



Admin Password

GL-AR750

Please enter password



Login

[Forgot Password ?](#)

INTERNET

WIRELESS

CLIENTS

UPGRADE

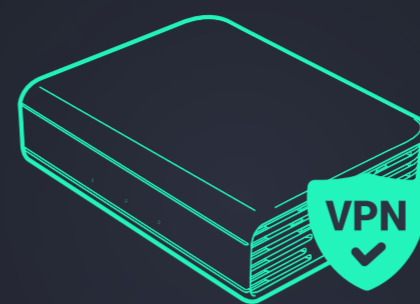
FIREWALL

VPN

APPLICATIONS

MORE SETTINGS

- Cable
- minicooper
- Tethering
- 3G/4G Modem



GL-2.4G
GL-2.4G-Guest
GL-5G
GL-Guest-5G

- 0 WLAN Clients
- 1 LAN Clients

Cable

Protocol	DHCP
IP Address	192.168.98.68
Netmask	255.255.255.0
Gateway	192.168.98.1
DNS Server	192.168.98.69

Modify



minicooper 5G

Scan

IP Address	192.168.189.2
Netmask	255.255.255.0
Gateway	192.168.189.1
DNS Server	192.168.189.1

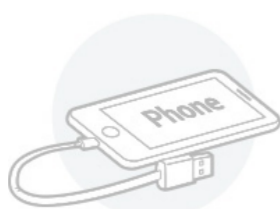
Disconnect



Saved Networks

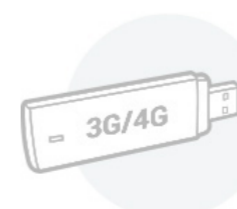
Repeater Options

Tethering



No Tethering device found. Plug in your smartphone or USB modem to start.

3G/4G Modem



No Modem device found. Plug in your USB modem to start.

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
- MORE SETTINGS

- 2.4G WiFi
- 2.4G Guest WiFi

GL-2.4G ON

Wi-Fi Name (SSID)	GL-2.4G
Wi-Fi Security	WPA/WPA2-PSK
Wi-Fi Key
SSID Visibility	Shown
Wi-Fi Mode	802.11b/g/n
Bandwidth	20/40 MHz
Channel	11
TX Power (dBm)	Max

Modify
Channel Optimization

- 5G WiFi
- 5G Guest WiFi

GL-5G 5G ON

Wi-Fi Name (SSID)	GL-5G
Wi-Fi Security	WPA/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

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN

APPLICATIONS

MORE SETTINGS

2.4G WiFi

2.4G Guest WiFi

GL-2.4G-Guest



Wi-Fi Name (SSID)

GL-2.4G-Guest

Wi-Fi Security

WPA2-PSK

Wi-Fi Key

.....

Modify

5G WiFi

5G Guest WiFi

GL-5G 5G



Wi-Fi Name (SSID)

GL-5G

Wi-Fi Security

WPA/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

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

● CLIENTS

Enable real-time speed and traffic statistics. This requires higher CPU load.



Brand	Name	IP	MAC	Block
Wired Device				
	GG-i5	192.168.8.125	00:60:6E:43:E6:38	<input checked="" type="checkbox"/>
Offline Device				
	*	192.168.8.100	00:0E:2E:84:C7:59	<input type="checkbox"/>
	gg-probook	192.168.8.149	98:E7:F4:57:A1:E2	<input type="checkbox"/>
	*	192.168.8.183	7C:B0:C2:84:74:07	<input type="checkbox"/>

 INTERNET

 WIRELESS


 CLIENTS

 **UPGRADE**

 FIREWALL

 VPN ▾

 APPLICATIONS ▾

 MORE SETTINGS ▾

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

Current Version

-

Compile Time

-

Last Update

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade



Select a file or drag it here.

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

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

Router Time

Sat Feb 20 09:47:48 CET 2021

Enable Auto Upgrade



Auto Upgrade Time

07:00 ▾

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL**
- VPN
- APPLICATIONS
- MORE SETTINGS

Firewall

- Port Forwards
- Open Ports on Router
- DMZ

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.)

