GL·iNet



Benutzerhandbuch

GL-MT2500 / Brume 2

Sicherheitsgateway

Firmware-Version 4.7.4

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 5

Kapitel 1 Ihren Router kennenlernen 7

1.1 Produktübersicht 8

1.1.1 Geräteansicht 8

1.1.2 Anschlüsse und Bedienelemente 9

1.1.3 LED-Anzeige 10

1.2 Technische Daten 10

1.3 Lieferumfang 12

Kapitel 2 Hardware anschließen 13

2.1 Standort auswählen 14

2.2 Router anschließen 14

Kapitel 3 Am Router anmelden 15

Kapitel 4 Internetverbindung einrichten 17

4.1 Schnelleinrichtungsassistent verwenden 18

4.2 Internetverbindung manuell einrichten 19

4.2.1 Internetverbindung über Ethernetkabel 20

4.2.2 Internetverbindung über USB-Tethering 25

4.2.3 Internetverbindung über ein USB-Modem 31

Kapitel 5 Verbundene Geräte 34

5.1 Gerätedetails 35

5.2 Aktionen 37

5.3 Geräte entfernen 40

5.4 Sortierung 41

Kapitel 6 Cloud-Dienste 42

6.1 GoodCloud 43

6.1.1 GoodCloud aktivieren 44

6.1.2 Router verwalten 47

6.1.3 Geräteverknüpfung aufheben 52

6.1.4 GoodCloud deaktivieren 52

6.2 AstroWarp 53

Kapitel 7 VPN kennenlernen 54

7.1 Einführung 55
7.2 Einsatzmöglichkeiten 56
Kapitel 8 VPN-Dashboard 59
8.1 VPN-Client 61
8.1.1 Client-Optionen 61
8.1.2 Proxy-Modus 63
8.1.3 Globale Optionen 64
8.2 VPN-Server 67
8.2.1 Server-Optionen 67
8.2.2 Server-Routingregeln 69
8.2.3 Globale Optionen 70
Kapitel 9 VPN-Server einrichten 71
9.1 OpenVPN-Server einrichten 72
9.1.1 Vorbereitung 72
9.1.2 Einrichtung 73
9.1.3 Fehlerbehebung 75
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 Hide.me einrichten 97
10.2.4 IPVanish einrichten 100
10.2.5 Mullvad einrichten 105
10.2.6 NordVPN einrichten 109
10.2.7 PIA (Private Internet Access) einrichten 115
10.2.8 Surfshark einrichten 120

10.2.9 WireGuard-Client manuell einrichten (andere Anbieter) 125
Kapitel 11 Tor 130
Kapitel 12 Anwendungen 133
12.1 Plug-ins 134
12.2 Dynamisches DNS 135
12.2.1 DDNS aktivieren 135
12.2.2 DDNS-Funktion prüfen 138
12.2.3 HTTPS-Fernzugriff 140
12.2.4 SSH-Fernzugriff 142
12.3 Netzwerkspeicher 144
12.3.1 Speicher anschließen 144
12.3.2 Samba einrichten 145
12.3.3 WebDAV einrichten 149
12.3.4 DLNA einrichten 152
12.4 AdGuard Home 153
12.5 Kindersicherung 156
12.5.1 Schnelleinrichtung 156
12.5.2 Fehlerbehebung 165
12.6 ZeroTier 166
12.6.1 ZeroTier einrichten 166
12.6.2 Fernzugriff auf WAN erlauben 171
12.6.3 Fernzugriff auf LAN erlauben 172
12.7 Tailscale 173
12.7.1 Tailscale einrichten 173
12.7.2 Fernzugriff auf WAN erlauben 176
12.7.3 Fernzugriff auf LAN erlauben 177
12.7.4 Eigene Exit-Nodes 178
Kapitel 13 Netzwerk 180
13.1 Portweiterleitung 181
13.1.1 DMZ 181
13.1.2 Portweiterleitung 182
13.2 Multi-WAN 185
13.2.1 Schnittstellenstatus überwachen 185
13.2.2 Multi-WAN-Modus 188

13.3 LAN 191
13.3.1 Grundeinstellungen 191
13.3.2 DHCP-Server 192
13.3.3 Adressreservierung 194
13.4 DNS 195
13.4.1 DNS-Servereinstellungen 196
13.4.2 Hosts bearbeiten 198
13.5 Portverwaltung 201
13.6 Netzwerkmodus 202
13.7 IPv6 204
13.7.1 IPv6-Modus 205
13.7.2 DNS-Adressen beziehen 205
13.8 Drop-in Gateway 206
13.9 IGMP Snooping 208
13.10 Netzwerkbeschleunigung 209
13.11 NAT-Einstellungen 211
Kapitel 14 System 212
14.1 Übersicht 213
14.2 Aktualisierung 214
14.2.1 Online-Aktualisierung 214
14.2.2 Lokale Aktualisierung 215
14.3 Geplante Aufgaben 216
14.3.1 LED-Zeitplan 216
14.3.2 Geplanter Neustart 217
14.4 Zeitzone 218
14.5 Protokolle 219
14.6 Sicherheit 221
14.6.1 Administratorpasswort 221
14.6.2 Zugriffskontrolle 222
14.6.3 Fernzugriffskontrolle 225
14.6.4 Ports am Router öffnen 226
14.7 Firmware zurücksetzen 227
14.8 Erweiterte Einstellungen 228

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.

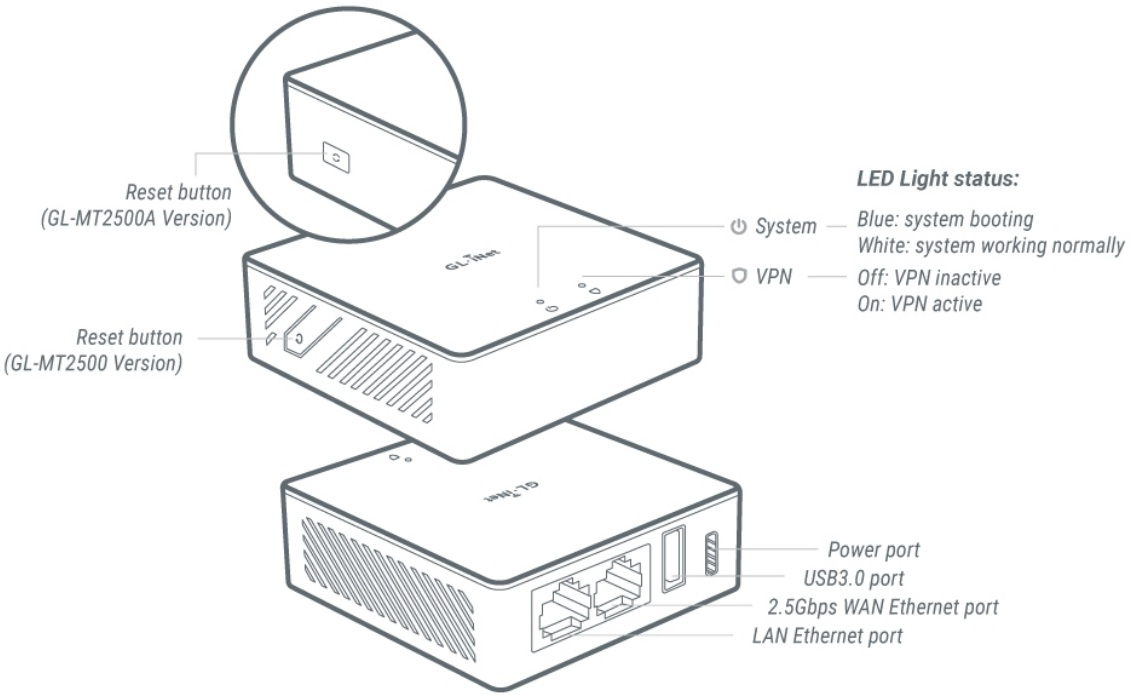
1.1 Produktübersicht

Brume 2 (GL-MT2500/GL-MT2500A) ist ein leichtes und leistungsfähiges VPN-Gateway mit dem Betriebssystem OpenWrt v21.02. Das kompakte Gerät eignet sich für den Betrieb eines VPN-Servers zu Hause oder eines SD-WAN (Site-to-Site) in kleinen und mittleren Unternehmen. Es ist in zwei Ausführungen erhältlich: GL-MT2500 mit Kunststoffgehäuse und GL-MT2500A mit Aluminiumgehäuse.

1.1.1 Geräteansicht



1.1.2 Anschlüsse und Bedienelemente



Element	Beschreibung
Stromanschluss	Zum Anschließen des Netzteils.
2,5-Gbit/s-WAN-Anschluss	Zum Anschließen eines Modems oder einer Ethernetdose für den Internetzugang.
LAN-Anschluss	Zum Anschließen kabelgebundener Geräte bei Bedarf.
USB-3.0-Anschluss	Für USB-Speichergeräte, USB-Tethering mit einem Smartphone und kompatible Mobilfunksticks.
Reset-Taste	Halten Sie die Taste **4 Sekunden** gedrückt und lassen Sie sie dann los, um Ihr Netzwerk zu reparieren. Die System-LED leuchtet blau und blinkt langsam, bis Ihre Netzwerkverbindung wiederhergestellt ist.

	Halten Sie die Taste **10 Sekunden** gedrückt und lassen Sie sie dann los, um den Router auf die Werkseinstellungen zurückzusetzen. Die System-LED leuchtet blau und blinkt schnell. Alle Daten werden gelöscht, sobald die LED dauerhaft blau leuchtet.

1.1.3 LED-Anzeige

LED	**Status**
System	Blau: System startet
	Weiß: Mit dem Internet verbunden
VPN	Aus: VPN inaktiv
	Ein: VPN aktiv

1.2 Technische Daten

Anschlüsse	1 × 2,5-Gbit/s-WAN-Ethernetanschluss 2 × 2,5-Gbit/s-LAN-Ethernetanschlüsse 1 × USB-3.0-Typ-C-Anschluss 1 × USB-C-Stromanschluss 1 × Reset-Taste
CPU	MediaTek MT7981B, Dual-Core, 1,3 GHz
Arbeitsspeicher / Speicher	1 GB DDR4 / 8 GB eMMC
Ethernet-Geschwindigkeit	WAN-Anschluss: 10/100/1000/2500 Mbit/s LAN-Anschluss: 10/100/1000 Mbit/s
Stromversorgung	USB-C, 5 V / 2 A
Leistungsaufnahme	< 2.6W
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Lagertemperatur	-20 ~ 70°C (-4 ~ 158°F)

Abmessungen / Gewicht	GL-MT2500: 70 × 70 × 22 mm / 60 g GL-MT2500A: 70 × 70 × 22 mm / 157 g
Weitere Ressourcen	Datenblatt / Firmware / App / Auspacken / Anleitungen

1.3 Lieferumfang

Im Lieferumfang enthalten:

- 1 × Brume 2 (GL-MT2500/GL-MT2500A)
- 1 × Benutzerhandbuch (Kurzanleitung)
- 1 × Ethernetkabel
- 1 × Dankeskarte
- 1 × Garantiekarte
- 1 × Netzteil
- 1 × Steckdosenadapter (je nach Lieferland)









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 - belüfteten 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.

2.2 Router anschließen

1. **Einschalten**
   Setzen Sie das zweiteilige Netzteil zusammen. Schließen Sie es an Ihren Brume 2 an und stecken Sie es in eine Steckdose. Das Gerät startet automatisch.
2. **Ein Gerät mit dem Router verbinden**
   Verbinden Sie ein kabelgebundenes Gerät, z. B. einen Computer oder Laptop, über ein Ethernetkabel mit dem LAN-Anschluss des Brume 2.
3. **Am Router anmelden**
   Wenn Sie sich zum ersten Mal mit dem Router verbinden, steht noch kein Internetzugang zur Verfügung. Melden Sie sich wie in Kapitel 3 beschrieben am Router an und schließen Sie die Ersteinrichtung ab, um auf das Internet zuzugreifen.

Kapitel 3

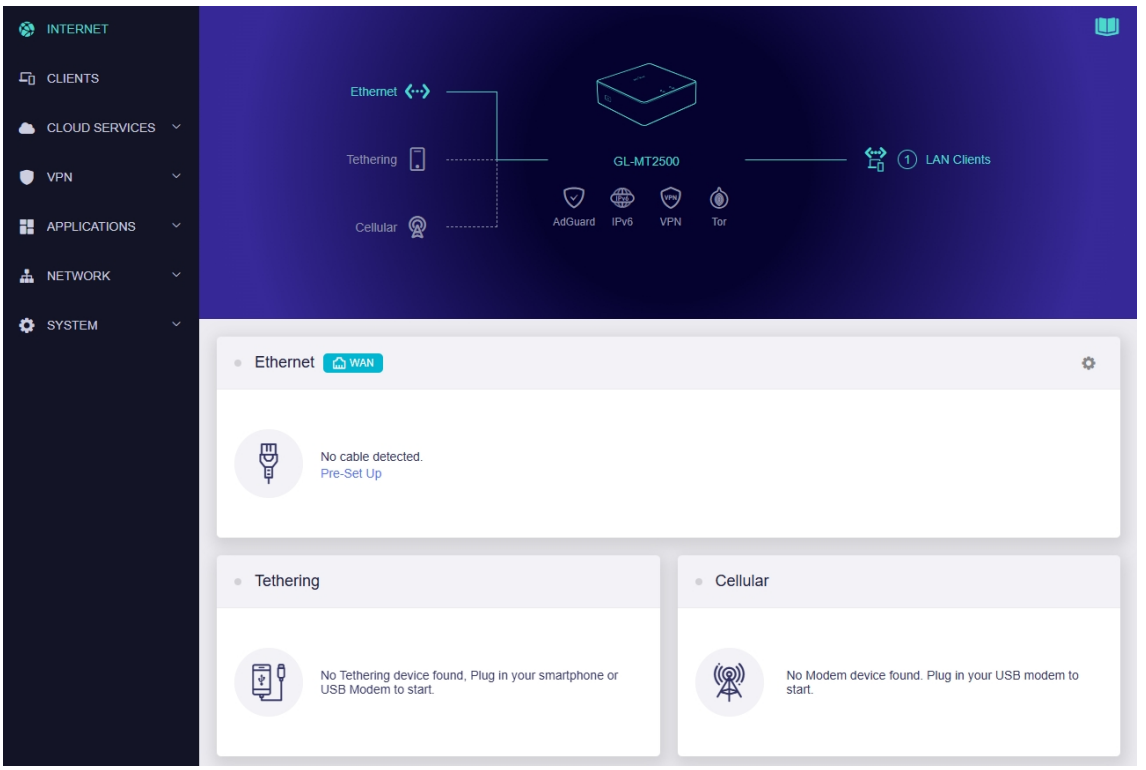
Am Router anmelden

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.

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

1. Verbinden Sie ein Gerät, z. B. einen Computer oder Laptop, über ein Ethernetkabel mit dem LAN-Anschluss des Brume 2.
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 öffnet sich die Weboberfläche des Brume 2.



Kapitel 4

Internetverbindung einrichten

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

4.1 Schnelleinrichtungsassistent verwenden

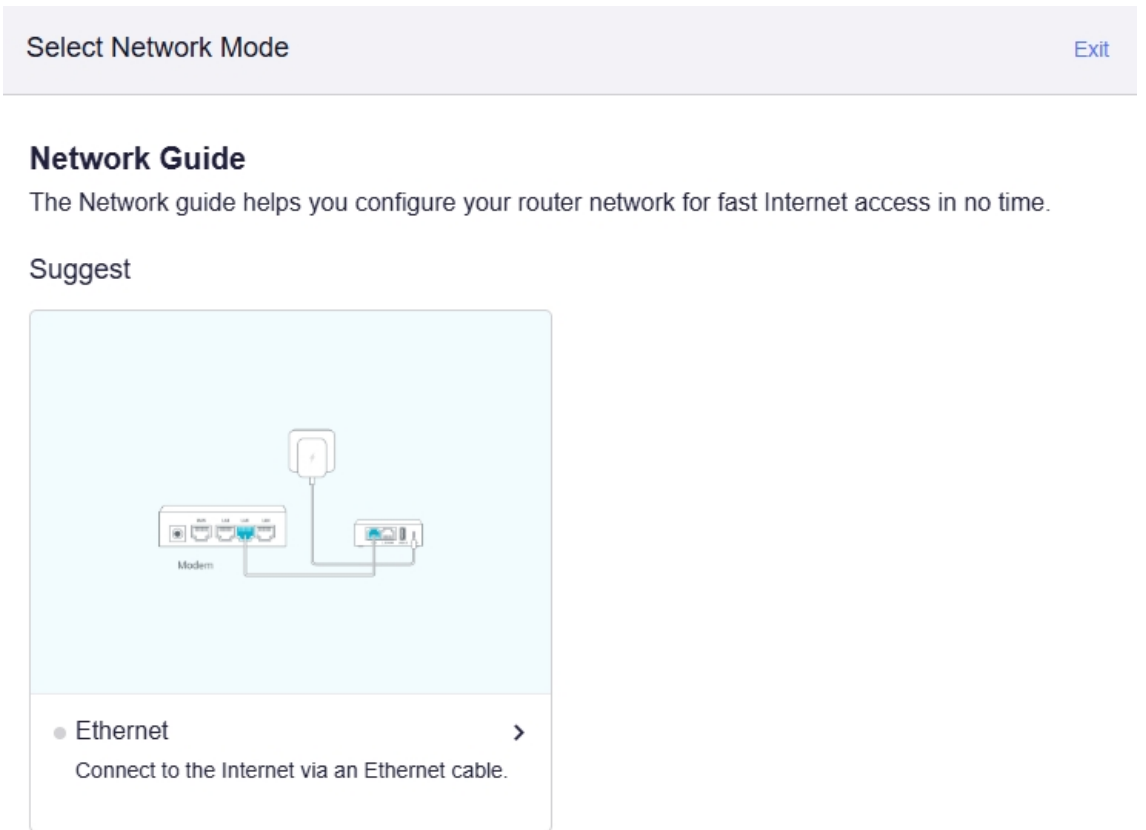
Der Einrichtungsassistent in der Weboberfläche führt Sie durch die Netzwerkkonfiguration des Routers.

Gehen Sie wie folgt vor, um den Assistenten zu starten.

1. Melden Sie sich an der Weboberfläche des Routers an, wie in Kapitel 3 beschrieben.
2. Klicken Sie auf der Startseite oben rechts auf das Buchsymbol.



3. Folgen Sie dem Einrichtungsassistenten, um Ihren Router zu konfigurieren und eine Internetverbindung herzustellen.



4.2 Internetverbindung manuell einrichten

Der Einrichtungsassistent ermöglicht eine schnelle Netzwerkeinrichtung. Bei der manuellen Einrichtung können Sie erweiterte Netzwerkeinstellungen an besondere Anforderungen anpassen und vorhandene Verbindungen bei Bedarf prüfen oder ändern.

Brume 2 unterstützt drei Arten des Internetzugangs: Ethernet, USB-Tethering und USB-Modem/Mobilfunk. Wählen Sie die für Ihren Einsatzzweck geeignete Verbindung.

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. **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.

3. **USB-Modem/Mobilfunk**: Stecken Sie ein USB-Mobilfunkmodem mit bereits eingesetzter SIM-Karte in den Router. Der Router verbindet sich dann über ein 4G-/5G-Mobilfunknetz mit dem Internet, unabhängig von einem festen Breitbandanschluss. Diese Verbindungsart bietet hohe Mobilität und eignet sich beispielsweise für den Einsatz im Fahrzeug oder im Freien.

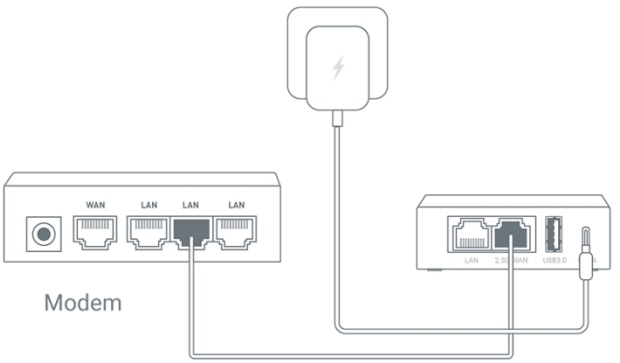
4.2.1 Internetverbindung über Ethernetkabel

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.

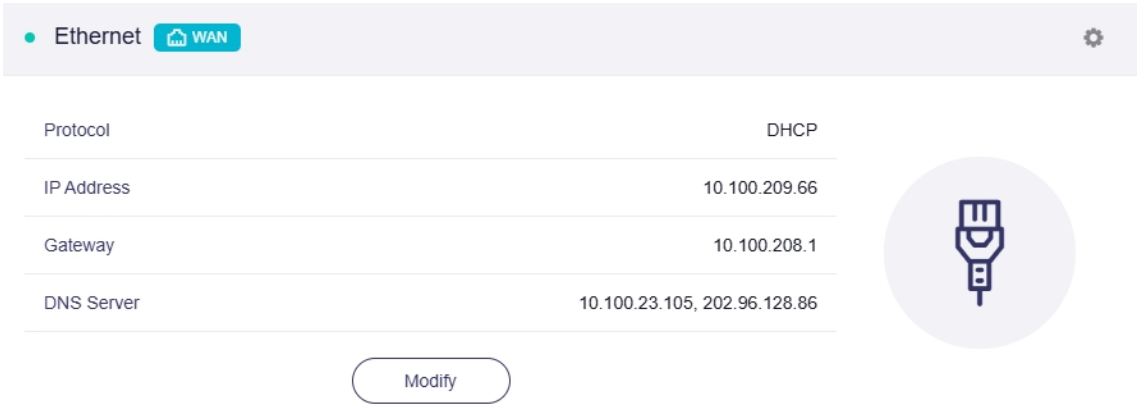
Grundeinrichtung

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.

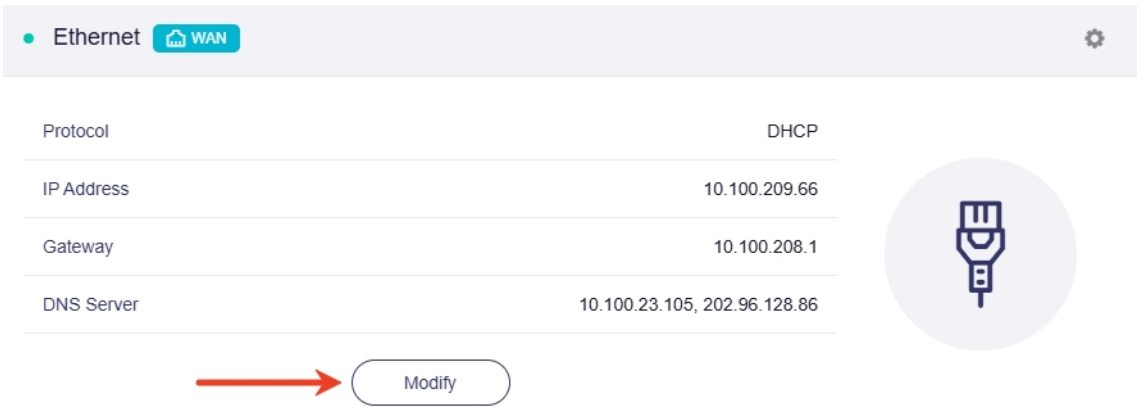


2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Ethernet**. Bei erfolgreicher Verbindung werden im Abschnitt Ethernet die Netzwerkdaten angezeigt, darunter Protokoll, IP-Adresse, Gateway und DNS-Server.

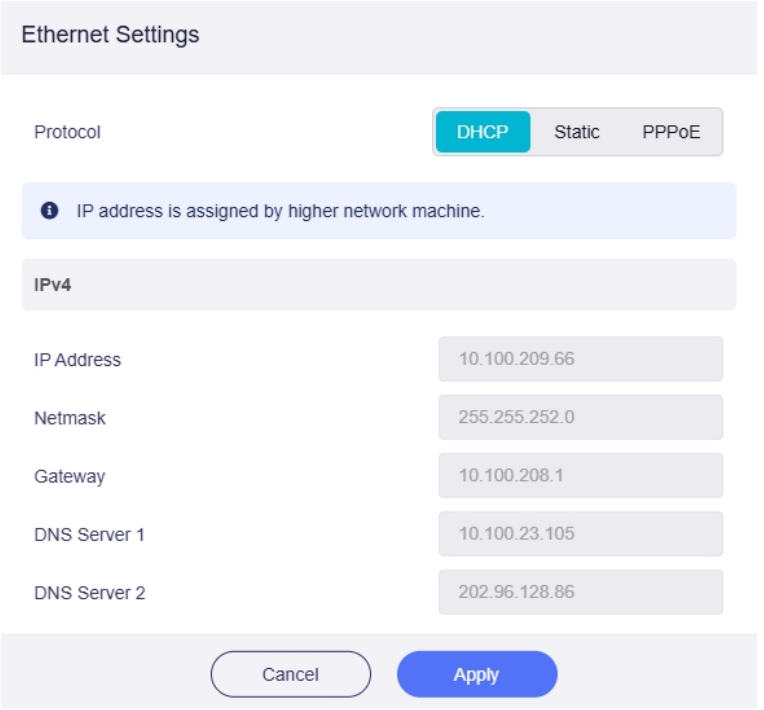


Protokoll

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

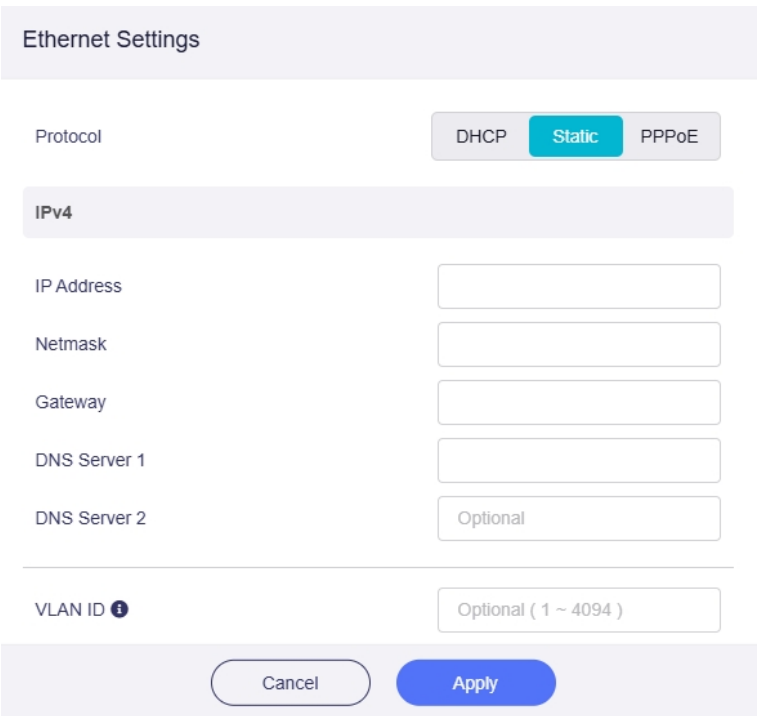


- **DHCP**
  DHCP ist das voreingestellte und am häufigsten verwendete Netzwerkprotokoll. Es weist Geräten in einem IP-Netzwerk nach dem Client-Server-Prinzip automatisch IP-Adressen und weitere Netzwerkeinstellungen zu.



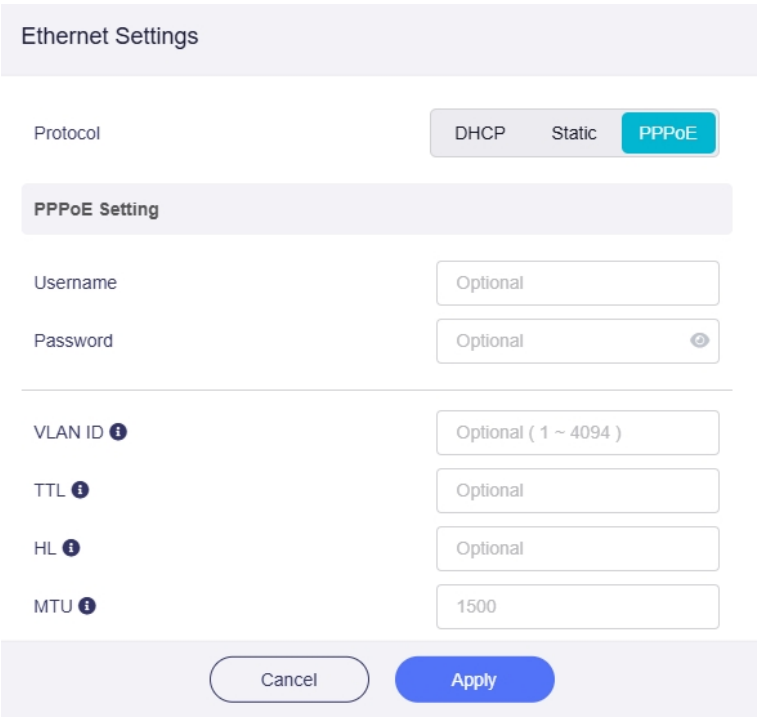
- **Statische IP-Adresse**

  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.



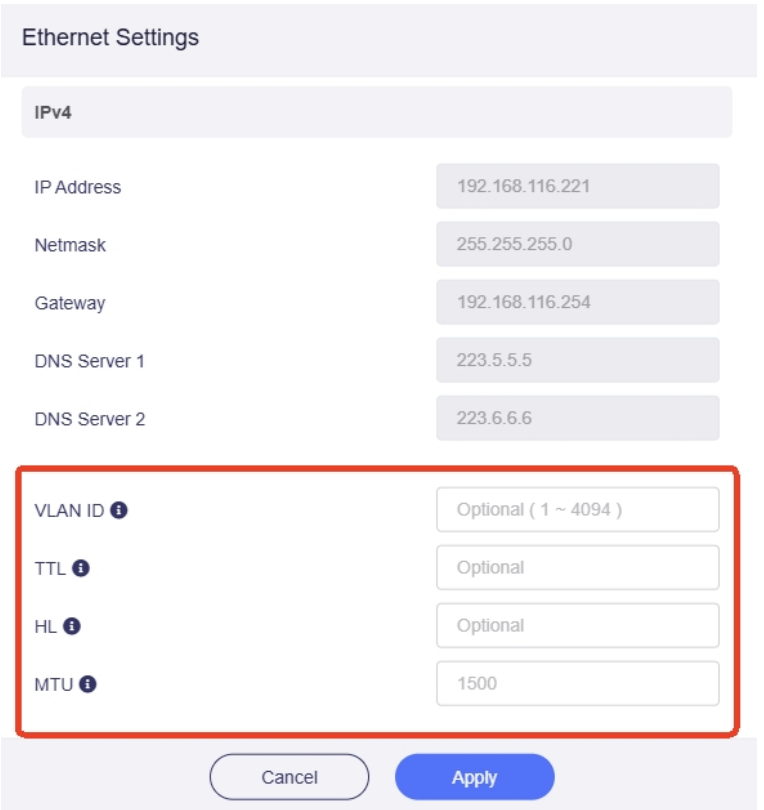
- **PPPoE**

  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.



Erweiterte Einstellungen

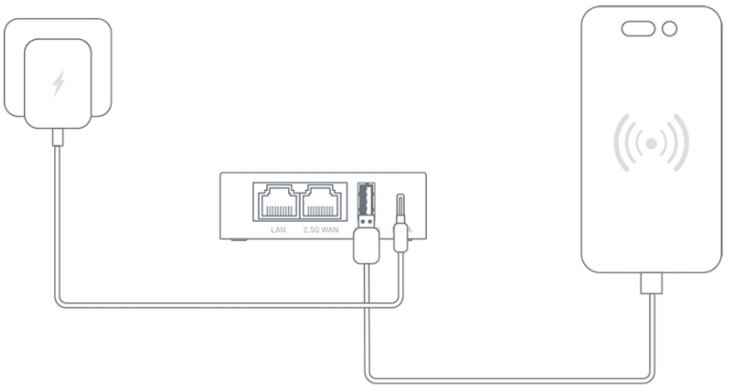
Zusätzlich zu den grundlegenden Einstellungen stehen für die drei oben genannten Protokolle optionale erweiterte Einstellungen zur Verfügung.



- **VLAN ID**
  Diese Einstellung ist nur erforderlich, wenn der Server des Internetanbieters eine bestimmte getaggte VLAN-ID für die Schnittstelle voraussetzt.
- **TTL**
  TTL (Time To Live) legt fest, wie lange Pakete höchstens im Netzwerk verbleiben dürfen. Standardmäßig verringert der Router die TTL eingehender Pakete von Clientgeräten vor der Weiterleitung um 1. Wenn Sie die TTL überschreiben bzw. vortäuschen möchten, geben Sie den gewünschten effektiven TTL-Wert plus 1 ein, um die automatische Verringerung auszugleichen. TTL gilt nur für IPv4.
- **HL**
  Bei IPv6 begrenzt das Feld HL (Hop Limit) die Anzahl der Übertragungsschritte eines Datenpakets im Netzwerk. Es entspricht der TTL bei IPv4.
- **MTU**
  Der Standardwert für die MTU beträgt 1500 Byte.

4.2.2 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.

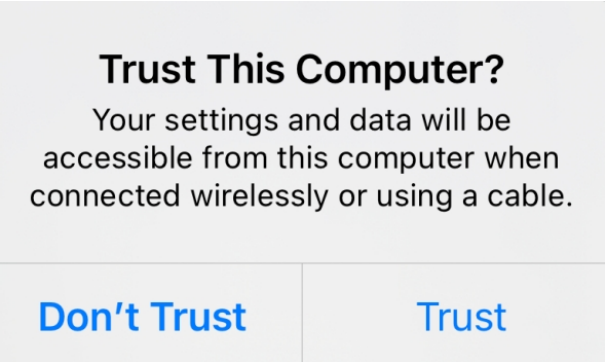


Auch ein Hostless-Modem kann bei seiner Einrichtung über die Tethering-Funktion betrieben werden.

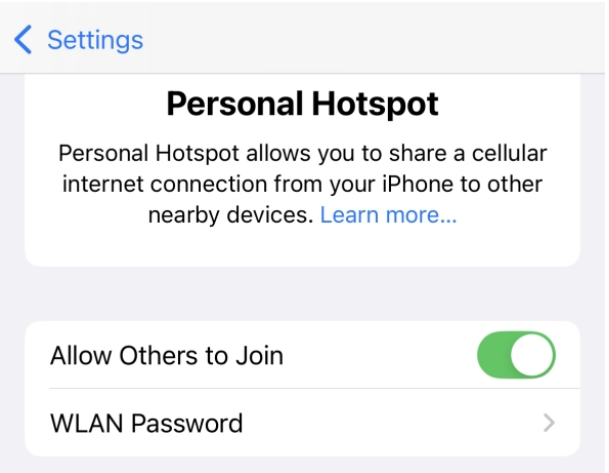
Hinweis: Einige Mobilfunkanbieter beschränken Tethering oder berechnen zusätzliche Gebühren. Erkundigen Sie sich bei Ihrem Anbieter.

Tethering mit einem iPhone

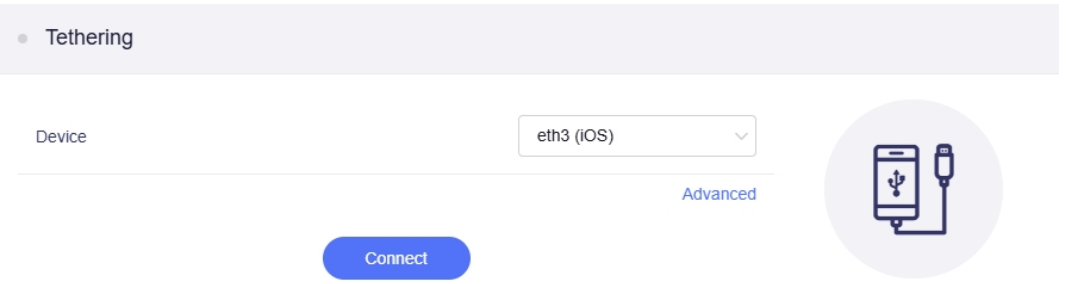
1. Verbinden Sie ein iPhone per USB-Kabel mit dem USB-Anschluss des Routers. Ein Systemdialog fragt, ob Sie diesem Gerät vertrauen. Tippen Sie auf **Vertrauen**, um fortzufahren.



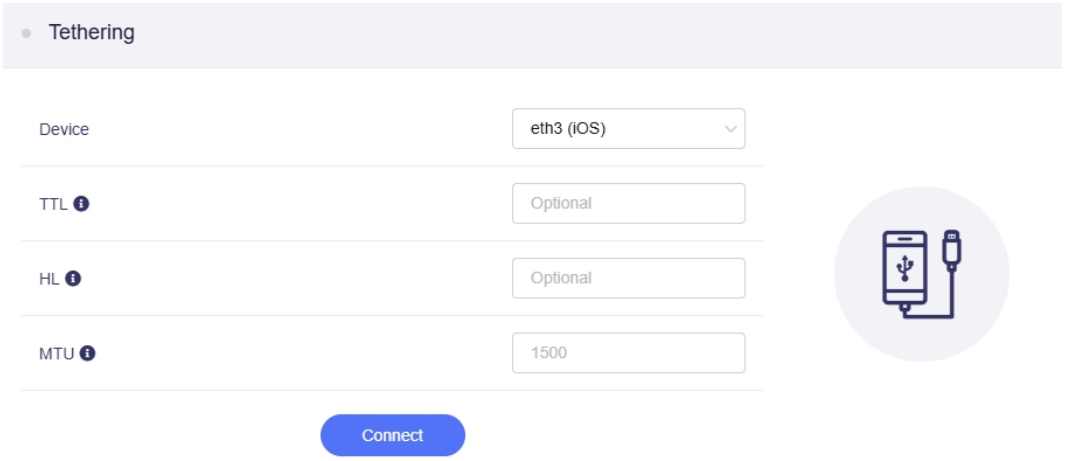
2. Öffnen Sie auf dem iPhone **Einstellungen** > **Persönlicher Hotspot**. Aktivieren Sie **Zugriff für andere erlauben**.



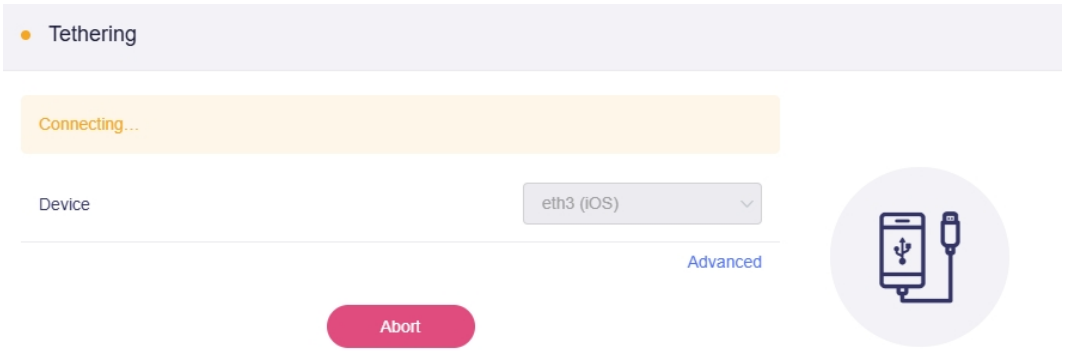
3. Verbinden Sie einen Computer oder ein anderes Smartphone mit dem Router. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie anschließend auf **Connect**.



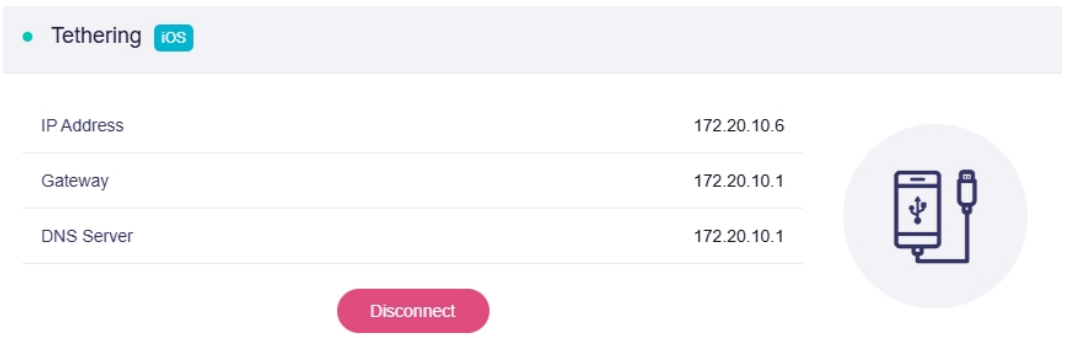
Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU anpassen möchten, klicken Sie auf **Advanced** und nehmen Sie die gewünschten Änderungen vor, bevor Sie auf **Connect** klicken.



4. Die Verbindung wird hergestellt.

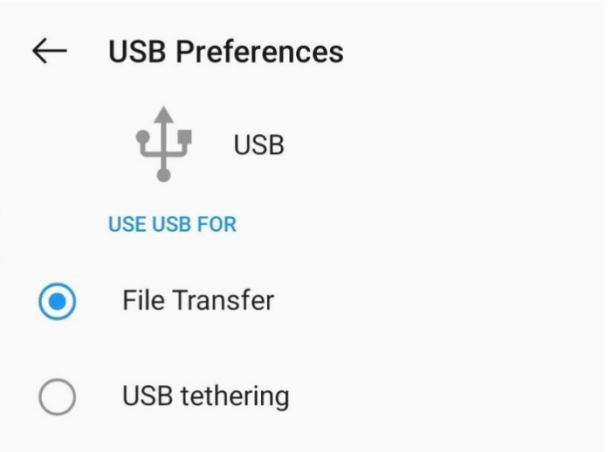


Nach erfolgreicher Verbindung werden auf dieser Seite die Details der Tethering-Verbindung angezeigt.

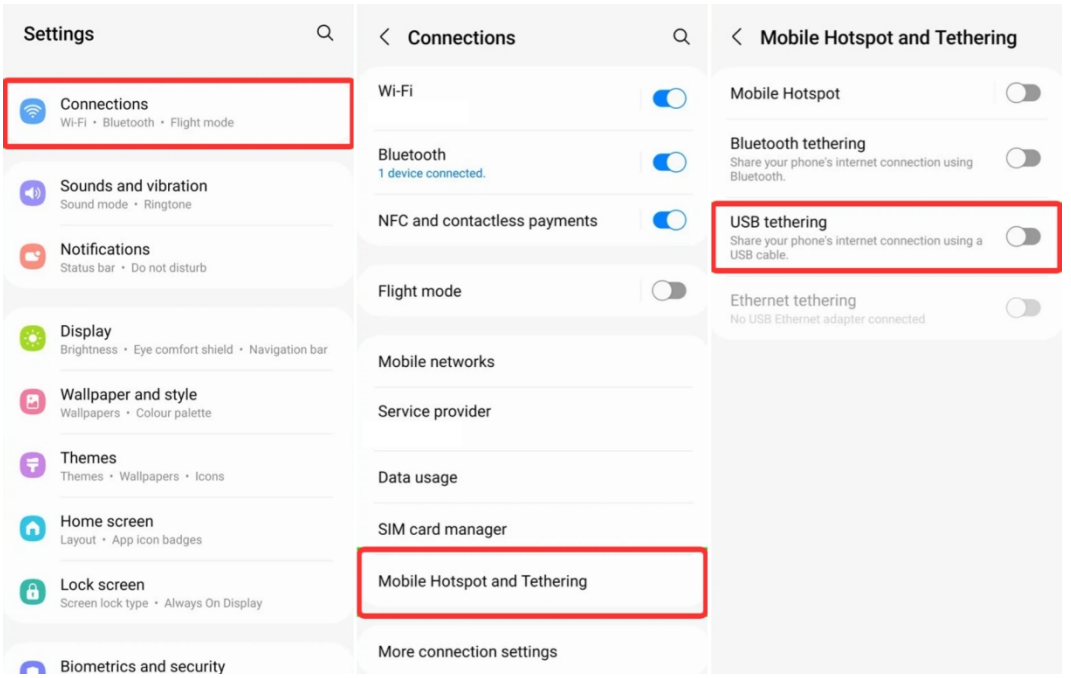


Tethering mit einem Android-Smartphone

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.

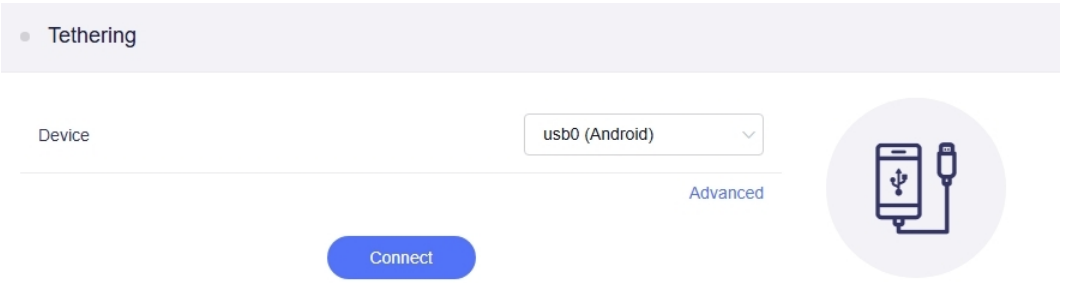


2. Öffnen Sie auf Ihrem Smartphone **Einstellungen** > **Netzwerk & Internet** > **Persönlicher Hotspot**.
   Aktivieren Sie **Persönlicher Hotspot** oder **USB-Tethering**.

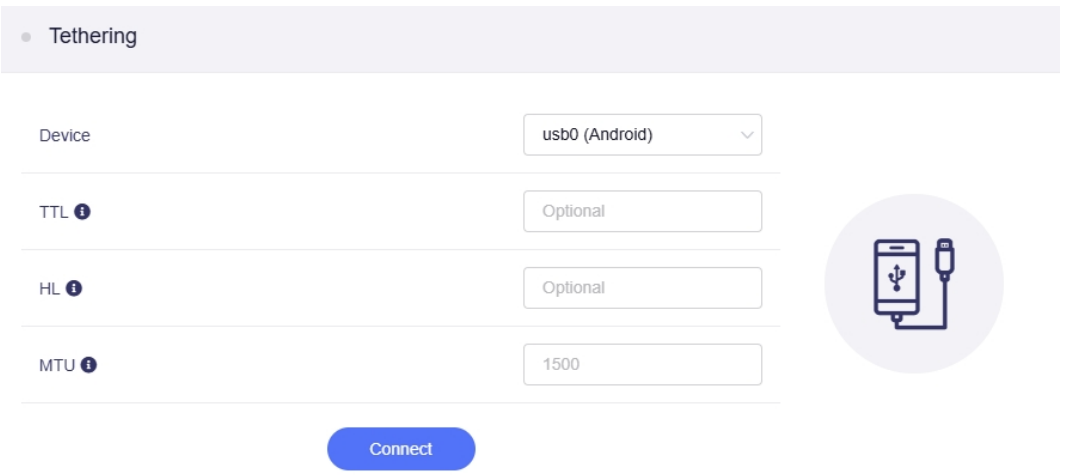


   (Die Schritte zum Aktivieren von USB-Tethering unterscheiden sich je nach Hersteller. Suchen Sie die entsprechende Option in den Geräteeinstellungen und wenden Sie sich bei Bedarf an den Support des Herstellers.)

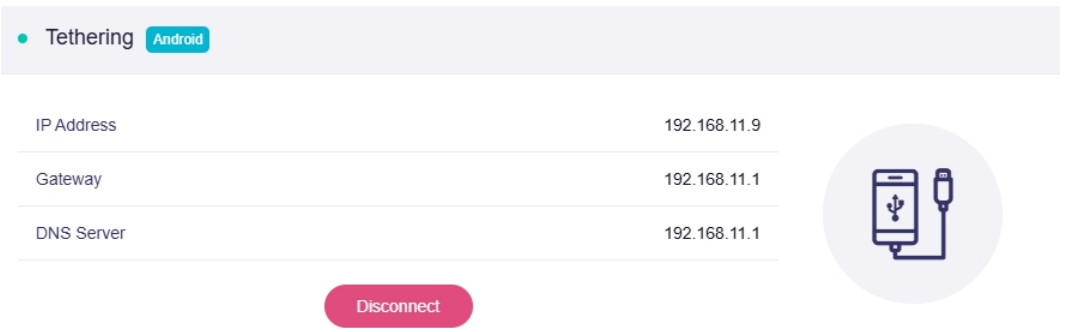
3. Verbinden Sie einen Computer oder ein anderes Smartphone mit dem Router. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie auf **Connect**.



Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU anpassen möchten, klicken Sie auf **Advanced** und nehmen Sie die gewünschten Änderungen vor, bevor Sie auf **Connect** klicken.



4. Die Verbindung wird hergestellt. Nach erfolgreichem Verbindungsaufbau zeigt diese Seite den Status der Tethering-Verbindung an.



Fehlerbehebung

Falls die Tethering-Verbindung fehlschlägt, versuchen Sie Folgendes:

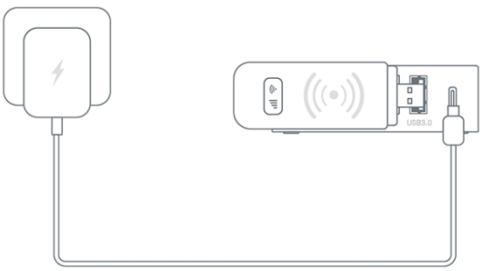
- Verwenden Sie das Originalnetzteil des Routers.
- Ziehen Sie das USB-Kabel ab und schließen Sie es erneut an.

- 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.

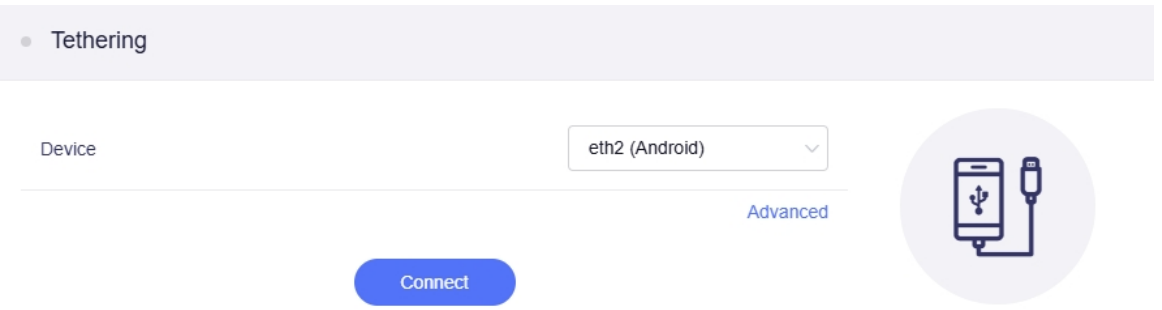
4.2.3 Internetverbindung über ein USB-Modem

Schließen Sie ein USB-Mobilfunkmodem an den USB-Anschluss des Routers an, um eine Internetverbindung herzustellen. So kann sich der Router über 4G/5G-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.

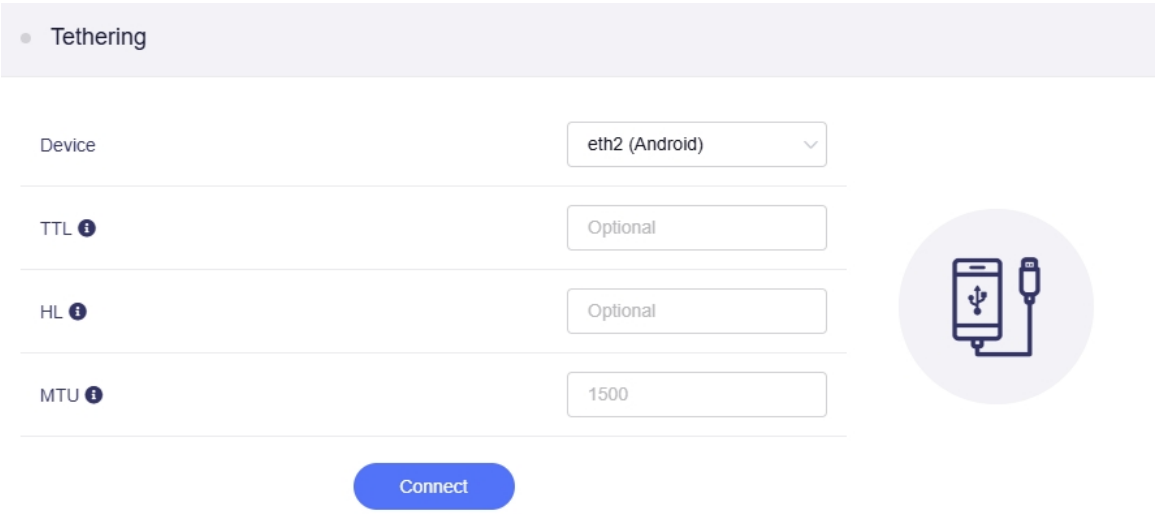


Gehen Sie wie folgt vor, um Ihren Router über ein USB-Modem mit dem Internet zu verbinden.

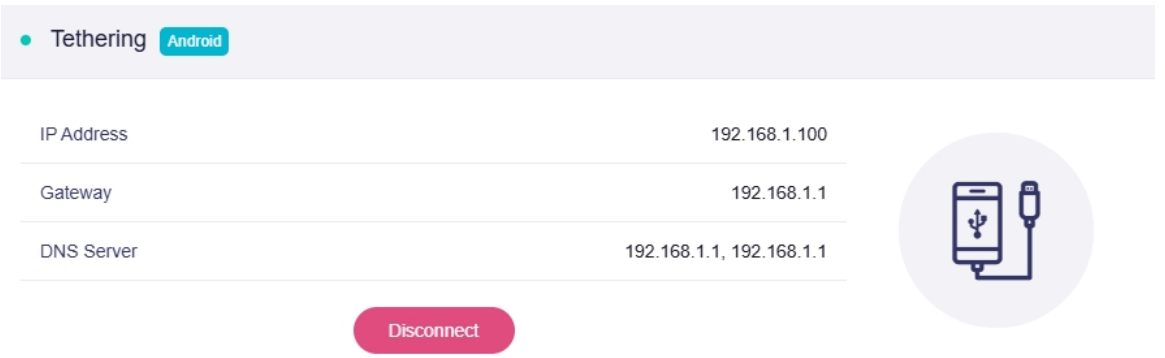
1. Stecken Sie vor dem Einschalten ein USB-Modem mit eingesetzter SIM-Karte in den USB-Anschluss des Routers.
2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie anschließend auf **Connect**.



Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU anpassen möchten, klicken Sie auf **Advanced** und nehmen Sie die gewünschten Änderungen vor. Klicken Sie anschließend auf **Connect**.

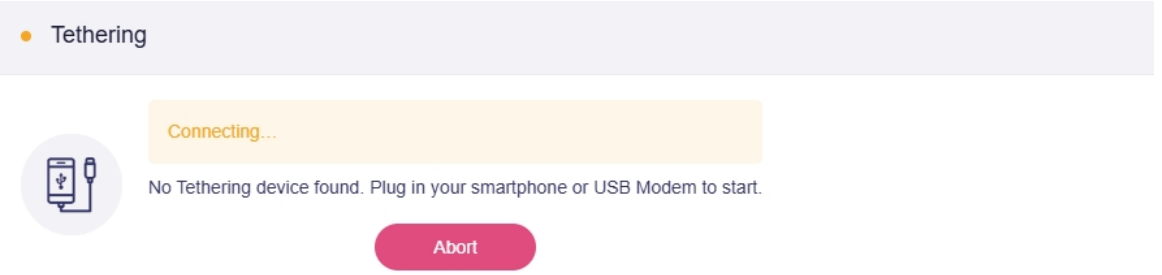


3. Die Verbindung wird hergestellt. Nach erfolgreicher Verbindung werden auf dieser Seite die Netzwerkdaten angezeigt.



Tipps:

1. 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.
2. Wenn Sie das USB-Modem abziehen, erscheint die unten gezeigte Meldung „No Tethering device found“. Die Tethering-Schnittstelle bleibt dabei im Status „Connecting“.


Tethering
Connecting...
No Tethering device found. Plug in your smartphone or USB Modem to start.
Abort

Kapitel 5

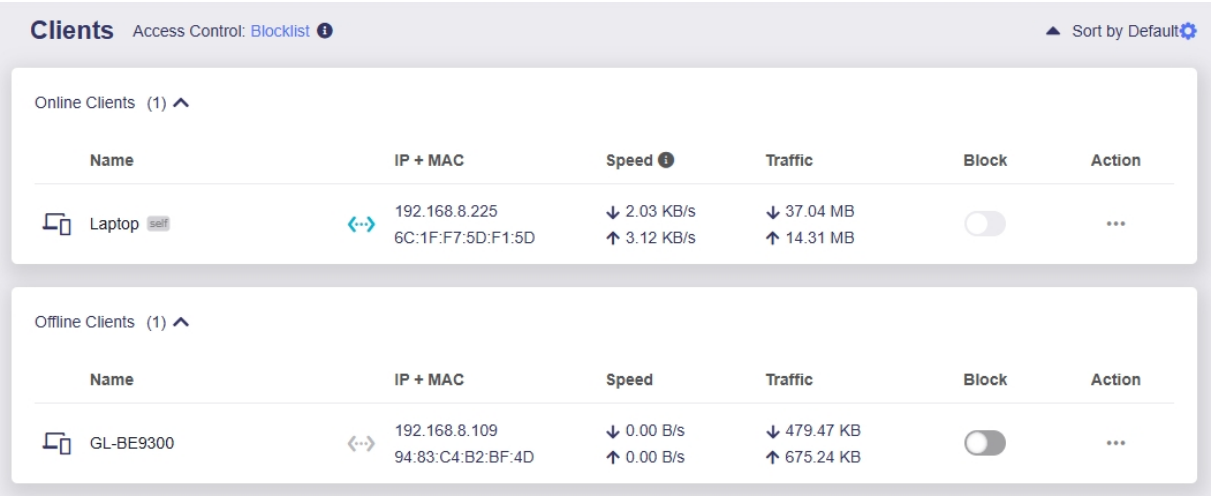
Verbundene Geräte

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.

5.1 Gerätedetails

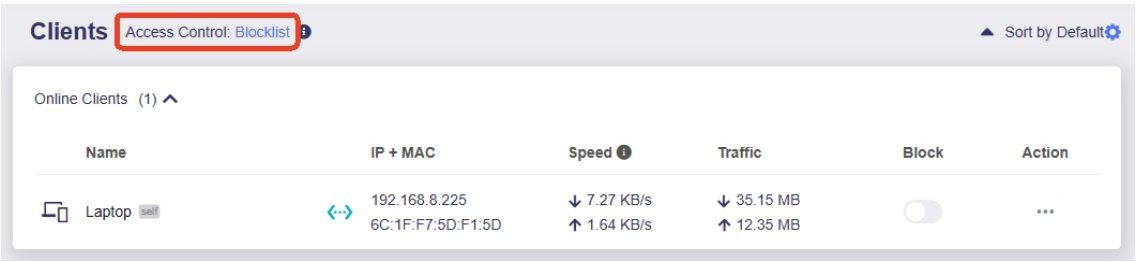


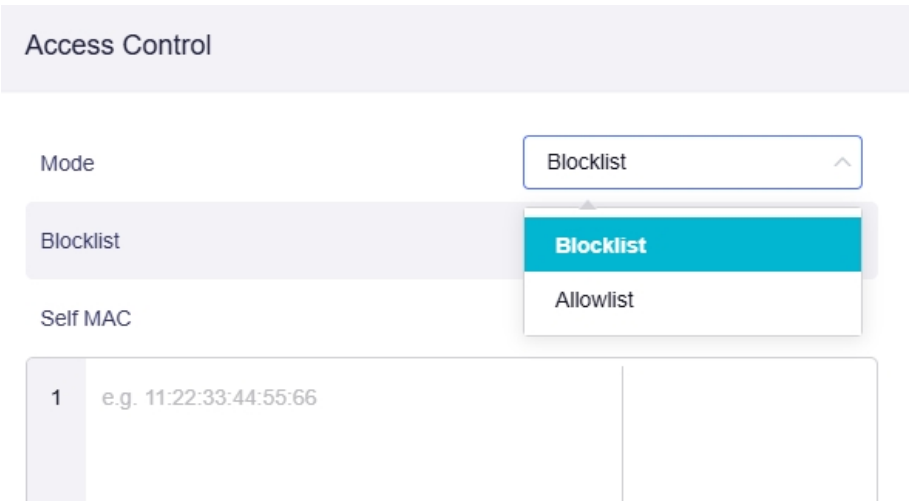
1. **Gerätename**
   Die erste Spalte zeigt den Namen und den Typ des Geräts an. Der Name richtet sich nach dem auf dem Gerät festgelegten Hostnamen. Das blaue Symbol neben dem Gerätenamen kennzeichnet die Verbindungsart und zeigt an, dass das Gerät über ein Ethernetkabel mit dem Router verbunden ist.
2. **IP- und MAC-Adresse**
   Die zweite Spalte enthält die IP- und MAC-Adresse des verbundenen Geräts.
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. **Sperren**

In der fünften Spalte können Sie ein bestimmtes verbundenes Gerät mit einem Klick sperren.

Die Zugriffskontrolle verwendet standardmäßig eine Sperrliste (Blocklist). Bei Bedarf können Sie oben auf eine Freigabeliste (Allowlist) wechseln.



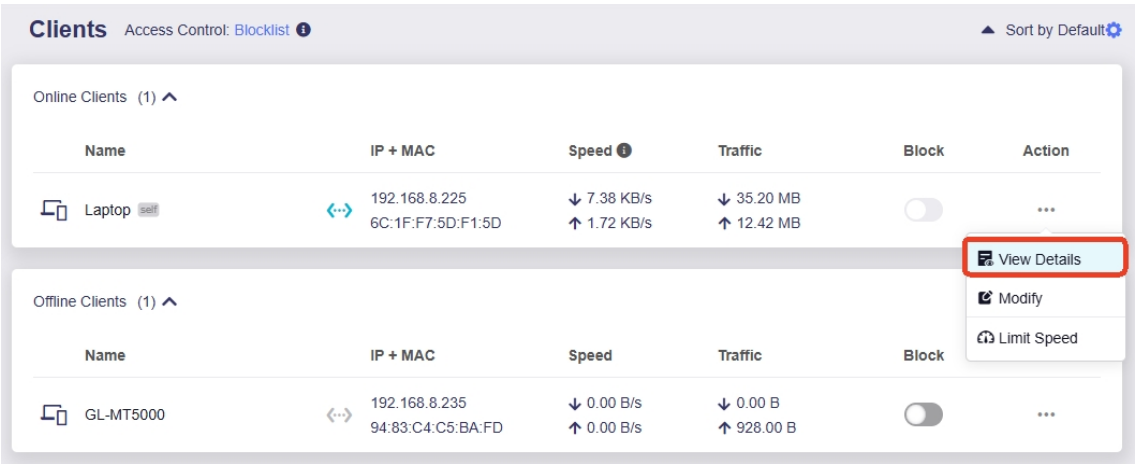


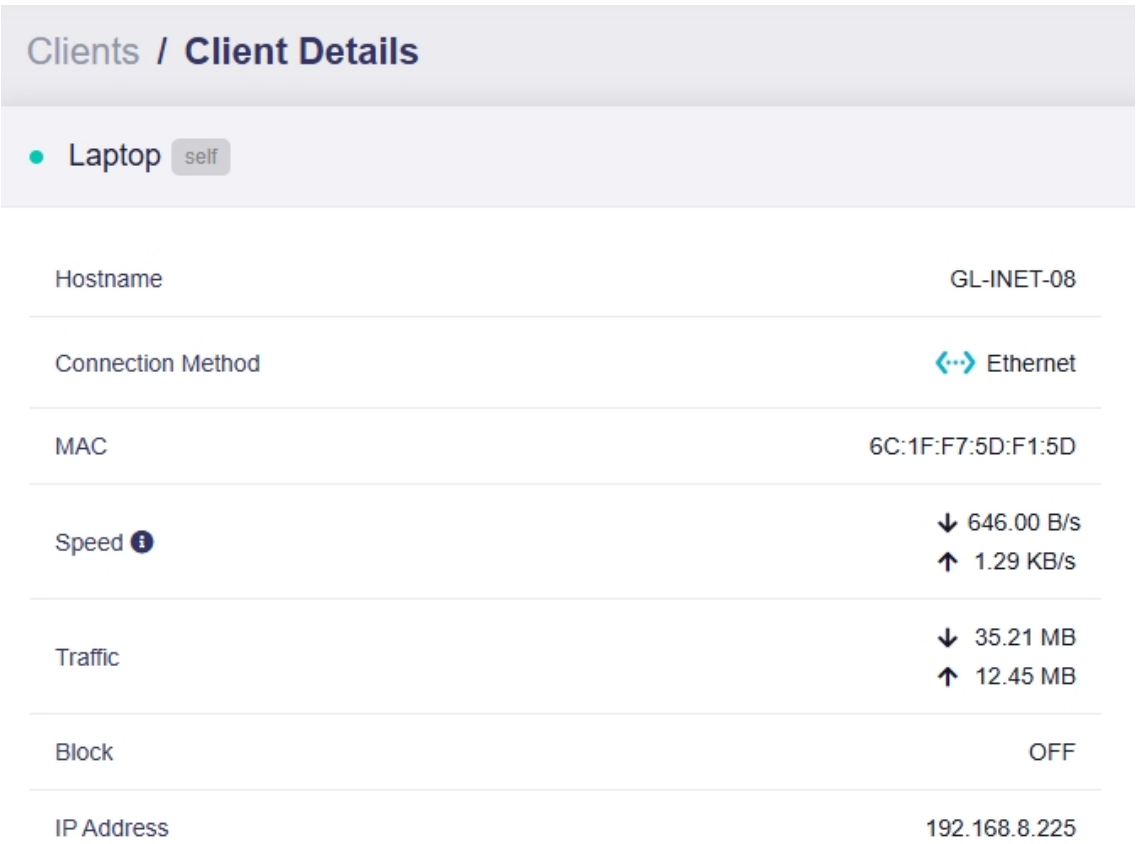
- **Blacklist**: Geräte, deren MAC-Adressen auf der Sperrliste stehen, dürfen sich nicht mit diesem Router verbinden. Die Sperre basiert auf der MAC-Adresse des Geräts. Verwendet ein gesperrtes Gerät beim nächsten Verbindungsversuch eine andere MAC-Adresse, kann es sich dennoch verbinden.
- **Allowlist**: Nur Geräte mit den festgelegten MAC-Adressen dürfen sich mit dem Router verbinden. Dies eignet sich für IoT-Geräte und die Verwaltung von Unternehmensnetzwerken.

5.2 Aktionen

1. **Details anzeigen**

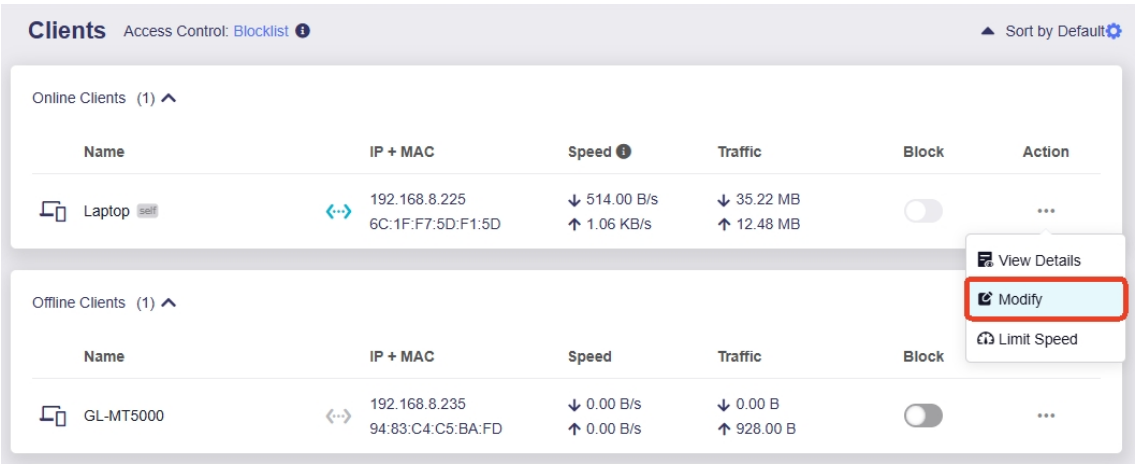
   Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Dropdown-Menü **View Details**, um die Gerätedetails auf einer eigenen Seite anzuzeigen.

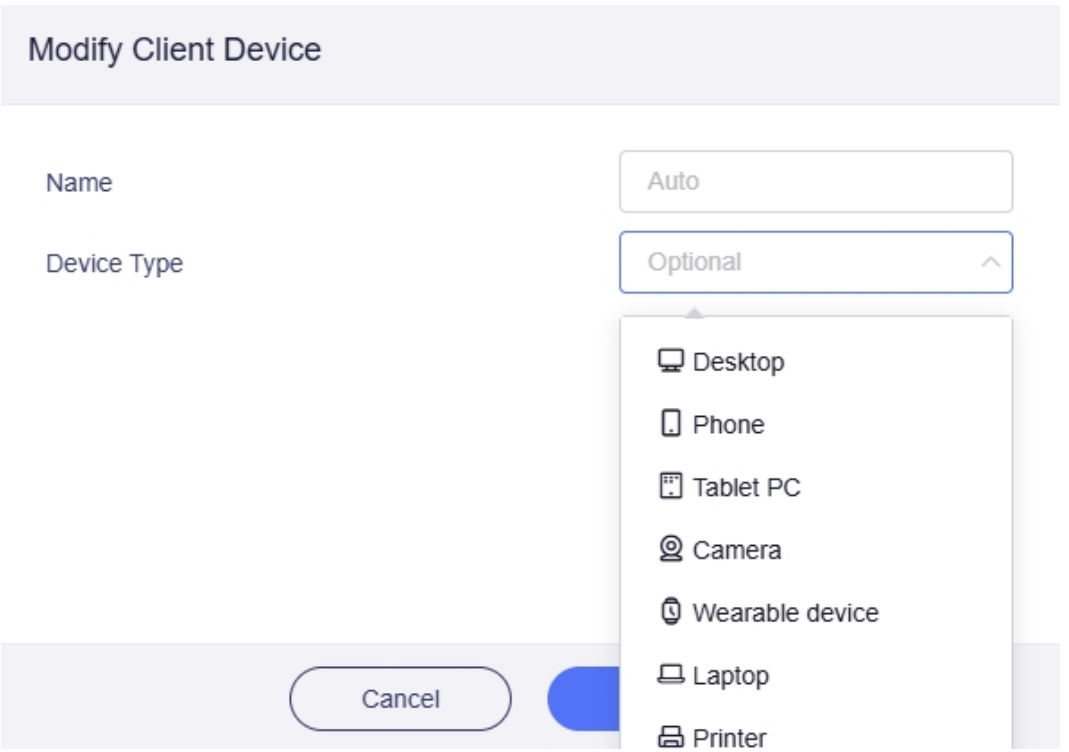




2. **Gerät bearbeiten**

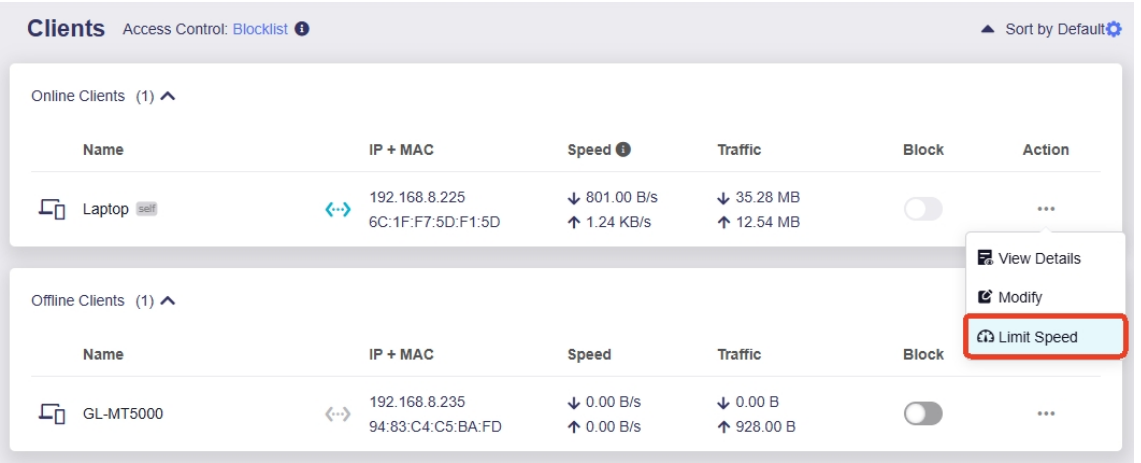
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Modify**, um den Gerätenamen und -typ zu ändern.



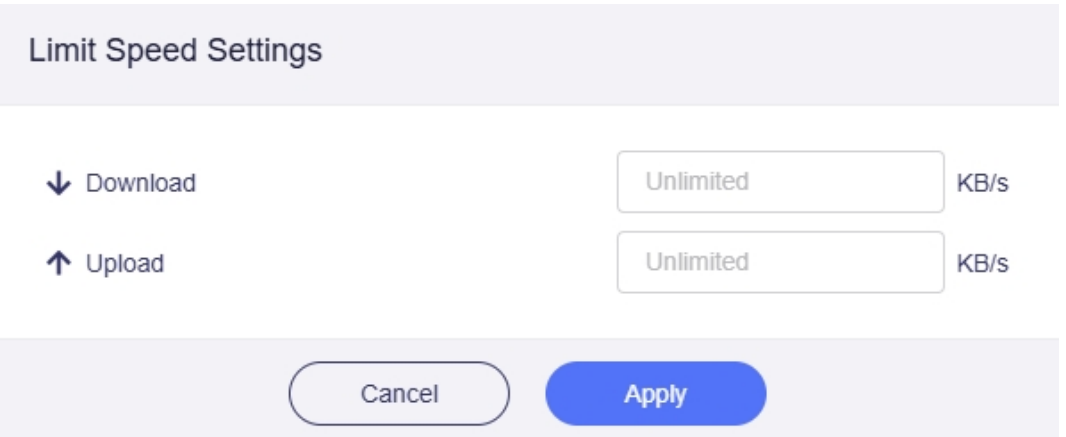


3. **Geschwindigkeit begrenzen**

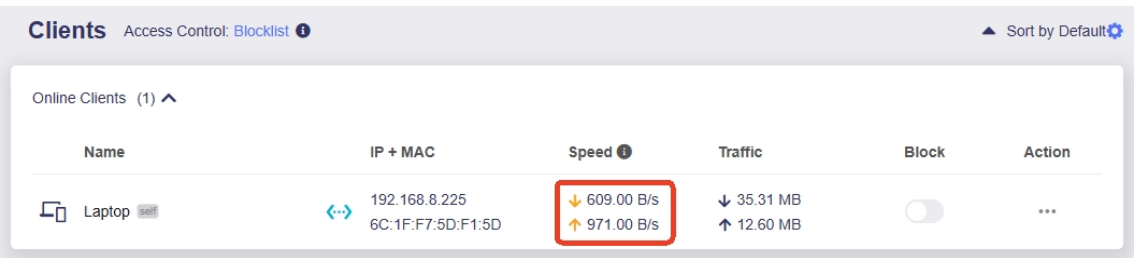
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Limit Speed**.



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



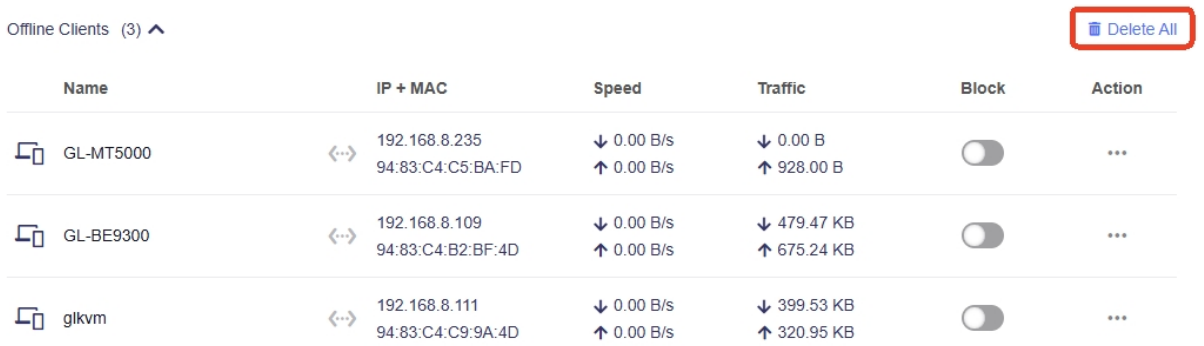
Bei Geräten mit aktivierter Geschwindigkeitsbegrenzung werden die Pfeile für die Upload- und Downloadgeschwindigkeit gelb angezeigt.



Tipp: Falls die Option Limit Speed fehlt, öffnen Sie **NETWORK** > **Network Acceleration** und deaktivieren Sie die Netzwerkbeschleunigung. Danach ist die Option Limit Speed verfügbar.

5.3 Geräte entfernen

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

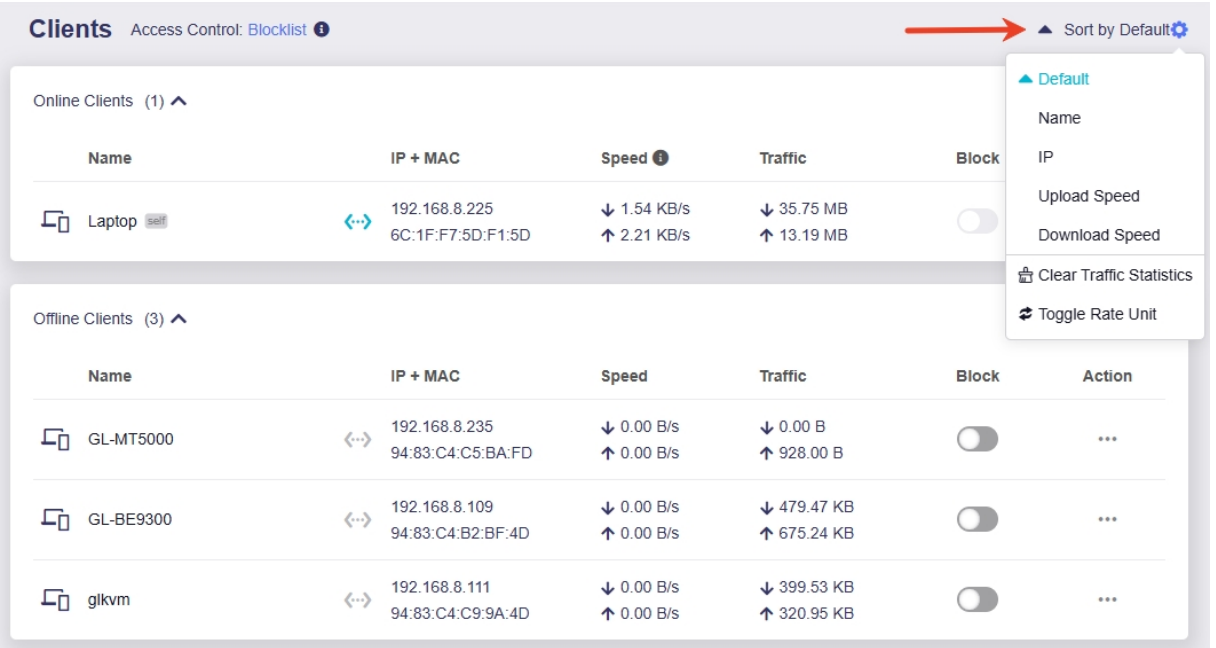


Um ein einzelnes Gerät zu entfernen, klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Remove Client**.



5.4 Sortierung

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



Standardmäßig gilt folgende Sortierung:

- 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.

Kapitel 6

Cloud-Dienste

Dieses Kapitel stellt die beiden Cloud-Dienste GoodCloud und AstroWarp vor.

6.1 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.

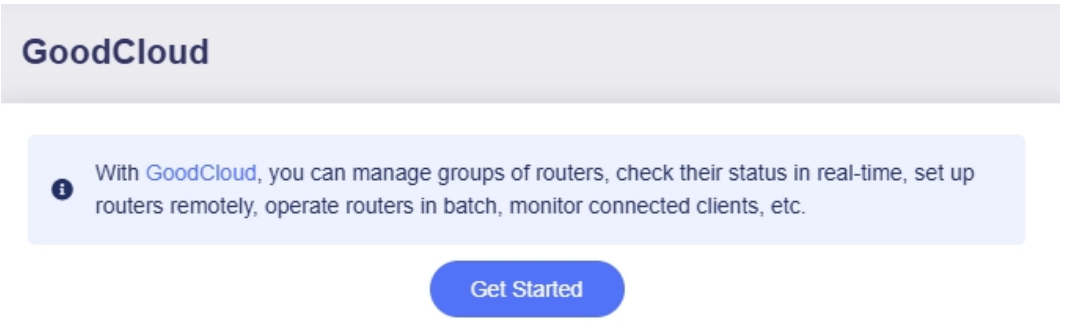
Mit GoodCloud können Sie:

- 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

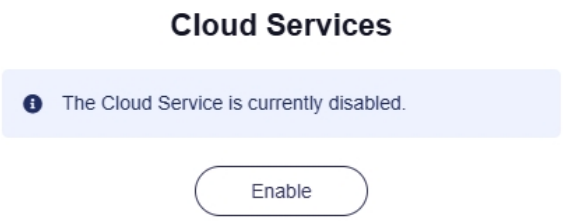
Einige Funktionen sind im Enterprise-Tarif und im VAR-Tarif (Value Added Reseller) verfügbar. Weitere Informationen finden Sie hier.

