GL·iNet



Benutzerhandbuch

GL-AR300M16 / Shadow

Kompakter WLAN-Router

Firmware-Version 4.3.27

Über dieses Handbuch

Dieses Handbuch hilft Ihnen bei der Inbetriebnahme Ihres Geräts. Es enthält grundlegende Produktinformationen, Anleitungen zum Anschließen der Hardware, zur Anmeldung an der Weboberfläche und zur Ersteinrichtung sowie ausführliche Beschreibungen aller Softwarefunktionen der Weboberfläche.

Mit diesem Handbuch können Sie:

- Die wichtigsten Produkteigenschaften kennenlernen
- Einen geeigneten Standort für das Gerät auswählen
- Die Hardware Schritt für Schritt anschließen
- Sich einfach an der Weboberfläche anmelden
- Die Ersteinrichtung vornehmen und alle Softwarefunktionen der Weboberfläche nutzen

Darstellungskonventionen

Diese Symbole und Farben erleichtern Ihnen das Befolgen der Anweisungen.

Darstellung	Bedeutung
Unterstrichener türkisfarbener Text	Anklickbarer Link zu einer Webseite oder einem bestimmten Abschnitt
Fettdruck	Hebt wichtige Informationen hervor, etwa Überschriften, Hyperlinks und die genauen Bezeichnungen von Menüs und Einträgen auf der Weboberfläche des Geräts
>	Menüpfad zum Aufrufen der entsprechenden Seite (z. B. System > Firmware)
Hinweis	Wichtige Informationen zur Einrichtung, Bedienung und Sicherheit. Die Nichtbeachtung kann zu Fehlern bei der Einrichtung, Fehlfunktionen oder Schäden am Gerät führen
Tipps	Empfehlungen für die optimale Nutzung Ihres Geräts

Hinweis:

- Die Gerätefunktionen können je nach Modell und Firmwareversion variieren.
- Die Produktverfügbarkeit kann je nach Region oder Vorgaben des Internetanbieters abweichen.
- Alle Abbildungen, Abläufe und Beschreibungen in diesem Handbuch dienen nur der Veranschaulichung und können von Ihrer tatsächlichen Nutzungssituation abweichen.

Weitere Hilfe und Informationen

- Firmware aktualisieren: GL.iNet Firmware-Downloadcenter | Router
- Community: Diskutieren Sie über unsere Produkte und tauschen Sie Erfahrungen aus im GL.iNet Community-Forum
- Technischer Support: Kontaktieren Sie unseren technischen Support über die Kontaktseite

Copyright © 2026 GL.iNet Technology (HK) Ltd. Alle Rechte vorbehalten.
Ohne vorherige schriftliche Genehmigung von GL.iNet Technology (HK) Ltd. darf dieses Handbuch weder ganz noch teilweise in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, abgeschrieben, übersetzt oder verbreitet werden. GL.iNet ist eine eingetragene Marke von GL.iNet Technology (Hong Kong) Ltd. in China und/oder anderen Ländern und Regionen. Alle anderen hier genannten Marken- und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer.
Der Inhalt dieses Dokuments kann aufgrund von Produktaktualisierungen oder aus anderen Gründen ohne vorherige Ankündigung geändert werden. Sofern nicht anders vereinbart, dient dieses Dokument ausschließlich zu Informationszwecken. Die darin enthaltenen Aussagen, Informationen und Empfehlungen stellen keinerlei Garantie dar.

GL Tech (HK) Ltd: #601, 5W, Hong Kong Science Park, N.T. Hong Kong
GL Intelligence, Inc.: 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Inhaltsverzeichnis

Sicherheitshinweise 8

Kapitel 1 Ihren Router kennenlernen 10

1.1 Produktübersicht 11

1.1.1 Geräteansicht 11

1.1.2 Anschlüsse und Bedienelemente 13

1.1.3 LED-Anzeige 15

1.2 Technische Daten 15

1.3 Lieferumfang 16

Kapitel 2 Hardware anschließen 18

2.1 Standort auswählen 19

2.2 Router anschließen 19

Kapitel 3 Am Router anmelden 21

Kapitel 4 Internetverbindung einrichten 23

4.1 Internetverbindung über Ethernetkabel 25

4.1.1 Grundeinrichtung 25

4.1.2 Protokoll 27

4.2 Internetverbindung über ein vorhandenes WLAN 30

4.2.1 Grundeinrichtung 31

4.2.2 Repeater-Optionen 34

4.3 Internetverbindung über USB-Tethering 35

4.3.1 Tethering mit einem iPhone 35

4.3.2 Tethering mit einem Android-Smartphone 37

4.3.3 Fehlerbehebung 38

4.4 Internetverbindung über ein USB-Modem 39

Kapitel 5 WLAN 41

Kapitel 6 Verbundene Geräte 44

6.1 Gerätedetails 46

6.2 Aktionen 48

6.3 Geräte entfernen 50

6.4 Sortierung 51

Kapitel 7 VPN kennenlernen 52

7.1 Einführung 53
7.2 Einsatzmöglichkeiten 54
Kapitel 8 VPN-Dashboard 57
8.1 VPN-Client 58
8.1.1 Client-Optionen 59
8.1.2 Richtlinienmodus 61
8.1.3 Globale Optionen 62
8.2 VPN-Server 65
8.2.1 Server-Optionen 66
8.2.2 Server-Routingregeln 67
8.2.3 Globale Optionen 69
Kapitel 9 VPN-Server einrichten 70
9.1 OpenVPN-Server einrichten 71
9.1.1 Vorbereitung 71
9.1.2 Einrichtung 72
9.1.3 Fehlerbehebung 74
9.2 WireGuard-Server einrichten 76
9.2.1 Vorbereitung 76
9.2.2 Einrichtung 77
9.2.3 Fehlerbehebung 80
Kapitel 10 VPN-Client einrichten 81
10.1 OpenVPN-Client einrichten 82
10.1.1 Vorbereitung 82
10.1.2 NordVPN einrichten 82
10.1.3 OpenVPN-Client manuell einrichten (andere Anbieter) 88
10.2 WireGuard-Client einrichten 91
10.2.1 Vorbereitung 91
10.2.2 AzireVPN einrichten 92
10.2.3 Mullvad einrichten 95
10.2.4 WireGuard-Client manuell einrichten (andere Anbieter) 99
Kapitel 11 Anwendungen 104
11.1 Plug-ins 105
11.2 Dynamisches DNS 106
11.2.1 DDNS aktivieren 106

11.2.2 DDNS-Funktion prüfen 108
11.2.3 HTTP-Fernzugriff 110
11.2.4 HTTPS-Fernzugriff 111
11.2.5 SSH-Fernzugriff 113
11.3 GoodCloud 114
11.3.1 GoodCloud aktivieren 115
11.3.2 Router verwalten 120
11.3.3 Geräteverknüpfung aufheben 126
Kapitel 12 Netzwerk 127
12.1 Firewall 128
12.1.1 Portweiterleitungen 128
12.1.2 Ports am Router öffnen 130
12.1.3 DMZ 131
12.2 Multi-WAN 132
12.2.1 Schnittstellenstatus überwachen 132
12.2.2 Multi-WAN-Modus 135
12.3 LAN 138
12.3.1 Privates Netzwerk 138
12.3.2 Gastnetzwerk 140
12.3.3 Adressreservierung 142
12.4 DNS 144
12.4.1 Allgemeine Einstellungen 144
12.4.2 DNS-Servereinstellungen 145
12.4.3 Hosts bearbeiten 147
12.5 Netzwerkmodus 149
12.6 IPv6 151
12.6.1 IPv6-Modus 151
12.6.2 DNS-Adressen beziehen 152
12.7 MAC-Adresse 153
12.8 Drop-in Gateway 155
12.9 IGMP Snooping 157
Kapitel 13 System 158
13.1 Übersicht 159
13.2 Aktualisierung 160

13.2.1 Online-Aktualisierung 160
13.2.2 Lokale Aktualisierung 161
13.3 Geplante Aufgaben 162
13.3.1 LED-Zeitplan 162
13.3.2 Geplanter Neustart 163
13.3.3 Zeitplan für das 2,4-GHz-WLAN 164
13.4 Administratorpasswort 167
13.5 Zeitzone 168
13.6 Schiebeschalter konfigurieren 169
13.7 Protokolle 170
13.8 Firmware zurücksetzen 171
13.9 Erweiterte Einstellungen 172

Sicherheitshinweise

Lesen Sie vor der Verwendung des Geräts alle nachstehenden Sicherheitsinformationen sorgfältig durch. Die nachfolgenden Sicherheitsempfehlungen können nicht sämtliche möglicherweise auftretenden Gefahrensituationen abdecken.

Installieren oder verwenden Sie das Gerät nicht in Umgebungen mit hohen Temperaturen, starker Staubentwicklung, schädlichen Gasen, Brandgefahr, Explosionsgefahr, starken elektromagnetischen Störungen, instabiler Netzspannung, starken Vibrationen oder starker Lärmeinwirkung.

Installieren oder verwenden Sie das Gerät nicht in feuchten Umgebungen, in denen Wasseransammlungen, eindringendes Wasser, Tropfwasser oder Kondensat auftreten können, da dies einen Stromschlag verursachen kann.

Elektromagnetische Störungen können von jedem Gerät ausgehen, das elektromagnetische Signale aussendet. Um Störungen medizinischer Geräte zu vermeiden, befolgen Sie beim Betrieb dieses Geräts insbesondere in Krankenhäusern, ambulanten Gesundheitszentren, Arztpraxen und sonstigen medizinischen Einrichtungen die Anweisungen und Vorgaben des autorisierten Personals, um eine Beeinflussung empfindlicher medizinischer Geräte auszuschließen.

Sofern das Gerät mit einem Netzteil ausgeliefert wird, verwenden Sie zur Stromversorgung ausschließlich das mitgelieferte Netzteil.

Sofern das Gerät mit einem Bildschirm ausgestattet ist und dieser Risse oder Beschädigungen aufweist, verwenden Sie das Gerät nicht weiter. Gebrochenes Glas oder gebrochener Kunststoff kann zu Verletzungen an Händen oder im Gesicht führen.

Sofern das Gerät mit einer Batterie ausgestattet ist, verwenden Sie ausschließlich Batterien, die den Anforderungen der Spezifikation entsprechen. Weist die Batterie sichtbare Beschädigungen auf, tauschen Sie sie aus, da es andernfalls zu Personenschäden kommen kann. Funkendgeräte dürfen nur bei geschlossener Batterieabdeckung betrieben werden.

Bewahren Sie kleine Batterien und Kleinteile, die verschluckt werden könnten, für Kinder unzugänglich auf. Das Verschlucken einer Batterie kann schwere Verletzungen verursachen; nehmen Sie in diesem Fall unverzüglich ärztliche Hilfe in Anspruch.

Vermeiden Sie ein häufiges Umstellen des Geräts. Schalten Sie vor jedem Bewegen oder Transportieren sämtliche Stromversorgungen aus und ziehen Sie alle Netz- und Anschlusskabel ab.

Überlastete Steckdosen, Verlängerungskabel und Steckdosenleisten können Brände und Stromschläge verursachen.

Durch Wärmestau kann sich das Gerät übermäßig erhitzen. Stellen Sie das Gerät daher nicht auf Teppiche oder weiche Unterlagen und sorgen Sie für eine ausreichende Luftzirkulation im Umfeld des Geräts. Stellen Sie das Gerät nicht auf Oberflächen von Gegenständen, die empfindlich auf Wärme reagieren.

Um den einwandfreien Betrieb des Geräts zu gewährleisten, beachten Sie die in den technischen Daten angegebene zulässige Betriebsumgebungstemperatur des Geräts.

Unsachgemäßes Öffnen oder unsachgemäße Instandsetzung kann den Benutzer des Geräts gefährden.

Schalten Sie bei einem Störfall zuerst den Netzschalter aus.

Kapitel 1

Ihren Router kennenlernen

Dieses Kapitel enthält eine Übersicht über den Router, seine technischen Daten und den Lieferumfang.

1.1 Produktübersicht

Shadow (GL-AR300M16) ist ein kompakter, leicht transportierbarer Mini-Router für unterwegs mit einer WLAN-Übertragungsrate von bis zu 300 Mbit/s. Er bietet erweiterte Sicherheitsfunktionen mit Unterstützung für OpenVPN, WireGuard® und einen DNS-Server. Sie können ein öffentliches Netzwerk in ein privates WLAN für sicheres Surfen umwandeln. Außerdem lassen sich VPN-Konfigurationsdateien von mehr als 30 Anbietern hochladen, um den Router als VPN-Client einzurichten. Die verschlüsselte Datenübertragung zwischen Ihrem Gerät und dem VPN-Server bietet zusätzlichen Schutz für Ihre Privatsphäre und Sicherheit.

1.1.1 Geräteansicht

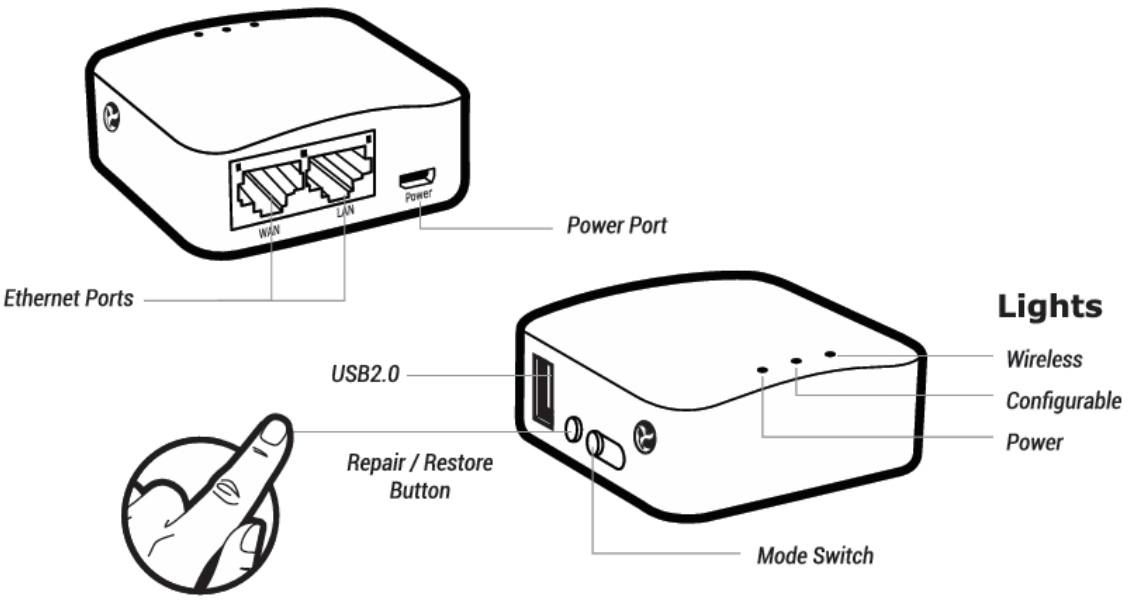





WAN
LAN
Power


USB
Reset

1.1.2 Anschlüsse und Bedienelemente



Element	Beschreibung
Stromanschluss	Zum Anschließen des Netzteils.
WAN-Ethernetanschluss	Zum Anschließen eines Modems oder einer Ethernetdose für den Internetzugang.
LAN-Ethernetanschluss	Zum Anschließen kabelgebundener Geräte bei Bedarf.
USB 2.0	Für USB-Speichergeräte, USB-Tethering mit ei- nem Smartphone und kompatible Mobilfunksticks.
Modusschalter	Ein Schalter zum schnellen Umschalten ausgewählter Routerfunktionen. Über die Weboberfläche können Sie festlegen, welche Funktion mit dem Schalter ein- oder ausgeschaltet wird.

Taste zum Reparieren/Zurücksetzen	Halten Sie die Taste **4 Sekunden** gedrückt, um Ihr Netzwerk zu reparieren. Halten Sie die Taste **10 Sekunden** gedrückt und lassen Sie sie dann los, um den Router auf die Werkseinstellungen zurückzusetzen.

1.1.3 LED-Anzeige

LED-Anzeige	Bedeutung
Betriebs-LED	Ein: Gerät eingeschaltet Aus: Gerät ausgeschaltet
Mittlere LED (konfigurierbar)	Ein: Dieser LED wurde eine Funktion zugewiesen Aus: Dieser LED wurde keine Funktion zugewiesen (Standard)
WLAN-LED	Ein: 2,4-GHz-WLAN verbunden Aus: 2,4-GHz-WLAN nicht verbunden

1.2 Technische Daten

Anschlüsse	1 × WAN-Ethernetanschluss 1 × LAN-Ethernetanschluss 3 × LED-Anzeigen 1 × USB-2.0-Anschluss 1 × Micro-USB-Stromanschluss 1 × Reset-Taste 1 × Schiebeschalter
CPU	QCA9531-SoC mit 650 MHz
Arbeitsspeicher / Speicher	128 MB DDR2 / 16 MB NOR-Flash
Protokoll	IEEE 802.11/b/g/n
WLAN-Geschwindigkeit	300 Mbit/s (2,4 GHz)
Ethernet-Geschwindigkeit	10/100 Mbit/s
Stromversorgung	Micro-USB, 5 V/2 A
LED-Anzeigen	Betrieb / WLAN
Leistungsaufnahme	< 2W
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Lagertemperatur	-20 ~ 70°C (-4 ~ 158°F)

Abmessungen / Gewicht	58 × 58 × 25 mm / 40 g
Weitere Ressourcen	Datenblatt / Firmware / App

*Die tatsächliche WLAN-Geschwindigkeit und Reichweite können durch Hindernisse, Netzauslastung und die Leistungsfähigkeit der Endgeräte variieren.

1.3 Lieferumfang

Bitte beachten Sie, dass das mitgelieferte Netzteil vom Lieferland abhängt.

Im Lieferumfang enthalten:

- 1 × Shadow (GL-AR300M16)
- 1 × Benutzerhandbuch
- 1 × Dankeskarte
- 1 × Ethernetkabel
- 1 × USB-Kabel



1 x User manual


1 x Shadow (GL-AR300M16)



1 x Thank you card


1 x Ethernet cable


1 x USB cable

(GL-AR300M16-Ext)



1 x User manual



1 x Shadow (GL-AR300M16)



1 x Thank you card



1 x Ethernet cable



1 x USB cable

(GL-AR300M16)

Kapitel 2

Hardware anschließen

Dieses Kapitel beschreibt die Standortwahl und die Schritte zum Anschließen des Routers.

2.1 Standort auswählen

Beachten Sie bei der Standortwahl die folgenden Tipps, um eine optimale Leistung zu erzielen.

- **Feuchtigkeit und Hitze vermeiden**: Stellen Sie den Router nicht an Orten auf, an denen er Wasser, hoher Luftfeuchtigkeit oder hohen Temperaturen ausgesetzt ist, etwa neben Waschbecken oder Heizkörpern.
- **Belüftung und Kühlung**: Stellen Sie den Router an einem kühlen, gut belüf- teten Ort auf, damit die Wärme ausreichend abgeführt werden kann.
- **Zentraler Standort**: Stellen Sie den Router so auf, dass er sich einfach mit der Stromversorgung und mehreren Geräten verbinden lässt, etwa an einer zentralen Stelle im Wohnzimmer.
- **Sichere Kabelführung**: Verlegen Sie Netzwerk- und Stromkabel so, dass keine Stolpergefahr besteht.
- **Stabile Oberfläche**: Stellen Sie den Router auf eine waagerechte, ebene Fläche, etwa ein Regal oder einen Schreibtisch.
- **Störquellen vermeiden**: Halten Sie Abstand zu elektromagnetischen Störquellen wie Bluetooth-Geräten oder Mikrowellen, um Signalstörungen zu minimieren.

2.2 Router anschließen

1. **Einschalten**
   Setzen Sie das zweiteilige Netzteil zusammen. Schließen Sie es an den Router an und stecken Sie es in eine Steckdose. Der Router startet automatisch.
2. **Ein Gerät mit dem Router verbinden**
   Verbinden Sie ein Gerät, etwa einen Laptop oder ein Smartphone, per WLAN oder Ethernetkabel mit dem Router.
   - **WLAN**: Öffnen Sie auf Ihrem Gerät Einstellungen > WLAN, wählen Sie den WLAN-Namen des Routers aus der Liste der verfügbaren Netzwerke aus und geben Sie das Passwort ein. Den voreingestellten Netzwerknamen und das Passwort finden Sie auf dem Geräteetikett.
   - **Ethernet**: Verbinden Sie Ihr Gerät über ein Ethernetkabel mit einem LAN-Anschluss des Routers.

3. **Am Router anmelden**

   Wenn Sie sich zum ersten Mal mit dem Router verbinden, steht noch keine Internetverbindung zur Verfügung. Melden Sie sich wie in Kapitel 3 beschrieben am Router an und schließen Sie die Ersteinrichtung ab, bevor Sie auf das Internet zugreifen.

Kapitel 3

Am Router anmelden

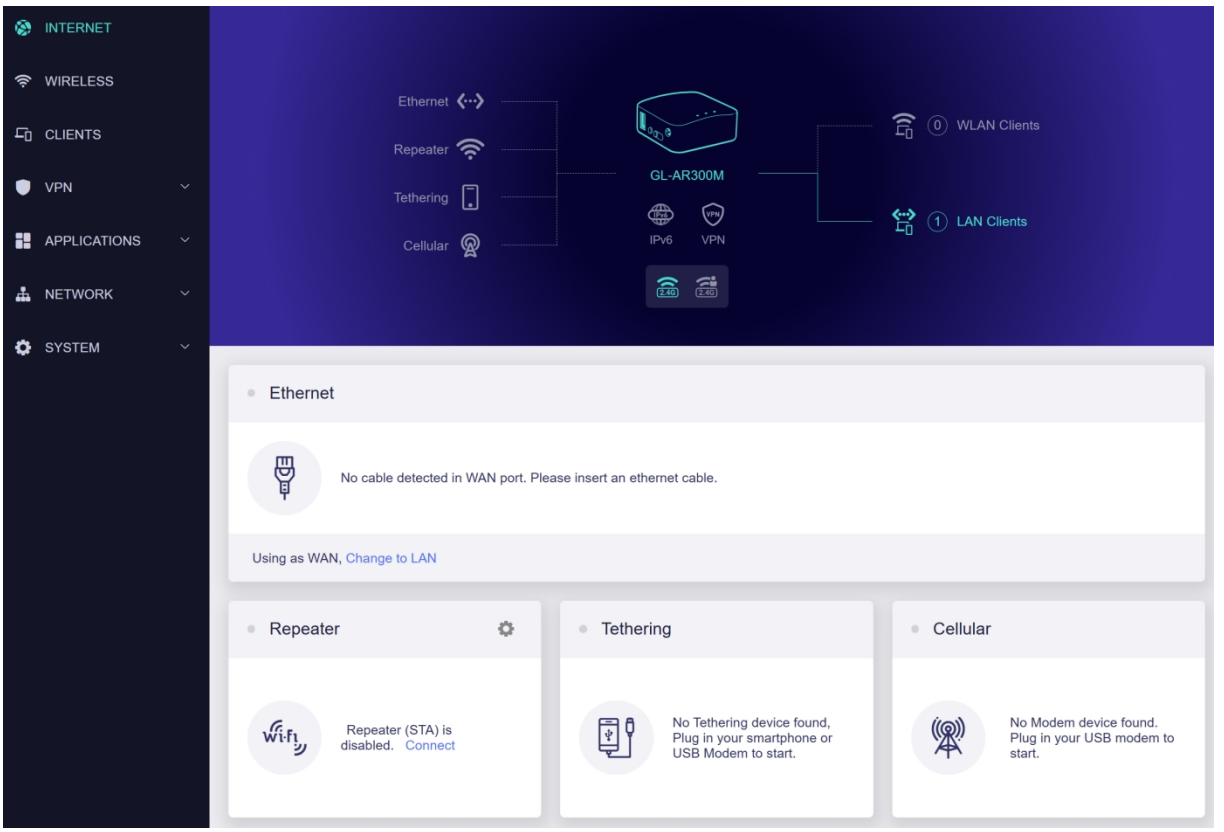
Dieses Kapitel erklärt, wie Sie sich über die Weboberfläche an Ihrem Router anmelden.

Sie können Ihren Router über eine webbasierte Verwaltungsoberfläche konfigurieren und verwalten. Diese lässt sich unter Windows, macOS oder Linux mit einem Webbrowser wie Microsoft Edge, Google Chrome, Mozilla Firefox oder Apple Safari aufrufen.

Hinweis: Wenn Sie die GL.iNet-App verwenden möchten, laden Sie die App herunter und folgen Sie den Anweisungen auf dem Bildschirm.

Gehen Sie wie folgt vor, um sich über die Weboberfläche an Ihrem Router anzumelden.

1. Verbinden Sie ein Gerät, etwa einen Computer oder Laptop, per WLAN oder Ethernetkabel mit dem Router.
2. Öffnen Sie einen Webbrowser (empfohlen werden Chrome und Edge) und rufen Sie http://192.168.8.1 auf. Sie gelangen zur Anmeldeseite der Weboberfläche. Falls Sie die Weboberfläche nicht erreichen können, finden Sie hier Hinweise zur Fehlerbehebung.
3. Legen Sie Ihr Administratorpasswort fest. Verwenden Sie aus Sicherheitsgründen ein starkes Passwort. Klicken Sie anschließend auf **Next**, um fortzufahren.
4. Anschließend wird die Weboberfläche des Routers angezeigt.



Kapitel 4

Internetverbindung einrichten

Dieses Kapitel stellt verschiedene Methoden vor, mit denen Sie den Router in unterschiedlichen Netzwerkumgebungen mit dem Internet verbinden können.

Shadow unterstützt vier Arten der Internetverbindung: Ethernet, Repeater, USB-Tethering und USB-Modem. Wählen Sie die für Ihren Einsatzzweck geeignete Methode.

1. **Ethernet**: Verbinden Sie den WAN-Anschluss des Routers über ein Ethernetkabel mit einem Breitbandnetz. In der Regel erhält der Router automatisch per DHCP eine IP-Adresse. Sie können auch eine statische IP-Adresse oder PPPoE manuell konfigurieren. Diese Methode bietet eine besonders stabile und schnelle Verbindung und eignet sich ideal für zu Hause oder das Büro mit festem Breitbandanschluss.

2. **Repeater**: In diesem Modus verbindet sich der Router mit einem vorhandenen WLAN, erweitert dessen Signalabdeckung und erstellt ein separates, sicheres lokales Netzwerk. Dabei kann die Übertragungsgeschwindigkeit etwas sinken. Der Modus eignet sich für Bereiche mit schwachem WLAN-Empfang und für öffentliche Orte, an denen zusätzliche Netzwerksicherheit erforderlich ist.

3. **USB-Tethering**: Verbinden Sie ein Smartphone oder ein anderes kompatibles Gerät per USB-Kabel mit dem Router, um dessen mobile Datenverbindung, etwa über 4G/5G, freizugeben. Dies ist eine praktische Lösung für einen vorübergehenden Internetzugang, besonders unterwegs oder an Orten ohne festen Breitbandanschluss.

4. **USB-Modem**: Stecken Sie ein USB-Mobilfunkmodem mit eingesetzter SIM-Karte in den Router. Dieser stellt dann über ein 4G/5G-Mobilfunknetz eine Internetverbindung her, unabhängig von einem Festnetzanschluss. Diese mobile Lösung eignet sich beispielsweise für den Einsatz im Fahrzeug oder im Freien.

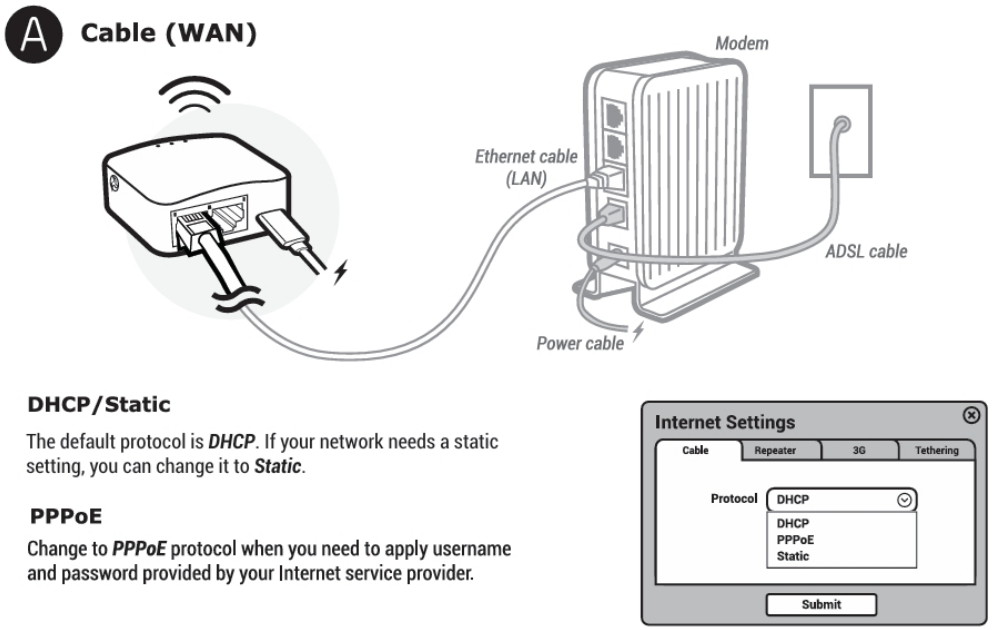
4.1 Internetverbindung über Ethernetkabel

Verbinden Sie den WAN-Anschluss des Routers über ein Ethernetkabel mit einem Breitbandnetz. In der Regel erhält der Router automatisch per DHCP eine IP-Adresse. Sie können auch eine statische IP-Adresse oder PPPoE manuell konfigurieren. Diese Methode bietet eine besonders stabile und schnelle Verbindung und eignet sich ideal für zu Hause oder das Büro mit festem Breitbandanschluss.

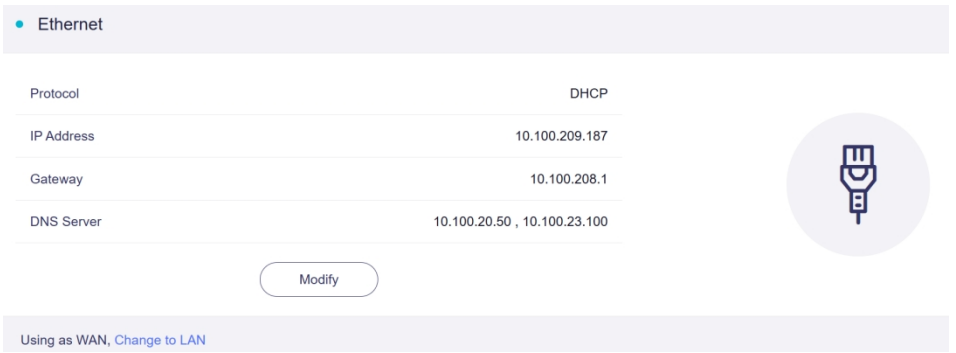
4.1.1 Grundeinrichtung

Gehen Sie wie folgt vor, um Ihren Router über ein Ethernetkabel mit dem Internet zu verbinden.

1. Verbinden Sie den **WAN**-Anschluss Ihres Routers über ein Ethernetkabel mit dem vorgeschalteten Gerät, etwa einem Modem des Internetanbieters, dem Hauptrouter, einem Netzwerkswitch oder einer Ethernetdose.

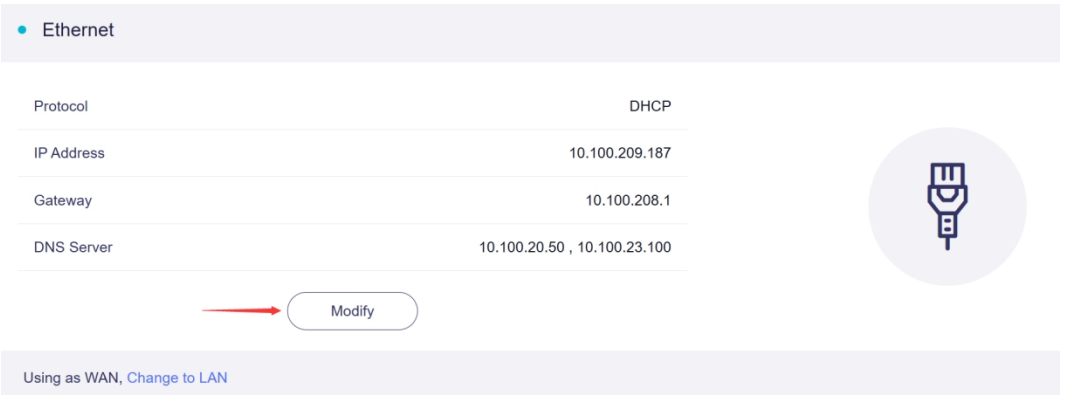


2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Ethernet**. Bei erfolgreicher Verbindung werden im Abschnitt Ethernet die Netzwerkdaten angezeigt, darunter Protokoll, IP-Adresse, Gateway und DNS-Server.


Ethernet
Protocol
DHCP
IP Address
10.100.209.187
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Modify
Using as WAN, Change to LAN

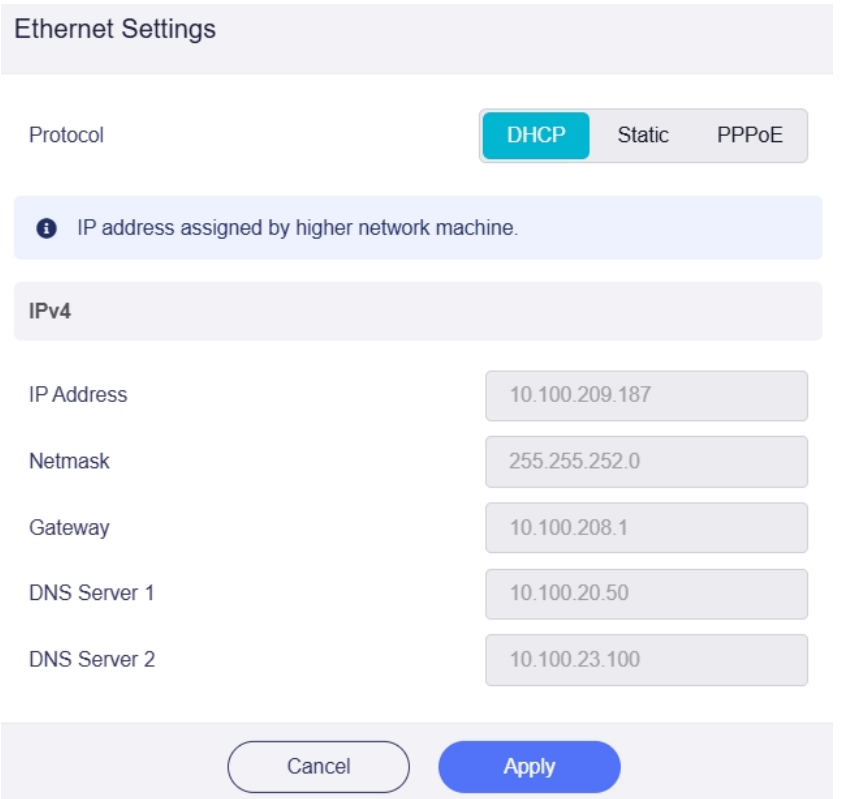
4.1.2 Protokoll

Es stehen drei Protokolle zur Auswahl: DHCP, Static und PPPoE. Klicken Sie auf **Modify**, um das Protokoll zu ändern.



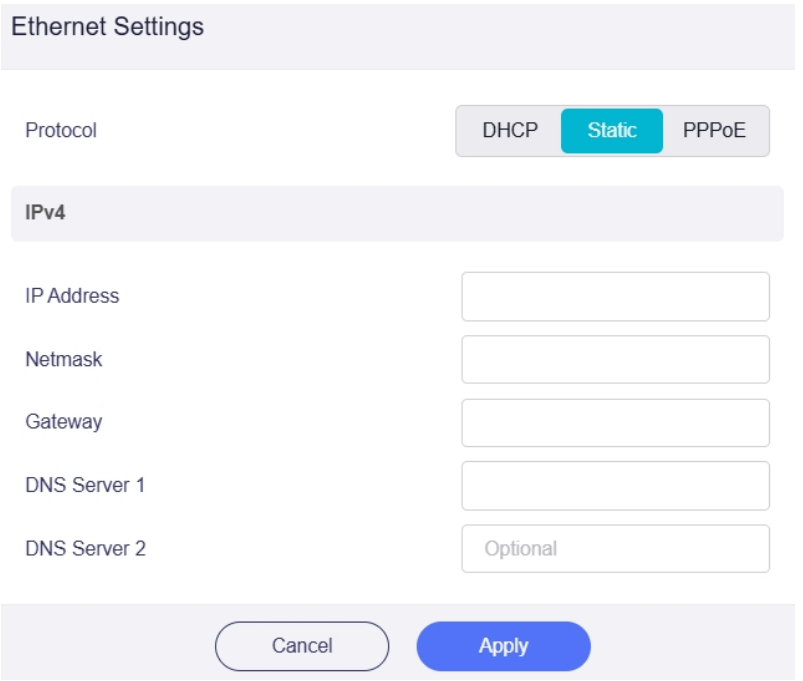
- **DHCP**

  DHCP ist das voreingestellte und am häufigsten verwendete Netzwerkprotokoll. Es weist Geräten in einem IP-Netzwerk nach dem Client-Server-Prinzip automatisch IP-Adressen und weitere Netzwerkeinstellungen zu.



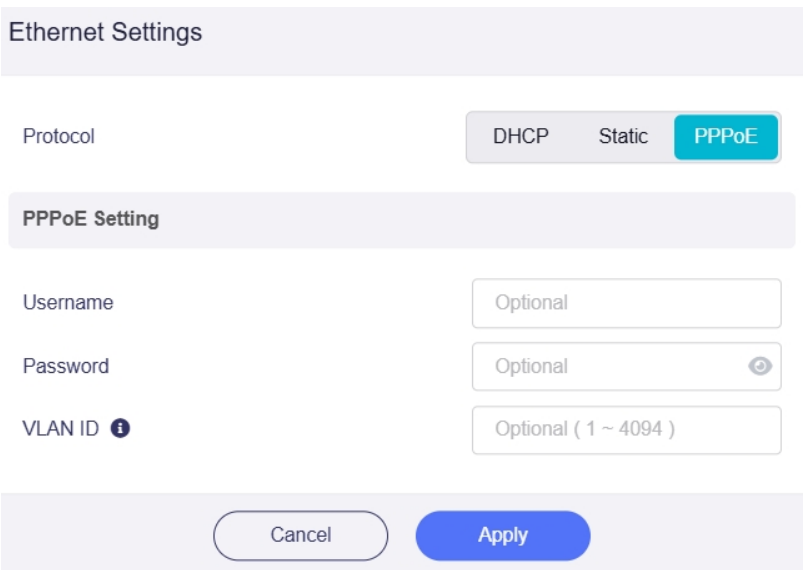
- **Statische IP-Adresse**

  Eine statische IP-Adresse ist erforderlich, wenn Ihr Internetanbieter Ihnen eine feste öffentliche IP-Adresse zuweist oder wenn Sie Netzwerkparameter wie IP-Adresse, Gateway und Subnetzmaske manuell festlegen müssen.



- **PPPoE**

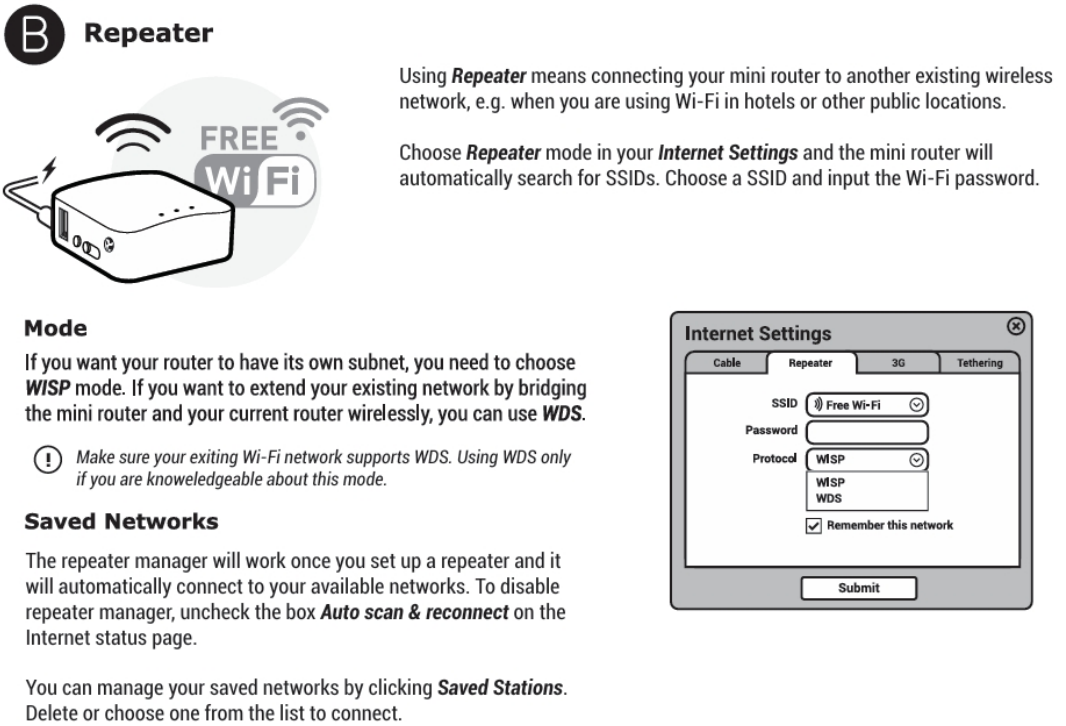
  PPPoE (Point-to-Point Protocol over Ethernet) ist ein von Internetanbietern häufig verwendetes Netzwerkprotokoll. In der Regel stellt der Anbieter ein Modem sowie einen individuellen Benutzernamen und ein Passwort bereit, die Sie zur Einrichtung der Internetverbindung benötigen.



Sie können eine **VLAN ID** konfigurieren, wenn Ihr Anbieter für die Schnittstelle eine bestimmte getaggte VLAN-ID vorschreibt.

4.2 Internetverbindung über ein vorhandenes WLAN

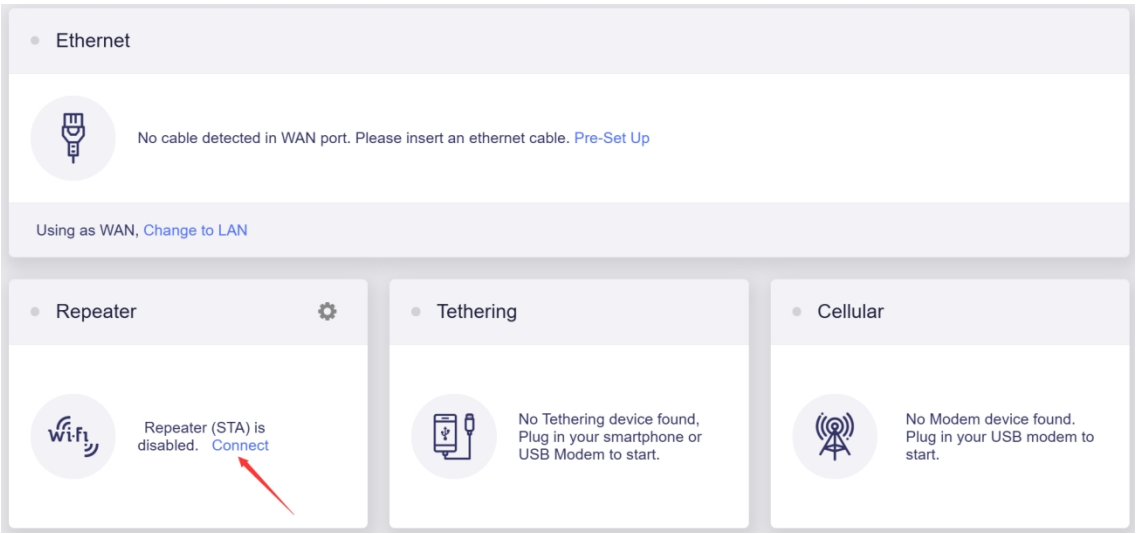
Verbinden Sie den Router als Repeater mit einem vorhandenen WLAN, um die Signalabdeckung zu erweitern und ein vom Hauptnetzwerk getrenntes lokales Netzwerk aufzubauen. An Orten mit kostenlosen öffentlichen Hotspots, etwa Hotels oder Cafés, verbessert der Repeater die WLAN-Abdeckung, ermöglicht mehreren Geräten einen kabelgebundenen oder drahtlosen Zugang und schützt Ihr Netzwerk.



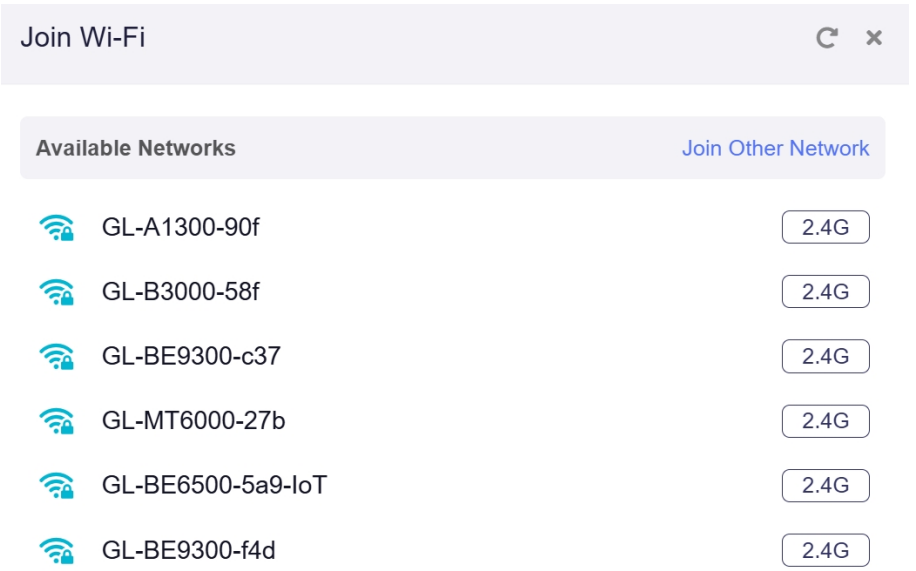
Die Repeater-Funktion von GL.iNet arbeitet standardmäßig im WISP-Modus (Wireless Internet Service Provider). Dabei erstellt der Router ein eigenes Subnetz und schützt Sie durch seine Firewall vor dem öffentlichen Netzwerk.

4.2.1 Grundeinrichtung

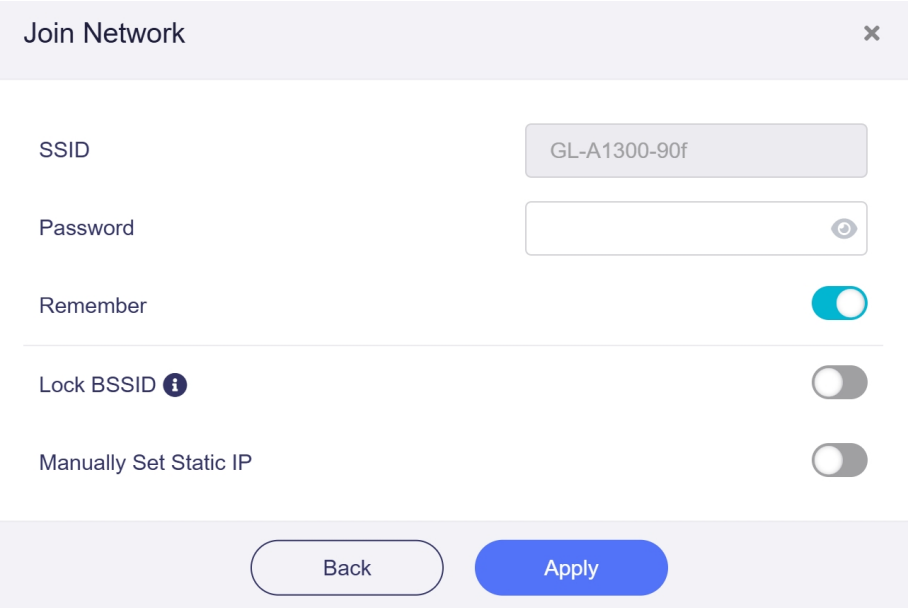
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Repeater**. Klicken Sie auf **Connect**.



2. Wählen Sie im eingeblendeten Fenster das gewünschte WLAN aus der Liste der verfügbaren Netzwerke aus.

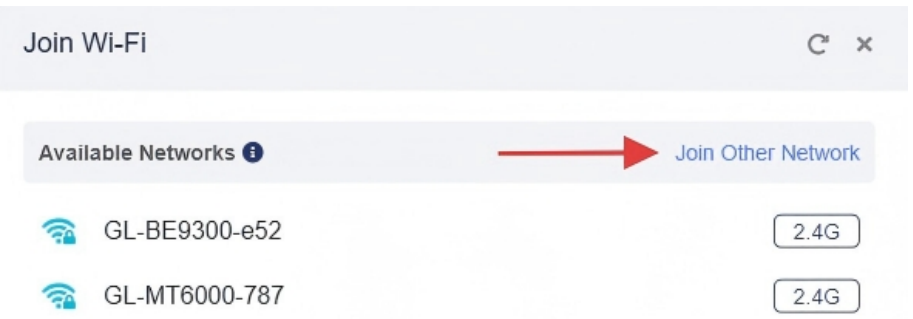


3. Geben Sie das richtige WLAN-Passwort ein und klicken Sie auf **Apply**.

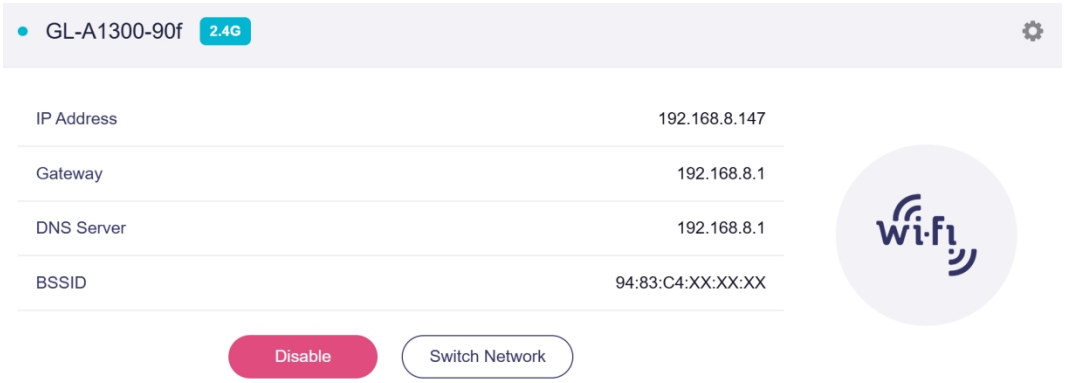


- **Remember**: Aktivieren Sie diese Option, um das aktuell als Repeater genutzte WLAN zu speichern.
- **Lock BSSID**: Wenn diese Option aktiviert ist, verbindet sich der Router ausschließlich mit dem Zugangspunkt (AP) der ausgewählten BSSID, auch wenn andere Zugangspunkte dieselbe SSID verwenden.
- **Manually Set Static IP**: Aktivieren Sie diese Option, um IP-Adresse, Subnetzmaske, Gateway und DNS-Server manuell festzulegen, anstatt die IP-Einstellungen automatisch per DHCP zu beziehen.

4. Falls die gewünschte WLAN-SSID nicht in der Liste verfügbarer Netzwerke erscheint, klicken Sie oben rechts auf **Join Other Network**. Geben Sie die WLAN-SSID und die weiteren erforderlichen Daten manuell ein und klicken Sie auf **Apply**.

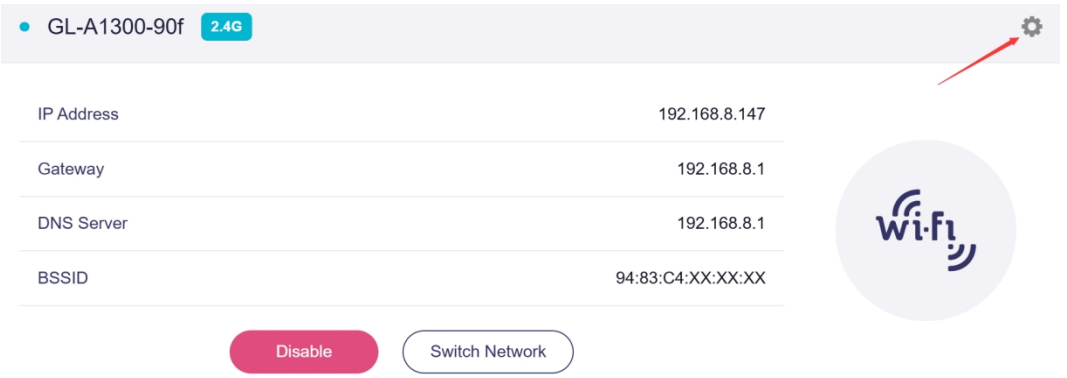


5. Warten Sie etwa eine Minute, bis der Router verbunden ist. Nach erfolgreicher Verbindung erscheint die folgende Ansicht.

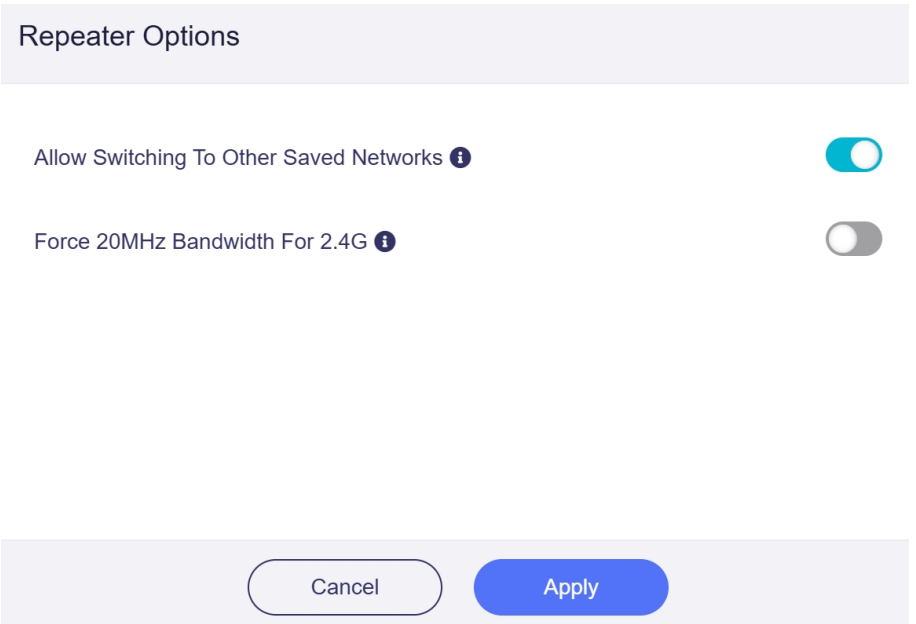

GL-A1300-90f
2.4G
IP Address
192.168.8.147
Gateway
192.168.8.1
DNS Server
192.168.8.1
BSSID
94:83:C4:XX:XX:XX
Disable
Switch Network

4.2.2 Repeater-Optionen

Klicken Sie oben rechts auf das Zahnradsymbol, um die Repeater-Optionen zu konfigurieren.



Die Ansicht kann je nach Firmwareversion abweichen.

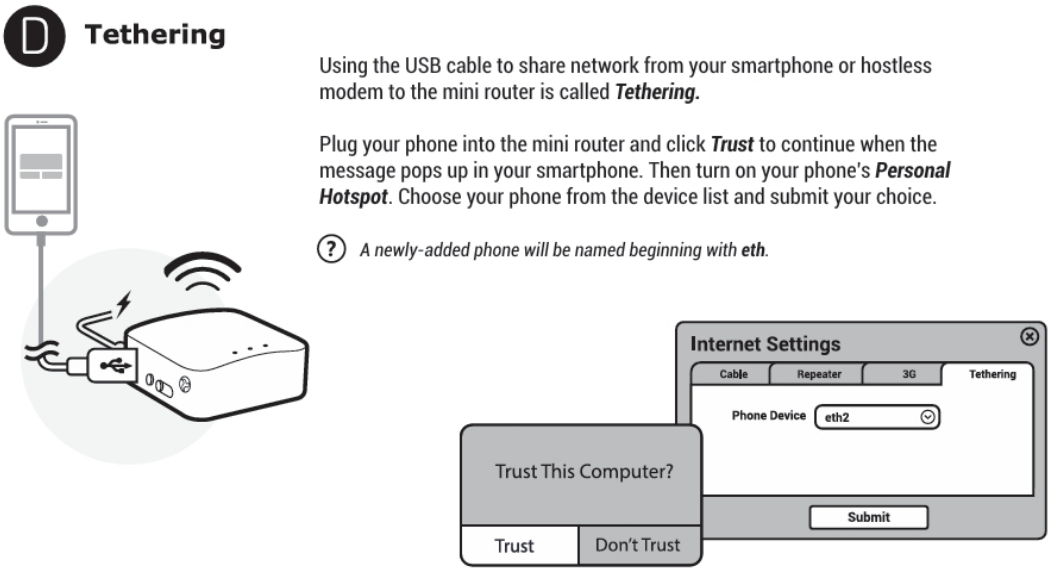


- **Allow Switching to Other Saved Networks**: Wenn diese Option aktiviert ist, verbindet sich der Router automatisch mit anderen gespeicherten Netzwerken, sobald er keine Verbindung zum aktuellen WLAN herstellen kann.
- **Force 20MHz Bandwidth for 2.4G**: Diese Option verbessert die Verbindungsstabilität, indem sie die Übertragungsrate reduziert.

