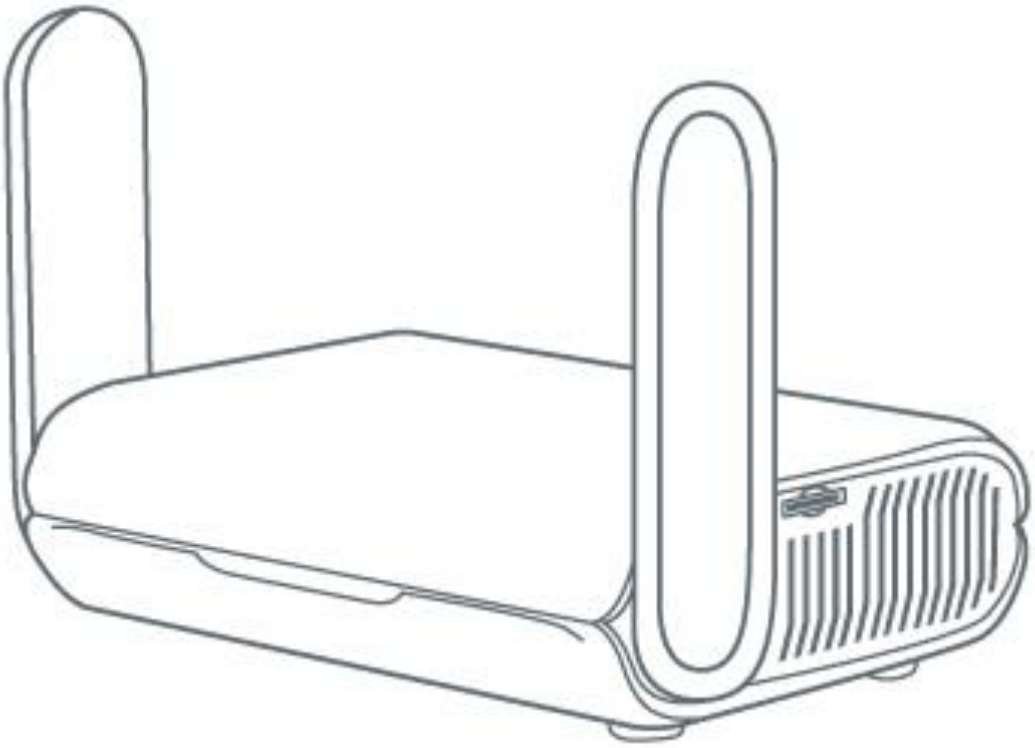
GL·iNet



Slate AX

(GL-AXT1800)

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 20
   2.4 Connect to the Internet via cellular 23
3. Wireless 28
   Main WiFi 28
   Guest WiFi 30
4. CLIENTS 31
   Blocking client 31
   Limiting speed 31
   Remove offline clients 32
5. Firmware Upgrade 33
   Online Upgrade 33
   Local Upgrade 33
6. FIREWALL 36
   Port Forwards 36
   Open Ports on Router 38
   DMZ 39
7. VPN 41
   7.1 VPN Dashboard 41

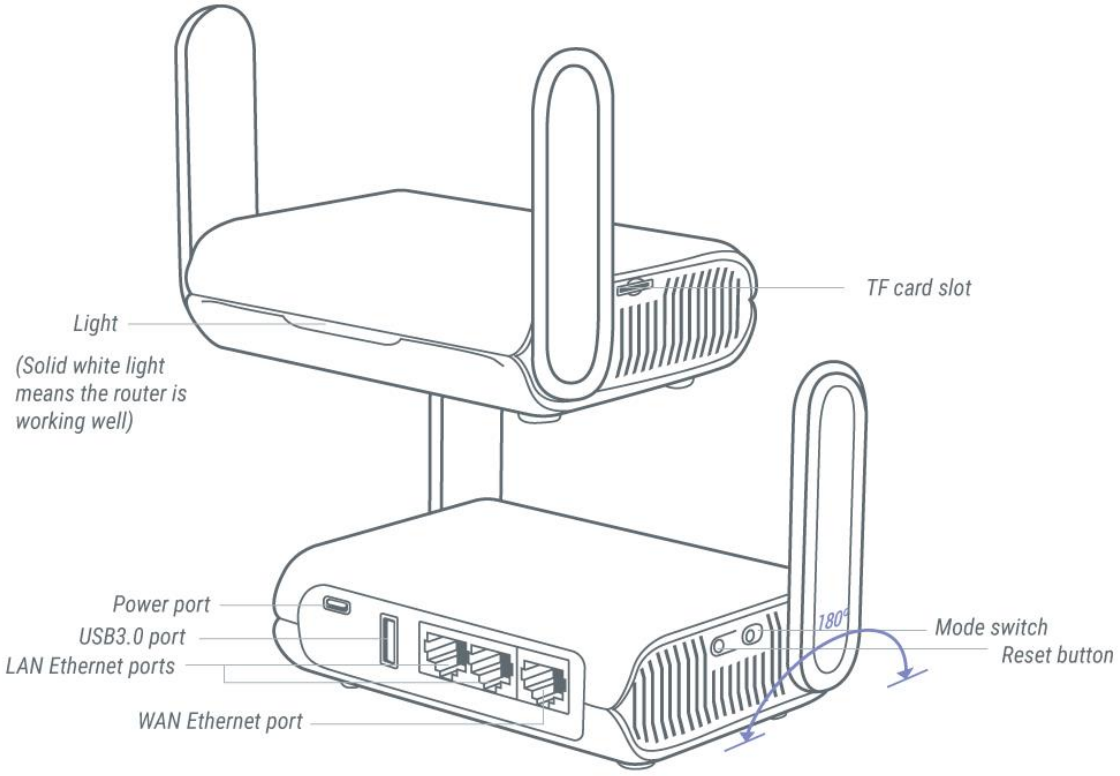
VPN Client 41
Proxy mode 42
Global Options 43
VPN Server 44
OpenVPN Server Options 44
OpenVPN Server Route Rule 45
WireGuard Server Options 45
WireGuard Server Route Rule 46
OpenVPN 47
7.2 How to Setup OpenVPN Client on GL.iNet router 47
Setup NordVPN 47
Setup OpenVPN client 51
Setup OpenVPN server on GL.iNet router 54
Get configuration files from OpenVPN service providers¶ 54
7.3 Setup OpenVPN Server on GL.iNet router 55
Make sure Internet Service Provider assigns you a public IP address 55
Network Topology 55
Setup OpenVPN Server 55
To check if OpenVPN Server is working properly 59
Advanced Configuration 61
OpenVPN Client App 62
WireGuard 62
7.4 How to Setup WireGaurd Client on GL.iNet router 62
Setup AzireVPN 62
Setup Mullvad 65
Setup WireGuard client 68
Setup WireGuard server on GL.iNet router 75
Get configuration files from WireGuard service providers 75
7.5 Setup WireGuard Server on GL.iNet router 76
Make sure Internet Service Provider assigns you a public IP address¶ 76
Network Topology 76
Setup WireGuard Server 76
WireGuard Client App 82

8. APPLICATIONS 83
8.1 Plug-ins 83
8.2 Dynamic DNS 84
Enable DDNS 84
Check if DDNS is in effect 85
HTTP Remote Access 86
HTTPS Remote Access 87
SSH Remote Access 92
8.3 GL.iNet GoodCloud 93
Contents 93
Introduction 94
Setup 95
Manage your devices 102
Site to Site 110
Batch Setting 119
Template Management 122
Task List 126
GoodCloud and VPN 127
Turn off cloud 128
8.4 AdGuard Home 130
8.5 Network Storage 132
Contents 132
Introduction 132
Insert storage device 132
Set up Samba 133
Set up WebDAV 137
Set up DLNA 141
Samba Client 142
WebDAV Client 147
8.6 Log 149
9. MORE SETTINGS 150
9.1 Admin Password 150
9.2 LAN 151

Private Network 151
Reserve an IP for a client 153
Guest Network 153
9.3 Time Zone 156
9.4 DNS 157
DNS Server Settings 157
Edit Hosts 160
9.5 Network Mode 161
9.6 IPv6 163
9.7 Toggle Button Settings 165
9.8 Reset Firmware 166
9.9 Advanced Settings 167

1. Hardware info

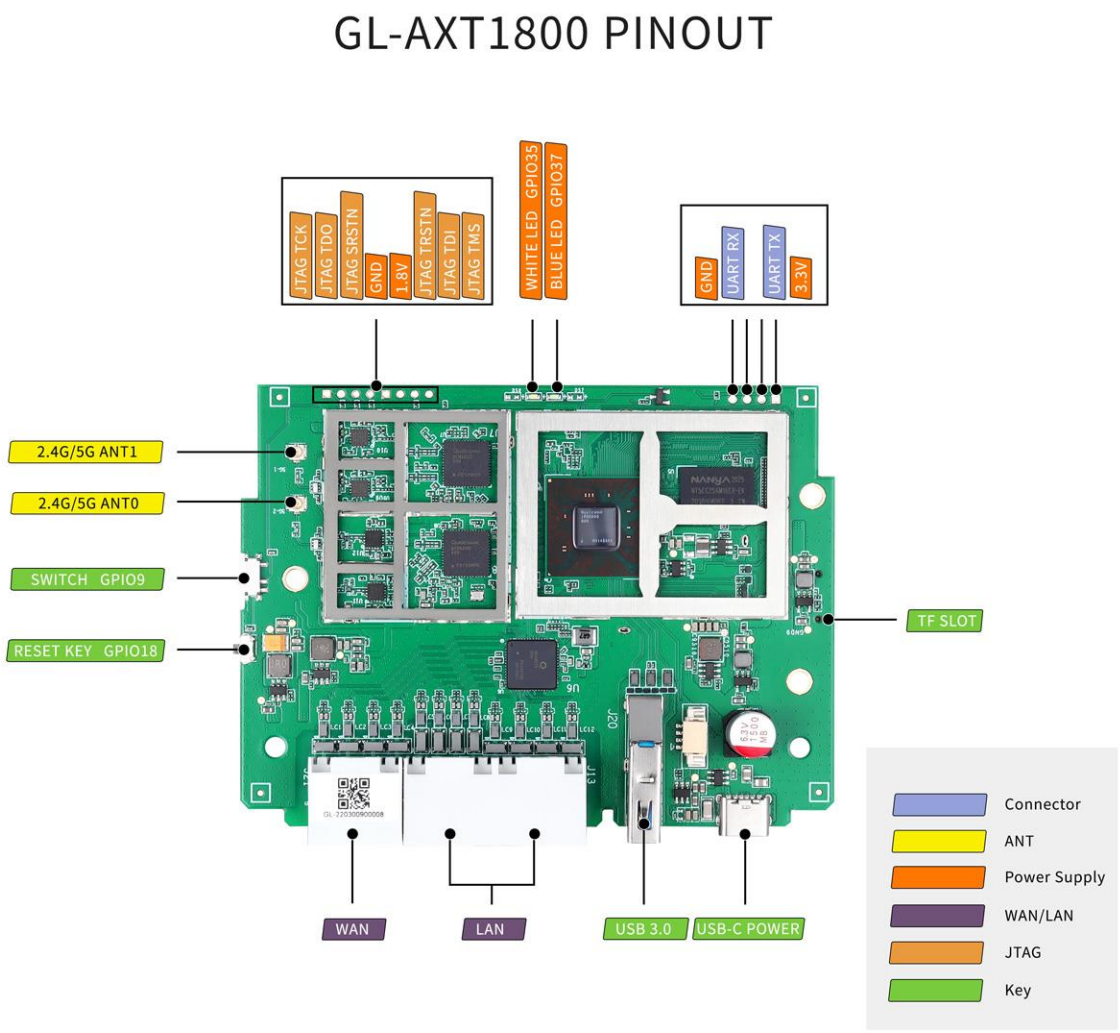
GL-AXT1800 (Slate AX) is the first Wi-Fi 6 travel router designed by GL.iNet. It comes with an IPQ6000 1.2GHz quad-core processor and runs on OpenWrt 21.02. With the latest Wi-Fi 6 technology, you can enjoy more capacity for connected devices and faster wireless speed on the road or at home.



1.1. Specification

Interface	1 x WAN Ethernet port 2 x LAN Ethernet ports 1 x USB 3.0 port 1 x Type-C power port 1 x MicroSD card slot (Max.512GB) 1 x Reset button 1 x Switch button
CPU	IPQ6000 1.2GHz Quad-core Processor
Memory / Storage	DDR3L 512MB / NAND Flash 128MB
Protocol	IEEE 802.11a/b/g/n/ac/ax
Wi-Fi Speed	600Mbps (2.4GHz), 1200Mbps (5GHz)
Ethernet Speed	10/100/1000Mbps
Antennas	2 x undetachable external Wi-Fi antennas
Power Input	Type-C, 5V/4A
Operating Temperature	0 ~ 40°C (32 ~ 104°F)
Storage Temperature	-20 ~ 70°C (-4 ~ 158°F)
Dimension / Weight	125 x 82 x 36mm / 245g

1.2. PCB Pinout



2. First time setup

The first setup of the GL.iNet router is very similar, here is the example of GL-AXT1800(Slate AX).

Please prepare the following items that included in the package.

GL-AXT1800, power adapter, ethernet cable.

There is a video guide:

https://youtu.be/f7DYULL6ZSI

Power on

If you want to use TF card, please insert before powering on the router. Hot plugging for TF card is not supported.

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-AXT1800-XXX or **GL-AXT1800-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**.

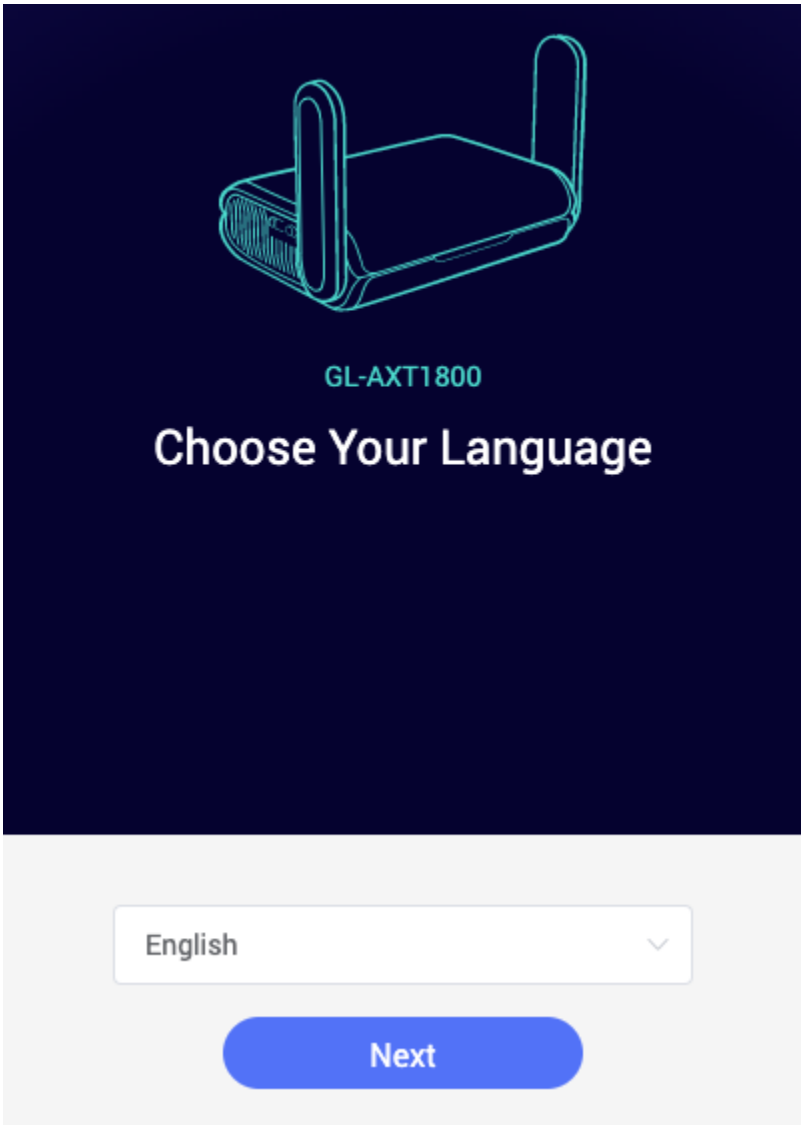
  Tip: The QR code on the label on the back of the GL-AXT1800 is with wifi connection information and can be quickly connected using your phone's QR code scanning tool.

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

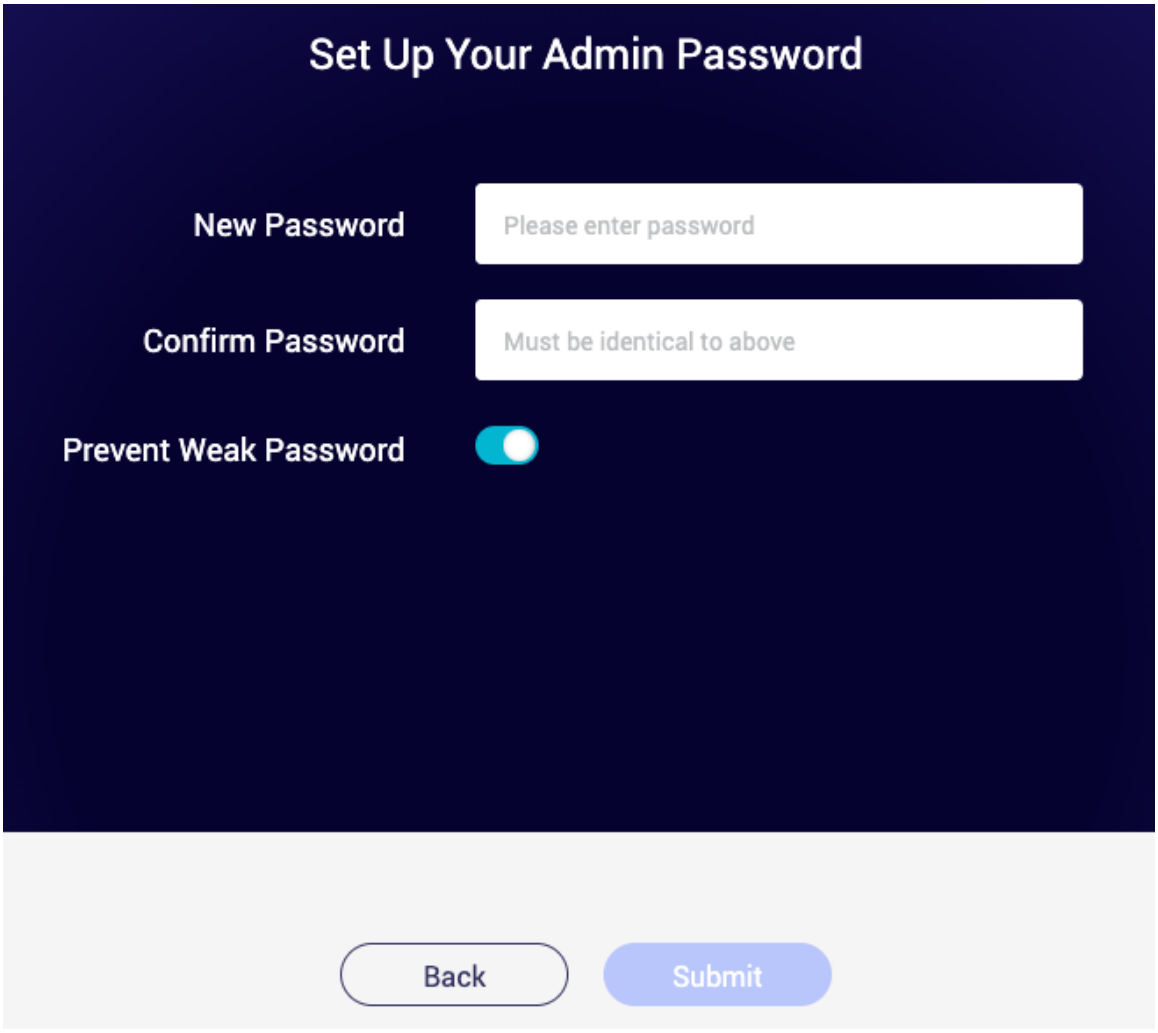
Open a web browser (we recommend Chrome, Edge, Safari) and visit http://192.168.8.1. You will be directed to the initial setup of the web Admin Panel.

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

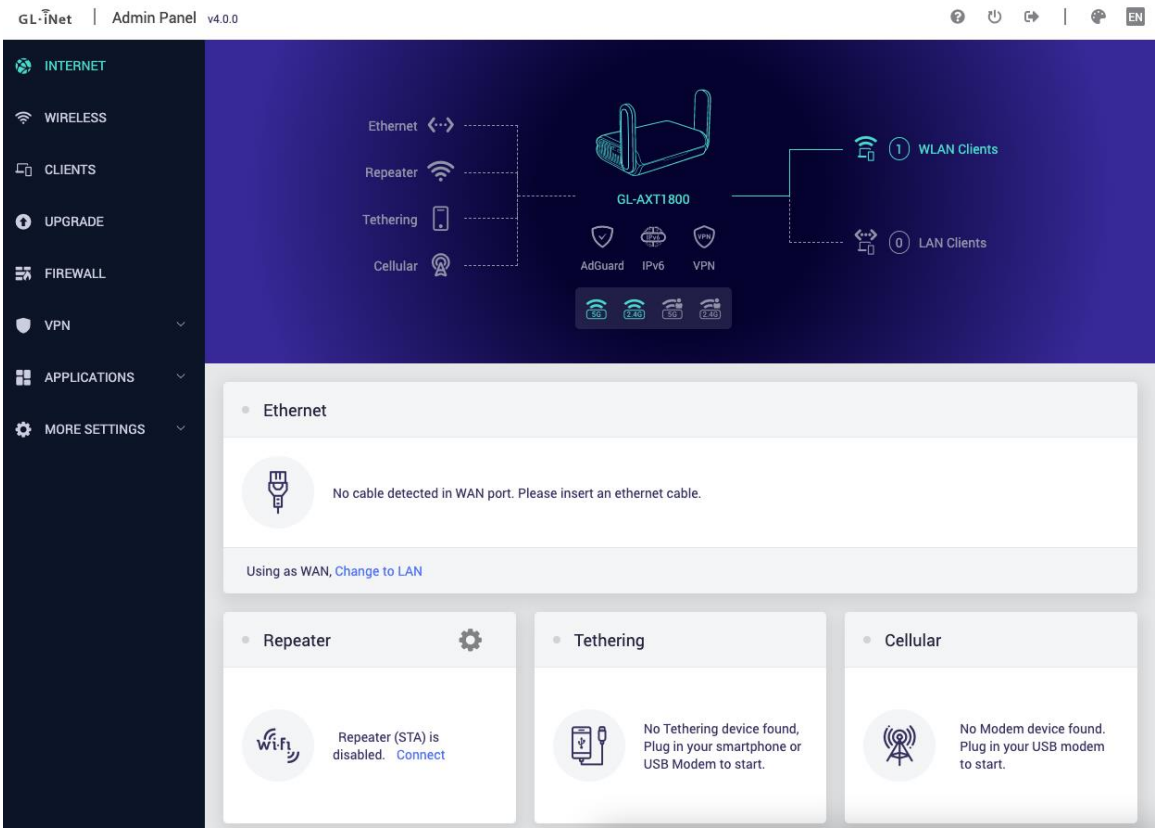


Set up admin password, we recommend using a strong password. Click **Submit** to continue.

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



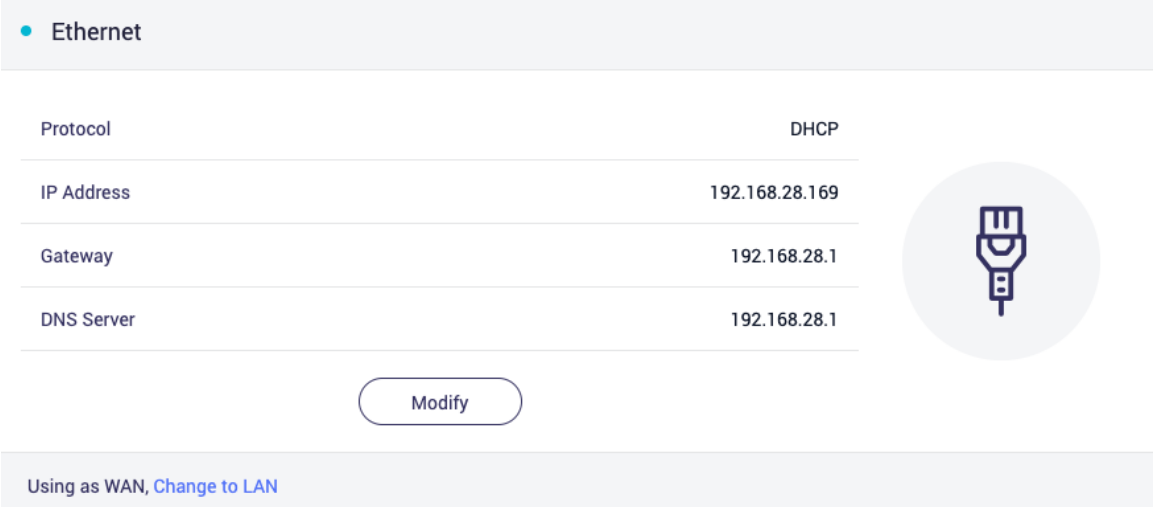
After the initial setup, you will enter the web Admin Panel of the router.



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.



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.

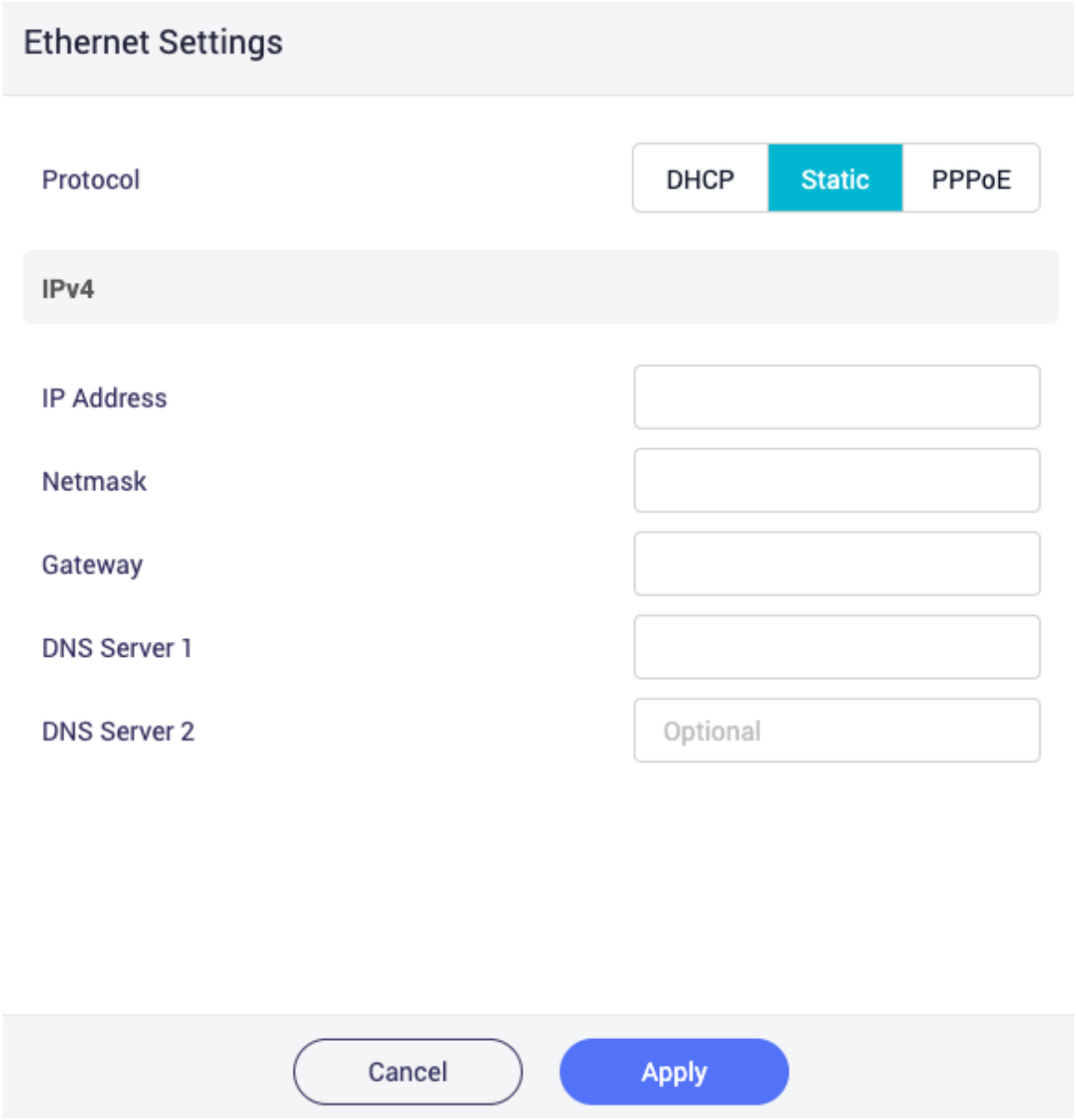
- DHCP

  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

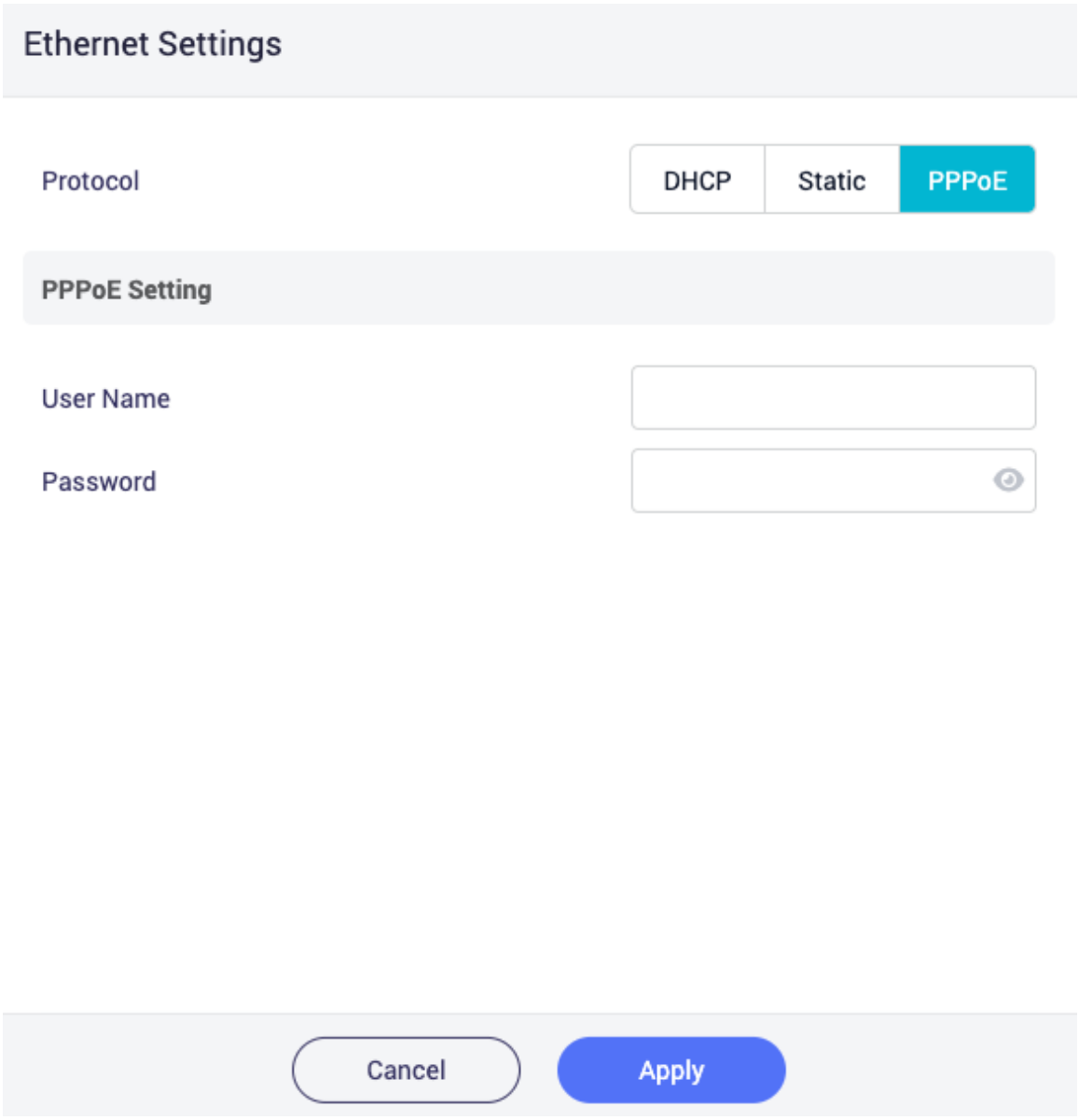
  Static is required if your Internet Service Provider (ISP) has provided a fixed IP address for you or you want to configure the

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



- 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

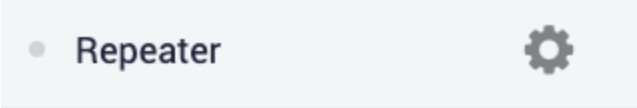
2.2 Connect to the Internet via an existing Wi-Fi by Repeater

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.

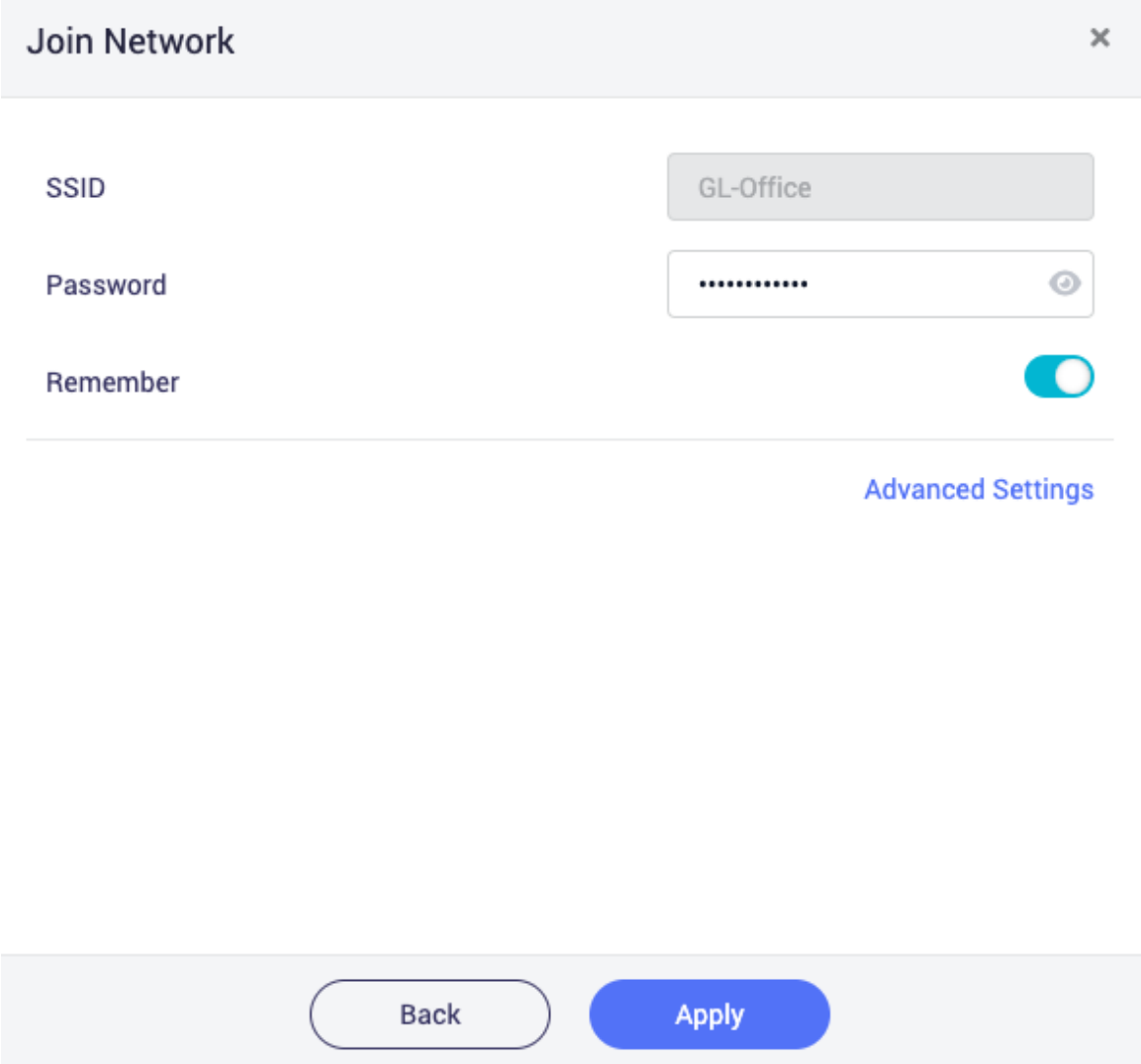
On the left side of web Admin Panel -> INTERNET, Repeater sector.

Basic steps



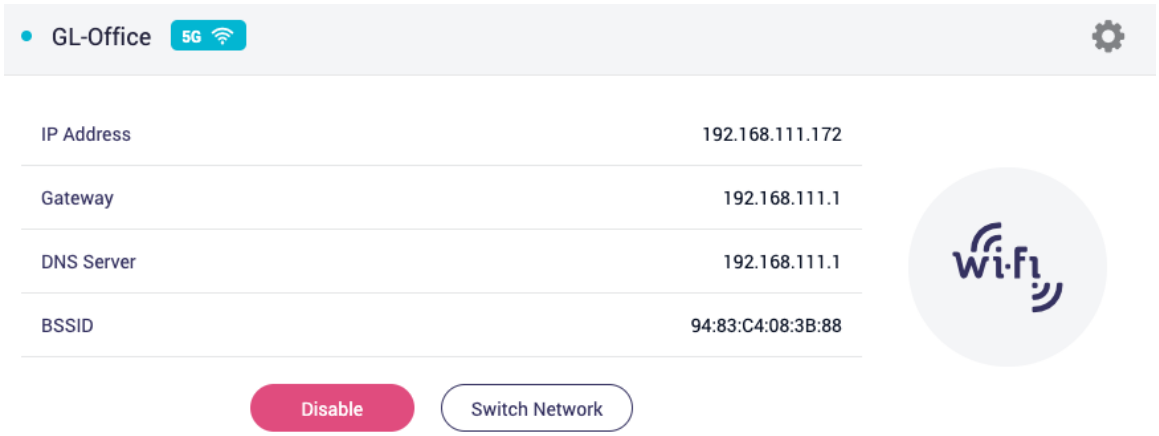
Click **Connect** in the image above.

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.



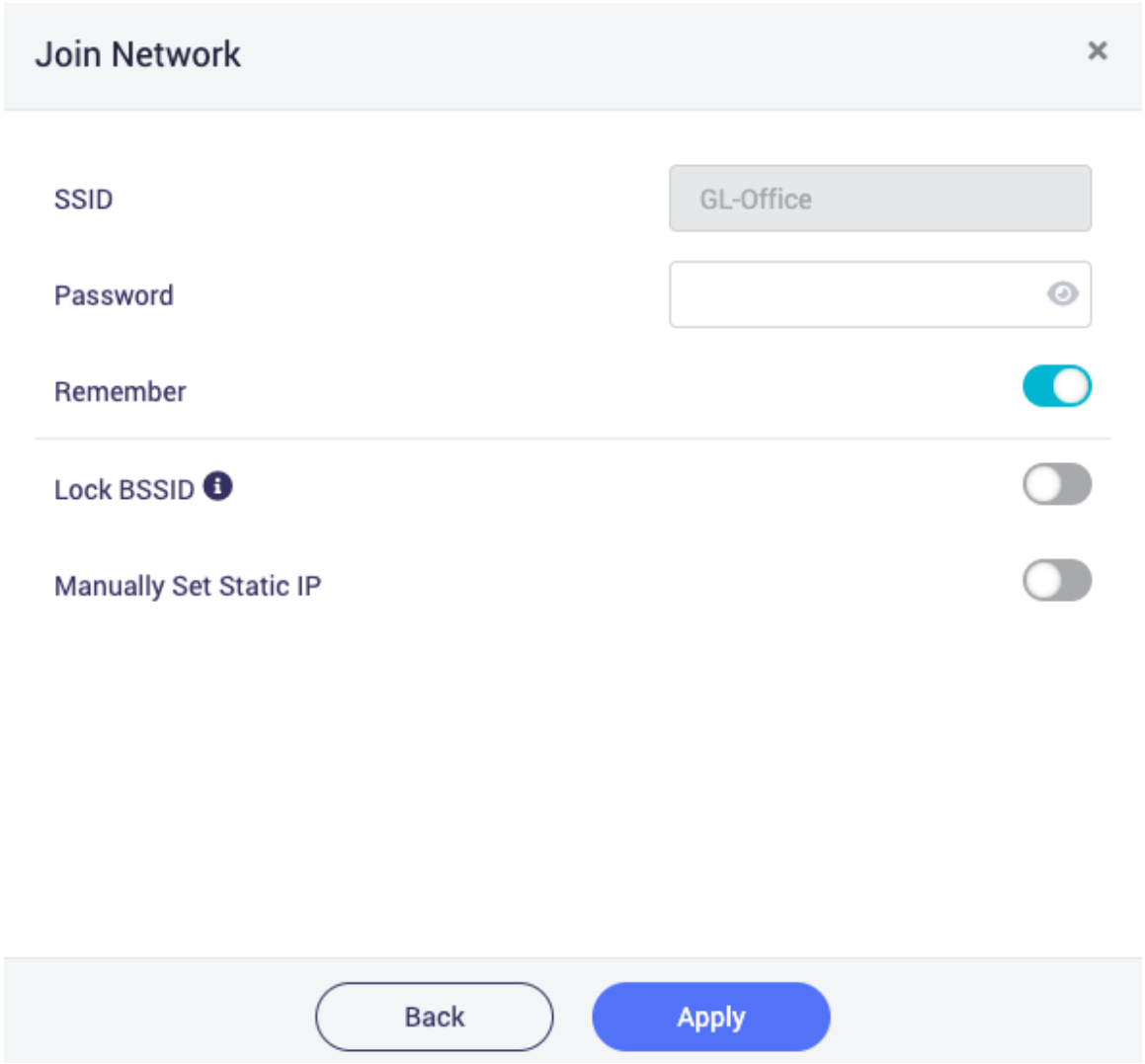
For Advanced Settings.

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



Join network advanced setting

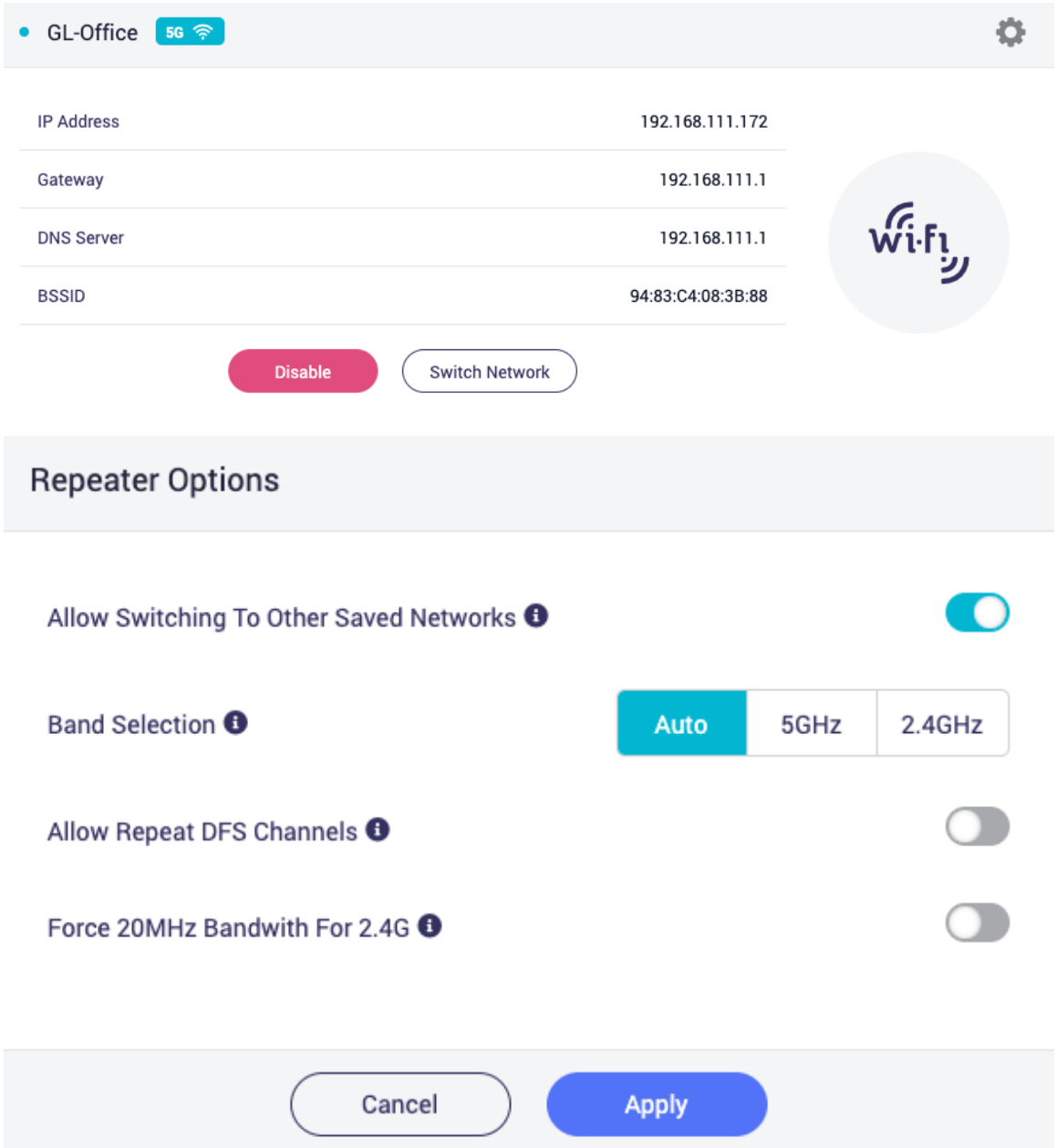
When joining the network, there are two additional options.



- **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

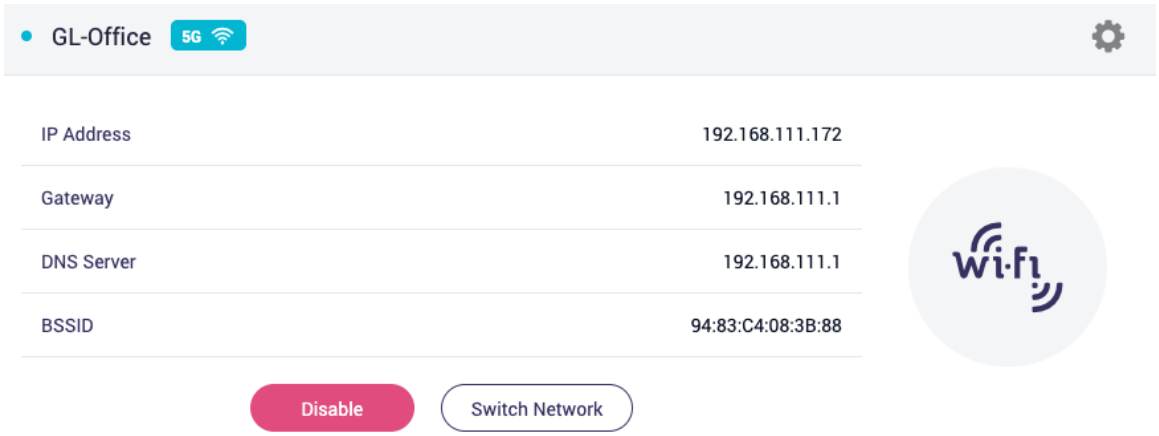
Click the cog icon for Repeater options.



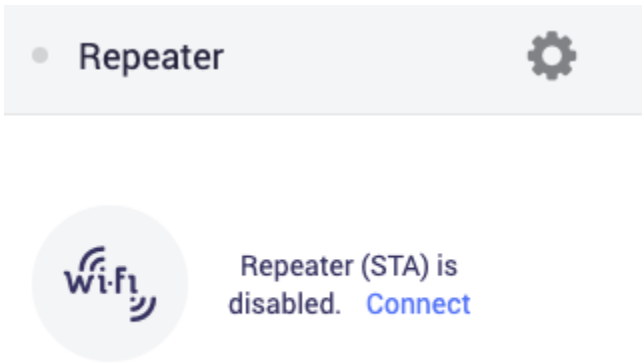
- **Allow Switching To Other Saved Network**. If the option is enabled, the router will automatically connect to other saved networks when it is unable to connect to the current Wi-Fi network.
- **Band Selection**. If you manually select a band, the router will not scan or connect to any Wi-Fi with another band.
- **Allow Repeat DFS Channels**. If the option is enabled, 5GHz Wi-Fi will be temporarily unavailable when a radar is using the channel which is currently router using; Otherwise, the router will not connect to any Wi-Fi using DFS channels.
- **Force 20MHz Bandwith 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**.

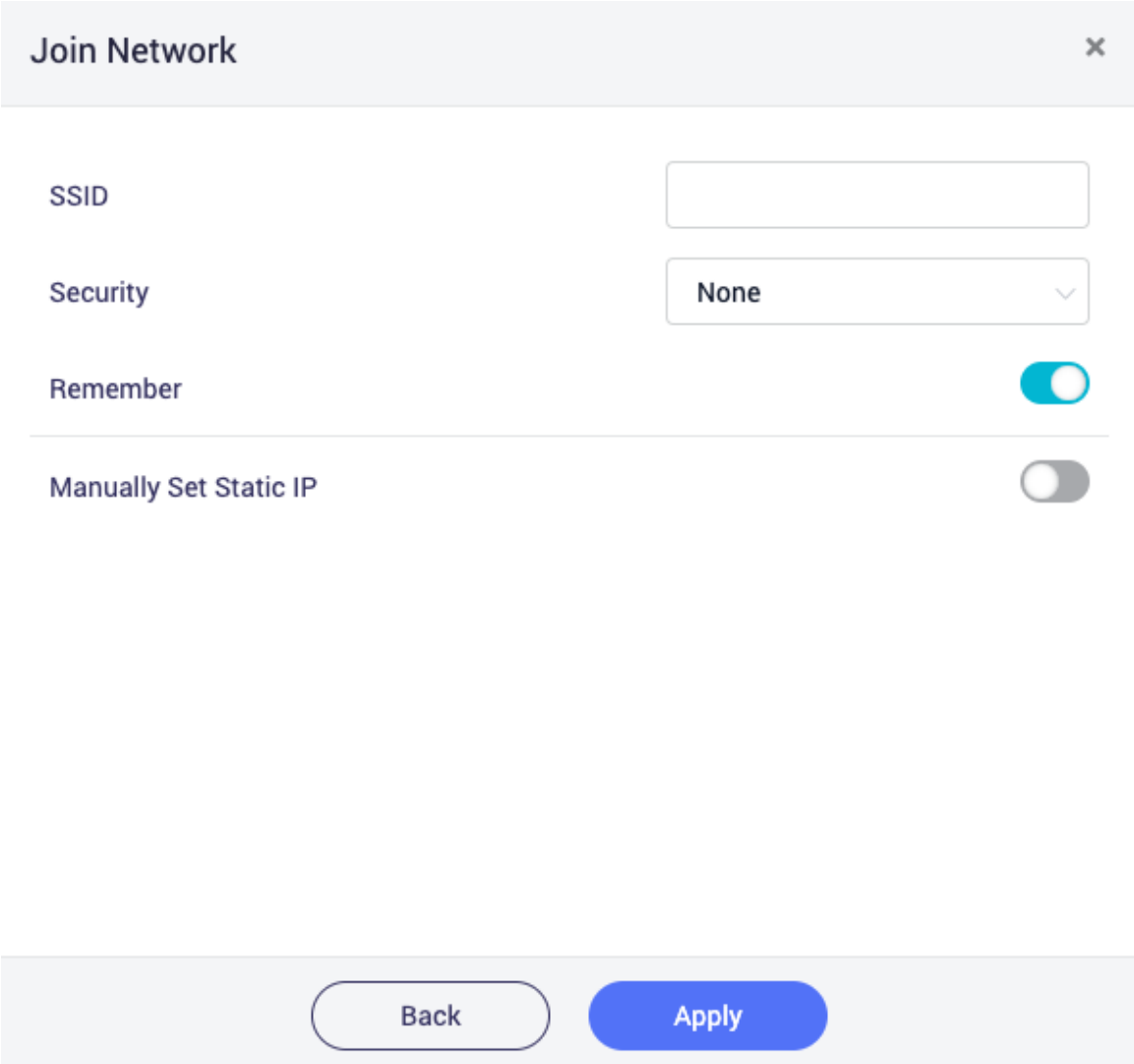


Or click **Connect**.



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

Join other network



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-AXT1800 and GL-AX1800, 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.

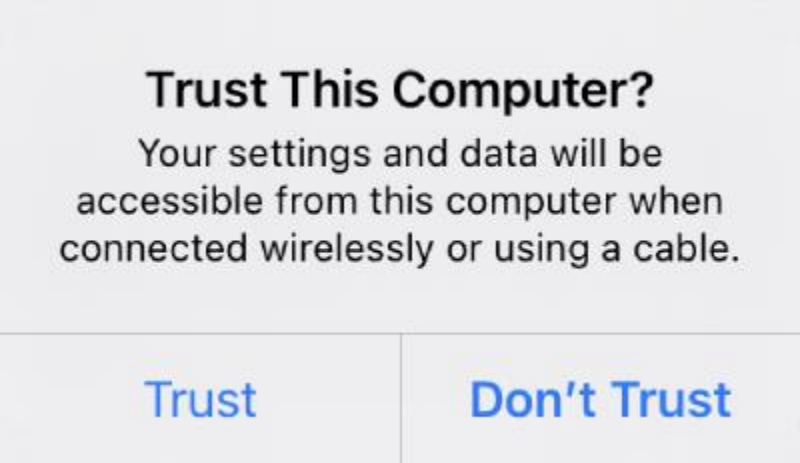
2.3 Connect to the Internet via usb tethering

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.

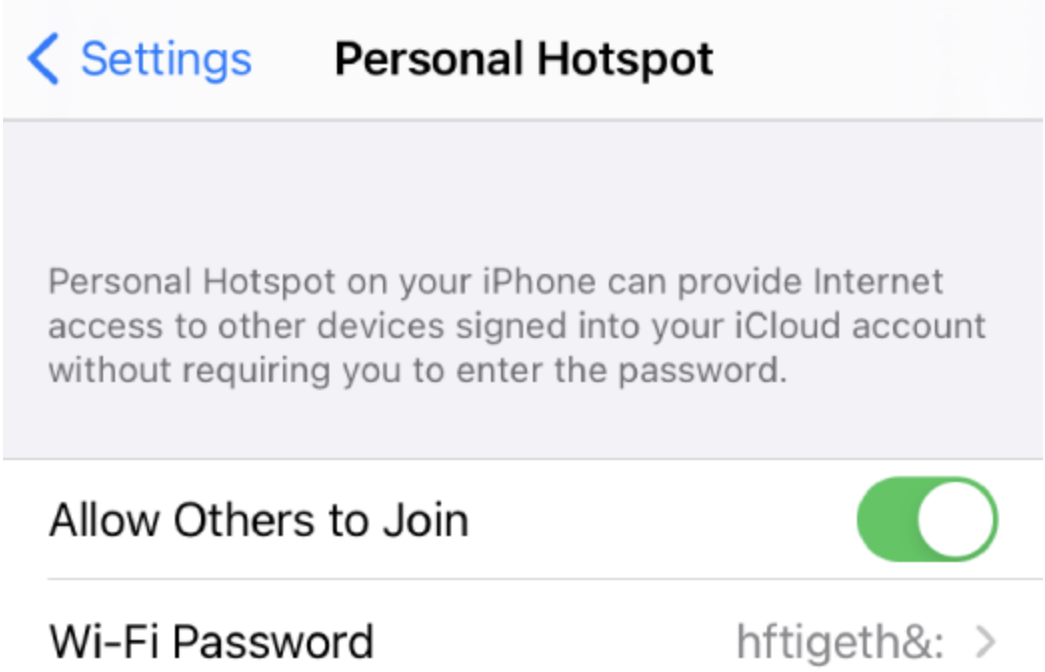
Note: Some mobile carriers limit or charge extra for tethering. We recommend checking with your carrier.

- iPhone

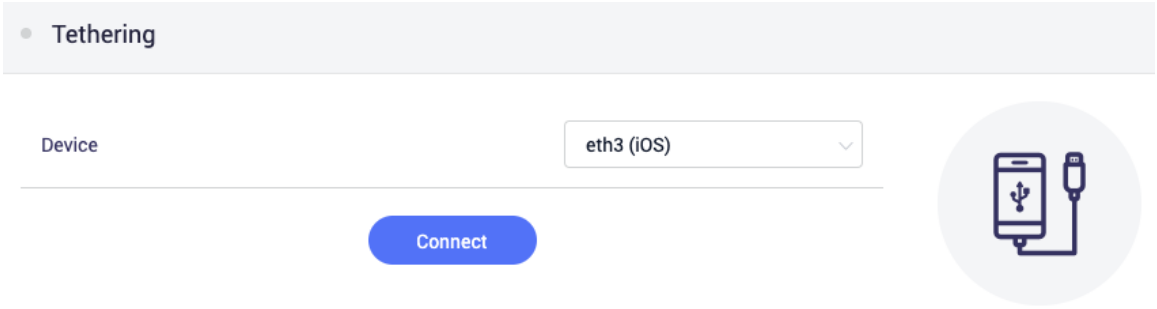
    1. Connect iPhone to the USB port of the router. It will pop up a message asking to trust this computer? Click "Trust" to contine. Because we are connecting the iPhone to the router, so here is to TRUST the router.

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

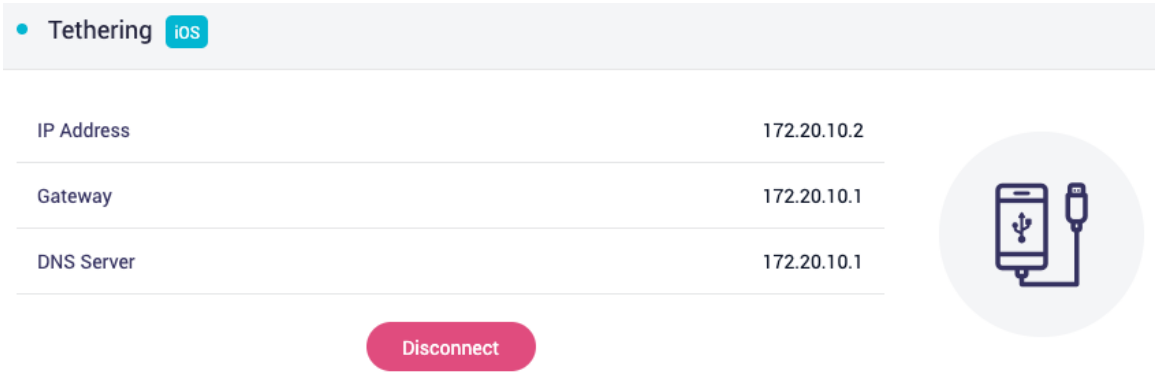


3. Go to web Admin Panel, on the left side bar, choose "INTERNET" and click "Connect" in the middle of the page.



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

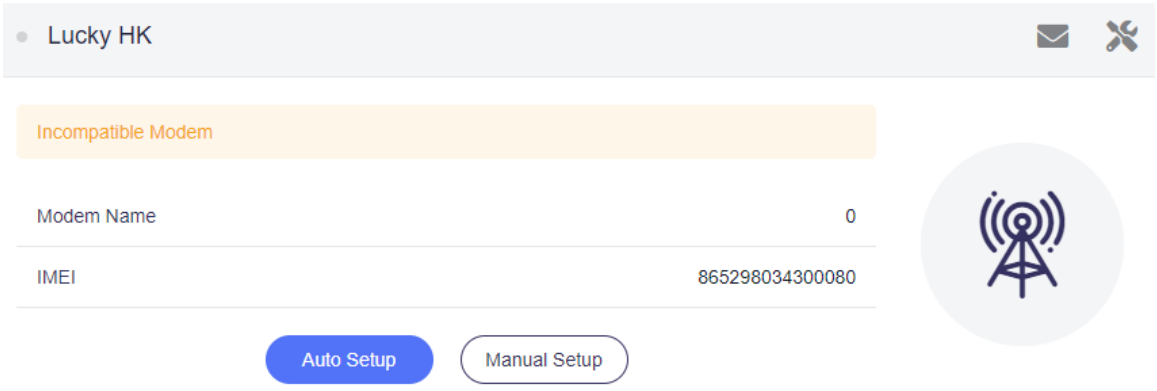
The router can be used to access the Internet through cellular. There are two cases, some models have a built-in 3G/4G model; some models have a usb port and can be plugged into a usb 3G/4G modem. The operation steps are similar, here is GL-AXT1800 as an example.

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.

