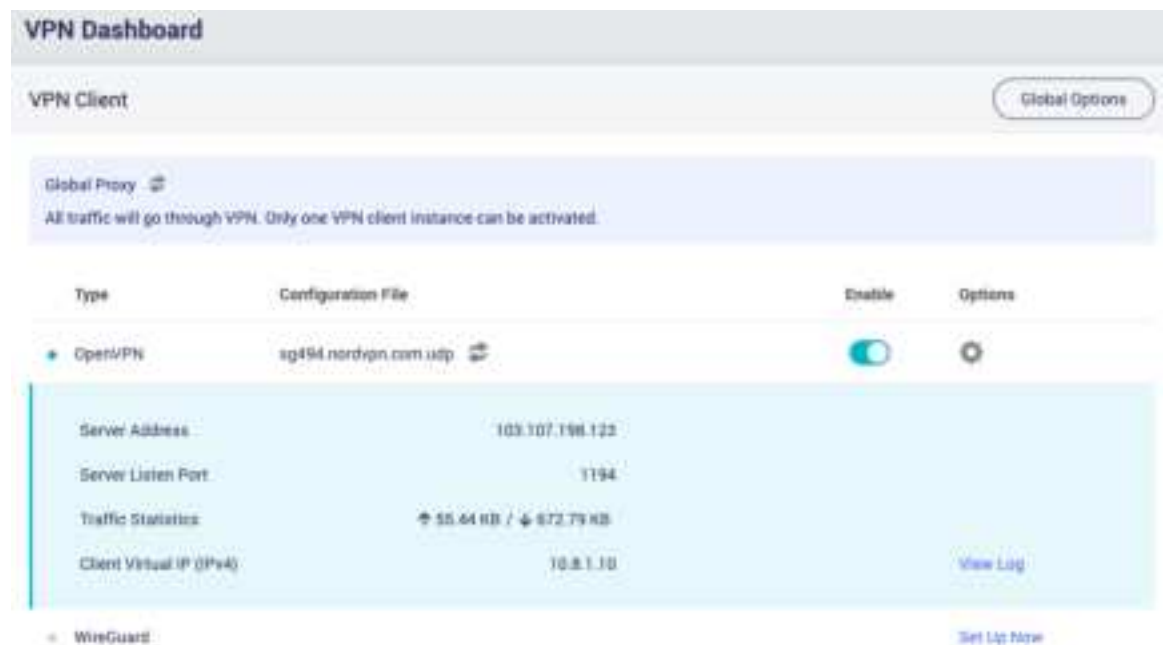
jp511.nordvpn.com.udp	Japan, Tokyo	
-----------------------	--------------	---



3. Go to VPN Dashboard to enable the connection.

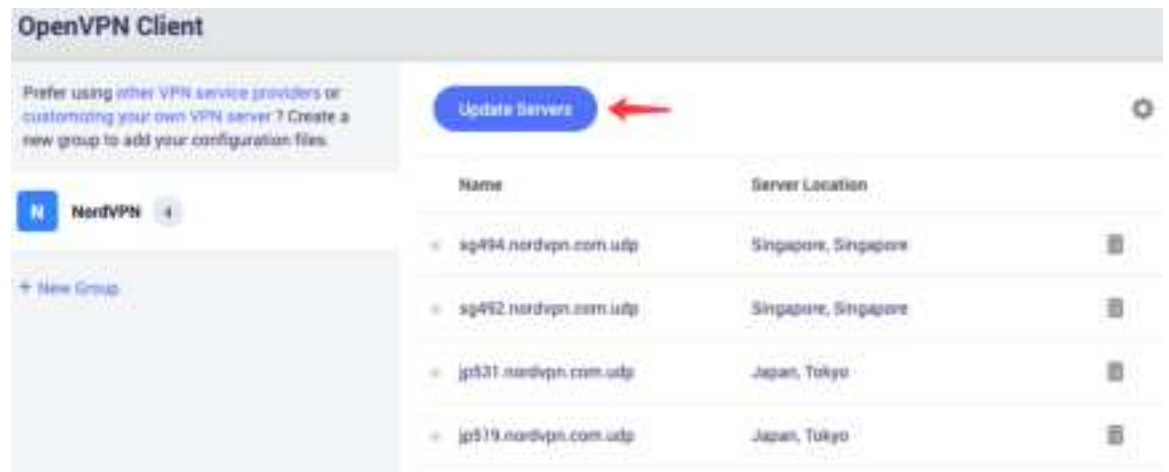


Toggle the switch to enable the connection.



4. Update servers

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



5. Edit credential

Click the cog icon to edit the credential.



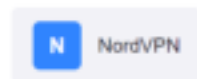
Setup OpenVPN client

As of firmware 4.0, it brings grouping to manage OpenVPN profiles. Please make sure all the profiles in the same group with the same credentials. For example, if you are ExpressVPN user, you can add a group named *expressvpn*, then upload all the ExpressVPN OpenVPN profiles you wanted to this group. For another OpenVPN service provider, please create another group.

Next steps, we will use ExpressVPN as an example.

1. Click **Add Manually**.

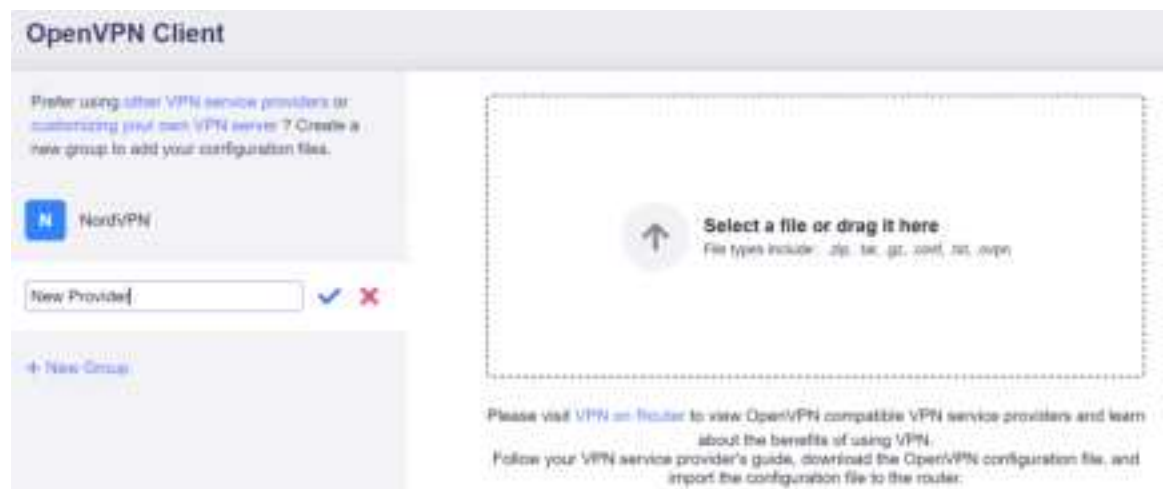
Request the VPN configuration file from your VPN service provider.



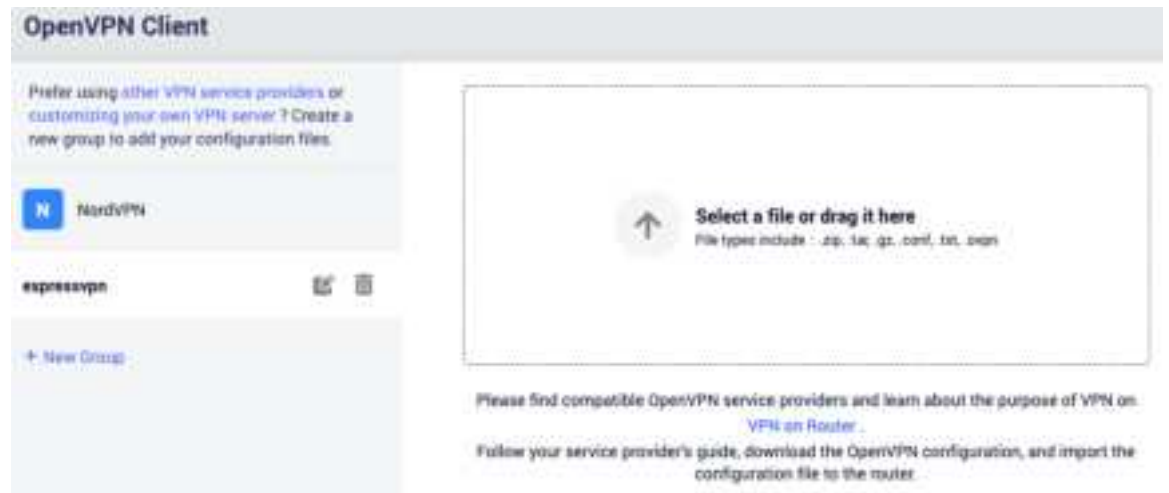
Please visit [VPN on Router](#) to view OpenVPN compatible VPN service providers and learn about the benefits of using VPN. Follow your VPN service provider's guide, download the OpenVPN configuration file, and import the configuration file to the router.



2. It will create a group.

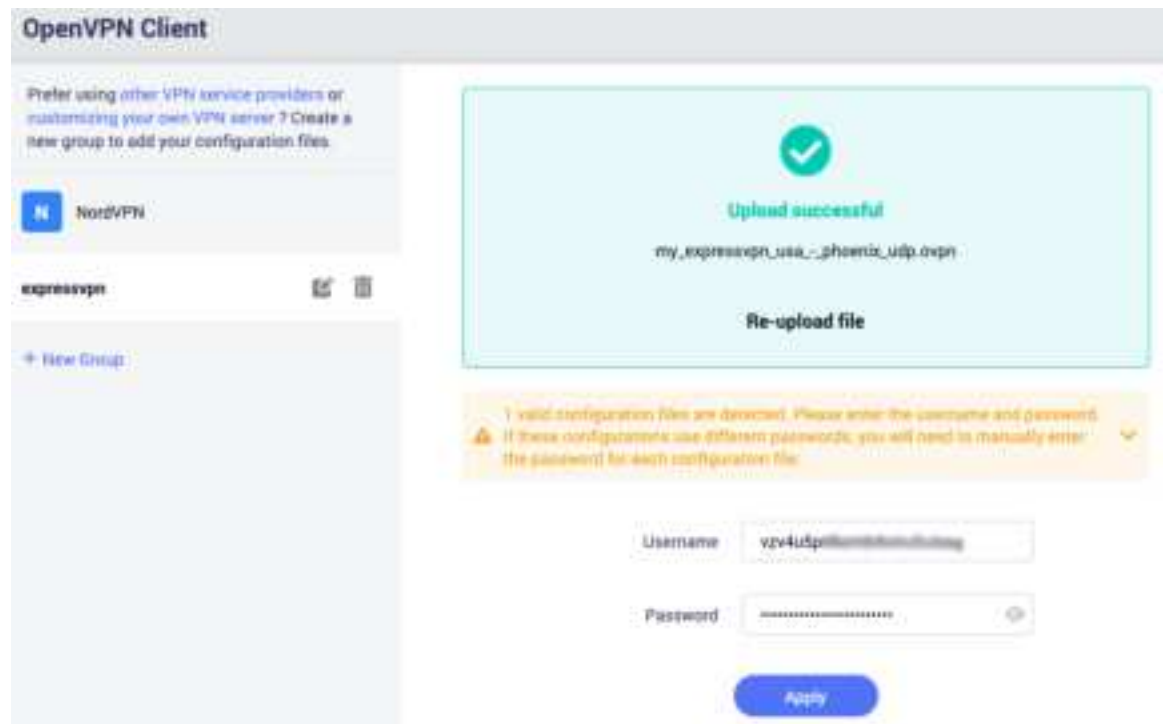


3. Give the group a descriptive name, e.g. expressvpn.

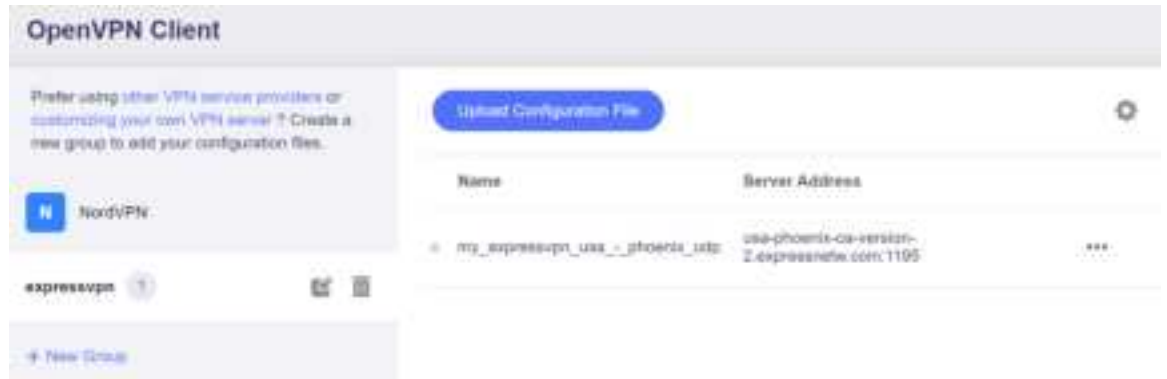


The screenshot shows the 'OpenVPN Client' web interface. On the left, there's a sidebar with a 'New Group' button and a list of groups including 'NordVPN' and 'expressvpn'. The main area on the right has a large box with an upload icon and the text 'Select a file or drag it here'. Below this, it lists supported file types: '.zip, .tar, .gz, .conf, .txt, .open'. At the bottom, there's a note about finding compatible OpenVPN service providers and a link to 'VPN on Router'.

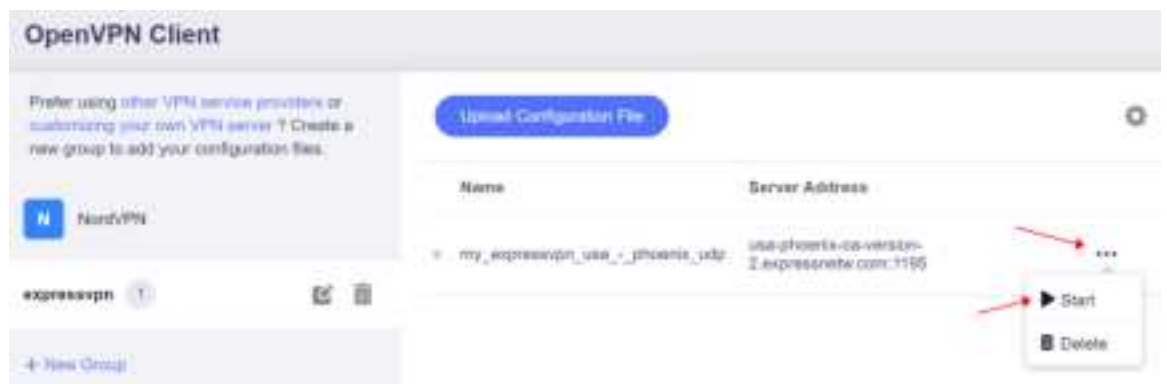
4. Upload your OpenVPN configuration file, then input the credential, click **Apply**.



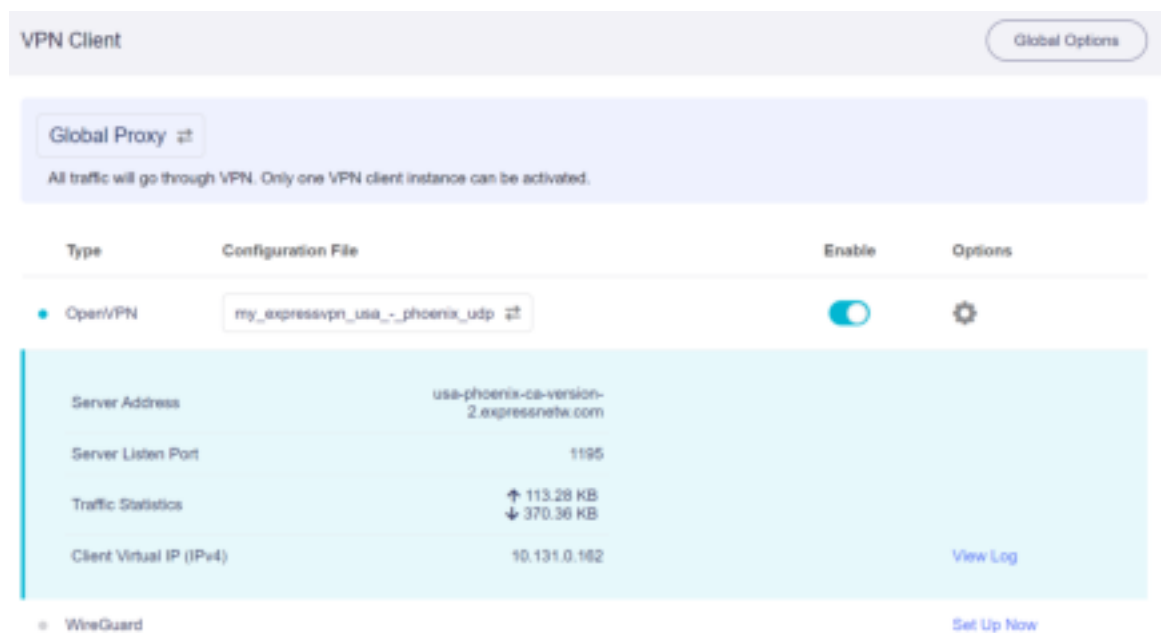
The screenshot shows the 'OpenVPN Client' web interface after a successful upload. A green checkmark and the text 'Upload successful' are displayed, along with the filename 'my_expressvpn_usa_-_phoenix_udp.open'. Below this, there's a 'Re-upload file' button. A yellow warning box states: '1 valid configuration files are detected. Please enter the username and password. If these configurations use different passwords, you will need to manually enter the password for each configuration file.' At the bottom, there are input fields for 'Username' (containing 'vzv4u5p...') and 'Password' (masked with dots), followed by an 'Apply' button.



- Click the three dots icon to start / delete the profile.



- Check the connection status by go to [VPN Dashboard](#) page.



Setup OpenVPN server on GL.iNet router

You can get a GL.iNet router to set as OpenVPN server, and get another GL.iNet router to set as OpenVPN client. For setup OpenVPN server, please check out [here](#).

Get configuration files from OpenVPN service providers¶

We have tested different OpenVPN service providers. Therefore, if you don't know how to get the configuration file, you can follow the instruction below. However, you have to contact your service provider for the configuration file if they are not listed below.

If you have any problem in the setup of OpenVPN, please contact support@glinet.biz or report in [this forum post](#).

Please check the list from our Docs:

https://docs.gl-inet.com/en/4/tutorials/openvpn_client/#get-configuration-files-from-openvpn-service-providers

7.3 Setup OpenVPN Server on GL.iNet router

OpenVPN is an open-source VPN protocol that makes use of virtual private network (VPN) techniques to establish safe site-to-site or point-to-point connections.

GL.iNet routers have pre-installed OpenVPN Client and Server.

We recommend WireGuard over OpenVPN because it is much faster. For setup a WireGuard Server, please check out [here](#).

Make sure Internet Service Provider assigns you a public IP address

Please check if you Internet Service Provider assigns you a public IP address [here](#).

If no, you can't connect to the OpenVPN Server.

An alternative method is to use a reverse proxy solution, we suggest [AstroRelay](#).

Network Topology

- If GL.iNet router is the main router in your network, this is simple, please move to the [next step](#).
- If you already have a main router, then the GL.iNet router is under the main router, you may need to setup a port forwarding on the main router.
- If you already have a main router, the GL.iNet router is several levels below it and you need to set up port forwarding on each level.

Setup OpenVPN Server

1. Click **Generate Configuration** (Only the first time).

OpenVPN Server

OpenVPN is an open-source software application that implements virtual private network (OpenVPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities, please follow the steps below:

1. Generate a OpenVPN configuration file;
2. Modify the default configuration, then save;
3. Export the client configuration file to your client device;
4. Go to the VPN Dashbord page and start the VPN server.

You don't have any OpenVPN configuration files yet, please get started by generating a new one.

Generate Configuration

2. Apply the configuration.

The screenshot shows the 'OpenVPN Server' configuration page. At the top, a status bar indicates 'The OpenVPN server is currently OFF' with a 'Start' button. Below this are two tabs: 'Configuration' (selected) and 'Users'. The configuration fields are as follows:

Field	Value
Device Mode	TUN
Protocol	UDP
Local Port	1194
IPv4 Subnet	10.8.0.0
IPv4 Netmask	255.255.255.0
Authentication Mode	Only Certificate

Below the fields is an 'Advanced Configuration' dropdown menu. At the bottom, there are two buttons: 'Reset' and 'Apply'. Below the buttons is a link that says 'Export Client Configuration'.