  Hinweis: Dies funktioniert nur bei einer Repeater-Verbindung mit einem 2,4-GHz-WLAN.

4.3 Internetverbindung über USB-Tethering

Wenn ein Smartphone über ein USB-Kabel mit dem Router verbunden wird, um seine mobile Datenverbindung, etwa über 4G/5G, freizugeben, spricht man von Tethering. Dies ist eine praktische Lösung für einen vorübergehenden Internetzugang, besonders unterwegs oder an Orten ohne festen Breitbandanschluss.

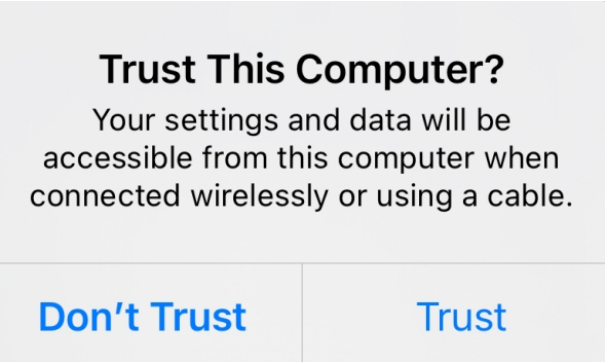


Auch ein Hostless-Modem kann bei seiner Einrichtung über die Tethering-Funktion betrieben werden.

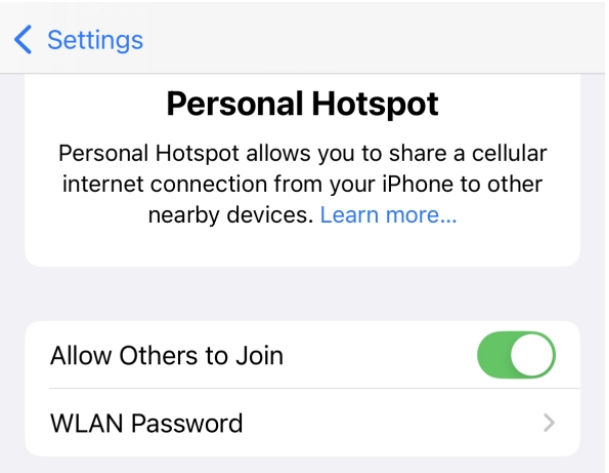
Hinweis: Einige Mobilfunkanbieter beschränken Tethering oder berechnen zusätzliche Gebühren. Erkundigen Sie sich bei Ihrem Anbieter.

4.3.1 Tethering mit einem iPhone

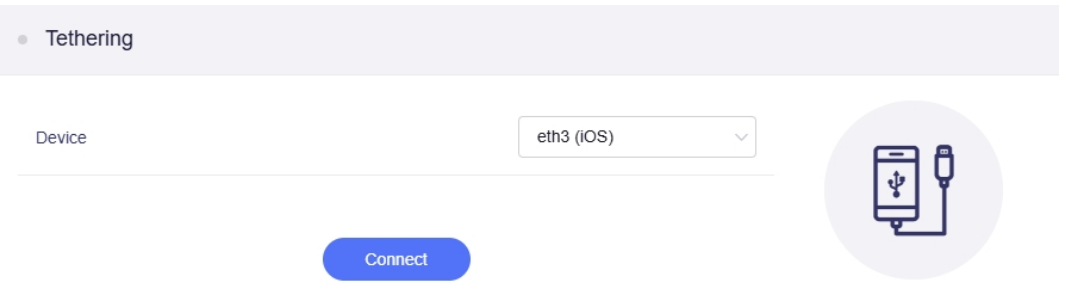
1. Verbinden Sie ein iPhone per USB-Kabel mit dem USB-Anschluss des Routers. Ein Systemdialog fragt, ob Sie diesem Gerät vertrauen. Tippen Sie auf **Vertrauen**, um fortzufahren.



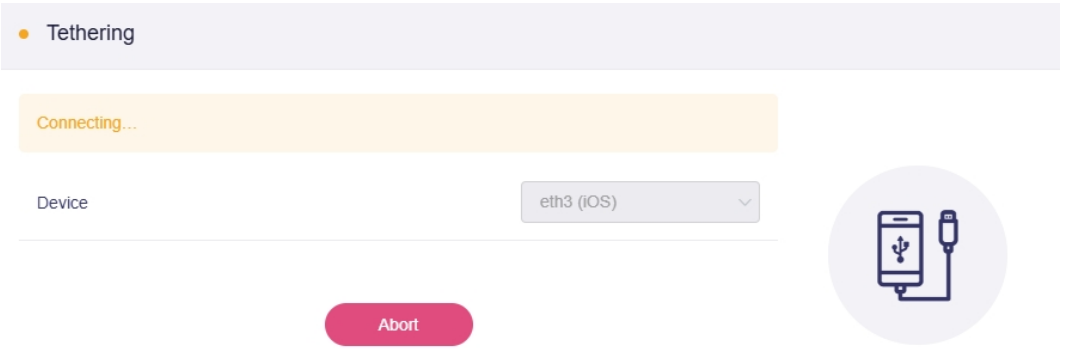
2. Öffnen Sie auf dem iPhone **Einstellungen** > **Persönlicher Hotspot**. Aktivieren Sie **Zugriff für andere erlauben**.



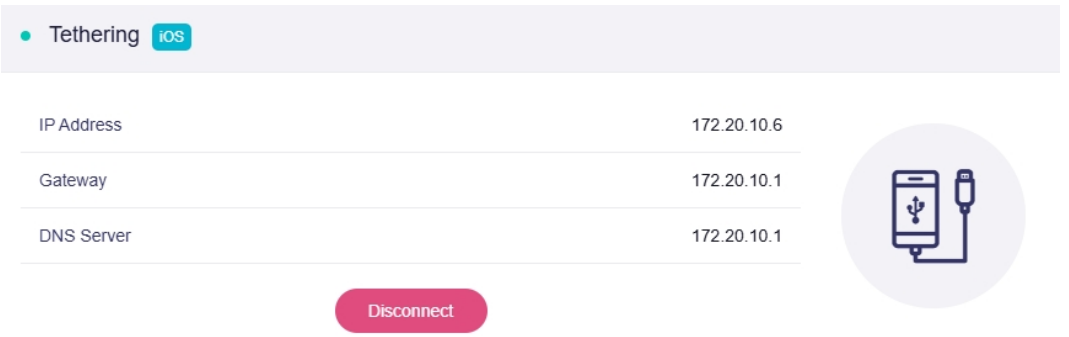
3. Verbinden Sie einen Computer oder ein anderes Smartphone mit dem Router. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie anschließend auf **Connect**.



4. Die Verbindung wird hergestellt.

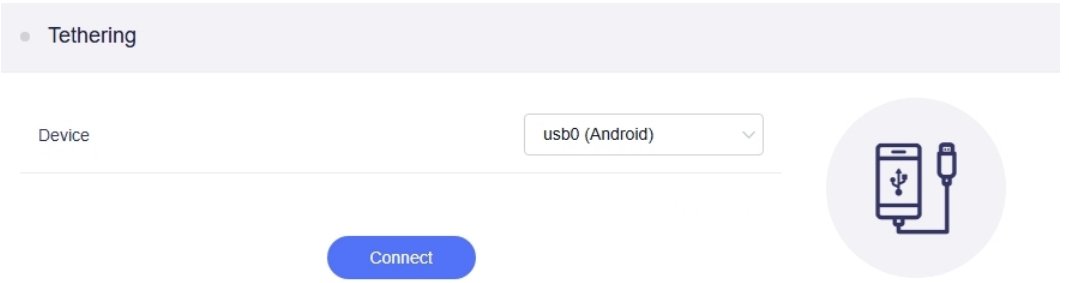


Nach erfolgreicher Verbindung werden auf dieser Seite die Details der Tethering-Verbindung angezeigt.

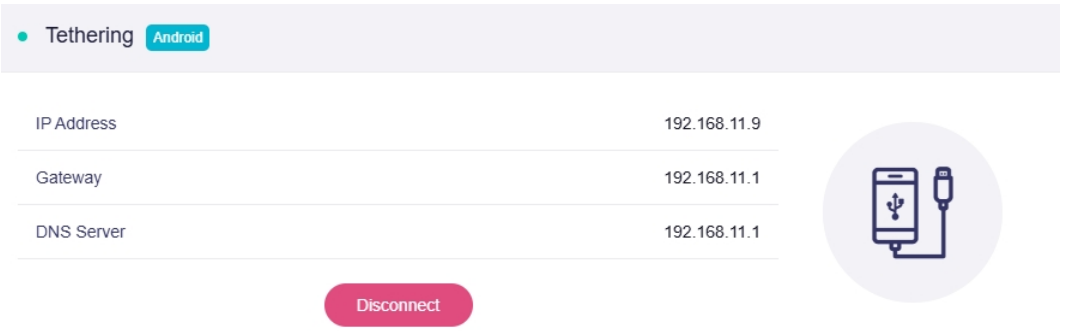


4.3.2 Tethering mit einem Android-Smartphone

1. Verbinden Sie ein Android-Smartphone per USB-Kabel mit dem USB-Anschluss des Routers. Möglicherweise erscheint ein Systemdialog mit USB-Einstellungen. Wählen Sie bei entsprechender Aufforderung **USB-Tethering** oder **Dateiübertragung** aus.
2. Öffnen Sie auf Ihrem Smartphone **Einstellungen** > **Netzwerk & Internet** > **Persönlicher Hotspot**. Aktivieren Sie **Persönlicher Hotspot** oder **USB-Tethering**.
   (Die Schritte zum Aktivieren von USB-Tethering unterscheiden sich je nach Hersteller. Suchen Sie die Funktion in den Einstellungen Ihres Geräts und wenden Sie sich bei Bedarf an den Support des Herstellers.)
3. Verbinden Sie einen Computer oder ein anderes Smartphone mit dem Router. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie auf **Connect**.



4. Nach erfolgreicher Verbindung wird auf dieser Seite der Status der Tethering-Verbindung angezeigt.



4.3.3 Fehlerbehebung

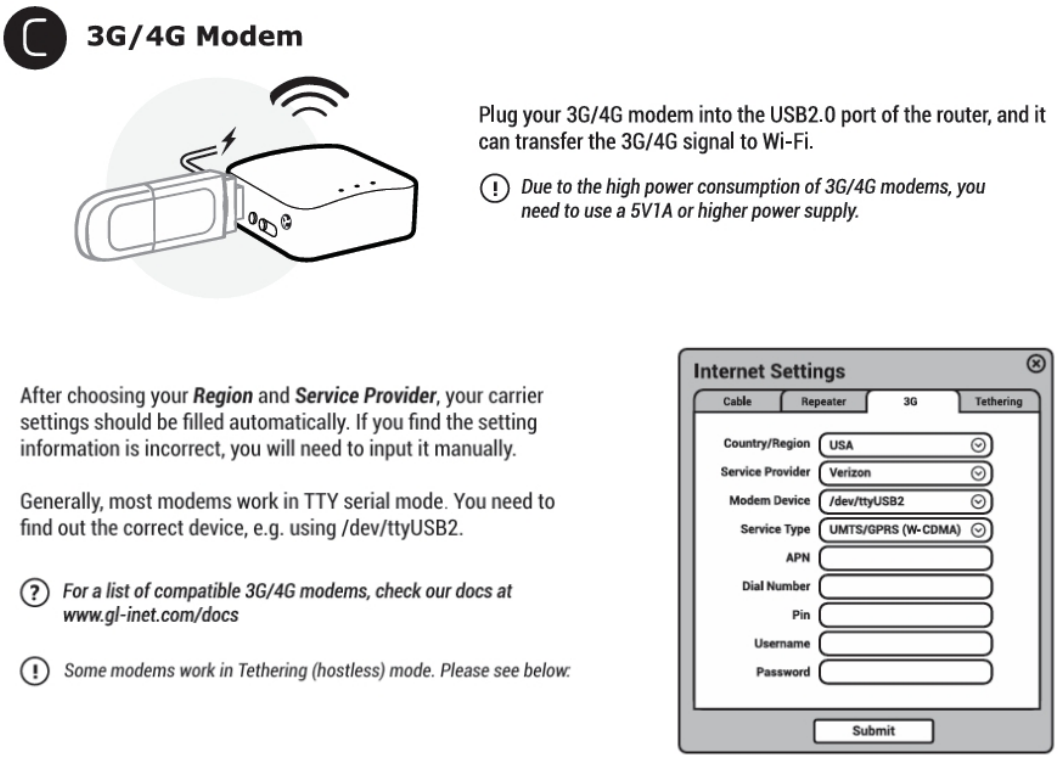
Falls die Tethering-Verbindung fehlschlägt, versuchen Sie Folgendes:

- Verwenden Sie das Originalnetzteil des Routers.
- Ziehen Sie das USB-Kabel ab und schließen Sie es erneut an.
- Verwenden Sie ein anderes USB-Kabel. Achten Sie darauf, dass es Daten übertragen kann und nicht ausschließlich zum Laden geeignet ist.
- Schalten Sie „USB-Tethering“ mehrmals aus und wieder ein (Android).
- Schalten Sie „Zugriff für andere erlauben“ mehrmals aus und wieder ein (iPhone).
- Starten Sie Ihr Smartphone neu und versuchen Sie es erneut.

Falls das Problem weiterhin besteht, wenden Sie sich an unseren technischen Support unter support@gl-inet.com.

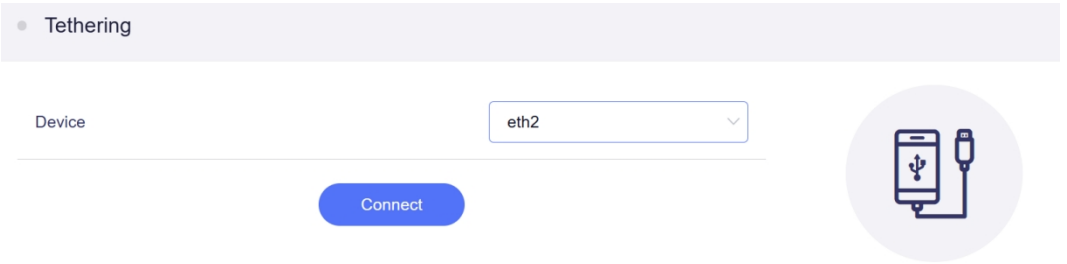
4.4 Internetverbindung über ein USB-Modem

Schließen Sie ein USB-Mobilfunkmodem an den USB-Anschluss des Routers an, um eine Internetverbindung herzustellen. So kann sich der Router über 3G/4G-Netze mit dem Internet verbinden, unabhängig von einem festen Breitbandanschluss. Diese Lösung eignet sich für den Einsatz im Fahrzeug oder im Freien. Die Verbindung wird über die Schnittstelle Tethering oder Cellular des Routers eingerichtet.

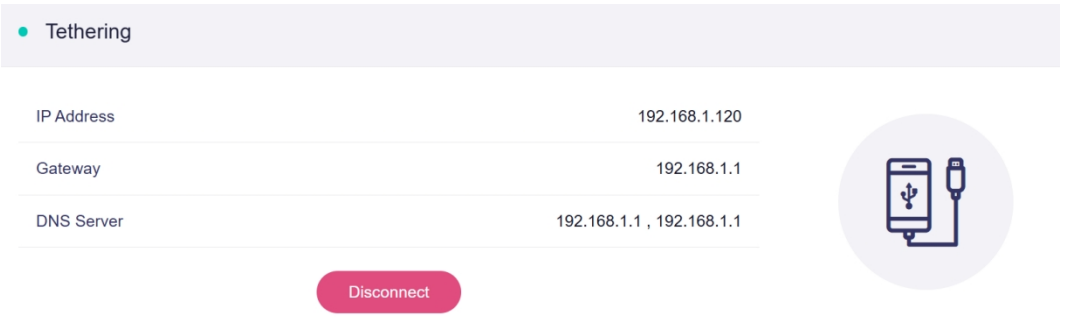


Gehen Sie wie folgt vor, um Ihren Router über ein USB-Modem mit dem Internet zu verbinden.

1. Stecken Sie vor dem Einschalten ein USB-Modem mit eingesetzter SIM-Karte in den USB-Anschluss des Routers.
2. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie auf **Connect**.



3. Die Verbindung wird hergestellt. Nach erfolgreicher Verbindung werden auf dieser Seite die Netzwerkdaten angezeigt.



Tipp: Nach der Ersteinrichtung erkennt der Router das USB-Modem automatisch wieder, wenn Sie ihn mit angeschlossenem Modem neu starten oder das Modem erneut einstecken. Die Netzwerkverbindung wird dann hergestellt, ohne dass Sie erneut auf „Connect“ klicken müssen.

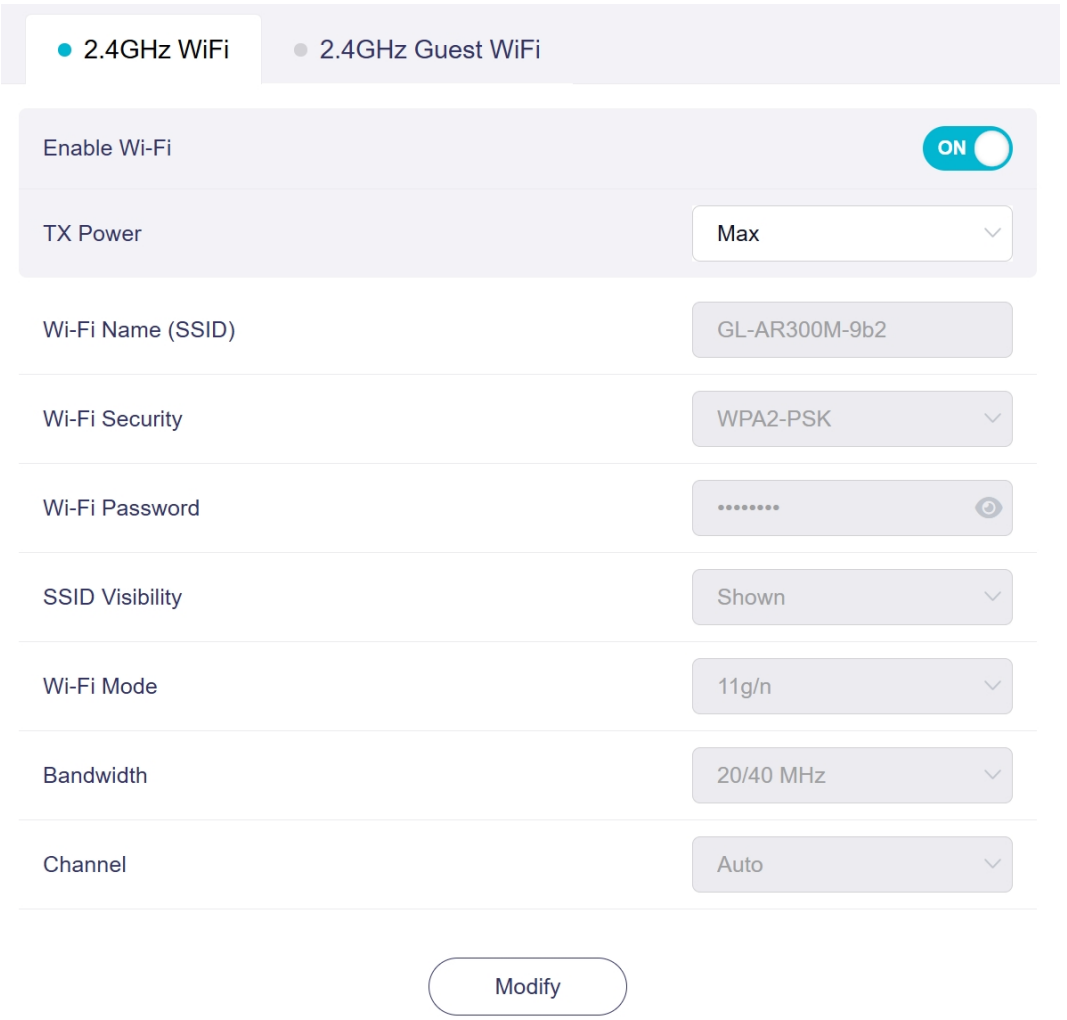
Kapitel 5

WLAN

Dieses Kapitel beschreibt, wie Sie den WLAN-Status prüfen und die WLAN-Einstellungen konfigurieren.

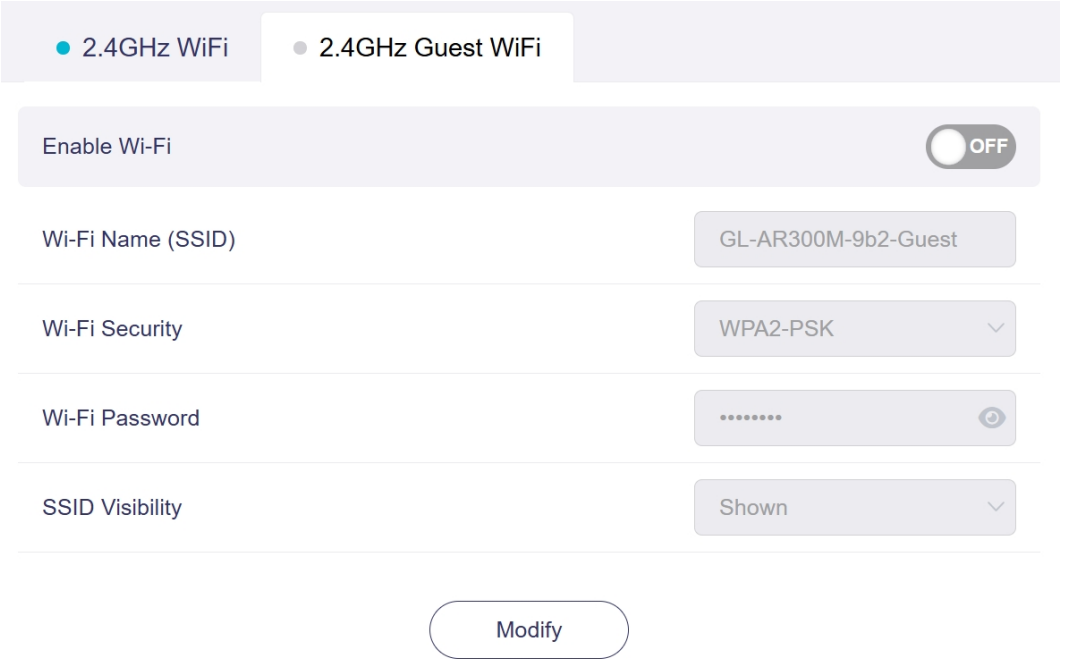
Melden Sie sich an der Weboberfläche an und öffnen Sie **WIRELESS**.
Die WLAN-Seite zeigt die Einstellungen für das 2,4-GHz-WLAN. Dieses ist für eine flexible Verwaltung in ein Haupt- und ein Gastnetzwerk unterteilt.

Für das 2,4-GHz-Hauptnetzwerk können Sie das WLAN ein- und ausschalten sowie Sendeleistung, WLAN-Namen (SSID), Sicherheitsverfahren, Passwort, Sichtbarkeit der SSID, Modus, Bandbreite und Kanal festlegen.



Hinweis: Die Einstellungen **Bandwidth** und **Channel** lassen sich nicht ändern, wenn der Router als Repeater eingerichtet ist, da sie vom übergeordneten WLAN übernommen werden.

Für das 2,4-GHz-Gastnetzwerk stehen vereinfachte Einstellungen zur Verfügung: WLAN ein- oder ausschalten sowie WLAN-Name (SSID), Sicherheitsverfahren, Passwort und Sichtbarkeit der SSID festlegen.


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
OFF
Wi-Fi Name (SSID)
GL-AR300M-9b2-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
••••••••
SSID Visibility
Shown
Modify

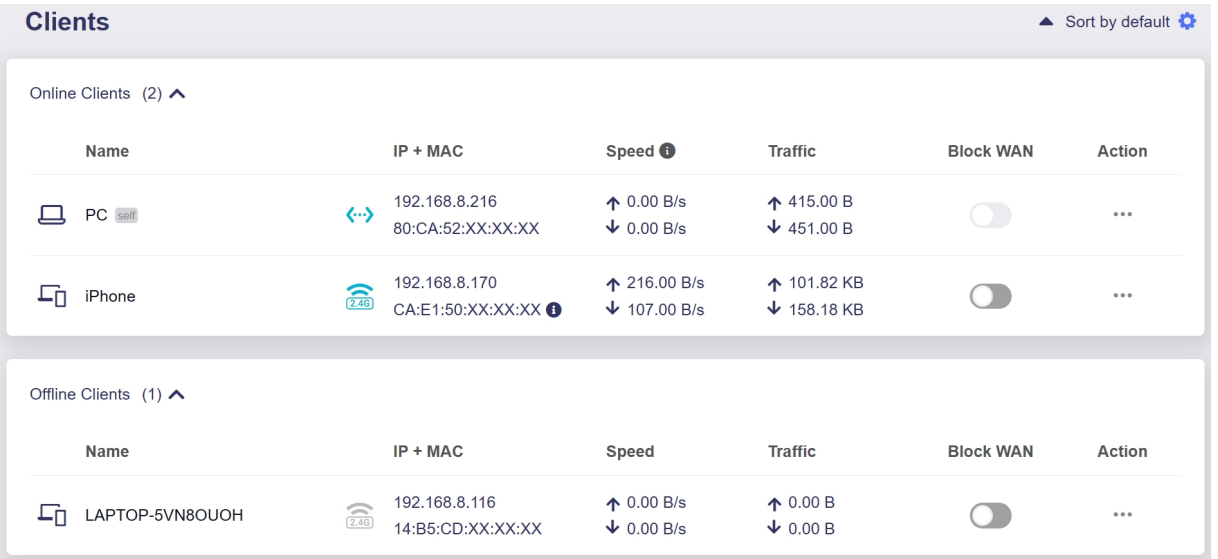
Kapitel 6

Verbundene Geräte

Dieses Kapitel beschreibt, wie Sie Details zu verbundenen Geräten anzeigen und deren Verbindungen verwalten.

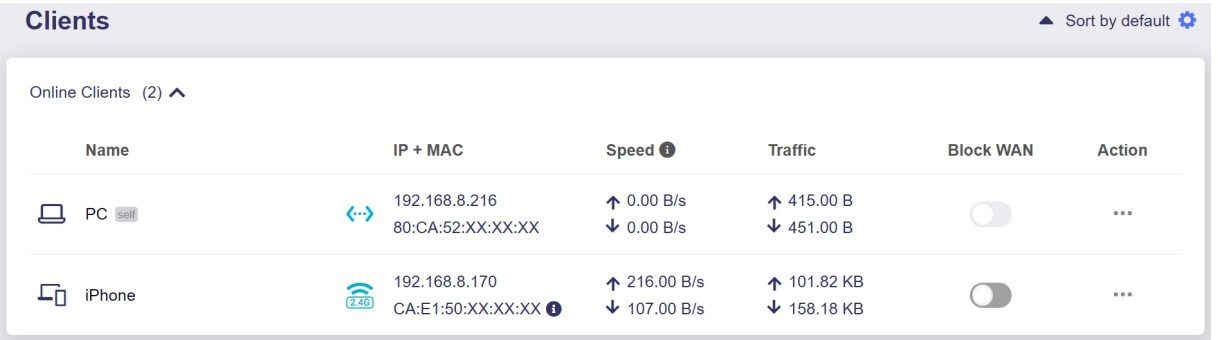
Melden Sie sich an der Weboberfläche an und öffnen Sie **CLIENTS**.

Die Seite Clients zeigt von links nach rechts Gerätename, Verbindungsart, IP- und MAC-Adresse, Geschwindigkeit und Datenverkehr der verbundenen Geräte an. Außerdem können Sie dort schnell IP-Adressen reservieren, Geräte sperren und weitere Aktionen ausführen.



- **Online Clients**: Geräte, die derzeit mit dem Netzwerk des Routers verbunden sind.
- **Offline Clients**: Geräte, die bereits mit dem Router verbunden waren, derzeit jedoch keine Netzwerkverbindung haben.

6.1 Gerätedetails



1. **Gerätename**

   Die erste Spalte zeigt den Namen und den Typ des Geräts an. Der Name richtet sich nach dem auf dem Gerät festgelegten Hostnamen. Das blaue Symbol neben dem Gerätenamen kennzeichnet die Verbindungsart und zeigt an, dass das Gerät über ein Ethernetkabel mit dem Router verbunden ist.

2. **IP- und MAC-Adresse**

   Die zweite Spalte zeigt die IP- und MAC-Adresse des verbundenen Geräts an. Verwendet ein Gerät eine zufällige MAC-Adresse, erscheint ein entsprechender Hinweis.



   Ist das zweite Zeichen der MAC-Adresse 2, 6, A oder E (unabhängig von Groß- und Kleinschreibung), wird sie als zufällige MAC-Adresse erkannt. Manche Geräte erzeugen zufällige MAC-Adressen jedoch nach anderen Regeln, sodass diese Erkennung nicht immer zuverlässig ist.

3. **Geschwindigkeit**

   Die dritte Spalte zeigt die durchschnittliche Internetgeschwindigkeit des Geräts während der letzten drei Minuten. Die Berechnung beginnt beim Öffnen dieser Seite. Ist die Seite beispielsweise erst seit zehn Sekunden geöffnet, basiert der Durchschnitt nur auf den Daten dieser zehn Sekunden.

4. **Datenverkehr**: Die vierte Spalte zeigt das übertragene Internetdatenvolumen des Geräts an.

5. **Sperrliste**

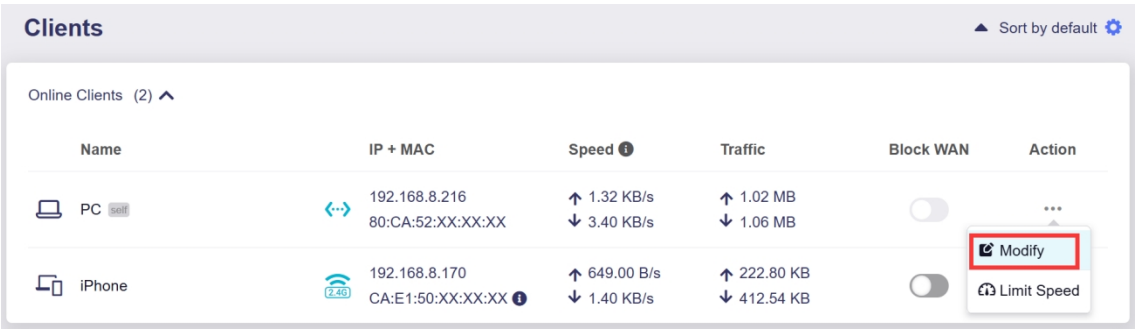
   In der fünften Spalte können Sie einzelne Geräte mit einem Klick sperren. Geräte mit MAC-Adressen auf der Sperrliste dürfen sich dann nicht mehr mit dem Router verbinden.

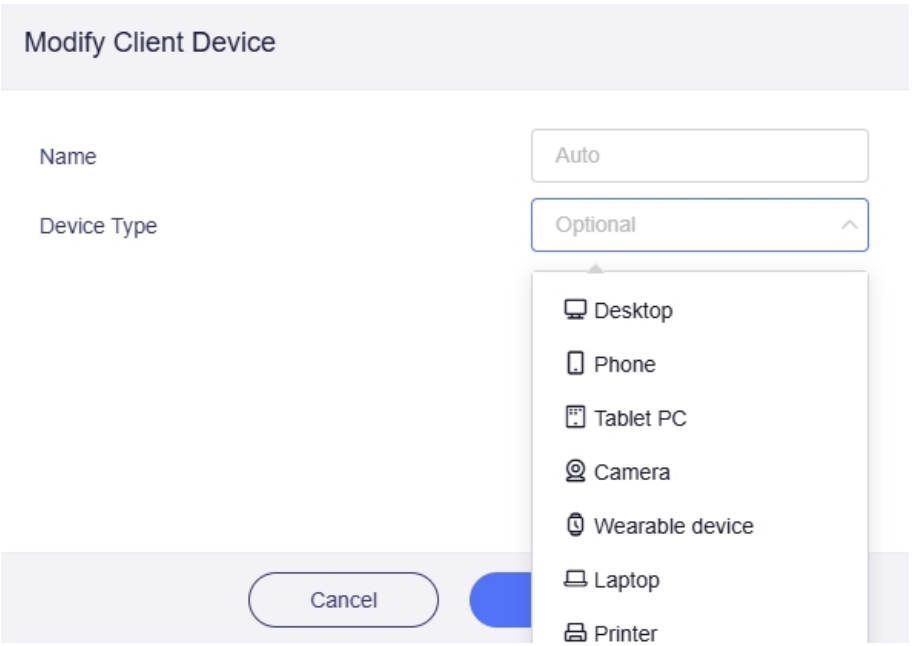
Die Sperre basiert auf der MAC-Adresse: Verwendet das gesperrte Gerät beim nächsten Mal eine andere Adresse, kann es sich weiterhin verbinden.

6.2 Aktionen

1. **Gerät bearbeiten**

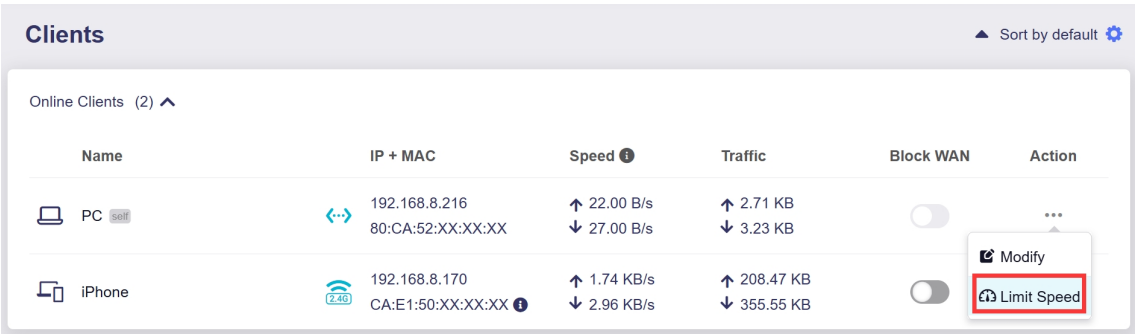
   Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Modify**, um den Gerätenamen und -typ zu ändern.



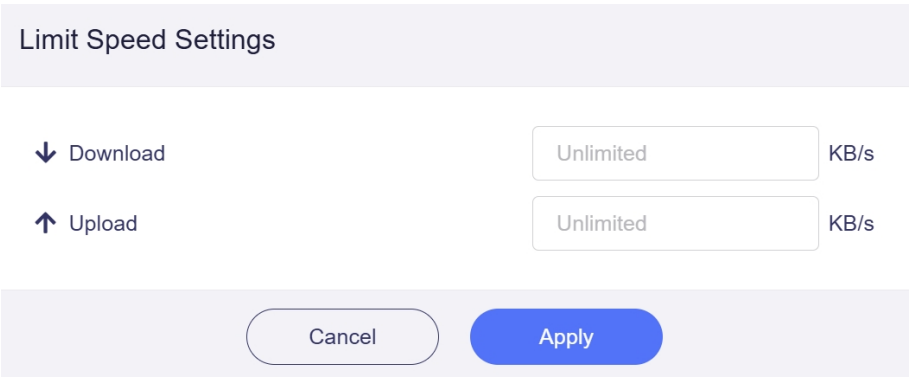


2. **Geschwindigkeit begrenzen**

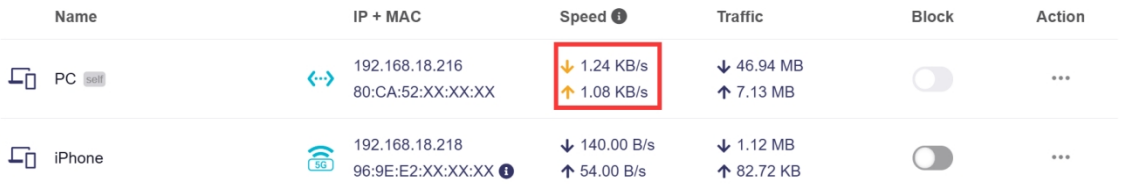
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Limit Speed**.



Sie können die Geschwindigkeit eines verbundenen Geräts in KB/s begrenzen.

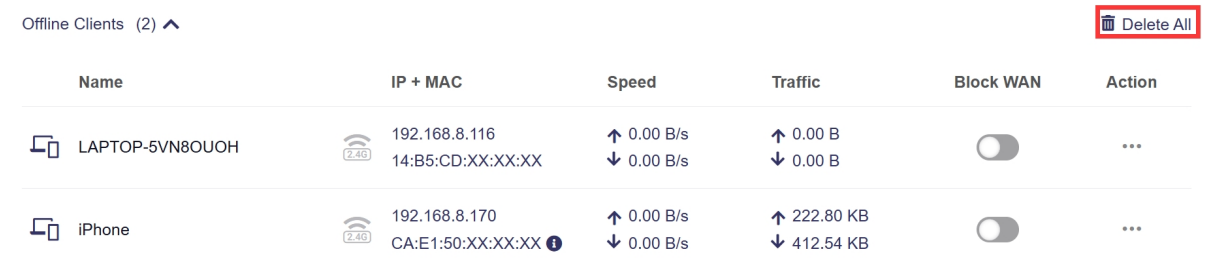


Bei Geräten mit aktivierter Geschwindigkeitsbegrenzung werden die Pfeile für die Upload- und Downloadgeschwindigkeit gelb angezeigt.

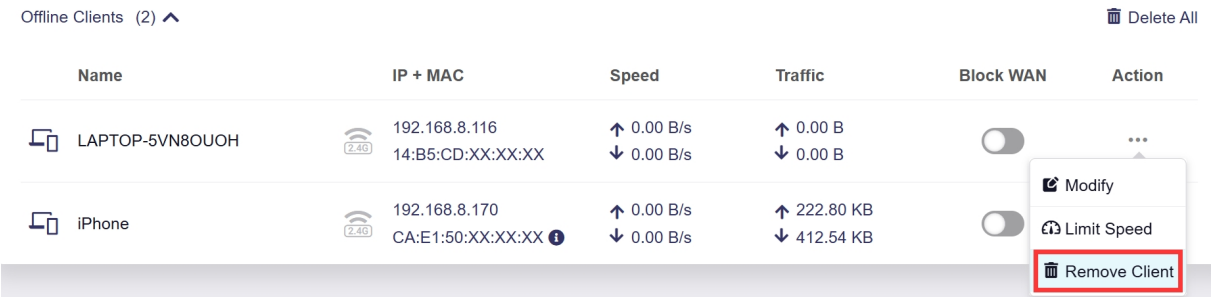


6.3 Geräte entfernen

Klicken Sie im Abschnitt **Offline Clients** oben rechts auf **Delete All**, um alle nicht verbundenen Geräte zu löschen.

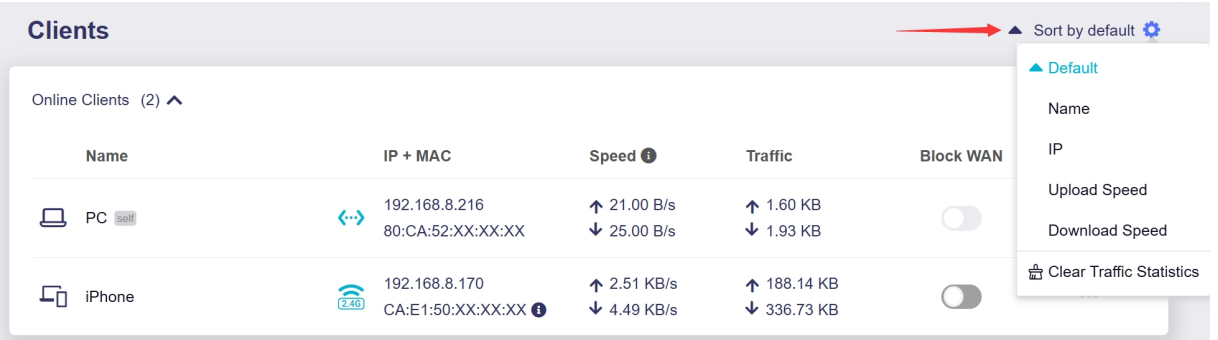


Um ein einzelnes Gerät zu entfernen, klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Remove Client**.



6.4 Sortierung

Oben rechts auf der Seite Clients können Sie festlegen, wie die Geräte sortiert werden.



Standardmäßig gilt folgende Reihenfolge:

- Das Gerät, mit dem Sie auf die Weboberfläche des Routers zugreifen, steht immer an erster Stelle.
- Unter **Online Clients** stehen Geräte weiter oben, wenn sie früher verbunden wurden.
- Unter **Offline Clients** stehen Geräte weiter oben, wenn ihre Verbindung früher getrennt wurde.

Neben der Sortierung bietet das Auswahlmenü die Funktion **Clear Traffic Statistics**. Diese setzt die Datenverkehrsstatistiken aller verbundenen Geräte mit einem Klick auf null zurück. Anschließend werden die Daten erneut erfasst.



Kapitel 7

VPN kennenlernen

Dieses Kapitel erläutert die Grundlagen von VPN und typische Einsatzmöglichkeiten.

7.1 Einführung

VPN

Ein VPN (Virtual Private Network, virtuelles privates Netzwerk) baut einen verschlüsselten, privaten Tunnel zwischen einem Gerät und einem entfernten Server auf. Es schützt die Datenübertragung und ermöglicht den sicheren Zugriff auf private oder zugangsbeschränkte Netzwerke.

VPN-Router

Ein VPN-Router verfügt über integrierte VPN-Funktionen und schützt alle verbundenen Geräte über das VPN. Wenn Sie den Router als VPN-Client einrichten, wird der gesamte Datenverkehr durch einen verschlüsselten Tunnel geleitet. Eine separate Einrichtung auf jedem Gerät ist dann nicht erforderlich. So schützen Sie mehrere Geräte gleichzeitig, sparen Zeit und gewährleisten einheitliche VPN-Einstellungen. Risiken durch fehlerhafte Einzelkonfigurationen werden verringert.

GL.iNet-Router unterstützen mehr als 30 gängige kommerzielle OpenVPN- und WireGuard-VPN-Dienste. Laden Sie Ihre VPN-Konfigurationsdateien hoch, um die VPN-Verbindung für einen sicheren Netzwerkzugang zu aktivieren. Die vollständige Liste unterstützter VPN-Drittanbieter finden Sie hier.

OpenVPN

OpenVPN ist ein quelloffenes VPN-Protokoll, das SSL/TLS für sichere Verbindungen zwischen einzelnen Geräten und Netzwerken oder zwischen zwei Standorten nutzt. Es unterstützt verschiedene Verschlüsselungsverfahren sowie TCP/UDP und lässt sich einfach durch Firewalls und NAT betreiben.

WireGuard

WireGuard ist ein schlankes, schnelles VPN-Protokoll, das einfacher und effizienter als OpenVPN ist. Es nutzt moderne Kryptografie und eine kleine, leicht überprüfbare Codebasis. Aktuelle Verfahren wie ChaCha20 und Poly1305 sorgen für Verschlüsselung und Datenintegrität.

7.2 Einsatzmöglichkeiten

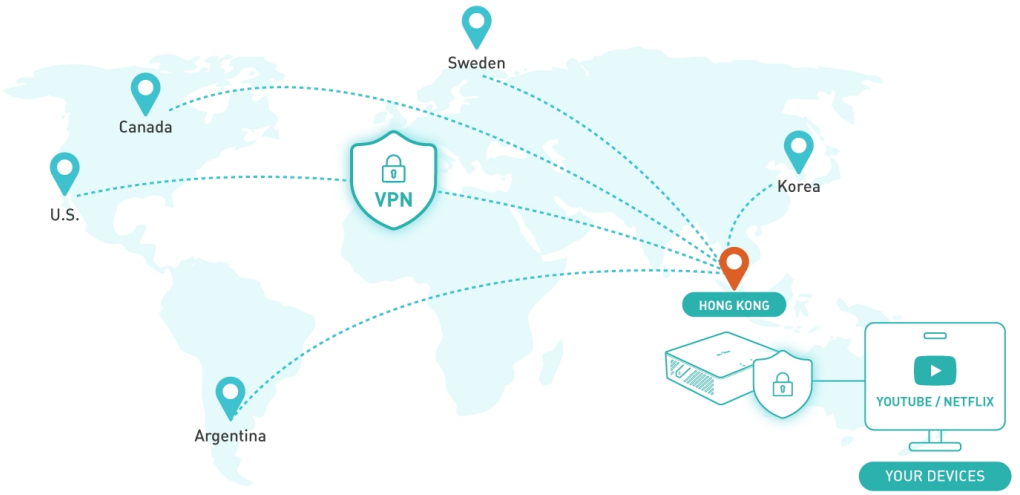
1. **Schutz persönlicher Daten**

   Über unseren Router lässt sich der VPN-Dienst mit vielen Geräten nutzen: neben Laptops, Smartphones und Tablets auch mit Spielkonsolen, Fernsehern und Streaminggeräten. Ihre Daten werden sowohl bei drahtlosen als auch bei kabelgebundenen Verbindungen geschützt. Mit individuellen VPN-Regeln können Sie den Schutz gezielt auf bestimmte Geräte abstimmen.



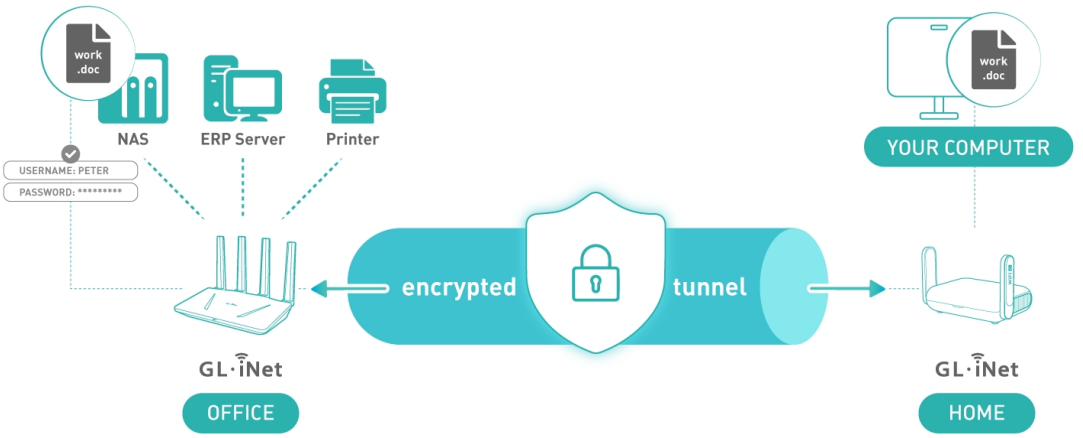
2. **Weltweiter Zugriff ohne Einschränkungen**

   Der Zugriff auf manche Webseiten ist regional eingeschränkt. Mit einem VPN können Sie solche Einschränkungen bei Bedarf umgehen. Durch die Verbindung mit unterschiedlichen Servern eines Drittanbieters erhalten Sie andere IP-Adressen zum Surfen und zum Zugriff auf regional gesperrte Inhalte.


Sweden
Canada
U.S.
VPN
Korea
HONG KONG
Argentina
YOUTUBE / NETFLIX
YOUR DEVICES

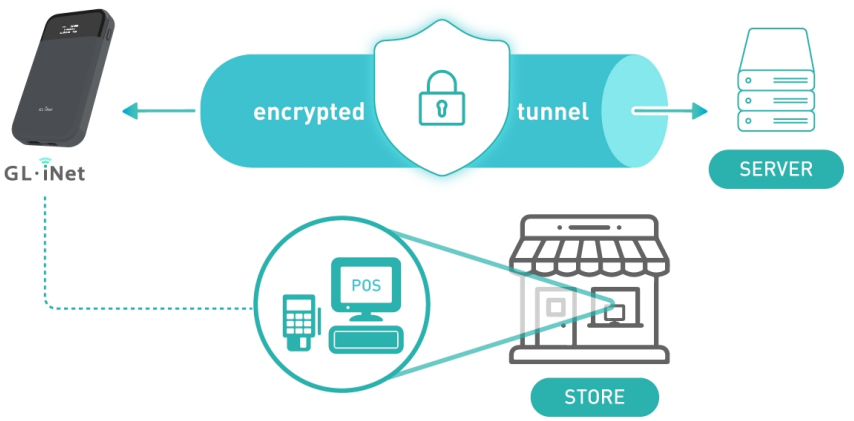
3. **Datensicherheit für kleine Unternehmen**

Viele Menschen arbeiten in Coworking-Spaces oder Cafés und nutzen kostenloses öffentliches WLAN. Solche Netzwerke sind anfällig für Angriffe durch Cyberkriminelle. Wenn Sie Ihren Reiserouter als VPN-Client einrichten, können Sie überall sicher arbeiten.



4. **Sichere Zahlungsabwicklung**

Kleine Einzelhändler verarbeiten bei Zahlungen vor Ort die Zahlungsdaten ihrer Kunden. Mit einem VPN-Router können Kassenterminals Kreditkarteninformationen durch einen verschlüsselten VPN-Tunnel übertragen und so die Sicherheit des Zahlungsvorgangs gewährleisten.



Kapitel 8

VPN-Dashboard

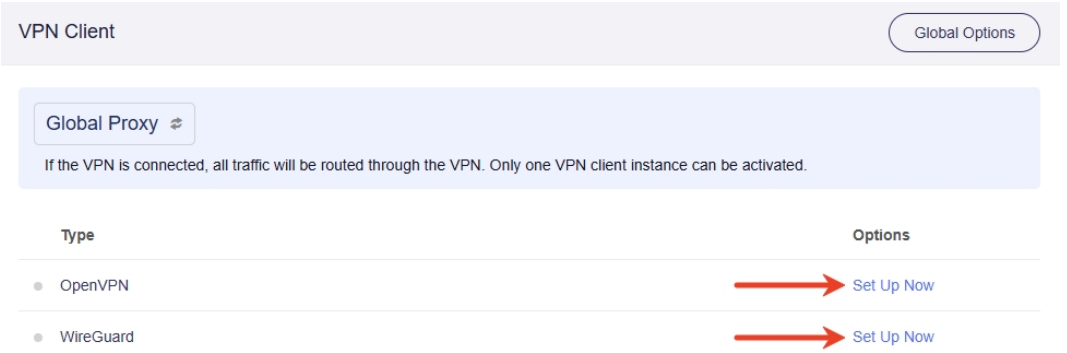
Dieses Kapitel beschreibt die Verwaltung von VPN-Verbindungen über die Weboberfläche.

Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **VPN Dashboard**.

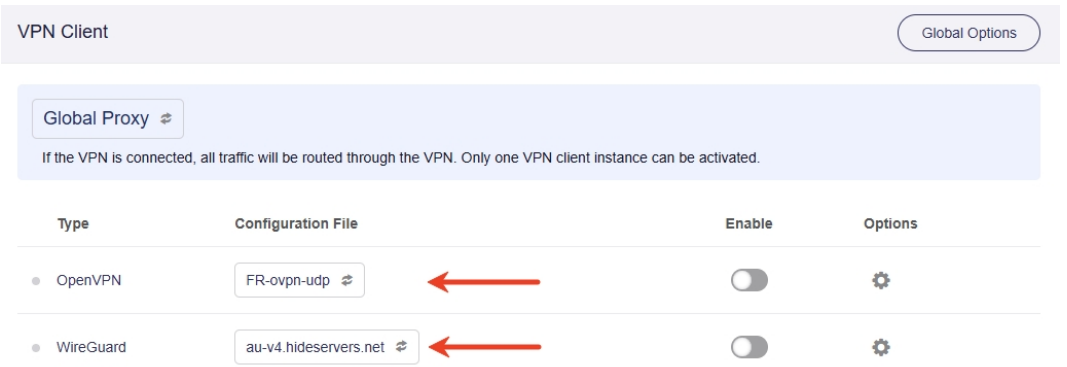
Wenn der Router als aktiver VPN-Client eingerichtet ist, zeigt das VPN-Dashboard Verbindungsdetails wie Serveradresse, Datenverkehrsstatistik, virtuelle Client-IP-Adresse und Verbindungsprotokoll an. Sie können außerdem erweiterte Optionen wie Block non-VPN traffic, Allow Access WAN und Services from GL.iNet Use VPN konfigurieren.

8.1 VPN-Client

Wenn Sie das **VPN Dashboard** zum ersten Mal öffnen und noch keine OpenVPN- oder WireGuard-Konfigurationsdateien vorhanden sind, erscheint die folgende Ansicht. Klicken Sie auf **Set Up Now**, um zur Seite **OpenVPN Client** oder **WireGuard Client** zu gelangen und Ihre VPN-Konfigurationsdateien hochzuladen.

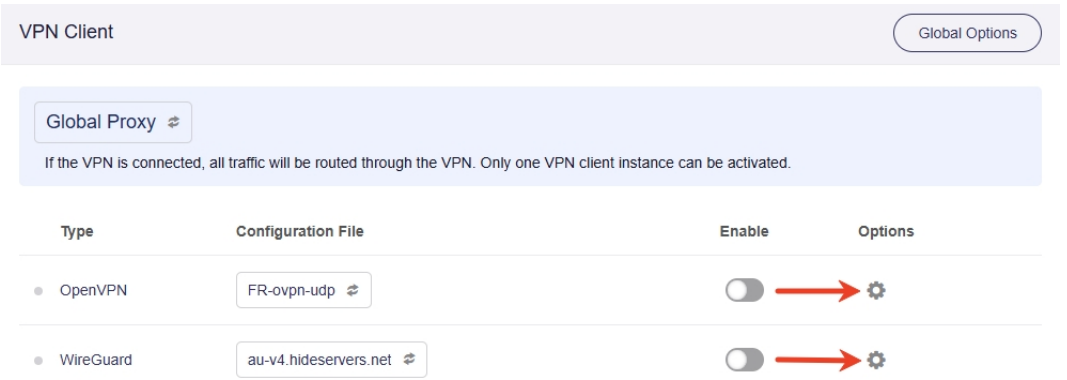


Nach dem Hochladen wird Ihre Konfiguration in der Spalte **Configuration File** angezeigt. Wenn mehrere Konfigurationsdateien vorhanden sind, können Sie über das Auswahlfeld zwischen ihnen wechseln.

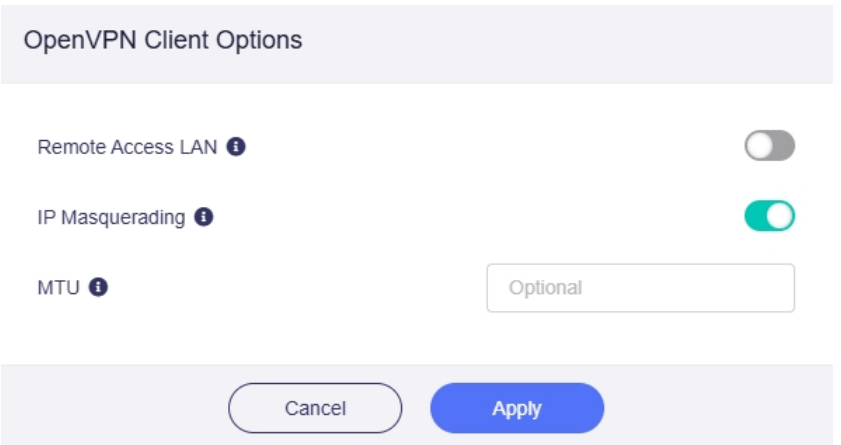


8.1.1 Client-Optionen

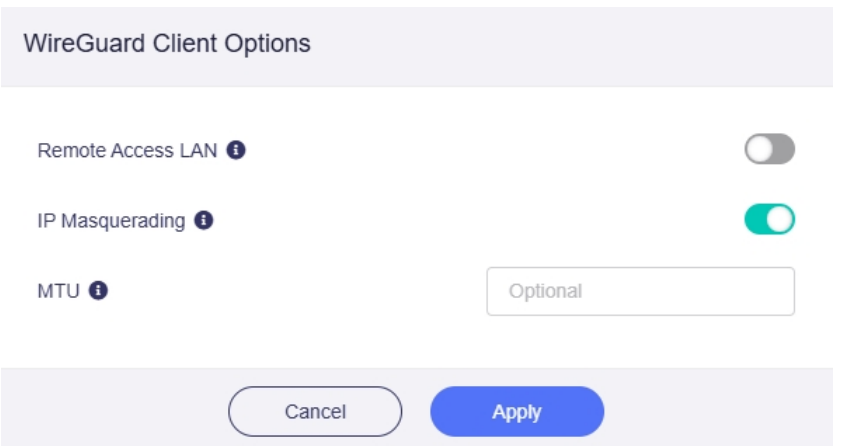
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Clients zu öffnen.