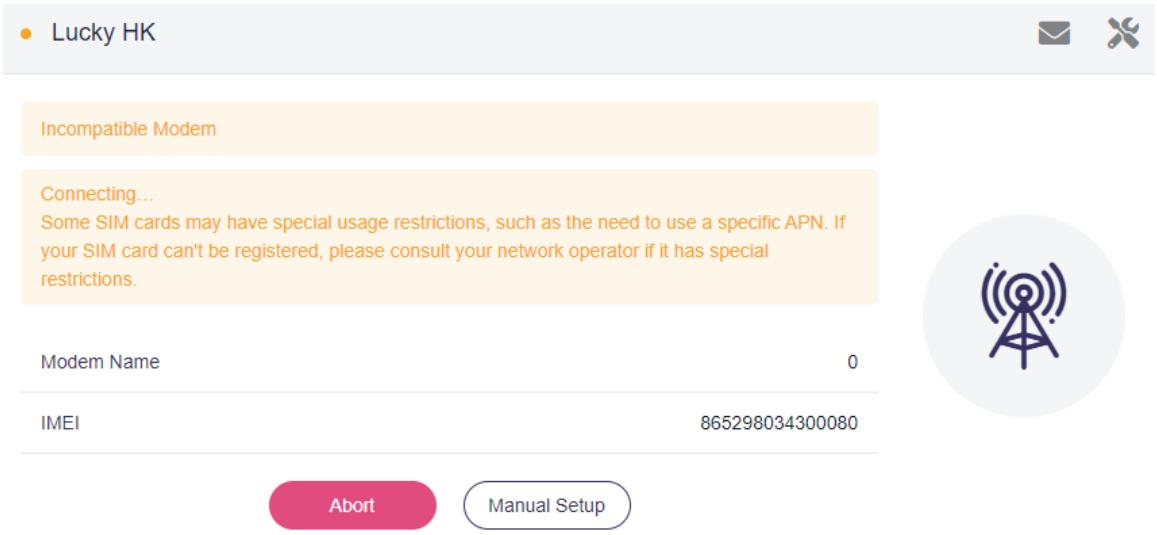
1. We recommend to turn off the router first, insert your SIM card into the USB modem then plug the USB modem into the USB port of the router, and then turn it on again. If you insert a usb modem at power on, the page may be no change, please refresh the page.
2. Please access the web Admin Panel -> 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*



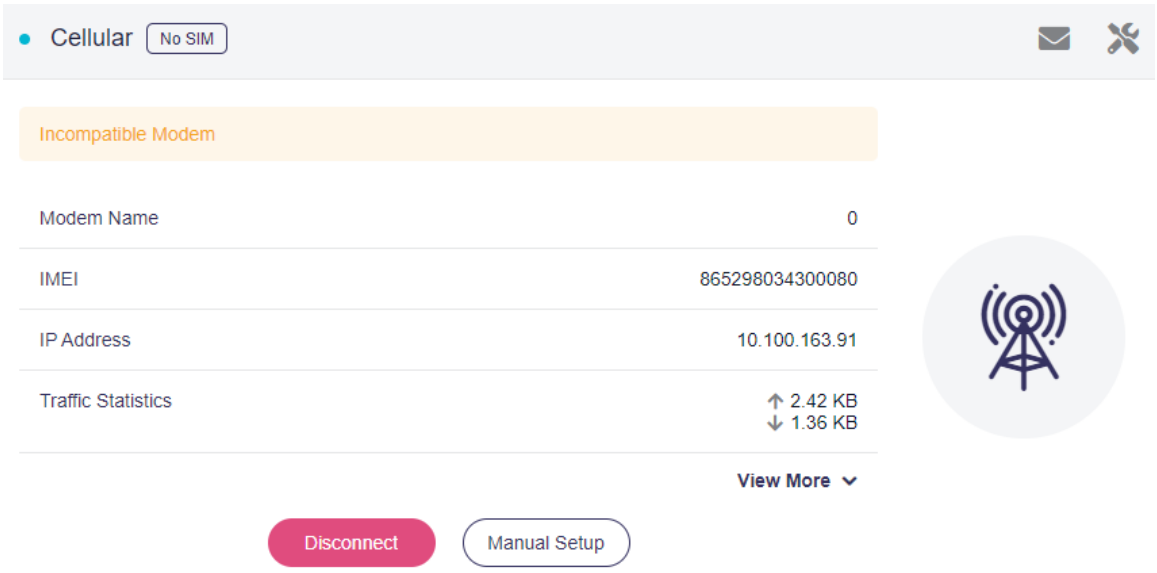
3. Connecting.

   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.



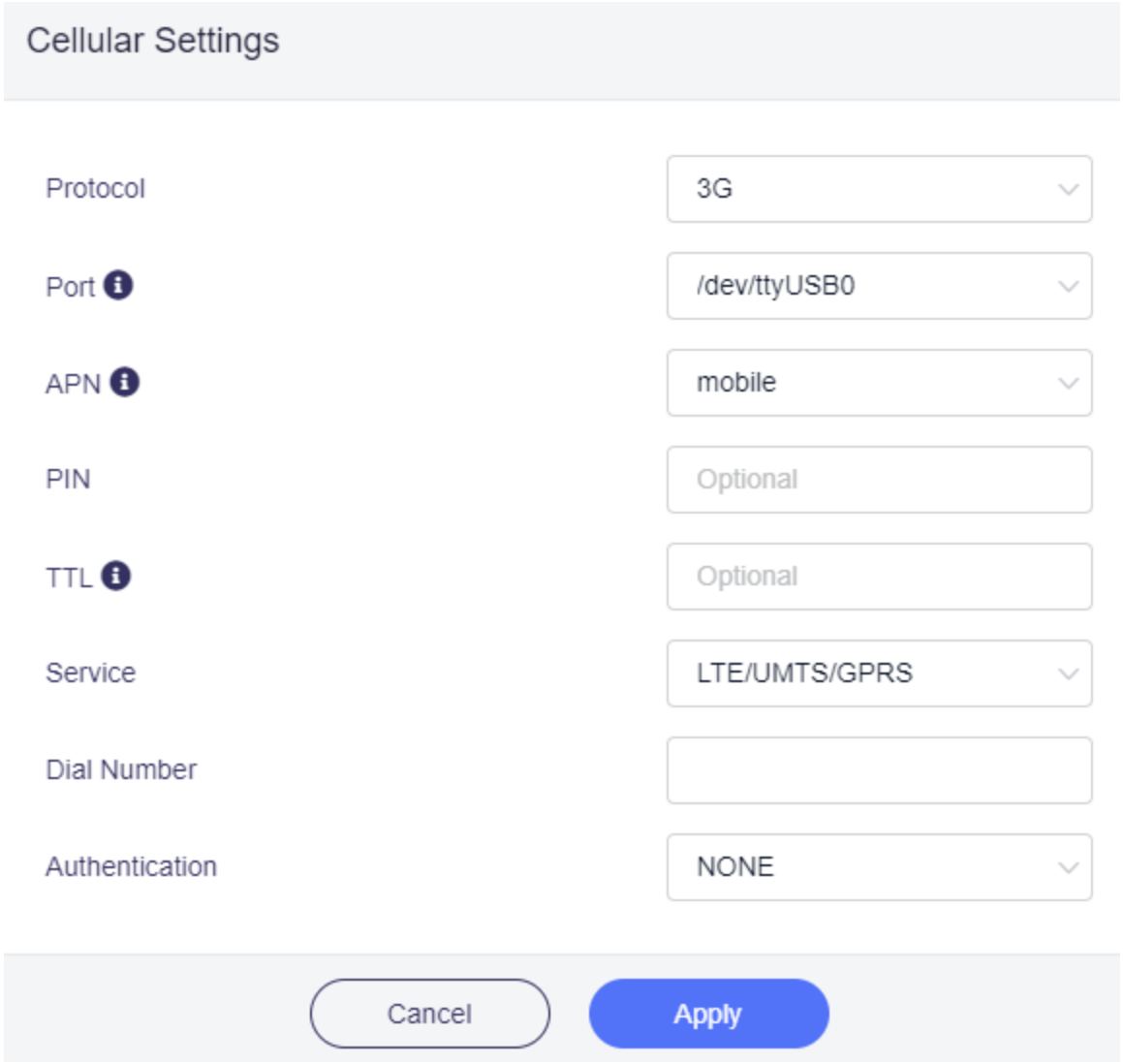
4. After a while, it will be connected. Otherwise, try Manual Setup.

   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**.



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.

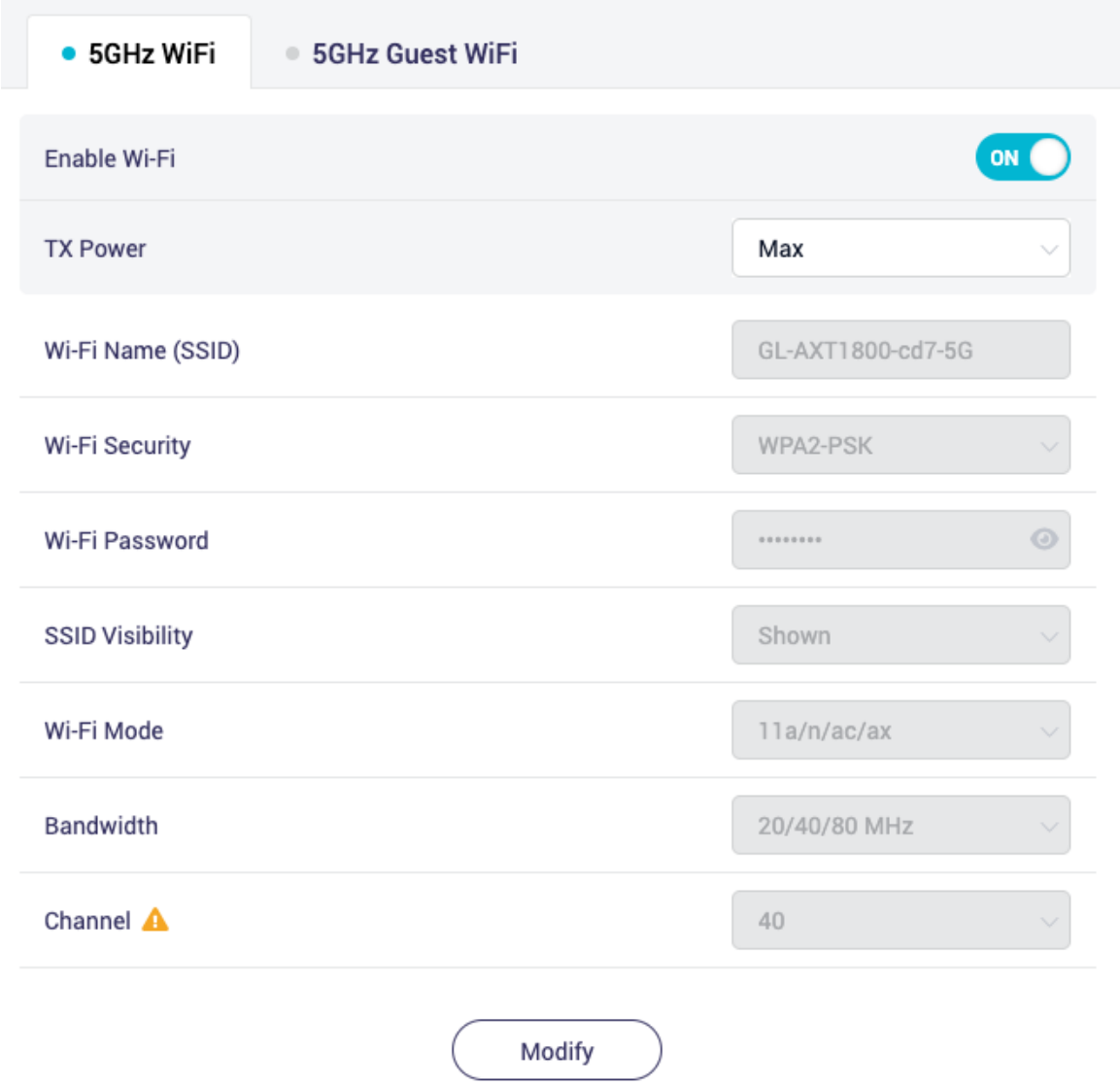
You can also search on the forum or create a post for asking.

3. Wireless

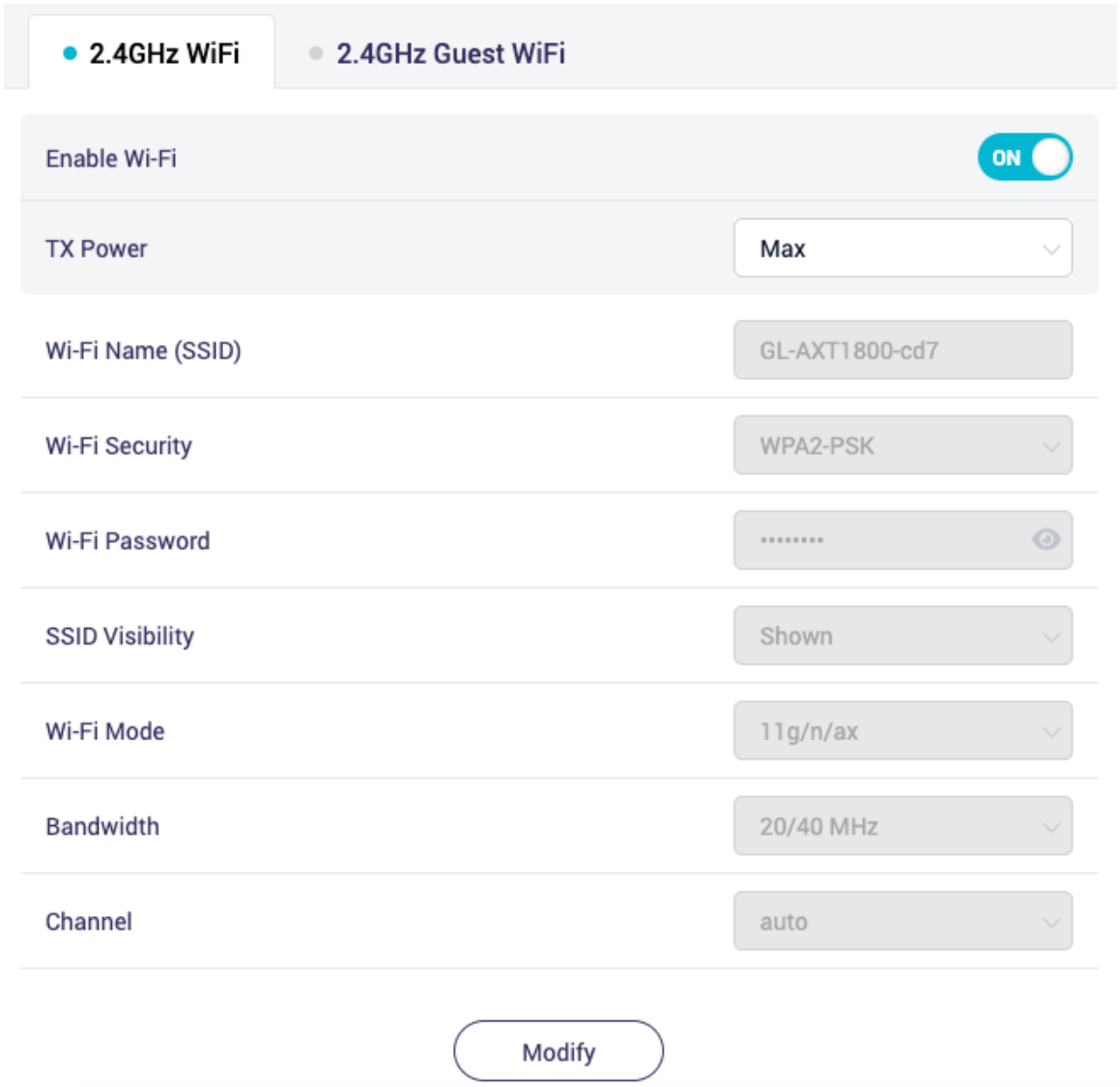
The wireless interface may vary a bit from model to model, here is an example of GL-AXT1800.

On the left side of web Admin Panel -> WIRELESS

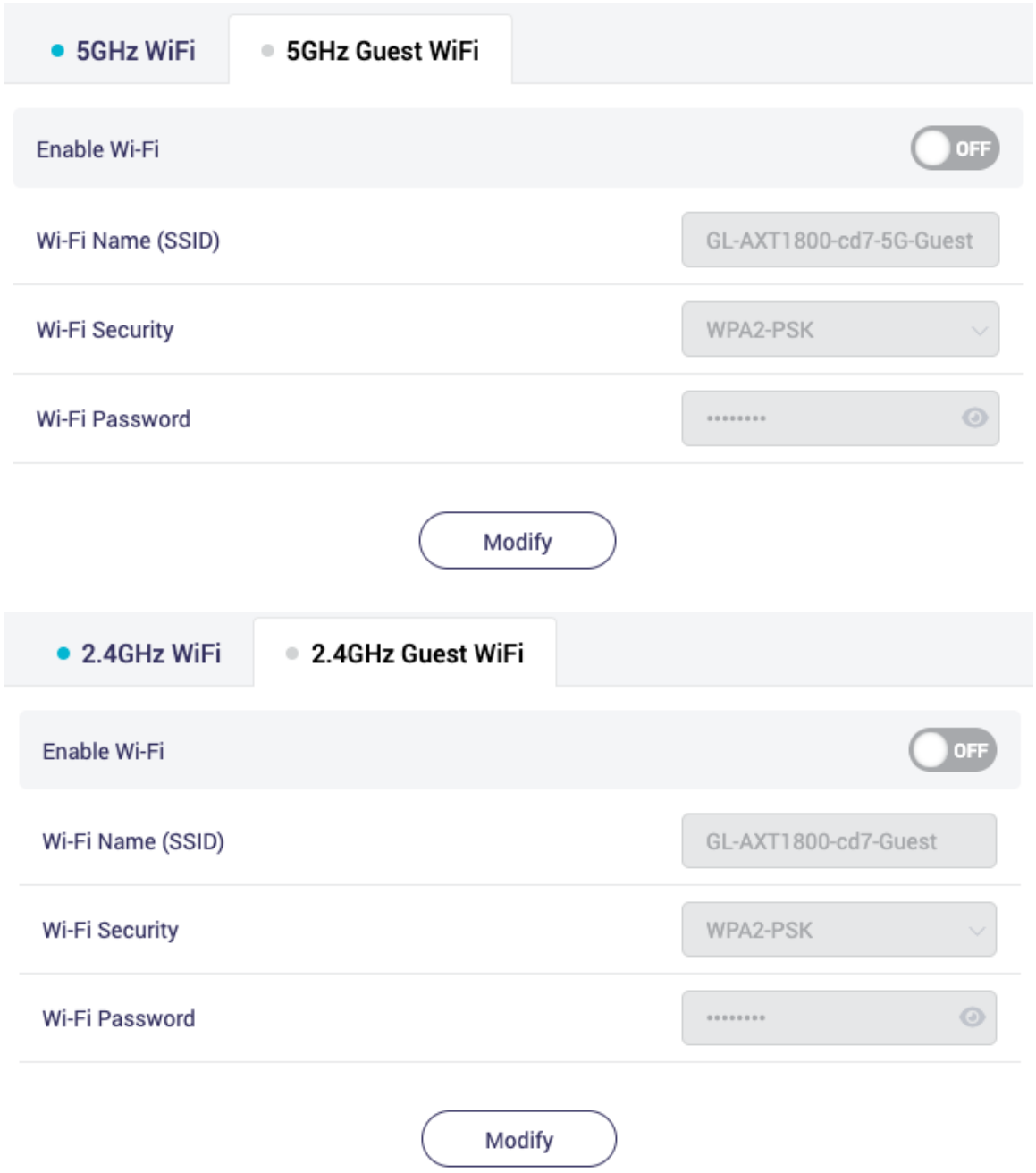
Main WiFi



Note: The **Channel** can't be modified when repeater is enabled.


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
ON
TX Power
Max
Wi-Fi Name (SSID)
GL-AXT1800-cd7
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

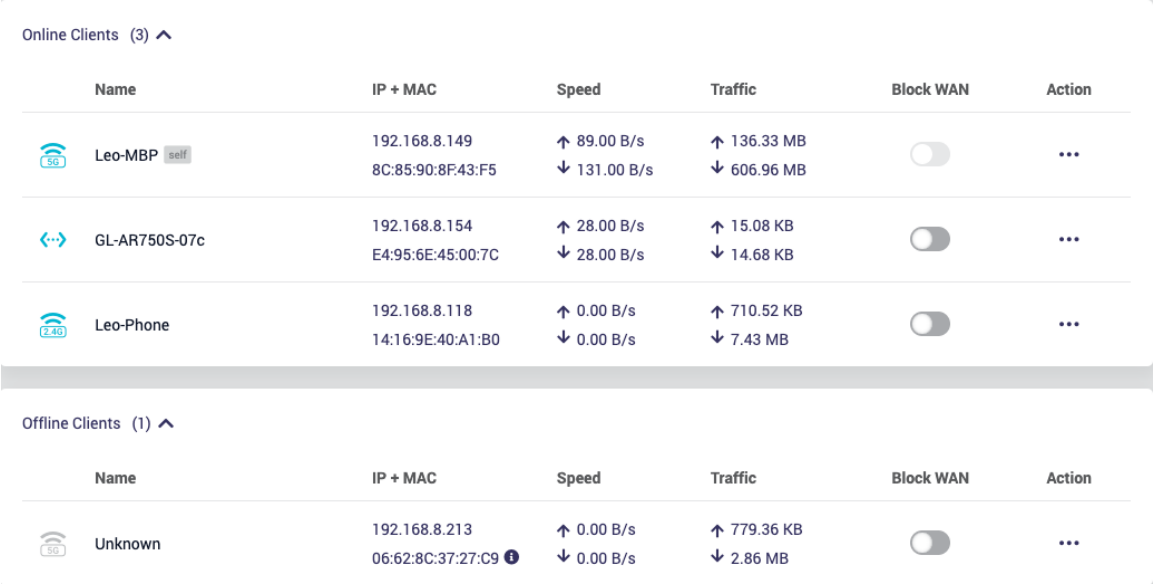
4. CLIENTS

On the left side of web Admin Panel -> CLIENTS

You can manage all connected devices in CLIENTS page.

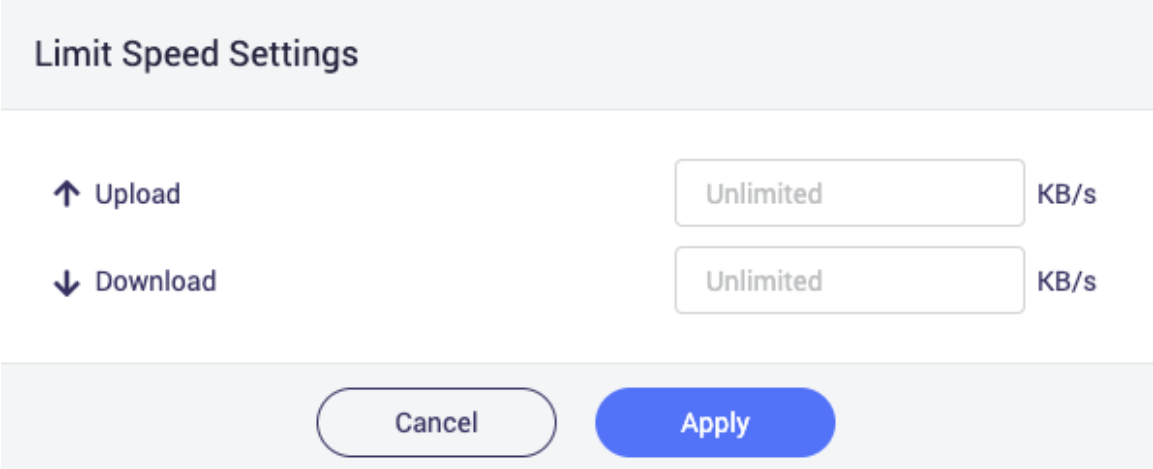
Blocking client

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

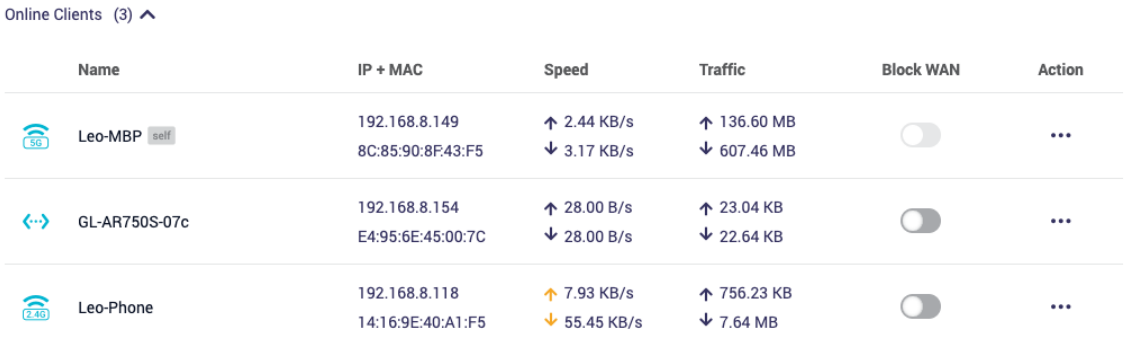


Limiting speed

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



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



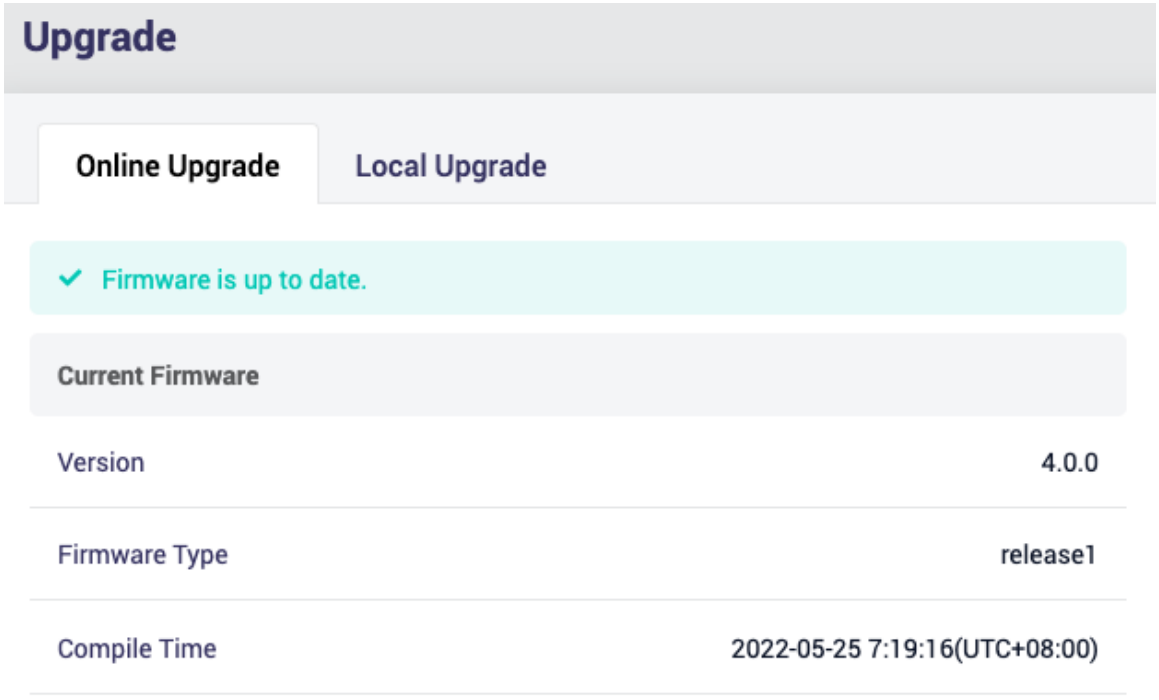
Click **Action** to disable limiting.

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

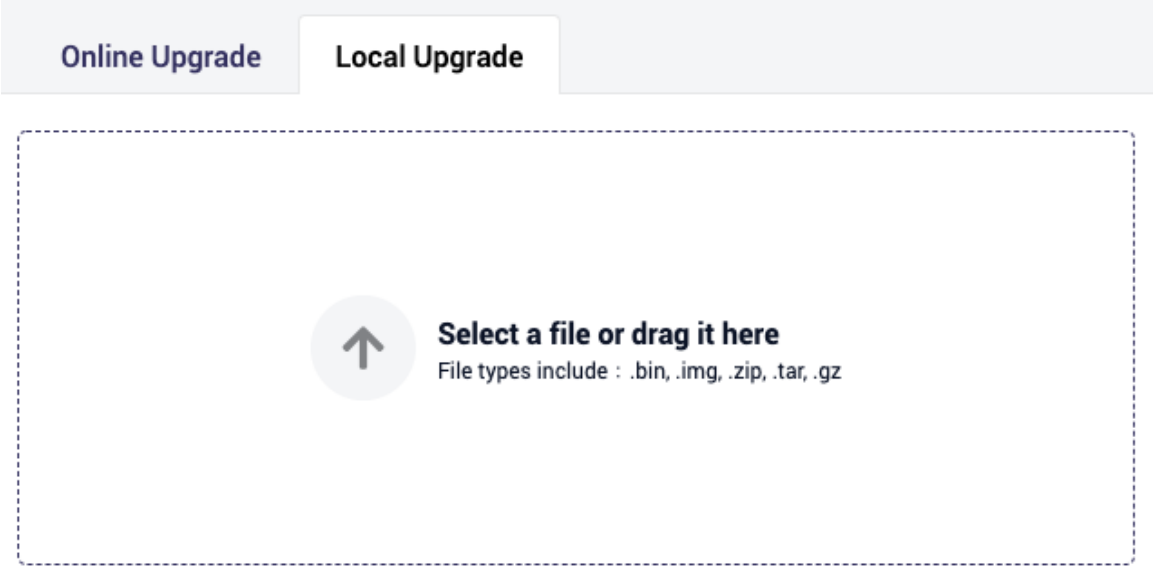


Online Upgrade

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.

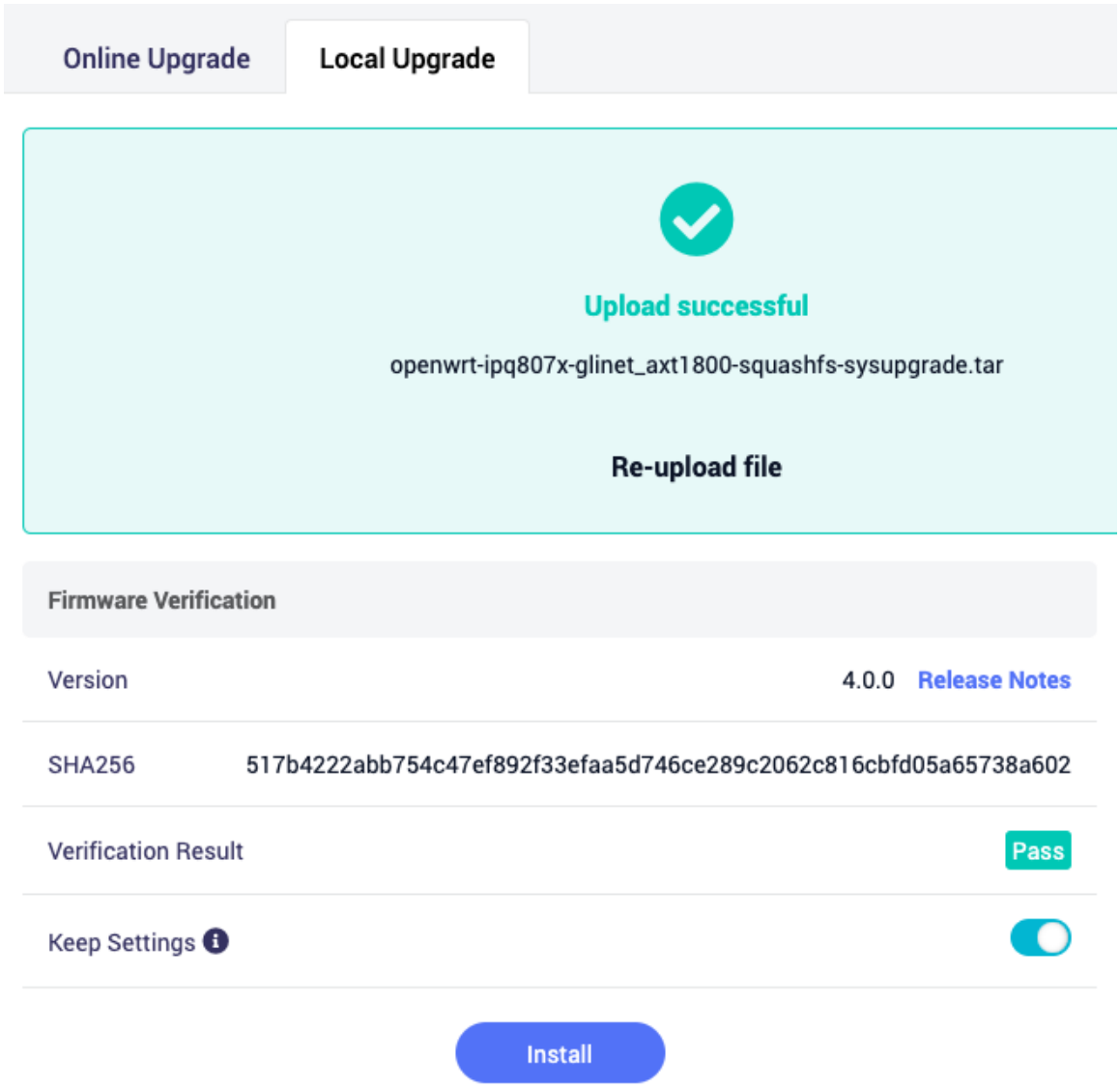


After uploaded, it will verify the firmware.

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
openwrt-ipq807x-glinet_axt1800-squashfs-sysupgrade.tar
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

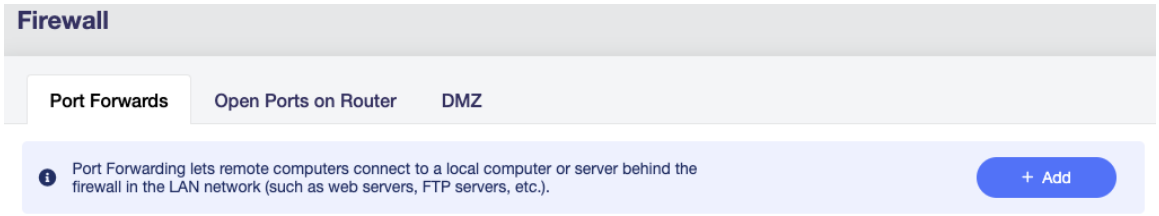
On the left side of web Admin Panel -> FIREWALL

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

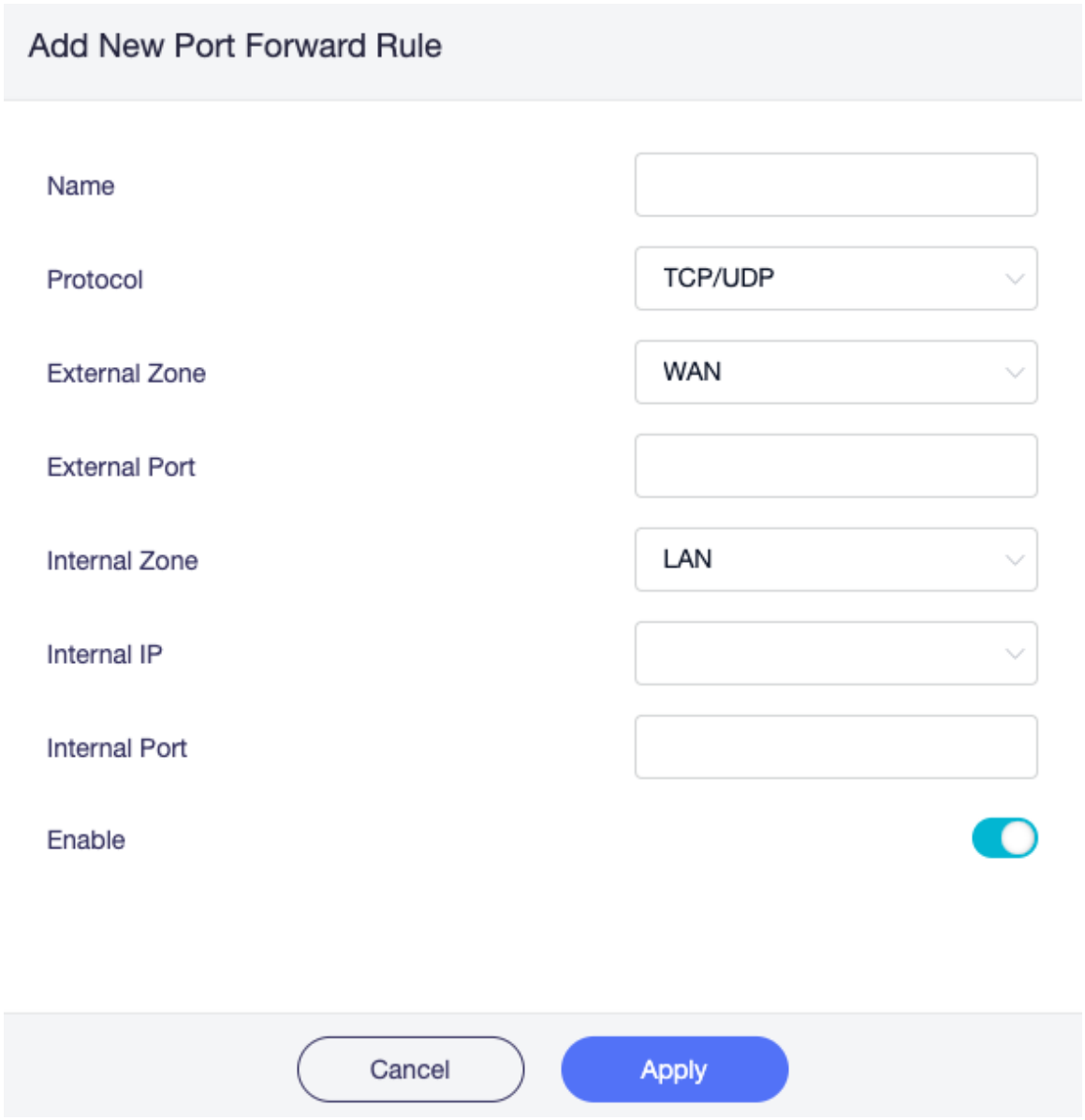
Port Forwards

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.



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.

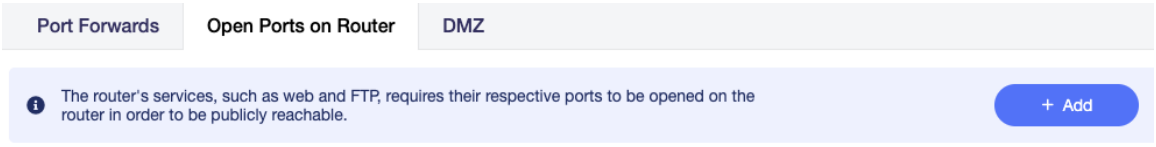
Internal Port: The internal port number of the device. You can enter a specific port number. Leave it blank if it is same as the external port.

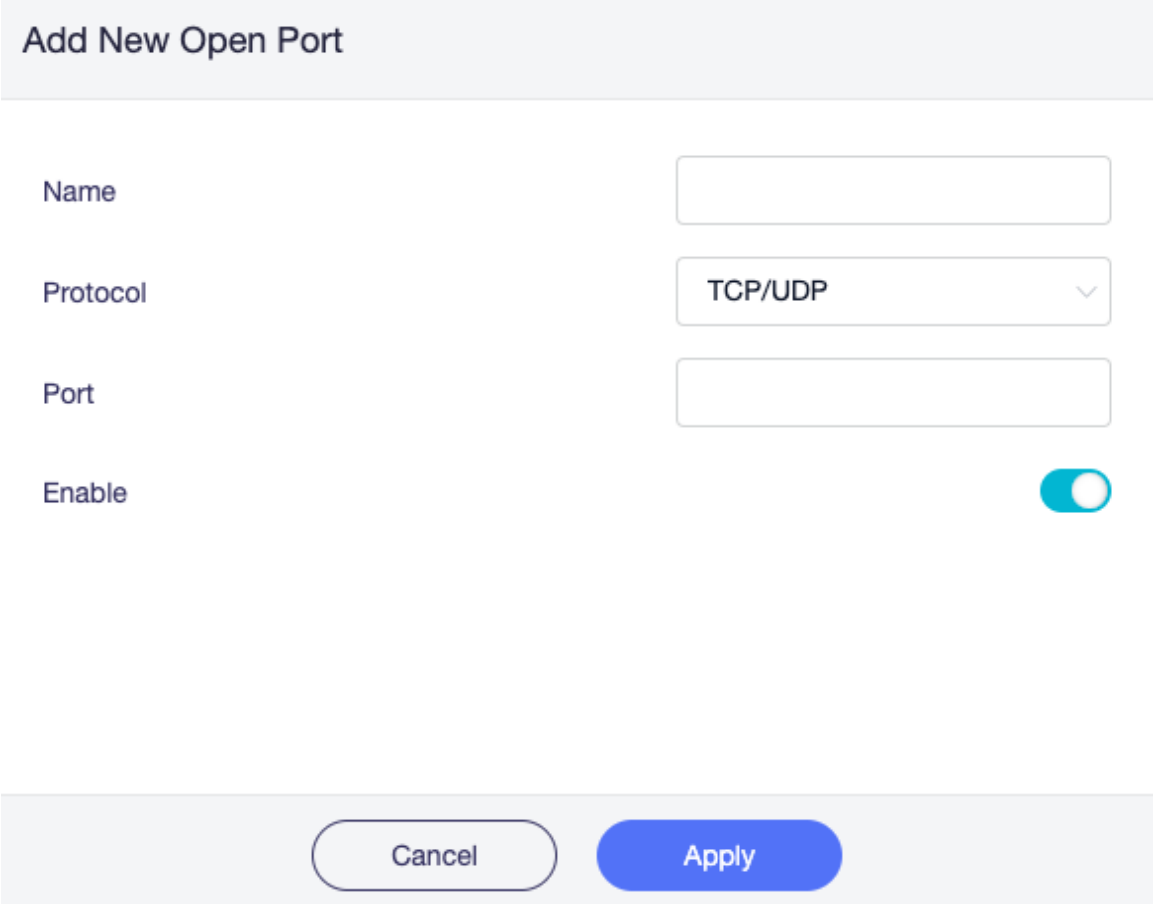
Enable: Enable of disable of the rule.

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**.





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.

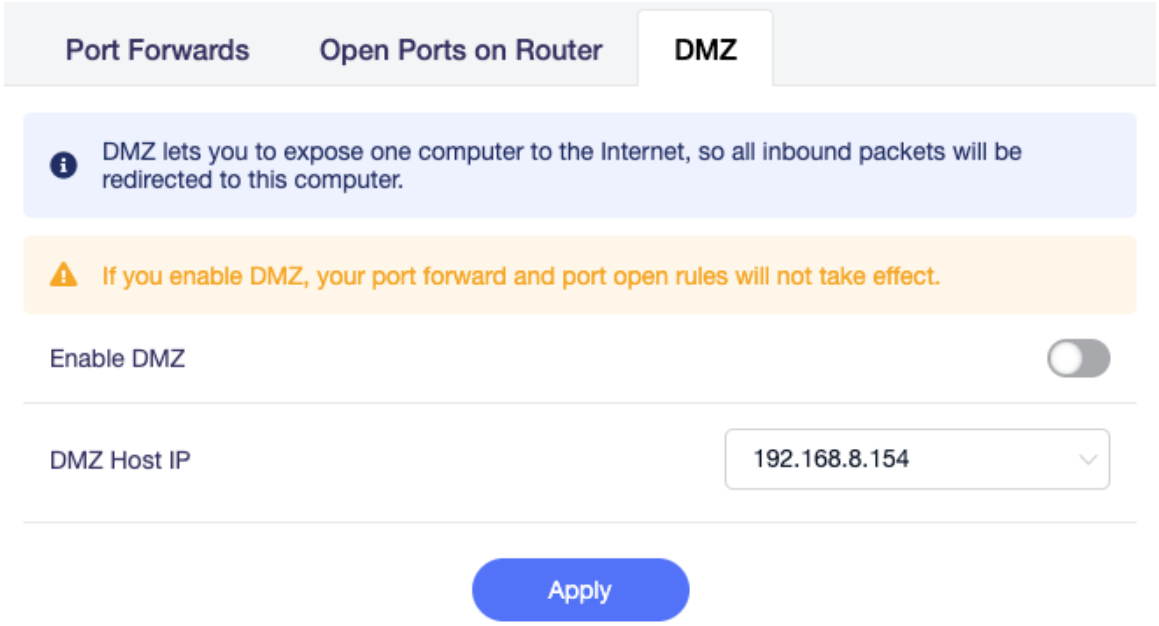
Port: The port number that you want to open.

Enable: Enable of 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

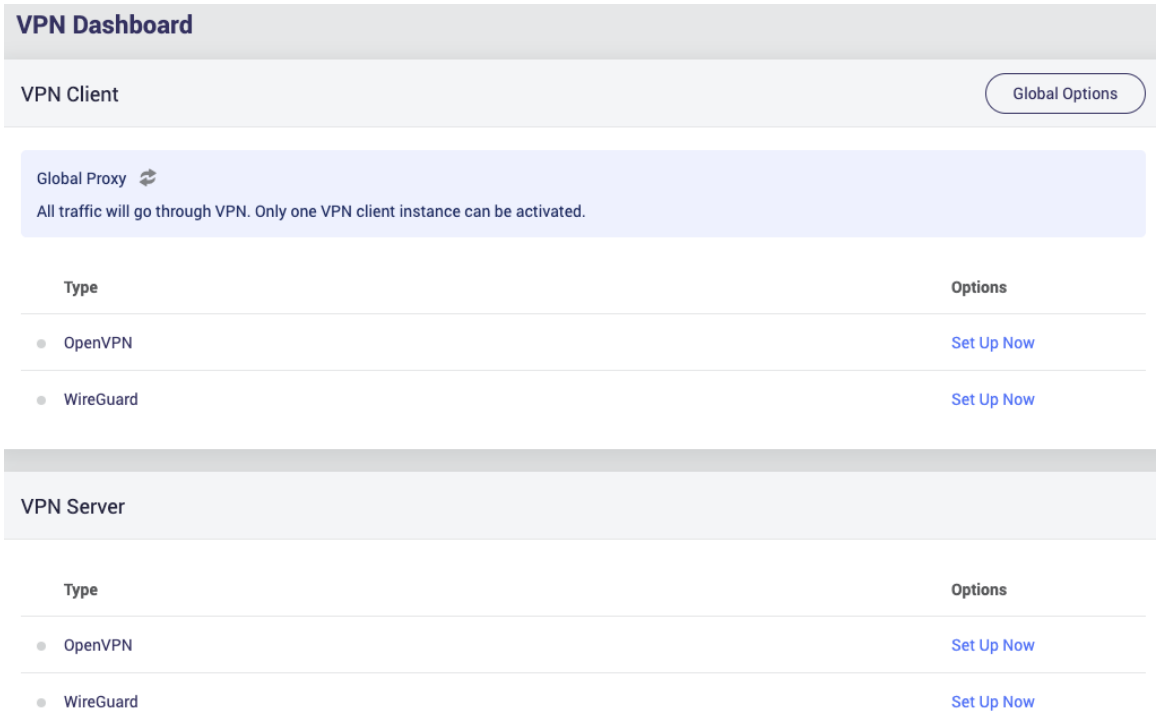
7. VPN

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

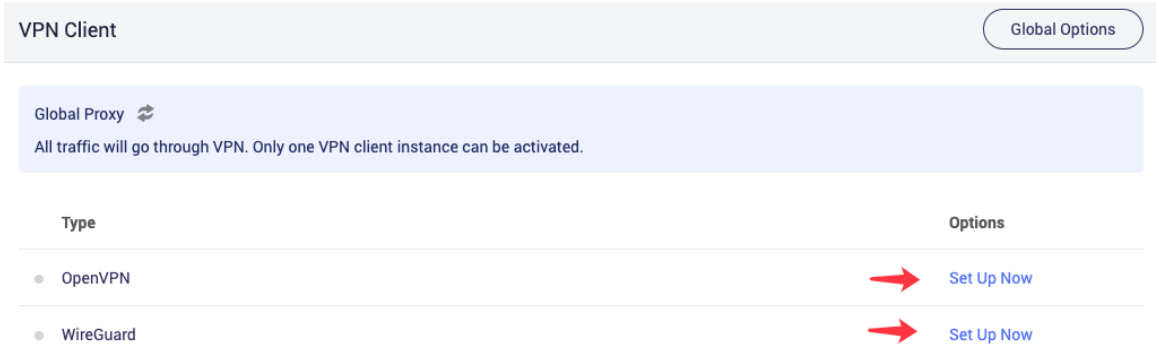
Access to web Admin Panel, on the left side -> VPN -> VPN Dashboard

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

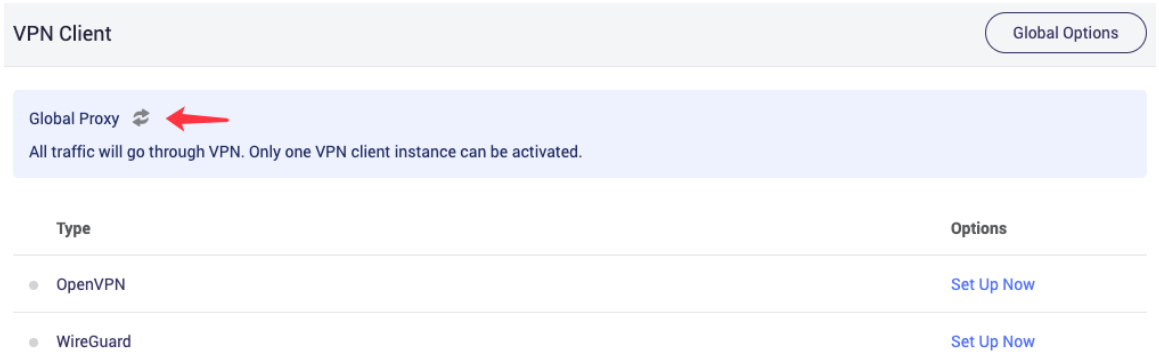


VPN Client

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.



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

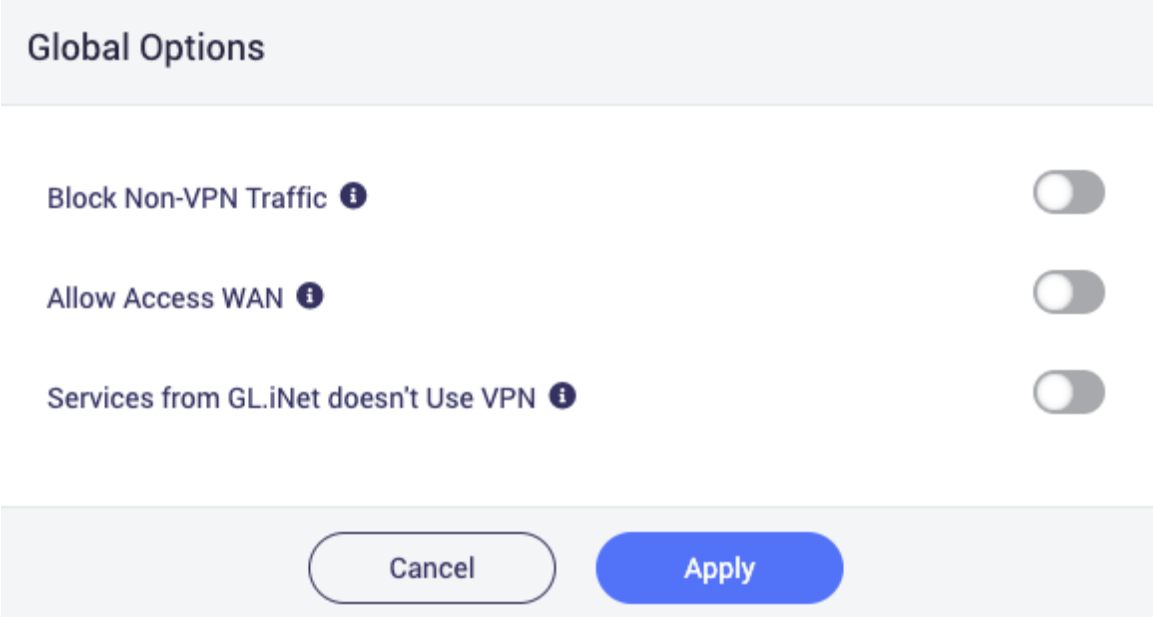
- Auto detect

  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.



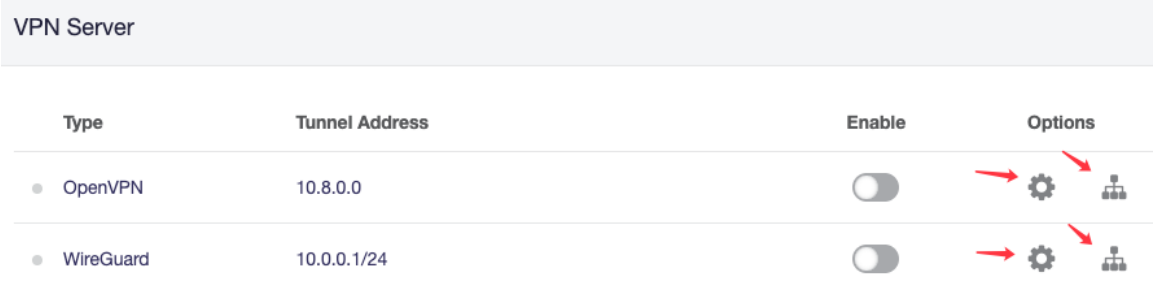
1. Block Non-VPN Traffic

   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

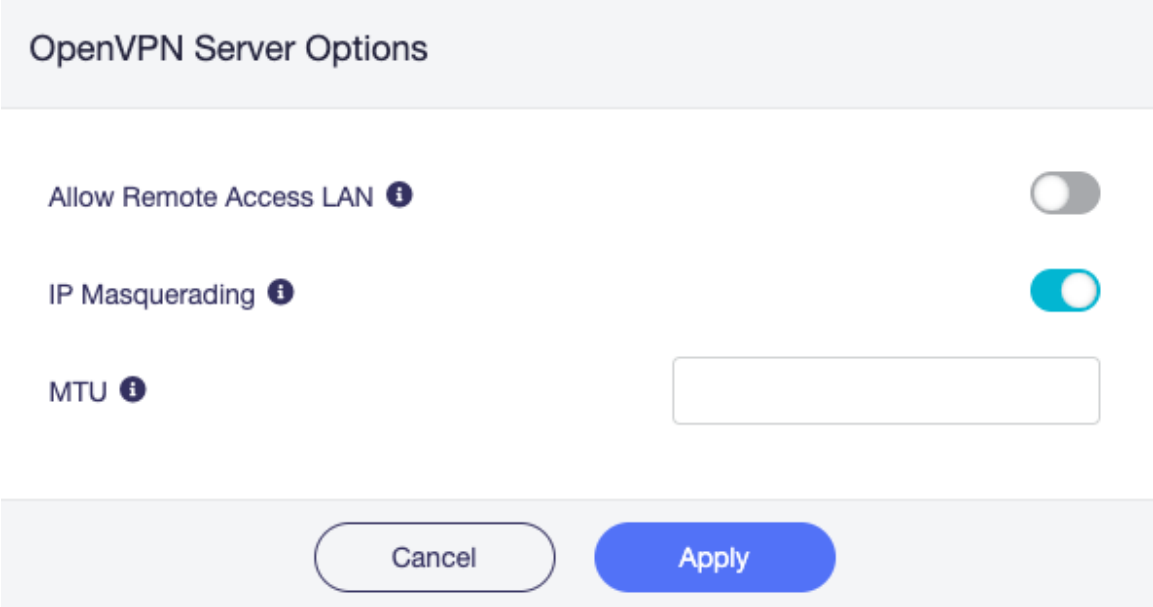
If this option is enabled, services on routers that usually require the use of a real IP will not use VPN. Including GoodCloud, DDNS, rtty.

VPN Server



OpenVPN Server Options

Click the cog icon of OpenVPN server.



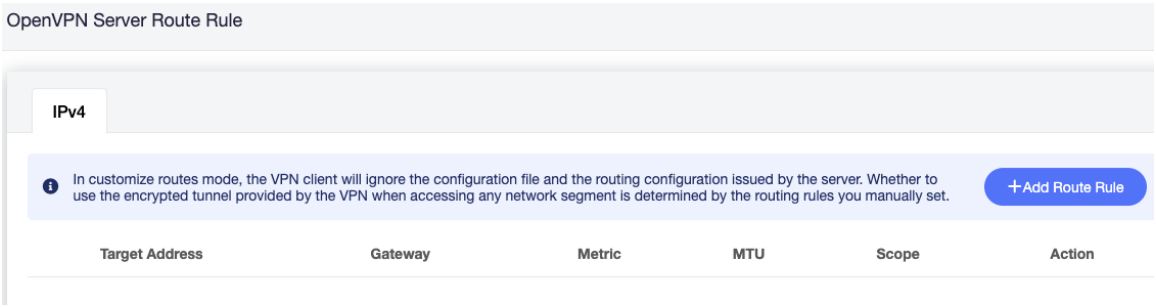
- **Allow Remote Access LAN:** If this option is enabled, resources inside the LAN subnet can be accessed through the VPN tunnel.
- **IP Masquerading:** If this option is enabled, when clients devices on LAN send their IP packets, the router replaces the source IP address with its own address and then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

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

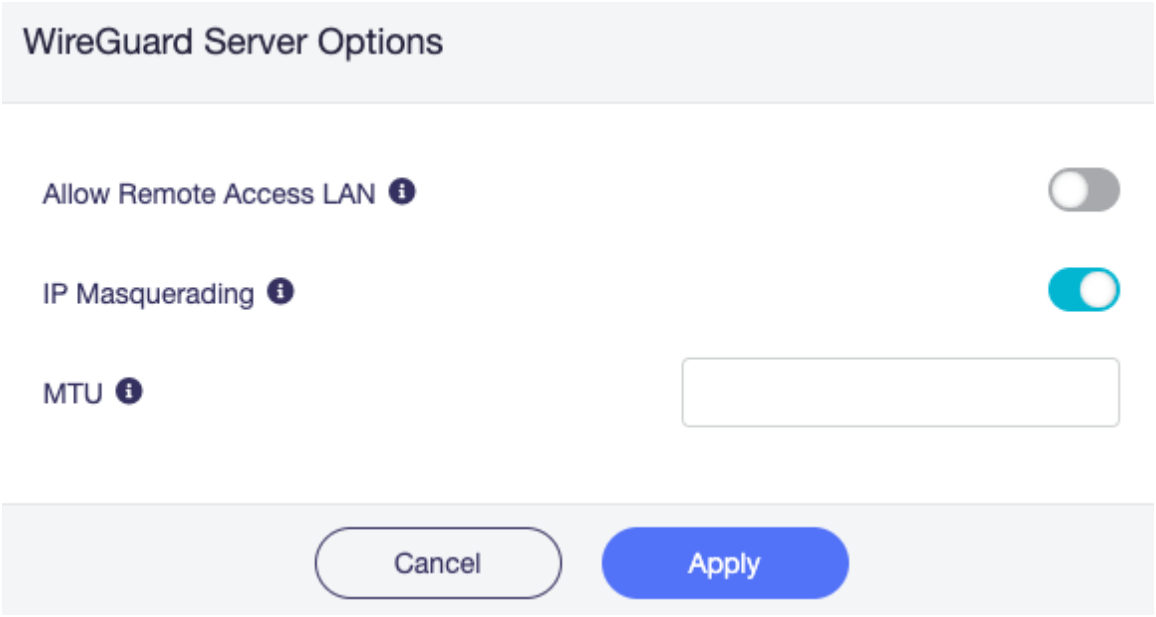
OpenVPN Server Route Rule

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

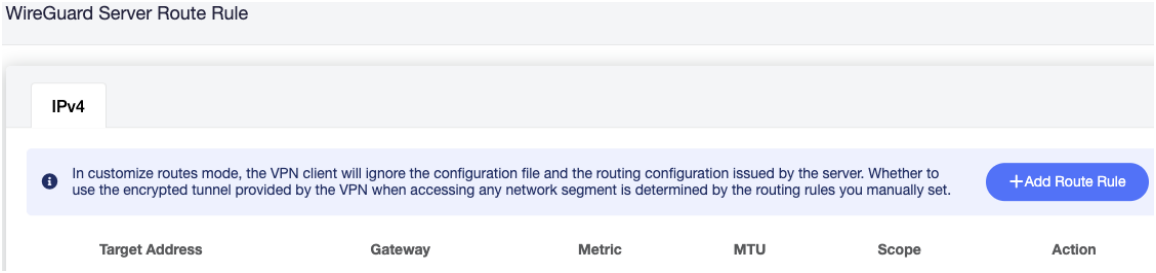
address with its own address and then forwards it to the VPN tunnel.

- **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.



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

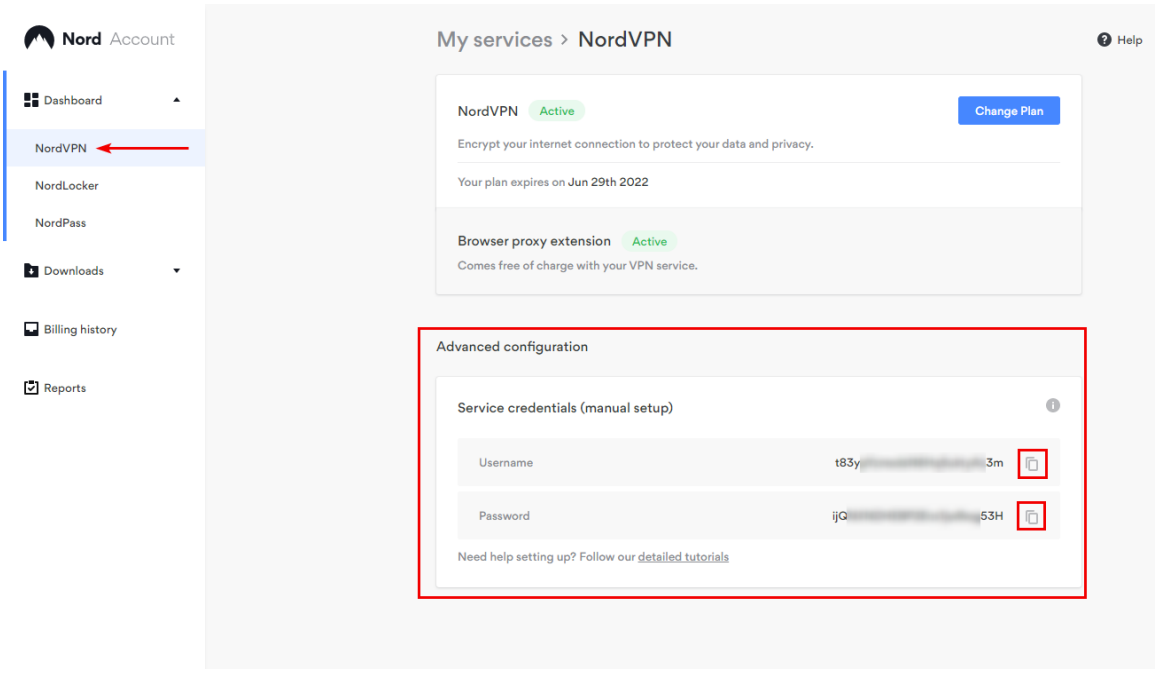
NordVPN is the top online VPN service for speed and security.

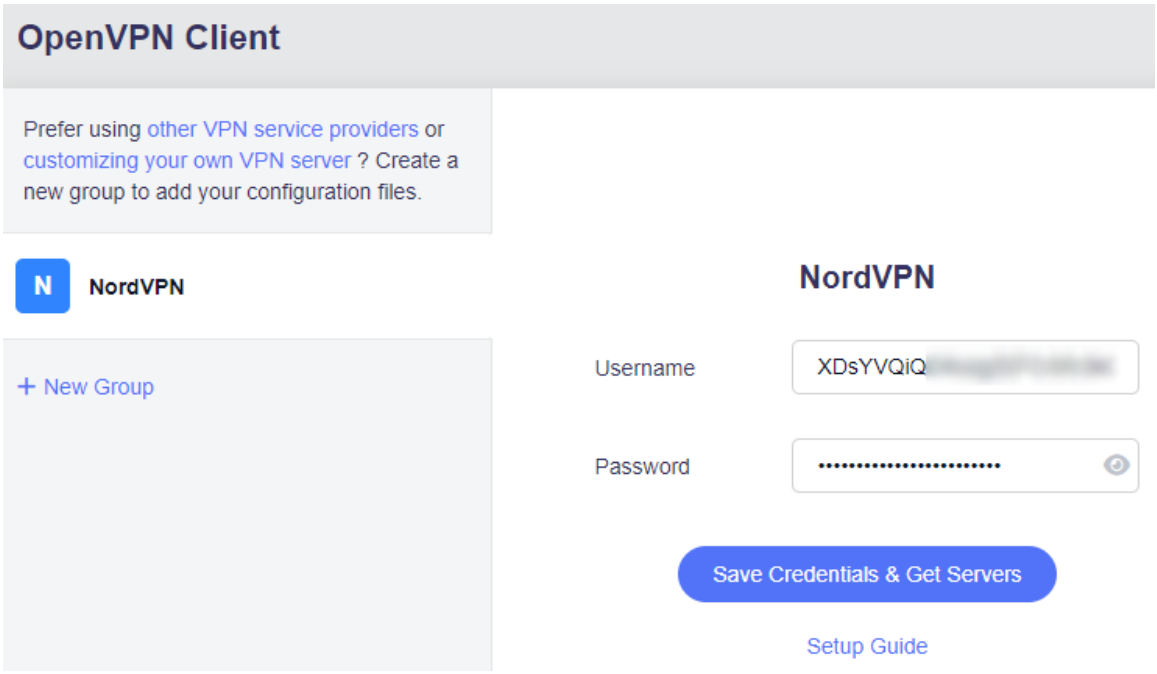
From firmware 4.0.0, it has integrated NordVPN OpenVPN service.

