GL·iNet



Benutzerhandbuch

GL-X3000 / Spitz AX

Wi-Fi-6-Mobilfunkrouter mit Dual-SIM für 4G/5G

Firmware-Version 4.8.3

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
- 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 zur 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 9

Kapitel 1 Ihren Router kennenlernen 11

1.1 Produktübersicht 12

1.1.1 Geräteansicht 12

1.1.2 Anschlüsse und Bedienelemente 13

1.1.3 LED-Anzeige 14

1.2 Technische Daten 15

1.3 Lieferumfang 16

Kapitel 2 Hardware anschließen 18

2.1 Standort auswählen 19

2.2 Router anschließen 19

Kapitel 3 Am Router anmelden 21

Kapitel 4 Internetverbindung einrichten 23

4.1 Schnelleinrichtung mit dem Assistenten 24

4.2 Internetverbindung manuell einrichten 25

4.2.1 Internetverbindung über Ethernetkabel 25

4.2.2 Internetverbindung über ein vorhandenes WLAN 31

4.2.3 Internetverbindung über USB-Tethering 45

4.2.4 Internetverbindung über Mobilfunk herstellen 49

Kapitel 5 WLAN 75

5.1 WLAN-Statusanzeige 76

5.2 WLAN-Einstellungen 77

5.2.1 5-GHz-WLAN 77

5.2.2 2,4-GHz-WLAN 79

5.2.3 Zufällige BSSID 81

Kapitel 6 Verbundene Geräte 84

6.1 Gerätedetails 85

6.2 Aktionen 88

6.3 Geräte entfernen 91

6.4 Sortierung 91

Kapitel 7 Cloud-Dienste 92

7.1 GoodCloud 93

7.1.1 GoodCloud aktivieren 94
7.1.2 Router verwalten 97
7.1.3 Geräteverknüpfung aufheben 102
7.1.4 GoodCloud deaktivieren 102
7.2 AstroWarp 104
Kapitel 8 VPN kennenlernen 105
8.1 Einführung 106
8.1.1 VPN 106
8.1.2 VPN-Router 106
8.1.3 OpenVPN 106
8.1.4 WireGuard 106
8.2 Einsatzmöglichkeiten 107
Kapitel 9 VPN-Dashboard 110
9.1 VPN-Einrichtungsassistent 111
9.2 VPN-Modus 114
9.2.1 Globaler Modus 115
9.2.2 Richtlinienmodus 116
Kapitel 10 VPN-Server einrichten 127
10.1 OpenVPN-Server 128
10.1.1 Vorbereitung 128
10.1.2 Einrichtung 129
10.1.3 Verbindung prüfen 132
10.1.4 Server-Optionen 133
10.1.5 Kommunikation zwischen Clients 134
10.2 WireGuard-Server 137
10.2.1 Vorbereitung 137
10.2.2 Einrichtung 139
10.2.3 Verbindung prüfen 143
10.2.4 Server-Optionen 144
Kapitel 11 VPN-Client einrichten 146
11.1 OpenVPN-Client 147
11.1.1 Vorbereitung 147
11.1.2 NordVPN einrichten 147
11.1.3 OpenVPN-Client manuell einrichten (andere Anbieter) 153

11.2 WireGuard-Client einrichten 156
11.2.1 Vorbereitung 156
11.2.2 AzireVPN einrichten 157
11.2.3 Hide.me einrichten 162
11.2.4 IPVanish einrichten 165
11.2.5 Mullvad einrichten 170
11.2.6 NordVPN einrichten 174
11.2.7 PIA (Private Internet Access) einrichten 180
11.2.8 Surfshark einrichten 185
11.2.9 WireGuard-Client manuell einrichten (andere Anbieter) 190
Kapitel 12 Tor 195
Kapitel 13 Anwendungen 197
13.1 Plug-ins 198
13.2 Dynamisches DNS 199
13.2.1 DDNS aktivieren 199
13.2.2 DDNS-Funktion prüfen 202
13.2.3 HTTPS-Fernzugriff 204
13.2.4 SSH-Fernzugriff 206
13.3 Netzwerkspeicher 208
13.3.1 Speicher anschließen 208
13.3.2 Samba einrichten 209
13.3.3 WebDAV einrichten 213
13.3.4 DLNA einrichten 216
13.4 AdGuard Home 217
13.5 Kindersicherung 220
13.5.1 Schnelleinrichtung 220
13.5.2 Fehlerbehebung 229
13.6 ZeroTier 230
13.6.1 ZeroTier einrichten 231
13.6.2 Fernzugriff auf WAN erlauben 235
13.6.3 Fernzugriff auf LAN erlauben 237
13.7 Tailscale 238
13.7.1 Tailscale einrichten 239
13.7.2 Fernzugriff auf WAN erlauben 242

13.7.3 Fernzugriff auf LAN erlauben 243
13.7.4 Eigene Exit-Nodes 244
13.8 eSIM-Verwaltung 245
13.8.1 Aktueller eSIM-Status 246
13.8.2 eSIM-Profilliste 247
Kapitel 14 Netzwerk 254
14.1 Portweiterleitung 255
14.1.1 DMZ 255
14.1.2 Portweiterleitung 256
14.2 Multi-WAN 259
14.2.1 Schnittstellenstatus überwachen 259
14.2.2 Multi-WAN-Modus 262
14.3 LAN 265
14.3.1 Grundeinstellungen 265
14.3.2 DHCP-Server 266
14.3.3 Adressreservierung 268
14.4 Gastnetzwerk 269
14.4.1 Grundeinstellungen 269
14.4.2 DHCP-Server 270
14.5 DNS 272
14.5.1 Allgemeine Einstellungen 272
14.5.2 DNS-Servereinstellungen 273
14.5.3 Hosts bearbeiten 275
14.6 Ethernetanschlüsse 277
14.7 Netzwerkmodus 278
14.8 IPv6 281
14.8.1 IPv6-Modus 282
14.8.2 DNS-Adressen beziehen 282
14.9 Drop-in Gateway 283
14.10 IGMP Snooping 285
14.11 Netzwerkbeschleunigung 286
14.12 NAT-Einstellungen 287
Kapitel 15 System 288
15.1 Übersicht 289

15.2 Aktualisierung 290
15.2.1 Firmware online aktualisieren 290
15.2.2 Firmware lokal aktualisieren 291
15.2.3 Modem online aktualisieren 292
15.2.4 Modem lokal aktualisieren 292
15.3 Geplante Aufgaben 293
15.3.1 LED-Zeitplan 293
15.3.2 Geplanter Neustart 294
15.3.3 Zeitplan für das 5-GHz-WLAN 295
15.3.4 Zeitplan für das 2,4-GHz-WLAN 297
15.4 Zeitzone 299
15.5 Protokolle 301
15.6 Sicherheit 303
15.6.1 Administratorpasswort 303
15.6.2 Zugriffskontrolle 304
15.6.3 Fernzugriffskontrolle 307
15.6.4 Ports am Router öffnen 308
15.7 Firmware zurücksetzen 309
15.8 Erweiterte Einstellungen 310
Konformitätserklärung 312

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

Spitz AX (GL-X3000) ist ein Mobilfunkgateway mit Dual-SIM und Wi-Fi 6, das insbesondere in abgelegenen Gebieten und auf Reisen schnelle, zuverlässige Verbindungen ermöglicht. Es bietet vier Möglichkeiten für den Internetzugang: Mobilfunk (SIM-Karten), Ethernet, Repeater und Tethering. Es unterstützt unter anderem Multi-WAN (Ausfallsicherung und Lastverteilung), VPN (OpenVPN und WireGuard), Kindersicherung, AdGuard Home, Portweiterleitung und Tailscale.

1.1.1 Geräteansicht

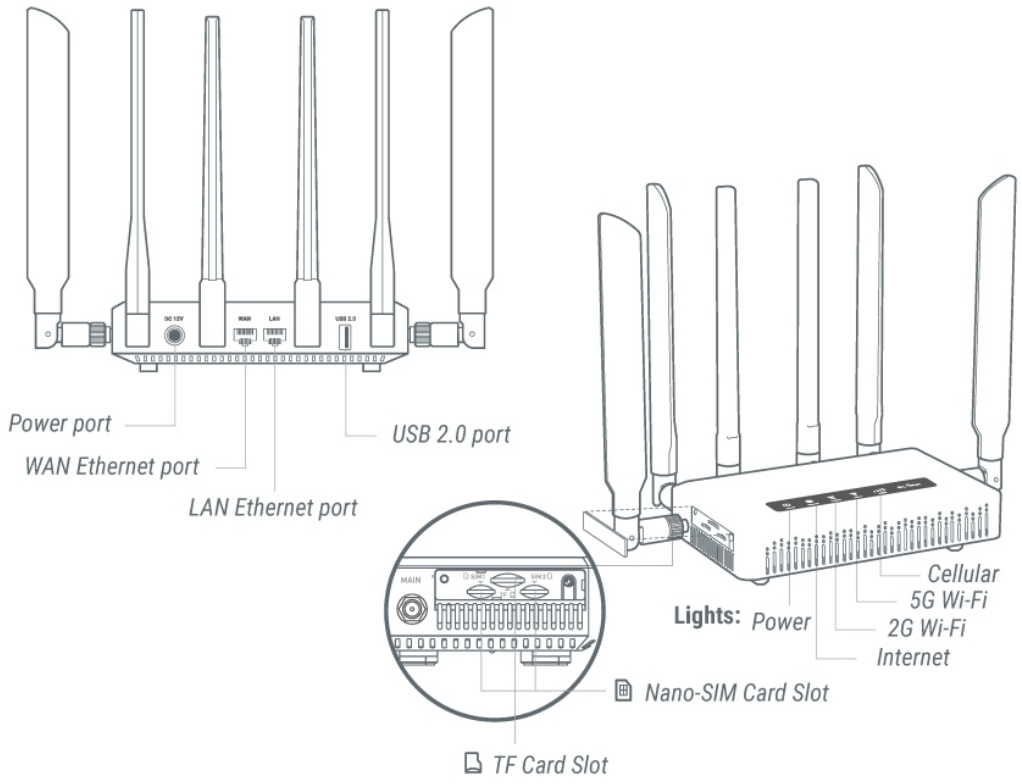








1.1.2 Anschlüsse und Bedienelemente



Element	Beschreibung
WAN-Ethernetanschluss	Verbindet den Router mit einem übergeordneten Netzwerk mit 10/100/1000/2500 Mbit/s.
LAN-Ethernetanschluss	Verbindet ein kabelgebundenes Endgerät mit dem Router mit 10/100/1000 Mbit/s.
USB-2.0-Anschluss	Zum Anschließen eines unterstützten USB-Modems, eines Tethering-Geräts oder eines USB-Speichergeräts.
MicroSD-Kartensteckplatz	Für eine MicroSD-Karte mit einer maximalen Kapazität von 1 TB.

Element	Beschreibung
Nano-SIM-Kartensteckplätze	Für zwei Nano-SIM-Karten. Es ist jeweils nur eine SIM-Karte aktiv; die andere dient als Reserve.
Reset-Taste	Drücken Sie die Taste kürzer als 3 Sekunden, um die Netzwerkeinstellungen zurückzusetzen, oder 10 Sekunden lang, um die Werkseinstellungen wiederherzustellen.
DC5521-Stromanschluss	Für das mitgelieferte Netzteil mit 12 V/2,5 A oder eine Gleichstromversorgung mit 9–36 V.
Mobilfunkantennenanschlüsse	Zum Anschließen von vier Mobilfunkantennen (SMA, 600 MHz bis 6 GHz).
WLAN-Antennenanschlüsse	Zum Anschließen von zwei WLAN-Antennen (PR-SMA, 2,4–2,5 GHz und 5,15–5,84 GHz).

1.1.3 LED-Anzeige

Gerätestatus	Strom	Internet	2,4 GHz	5 GHz	Mobilfunk
Internetzugang vorhanden (Mobilfunk aktiv)	Leuchtet grün	Leuchtet grün	Leuchtet grün	Leuchtet grün	Leuchtet grün
Internetzugang vorhanden (Mobilfunk inaktiv)	Leuchtet grün	Leuchtet grün	Leuchtet grün	Leuchtet grün	Aus
Kein Internetzugang	Leuchtet grün	Aus	Leuchtet grün	Leuchtet grün	Aus
Firmware wird aktualisiert	Leuchtet grün	Blinkt alle 0,5 Sekunden	Blinkt alle 0,5 Sekunden	Blinkt alle 0,5 Sekunden	Leuchtet grün

Gerätestatus	Strom	Internet	2,4 GHz	5 GHz	Mobilfunk
Netzwerk zurücksetzen (Reset-Taste kürzer als 3 Sekunden drücken)	Blinkt jede Sekunde	Leuchtet grün	Leuchtet grün	Leuchtet grün	Leuchtet grün
Werkszustand wiederherstellen (Reset-Taste 10 Sekunden drücken)	Blinkt alle 0,25 Sekunden	Leuchtet grün	Leuchtet grün	Leuchtet grün	Leuchtet grün

Tipps: Wenn eine Internetverbindung besteht, zeigt eine blinkende LED für 2,4 GHz oder 5 GHz an, dass WLAN-Geräte verbunden sind und Daten übertragen.

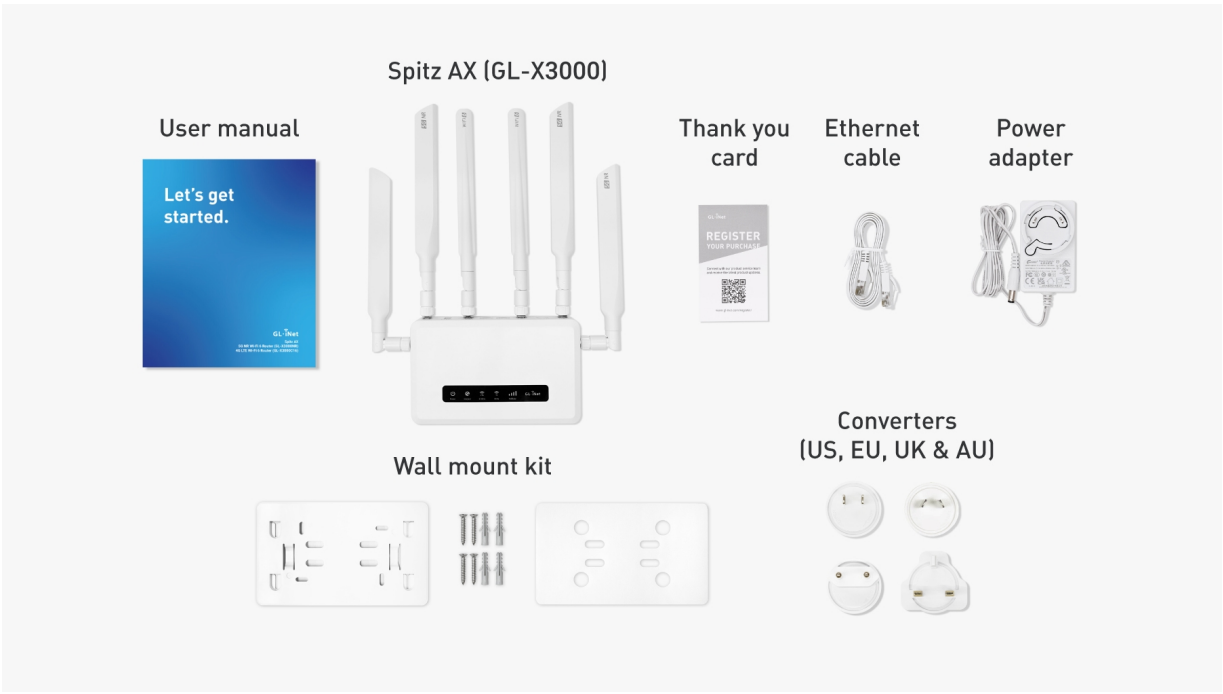
1.2 Technische Daten

Element	Details
Anschlüsse	1 × WAN-Ethernetanschluss 1 × LAN-Ethernetanschluss 1 × USB-2.0-Anschluss 1 × MicroSD-Kartensteckplatz (max. 1 TB) 2 × Nano-SIM-Kartensteckplätze 1 × Reset-Taste
CPU	MediaTek Dual-Core, 1,3 GHz
Arbeitsspeicher / Speicher	512 MB DDR4 / 8 GB eMMC
Protokoll	IEEE 802.11a/b/g/n/ac/ax
WLAN-Geschwindigkeit	574 Mbit/s (2,4 GHz), 2402 Mbit/s (5 GHz)

Element	Details
Ethernet-Geschwindigkeit	WAN-Anschluss: 10/100/1000/2500 Mbit/s LAN-Anschluss: 10/100/1000 Mbit/s
Antennen	4 × Mobilfunkantenne (SMA, 600 MHz bis 6 GHz) 2 × WLAN-Antenne (PR-SMA, 2,4–2,5 GHz, 5,15–5,84 GHz)
LED-Anzeigen	System / 5-GHz-WLAN / 2,4-GHz-WLAN / Internet / Mobilfunksignalstärke
Stromversorgung	DC5521, 12 V/2,5 A (5,5 × 2,1 mm) [mitgeliefertes Netzteil] / 9–36 V
Leistungsaufnahme	<14W
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Lagertemperatur	-20 ~ 70°C (-4 ~ 158°F)
Abmessungen / Gewicht	155 × 95 × 36 mm / 520 g
Weitere Ressourcen	Datenblatt | Firmware | App | Auspacken | Anleitungen | Pressekit

1.3 Lieferumfang

- 1 × Spitz AX (GL-X3000)
- 1 × Benutzerhandbuch
- 1 × Dankeskarte
- 1 × Ethernetkabel
- 1 × Wandmontageset
- 1 × Netzteil
- 4 × Adapter


Spitz AX (GL-X3000)
User manual
Let's get started.
Thank you card
REGISTER
Ethernet cable
Power adapter
Wall mount kit
Converters (US, EU, UK & AU)

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, Feuchtigkeit 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: Wählen Sie einen Standort, an dem sich der Router leicht an die Stromversorgung und mehrere Geräte anschließen lässt, etwa in der Mitte des Wohnzimmers.
- Sichere Kabelführung: Verlegen Sie Kabel und Netzkabel so, dass keine Stolpergefahr entsteht.
- Aufstellung: Stellen Sie den Router auf eine ebene, stabile Fläche, etwa ein Regal oder einen Schreibtisch, oder befestigen Sie ihn mit dem mitgelieferten Wandmontagesatz an der Wand.
- Elektromagnetische Störungen vermeiden: Halten Sie den Router von Störquellen wie Bluetooth-Geräten und Mikrowellen fern, um Signalstörungen zu verringern.

2.2 Router anschließen

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

3. **Am Router anmelden**

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

Kapitel 3

Am Router anmelden

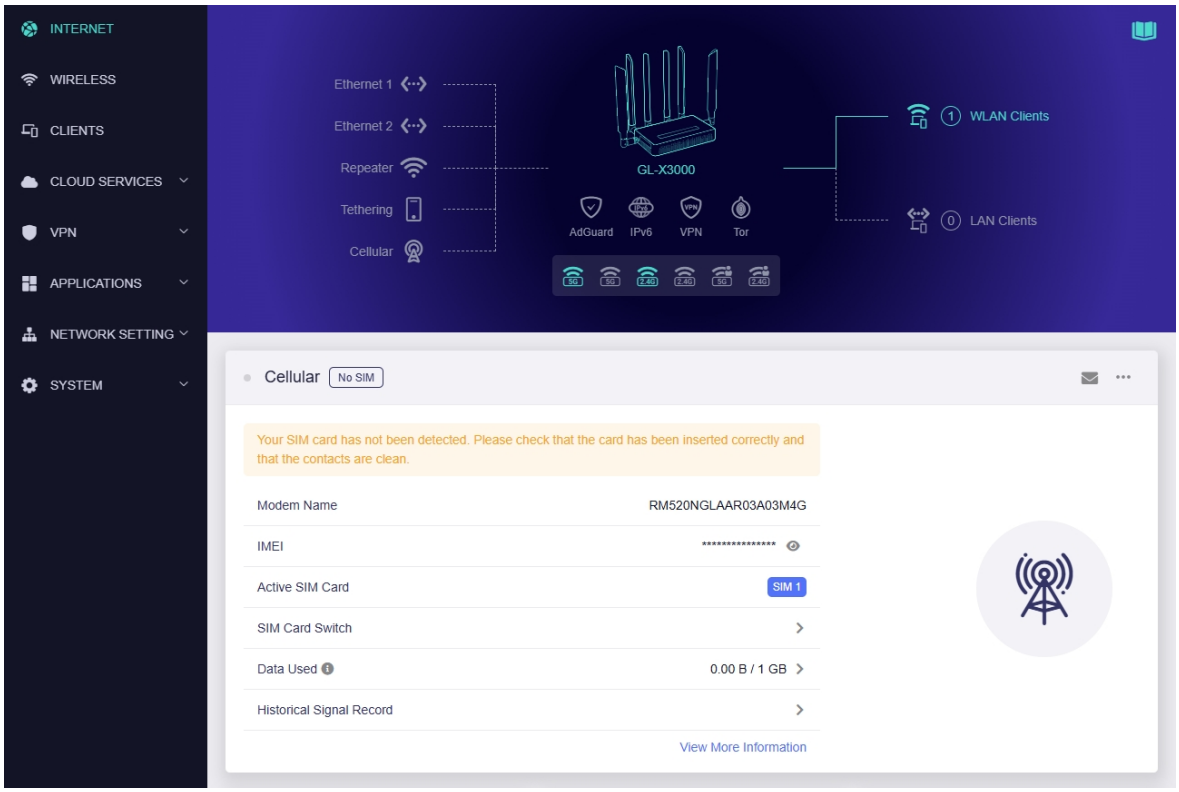
Dieses Kapitel erklärt, wie Sie sich über die Weboberfläche an Ihrem Router anmelden.

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

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

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

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



Kapitel 4

Internetverbindung einrichten

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

4.1 Schnelleinrichtung mit dem Assistenten

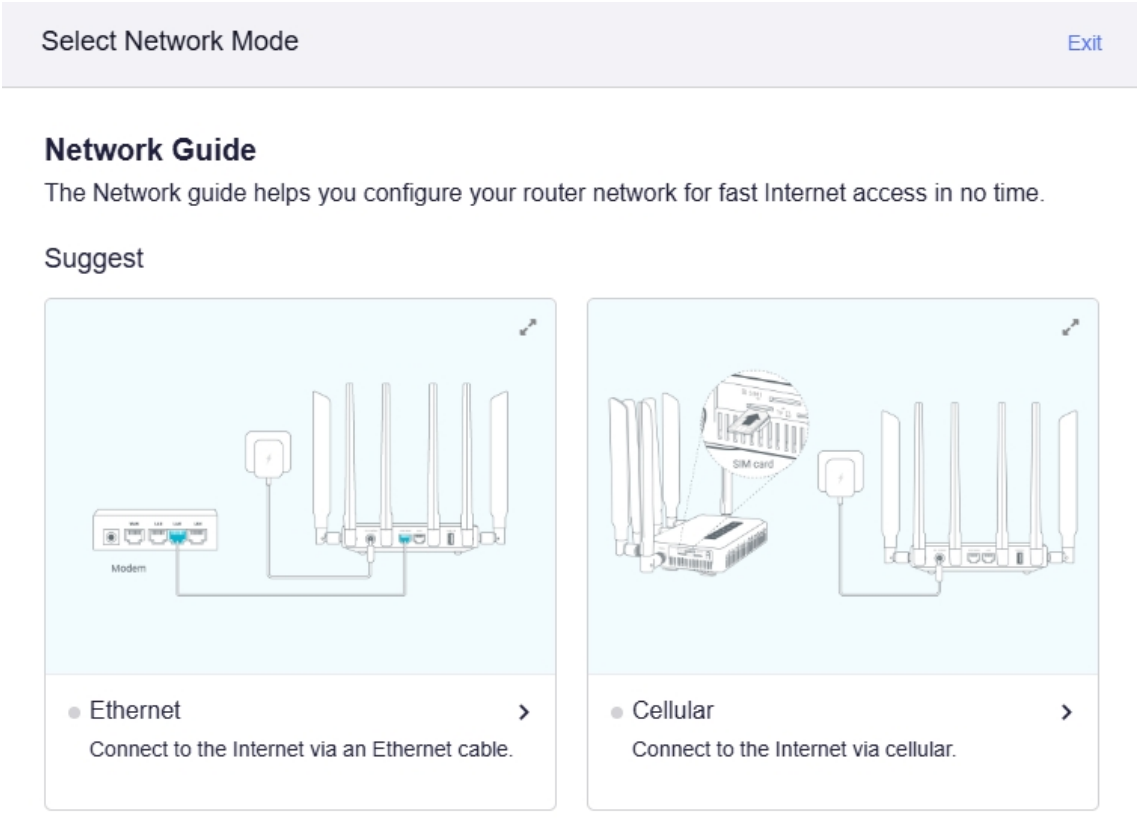
Der Einrichtungsassistent in der Weboberfläche führt Sie durch die Netzwerkkonfiguration des Routers.

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.



Wenn Sie die GL.iNet-App verwenden, folgen Sie den Bildschirmanweisungen, um den Internetzugang einzurichten.

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.

Dieser Router unterstützt vier Möglichkeiten für die Internetverbindung: Ethernet, Repeater, USB-Tethering und Mobilfunk. Wählen Sie die für Ihren Bedarf geeignete Methode.

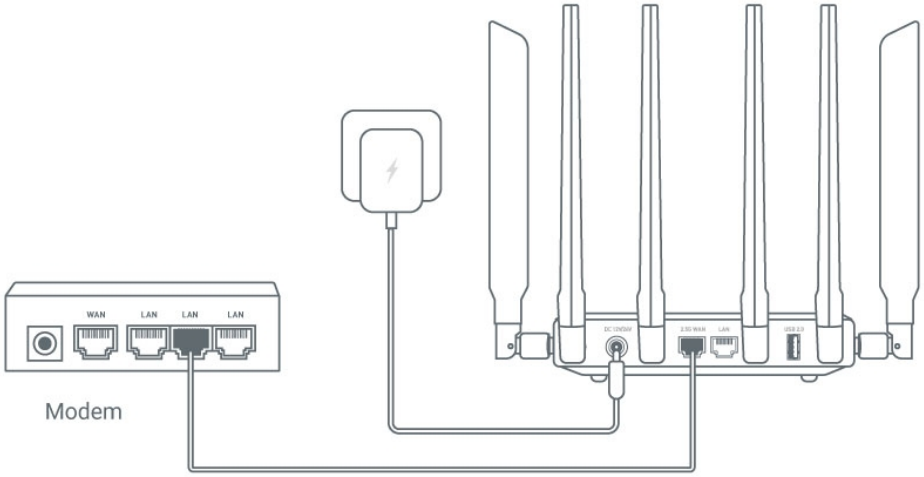
4.2.1 Internetverbindung über Ethernetkabel

Verbinden Sie den Router über ein Ethernetkabel am WAN-Anschluss mit einem Breitbandnetzwerk. In der Regel erhält er automatisch eine IP-Adresse (DHCP). Sie können auch manuell eine statische IP-Adresse oder PPPoE konfigurieren. Diese Methode bietet eine hohe Stabilität und Geschwindigkeit und eignet sich besonders für Privathaushalte und Büros mit festem Breitbandanschluss.

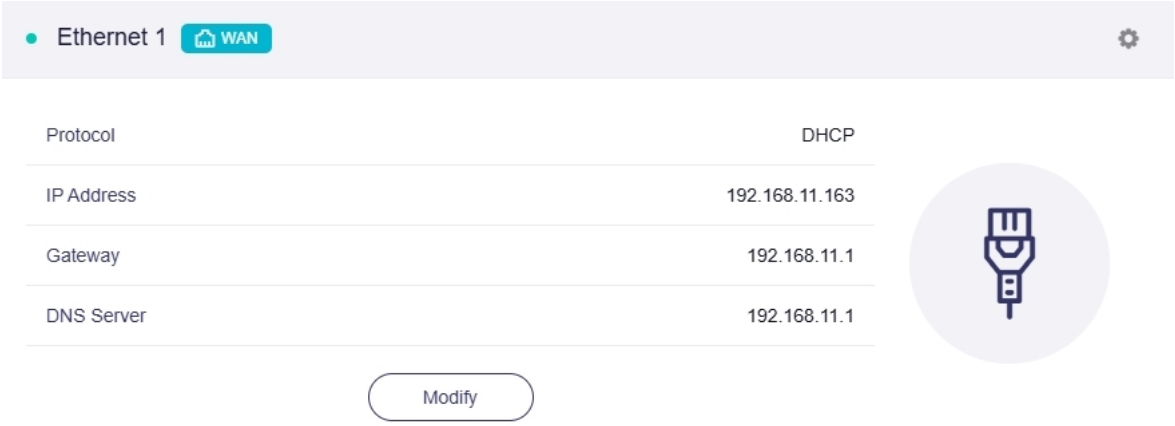
4.2.1.1 Grundlegende Schritte

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, einem Router, einem Netzwerkswitch oder einer Ethernetdose.



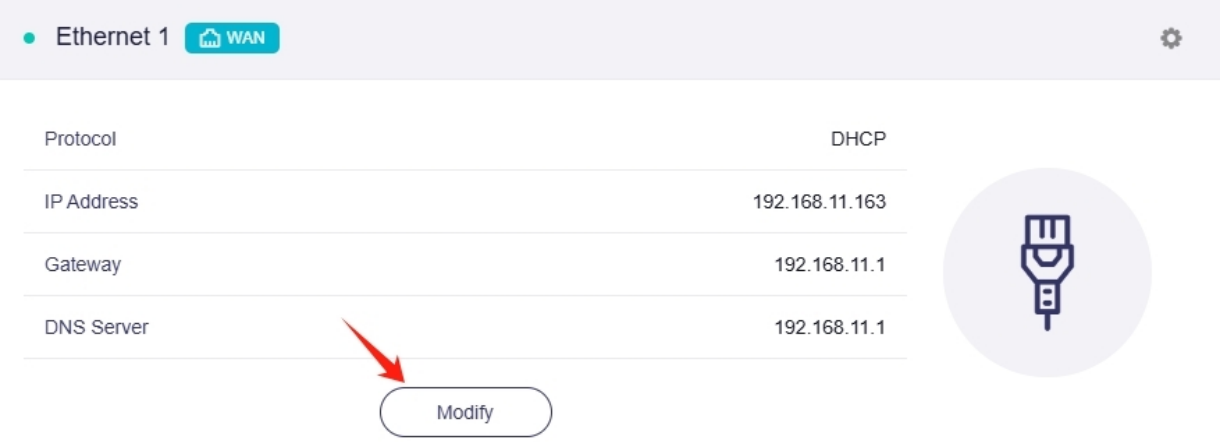
2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie den Bereich **INTERNET** > **Ethernet**.
   Bei erfolgreicher Verbindung werden im Bereich Ethernet die Netzwerkdetails angezeigt, darunter Protokoll, IP-Adresse, Gateway und DNS-Server.



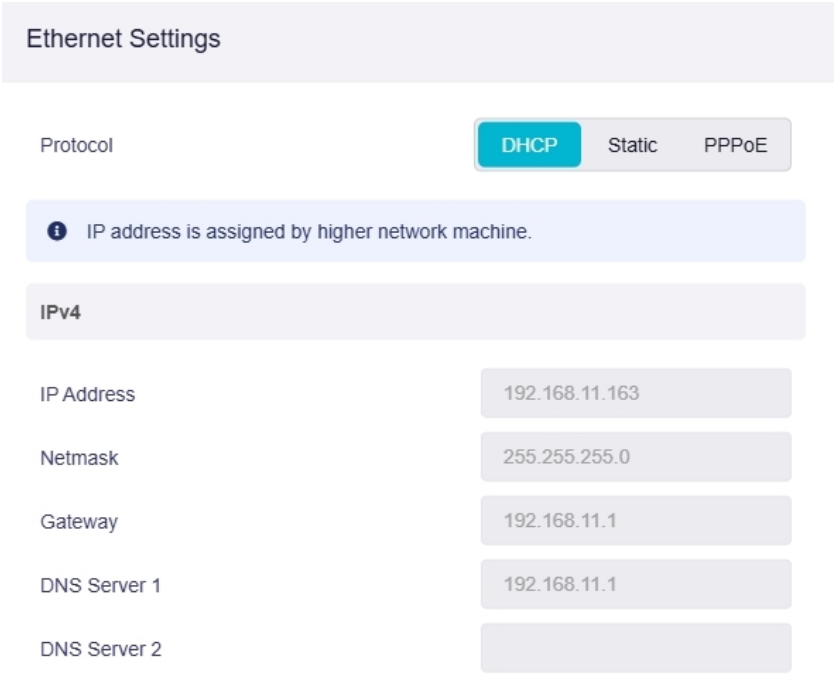
Tipp: Bei Bedarf können Sie den WAN-Anschluss als LAN-Anschluss verwenden. Dies ist nützlich, wenn Sie den Router als Repeater einsetzen und der physische WAN-Anschluss ungenutzt bleibt. Dadurch steht Ihnen ein zusätzlicher LAN-Anschluss zur Verfügung.

4.2.1.2 Protokoll

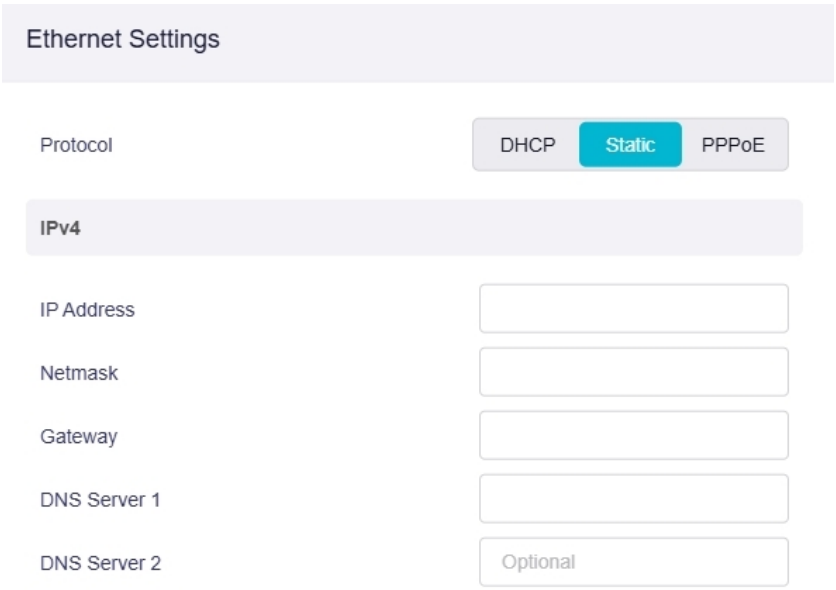
Es stehen drei Protokolle zur Verfügung: DHCP, Static und PPPoE. Klicken Sie zum Ändern auf **Modify**.



- **DHCP**
  DHCP ist das voreingestellte und am häufigsten verwendete Protokoll. Es weist Netzwerkgeräten in IP-Netzwerken über eine Client-Server-Architektur automatisch IP-Adressen und andere Kommunikationsparameter zu.

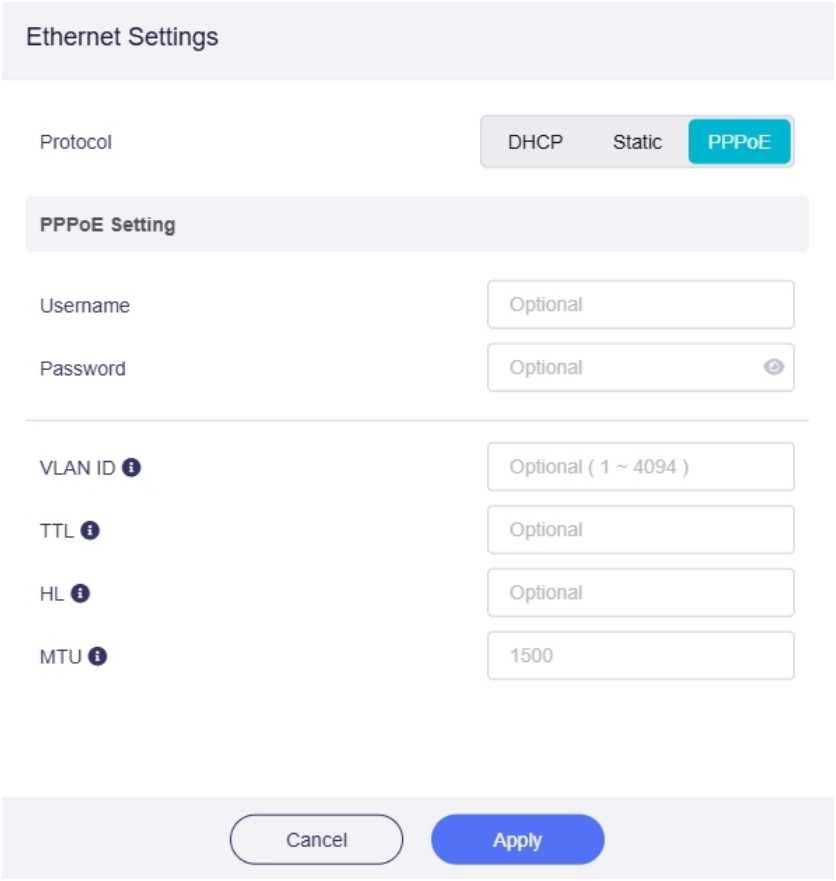


- **Statische IP-Adresse**
  Static ist erforderlich, wenn Ihr Internetanbieter eine feste IP-Adresse bereitstellt oder Sie Netzwerkinformationen wie IP-Adresse, Gateway und Netzmaske manuell konfigurieren möchten.



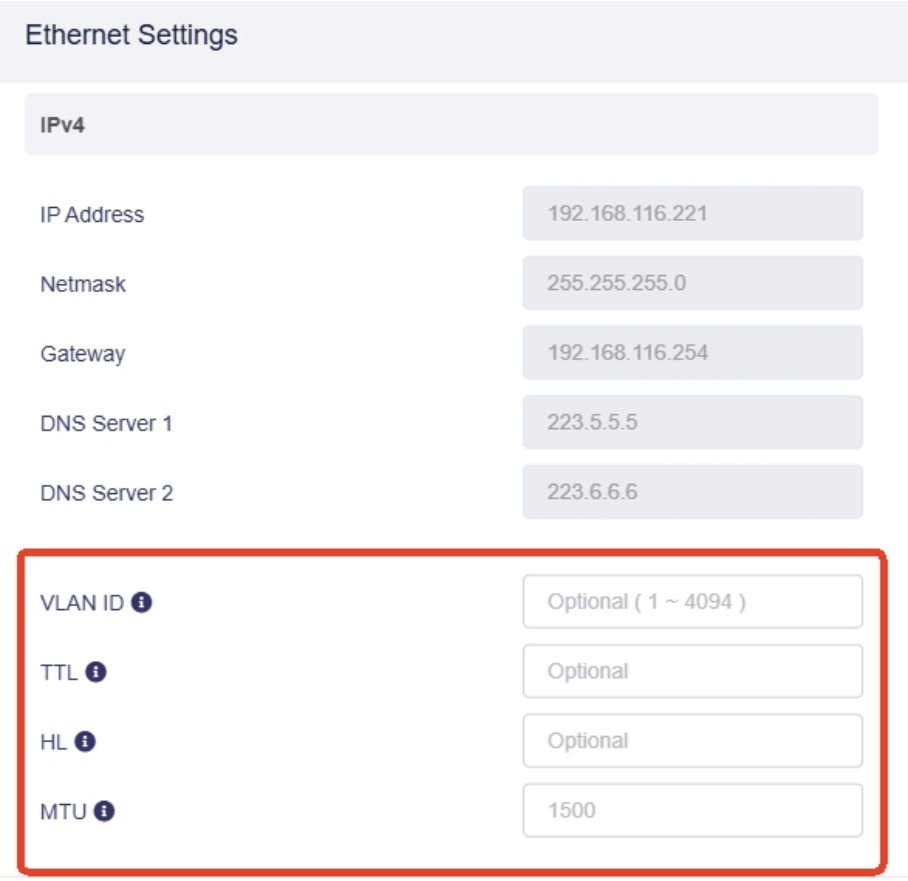
- **PPPoE**

  PPPoE ist ein von vielen Internetanbietern verwendetes Protokoll. In der Regel stellen diese ein Modem sowie einen Benutzernamen und ein Passwort bereit, die für die Einrichtung des Internetzugangs benötigt werden.



4.2.1.3 Erweiterte Einstellungen

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

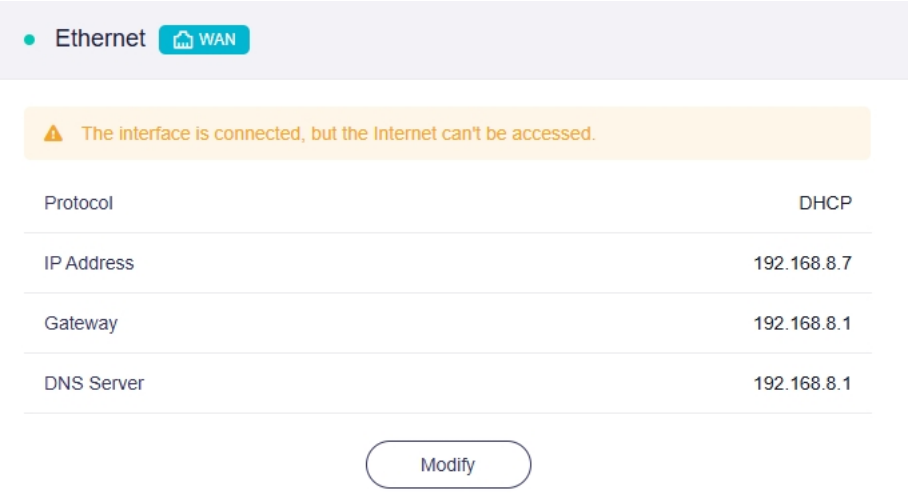


- **VLAN ID**: Diese Einstellung ist nur erforderlich, wenn der Server des Anbieters für die Schnittstelle eine bestimmte VLAN-ID mit Tag verlangt.
- **TTL**: TTL (Time To Live) legt fest, wie lange Datenpakete maximal im Netzwerk verbleiben dürfen. Standardmäßig verringert der Router den TTL-Wert eingehender Pakete von Endgeräten vor der Weiterleitung um 1. Die TTL-Einstellung gilt nur für IPv4. Wenn Sie den TTL-Wert überschreiben oder einen anderen Wert vortäuschen möchten, legen Sie hier einen festen Wert fest. Geben Sie bei den meisten Modellen den gewünschten wirksamen TTL-Wert plus 1 ein, um die automatische Verringerung auszugleichen.
- **HL**: Bei IPv6 begrenzt das Feld HL (Hop Limit) die Anzahl der Übertragungsschritte von Datenpaketen im Netzwerk. Es entspricht der TTL bei IPv4.
- **MTU**: Der Standardwert der MTU beträgt 1500 Byte.

4.2.1.4 Fehlerbehebung

Wenn ein Ethernetkabel am WAN-Anschluss angeschlossen ist, aber kein Internetzugang besteht, wird die folgende gelbe Meldung angezeigt.

„Die Schnittstelle ist verbunden, aber es besteht kein Internetzugang.“

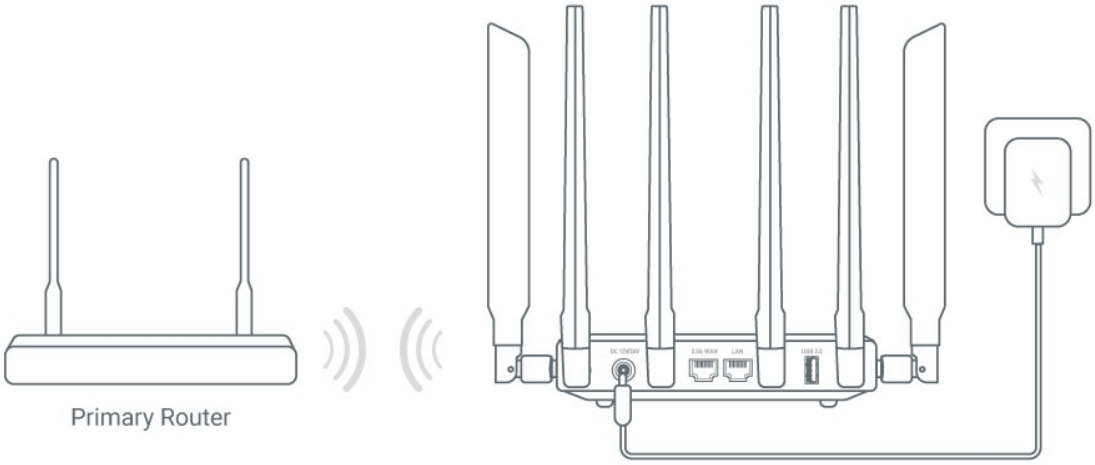


So beheben Sie das Problem:

1. Prüfen Sie, ob das vorgeschaltete Gerät Internetzugang hat.
2. Öffnen Sie die Seite Multi-WAN und prüfen Sie den Status der Ethernet-Schnittstelle.

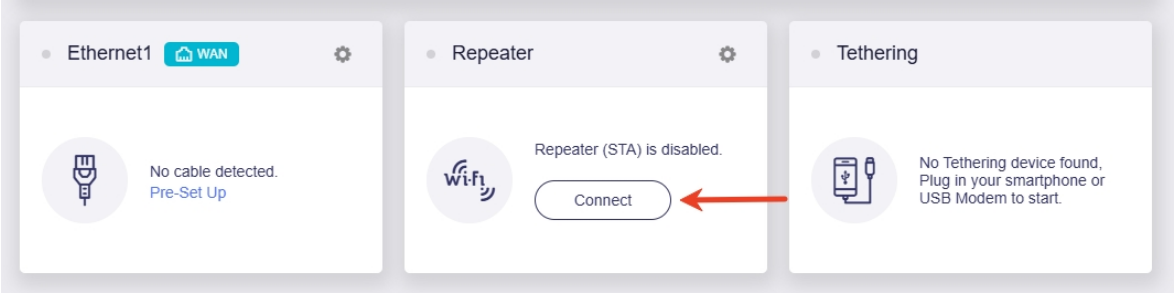
4.2.2 Internetverbindung über ein vorhandenes WLAN

Im Repeater-Betrieb verbindet sich der Router mit einem vorhandenen WLAN, etwa dem kostenlosen WLAN eines Hotels oder Cafés. Standardmäßig arbeitet er im WISP-Modus (Wireless Internet Service Provider). Dabei erstellt der Router ein eigenes Subnetz und schützt Sie durch seine Firewall vor dem öffentlichen Netzwerk.

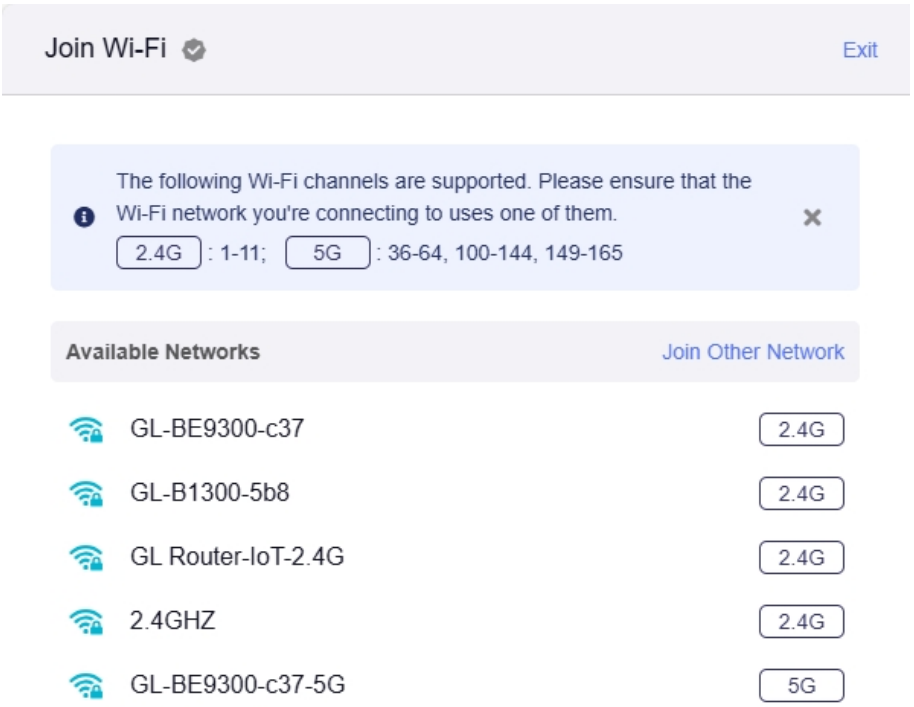


4.2.2.1 Grundlegende Schritte

1. Melden Sie sich an der Weboberfläche des Routers an, öffnen Sie den Bereich **INTERNET** > **Repeater** und klicken Sie auf **Connect**.



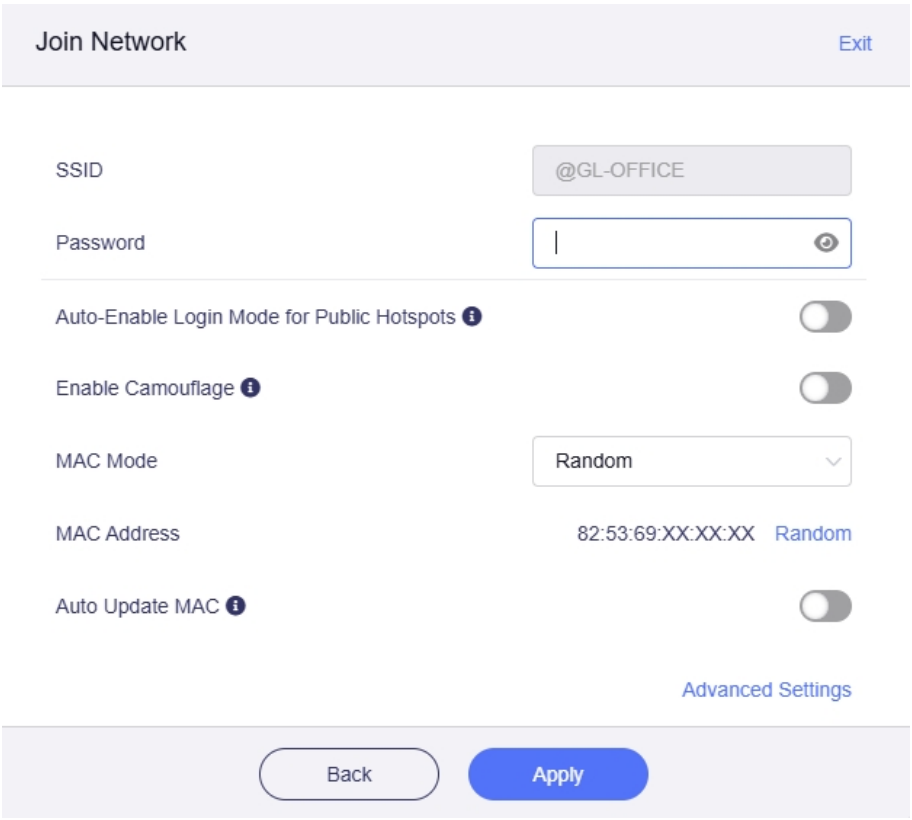
2. Wählen Sie in der Liste der verfügbaren Netzwerke das WLAN aus, mit dem Sie sich verbinden möchten.



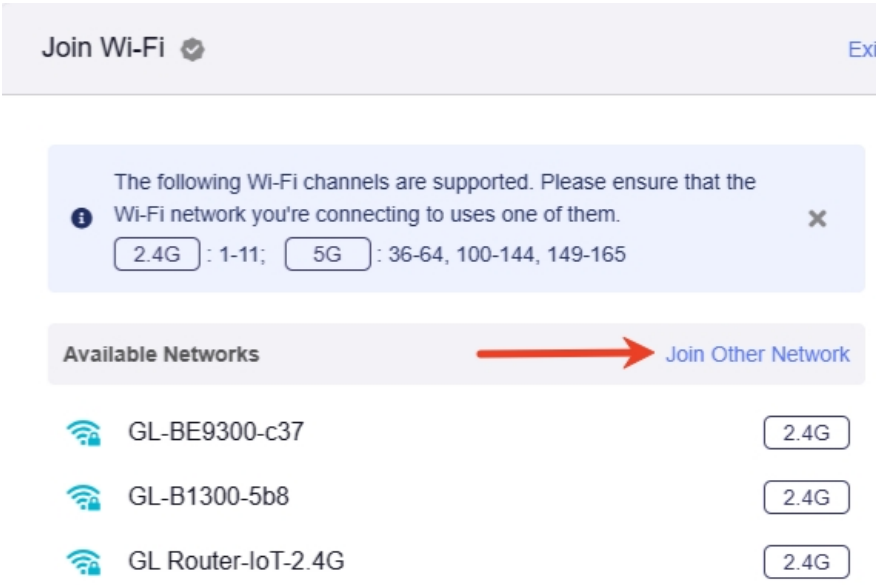
Hinweis:

1. Diese Seite zeigt die vom Router unterstützten WLAN-Kanäle an. Vergewissern Sie sich, dass das gewünschte WLAN einen dieser Kanäle verwendet. Andernfalls wird es möglicherweise nicht in der Liste der verfügbaren Netzwerke angezeigt.
2. Lassen Sie Ihr iPhone beim Suchen nach dessen persönlichem Hotspot entsperrt, damit es weiterhin WLAN-Beacons sendet. Andernfalls kann der Router den Hotspot möglicherweise nicht erkennen.

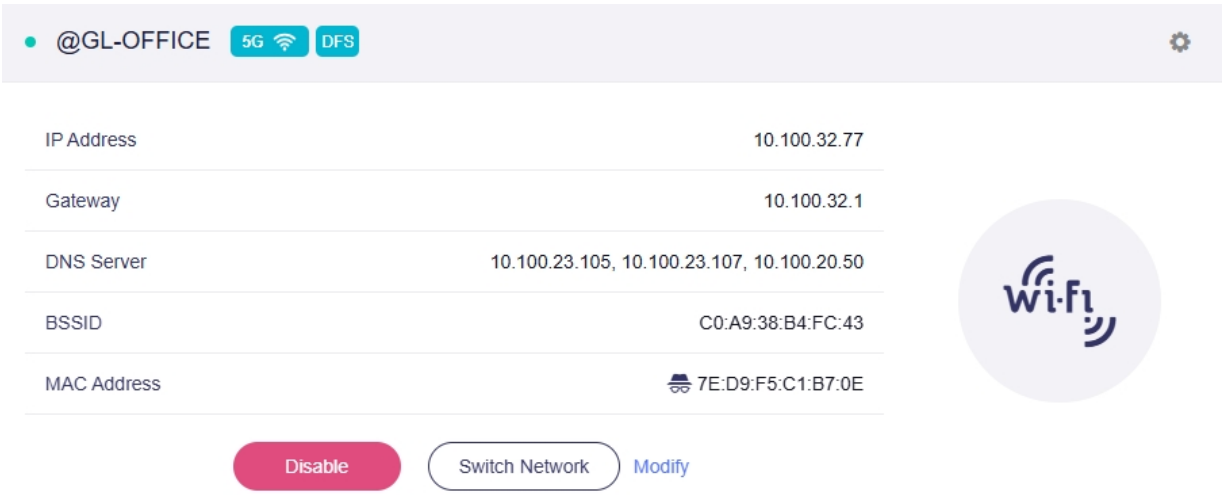
3. Geben Sie das richtige WLAN-Passwort ein und klicken Sie auf **Apply**.



Tipp: Wenn die gewünschte WLAN-SSID nicht in der Liste der verfügbaren Netzwerke angezeigt wird, klicken Sie oben rechts auf **Join Other Network**. Geben Sie die WLAN-SSID und die weiteren erforderlichen Informationen manuell ein und klicken Sie auf **Apply**.

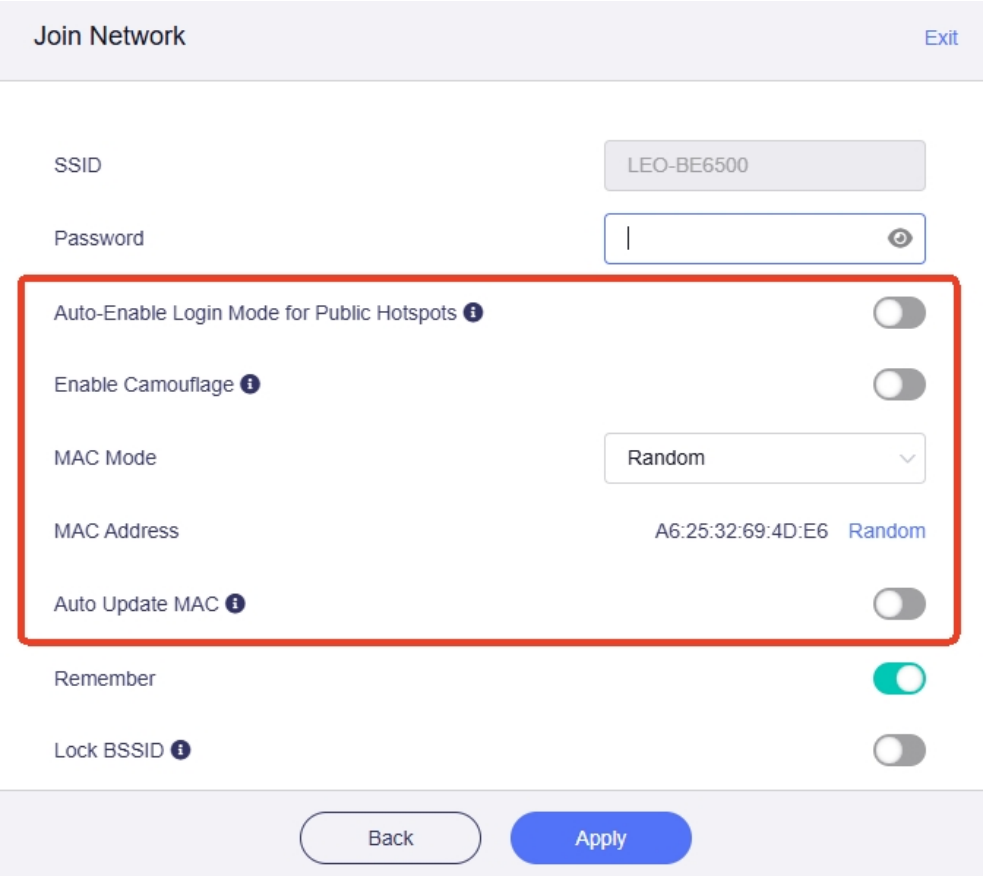


4. Wenn das Passwort korrekt ist, wird die Verbindung nach kurzer Zeit hergestellt.


@GL-OFFICE
5G
DFS
IP Address
10.100.32.77
Gateway
10.100.32.1
DNS Server
10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID
C0:A9:38:B4:FC:43
MAC Address
7E:D9:F5:C1:B7:0E
Disable
Switch Network
Modify

4.2.2.2 Öffentliche Hotspots

Beim Verbinden mit einem öffentlichen Hotspot mit Anmeldeportal können die folgenden Funktionen die Erfolgsaussichten verbessern.



- **Anmeldemodus für öffentliche Hotspots automatisch aktivieren**
  Bei aktivierter Option wechselt der Router automatisch in den Anmeldemodus für öffentliche Hotspots, wenn er mit einem Hotspot verbunden ist, aber keinen Internetzugang hat. In diesem Modus werden einige Dienste angehalten und der DNS-Modus auf automatisch umgestellt. Dadurch kann Ihr Netzwerkverkehr für den Netzwerkanbieter, beispielsweise ein Hotel oder Einkaufszentrum, sichtbar werden. Auch bei deaktivierter Option fordert der Router Sie zum Wechsel in diesen Modus auf, wenn er eine Hotspot-Anmeldeseite erkennt oder die Anmeldung fehlschlägt.
- **Tarnmodus aktivieren**
  Bei aktivierter Option gibt sich der Router als das Endgerät aus, mit dem Sie auf die Weboberfläche zugreifen, indem er dessen MAC-Adresse nachbildet.

- **MAC-Modus**
  Wählen Sie die MAC-Adresse aus, die der Router für die Verbindung mit dem öffentlichen Hotspot verwenden soll.

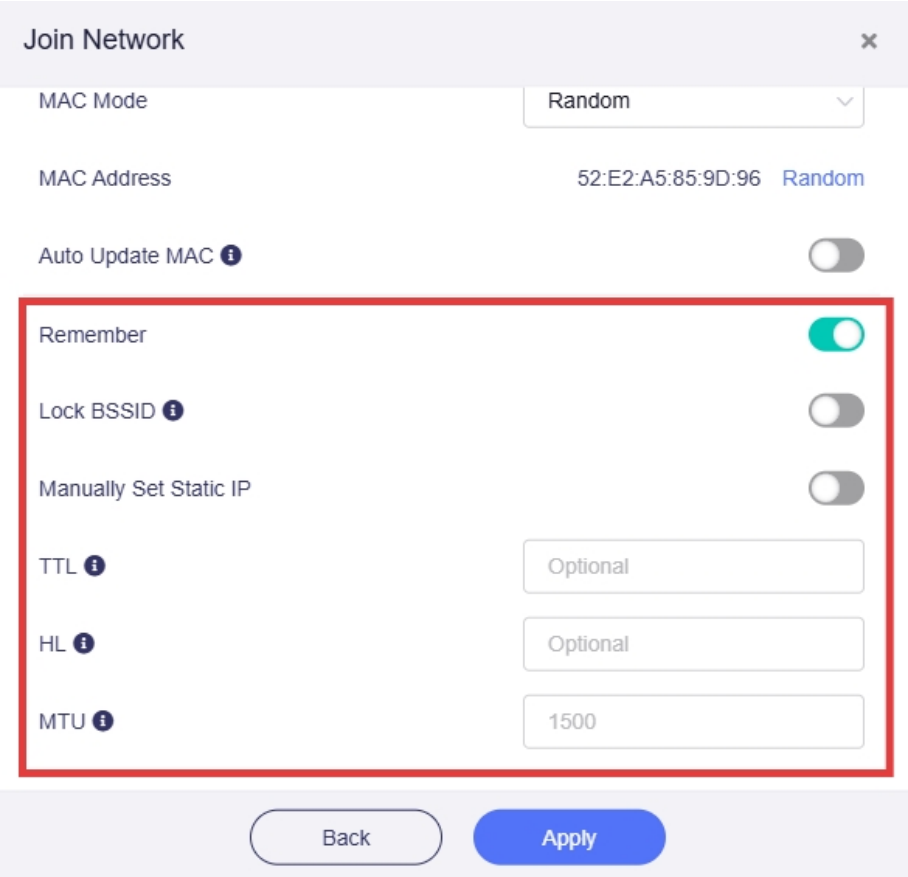
Werkseinstellung	Verwendet die dem Gerät ab Werk zugewiesene MAC-Adresse.
Klonen	Übernimmt für die Verbindung die MAC-Adresse eines Endgeräts. Wenn die gewünschte MAC-Adresse nicht aufgeführt ist, geben Sie die zu klonende Adresse manuell ein. Hinweis: Viele Geräte verwenden beim Verbinden mit WLANs zufällige MAC-Adressen, häufig als „Private WLAN-Adresse“ oder „Zufällige Hardwareadresse“ bezeichnet. Die hier angezeigte MAC-Adresse kann daher von der tatsächlichen Hardwareadresse des Geräts abweichen.
Zufällig	Erzeugt automatisch eine zufällige MAC-Adresse für die Verbindung.

- **MAC-Adresse automatisch aktualisieren**
  Bei aktivierter Option wird die MAC-Adresse automatisch aktualisiert.

Beim Speichern der Netzwerkkonfiguration wird der MAC-Modus einschließlich einer geklonten oder zufälligen MAC-Adresse der jeweiligen gespeicherten SSID zugeordnet. Sie können diese Einstellungen jederzeit für jede SSID manuell ändern.

4.2.2.3 Erweiterte Einstellungen

Beim Beitreten zum Netzwerk stehen weitere Optionen zur Verfügung.

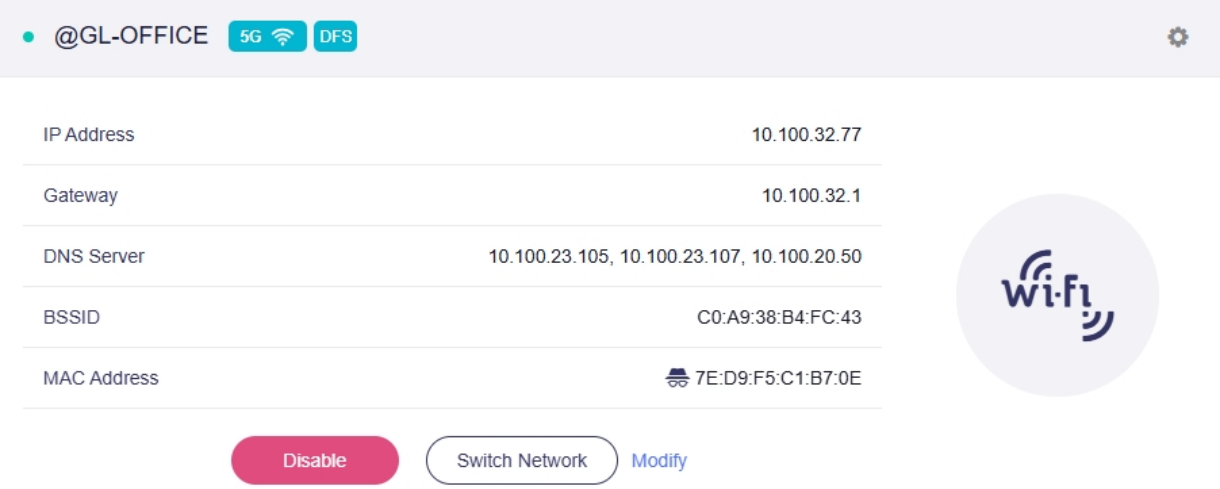


- **Remember**: Aktivieren Sie diese Option, um das aktuell als Repeater genutzte WLAN zu speichern.
- **Lock BSSID**: Wenn diese Option aktiviert ist, verbindet sich der Router ausschließlich mit dem Zugangspunkt (AP) der ausgewählten BSSID, auch wenn andere Zugangspunkte dieselbe SSID verwenden.
- **Manually Set Static IP**: Bei aktivierter Option können Sie für die Repeater-Verbindung des Routers eine feste IPv4-Adresse, Netzmaske, Gateway-Adresse und DNS-Server manuell festlegen, anstatt diese Einstellungen automatisch zu beziehen.
- **TTL**: TTL (Time To Live) legt die maximale Lebensdauer von Datenpaketen im Netzwerk fest. Standardmäßig verringert der Router die TTL eingehender Pakete von Endgeräten vor der Weiterleitung um 1. Um die TTL zu überschreiben bzw. einen anderen Wert vorzutäuschen, geben Sie die gewünschte effektive TTL plus 1 ein, damit die automatische Verringerung ausgeglichen wird. TTL gilt nur für IPv4.

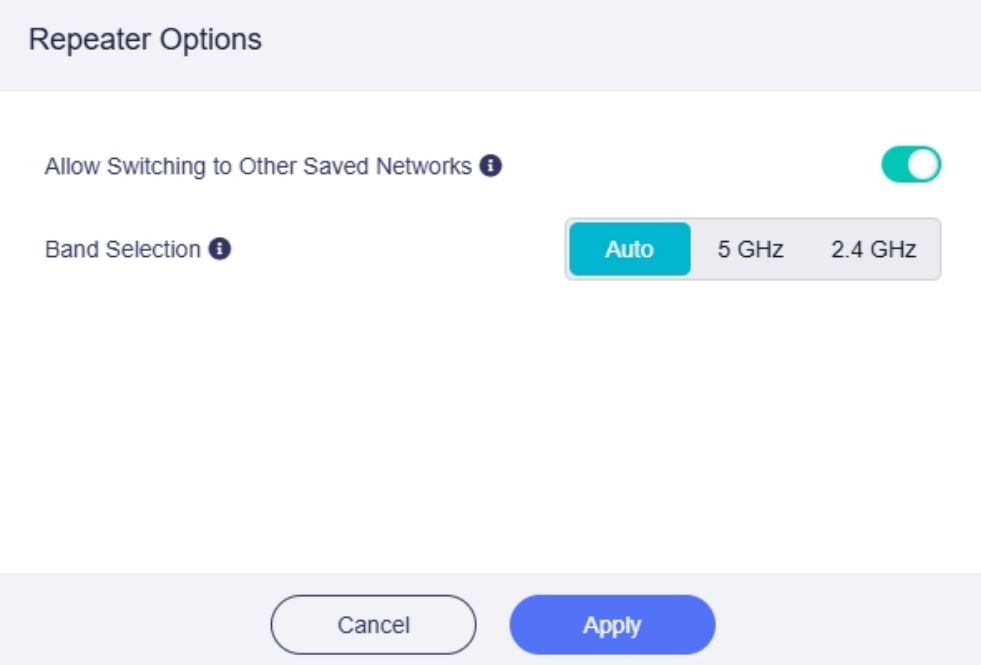
- **HL**: Bei IPv6 begrenzt das Feld HL (Hop Limit) die Anzahl der Übertragungsschritte eines Datenpakets im Netzwerk. Es entspricht der TTL bei IPv4.
- **MTU**: Der Standardwert beträgt 1500.

4.2.2.4 Repeater-Optionen

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



Die Ansicht kann je nach Firmwareversion abweichen.

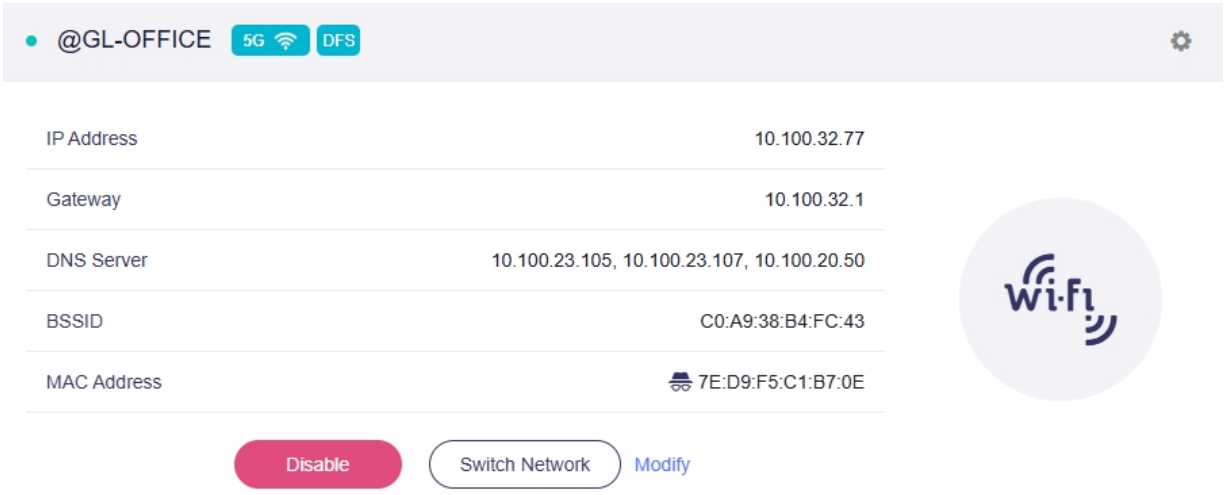


- **Allow Switching to Other Saved Networks**: Wenn diese Option aktiviert ist, verbindet sich der Router automatisch mit einem anderen gespeicherten Netzwerk, sobald das aktuell verbundene WLAN nicht mehr verfügbar ist.

- **Band Selection**: Wenn Sie ein Frequenzband manuell auswählen, sucht der Router ausschließlich nach WLANs in diesem Band und stellt nur zu diesen eine Verbindung her.

4.2.2.5 Bekannte Netzwerke verwalten

Klicken Sie auf **Switch Network**, um bekannte Netzwerke zu verwalten.

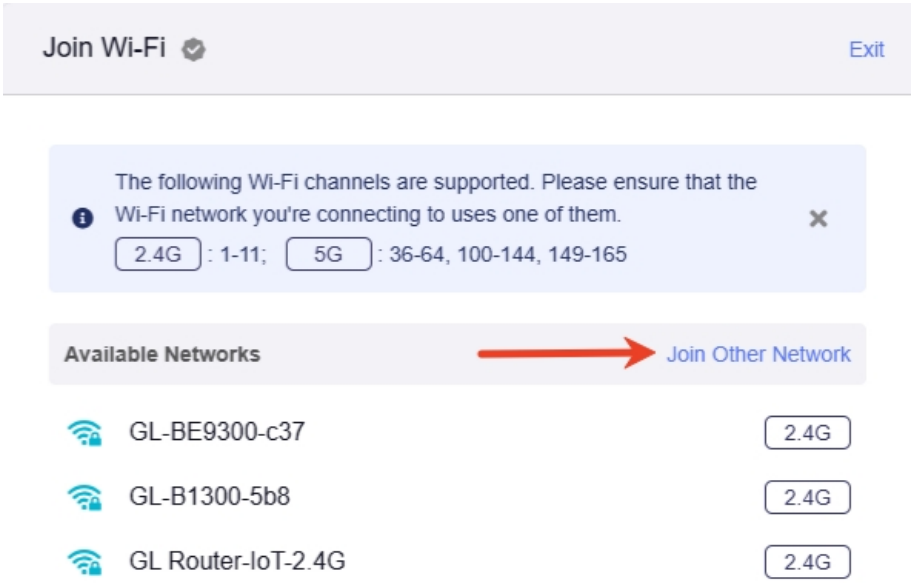


Klicken Sie im Bereich **Known Networks** auf das Papierkorbsymbol, um ein bekanntes Netzwerk zu löschen, oder auf das Zahnradsymbol, um es zu konfigurieren.

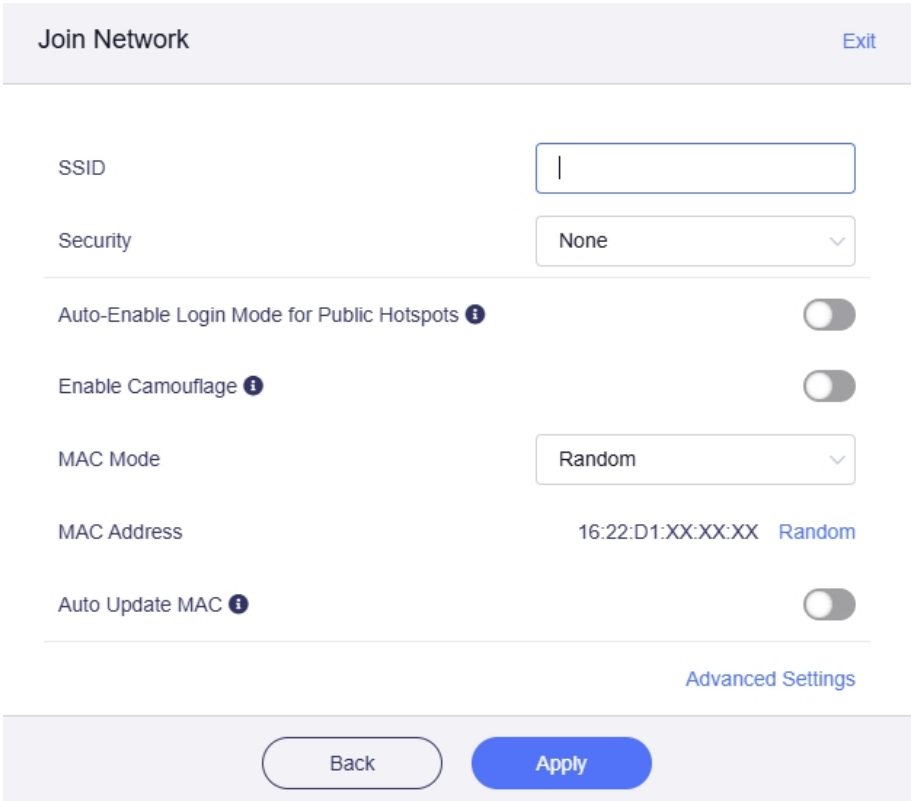


4.2.2.6 Einem anderen Netzwerk beitreten

Wenn die SSID nicht in der Liste der verfügbaren Netzwerke angezeigt wird oder verborgen ist, klicken Sie auf **Join Other Network**.

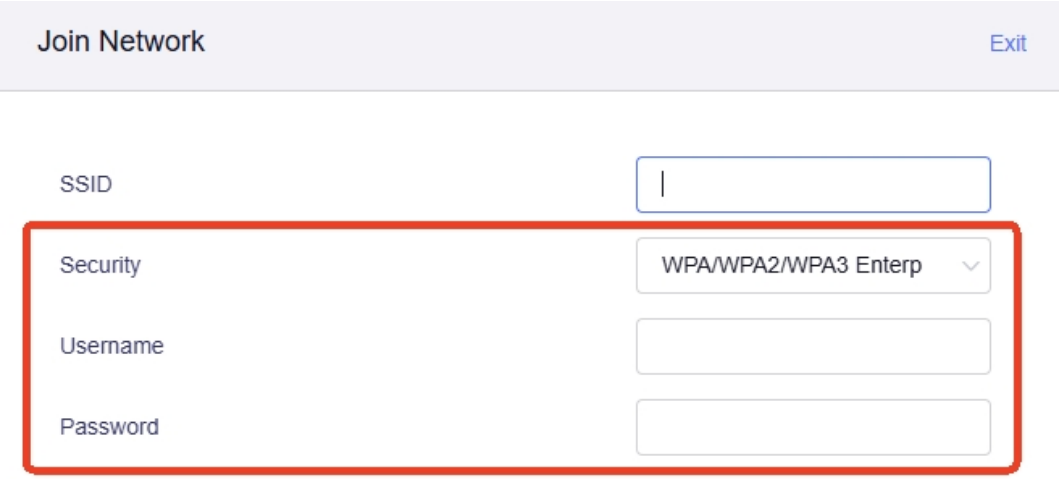


Geben Sie die **SSID** ein, wählen Sie unter **Security** die Sicherheitsmethode und geben Sie bei Bedarf das Passwort ein. Klicken Sie anschließend auf **Apply**.



Unter **Security** stehen je nach Modell zwei oder drei Optionen zur Verfügung.

- None: Es ist kein Passwort erforderlich.
- WPA/WPA2/WPA3: Diese Option ist weit verbreitet und wird von nahezu allen WLANs unterstützt.
- WPA/WPA2/WPA3 Enterprise: Diese Option verwendet das Extensible Authentication Protocol (EAP) zur Authentifizierung. Für die Verbindung sind ein gültiger Benutzername und ein Passwort erforderlich. Sie wird üblicherweise in Unternehmens- oder Hochschulnetzwerken eingesetzt.



Eine ausführliche Anleitung für den Repeater-Betrieb in EAP-Netzwerken finden Sie hier.

4.2.2.7 Erneut verbinden

In den folgenden Fällen versucht der Router in regelmäßigen Abständen automatisch, die WLAN-Verbindung wiederherzustellen. Bei Bedarf können Sie dies manuell deaktivieren. Wenn die SSID oder das Passwort falsch ist, entfernen Sie das Netzwerk aus den bekannten Netzwerken, um das Problem zu beheben.

1. Bei der Repeater-Einrichtung wurde eine falsche SSID oder ein falsches Passwort eingegeben.
2. Der Router wurde nach dem Verbindungsaufbau aus der Reichweite des übergeordneten Routers bewegt.
3. Der übergeordnete Router hat nach dem Verbindungsaufbau die SSID oder das Passwort geändert oder den Zugriff eingeschränkt.

Der erneute Verbindungsaufbau erfolgt in drei Phasen: Wartephase, Suchphase und Verbindungsphase.

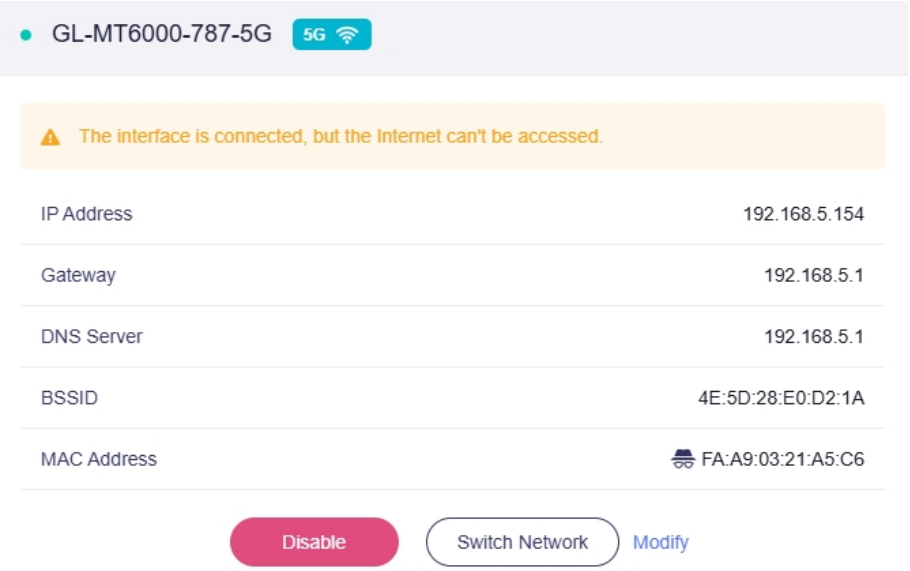
1. Wartephase: Es treten keine Störungen auf. Der Router wartet, bis die Bedingungen für einen erneuten Verbindungsaufbau erfüllt sind.
2. Suchphase: Auf dem gerade durchsuchten Frequenzband können Paketverluste auftreten. Neue Geräte können Schwierigkeiten beim Verbindungsaufbau haben. Bei den Modellen GL-AXT1800/GL-AX1800 wird das Gast-WLAN vorübergehend deaktiviert.
3. Verbindungsphase: Das Haupt-WLAN auf dem Zielband kann beim erneuten Verbindungsaufbau für einige Sekunden unterbrochen werden.

Hinweis: Störungen treten üblicherweise in der Such- und Verbindungsphase auf.

4.2.2.8 Fehlerbehebung

Wenn der Router als Repeater mit einem WLAN verbunden ist, aber kein Internetzugang besteht, wird die folgende gelbe Meldung angezeigt.

„Die Schnittstelle ist verbunden, aber es besteht kein Internetzugang.“



So beheben Sie das Problem:

1. Prüfen Sie, ob das übergeordnete Gerät, also das WLAN, mit dem Ihr Router verbunden ist, Internetzugang hat.
2. Öffnen Sie die Seite Multi-WAN und prüfen Sie den Status der Repeater-Schnittstelle.

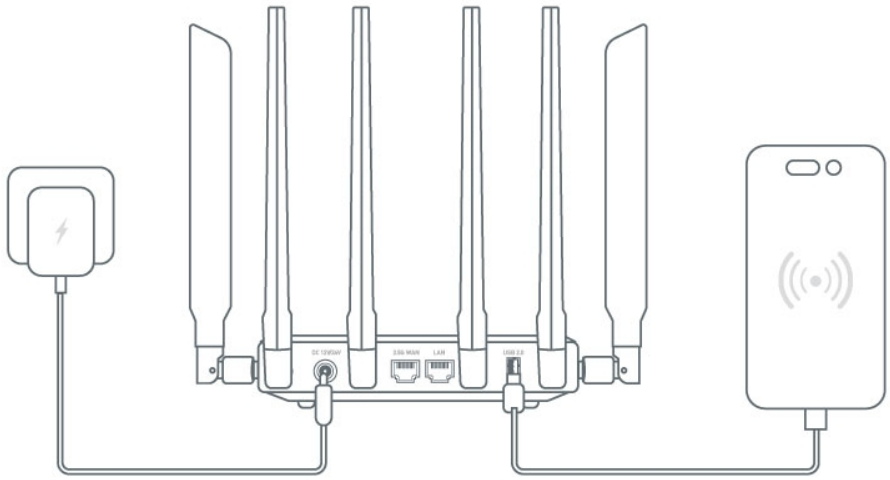
4.2.2.9 DFS

DFS (Dynamic Frequency Selection) ist ein Verfahren, bei dem WLAN-Kanäle automatisch gewechselt werden, um Störungen von Radarsignalen zu vermeiden. Bei einer Verbindung mit einem übergeordneten 5-GHz-WLAN richtet sich die Nutzung von DFS-Kanälen durch den Router nach diesem WLAN.

- Wenn das übergeordnete WLAN einen DFS-Kanal verwendet und bei der Suche erkannt werden kann, verwendet das 5-GHz-WLAN des Routers denselben Kanal.
- Wenn das übergeordnete WLAN bei der Suche nicht erkannt wird oder die Verbindung fehlschlägt, wechselt das 5-GHz-WLAN des Routers auf einen Kanal ohne DFS.

4.2.3 Internetverbindung über USB-Tethering

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

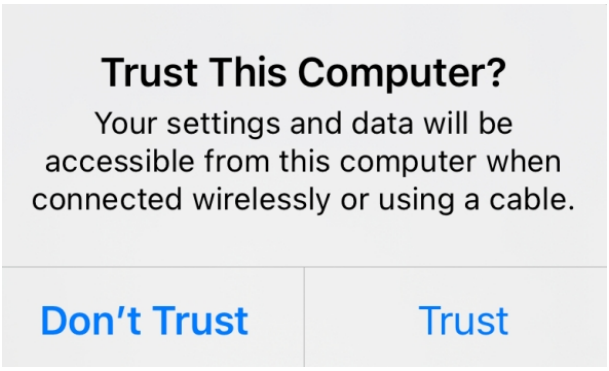


Ein Hostless-Modem kann bei seiner Einrichtung ebenfalls über die Tethering-Funktion betrieben werden.

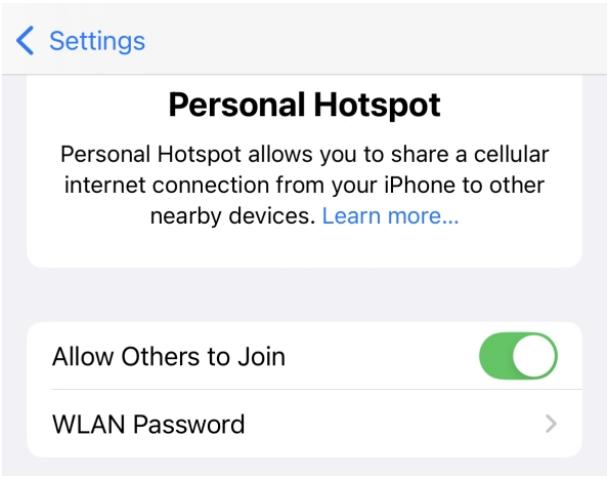
Hinweis: Einige Mobilfunkanbieter beschränken Tethering oder berechnen zusätzliche Gebühren. Erkundigen Sie sich bei Ihrem Anbieter.

4.2.3.1 iPhone

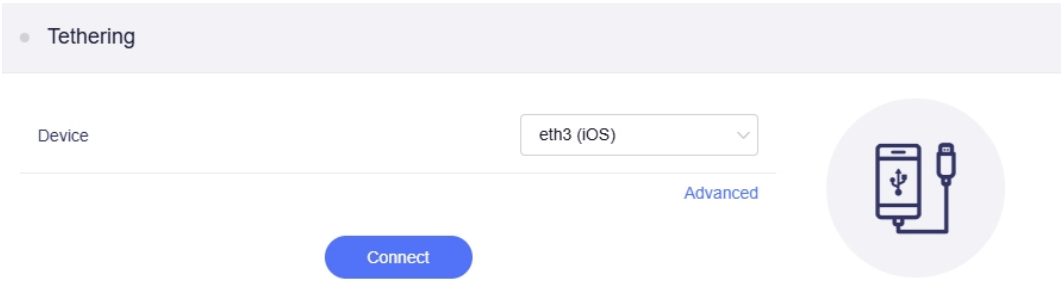
1. Verbinden Sie ein iPhone per USB-Kabel mit dem USB-Anschluss des Routers. Ein Systemdialog fragt, ob Sie diesem Gerät vertrauen. Tippen Sie auf **Vertrauen**, um fortzufahren.



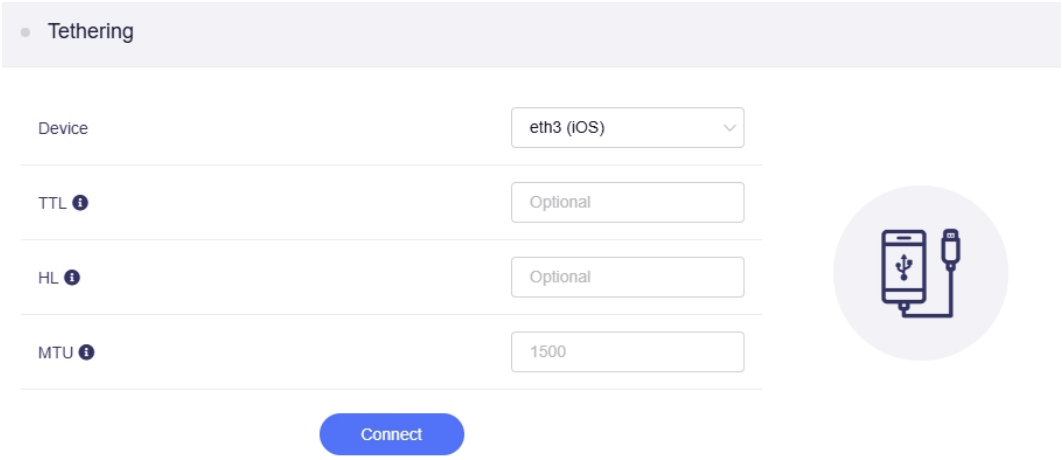
2. Öffnen Sie auf dem iPhone **Einstellungen** > **Persönlicher Hotspot**. Aktivieren Sie **Zugriff für andere erlauben**.



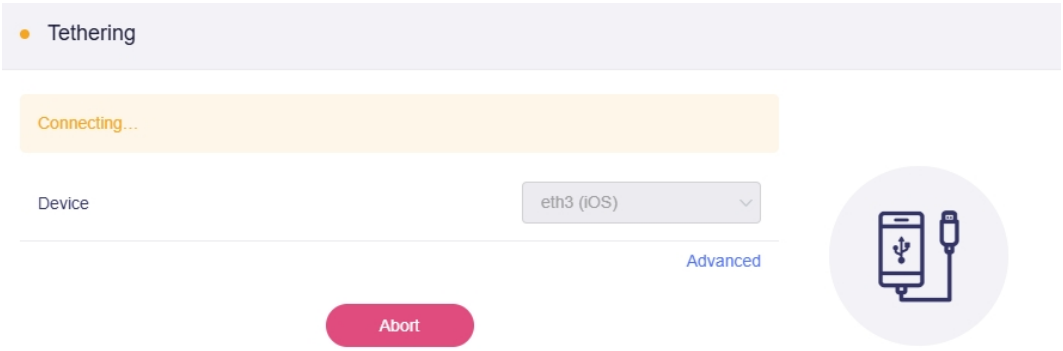
3. Verbinden Sie einen Computer oder ein anderes Smartphone mit dem Router. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Tethering**. Klicken Sie anschließend auf **Connect**.



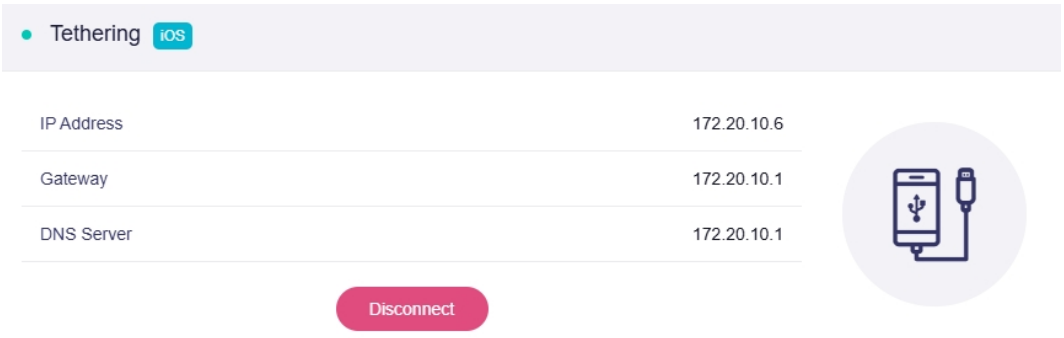
Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU anpassen möchten, klicken Sie auf **Advanced** und nehmen Sie die gewünschten Änderungen vor. Klicken Sie anschließend auf **Connect**.