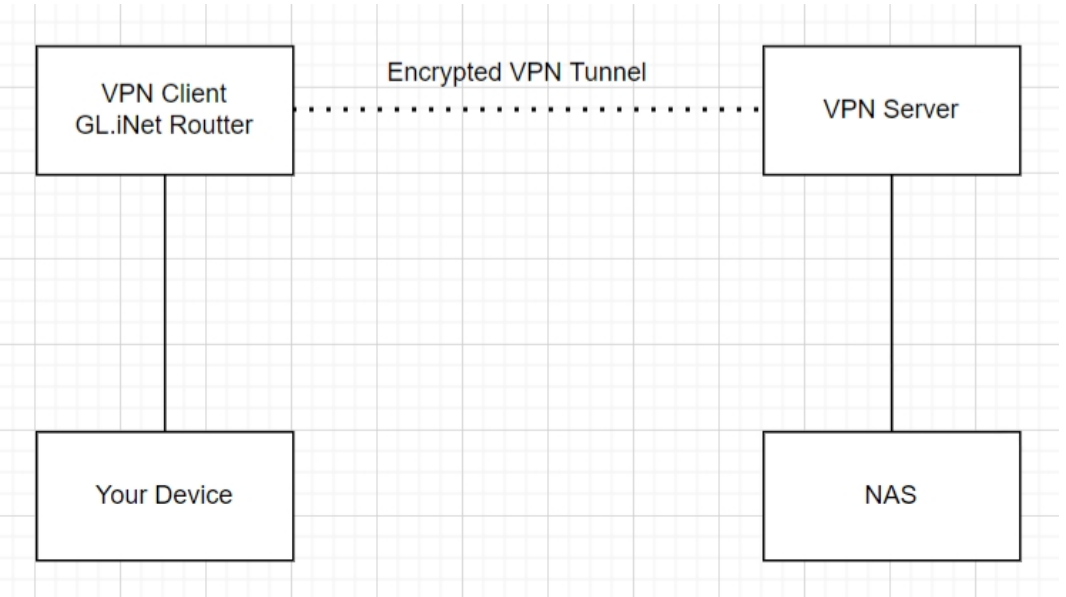
Die Optionen des OpenVPN-Clients werden wie folgt angezeigt.



Die Optionen des WireGuard-Clients werden wie folgt angezeigt.



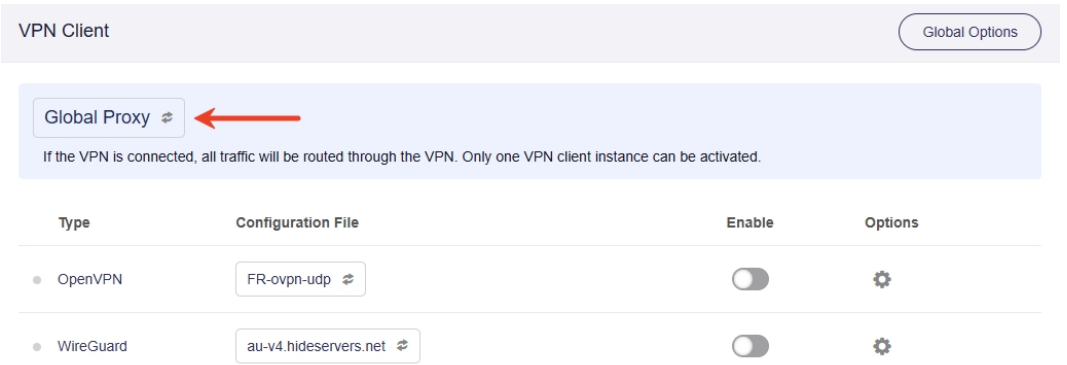
- **Remote Access LAN**: Erlaubt den Fernzugriff über VPN auf diesen Router und seine LAN-Geräte. Der VPN-Server muss eine Route zum LAN-Subnetz dieses Routers bekannt geben.
  Im folgenden Beispiel arbeitet der GL.iNet-Router als VPN-Client und ist über einen VPN-Tunnel mit einem VPN-Server verbunden. Wenn diese Option aktiviert ist, können Geräte auf der VPN-Serverseite, etwa ein NAS, auf den GL.iNet-Router und seine LAN-Geräte zugreifen. Dazu müssen Sie auf dem VPN-Server eine Routingregel zum LAN-Subnetz des GL.iNet-Routers hinzufügen.



- **IP Masquerading**: Ersetzt die Quell-IP-Adressen der LAN-Geräte durch die VPN-Tunnel-IP-Adresse des Routers. Deaktivieren Sie diese Option nur bei Standortvernetzungen, bei denen die Gegenstelle Ihre LAN-Subnetze kennt.
- **MTU**: Steht für Maximum Transmission Unit, die maximale Paketgröße. Mit dieser optionalen Einstellung legen Sie die MTU des VPN-Tunnels individuell fest und überschreiben den Wert aus der Konfigurationsdatei.

8.1.2 Richtlinienmodus

Der voreingestellte Proxy-Modus für VPN-Verbindungen ist **Global Proxy**. Über das Auswahlfeld oben rechts können Sie zu einem anderen Modus wechseln.



Es stehen drei Proxy-Modi zur Verfügung: Global Proxy, Policy Mode und Route Mode.

1. **Globaler Proxy**

   In diesem Modus wird der gesamte Datenverkehr durch das VPN geleitet. Es kann nur eine VPN-Client-Instanz aktiviert werden.

2. **Richtlinienmodus**

   Dieser Modus bietet drei Arten von Richtlinien.

   - **Nach Zieldomain oder Ziel-IP-Adresse.**

     In diesem Modus wird nur der Datenverkehr bestimmter Webseiten durch das VPN geleitet. Die Webseiten werden anhand ihrer IP-Adresse oder ihres Domainnamens festgelegt. Es kann nur eine VPN-Client-Instanz aktiviert werden.

   - **Nach Endgerät.**

     In diesem Modus wird nur der Datenverkehr bestimmter LAN-Geräte durch das VPN geleitet. Die Geräte werden anhand ihrer MAC-Adresse festgelegt. Es kann nur eine VPN-Client-Instanz aktiviert werden.

   - **Nach VLAN**.

     In diesem Modus wird nur der Datenverkehr eines bestimmten VLANs durch das VPN geleitet. Es kann nur eine VPN-Client-Instanz aktiviert werden.

3. **Routenmodus**

   - **Automatische Erkennung**

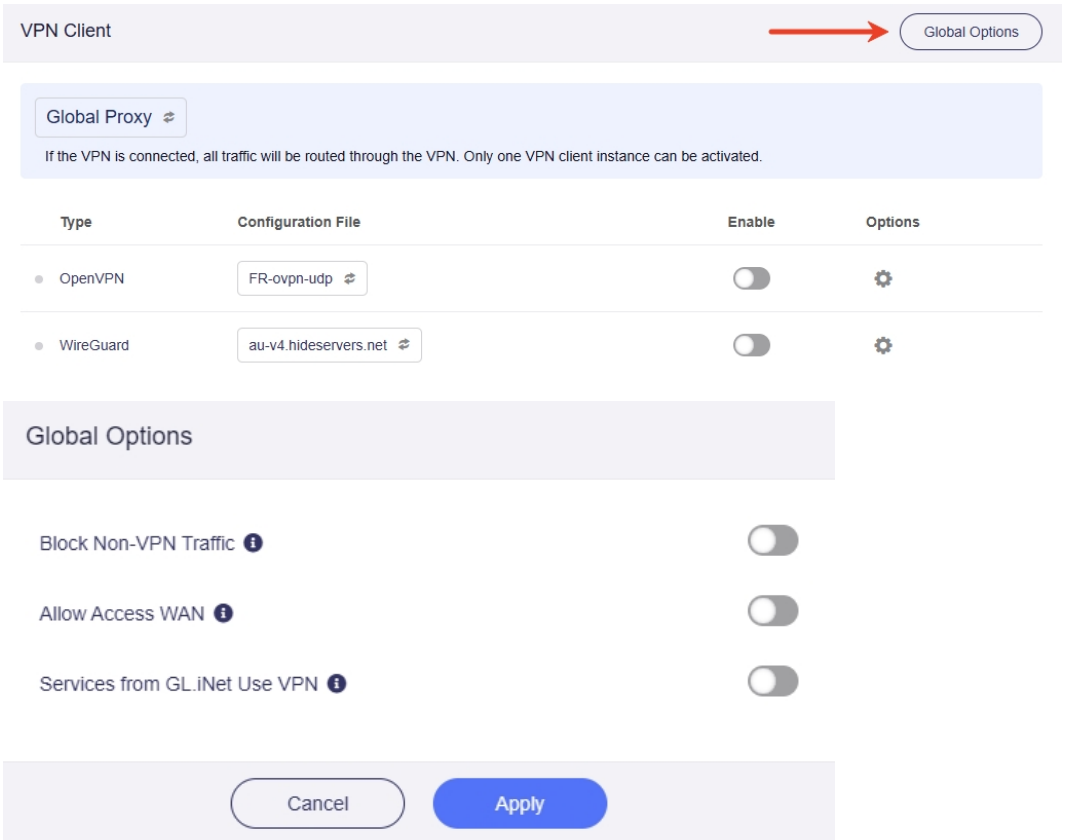
     Verwendet die Routingregeln aus der jeweiligen VPN-Client-Konfigurationsdatei oder die vom VPN-Server übermittelten Regeln.

   - **Eigene Routingregeln**

     Sie können die Routingregeln für jede VPN-Client-Instanz manuell festlegen.

8.1.3 Globale Optionen

Klicken Sie oben rechts auf **Global Options**, um die erweiterten Einstellungen Ihres VPN-Clients zu konfigurieren.



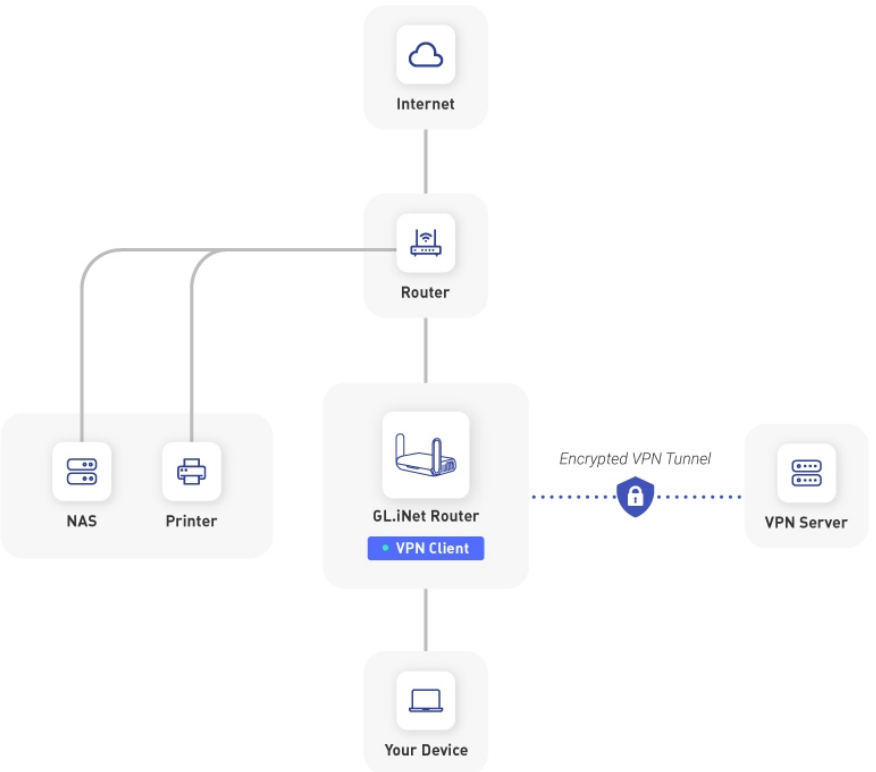
- **Block Non-VPN Traffic**: Erzwingt, dass sämtlicher Internetdatenverkehr ausschließlich durch den VPN-Tunnel geleitet wird. Andere Schnittstellen wie die WAN-Verbindung zum lokalen Internetanbieter können nicht verwendet werden. Bei einem unerwarteten Abbruch der VPN-Verbindung wird der gesamte Internetdatenverkehr gesperrt, damit er nicht auf die reguläre WAN-Verbindung ausweicht. Dies verhindert Datenlecks durch VPN-Ausfälle, falsche DNS-Einstellungen auf Endgeräten und ähnliche Probleme.

  Diese Funktion wird auch als VPN-Kill-Switch bezeichnet und verhindert, dass Nutzerdaten ungeschützt ins Internet gelangen. Ein typischer Kill-Switch unterbricht den Internetzugang automatisch, wenn die VPN-Verbindung ausfällt. Die Funktion Block Non-VPN Traffic auf GL.iNet-Routern bietet einen umfassenderen Schutz und deckt folgende Fälle ab:

  a. DNS-Lecks
  b. IPv6-Lecks

c. WebRTC-Lecks
d. Abbruch der VPN-Verbindung
e. Vor dem VPN-Verbindungsaufbau gestartete Anwendungen
f. Datenlecks einzelner Anwendungen

- **Allow Access WAN**: Erlaubt lokalen Geräten bei aktivem VPN weiterhin den Zugriff auf Dienste auf der WAN-Seite, etwa Drucker, NAS und andere Geräte im vorgeschalteten Subnetz.



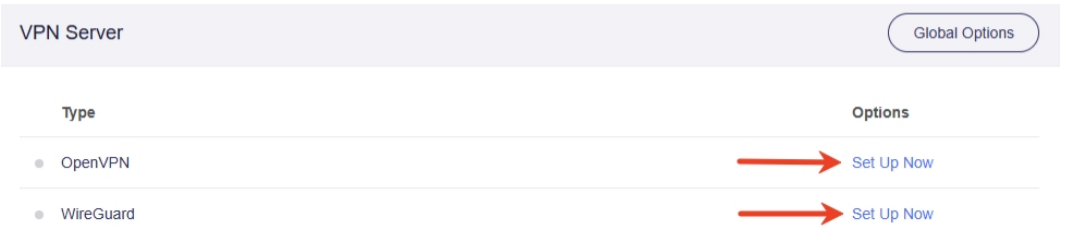
Wie im obigen Diagramm dargestellt, können Ihre lokalen Geräte nach Aktivierung dieser Funktion auf Geräte im vorgeschalteten Subnetz zugreifen, etwa Drucker und NAS.

Diese Option dient hauptsächlich dem Zugriff auf Geräte im vorgeschalteten Subnetz. Der Router kann den Datenverkehr zu diesem Subnetz jedoch nicht vom normalen Internetdatenverkehr unterscheiden. Greifen Endgeräte über öffentliche IP-Adressen direkt auf Ressourcen zu, besteht daher die Gefahr, dass Daten das VPN umgehen. Deshalb schließen sich **Allow Access WAN** und **Block Non-VPN Traffic** gegenseitig aus und können nicht gleichzeitig aktiviert werden.

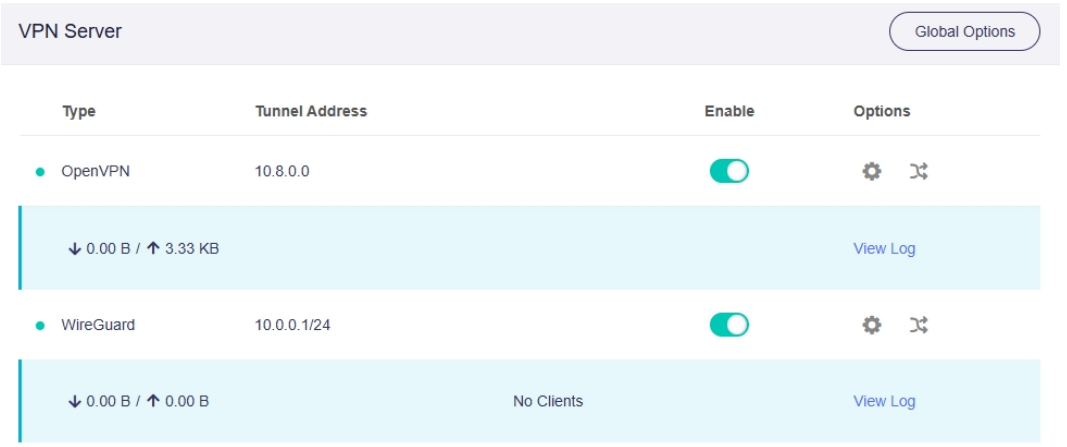
- **Services From GL.iNet Use VPN**: Leitet die Datenpakete von GoodCloud, DDNS und rtty durch die VPN-Tunnel. Diese Option ist standardmäßig deaktiviert, da diese Dienste für den ordnungsgemäßen Betrieb normalerweise die tatsächliche IP-Adresse des Geräts benötigen.

8.2 VPN-Server

Wenn der Router noch nie als OpenVPN- oder WireGuard-Server eingerichtet wurde, erscheint die folgende Ansicht. Klicken Sie auf **Set Up Now**, um zur Seite **OpenVPN Server** oder **WireGuard Server** zu gelangen und den VPN-Server einzurichten.

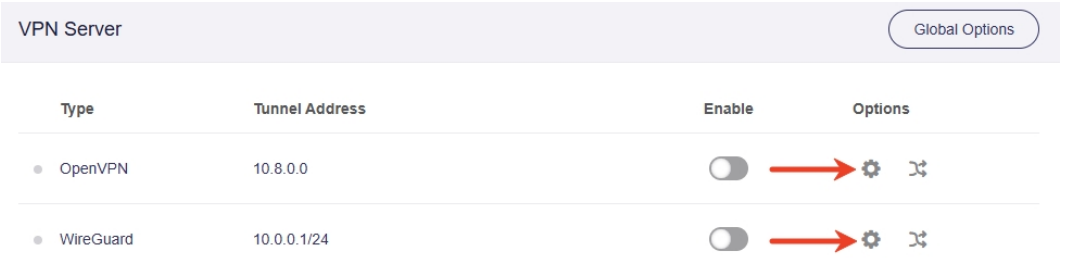


Nach dem Aktivieren des OpenVPN- oder WireGuard-Servers wird dessen Status wie folgt angezeigt.

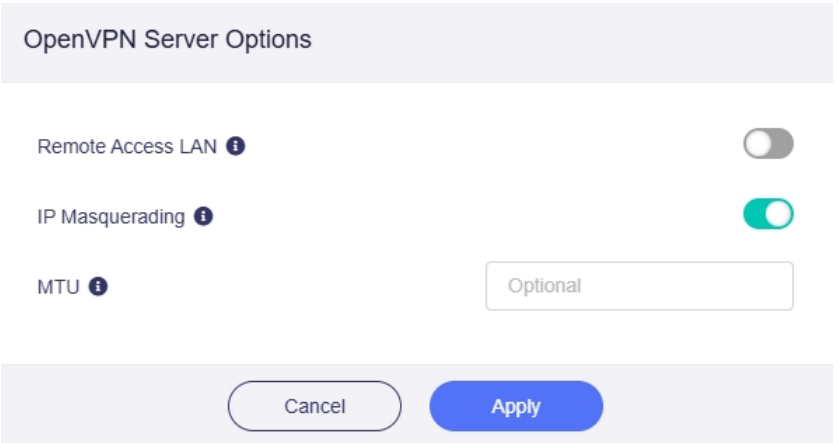


8.2.1 Server-Optionen

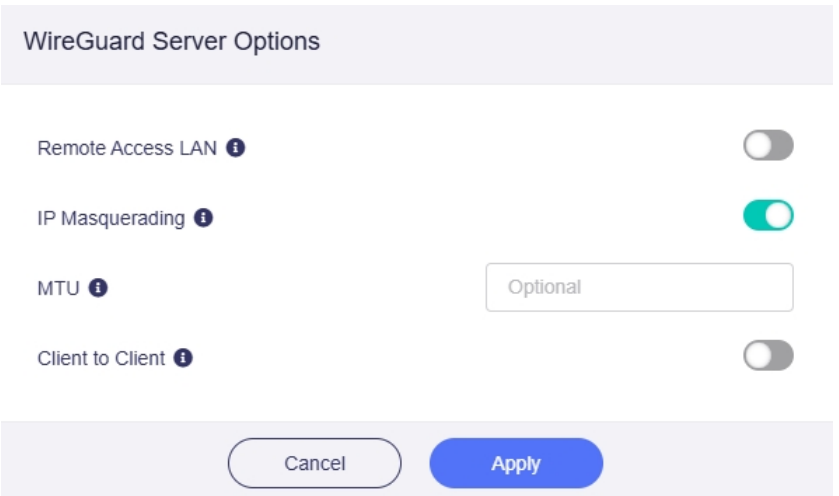
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Servers zu öffnen.



Die Optionen des OpenVPN-Servers werden wie folgt angezeigt.



Die Optionen des WireGuard-Servers werden wie folgt angezeigt.

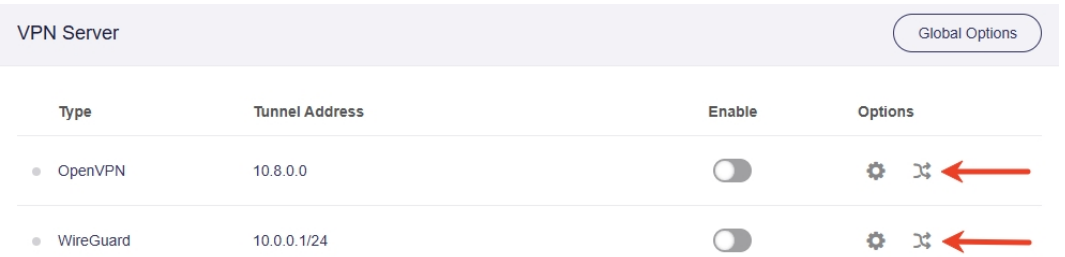


- **Remote Access LAN**: Erlaubt den Zugriff über den VPN-Tunnel auf Ressourcen im LAN-Subnetz des Servers.

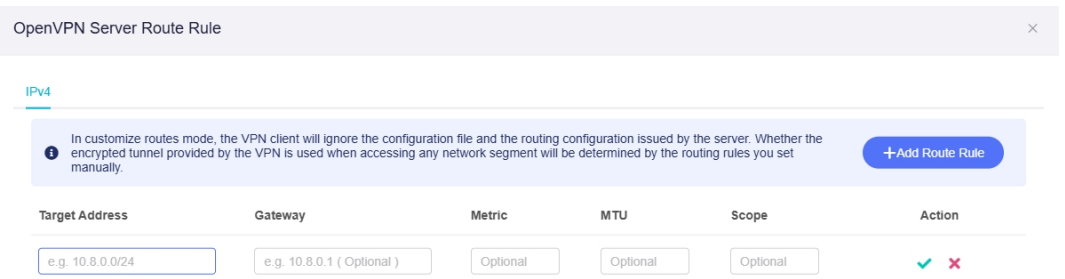
- **IP Masquerading**: Ersetzt die Quell-IP-Adressen der LAN-Geräte durch die VPN-Tunnel-IP-Adresse des Routers. Deaktivieren Sie diese Option nur bei Standortvernetzungen, bei denen die Gegenstelle Ihre LAN-Subnetze kennt.
- **MTU**: Steht für Maximum Transmission Unit, die maximale Paketgröße. Der hier festgelegte MTU-Wert für den Tunnel überschreibt die MTU-Einstellung in der Konfigurationsdatei.
- **Client to Client**: Erlaubt VPN-Clients, die mit diesem Server verbunden sind, den gegenseitigen Zugriff über ihre VPN-Tunnel-IP-Adressen. Sollen die Clients auch auf die LAN-Subnetze der jeweils anderen Clients zugreifen können, müssen Sie auf dem VPN-Server Routingregeln hinzufügen, die diese entfernten LAN-Subnetze bekannt geben.

8.2.2 Server-Routingregeln

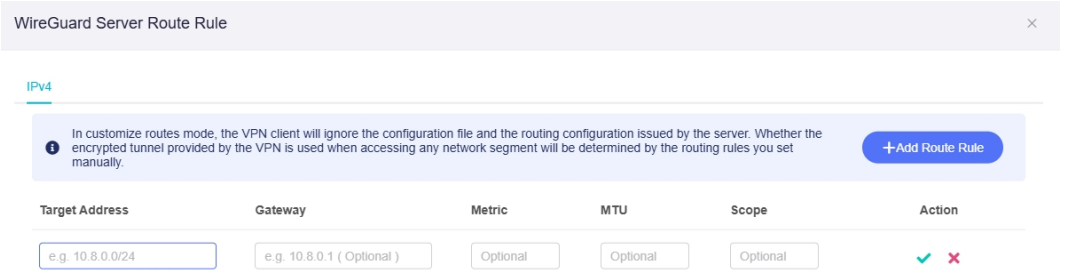
Klicken Sie rechts auf das Routensymbol, um die Routingregeln für OpenVPN oder WireGuard nach Bedarf anzupassen.



Die OpenVPN-Server-Routingregeln werden wie folgt angezeigt. Klicken Sie auf **Add Route Rule**, geben Sie **Target Address** und **Gateway** ein und klicken Sie zum Übernehmen auf das grüne Häkchen.



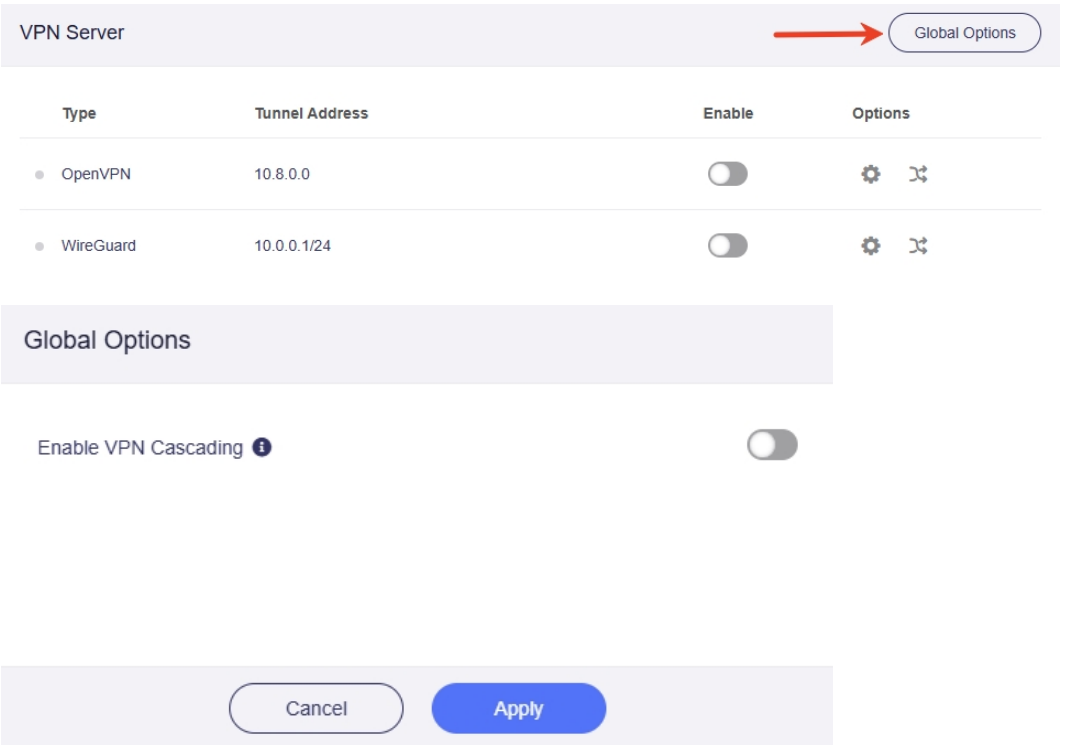
Die WireGuard-Server-Routingregeln werden wie folgt angezeigt. Klicken Sie auf **Add Route Rule**, geben Sie **Target Address** und **Gateway** ein und klicken Sie zum Übernehmen auf das grüne Häkchen.



Hinweis: Bei benutzerdefinierten Routen ignoriert der VPN-Client die Routingvorgaben der Konfigurationsdatei und des Servers. Ob der Zugriff auf ein Netzwerksegment durch den verschlüsselten VPN-Tunnel erfolgt, bestimmen ausschließlich die manuell festgelegten Routingregeln.

8.2.3 Globale Optionen

Klicken Sie oben rechts auf **Global Options**, um die erweiterten Einstellungen Ihres VPN-Servers zu konfigurieren.



Wenn **VPN Cascading** aktiviert ist und der Router gleichzeitig als VPN-Server und VPN-Client arbeitet, wird der Datenverkehr entfernter VPN-Clients, die mit seinem VPN-Server verbunden sind, durch den vorgeschalteten VPN-Tunnel geleitet, den der Router als VPN-Client nutzt. Mehr über VPN-Kaskadierung erfahren.

Kapitel 9

VPN-Server einrichten

Dieses Kapitel beschreibt, wie Sie einen GL.iNet-Router als OpenVPN- oder WireGuard-Server einrichten.

9.1 OpenVPN-Server einrichten

OpenVPN ist ein quelloffenes VPN-Protokoll, das SSL/TLS-Verschlüsselung für sichere Punkt-zu-Punkt-Verbindungen und Standortvernetzungen nutzt. Um einen OpenVPN-Server auf einem GL.iNet-Router einzurichten, sehen Sie sich dieses Video an oder befolgen Sie die nachstehenden Schritte.

9.1.1 Vorbereitung

1. **Öffentliche IP-Adresse sicherstellen**

   Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Ohne öffentliche IP-Adresse können Sie Ihren Router nicht als OpenVPN-Server einrichten.

   Alternativen:

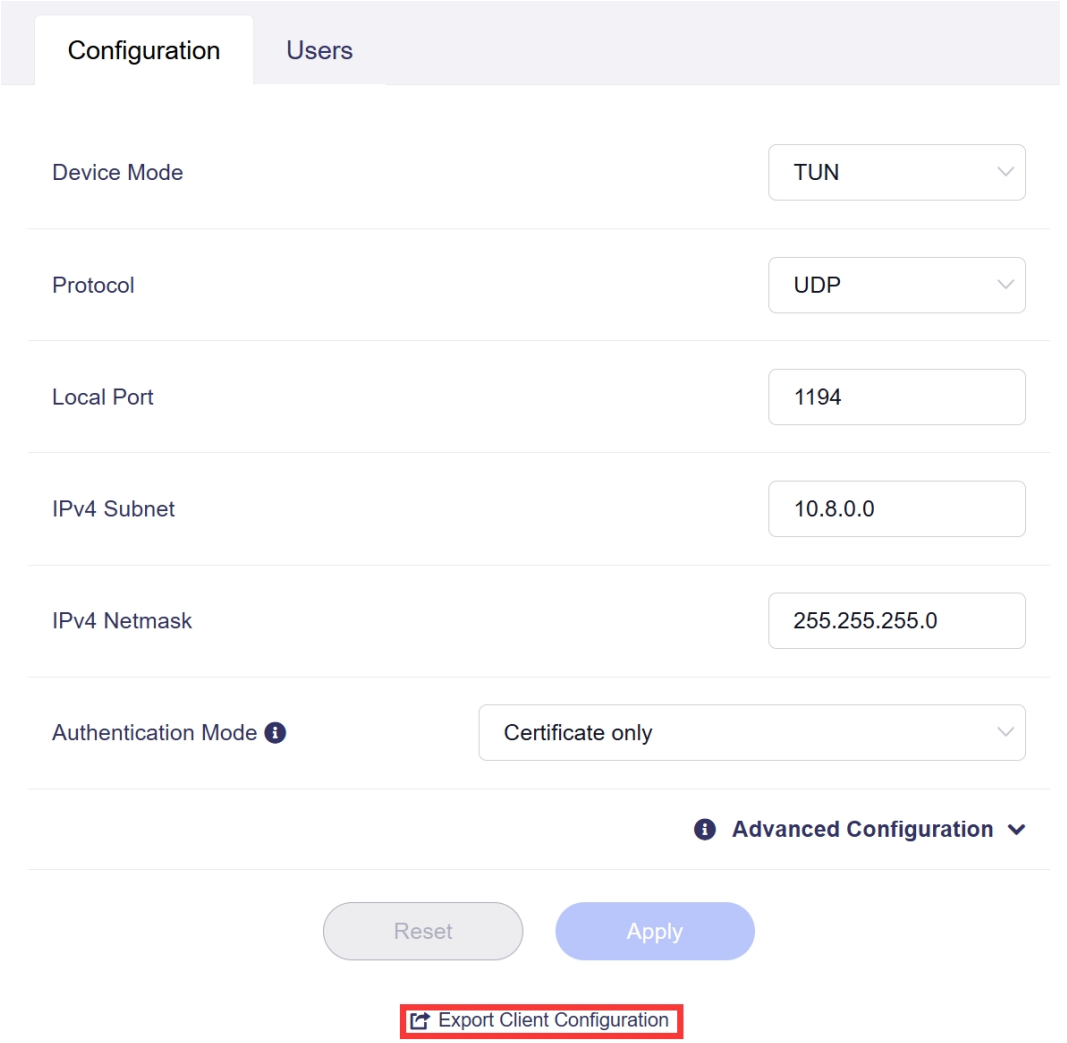
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.

2. **Erforderliche Portweiterleitung prüfen**

   - Wenn Ihr GL.iNet-Router der Hauptrouter Ihres Netzwerks ist, benötigen Sie keine Portweiterleitung. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn bereits ein Hauptrouter vorhanden ist und Ihr GL.iNet-Router als nachgeschalteter Router arbeitet, müssen Sie auf dem Hauptrouter eine Portweiterleitung einrichten.
   - Ist Ihr GL.iNet-Router über mehrere Router hinter dem Hauptrouter angeschlossen, richten Sie die Portweiterleitung auf jedem dazwischenliegenden Gerät ein.

9.1.2 Einrichtung

1. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Server** und klicken Sie auf **Generate Configuration** (nur bei der Ersteinrichtung des VPN-Servers).
2. Konfiguration übernehmen.
   Die Standardkonfiguration eignet sich für die meisten Fälle. Klicken Sie unten auf **Export Client Configuration** und fahren Sie mit Schritt 3 fort. Falls Sie die Konfiguration geändert haben, klicken Sie vor dem Export auf **Apply**.

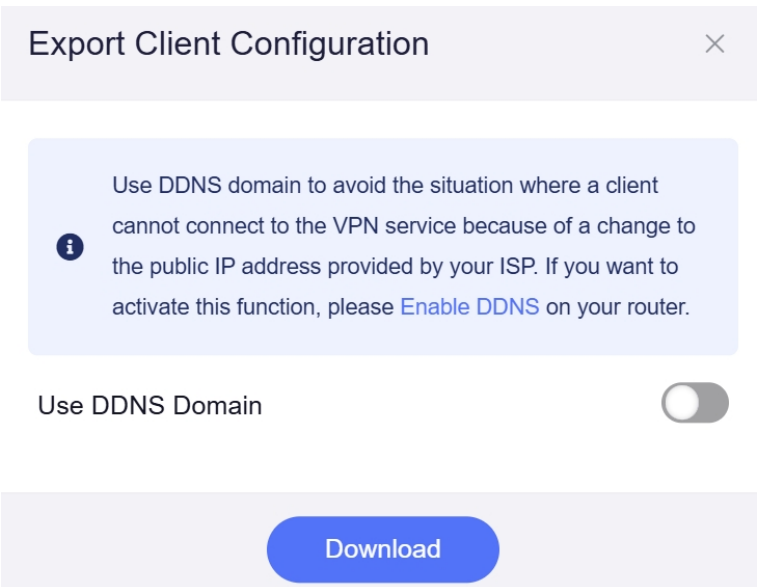


- **Device Mode**: TAP-S2S oder Tun. Die Unterschiede werden hier erläutert.
- **Protocol**: UDP oder TCP. Die Unterschiede werden hier erläutert.
- **Authentication Mode**: Legt fest, wie sich der Client beim Verbinden mit dem Server authentifiziert. Es gibt drei Optionen:

- **Certificate Only**: Der Router erzeugt automatisch die Zertifikate und Schlüssel für Server und Client und bettet sie in die Konfigurationsdatei ein. Nach dem Hochladen der Konfiguration auf den Client sind keine weiteren Zugangsdaten erforderlich.
- **Username/Password Only**: Der Router erzeugt eine Client-Konfiguration ohne Zertifikatschlüssel. Fügen Sie vor dem Export der Client-Konfiguration auf der Registerkarte **Users** einen Benutzernamen und ein Passwort hinzu. Geben Sie diese Zugangsdaten beim Hochladen der Konfiguration auf den Client zur Authentifizierung ein.
- **Username/Password and Certificate**: Fügen Sie vor dem Export der Client-Konfiguration zunächst auf der Registerkarte **Users** einen Benutzernamen und ein Passwort hinzu. Der Router erzeugt außerdem automatisch Zertifikate und Schlüssel für Server und Client und bettet sie in die Konfigurationsdatei ein. Beim Hochladen auf den Client wird zuerst der Zertifikatschlüssel geprüft, anschließend erfolgen Benutzername-/Passwortprüfung als zusätzliche Authentifizierung.

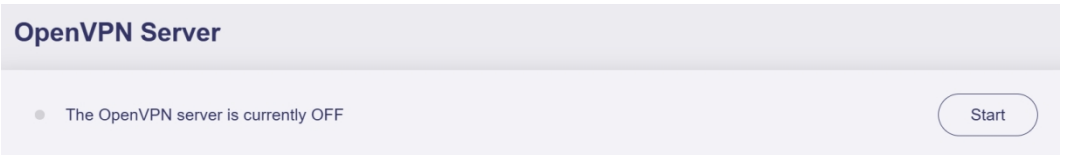
- **Advanced Configuration**: Hier können Sie bei Bedarf weitere Servereinstellungen anpassen.

3. Client-Konfiguration exportieren.
   Nach einem Klick auf **Export Client Configuration** unten auf der Registerkarte Configuration oder nach dem Übernehmen einer geänderten Konfiguration erscheint das folgende Fenster. Klicken Sie auf **Download**, um die Konfiguration zu exportieren.

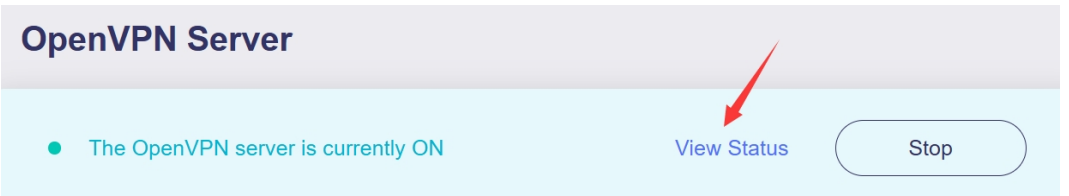


Tipp: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Sie können dann den DDNS-Domainnamen als Serveradresse verwenden.

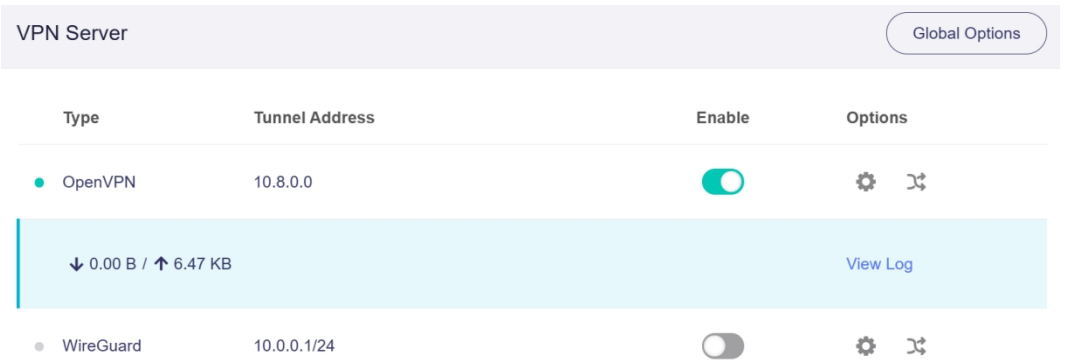
4. OpenVPN-Server starten.
   Klicken Sie auf der Seite **OpenVPN Server** oben rechts auf **Start**, um den Server zu starten.



   Um den Verbindungsstatus des Servers anzuzeigen, klicken Sie auf **View Status**.



   Sie werden zum VPN-Dashboard weitergeleitet. Wenn dort die Upload- und Downloadstatistiken angezeigt werden, ist der OpenVPN-Server in Betrieb.



9.1.3 Fehlerbehebung

Wenn die Verbindung fehlschlägt, kommen unter anderem folgende Ursachen infrage:

- Der VPN-Server hat keine öffentliche IP-Adresse. Hinweise zur Fehlerbehebung finden Sie hier.
- Möglicherweise müssen Sie eine Portweiterleitung einrichten. Hinweise zur Fehlerbehebung finden Sie hier.

- Ihr Internetanbieter sperrt den vom OpenVPN-Server verwendeten Port. Wechseln Sie zu einem anderen Port oder bitten Sie Ihren Internetanbieter um Unterstützung.
- In bestimmten Ländern oder Regionen kann die VPN-Verbindung gesperrt sein.

9.2 WireGuard-Server einrichten

WireGuard® ist eine einfache, schnelle und moderne VPN-Lösung mit aktueller Kryptografie. Sie soll schneller, einfacher und praktischer als IPSec sein und dessen hohe Komplexität vermeiden. Außerdem zielt sie auf eine deutlich höhere Leistung als OpenVPN ab. Um einen WireGuard-Server auf einem GL.iNet-Router einzurichten, sehen Sie sich dieses Video an oder befolgen Sie die nachstehenden Schritte.

9.2.1 Vorbereitung

1. **Öffentliche IP-Adresse sicherstellen**

   Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Ohne öffentliche IP-Adresse können Sie Ihren Router nicht als WireGuard-Server einrichten.

   Alternativen:

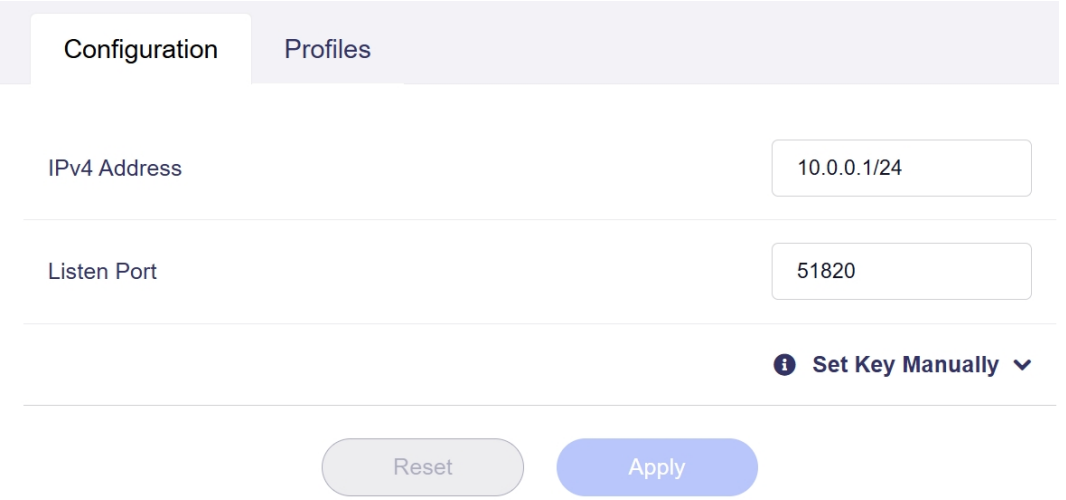
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.

2. **Erforderliche Portweiterleitung prüfen**

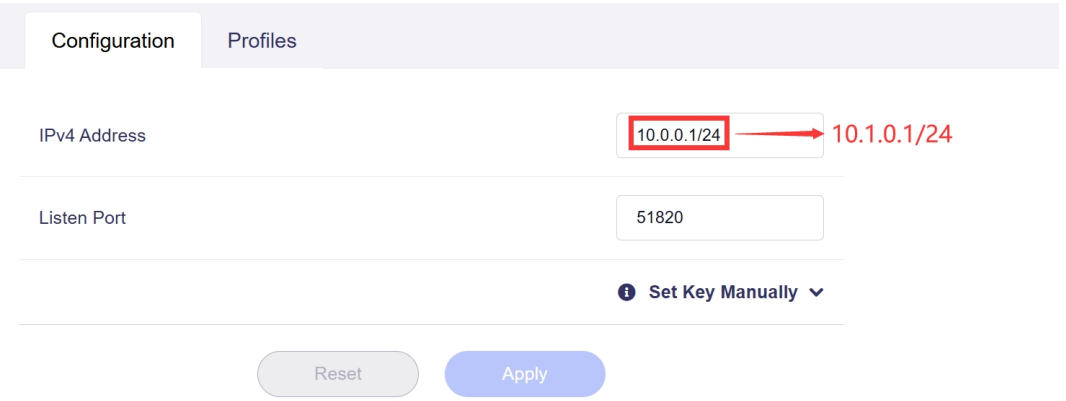
   - Wenn Ihr GL.iNet-Router der Hauptrouter Ihres Netzwerks ist, benötigen Sie keine Portweiterleitung. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn bereits ein Hauptrouter vorhanden ist und Ihr GL.iNet-Router als nachgeschalteter Router arbeitet, müssen Sie auf dem Hauptrouter eine Portweiterleitung einrichten.
   - Ist Ihr GL.iNet-Router über mehrere Router hinter dem Hauptrouter angeschlossen, richten Sie die Portweiterleitung auf jedem dazwischenliegenden Gerät ein.

9.2.2 Einrichtung

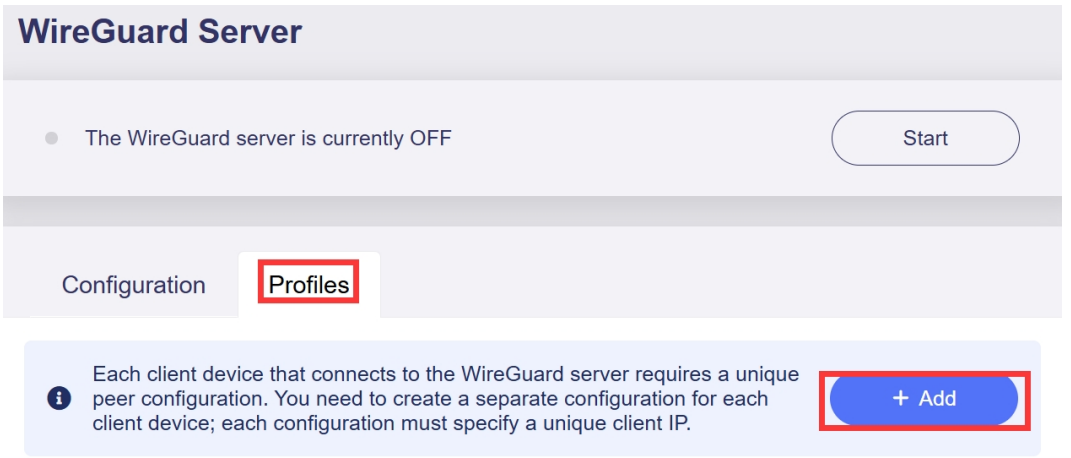
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **WireGuard Server** und klicken Sie auf **Generate Configuration** (nur bei der Ersteinrichtung des VPN-Servers).
2. Konfiguration übernehmen.
   Die Standardkonfiguration eignet sich für die meisten Fälle. Die IPv4-Adresse müssen Sie nur ändern, wenn sie mit der Gateway-Adresse Ihres vorgeschalteten Routers kollidiert.



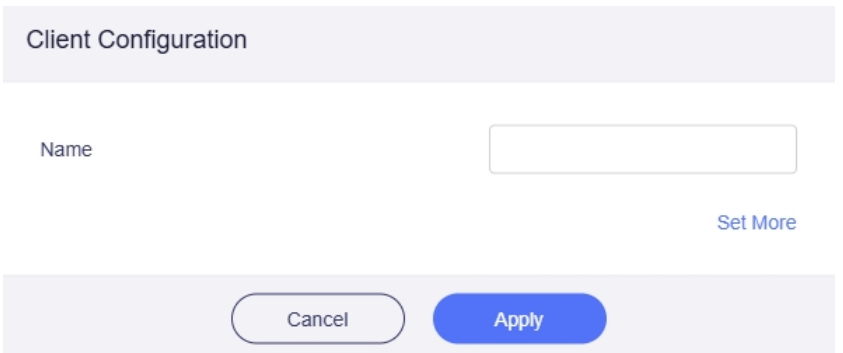
   Bei einem solchen Adresskonflikt wählen Sie eine andere IPv4-Adresse, etwa **10.1.0.1/24**, und klicken Sie auf **Apply**. Achten Sie darauf, die CIDR-Angabe „/24“ beizubehalten, um Verbindungsprobleme zu vermeiden.



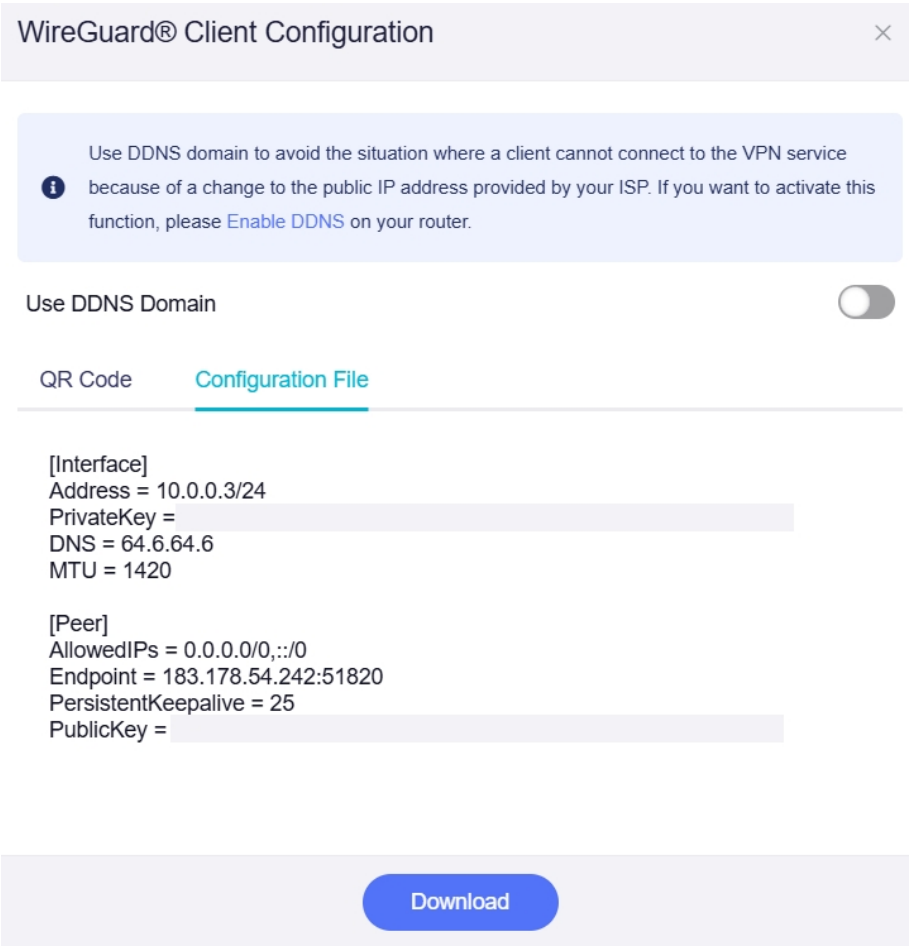
3. Profil hinzufügen.
   Wechseln Sie zur Registerkarte **Profiles** und klicken Sie auf **Add**, um ein Profil für Ihr Gerät zu erzeugen.



Vergeben Sie einen aussagekräftigen Namen und klicken Sie auf **Apply**, um fortzufahren.

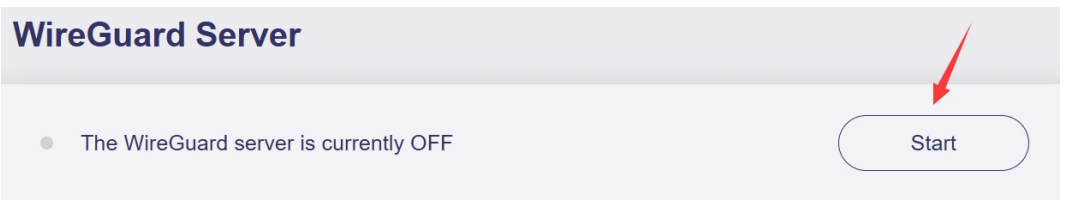


4. Konfiguration herunterladen.
   Nach dem Hinzufügen eines Profils stellt der Router die Konfiguration in drei Formen bereit: als QR-Code, als Klartext und als .conf-Datei. Wählen Sie die gewünschte Form aus.
   - **QR-Code**: Geeignet für Geräte wie Smartphones, Tablets oder Laptops mit installierter WireGuard-App. Öffnen Sie auf dem gewünschten WireGuard-Client die WireGuard-App und scannen Sie den QR-Code, um die Konfiguration zu importieren.
   - **Klartext**: In dieser Ansicht können Sie die Konfigurationsdetails prüfen und durch Kopieren und Einfügen an anderer Stelle manuell einrichten, etwa in der WireGuard-App oder auf einem GL.iNet-Router.
   - **.conf-Datei**: Klicken Sie auf **Download**, um die .conf-Datei lokal zu speichern. Diese lässt sich anschließend direkt in die WireGuard-App oder auf einen GL.iNet-Router hochladen.

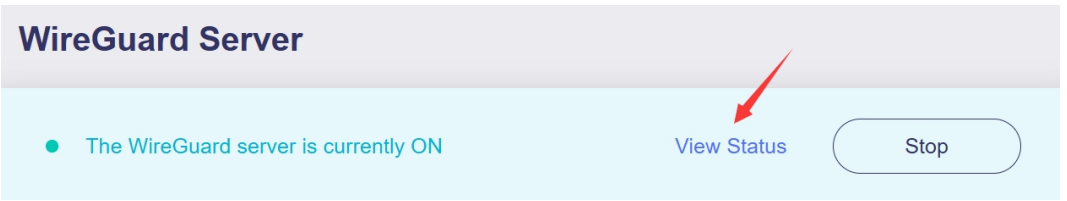


Tipp: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Sie können dann den DDNS-Domainnamen als Serveradresse verwenden.

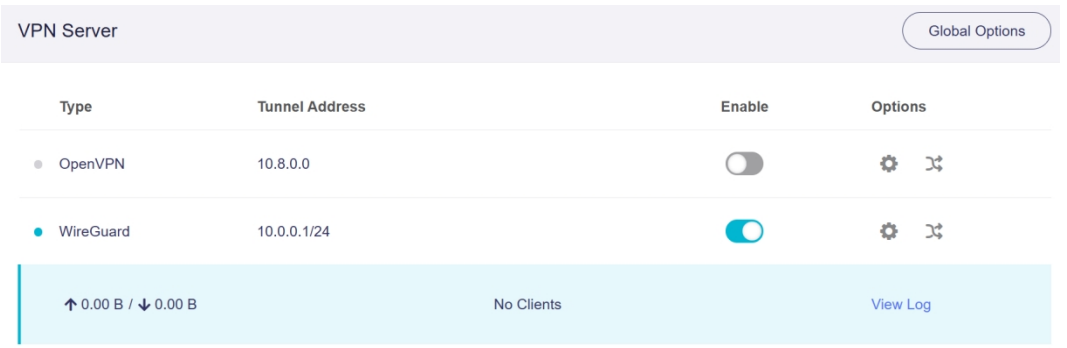
5. WireGuard-Server starten.
   Klicken Sie auf der Seite **WireGuard Server** oben rechts auf **Start**, um den Server zu starten.



Um den Verbindungsstatus des Servers anzuzeigen, klicken Sie auf **View Status**.



Sie werden zum VPN-Dashboard weitergeleitet. Wenn dort die Upload- und Downloadstatistiken angezeigt werden, ist der OpenVPN-Server in Betrieb.



9.2.3 Fehlerbehebung

Wenn die Verbindung fehlschlägt, kommen unter anderem folgende Ursachen infrage:

- Der VPN-Server hat keine öffentliche IP-Adresse. Hinweise zur Fehlerbehebung finden Sie hier.
- Möglicherweise müssen Sie eine Portweiterleitung einrichten. Hinweise zur Fehlerbehebung finden Sie hier.
- Ihr Internetanbieter sperrt den vom WireGuard-Server verwendeten Port. Wechseln Sie zu einem anderen Port oder bitten Sie Ihren Internetanbieter um Unterstützung.
- In bestimmten Ländern oder Regionen kann die VPN-Verbindung gesperrt sein.

Kapitel 10

VPN-Client einrichten

Dieses Kapitel beschreibt, wie Sie einen GL.iNet-Router als OpenVPN- oder WireGuard-Client einrichten.

10.1 OpenVPN-Client einrichten

10.1.1 Vorbereitung

Stellen Sie zunächst sicher, dass Sie ein aktives Abonnement bei einem VPN-Anbieter haben, der die manuelle OpenVPN-Konfiguration unterstützt. Mit GL.iNet kompatible OpenVPN-Anbieter finden Sie hier.

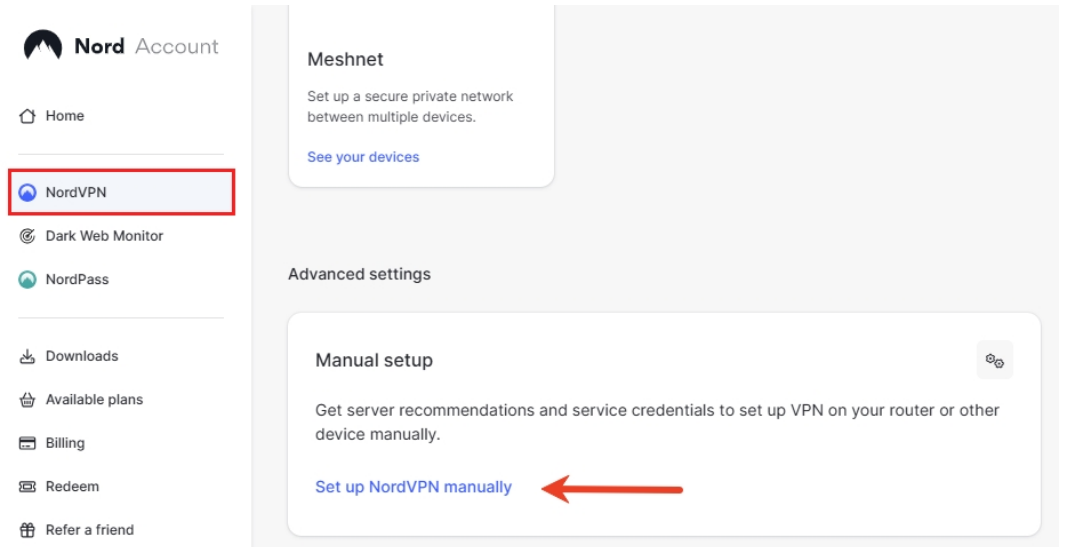
Rufen Sie anschließend die offizielle Webseite Ihres VPN-Anbieters auf und beschaffen Sie die Dienstzugangsdaten oder eine Konfigurationsdatei. Falls Sie nicht wissen, wie Sie die Datei erhalten, folgen Sie diesem Link oder wenden Sie sich an den Support des Anbieters.