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

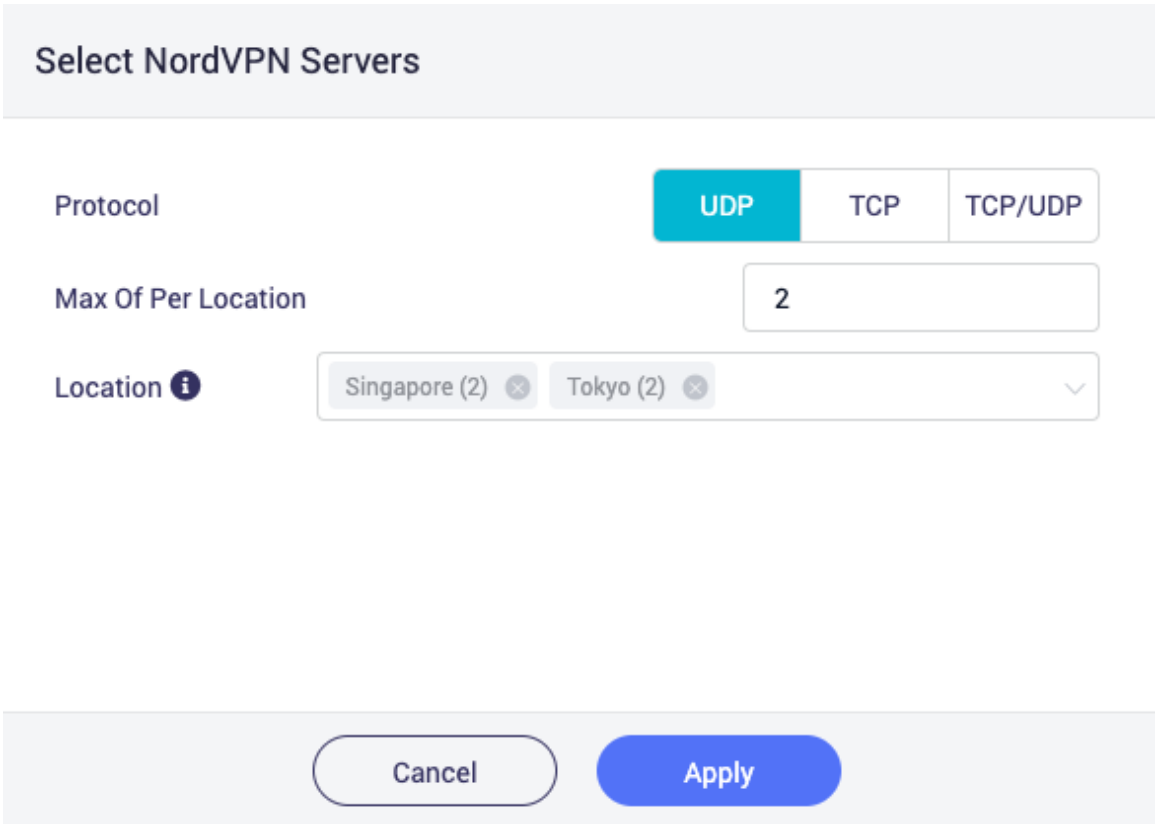
1. Input your NordVPN account's service credentials, then click **Save Credentials & Get Servers**

   Where to find the NordVPN service credentials.

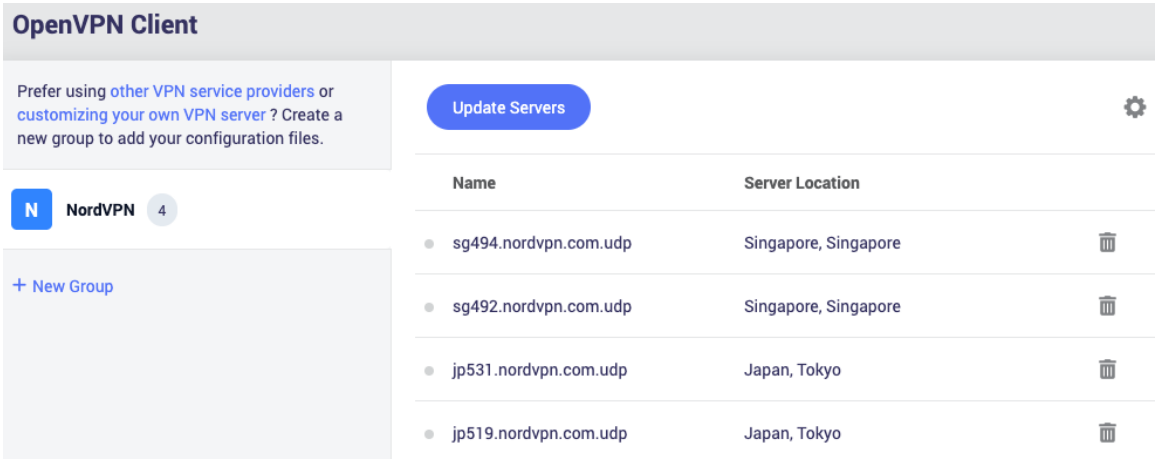




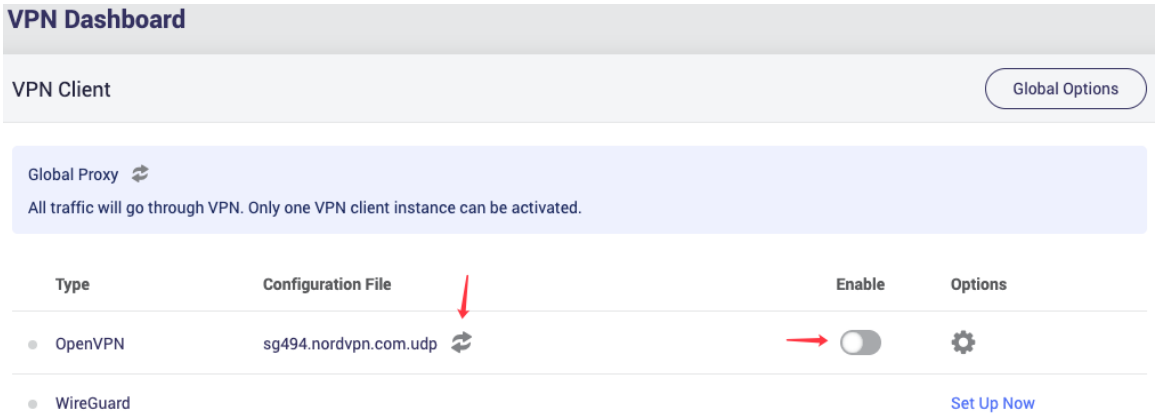
2. Select protocol, max server count of each location, locations, then click **Apply**.



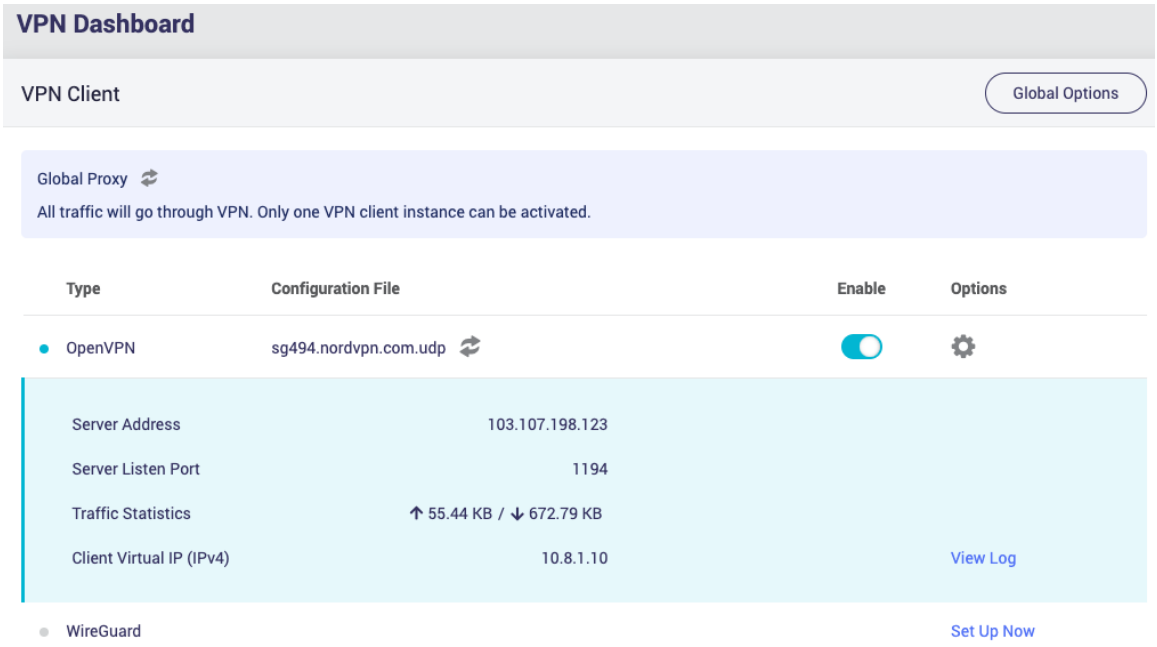
It will download configuration files.



3. Go to VPN Dashboard to enable the connection.

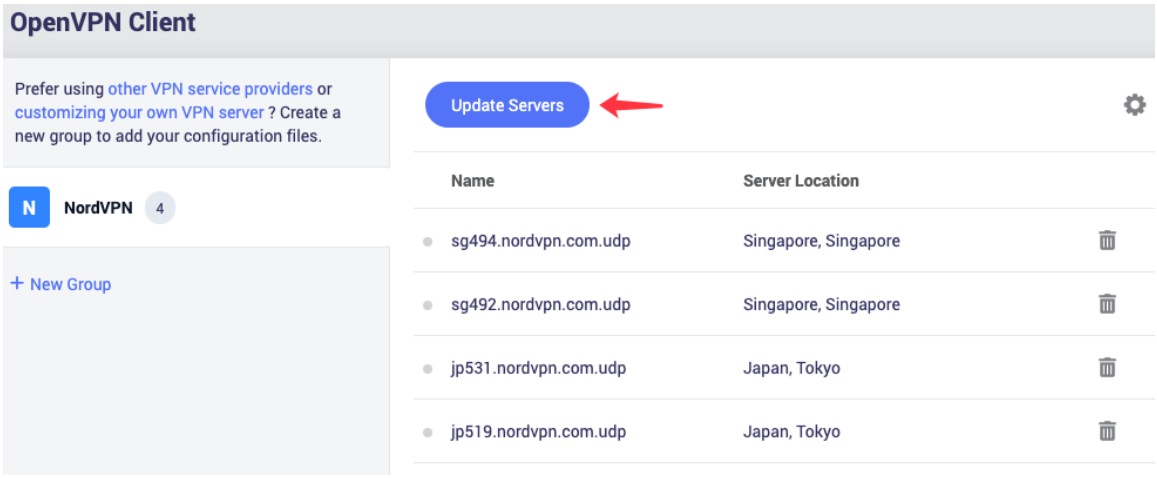


Toggle the switch to enable the connection.



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

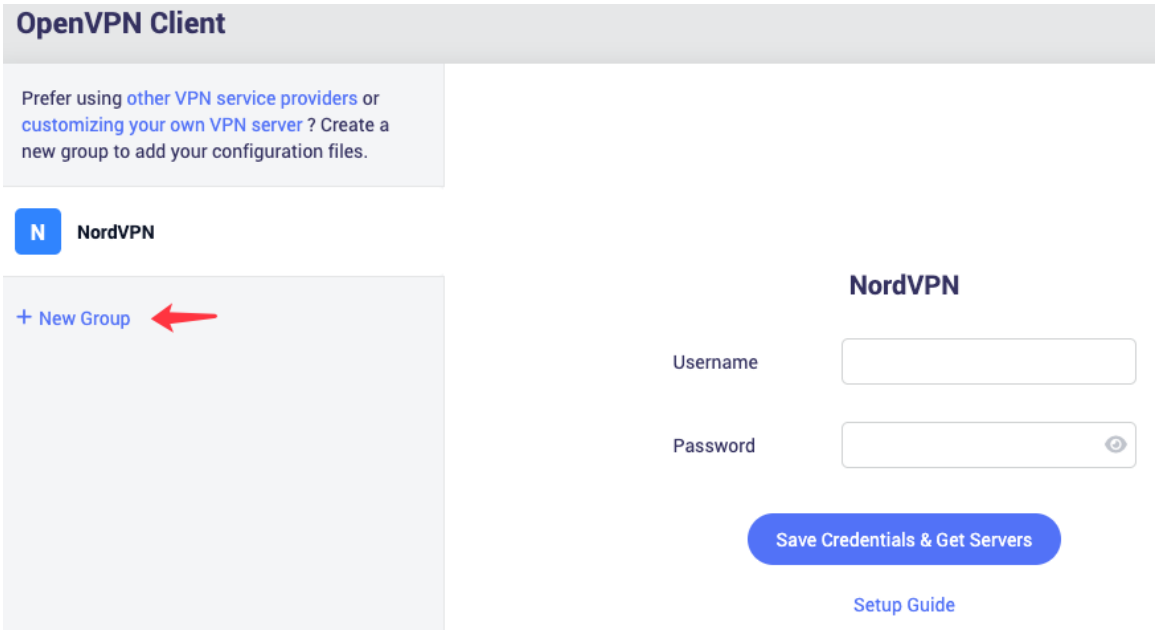
   Click the cog icon to edit the credential.

Setup OpenVPN client

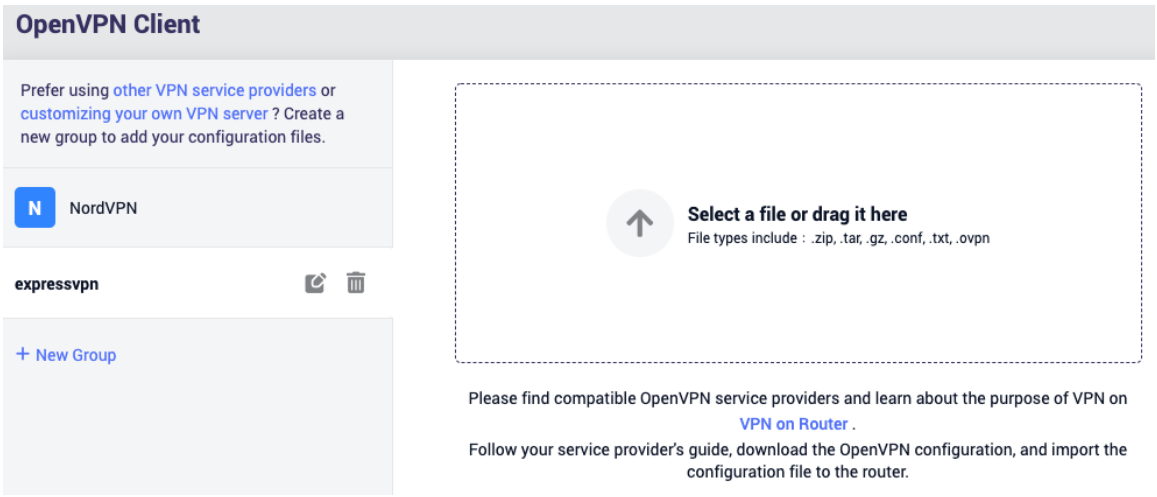
As of frimware 4.0, it brings grouping to manage OpenVPN profiles. Please make sure all the profiles in the same group with the same credentials. For example, if you are ExpressVPN user, you can add a group named *expressvpn*, then upload all the ExpressVPN OpenVPN profiles you wanted to this group.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

Next steps, we will use ExpressVPN as an example.

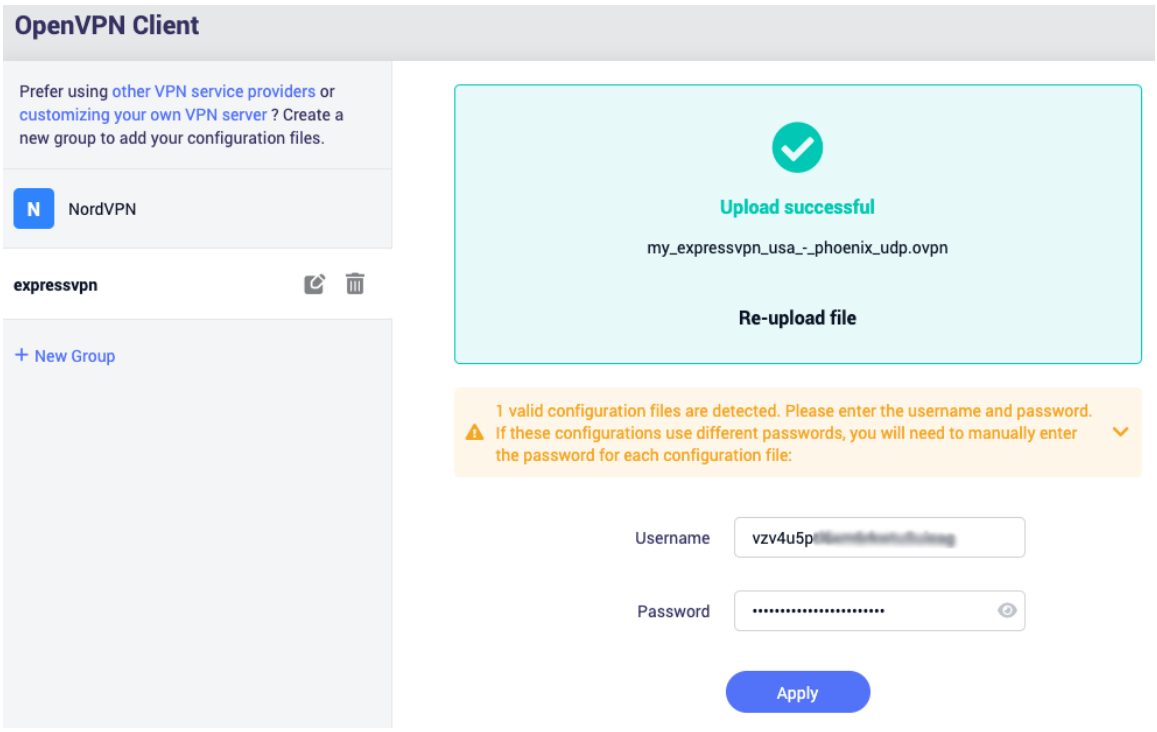
1. Access to web Admin Panel, on the left side -> VPN -> OpenVPN Client
2. Add a new group

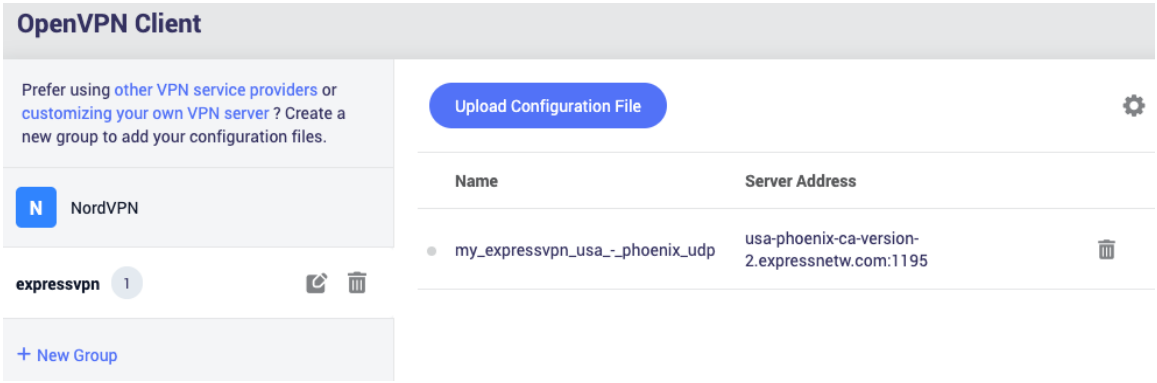


3. Give the group a descriptive name, e.g. expressvpn.

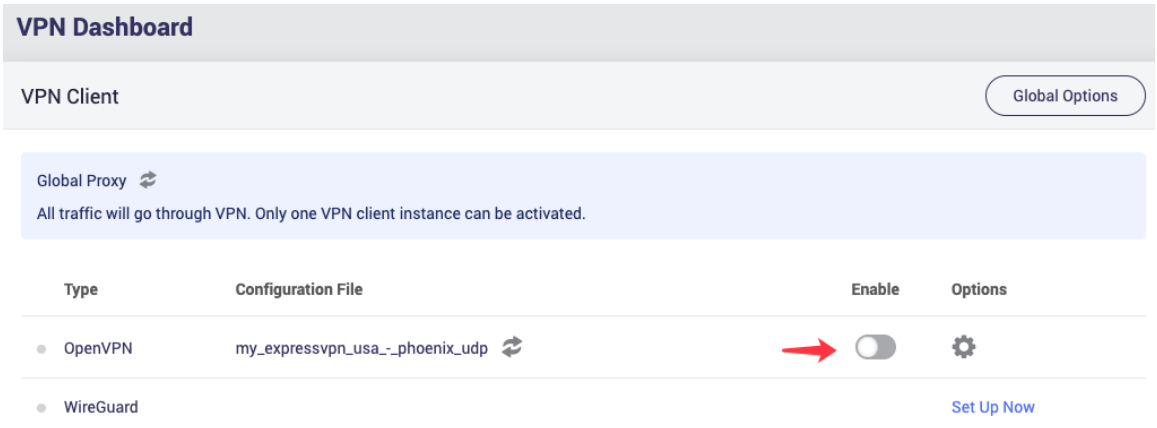


4. Upload your OpenVPN configuration file, then input the credential, click **Apply**.





5. Go to VPN Dashboard to enable the connection.



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.

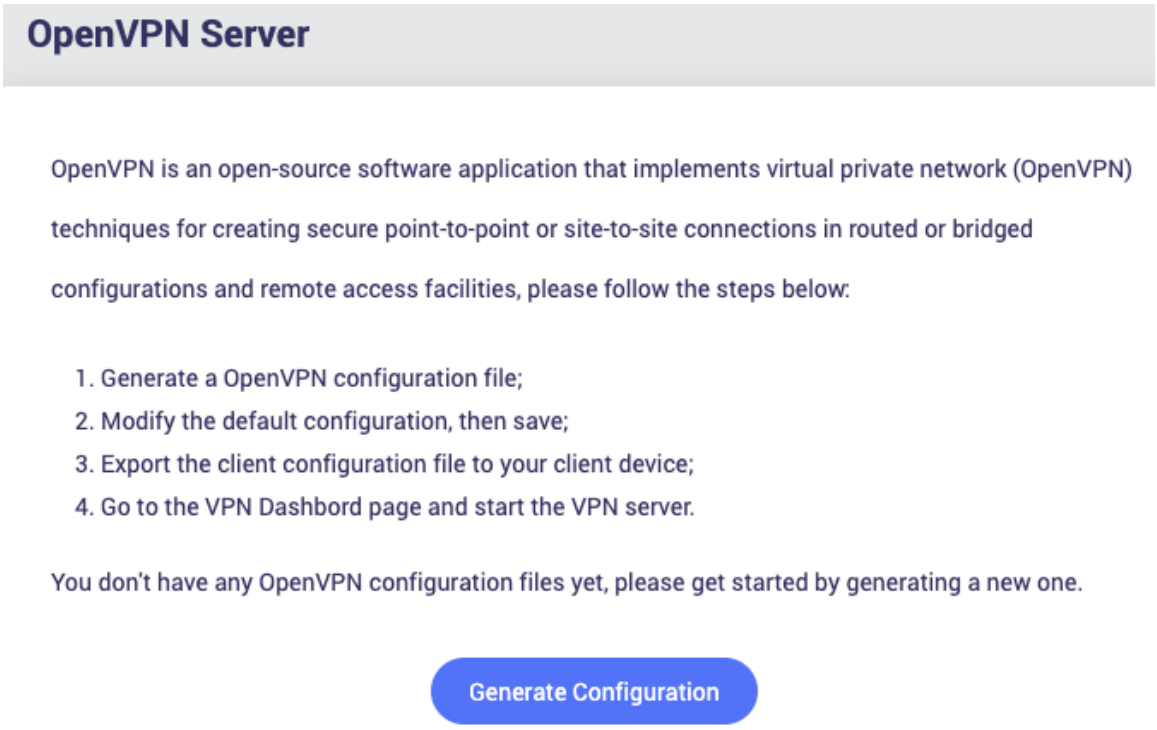
An alternative method is to use a reverse proxy solution, we suggest AstroRelay.

Network Topology

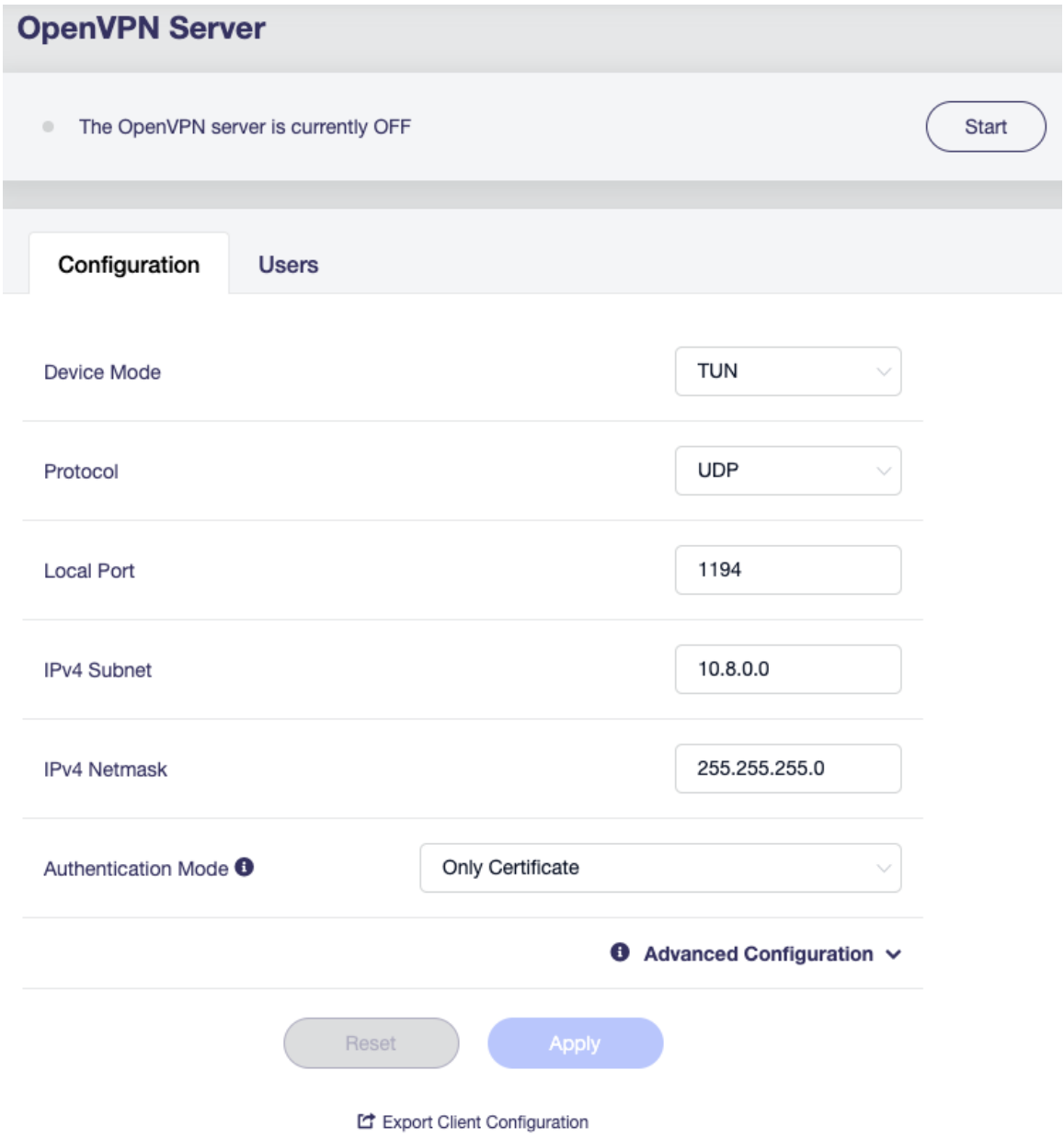
- If GL.iNet router is the main router in your network, this is simple, please move to the next step.
- If you already have a main router, then the GL.iNet router is under the main router, you may need to setup a port forwarding on the main router.
- If you already have a main router, the GL.iNet router 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).



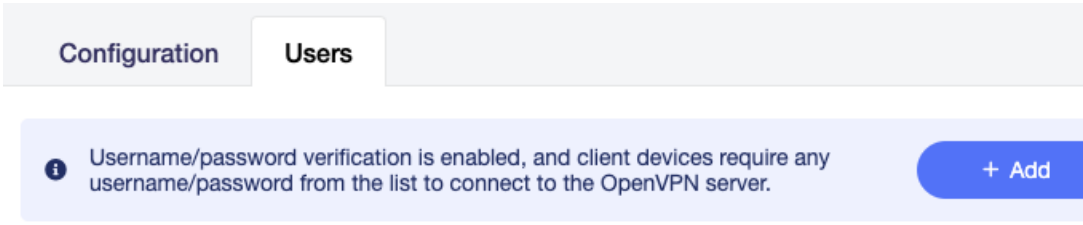
2. Apply the configuration.



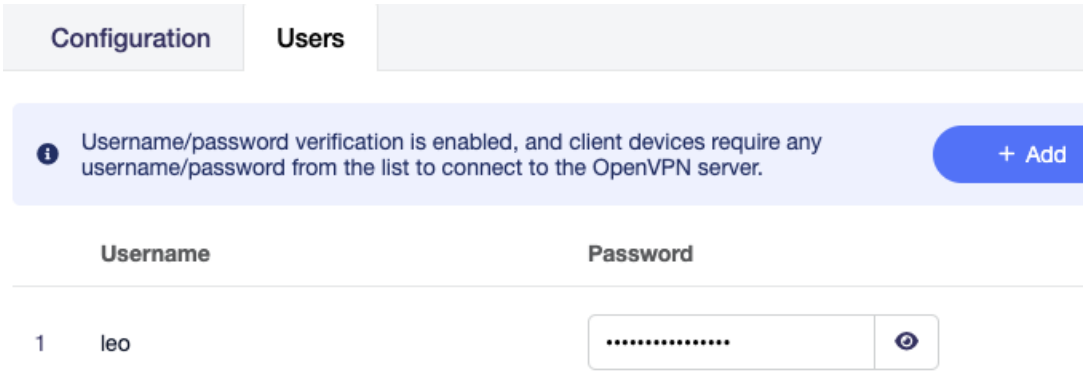
If you do not need to modify the configuration, please click directly the **Export Client Configuration** at the bottom of page. If you have modified the configuration, please click the **Apply** button to continue.

- **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**, **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.



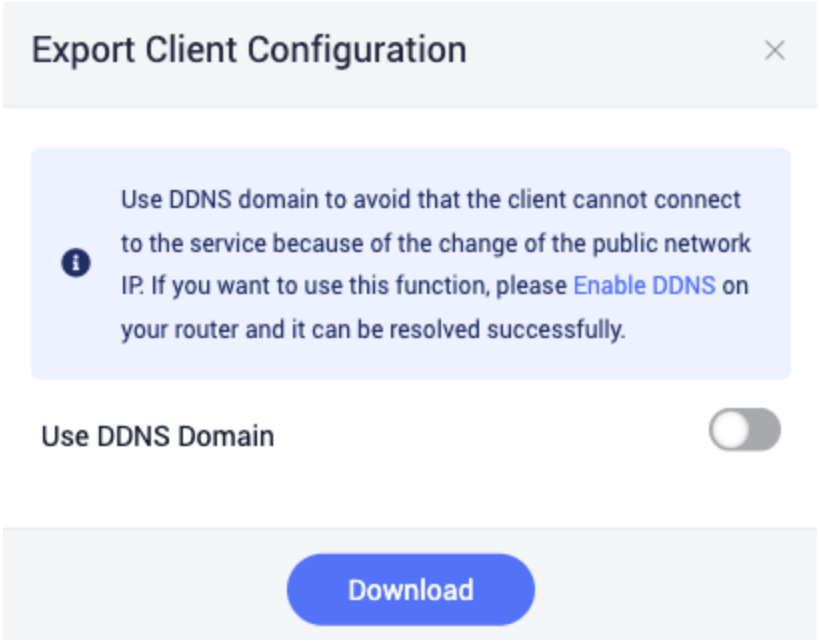
For **Only Certificate** and **Username/Password and Certificate**, the router will automatically generate a server and client certificate-key, and write into the configuration file when generating the client configuration file.

Please check here for **Advanced Configuration**.

3. Export Client Configuration

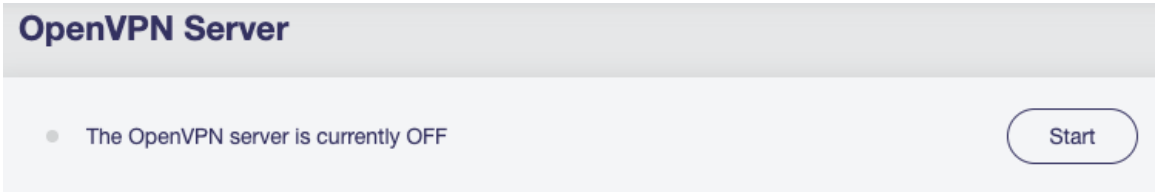
   Clicking the **Export Client Configuration** button at the bottom or applying the modified configuration will pop up this dialog.

   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.

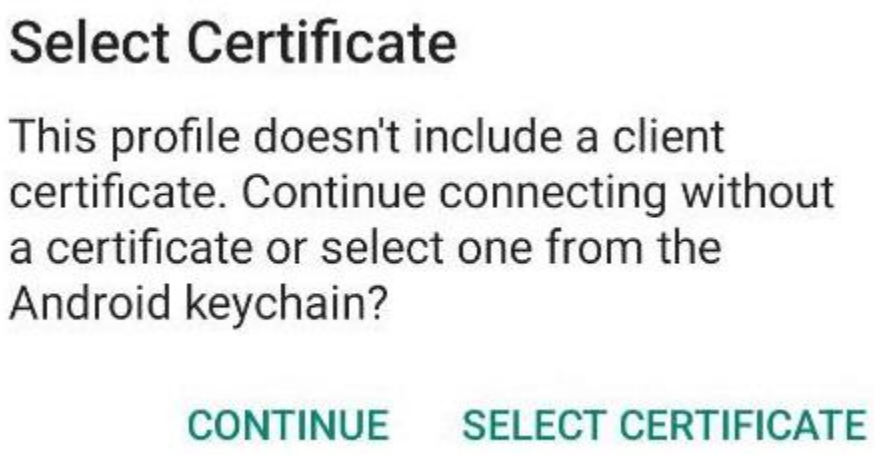


To check if OpenVPN Server is working properly

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 simpliest 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.

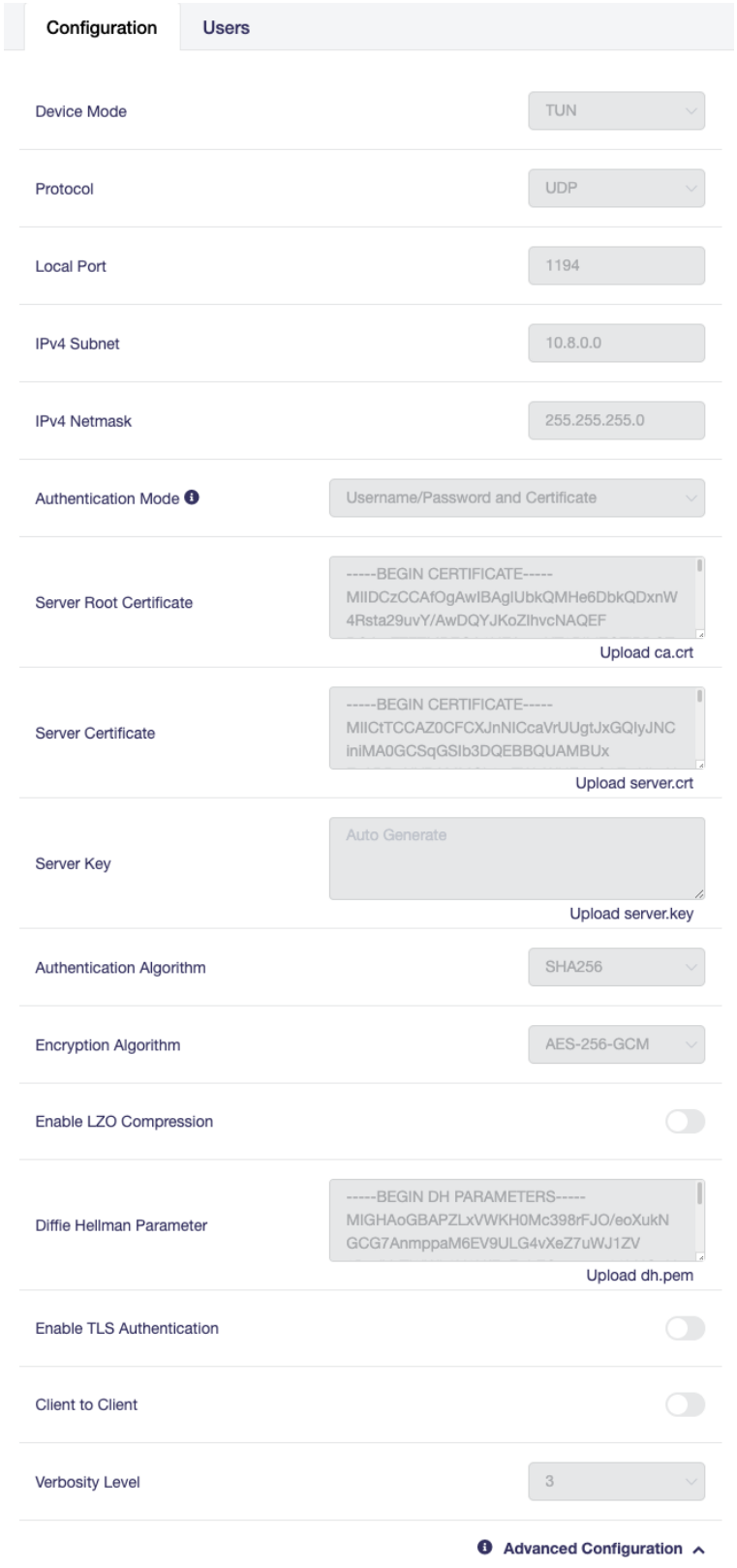
When importing the configuration file to the OpenVPN app, it may has a reminder as below, please click **CONTINUE** as the certificate is already included in the configuration file.



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



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.

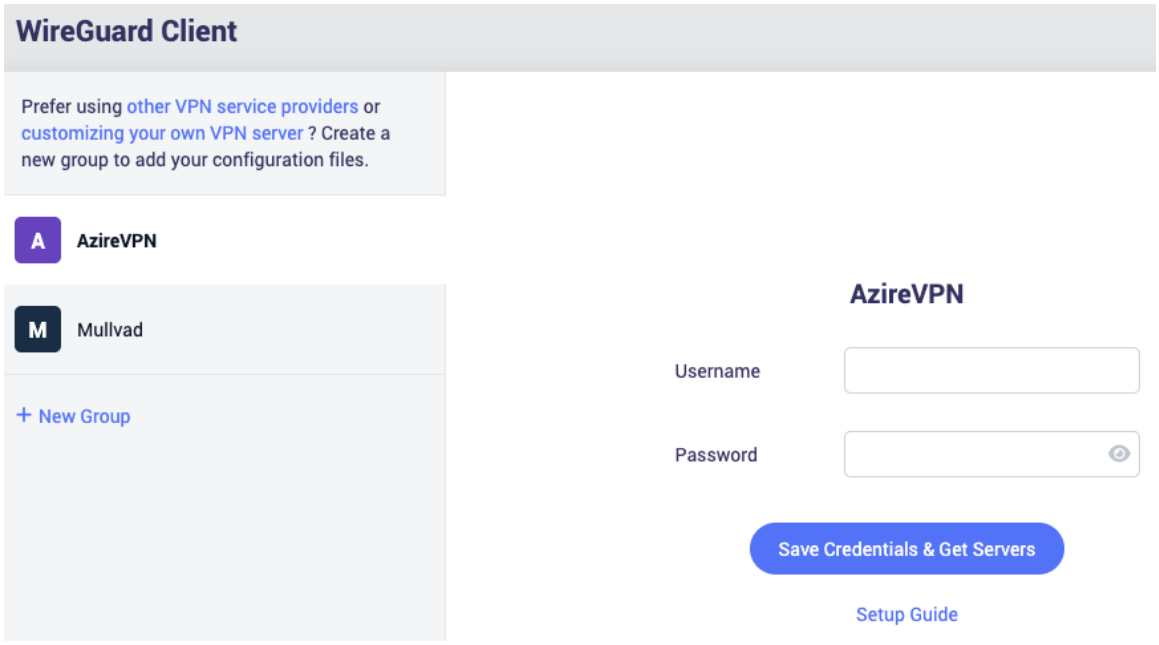
You can setup WireGuard Client via web Admin Panel and mobile app. For the mobile app, it has already integrated some WireGuard Service Providers, they are AzireVPN, Mullvad VPN, TorGuard VPN, OVPN, WeVPN, StrongVPN, PIA VPN, SpiderVPN.

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

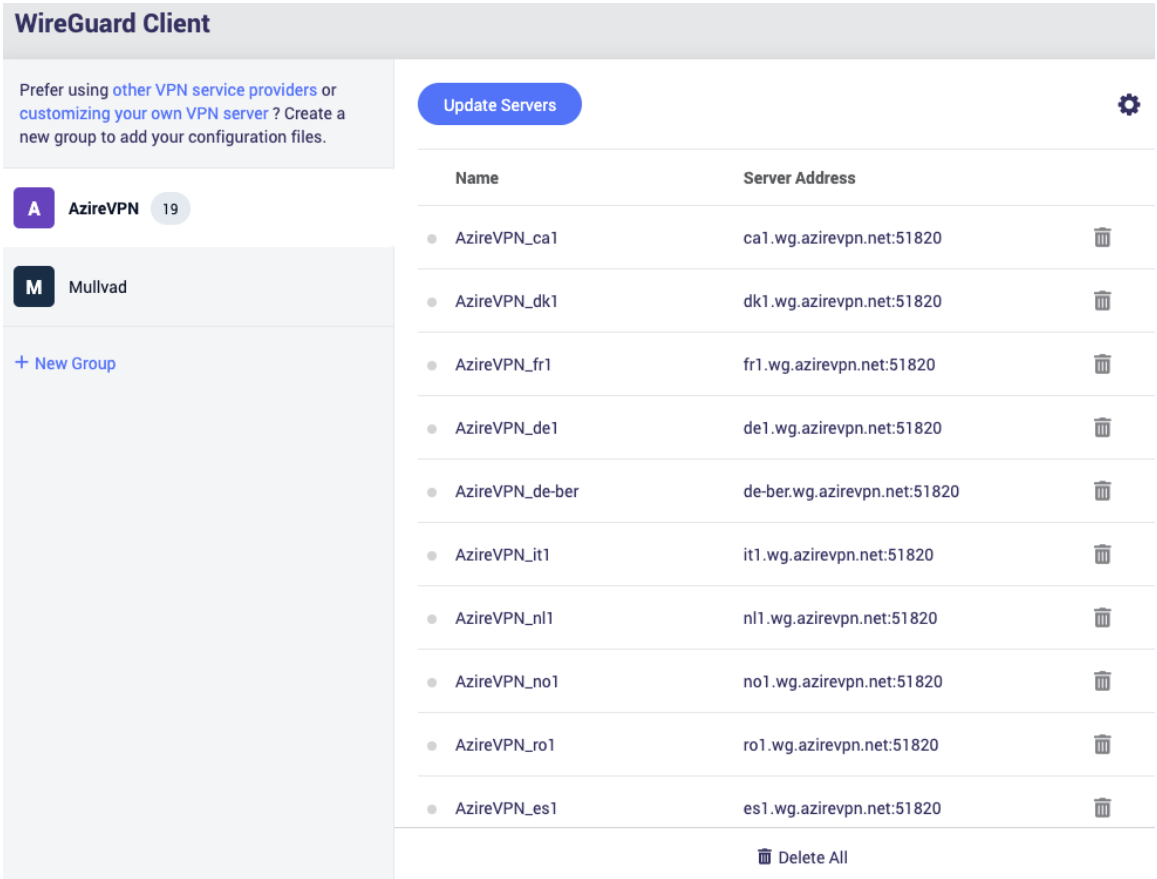
Setup AzireVPN

AzireVPN is privacy-minded VPN service providing secure, modern and robust tunnels such as WireGuard.

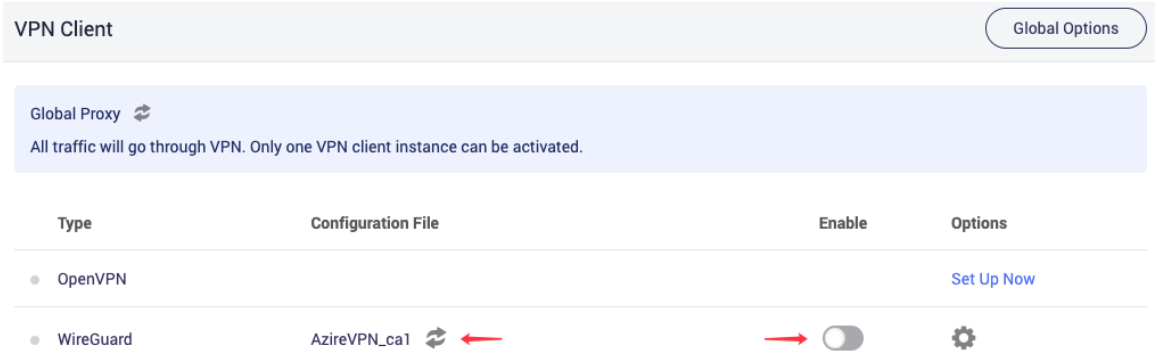
Firmware 4.x has integrated AzireVPN WireGaurd service.



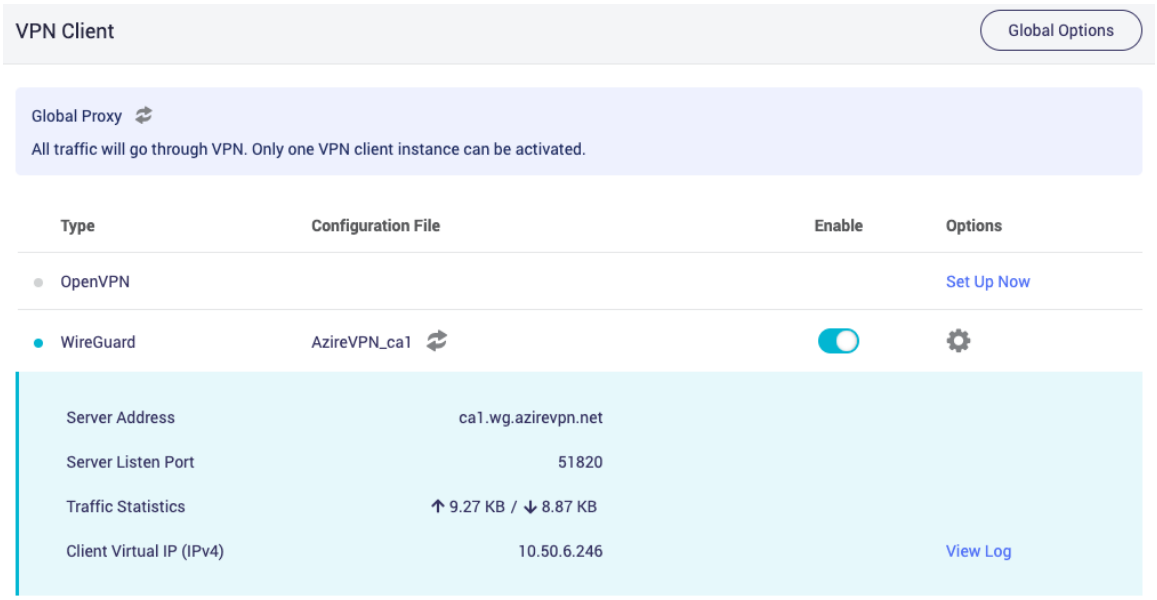
1. Input **Username** and **Password**, then click **Save Credentials & Get Servers**. It will generate configuration files for each servers.



2. Go to VPN Dashboard to enable the connection.

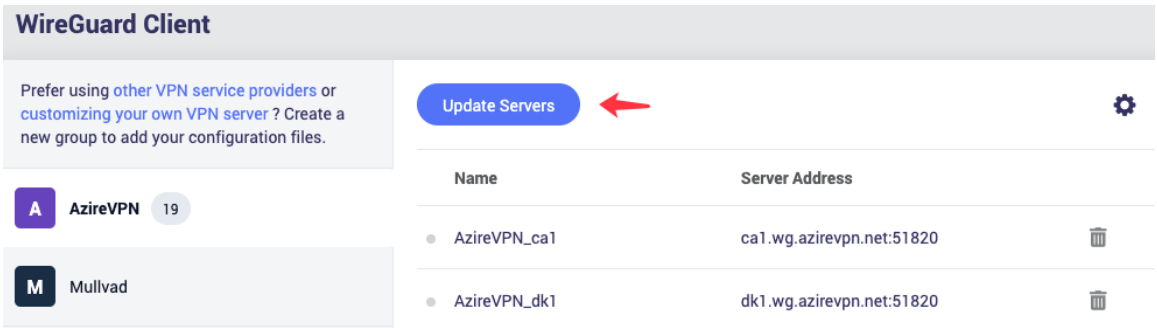


Once connected, you should see your user IP address and the number of Bytes send/received.



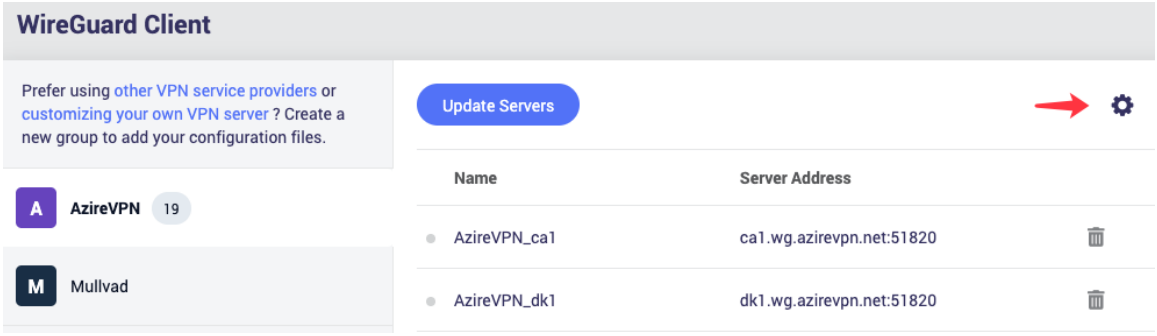
3. Update servers

   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

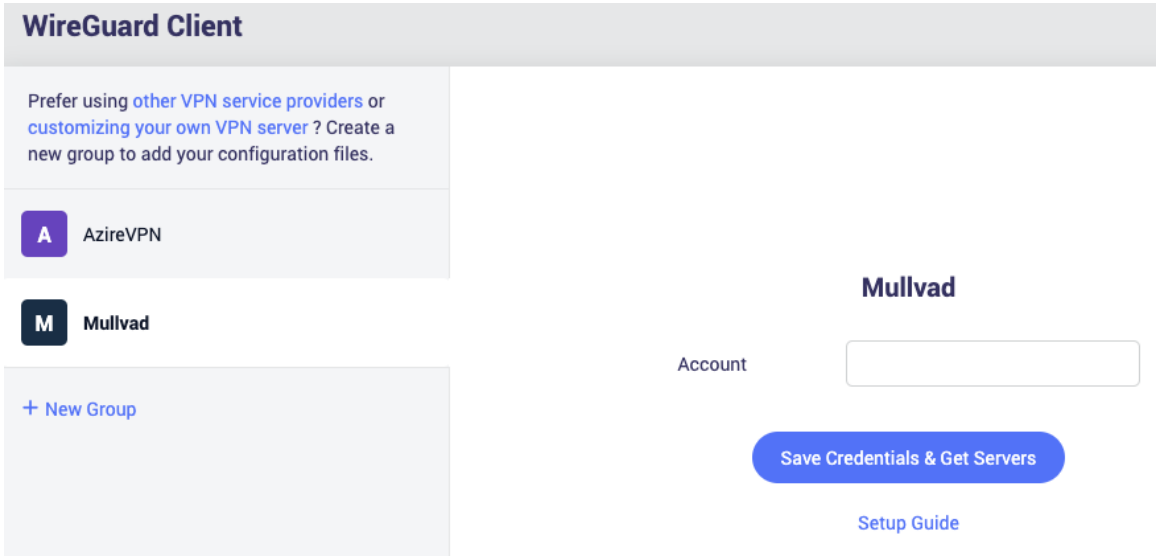
Click the cog icon to edit the credential.



Setup Mullvad

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

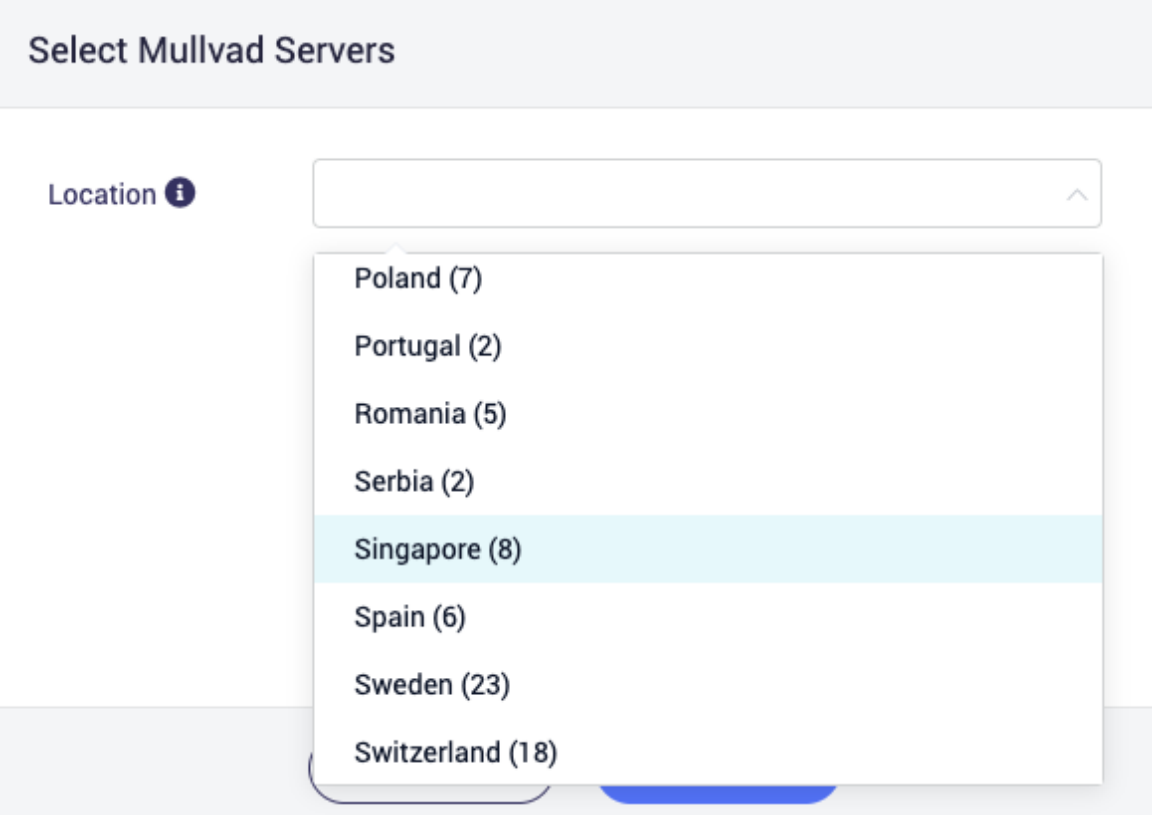
Firmware 4.x has integrated Mullvad WireGaurd service.



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

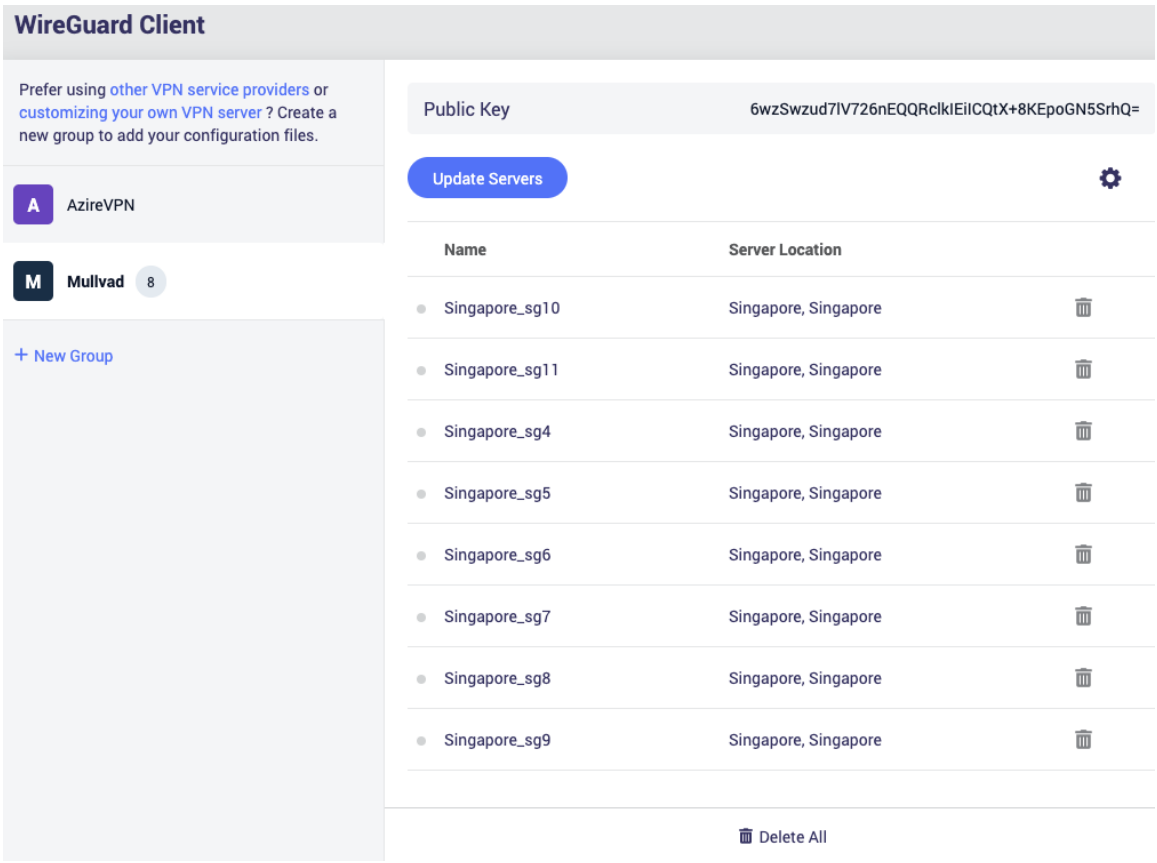
   Mullvad account number is a 16-digit decimal in the "1000 0000 0000 0000" to "9999 9999 9999 9999" range.

   It will pop up a dialog to select a location.

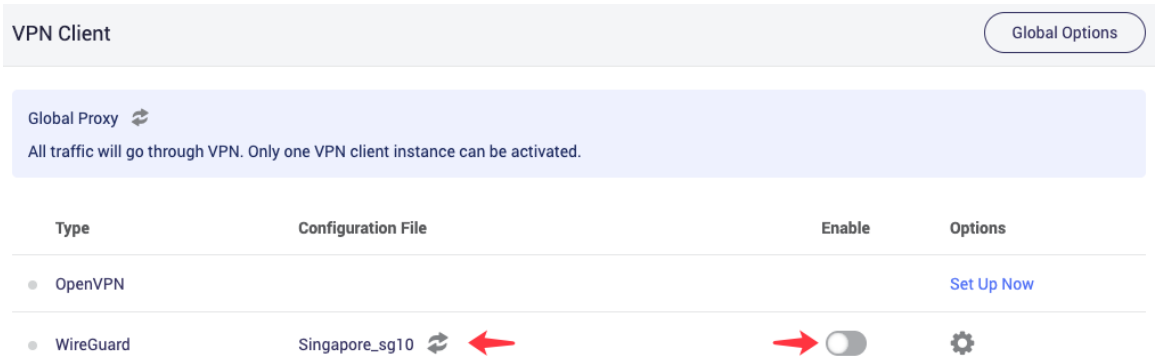


Then it will generate the configuration files of the selected location server.

