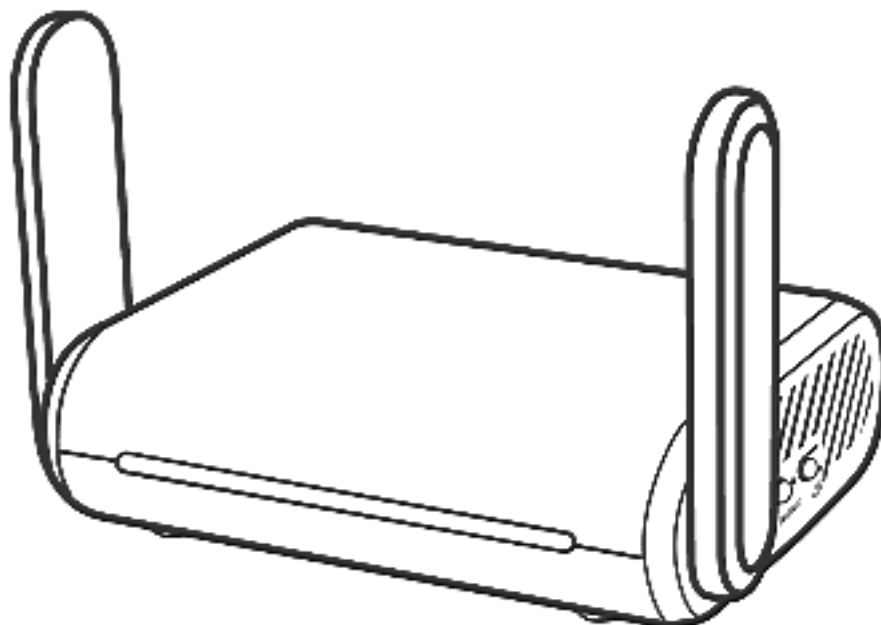


GL·iNet



Opal

(GL-SFT1200)
USER MANUAL

Table of Contents

1. Getting Started with GL.iNet Opal.....	1
1.1. Power on.....	1
1.2. Connect.....	2
(1) Connect via LAN.....	2
(2) Connect via Wi-Fi	3
1.3. Access the Web Admin Panel	3
(1) Language Setting.....	4
(2) Admin Password Setting.....	4
(3) Admin Panel	5
2. INTERNET	6
2.1. Cable.....	8
(1) DHCP	9
(2) Static.....	9
(3) PPPoE.....	10
2.2. Repeater.....	11
2.3. USB 3G/4G Modem	12
Compatible Modems.....	14
2.4. Tethering.....	15
EasyTether.....	17
3. WIRELESS	17
4. CLIENTS.....	21
5. UPGRADE	24
5.1. Online Upgrade	24
5.2. Upload Firmware.....	24
(1) Official OpenWrt/LEDE firmware.....	25
(2) Compile your own firmware.....	26
(3) Third party firmware	26
5.3. Auto Upgrade.....	26
6. FIREWALL	27
6.1. Port Forwards.....	27
6.2. Open Ports on Router	28

6.3.	DMZ.....	28
7.	VPN.....	29
7.1.	OpenVPN	29
7.1.1.	OpenVPN Client	29
7.1.2.	OpenVPN Server	37
7.2.	WireGuard	41
7.2.1.	WireGuard Client.....	41
7.2.2.	WireGuard Providers	44
7.2.3.	WireGuard Server	47
7.2.4.	Wireguard App Support.....	49
7.2.5.	Visit Client's LAN Subnet.....	50
7.3.	VPN Policies	50
7.3.1.	Settings.....	51
7.3.2.	Add VPN policy.....	52
7.3.3.	Clear DNS cache.....	53
8.	APPLICATIONS	53
8.1.	Plug-ins.....	54
8.2.	Internet Kill Switch	54
	Setup	55
8.3.	File Sharing.....	57
8.3.1.	Router settings.....	58
8.3.2.	Access the storage device.....	61
8.4.	DLNA Server	78
8.4.1.	Install Plug-ins	78
8.4.2.	Use the DLNA server in GL.iNet Routers	79
8.5.	DDNS	85
8.6.	Cloud	92
	Introduction.....	92
	Setup	93
	Manage your devices	101
	Site to Site	107
	Batch Setting	116
	Template Management.....	119

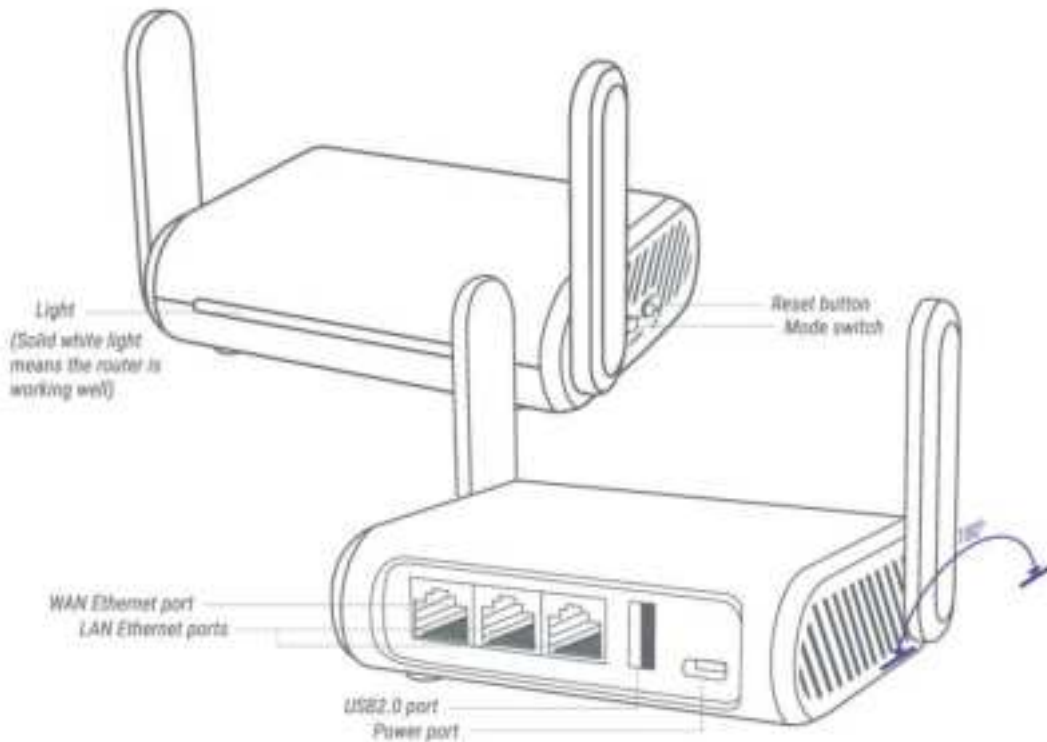
Task List	121
BLE MQTT Bridge.....	122
GoodCloud and VPN.....	122
Disable.....	123
9. MORE SETTINGS	126
9.1. Admin Password.....	126
9.2. LAN IP	127
9.3. Time Zone	127
9.4. MAC Clone	128
9.5. Custom DNS Server	129
9.6. Button Settings	129
9.7. Network Mode.....	130
9.8. Revert Firmware	131
9.9. Advanced.....	132
10.Troubleshooting.....	133
10.1 LED Indicators	133
GL-MT1300/ SFT1200	133
LED Customization.....	133
10.2 Repair or Reset	134
10.3 Debrick via Uboot	135
Windows 7 / Windows 10.....	137
Mac	138
10.4 Change WAN to LAN.....	139
10.5 Captive Portal.....	141
10.6 GL.iNet app	143
10.7 Access Web Panel	145
Check connection/router's IP address	145
Your IP address is incorrect	145
Your IP address is correct.....	145
10.8 Extensible Authentication Protocol (EAP)	146
Introduction	146
Connect via web panel.....	147
Connect via Luci	150

10.9	GoodCloud issues	152
	How to fix if my device show "Deactivated"	152

1. Getting Started with GL.iNet Opal

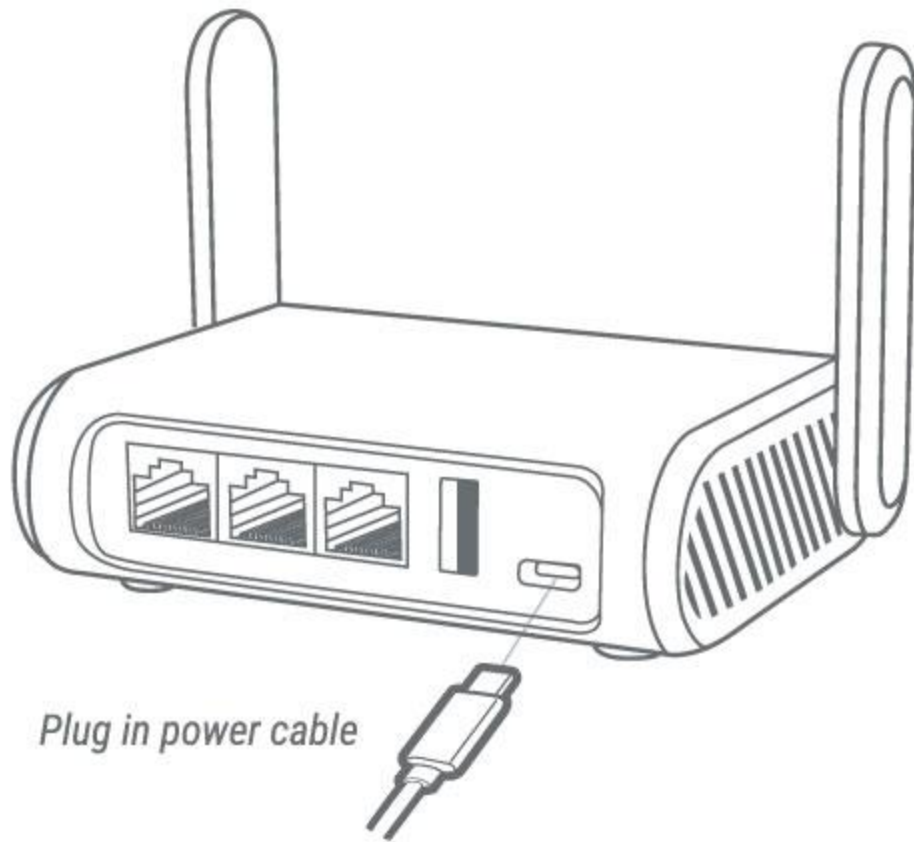
Model:

GL-SFT1200



1.1. Power on

Plug the Micro USB power cable into the power port of the router. Make sure you are using a standard **5V/3A** power adapter. Otherwise, it may cause malfunction.



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

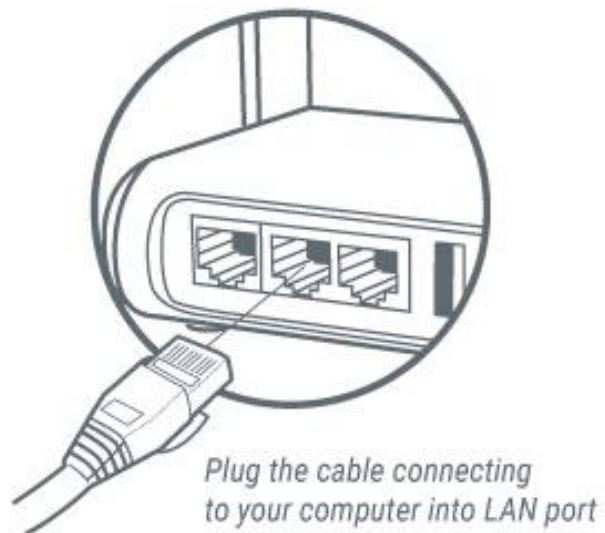
1.2. Connect

You can connect to the router via Ethernet cable or Wi-Fi.

Note: This step only connects your devices to the local area network (LAN) of the router. You cannot access the Internet currently. In order to connect to the Internet, please finish the setup procedures below and then follow Internet to set up an Internet connection.

(1) Connect via LAN

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



(2) Connect via Wi-Fi

Search for the SSID of the router in your device and input the default password: *goodlife*.

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

- **GL-SFT1200-XXX**
- **GL-SFT1200-XXX-5G**

1.3. Access the Web Admin Panel

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

(1) Language Setting

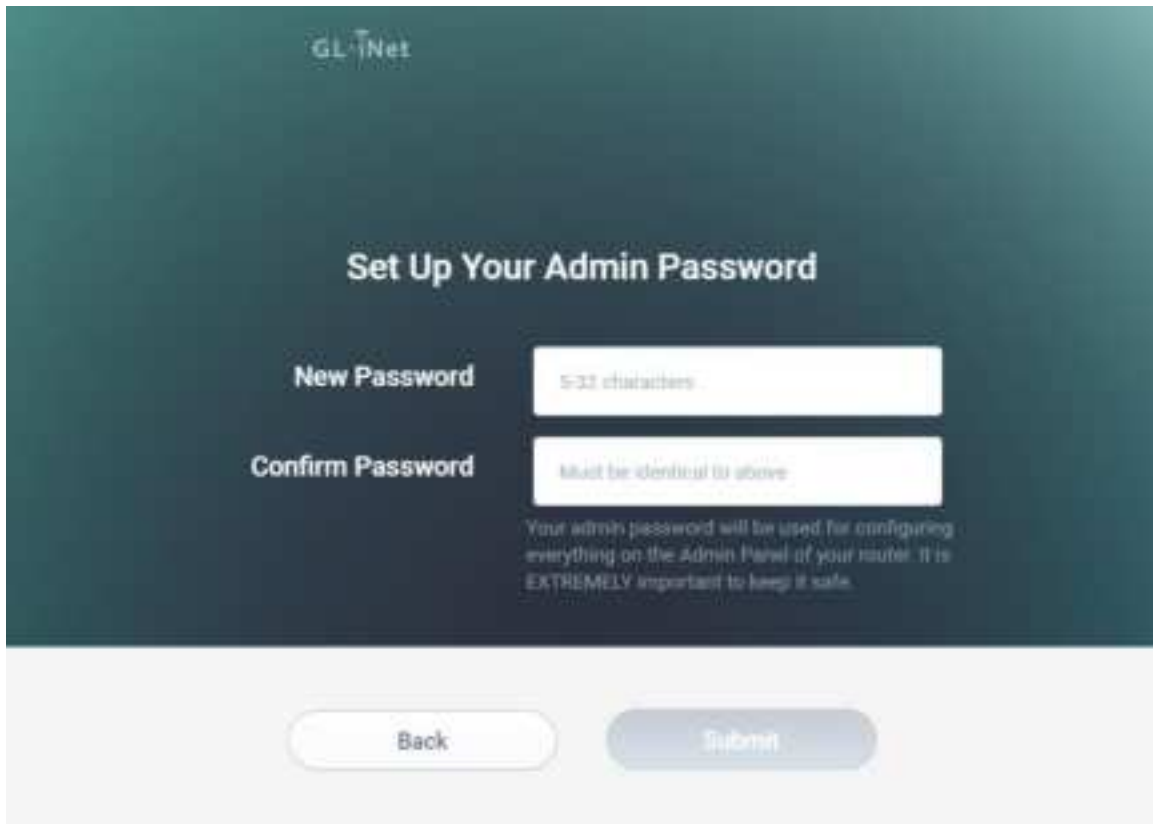
You need to choose the display language of the Admin Panel. Currently, our routers support English, 简体中文, 繁體中文, Deutsch, Français, Español and 日本語, 한국어, русский .



Note: If your browser always redirects to Luci (<http://192.168.8.1/cgi-bin/luci>), you can visit: <http://192.168.8.1/index.html> instead of <http://192.168.8.1>.

(2) Admin Password Setting

There is no default password for the Admin Panel. You have to set your own password, which must be at least 5 characters long. Then, click Submit to proceed.

The image shows a web interface for setting an admin password. At the top, the GL.iNet logo is visible. The main heading is "Set Up Your Admin Password". Below this, there are two input fields. The first is labeled "New Password" and contains the text "5-33 characters". The second is labeled "Confirm Password" and contains the text "Must be identical to above". Below the input fields, there is a note: "Your admin password will be used for configuring everything on the Admin Panel of your router. It is EXTREMELY important to keep it safe." At the bottom of the form, there are two buttons: "Back" and "Submit".

GL.iNet

Set Up Your Admin Password

New Password 5-33 characters

Confirm Password Must be identical to above

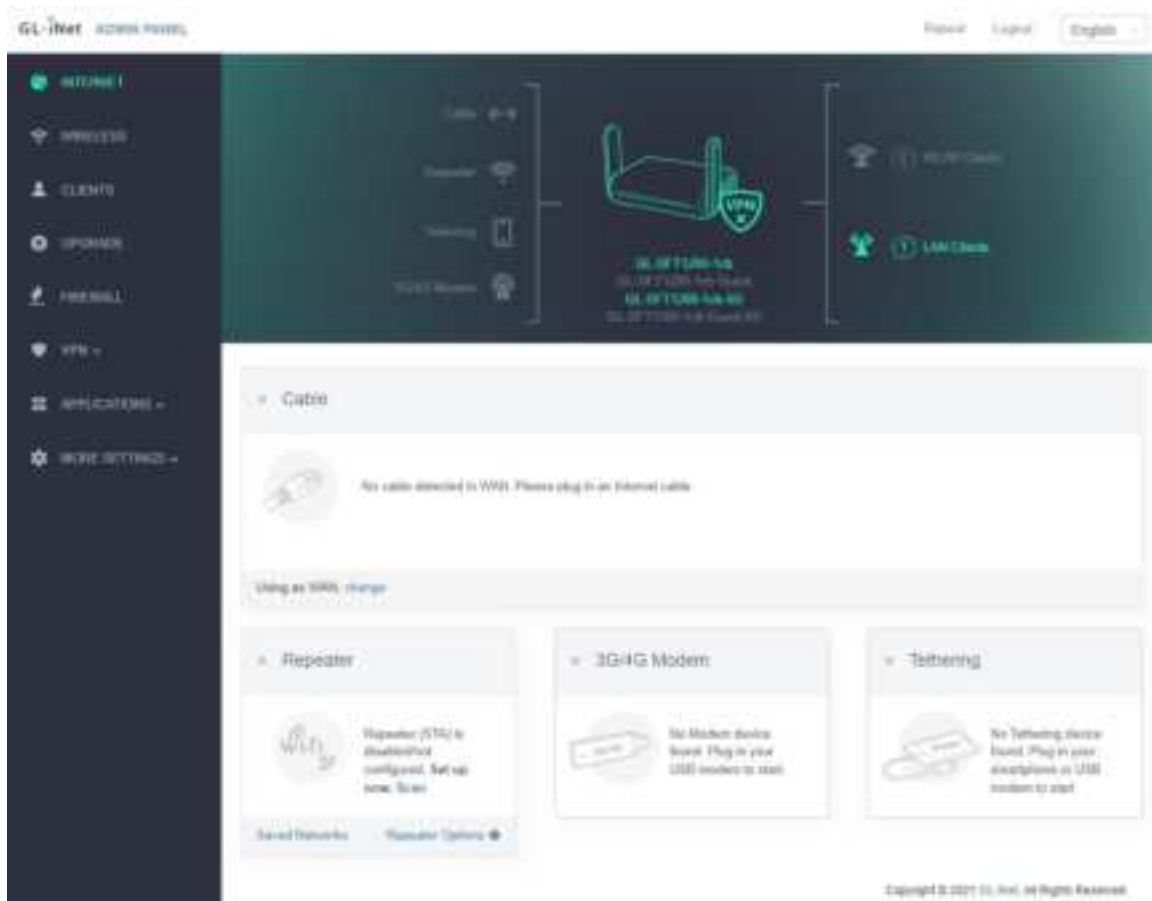
Your admin password will be used for configuring everything on the Admin Panel of your router. It is EXTREMELY important to keep it safe.

Back Submit

Note: This password is for this web Admin Panel and the embedded Linux system. It will not change your Wi-Fi password.

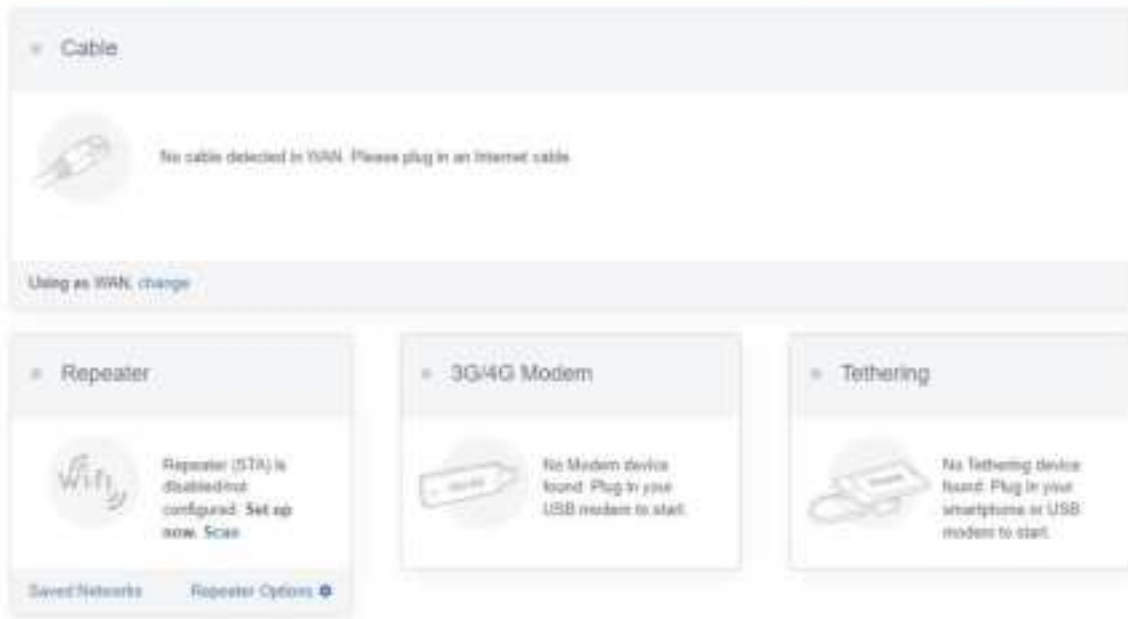
(3) Admin Panel

After the initial setup, you will enter the web Admin Panel of the router. It allows you to check the status and manage the settings of the router.



2. INTERNET

There are total 4 types of connection method that you can use to access the Internet: **Cable**, **Repeater**, **3G/4G Modem** and **Tethering**.

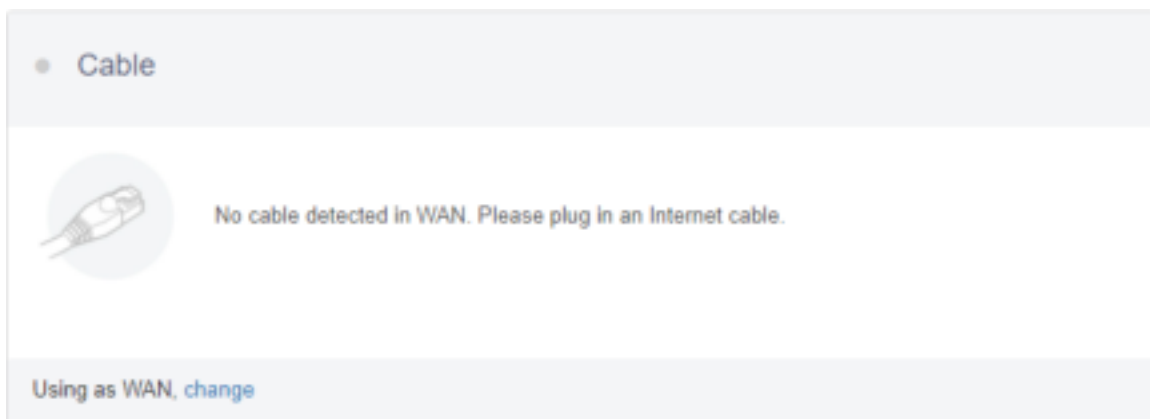


Click INTERNET to create an Internet connection.

2.1. Cable

Connect the router to the modem or main router via Ethernet cable to access the Internet.

Before plugging the Ethernet cable into the WAN port of the router, you can click Use as 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.




Plug the Ethernet cable into the WAN port of the router. The information of your connection will be shown on the Cable section. DHCP is the default protocol. You can click Modify to change the protocol.

• Cable

Protocol	DHCP
IP Address	192.168.51.197
Netmask	255.255.255.0
Gateway	192.168.51.1
DNS Server	192.168.51.1

Modify




(1) DHCP

DHCP is the default and most common protocol. It doesn't require any manual configuration.

• Cable

Protocol

Cancel Apply Using as WAN, change



(2) 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.

The current settings will be automatically filled once you choose Static. Change it according to your needs and then click Apply.

Cable

Protocol	Static
IP Address	192.168.51.197
Netmask	255.255.255.0
Gateway	192.168.51.1
DNS Server1	192.168.51.1
DNS Server2	

Cancel
Apply
Using as WAN change

(3) 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.

Under PPPoE protocol, enter your username and password, then click Apply.

Cable

Protocol	PPPoE
User Name	Regained
Password	Regained

Cancel
Apply
Using as WAN change

2.2. 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.

In Repeater section, click Scan to search for the available wireless networks nearby.



Choose a SSID from the drop-down list and enter its password. You can also enable the **Remember** button to save the current chose wireless network. Finally, click Join.

• Wi-Fi
Scan

SSIDGL-Office

Password

Remember

Join

2.3. USB 3G/4G Modem

You can connect to the Internet using a USB 3G/4G modem. Insert your SIM card into the USB modem Plug the USB modem into the USB port of the router. Once it has been detected, the 3G/4G modem section will be activated and you will be able to set up your USB modem.

Be aware that some modems work in host-less mode, which will be configured through [Tethering](#) but not 3G/4G modem.

In General, you can set up your 3G/4G modem by the three basic parameters below. Click Apply to connect.

• CSL

Modem Name

IMEI

Auto Setup

Manual Setup

AT Command

Modem Reset

Cells Info


- **Device:** Choose `/dev/cdc-wdm0` if your modem supports QMI, otherwise you need to choose `/dev/ttyUSB`, which may include several **ttyUSB** from 0 to 3.

You need to choose the correct one based on the modem spec. We suggest you to try **ttyUSB0** first.

- **Service Type:** Indicate the service type of your SIM card.
- **APN:** Confirm with your SIM card carrier.

Advanced Settings:

- **Dial Number:** Generally, it is a default value and you don't need to set it manually. However, if you have this info, please input it.
- **Pincode, Username and Password:** Generally, these are not necessary for an unlocked SIM card. However, if you have a locked SIM card, please consult your service provider.

Pincode	<input type="text"/>
Dial number	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/> 

Apply

It is connected when the IP address of your SIM card shows up.

3G/4G Modem

Device: Novus USB

Service: LTE/LTE+GPRS

APN: internet

Advanced Modem Reset

Apply

Compatible Modems

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

Model	3G/4G	Tested	Tested by	Comments*
Quectel EC20-E, EC20-A, EC20-C	4G	Yes	GL.iNet	
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	QMI
Pantech UML295 (Verizon)	4G	Yes	GL.iNet/steven	Host-less
Novatel USB551L (Verizon)	4G	Yes	GL.iNet/steven	QMI
Verizon U620L (Verizon)	4G	Yes		Host-less

*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.

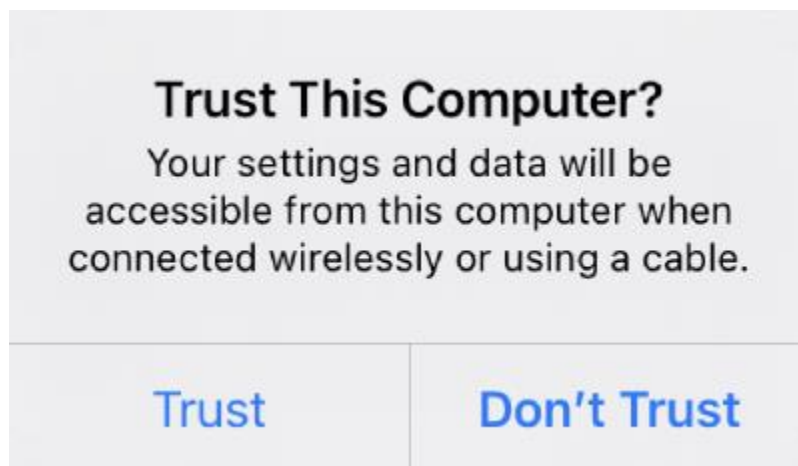
You can also refer to <http://ofmodemsandmen.com/modems.html> for a well-supported modem list.

2.4. Tethering

Using 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.

For host-less modem tethering, plug it into the USB port of the router.

For smartphone tethering, connect it to the USB port of the router and click **Trust** to continue when the message pops up in your smartphone.



After plugging in your device, the Tethering section will update and your device will be shown on the device list. The device name will begin with **eth** or **usb** such as **eth2**, **usb0**. Choose your device and click Connect.

[Settings](#)

Personal Hotspot

Personal Hotspot on your iPhone can provide Internet access to other devices signed into your iCloud account without requiring you to enter the password.

Allow Others to Join



Wi-Fi Password

hftigeth&: >

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



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



EasyTether

Some carriers prohibit the sharing of the data so that you may not be able to use tethering. However, you can try [easytethering](#).

Note: Easytether is not a free service and we have no affiliation with them.

3. WIRELESS

In WIRELESS, you can check the current status and change the settings of the wireless network created by the router. The wireless network can be turned on or off by switching the ON/OFF button. Also you can enable Guest Wi-Fi(disable default) to provide internet services to your visitors.

Wi-Fi Name (SSID): The name of the Wi-Fi. It is not suggested to use unicode characters such as Chinese.

Wi-Fi Security: The encryption method of the Wi-Fi.

Wi-Fi Key: The password of the Wi-Fi, which must be at least 6 characters long. We suggest you to change it when you receive the router.

SSID Visibility: Show/hide the Wi-Fi SSID.

Wi-Fi Mode: The protocol of the Wi-Fi. It is suggested to use default settings (2.4GHz is b/g/n, 5GHz is a/n/ac).

Bandwidth: The channel frequency coverage range of the Wi-Fi. It is suggested to use default parameter.

Channel: The router will not choose the best channel itself. You need to choose a channel manually. If your router is used as a Wi-Fi repeater, the channel will be fixed according to the connected wireless network.

TX Power (dBm): It specifies the signal strength.

Channel Optimization: It will optimize your Wi-Fi signal and channel according to the Wi-Fi environment.

• 2.4G WiFi

• 2.4G Guest WiFi

• GL-SFT1200-1cb



Wi-Fi Name (SSID)

GL-SFT1200-1cb

Wi-Fi Security

WPA2-PSK

Wi-Fi Key ⓘ

SSID Visibility

Shown

Wi-Fi Mode

802.11b/g/n

Bandwidth

20/40 MHz

Channel

Auto

TX Power (dBm) ⓘ

Max

Modify

Channel Optimization

5G WiFi
5G Guest WiFi

GL-SFT1200-1cb-5G
ON

Wi-Fi Name (SSID)	GL-SFT1200-1cb-5G
Wi-Fi Security	WPA2-PSK
Wi-Fi Key	*****
SSID Visibility	Shown
Wi-Fi Mode	802.11a/n/ac
Bandwidth	20/40/80 MHz
Channel	36
TX Power (dBm)	Max

Modify
Channel Optimization

Click Modify to change the settings of the wireless network.

Guest WiFi:

You can switch on/off Guest WiFi in Wireless, the Guest WiFi will create a different subnet to your visitors to prevent any un-authority visiting to your other devices in the network.

2.4G WiFi

2.4G Guest WiFi

GL-SFT1200-1cb-Guest

OFF

Wi-Fi Name (SSID)

GL-SFT1200-1cb-G...

Wi-Fi Security

WPA2-PSK

Wi-Fi Key ⓘ

Modify

5G WiFi

5G Guest WiFi

GL-SFT1200-1cb-Guest-5G 5G

OFF

Wi-Fi Name (SSID)

GL-SFT1200-1cb-G...

Wi-Fi Security

WPA2-PSK

Wi-Fi Key ⓘ







Modify

4. CLIENTS

You can manage all connected clients in CLIENTS.

You can see their name, IP, MAC address and connection type.

Click the button on the right to block any unwanted client.

CLIENTS				
Enable real-time speed and traffic statistics. This requires higher CPU load. <input type="checkbox"/>				
Brand	Name	IP	MAC	Block
Wired Device				
	DESKTOP-5PTHICI	192.168.51.217	84-A9-3E-82-99-B8	<input checked="" type="checkbox"/>
5G Wireless Device				
	Leo-Phone	192.168.51.118	14-16-9E-A0-A1-F5	<input type="checkbox"/>
Offline Device Delete All				
	GL-MV1000...	192.168.51.220	94-83-C4-02-08-23	<input type="checkbox"/> 
	GL-MT300N...	192.168.51.194	E4-95-6E-48-F5-90	<input type="checkbox"/> 

After you turn on Enable real-time speed and traffic statistics.

You can see all devices' traffic and speed information, click the button on the right to block any unwanted clients.