10.1.2 NordVPN einrichten

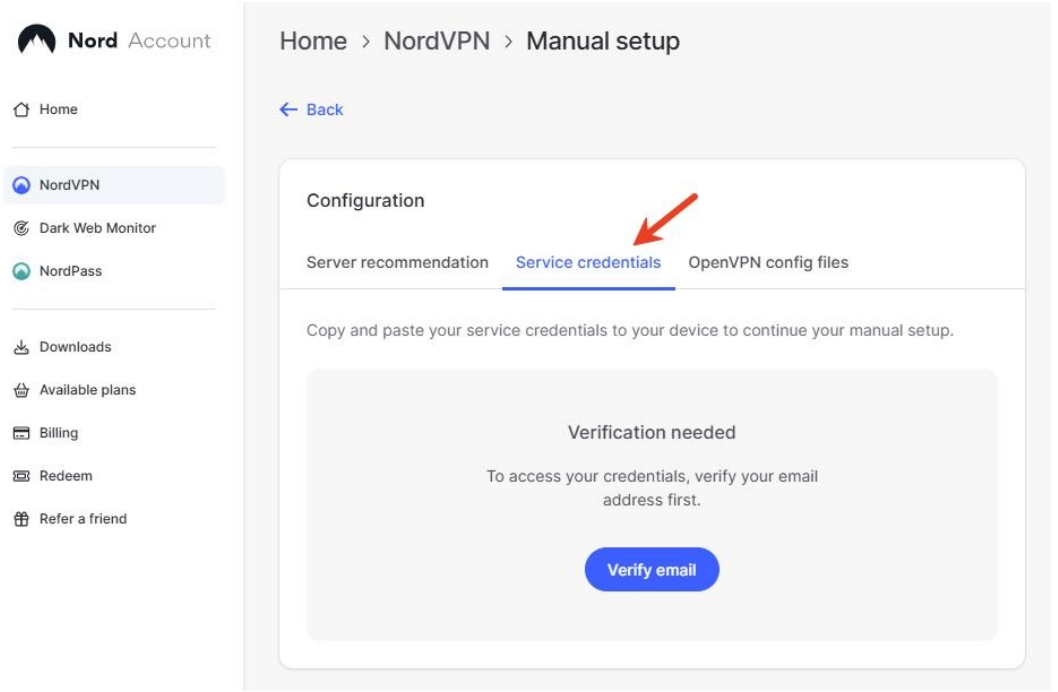
NordVPN ist in die GL.iNet-Weboberfläche integriert. Geben Sie Ihre im NordVPN-Dashboard erhältlichen Zugangsdaten in der Weboberfläche des Routers oder in der GL.iNet-App ein, um die Konfigurationsdateien aller NordVPN-Server abzurufen. Ein manuelles Hochladen der Dateien ist dadurch nicht erforderlich.

Gehen Sie wie folgt vor, um Ihren Router als NordVPN-Client einzurichten.

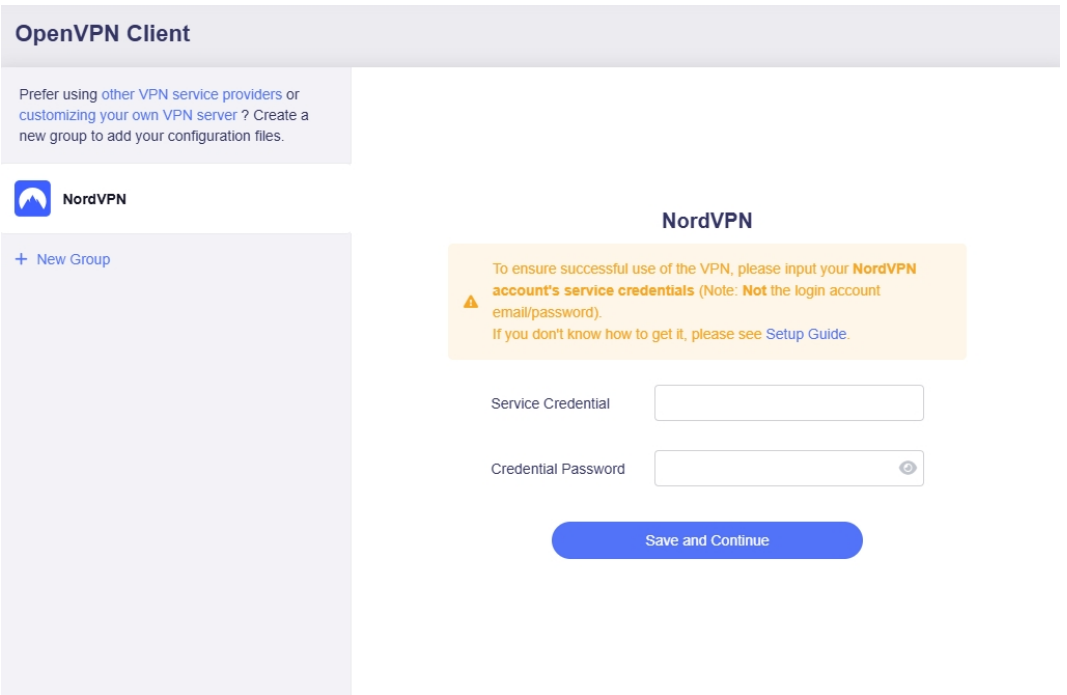
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



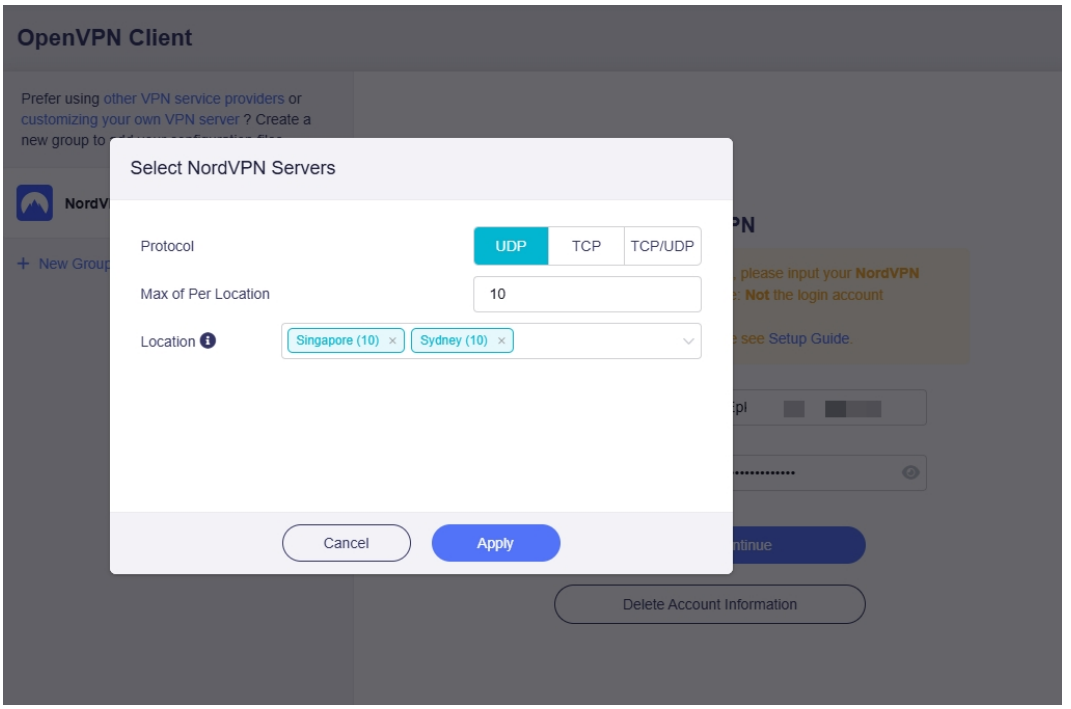
Dort finden Sie die **Dienstzugangsdaten**. Kopieren Sie diese für die spätere Verwendung.



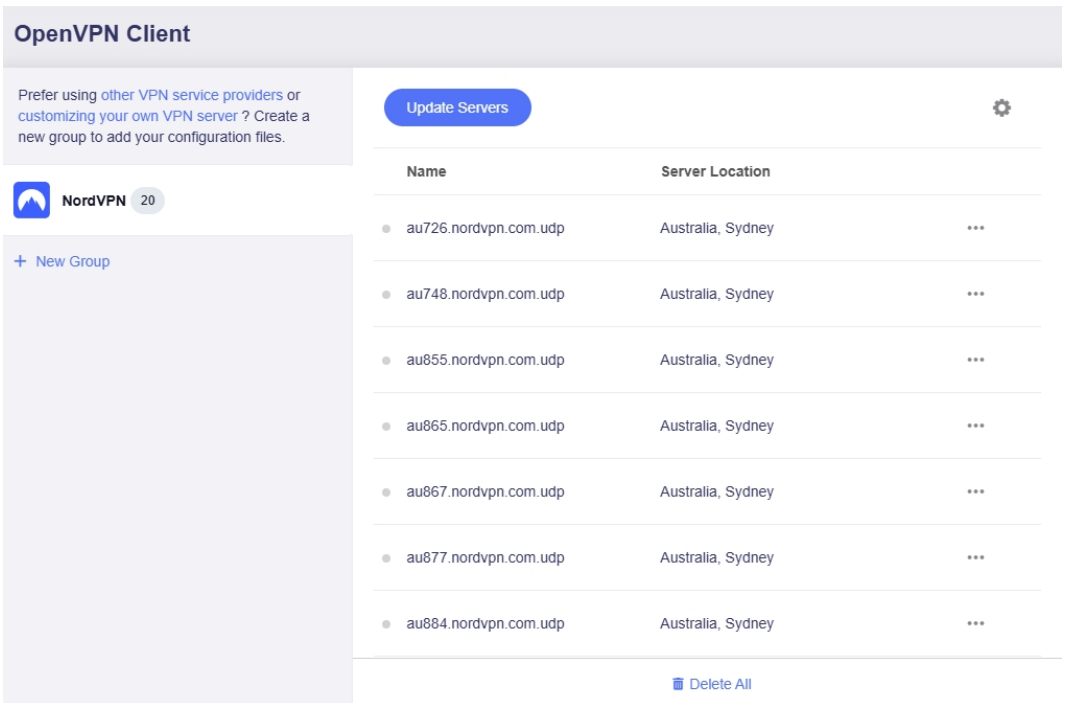
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **OpenVPN Client** > **NordVPN**. Geben Sie die Dienstzugangsdaten ein. Hinweis: Dies sind NICHT die E-Mail-Adresse und das Passwort Ihres Benutzerkontos. Klicken Sie anschließend auf **Save and Continue**.



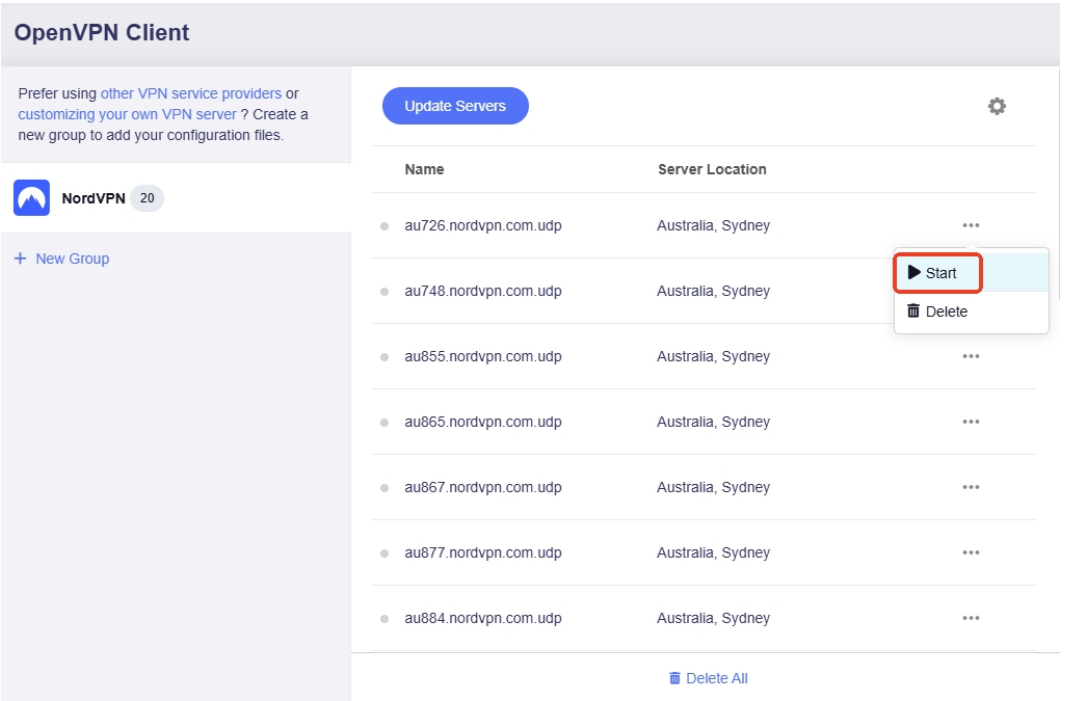
4. Wählen Sie das Protokoll, die maximale Serveranzahl pro Standort und die Standorte aus. Klicken Sie anschließend auf **Apply**.



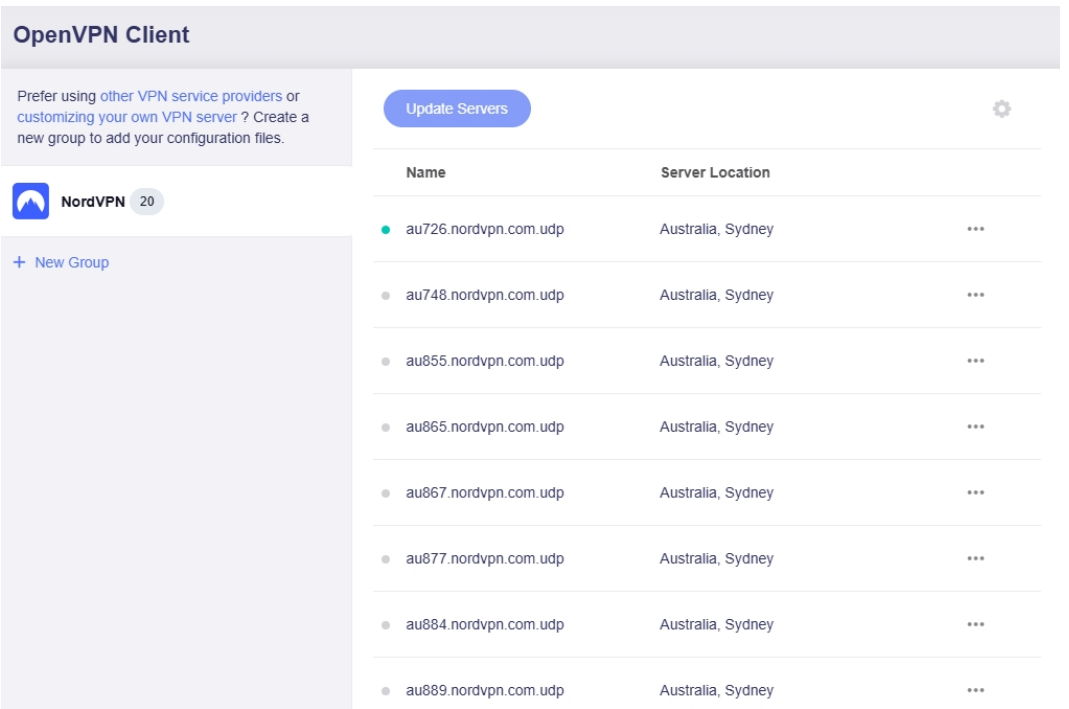
Die Konfigurationsdateien werden heruntergeladen.



5. Verbindung starten.
   Wählen Sie einen Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung zu starten.



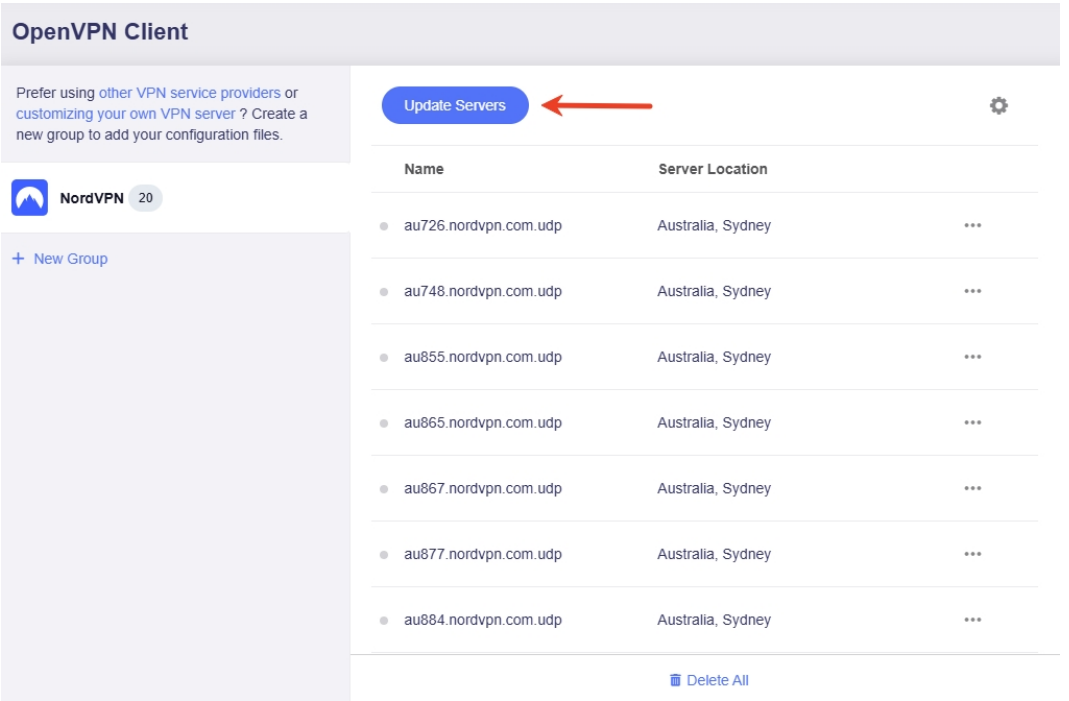
6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

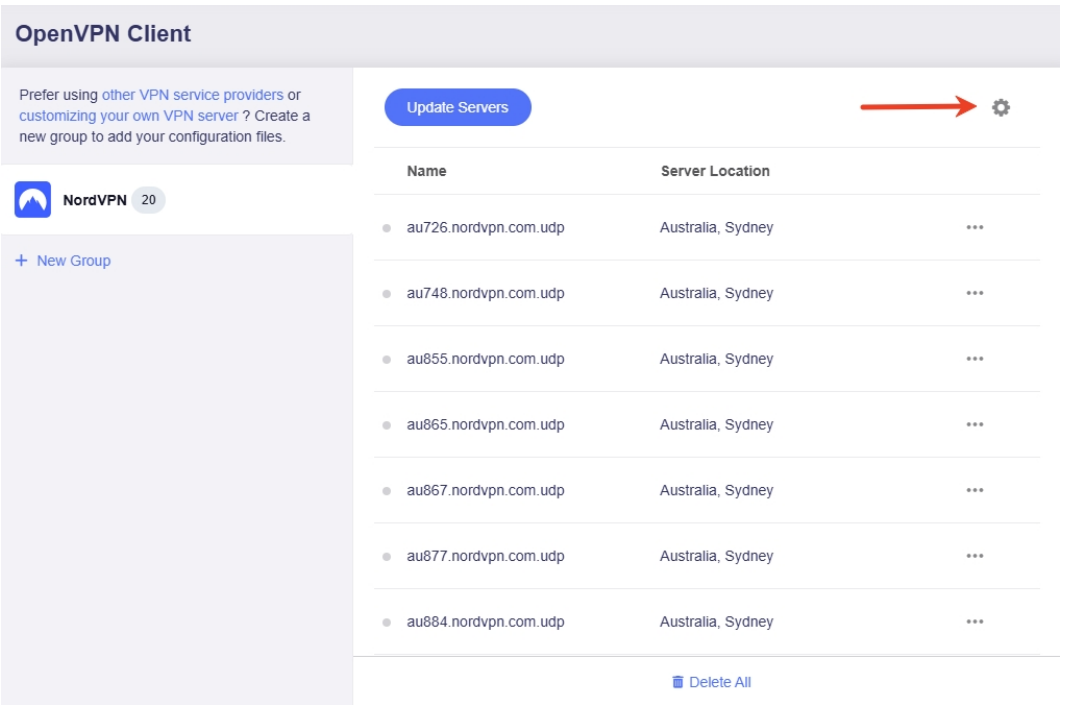
7. Server aktualisieren.

   Klicken Sie auf **Update Servers**, um die aktuelle Liste verfügbarer Server abzurufen. So vermeiden Sie Verbindungsfehler durch Serverwartung oder abgeschaltete Server.



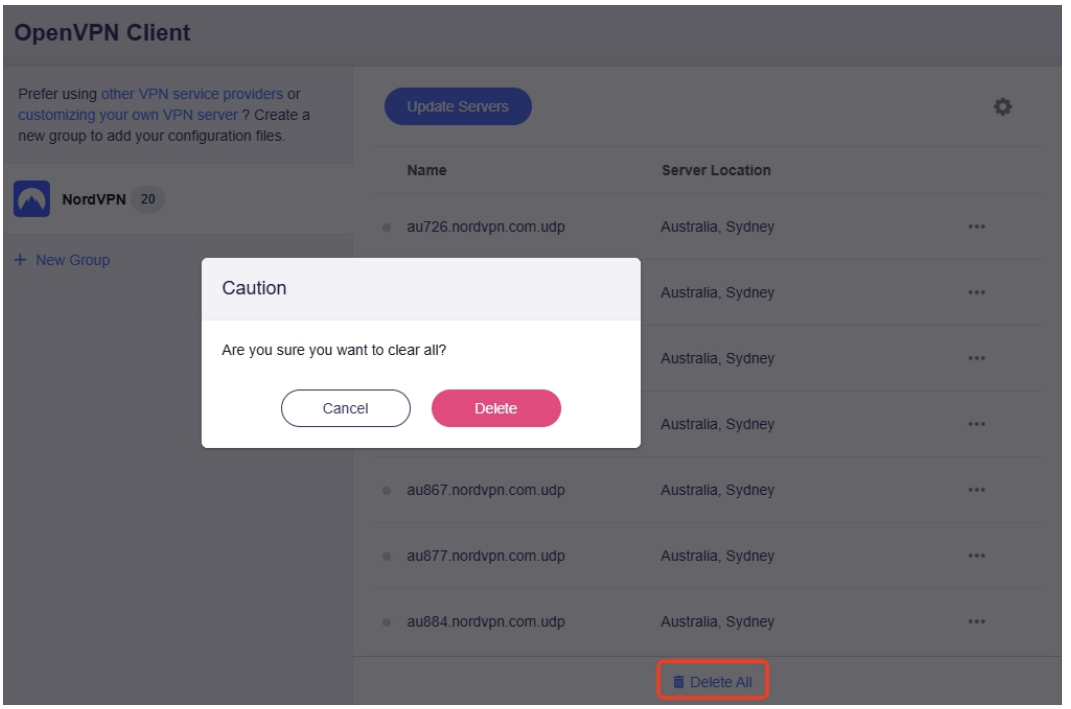
8. Zugangsdaten bearbeiten.

   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten.



9. Alle Dateien löschen.

   Klicken Sie auf **Delete All**, um alle Konfigurationsdateien mit einem Klick zu löschen.

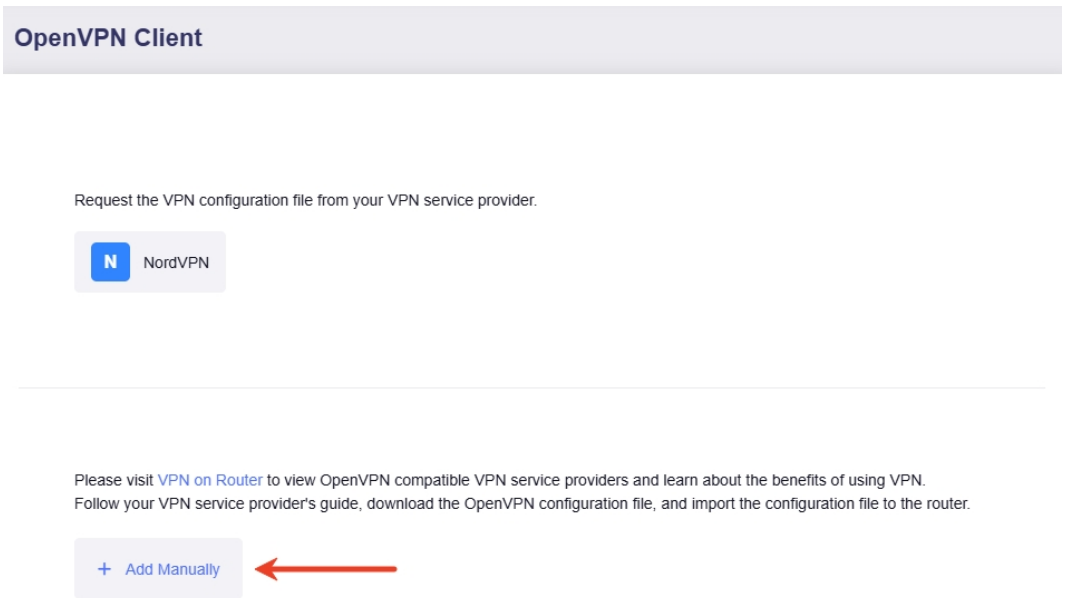

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp
Australia, Sydney
au877.nordvpn.com.udp
Australia, Sydney
au884.nordvpn.com.udp
Australia, Sydney
Delete All
Caution
Are you sure you want to clear all?
Cancel
Delete

10.1.3 OpenVPN-Client manuell einrichten (andere Anbieter)

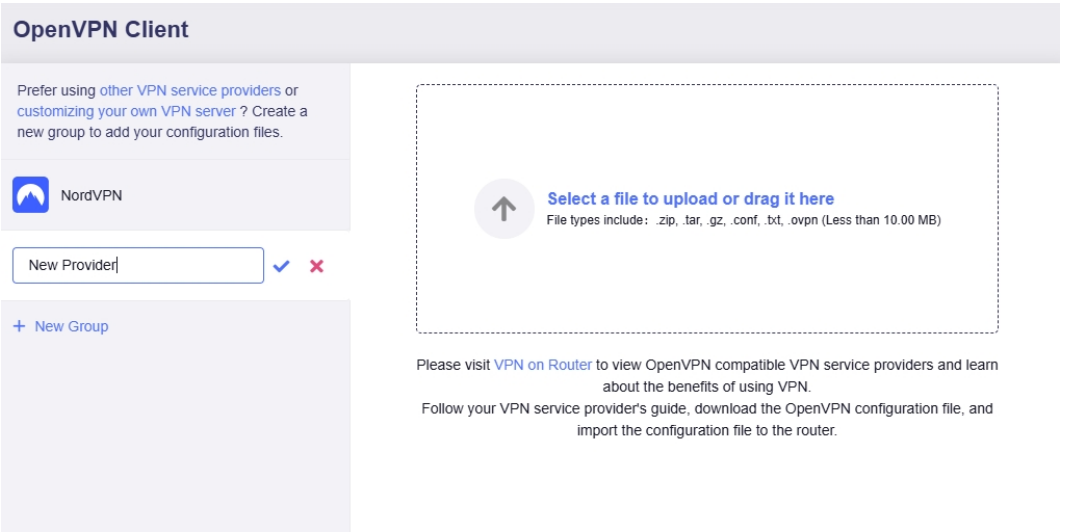
Wenn Ihr OpenVPN-Anbieter nicht in unsere Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den OpenVPN-Client einzurichten.

Die folgenden Schritte zeigen die Einrichtung am Beispiel von PIA (Private Internet Access).

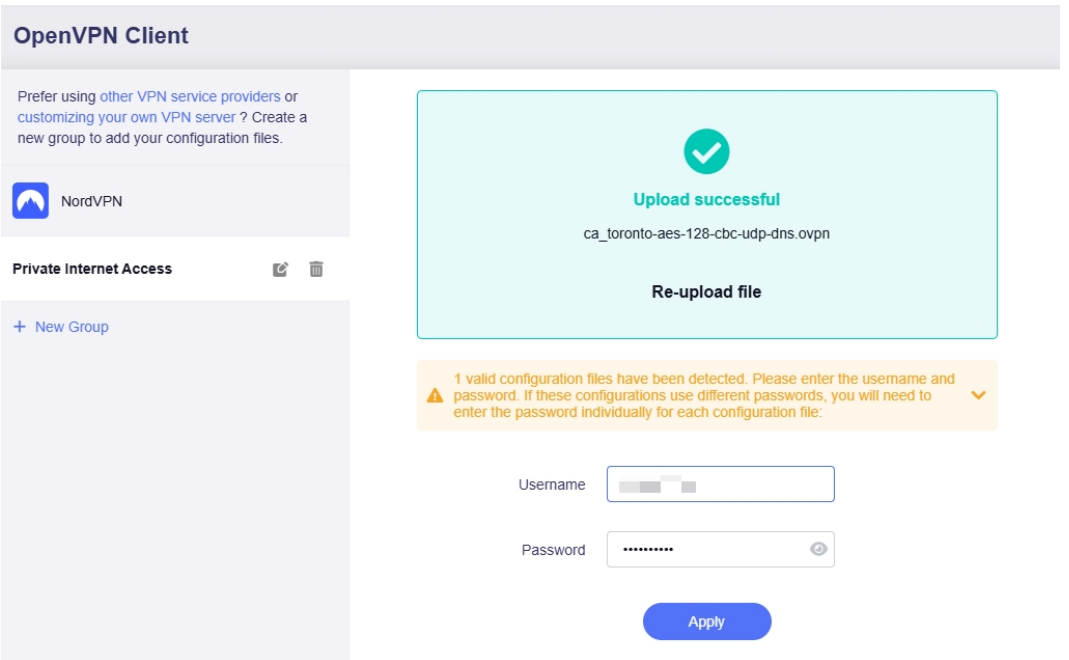
1. Laden Sie eine Konfigurationsdatei von der offiziellen Webseite von Private Internet Access herunter.
2. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Client** und klicken Sie auf **Add Manually**.



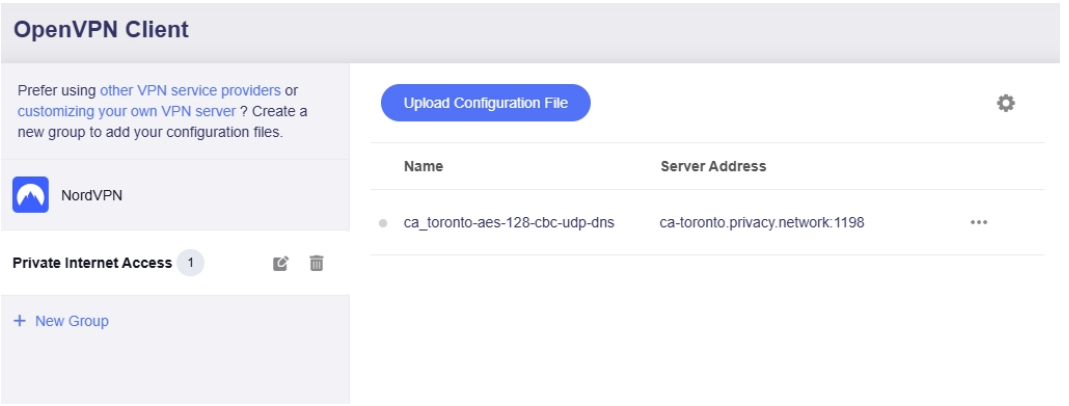
3. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



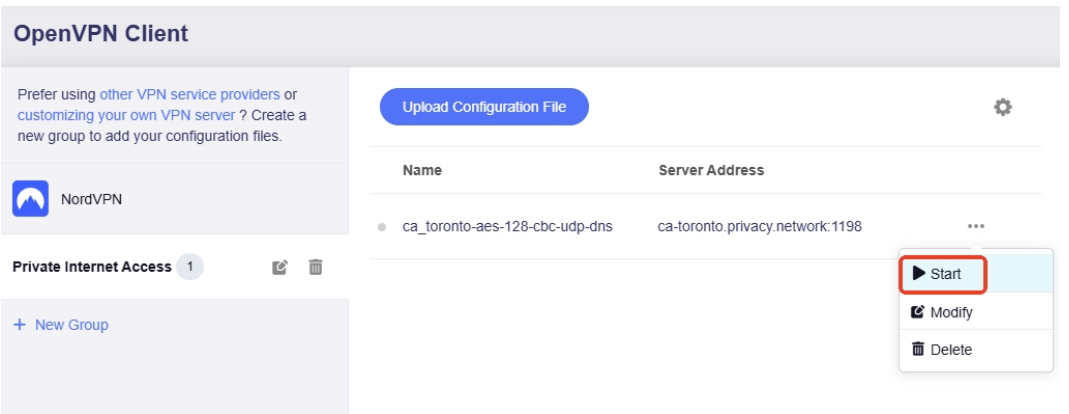
4. Laden Sie Ihre OpenVPN-Konfigurationsdatei hoch. Geben Sie bei Bedarf die Zugangsdaten ein und klicken Sie auf **Apply**.



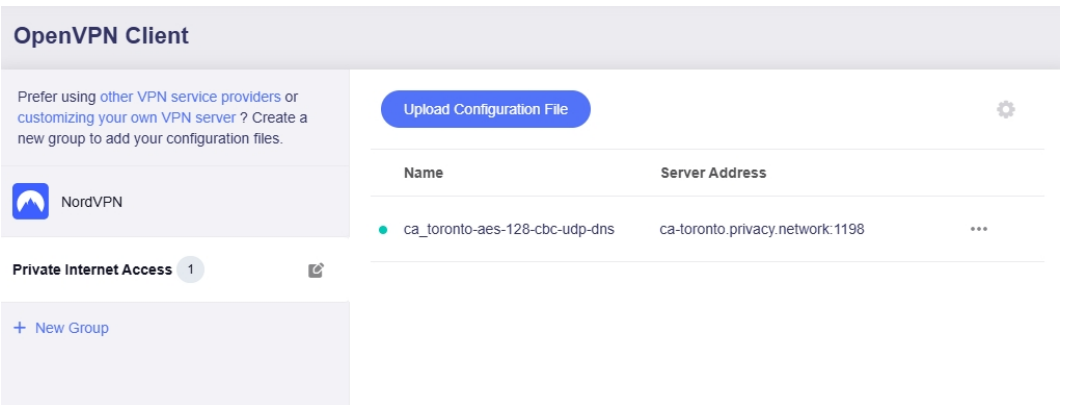
Die hochgeladene Konfigurationsdatei wird angezeigt.



5. Klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung zu starten.



6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

10.2 WireGuard-Client einrichten

Sie können den WireGuard-Client über die GL.iNet-App oder die Weboberfläche einrichten.

- In die App sind mehrere WireGuard-Anbieter integriert, darunter AzireVPN, Mullvad VPN, OVPN, StrongVPN und PIA VPN. Zur einfachen Einrichtung geben Sie die Zugangsdaten Ihres abonnierten WireGuard-Dienstes ein. Öffnen Sie die App und folgen Sie den Anweisungen auf dem Bildschirm.
- Die Weboberfläche bietet neben integrierten WireGuard-Anbietern auch eine manuelle Konfiguration. Für die schnelle Einrichtung geben Sie die Zugangsdaten Ihres WireGuard-Dienstes ein. Alternativ können Sie eine Konfigurationsdatei manuell hochladen.

10.2.1 Vorbereitung

Stellen Sie zunächst sicher, dass Sie ein aktives Abonnement bei einem VPN-Anbieter haben, der die manuelle WireGuard-Konfiguration unterstützt. Mit GL.iNet kompatible WireGuard-Anbieter finden Sie hier.

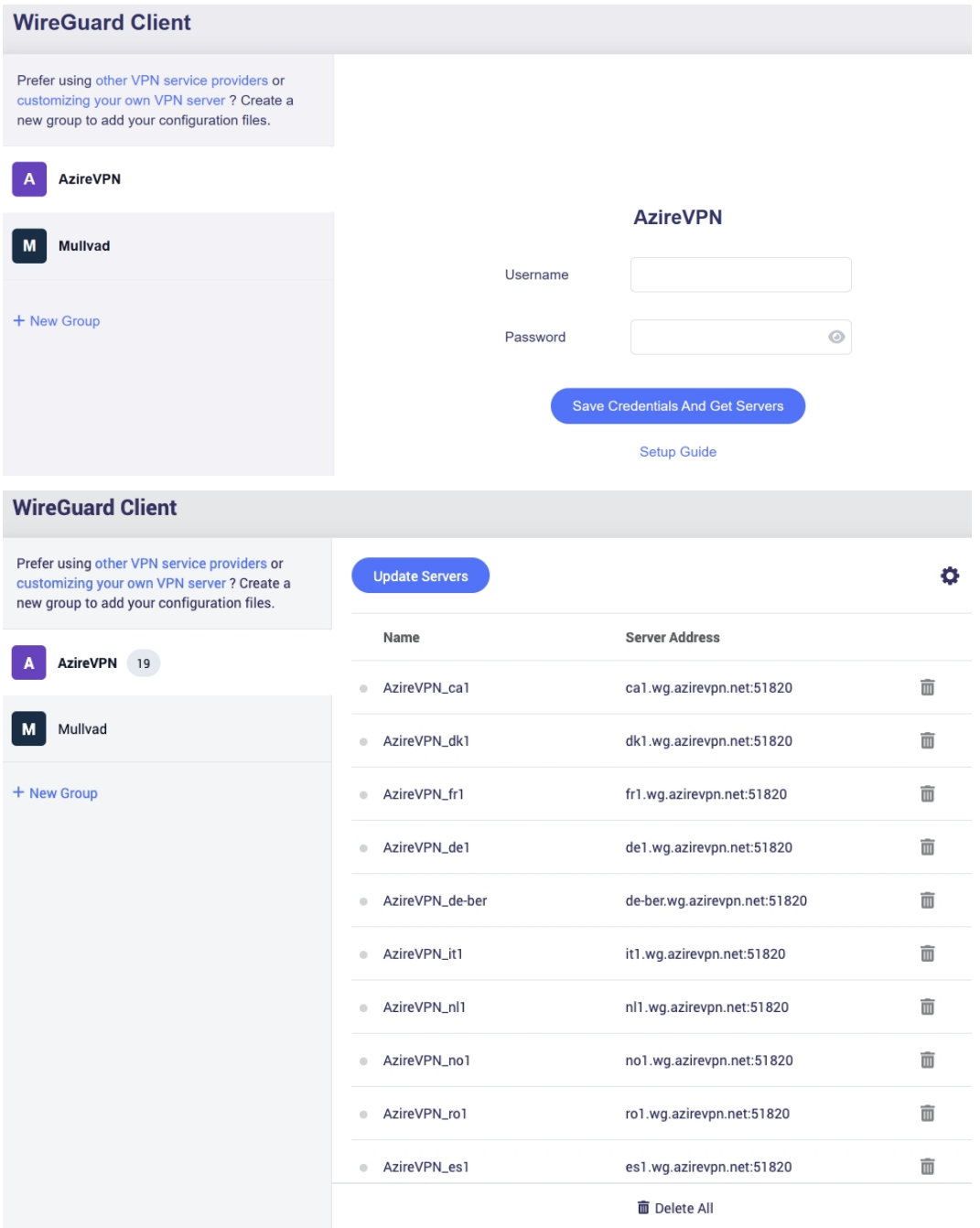
Wählen Sie nachstehend Ihren WireGuard-Anbieter aus, um direkt zur passenden Schritt-für-Schritt-Anleitung zu gelangen.

- AzireVPN einrichten
- Mullvad einrichten
- WireGuard-Client manuell einrichten (andere Anbieter)

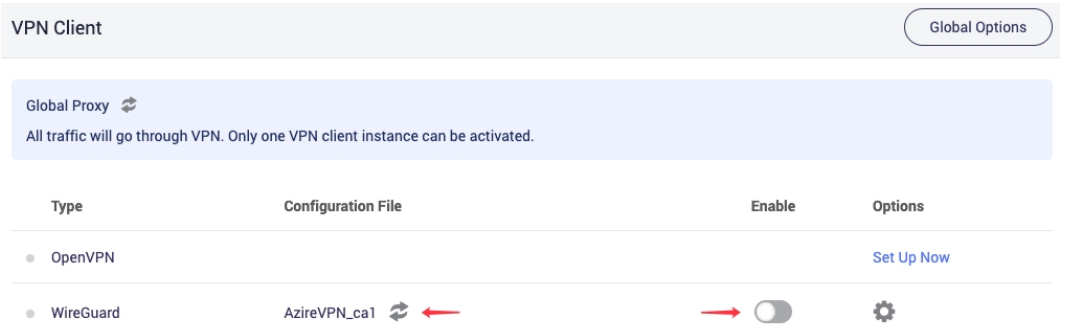
10.2.2 AzireVPN einrichten

Gehen Sie wie folgt vor, um Ihren Router als AzireVPN-Client einzurichten.

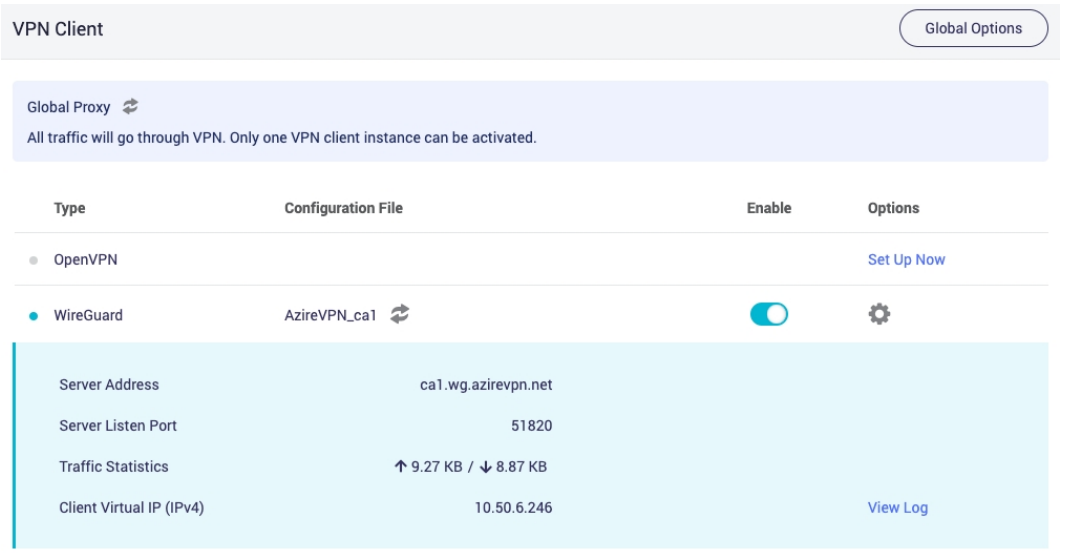
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **AzireVPN**.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Save Credentials And Get Servers**. Für jeden Server wird eine Konfigurationsdatei erzeugt.



3. Öffnen Sie das VPN-Dashboard, um die Verbindung zu aktivieren.

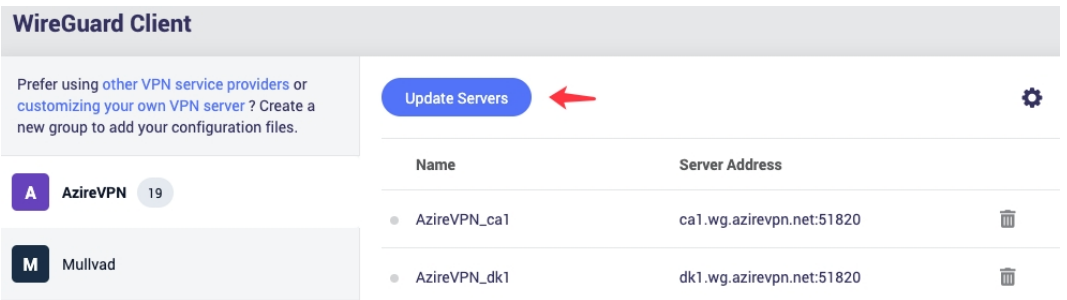


Nach erfolgreicher Verbindung werden Ihre Benutzer-IP-Adresse sowie die Anzahl der gesendeten und empfangenen Bytes angezeigt.



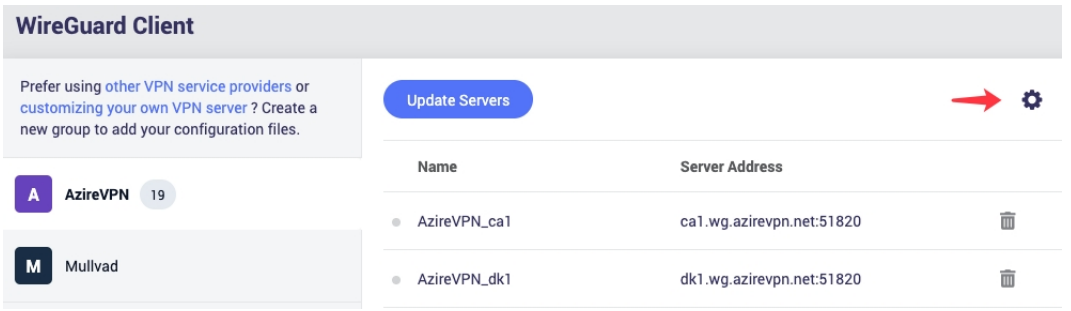
4. Server aktualisieren.

   Serverwartungen oder abgeschaltete Server bei AzireVPN können Verbindungsfehler verursachen. Klicken Sie auf **Update Servers**, um die aktuelle Liste verfügbarer Server abzurufen.



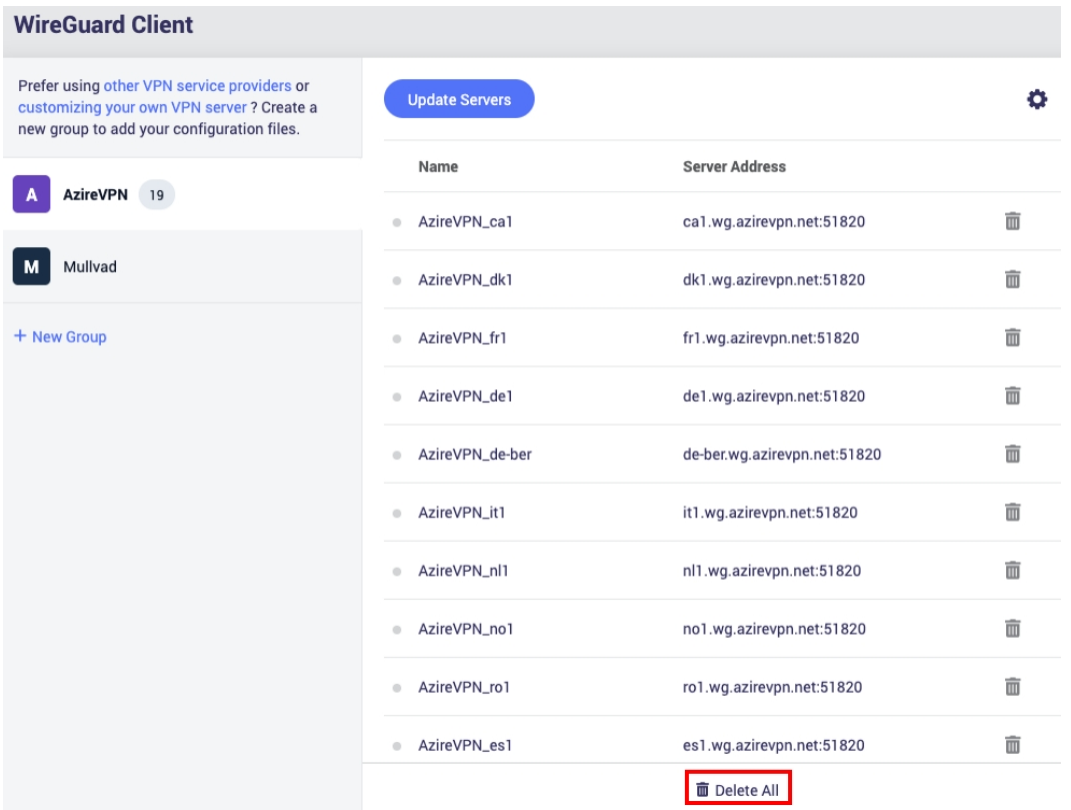
5. Zugangsdaten bearbeiten.

   Klicken Sie auf das Zahnradsymbol, um die Zugangsdaten zu bearbeiten.



6. Alle Dateien löschen.

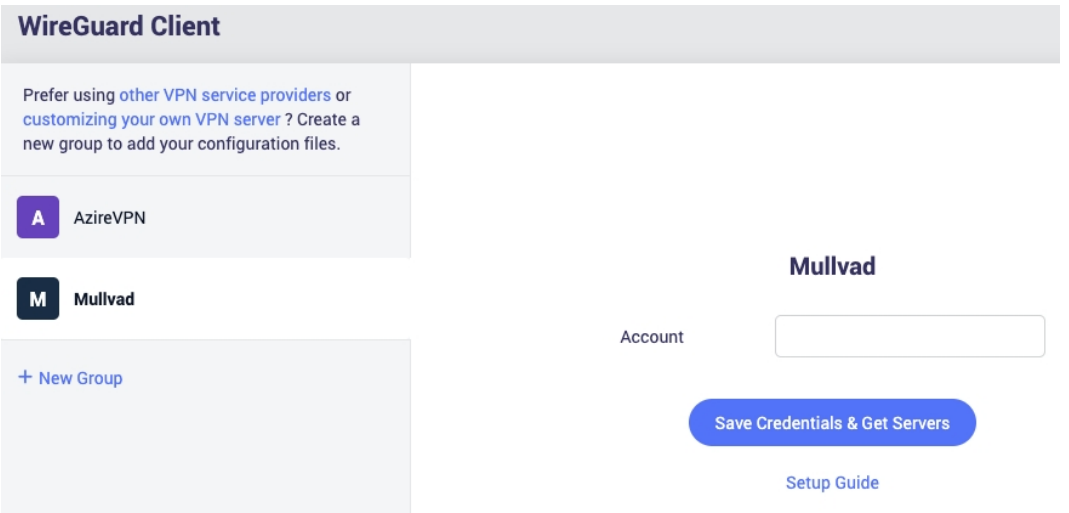
   Klicken Sie auf **Delete All**, um alle Konfigurationsdateien mit einem Klick zu löschen.



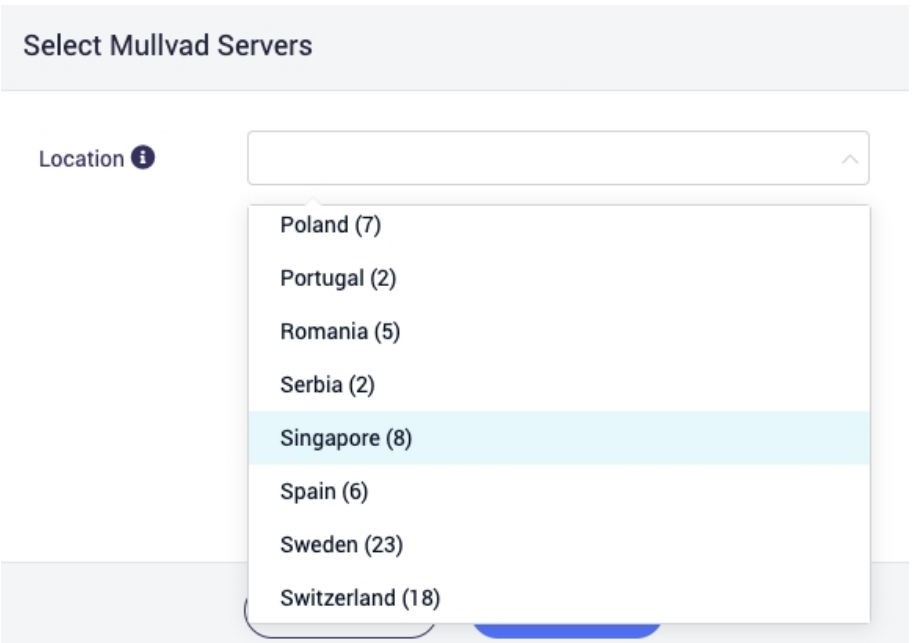
10.2.3 Mullvad einrichten

Gehen Sie wie folgt vor, um Ihren Router als Mullvad-Client einzurichten.

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Mullvad**.
2. Geben Sie Ihre Mullvad-Kontonummer (16-stellige Zahl) ein und klicken Sie auf **Save Credentials & Get Servers**.

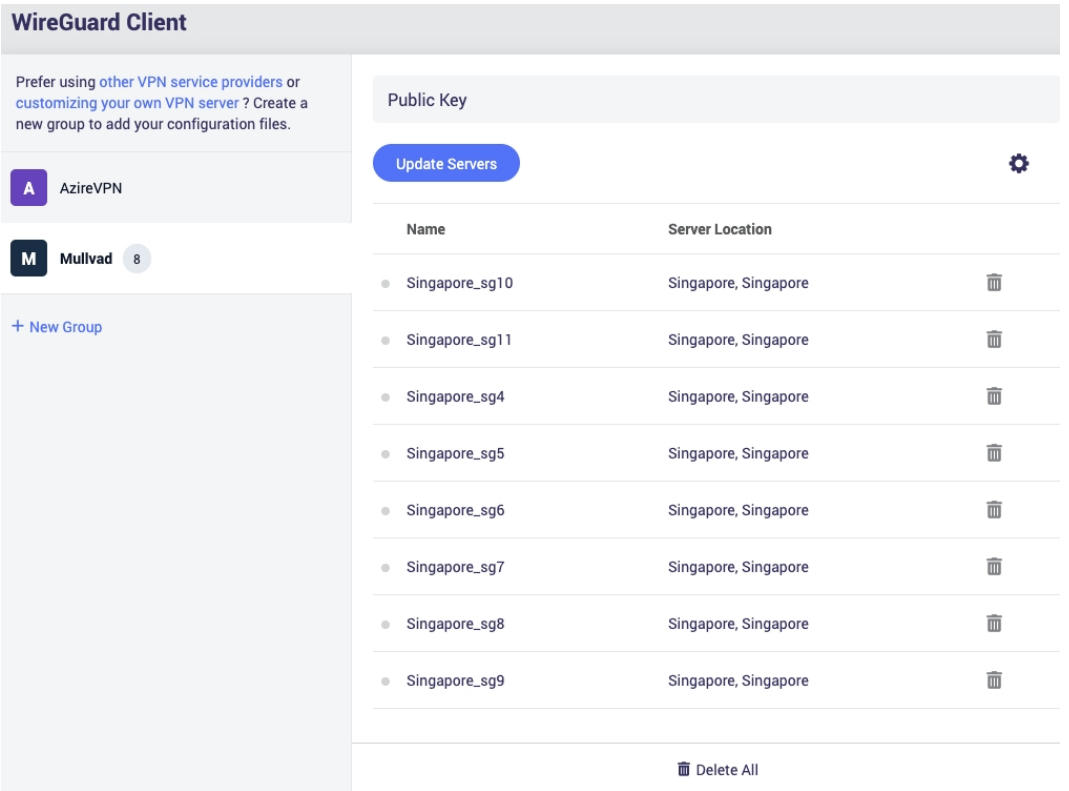


Es erscheint ein Dialog zur Standortauswahl.

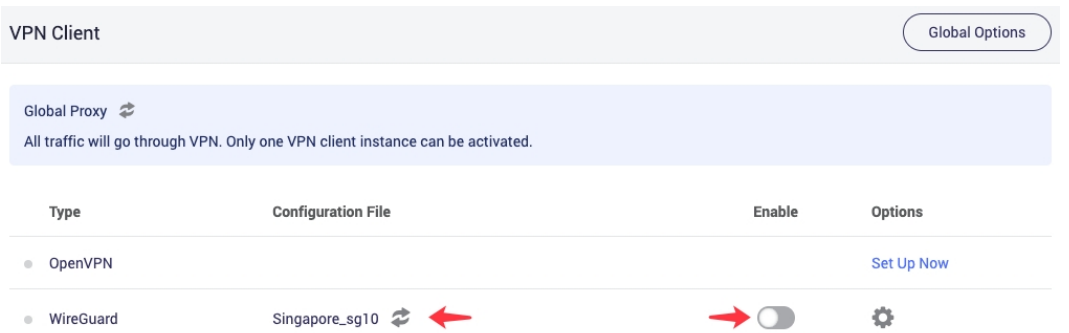


Anschließend werden die Konfigurationsdateien für den Server am ausgewählten Standort erzeugt.