If you do not need to modify the configuration, please click directly the **Export Client Configuration** at the bottom of page. If you have modified the configuration, please click the **Apply** button to continue.

- **Protocol:** UDP or TCP. To find out what the difference is, check out [this tutorial](#).
- **Authentication Mode:** There are three options **Only Certificate**, **Only Username/Password**, and **Username/Password and Certificate**.

For **Username/Password** and **Username/Password and Certificate** options, they need add user(s). Then, if a OpenVPN client connect to this server, it need to input the username and password.



Created a user.



For **Only Certificate** and **Username/Password and Certificate**, the router will automatically generate a server and client certificate-key, and write into the configuration file when generating the client configuration file.

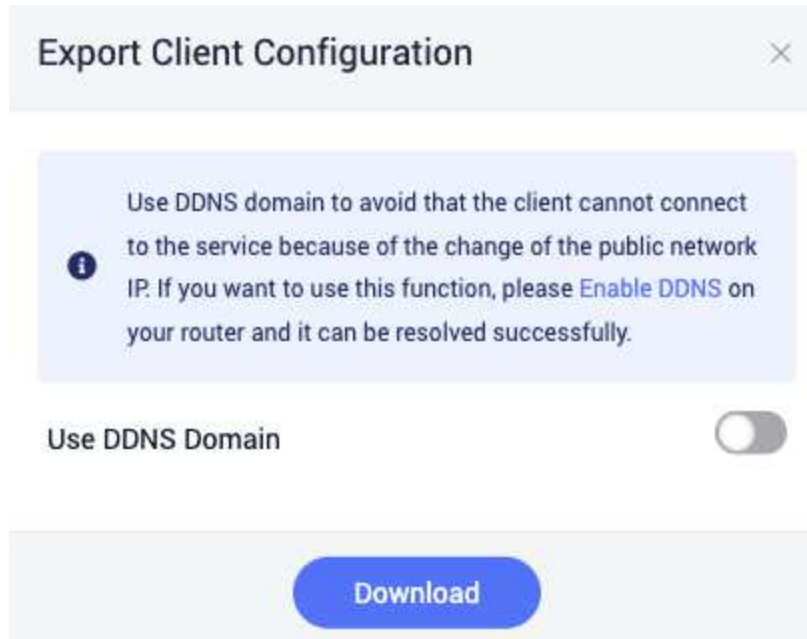
Please check [here](#) for **Advanced Configuration**.

3. Export Client Configuration

Clicking the **Export Client Configuration** button at the bottom or applying the modified configuration will pop up this dialog.

If your network's public IP changes from time to time, you can enable [DDNS](#) by using DDNS domain in the configuration.

Click **Download** to export the configuration for further setup.



4. Start OpenVPN server

Click the **Start** button in the upper right corner on OpenVPN Server page to start the server. Then go to [VPN Dashboard page](#) to check its status and other settings.



To check if OpenVPN Server is working properly

To check if OpenVPN Server is working properly, we can use another device connected to another network and use the OpenVPN configuration we exported earlier, to connect and see whether it connects properly and whether the IP address is the IP of OpenVPN Server.

The simplest way is to use a cell phone with [OpenVPN official client app](#) installed, turn off its Wi-Fi connection, and only connect to Internet via 3G/4G/5G. Then open the OpenVPN app, import the OpenVPN configuration we previously exported. Enable the connection, check if the phone has Internet access and whether its IP address is the IP of your OpenVPN Server.

When importing the configuration file to the OpenVPN app, it may have a reminder as below, please click **CONTINUE** as the certificate is already included in the configuration file.

Select Certificate

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

CONTINUE **SELECT CERTIFICATE**

There are several common reasons cause failed:

- The Internet Service Provider doesn't assign you a public IP address, please check [here](#).
- You may need setup port forwarding, please check [here](#).
- The port you are using for OpenVPN Server is blocked by the Internet Service Provider, change to another port, or contact the Internet Service Provider.
- Some countries/regions may block the VPN connection.

Advanced Configuration

Configuration	Users
Device Mode	TUN
Protocol	UDP
Local Port	1194
IPv4 Subnet	10.8.0.0
IPv4 Netmask	255.255.255.0
Authentication Mode ¹	Username/Password and Certificate
Server Root Certificate	<pre>-----BEGIN CERTIFICATE----- MIIDCCACDgwwHqgU2hCMWetDhwDwwR KhsuKum/AuDOm/guZhwKACBT </pre> Upload ca.crt
Server Certificate	<pre>-----BEGIN CERTIFICATE----- MIIDCCACDgwwHqgU2hCMWetDhwDwwR KhsuKum/AuDOm/guZhwKACBT </pre> Upload server.crt
Server Key	<pre>-----BEGIN PRIVATE KEY----- MIIEvQIBADANBgkqhkiG9w0BAQEw </pre> Upload serverkey
Authentication Algorithm	SHA256
Encryption Algorithm	AES-128-GCM
Enable LZO Compression	<input type="checkbox"/>
Diffie Hellman Parameter	<pre>-----BEGIN DH PARAMETERS----- MIhGAgEBAQEBBQYKCgQwAgEBAQEB </pre> Upload dh.pem
Enable TLS Authentication	<input type="checkbox"/>
Client to Client	<input type="checkbox"/>
Verbosity Level	3

OpenVPN Client App

We can use another GL.iNet router as OpenVPN Client, or use their official app on other devices with various OS.

- Please refer to OpenVPN Official Website: <https://openvpn.net/vpn-client/>

WireGuard

7.4 How to Setup WireGaurd Client on GL.iNet router

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

GL.iNet routers have pre-installed WireGuard Client and Server.

If you have already bought WireGuard service from a provider, but you don't know how to get the configuration files, please refer to [get configuration files from WireGuard service providers](#) or ask its support.

You can setup WireGuard Client via web Admin Panel and [mobile app](#). For the mobile app, it has already integrated some WireGuard Service Providers, they are AzireVPN, Mullvad VPN, TorGuard VPN, OVPN, WeVPN, StrongVPN, PIA VPN, SpiderVPN.

For setup via web Admin Panel, please follow the guide below.

Setup AzireVPN

[AzireVPN](#) is privacy-minded VPN service providing secure, modern and robust tunnels such as WireGuard.

Firmware 4.x has integrated AzireVPN WireGaurd service.

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

[Setup Guide](#)

[Save Credentials & Get Servers](#)

1. Input **Username** and **Password**, then click **Save Credentials & 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 15

M Mullvad

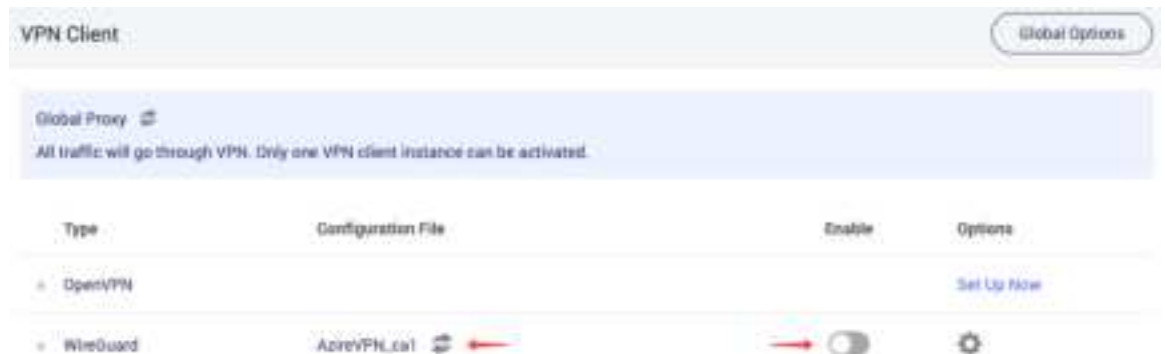
+ New Group

[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_ru1	ru1.wg.azirevpn.net:51820	
AzireVPN_es1	es1.wg.azirevpn.net:51820	

[Delete All](#)

2. Go to VPN Dashboard to enable the connection.



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



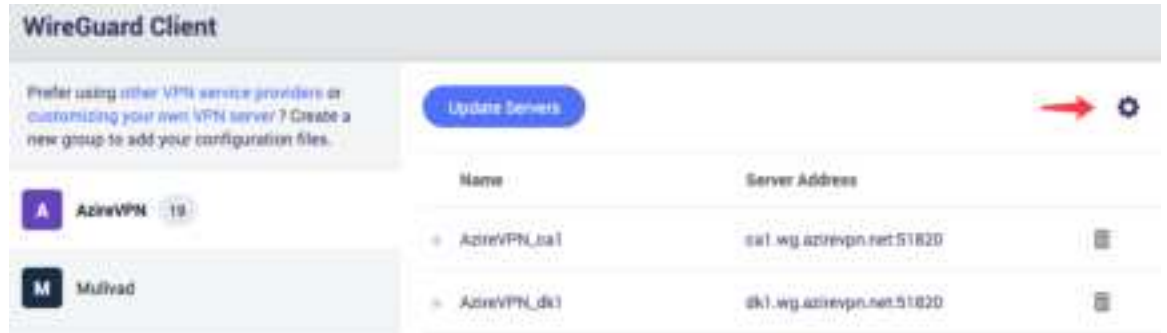
3. Update servers

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



4. Edit credential

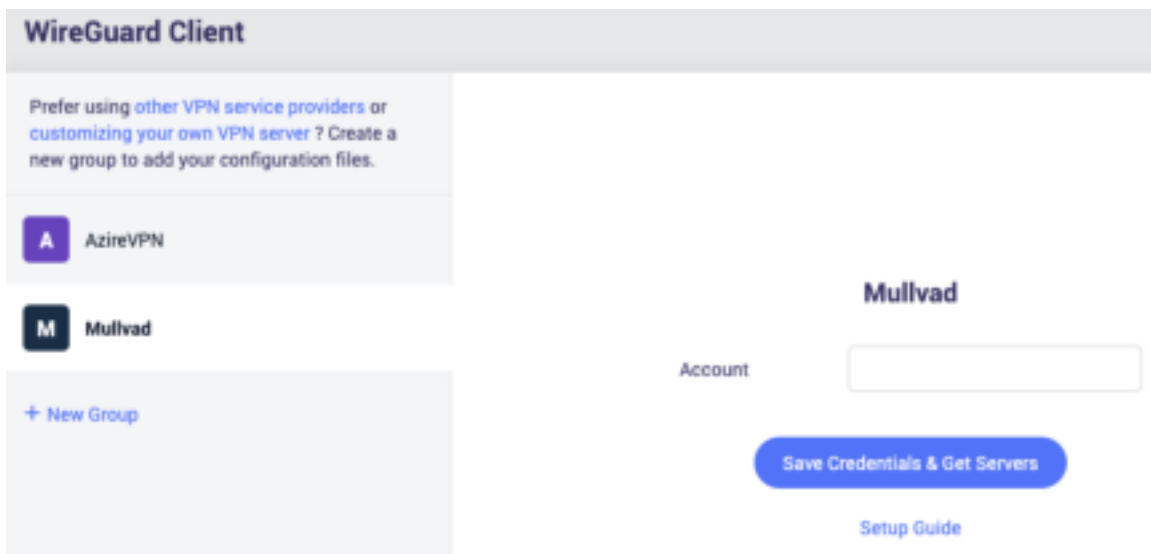
Click the cog icon to edit the credential.



Setup Mullvad

Mullvad is a VPN service that helps keep your online activity, identity, and location private.

Firmware 4.x has integrated Mullvad WireGaurd service.



1. Input **Account**, then click **Save Credentials & Get Servers**.

Mullvad account number is a 16-digit decimal in the "1000 0000 0000 0000" to "9999 9999 9999 9999" range.

It will pop up a dialog to select a location.

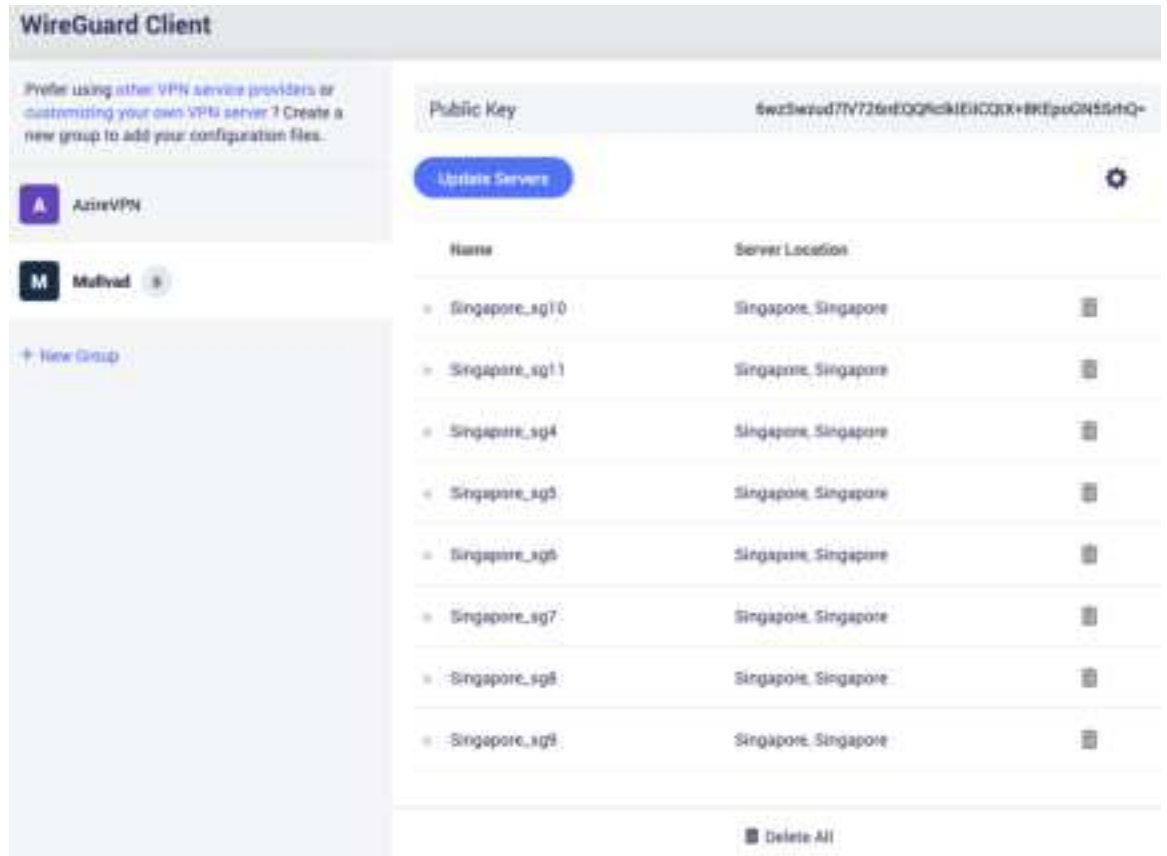
Select Mullvad Servers

Location ⓘ

Poland (7)
Portugal (2)
Romania (5)
Serbia (2)
Singapore (8)
Spain (6)
Sweden (23)
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, you can manage WireGuard keys on [Mullvad's page](#).



2. Go to VPN Dashboard to enable the connection.



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



3. 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.



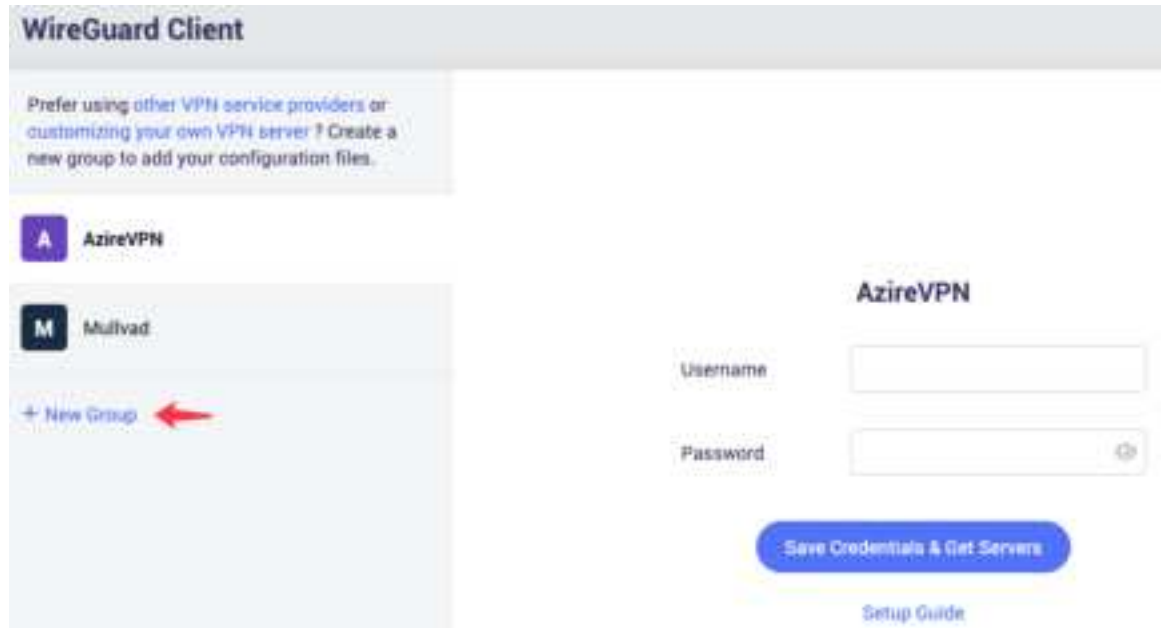
4. Edit credential



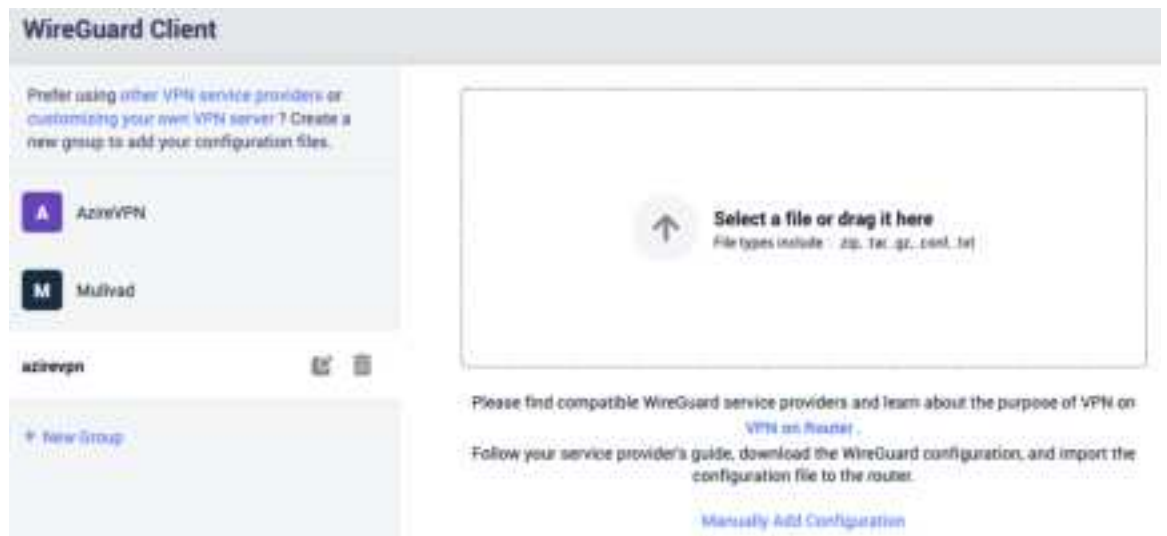
Setup WireGuard client

As of firmware 4.0, it brings grouping to manage WireGuard profiles.