6.1.1 GoodCloud aktivieren

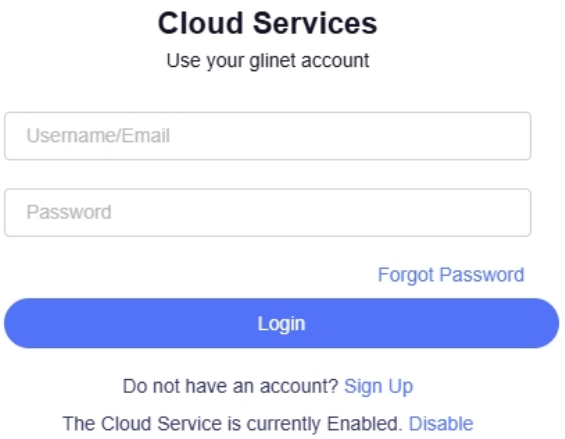
1. Melden Sie sich an der Weboberfläche Ihres Routers an, öffnen Sie **CLOUD SERVICE** > **GoodCloud** und klicken Sie auf **Get Started.**



2. Oben rechts öffnet sich ein Dropdown-Fenster. Klicken Sie auf **Enable**.



3. Melden Sie sich mit Ihrem GL.iNet-Cloud-Konto an. Falls Sie noch kein Konto haben, registrieren Sie sich und melden Sie sich anschließend an. Nach der Anmeldung wird der Router automatisch mit Ihrem Konto verknüpft.

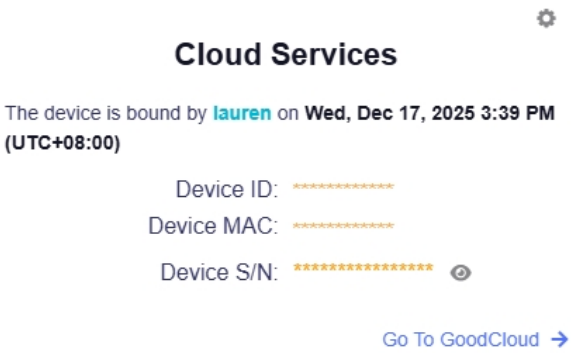


Tipps:

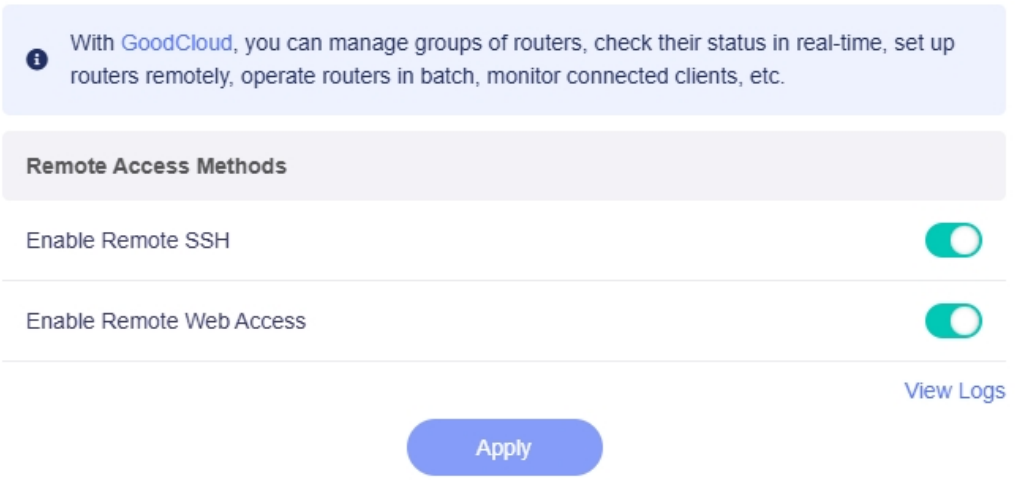
- Die Schritte zur Verknüpfung mit GoodCloud unterscheiden sich je nach Firmwareversion.

- 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.

4. Klicken Sie nach erfolgreicher Verknüpfung oben rechts in der Weboberfläche auf das **Cloud-Symbol**. Daraufhin werden die Details des verknüpften Geräts angezeigt: zugeordnetes Konto, Datum der Verknüpfung, Geräte-ID, Geräte-MAC-Adresse und Geräteseriennummer.



5. Öffnen Sie **CLOUD SERVICES** > **GoodCloud** und aktivieren Sie den Fernzugriff. GoodCloud ermöglicht den Fernzugriff auf die Weboberfläche und das Terminal des verknüpften Routers. Dies ist besonders für Fernverwaltung, Netzwerkkonfiguration und Fehlerbehebung hilfreich. Hier können Sie den Fernzugriff für Ihren Router ein- oder ausschalten.



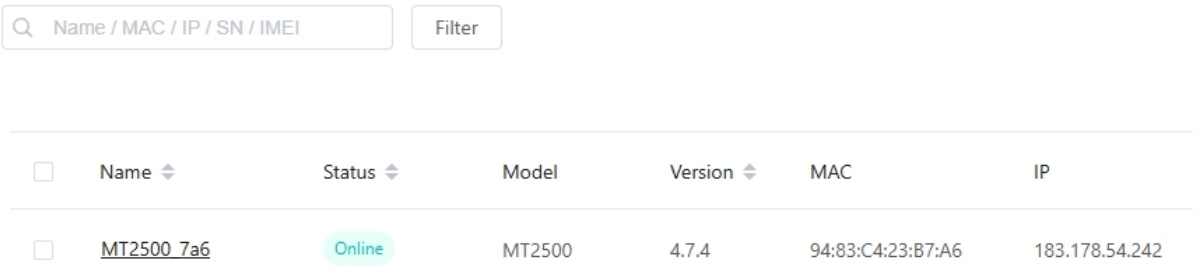
- **Remote SSH**: Fernzugriff auf das Terminal des Routers über GoodCloud per SSH.
- **Remote Web Access**: Fernzugriff auf die Weboberfläche des Routers über GoodCloud per HTTP/HTTPS.

- **View Logs**: Öffnet die Protokollseite und zeigt das Cloud-Protokoll an.

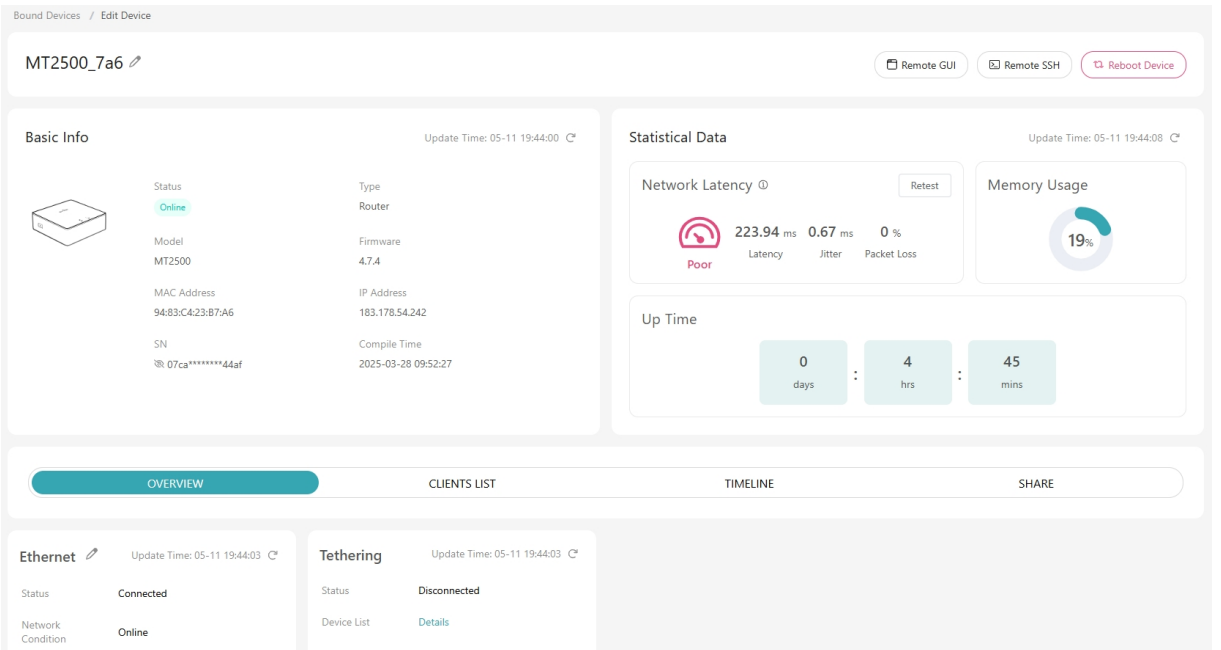
6.1.2 Router verwalten

Gerätedetails prüfen

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

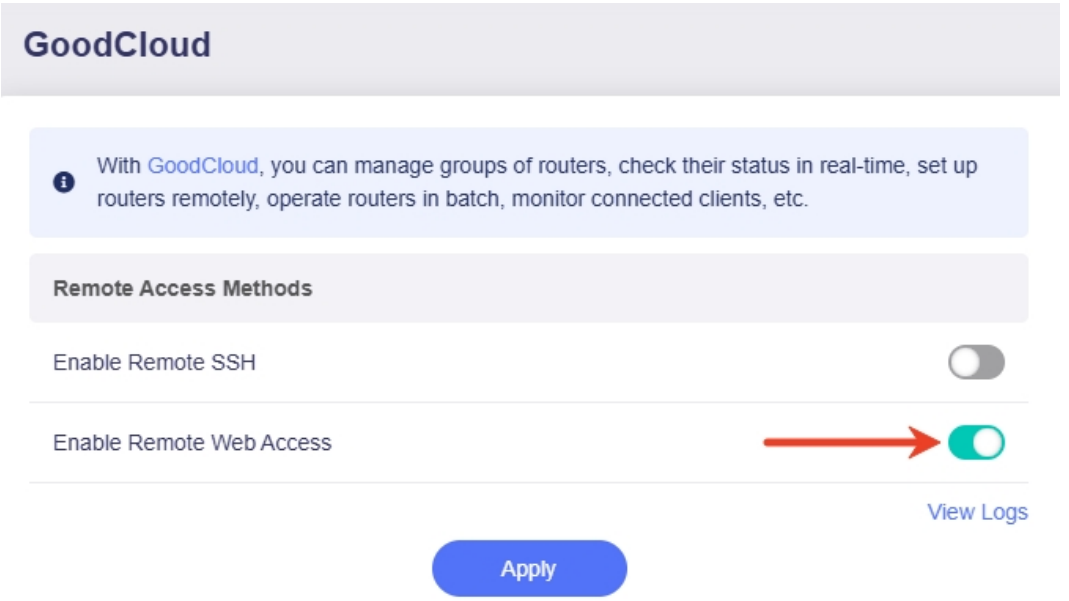


Klicken Sie auf den Gerätenamen, um die Detailseite zu öffnen. Diese enthält grundlegende Informationen, Statistiken, eine Netzwerkübersicht, die Geräteliste und eine Zeitleiste. Außerdem können Sie erweiterte Aktionen ausführen, etwa aus der Ferne auf den Router zugreifen oder ihn neu starten.

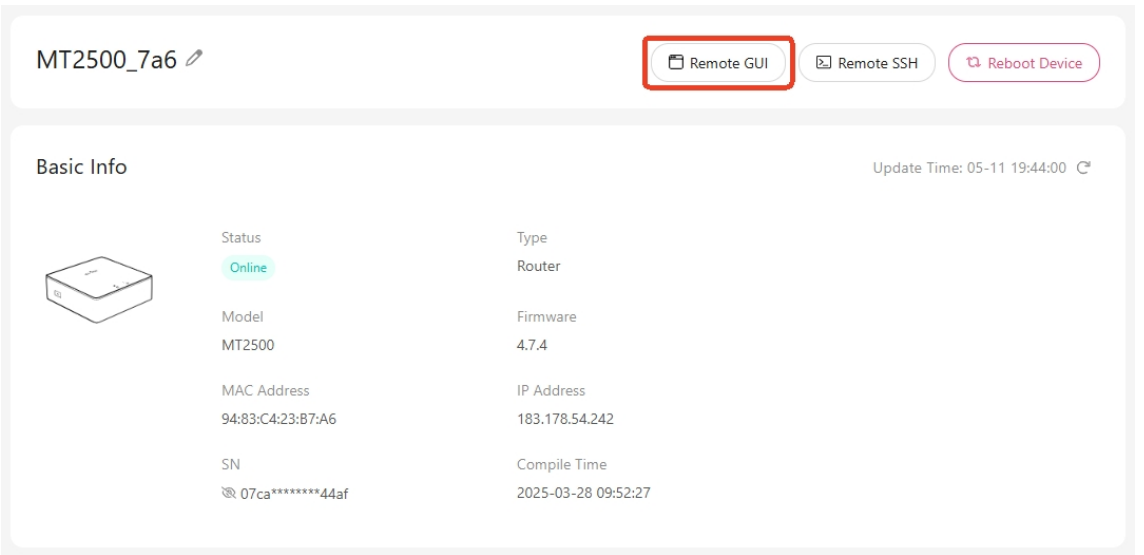


Fernzugriff auf die Weboberfläche

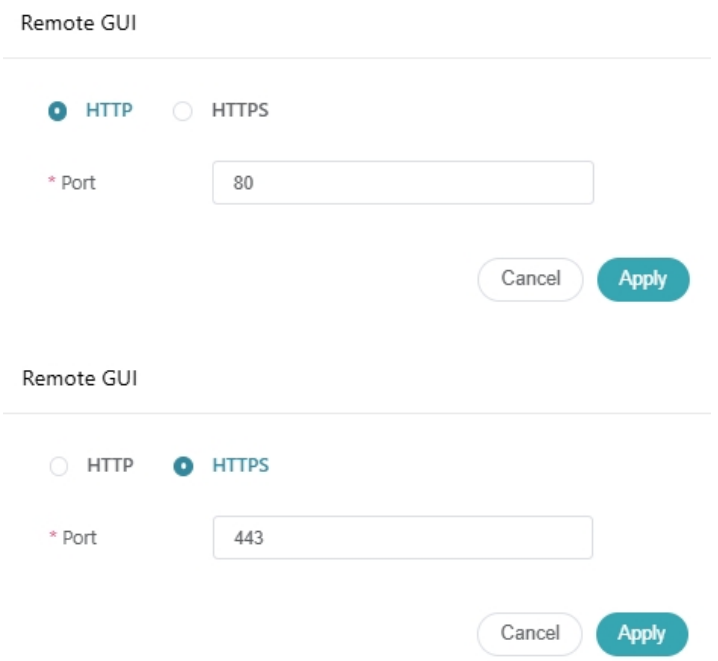
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote Web Access** und klicken Sie auf **Apply**.



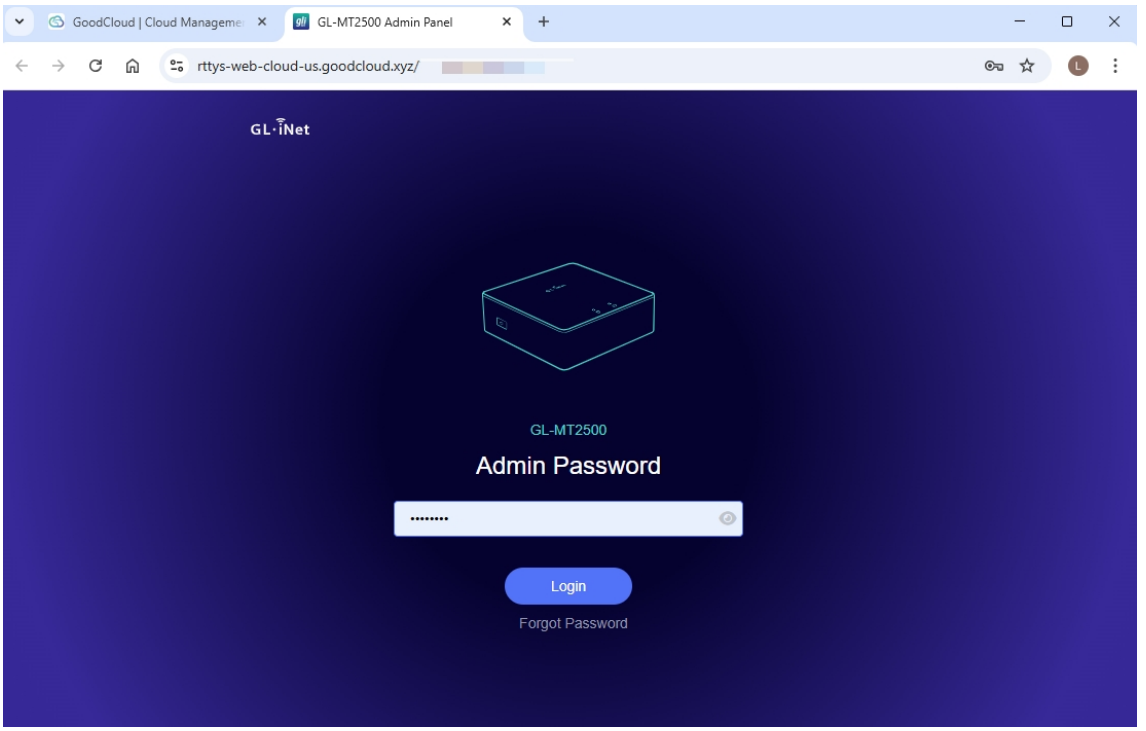
2. Melden Sie sich bei GoodCloud an und öffnen Sie **Device** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote GUI**.



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**.

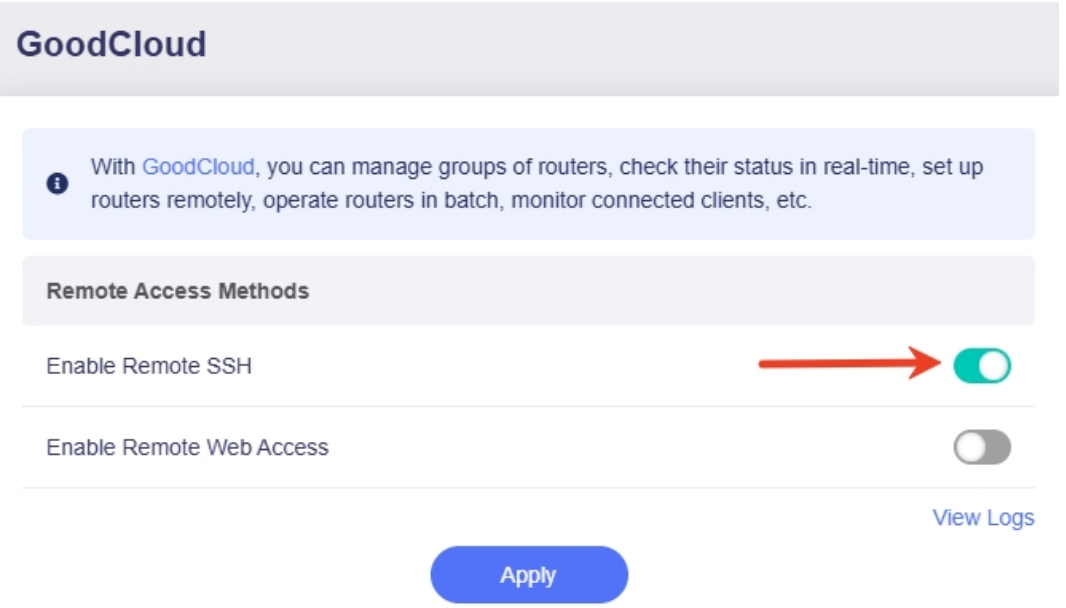


5. Sie werden zur Anmeldeseite des Routers weitergeleitet. Geben Sie das Administratorpasswort ein, um aus der Ferne auf die Weboberfläche zuzugreifen.

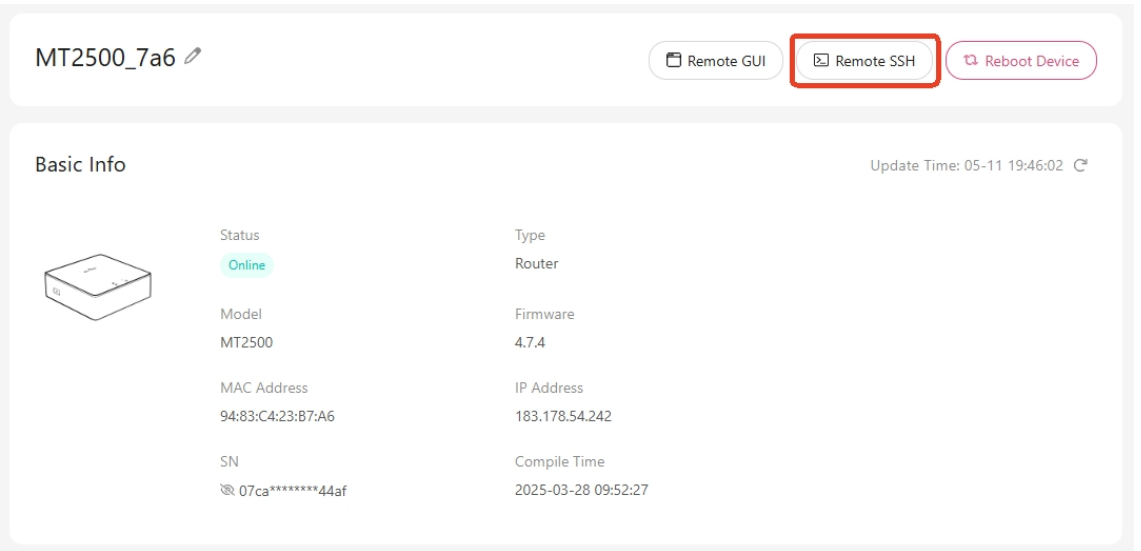


Fernzugriff auf das Terminal

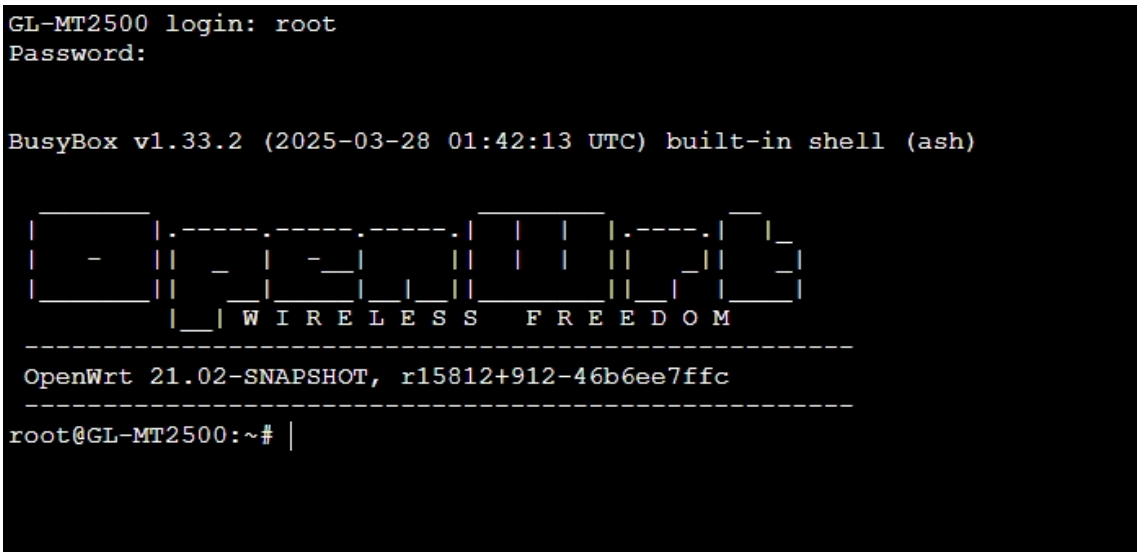
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote SSH** und klicken Sie auf **Apply**.



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

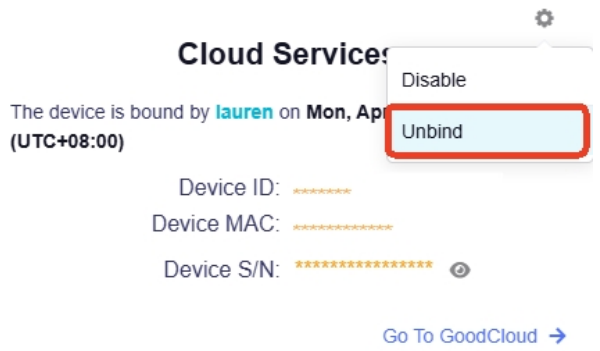


4. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

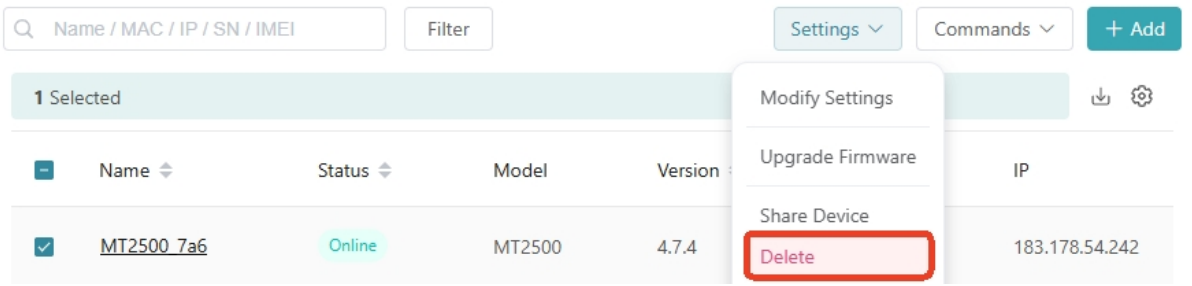

GL-MT2500 login: root
Password:
BusyBox v1.33.2 (2025-03-28 01:42:13 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT, r15812+912-46b6ee7ffc
root@GL-MT2500:~#

6.1.3 Geräteverknüpfung aufheben

Klicken Sie in der Weboberfläche des Routers oben rechts auf das Cloud-Symbol. Klicken Sie im Dropdown-Menü auf das Zahnradsymbol und wählen Sie **Unbind**. Die Verknüpfung Ihres Geräts mit Ihrem GoodCloud-Konto wird daraufhin aufgehoben.

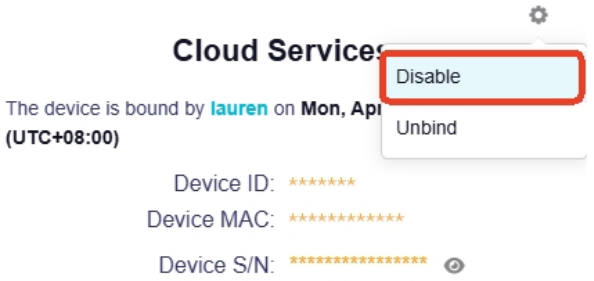


Alternativ können Sie sich an der Cloud-Plattform anmelden und **Device** > **Bound Devices** öffnen. Wählen Sie das Gerät aus, dessen Verknüpfung Sie aufheben möchten. Klicken Sie oben rechts auf **Settings** und wählen Sie **Delete**. Die Verknüpfung Ihres Geräts mit Ihrem GoodCloud-Konto wird daraufhin aufgehoben.



6.1.4 GoodCloud deaktivieren

Wenn Sie das Gerät nicht mehr mit der Cloud verbinden möchten, klicken Sie oben rechts auf das Cloud-Symbol. Klicken Sie im Dropdown-Menü auf das Zahnradsymbol und wählen Sie **Disable**. Der Cloud-Dienst wird daraufhin deaktiviert.



6.2 AstroWarp

AstroWarp ist eine leistungsfähige Netzwerkplattform für den nahtlosen Fernzugriff auf Netzwerke und die Fernverwaltung von Geräten.

Die Plattform wurde speziell für die Integration mit GL.iNet-Routern entwickelt und unterstützt die umfassende Verwaltung von Geräten im gesamten Netzwerk, einschließlich über- und untergeordneter Geräte.

Mit seinem Schwerpunkt auf netzwerkweiter Verwaltung und der künftig vorgesehenen Steuerung auf Hardwareebene bietet AstroWarp eine robuste, zuverlässige Lösung zur Geräteverwaltung und zum Betrieb sicherer, stabiler Netzwerke.

Weitere Informationen finden Sie unter astrowarp.net.

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

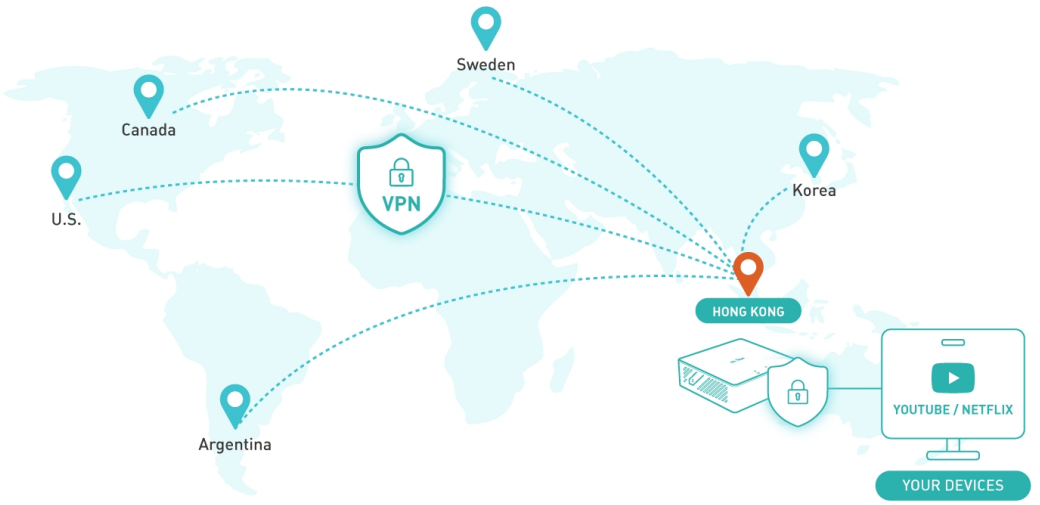
1. **Schutz persönlicher Daten**

   Der VPN-Dienst dieses Routers unterstützt zahlreiche kabelgebundene Geräte, darunter Desktopcomputer, Laptops, Spielekonsolen, Smart-TVs und Streaminggeräte. Sämtliche über Kabelverbindungen übertragenen Daten werden durch das VPN geschützt. Mit individuellen VPN-Richtlinien können Sie den Schutz auch gezielt für bestimmte Geräte festlegen.



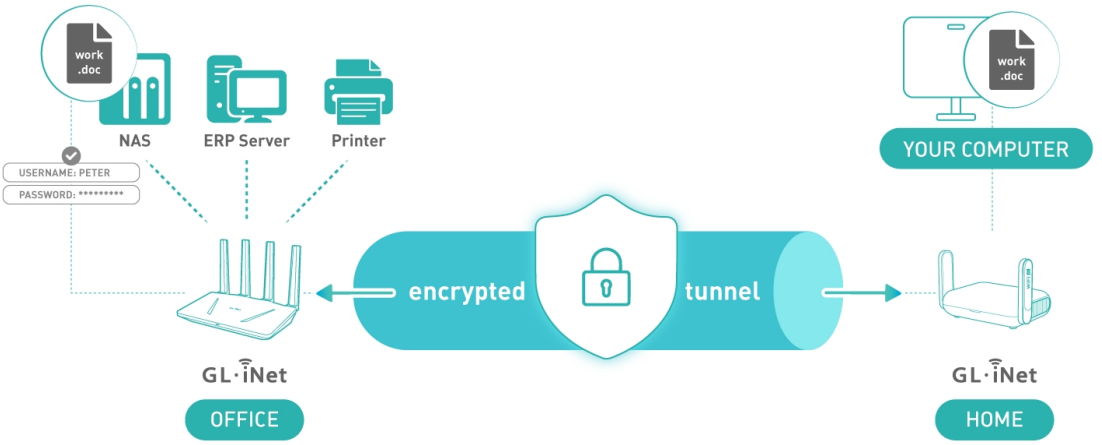
2. **Weltweiter Zugriff ohne Einschränkungen**

   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

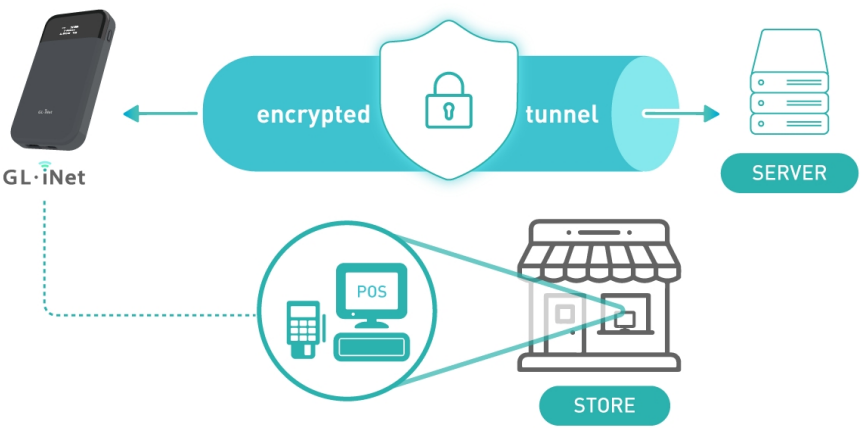
3. **Datensicherheit für kleine Unternehmen**

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

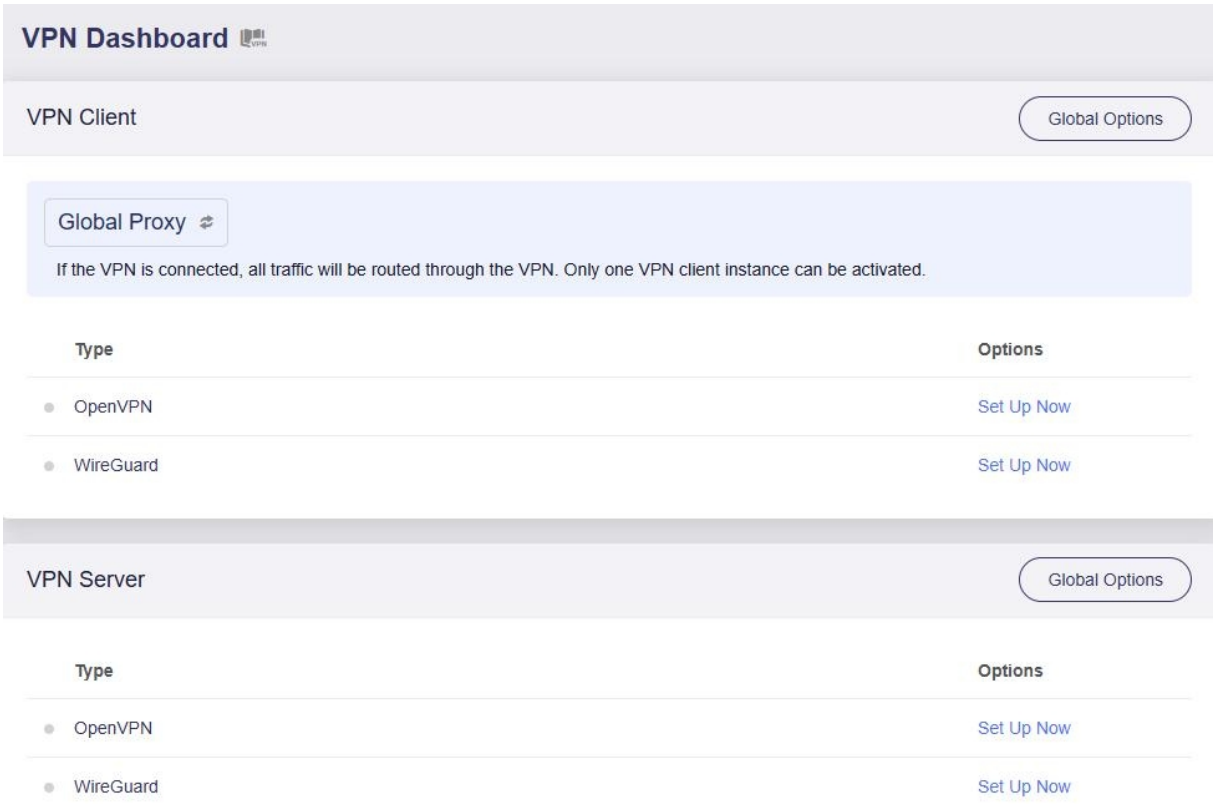
VPN-Dashboard

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

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

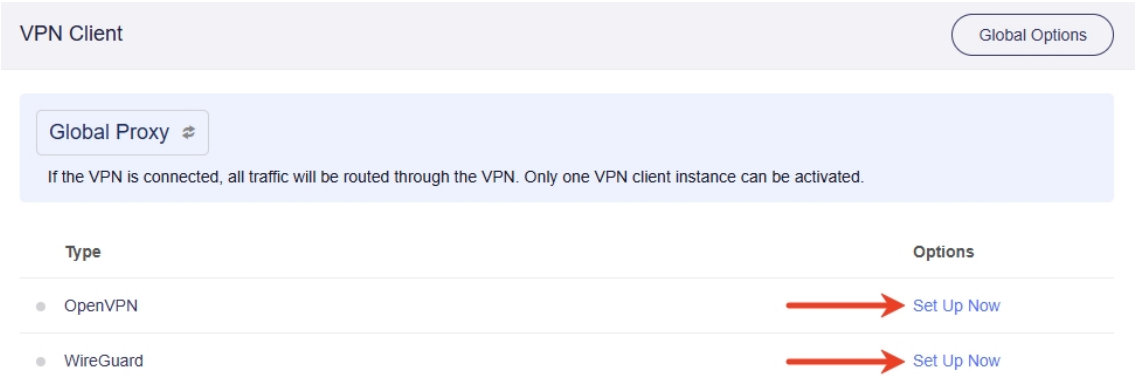
Das VPN-Dashboard zeigt Details zur VPN-Verbindung an, darunter Serveradresse, Datenverkehrsstatistik, virtuelle Client-IP und Verbindungsprotokoll. Außerdem lassen sich hier erweiterte Einstellungen wie VPN-Kill-Switch, VPN-Richtlinien, IP-Masquerading, MTU und VPN-Kaskadierung konfigurieren.

Diese Seite ist in zwei Bereiche unterteilt: **VPN Client** und **VPN Server**.

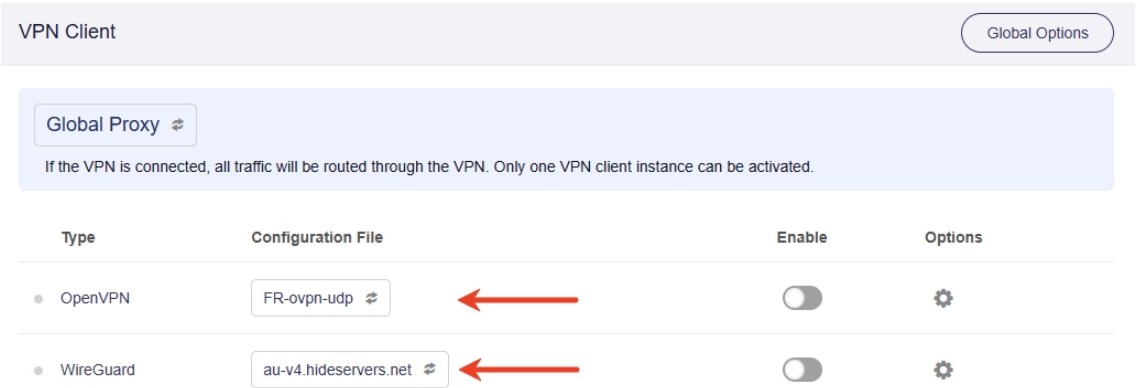


8.1 VPN-Client

Wenn Sie diese Seite zum ersten Mal öffnen und noch keine Konfigurationsdatei für OpenVPN oder WireGuard vorhanden ist, sieht sie wie folgt aus. Klicken Sie auf **Set Up Now**. Sie gelangen zur Seite OpenVPN Client bzw. WireGuard Client, auf der Sie Ihre VPN-Konfigurationsdatei hochladen können.



Nach dem Hochladen erscheint Ihre Konfiguration in der Spalte Configuration File. Wenn Sie mehrere Konfigurationsdateien hochgeladen haben, können Sie durch Anklicken des Felds zwischen ihnen wechseln.

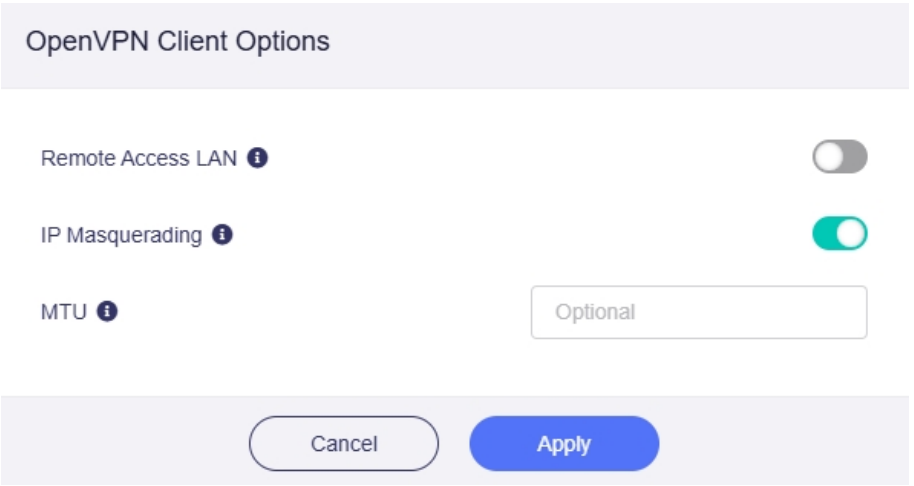


8.1.1 Client-Optionen

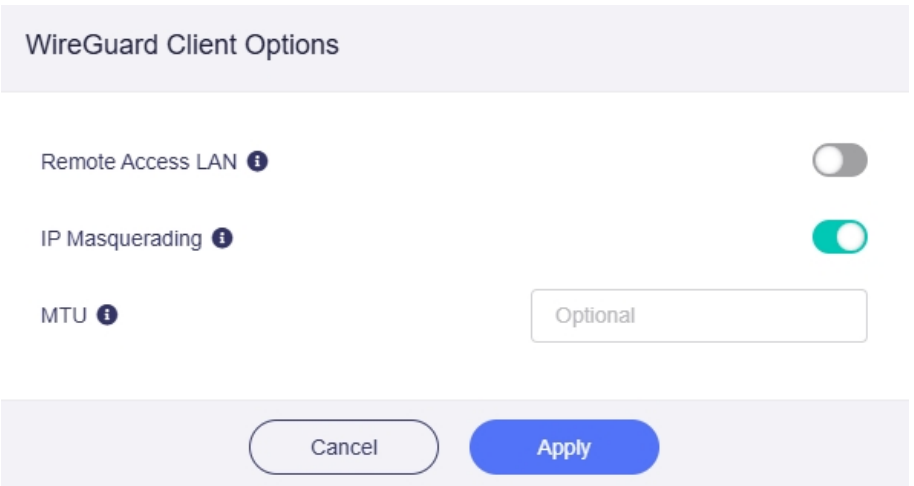
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Clients zu öffnen.



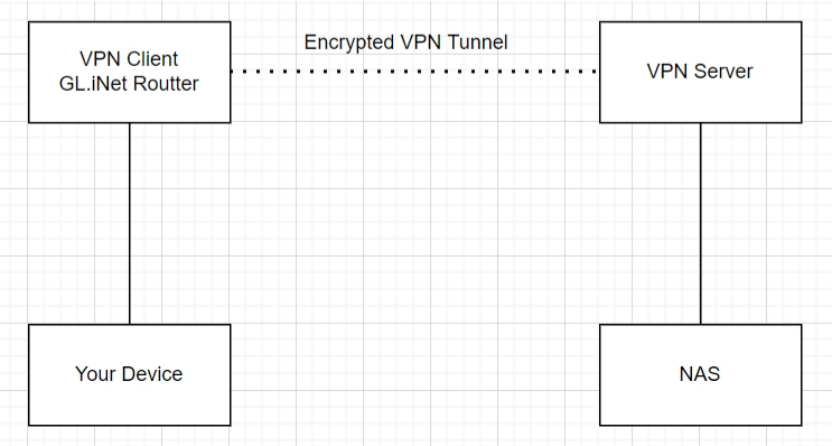
Die Optionen des OpenVPN-Clients werden wie folgt angezeigt.



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.

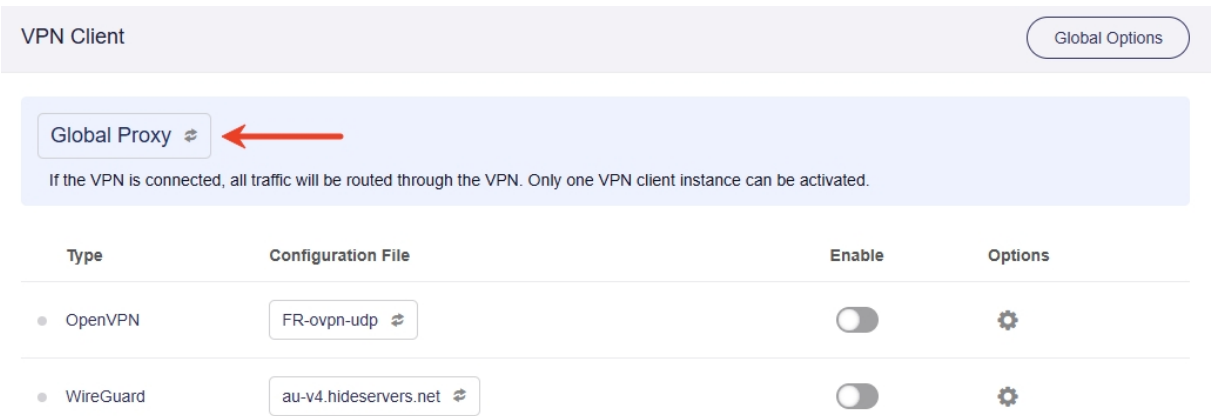


Im obigen Diagramm arbeitet der GL.iNet-Router beispielsweise als VPN-Client und verbindet sich über den VPN-Tunnel mit einem VPN-Server. Bei aktivierter Option können Geräte auf der VPN-Serverseite, z. B. ein NAS, sowohl auf den GL.iNet-Router als auch auf dessen LAN-Geräte zugreifen. Dazu müssen Sie 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 Proxy-Modus

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.

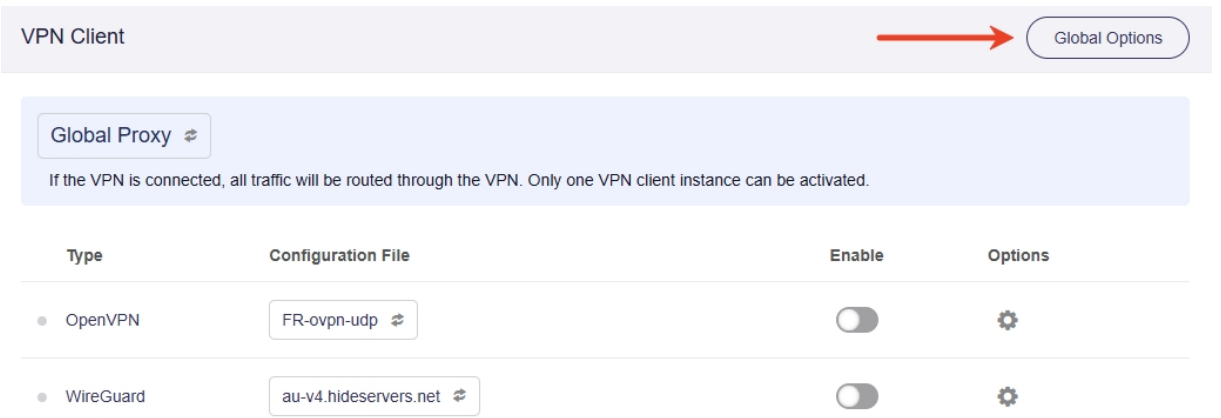
   - **Based on the Target Domain or IP**: In diesem Modus wird nur der Datenverkehr bestimmter Websites über das VPN geleitet, die anhand ihrer IP-Adresse oder ihres Domainnamens ausgewählt werden. Es kann nur eine VPN-Clientinstanz aktiviert werden.
   - **Based on the Client Device**: In diesem Modus wird nur der Datenverkehr bestimmter LAN-Geräte über das VPN geleitet, die anhand ihrer MAC-Adresse ausgewählt werden. Es kann nur eine VPN-Clientinstanz aktiviert werden.
   - **Based on the VLAN**: In diesem Modus wird nur der Datenverkehr eines bestimmten VLANs über das VPN geleitet. Es kann nur eine VPN-Clientinstanz aktiviert werden.

3. **Routenmodus**

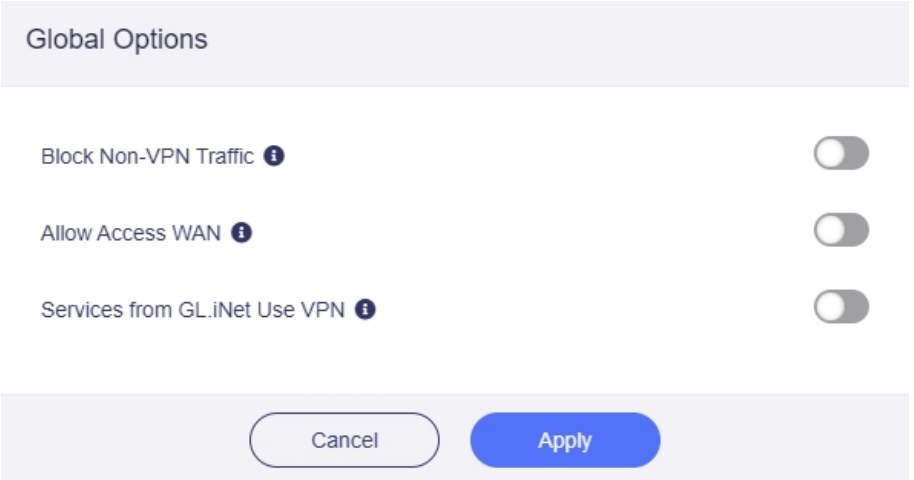
   - **Auto Detect**: Verwendet die Routingregeln, die in der Konfigurationsdatei des jeweiligen VPN-Clients festgelegt oder vom VPN-Server bereitgestellt werden.
   - **Customize Routing Rules**: Sie können die Routingregeln für jede VPN-Clientinstanz manuell konfigurieren.

8.1.3 Globale Optionen

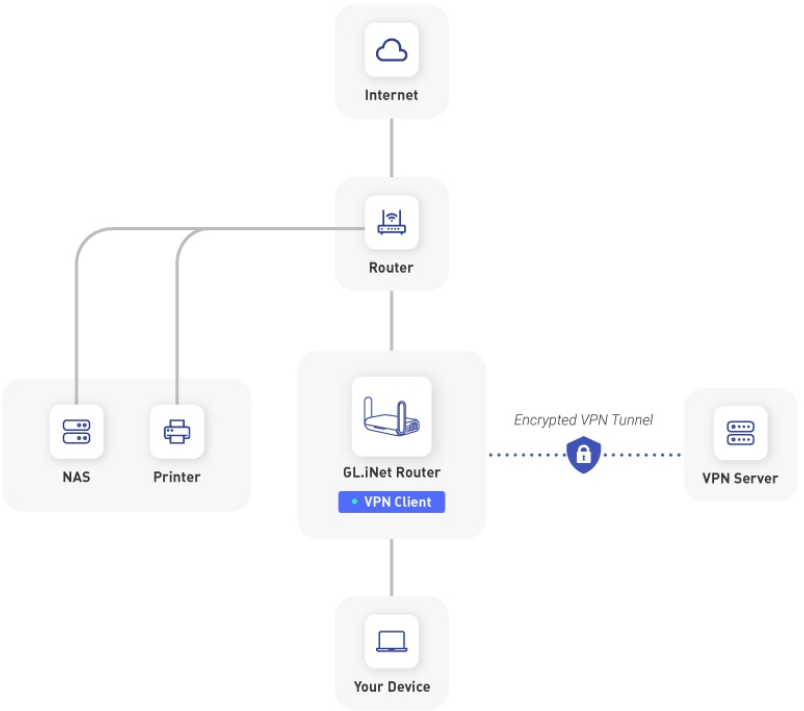
Klicken Sie oben rechts auf **Global Options**, um die Einstellungen Ihres VPN-Clients zu konfigurieren.



Das folgende Fenster wird eingeblendet.



- **Block Non-VPN Traffic**: Auch als **VPN-Kill-Switch** bezeichnet. Bei aktivierter Option wird sämtlicher Internetverkehr ausschließlich durch den VPN-Tunnel geleitet. Andere Schnittstellen, etwa der lokale WAN-Zugang des Internetanbieters, können dafür nicht verwendet werden. Wird die VPN-Verbindung unerwartet getrennt, wird der gesamte Internetverkehr gesperrt, damit er nicht auf die reguläre WAN-Verbindung ausweicht. So werden VPN-Lecks durch VPN-Ausfälle, fehlerhafte DNS-Einstellungen der Clients und ähnliche Probleme verhindert.
- **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.

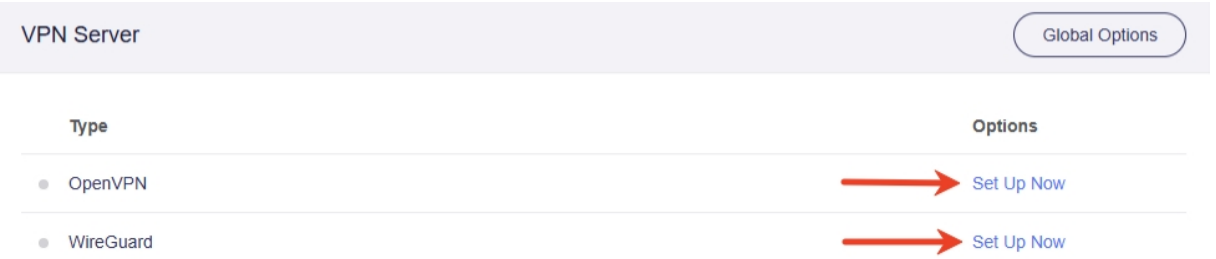


Wie im obigen Diagramm dargestellt, können Ihre lokalen Geräte nach Aktivierung dieser Funktion auf Geräte im vorgeschalteten Subnetz zugreifen, etwa Drucker und NAS. Diese Option dient hauptsächlich dem Zugriff auf Geräte im vorgeschalteten Subnetz. Der Router kann den Datenverkehr zu diesem Subnetz 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.

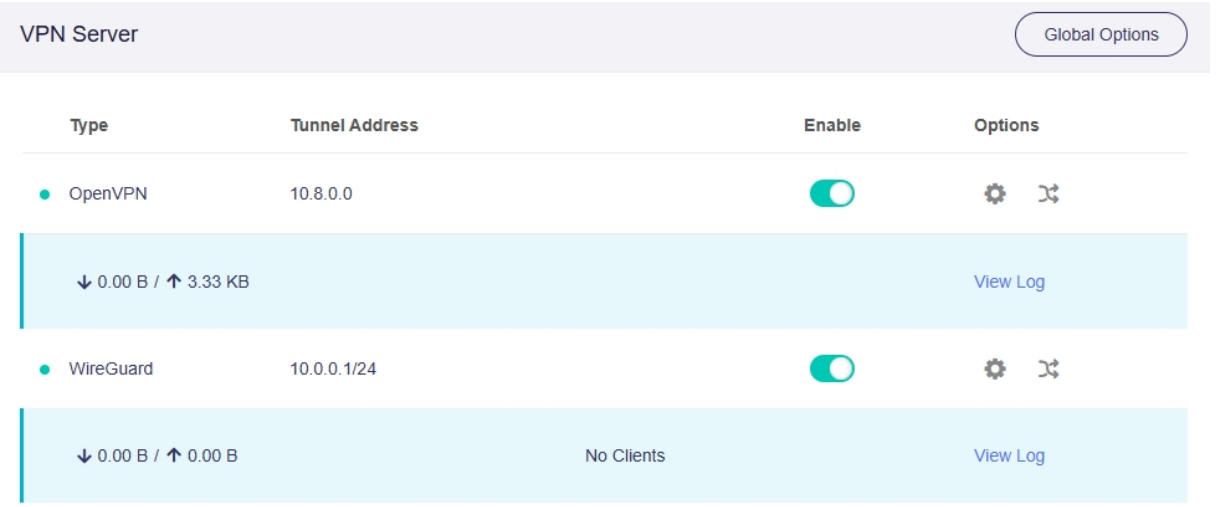
- **Services From GL.iNet Use VPN**: Leitet die Datenpakete von GoodCloud, DDNS und rtty durch die VPN-Tunnel. Diese Option ist standardmäßig deaktiviert, da diese Dienste für den ordnungsgemäßen Betrieb normalerweise die tatsächliche IP-Adresse des Geräts benötigen.

8.2 VPN-Server

Wenn der Router noch nie als OpenVPN- oder WireGuard-Server eingerichtet wurde, sieht die Seite wie folgt aus. Klicken Sie auf **Set Up Now**. Sie gelangen zur Seite OpenVPN Server bzw. WireGuard Server, um Ihren VPN-Server einzurichten.

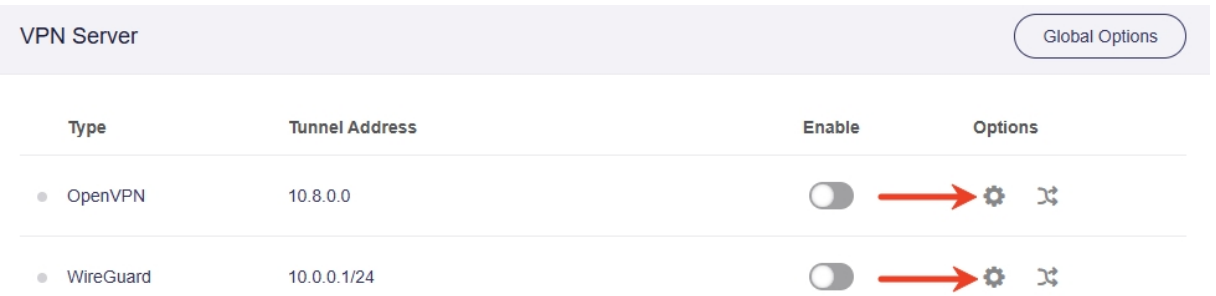


Nach dem Aktivieren des OpenVPN- oder WireGuard-Servers wird dessen Status wie folgt angezeigt.

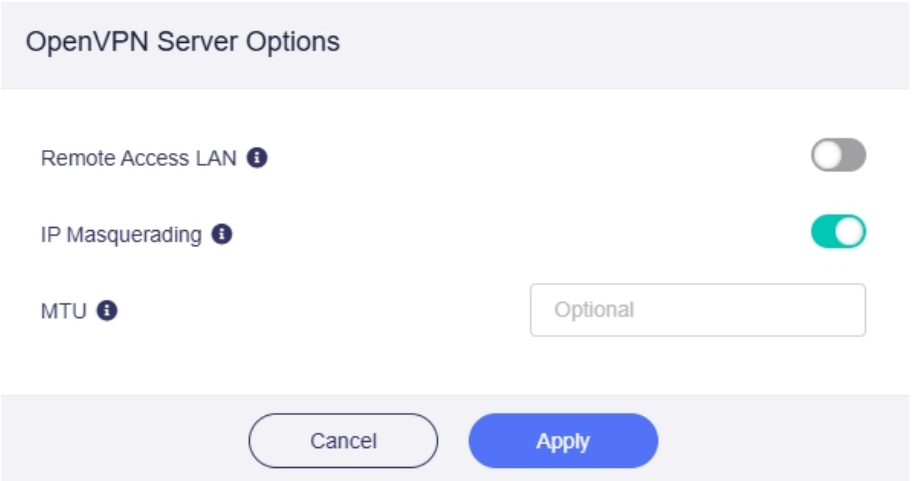


8.2.1 Server-Optionen

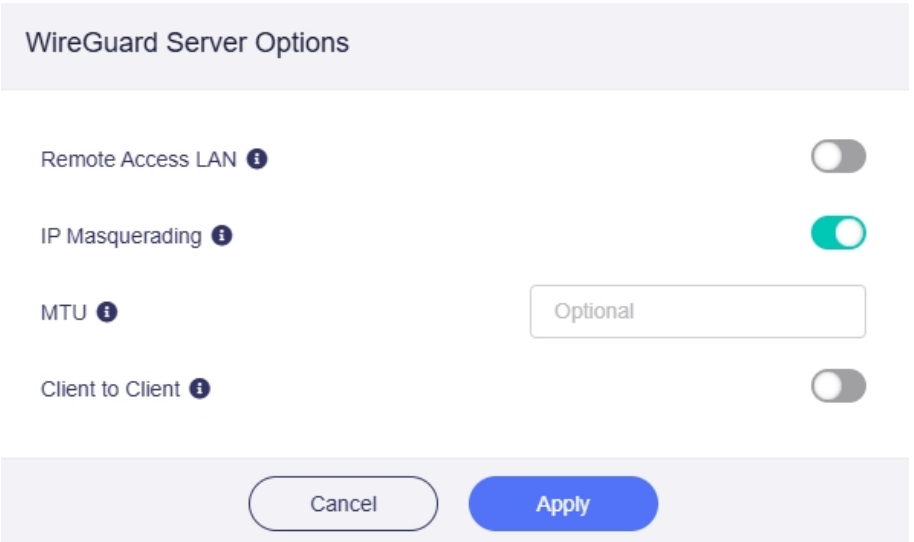
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Servers zu öffnen.



Die Optionen des OpenVPN-Servers werden wie folgt angezeigt.



Die Optionen des WireGuard-Servers werden wie folgt angezeigt.

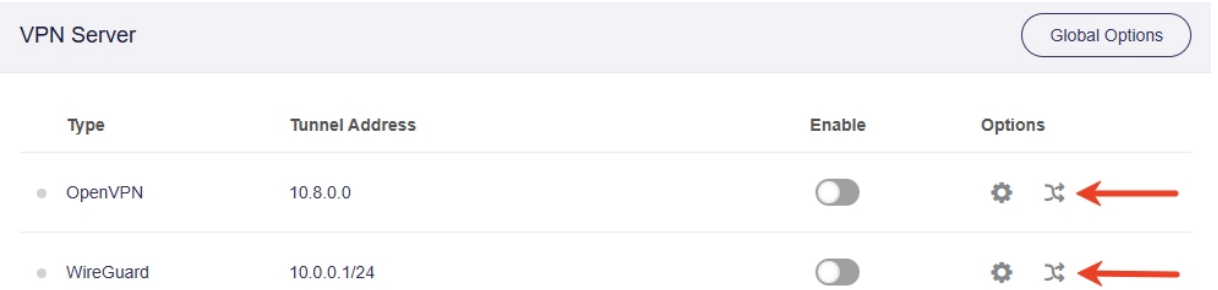


- **Remote Access LAN**: Erlaubt den Zugriff über den VPN-Tunnel auf Ressourcen im LAN-Subnetz des Servers.
- **IP Masquerading**: Ersetzt die Quell-IP-Adressen der LAN-Geräte durch die VPN-Tunnel-IP-Adresse des Routers. Deaktivieren Sie diese Option nur bei Standortvernetzungen, bei denen die Gegenstelle 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**: Bei aktivierter Option können die mit diesem Server verbundenen VPN-Clients über ihre VPN-Tunnel-IP-Adressen aufeinander zugreifen. Sollen die Clients

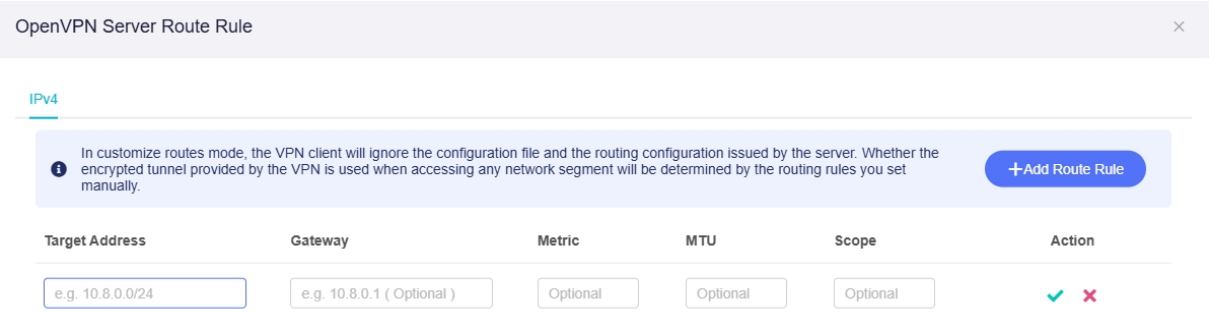
auch auf die LAN-Subnetze der anderen Clients zugreifen können, muss der VPN-Server die entsprechenden Routen zu diesen entfernten LAN-Subnetzen bekannt geben.

8.2.2 Server-Routingregeln

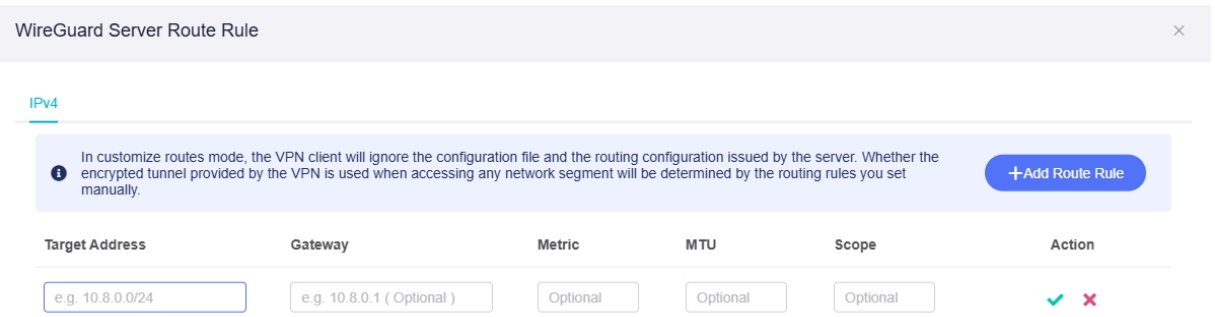
Klicken Sie rechts auf das Routensymbol, um die Routingregeln für OpenVPN oder WireGuard nach Bedarf anzupassen.



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.

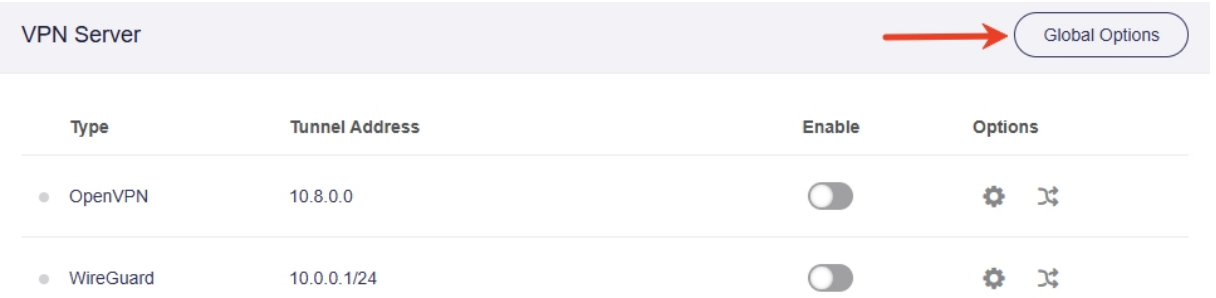


Die WireGuard-Server-Routingregeln werden wie folgt angezeigt. Klicken Sie auf **Add Route Rule**, geben Sie **Target Address** und **Gateway** ein und klicken Sie zum Übernehmen auf das grüne Häkchen.

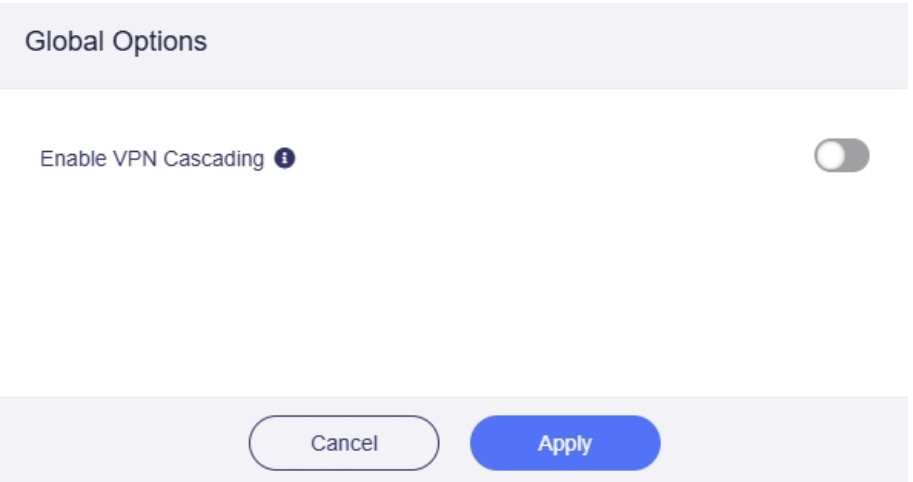


8.2.3 Globale Optionen

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



Das folgende Fenster wird eingeblendet.



- **VPN Cascading**: Wenn diese Option 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 verwendet. Weitere Informationen finden Sie hier.

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:

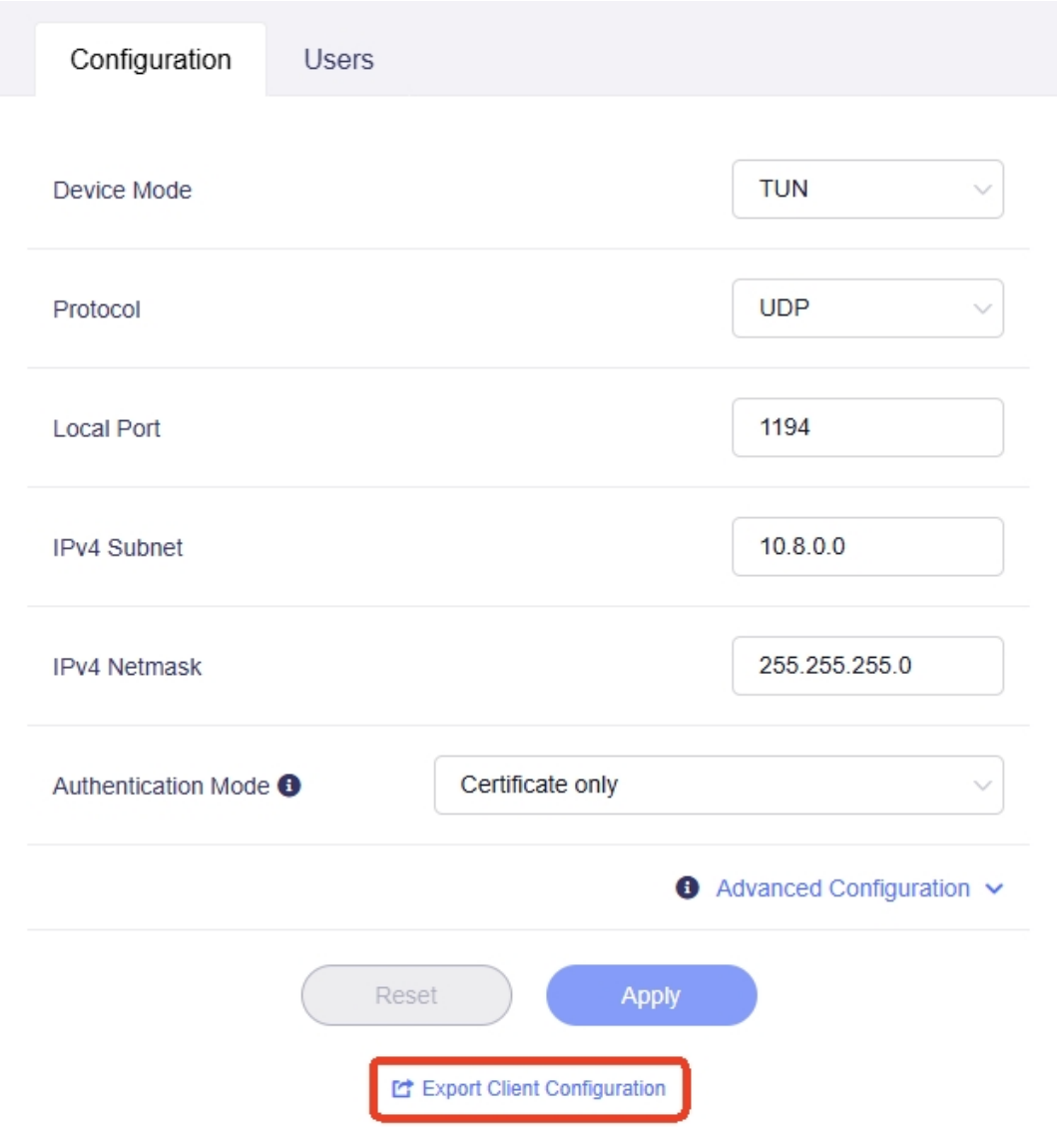
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.
   - Wenn die beiden oben genannten Methoden nicht funktionieren, beispielsweise bei einem Anschluss hinter CGNAT, können Sie unsere SD-WAN-Lösung AstroWarp ausprobieren.

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**.

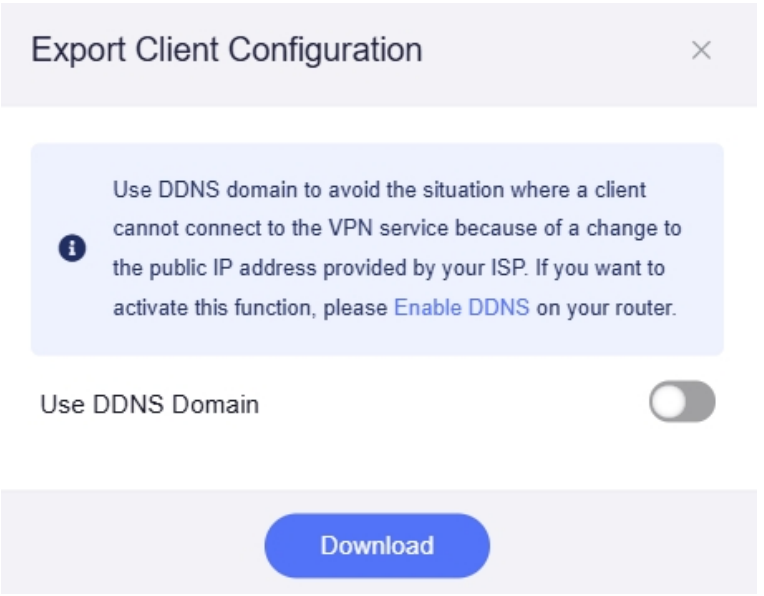


- **Device Mode**: TAP-S2S oder Tun. Die Unterschiede werden hier erläutert.
- **Protocol**: UDP oder TCP. Die Unterschiede werden hier erläutert.
- **Authentication Mode**: Legt fest, wie sich der Client beim Verbinden mit dem Server authentifiziert. Es gibt drei Optionen:

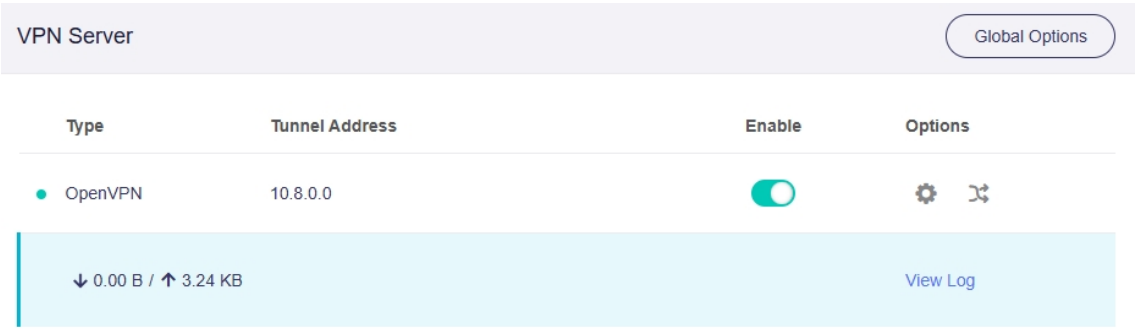
- **Certificate Only**: Der Router erzeugt automatisch die Zertifikate und Schlüssel für Server und Client und bettet sie in die Konfigurationsdatei ein. Nach dem Hochladen der Konfiguration auf den Client sind keine weiteren Zugangsdaten erforderlich.
- **Username/Password Only**: Der Router erzeugt 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. Wenn Sie unten auf der Registerkarte Configuration auf **Export Client Configuration** klicken oder eine geänderte Konfiguration übernehmen, wird das folgende Fenster eingeblendet. Klicken Sie auf **Download**, um die Konfiguration zu exportieren. **Hinweis**: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, aktivieren Sie DDNS, bevor Sie auf Download klicken. Anschließend können Sie die DDNS-Domain als Serveradresse verwenden.



4. OpenVPN-Server aktivieren.
   Öffnen Sie das **VPN Dashboard** und aktivieren Sie den OpenVPN-Server mit dem Schalter. Er wird wie unten dargestellt gestartet.



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:

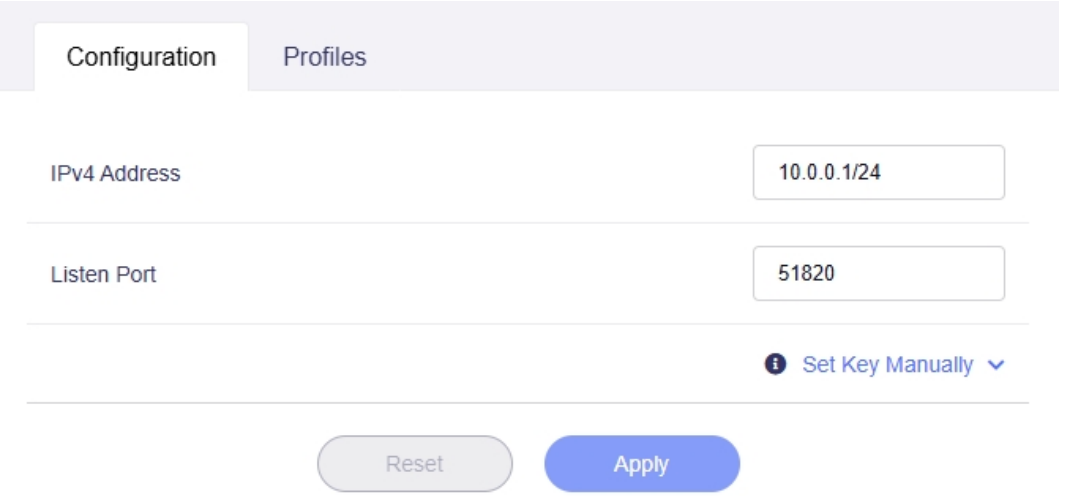
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.
   - Wenn die beiden oben genannten Methoden nicht funktionieren, beispielsweise bei einem Anschluss hinter CGNAT, können Sie unsere SD-WAN-Lösung AstroWarp ausprobieren.

2. **Erforderliche Portweiterleitung prüfen**

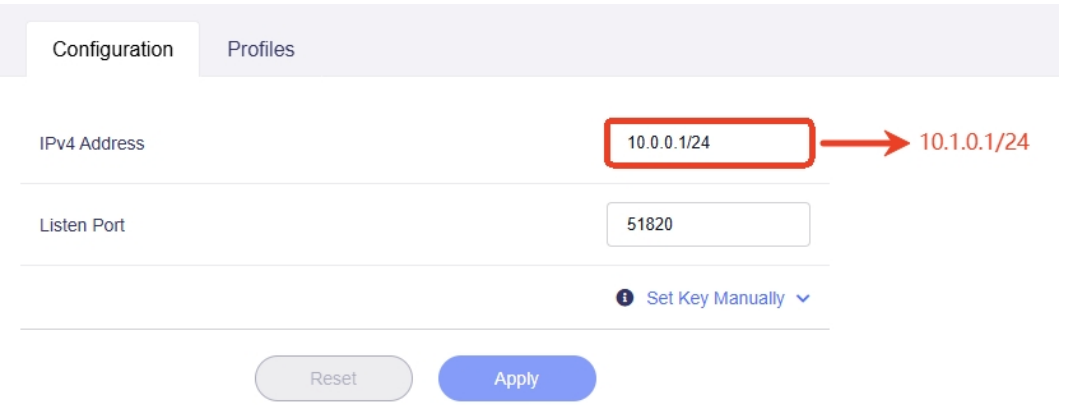
   - Wenn Ihr GL.iNet-Router der Hauptrouter Ihres Netzwerks ist, benötigen Sie keine Portweiterleitung. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn bereits ein Hauptrouter vorhanden ist und Ihr GL.iNet-Router als nachgeschalteter Router arbeitet, müssen Sie auf dem Hauptrouter eine Portweiterleitung 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.