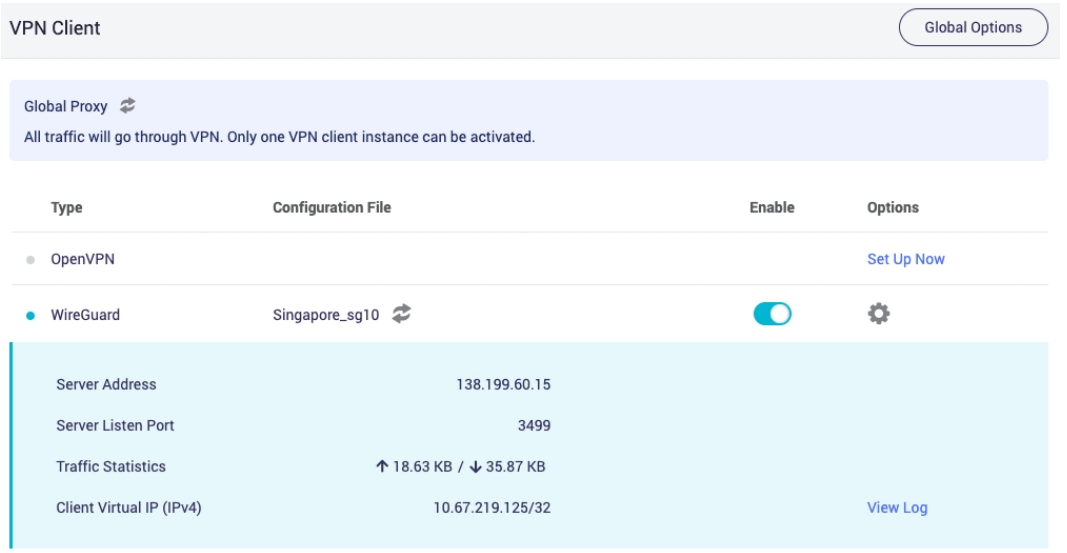
Der **Public Key** ist der öffentliche WireGuard-Schlüssel, der an den Mullvad-Server gesendet wird. Sie können bis zu fünf Schlüssel gleichzeitig verwenden und diese auf Ihrer Mullvad-Kontoseite verwalten.



3. Öffnen Sie das VPN-Dashboard, um die Verbindung zu aktivieren.

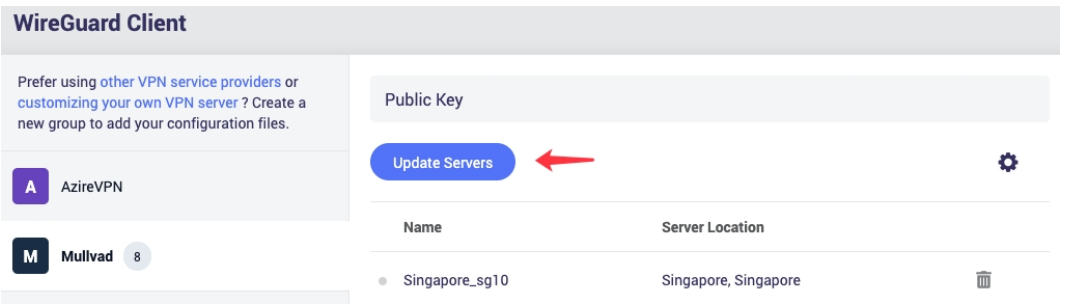


Nach erfolgreicher Verbindung werden Ihre Benutzer-IP-Adresse sowie die Anzahl der gesendeten und empfangenen Bytes angezeigt.



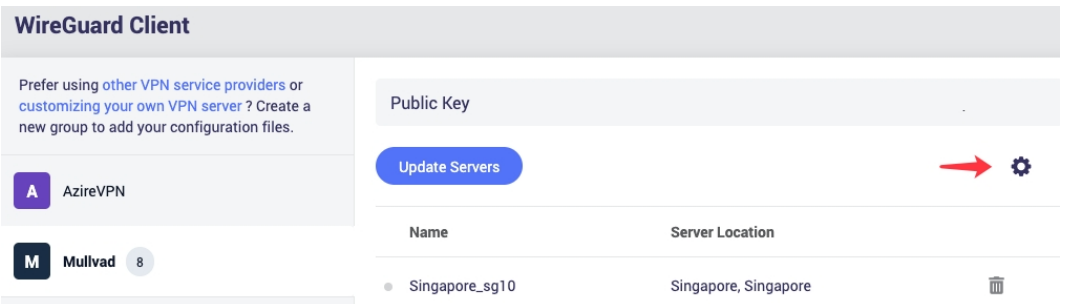
4. Server aktualisieren.

   Serverwartungen oder abgeschaltete Server bei Mullvad können Verbindungsfehler verursachen. Klicken Sie auf **Update Servers**, um die aktuelle Liste verfügbarer Server abzurufen.



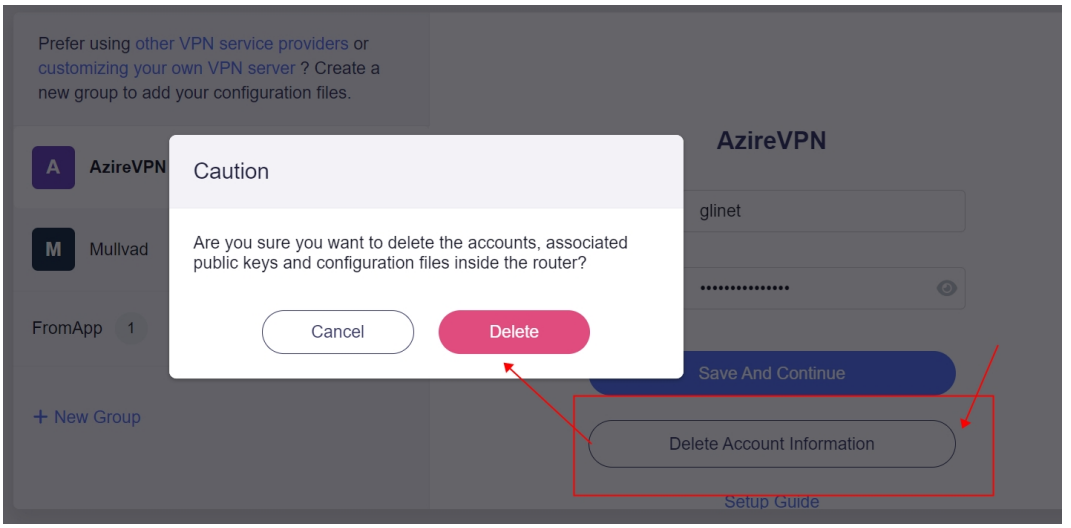
5. Zugangsdaten bearbeiten

   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten.



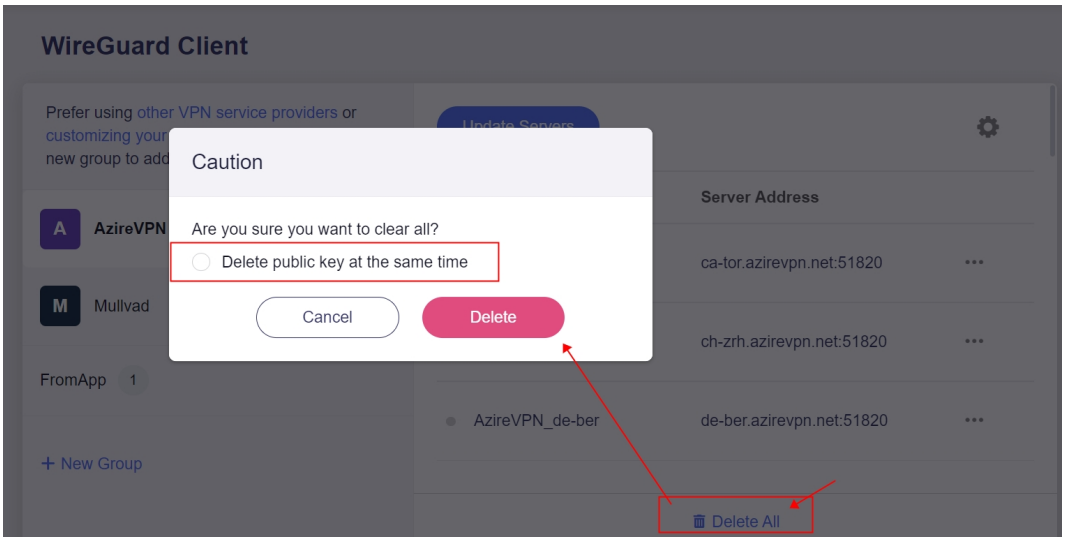
6. Kontoinformationen löschen

   Mit einem Klick auf **Delete** löschen Sie die Kontozugangsdaten, den privaten und den öffentlichen Schlüssel sowie die Konfigurationsdateien **auf dem Router**.



7. Löschen

   Sie können alle Konfigurationsdateien mit einem Klick löschen. Eine zusätzliche Abfrage ermöglicht es, auch den privaten und den öffentlichen Schlüssel zu löschen.

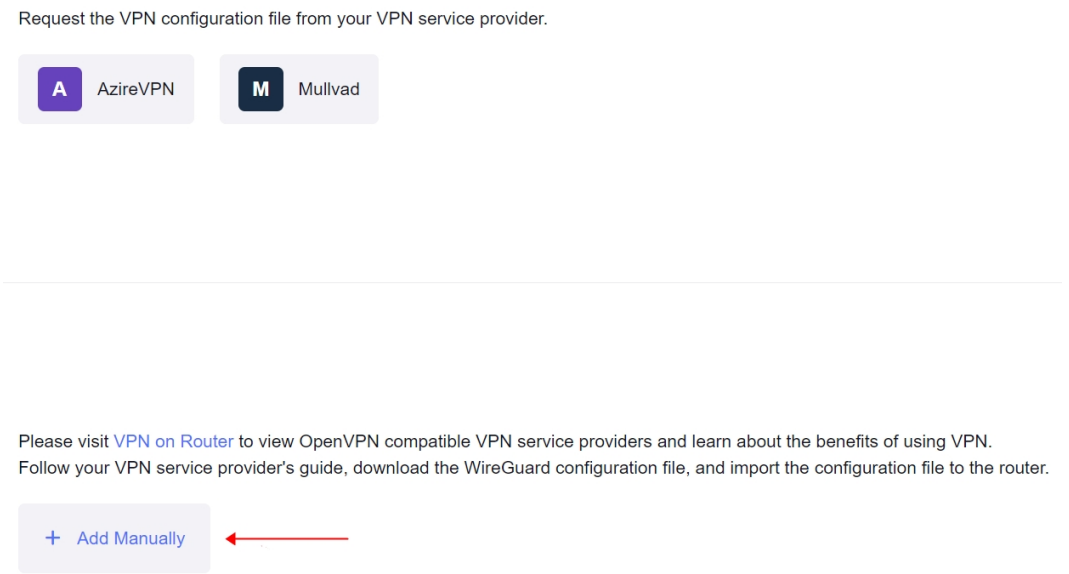


10.2.4 WireGuard-Client manuell einrichten (andere Anbieter)

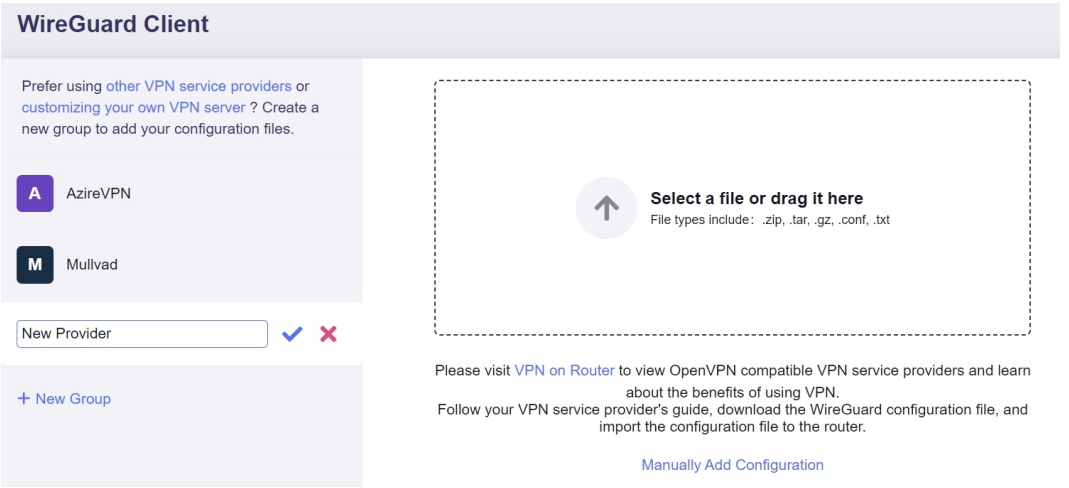
Wenn Ihr WireGuard-Anbieter nicht in die Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den WireGuard-Client einzurichten. Falls Sie nicht wissen, wie Sie die Dateien herunterladen, lesen Sie diese Anleitung oder wenden Sie sich an den Support des Anbieters.

Gehen Sie wie folgt vor, um die Konfigurationsdatei auf den Router hochzuladen und einen WireGuard-Client einzurichten.

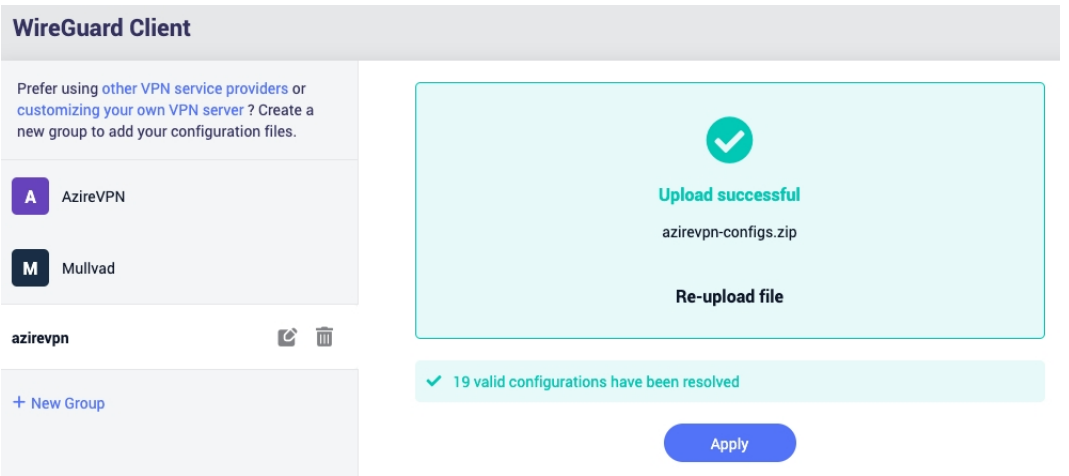
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Add Manually**.



2. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.

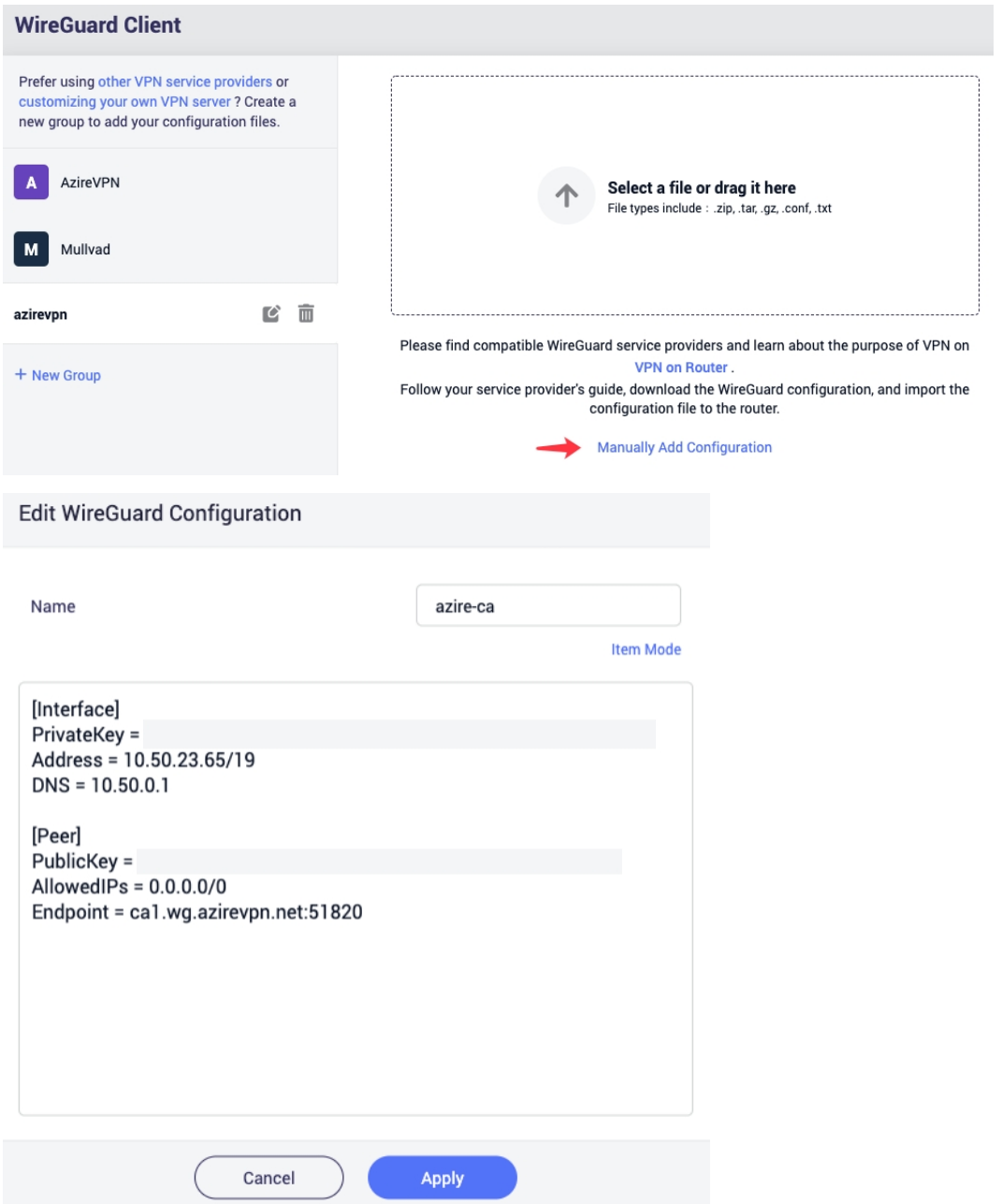


3. Klicken Sie auf den Upload-Bereich, laden Sie Ihre WireGuard-Konfigurationsdatei hoch und klicken Sie auf **Apply**. Unterstützte Formate: zip, tar, gz, conf und txt.

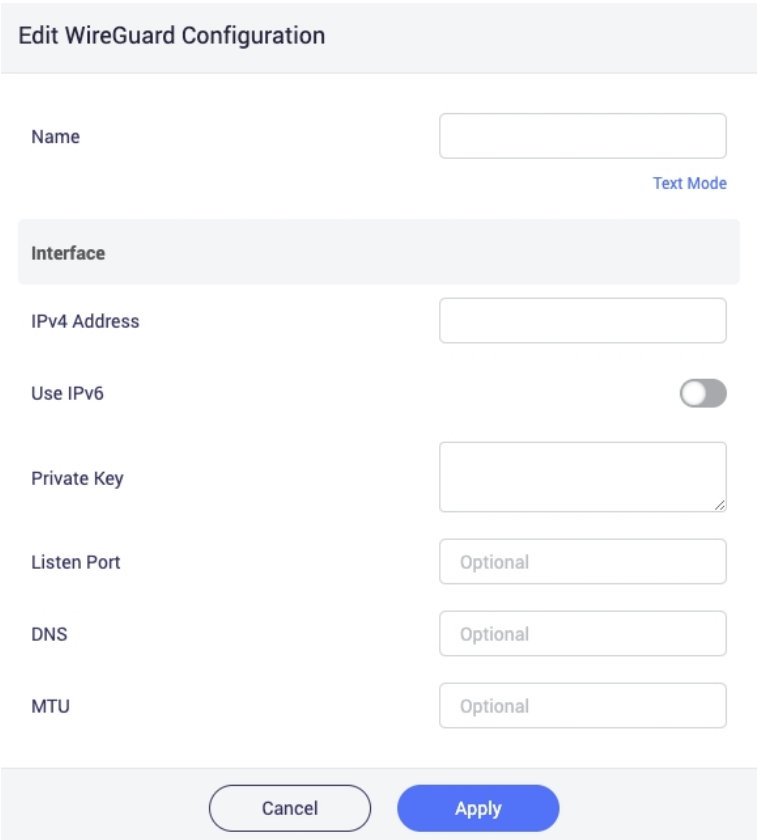


Wenn Sie ein Archiv mit mehreren Konfigurationsdateien hochladen, wird es automatisch entpackt.

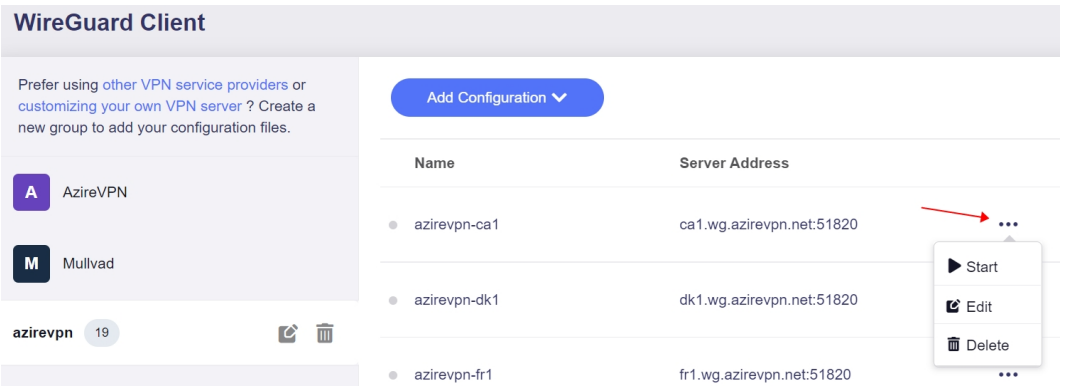
Alternativ klicken Sie unten im Upload-Bereich auf **Manually Add Configuration**, geben die Konfiguration als Text ein und klicken auf **Apply**.



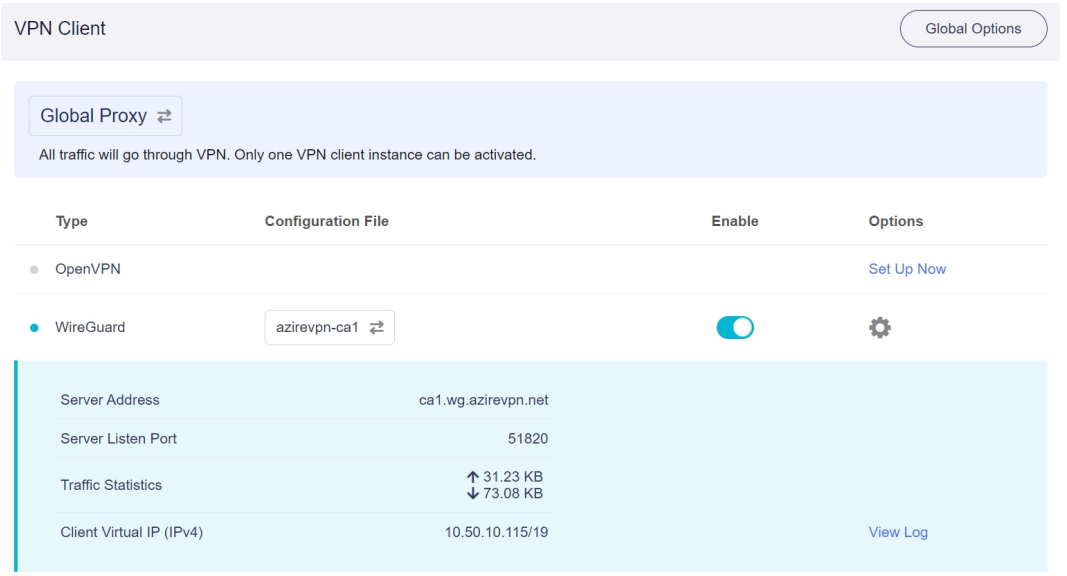
Um die einzelnen Einträge zu prüfen, wechseln Sie in den Modus Item und kontrollieren Sie die Konfigurationsdetails. Klicken Sie anschließend auf **Apply**.



4. Klicken Sie rechts auf das Dreipunktsymbol, um die Verbindung zu starten.



5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt. Details zur VPN-Verbindung finden Sie im **VPN Dashboard**.


VPN Client
Global Options
Global Proxy
All traffic will go through VPN. Only one VPN client instance can be activated.
Type
Configuration File
Enable
Options
OpenVPN
Set Up Now
WireGuard
azirevpn-ca1
Server Address
ca1.wg.azirevpn.net
Server Listen Port
51820
Traffic Statistics
31.23 KB
73.08 KB
Client Virtual IP (IPv4)
10.50.10.115/19
View Log

Kapitel 11

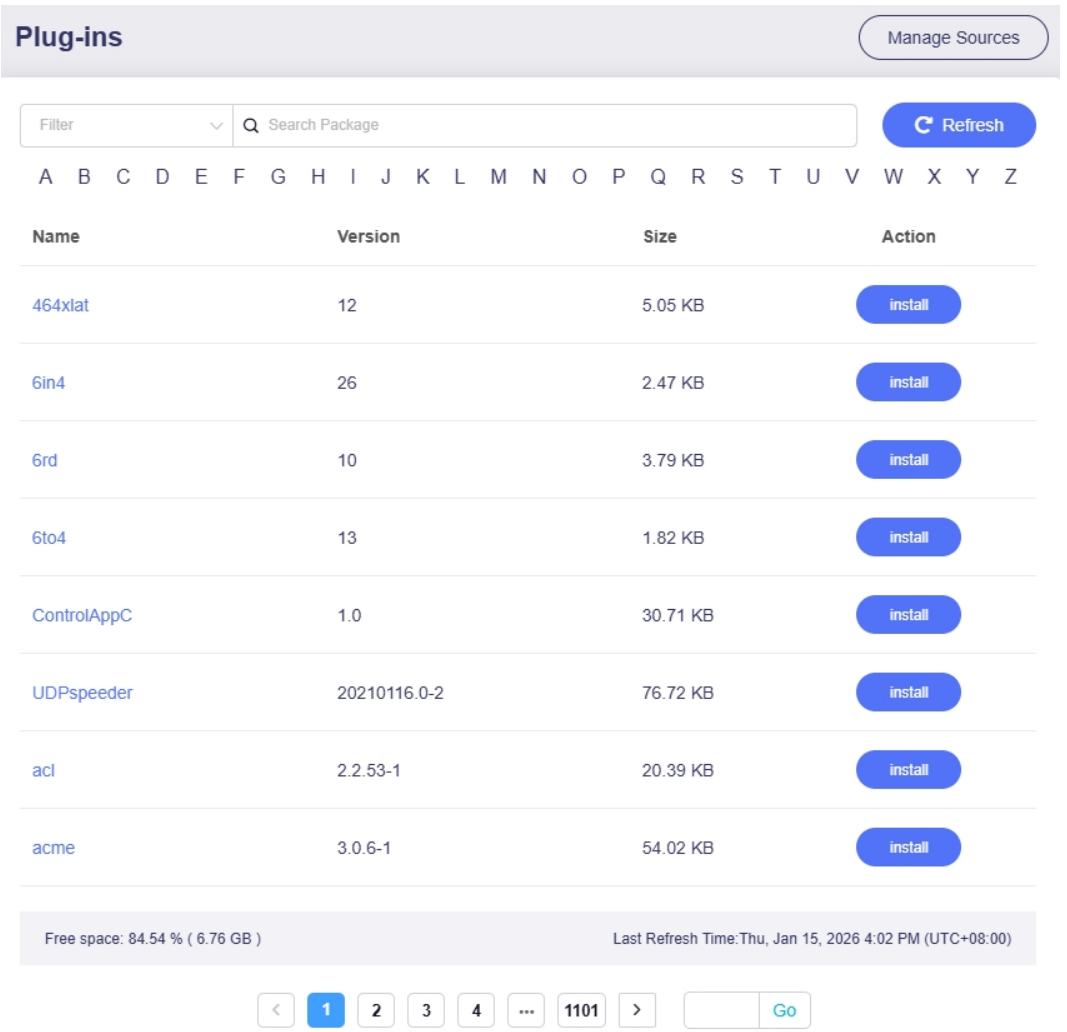
Anwendungen

Dieses Kapitel stellt Anwendungen auf GL.iNet-Routern vor, darunter Plug-ins, Dynamic DNS und GoodCloud.

11.1 Plug-ins

Auf der Seite Plug-ins können Sie OpenWrt-Pakete verwalten.

Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Plug-ins.** Sie können die im Repository verfügbaren Pakete installieren oder entfernen. Klicken Sie vor der Installation auf **Refresh**, um die Paketliste zu aktualisieren.



Hinweis:

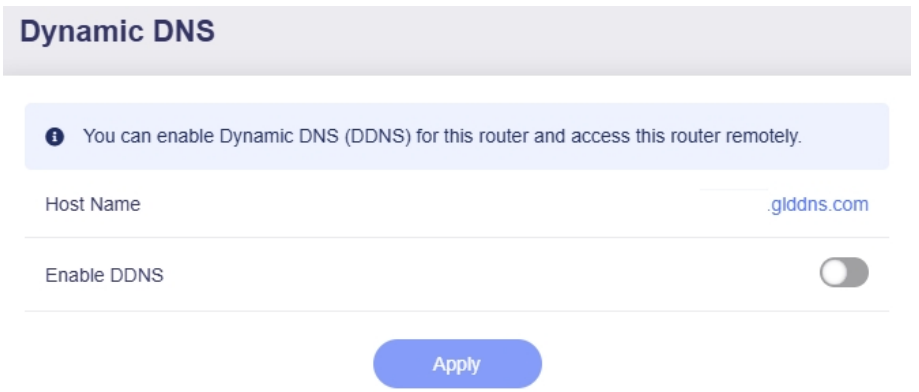
1. Es wird davon abgeraten, in der offiziellen GL.iNet-Firmware vorinstallierte Plug-ins wie nginx zu aktualisieren.
2. Manuell installierte Plug-ins von Drittanbietern können aktualisiert werden. GL.iNet haftet jedoch nicht für Sicherheitsprobleme durch solche Plug-ins. Wenden Sie sich bei Fragen an die jeweiligen Entwickler.

11.2 Dynamisches DNS

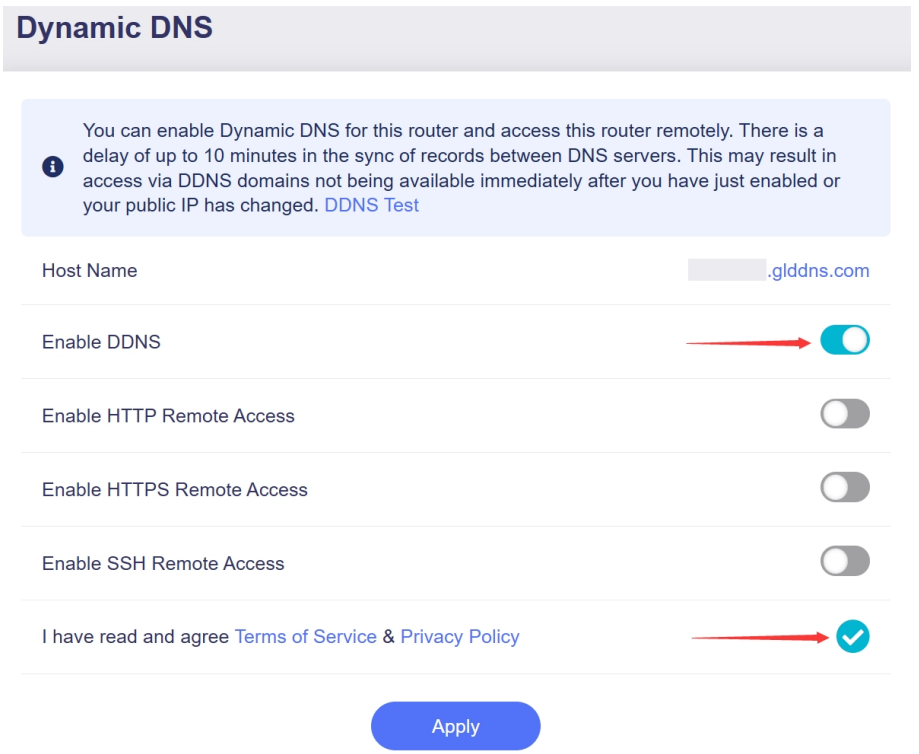
Dynamic DNS (DDNS) ordnet einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zu. Damit können Sie aus der Ferne auf Ihren Router zugreifen. Für diese Funktion ist eine öffentliche IP-Adresse erforderlich.

11.2.1 DDNS aktivieren

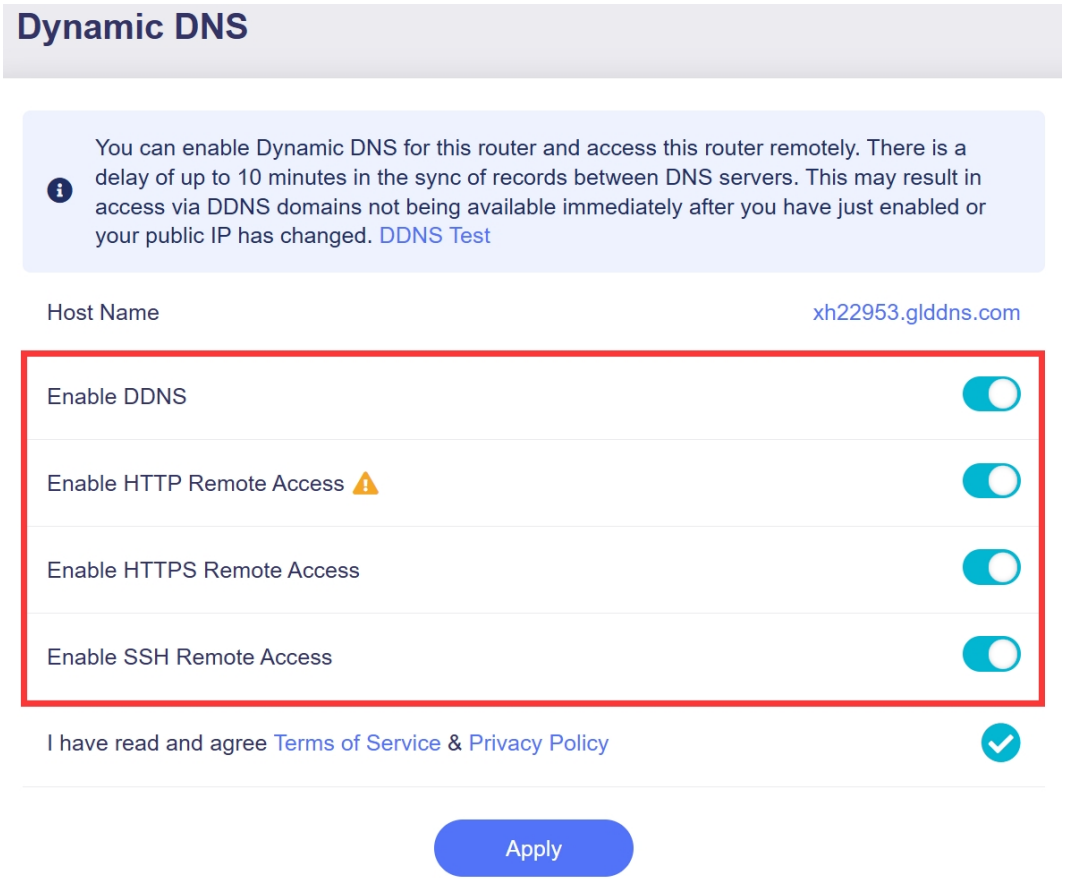
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Dynamic DNS**. Die folgende Seite wird angezeigt.



2. Aktivieren Sie **Enable DDNS**, lesen und akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



3. Wenn Sie Fernzugriff benötigen, aktivieren Sie auf dieser Seite die gewünschten Dienste: **HTTP**, **HTTPS** und **SSH**.



Hinweis:

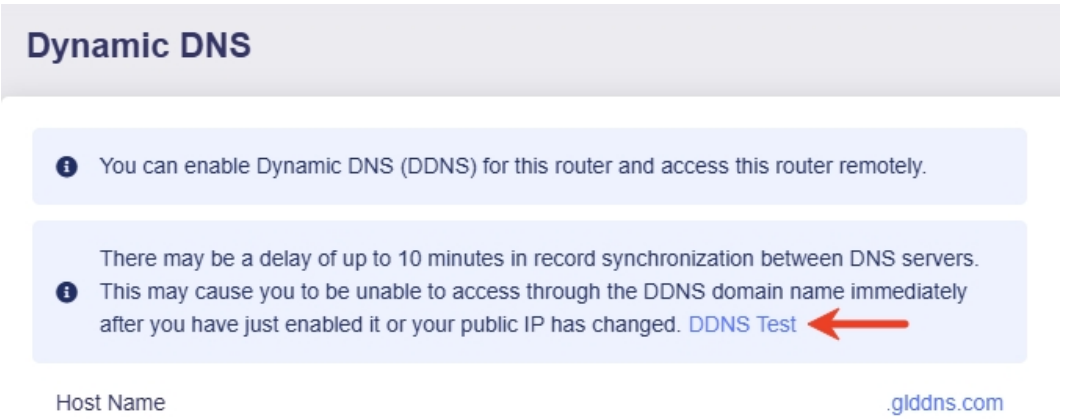
1. Die Synchronisierung der Einträge zwischen DNS-Servern kann bis zu zehn Minuten dauern. Deshalb kann der Zugriff über den DDNS-Domainnamen direkt nach der Aktivierung oder nach einer Änderung Ihrer öffentlichen IP-Adresse vorübergehend nicht möglich sein.
2. Wenn Sie DDNS und einen VPN-Client gleichzeitig verwenden, stellen Sie sicher, dass Services From GL.iNet Use VPN deaktiviert ist.

11.2.2 DDNS-Funktion prüfen

Sie können DDNS mit dem integrierten Testwerkzeug oder manuell über Befehle prüfen.

Methode 1: DDNS-Testwerkzeug verwenden

1. Klicken Sie auf der Seite Dynamic DNS auf **DDNS Test**.



2. Prüfen Sie, ob die per DDNS aufgelöste IP-Adresse mit der WAN-IP-Adresse des Routers übereinstimmt. Andernfalls erscheint oben ein gelber Hinweis: Der Router befindet sich möglicherweise hinter NAT, und Sie müssen auf dem vorgeschalteten Router eine Portweiterleitung einrichten.



Methode 2: Befehle verwenden

1. Verwenden Sie den Befehl *nslookup xxxxxxx.glddns.com 8.8.8.8*, um die Zuordnung zwischen Domainname und IP-Adresse wie unten dargestellt abzufragen.



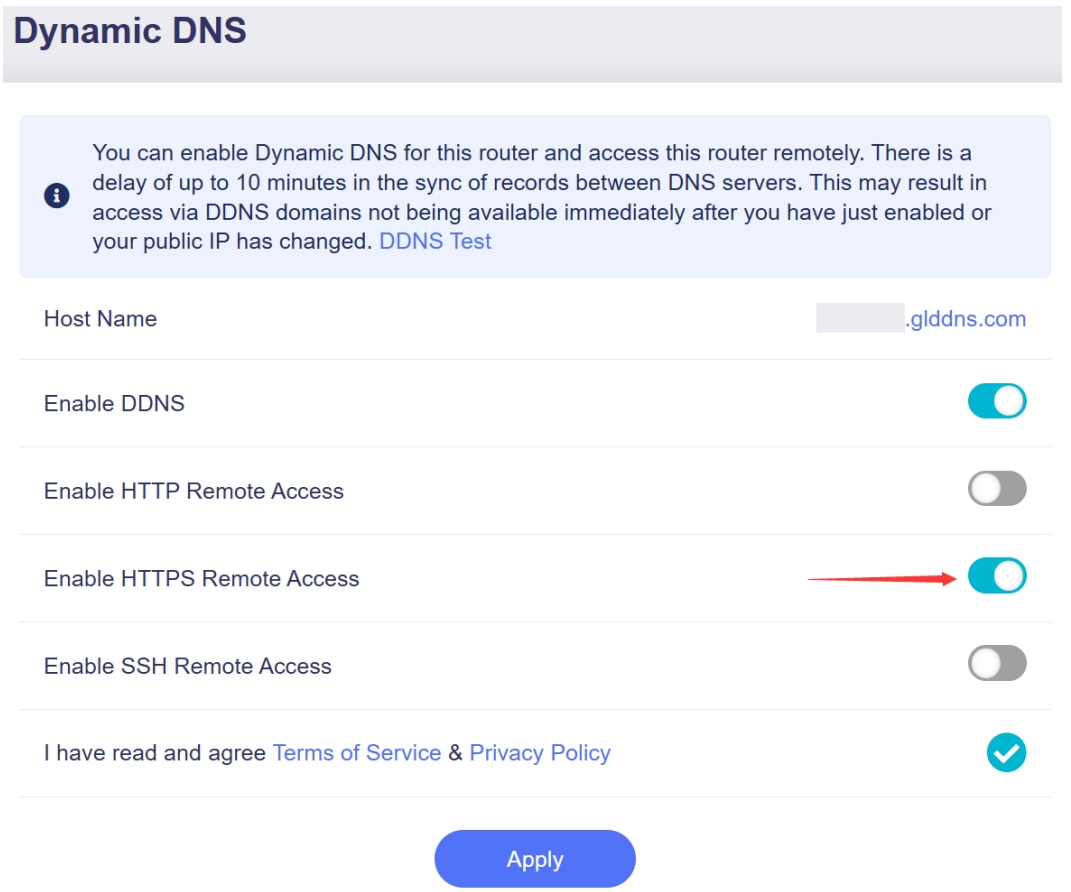
   - Ersetzen Sie „xxxxxxx.glddns.com“ in der obigen Abbildung durch Ihren Hostnamen.
   - „8.8.8.8“ ist ein DNS-Server von Google. Verwenden Sie diesen oder ersetzen Sie ihn durch einen anderen DNS-Server und drücken Sie die Eingabetaste.
2. Wenn eine öffentliche IP-Adresse wie „183.178.10.100“ in der obigen Abbildung angezeigt wird, wurde Ihre DDNS-Domain erfolgreich einer öffentlichen IP-Adresse zugeordnet. Eine Meldung wie „server can’t find xxxxxxx.glddns.com“ kann bedeuten, dass die Namensauflösung fehlgeschlagen ist und die Zuordnung nicht erfolgreich war. Prüfen Sie dies im nächsten Schritt.
3. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET**. Suchen Sie bei der aktuell aktiven Schnittstelle die WAN-IP-Adresse Ihres Routers. Vergleichen Sie diese mit der oben ermittelten öffentlichen IP-Adresse. Stimmen beide überein, funktioniert DDNS; andernfalls nicht.

11.2.3 HTTP-Fernzugriff

Für den HTTP-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 80** ein.

Gehen Sie wie folgt vor, um den HTTP-Fernzugriff auf Ihren Router zu aktivieren.

1. Aktivieren Sie auf der Seite Dynamic DNS **Enable DDNS** und **HTTP Remote Access**, akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



2. Nach der Aktivierung können Sie die Weboberfläche von überall über den DDNS-Hostnamen per HTTP aufrufen, etwa unter **http://xxxxxxx.glddns.com**. Bei eingerichteter Portweiterleitung verwenden Sie **http://xxxxxxx.glddns.com:external_port** und ersetzen external_port durch die tatsächliche Portnummer.

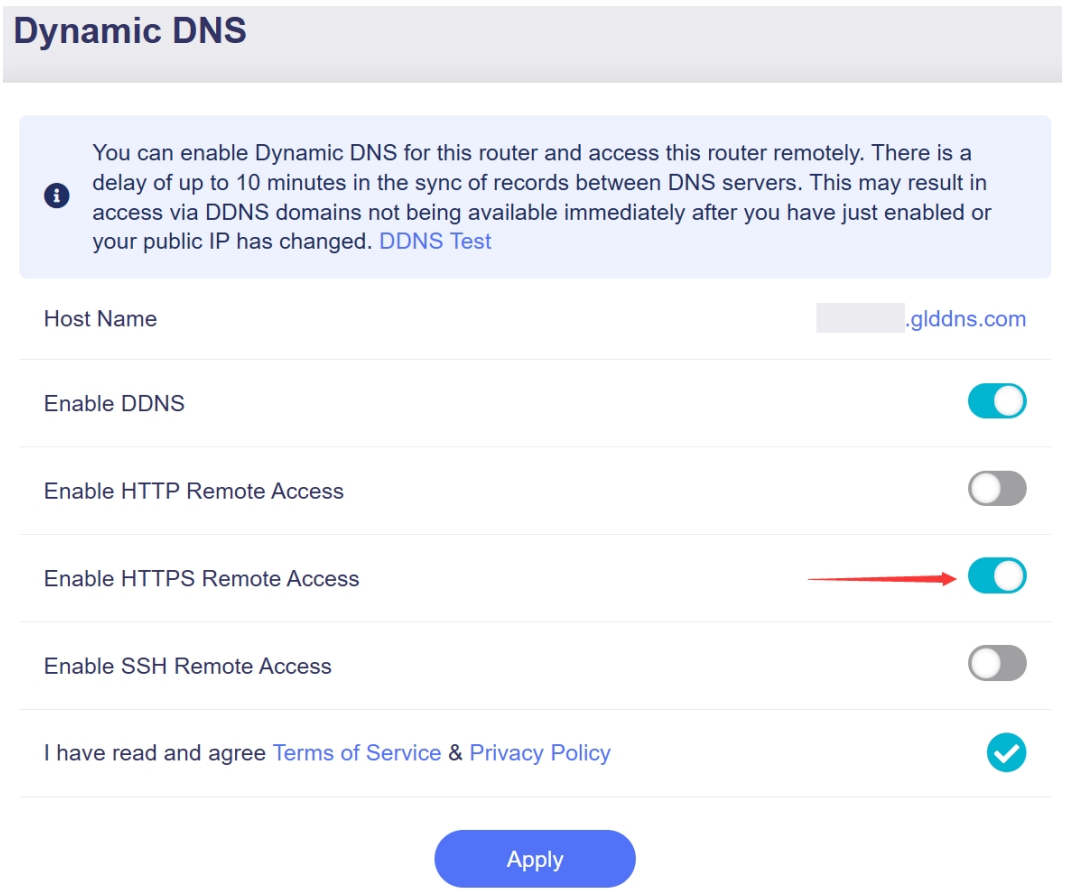
Hinweis: HTTP ist unverschlüsselt. Alle übertragenen Daten einschließlich Ihrer Zugangsdaten werden im Klartext gesendet. Dies birgt Sicherheitsrisiken. Verwenden Sie den HTTP-Fernzugriff mit Bedacht.

11.2.4 HTTPS-Fernzugriff

Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 443** ein.

Gehen Sie wie folgt vor, um den HTTPS-Fernzugriff auf Ihren Router zu aktivieren.

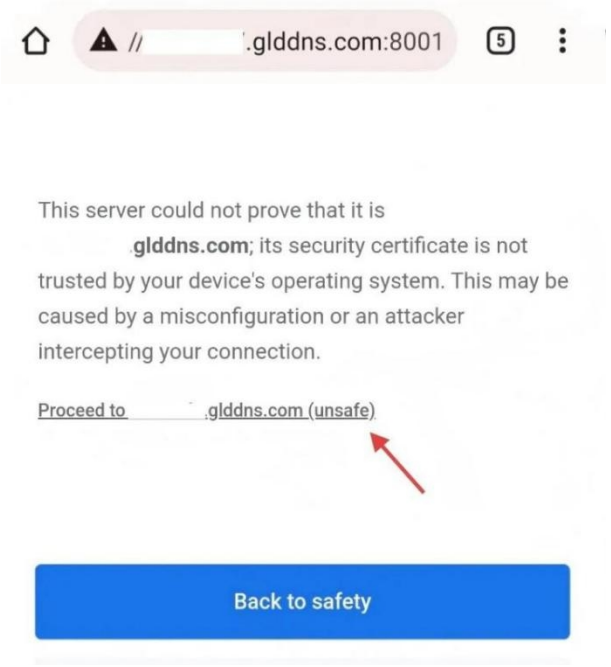
1. Aktivieren Sie auf der Seite Dynamic DNS **Enable DDNS** und **HTTPS Remote Access**, akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



2. Nach der Aktivierung können Sie die Weboberfläche von überall über den DDNS-Hostnamen per HTTPS aufrufen, etwa unter **https://xxxxxxx.glddns.com**. Bei eingerichteter Portweiterleitung verwenden Sie **https://xxxxxxx.glddns.com:external_port** und ersetzen external_port durch die tatsächliche Portnummer.

Hinweis: Diese Funktion verwendet selbstsignierte Zertifikate. Deshalb zeigt der Browser beim HTTPS-Zugriff über den DDNS-Hostnamen die Meldung „Ihre Verbindung ist nicht

privat“ an. Klicken Sie unten auf **Erweitert** und anschließend auf **Weiter zu xxxxxxx.glddns.com** , um den HTTPS-Fernzugriff fortzusetzen.



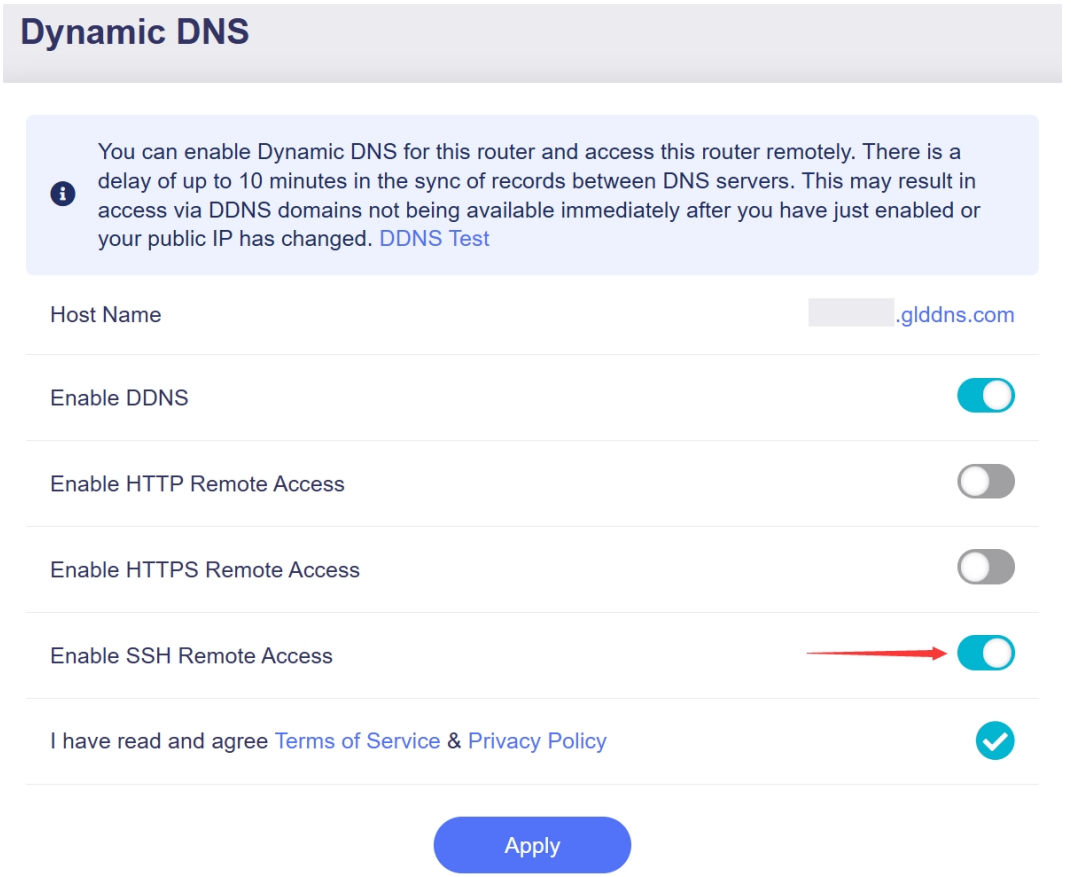
Sie können nun über den DDNS-Hostnamen per **HTTPS** auf die Weboberfläche des Routers zugreifen.

11.2.5 SSH-Fernzugriff

Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 22** ein.

Gehen Sie wie folgt vor, um den SSH-Fernzugriff auf Ihren Router zu aktivieren.

1. Aktivieren Sie auf der Seite Dynamic DNS **Enable DDNS** und **SSH Remote Access**, akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



Nach der Aktivierung können Sie von überall über den DDNS-Hostnamen per SSH auf den Router zugreifen, etwa mit **ssh root@xxxxxxx.glddns.com**. Bei eingerichteter Portweiterleitung verwenden Sie **ssh root@xxxxxxx.glddns.com:external_port** und ersetzen external_port durch die tatsächliche Portnummer.

11.3 GoodCloud

GL.iNet GoodCloud vereinfacht die Bereitstellung und Verwaltung vernetzter Geräte aus der Ferne. Die Plattform ermöglicht den einfachen Fernzugriff auf GL.iNet-Router. Durch die zentrale Verwaltung in der Cloud können Sie mehrere Netzwerkgeräte effizient gemeinsam konfigurieren oder deren Software aktualisieren. Außerdem können Sie die Weboberfläche des Routers aus der Ferne öffnen oder per SSH auf sein Terminal zugreifen. So lassen sich Netzwerkgeräte standortübergreifend und durchgängig verwalten.

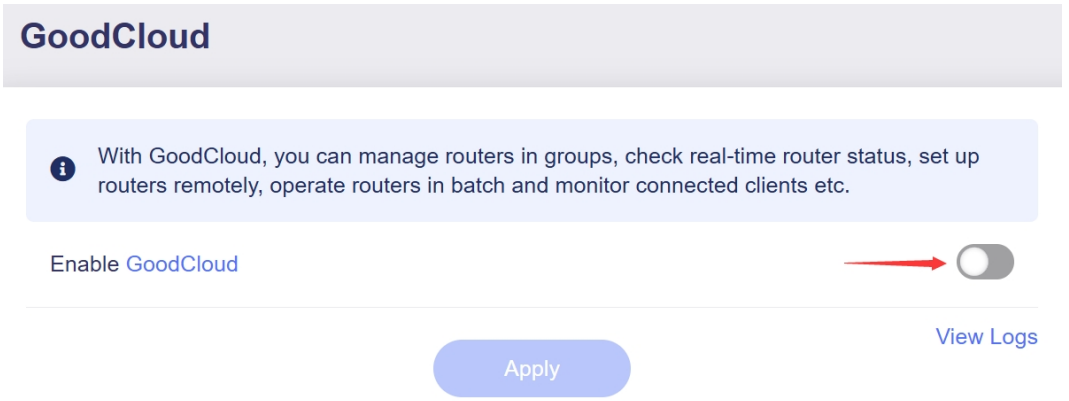
Mit GoodCloud können Sie:

- Den Routerstatus in Echtzeit prüfen
- Gruppen von Routern verwalten
- Router aus der Ferne einrichten
- Verbundene Geräte überwachen
- Aktionen auf mehreren Routern gleichzeitig ausführen
- Standortvernetzungen einrichten

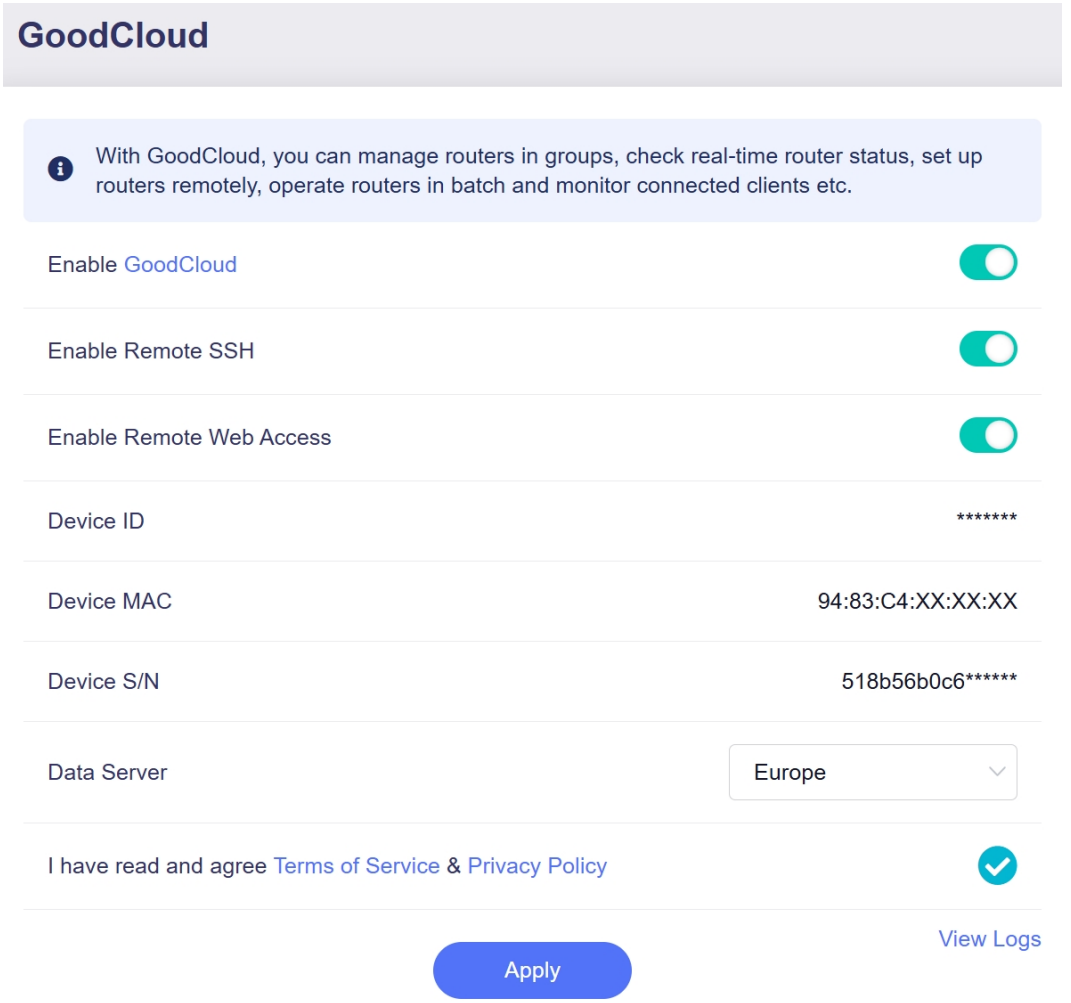
Einige Funktionen sind im Enterprise-Tarif und im VAR-Tarif (Value Added Reseller) verfügbar. Weitere Informationen finden Sie hier.