4. Die Verbindung wird hergestellt.



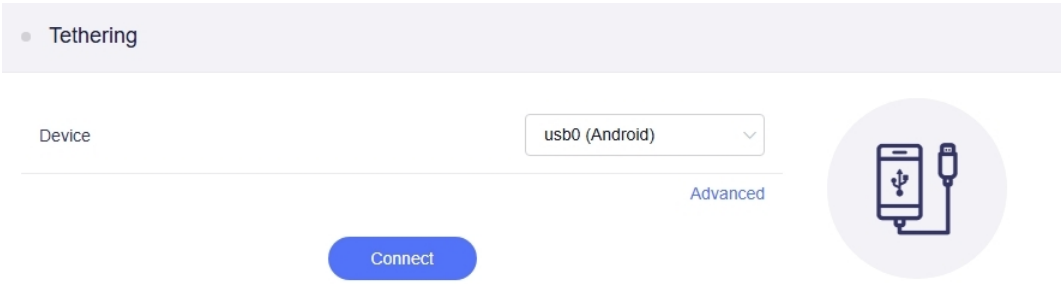
Nach erfolgreicher Verbindung werden auf dieser Seite die Details der Tethering-Verbindung angezeigt.



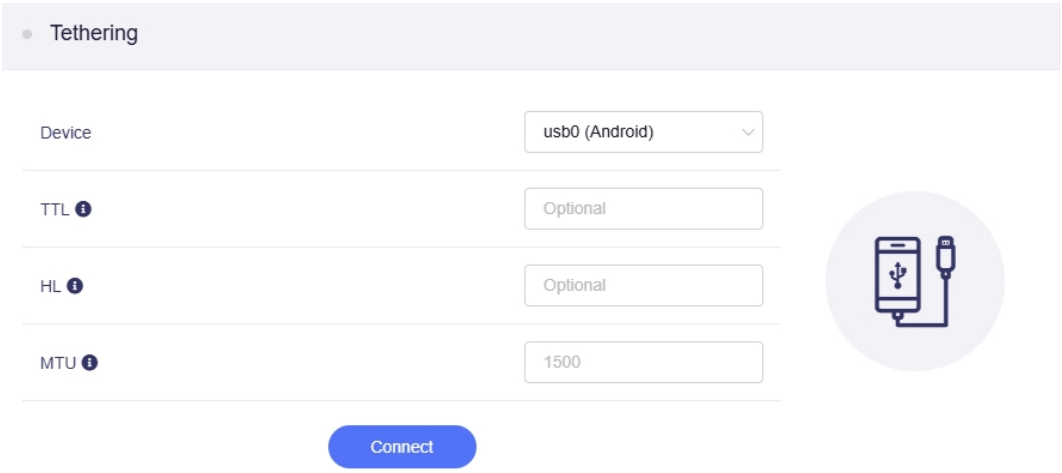
4.2.3.2 Android

1. Verbinden Sie ein Android-Smartphone per USB-Kabel mit dem USB-Anschluss des Routers. Möglicherweise erscheint ein Systemdialog mit USB-Einstellungen. Wählen Sie bei entsprechender Aufforderung **USB-Tethering** oder **Dateiübertragung** aus.

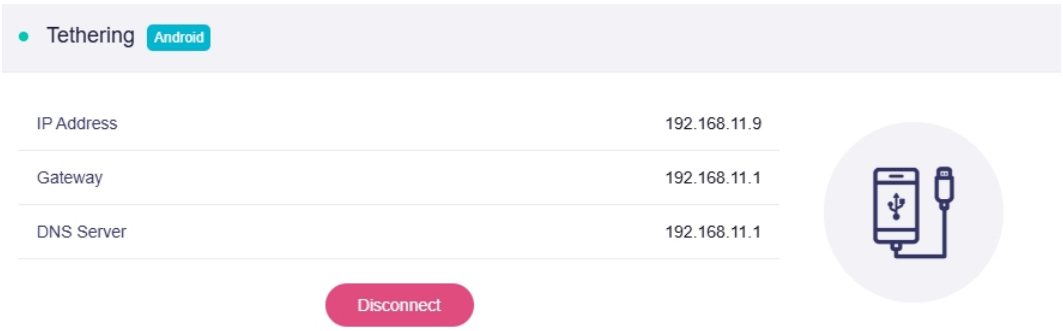
2. Öffnen Sie auf Ihrem Smartphone **Einstellungen** > **Netzwerk & Internet** > **Persönlicher Hotspot**. Aktivieren Sie **Persönlicher Hotspot** oder **USB-Tethering**.
   (Die Schritte zum Aktivieren von USB-Tethering unterscheiden sich je nach Hersteller. Suchen Sie die Funktion in den Einstellungen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



   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**.



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



4.2.3.3 Fehlerbehebung

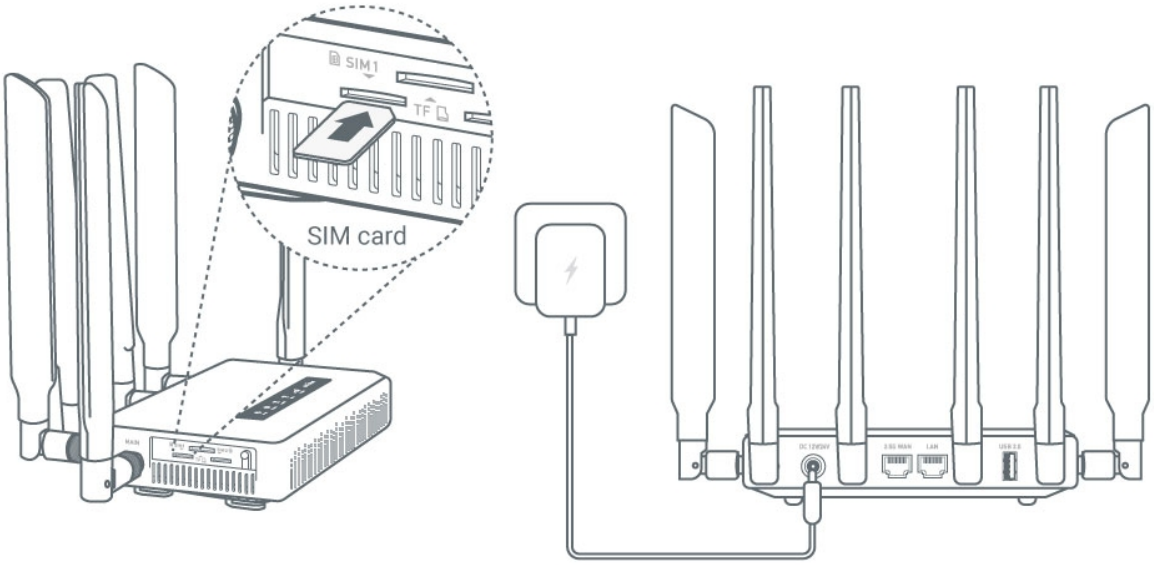
Wenn die Verbindung fehlschlägt, versuchen Sie die folgenden Schritte zur Fehlerbehebung:

- 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.

4.2.4 Internetverbindung über Mobilfunk herstellen

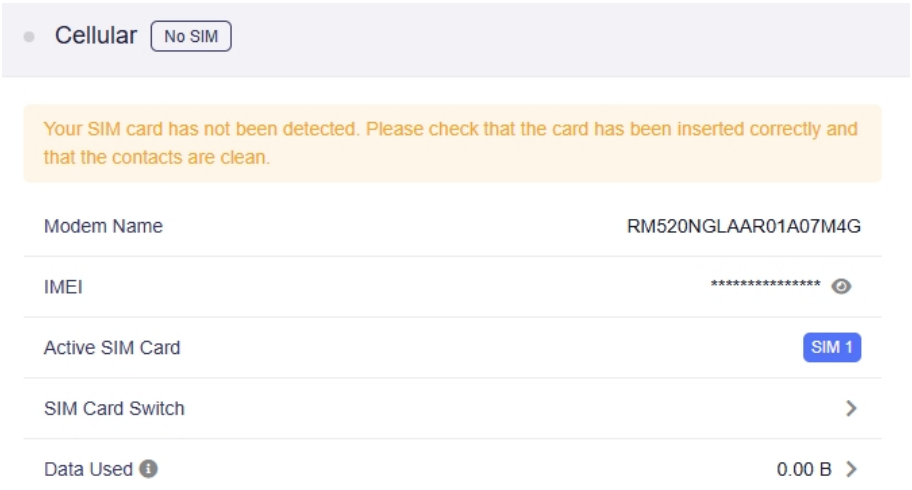
Spitz AX (GL-X3000) verfügt über ein integriertes Mobilfunkmodem mit Dual-SIM. Es ist jeweils nur eine SIM-Karte aktiv; die andere dient als Reserve. Sie können manuell zwischen den beiden SIM-Karten wechseln.



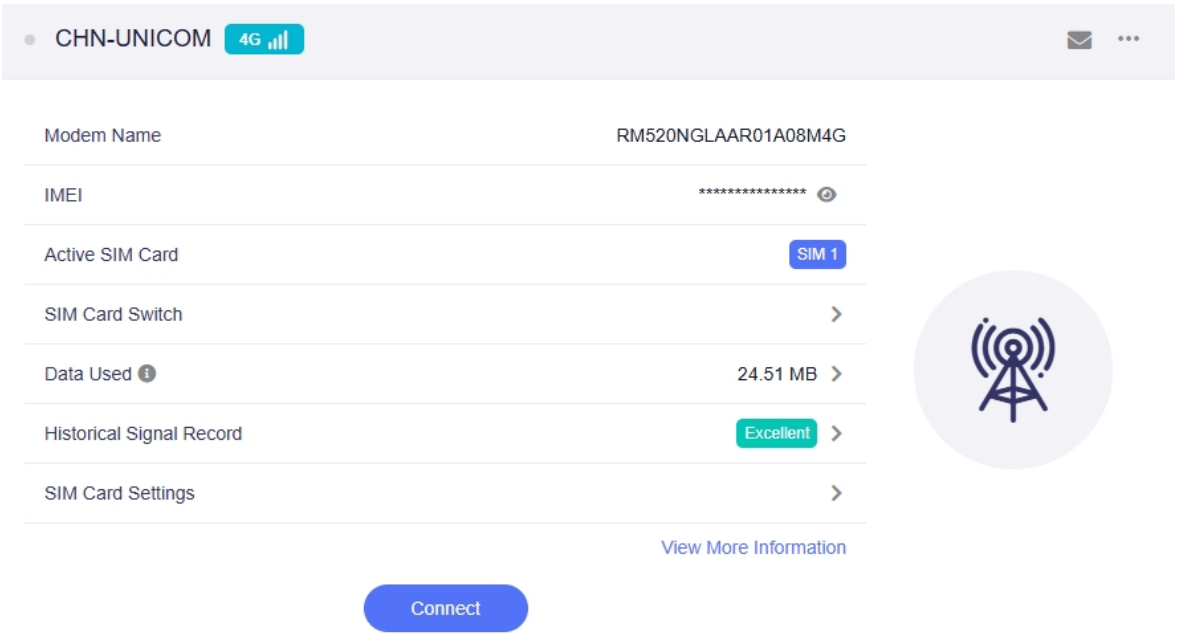
4.2.4.1 Automatische Einrichtung

Wir empfehlen, den Router zunächst auszuschalten, Ihre bereits aktivierten SIM-Karten in die Steckplätze einzusetzen und ihn anschließend wieder einzuschalten. Wenn Sie die SIM-Karte erst nach dem Start des Routers einsetzen, wird die Weboberfläche möglicherweise nicht automatisch aktualisiert. Laden Sie in diesem Fall die Seite neu oder starten Sie den Router neu.

1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Cellular**.
2. Wenn keine SIM-Karte eingesetzt ist, wird die Meldung „Your SIM card has not been detected“ angezeigt.

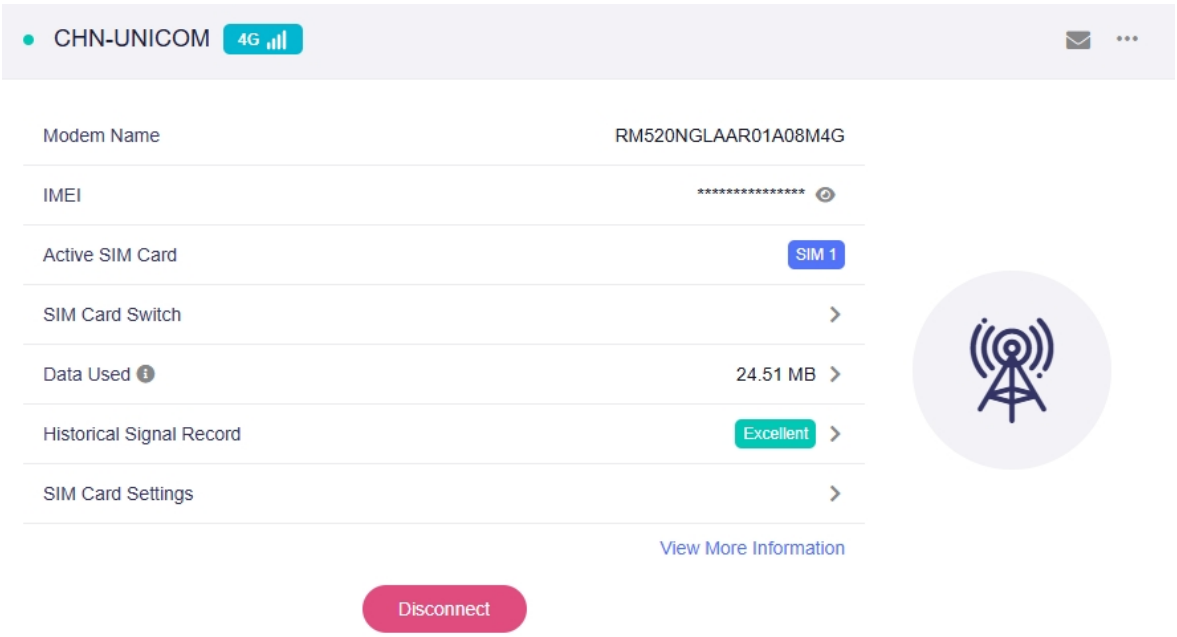


3. Wenn eine SIM-Karte eingesetzt ist, wird die folgende Seite angezeigt. Klicken Sie auf **Connect**.

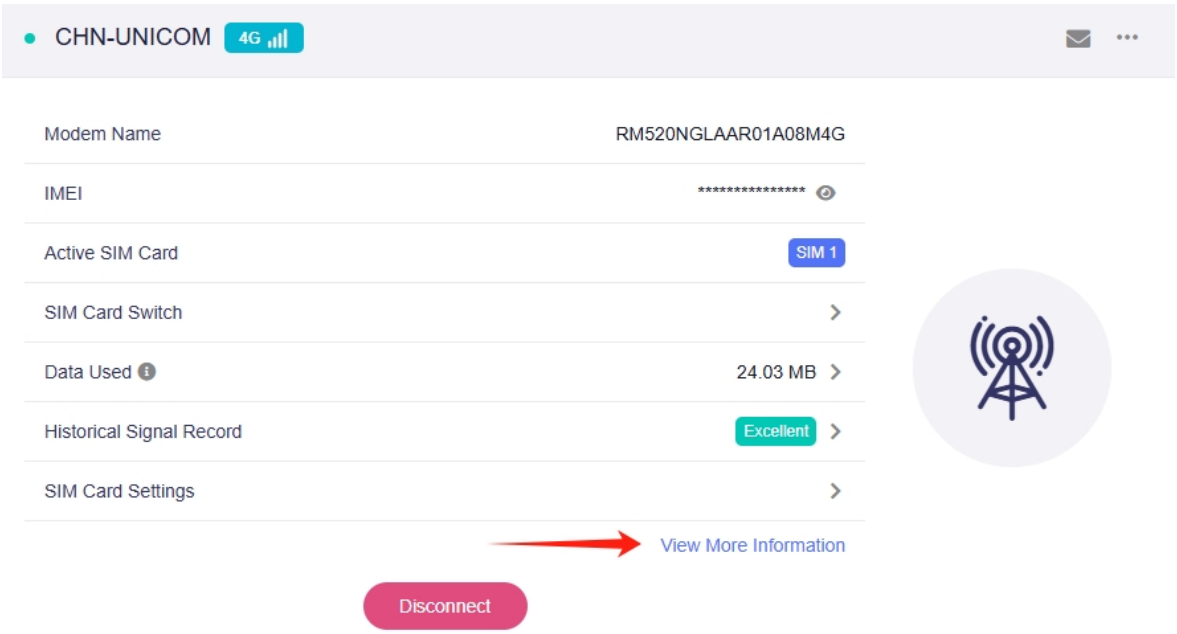


Tipp: Wenn die SIM-Karte nicht erkannt wird, starten Sie den Router neu und prüfen Sie, ob sie anschließend erkannt wird.

4. Sobald die Mobilfunkverbindung hergestellt ist, werden die Netzwerkdetails mit einem grünen Punkt angezeigt. Dieser signalisiert eine erfolgreiche Verbindung.



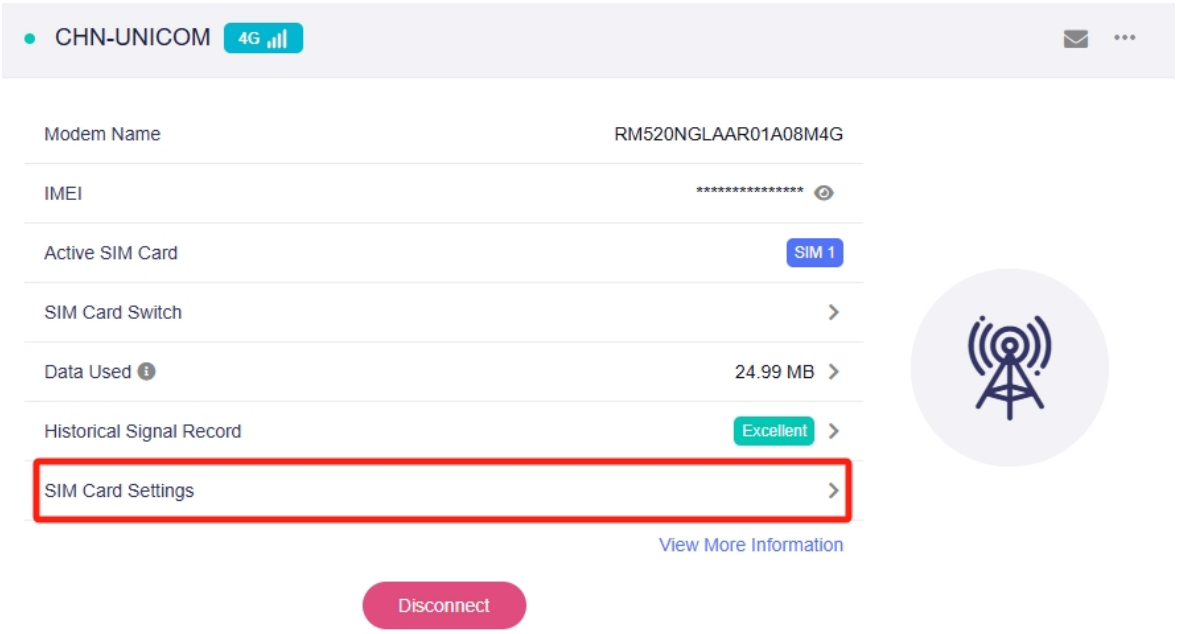
5. Klicken Sie auf **View More Information**, um weitere Mobilfunkinformationen anzuzeigen, darunter Details zum Modem, zur SIM-Karte, zum Internetzugang und zum Mobilfunksignal.



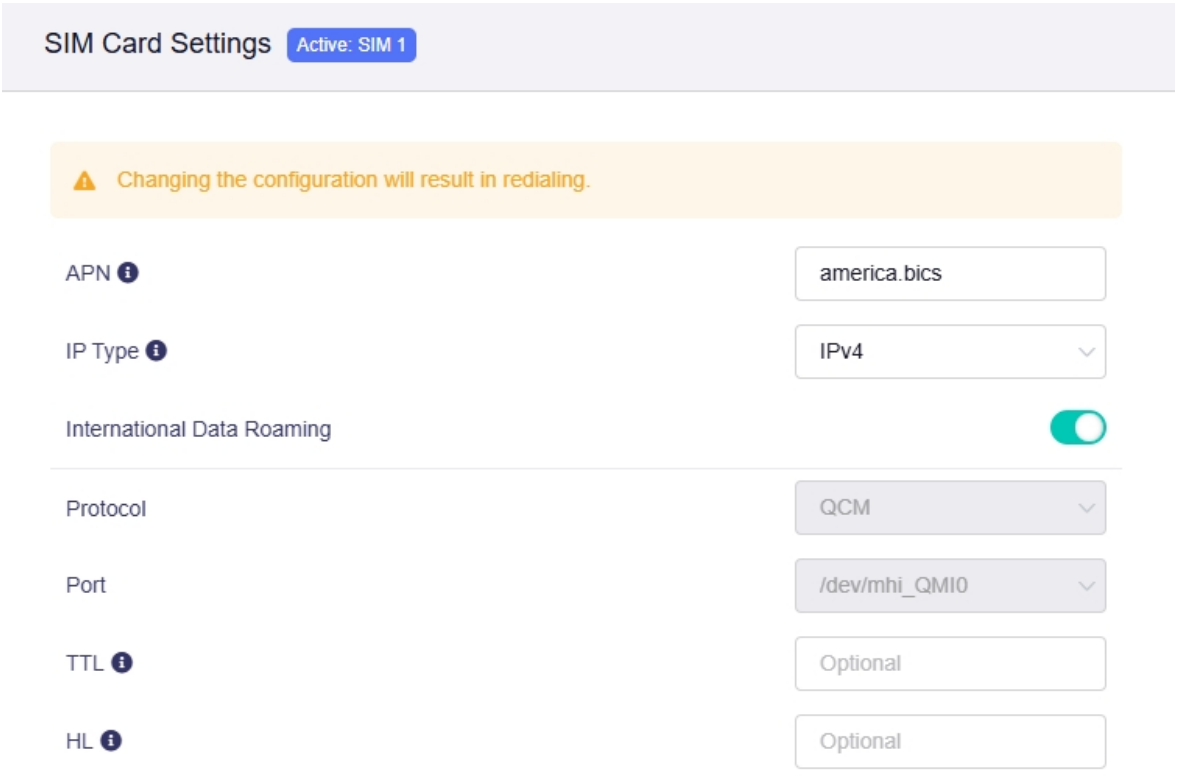
Wenn die automatische Einrichtung fehlschlägt, versuchen Sie **Manual Setup**.

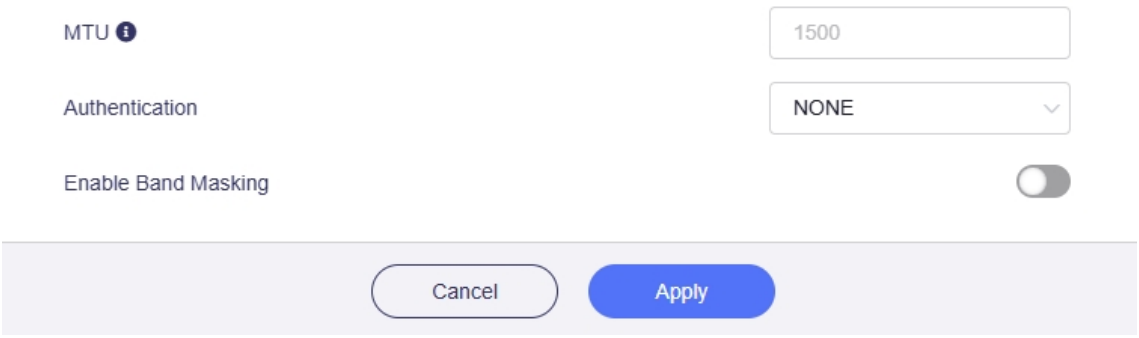
4.2.4.2 Manuelle Einrichtung

1. Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular** und klicken Sie auf **SIM Card Settings**.



2. Sie können die Mobilfunkeinstellungen der aktuellen SIM-Karte anzeigen oder ändern. Beim Übernehmen der Änderungen wird die Verbindung neu aufgebaut.

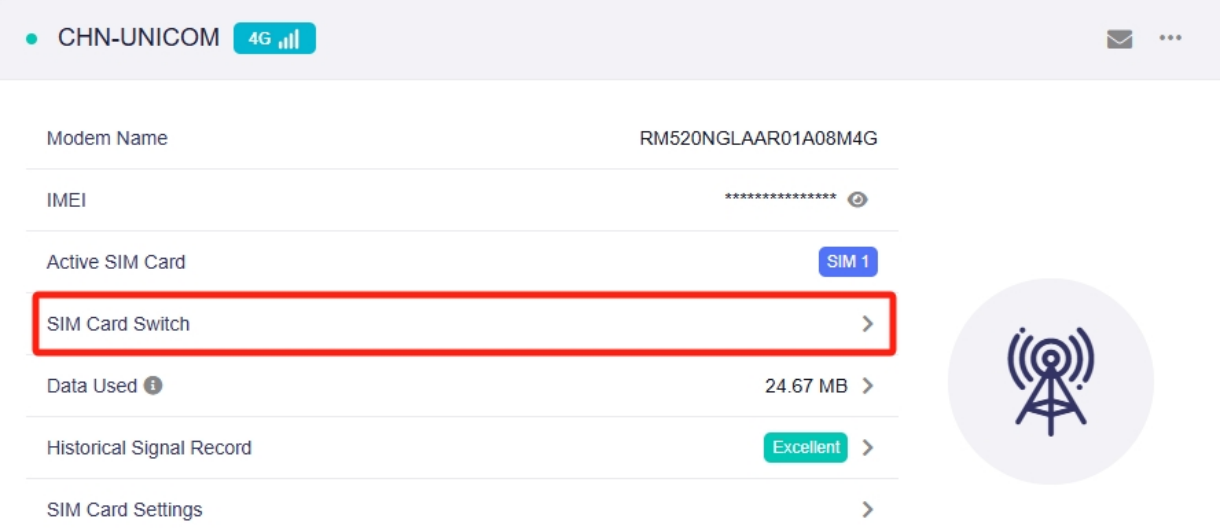




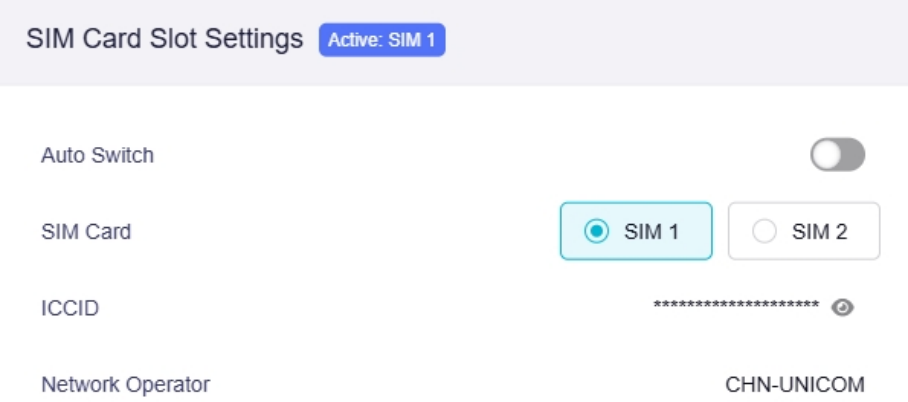
- **APN**: Der APN (Access Point Name) ist ein Gateway-Parameter, der für eine Mobilfunkverbindung erforderlich ist. Er ermöglicht dem Router den Zugang zum Internet Ihres Mobilfunkanbieters. Sie können den voreingestellten APN verwenden oder einen von Ihrem Anbieter bereitgestellten APN festlegen.
- **Protocol**: Das anhand von Modem und Mobilfunkanbieter automatisch erkannte Kommunikationsprotokoll, etwa QMI oder QCM.
- **Port**: Der automatisch erkannte serielle Anschluss für die Kommunikation mit dem Mobilfunkmodem.
- **TTL**: TTL (Time To Live) legt fest, wie lange Datenpakete maximal im Netzwerk verbleiben dürfen. Diese Einstellung gilt nur für IPv4. Standardmäßig verringert der Router den TTL-Wert eingehender Pakete von Endgeräten vor der Weiterleitung um 1. Zum Überschreiben geben Sie den gewünschten wirksamen TTL-Wert plus 1 ein, um die automatische Verringerung auszugleichen.
- **HL**: Bei IPv6 begrenzt HL (Hop Limit) die Anzahl der Weiterleitungsschritte für Datenpakete im Netzwerk und entspricht damit der TTL bei IPv4.
- **MTU**: Der Standardwert der MTU beträgt 1500 Byte.
- **Authentication**: Wählen Sie das von Ihrem Mobilfunkanbieter benötigte Authentifizierungsverfahren, beispielsweise NONE, PAP oder CHAP. Sind keine Zugangsdaten erforderlich, ist normalerweise NONE eingestellt.
- **Band Masking**: Aktivieren Sie diese Funktion, wenn der Router bestimmte Mobilfunkbänder sperren oder ausschließlich ausgewählte Bänder verwenden soll. Einzelheiten finden Sie unter 4.2.4.6 Frequenzbänder filtern.

4.2.4.3 Einstellungen der SIM-Kartensteckplätze

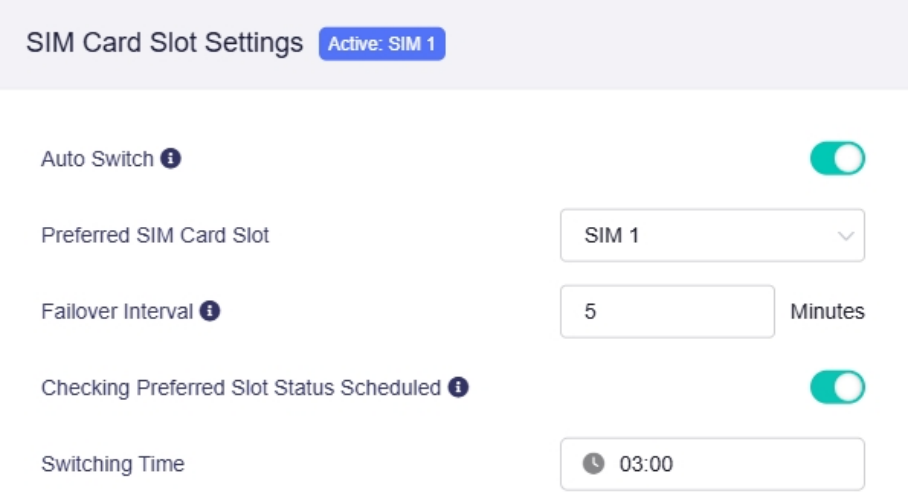
Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular** und klicken Sie auf **SIM Card Switch**.



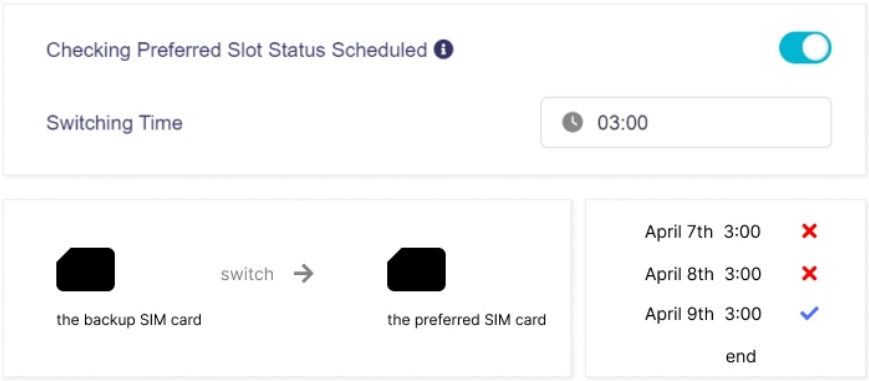
Hier werden der Schalter für den automatischen Wechsel, die aktive SIM-Karte, die ICCID und der Netzbetreiber angezeigt.



Wenn zwei SIM-Karten eingesetzt sind, können Sie **Auto Switch** aktivieren.



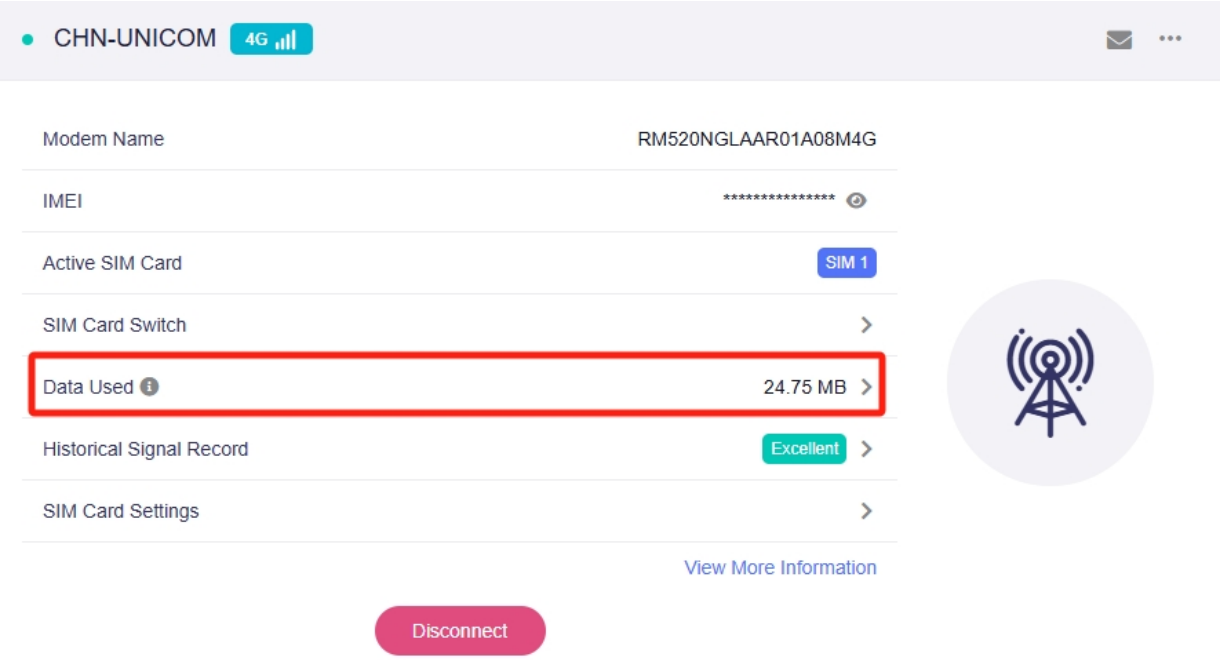
- **Auto Switch**: Aktiviert den automatischen Wechsel zwischen SIM 1 und SIM 2. Für den automatischen SIM-Wechsel wird dieselbe Methode zur Netzwerkprüfung verwendet, die auf der Seite Multi-WAN konfiguriert ist.
- **Preferred SIM Card Slot**: Wählen Sie SIM 1 oder SIM 2 als bevorzugte SIM-Karte aus.
- **Failover Interval**: Es können Werte zwischen 5 Minuten und 24 Stunden eingestellt werden. Wenn nach einem Wechsel weiterhin kein Internetzugang besteht, wechselt das Gerät zum bevorzugten SIM-Steckplatz zurück und wartet das festgelegte Intervall ab, bevor es einen erneuten Wechsel versucht.
  Diese Option greift, wenn weder die bevorzugte SIM-Karte noch die Reserve-SIM-Karte ein Signal empfängt. Das Gerät wechselt zwischen den SIM-Karten, bis eine davon ein nutzbares Signal empfängt.
- **Checking Preferred Slot Status Scheduled**
  Wenn diese Option aktiviert ist, prüft das Gerät den bevorzugten SIM-Steckplatz täglich zur festgelegten Uhrzeit und versucht zurückzuwechseln, sobald die bevorzugte SIM-Karte wieder Internetzugang hat.
  Dadurch wird verhindert, dass die Reserve-SIM-Karte übermäßig viel Datenvolumen verbraucht. Wenn die bevorzugte SIM-Karte weiterhin kein Signal empfängt, verwendet das Gerät die Reserve-SIM-Karte weiter.



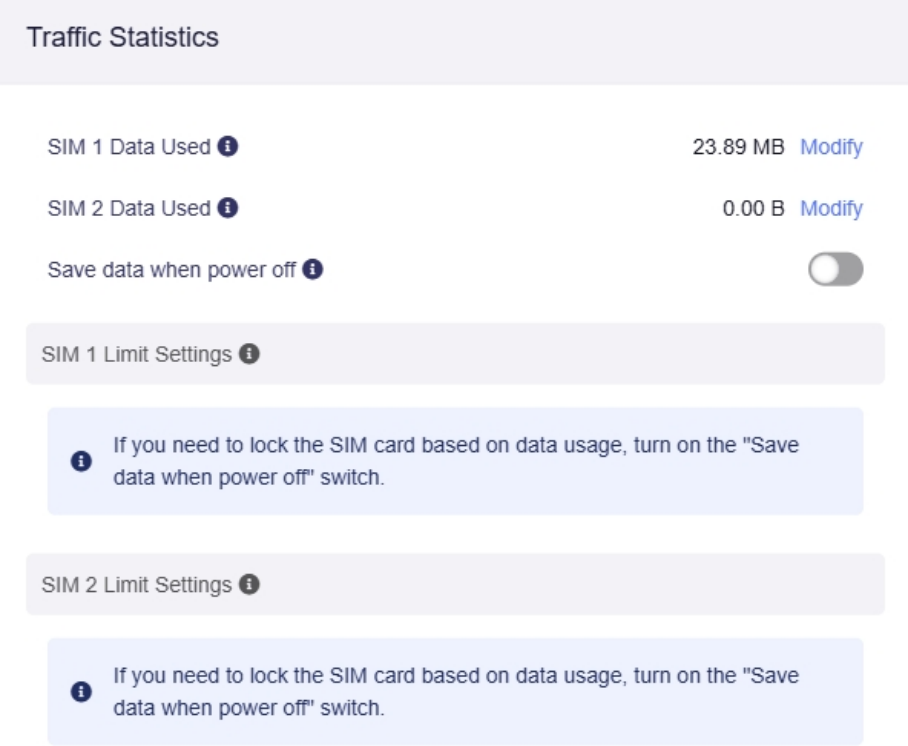
Hinweis: Die Funktion Auto Switch wechselt nicht sofort zur anderen SIM-Karte. Zunächst benötigt das Gerät Zeit, um festzustellen, dass die aktuelle SIM-Karte keinen Internetzugang ermöglicht. Außerdem befindet sich die andere SIM-Karte nicht im Bereitschaftsmodus und muss erst aktiviert werden.

4.2.4.4 Datenverbrauchsstatistik

Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular** und klicken Sie auf **Data Used**.



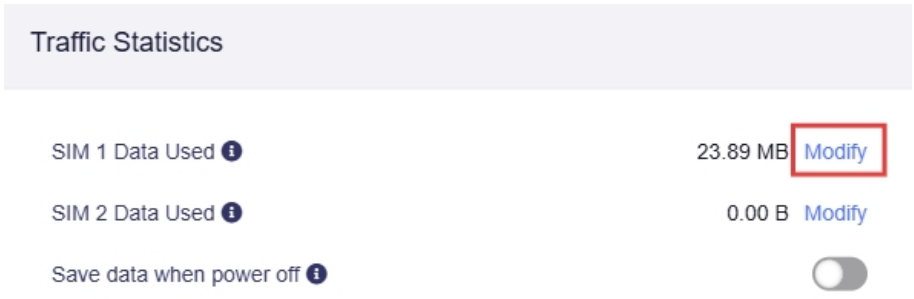
Die Seite **Traffic Statistics** wird geöffnet. Sie zeigt den Datenverbrauch der SIM-Karten an und bietet Einstellungen für Datenlimits.



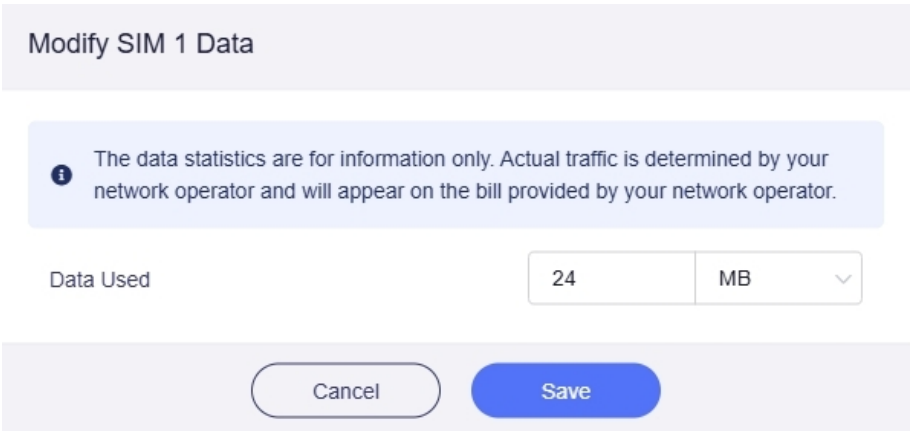
Wenn der unter Data Used angezeigte Verbrauch den Wert unter Data Cap Amount überschreitet, ändern Sie **Data Cap Amount** oder **Data Used** manuell. Andernfalls kann die Netzwerkverbindung getrennt werden oder bei Dual-SIM-Modellen ein automatischer SIM-Wechsel erfolgen.

- **Datenverbrauch ändern**

  Klicken Sie rechts neben SIM 1/2 Data Used auf **Modify**.



  Anschließend können Sie den Datenverbrauch ändern oder zurücksetzen.

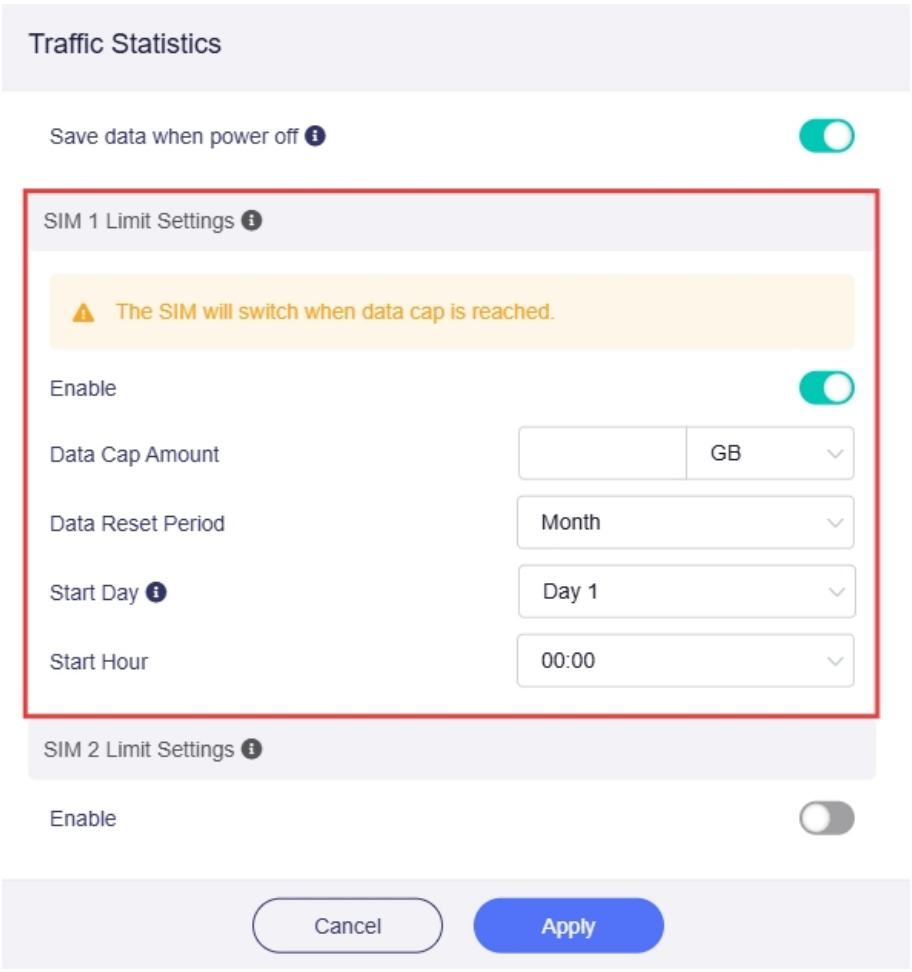


- **Datenlimit für die SIM-Karte festlegen**

  Wenn Sie ein Datenlimit für die SIM-Karte festlegen möchten, aktivieren Sie zunächst **Save data when power off**. Dadurch werden die Daten auch beim Ausschalten des Geräts gespeichert.



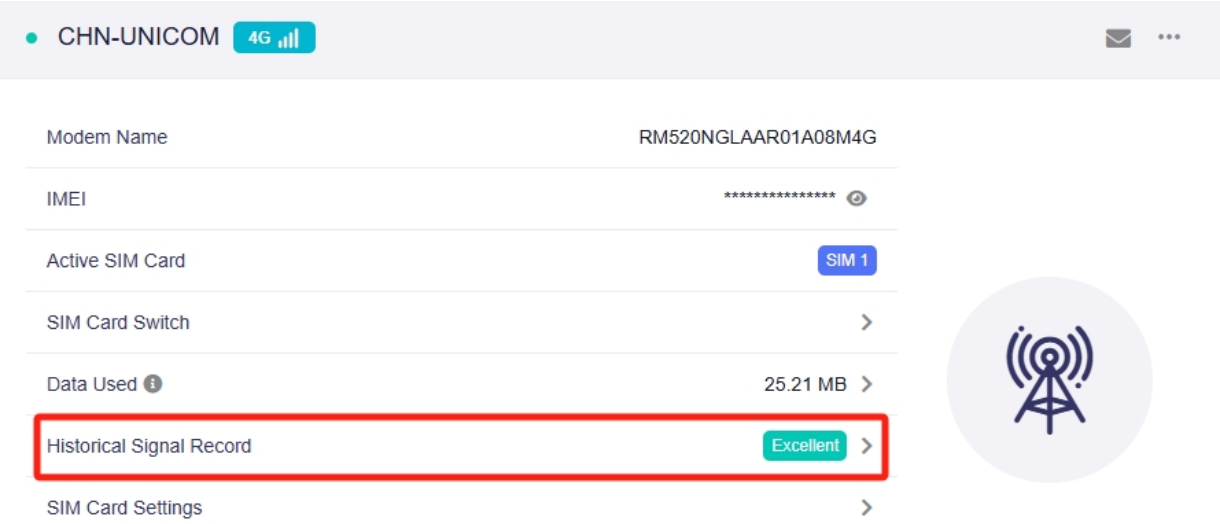
  Aktivieren Sie anschließend die Limit-Einstellungen für SIM 1 oder SIM 2.



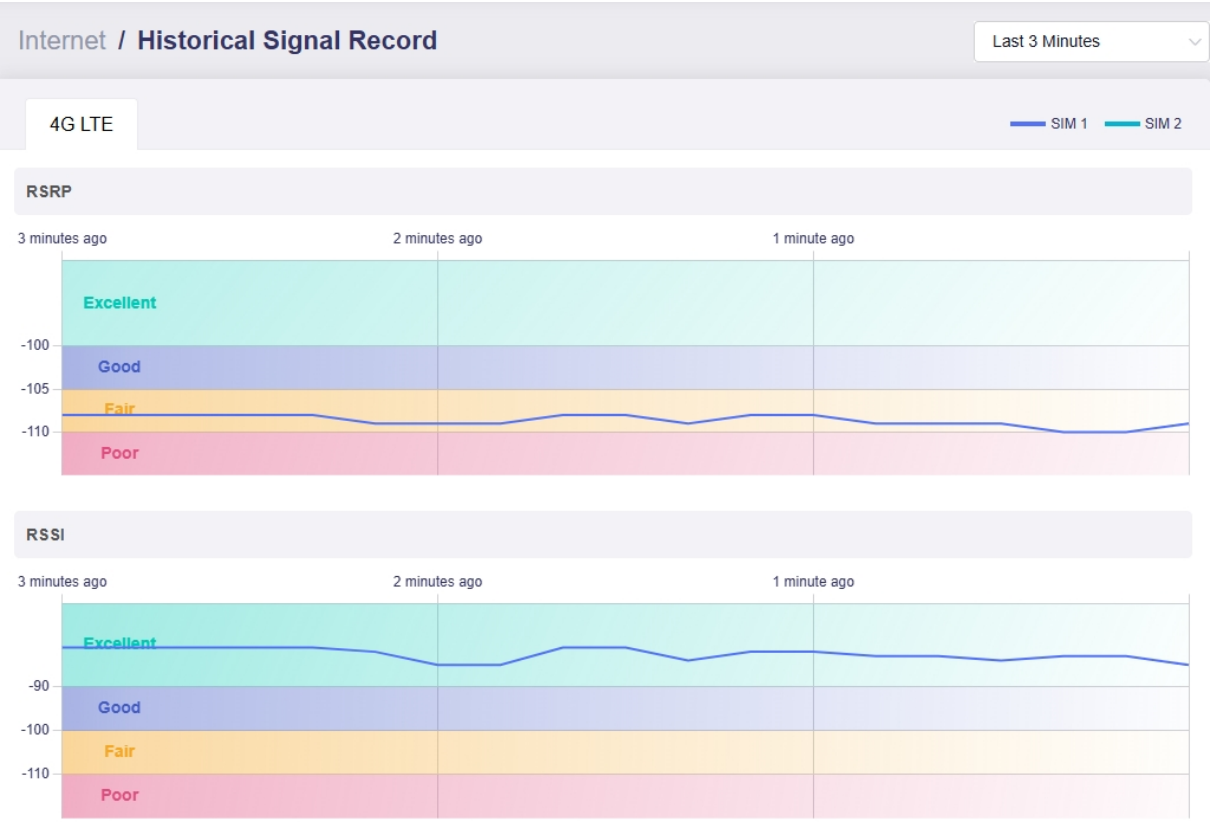
Bei Dual-SIM-Modellen empfehlen wir, gleichzeitig **SIM Card Slot Auto Switch** zu aktivieren. Wenn für SIM 1 ein Datenlimit festgelegt und der automatische SIM-Wechsel aktiviert ist, wechselt das Gerät bei Überschreiten des Limits automatisch von SIM 1 zu SIM 2 und deaktiviert SIM 1.

4.2.4.5 Verlauf der Signalstärke

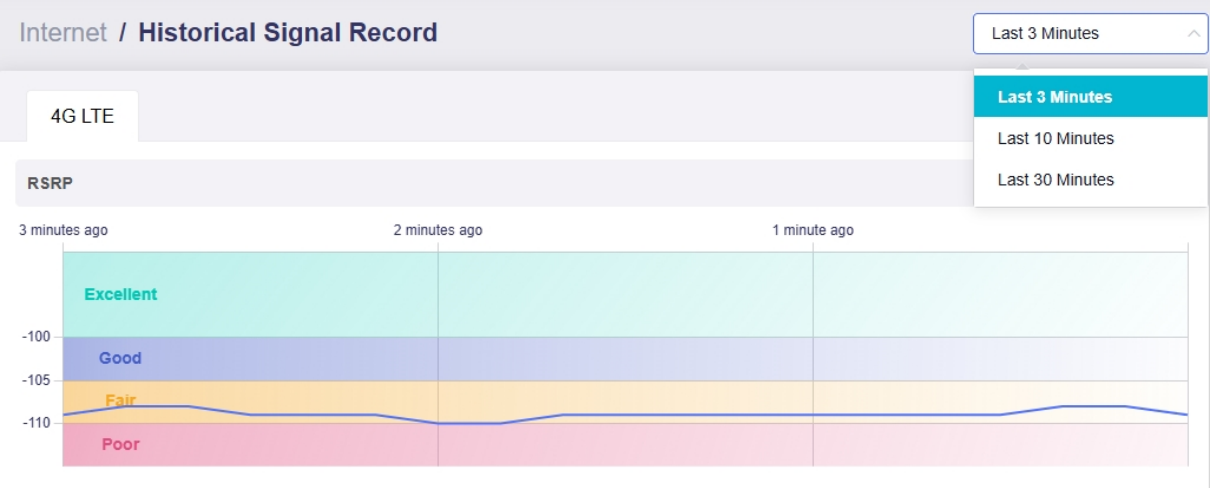
Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular** und klicken Sie auf **Historical Signal Record**.



Hier können Sie die Qualität Ihrer Mobilfunkverbindung prüfen. Versuchen Sie bei schwachem Signal, für einen besseren Empfang zu einem anderen Mobilfunkmast zu wechseln.

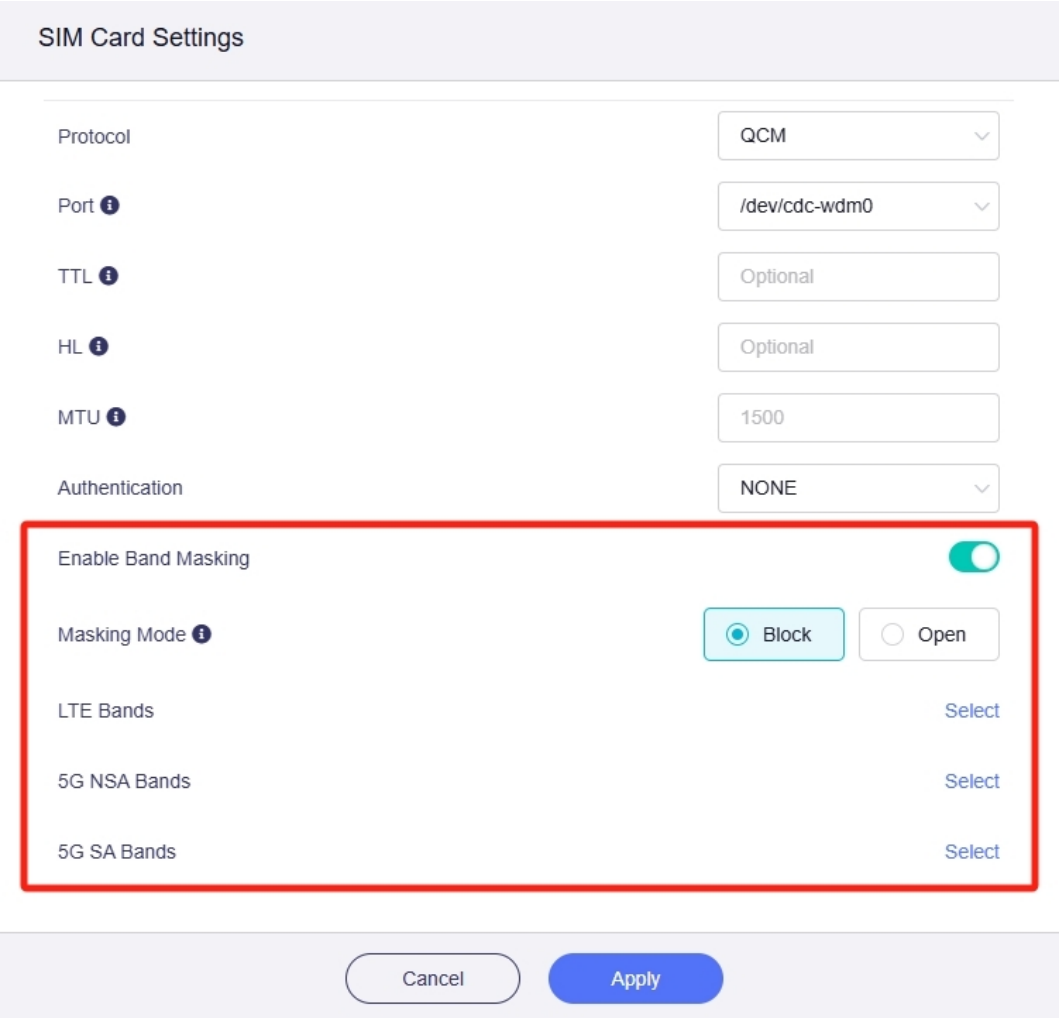


Wählen Sie oben rechts unterschiedliche Zeiträume aus, um den Verlauf der Signalstärke anzuzeigen.



4.2.4.6 Frequenzbänder filtern

Mit Band Masking können Sie bestimmte Mobilfunkbänder sperren oder ausschließlich bevorzugte Bänder verwenden, um einen schwachen Mobilfunkempfang zu verbessern. Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular** > **SIM Card Settings** und aktivieren Sie **Enable Band Masking**.



Wählen Sie den **Masking Mode** (Block oder Open) und anschließend die LTE-, 5G-NSA- und 5G-SA-Bänder aus.

4.2.4.7 SMS und SMS-Weiterleitung

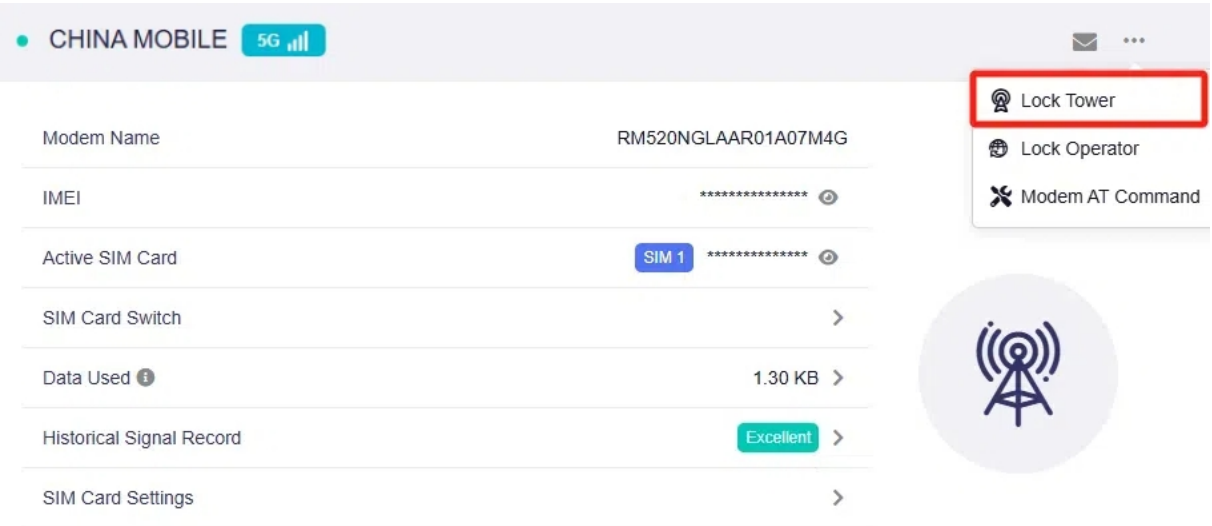
Siehe SMS und SMS-Weiterleitung.

4.2.4.8 Mobilfunkmast festlegen

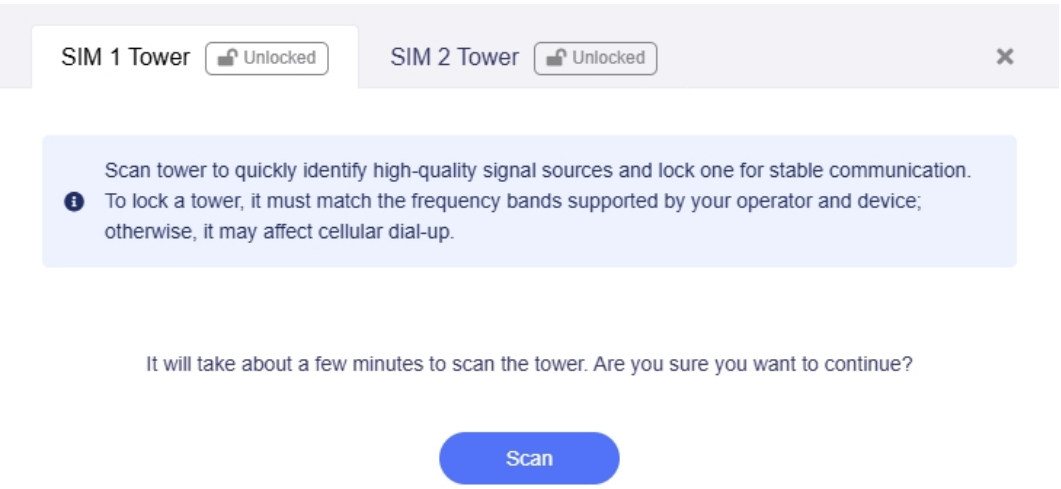
Für eine hohe Signalqualität und eine stabile Mobilfunkverbindung können Sie versuchen, die Verbindung auf einen bestimmten Mobilfunkmast festzulegen.

Hinweis: Der festgelegte Mobilfunkmast muss die von Ihrem Anbieter und Ihrem Gerät unterstützten Frequenzbänder nutzen. Andernfalls kann die Verbindung fehlschlagen.

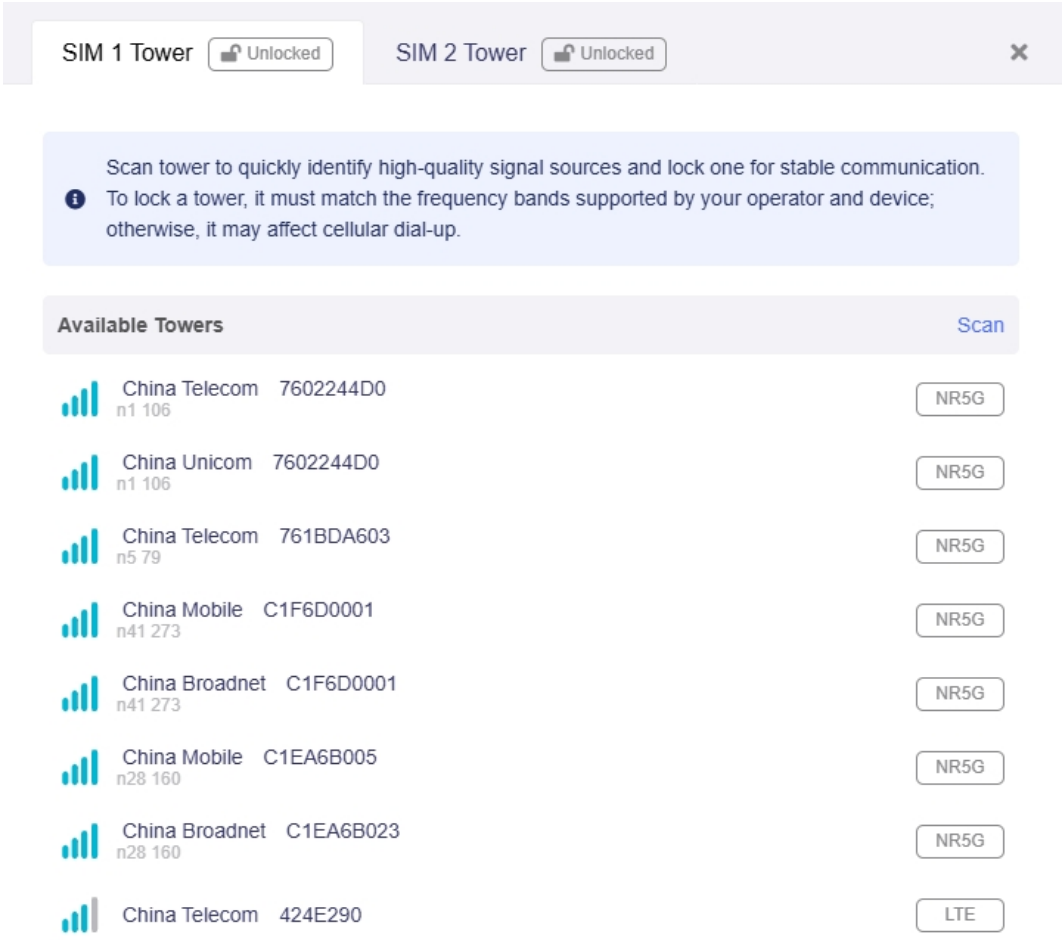
Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular**. Klicken Sie oben rechts auf das Symbol mit den drei Punkten und wählen Sie **Lock Tower**.



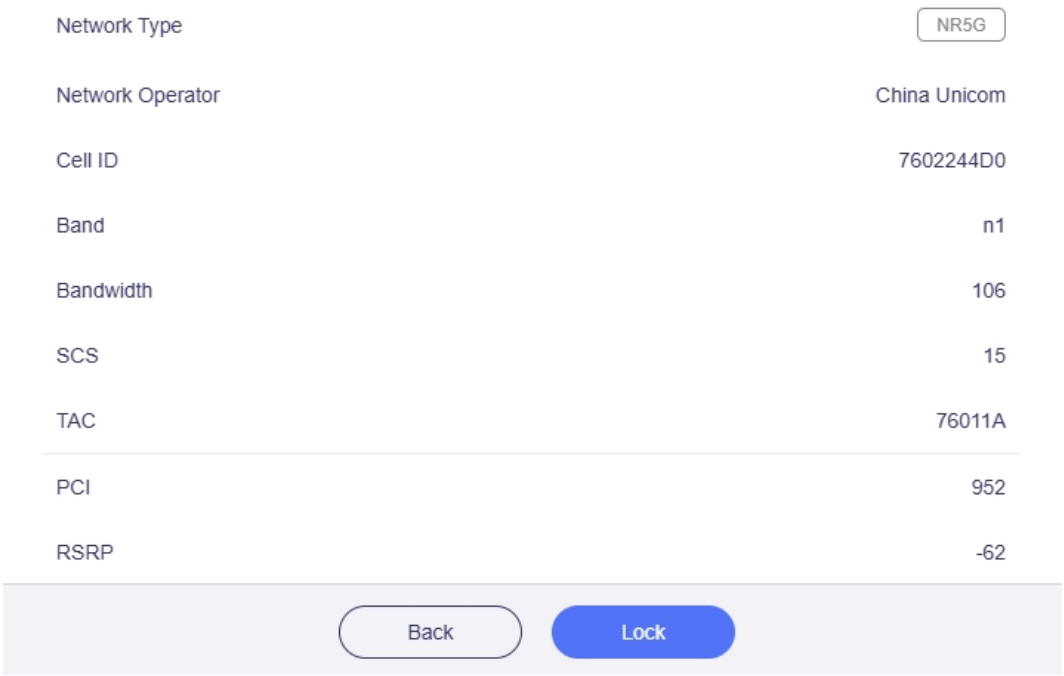
Klicken Sie auf **Scan**, um nach Mobilfunkmasten zu suchen. Dies dauert einige Minuten. Laden Sie die Seite während der Suche nicht neu.



Die verfügbaren Mobilfunkmasten werden angezeigt.



Klicken Sie auf einen Mobilfunkmast, um Details anzuzeigen und ihn festzulegen.



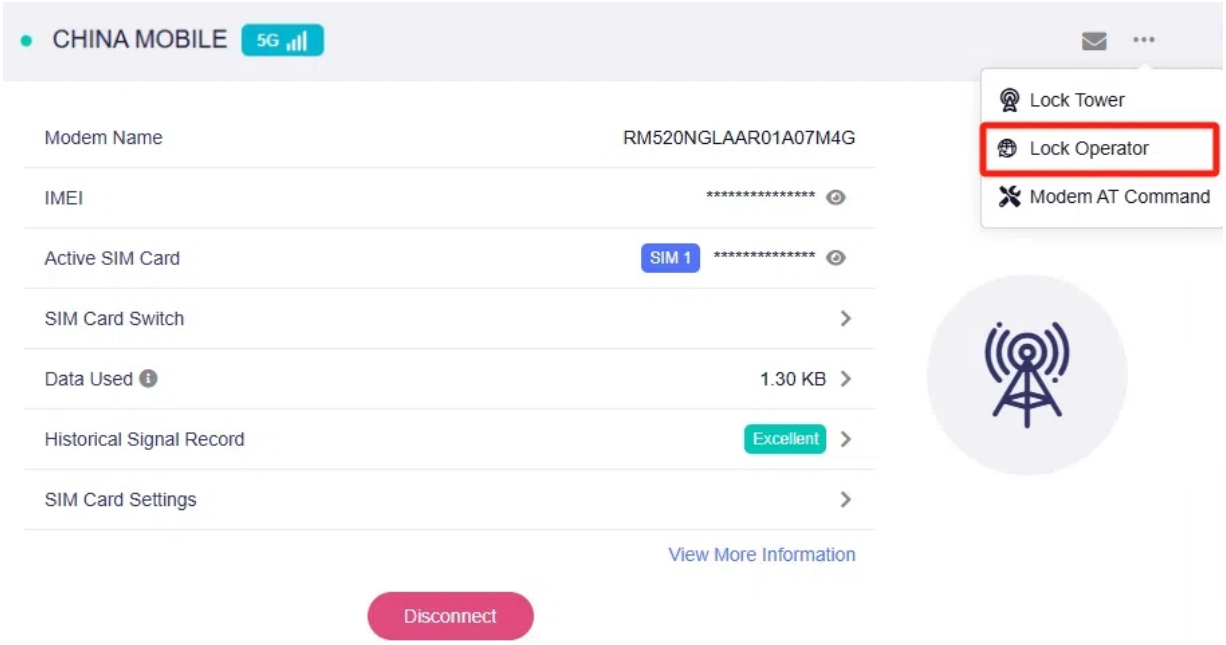
Hinweis:

1. Wenn die Mobilfunkschnittstelle aktiviert ist, kann das Gerät möglicherweise nicht alle Mobilfunkmasten finden.
2. Wenn der festgelegte Mobilfunkmast nicht mit dem Bandfilter oder den APN-Parametern Ihrer Mobilfunkeinstellungen übereinstimmt, kann der Router keine Mobilfunkverbindung herstellen.
3. Wenn Sie den Router nach dem Festlegen eines Mobilfunkmasts an einen anderen Standort bringen, versucht er auch nach einem Neustart weiterhin, sich mit diesem Mast zu verbinden. Dadurch kann die automatische Mobilfunkverbindung am neuen Standort verhindert werden. Heben Sie in diesem Fall die Festlegung auf oder legen Sie manuell einen anderen Mobilfunkmast fest.

4.2.4.9 Netzbetreiber festlegen

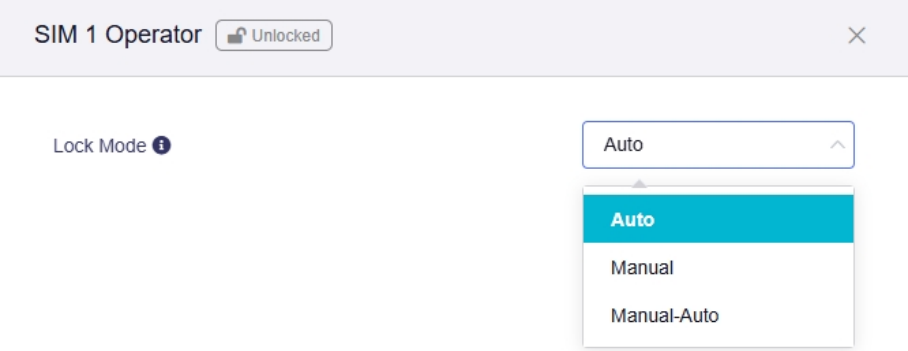
Wenn Sie einen bestimmten Mobilfunkanbieter festlegen, verwendet der Router ausschließlich dessen Netzwerk. Dies ermöglicht eine stabile Verbindung und vermeidet unbeabsichtigte Roaminggebühren, insbesondere in Grenzgebieten, in denen sich das Gerät sonst mit ausländischen Netzen verbinden könnte.

Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular**. Klicken Sie oben rechts auf das Symbol mit den drei Punkten und wählen Sie **Lock Operator**.



Es stehen drei Modi zur Verfügung:

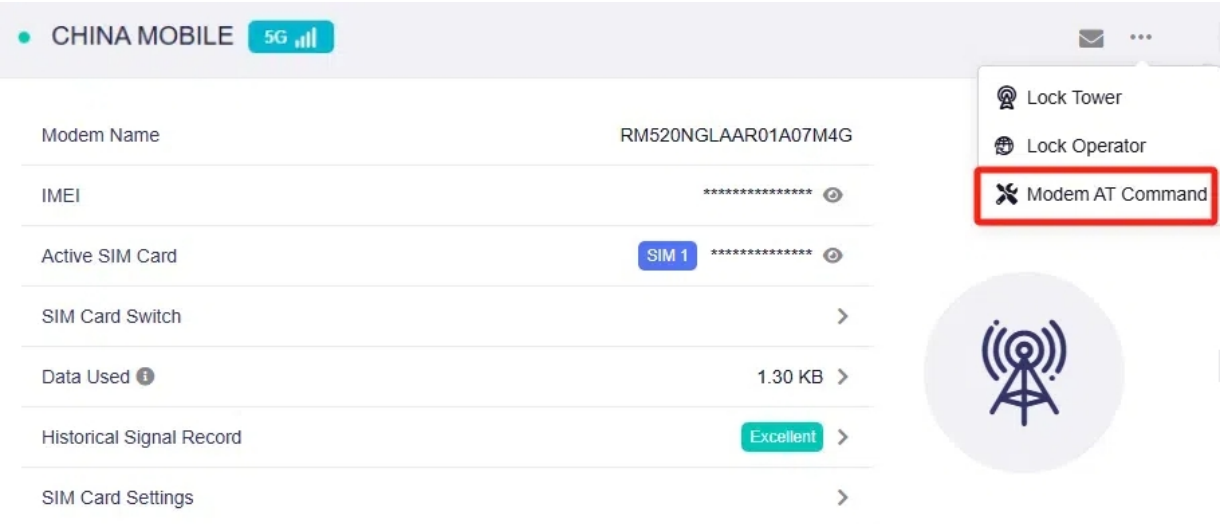
- **Auto**: Automatische Verbindung mit einem verfügbaren Mobilfunknetz.
- **Manual**: Manuelle Festlegung auf einen bestimmten Netzbetreiber.
- **Manual-Auto**: Automatischer Wechsel zu einem verfügbaren Mobilfunknetz, wenn die manuelle Festlegung fehlschlägt.



4.2.4.10 AT-Befehle für das Modem

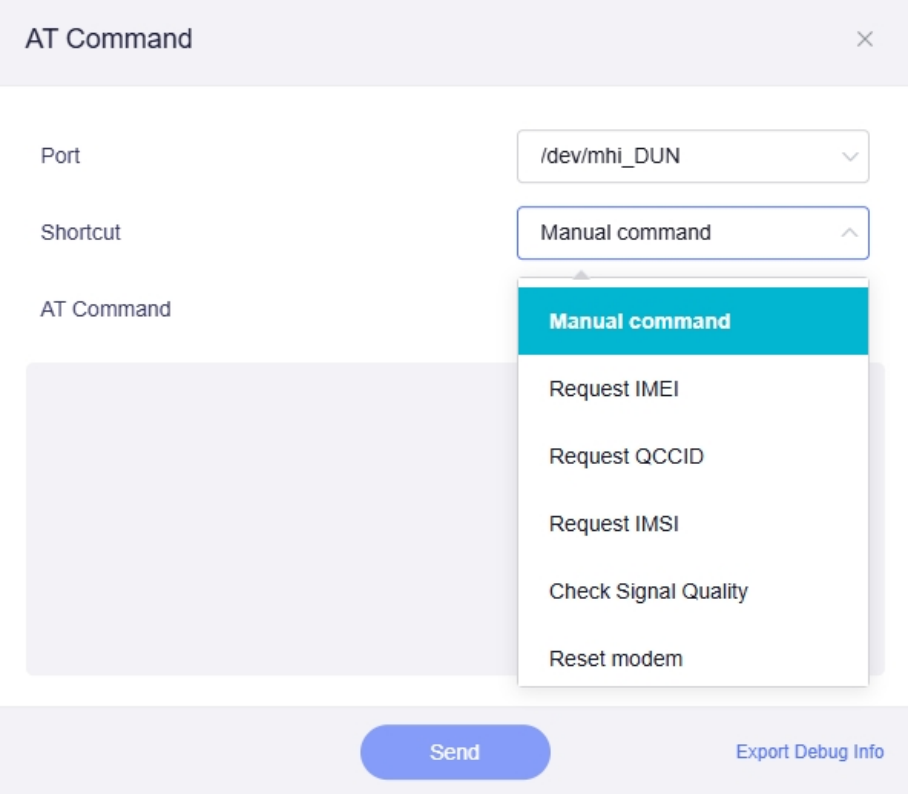
AT-Befehle sind standardisierte Anweisungen zur Kommunikation mit dem Mobilfunkmodem. Mit dieser Funktion können Sie Befehle senden und den Modemstatus prüfen.

Öffnen Sie in der Weboberfläche des Routers **INTERNET** > **Cellular**. Klicken Sie oben rechts auf das Symbol mit den drei Punkten und wählen Sie **Modem AT Command**.

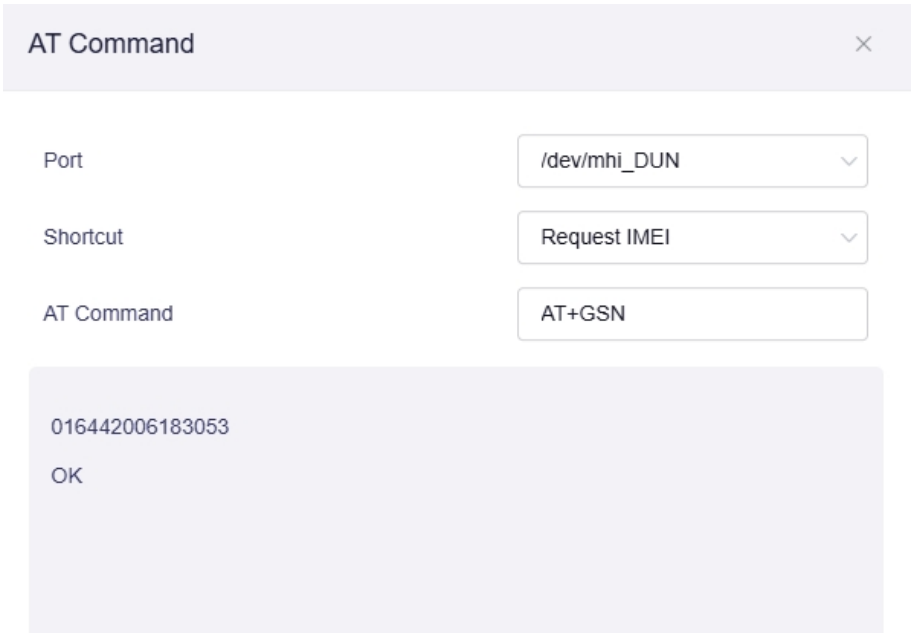


Die Seite AT Command wird geöffnet.

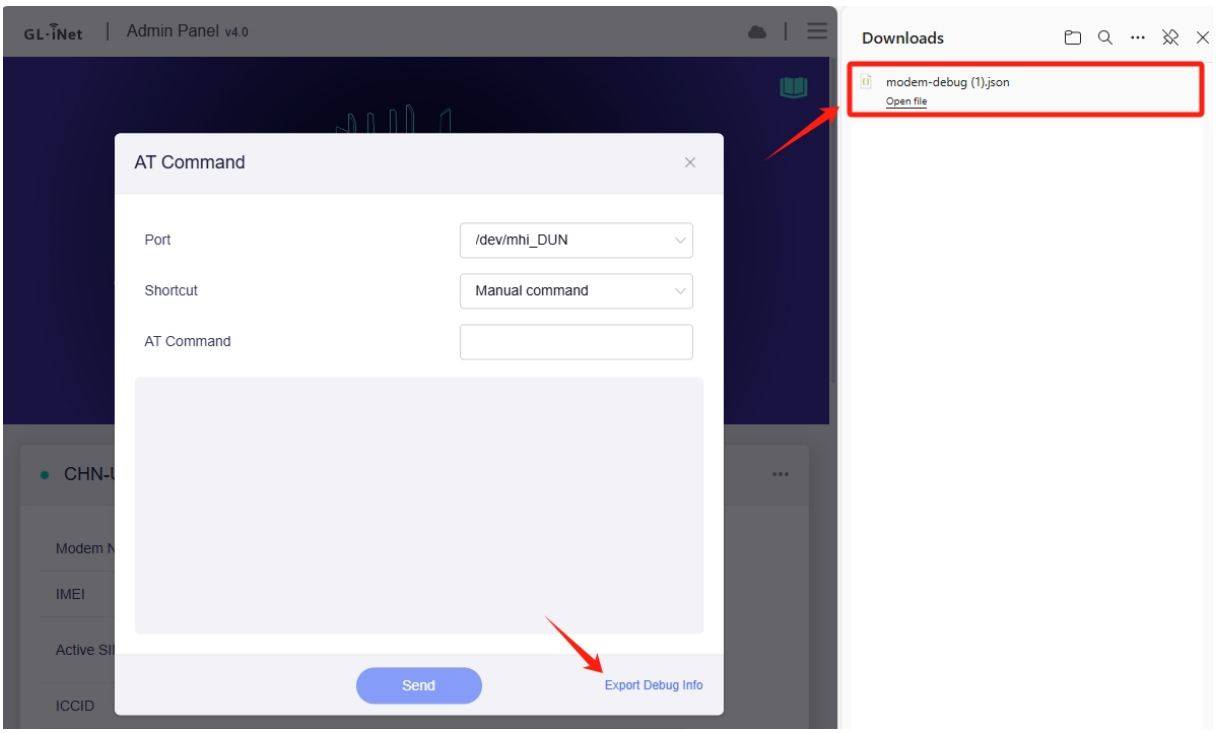
- **Befehl manuell eingeben**
  Wenn unter Shortcut die Option Manual command ausgewählt ist, können Sie den gewünschten Befehl im Feld AT Command eingeben. Die Ergebnisse werden im grauen Feld unten angezeigt.
- **Voreingestellter Befehl**
  Sie können auch auf das Feld Shortcut klicken und einen voreingestellten Befehl aus der Liste auswählen, etwa Request IMEI, Check Signal Quality oder Reset Modem.



Wählen Sie beispielsweise „Request IMEI“ aus und klicken Sie auf „Send“. Das Ergebnis wird wie unten dargestellt angezeigt.



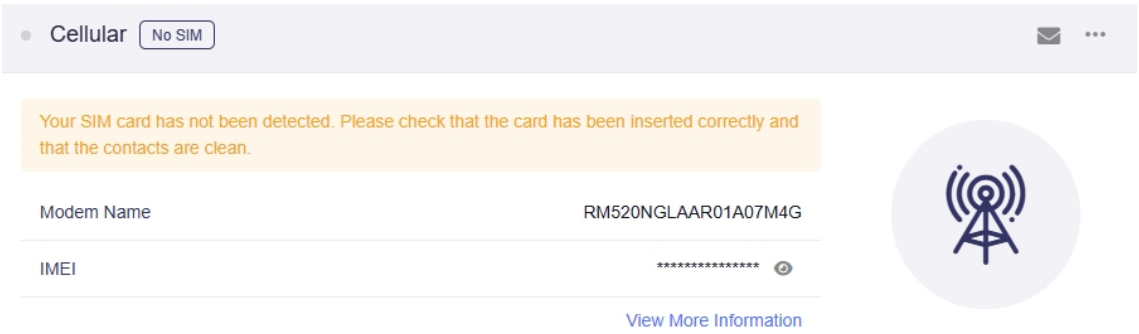
Klicken Sie unten rechts auf **Export Debug Info**, um eine JSON-Datei herunterzuladen.



4.2.4.11 Fehlerbehebung

Wenn keine Mobilfunkverbindung hergestellt werden kann, wählen Sie anhand der angezeigten Fehlermeldung die passende Lösung.

- **Keine SIM-Karte / Ihre SIM-Karte wurde nicht erkannt.**



Versuchen Sie Folgendes:

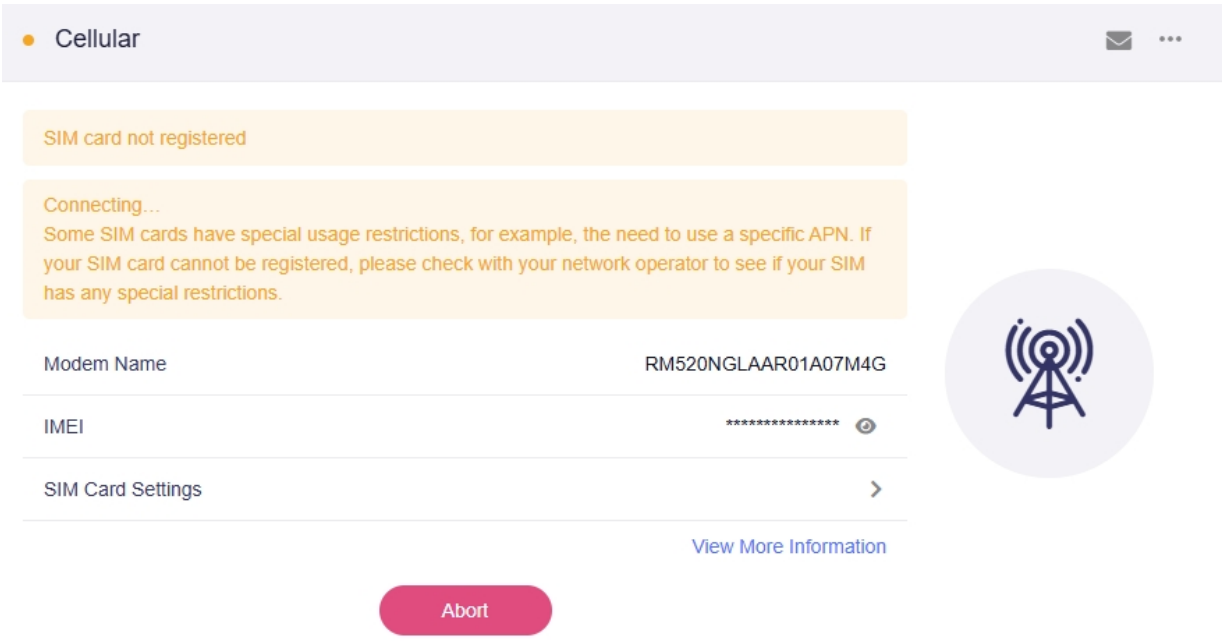
1. Laden Sie die Seite neu und warten Sie einige Minuten, um zu prüfen, ob die SIM-Karte erkannt wird.
2. Prüfen Sie, ob die SIM-Karte richtig eingesetzt ist. Richten Sie die abgeschrägte Ecke der SIM-Karte an der entsprechenden Markierung des Steckplatzes aus, um die korrekte Ausrichtung sicherzustellen.
3. Schalten Sie den Router aus, entnehmen Sie die SIM-Karte, setzen Sie sie erneut ein und schalten Sie den Router wieder ein.
4. Versuchen Sie es nach Möglichkeit mit einer anderen SIM-Karte.

Wenn das Problem weiterhin besteht, laden Sie die Protokolle herunter und senden Sie sie an support@gl-inet.com.

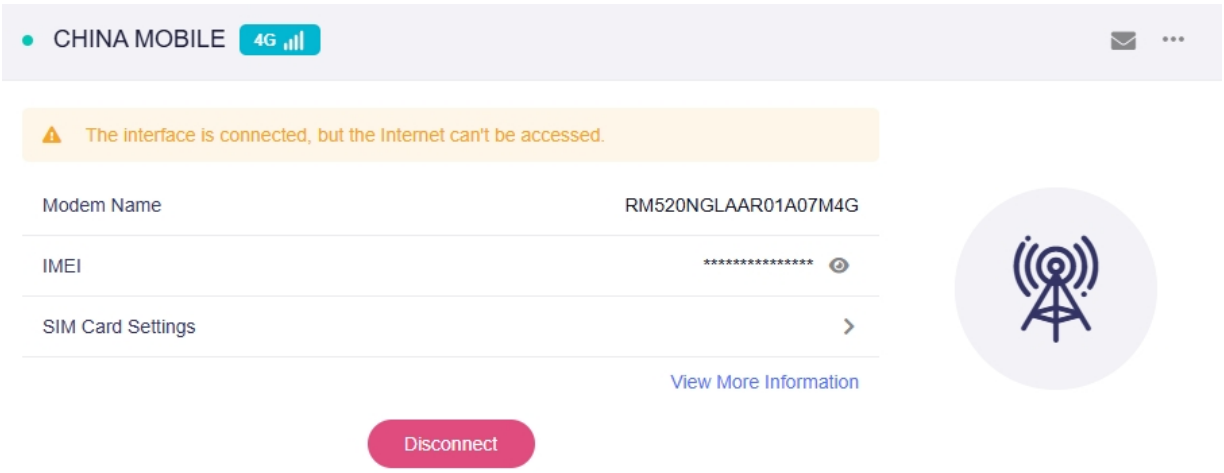
- **SIM-Karte nicht registriert / Die Schnittstelle ist verbunden, aber es besteht kein Internetzugang.**

  Bei diesem Problem können zwei Fehlermeldungen auftreten:

  (1) SIM-Karte nicht registriert.



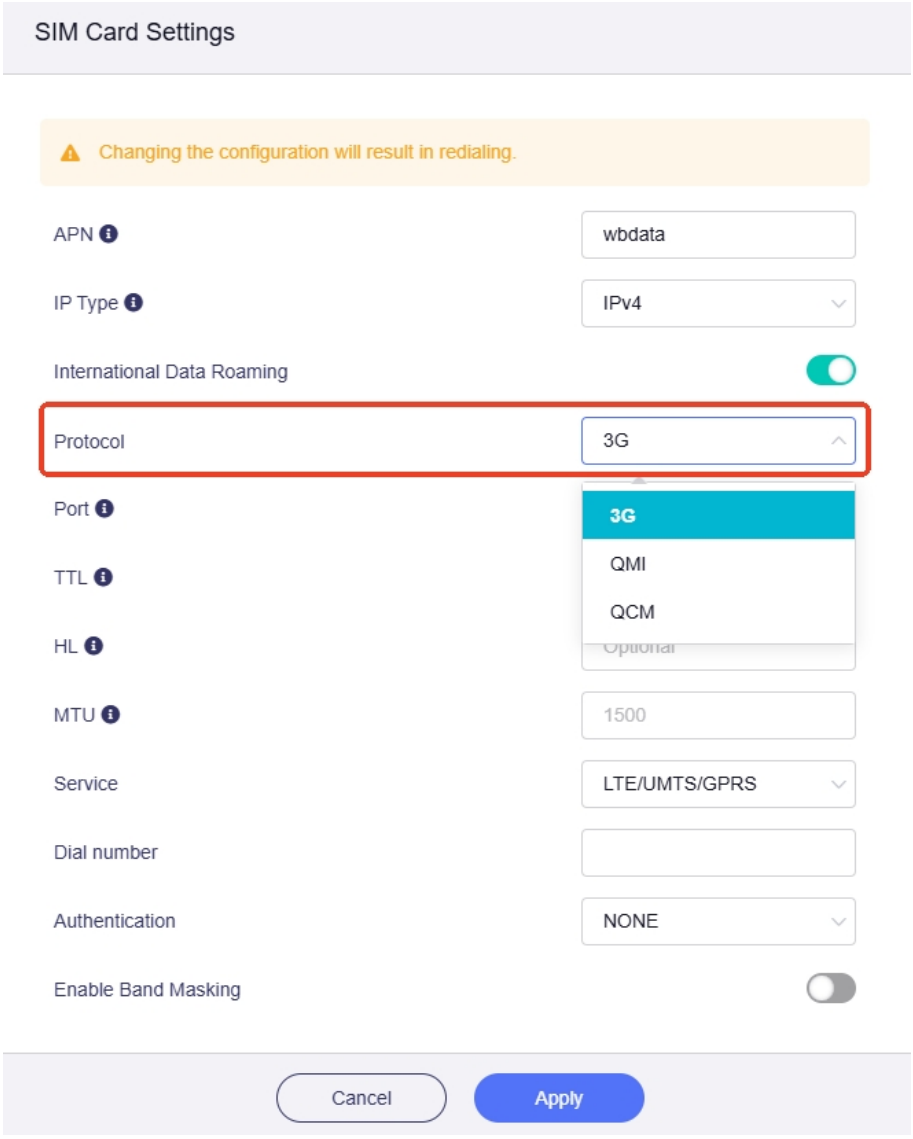
(2) Die Schnittstelle ist verbunden, aber es besteht kein Internetzugang.