CLIENTS						
Enable real-time speed and traffic statistics. This requires higher CPU load. <input checked="" type="checkbox"/>						
Brand	Name	IP + MAC	Speed	Traffic	QoS	Block
Wired Device						
?	DESKTOP-SPTHCI	192.168.51.217 84:A5:3E:82:99:B5	↑ 14.5 KB/s ↓ 0.0 KB/s	↑ 6.2 MB ↓ 42.0 MB	Set	<input checked="" type="checkbox"/>
5G Wireless Device						
?	Leo-Phone	192.168.51.118 14:16:5E:40:A1:F5	↑ 237.0 B/s ↓ 1.1 KB/s	↑ 75.2 KB ↓ 276.5 KB	Set	<input type="checkbox"/>
Other Device						Delete All
G	GL-MF1000...	192.168.51.220 94:83:C4:92:68:23	↑ 0.0/s ↓ 0.0/s	↑ 0.0 ↓ 0.0	Set	<input type="checkbox"/>
G	GL-MT300N...	192.168.51.194 E4:95:6E:48:F5:30	↑ 0.0/s ↓ 0.0/s	↑ 0.0 ↓ 0.0	Set	<input type="checkbox"/>

You can set tech QoS for certain clients by click **Set**,

QoS Speed limit range (1KB/s-1GB/s)

↑ Upload Speed Limit	<input type="text" value="100"/>	KB/s
↓ Download Speed Limit	<input type="text" value="100"/>	KB/s

Cancel
Apply

a speed limitation range window will pop-up, set the speed and click **Apply**.

CLIENTS						
Enable real-time speed and traffic statistics. This requires higher CPU load. <input checked="" type="checkbox"/>						
Brand	Name	IP + MAC	Speed	Traffic	QoS	Block
Wired Device						
?	DESKTOP-SPTHCI	192.168.51.217 84:A5:3E:82:99:B5	↑ 36.6 KB/s ↓ 60.0 KB/s	↑ 10.7 MB ↓ 87.4 MB	Set	<input checked="" type="checkbox"/>
5G Wireless Device						
?	Leo-Phone	192.168.51.118 14:16:5E:40:A1:F5	↑ 0.0/s ↓ 0.0/s	↑ 830.1 KB ↓ 597.6 KB	Set Reset	<input type="checkbox"/>

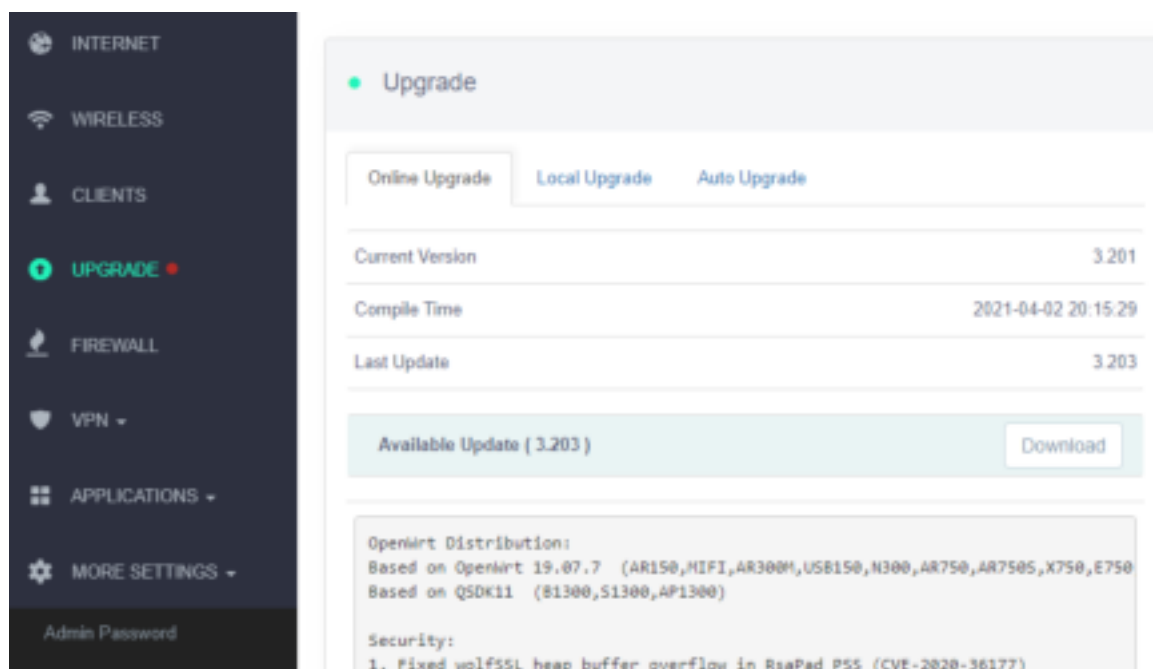
There is an yellow "exclamation mark" besides speed limited client.

5. UPGRADE

Click UPGRADE to check any available update and upgrade the firmware.

5.1. 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.



*Note: It is suggested to uncheck **Keep setting**. If you keep the settings and encounter problems after the upgrade, please reset the router.*

5.2. Upload Firmware


Click Local Upgrade to upload a firmware file to the router. Simply drag and drop your firmware file to the area indicated.

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade



Select a file or drag it here.

File types include .bin .img .zip .tar .gz

(1) Official OpenWrt/LEDE firmware

You can download the official firmware from our [website](#).

- GL-MT1300(Beryl): <https://dl.gl-inet.com/firmware/mt1300/>

Find the available firmwares from the folder according to your device model, and they are located in different sub-folders:

V1/Release: Official GL.iNet OpenWrt/LEDE firmware.

testing: Beta version of GL.iNet OpenWrt/LEDE firmware.

Snapshots: Testing firmware with special functions.

Note: You have to upload the .tar .bin file. The .img file can only be flashed to the router through Uboot.

(2) Compile your own firmware

You can compile your own firmware and flash to the router. Please refer to

<https://github.com/gl-inet/openwrt>

<https://github.com/gl-inet/imagebuilder>

(3) Third party firmware

You may also try other firmwares such as DDWRT.

Note: If you uploaded an incompatible firmware thus bricked the router, please use Uboot to re-install the correct firmware.

5.3. Auto Upgrade

You can enable auto upgrade. The router will search for available update and upgrade automatically according to the time that you set.

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

Router Time

Fri Sep 3 03:59:56 UTC 2021

Enable Auto Upgrade

☐

Auto Upgrade Time

04:00

6. FIREWALL

In FIREWALL, you can set up firewall rules like **port forwarding**, **open port** and **DMZ**.



6.1. Port Forwards

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

To set up port forwarding, click Port Forwards and input the required parameters or click Add a New One.



Name: The name of the rule which can be specified by the user.

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

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

Internal Ports: 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.

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

Status: Activate or Deactivate the rule.

6.2. Open Ports on Router

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

To open a port, click Open Ports on Router and input the required parameters or click Add a New One.

Firewall

Port Forwards Open Ports on Router DMZ

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

Name	Port	Protocol	Status	Action
Required	Required	TCP/UDP	Enabled	Add

Name: The name of the rule which can be specified by the user.

Port: The port number that you want to open.

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

Status: Activate or Deactivate the rule.

6.3. DMZ

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

Click DMZ and enable Open DMZ. Input the internal IP address (E.g. 192.168.8.100) of your device which is going to receive all the inbound packets.

● Firewall

Port Forwards

Open Ports on Router

DMZ

DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set.

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

Open DMZ



DMZ Host IP

Apply

7. VPN

GL.iNet routers have pre-installed VPN server and client in OpenVPN and WireGuard.

7.1. OpenVPN

GL.iNet routers have pre-installed OpenVPN server and client.

7.1.1. OpenVPN Client

OpenVPN client requires OpenVPN configuration file (.ovpn) to create the OpenVPN connection. If you have your own VPN service provider but you don't know how to get the configuration file, please refer to [Get your configuration file](#).

Click + Add a New VPN Configuration to upload the configuration file.

● OpenVPN Client

OpenVPN (Virtual Private Network) client is often used to connect to a OpenVPN server to access private resources securely over a public network.

Please find out the compatible OpenVPN Service Provider and instructions from [VPN on Router](#).

From follow the guide and download the ovpn configurations and import to the router by clicking the button below.

[+ Add a New OpenVPN Configuration](#)


You can also download our [smartphone app](#) to simplify the setup process.

(1) Upload your OpenVPN configuration file

Simply drag and drop your file to the pop up windows. It can be a single .ovpn file or a zip/tar.gz file which contains multiple .ovpn files.

Be careful that some .ovpn files use separated ca, cert, crl files. These files must be zipped together with the .ovpn file before upload.

Add a New OpenVPN Configuration



Select a file or drag it here.
Filetypes include .zip .tar .gz .conf .txt .ovpn

Config Count 0

Cancel

Submit

(2) Enter Description, Username and Password

Enter a description for your OpenVPN configuration file and then click Submit to finish the upload process. In some cases, it will ask you to enter your username and password.

Add a New OpenVPN Configuration

You need to subscribe VPN service first and then the service provider will give you the username, password or passphrase.

Learn more: <https://www.gl-inet.com/solutions/vpn/>

SUCCESS! **Re-upload file.**

hk272.nordvpn.com.udp.ovpn

Config Count

1

Description

nordvpn-hk

User Name

Required

Password ⓘ

Required

Cancel

Submit

(3) Connect to the OpenVPN server

You can now click Connect to start the OpenVPN connection.

● OpenVPN Client

❗ If you enabled VPN but the VPN cannot connect to its server, there will be NO Internet.
When you change server while VPN is connected, VPN will not be leaked.

Status

Management

Access Local Network ⓘ



Current OpenVPN Configuration

nordvpn-hk



Server

hk272.nordvpn.com.udp.ovpn ⚙

Connect

If your configuration file is an archive file, like .zip, you can switch server at the cog icon.

• OpenVPN Client

❗ If you enabled VPN but the VPN cannot connect to its server, there will be NO Internet.
When you change server while VPN is connected, VPN will not be leaked.

Status

Management

Access Local Network ⓘ



Current OpenVPN Configuration

nordvpn-hk-zip



Server

hk272.nordvpn.com.tcp.ovpn ⚙

Connect

Once connected, you should find your IP address, data received/sent.

●

OpenVPN Client

❗

If you enabled VPN but the VPN cannot connect to its server, there will be NO Internet.
 When you change server while VPN is connected, VPN will not be leaked.

Status

Management

Access Local Network

❗

Current OpenVPN Configuration

nordvpn-hk

Server

hk272.nordvpn.com.udp.ovpn

⚙️

IP Address

10.8.1.5

Data Received / Sent

31KB / 20KB

Disconnect

Note: It can't running VPN Client and Server at the same time, and also can't running OpenVPN Client and WireGuard Client at the same time.

(4) Manage configuration files

Click Management to check the list of configuration files. You can modify the **Description**, **User name** or **Password** of each configuration file. You can also add, delete a configuration file or even purge all your uploaded configuration files.

If your configuration file is a zip/tar.gz file which includes multiple ovpn files, you can choose an individual .ovpn file that you would like to connect in **Server**.

- OpenVPN Client

❗ If you enabled VPN but the VPN cannot connect to its server, there will be NO Internet. When you change server while VPN is connected, VPN will not be leaked.

Status

Management

OpenVPN Configurations	2
------------------------	---

● nordvpn-hk

Type	OpenVPN
------	---------

Config Count	1
--------------	---

Server hk272.nordvpn.com.udp.ovpn

Description	<u>nordvpn-hk</u>
-------------	-------------------

User Name

Password

Remove

Apply

Get your configuration file

We have tested different VPN 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.

Get your configuration file

If you have any problem in the setup of OpenVPN, please contact support@gl-inet.com

7.1.2. OpenVPN Server

You can set up an OpenVPN server on GL.iNet router. Click + Generate a configuration file.

● OpenVPN Server

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

1. Add a new certificate
2. Modify the default configuration, then save.
3. Export the configuration file.
4. Start

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

 Generate a Configuration File

(1) Server configuration

There are preset OpenVPN server configurations. You can also click Modify to change them manually. Click Apply when you finish.

• OpenVPN Server

Access Local Network ⓘ

Type

Router

IP Address

10.8.0.0

IPv6 Address ⓘ

fd00:db8:0:123::0

Netmask

255.255.255.0

Port

1194

Encryption

AES-256-GCM

Authentication

SHA256

Protocol

UDP

Modify

Start

Export Config

Allow Access Local Network: Enable this will allow every client that connect to this OpenVPN Server be able to access your LAN. Please use with caution.

Note that you can't running VPN Client and Server at the same time, and also can't running OpenVPN Client and WireGuard Client at the same time.

(2) Export OpenVPN configuration file

Click Export Config to download the OpenVPN configuration file which you need to upload when you are configuring your OpenVPN client.

• OpenVPN Server

Access Local Network ⓘ

Type

Router

IP Address

10.8.0.0

IPv6 Address ⓘ

fd00:db8:0:123::0

Netmask

255.255.255.0

Port

1194

Encryption

AES-256-GCM

Authentication

SHA256


Protocol

UDP

Modify

Start

Export Config



(3) Start the OpenVPN server

Click Start to start your OpenVPN server. Otherwise, you will not be able to connect to the OpenVPN server by using its configuration file.

• OpenVPN Server

Access Local Network ⓘ

Type

Router

IP Address

10.8.0.0

IPv6 Address ⓘ

fd00:db8:0:123::0

Netmask

255.255.255.0

Port

1194

Encryption

AES-256-GCM

Authentication

SHA256

Protocol

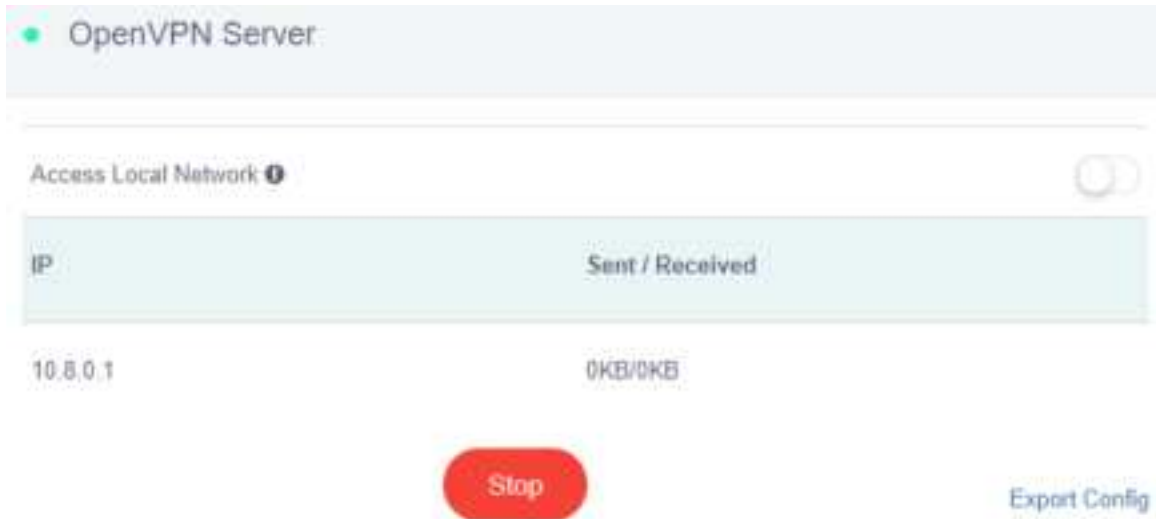
UDP

Modify

Start

Export Config

It started.



7.2. WireGuard

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.

7.2.1. WireGuard Client

To set up a WireGuard client, please click + Add New Profiles.

• WireGuard® Client

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

To use WireGuard, you need either subscribe to a commercial VPN service or set up your own WireGuard Server.

Here is a list of commercial WireGuard Services that you can set up directly on the router:

azirevpn

Now set Up ->

To find more supported commercial WireGuard Service providers, please go to [VPN on Router](#).

You can also set up your WireGuard manually.

+ Set up WireGuard Manually

You can also download our [smartphone app](#) to simplify the setup process.

(1) Specify the name of your server

Specify the name and then click Next.

Add a New WireGuard® Client

Providers

Configuration

Manual Input

Provider

azirevpn

Setup guide

User Name

Password

Cancel

Next

(2) Input the configurations!

There are different methods to input the configurations.

Add a New WireGuard® Client

Providers

Configuration

Manual Input

Provider

mullvad

Setup guide

Account Number

Required

Cancel

Next

You can copy the JSON or Plain Text configurations from your server to Configuration or input the settings manually.

GL.iNet ADMIN PANEL

Reboot

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

Internet K8 Switch

WireGuard® Client

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

To use WireGuard, you need either subscribe to a commercial VPN service or set up your own WireGuard Server.

Here is a list of commercial WireGuard Services that you can set up directly on the router:

azirevpn

Now set Up ->

To find more supported commercial WireGuard Service providers, please go to VPN on Router.

You can also set up your Wireguard manually.

+ Set up WireGuard Manually

You can also download our [smartphone app](#) to simplify the setup process.

Copyright © 2021 G

After copy the JSON or Plain Text from your server, you can paste it in the Configuration and then click **Add** to finish the WireGuard Client setup.

Add a New WireGuard® Client

The screenshot shows a window titled "Add a New WireGuard® Client". At the top, there are three tabs: "Providers", "Configuration", and "Manual Input". The "Configuration" tab is selected and highlighted with a red rectangular box. Below the tabs is a large, empty text area with the placeholder text "Paste the copied configuration here or switch to manual tab". At the bottom right of the window, there are two buttons: "Cancel" and "Next".

7.2.2. WireGuard Providers

If you are using **Azurevpn** or **Mullvad**, you can click Others and use your **AzureVPN** or **Mullvad** account to set up WireGuard client directly.

AzureVPN: Select **AzureVPN** as the provider, enter your User Name and Password and then click "Add" finish the WireGuard Client setup

Add a New WireGuard® Client

Providers Configuration Manual Input

```
[Interface]
PrivateKey = yGkRI0pQc
Address = 100.83.7.179/32
DNS = 100.83.0.1

[Peer]
PublicKey = 8GjeotHyZrQXF2zkELuxYm4IEGij6JnmphfcZdbZsXAc
AllowedIPs = 0.0.0.0/0
Endpoint = us3.wg.azurevpn.net:51820
```

Cancel Next

Mullvad: Select Mullvad as the provider, enter your Account Number and then click "Add" to finish the WireGuard Client setup.

Waiting for the adding.

Add a New WireGuard® Client

Name

Cancel Add

⚙ Adding, please wait...

- WireGuard® Client

WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. Please follow the steps below

1. Add a New WireGuard® Configuration.
2. Paste or Enter WireGuard® Information Manually.
3. Select a configuration.
4. Click the Connect button.

You have not set up any WireGuard® configurations yet. Get started by adding a WireGuard® configuration.

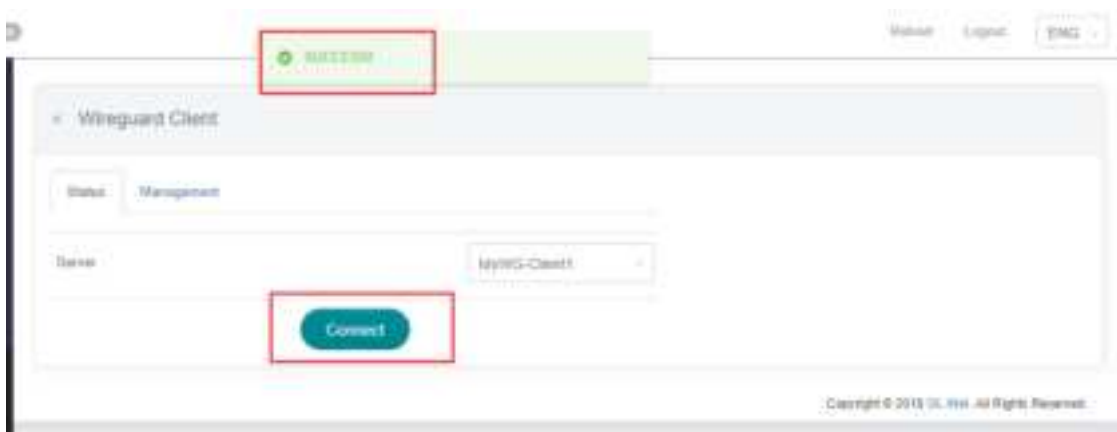
Wireguard is functional in GL.iNet products, however, until the upstream project publishes a stable 1.0 version, Wireguard will remain a beta feature.

+ Add New Profiles ⚙

Other recommended WireGuard provider, please click [this link](#).

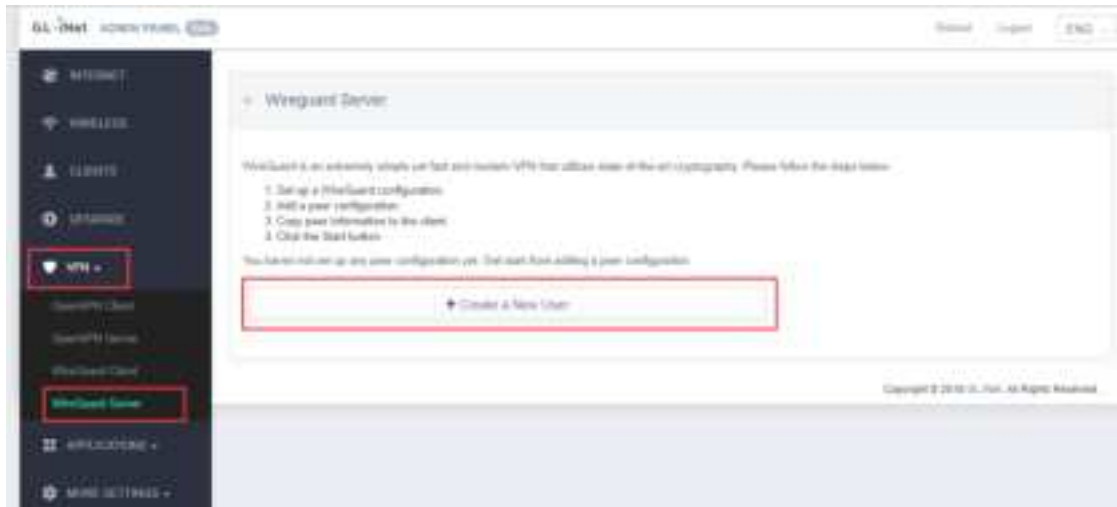
(3) Connect to the WireGuard server

Click Connect. You will see the upload and download traffic when it is connected successfully.



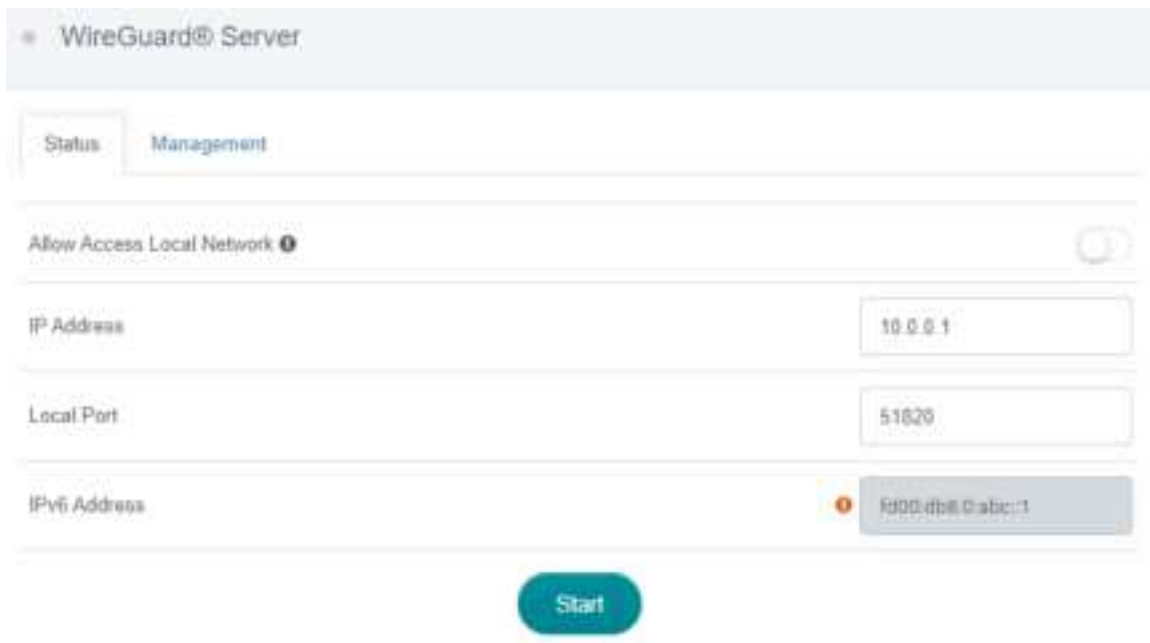
7.2.3. WireGuard Server

You can set up a WireGuard server on GL.iNet router with firmware 3.0. Click + Create a New User.



(1) Start a WireGuard Server

You can simply use the default parameters of **Local IP** and **Local Port**, or you can set your own value. Then click Start to start your own WireGuard server.



(2) Add a new client

You have to add a new user and apply the configurations when you are connecting to this WireGuard server.

Click Management tab and then Create a New User.



Specify the **Name** of the new client and then click Add.

Add a New WireGuard® Client

Name Required

Cancel Add

(3) Get the configuration details for your client



You can now check the list of the clients you added. You can Delete any unwanted client. Please click Configurations to find the configuration details which you need to use when you are setting up WireGuard client. We provide QRcode, Plain Text and JSON configurations currently.

WireGuard® Server

Status

Management

WireGuard® Clients

Name	Client IP	Configurations	Delete
phone	10.0.0.2/32		

+ Add a New User

If you are using another GL.iNet router as a client, please copy the **JSON** configuration and paste it directly when you are setting up WireGuard client.

WireGuard® Client Configurations

QRCode

Plain Text

Please use the following configuration to set up your WireGuard® client.

```
[Interface]
Address = 10.0.0.2/32
ListenPort = 9442
PrivateKey = MAYjAZSr/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
DNS = 64.6.64.6

[Peer]
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = 42.XXX.XXX.XXX:51820
PersistentKeepalive = 25
PublicKey = 0RT1x9GoyJY6aQ/LX1KwB7FCnzxXeVidj4q6NSO/3hE=
```

7.2.4. Wireguard App Support

You can also use WireGuard App on other devices with various OS

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

7.2.5. Visit Client's LAN Subnet

Visit Client's LAN Subnet from WireGuard Server LAN Subnet

- 1) Change WireGuard clients LAN IP to avoid IP confliction with Server
- 2) Modify Wireguard_Server Configuration

WinSCP or SSH into your the WireGuard Server (router) find and modify the file

`/etc/config/wireguard_server`

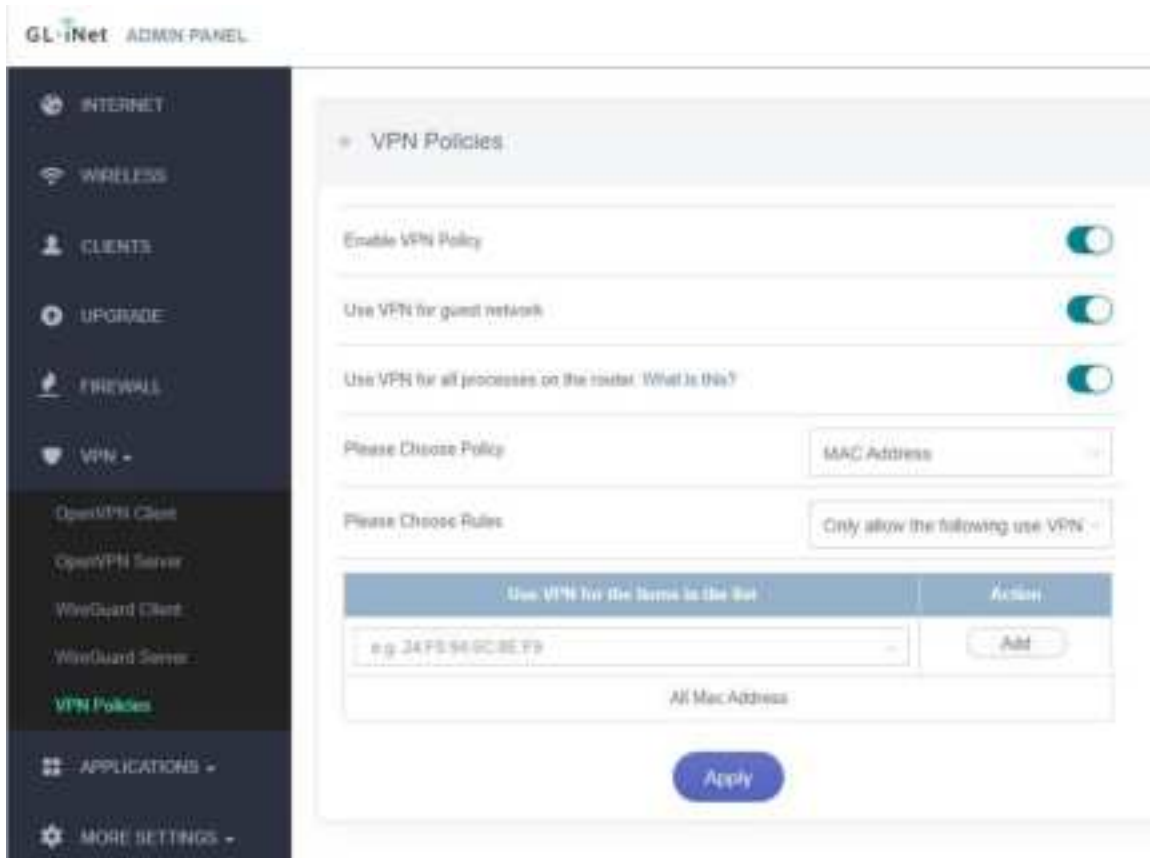
Add a line to the end of the config file of clients you want to visit.

```
list subnet '192.168.xxx.0/24'
```

Save and Exit

7.3. VPN Policies

Starting from firmware version 3.022, users can define VPN routing policies. For example, it is possible to use VPN for a specific website/IP while maintaining a normal Internet traffic without VPN for others.



7.3.1. Settings

Enable VPN Policy: Turn on/off VPN policies.

Use VPN for guest network: Turn on/off use VPN for guest network.

Use VPN for all process on the router: Generally, the traffic of all processes running on the router such as GoodCloud will be routed through VPN if there is a connected VPN client (e.g. WireGuard, OpenVPN, Shadowsocks). In this case, these processes will lose Internet if VPN is disconnected. In order to ensure a proper operation of these processes, you can disable this option. As a result, they will not use VPN.

Please Choose Policy: The item can be either **Domain/IP** (e.g. gl-inet.com / 192.168.1.1 / 192.168.1.0/24) or **Mac address** (24:F0:94:5C:8E:F9).

Enable VPN Policy

Use VPN for all processes on the router. What is this?

Please Choose Policy

Domain/IP Based

7.3.2. Add VPN policy

You can only configure either **Only allow the following use VPN** or **Do not use VPN for the following**. Click the drop box to switch among **Only allow the following use VPN** and **Do not use VPN for the following**. To add a policy, enter the domain/IP or Mac address into the box and then click **Add**. Finally, click **Apply** to activate the policy.

For example, if we want to route only the traffic of `netflix.com` through VPN, we need to choose Policy **Domain/IP**, choose Rule **Only allow the following use VPN**, input `netflix.com` and click **Apply**.

Please Choose Policy

Domain/IP

Please Choose Rules

Only allow the following use VPN

Use VPN for the items in the list	Action
e.g. google.com 192.168.1.1 192.168.1.0/24	Add
netflix.com	Delete

If you want your Domain-based policy take effect immediatelly, you need to clear your DNS cache. [Help?](#)

Apply

However, if we want to route all traffic through VPN except `gl-inet.com`, we need to add `gl-inet.com` under **Do not use VPN for**.

Please Choose Policy
Domain/IP

Please Choose Rules
Do not use VPN for the following

Do not use VPN for the items in the list	Action
e.g. google.com 192.168.1.1 192.168.1.0/24	Add
netflix.com	Delete

If you want your Domain-based policy take effect immediately, you need to clear your DNS cache. [Help?](#)

Apply

7.3.3. Clear DNS cache

If you are using domain-based policy, it may not work unless you clear your DNS cache. Please follow the instructions below to clear your DNS cache.

Windows: Press **Win + R** and run **cmd**. Execute command `ipconfig /flushdns`.

MacOS: Open **Terminal** and execute command `sudo killall -HUP mDNSResponder`.

Ubuntu: Open **Terminal** and execute command `sudo service network-manager restart`.

You may also need to clear DNS cache in your browser.

Chrome: Visit <chrome://net-internals/#dns>. Click Clear host cache.

Firefox: Open Firefox and press **Ctrl + Shift + Delete**. Select **Time range** to **Everything** and check only **Cache**. Finally, click Clear Now.

8. APPLICATIONS

8.1. Plug-ins

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

Remember to click Update whenever you access this packages repository.