1. Add a new group



2. Give the group a descriptive name, e.g. azirevpn.



3. Upload your WireGuard configuration file, then input the credential, click **Apply**.

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

+ New Group

✓

Upload successful

azurevpn-configs.zip

Re-upload file

✓ 19 valid configurations have been received

Apply

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

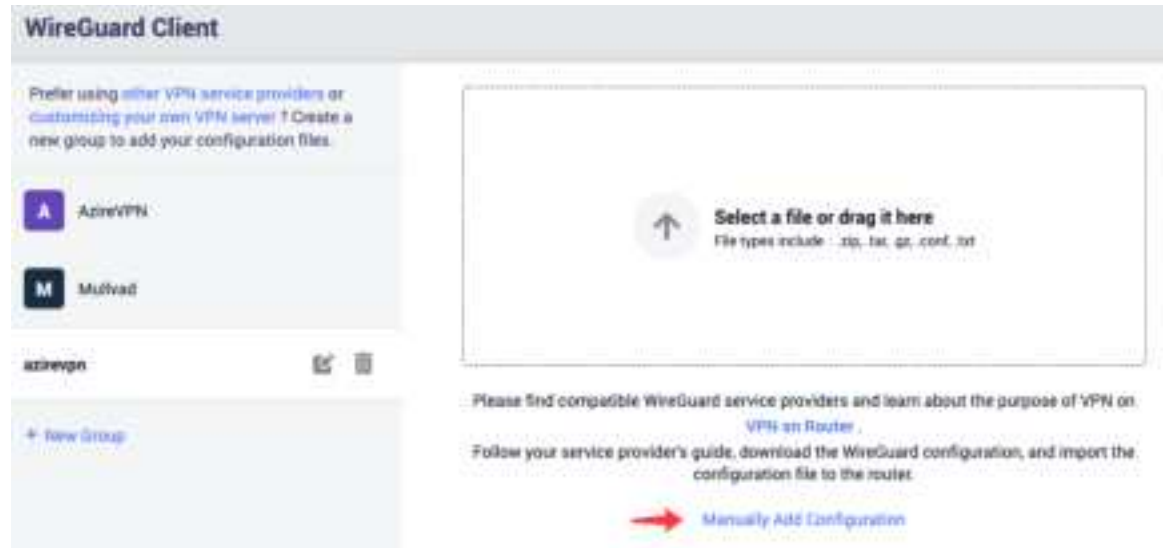
+ New Group

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		
• azurevpn-de1	de1.wg.azurevpn.net:51820		
• azurevpn-de-ber	de-ber.wg.azurevpn.net:51820		
• azurevpn-it1	it1.wg.azurevpn.net:51820		
• azurevpn-es2	es2.wg.azurevpn.net:51820		
• azurevpn-es1	es1.wg.azurevpn.net:51820		
• azurevpn-nl1	nl1.wg.azurevpn.net:51820		

Delete All

Manually Add Configuration is for if you want to paste the WireGuard configuration or fill in each item.



Give a descriptive name and paste the configuration, click **Apply** to continue.

Edit WireGuard Configuration

Name

azure-ca

[Item Mode](#)

[Interface]

PrivateKey = KLP/4xypabM2nqvZawefKwMzDRkkg/w/5fpYTAwlkWk=

Address = 10.50.23.65/19

DNS = 10.50.0.1

[Peer]

PublicKey = GO8BFrBxXHIsWryhwrz+QeYdJHXU0q1gzViUqp5rgQ=

AllowedIPs = 0.0.0.0/0

Endpoint = ca1.wg.azurevpn.net:51820

Cancel

Apply

Or you can add configuration by fill in each item, click **Item Mode**.

Edit WireGuard Configuration

Name



Item Mode

Cancel

Apply

Edit WireGuard Configuration

Name

[Text Mode](#)

Interface

IPv4 Address

Use IPv6

☐

Private Key

Listen Port

Optional

DNS

Optional

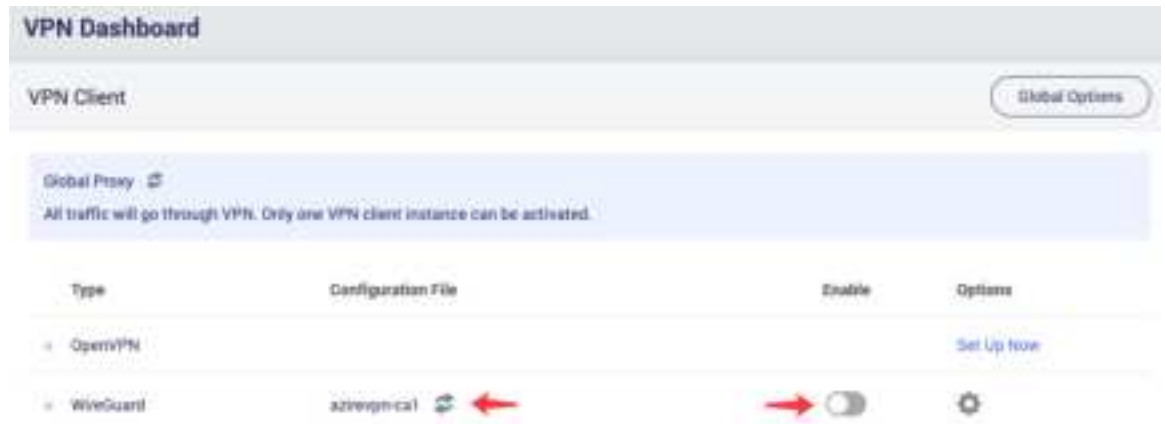
MTU

Optional

Cancel

Apply

4. Go to VPN Dashboard to enable the connection.



Setup WireGuard server on GL.iNet router

You can get a GL.iNet router to set as WireGuard server, and get another GL.iNet router to set as WireGuard client. For setup WireGuard server, please check out [here](#).

Get configuration files from WireGuard service providers

Please check our Docs:

https://docs.gl-inet.com/en/4/tutorials/wireguard_client/#get-configuration-files-from-wireguard-service-providers

7.5 Setup WireGuard Server on GL.iNet router

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

GL.iNet routers have pre-installed WireGuard Server and Client.

Make sure Internet Service Provider assigns you a public IP address

Please check if you Internet Service Provider assigns you a public IP address [here](#).

If no, you can't connect to the WireGaurd Server.

An alternative method is to use a reverse proxy solution, we suggest [AstroRelay](#).

Network Topology

- If GL.iNet router is the main router in your network, this is simple, please move to the next step.
- If you already have a main router, then the GL.iNet router is under the main router, you may need to setup a port forwarding on the main router.
- If you already have a main router, the GL.iNet router is several levels below it and you need to set up port forward on each level.

Setup WireGuard Server

Access to web Admin Panel, on the left side -> VPN -> WireGuard Server.

1. Click **Generate Configuration** (Only the first time).

WireGuard Server

WireGuard® is an extremely simple, fast and modern VPN that utilizes state-of-the-art cryptography.

Please follow the steps below:

1. Generate a WireGuard® configuration file;
2. Add a peer configuration;
3. Copy peer information to the client;
4. Go to the VPN Dashboard page and start the VPN server.

You don't have any peer configuration yet. Get started by adding a peer configuration.

Generate Configuration

2. Apply the configuration

The default configuration works for most cases. Also modify it according to your network situation, click the **Apply** button after modification.

WireGuard Server

The WireGuard server is currently OFF

Start

Configuration

Profiles

IPv4 Address

10.0.0.1/24

Listen Port

51820

i Set Key Manually ▾

Reset

Apply

For **Set Key Manually**.

Configuration

Profiles

IPv4 Address

10.0.0.1/24

Listen Port

51820

Private Key

EMdfXmEjpDjexwGi2O5objzXLmbiv87bGnKGgnfA9UM=

Public Key

A3s38BeCuLX6j1OF/eGYw+5zc/znsVePwQpk1To1TEo=

Set Key Manually

Reset

Apply

3. Add a profile

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

WireGuard Server

The WireGuard server is currently OFF

Start

Configuration

Profiles

Each client device to connect to the WireGuard server requires a unique peer configuration, you need to create a configuration for each device. Each configuration must use a unique client IP.

+ Add

Enter a descriptive name.

Client Configuration

Name

[Set More](#)

Cancel

Apply

Set More is for advanced settings.

Client Configuration

Name

Allowed IPs

Optional

[+ Add New](#)

DNS Server

Optional

MTU

Optional

Keep Alive

Optional

Use Preshare Key

☐

Cancel

Apply

Click **Apply** to continue. It will generate a profile.

WireGuard® Client Configuration



Use DDNS domain to avoid that the client cannot connect to the service because of the change of the public network IP. If you want to use this function, please [Enable DDNS](#) on your router and it can be resolved successfully.

Use DDNS Domain



QR Code

Configuration File



Download

If your network's public IP changes from time to time, you can enable [DDNS](#), then using DDNS domain in the configuration.

Click **Download** to save the profile.

4. Start WireGuard server

Click the **Start** button in the upper right corner to start WireGuard server. Go to VPN Dashboard page to check its status and other settings.

WireGuard Server

⦿ The WireGuard server is currently OFF

Start

To check if WireGuard Server is working properly

To check if WireGaurd Server is working properly, we can use another device connected to another network and use the WireGuard configuration we exported earlier to connect and see whether it connects properly and whether the IP address is the IP of WireGuard Server.

The simpliest way is to use a cell phone with [WireGuard official client app](#) installed, turn off its Wi-Fi connection, and only connect to Internet via 3G/4G/5G. Then open the WireGaurd app, import the WireGaurd configuration from QR code. Enable the connection, check if the phone has Internet access and whether its IP address is the IP of your WireGuard Server.

There are several common reasons cause failed:

- The Internet Service Provider doesn't assign you a public IP address, please check [here](#).
- You may need setup port forwarding, please check [here](#).
- The port you are using for WireGuard Server is blocked by the Internet Service Provider, change to another port, or contact the Internet Service Provider.
- Some countries/regions may block the VPN connection.

WireGuard Client App

We can use another GL.iNet router as WireGuard Client, or use their official app on other devices with various OS.

- Please refer to WireGuard Official Website: <https://www.wireguard.com/install>

How to let all data go through VPN?

If you want all the data on the router to go through vpn, please follow the steps below.

On the left side of web Admin Panel -> VPN -> VPN Dashboard.

In the **VPN Client** section, click **Global Options**, toggle on **Block Non-VPN Traffic**, then click **Apply** button.

Global Options

Block Non-VPN Traffic ⓘ

☐

Allow Access WAN ⓘ

☐

Services from GL.iNet doesn't Use VPN ⓘ

☐

Cancel

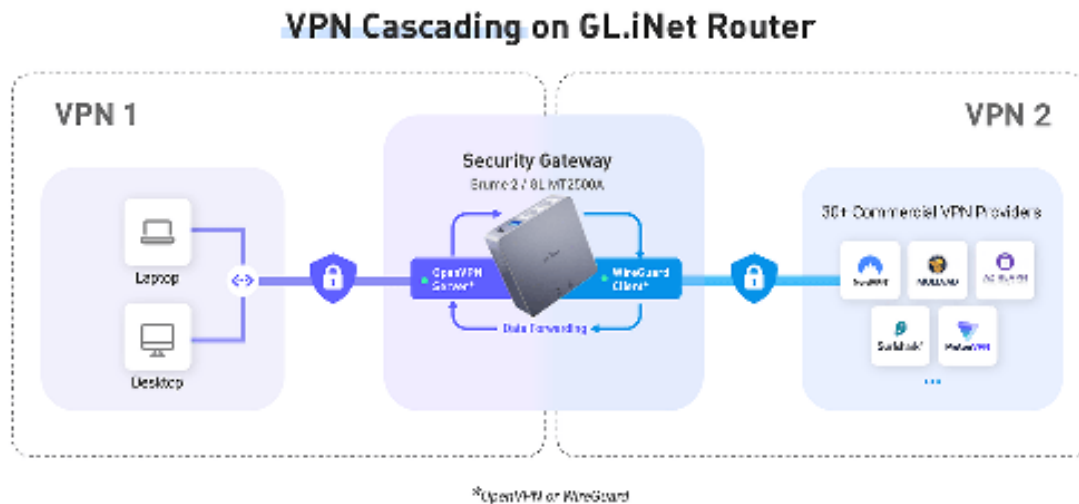
Apply

Note: It need to run the VPN Client, otherwise it can't access the Internet.

VPN Cascading

How VPN Cascading works

VPN Cascading is also called double VPN in various scenarios. But GL.iNet VPN Cascading may be a little different. Please refer to the following figure for the idea.



VPN 1: The router is used as VPN server. Clients connected to this server will go to Internet using the router's ISP Network by default.

VPN 2: The router is used as VPN client to 3rd party VPN services.

VPN Cascading: You can forward data of VPN1 tunnel to VPN2 tunnel. So when the Laptop, Desktop and Smartphones (end devices) connected on VPN1 will go to 3rd party VPN services, without any other setup in these end devices.

How to enable VPN cascading

The following figure has OpenVPN and Wireguard servers enabled on the router. And also connect to NordVPN via OpenVPN protocol.

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
<div> <div></div> <div>OpenVPN</div> </div>	<div>app-nordvpn-Example1.ovpn</div>	<div></div>	<div></div>
<div> <div>Server Address</div> <div>193.176.25</div> </div> <div> <div>Server Listen Port</div> <div>1194</div> </div> <div> <div>Traffic Statistics</div> <div> <div>↑ 24.79 KB</div> <div>↓ 24.39 KB</div> </div> </div> <div> <div>Client/Virtual IP(Pool)</div> <div>10.0.2.4</div> <div>View Log</div> </div>			
<div> <div></div> <div>WireGuard</div> </div>			<div>Get Up Now</div>

VPN Server

Set up VPN Cascading here

Global Options

Type	Tunnel Address	Enable	Options
<div> <div></div> <div>OpenVPN</div> </div>	10.0.0.0	<div></div>	<div> <div></div> <div></div> </div>
<div> <div>↑ 672.00 KB / ↓ 0.00 B</div> <div>View Log</div> </div>			
<div> <div></div> <div>WireGuard</div> </div>	10.0.0.104	<div></div>	<div> <div></div> <div></div> </div>
<div> <div>↑ 0.00 KB / ↓ 0.00 B</div> <div>No Clients</div> <div>View Log</div> </div>			

You can enable VPN cascading in **Global Options** in VPN server section.

Global Options

Enable VPN Cascading ⓘ ☒

Cancel

Apply

Does VPN policy affect VPN Cascading?

- Policies DO NOT affect VPN Cascading

VPN policies, including **Global Proxy**, **Based on the Target Domain or IP**, **Based on the Client Device** and **Based on the VLAN**, does not affect VPN cascading. These policies only affect on the devices connected on the router physically, i.e. in the router's own subnet.

Modify Proxy Mode



Global Proxy

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

Policy Mode



Based on the Target Domain or IP

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



Based on the Client Device

In this mode, only the traffic of certain local client devices defined by MAC address will go through VPN. Only one VPN client instance can be activated.



Based on the VLAN

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

- Policies DO affect VPN Cascading

When you use **Auto Detect** or **Customized Routing Rules**, the routing rules comes with the VPN config or you set up will affect how the router route data so VPN cascading may not work.

Modify Proxy Mode

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.

Tor

Tor (derived from **The Onion Router**) is a free and open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More about the Tor](#).

Note: This feature is currently in beta, and may be problematic in some countries. When Tor is enabled, the following features will not work properly:

- VPN
- DNS
- IPv6
- ADGuard Home.

Supported models¶

Router Model	Support Tor
GL-MT3000 (Beryl AX)	√
GL-AXT1800 (Slate AX)	√
GL-A1300 (Slate Plus)	√
GL-MT2500/GL-MT2500A (Brume 2)	√
GL-SFT1200	√
GL-S1300 (Convexa-S)	√
GL-MT1300 (Beryl)	√
GL-AX1800 (Flint)	√
GL-B1300 (Convexa-B)	√
GL-AP1300 (Cirrus)	√

Setup

Just toggle to enable it, then click **Apply** button. You can also choose a **Custom Exit Nodes**.

Tor

Tor (derived from "The Onion Router") is a free and open-sourcesoftware for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)

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

This feature is currently in beta, and may be problematic in some countries.

Enable ☐

Custom Exit Nodes ☐

Apply

Wait a while, depending on your network, and it will show connected.

Tor

Tor (derived from "The Onion Router") is a free and open-sourcesoftware for enabling anonymous communication. It helps users to explore the internet with privacy. [Learn More >](#)

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

This feature is currently in beta, and may be problematic in some countries.

Enable ☒

Custom Exit Nodes ☐

Tor Log Connected

tor connection succeeded

Apply

1. APPLICATIONS

GL.inet routers include a wide range of add-on features that simplifies device management, improves user's internet experience, automates firmware update, and more.

8.1 Plug-ins

On the left side of web Admin Panel -> APPLICATIONS -> Plug-ins

Plug-ins allows you to manage OpenWrt packages. You can install or remove any package.

It is recommended to click the **Update** button before use.

The following figure shows the Plug-ins page of GL-MT3000.

Name	Version	Size	Action
454x30	12	4.08 KB	install
454x30	28	2.48 KB	install
454x30	10	3.48 KB	install
454x30	13	1.81 KB	install
LCPspeeder	20210116-D-2	70.34 KB	install
acf	2.2.53-1	18.82 KB	Uninstall
acf	2.2.53-1	18.72 KB	Uninstall
acf110	3.0.1-1	50.88 KB	install

Free space: 43.78 % (52.20 MB)

Time Last Update: 2022-05-31 15:01:35

1 2 3 4 ... 1100 Go

8.2 Dynamic DNS

Dynamic Domain Name Service (Dynamic DNS or DDNS) is a service used to map a domain name to the dynamic IP address of a network device.

On the left side of web Admin Panel -> APPLICATIONS -> Dynamic DNS



The screenshot shows the 'Dynamic DNS' configuration page. At the top, there is a header 'Dynamic DNS'. Below it, a light blue box contains a note: 'You can enable Dynamic DNS for this router and access this router remotely. [DDNS Test](#) Note: You need an Internet Public IP address to use the Dynamic DNS. If this router is behind NAT, you may need to set up port forward in your ISP router.' Below the note, there is a 'Host Name' field with the value 'zw72cd7.glddns.com'. Underneath, there is a toggle switch for 'Enable DDNS' which is currently turned off. At the bottom, there is a blue 'Apply' button.

Enable DDNS

Toggle on **Enabled DDNS**, option in Terms of Services & Privacy Policy, then click **Apply** button. Generally it take several minutes to take effect.

DDNS update frequency is once every 10 minutes.

You can enable Dynamic DNS for this router and access this router remotely. [DDNS Test](#)
Note: You need an Internet Public IP address to use the Dynamic DNS. If this router is behind NAT, you may need to set up port forward in your ISP router.

Host Name zw72cd7.glddns.com

Enable DDNS ☒

Enable HTTP Remote Access ☐

Enable HTTPS Remote Access ☐

Enable SSH Remote Access ☐

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

[Apply](#)

Check if DDNS is in effect

Using DDNS Tools.


Click the **DDNS Test**

Dynamic DNS

You can enable Dynamic DNS for this router and access this router remotely. [DDNS Test](#)
Note: You need an Internet Public IP address to use the Dynamic DNS. If this router is behind NAT, you may need to set up port forward in your ISP router.

If it says **Your DDNS is resolved as x.x.x.x** as show below, it means the DDNS is worked. In other words, this **Host Name** has mapped to the final exit IP of the router for Internet access.

DDNS Test×



Your DDNS is resolved as 103.81.180.10



But this router is behind NAT or you do not have a Public IP address.


Retry

HTTP Remote Access

This function requires a public IP address. To check if your Internet Provider Service assign your a public IP address, please check [here](#).

If your router is behind NAT, you may need to set up port forwarding in higher level router. It use port **80**.

Host Name	zw72cd7.glddns.com
Enable DDNS	<input checked="" type="checkbox"/>
Enable HTTP Remote Access 	 <input checked="" type="checkbox"/>
Enable HTTPS Remote Access	<input type="checkbox"/>
Enable SSH Remote Access	<input type="checkbox"/>
I have read and agree Terms of Service & Privacy Policy	<input checked="" type="checkbox"/>



Follow the steps above, to enable HTTP Remote Access.



HTTP is not encrypted, use at your own risk.

After you enable HTTP Remote Access, you can access Admin Panel anywhere by your DDNS Host Name of **http**, e.g. `http://xxxxxxx.glddns.com`. If you use port forwarding, you should be access like `http://xxxxxxx.glddns.com:YourExternalPort`.

HTTPS Remote Access

This function requires a public IP address. To check if your Internet Provider Service assign your a public IP address, please check [here](#).

If your router is behind NAT, you may need to set up port forwarding in higher level router. It use port **443**.

Host Name	zw72cd7.glddns.com
Enable DDNS	<input checked="" type="checkbox"/>
Enable HTTP Remote Access	<input type="checkbox"/>
Enable HTTPS Remote Access	 <input checked="" type="checkbox"/>
Enable SSH Remote Access	<input type="checkbox"/>
I have read and agree Terms of Service & Privacy Policy	<input checked="" type="checkbox"/>
<div>Apply </div>	

After you enable HTTPS Remote Access, you can access Admin Panel anywhere by your DDNS Host Name of **https**, e.g. `https://xxxxxxx.glddns.com`. If you use port forwarding, you should be access like `https://xxxxxxx.glddns.com:YourExternalPort`.

This function use self-signed certificates, so the browsers will indicate that **Your connection is not private**. I will show you how to use it anyway on Chrome Android, other browsers are the similar process. I will turn off the WiFi on my phone and only use 4G to access the Internet.

Open chrome and type the URL in the address bar, I'll use `https://zw72cd7.glddns.com:8001` as an example. Click **Advanced** at the bottom to continue.