Versuchen Sie Folgendes:

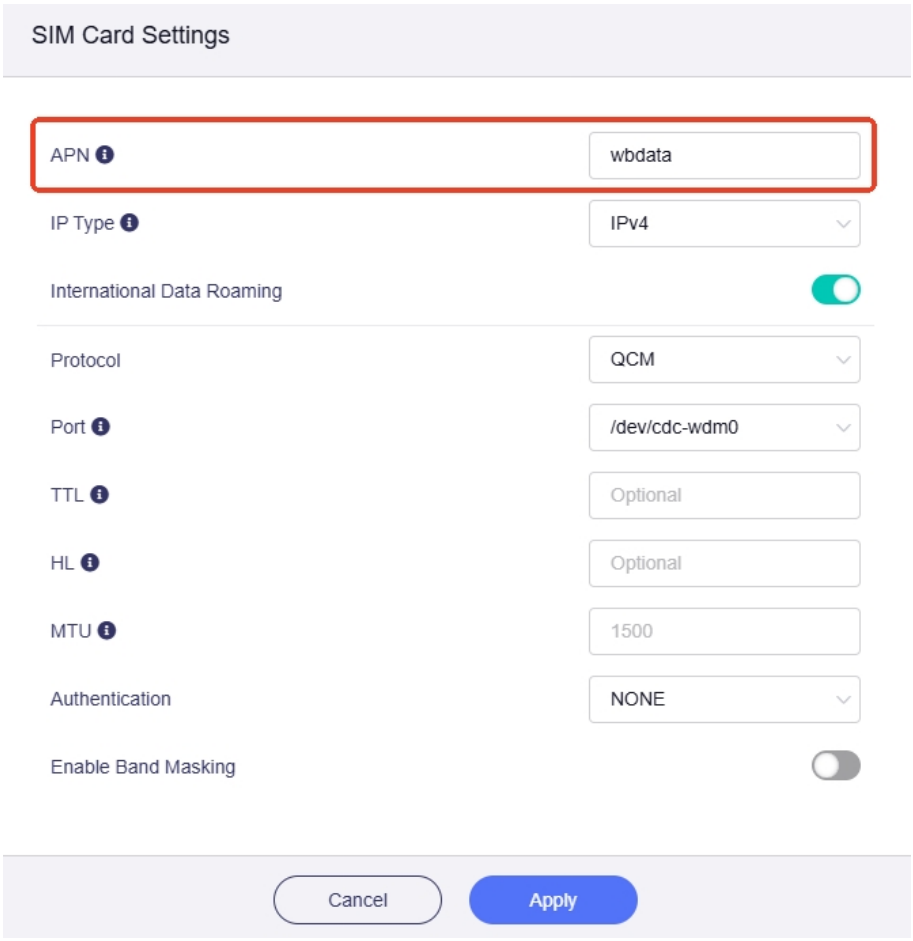
1. Laden Sie die Seite neu und warten Sie einige Minuten, um zu prüfen, ob die Fehlermeldung verschwindet.
2. Klicken Sie auf **Disconnect**/**Abort** und anschließend auf **Connect**, um die Verbindung erneut herzustellen.
3. Starten Sie den Router neu.
4. Prüfen Sie den Status der SIM-Karte und stellen Sie sicher, dass sie aktiviert ist. Setzen Sie die SIM-Karte testweise in ein Smartphone ein und prüfen Sie, ob sie mit einem aktiven Datentarif regulären Internetzugang ermöglicht. Wenden Sie sich alternativ zur Überprüfung an Ihren Mobilfunkanbieter.

5. Einige Mobilfunkanbieter benötigen für die Netzwerkverbindung das 3G-Protokoll. Öffnen Sie **SIM Card Settings** > **Protocol**, wählen Sie **3G** und klicken Sie auf **Apply**.



Das Gerät stellt die Verbindung automatisch neu her. Warten Sie einige Minuten und prüfen Sie, ob die Verbindung erfolgreich hergestellt wurde.

6. Für einige SIM-Karten gelten besondere Nutzungsvorgaben, etwa ein bestimmter APN. Wenn sich Ihre SIM-Karte nicht registrieren lässt, fragen Sie Ihren Anbieter nach solchen Einschränkungen. Öffnen Sie bei Bedarf **SIM Card Settings** > **APN**, konfigurieren Sie den richtigen APN auf dem Router und klicken Sie auf **Apply**.



7. Klicken Sie auf **View More Information**, um die Mobilfunksignalstärke zu prüfen. Vergewissern Sie sich bei schwachem Signal, dass die Antenne richtig montiert ist. Stellen Sie den Router für einen besseren Empfang an einem offenen, hindernisfreien Ort auf.
8. Prüfen Sie, ob **Band Masking** oder **Lock Tower** aktiviert ist. Deaktivieren Sie diese Funktionen gegebenenfalls und versuchen Sie erneut, eine Verbindung herzustellen.

Wenn das Problem weiterhin besteht, laden Sie die Protokolle herunter und senden Sie sie an support@gl-inet.com.

Kapitel 5

WLAN

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

5.1 WLAN-Statusanzeige

Die WLANs des Routers sind standardmäßig aktiviert. Das entsprechende WLAN-Symbol unter der Geräteabbildung auf der Seite INTERNET leuchtet.



Wenn Sie den Mauszeiger über ein aktives WLAN-Symbol bewegen, wird wie unten dargestellt ein WLAN-QR-Code angezeigt. Scannen Sie diesen QR-Code, um sich schnell mit dem jeweiligen WLAN zu verbinden.

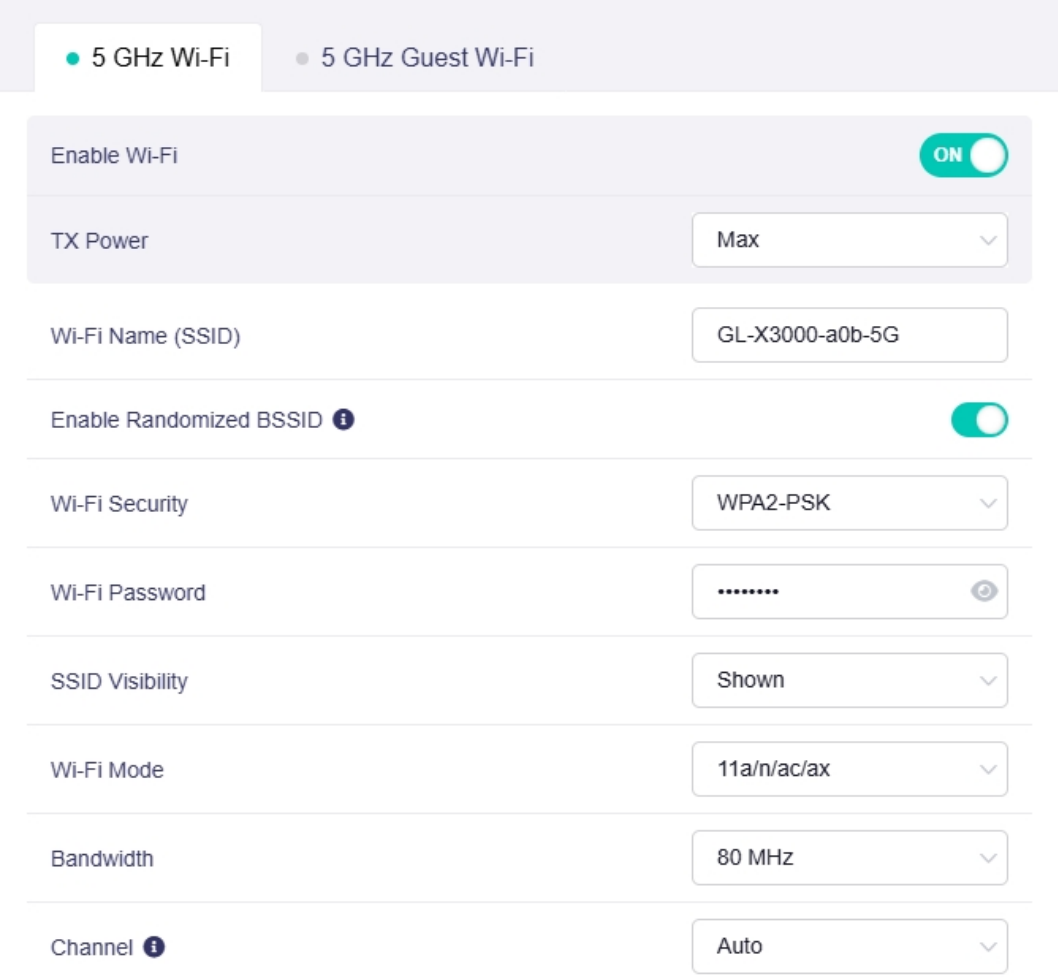


5.2 WLAN-Einstellungen

Melden Sie sich an der Weboberfläche an und öffnen Sie **WIRELESS**.
Die WLAN-Seite zeigt die Einstellungen für das 2,4-GHz- und das 5-GHz-WLAN des Routers. Beide Frequenzbänder sind zur flexiblen Verwaltung jeweils in Haupt- und Gastnetzwerk unterteilt.

5.2.1 5-GHz-WLAN

Für das 5-GHz-Hauptnetzwerk stehen folgende Einstellungen zur Verfügung: WLAN ein- oder ausschalten, Sendeleistung, zufällige BSSID ein- oder ausschalten, WLAN-Name (SSID), Sicherheit, Passwort, Sichtbarkeit der SSID, Modus, Bandbreite und Kanal.



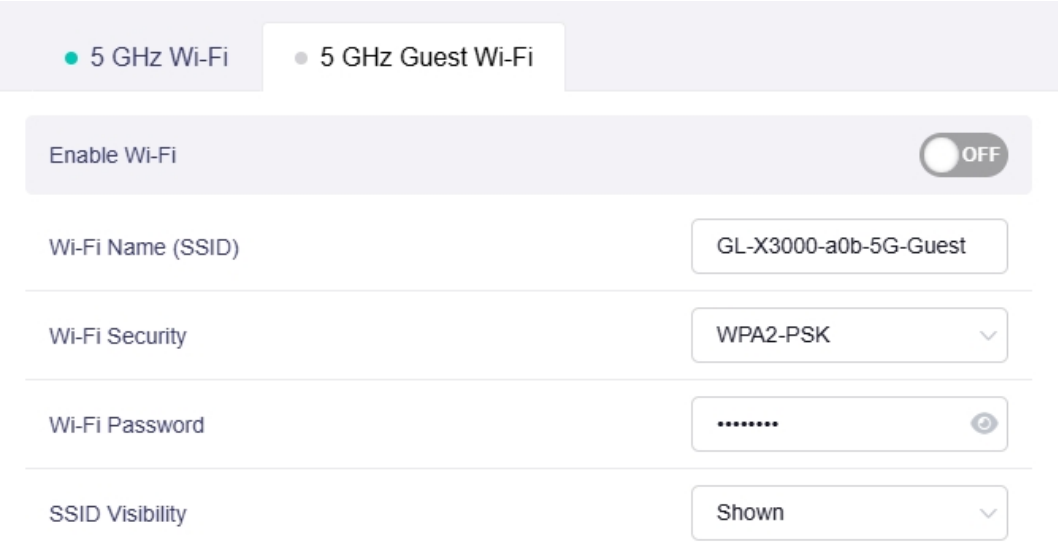
Hinweis:

1. **Randomized BSSID** ist standardmäßig aktiviert. Diese Funktion erschwert es, den Router anhand einer festen BSSID zu orten. Endgeräte können die BSSIDs in ihrer Umgebung

zusammen mit dem eigenen Standort an Betriebssystem- oder Gerätehersteller melden, die daraus eine Datenbank zur Zuordnung von BSSIDs zu Standorten erstellen. Bei aktivierter Funktion verwendet der Router eine zufällig erzeugte BSSID, die bei jedem Neustart erneuert wird. So lässt sich die BSSID keinem festen Standort zuordnen.

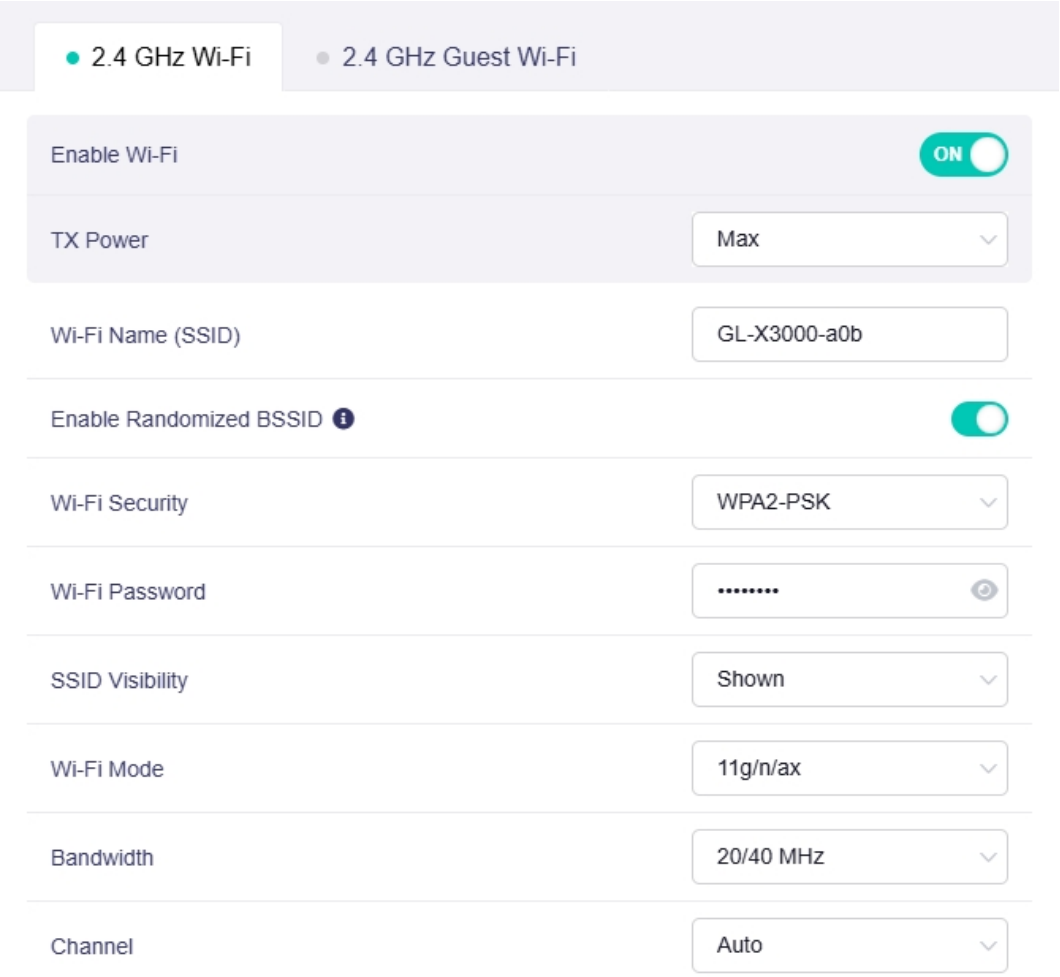
2. Die Einstellungen **Bandwidth** und **Channel** lassen sich nicht ändern, wenn der Router als Repeater eingerichtet ist, da sie vom übergeordneten WLAN übernommen werden.
3. Wenn **Channel** auf **Auto** eingestellt ist, wechselt das WLAN des Routers nicht automatisch auf einen DFS-Kanal.
4. Wenn **Bandwidth** auf **160 MHz** eingestellt ist (nur bei einigen Modellen verfügbar), verwendet das WLAN immer einen DFS-Kanal, auch wenn Sie einen Kanal ohne DFS oder Auto auswählen.

Für das 5-GHz-Gastnetzwerk stehen vereinfachte Einstellungen zur Verfügung: WLAN ein- oder ausschalten, WLAN-Name (SSID), Sicherheit, Passwort und Sichtbarkeit der SSID.



5.2.2 2,4-GHz-WLAN

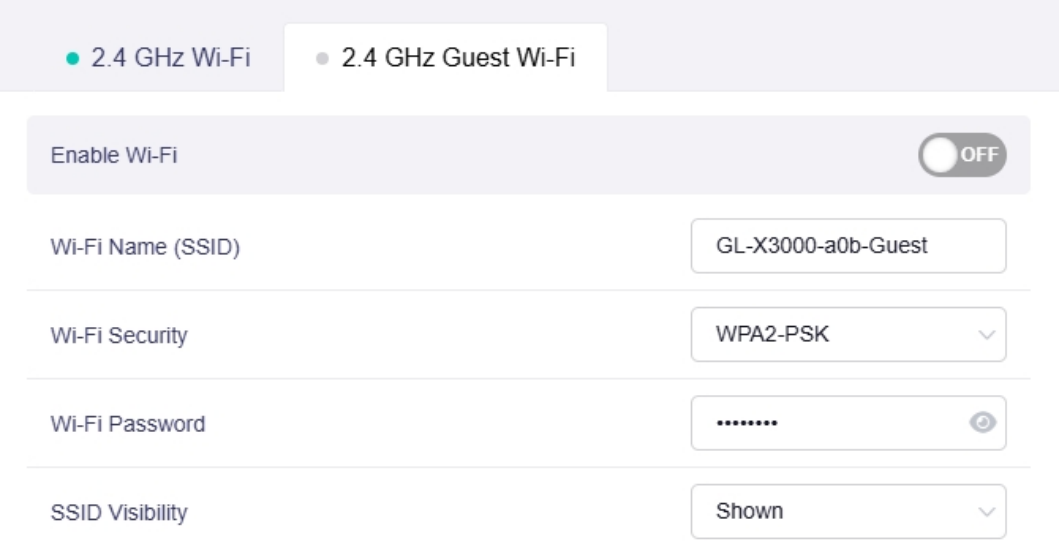
Für das 2,4-GHz-Hauptnetzwerk stehen folgende Einstellungen zur Verfügung: WLAN ein- oder ausschalten, Sendeleistung, zufällige BSSID ein- oder ausschalten, WLAN-Name (SSID), Sicherheit, Passwort, Sichtbarkeit der SSID, Modus, Bandbreite und Kanal.



Hinweis:

1. **Randomized BSSID** ist standardmäßig aktiviert. Diese Funktion erschwert es, den Router anhand einer festen BSSID zu orten. Endgeräte können die BSSIDs in ihrer Umgebung zusammen mit dem eigenen Standort an Betriebssystem- oder Gerätehersteller melden, die daraus eine Datenbank zur Zuordnung von BSSIDs zu Standorten erstellen. Bei aktivierter Funktion verwendet der Router eine zufällig erzeugte BSSID, die bei jedem Neustart erneuert wird. So lässt sich die BSSID keinem festen Standort zuordnen.
2. Die Einstellungen **Bandwidth** und **Channel** lassen sich nicht ändern, wenn der Router als Repeater eingerichtet ist, da sie vom übergeordneten WLAN übernommen werden.

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



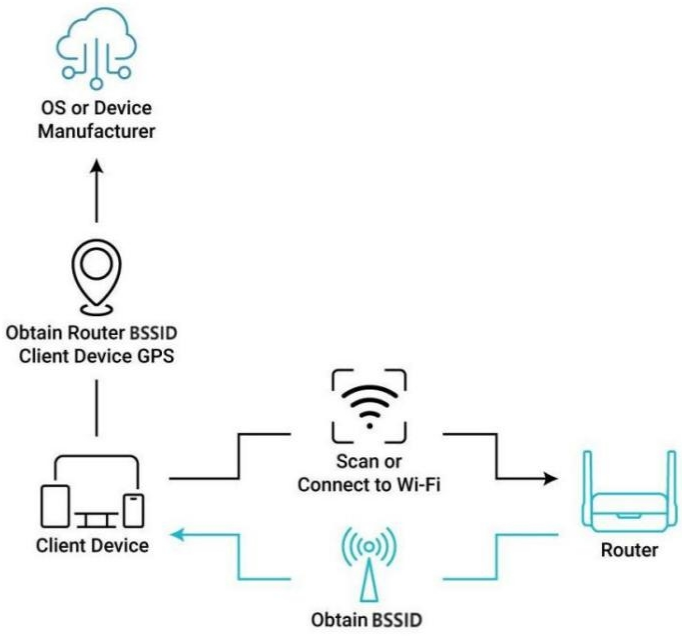
5.2.3 Zufällige BSSID

Die zufällige BSSID ist eine Datenschutzfunktion, die seit Firmware v4.6 verfügbar und standardmäßig aktiviert ist. Sie verhindert, dass Ihr Router anhand einer festen WLAN-BSSID, also der MAC-Adresse seiner WLAN-Schnittstelle, geortet und verfolgt wird.

Warum eine feste BSSID ein Datenschutzrisiko

darstellt: Mobile Betriebssysteme wie Android und iOS nutzen gemeinsam gesammelte WLAN-Positionsdaten für ihre Standortdienste:

1. Endgeräte wie Smartphones und Laptops übermitteln regelmäßig die von ihnen erkannten BSSIDs zusammen mit ihrem per GPS ermittelten Standort an den Server des Betriebssystem- oder Geräteherstellers.
2. Die Hersteller führen diese Daten in einer weltweiten Datenbank zusammen, die BSSIDs Standorten zuordnet.
3. Jedes Gerät mit aktiviertem WLAN kann diese Datenbank abfragen, um seinen Standort anhand der BSSIDs in der Umgebung zu schätzen – auch ohne GPS.
4. Ein Router mit einer festen BSSID wirkt dadurch wie ein stationärer Standortsender: Er kann aus der Ferne geortet werden, und seine Bewegungen, beispielsweise auf Reisen, lassen sich über längere Zeit verfolgen. Angreifer können solche Datenbanken ebenfalls abfragen, um Router zu orten oder anhand der Herstellerkennung (OUI) in ihrer BSSID wiederzuerkennen.


OS or Device
Manufacturer
Obtain Router BSSID
Client Device GPS
Scan or
Connect to Wi-Fi
Client Device
Router
Obtain BSSID

So schützt Sie die zufällige BSSID

Bei aktivierter Funktion erzeugt der Router eine zufällige BSSID und erneuert sie bei jedem Start. Da sich die BSSID laufend ändert, kann sie in den Herstellerdatenbanken keinem festen Standort mehr zugeordnet werden. Die zur Nachverfolgung genutzte Verknüpfung zwischen BSSID und Standort wird dadurch unterbrochen.

Status	Verhalten
Aktiviert (Standard)	Bei jedem Start wird eine neue zufällige BSSID erzeugt.
Deaktiviert	Der Router verwendet seine tatsächliche werkseitige MAC-Adresse als BSSID.

Hinweise:

1. Die BSSID ändert sich nur beim Neustart des Routers. Während des laufenden Betriebs bleibt sie gleich.
2. Die BSSID des Gastnetzwerks bleibt auf demselben Frequenzband auf die BSSID des Hauptnetzwerks abgestimmt.
3. Die zufällige BSSID verhindert die Nachverfolgung über die BSSID des Routers. Sie hindert Endgeräte jedoch nicht daran, ihren eigenen Standort zu melden, und bietet keinen vollständigen Schutz der Privatsphäre: SSID, Kanal und Signaleigenschaften bleiben weiterhin erkennbar.

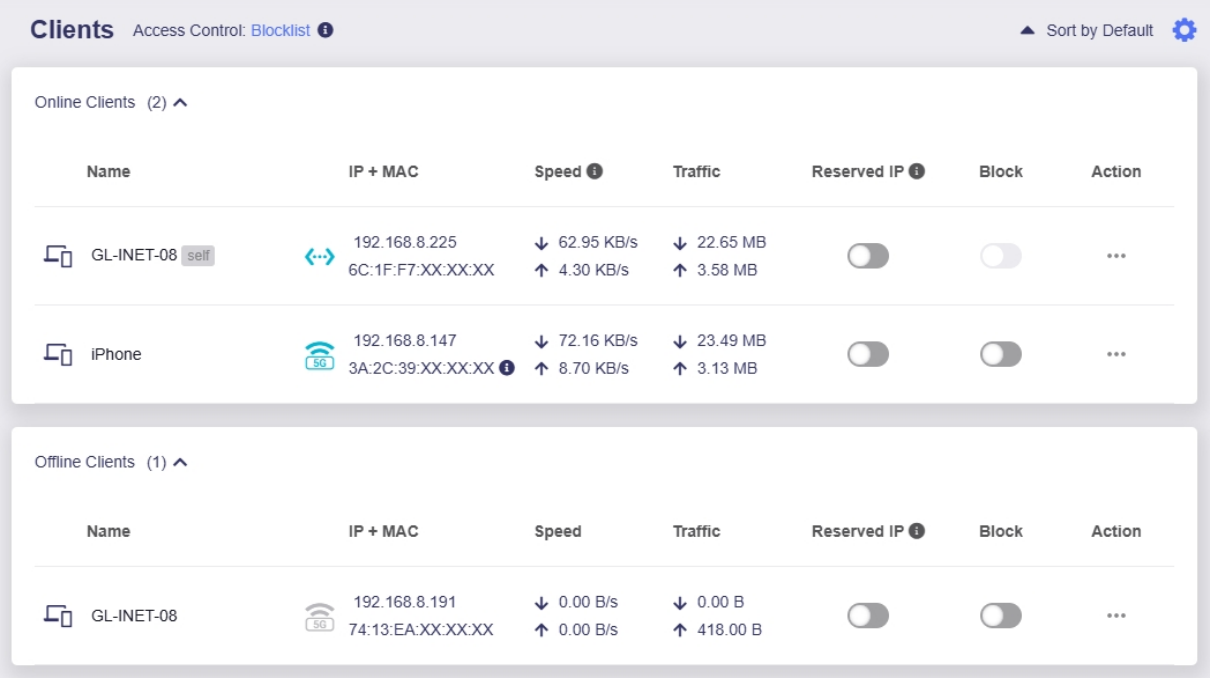
Kapitel 6

Verbundene Geräte

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

6.1 Gerätedetails

Melden Sie sich an der Weboberfläche Ihres Routers 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.



Tipp: Online Clients sind Geräte, die derzeit mit dem Netzwerk des Routers verbunden sind. Offline Clients sind Geräte, die früher verbunden waren, derzeit aber keine Verbindung zum Netzwerk haben.

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



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

3. **Geschwindigkeit**

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

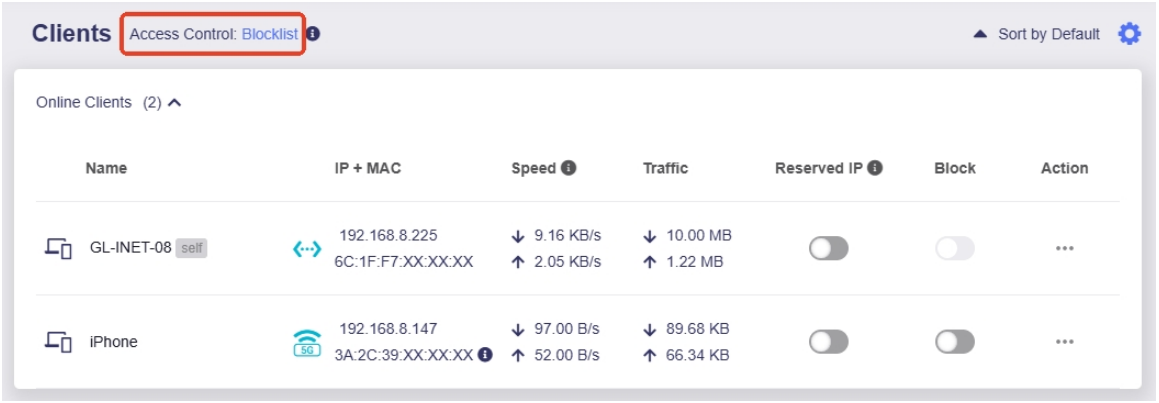
4. **Datenverkehr**: Die vierte Spalte zeigt das übertragene Internetdatenvolumen des Geräts an.

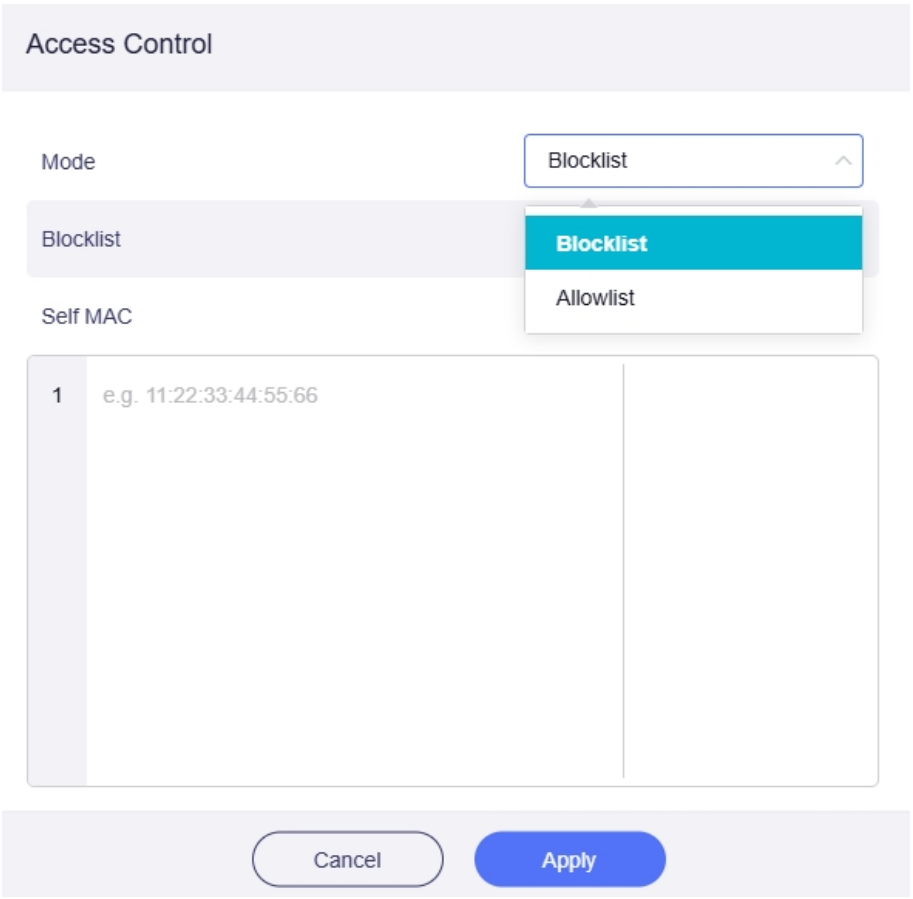
5. **IP-Adresse reservieren**

   In der fünften Spalte können Sie mit einem Klick eine IP-Adresse für ein verbundenes Gerät reservieren. Wenn Sie einem Endgerät im lokalen Netzwerk eine reservierte IP-Adresse zuweisen, erhält es bei jeder Verbindung mit dem Router dieselbe IP-Adresse.

6. **Sperrliste**

   In der sechsten Spalte können Sie bestimmte verbundene Geräte mit einem Klick sperren. Die Zugriffskontrolle verwendet standardmäßig eine Sperrliste (Blocklist). Bei Bedarf können Sie oben auf der Seite zu einer Freigabeliste (Allowlist) wechseln.



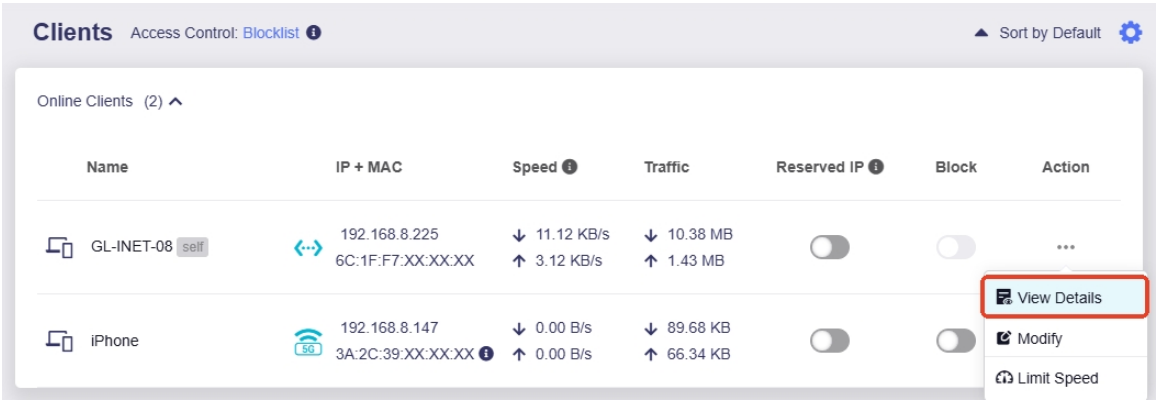


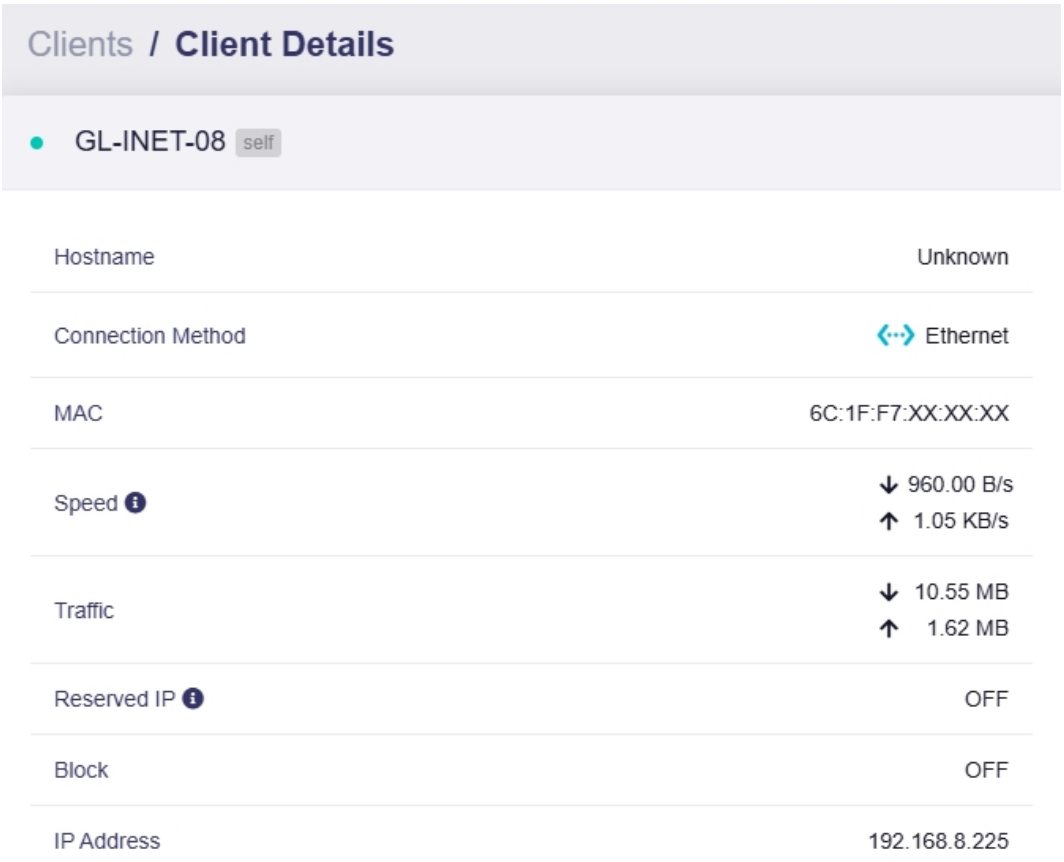
- **Blacklist**: Geräte, deren MAC-Adressen auf der Sperrliste stehen, dürfen sich nicht mit diesem Router verbinden. Die Sperre basiert auf der MAC-Adresse des Geräts. Verwendet ein gesperrtes Gerät beim nächsten Verbindungsversuch eine andere MAC -Adresse, kann es sich dennoch verbinden.
- **Allowlist**: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

6.2 Aktionen

1. **Details anzeigen**

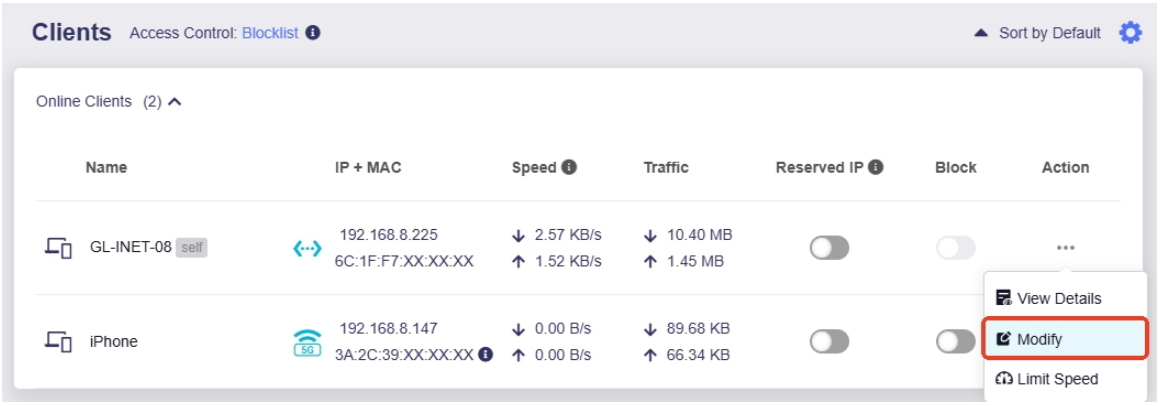
   Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Dropdown-Menü **View Details**, um die Gerätedetails auf einer eigenen Seite anzuzeigen.

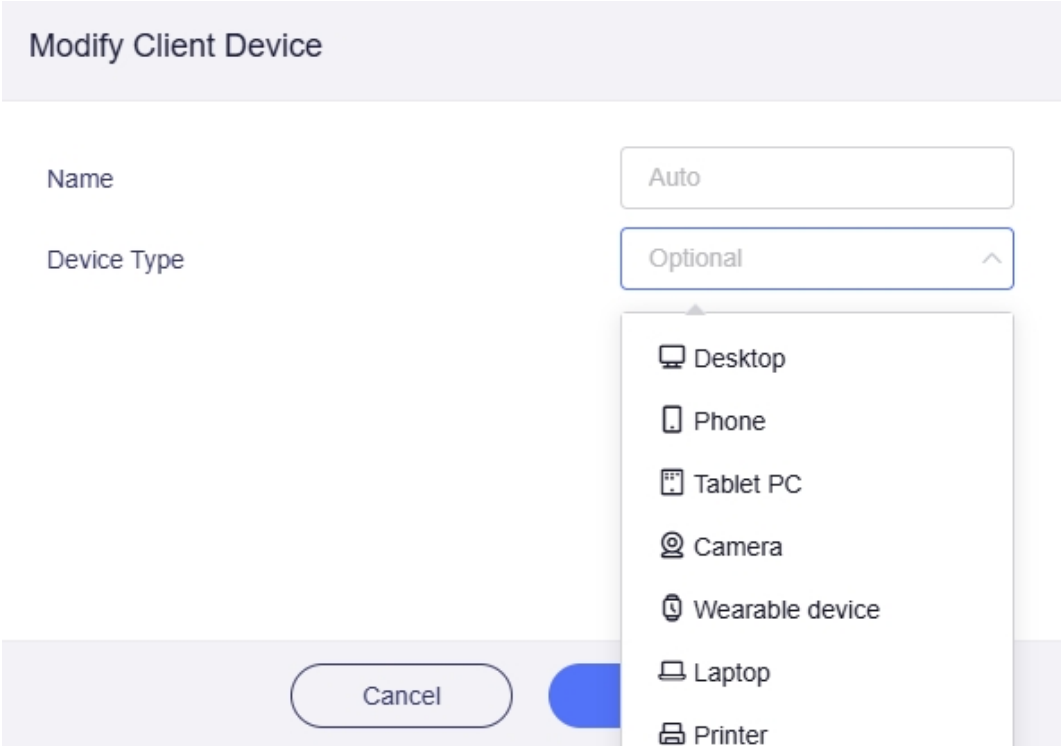




2. **Gerät bearbeiten**

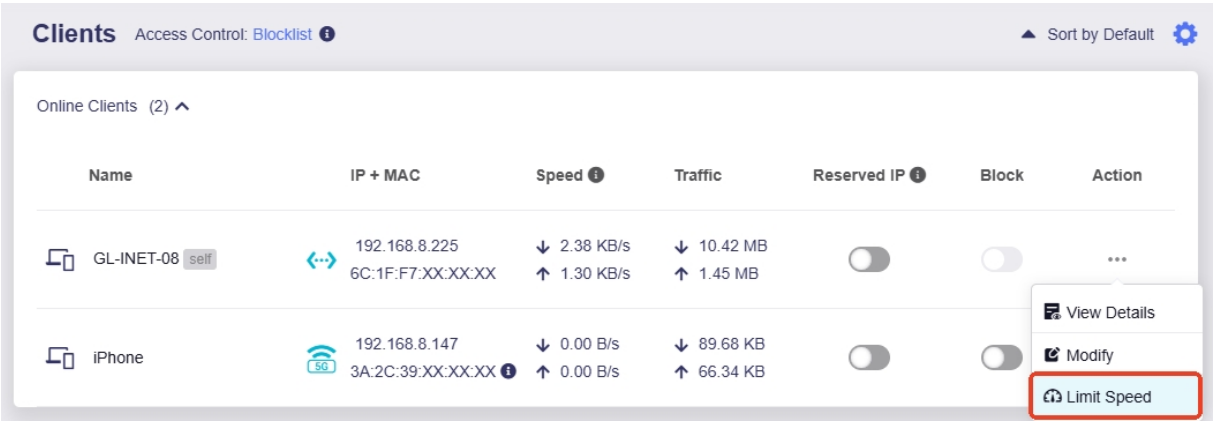
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Modify**, um den Gerätenamen und -typ zu ändern.



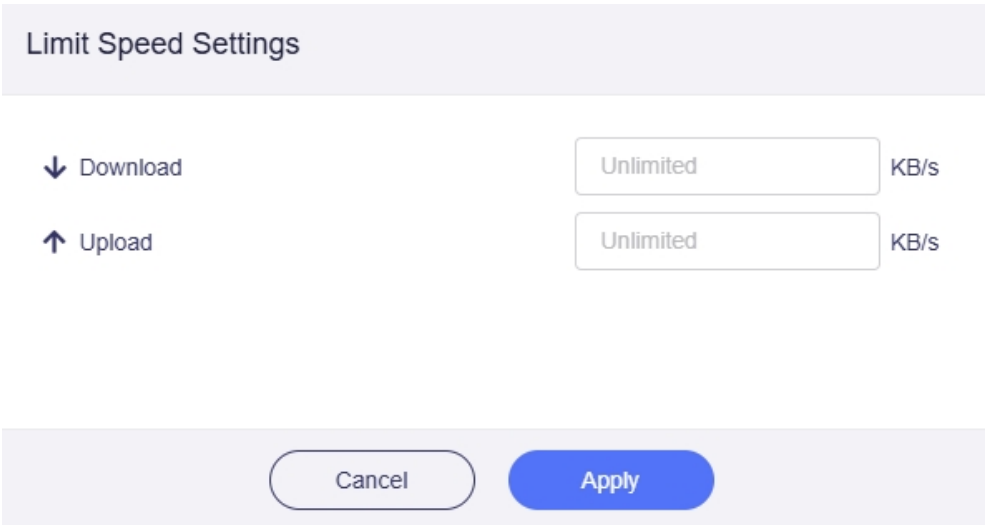


3. **Geschwindigkeit begrenzen**

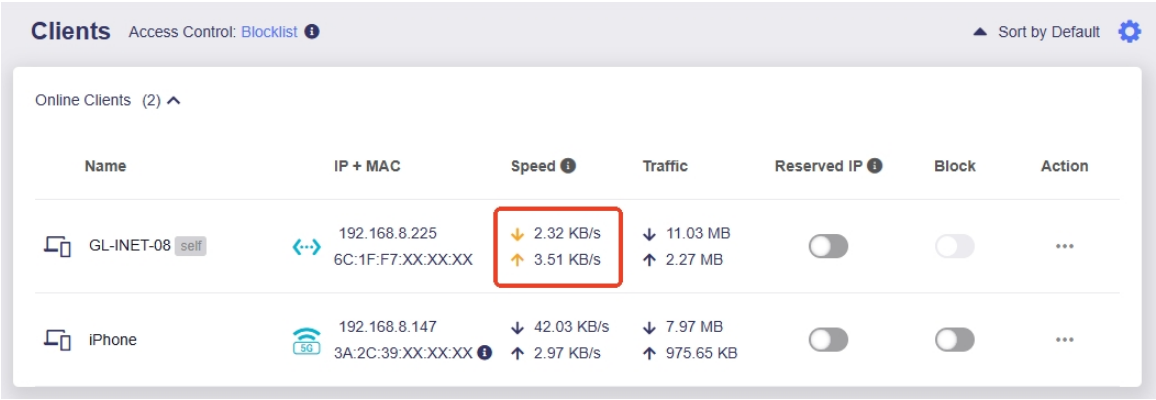
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Limit Speed**.



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

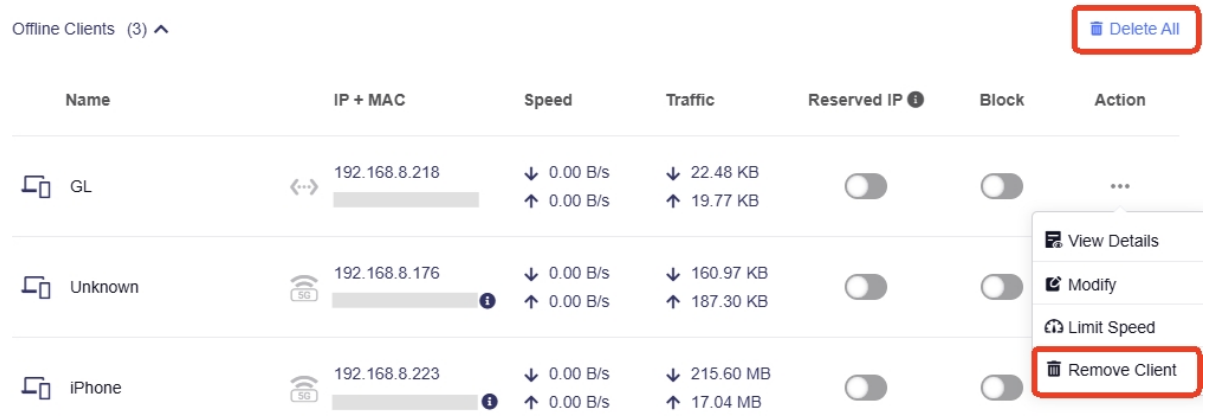


Bei Geräten mit aktivierter Geschwindigkeitsbegrenzung werden die Pfeile für die Upload- und Downloadgeschwindigkeit gelb angezeigt.



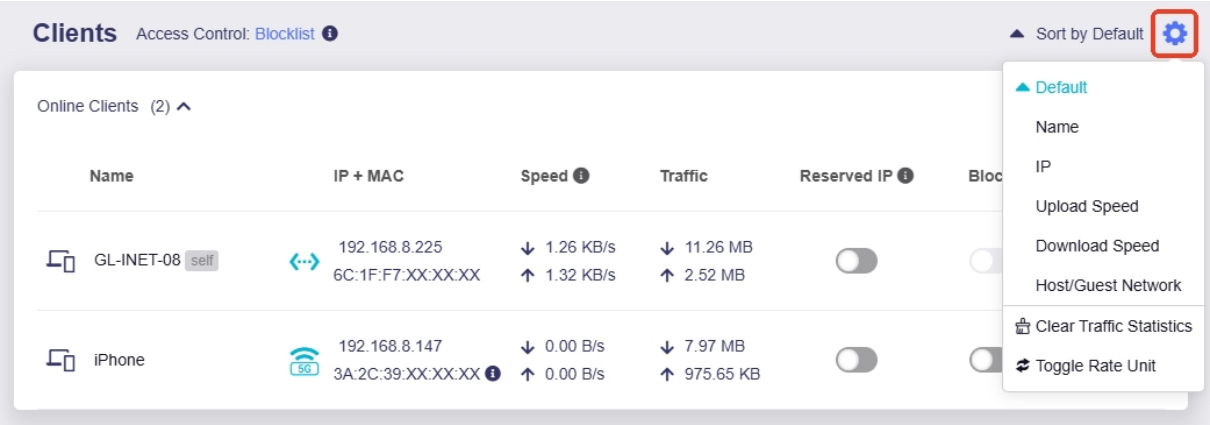
6.3 Geräte entfernen

Im Abschnitt **Offline Clients** können Sie oben rechts auf **Delete All** klicken, um alle nicht verbundenen Clients zu löschen. Um einen bestimmten Client zu entfernen, klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen im Dropdown-Menü **Remove Client**.



6.4 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 7

Cloud-Dienste

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

7.1 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.

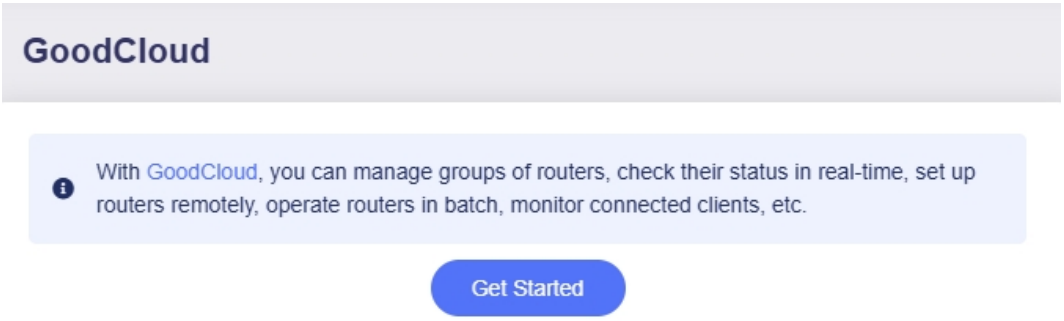
Mit GoodCloud können Sie:

- 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

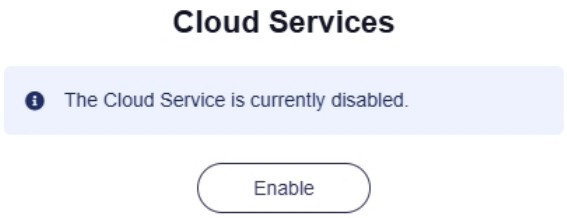
Einige Funktionen sind im Enterprise-Tarif und im VAR-Tarif (Value Added Reseller) verfügbar. Weitere Informationen finden Sie hier.

7.1.1 GoodCloud aktivieren

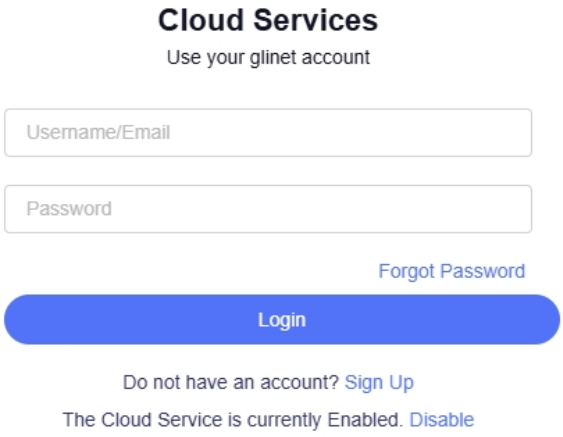
1. Melden Sie sich an der Weboberfläche Ihres Routers an, öffnen Sie **CLOUD SERVICE** > **GoodCloud** und klicken Sie auf **Get Started**.



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.

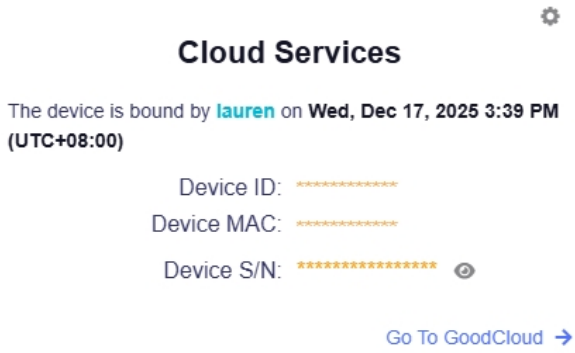


Tipps:

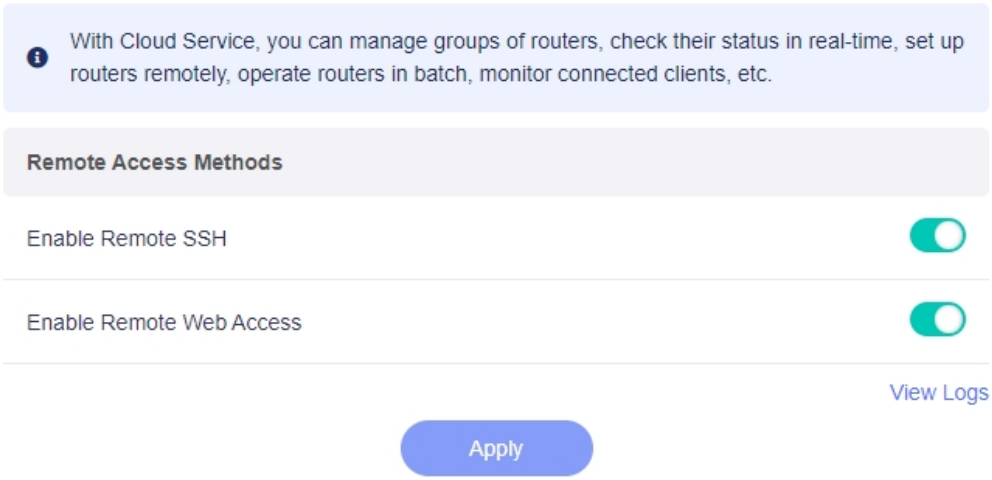
- Die Schritte zur Verknüpfung mit GoodCloud unterscheiden sich je nach Firmwareversion.

- 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. Hier können Sie den Fernzugriff für Ihren Router aktivieren oder deaktivieren.



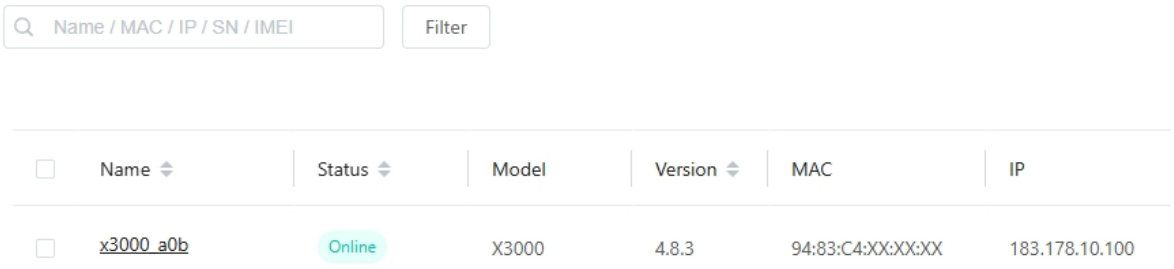
- **Remote SSH:** Per SSH von GoodCloud aus auf das Terminal des Routers zugreifen.
- **Remote Web Access:** Über HTTP/HTTPS von GoodCloud aus auf die Weboberfläche des Routers zugreifen.

- **View Logs:** Die Protokollseite öffnen und das Cloud-Protokoll anzeigen.

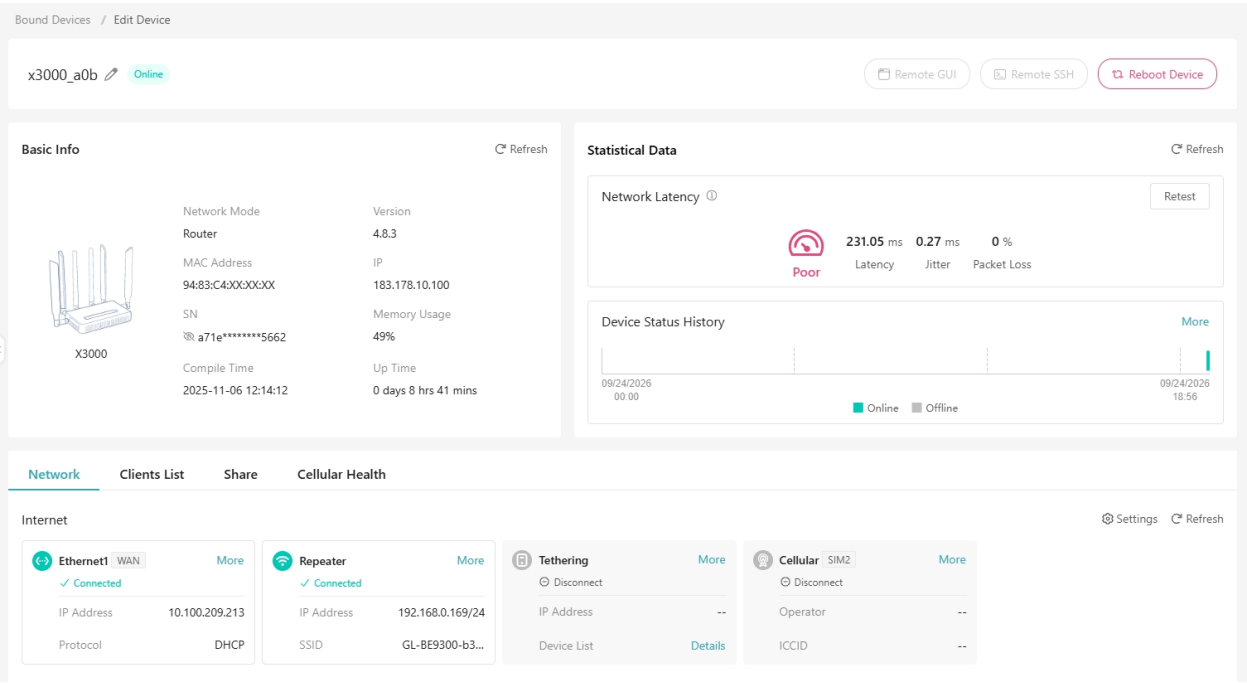
7.1.2 Router verwalten

7.1.2.1 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.

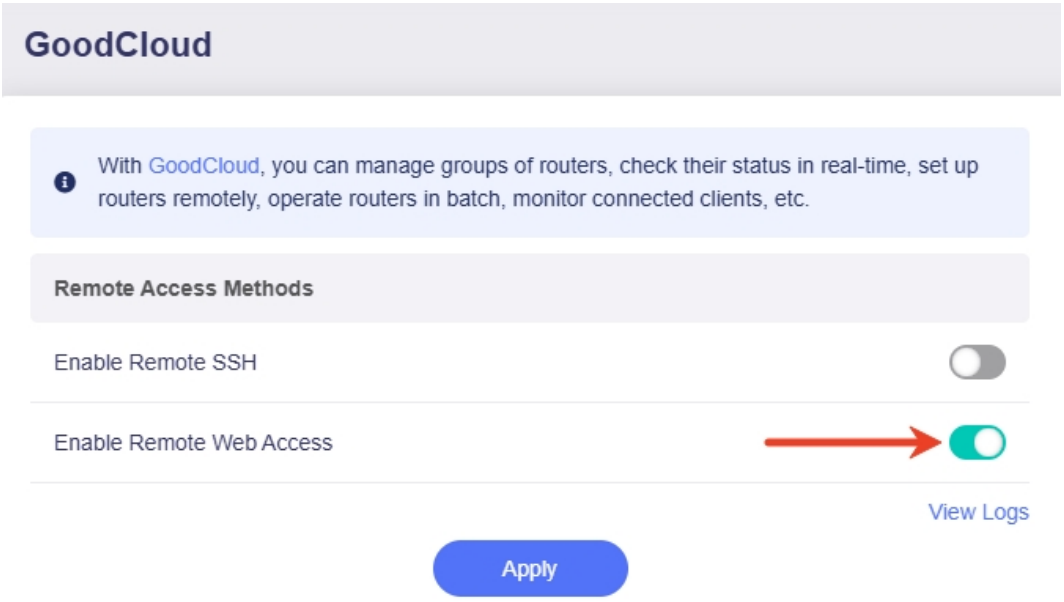


Klicken Sie auf den Gerätenamen, um die Detailseite zu öffnen. Diese enthält grundlegende Informationen, Statistiken, eine Netzwerkübersicht, die Geräteliste und eine Zeitleiste. Außerdem können Sie erweiterte Aktionen ausführen, etwa aus der Ferne auf den Router zugreifen oder ihn neu starten.

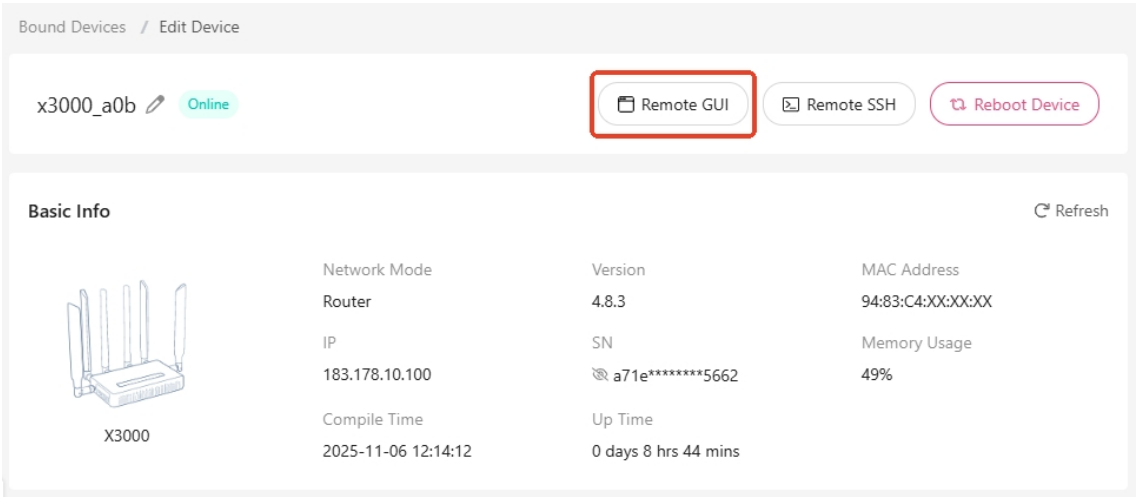


7.1.2.2 Fernzugriff auf die Weboberfläche

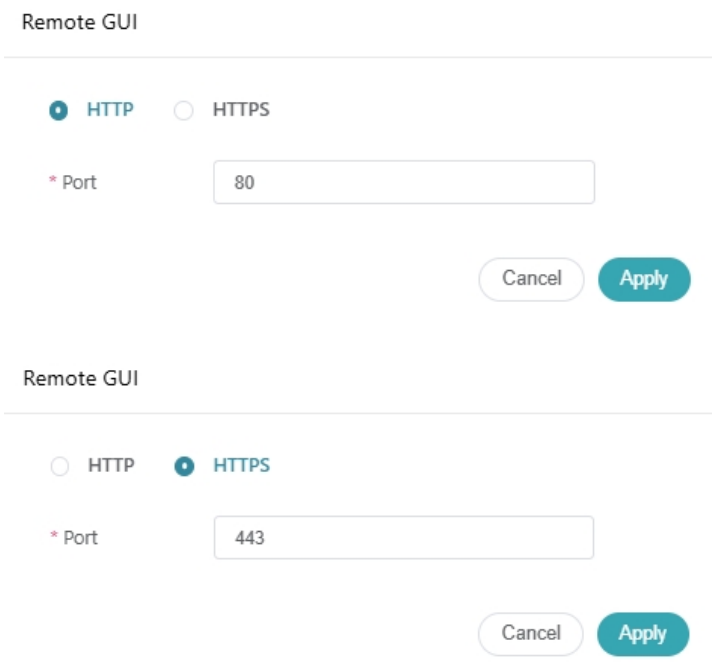
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote Web Access** und klicken Sie auf **Apply**.



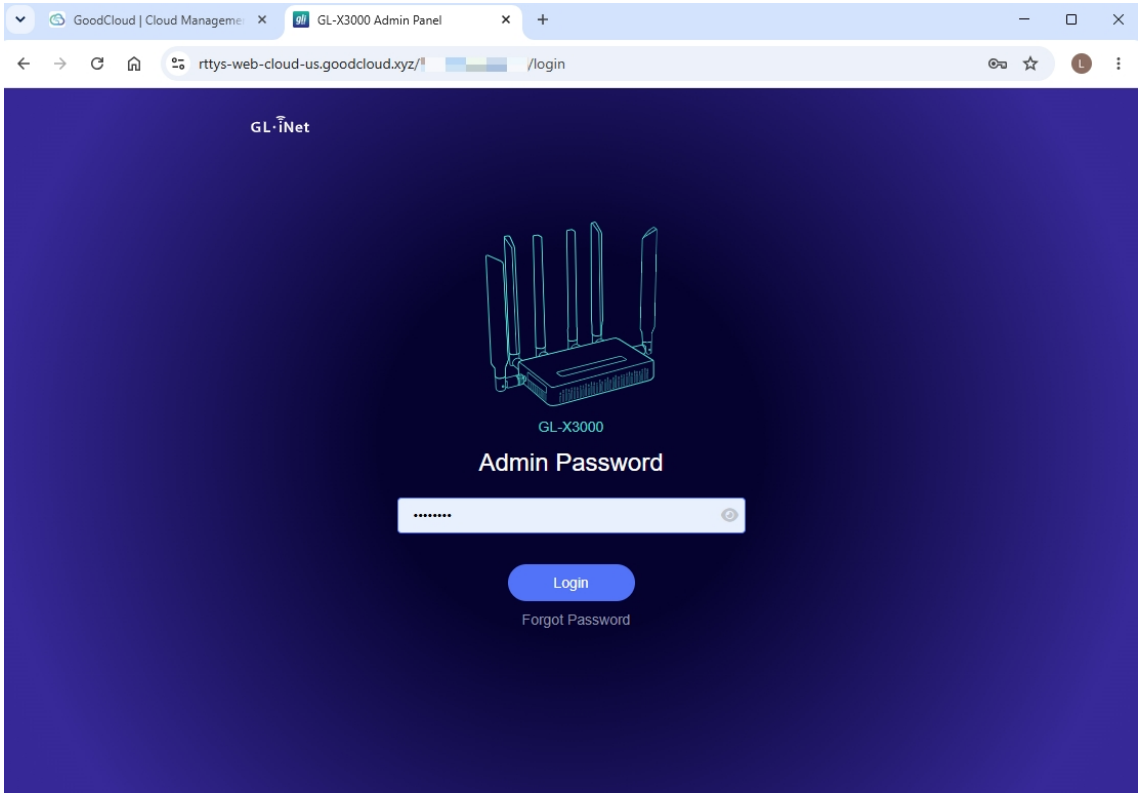
2. Melden Sie sich bei GoodCloud an und öffnen Sie **Device** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote GUI**.



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**.

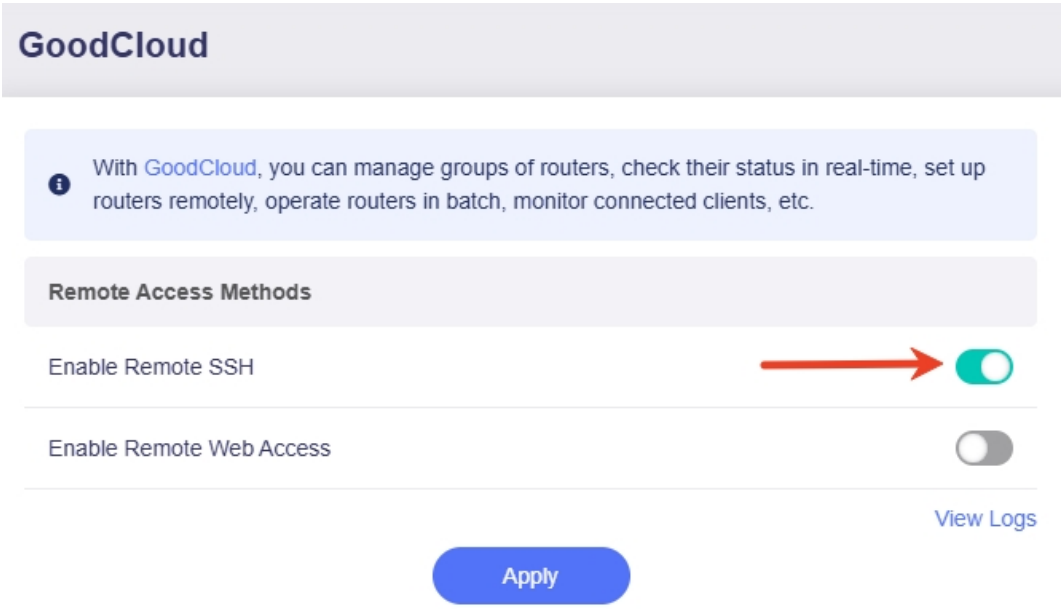


5. Sie werden zur Anmeldeseite des Routers weitergeleitet. Geben Sie das Administratorpasswort ein, um aus der Ferne auf die Weboberfläche zuzugreifen.

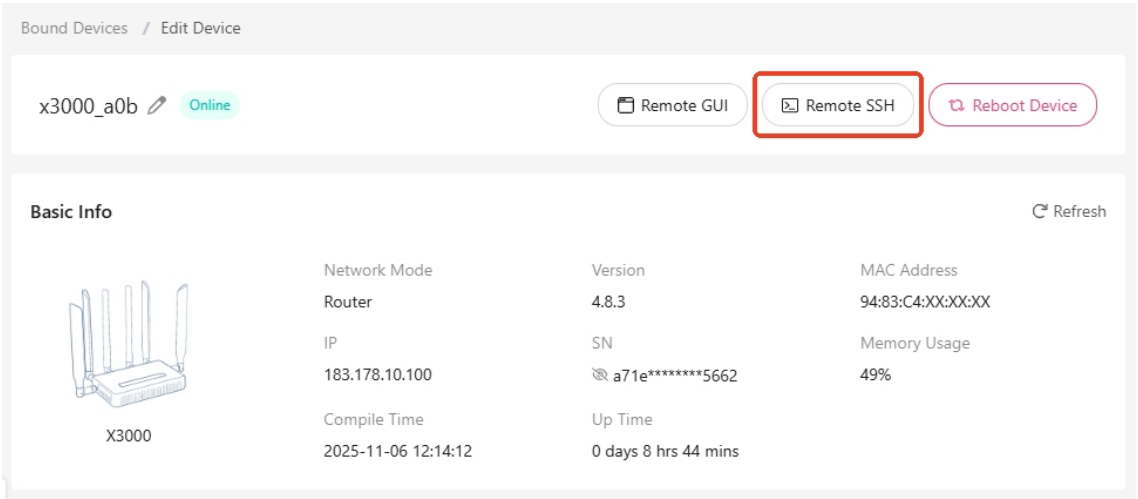


7.1.2.3 SSH-Fernzugriff

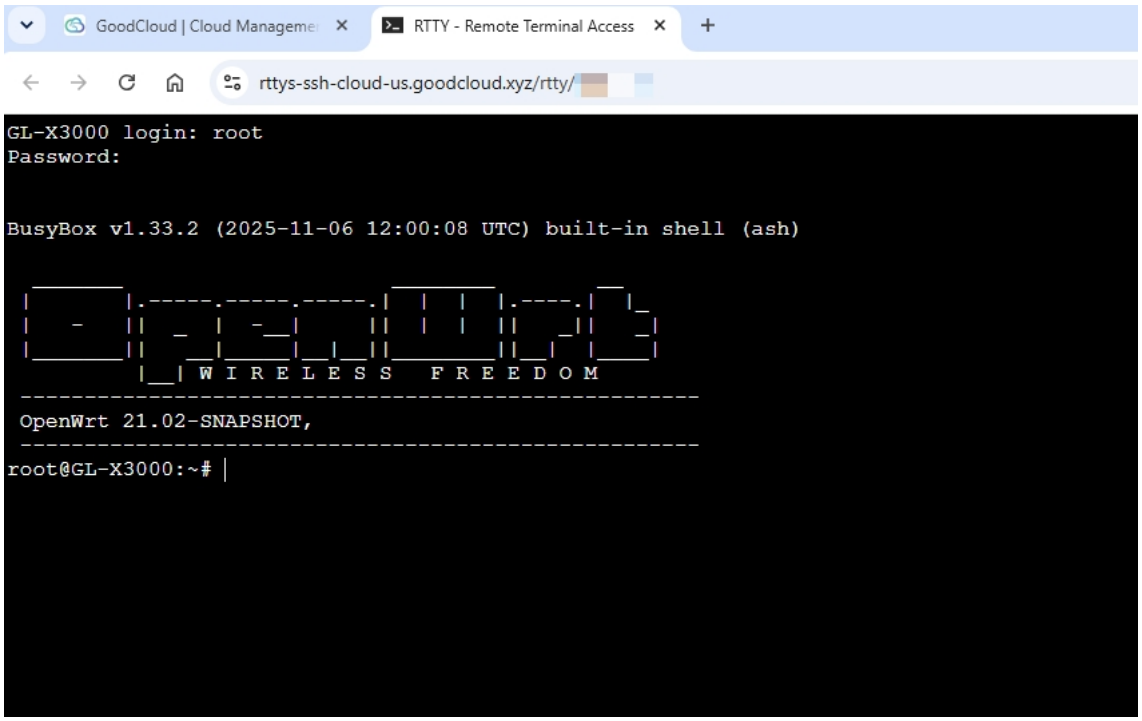
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote SSH** und klicken Sie auf **Apply**.



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**.

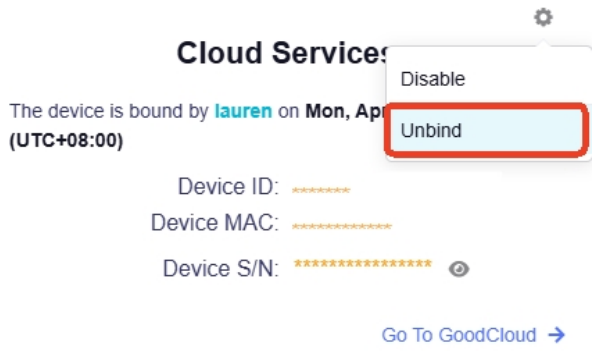


4. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

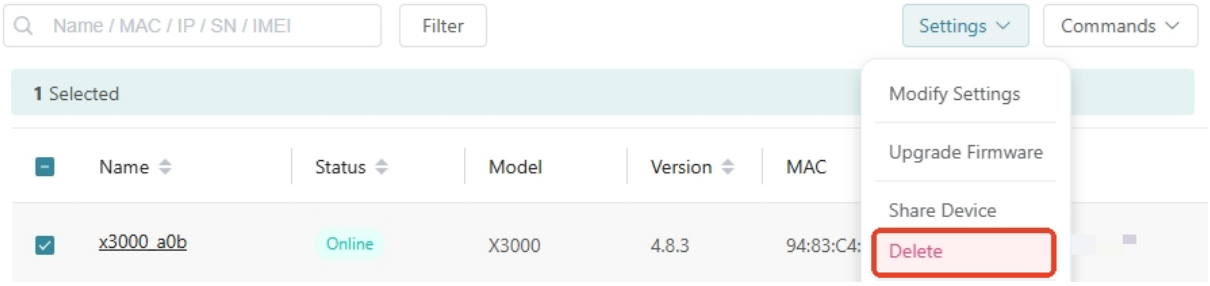

GoodCloud | Cloud Manageme
RTTY - Remote Terminal Access
rttys-ssh-cloud-us.goodcloud.xyz/rtty/
GL-X3000 login: root
Password:
BusyBox v1.33.2 (2025-11-06 12:00:08 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-X3000:~#

7.1.3 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.

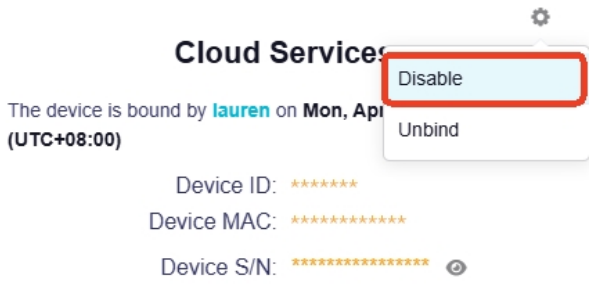


Alternativ können Sie sich an der Cloud-Plattform anmelden und **Device** > **Bound Devices** öffnen. Wählen Sie das Gerät aus, dessen Verknüpfung Sie aufheben möchten. Klicken Sie oben rechts auf **Settings** und wählen Sie **Delete**. Die Verknüpfung Ihres Geräts mit Ihrem GoodCloud-Konto wird daraufhin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



7.1.4 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**.

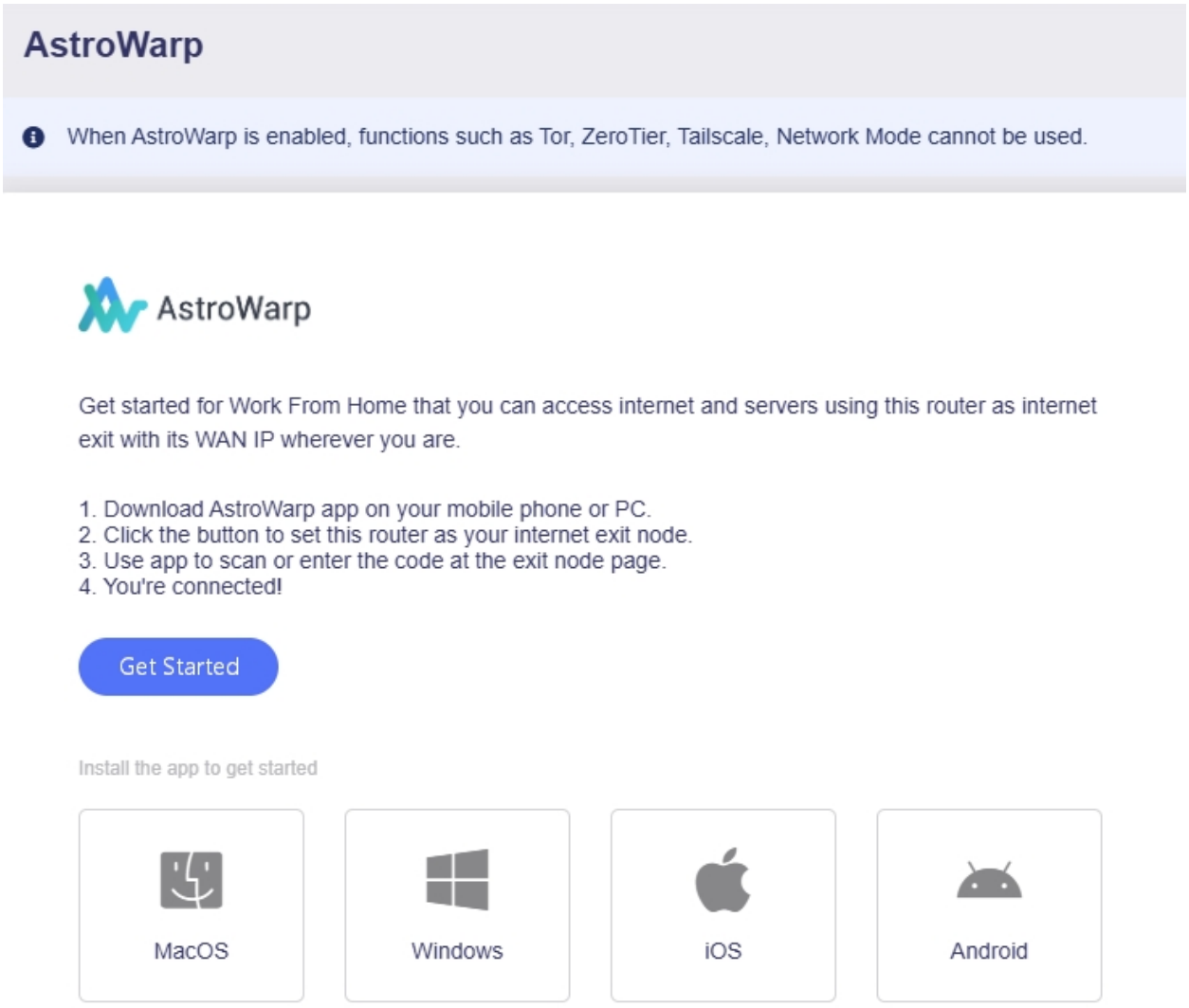


Der Cloud-Dienst wird daraufhin deaktiviert.

7.2 AstroWarp

AstroWarp ist eine Netzwerkplattform, die mehrere GL.iNet-Router nahtlos zu einem gemeinsamen Netzwerk verbindet und so einen einfachen Fernzugriff ermöglicht. Mit flexiblen Netzwerkfunktionen, benutzerfreundlicher Konfiguration und zuverlässigem Datenschutz bietet AstroWarp jederzeit sichere und verlässliche Verbindungen. Die Plattform eignet sich sowohl für die Arbeit aus der Ferne als auch für den sicheren Zugriff auf interne Unternehmensressourcen an mehreren Standorten und ermöglicht leistungsfähige, geschützte Netzwerke.

Melden Sie sich an der Weboberfläche Ihres Routers an, öffnen Sie **CLOUD SERVICE** > **AstroWarp** und klicken Sie auf **Get Started**. Folgen Sie anschließend den Anweisungen zur Einrichtung Ihres Netzwerks. Einzelheiten finden Sie auf astrowarp.net.



Kapitel 8

VPN kennenlernen

Dieses Kapitel erläutert die Grundlagen von VPN und typische Einsatzmöglichkeiten.

8.1 Einführung

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 WireGuard

WireGuard® ist ein schlankes, schnelles VPN-Protokoll, das einfacher und effizienter als OpenVPN ist. Es verwendet moderne Kryptografie für einen effizienten Betrieb, eine kleine Codebasis für eine einfachere Sicherheitsprüfung sowie moderne Algorithmen (ChaCha20/Poly1305) zur Verschlüsselung und Gewährleistung der Datenintegrität.
*WireGuard® ist eine eingetragene Marke von Jason A. Donenfeld.

8.2 Einsatzmöglichkeiten

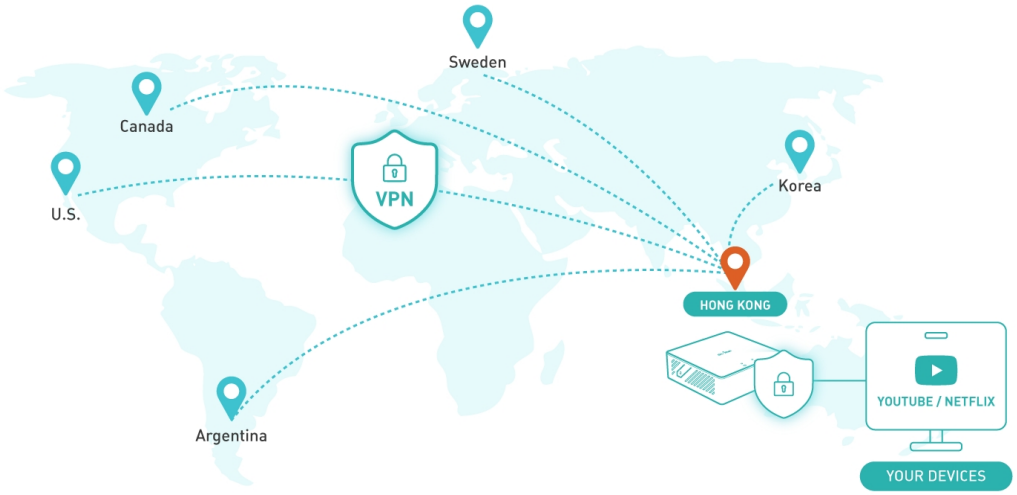
1. **Schutz persönlicher Daten**

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



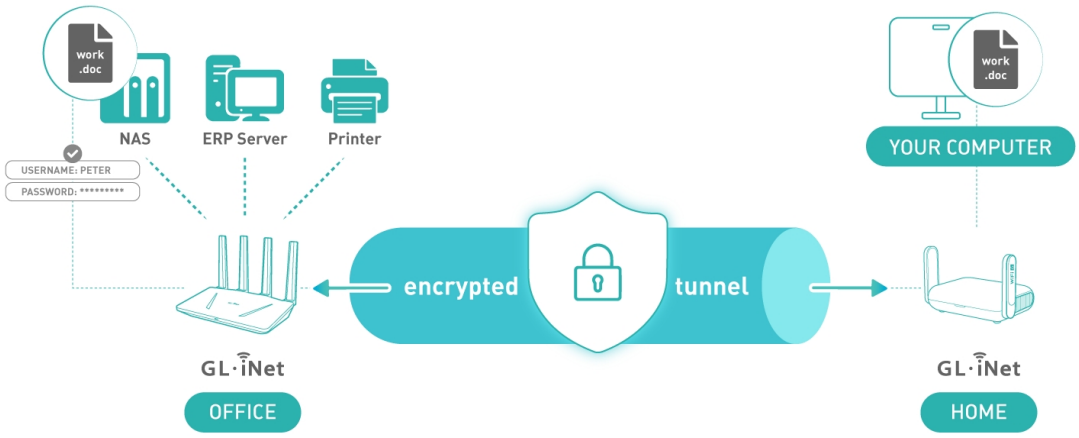
2. **Weltweiter Zugriff ohne Einschränkungen**

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


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

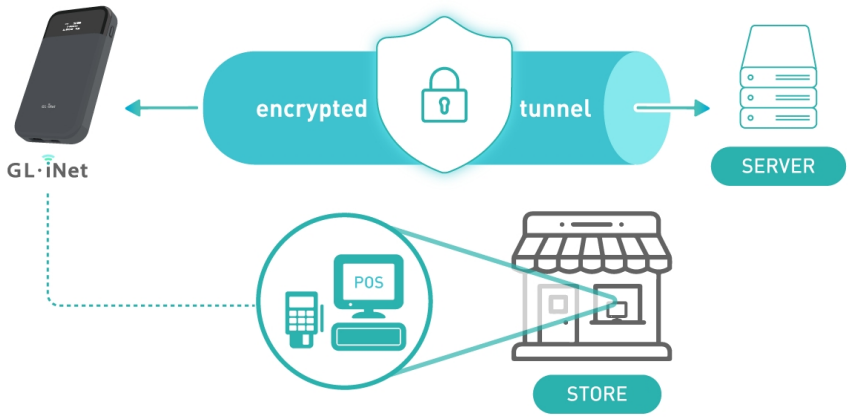
3. **Datensicherheit für kleine Unternehmen**

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



4. **Sichere Zahlungsabwicklung**

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



Kapitel 9

VPN-Dashboard

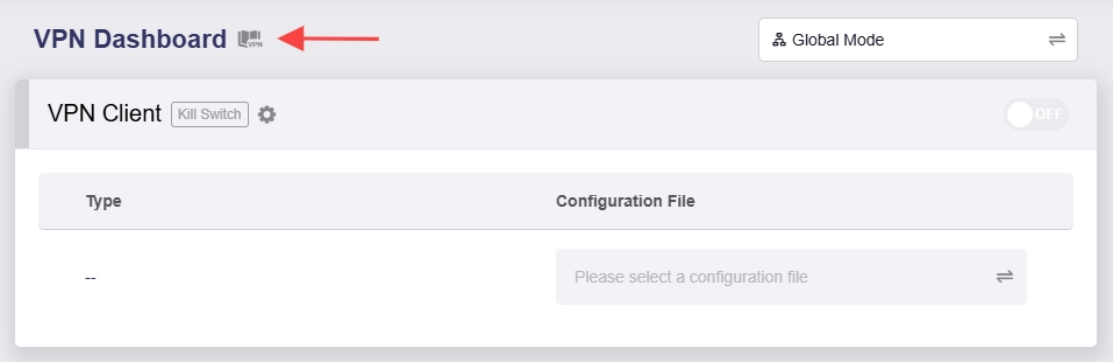
Dieses Kapitel beschreibt die Verwaltung von VPN-Verbindungen über die Weboberfläche.

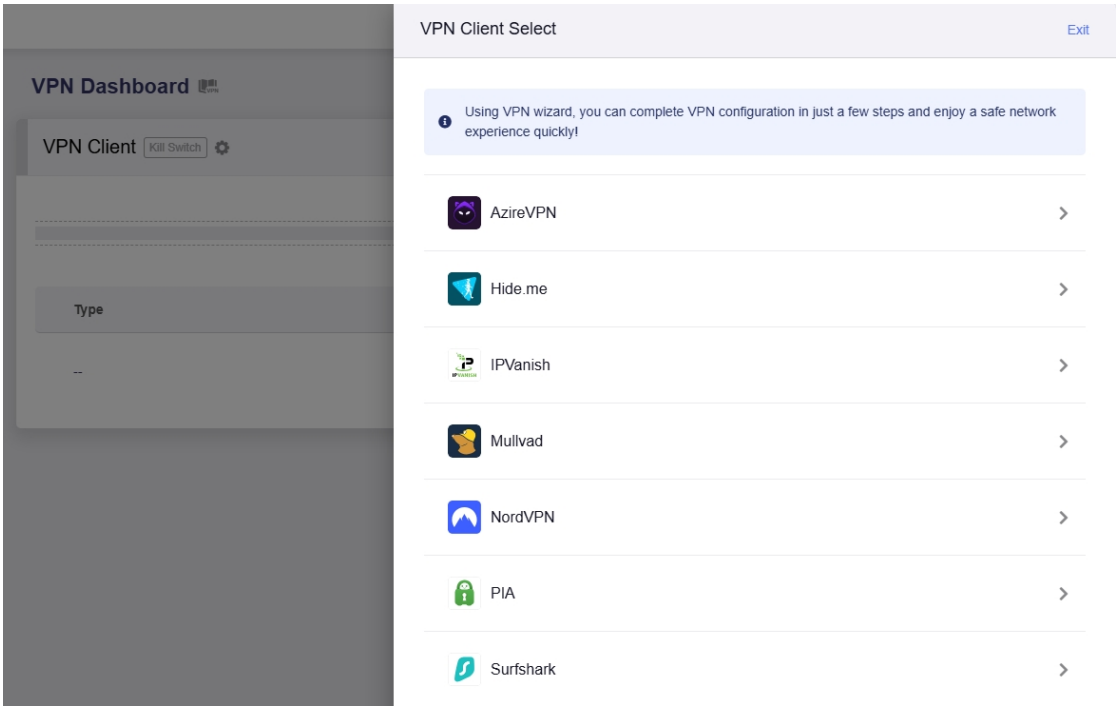
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **VPN Dashboard**.

Das VPN-Dashboard zeigt Verbindungsdetails wie Tunnelregeln, Serveradresse, Datenverkehrsstatistiken, virtuelle Client-IP-Adresse und Verbindungsprotokoll an. Außerdem können Sie erweiterte Einstellungen wie VPN-Kill-Switch, IP-Masquerading und MTU konfigurieren. Für Szenarien mit mehreren Tunneln können Sie auch mehrere VPN-Verbindungen aktivieren.

9.1 VPN-Einrichtungsassistent

Klicken Sie zunächst oben links auf das Buchsymbol und folgen Sie dem VPN-Einrichtungsassistenten, um die VPN-Konfiguration schnell abzuschließen.



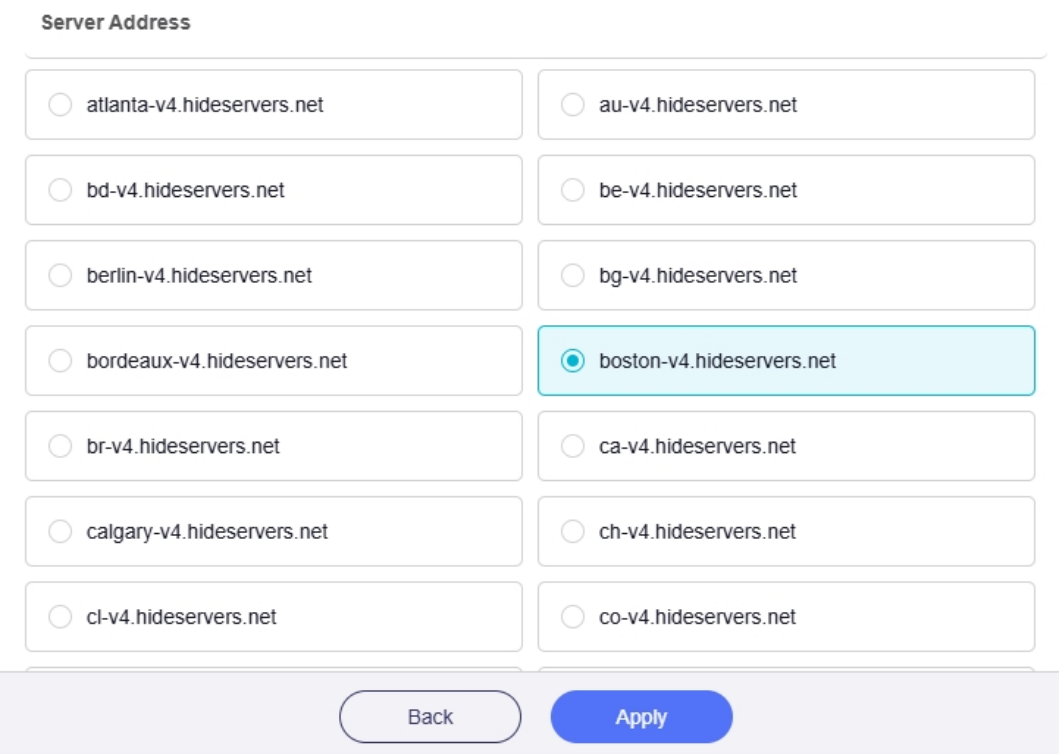


Hinweis: Der VPN-Einrichtungsassistent unterstützt nur die integrierten VPN-Dienste AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA und Surfshark. Bei anderen VPN-Anbietern überspringen Sie den Assistenten und öffnen **VPN** > **OpenVPN Client** oder **WireGuard Client**, um das VPN manuell einzurichten.