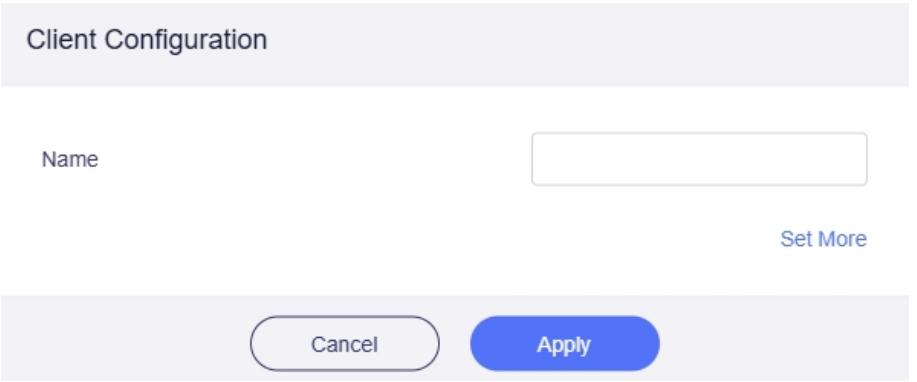
   Bei einem solchen Adresskonflikt wählen Sie eine andere IPv4-Adresse, etwa **10.1.0.1/24**, und klicken Sie auf **Apply**. Achten Sie darauf, die CIDR-Angabe „/24“ beizubehalten, um Verbindungsprobleme zu vermeiden.



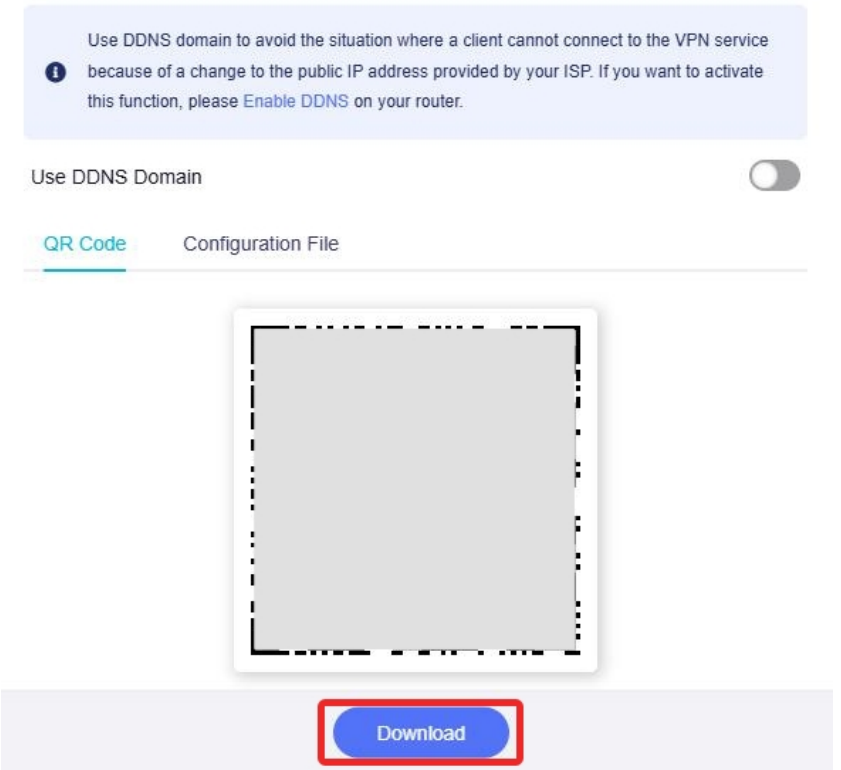
3. Profil hinzufügen.
   Wechseln Sie zur Registerkarte **Profiles** und klicken Sie auf **Add**, um ein Profil für Ihr Gerät zu erzeugen.



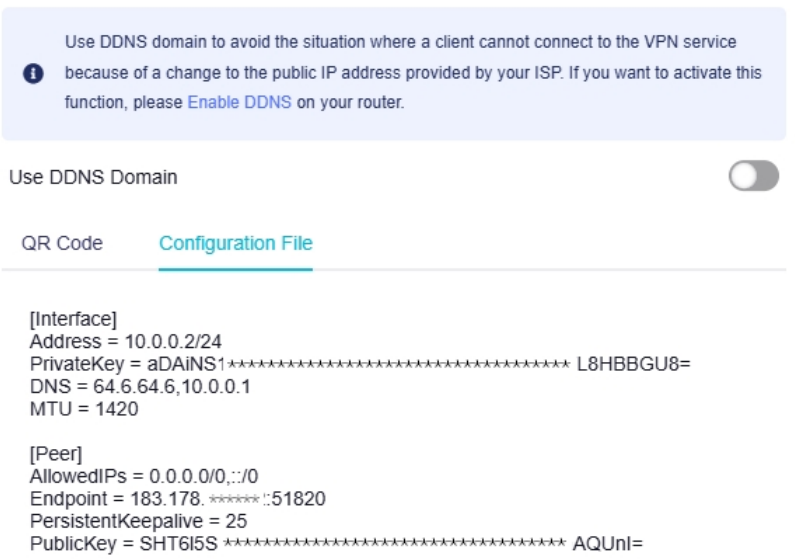
Vergeben Sie einen aussagekräftigen Namen und klicken Sie auf **Apply**, um fortzufahren.



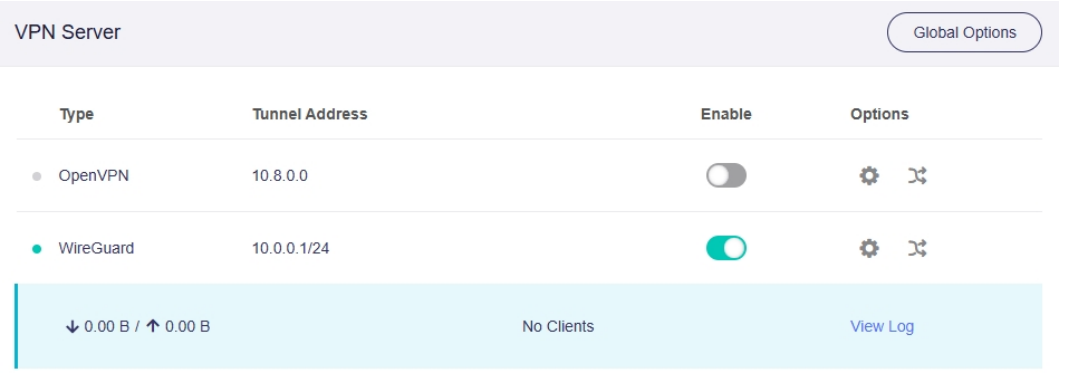
4. Nach dem Hinzufügen eines Profils erstellt der Router eine Konfiguration in drei Formaten: QR-Code, .conf-Datei und Klartext. Wählen Sie das gewünschte Format. **Hinweis**: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, aktivieren Sie DDNS, bevor Sie die Datei herunterladen.
   - **QR-Code**: 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.
   - **.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.



- **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.



5. WireGuard-Server aktivieren.
   Öffnen Sie das **VPN Dashboard** und aktivieren Sie Ihren WireGuard-Server mit dem Schalter. Er wird wie unten dargestellt gestartet.



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.

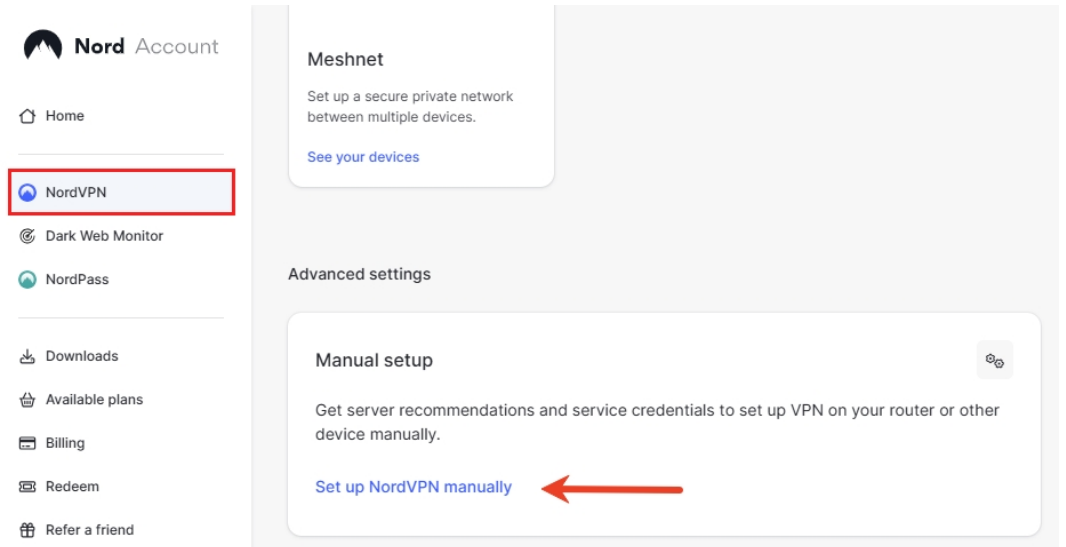
Rufen Sie anschließend die offizielle Webseite Ihres VPN-Anbieters auf und beschaffen Sie die Dienstzugangsdaten oder eine Konfigurationsdatei. Falls Sie nicht wissen, wie Sie die Datei erhalten, folgen Sie diesem Link oder wenden Sie sich an den Support des Anbieters.

10.1.2 NordVPN einrichten

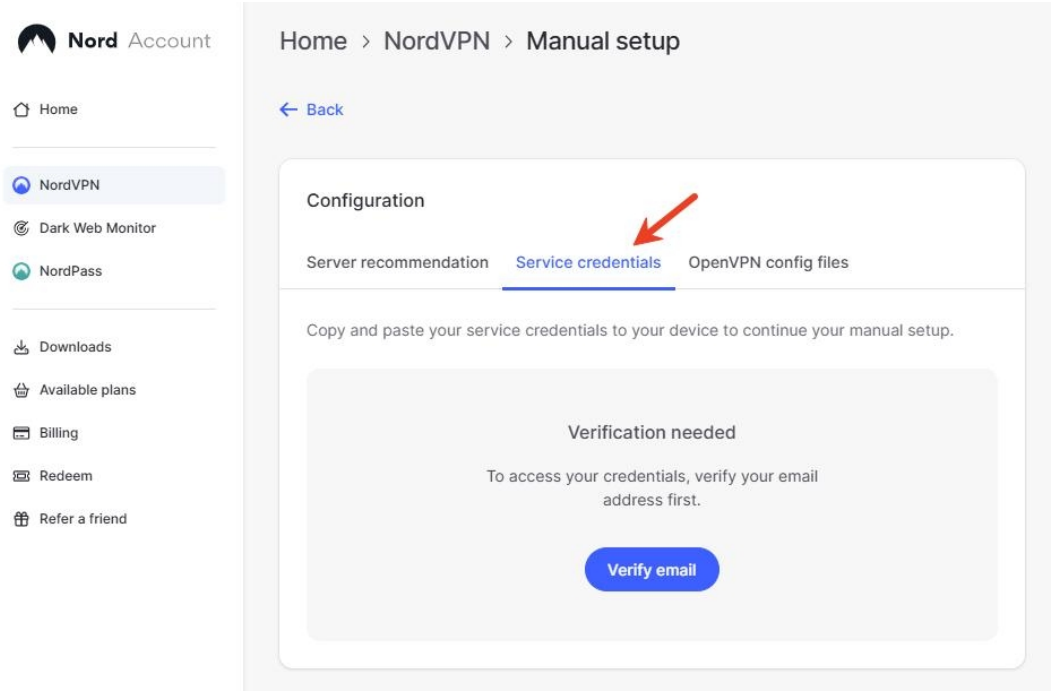
NordVPN ist in die GL.iNet-Weboberfläche integriert. Geben Sie Ihre im NordVPN-Dashboard erhältlichen Zugangsdaten in der Weboberfläche des Routers oder in der GL.iNet-App ein, um die Konfigurationsdateien aller NordVPN-Server abzurufen. Ein manuelles Hochladen der Dateien ist dadurch nicht erforderlich.

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

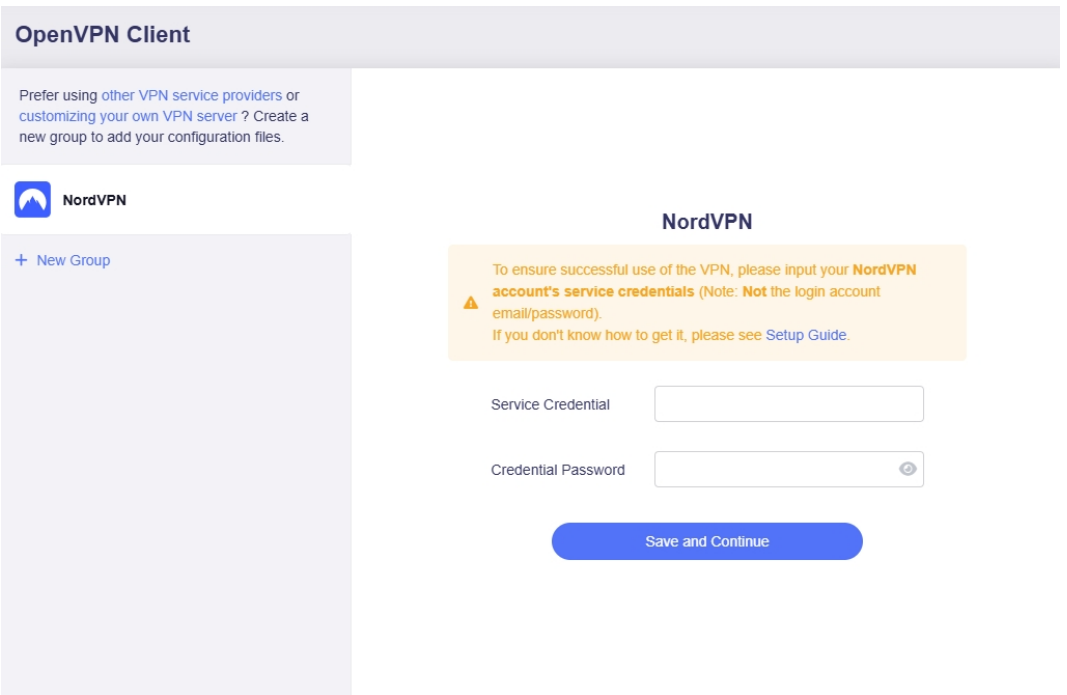
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



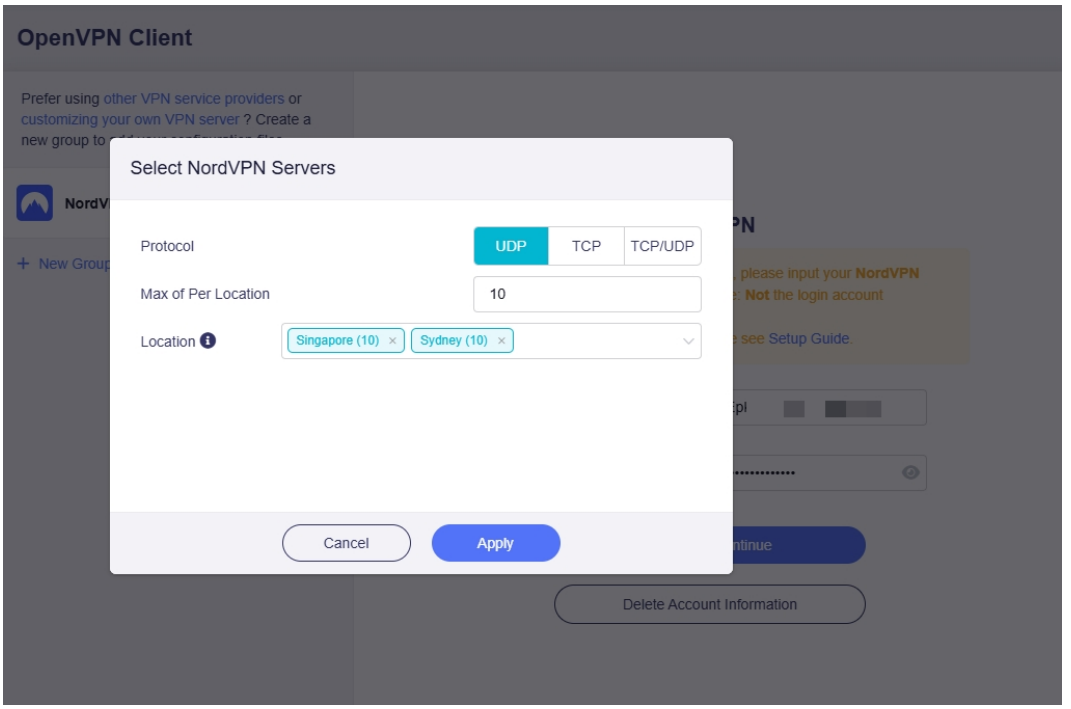
Dort finden Sie die **Dienstzugangsdaten**. Kopieren Sie diese für die spätere Verwendung.



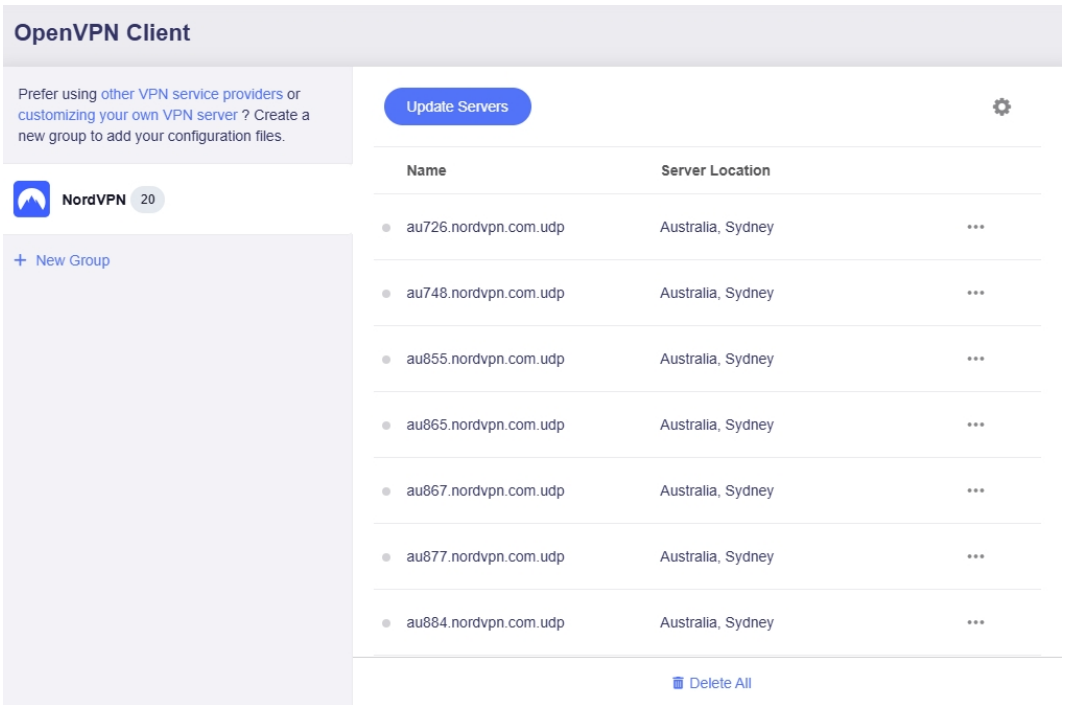
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **OpenVPN Client** > **NordVPN**. Geben Sie die Dienstzugangsdaten ein. Hinweis: Dies sind NICHT die E-Mail-Adresse und das Passwort Ihres Benutzerkontos. Klicken Sie anschließend auf **Save and Continue**.



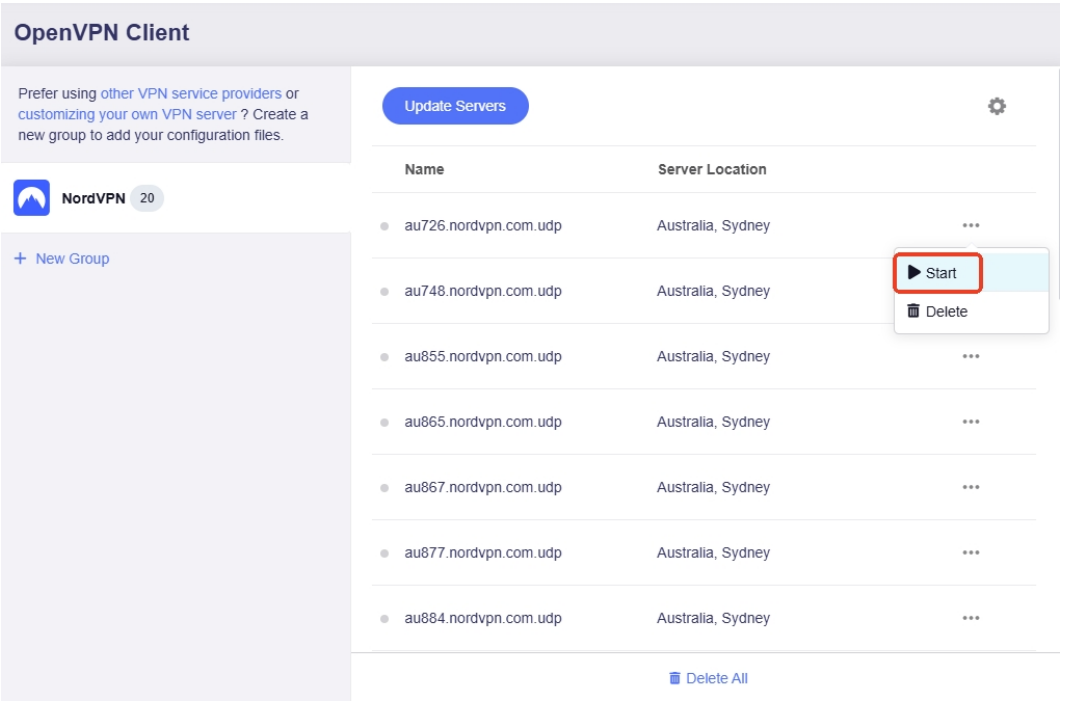
4. Wählen Sie das Protokoll, die maximale Serveranzahl pro Standort und die Standorte aus. Klicken Sie anschließend auf **Apply**.



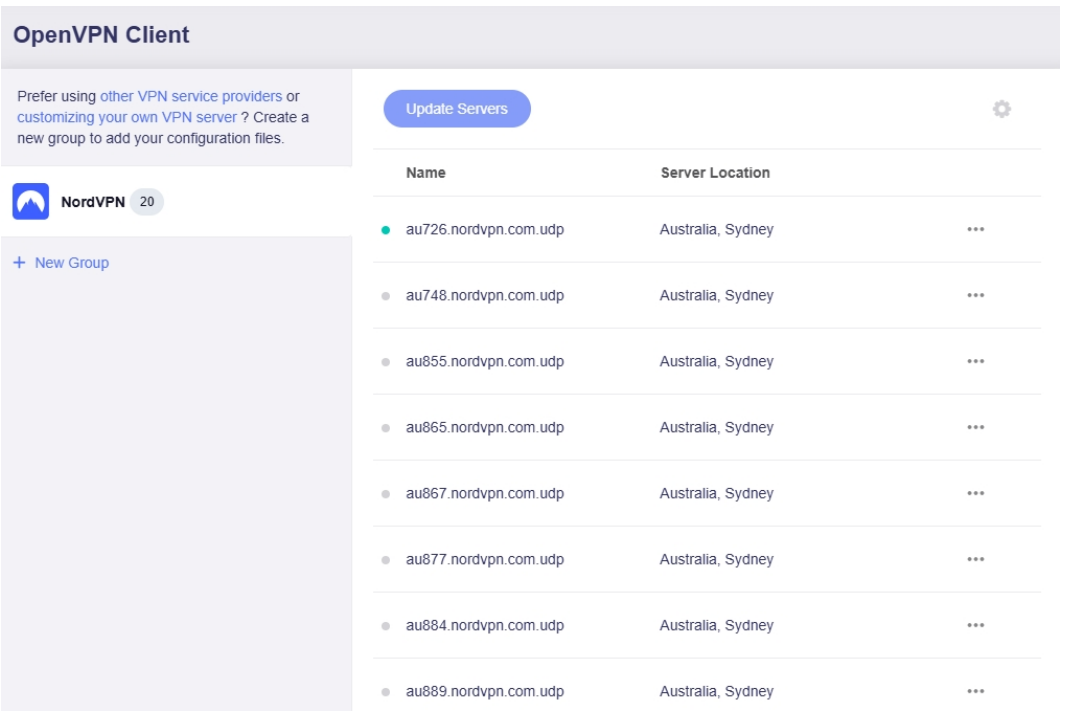
Die Konfigurationsdateien werden heruntergeladen.



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



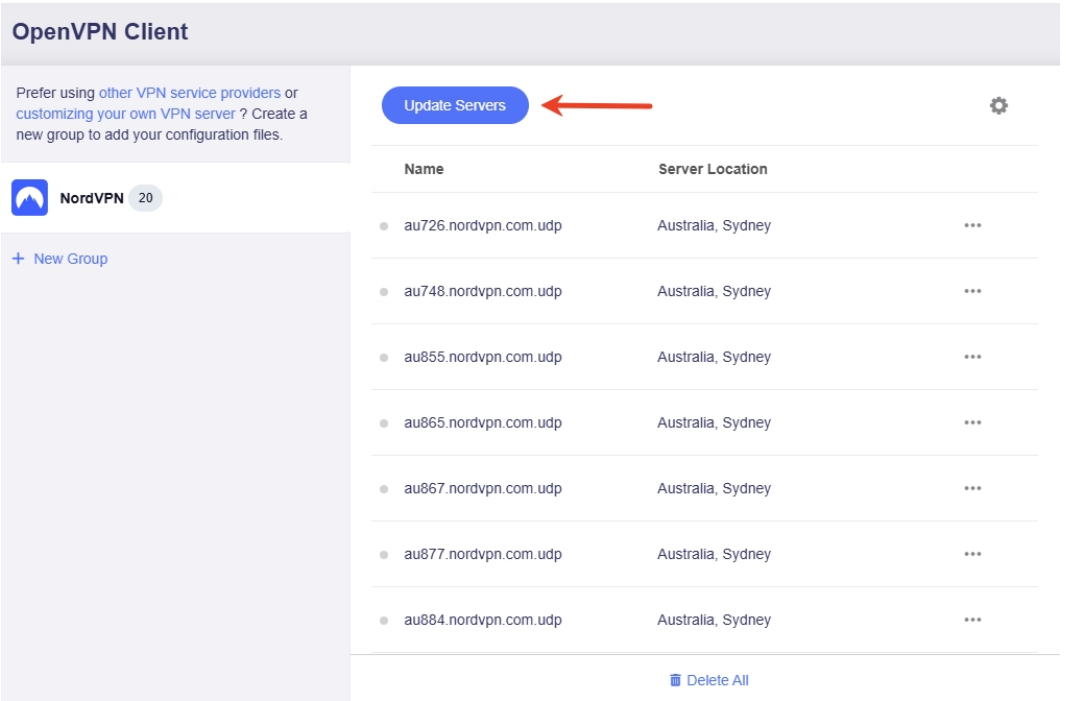
6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

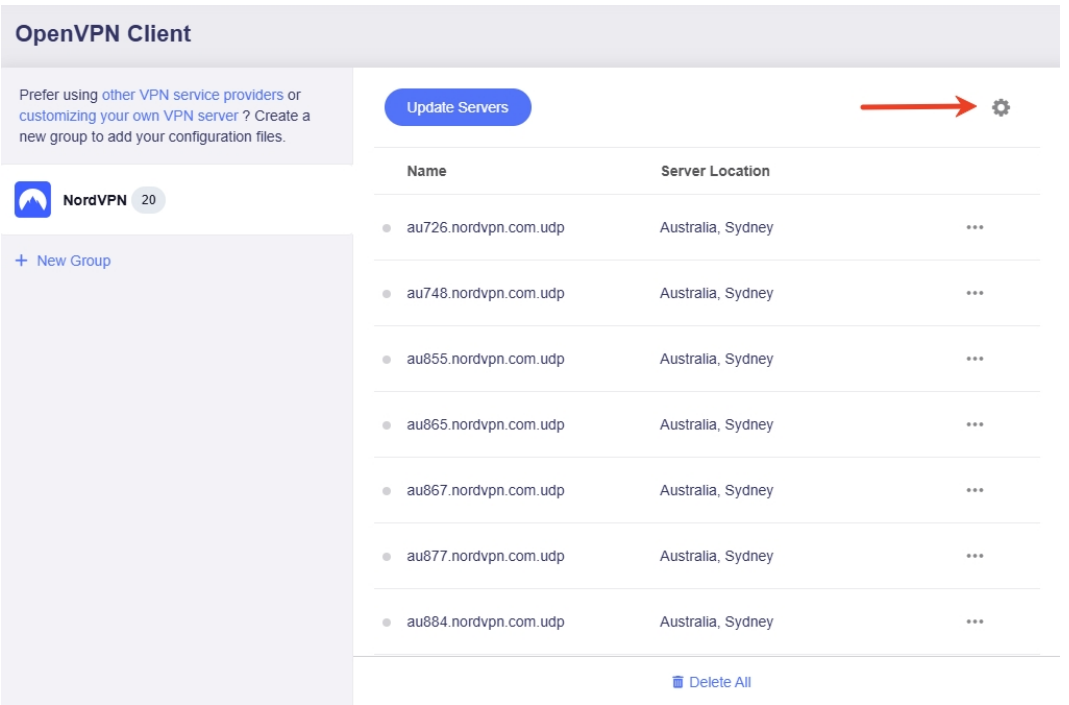
7. Server aktualisieren.

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



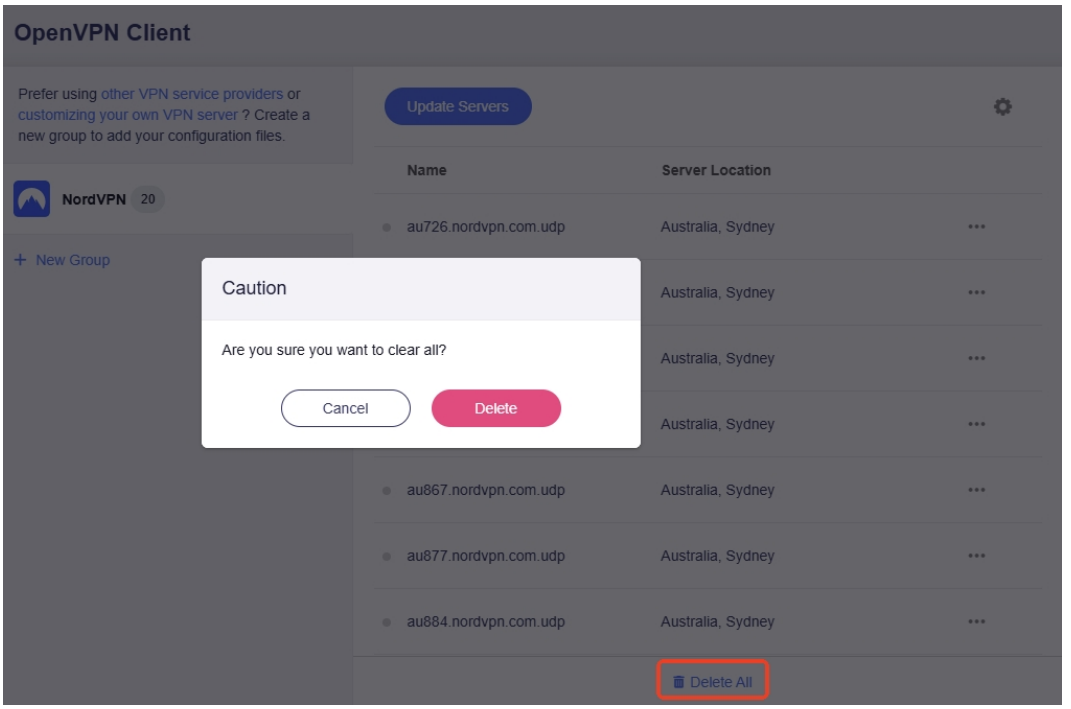
8. Zugangsdaten bearbeiten.

   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.

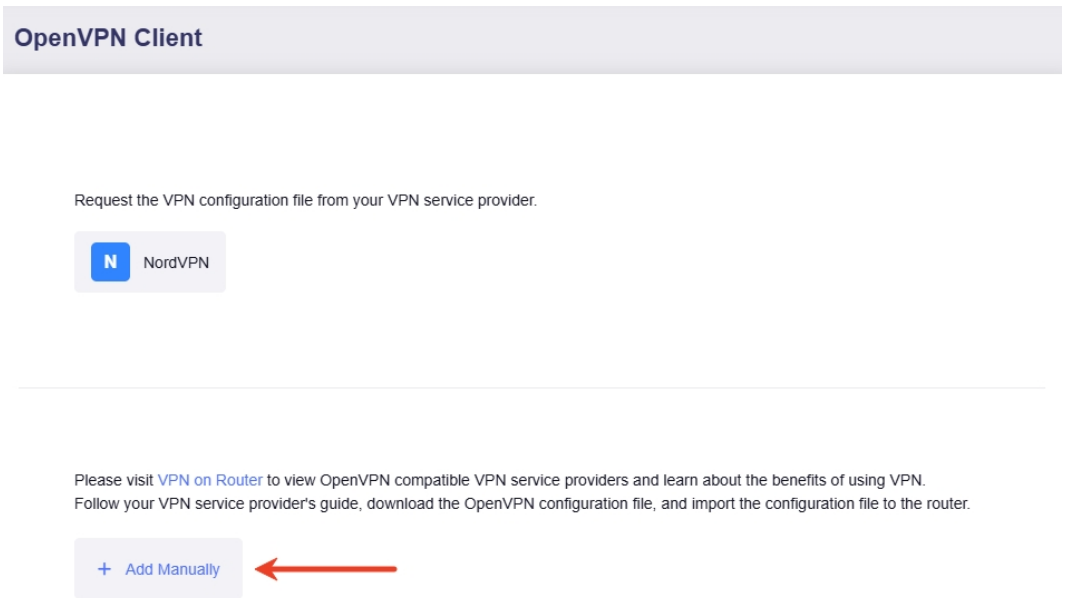

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp
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)

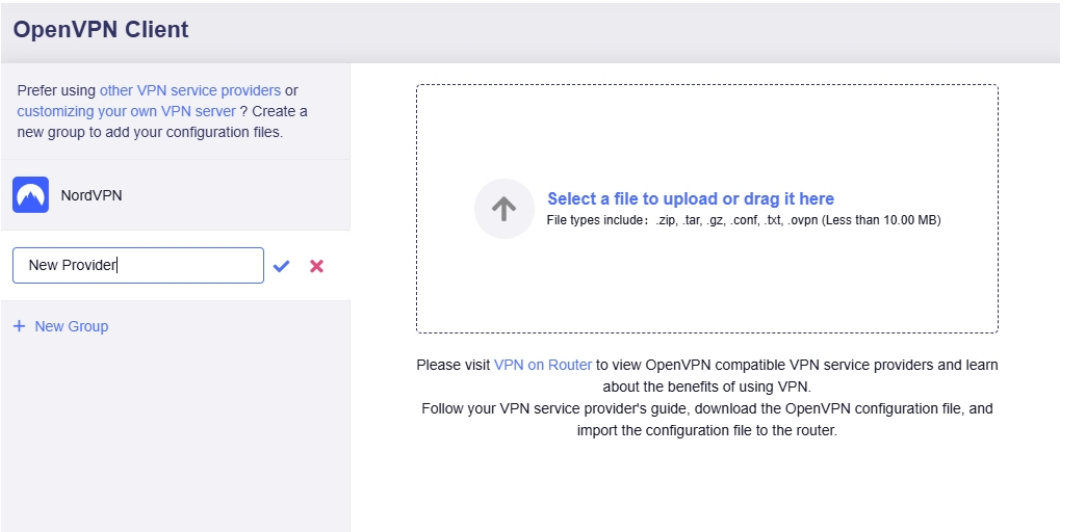
Wenn Ihr OpenVPN-Anbieter nicht in unsere Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den OpenVPN-Client einzurichten.

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

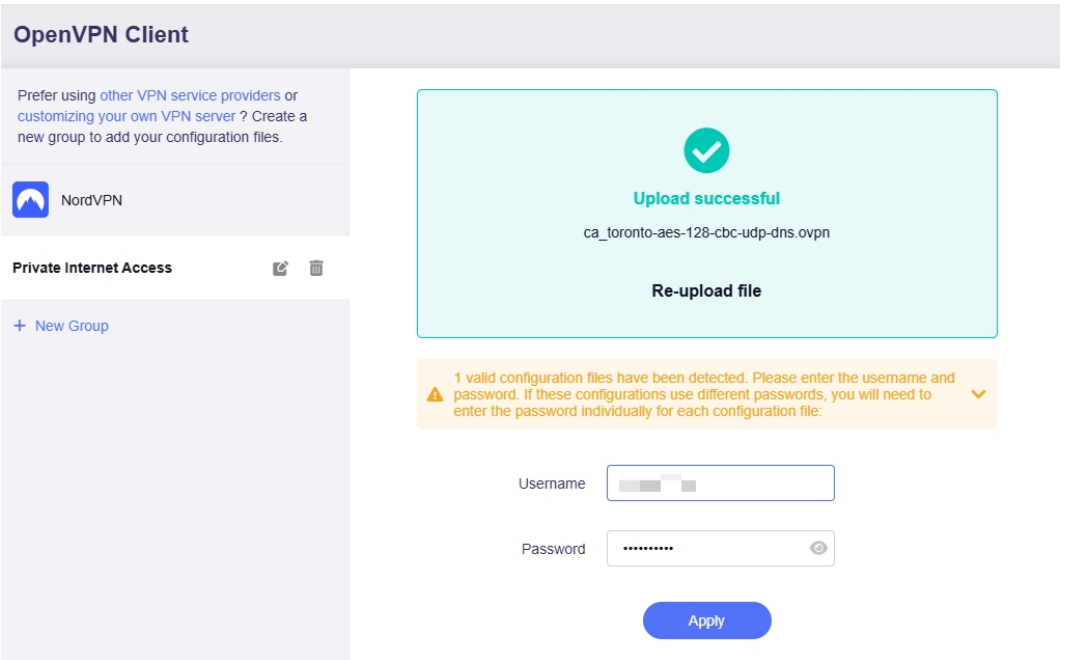
1. Laden Sie eine Konfigurationsdatei von der offiziellen Webseite von Private Internet Access herunter.
2. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Client** und klicken Sie auf **Add Manually**.



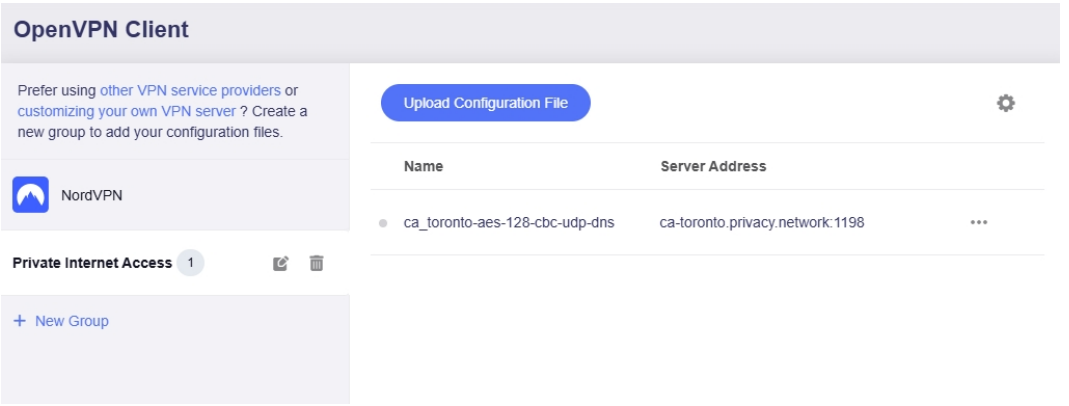
3. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



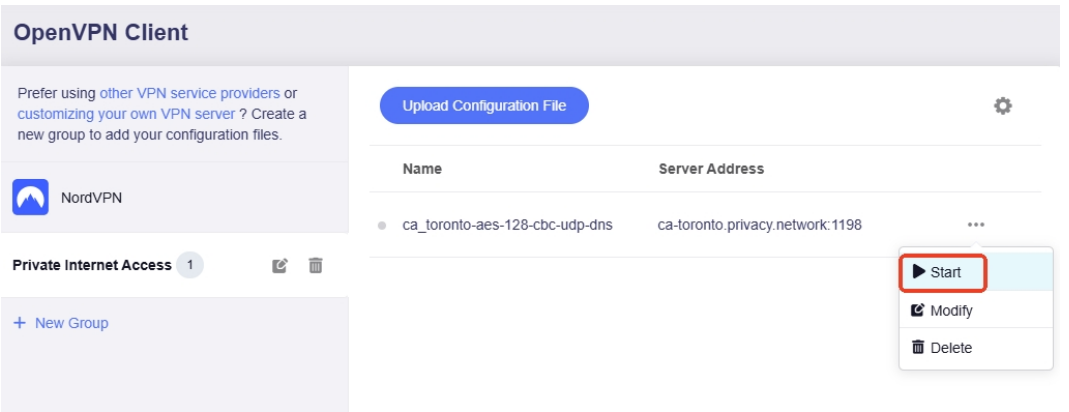
4. Laden Sie Ihre OpenVPN-Konfigurationsdatei hoch. Geben Sie bei Bedarf die Zugangsdaten ein und klicken Sie auf **Apply**.



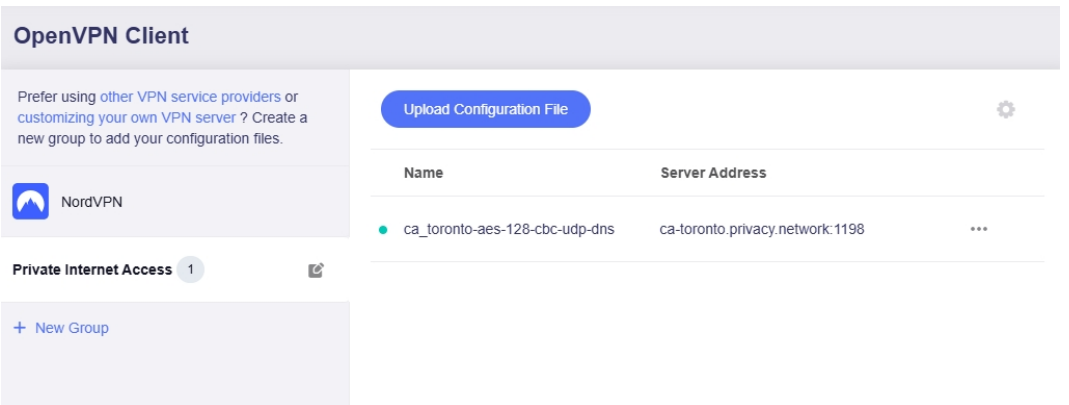
Die hochgeladene Konfigurationsdatei wird angezeigt.



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.

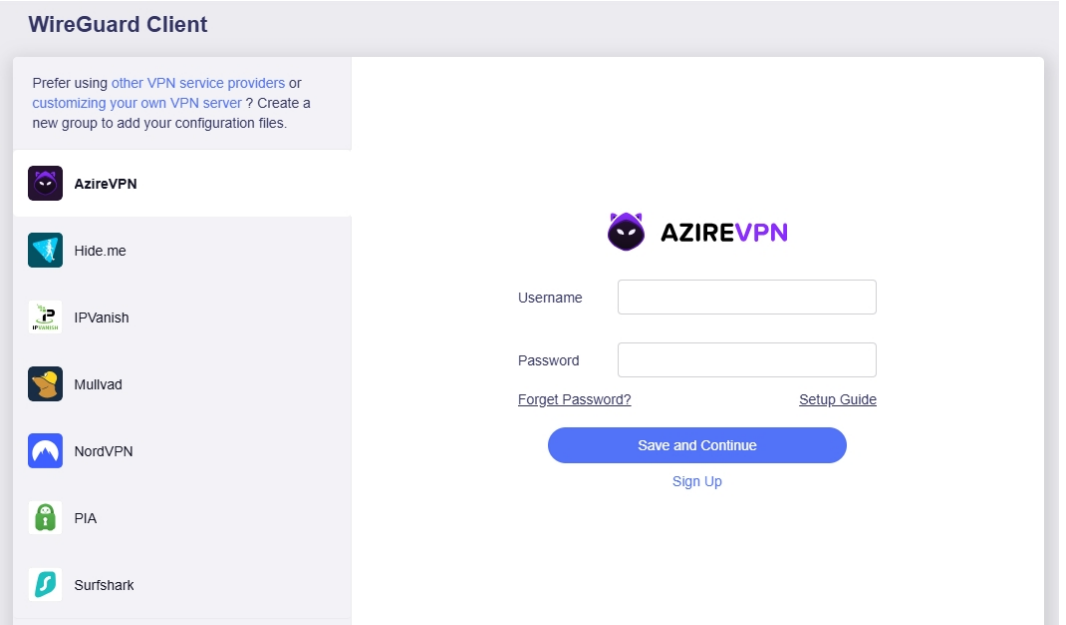
Wählen Sie nachstehend Ihren WireGuard-Anbieter aus, um direkt zur passenden Schritt-für-Schritt-Anleitung zu gelangen.

- AzireVPN einrichten
- Hide.me einrichten
- IPVanish einrichten
- Mullvad einrichten
- NordVPN einrichten
- PIA (Private Internet Access) einrichten
- Surfshark einrichten
- WireGuard-Client manuell einrichten (andere Anbieter)

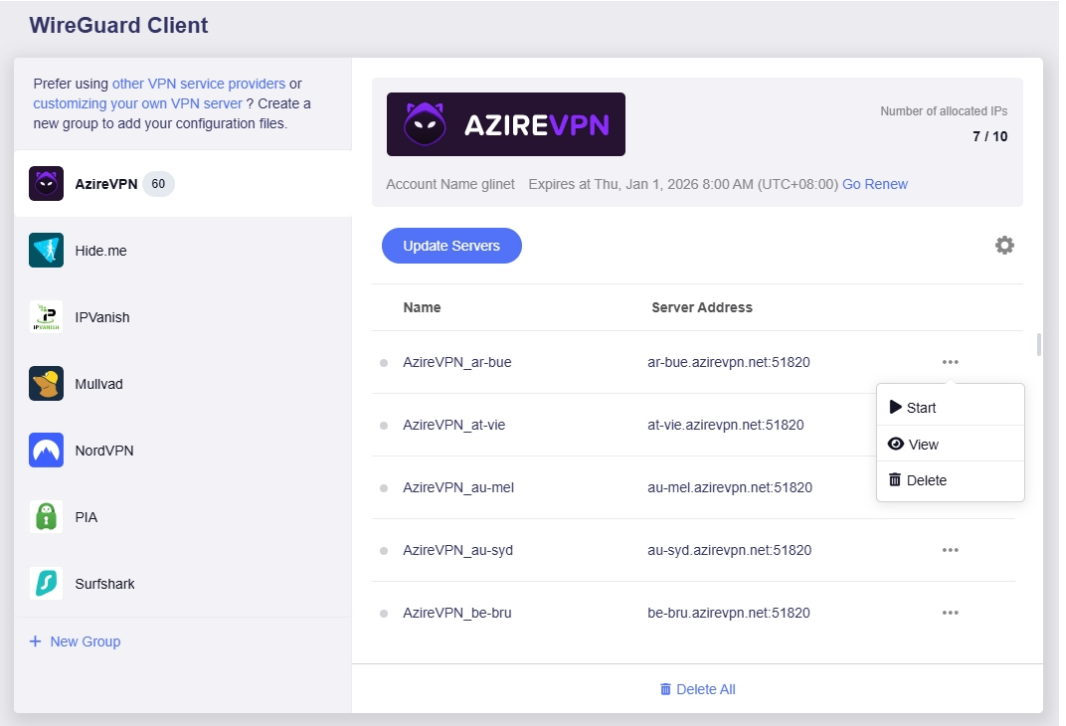
10.2.2 AzireVPN einrichten

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

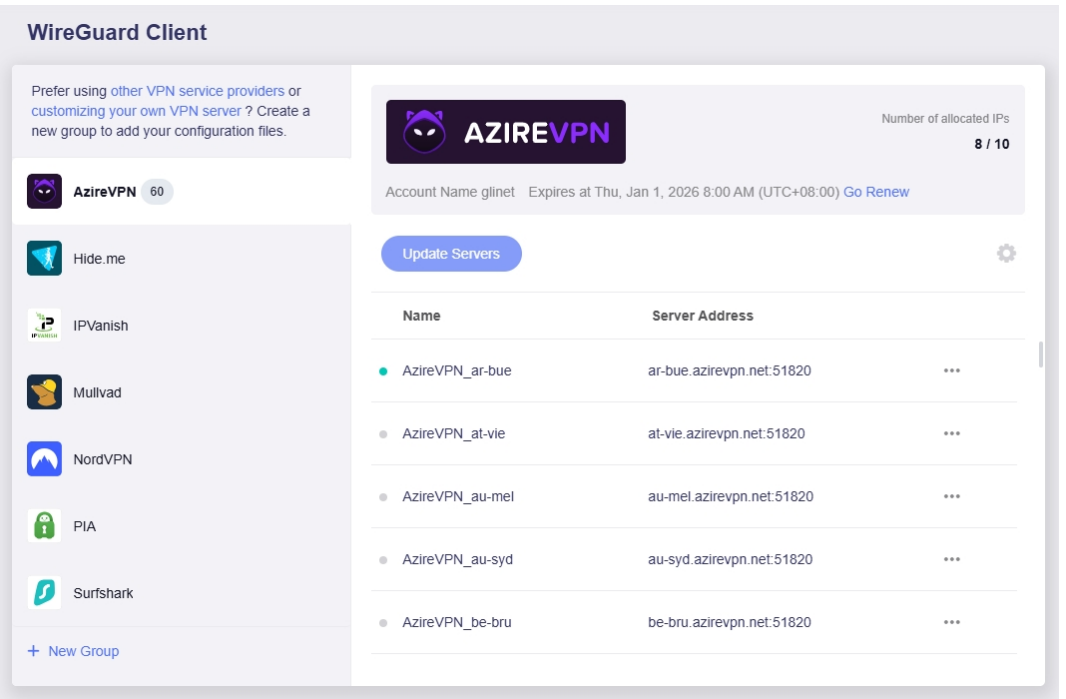
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **AzireVPN**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



3. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



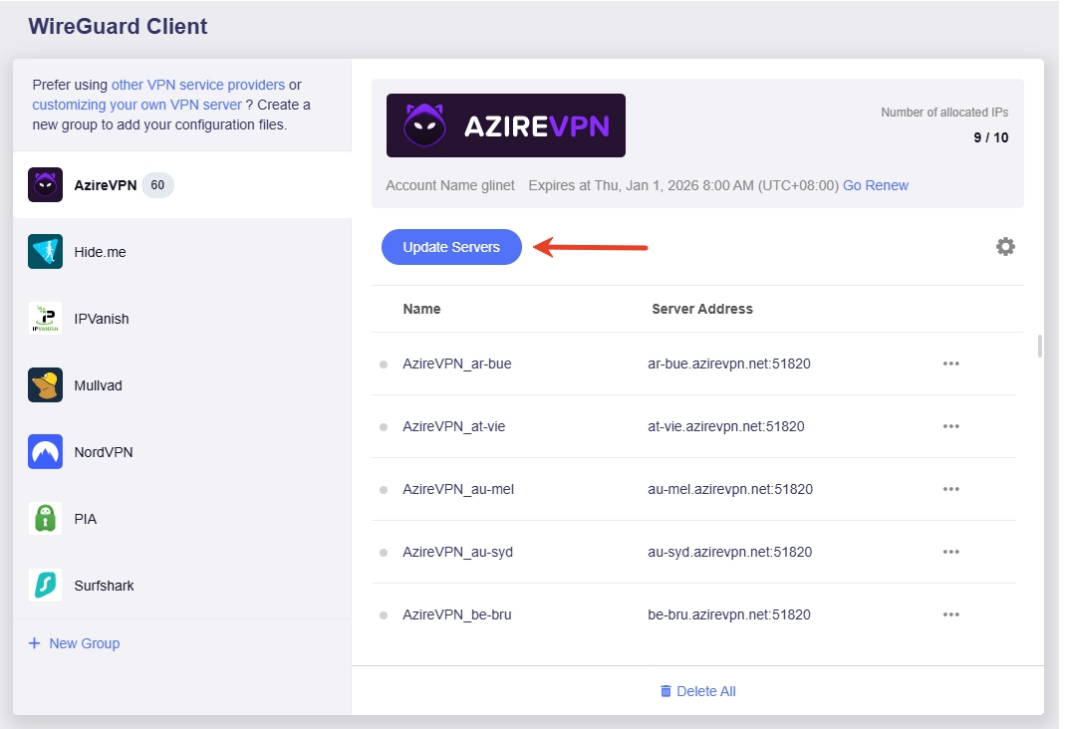
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

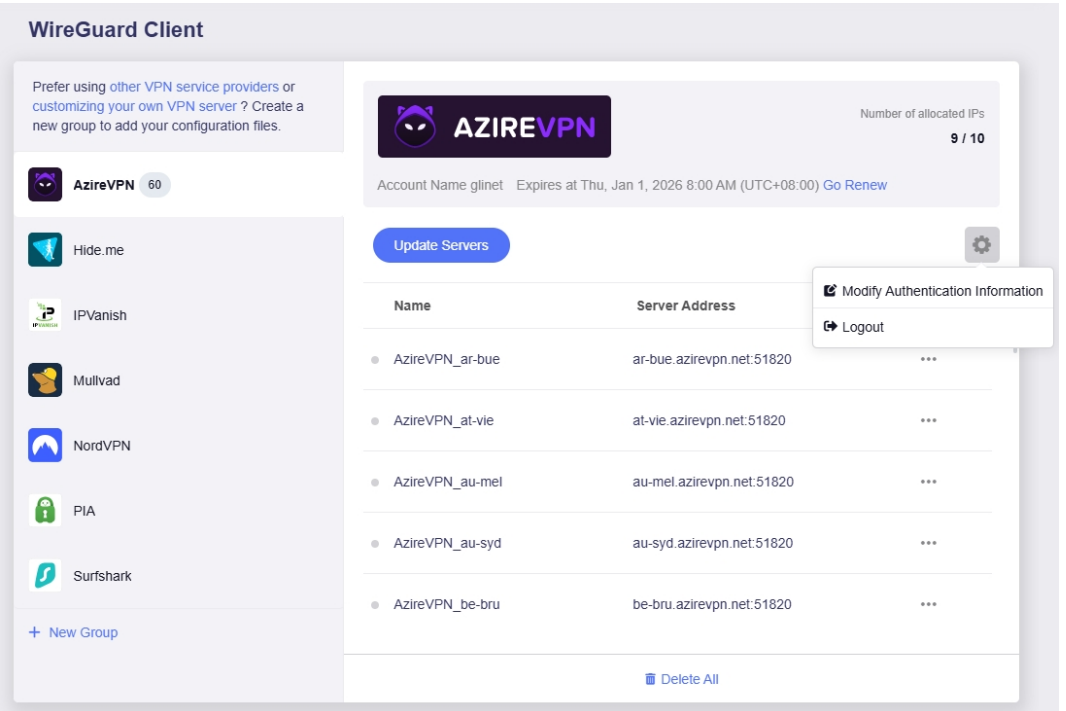
5. Server aktualisieren.

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



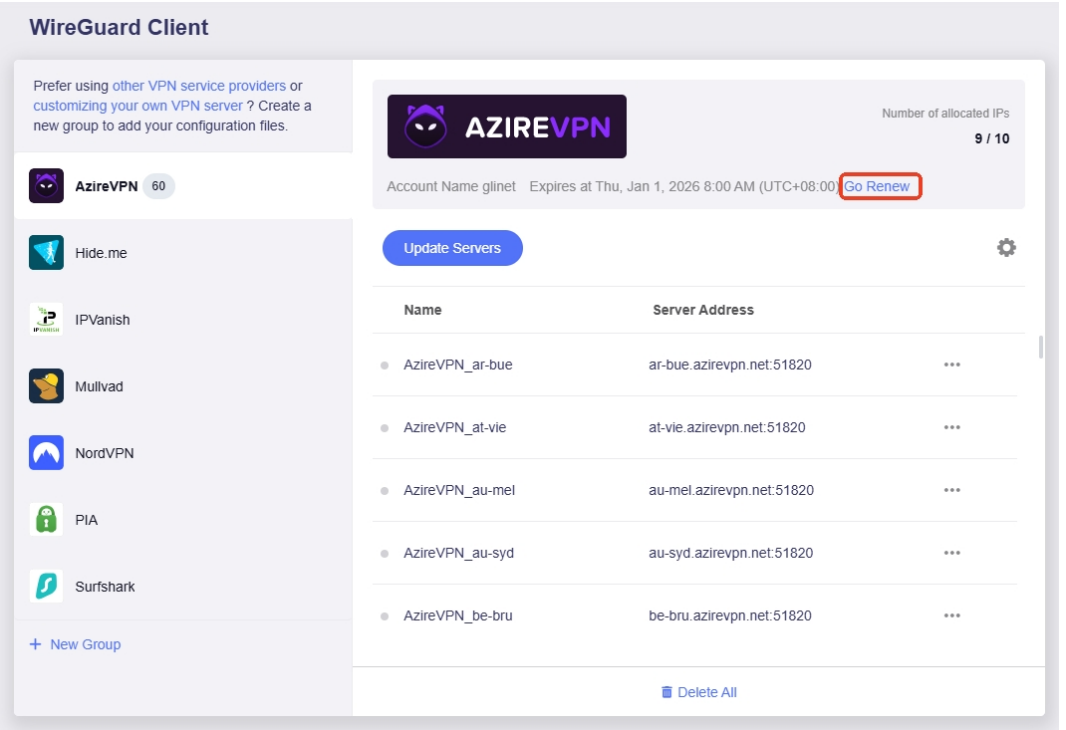
6. Zugangsdaten bearbeiten oder abmelden.

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

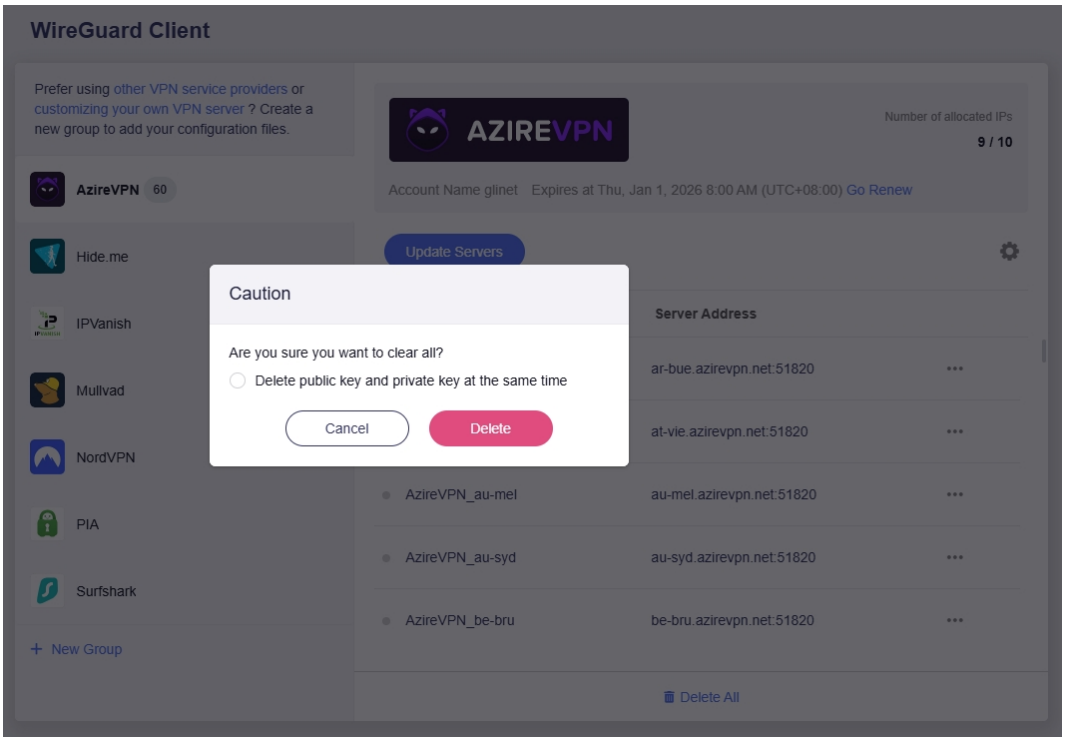


7. Abonnement verlängern.

Wenn Sie auf **Go Renew** klicken, werden Sie zur offiziellen Website weitergeleitet, auf der Sie Ihr Abonnement verlängern können.



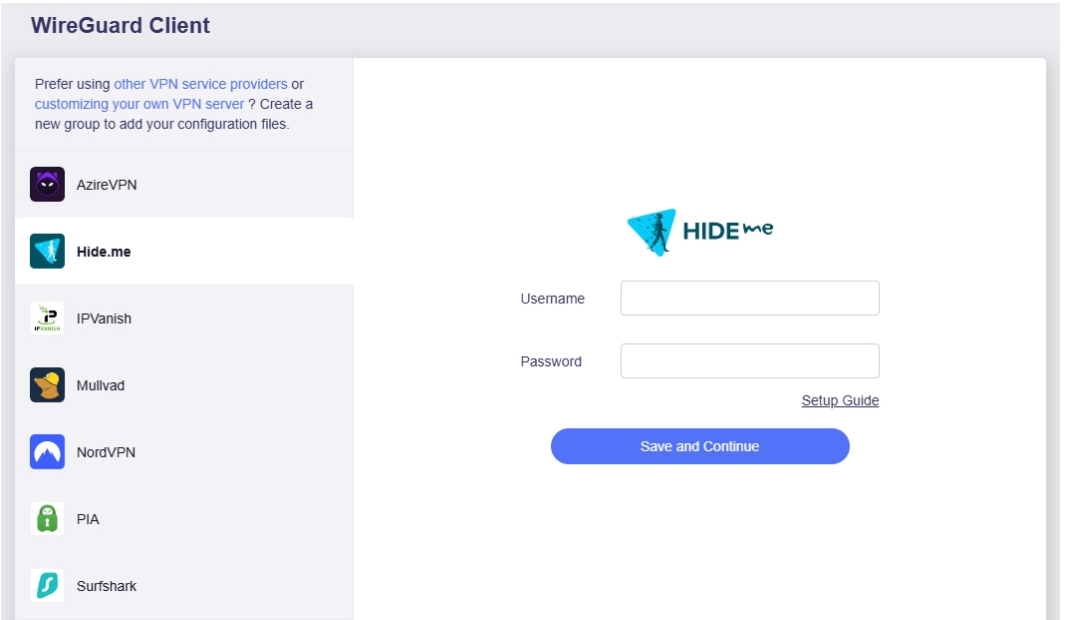
8. Alle Dateien löschen.
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
AzireVPN 60
Hide.me
IPVanish
Mullvad
NordVPN
PIA
Surfshark
New Group
AZIREVPN
Number of allocated IPs
9 / 10
Account Name glinet Expires at Thu, Jan 1, 2026 8:00 AM (UTC+08:00) Go Renew
Update Servers
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete
Server Address
ar-bue.azirevpn.net:51820
at-vie.azirevpn.net:51820
AzireVPN_au-mel
au-mel.azirevpn.net:51820
AzireVPN_au-syd
au-syd.azirevpn.net:51820
AzireVPN_be-bru
be-bru.azirevpn.net:51820
Delete All

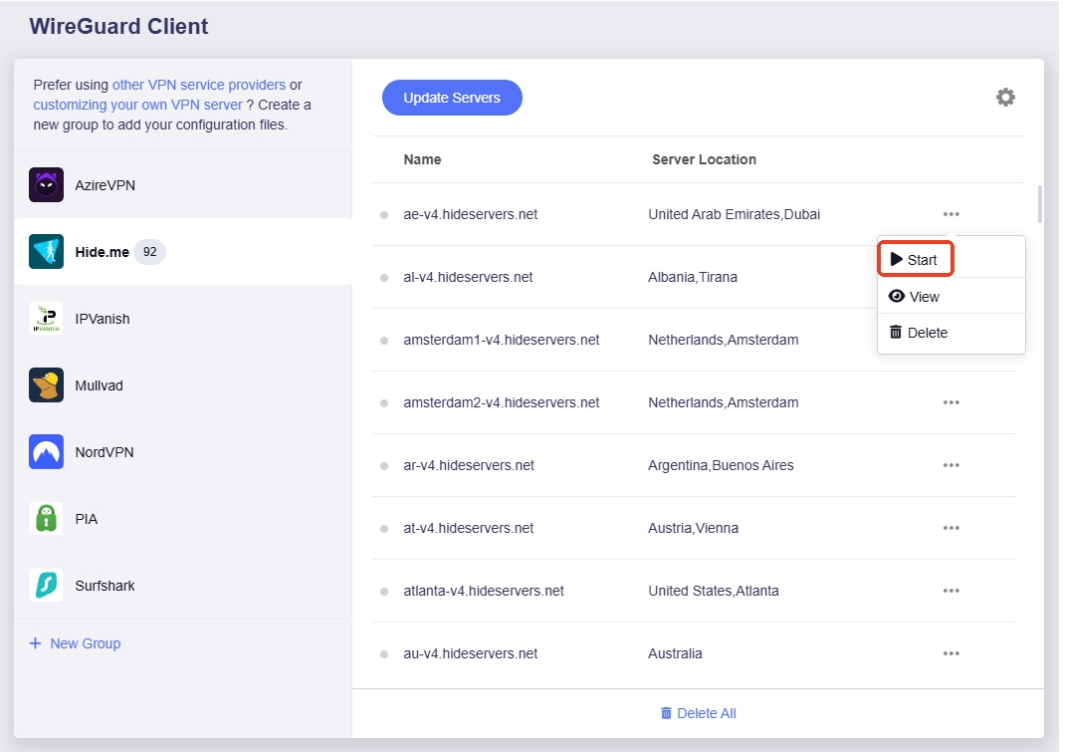
10.2.3 Hide.me einrichten

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

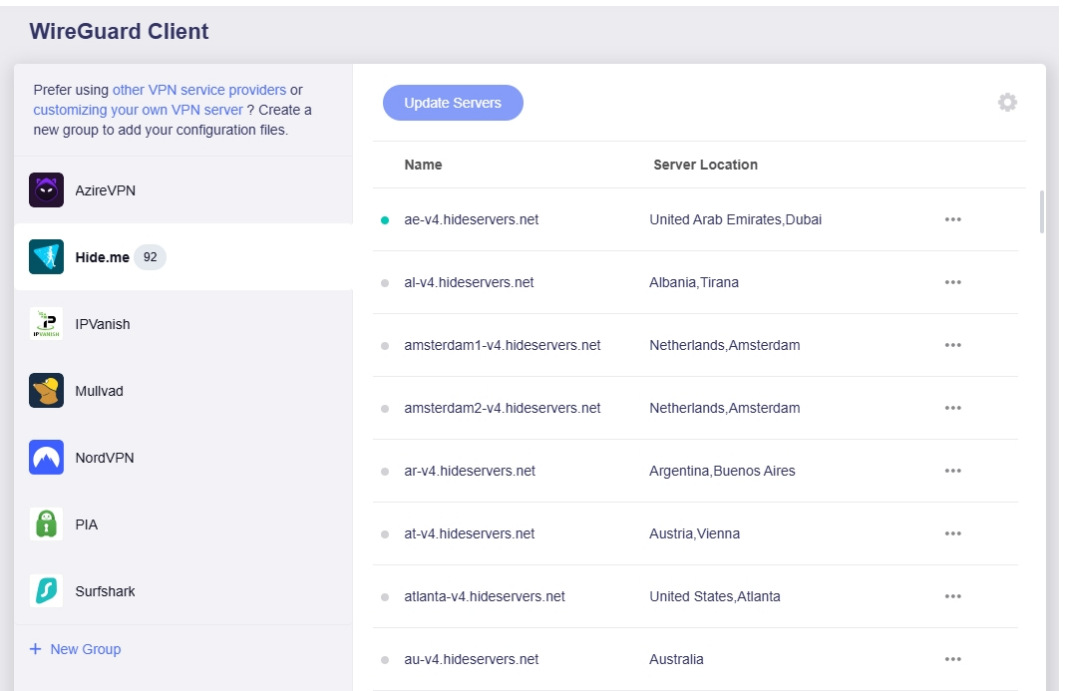
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Hide.me**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



3. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



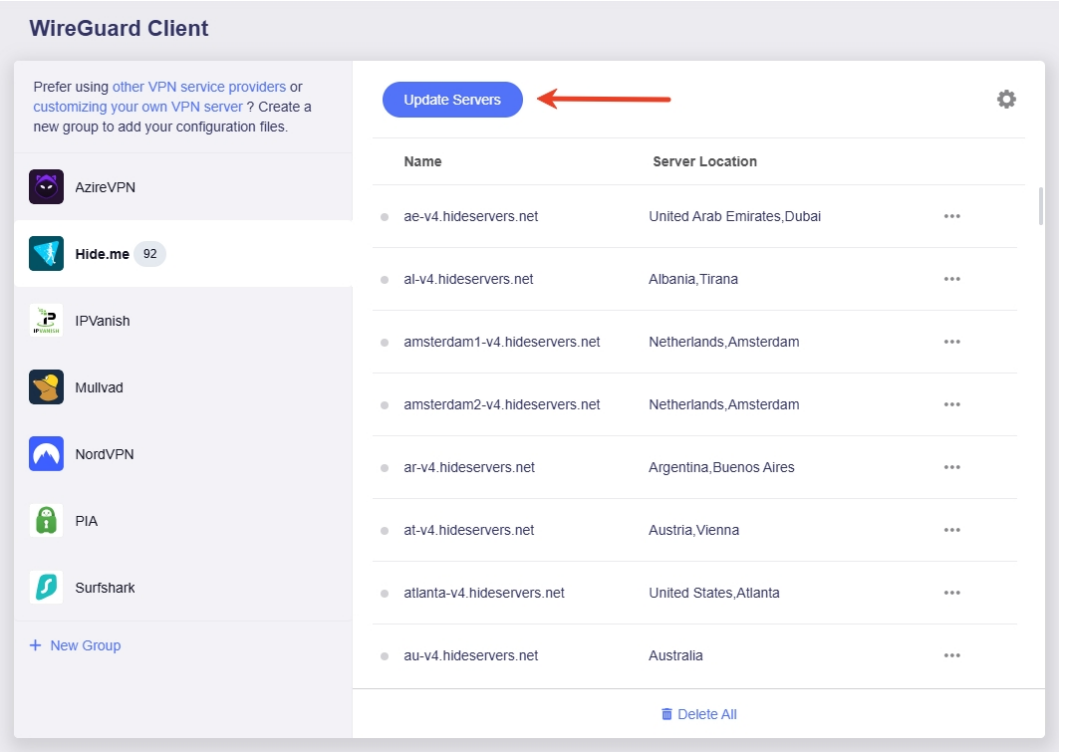
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

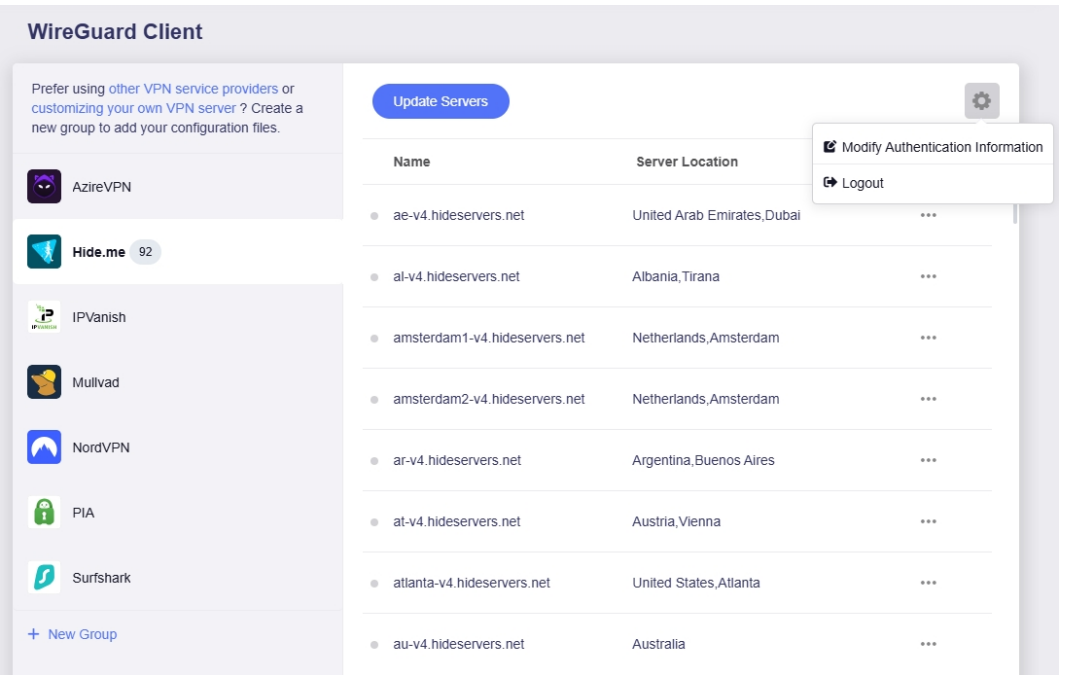
5. Server aktualisieren.

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



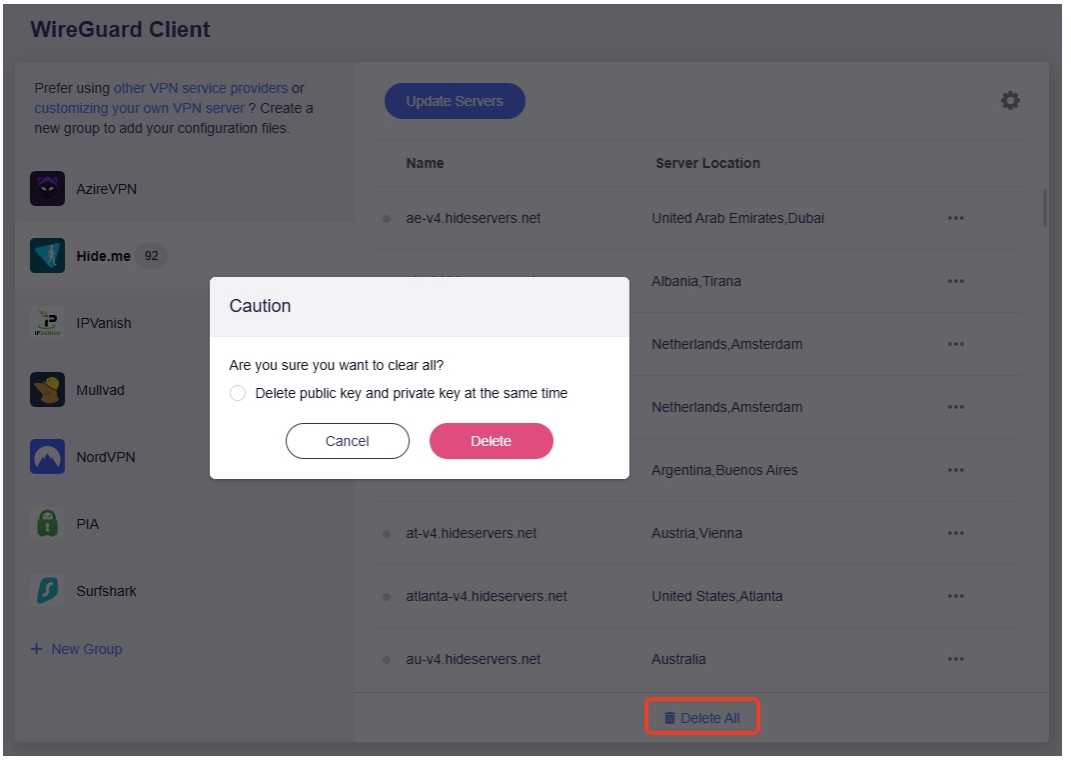
6. Zugangsdaten bearbeiten oder abmelden.