● Plug-ins

Update

Filter

Q Search Package

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

Name	Version	Action
464xlas	11	Install
6in4	25-1	Install
6rd	9-4	Install
6to4	12-2	Install
AdGuardHome	0.104.3-1	Install
ChinaDNS	1.3.2-8	Install
acl	20180121-1	Install
acme	2.7.8-3	Install

Free space: 69% (87 MB)

◀ 1 2 3 ... 660 661 ▶

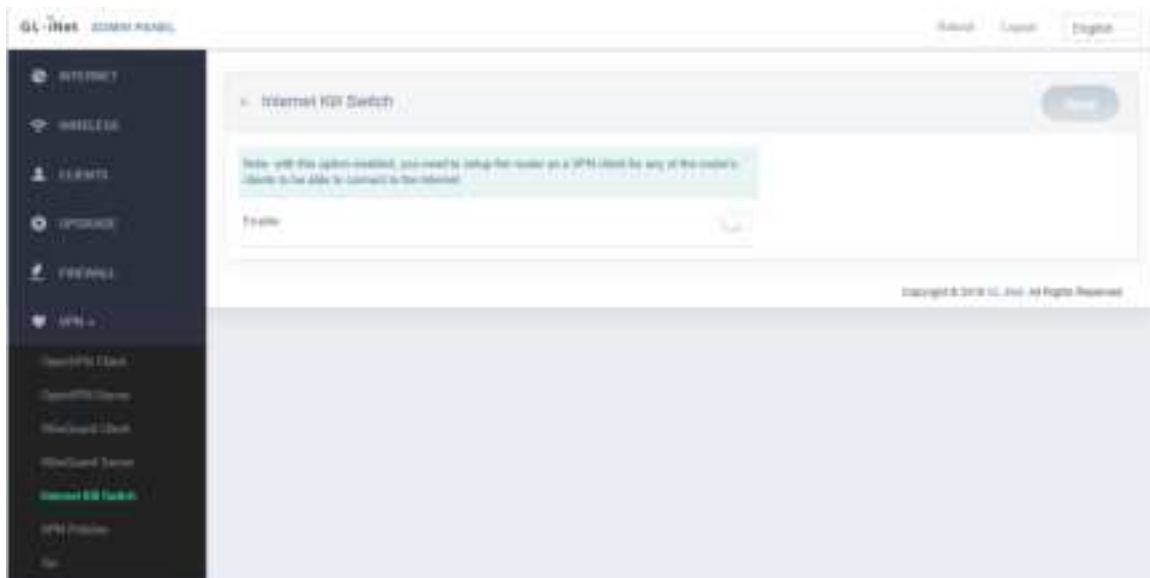
Go

8.2. Internet Kill Switch

Internet Kill Switch feature is built-in from firmware version 3.100, please upgrade.

Note: With this option enabled, you need to set up the router as a VPN client for any of the router's clients to be able to connect to the internet.

After this setting is on, the router needs to run the VPN client all the time, if the VPN client is not running, the clients are **Not Allowed** to access the Internet.



Setup

1) Choose "Internet Kill Switch".

Choose "Internet Kill Switch" from "VPN".



2) Enable "Internet Kill Switch".

Switch on the "Enable" button in the middle of the page.



3) Apply "Internet Kill Switch".

Click "Apply" in the upper right corner.



4) Wait for the "Success" notice

The "SUCCESS!" Message will pop-up if the Internet Kill Switch turn on correctly.



8.3. File Sharing

You can use GL.iNet routers with external storage device such as USB stick, MicroSD card, etc, thus the contents can be shared among all your connected clients. You can easily read or modify its contents.

● File Sharing

Share via LAN ⓘ



Share via WAN ⓘ



Writable ⓘ



Current Directory

/mnt

Apply

8.3.1. Router settings

The contents of the external storage device are shared to LAN but not WAN and they are unwritable by default. Please click on your router model below to check how to change the file sharing settings of the router.

● Multimedia File Sharing

You can enable this feature for multimedia file sharing.

Share via DLNA



Name

OpenWrt DLNA Server

Current Directory

/mnt

Apply

Supported external storage models

Router Model	USB Stick	USB Hard Drive	MicroSD Card	Internal Storage
GL-MT3000 (Beryl AX)	✓	✓	–	–
GL-AXT1800 (Slate AX)	✓	✓	✓	–
GL-A1300 (Slate Plus)	✓	✓	–	–
GL-MT2500/GL-MT2500A (Brume 2)	✓	✓	–	–
GL-SFT1200	✓	✓	–	–
GL-MT300N-V2 (Mango)	✓	✓	–	–
GL-AR150 Series	✓	✓	–	–
GL-AR300M Series	✓	✓	–	–
GL-USB150	–	–	–	–
GL-MiFi	✓	✓	✓	–
GL-AR750 (Creta)	✓	✓	✓	–

Router Model	USB Stick	USB Hard Drive	MicroSD Card	Internal Storage
GL-AR750S-EXT (Slate)	✓	✓	✓	–
GL-B1300 (Convexa-B)	✓	✓	–	–
GL-S1300 (Convexa-S)	✓	✓	–	–
GL-X750 (Spitz)	✓	✓	✓	–
GL-X1200 (Amarok)	✓	✓	✓	–
GL-E750 (Mudi)	✓	✓	✓	–
GL-MV1000 (Brume)	✓	✓	✓	–
GL-MV1000W (Brume-W)	✓	✓	✓	–
GL-MT1300 (Beryl)	✓	✓	✓	–
GL-XE300 (Puli)	✓	✓	✓	–
GL-AX1800 (Flint)	✓	✓	–	–
GL-AP1300 (Cirrus)	–	–	–	–
GL-B2200 (Velica)	–	–	–	✓

Router Model	USB Stick	USB Hard Drive	MicroSD Card	Internal Storage
GL-X300B (Collie)	–	–	–	–
GL-SF1200	–	–	–	–
microuter-N300	–	–	–	–
VIXMINI	–	–	–	–

Note: The power consumption of USB hard drive is quite high. You should use it with an external power supply. Otherwise, it may cause malfunction.

8.3.2. Access the storage device

You can access the contents of the external storage device from your computer or smart phone. Please check the following guidance for the using of file sharing among different operating systems.

General Notes

You may be able to access the share via `\\192.168.8.1\` or `smb://192.168.8.1/` or with GL-Samba instead of 192.168.8.1 (eg `\\GL-MT1300\GL-Samba\`) in your system's file explorer. Since sharing is enabled to the LAN by default (this includes both wired AND wireless clients) and maps a "bad user" to Guest, then even if they don't supply a username and password or an invalid one, ANYONE connected to your router can access the files in the share in Read-Only mode. If you enable Writable mode this applies to both Guests AND the default `root` user. If you enable write access, anybody can create or delete files and folders, if you disable write access, not even the `root` user can delete them via SMB (they can through the CLI though). We can hope that in a future revision there is a simple user management and that a named user (or `root`) can read and/or write while Guests

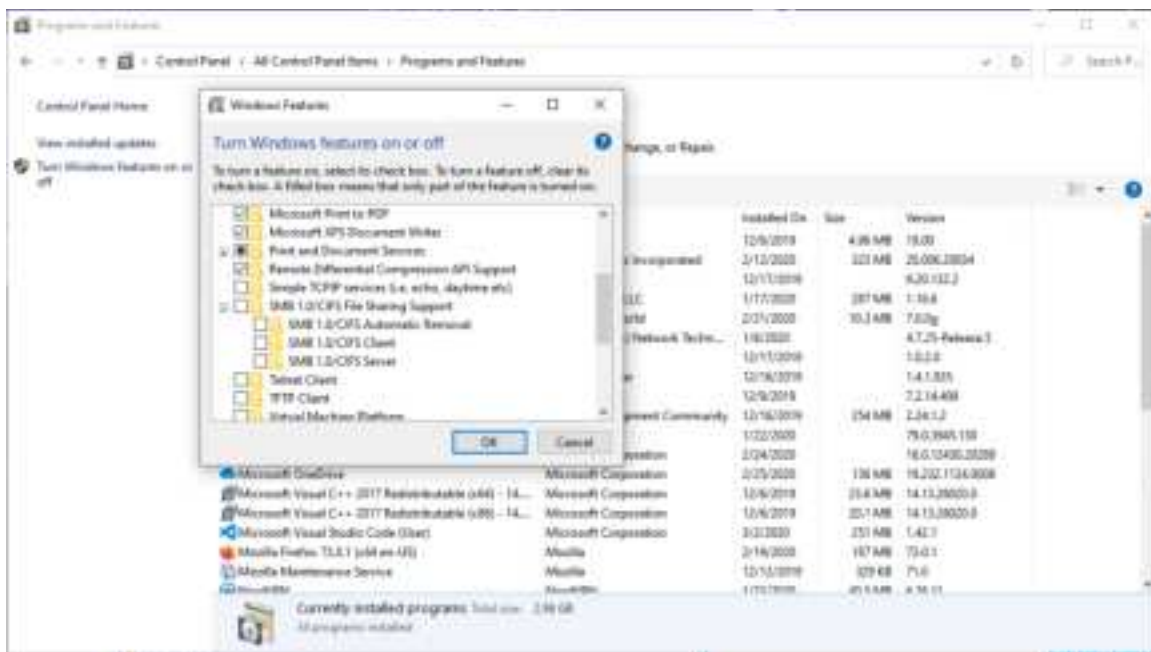
are limited by the Writable or a Public Write flag on a share (and having multiple shares would be great as well).

Windows

Method 1: Samba 2.0 (SMB2.0) Support

We suggest Samba 2.0 support for Windows 10 users.

Due to the security vulnerability of the Samba1.0 protocol, Samba1.0 is not enabled by default in Window 10. You may modify the router Samba configuration.



1). SSH into your router, you can gain control of both the router and the network that the router is controlling. You can refer to the following link: <https://docs.glinet.com/en/3/app/ssh/>

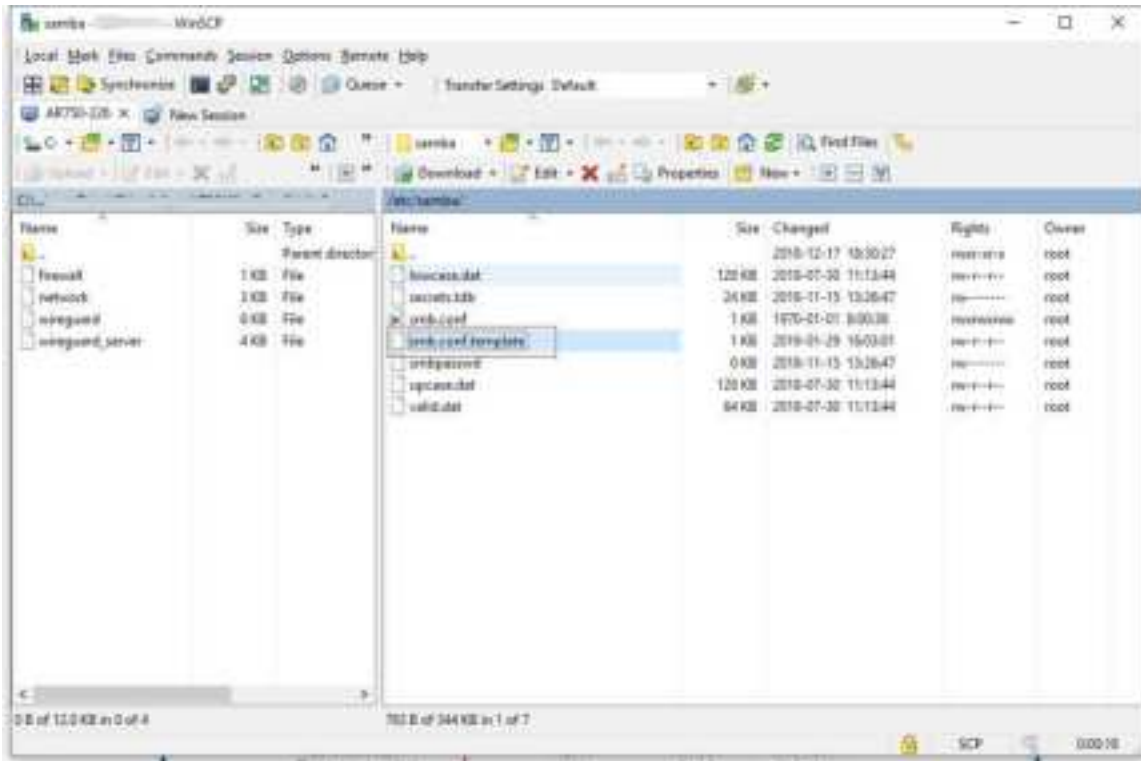
2). Modify the Samba configuration file, type the following command:

```
sed -i 's/security = share/security = user/' /etc/samba/smb.conf.template
```

3). Restart the Samba service, type the following command:

```
/etc/init.d/samba restart
```

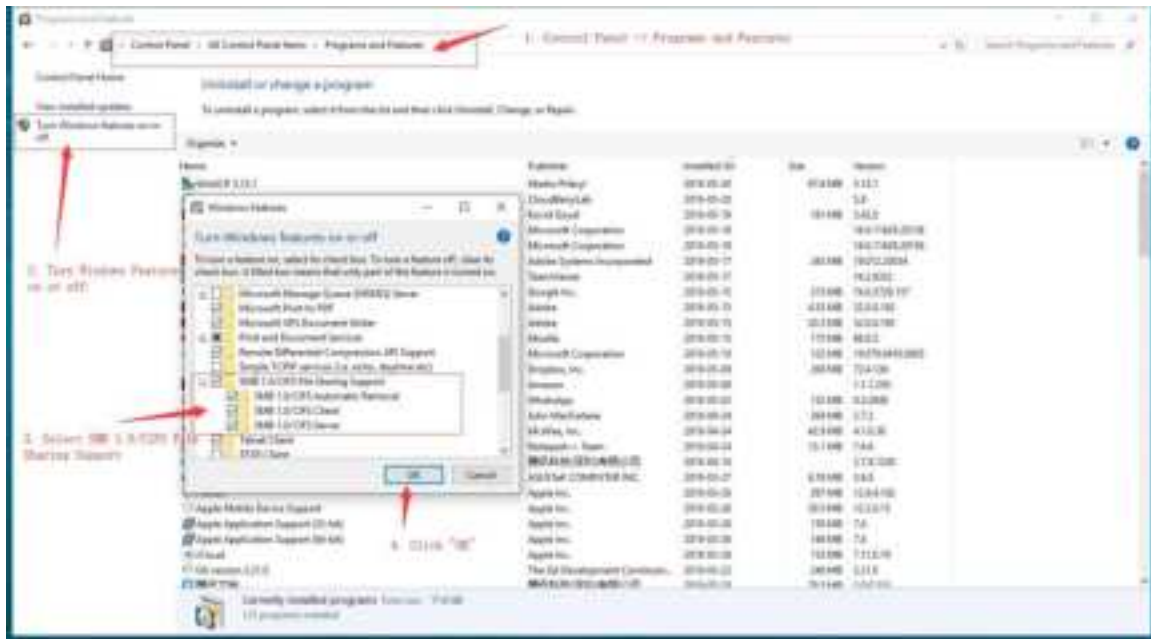

3.0 firmware supports SMB2, and if you need SMB3, use [WinSCP to router](#), edit `/etc/samba/smb.conf.template`.



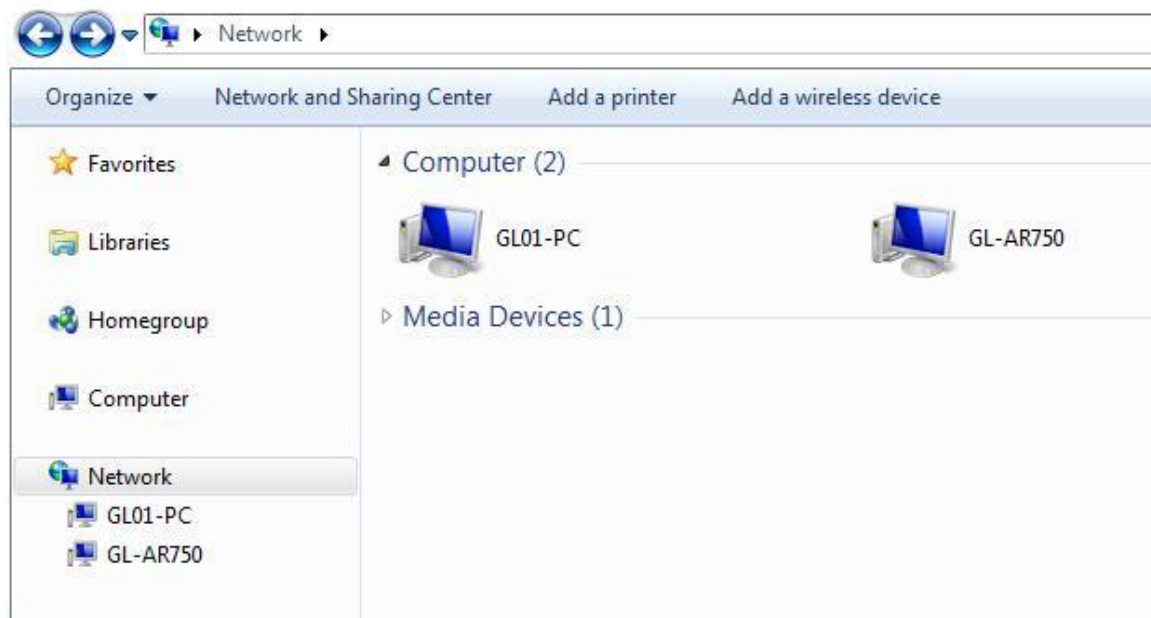
Change the "max protocol = SMB2" to

```
"min protocol = SMB1"
```

"max protocol = SMB3", then **save** and **exit** WinSCP.



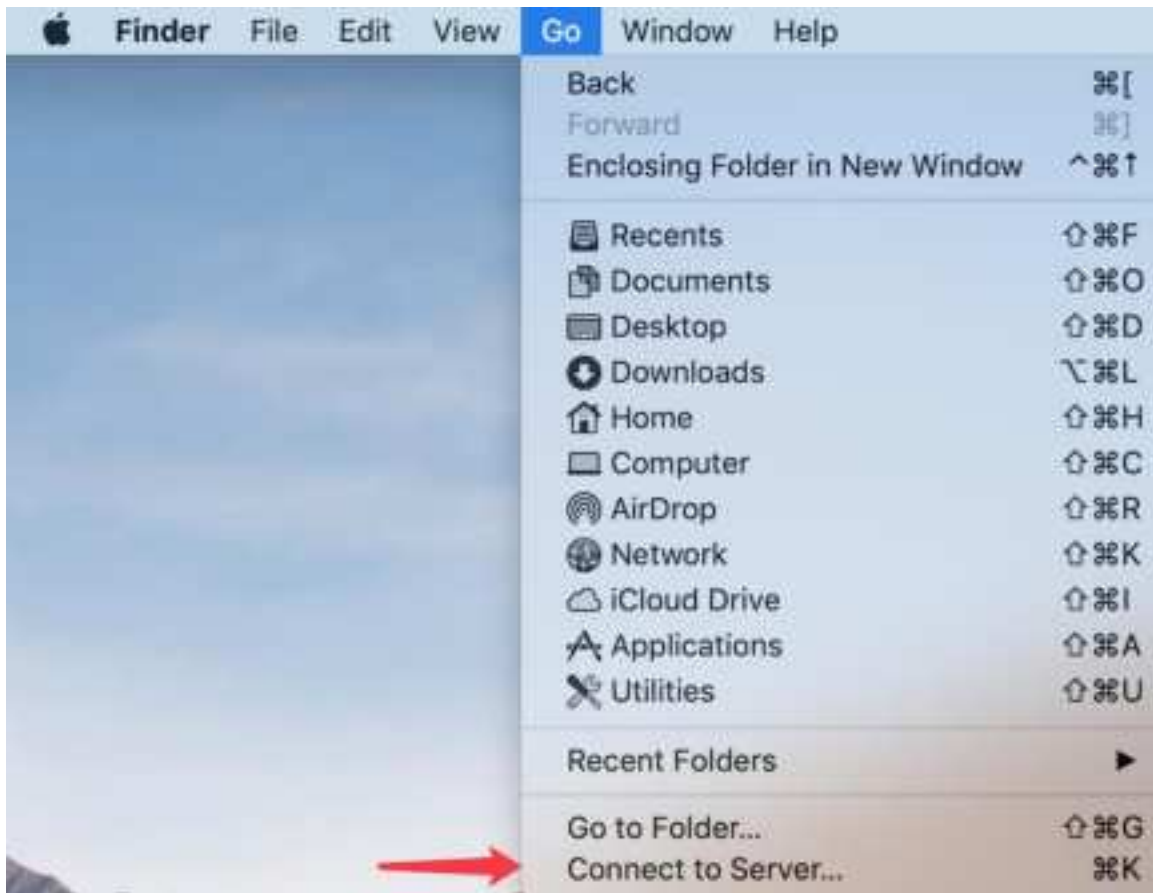
2) Open a Windows explorer, you can find **Network** in the folder directory. Double click your router to access its contents.



Mac OS

Method 1

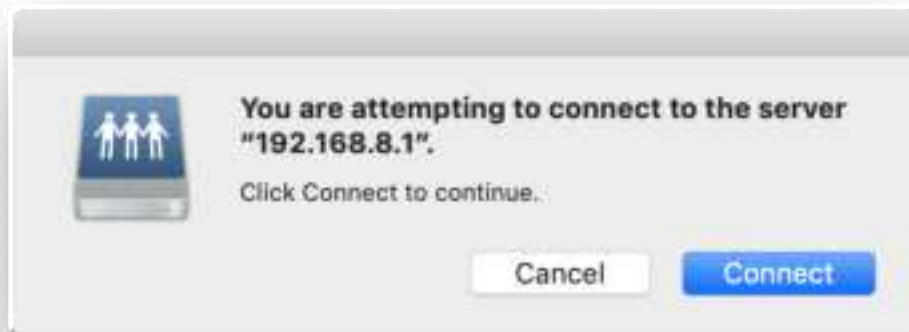
1) Open Finder, Menu -> Go -> Connect to Server...



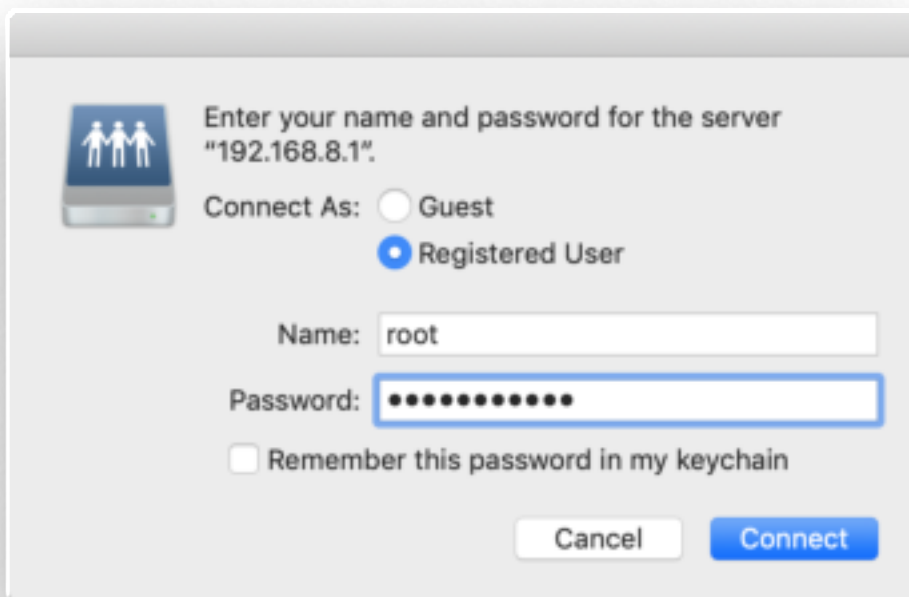
2) Input `smb://192.168.8.1`, you need to change this if your router IP address is not 192.168.8.1



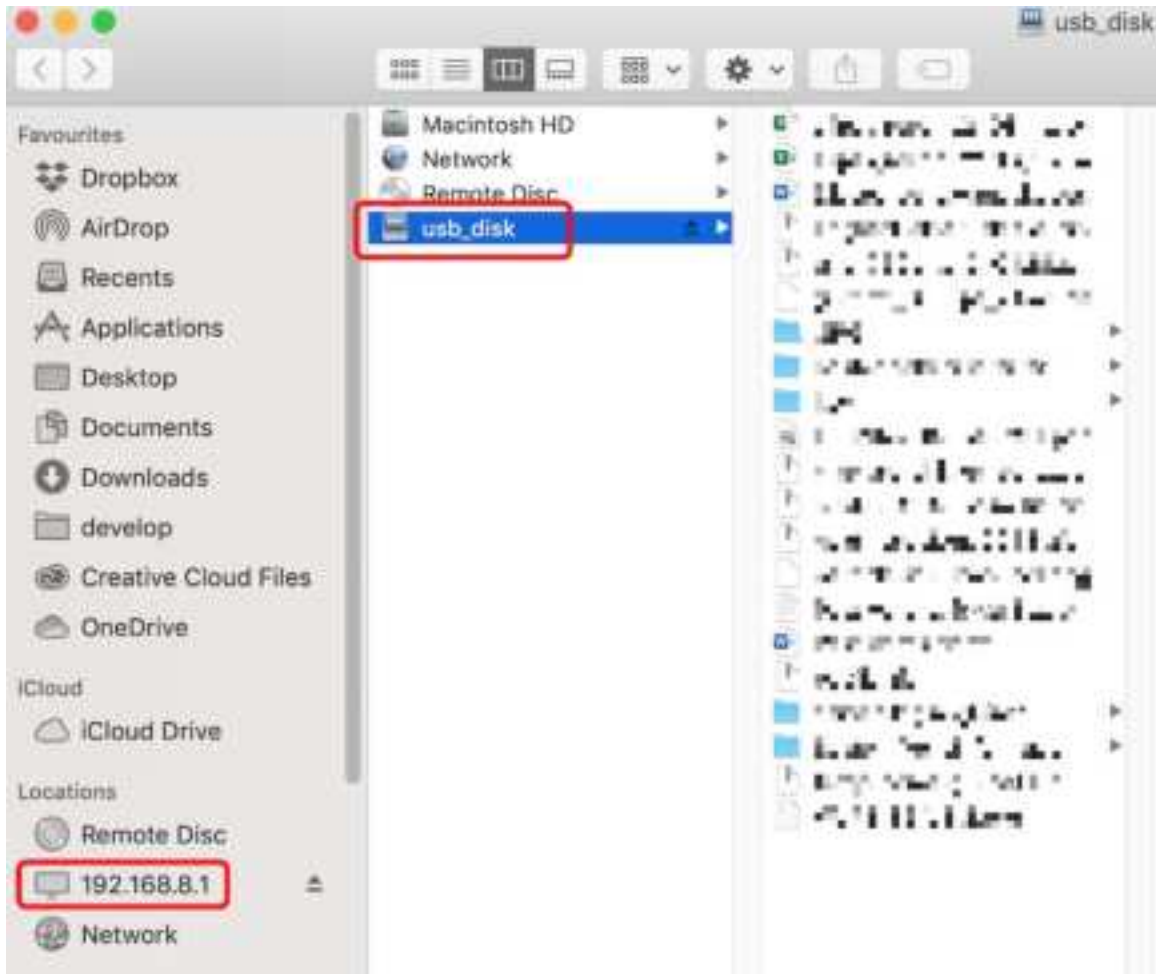
3) Click Connect.



4) Input username and password, they are the same when you login Web Admin Panel.



5) Then Finder will display files of USB disk.



Method 2

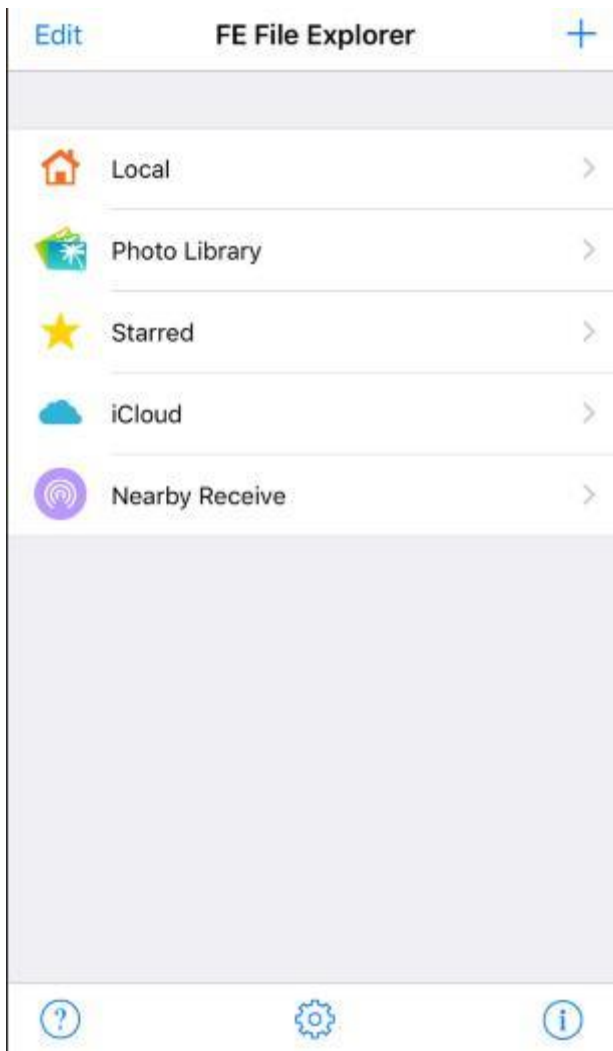
- 1) Go to System Preferences -> Sharing -> File sharing. Click Options and then enable SMB.
- 2) Open Finder. You should be able to find your router under Shared.

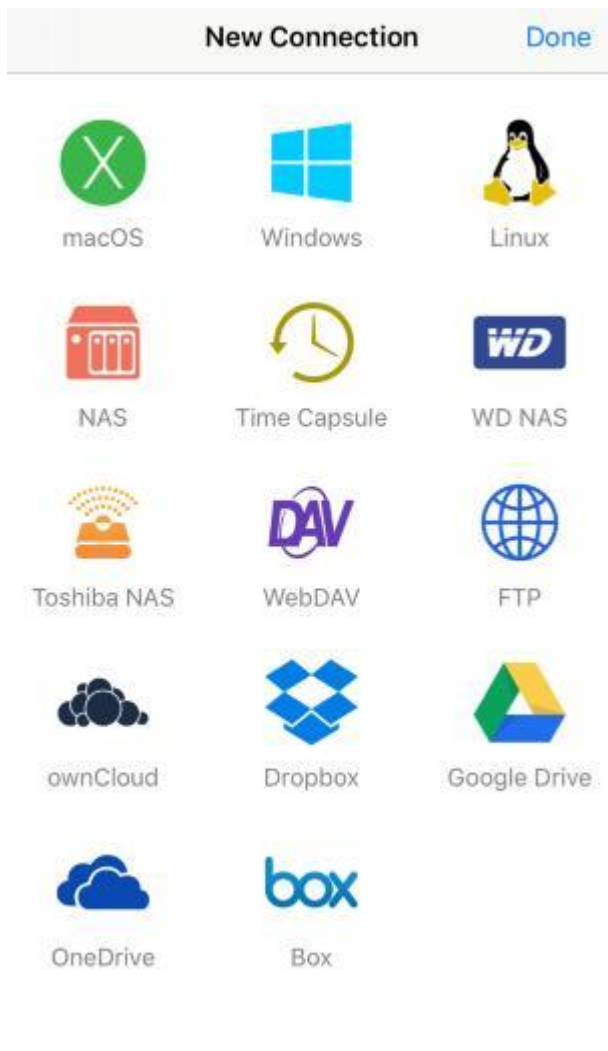
iOS

You have to use file manage app to access the contents of your external storage device.

You may use **FE File Explorer**:

- 1) Click + to create a Windows connection.





2) Enter the **IP address** of your router (192.168.8.1). The **User Name** is root and the **Password** is the one that you use to login the web Admin Panel. Finally, click Save.

[< New Connection](#)[Save](#)

CONNECTION

Display Name	Optional
Host Name/IP	192.168.8.1
DNS Domain	Optional
Path	Optional
Port	445
Show Hidden Files	<input type="checkbox"/>
Show Admin Shares	<input type="checkbox"/>
Support DFS	<input type="checkbox"/>

CONNECT AS

User Name	root
Password	●●●●●●

If you try to access network share in domain, please input 'Domain\User' or 'User@Domain' in 'User Name'

3) Click your newly created connection to access the contents.



Linux

If you are using Linux you are probably comfortable with connecting to servers, and how to do this can vary greatly from distribution to distribution and largely depends on your window manager/display environment. Most systems come with Gnome and it is the default on the very popular Ubuntu distribution, so we'll give an example using the Files tool (also called Nautilus). If you open the app you should have a "Connect to server" option, there you can enter either the `\\servername\share` or `smb://servername/share` format.

ChromeOS or ChromiumOS (Neverware CloudReady and others)

There is a built in Samba/SMB client in the Files app, but it doesn't really seem to work very well. Instead the most useful ChromeOS app to allow mounting Samba shares even though it doesn't have high ratings is "File System for Windows". It is open source and works far better than the built in version.