▲ //zw72cd7.glddns.com:8001



Your connection is not private

Attackers might be trying to steal your information from **zw72cd7.glddns.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID



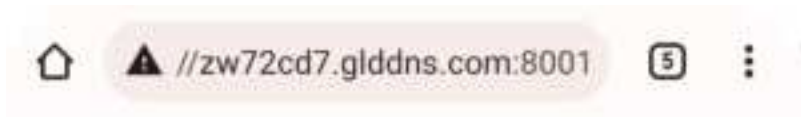
To get Chrome's highest level of security, [turn on enhanced protection](#)

Back to safety



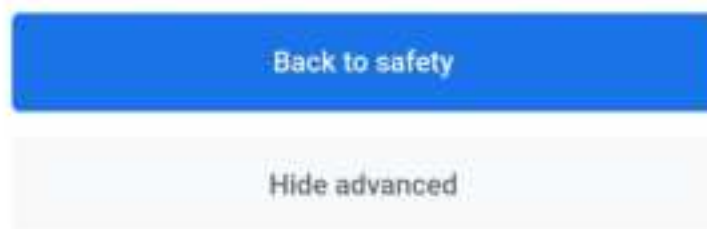
Advanced

Click **Processed to xxxxxxx.glddns.com (unsafe)** to continue.

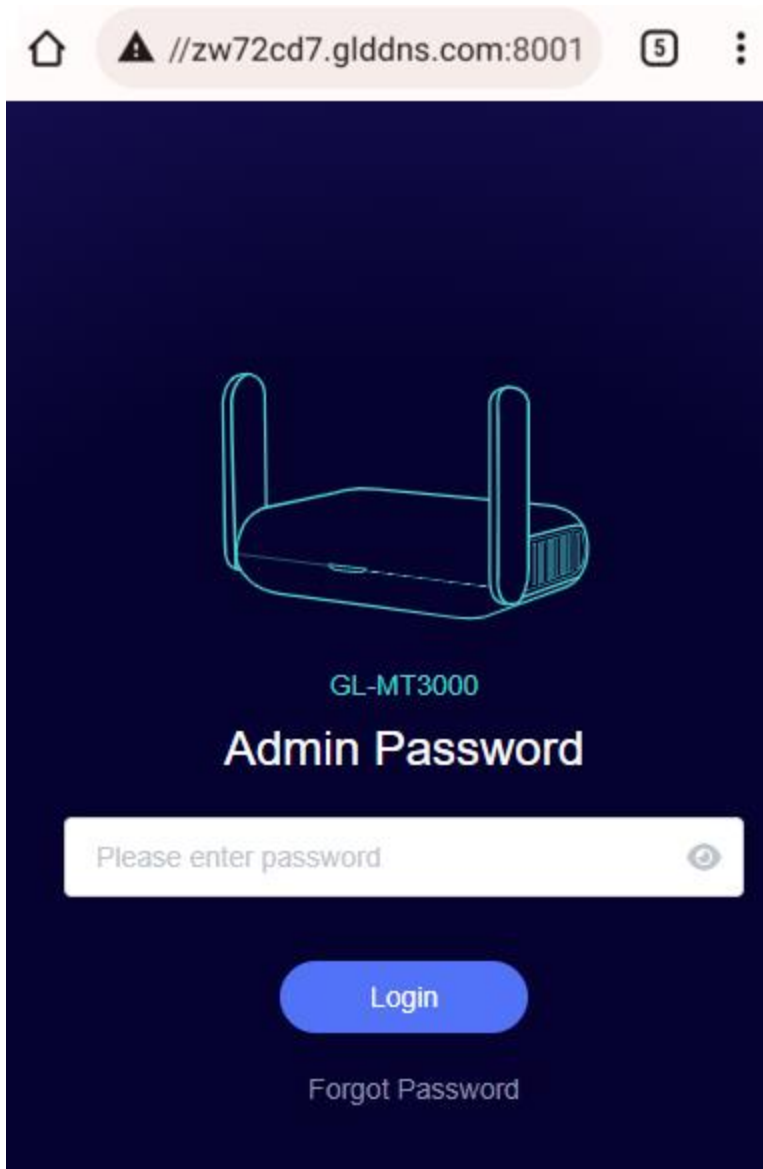


This server could not prove that it is **zw72cd7.glddns.com**; its security certificate is not trusted by your device's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to zw72cd7.glddns.com \(unsafe\)](#)





Then, it will access the web Admin Panel.



SSH Remote Access

This function requires a public IP address. To check if your Internet Provider Service assign your a public IP address, please check [here](#).

If your router is behind NAT, you may need to set up port forwarding in higher level router. It use port **22**.

Host Name	zw72cd7.glddns.com
Enable DDNS	<input checked="" type="checkbox"/>
Enable HTTP Remote Access	<input type="checkbox"/>
Enable HTTPS Remote Access	<input type="checkbox"/>
Enable SSH Remote Access	 <input checked="" type="checkbox"/>
I have read and agree Terms of Service & Privacy Policy	<input checked="" type="checkbox"/>
<div>Apply </div>	

Follow the steps above, to enable SSH Remote Access, then you can ssh to your router anywhere.

Your SSH command should like below.

```
ssh root@xxxxxxx.glddns.com
```

or

```
ssh root@xxxxxxx.glddns.com:YourExternalPort
```

8.3 GL.iNet GoodCloud

Contents

- Introduction
- Setup
 - Enable GoodCloud on router
 - Sign up GoodCloud account
 - Select server region
 - Add a new group
 - Add device
 - Bound info on router web Admin Panel
 - Unbind router
- Manage your devices
 - Devices info and status
 - LTE Signal
 - Device detail info
 - Remote access web Admin Panel
 - Remote access router's terminal
 - Set email alarm
- Site to Site
 - Introduction
 - Conditions
 - Steps to build a Site to Site network
 - Testing the Site to Site connection
 - Route and other options
- Batch Setting
 - Batch Setting of Single Device
 - Batch Setting of Mutiple Devices
 - Other Batch Operations
- Template Management

- [Add a Template](#)
- [Upgrade](#)
- [Apply a template to a router](#)
- [Apply a template to multiple routers](#)
- [Task List](#)
- [GoodCloud and VPN](#)
- [Turn off cloud](#)

Introduction

GL.iNet [GoodCloud](#) cloud management service provide an easy and simple way to remotely access and manage routers. There is a video introduction below.

Introducing GoodCloud, Your Remote Device Management Solution.

Easy Guide to Setting Up your GoodCloud Wi-Fi Management System for SMEs.

Features:

- Check live router status
 - Live online offline status check
 - Live RAM and Load Average check
 - LTE Signal
 - Email alarm about online offline status update
- Set up routers remotely
 - Set up routers (e.g. SSID and Key) remotely
 - Remote SSH
 - Remote access web Admin Panel
- Monitoring clients on routers remotely
 - Check who is on your network
 - Realtime traffic monitoring and block clients
 - Email alarm about new client and block
- Operate routers in batch

- Set up config templates and configure routers in batch
 - Reboot or upgrade routers in batch
- Manage routers in groups
 - Divide devices in different groups
 - Manage devices in one page
- Site to Site
 - Virtual Office: extend your office network to other offices
 - Business Travel: remote access office's OA, CRM, MySQL systems
 - Smart Home: remote access IP camera, NAS and other devices at home

Setup

There is a video tutorial below about how to enable cloud function and bind it to GoodCloud.

Enable GoodCloud on router

On the left side of web Admin Panel -> APPLICATIONS -> 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.
Your device ID is **az0b47a**, Please use this ID to bind the device to your cloud account.

Enable GoodCloud



Enable Remote SSH



Enable Remote Web Access



Device ID

az0b47a

Device MAC

E4:95:6E:40:B4:7A

Device S/N

21d88287cbc189f7

Data Server



Asia Pacific

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



[View Logs](#)

Apply



Follow the steps above, to enable the cloud function, which will allow the router to connect to the GoodCloud server.

- **Remote SSH** is for remote access router's terminal via GoodCloud. Check out [here](#).
- **Remote Web Access** is for remote access router's web Admin Panel via GoodCloud. Check out [here](#).
- **Data Server**, please choose the server which is nearest your devices located. There are three Data Server, **Asia Pacific**(Japan), **America**(Oregon) and **Europe**(Ireland).

Sign up GoodCloud account

Visit <https://www.goodcloud.xyz>, sign up then sign in. If you don't find the verify email, look in spam or check email later. If you have any difficulty with sign up, please send email to support@glinet.biz for help.

Select server region

At the first time when you sign in, it will pop up a dialog to let you select the region, please select the region same as your device selected Data Server on the web Admin Panel ([Step of enable GoodCloud on router](#)).

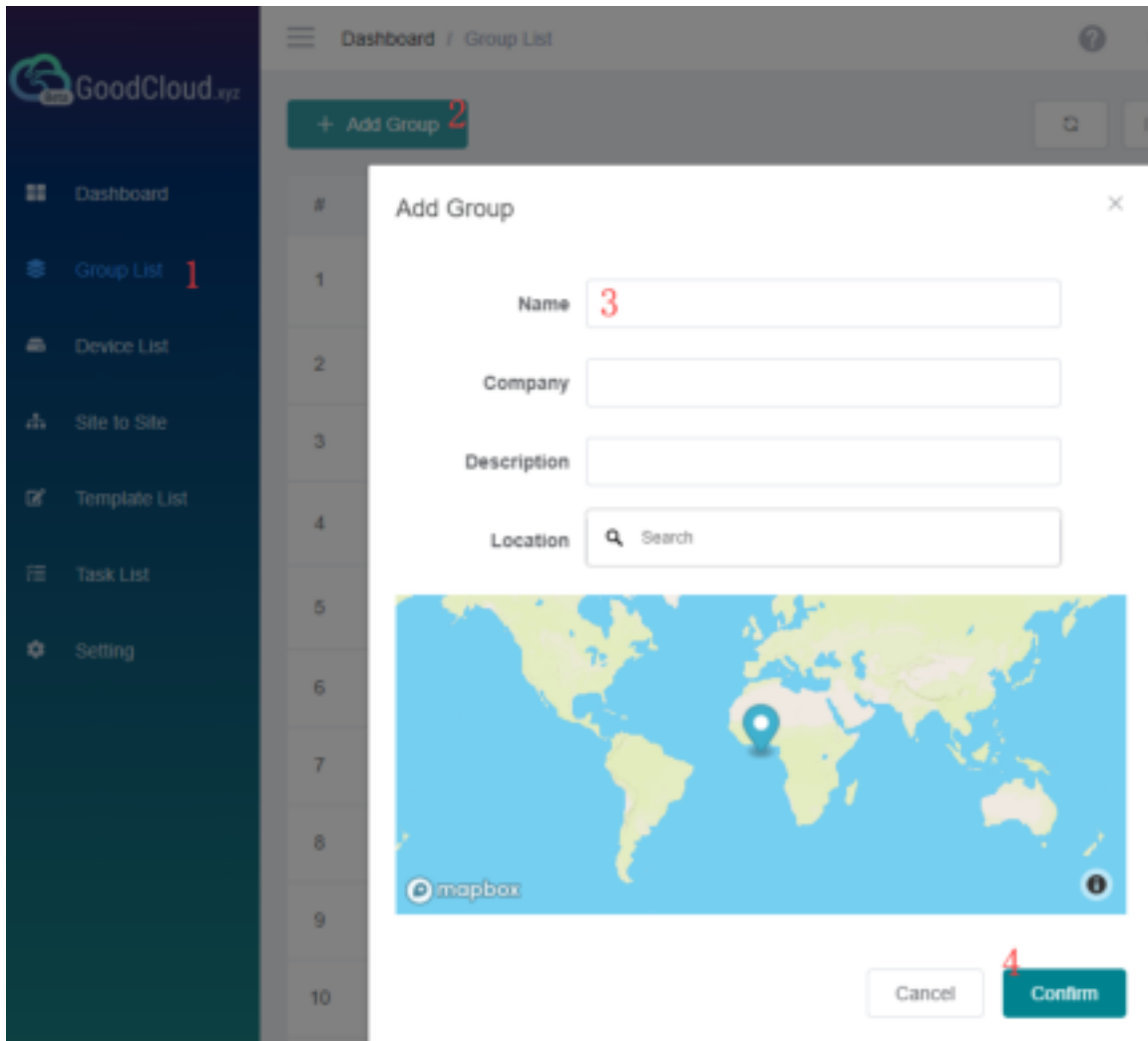
You can change the region on the top right corner at anytime.



Add a new group

On the left side -> Groups List -> Add group.

Follow the steps below to add a new group.



Set the group name, company, description and location.

Each device must belong to a group.

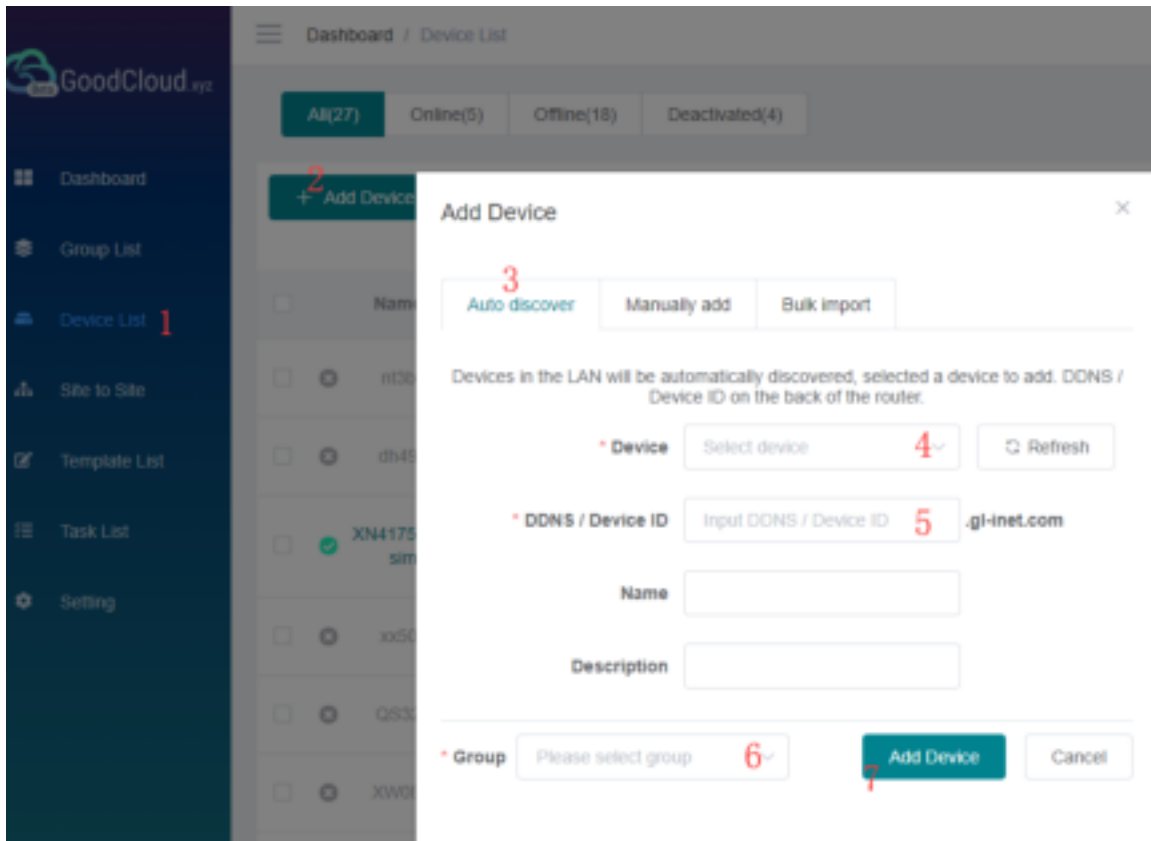
Add device

On the left side -> Devices List -> Add Device. There are three methods to bind device to your GoodCloud account, **Auto discover**, **Manually add** and **Bulk import**.

☐ Auto discover

If your router and PC(which opened GoodCloud website) are in the same network, please try the **Auto discover**.

Follow the steps below to add your device.



Check out [here](#) to find the Device ID.

Note: Input "DDNS/Device ID" here just to verify that the router is really original/valid.

If you haven't added a group before, it will automatically create a default group.

Click Refresh to force auto discover devices again.

Auto discover

Manually add

Bulk import

Devices in the LAN will be automatically discovered, selected a device to add. DDNS / Device ID on the back of the router.

* Device

Select device

Refresh

* DDNS / Device ID

Model: mifi Mac: e4956 ssid: GL-MIFI

Name

Description

* Group

Please select group

Add Device

Cancel

☐ Manually add ☐ Bulk import

Bound info on router web Admin Panel

After you seccessfully add router to GoodCloud, go back to router web Admin Panel, on the left side, APPLICATION -> GoodCloud, refresh this page, It will display the bound GoodCloud username and date.

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.

The device is bound by **leo** on **2022-05-19 10:18**, [Unbind](#)

Enable [GoodCloud](#)



Enable Remote SSH



Enable Remote Web Access



Device ID

zw72cd7

Device MAC

94:B3:C4:17:2C:D7

Device S/N

7faca80bc95c02d3

Data Server

Asia Pacific

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



Apply

[View Logs](#)

Unbind router

If you want to unbind the router, go to router web Admin Panel, on the left side, APPLICATION -> GoodCloud, click **Unbind** button.

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.

The device is bound by **leo** on **2022-05-19 10:18**, [Unbind](#)



Enable [GoodCloud](#)



Enable Remote SSH



Enable Remote Web Access



Device ID

zw72cd7

Device MAC

94:83:C4:17:2C:D7

Device S/N

7faca80bc95c02d3

Data Server

Asia Pacific

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













Apply

[View Logs](#)




Manage your devices

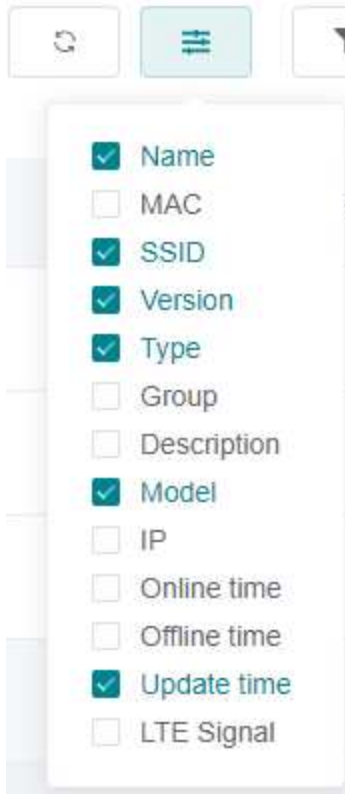
Devices info and status

Sign in [Goodcloud](#), check at left side -> Device List

All(27) Online(5) Offline(18) Deactivated(4)							
<div> <div>+ Add Device</div> <div>⌵ Bulk Action</div> <div>🔍</div> <div>☰</div> <div>More Filter</div> </div>							
<input type="checkbox"/>	Name	SSID	Version	Type	Model	Update time	Actions
<input type="checkbox"/>	 XN41758_2s_simon	GL-AR750-758 GL-AR750-758-5G	3.026	router	GL-AR750	2019-07-26 00:51	
<input type="checkbox"/>	 NC00014_2s_home	GL-AR750-014 GL-AR750-014-5G	3.026	s2s	GL-AR750	2019-07-29 21:49	
<input type="checkbox"/>	 cn00006-wg-client	GL-AR750-3b6 GL-AR750-3b6-5G	3.026	router	GL-AR750	2019-07-29 12:28	
<input type="checkbox"/>	 T8397BC_2s_HKSTP	GL-AR750-7bc GL-AR750-7bc-5G	3.026	s2s	GL-AR750	2019-07-25 18:17	
<input type="checkbox"/>	 YK000ES	GL-AR150-000	3.026	s2s	GL-AR150	2019-07-25 18:17	

there is icon at the first column of this table,

-  means this device is online.
-  means this device is offline.
-  means this device is deactivated, it has never connected to GoodCloud before.



Select the column you want to display.

Online time is the latest time when device connected GoodCloud.

Offline time is the latest time when device disconnected GoodCloud.

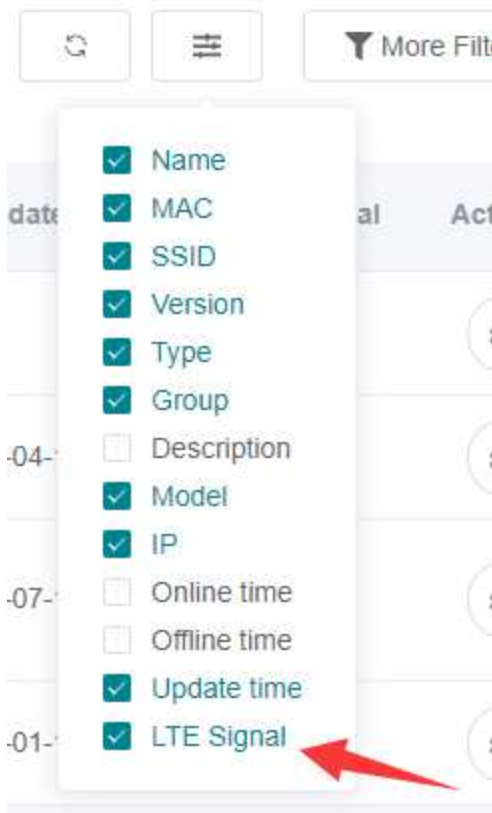
Update time is the latest time when device connected or disconnected GoodCloud.