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



7. Alle Dateien löschen.

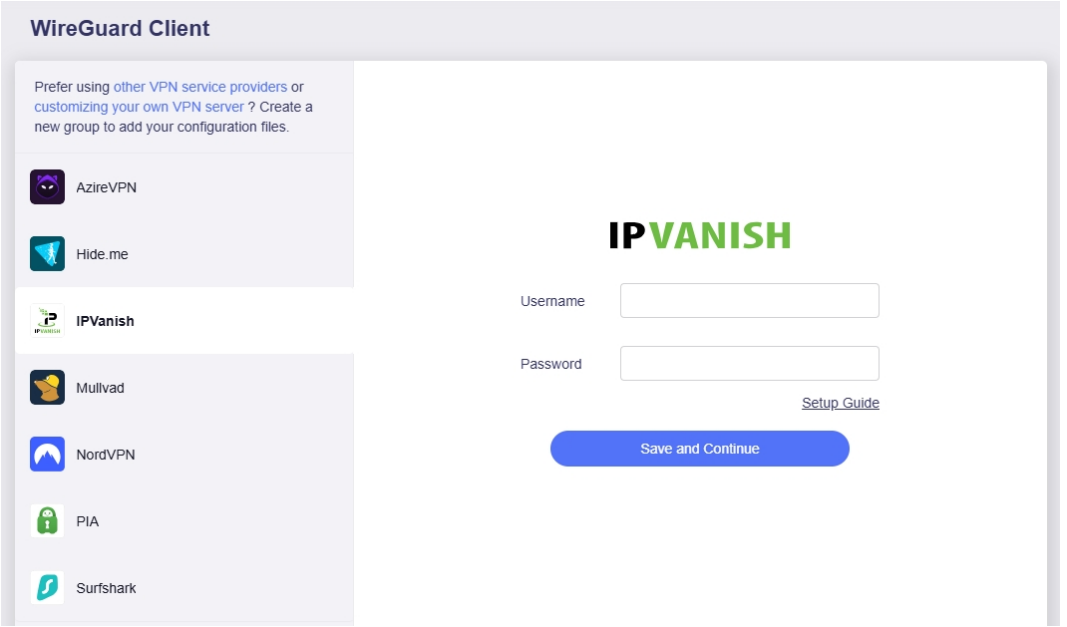
Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



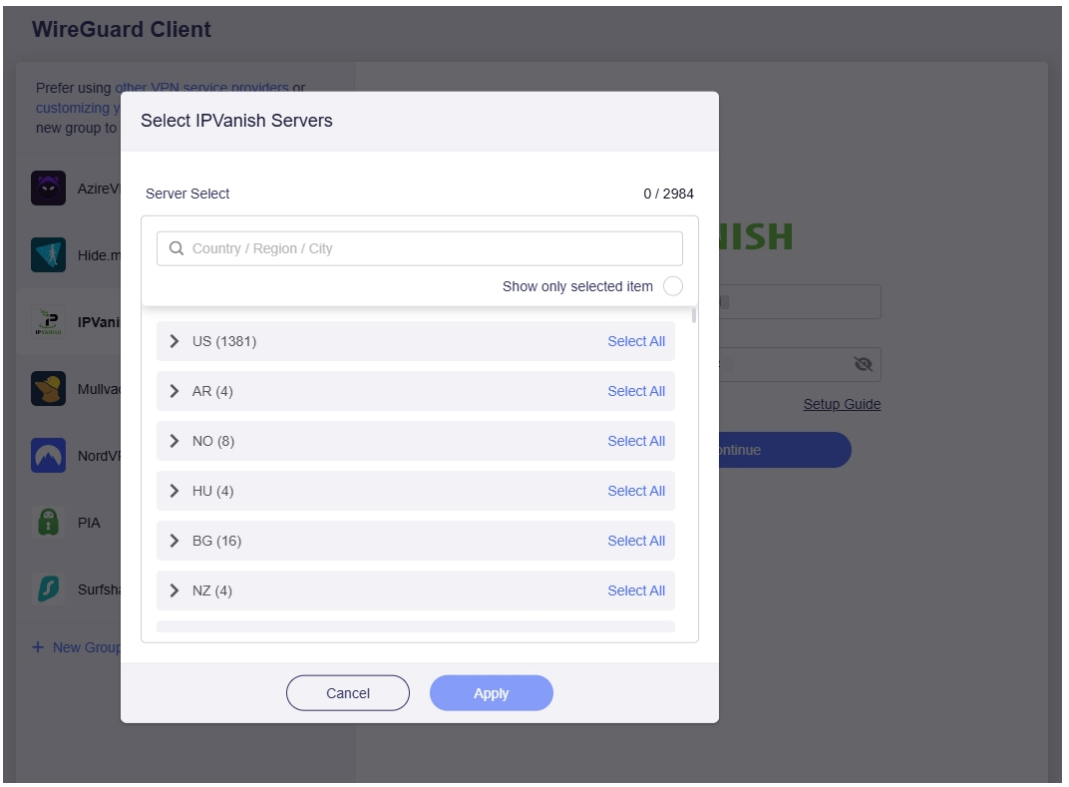
10.2.4 IPVanish einrichten

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

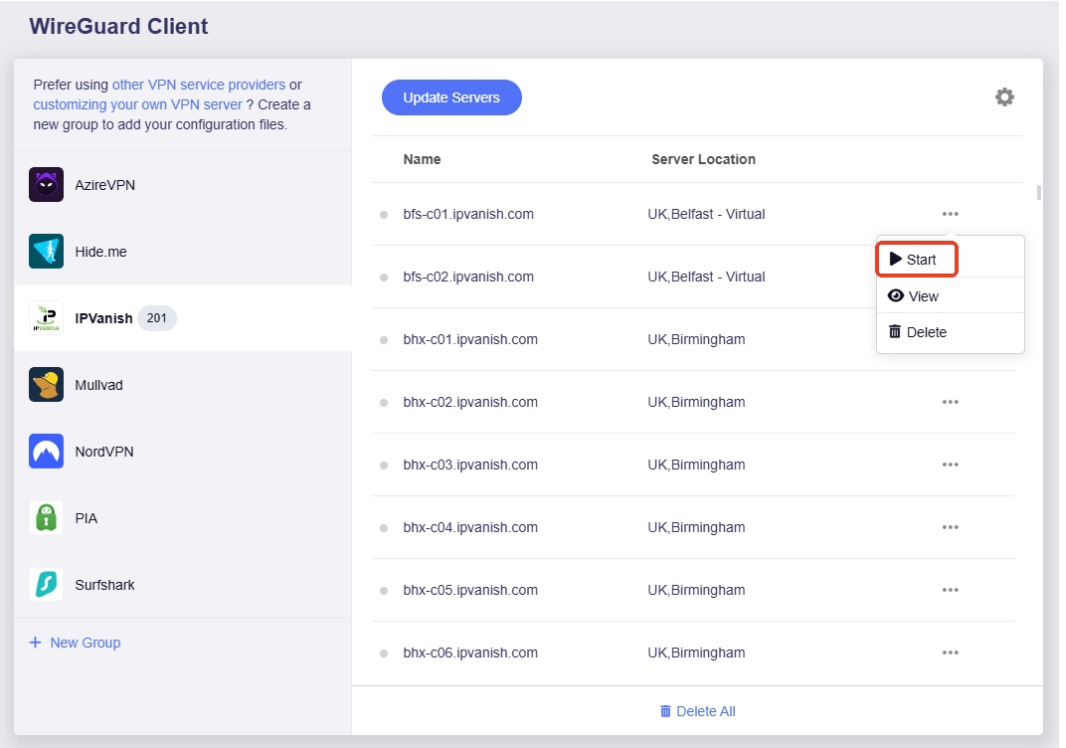
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **IPVanish**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



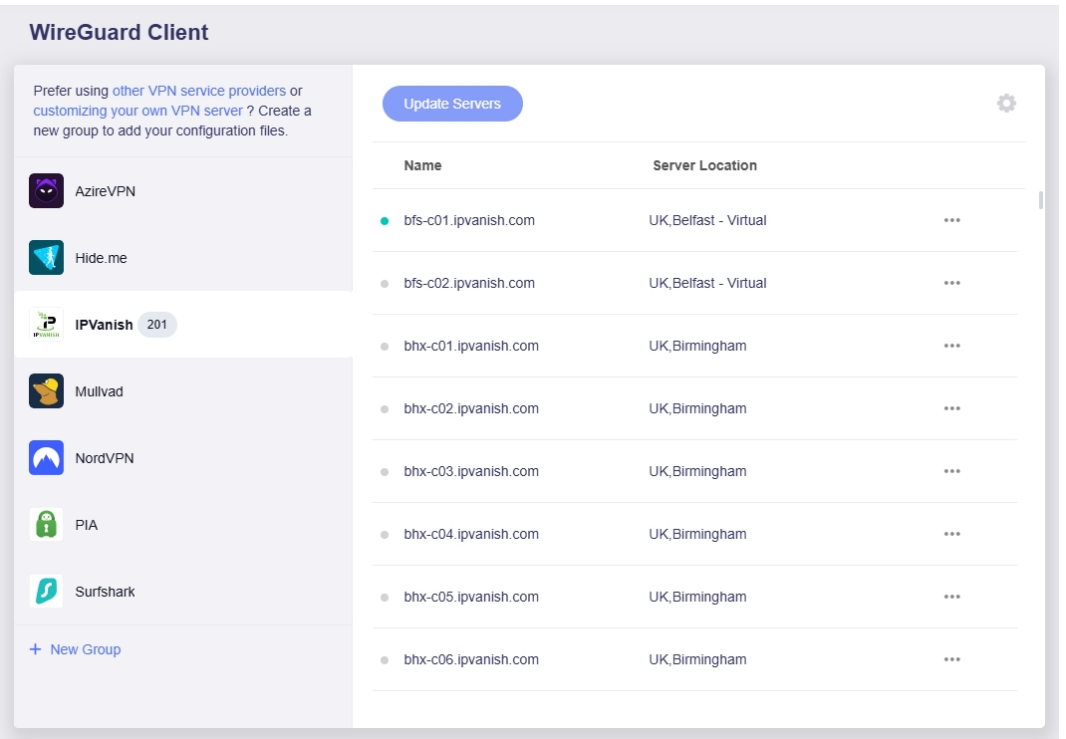
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



4. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



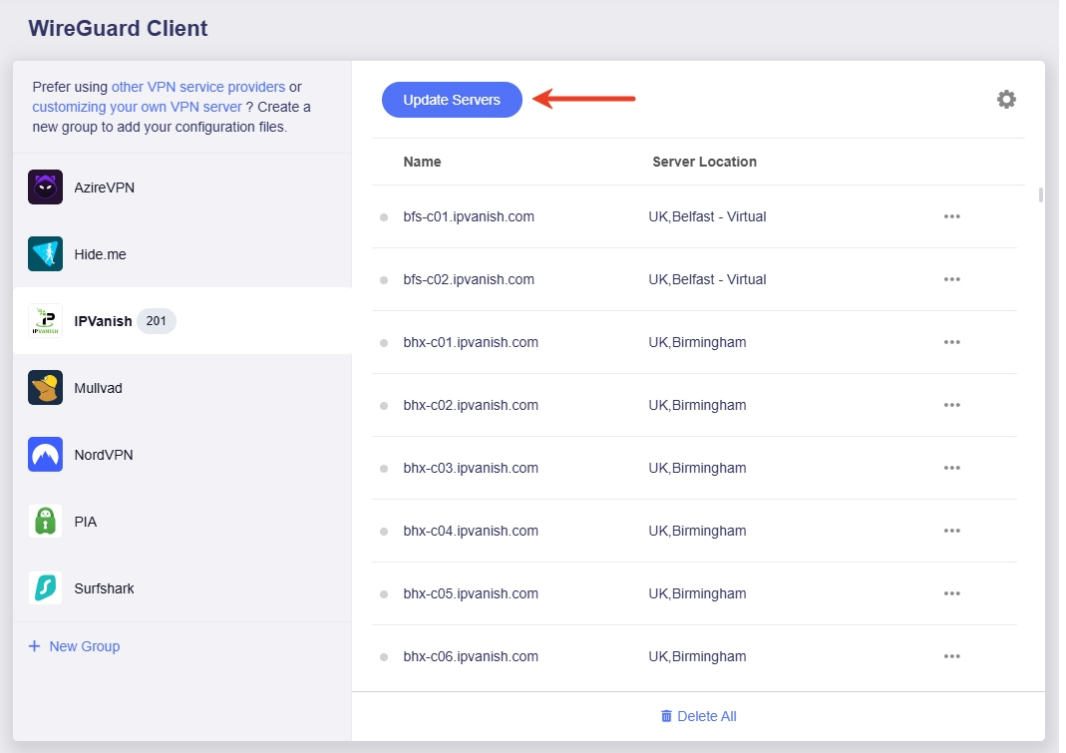
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



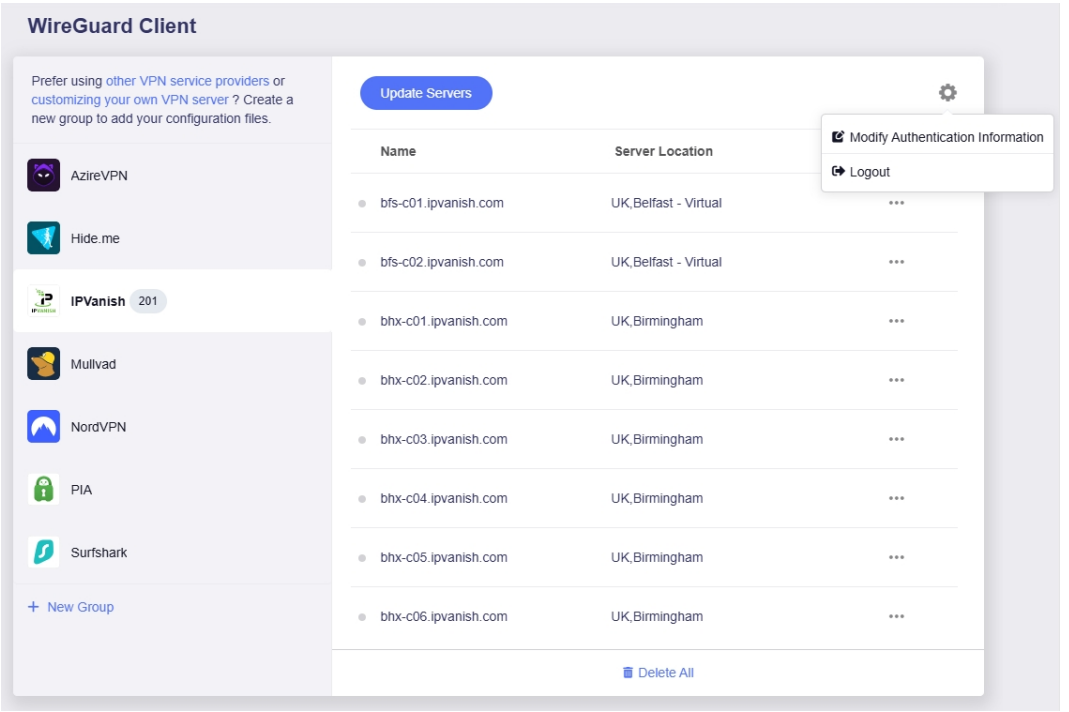
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

6. Server aktualisieren.

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

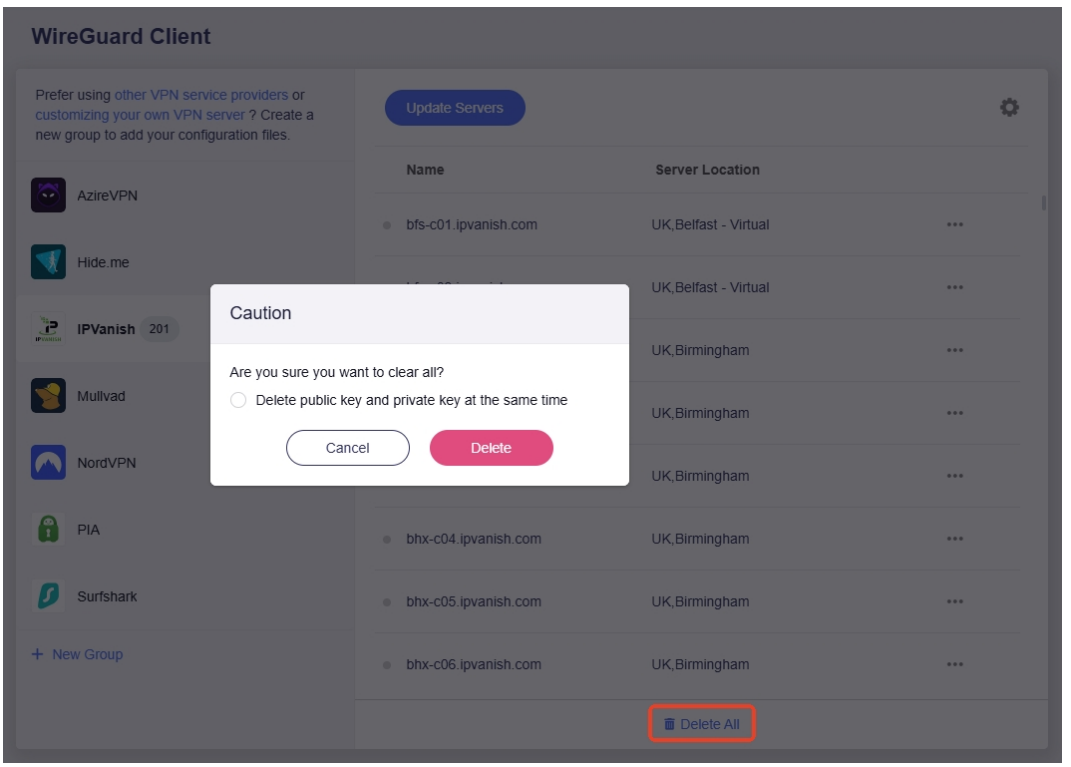


7. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



8. Alle Dateien löschen.

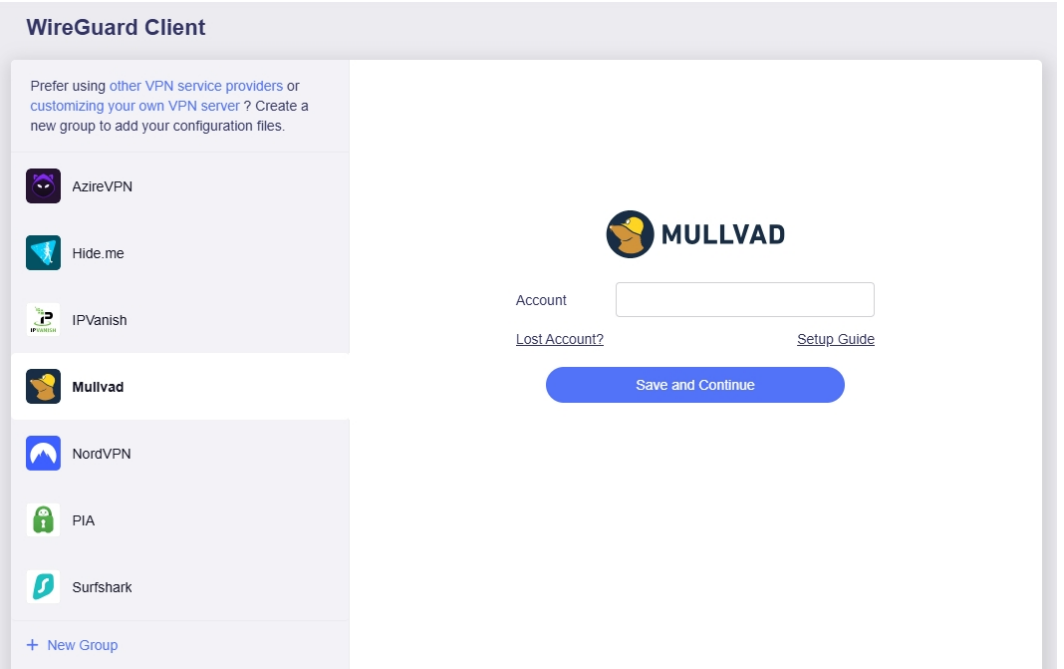
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



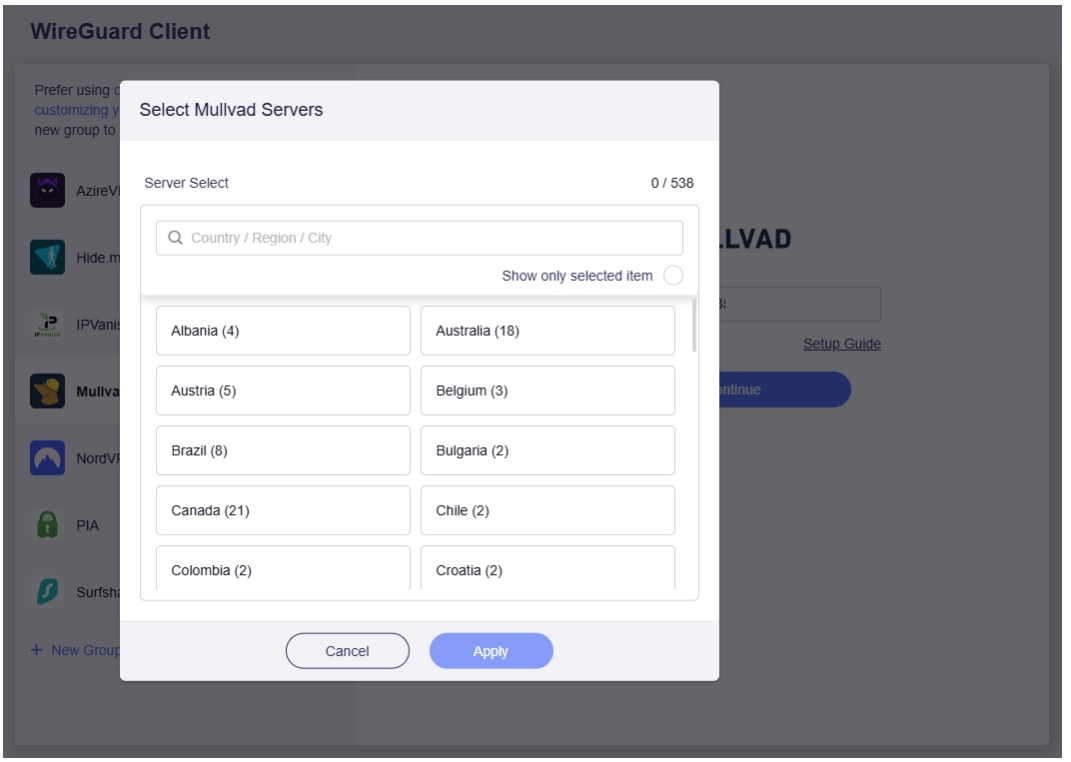
10.2.5 Mullvad einrichten

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

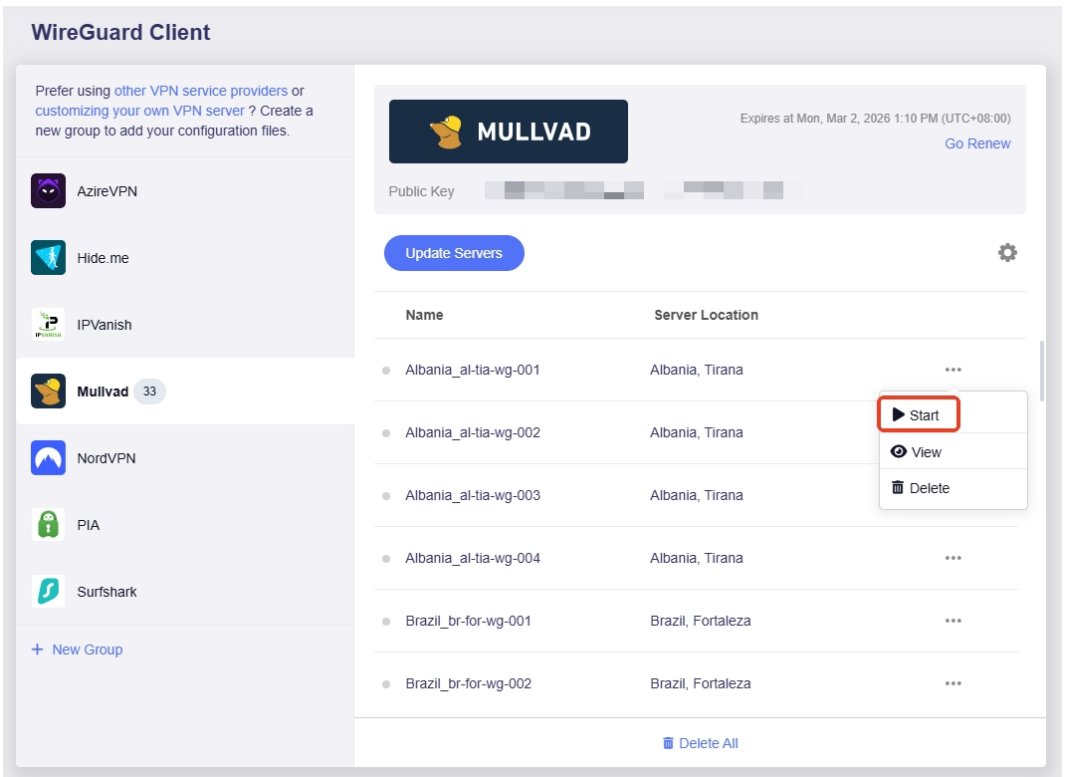
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Mullvad**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



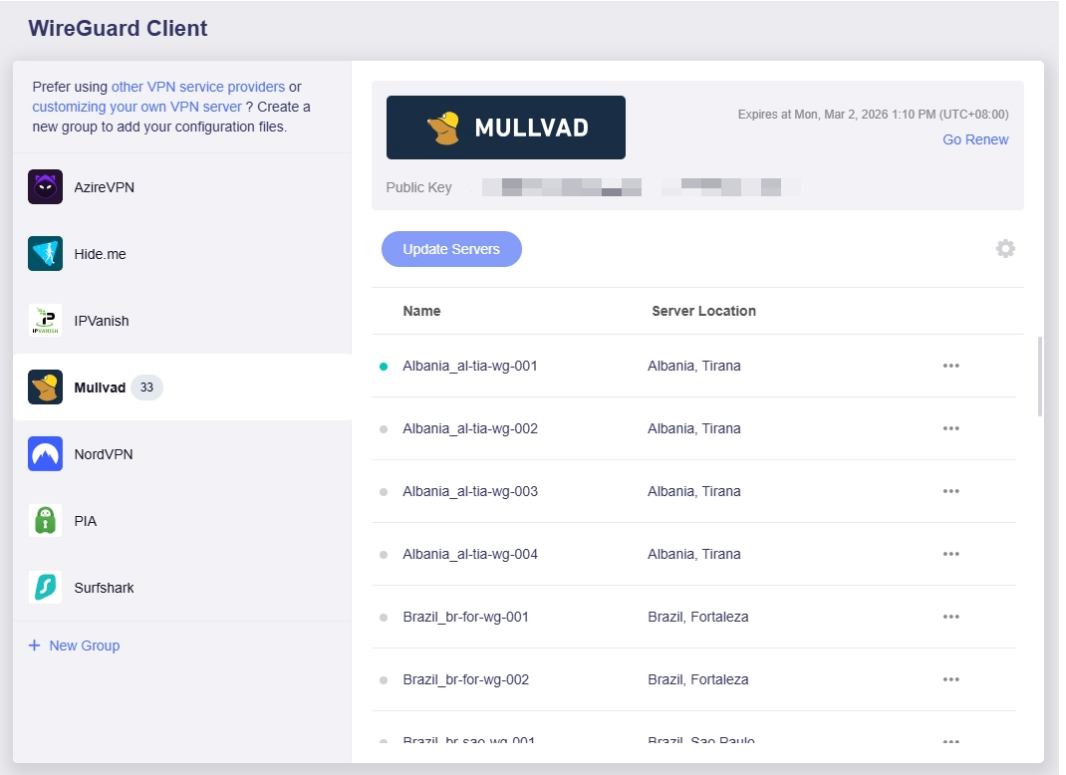
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



4. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



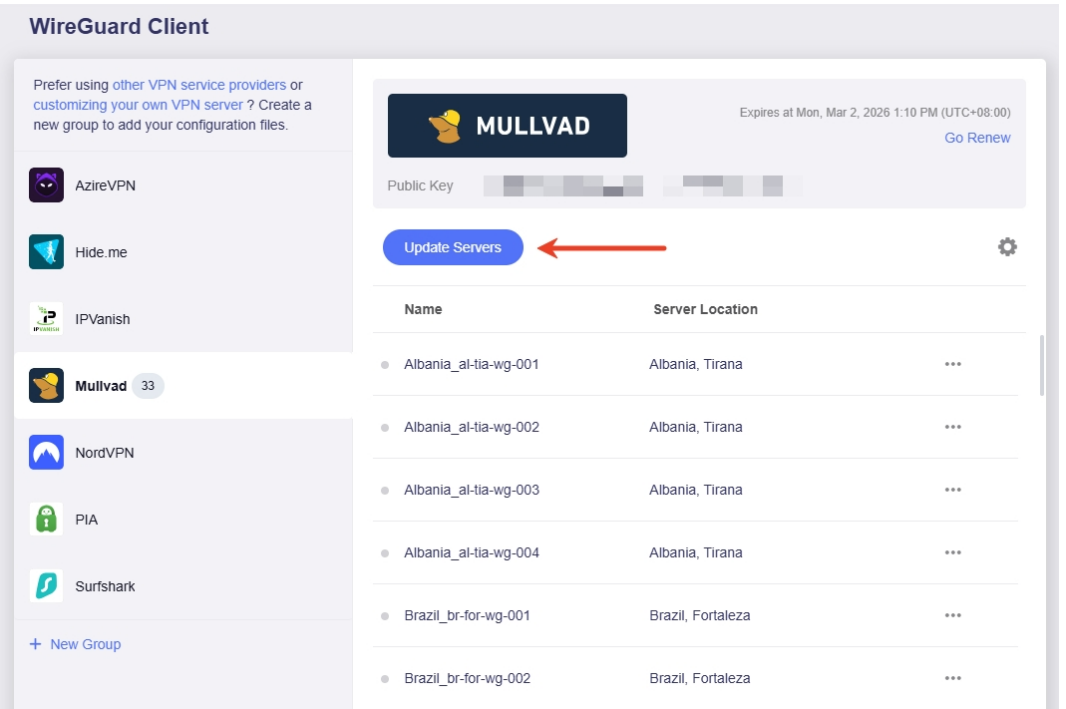
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

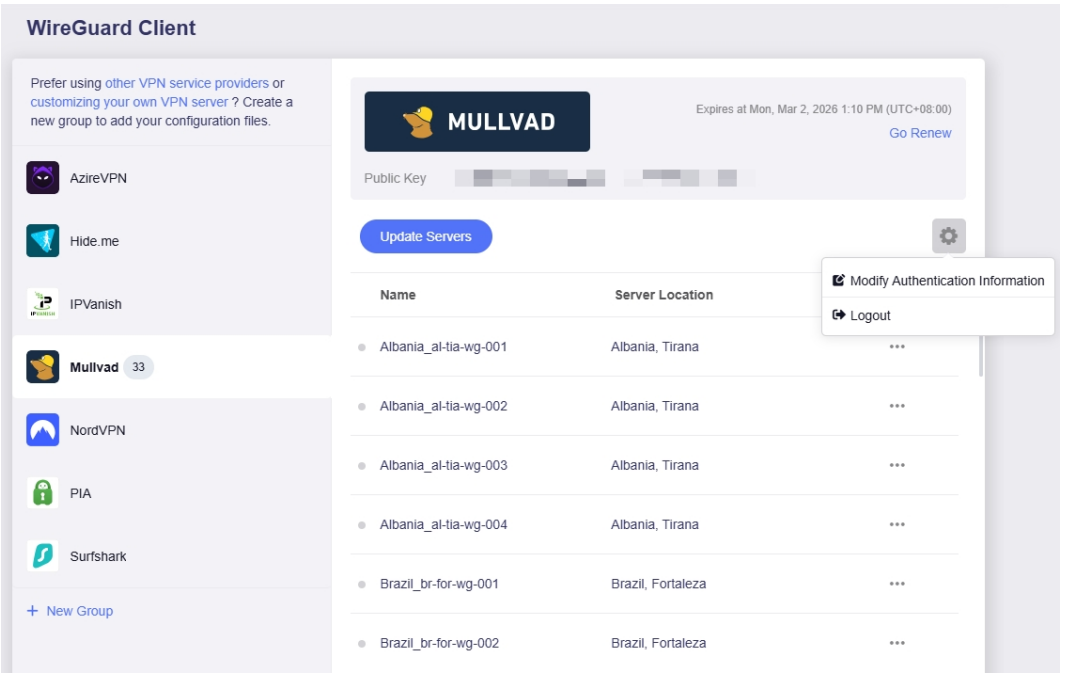
6. Server aktualisieren.

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



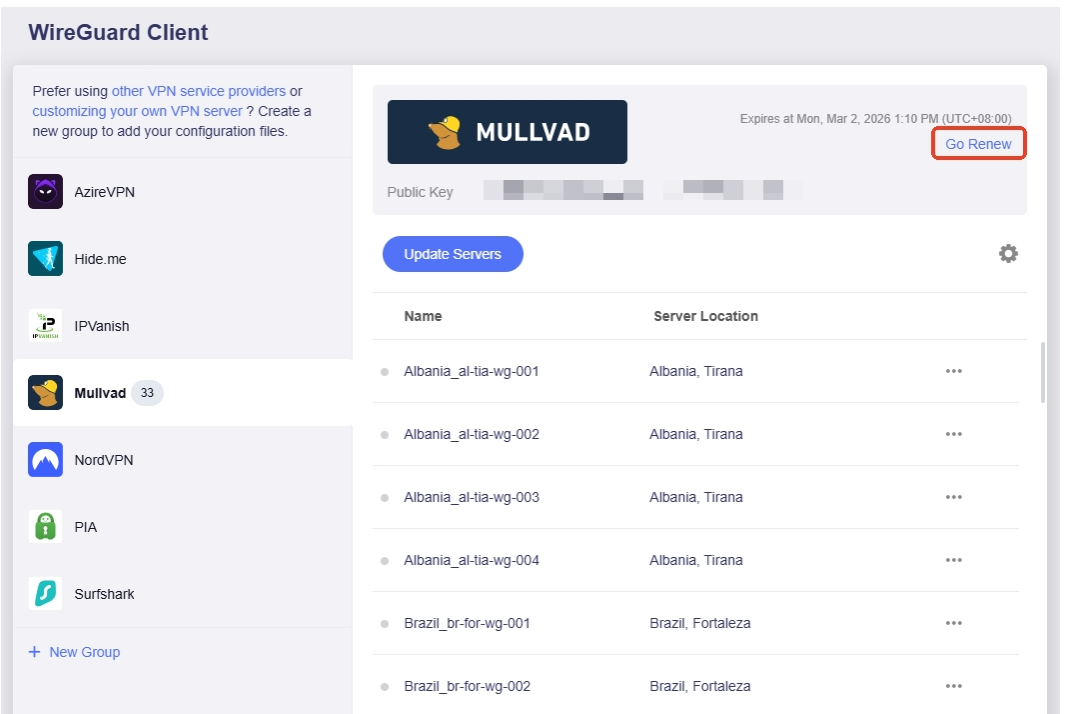
7. Zugangsdaten bearbeiten oder abmelden.

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



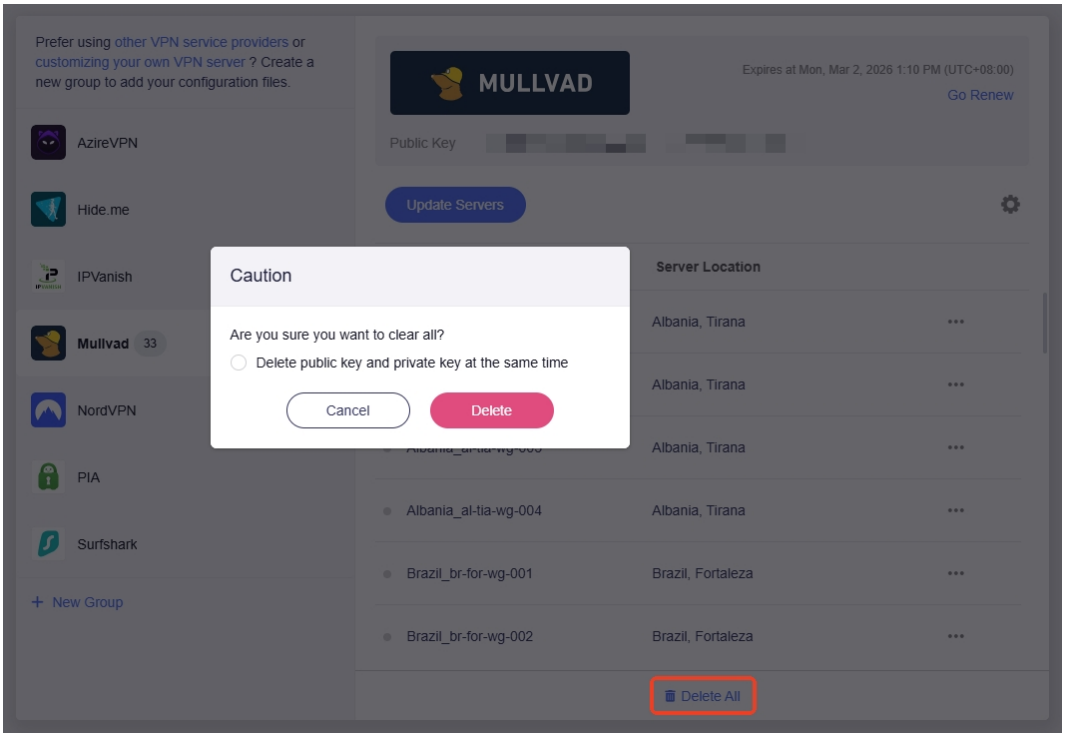
8. Abonnement verlängern.

   Wenn Sie auf **Go Renew** klicken, werden Sie zur offiziellen Website weitergeleitet, auf der Sie Ihr Abonnement verlängern können.



9. Alle Dateien löschen.

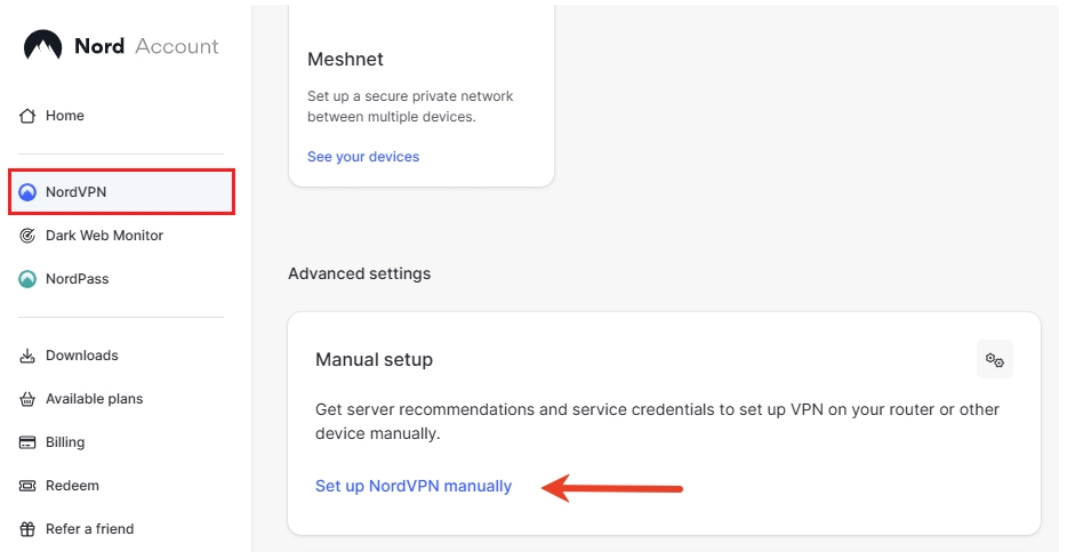
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



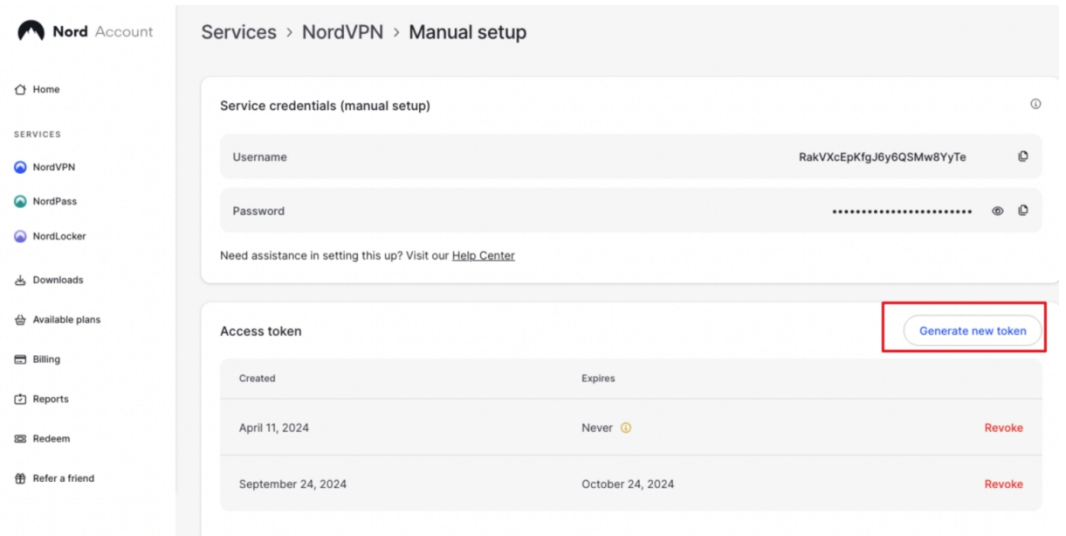
10.2.6 NordVPN einrichten

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

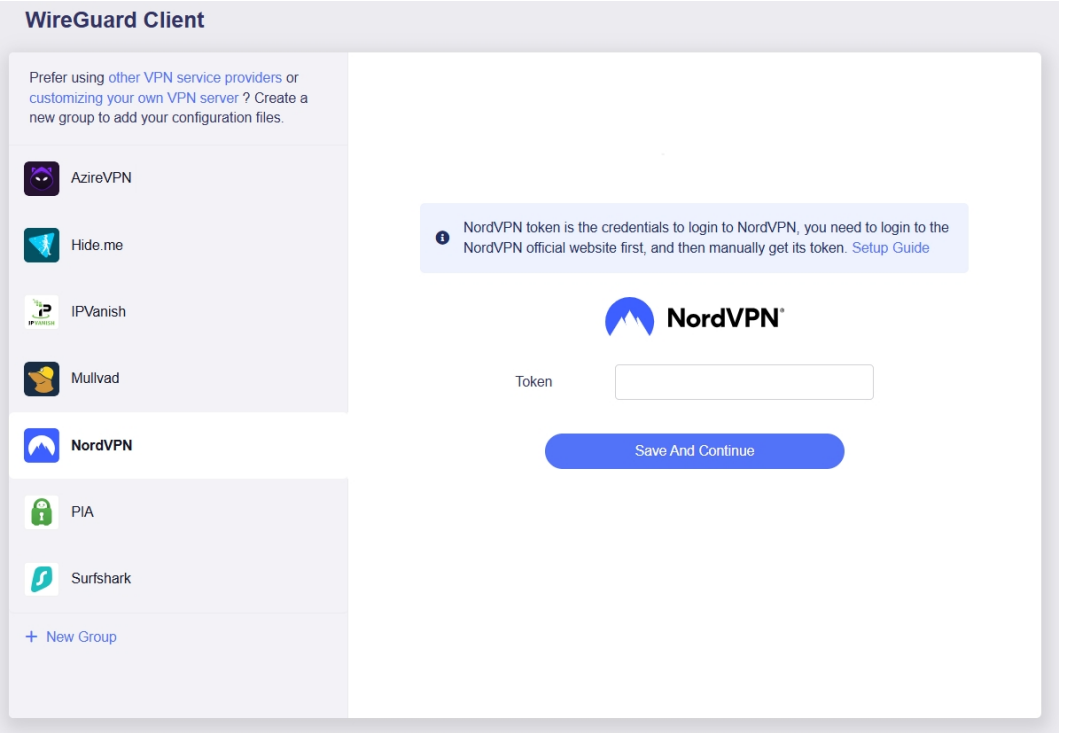
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



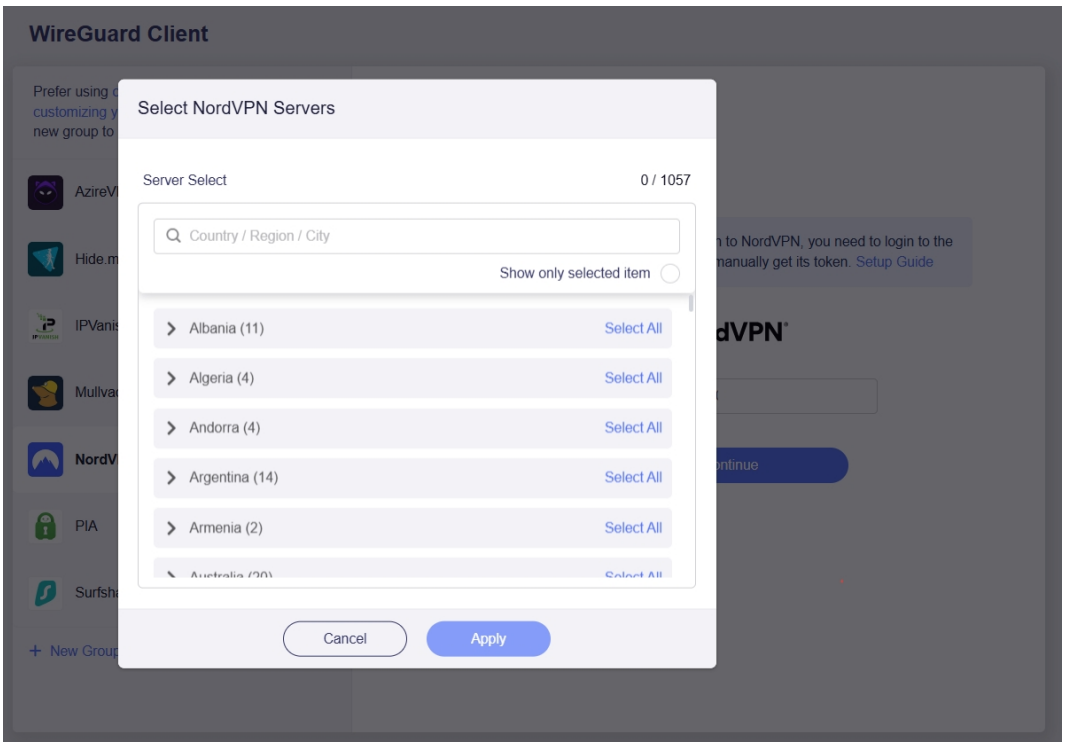
Dort finden Sie den Bereich **Access Token**. Erstellen Sie ein Zugriffstoken und kopieren Sie es zur späteren Verwendung.



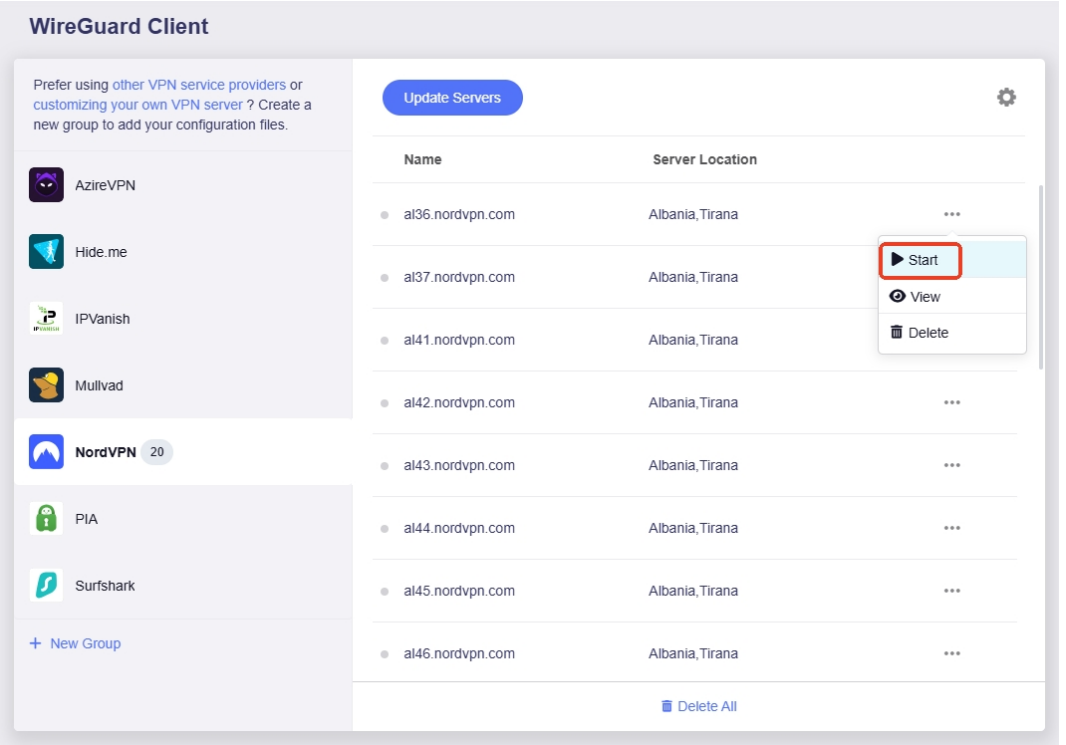
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **NordVPN**.
4. Geben Sie das Token ein und klicken Sie auf **Save and Continue**.



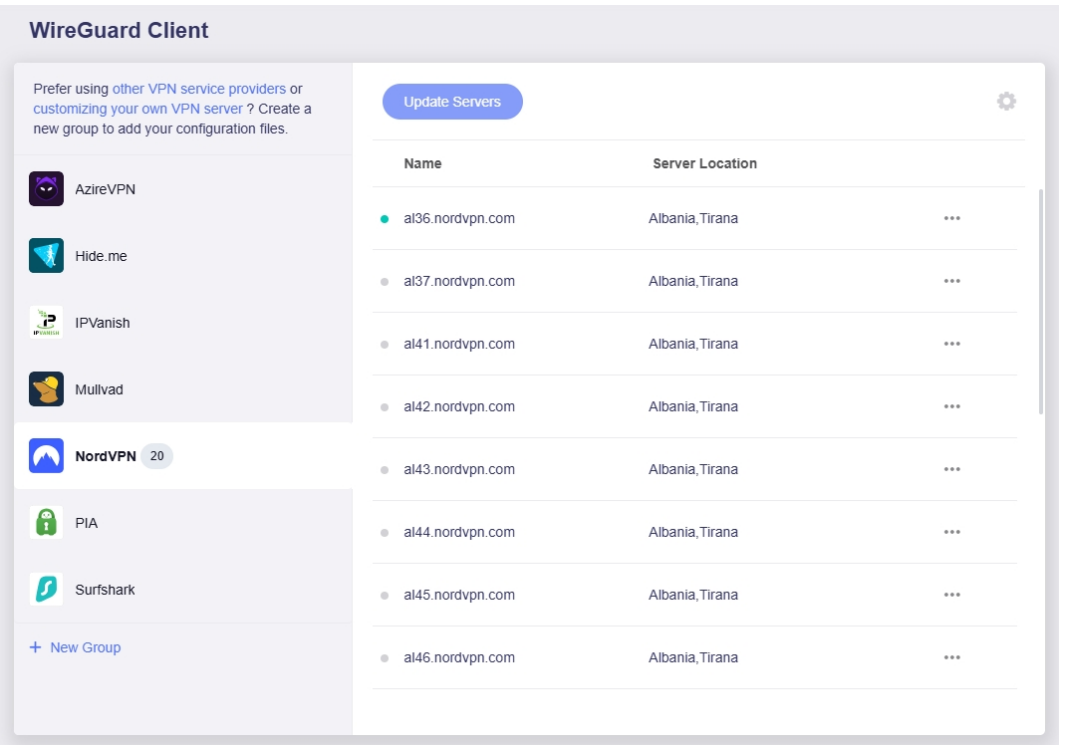
5. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



6. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



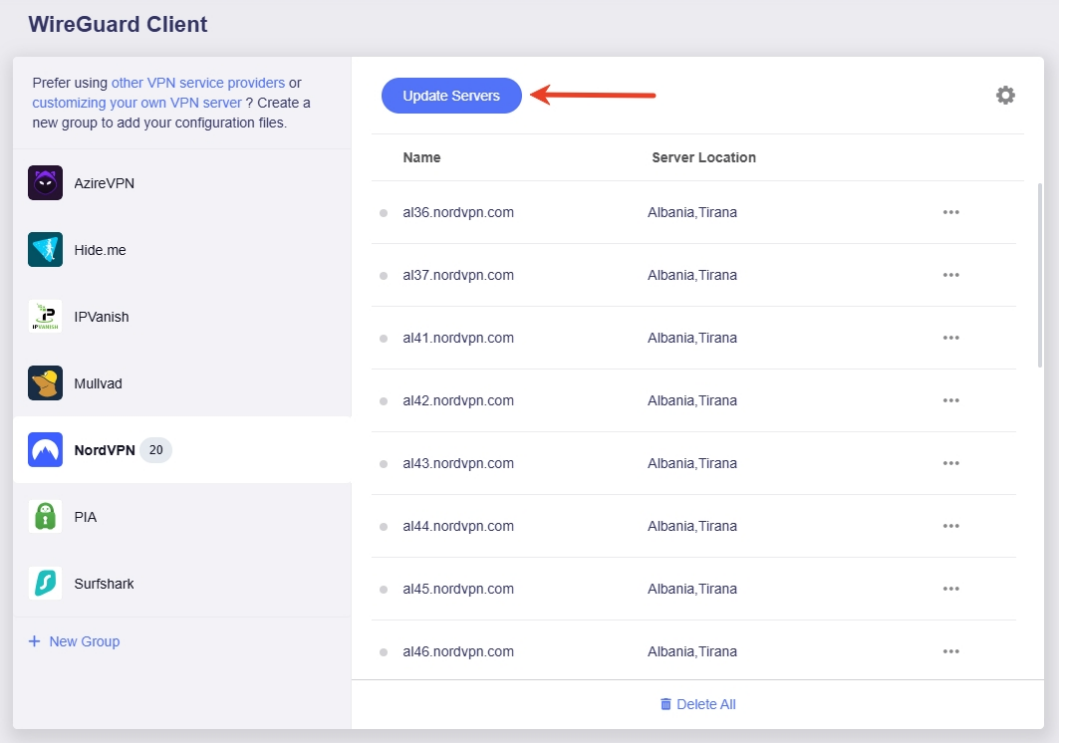
7. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



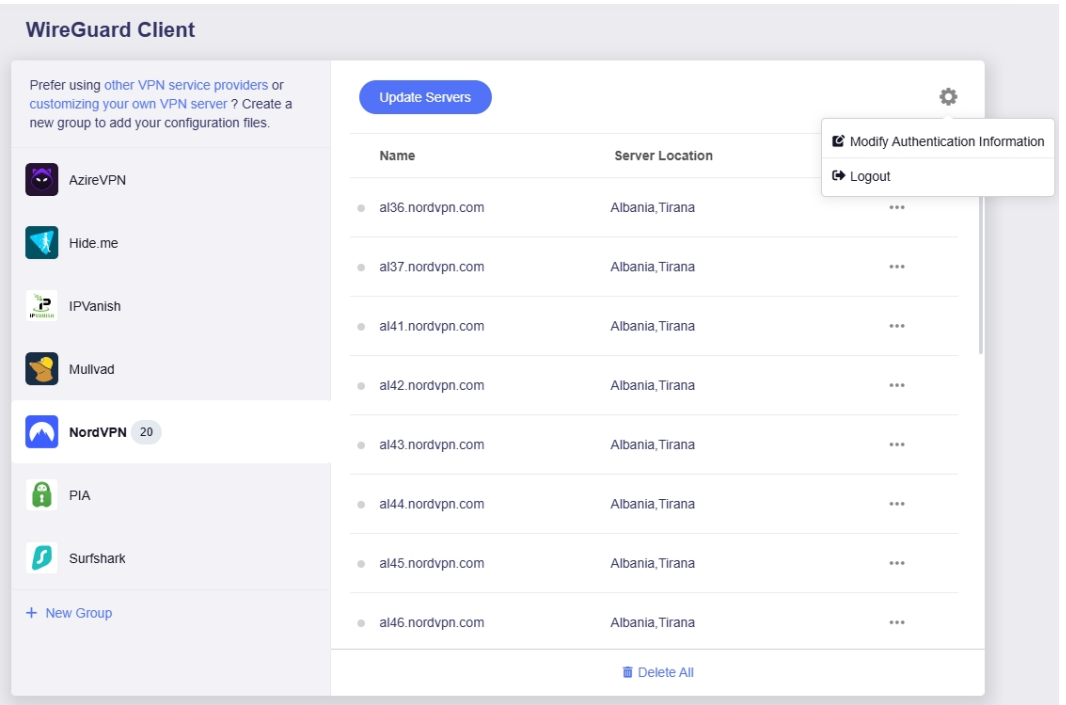
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

8. Server aktualisieren.

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

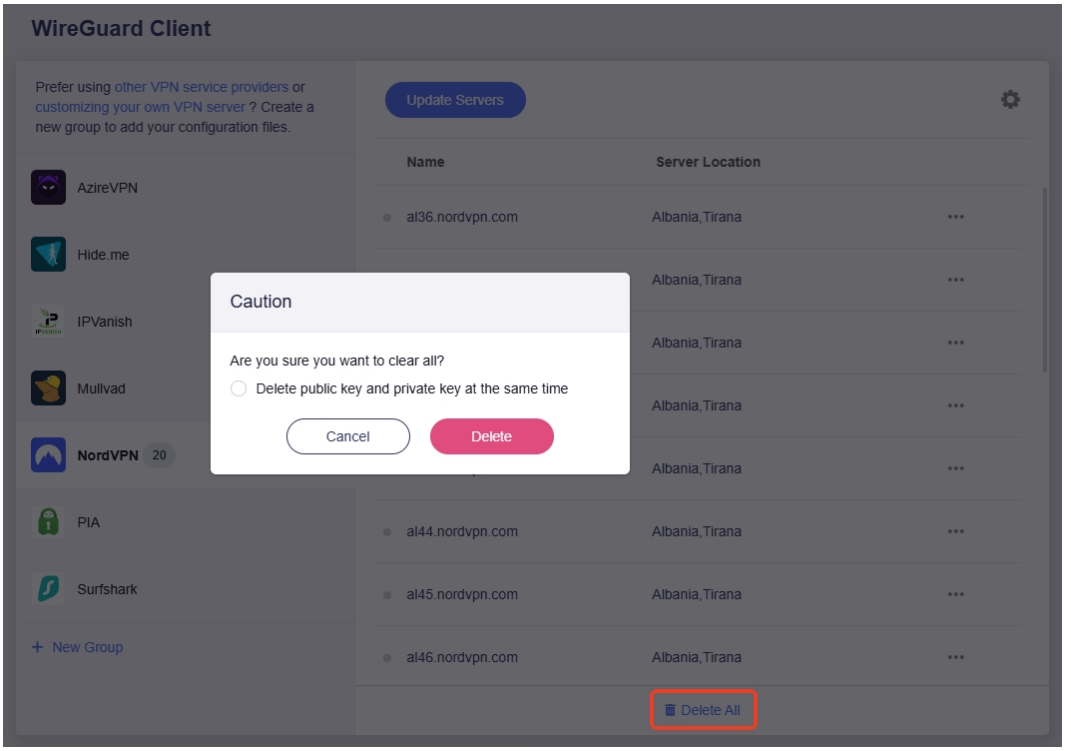


9. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



10. Alle Dateien löschen.

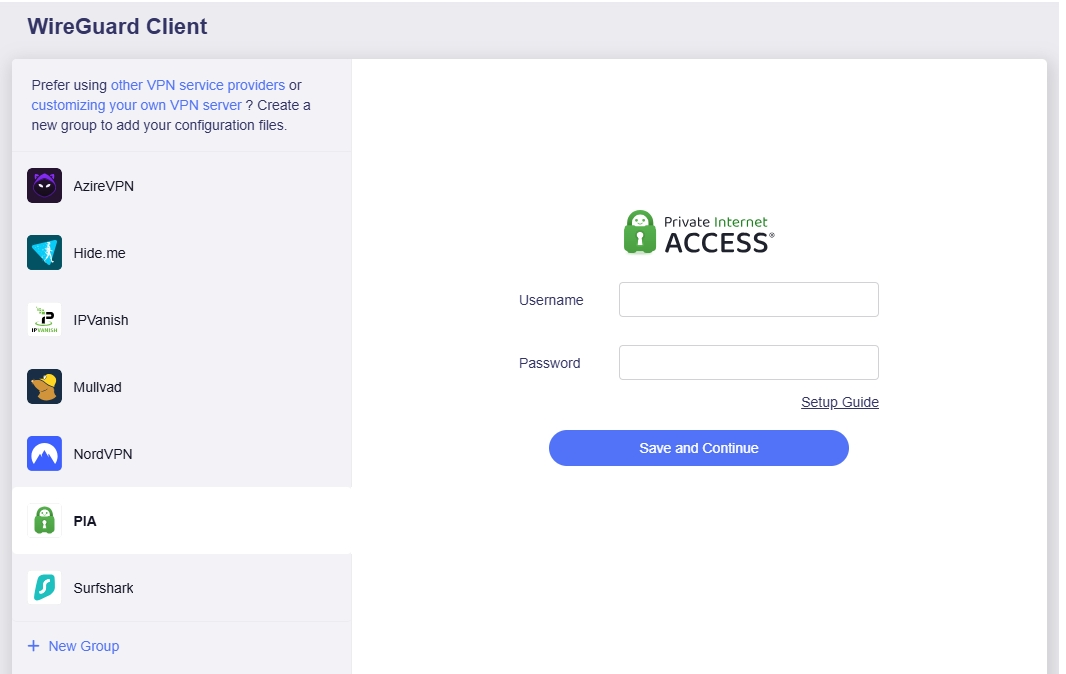
    Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



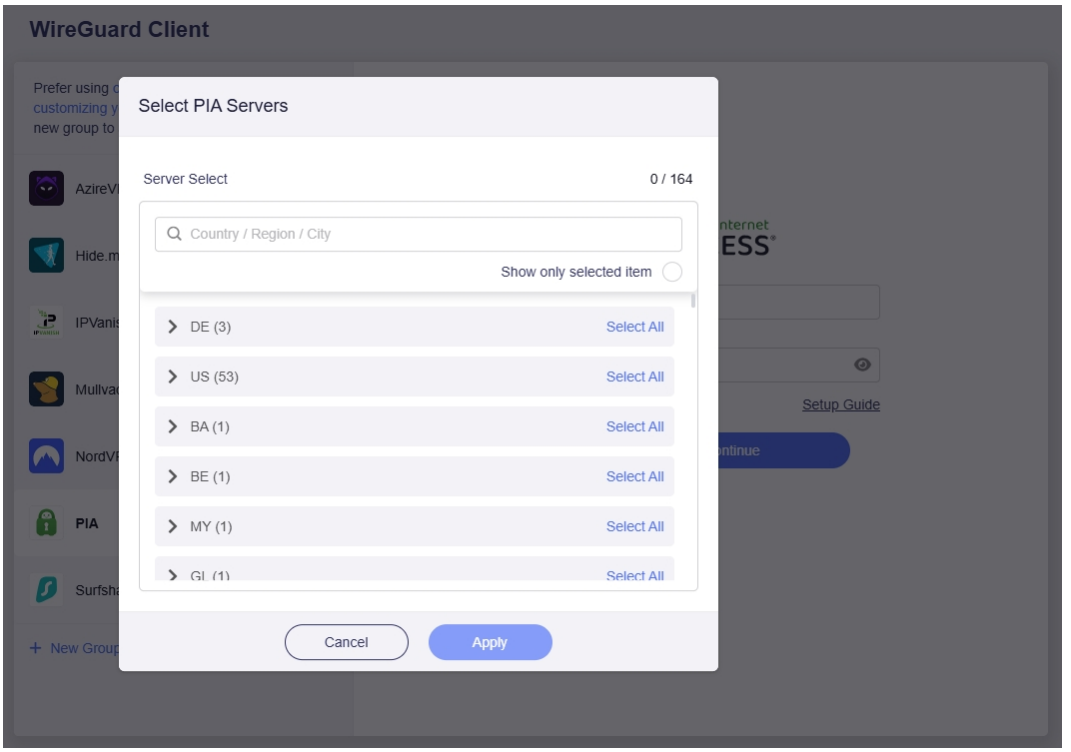
10.2.7 PIA (Private Internet Access) einrichten

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

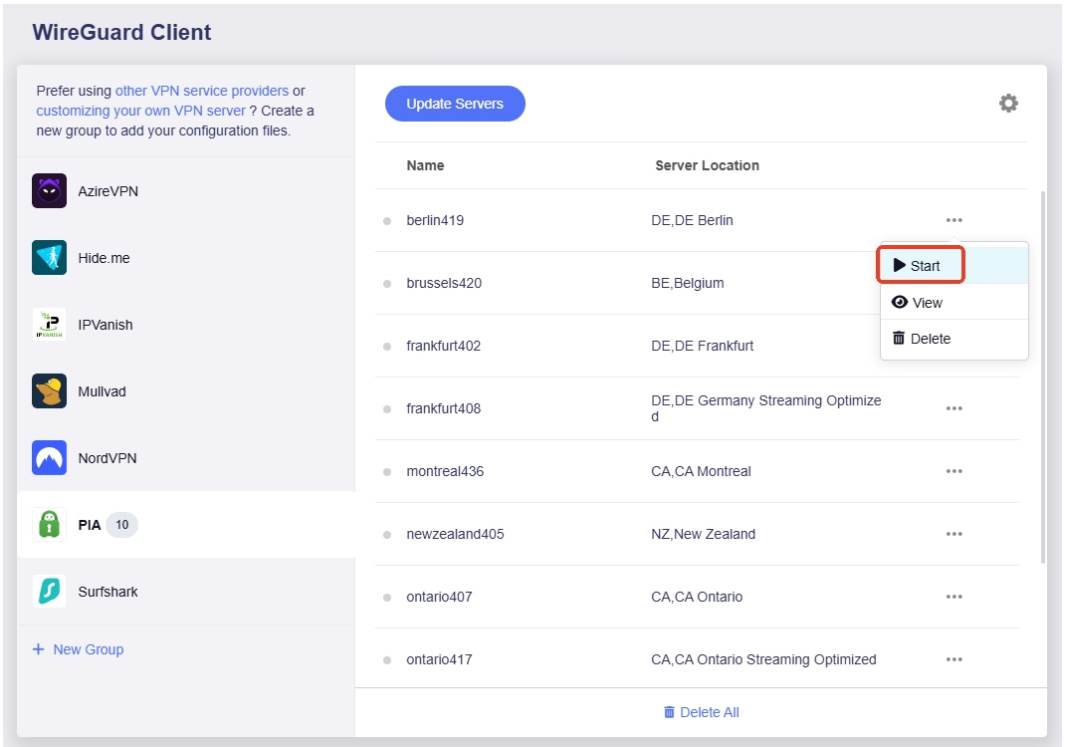
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **PIA**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



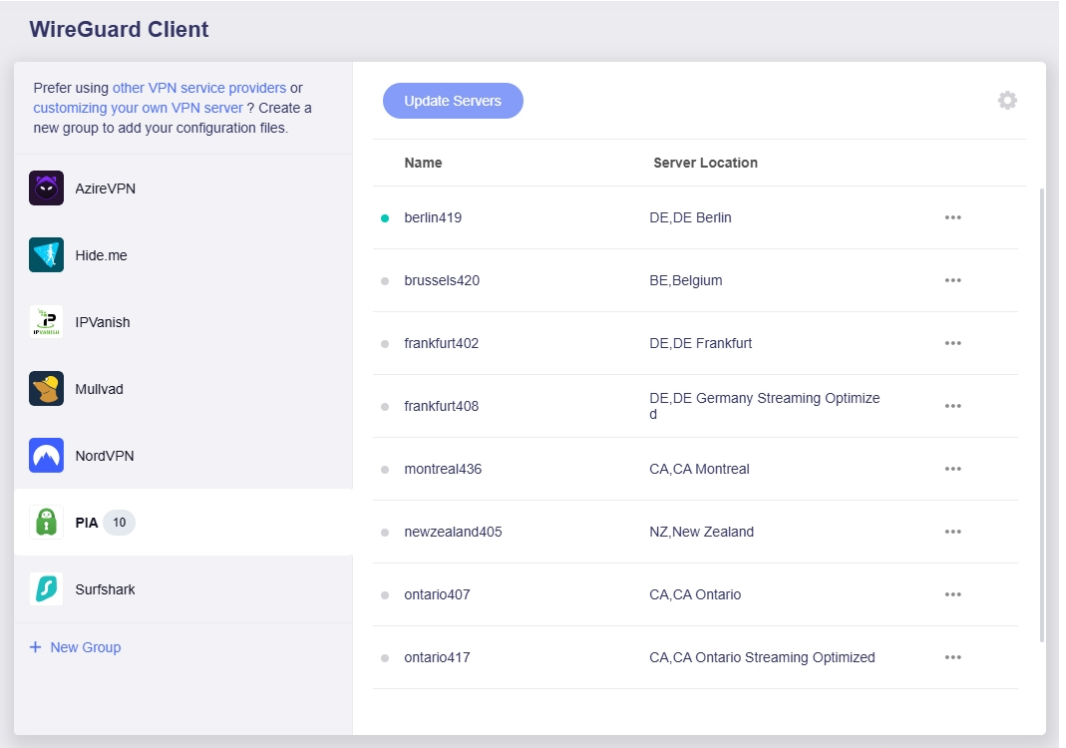
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



4. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.



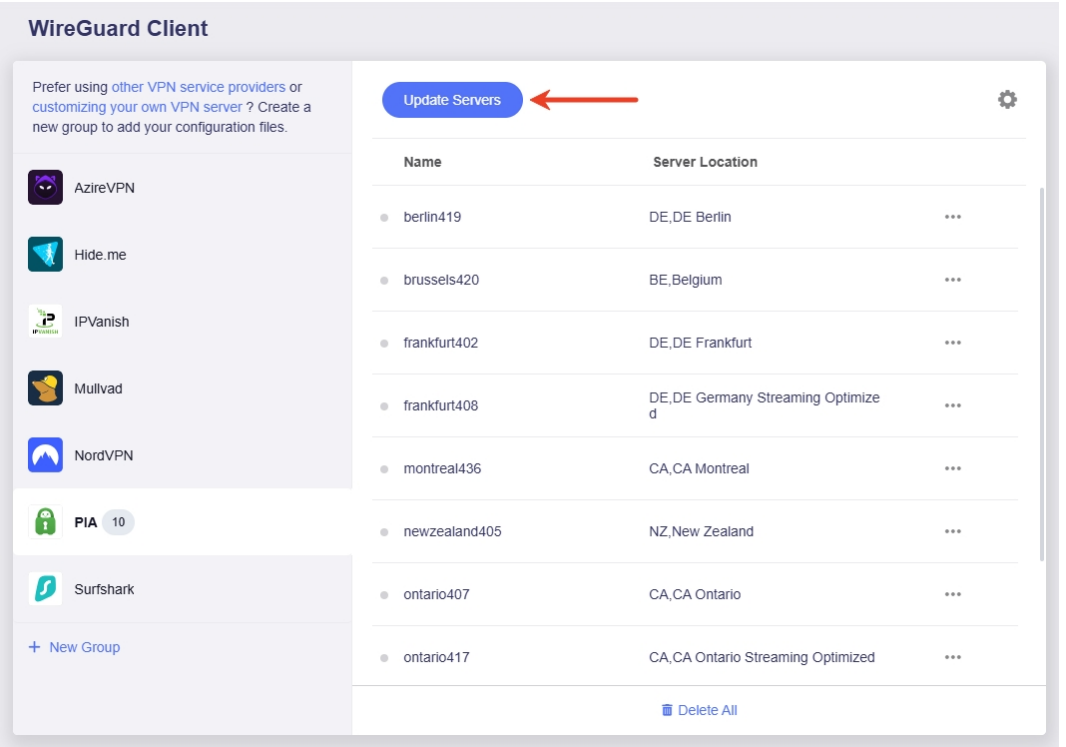
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



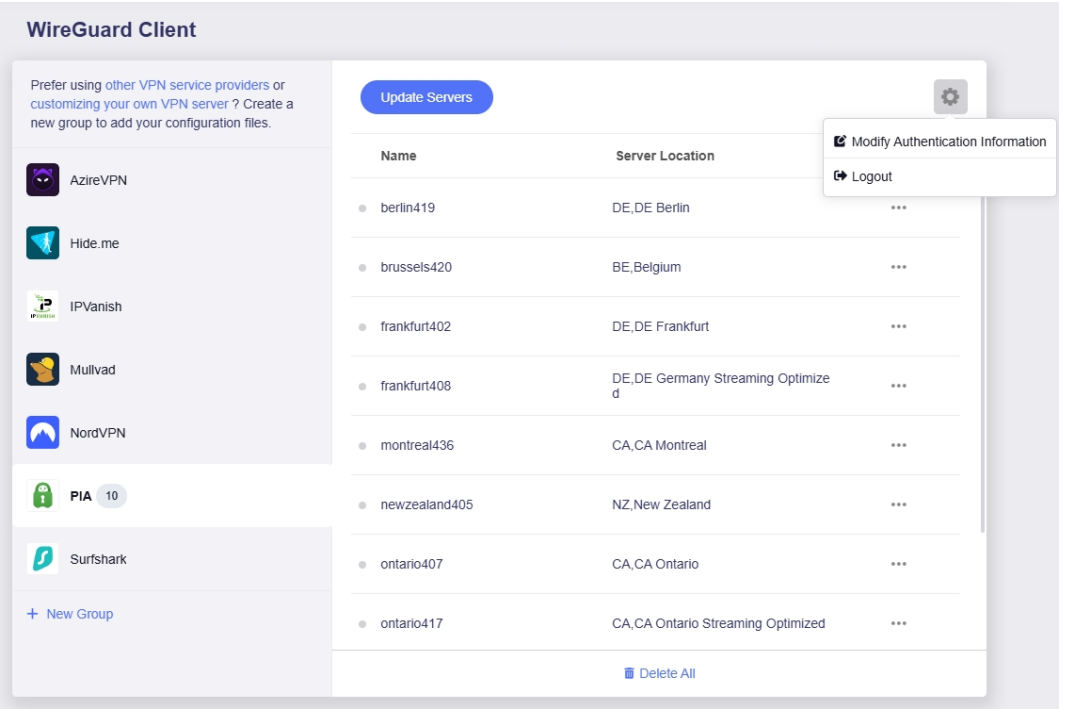
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

6. Server aktualisieren.

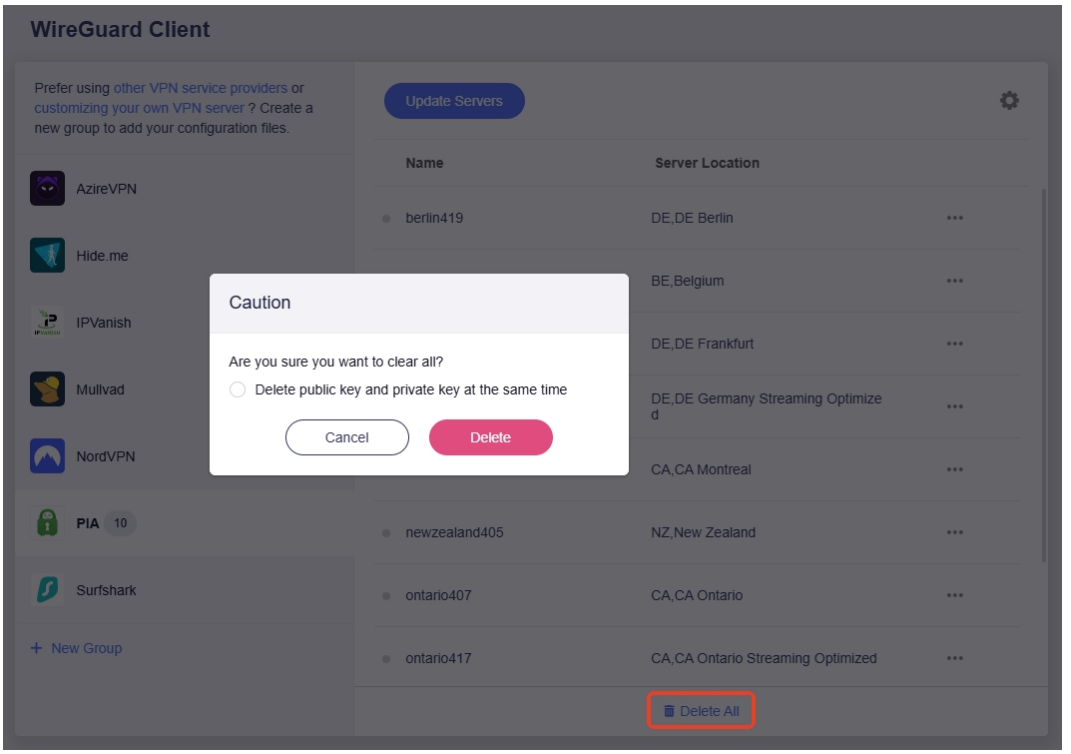
   Klicken Sie auf **Update Servers**, um die aktuelle Liste verfügbarer Server abzurufen. So vermeiden Sie Verbindungsfehler durch Serverwartung oder abgeschaltete Server.



7. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



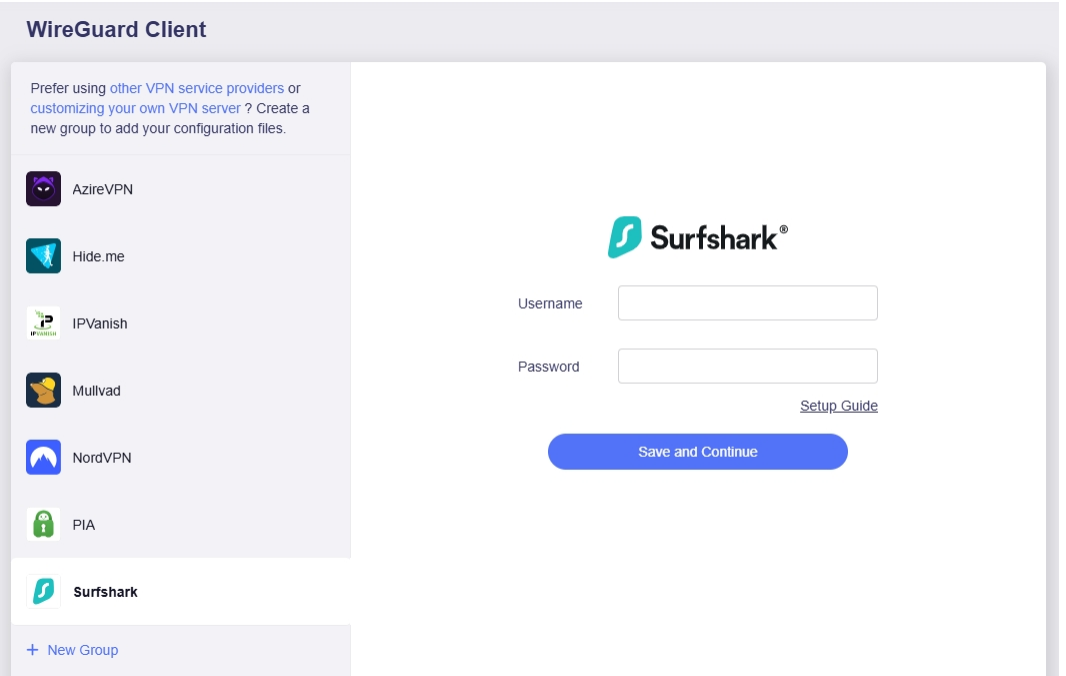
8. Alle Dateien löschen.
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
AzireVPN
Hide.me
IPVanish
Mullvad
NordVPN
PIA 10
Surfshark
New Group
Update Servers
Name
Server Location
berlin419
DE,DE Berlin
BE,Belgium
DE,DE Frankfurt
DE,DE Germany Streaming Optimized
CA,CA Montreal
newzealand405
NZ,New Zealand
ontario407
CA,CA Ontario
ontario417
CA,CA Ontario Streaming Optimized
Delete All
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete

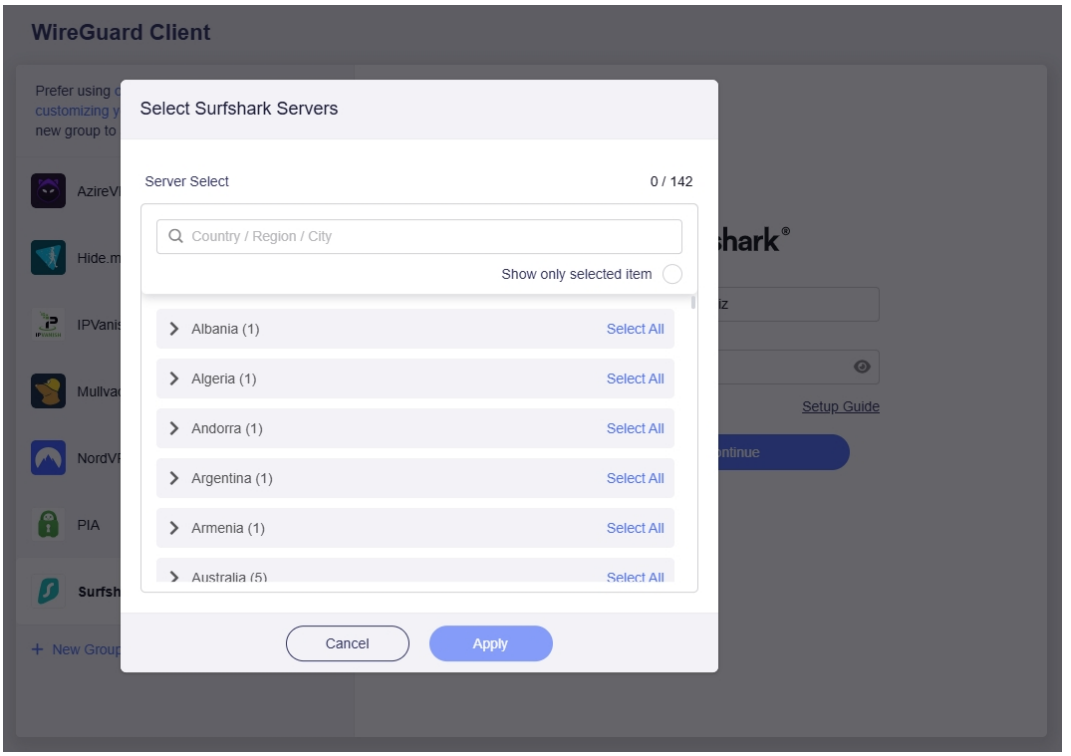
10.2.8 Surfshark einrichten

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

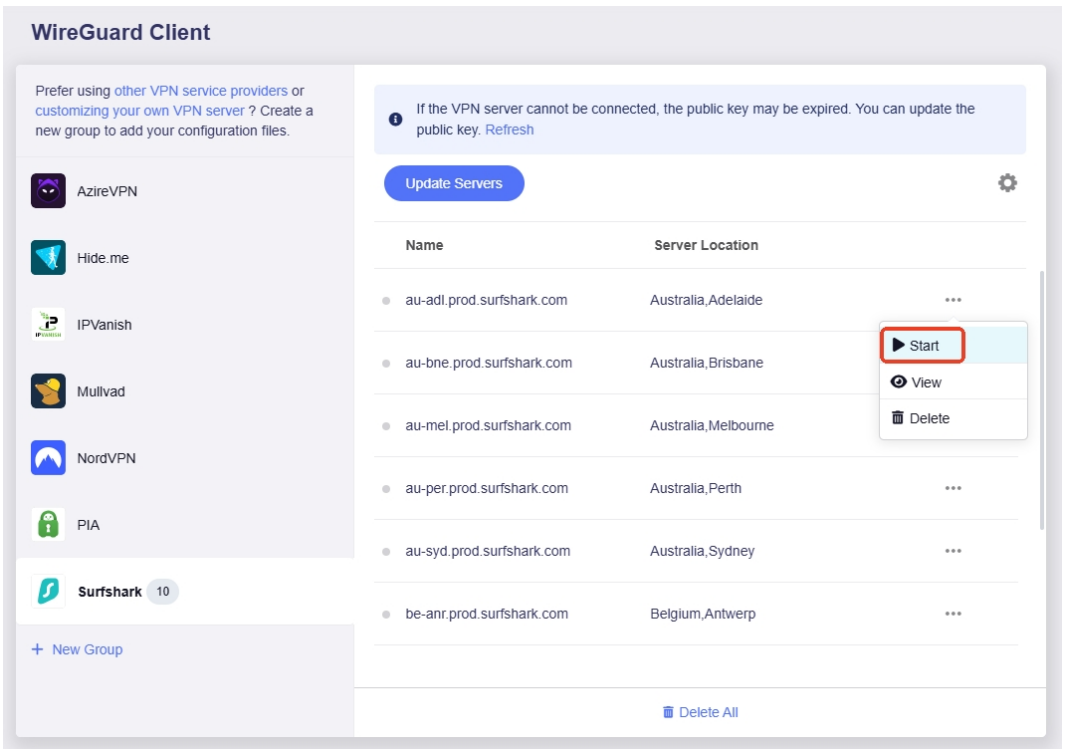
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Surfshark**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



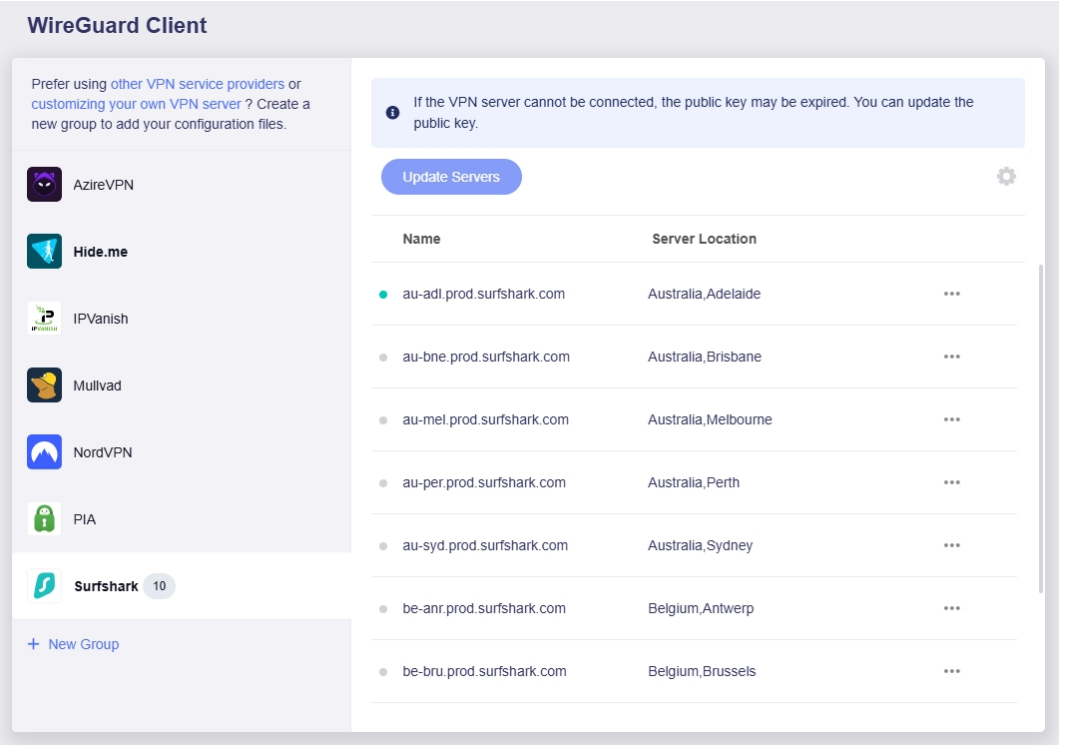
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



4. Wählen Sie den gewünschten Server aus und klicken Sie rechts auf das Dreipunktsymbol, um eine Verbindung herzustellen.