Name	Protocol	External Zone	External Ports ⓘ	Internal Zone	Internal IP	Internal Ports ⓘ	Status	Action
Required	TCP/U	wan	Required	lan	Required	Required	Enable	Add

Add a New One

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

● 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
<input type="text" value="Required"/>	<input type="text" value="Required"/>	TCP/UDP ▾	Enabled ▾	Add
web	80	TCP	Enabled	Modify Delete
https	443	TCP	Enabled	Modify Delete

Delete All

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

● 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

192.168.8.149 ▾

Apply

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

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

Current OpenVPN Configuration

device ▾

Server cablant-device-22-gerhard-openwrt.ovpn ⚙

IP Address	10.1.0.13
Data Received / Sent	10MB / 30MB

Disconnect

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

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

● device ▾

Type

OpenVPN

Config Count

1

Server

cablant-device-22-gerhard-openwrt.ovpn ⚙

Description

device








Remove

Apply

● cablant09 ▾

+ Add a New OpenVPN Configuration

🗑 Purge All Profiles

-  INTERNET
-  WIRELESS
-  CLIENTS
-  UPGRADE
-  FIREWALL
-  VPN ▾
 -  OpenVPN Client
 - OpenVPN Server**
 - WireGuard Client
 - WireGuard Server
 - SS Server
 - SS Client
 - Internet Kill Switch
 - VPN Policies

● OpenVPN Server

Access Local Network 

Type Router ▾

IP Address 10.8.0.0

Netmask 255.255.255.0

Port 1195

Encryption BF-CBC ▾

Authentication SHA1 ▾

Protocol TCP ▾

Modify

Start

[Export Config](#)

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN ▾**

- OpenVPN Client**
- OpenVPN Server
- WireGuard Client**
- WireGuard Server
- SS Server
- SS Client
- Internet Kill Switch
- VPN Policies

- APPLICATIONS ▾
- MORE SETTINGS ▾

WireGuard® 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.

Server

Connect

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

WireGuard® 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

WireGuard® Server

3

● schweiz155



● egersdorf



● blackbox193



+ Add New Profiles

🗑️ Purge All Profiles

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

WireGuard® Server

Status

Management

Allow Access Local Network ⓘ



Local IP

10.0.0.1

Local Port

51825

Start

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾



MORE SETTINGS ▾

WireGuard® Server

Status

Management

WireGuard® Clients

Name	Client IP	Configurations	Delete
gg-laptop	10.0.0.2/32		

+ Add a New User

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

Shadowsocks Server

Port

Password

Encryption

 ▾

Start

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

Shadowsocks Client

ⓘ Shadowsocks only proxy TCP traffic. UDP traffic will not be monitored. Use OpenVPN or WireGuard to protect data leaks. Shadowsocks doesn't resolve DNS. Use DNS via TLS to protect DNS leaks.

Status

Management

SS Client

egersdorf ▾

Connect

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

Shadowsocks Client

⚠ Shadowsocks only proxy TCP traffic. UDP traffic will not be monitored. Use OpenVPN or WireGuard to protect data leaks. Shadowsocks doesn't resolve DNS. Use DNS via TLS to protect DNS leaks.

Status

Management

SS Configurations

1

egersdorf



+ Add a New Shadowsocks Client

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

OpenVPN Client

OpenVPN Server

WireGuard Client

WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

APPLICATIONS ▾

MORE SETTINGS ▾

Internet Kill Switch

Apply

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

Enable



 INTERNET WIRELESS CLIENTS UPGRADE FIREWALL VPN ▾ OpenVPN Client

OpenVPN Server

WireGuard Client


WireGuard Server

SS Server

SS Client

Internet Kill Switch

VPN Policies

 APPLICATIONS ▾ MORE SETTINGS ▾

● VPN Policies

Enable VPN Policy



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
<input type="text" value="e.g. google.com 192.168.1.1 192.168.1.0/24"/>	<input type="button" value="Add"/>
192.168.98.0/24	<input type="button" value="Delete"/>
192.168.2.0/24	<input type="button" value="Delete"/>
192.168.189.0/24	<input type="button" value="Delete"/>
192.168.178.0/24	<input type="button" value="Delete"/>
192.168.179.0/24	<input type="button" value="Delete"/>

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

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
 - Plug-ins
 - File Sharing
 - Remote Access
 - Captive Portal
- MORE SETTINGS

Plug-ins

Update

Filter

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	Description	Action
ath10k-firmware-qca9887	2018-04-19-71e50312-1	-	✕ Uninstall
base-files	194-r7258-5eb055306f	-	✕ Uninstall
blkid	2.32-2	-	✕ Uninstall
bridge	1.5-5	-	✕ Uninstall
busybox	1.28.3-6	-	✕ Uninstall
ca-bundle	20200601	-	✕ Uninstall
ca-certificates	20200601	-	✕ Uninstall
chat	2.4.7-13	-	✕ Uninstall

Free space: 10% (1 MB)

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

Plug-ins

File Sharing

Remote Access

Captive Portal

MORE SETTINGS ▾

● File Sharing

Share via LAN ⓘ



Share via WAN ⓘ



Writable ⓘ



Current Directory

/mnt ▾

Apply


 INTERNET WIRELESS CLIENTS UPGRADE FIREWALL VPN ▾ APPLICATIONS ▾

Plug-ins

File Sharing

Remote Access

Captive Portal

 MORE SETTINGS ▾

● 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.