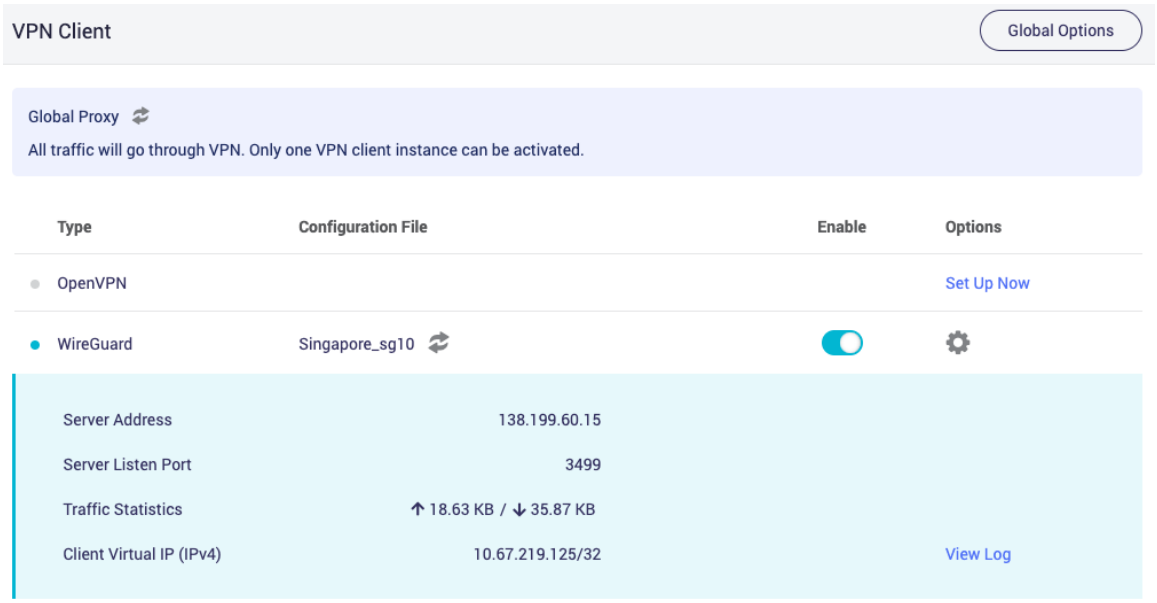
The **Public Key** is the WireGuard public key to send to Mullvad server, you can have up to five keys at the same time, you can manage WireGuard keys on Mullvad's page.



2. Go to VPN Dashboard to enable the connection.

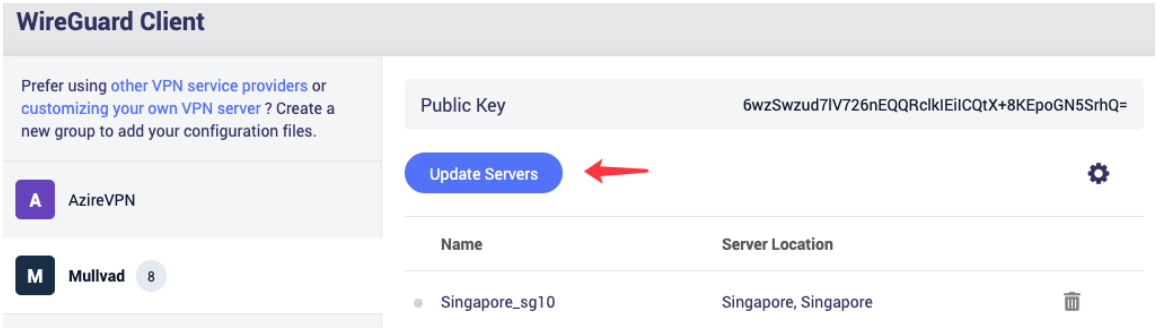


Once connected, you should see your user IP address and the number of Bytes send/received.

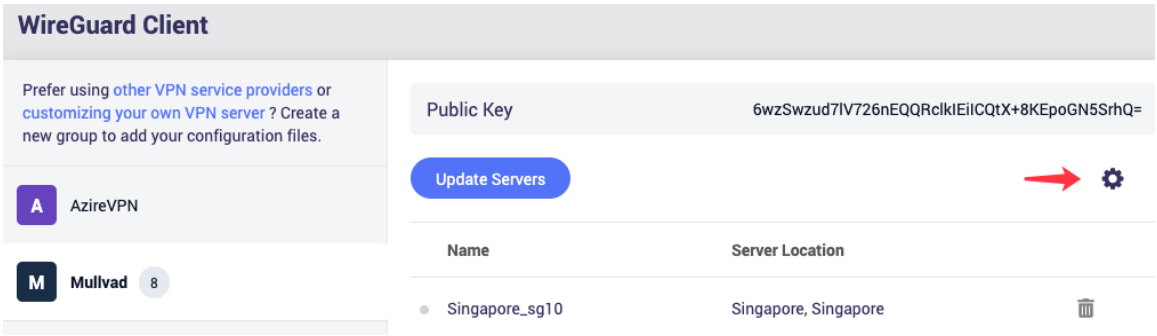


3. Update servers

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



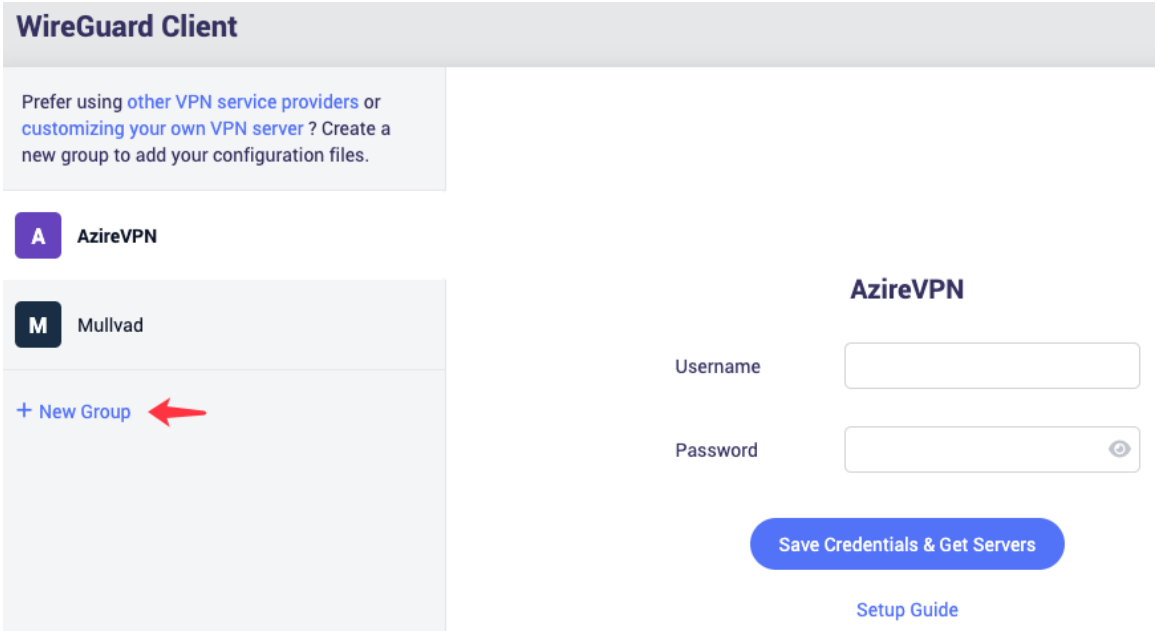
4. Edit credential



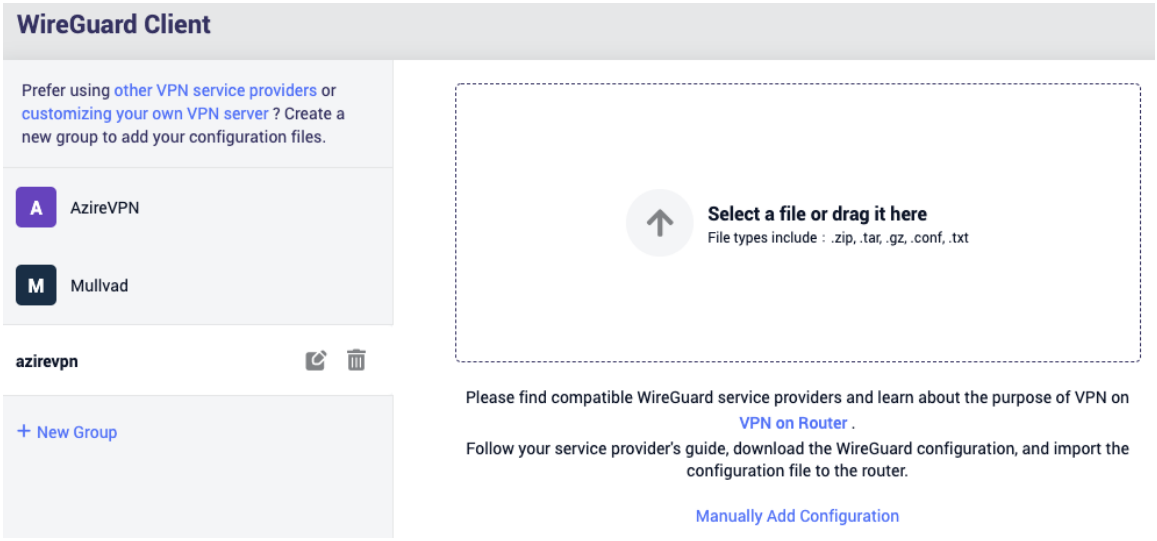
Setup WireGuard client

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

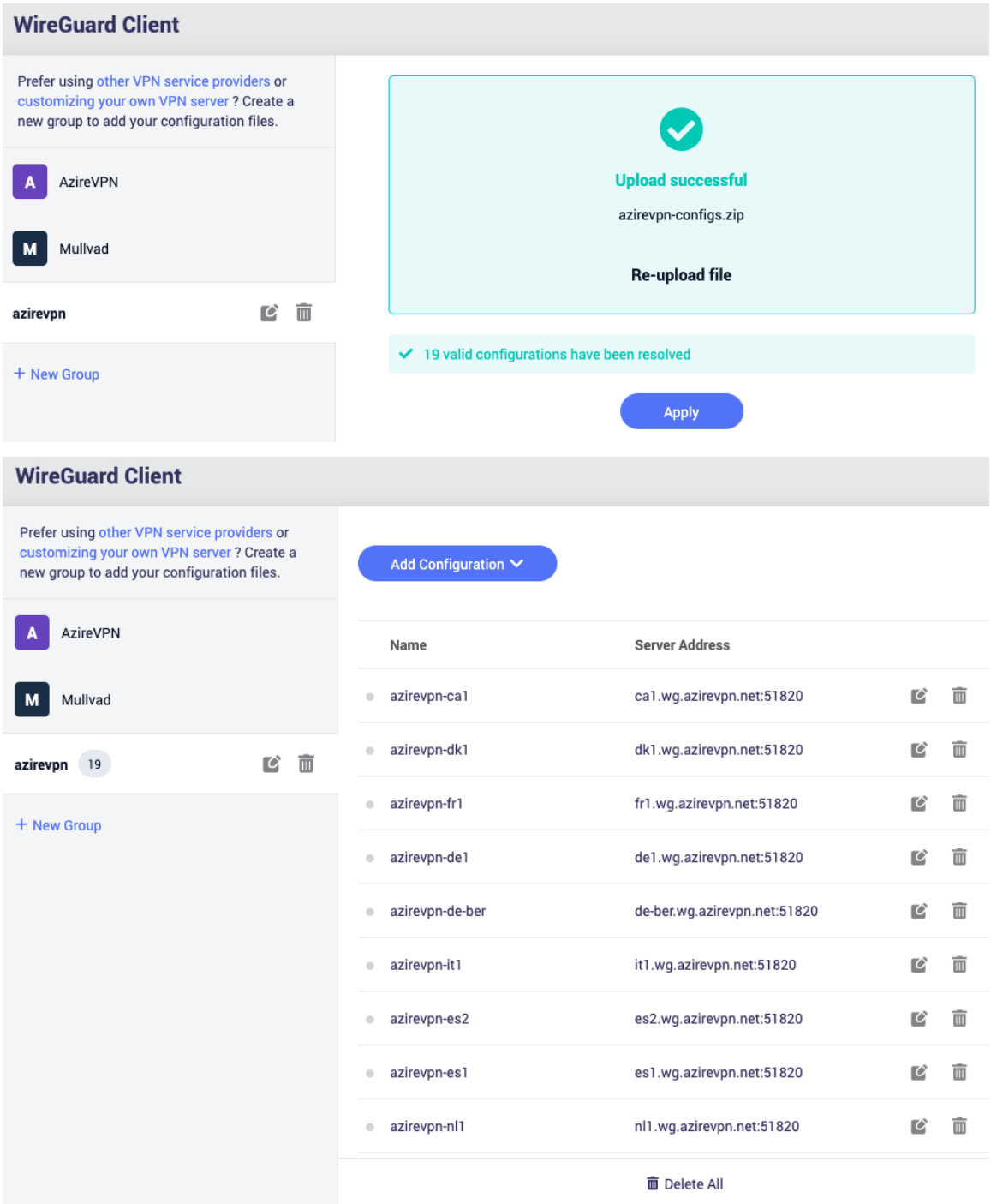
1. Add a new group



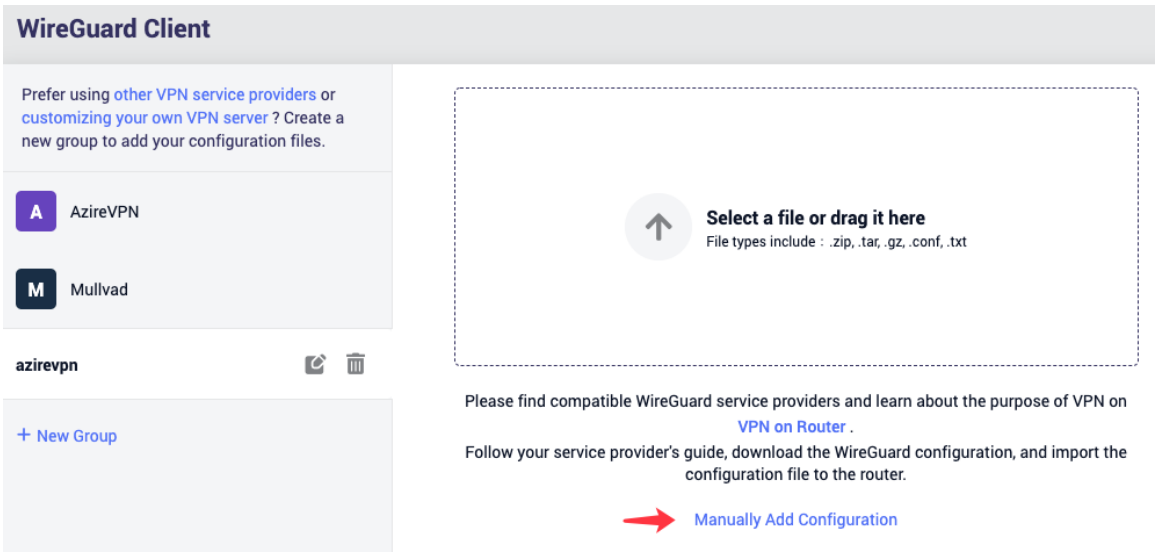
2. Give the group a descriptive name, e.g. azirevpn.



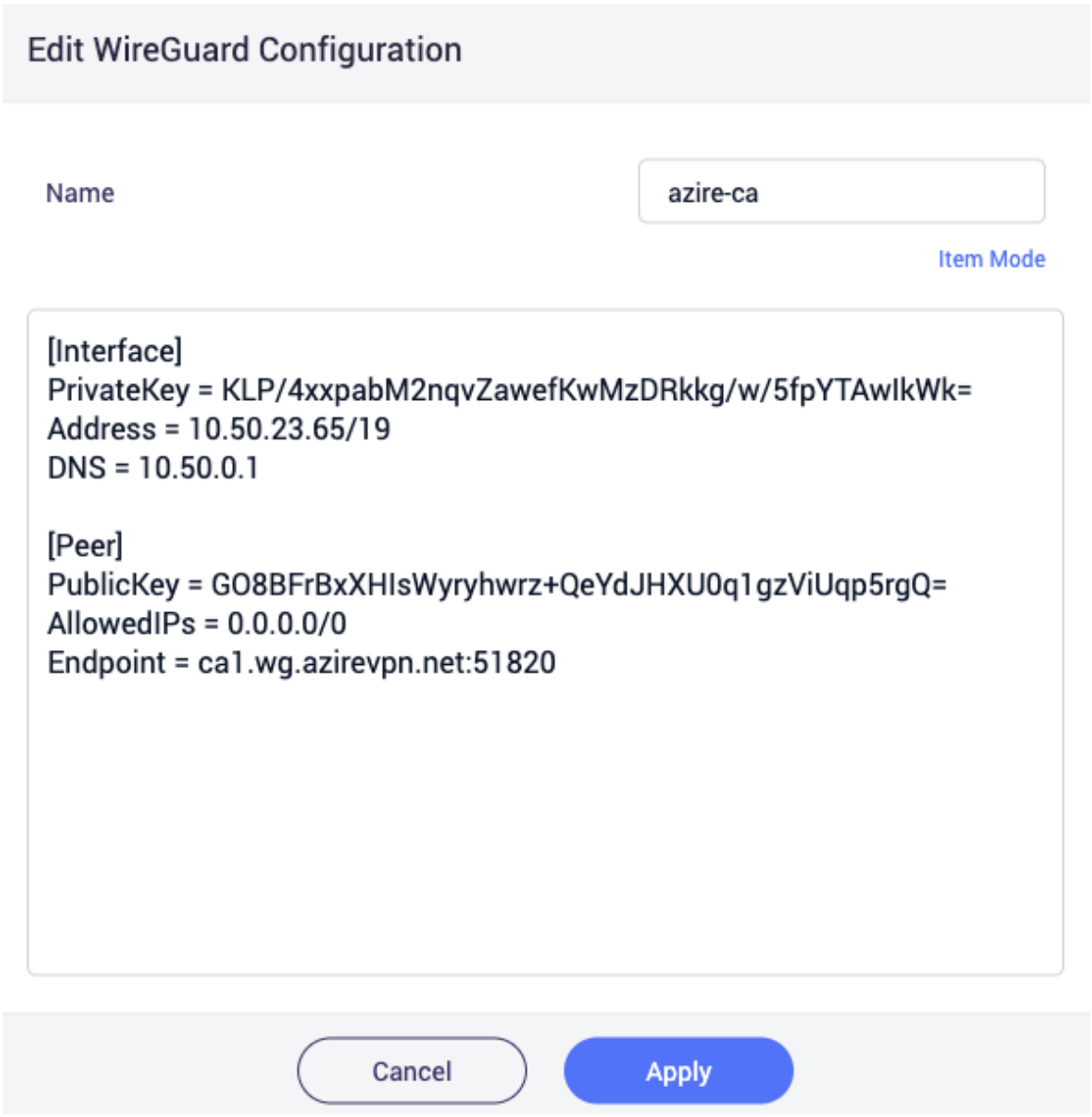
3. Upload your WireGuard configuration file, then input the credential, click **Apply**.



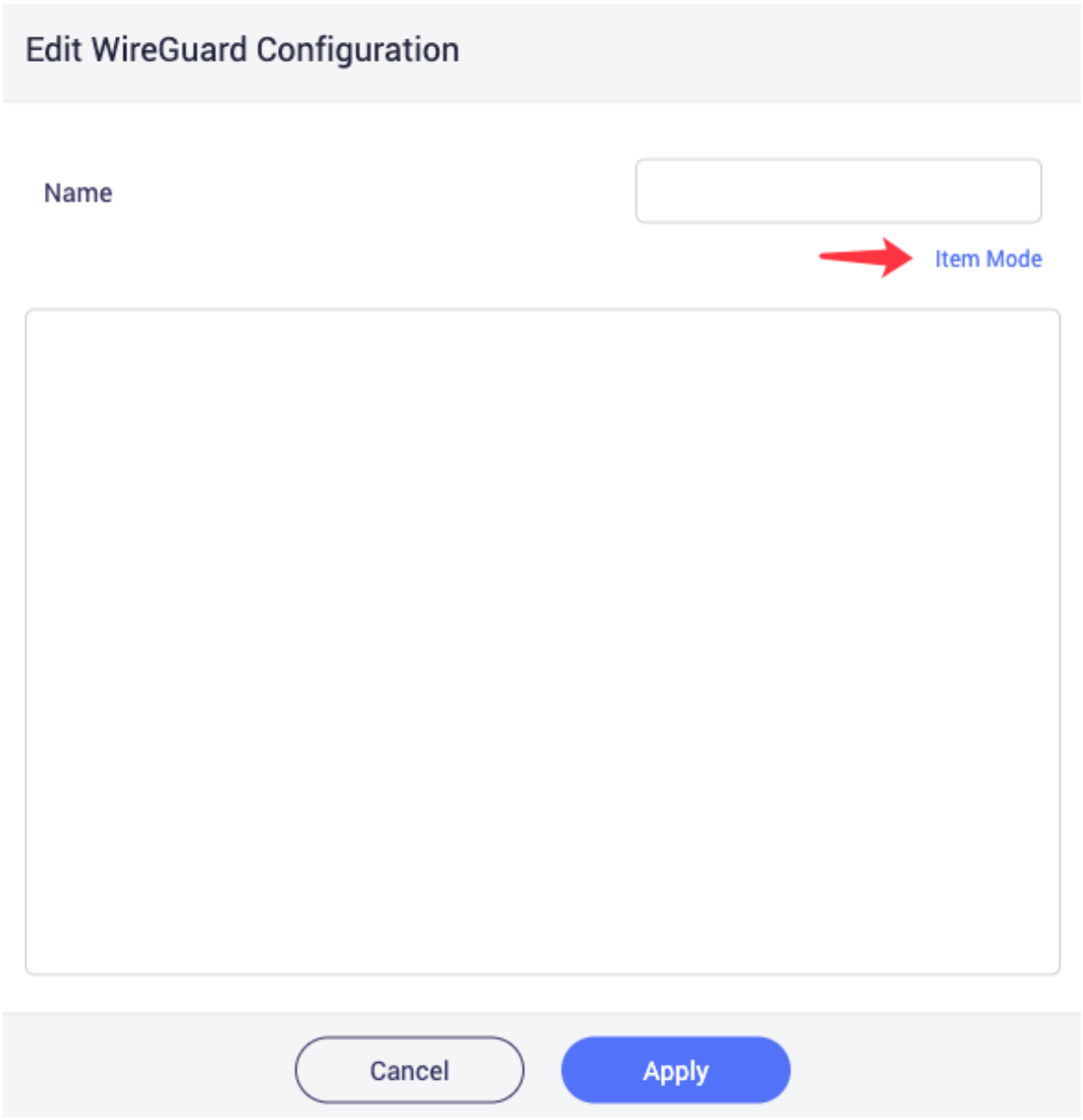
Manually Add Configuration is for if you want to paste the WireGuard configuration or fill in each item.

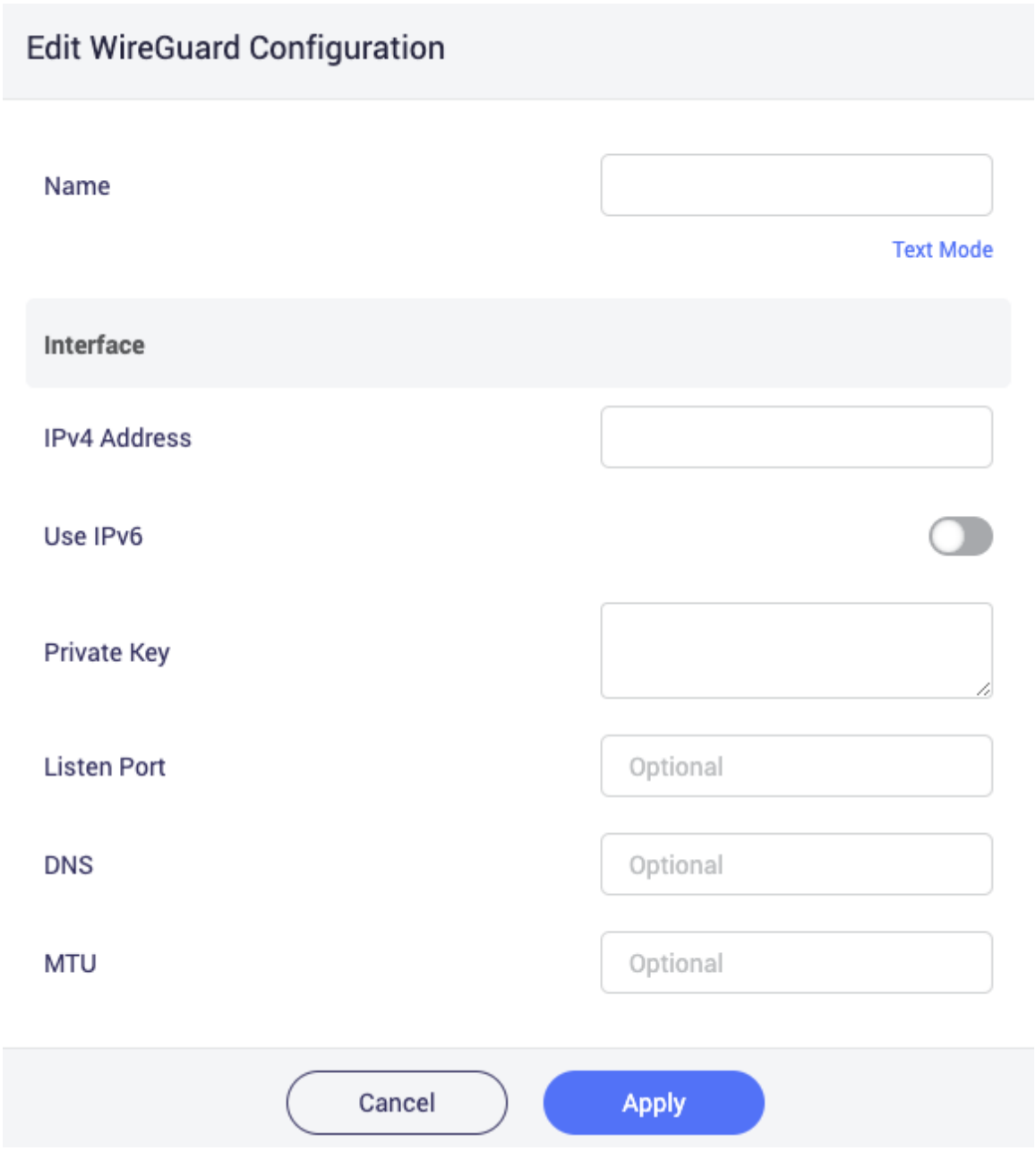


Give a descriptive name and paste the configuration, click **Apply** to continue.

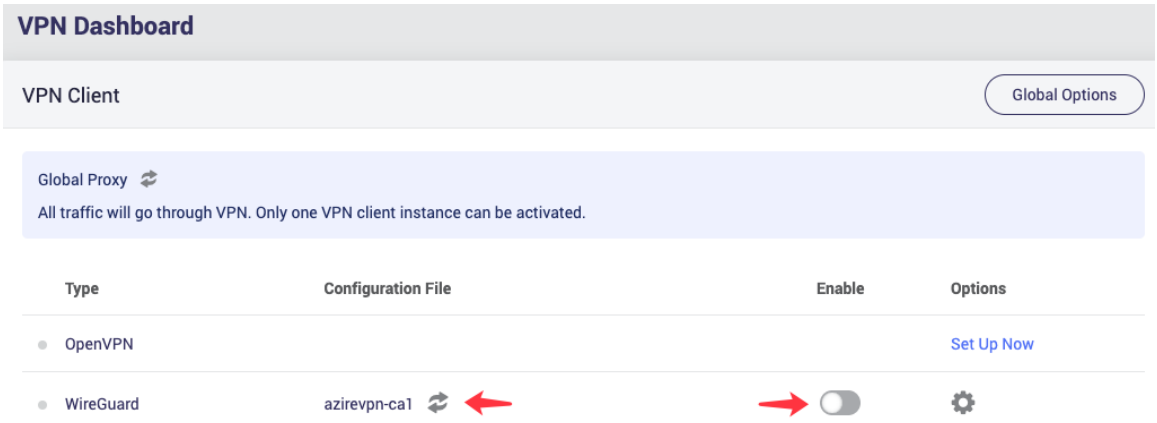


Or you can add configuration by fill in each item, click **Item Mode**.


Edit WireGuard Configuration
Name
Item Mode
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 WireGaurd 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.

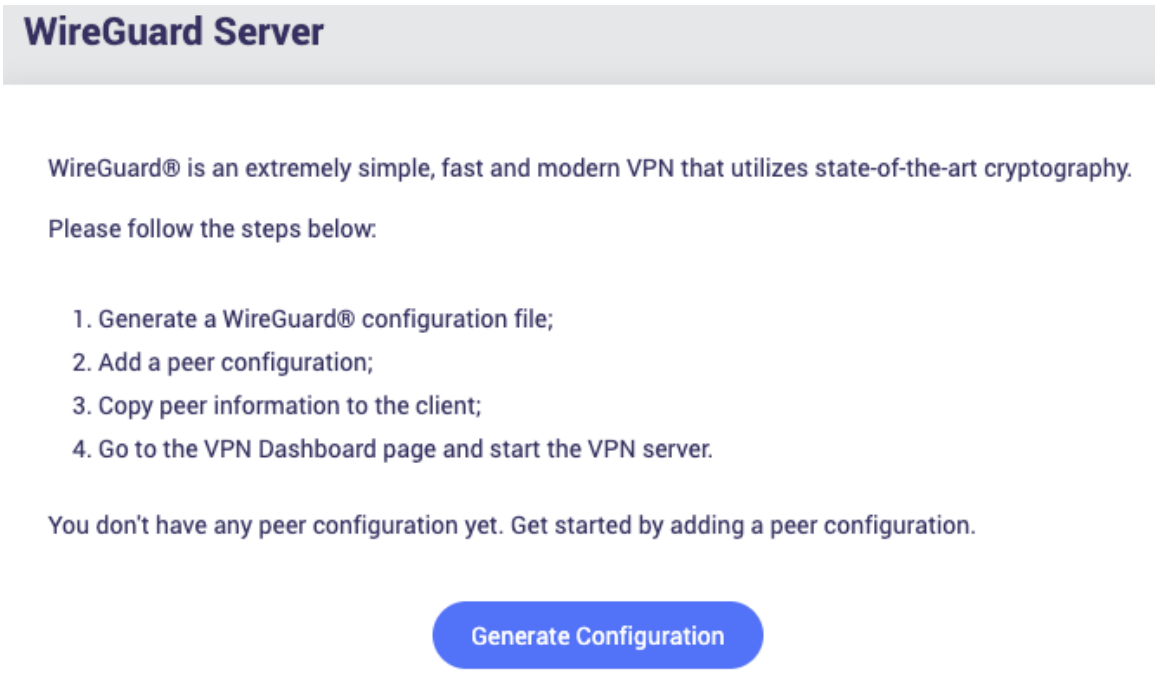
Network Topology

- 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

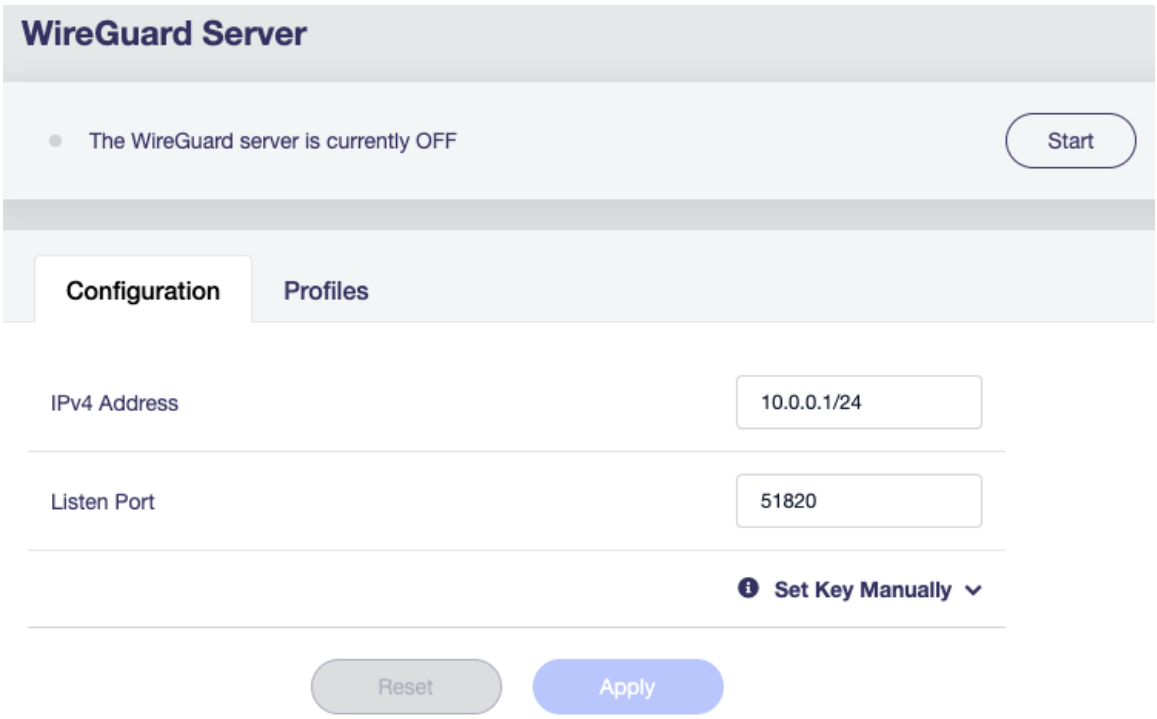
Access to web Admin Panel, on the left side -> VPN -> WireGuard Server.

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

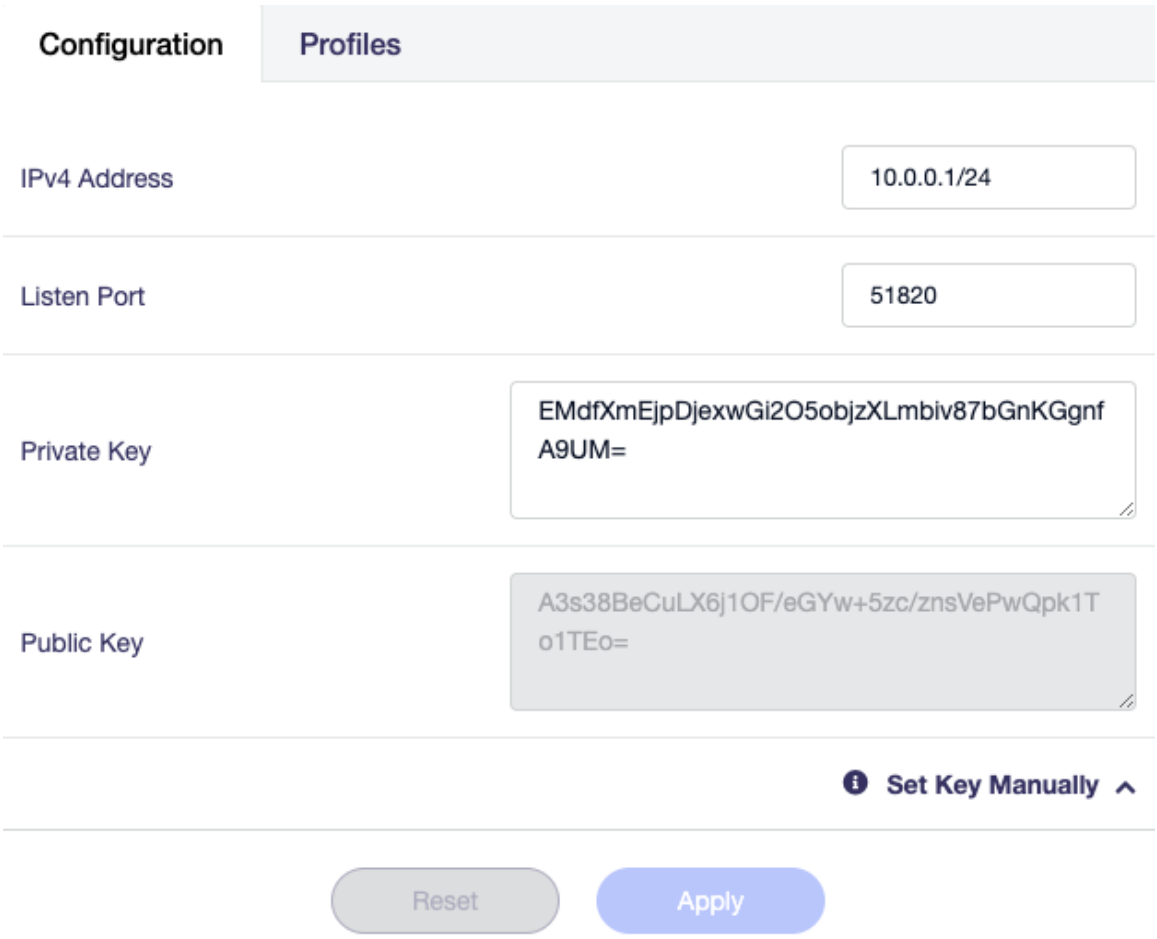


2. Apply the configuration

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

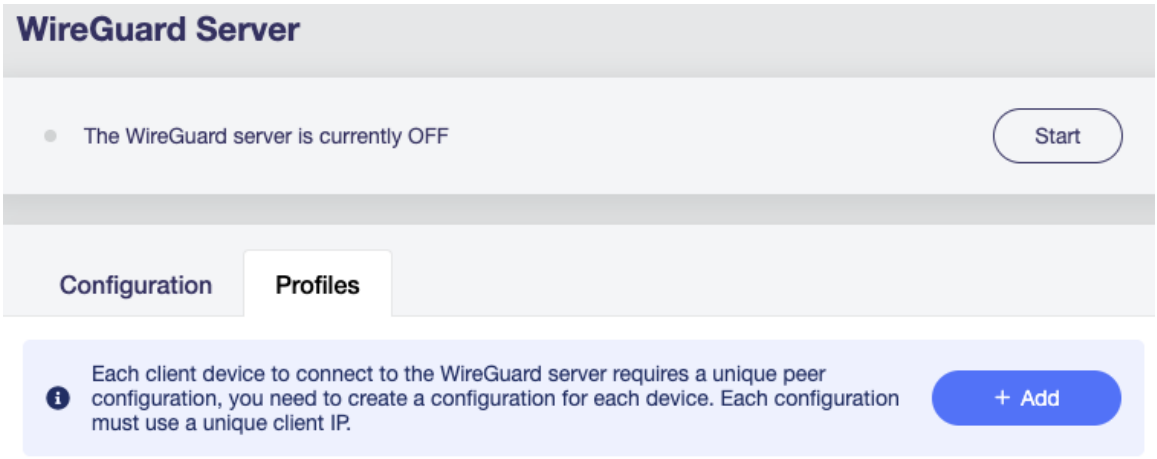


   For **Set Key Manually**.

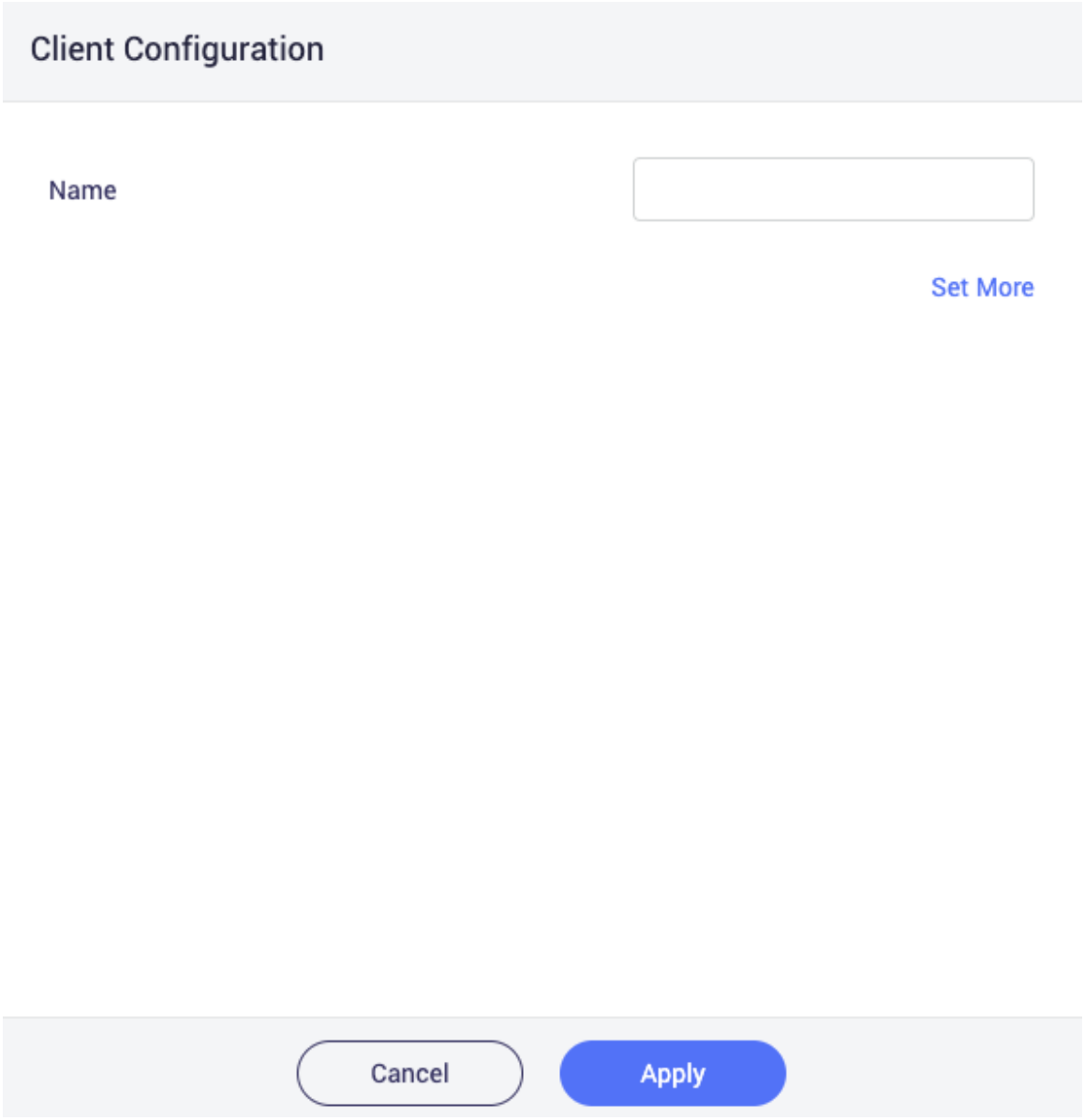


3. Add a profile

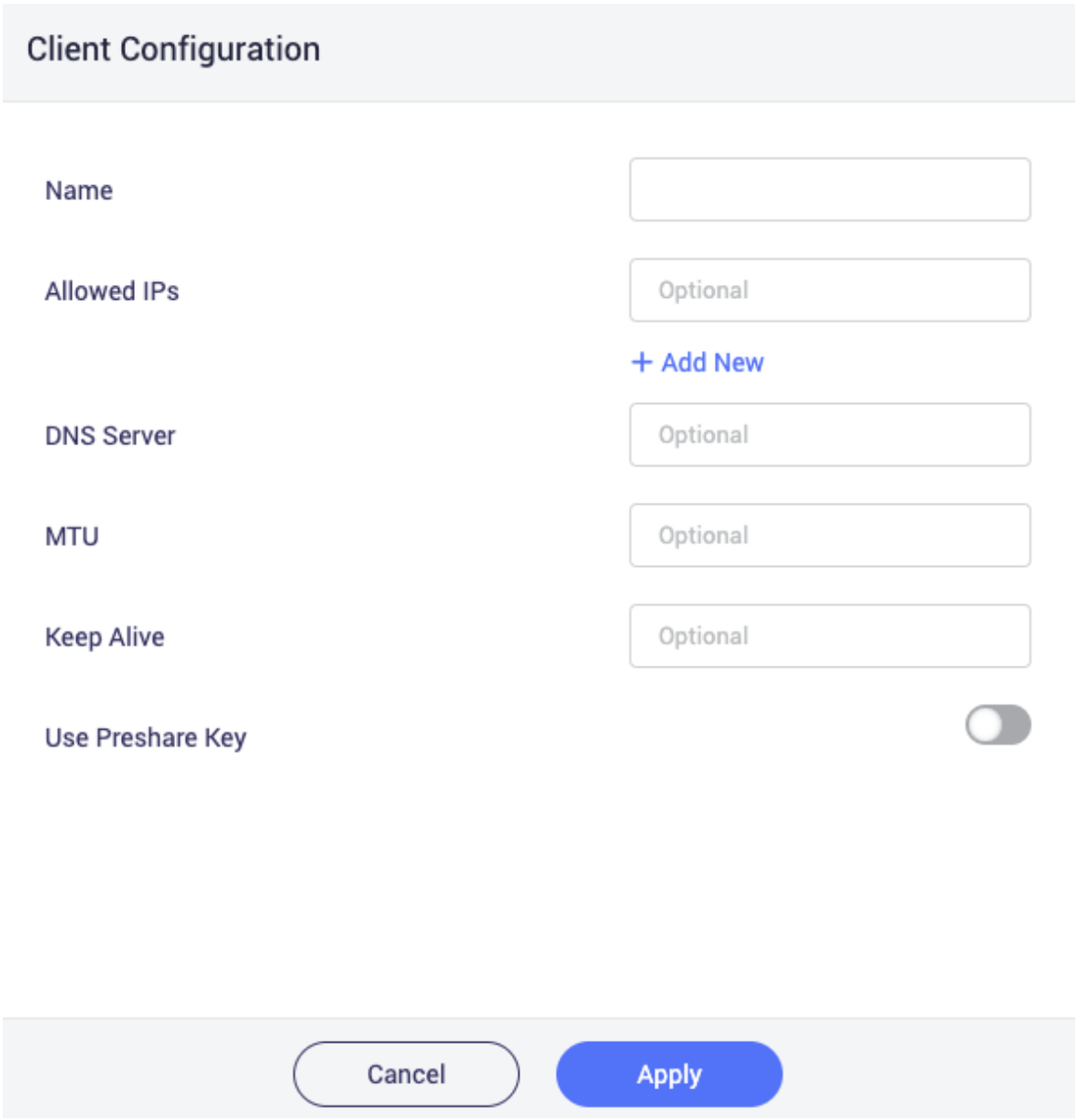
   Switch to **Profiles** tab, generate a profile for your device by click the **Add** button.



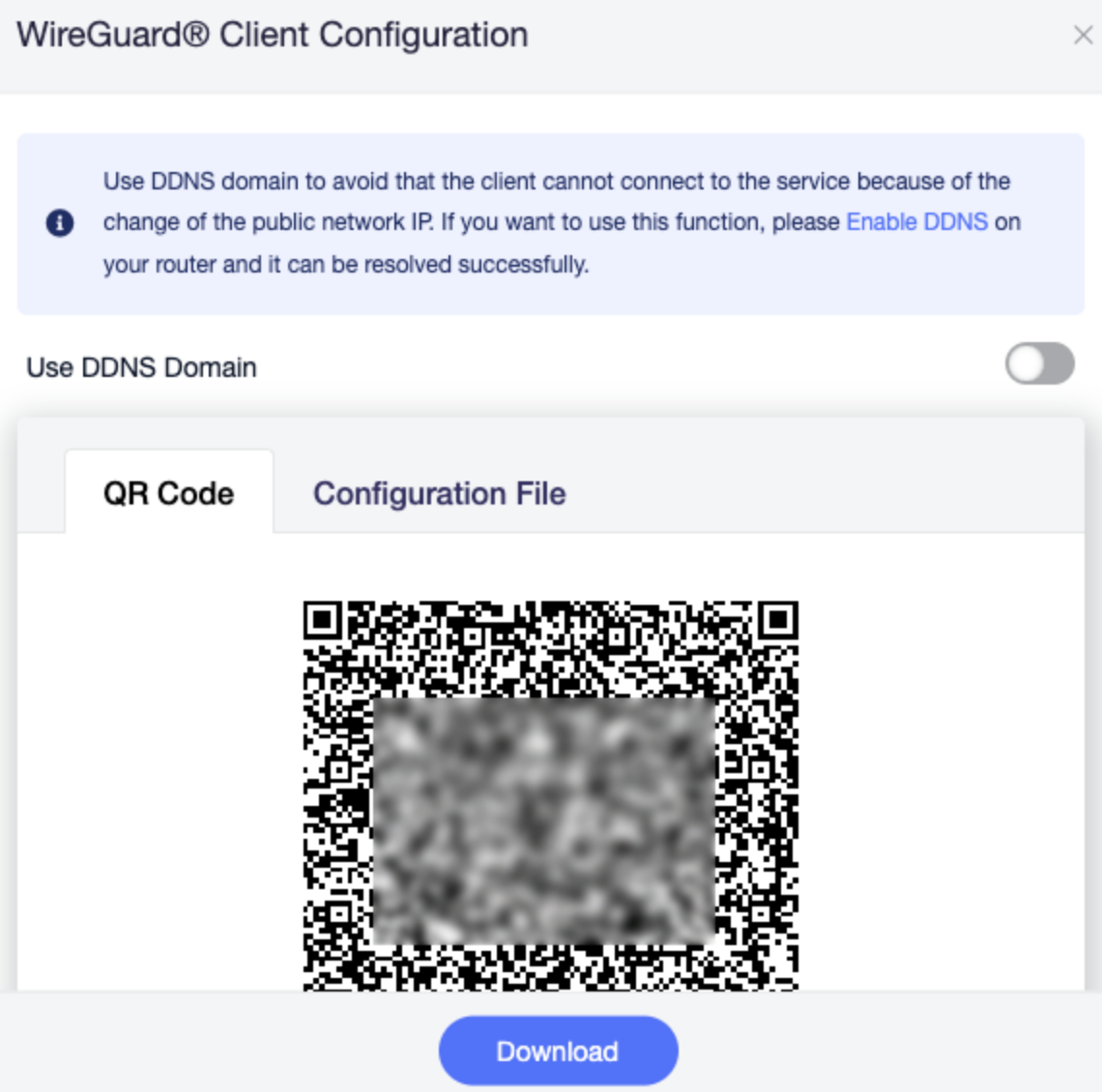
   Enter a descriptive name.



Set More is for advanced settings.



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

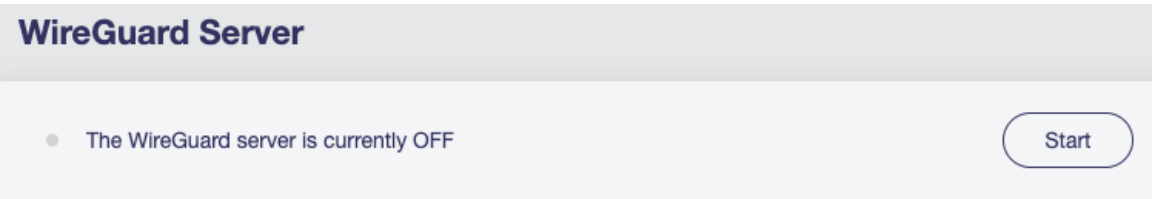


If your network's public IP changes from time to time, you can enable DDNS, then using DDNS domain in the configuration.

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.



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

8. 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.

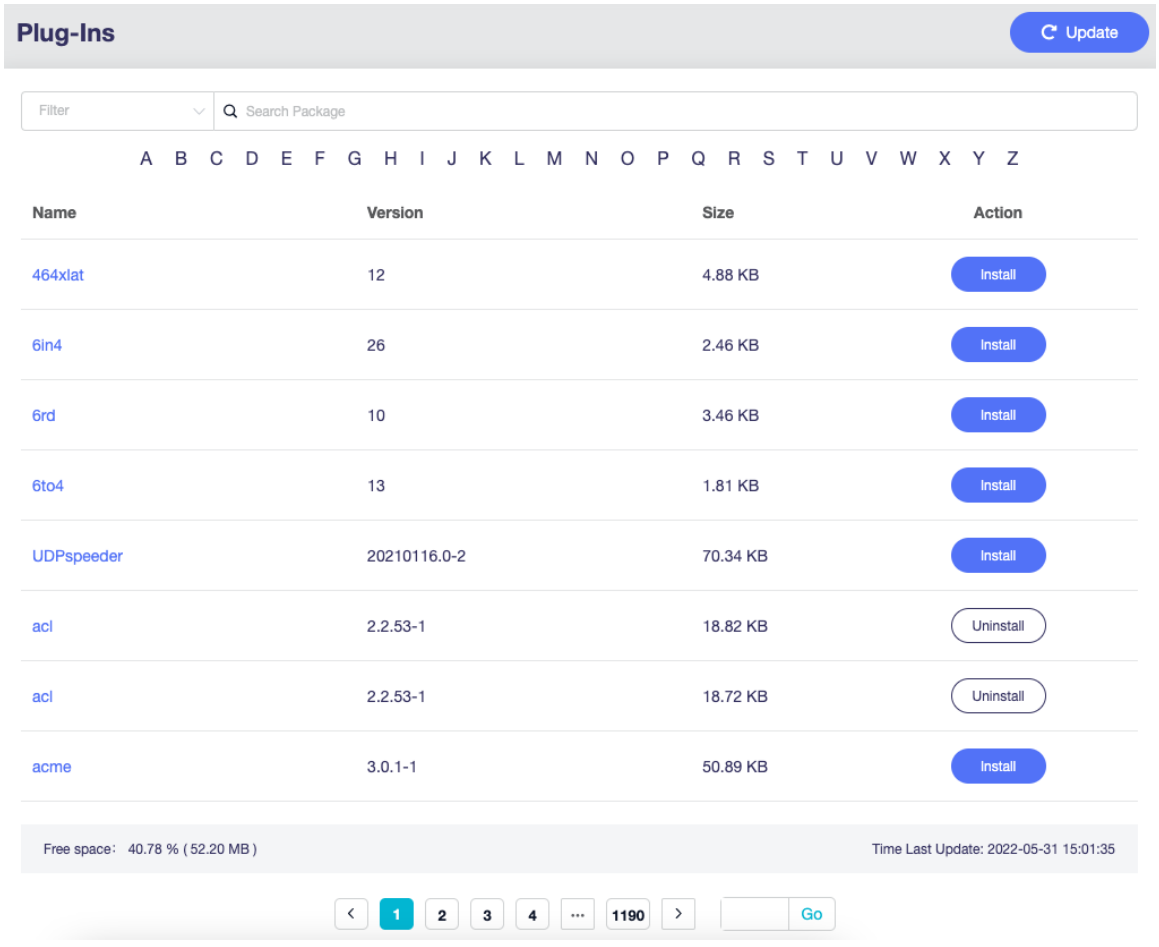
8.1 Plug-ins

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.

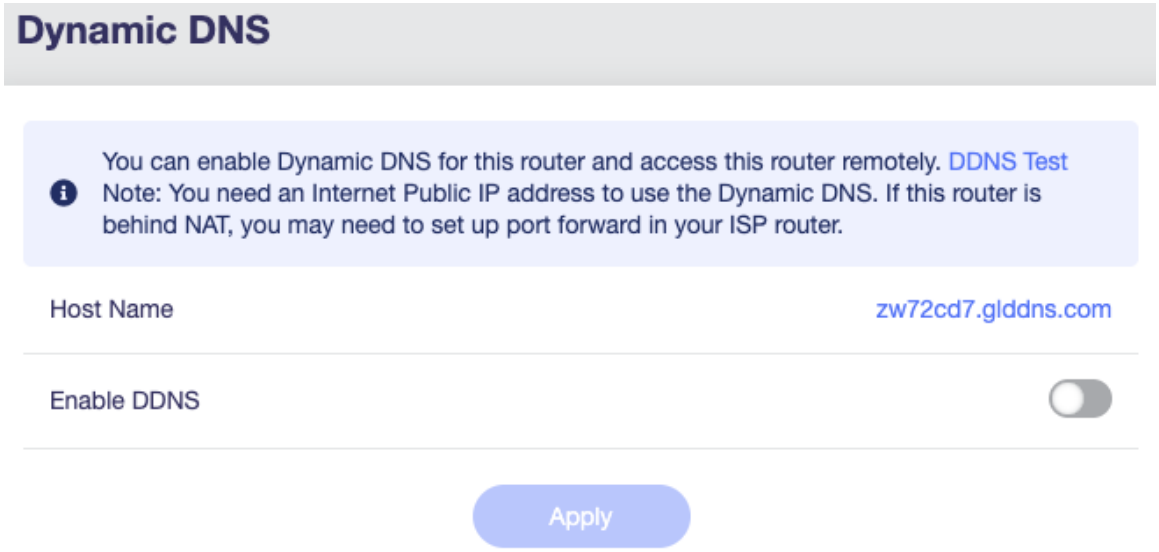
The following figure shows the Plug-ins page of GL-AXT1800.



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.

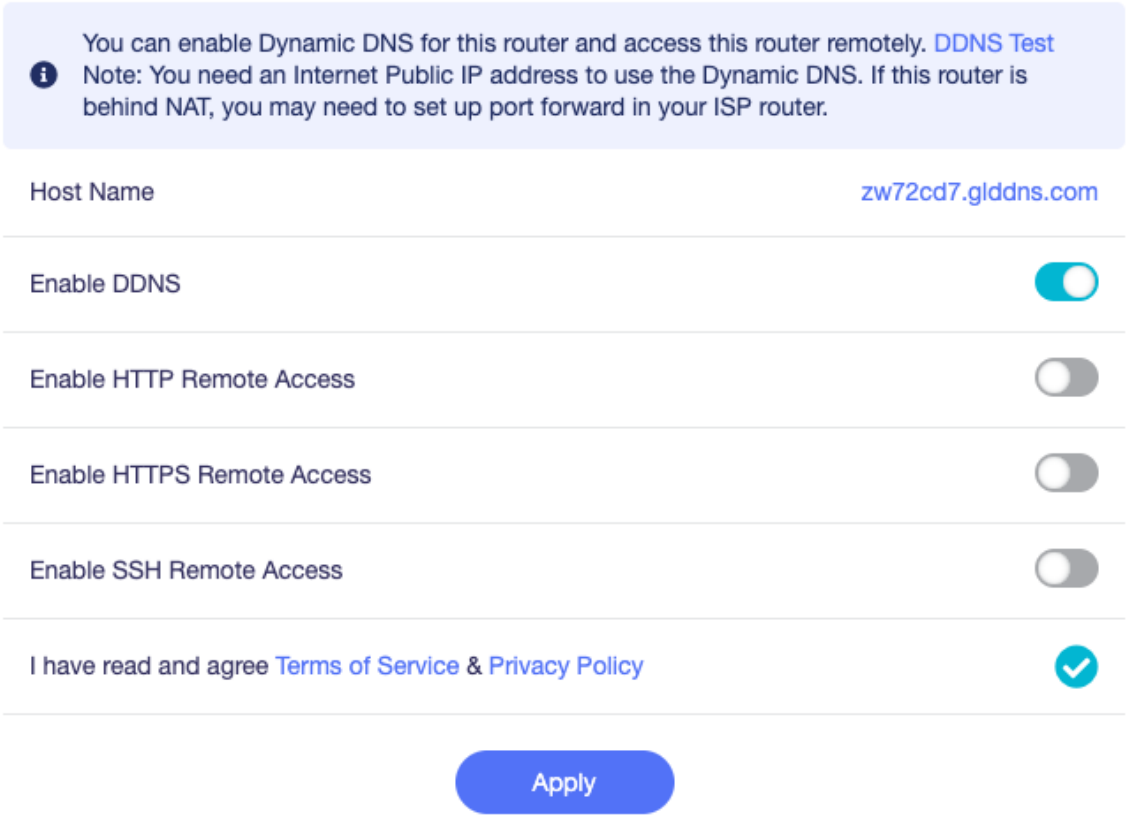
On the left side of web Admin Panel -> APPLICATIONS -> Dynamic DNS



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.

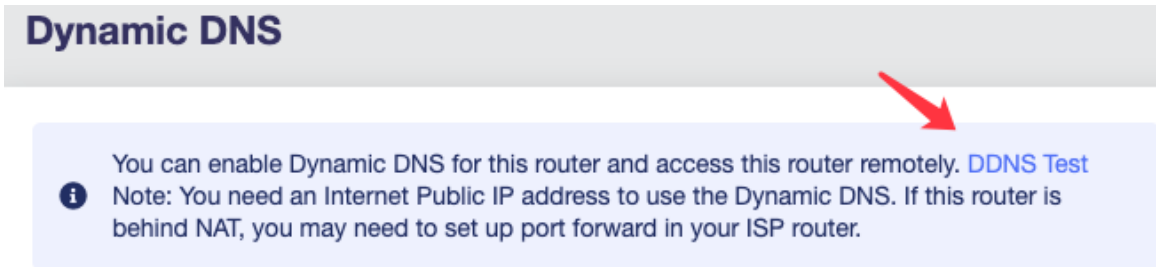
DDNS update frequency is once every 10 minutes.



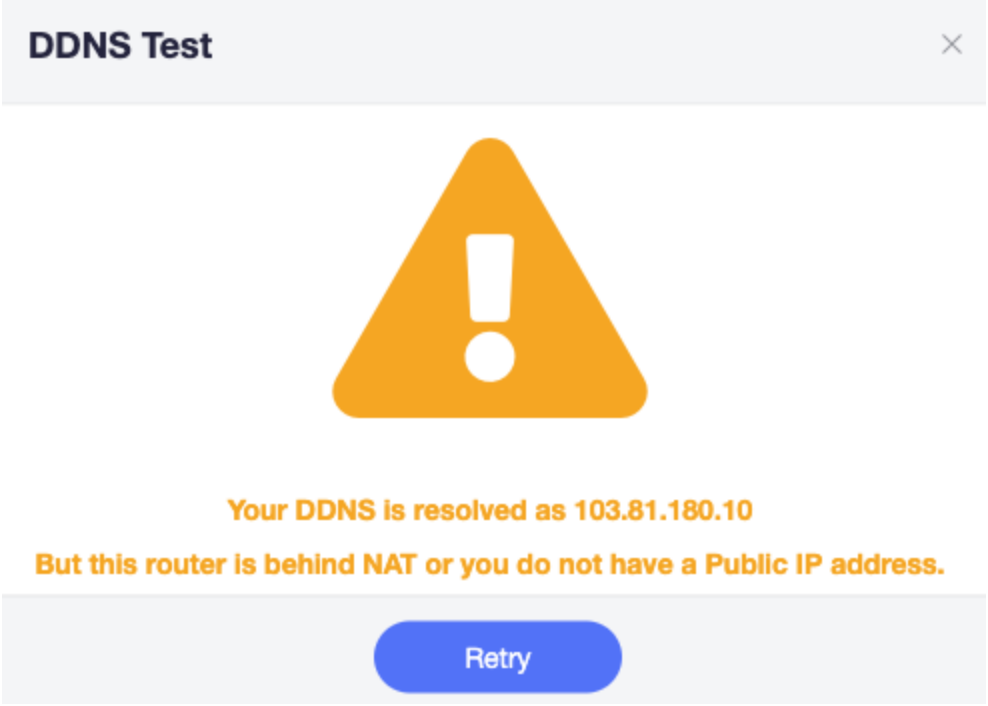
Check if DDNS is in effect

- Using the DDNS Test tool

Click the **DDNS Test**



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 maped to the final exit IP of the router for Internet access.