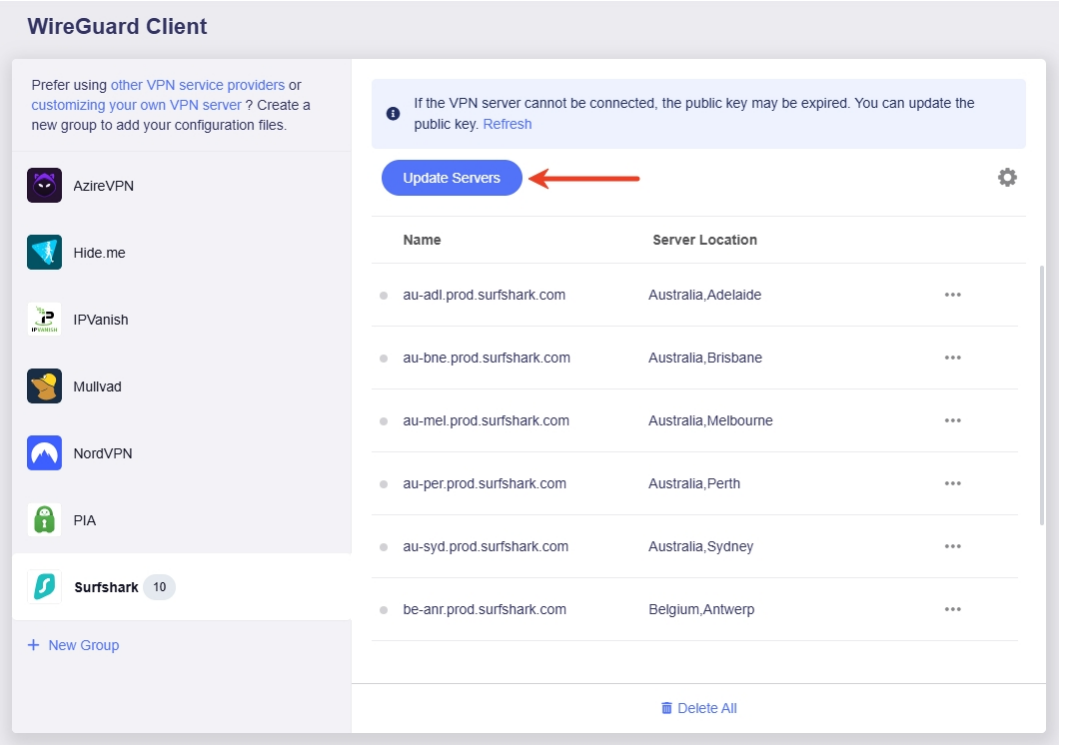


5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



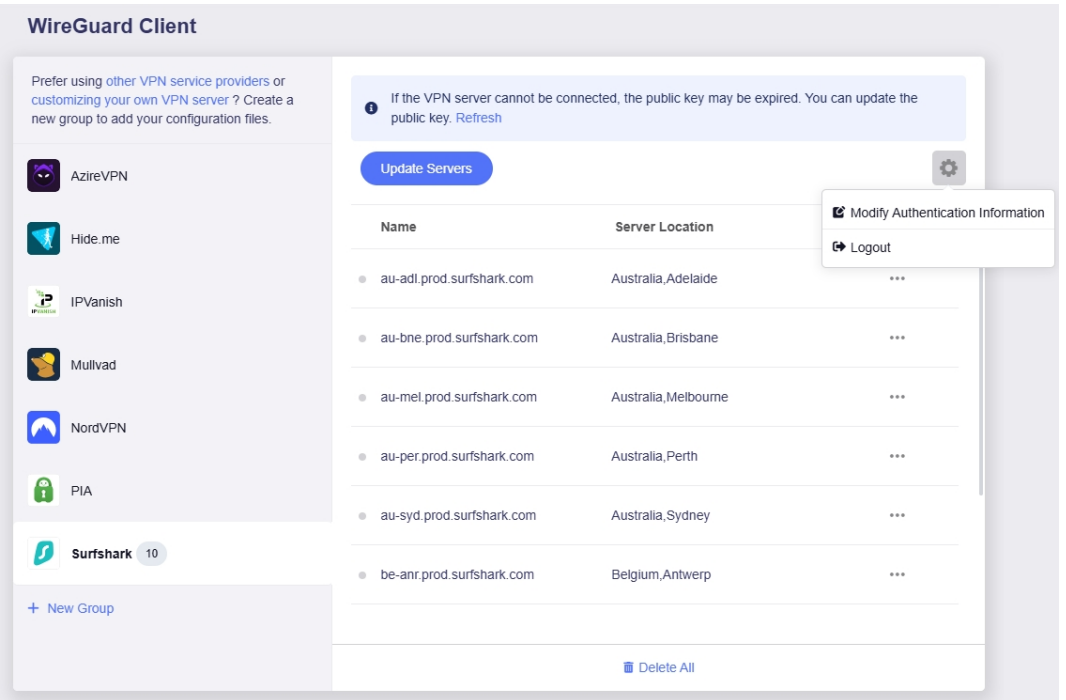
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

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



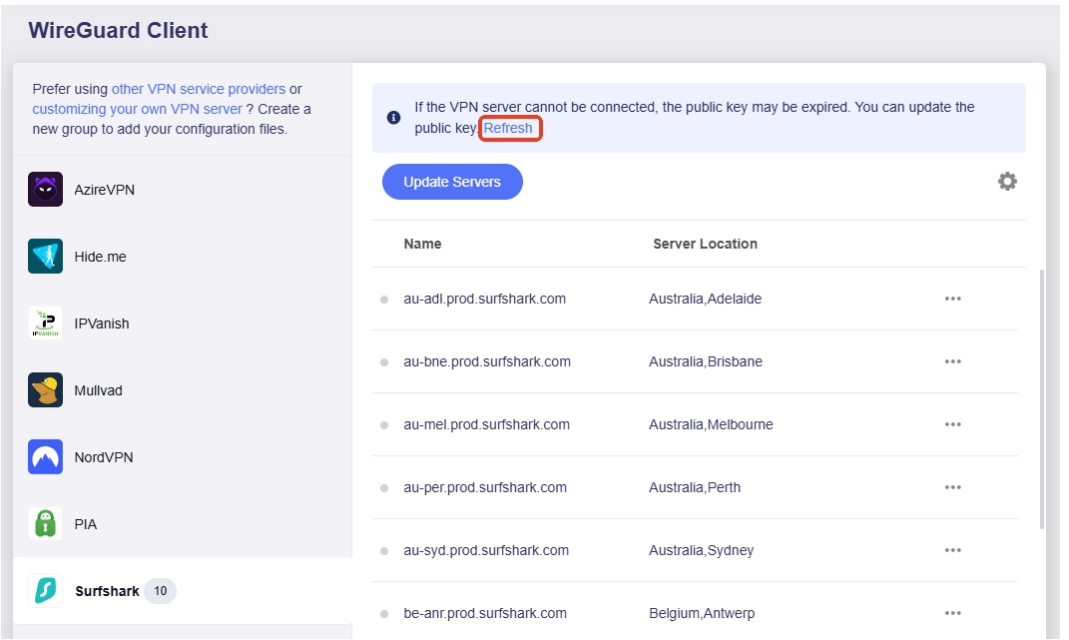
7. Zugangsdaten bearbeiten oder abmelden.

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



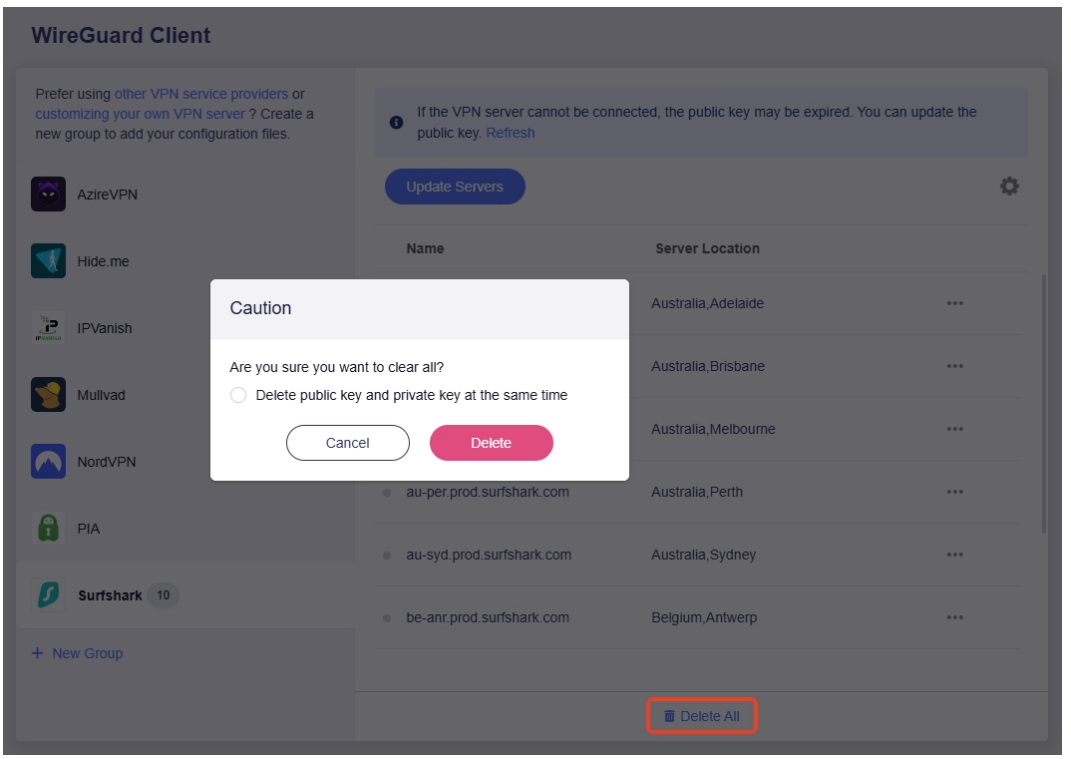
8. Aktualisieren.

Wenn keine Verbindung zum VPN-Server hergestellt werden kann, klicken Sie auf **Refresh**, um den öffentlichen Schlüssel zu aktualisieren.



9. Alle Dateien löschen.

   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.

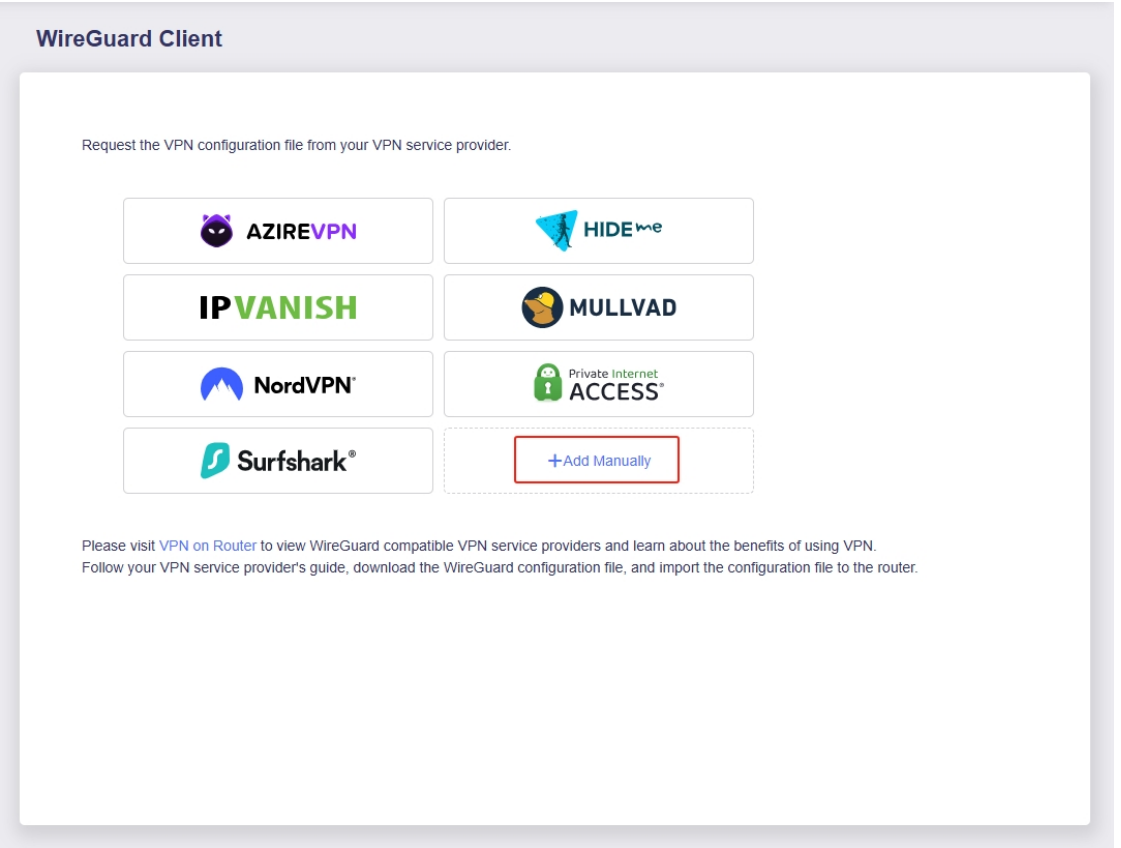


10.2.9 WireGuard-Client manuell einrichten (andere Anbieter)

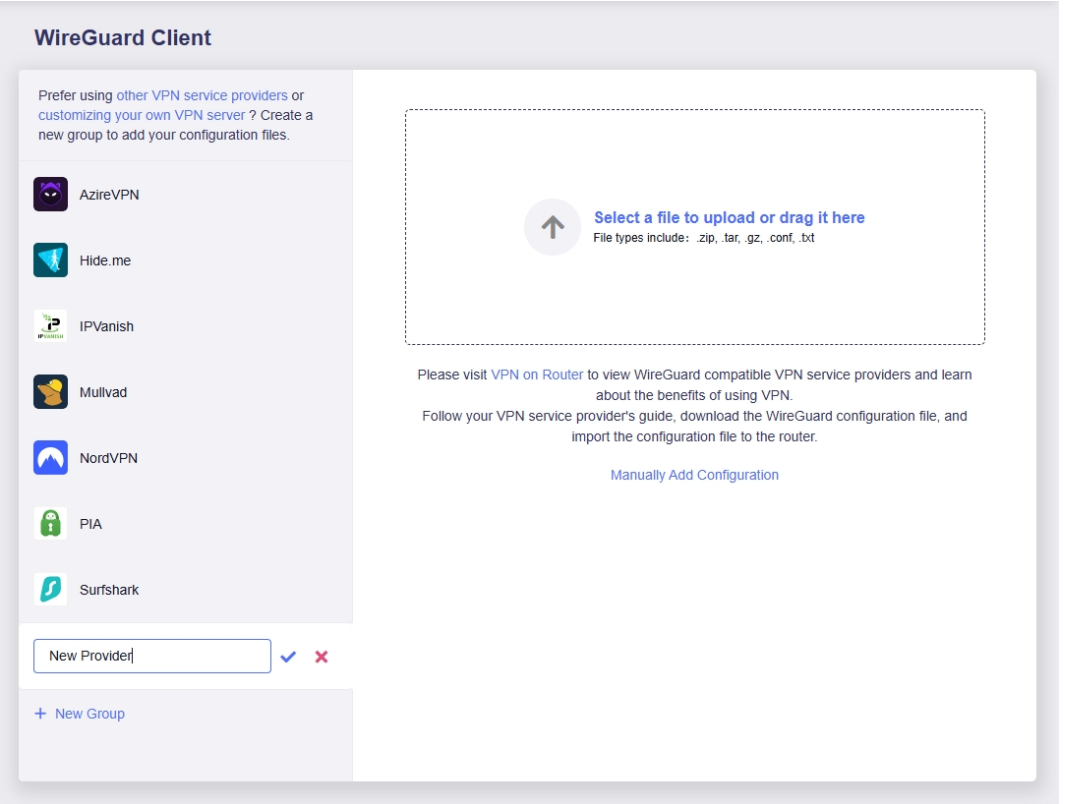
Wenn Ihr WireGuard-Anbieter nicht in die Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den WireGuard-Client einzurichten. Falls Sie nicht wissen, wie Sie die Dateien herunterladen,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

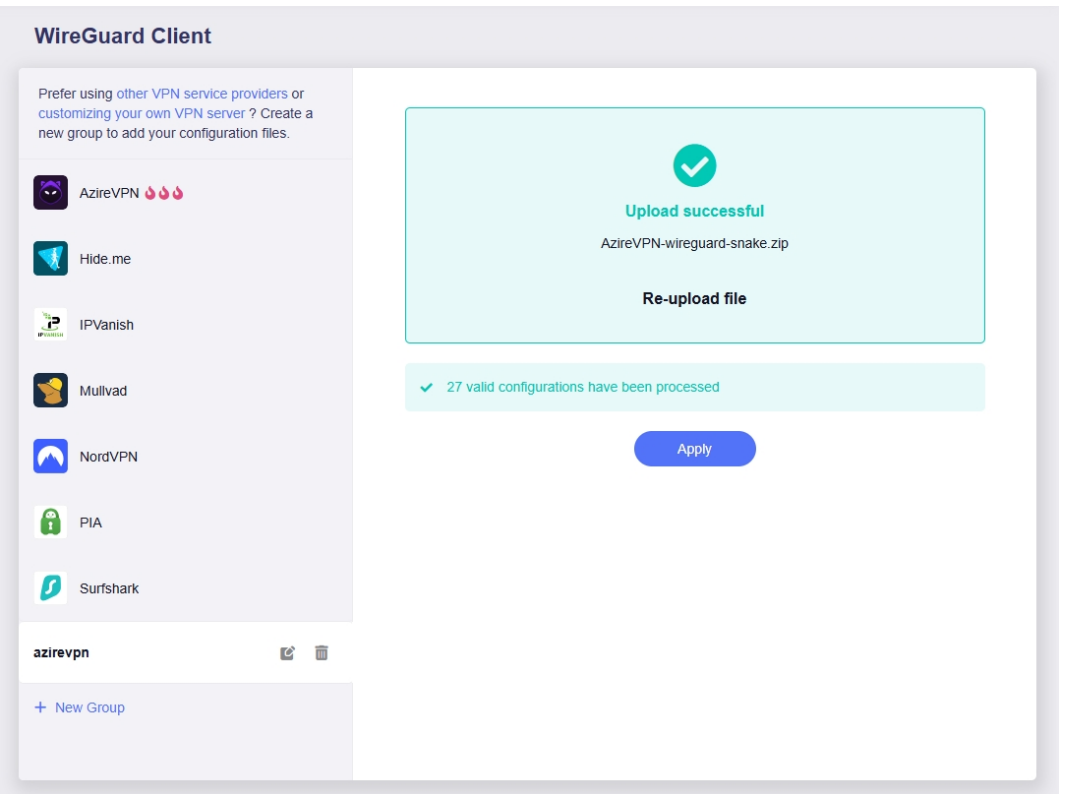
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Add Manually**.



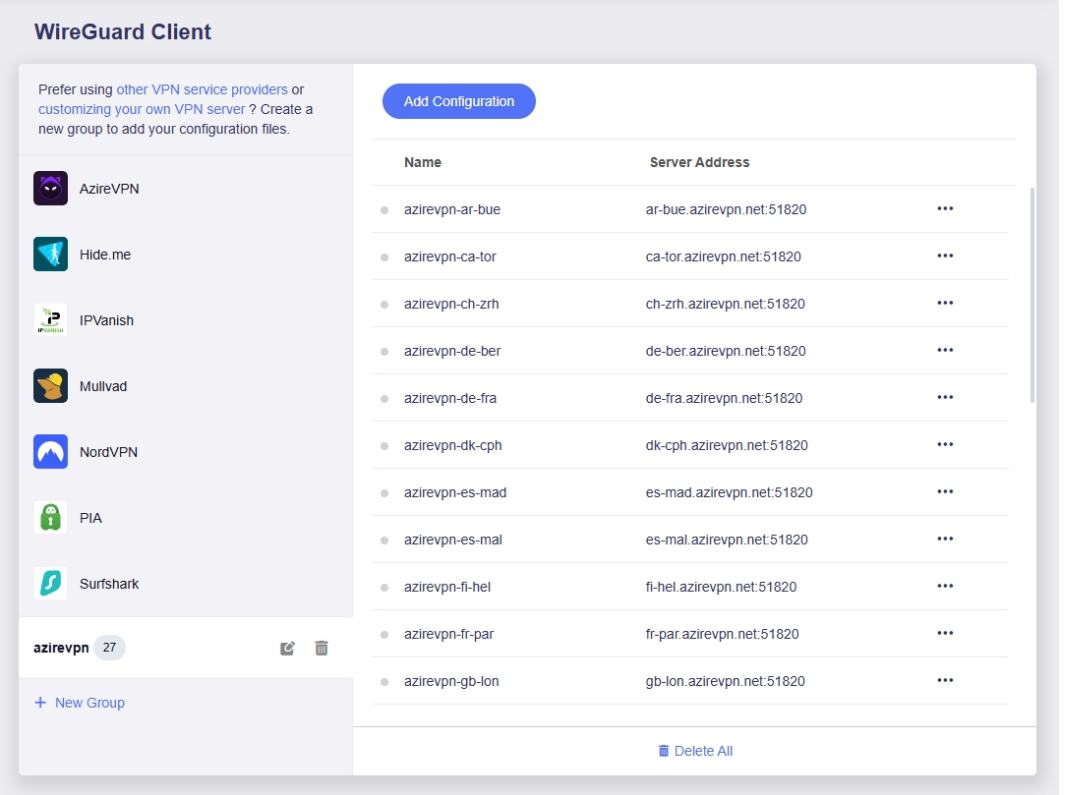
2. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



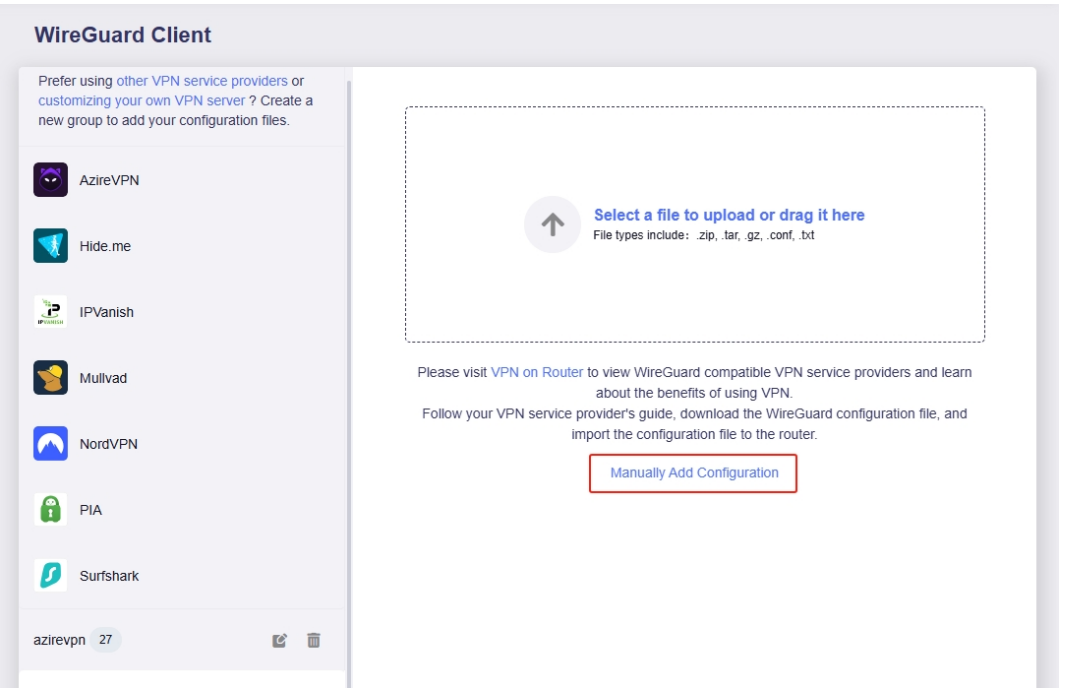
3. Klicken Sie auf den Upload-Bereich, laden Sie Ihre WireGuard-Konfigurationsdatei hoch und klicken Sie auf **Apply**. Unterstützte Formate: zip, tar, gz, conf und txt.

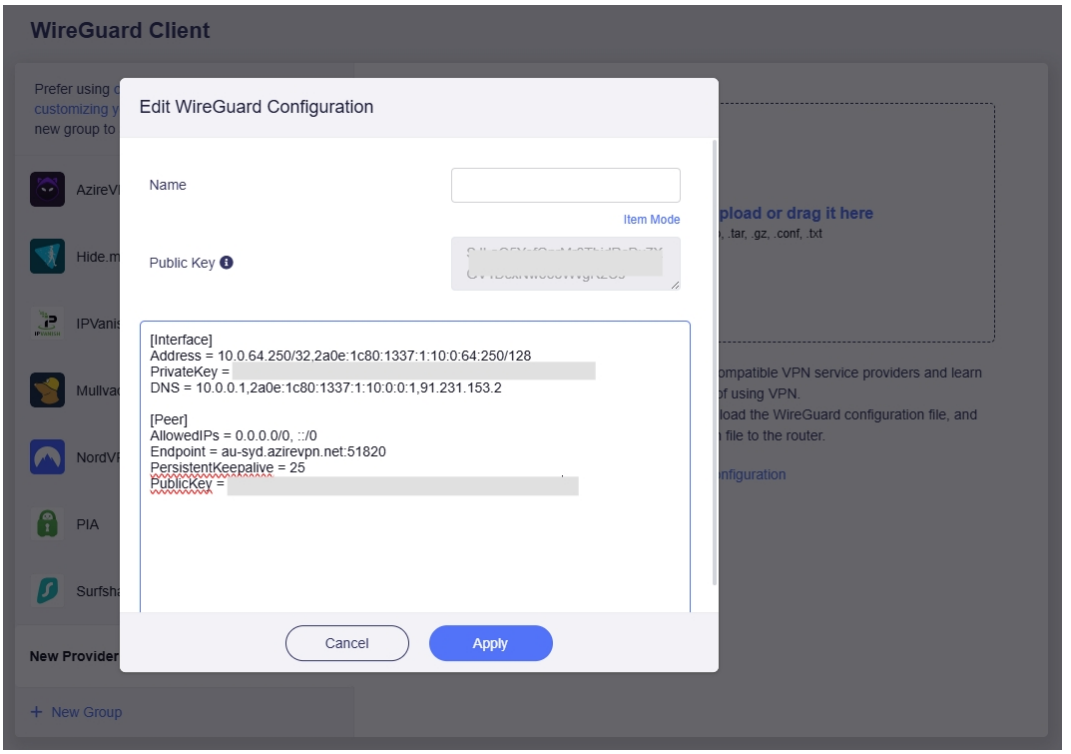


Wenn Sie eine komprimierte Datei mit mehreren Konfigurationsdateien hochladen, wird sie wie unten gezeigt automatisch entpackt.

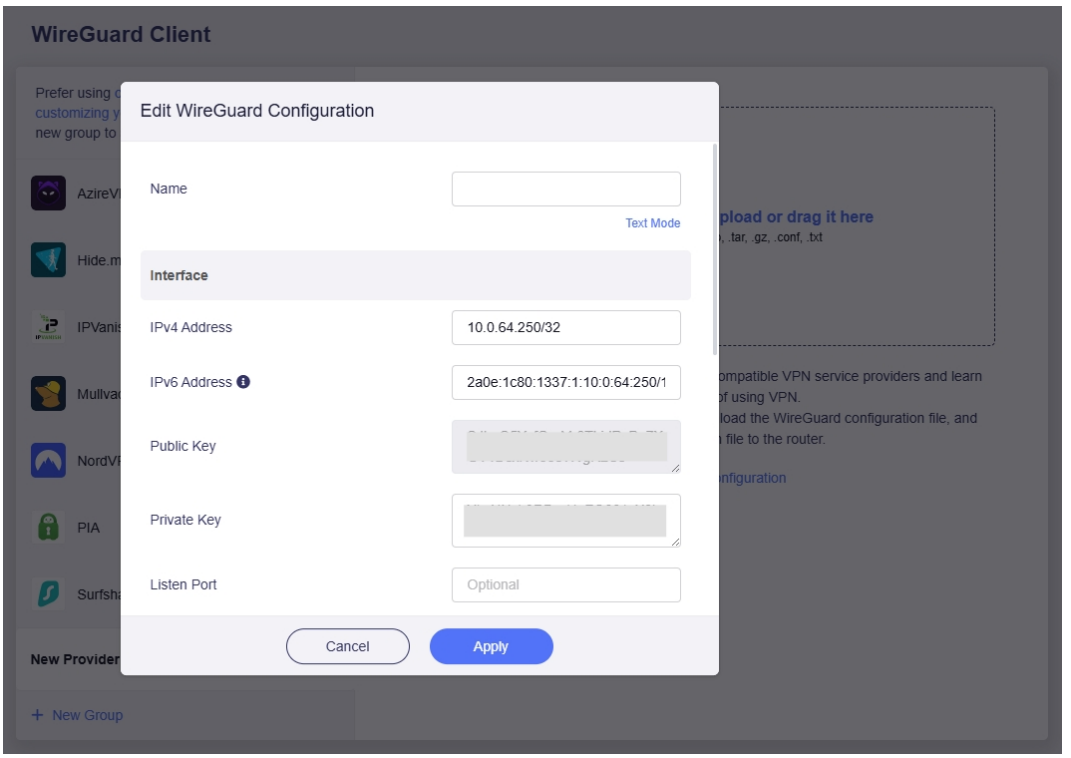


Alternativ klicken Sie unten im Upload-Bereich auf **Manually Add Configuration**, geben die Konfiguration als Text ein und klicken auf **Apply**.

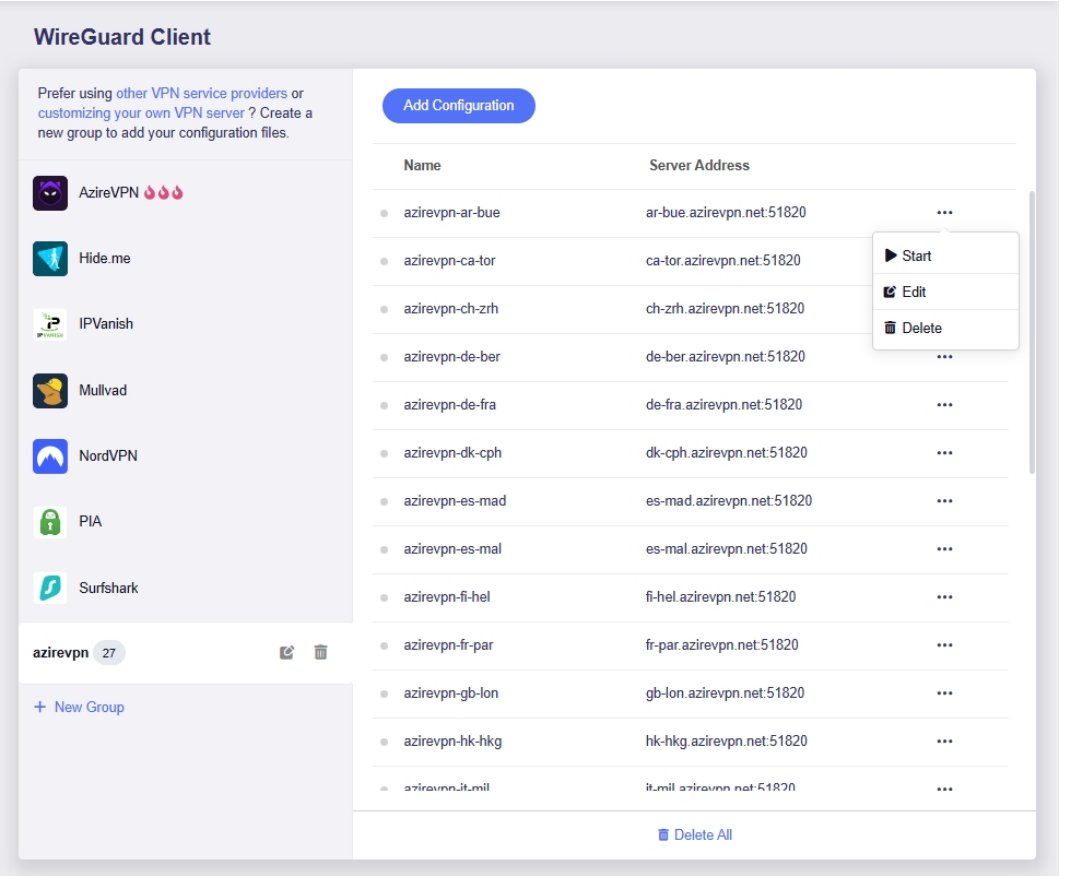




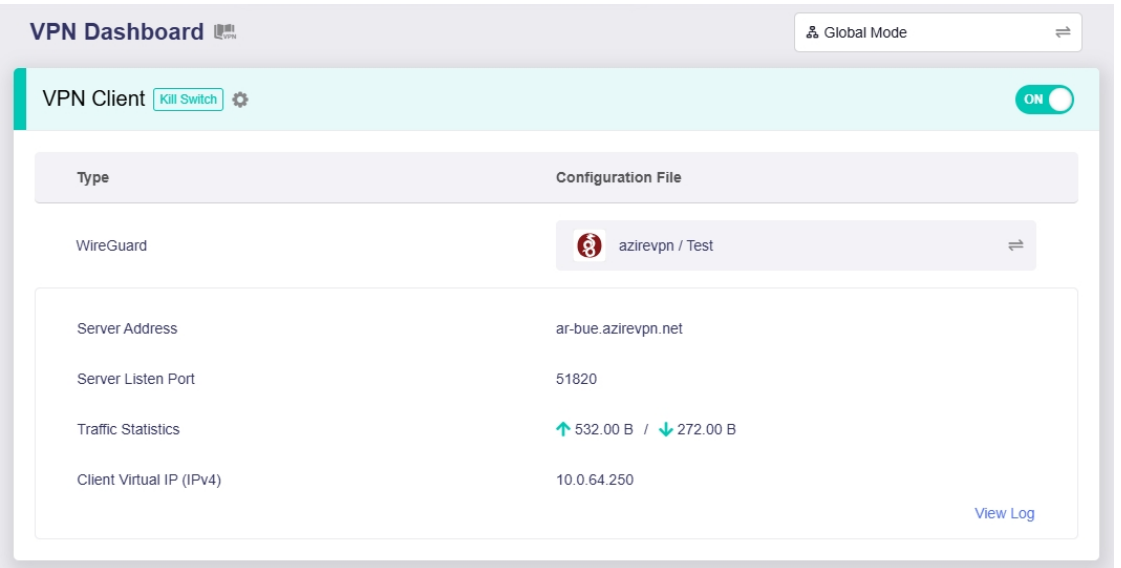
Um die einzelnen Einträge zu prüfen, wechseln Sie in den Modus Item und kontrollieren Sie die Konfigurationsdetails. Klicken Sie anschließend auf **Apply**.



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**.



Kapitel 11

Tor

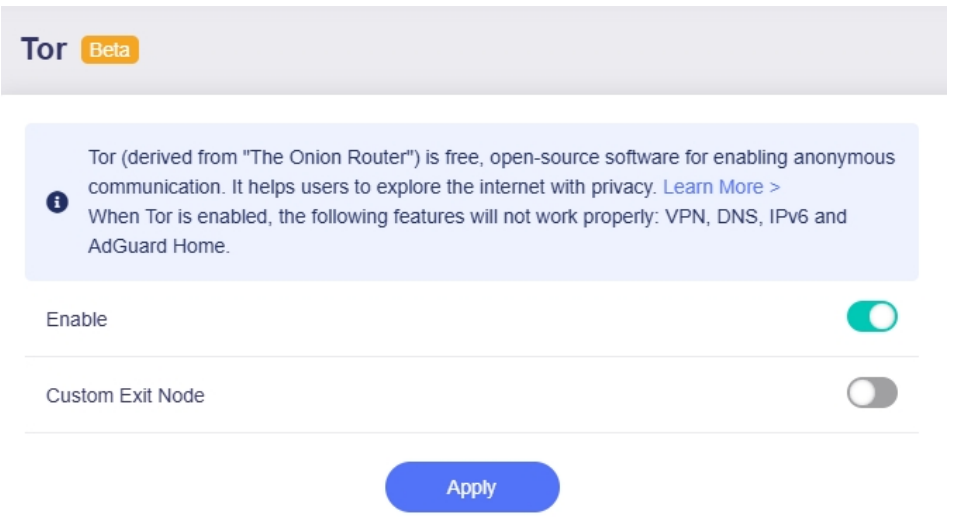
Dieses Kapitel stellt Tor (The Onion Router) vor, eine freie, quelloffene Software für anonyme Kommunikation.

Tor (abgeleitet von **The Onion Router**) ist eine freie, quelloffene Software für anonyme Kommunikation. Sie hilft Ihnen, mit mehr Privatsphäre im Internet zu surfen. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

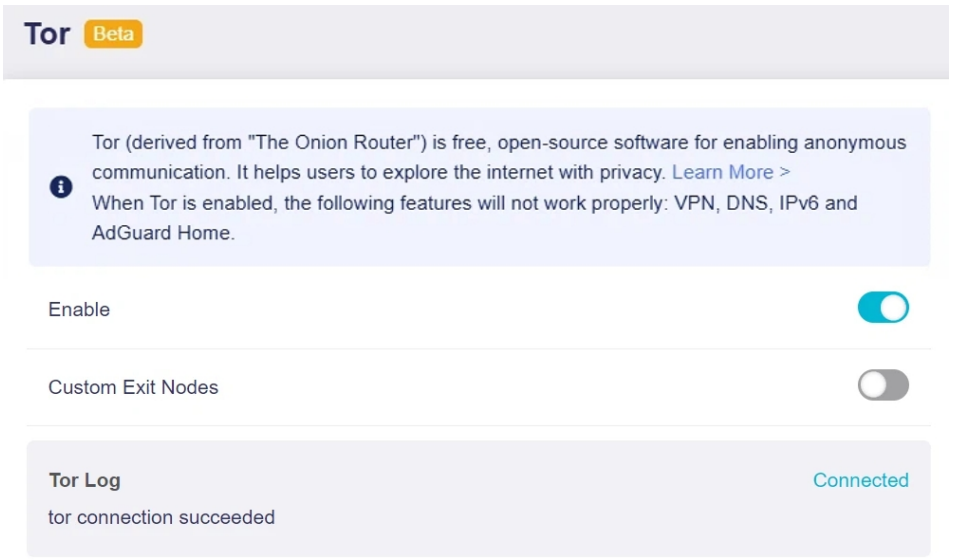
Bei aktiviertem Tor funktionieren VPN, DNS, IPv6 und AdGuard Home nicht ordnungsgemäß.

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

1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **Tor**. Aktivieren Sie die Funktion und bei Bedarf Custom Exit Nodes. Klicken Sie anschließend auf **Apply**.



2. Die Verbindung wird hergestellt. Wenn Ihr Netzwerk die Voraussetzungen erfüllt, wird der Status „verbunden“ angezeigt.


Tor
Beta
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Learn More >
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.
Enable
Custom Exit Nodes
Tor Log
Connected
tor connection succeeded

Kapitel 12

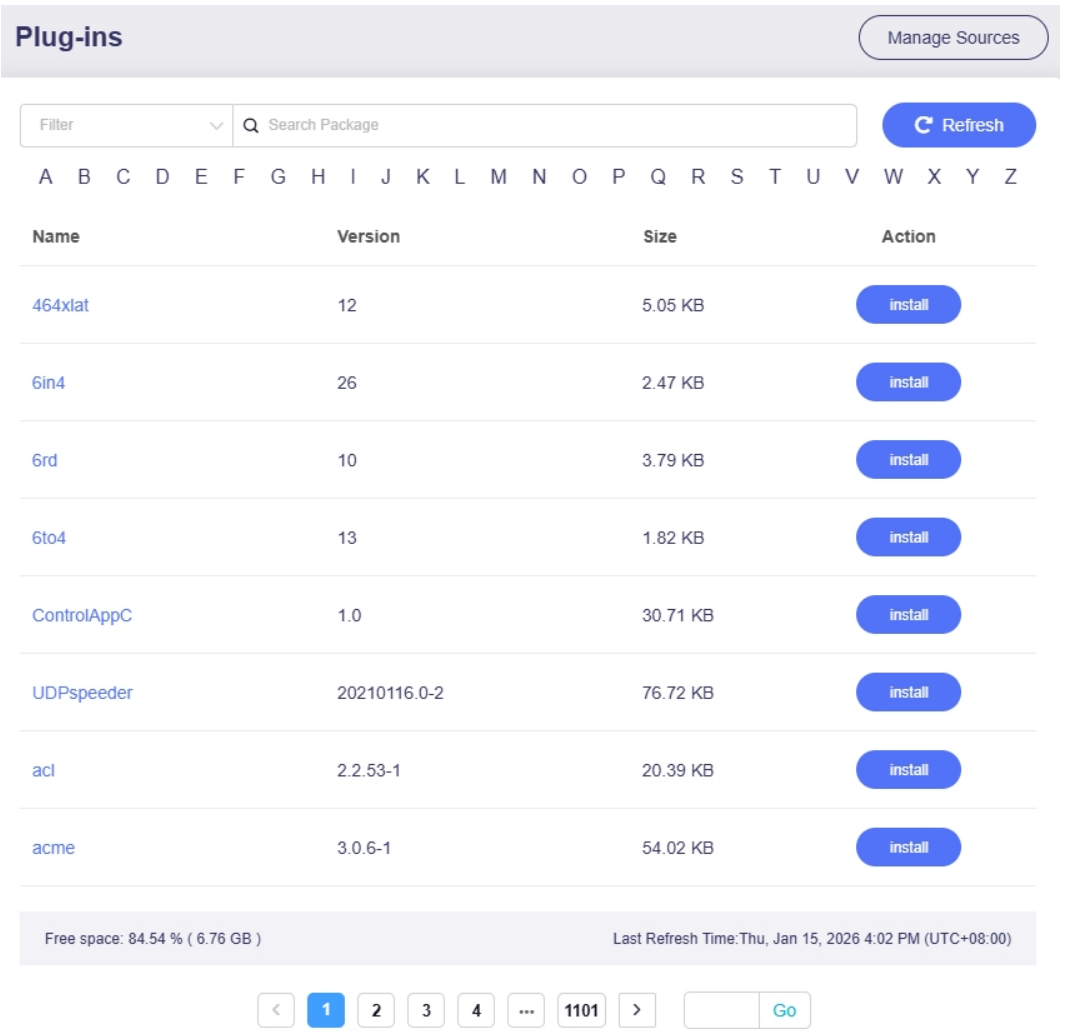
Anwendungen

Dieses Kapitel stellt einige Anwendungen der GL.iNet-Router vor, darunter Plug-ins, dynamisches DNS, Netzwerkspeicher, AdGuard Home, Kindersicherung, ZeroTier und Tailscale.

12.1 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:

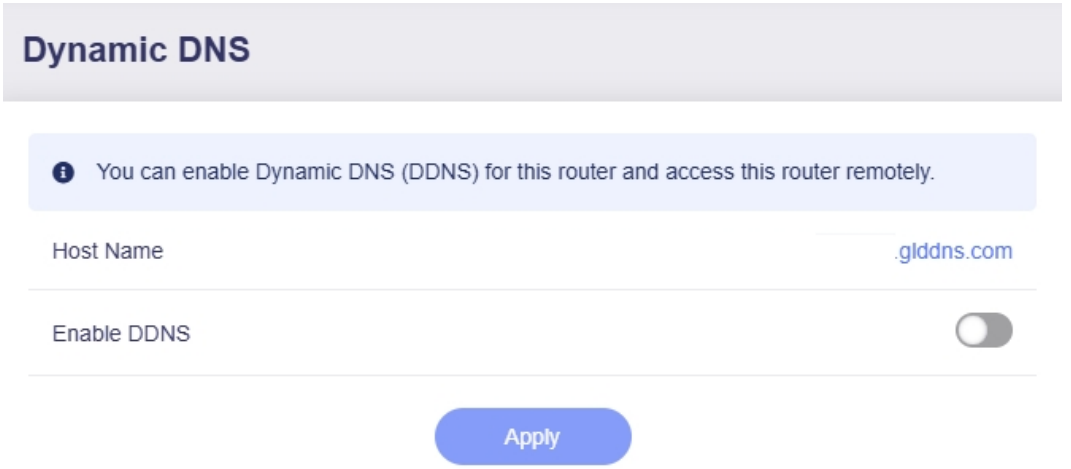
1. Es wird davon abgeraten, in der offiziellen GL.iNet-Firmware vorinstallierte Plug-ins wie nginx, AdGuard Home oder Tailscale zu aktualisieren.
2. Manuell installierte Plug-ins von Drittanbietern können aktualisiert werden. GL.iNet haftet jedoch nicht für Sicherheitsprobleme durch solche Plug-ins.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

12.2 Dynamisches DNS

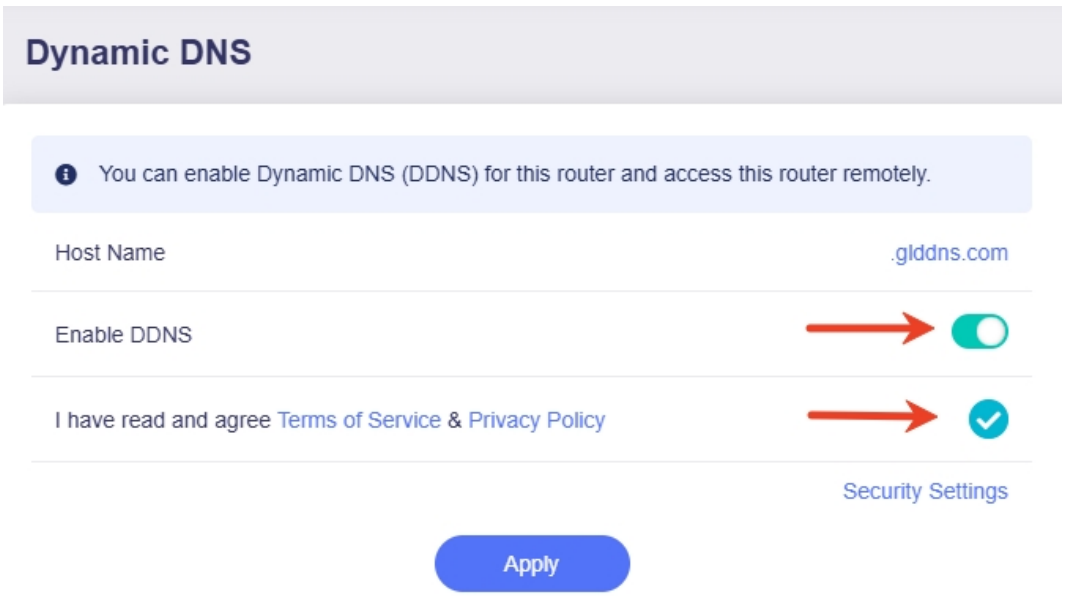
Dynamic DNS (DDNS) ordnet einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zu. Damit können Sie aus der Ferne auf Ihren Router zugreifen. Für diese Funktion ist eine öffentliche IP-Adresse erforderlich.

12.2.1 DDNS aktivieren

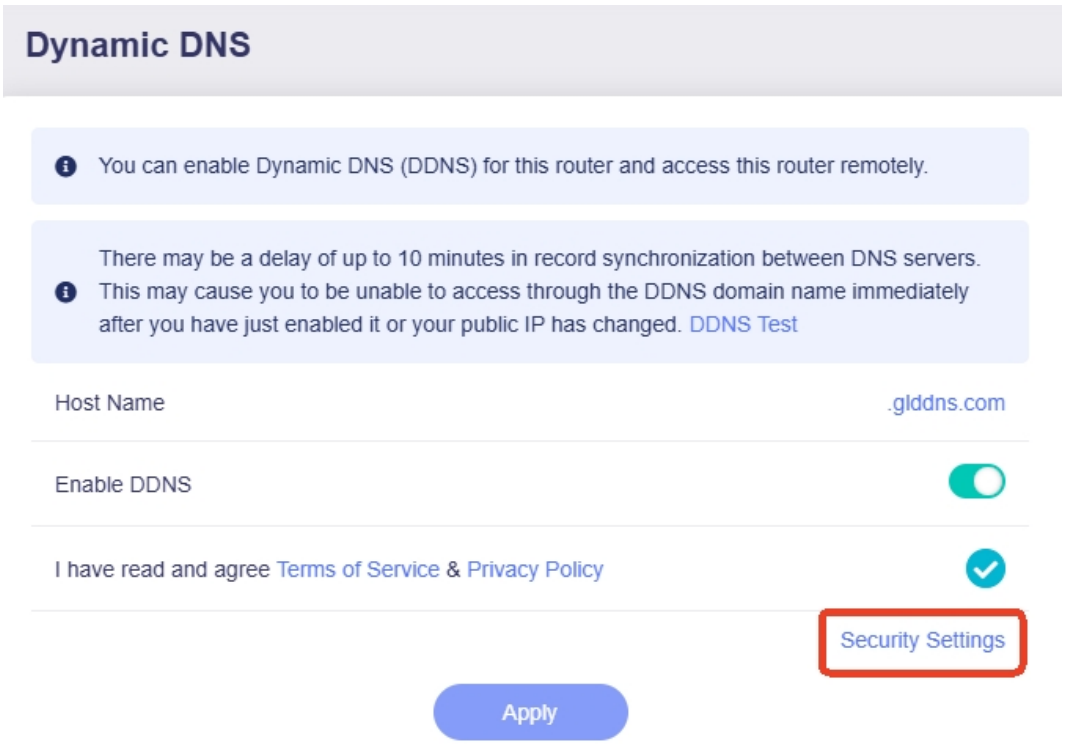
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Dynamic DNS**. Die folgende Seite wird angezeigt.



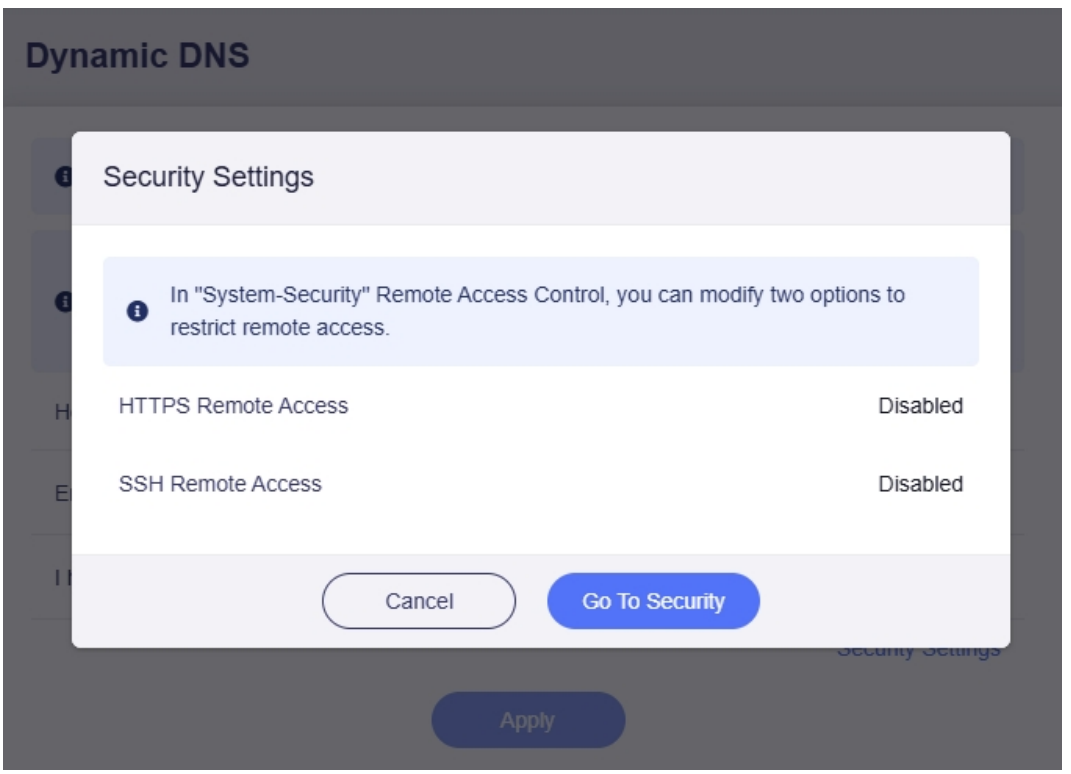
2. Aktivieren Sie **Enable DDNS**, lesen und akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



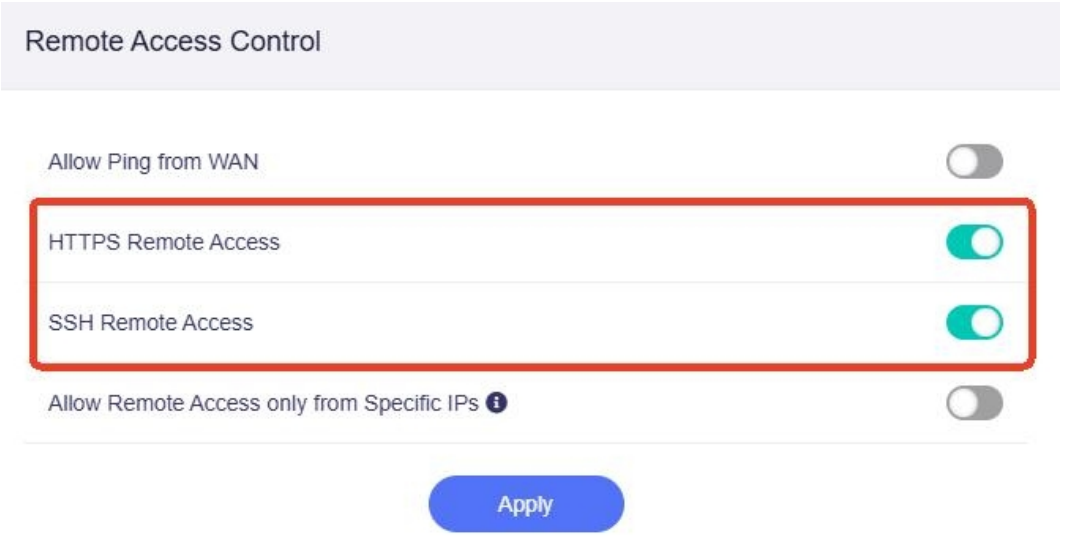
3. Klicken Sie unten rechts auf **Security Settings**.



4. Prüfen Sie im eingeblendeten Fenster, ob die gewünschte Art des Fernzugriffs aktiviert ist.



Falls nicht, öffnen Sie **SYSTEM** > **Security** > **Remote Access Control**, aktivieren Sie die betreffende Option und klicken Sie auf **Apply**.



Hinweis:

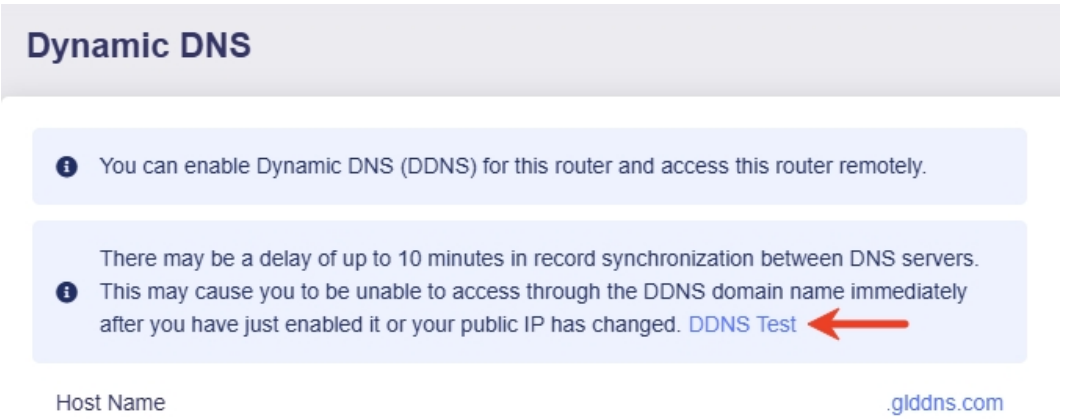
1. Die Synchronisierung der Einträge zwischen DNS-Servern kann bis zu zehn Minuten dauern. Deshalb kann der Zugriff über den DDNS-Domainnamen direkt nach der Aktivierung oder nach einer Änderung Ihrer öffentlichen IP-Adresse vorübergehend nicht möglich sein.
2. Wenn Sie DDNS und einen VPN-Client gleichzeitig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

12.2.2 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 abzufragen. Das folgende Beispiel zeigt Beryl AX GL-MT3000.



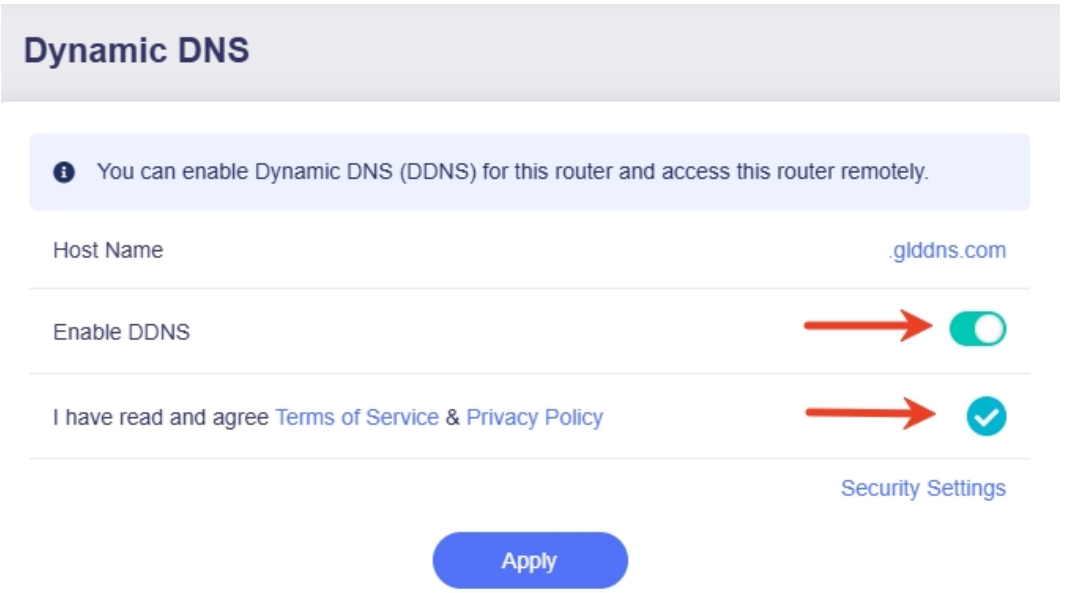
   - Ersetzen Sie „xxxxxxx.glddns.com“ in der obigen Abbildung durch Ihren Hostnamen.
   - „8.8.8.8“ ist ein DNS-Server von Google. Verwenden Sie diesen oder ersetzen Sie ihn durch einen anderen DNS-Server und drücken Sie die Eingabetaste.
2. Wenn eine öffentliche IP-Adresse wie „183.178.10.100“ in der 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.

12.2.3 HTTPS-Fernzugriff

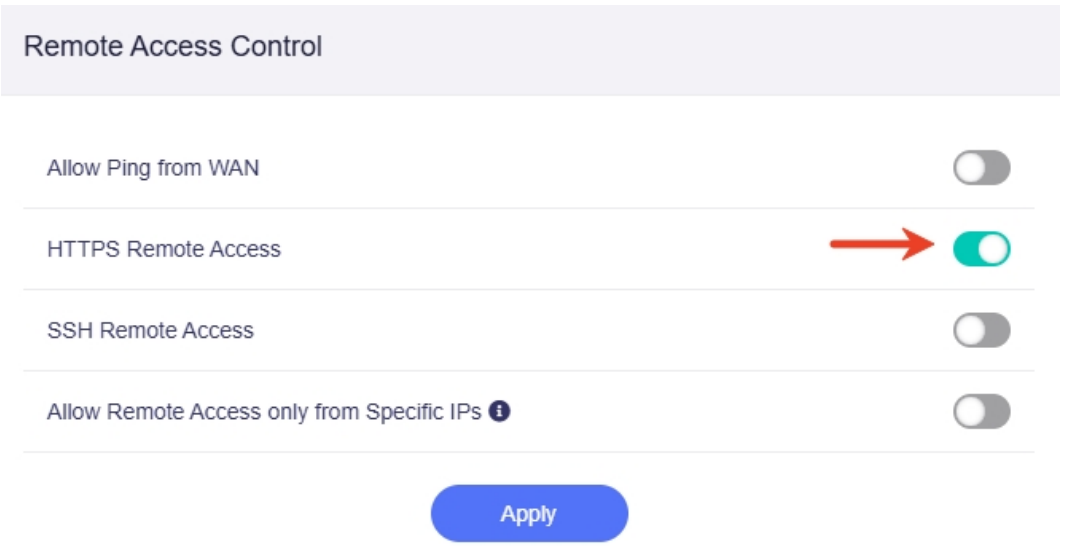
Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 443** ein.

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

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

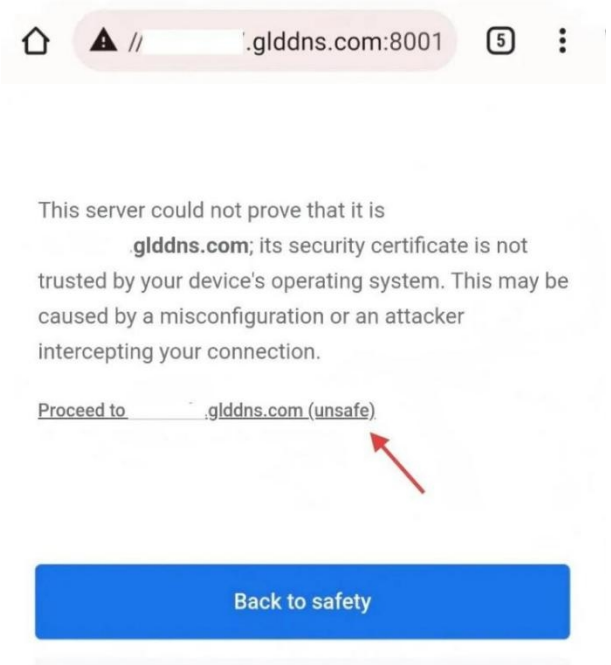


2. Öffnen Sie in der Weboberfläche **SYSTEM** > **Security** > **Remote Access Control**. Aktivieren Sie **HTTPS Remote Access** und klicken Sie auf **Apply**.



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.



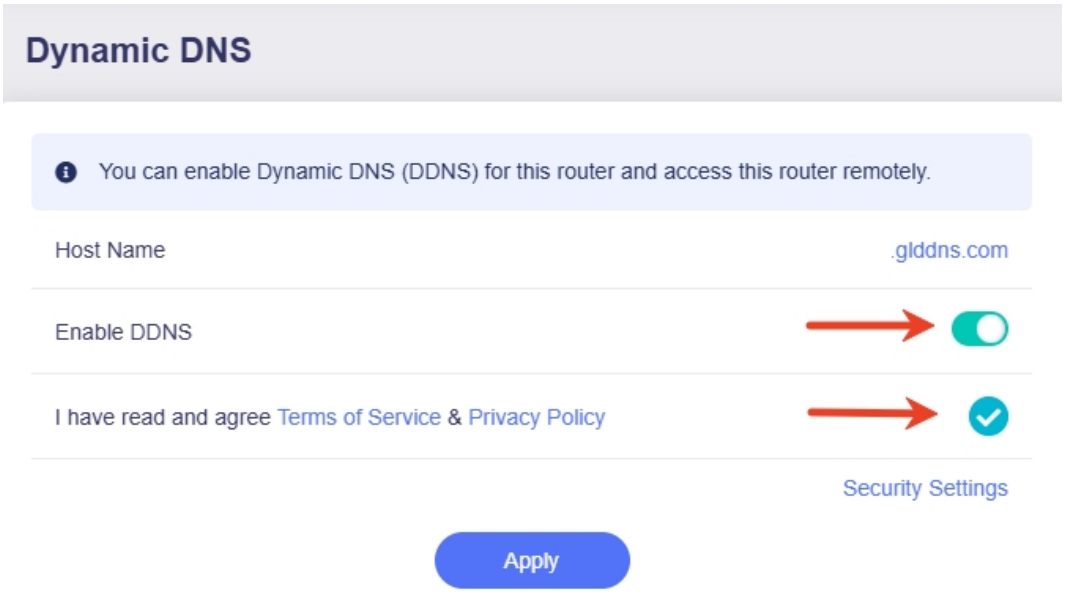
Sie können nun über den DDNS-Hostnamen per **HTTPS** auf die Weboberfläche des Routers zugreifen.

12.2.4 SSH-Fernzugriff

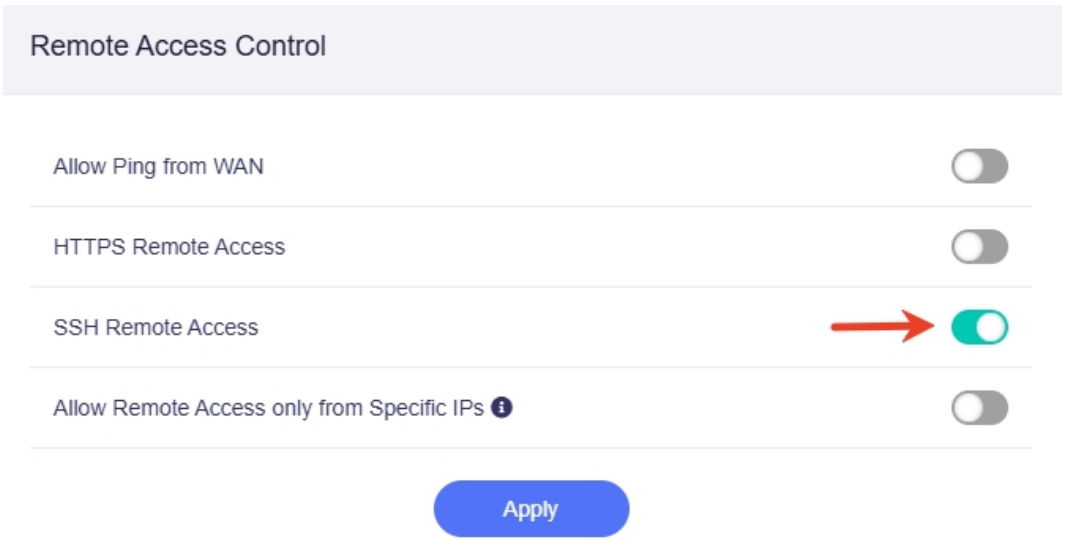
Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 22** ein.

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

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



2. Öffnen Sie in der Weboberfläche **SYSTEM** > **Security** > **Remote Access Control**. Aktivieren Sie **SSH Remote Access** 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.

12.3 Netzwerkspeicher

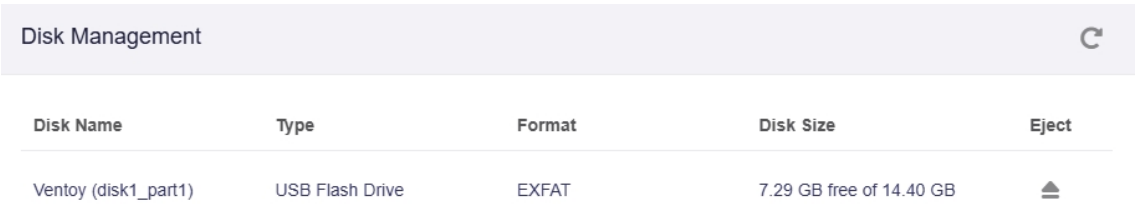
Die Netzwerkspeicherfunktion ermöglicht die gemeinsame Nutzung von Dateien auf mehreren Geräten. Schließen Sie dazu einen USB-Datenträger oder eine SD-Karte an Ihren Router an. Der Router stellt den Speicher als gemeinsames Netzlaufwerk bereit, auf das alle verbundenen Geräte zugreifen können.

Brume 2 verfügt über einen USB-Anschluss für USB-Sticks und tragbare externe Festplatten. Für diese Speichergeräte können Sie Samba, WebDAV oder DLNA einrichten. Gängige Dateisysteme wie NTFS, FAT32 und EXT4 werden unterstützt.

Hinweis: USB-Festplatten haben einen relativ hohen Strombedarf. Verwenden Sie eine externe Stromversorgung, da es sonst zu Fehlfunktionen kommen kann.

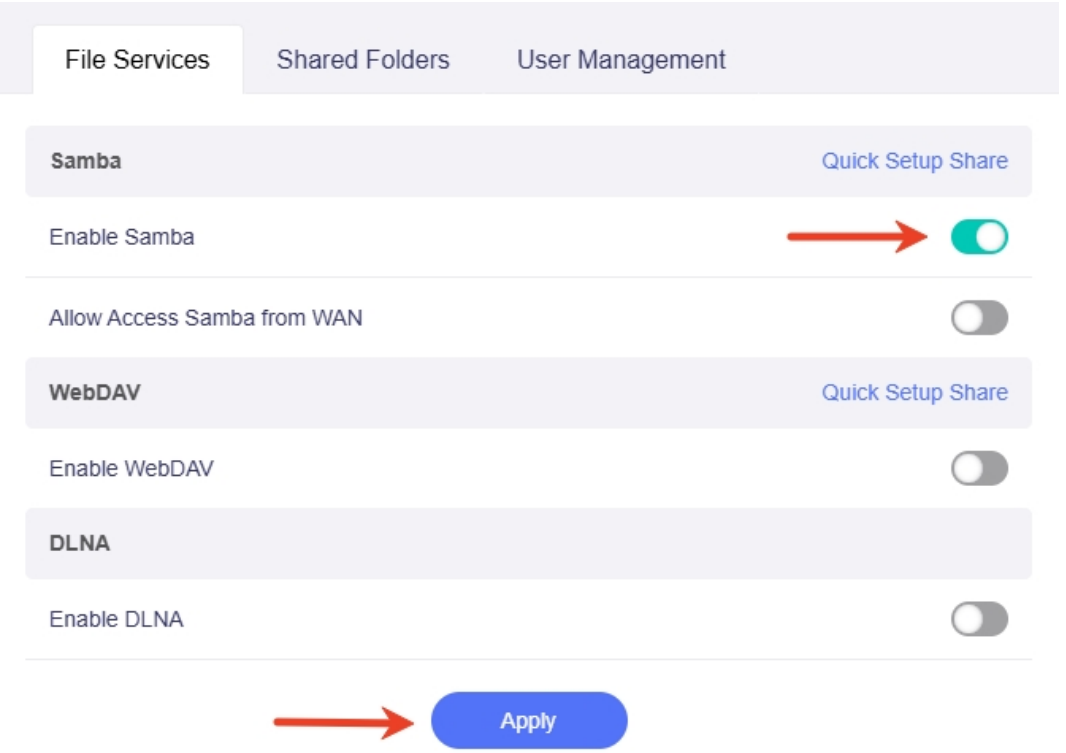
12.3.1 Speicher anschließen

1. Schließen Sie Ihr Speichergerät an den Router an.
   - USB-Stick: Stecken Sie ihn direkt in den USB-Anschluss.
   - Externe Festplatte: Schließen Sie gegebenenfalls eine separate Stromversorgung an und verbinden Sie die Festplatte anschließend mit dem Router.
2. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Network Storage**. Hier können Sie Dateiübertragungsdienste aktivieren und freigegebene Ordner verwalten.
3. Wenn das Speichergerät erkannt wird, erscheint **Disk Management** wie folgt.



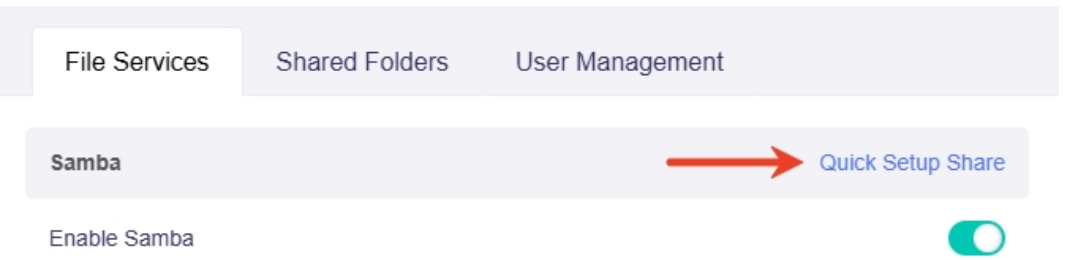
12.3.2 Samba einrichten

1. Aktivieren Sie im Abschnitt **File Services** die Option **Enable Samba** und klicken Sie auf **Apply**.

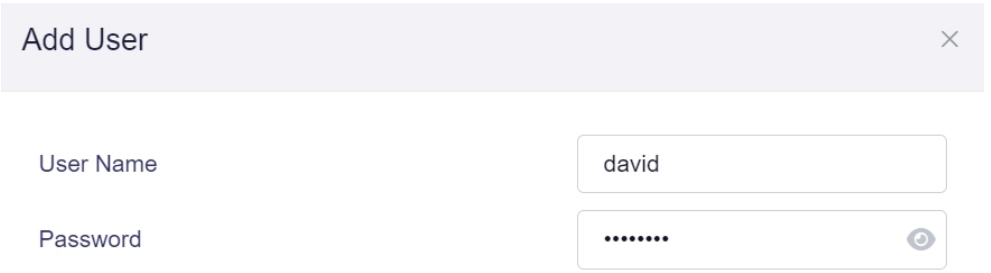


   - **Allow Access Samba from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den Samba-Dienst zugreifen sollen.

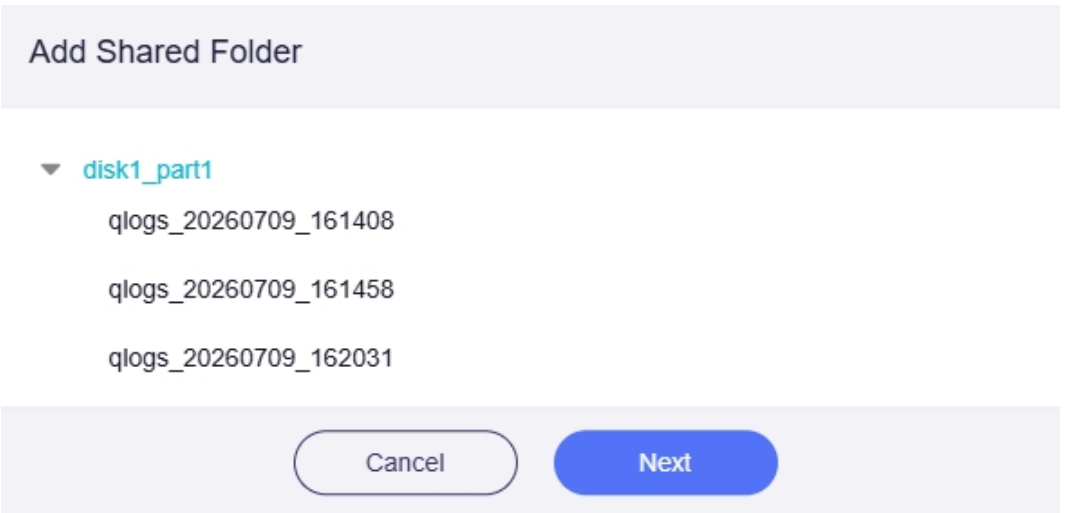
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



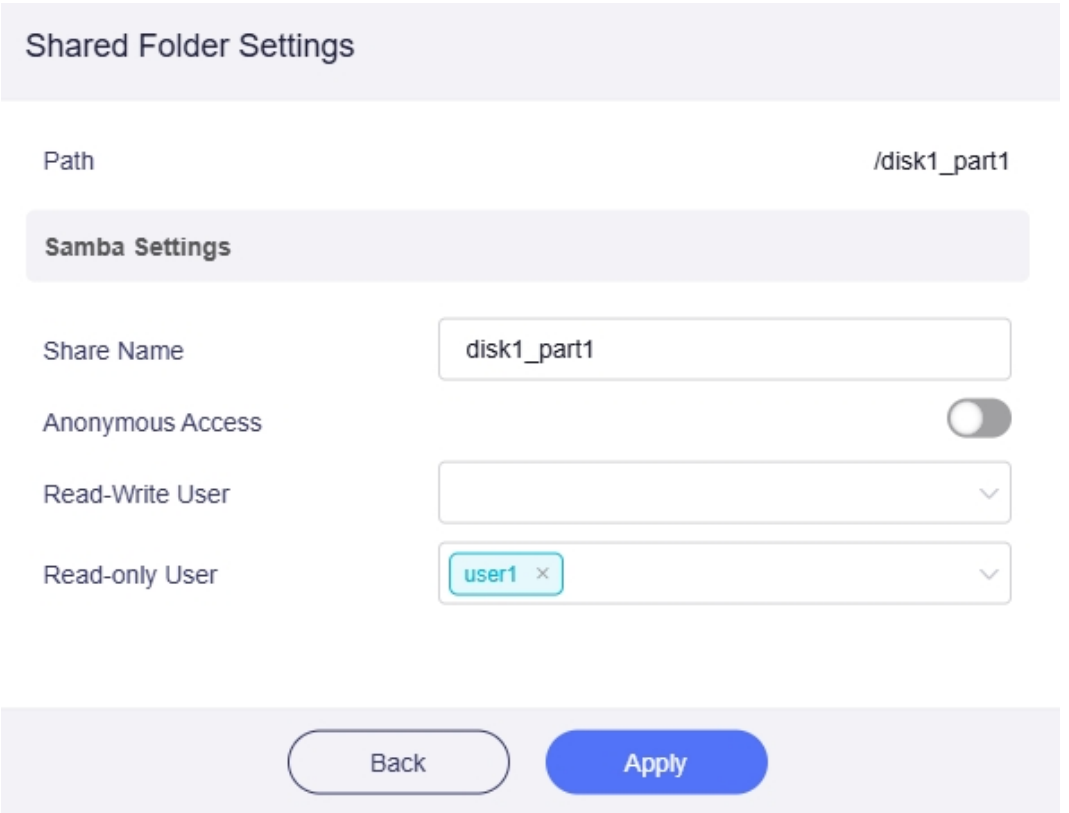
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



4. Klicken Sie auf das Dreiecksymbol, um alle Ordner anzuzeigen. Wählen Sie einen freizugebenden Ordner aus und klicken Sie auf **Next**. Um das gesamte Laufwerk freizugeben, klicken Sie auf dessen Namen, etwa disk1_part1.