Your device ID is **fef0054**, Please use the ID to add this device to your cloud account. [?](#)








Enabled [GoodCloud](#)[Apply](#)[View Logs](#)

● 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](#) [i](#)[Apply](#)

-  INTERNET
-  WIRELESS
-  CLIENTS
-  UPGRADE
-  FIREWALL
-  VPN ▾
-  APPLICATIONS ▾
- Plug-ins
- File Sharing
- Remote Access
- Captive Portal

● Captive Portal

You can set up a captive portal to display a web page when a user connects to your Wi-Fi network. [Help?](#)

- ❗ If Guest network is disabled, captive portal function is unavailable.**
- ❗ Opening the captival portal will cause the block function to fail.**

Enable captive portal

Virtual network interface Guest

Lease time minutes (1-1440):

Forward URL after Authorization

Apply

-  MORE SETTINGS ▾

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● Admin Password

Apply

Old Password

Required



New Password ⓘ

Required



Confirm Password ⓘ

Required



- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
- MORE SETTINGS
- Admin Password
- LAN IP
- Time Zone
- MAC Clone
- Custom DNS Server
- Button Settings
- Network Mode
- Revert Firmware
- Advanced

LAN IP Guest IP

LAN IP

Apply

GL routers use 192.168.8.1 as the default LAN IP address. This is the address you would enter into your browser 's address bar to access the router admin page. You can manually setup one within these three ranges:192.168.x.x , 172.x(16-31).x.x or 10.x.x.x

Note: The starting IP address and ending IP address must be in the range of 2~254, and the ending address should be greater than starting address.

LAN IP

Start IP Address

End IP Address

Static IP Address Binding

Usually your computer's IP address is dynamically assigned by the router. If you want your computer to have a static IP address, you can manually add your computer's MAC address and the static IP address you want to use.

Mind the configured client has to reconnect the router to come into effect.

MAC	IP	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▼

APPLICATIONS ▼

MORE SETTINGS ▼

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

LAN IP

Guest IP

GUEST IP

Apply

The GL router uses 192.168.9.1 as the default guest IP address. Note: Do not conflict with the LAN IP when modifying the guest IP. You can manually setup one within these three ranges: 192.168.x.x , 172.x(16-31).x.x or 10.x.x.x

Note: The starting IP address and ending IP address must be in the range of 2~254, and the ending address should be greater than starting address.

GUEST IP

192.168.9.1

Start IP Address

192.168.9. 100

End IP Address

192.168.9. 249

Static IP Address Binding

Usually your computer's IP address is dynamically assigned by the router. If you want your computer to have a static IP address, you can manually add your computer's MAC address and the static IP address you want to use.

Mind the configured client has to reconnect the router to come into effect.

MAC	IP	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● Time Zone

Apply

Router Time

Sat Feb 20 09:53:28 CET 2021

Europe/Berlin ▾

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● MAC Clone









Apply

MAC Clone is useful when you connect to a public hotspot but you do not want the server to check your real MAC address or limit your Internet connections based on your MAC address. e.g. If you get your smartphone registered on the network, you can clone your smartphone's MAC address to the router so that the router can also connect.

Your Current Client 00:60:6E:43:E6:38

Factory Default E4:95:6E:4F:00:54

Your Router (WAN) E4:95:6E:4F:00:54 ▾

-  INTERNET
-  WIRELESS
-  CLIENTS
-  UPGRADE
-  FIREWALL
-  VPN ▾
-  APPLICATIONS ▾
-  MORE SETTINGS ▾
- Admin Password
- LAN IP
- Time Zone
- MAC Clone
- Custom DNS Server
- Button Settings
- Network Mode
- Revert Firmware
- Advanced

● Custom DNS Server

Apply

- DNS Rebinding Attack Protection ?
- Override DNS Settings for All Clients ?
- DNS over TLS (Cloudflare or NextDNS)
- Select DNS Server Cloudflare ▾
- Dnscrypt-Proxy Settings
- Manual DNS Server Settings

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● Button Settings

Apply

Switch Button

No function (default) ▾



INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● Network Mode



- i** When you change the router's working mode, you may need to re-connect all your client devices.
- i** When you use Access Point/Extender/WDS mode, you may not connect to this UI again. You can Press and hold the reset button for 4 seconds to revert back to router mode.
- i** **OpenVPN or Wireguard client is enabled. Please disable them in order to set up bridge mode.**

🏠 Mode Switch

 Router Access Point Extender WDS

Apply

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Button Settings

Network Mode

Revert Firmware

Advanced

● Revert Firmware

⚠ In case of malfunction, you can revert to factory default settings. All your current settings, applications and data will be lost. The process will take about 3 minutes. DO NOT power off the router during this process.

Revert Now

Authorization Required

Please enter your username and password.

Username

Password