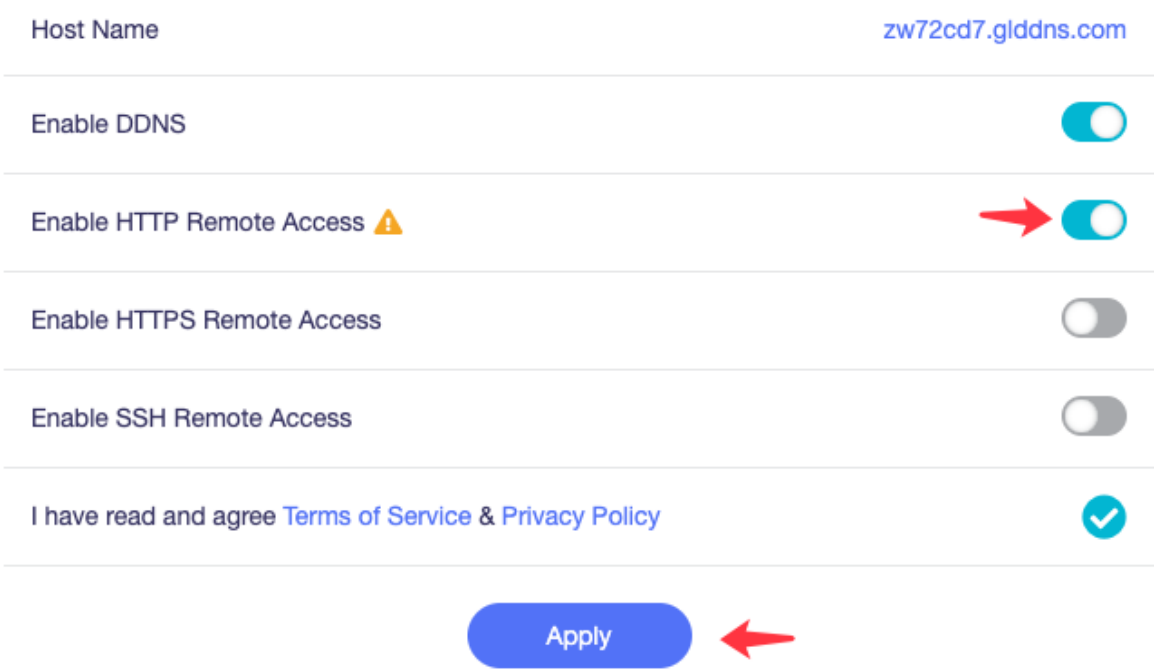


Or check it manually

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**.



Follow the steps above, to enable HTTP Remote Access.

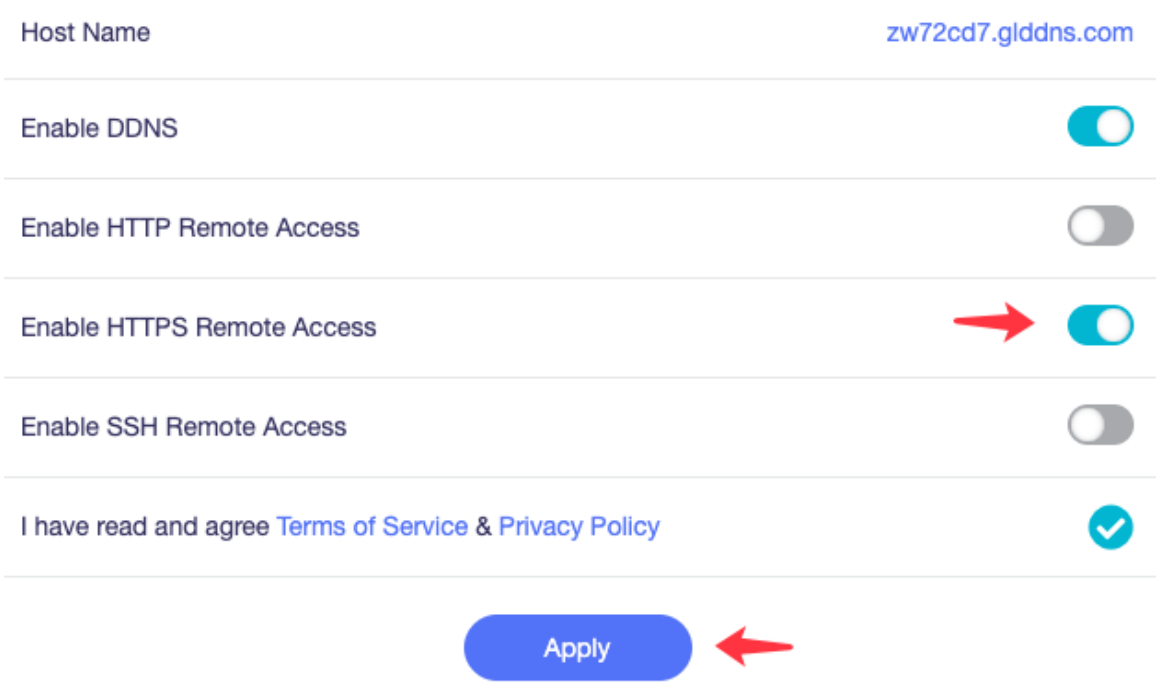
HTTP is not encrypted, use at your own risk.

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.

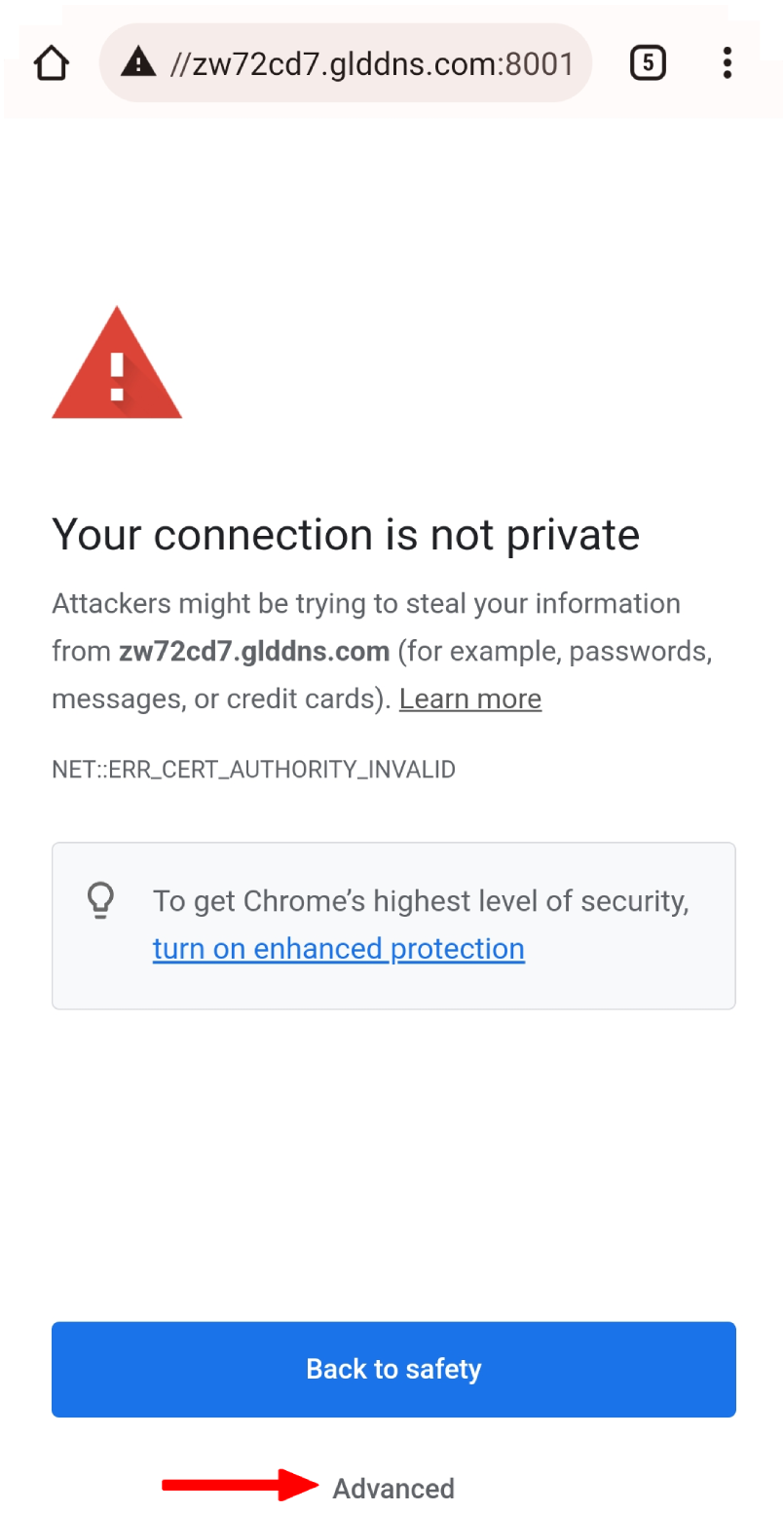
If your router is behind NAT, you may need to set up port forwarding in higher level router. It use port **443**.



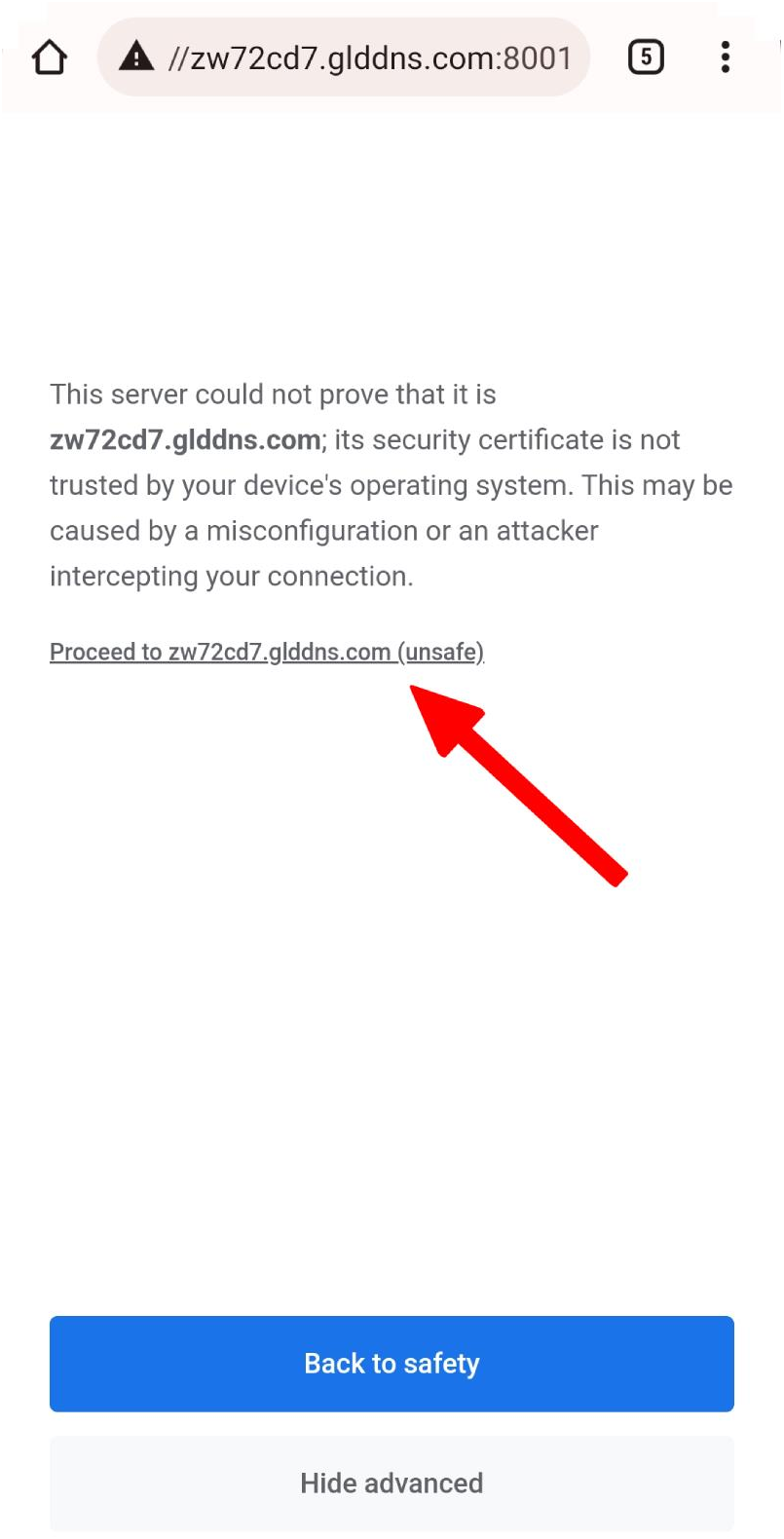
After you enable HTTPS Remote Access, you can access Admin Panel anywhere by your DDNS Host Name of **https**, e.g. `https://xxxxxxx.glddns.com`. If you use port forwarding, you should be access like `https://xxxxxxx.glddns.com:YourExternalPort`.

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

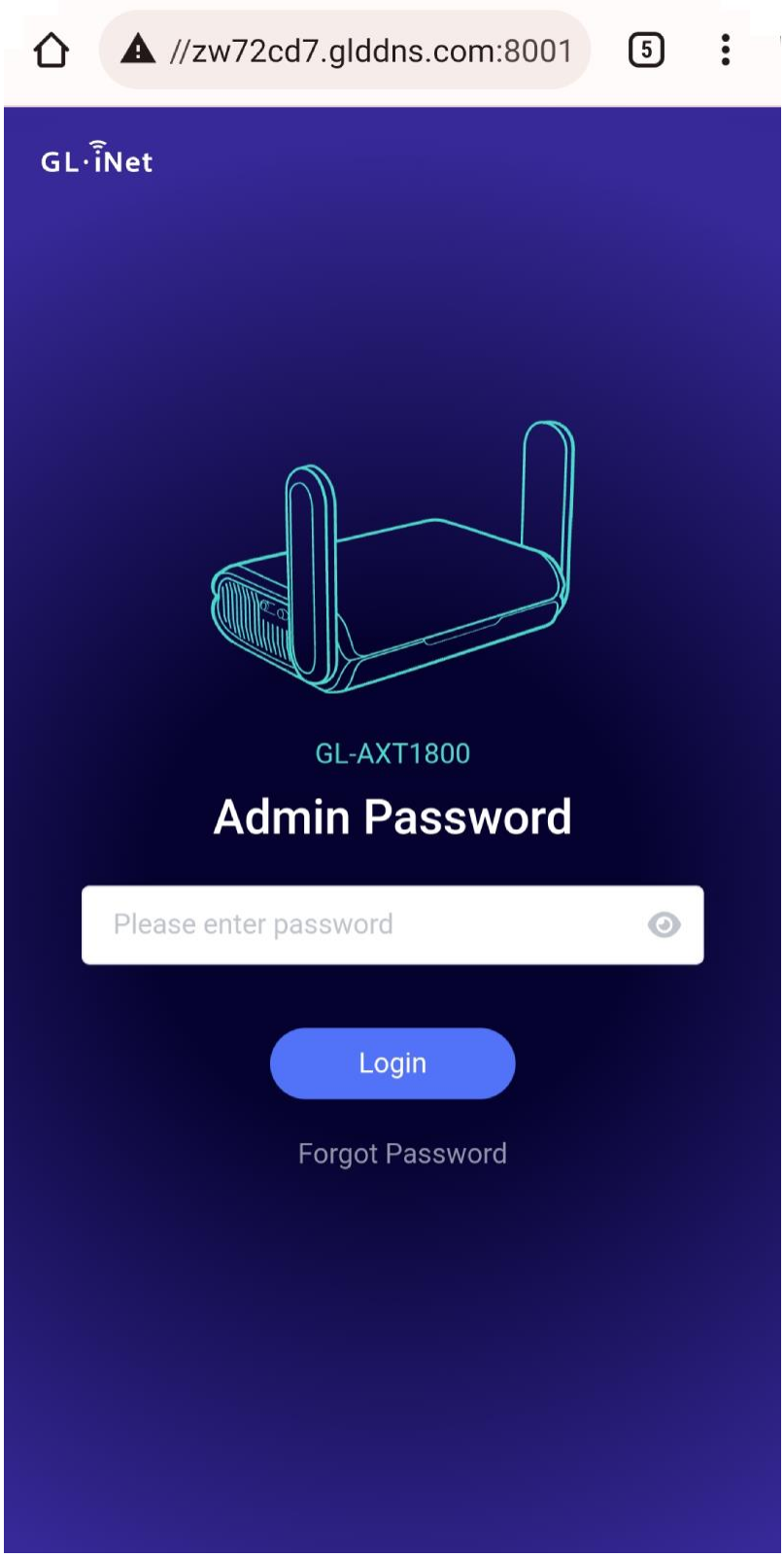
Open chrome and type the URL in the address bar, I'll use `https://zw72cd7.glddns.com:8001` as an example. Click **Advanced** at the bottom to continue.



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



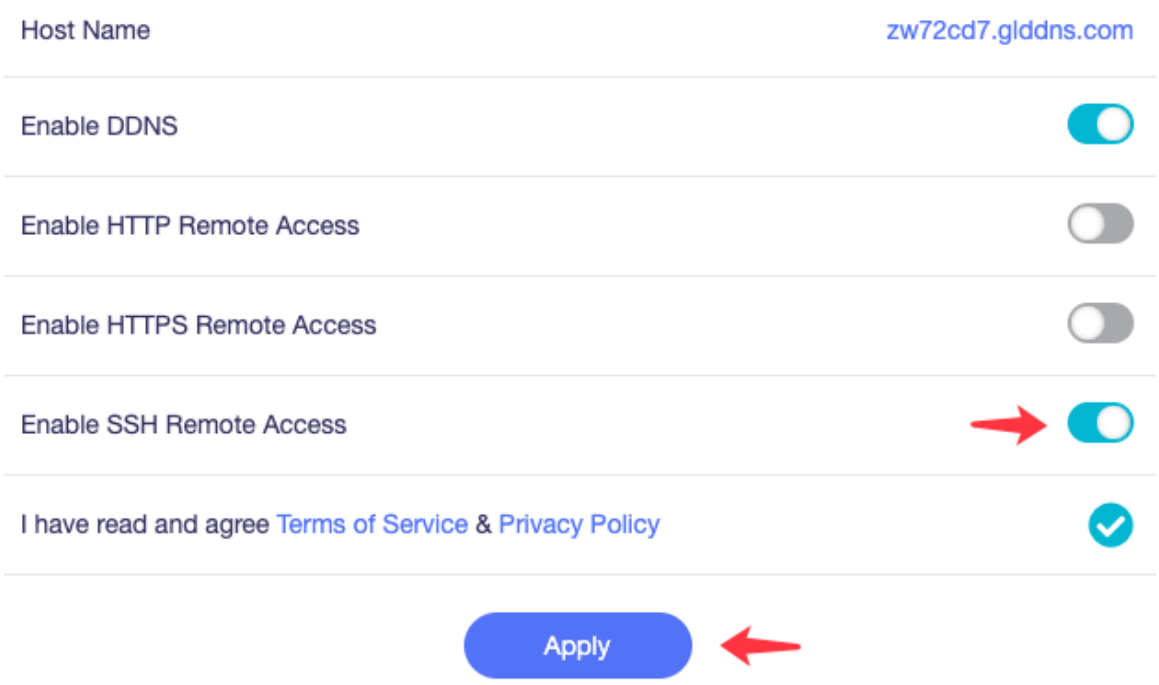
Then, it will access the web Admin Panel.


//zw72cd7.glddns.com:8001
GL·iNet
GL-AXT1800
Admin Password
Please enter password
Login
Forgot Password

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**.



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

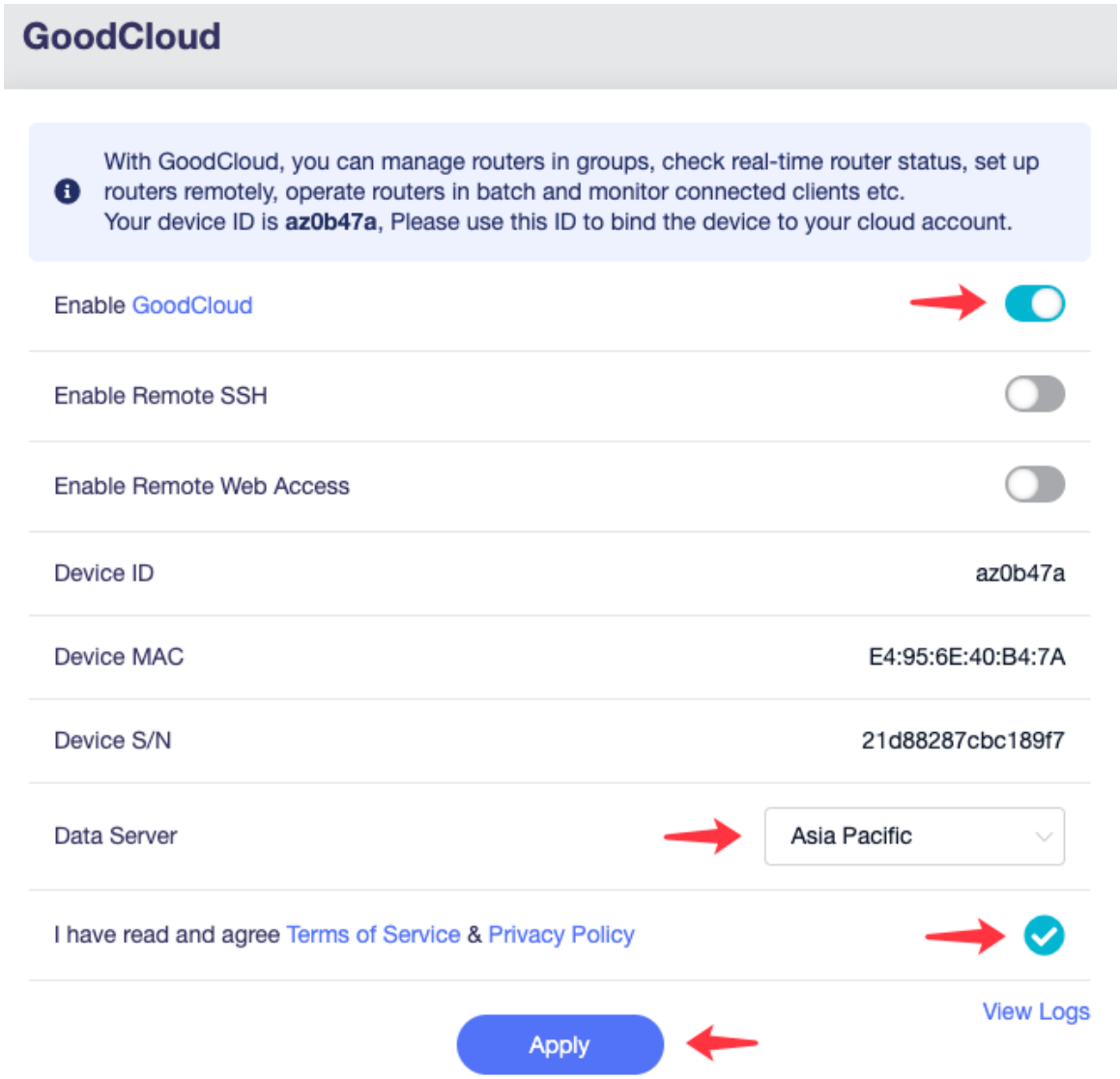
        - Set up config templates and configure routers in batch
        - Reboot or upgrade routers in batch
    - Manage routers in groups
        - Divide devices in different groups
        - Manage devices in one page
    - Site to Site
        - Virtual Office: extend your office network to other offices
        - 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.



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).

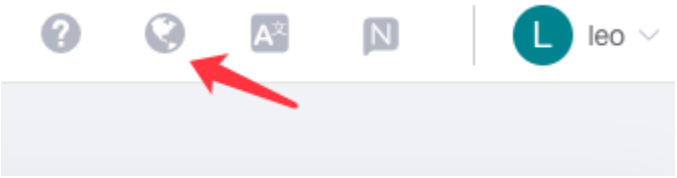
Sign up GoodCloud account

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).

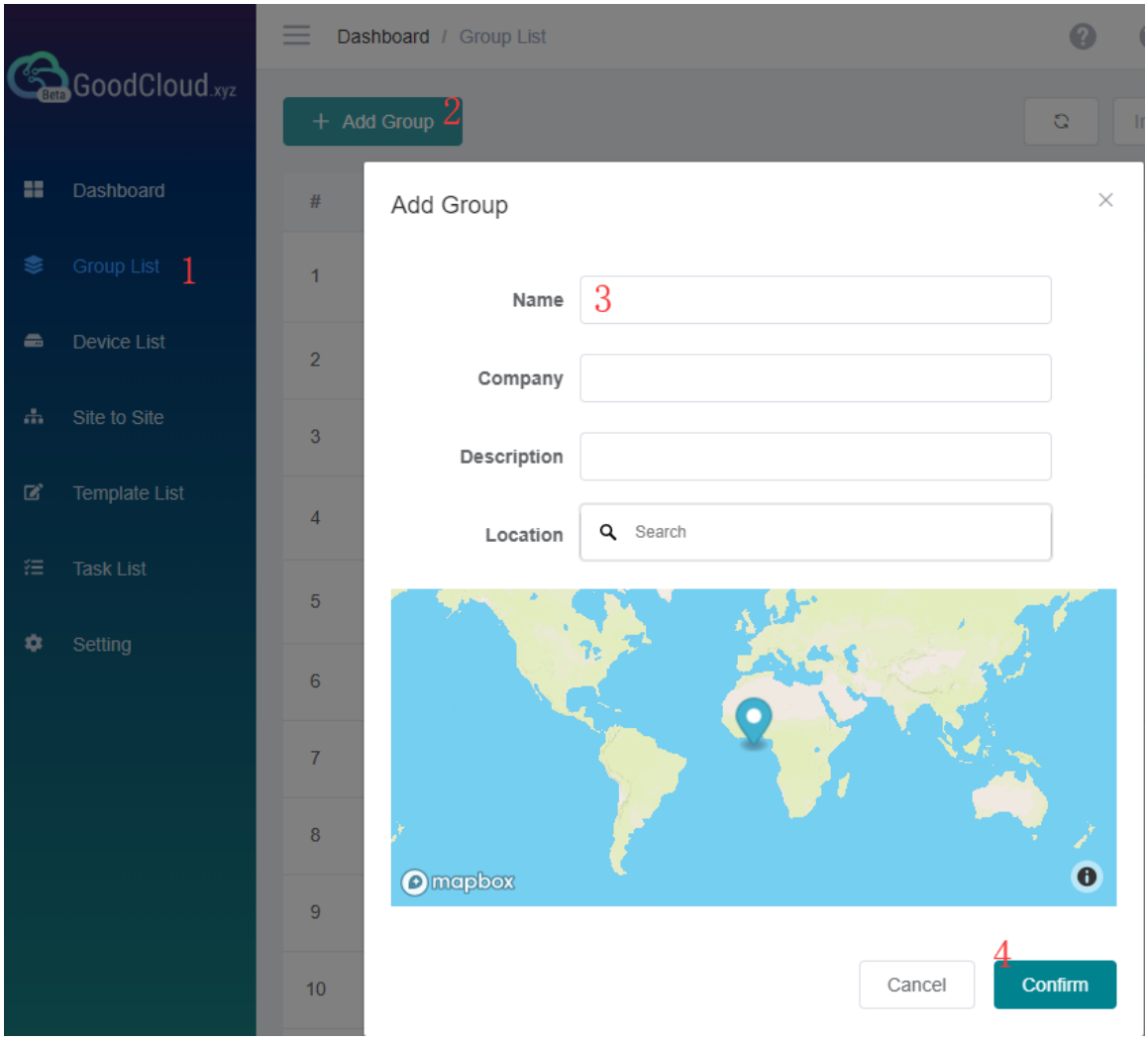
You can change the region on the top right corner at anytime.



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.

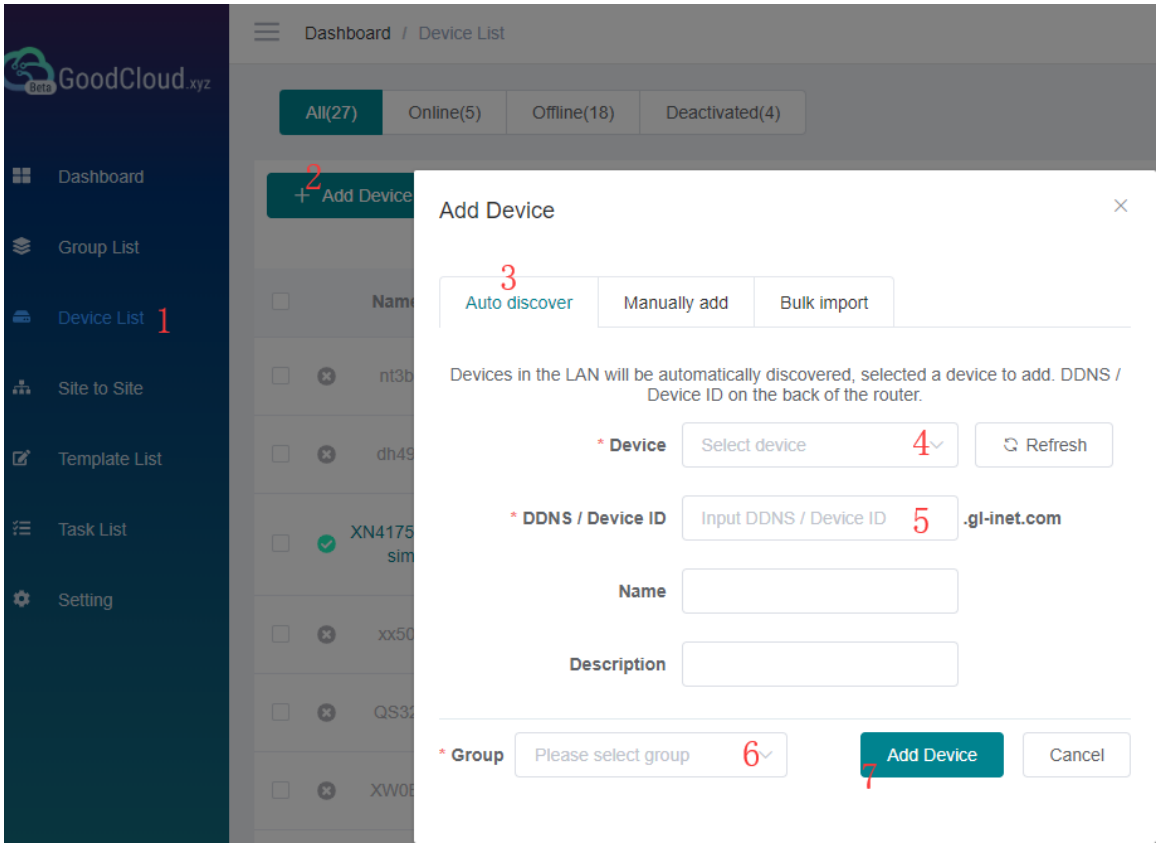
Add device

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.

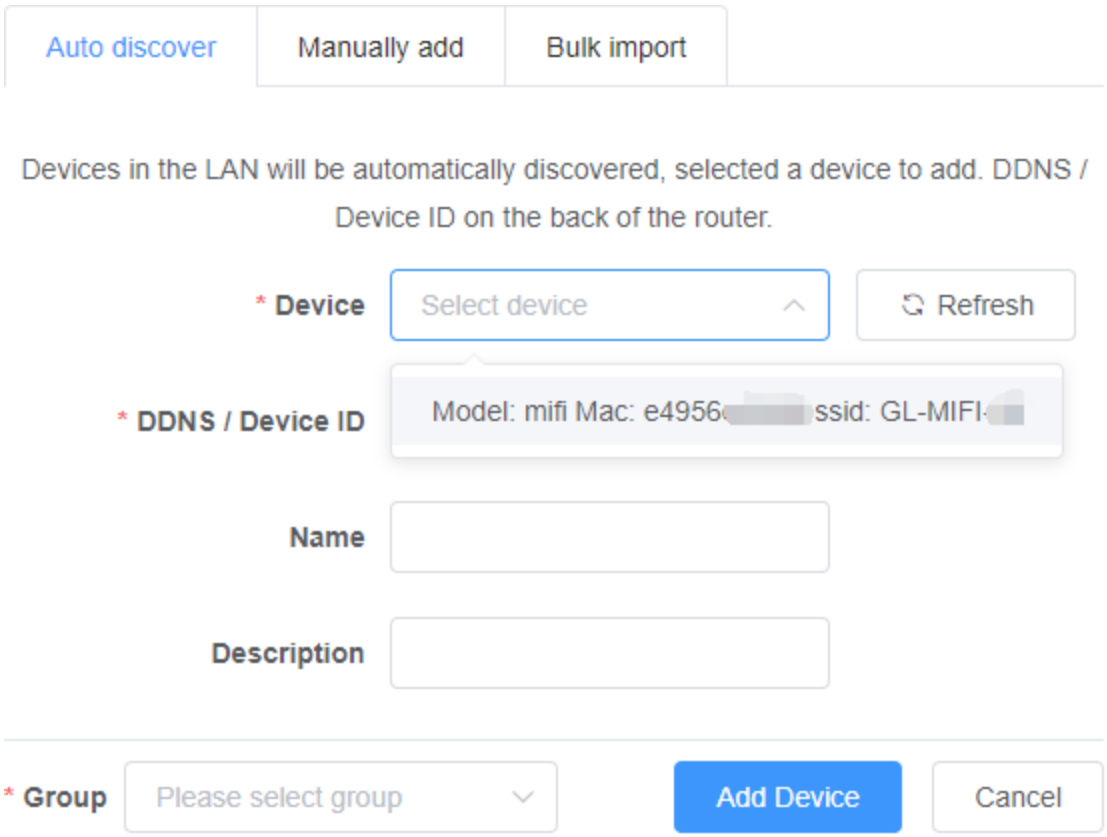


Check out here to find the Device ID.

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.

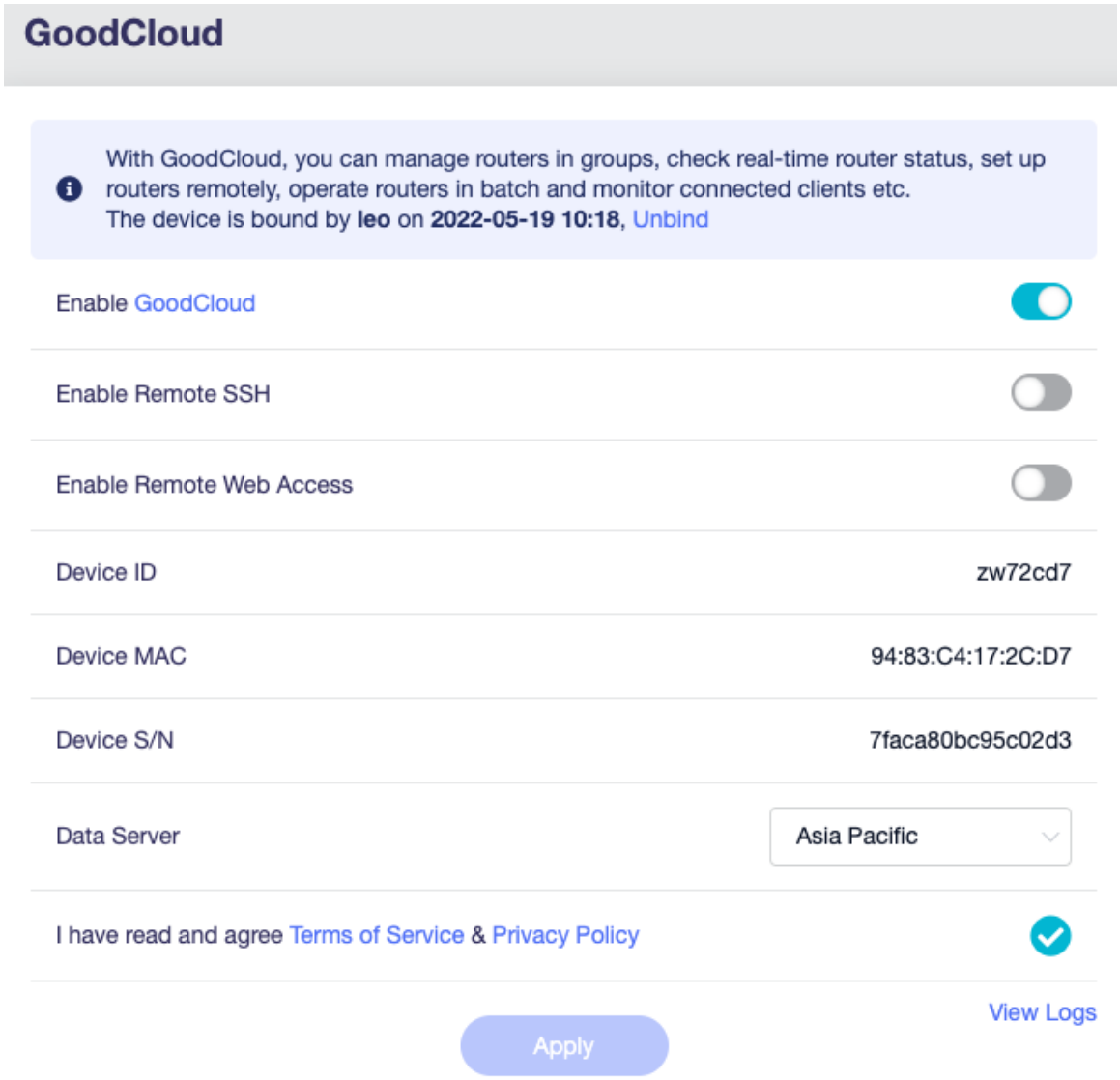


Manually add Bulk import

Bound info on router web Admin Panel

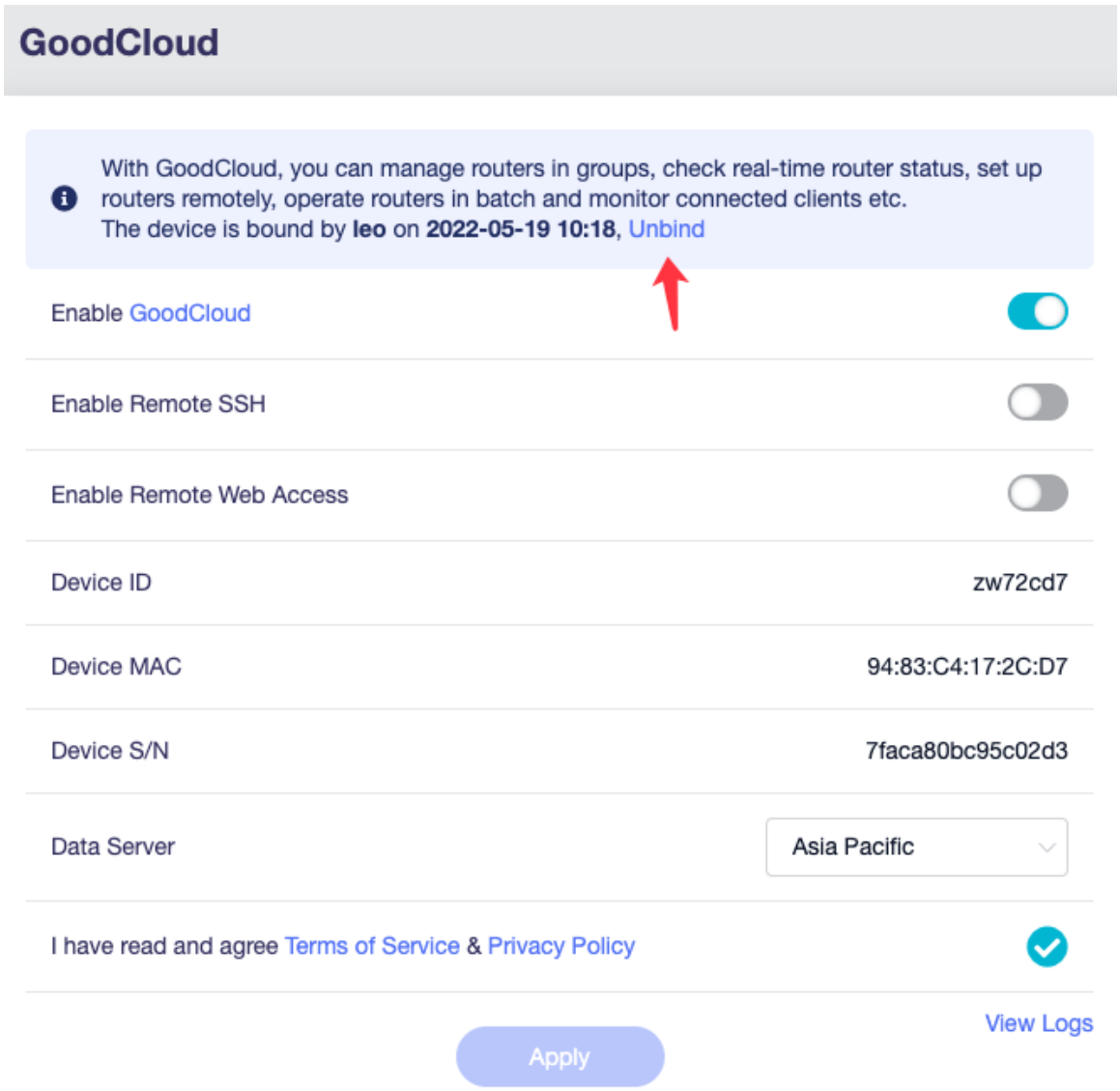
After you seccessfully add router to GoodCloud, go back to router web Admin Panel, on the left side, APPLICATION -> GoodCloud,

refresh this page, It will display the bound GoodCloud username and date.



Unbind router

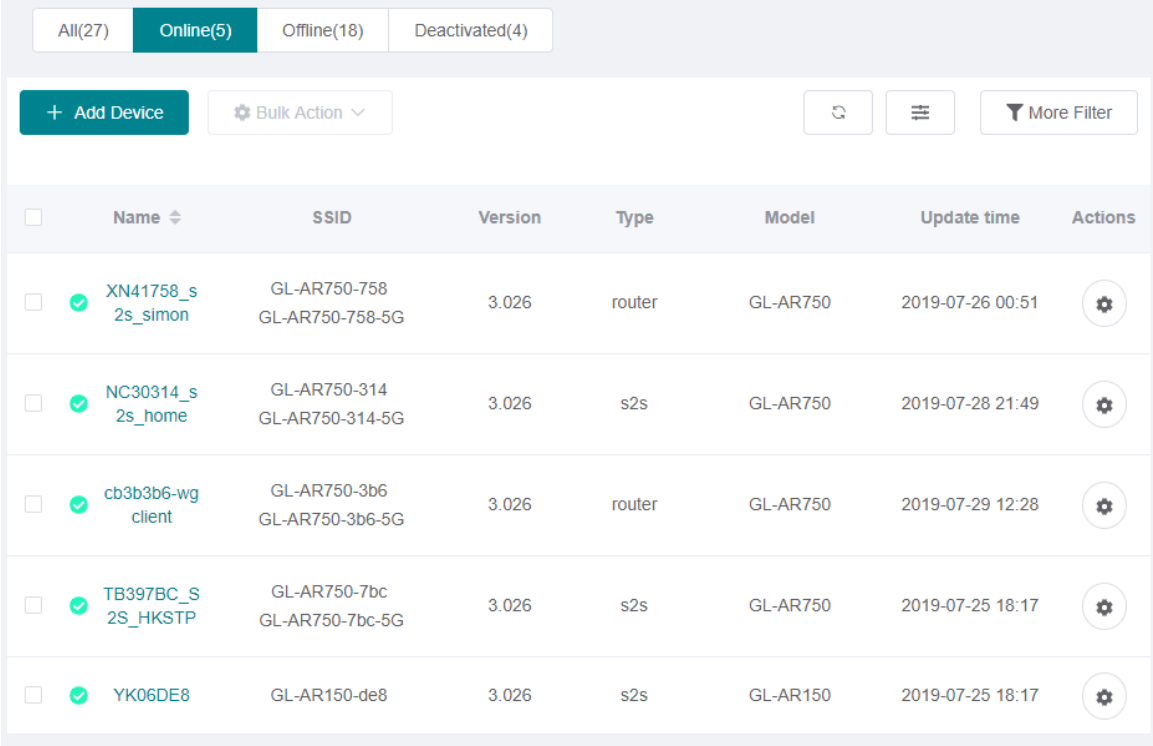
If you want to unbind the router, go to router web Admin Panel, on the left side, APPLICATION -> GoodCloud, click **Unbind** button.



Manage your devices

Devices info and status

Sign in Goodcloud, check at left side -> Device List

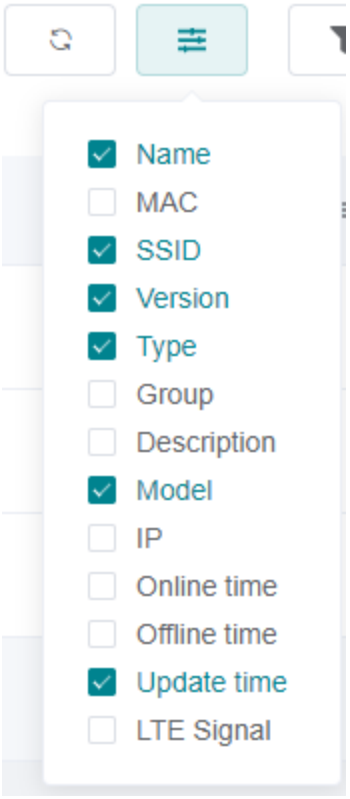


there is icon at the first column of this table,

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.

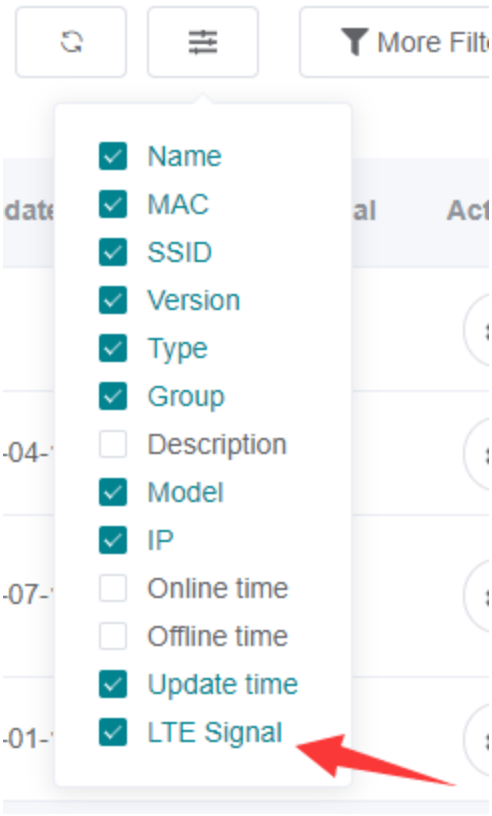
`Update time` is the latest time when device connected or disconnected GoodCloud.

`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

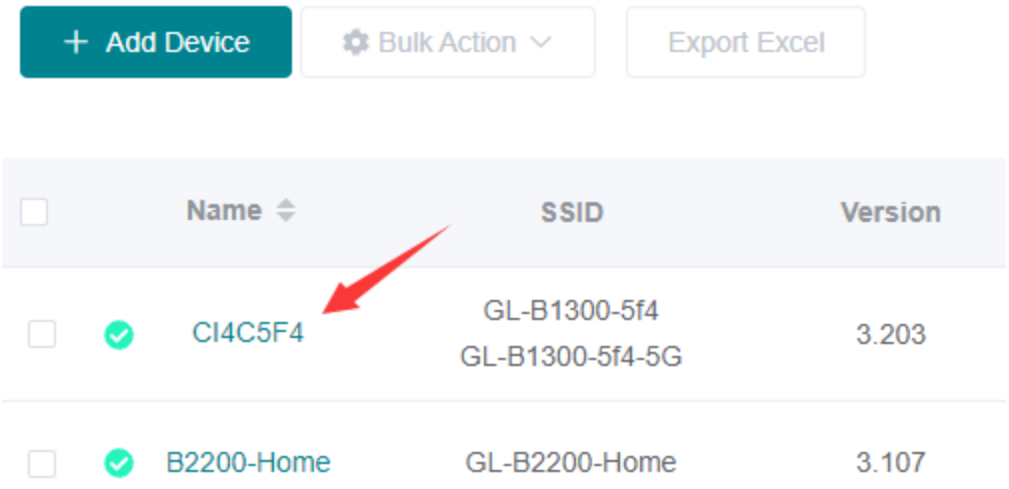
Toggle the column on Device List page.



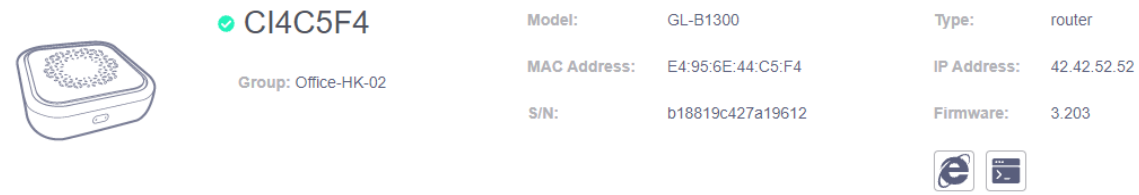
It will show Signal strength, Type, and relavant parameters.

Device detail info

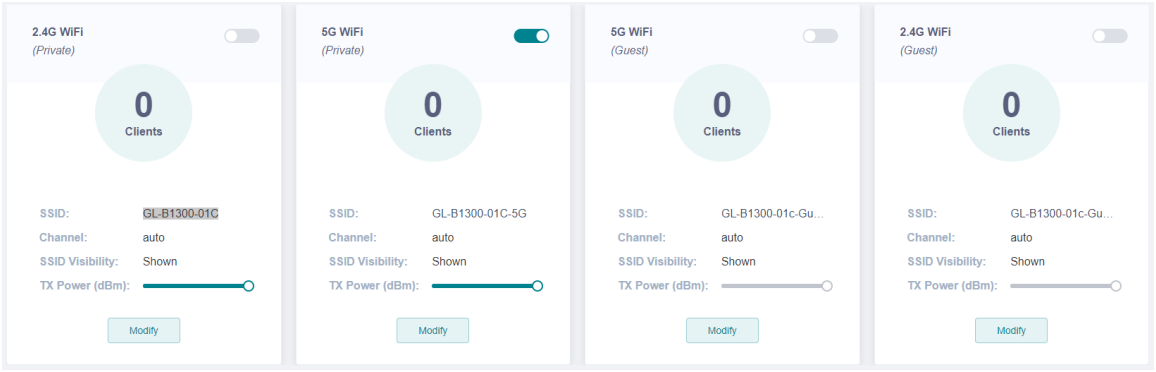
At left side -> Device List, click the name of an online device, it will open a page to manage this device of WiFi, Clients and view router info, memory usage, up time, load average and log.



Device info¶

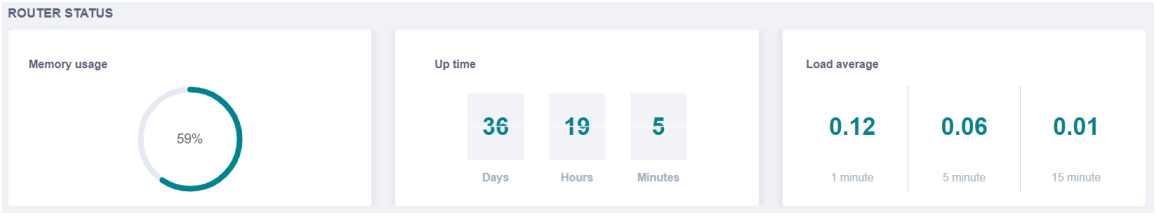


WiFi¶

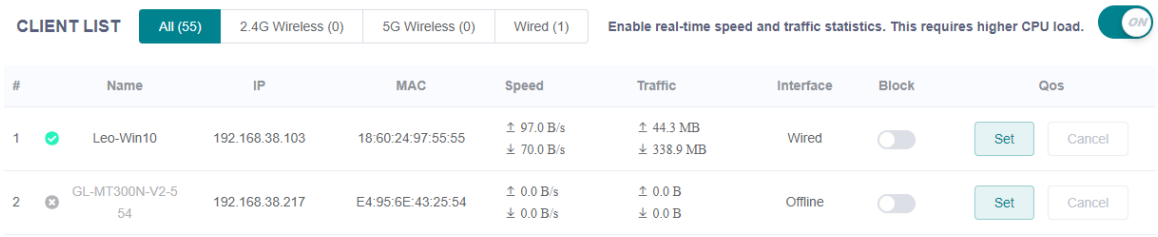


Modify all WiFi settings.

Router status¶

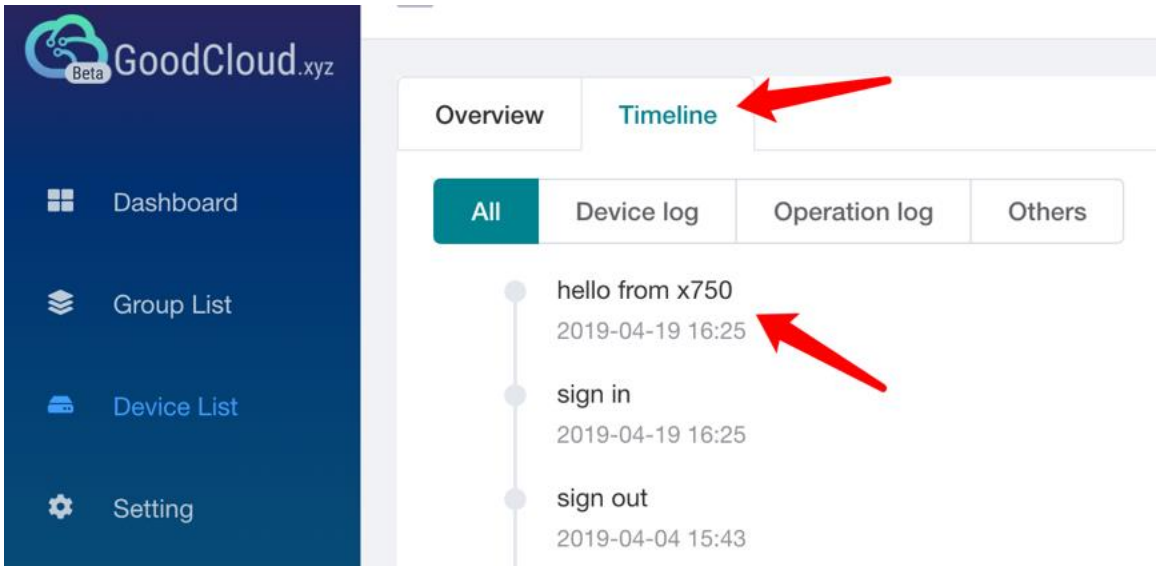


Client list¶



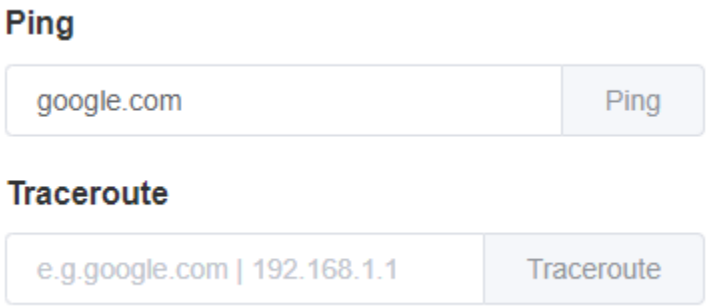
Timeline¶

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



Tools¶

There are two tools, `Ping` and `Traceroute`.

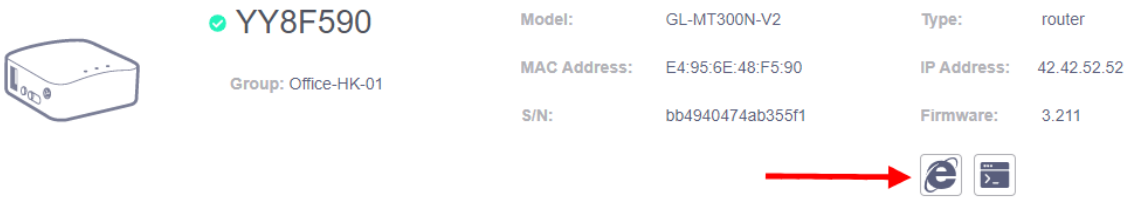


Remote access web Admin Panel

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.

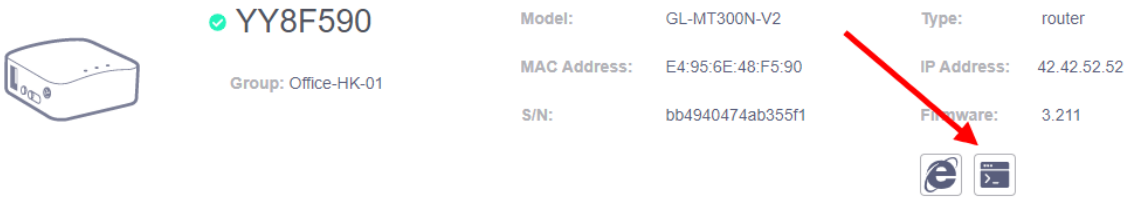


Remote access router's terminal

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.

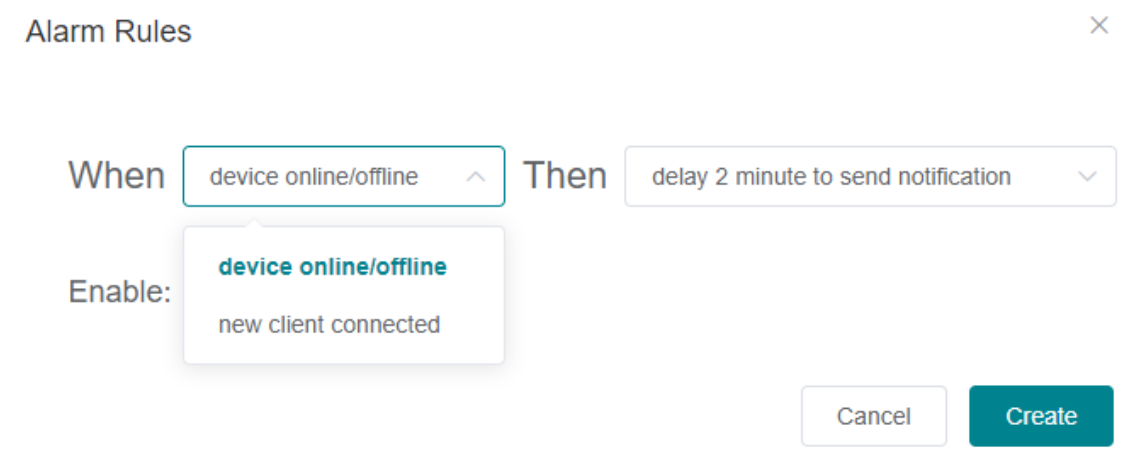
If this feature not work, please try the incognito mode of browser.



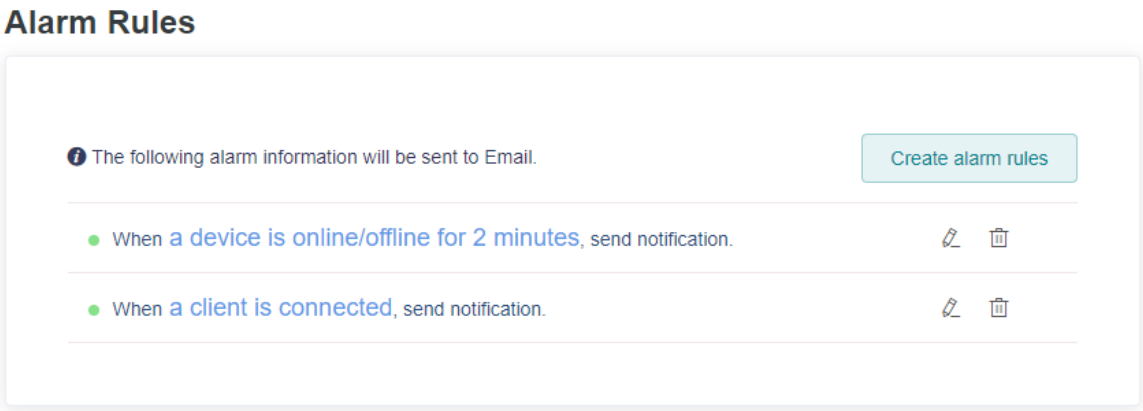
Set email alarm

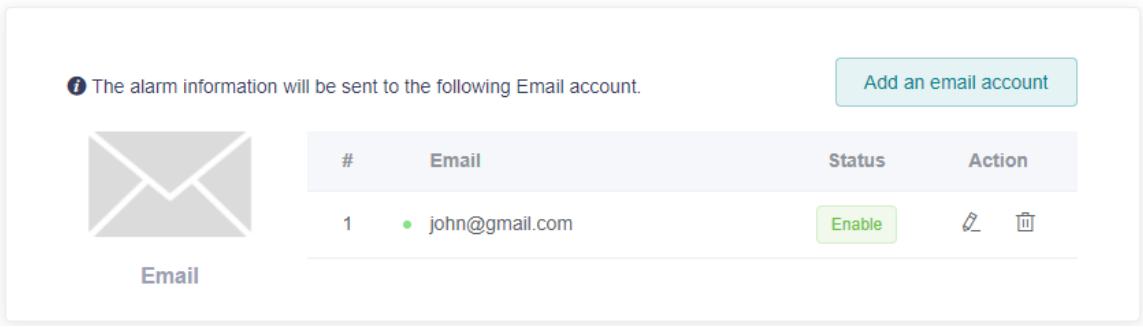
You can set email alarm when a device is online, offline, and new client connected.

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



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.

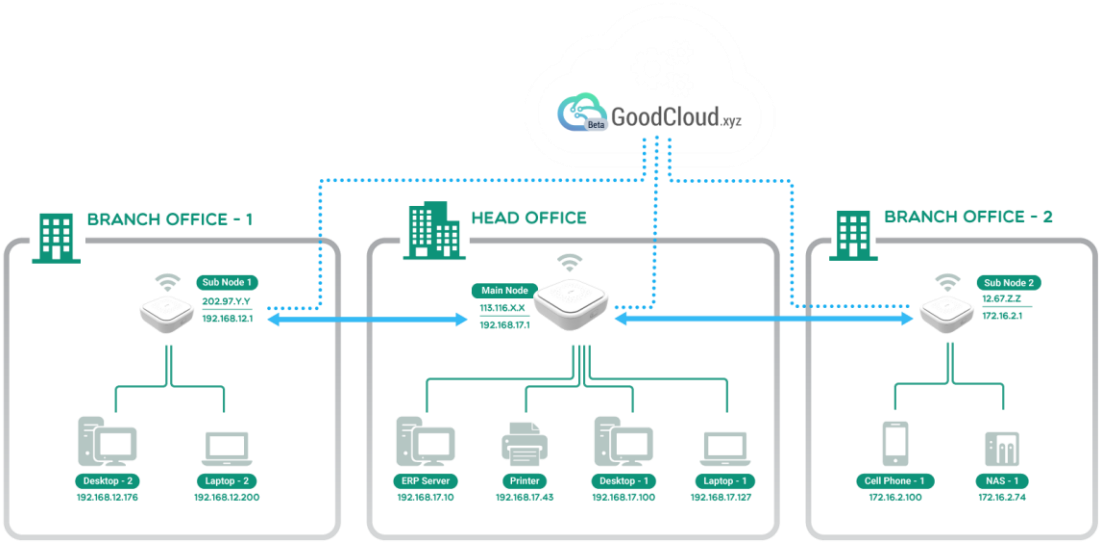




Site to Site

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.