IP, if your router run VPN client, this IP will be your VPN IP by default. [Learn More](#)

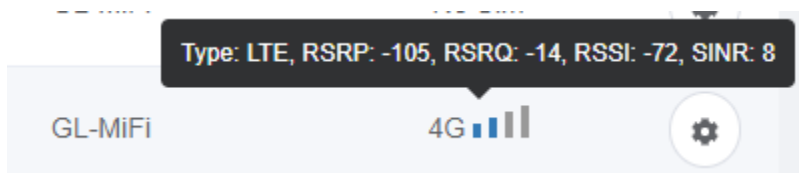
LTE Signal

Only available for 4G devices, e.g. GL-MiFi, GL-X750

Toggle the column on Device List page.



It will show Signal strength, Type, and relevant parameters.



Device detail info

At left side -> Device List, click the name of an online device, it will open a page to manage this device of WiFi, Clients and view router info, memory usage, up time, load average and log.

+ Add Device
⚙ Bulk Action ▾
Export Excel

<input type="checkbox"/>	Name ▾	SSID	Version
<input type="checkbox"/>	<div> <div>✓</div> <div>CI4C5F4</div> </div>	GL-B1300-5f4 GL-B1300-5f4-5G	3.203
<input type="checkbox"/>	<div> <div>✓</div> <div>B2200-Home</div> </div>	GL-B2200-Home	3.107

Device info



✓

CI4C5F4

Group: Office-HK-02

Model:

GL-B1300

MAC Address:

E4:95:5E:44:C5:F4

S/N:

b18819c427a19612

Type:

router

IP Address:

42.42.52.52

Firmware:

3.203




WiFi

2.4G WiFi (Private)

☐

0 Clients

SSID: **GLB1300-5f4**

Channel: auto

SSID Visibility: Shown

TX Power (dBm):

Modify

5G WiFi (Private)

☒

0 Clients

SSID: GL-B1300-5f4-5G

Channel: auto

SSID Visibility: Shown

TX Power (dBm):

Modify

5G WiFi (Guest)

☐

0 Clients

SSID: GL-B1300-0f4-Gu...

Channel: auto

SSID Visibility: Shown

TX Power (dBm):

Modify

2.4G WiFi (Guest)

☐

0 Clients

SSID: GL-B1300-5f4-Gu...

Channel: auto

SSID Visibility: Shown

TX Power (dBm):

Modify

Modify all WiFi settings.

Router status

ROUTER STATUS

Memory usage

59%

Up time

36 Days

19 Hours

5 Minutes

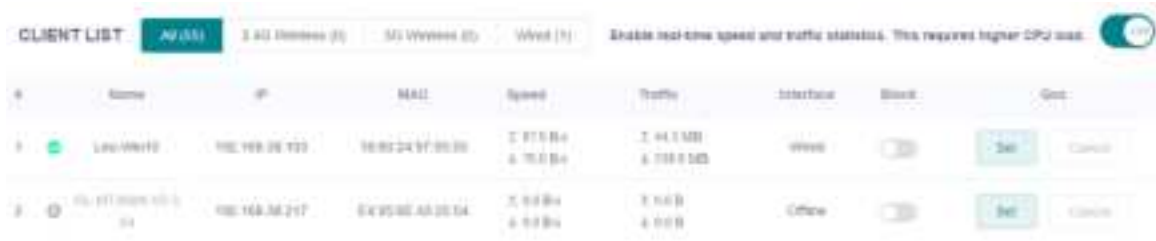
Load average

0.12 1 minute

0.06 5 minute

0.01 15 minute

Client list

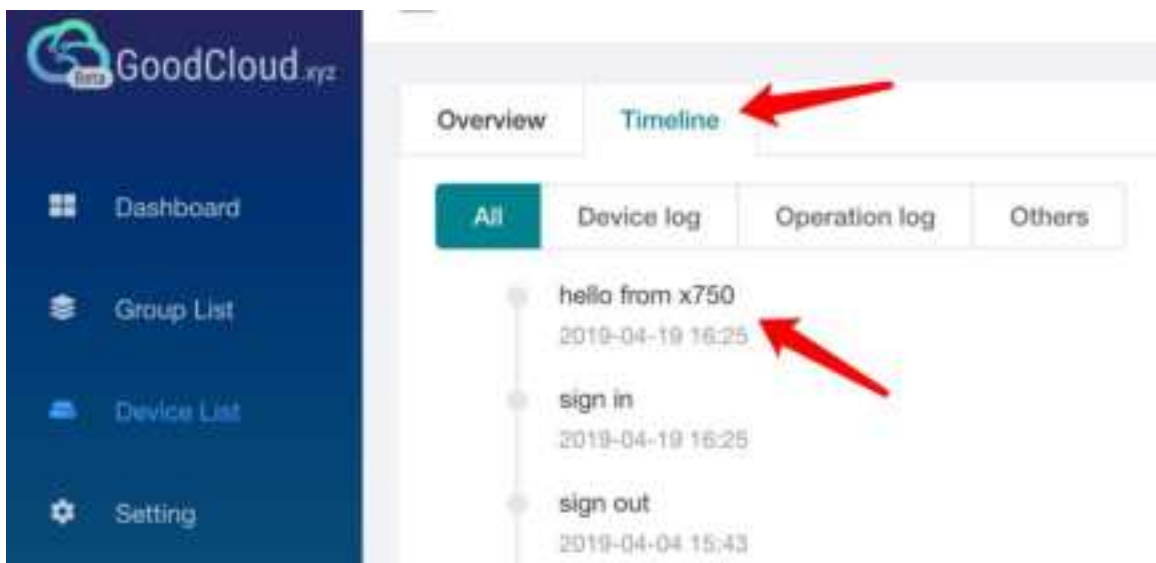


CLIENT LIST: ALL (3) 3 All Wireless (3) 0 Wired (0) 0 Wired (0) Enable real-time speed and traffic statistics. This requires higher CPU usage. ON

#	Name	IP	MAC	Speed	Traffic	Interface	Block	Get
1	Leo-Wifi10	192.168.26.133	18:8F:24:97:90:30	2.875 B/s 4.75.0 B/s	2.44.1 MB 4.738.0 MB	wire	<input type="checkbox"/>	Set Cancel
2	192.168.26.134	192.168.26.134	84:95:8E:AA:20:54	2.14.0 B/s 4.11.0 B/s	2.14.0 B 4.11.0 B	Other	<input type="checkbox"/>	Set Cancel

Timeline

Timeline tab display the activities of router, and messages uploaded by the router's associated IoT device.



GoodCloud.xyz

Dashboard
Group List
Device List
Setting

Overview **Timeline**

All Device log Operation log Others

- hello from x750
2019-04-19 16:25
- sign in
2019-04-19 16:25
- sign out
2019-04-04 15:43

Tools

There are two tools, Ping and Traceroute.

Ping

Traceroute

Remote access web Admin Panel

Note: Please upgrade to 3.211 to use this feature.

If you can't find these icons, please make sure you have enable it, check out [here](#).

If this feature not work, please try the incognito mode of browser.



Remote access router's terminal

Note: Please upgrade to 3.211 to use this feature.

If you can't find these icons, please make sure you have enable it, check out [here](#).

If this feature not work, please try the incognito mode of browser.



Set email alarm

You can set email alarm when a device is online, offline, and new client connected.

At left side -> Setting -> Alarm Setting, create alarm rules

Alarm Rules



When device online/offline Then delay 2 minute to send notification

Enable: device online/offline
new client connected

Cancel Create

Then set the email you want to receive notification. To ensure you get email successful, please add admin@goodcloud.xyz to your email address book.


Alarm Rules

The following alarm information will be sent to Email. Create alarm rules

- When a device is online/offline for 2 minutes, send notification. 🔗 🗑️
- When a client is connected, send notification. 🔗 🗑️

Email Account

The alarm information will be sent to the following Email account. Add an email account

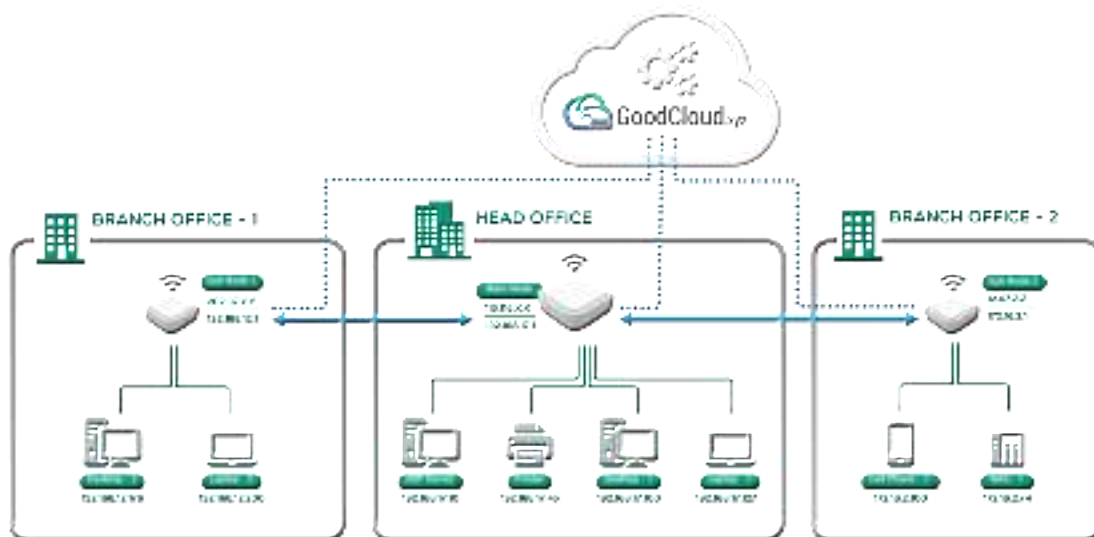

Email

#	Email	Status	Action
1	• john@gmail.com	Enable	🔗 🗑️

Site to Site

Introduction

Site to Site allows offices in multiple locations to establish secure connections with each other over internet. It extends the company's network, making computers resources from one location available to employees at other locations.



Senerio 1: A company has dozens of branch offices that they wish to join in a single private network to share resources.

Senerio 2: A company has a close relationship with a partner company, the Site to Site allows the companies to work together in a secure, shared network environment.

Senerio 3: A family has IP camera and when they are not at home, the Site to Site allows to remote access the IP camera.

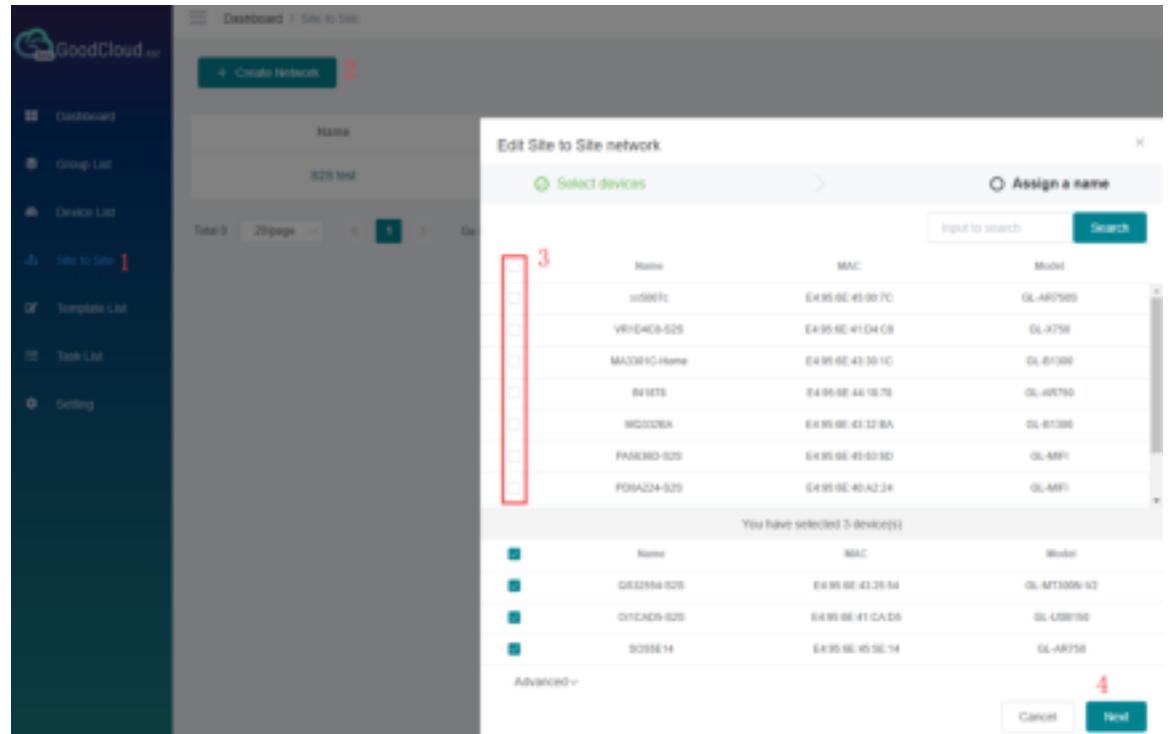
Conditions

It requires at least two routers, each in a different location, one of which has a public IP address. Please [check if your ISP assigns you a public IP address](#). It requires firmware version 3.026 and above.

Note: It is not recommended to run Site to Site while its nodes are also running VPN client, which can make the network particularly complex.

Steps to build a Site to Site network

1. Bind your routers to GoodCloud. ([how?](#))
2. Follow the steps below to create a Site to Site network.



Default port is 51830, if you want to use another port, find the Advanced option at the lower left corner.

Due to the device's performance, each Site to Site network can have up to 10 devices.

After you had chosen the devices, click Continue.

Create a Site to Site network ✕

Select devices ➔ Assign a name

* Name

Description

Back Next

Then, it will test each device if it can be set as the Main Node of Site to Site.

We suggest that the router with strong performance and best network speed to be the Main Node.

Create a Site to Site network ✕



Node Usability Testing

2%

We are testing each device if it can be set as the Main Node of Site to Site.

- One of routers has a public IP, dynamic public IP works.
- Port is open, default is 51030.
- If the router is behind NAT, you may need to set up port forwarding.

Help Cancel Continue

If none of the devices can be used as the Main Node, make sure that:

- One of routers has a public IP, either static public IP or dynamic public IP.
- Port is open, default is 51830.
- If the router is behind NAT, you may need to set up port forwarding.

You can also change port and try again.



If there are more than one device can be set as the Main Node, you need to choose one to continue.



Node Usability Testing

0%

There are multiple devices that can be set as the Main Node of Site to Site, select one and the others will be set as Sub Node.

Select

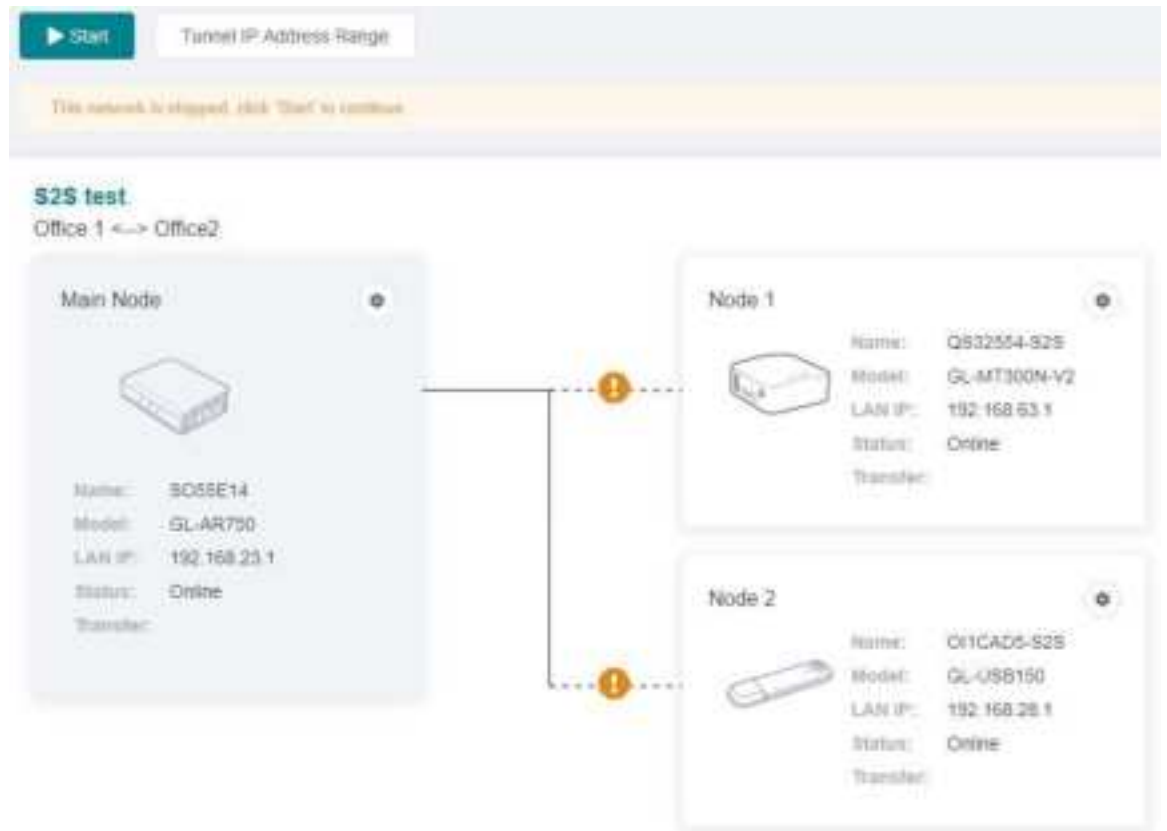
 Help

Cancel

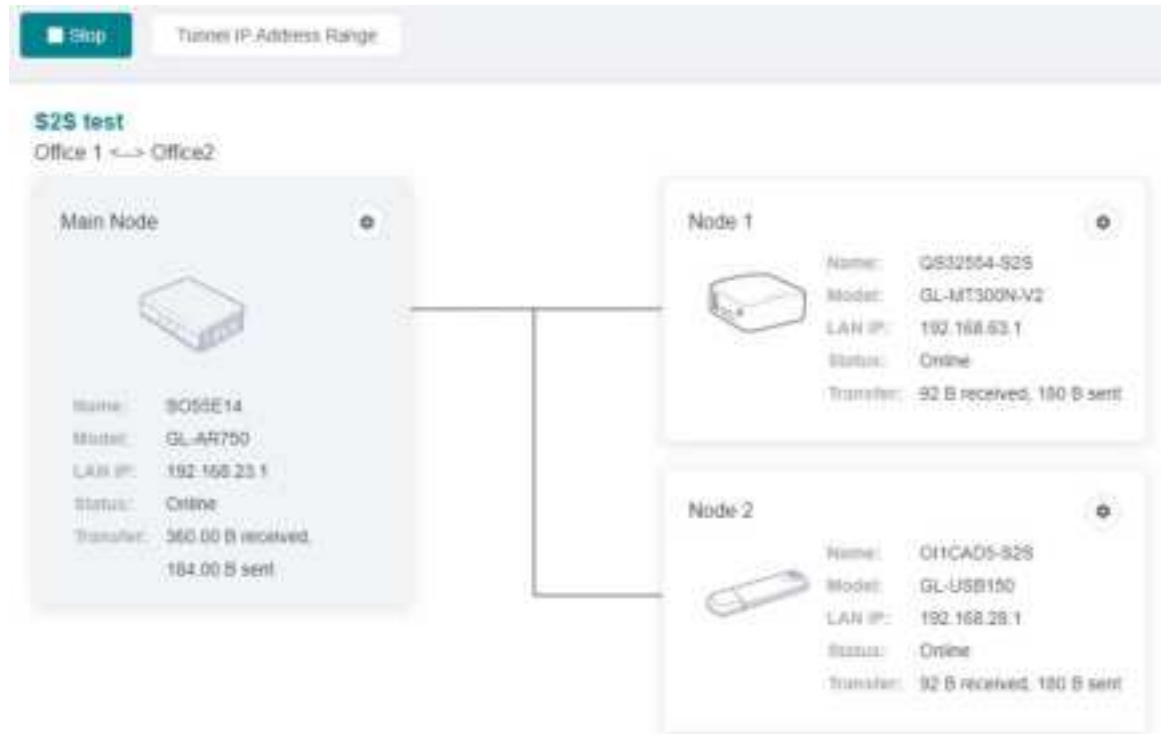
Continue

If there is only one device can be set as the Main Node, it will go to the Site to Site detail page directly.