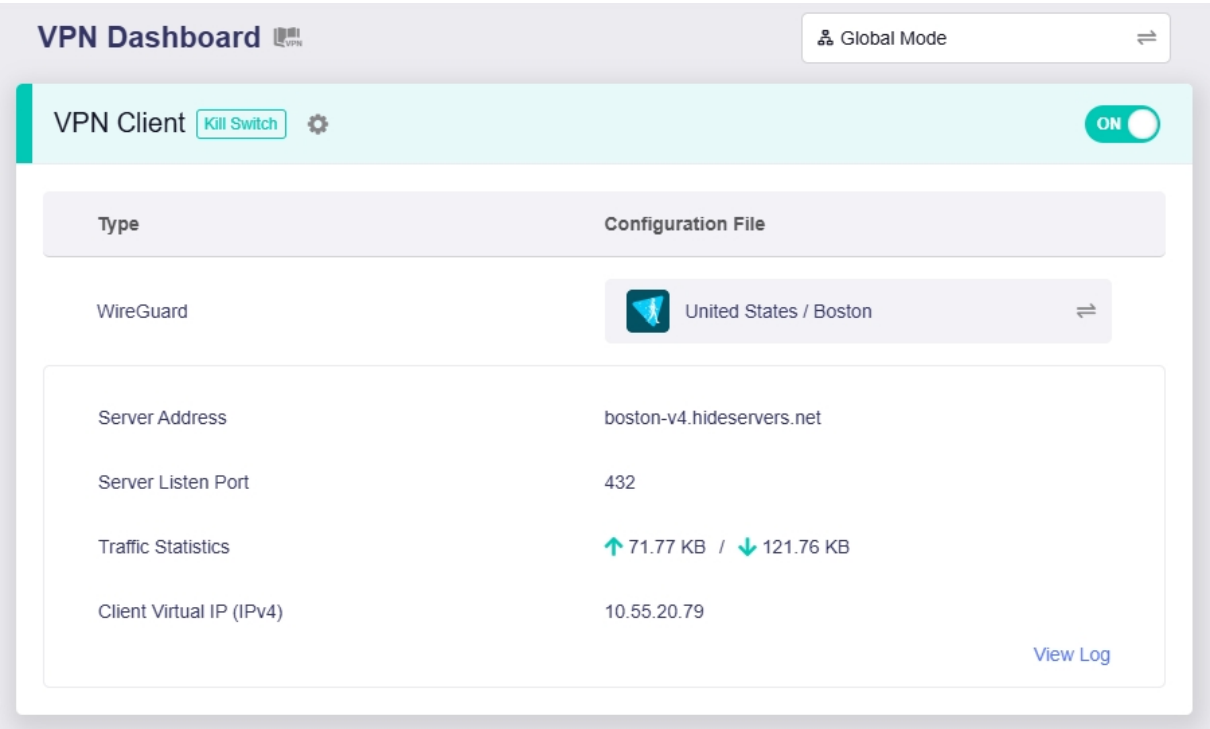
Das folgende Beispiel verwendet **Hide.me**. Melden Sie sich mit Ihren Hide.me-Zugangsdaten an.



Wählen Sie einen VPN-Server aus und klicken Sie auf **Apply**. Zu diesem Server wird die Verbindung hergestellt. Ihre öffentliche IP-Adresse erscheint dann so, als befänden Sie sich am Standort des ausgewählten Servers.

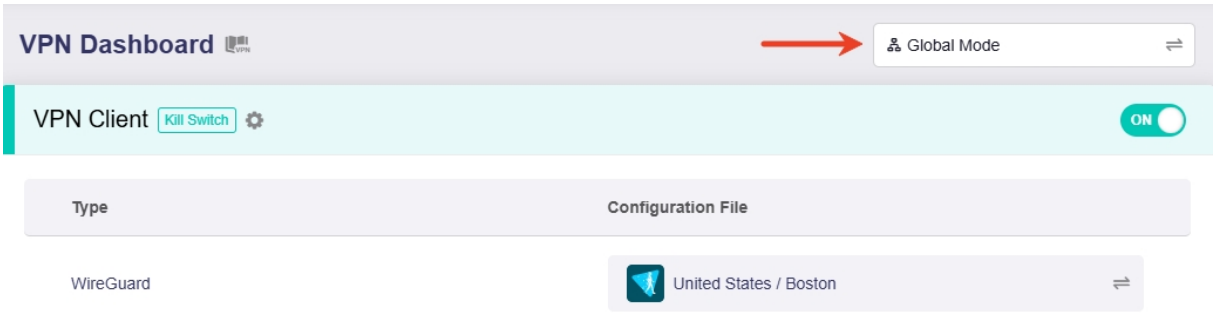


Die Verbindung wird automatisch hergestellt. Öffnen Sie anschließend das **VPN Dashboard**. Dort sehen Sie den aktivierten VPN-Tunnel mit Angaben zu VPN-Protokoll (z. B. WireGuard), Konfigurationsdatei, Serveradresse, Serverport, Datenverkehrsstatistiken und virtueller Client-IP -Adresse. Unten rechts können Sie außerdem die Verbindungsprotokolle einsehen.

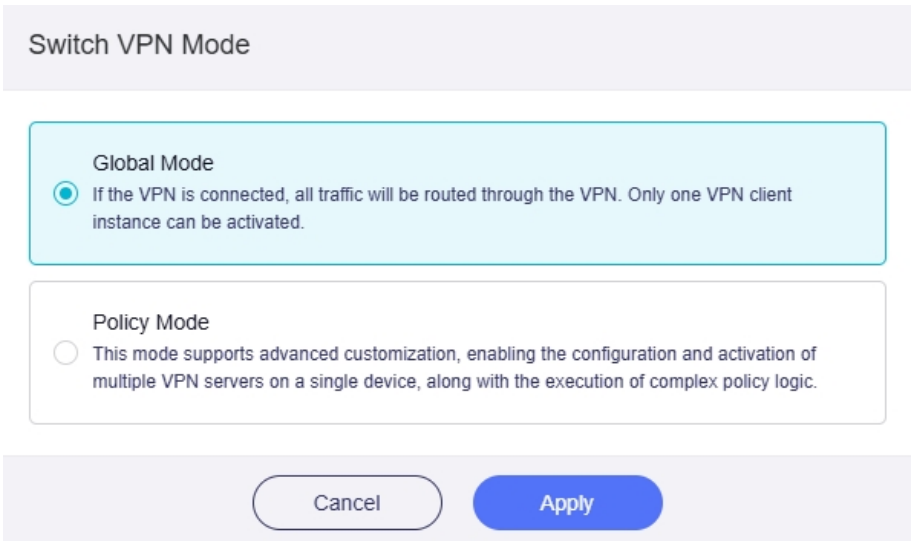


9.2 VPN-Modus

Klicken Sie bei Bedarf im VPN-Dashboard oben rechts auf die Schaltfläche zum Wechseln des VPN-Modus.



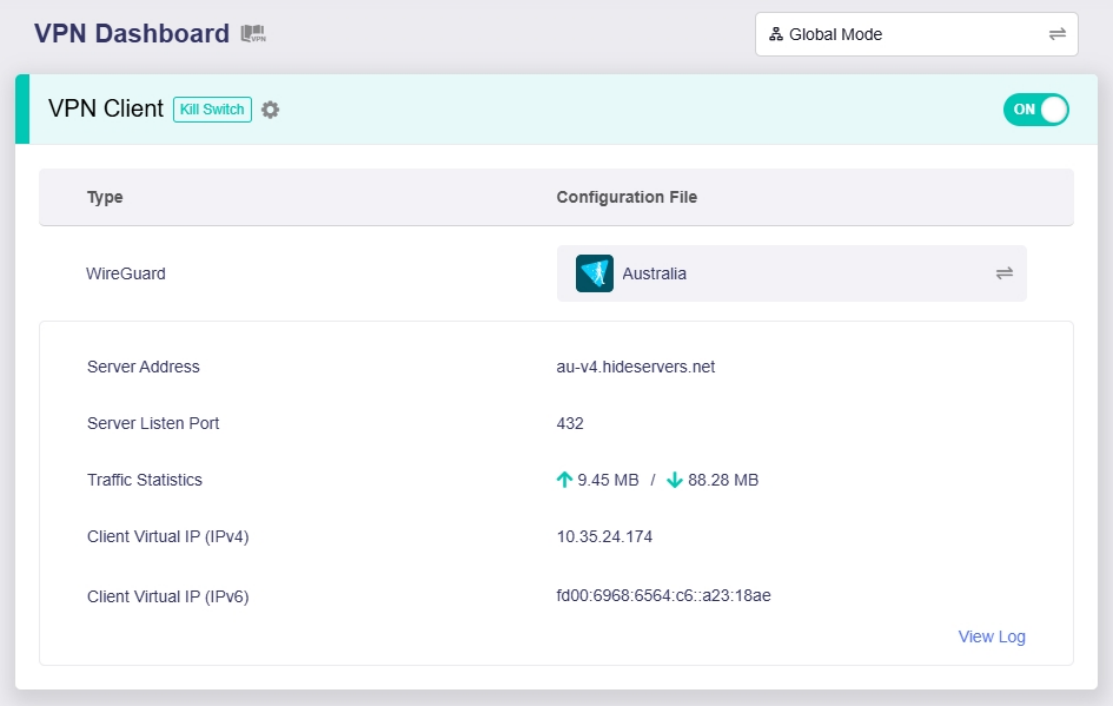
Es stehen zwei Modi zur Verfügung: **Global Mode** und **Policy Mode**.



9.2.1 Globaler Modus

In diesem Modus wird der gesamte Datenverkehr durch den VPN-Tunnel geleitet. Es kann nur eine VPN-Client-Instanz aktiviert werden. Dieser Modus eignet sich, wenn der gesamte Geräteverkehr einen einzigen VPN-Server nutzen soll, beispielsweise für einheitliche Netzwerksicherheit oder den Zugriff auf regionsgebundene Inhalte.

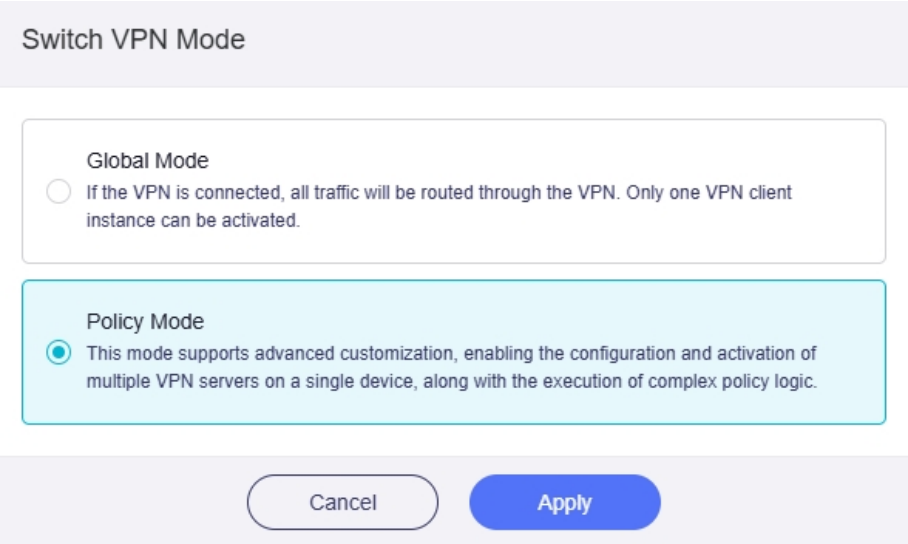
Im folgenden Beispiel verbindet sich der Router über das WireGuard-Protokoll mit einem australischen Server. Der gesamte Datenverkehr der verbundenen Endgeräte wird durch diesen VPN-Tunnel geleitet.



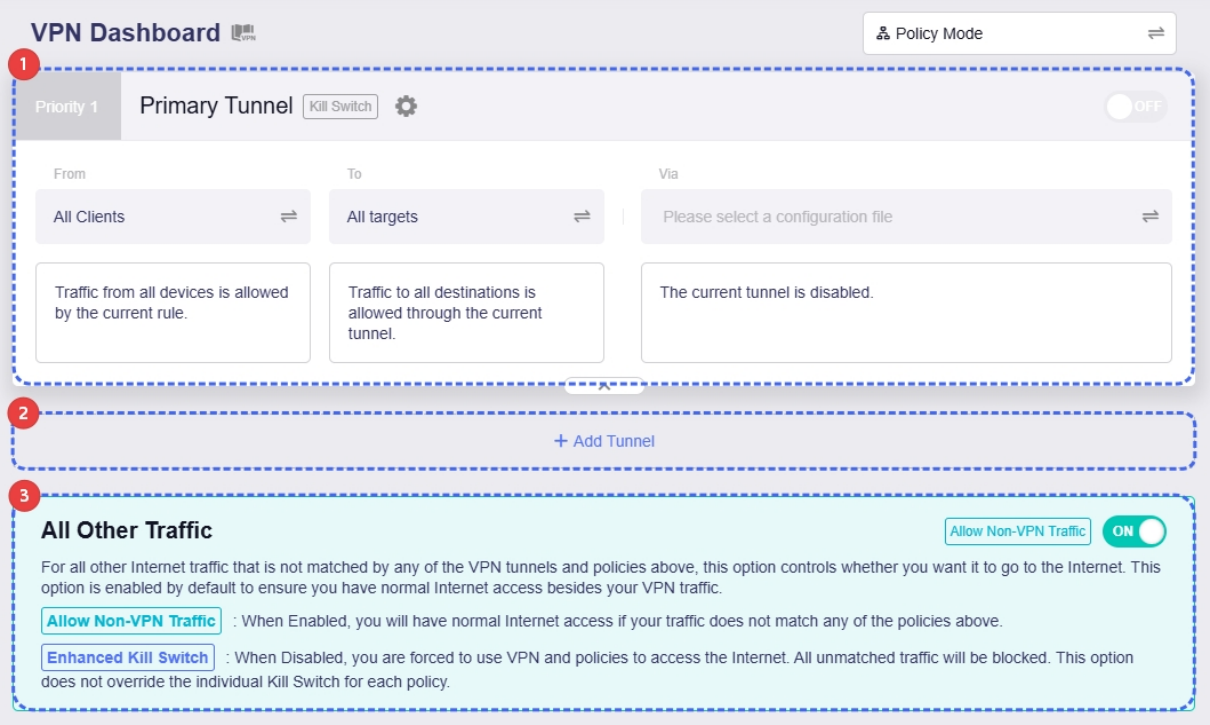
9.2.2 Richtlinienmodus

In diesem Modus können Sie einen einzelnen Router mit mehreren VPN-Servern verbinden und individuelle VPN-Regeln festlegen. Er eignet sich für eine flexible Verkehrssteuerung, beispielsweise um unterschiedliche Datenströme über mehrere VPN-Server an verschiedene Ziele zu leiten.

Stellen Sie den VPN-Modus auf **Policy Mode** und klicken Sie auf **Apply**.



Wenn das VPN nach dem Wechsel nicht aktiviert ist, erscheint die unten gezeigte Seite mit drei Bereichen: **Primary Tunnel**, **Add Tunnel** und **All Other Traffic**.

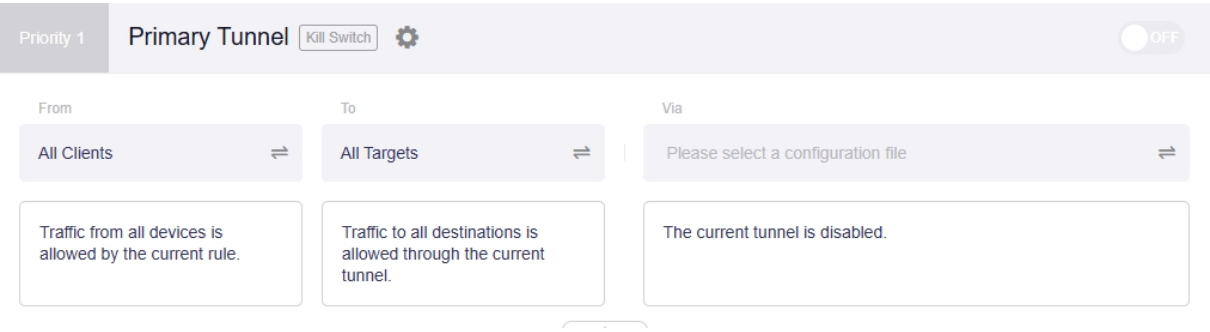


9.2.2.1 Primärer Tunnel

Der primäre Tunnel ist im Richtlinienmodus bereits vorgegeben. Er hat standardmäßig die höchste Priorität. Wenn mehrere Tunnel konfiguriert sind, können Sie seine Priorität ändern.

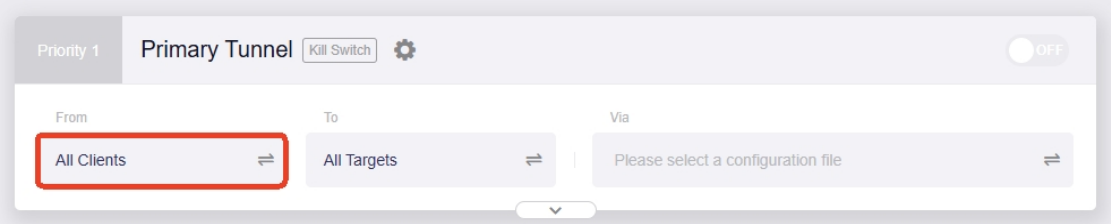
Für die Tunnelregel können Sie drei Merkmale festlegen:

- **From**: Quelle des Datenverkehrs, also der Verkehr, der durch diesen Tunnel geleitet werden soll.
- **To**: Ziel des Datenverkehrs, an das der Verkehr durch diesen Tunnel geleitet wird.
- **Via**: Weiterleitungsmethode, also ob das VPN verwendet werden soll.

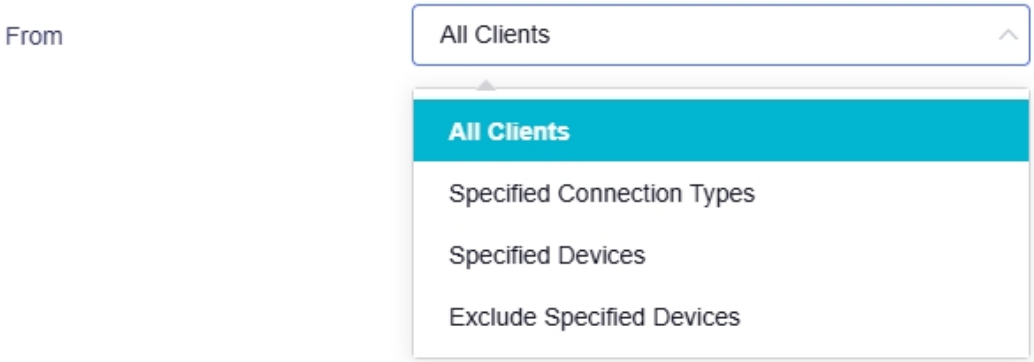


Gehen Sie wie folgt vor, um die Tunnelregel zu konfigurieren.

1. Klicken Sie auf das linke ausgegraute Feld.

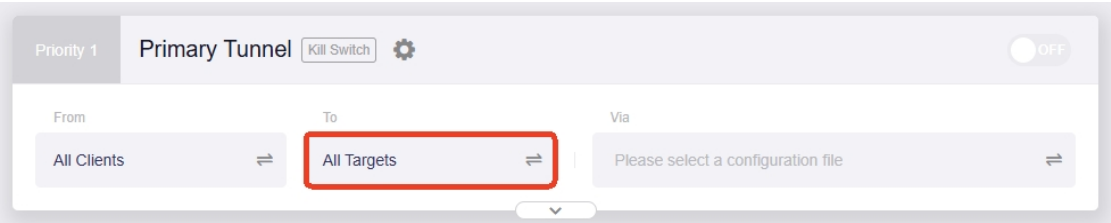


2. Wählen Sie die Geräte aus, auf die diese Regel zutreffen soll, und klicken Sie auf **Apply**.

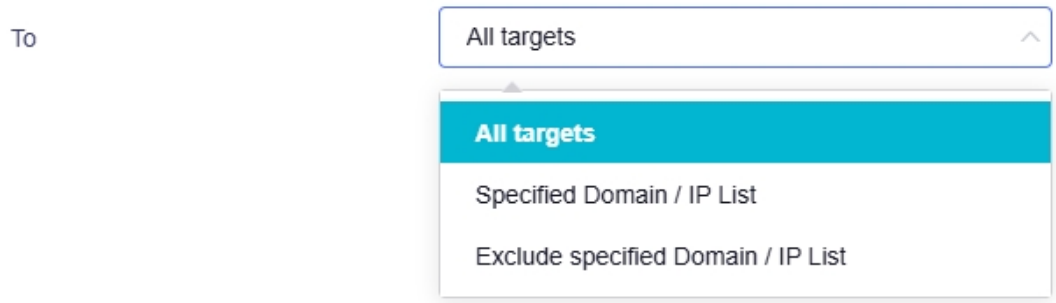


- **All Clients**: Die Regel gilt für den Datenverkehr aller Geräte.
- **Specified Connection Types**: Die Regel gilt für den Datenverkehr bestimmter Verbindungstypen, beispielsweise LAN-Subnetz, Drop-in Gateway oder Gastnetzwerk.
- **Specified Devices**: Die Regel gilt für den Datenverkehr bestimmter, anhand ihrer MAC -Adresse identifizierter Geräte.
- **Exclude Specified Devices**: Die Regel gilt **NICHT** für den Datenverkehr der angegebenen, anhand ihrer MAC-Adresse identifizierten Geräte.

3. Klicken Sie auf das mittlere ausgegraute Feld.



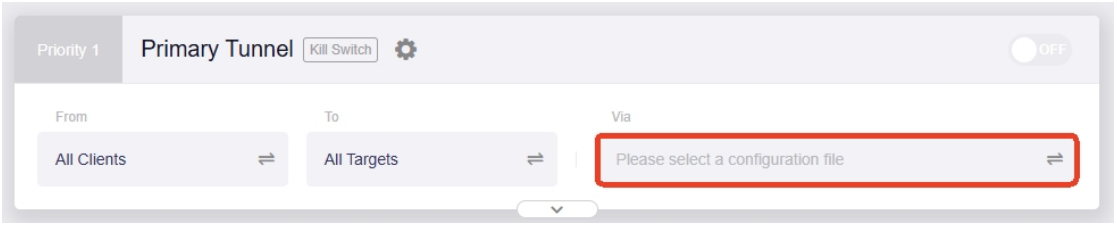
4. Wählen Sie das Ziel aus, an das der Datenverkehr durch diesen Tunnel geleitet werden soll, und klicken Sie auf **Apply**.



- **All Targets**: Der dieser Regel entsprechende Datenverkehr wird an alle Ziele geleitet.
- **Specified Domain / IP List**: Der dieser Regel entsprechende Datenverkehr wird an die angegebenen Domains bzw. IP-Adressen geleitet. Geben Sie die Domains/IP-Adressen manuell ein oder tragen Sie die Abonnement-URL ein. Die Angabe einer Hauptdomain schließt alle ihre Subdomains ein.
- **Exclude specified Domain / IP List**: Der dieser Regel entsprechende Datenverkehr wird **NICHT** an die angegebenen Domains bzw. IP-Adressen geleitet. Geben Sie die Domains/IP-Adressen manuell ein oder tragen Sie die Abonnement-URL ein. Die Angabe einer Hauptdomain schließt alle ihre Subdomains ein.

Hinweis: Wenn Sie Subscribe URL wählen, werden die über die URL bereitgestellten Domainnamen oder IP-Adressen täglich automatisch aktualisiert. Achten Sie auf eine korrekte URL. Die URL-Prüfung prüft die Gültigkeit der Domainnamen bzw. IP-Adressen.

5. Klicken Sie auf das rechte ausgegraute Feld.

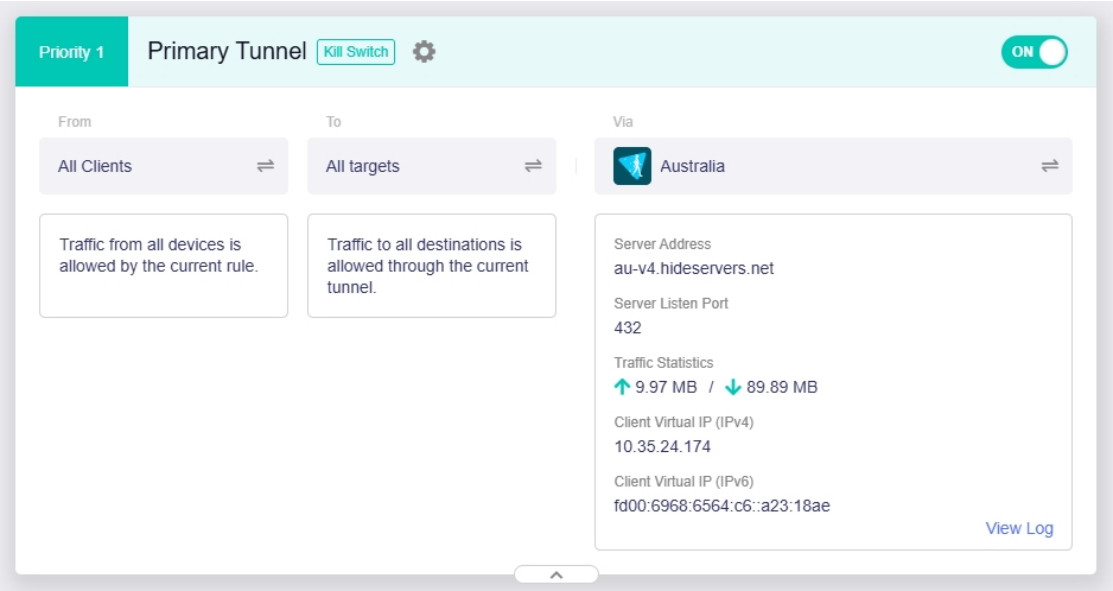


6. Wählen Sie die Weiterleitungsmethode für diesen Tunnel: **Use VPN** oder **Not Use VPN**.



- **Use VPN**: Der dieser Regel entsprechende Datenverkehr wird durch den VPN-Tunnel an die ausgewählten Ziele geleitet. Für diese Regel müssen Sie eine VPN-Konfigurationsdatei auswählen.
- **Not Use VPN**: Der dieser Regel entsprechende Datenverkehr wird über die lokale WAN-Verbindung an die ausgewählten Ziele geleitet.

7. Nachdem Sie Quelle, Ziel und Weiterleitungsmethode festgelegt haben, ist die Regel für den primären Tunnel eingerichtet. Im folgenden Beispiel lautet die Regel: Alle mit diesem Router verbundenen Endgeräte nutzen das VPN für den Internetzugang. Ihr Datenverkehr wird durch diesen VPN-Tunnel an den australischen Server geleitet und gelangt von dort ins Internet.



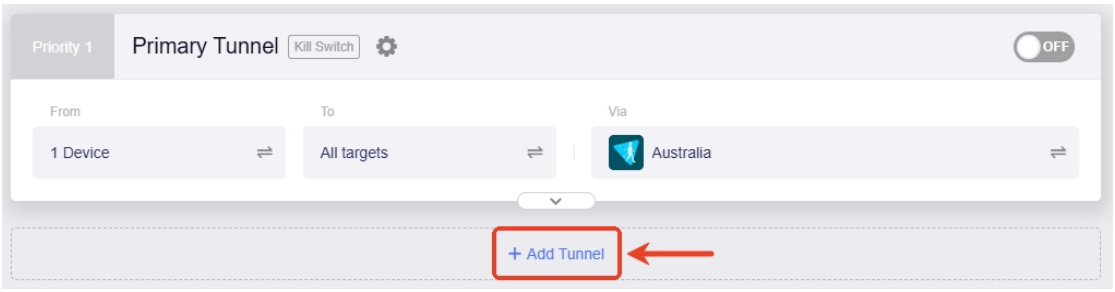
Hinweis: Prüfen Sie aus Sicherheitsgründen vor der Aktivierung dieses Tunnels die weiteren Einstellungen unter **9.2.2.3 Gesamter übriger Datenverkehr** und **9.2.2.4 Tunneloptionen**.

9.2.2.2 Tunnel hinzufügen

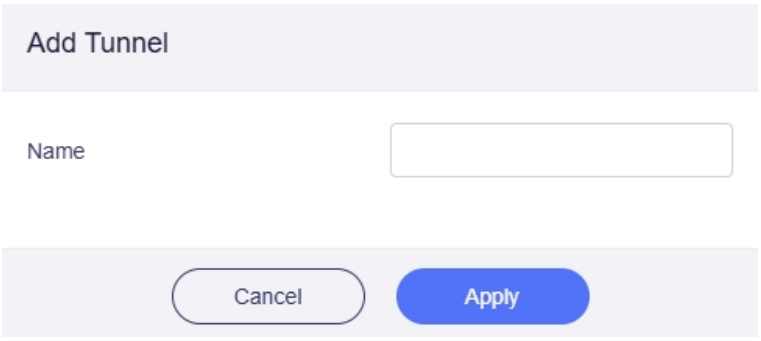
Fügen Sie weitere Tunnel hinzu, wenn Sie den Datenverkehr verschiedener Geräte an unterschiedliche Ziele leiten möchten.

Gehen Sie wie folgt vor, um einen Tunnel hinzuzufügen.

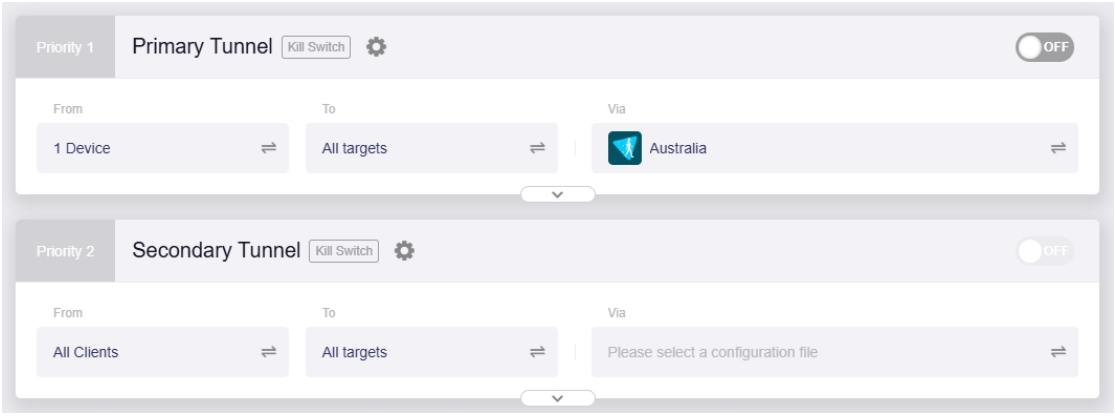
1. Klicken Sie unter dem primären Tunnel auf **Add Tunnel**.



2. Geben Sie dem Tunnel einen Namen.



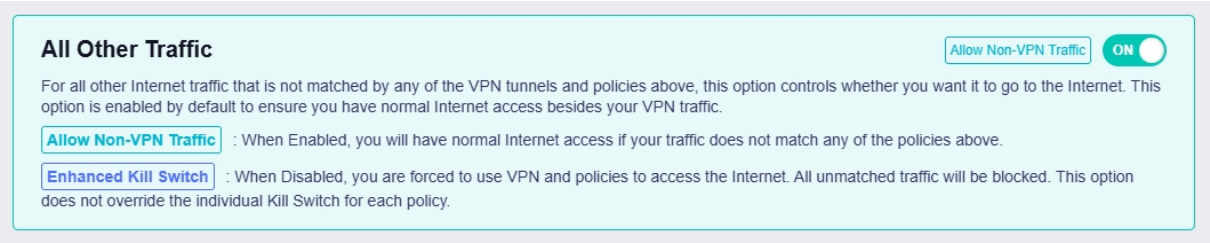
3. Im VPN-Dashboard wird ein weiterer Tunnel angezeigt. Sie können bis zu fünf Tunnel einschließlich des vorgegebenen primären Tunnels erstellen.



4. Konfigurieren Sie die Tunnelregeln, indem Sie Datenquelle, Ziele und Routingmethode festlegen. Prüfen Sie anschließend vor der Aktivierung dieses Tunnels die weiteren Einstellungen unter **9.2.2.3 Gesamter übriger Datenverkehr** und **9.2.2.4 Tunneloptionen**.

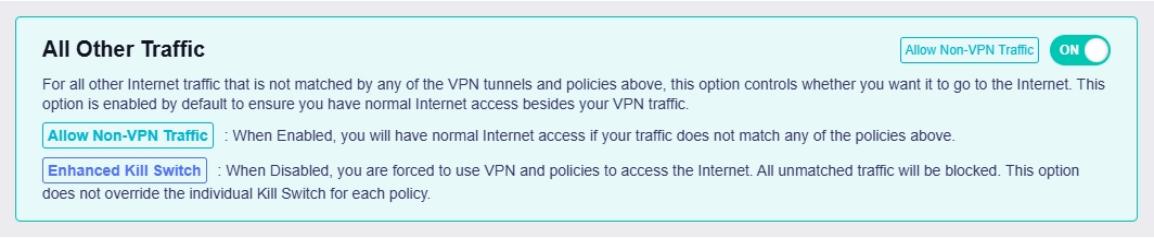
9.2.2.3 Sonstiger Datenverkehr

Im Richtlinienmodus wird unten im VPN-Dashboard ein standardmäßig aktivierter Tunnel angezeigt.

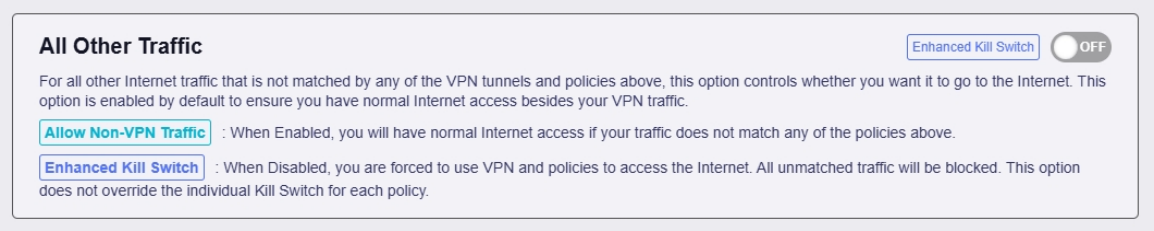


Dieser Tunnel steuert, ob Datenverkehr, auf den keine der darüberstehenden VPN-Tunnelgruppen zutrifft, auf das Internet zugreifen darf. Er ist standardmäßig aktiviert, um den normalen Internetzugang für Datenverkehr außerhalb des VPN zu gewährleisten.

- Bei aktiviertem Tunnel kann Datenverkehr, der keiner Regel entspricht, weiterhin auf das Internet zugreifen.

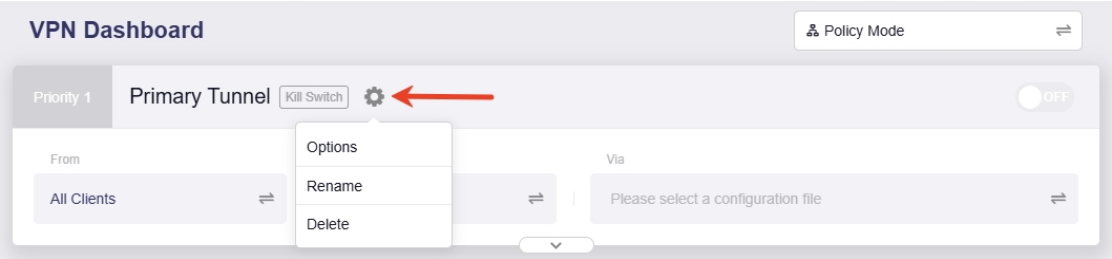


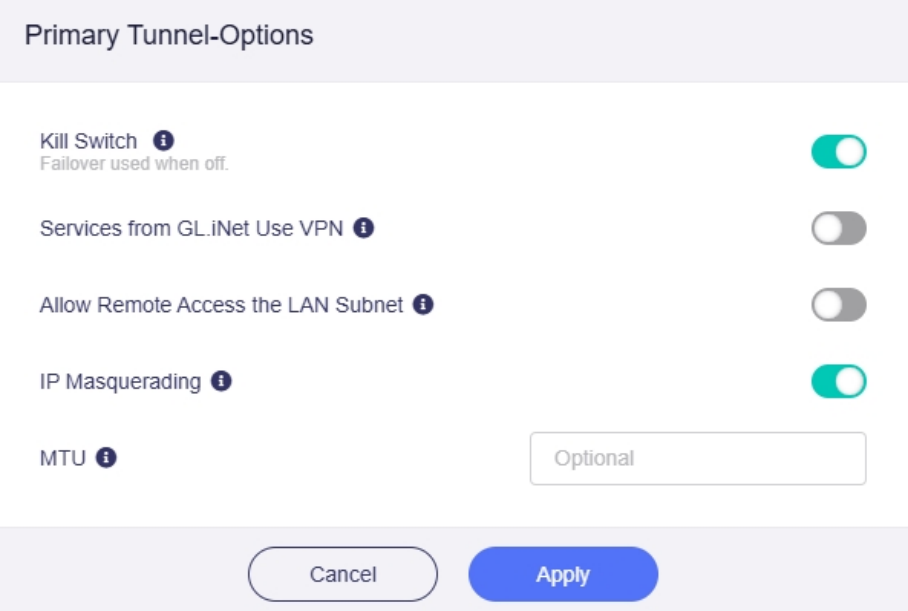
- Bei deaktiviertem Tunnel darf nur durch das VPN geleiteter Datenverkehr auf das Internet zugreifen. Der gesamte übrige Datenverkehr sowie bei einem VPN-Ausfall umgeleiteter Verkehr werden gesperrt. Diese Option setzt den individuellen Kill-Switch der einzelnen VPN-Tunnel nicht außer Kraft.



9.2.2.4 Tunneloptionen

Für jeden VPN-Tunnel können Sie erweiterte Einstellungen wie VPN-Kill-Switch, IP-Masquerading und MTU konfigurieren. Klicken Sie dazu auf das Zahnradsymbol neben dem Tunnelnamen.





- **Kill Switch**: Bei aktivierter Option wird der diesem VPN-Tunnel zugeordnete Datenverkehr gesperrt, wenn die Verbindung unerwartet ausfällt. Andernfalls wird er an Tunnel mit niedrigerer Priorität oder an das WAN übergeben.
- **Services from GL.iNet Use VPN**: Bei aktivierter Option übertragen GoodCloud, DDNS und rtty ihre Pakete durch VPN-Tunnel. Die Option ist standardmäßig deaktiviert, da diese Dienste für den ordnungsgemäßen Betrieb normalerweise die tatsächliche IP-Adresse des Geräts benötigen.
- **Allow Remote Access the LAN Subnet**: Bei aktivierter Option ist der Fernzugriff über das VPN auf diesen Router (Tunnel-IP-Adresse) und auf LAN-Geräte zulässig. Dafür muss der VPN-Server eine Rückroute zum LAN-Subnetz dieses Routers bekannt geben.

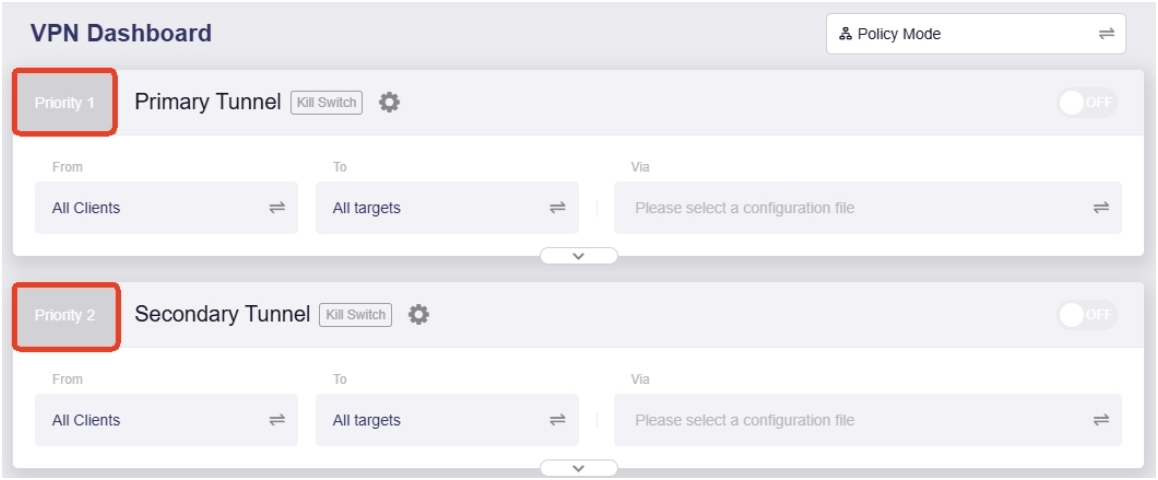
- **IP Masquerading**: Bei aktivierter Option werden die Quell-IP-Adressen der LAN-Endgeräte durch die VPN-Tunnel-IP-Adresse des Routers ersetzt. Deaktivieren Sie die Option nur für Standortverbindungen (Site-to-Site), bei denen die Gegenstelle Ihre LAN-Subnetze kennt.
- **MTU**: Der für den Tunnel eingestellte MTU-Wert überschreibt den MTU-Eintrag in der Konfigurationsdatei.

9.2.2.5 Tunnelpriorität

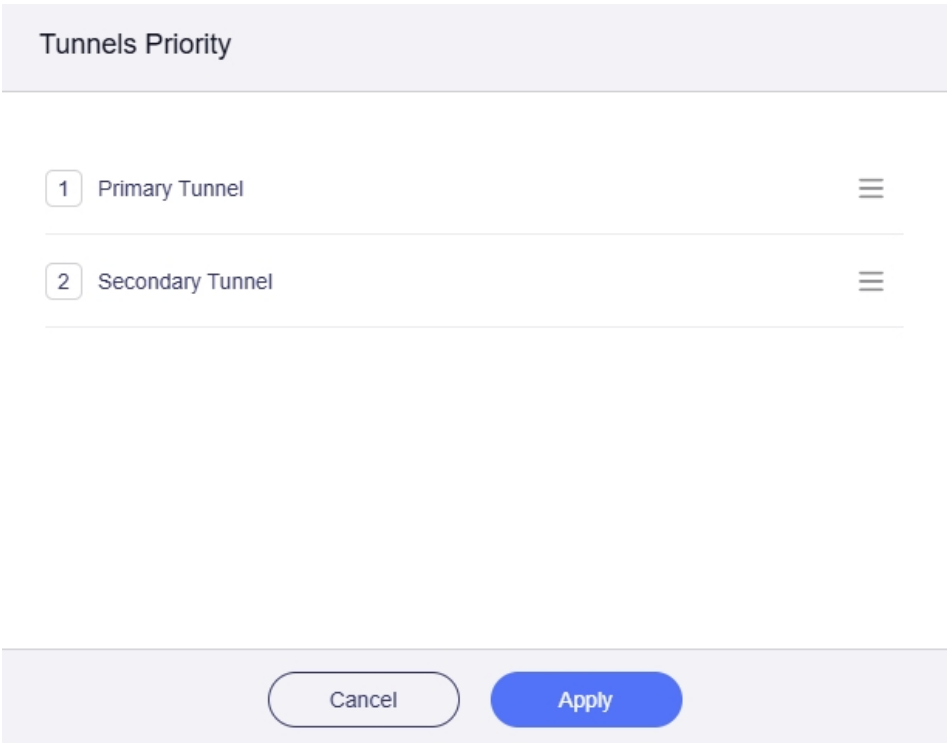
Standardmäßig hat der vorgegebene primäre Tunnel die höchste Priorität. Darauf folgen gegebenenfalls manuell hinzugefügte Tunnel und zuletzt der vorgegebene Tunnel „All Other Traffic“, der die Verbindung über das lokale Netz des Internetanbieters (WAN) sicherstellt.

Gehen Sie wie folgt vor, um die Tunnelpriorität zu ändern.

1. Klicken Sie oben links in einem beliebigen Tunnel auf die Prioritätsangabe, beispielsweise Priority 1 oder Priority 2.



2. Halten Sie im eingeblendeten Fenster das Symbol mit den drei Linien rechts gedrückt und ziehen Sie den Tunnel an die gewünschte Position. Klicken Sie anschließend auf **Apply**.



Wenn mehrere Tunnel aktiviert sind, leitet der Router den Datenverkehr in folgender Reihenfolge weiter:

1. Zunächst wird geprüft, ob der Datenverkehr der Tunnelregel mit der höchsten Priorität entspricht. Falls ja, wird er durch diesen Tunnel geleitet. Andernfalls wird die Regel des nächsten Tunnels geprüft. Dies wird bis zum Tunnel „All Other Traffic“ fortgesetzt.
2. Wenn ein VPN-Tunnel unerwartet getrennt wird, bestimmt dessen **Kill-Switch**, ob der Datenverkehr an den Tunnel mit der nächstniedrigeren Priorität übergeben wird.
   - Bei aktiviertem Kill-Switch wird der Datenverkehr gesperrt und nicht an den nächsten Tunnel übergeben.
   - Bei deaktiviertem Kill-Switch wird der Datenverkehr an den nächsten Tunnel übergeben und anhand dessen Tunnelregeln geprüft.
3. Der Tunnel **All Other Traffic** ist standardmäßig aktiviert, damit Datenverkehr, der keinem VPN-Tunnel entspricht, weiterhin auf das Internet zugreifen kann.
   - Bei aktiviertem Tunnel wird nicht zugeordneter oder bei einem Ausfall übergebener Datenverkehr über die lokale WAN-Verbindung geleitet.
   - Bei deaktiviertem Tunnel wird die Schutzwirkung des Kill-Switch verstärkt und der reguläre Internetzugang gesperrt, um die Offenlegung der IP-Adresse zu verhindern.

Kapitel 10

VPN-Server einrichten

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

10.1 OpenVPN-Server

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.

10.1.1 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:

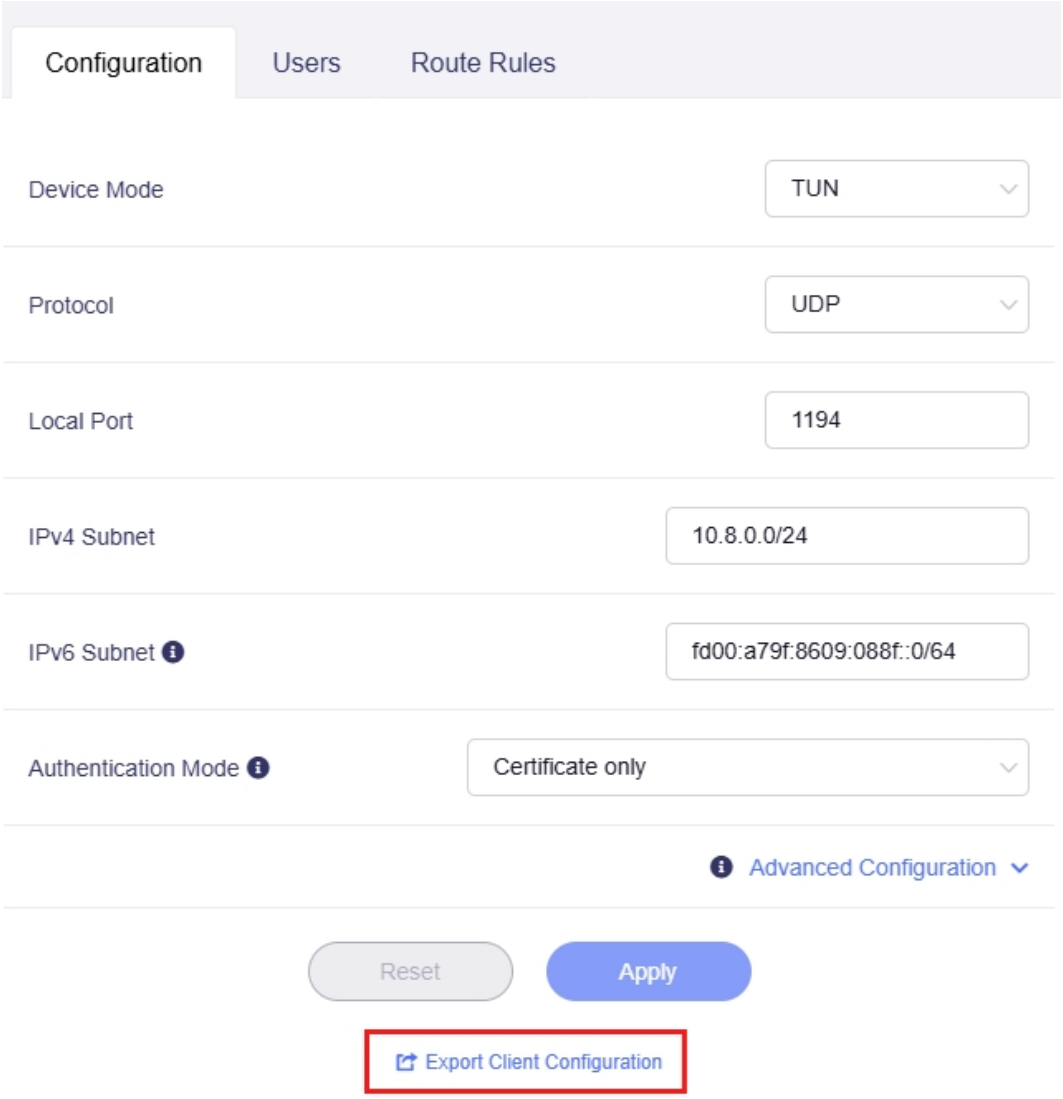
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.
   - Wenn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

10.1.2 Einrichtung

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



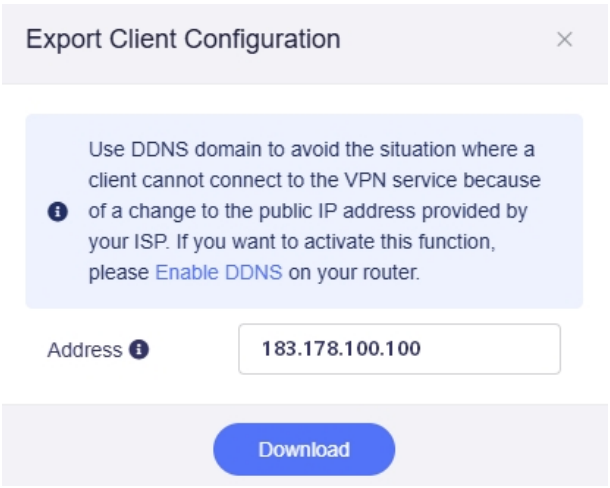
- **Device Mode**: TAP-S2S oder Tun. Die Unterschiede werden hier erläutert.
- **Protocol**: UDP oder TCP. Die Unterschiede werden hier erläutert.
- **Authentication Mode**: Legt fest, wie sich der Client beim Verbinden mit dem Server authentifiziert. Es gibt drei Optionen:

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

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

3. Client-Konfiguration exportieren.

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

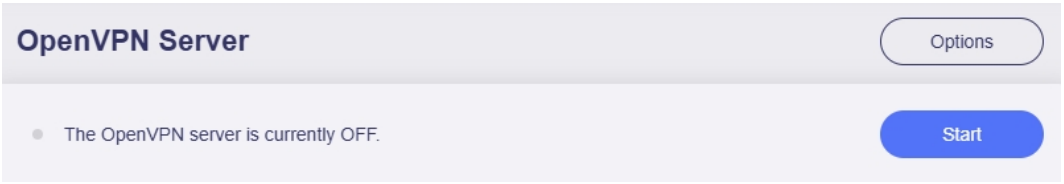


   Tipps:

- Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Anschließend können Sie die DDNS-Domain als Serveradresse verwenden.
- Seit Firmware v4.8 können Sie die Serveradresse vor dem Export der Konfigurationsdatei aus einer Dropdown-Liste auswählen: öffentliche IP-Adresse, DDNS-Domain oder aktuelle WAN-IP-Adresse. Die Serveradresse in der Konfigurationsdatei wird entsprechend automatisch aktualisiert. Laden Sie die Konfigurationsdatei erneut herunter, wenn sich die Serveradresse ändert.

4. OpenVPN-Server starten.

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



   Der Verbindungsstatus des Servers wird oben angezeigt. Wenn Statistiken zum hoch- und heruntergeladenen Datenvolumen erscheinen, läuft der OpenVPN-Server.

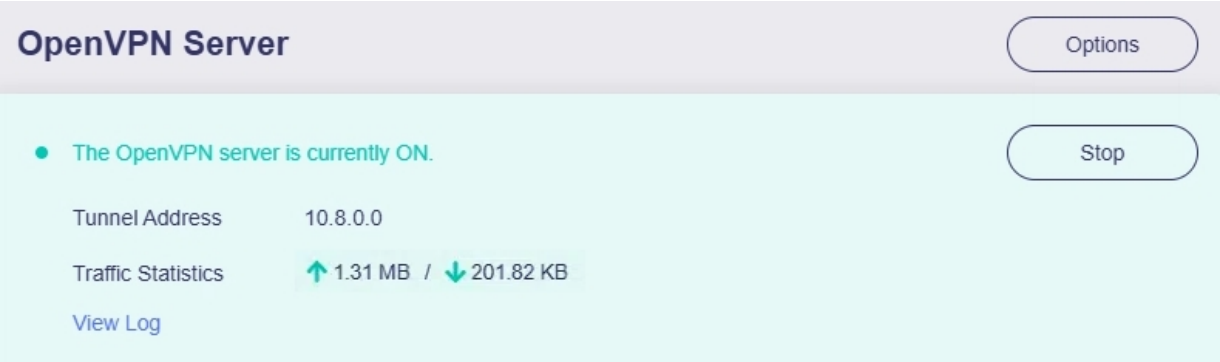


10.1.3 Verbindung prüfen

Methode 1: Serverstatus prüfen

Ab Firmware v4.8 können Sie den Verbindungsstatus des Servers auf der Seite **OpenVPN Server** prüfen.

Wenn Upload- und Downloadstatistiken angezeigt werden, läuft der OpenVPN-Server.



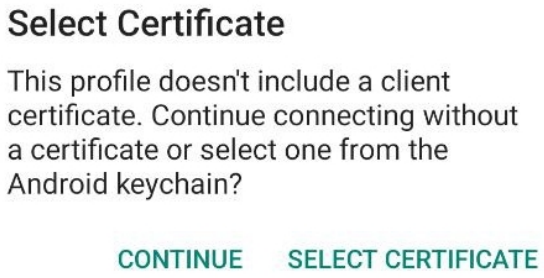
Methode 2: IP-Adresse des Clients prüfen

Importieren Sie die zuvor exportierte OpenVPN-Konfiguration auf ein Gerät in einem anderen Netzwerk als dem lokalen Netzwerk des Servers. Öffnen Sie anschließend einen Webbrowser und ermitteln Sie Ihre IP-Adresse und Ihren Standort. Wenn diese mit der IP-Adresse und dem Standort des VPN-Servers übereinstimmen und nicht mit denen Ihres Internetanbieters, besteht die VPN-Verbindung erfolgreich.

Im folgenden Beispiel erfolgt die Überprüfung mit einem Smartphone, auf dem die offizielle OpenVPN-App installiert ist.

1. Deaktivieren Sie zunächst das WLAN des Smartphones und aktivieren Sie ausschließlich die mobile Datenverbindung (4G/5G).
2. Öffnen Sie anschließend die OpenVPN-App, importieren Sie die Konfigurationsdatei und stellen Sie die Verbindung her.
3. Prüfen Sie, ob das Smartphone Internetzugang hat und seine IP-Adresse mit der des OpenVPN-Servers übereinstimmt.

   Tipp: Beim Importieren der Konfigurationsdatei in die OpenVPN-App wird möglicherweise der folgende Hinweis angezeigt. Klicken Sie auf **CONTINUE**, um fortzufahren, da das Zertifikat bereits in die Konfigurationsdatei eingebettet ist.

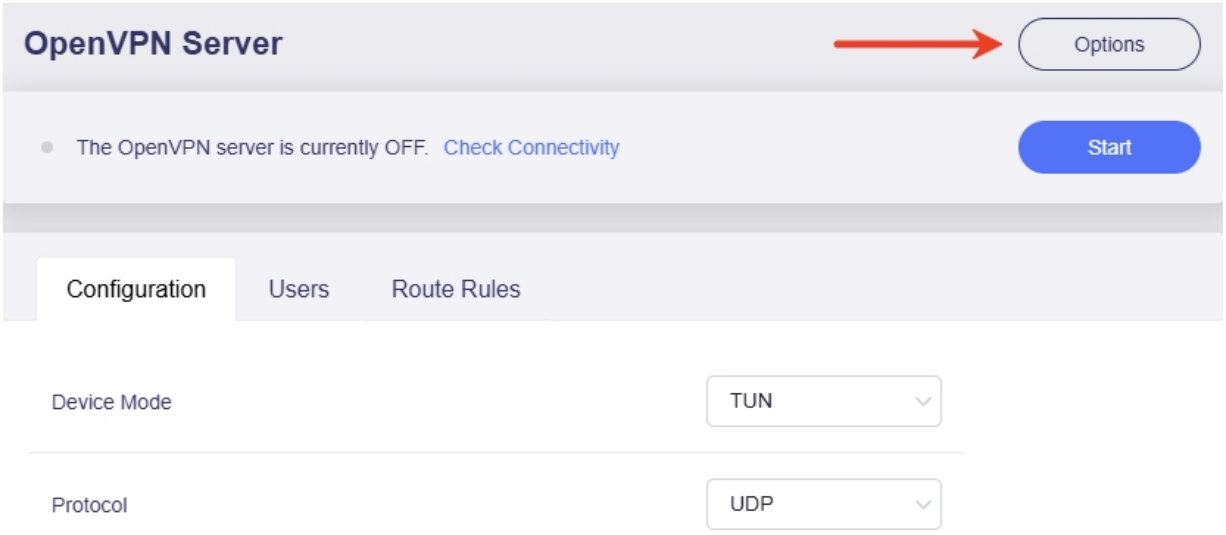


Wenn die Verbindung fehlschlägt, kommen unter anderem folgende Ursachen infrage:

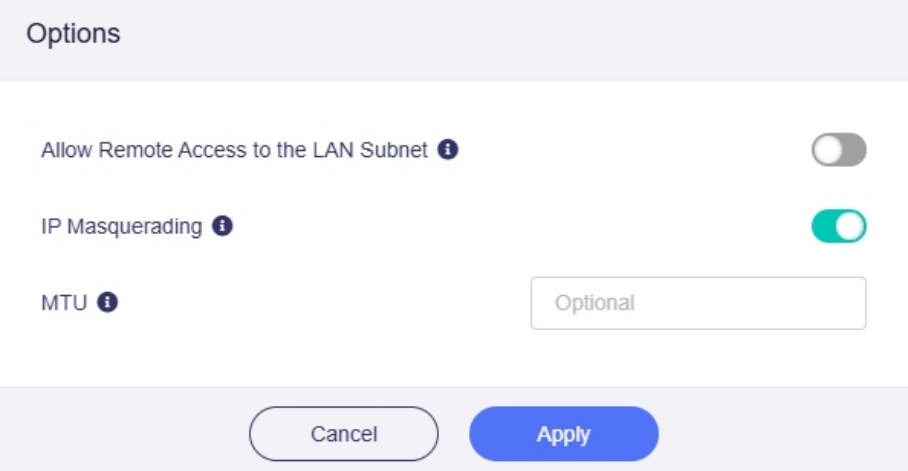
- Der VPN-Server hat keine öffentliche IP-Adresse. Einzelheiten finden Sie unter **10.1.1 Vorbereitung**.
- Möglicherweise müssen Sie eine Portweiterleitung einrichten. Einzelheiten finden Sie unter **10.1.1 Vorbereitung**.
- Ihr Internetanbieter sperrt den vom OpenVPN-Server verwendeten Port. Wechseln Sie zu einem anderen Port oder bitten Sie Ihren Internetanbieter um Unterstützung.
- In bestimmten Ländern oder Regionen kann die VPN-Verbindung gesperrt sein.

10.1.4 Server-Optionen

Die Serveroptionen enthalten erweiterte serverseitige Einstellungen, etwa den Fernzugriff auf das LAN des Servers oder IP-Masquerading. Konfigurieren Sie diese Einstellungen nach Bedarf. Klicken Sie auf der Seite **OpenVPN Server** oben rechts auf **Options**.



Im eingeblendeten Fenster stehen die folgenden Funktionen zur Verfügung.

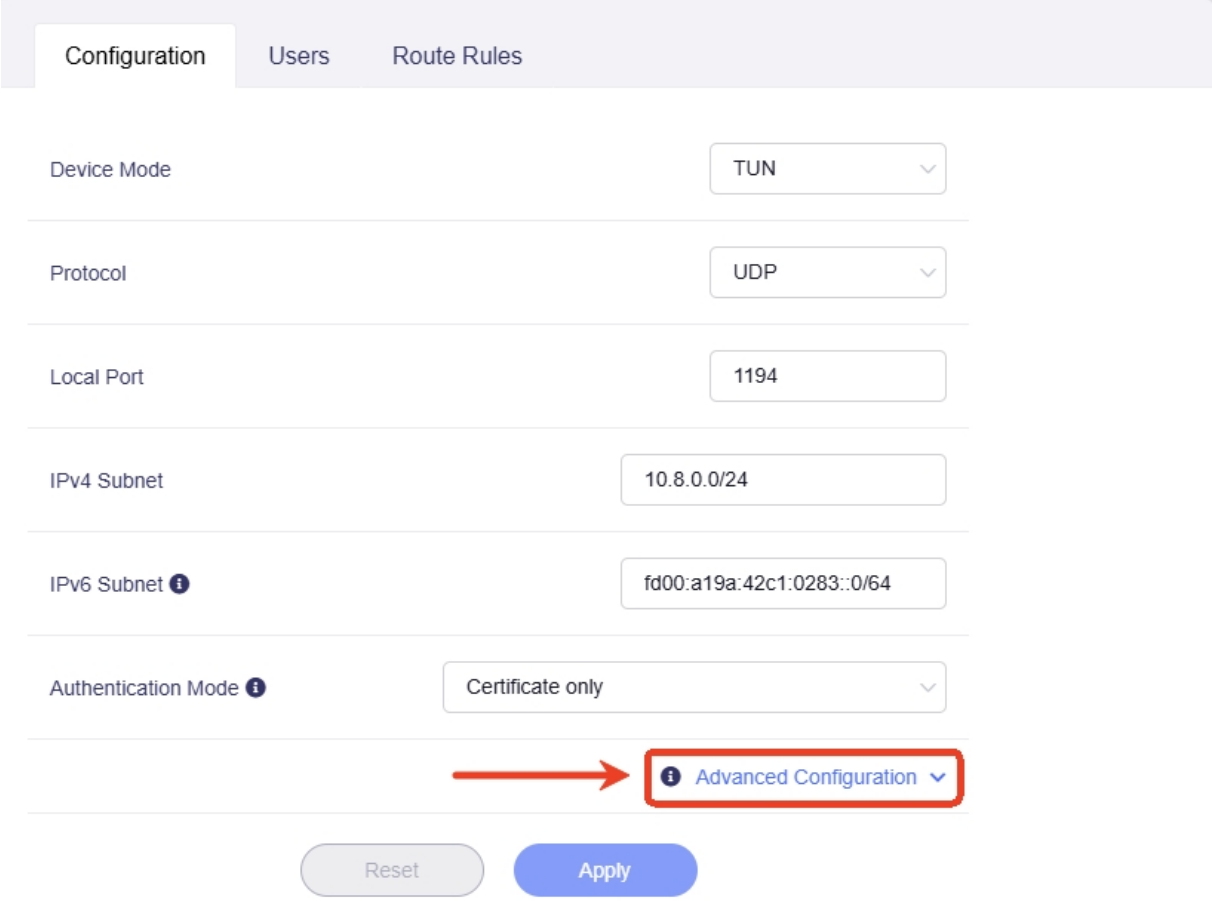


- **Allow Remote Access to the LAN Subnet**: Wenn diese Option aktiviert ist, können Ressourcen im LAN-Subnetz des Servers über den VPN-Tunnel aufgerufen werden.
- **IP Masquerading**: Ersetzt die Quell-IP-Adressen der LAN-Geräte durch die VPN-Tunnel-IP-Adresse des Routers. Deaktivieren Sie diese Option 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.

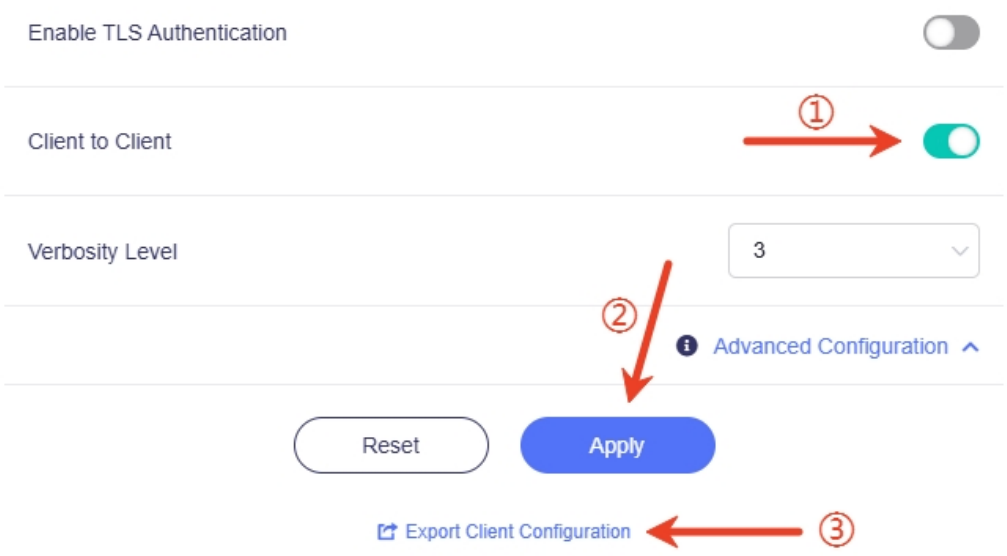
10.1.5 Kommunikation zwischen Clients

Client-to-Client ist eine serverseitige VPN-Funktion. Wenn sie aktiviert ist, können verbundene VPN-Clients über ihre jeweiligen IP-Adressen im VPN-Tunnel miteinander kommunizieren. Führen Sie bei Bedarf die folgenden Schritte aus, um Client to Client auf Ihrem OpenVPN-Server zu aktivieren.

1. Klicken Sie auf der Seite **OpenVPN Server** unten rechts auf **Advanced Configuration**.



2. Aktivieren Sie **Client to Client** und klicken Sie auf **Apply**. Exportieren Sie anschließend eine neue Konfiguration und laden Sie diese auf Ihre OpenVPN-Clients hoch.



Tipp: Client-to-Client gibt lediglich die Tunnel-IP-Adresse jedes Clients bekannt. Die lokalen LAN-Subnetze hinter den einzelnen VPN-Clients werden dadurch nicht automatisch erreichbar. Wenn Clients auf die LAN-Subnetze der jeweils anderen Clients zugreifen sollen, ergänzen Sie auf dem VPN-Server Routingregeln, die diese entfernten LAN-Subnetze bekannt geben.

10.2 WireGuard-Server

WireGuard® ist eine äußerst einfache, schnelle und moderne VPN-Lösung mit aktueller Kryptografie. Sie soll schneller, einfacher, schlanker und praktischer als IPSec sein und dabei dessen Komplexität vermeiden. Gegenüber OpenVPN soll sie eine deutlich höhere Leistung bieten.
*WireGuard® ist eine eingetragene Marke von Jason A. Donenfeld.

Um einen WireGuard-Server auf einem GL.iNet-Router einzurichten, sehen Sie sich dieses Video an oder befolgen Sie die nachstehenden Schritte.

10.2.1 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.

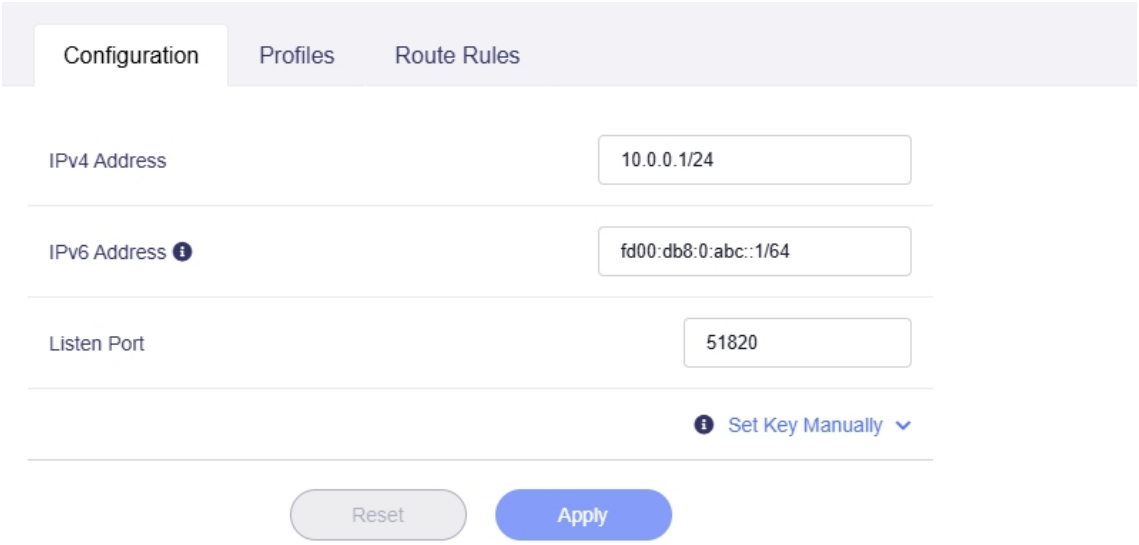
   Alternativen:
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.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

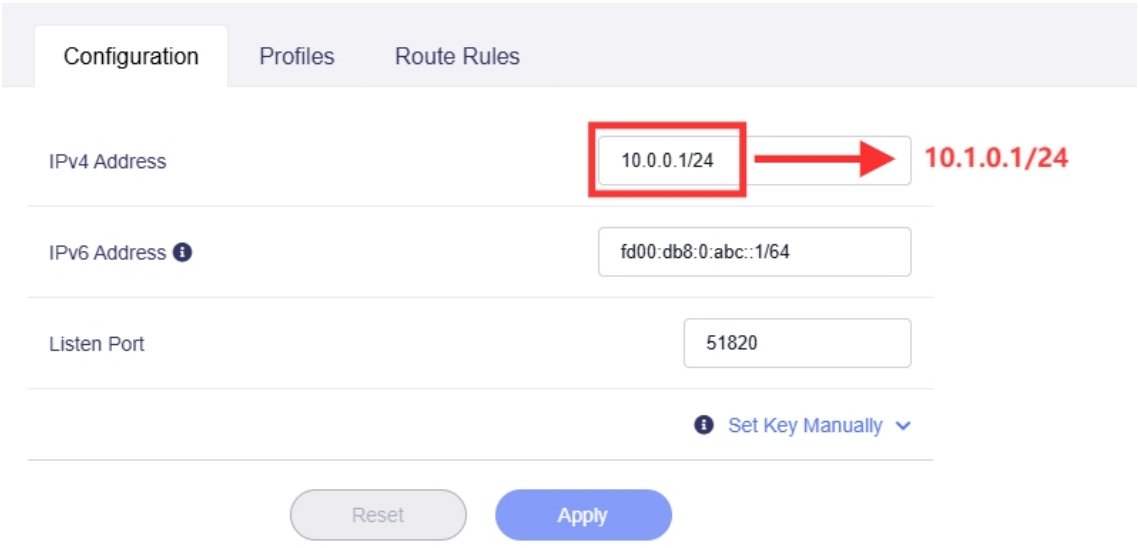
- Ist Ihr GL.iNet-Router über mehrere Router hinter dem Hauptrouter angeschlossen, richten Sie die Portweiterleitung auf jedem dazwischenliegenden Gerät ein.

10.2.2 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.

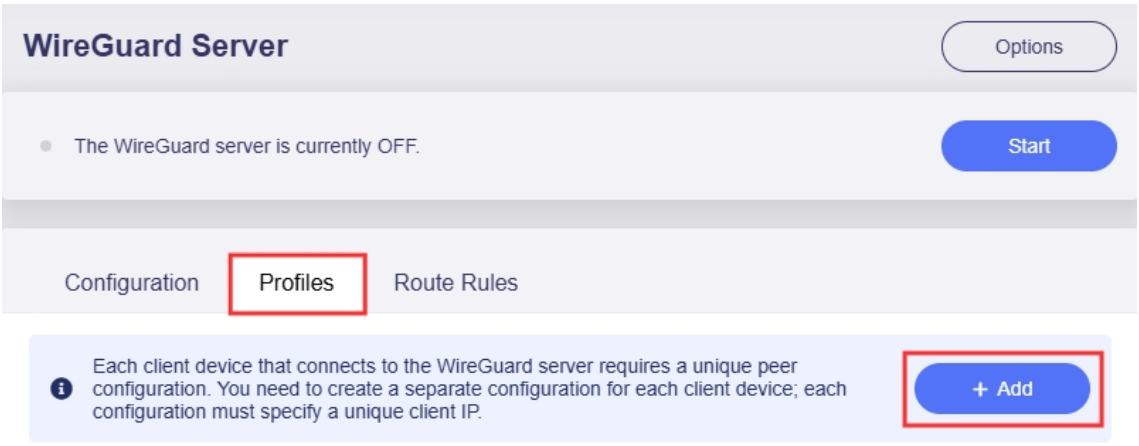


   Bei einem solchen Adresskonflikt wählen Sie eine andere IPv4-Adresse, etwa **10.1.0.1/24**, und klicken Sie auf **Apply**. Achten Sie darauf, die CIDR-Angabe „/24“ beizubehalten, um Verbindungsprobleme zu vermeiden.

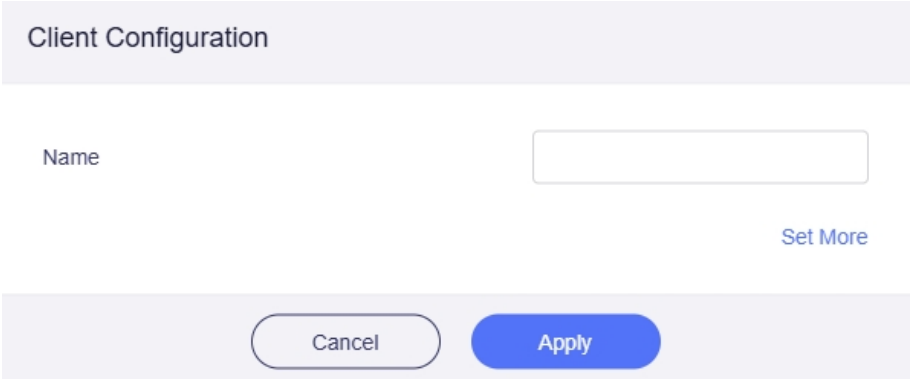


3. Profil hinzufügen.

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.



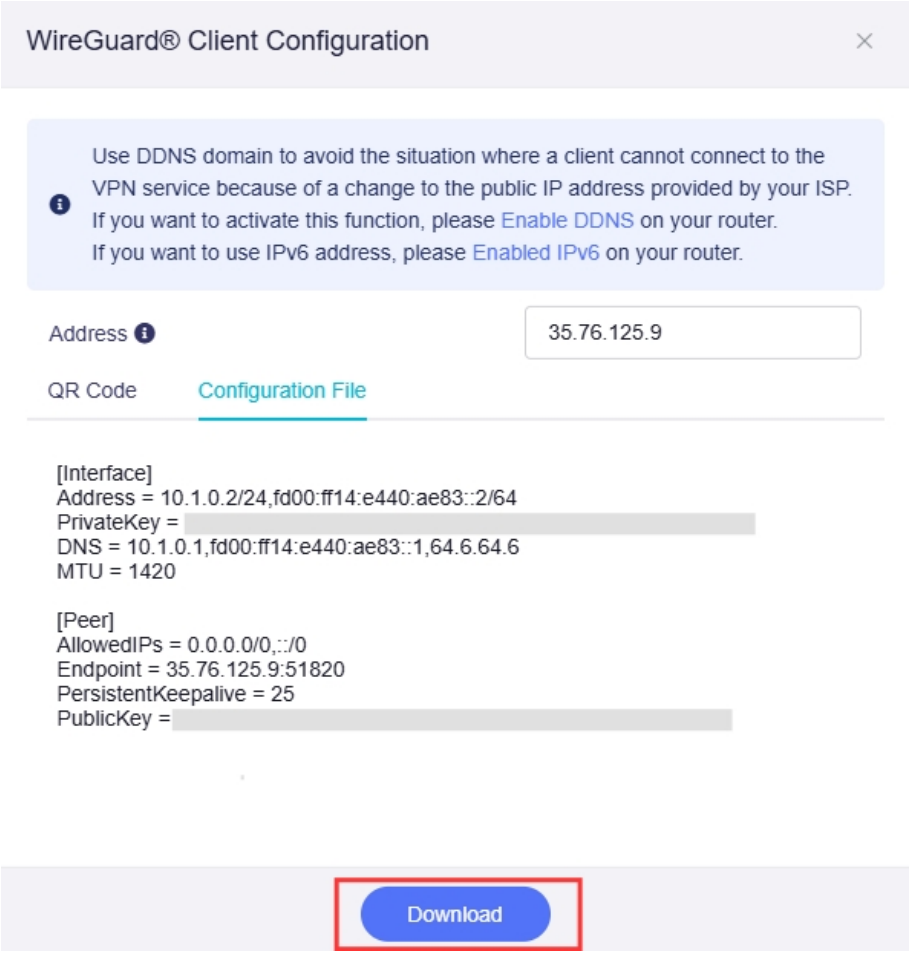
Tipp: Wenn Sie vom WireGuard-Server auf die LAN-Geräte des WireGuard-Clients zugreifen möchten, öffnen Sie die Registerkarte **Route Rules** und konfigurieren Sie die Routingregeln. Einzelheiten finden Sie hier.

4. Konfiguration herunterladen.

   Nach dem Hinzufügen eines Profils stellt der Router die Konfiguration in drei Formen bereit: als QR-Code, als Klartext und als .conf-Datei. Wählen Sie die gewünschte Form aus.

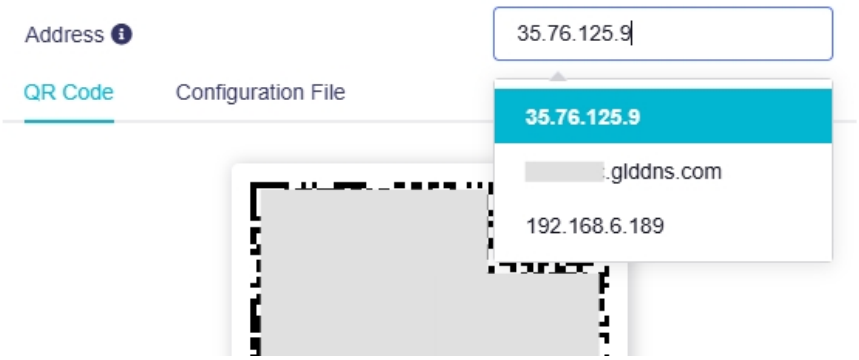
   - **QR-Code**: Geeignet für Geräte wie Smartphones, Tablets oder Laptops mit installierter WireGuard-App. Öffnen Sie auf dem gewünschten WireGuard-Client die WireGuard-App und scannen Sie den QR-Code, um die Konfiguration zu importieren.
   - **Klartext**: In dieser Ansicht können Sie die Konfigurationsdetails prüfen und durch Kopieren und Einfügen an anderer Stelle manuell einrichten, etwa in der WireGuard-App oder auf einem GL.iNet-Router.

- **.conf-Datei**: Klicken Sie auf **Download**, um die .conf-Datei lokal zu speichern. Diese lässt sich anschließend direkt in die WireGuard-App oder auf einen GL.iNet-Router hochladen.



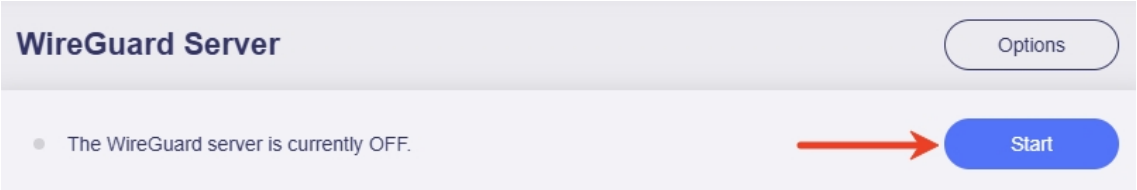
Tipps:

- Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Anschließend können Sie die DDNS-Domain als Serveradresse verwenden.
- Seit Firmware v4.8 können Sie die Serveradresse vor dem Export der Konfigurationsdatei aus einer Dropdown-Liste auswählen: öffentliche IP-Adresse, DDNS-Domain oder aktuelle WAN-IP-Adresse. Die Serveradresse in der Konfigurationsdatei wird entsprechend automatisch aktualisiert. Laden Sie die Konfigurationsdatei erneut herunter, wenn sich die Serveradresse ändert.

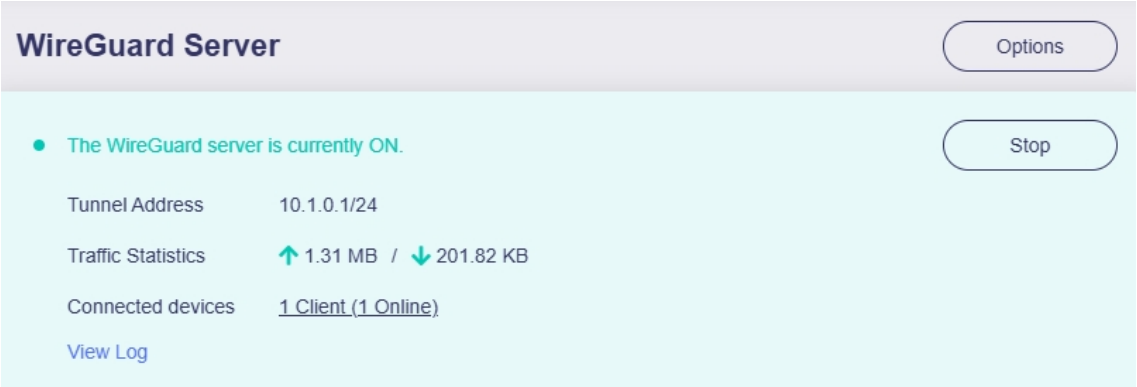


5. WireGuard-Server starten.

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



   Der Verbindungsstatus des Servers wird oben angezeigt. Wenn Statistiken zum hoch- und heruntergeladenen Datenvolumen sowie online verbundene Geräte erscheinen, läuft der WireGuard-Server.

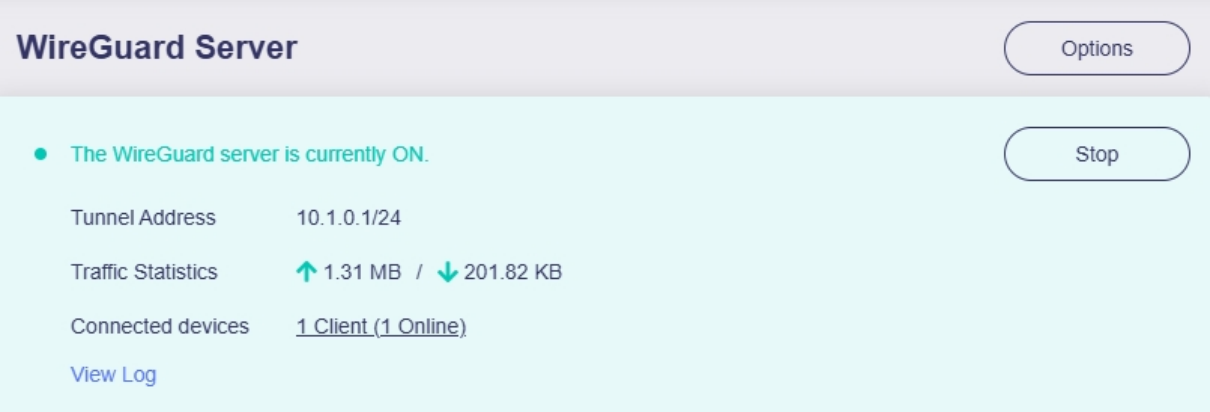


10.2.3 Verbindung prüfen

Methode 1: Serverstatus prüfen

Ab Firmware v4.8 können Sie den Verbindungsstatus des Servers auf der Seite **WireGuard Server** prüfen.

Wenn Upload- und Downloadstatistiken sowie verbundene Geräte angezeigt werden, läuft der WireGuard-Server und es sind WireGuard-Clients mit ihm verbunden.



Wenn kein Datenverkehr und keine Clients angezeigt werden, ist kein WireGuard-Client verbunden.



Methode 2: IP-Adresse des Clients prüfen

Importieren Sie die zuvor exportierte WireGuard-Konfiguration auf ein Gerät in einem anderen Netzwerk als dem lokalen Netzwerk des Servers. Öffnen Sie anschließend einen Webbrowser und ermitteln Sie Ihre IP-Adresse und Ihren Standort. Wenn diese mit der IP-Adresse und dem Standort des VPN-Servers übereinstimmen und nicht mit denen Ihres Internetanbieters, besteht die VPN-Verbindung erfolgreich.

Im folgenden Beispiel erfolgt die Überprüfung mit einem Smartphone, auf dem die offizielle WireGuard-App installiert ist.

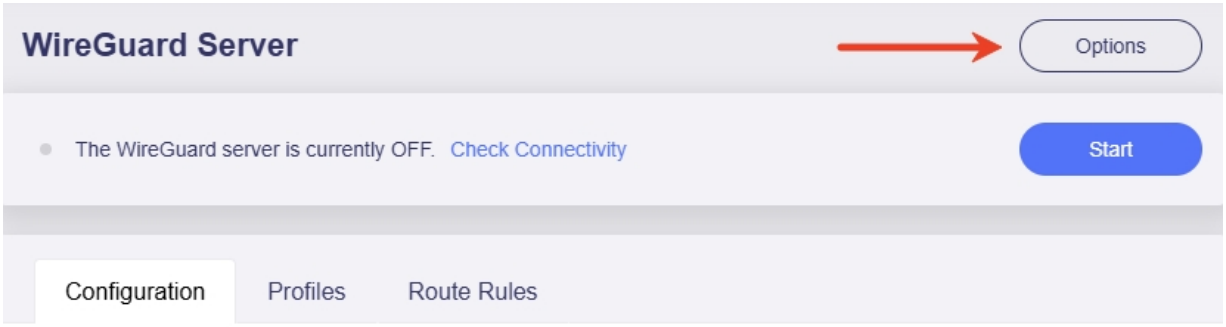
1. Deaktivieren Sie zunächst das WLAN des Smartphones und aktivieren Sie ausschließlich die mobile Datenverbindung (4G/5G).
2. Öffnen Sie anschließend die WireGuard-App, importieren Sie die Konfigurationsdatei und stellen Sie die Verbindung her.
3. Prüfen Sie, ob das Smartphone Internetzugang hat und seine IP-Adresse mit der des WireGuard-Servers übereinstimmt.

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

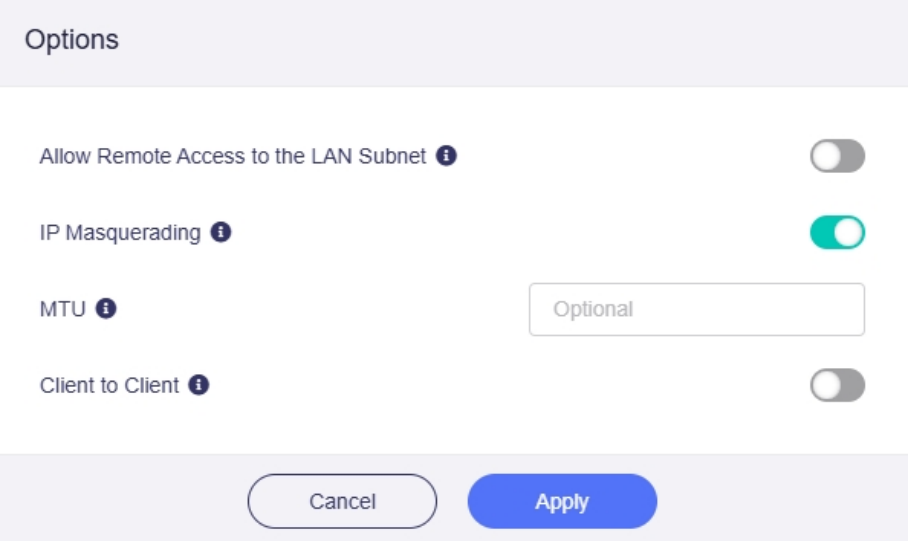
- Der VPN-Server hat keine öffentliche IP-Adresse. Einzelheiten finden Sie unter **10.2.1 Vorbereitung**.
- Möglicherweise müssen Sie eine Portweiterleitung einrichten. Einzelheiten finden Sie unter **10.2.1 Vorbereitung**.
- Ihr Internetanbieter sperrt den vom WireGuard-Server verwendeten Port. Wechseln Sie zu einem anderen Port oder bitten Sie Ihren Internetanbieter um Unterstützung.
- In bestimmten Ländern oder Regionen kann die VPN-Verbindung gesperrt sein.

10.2.4 Server-Optionen

Die Serveroptionen enthalten erweiterte serverseitige Einstellungen, etwa den Fernzugriff auf das LAN des Servers oder IP-Masquerading. Konfigurieren Sie diese Einstellungen nach Bedarf. Klicken Sie auf der Seite **WireGuard Server** oben rechts auf **Options**.



Im eingeblendeten Fenster stehen die folgenden Funktionen zur Verfügung.



- **Allow Remote Access to the LAN Subnet**: Wenn diese Option aktiviert ist, können Ressourcen im LAN-Subnetz des Servers über den VPN-Tunnel aufgerufen werden.
- **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**: Wenn diese Option aktiviert ist, können die mit diesem Server verbundenen VPN-Clients über ihre jeweiligen IP-Adressen im VPN-Tunnel aufeinander zugreifen.
  Client-to-Client gibt lediglich die Tunnel-IP-Adresse jedes Clients bekannt. Die lokalen LAN-Subnetze hinter den einzelnen VPN-Clients werden dadurch nicht automatisch erreichbar. Wenn Clients auf die LAN-Subnetze der jeweils anderen Clients zugreifen sollen, ergänzen Sie auf dem VPN-Server Routingregeln, die diese entfernten LAN-Subnetze bekannt geben.

Kapitel 11

VPN-Client einrichten

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

11.1 OpenVPN-Client

11.1.1 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.

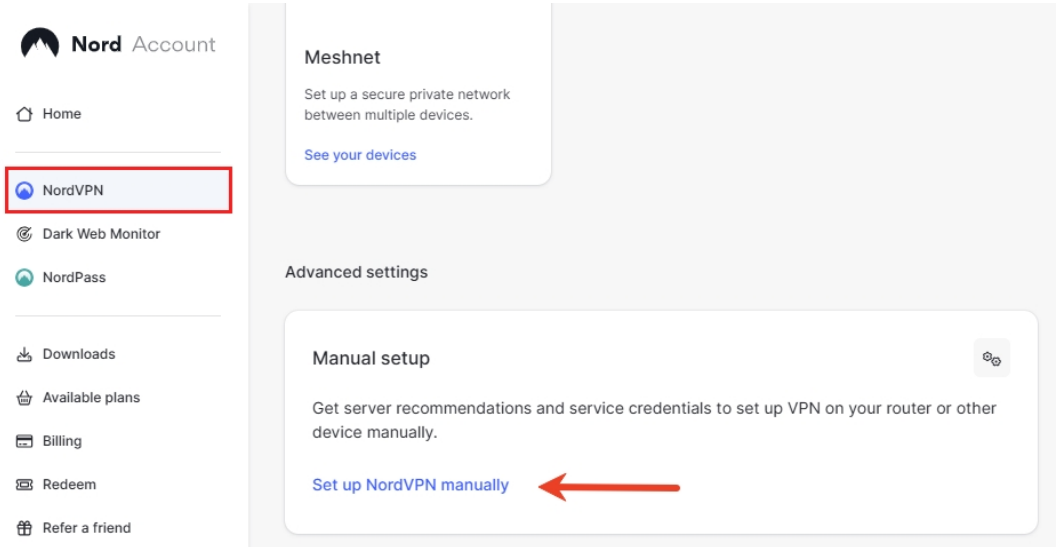
Rufen Sie anschließend die offizielle Webseite Ihres VPN-Anbieters auf und beschaffen Sie die Dienstzugangsdaten oder eine Konfigurationsdatei. Falls Sie nicht wissen, wie Sie die Datei erhalten, folgen Sie diesem Link oder wenden Sie sich an den Support des Anbieters.