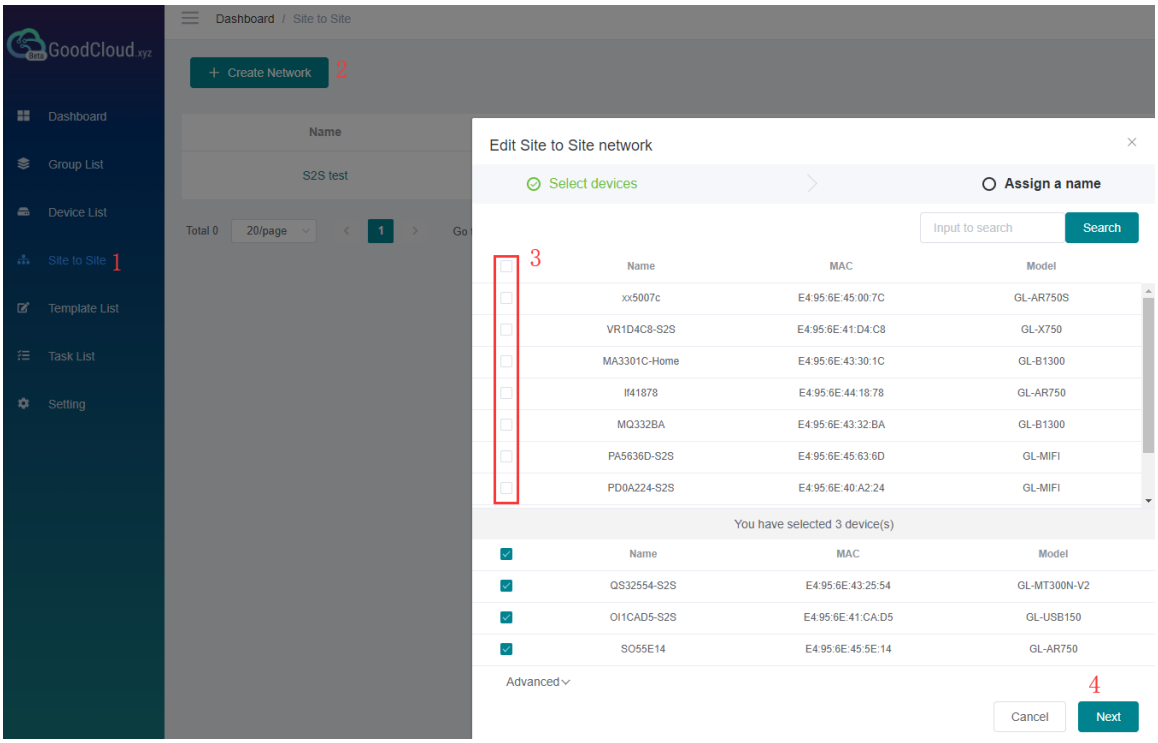
Conditions

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

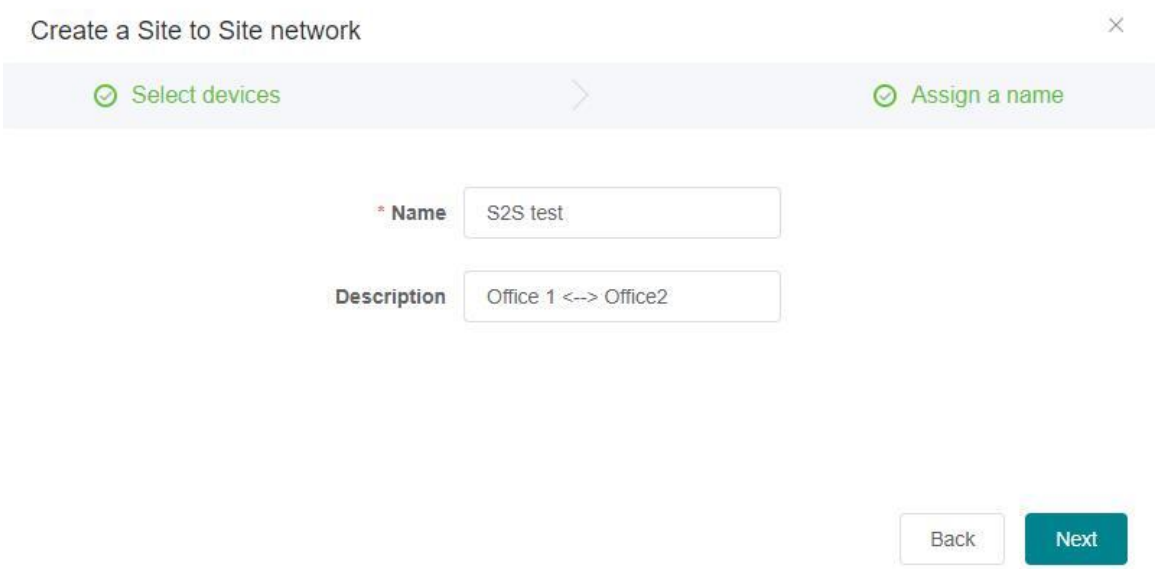
1. Bind your routers to GoodCloud. (how?)
2. Follow the steps below to create a Site to Site network.



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

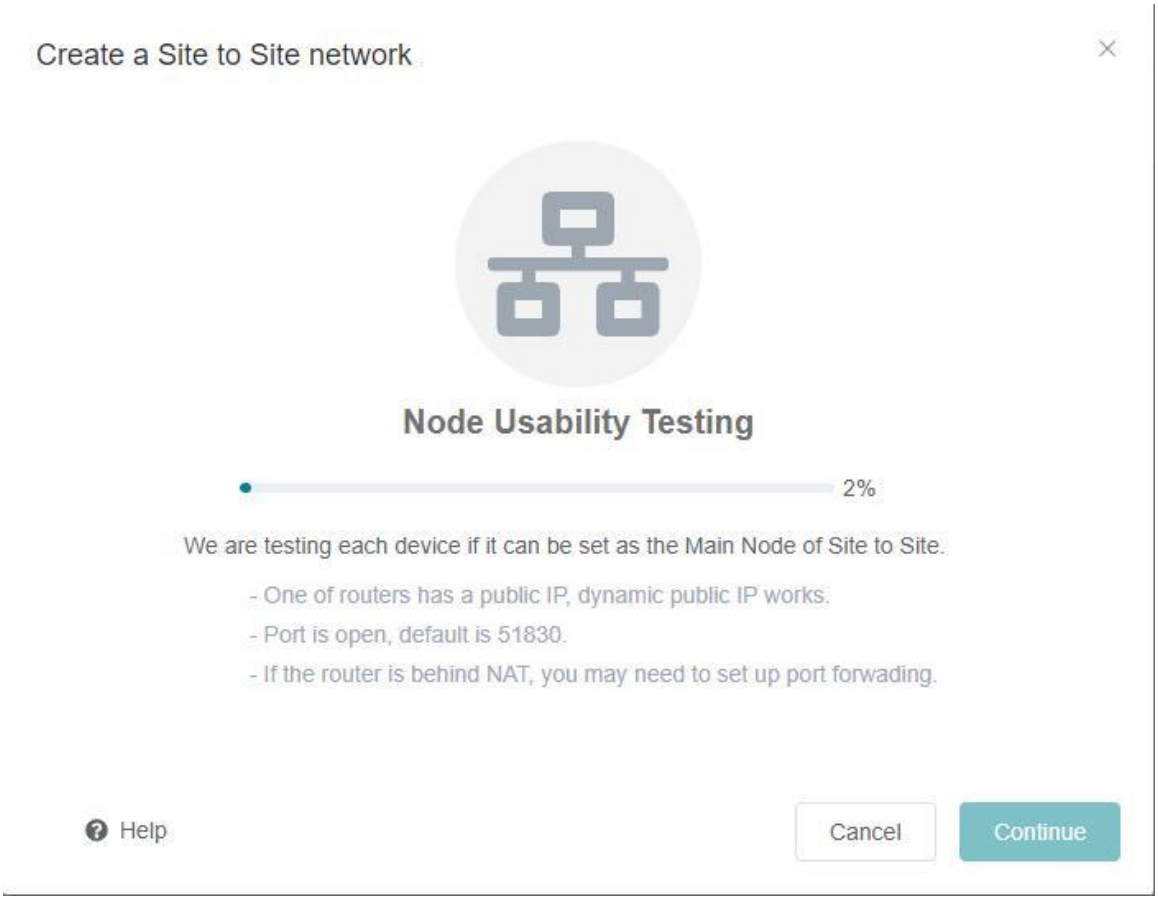
Due to the device's performance, each Site to Site network can have up to 10 devices.

After you had chosen the devices, click Continue.



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

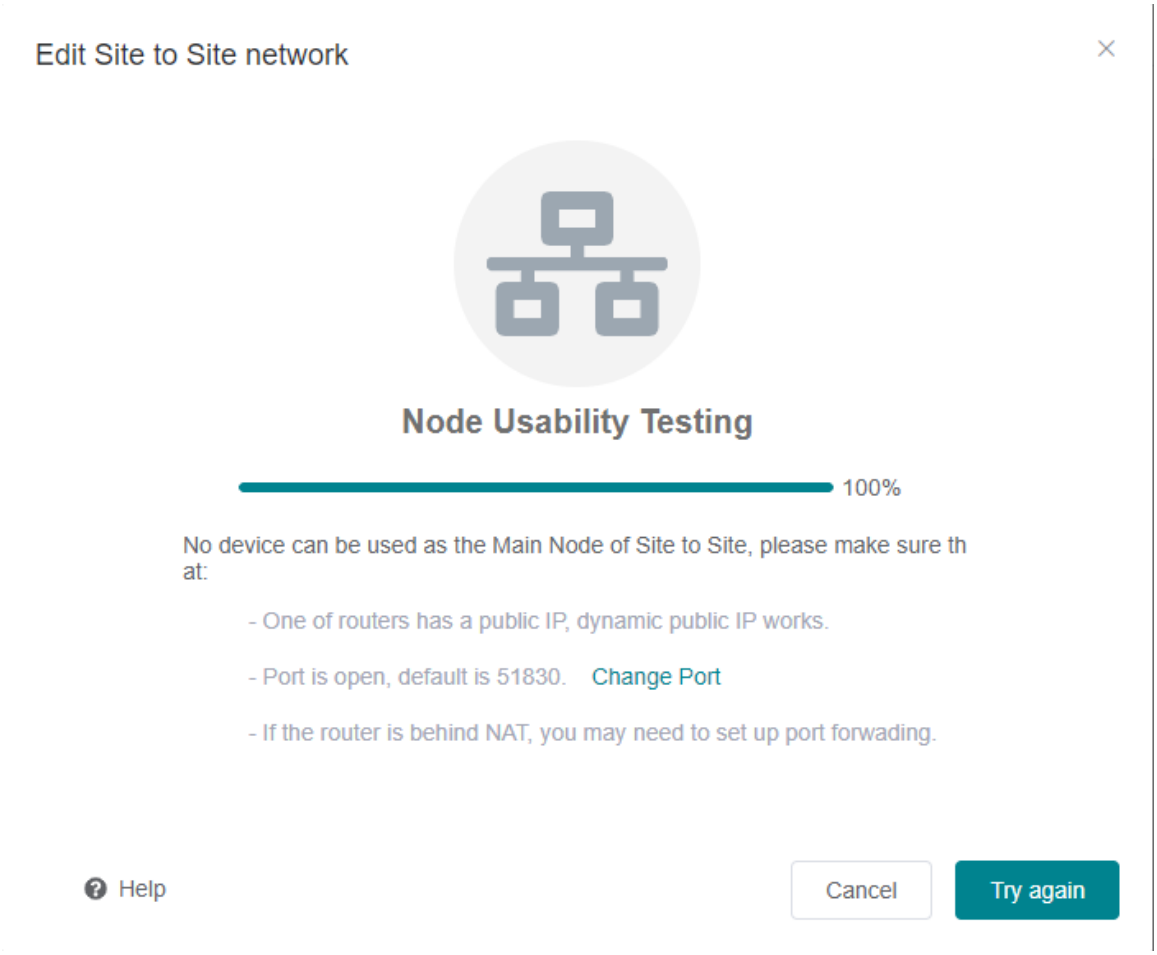
We suggest that the router with strong performance and best network speed to be the Main Node.



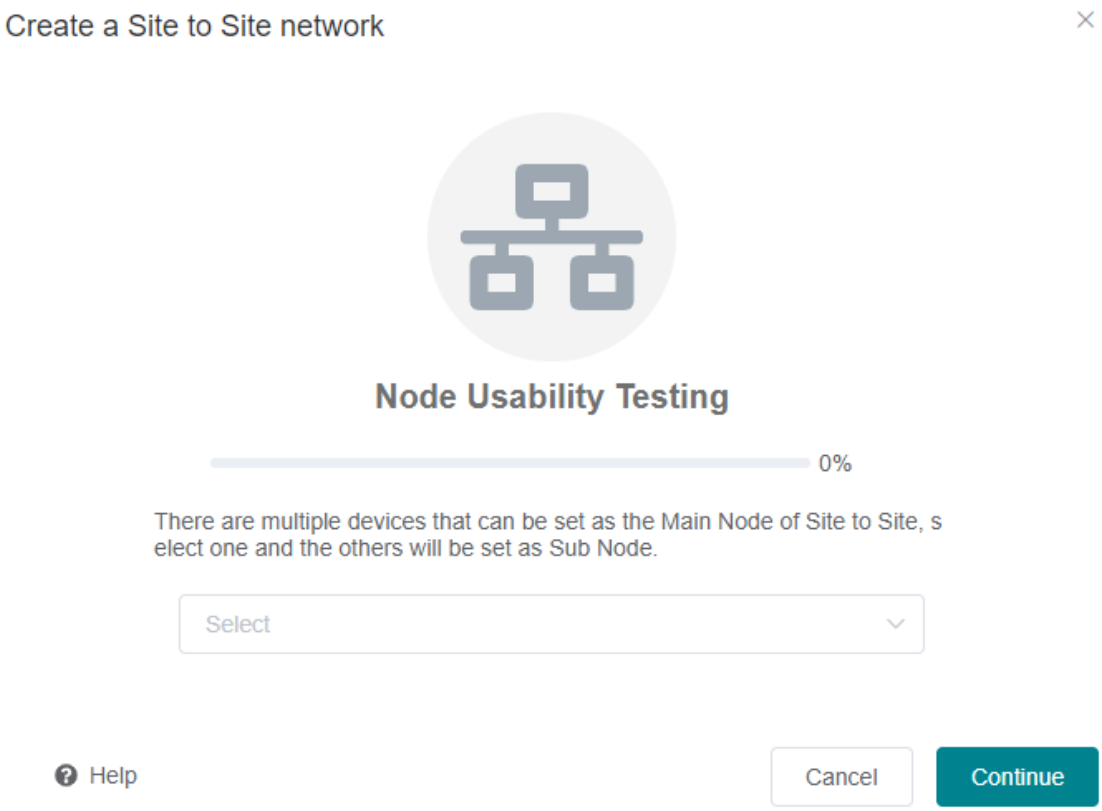
If none of the devices can be used as the Main Node, make sure that:

- 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 forwading.

You can also change port and try again.

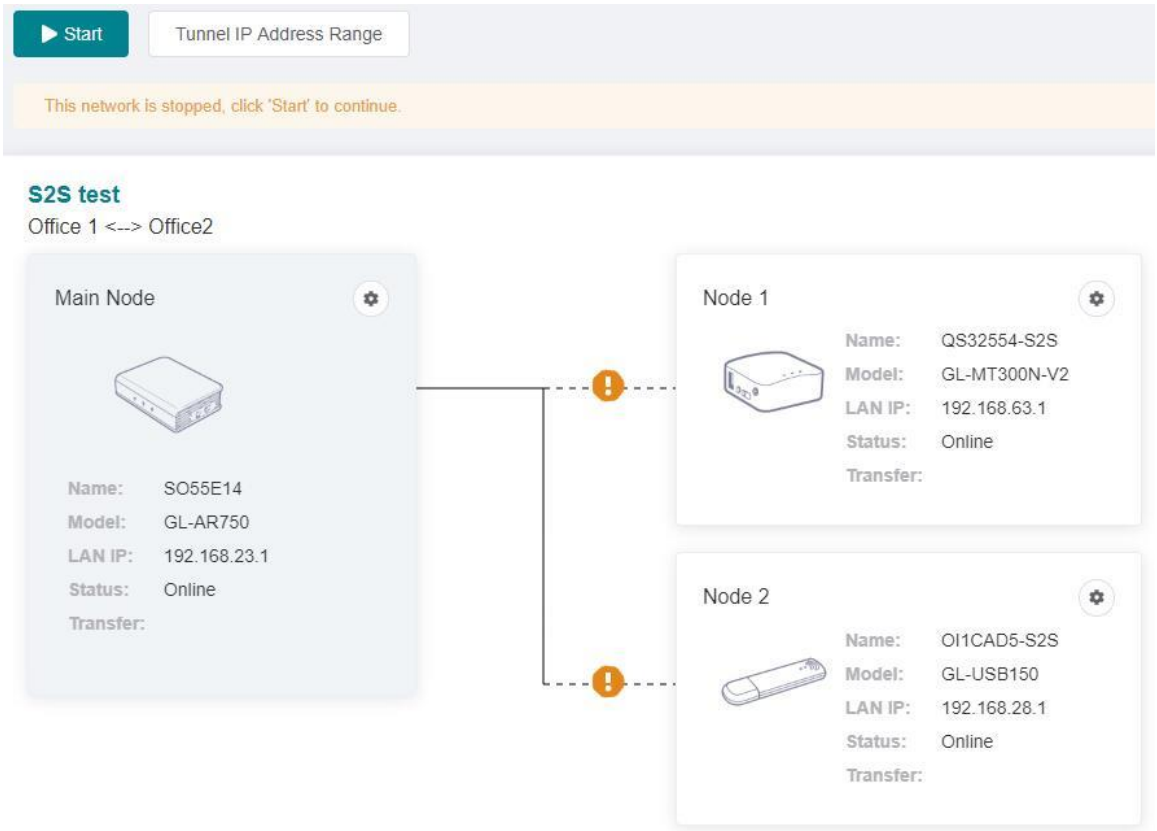


If there are more than one device can be set as the Main Node, you need to choose one to continue.

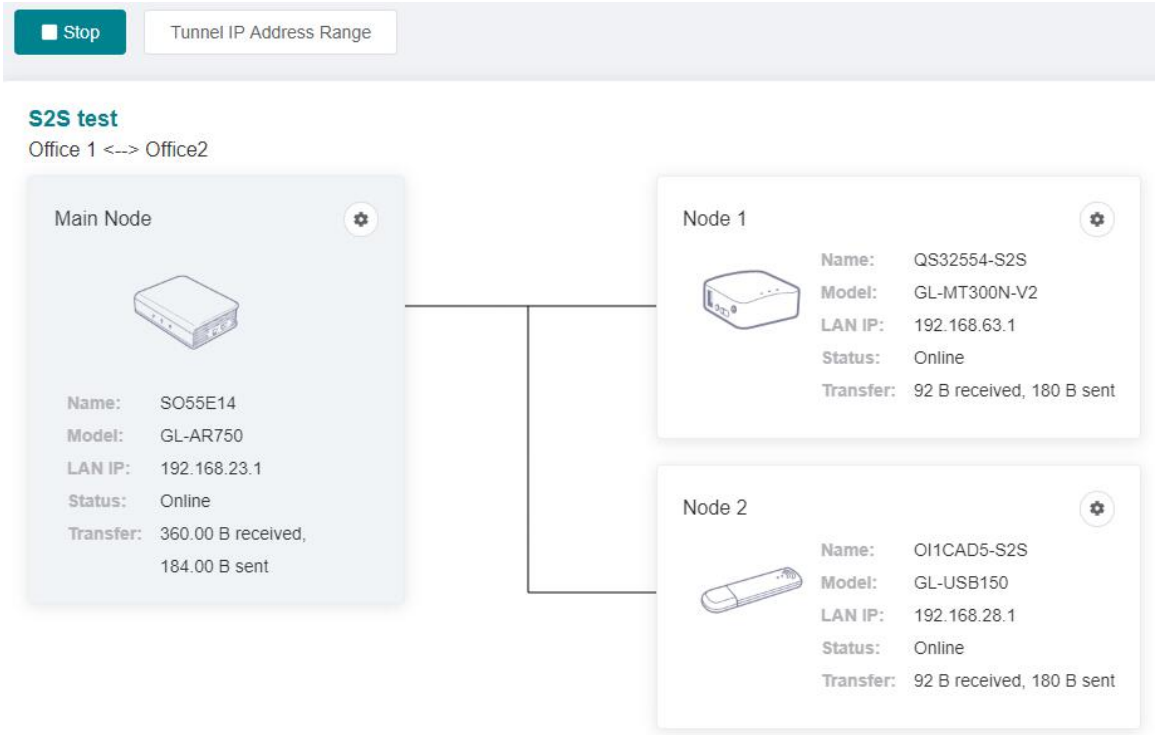


If there is only one device can be set as the Main Node, it will go to the Site to Site detail page directly.

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

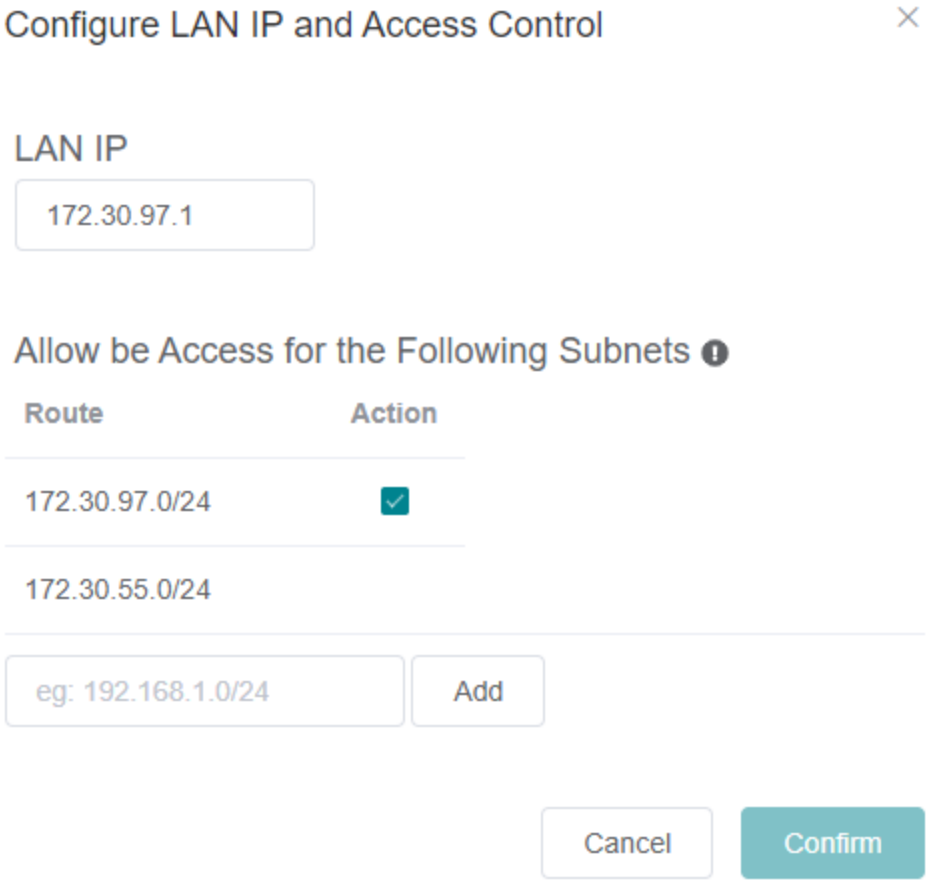
Now the Site to Site network is created and started, let's test the connection.

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.

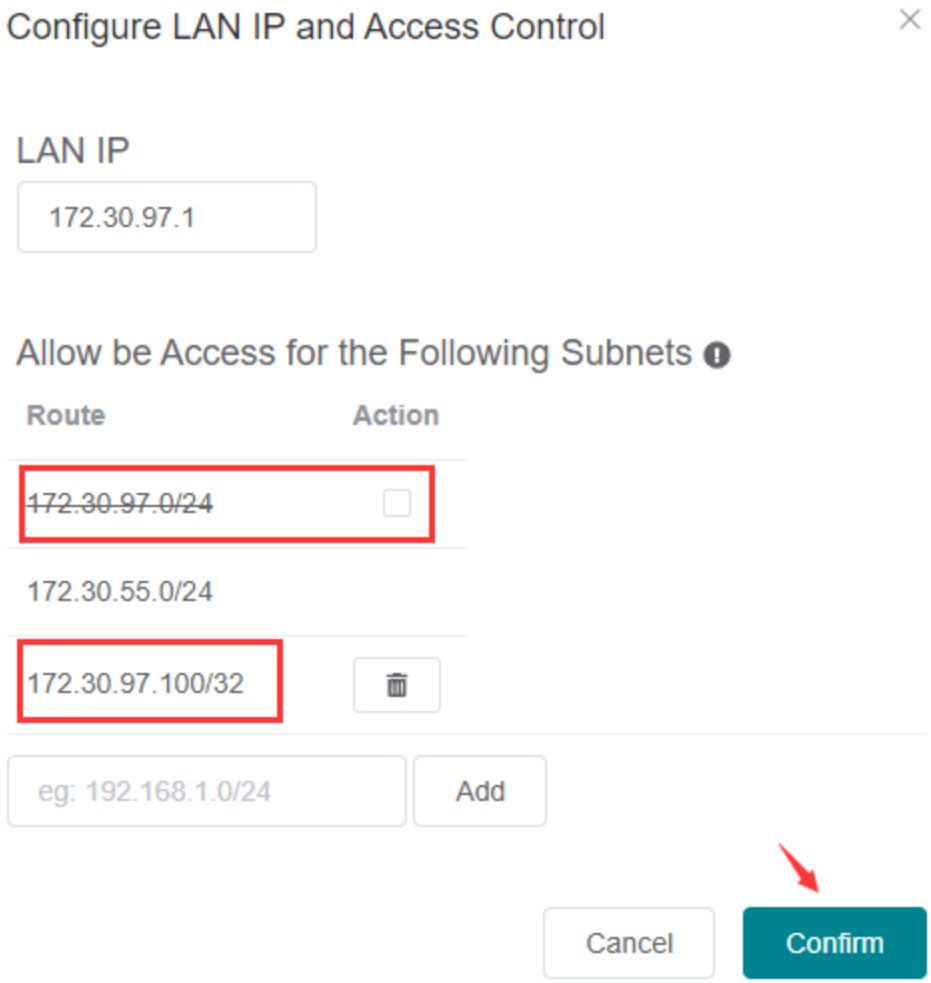
Route and other options

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



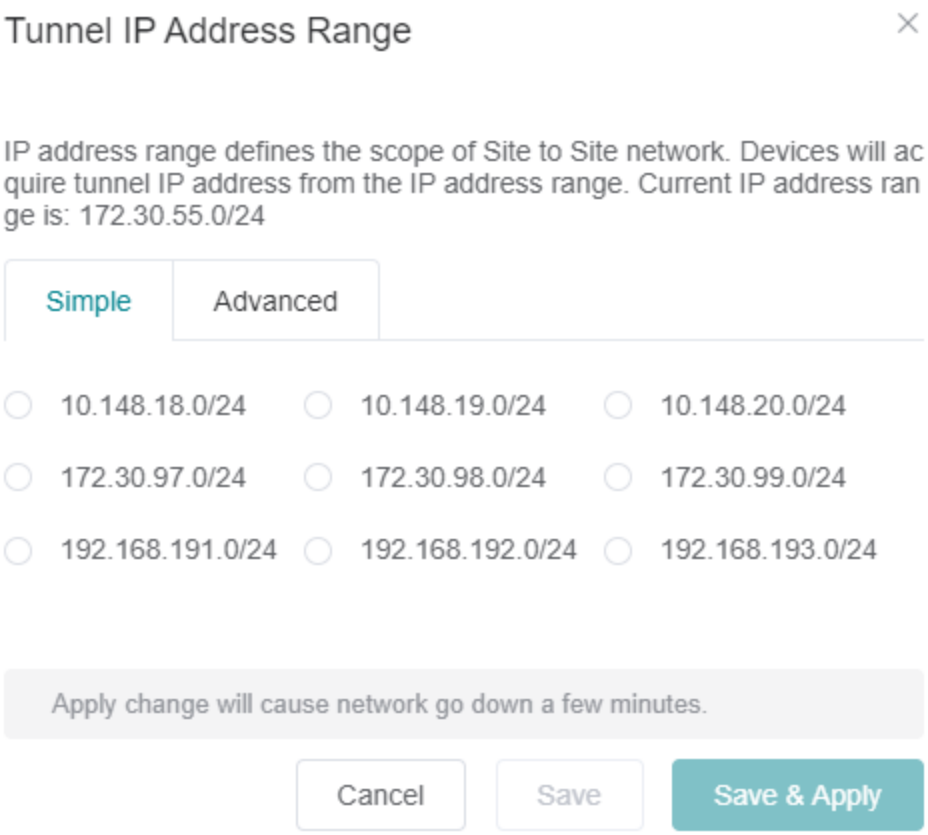
By default, each node can access other's LAN, based on security, we recommend only open the corresponding service IPs.

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



You can add node's parent routes too.

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



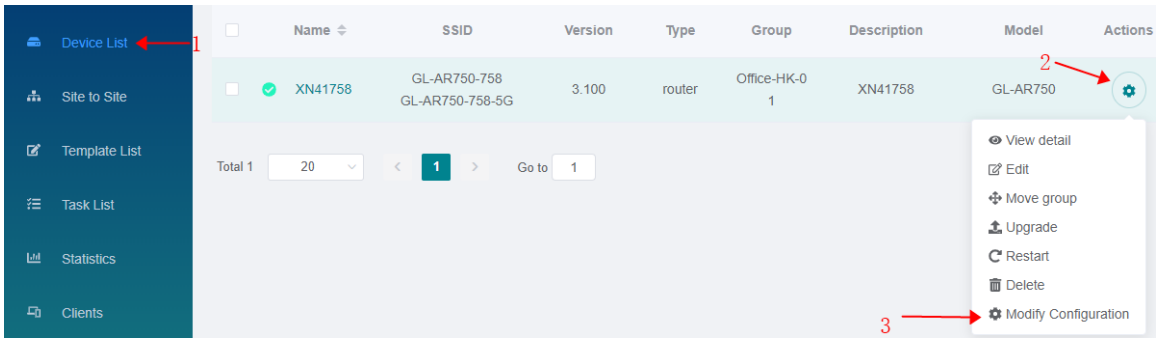
Batch Setting

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

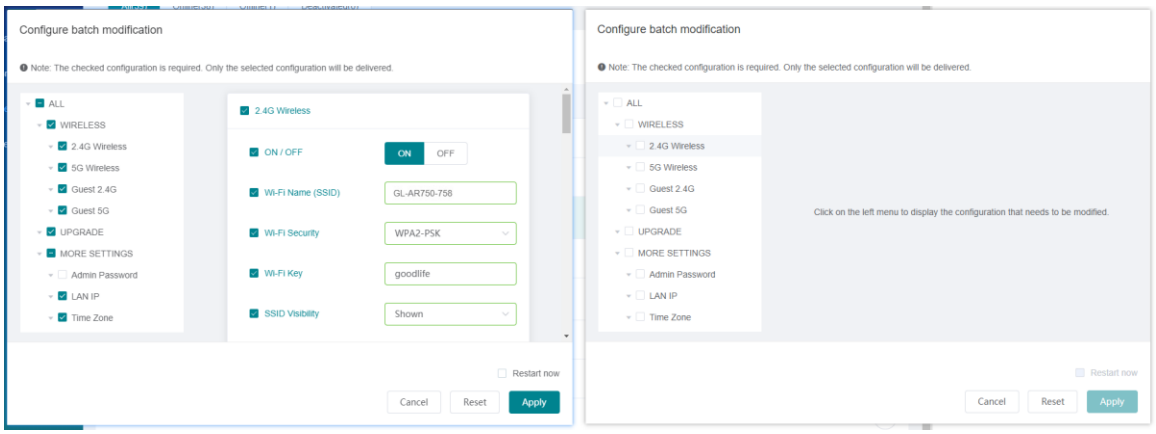
`Note: This feature is only available to business users.`

Batch Setting of Single Device

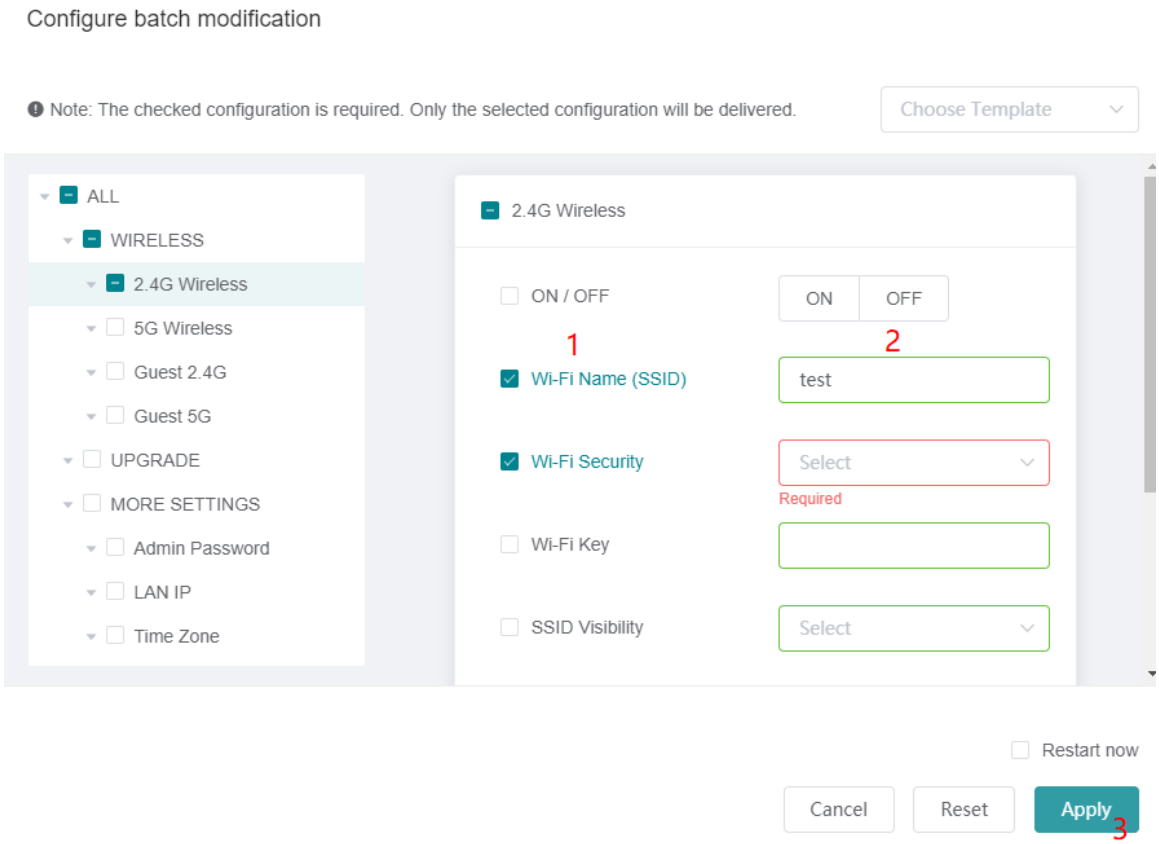
To configure single device, as show below.



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.



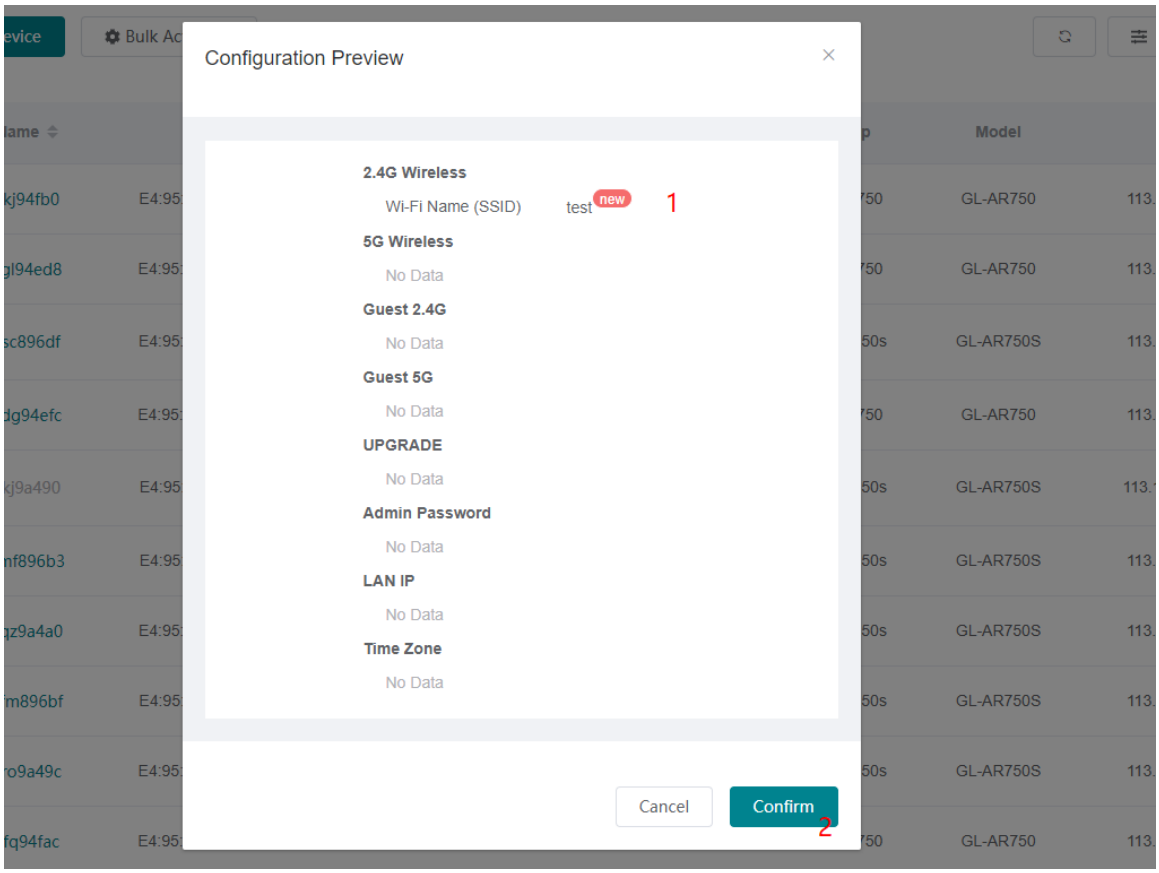
Check the configuration that needs to be modified and input value.



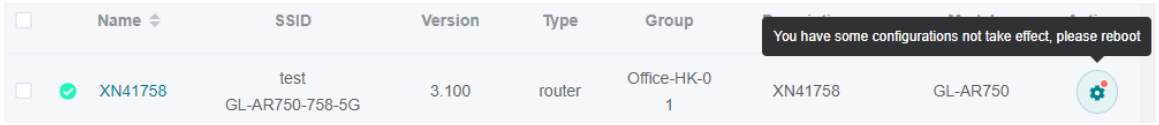
The checked configuration is required, and only the configuration that conforms to the rule can be filled out. After the configuration is delivered, it does not take effect immediately. The configuration takes effect and the device needs to be restarted. You can check the Restart now option in the

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

Preview the configuration and confirm the delivery.

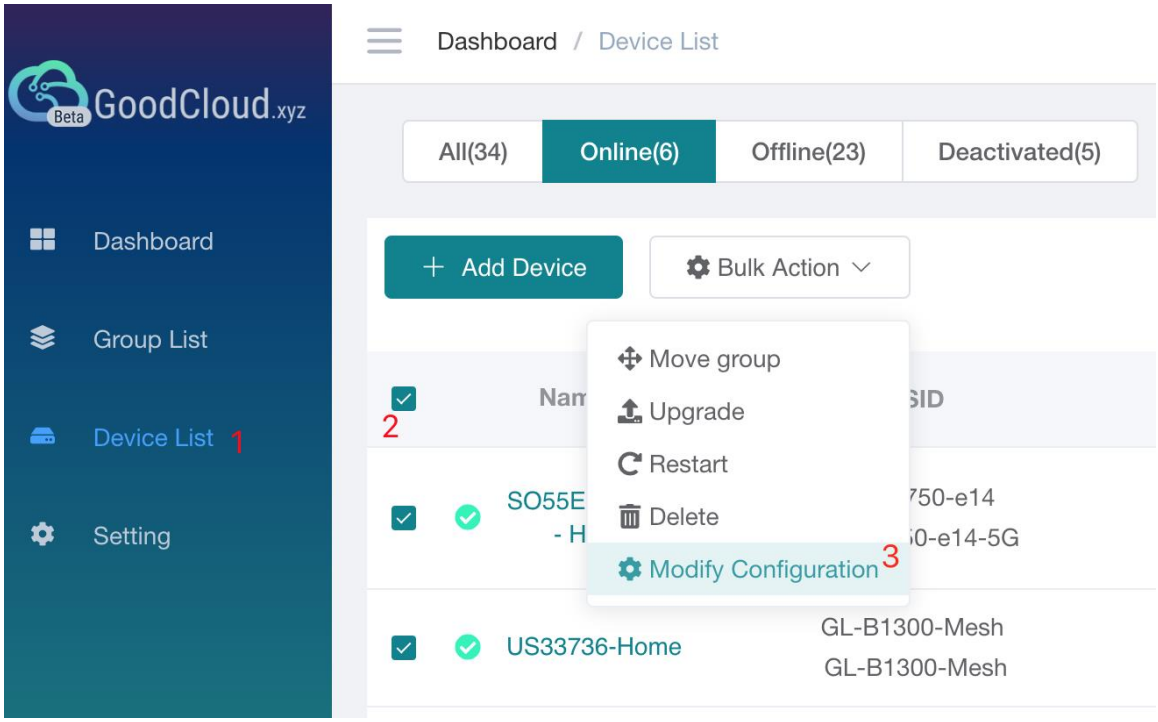


Unchecked **Restart now** option will prompt.



Batch Setting of Mutiple Devices

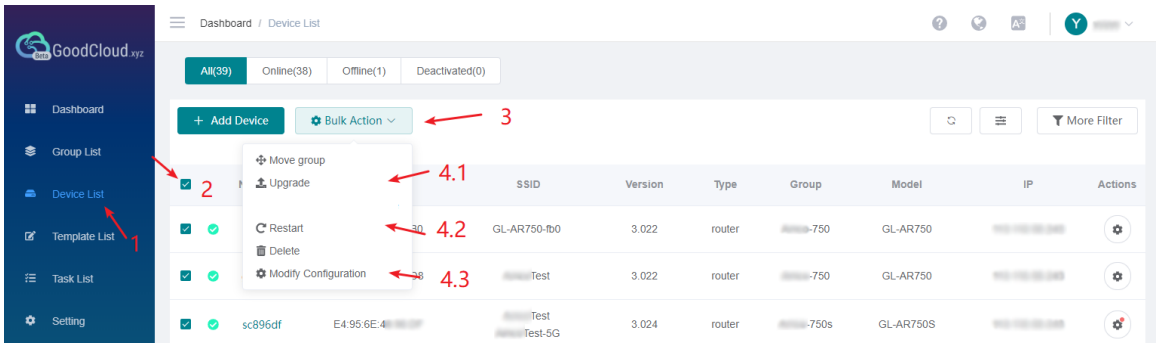
Select the devices you want to configure.



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

Other Batch Operations

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



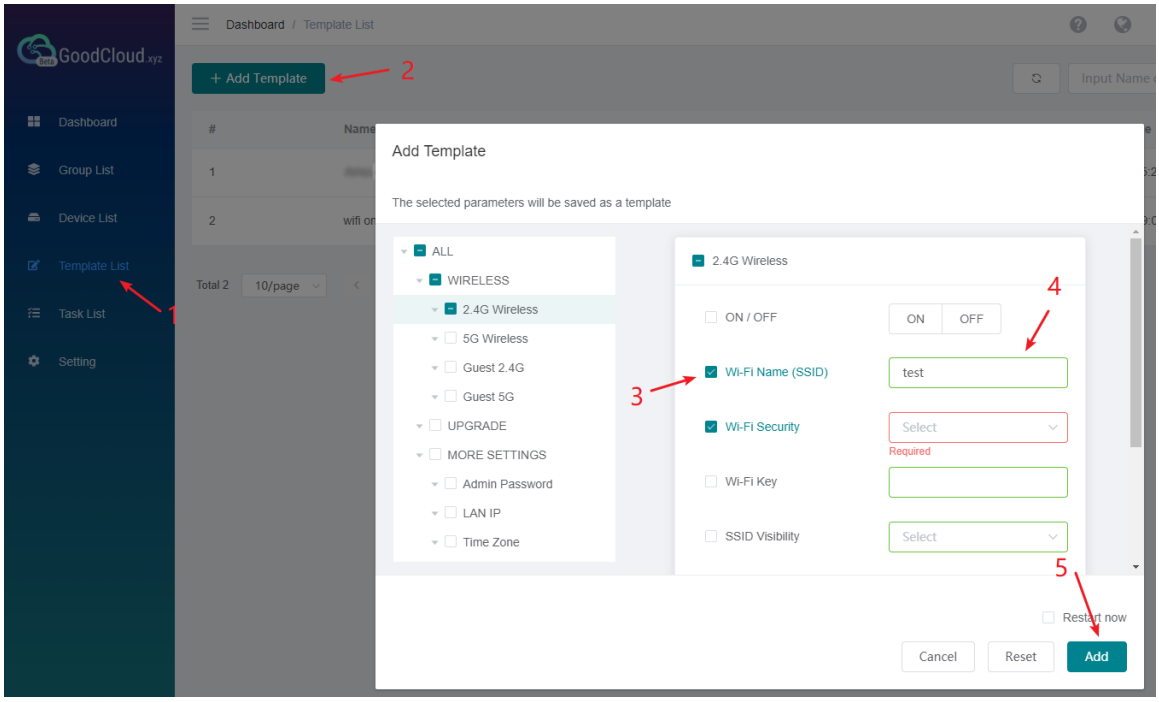
Template Management

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

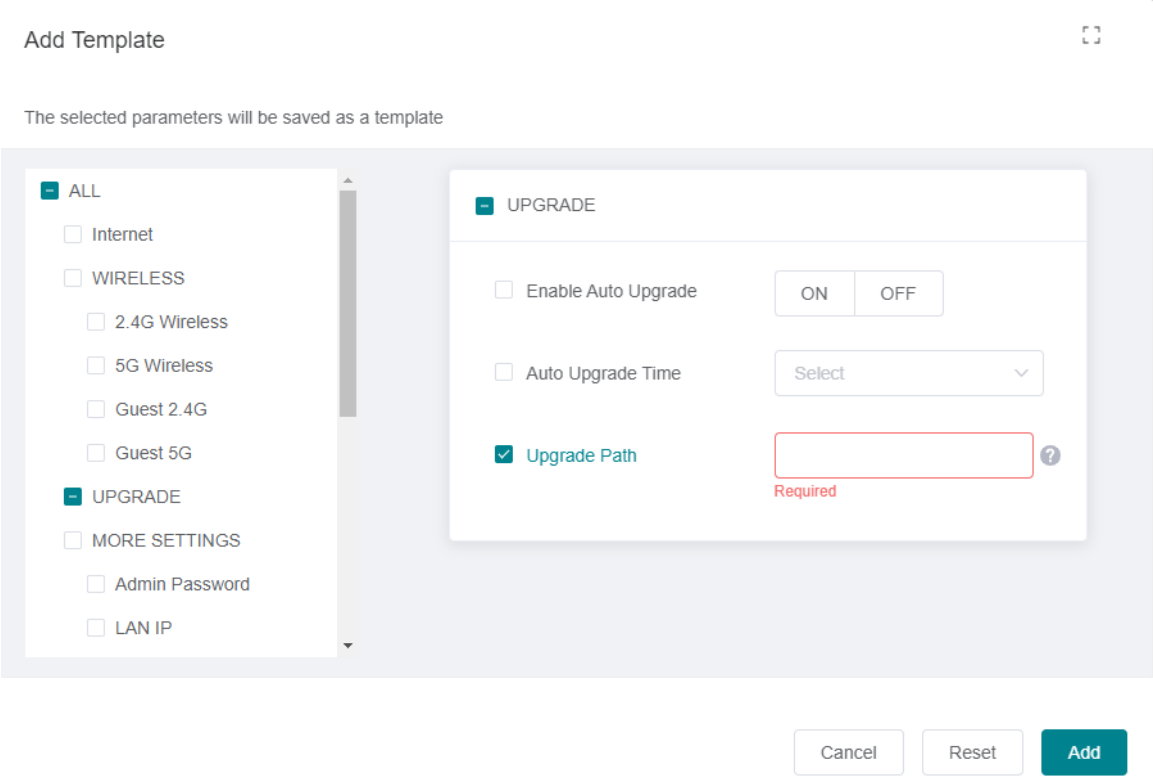
Check the configuration that needs to be modified and input value. Most of the options are the same as those on web Admin Panel.



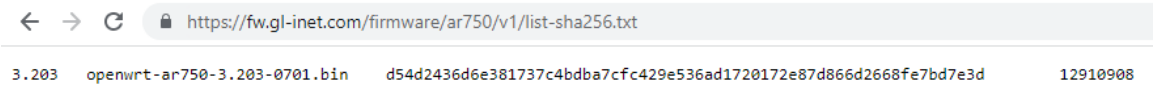
Upgrade

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.

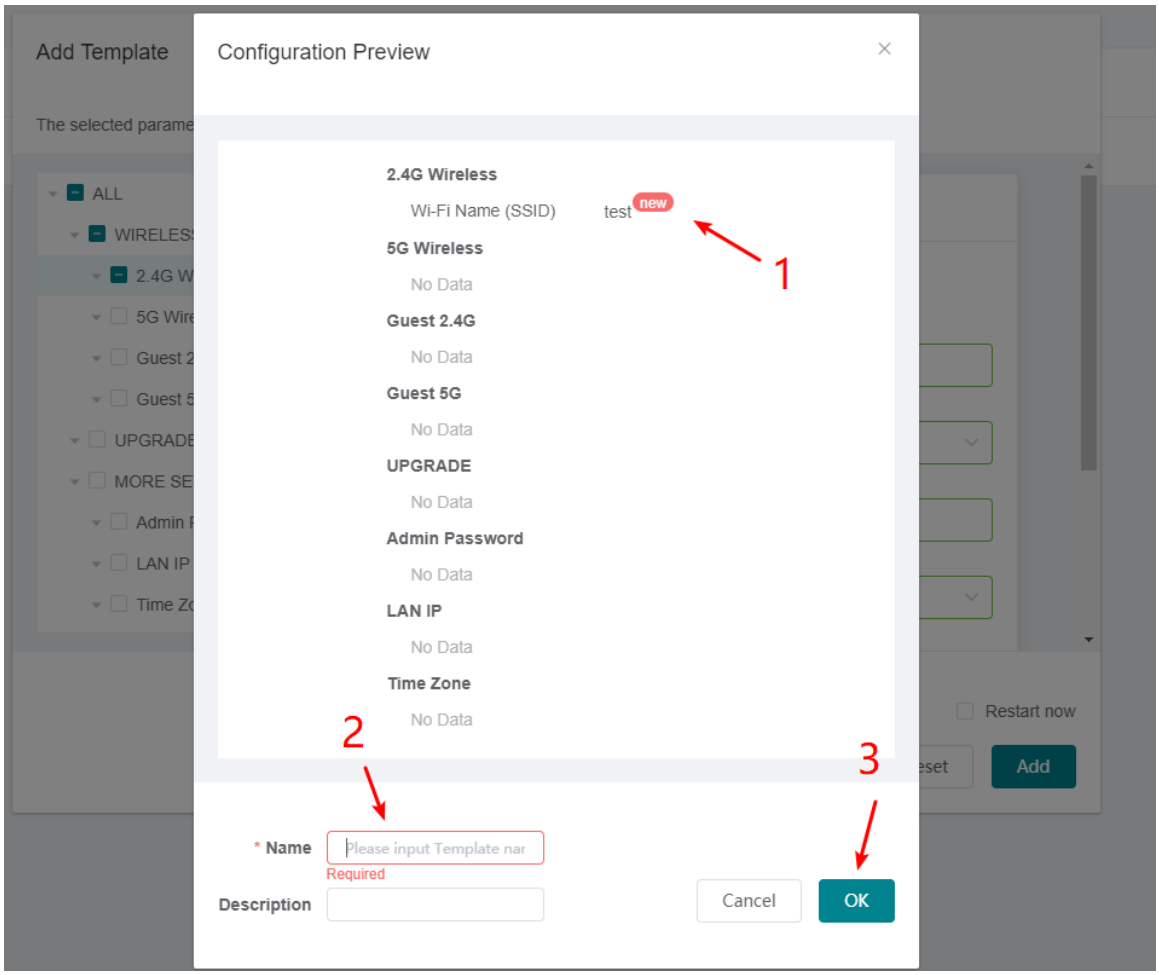
`Note: GL-AX1800, GL-S1300, GL-B1300, GL-AP1300 only support http path for now.`



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 thrid column is the sha256 of firmware file, the forth column is the size of firmware file.



Give the template a name and description.



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.

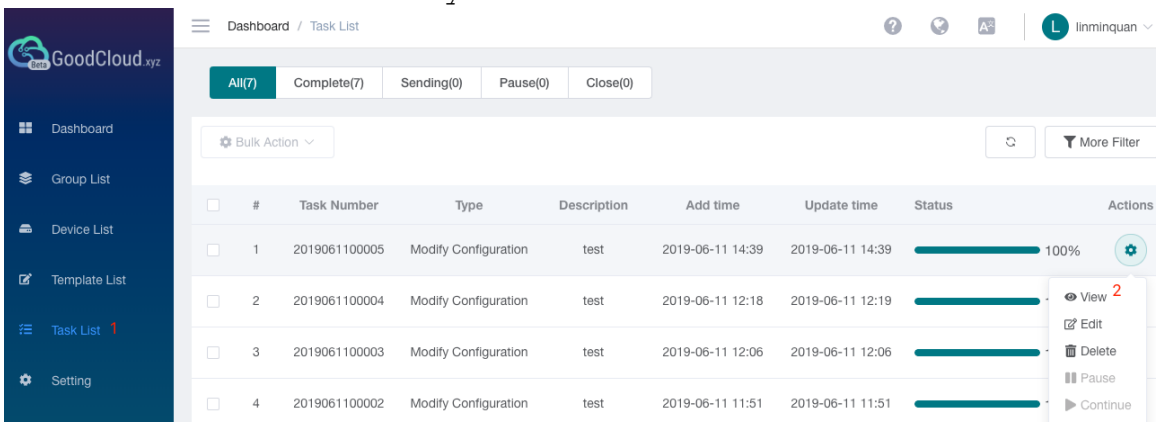
It will pop up another dialog to review the configuration of the template, scroll down to the bottom to click the **Confirm** button, it will load the configuration of template overwrite to this time modification.

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

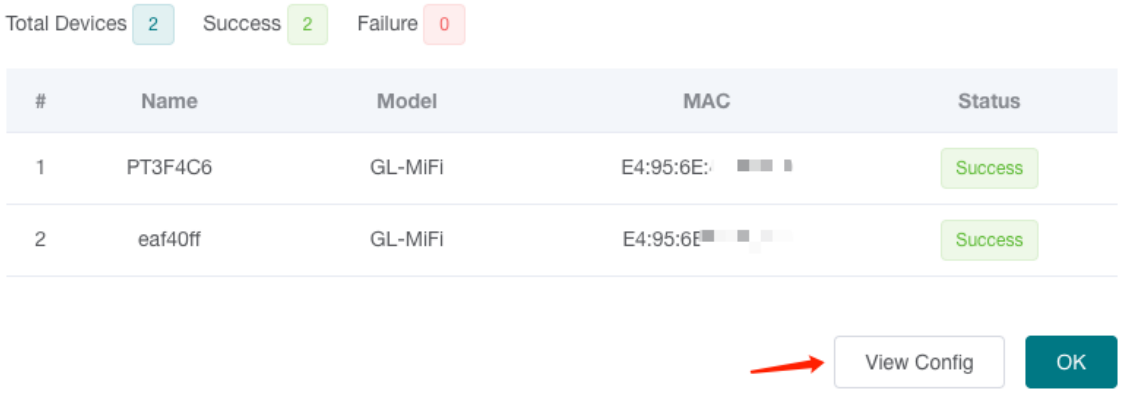
Task List

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

Note: This feature is only available to business users.



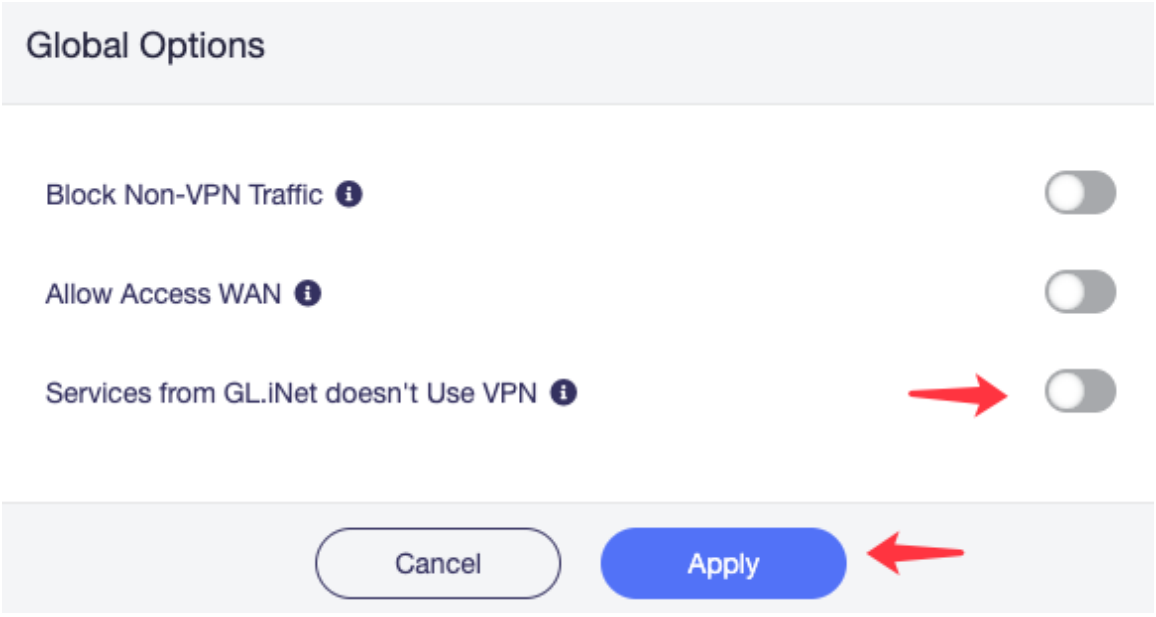
You can view the execution result of each device and configuration.



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.

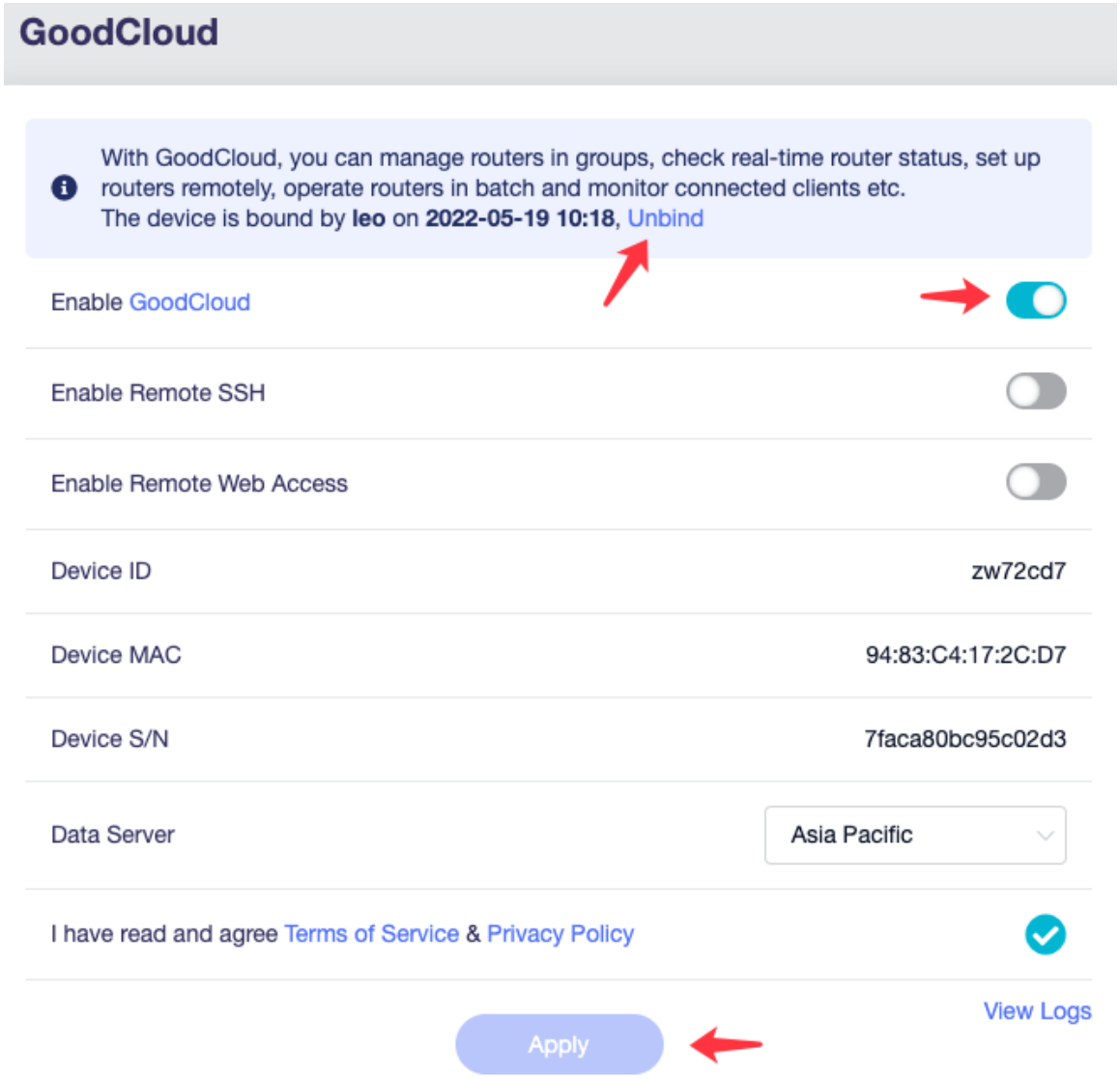
Go to web Admin Panel, on the left side, VPN -> VPN Dashboard -> VPN Client -> Global Options.