The network is stopped by default, check the LAN IP, if it is OK then you need to click Start button, otherwise click Setting to change LAN IP.



Wait a few minutes, the node's connect status will display as lines. Solid line means connected, dashed line means disconnected.



Testing the Site to Site connection

Now the Site to Site network is created and started, let's test the connection.

Use your PC or Phone to connect to one of the Node of this Site to Site, and use browser to access another Node's LAN ip, if you see the login page, the connection between these two nodes is worked.

For example, my PC connect to Node 1 device, and then I use browser to access Main Node's LAN IP (192.168.48.1), if I see the login page, it means the connection between Node1 and Main Node is worked.

Route and other options

You can change each device's LAN IP and routes.

Configure LAN IP and Access Control



LAN IP

172.30.97.1

Allow be Access for the Following Subnets ⓘ

Route	Action
172.30.97.0/24	<input checked="" type="checkbox"/>
172.30.55.0/24	<input type="checkbox"/>

eg: 192.168.1.0/24

Add

Cancel

Confirm

By default, each node can access other's LAN, based on security, we recommend only open the corresponding service IPs.

E.g. There is a Server A(172.30.97.100) in Node 1's subnet, if you want other Site nodes only can access Node 1's Service A, you can set it like below:


Configure LAN IP and Access Control



LAN IP

172.30.97.1

Allow be Access for the Following Subnets

Route	Action
172.30.97.0/24	<input type="checkbox"/>
172.30.55.0/24	
172.30.97.100/32	

You can add node's parent routes too.

Each sub Node build an encrypted tunnel network to Main Node, if you want to change the IP of tunnel subnet. Click 'IP Address Range'.

Tunnel IP Address Range



IP address range defines the scope of Site to Site network. Devices will acquire tunnel IP address from the IP address range. Current IP address range is: 172.30.55.0/24

Simple

Advanced

- ☐ 10.148.18.0/24 ☐ 10.148.19.0/24 ☐ 10.148.20.0/24
- ☐ 172.30.97.0/24 ☐ 172.30.98.0/24 ☐ 172.30.99.0/24
- ☐ 192.168.191.0/24 ☐ 192.168.192.0/24 ☐ 192.168.193.0/24

Apply change will cause network go down a few minutes.

Cancel

Save

Save & Apply

Batch Setting

You can use this feature to configure multiple parameters for a single device, or you can configure multiple parameters for multiple devices.

Note: This feature is only available to business users.

Batch Setting of Single Device

To configure single device, as show below.



The left side of image below is correct. If your interface is like the right side of image below, please upgrade to latest testing firmware.



Check the configuration that needs to be modified and input value.

Configure batch modification

Note: The checked configuration is required. Only the selected configuration will be delivered.

Choose Template

ALL

WIRELESS

2.4G Wireless

5G Wireless

Guest 2.4G

Guest 5G

UPGRADE

MORE SETTINGS

Admin Password

LAN IP

Time Zone

2.4G Wireless

ON / OFF

ON OFF

1

Wi-Fi Name (SSID)

test

2

Wi-Fi Security

Select

Required

Wi-Fi Key

SSID Visibility

Select

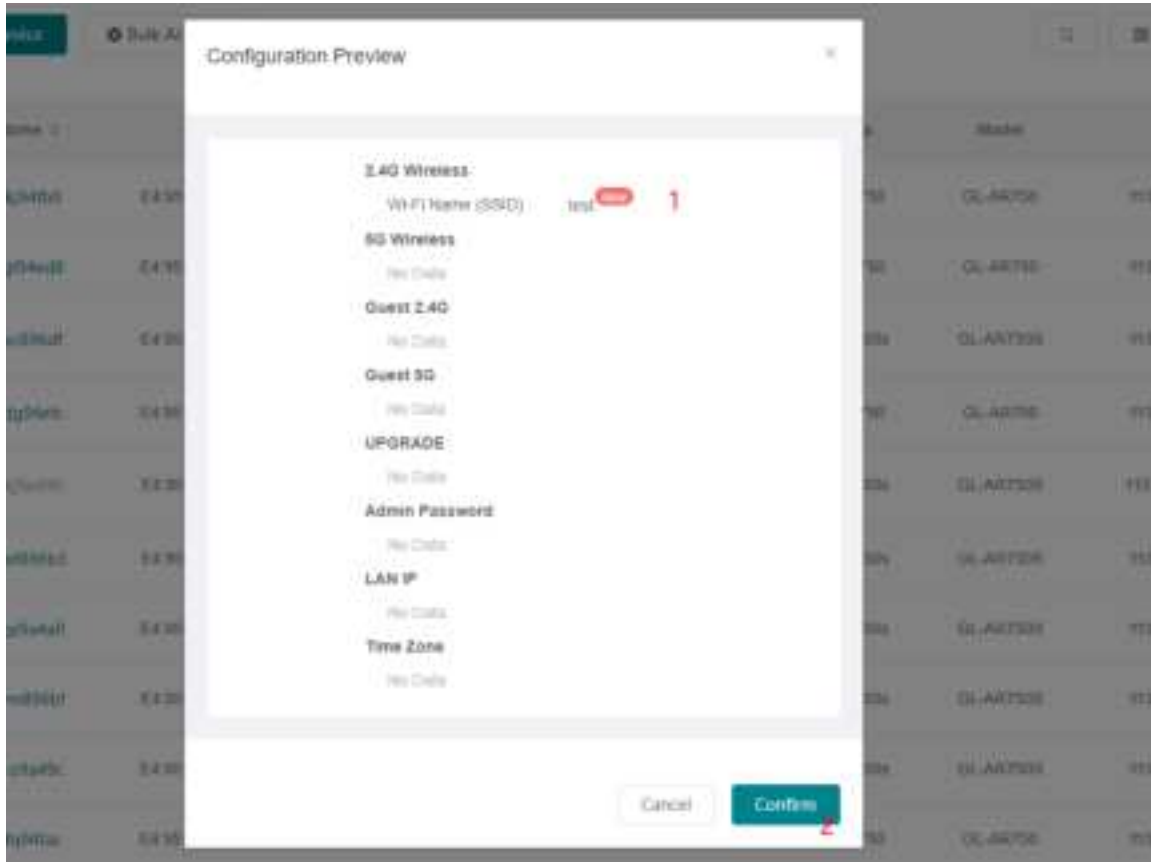
☐ Restart now

Cancel Reset Apply 3

The checked configuration is required, and only the configuration that conforms to the rule can be filled out. After the configuration is delivered, it does not take effect immediately. The configuration takes effect and the device needs to be restarted. You can check the Restart now option in the

lower right corner of the above figure. After the configuration is completed, the device will restart immediately.

Preview the configuration and confirm the delivery.

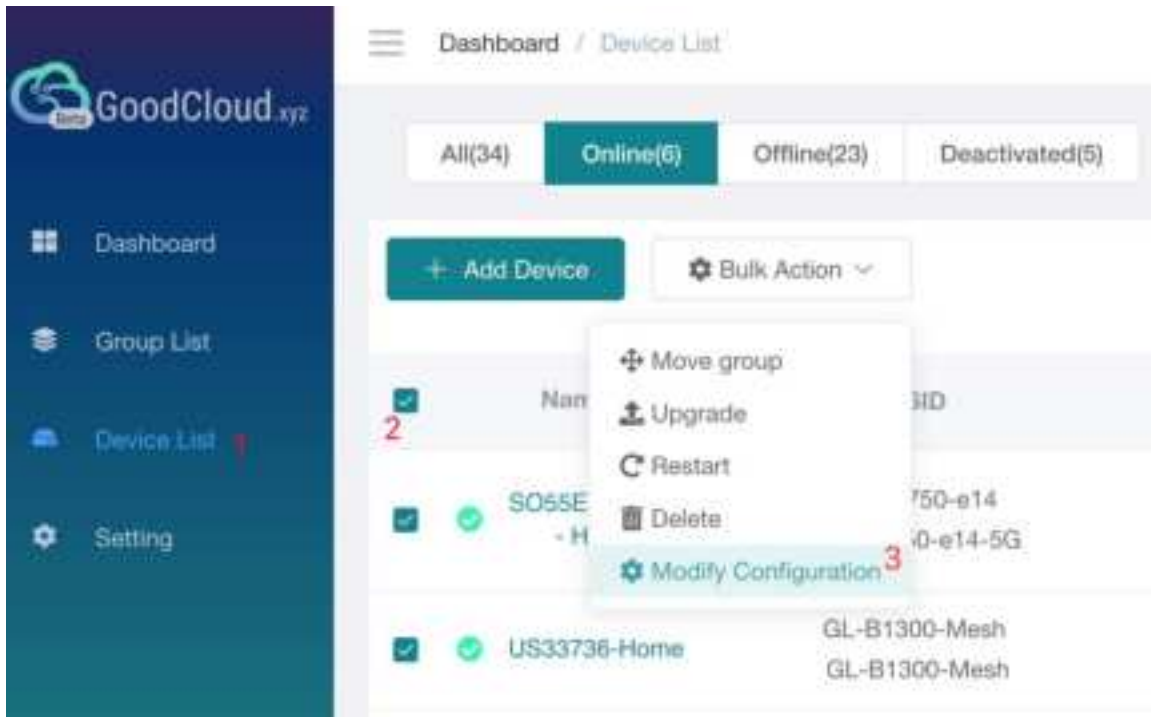


Unchecked **Restart now** option will prompt.



Batch Setting of Mutiple Devices

Select the devices you want to configure.



Other operations are the same as when operating a single device.

Other Batch Operations

Other Batch Operations: Move to other group, upgrade, restart, delete.



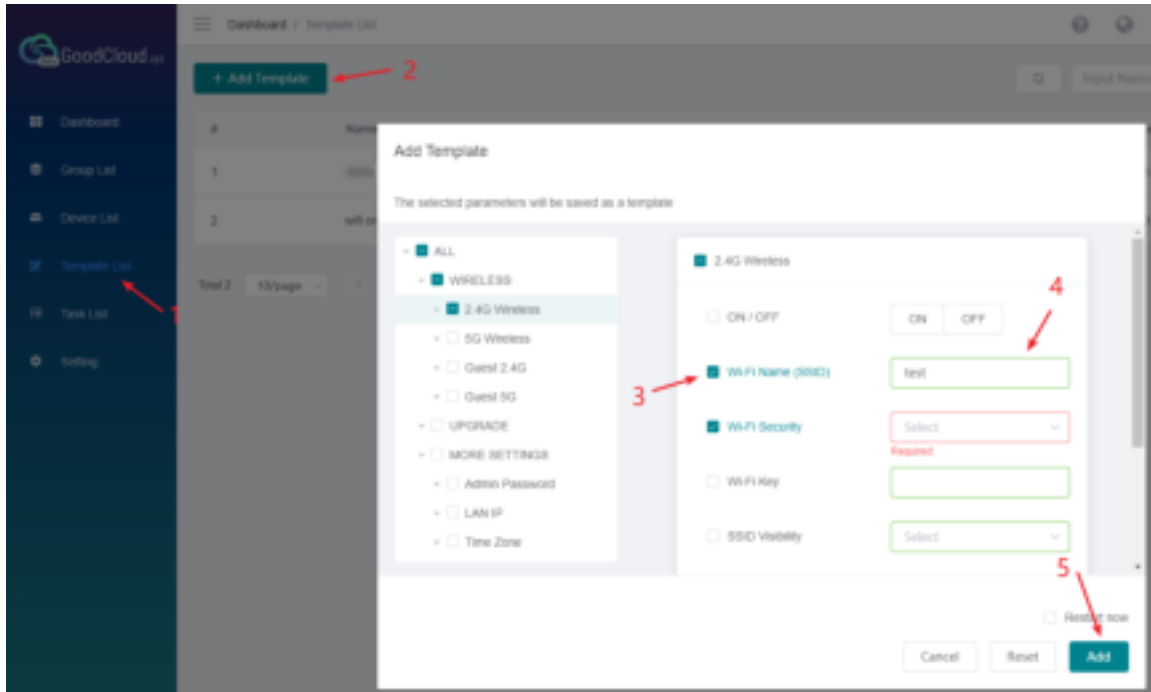
Template Management

Save frequently used configurations as templates and quickly apply them when you modify configurations in batches.

Note: This feature is only available to business users.

Add a Template

Check the configuration that needs to be modified and input value. Most of the options are the same as those on web Admin Panel.



Upgrade

Upgrade Path is for upgrading custom firmware. Put the firmware and a text file on a web server, then put the url path on the **Upgrade Path**. For example, <https://fw.gl-inet.com/firmware/ar750/v1/> is a Upgrade Path, it has a **list-sha256.txt** file <https://fw.gl-inet.com/firmware/ar750/v1/list-sha256.txt> and a corresponding firmware file <https://fw.gl-inet.com/firmware/ar750/v1/openwrt-ar750-3.203-0701.bin>.

Note: GL-AX1800, GL-S1300, GL-B1300, GL-AP1300 only support http path for now.

Add Template

The selected parameters will be saved as a template

ALL

☐ Internet

☐ WIRELESS

☐ 2.4G Wireless

☐ 5G Wireless

☐ Guest 2.4G

☐ Guest 5G

☒ UPGRADE

☐ MORE SETTINGS

☐ Admin Password

☐ LAN IP

UPGRADE

☐ Enable Auto Upgrade

ON
OFF

☐ Auto Upgrade Time

Select

☒ Upgrade Path

Required

Cancel
Reset
Add

The content of the text file is like [this](#), its name should be **list-sha256.txt**. It has 4 columns, the first column is firmware version, the second column is the name of firmware file, the third column is the sha256 of firmware file, the fourth column is the size of firmware file.

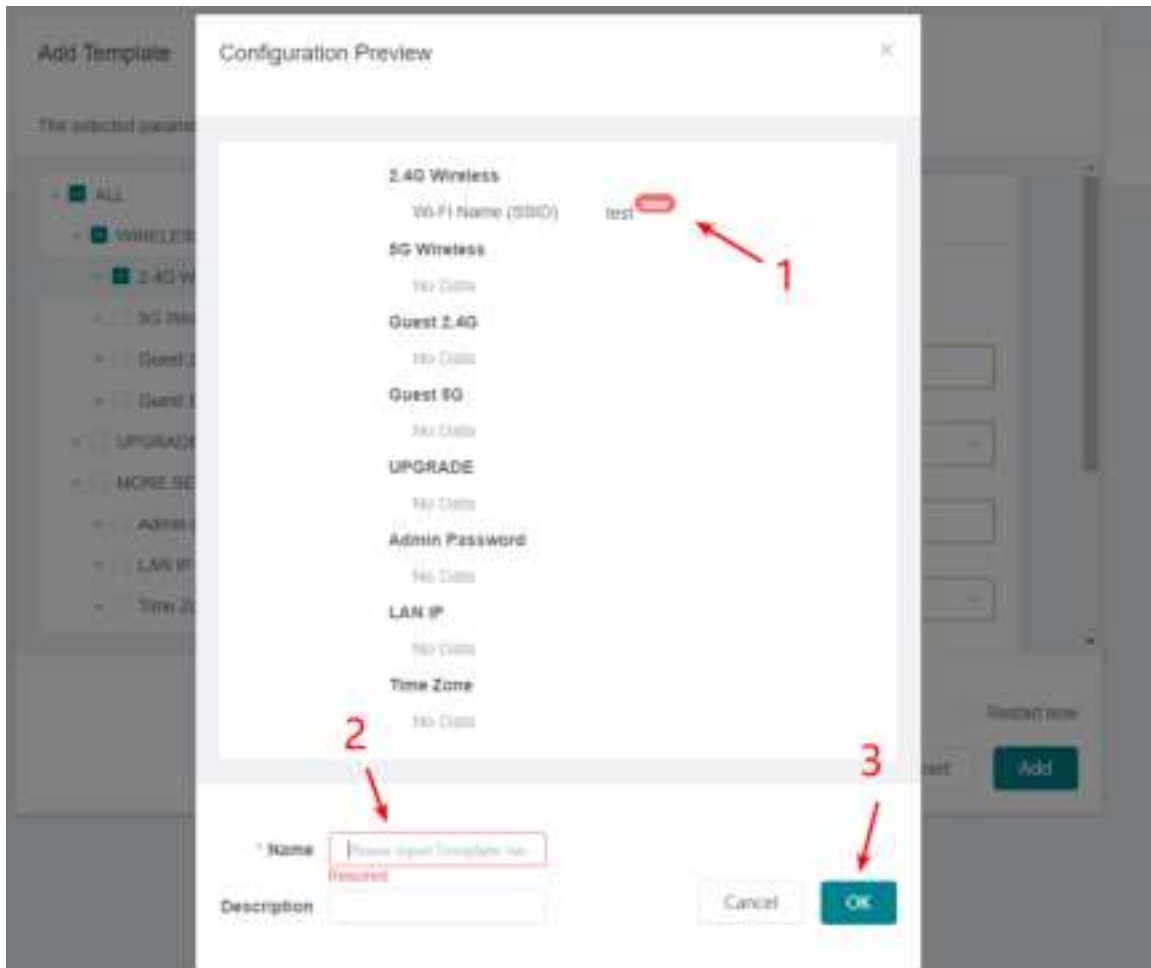
<https://fw.gl-inet.com/firmware/ar/5.0/v1/list-sha256.txt>

1.201	openwrt-ar750-1.201-8781.bin	d54d7416d6e301717c4bsha256c429ae916ad1728172e87d0f6d06f0fe7bd7e1d	12618800
-------	------------------------------	---	----------

Give the template a name and description.

GL·iNet

Page 136 | 178



Apply a template to a router

If you have created a template, then want to apply this template to a router. On the **Device List** page, find the router that you want to apply the template, make sure it is online, on the Actions column, click the cog icon, click **Modify Configuration** item. It will pop up a dialog **Configure batch modification**.

On the top right corner of the dialog, you can choose a template that has already created. Then click **Apply** button on the bottom right corner.

It will pop up another dialog to review the configuration of the template, scroll down to the bottom to click the **Confirm** button, it will load the configuration of template overwrite to this time modification.

Click **Apply** button, please note that the router will restart to take effect after click the **Apply** button.

Apply a template to multiple routers

If you have created a template, then want to apply this template to multiple routers. This procedure is similar to that applied to a single router. On the **Device List** page, multiple select routers, then click **Bulk Action**, click **Modify Configuration** item. It will pop up a dialog **Configure batch modification**.

On the top right corner of the dialog, you can choose a template that has already created. Then click **Apply** button on the bottom right corner.

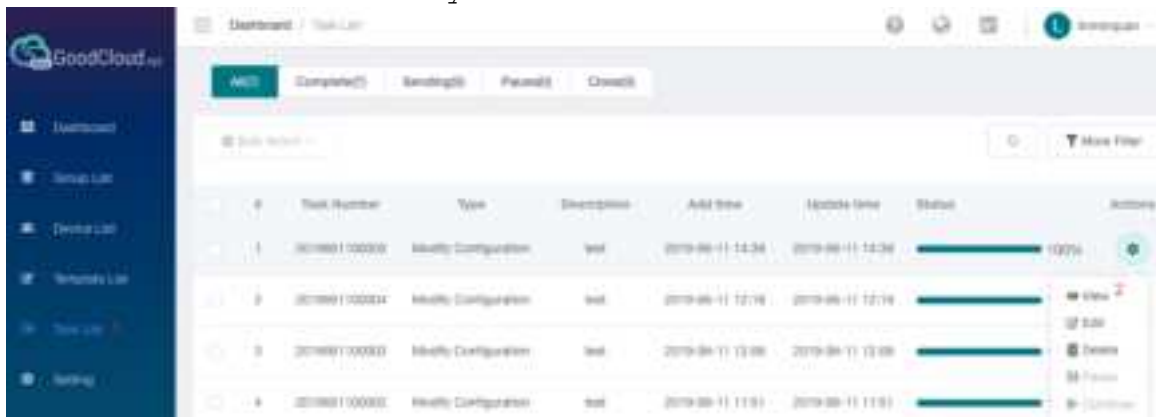
It will pop up another dialog to review the configuration of the template, scroll down to the bottom to click the **Confirm** button, it will load the configuration of template overwrite to this time modification.

Click **Apply** button, please note that the router will restart to take effect after click the **Apply** button.

Task List

At task list page, it shows the execution result of the configuration template.

Note: This feature is only available to business users.



The screenshot shows the 'Task List' page in the GoodCloud interface. The page has a sidebar with navigation options: Dashboard, Device List, Template List, Task List (selected), and Setting. The main content area displays a table of tasks. At the top, there are tabs for 'Add', 'Completed(5)', 'Sending(5)', 'Failed(5)', and 'Queue(5)'. Below the tabs, there is a search bar and a 'More Filter' button. The table has columns for 'Task Number', 'Type', 'Description', 'Add Time', 'Modify Time', 'Status', and 'Actions'. The table contains four rows of tasks, all of which are 'Modify Configuration' tasks and have a status of 'Succeeded'.