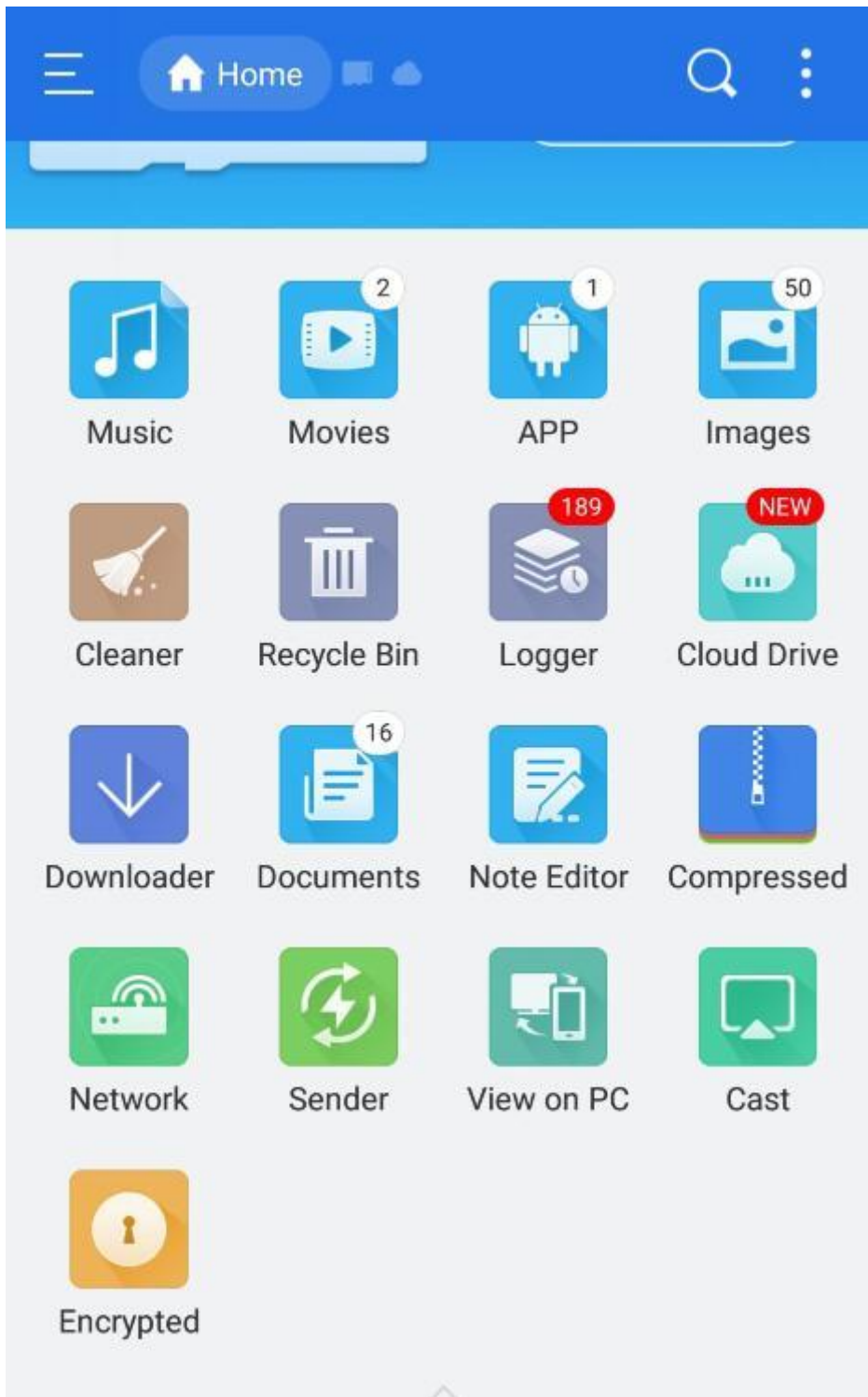
<https://chrome.google.com/webstore/detail/file-system-for-windows/mfhnnfciefdpolbelmfkpmhhmlkehbf/related?hl=en>

Once you have installed the app you can launch it from that page, and if you want to access it again in the future, in the Files app if you go to the 3 dot menu at the top right and "Add new service" you then select "File System for Windows" from the list and it will give you the dialog to fill out with the server name and some other details, but only the server name/IP and share name are required. You can click the gear icon to enable saving the password for a share indefinitely, and you can click the "Keep" button to save the share to easily mount again in the future.

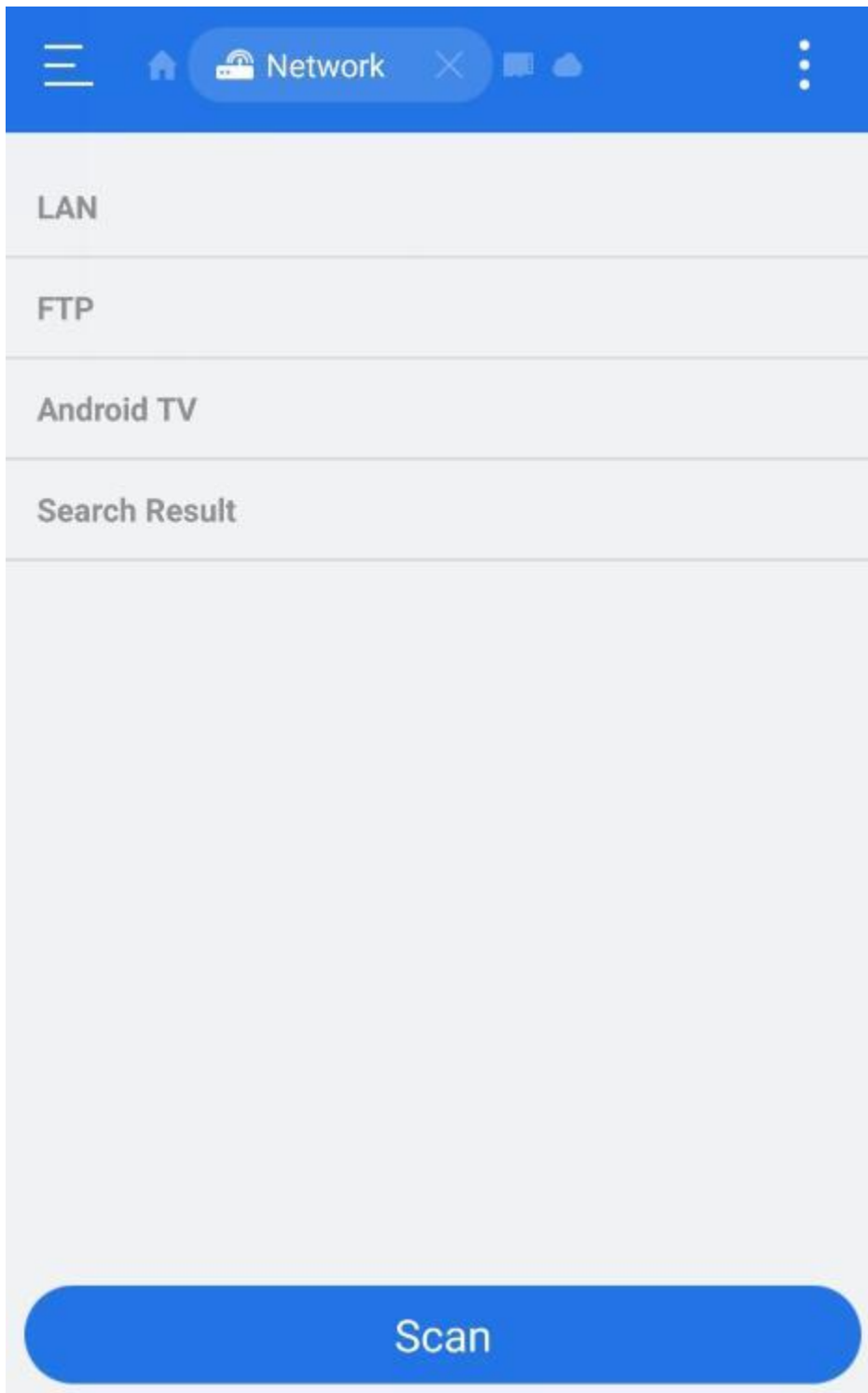
Android

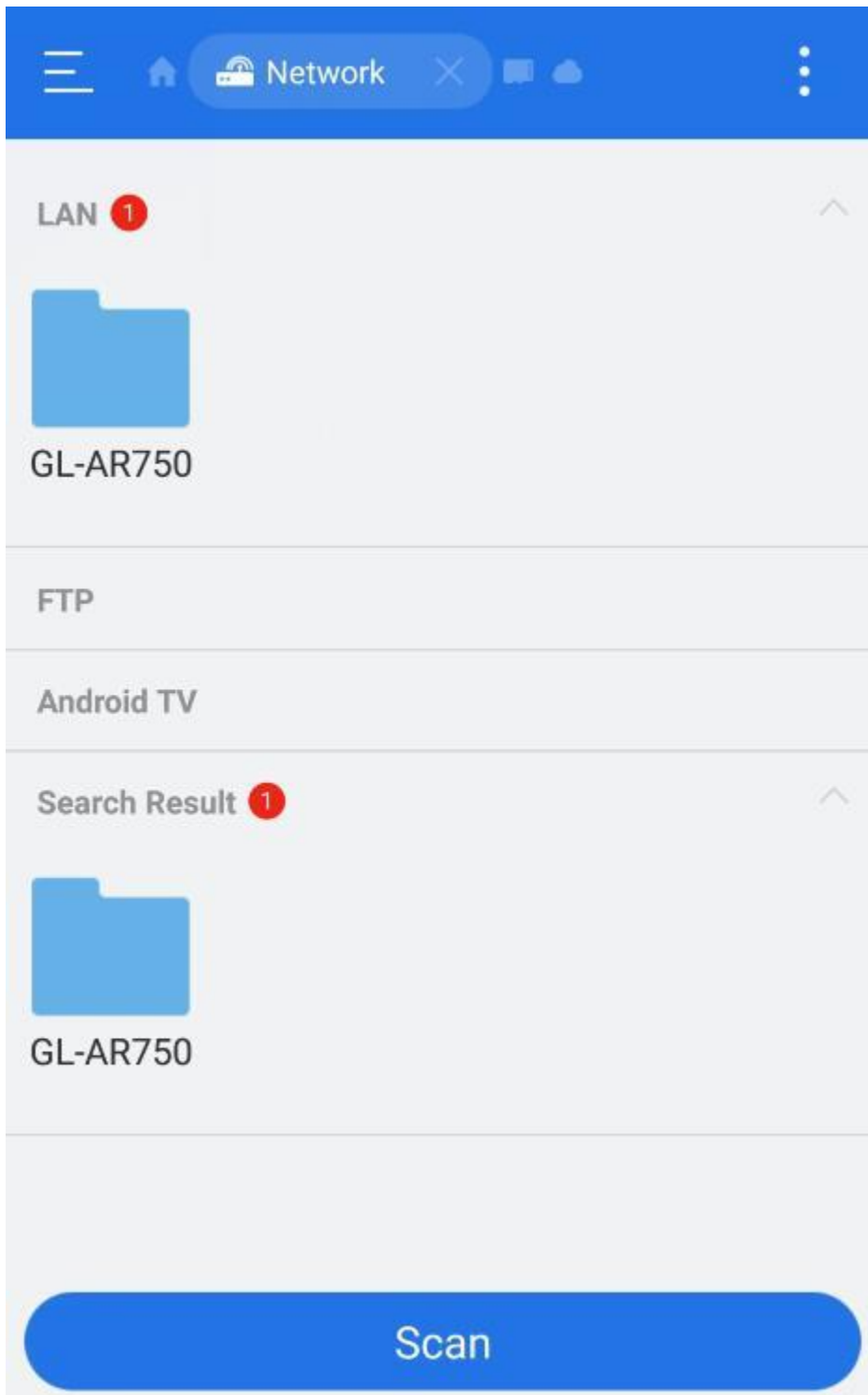
Most Android devices have file manager which you can use to access the contents of your external storage device. Or you can use **ES file explorer**:

- 1) Open the app and then click `Network`.



2) Click Scan to find your network storage device.





8.4. DLNA Server

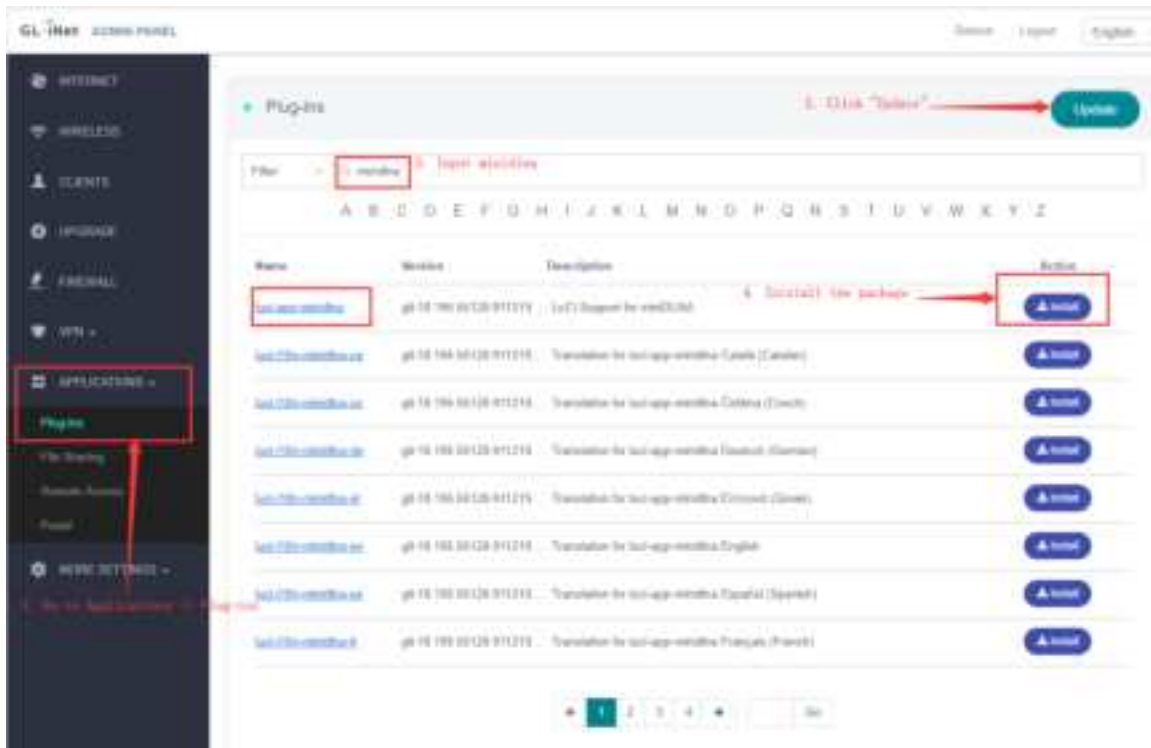
Some of GL.iNet routers support DLNA Server, but this is not a default function. You need to install a little plug-ins to make it workable.

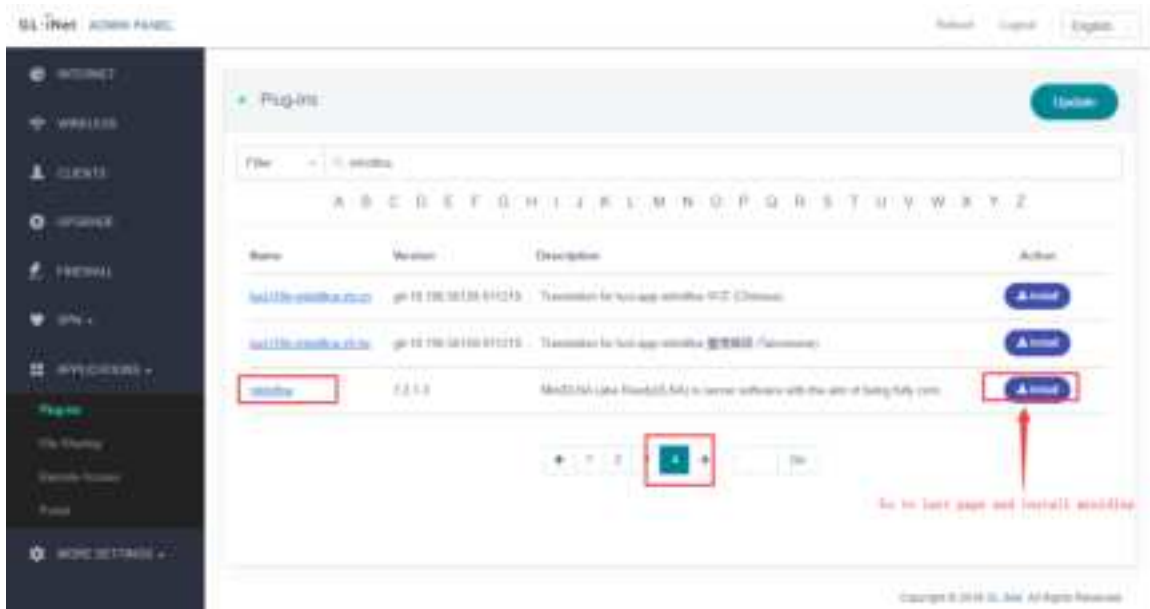
Supporting List: GL-AR750S-Ext, GL-AR750, GL-MT1300, GL-MT300N-V2, GL-AR300M series, GL-AR150 series, GL-MiFi and GL-X750

8.4.1. Install Plug-ins

Go to **APPLICATIONS**, then **Plug-ins**. Install two apps:

1. luci-app-minidlna
2. miniDLNA





8.4.2. Use the DLNA server in GL.iNet Routers

After Installation of two applications, you can now use your GL.iNet router as as DLNA server.

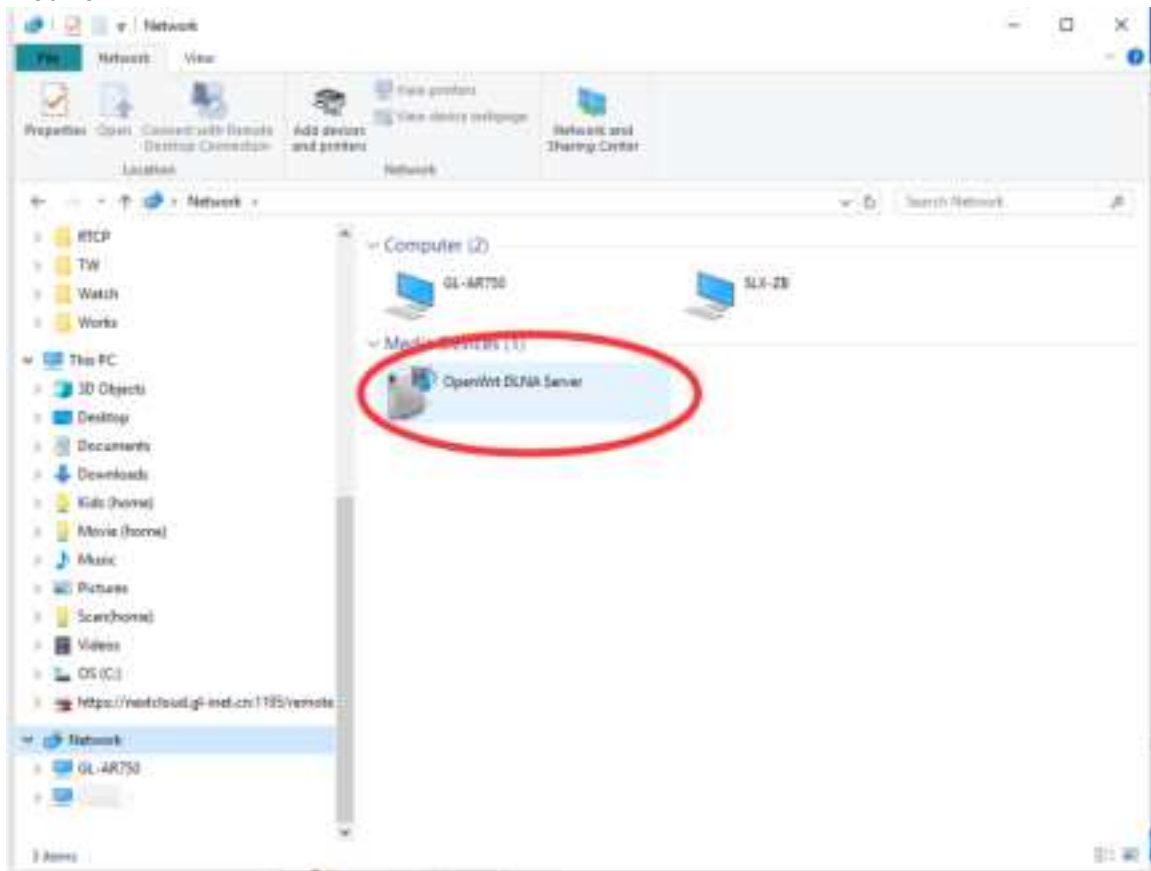
1. Make suer you already has a TF card inserted into the card slot before you power up your router. *Hot-plug* is not supported on GL.iNET routers.
2. Or you can insert an USB drive into the USB port.
3. Connnet your PC, Laptop, tablet, smart TV or Smartphone to GL.iNET router's WiFi(SSID). Here is the sample: GL-MT1300-xxx
4. Then you can find the **OpenWrt DLNA Server** in your devices.

Take Windows as example:

In Windows Media
Player:

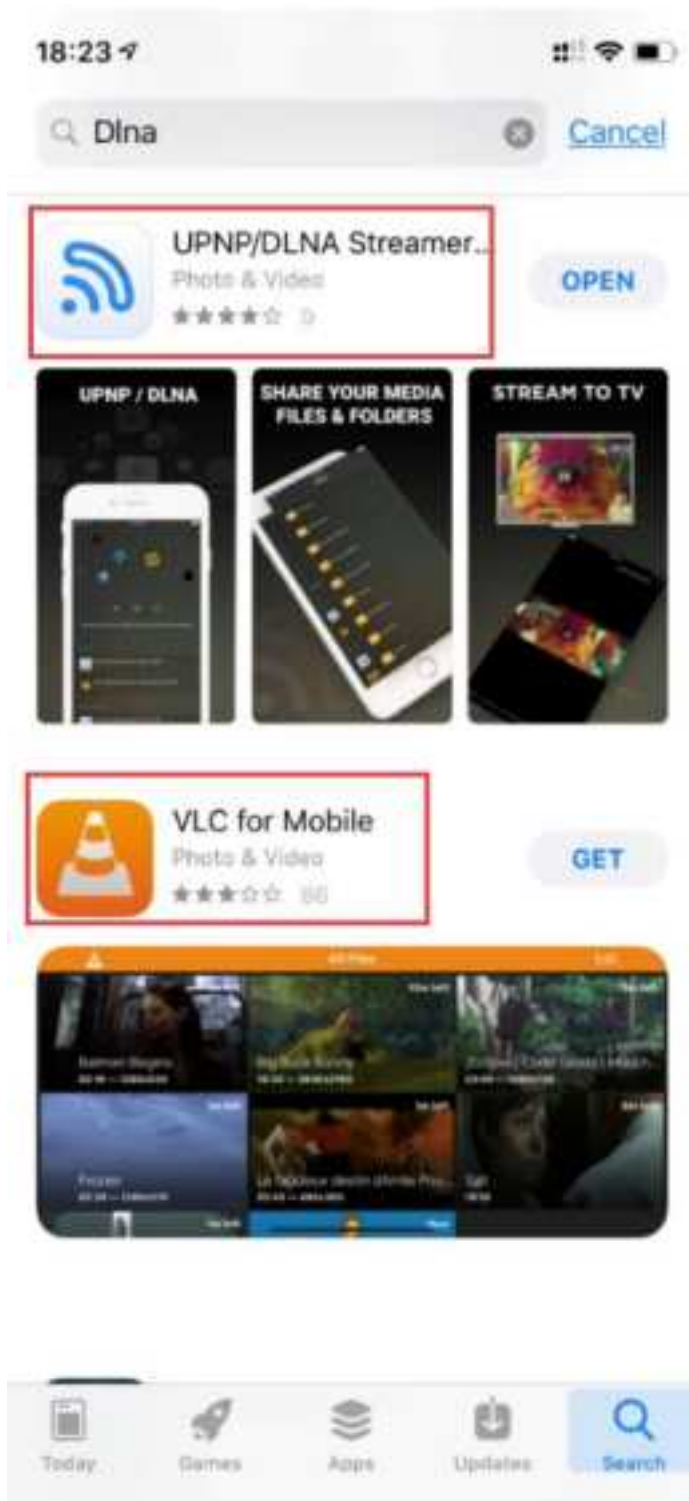


In Windows File Explorer ->
Network



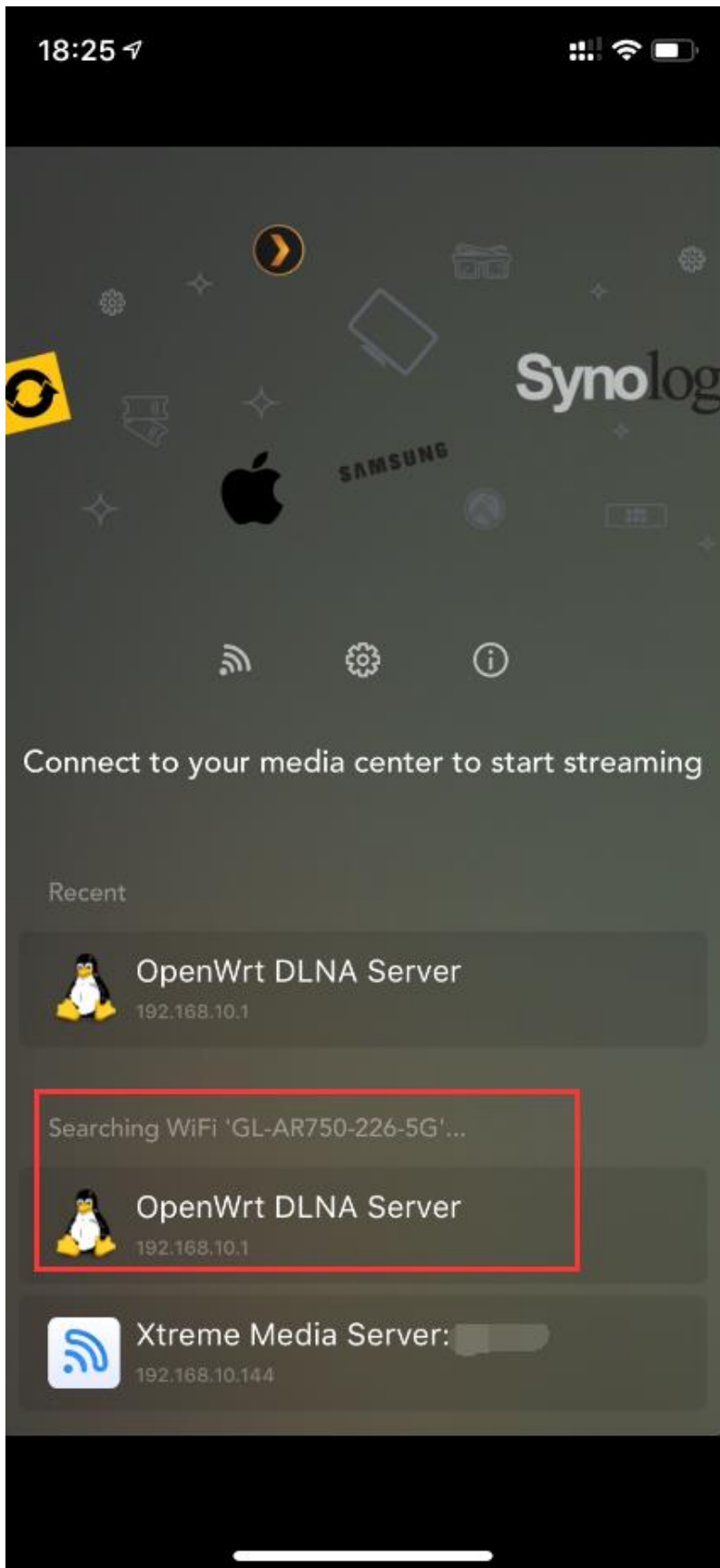
IOS: Install VLC or UPNP Extreme in App Store:

You can easily find the OpenWrt DLNA Sever in UPNP: UPNP Extreme and VLC Installation | UPNP Setup:

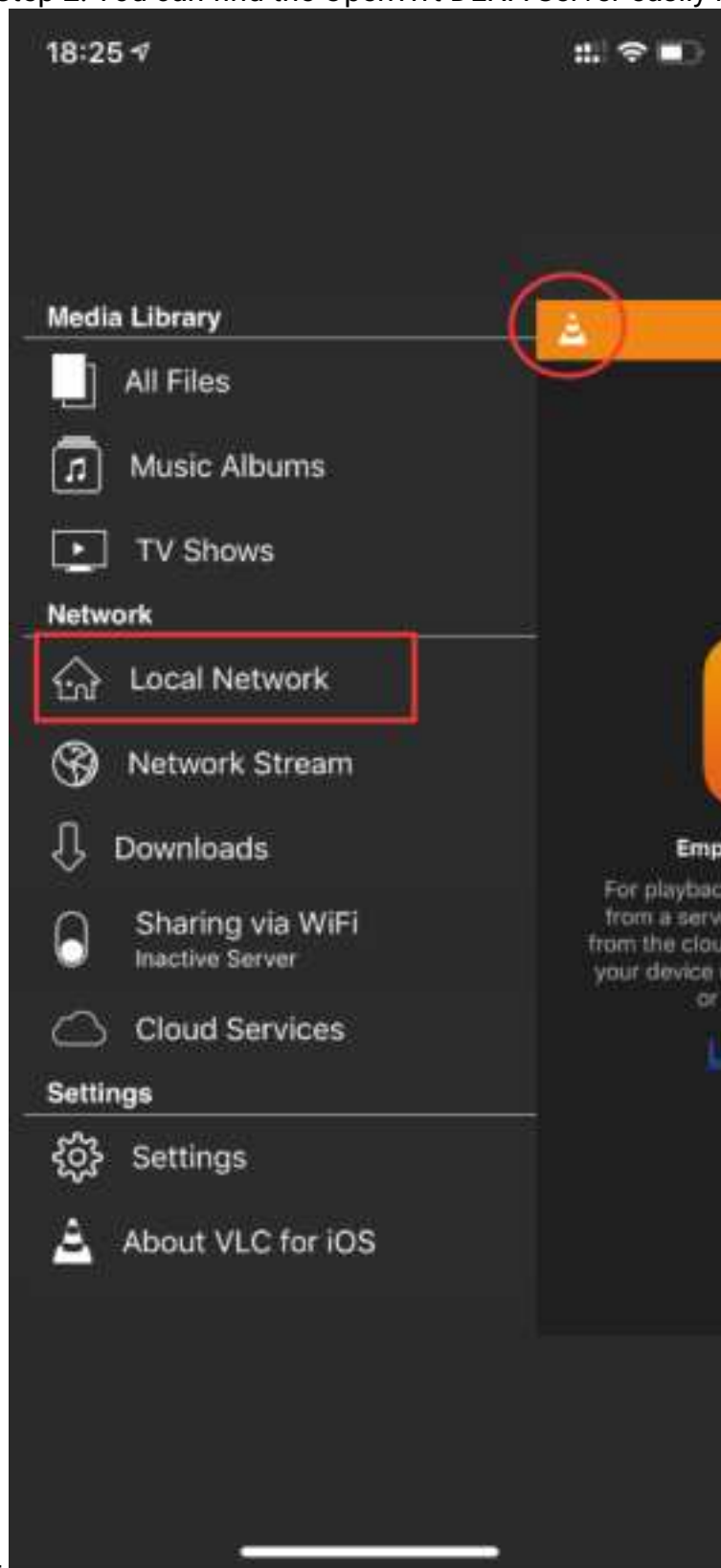


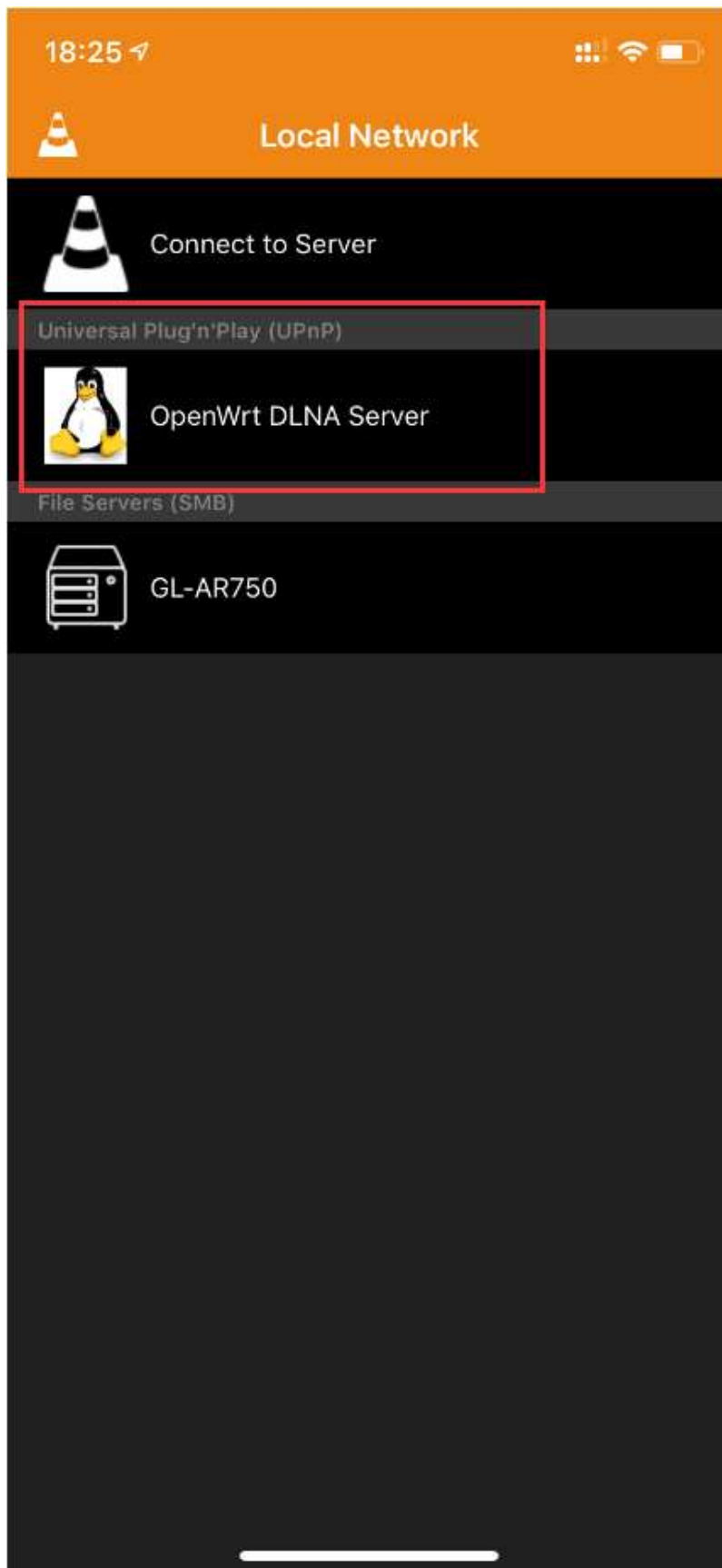
VLC Setup:

Step 1: Click the **Traffic Cones** Logo on the left top, select Local Network



Step 2: You can find the OpenWrt DLNA Server easily in Local Network.