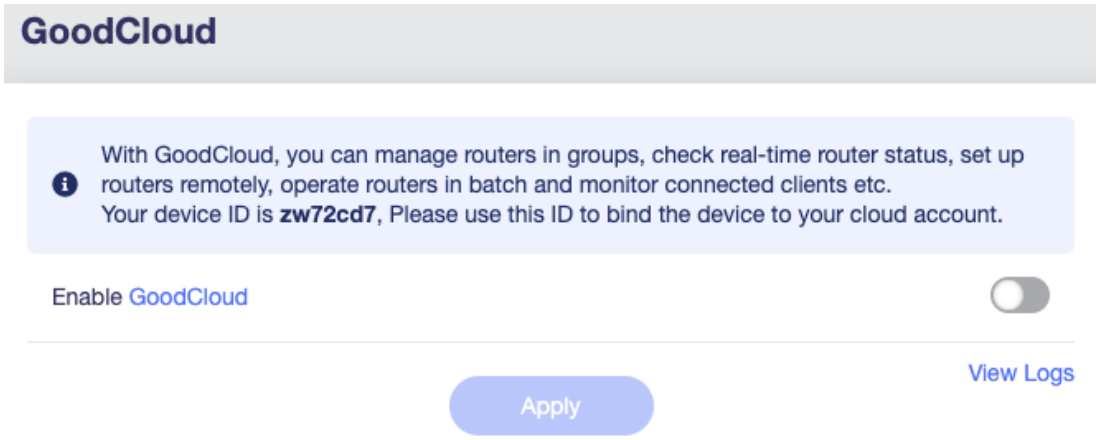
It is not recommended to run Site to Site while its nodes are also running VPN client, which can make the network particularly complex.

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.

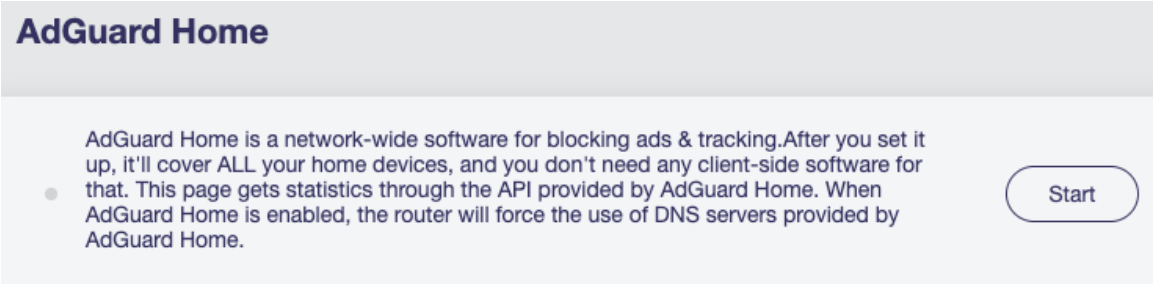


After disable Cloud, the interface is like below.

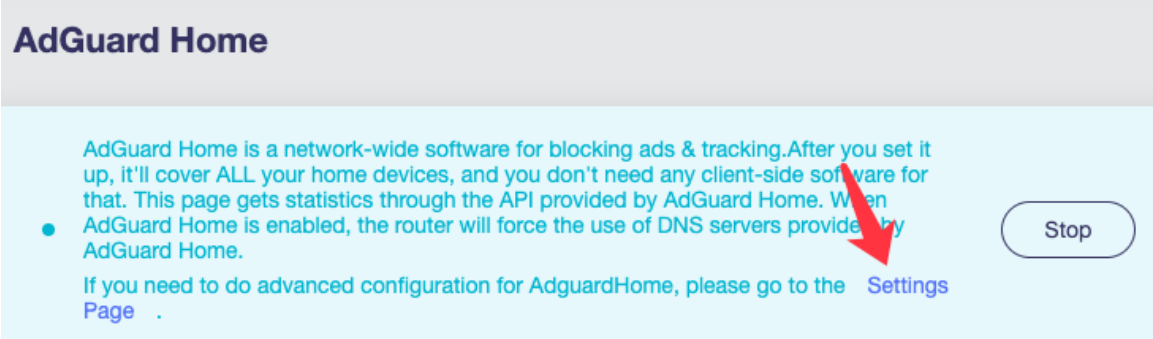

GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is zw72cd7, Please use this ID to bind the device to your cloud account.
Enable GoodCloud
View Logs
Apply

8.4 AdGuard Home

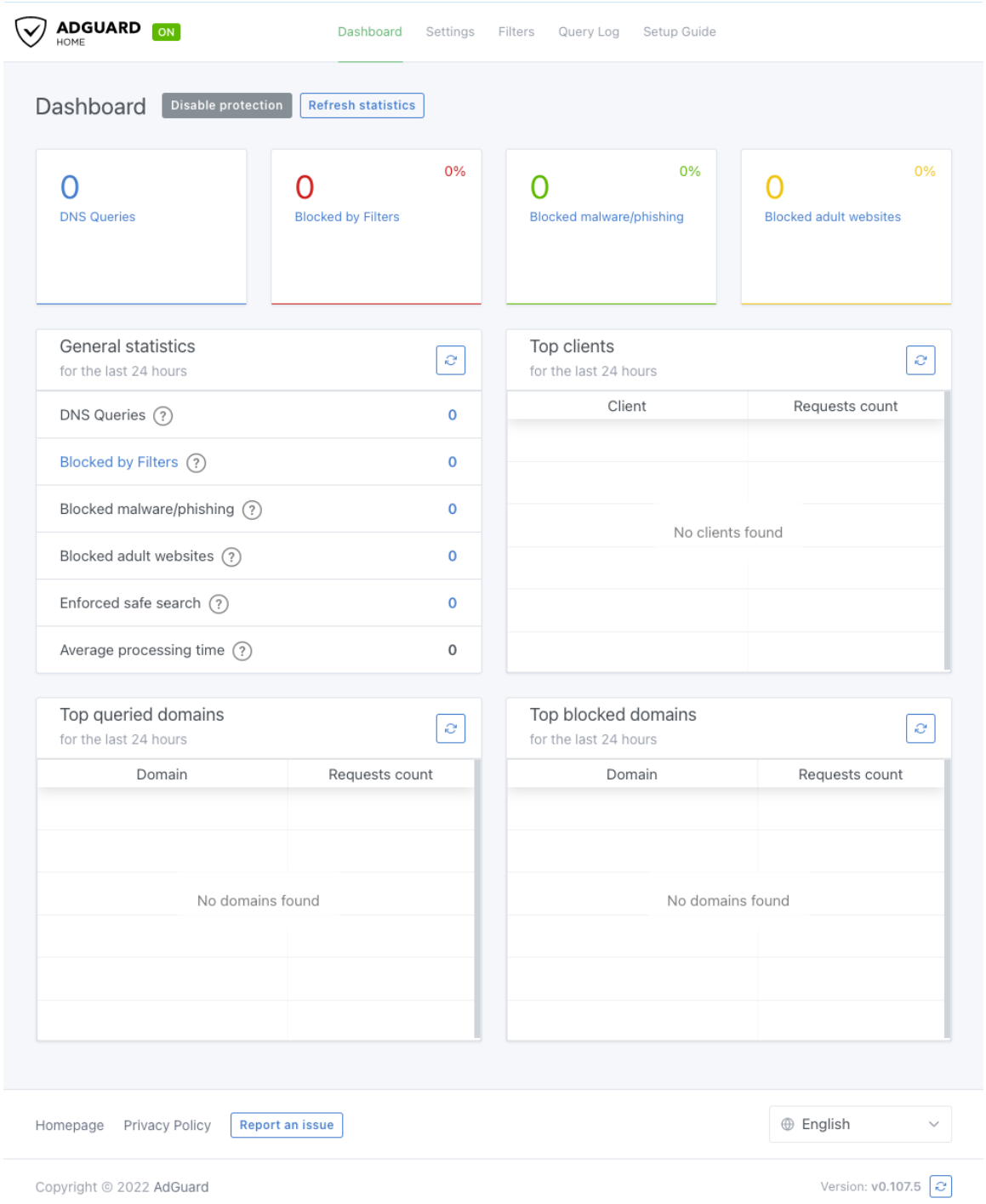
AdGuard Home is a network-wide software for blocking ads & tracking. Click **Start** button to continue.



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
ON
Dashboard
Settings
Filters
Query Log
Setup Guide
Dashboard
Disable protection
Refresh statistics
0
DNS Queries
0
0%
Blocked by Filters
0
0%
Blocked malware/phishing
0
0%
Blocked adult websites
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: v0.107.5

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.

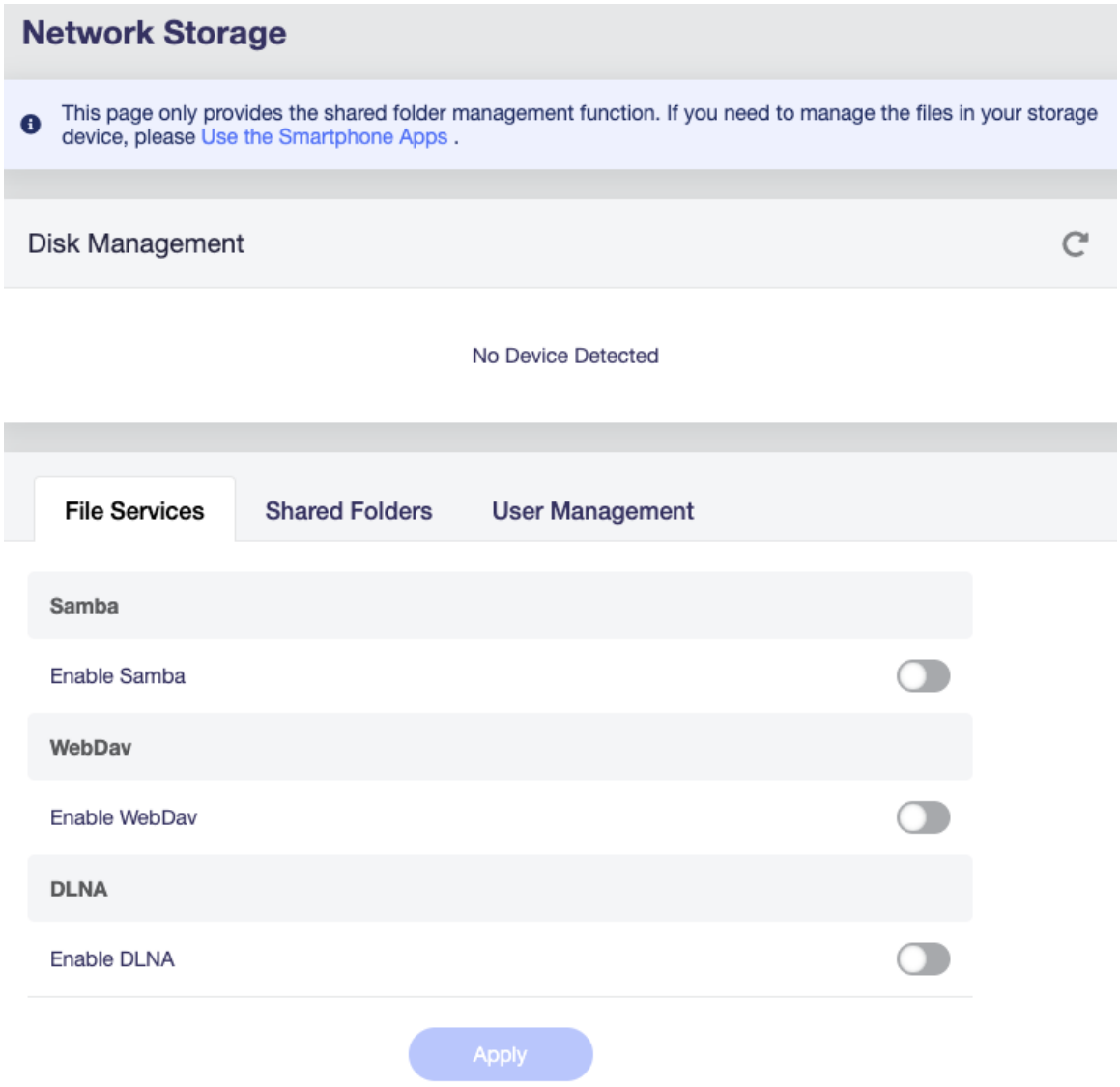
The supported disk formats are NTFS, exFAT, FAT32, Ext3, Ext4.

Insert storage device

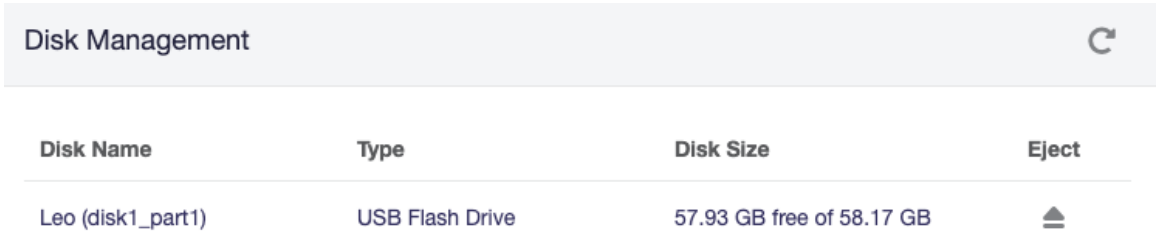
For TF card, you need to power off the router first, insert the TF card and then power on the router.

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

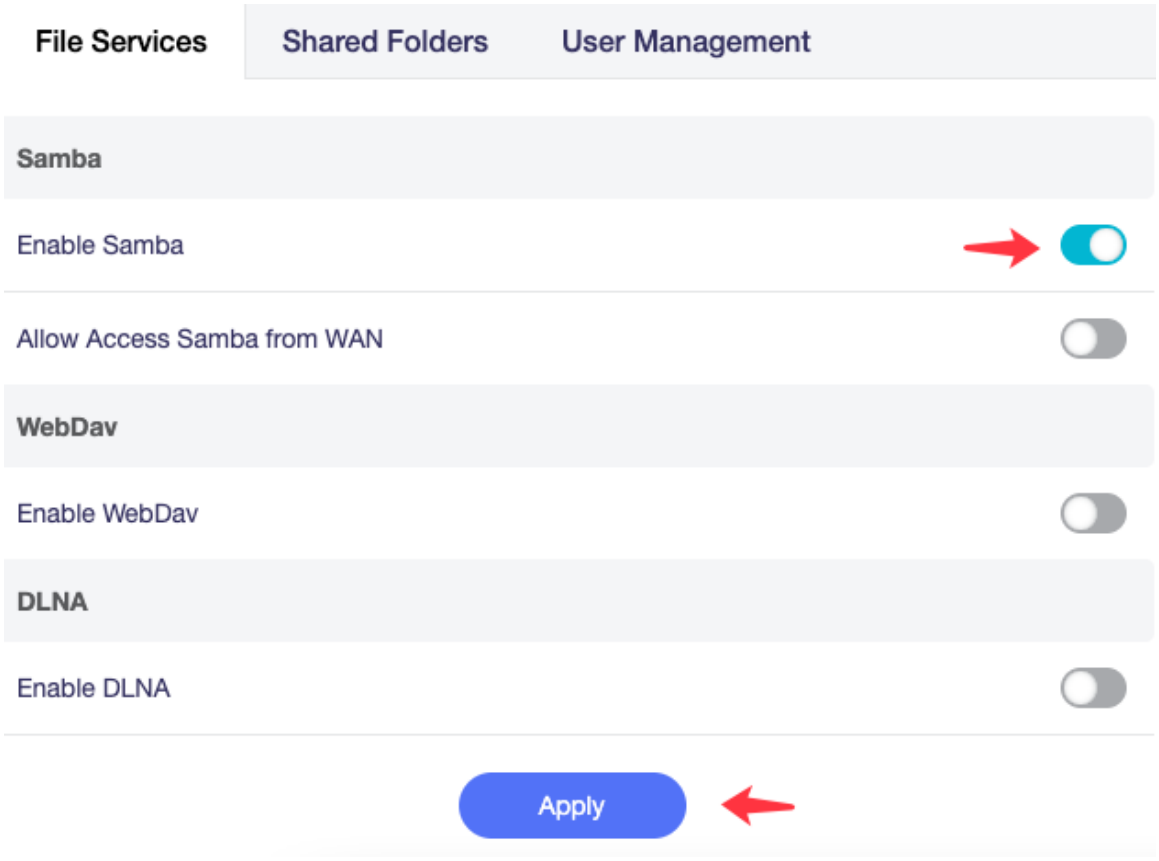


When a disk is found.

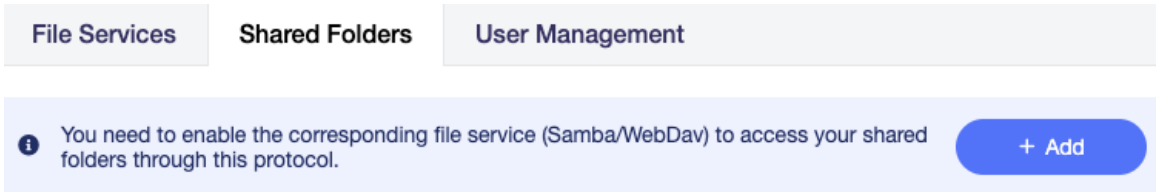


Set up Samba

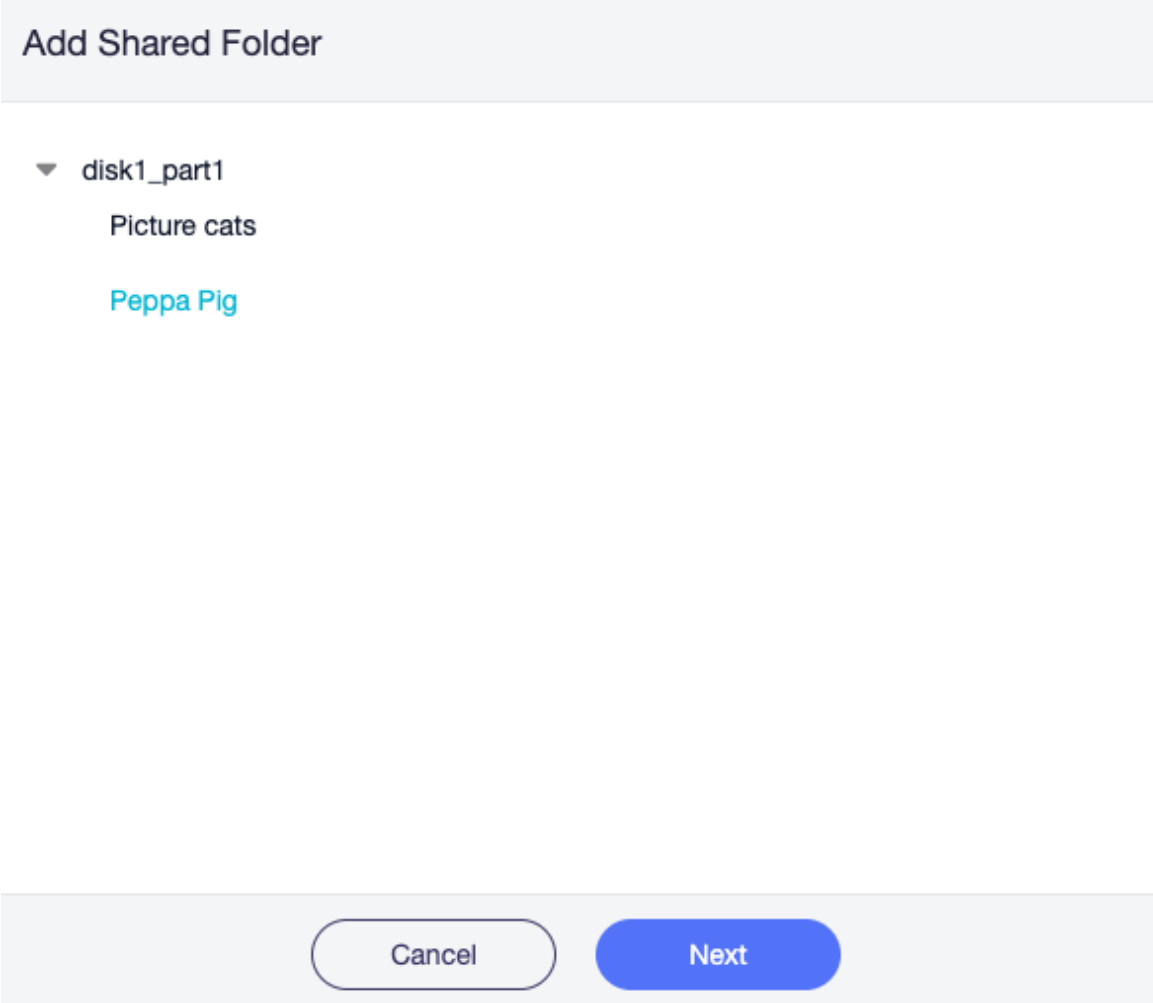
Toggle to enable Samba, click **Apply**.



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



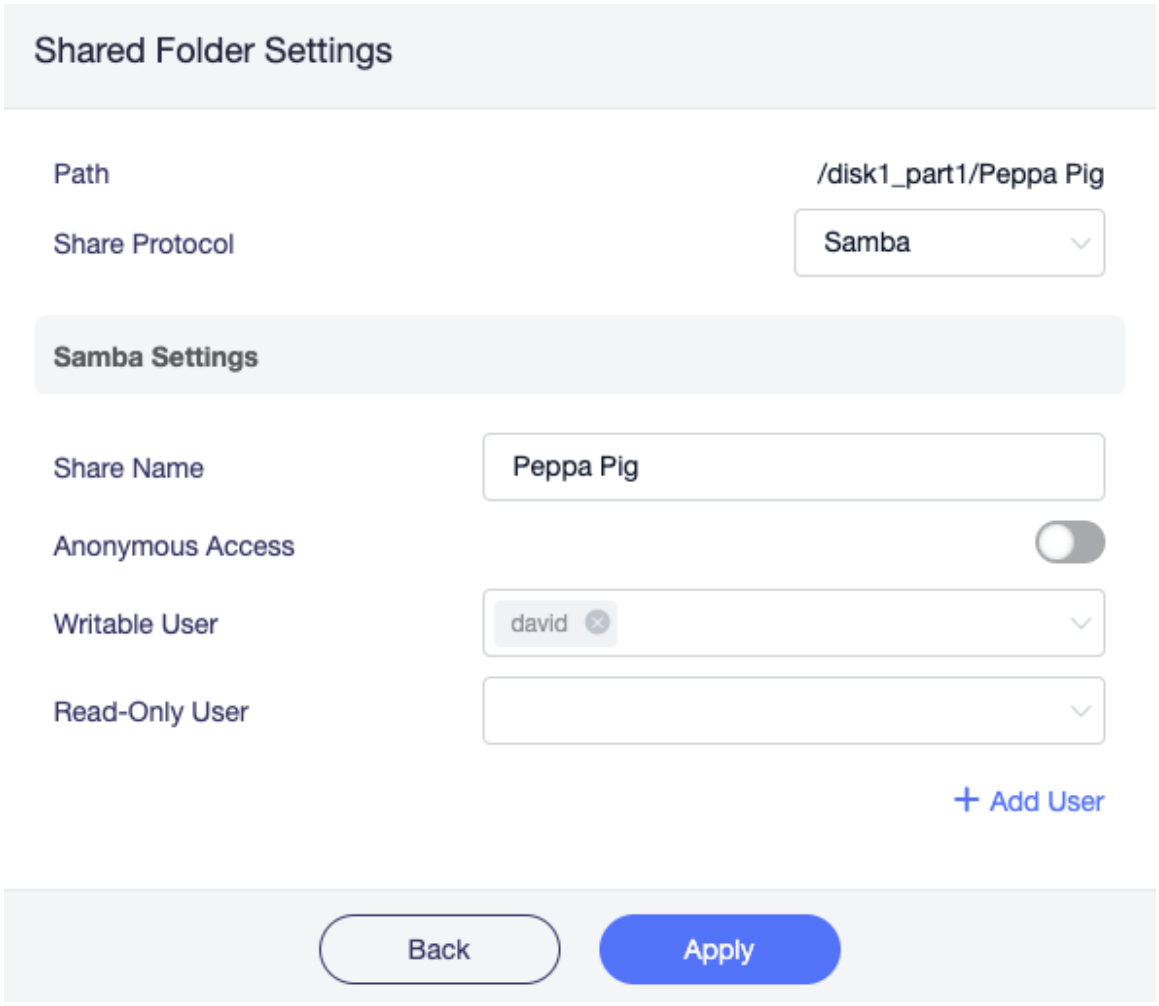
Choose a folder to share, then click **Next**.



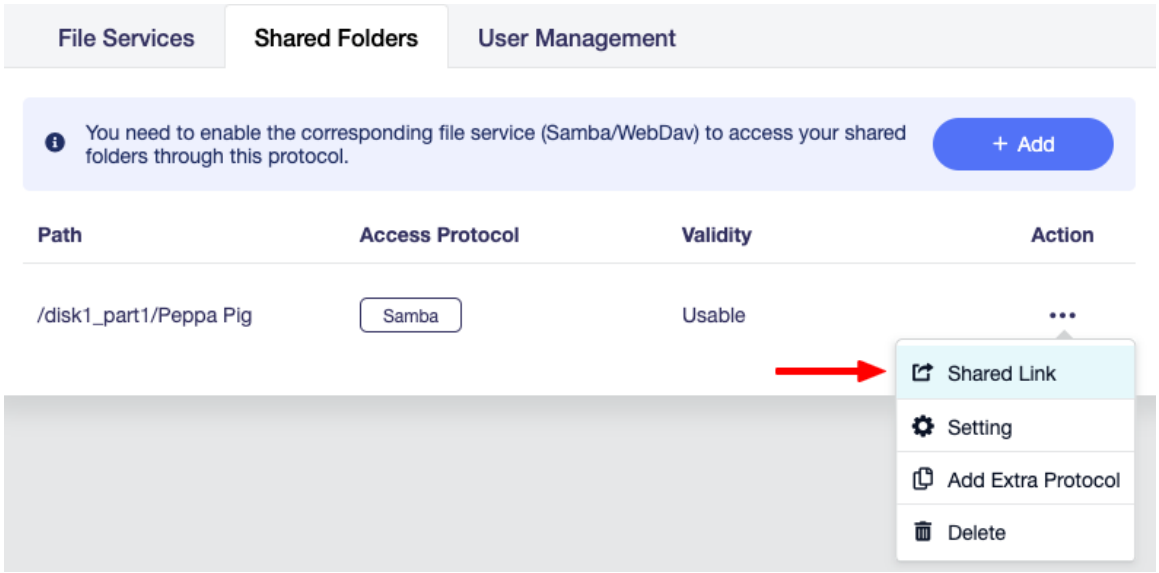
For security reasons, we do not recommend enabling **Anonymous Access**.

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.

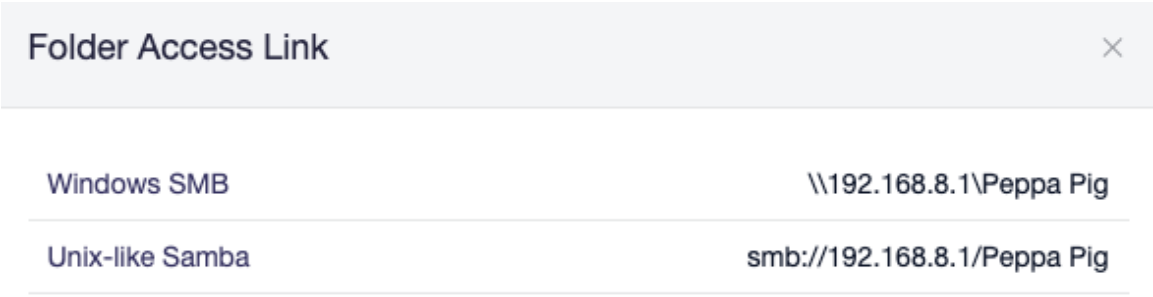


That is it. The access link can be found in **Shared Link**.



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.



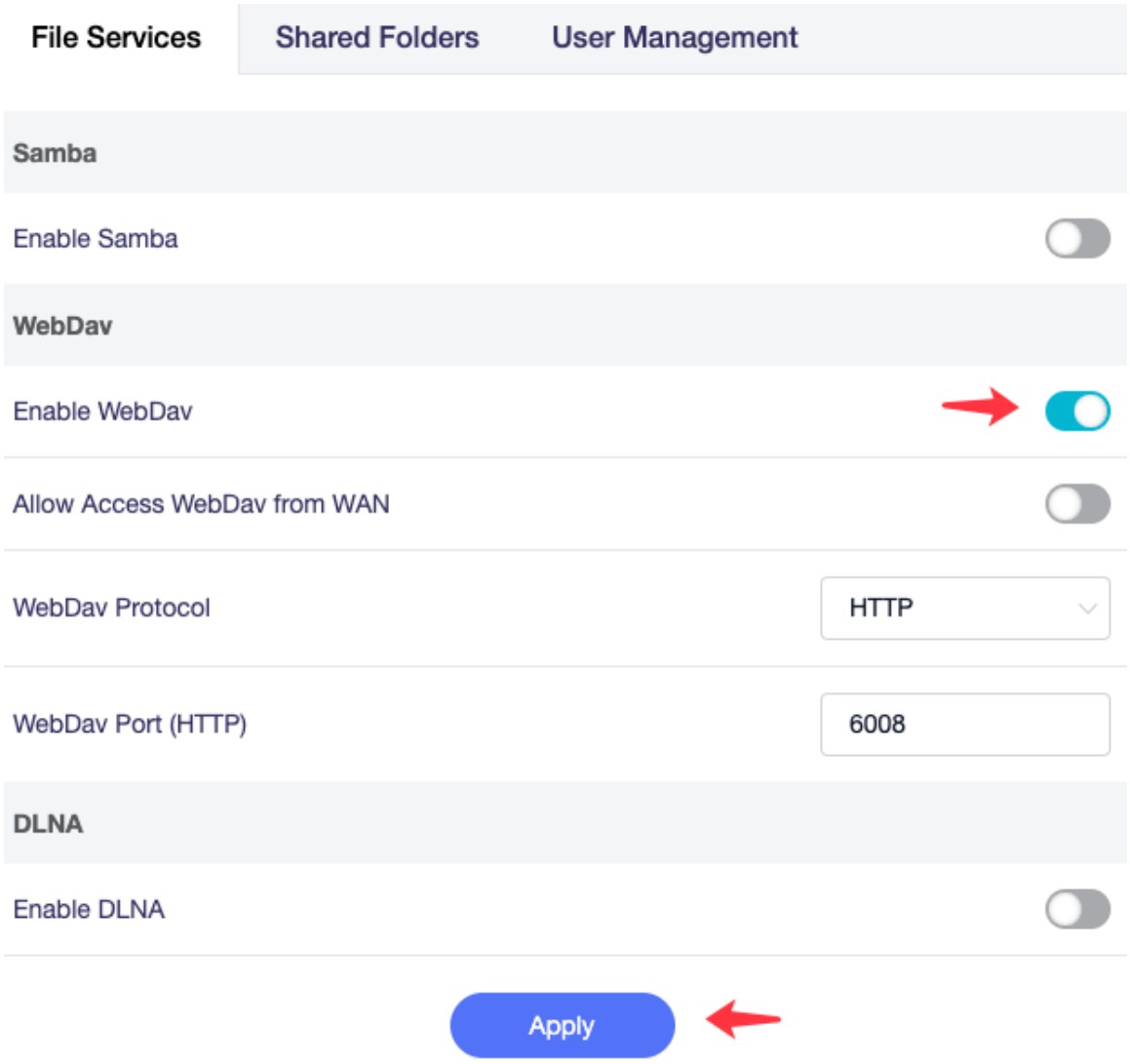
Then try to access the Samba on various OS, check out here.

Set up WebDAV

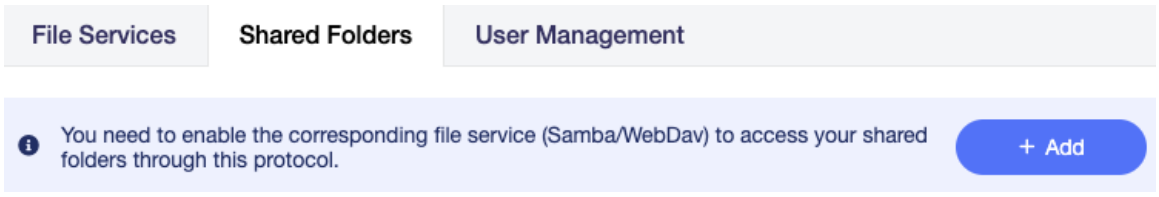
Toggle to enable WebDAV.

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

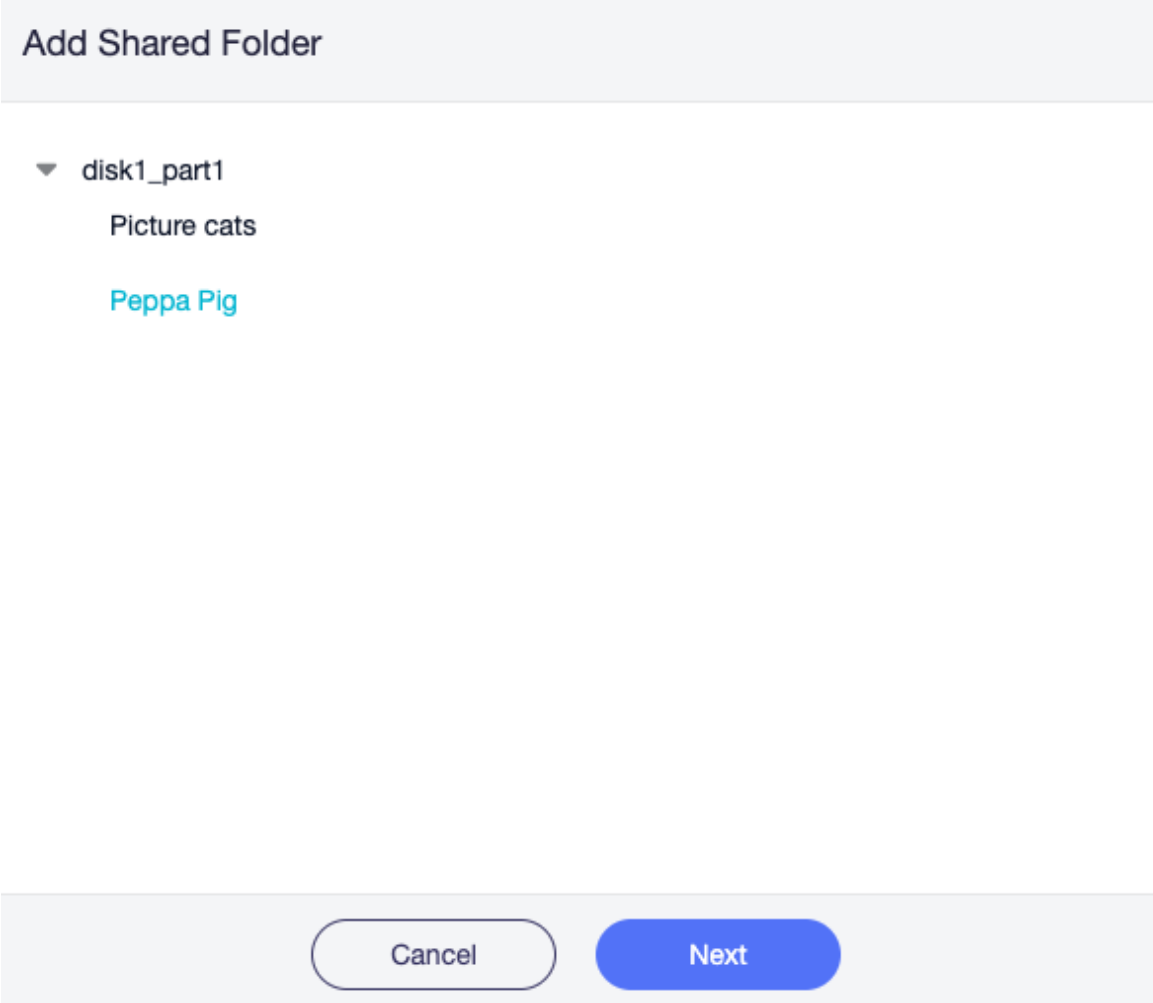
Then click **Apply**.



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



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

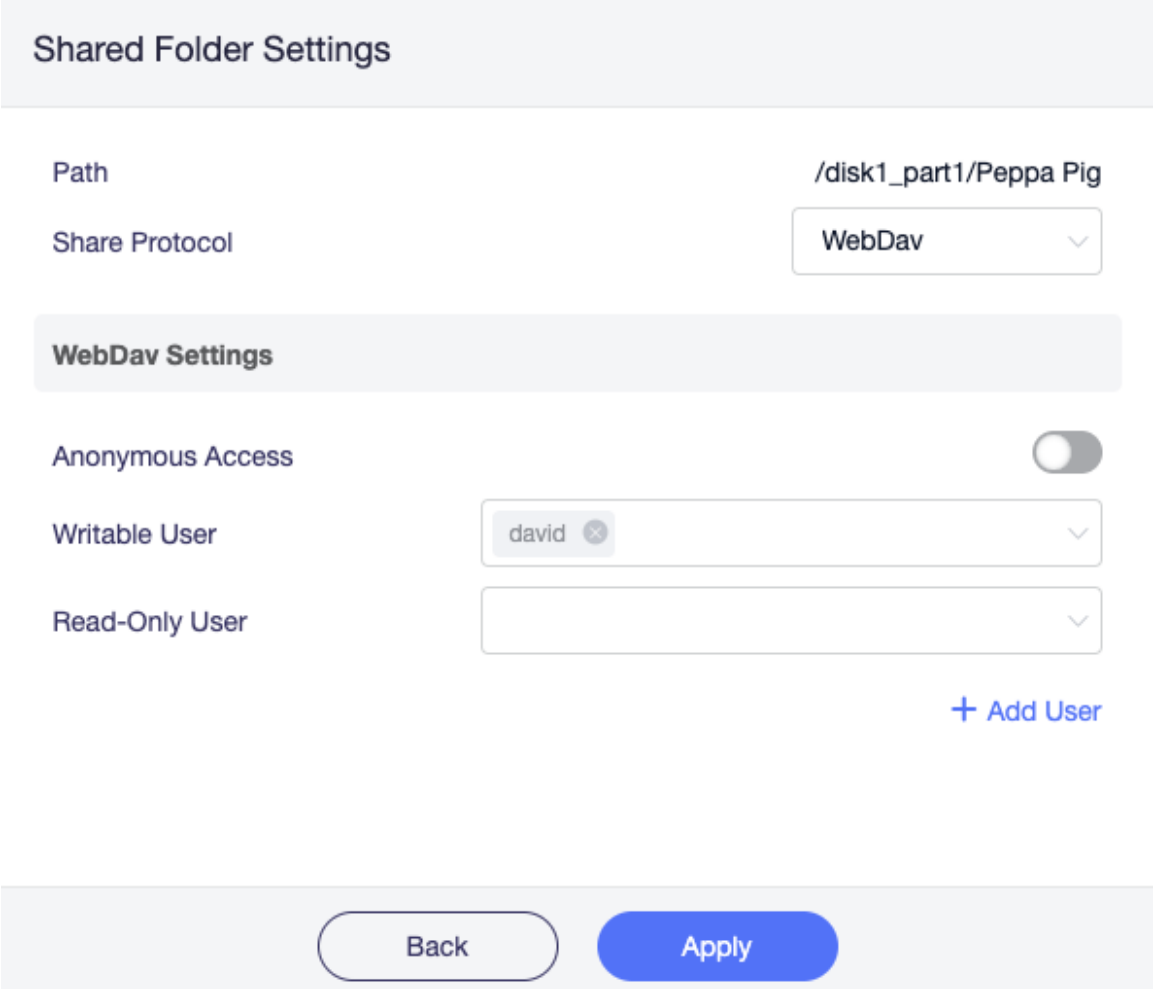


Select the **Share Protocol** as **WebDAV**.

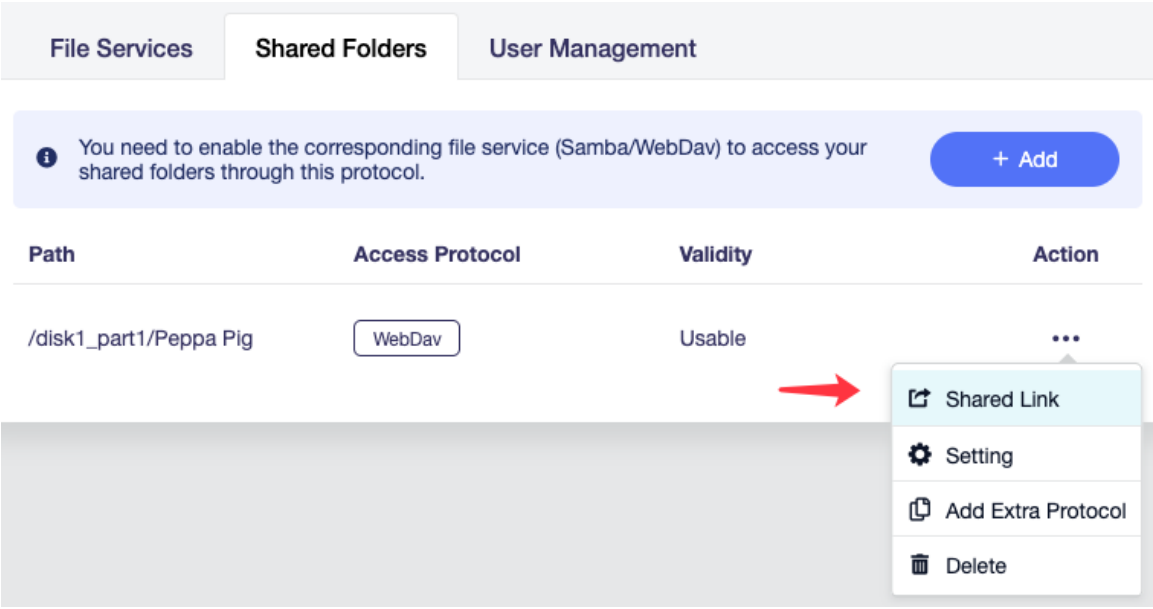
For security reasons, we do not recommend enabling **Anonymous Access**.

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.



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



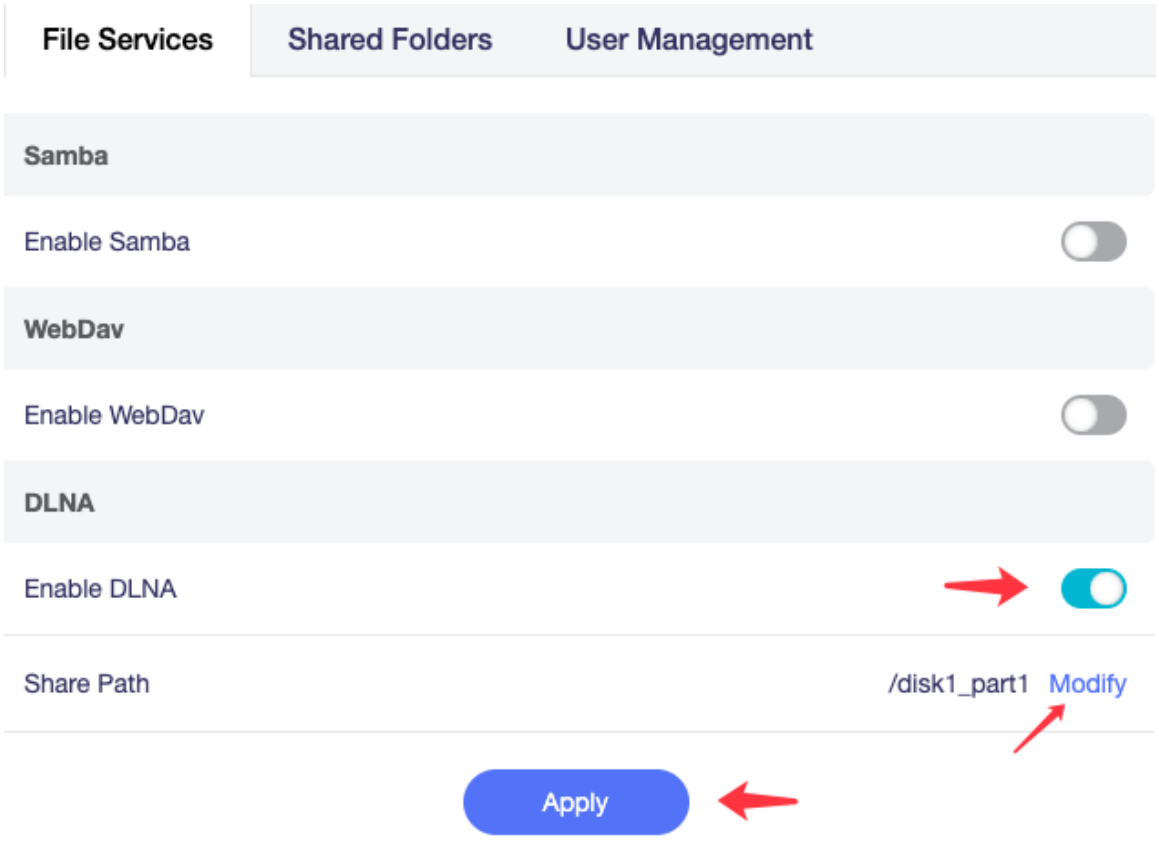
Click **Shared Link**, it will show the access link for each system. The Unix-like system include Android, iOS, macOS, Ubuntu etc.

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.

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.



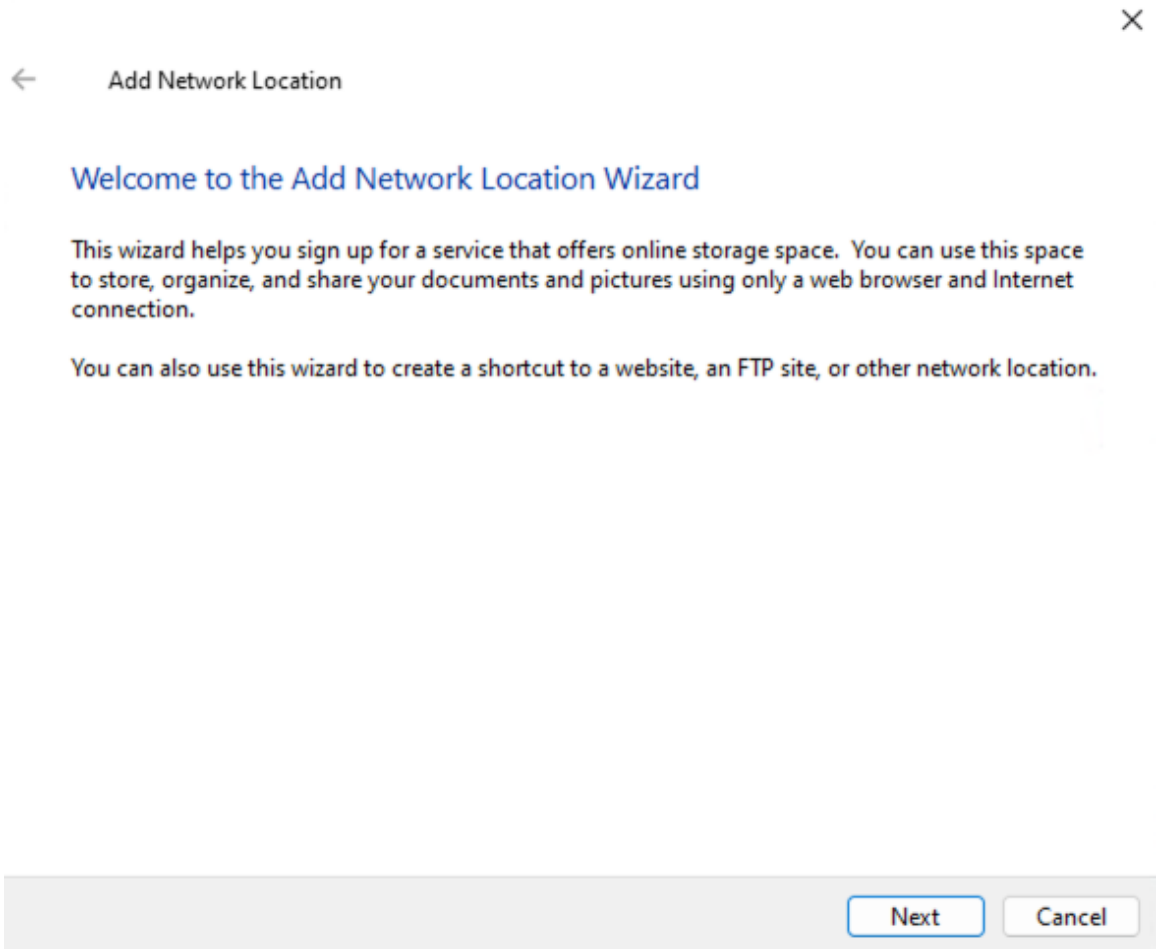
Connect your smart TV to the router, it will find the DLNA Server.

Samba Client

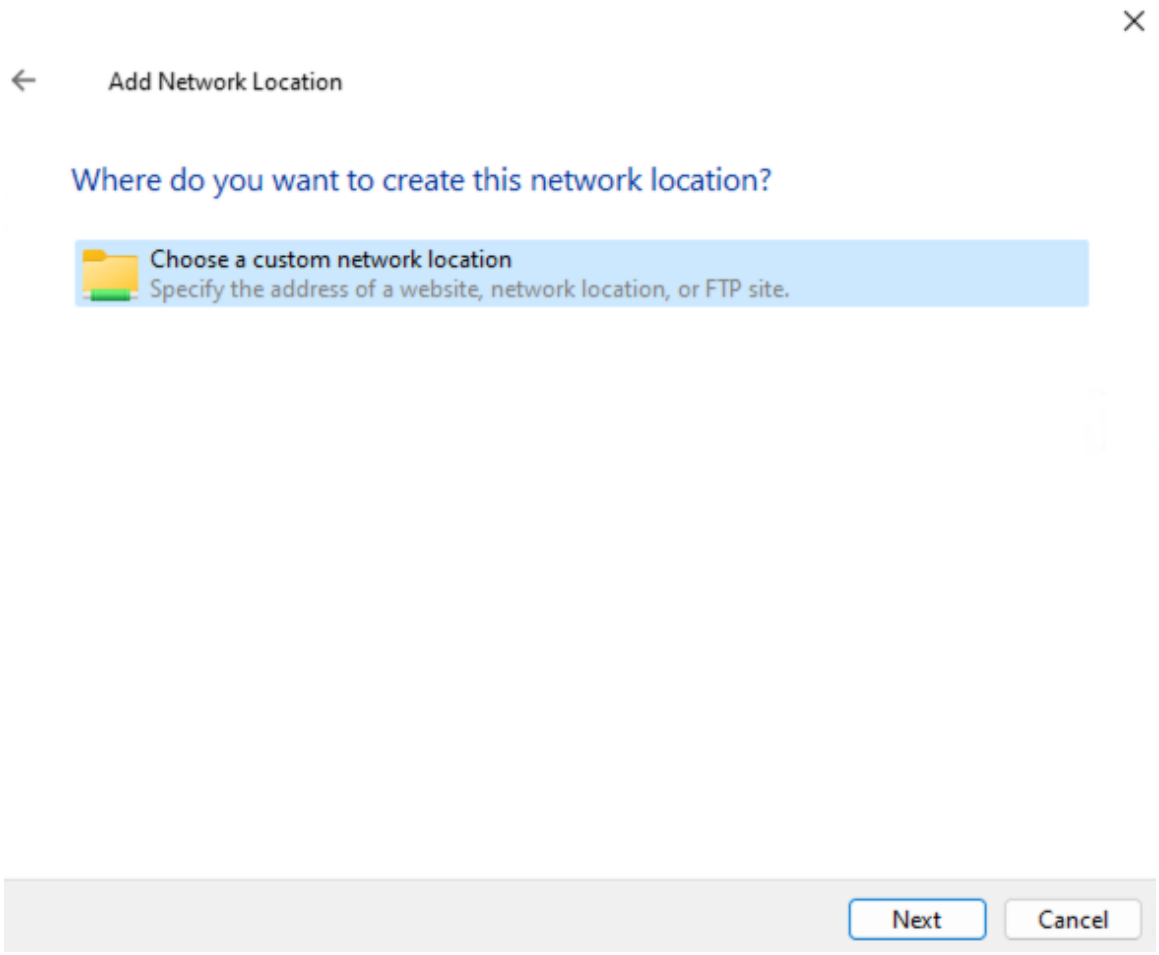
Windows

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

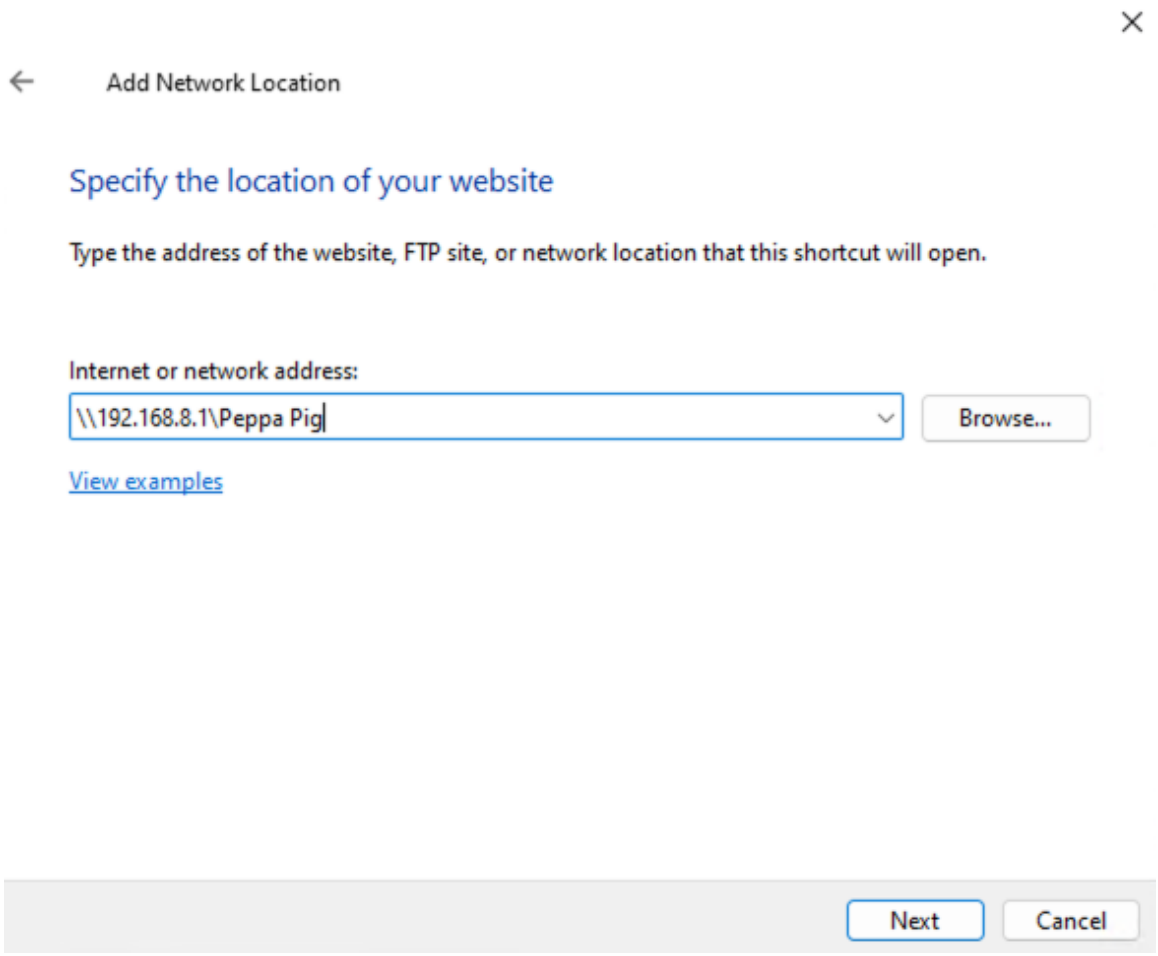
Open up File Explorer and then right-click on **This PC** (in the left pane). From the resulting context menu, select **Show more options** -> **Add a network location**



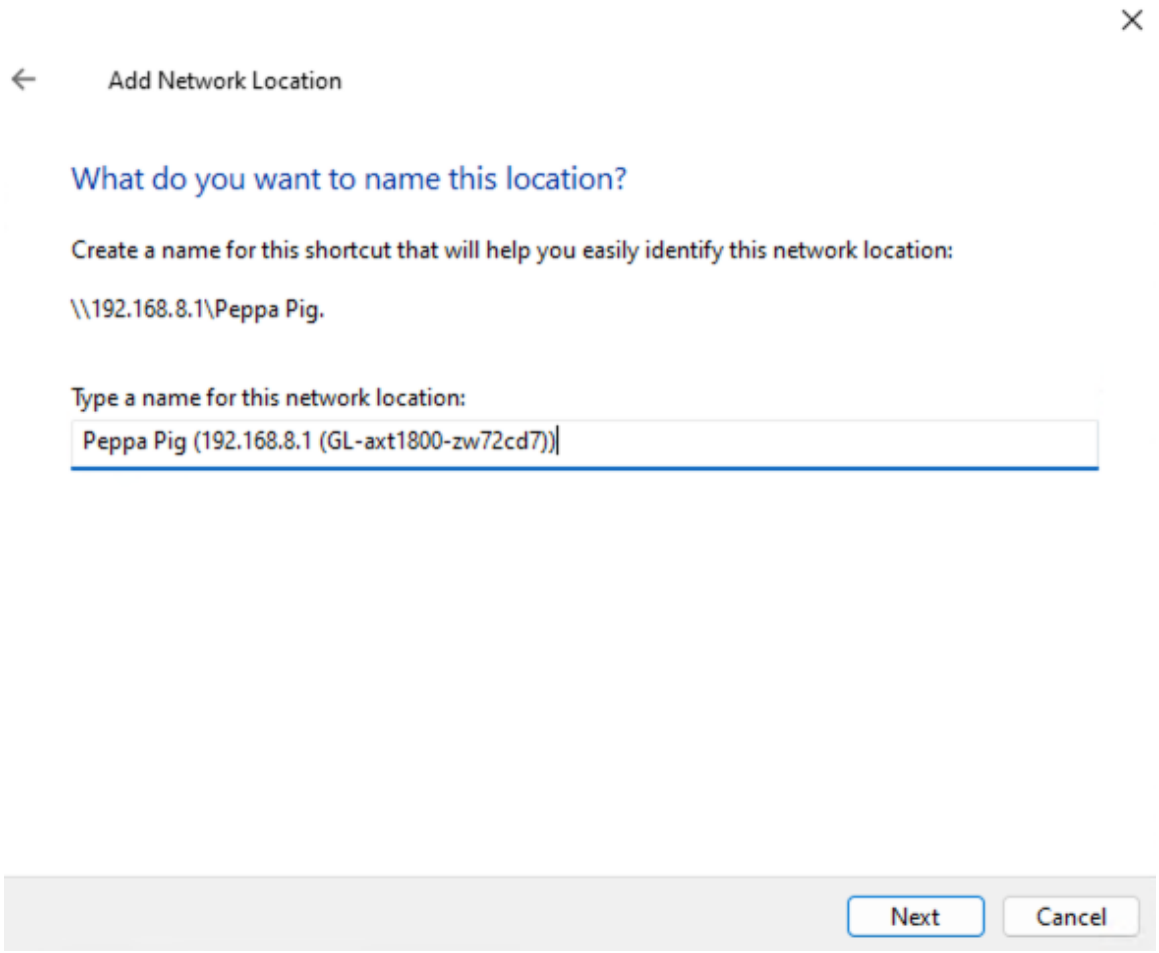
Click **Choose a custom network location** and then click **Next**.



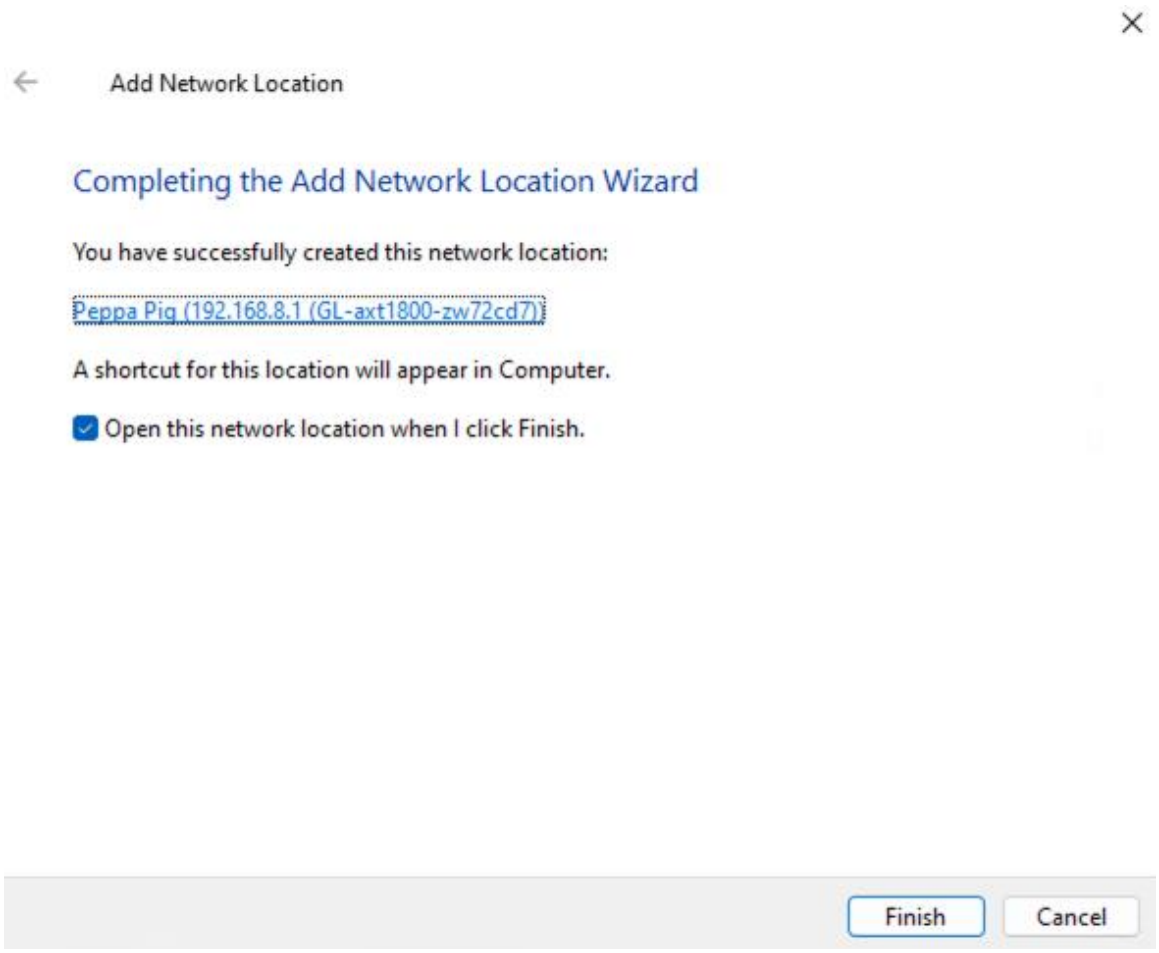
Enter the Samba access link. Then click **Next**.