#	Task Number	Type	Description	Add Time	Modify Time	Status	Actions
1	2019091100000	Modify Configuration	test	2019-09-11 14:24	2019-09-11 14:24	100%	View
2	2019091100004	Modify Configuration	test	2019-09-11 12:16	2019-09-11 12:16	100%	View
3	2019091100003	Modify Configuration	test	2019-09-11 13:00	2019-09-11 13:00	100%	View
4	2019091100005	Modify Configuration	test	2019-09-11 11:53	2019-09-11 11:53	100%	View

You can view the execution result of each device and configuration.

Total Devices 2 Success 2 Failure 0

#	Name	Model	MAC	Status
1	PT3F4C6	GL-MiFi	E4:95:6E:...	Success
2	ea40ff	GL-MiFi	E4:95:6E:...	Success

[View Config](#) [OK](#)

GoodCloud and VPN

If you enable GoodCloud function and running VPN client at the same time on router, by default, the connection between the router and the GoodCloud server will also go through the VPN, but sometimes the VPN connection is unstable, or the VPN provider mistakenly filters the GoodCloud connection, you can make the GoodCloud connection not go through the VPN by using the following settings.

Go to web Admin Panel, on the left side, VPN -> VPN Dashboard -> VPN Client -> Global Options.

Global Options

Block Non-VPN Traffic ⓘ ☐

Allow Access WAN ⓘ ☐

Services from GL.iNet doesn't Use VPN ⓘ ☐

[Cancel](#) [Apply](#)


It is not recommended to run Site to Site while its nodes are also running VPN client, which can make the network particularly complex.


Turn off cloud


To stop GoodCloud service, turn it off on router web Admin Panel. Please follow the steps below. No action needed on the GoodCloud website.

GoodCloud

i 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.
The device is bound by **leo** on **2022-05-19 10:18**, [Unbind](#)

Enable [GoodCloud](#) 

Enable Remote SSH 


Enable Remote Web Access 

Device ID zw72cd7

Device MAC 94:B3:C4:17:2C:D7

Device S/N 7faca80bc95c02d3

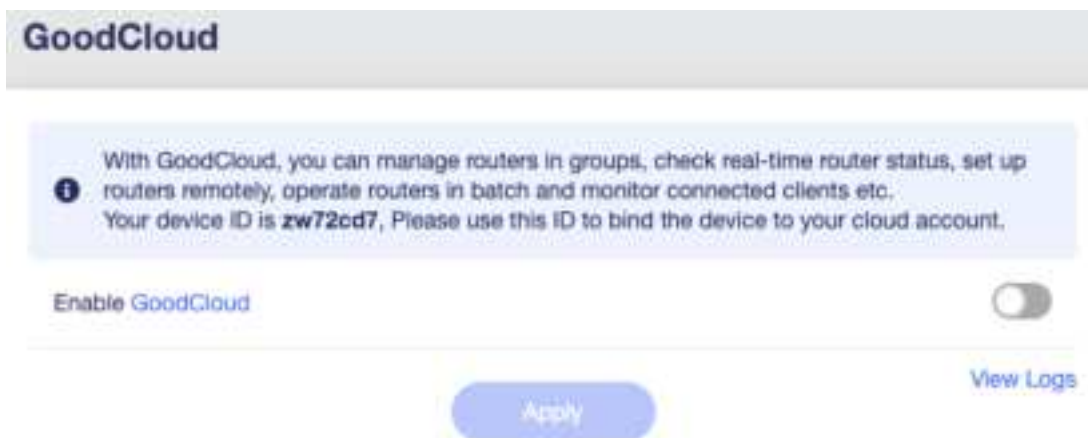
Data Server Asia Pacific

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

[View Logs](#)

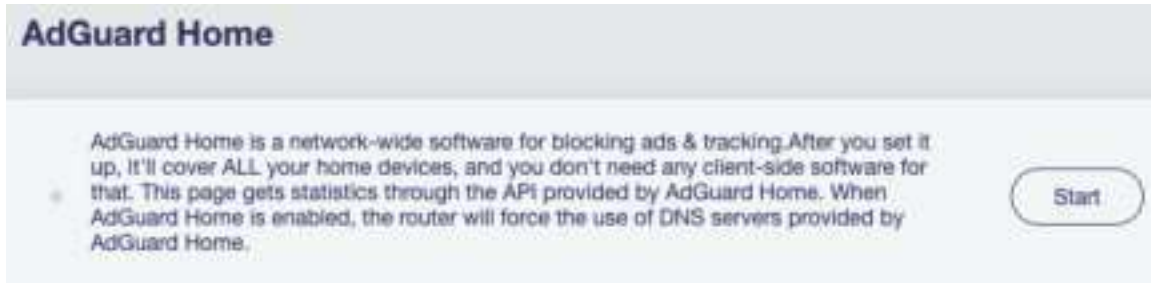
[Apply](#)

After disable Cloud, the interface is like below.



8.4 AdGuard Home


AdGuard Home is a network-wide software for blocking ads & tracking. Click **Start** button to continue.



When it starts, click **Setting Page** for advanced configuration.



It will go to the AdGuard Home's own settings page. If you have any questions, please visit [Adguard Home Support Center](#) for help.


ADGUARD
HOME

[Dashboard](#)
[Settings](#)
[Filters](#)
[Query Log](#)
[Setup Guide](#)

Dashboard
[Disable protection](#)
[Refresh statistics](#)

0

DNS Queries

0

Blocked by Filters

0%

0

Blocked malware/phishing

0%

0

Blocked adult websites

0%

General statistics
for the last 24 hours

DNS Queries	0
Blocked by Filters	0
Blocked malware/phishing	0
Blocked adult websites	0
Enforced safe search	0
Average processing time	0

Top clients
for the last 24 hours

Client	Requests count
No clients found	

Top queried domains
for the last 24 hours

Domain	Requests count
No domains found	

Top blocked domains
for the last 24 hours

Domain	Requests count
No domains found	

[Homepage](#)
[Privacy Policy](#)
[Report an issue](#)

English

Copyright © 2022 AdGuard

Version v0.107.8

8.5 Network Storage

Contents

- [Introduction](#)
- [Insert storage device](#)
- [Set up Samba](#)
- [Set up WebDAV](#)
- [Set up DLNA](#)
- [Samba Client](#)
- [WebDAV Client](#)

Introduction

Some GL.iNet models support TF card, some models have USB port and support USB flash drive and portable external hard drive, you can set up Samba, WebDAV, DLNA on this page for the disk.

The supported disk formats are NTFS, exFAT, FAT32, Ext3, Ext4.

Insert storage device

For TF card, you need to power off the router first, insert the TF card and then power on the router.

For USB Drive, you can directly plug it into the USB port. For portable external hard drive, if you have a separate power supply, please connect it to the power supply.

Go to web Admin Panel -> APPLICATIONS -> Network Storage

Network Storage

This page only provides the shared folder management function. If you need to manage the files in your storage device, please [Use the Smartphone Apps](#) .

Disk Management

No Device Detected

File Services

Shared Folders

User Management

Samba

Enable Samba

WebDav

Enable WebDav

DLNA

Enable DLNA

Apply

When a disk is found.

Disk Management			
Disk Name	Type	Disk Size	Eject
Leo (disk1_part1)	USB Flash Drive	57.93 GB free of 58.17 GB	

Set up Samba

Toggle to enable Samba, click **Apply**.



File Services

Shared Folders


User Management

Samba

Enable Samba




Allow Access Samba from WAN




WebDav

Enable WebDav




DLNA

Enable DLNA



Apply



Go to **Shared Folder** tab. Click **+ Add** button to add a shared folder.

File Services

Shared Folders

User Management

 You need to enable the corresponding file service (Samba/WebDav) to access your shared folders through this protocol.

+ Add

Choose a folder to share, then click **Next**.

Add Shared Folder

▼ disk1_part1
Picture cats
Peppa Pig

Cancel

Next

For security reasons, we do not recommend enabling **Anonymous Access**.

If you leave the **Anonymous Access** off, you need to create a user by clicking the **+ Add User** button or choose an existing user, and then check the user in the option **Writable User** or **Read-Only User**. The User is for the connection to the Samba Server. You can manage the user in the **User Management** tab.

Finally, click the **Apply** button.

Shared Folder Settings

Path

/disk1_part1/Peppa Pig

Share Protocol

Samba

Samba Settings

Share Name

Peppa Pig

Anonymous Access

☐

Writable User

david

Read-Only User

[+ Add User](#)

Back

Apply

That is it. The access link can be found in **Shared Link**.

File Services

Shared Folders

User Management

You need to enable the corresponding file service (Samba/WebDev) to access your shared folders through this protocol.

+ Add

Path	Access Protocol	Validity	Action
/disk1_part1/Peppa Pig	Samba	Usable	<div><div>...</div><div><div>Shared Link</div><div>Setting</div><div>Add Extra Protocol</div><div>Delete</div></div></div>

Click **Shared Link**, it will show the access link for each system. The Unix-like system include Android, iOS, macOS, Ubuntu etc.

Note: If you enabled **Allow Access Samba from WAN** and access from WAN, you need to replace the Router IP (default 192.168.8.1) in the figure below with WAN IP which can be found in the INTERNET page.

Folder Access Link		×
Windows SMB	\\192.168.8.1\Peppa Pig	
Unix-like Samba	smb://192.168.8.1/Peppa Pig	

Then try to access the Samba on various OS, check out [here](#).

Set up WebDAV

Toggle to enable WebDAV.

For the protocol, **HTTP** is not encrypted, using on your risk; **HTTPS** is encrypted, it uses self signed certificate.

Then click **Apply**.

File Services

Shared Folders

User Management


Samba

Enable Samba

☐

WebDav

Enable WebDav

☒

Allow Access WebDav from WAN

☐

WebDav Protocol

HTTP

WebDav Port (HTTP)


6008

DLNA

Enable DLNA

☐

Apply



Go to **Shared Folder** tab. Click **+ Add** button to add a shared folder.

File Services

Shared Folders

User Management

 You need to enable the corresponding file service (Samba/WebDav) to access your shared folders through this protocol.

+ Add

Choose a folder to share, then click **Next**.

Add Shared Folder

▼ disk1_part1
Picture cats
Peppa Pig

Cancel

Next

Select the **Share Protocol** as **WebDAV**.

For security reasons, we do not recommend enabling **Anonymous Access**.

If you leave the **Anonymous Access** off, you need to create a user by clicking the **+ Add User** button or choose an existing user, and then check the user in the option **Writable User** or **Read-Only User**. The User is for the connection to the WebDAV Server. You can manage the user in the **User Management** tab.

Finally, click the **Apply** button.

Shared Folder Settings

Path

/disk1_part1/Peppa Pig

Share Protocol

WebDav

WebDav Settings

Anonymous Access

☐

Writable User

david

Read-Only User

+ Add User

Back

Apply

That is it. The access link can be found in **Shared Link**.

File Services

Shared Folders

User Management

You need to enable the corresponding file service (Samba/WebDav) to access your shared folders through this protocol.

+ Add

Path	Access Protocol	Validity	Action
/disk1_part1/Peppa Pig	WebDav	Usable	<div><div>...</div><div><div>Shared Link</div><div>Setting</div><div>Add Extra Protocol</div><div>Delete</div></div></div>

Click **Shared Link**, it will show the access link for each system. The Unix-like system include Android, iOS, macOS, Ubuntu etc.

Note: If you enabled **Allow Access Samba from WAN** and access from WAN, you need to replace the Router IP (default 192.168.8.1) in the figure below with WAN IP which can be found in the INTERNET page.

Folder Access Link		×
HTTPS	https://192.168.8.1:6008/disk1_part1/Peppa Pig	
Dav	dav://192.168.8.1:6008/disk1_part1/Peppa Pig	

Then try to access the WebDAV on various OS, check out [here](#).

Set up DLNA

Toggle to enable DLNA, modify **Share Path** if needed, click **Apply**. That is it.

File Services

Shared Folders

User Management

Samba

Enable Samba

☐

WebDav

Enable WebDav

☐

DLNA

Enable DLNA

☒

Share Path

/disk1_part1

Modify

Apply

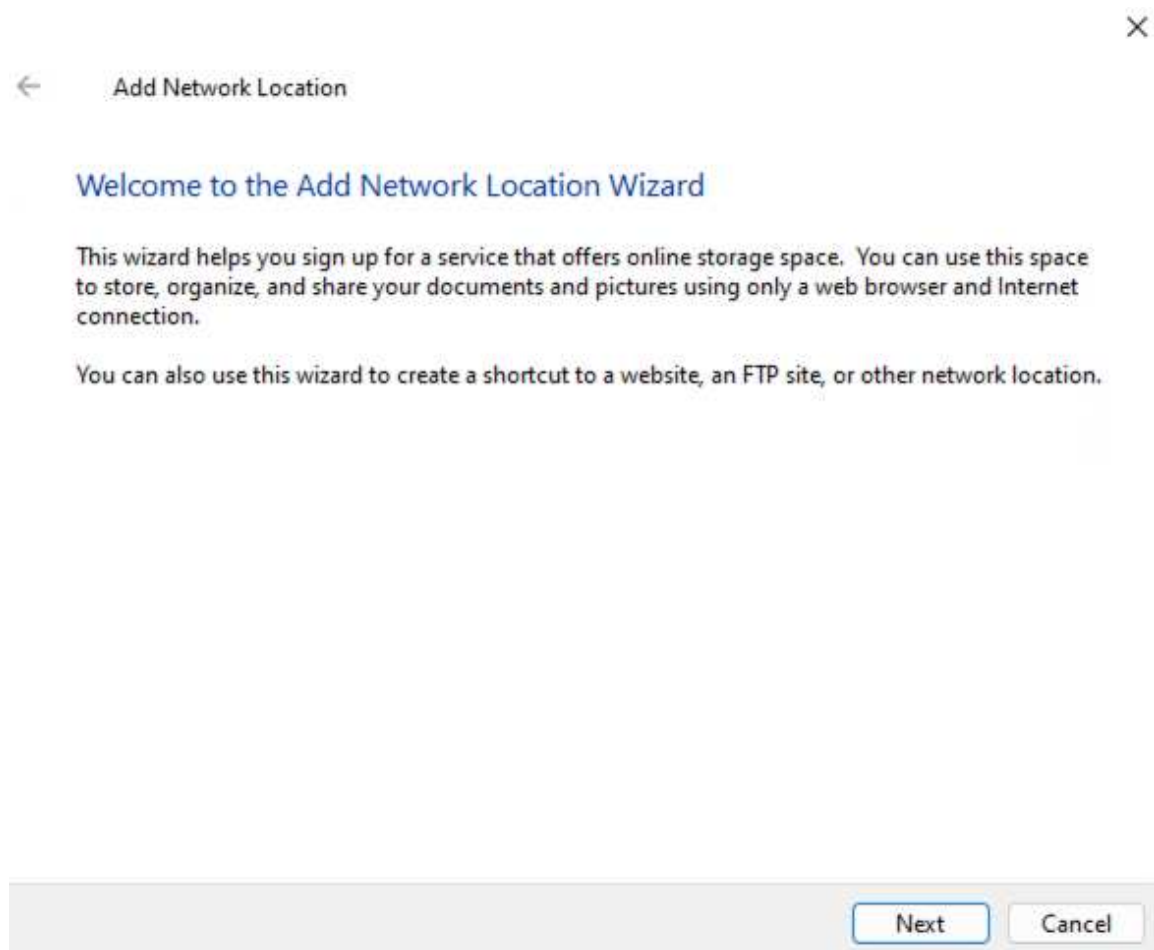
Connect your smart TV to the router, it will find the DLNA Server.

Samba Client

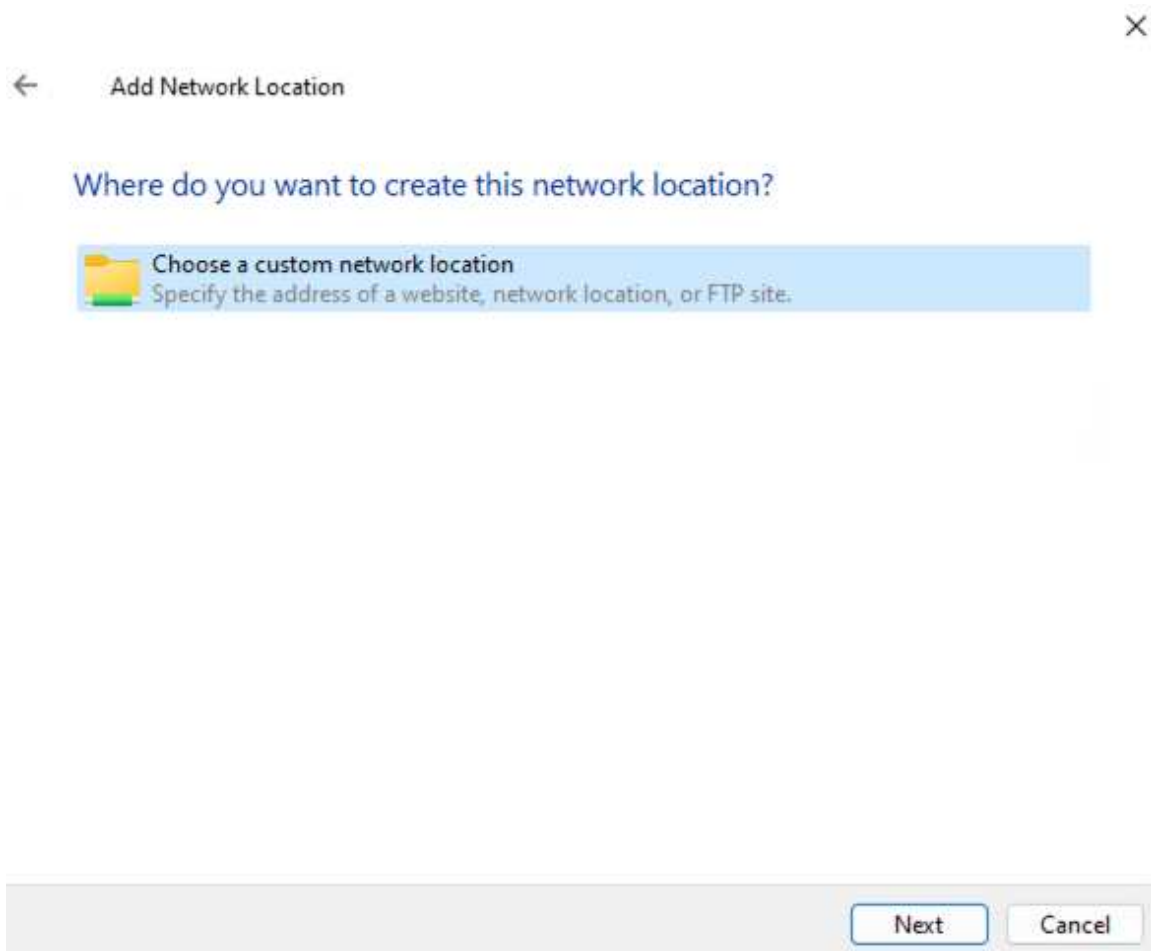
☐ Windows

Here is an example of Windows 11, Windows 10 is similar.

Open up File Explorer and then right-click on **This PC** (in the left pane). From the resulting context menu, select **Show more options** -> **Add a network location**



Click **Choose a custom network location** and then click **Next**.



Enter the Samba access link. Then click **Next**.



Add Network Location

Specify the location of your website

Type the address of the website, FTP site, or network location that this shortcut will open.

Internet or network address:

[View examples](#)

Give a name of this location. Click **Next**.

×

← Add Network Location

What do you want to name this location?

Create a name for this shortcut that will help you easily identify this network location:

\\192.168.8.1\Peppa Pig.