Also other devices can easily find the OpenWrt DLNA Server easily.

Enjoy your media DLNA Server by GL.iNET routers.

8.5. DDNS

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

Setup

DDNS requires firmware v3.010 or higher.

Download firmware file

Open this website to download the latest firmware https://docs.gl-inet.com/en/3/release_notes/

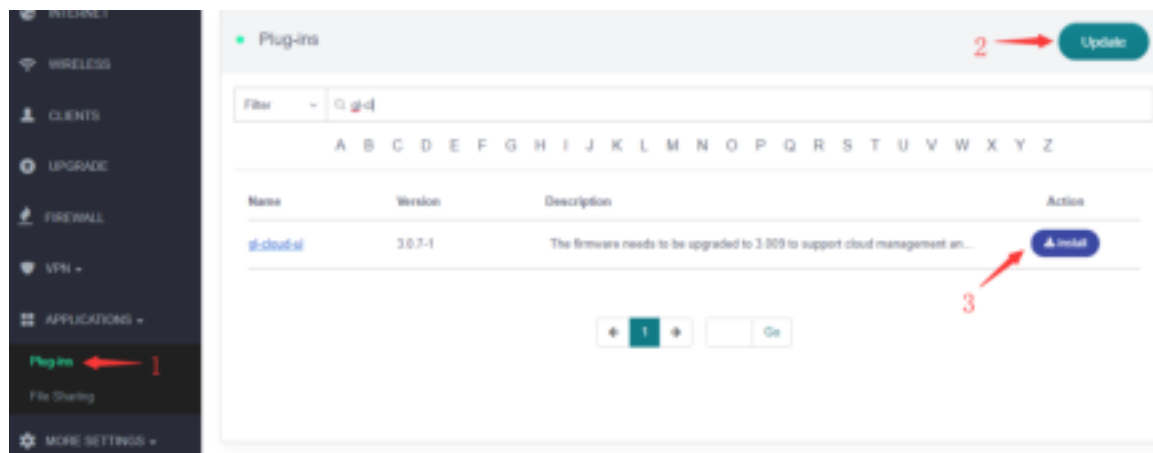
Local upgrade

Open a web browser (we recommend Chrome) to access router Web Admin Panel(default url is <http://192.168.8.1>).

At the left side, UPGRADE -> Local Upgrade, select the firmware file you have downloaded, you can turn off "Keep Settings" for a clean install and more stable, click "Install" button. It takes several minutes to install.

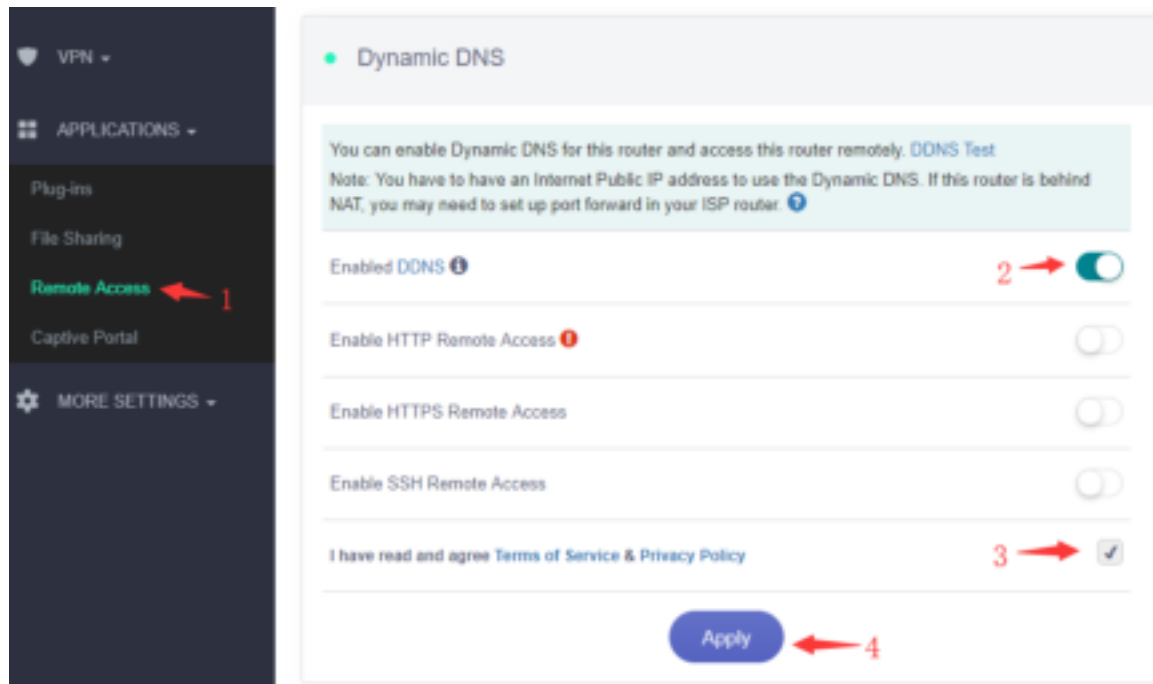
1) Install gl-cloud-ui plug

(If your firmware version is equal or greater than v3.021, please jump to [Step 2](#))



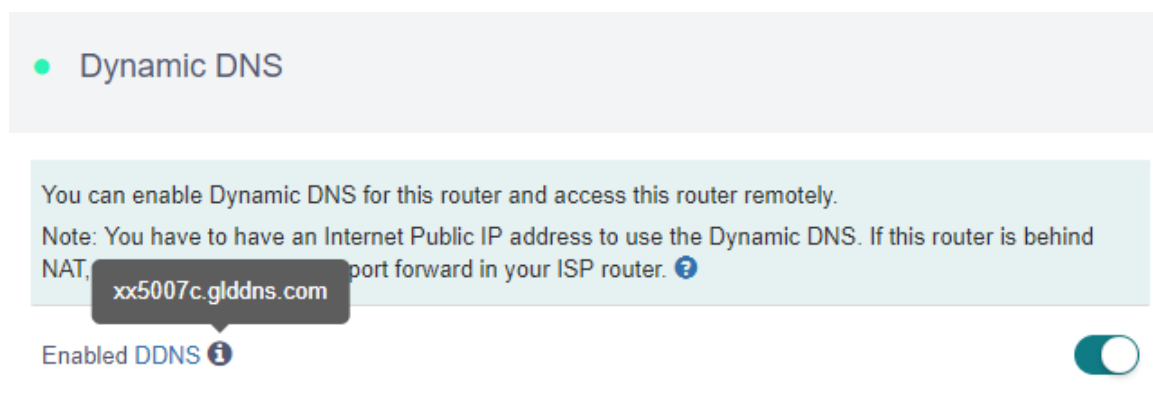
Access to router Admin Panel (default is <http://192.168.8.1>), at the left sidebar, APPLICATIONS -> Plug-ins, click "Update" button to update Plug-ins, then input "gl-cloud-ui" and click "Install" button. After installation, press "F5" to refresh Admin Panel, a new item "Remote Access" will appear inside APPLICATIONS.

2) Enable DDNS



At the left sidebar, APPLICATIONS -> Remote Access, toggle "Enabled DDNS", agree Terms of Services & Privacy Policy, click "Apply" button. Generally, it takes several minutes to take effect.

Move mouse to hover the icon besides "Enabled DDNS", it will display the DDNS url of your device.



The DDNS domain printed on the back label of router has changed. If your DDNS url is xxxxxxxx.gl-inet.com on the back of router, new DDNS url will be xxxxxxxx.glddns.com.

3) Check if DDNS is enabled

Use `nslookup` command to check if your DDNS is enabled. You need to change `xx5007c.glddns.com` to your DDNS url when use `nslookup` command.

nslookup xx5007c.glddns.com 8.8.8.8

```
C:\Users\User>nslookup xx5007c.glddns.com 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: xx5007c.glddns.com
Address: 223.111.111.111
```

The output above means the DDNS url has mapped to a IP address.

4) HTTP Remote Access

This function requires a public network IP.

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

Dynamic DNS

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

Enabled DDNS ⓘ ☒

Enable HTTP Remote Access ⓘ ☒ 1 →

Enable HTTPS Remote Access ☐

Enable SSH Remote Access ☐

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

Apply ← 2

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 url of http, e.g. <http://xxxxxxx.glddns.com>. If you use port forward, you should be access like <http://xxxxxxx.glddns.com:YourExternalPort>.

5) HTTPS Remote Access

This function requires a public network IP.

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

Dynamic DNS

You can enable Dynamic DNS for this router and access this router remotely. [DDNS Test](#)

Note: You have to have an Internet Public IP address to use the Dynamic DNS. If this router is behind NAT, you may need to set up port forward in your ISP router. [?](#)

Enabled DDNS ⓘ

☒

Enable HTTP Remote Access ⓘ

☒

Enable HTTPS Remote Access

1 → ☒

Enable SSH Remote Access

☐

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

☒

Apply

← 2

This function use self-signed certificates, so the browsers will indicate that "Your connection is not private". I will show you how to use it anyway on Chrome iOS. Other browsers are the similar process.

⚠ [REDACTED].glddns.com: [REDACTED]



Your connection is not private

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

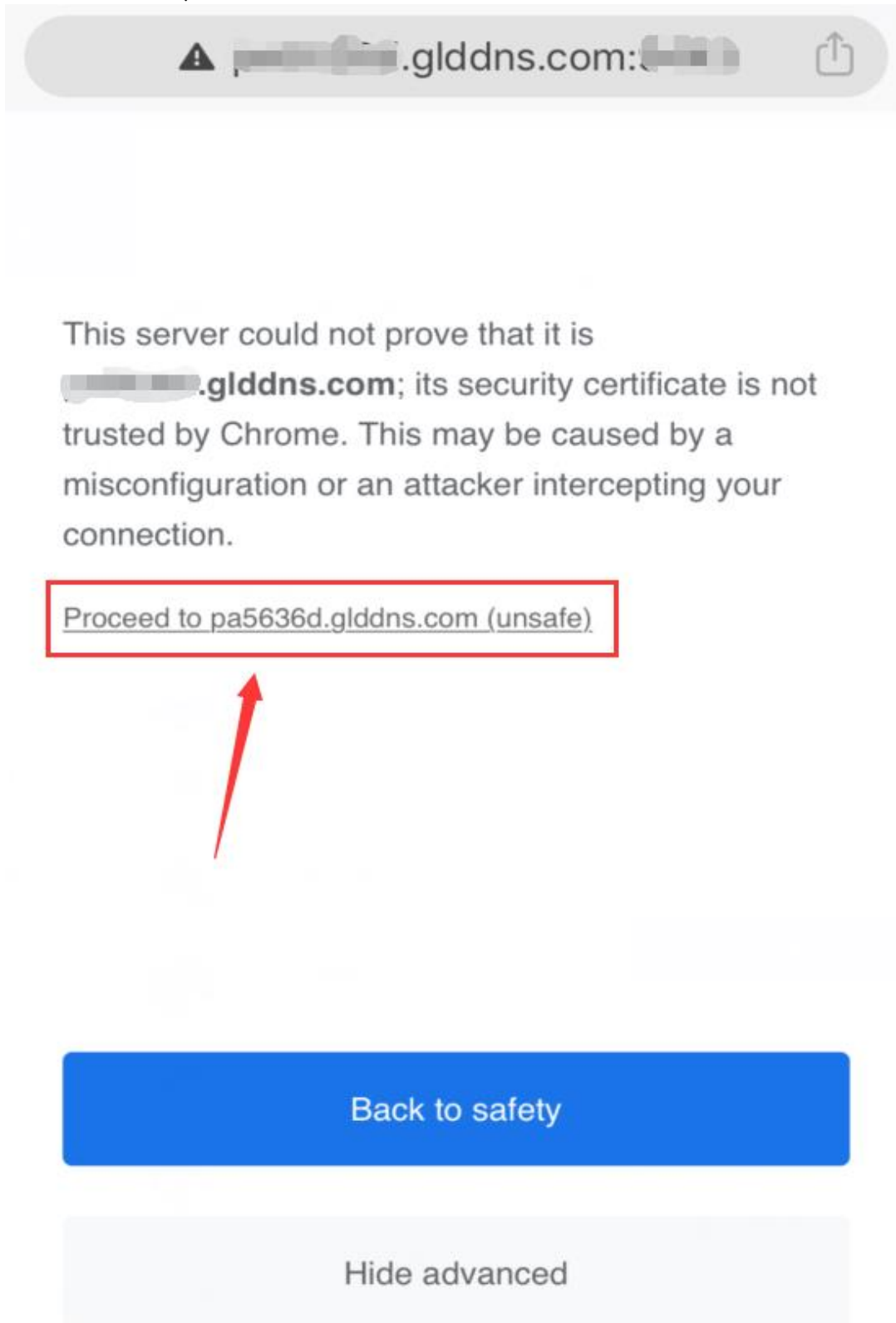
NET::ERR_CERT_AUTHORITY_INVALID

Back to safety



Advanced

As show above, click "Advanced



As show above, click "Processed to xxxxxxxx.glddns.com (unsafe)".

After you enable HTTPS Remote Access, you can access Admin Panel anywhere by your DDNS url of https, e.g. <https://xxxxxxx.glddns.com>. If you use port forward, you should be access like <https://xxxxxxx.glddns.com:YourExternalPort>.

6) SSH Remote Access

This function requires a public network IP.

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


Dynamic DNS

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


Enabled DDNS [?](#)

Enable HTTP Remote Access [!](#)

Enable HTTPS Remote Access

Enable SSH Remote Access 1 

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

Apply 2 

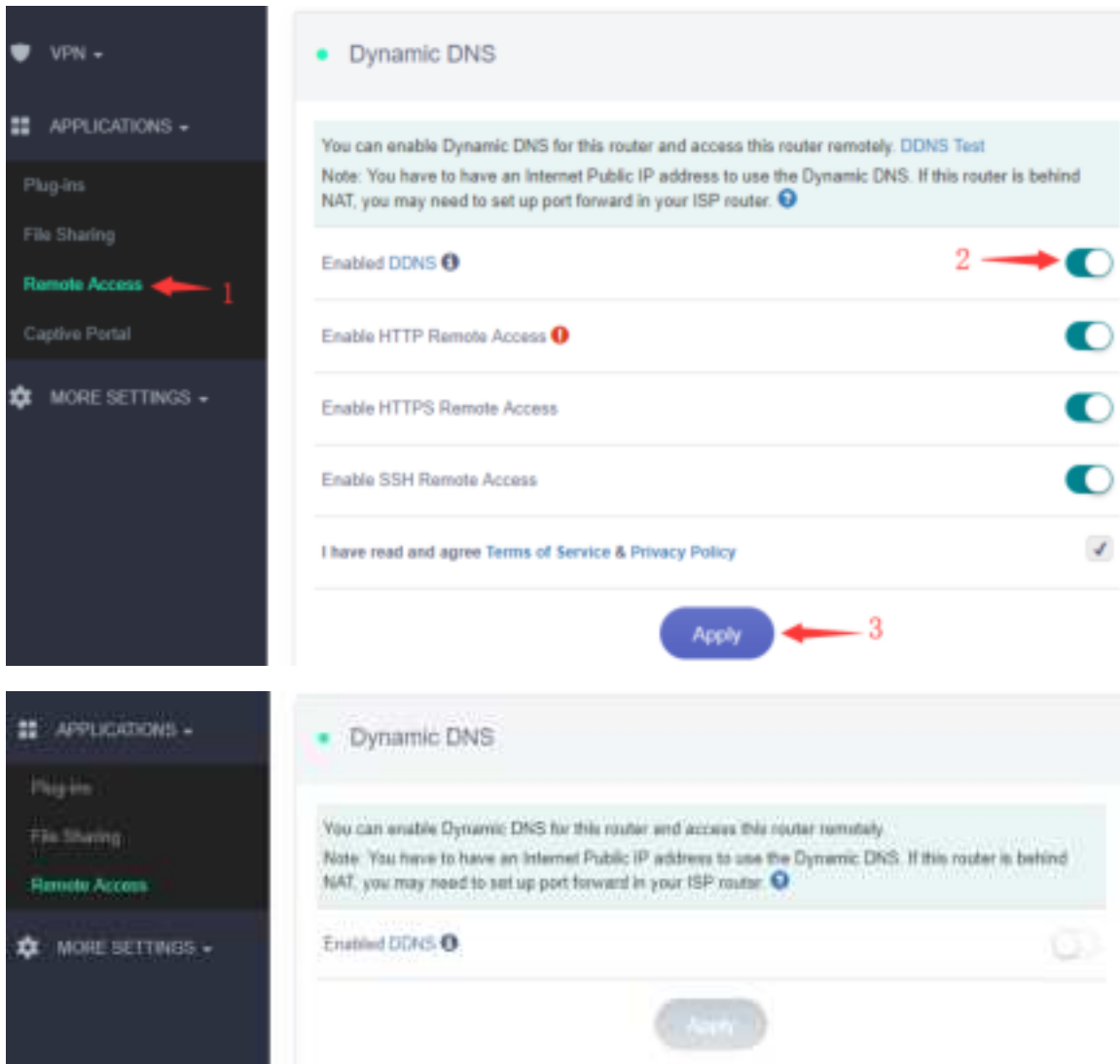
Follow the steps above, to enable SSH Remote Access, then you can ssh to your router anywhere.

7) Turn Off

If you don't want to use DDNS, just disable it.

GL·iNet

Page 91 | 153



After disable DDNS, the interface is like above.

8.6. Cloud

Introduction

GL.iNet GoodCloud cloud management service provide an easy and simple way to remotely access and manage routers.

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

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

GoodCloud only support firmware v3.021 and above right now, we recommend to upgrade to the latest testing version(Pre-release) for better cloud experience.

This document is based on the latest testing firmware.

Download firmware file

Choose the Pre-release column of this url https://docs.glinet.com/en/3/release_notes/

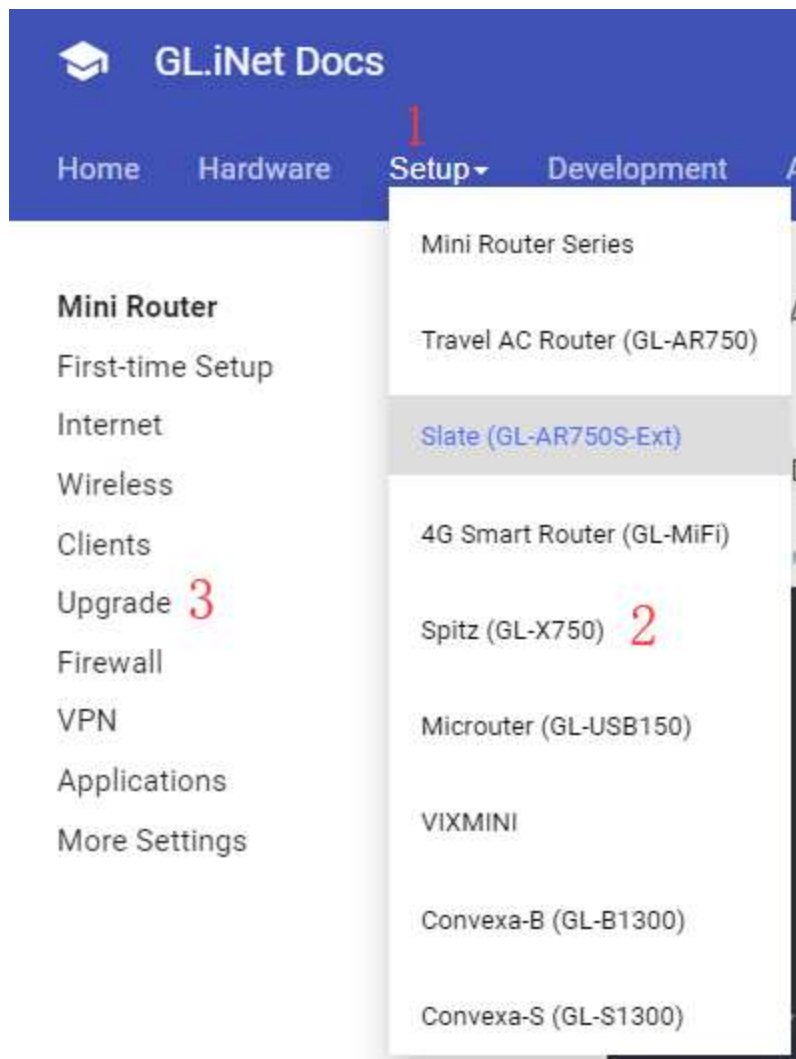
For GL-USB150, it can use GoodCloud too, but it only can be binded to GoodCloud by "Auto discover". (about [Add device](#))

Local upgrade

Open a web browser (we recommend Chrome) and to access router Web Admin Panel (default url is <http://192.168.8.1>).

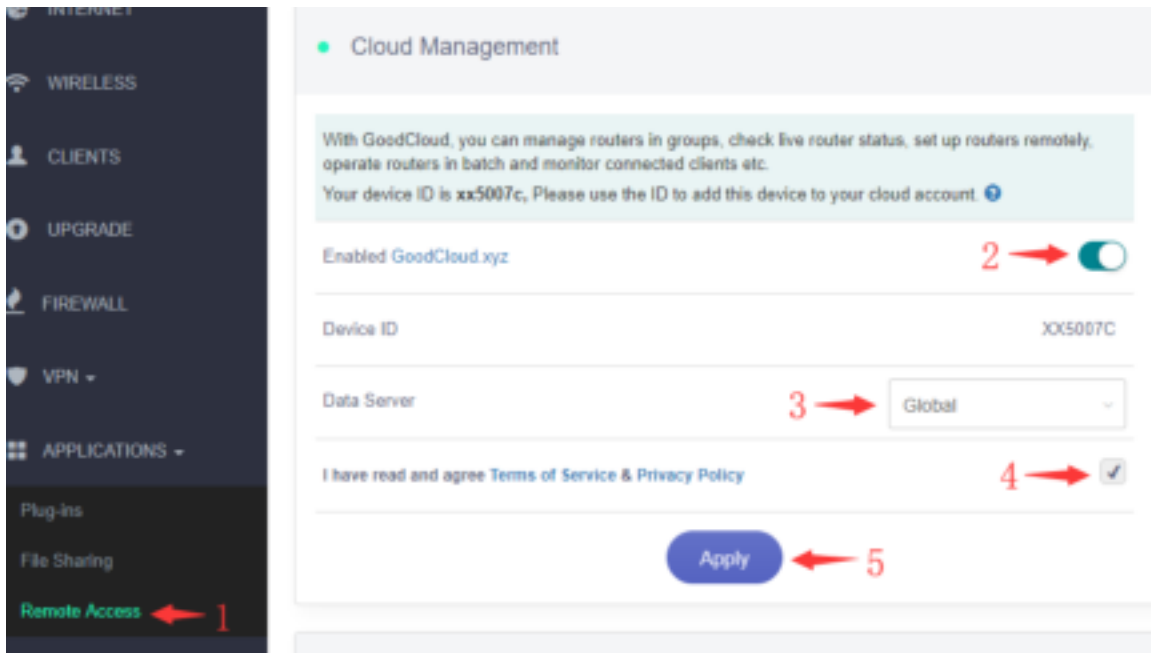
At the left side, UPGRADE -> Local Upgrade, select the firmware file you download, you can turn off "Keep Settings" for more stable, click "Install" button. It takes several minutes to install.

If you want to learn more about upgrade, please scroll top -> Setup -> Choose the model -> Upgrade



Enable Cloud Manage on router Web Admin Panel

Open a web browser (we recommend Chrome) and to access router Web Admin Panel (default url is <http://192.168.8.1>).



Follow the steps above, to enable cloud management feature, choose the Data Server which is nearest your devices located. There are three Data Server, 'Global', 'America' and 'Europe'. If your devices are neither in America nor in Europe, just select 'Global'. Global Data Server is at Japan.

Create GoodCloud account

Visit <https://www.goodcloud.xyz> to access GoodCloud web site by Chrome or your favorite browser.

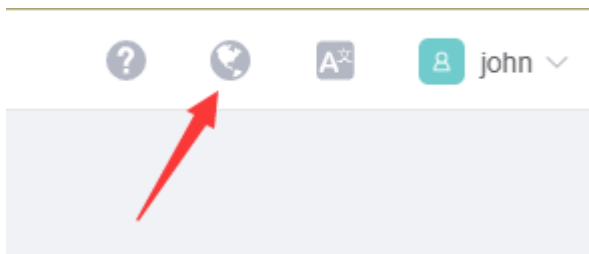
Sign up an account, and sign in. If you don't find the verify email, look in spam or check email later.

If you have any difficulty with sign up, please send email to admin@goodcloud.xyz for help.

Select region

At the first time when you sign in, it will pop up a dialog to let you select the region, select the region that your device selected Data Server on the Web Admin Panel (Step 1.2).

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.

 A screenshot of the 'Add Group' modal form. The form is titled 'Add Group' and has a close button (X) in the top right corner. It contains four input fields: 'Name' (with a red '3' next to it), 'Company', 'Description', and 'Location' (with a search icon and the text 'Search'). Below the input fields is a world map with a location pin. At the bottom right, there are two buttons: 'Cancel' and 'Confirm' (with a red '4' next to it). The background shows the 'Group List' page with a sidebar on the left containing links to 'Dashboard', 'Group List' (with a red '1' next to it), 'Device List', 'Site to Site', 'Template List', 'Task List', and 'Setting'. The top bar shows 'Dashboard / Group List' and a '+ Add Group' button (with a red '2' next to it).

Set the group name, company, description and location.

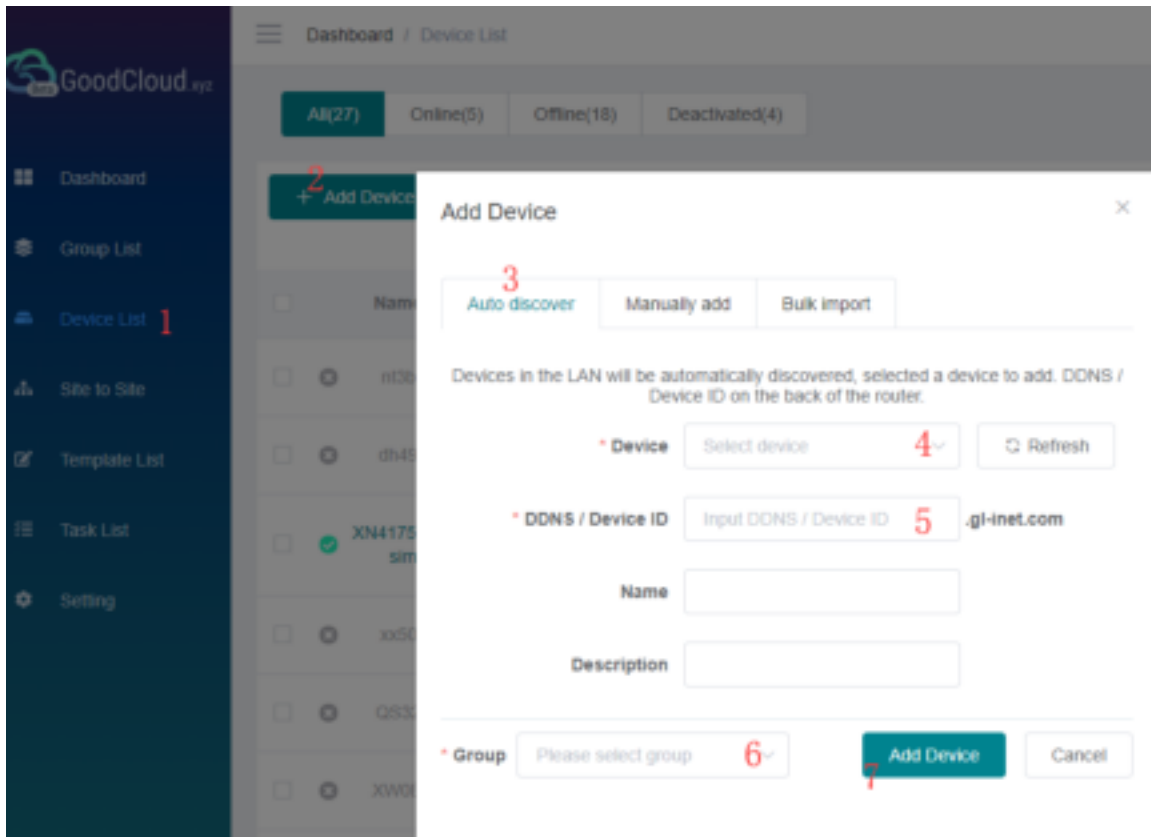
Each device must belong to a group.

Add device

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

Auto discover

Follow the steps below to add your device.



If the router and PC (which opened goodcloud.xyz page) are at the same public IP, it will be automatically discovered, and can be found when click "Device" list. DDNS or Device ID can be found on the back of your router.

PS: Input "DDNS" / "Device ID" here just to verify that the router is really original/valid. DDNS feature and the Cloud feature are separate things.

For most models, it is "DDNS" on the back, but for some new models, it is "Device ID" on the back.

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

Click "Refresh" to force auto discover devices again.

Auto discover	Manually add	Bulk import
-------------------------------	------------------------------	-----------------------------

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

* **Device** 

* **DDNS / Device ID**

Model: mifi Mac: e4956c ssid: GL-MIFI

Name

Description

* **Group**

Please select group



Add Device

Cancel

Manually add

If it can't discover automatically, try "Manually add". All information that need to input can be found on the back of the router.

PS: Input "MAC", "SN" and "DDNS" / "Device ID" here just to verify that the router is really original and valid. DDNS feature and the Cloud feature are separate things.

Add Device

Auto discover **Manually add** Bulk import

The information need to input below can be found on the back of the router:

* MAC

* S/N

* DDNS / Device ID

Name

Description

* Group

Add Device Cancel

GL·iNet
750M Travel AC Router

Model: GL-AR750
Input: 5V \Rightarrow 2A
IP: 192.168.8.1
SSID: GL-AR750-ba1
Key: goodlife
MAC: E4:95:6E:40:00:00
S/N: 7c0be4bb45d9000
DDNS: hh00000.gl-inet.com
FCC ID: 2AFIW-AR750

For some new models, DDNS has been changed to Device ID on the back of router.

Auto discover **Manually add** Bulk import

The information need to input below can be found on the bac

* MAC

* S/N

* DDNS / Device ID

Name

Description

* Group

Add Device Cancel

GL·iNet
Spitz 4G LTE Smart Rou

Model: GL-X750C4
Input: 12V \Rightarrow 1.5A
IP: 192.168.8.1
MAC: E4:95:6E:40:00:00
SSID: GL-X750-ba1
Key: goodlife
Device ID: hh00000
S/N: 7c0be4bb45000000
FCC ID: 2AFIW-X750C4

Bulk import

"Bulk import" is for user who have a great number of devices to add. By "Bulk import" you can import many devices by a Microsoft excel file.

Bound info on router Web Admin Panel

After you successfully add router to GoodCloud, go back to router Web Admin Panel,

APPLICATION -> Remote Access -> Cloud Management,

press 'F5' to refresh this page, It will display the binded GoodCloud username, hover the username it will show the corresponding GoodCloud email account.

Cloud Management

With GoodCloud, you can manage routers in groups, check live router status, set up routers remotely, operate routers, manage connected clients etc.

The device is bound by john on 12-7-2018 16:25. [Unbind](#)

Enabled [GoodCloud.xyz](#)

your GoodCloud username

Device ID

XX5007C

Data Server

Europe

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

☒

Apply

[View Logs](#)

Click 'View Logs' will show api call logs by GoodCloud.

Unbind router

● Cloud Management

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

The device is bound by john on 12-7-2018 16:25. [Unbind](#)

Enabled [GoodCloud.xyz](#)



Device ID

XX5007C

Data Server

Europe

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



Apply

[View Logs](#)











If you want to unbind router, click Unbind button.

If you have any difficulties, please send email to admin@goodcloud.xyz for help.