11.3.1 GoodCloud aktivieren

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **GoodCloud**. Aktivieren Sie GoodCloud mit dem Schalter.

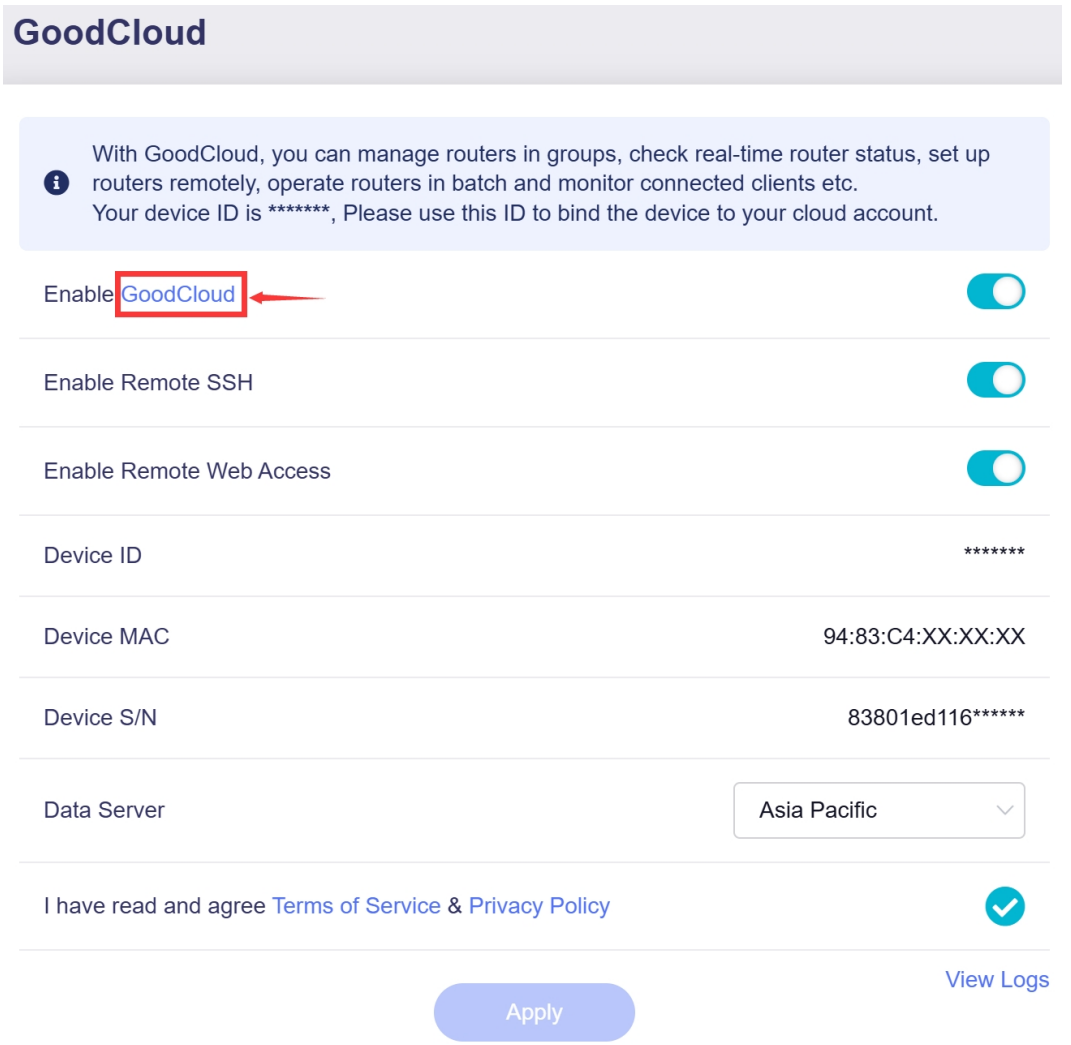


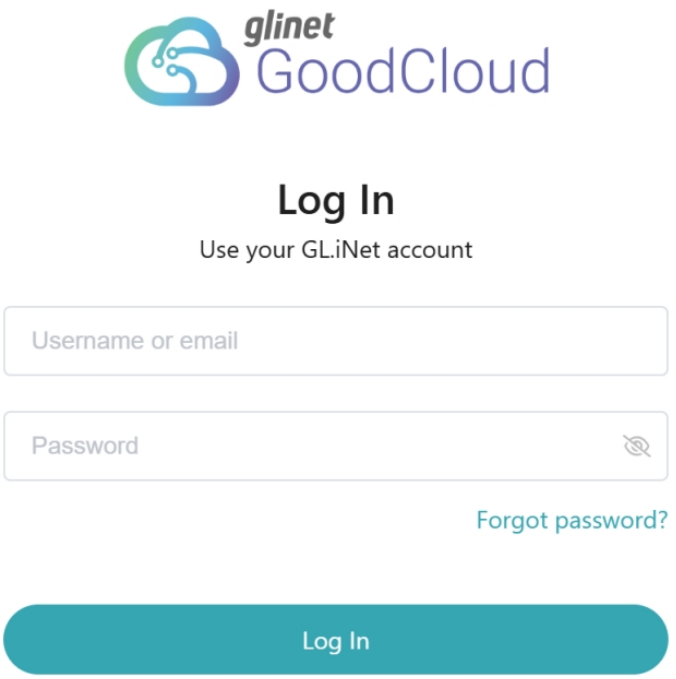
   Aktivieren Sie bei Bedarf **Remote SSH** und **Remote Web Access**. Wählen Sie den nächstgelegenen Server aus, lesen und akzeptieren Sie die **Terms of Service & Privacy Policy** und klicken Sie auf **Apply**.



- **Remote SSH:** Ermöglicht den Fernzugriff auf das Routerterminal per SSH über die GoodCloud-Plattform.
- **Remote Web Access:** Ermöglicht den Fernzugriff auf die Weboberfläche des Routers per HTTP/HTTPS über die GoodCloud-Plattform.
- **Data Server:** Wählen Sie den Server aus, der dem Standort Ihres Geräts am nächsten liegt. Zur Auswahl stehen Asien-Pazifik (Japan), Amerika (Oregon) und Europa (Irland).
- **View Logs**: Öffnet die Protokollseite und zeigt das Cloud-Protokoll an.

2. Klicken Sie auf GoodCloud, um die Anmeldeseite zu öffnen, und melden Sie sich mit Ihrem GL.iNet-Cloud-Konto an. Falls Sie noch kein Konto haben, registrieren Sie sich zuerst. Nach der Anmeldung wird der Router automatisch Ihrem Konto zugeordnet.

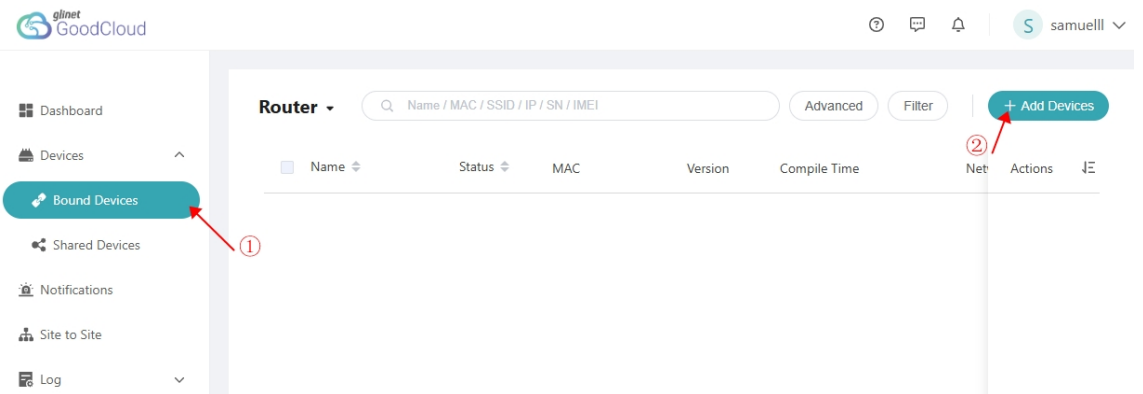

GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is *******, Please use this ID to bind the device to your cloud account.
Enable GoodCloud
Enable Remote SSH
Enable Remote Web Access
Device ID
****
Device MAC
94:83:C4:XX:XX:XX
Device S/N
83801ed116******
Data Server
Asia Pacific
I have read and agree Terms of Service & Privacy Policy
View Logs
Apply



Tipps:

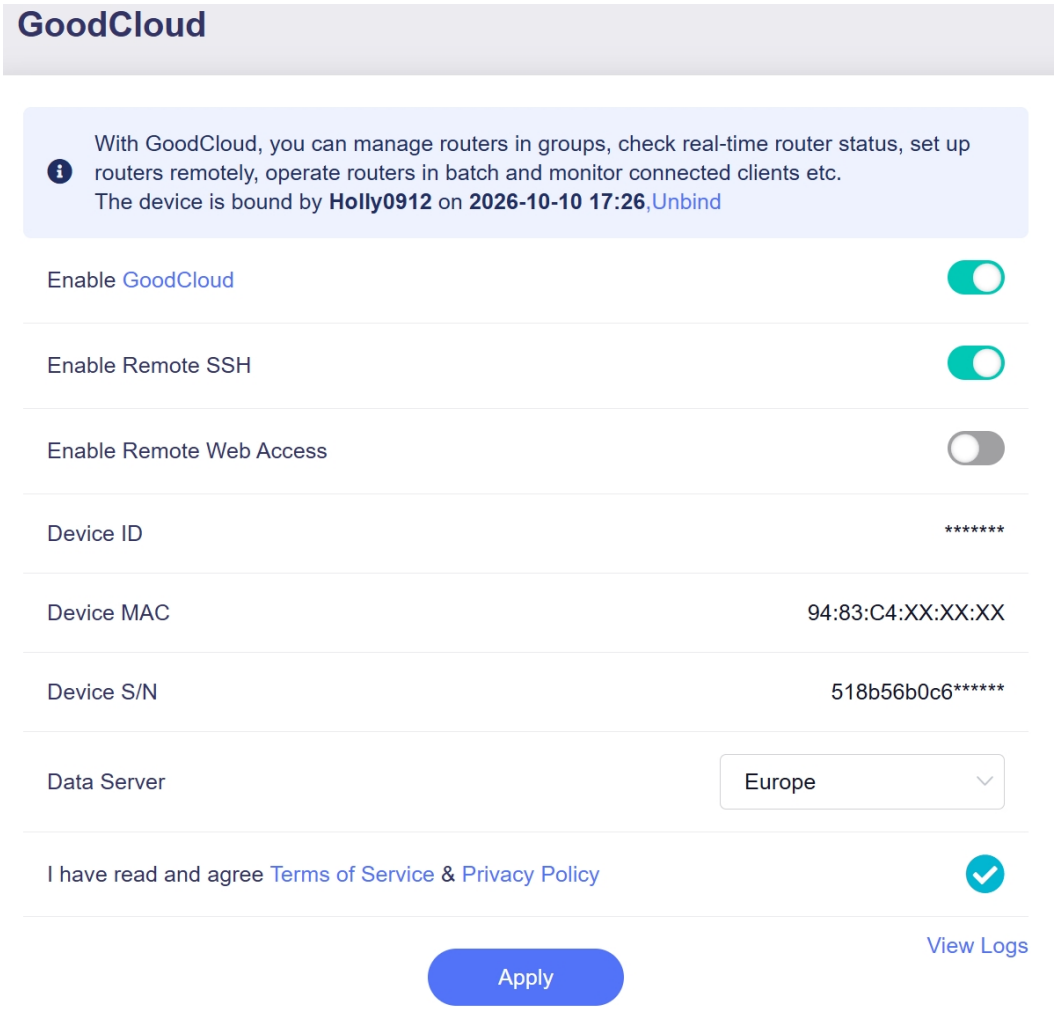
- Die Schritte zur Verknüpfung mit GoodCloud unterscheiden sich je nach Firmwareversion.
- Falls Sie keine Bestätigungs-E-Mail erhalten, prüfen Sie Ihren Spamordner oder versuchen Sie es später erneut. Weitere Unterstützung erhalten Sie unter support@gl-inet.com.

3. Öffnen Sie auf der Cloud-Plattform **Devices** > **Bound Devices** > **Add Devices**.



Sie können ein Gerät auf drei Arten mit Ihrem GoodCloud-Konto verknüpfen: Auto Discover, Manually Add und Bulk Import. Weitere Einzelheiten finden Sie hier.

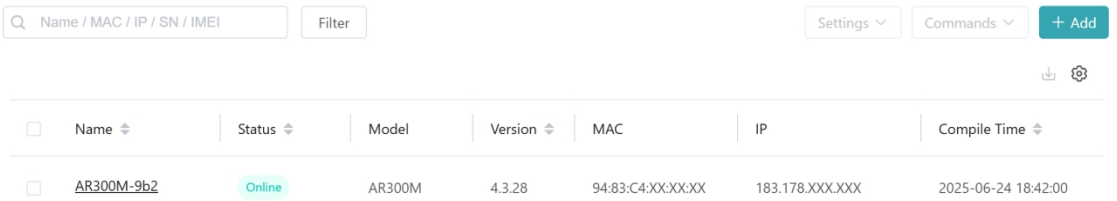
4. Kehren Sie nach erfolgreicher Verknüpfung zur Weboberfläche des Routers zurück und öffnen Sie **APPLICATIONS** > **GoodCloud**. Auf dieser Seite erscheinen die Verknüpfungsdaten, darunter Benutzername und Zeitpunkt.



11.3.2 Router verwalten

Gerätedetails prüfen

Melden Sie sich bei GoodCloud an und öffnen Sie **Devices** > **Bound Devices**. Dort sehen Sie grundlegende Geräteinformationen wie Hostname, Status (online/offline), Modell, Firmwareversion und MAC-Adresse.



Klicken Sie auf den Gerätenamen, um die Detailseite zu öffnen. Diese enthält grundlegende Informationen, Statistiken, eine Netzwerkübersicht, die Geräteliste und eine Zeitleiste. Außerdem können Sie erweiterte Aktionen ausführen, etwa aus der Ferne auf den Router zugreifen oder ihn neu starten.

AR300M-9b2 Online

Remote GUI | Remote SSH | Reboot Device

Basic Info

Refresh



AR300M

Network Mode	Version	MAC Address	IP
Router	4.3.28	94:83:C4:XX:XX:XX	183.178.XXX.XXX
SN	**Memory Usage**	**Compile Time**	**Up Time**
518b**********	31%	2025-06-24 18:42:00	0 days 0 hrs 44 mins

Statistical Data

Refresh

Network Latency

Retest

Poor

241.61 ms Latency | 2.27 ms Jitter | 0 % Packet Loss

Device Status History

More



Network | Clients List | Share | Cellular Health

Internet

Refresh

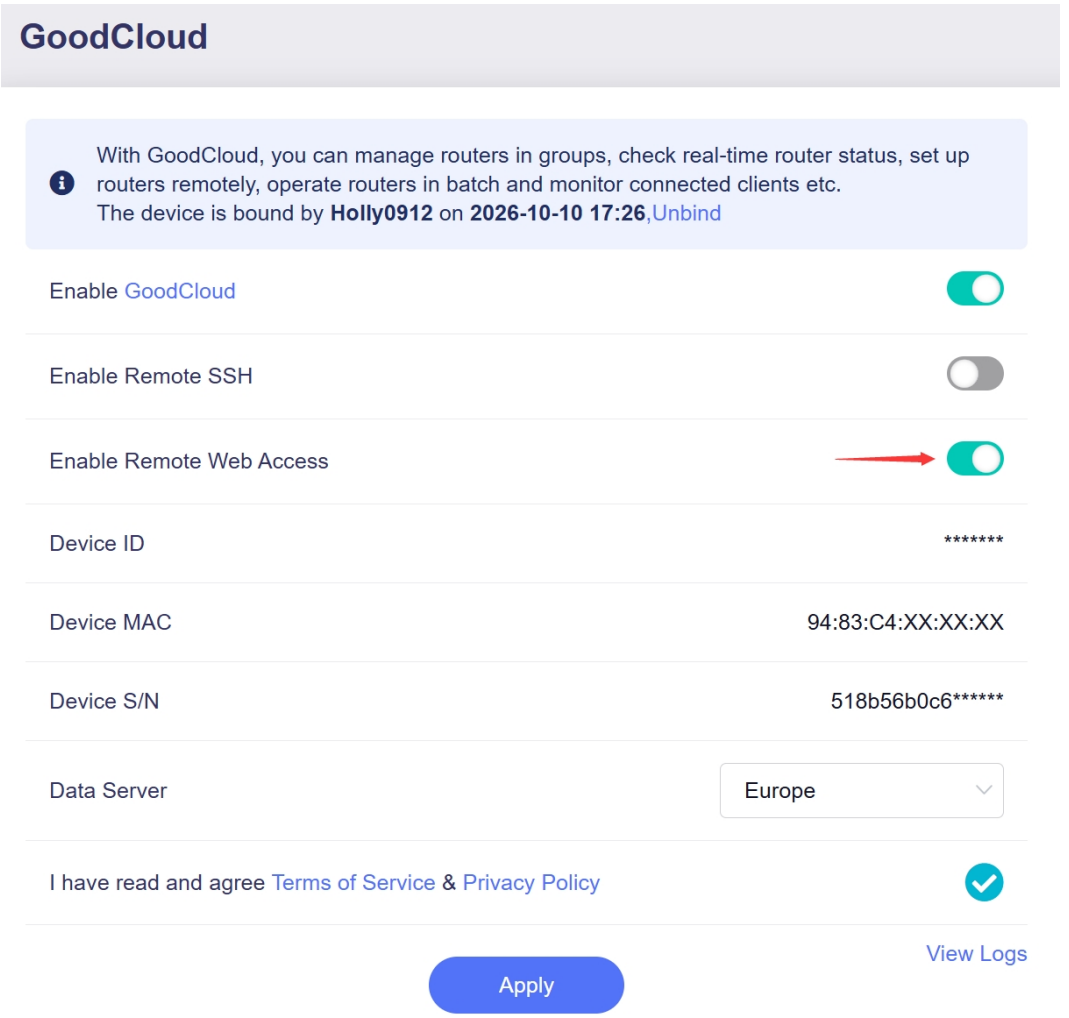
Ethernet1 More
✓ Connected
IP Address 10.100.210.196/22
Protocol DHCP

Repeater More
Disabled
IP Address --
SSID --

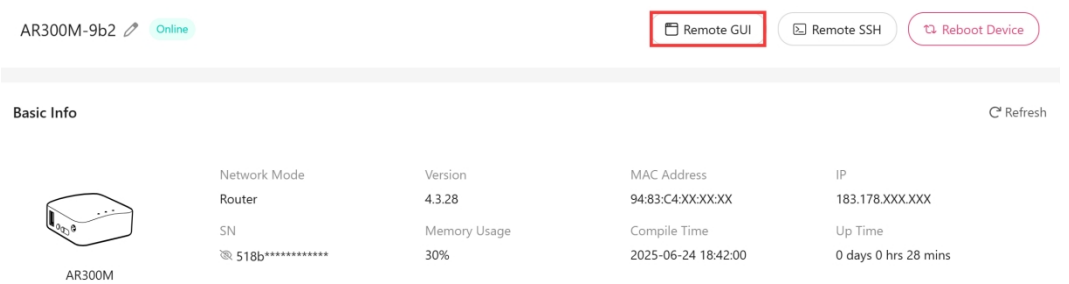
Tethering More
Disabled
IP Address --
Device List Details

Fernzugriff auf die Weboberfläche

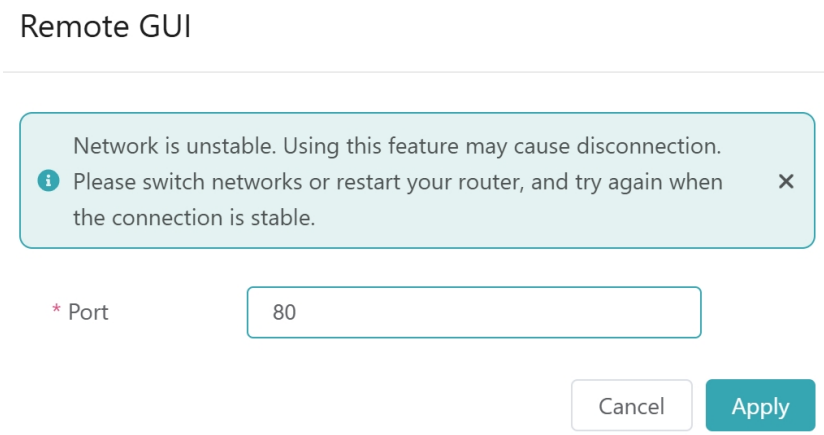
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **APPLICATIONS** > **GoodCloud**, aktivieren Sie **Remote Web Access** und klicken Sie auf **Apply**.



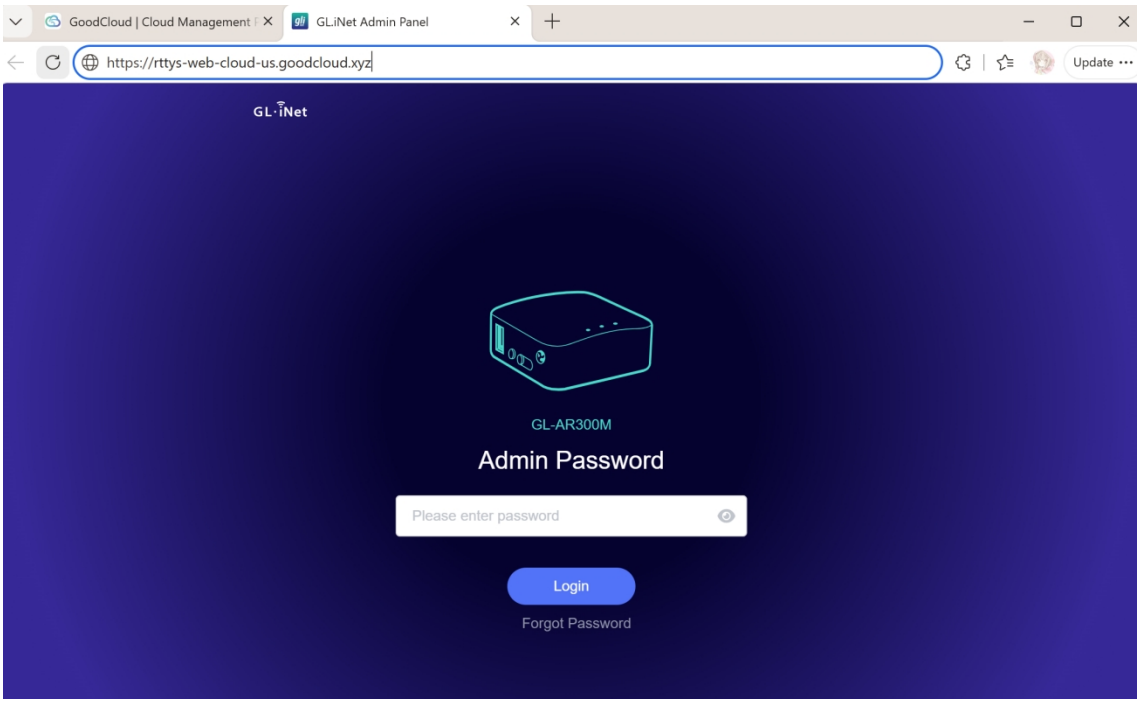
2. Melden Sie sich bei GoodCloud an und öffnen Sie **Devices** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote GUI**.



4. Wählen Sie Übertragungsprotokoll und Port aus. Standardmäßig sind **HTTP** und Port **80** eingestellt. Bei Bedarf können Sie zu HTTPS wechseln; der Port wird dann automatisch auf 443 geändert. Klicken Sie anschließend auf **Apply**.

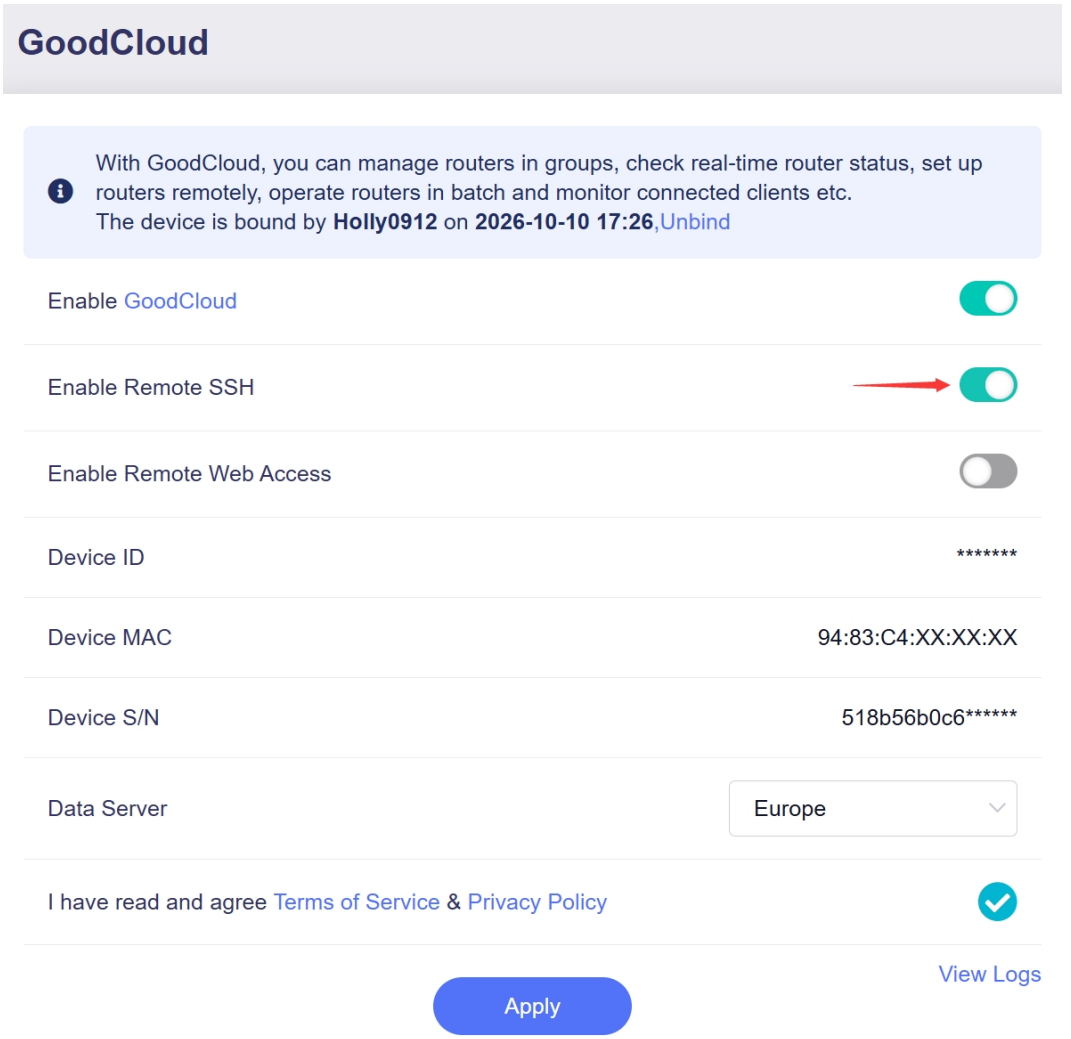


5. Sie werden zur Anmeldeseite des Routers weitergeleitet. Geben Sie das Administratorpasswort ein, um aus der Ferne auf die Weboberfläche zuzugreifen.

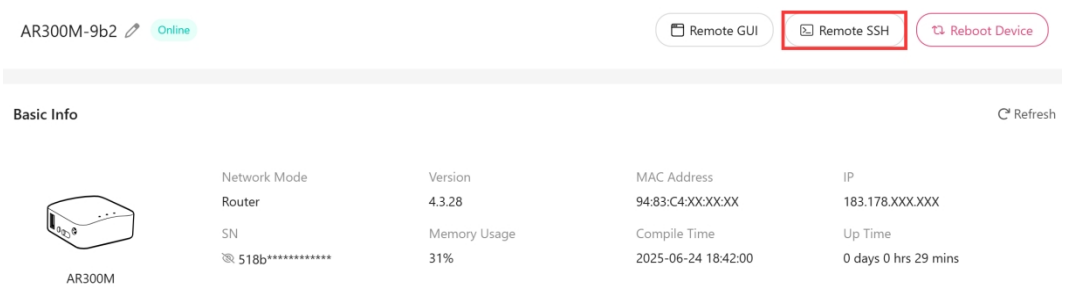


SSH-Fernzugriff

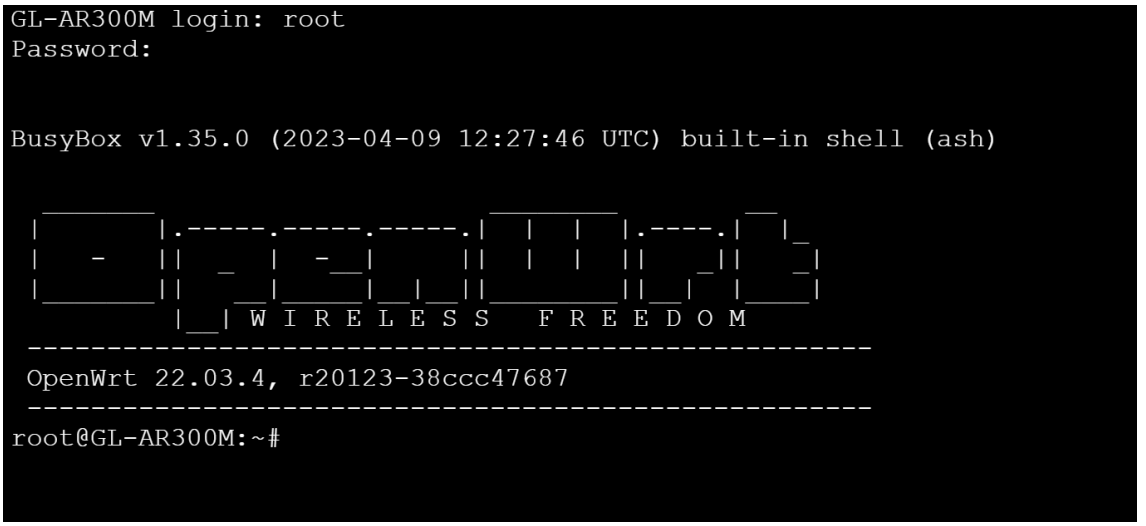
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **APPLICATIONS** > **GoodCloud**, aktivieren Sie **Remote SSH** und klicken Sie auf **Apply**.



2. Melden Sie sich bei GoodCloud an und öffnen Sie **Devices** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote SSH**.

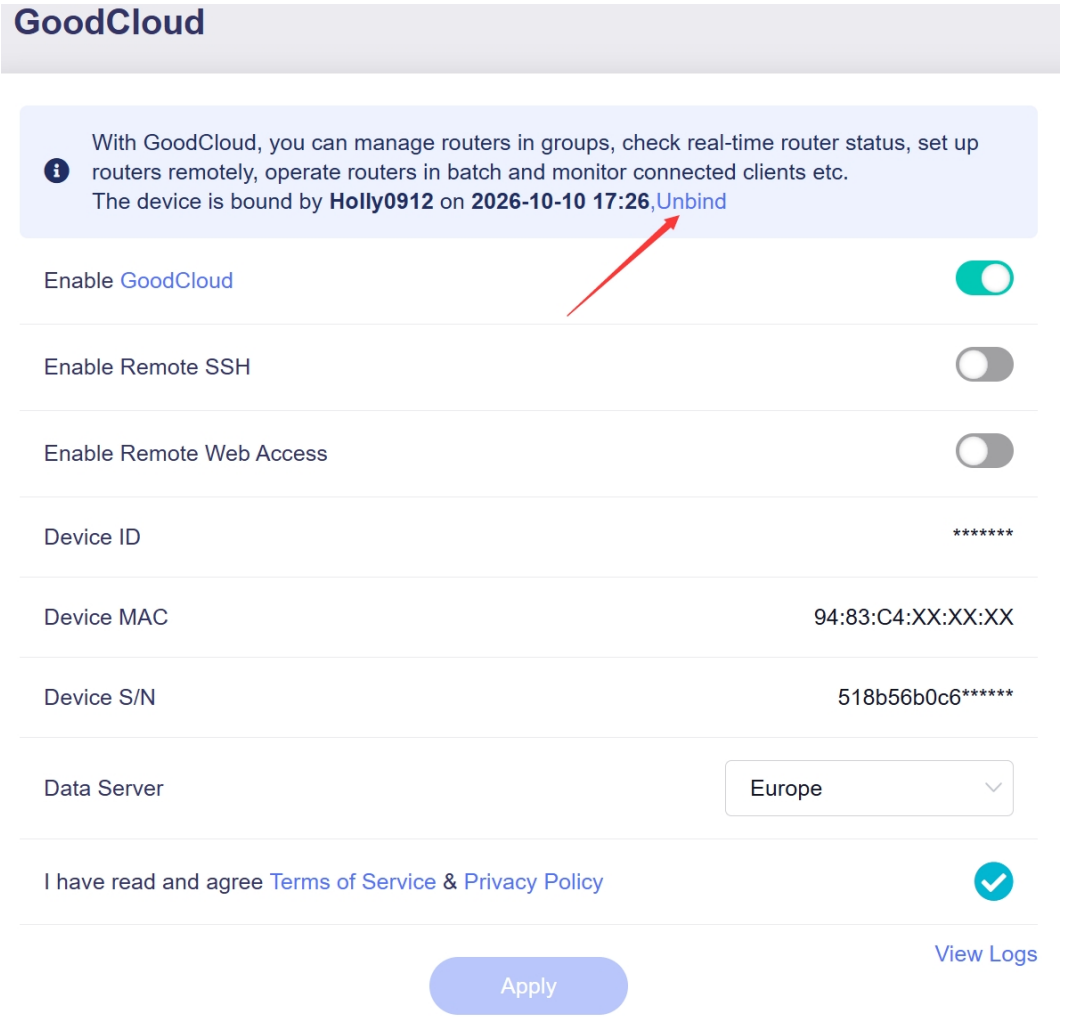


4. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

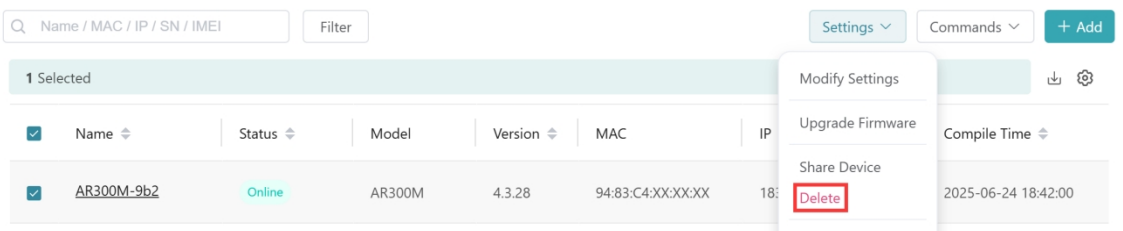


11.3.3 Geräteverknüpfung aufheben

Klicken Sie in der Weboberfläche auf **Unbind**. Die Verknüpfung Ihres Geräts mit Ihrem GoodCloud-Konto wird aufgehoben.



Alternativ melden Sie sich auf der Cloud-Plattform an und öffnen **Devices** > **Bound Devices**. Wählen Sie das Gerät aus, klicken Sie oben rechts auf **Settings** und wählen Sie **Delete**. Die Verknüpfung des Geräts mit Ihrem GoodCloud-Konto wird aufgehoben.



Kapitel 12

Netzwerk

Dieses Kapitel beschreibt die Konfiguration und Verwaltung von Netzwerkeinstellungen wie LAN, DNS und IPv6.

12.1 Firewall

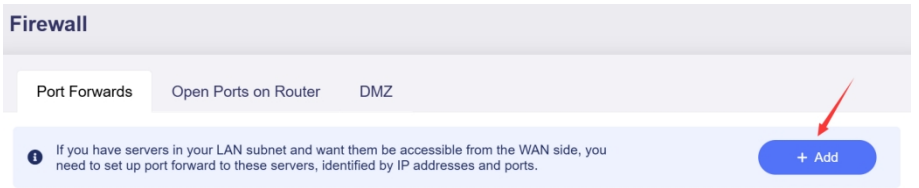
Über die Firewall-Einstellungen lassen sich externe Anfragen an bestimmte Geräte im lokalen Netzwerk weiterleiten. Die Firewall-Seite bietet drei zentrale Funktionen: **Port Forwards** für den gezielten Zugriff auf bestimmte Geräteports, **Open Ports on Router** für den Zugriff auf Dienste des Routers selbst und **DMZ** für den direkten vollständigen Zugriff auf ein einzelnes Gerät.

12.1.1 Portweiterleitungen

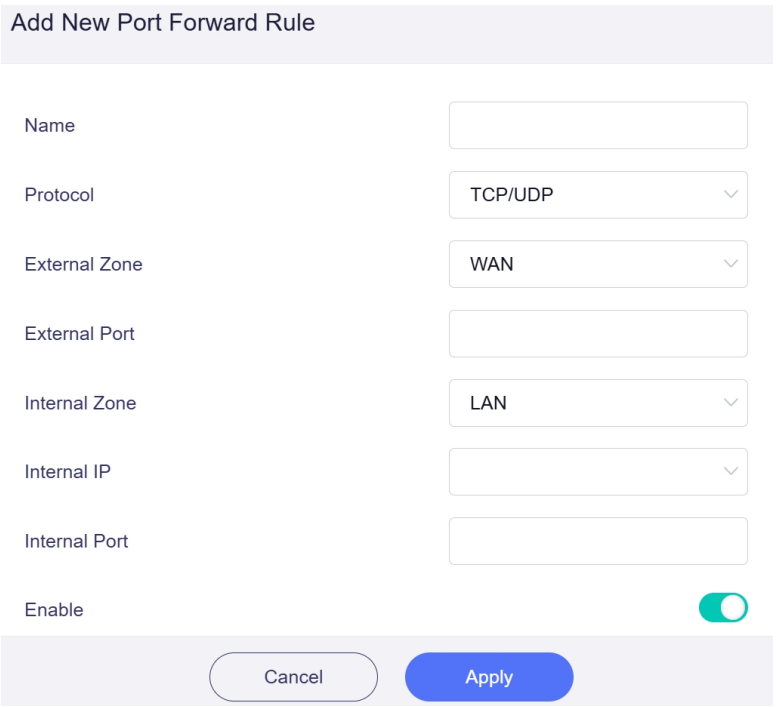
Portweiterleitungen ermöglichen entfernten Computern den Zugriff auf einen lokalen Computer oder Server hinter der LAN-Firewall, etwa einen Web- oder FTP-Server.

Gehen Sie bei Bedarf wie folgt vor, um Portweiterleitungen einzurichten.

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Firewall** > **Port Forwards**. Klicken Sie auf **Add**.



2. Geben Sie im eingeblendeten Fenster die erforderlichen Parameter ein oder wählen Sie sie aus den Listen aus. Klicken Sie auf **Apply**, um die Portweiterleitungsregel hinzuzufügen.

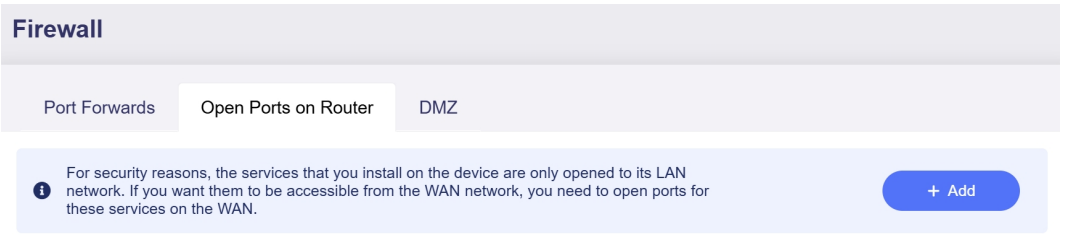


- **Name**: Ein frei wählbarer Name für die Regel.
- **Protocol**: Das verwendete Protokoll. Sie können TCP, UDP oder beide auswählen.
- **External Zone**: Zur Auswahl stehen WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN und Guest.
- **External Port**: Die externe Portnummer oder der Portbereich. Zulässig sind Ports von 1 bis 65535. Geben Sie einen einzelnen Port oder einen Bereich mit Bindestrich zwischen erster und letzter Portnummer ein, etwa 501-510.
- **Internal Zone**: Zur Auswahl stehen LAN, Guest, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server und WAN.
- **Internal IP**: Die vom Router zugewiesene IP-Adresse des Geräts, auf das aus der Ferne zugegriffen werden soll. Wenn unter External Port ein einzelner Port angegeben ist, legen Sie hier ebenfalls einen einzelnen Port fest. Bei einem externen Portbereich legen Sie den entsprechenden internen Portbereich fest.
- **Internal Port**: Die interne Portnummer des Geräts. Geben Sie einen bestimmten Port ein. Lassen Sie das Feld leer, wenn interner und externer Port übereinstimmen.
- **Enable**: Aktiviert oder deaktiviert diese Regel.

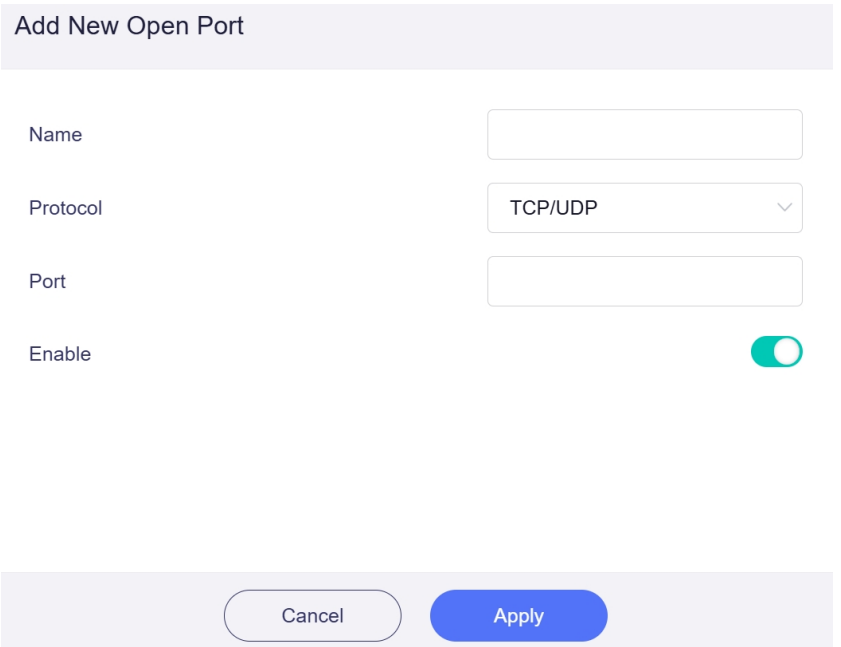
12.1.2 Ports am Router öffnen

Damit Dienste des Routers wie Web oder FTP öffentlich erreichbar sind, müssen die jeweiligen Ports am Router geöffnet werden.

Öffnen Sie dazu die Registerkarte Open Ports on Router und klicken Sie auf Add.



Legen Sie im eingeblendeten Fenster den zu öffnenden Port fest und klicken Sie auf Apply.



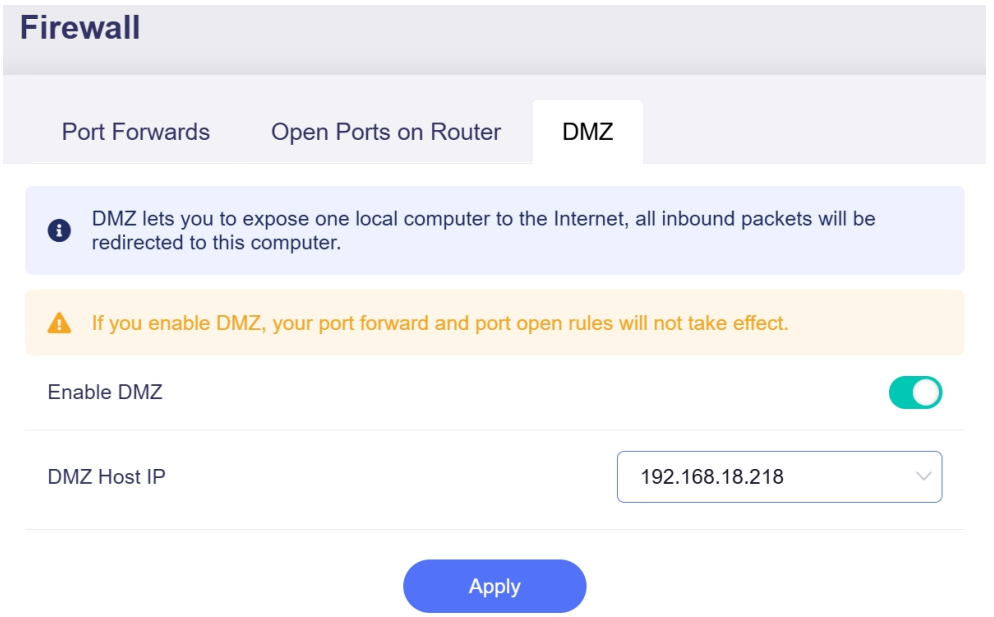
- **Name**: Ein frei wählbarer Name für die Regel.
- **Protocol**: Das verwendete Protokoll. Sie können TCP, UDP oder beide auswählen.
- **Port**: Die Nummer des Ports, den Sie öffnen möchten.
- **Enable**: Aktiviert oder deaktiviert diese Regel.

12.1.3 DMZ

Mit DMZ können Sie einen Computer direkt aus dem Internet erreichbar machen. Alle eingehenden Pakete werden dann an diesen Computer weitergeleitet.

Gehen Sie bei Bedarf wie folgt vor, um DMZ zu aktivieren.

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Firewall** > **DMZ**.
2. Aktivieren Sie **Enable DMZ** und wählen Sie unter **DMZ Host IP** die IP-Adresse des Zielgeräts aus. Dieses Gerät erhält alle eingehenden Pakete. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.



12.2 Multi-WAN

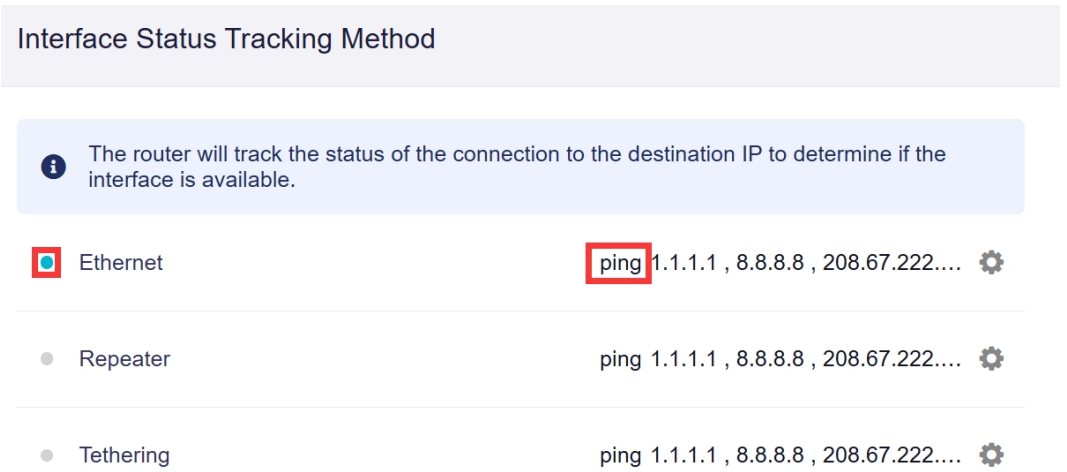
Multi-WAN ermöglicht die gleichzeitige Nutzung mehrerer Internetzugangsarten und bietet unterschiedliche Verbindungsoptionen auf dem Router. Es stehen zwei Betriebsmodi zur Verfügung:

- **Failover**: Schaltet bei einem Ausfall der Hauptverbindung innerhalb kurzer Zeit automatisch auf eine Ersatzverbindung um und gewährleistet so einen unterbrechungsfreien Netzwerkzugang.
- **Load Balance**: Verteilt den Datenverkehr nach einem festgelegten Verhältnis auf alle verfügbaren Verbindungen. So werden mehrere Verbindungen gleichzeitig genutzt und die verfügbare Bandbreite optimal ausgeschöpft.

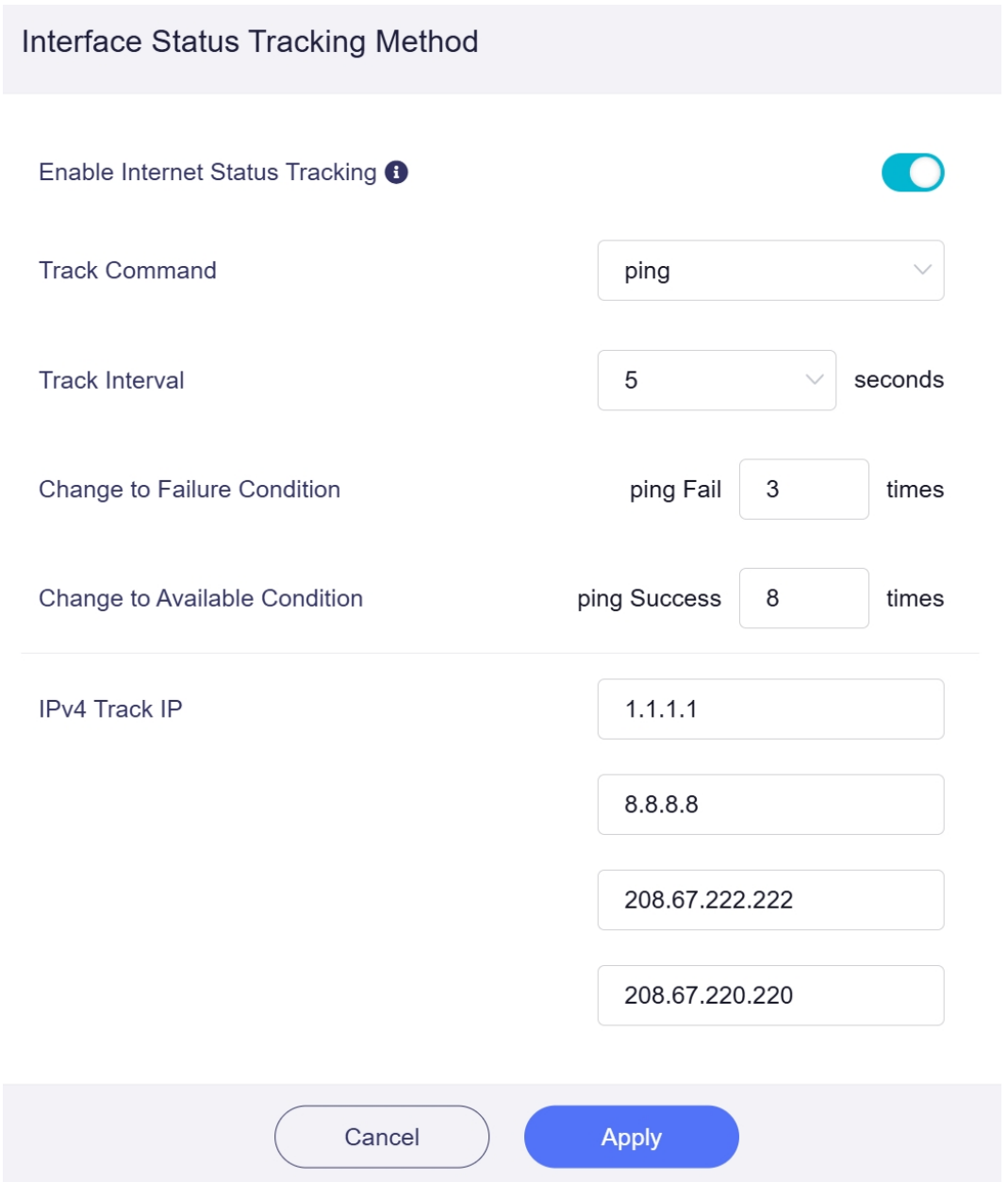
Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Multi-WAN**. Die Seite enthält die Abschnitte Interface Status Track und Multi-WAN Mode.

12.2.1 Schnittstellenstatus überwachen

GL.iNet-Router prüfen mit dem Befehl **ping** die Verbindung zu einer Ziel-IP-Adresse und ermitteln so, ob eine Schnittstelle verfügbar ist. Bei verfügbarer Schnittstelle erscheint links ein grüner Punkt, andernfalls ein grauer.



Klicken Sie im Abschnitt **Interface Status Track** rechts auf das Zahnradsymbol, um die Überwachung für die jeweilige Schnittstelle einzustellen. Nachfolgend sind die Einstellungen für Ethernet abgebildet. Für andere Schnittstellen gilt dieselbe Vorgehensweise.



- **Enable Interface Status Track**: Standardmäßig aktiviert. Bei deaktivierter Überwachung beurteilt der Router den Schnittstellenstatus anhand physischer Merkmale, etwa ob ein Ethernetkabel angeschlossen ist.
- **Track Command**: Der Befehl ping prüft die Verbindung zur Ziel-IP-Adresse und damit die Verfügbarkeit der Schnittstelle.
- **Track Interval**: Legt in Sekunden fest, wie häufig der Router den Überwachungsbefehl ausführt.
- **Change to Failure Condition**: Anzahl aufeinanderfolgender fehlgeschlagener Ping-Anfragen, nach der der Router die Schnittstelle als getrennt kennzeichnet.

- **Change to Available Condition**: Anzahl aufeinanderfolgender erfolgreicher Ping-Anfragen, nach der der Router die Schnittstelle wieder als verbunden kennzeichnet.
- **IPv4 Track IP**: Passen Sie bei Bedarf die zur Überwachung verwendeten IPv4-Adressen an.

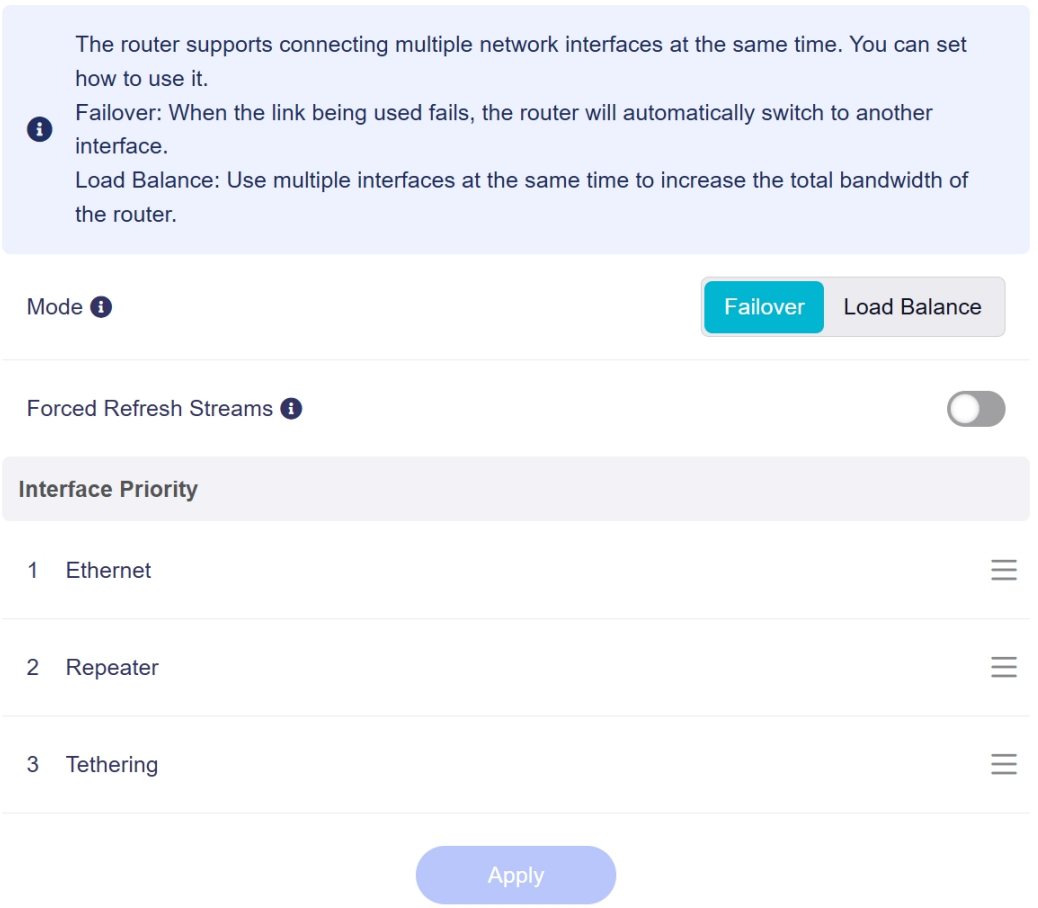
12.2.2 Multi-WAN-Modus

Multi-WAN bietet zwei Modi: **Failover** und **Load Balance**. Diese schließen sich gegenseitig aus.