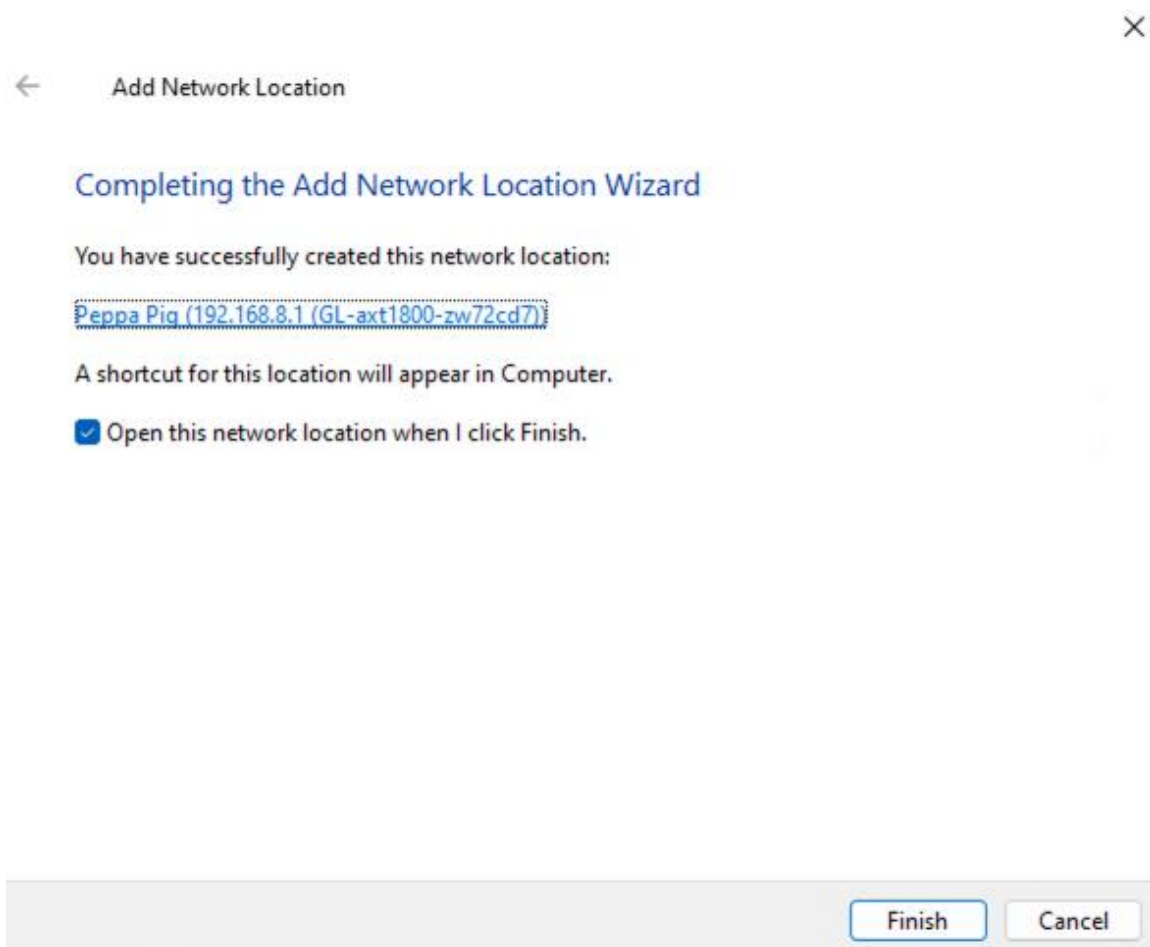
Type a name for this network location:

Peppa Pig (192.168.8.1 (GL-axt1800-zw72cd7))

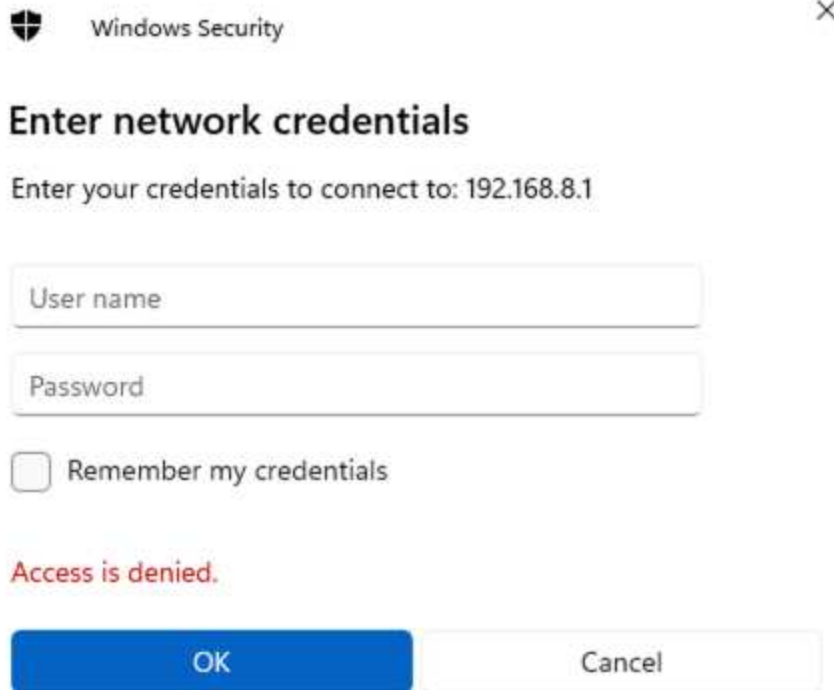
Next

Cancel

Click **Finish**.



If it need username and password, it will ask to enter the credential. Then click **OK**.



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.8.1

User name

Password

☐ Remember my credentials

Access is denied.

OK Cancel

☐ Mac OS ☐ Android ☐ iOS

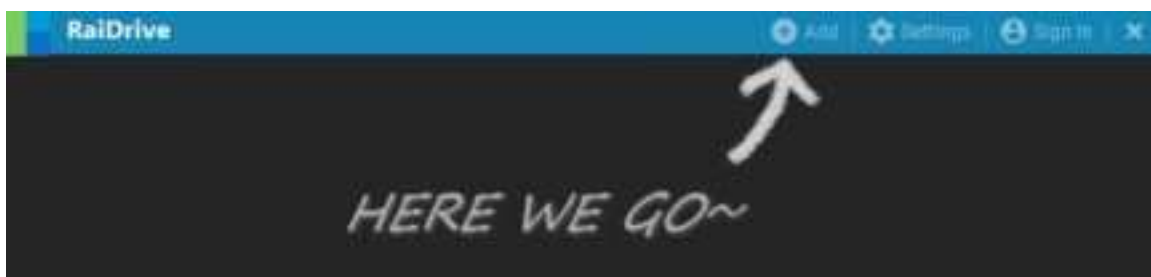
WebDAV Client

☒ Windows

There is a lot of software that supports WebDAV, for example [RaiDrive](#), [Cyberduck](#), [WinSCP](#).

Here is an example of RaiDrive.

Click **Add**.

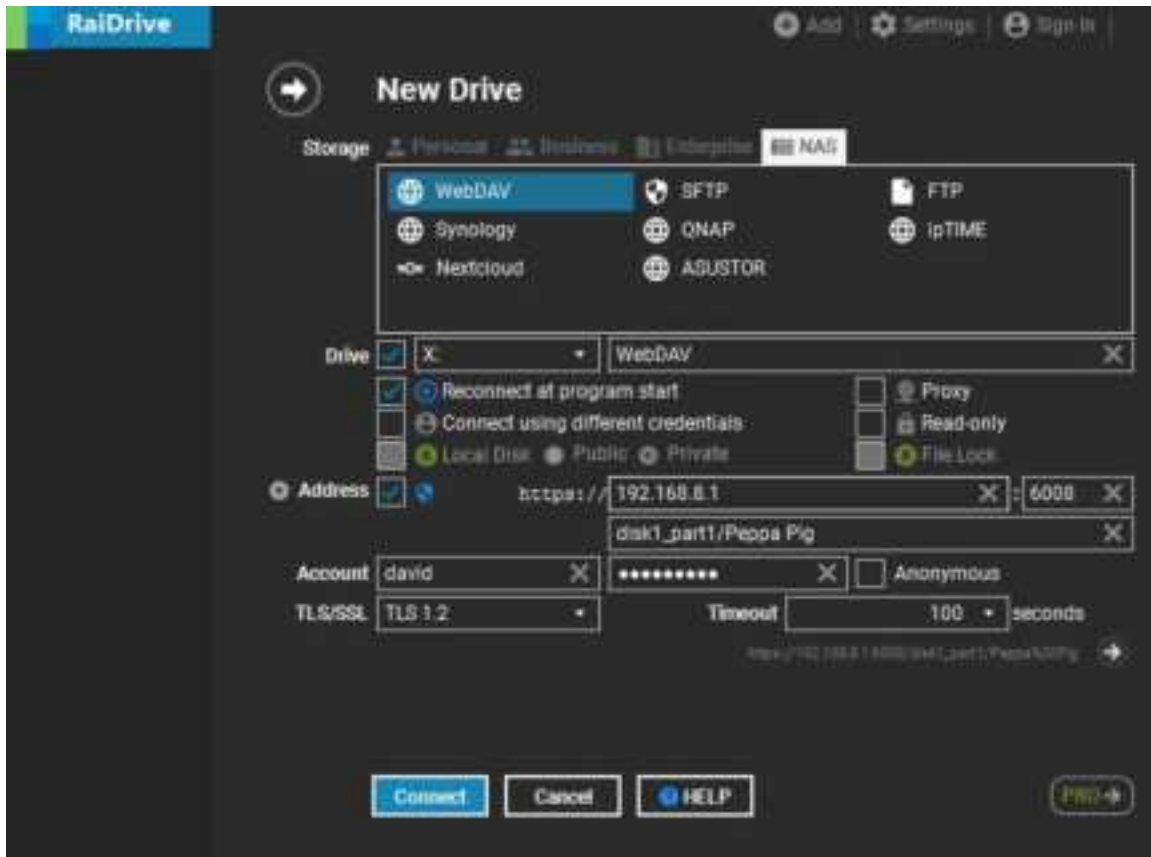


In the **Storage** area, click **NAS** -> **WebDAV**.

In the **Address** area, check/uncheck the checkbox near Address to switch https/http, enter the address.

In the **Account** area, enter username and password, or check the **Anonymous**.

Finally, click **Connect**, it will add a X drive in the File Explorer.



8.6 Log

On the left side of web Admin Panel -> APPLICATIONS -> Log.

The Log page allows you to view logs of System, Kernel, Crash, Cloud for analysis and troubleshooting.



Click **Refresh** to get the latest log information.

Click **Export Log** to export log information of System, Kernel, Crash and Cloud. When you give feedback to GL.iNet, you can send the exported log file to GL.iNet technical support for faster problem analysis.

2. MORE SETTINGS

9.1 Admin Password

On the left side of web Admin Panel -> MORE SETTINGS -> Admin Password

Admin Password

Old Password

Enter old password

New Password

Enter new password

Confirm Password

Enter new password again

Prevent Weak Password

Apply

Change the password of login the web Admin Panel. You have to input your current password to change it.

For security reasons, we recommend that you turn on **Prevent Weak Password**.

When **Prevent Weak Password** is turned on, the requirements for new passwords are as follows.

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

9.2 LAN

On the left side of web Admin Panel -> MORE SETTINGS -> LAN

LAN

Private Network Guest Network

Router IP Address ⓘ 192.168. .1

Maximum Number of Users

Start IP Address

End IP Address

[Advanced](#)

ⓘ When you specify a reserved IP address for a client within the LAN, the client always receives 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: Configured clients have to reconnect the router to activate.

Private Network

The **Private Network** is the network if your devices connect to the Main WiFi or connect via an ethernet cable.

The **Router IP Address** is **192.168.8.1** by default. You can change it if it conflicts with your network.

Private Network

Guest Network

Router IP Address ⓘ
192.168.
8
.1

Maximum Number of Users
150

Start IP Address
192.168.8.100

End IP Address
192.168.8.249

Advanced

Apply

You can just simply change the **Maximum Number of Users** to fit your need. Or click **Advanced** for more manually settings.

Private Network

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

Router IP Address ⓘ
192.168.8.1

Netmask
255.255.255.0

Start IP Address
192.168.8.100

End IP Address
192.168.8.249

Reserve an IP for a client

When you specify a reserved IP address for a client within the LAN, the client always receives 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: Configured clients have to reconnect the router to activate.

Click **Add** to reserve an IP.

When you specify a reserved IP address for a client within the LAN, the client always receives 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: Configured clients have to reconnect the router to activate.

Add

Select the **MAC**, it will fill the **IP** automatically after select MAC. Give it a descriptive name. Then click **Submit**.

Add A New Reservation Entry

MAC	<input type="text"/>
IP	<input type="text"/>
Name	<input type="text" value="Optional"/>

CancelSubmit

Guest Network

The **Guest Network** is the network if your device connect to the Guest WiFi.

The **Default Gate Way** is **192.168.9.1**, If you have enable the Guest WiFi and it conflicts with your network, you can change it.

Private Network

Guest Network

Default Gateway

192.168.9.1

Maximum Number of Users

150

Start IP Address

192.168.9.100

End IP Address

192.168.9.249

Advanced

Apply

You can just simply change the **Maximum Number of Users** to fit your need. Or click **Advanced** for more manually settings.

Private Network**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

Default Gateway

192.168.9.1

Netmask

255.255.255.0

Start IP Address

192.168.9.100

End IP Address

192.168.9.249

Apply


9.3 Time Zone

On the left side of web Admin Panel -> MORE SETTINGS -> Time Zone

The time of the router's activities will be recorded according to the router time. So, make sure you have sync/select the right time zone.

It does not automatically synchronize the time zone and requires a click on the **Sync** button.

Time Zone

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

Sync

Router Time

Thu, Jun 9, 2022 8:31 AM (UTC+00:00)

UTC

Apply

After synchronization.

Time Zone

Router Time

Thu, Jun 9, 2022 4:32 PM (UTC+08:00)

Asia/Hong Kong

Apply

9.4 DNS

On the left side of web Admin Panel -> MORE SETTINGS -> DNS

If you set custom DNS servers, any dns name will be resolved through the DNS servers set here instead of the one obtained from wan, repeater, cellular, hotspot sharing or VPN configuration DNS server.

The screenshot shows the DNS configuration interface. At the top, there is a header bar with the title 'DNS' on the left and an 'Edit Hosts' button on the right. Below the header, a light blue informational box contains a note: 'If you set custom DNS servers, any dns name will be resolved through the DNS servers set here instead of the one obtained from wan, repeater, cellular, hotspot sharing or VPN configuration DNS server.' Below this, there are two toggle switches: 'DNS Rebinding Attack Protection' and 'Override DNS Settings for All Clients', both currently turned off. Underneath these is a section titled 'DNS Server Settings'. It contains a 'Mode' dropdown menu set to 'Automatic'. Below the dropdown is a field labeled 'DNS from Ethernet' with the value '192.168.28.1'. At the bottom of the form is a large blue 'Apply' button.

DNS Rebinding Attack Protection: Turning on this option may cause private DNS lookup failure. If your network has a captive portal please disable this option.

Override DNS Settings for All Clients: If enabled, your router will override unencrypted DNS settings for all clients.

DNS Server Settings

There are four modes.

- Automatic, use the gateway of the parent router.

DNS Server Settings

Mode

Automatic

DNS from Ethernet

192.168.28.1

Apply

- Encrypted DNS

DNS Server Settings

Mode

Encrypted DNS

Encryption Type

DNS over TLS

DNS Provider

NextDNS

NextDNS ID

Optional

Apply

Encrypted Type has four type, DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS, Oblivious DNS over HTTPS.

- For DNS over TLS, the DNS Provider has two options, NextDNS and Cloudflare.
- For DNSCrypt-Proxy, DNS over HTTPS and Oblivious DNS over HTTPS, they can select DNS Server.

DNS Server Settings	
Mode	Encrypted DNS
Encryption Type	DNSEncrypt-Proxy
Server i	Select at least one server + Select Server
<div>Apply</div>	

- Manual DNS

DNS Server Settings	
Mode	Manual DNS
DNS Server 1	
DNS Server 2	Optional
DNS Server 3	Optional
DNS Server 4	Optional
<div>Apply</div>	

- DNS Proxy

DNS Server Settings

Mode

DNS Proxy

Proxy Server Address

192.168.8.1#53

Apply

Edit Hosts

Requests from clients will be resolved preferentially using the static DNS rules you write in Hosts.

Edit Hosts

Requests from clients will be resolved preferentially using the static DNS rules you write in Hosts.

1127.0.0.1 localhost

2

3::1 localhost ip6-localhost ip6-loopback

4ff02::1 ip6-allnodes

5ff02::2 ip6-allrouters

6

Cancel

Apply

9.5 Network Mode

On the left side of web Admin Panel -> MORE SETTINGS -> Network Mode

When you change the router's network mode, you may need to re-connect all your client devices.

When you use Access Point/Extender/WDS mode, you may not connect to the web Admin Panel again. Try to access the web Admin Panel by the IP address that parent router assigned to this router. Or you can Press and hold the reset button for 4 seconds to revert to Router mode.

Note: some models do not support WDS mode.

Network Mode

When you change the router's network mode, you may need to re-connect all your client devices.

i When you use Access Point/Extender/WDS mode, you may not connect to this [Learn More](#) UI again. You can Press and hold the reset button for 4 seconds to revert to router mode.

☒ 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.

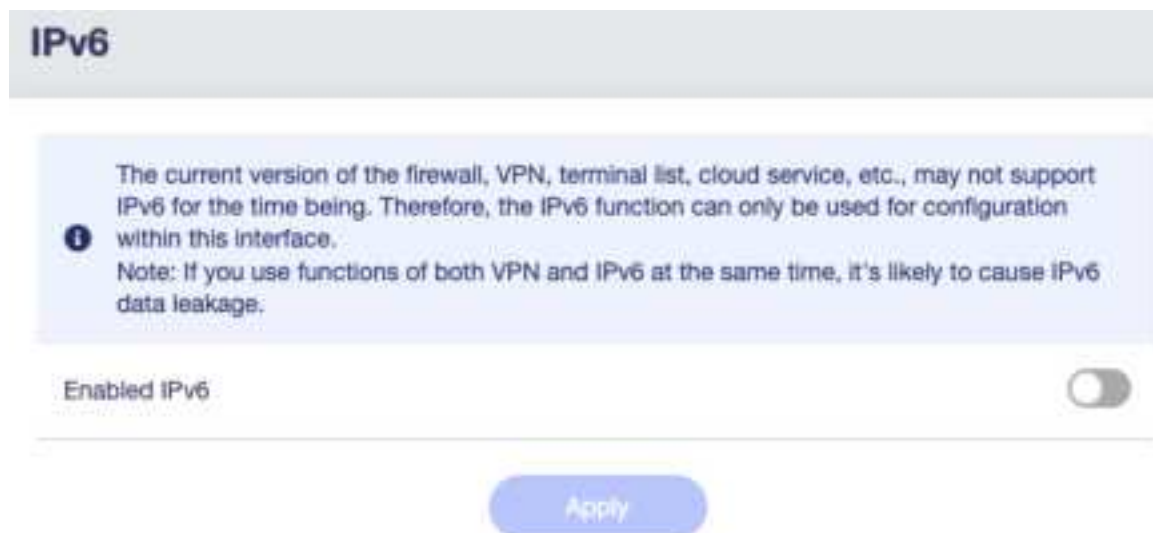
Apply

- Router. Create your own private network. The router will act as NAT, firewall and DHCP server. This is the default mode.
- 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.

9.6 IPv6

On the left side of web Admin Panel -> MORE SETTINGS -> IPv6

The IPv6 function allows you to enable and configure IPv6 on router.



The current version of the firewall, VPN, terminal list, cloud service, etc., may not support IPv6 for the time being. Therefore, the IPv6 function can only be used for configuration within this interface.

Note: If you use functions of both VPN and IPv6 at the same time, it's likely to cause IPv6 data leakage.

After enabled.

IPv6



The current version of the firewall, VPN, terminal list, cloud service, etc., may not support IPv6 for the time being. Therefore, the IPv6 function can only be used for configuration within this interface.

Note: If you use functions of both VPN and IPv6 at the same time, it's likely to cause IPv6 data leakage.

Enabled IPv6



LAN

Mode

Native

DNS acquisition method

Automatic

Apply

- **Mode.** There are three modes, **NAT6**, **Native** and **Static IPv6**.
- **DNS acquisition method.** It has two options. **Automatic** and **Manual**.


9.7 Toggle Button Settings

Some models have a toggle button, and you can customize what this button does in this page.


On the left side of web Admin Panel -> MORE SETTINGS -> Toggle Button Settings

Toggle Button Settings

LEFT



RIGHT



⇌

Toggle Button Function

No Function

Apply

There are four options.

- No Function.
- AdGuard Home (On/Off)
- OpenVPN Client (On/Off)
- WireGuard Client (On/Off)

9.8 Reset Firmware

On the left side of web Admin Panel -> MORE SETTINGS -> Reset Firmware

In case of malfunction, you can reset router.

Note: All your current settings, applications and data will be lost. The process will take about 3 minutes. DO NOT power off the router during this process.

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 3 minutes. DO NOT power off the router during this process.

Delete All And Reboot

If you can't access the web Admin Panel, you can use the reset button as well, please check out [here](#).

9.9 Advanced Settings

On the left side of web Admin Panel -> MORE SETTINGS -> 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.

Click the link **192.168.8.1/cgi-bin/luci** to access LuCI 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