11.1.2 NordVPN einrichten

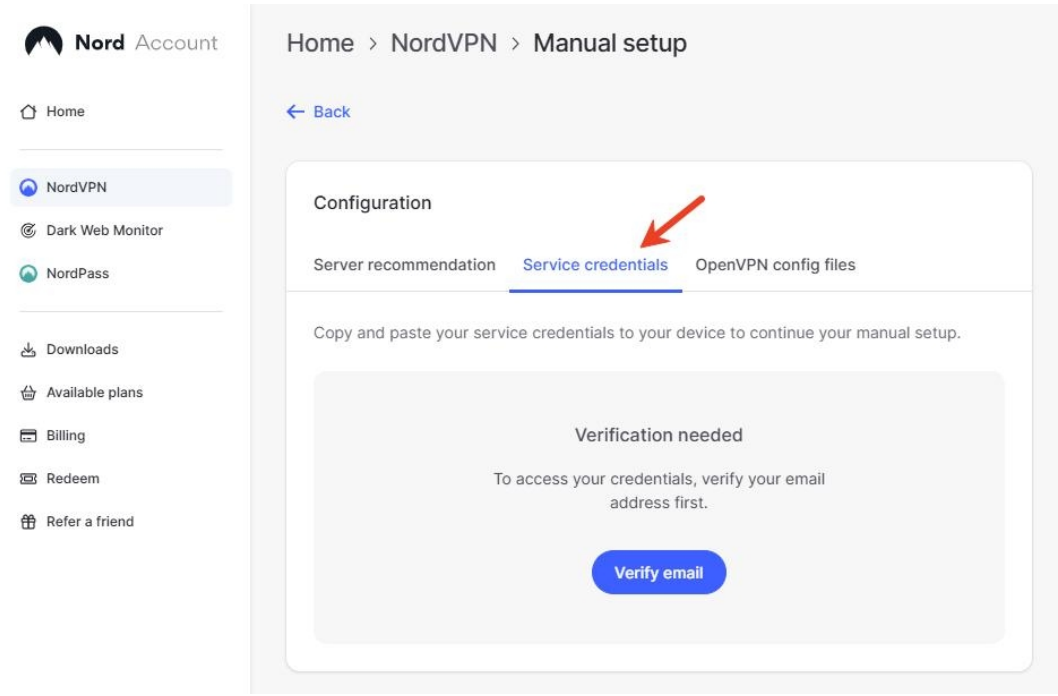
NordVPN ist in die GL.iNet-Weboberfläche integriert. Geben Sie Ihre im NordVPN-Dashboard erhältlichen Zugangsdaten in der Weboberfläche des Routers oder in der GL.iNet-App ein, um die Konfigurationsdateien aller NordVPN-Server abzurufen. Ein manuelles Hochladen der Dateien ist dadurch nicht erforderlich.

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

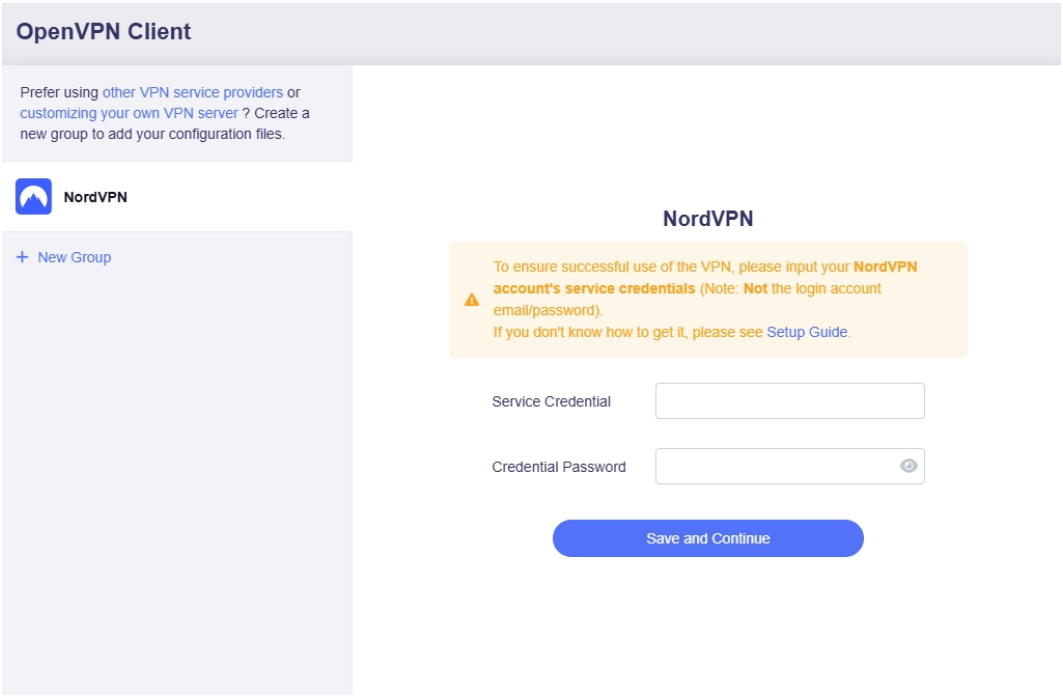
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



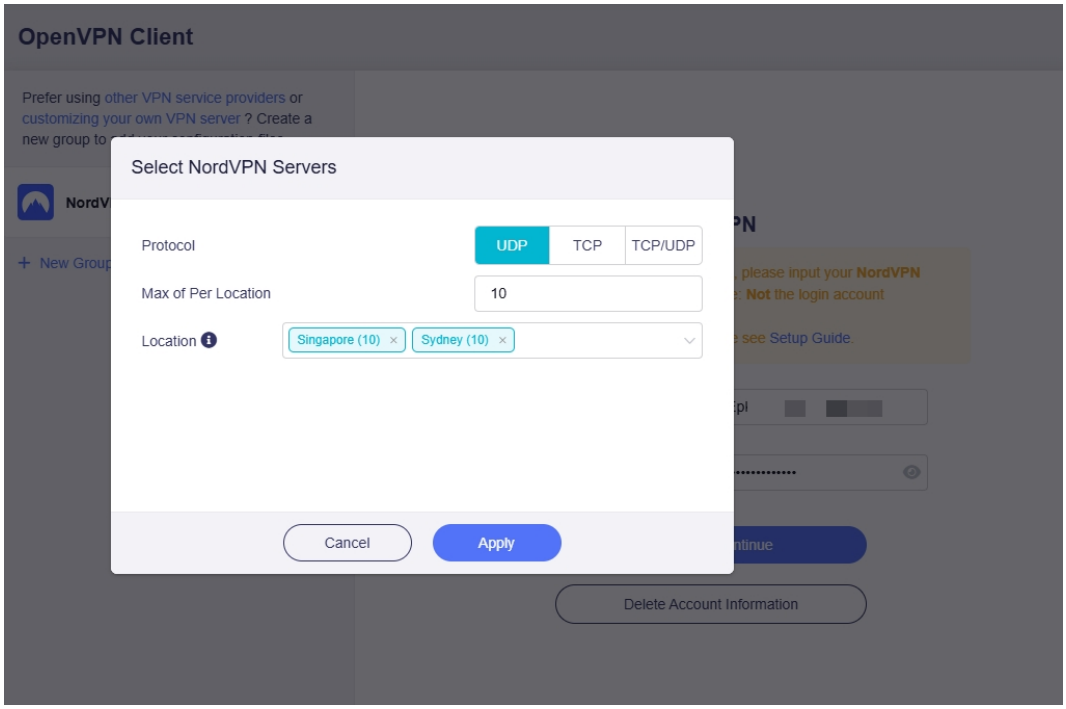
Dort finden Sie die **Dienstzugangsdaten**. Kopieren Sie diese für die spätere Verwendung.



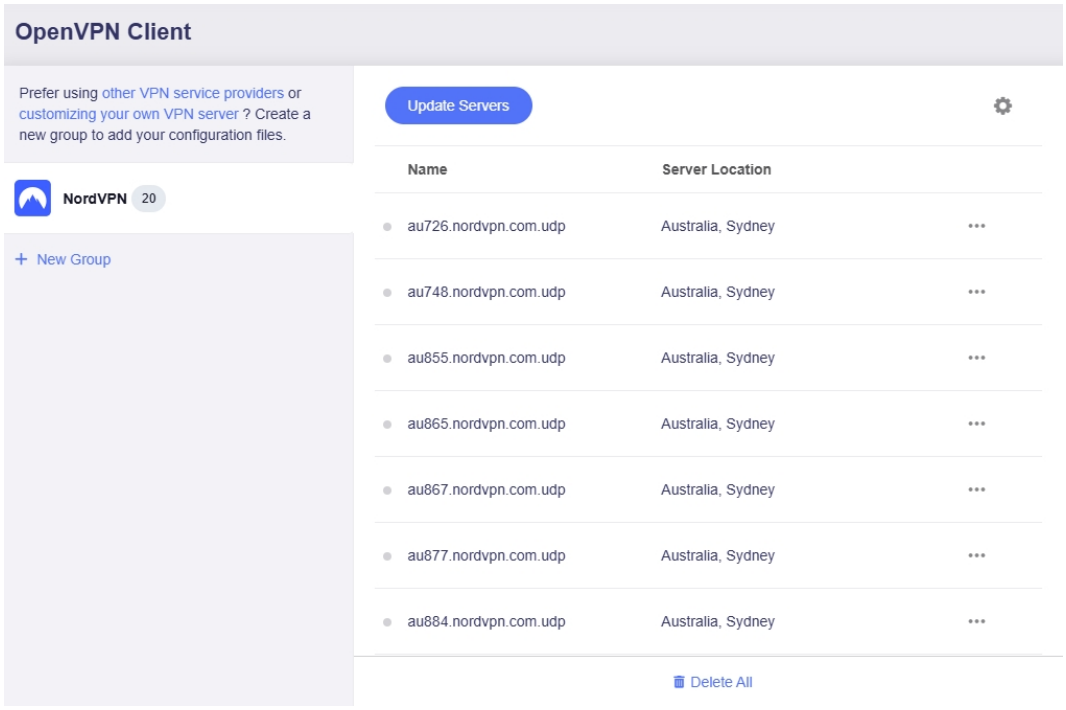
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **OpenVPN Client** > **NordVPN**. Geben Sie die Dienstzugangsdaten ein. Hinweis: Dies sind NICHT die E-Mail-Adresse und das Passwort Ihres Benutzerkontos. Klicken Sie anschließend auf **Save and Continue**.



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

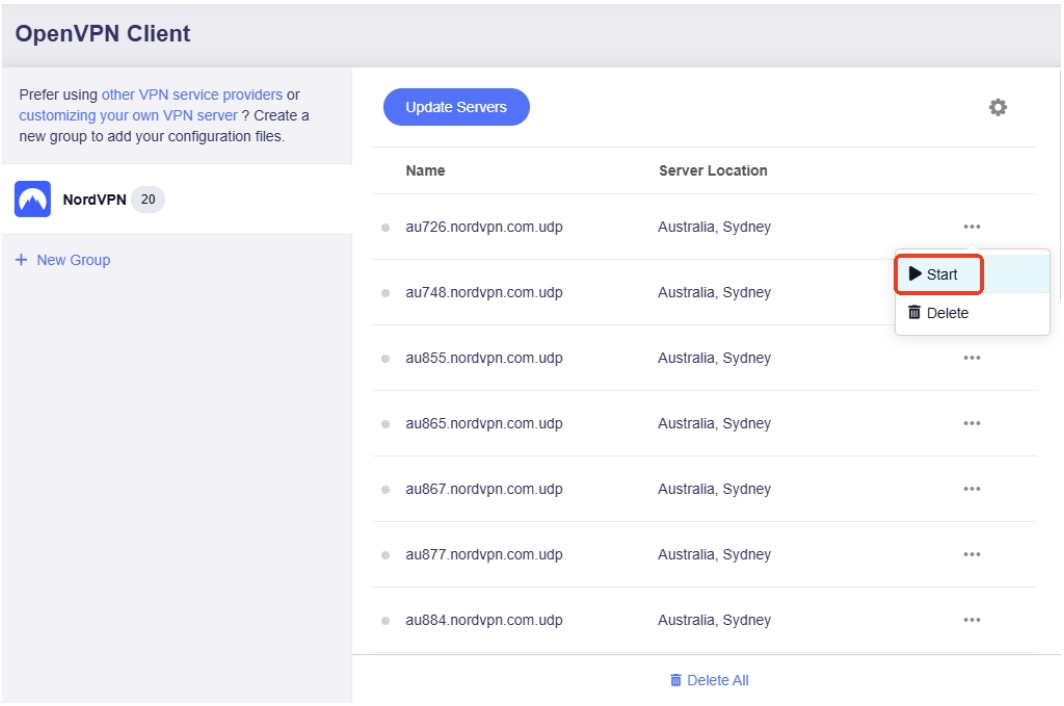


Die Konfigurationsdateien werden heruntergeladen.

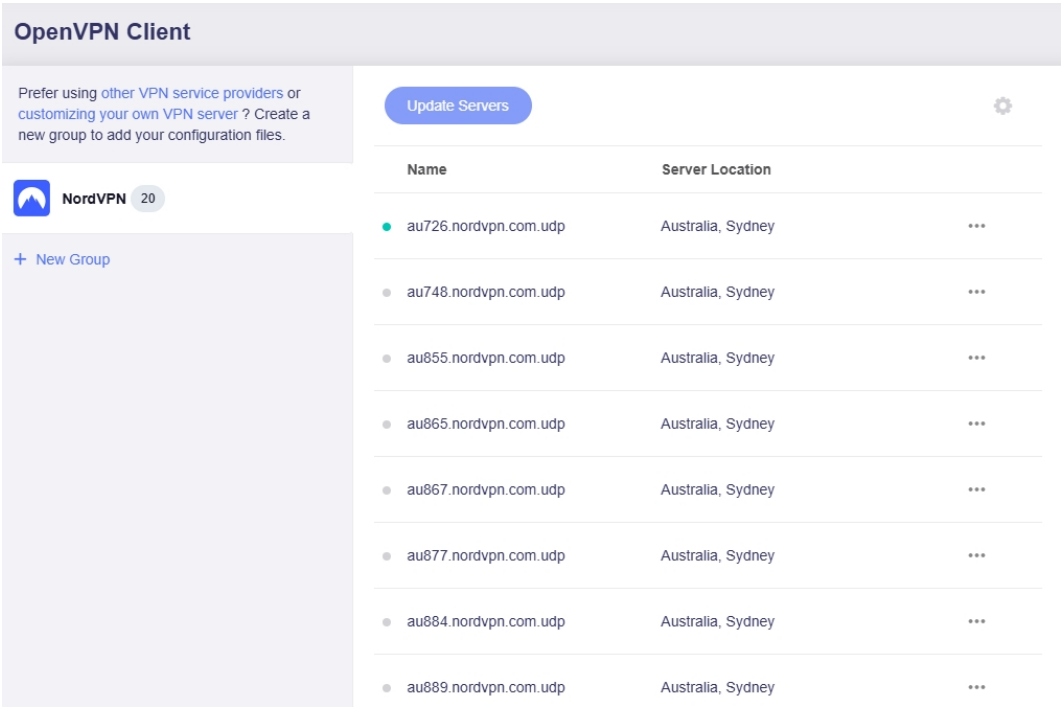


5. Verbindung starten.

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



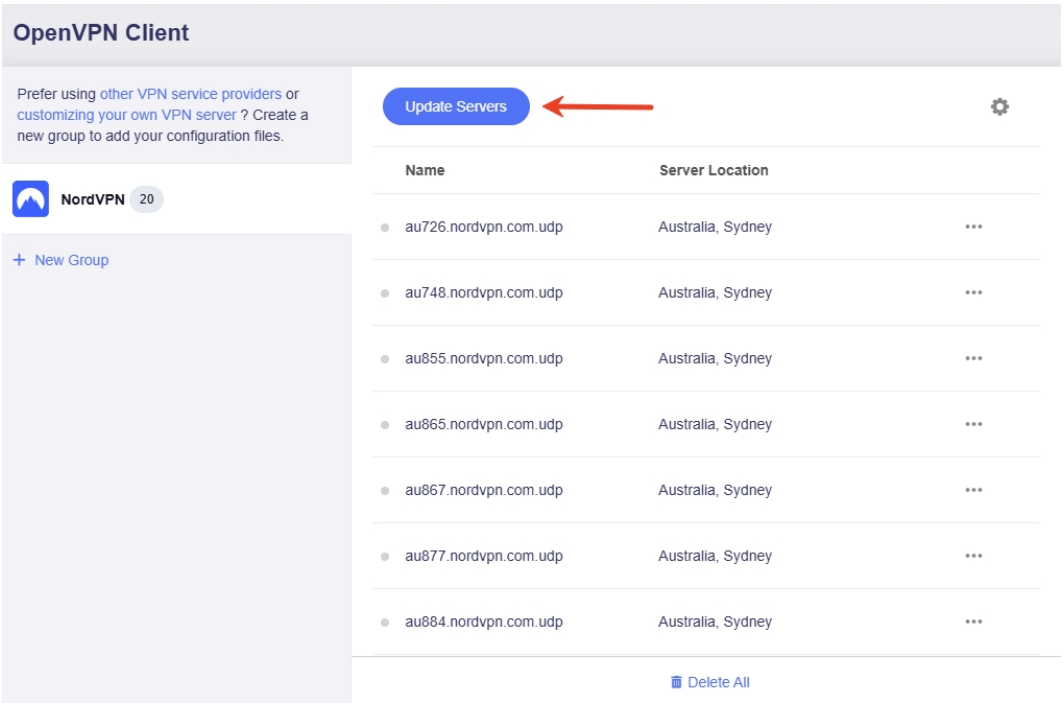
6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

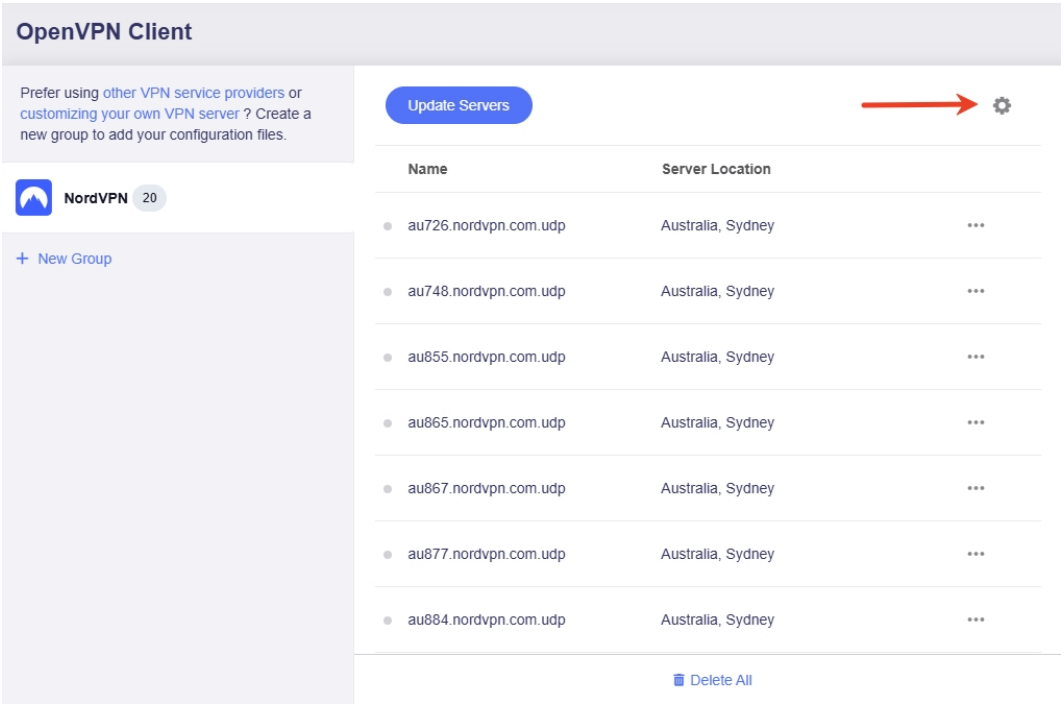
7. Server aktualisieren.

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



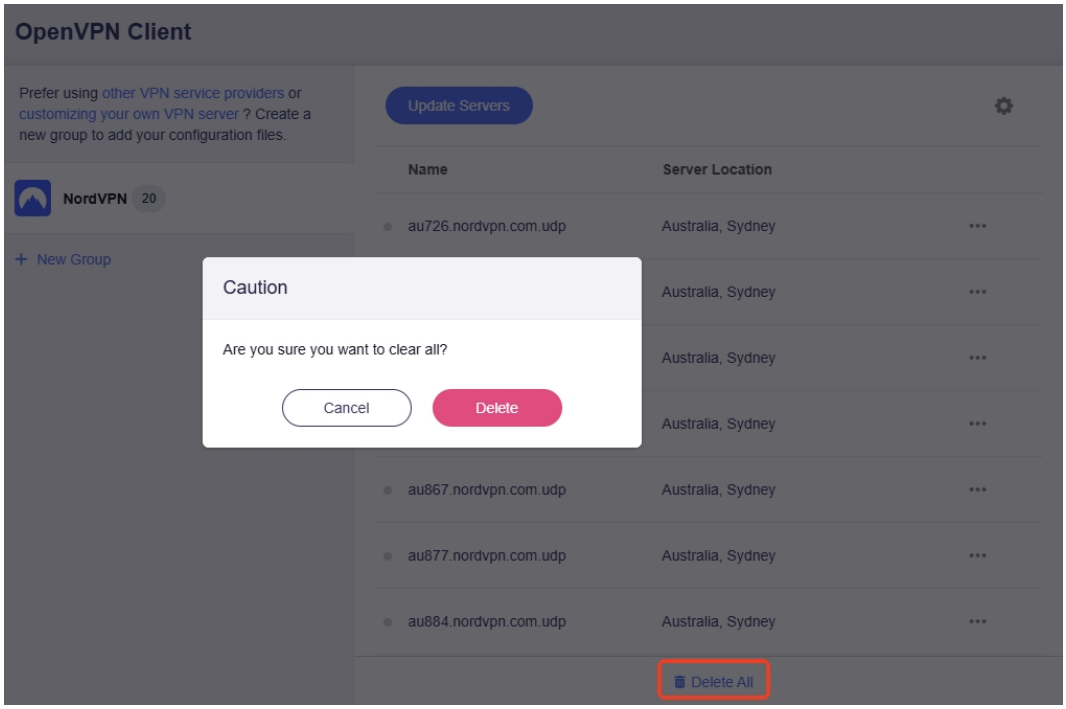
8. Zugangsdaten bearbeiten.

   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.

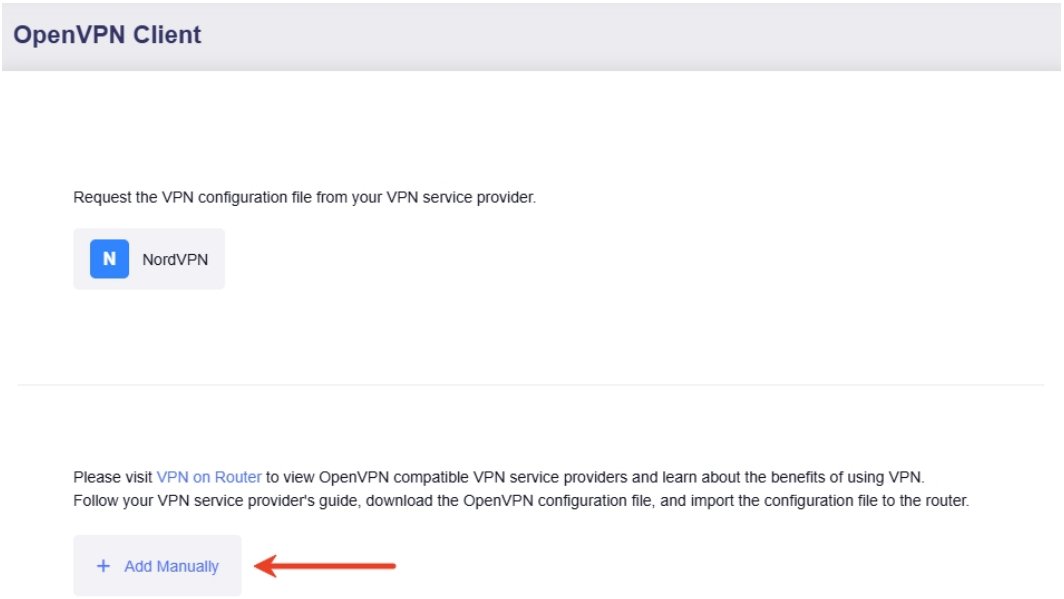

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

11.1.3 OpenVPN-Client manuell einrichten (andere Anbieter)

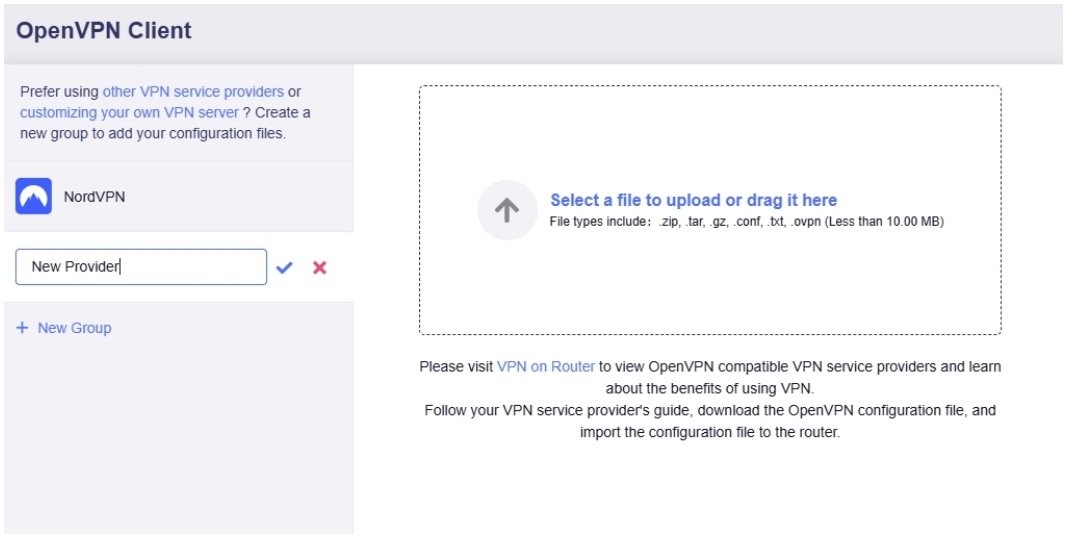
Wenn Ihr OpenVPN-Anbieter nicht in unsere Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den OpenVPN-Client einzurichten.

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

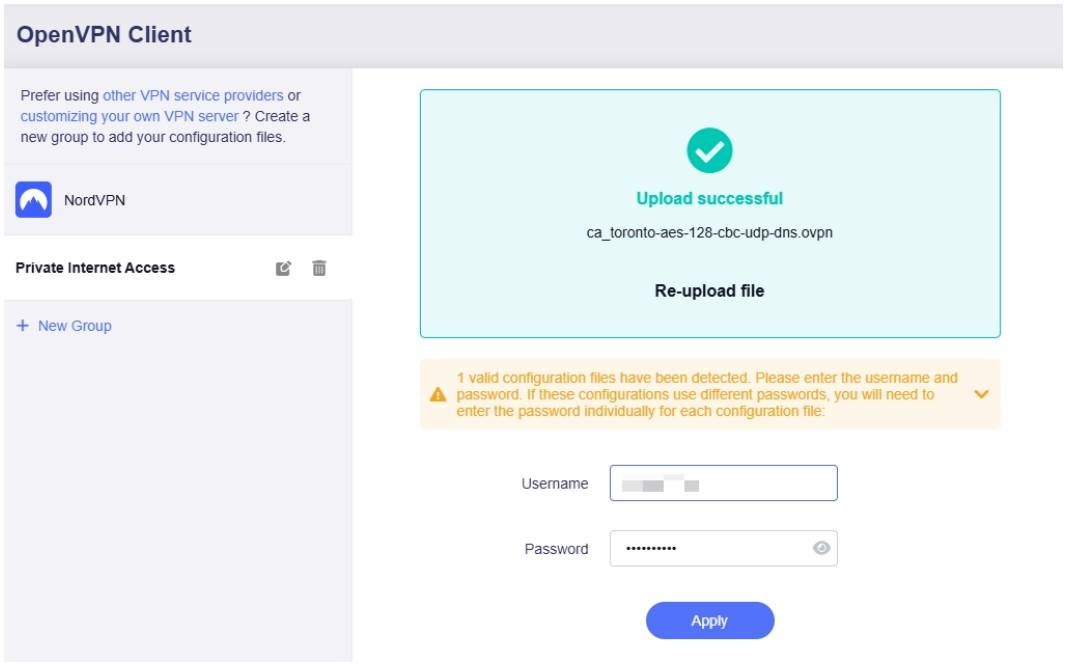
1. Laden Sie eine Konfigurationsdatei von der offiziellen Webseite von Private Internet Access herunter.
2. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Client** und klicken Sie auf **Add Manually**.



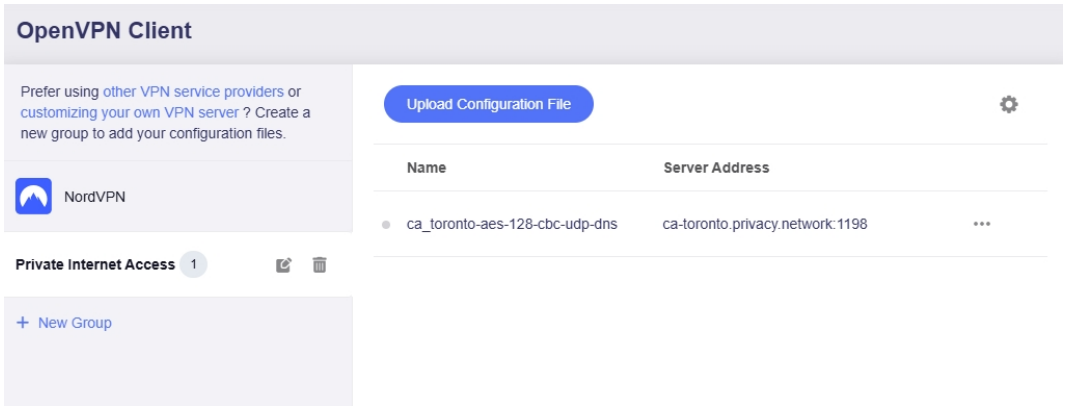
3. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



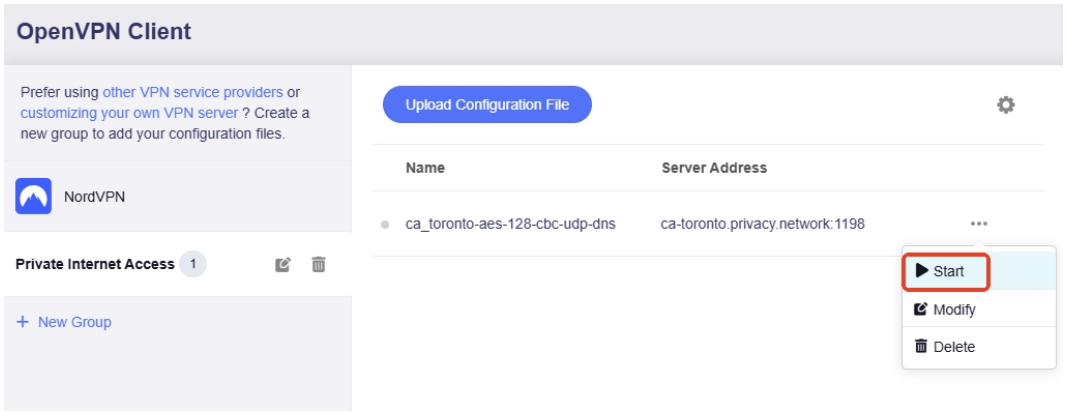
4. Laden Sie Ihre OpenVPN-Konfigurationsdatei hoch. Geben Sie bei Bedarf die Zugangsdaten ein und klicken Sie auf **Apply**.



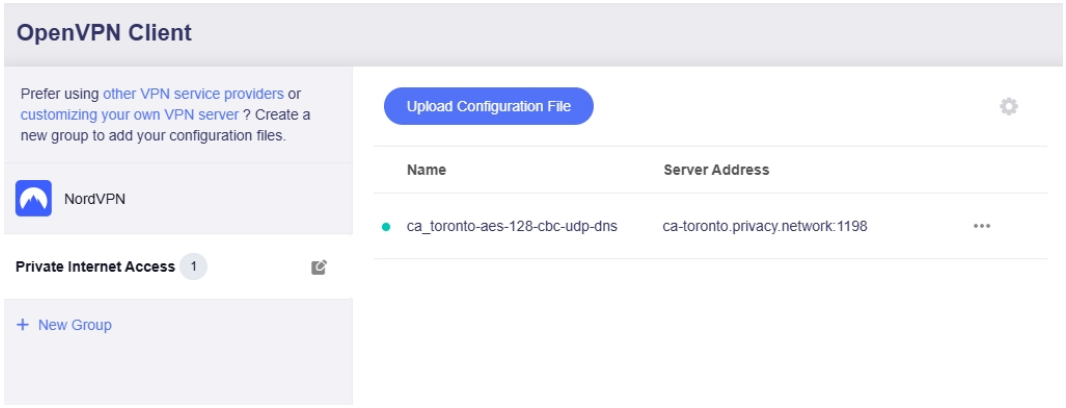
Die hochgeladene Konfigurationsdatei wird angezeigt.



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.

11.2 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.

*WireGuard® ist eine eingetragene Marke von Jason A. Donenfeld.

11.2.1 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.

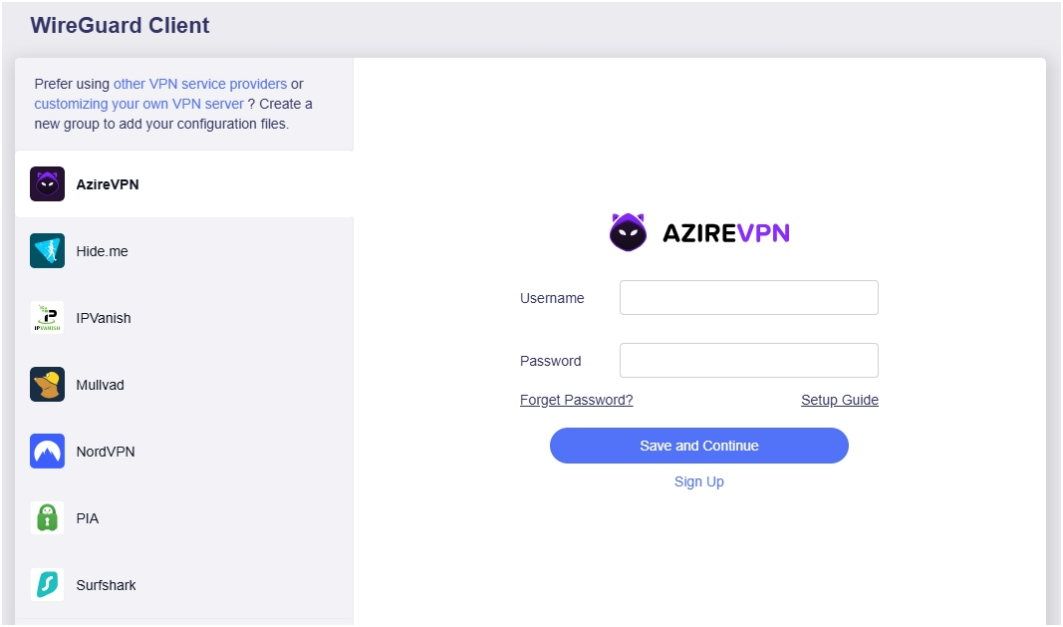
Wählen Sie nachstehend Ihren WireGuard-Anbieter aus, um direkt zur passenden Schritt-für-Schritt-Anleitung zu gelangen.

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

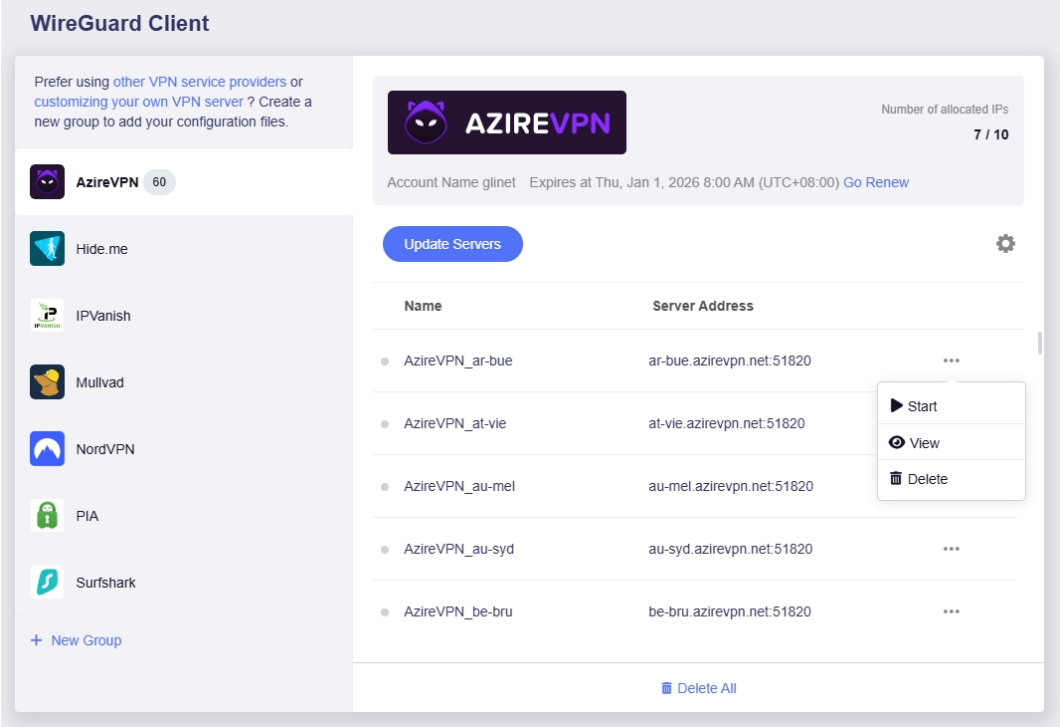
11.2.2 AzireVPN einrichten

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

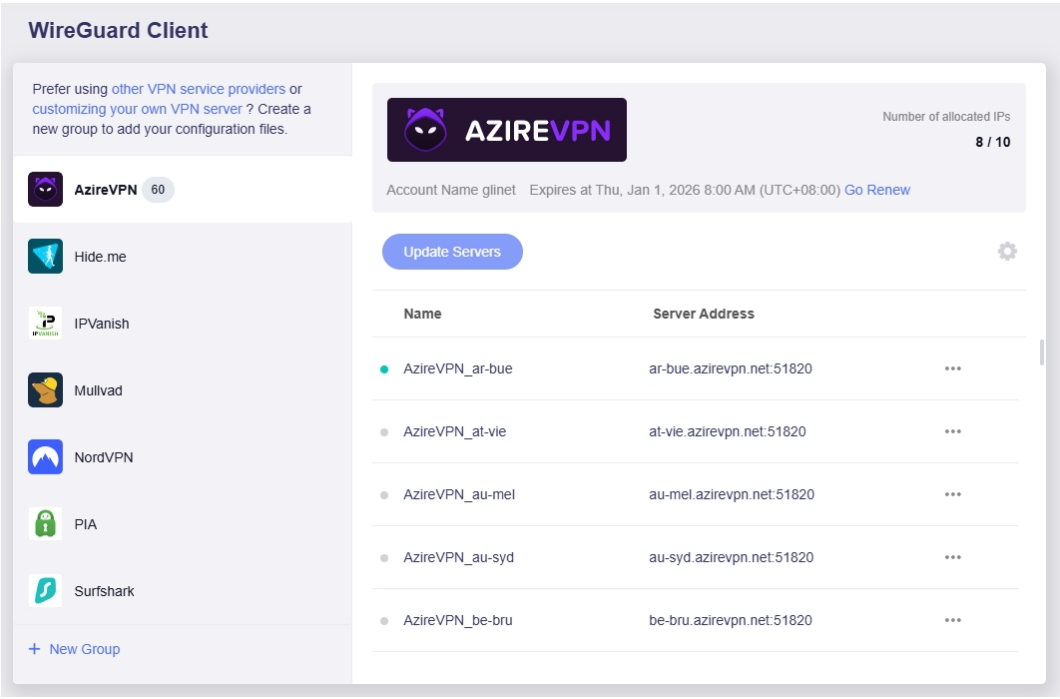
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **AzireVPN**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



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



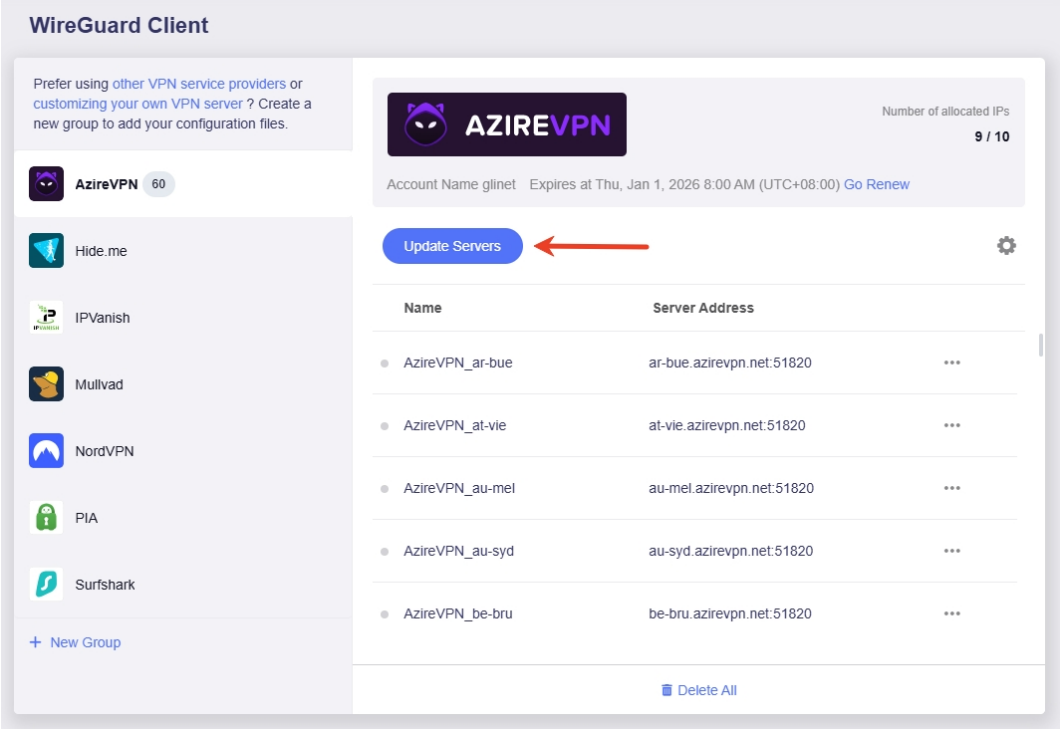
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

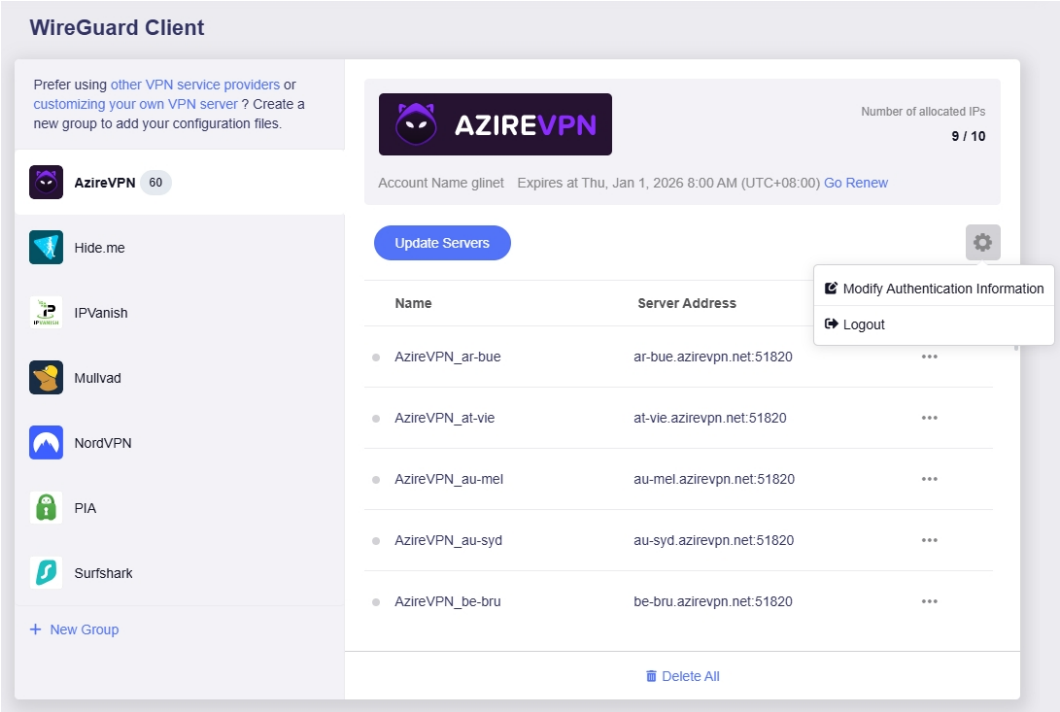
5. Server aktualisieren.

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



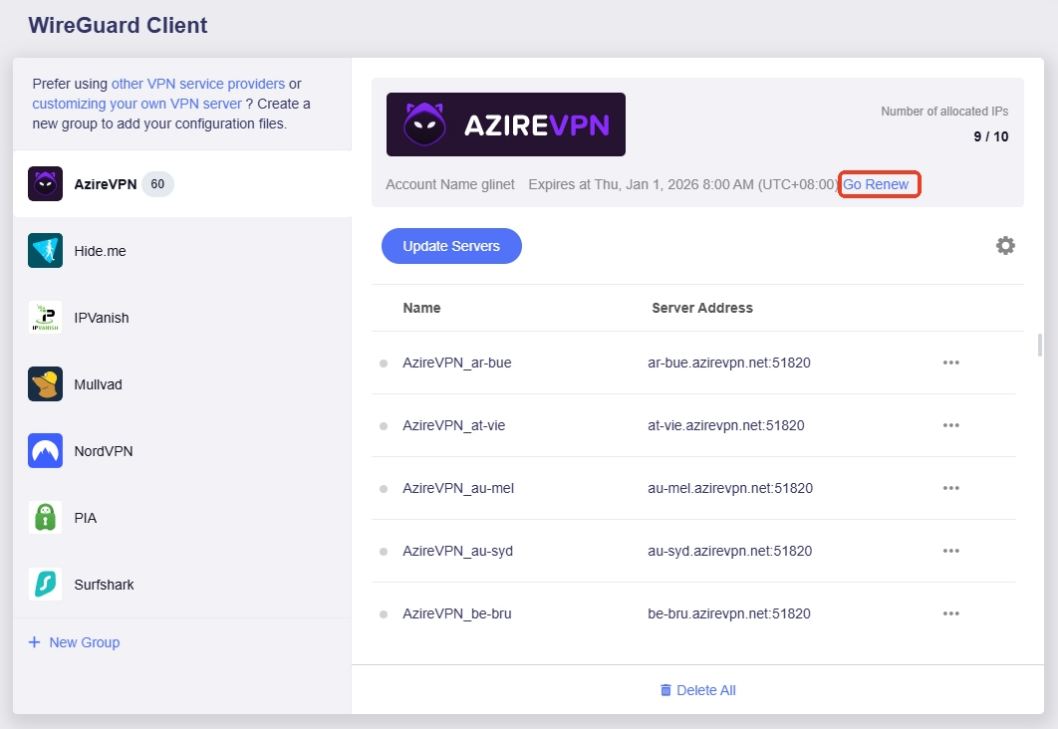
6. Zugangsdaten bearbeiten oder abmelden.

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



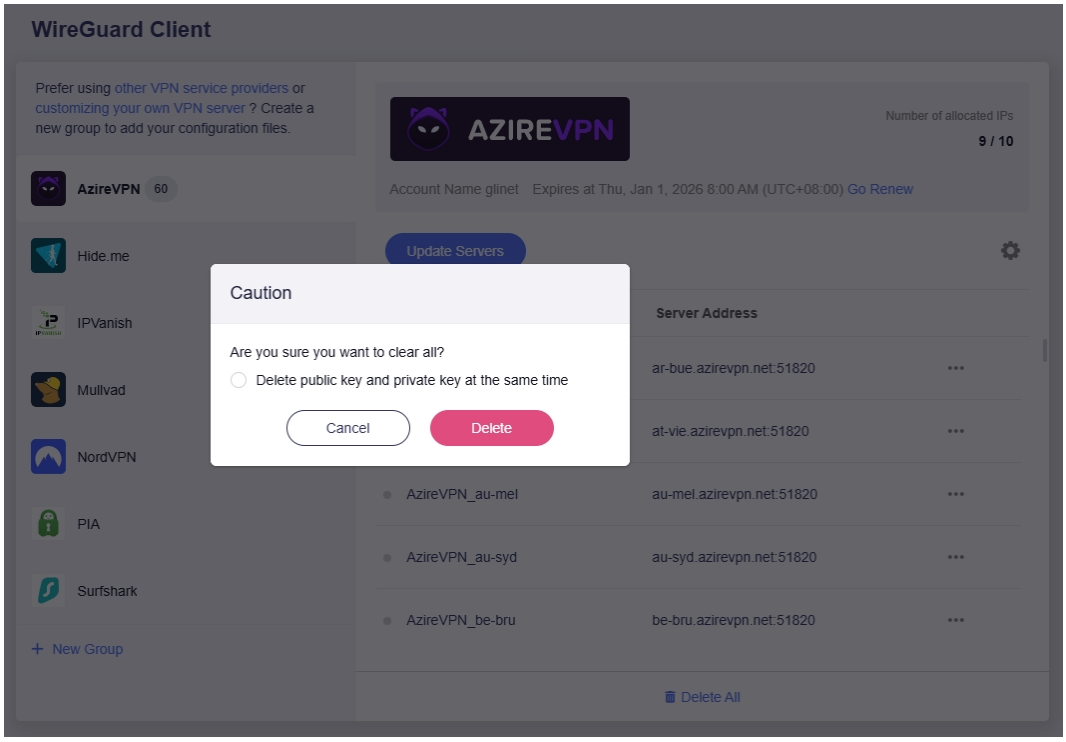
7. Abonnement verlängern.

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



8. Alle Dateien löschen.

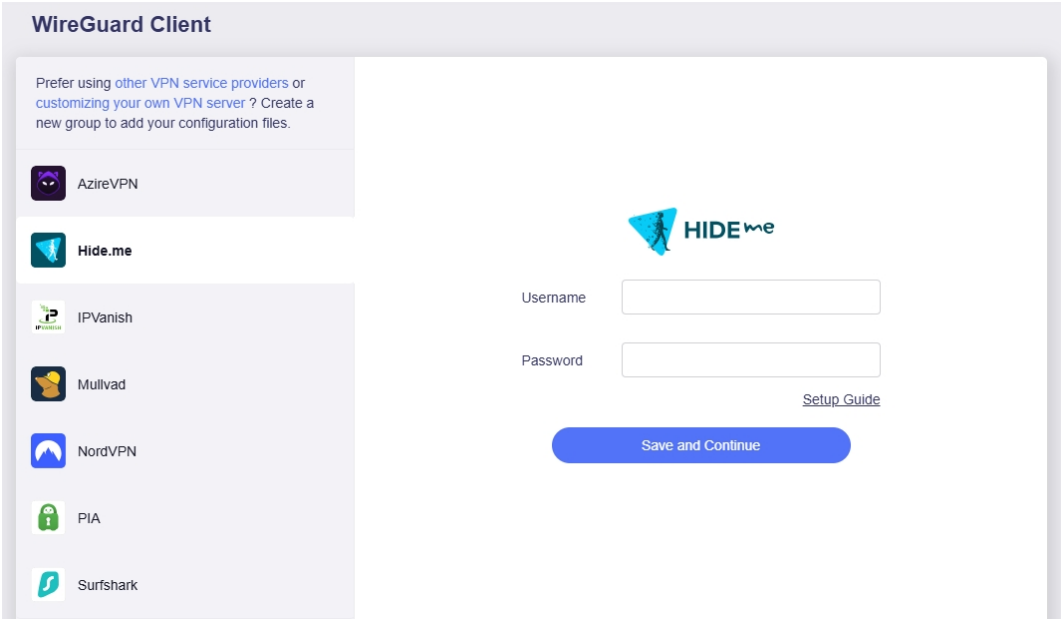
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


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

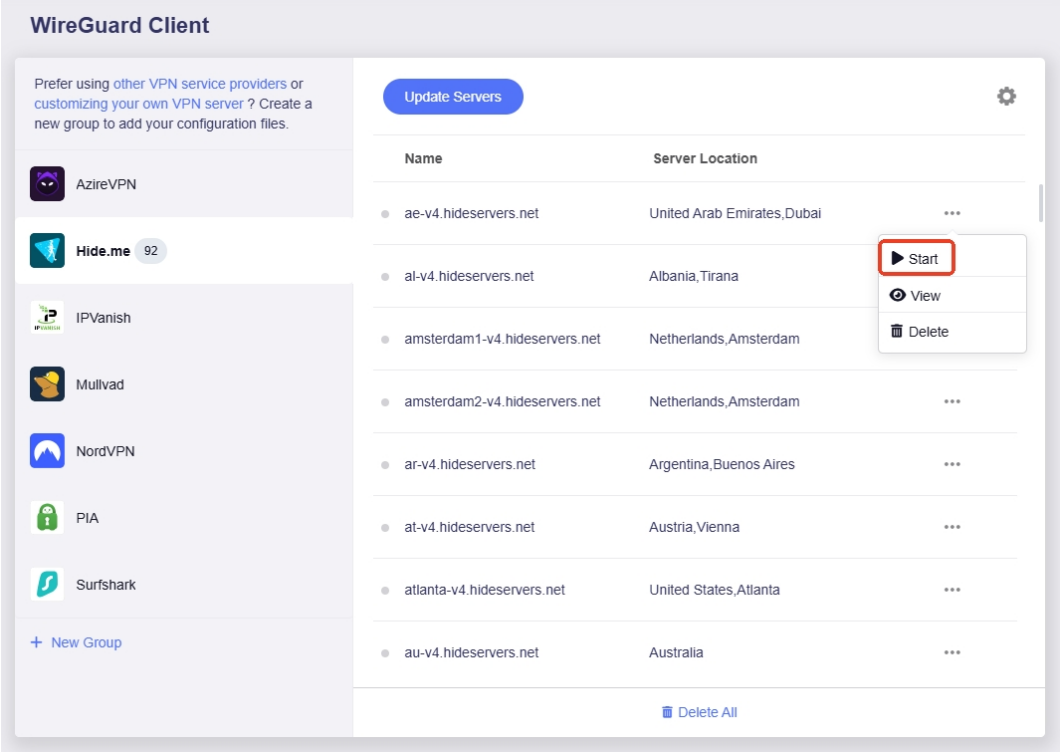
11.2.3 Hide.me einrichten

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

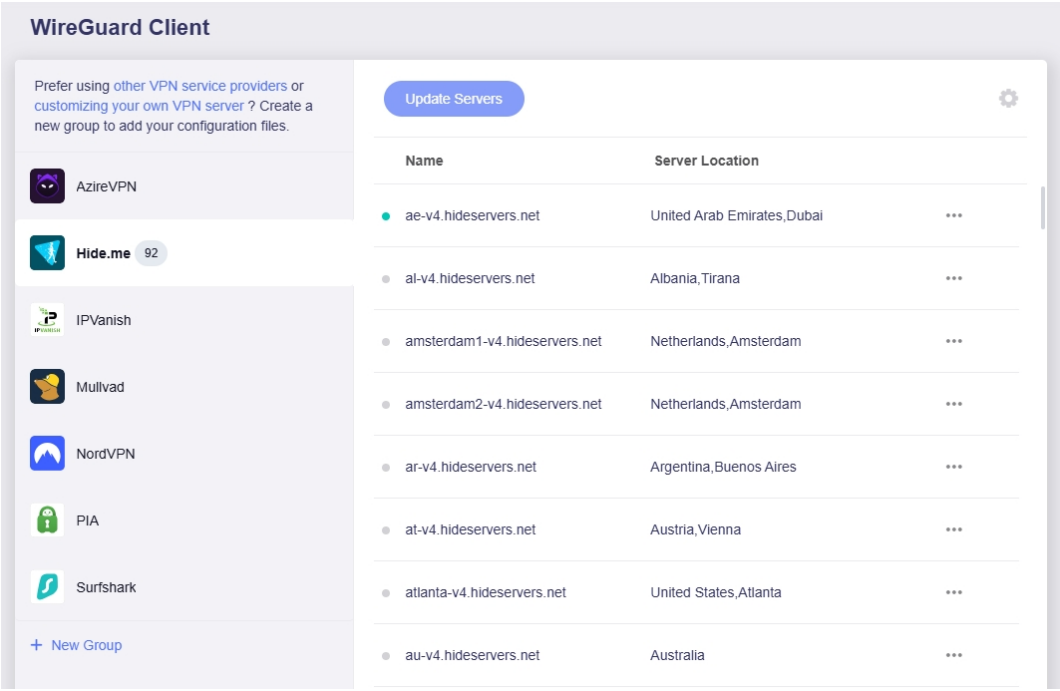
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Hide.me**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



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



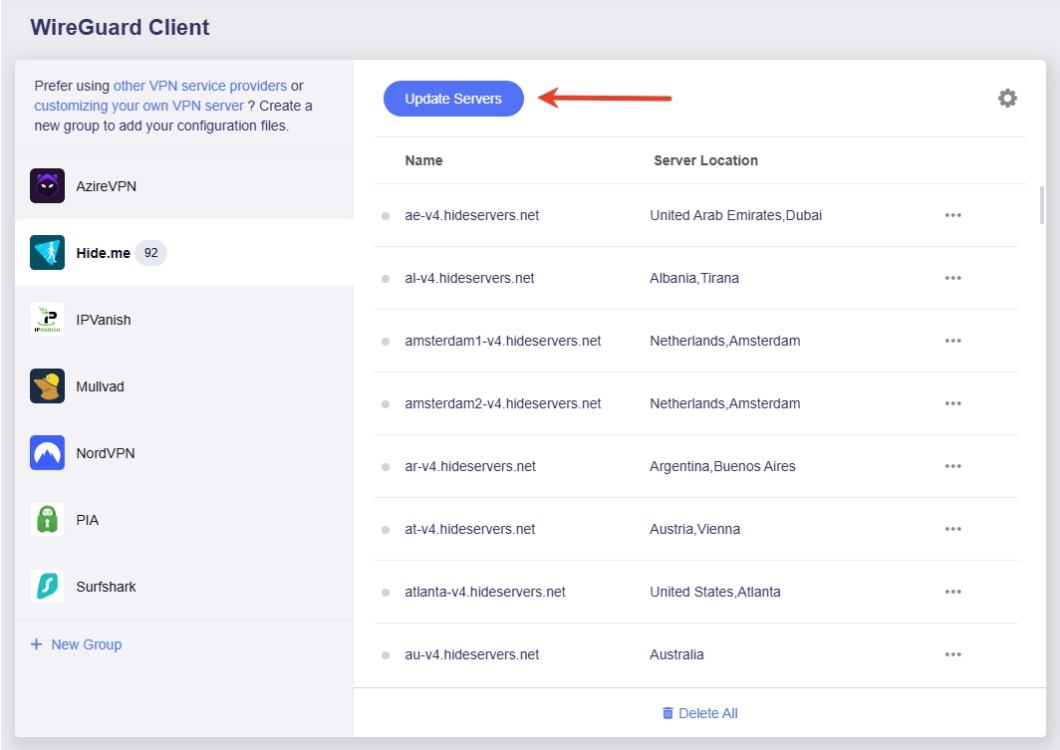
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

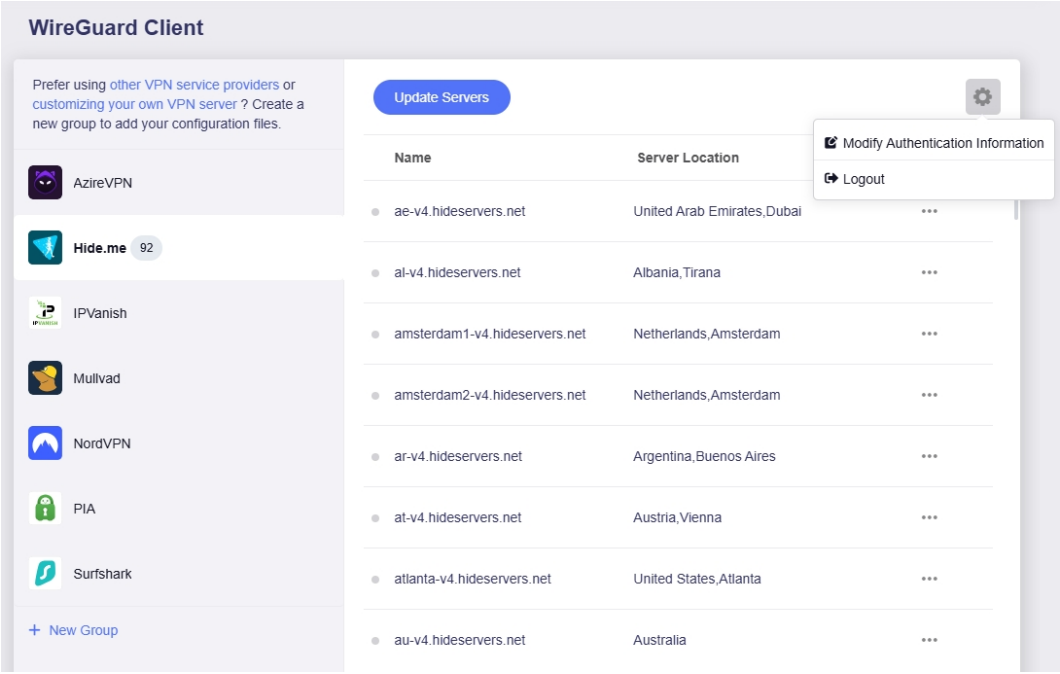
5. Server aktualisieren.

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



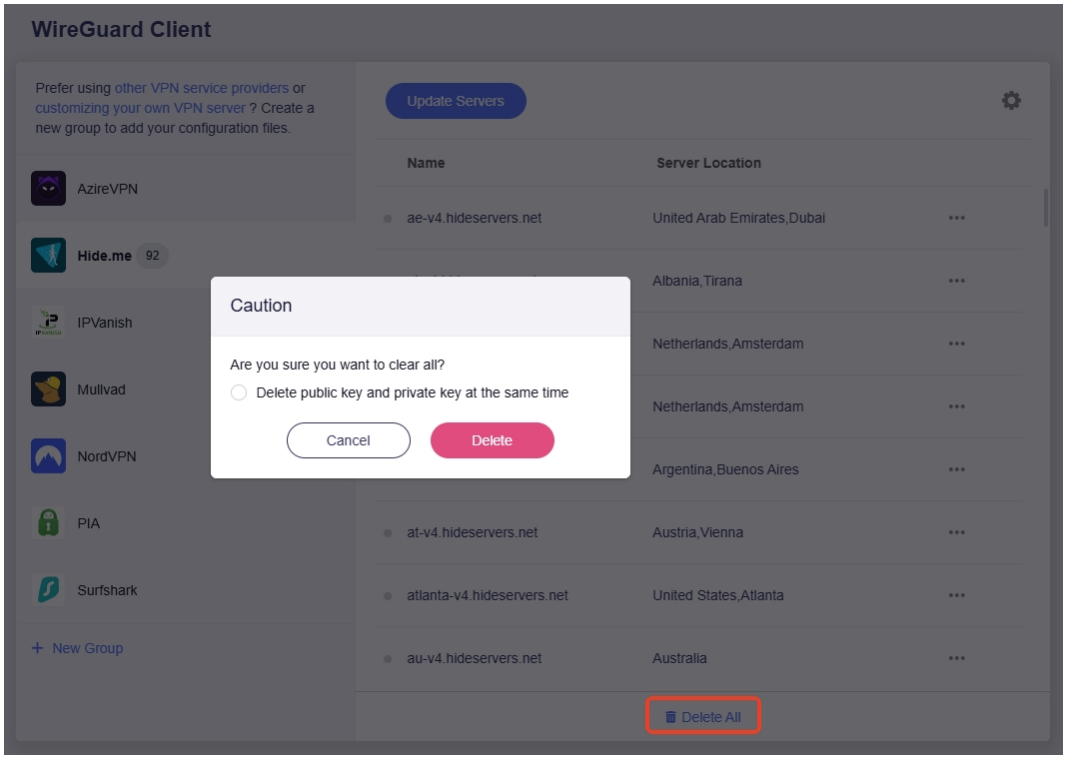
6. Zugangsdaten bearbeiten oder abmelden.

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



7. Alle Dateien löschen.

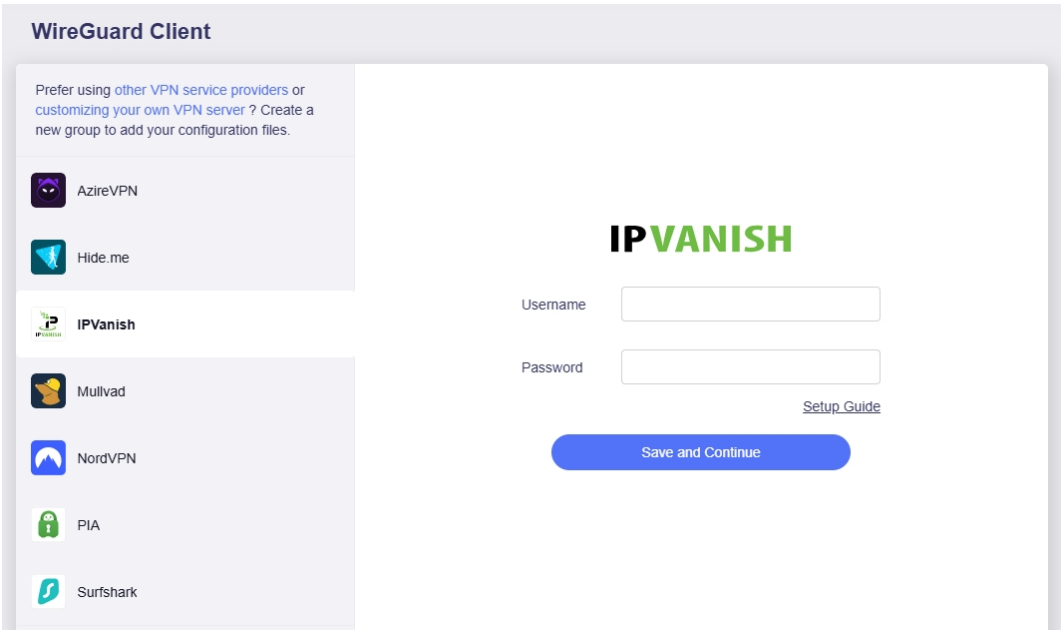
Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



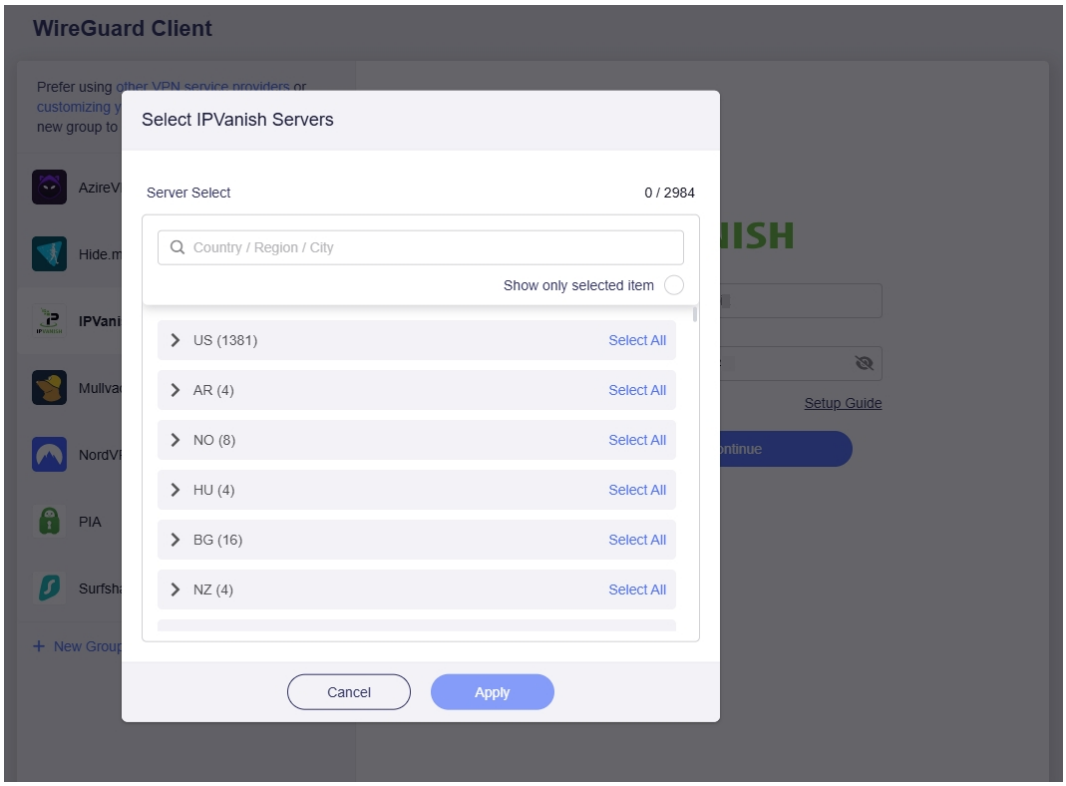
11.2.4 IPVanish einrichten

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

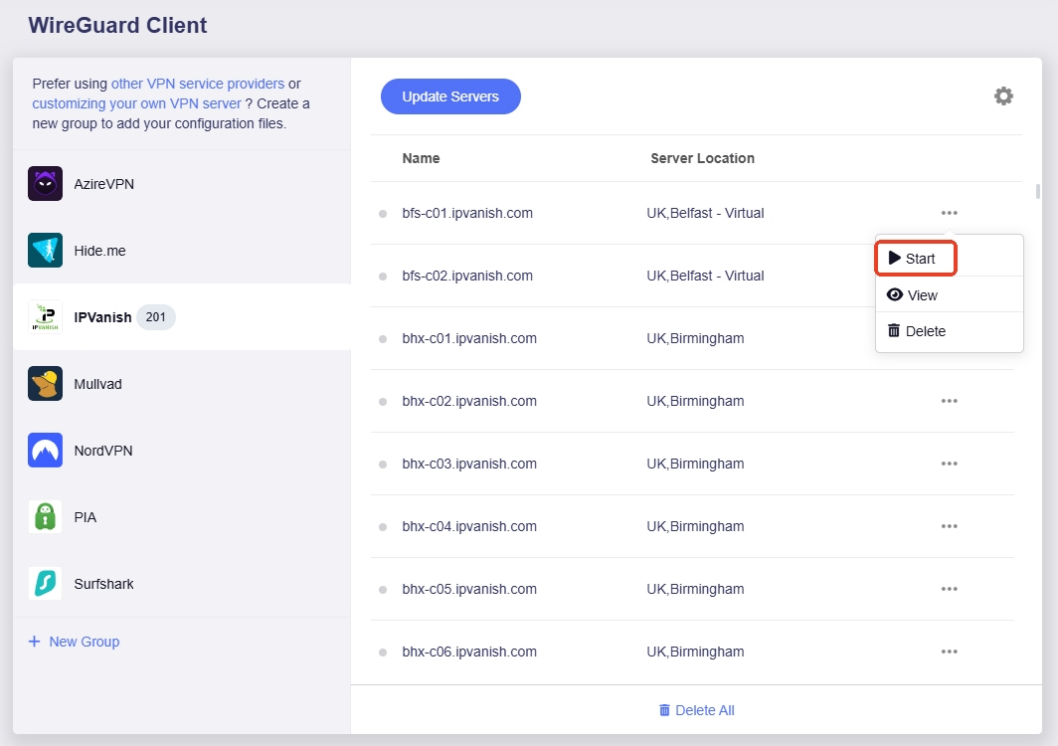
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **IPVanish**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



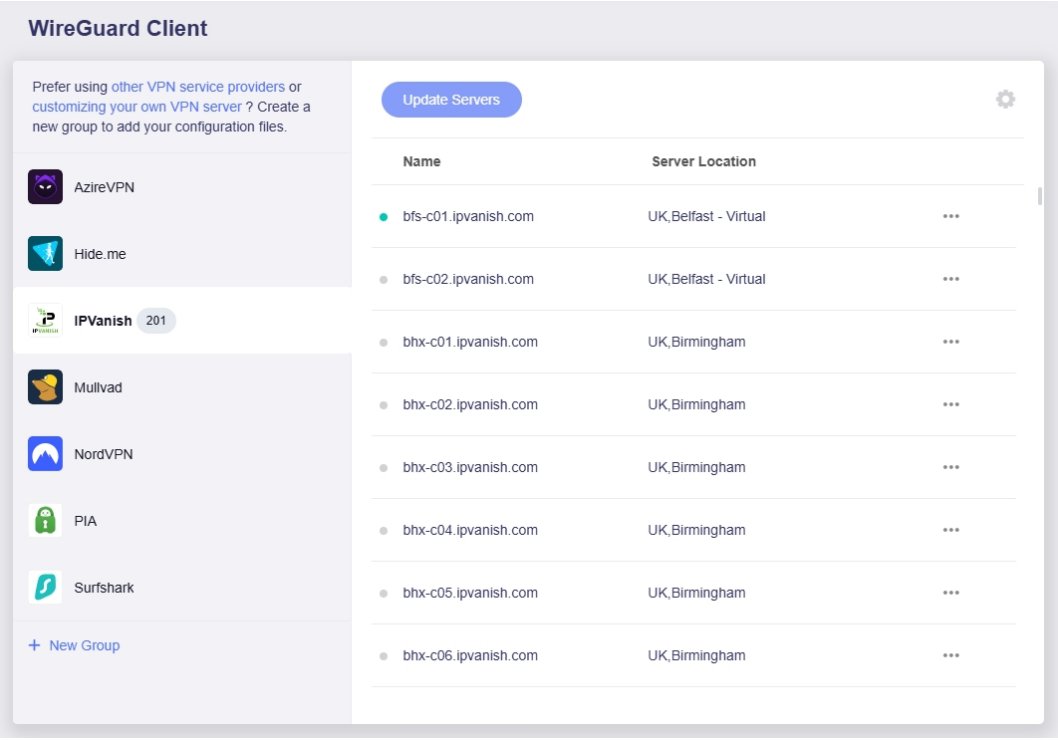
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



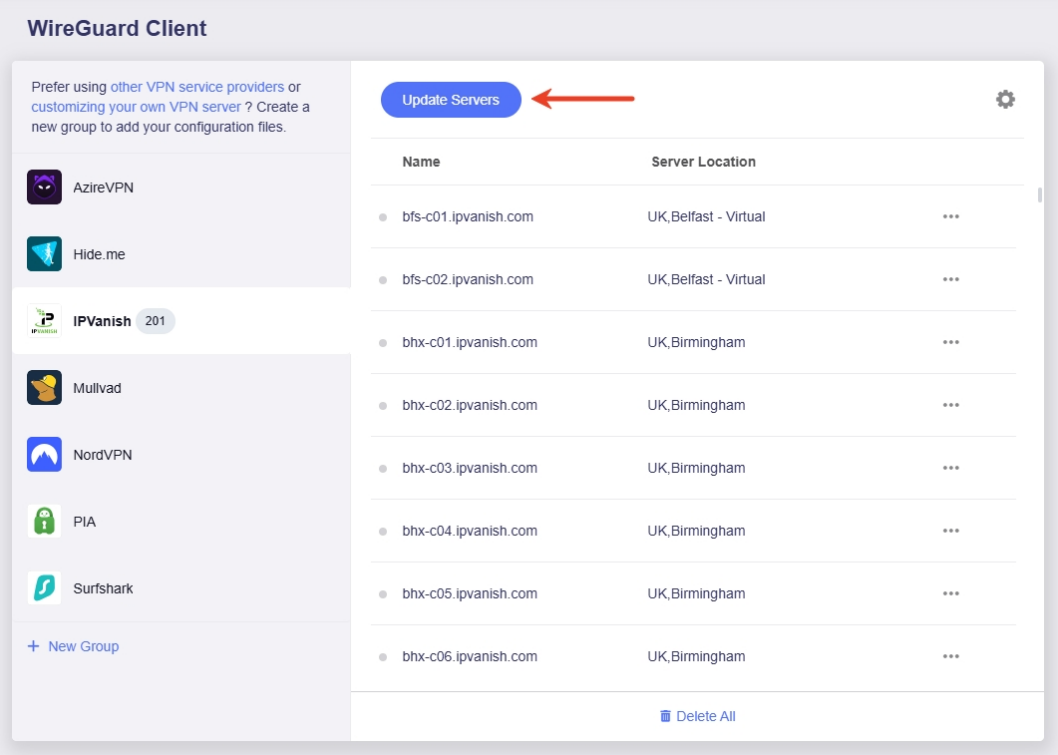
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



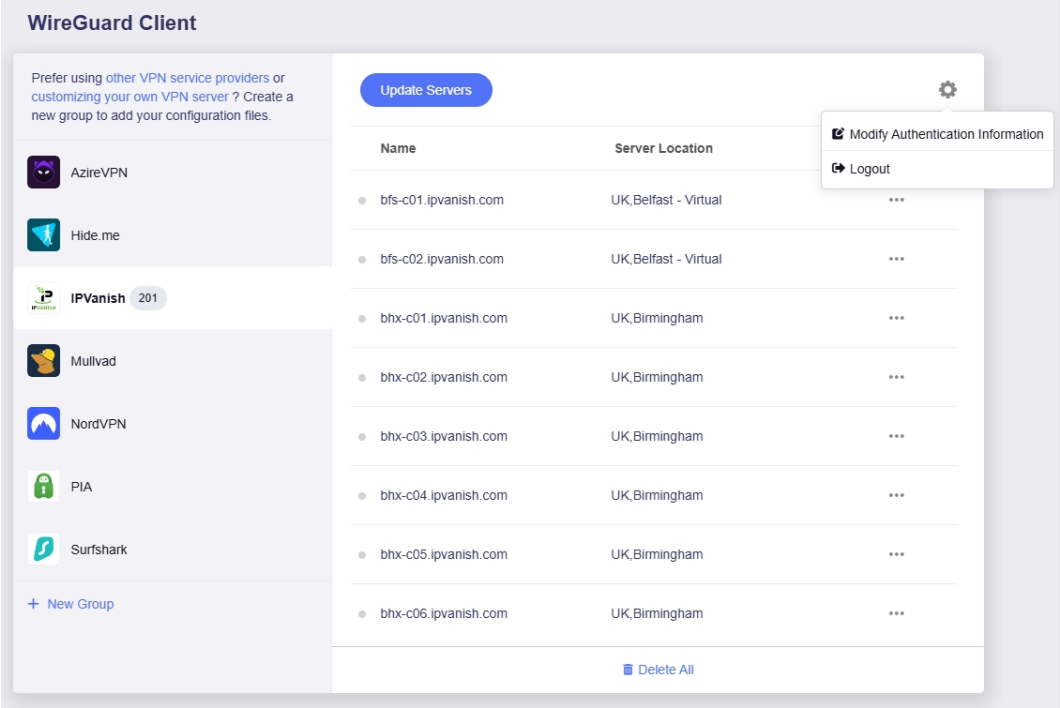
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

6. Server aktualisieren.

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

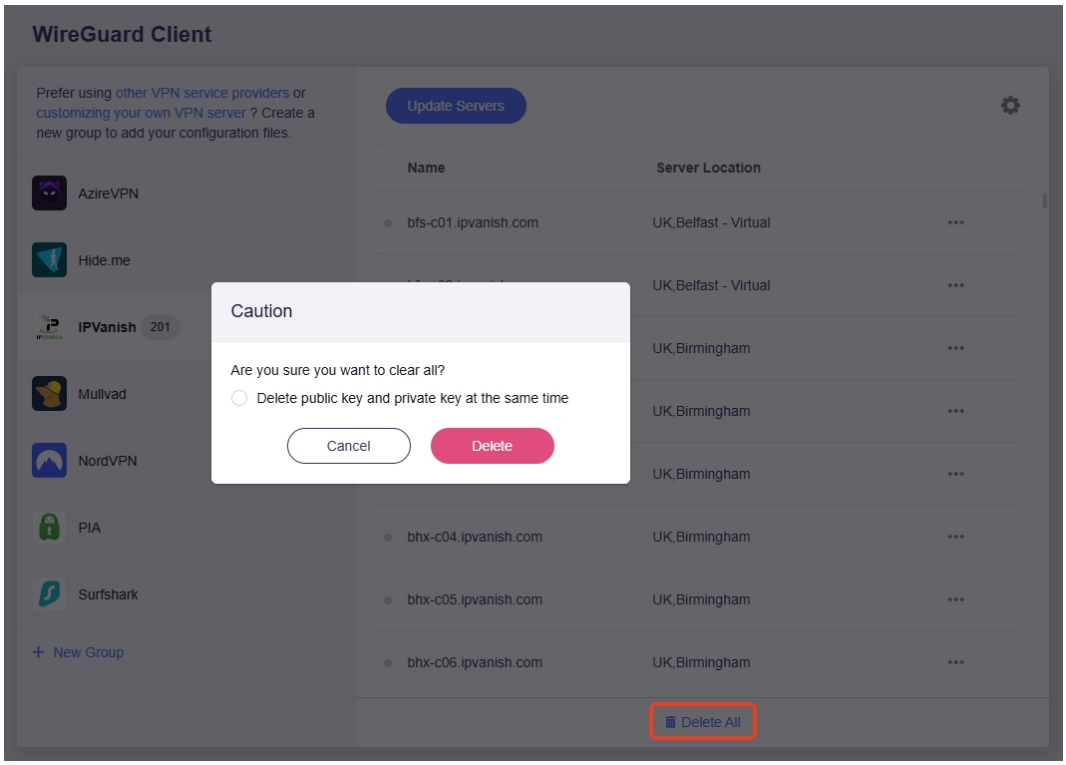


7. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



8. Alle Dateien löschen.

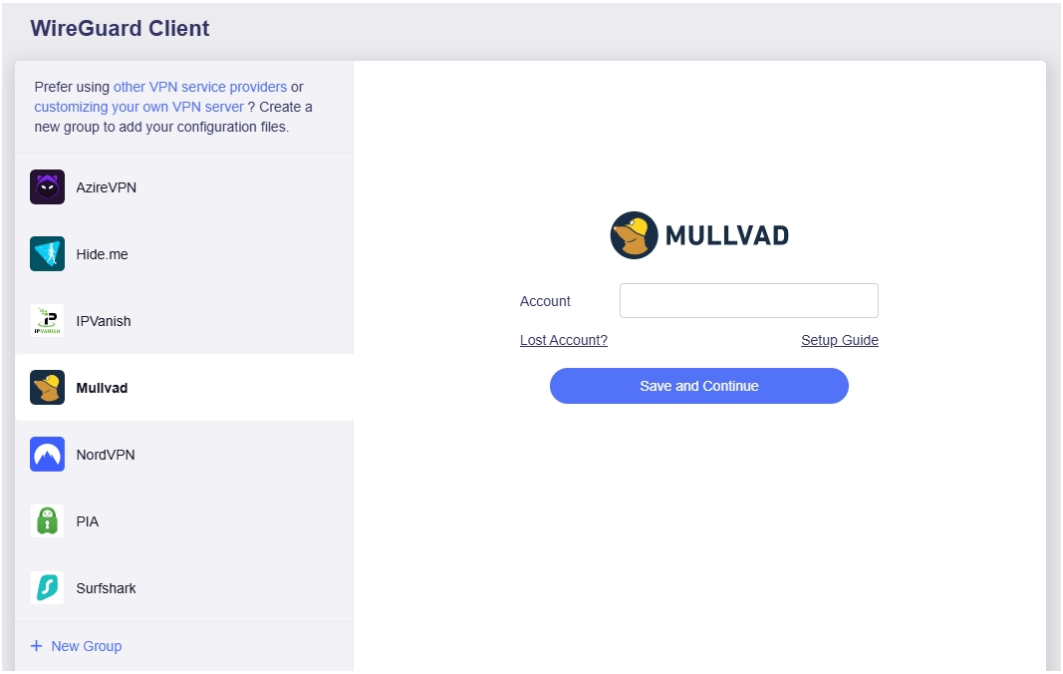
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



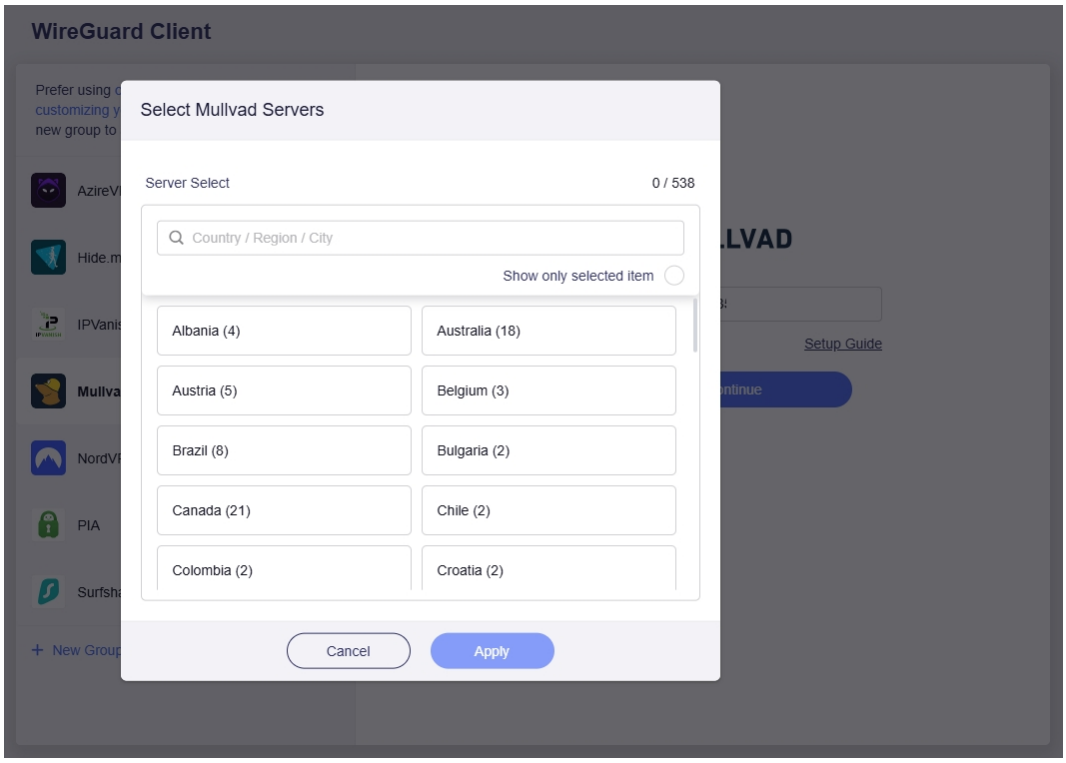
11.2.5 Mullvad einrichten

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

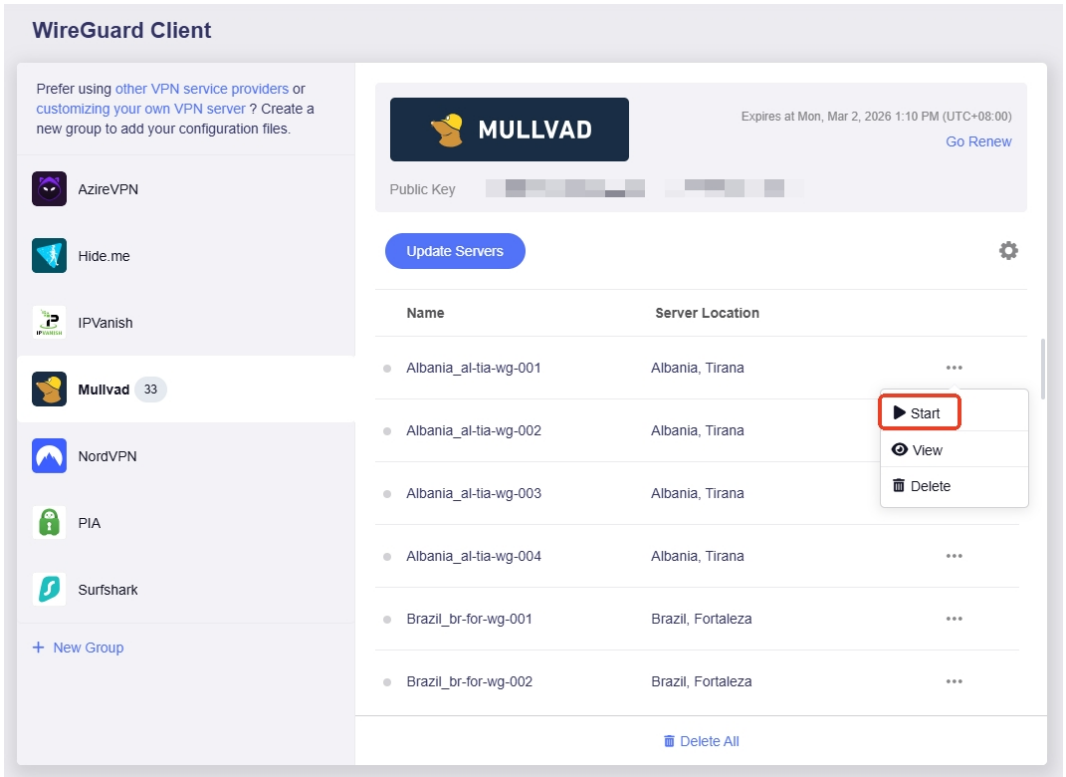
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Mullvad**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



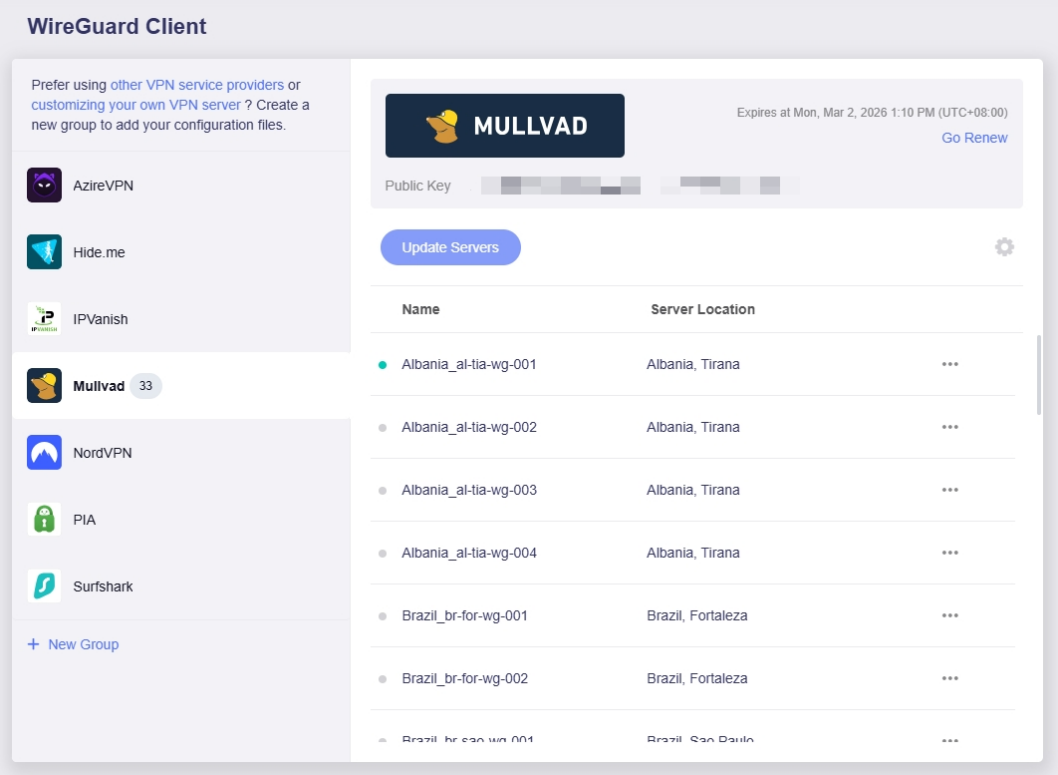
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



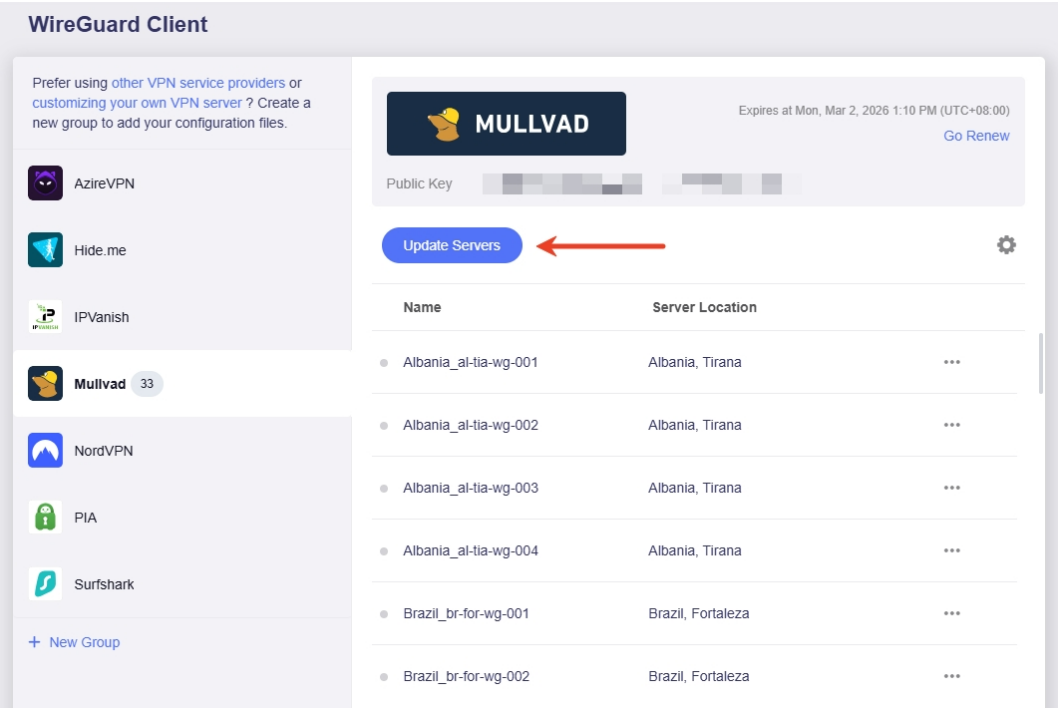
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

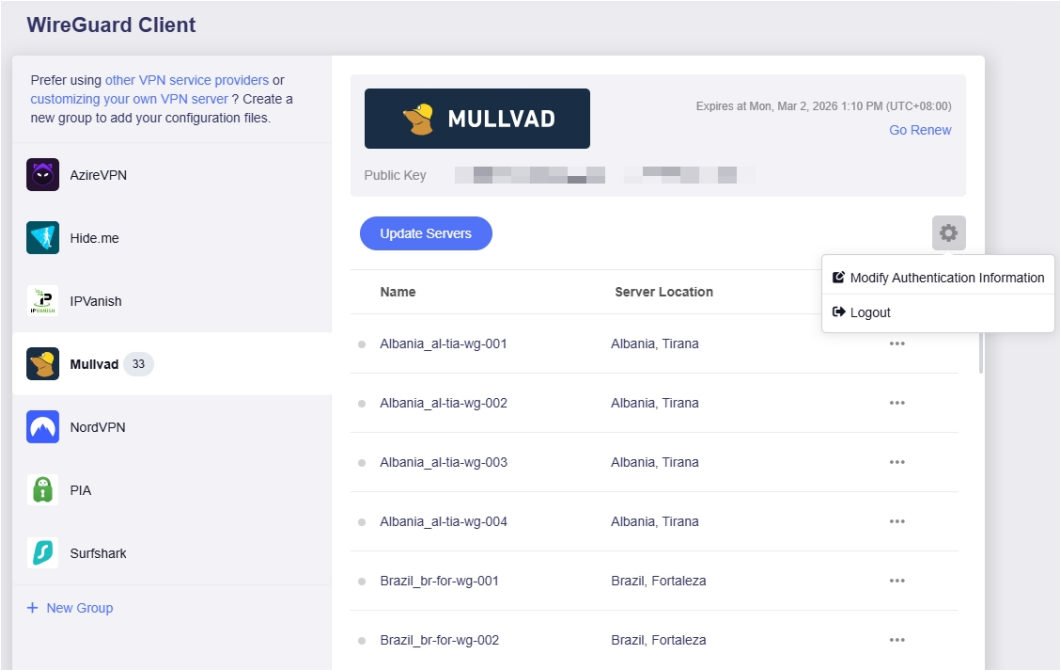
6. Server aktualisieren.