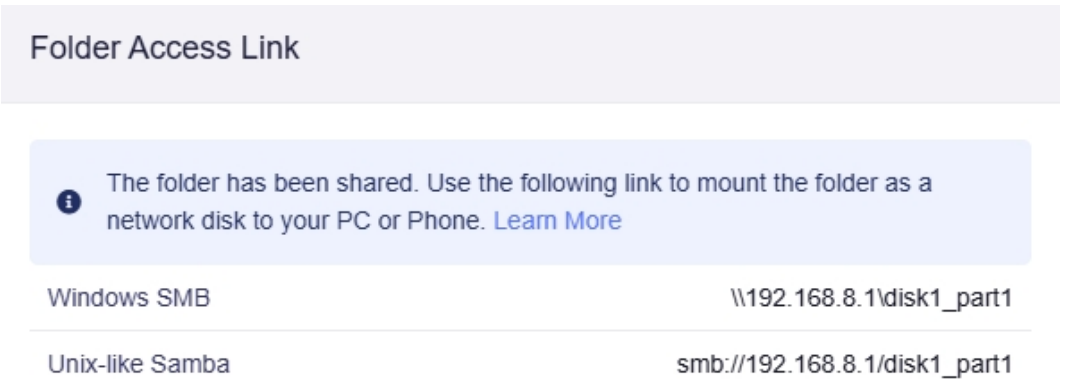
5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll er Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn dort und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend auf **Apply**.



Tipp: Aus Sicherheitsgründen wird davon abgeraten, Anonymous Access zu aktivieren.

6. Zugriffsadresse des Ordners abrufen.

   Die Seite zeigt die Zugriffsadressen für Windows und Unix-ähnliche Betriebssysteme an. Zu Letzteren gehören Android, iOS, macOS und Ubuntu. Über diese Adressen können Sie nun per Samba auf den freigegebenen Ordner zugreifen.

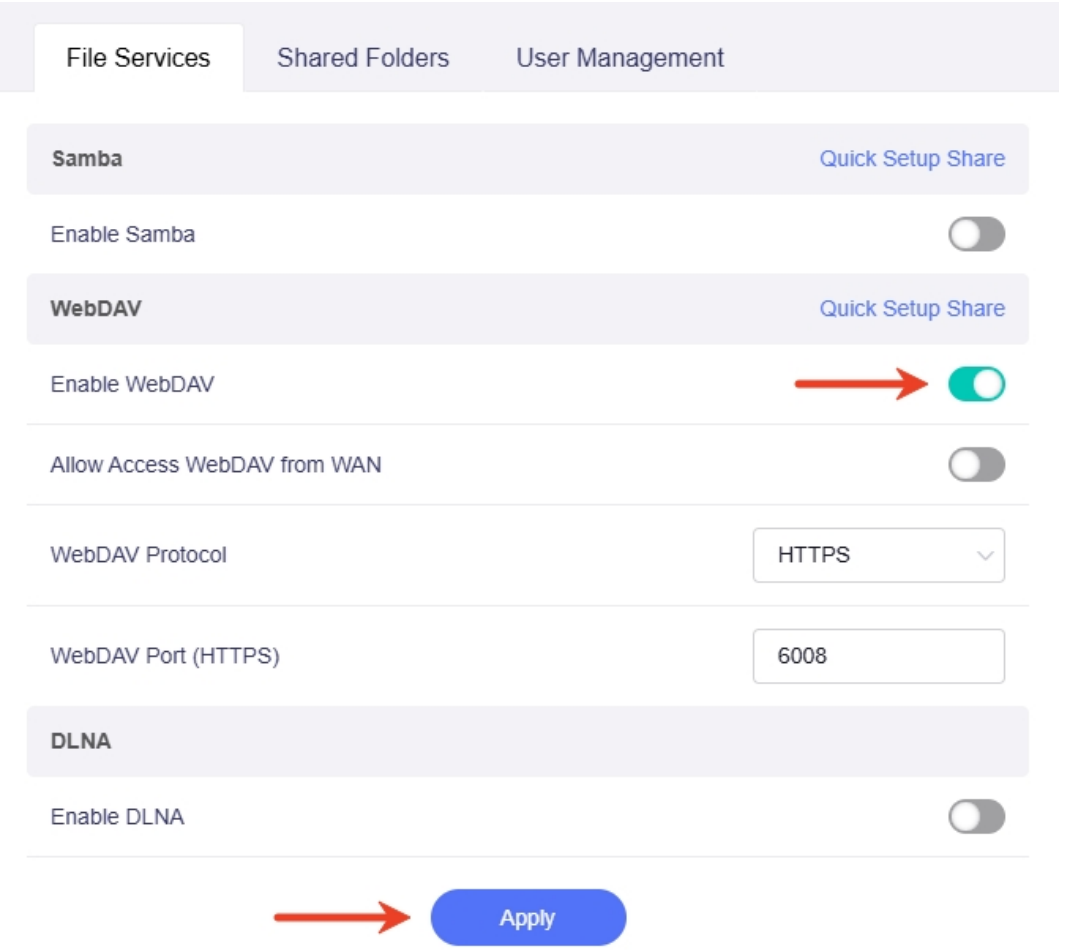


Hinweis: Wenn Sie **Allow Access Samba from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der

Zugriffsadresse (standardmäßig 192.168.8.1) durch die WAN-IP-Adresse des Routers. Diese finden Sie auf der Seite INTERNET der Weboberfläche.

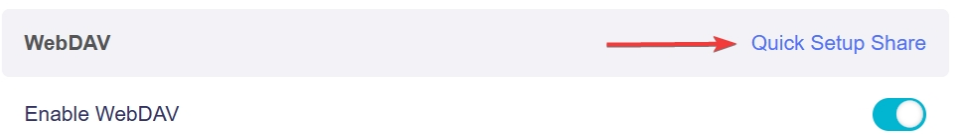
12.3.3 WebDAV einrichten

1. Aktivieren Sie im Abschnitt **File Services** die Option **Enable WebDAV** und klicken Sie auf **Apply**.

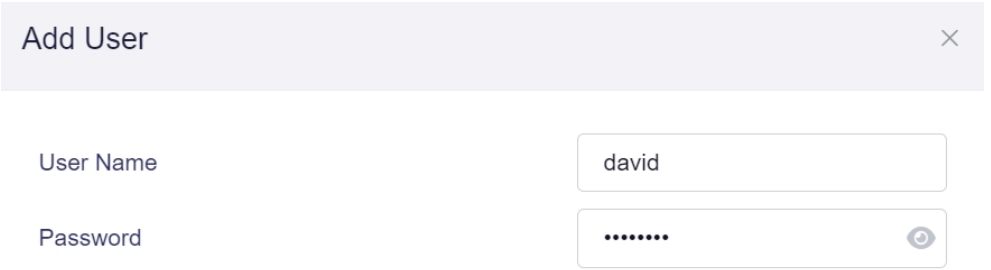


- **Allow Access WebDAV from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den WebDAV-Dienst zugreifen sollen.
- **WebDAV Protocol**: HTTP ist unverschlüsselt und wird auf eigenes Risiko verwendet. HTTPS ist verschlüsselt und verwendet ein selbstsigniertes Zertifikat.
- **WebDAV Port**: Ändern Sie die Portnummer nur bei einem Konflikt. Empfohlen wird der Bereich 1024–65535.

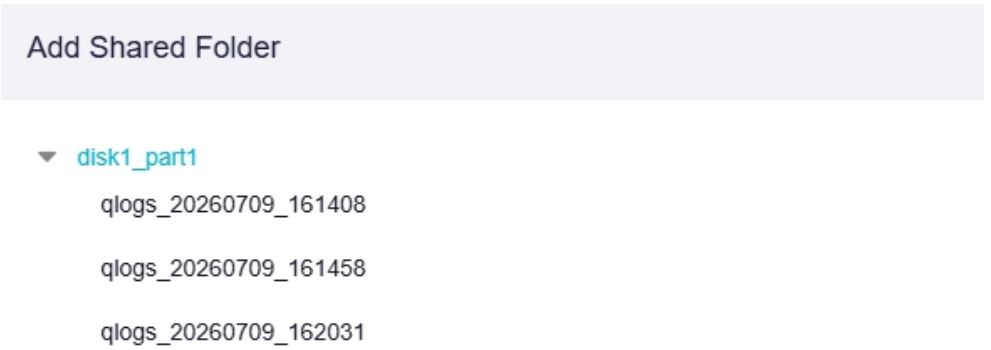
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



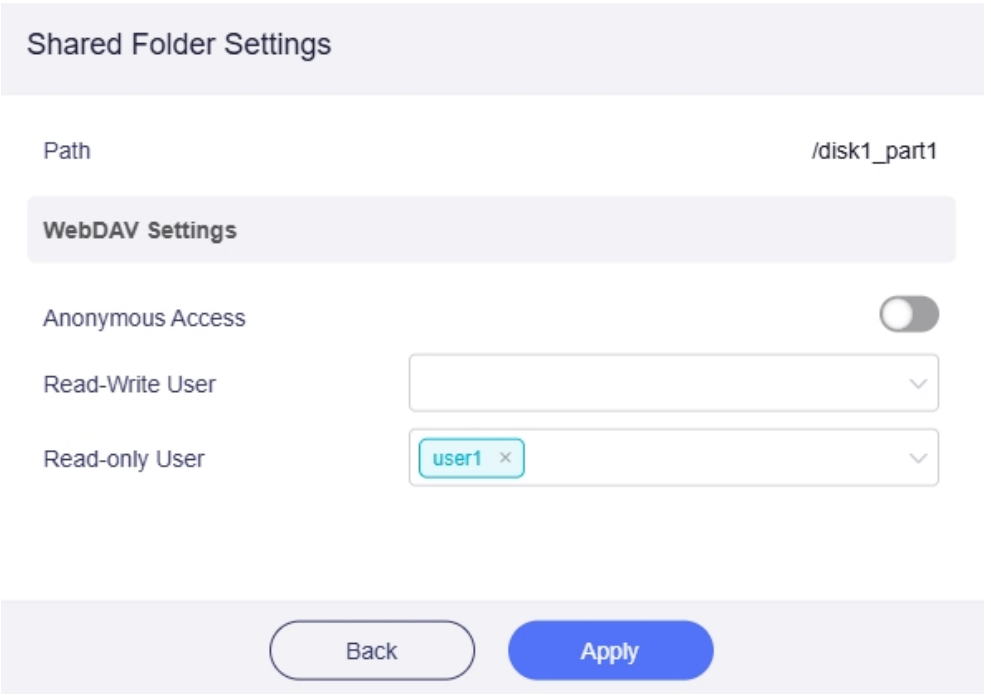
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



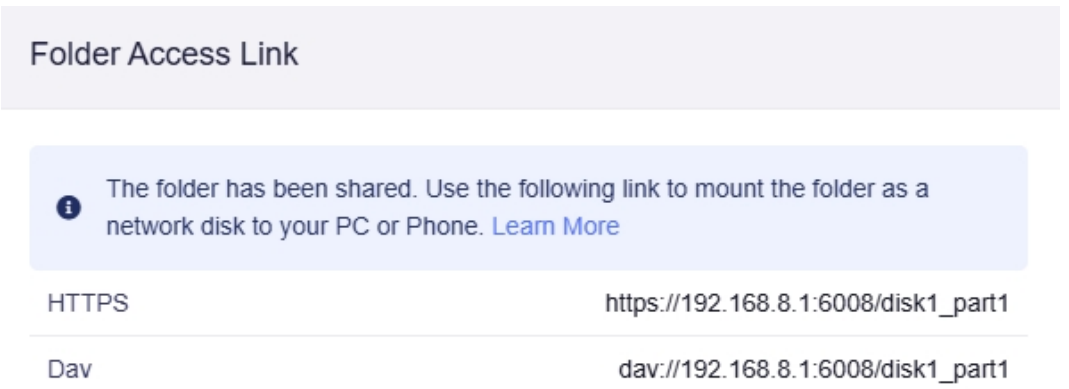
4. Klicken Sie auf das Dreiecksymbol, um alle Ordner anzuzeigen. Wählen Sie einen freizugebenden Ordner aus. Um das gesamte Laufwerk freizugeben, klicken Sie auf dessen Namen, etwa disk1_part1.



5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll dieser Benutzer Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn unter Read-Only User und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend auf **Apply**.



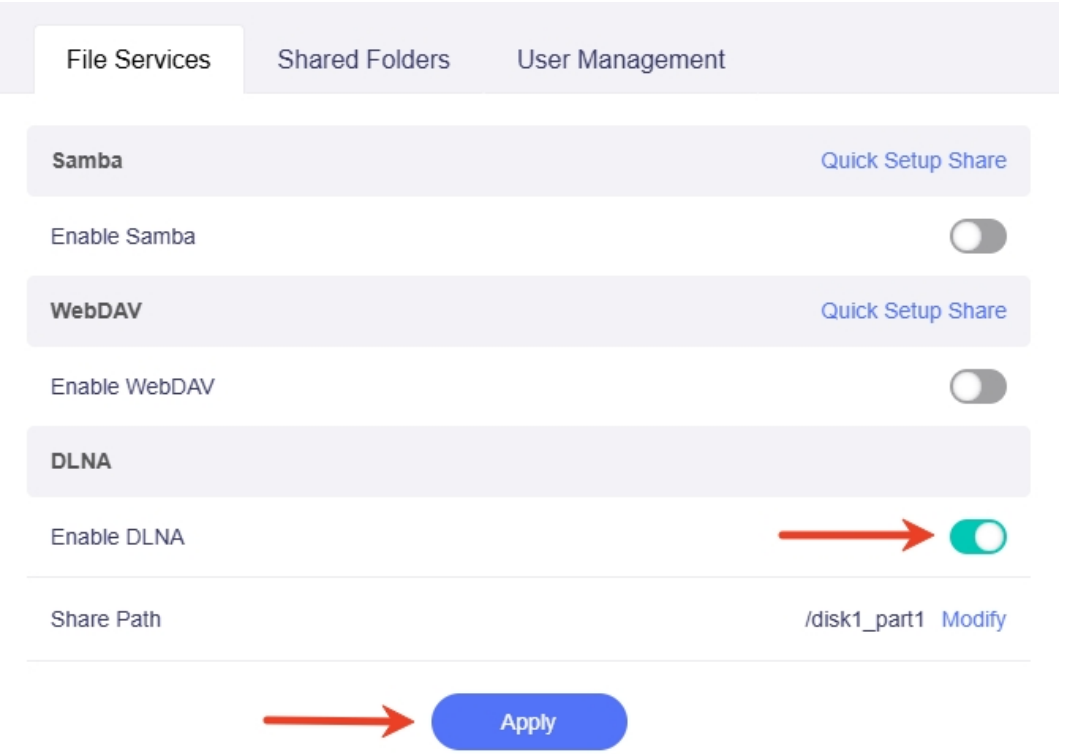
6. Zugriffsadresse des Ordners abrufen.
   Die Seite zeigt die Zugriffsadressen für Windows und Unix-ähnliche Betriebssysteme an. Zu Letzteren gehören Android, iOS, macOS und Ubuntu. Über diese Adressen können Sie nun per WebDAV auf den freigegebenen Ordner zugreifen.



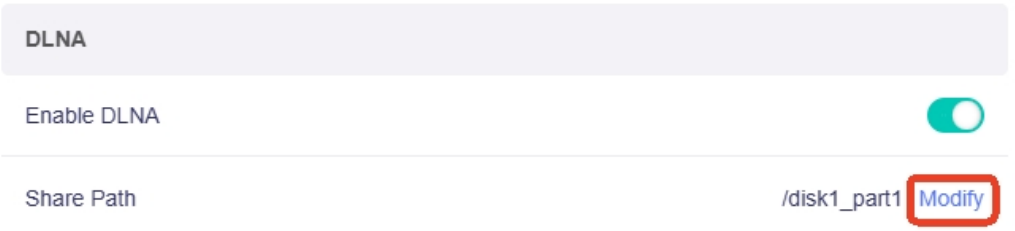
Hinweis: Wenn Sie **Allow Access WebDAV from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der Zugriffsadresse (standardmäßig 192.168.8.1) durch die WAN-IP-Adresse des Routers. Diese finden Sie auf der Seite INTERNET der Weboberfläche.

12.3.4 DLNA einrichten

1. Aktivieren Sie im Abschnitt **File Services** die Option **Enable DLNA** und klicken Sie auf **Apply**.



2. Passen Sie bei Bedarf rechts den Freigabepfad an.



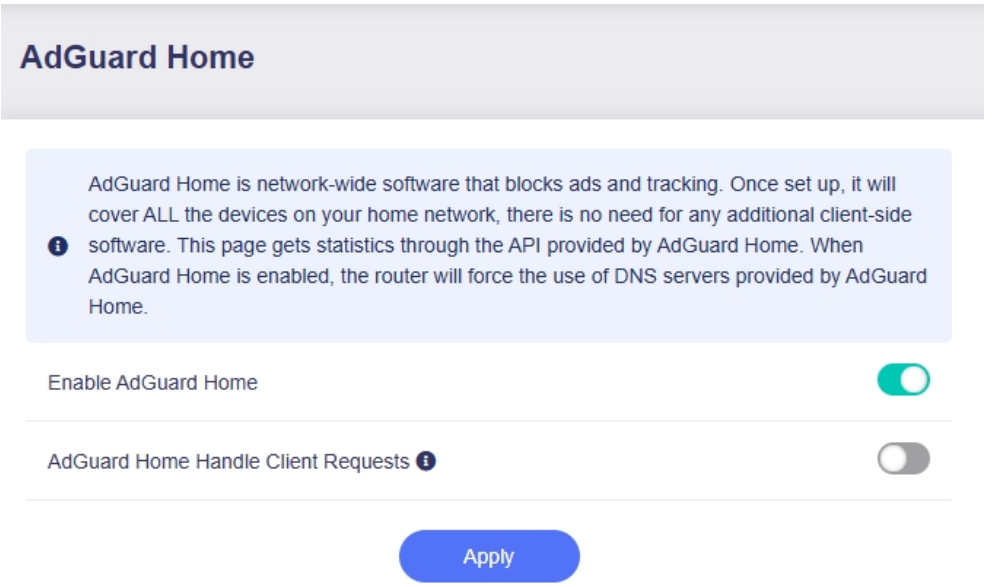
3. Verbinden Sie Ihren Smart-TV mit dem Router. Er erkennt den DLNA-Server automatisch.

12.4 AdGuard Home

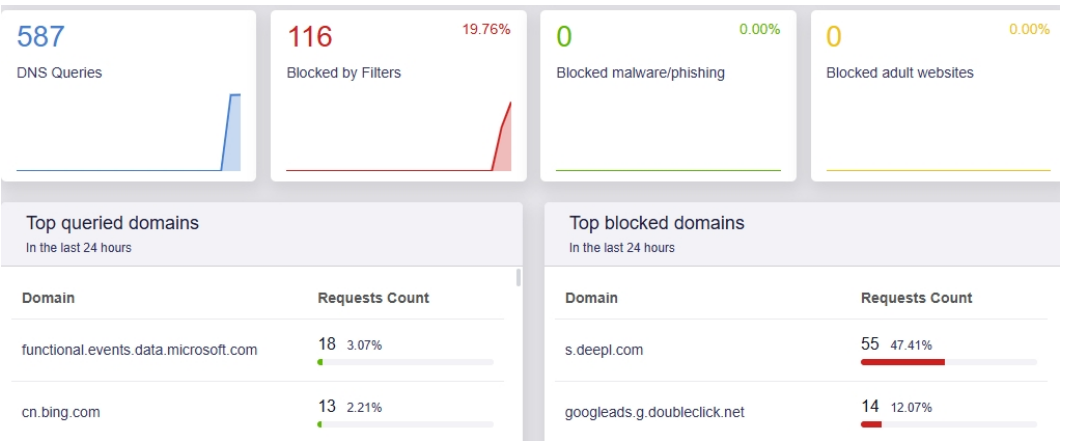
AdGuard Home blockiert Werbung und Tracking im gesamten Netzwerk. Nach der Einrichtung schützt die Software alle Endgeräte, ohne dass auf diesen zusätzliche Software installiert werden muss.

Gehen Sie wie folgt vor, um AdGuard Home einzurichten.

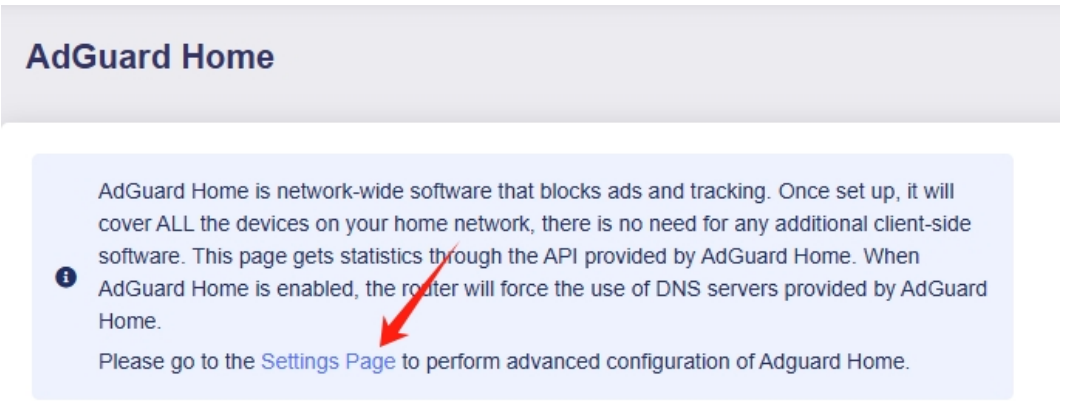
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **AdGuard Home**. Aktivieren Sie **Enable AdGuard Home** und klicken Sie auf **Apply**.



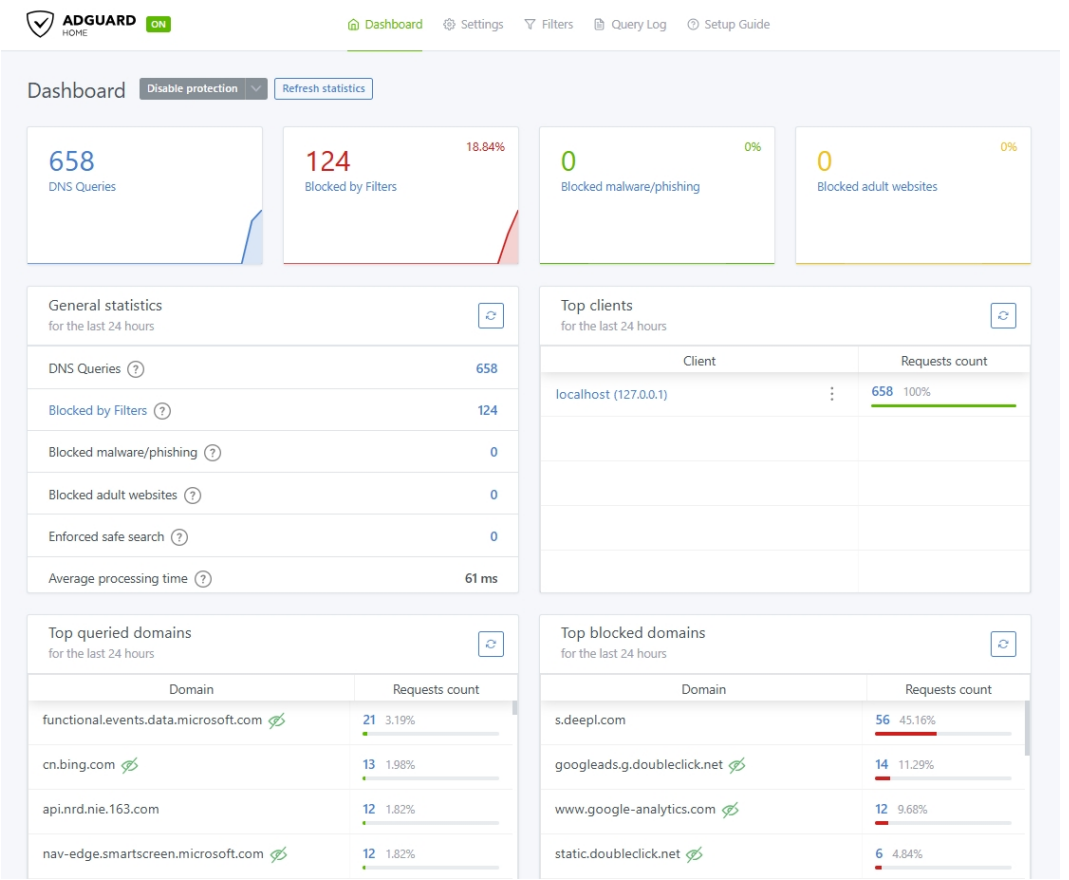
   - **AdGuard Home Handles Client Requests**: Leitet DNS-Anfragen der Endgeräte direkt an AdGuard Home weiter. Dadurch funktionieren jedoch domainbasierte VPN-Richtlinien nicht mehr.
2. Die Seite lädt automatisch DNS-Statistiken wie Anfragen und blockierte Domains über die API von AdGuard Home.



3. Klicken Sie auf **Settings Page**, um die erweiterten Einstellungen von AdGuard Home zu konfigurieren.



4. Sie werden zur Einstellungsseite von AdGuard Home weitergeleitet. Unterstützung finden Sie im [AdGuard Home Support Center].


ADGUARD HOME
ON
Dashboard
Settings
Filters
Query Log
Setup Guide
Dashboard
Disable protection
Refresh statistics
658
DNS Queries
124
18.84%
Blocked by Filters
0
0%
Blocked malware/phishing
0
0%
Blocked adult websites
General statistics
for the last 24 hours
DNS Queries 658
Blocked by Filters 124
Blocked malware/phishing 0
Blocked adult websites 0
Enforced safe search 0
Average processing time 61 ms
Top clients
for the last 24 hours
Client
Requests count
localhost (127.0.0.1)
658 100%
Top queried domains
for the last 24 hours
Domain
Requests count
functional.events.data.microsoft.com 21 3.19%
cn.bing.com 13 1.98%
api.nrd.nie.163.com 12 1.82%
nav-edge.smartscreen.microsoft.com 12 1.82%
Top blocked domains
for the last 24 hours
Domain
Requests count
s.deepl.com 56 45.16%
googleads.g.doubleclick.net 14 11.29%
www.google-analytics.com 12 9.68%
static.doubleclick.net 6 4.84%

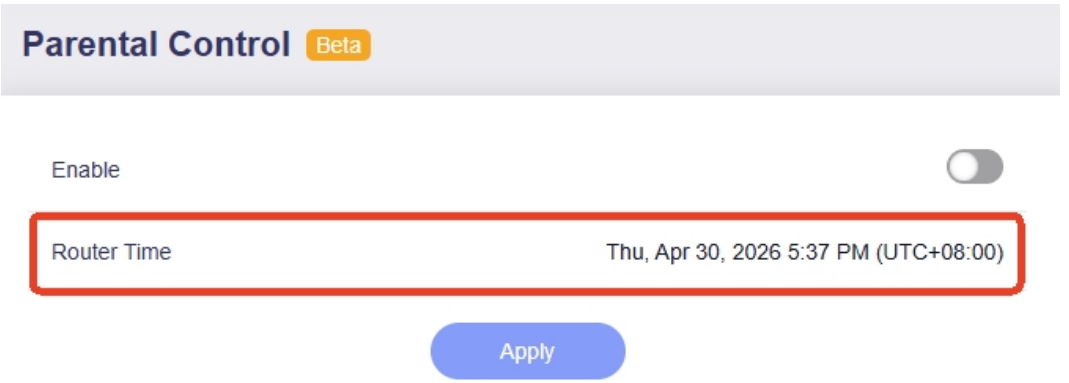
12.5 Kindersicherung

Die Kindersicherung schützt Kinder im Internet, indem sie ungeeignete Webseiten sperrt und die Gerätenutzung zeitlich begrenzt. Sie hilft, schädliche Inhalte zu vermeiden, Bildschirmzeiten zu steuern und einen verantwortungsvollen Umgang mit dem Internet zu fördern.

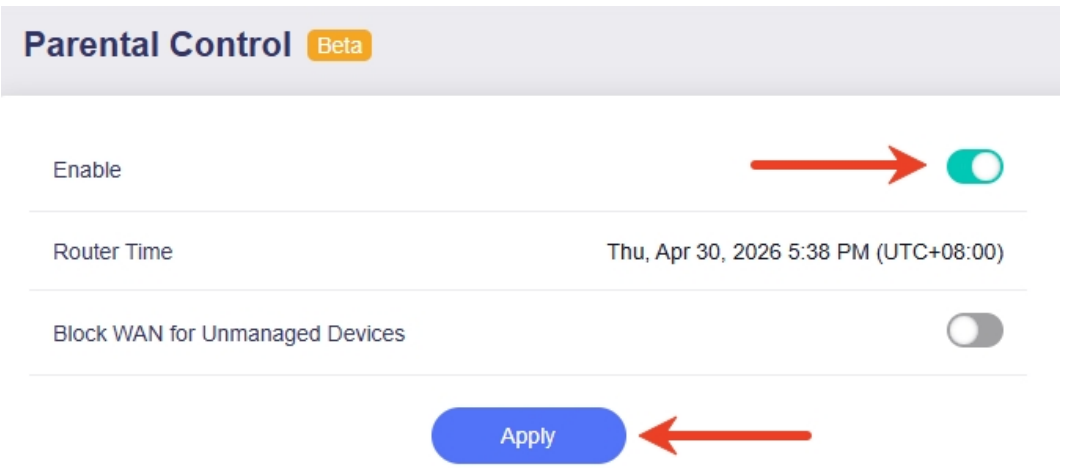
12.5.1 Schnelleinrichtung

Gehen Sie wie folgt vor, um die Kindersicherung auf einem GL.iNet-Router einzurichten.

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Parental Control.** Prüfen Sie, ob die Routerzeit stimmt. Falls nicht, synchronisieren Sie diese zunächst unter **SYSTEM** > **Time Zone**.



2. Aktivieren Sie die Kindersicherung und klicken Sie auf **Apply**. Folgen Sie anschließend dem Einrichtungsassistenten. Ein Video zur Einrichtung finden Sie hier.



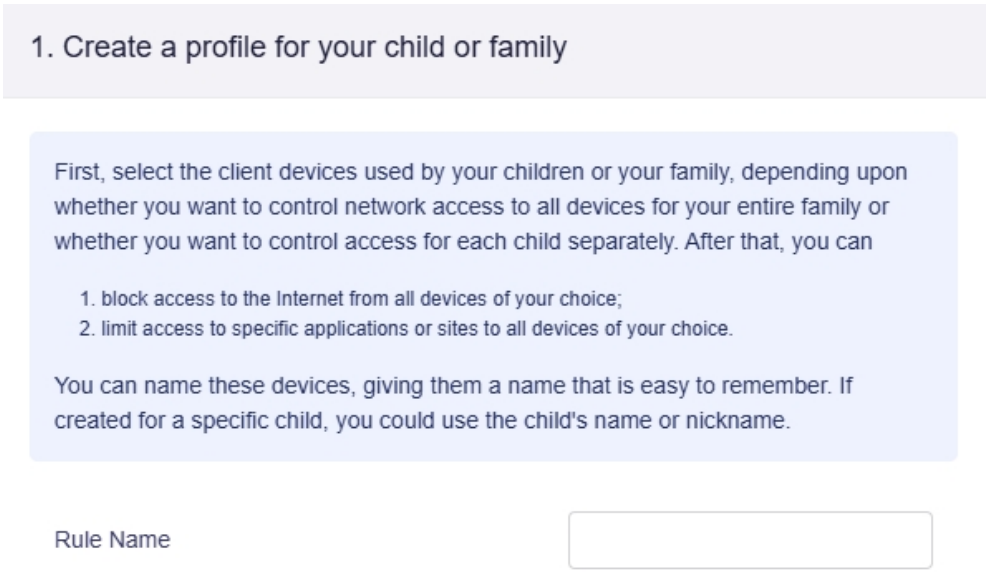
- **Block WAN for Unmanaged Devices**: Sperrt den Internetzugang für alle Geräte, die nicht in der Kindersicherungsliste stehen.

Das folgende Beispiel zeigt eine mögliche Anwendung.

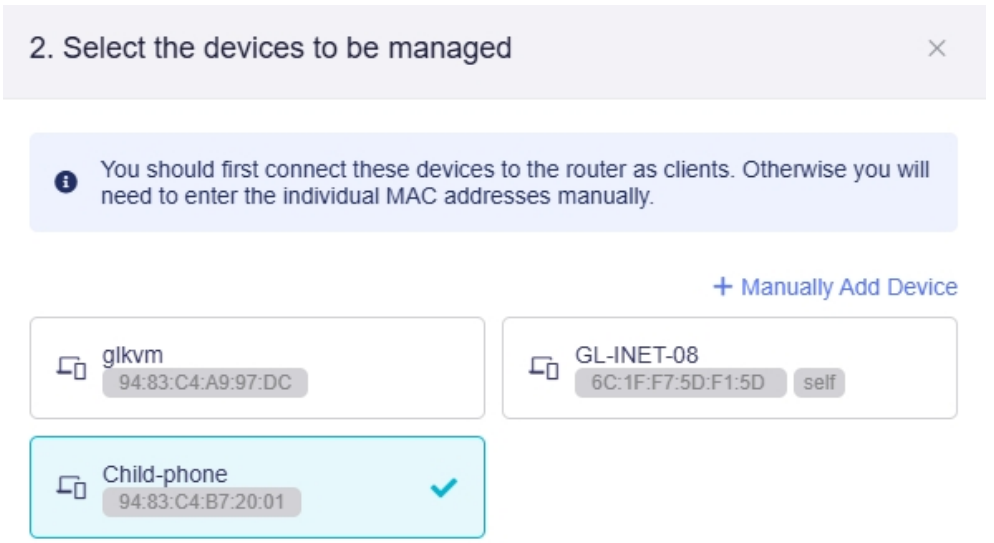
Szenario: Geräte in diesem Profil dürfen an Wochentagen von 08:00 bis 11:00 Uhr zum Lernen und am Wochenende von 18:00 bis 20:00 Uhr zum Spielen auf das Internet zugreifen. Zu allen anderen Zeiten ist der Internetzugang standardmäßig gesperrt.

Einrichtung:

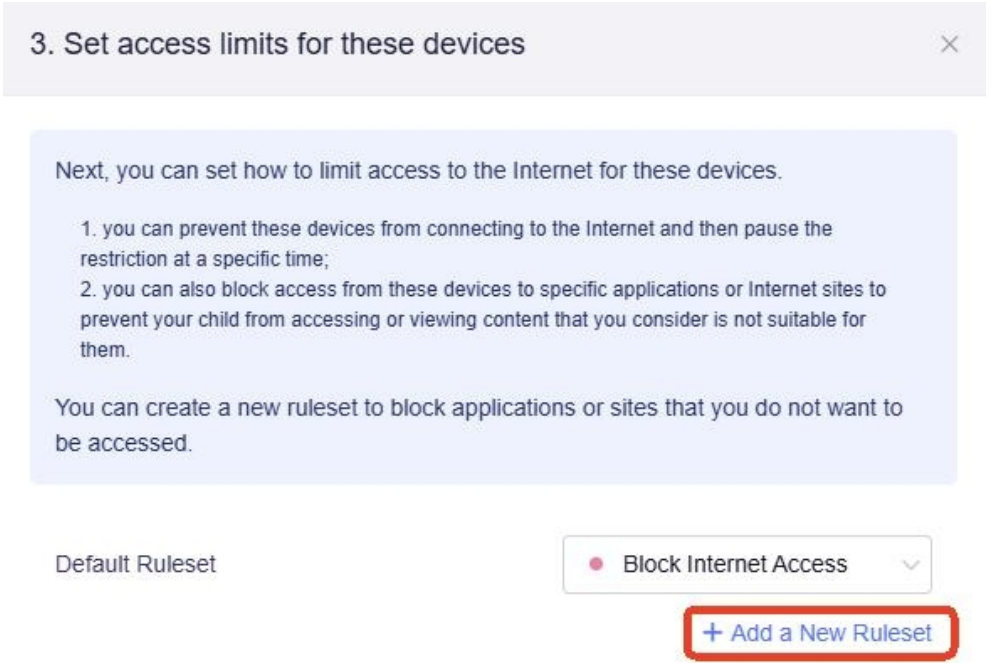
1. Erstellen Sie ein Profil und vergeben Sie einen Namen.



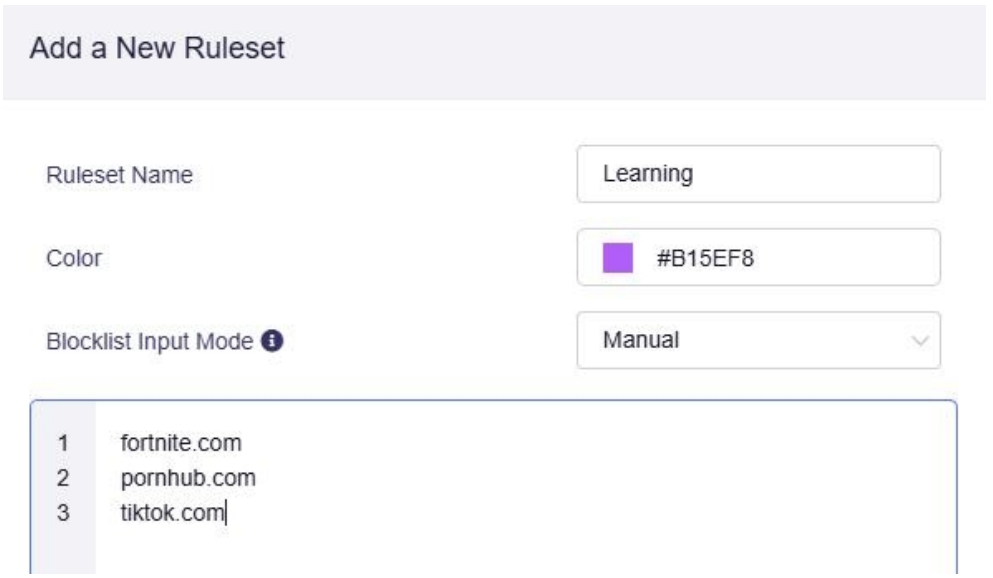
2. Wählen Sie die zu verwaltenden Geräte aus. Verbinden Sie diese zunächst mit dem Router. Noch nicht verbundene Geräte können Sie durch Eingabe ihrer MAC-Adressen manuell hinzufügen.



3. Zugriffsbeschränkungen festlegen.
   Es gibt zwei voreingestellte Regelsätze: **Block Internet Access** und **No Limit**.
   Klicken Sie auf **Add a New Ruleset** und erstellen Sie zwei weitere Regelsätze für die spätere Verwendung: **Learning** und **Play**.

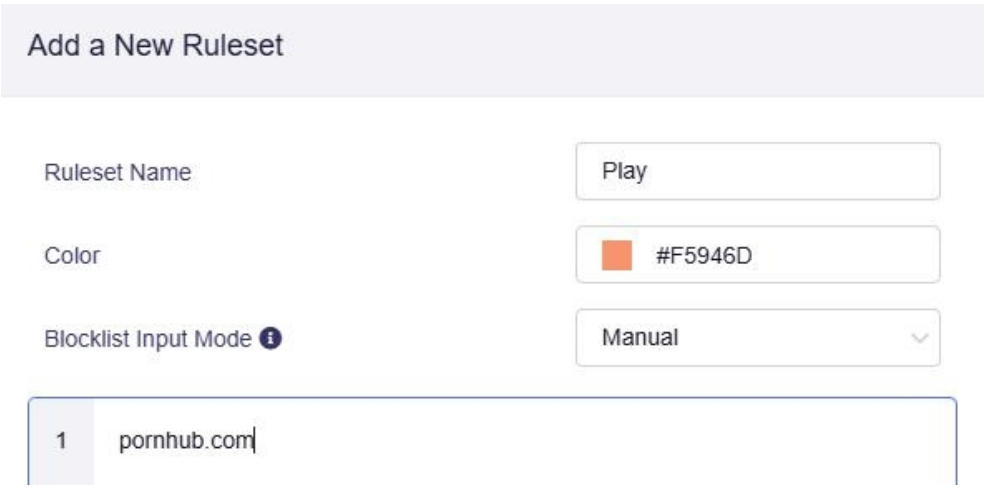


   Legen Sie Namen, etwa Learning, und Farbe des Regelsatzes fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.

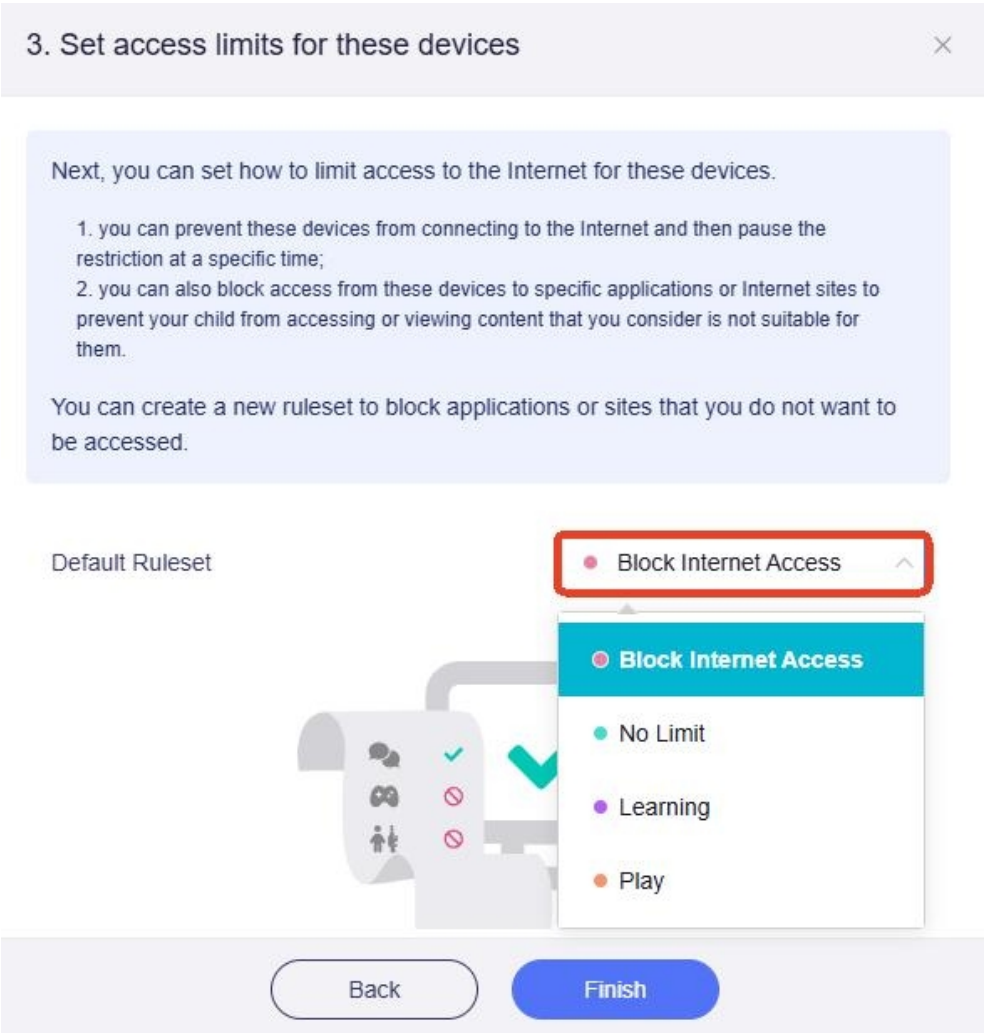


   Hinweis: Die Domainnamen auf der Sperrliste umfassen auch ihre Subdomains. Der Eintrag „example.com“ schließt beispielsweise „subdomain.example.com“ und alle weiteren Subdomains ein.

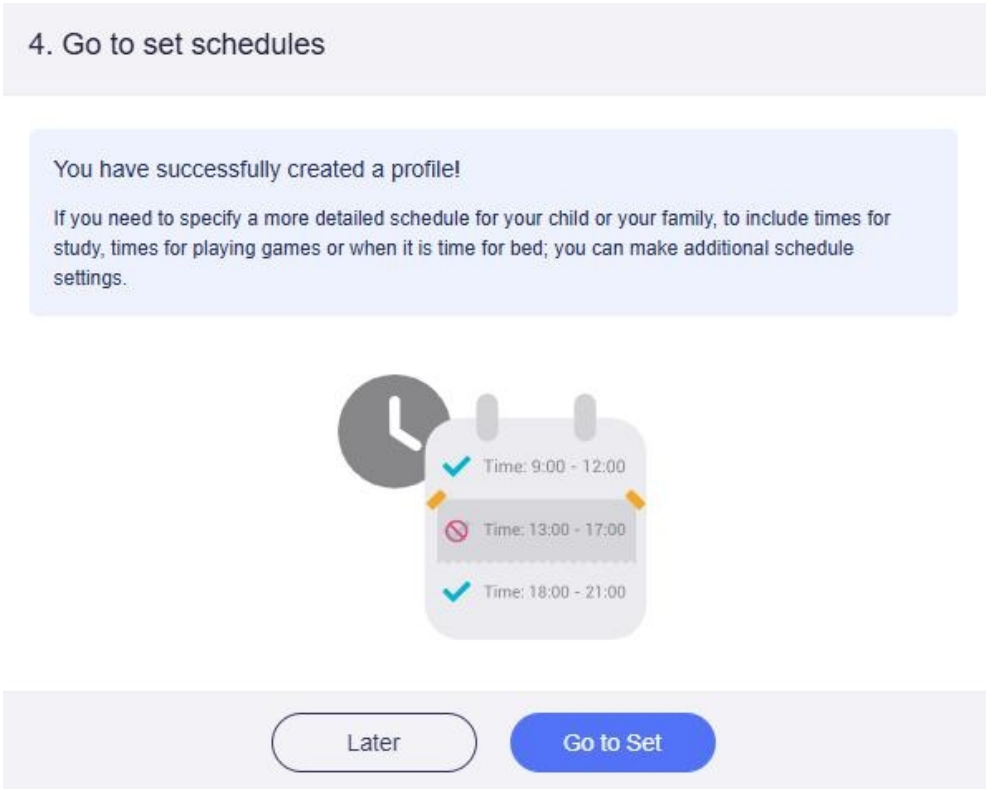
Erstellen Sie auf dieselbe Weise den zweiten Regelsatz. Legen Sie Namen, etwa Play, und Farbe fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.



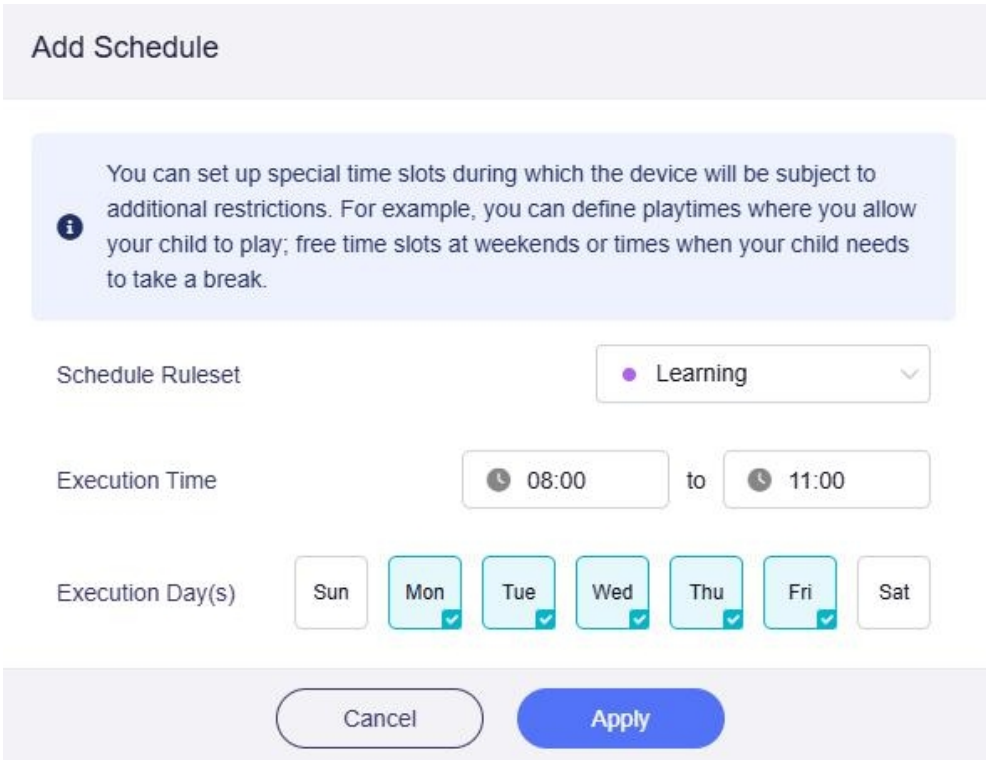
Nun sind insgesamt vier Regelsätze vorhanden. Wählen Sie **Block Internet Access** als **Default Ruleset** aus und klicken Sie auf **Finish**.



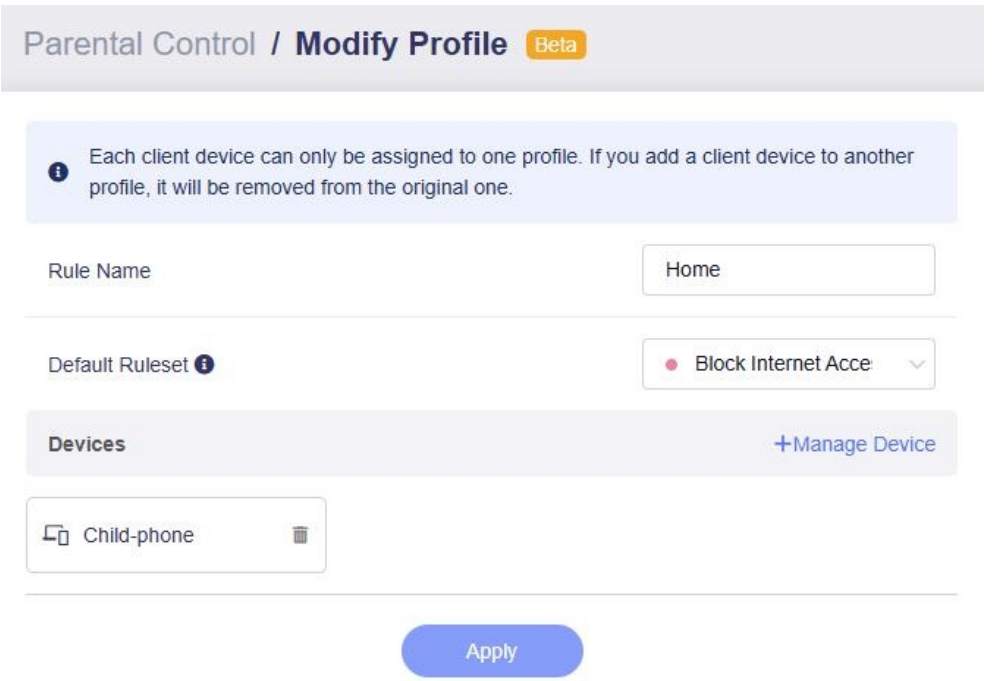
4. Erstellen Sie anschließend einen Zeitplan für Ihr Profil. Klicken Sie auf **Go to Set**.



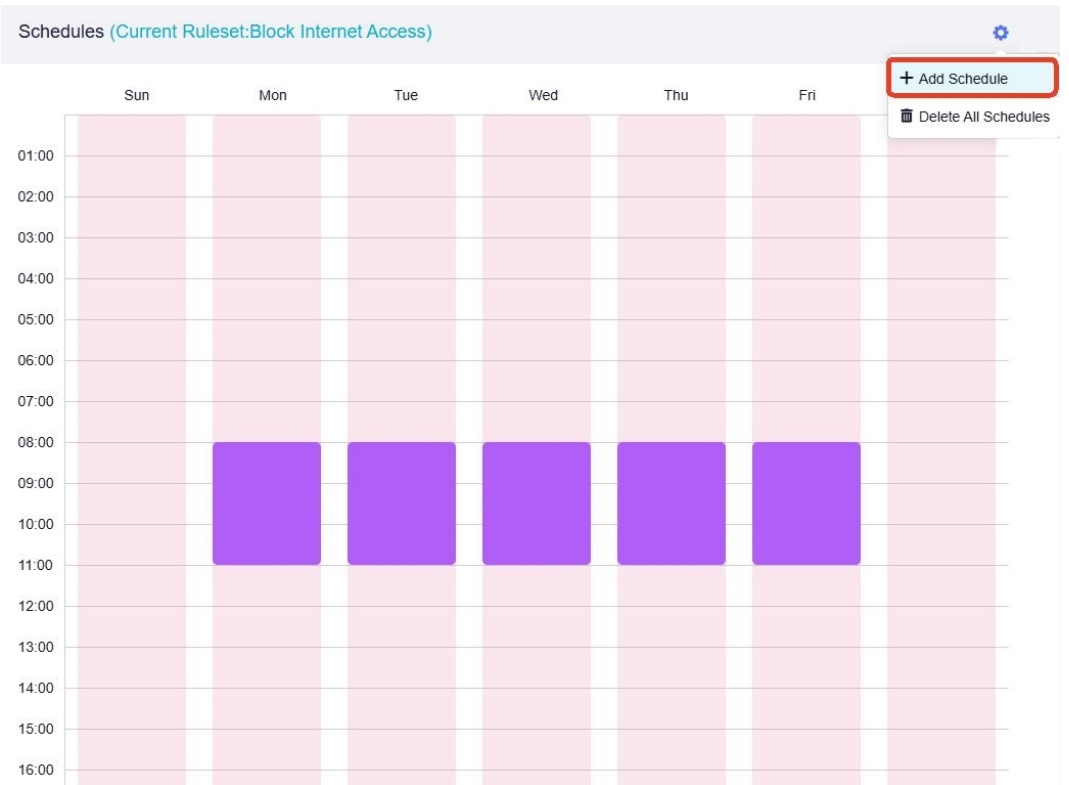
Fügen Sie den Regelsatz **Learning** zum Zeitplan hinzu. Legen Sie unter **Execution Time** an Wochentagen 08:00 bis 11:00 Uhr fest und klicken Sie auf **Apply**.



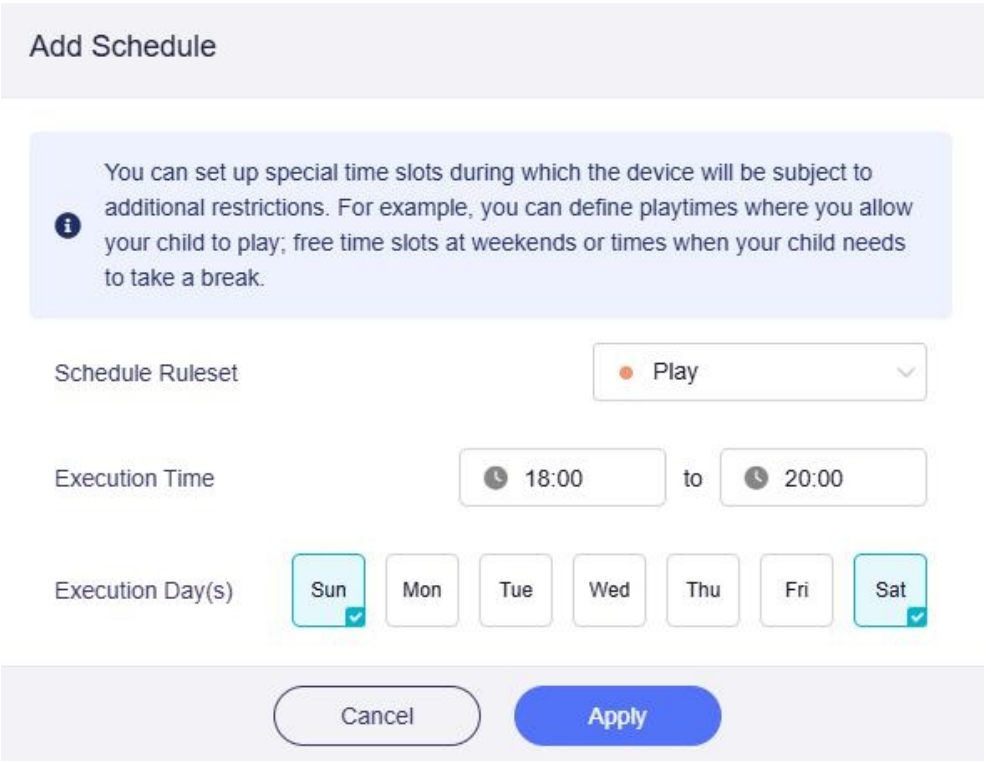
5. Sie gelangen zur Bearbeitungsseite des angelegten Profils.



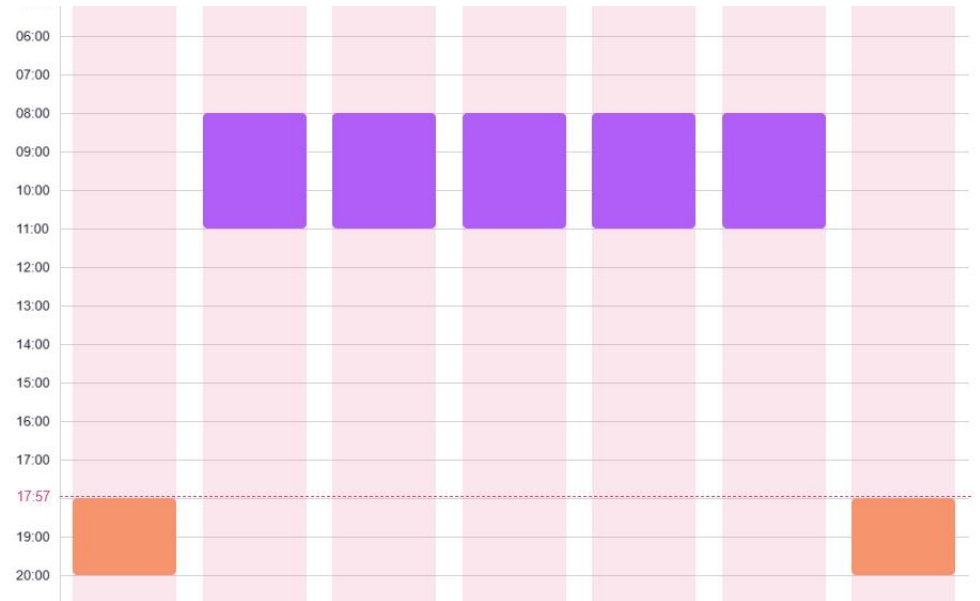
Unten sehen Sie den angelegten Zeitplan. Klicken Sie oben rechts auf das Zahnradsymbol und wählen Sie **Add Schedule**.



6. Fügen Sie den Regelsatz **Play** hinzu. Legen Sie unter **Execution Time** am Wochenende 18:00 bis 20:00 Uhr fest und klicken Sie auf **Apply**.



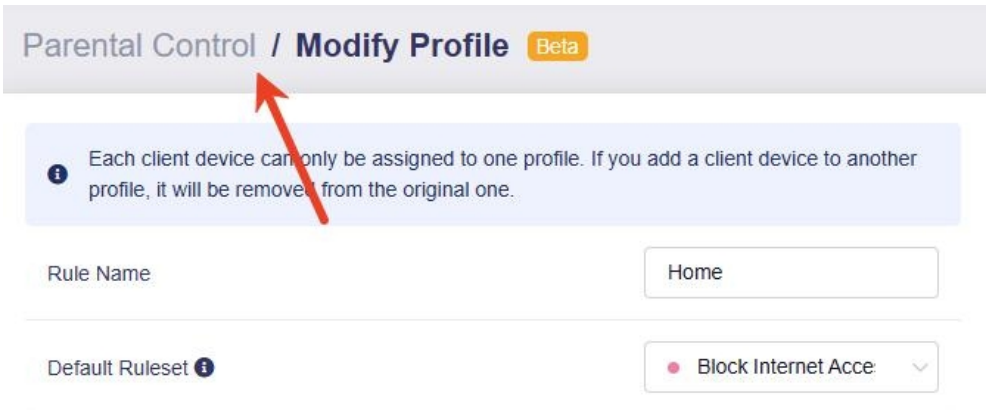
Der Regelsatz Play wird in den Zeitplan aufgenommen.



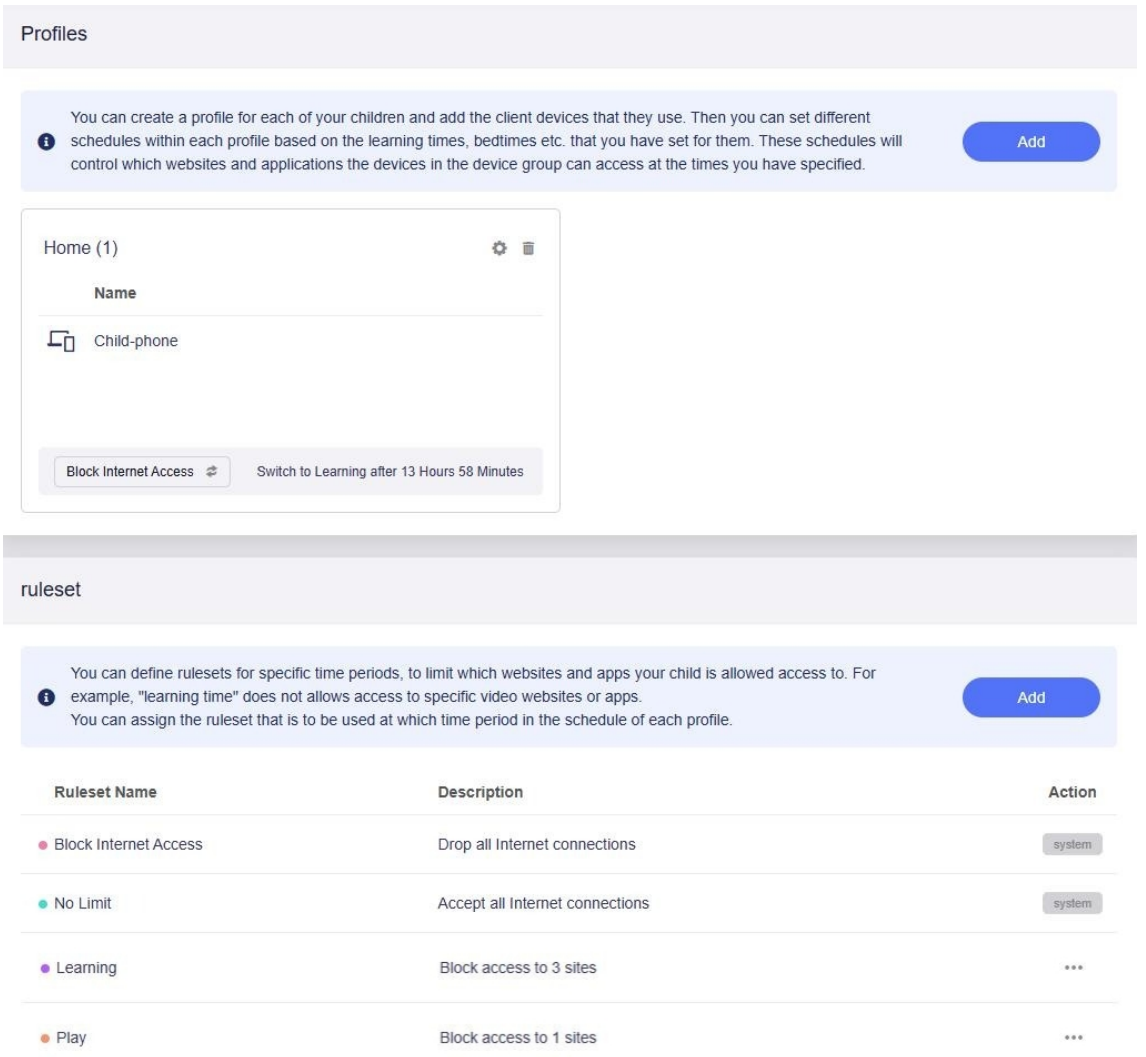
Tipps:

- Die rote gestrichelte Linie zeigt die aktuelle Uhrzeit an.
- Klicken Sie im Zeitplan auf einen Regelsatz, um seine Ausführungszeit zu ändern.

7. Klicken Sie oben auf **Parental Control**, um zur Seite der Kindersicherung zurückzukehren.



Sie sehen nun die fertige Konfiguration. Die Kindersicherung arbeitet gemäß dem Zeitplan. Bei Bedarf können Sie vorhandene Profile und Regelsätze bearbeiten oder weitere hinzufügen.



12.5.2 Fehlerbehebung

Falls Ihre Einstellungen nicht wirksam werden, prüfen Sie die folgenden möglichen Ursachen.

1. DNS-Cache.
   Browser und Betriebssysteme speichern DNS-Einträge zwischen. Dadurch können Konfigurationsänderungen verzögert wirksam werden. Leeren Sie den DNS-Cache, um die Änderungen sofort anzuwenden.
2. Der Zeitplan des Profils hat noch nicht begonnen.
3. Der eingegebene Domainname ist möglicherweise falsch.
   Die öffentliche Domain einer Webseite lässt sich leicht ermitteln. Die von Apps verwendeten API-Domains sind dagegen oft nicht öffentlich dokumentiert. Nutzen Sie ein Werkzeug zur Paketanalyse wie Wireshark oder recherchieren Sie die entsprechenden Domaininformationen.
   Um beispielsweise „www.google.com“ zu sperren, ist „google.com“ als Eintrag wirksamer als „www.google.com“.
4. Das Zielgerät verwendet bei jeder Verbindung eine zufällige MAC-Adresse. Dadurch greifen die Zugriffsregeln nicht. Deaktivieren Sie die zufällige MAC-Adresse auf dem Gerät und fügen Sie es erneut zum Profil hinzu.

12.6 ZeroTier

ZeroTier ist ein softwaredefiniertes VPN, das eine sichere, verschlüsselte Kommunikation zwischen Geräten über das Internet ermöglicht. Es erstellt ein privates virtuelles Netzwerk, in dem Geräte unabhängig von ihrem Standort oder der Netzwerktopologie wie im selben LAN kommunizieren können. ZeroTier lässt sich einfach einrichten und bedienen und bietet Ende-zu-Ende-Verschlüsselung, Netzwerksegmentierung und Netzwerkbrücken.

Mit der ZeroTier-Funktion kann Ihr GL.iNet-Router einem virtuellen ZeroTier-Netzwerk beitreten. Dadurch wird der Fernzugriff auf den Router sowie auf Ressourcen auf seiner WAN- und LAN-Seite möglich.

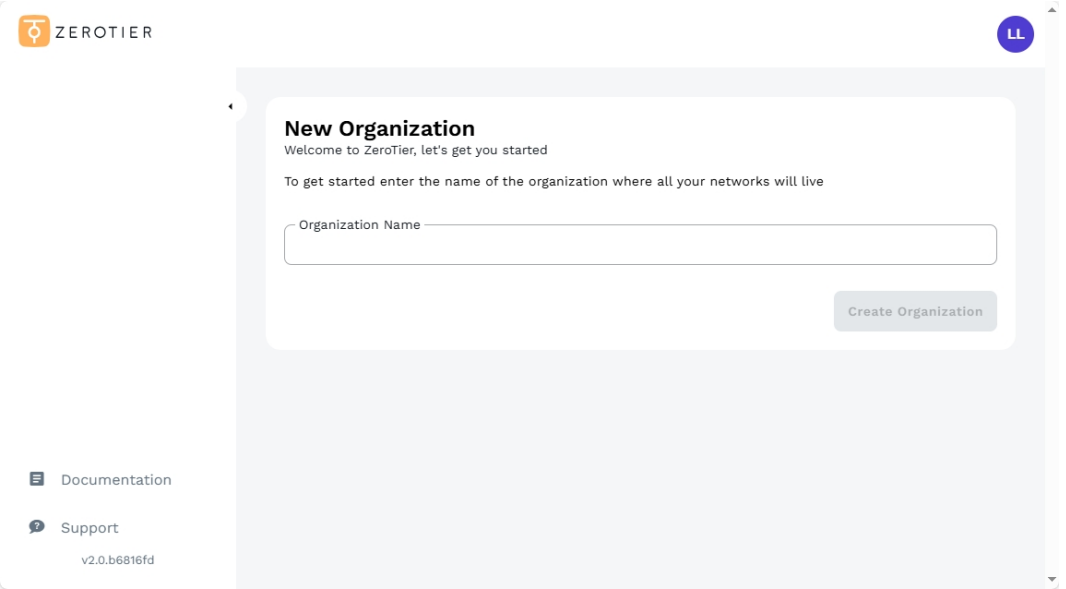
Hinweis:

1. Die gleichzeitige Verwendung von ZeroTier mit folgenden Funktionen oder Diensten wird wegen möglicher Routingkonflikte nicht empfohlen: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale und AstroWarp.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

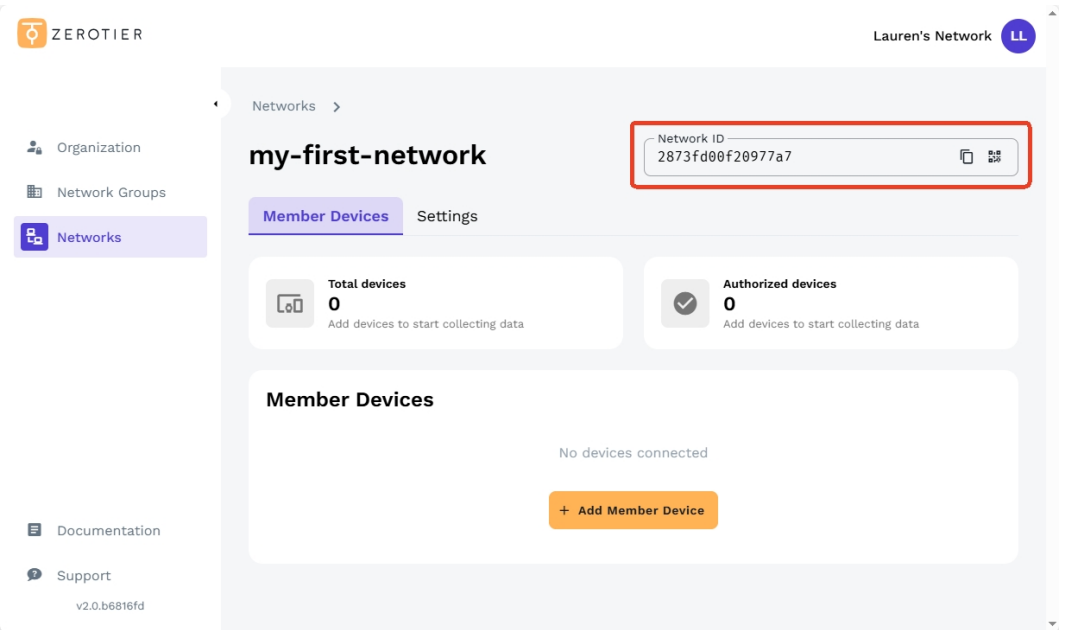
12.6.1 ZeroTier einrichten

ZeroTier Central ist in zwei Versionen verfügbar: New Central und Legacy Central.
Die folgenden Schritte verwenden New Central als Beispiel.

1. Rufen Sie die offizielle ZeroTier-Webseite auf und melden Sie sich mit Ihrem Konto an.
2. Erstellen Sie eine Organisation.

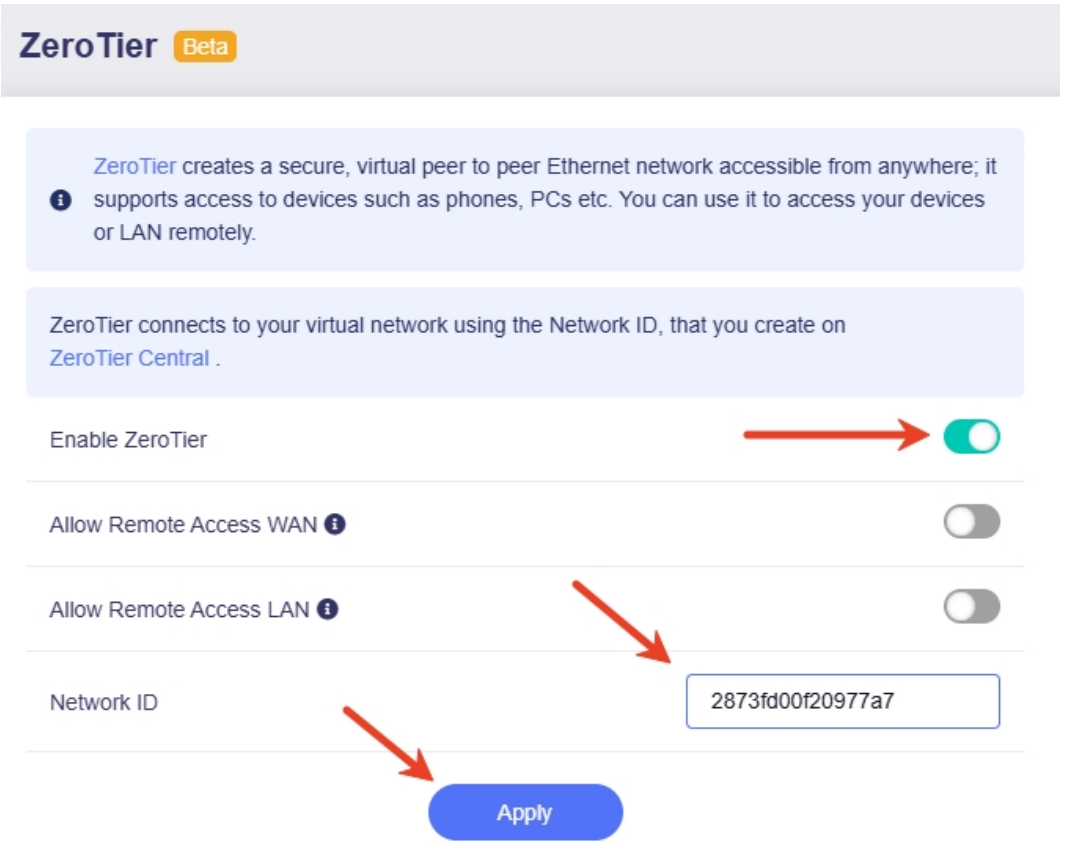


3. Wählen Sie einen Tarif aus. In diesem Beispiel verwenden wir den **Personal-Tarif** mit zehn Geräten, einem Netzwerkadministrator und einem Netzwerk. Wenn Sie mehr Netzwerke, zusätzliche Geräte, eigene Routen oder DNS-Einstellungen benötigen, wählen Sie einen kostenpflichtigen Tarif.
4. Ihr ZeroTier-Netzwerk ist nun erstellt.

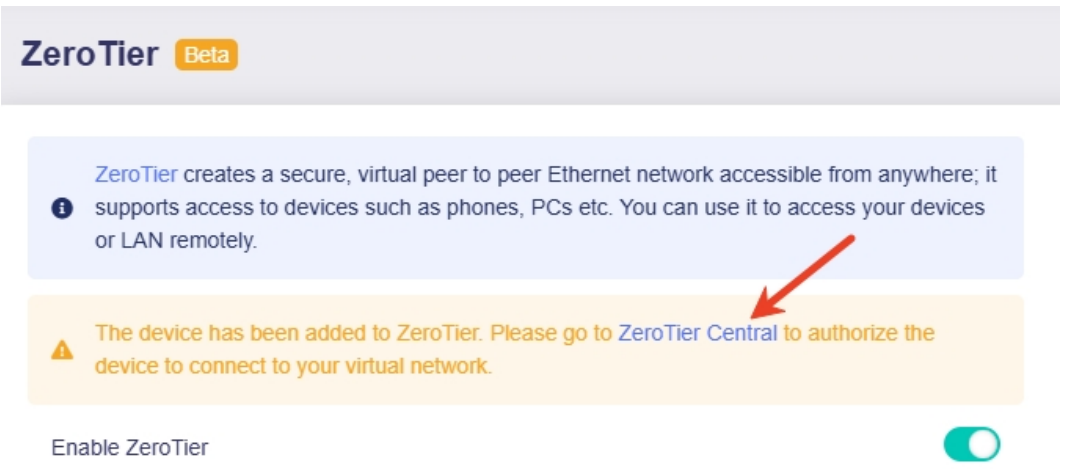


Notieren Sie die **Network ID** oben rechts. Diese besteht aus 16 Buchstaben und Ziffern und wird später benötigt, um weitere Geräte zu verbinden.

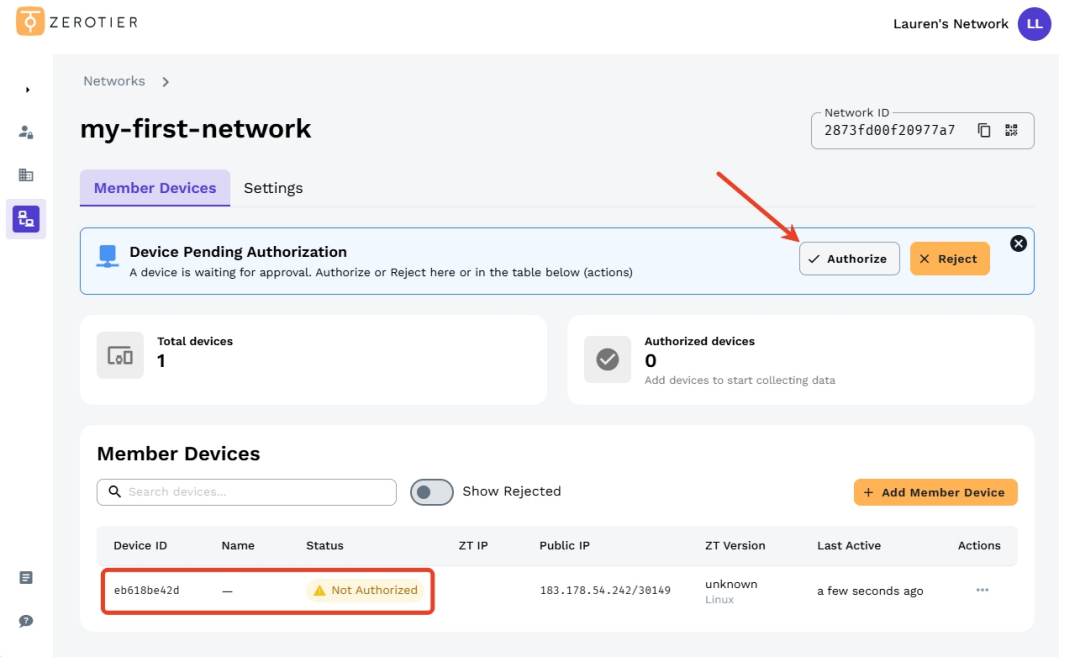
5. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **APPLICATIONS** > **ZeroTier**. Aktivieren Sie ZeroTier, geben Sie die **Network ID** ein und klicken Sie auf **Apply**.