Ausfallsicherung

Failover ist der Standardmodus bei mehreren eingerichteten Verbindungen. Fällt die aktive Verbindung aus, schaltet der Router automatisch auf eine andere Netzwerkschnittstelle für den Internetzugang um.

Sie können jeder Schnittstelle eine Priorität zuweisen. Fällt die verwendete Schnittstelle aus, wechselt der Router zur verfügbaren Schnittstelle mit der nächsthöheren Priorität. Sobald eine Verbindung mit höherer Priorität wieder verfügbar ist, wechselt er automatisch zurück.

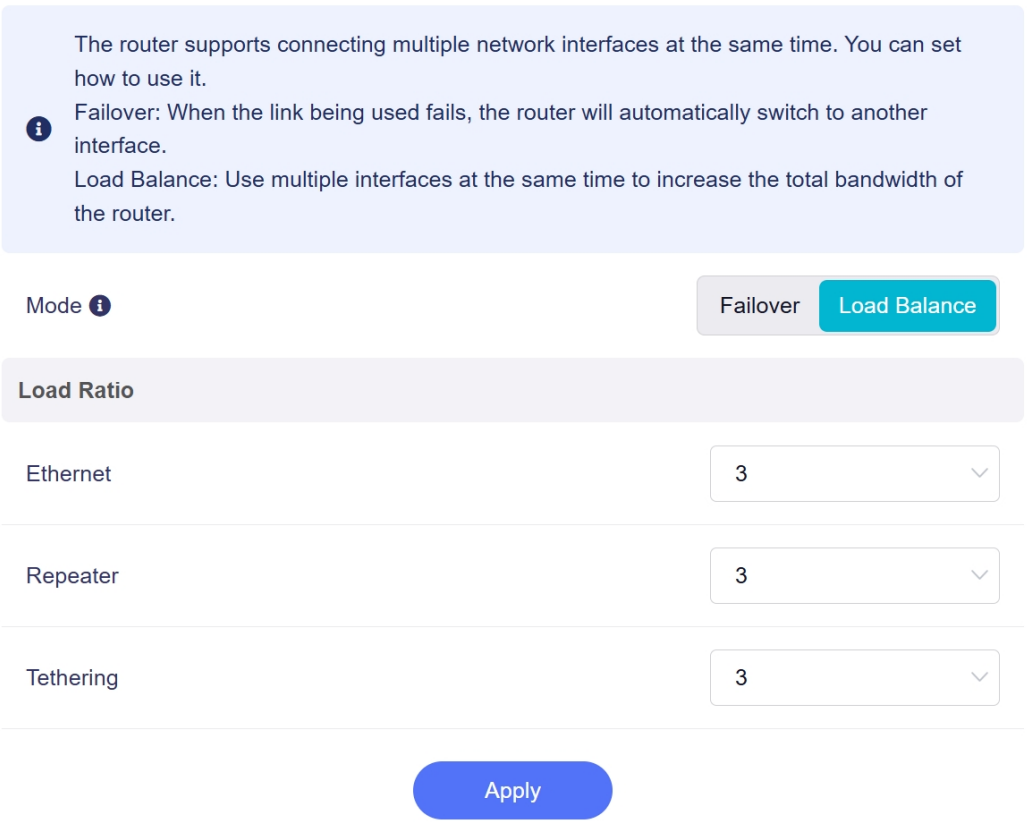


Lastverteilung

Im Modus Load Balance werden mehrere Netzwerkschnittstellen gleichzeitig genutzt, um die Gesamtbandbreite zu erhöhen. Das System verteilt neue Verbindungen gemäß einem festgelegten Lastverhältnis auf die Schnittstellen. Verbindungen zu derselben Anwendung oder Webseite laufen dabei in der Regel nur über eine Schnittstelle.

Das Lastverhältnis beschreibt die Gewichtung der einzelnen Schnittstellen. Das System ordnet neue Verbindungen entsprechend dieser Gewichtung zu.

Ist der Router beispielsweise gleichzeitig über Ethernet, Repeater und Tethering mit drei funktionsfähigen Internetzugängen verbunden, verteilt Load Balance bei einem Verhältnis von 1:1:1 neue Verbindungen gleichmäßig auf alle drei Schnittstellen. Diese teilen sich damit die Netzwerklast zu gleichen Anteilen.



Sie können das Lastverhältnis anpassen. Hat Ethernet beispielsweise 100 Mbit/s und die Repeater-Verbindung 200 Mbit/s, während Tethering nicht aktiv ist, setzen Sie die Werte auf 1 für Ethernet, 2 für Repeater und 0 für Tethering. Neue Verbindungen werden dann im Verhältnis 1:2 verteilt: Ethernet übernimmt halb so viele Verbindungen wie Repeater. Im

Unterschied zur Ausfallsicherung optimiert dieser Modus den Gesamtdurchsatz, indem er den Datenverkehr auf alle verfügbaren Schnittstellen verteilt.

Hinweis: Bereits bestehende Verbindungen und der tatsächliche Datenverkehr entsprechen nicht zwingend dem eingestellten Lastverhältnis. Die Verteilung nähert sich diesem bei längerer Nutzung schrittweise an.

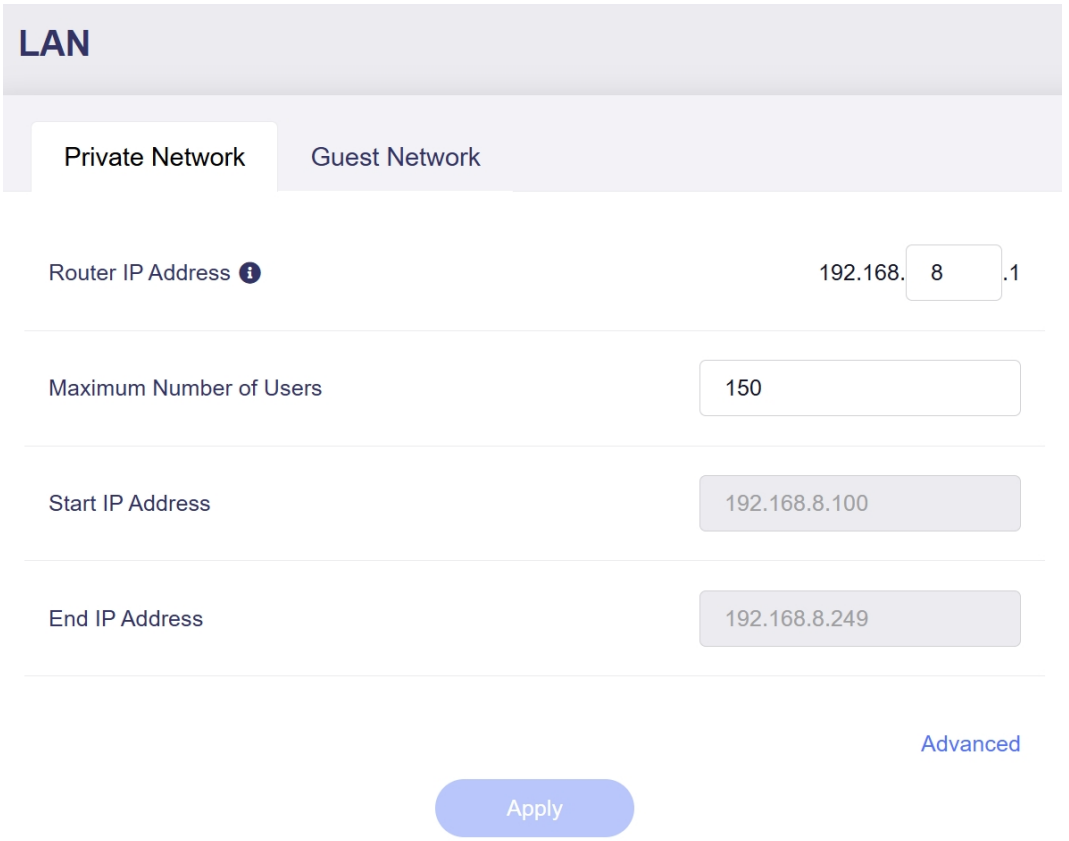
12.3 LAN

LAN (Local Area Network) bezeichnet das private lokale Netzwerk, mit dem Sie Ihre Geräte über Ethernetkabel verbinden.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **LAN**. Hier konfigurieren Sie die LAN-Einstellungen für das private Netzwerk und das Gastnetzwerk.

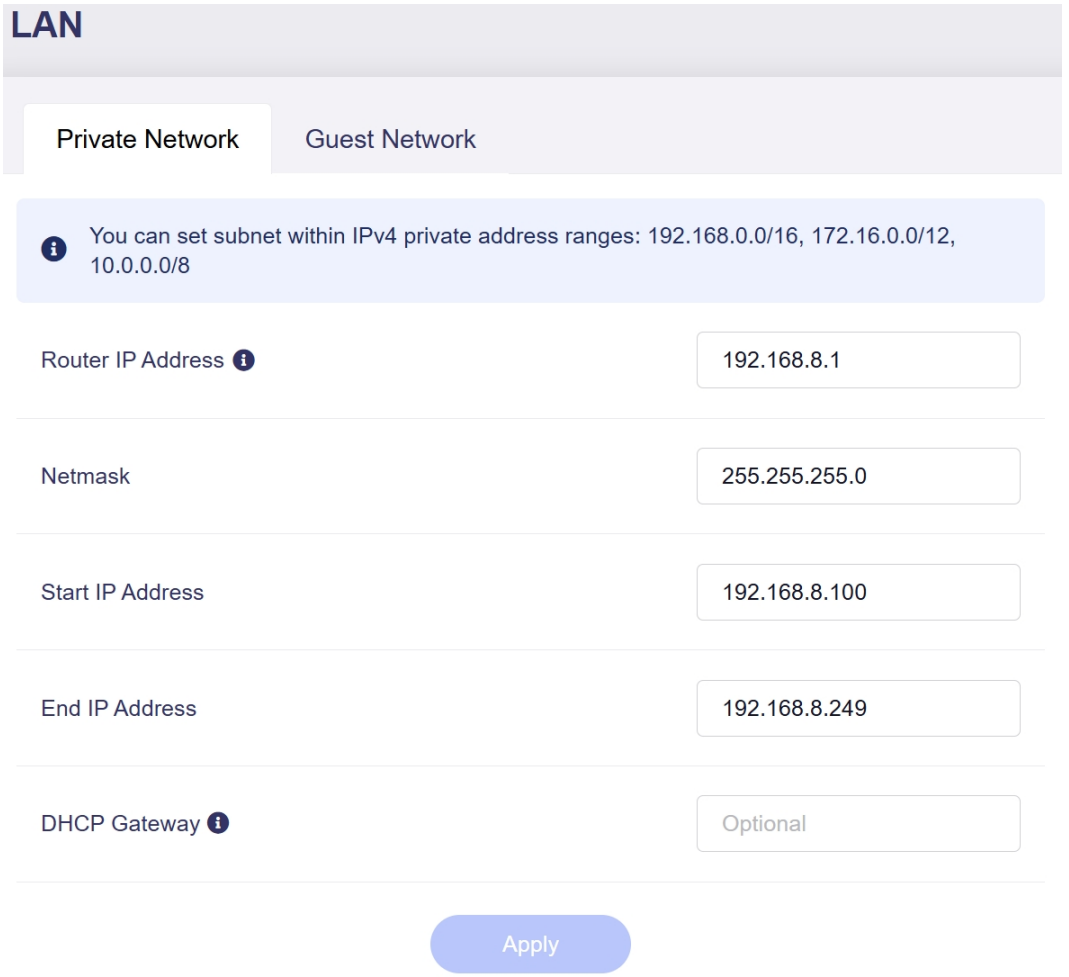
12.3.1 Privates Netzwerk

Das private Netzwerk ist das Haupt-LAN für Ihre verbundenen Geräte. Sie können die IP-Adresse des Routers, den DHCP-Adressbereich und die maximale Anzahl verbundener Geräte festlegen.



- **Router IP Address**: Über diese Adresse rufen Sie die Weboberfläche im Browser auf. Standardmäßig lautet sie 192.168.8.1. Bei einem Konflikt mit dem vorgeschalteten Netzwerk können Sie sie ändern.
- **Maximum Number of Users**: Legt fest, wie viele Geräte sich höchstens mit dem Gastnetzwerk verbinden dürfen.

Klicken Sie auf **Advanced**, um erweiterte Einstellungen zu ändern, darunter Default Gateway, Netmask, Start IP Address, End IP Address und DHCP Gateway.

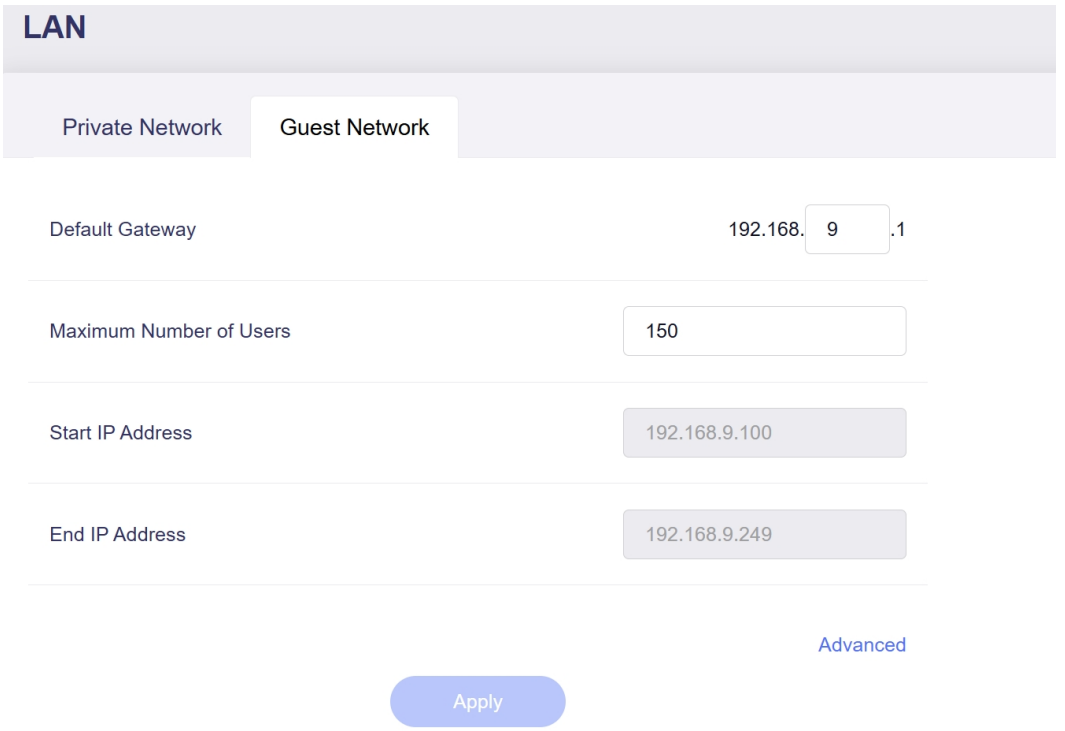


- **DHCP Gateway**: Die Standardgateway-Adresse, die der DHCP-Server den Endgeräten zuweist. Über dieses Gateway wird Datenverkehr aus dem lokalen Netzwerk an externe Netzwerke wie das Internet weitergeleitet.
- **Netmask**: Die Subnetzmaske des privaten Netzwerks. Standardmäßig 255.255.255.0.

12.3.2 Gastnetzwerk

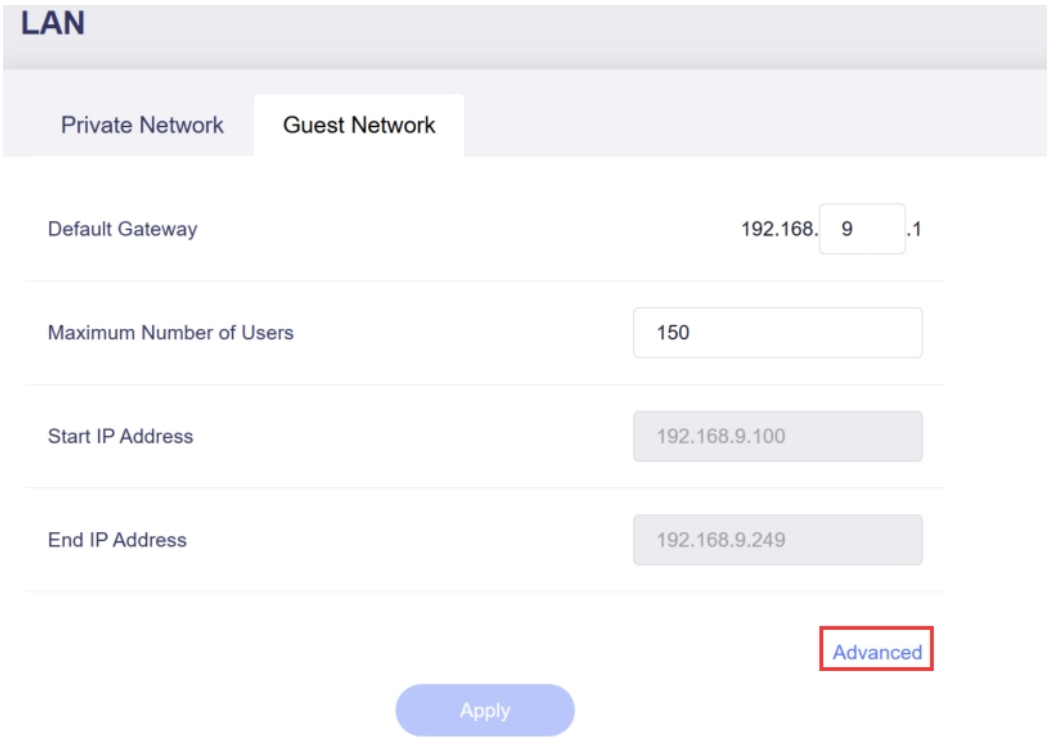
Ein Gastnetzwerk ist ein separates Netzwerk für Besucher. Es ist vom Haupt-LAN getrennt und schützt so Ihr privates Netzwerk.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **LAN** > **Guest Network**. Hier konfigurieren Sie das Gastnetzwerk.

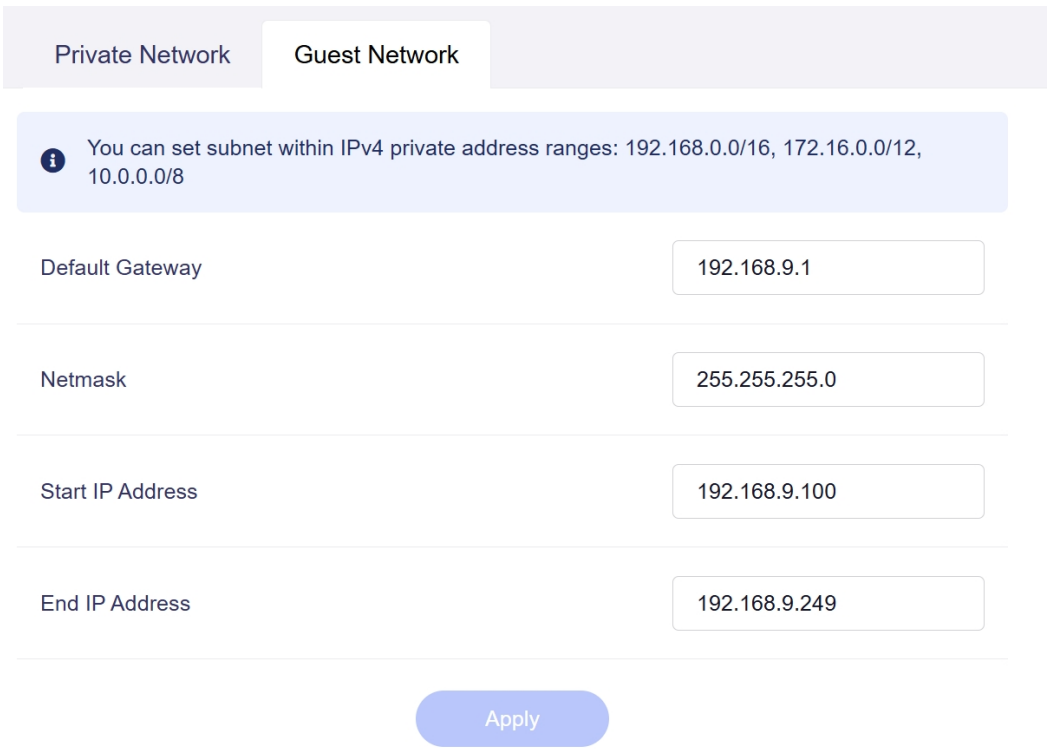


- **Default Gateway**: Standardmäßig 192.168.9.1. Sie können diese Adresse ändern, sie darf jedoch nicht mit dem Gateway des Hauptnetzwerks kollidieren.
- **Maximum Number of Users**: Legt fest, wie viele Geräte sich höchstens mit dem Gastnetzwerk verbinden dürfen.

Klicken Sie unten rechts auf **Advanced**.



Hier konfigurieren Sie erweiterte Einstellungen wie Default Gateway, Netmask, Start IP Address und End IP Address.



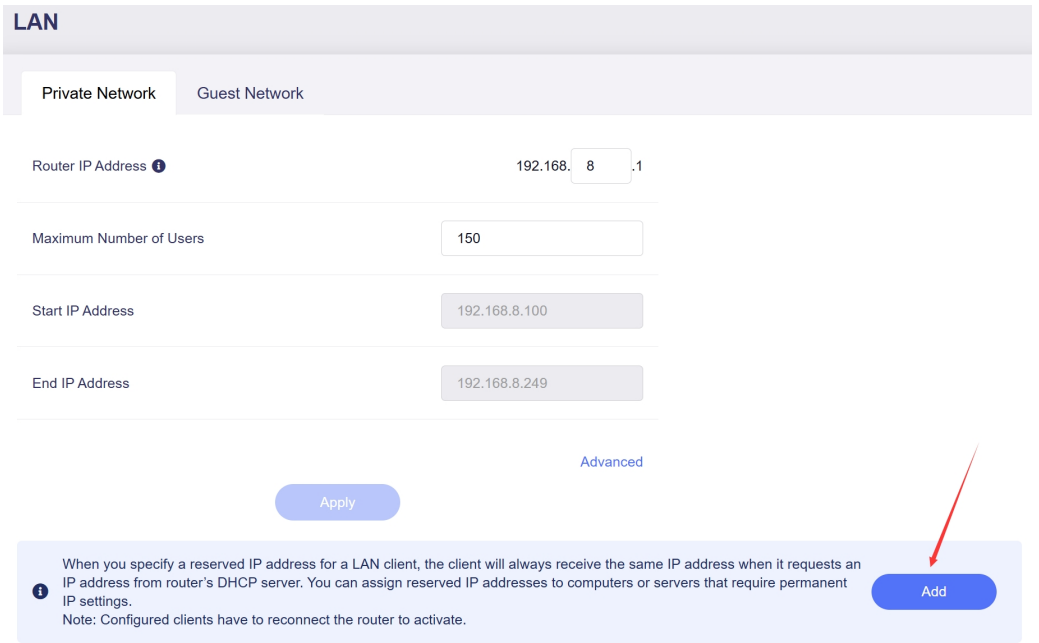
Die **Netmask** lautet standardmäßig 255.255.255.0. Für ein größeres Subnetz mit mehr IP-Adressen können Sie auch 255.255.0.0 auswählen.

12.3.3 Adressreservierung

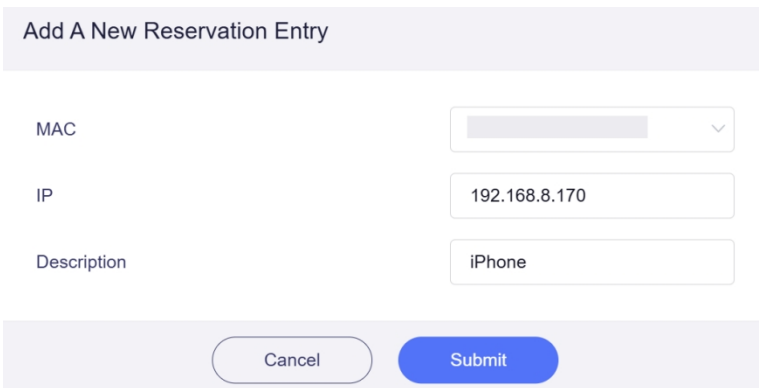
Mit der Adressreservierung weisen Sie einem LAN-Gerät eine feste IP-Adresse zu, die es bei jeder Anfrage an den DHCP-Server des Routers erneut erhält. Dies eignet sich für Computer oder Server, die dauerhaft dieselbe IP-Adresse benötigen. Damit eine neue Reservierung wirksam wird, muss sich das betreffende Gerät erneut mit dem Router verbinden.

Gehen Sie bei Bedarf wie folgt vor, um eine Adressreservierung einzurichten.

1. Melden Sie sich an der Weboberfläche an, öffnen Sie **NETWORK** > **LAN** > **Address Reservation** und klicken Sie auf **Add**.



2. Wählen Sie im eingeblendeten Fenster die MAC-Adresse aus. Die zugehörige IP-Adresse wird automatisch eingetragen. Geben Sie einen aussagekräftigen Namen ein und klicken Sie auf **Submit**.



3. Nach dem Hinzufügen erscheint die neue IP-Adressreservierung wie folgt auf der Seite.

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

Add

MAC	IP	Description	Action
CA:E1:50:XX:XX:XX	192.168.8.170	iPhone	•••

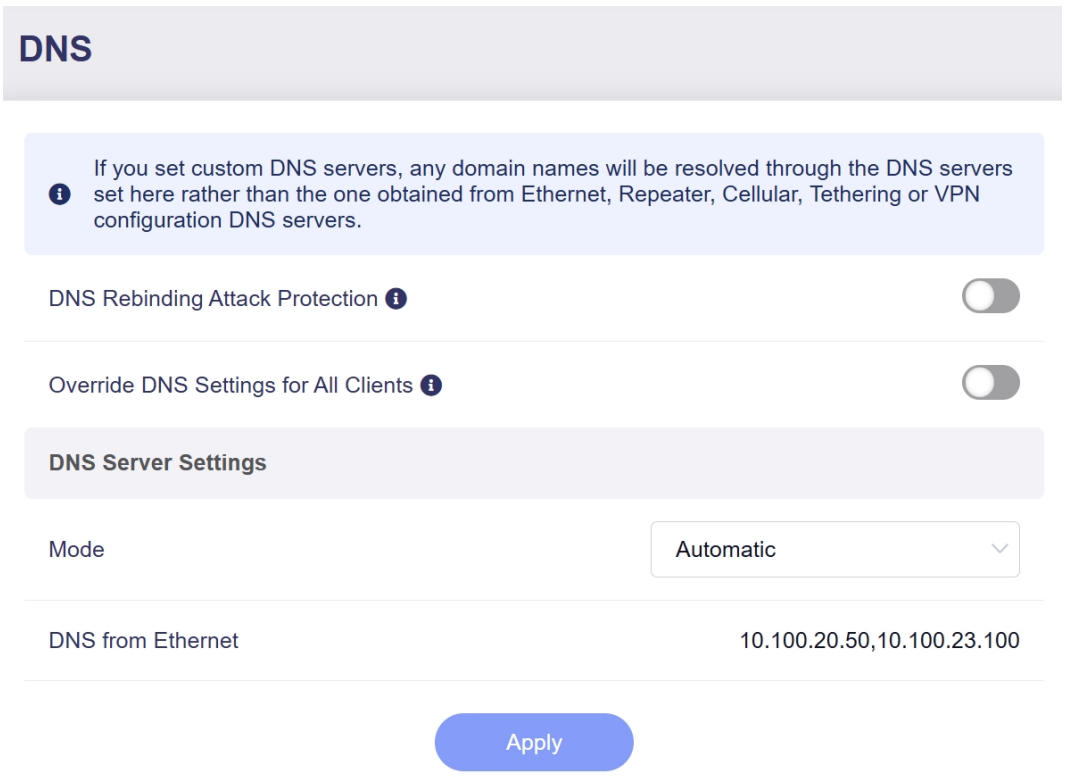
12.4 DNS

DNS (Domain Name System) übersetzt lesbare Domainnamen wie www.google.com in IP-Adressen. So können Geräte Webseiten und Onlinedienste finden und eine Verbindung zu ihnen herstellen.

Die DNS-Einstellungen eines Routers legen in der Regel fest, welche DNS-Server die verbundenen Geräte verwenden. Meist bezieht der Router deren Adressen automatisch vom Internetanbieter oder dem vorgeschalteten Netzwerk. Alternativ können Sie in der Weboberfläche öffentliche DNS-Server wie 8.8.8.8 manuell eintragen. Die Einstellungen werden normalerweise automatisch an die verbundenen Geräte verteilt, sodass keine separate DNS-Konfiguration auf jedem Gerät erforderlich ist.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **DNS**. Hier konfigurieren Sie die DNS-Einstellungen.

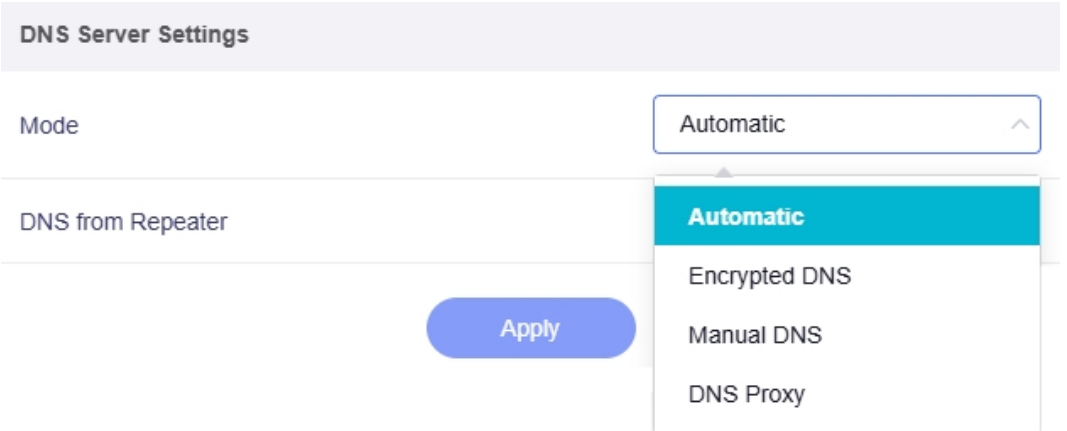
12.4.1 Allgemeine Einstellungen



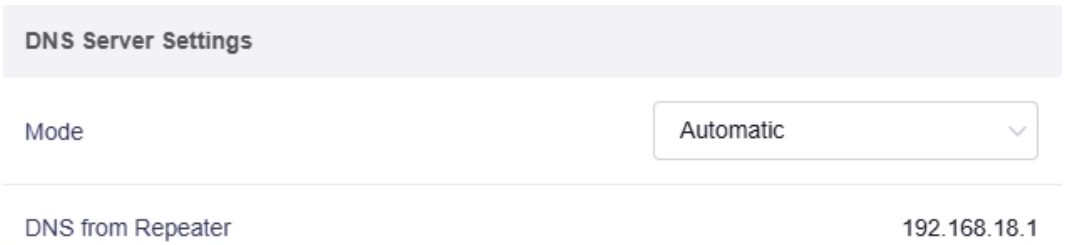
- **DNS Rebinding Attack Protection**: Schützt vor DNS-Rebinding-Angriffen, indem bösartige Namensauflösungen blockiert werden. Dadurch kann die Auflösung privater Adressen fehlschlagen. Deaktivieren Sie die Option, wenn Ihr Netzwerk ein Captive Portal verwendet, etwa eine Anmeldeseite in einem öffentlichen WLAN.
- **Override DNS Settings of All Clients**: Erzwingt für alle verbundenen Geräte die auf dem Router konfigurierten DNS-Server. Eigene DNS-Einstellungen der Geräte werden ignoriert, sodass eine einheitliche DNS-Konfiguration gilt.

12.4.2 DNS-Servereinstellungen

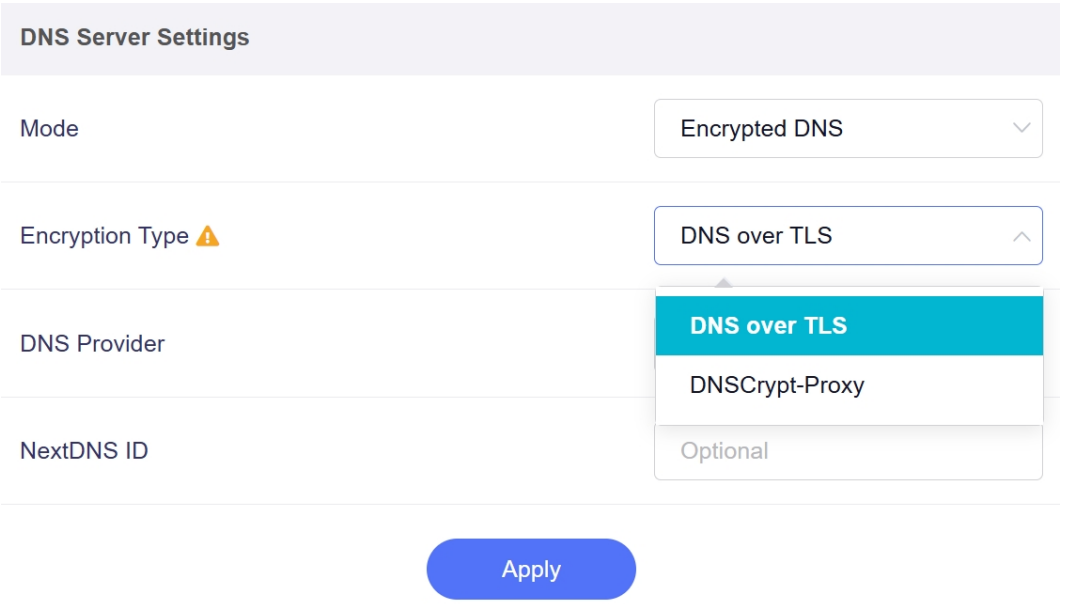
Für den DNS-Server stehen vier Modi zur Verfügung: Automatic, Encrypted DNS, Manual DNS und DNS Proxy.



1. **Automatic**: Der Router bezieht die DNS-Serveradressen automatisch aus dem vorgeschalteten Netzwerk und verwendet sie für alle verbundenen Geräte.

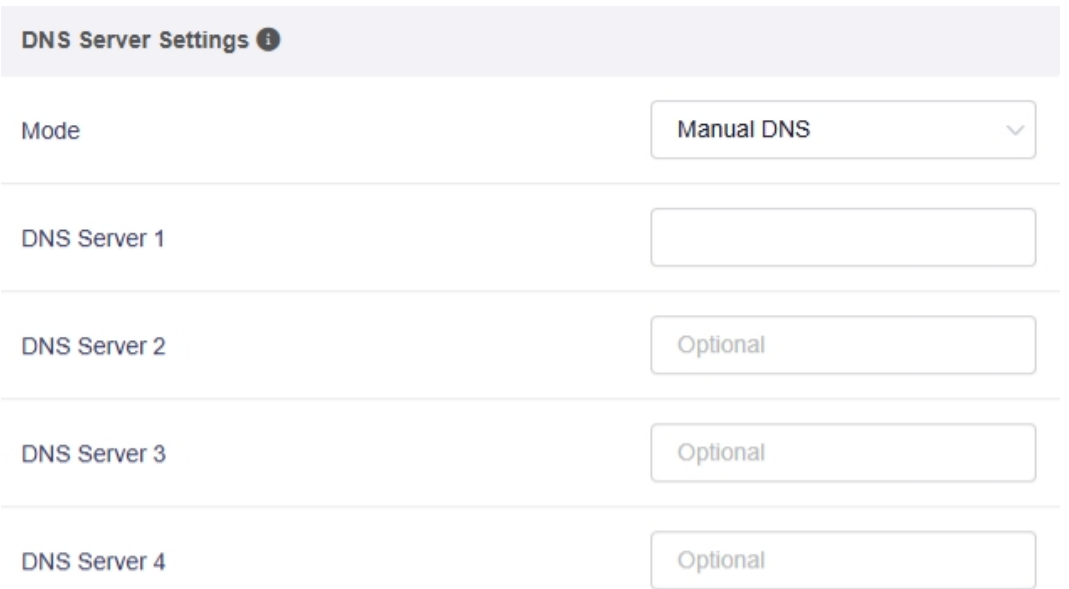


2. **Encrypted DNS**: Der Router verarbeitet DNS-Anfragen über verschlüsselte Protokolle und schützt die Auflösungsdaten so vor Abhören und Manipulation.
   Es stehen zwei Verschlüsselungsverfahren zur Auswahl: DNS over TLS und DNSCrypt-Proxy.



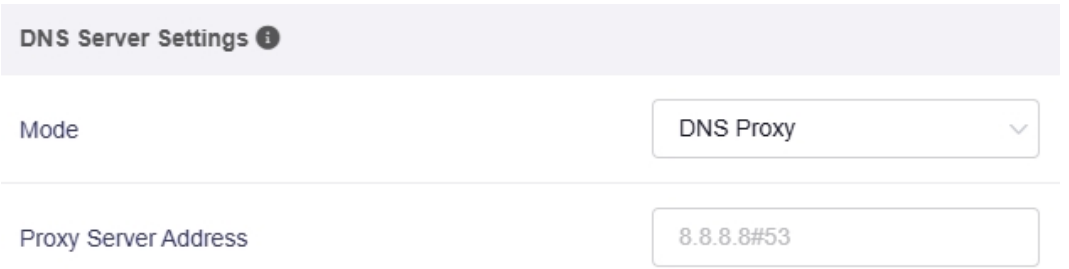
- Bei DNS over TLS wählen Sie Control D, NextDNS oder Cloudflare als DNS-Anbieter aus.
- Bei DNSCrypt-Proxy wählen Sie mindestens einen DNS-Server aus dem Verzeichnis aus. Es sind bis zu acht Server möglich. Bei mehreren ausgewählten Servern verwendet der Router automatisch den schnellsten.

3. **Manual DNS**: Hier legen Sie die DNS-Server des Routers selbst fest. Klicken Sie auf DNS Server 1 und wählen Sie einen Server aus der Liste aus. Die übrigen DNS-Felder werden automatisch angepasst.



Hinweis: Wenn Sie IPv6-Adressen für manuelles DNS verwenden möchten, aktivieren Sie zunächst IPv6 auf dem Router.

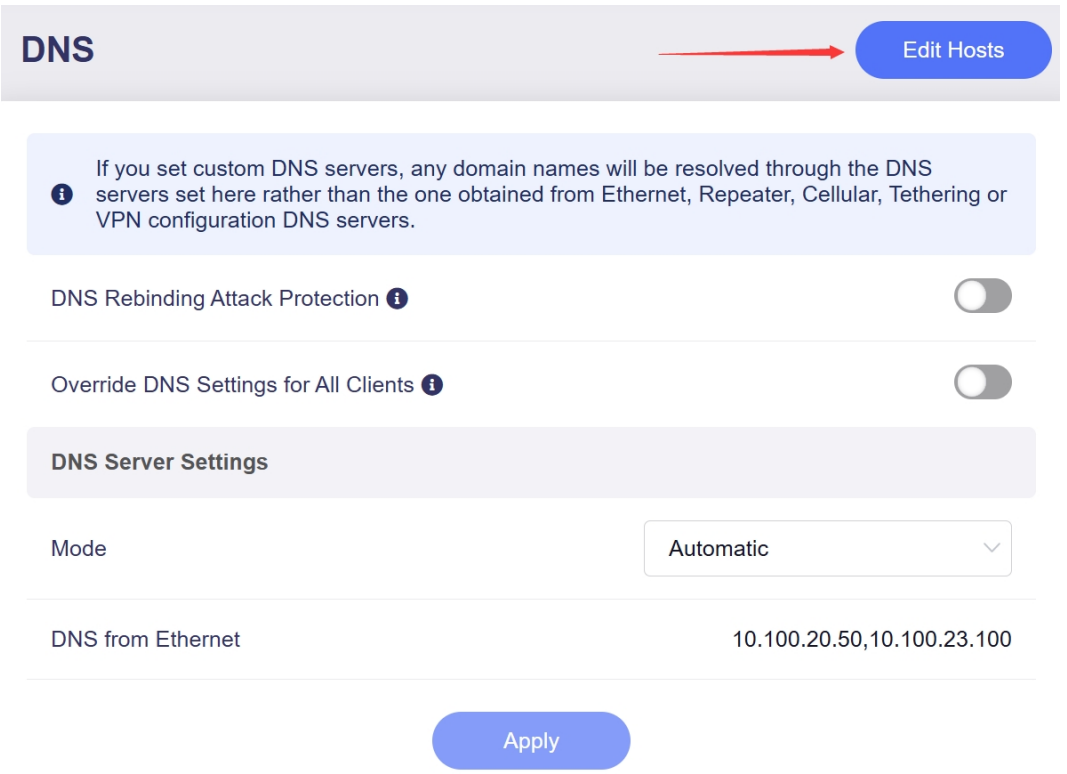
4. **DNS Proxy**: Der Router leitet alle DNS-Anfragen über einen Proxyserver weiter. Die Namensauflösung erfolgt in dessen Netzwerkumgebung, um besondere Zugriffsanforderungen zu erfüllen.



12.4.3 Hosts bearbeiten

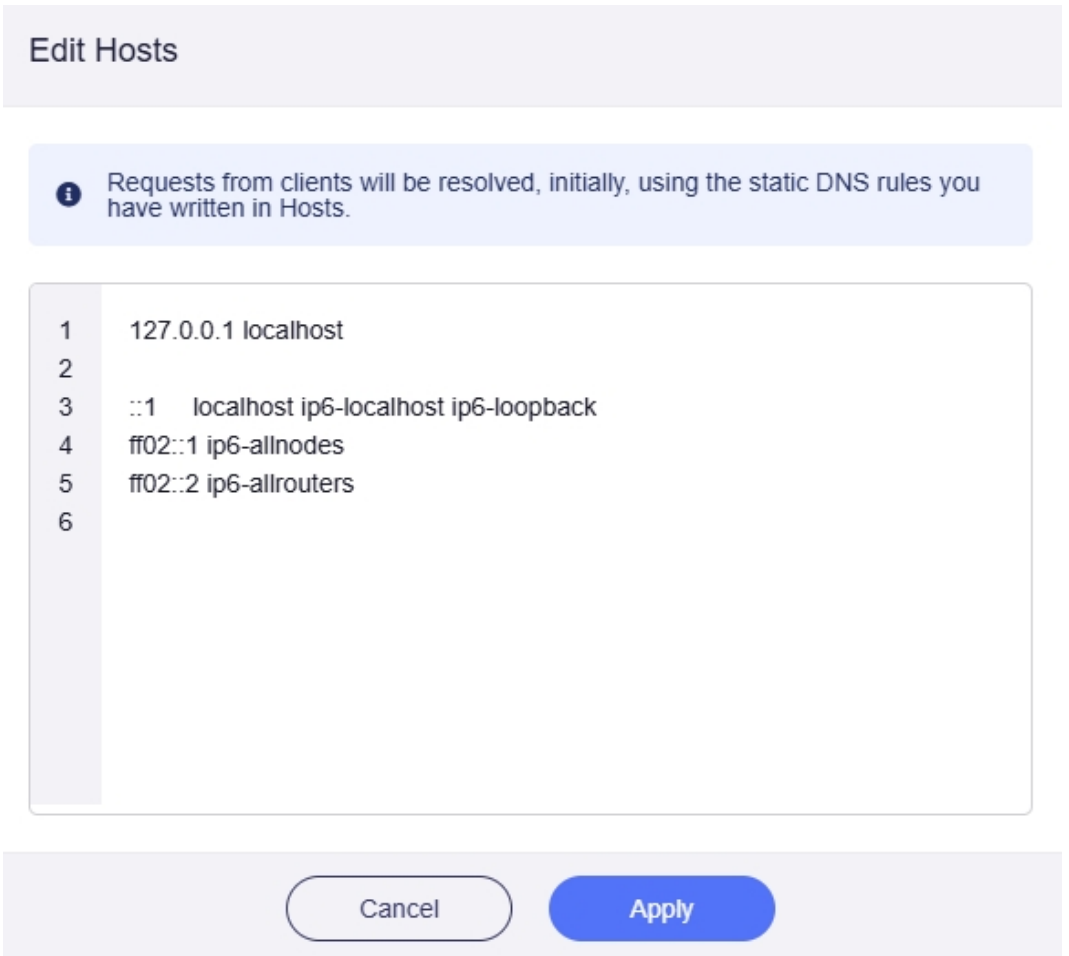
Bei Bedarf können Sie statische Regeln für die DNS-Auflösung festlegen.

Klicken Sie auf der DNS-Seite oben rechts auf **Edit Hosts**.



Anfragen von Endgeräten werden vorrangig anhand der hier eingetragenen statischen DNS-Regeln aufgelöst. Sie können Hostnamen manuell IP-Adressen zuordnen und so die

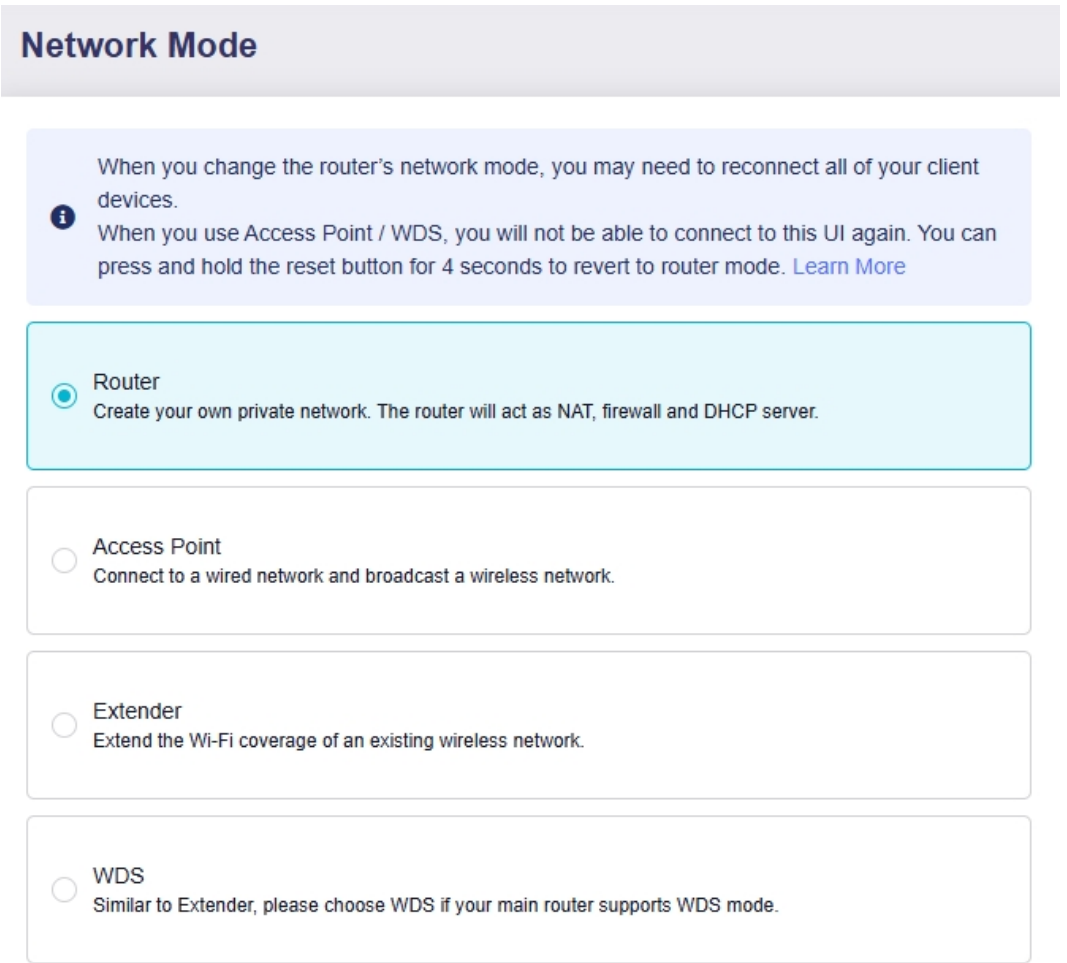
Namensauflösung gezielt steuern. Ein Beispiel ist der Standardeintrag „127.0.0.1 localhost“ fü
r die lokale Loopback-Adresse.



12.5 Netzwerkmodus

Der Netzwerkmodus bestimmt die Rolle und die Funktionen des Routers für unterschiedliche Netzwerkanforderungen.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Network Mode**. Hier können Sie den Netzwerkmodus des Routers ändern.



- **Router**: Der Standardmodus der meisten Router für zu Hause und kleine Büros. Er erstellt ein privates lokales Netzwerk und dient als Gateway zwischen dem öffentlichen Internet und den verbundenen Geräten. NAT, DHCP und die integrierte Firewall sind aktiv. Der Router verbindet sich mit einem vorgeschalteten Anschluss, etwa Glasfaser, weist Endgeräten automatisch private IP-Adressen zu und schützt das gesamte private Netzwerk.
- **Access Point**: In diesem Modus wird der Router per LAN-Kabel mit einem kabelgebundenen Netzwerk verbunden und stellt WLAN bereit. Dadurch vergrößert sich

die WLAN-Abdeckung, und weitere Geräte können auf das Netzwerk zugreifen. NAT und DHCP sind deaktiviert. Der Router arbeitet ausschließlich als WLAN-Zugangspunkt und Switch, nicht als eigenständiges Gateway.

- **Extender**: Dieser Modus erweitert die Reichweite eines vorhandenen WLANs und versorgt Bereiche mit schlechtem Empfang. Der Router empfängt das Signal des Hauptrouters drahtlos und sendet es erneut aus. Anders als im Access-Point-Modus ist keine Kabelverbindung zum Hauptrouter nötig. Da das Gerät gleichzeitig empfangen und senden muss, kann sich die verfügbare Bandbreite halbieren.
- **WDS**: Wireless Distribution System erweitert wie der Extender-Modus die WLAN-Abdeckung drahtlos, unterstützt jedoch zusätzlich WLAN-Brücken zwischen mehreren kompatiblen Routern. Dieser Modus wird empfohlen, wenn der vorgeschaltete Router WDS unterstützt.
  WDS eignet sich etwa für mehrstöckige Gebäude oder kleine Bürogelände, in denen mehrere Router gemeinsam ein einheitliches WLAN bilden sollen. Während im Extender-Modus ein Hauptrouter mit einem einzelnen Extender kommuniziert, können in WDS miteinander verbundene Router Signale sowohl senden als auch empfangen. Mehrere Funkknoten ermöglichen so eine durchgängige Abdeckung größerer Bereiche.

Hinweis:

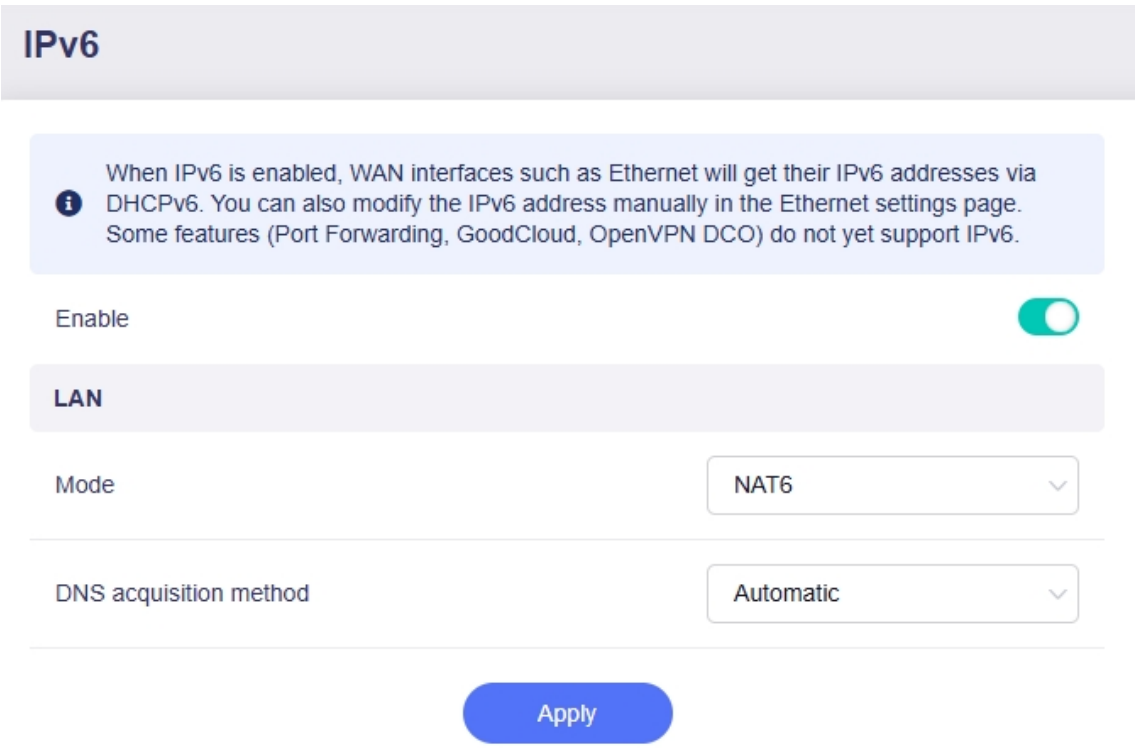
1. Nach einer Änderung des Netzwerkmodus sollten sich alle Endgeräte erneut mit dem Router verbinden, um eine stabile Verbindung sicherzustellen.
2. **Im Access-Point- und WDS-Modus ist die Weboberfläche nicht mehr über die ursprüngliche IP-Adresse erreichbar**. Melden Sie sich am vorgeschalteten Router an und ermitteln Sie die diesem Router zugewiesene IP-Adresse. Rufen Sie die Weboberfläche über diese Adresse auf. Haben Sie keinen Zugriff auf den vorgeschalteten Router, halten Sie die Reset-Taste vier Sekunden gedrückt, um zum standardmäßigen Routermodus zurückzukehren.
3. **Im Access-Point-, Extender- und WDS-Modus stehen folgende Funktionen nicht zur Verfügung**: Zugriffskontrolle (Freigabe- und Sperrliste), VPN, Firewall, Multi-WAN, DHCP-Server, Adressreservierung, Gastnetzwerk, DNS, IPv6, Drop-in Gateway und IGMP Snooping.

12.6 IPv6

IPv6 (Internet Protocol Version 6) ist die neueste Version des Internetprotokolls und soll IPv4 ablösen. Sein erheblich größerer Adressraum behebt die IPv4-Adressknappheit und unterstützt die weltweit wachsende Zahl vernetzter Geräte.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **IPv6**. Hier können Sie IPv6 aktivieren und konfigurieren. Bei aktiviertem IPv6 beziehen WAN-Schnittstellen wie Ethernet ihre IPv6-Adressen über DHCPv6.

Aktivieren Sie **Enable**, wählen Sie den Modus für Ihr Hauptnetzwerk und das Verfahren zum Beziehen der DNS-Adressen aus und klicken Sie auf **Apply.**



Hinweis: Einige Funktionen, etwa Firewall und GoodCloud, unterstützen IPv6 noch nicht. Die gleichzeitige Aktivierung dieser Funktionen und IPv6 kann zu Verbindungsproblemen führen.

12.6.1 IPv6-Modus

Vier Modi stehen zur Verfügung: Native, Passthrough, NAT6 und Static IPv6.

- **Native**: Der Router erhält direkt eine öffentliche IPv6-Adresse und weist den verbundenen Geräten automatisch IPv6-Adressen zu. Dieser Modus deckt die Anforderungen der meisten Nutzer ab.
- **Passthrough**: IPv6-Pakete werden ohne Verarbeitung oder Umwandlung direkt durchgeleitet. Dies ist nützlich, wenn Anwendungen oder Dienste unveränderte IPv6-Pakete zur weiteren Verarbeitung oder Analyse benötigen. Fachpersonal nutzt diesen Modus zur Netzwerkfehlerdiagnose oder Sicherheitsanalyse.
- **NAT6**: Dieser Modus eignet sich, wenn der Router als Gateway jedem Netzwerkgerät eine dynamische interne IPv6-Adresse zuweisen soll. Die Endgeräte sind dabei über ein optisches Netzabschlussgerät (ONT) verbunden und erhalten eine lokale IPv6-Adresse.
- **Static IPv6**: Für Geräte oder Dienste, die eine feste IPv6-Adresse benötigen, etwa Server oder Netzwerkdrucker. Das Gerät verwendet dauerhaft dieselbe Adresse, was Verwaltung und Zugriff vereinfacht.