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



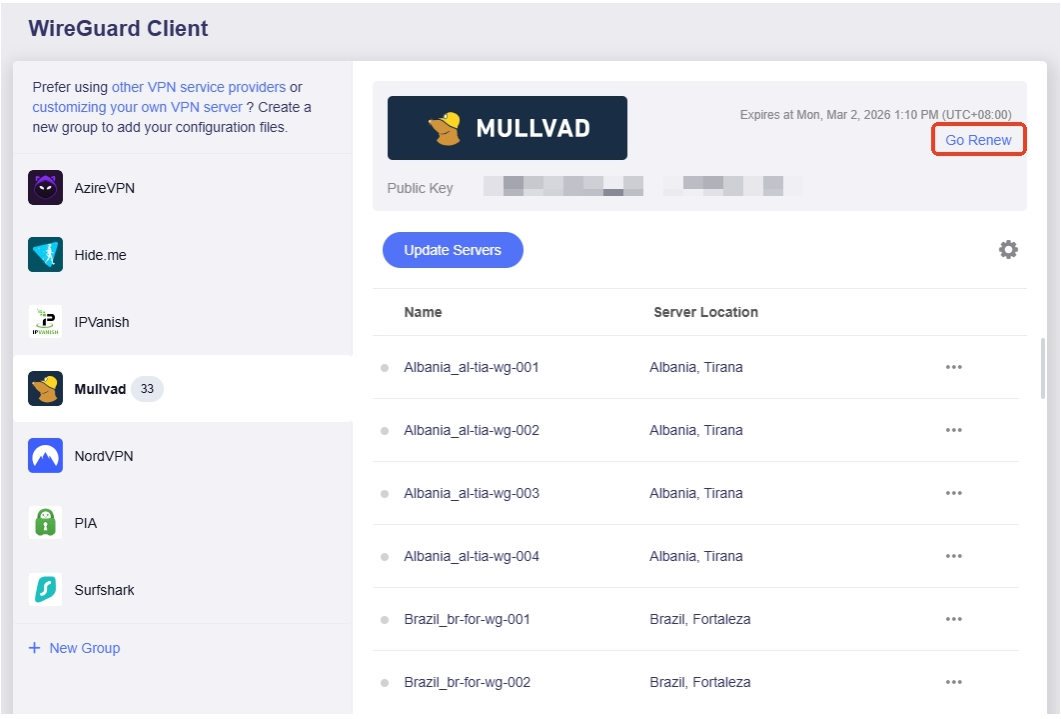
7. Zugangsdaten bearbeiten oder abmelden.

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



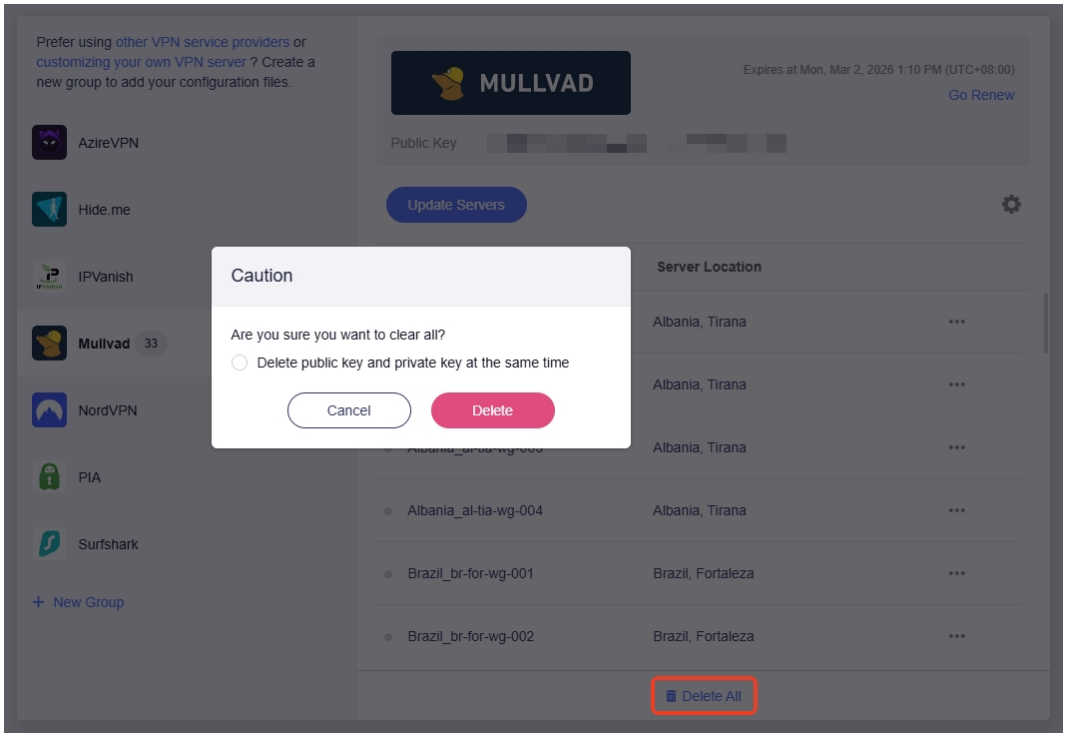
8. Abonnement verlängern.

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



9. Alle Dateien löschen.

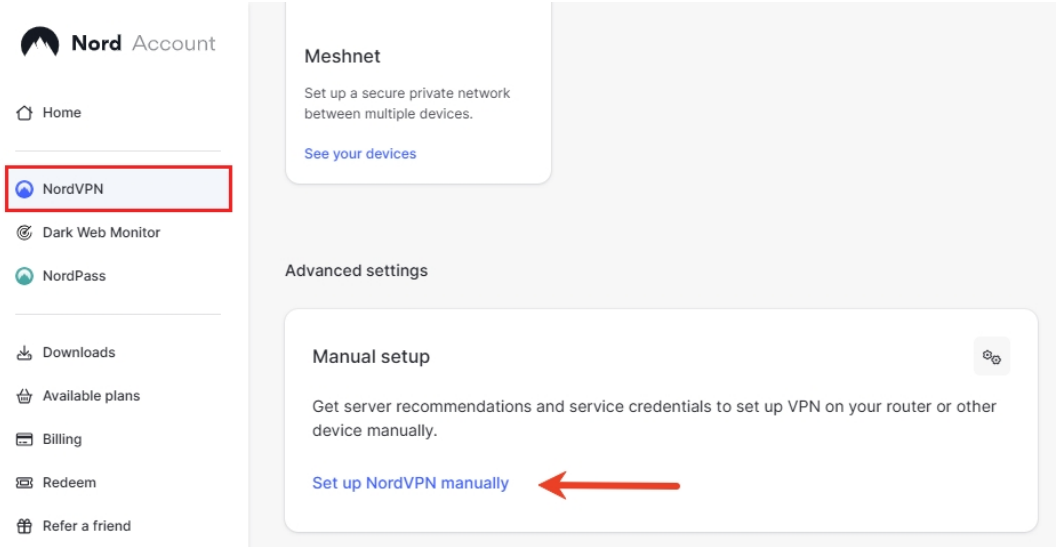
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



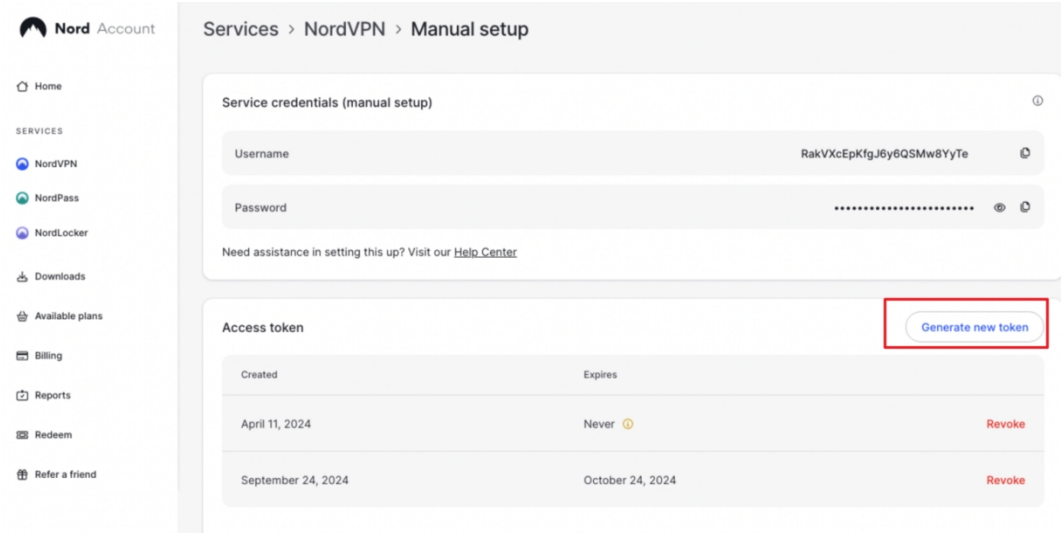
11.2.6 NordVPN einrichten

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

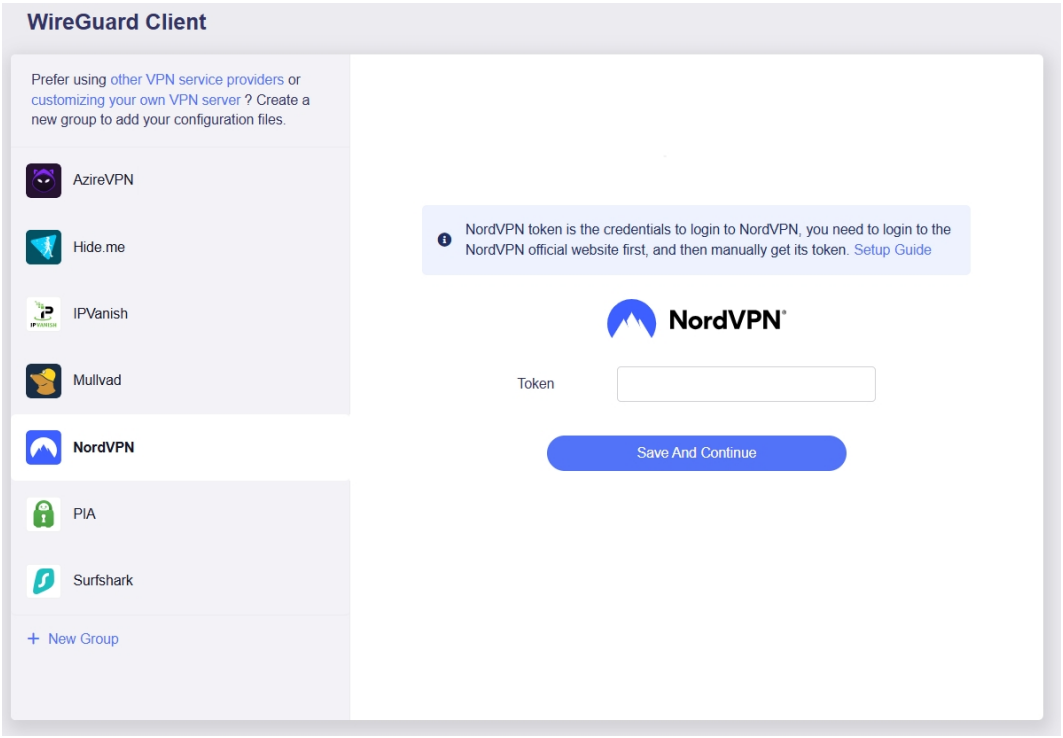
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



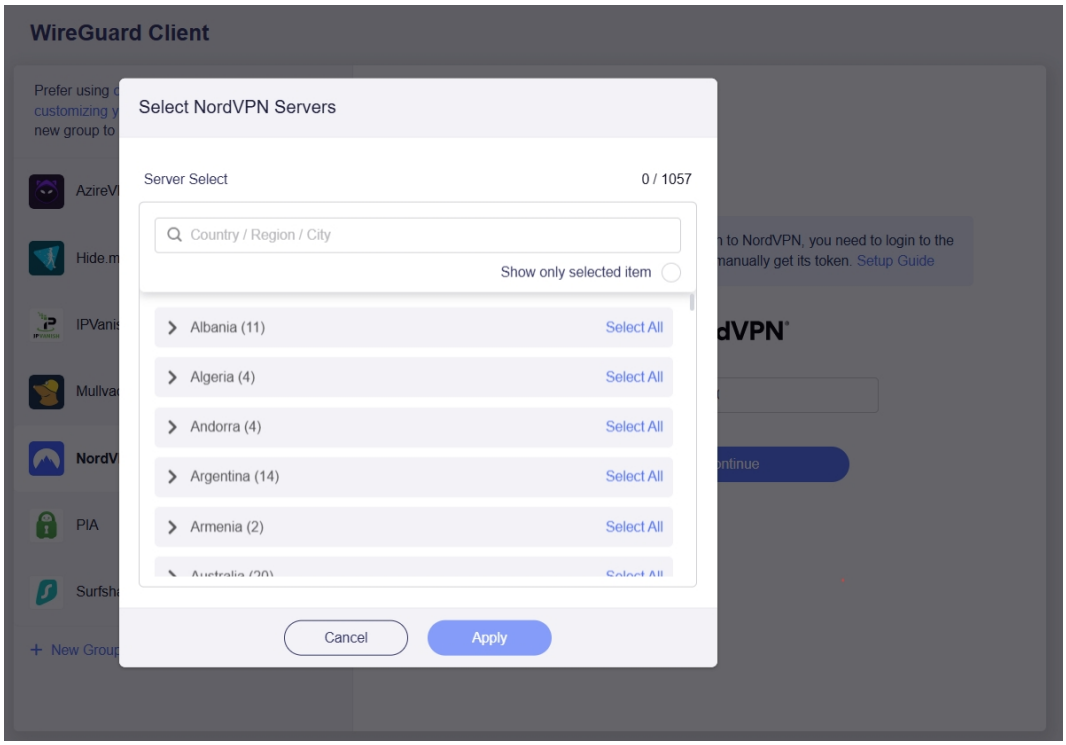
Dort finden Sie den Bereich **Access Token**. Erstellen Sie ein Zugriffstoken und kopieren Sie es zur späteren Verwendung.



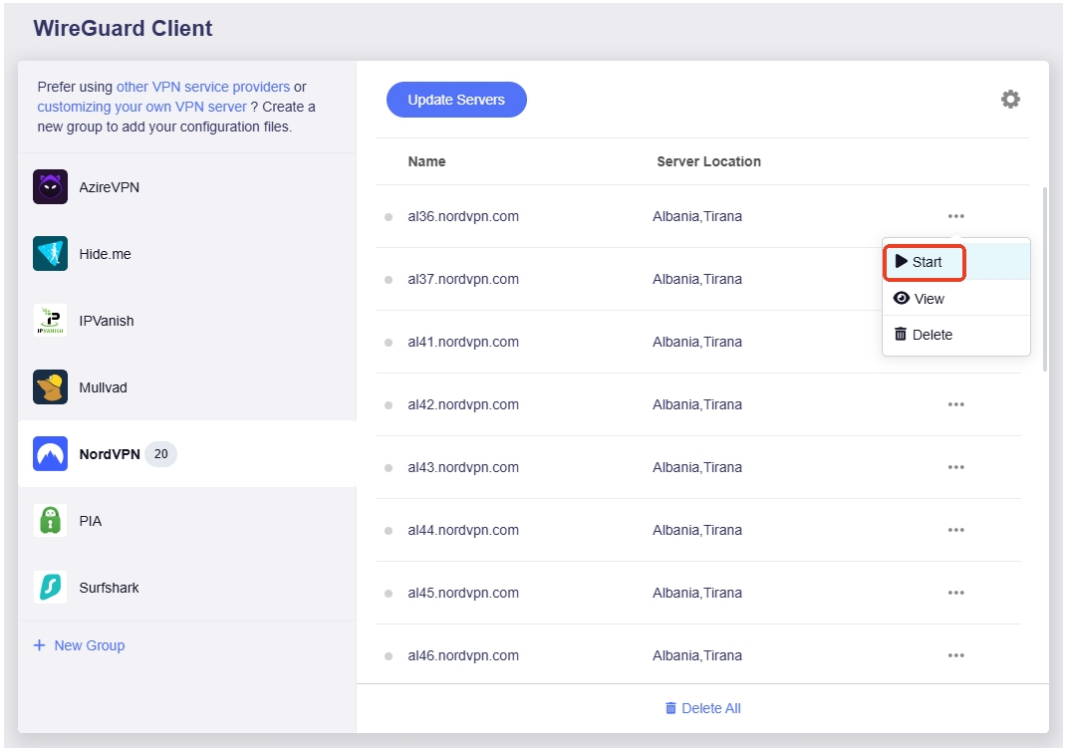
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **NordVPN**.
4. Geben Sie das Token ein und klicken Sie auf **Save and Continue**.



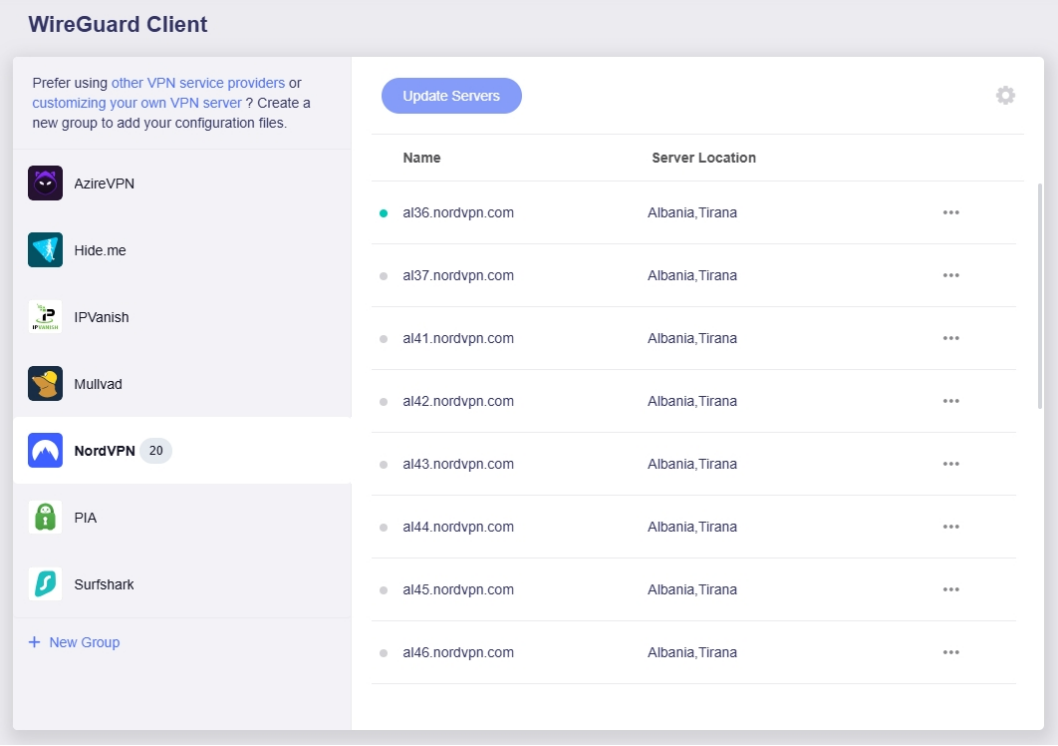
5. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



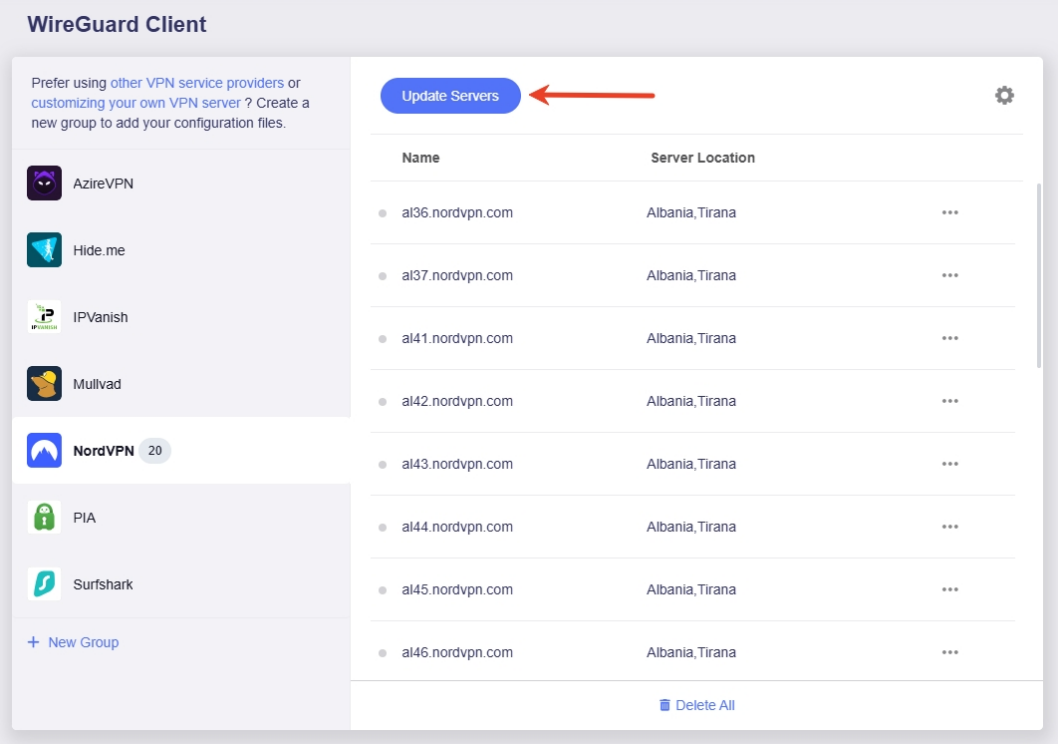
7. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

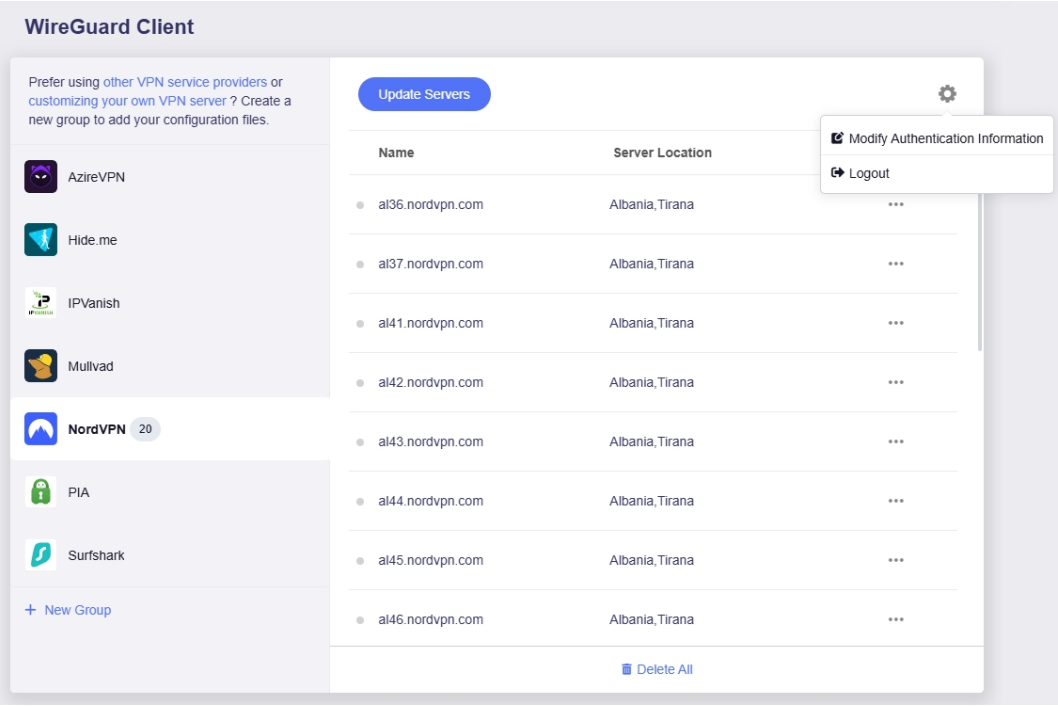
8. Server aktualisieren.

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



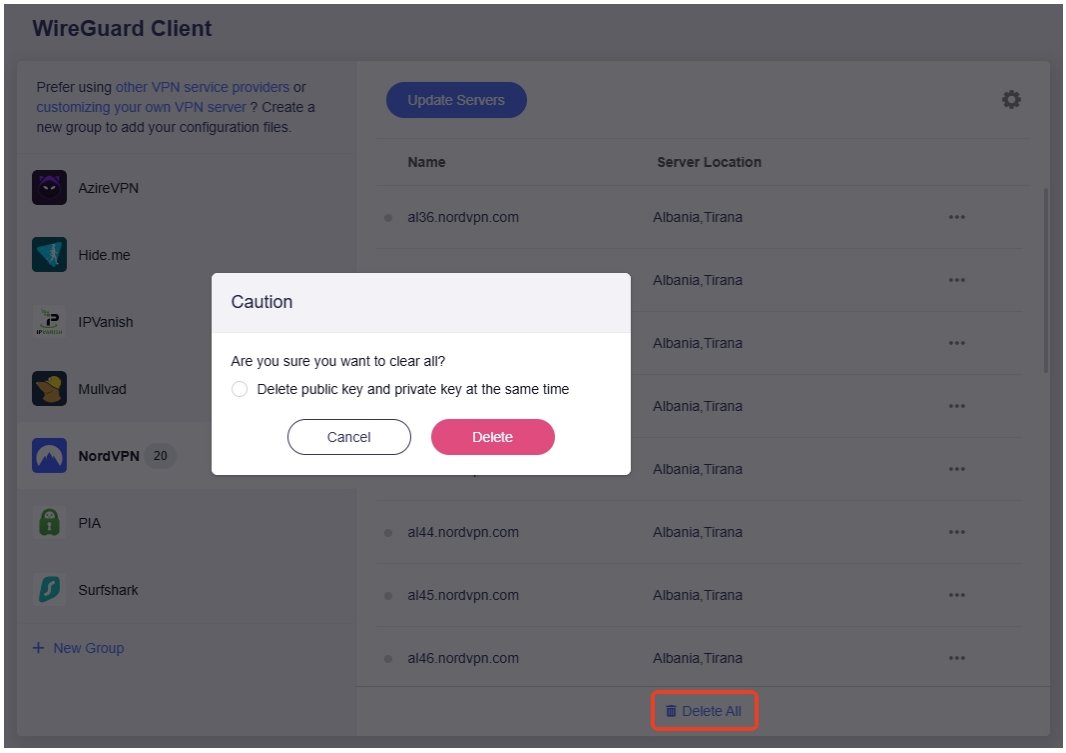
9. Zugangsdaten bearbeiten oder abmelden.

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



10. Alle Dateien löschen.

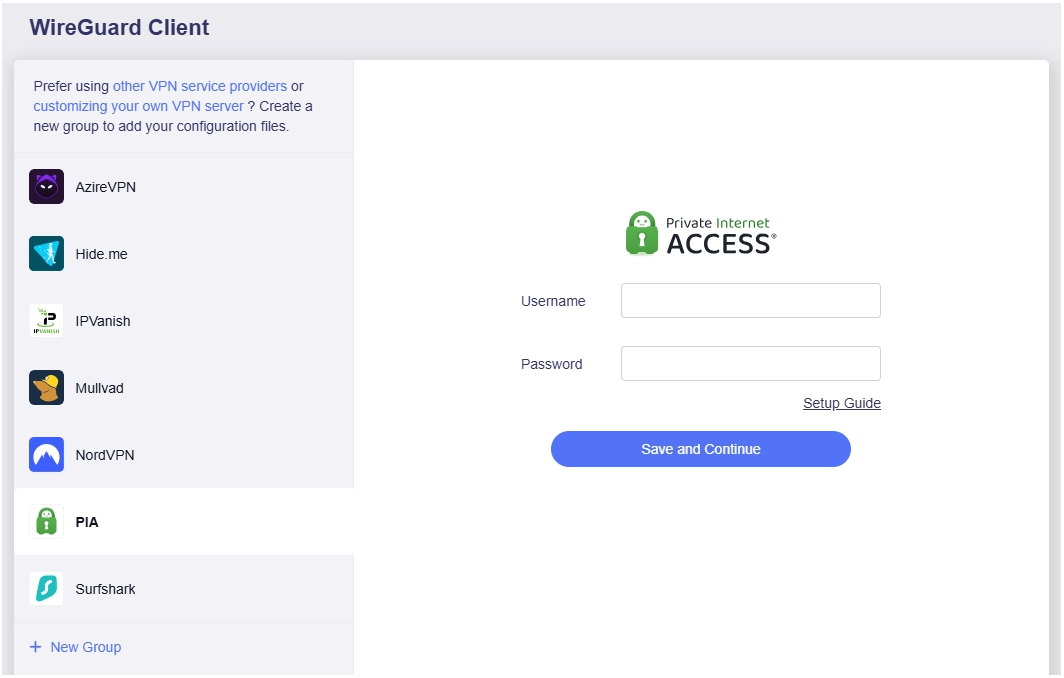
    Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


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 20
PIA
Surfshark
New Group
Update Servers
Name
Server Location
al36.nordvpn.com
Albania,Tirana
Albania,Tirana
Albania,Tirana
Albania,Tirana
Albania,Tirana
al44.nordvpn.com
Albania,Tirana
al45.nordvpn.com
Albania,Tirana
al46.nordvpn.com
Albania,Tirana
Delete All
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete

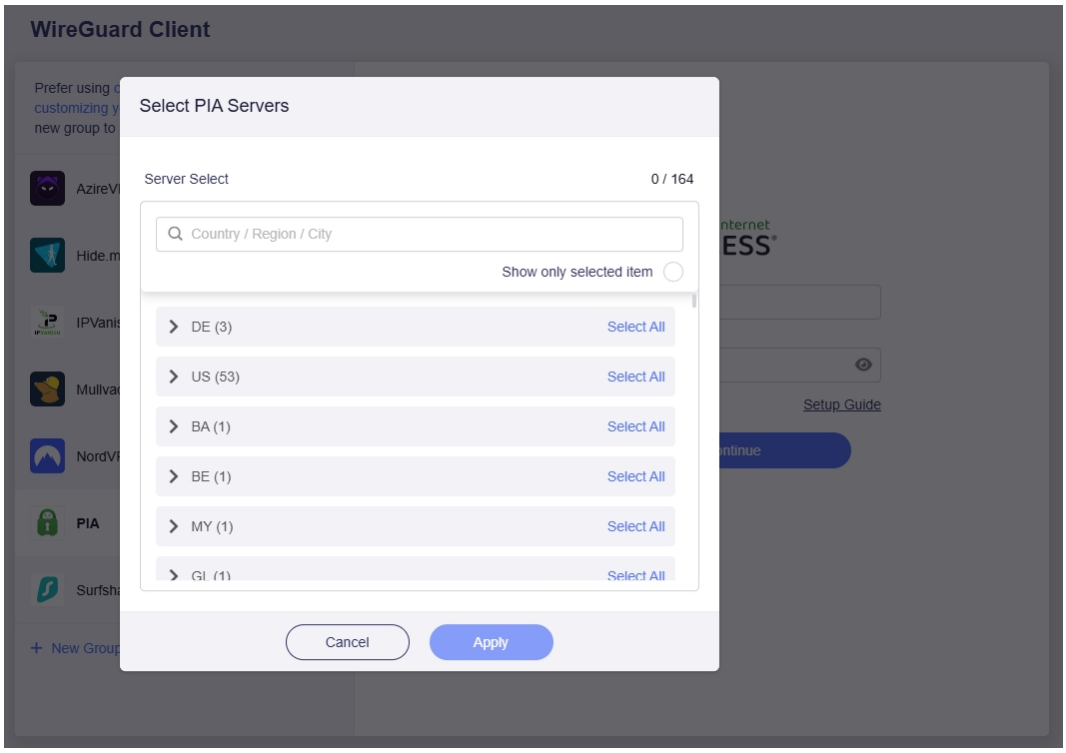
11.2.7 PIA (Private Internet Access) einrichten

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

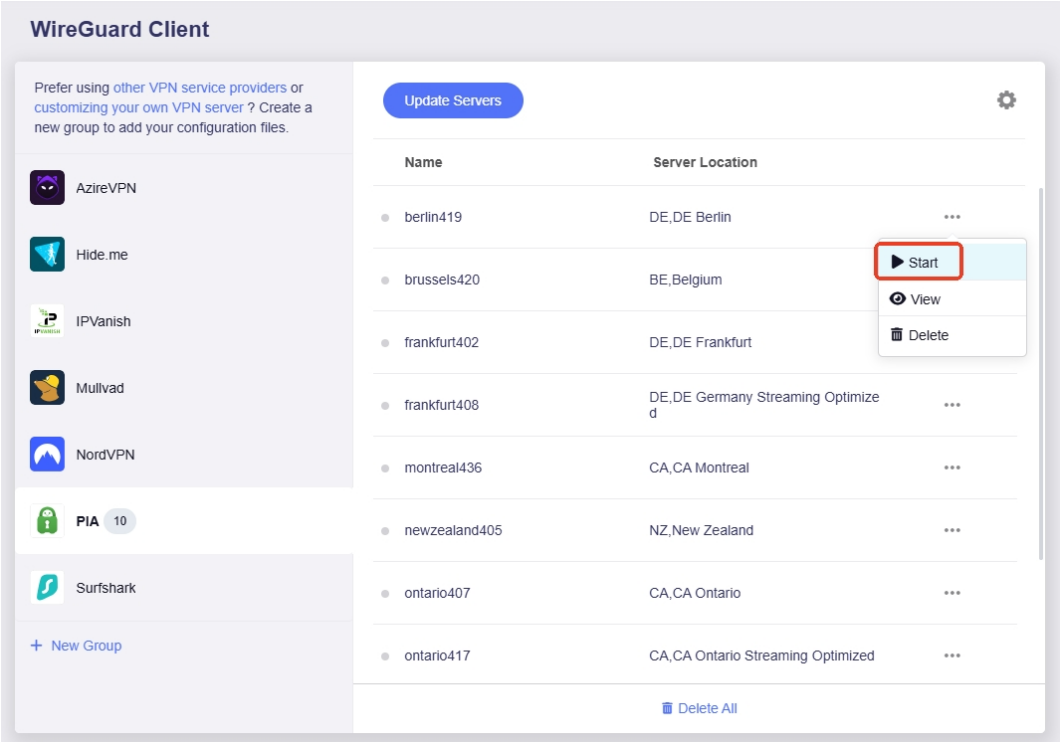
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **PIA**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



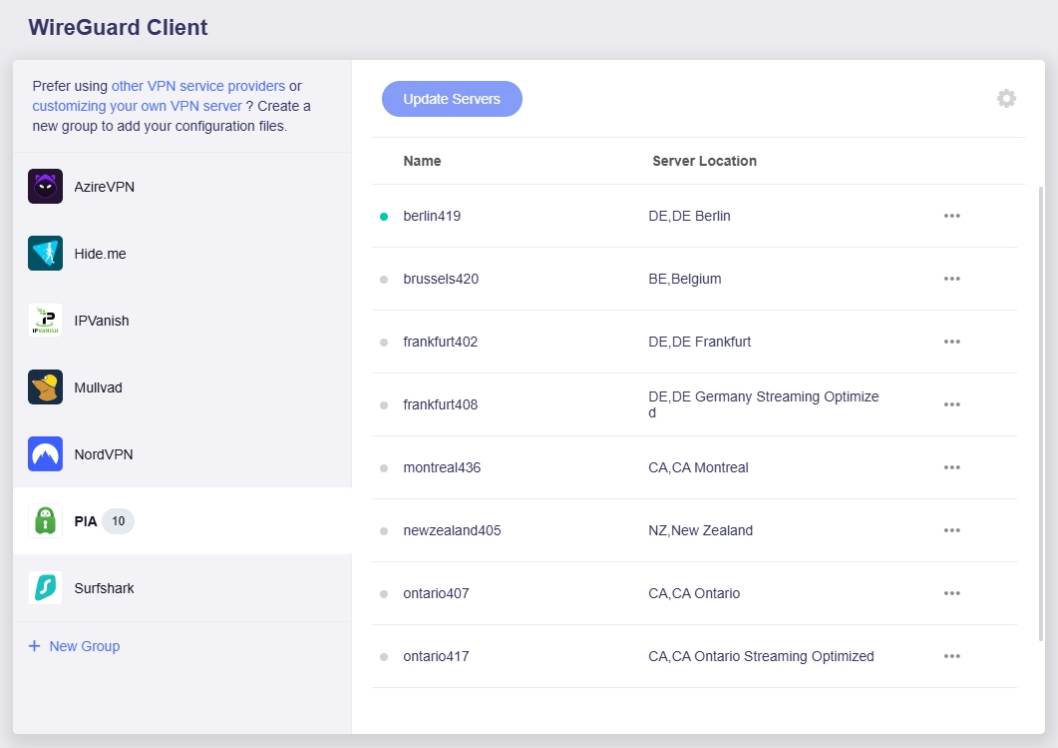
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



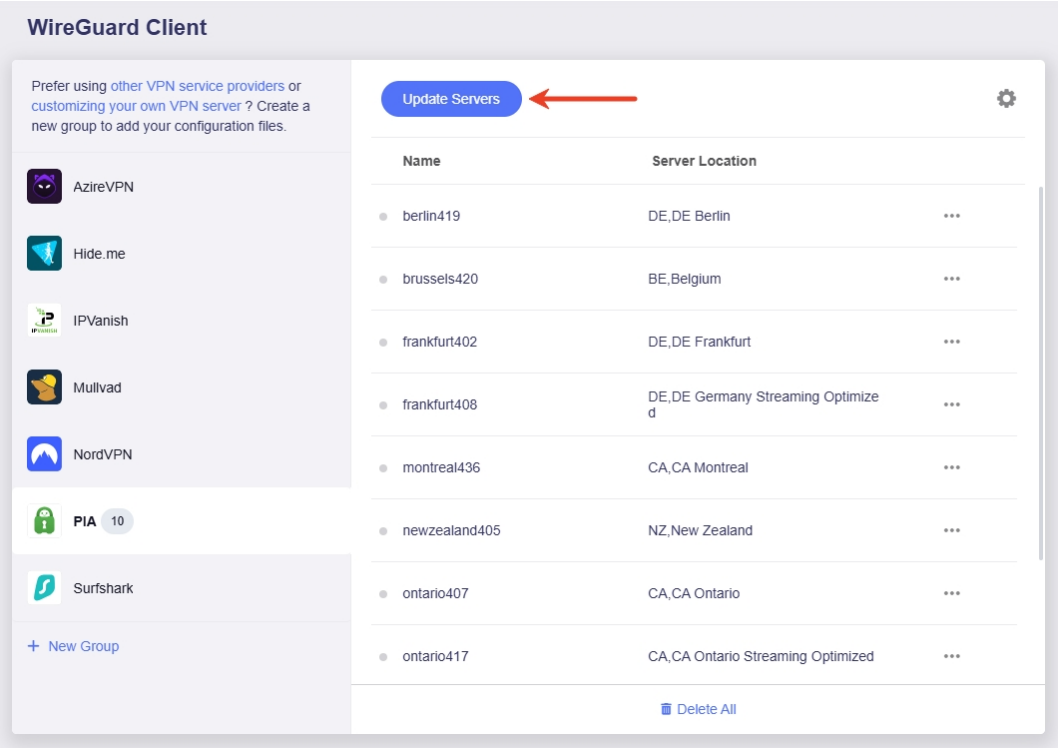
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

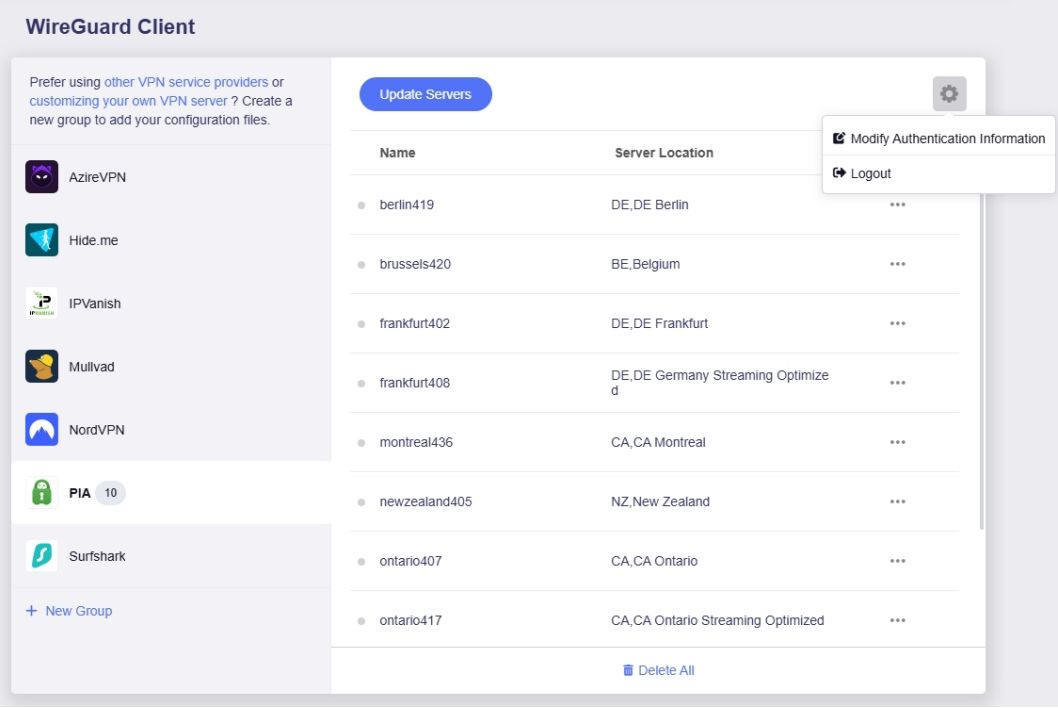
6. Server aktualisieren.

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



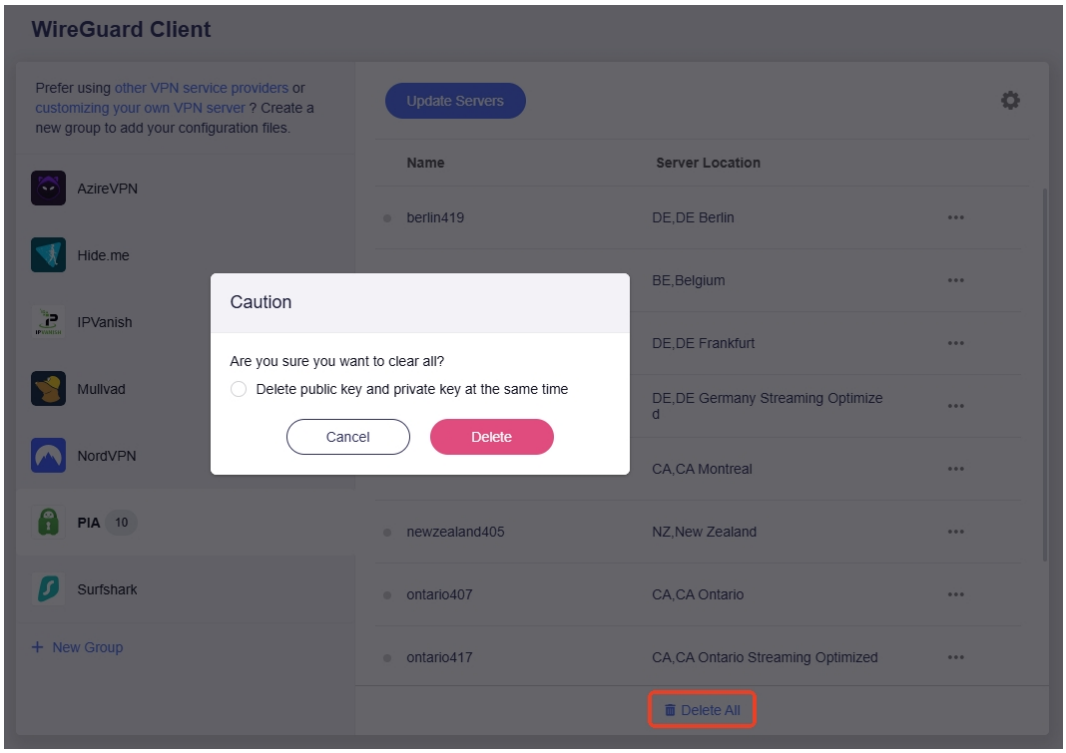
7. Zugangsdaten bearbeiten oder abmelden.

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



8. Alle Dateien löschen.

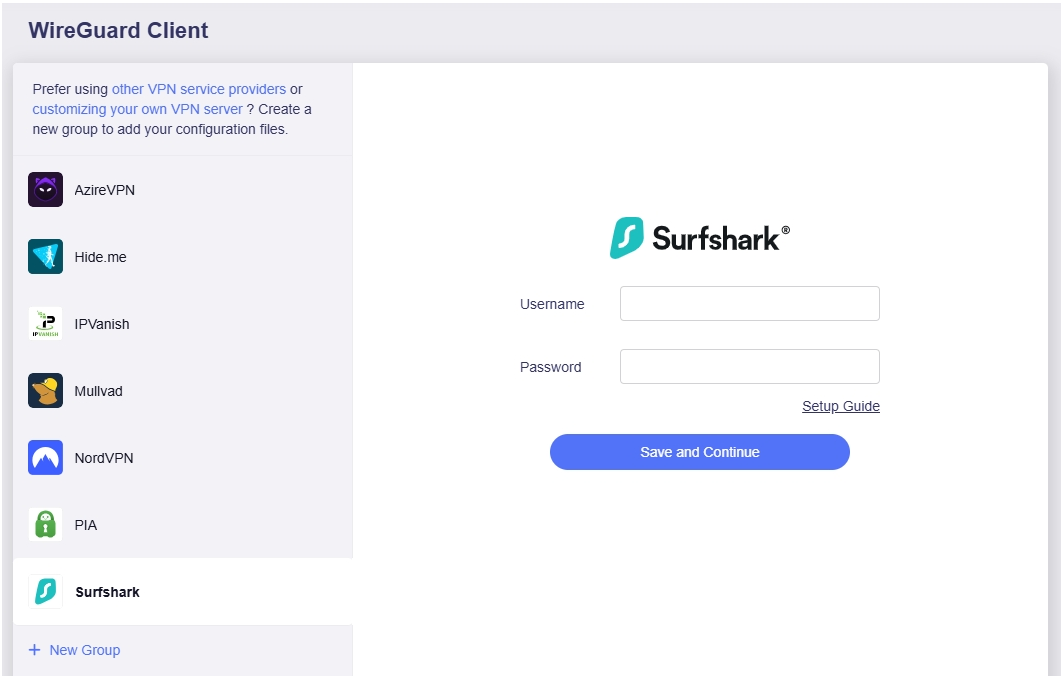
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
Update Servers
AzireVPN
Hide.me
IPVanish
Mullvad
NordVPN
PIA 10
Surfshark
New Group
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

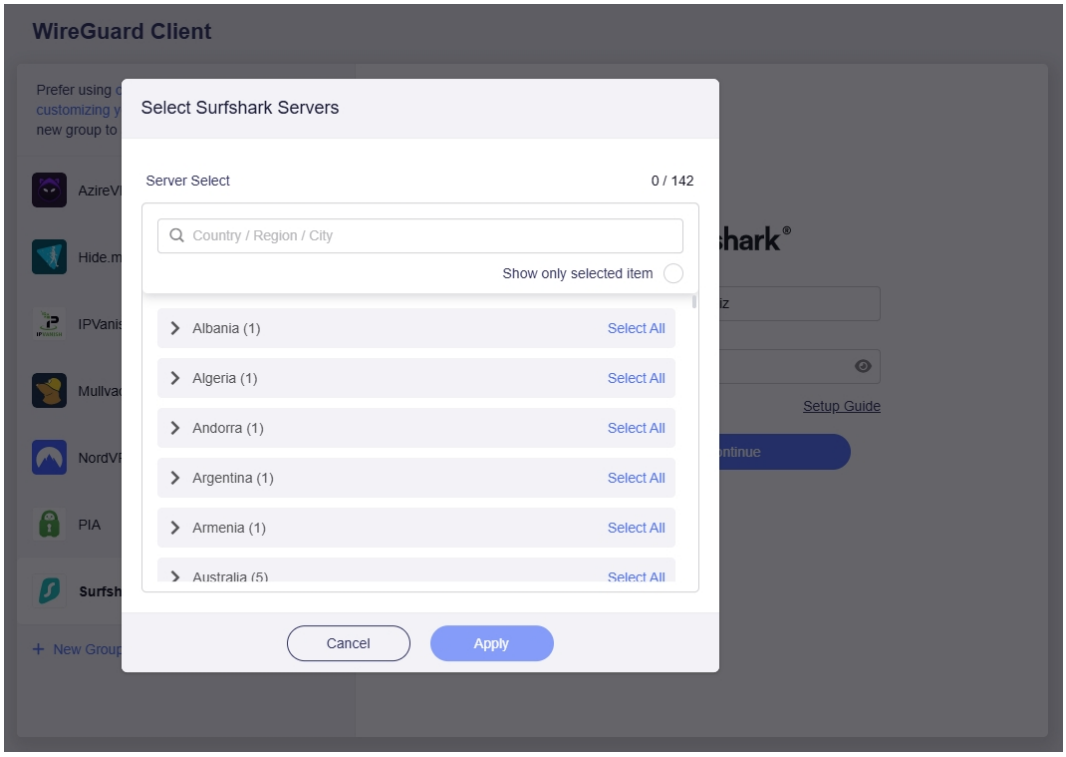
11.2.8 Surfshark einrichten

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

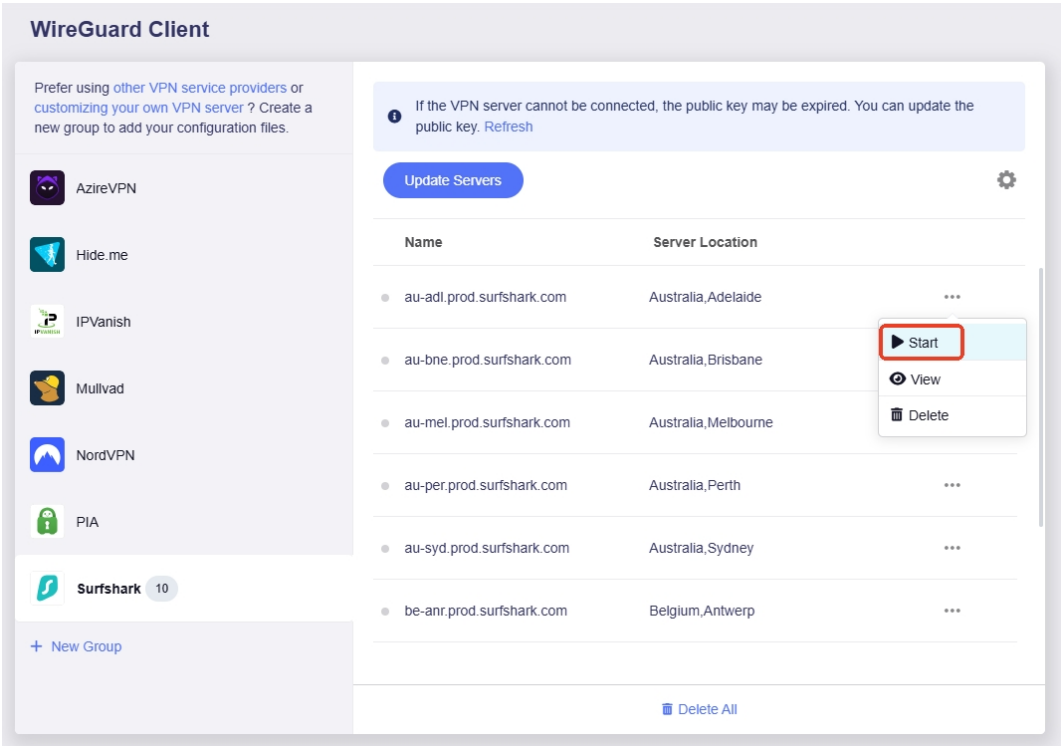
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Surfshark**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



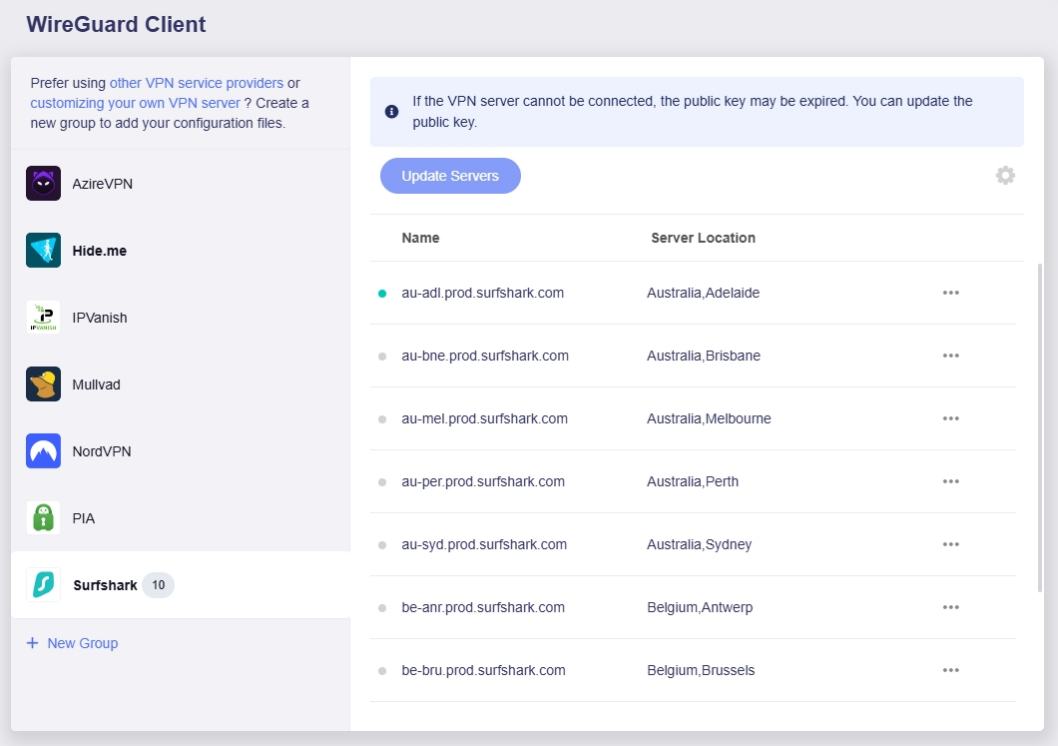
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



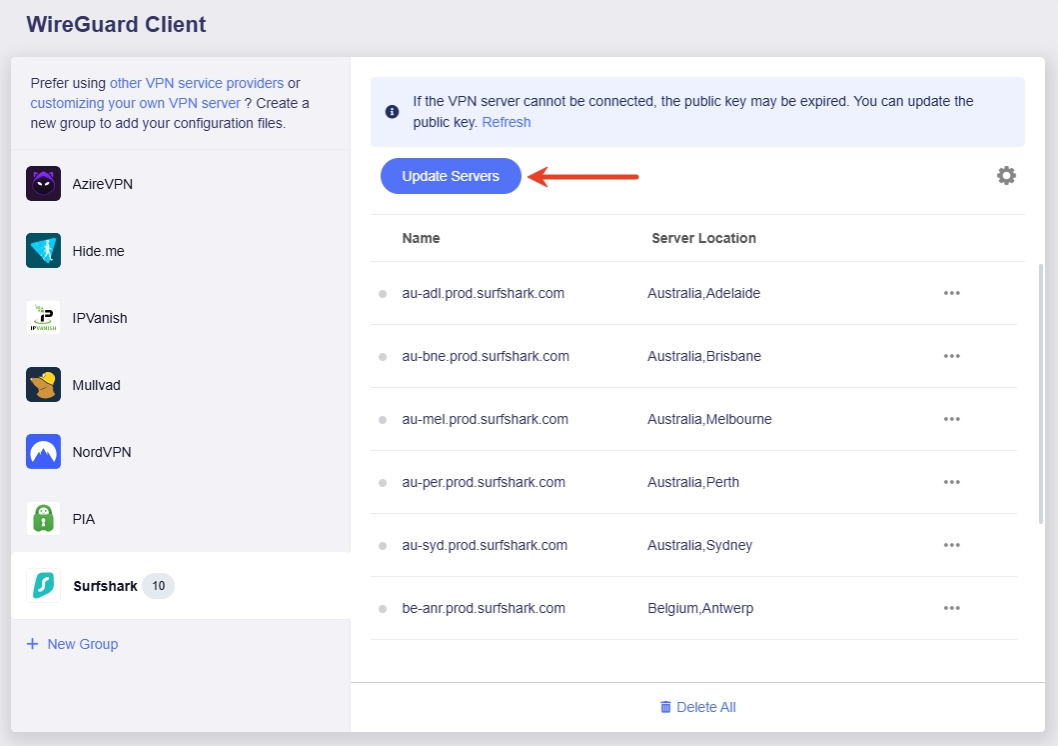
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

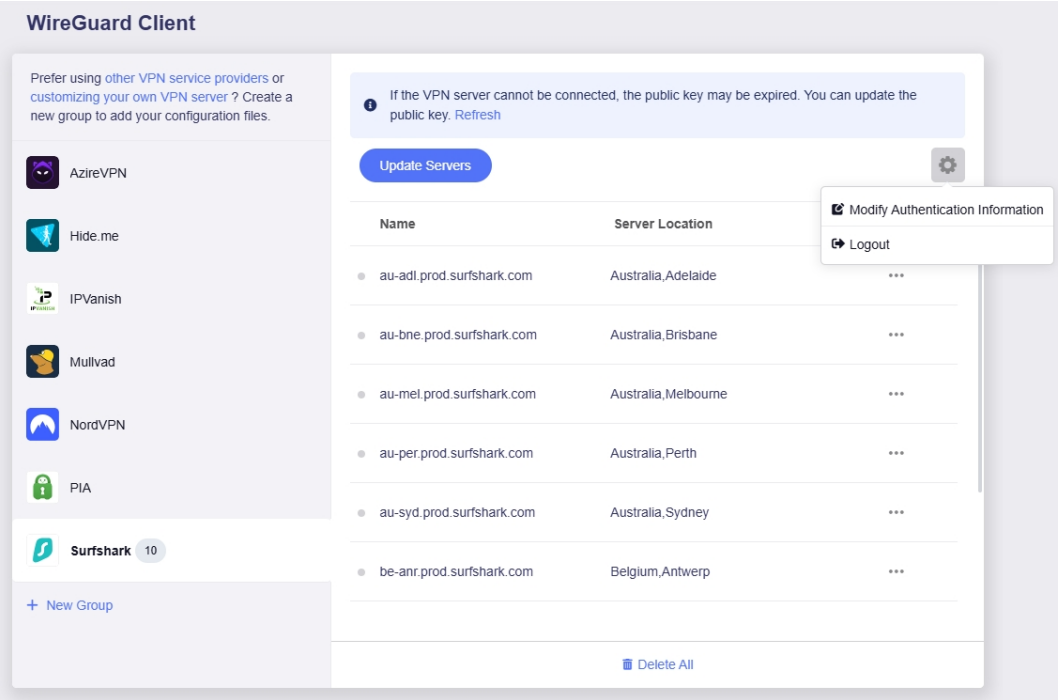
6. Server aktualisieren.

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



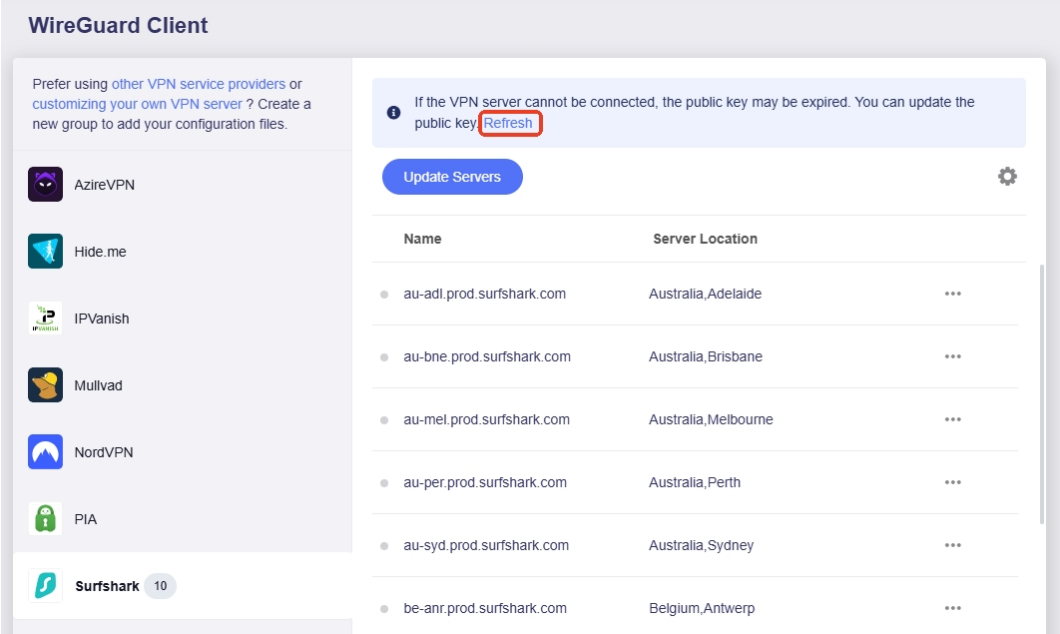
7. Zugangsdaten bearbeiten oder abmelden.

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



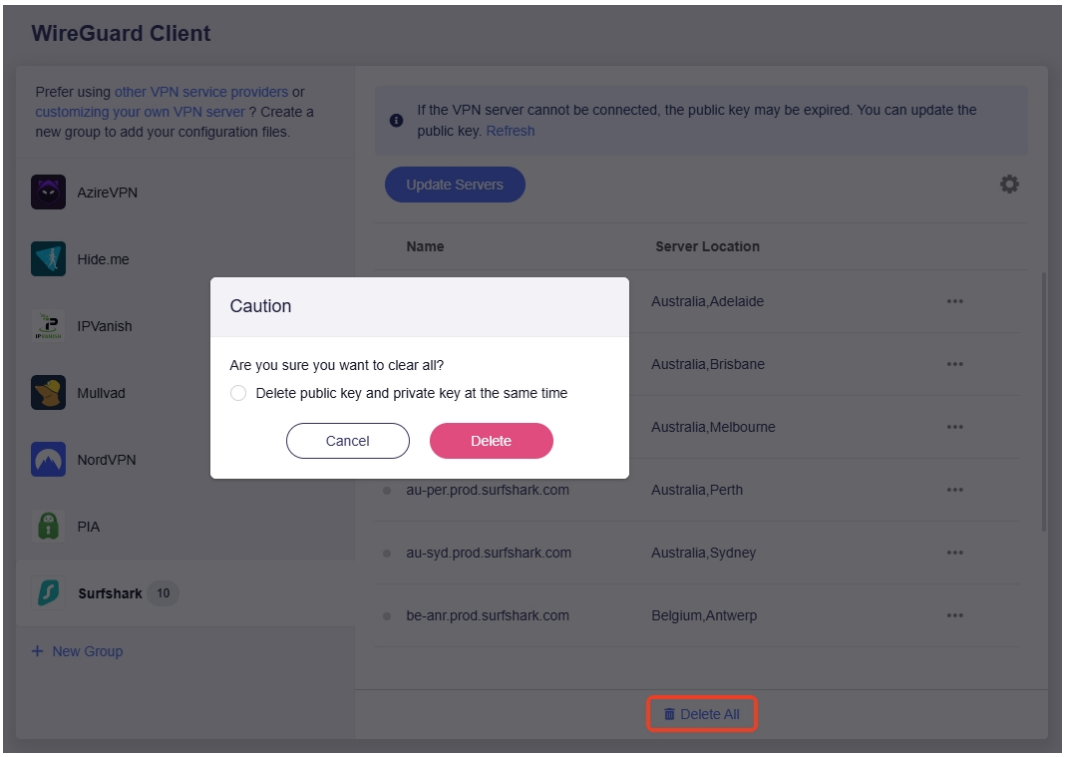
8. Aktualisieren.

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.

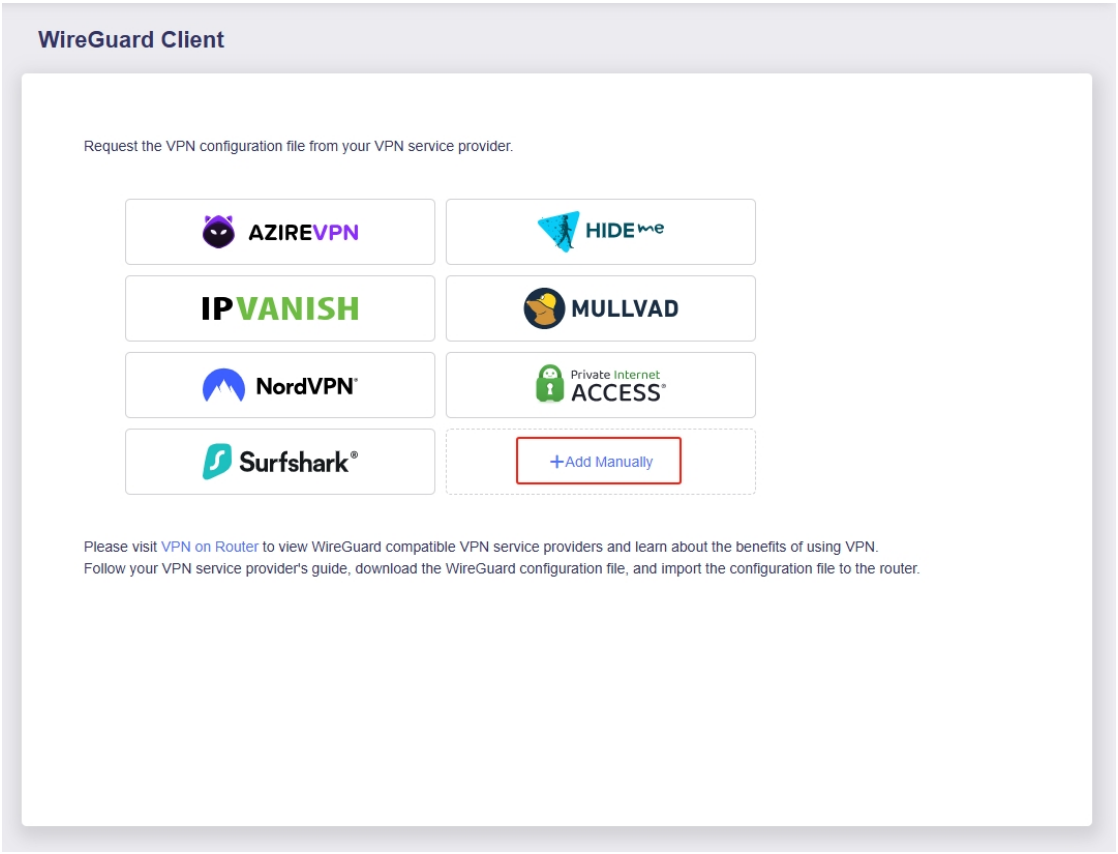


11.2.9 WireGuard-Client manuell einrichten (andere Anbieter)

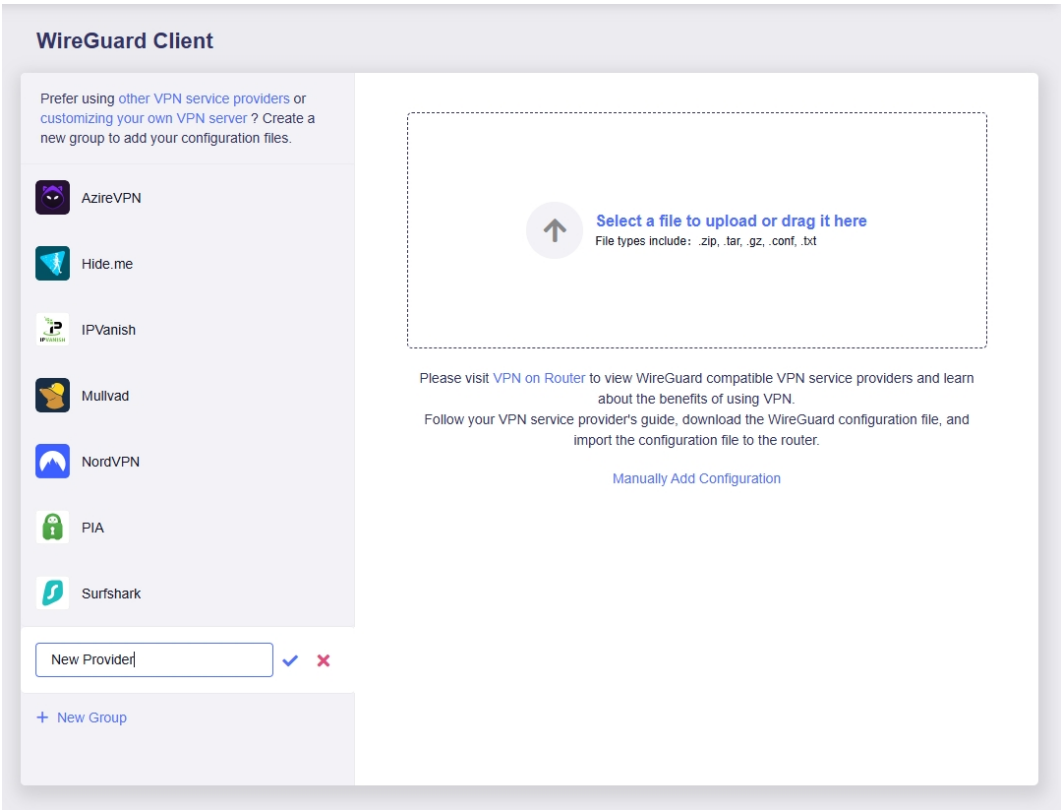
Wenn Ihr WireGuard-Anbieter nicht in die Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den WireGuard-Client einzurichten. Falls Sie nicht wissen, wie Sie die Dateien herunterladen,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

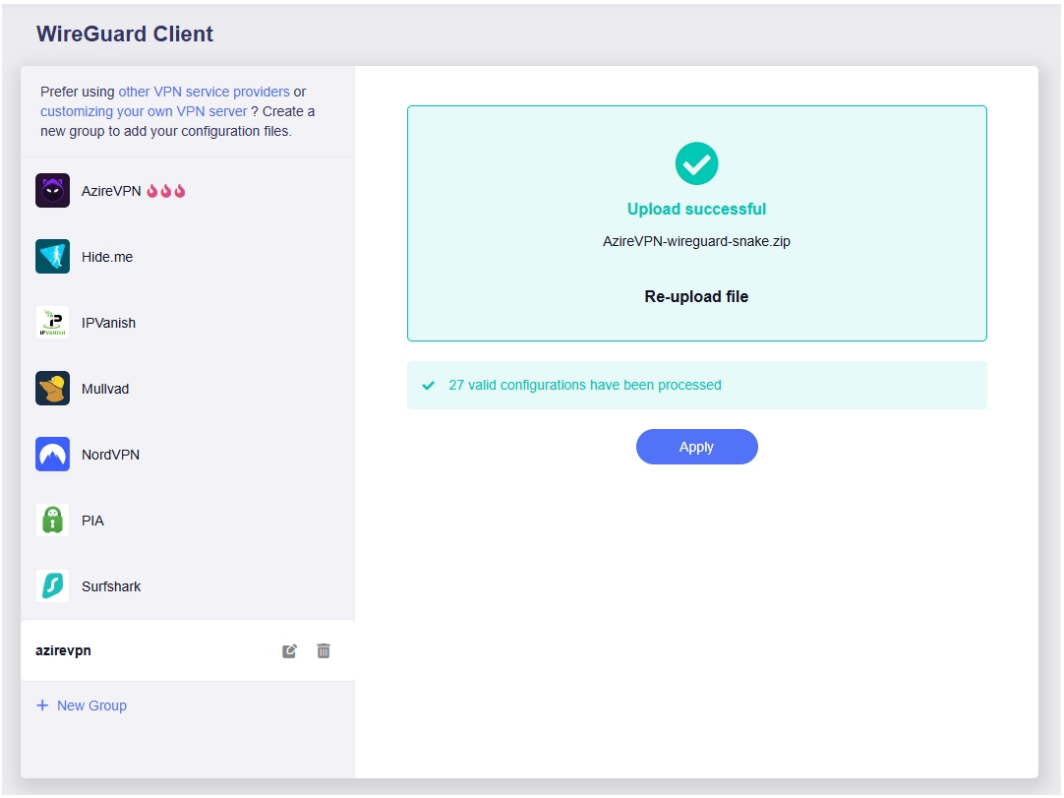
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Add Manually**.



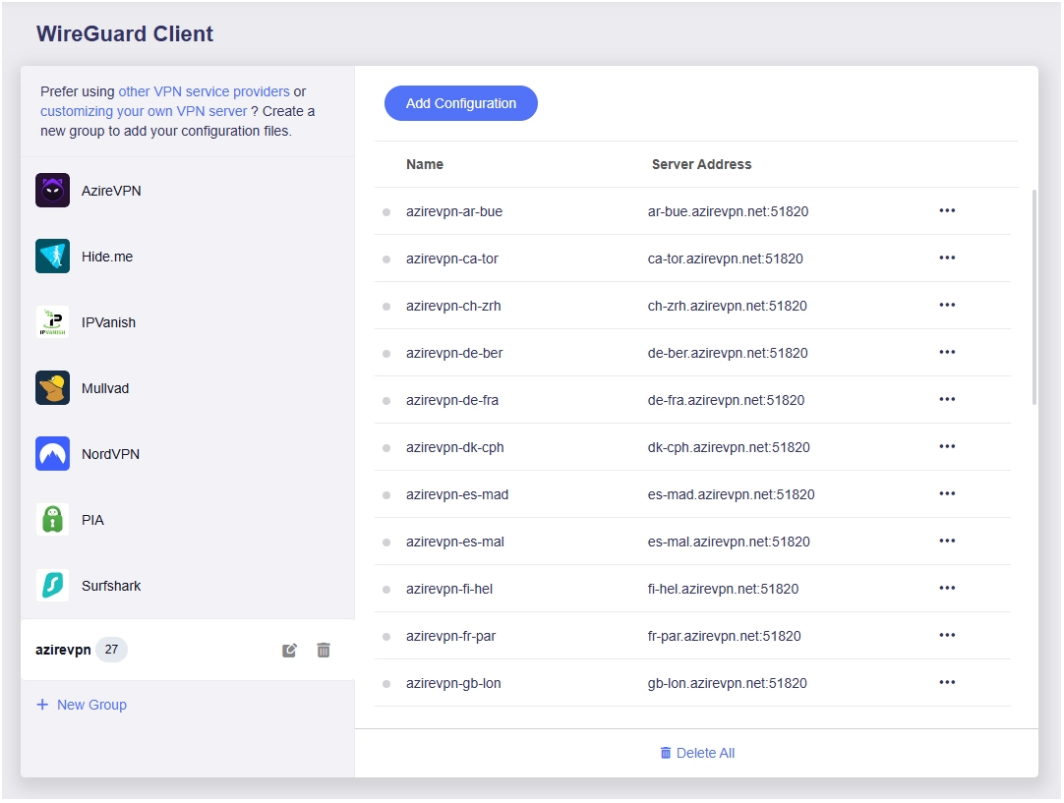
2. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



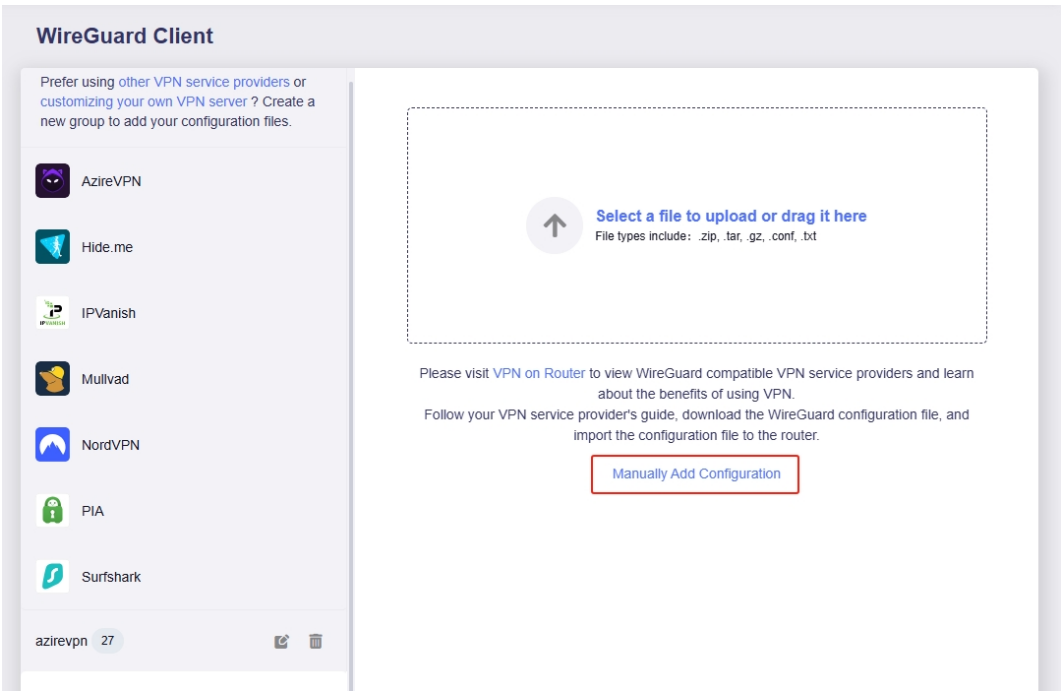
3. Klicken Sie auf den Upload-Bereich, laden Sie Ihre WireGuard-Konfigurationsdatei hoch und klicken Sie auf **Apply**. Unterstützte Formate: zip, tar, gz, conf und txt.

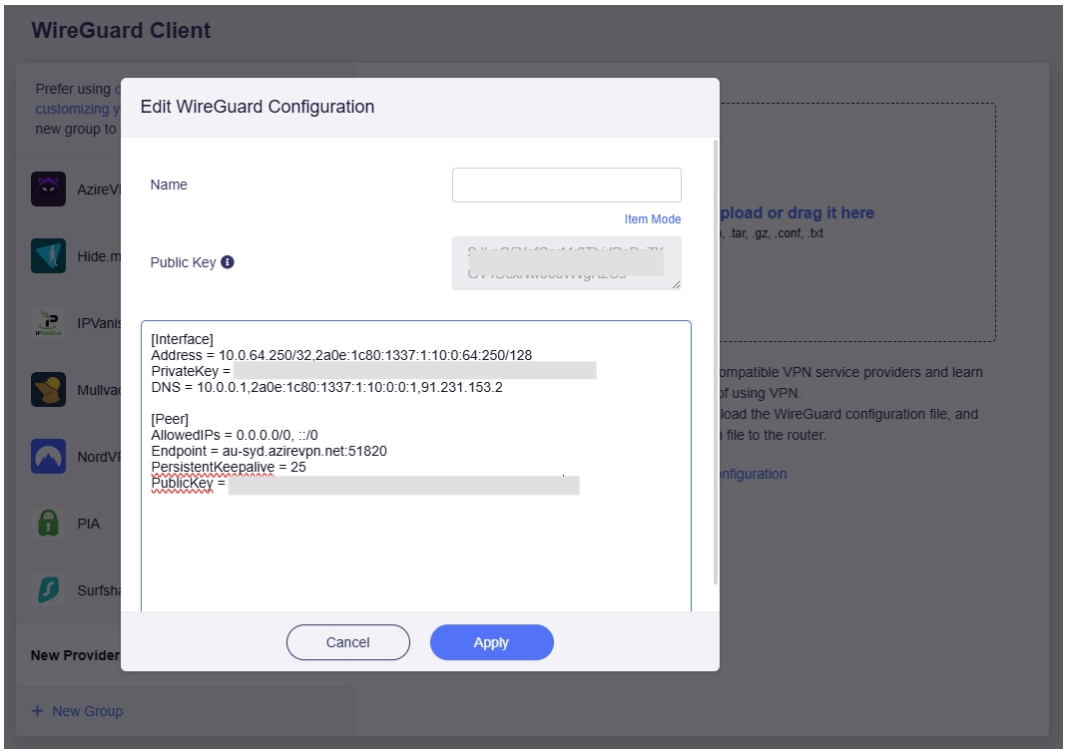


Wenn Sie eine komprimierte Datei mit mehreren Konfigurationsdateien hochladen, wird sie wie unten gezeigt automatisch entpackt.

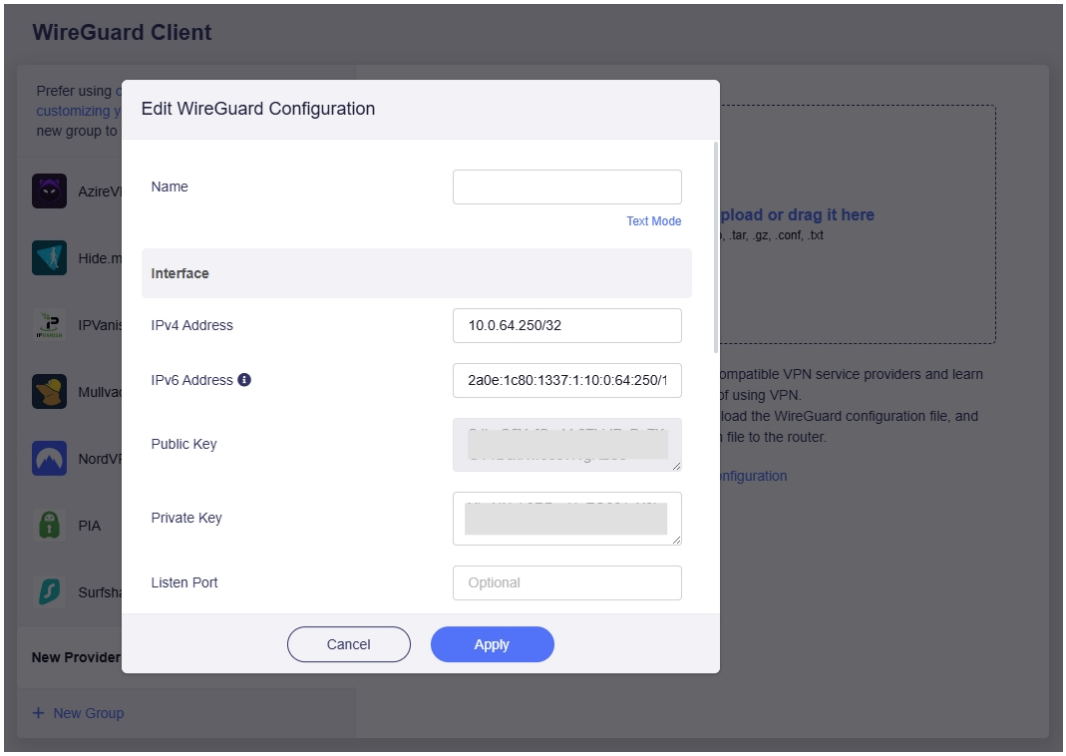


Alternativ klicken Sie unten im Upload-Bereich auf **Manually Add Configuration**, geben die Konfiguration als Text ein und klicken auf **Apply**.

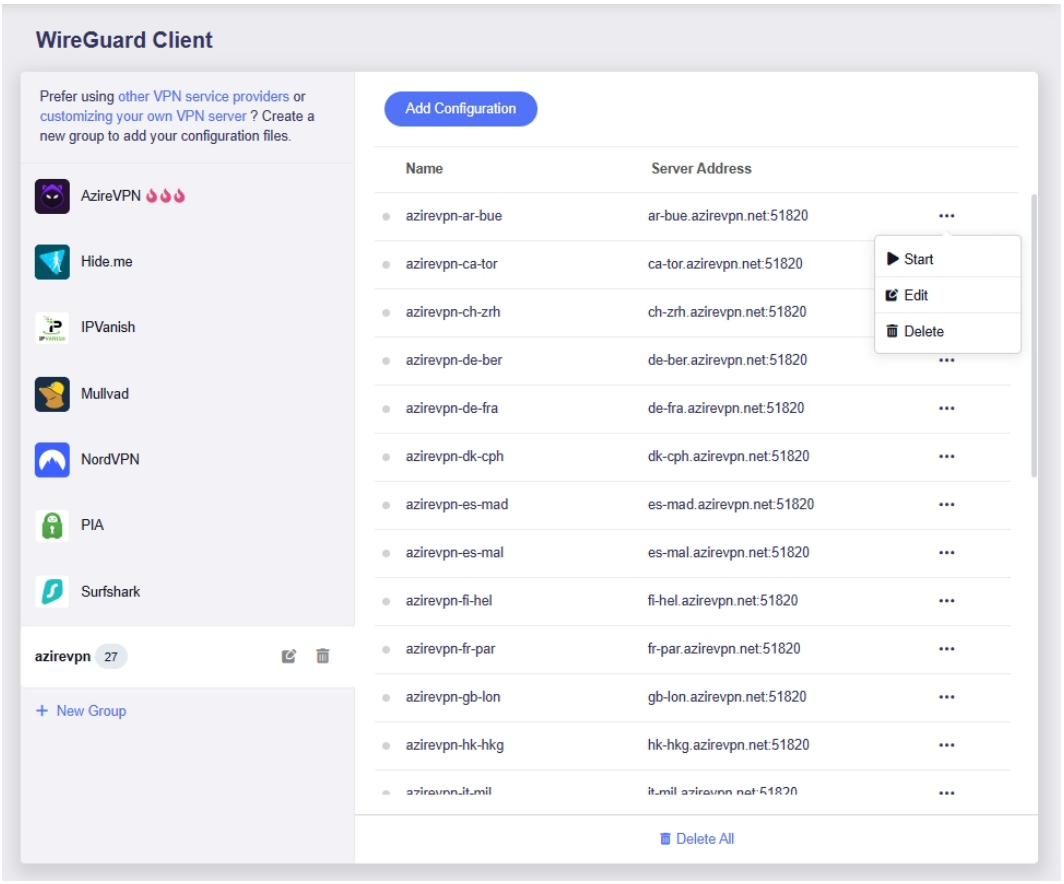




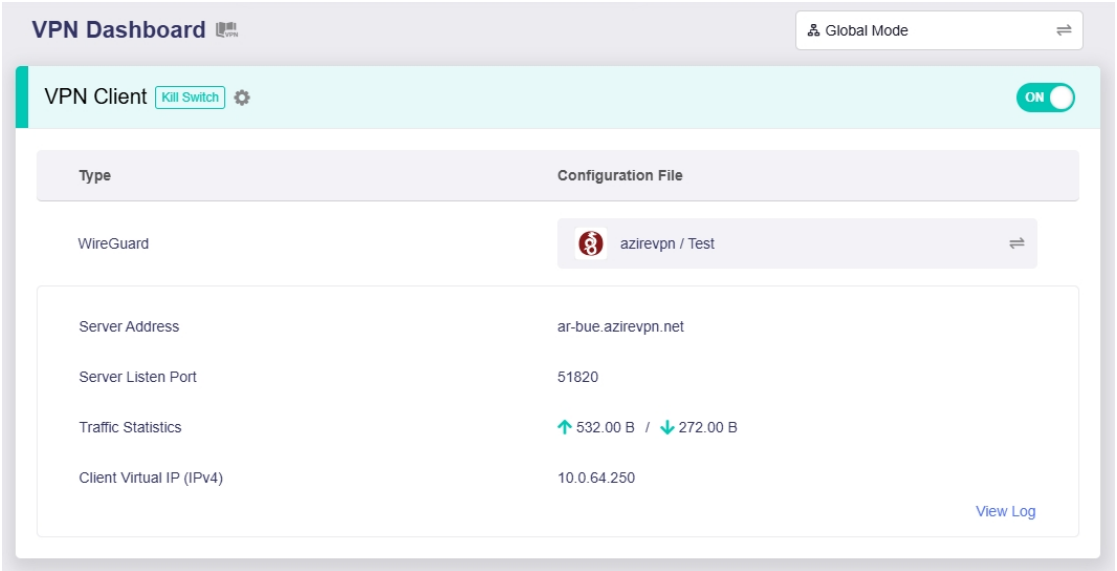
Um die einzelnen Einträge zu prüfen, wechseln Sie in den Modus Item und kontrollieren Sie die Konfigurationsdetails. Klicken Sie anschließend auf **Apply**.