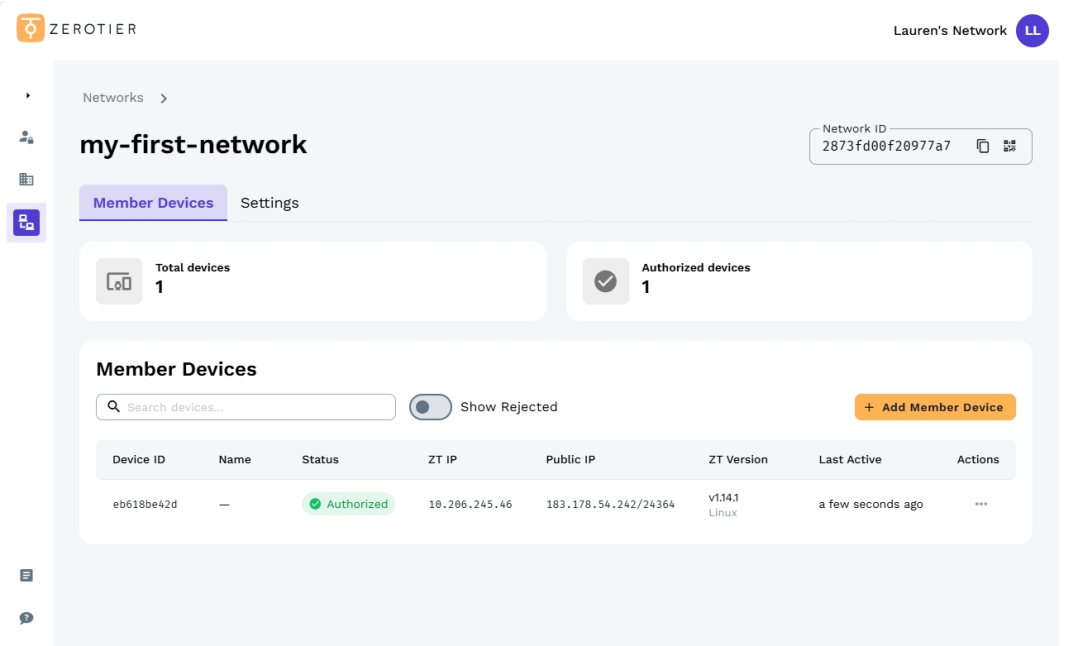
Nach kurzer Zeit erscheint der Hinweis, dass eine Autorisierung erforderlich ist. Klicken Sie auf den Link **ZeroTier Central**, um ZeroTier Central zu öffnen.



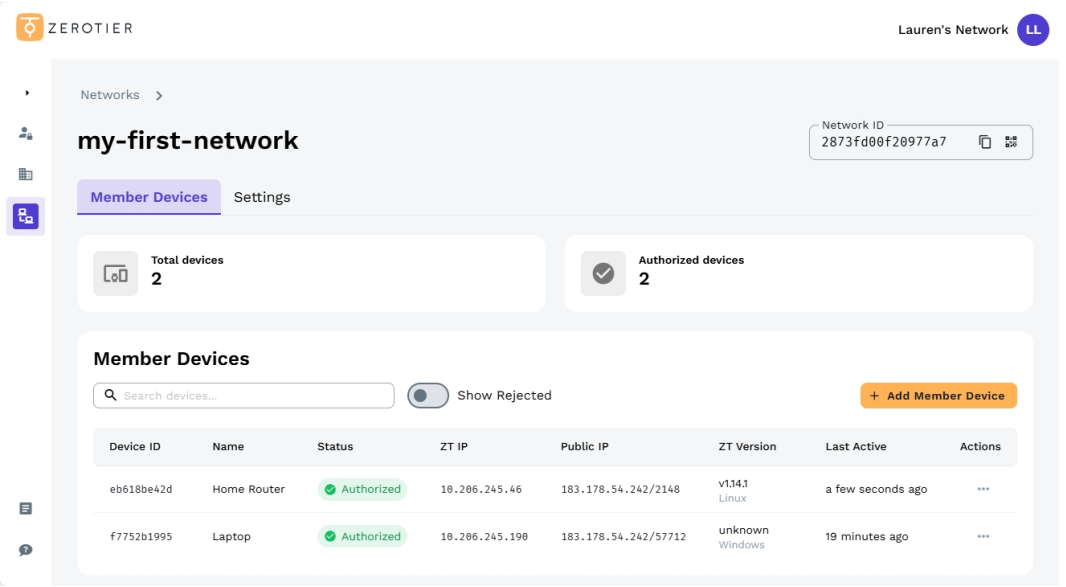
6. Suchen Sie in ZeroTier Central das ausstehende Gerät unter Pending und autorisieren Sie es.



Nach der Autorisierung erscheint die folgende Ansicht.

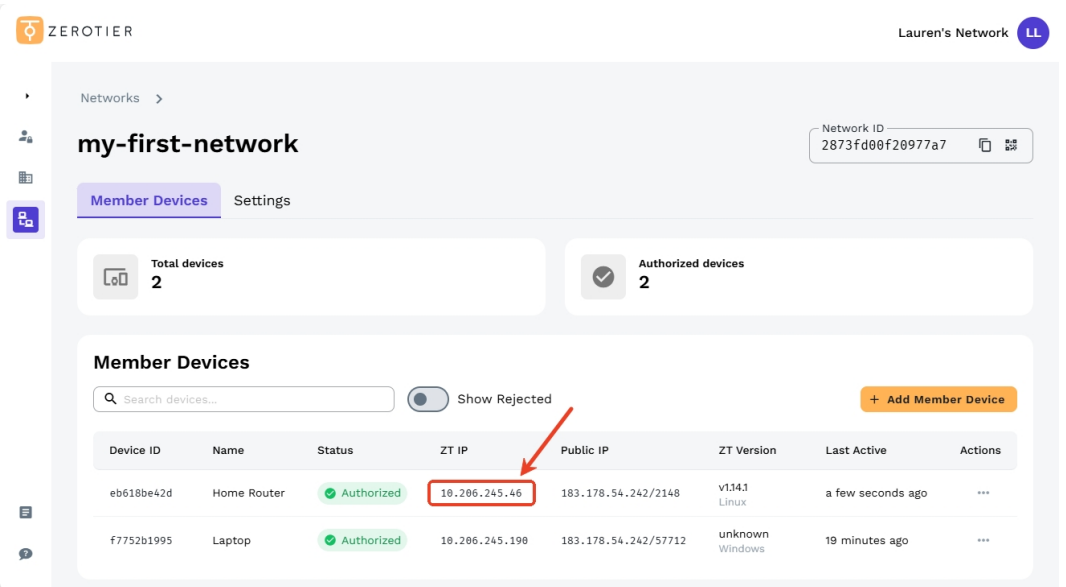


7. Fügen Sie anhand dieser Anleitung ein weiteres Gerät, etwa einen Computer oder ein Smartphone, zum selben ZeroTier-Netzwerk hinzu. Nach erfolgreichem Hinzufügen erscheint die folgende Ansicht **mit** Gerätedetails wie **Device ID, Name, Status,** Managed IP **und Public IP**.



Tipp: Über das Dreipunktsymbol rechts können Sie die Einstellungen eines Mitgliedsgeräts bearbeiten, darunter Gerätename, Managed IP(s) und erweiterte Einstellungen.

8. Klicken Sie auf die Managed **IP des Routers,** um sie zu kopieren.



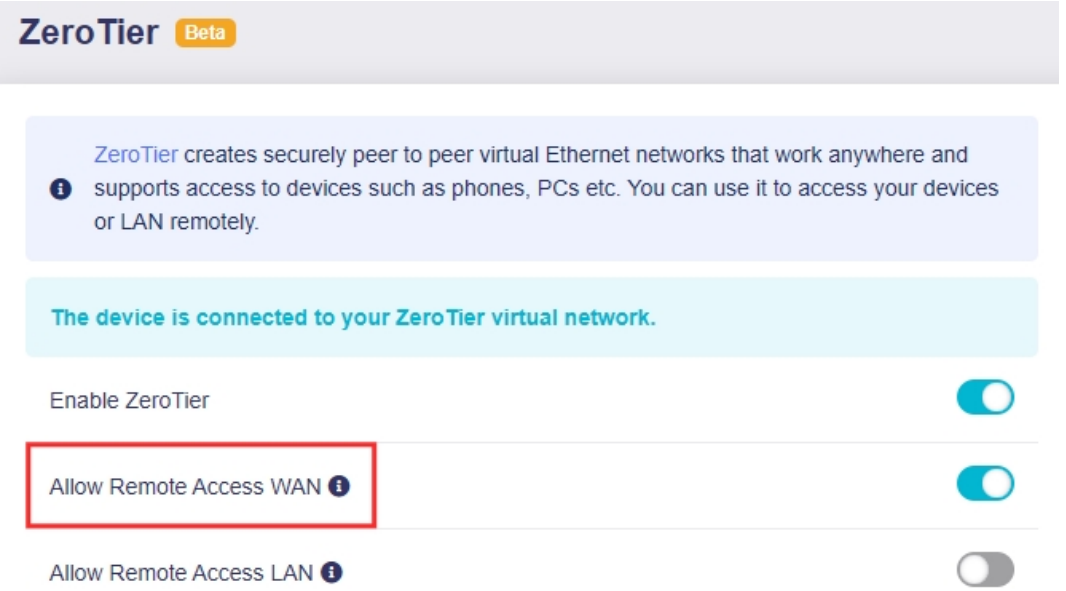
Über diese verwaltete IP-Adresse können Sie von einem Laptop im selben ZeroTier-Netzwerk auf den Router zugreifen.

9. Verbindung prüfen.

   Öffnen Sie auf dem Laptop im selben ZeroTier-Netzwerk einen Webbrowser und geben Sie die zuvor ermittelte Managed IP des Routers ein. Wenn Sie dessen Weboberfläche erreichen, funktioniert die ZeroTier-Verbindung.

12.6.2 Fernzugriff auf WAN erlauben

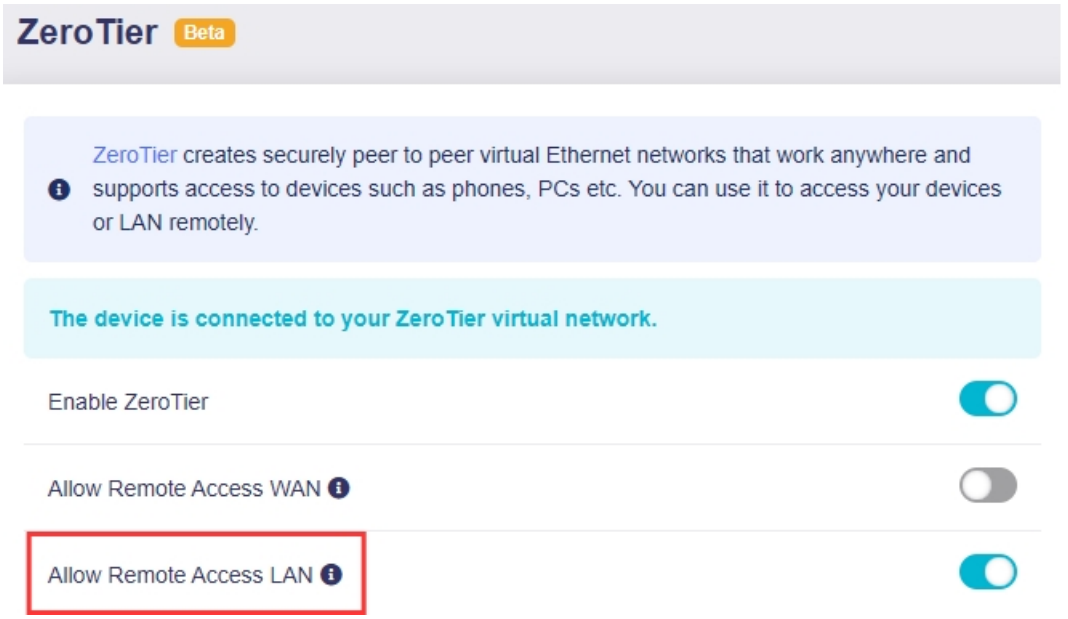
Diese Option erlaubt den Zugriff auf Ressourcen auf der WAN-Seite des Geräts über das virtuelle ZeroTier-Netzwerk. Weitere Informationen finden Sie hier.



Hinweis: Damit diese Funktion wirksam wird, müssen Sie dem ZeroTier-Netzwerk Routingregeln hinzufügen. In Legacy Central lässt sich eine eigene Route kostenlos einrichten. In New Central benötigen Sie dafür mindestens den Essential-Tarif. Informationen zu den Tarifen finden Sie hier.

12.6.3 Fernzugriff auf LAN erlauben

Diese Option erlaubt den Zugriff auf Ressourcen auf der LAN-Seite des Geräts über das virtuelle ZeroTier-Netzwerk. Weitere Informationen finden Sie hier.



Hinweis: Damit diese Funktion wirksam wird, müssen Sie dem ZeroTier-Netzwerk Routingregeln hinzufügen. In Legacy Central lässt sich eine eigene Route kostenlos einrichten. In New Central benötigen Sie dafür mindestens den Essential-Tarif. Informationen zu den Tarifen finden Sie hier.

12.7 Tailscale

Tailscale ist ein VPN-Dienst, mit dem Sie weltweit einfach und sicher auf Ihre persönlichen Geräte und Anwendungen zugreifen können. Weitere Informationen finden Sie hier.

Mit der Tailscale-Funktion kann Ihr GL.iNet-Router einem virtuellen Tailscale-Netzwerk beitreten. Dadurch wird der Fernzugriff auf den Router sowie auf Ressourcen auf seiner WAN- und LAN-Seite möglich.

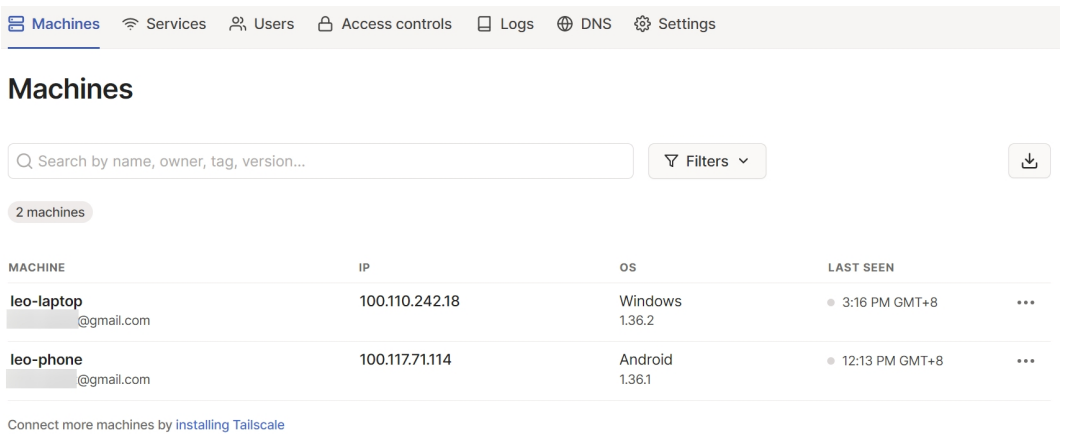
Hinweis:

1. Da Tailscale auf WireGuard basiert, wird die gleichzeitige Verwendung mit folgenden Funktionen oder Diensten wegen möglicher Routingkonflikte nicht empfohlen: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier und AstroWarp.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.
3. GL.iNet-Router können derzeit noch nicht als Exit-Nodes verwendet werden.

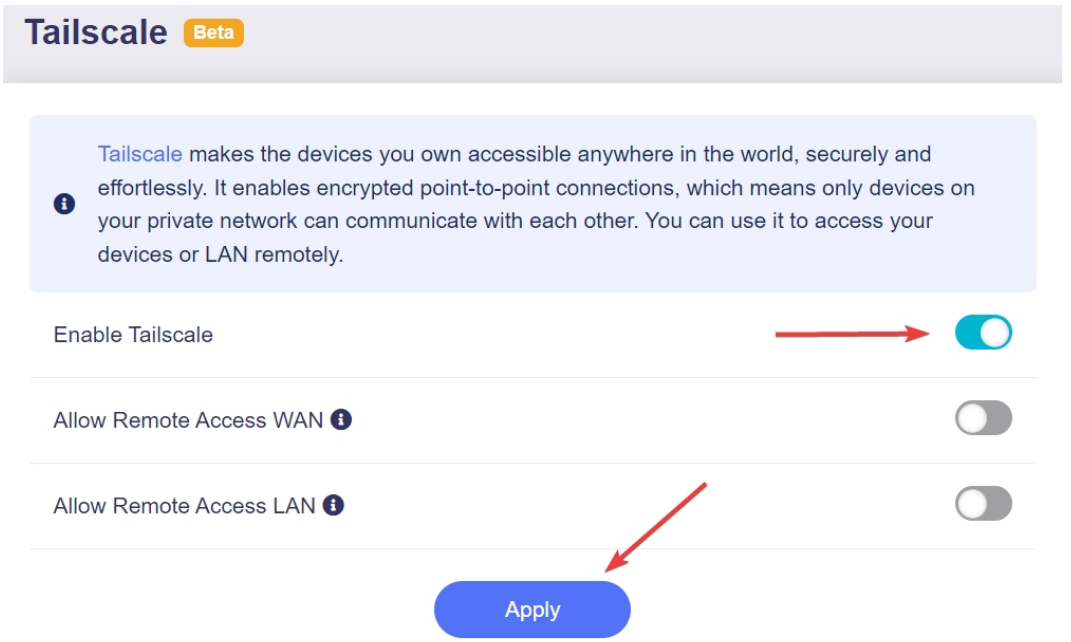
12.7.1 Tailscale einrichten

Das folgende Beispiel zeigt die Einrichtung eines Tailscale-Netzwerks mit GL-MT2500.

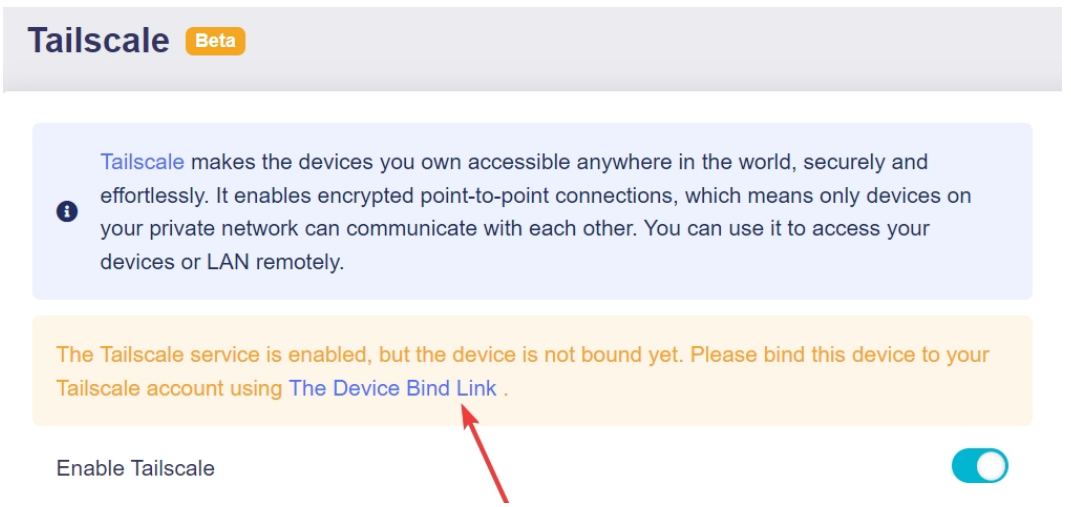
1. Registrieren Sie zunächst ein Tailscale-Konto und verknüpfen Sie zu Testzwecken ein oder zwei Geräte damit. Anschließend werden diese in der Tailscale-Konsole angezeigt.



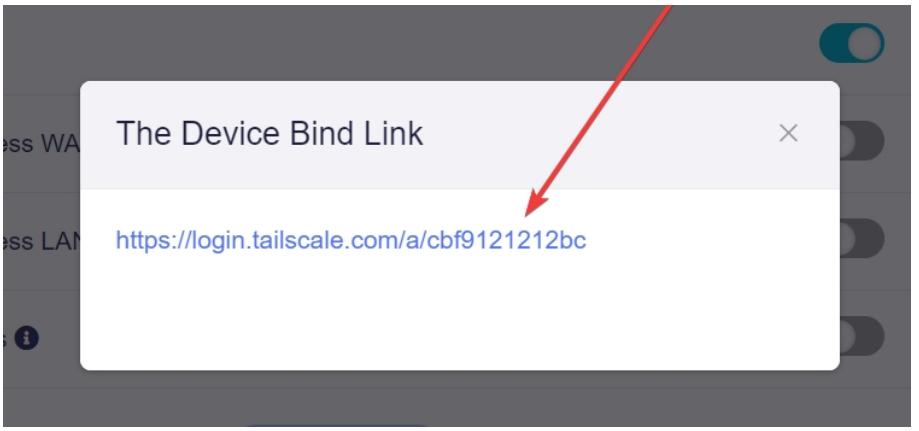
2. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Tailscale**. Aktivieren Sie **Enable Tailscale** und klicken Sie **auf Apply.**



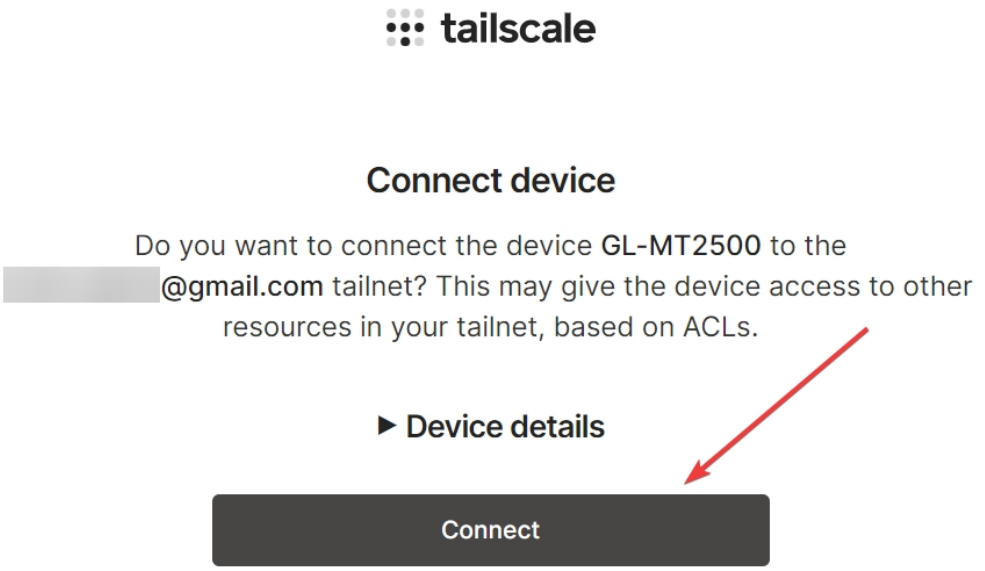
3. Sie werden aufgefordert, das Gerät zu verknüpfen. Klicken Sie auf **Device Bind Link**.



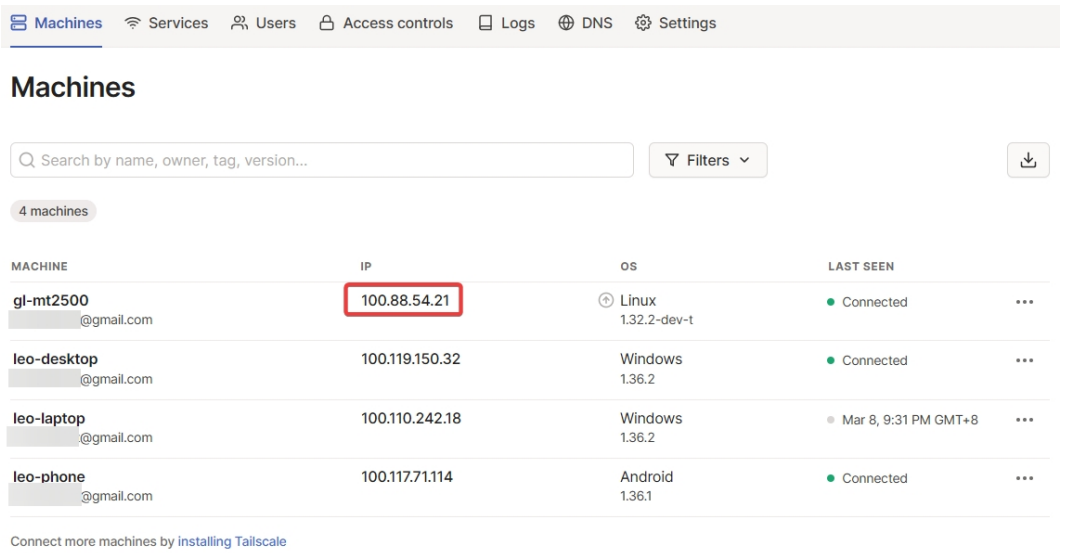
4. Klicken Sie im eingeblendeten Fenster auf den Link und melden Sie sich mit Ihrem Tailscale-Konto an.



5. Nach der Anmeldung müssen Sie das Gerät bestätigen. Klicken Sie auf **Connect**.



6. Sie werden anschließend zur Tailscale-Verwaltungskonsole weitergeleitet. Der Router wurde dem virtuellen Tailscale-Netzwerk hinzugefügt und ist über die virtuelle Tailscale-IP-Adresse 100.88.54.21 aus der Ferne erreichbar.

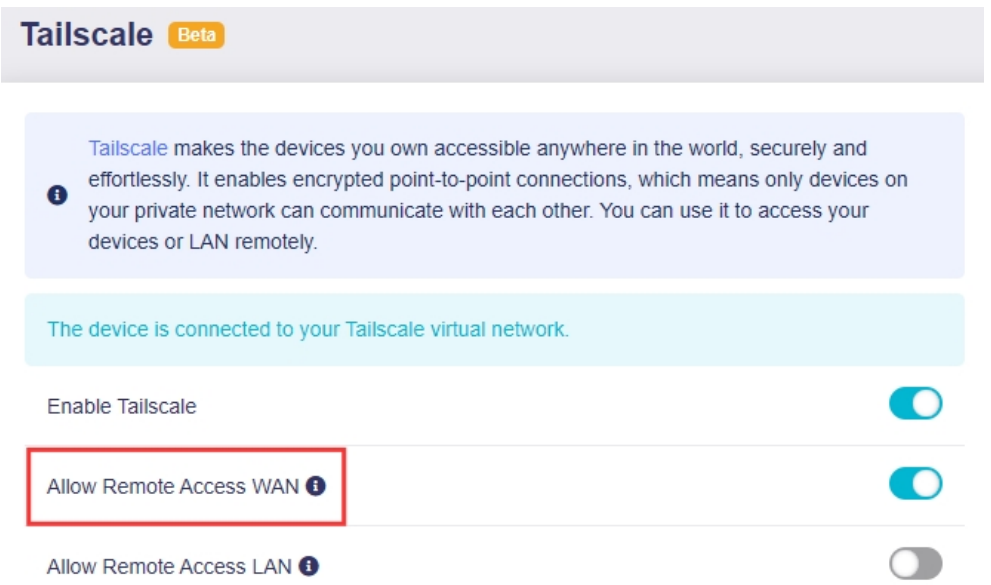


7. Verbindung prüfen.

   Öffnen Sie auf einem anderen Gerät im selben Tailscale-Netzwerk einen Webbrowser und geben Sie die virtuelle IP-Adresse des Routers ein. Wenn Sie seine Weboberfläche erreichen, funktioniert Tailscale. Alternativ können Sie die Verbindung mit ping oder durch eine SSH-Anmeldung am Routerterminal über die virtuelle IP-Adresse prüfen.

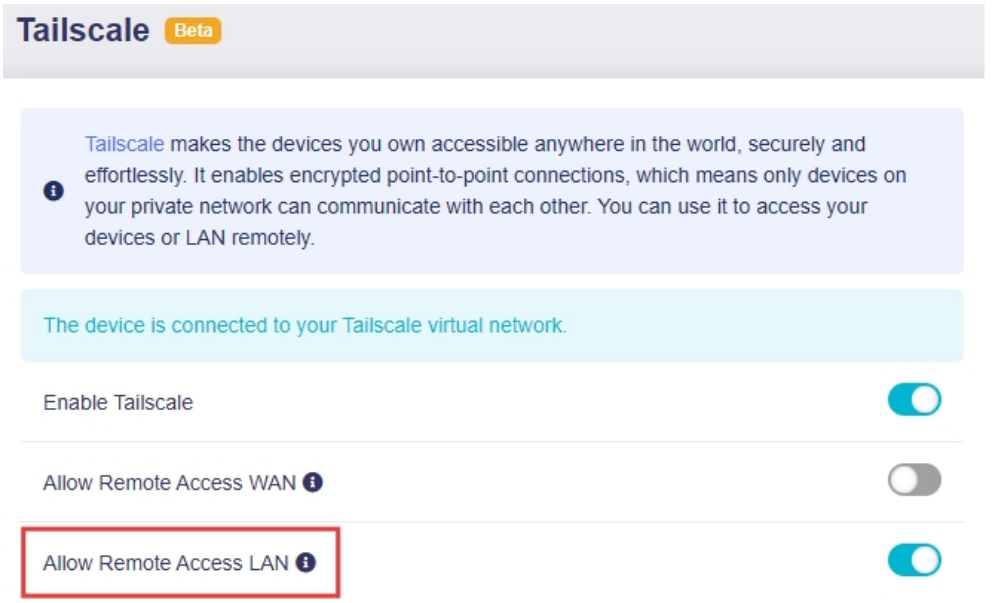
12.7.2 Fernzugriff auf WAN erlauben

Diese Option erlaubt den Zugriff auf Ressourcen auf der WAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk. Weitere Informationen finden Sie hier.



12.7.3 Fernzugriff auf LAN erlauben

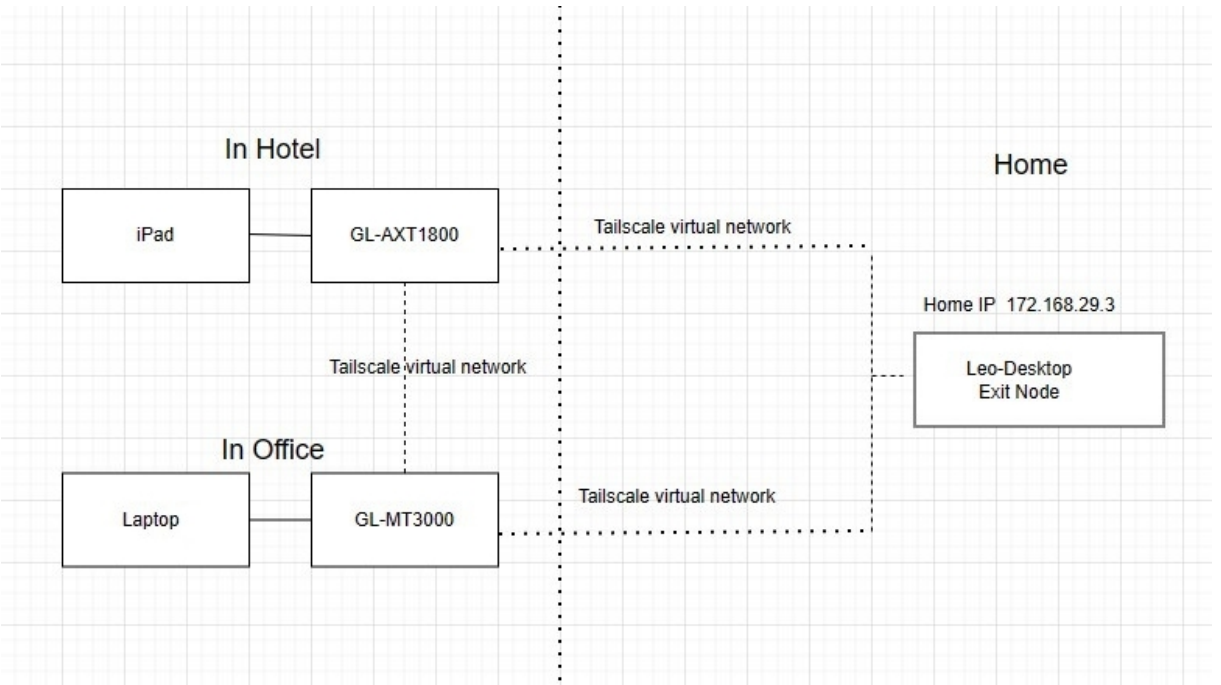
Diese Option erlaubt den Zugriff auf Ressourcen auf der LAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk. Weitere Informationen finden Sie hier.



12.7.4 Eigene Exit-Nodes

Standardmäßig arbeitet Tailscale als Overlay-Netzwerk: Es leitet nur Datenverkehr zwischen Geräten weiter, auf denen Tailscale läuft. Ihr öffentlicher Internetdatenverkehr, etwa beim Aufrufen von Google, wird nicht darüber übertragen.

Mitunter möchten Sie auch Ihren öffentlichen Internetdatenverkehr durch Tailscale leiten. Wenn Sie unterwegs oder im Ausland sind und beispielsweise Onlinebanking nutzen möchten, das nur in Ihrem Heimatland verfügbar ist, können Sie Ihren heimischen Desktopcomputer mit öffentlicher IP-Adresse als Exit-Node einrichten. Andere Geräte im selben Tailnet, etwa GL-AXT1800 und GL-MT3000 in der folgenden Abbildung, können ihren Datenverkehr dann über diesen Computer leiten. So wird Ihr gesamter öffentlicher Internetdatenverkehr über den Exit-Node weitergeleitet.



Ein Exit-Node leitet den ausgehenden Internetverkehr Ihrer Tailnet-Geräte weiter und übernimmt damit die Rolle eines VPN-Servers. Bei einer Verbindung über einen Exit-Node scheint Ihr gesamter Internetverkehr außerhalb von Tailscale von dessen Standort zu stammen. So können Sie regionsgebundene Inhalte erreichen und Ihre Privatsphäre verbessern. Das Gerät, das diese Weiterleitung übernimmt, wird als „Exit-Node“ bezeichnet. Weitere Informationen finden Sie hier.

Hinweis: Wenn der DNS-Server des Routers eine private IP-Adresse hat, die nur im lokalen Netzwerk erreichbar ist, kann die Internetverbindung bei Nutzung eines Exit-Nodes ausfallen. Legen Sie deshalb für den Router manuell einen öffentlichen DNS-Server fest, etwa 8.8.8.8.

Kapitel 13

Netzwerk

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

13.1 Portweiterleitung

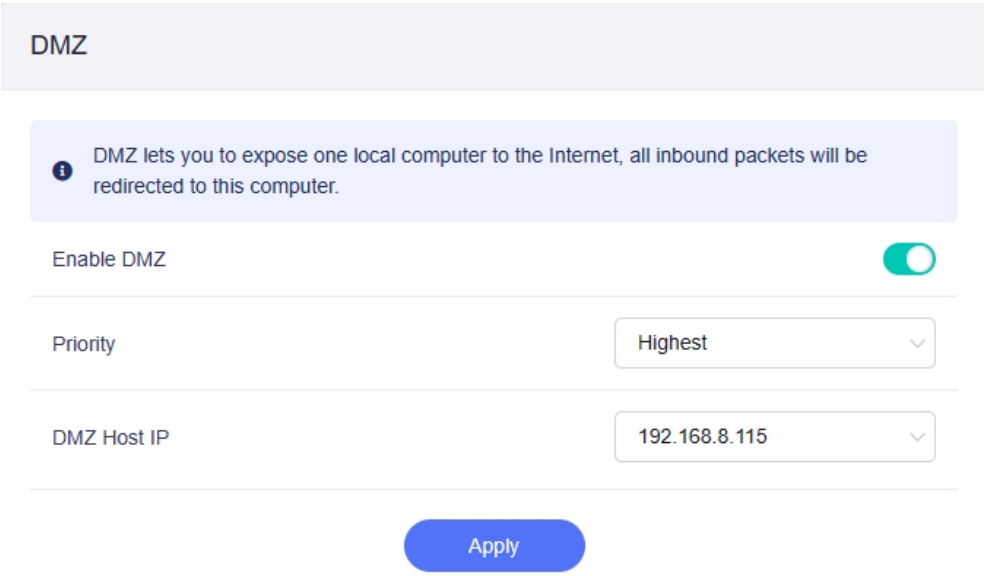
Portweiterleitung leitet externe Anfragen an bestimmte Geräte in Ihrem lokalen Netzwerk weiter. Die Seite Port Forwarding umfasst zwei zentrale Funktionen: **DMZ** für den direkten vollständigen Zugriff auf ein einzelnes Gerät und **Port Forwarding** für den gezielten Zugriff auf bestimmte Geräteports.

13.1.1 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 Ihres Routers an und öffnen Sie **NETWORK** > **Port Forwarding** > **DMZ**.
2. Aktivieren Sie **Enable DMZ**. Wählen Sie Priority und DMZ Host IP aus den Dropdown-Listen aus und klicken Sie auf **Apply**.



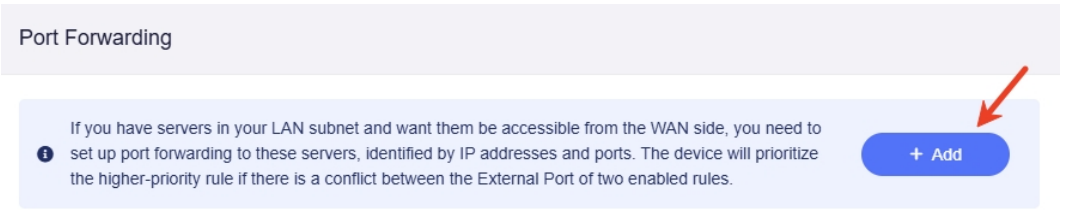
- **Priority**: Wählen Sie Highest oder Lowest. Hat DMZ eine höhere Priorität als die Portweiterleitungsregeln, werden alle Portweiterleitungsregeln außer Kraft gesetzt. Andernfalls werden Anfragen nur dann an das DMZ-Endgerät weitergeleitet, wenn für den angefragten Port keine Portweiterleitungsregel besteht.
- **DMZ Host IP**: Wählen Sie die interne IP-Adresse des Geräts, das alle eingehenden Pakete erhalten soll.

13.1.2 Portweiterleitung

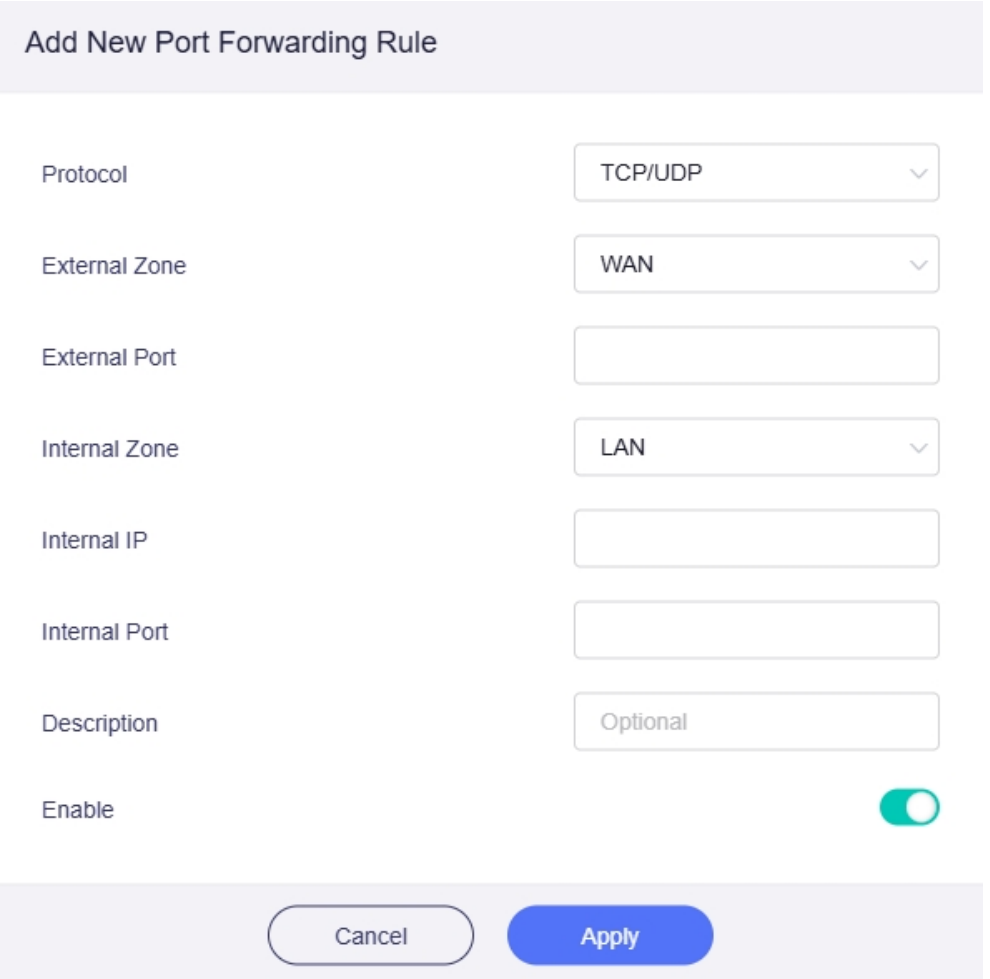
Portweiterleitungen ermöglichen entfernten Computern die Verbindung mit einem lokalen Computer oder Server hinter der LAN-Firewall, beispielsweise einem Web- oder FTP-Server.

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

1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Port Forwarding** > **Port Forwarding**. Klicken Sie auf **Add**.



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



- **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 und LAN.
- **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, 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.

- **Description**: Legen Sie einen Namen fest oder geben Sie eine Beschreibung für die Portweiterleitungsregel ein (optional).
- **Enable**: Aktiviert oder deaktiviert diese Regel.

13.2 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.

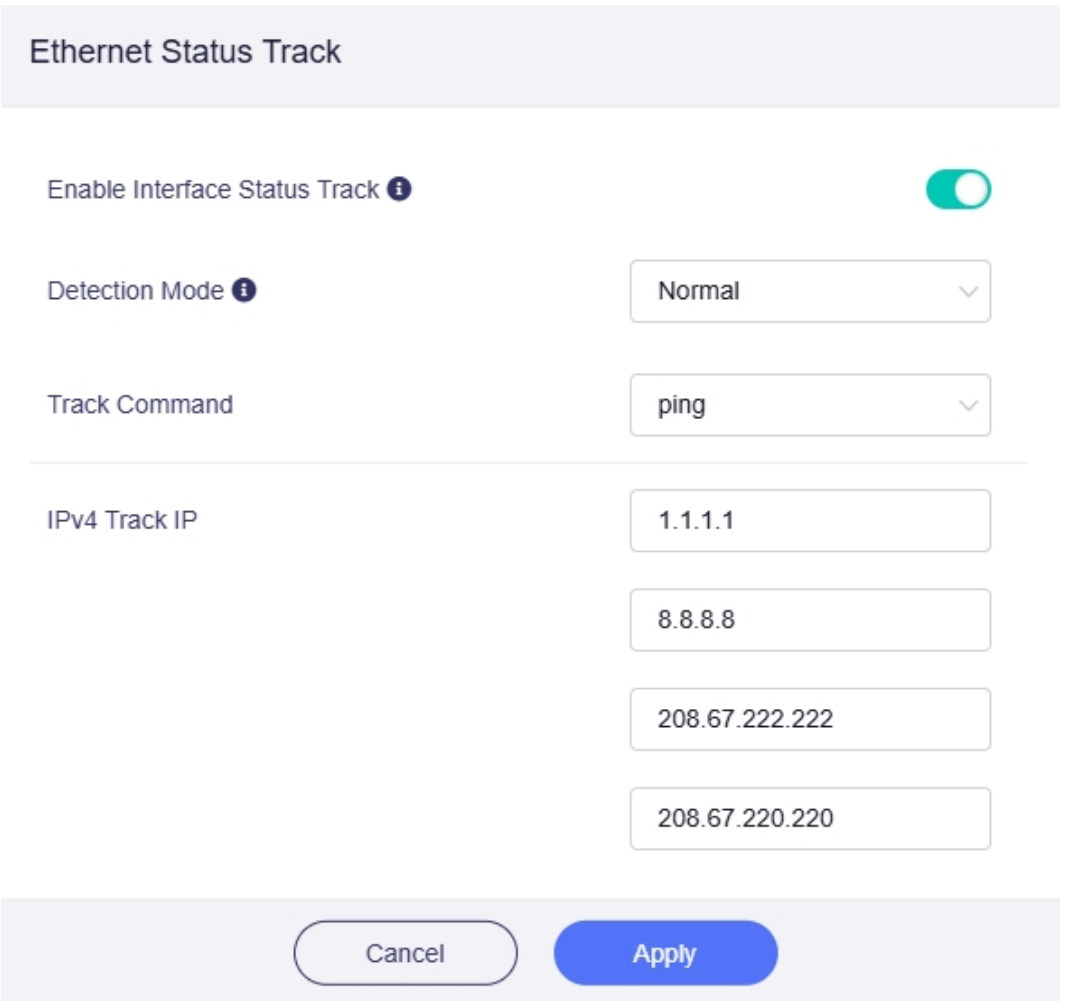
13.2.1 Schnittstellenstatus überwachen

Brume 2 verfügt über zwei Schnittstellen für den Internetzugang: Ethernet und Tethering. Mit dem Befehl ping überwacht er die Verbindung zur Ziel-IP-Adresse und ermittelt so, ob die 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 Einstellungen zur Statusüberwachung der jeweiligen Netzwerkschnittstelle zu öffnen.

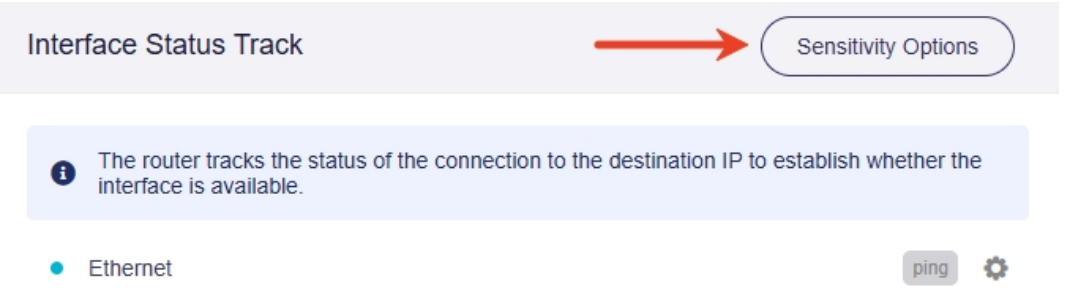
Nachfolgend sind die Einstellungen zur Statusüberwachung der Ethernet-Schnittstelle dargestellt. Für die andere Schnittstelle gilt das gleiche Konfigurationsprinzip.



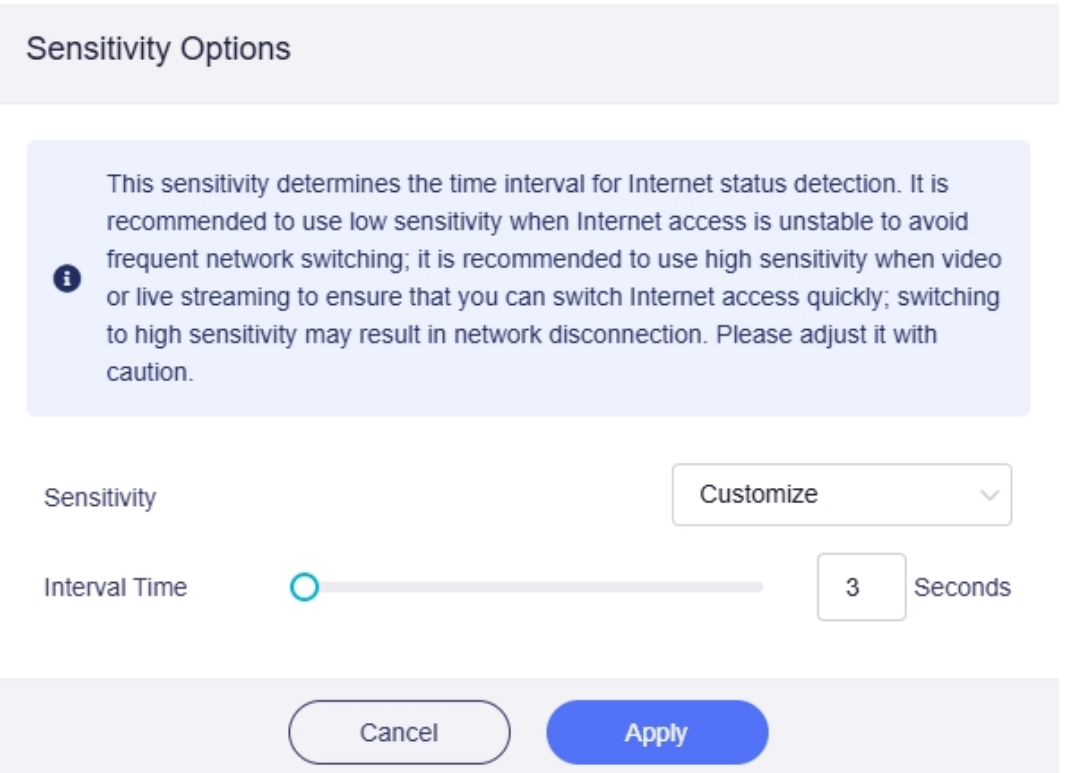
- **Enable Interface Status Track**: Standardmäßig aktiviert. Bei deaktivierter Überwachung beurteilt der Router den Schnittstellenstatus anhand physischer Merkmale, etwa ob ein Ethernetkabel angeschlossen ist.
- **Detection Mode**: Diese Funktion wurde in Firmware v4.5 als Low Data Mode eingeführt und in Firmware v4.7 in Detection Mode umbenannt. Es stehen drei Modi zur Verfügung: Normal Mode, Low Data Mode und Strict Mode.
  - **Normal Mode**: Dieser Modus wird standardmäßig verwendet.
  - **Low Data Mode**: Die Verbindungsüberwachung wird nur bei einem Netzwerkfehler an der Schnittstelle ausgelöst. Verwenden Sie diesen Modus bei einem Tarif mit begrenztem Datenvolumen. Beachten Sie, dass der erneute Verbindungsaufbau nach einem Ausfall etwas länger dauern kann als im Normalmodus. Standardmäßig ist dieser Modus nur für die Mobilfunkschnittstelle aktiviert.

    - **Strict Mode**: Der Schnittstellenstatus wird ausschließlich anhand der Ergebnisse eines an eine öffentliche IP-Adresse gesendeten Prüfbefehls bestimmt.
- **Track Command**: Der Befehl ping prüft die Verbindung zur Ziel-IP-Adresse und damit die Verfügbarkeit der Schnittstelle.
- **IPv4 Track IP**: Passen Sie bei Bedarf die für die Überwachung verwendeten IPv4-Adressen an.

Klicken Sie oben rechts auf **Sensitivity Options**.



Sie können das Prüfintervall über die Stufen Low, Medium oder High auswählen oder individuell festlegen. Der einstellbare Bereich reicht von 0,5 bis 90 Sekunden.



Tipps: Bei einem stabilen Netzwerk empfiehlt sich eine hohe Empfindlichkeit, damit bei einem Verbindungsausfall schnell umgeschaltet wird. Dies eignet sich beispielsweise für Videos, Livestreams oder Spiele. Bei einem instabilen Netzwerk empfiehlt sich eine niedrige Empfindlichkeit, um häufige Wechsel und fehlgeschlagene Verbindungen zu vermeiden. Dies eignet sich beispielsweise zum Herunterladen zwischengespeicherter Dateien.

Hinweis: Beim Umschalten auf eine hohe Empfindlichkeit kann die Netzwerkverbindung gelegentlich unterbrochen werden. Ändern Sie die Einstellung daher mit Bedacht.

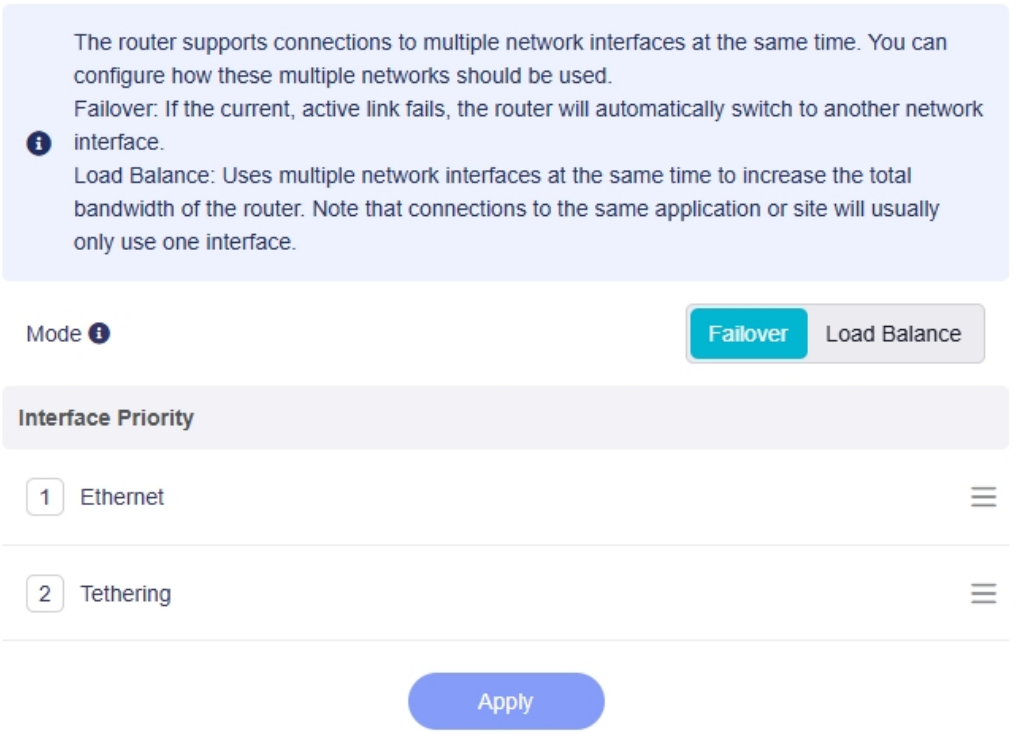
13.2.2 Multi-WAN-Modus

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.

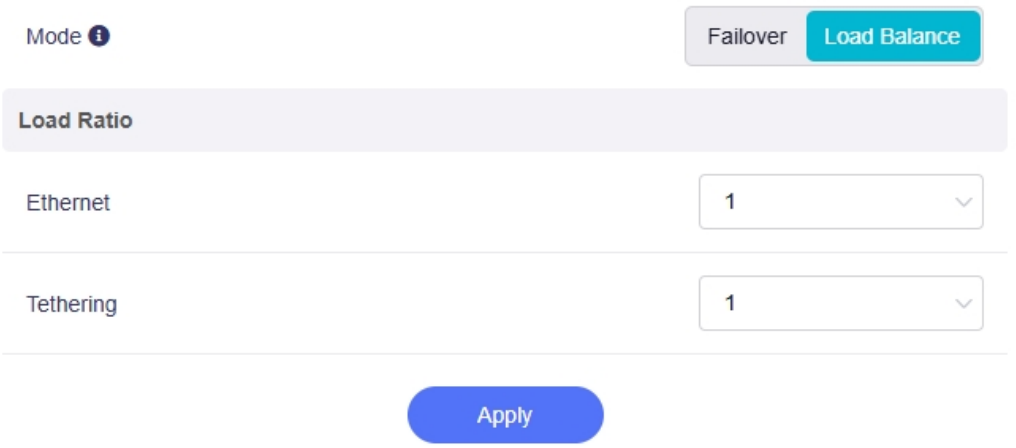
Sie können jeder Schnittstelle eine Priorität zuweisen. Fällt die verwendete Schnittstelle aus, wechselt der Router zur verfügbaren Schnittstelle mit der nächsthöheren Priorität. Sobald eine Verbindung mit höherer Priorität wieder verfügbar ist, wechselt er automatisch zurück.


The router supports connections to multiple network interfaces at the same time. You can configure how these multiple networks should be used.
Failover: If the current, active link fails, the router will automatically switch to another network interface.
Load Balance: Uses multiple network interfaces at the same time to increase the total bandwidth of the router. Note that connections to the same application or site will usually only use one interface.
Mode
Failover
Load Balance
Interface Priority
1
Ethernet
2
Tethering
Apply

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 das Verhältnis zwischen den einzelnen Netzwerkschnittstellen. Das System weist neue Verbindungen anhand dieses Verhältnisses den Schnittstellen zu. Wenn der Router beispielsweise gleichzeitig mit zwei Netzwerken, etwa Ethernet und Tethering, verbunden ist und beide Schnittstellen Internetzugang bieten, teilen sich bei aktivierter Lastverteilung und einem Verhältnis von 1:1 die vier Schnittstellen die Netzwerkbandbreite gleichmäßig. Das System verteilt neue Verbindungen entsprechend dem eingestellten Lastverhältnis auf diese vier Schnittstellen.



Sie können das Lastverhältnis bei Bedarf anpassen. Verfügt Ethernet beispielsweise über 100 Mbit/s und Tethering über 200 Mbit/s, stellen Sie für Ethernet den Wert 1 und für Tethering den Wert 2 ein. Das System verteilt neue Verbindungen dann im Verhältnis 1:2 auf die beiden Schnittstellen. Ethernet übernimmt somit halb so viele Verbindungen wie Tethering. Im Gegensatz zum Failover-Modus 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.

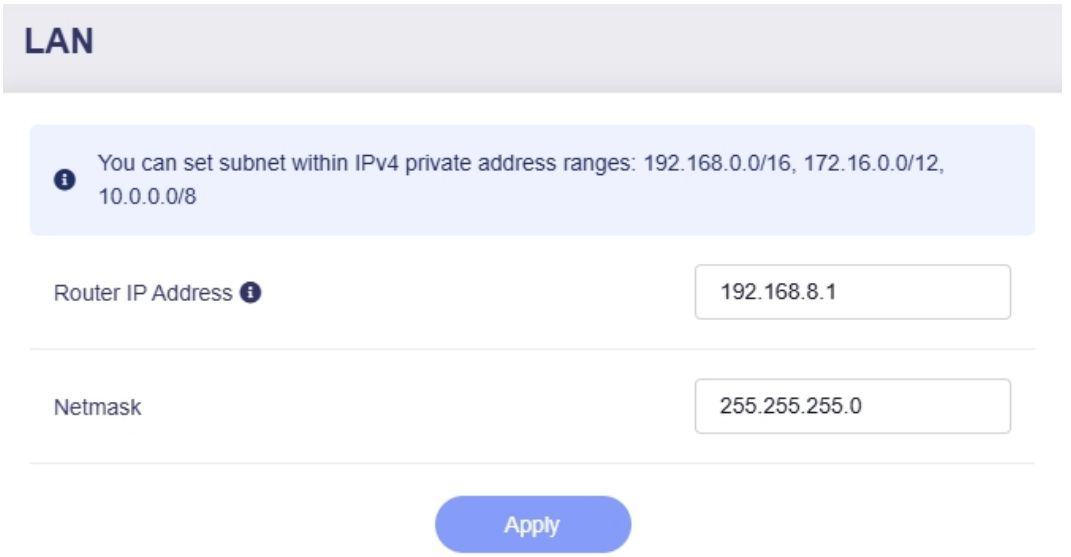
13.3 LAN

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 Grundeinstellungen, den DHCP-Server und die Adressreservierung.

13.3.1 Grundeinstellungen

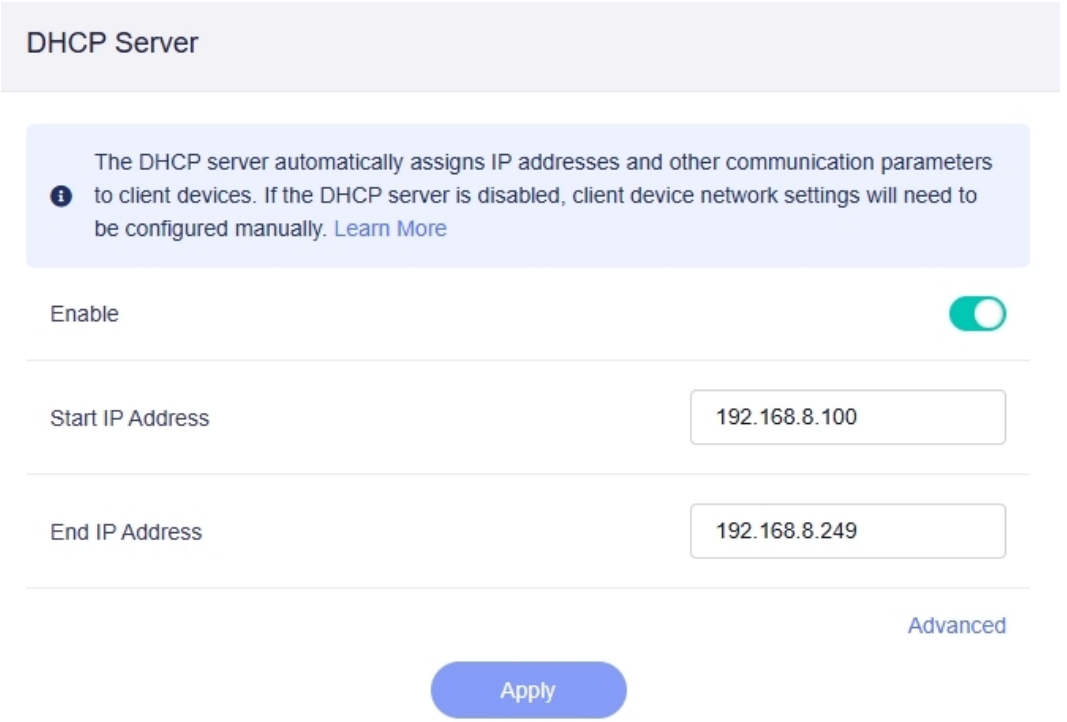
Zu den Grundeinstellungen gehören die IP-Adresse des Routers und die Netzmaske. Sie können ein Subnetz innerhalb der privaten IPv4-Adressbereiche 192.168.0.0/16, 172.16.0.0/12 oder 10.0.0.0/8 festlegen.



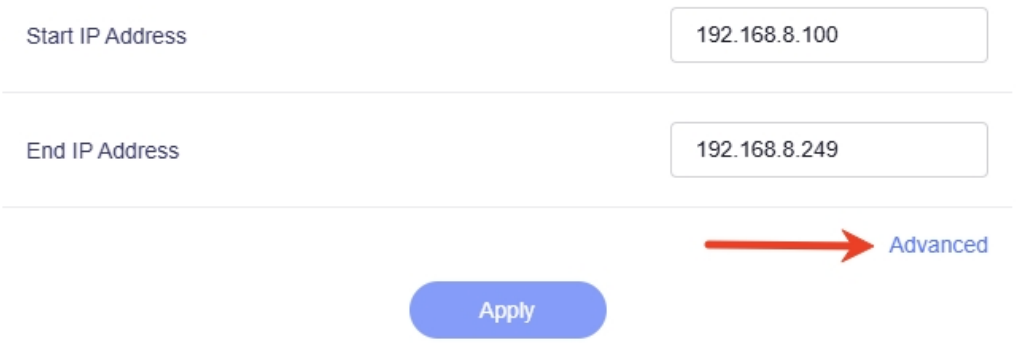
- **Router IP Address**: Über diese Adresse rufen Sie die Weboberfläche im Browser auf. Standardmäßig lautet sie 192.168.8.1. Bei einem Konflikt mit dem vorgeschalteten Netzwerk können Sie sie ändern.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.

13.3.2 DHCP-Server

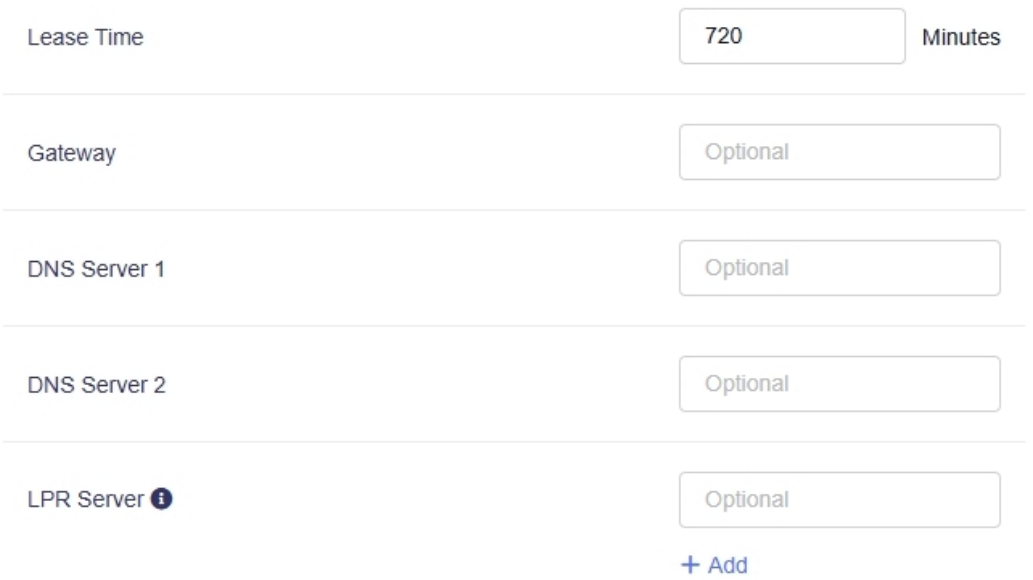
Der DHCP-Server weist jedem verbundenen Endgerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Auf GL.iNet-Routern ist er standardmäßig aktiviert und vergibt Adressen von 192.168.8.100 bis 192.168.8.249. Diesen Adressbereich können Sie bei Bedarf anpassen.



Klicken Sie unten rechts auf **Advanced**.



Hier konfigurieren Sie erweiterte Einstellungen wie Lease Time, Gateway, DNS-Server und LPR-Server.



- **Lease Time**: Die Zeitspanne, für die ein Gerät eine per DHCP zugewiesene IP-Adresse verwenden darf.
- **Gateway**: Die Routerkomponente, die Datenverkehr zwischen dem lokalen Netzwerk und externen Netzwerken wie dem Internet weiterleitet.
- **DNS Server 1**: Der primäre Server, der Domainnamen in IP-Adressen auflöst.
- **DNS Server 2**: Ein Ersatzserver für die Namensauflösung, falls der primäre DNS-Server ausfällt.
- **LPR Server**: Ein Line Printer Remote Server verwaltet Druckaufträge und ermöglicht Netzwerkgeräten, Druckanfragen an entfernte Drucker zu senden. Sie können mehrere LPR-Ports für Drucker konfigurieren.

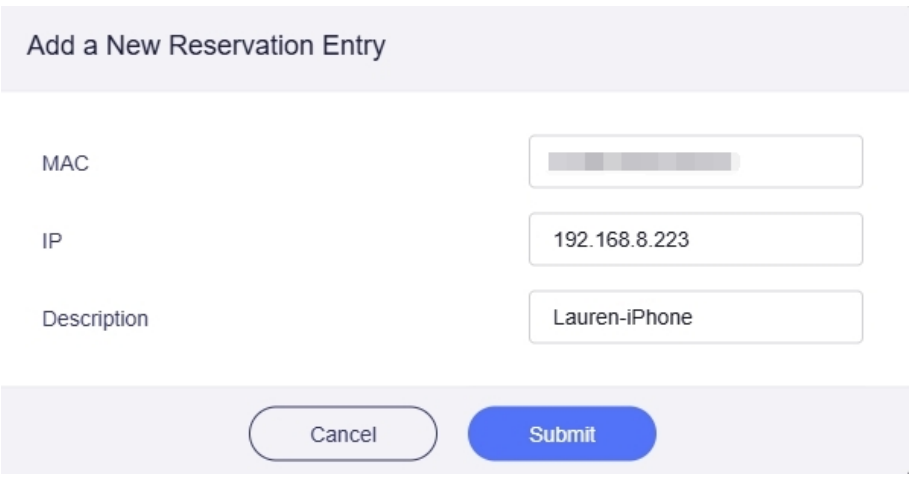
Hinweis: Bei deaktiviertem DHCP-Server müssen Sie für jedes Gerät eine statische IP-Adresse und weitere Kommunikationsparameter manuell festlegen. Einzelheiten finden Sie hier.

13.3.3 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.

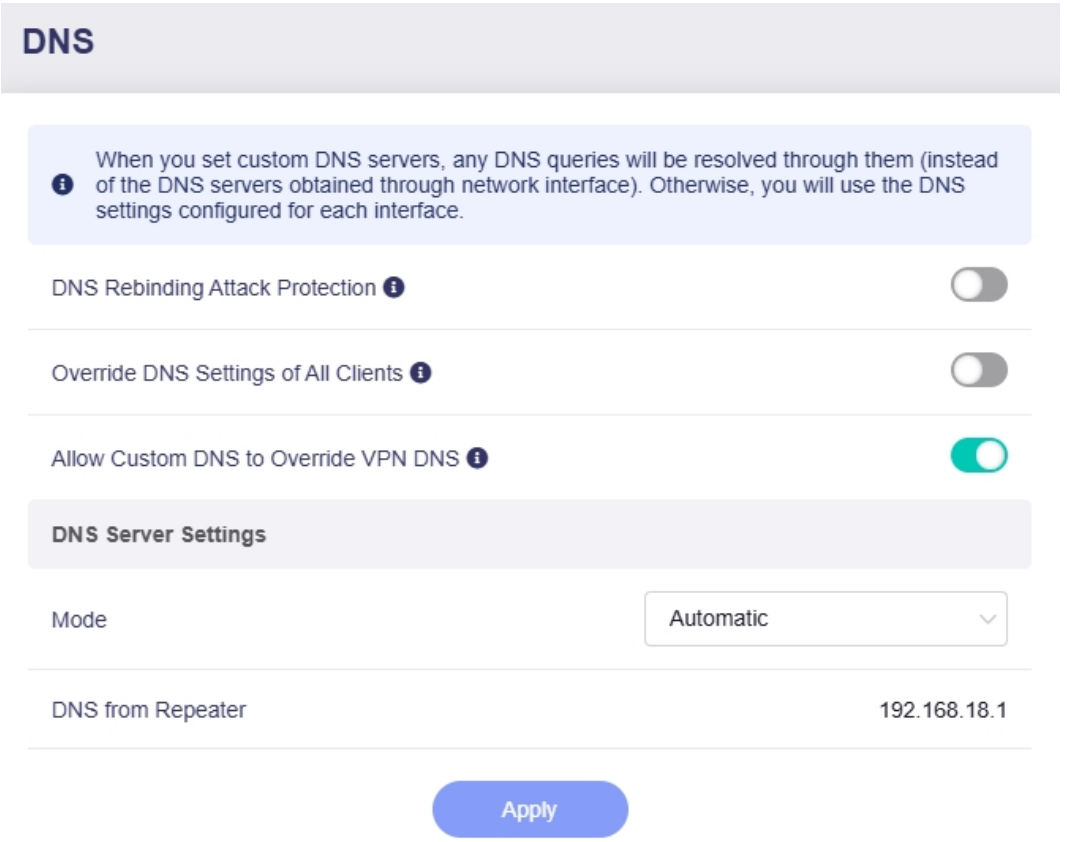


13.4 DNS

DNS (Domain Name System) ist ein Netzwerkdienst, der lesbare Domainnamen wie www.google.com in maschinenlesbare IP-Adressen wie 142.250.185.142 übersetzt. So können Geräte Verbindungen zu den gewünschten Websites oder Diensten herstellen.

Der DNS-Server des Routers ist dessen integrierter Dienst zur Übersetzung von Domainnamen in IP-Adressen für alle verbundenen Geräte. Er arbeitet üblicherweise auf zwei Arten: Zum einen bezieht er automatisch DNS-Adressen vom übergeordneten Netzwerk und stellt so die standardmäßige Namensauflösung bereit. Zum anderen können Sie in der Weboberfläche eigene öffentliche DNS-Adressen wie 8.8.8.8 festlegen, um den Netzwerkzugriff zu optimieren oder die Sicherheit zu erhöhen. Anschließend verwenden alle verbundenen Geräte standardmäßig diesen gemeinsamen DNS-Server. Eine separate DNS-Konfiguration an jedem Gerät ist dadurch nicht erforderlich.

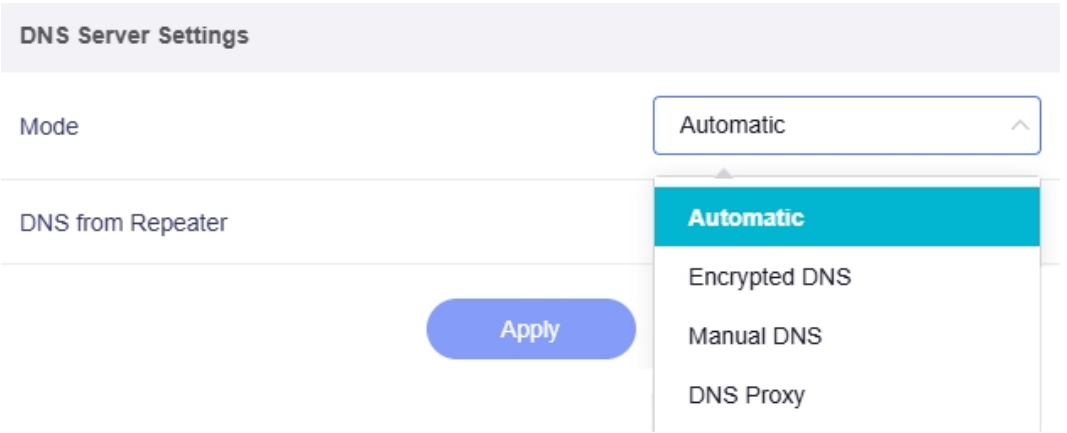
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **DNS**. Hier können Sie DNS-Einstellungen wie Sicherheitsoptionen, Servermodi und DNS-Prioritätsregeln für unterschiedliche Netzwerkszenarien konfigurieren.



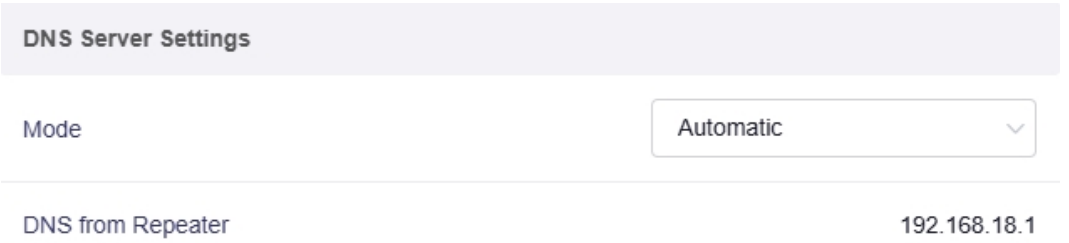
- **DNS Rebinding Attack Protection**: Schützt vor DNS-Rebinding-Angriffen, indem schädliche Versuche zur Namensauflösung blockiert werden. Beachten Sie, dass die Aktivierung zum Fehlschlagen privater DNS-Abfragen führen kann.
- **Override DNS Settings of All Clients**: Erzwingt für alle verbundenen Geräte die auf dem Router konfigurierten DNS-Server. Eigene DNS-Einstellungen der Geräte werden ignoriert, sodass eine einheitliche DNS-Konfiguration gilt.
- **Allow Custom DNS to Override VPN DNS**: Bei aktivierter Option verwenden Pakete im VPN-Tunnel die von Ihnen festgelegten DNS-Server anstelle der DNS-Server der VPN-Verbindung, sofern eigene DNS-Einstellungen vorhanden sind. Dadurch gelten Ihre eigenen Regeln zur Namensauflösung auch bei der VPN-Nutzung.

13.4.1 DNS-Servereinstellungen

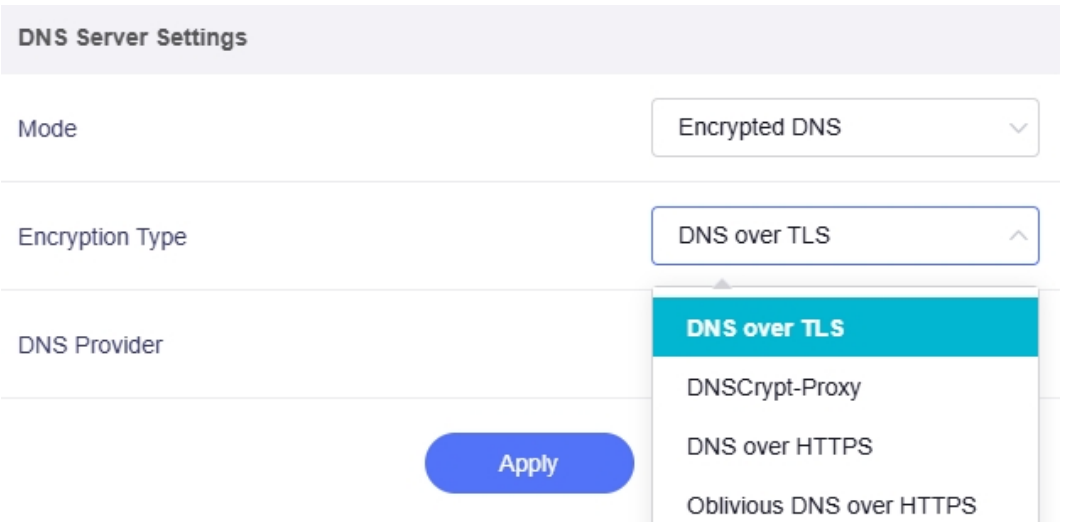
Für den DNS-Server stehen vier Modi zur Verfügung: Automatic, Encrypted DNS, Manual DNS und DNS Proxy.



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



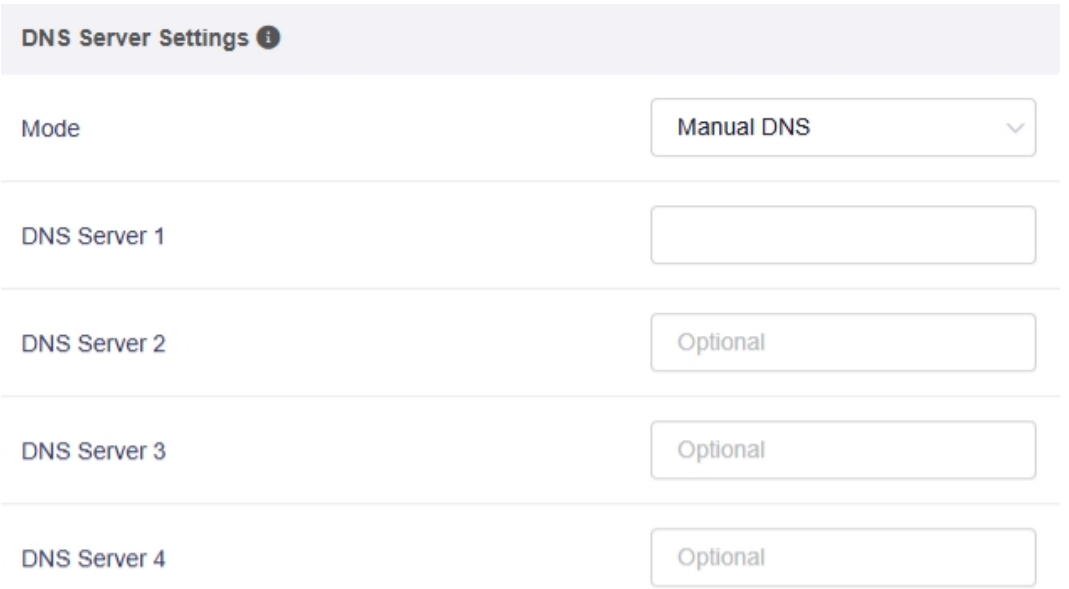
2. **Encrypted DNS**: Der Router verarbeitet DNS-Anfragen über verschlüsselte Protokolle und schützt die Auflösungsdaten so vor Abhören und Manipulation.
   Es stehen vier Verfahren zur Auswahl: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS.



   - Bei DNS over TLS wählen Sie Control D, NextDNS oder Cloudflare als DNS-Anbieter aus.

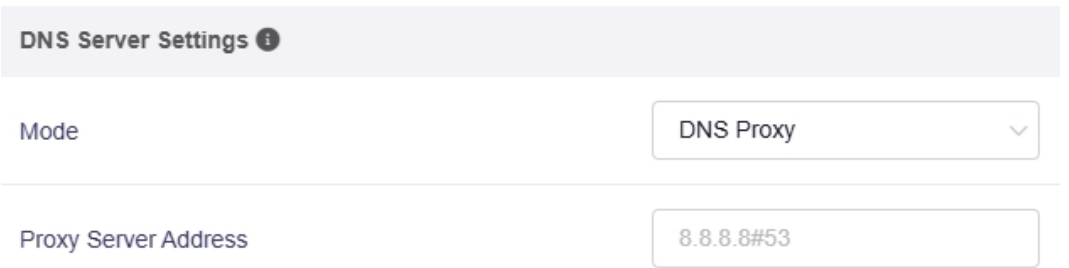
- Bei den drei anderen Verfahren wählen Sie mindestens einen DNS-Server aus dem Verzeichnis aus. Es sind bis zu acht Server möglich. Bei mehreren ausgewählten Servern verwendet der Router automatisch den schnellsten.

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.