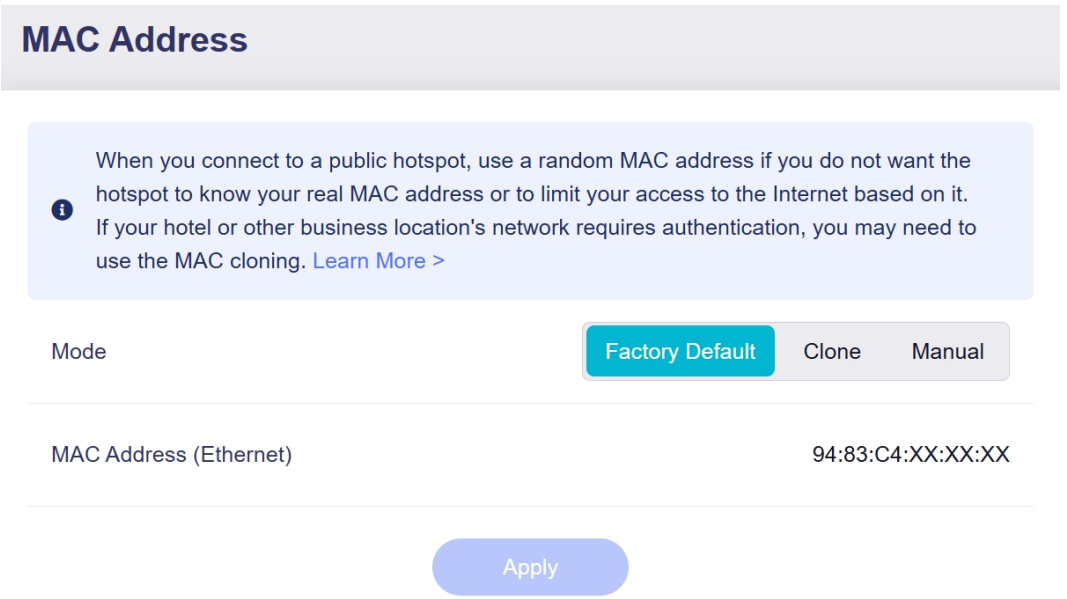
12.6.2 DNS-Adressen beziehen

Diese Einstellung bestimmt, wie der Router IPv6-DNS-Serveradressen erhält. Zur Auswahl stehen Automatic und Manual.

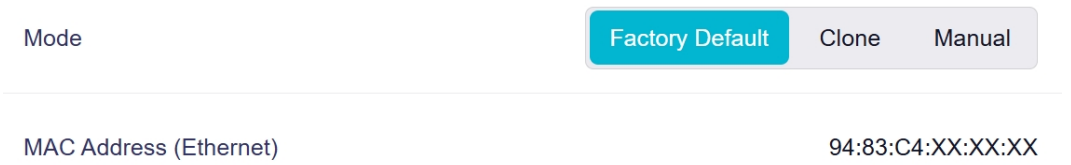
- **Automatic**: Der Router bezieht die IPv6-DNS-Serveradressen dynamisch, etwa über DHCPv6.
- **Manual**: Geben Sie eigene IPv6-DNS-Serveradressen ein. Da DNS Domainnamen in die zugehörigen IP-Adressen auflöst, kann eine manuelle Konfiguration zu Fehlern bei der Namensauflösung führen. Verwenden Sie diese Option mit Bedacht.

12.7 MAC-Adresse

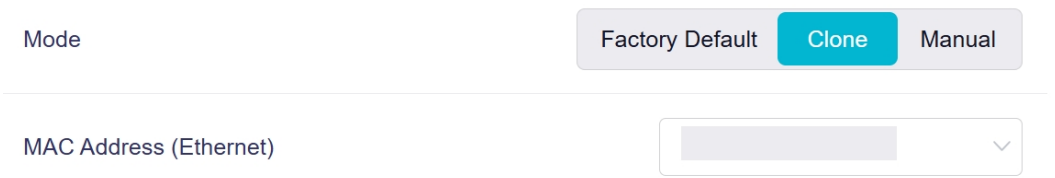
Auf der Seite MAC Address sehen Sie die voreingestellte MAC-Adresse des Routers. Sie können die MAC-Adresse eines Endgeräts klonen, eine Adresse manuell eingeben oder eine zufällige Adresse erzeugen. Unterstützt das Gerät mehrere Ethernetanschlüsse als WAN-Anschlüsse, lässt sich die MAC-Adresse jedes Anschlusses separat festlegen. Die Einstellung gilt nur, wenn der betreffende Anschluss als WAN-Anschluss verwendet wird.



- **Werkseitig voreingestellte MAC-Adresse.**

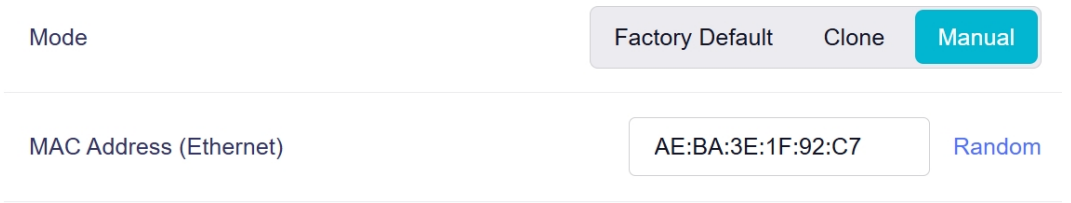


- **MAC-Adresse eines Endgeräts klonen.**



Hinweis: Viele neuere Geräte verwenden für unterschiedliche WLANs jeweils eine zufällige MAC-Adresse. Die hier angezeigte Adresse kann daher von der tatsächlichen Hardwareadresse abweichen. Je nach Gerät heißt diese Funktion auch „Private WLAN-Adresse“ oder „Zufällige Hardwareadresse“.

- **MAC-Adresse manuell eingeben oder zufällig erzeugen.**

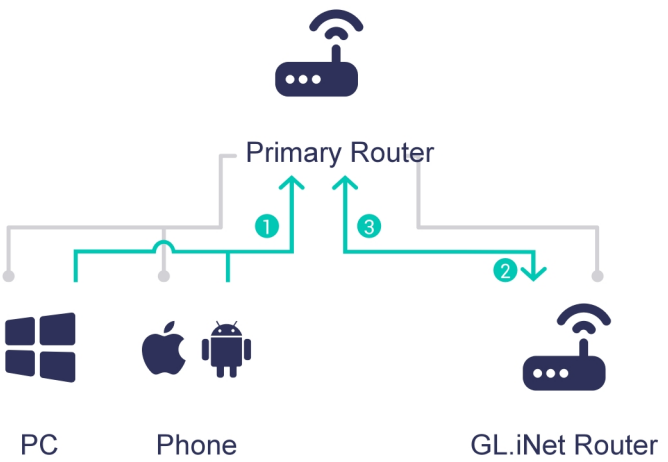


12.8 Drop-in Gateway

Drop-in Gateway erweitert die Funktionen eines vorhandenen Hauptrouters, ohne dass Sie ihn ersetzen oder neu konfigurieren müssen. Verbinden Sie den GL.iNet-Router per Ethernetkabel mit dem Hauptrouter, um das bestehende Netzwerk beispielsweise um folgende Funktionen zu ergänzen:

- VPN-Client verwenden
- Verschlüsseltes DNS nutzen

Drop-in Gateway arbeitet als zwischengeschaltetes System. Der Datenverkehr der Endgeräte wird zur Verarbeitung durch den GL.iNet-Router und anschließend über den Hauptrouter weitergeleitet. Die vorhandenen Netzwerkeinstellungen bleiben erhalten, damit alle Geräte durchgehend verbunden bleiben. Sie können den Datenverkehr aller oder nur ausgewählter Endgeräte verwalten.



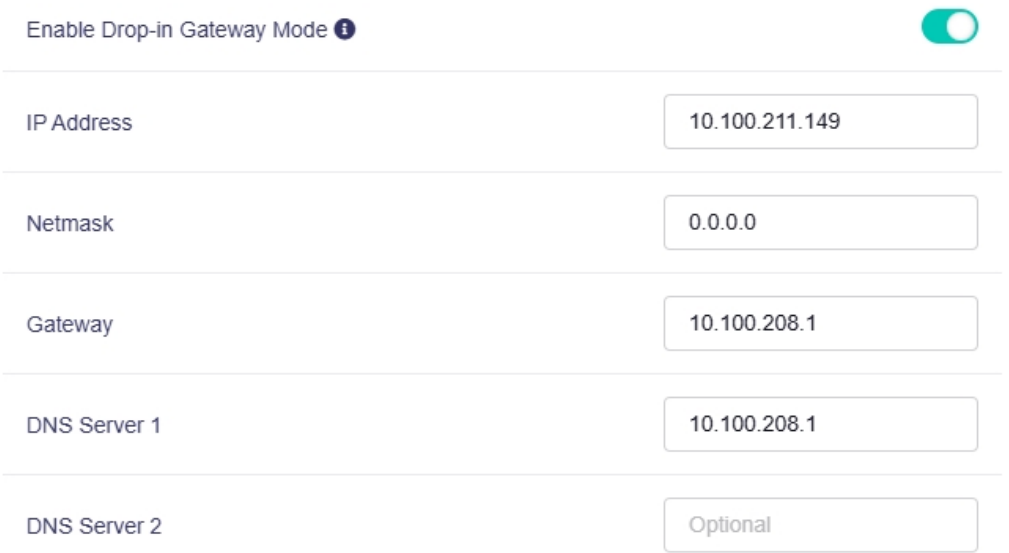
Das obige Diagramm enthält graue Linien sowie grüne Linien mit drei nummerierten Pfeilen.

- **Graue Linien** zeigen die physischen Verbindungen: Endgeräte wie Computer und Laptops sind mit dem Hauptrouter verbunden. Dessen LAN-Anschluss ist per Ethernetkabel mit dem WAN-Anschluss des GL.iNet-Routers verbunden, auf dem Drop-in Gateway aktiviert ist.
- **Grüne Linien** zeigen den Datenweg bei aktiviertem Drop-in Gateway. Die nummerierten Pfeile geben die Reihenfolge an:

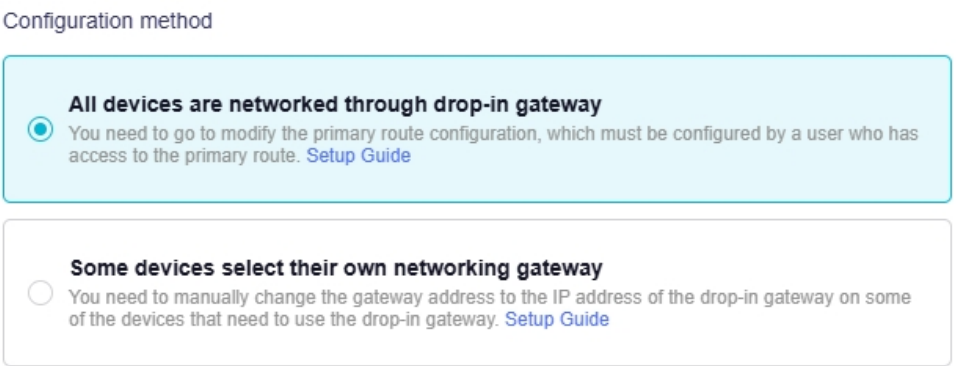
1. Der Datenverkehr der Endgeräte gelangt zunächst zum Hauptrouter.
2. Der Hauptrouter leitet ihn zur Verarbeitung an den GL.iNet-Router weiter, etwa zum Filtern von Werbung oder zur VPN-Verschlüsselung.
3. Nach der Verarbeitung gelangt der Datenverkehr zurück zum Hauptrouter. Dieser übermittelt die Daten an die ursprünglichen Endgeräte oder leitet sie ins Internet weiter.

Gehen Sie bei Bedarf wie folgt vor, um Drop-in Gateway zu aktivieren.

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Drop-in Gateway**. Aktivieren Sie **Enable Drop-in Gateway Mode** und prüfen Sie die Netzwerkparameter.



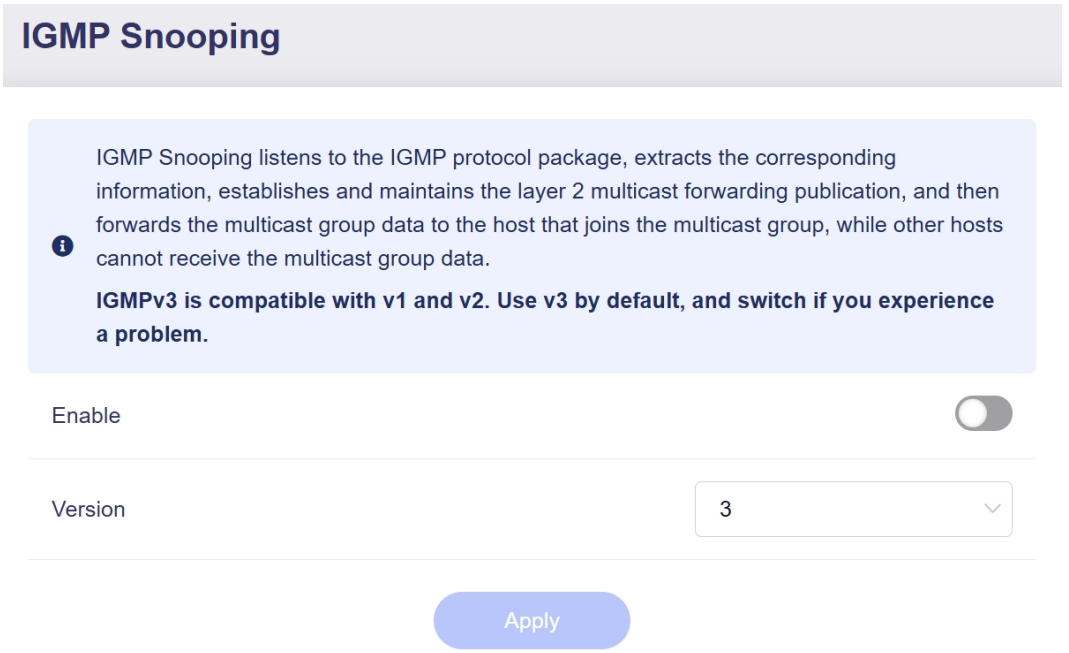
2. Wählen Sie die Konfigurationsmethode aus und klicken Sie auf **Apply**. Einzelheiten finden Sie in dieser Anleitung.



12.9 IGMP Snooping

IGMP Snooping überwacht IGMP-Protokollpakete und entnimmt ihnen die erforderlichen Informationen, um eine Multicast-Weiterleitungstabelle auf Schicht 2 aufzubauen und zu pflegen. Multicast-Daten werden dadurch nur an Geräte weitergeleitet, die der betreffenden Multicast-Gruppe beigetreten sind. Andere Geräte erhalten diese Daten nicht.

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **IGMP Snooping**. Aktivieren Sie die Funktion bei Bedarf, um Multicast auf Ihrem Router zu nutzen.



Kapitel 13

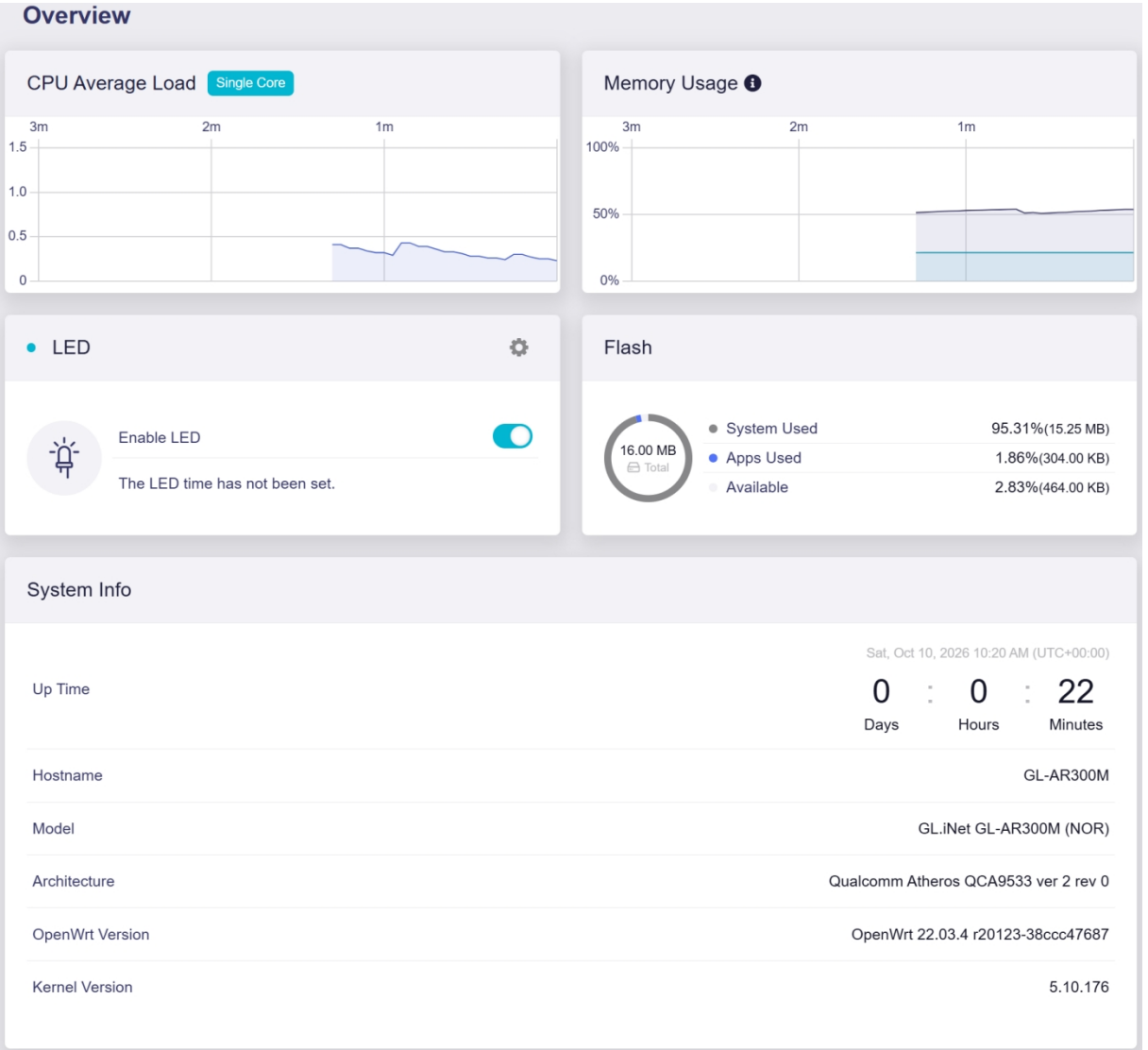
System

Dieses Kapitel beschreibt die Systemverwaltung des Geräts, darunter Systemübersicht, Aktualisierungen, geplante Aufgaben, Zeitzone, Protokolle, Zurücksetzen der Firmware und erweiterte Einstellungen.

13.1 Übersicht

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Overview**. Die Seite zeigt den Hardwarestatus und bietet einfache Steuerungsmöglichkeiten, darunter:

- CPU-, Arbeitsspeicher- und Flash-Status
- LED-Steuerung
- Geräteinformationen

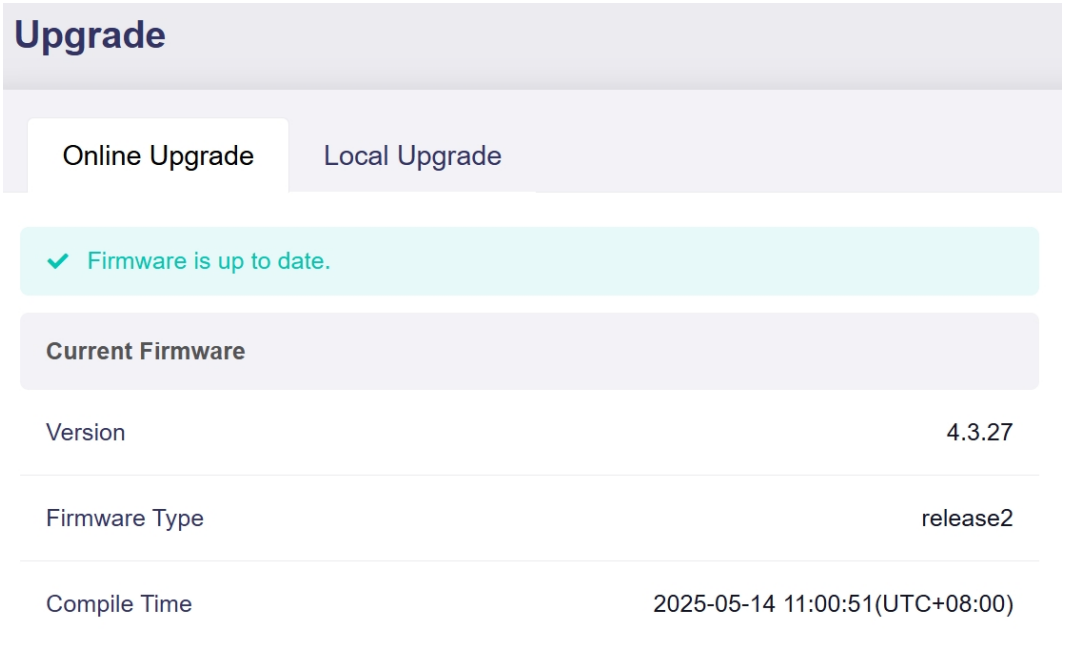


13.2 Aktualisierung

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Upgrade**. Sie können die Routerfirmware online oder lokal aktualisieren.

13.2.1 Online-Aktualisierung

Hier sehen Sie die aktuelle Firmwareversion, den Firmwaretyp (etwa Release oder Beta) und den Aktualisierungszeitpunkt. Bei bestehender Internetverbindung prüft der Router, ob eine neuere Firmware zum Herunterladen verfügbar ist.

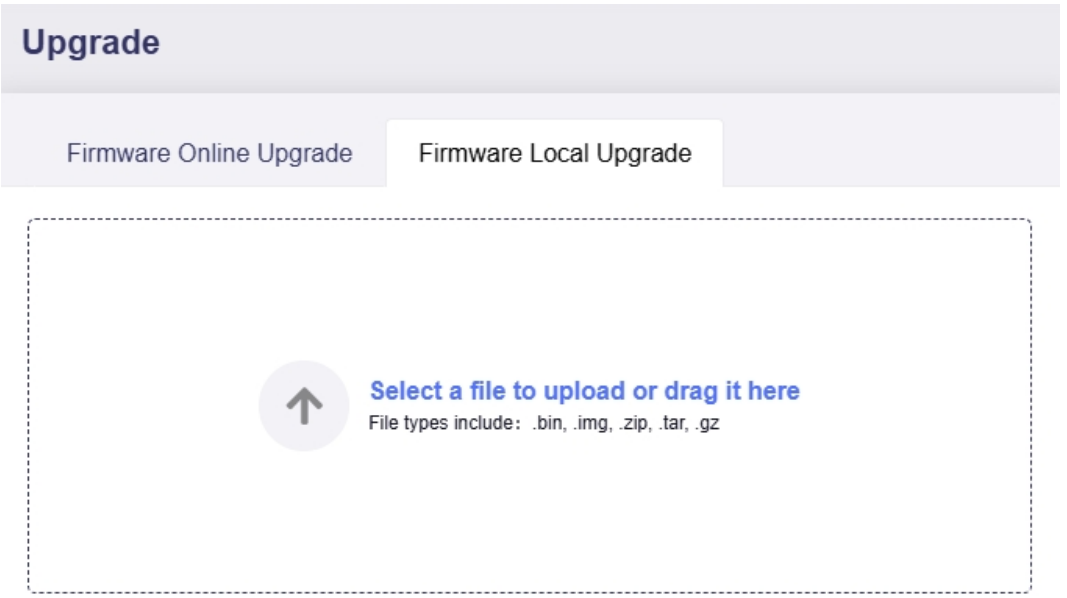


Tipp: Erscheint bei der Online-Aktualisierung **Download Failed**, öffnen Sie **SYSTEM** > **Time Zone** und korrigieren Sie die Zeitzone durch Synchronisierung mit dem Browser.

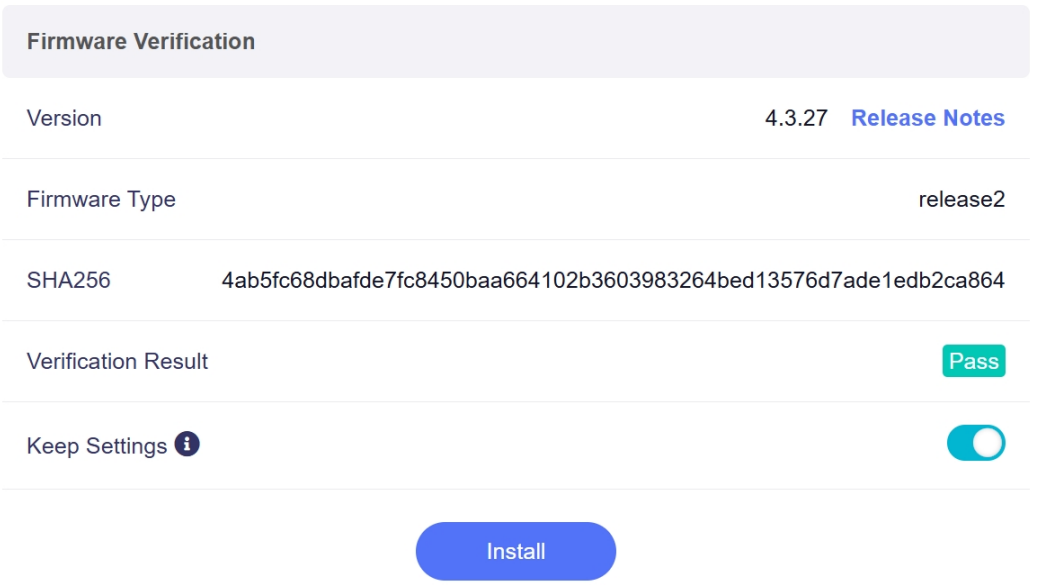
13.2.2 Lokale Aktualisierung

Für die lokale Aktualisierung benötigt der Router keine Internetverbindung.

Laden Sie das zu Ihrem Routermodell passende Firmwarepaket aus dem offiziellen Download Center auf Ihr lokales Gerät herunter. Melden Sie sich an der Weboberfläche an, öffnen Sie **SYSTEM** > **Upgrade** > **Local Upgrade** und laden Sie das Firmwarepaket hoch.



Die Firmwaredetails werden angezeigt. Prüfen Sie diese, bevor Sie auf **Install** klicken.



Bei aktiviertem **Keep Settings** bleiben die aktuellen Einstellungen erhalten. Manuell installierte Pakete müssen Sie nach der Aktualisierung erneut installieren. Aktivieren Sie diese Option nicht beim Wechsel auf eine ältere Firmwareversion.

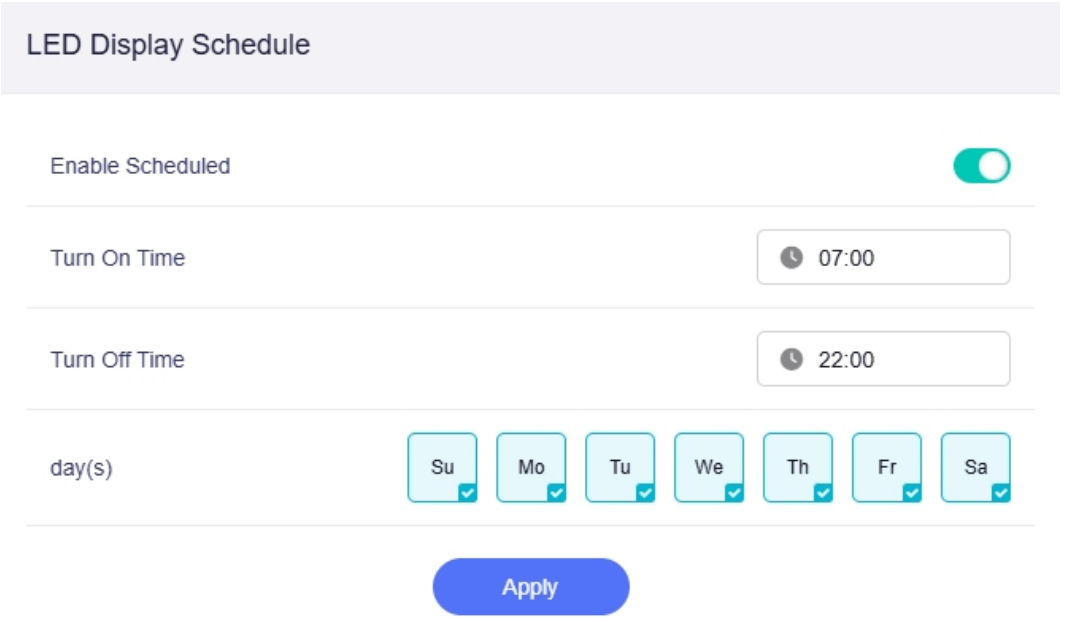
13.3 Geplante Aufgaben

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Scheduled Tasks**. Hier legen Sie tägliche Zeitpläne für grundlegende Aktionen fest, etwa das Ein- und Ausschalten der LED oder einen Routerneustart.

Hinweis: Synchronisieren Sie vor der Verwendung die Uhrzeit unter Time Zone. Ist das Gerät zum vorgesehenen Zeitpunkt ausgeschaltet, wird die Aufgabe nicht ausgeführt.

13.3.1 LED-Zeitplan

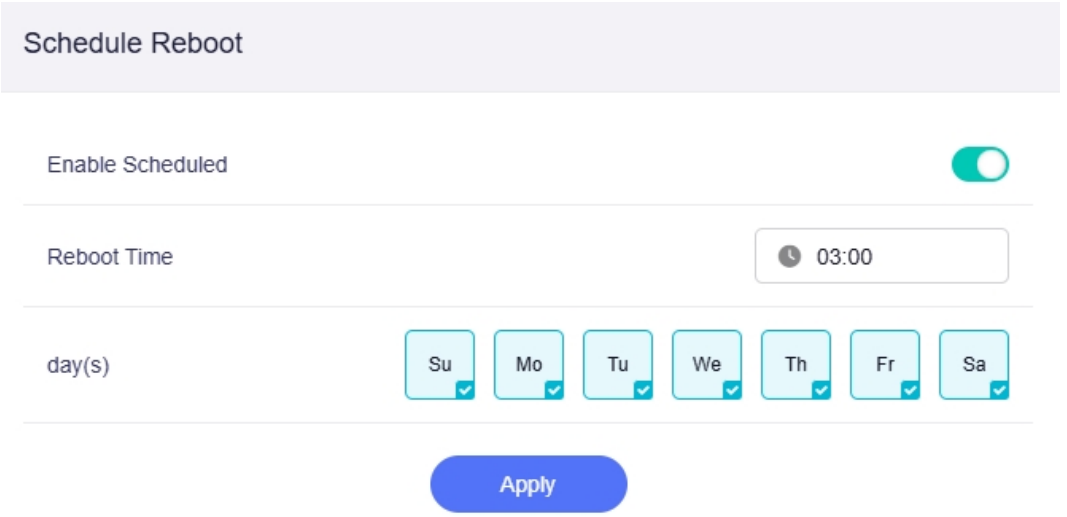
Legen Sie bei Bedarf einen Zeitplan für die Router-LED fest und klicken Sie auf **Apply**.



- **Enable Scheduled**: Aktiviert den LED-Zeitplan.
- **Turn On Time**: Uhrzeit zum Einschalten der LED, etwa 07:00 Uhr.
- **Turn Off Time**: Uhrzeit zum Ausschalten der LED, etwa 22:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

13.3.2 Geplanter Neustart

Legen Sie bei Bedarf einen Zeitplan für automatische Routerneustarts fest und klicken Sie auf **Apply**.



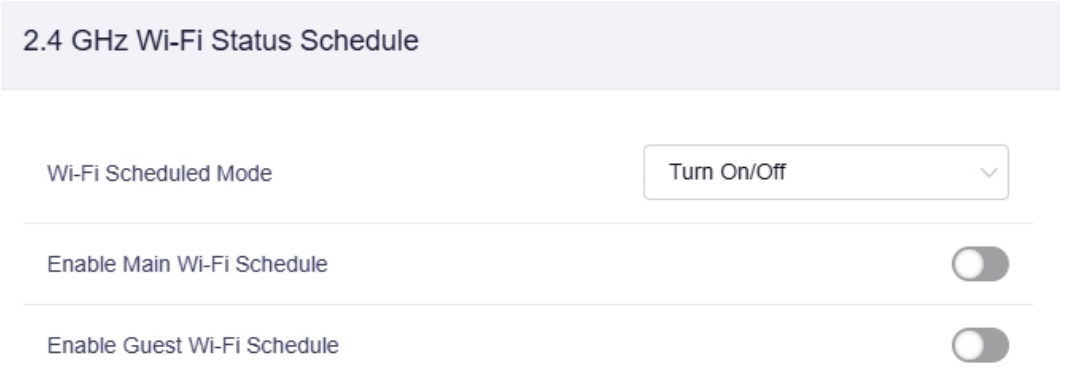
- **Enable Scheduled**: Aktiviert den geplanten Neustart.
- **Reboot Time**: Uhrzeit des Routerneustarts, etwa 03:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

13.3.3 Zeitplan für das 2,4-GHz-WLAN

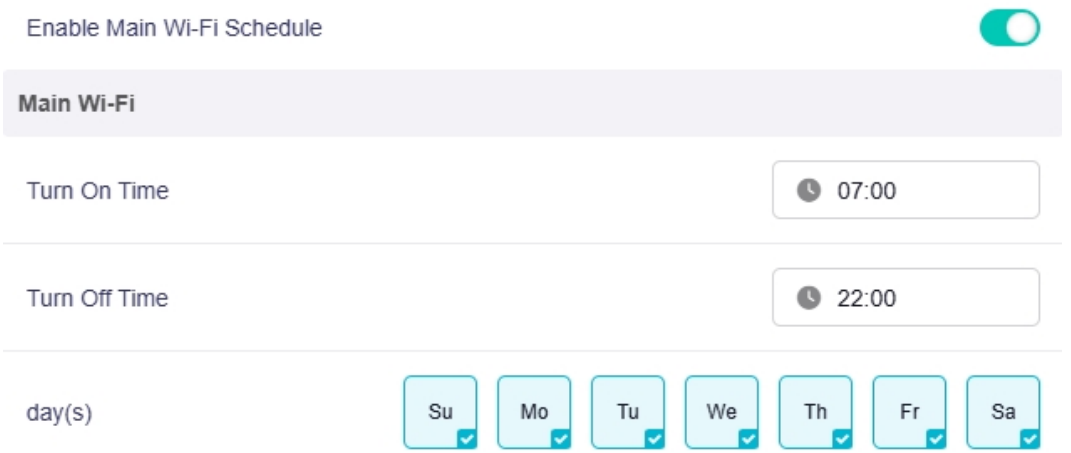
Hier legen Sie einen Zeitplan für Ihr 2,4-GHz-WLAN fest. Es gibt zwei Modi: Ein-/Ausschalten und Sendeleistung umschalten.

Modus 1: Ein-/Ausschalten

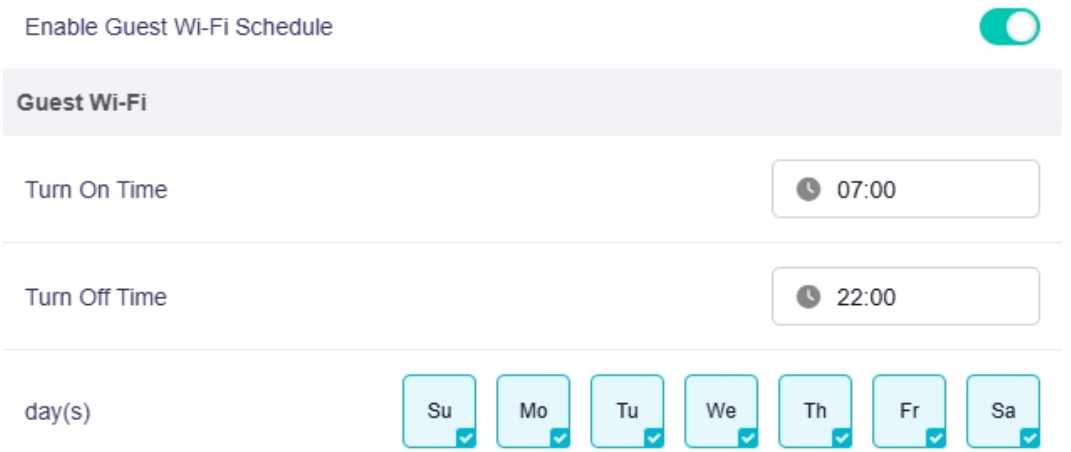
Sie können den Ein-/Ausschaltzeitplan sowohl für das 2,4-GHz-Hauptnetzwerk als auch für das Gastnetzwerk aktivieren.



- **Main Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 2,4-GHz-Hauptnetzwerk fest.

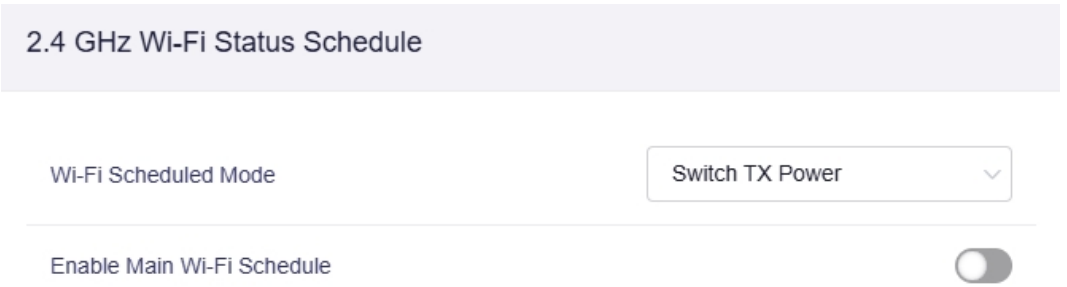


- **Guest Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 2,4-GHz-Gastnetzwerk fest.

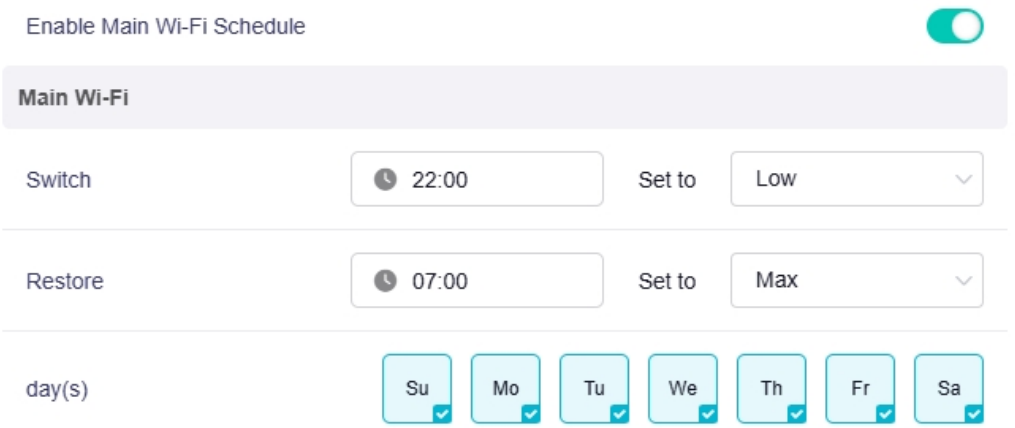


Modus 2: Sendeleistung umschalten

Für das 2,4-GHz-Hauptnetzwerk können Sie einen Zeitplan zum Umschalten der Sendeleistung aktivieren.



Legen Sie zwei zeitgesteuerte Aktionen zum Umschalten der Sendeleistung und die betreffenden Wochentage fest.

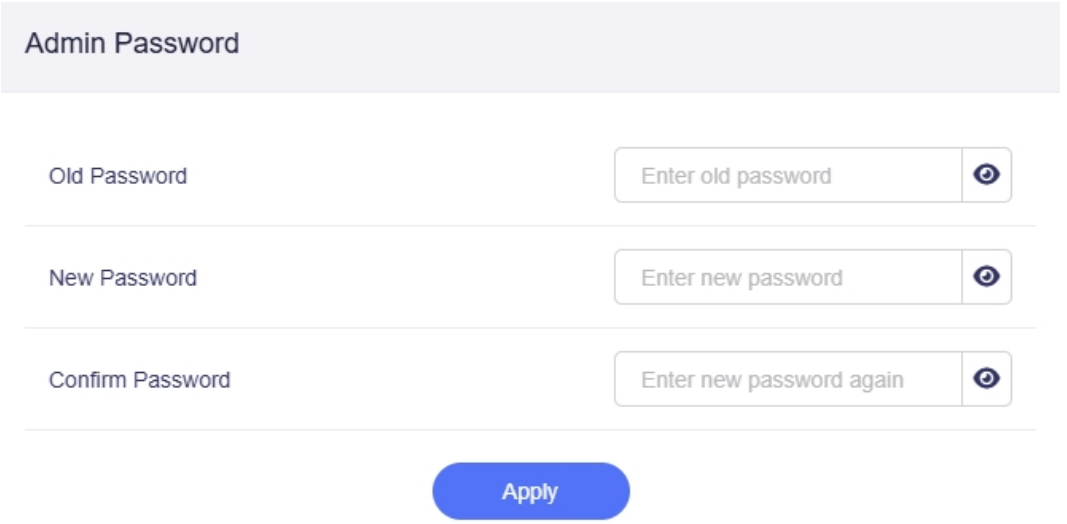


- **Switch**: Stellt die Sendeleistung zu einer bestimmten Uhrzeit, etwa 22:00 Uhr, auf eine festgelegte Stufe wie Low.

- **Restore**: Setzt die Sendeleistung zu einer anderen Uhrzeit, etwa 07:00 Uhr, auf eine andere Stufe wie Max zurück.
- **days**: Wochentage, an denen die Einstellungen gelten.

13.4 Administratorpasswort

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Admin Password**. Hier können Sie das Anmeldepasswort der Weboberfläche ändern.

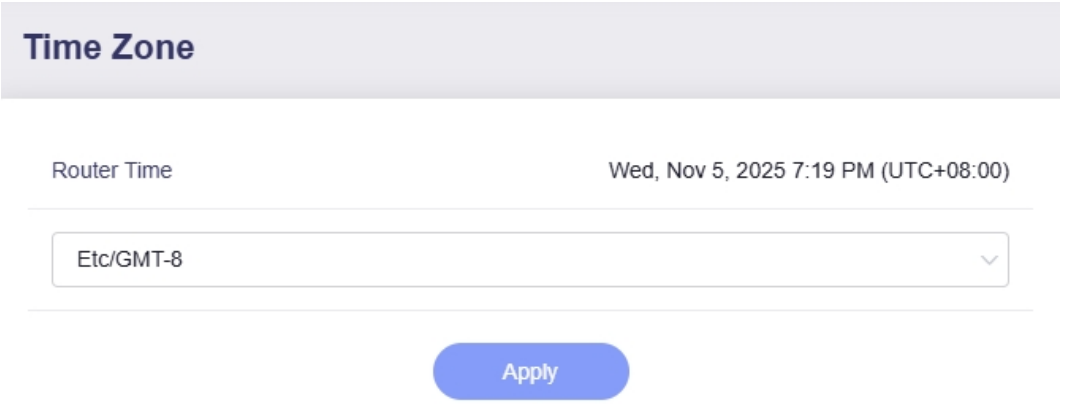


Für das Administratorpasswort gelten folgende Anforderungen:

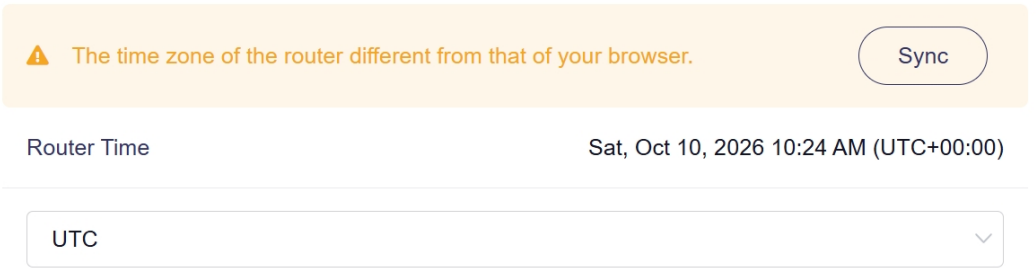
1. Mindestens 10 und höchstens 63 Zeichen.
2. Zulässig sind Buchstaben (Groß-/Kleinschreibung wird unterschieden), Ziffern und Sonderzeichen, etwa ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~ .
3. Mindestens zwei Zeichentypen aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen sind erforderlich.

13.5 Zeitzone

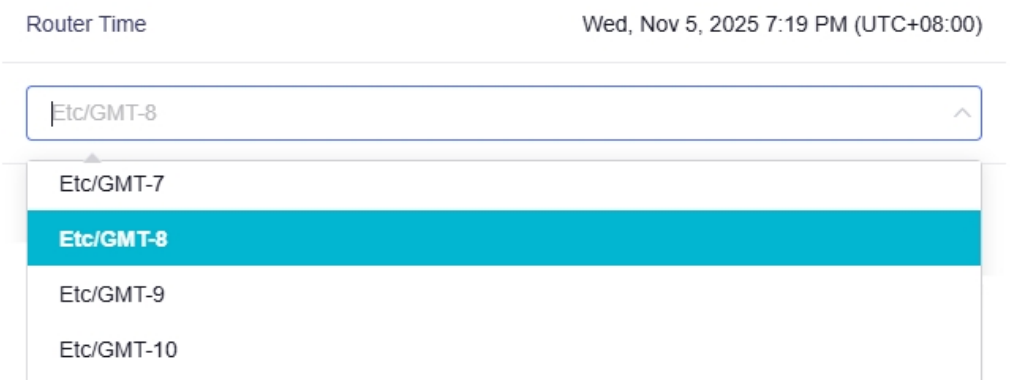
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Time Zone**. Die Seite zeigt die Systemzeit Ihres Routers mit Datum, Uhrzeit und Zeitzonenversatz an.



Einige Funktionen benötigen die korrekte Systemzeit. Stellen Sie deshalb sicher, dass die richtige Zeitzone synchronisiert ist. Weicht die Zeitzone des Routers von der des Browsers ab, erscheint der folgende Hinweis. Klicken Sie auf **Sync**, um die Zeitzone zu synchronisieren.

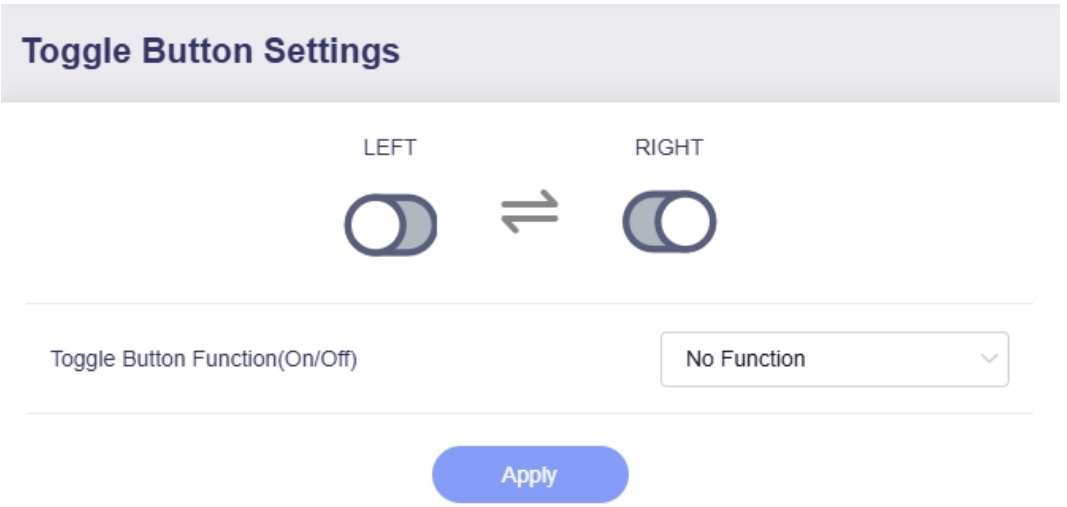


Wählen Sie zum Ändern der Zeitzone den passenden Eintrag aus der Liste, damit die Routerzeit Ihrer Ortszeit entspricht.

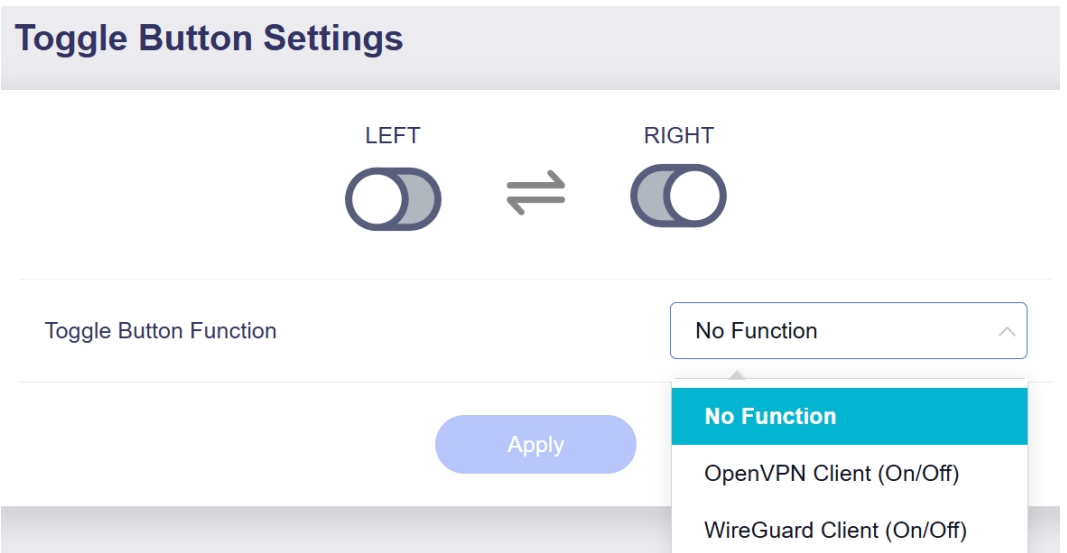


13.6 Schiebeschalter konfigurieren

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Toggle Button Settings**. Hier können Sie dem seitlichen Schiebeschalter eine Funktion zuweisen und so die Bedienung vereinfachen.

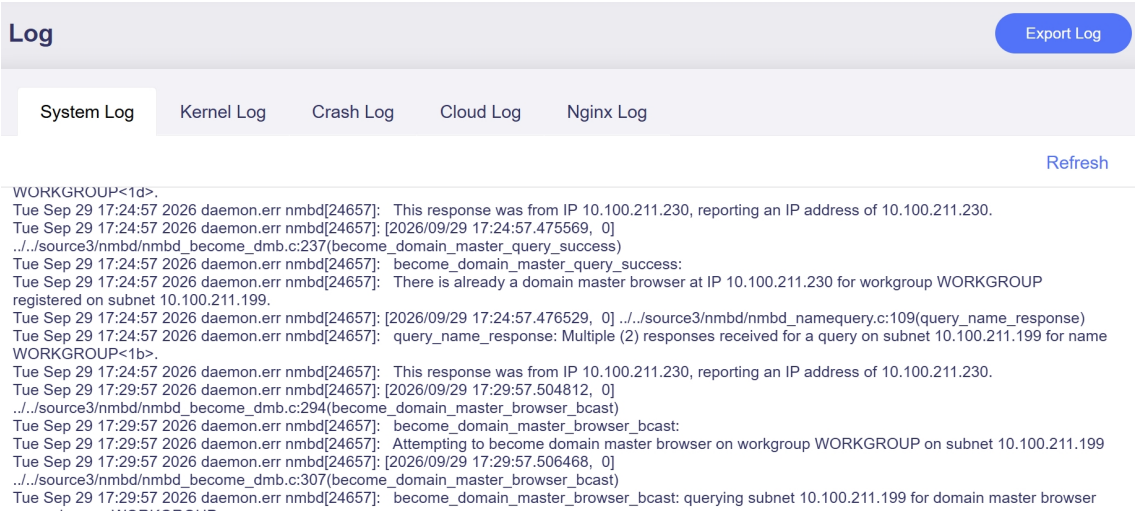


Standardmäßig ist dem Schalter keine Funktion zugewiesen. Bei Bedarf können Sie damit eine bestimmte Funktion durch einfaches Umschalten ein- oder ausschalten.



13.7 Protokolle

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Log**. Hier sehen Sie System-, Kernel-, Absturz-, Cloud- und Nginx-Protokolle zur Analyse und Fehlerbehebung.

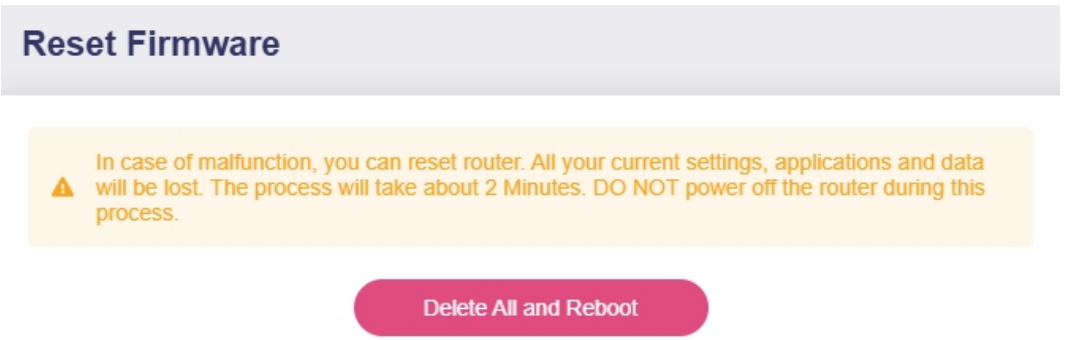


- **Refresh**: Aktualisiert die Protokolle.
- **Export Log**: Exportiert die Protokolle zusammen mit Debug-Informationen.

13.8 Firmware zurücksetzen

Bei Fehlfunktionen können Sie versuchen, das Problem durch Zurücksetzen der Firmware zu beheben.

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Reset Firmware**. Klicken Sie bei Bedarf auf **Delete All and Reboot**, um die Firmware zurückzusetzen.



Hinweis: Alle aktuellen Einstellungen, Anwendungen und Daten werden gelöscht. Der Vorgang dauert etwa zwei Minuten. Schalten Sie den Router währenddessen nicht aus.

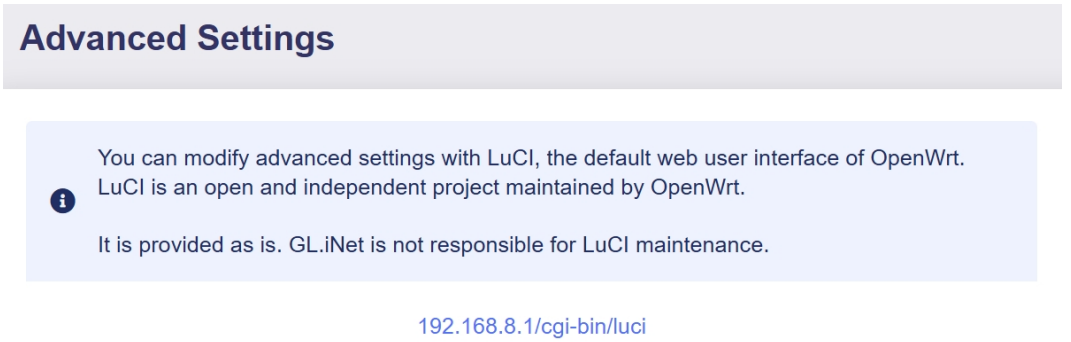
Falls Sie die Weboberfläche nicht erreichen, setzen Sie den Router mit der seitlichen Reset-Taste zurück.

13.9 Erweiterte Einstellungen

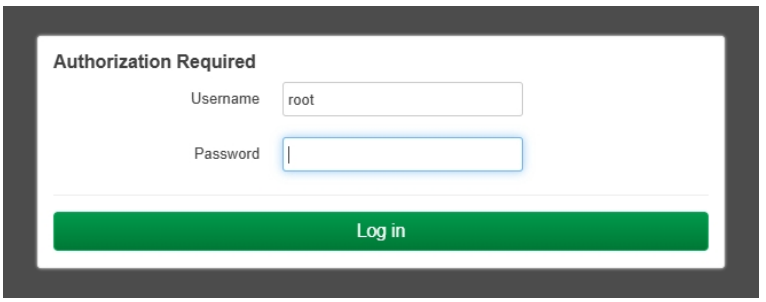
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Advanced Settings**. Hier ändern Sie erweiterte Einstellungen in LuCI, der standardmäßigen OpenWrt-Weboberfläche. LuCI ist ein offenes, unabhängiges Projekt, das von OpenWrt gepflegt und in der vorliegenden Form bereitgestellt wird. GL.iNet ist nicht für die Wartung von LuCI verantwortlich.

Gehen Sie wie folgt vor, um sich bei LuCI anzumelden.

1. Klicken Sie auf den Zugriffslink, um zur LuCI-Anmeldeseite zu gelangen.



2. Geben Sie das Anmeldepasswort ein. Es entspricht dem Passwort der Weboberfläche.



Sie sind nun an der LuCI-Oberfläche angemeldet.



Status

System

Hostname	GL-AR300M
Model	GL.iNet GL-AR300M (NOR)
Architecture	Qualcomm Atheros QCA9533 ver 2 rev 0
Target Platform	ath79/nand
Firmware Version	OpenWrt 22.03.4 r20123-38ccc47687 / LuCI openwrt-22.03 branch git-23.093.57104-ce20b4a
Kernel Version	5.10.176
Local Time	2026-10-10 10:36:47
Uptime	0h 6m 3s
Load Average	1.43, 1.09, 0.54