Manage your devices


[devices info and status](#)


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

<div> <div>All(27)</div> <div>Online(5)</div> <div>Offline(18)</div> <div>Deactivated(4)</div> </div>							
<div> <div>+ Add Device</div> <div>⌵ Bulk Action</div> <div>🔍</div> <div>☰</div> <div>More Filter</div> </div>							
<input type="checkbox"/>	Name	SSID	Version	Type	Model	Update time	Actions
<input type="checkbox"/>	 XN41758_5 2s_simon	GL-AR750-758 GL-AR750-758-5G	3.026	router	GL-AR750	2019-07-26 00:51	
<input type="checkbox"/>	 NC30314_5 2s_home	GL-AR750-314 GL-AR750-314-5G	3.026	s2s	GL-AR750	2019-07-29 21:49	
<input type="checkbox"/>	 cn30306-wg client	GL-AR750-3b6 GL-AR750-3b6-5G	3.026	router	GL-AR750	2019-07-29 12:28	
<input type="checkbox"/>	 TB397BC_5 2s_HKSTP	GL-AR750-7bc GL-AR750-7bc-5G	3.026	s2s	GL-AR750	2019-07-25 18:17	
<input type="checkbox"/>	 YK000E8	GL-AR150-0a0	3.026	s2s	GL-AR150	2019-07-25 18:17	

there is icon at the first column of this table,

 means this device is online.

 means this device is offline.

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



Select the column you want to display.

"Online time" is the latest time when device connected GoodCloud.

"Offline time" is the latest time when device disconnected GoodCloud.

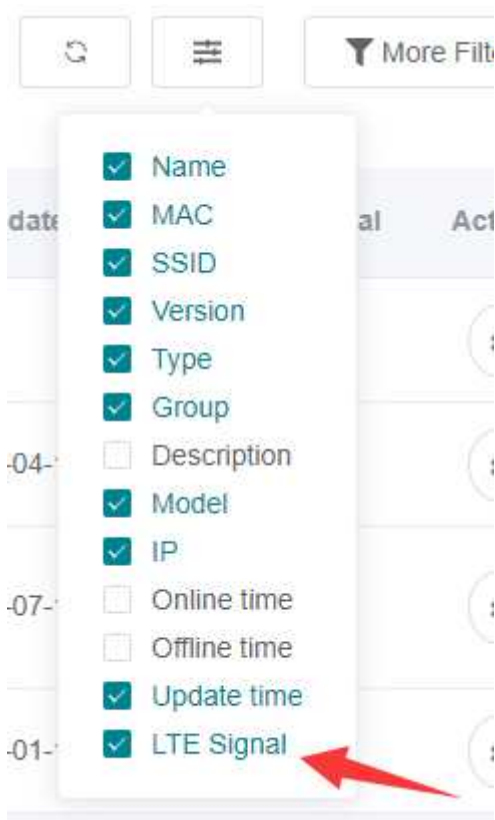
"Update time" is the latest time when device connected or disconnected GoodCloud.

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

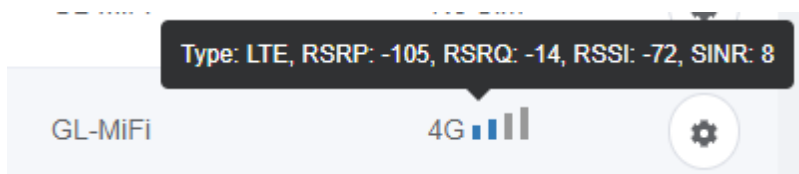
[LTE Signal](#)

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

Toggle the column on Device List page.





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







Device detail info




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

+ Add Device

 Bulk Action 

<input type="checkbox"/>	Name 
<input type="checkbox"/>	<div><div></div><div>XN41758_s2s_simon </div></div>
<input type="checkbox"/>	<div><div></div><div>NC30314_s2s_home</div></div>

Device info

DEVICE INFO			
		MA3301C 	
	B1300-Home		
	Group: Home-HK		
	Model:	GL-B1300	Type: router
	MAC Address:	E4 95 6E 40 00 00	IP Address: 223.223.223.223
	S/N:	ec59e14400000000	Firmware: 3.012

WiFi

2.4G WiFi (Private)	5G WiFi (Private)	5G WiFi (Guest)	2.4G WiFi (Guest)
			
SSID: GL-B1300-01C-SG	SSID: GL-B1300-01C-SG	SSID: GL-B1300-01C-SG	SSID: GL-B1300-01C-SG
Channel: auto	Channel: auto	Channel: auto	Channel: auto
SSID Visibility: Shown	SSID Visibility: Shown	SSID Visibility: Shown	SSID Visibility: Shown
TX Power (dBm): 	TX Power (dBm): 	TX Power (dBm): 	TX Power (dBm): 
			

Modify all WiFi settings.

Router status



Client list

#	Name	IP	MAC	Speed	Traffic	Interface	Block	Action
1	Leo-Wifi0	192.168.26.100	16:80:24:97:00:00	5.875 B/s 4.70.0 B/s	2.44.1 MB 4.700.0 MB	Wired	<input type="checkbox"/>	Set Cancel
2	192.168.26.101	192.168.26.101	84:95:8E:AA:20:04	2.00 B/s 4.00 B/s	2.14 B 4.00 B	Wired	<input type="checkbox"/>	Set Cancel

Timeline

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

The screenshot shows the GoodCloud app interface. On the left is a sidebar with navigation options: Dashboard, Group List, Device List, and Setting. The main area has two tabs: Overview and Timeline. The Timeline tab is selected, and it contains sub-tabs: All, Device log, Operation log, and Others. The 'All' sub-tab is active, displaying a list of events:

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

Set email alarm

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

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

Alarm Rules

×

When

device online/offline

Then

delay 2 minute to send notification

Enable:

device online/offline

new client connected

Cancel

Create

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

Alarm Rules

ⓘ

The following alarm information will be sent to Email.

Create alarm rules

•

When a device is online/offline for 2 minutes, send notification.

🔗

🗑️

•

When a client is connected, send notification.

🔗

🗑️

Email Account

ⓘ

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

Add an email account

✉️

Email

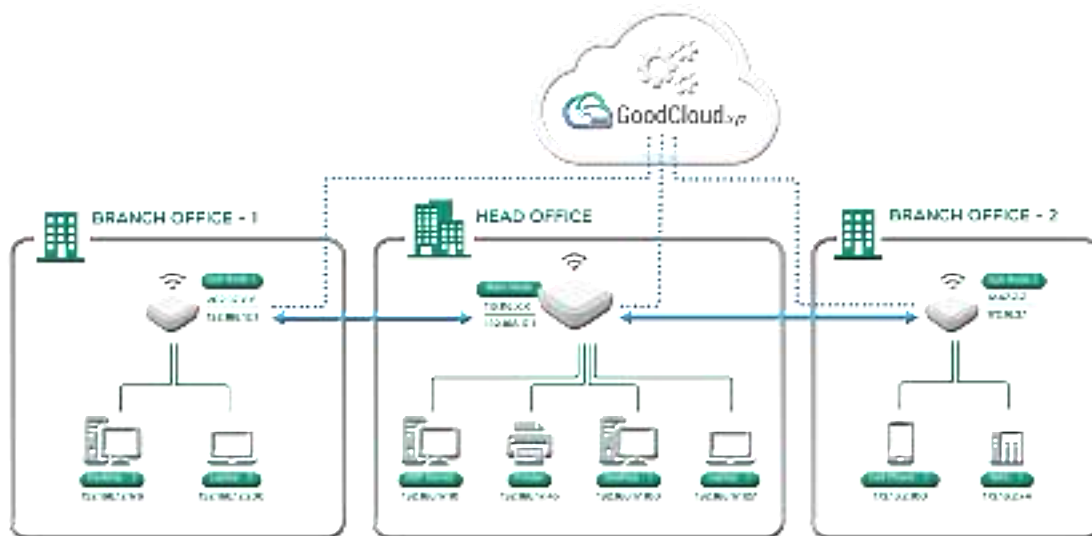
#	Email	Status	Action
1	• john@gmail.com	Enable	<div>🔗</div> <div>🗑️</div>

Site to Site

Site to Site only support firmware v3.026 and above.

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.



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

Scenario 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 while preventing access to their separate internets.

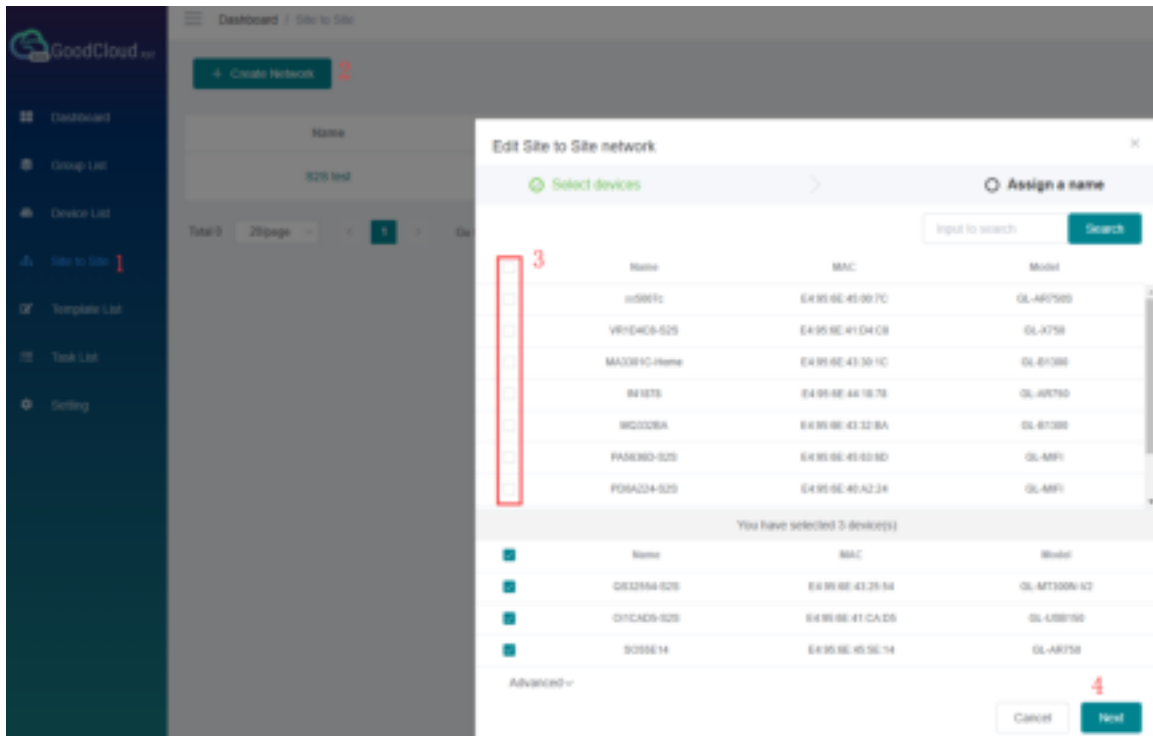
Scenario 3: A family has IP camera and when they are not at home, the Site to Site allows to remote access the IP camera.

What conditions do I need to create Site to Site?

One of the locations has a public static (or dynamic) IP, and two or more GL.iNet devices with latest testing firmware.

Steps to build a Site to Site network.

1. Upgrade your GL.iNet devices to latest testing firmware and binded to [Goodcloud.xyz](https://goodcloud.xyz). ([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 device's performance, each Site to Site network can have up to 10 devices.

After you had chosen the devices, click Continue.

The screenshot shows the 'Create a Site to Site network' dialog in the 'Assign a name' step. The dialog has a header with 'Select devices' and 'Assign a name' tabs. Below the tabs, there are two input fields: 'Name' with the value 'S2S test' and 'Description' with the value 'Office 1 <-> Office2'. At the bottom right, there are 'Back' and 'Next' buttons, with the 'Next' button being highlighted in teal.

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 forwarding.

You can also change port and try again.



Node Usability Testing

100%

No device can be used as the Main Node of Site to Site, please make sure that:

- One of routers has a public IP, dynamic public IP works.
- Port is open, default is 51830. [Change Port](#)
- If the router is behind NAT, you may need to set up port forwarding.

 Help

Cancel

Try again

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



Node Usability Testing

0%

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

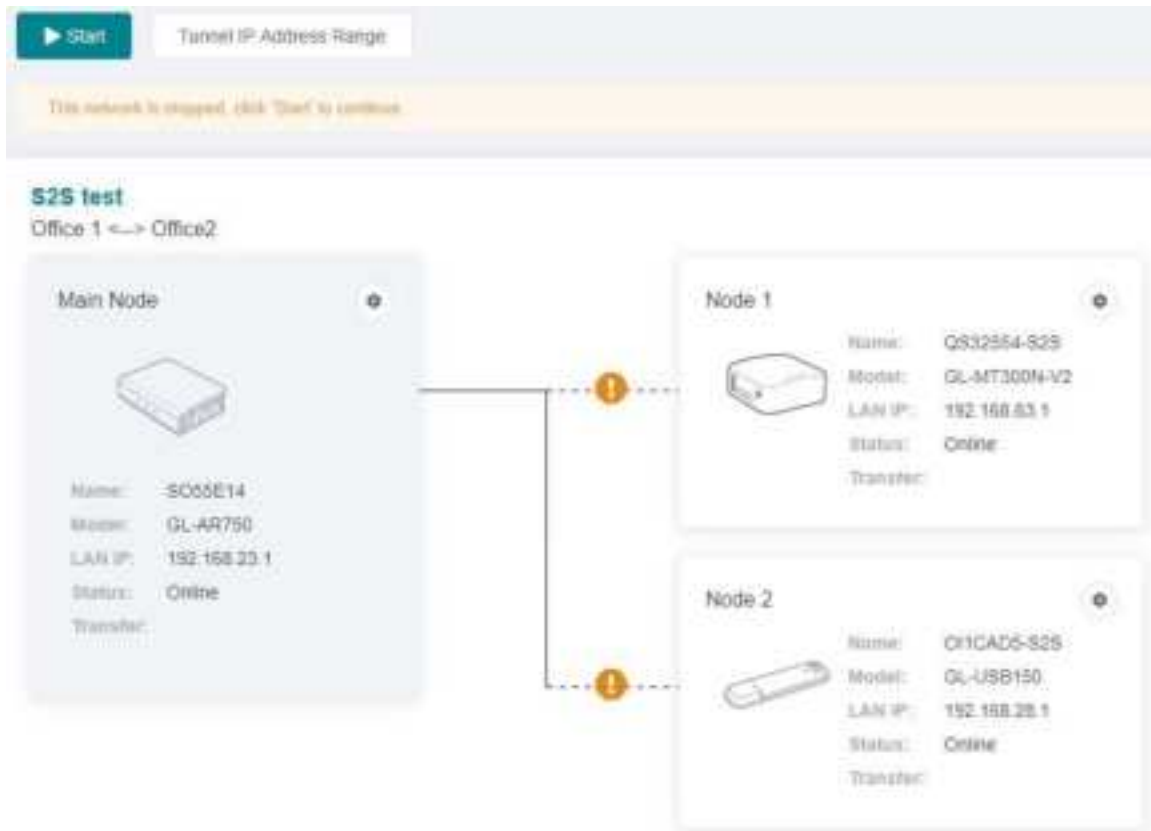
 Help

Cancel

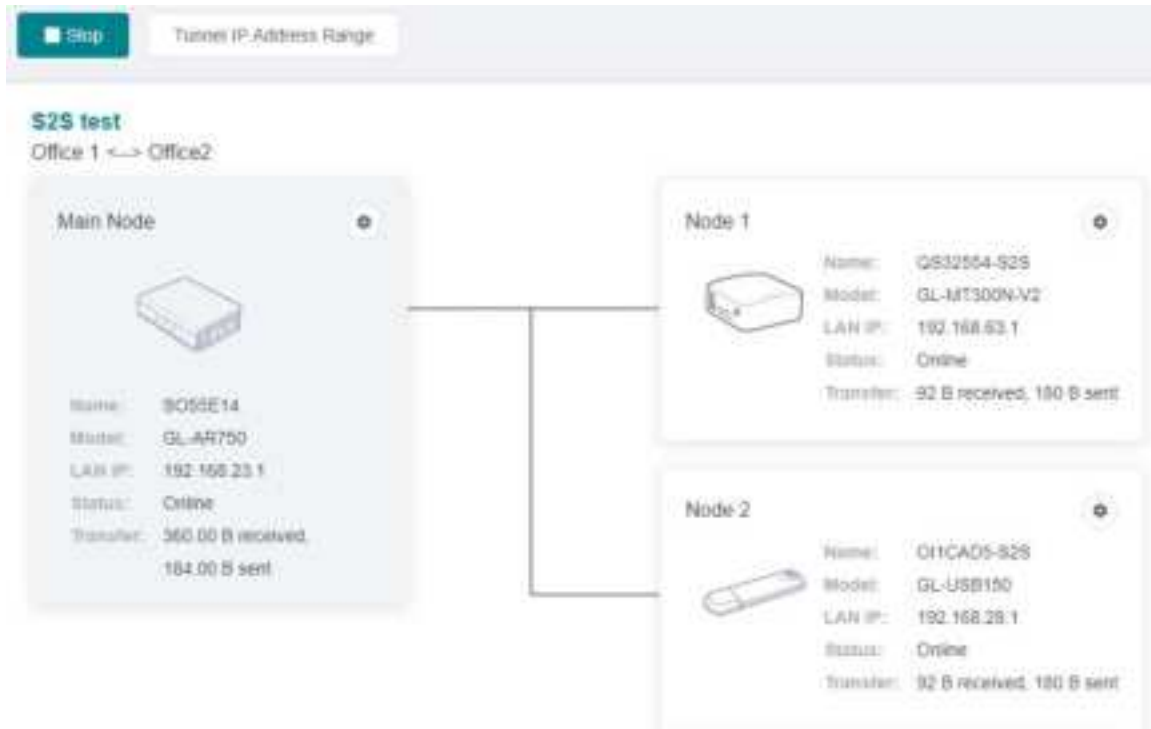
Continue

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

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



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



Testing the Site to Site connection

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

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

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

Route and other options

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

Configure LAN IP and Access Control



LAN IP

172.30.97.1

Allow be Access for the Following Subnets ⓘ

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

eg: 192.168.1.0/24

Add

Cancel

Confirm

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

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

Configure LAN IP and Access Control

LAN IP

172.30.97.1

Allow be Access for the Following Subnets ⓘ

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

eg: 192.168.1.0/24

Add

Cancel

Confirm

You can add node's parent routes too.

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

Tunnel IP Address Range



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

Simple

Advanced

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

Apply change will cause network go down a few minutes.

Cancel

Save

Save & Apply

Batch Setting

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

PS: This feature is only available to business users.

Batch Setting of Single Device

To configure single device, as show below.



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



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

Configure batch modification

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

Choose Template

ALL

WIRELESS

2.4G Wireless

5G Wireless

Guest 2.4G

Guest 5G

UPGRADE

MORE SETTINGS

Admin Password

LAN IP

Time Zone

2.4G Wireless

ON / OFF

ON OFF

1

Wi-Fi Name (SSID)

2

test

Wi-Fi Security

Select

Required

Wi-Fi Key

SSID Visibility

Select

Restart now

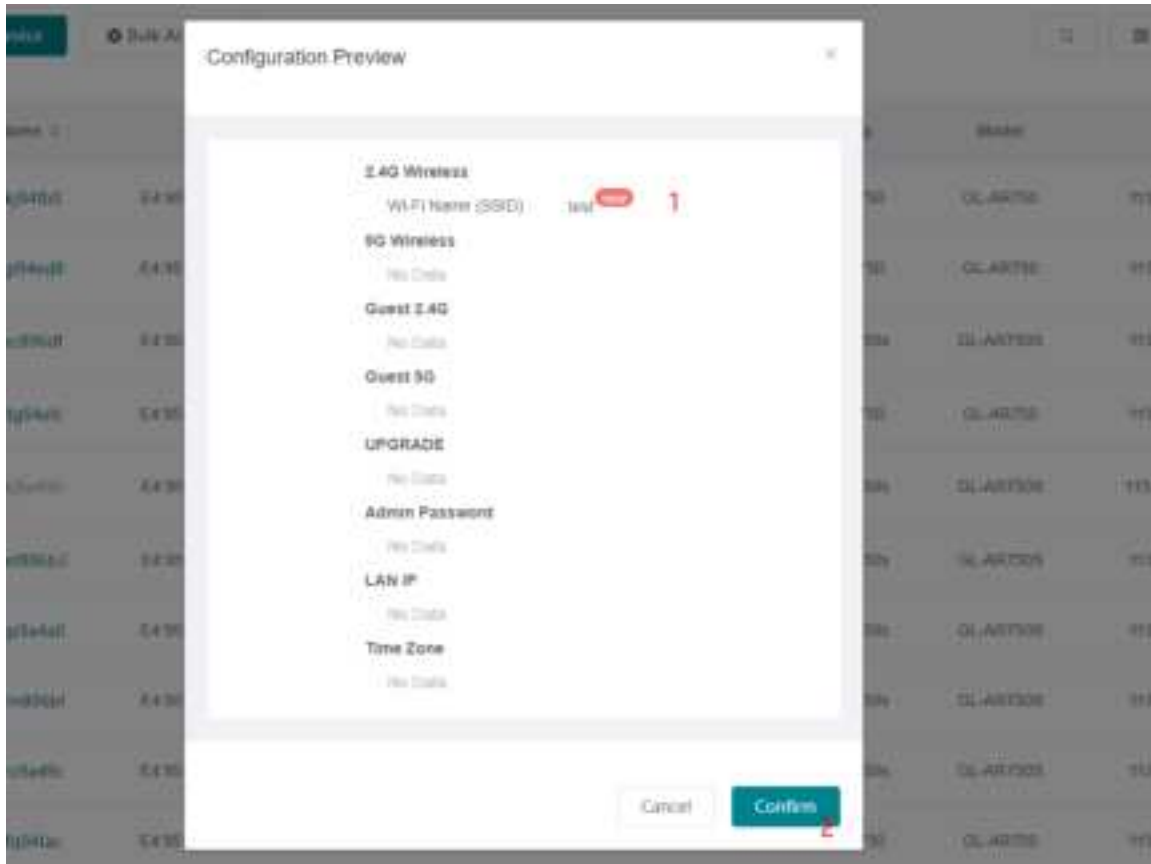
Cancel Reset Apply

3

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

above figure. After the configuration is completed, the device will restart immediately.

Preview the configuration and confirm the delivery.

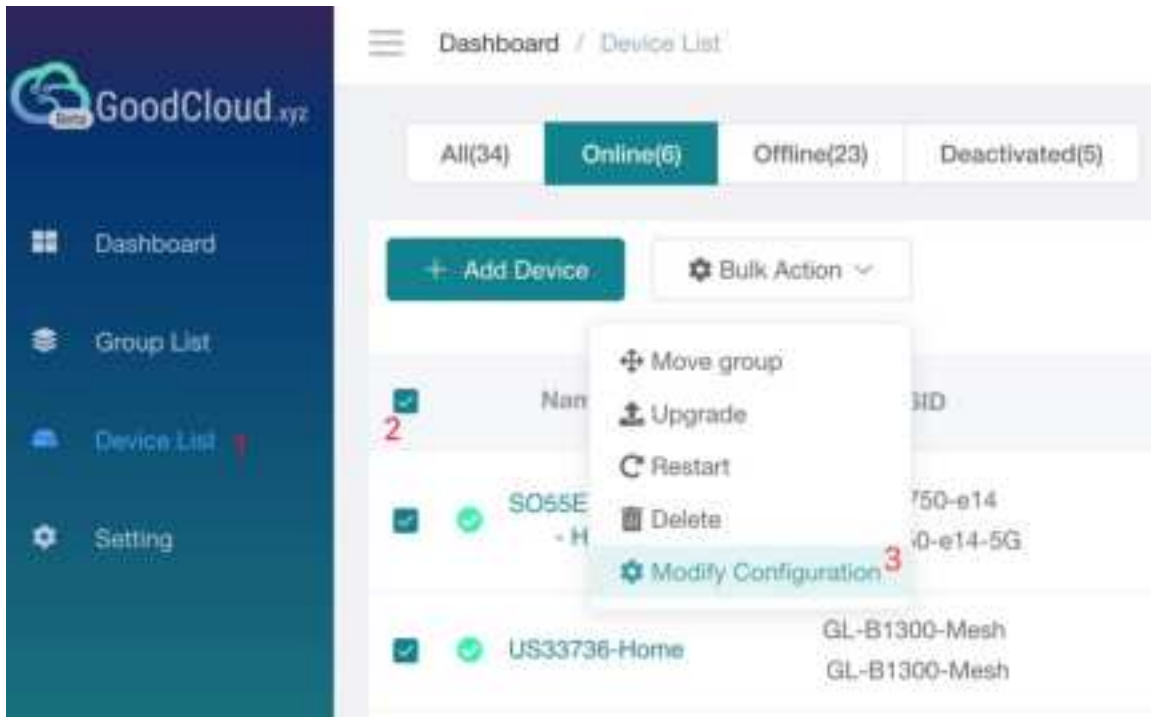


Unchecked **Restart now** option will prompt.



Batch Setting of Mutiple Device

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.



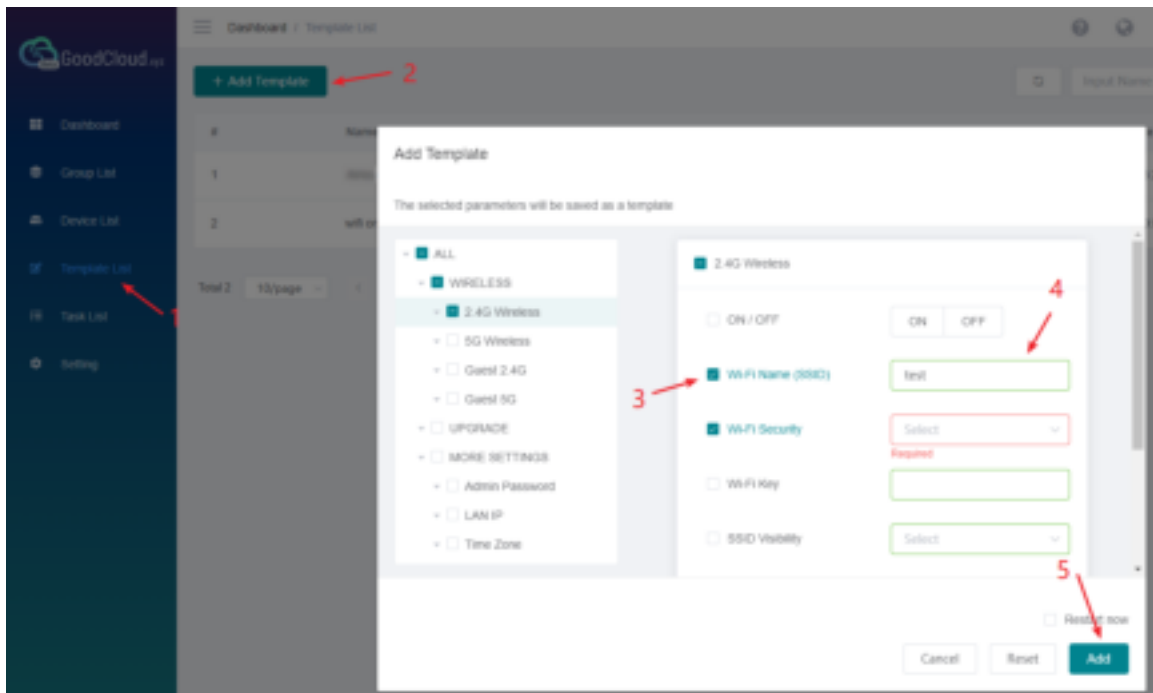
Template Management

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

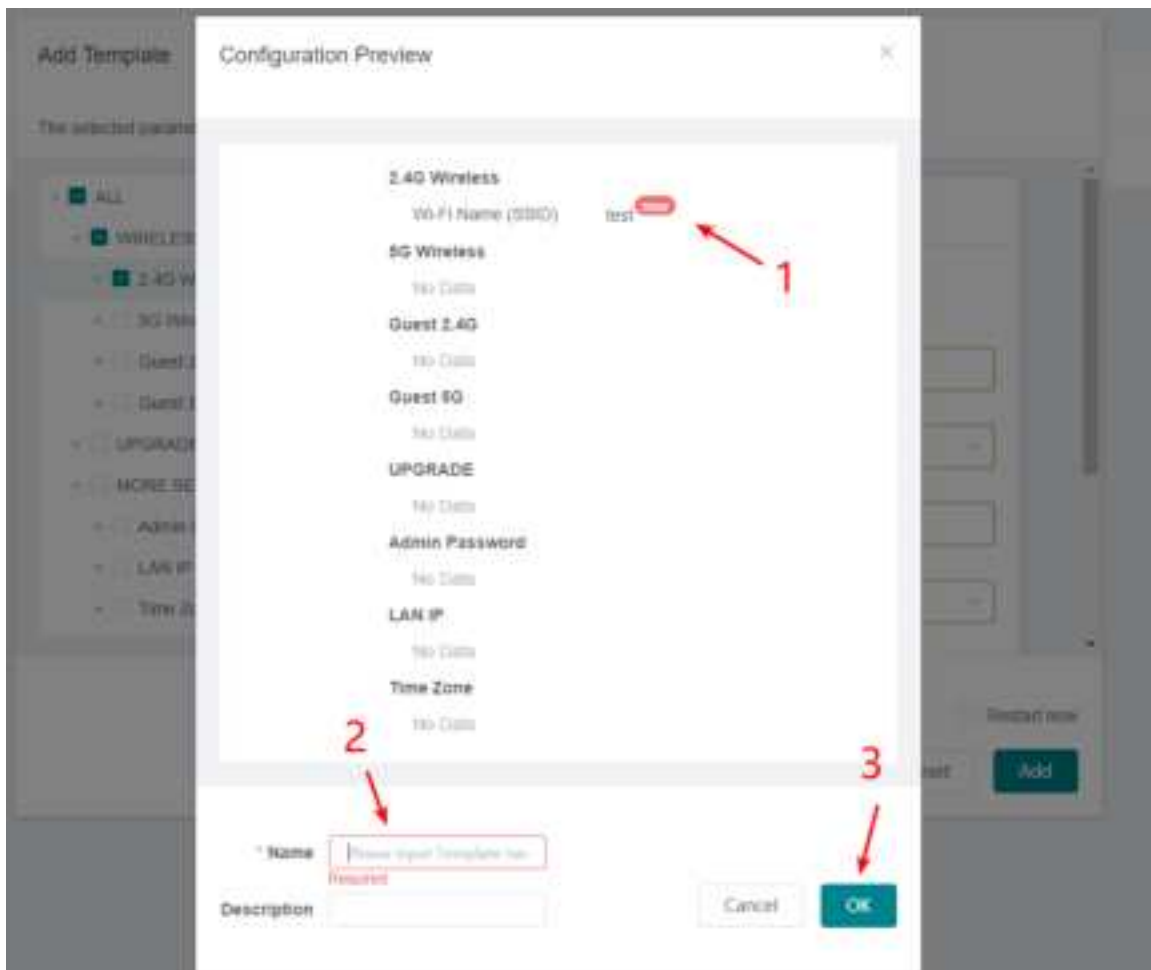
PS: This feature is only available to business users.

Add a Template

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



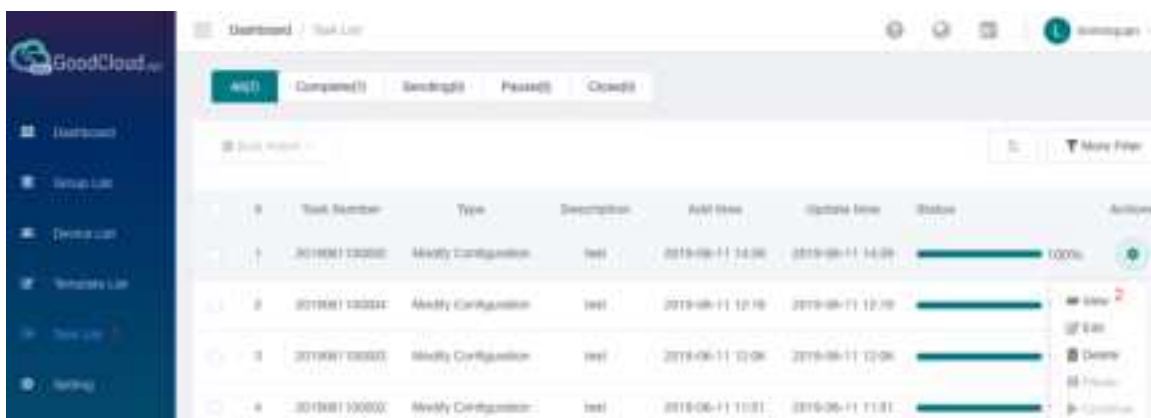
Give the template a name and description.



Task List

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

PS: This feature is only available to business users.