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 12

Tor

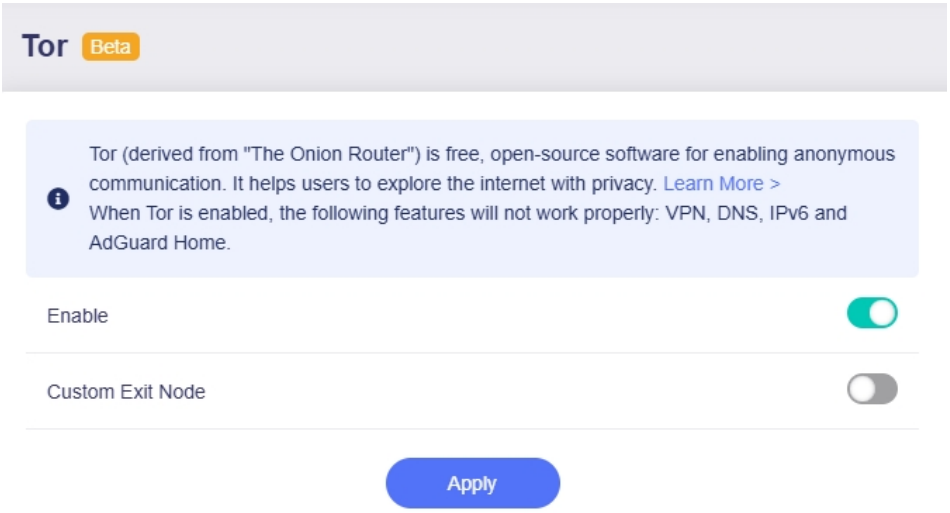
Dieses Kapitel stellt Tor (The Onion Router) vor, eine freie, quelloffene Software für anonyme Kommunikation.

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.

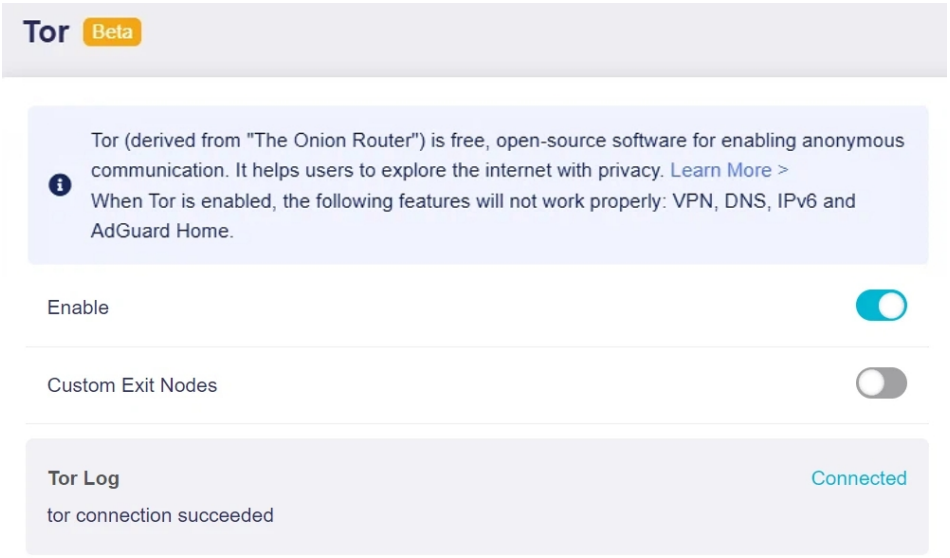
Bei aktiviertem Tor funktionieren VPN, DNS, IPv6 und AdGuard Home nicht ordnungsgemäß.

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

1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **Tor**. Aktivieren Sie Tor mit dem Schalter, aktivieren Sie bei Bedarf Custom Exit Nodes und klicken Sie auf **Apply**.



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



Kapitel 13

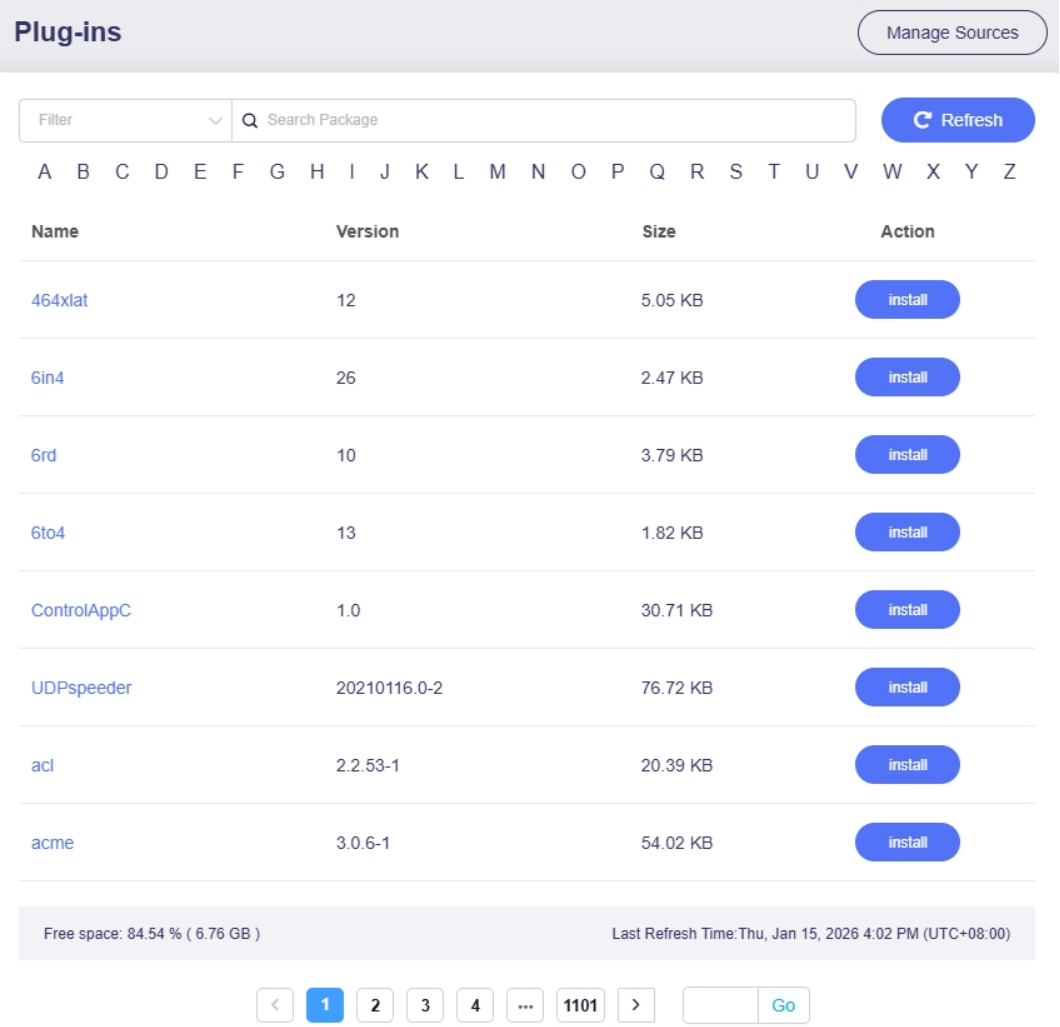
Anwendungen

Dieses Kapitel stellt einige Anwendungen auf GL.iNet-Routern vor, darunter Plug-ins, dynamisches DNS, Netzwerkspeicher, AdGuard Home, Kindersicherung, ZeroTier, Tailscale und die eSIM-Verwaltung.

13.1 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:

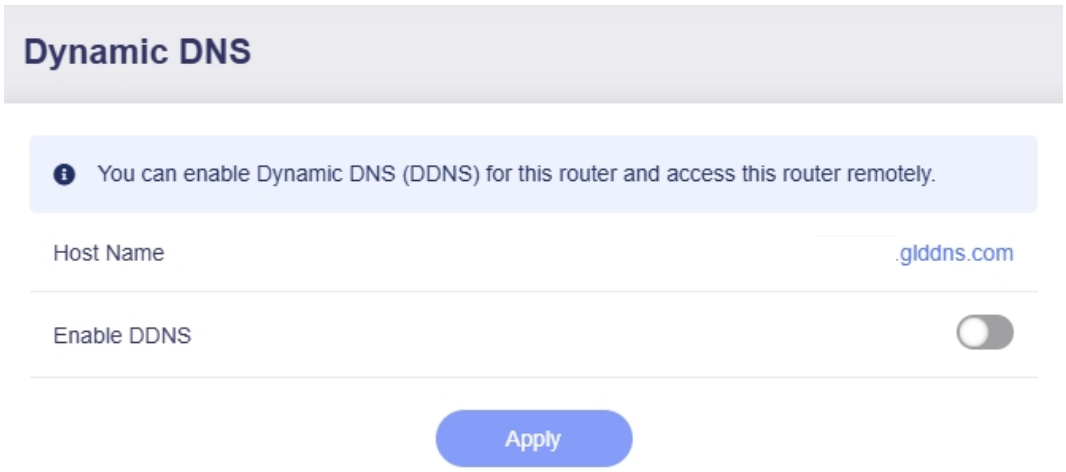
1. Es wird davon abgeraten, in der offiziellen GL.iNet-Firmware vorinstallierte Plug-ins wie nginx, AdGuard Home oder Tailscale zu aktualisieren.
2. Manuell installierte Plug-ins von Drittanbietern können aktualisiert werden. GL.iNet haftet jedoch nicht für Sicherheitsprobleme durch solche Plug-ins.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

13.2 Dynamisches DNS

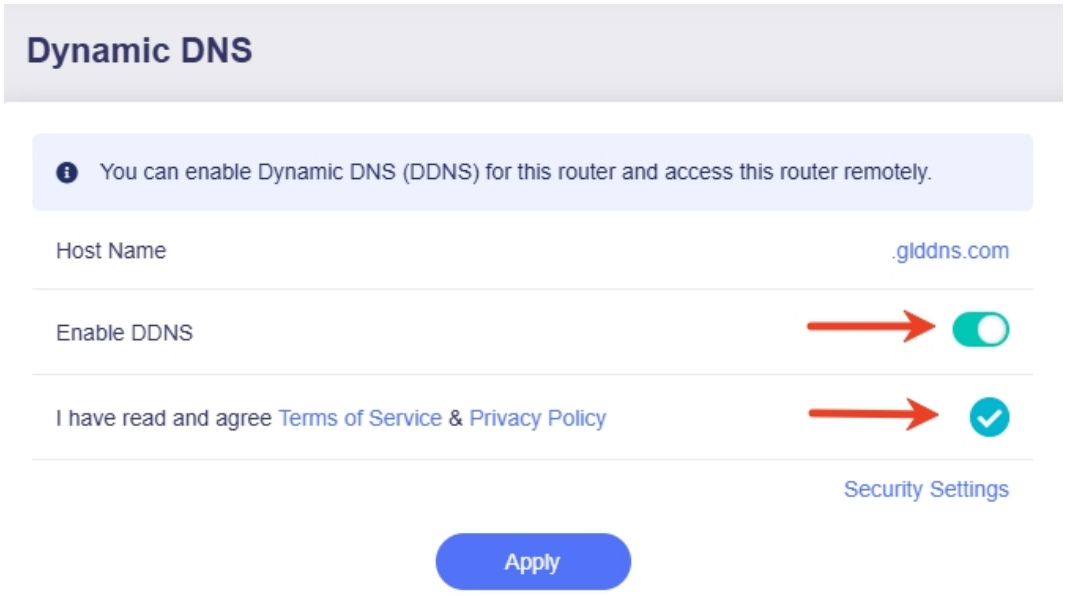
Dynamic DNS (DDNS) ordnet einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zu. Damit können Sie aus der Ferne auf Ihren Router zugreifen. Für diese Funktion ist eine öffentliche IP-Adresse erforderlich.

13.2.1 DDNS aktivieren

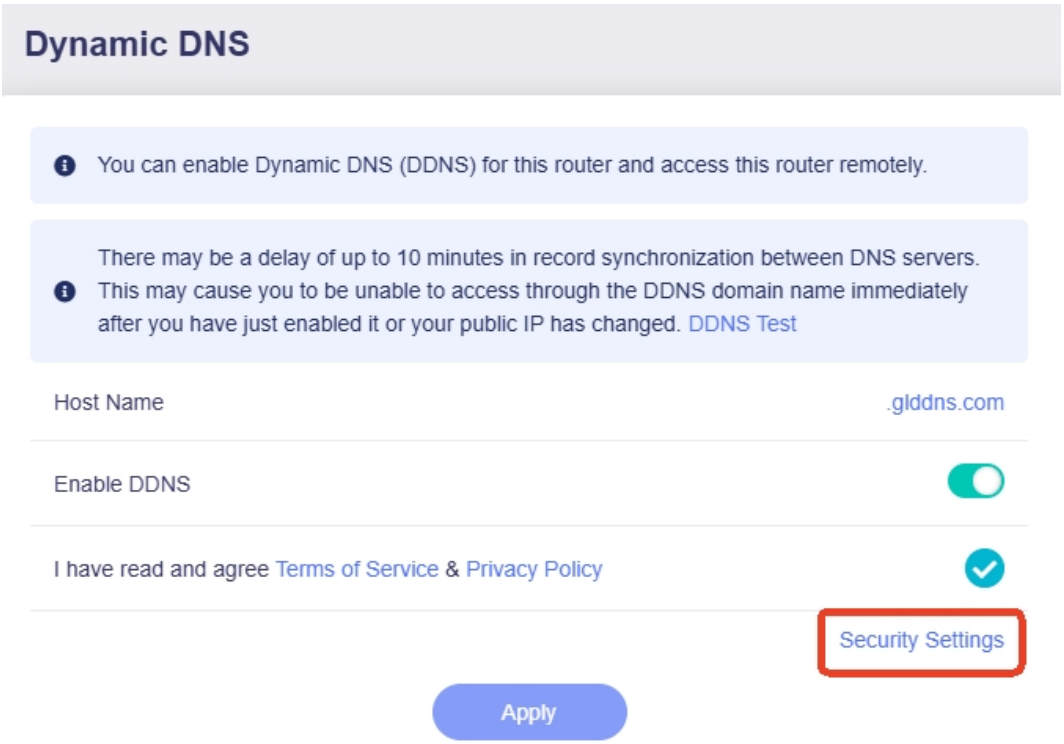
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Dynamic DNS**. Die folgende Seite wird angezeigt.



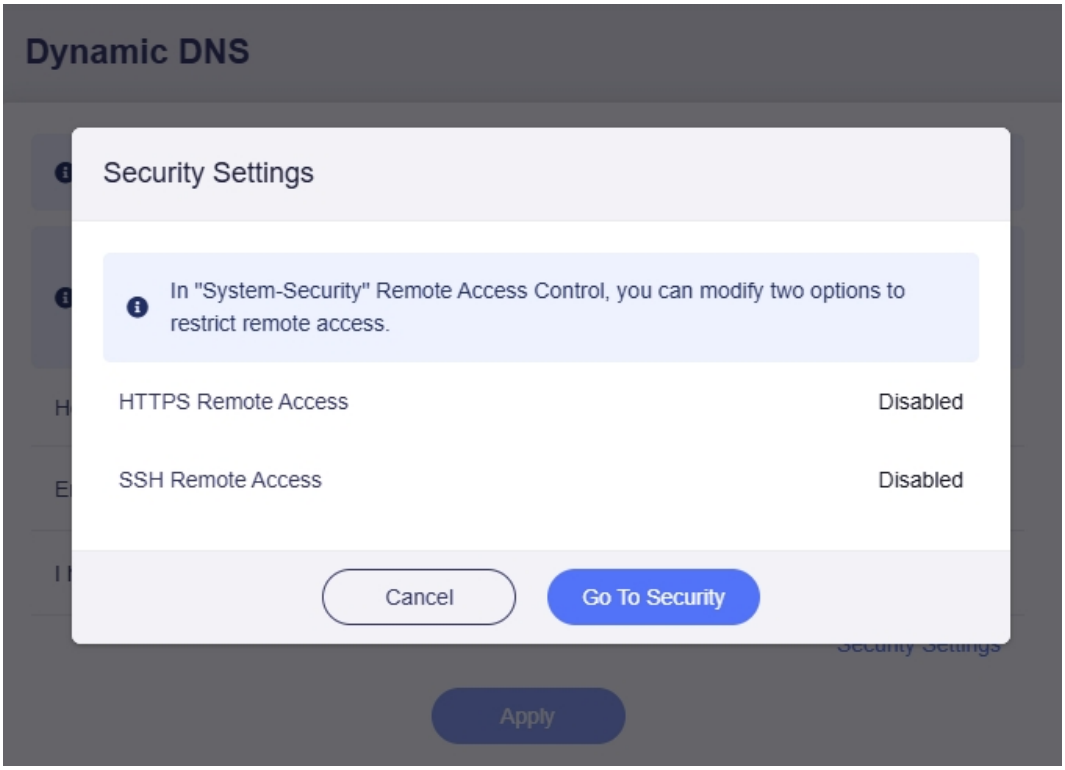
2. Aktivieren Sie **Enable DDNS**, lesen und akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



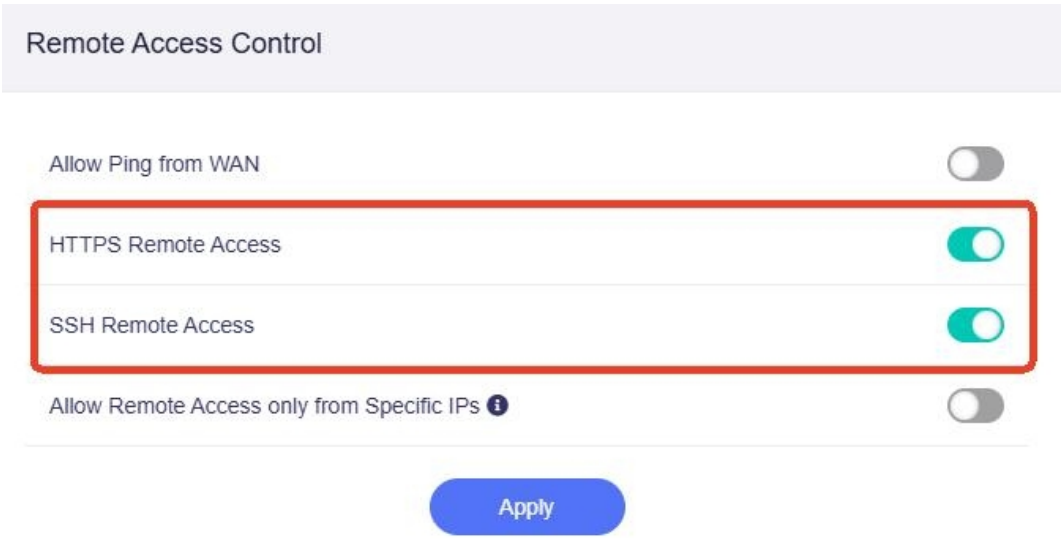
3. Klicken Sie unten rechts auf **Security Settings**.



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:

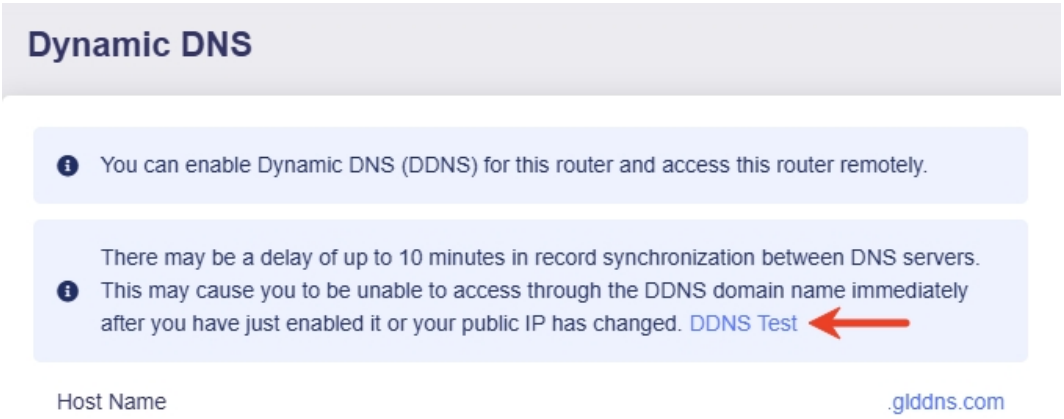
1. Die Synchronisierung der Einträge zwischen DNS-Servern kann bis zu zehn Minuten dauern. Deshalb kann der Zugriff über den DDNS-Domainnamen direkt nach der Aktivierung oder nach einer Änderung Ihrer öffentlichen IP-Adresse vorübergehend nicht möglich sein.
2. Wenn Sie DDNS und einen VPN-Client gleichzeitig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

13.2.2 DDNS-Funktion prüfen

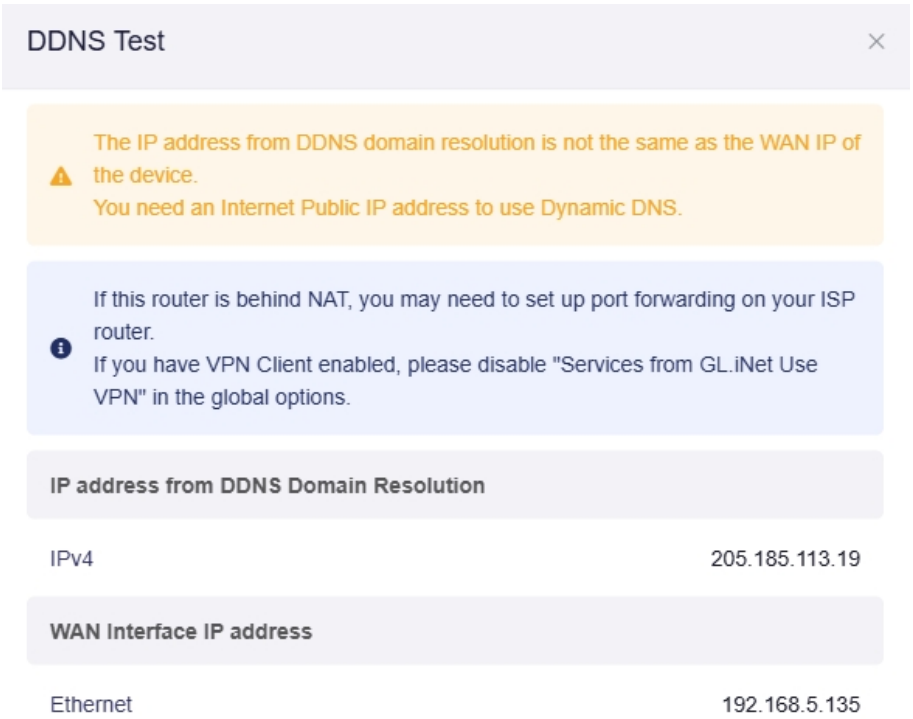
Sie können DDNS mit dem integrierten Testwerkzeug oder manuell über Befehle prüfen.

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 zu ermitteln. Nachfolgend ein Beispiel mit Beryl AX (GL-MT3000).



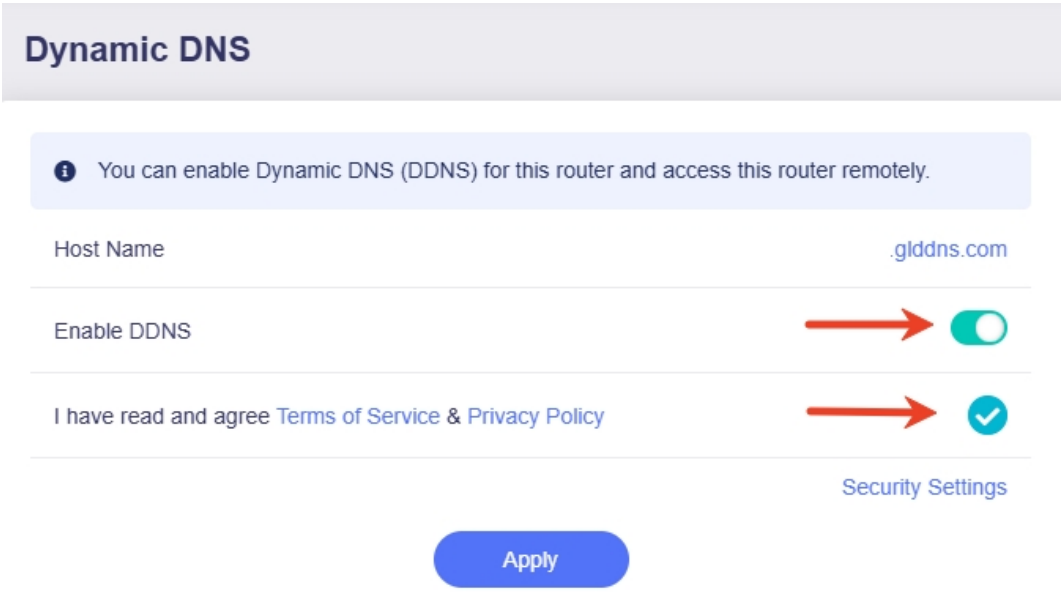
   - Ersetzen Sie „xxxxxxx.glddns.com“ in der obigen Abbildung durch Ihren Hostnamen.
   - „8.8.8.8“ ist ein DNS-Server von Google. Verwenden Sie diesen oder ersetzen Sie ihn durch einen anderen DNS-Server und drücken Sie die Eingabetaste.
2. Wenn eine öffentliche IP-Adresse wie „183.178.10.100“ in der 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 Ihres Routers an und öffnen Sie **INTERNET**. Suchen Sie die WAN-IP-Adresse des Routers in der derzeit aktiven Schnittstelle. Vergleichen Sie diese Adresse mit der oben ermittelten öffentlichen IP-Adresse. Stimmen sie überein, funktioniert DDNS; andernfalls nicht.

13.2.3 HTTPS-Fernzugriff

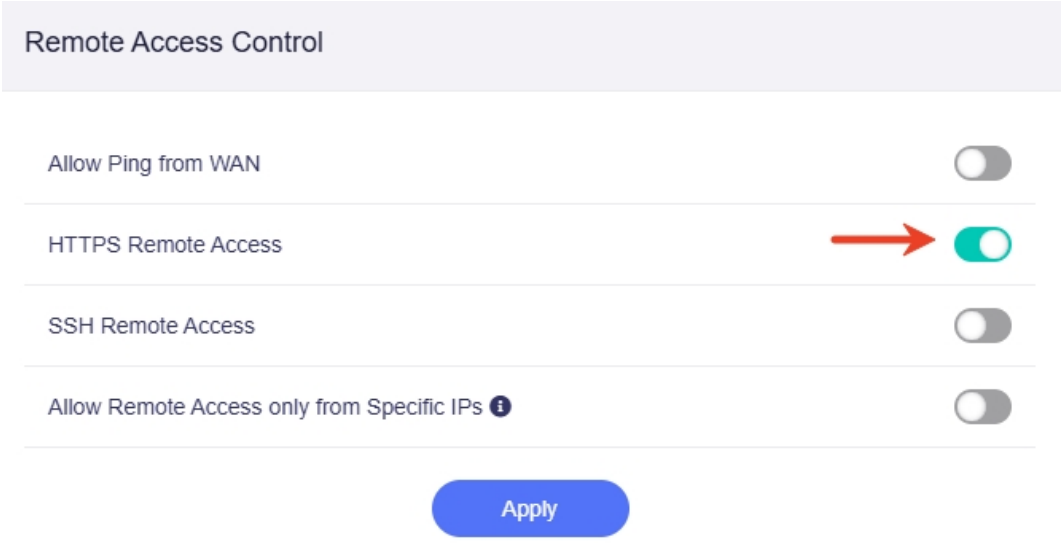
Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 443** ein.

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**.

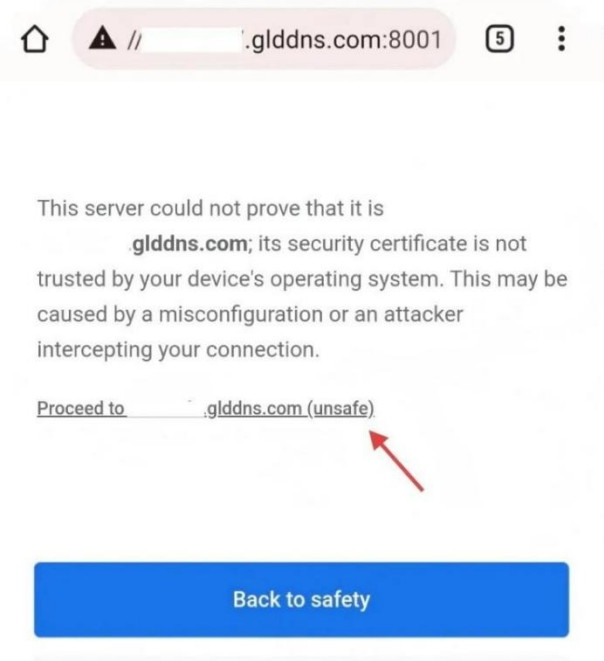


2. Öffnen Sie in der Weboberfläche **SYSTEM** > **Security** > **Remote Access Control**. Aktivieren Sie **HTTPS Remote Access** und klicken Sie auf **Apply**.



3. 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.



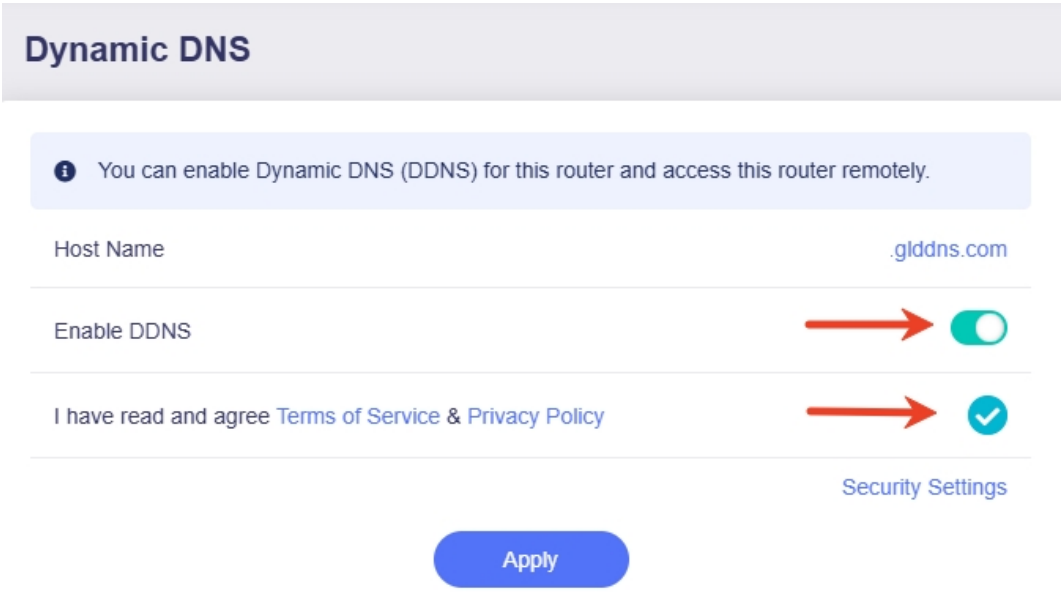
Sie können nun über den DDNS-Hostnamen per **HTTPS** auf die Weboberfläche des Routers zugreifen.

13.2.4 SSH-Fernzugriff

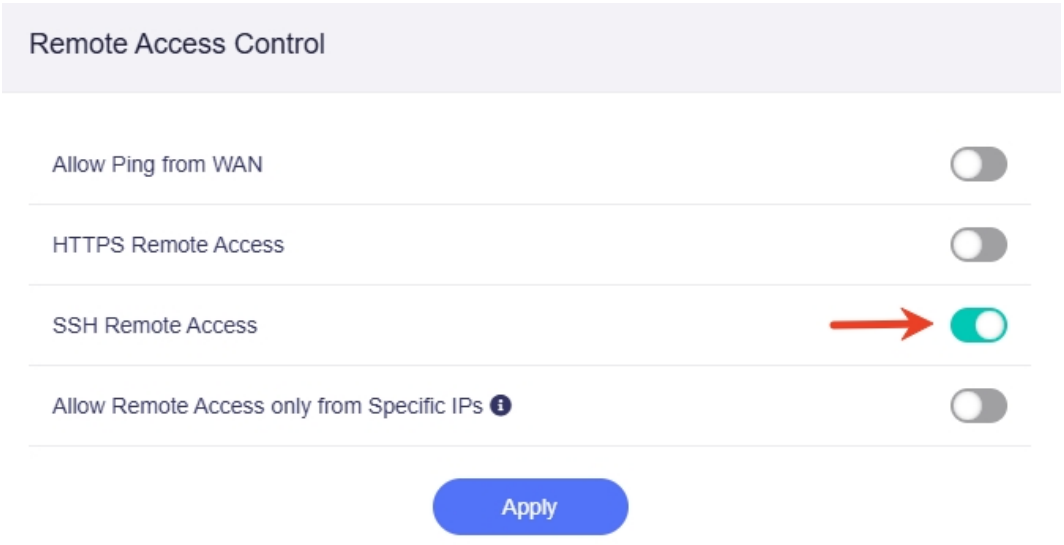
Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 22** ein.

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.

13.3 Netzwerkspeicher

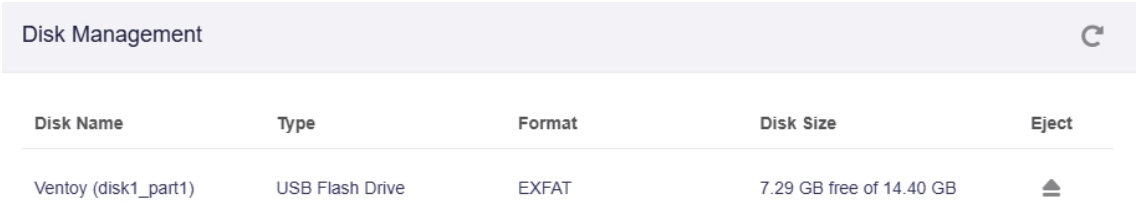
Die Netzwerkspeicherfunktion ermöglicht die drahtlose Dateifreigabe zwischen Geräten, wenn Sie ein USB-Laufwerk oder eine SD-Karte an Ihren Router anschließen. Der Router stellt den Speicher als gemeinsames Netzlaufwerk bereit, auf das alle per WLAN verbundenen Geräte zugreifen können.

Beryl AX 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.

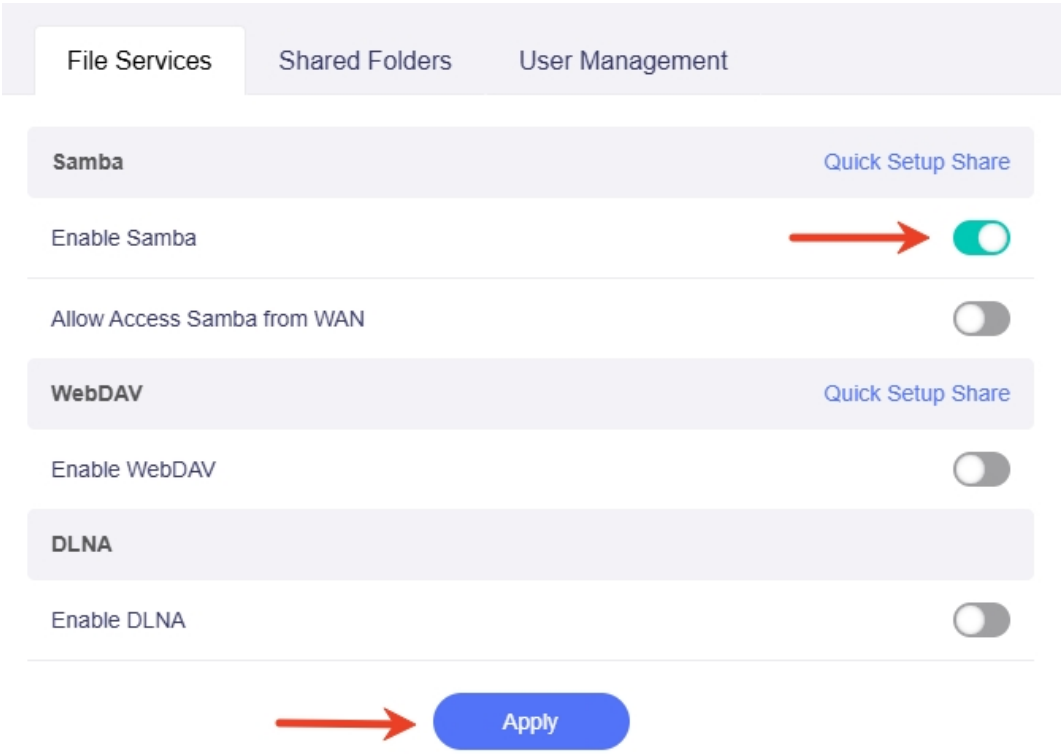
13.3.1 Speicher anschließen

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.



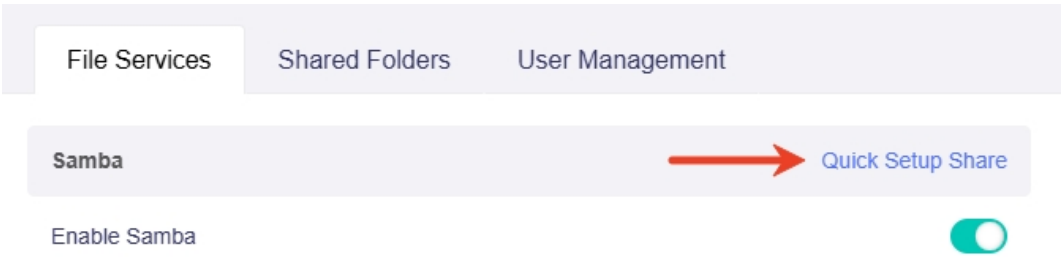
13.3.2 Samba einrichten

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

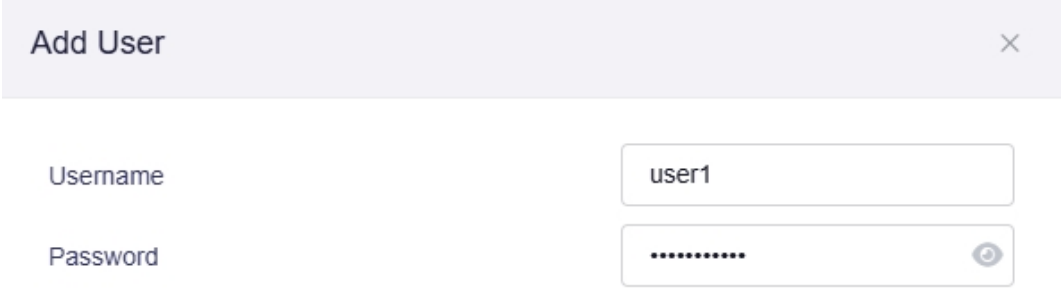


   - **Allow Access Samba from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den Samba-Dienst zugreifen sollen.

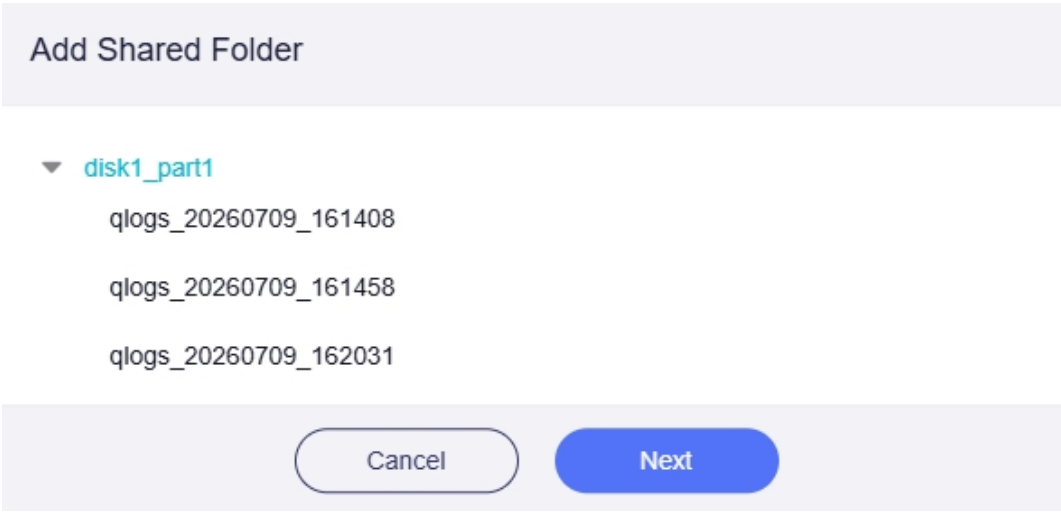
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



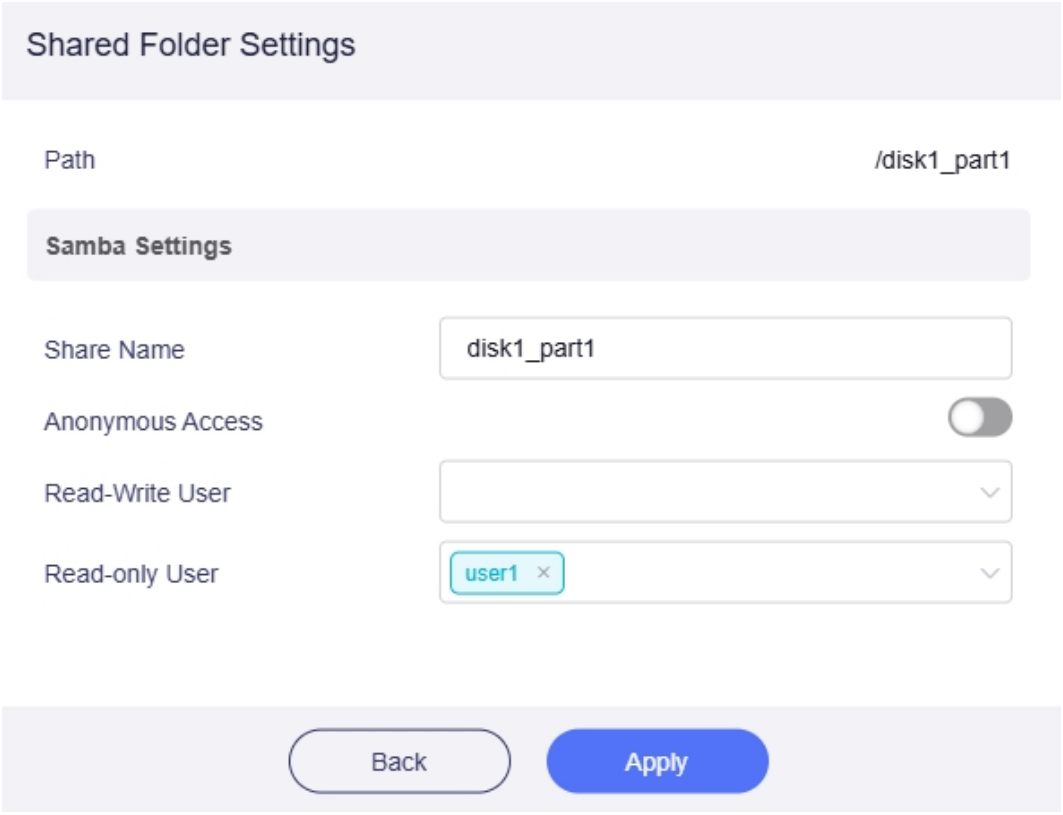
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



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.



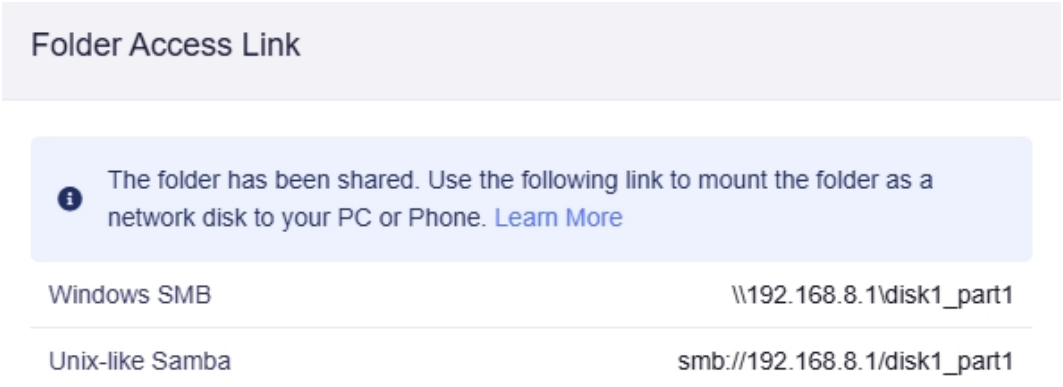
5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll er Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn dort und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend auf **Apply**.



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.

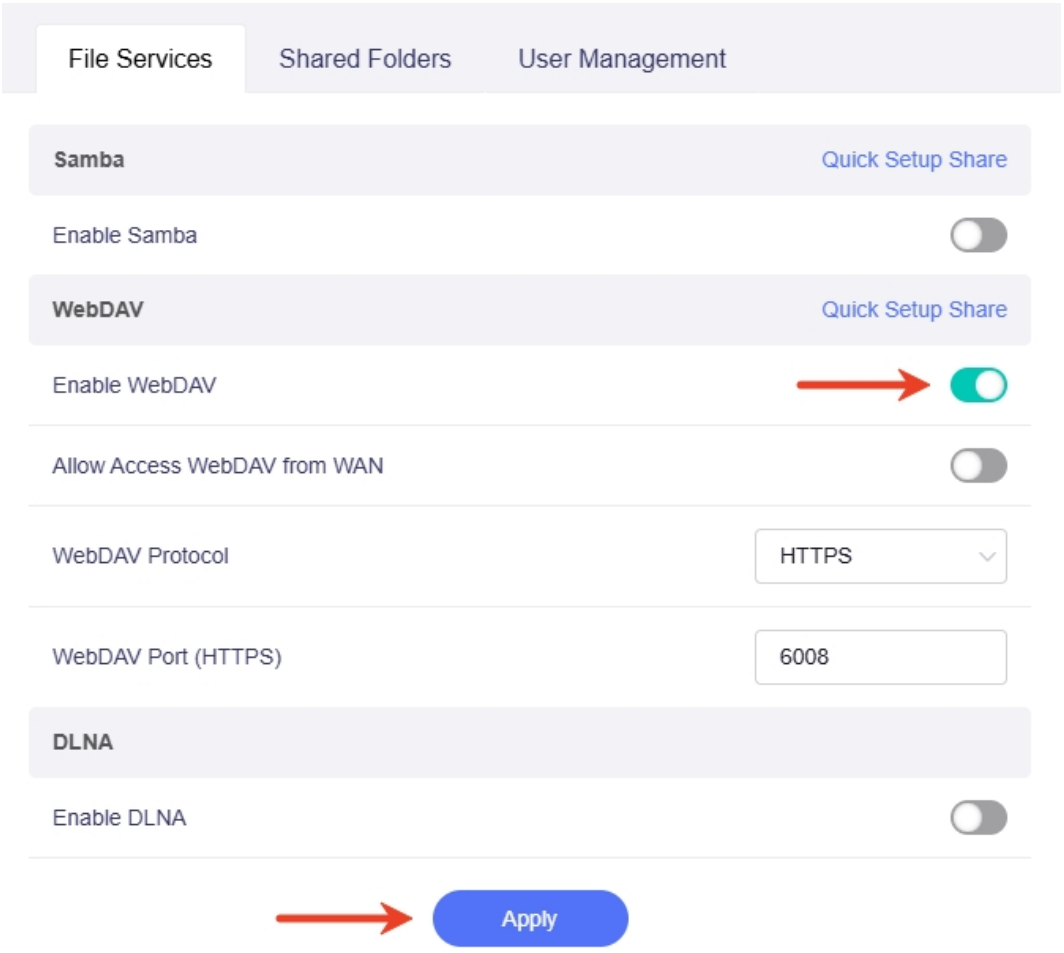


Hinweis: Wenn Sie **Allow Access Samba from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der Zugriffsadresse (standardmäßig

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

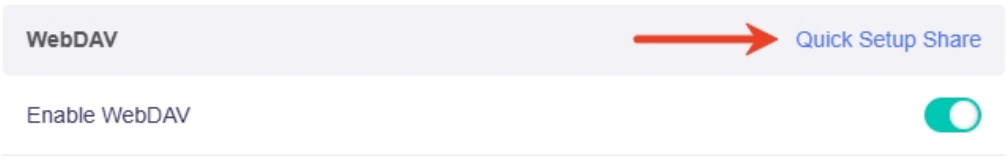
13.3.3 WebDAV einrichten

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

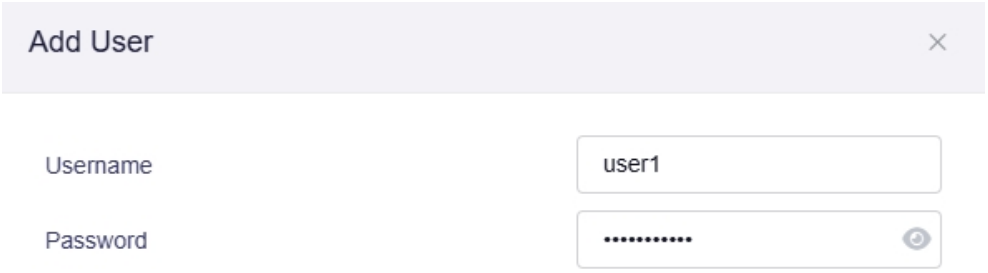


- **Allow Access WebDAV from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den WebDAV-Dienst zugreifen sollen.
- **WebDAV Protocol**: HTTP ist unverschlüsselt und wird auf eigenes Risiko verwendet. HTTPS ist verschlüsselt und verwendet ein selbstsigniertes Zertifikat.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

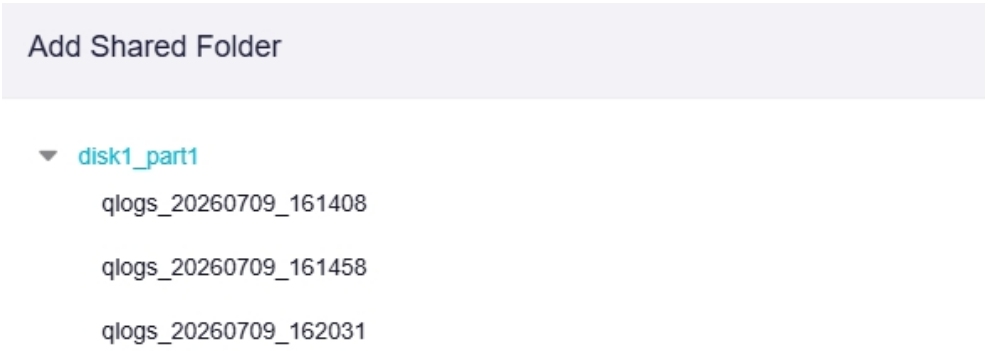
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



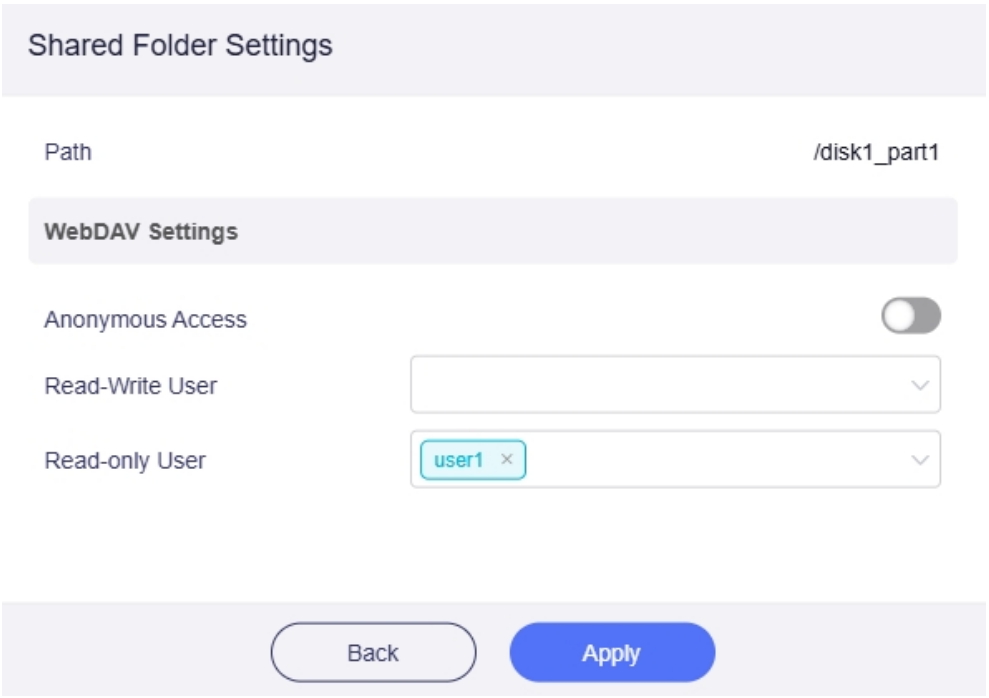
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



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.



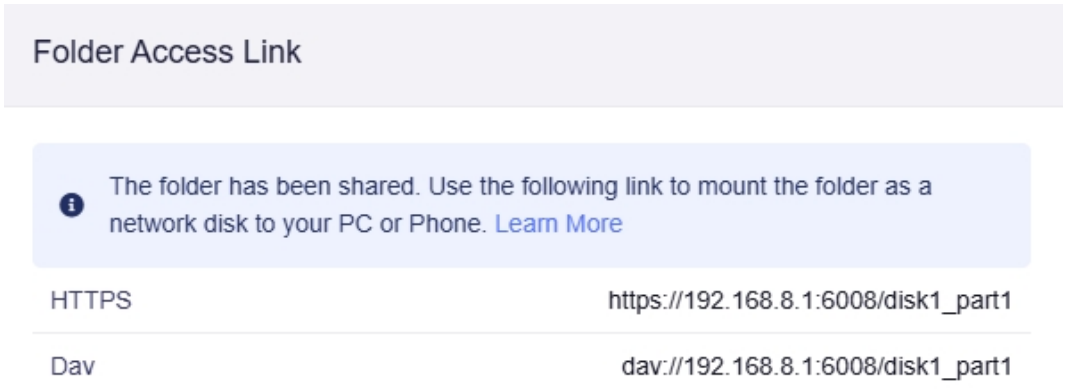
5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll dieser Benutzer Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn unter Read-Only User und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend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



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

6. Zugriffsadresse des Ordners abrufen.

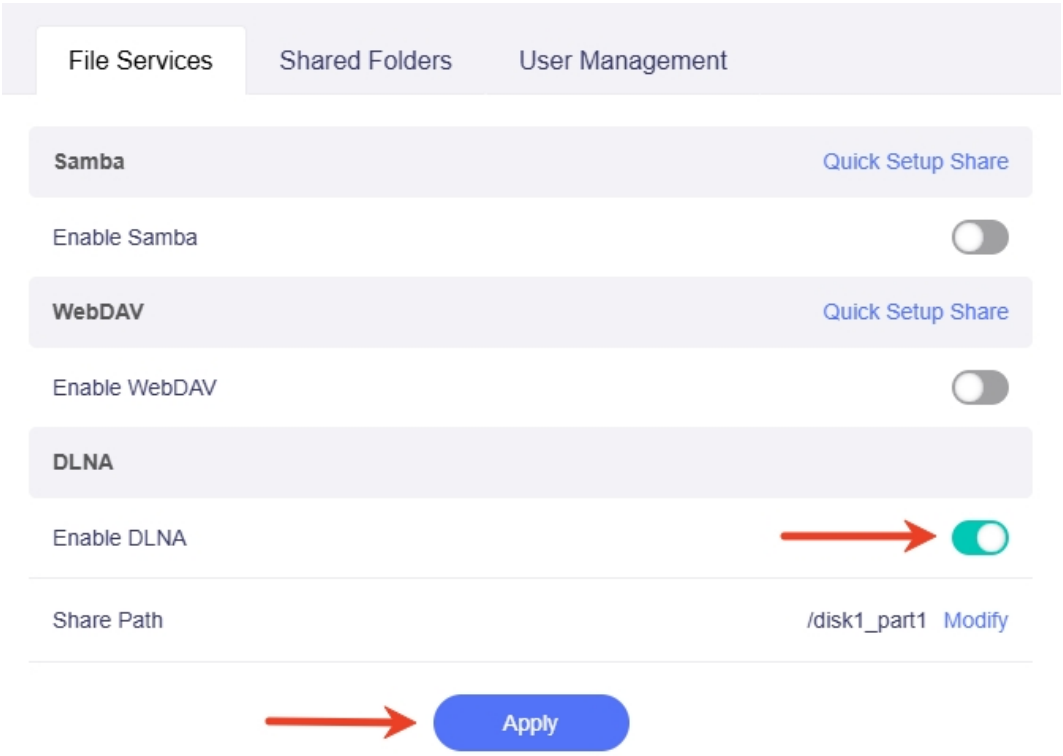
   Die Seite zeigt die Zugriffsadressen für Windows und Unix-ähnliche Betriebssysteme an. Zu Letzteren gehören Android, iOS, macOS und Ubuntu. Über diese Adressen können Sie nun per WebDAV auf den freigegebenen Ordner zugreifen.



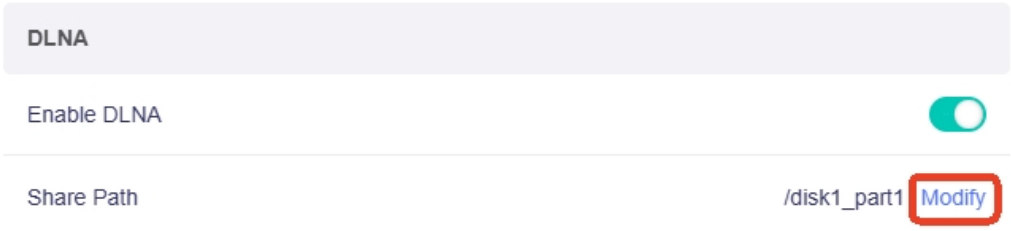
Hinweis: Wenn Sie **Allow Access WebDAV from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der Zugriffsadresse (standardmäßig 192.168.8.1) durch die WAN-IP-Adresse des Routers. Diese finden Sie auf der Seite INTERNET der Weboberfläche.

13.3.4 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.



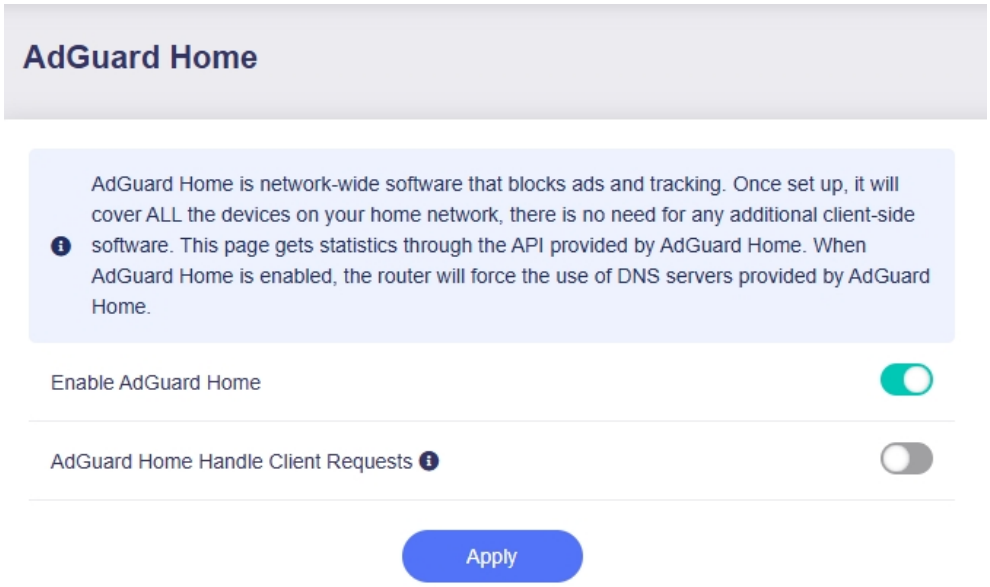
3. Verbinden Sie Ihren Smart-TV mit dem Router. Er erkennt den DLNA-Server automatisch.

13.4 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.

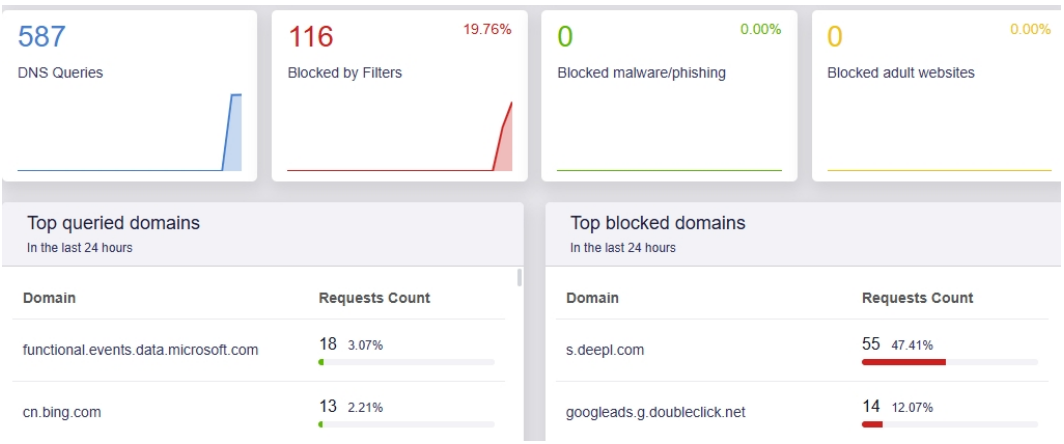
Gehen Sie wie folgt vor, um AdGuard Home einzurichten.

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

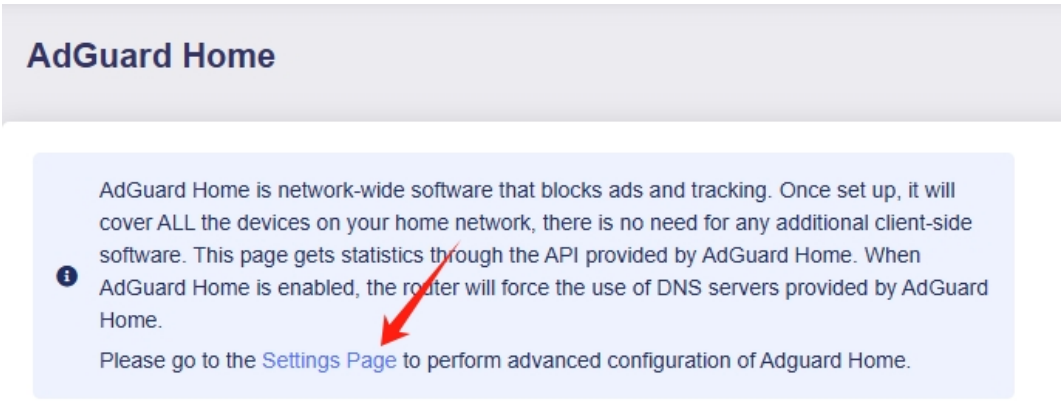


   - **AdGuard Home Handles Client Requests**: Leitet DNS-Anfragen der Endgeräte direkt an AdGuard Home weiter. Dadurch funktionieren jedoch domainbasierte VPN-Richtlinien nicht mehr.

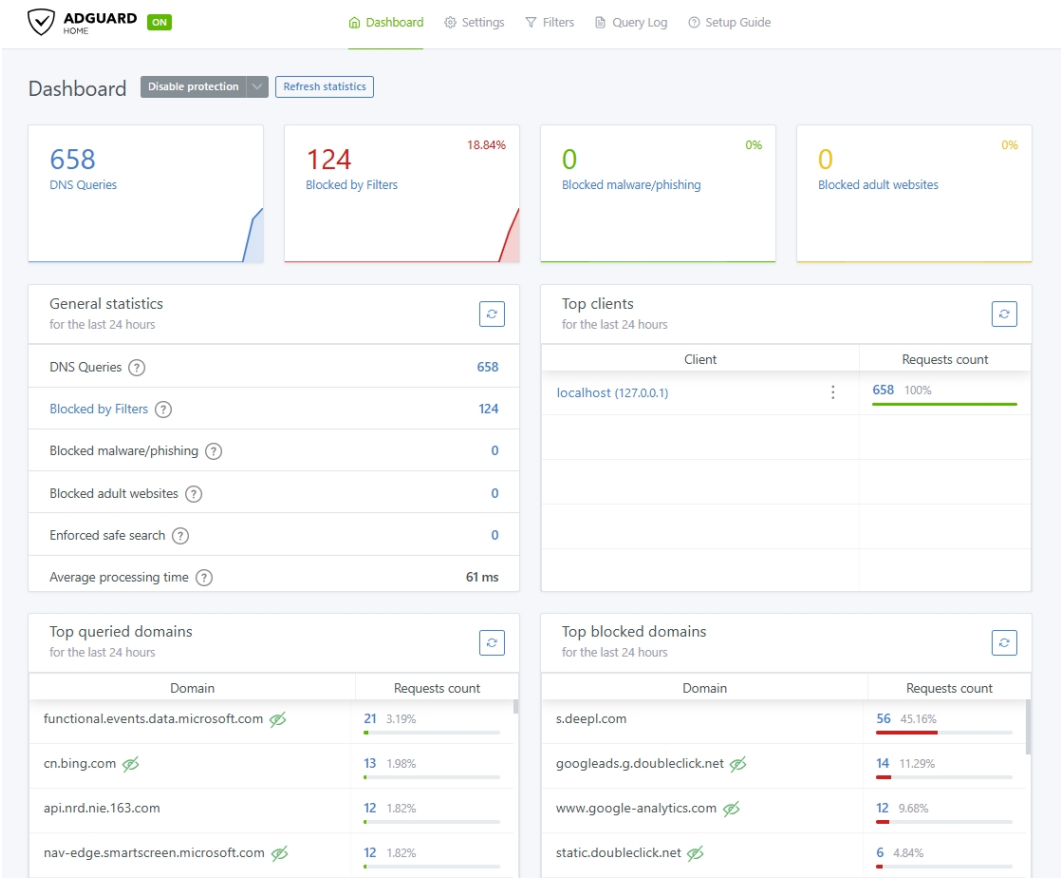
2. Die Seite lädt automatisch DNS-Statistiken wie Anfragen und blockierte Domains über die API von AdGuard Home.



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%

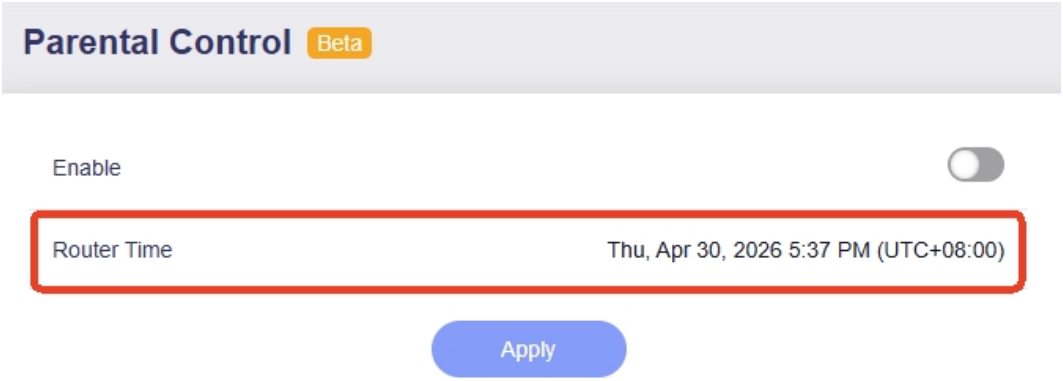
13.5 Kindersicherung

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.

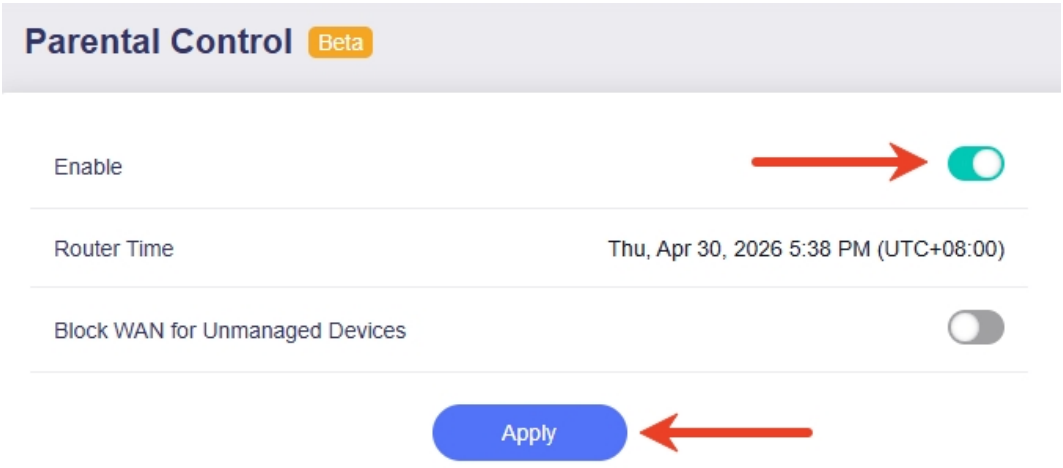
13.5.1 Schnelleinrichtung

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.



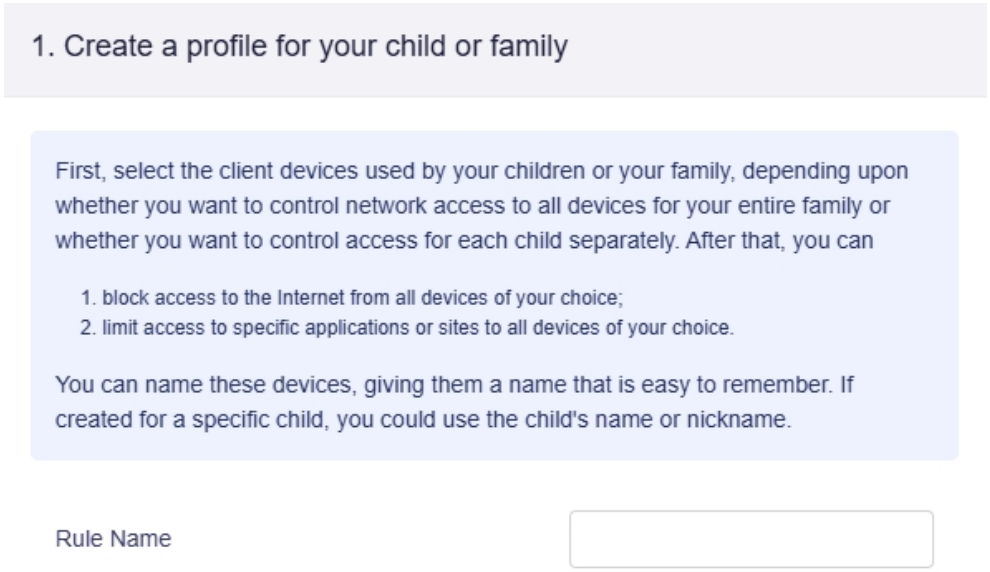
- **Block WAN for Unmanaged Devices**: Sperrt den Internetzugang für alle Geräte, die nicht in der Kindersicherungsliste stehen.

Das folgende Beispiel zeigt eine mögliche Anwendung.

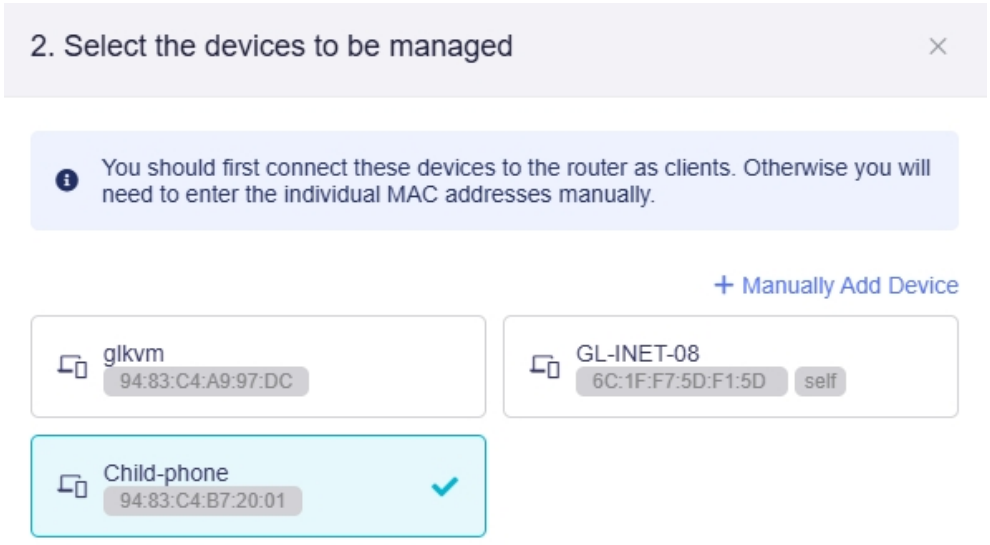
Szenario: Geräte in diesem Profil dürfen an Wochentagen von 08:00 bis 11:00 Uhr zum Lernen und am Wochenende von 18:00 bis 20:00 Uhr zum Spielen auf das Internet zugreifen. Zu allen anderen Zeiten ist der Internetzugang standardmäßig gesperrt.

Einrichtung:

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

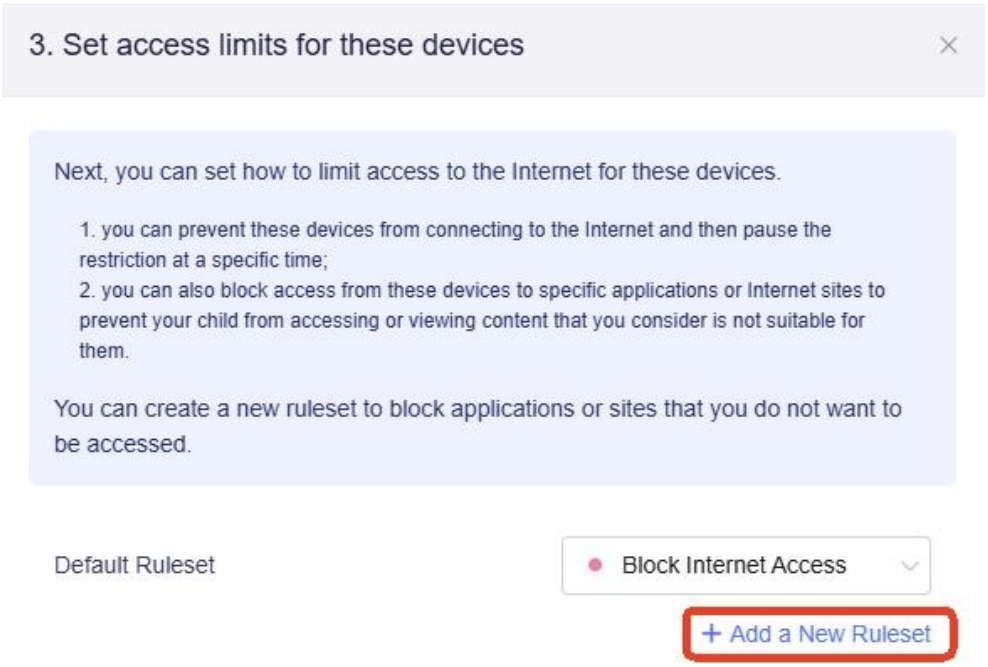


2. Wählen Sie die zu verwaltenden Geräte aus. Verbinden Sie diese zunächst mit dem Router. Noch nicht verbundene Geräte können Sie durch Eingabe ihrer MAC-Adressen manuell hinzufügen.

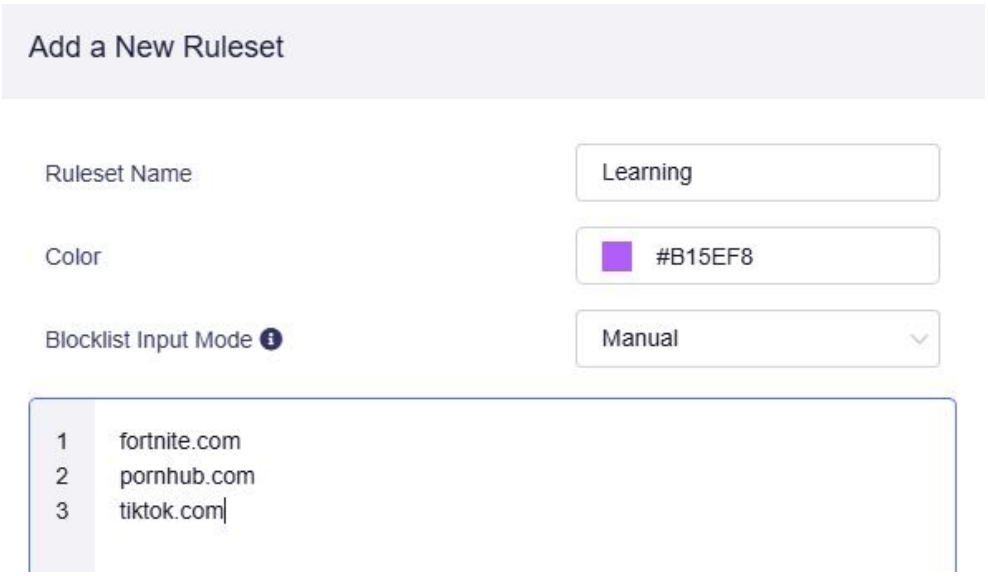


3. Zugriffsbeschränkungen festlegen.

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**.

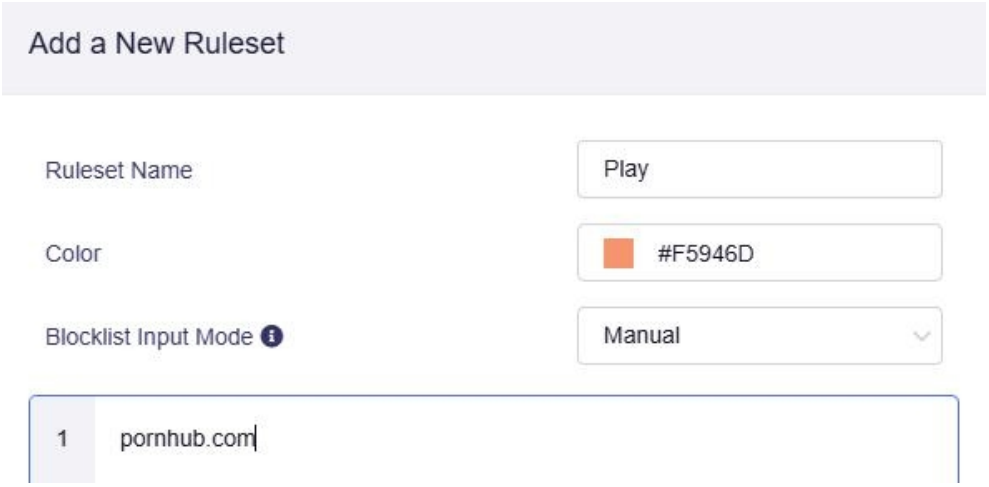


Legen Sie Namen, etwa Learning, und Farbe des Regelsatzes fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.

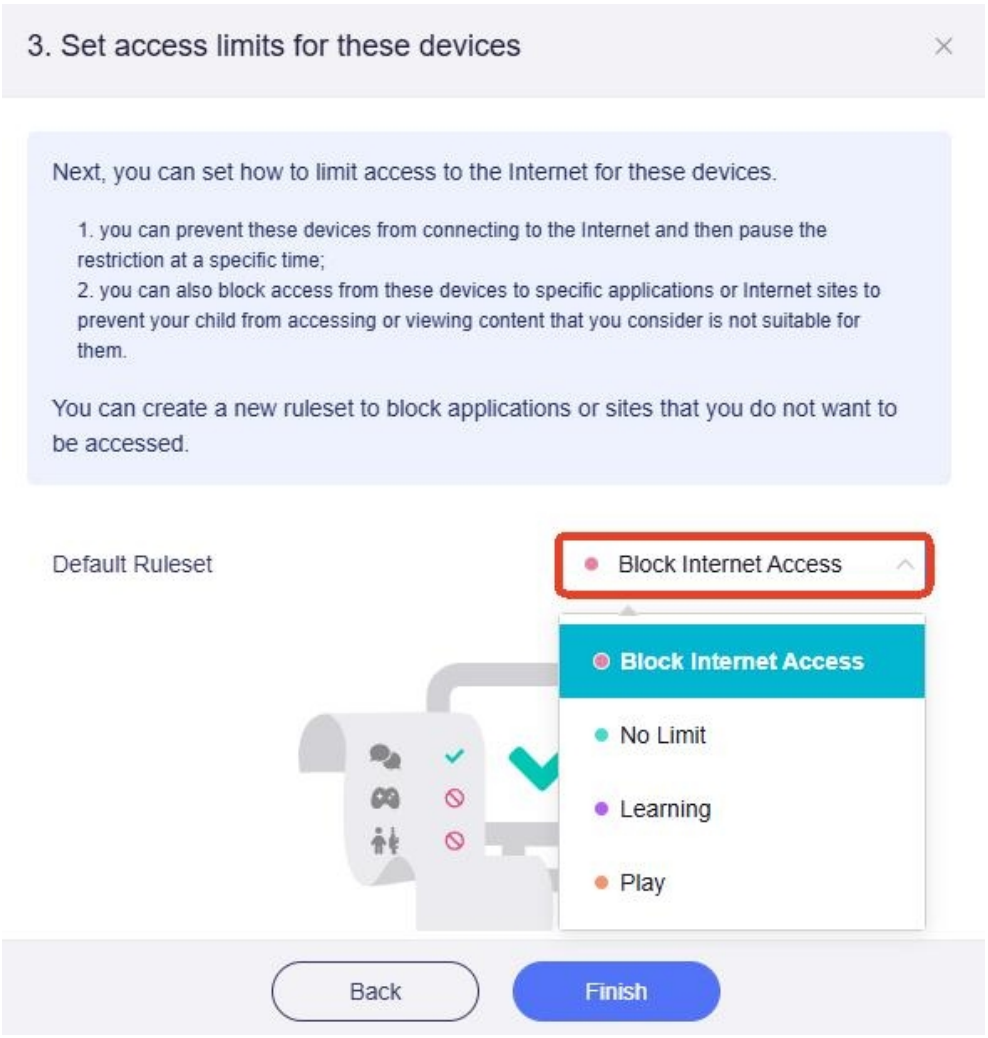


Hinweis: Die Domainnamen auf der Sperrliste umfassen auch ihre Subdomains. Der Eintrag „example.com“ schließt beispielsweise „subdomain.example.com“ und alle weiteren Subdomains ein.

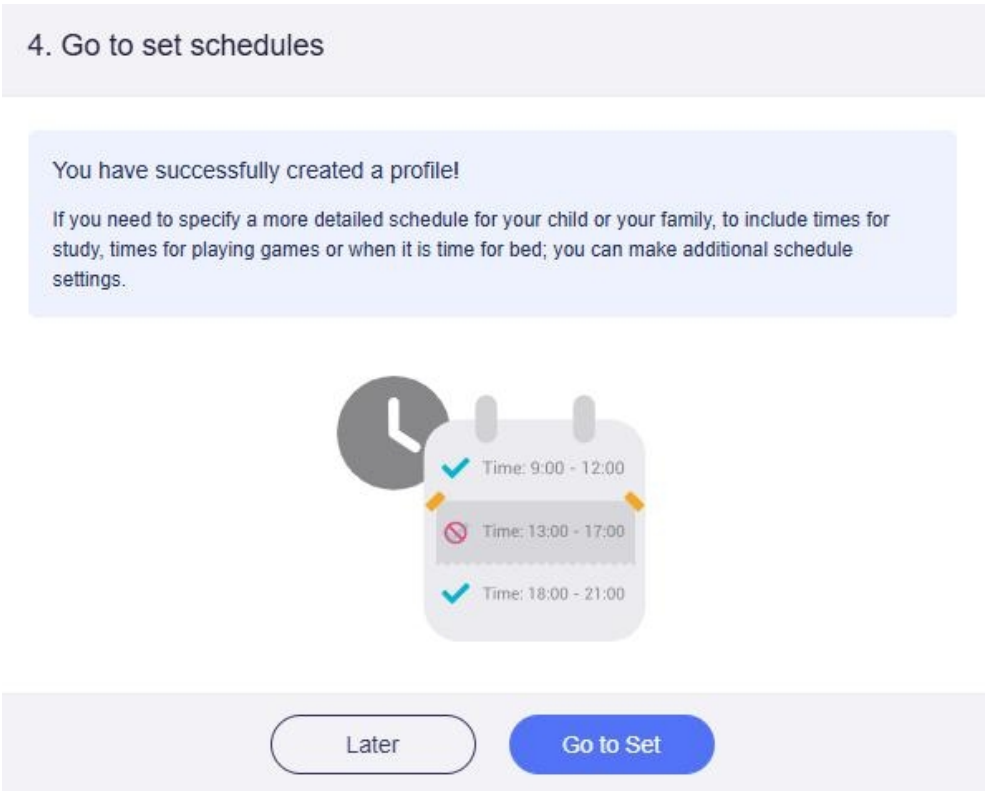
Erstellen Sie auf dieselbe Weise den zweiten Regelsatz. Legen Sie Namen, etwa Play, und Farbe fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.



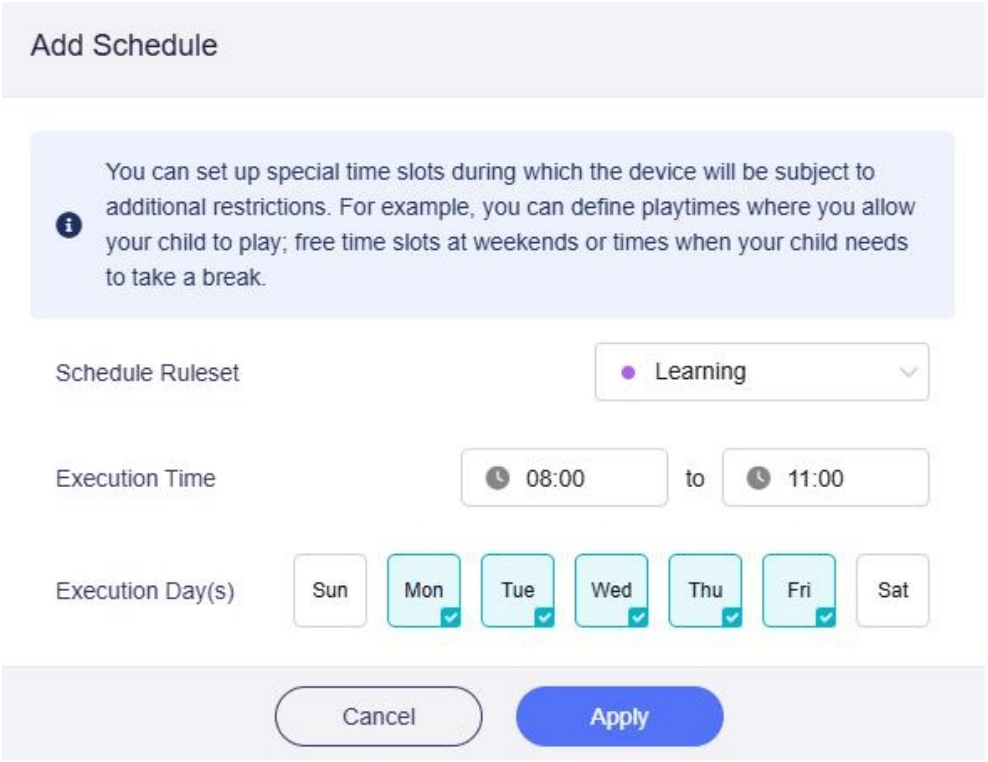
Nun sind insgesamt vier Regelsätze vorhanden. Wählen Sie **Block Internet Access** als **Default Ruleset** aus und klicken Sie auf **Finish**.



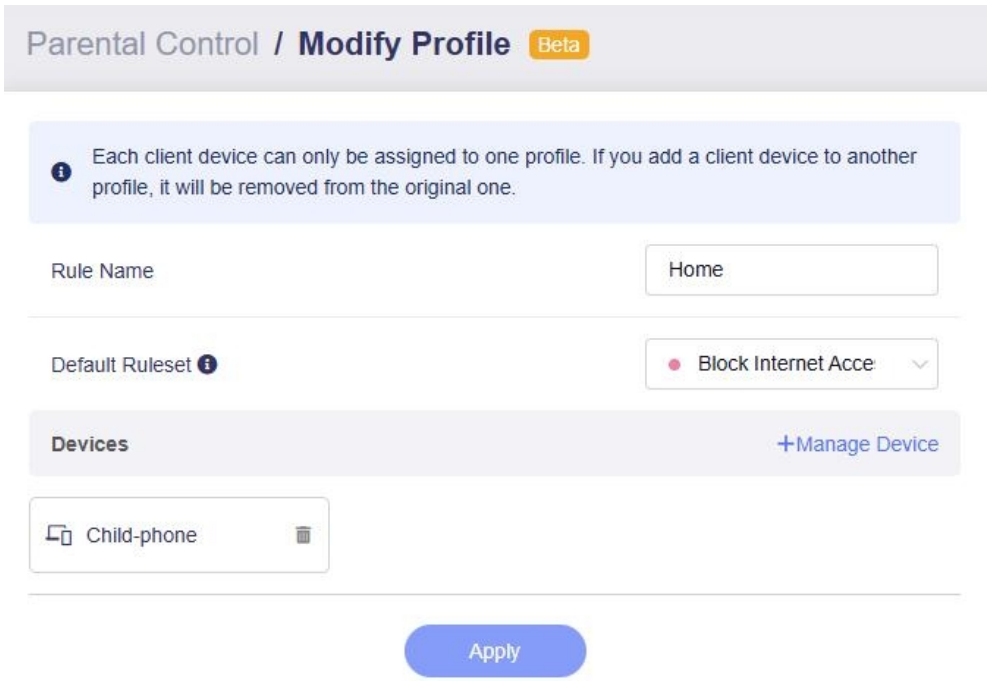
4. Erstellen Sie anschließend einen Zeitplan für Ihr Profil. Klicken Sie auf **Go to Set**.