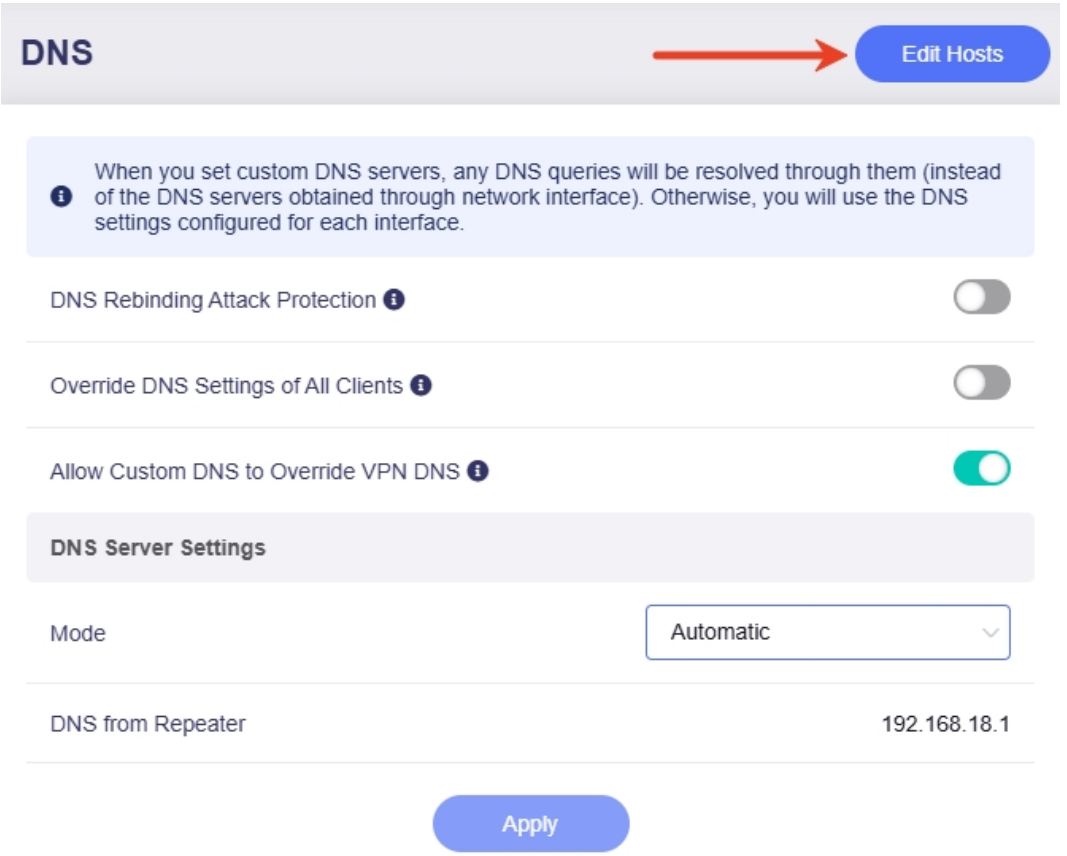
4. **DNS Proxy**: Der Router leitet alle DNS-Anfragen über einen Proxyserver weiter. Die Namensauflösung erfolgt in dessen Netzwerkumgebung, um besondere Zugriffsanforderungen zu erfüllen.



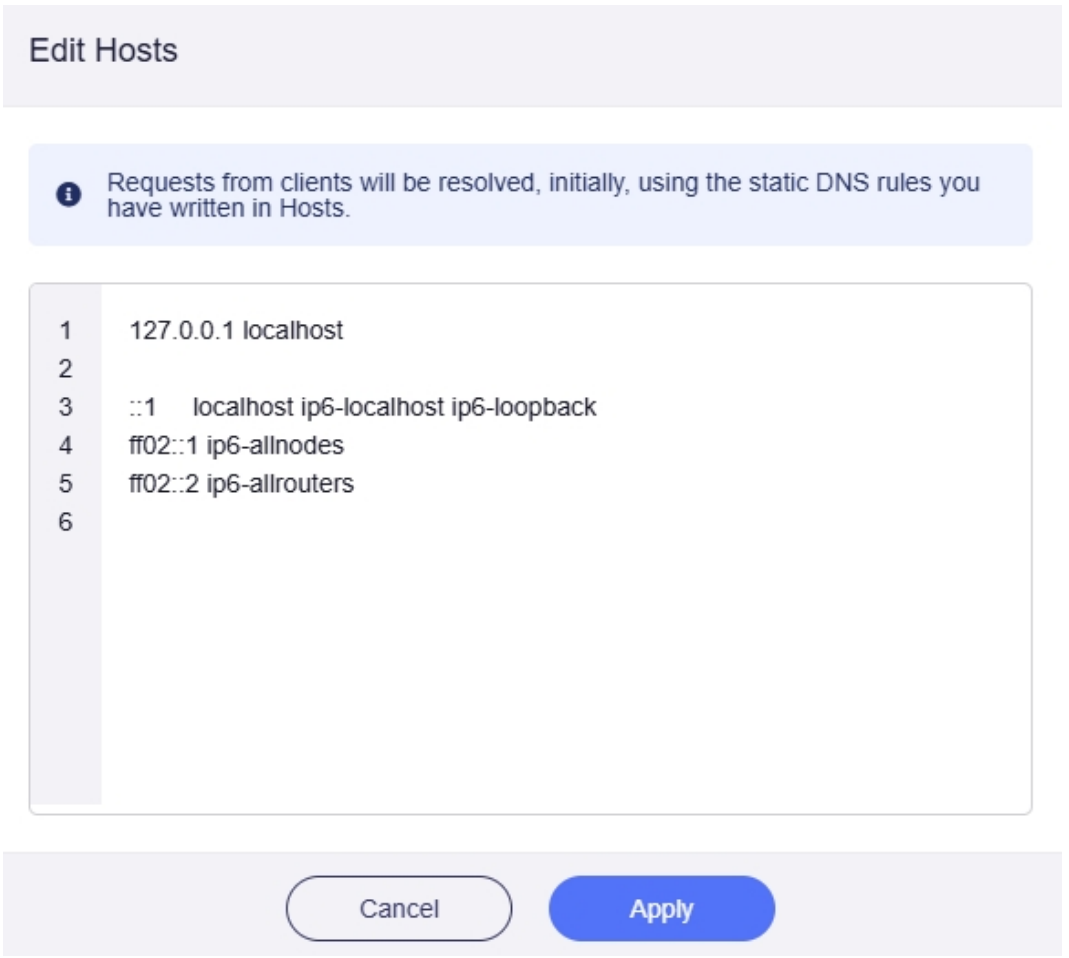
13.4.2 Hosts bearbeiten

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

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



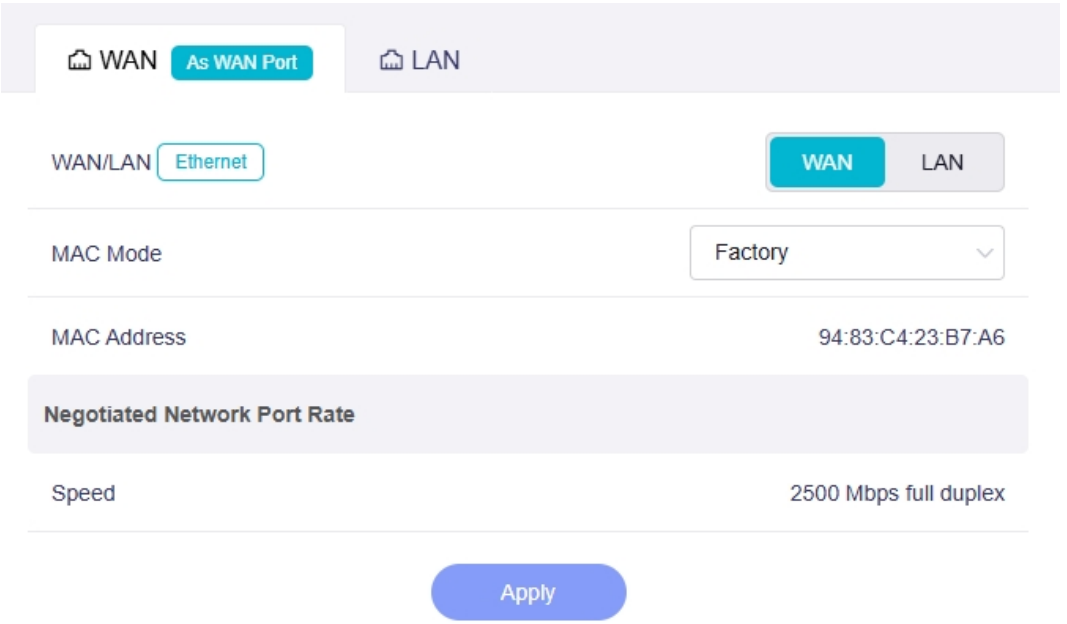
Anfragen von Endgeräten werden vorrangig anhand der hier eingetragenen statischen DNS-Regeln aufgelöst. Sie können Hostnamen manuell IP-Adressen zuordnen und so die Namensauflösung gezielt steuern. Ein Beispiel ist der Standardeintrag „127.0.0.1 localhost“ fü r die lokale Loopback-Adresse.


Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

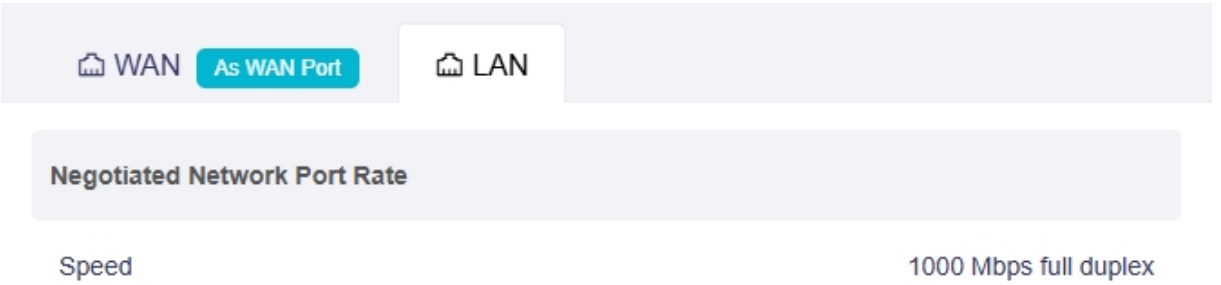
13.5 Portverwaltung

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Port Management**. Auf dieser Seite verwalten Sie die Ethernetanschlüsse des Routers.

Der Bereich **WAN** zeigt die Anschlussrolle (WAN oder LAN), die MAC-Adresse und die ausgehandelte Verbindungsgeschwindigkeit an.



Der Bereich **LAN** zeigt die ausgehandelte Verbindungsgeschwindigkeit des LAN-Anschlusses an.

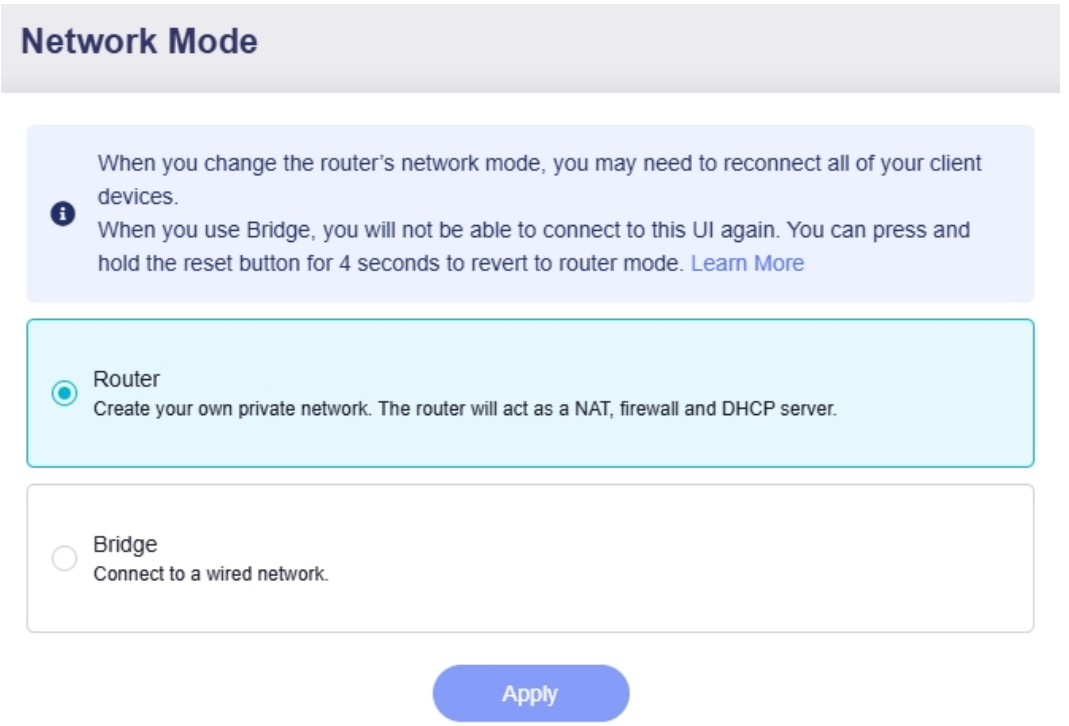


Hinweis: Die ausgehandelte Verbindungsgeschwindigkeit für WAN- und LAN-Anschlüsse wird nur bei angeschlossenem Ethernetkabel angezeigt. Sie hängt sowohl vom Ethernetanschluss als auch vom Ethernetkabel ab.

13.6 Netzwerkmodus

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

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Network Mode**. Hier können Sie den Netzwerkmodus ändern. Brume 2 unterstützt zwei Modi: Router und Bridge.



- **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.
- **Bridge**: Verbindet den Router mit einem kabelgebundenen Netzwerk, in dem er als Brücke zwischen Netzwerkgeräten arbeitet. In diesem Modus funktioniert der Router im Wesentlichen wie ein Switch: Er leitet Daten zwischen verbundenen Geräten weiter, ohne NAT, Firewall oder DHCP-Dienste bereitzustellen. Als einfacher Verbindungspunkt ermöglicht er die nahtlose Kommunikation zwischen Geräten im selben Netzwerk.

Hinweis:

1. Nach einer Änderung des Netzwerkmodus müssen sich die Geräte erneut mit dem Router verbinden, um eine stabile Verbindung sicherzustellen.
2. **Im Bridge-Modus ist die Weboberfläche nicht mehr über die ursprüngliche IP-Adresse erreichbar**. Melden Sie sich stattdessen am vorgeschalteten Router an und ermitteln Sie die IP-Adresse, die er diesem Router zugewiesen hat. Rufen Sie die Weboberfläche anschließend über diese Adresse auf. Falls Sie keinen Zugriff auf den vorgeschalteten Router haben, halten Sie die Reset-Taste 4 Sekunden gedrückt, um zum standardmäßigen Routermodus zurückzukehren.
3. **Im Bridge-Modus stehen folgende Funktionen nicht zur Verfügung**: Zugriffskontrolle (Freigabe- und Sperrliste), AstroWarp, VPN, Tor, AdGuard Home, Kindersicherung, ZeroTier, Tailscale, Portweiterleitung, Multi-WAN, DHCP-Server, Adressreservierung, DNS, Portverwaltung, IPv6, Drop-in-Gateway, IGMP Snooping, Netzwerkbeschleunigung und NAT-Einstellungen.

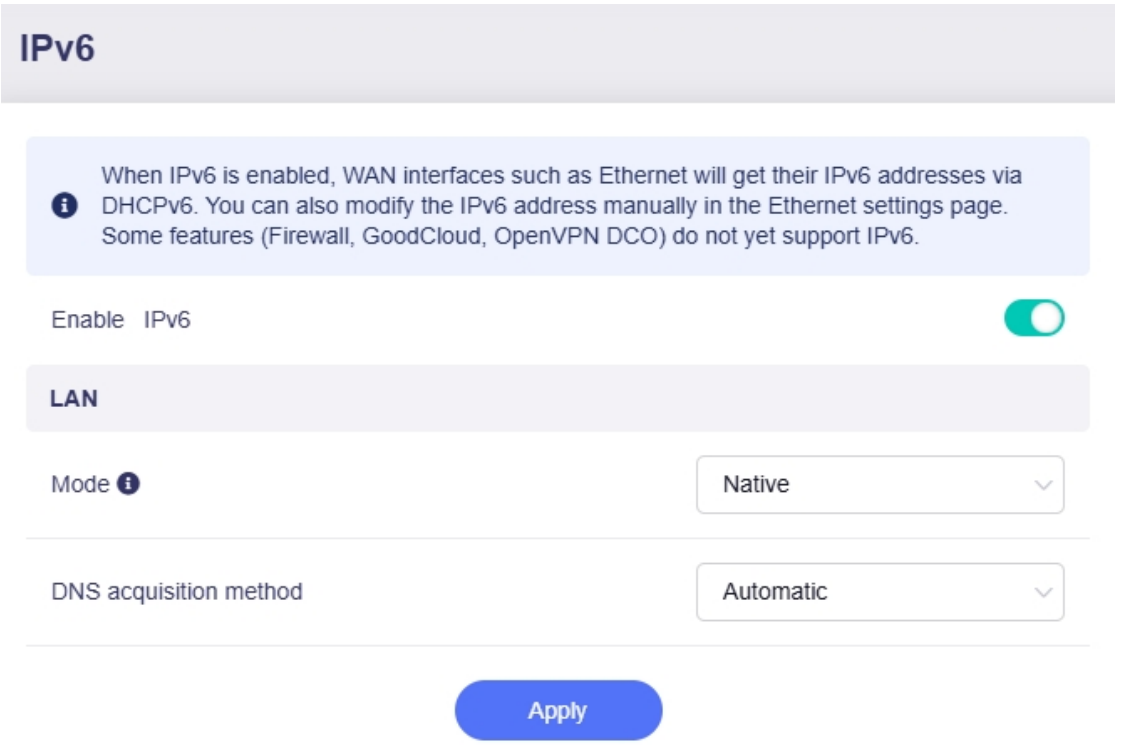
13.7 IPv6

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.

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

Aktivieren Sie **Enable IPv6**. Wählen Sie den Modus für Ihr Hauptnetzwerk und das Verfahren zum Beziehen der DNS-Adressen aus und klicken Sie auf **Apply.**



13.7.1 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.

13.7.2 DNS-Adressen beziehen

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

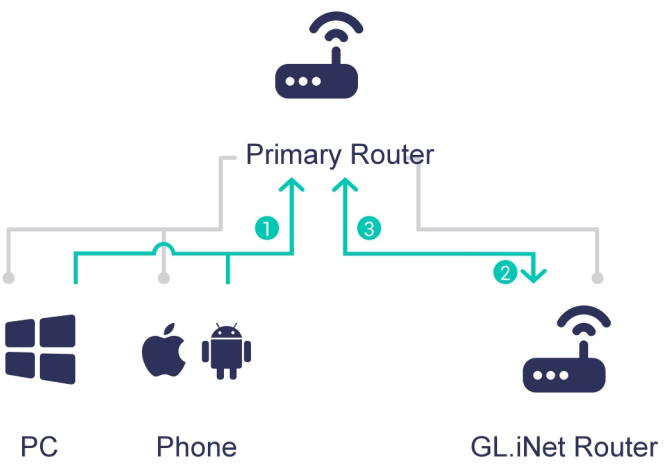
- **Automatic**: Der Router bezieht die IPv6-DNS-Serveradressen dynamisch, etwa über DHCPv6.
- **Manual**: Geben Sie eigene IPv6-DNS-Serveradressen ein. Da DNS Domainnamen in die zugehörigen IP-Adressen auflöst, kann eine manuelle Konfiguration zu Fehlern bei der Namensauflösung führen. Verwenden Sie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

13.8 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:

- Werbung mit AdGuard Home filtern
- VPN-Client verwenden
- Verschlüsseltes DNS nutzen

Drop-in Gateway arbeitet als zwischengeschaltetes Netzwerksystem. 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 verbundenen Geräte weiterhin unterbrechungsfrei arbeiten. Gleichzeitig können Sie den Datenverkehr aller oder ausgewählter Endgeräte nach Bedarf 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.

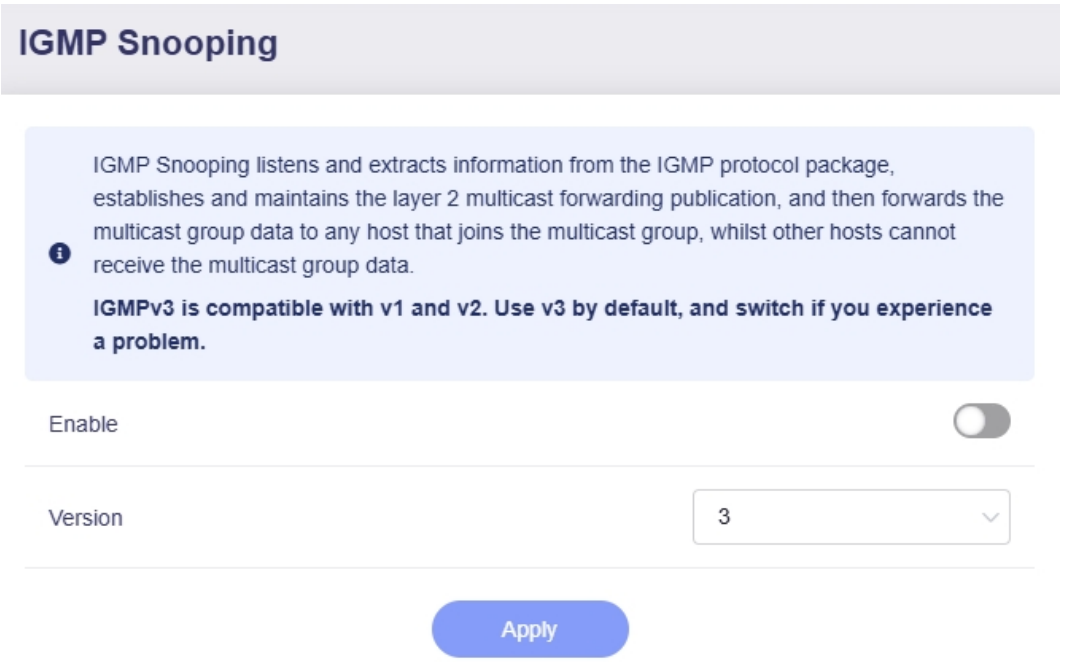
- **Grüne Linien** zeigen den Datenweg bei aktiviertem Drop-in Gateway. Die nummerierten Pfeile geben die Reihenfolge an:
    1. Der Datenverkehr der Endgeräte gelangt zunächst zum Hauptrouter.
    2. Der Hauptrouter leitet ihn zur Verarbeitung an den GL.iNet-Router weiter, etwa zum Filtern von Werbung 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.

Sie können das Drop-in-Gateway für alle oder für bestimmte Geräte aktivieren, die mit Ihrem Hauptrouter verbunden sind. Weitere Anweisungen finden Sie unter diesem Link.

13.9 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.

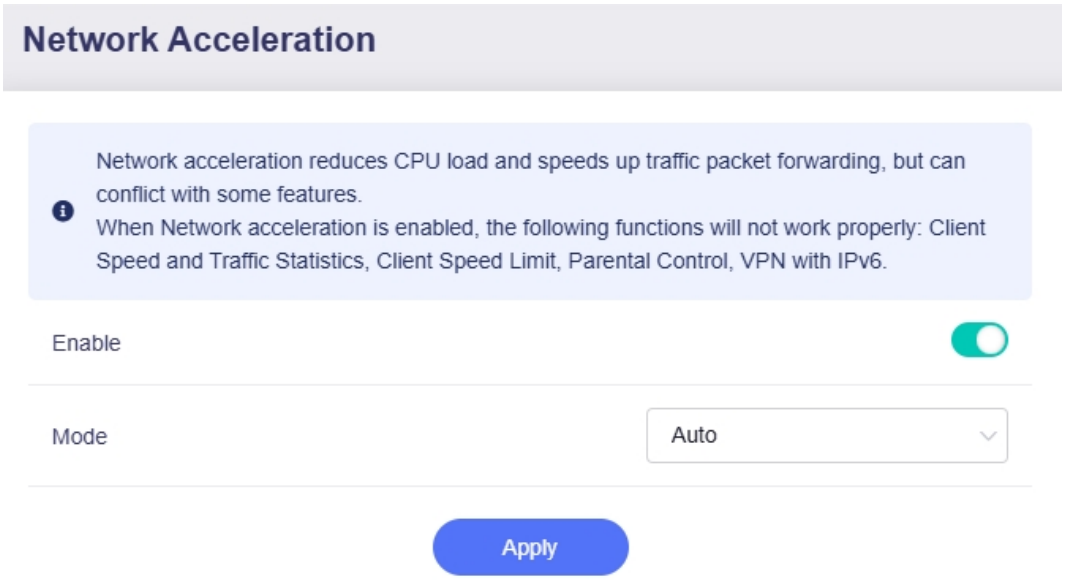
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **IGMP Snooping**. Aktivieren Sie die Funktion bei Bedarf, um Multicast auf Ihrem Router zu nutzen.



13.10 Netzwerkbeschleunigung

Die Netzwerkbeschleunigung verringert die CPU-Auslastung und beschleunigt die Weiterleitung von Datenpaketen. Bei einigen Funktionen kann sie jedoch zu Konflikten führen.

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Network Acceleration**. Hier können Sie die Netzwerkbeschleunigung aktivieren und zwischen Auto, Hardware Acceleration und Software Acceleration wählen.



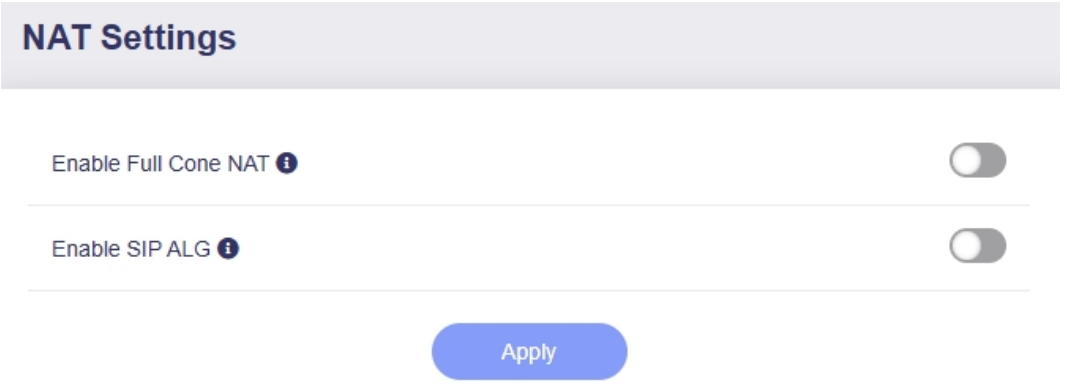
- **Auto**: Wechselt je nach tatsächlicher Nutzung automatisch zwischen den beiden Beschleunigungsmodi.
- **Hardware Acceleration**: Lagert häufig anfallende Netzwerkaufgaben wie NAT, Paketweiterleitung und Prüfsummenprüfung auf spezielle Hardware wie NPUs oder HWNAT-Chips aus. Sie arbeitet mit Ethernet-Verbindungen (kabelgebundenes WAN/LAN) und Repeater-Verbindungen, die auf Brume 2 nicht verfügbar sind. Bei festen Übertragungswegen und einfachen Regeln bietet sie hohen Durchsatz, geringe Latenz und minimale CPU-Auslastung für die Datenübertragung mit voller Leitungsgeschwindigkeit.
- **Software Acceleration**: Nutzt die allgemeine CPU des Routers zusammen mit optimierten Kerneln oder Treibern, etwa SWNAT. Sie arbeitet mit Mobilfunkverbindungen (4G/5G), bei denen eine Hardwarebeschleunigung üblicherweise nicht verfügbar ist, und bietet hohe Kompatibilität sowie Unterstützung komplexer Protokolle. Bei hoher

Bandbreitenauslastung kann die CPU jedoch zum Engpass werden, insbesondere bei der Nutzung erweiterter Funktionen wie QoS oder Portweiterleitung.

Hinweis: Bei aktivierter Netzwerkbeschleunigung funktionieren folgende Funktionen nicht ordnungsgemäß: Geschwindigkeitsstatistik für Clients, Datenverkehrsstatistik, Geschwindigkeitsbegrenzung, Kindersicherung, VPN mit IPv6, Datenstatistik, Inhaltsfilter, QoS und SQM.

13.11 NAT-Einstellungen

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **NAT Settings**. Hier konfigurieren Sie zwei wichtige NAT-Funktionen: Full Cone NAT und SIP ALG.



- **Full Cone NAT**: Kann die Latenz in Onlinespielen senken und deren Reaktionsgeschwindigkeit verbessern. Da uneingeschränkte eingehende Verbindungen erlaubt werden, kann die Aktivierung jedoch die Sicherheit verringern.
- **SIP ALG**: Soll die Auswirkungen mehrerer NAT-Stufen auf SIP-Datenverkehr (Session Initiation Protocol) verringern. In vielen Fällen bringt es jedoch keinen Vorteil und kann VoIP-Anrufe sogar beeinträchtigen. Mögliche Folgen sind einseitiger Ton, ausbleibendes Klingeln, unerwartete Gesprächsabbrüche oder eine direkte Weiterleitung an die Mailbox.

Kapitel 14

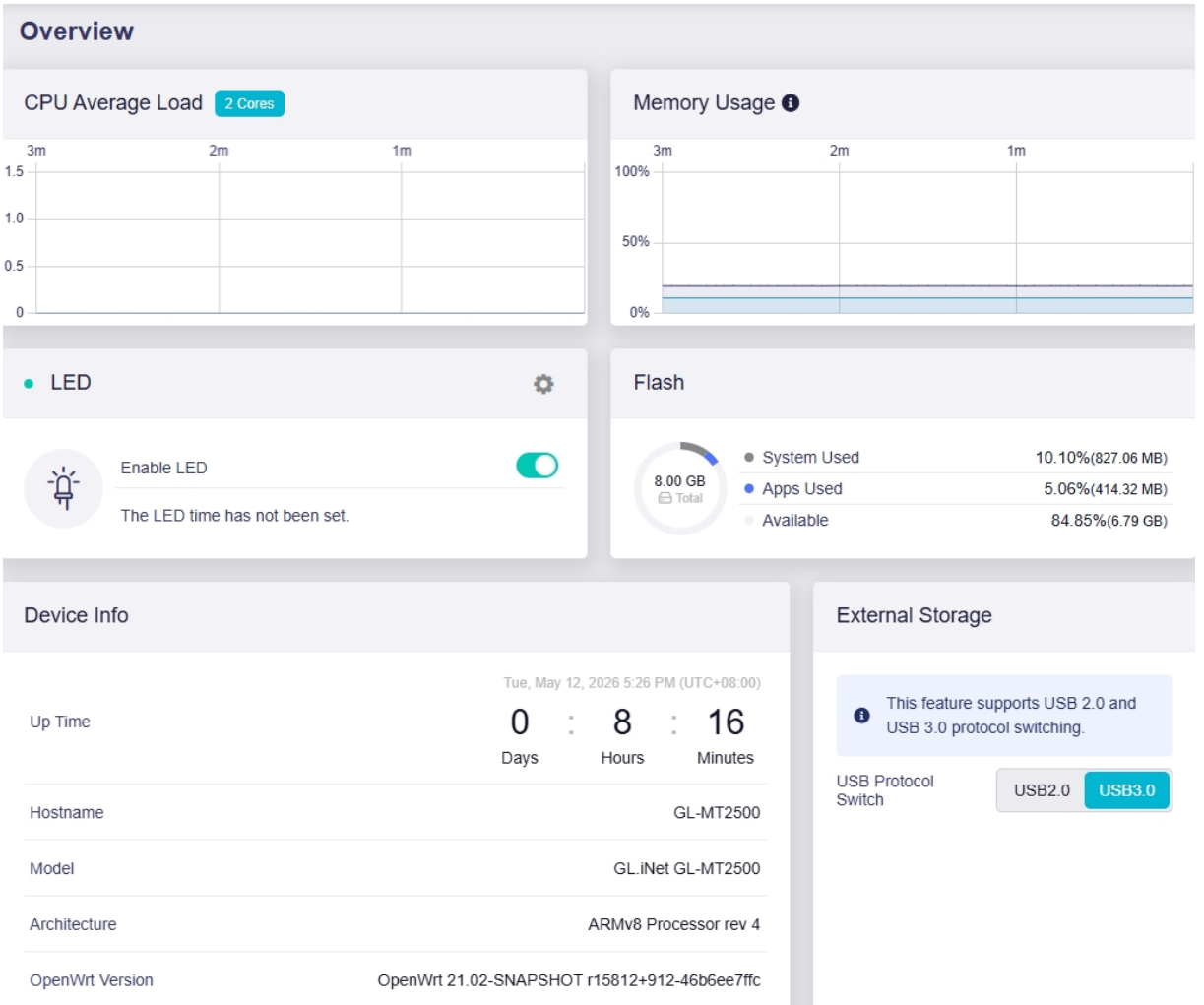
System

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

14.1 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
- Umschalten des Protokolls für externe Speicher

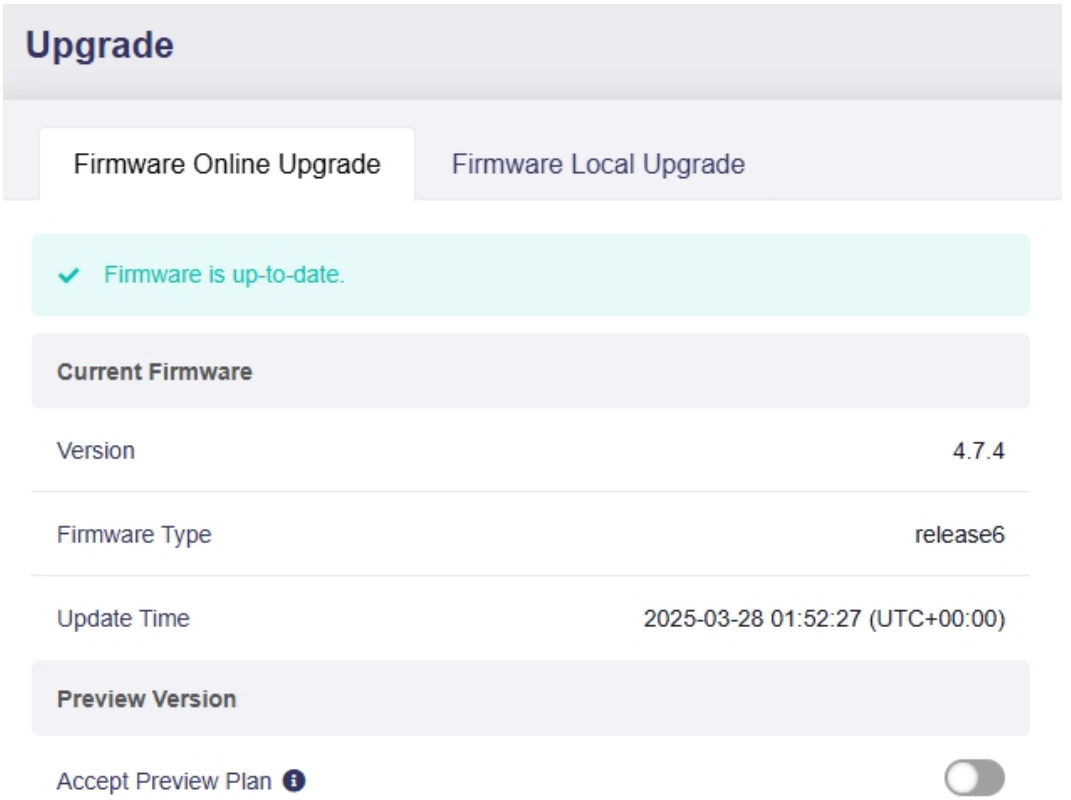


14.2 Aktualisierung

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

14.2.1 Online-Aktualisierung

Hier finden Sie die Angaben zur aktuellen Firmware, darunter Firmwareversion, Firmwaretyp (z. B. Release oder Beta) und Aktualisierungszeitpunkt.



- **Accept Preview Plan**: Bei aktivierter Option können Sie neue Funktionen vor der endgültigen Veröffentlichung ausprobieren und uns Rückmeldung geben. Die Option bleibt nach einmaliger Aktivierung eingeschaltet. Beachten Sie, dass diese Versionen möglicherweise nicht stabil sind.

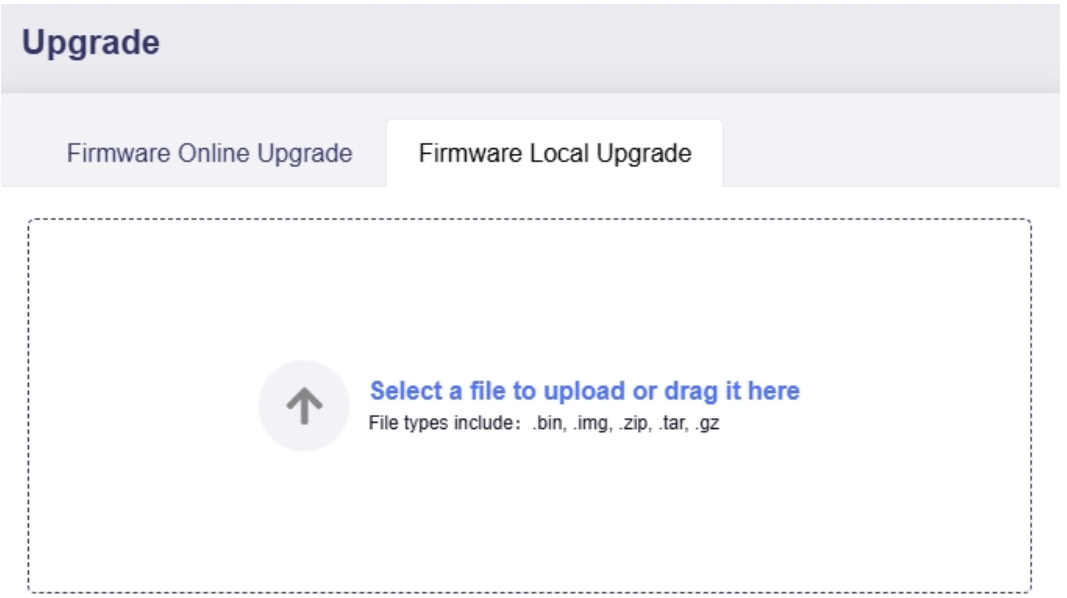
Bei bestehender Internetverbindung prüft der Router, ob eine neuere Firmwareversion zum Herunterladen verfügbar ist.

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

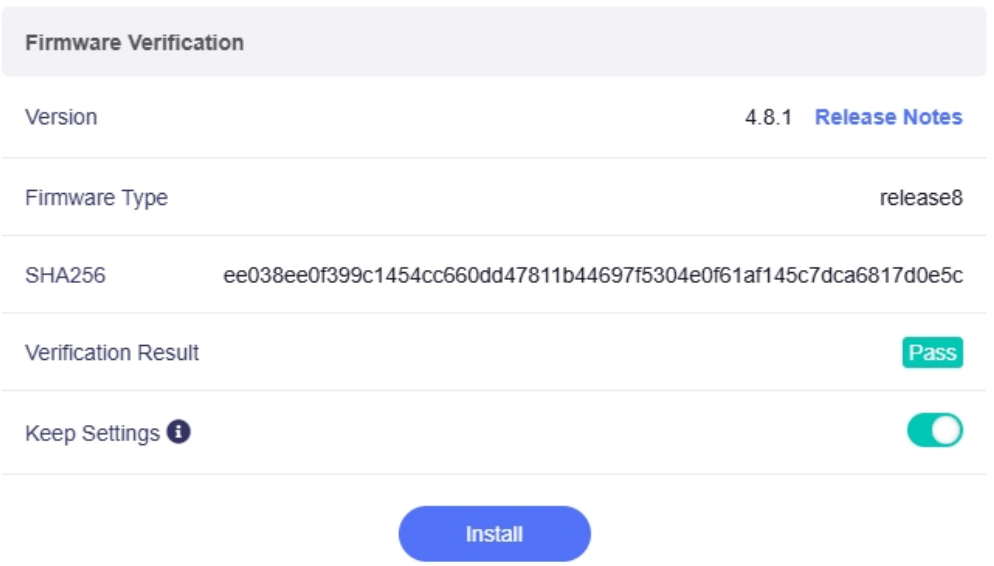
14.2.2 Lokale Aktualisierung

Für diese 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.



- **Keep Settings**: Bei aktivierter Option bleiben die aktuellen Einstellungen erhalten. Manuell installierte Pakete müssen nach der Aktualisierung jedoch erneut installiert werden. Aktivieren Sie diese Option nicht beim Wechsel auf eine ältere Firmwareversion.

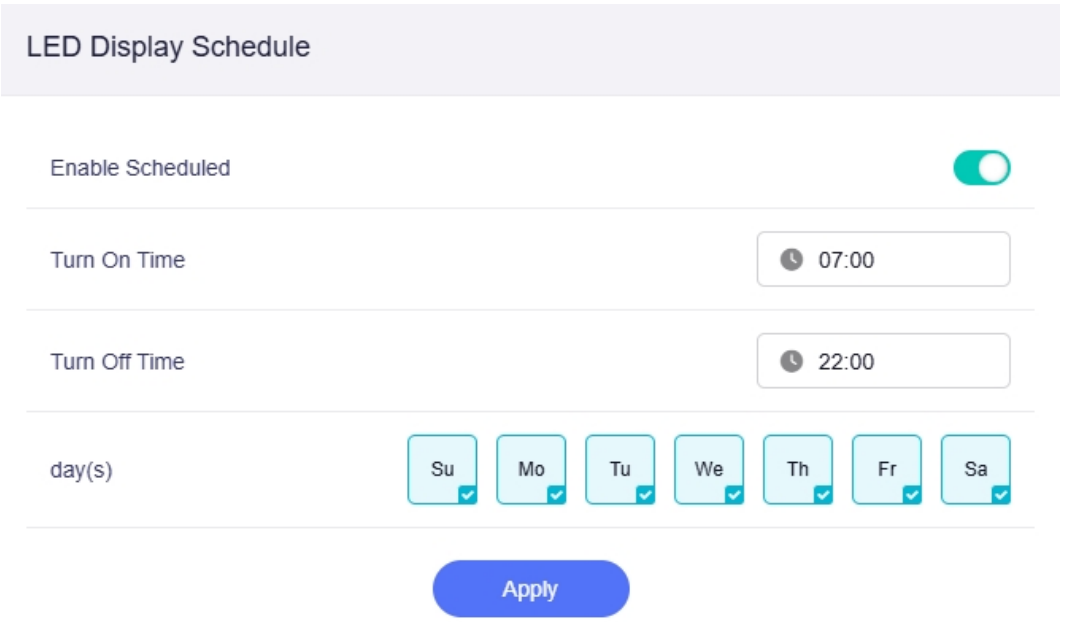
14.3 Geplante Aufgaben

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 dieser Funktion die Uhrzeit unter Time Zone. Ist das Gerät zum vorgesehenen Zeitpunkt ausgeschaltet, wird die Aufgabe nicht ausgeführt.

14.3.1 LED-Zeitplan

Mit dieser Funktion legen Sie einen Zeitplan für die LED Ihres Routers fest.

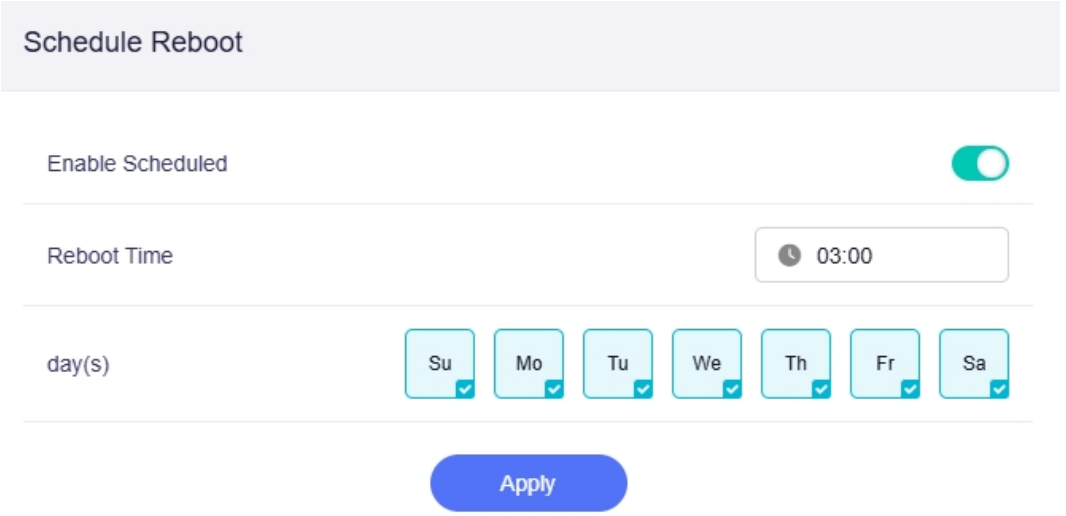


- **Enable Scheduled**: Aktiviert den LED-Zeitplan.
- **Turn On Time**: Uhrzeit zum Einschalten der LED, etwa 07:00 Uhr.
- **Turn Off Time**: Uhrzeit zum Ausschalten der LED, etwa 22:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

Klicken Sie nach der Konfiguration auf **Apply**, um Ihre Einstellungen zu speichern.

14.3.2 Geplanter Neustart

Mit dieser Funktion legen Sie einen Zeitplan für automatische Routerneustarts fest.

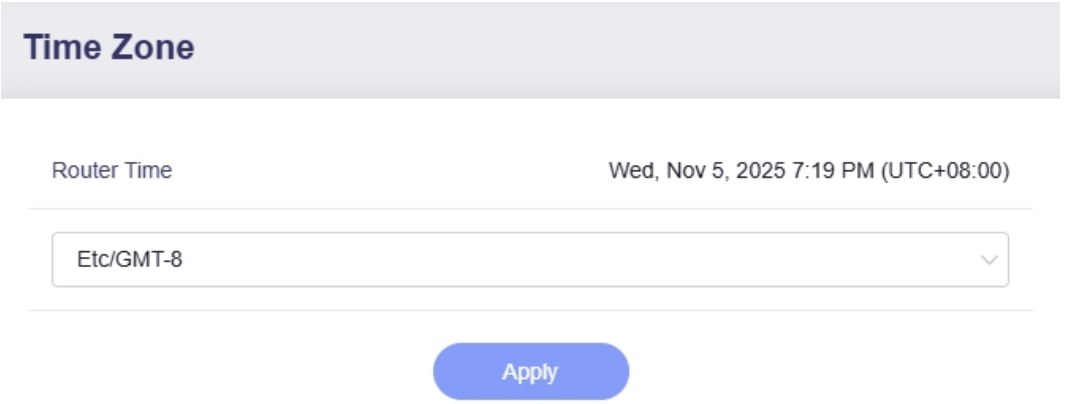


- **Enable Scheduled**: Aktiviert den geplanten Neustart.
- **Reboot Time**: Uhrzeit des Routerneustarts, etwa 03:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

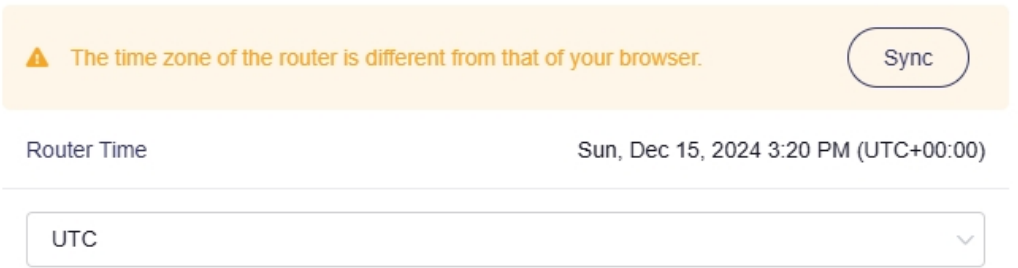
Klicken Sie nach der Konfiguration auf **Apply**, um Ihre Einstellungen zu speichern.

14.4 Zeitzone

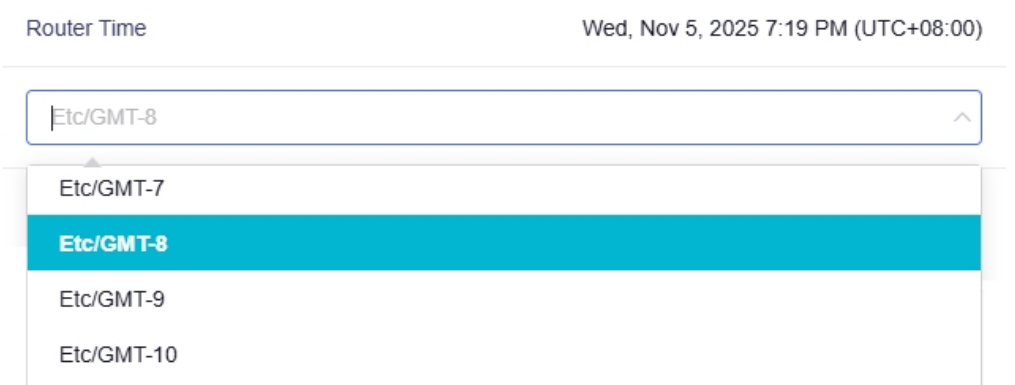
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Time Zone**. Die Seite zeigt die Systemzeit Ihres Routers mit Datum, Uhrzeit und Zeitzonenversatz an.



Einige Funktionen benötigen die Systemzeit des Routers, um wirksam zu werden. Stellen Sie daher sicher, dass die richtige Zeitzone synchronisiert ist. Weicht die Zeitzone des Routers von der Ihres Browsers ab, erscheint die folgende Meldung. Klicken Sie auf **Sync**, um die Zeitzone zu synchronisieren.

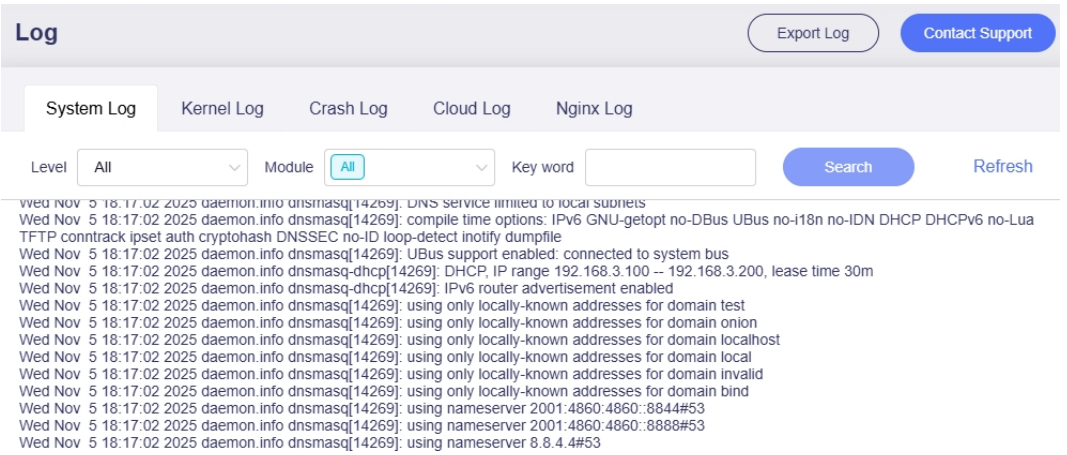


Wählen Sie zum Ändern der Zeitzone den passenden Eintrag aus der Liste, damit die Routerzeit Ihrer Ortszeit entspricht.

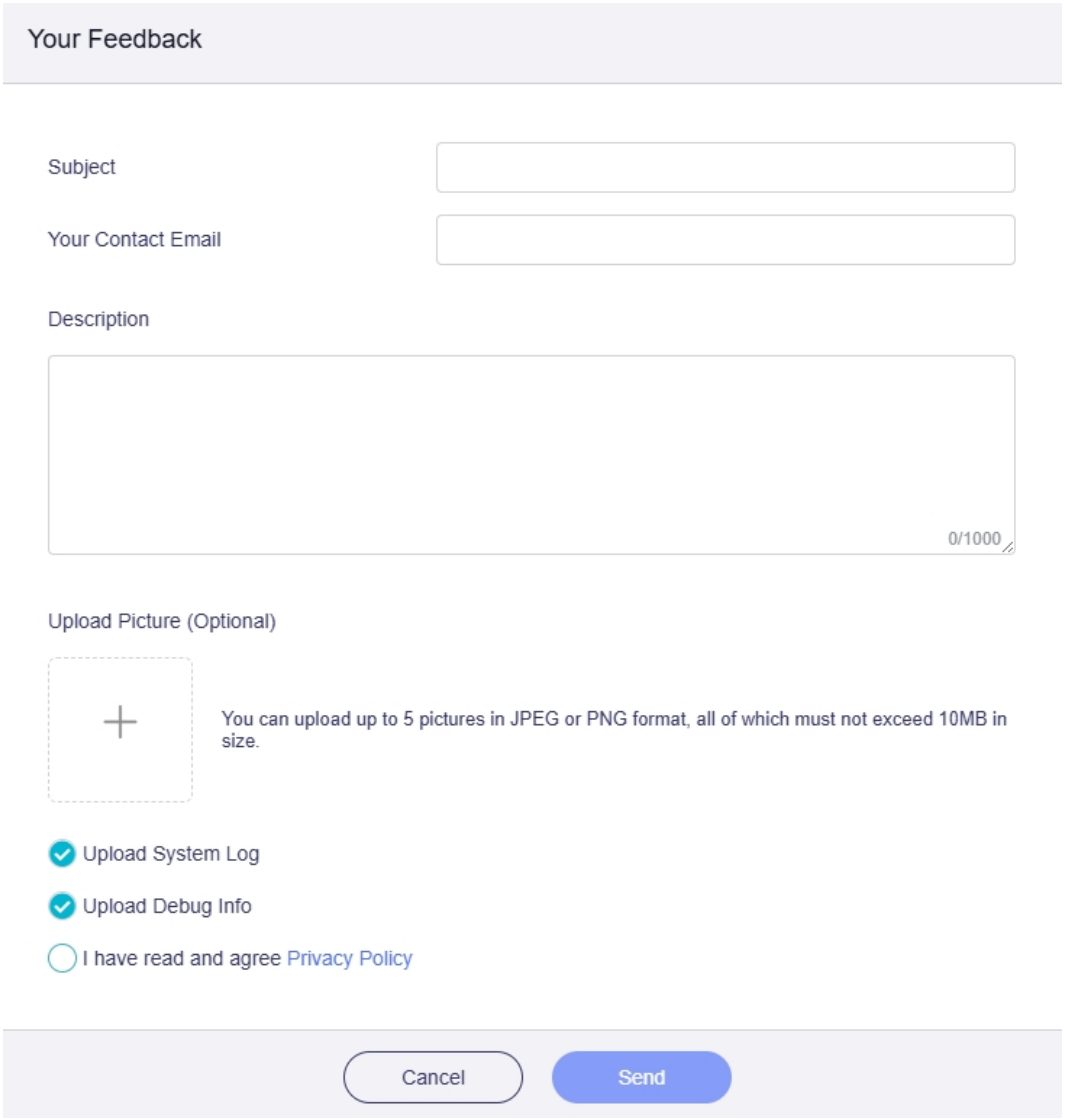


14.5 Protokolle

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SYSTEM** > **Log**. Hier können Sie System-, Kernel-, Absturz-, Cloud- und Nginx-Protokolle zur Analyse und Fehlerbehebung einsehen. Einige Mobilfunkmodelle mit eSIM-Unterstützung stellen außerdem ein eSIM-Protokoll bereit.



- **Search**: Auf der Systemprotokollseite können Sie Einträge für eine schnelle Suche filtern. Wählen Sie die Protokollstufe, beispielsweise all, info oder error, oder das Modul, beispielsweise IPv6, Tethering oder Cellular, aus der Dropdown-Liste aus. Alternativ können Sie Protokolle durch Eingabe von Suchbegriffen schnell abfragen.
- **Refresh**: Aktualisiert die Protokolle.
- **Export Log**: Exportiert die Protokolle zusammen mit Debug-Informationen.
- **Contact Support**: Klicken Sie auf diese Schaltfläche und geben Sie im rechts eingeblendeten Fenster ausführliche Informationen ein. Klicken Sie anschließend auf **Send**. Ihre Rückmeldung wird direkt an den technischen Support von GL.iNet gesendet.


Your Feedback
Subject
Your Contact Email
Description
0/1000
Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

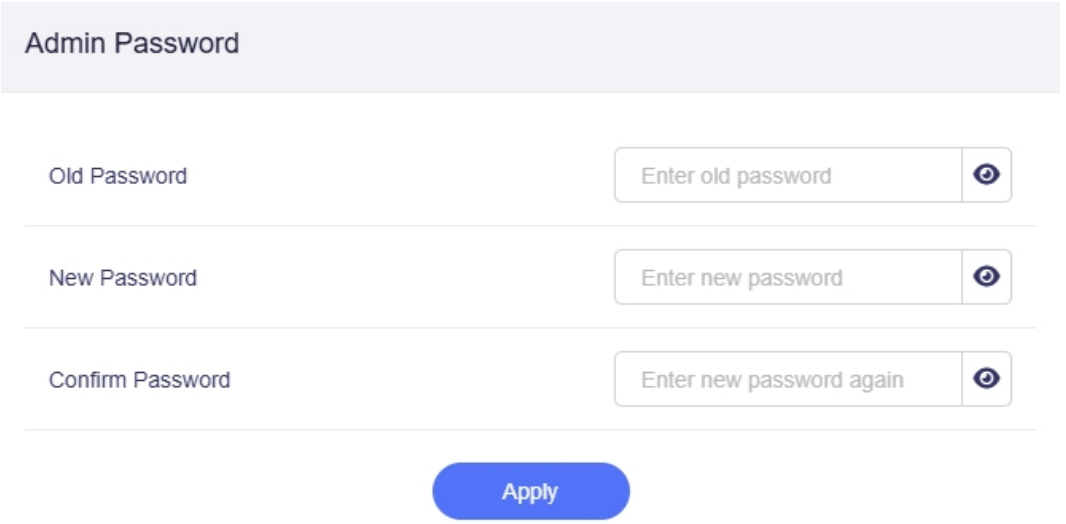
14.6 Sicherheit

Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Security**. Hier konfigurieren Sie die lokale Verwaltung und den Fernzugriff, darunter:

- Administratorpasswort
- Lokaler Zugriff auf Weboberfläche, LuCI und SSH
- HTTPS-/SSH-Fernzugriff
- Offene Ports des Routers verwalten

14.6.1 Administratorpasswort

In diesem Abschnitt ändern Sie das Anmeldepasswort der Weboberfläche.

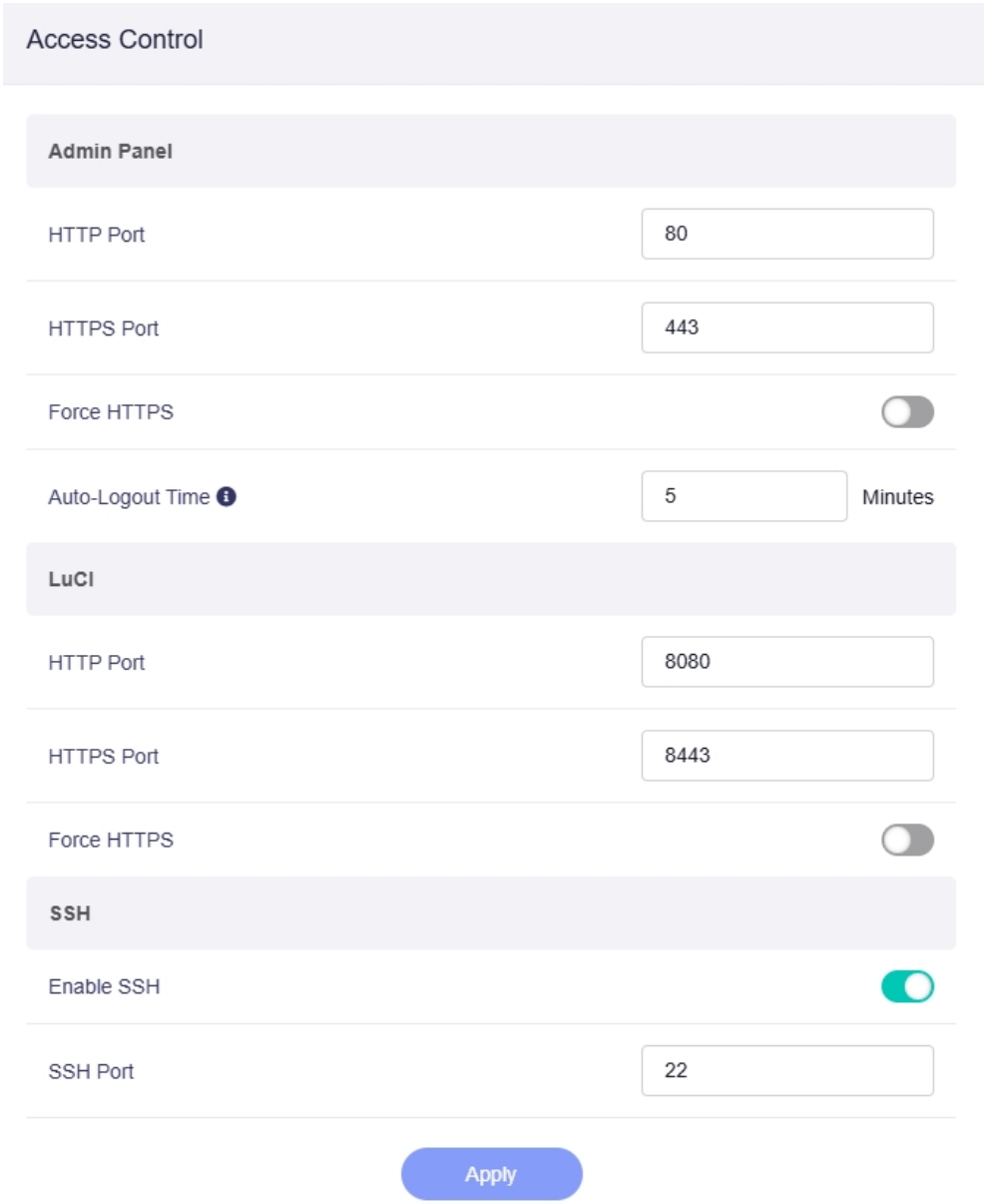


Für das Administratorpasswort gelten folgende Anforderungen:

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.

14.6.2 Zugriffskontrolle

Dieser Bereich verwaltet den Zugriff auf die verschiedenen Schnittstellen des Routers: Weboberfläche, LuCI und SSH. Damit können Sie Scan- und Einbruchsversuchen am Standardport vorbeugen und Netzwerkprobleme durch Portkonflikte vermeiden.



Weboberfläche

- **HTTP Port**: Standardmäßig 80; für den unverschlüsselten HTTP-Zugriff auf die Weboberfläche.
- **HTTPS Port**: Standardmäßig 443; für den sicheren HTTPS-Zugriff auf die Weboberfläche.

- **Force HTTPS**: Erzwingt eine sichere HTTPS-Verbindung beim Zugriff auf die Weboberfläche.
- **Auto-Logout Time**: Inaktive Administratorsitzungen werden aus Sicherheitsgründen nach der festgelegten Zeit automatisch abgemeldet. Standardmäßig sind fünf Minuten eingestellt. Möglich sind eine Minute bis drei Stunden.

LuCI

Hinweis: Installieren Sie LuCI unter Advanced Settings, bevor Sie die Zugriffskontrolle dafür konfigurieren.

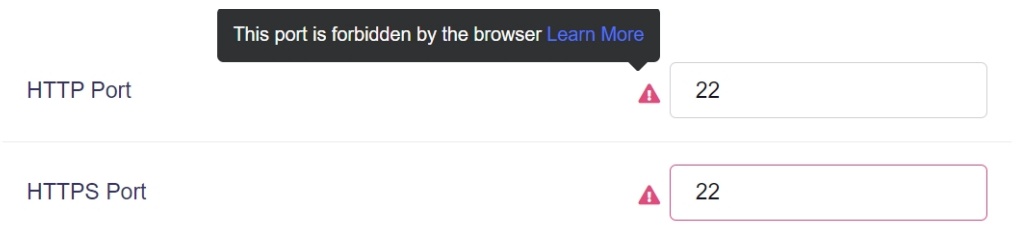
- **HTTP Port**: Standardmäßig 8080; wird für den unverschlüsselten HTTP-Zugriff auf die LuCI-Oberfläche verwendet.
- **HTTPS Port**: Standardmäßig 8443; wird für den sicheren HTTPS-Zugriff auf die LuCI-Oberfläche verwendet.
- **Force HTTPS**: Bei aktivierter Option ist der Zugriff auf die LuCI-Oberfläche ausschließlich über eine sichere HTTPS-Verbindung möglich.

SSH

- **Enable SSH**: Standardmäßig aktiviert; steuert, ob der SSH-Zugriff auf den Router erlaubt ist.
- **SSH Port**: Standardmäßig 22; für den SSH-Zugriff auf den Router.

Hinweis:

1. Wenn Sie einen reservierten Port oder einen von Browsern beziehungsweise Netzwerkkonventionen bestimmten Diensten vorbehaltenen Port auswählen, erscheint die Meldung „This port is forbidden by the browser“.

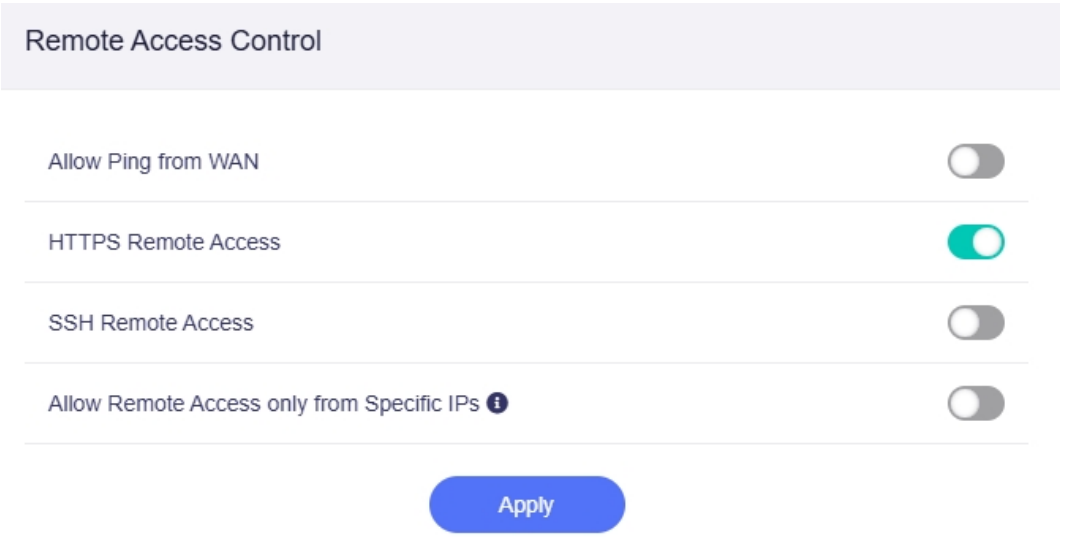


2. Nach einer Änderung der Portnummer in der Firmware müssen Sie die neue Portnummer beim Aufrufen der Weboberfläche angeben. Haben Sie sie vergessen, setzen Sie den Router zurück, um den Standardport wiederherzustellen.

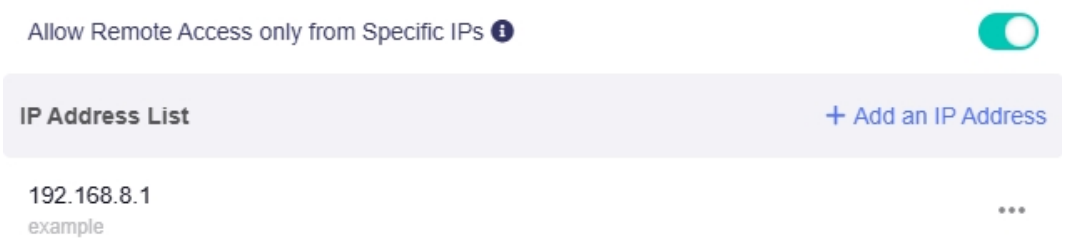
3. Die LuCI-Zugriffseinstellungen sind erst nach der Installation von LuCI verfügbar. Wenn diese Einstellungen nicht angezeigt werden, öffnen Sie **SYSTEM** > **Advanced Settings** und installieren Sie LuCI.

14.6.3 Fernzugriffskontrolle

Hier verwalten Sie den Fernzugriff über HTTPS und SSH sowie Ping-Anfragen von der WAN-Seite. Sie können den Zugriff auf bestimmte IP-Adressen begrenzen und so Fernzugriff und Netzwerksicherheit aufeinander abstimmen.

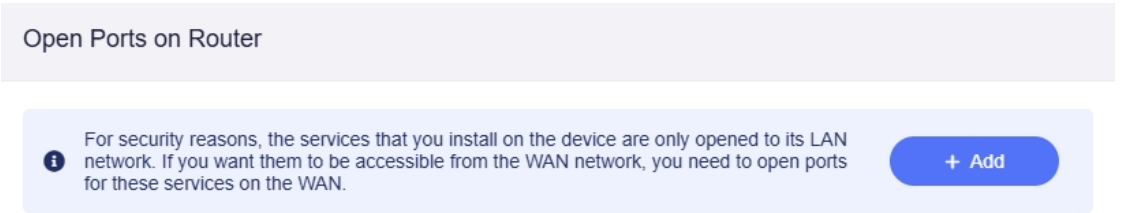


- **Allow Ping from WAN**: Erlaubt Ping-Anfragen von der WAN-Seite. Bei Netzwerkproblemen können Sie damit die Erreichbarkeit des Routers sowie Latenz und Paketverlust prüfen.
- **HTTPS Remote Access**: Ermöglicht den sicheren Fernzugriff auf die Weboberfläche über HTTPS. Die Datenübertragung bei der Verwaltung im Webbrowser wird verschlüsselt.
- **SSH Remote Access**: Ermöglicht den sicheren Fernzugriff auf das Routerterminal über SSH. Für Verwaltungsaufgaben wird ein verschlüsselter Tunnel aufgebaut.
- **Allow Remote Access from Specific IPs**: Diese Option ist verfügbar, sobald mindestens eine der drei vorstehenden Funktionen aktiviert ist. Sie können mehrere IP-Adressen angeben, damit die Fernverwaltung nur von Geräten mit diesen Adressen möglich ist.

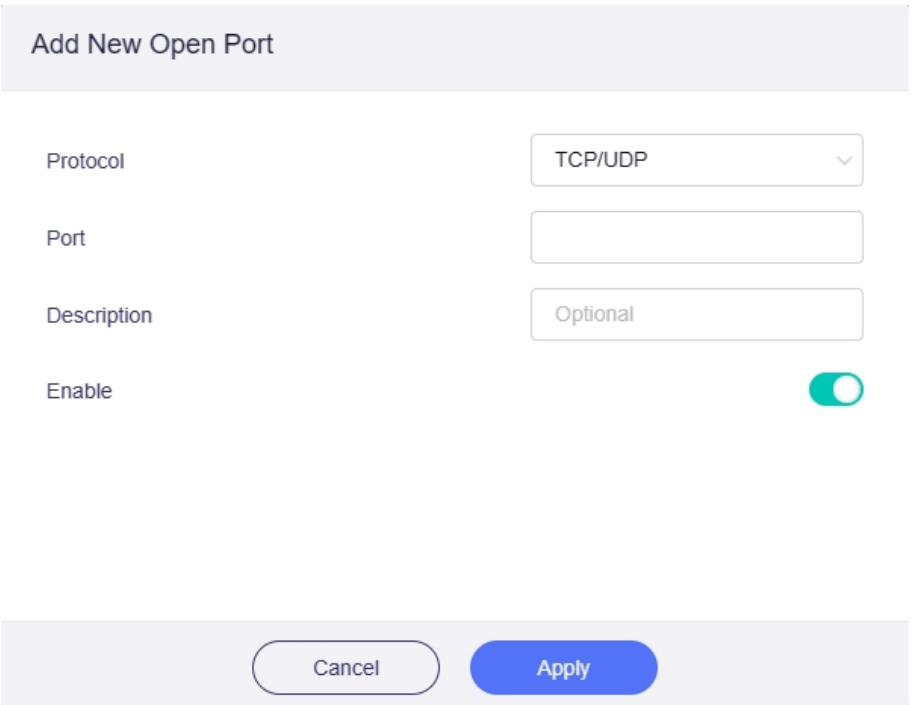


14.6.4 Ports am Router öffnen

In diesem Bereich verwalten Sie Portfreigaben für Dienste auf Ihrem Router. Damit Dienste wie Web und FTP vom WAN aus öffentlich erreichbar sind, müssen ihre jeweiligen Ports am Router geöffnet werden. Aus Sicherheitsgründen sind auf dem Gerät installierte Dienste standardmäßig nur im LAN erreichbar. Wenn Sie einen WAN-Zugriff benötigen, können Sie hier gezielt Ports öffnen.



Klicken Sie auf **Add** und geben Sie im eingeblendeten Fenster die erforderlichen Angaben ein, um einen Port zu öffnen.

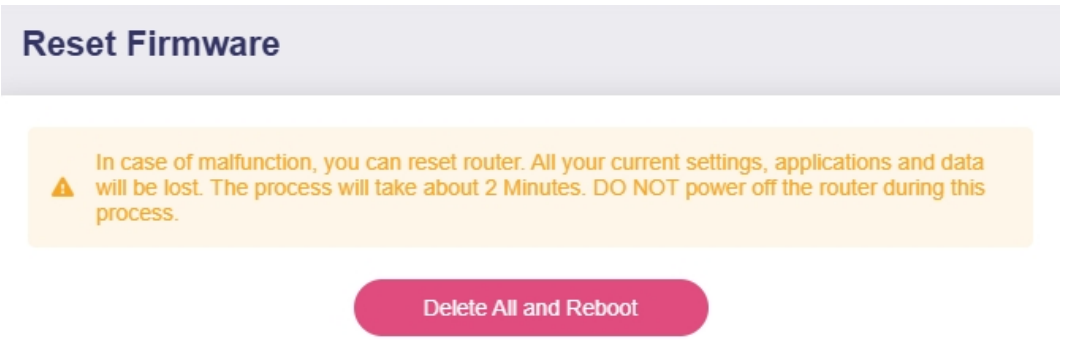


- **Protocol**: Wählen Sie das Netzwerkprotokoll für den Port aus: TCP, UDP oder TCP/UDP. Dies bestimmt die Art der Datenübertragung für den zugehörigen Dienst.
- **Port**: Geben Sie die Nummer des zu öffnenden Ports ein.
- **Description** (optional): Geben Sie zur einfacheren Verwaltung eine kurze Beschreibung des Verwendungszwecks ein, beispielsweise „Webserver“ oder „FTP-Dienst“.
- **Enable**: Aktiviert oder deaktiviert die Portweiterleitungsregel.

14.7 Firmware zurücksetzen

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SYSTEM** > **Reset Firmware**. Bei Fehlfunktionen können Sie versuchen, das Problem durch Zurücksetzen der Firmware zu beheben.

Klicken Sie bei Bedarf auf **Delete All and Reboot**, um die Firmware zurückzusetzen.



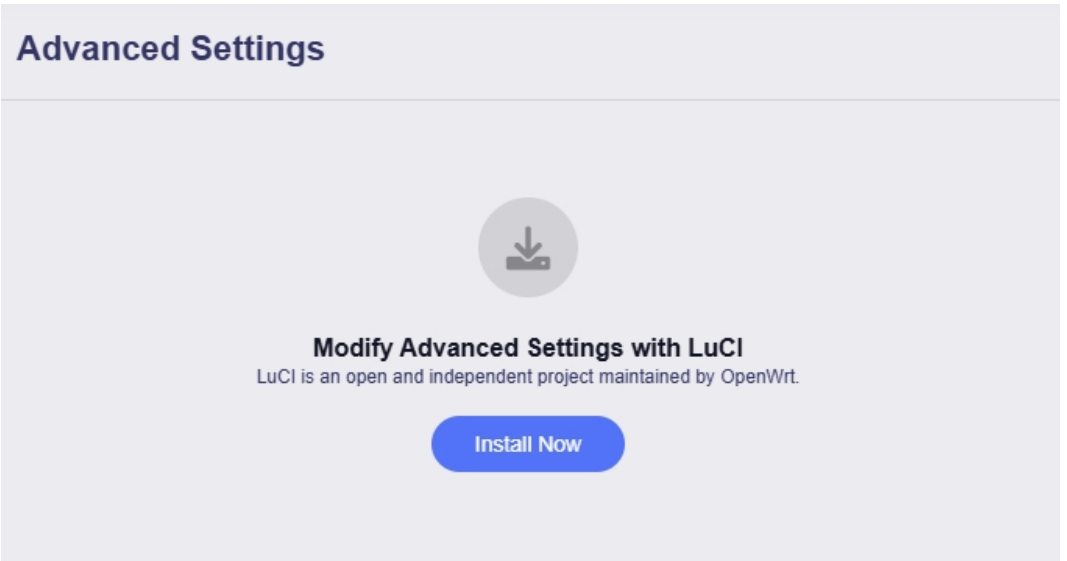
Hinweis: Alle aktuellen Einstellungen, Anwendungen und Daten werden gelöscht. Der Vorgang dauert etwa zwei Minuten. Schalten Sie den Router währenddessen nicht aus.

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

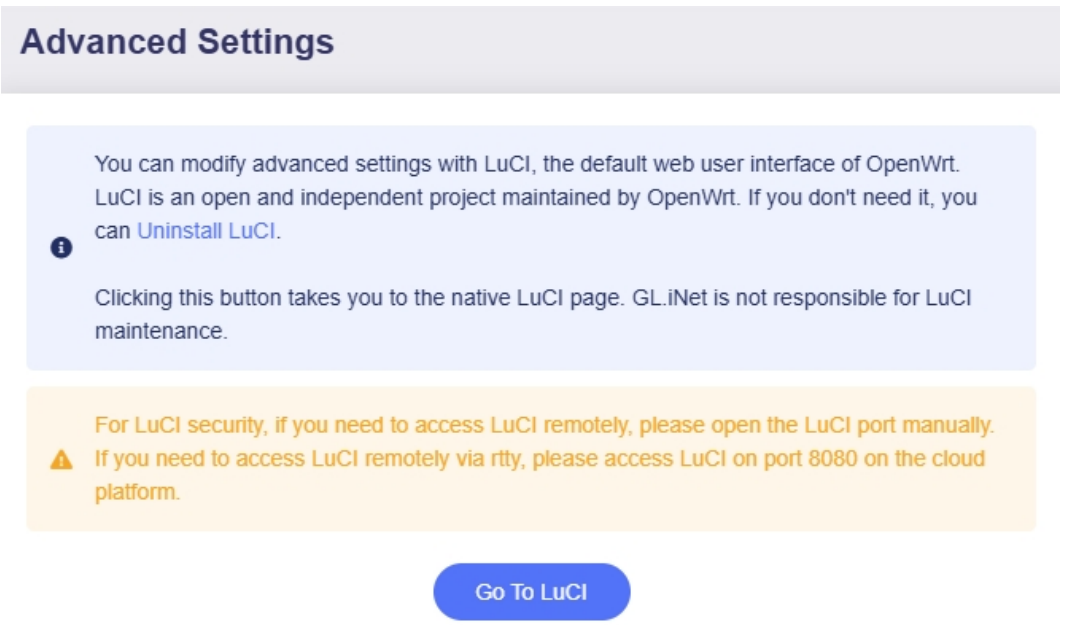
14.8 Erweiterte Einstellungen

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.

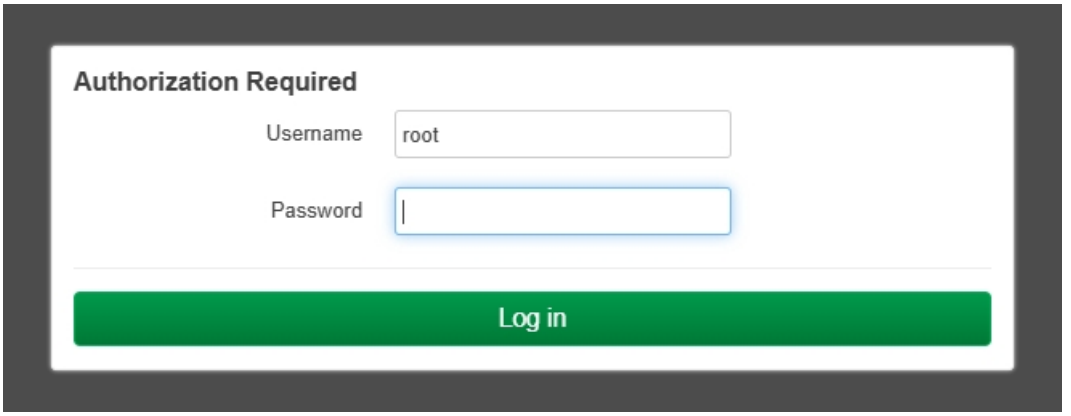
Klicken Sie auf **Install Now**, um die LuCI-Oberfläche zu installieren.



Klicken Sie auf **Go To LuCI**, um zur LuCI-Anmeldeseite zu gelangen.



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



Sie sind nun an der LuCI-Oberfläche angemeldet.