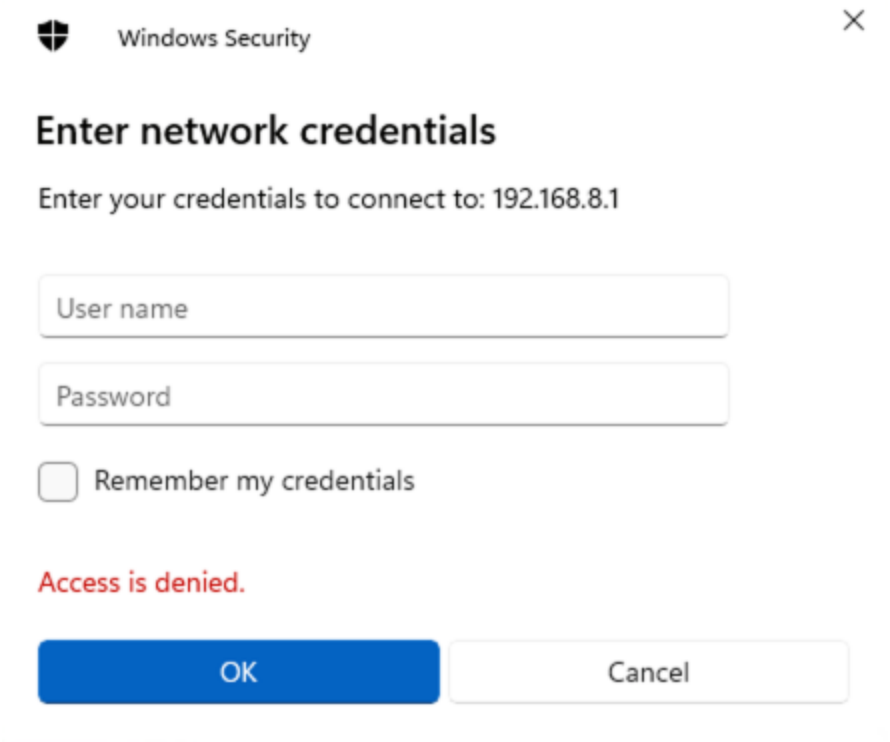
Give a name of this location. Click **Next**.



Click **Finish**.



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



Mac OS Android iOS

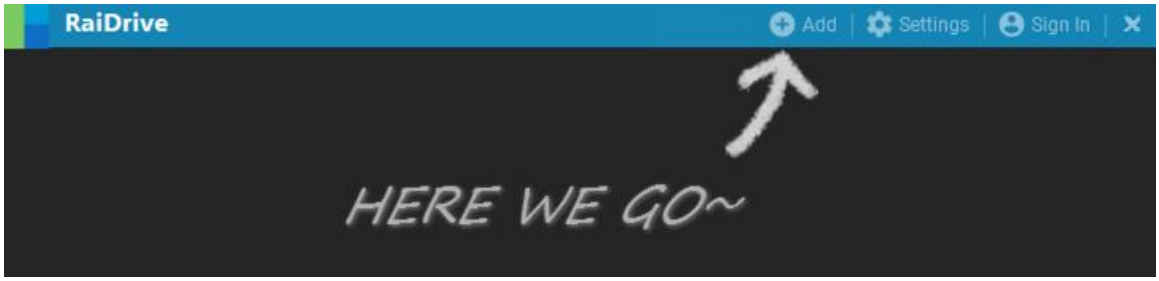
WebDAV Client

Windows

There is a lot of software that supports WebDAV, for example RaiDrive, Cyberduck, WinSCP.

Here is an example of RaiDrive.

Click **Add**.

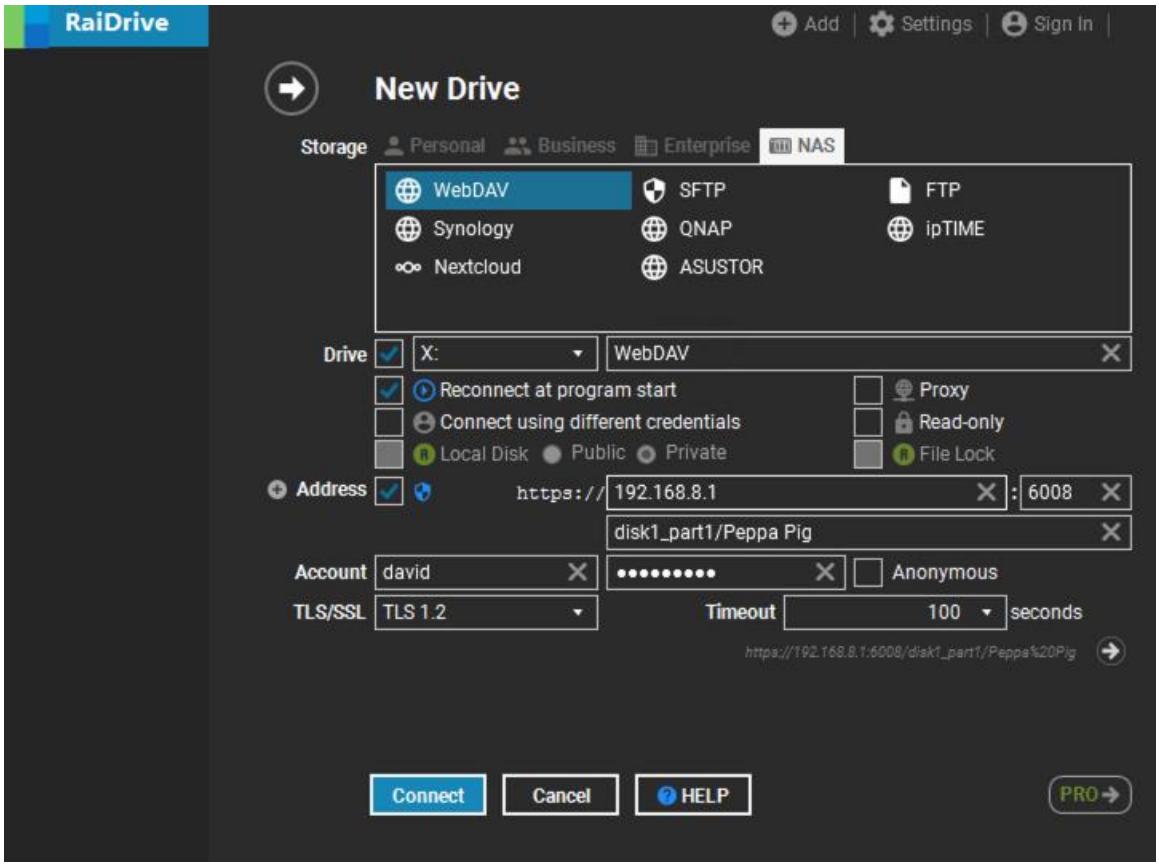


In the **Storage** area, click **NAS** -> **WebDAV**.

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.

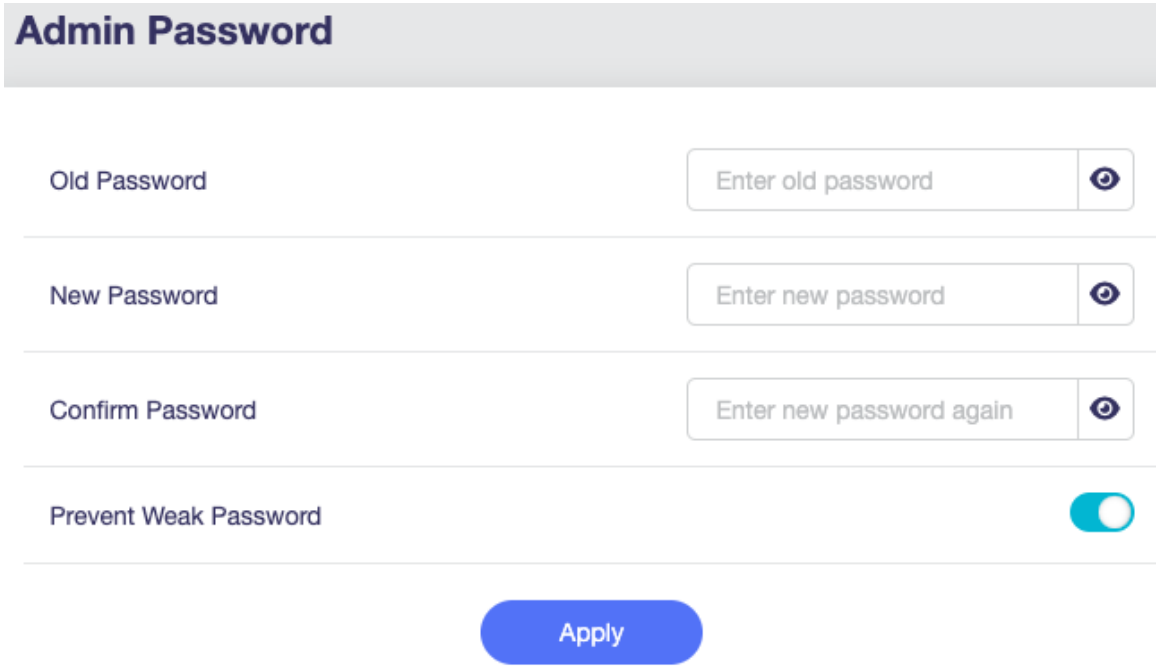
Click **Refresh** to get the latest log information.

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.

9. MORE SETTINGS

9.1 Admin Password

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



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

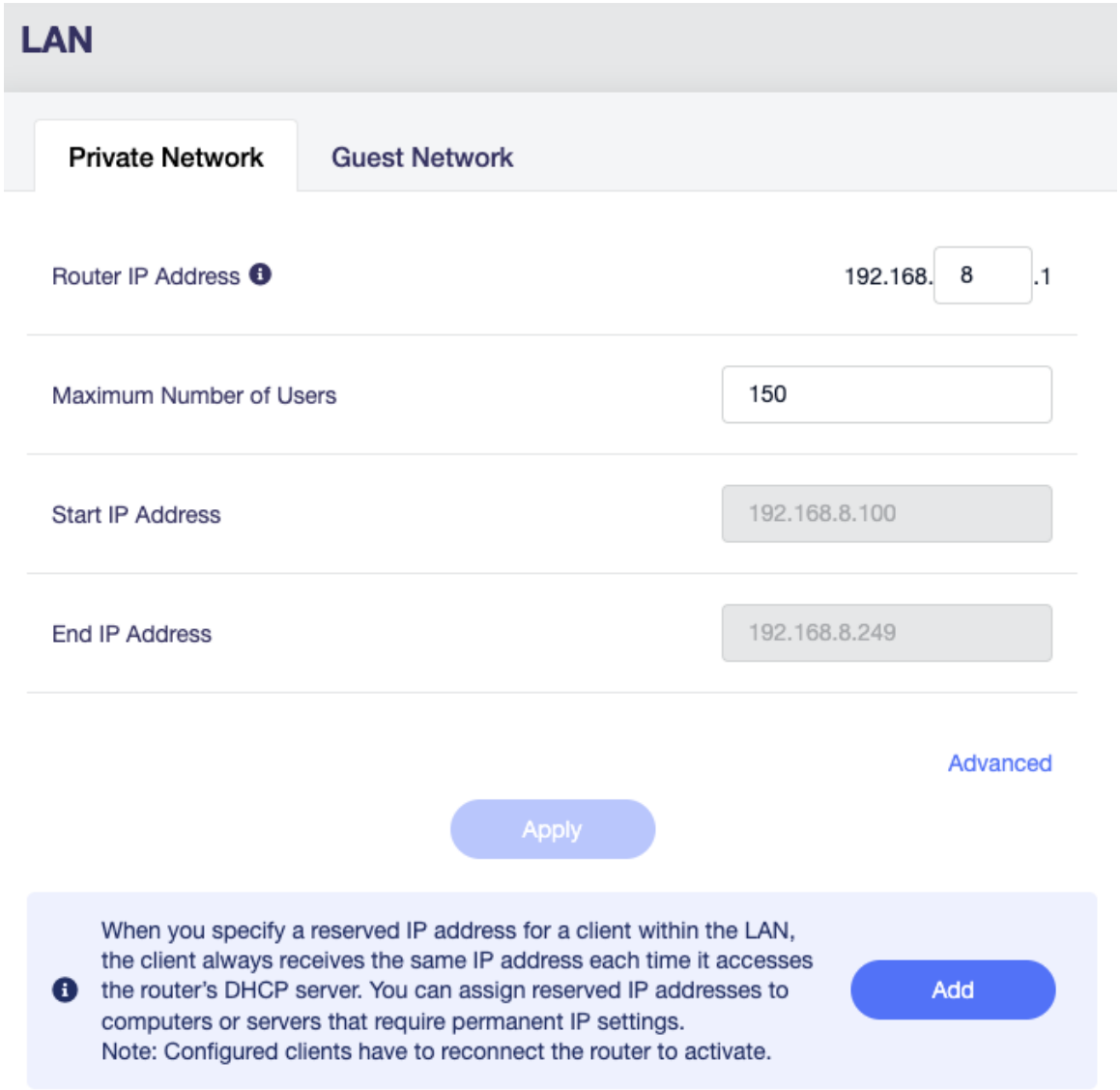
For security reasons, we recommend that you turn on **Prevent Weak Password**.

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

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

9.2 LAN

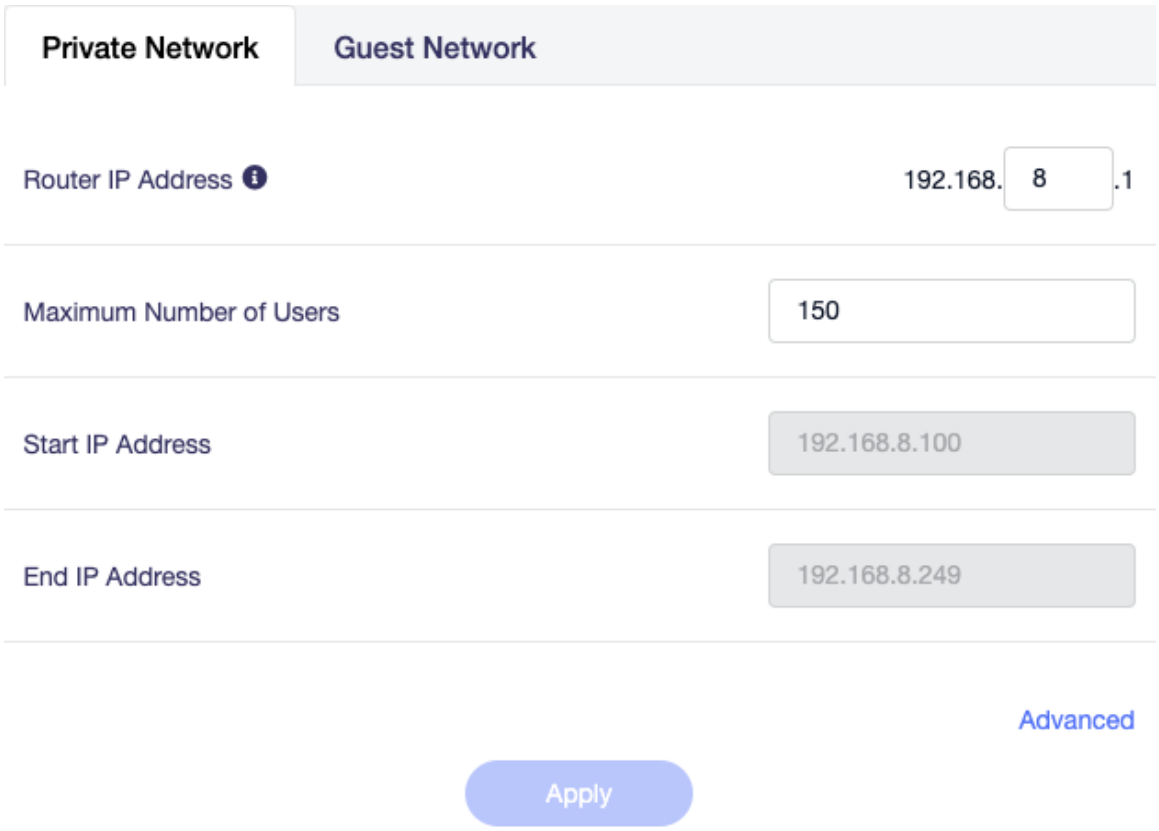
On the left side of web Admin Panel -> MORE SETTINGS -> LAN



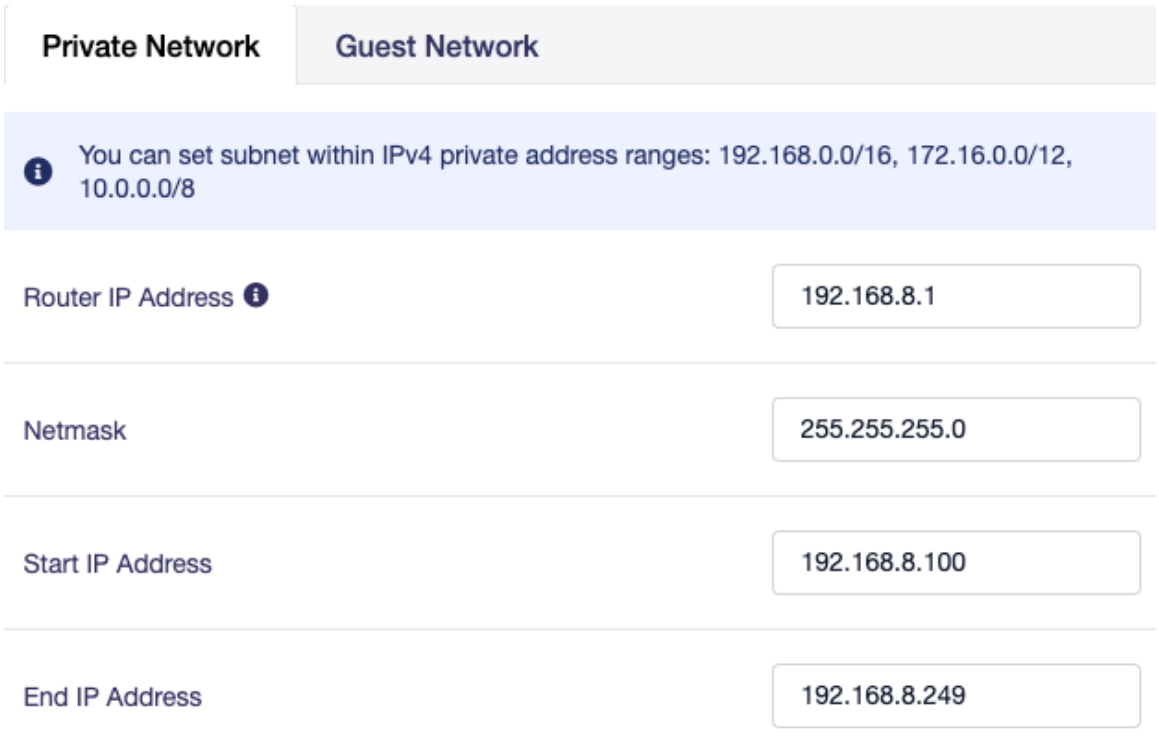
Private Network

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.



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

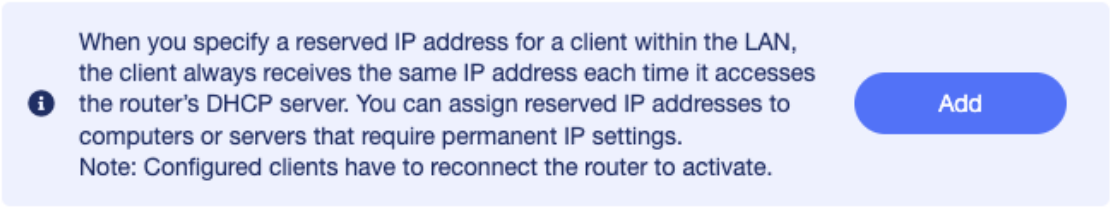


Reserve an IP for a client

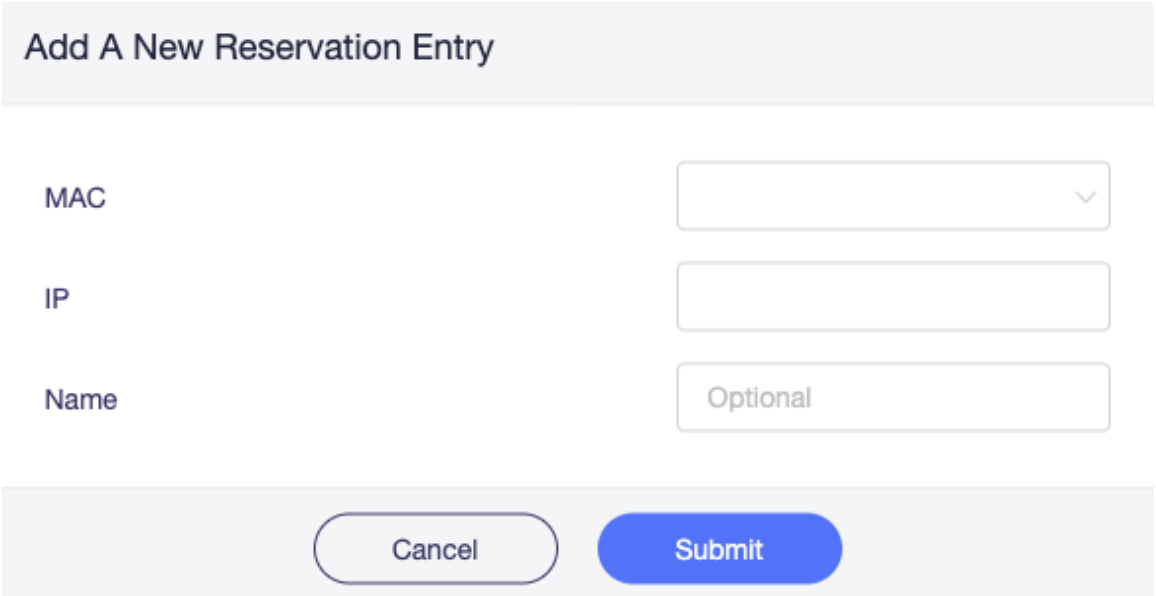
When you specify a reserved IP address for a client within the LAN, the client always receives the same IP address each time it accesses the router's DHCP server. You can assign reserved IP addresses to computers or servers that require permanent IP settings.

Note: Configured clients have to reconnect the router to activate.

Click **Add** to reserve an IP.



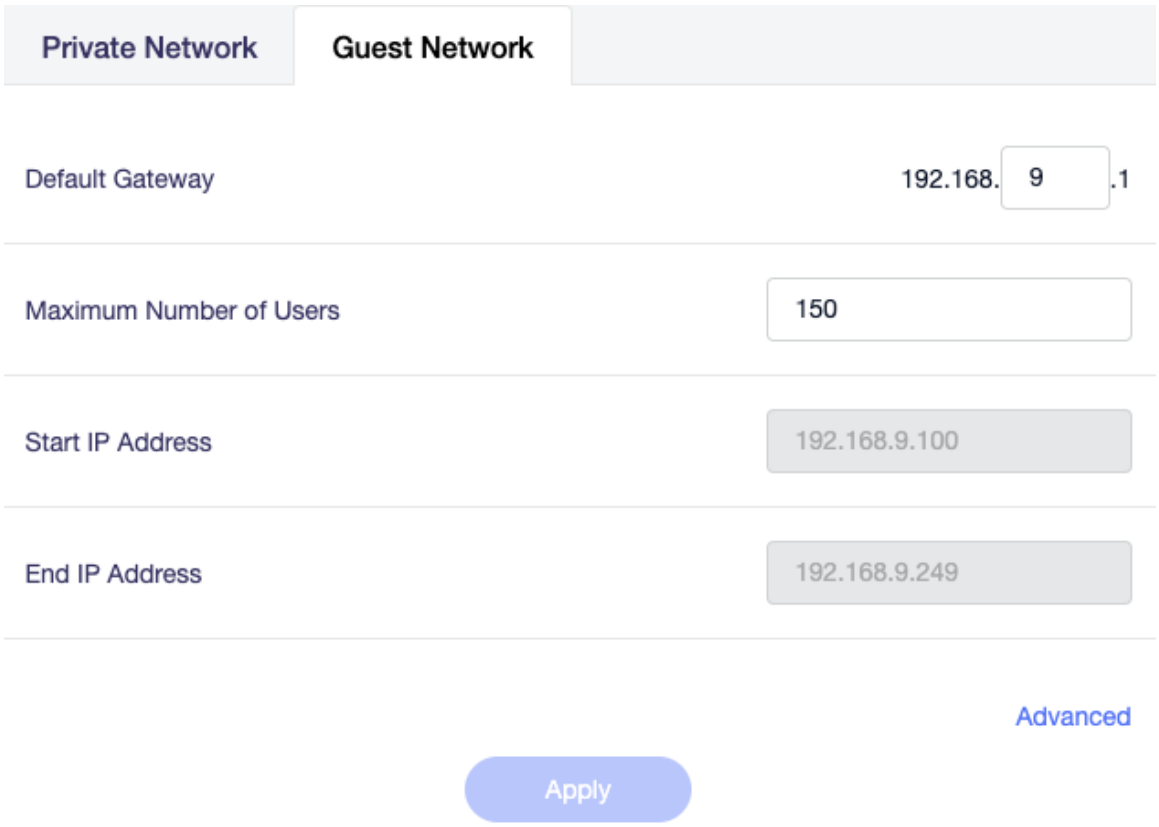
Select the **MAC**, it will fill the **IP** automatically after select MAC. Give it a descriptive name. Then click **Submit**.



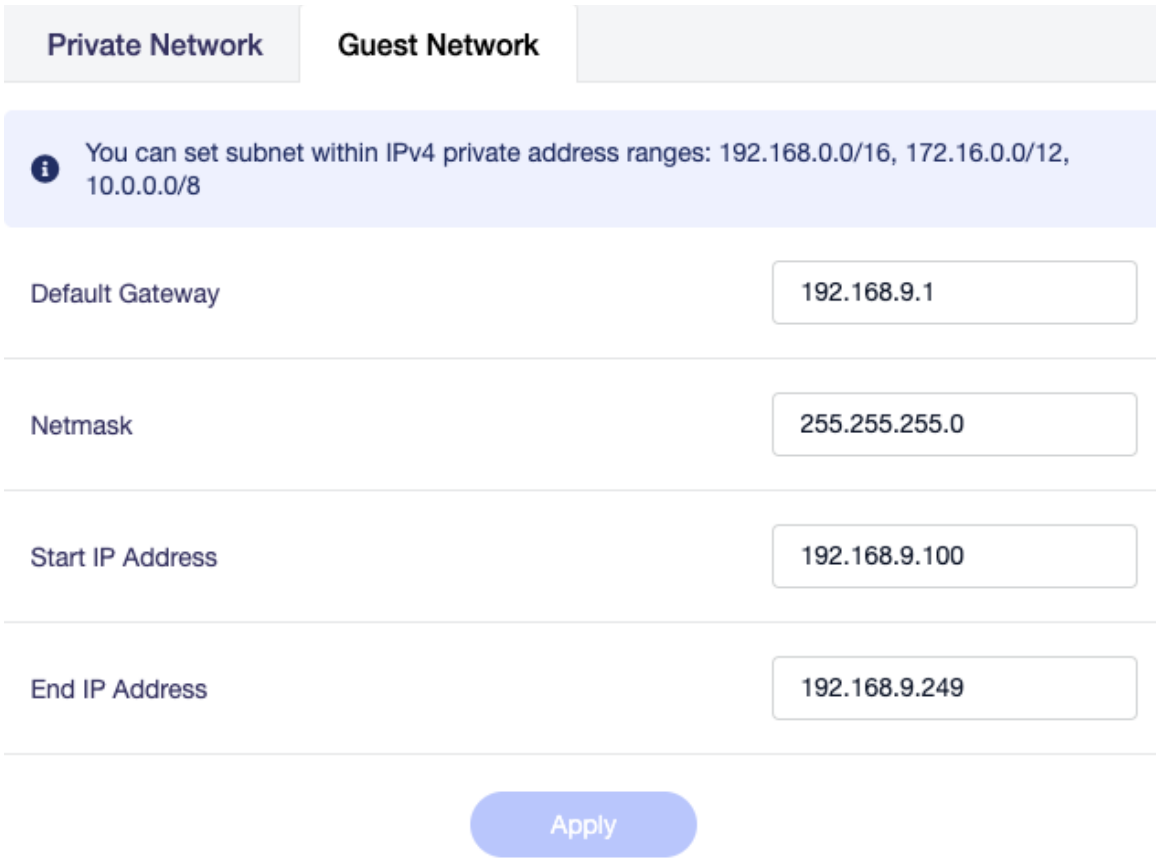
Guest Network

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

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



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

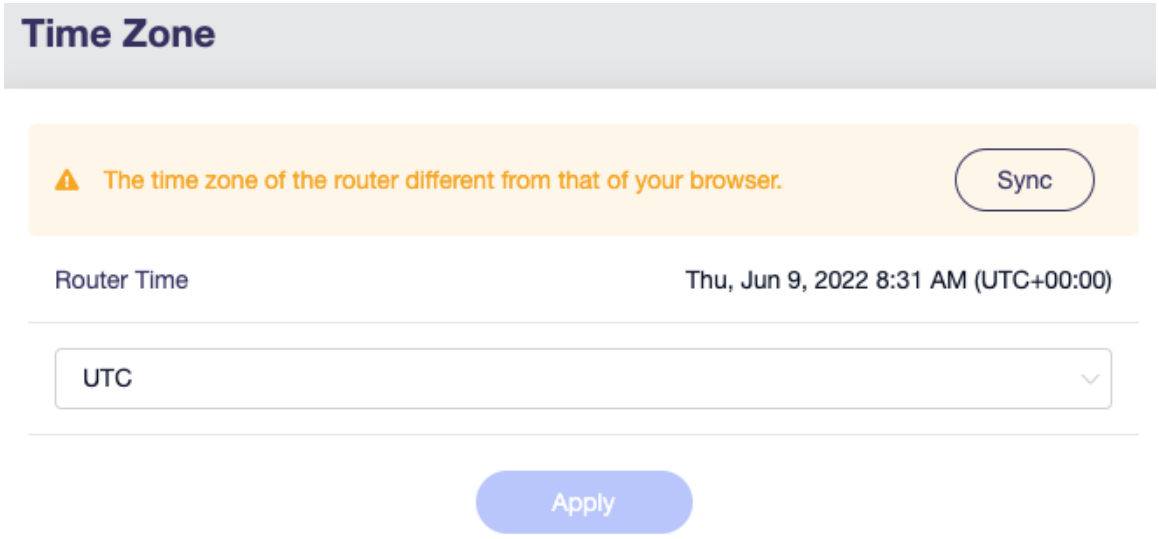

Private Network
Guest Network
You can set subnet within IPv4 private address ranges: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
Default Gateway
192.168.9.1
Netmask
255.255.255.0
Start IP Address
192.168.9.100
End IP Address
192.168.9.249
Apply

9.3 Time Zone

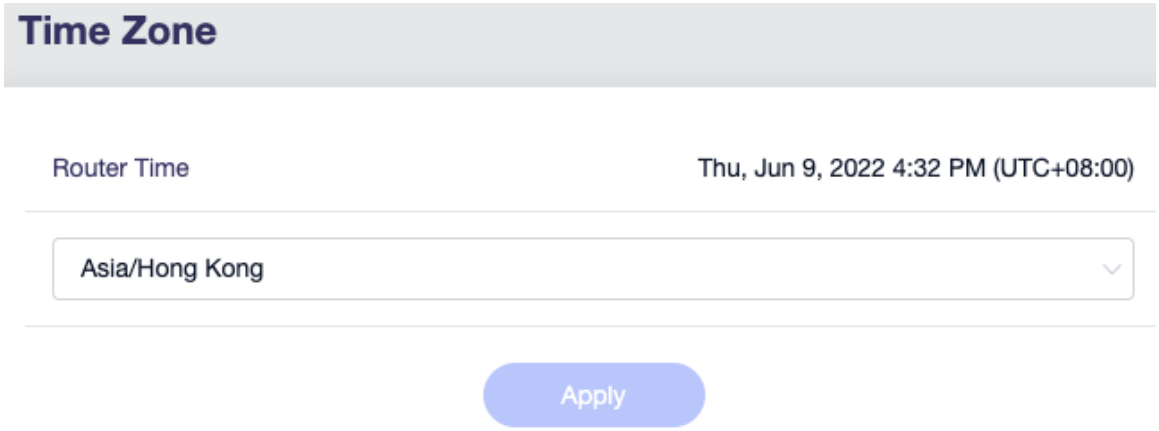
On the left side of web Admin Panel -> MORE SETTINGS -> Time Zone

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.



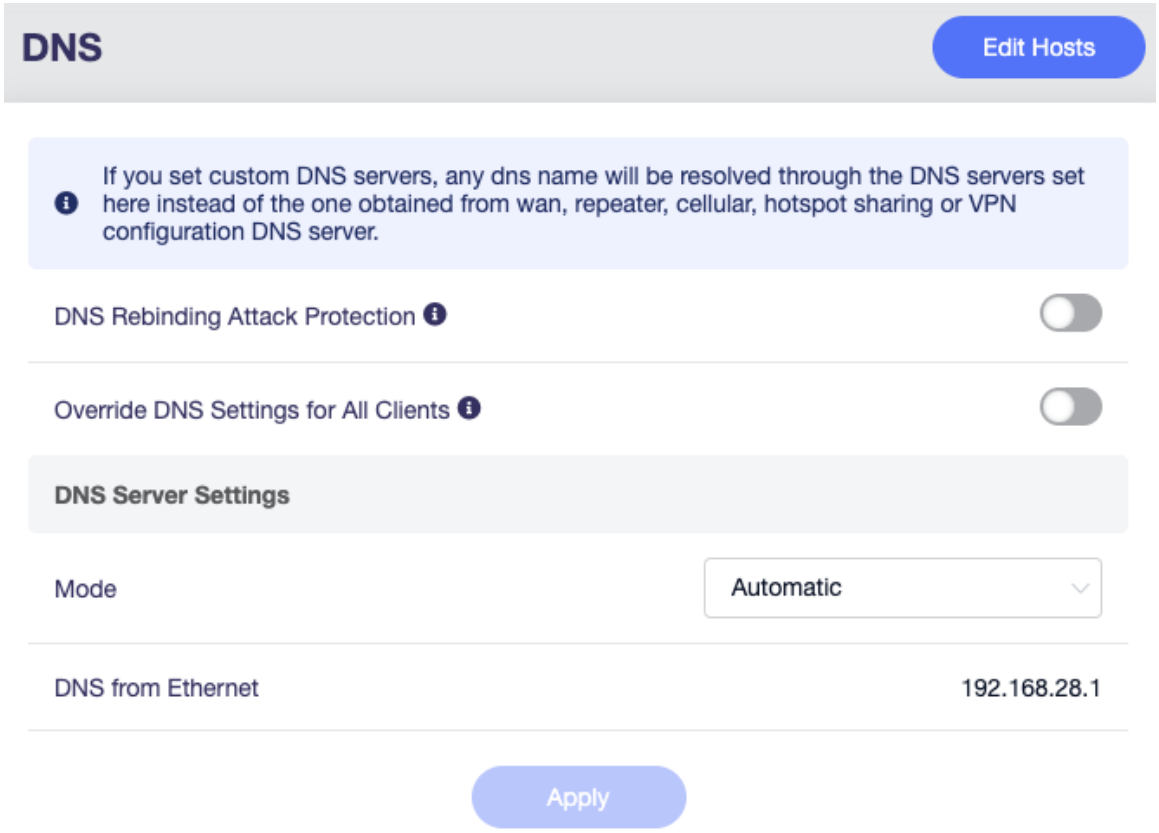
After synchronization.



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.



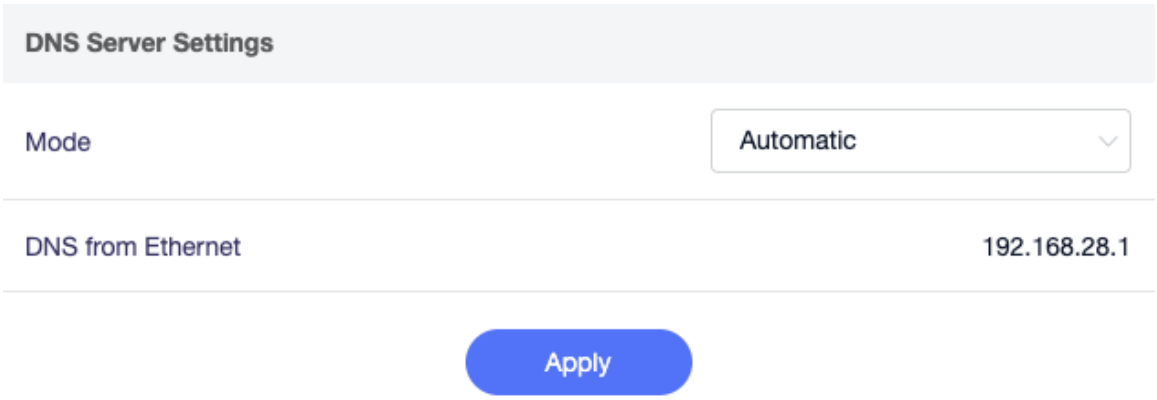
DNS Rebinding Attack Protection: Turning on this option may cause private DNS lookup failure. If your network has a captive portal please disable this option.

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

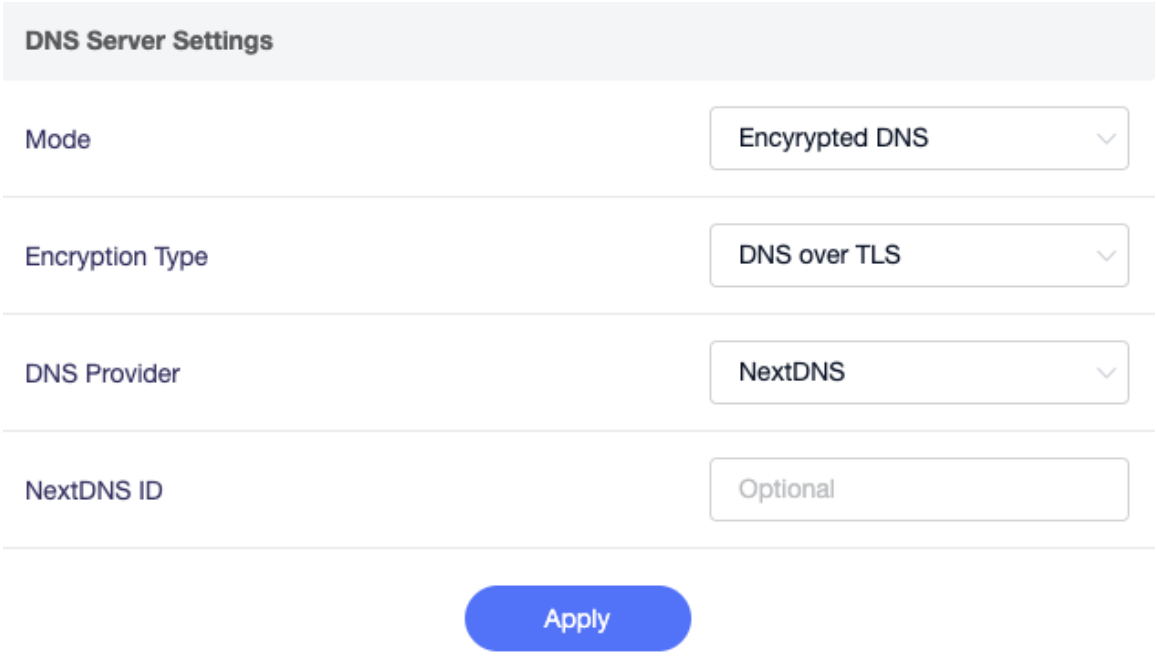
DNS Server Settings

There are four modes.

- Automatic, use the gateway of the parent router.

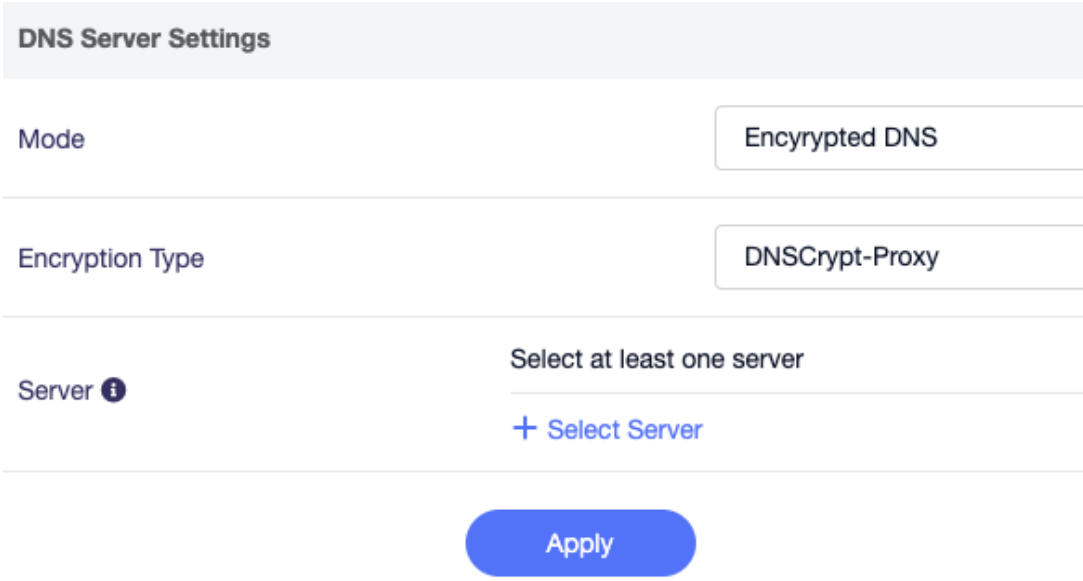


- Encrypted DNS

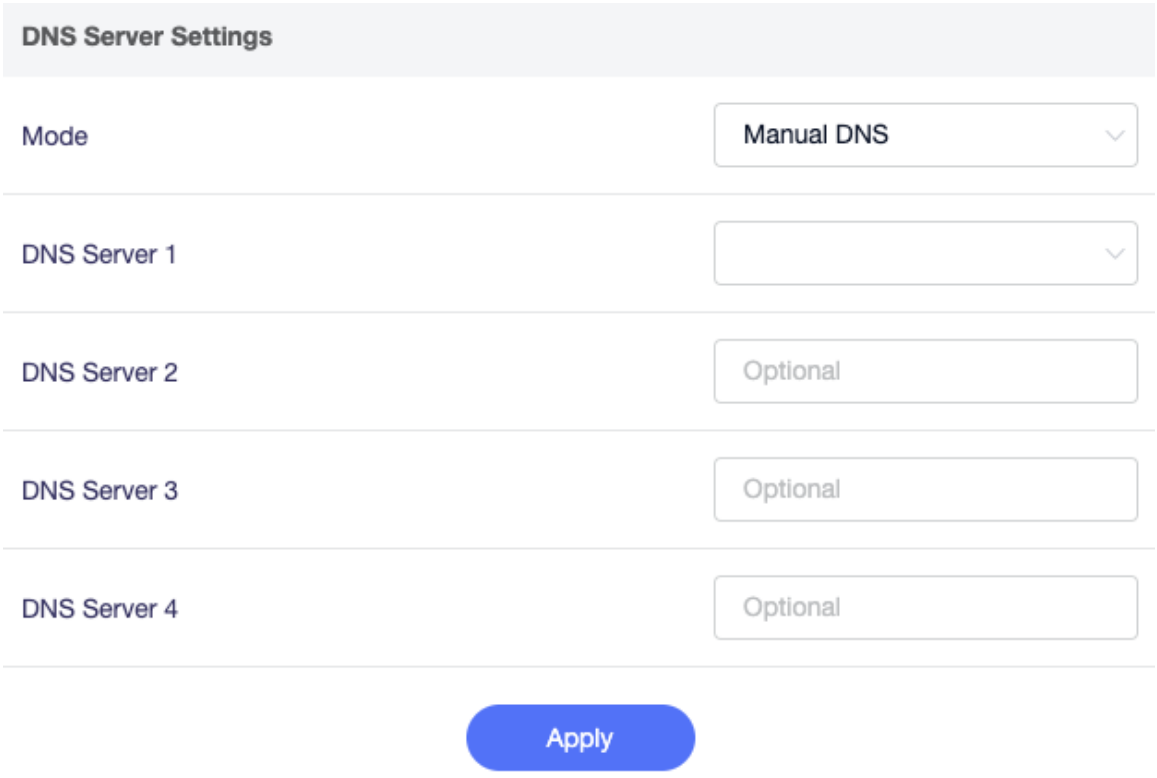


Encrypted Type has four type, DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS, Oblivious DNS over HTTPS.

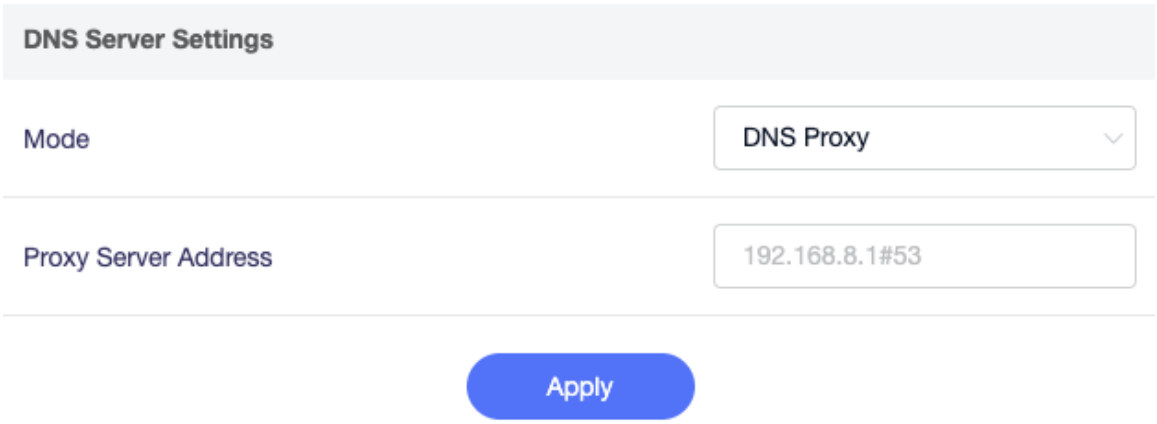
- For DNS over TLS, the DNS Provider has two options, NextDNS and Cloudflare.
- For DNSCrypt-Proxy, DNS over HTTPS and Oblivious DNS over HTTPS, they can select DNS Server.



- Manual DNS

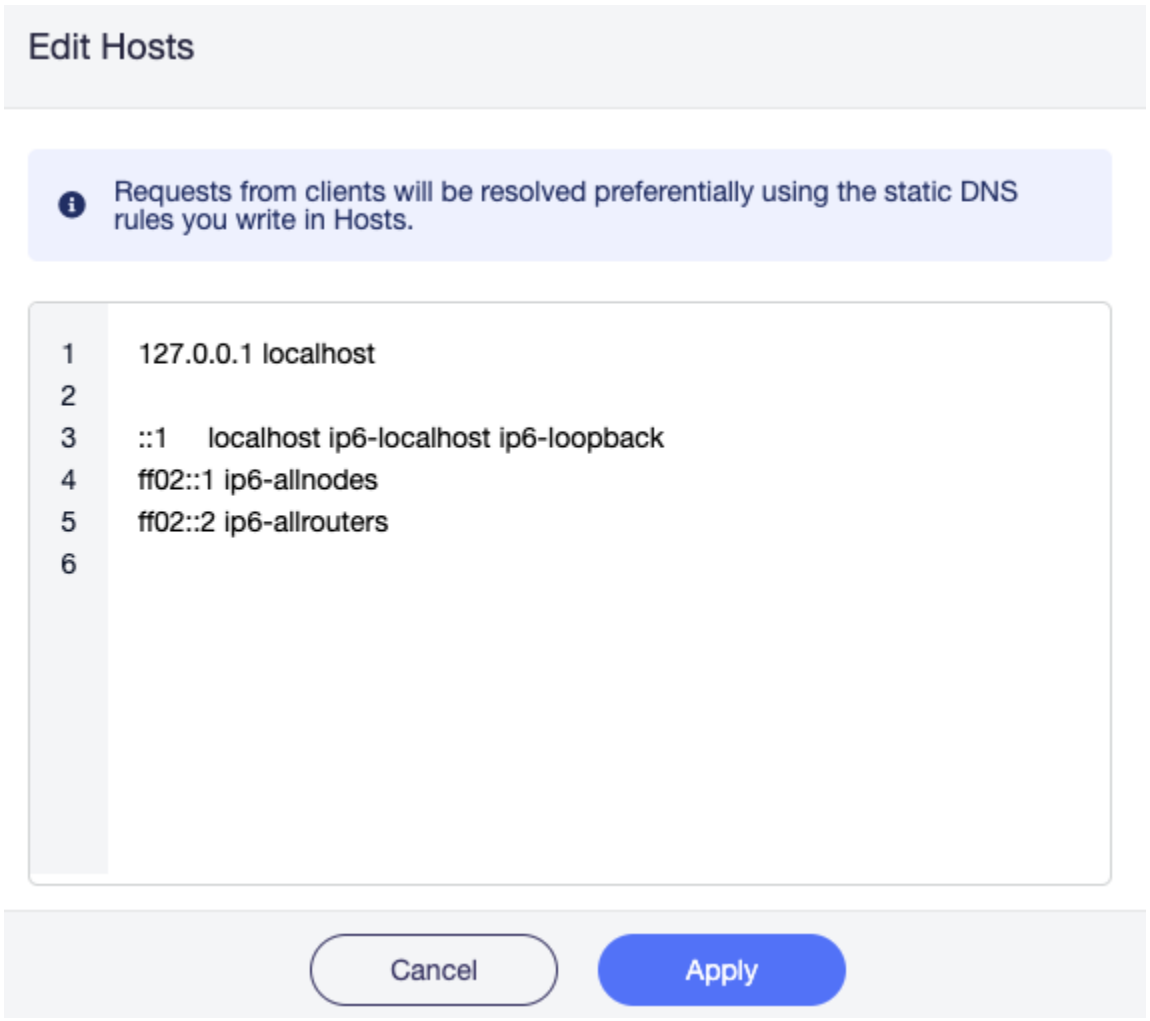


- DNS Proxy



Edit Hosts

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



9.5 Network Mode

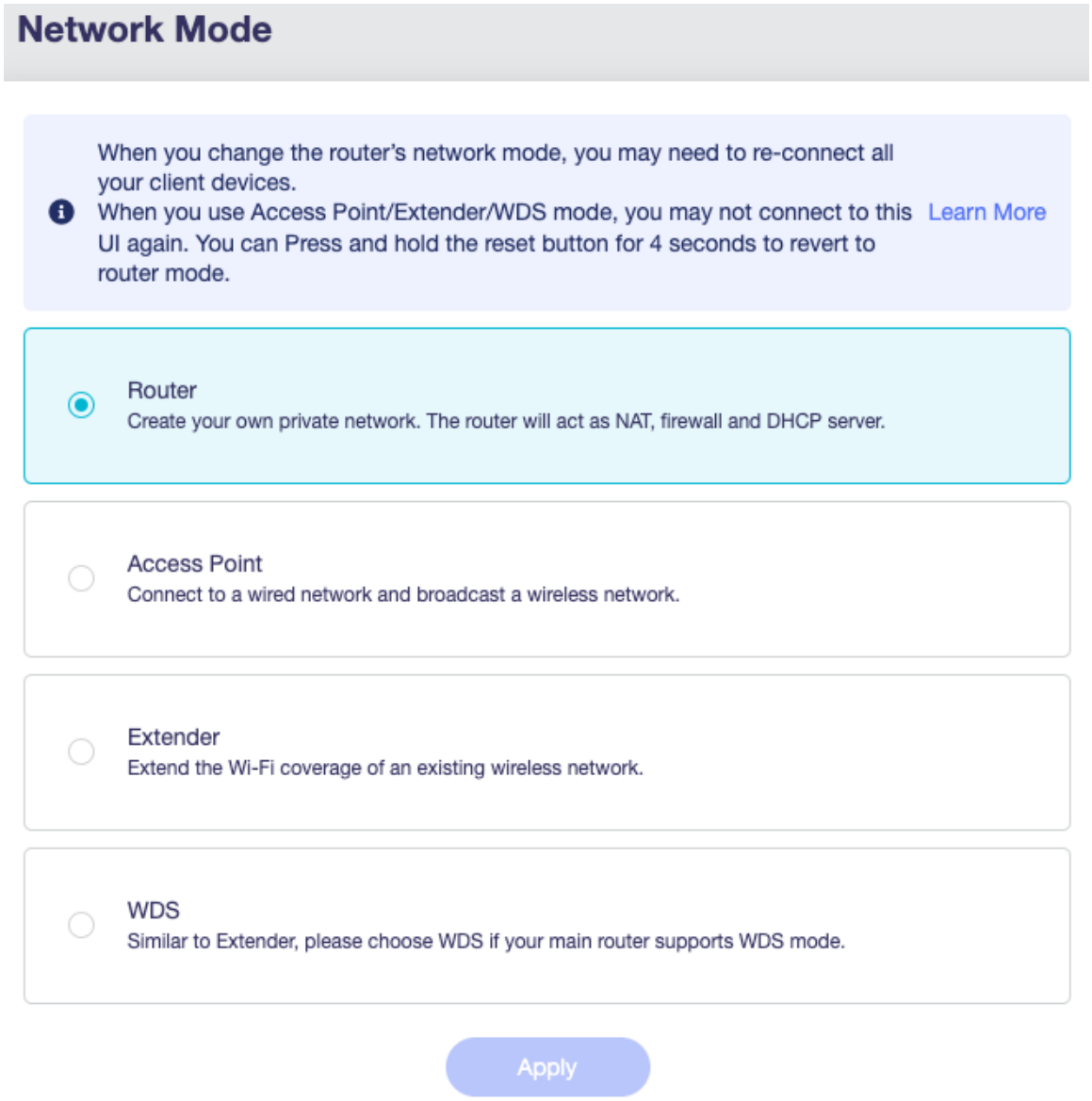
On the left side of web Admin Panel -> MORE SETTINGS -> Network Mode

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.

Here is an example of GL-AXT1800.

Note: some models do not support WDS mode.

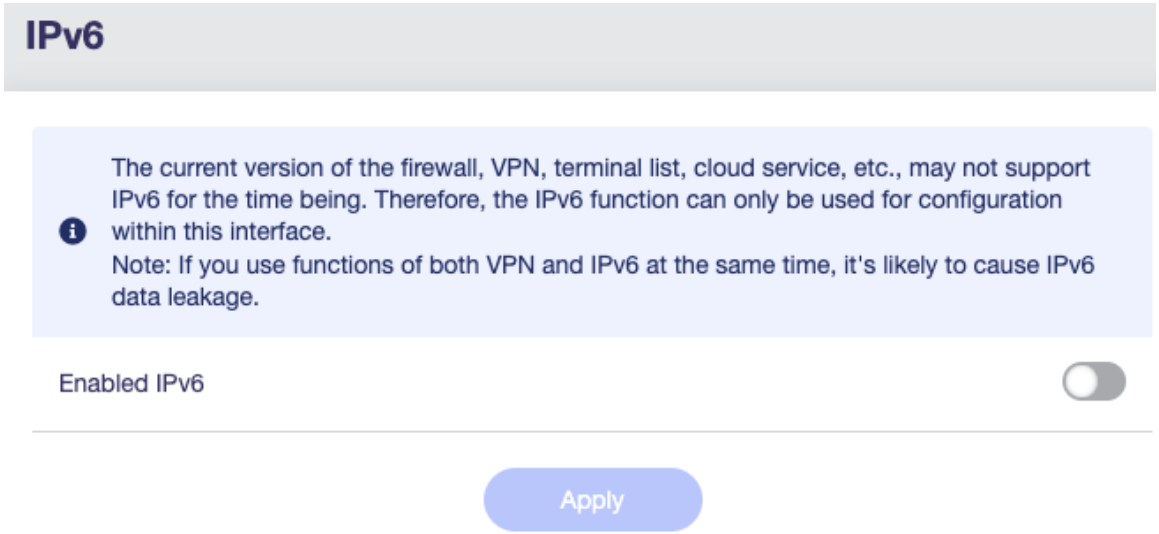


- Router. Create your own private network. The router will act as NAT, firewall and DHCP server. This is the default mode.
- Access Point. Connect to a wired network and broadcast a wireless network.
- Extender. Extend the Wi-Fi coverage of an existing wireless network.
- WDS. Similar to Extender, please choose WDS if your main router supports WDS mode.

9.6 IPv6

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

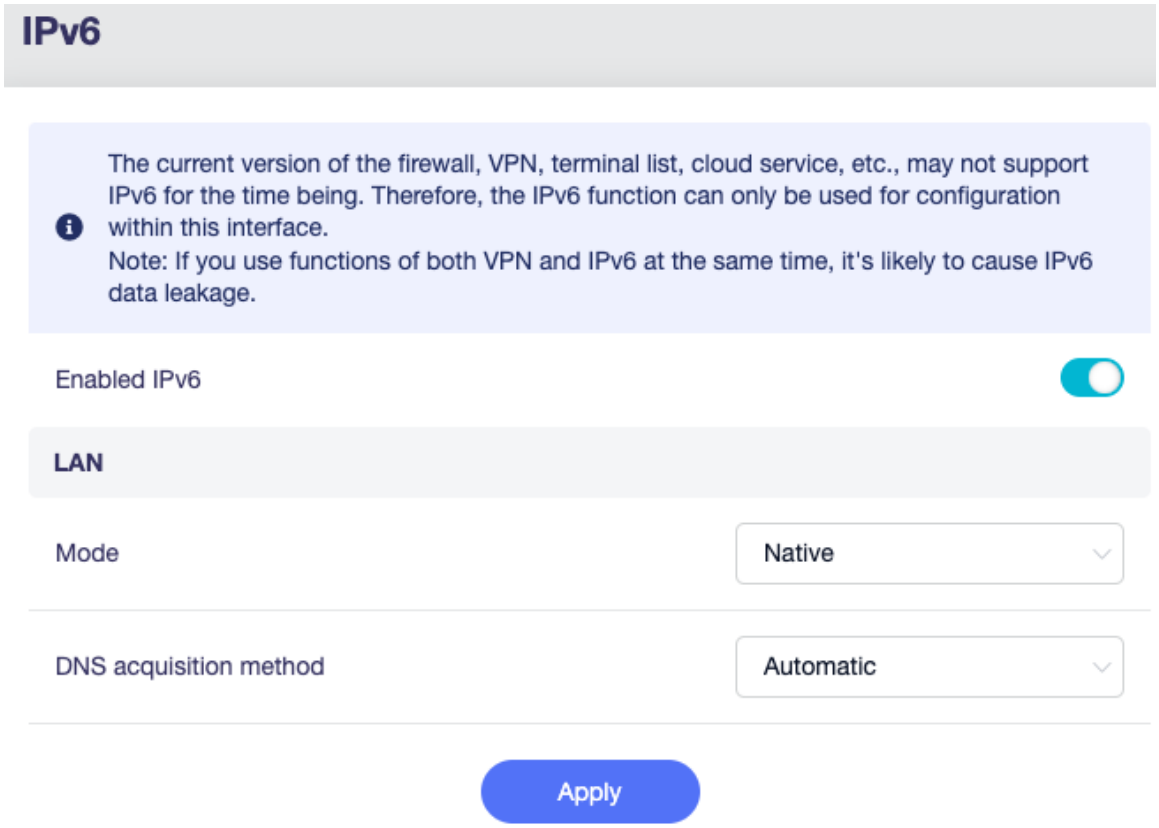
The IPv6 function allows you to enable and configure IPv6 on router.



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.

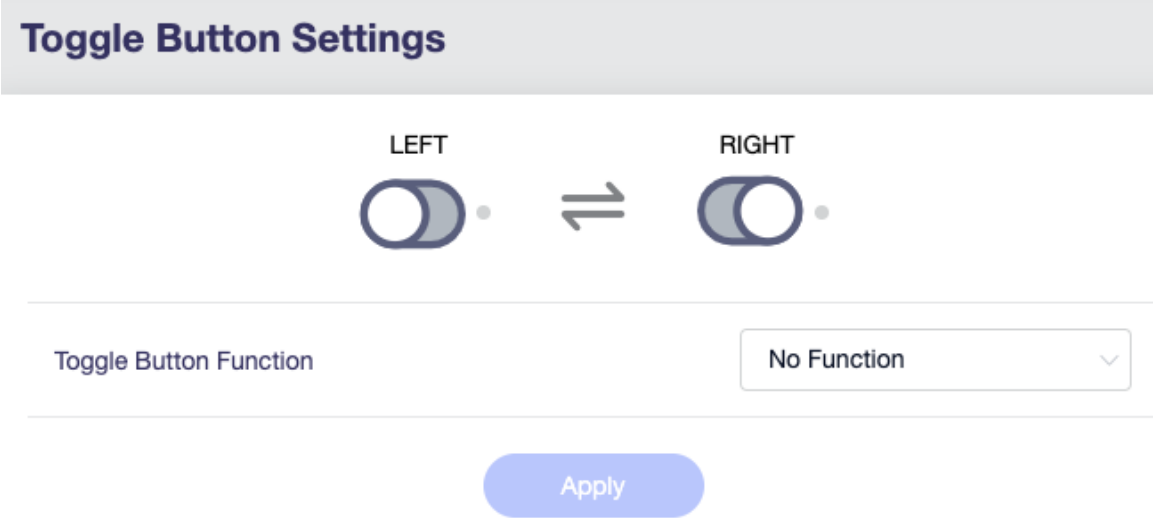


- **Mode**. There are three modes, **NAT6**, **Native** and **Static IPv6**.
- **DNS acquisition method**. It has two options. **Automic** and **Manual**.

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



There are four options.

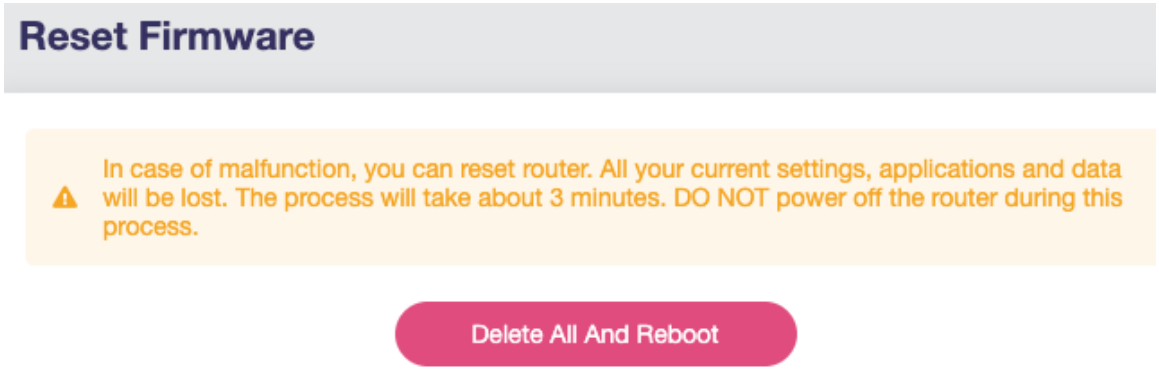
- No Function.
- AdGuard Home (On/Off)
- OpenVPN Client (On/Off)
- WireGuard Client (On/Off)

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.



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.