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

Total Devices 2 Success 2 Failure 0

#	Name	Model	MAC	Status
1	PT3F4C6	GL-MiFi	E4:95:6E: 00:00:00	Success
2	ea140ff	GL-MiFi	E4:95:6E: 00:00:00	Success

View ConfigOK

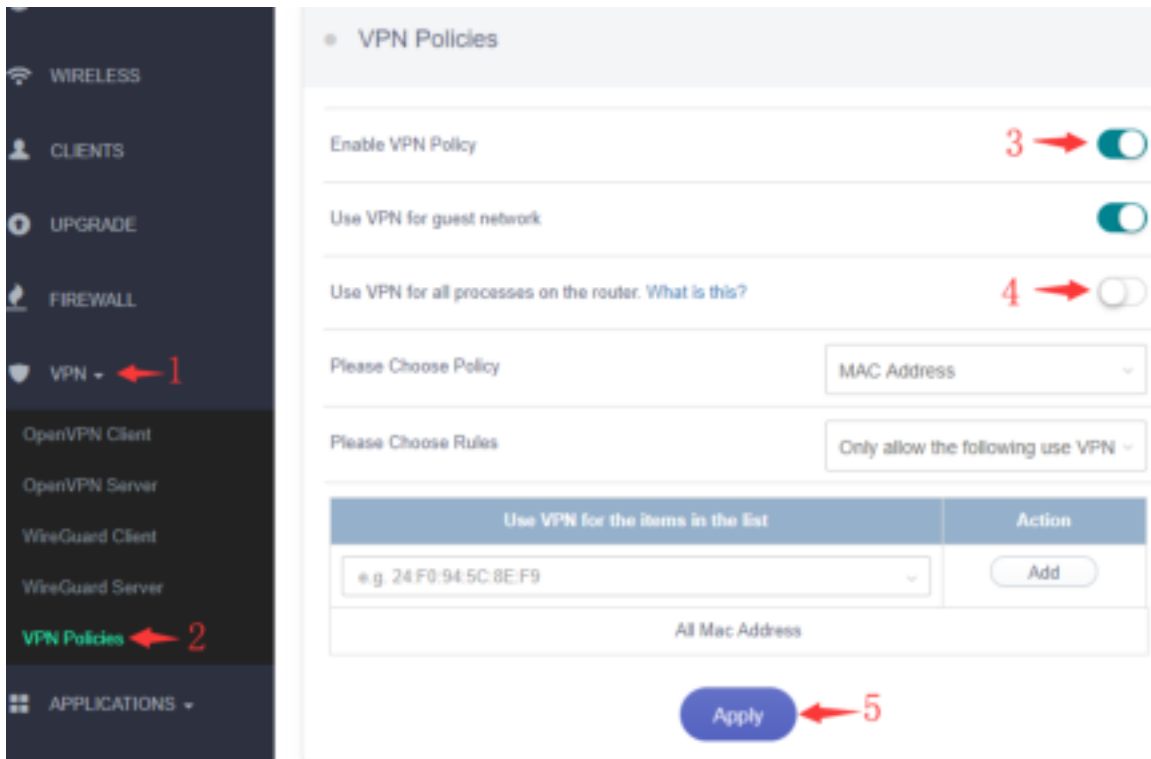
BLE MQTT Bridge

Bluetooth Low Energy (BLE) is widely used for smart home, wearable and IoT sensors. This feature is for GL.iNet BLE gateway, GL-X750 Spitz and GL-S1300 convexa S which has built-in BLE modules. [Read this](#) to learn how to use them forward your BLE data to the cloud based on MQTT protocol, including GL.iNet GoodCloud and AWS IoT.

GoodCloud and VPN

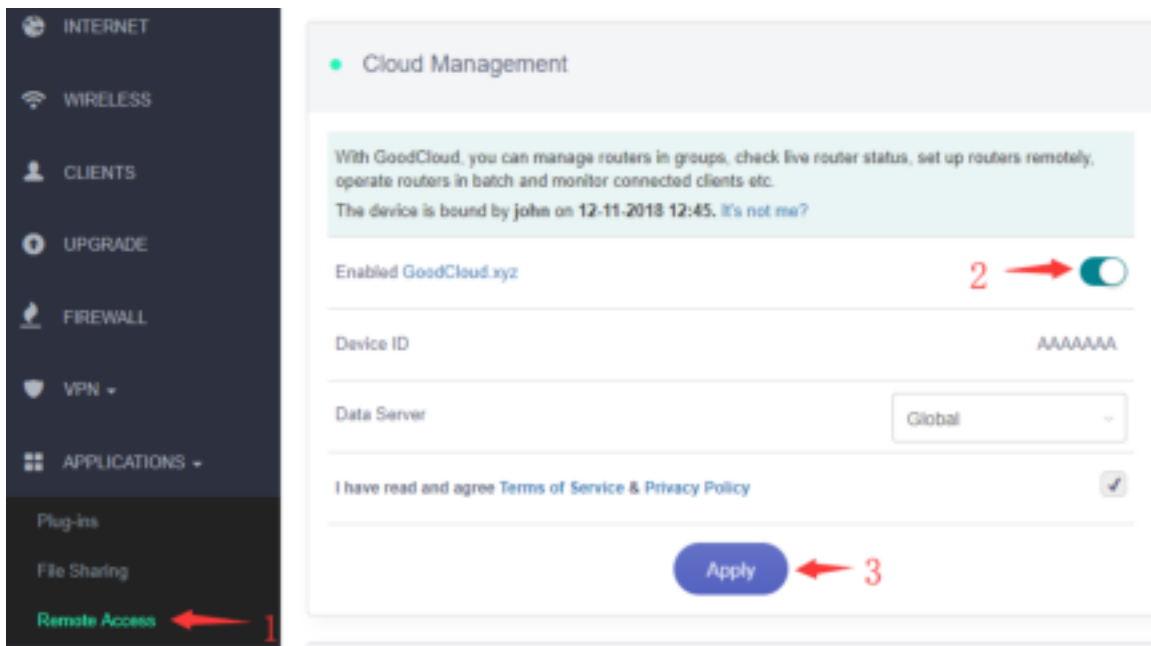
If you enable GoodCloud feature on router and also use it as VPN client, there is something important you need to know.

At default, GoodCloud process use VPN if you enable VPN client(eg. WireGuard, OpenVPN, Shadowsocks), this bring a problem that if you VPN is configured incorrectly, GoodCloud will not work properly. In order to ensure the normal use of GoodCloud, we suggest you to follow the steps below to enable VPN Policies and disable "Use VPN for all process on the router". After you've done these steps, GoodCloud precess will not use VPN.



Disable

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



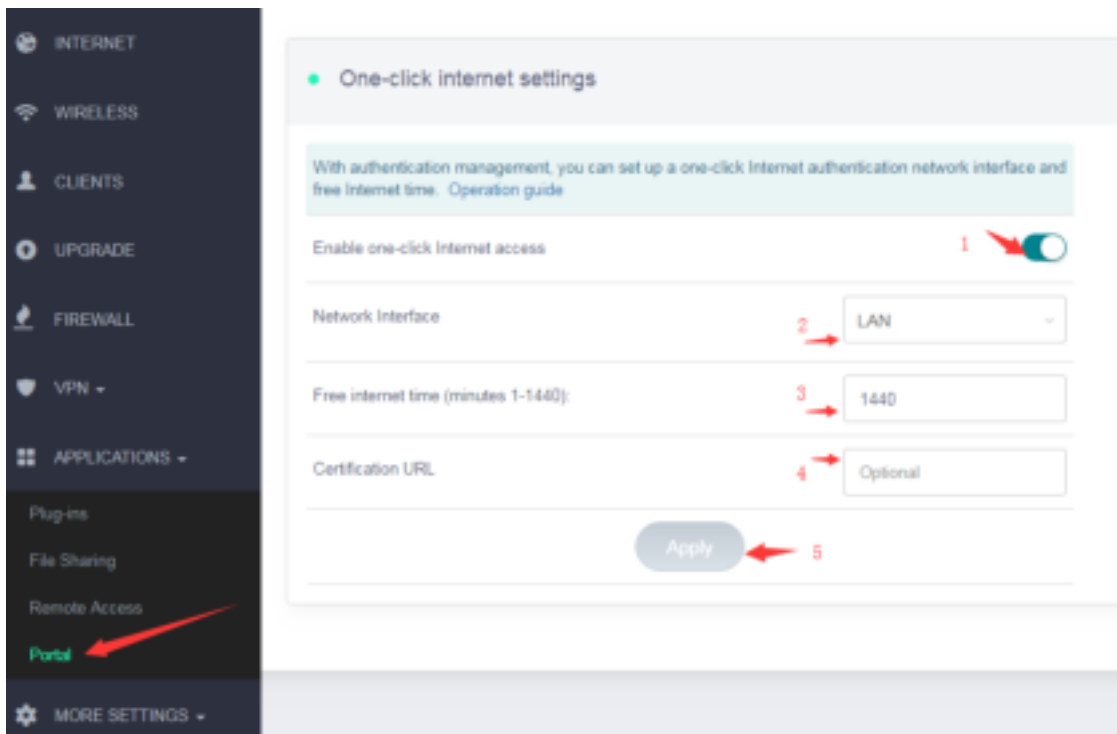


After disable Cloud, the interface is like above.

Turn on Captive Portal

Open a web browser (we recommend Chrome) and to access router Web Admin Panel(default url is <http://192.168.8.1>).

At the left sidebar, APPLICATIONS -> Portal, follow the steps below to enable Captive Portal.



- 1) Turn on one-click Internet access
- 2) Choose the network that you want to use Portal. LAN is for LAN clients, include wired clients. Guest is for Guest clients which access by Guest Wi-Fi.
- 3) Set free internet time.
- 4) Certification URL is the default page that clients will force redirect to when they are connected, e.g. <https://www.gl-inet.com>
- 5) Apply the configuration.

For wired desktop client, please use browser to access a http(not https) website, e.g. <http://neverssl.com> or <http://apple.com/?> , then you will see the portal.

Below is the Portal on iPhone, click the "GET CONNECTED" button to access the internet. On Android and desktop platform, it's a similar interface.



Change the default page

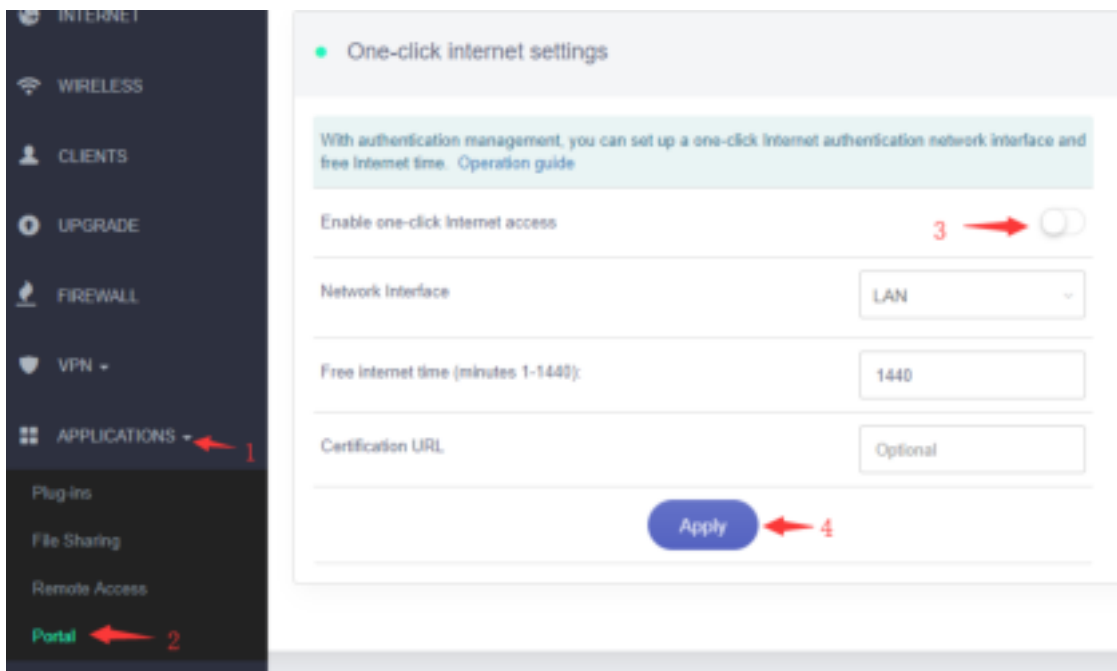
The default page is located `/etc/nodogsplash/htdocs/`, use SSH or WinSCP to change this page. For more information about how to use SSH and WinSCP, please access this. You may need basic HTML and CSS knowledge to change this page, please learn these from w3school or other sites.

If you want to change the picture on the default page, just replace the image on `/etc/nodogsplash/htdocs/portal_login.png`.

After you had change the page, it need to disable Portal and enable Portal again to enable the modified default page.

Disable Captive Portal

Follow the steps below to disable Captive Portal.



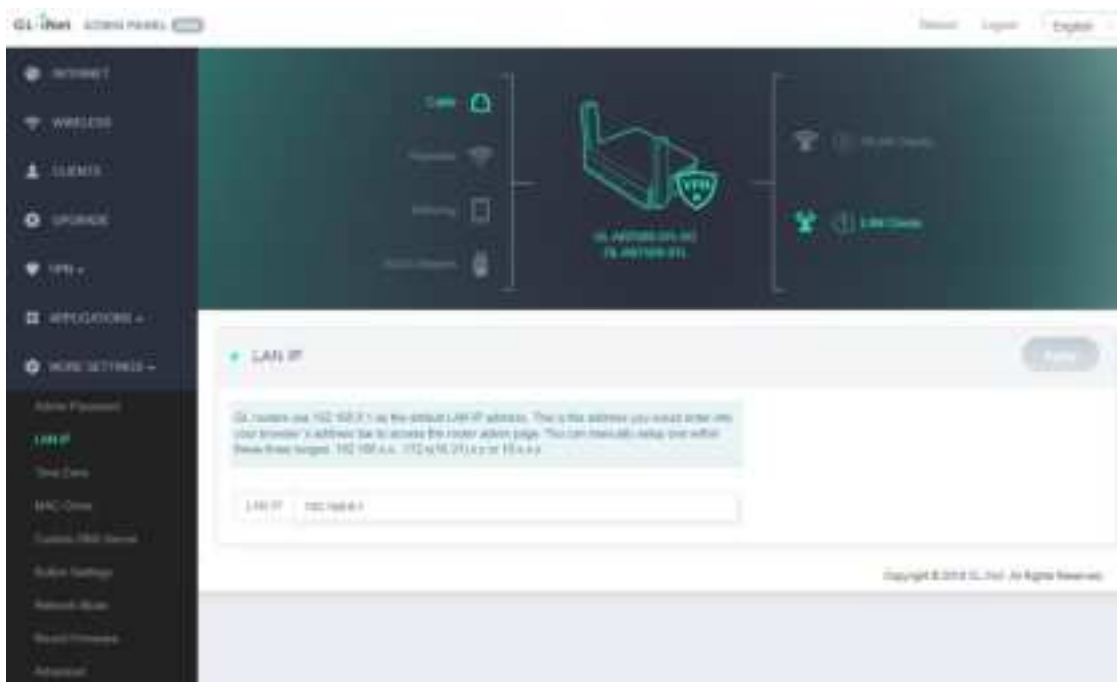
9. MORE SETTINGS

9.1. Admin Password

Change the password of the web Admin Panel, which must be at least 5 characters long. You have to input your current password in order to change it.

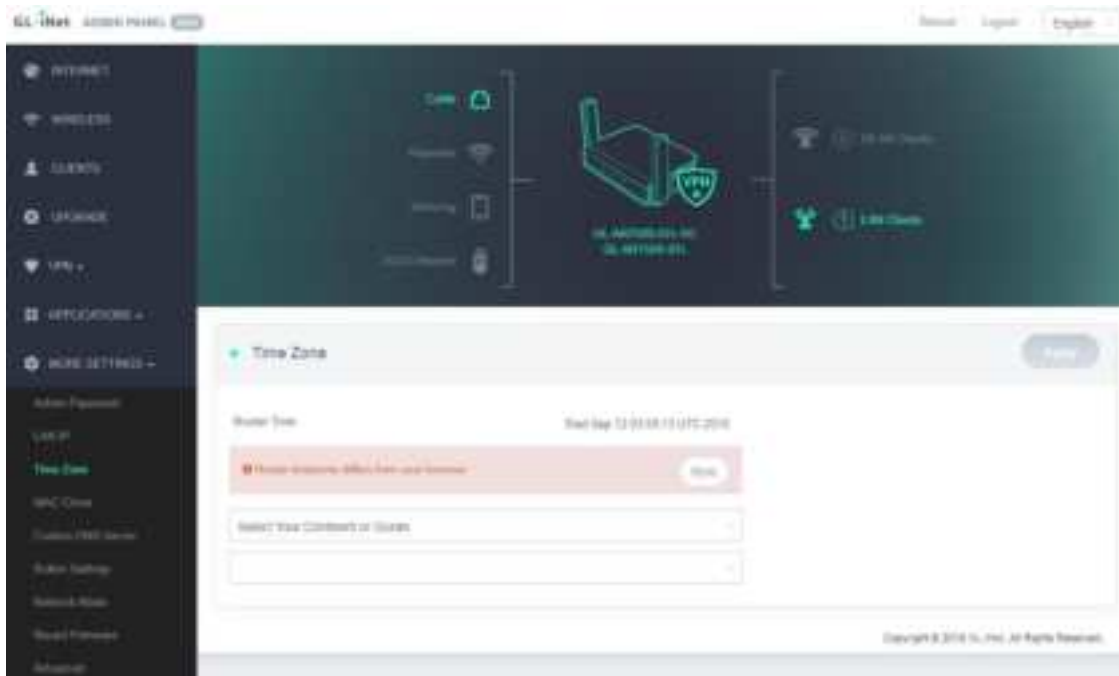
9.2. LAN IP

LAN IP is the IP address that you use to connect to this router. The default IP address of GL.iNet router is 192.168.8.1. If it conflicts with the IP address of your main router, you can change it.



9.3. Time Zone

The time of the router's activities will be recorded according to the router time. Therefore, choosing the time zone of your location is recommended.



9.4. MAC Clone

Clone the MAC address of your current client to the router. It is used especially in hotel when the network checks your MAC address. For example, if you got your smartphone registered on the network, you can clone the MAC address of your smartphone to the router so that the router can also connect to the network.



9.5. Custom DNS Server

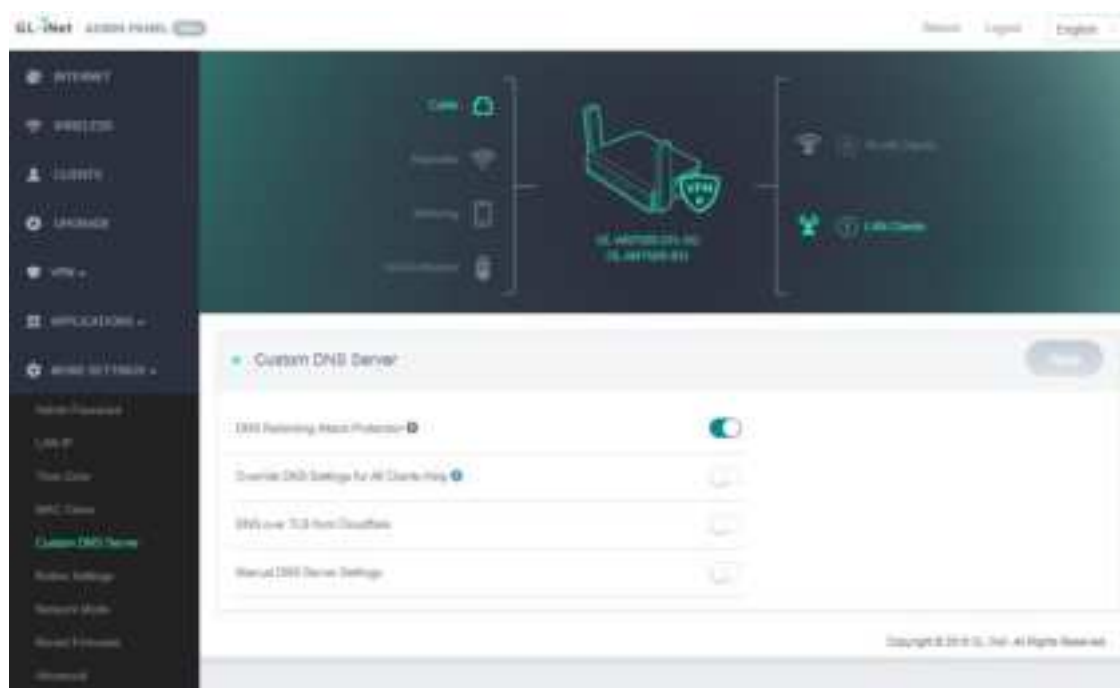
You can configure the DNS server of the router in order to prevent DNS leak or other purposes.

DNS Rebinding Attack Protection: Some network may require authentication in captive portal. Disable this option if the captive portal of your network cannot be resolved.

Override DNS Settings for All Clients: Enabling this option will capture DNS request from all connected clients.

DNS over TLS from Cloudflare: Cloudflare DNS over TLS uses the TLS security protocol for encrypting DNS queries, which helps increase privacy and prevent eavesdropping.

Manual DNS Server Settings: Input a custom DNS server manually.



9.6. Button Settings

Configure the function of the mode switch. It doesn't have any function by default. You can set it as a toggle to turn on or off Wireguard/OpenVPN client.



9.7. Network Mode

Change the network mode to cater your usage scenario. You may need to reconnect your client device whenever you change the network mode of the router.

Be aware that you may not be able to access the web Admin Panel with the default IP 192.168.8.1 if you use the router in **Access Point**, **Extender** or **WDS** mode. If you want to access the web Admin Panel in this case, you have to use the IP address assigned by the main router to the GL.iNet router.

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

Access Point: Connect to a wired network and broadcast a wireless network.

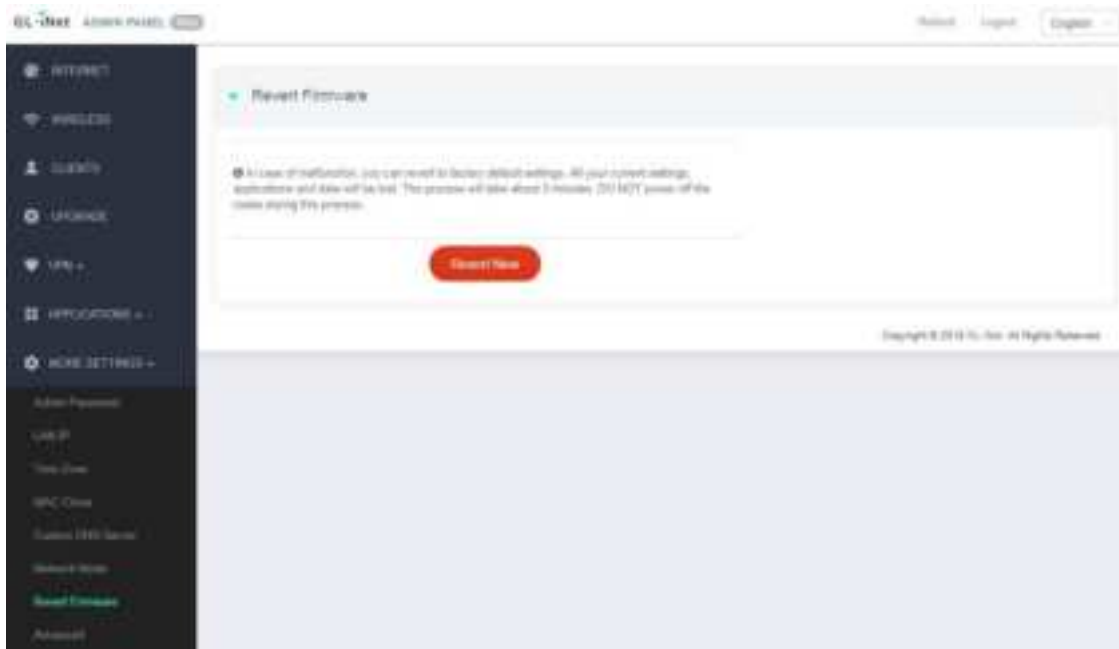
Extender: Extend the Wi-Fi coverage of an existing wireless network.

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



9.8. Revert Firmware

Revert the router to factory default settings. All your settings, applications and data will be erased.



9.9. Advanced

Click Advanced to direct to Luci which is the default web interface of OpenWrt. You can check the detailed system log or conduct more advanced configurations there.



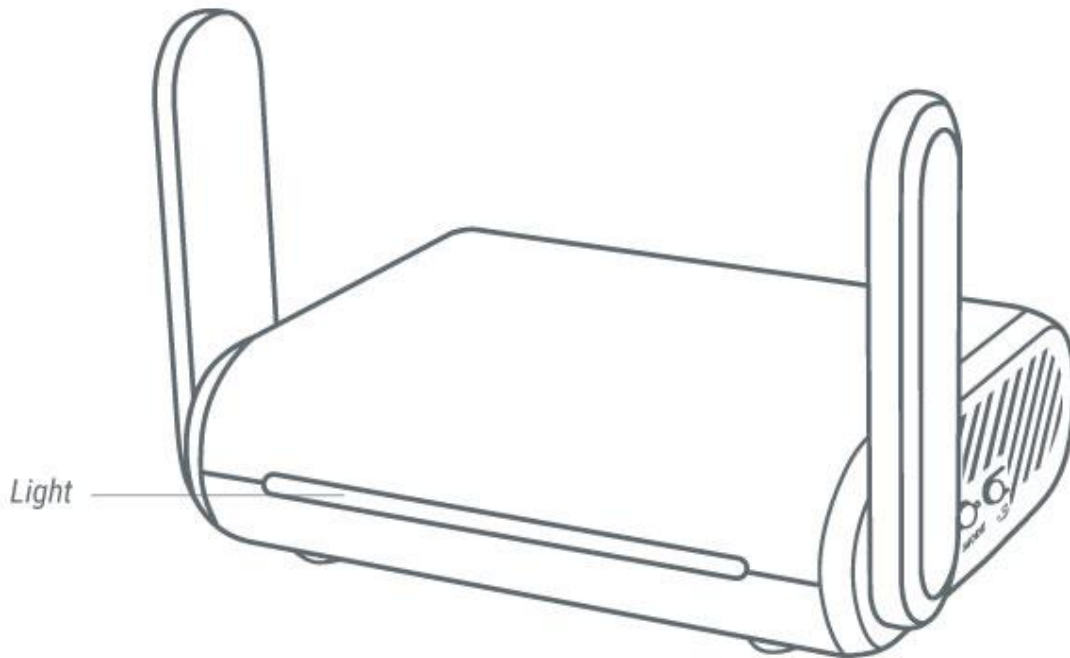
*Note: The username is **root**. The password is same as the one that you use to access the web Admin Panel.*

10.Troubleshooting

10.1 LED Indicators

LED Status Indication

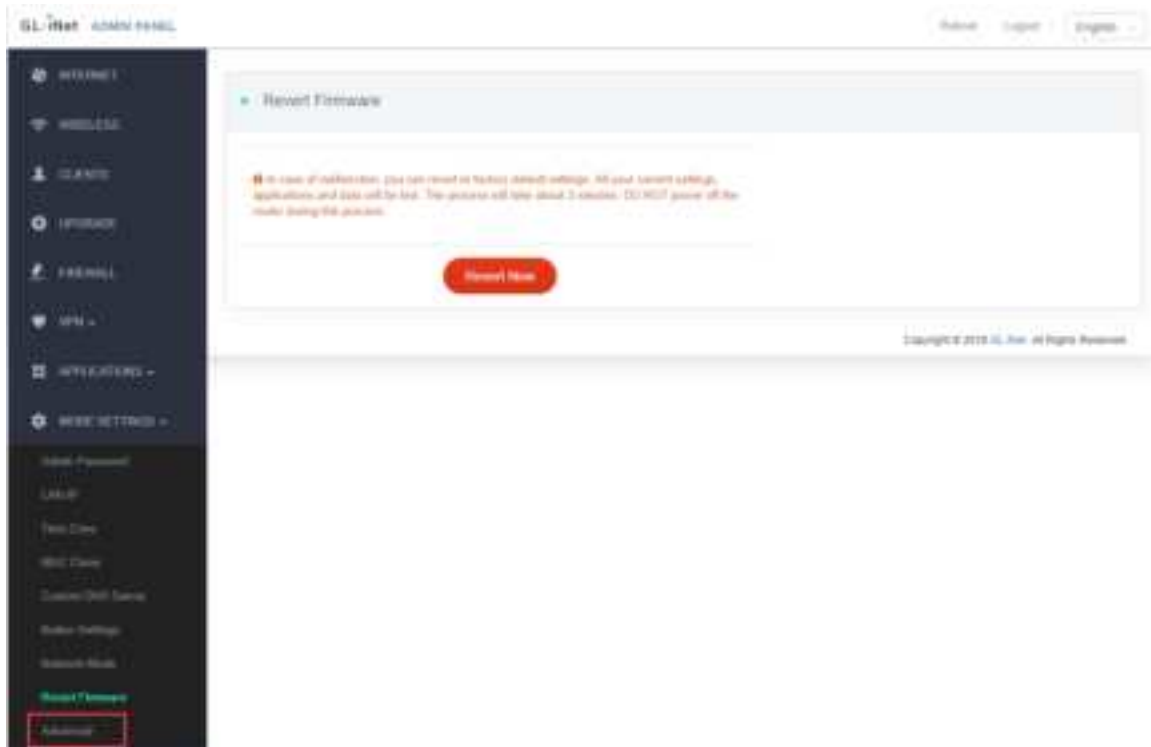
GL-MT1300/ SFT1200



- **Solid blue light:** Device is powering up.
- **Solid white light:** Network is connected.
- **Slowly growing blue light:** Network disconnects/ No cable connection.
- **Fast flashing blue light:** In reset process.
- **Slowly flashing blue light:** Upgrading firmware in process.

LED Customization

To configure the LED of GL.iNet routers, please login to Luci by clicking **Advanced settings** at the bottom-left corner of the web admin page.



Then please choose **System > LED Configuration**.

10.2 Repair or Reset

How to Repair / Reset

All GL.iNet Routers have reset buttons, you can use them to repair your network or reset your routers to factory default. If you can neither access the web-based setup page nor the router, you can press the `reset` button: Repair

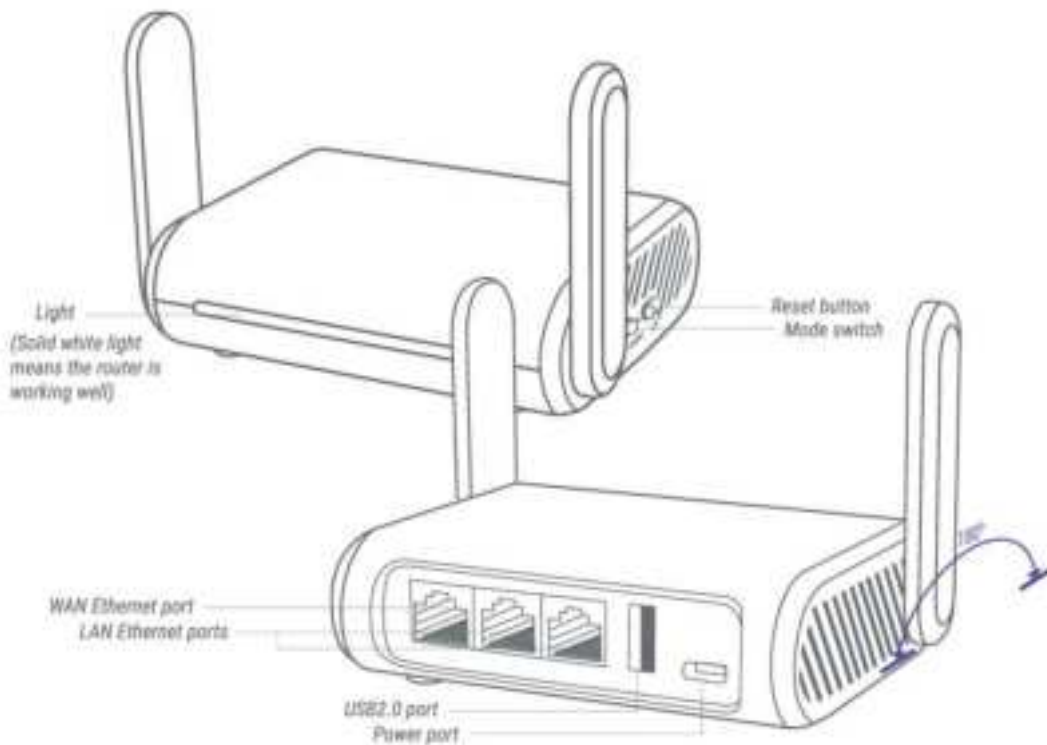
Press and hold for **4 seconds** then release to repair your network.

Reset

Press and hold for **10 seconds** then release to reset the router to factory settings. All user data will be cleared.

Reset Button

GL-SFT1200 Travel AC Router



10.3 Debrick via Uboot

Using Uboot to Debrick Your Router

You may have bricked your router if you were doing some DIY projects or flashed a wrong firmware. You may not be able to access your router but you can re-install the firmware by using Uboot failsafe.

Please follow the procedures below to access the Uboot Web UI and re-install the firmware.

You can also refer to our video, [How to Recover GL.iNet Mini Router by U-Boot FailSafe](#).

1. First you have to download **firmware** to your computer. You can download the firmware [here](#). For GL-AR300M, GL-AR300M-Ext, GL-AR750S-Ext, GL-E750, GL-X1200, please download the .img firmware file. For GL-B1300, GL-S1300, please download the .img firmware. Everyone else, download the .bin firmware file.
2. Connect your computer to the **Ethernet port (either LAN or WAN)** of the router. You **MUST** leave the other port **unconnected**.
3. Press and hold the Reset button firmly first, and then power on your device. (If your device does not have a power button, plugging it in will power it on automatically.)

If you can not find the reset button, please refer to our page, [How to Repair and Reset](#).

Release your finger when you see the LED has flashed:

4. The Power LED will light up. Then, other LEDs will start flashing.
 - **6 times** for GL-MiFi, and then the LTE light will faintly flash twice.
 - **5 times** for GL-AR150, GL-AR300M, GL-USB150, GL-AR750, GL-AR750S-Ext (Slate), GL-X750-Ext (Spitz), GL-MT300N-V2, GL-E750 (Mudi).
 - **4 times** for GL-S1300, GL-B1300.

The leftmost LED may stay on the whole time while the rightmost LED flashes 4 times, then the middle LED turns on and stays on.

(For some old GL-B1300, the leftmost LED stays on the whole time, and both the middle LED and the rightmost LED flash 5 times at the same time then they stay on.)

- **3 times** for GL-MT300N, GL-MT300A.

- **For GL-MT1300**, the LED is blue at first, flash twice slowly, then light 5 times a bit quick and turn to white and stay on.
- **For GL-SFT1200(Opal)**, the blue LED flashes 5 times then turns white and stay on.
- **For GL-B2200**, the two LEDs are blue at first, then turn white to flash 5 times, then turn blue and stay on.
- **No repeat LED flashes signal** for GL-MV1000.

(Power and WAN LEDs will stay on the whole time.)

5. Set your computer's IP address to **192.168.1.2**. Please check the step-by-step guide for different operating systems below:

Windows 7 / Windows 10

- a. Go to Control Panel -> Network and Internet -> Network and Sharing Center -> Change adapter settings.
- b. Right click Local Area Connection -> Properties.
- c. Click Internet Protocol Version 4 (TCP/IPv4) -> Properties.
- d. Set the IP address to 192.168.1.2 manually.



Set computer's IP address
to 192.168.1.2

Mac

- a. Go to System Preferences -> Network.
- b. Choose Ethernet -> Advanced -> TCP/IP.
- c. In Configure IPv4, choose Manually.
- d. Set the IPv4 Address to 192.168.1.2 manually.

6. Use Firefox or Chrome to visit <http://192.168.1.1>.



7. Click **Choose File** to find the firmware file. Then click **Update firmware**.
For GL-AR300M, GL-AR300M-Ext, GL-AR750S-Ext, please download the .img firmware file and upload to the NAND

flash.

The image shows a web interface for a 'FIRMWARE UPDATE'. At the top, the title 'FIRMWARE UPDATE' is in large blue letters. Below it, a message states: 'You are going to update firmware on the device. Please, choose file from your local hard drive and click Update firmware button.' There are two sections for file selection. The first is for 'NAND flash firmware (*.img)', with a 'Choose File' button, a 'No file chosen' status, and an 'Update nand firmware' button. The second is for 'NOR flash firmware (*.bin)', with a 'Choose File' button, a 'No file chosen' status, and an 'Update nor: firmware' button. A yellow 'WARNINGS' box contains three bullet points: 'do not power off the device during update', 'if everything goes well, the device will restart', and 'you can upload whatever you want, so be sure that you choose proper firmware image for your device'. At the bottom, a link says 'You can find more information about this project on: [Github](#)'.

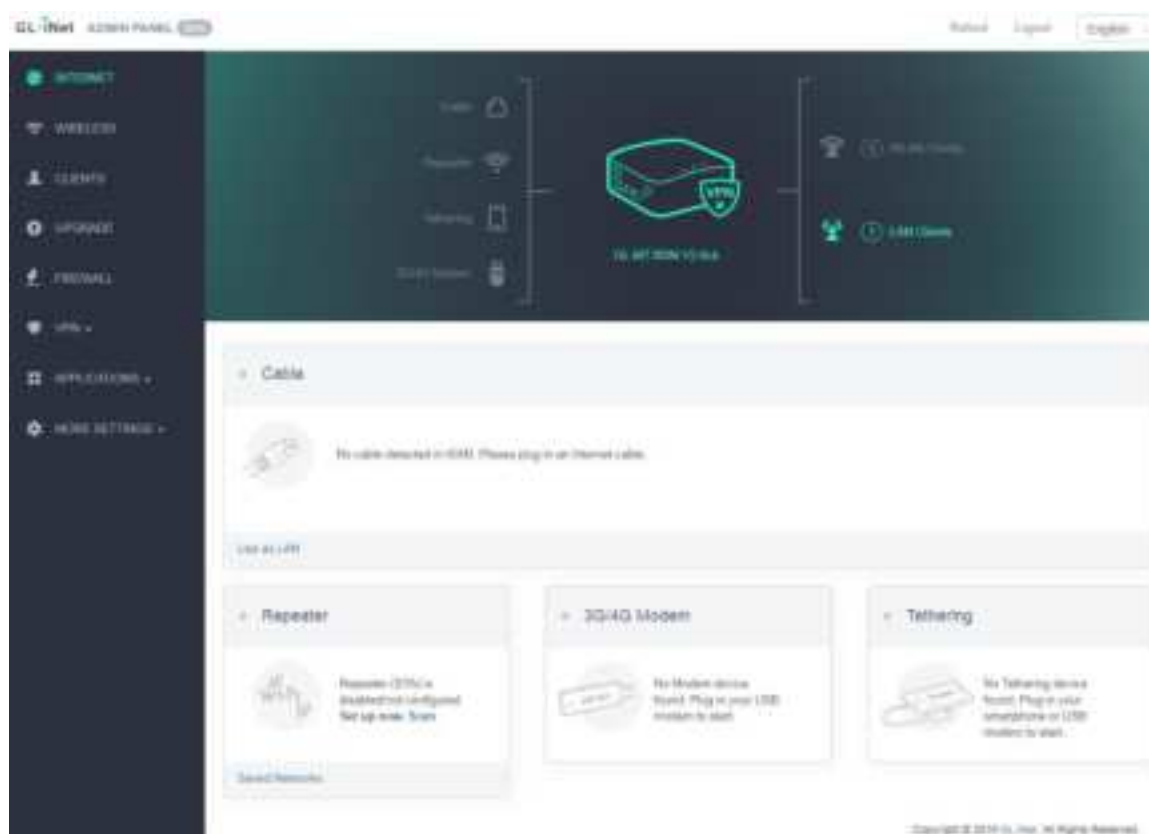
8. Wait for around 3 minutes. Don't power off your device when updating. The router is ready when both power and Wi-Fi LED are on or you can find its SSID on your device.
9. Revert the IP setting you did in step 6 and connect your device to the LAN or Wi-Fi of the router. You will be able to access the router via 192.168.8.1 again.

10.4 Change WAN to LAN

You can configure the WAN port of the router so that it can be used as a LAN port. That's useful when you are using the router in repeater mode which the WAN port is not required. As a result, you can have one more LAN port.

Especially for **GL-AR300M-Lite**, it only has one Ethernet port which works as WAN by default. Therefore, you must connect to it via Wi-Fi. However, once you have connected to it, you can change its WAN port to LAN so that you can connect to it via an Ethernet cable.

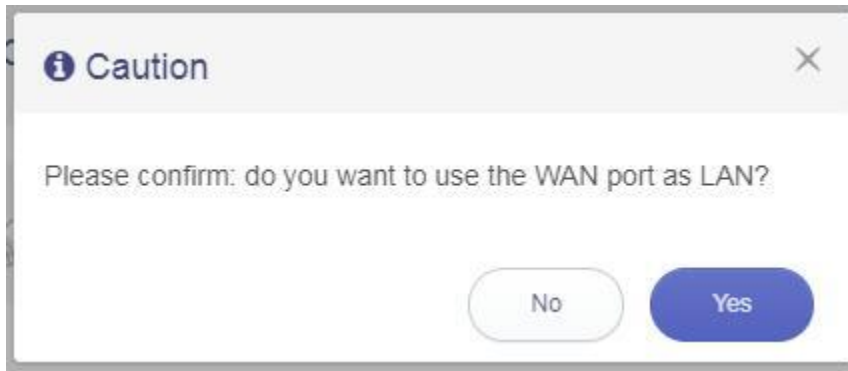
1. Leave the WAN port of the router unconnected.
2. Connect your device to the router and access the web Admin Panel.



3. Go to **Internet**, click **Use as LAN** under the Cable section.



4. Click **Yes** to confirm.



You can simply revert the setting by repeating the above procedures. This time, it will show **Use as WAN** in step 3.



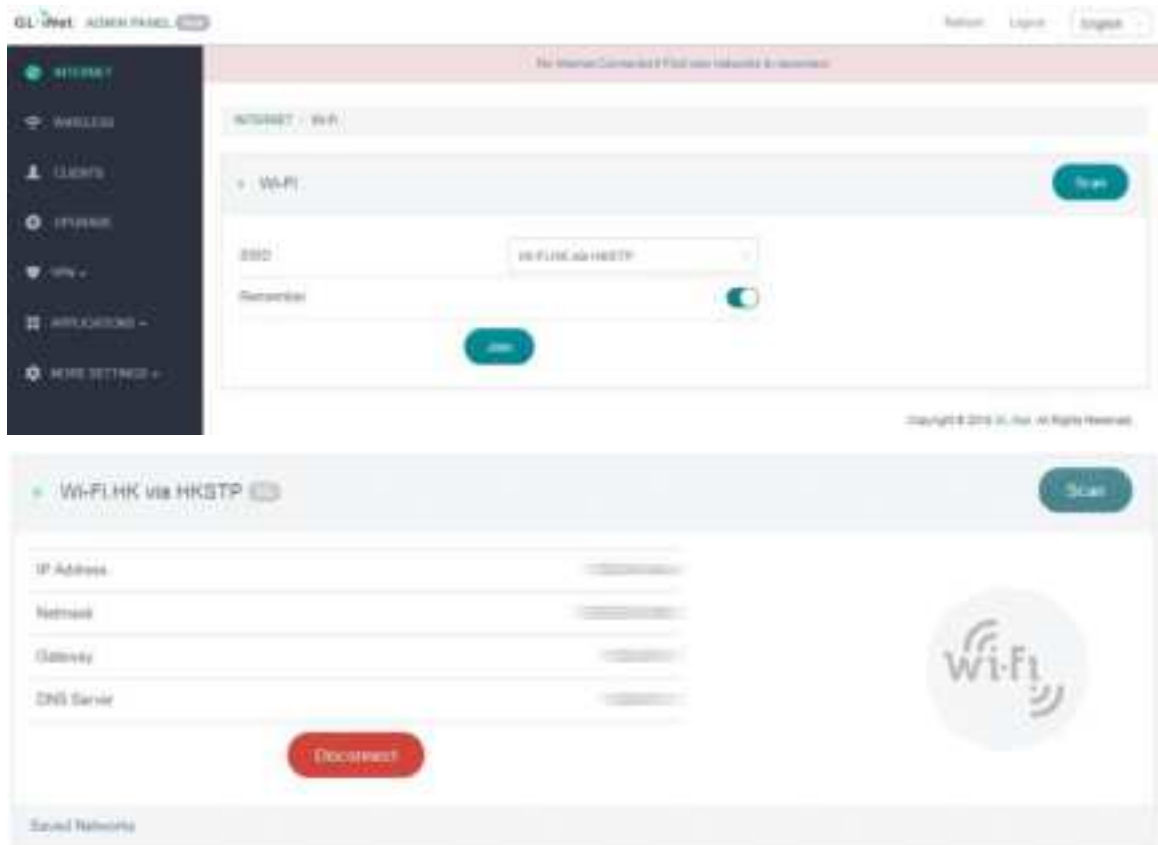
10.5 Captive Portal

Connect to a Hotspot with Captive Portal

Some public hotspots especially those in hotel, cafe or airport, require you to input your authentication information or agree the terms and conditions through a web page (**Captive Portal**) before you can connect to it or access the Internet.

However, you may find that you are not able to enter the captive portal so that you cannot connect to the hotspot or access the Internet. In this case, please follow the following procedures to disable the **DNS rebind protection**.

-
1. Connect to the public hotspot which requires authentication through captive portal.



2. Go to Admin Panel -> MORE SETTINGS -> Custom DNS Server. Then, disable **DNS Rebinding Attack Protection**.



3. Use your web browser to visit a webpage, it will be redirected to the captive portal of the hotspot automatically.

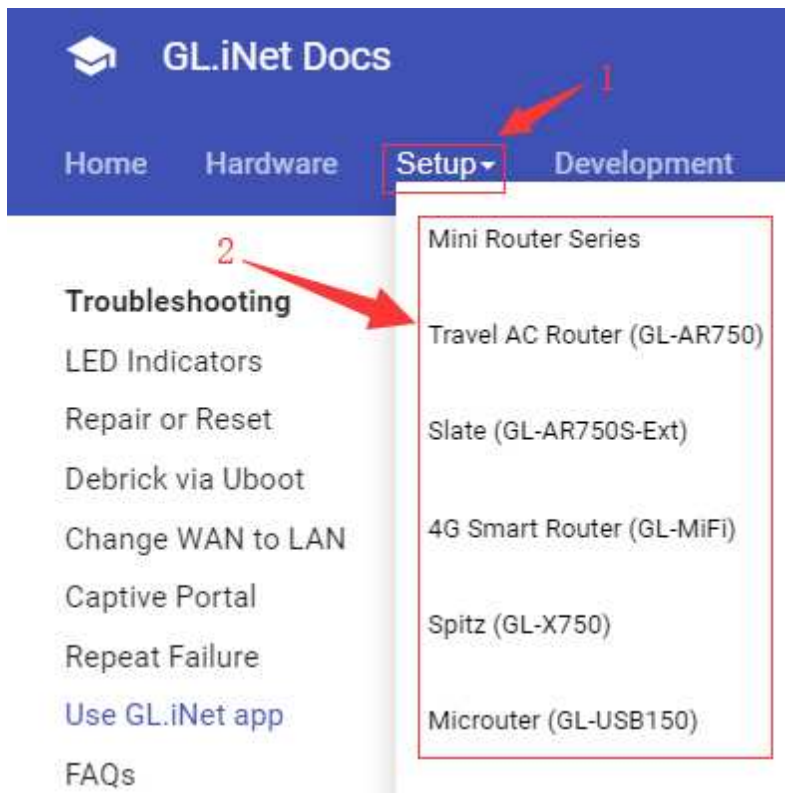
If you are using smartphone but your web browser doesn't redirect to the captive portal. Please turn off the Wi-Fi of your smartphone and then turn it on and reconnect to the Wi-Fi of your router again. The captive portal should be popped up directly after you entered the Wi-Fi password.



10.6 GL.iNet app

GL.iNet app requires router firmware version 3.100 and above. Please upgrade.

Click the Setup menu, choose your model.



Then click the Upgrade on the left side.

First-time Setup
Internet
Wireless
Clients
[Upgrade](#)
Firewall
VPN
Applications
More Settings

Some models don't have V3.100 release firmware yet, please try testing(pre-release) firmware. Please find the download info at [Firmware Release](#) page.

10.7 Access Web Panel

Sometimes you may be unable to access 192.168.8.1 to login web admin panel, please follow the guide below to solve this problem.

Check connection/router's IP address

Make sure your WAN/LAN port connection is correct. WAN port is connected to an internet source and LAN port is connected to devices. If connected by wifi, make sure the SSID is correct.

Then follow the steps below to check the router's IP address.

Windows 7 / Windows 10

Your ip address results determine the next step.

Your IP address is incorrect

If the IP address is incorrect, check your connection again.

1. Try [Reset](#) to back to factory default.
 2. If the reset doesn't work, you can try [Debrick via uboot](#).
-

Your IP address is correct

1. Make sure you are using Chrome/Firefox, then try to access 192.168.8.1 again.
2. In order to avoid problems caused by the cache, click **ctrl+shift+n** in Chrome to enter the incognito mode. Then try to access 192.168.8.1 again.



10.8 Extensible Authentication Protocol (EAP)

Introduction

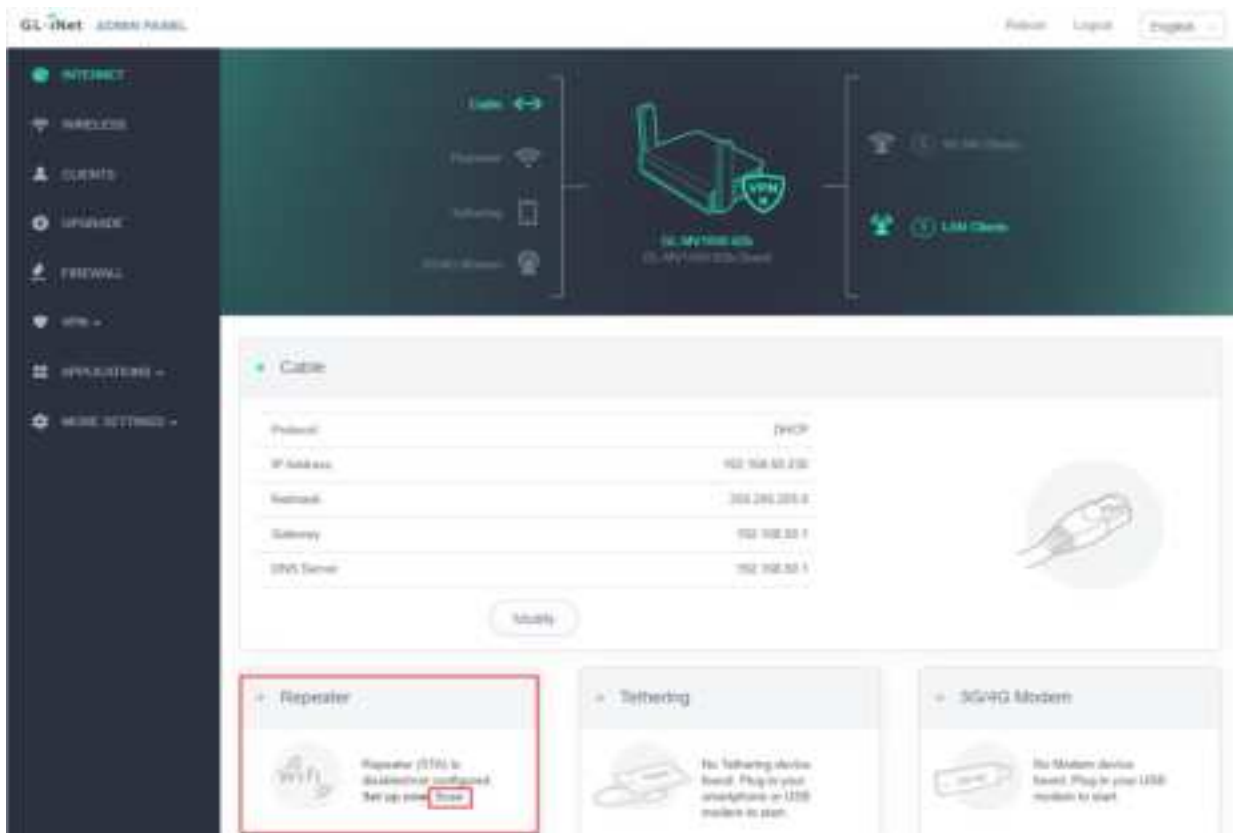
You can connect to EAP (Extensible Authentication Protocol) Wi-Fi network which requires username and password authentication on GL.iNet routers.

This guide is how to connect an EAP Wi-Fi network via GL admin panel.

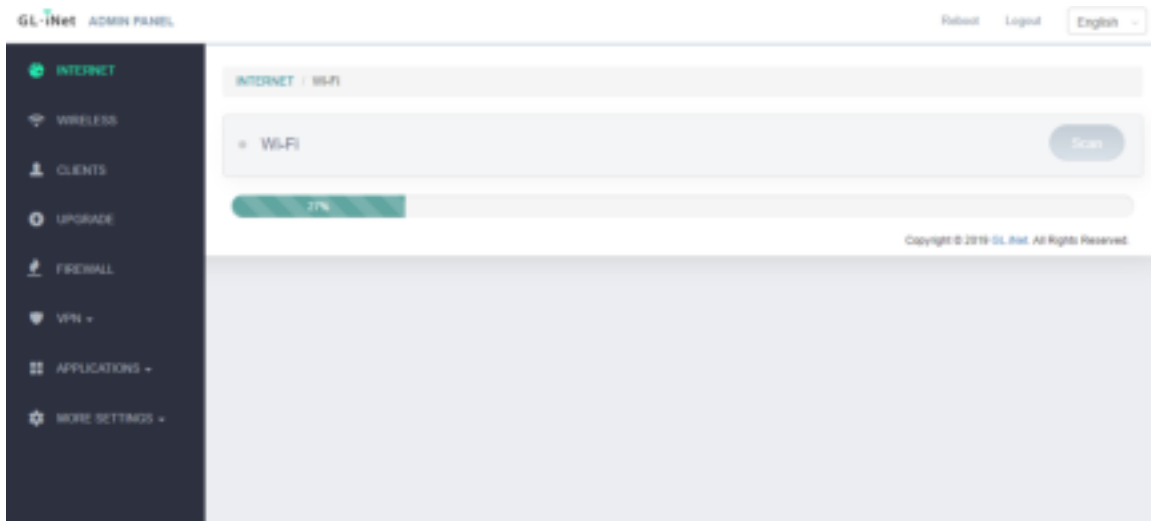
- Supported models: GL-AR300M Series, GL-USB150, GL-AR750, GL-AR750S, GL-B1300, GL-S1300, GL-AP1300, GL-E750, GL-X750, GL-MiFi, GL-XE300, GL-AX1800, GL-B2200, GL-X300B, GL-X1200, GL-AXT1800
 - Not supported models: GL-MT300N-V2, microuter-N300, GL-MT1300, GL-MV1000W, GL-MV1000, GL-SF1200, GL-SFT1200
-

Connect via web panel

1. Visit the Admin Panel



Visit the Admin Panel and click “Scan” in the Internet -> Repeater.



You can find and connect to the EAP SSID to connect directly.

2. SSID



Or choose “Other” in the drop-down list of SSID, then select EAP type in Wi-Fi Security drop-down list.

3. Wi-Fi Security



Currently, we only support two types: 802.1X EAP/WAP and 802.1X EAP/WAP2.

4. Type

The screenshot shows the 'Wi-Fi' configuration page. The 'Type' dropdown menu is open, showing options for '2.4G' and '5G'. The '2.4G' option is highlighted. The 'Join' button is visible at the bottom.

INTERNET Wi-Fi

Wi-Fi

SSID

Wi-Fi Security

Type

User Name

Password

Remember

Join

Copyright © 2019 GL.iNet. All Rights Reserved

Choose 2.4G or 5G.

5. User Name and Password

The screenshot shows the 'Wi-Fi' configuration page. The 'User Name' and 'Password' fields are highlighted. The 'Join' button is visible at the bottom.

INTERNET Wi-Fi

Wi-Fi

SSID

Wi-Fi Security

Type

User Name

Password

Remember

Join

Copyright © 2019 GL.iNet. All Rights Reserved

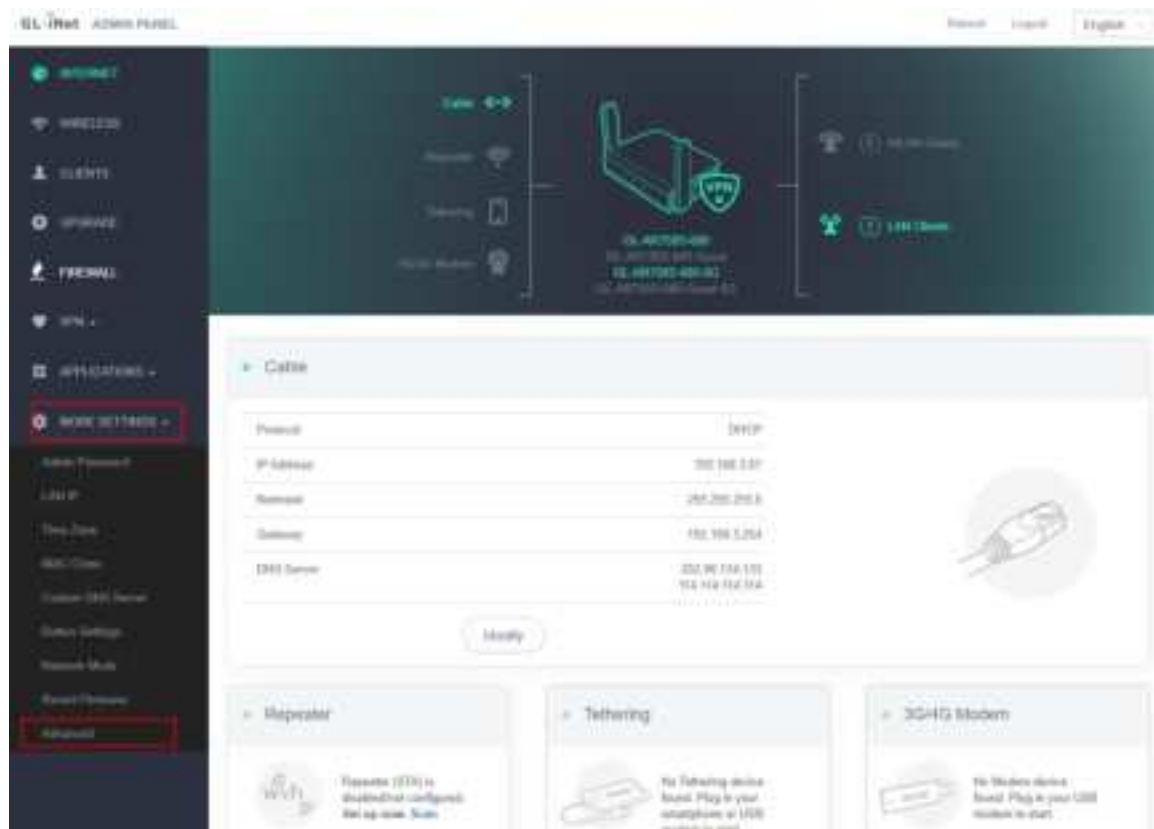
Enter your User Name and Password and then click join.

Connect via Luci

Our web page only supports few EAP types for now so you may need to connect via Luci page in most situations.

1. Visit the Luci page

Go to MORE SETTINGS->Advanced.



Input your web password.



Then you will enter luci page.

2. Connect to EAP wifi

Go to Network->Wifi(or Wireless).

The screenshot shows the GL-AR750S web interface. The top navigation bar includes 'Status', 'System', 'Network', and 'Logout'. The 'Status' page is active, displaying system information. A dropdown menu is open under the 'Network' tab, showing options: 'Status', 'Wireless', 'Switch', 'DHCP and DNS', 'Networks', 'Static Routes', 'Firewall', and 'Diagnosis'. The 'Wireless' option is highlighted. The system information table shows details like Hostname, Model, Architecture, Firmware Version, Kernel Version, Local Time, Uptime, and Load Average. The Memory section shows Total Available, Free, and Buffered memory usage. The Network section shows two IP4 interfaces: 'eth0' (Software VLAN) and 'eth1' (Software VLAN). The 'eth0' interface is connected to a DHCP client, showing IP address, netmask, gateway, and DNS servers. The 'eth1' interface is not connected.

System	
Hostname	
Model	
Architecture	QCA9558 ver 1 rev 0
Firmware Version	OpenWrt 18.06.1 r255-6a05c588 / LuCI openwrt-18.06 branch (gl-18.196.58135-9112198)
Kernel Version	4.8.123
Local Time	Thu Mar 18 13:02:58 2020
Uptime	3h 13m 29s
Load Average	0.22, 0.26, 0.23

Memory	
Total Available	80194 MB / 134048 MB (54%)
Free	80862 MB / 134048 MB (48%)
Buffered	8012 MB / 134048 MB (5%)

Network	
eth0 Software VLAN: 'veth0.7'	eth1 Software VLAN: 'veth1.7'
Protocol: DHCP client	Protocol: Not connected
Address: 192.168.1.67	Address: --
Netmask: 255.255.255.0	Gateway: --
Gateway: 192.168.1.254	
DNS 1: 202.96.134.133	
DNS 2: 114.114.114.114	
Expires: 32h 42m 31s	
Connected: 3h 12m 29s	
IP Device: Software VLAN: 'veth0.7'	
MAC Address: 94:83:C4:D8:20:80	
Active Connections	
238 / 1024 (15%)	

Click 'Scan' on 2.4G section or 5G section.

GL-AR750S Status System Network Logout

rednet Master "GL-AR750S-888-Guest-SG" rednet Master "GL-AR750S-888-SG" rednet Master "GL-AR750S-888-Guest"

rednet Master "GL-AR750S-888"

Wireless Overview

Signal	SSID	Channel	Mode	Encryption	Buttons
0%	Generic MAC90211 802.11nac	6 (129) (HWT)	Master		Restart Scan Add
0%	SSID: GL-AR750S-888-SG Mode: Master			Encryption: WPA2-PSK (CCMP)	Disable Edit Remove
0%	SSID: GL-AR750S-888-Guest-SG Mode: Master			Encryption: WPA2-PSK (CCMP)	Disable Edit Remove
0%	SSID: GL-AR750S-888-Guest Mode: Master			Encryption: WPA2-PSK (CCMP)	Disable Edit Remove

Associated Stations

Network	MAC Address	Host	Signal/Noise	RX Rate / TX Rate
No information available				

Powered by LuCI openwrt 18.06 branch (git 18.06.50128-0112196) / OpenWrt 18.06.1 r7258-5ad5530f

Join the network you want.

GL-AR750S Status System Network Logout

Join Network: Wireless Scan

Signal	SSID	Channel	Mode	Encryption	Buttons
21%	GL-81089-8C2	6	Master	Encryption: WPA2-PSK (CCMP)	Join Network
42%	GL-0FFHC21	6	Master	Encryption: WPA2-PSK (CCMP)	Join Network
35%	GL-0FFHC21	6	Master	Encryption: WPA2-PSK (CCMP)	Join Network
42%	GL-0758-460	11	Master	Encryption: WPA2-PSK (CCMP)	Join Network

Back to overview Repeat scan

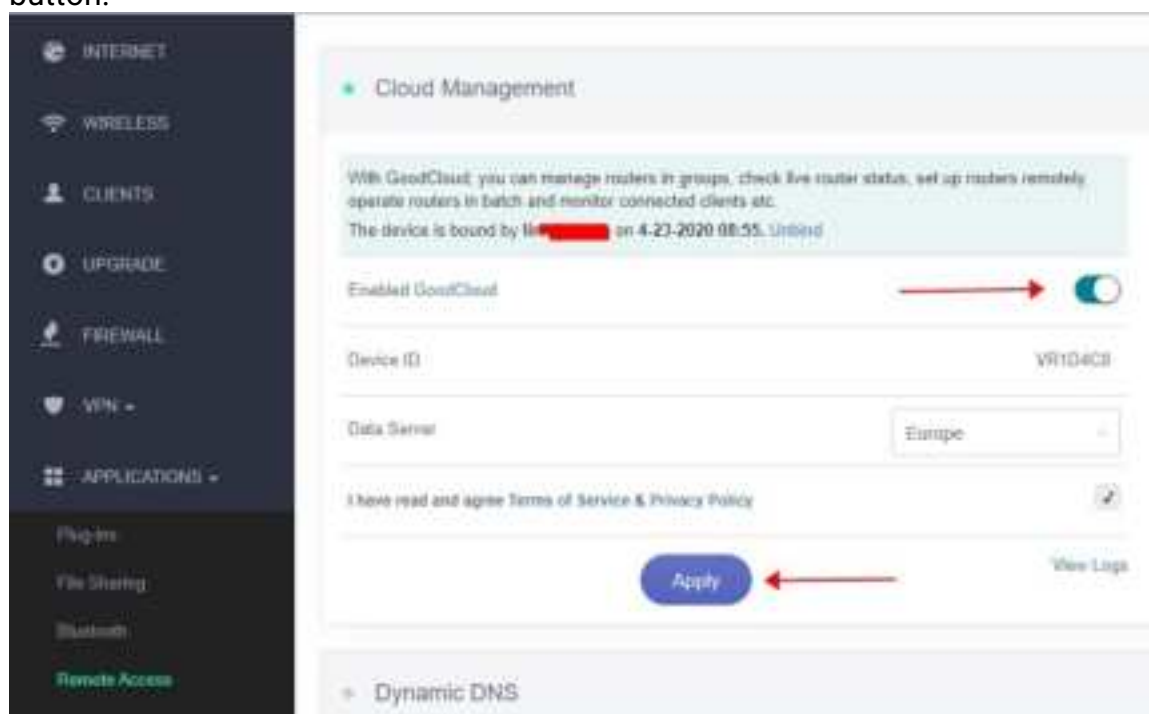
Powered by LuCI openwrt 18.06 branch (git 18.06.50128-0112196) / OpenWrt 18.06.1 r7258-5ad5530f

10.9 GoodCloud issues

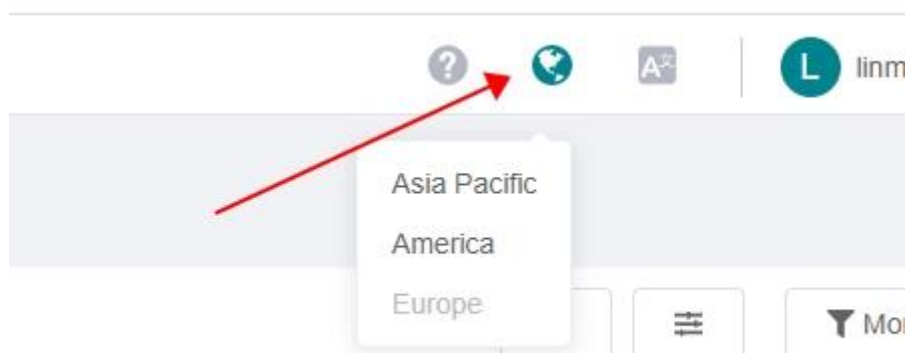
How to fix if my device show "Deactivated"

The "Deactivated" mean the device never been connected to the server before.

1. Make sure the router has connected to the Internet.
2. And try to disable and re-enable the GoodCloud on router's Admin Panel.
Don't forget to click "Apply" button.



3. Make sure to access to the right region of



GoodCloud.