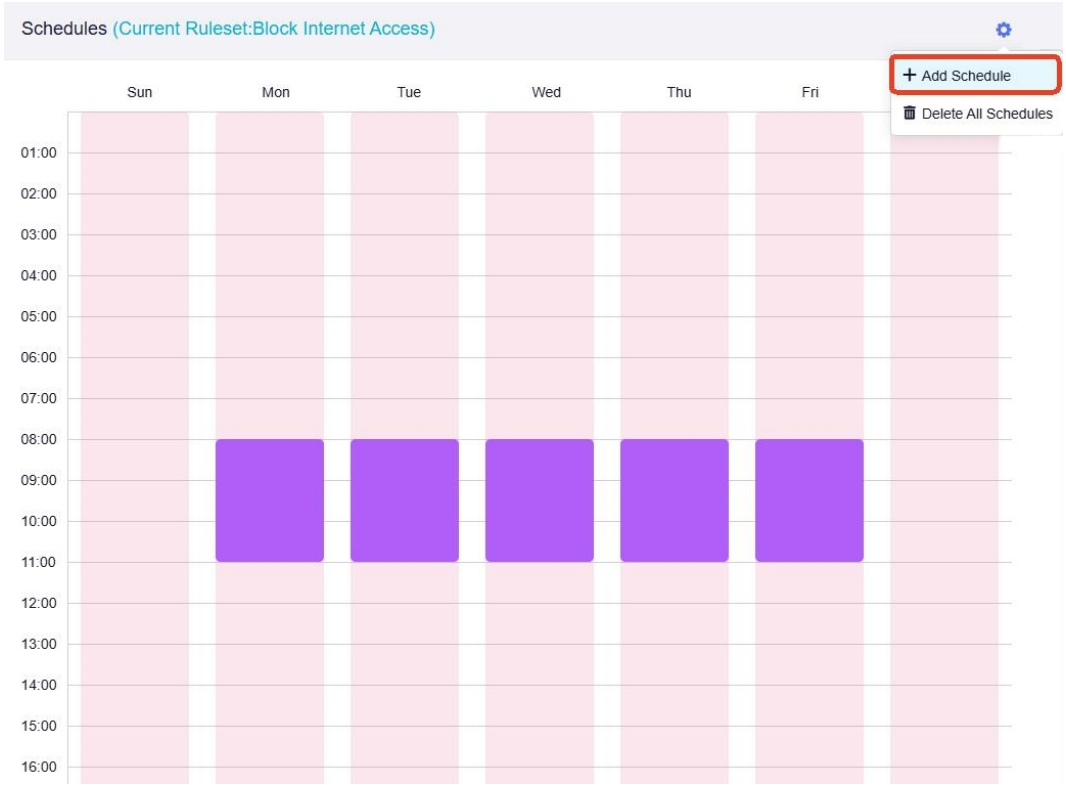
Fügen Sie den Regelsatz **Learning** zum Zeitplan hinzu. Legen Sie unter **Execution Time** an Wochentagen 08:00 bis 11:00 Uhr fest und klicken Sie auf **Apply**.



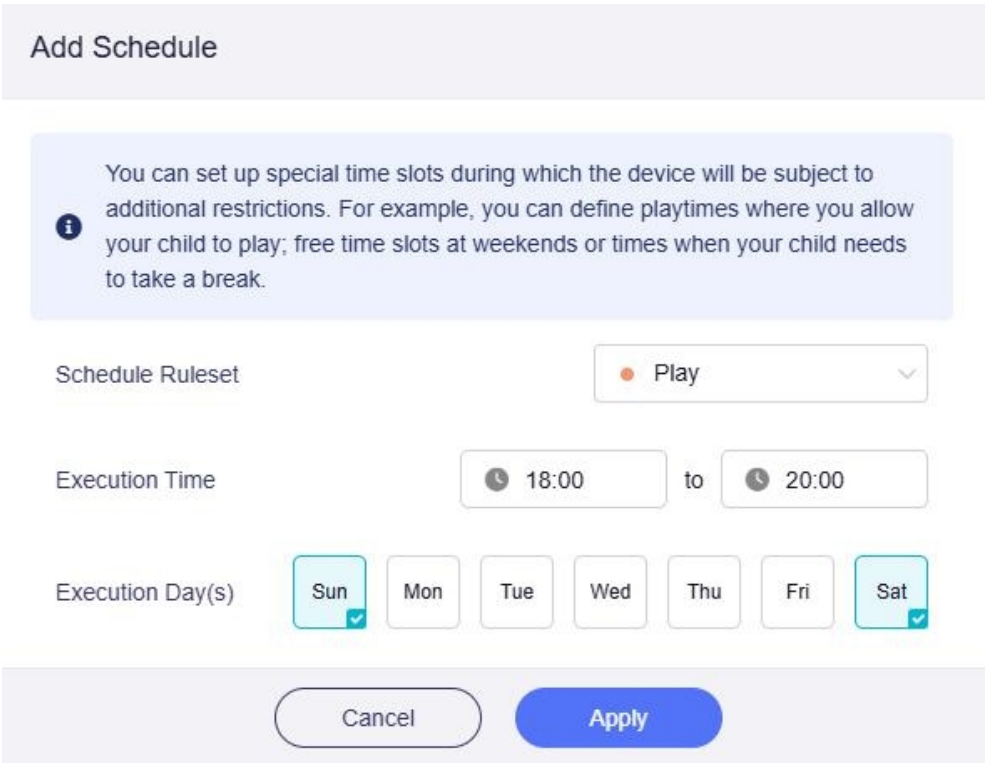
5. Sie gelangen zur Bearbeitungsseite des angelegten Profils.



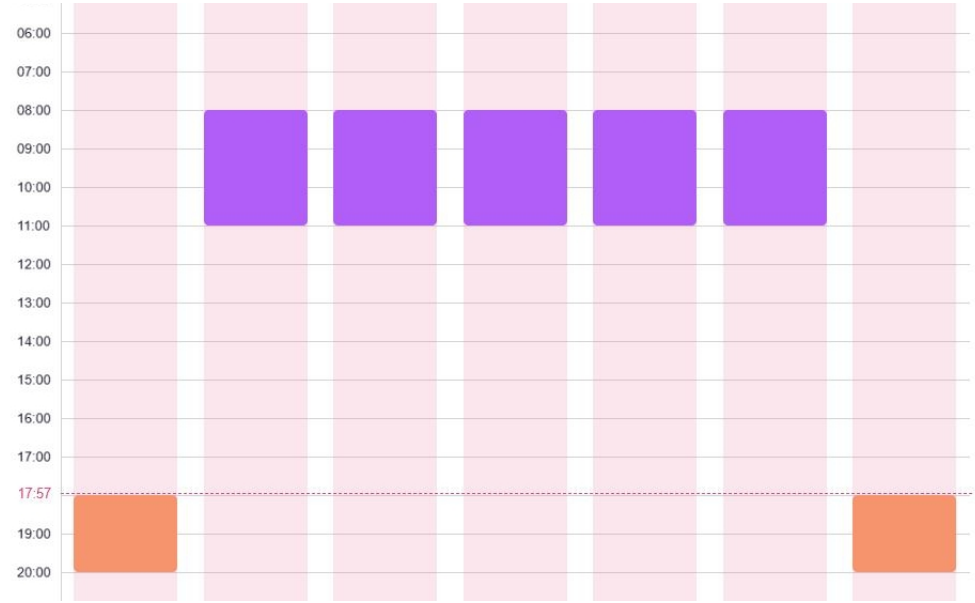
Unten sehen Sie den angelegten Zeitplan. Klicken Sie oben rechts auf das Zahnradsymbol und wählen Sie **Add Schedule**.



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**.



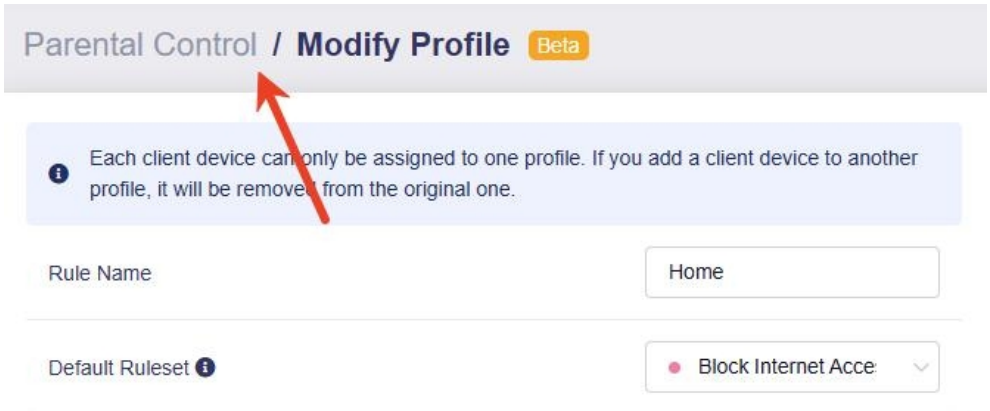
Der Regelsatz Play wird in den Zeitplan aufgenommen.



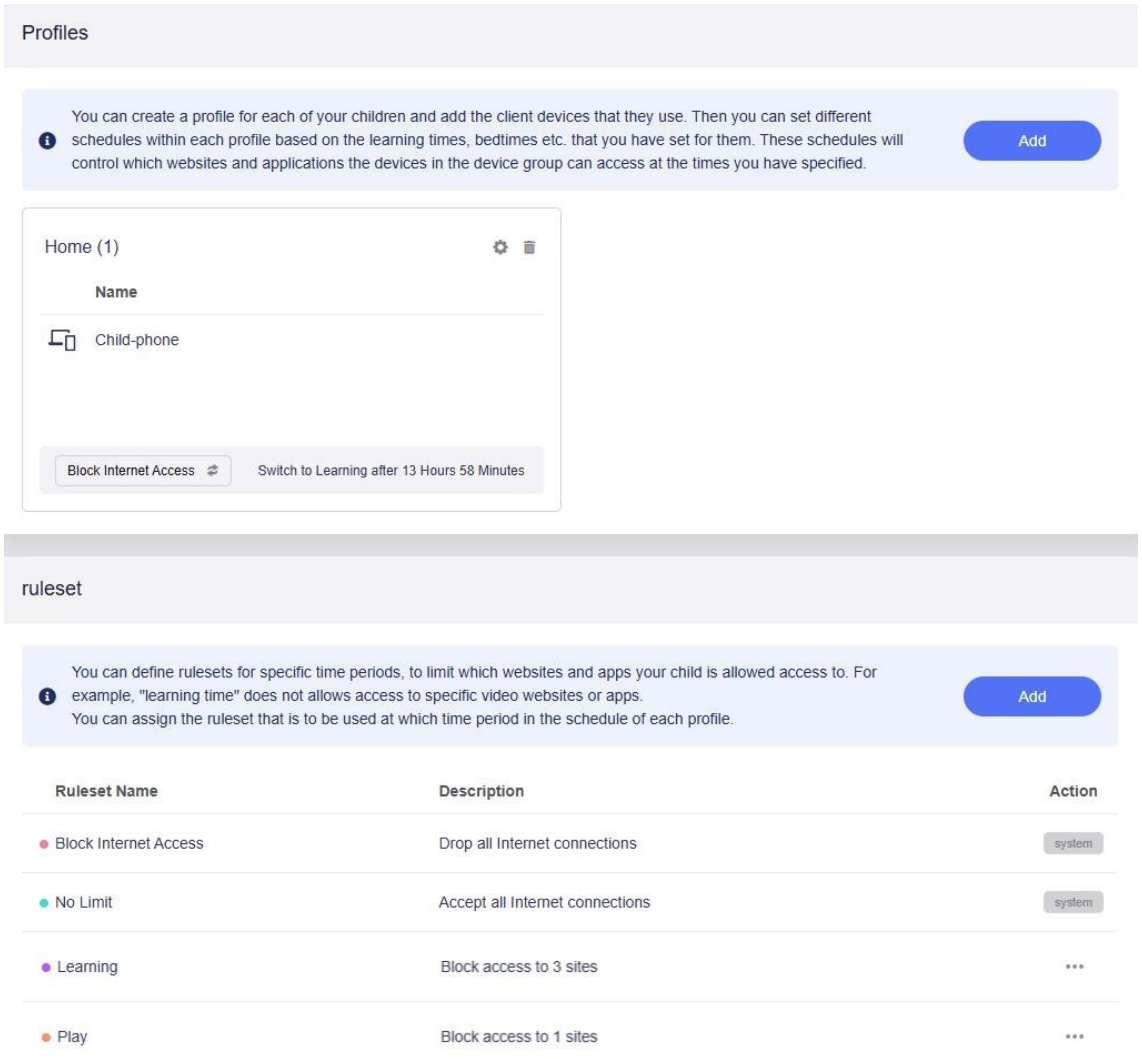
Tipps:

- 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.



13.5.2 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.

13.6 ZeroTier

ZeroTier ist ein softwarebasiertes virtuelles privates Netzwerk (VPN) für sichere, verschlüsselte Kommunikation zwischen Geräten über das Internet. Es erstellt ein privates virtuelles Netzwerk, in dem Geräte unabhängig von Standort oder Netzwerktopologie so miteinander kommunizieren können, als befänden sie sich im selben lokalen Netzwerk. ZeroTier ist einfach einzurichten und zu 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:

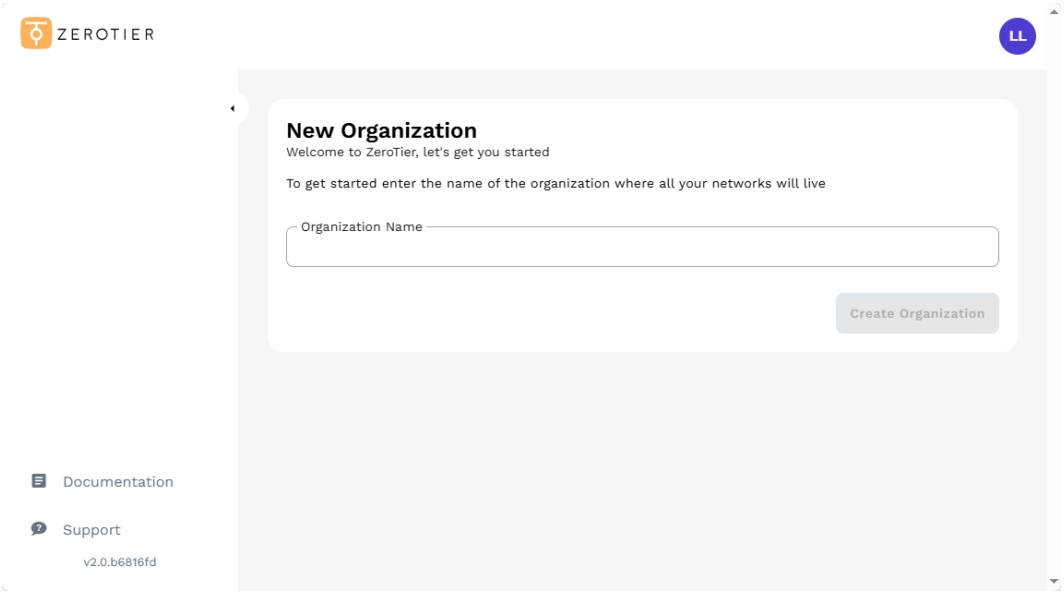
1. Die gleichzeitige Verwendung von ZeroTier mit folgenden Funktionen oder Diensten wird wegen möglicher Routingkonflikte nicht empfohlen: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale und AstroWarp.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

13.6.1 ZeroTier einrichten

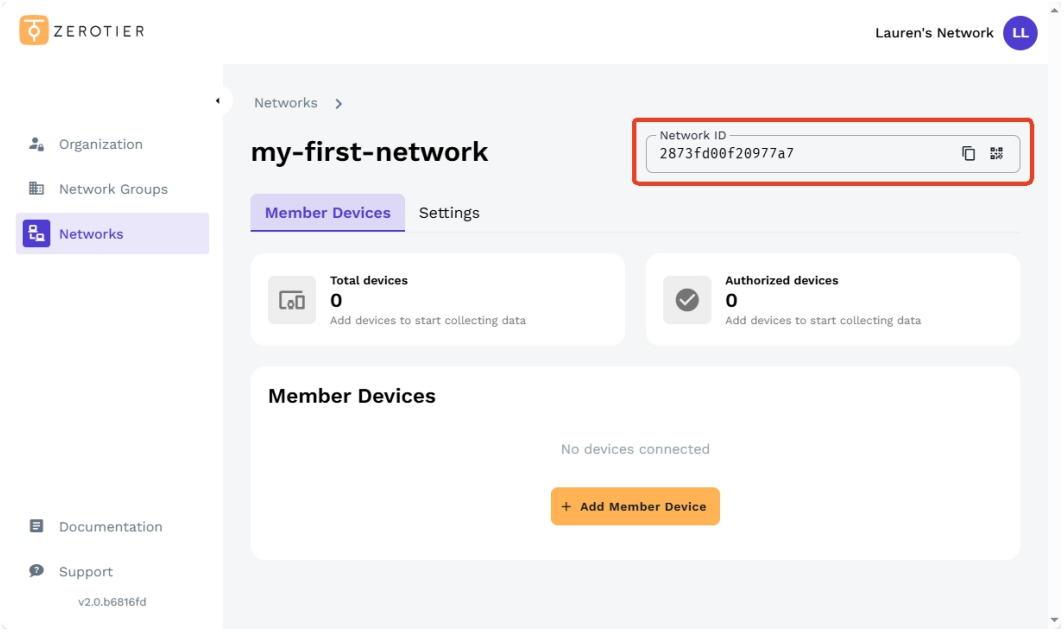
ZeroTier Central ist in zwei Versionen verfügbar: New Central und Legacy Central.

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.

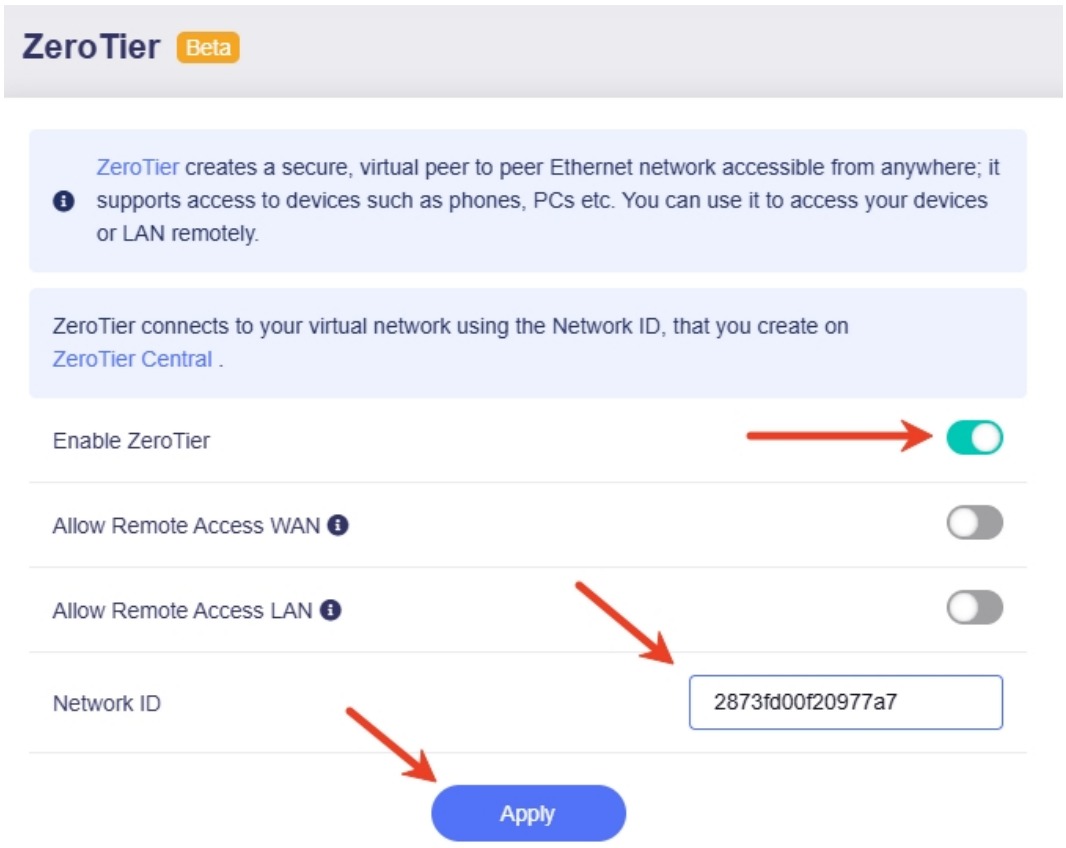


3. Wählen Sie einen Tarif aus. In diesem Beispiel verwenden wir den **Personal-Tarif** mit zehn Geräten, einem Netzwerkadministrator und einem Netzwerk. Wenn Sie mehr Netzwerke, zusätzliche Geräte, eigene Routen oder DNS-Einstellungen benötigen, wählen Sie einen kostenpflichtigen Tarif.
4. Ihr ZeroTier-Netzwerk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

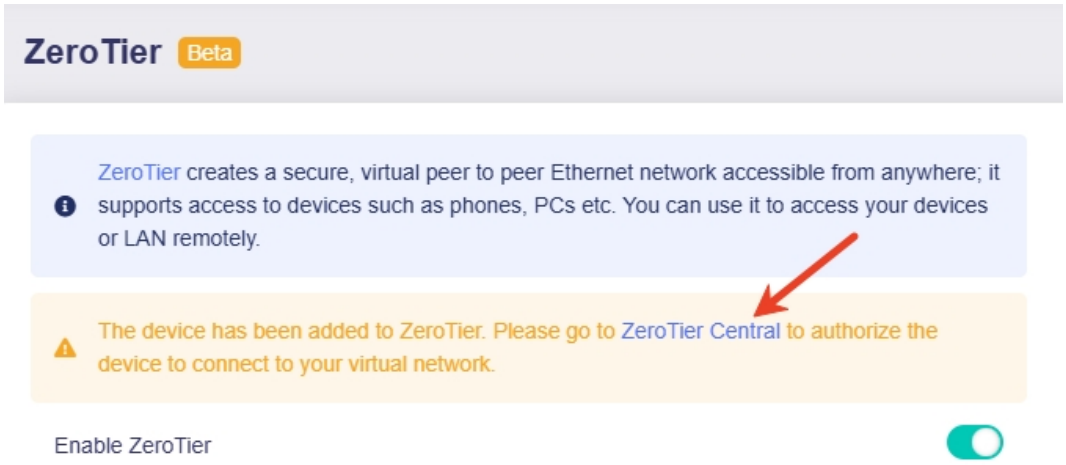


Notieren Sie die **Network ID** oben rechts. Diese besteht aus 16 Buchstaben und Ziffern und wird später benötigt, um weitere Geräte zu verbinden.

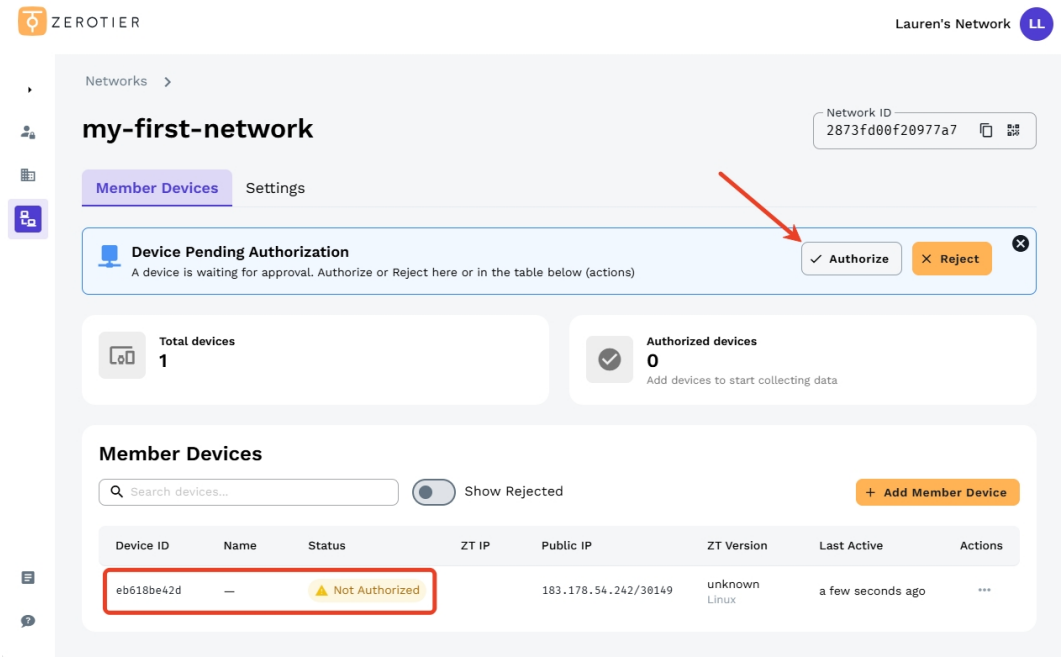
5. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **APPLICATIONS** > **ZeroTier**. Aktivieren Sie ZeroTier, geben Sie die **Network ID** ein und klicken Sie auf **Apply**.



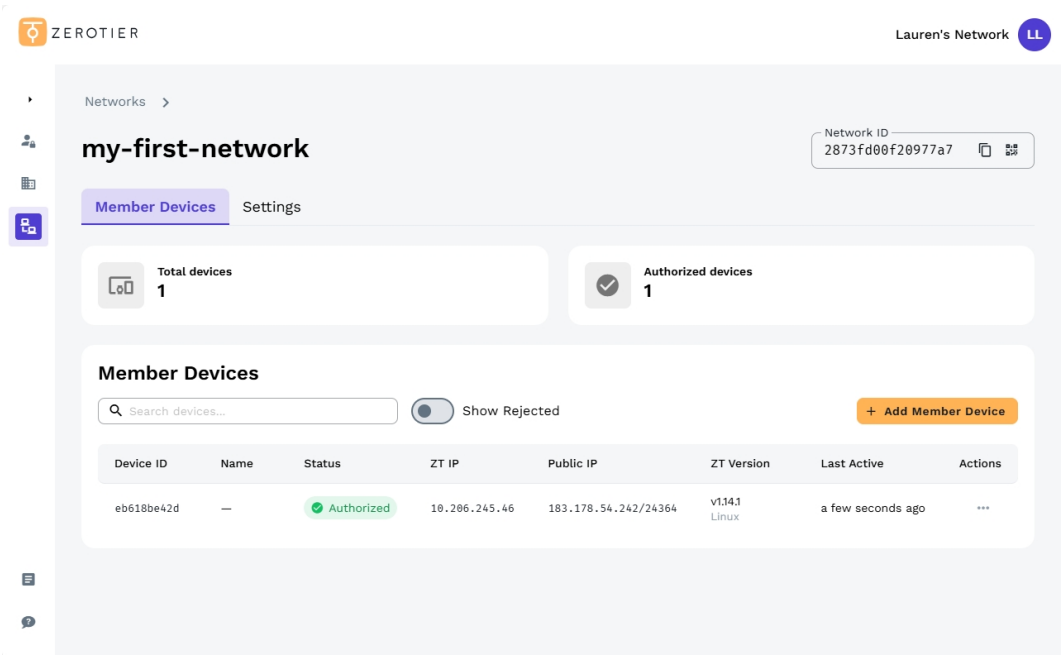
Nach kurzer Zeit erscheint der Hinweis, dass eine Autorisierung erforderlich ist. Klicken Sie auf den Link **ZeroTier Central**, um ZeroTier Central zu öffnen.



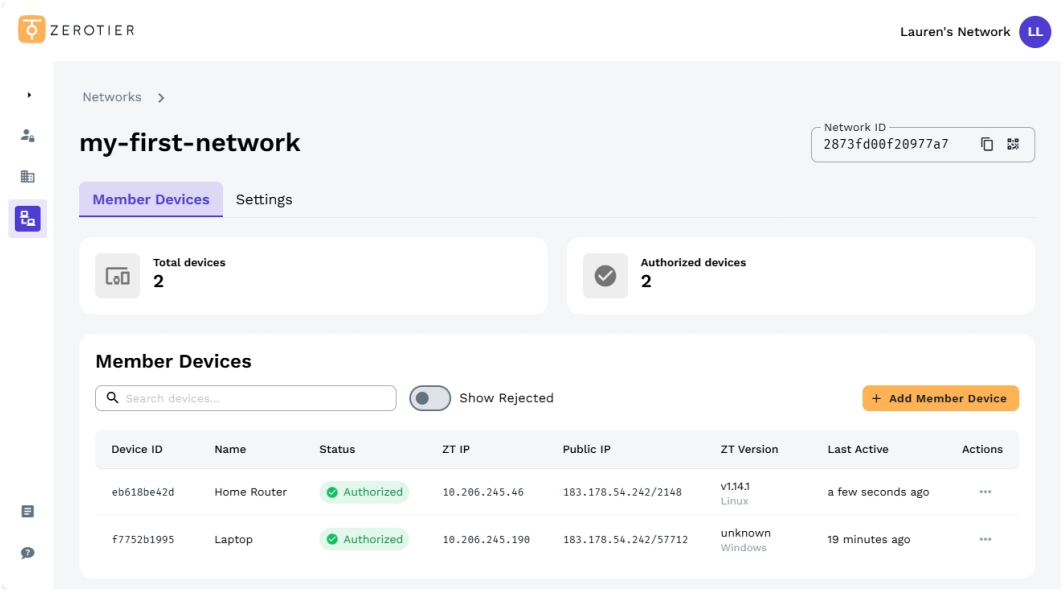
6. Suchen Sie in ZeroTier Central das ausstehende Gerät unter Pending und autorisieren Sie es.



Nach der Autorisierung erscheint die folgende Ansicht.

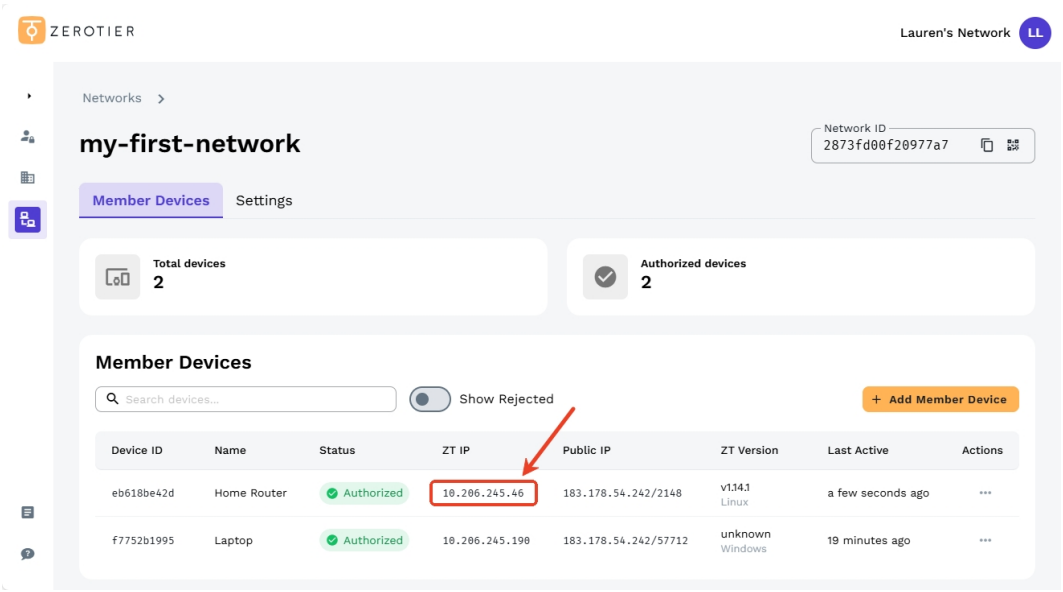


7. Fügen Sie ein weiteres Gerät, etwa einen Computer oder ein Smartphone, gemäß dieser Anleitung demselben ZeroTier-Netzwerk hinzu. Nach erfolgreichem Hinzufügen erscheint die folgende Seite. Hier sehen Sie die Angaben zu den Mitgliedsgeräten, darunter **Device ID**, **Name**, **Status**, **Managed IP** und **Public IP**.



Tipp: Klicken Sie rechts auf das Symbol mit den drei Punkten, um Einstellungen eines Mitgliedsgeräts zu bearbeiten, etwa Gerätename, verwaltete IP-Adressen und erweiterte Einstellungen.

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



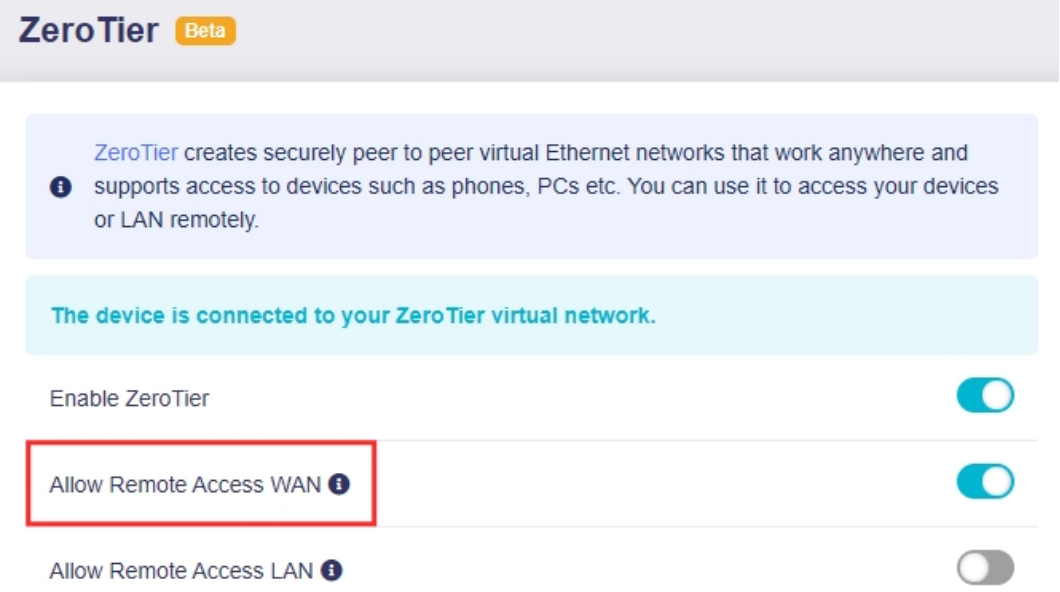
Über diese verwaltete IP-Adresse können Sie von einem Laptop im selben ZeroTier-Netzwerk auf den Router zugreifen.

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.

13.6.2 Fernzugriff auf WAN erlauben

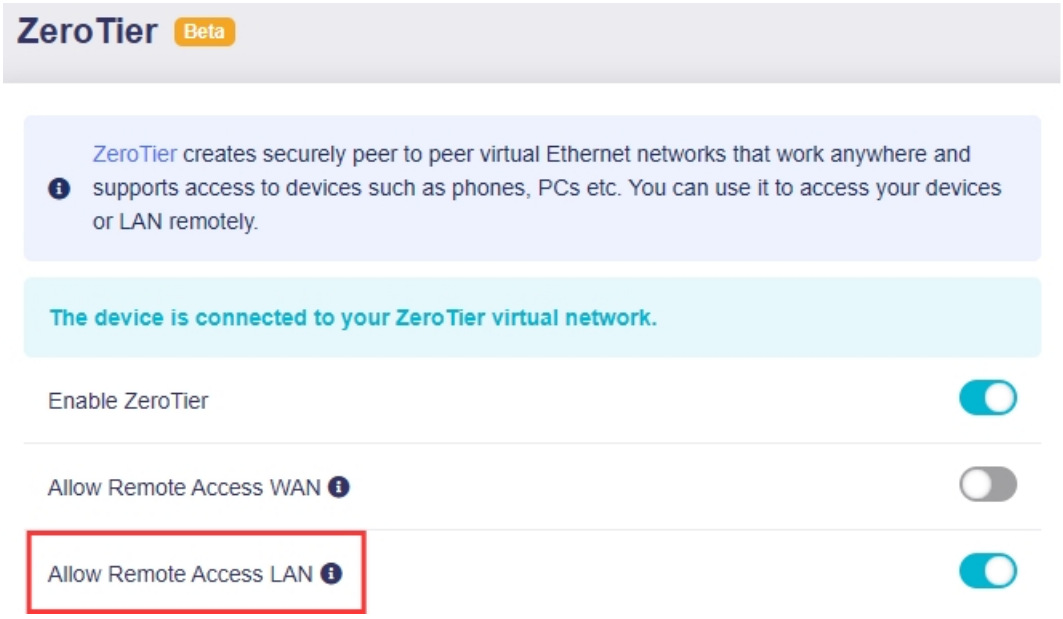
Diese Option erlaubt den Zugriff auf Ressourcen auf der WAN-Seite des Geräts über das virtuelle ZeroTier-Netzwerk. Weitere Informationen finden Sie hier.



Hinweis: Damit diese Funktion wirksam wird, müssen Sie dem ZeroTier-Netzwerk Routingregeln hinzufügen. In Legacy Central kann eine benutzerdefinierte Route kostenlos hinzugefügt werden. In New Central können benutzerdefinierte Routen nur mit einem Essential-Tarif oder höher konfiguriert werden. ZeroTier-Preise

13.6.3 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 kann eine benutzerdefinierte Route kostenlos hinzugefügt werden. In New Central können benutzerdefinierte Routen nur mit einem Essential-Tarif oder höher konfiguriert werden. ZeroTier-Preise

13.7 Tailscale

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

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.

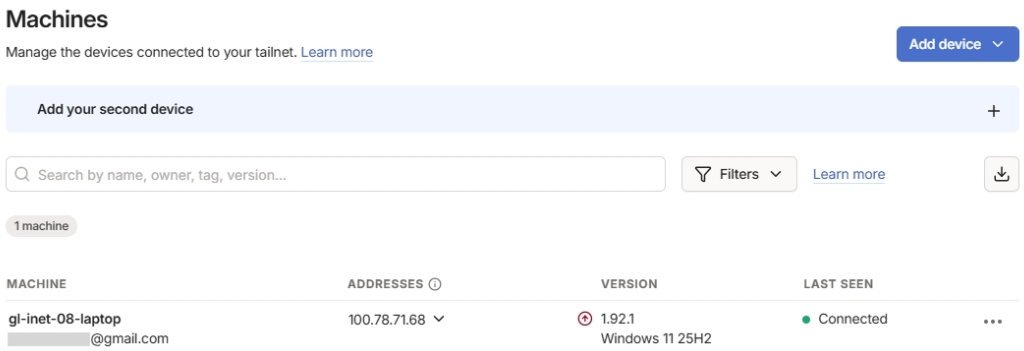
Hinweis:

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. Diese Funktion wird ab Firmware v4.9 verfügbar sein.

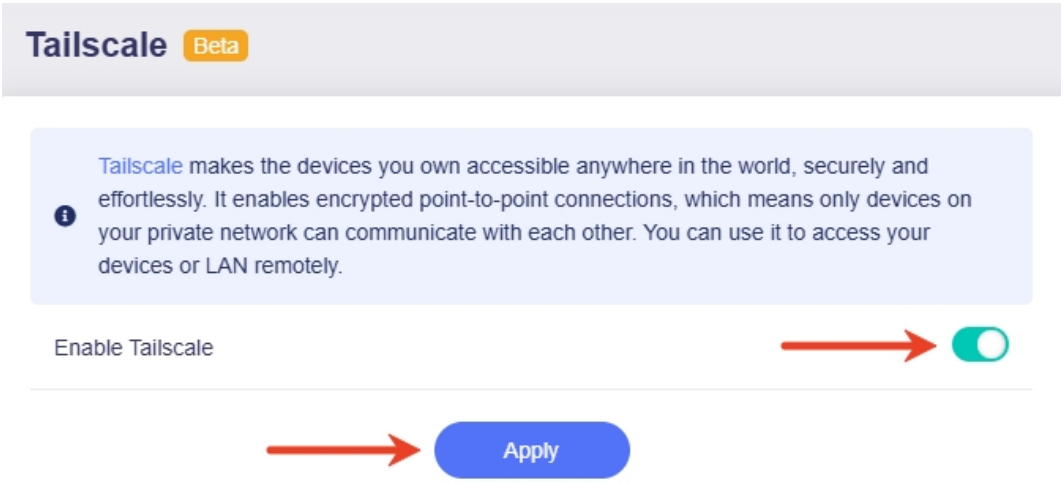
13.7.1 Tailscale einrichten

Im folgenden Beispiel werden ein Beryl AX (GL-MT3000) und ein Laptop verwendet.

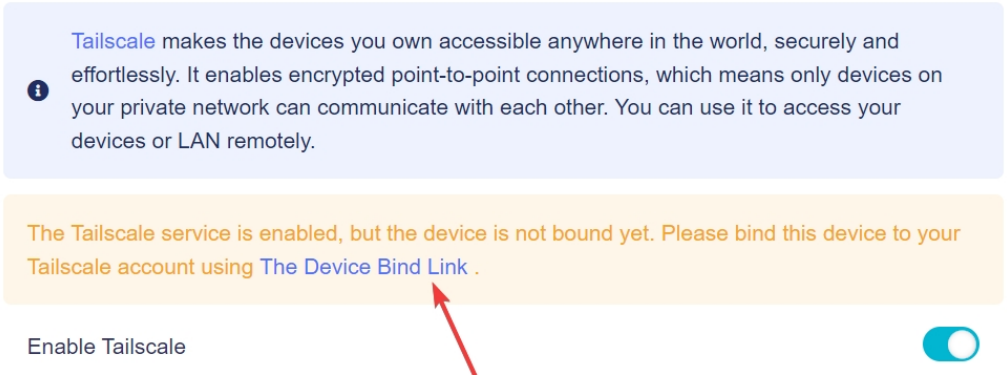
1. Registrieren Sie zunächst ein Tailscale-Konto und verknüpfen Sie zu Testzwecken ein oder zwei Geräte damit. Anschließend werden diese in der Tailscale-Konsole angezeigt.



2. Melden Sie sich an der Weboberfläche Ihres Routers 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**.



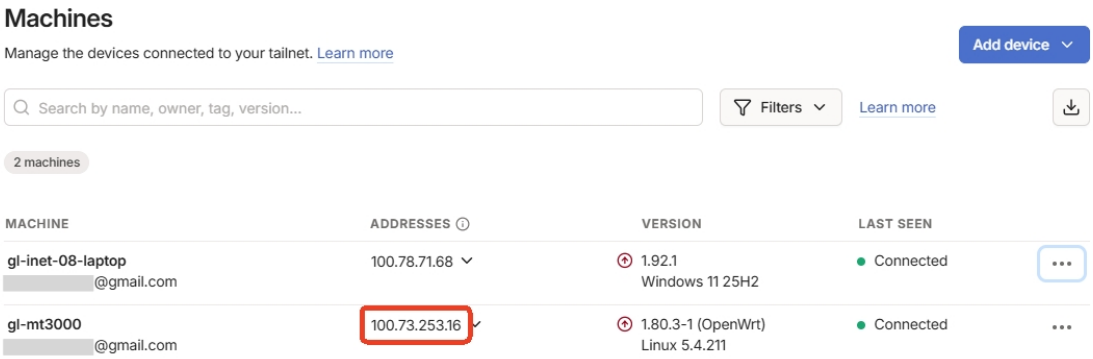
4. Klicken Sie im eingeblendeten Fenster auf den Link und melden Sie sich mit Ihrem Tailscale-Konto an.



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



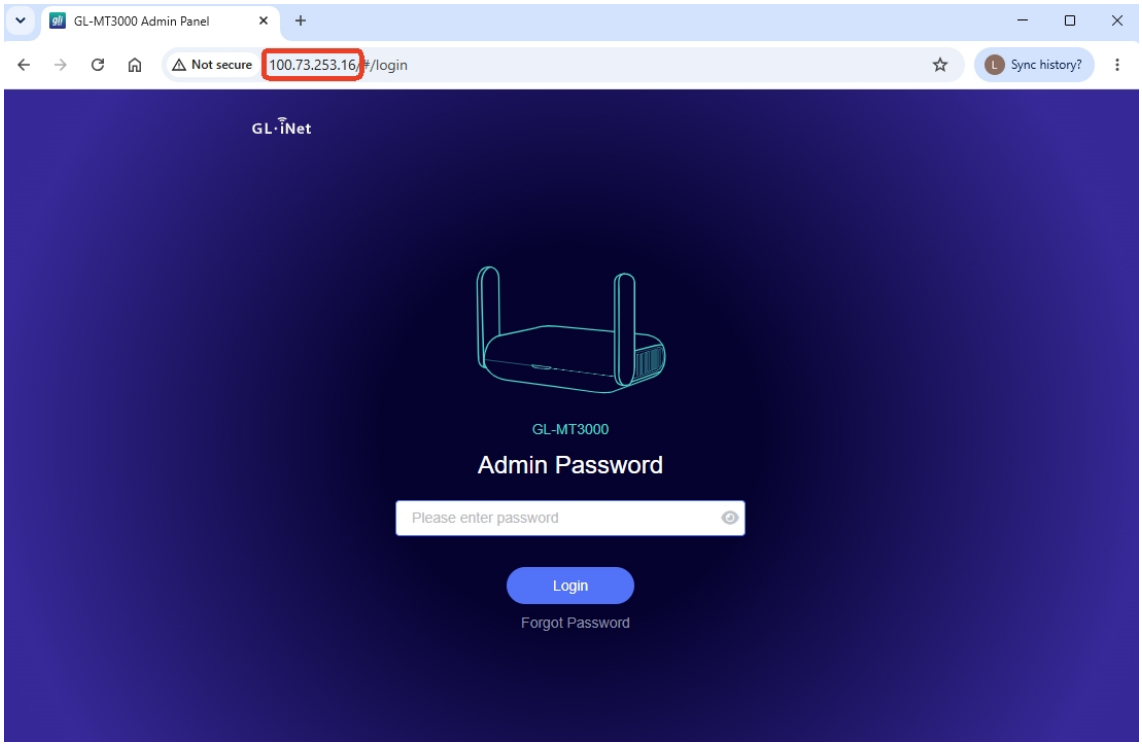
6. Sie werden zur Tailscale-Verwaltungskonsole weitergeleitet. Der Router wurde dem virtuellen Tailscale-Netzwerk hinzugefügt und ist nun über seine virtuelle Tailscale-IP-Adresse **100.73.253.16** aus der Ferne erreichbar.



7. Verbindung prüfen.

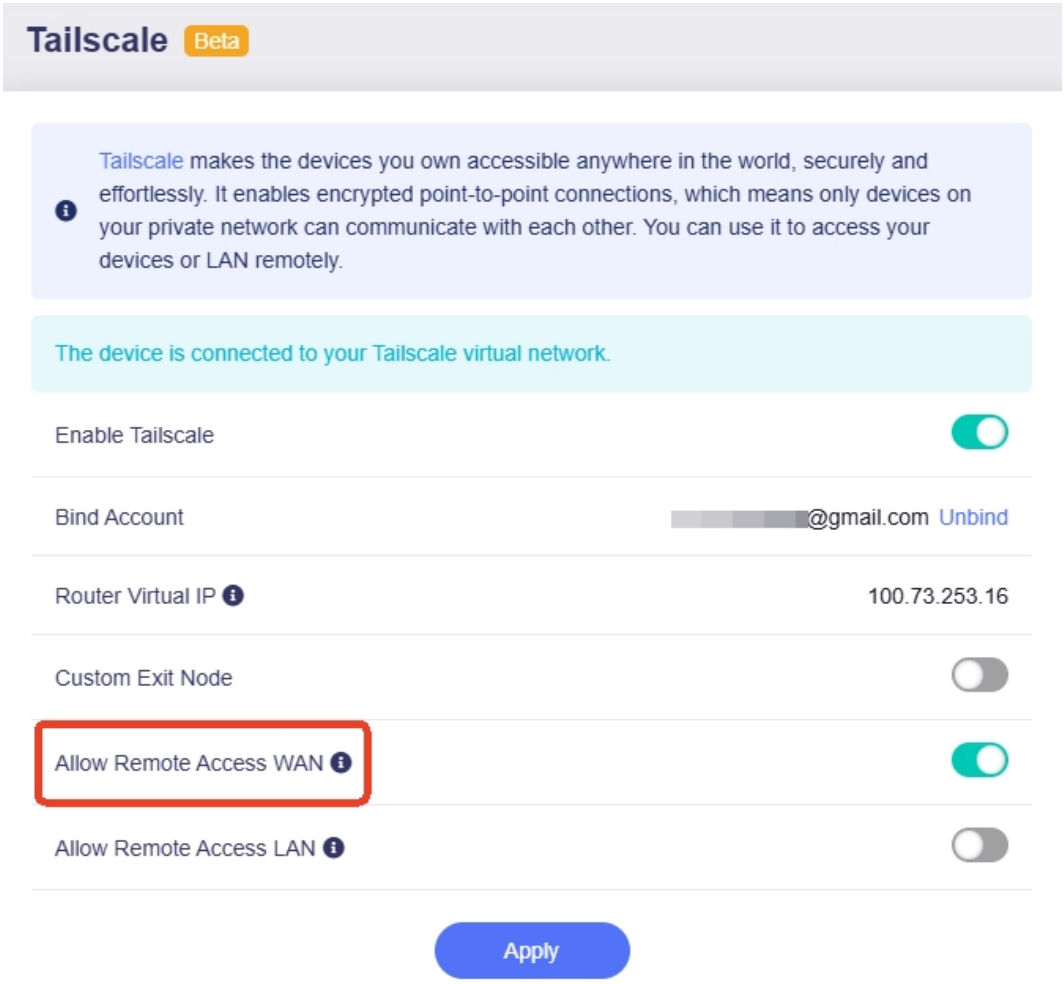
   Öffnen Sie auf einem anderen Gerät im selben Tailscale-Netzwerk einen Webbrowser und geben Sie die virtuelle IP-Adresse des Routers ein. Wenn Sie seine Weboberfläche

erreichen, funktioniert Tailscale. Alternativ können Sie die Verbindung mit ping oder durch eine SSH-Anmeldung am Routerterminal über die virtuelle IP-Adresse prüfen.



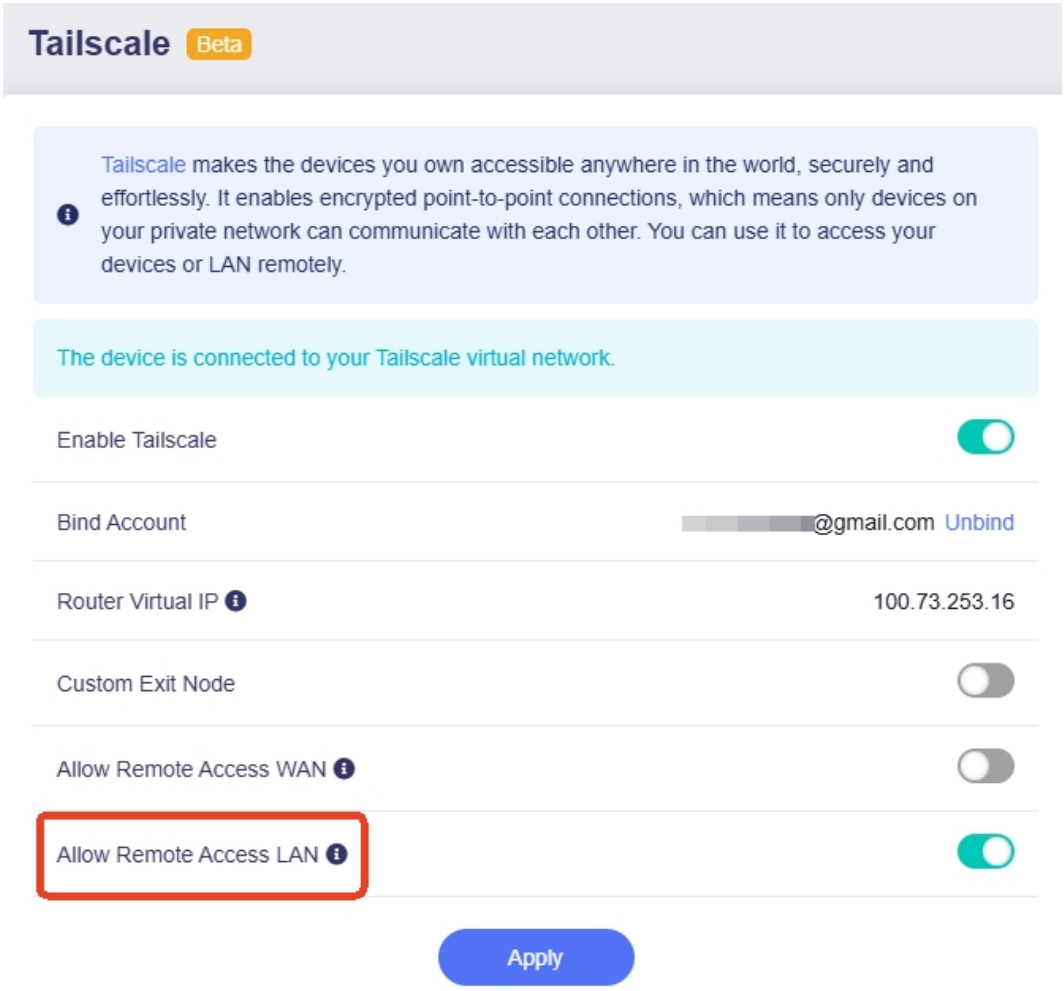
13.7.2 Fernzugriff auf WAN erlauben

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



13.7.3 Fernzugriff auf LAN erlauben

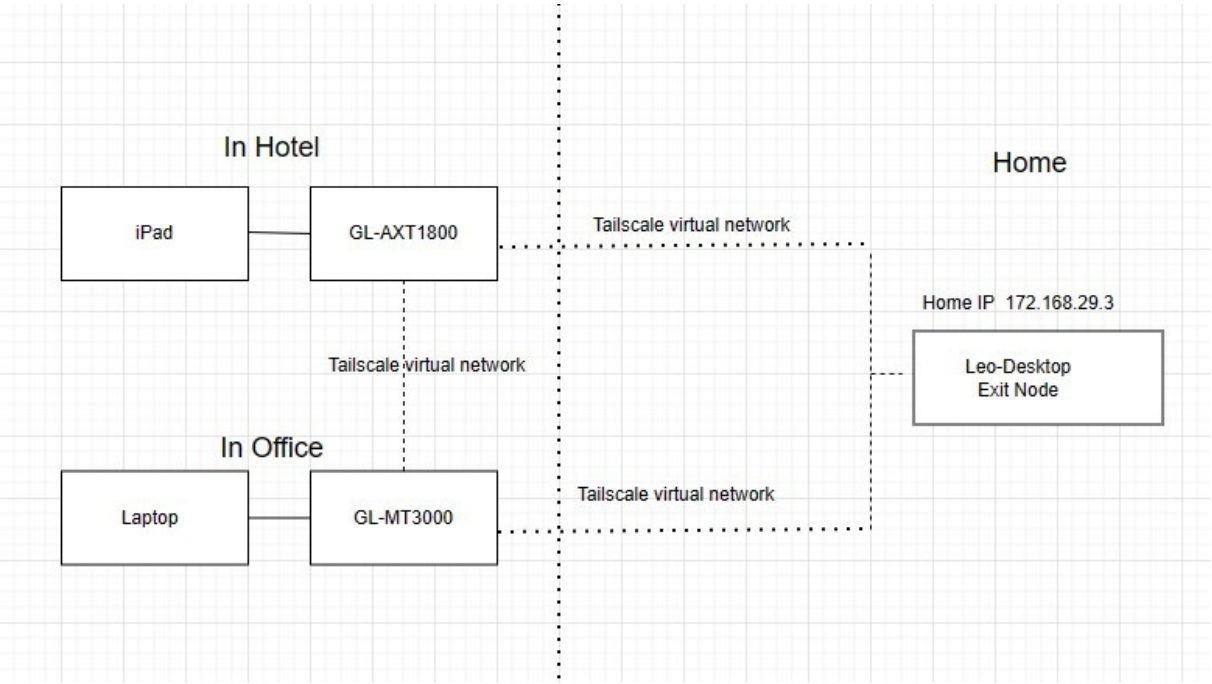
Diese Option erlaubt den Zugriff auf Ressourcen auf der LAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk. Weitere Informationen finden Sie hier.



13.7.4 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.



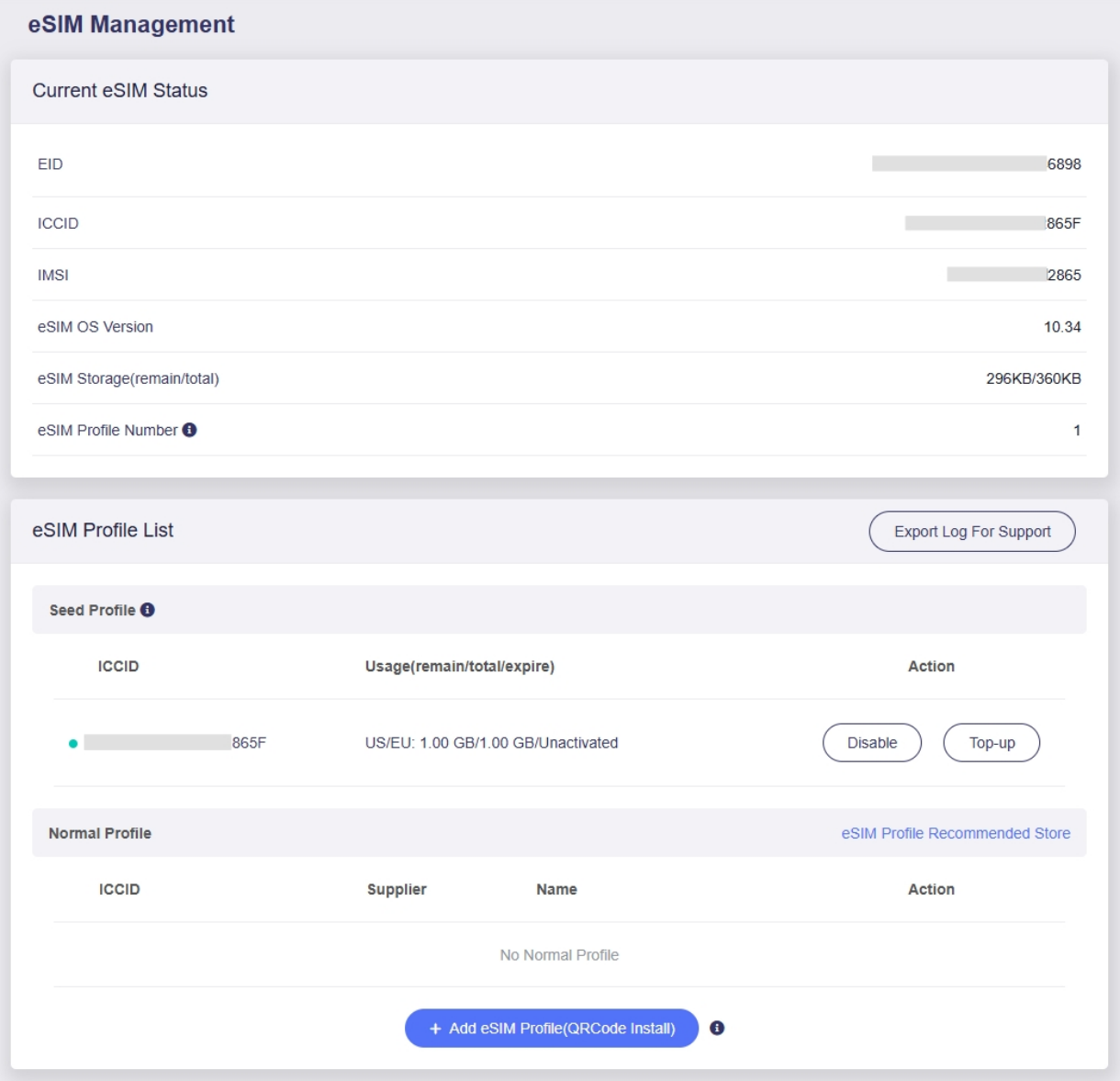
Ein Exit-Node leitet also den ausgehenden Internetdatenverkehr Ihrer Tailnet-Geräte weiter und übernimmt damit die Rolle eines VPN-Servers. Bei einer Verbindung über einen Exit-Node scheint Ihr gesamter Internetdatenverkehr außerhalb von Tailscale von dessen Standort zu stammen. So können Sie regional beschränkte Inhalte erreichen und Ihre Privatsphäre verbessern. Das Gerät, das diese Weiterleitung übernimmt, wird als „Exit-Node“ bezeichnet. Zur Einrichtung auf GL.iNet-Routern lesen Sie diese Anleitung.

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.

13.8 eSIM-Verwaltung

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **APPLICATIONS** > **eSIM Management**.

Auf dieser Seite können Sie den Status der physischen eSIM-Karte prüfen und eSIM-Profile verwalten. Sie besteht aus den Bereichen **Current eSIM Status** und **eSIM Profile List**.



13.8.1 Aktueller eSIM-Status

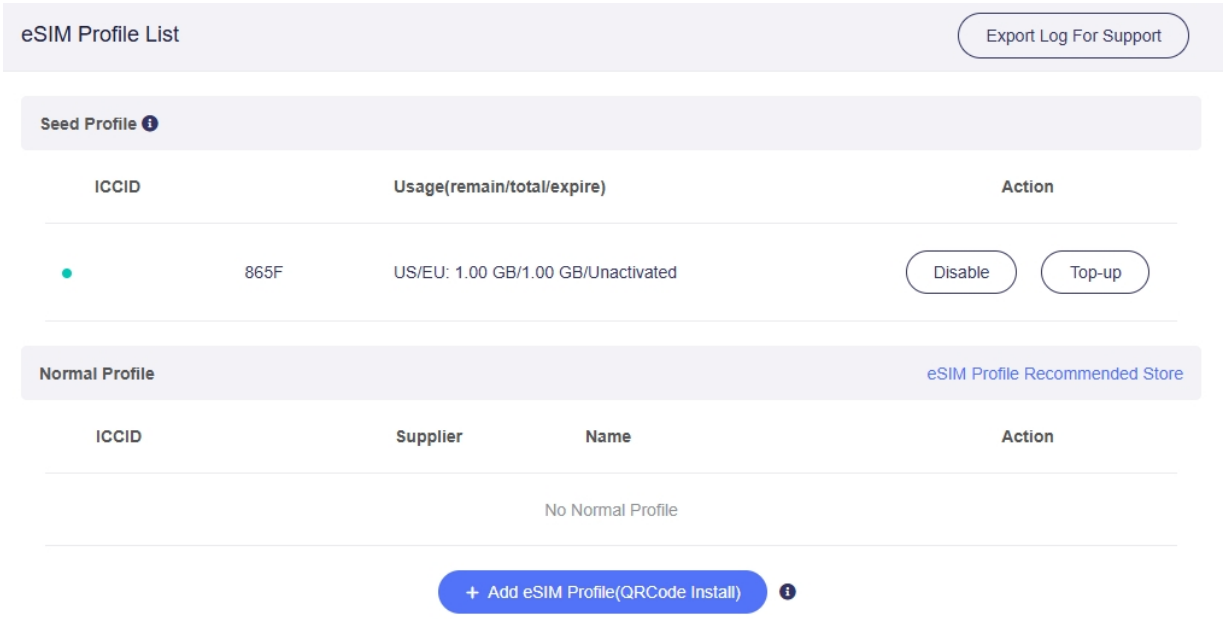
Dieser Bereich zeigt grundlegende Informationen und Details zum aktuell aktiven eSIM-Profil an.



- **EID:** Die weltweit eindeutige Kennung der eUICC (eSIM-Chip), die zur Identifizierung und Profilverwaltung verwendet wird.
- **ICCID:** Die Integrated Circuit Card Identifier des derzeit aktiven eSIM-Profils.
- **IMSI:** Die International Mobile Subscriber Identity des derzeit aktiven eSIM-Profils.
- **eSIM OS Version:** Die Betriebssystemversion der eUICC, die deren Kompatibilität und unterstützte Funktionen bestimmt.
- **eSIM Storage (remain/total):** Der verfügbare und der gesamte Speicherplatz auf der eUICC zum Speichern von eSIM-Profilen.
- **eSIM Profile Number:** Die Anzahl der derzeit auf der eUICC gespeicherten eSIM-Profile. Da die Profile verschiedener Anbieter unterschiedlich groß sind, variiert auch die Anzahl der Profile, die auf der eUICC gespeichert werden können.

13.8.2 eSIM-Profilliste

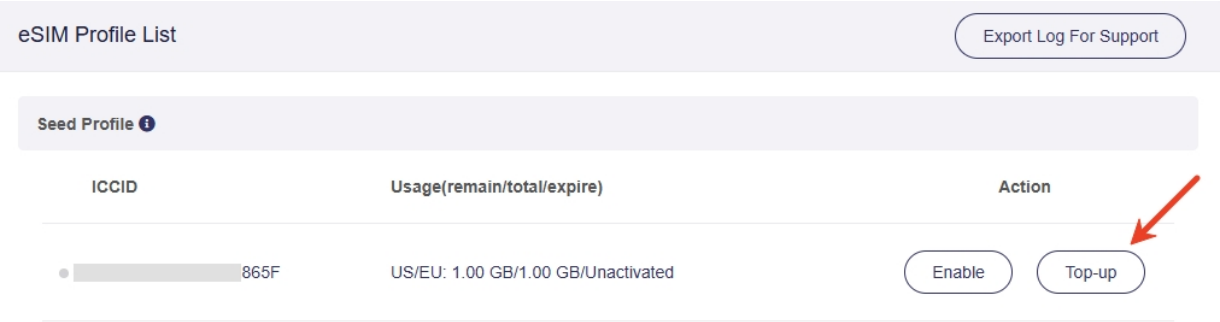
Dieser Bereich zeigt Informationen zum Seed-Profil und zu den regulären Profilen an.



- **Seed Profile**: Das vorinstallierte Seed-Profil enthält 1 GB kostenloses Datenvolumen für die USA und Europa sowie 100 MB weltweit nutzbares Datenvolumen. Es ist ab dem Aktivierungsdatum ein Jahr lang gültig. Mit diesem Datenvolumen können Sie überall auf der Welt weitere Profile herunterladen. Außerdem können Sie die Nutzung des Seed-Profils überwachen, einschließlich des verbleibenden Datenvolumens, des gesamten Datenkontingents und des Ablaufdatums.
- **Normal Profile**: Wenn Sie ein eSIM-Profil kaufen und über einen QR-Code oder Aktivierungscode hochladen, wird es hier angezeigt.

13.8.2.1 Seed-Profil aufladen

GL.iNet stellt ein vorinstalliertes Seed-Profil mit 100 MB weltweit nutzbarem Datenvolumen und 1 GB Datenvolumen für Europa und die USA bereit. Es dient der Ersteinrichtung und Aktivierung von eSIM-Profilen. Dieser Tarif ermöglicht das Herunterladen neuer eSIM-Profile, wenn Sie an einem Reiseziel ohne Internetzugang ankommen.
Wenn Sie das kostenlose vorinstallierte Datenvolumen aufgebraucht haben oder es abgelaufen ist und Sie den Dienst weiter nutzen möchten, können Sie Ihr Seed-Profil aufladen.
Klicken Sie im Bereich Seed Profile rechts auf die Schaltfläche **Top-up**.



Scannen Sie im eingeblendeten Fenster den QR-Code und folgen Sie den Anweisungen, um das Guthaben aufzuladen.

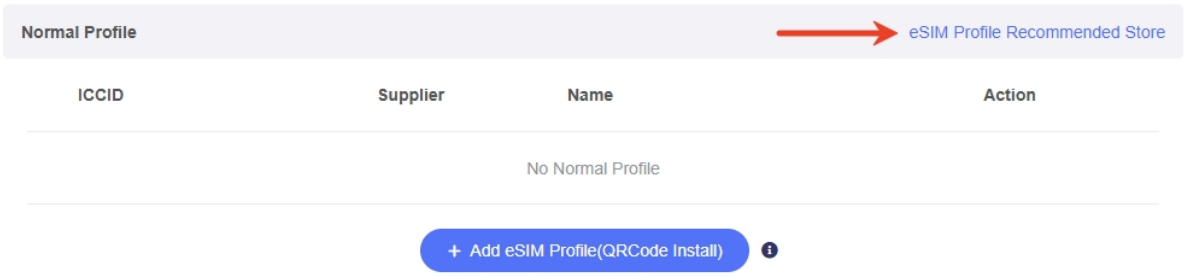


13.8.2.2 eSIM-Profil kaufen

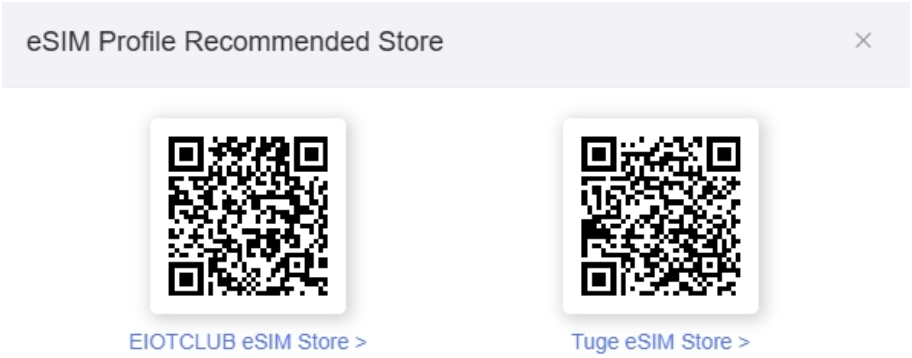
Sie können eSIM-Profile in unseren empfohlenen oder getesteten Shops sowie bei anderen eSIM-Drittanbietern kaufen.

Option 1: Kauf in unseren empfohlenen Shops.
Es gibt zwei empfohlene Shops: EIOTCLUB eSIM Store und Tuge eSIM Store.

Klicken Sie im Bereich Normal Profile rechts auf **eSIM Profile Recommended Store**.



Scannen Sie den QR-Code oder klicken Sie auf die Links, um eSIM-Profile zu kaufen.



Hinweis: Alle in diesen beiden Shops gekauften eSIM-Profilpakete sind vollständig mit GL.iNet-Routern kompatibel. Bei Fragen wenden Sie sich an unser Supportteam unter support@gl-inet.com.

Option 2: Kauf in getesteten Shops.

Eine Liste der von GL.iNet getesteten Shops finden Sie unter diesem Link.

Hinweis: Wir können die vollständige Kompatibilität aller Profile und Pakete dieser Shops mit GL.iNet-Routern nicht garantieren. Da GL.iNet keine Partnerschaften mit diesen Anbietern unterhält, können wir keinen Kundendienst nach dem Kauf leisten oder bei Erstattungen helfen.

Option 3: Kauf bei anderen eSIM-Drittanbietern.

Sie können eSIM-Profile auch bei anderen Drittanbietern Ihrer Wahl kaufen.

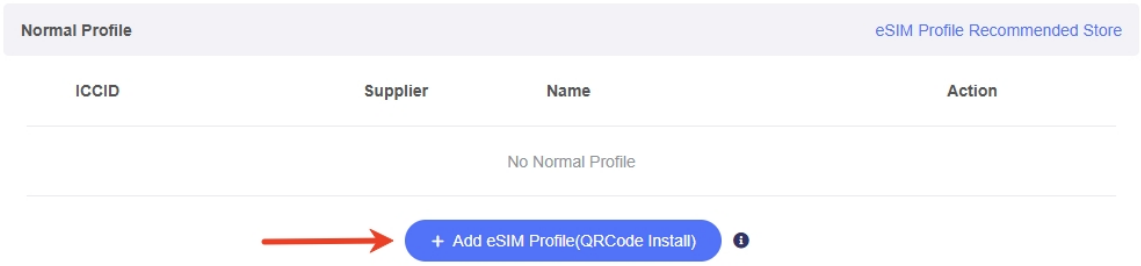
Für eSIM-Profile anderer Drittanbieter können wir jedoch keine vollständige Kompatibilität mit GL.iNet-Routern garantieren. Treffen Sie Ihre Kaufentscheidung nach eigenem Ermessen. GL.iNet übernimmt keine Verantwortung für Inkompatibilitäten.

Wenden Sie sich für Unterstützung nach dem Kauf oder für Erstattungen an den jeweiligen eSIM-Anbieter.

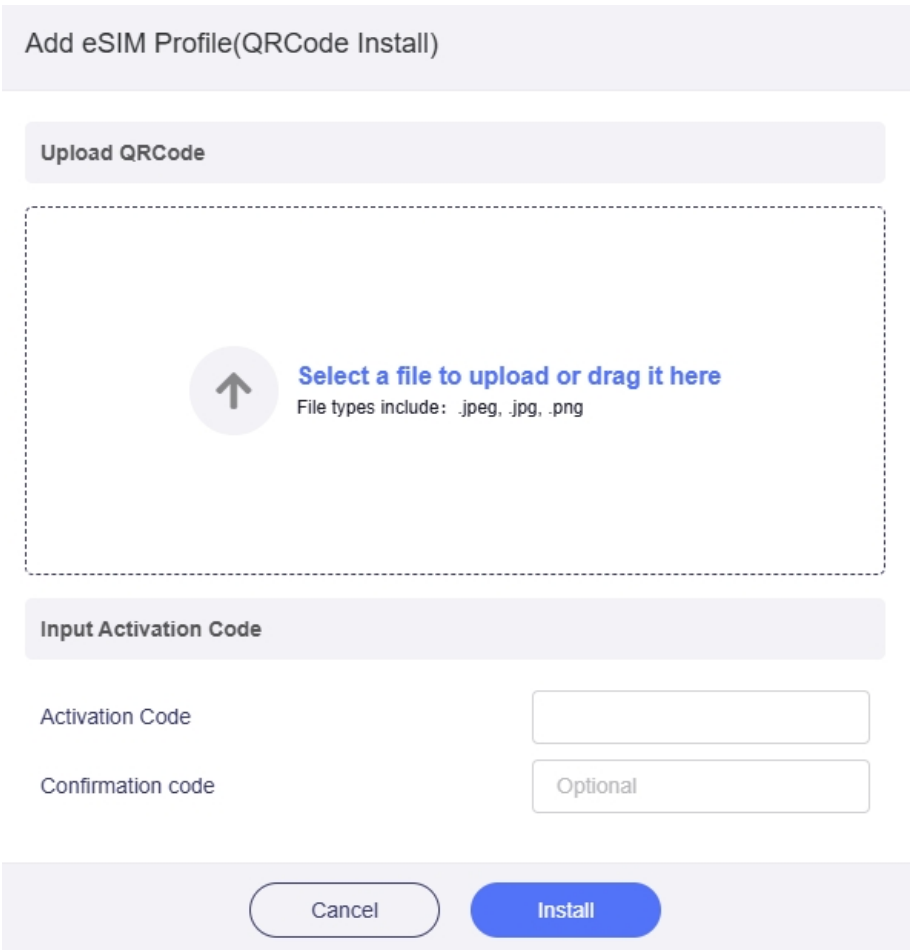
13.8.2.3 eSIM-Profil hochladen

Nach dem Kauf eines eSIM-Profils erhalten Sie in der Regel einen QR-Code oder einen Aktivierungscode. Speichern Sie den QR-Code lokal und gehen Sie anschließend wie folgt vor, um Ihr eSIM-Profil hochzuladen.

1. Klicken Sie im Bereich Normal Profile unten auf **Add eSIM Profile**.

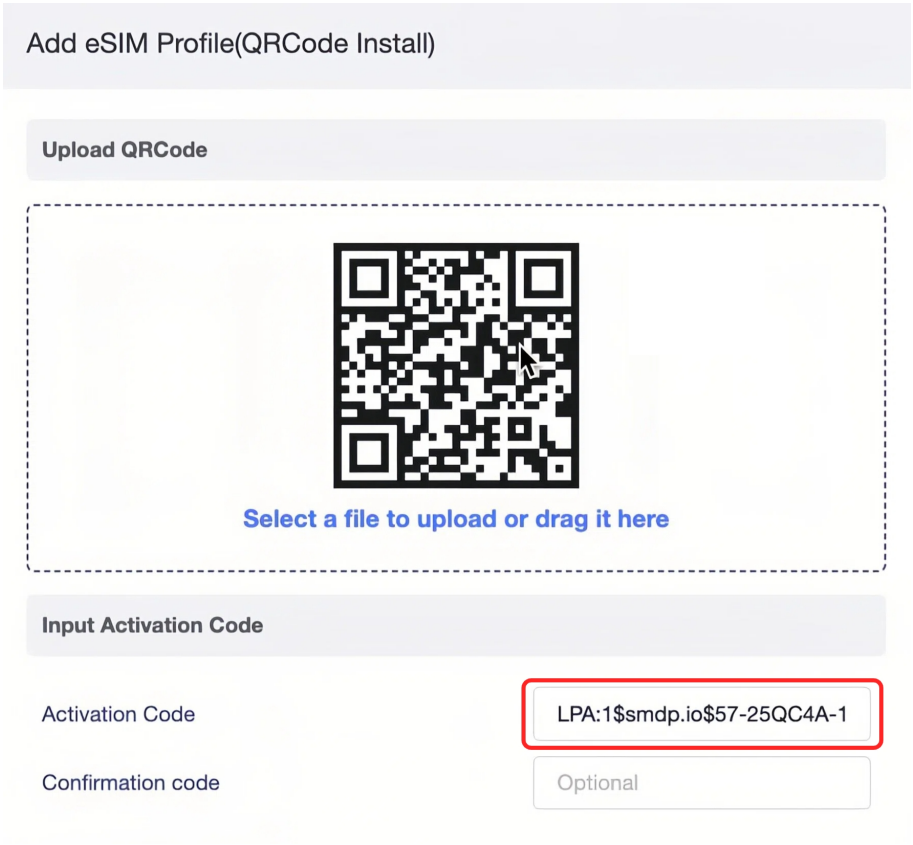


2. Laden Sie den QR-Code Ihrer eSIM hoch oder geben Sie den Aktivierungscode ein und klicken Sie auf **Install**. Das eSIM-Profil wird anschließend heruntergeladen und auf Ihrem Router installiert.



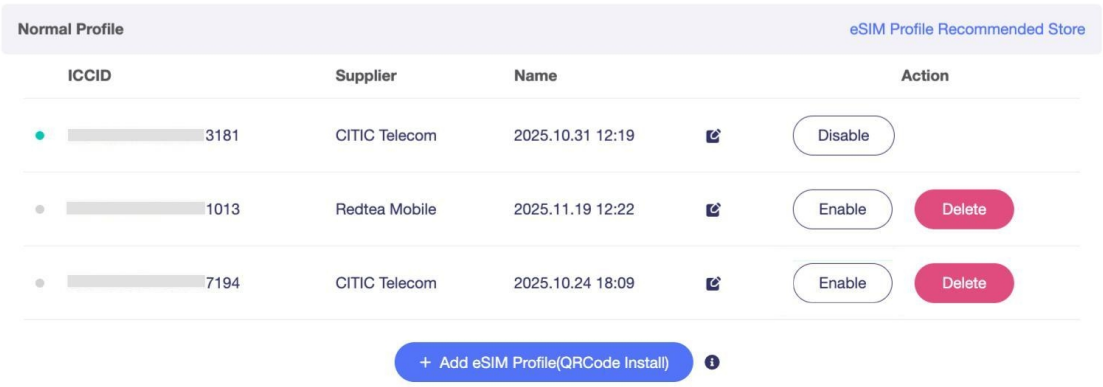
Hinweis:

1. Die meisten eSIM-Profile können nur einmal heruntergeladen und installiert werden.
2. Ein korrekt formatierter QR-Code zeigt einen Aktivierungscode an, der mit **LPA:** beginnt. Einige nicht standardkonforme QR-Codes enthalten jedoch nur einen Aktivierungscode ohne dieses Präfix. Fügen Sie in diesem Fall LPA: manuell am Anfang des Codes hinzu, bevor Sie auf Install klicken.

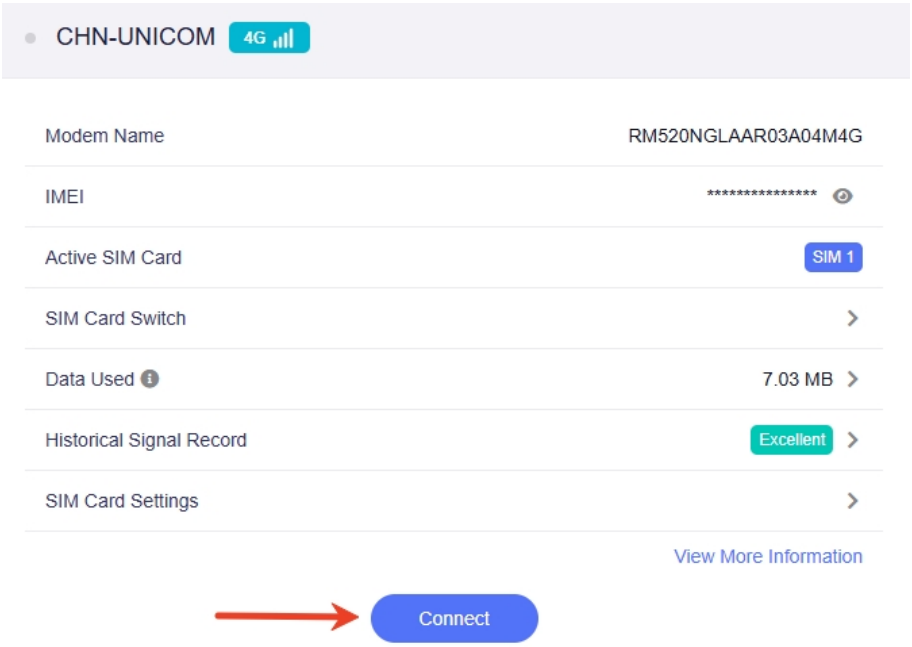


3. Wenn Sie noch kein eSIM-Profil gekauft haben, können Sie eines im empfohlenen Shop für eSIM-Profile erwerben. Einzelheiten finden Sie unter 13.8.2.2 eSIM-Profil kaufen.

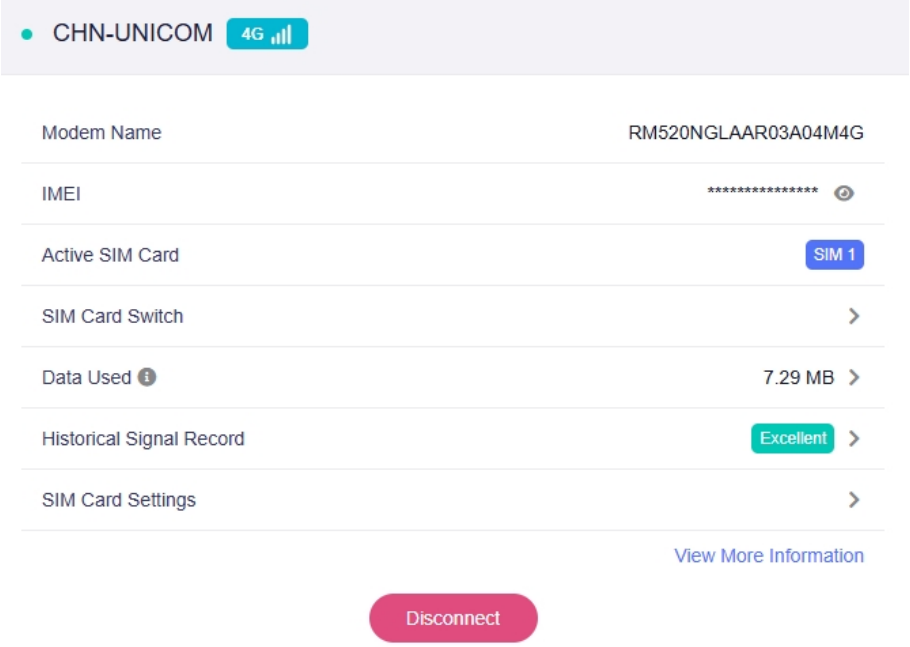
3. Nach dem erfolgreichen Hochladen erscheint Ihr neues eSIM-Profil in der Liste **Normal Profile**. Klicken Sie auf **Enable**, um es zu aktivieren.



4. Stellen Sie eine Internetverbindung her.
   Öffnen Sie nach dem Aktivieren des eSIM-Profils **INTERNET** > **Cellular**. Klicken Sie auf **Connect**, um über Ihr eSIM-Profil eine Internetverbindung herzustellen.

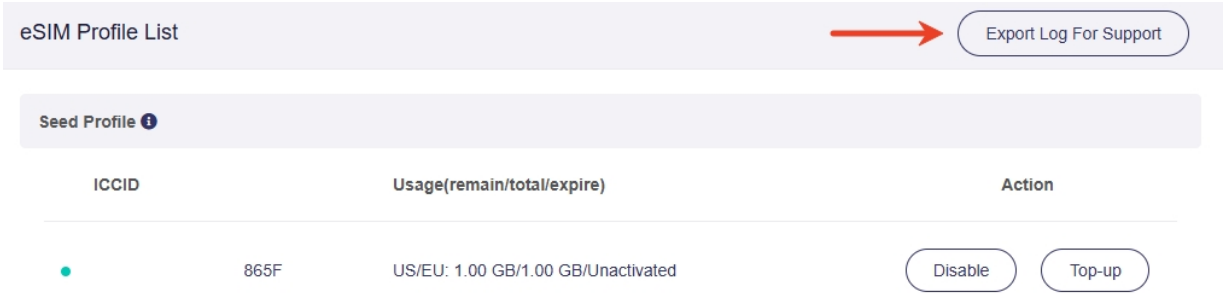


   Hinweis: Einige eSIM-Profile erfordern zusätzliche Einstellungen, etwa APN, PIN oder TTL. Klicken Sie bei Bedarf auf **Manual Setup** oder **SIM Card Settings**, um diese Parameter anzupassen. In manchen Fällen müssen Sie das Gerät neu starten, um eine Internetverbindung herzustellen.
5. Nach erfolgreicher Verbindung über das eSIM-Profil wird die Seite wie folgt angezeigt:



13.8.2.4 Protokoll für den Support exportieren

Klicken Sie auf **Export Log for Support**, um alle eSIM-bezogenen Protokolle anzuzeigen. Wenn Probleme auftreten und Sie technische Unterstützung benötigen, exportieren Sie die eSIM-Protokolle und senden Sie sie per E-Mail an unser Supportteam unter support@gl-inet.com.



Kapitel 14

Netzwerk

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

14.1 Portweiterleitung

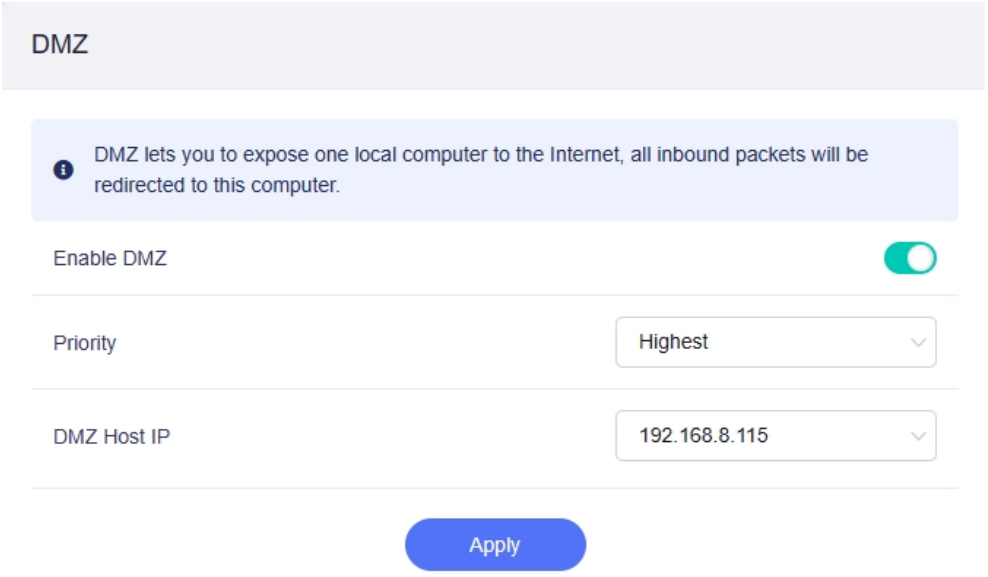
Portweiterleitung leitet externe Anfragen an bestimmte Geräte in Ihrem lokalen Netzwerk weiter. Die Seite Port Forwarding umfasst zwei zentrale Funktionen: **DMZ** für den direkten vollständigen Zugriff auf ein einzelnes Gerät und **Port Forwarding** für den gezielten Zugriff auf bestimmte Geräteports.

14.1.1 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**.



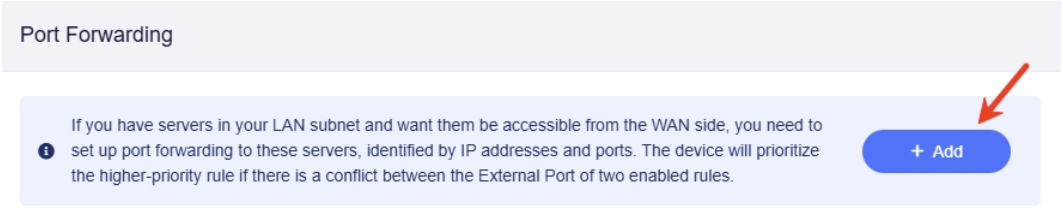
- **Priority**: Wählen Sie Highest oder Lowest. Hat DMZ eine höhere Priorität als die Portweiterleitungsregeln, werden alle Portweiterleitungsregeln außer Kraft gesetzt. Andernfalls werden Anfragen nur dann an das DMZ-Endgerät weitergeleitet, wenn für den angefragten Port keine Portweiterleitungsregel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

14.1.2 Portweiterleitung

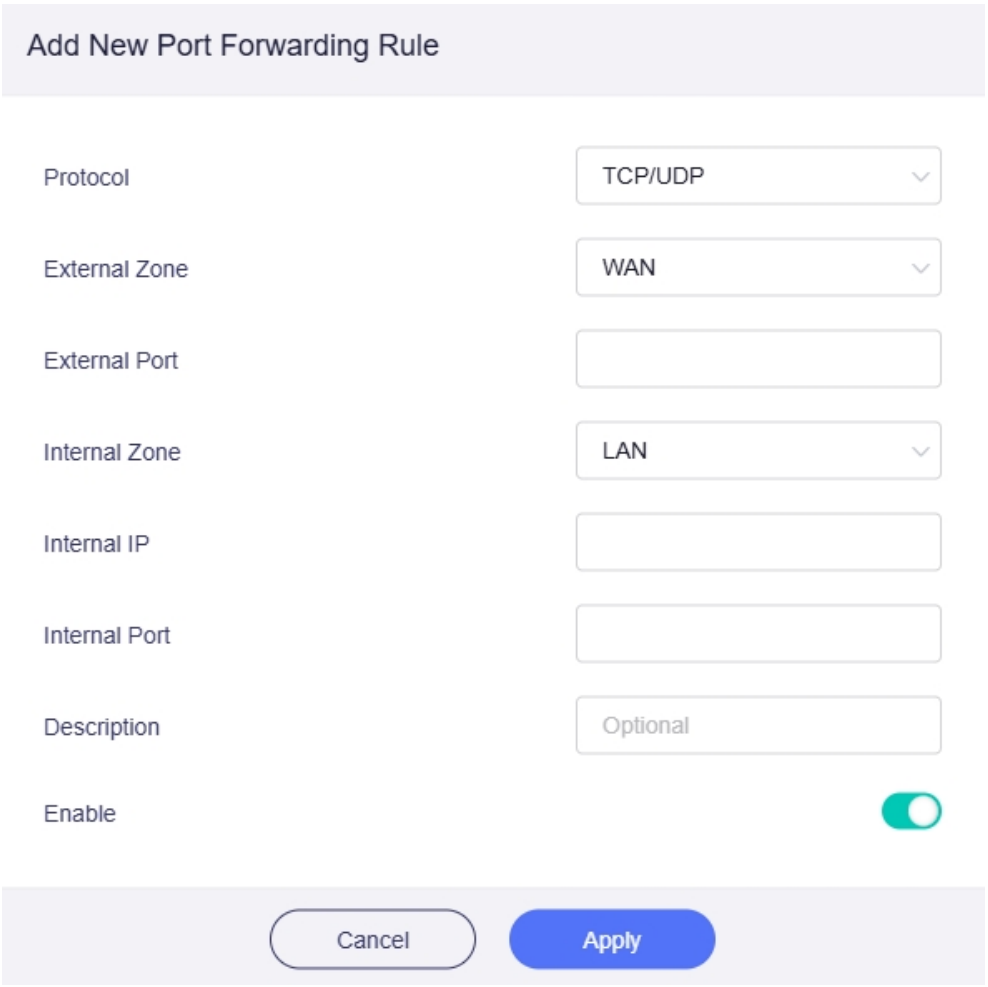
Portweiterleitungen ermöglichen entfernten Computern die Verbindung mit einem lokalen Computer oder Server hinter der LAN-Firewall, beispielsweise einem Web- oder FTP-Server.

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

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

14.2 Multi-WAN

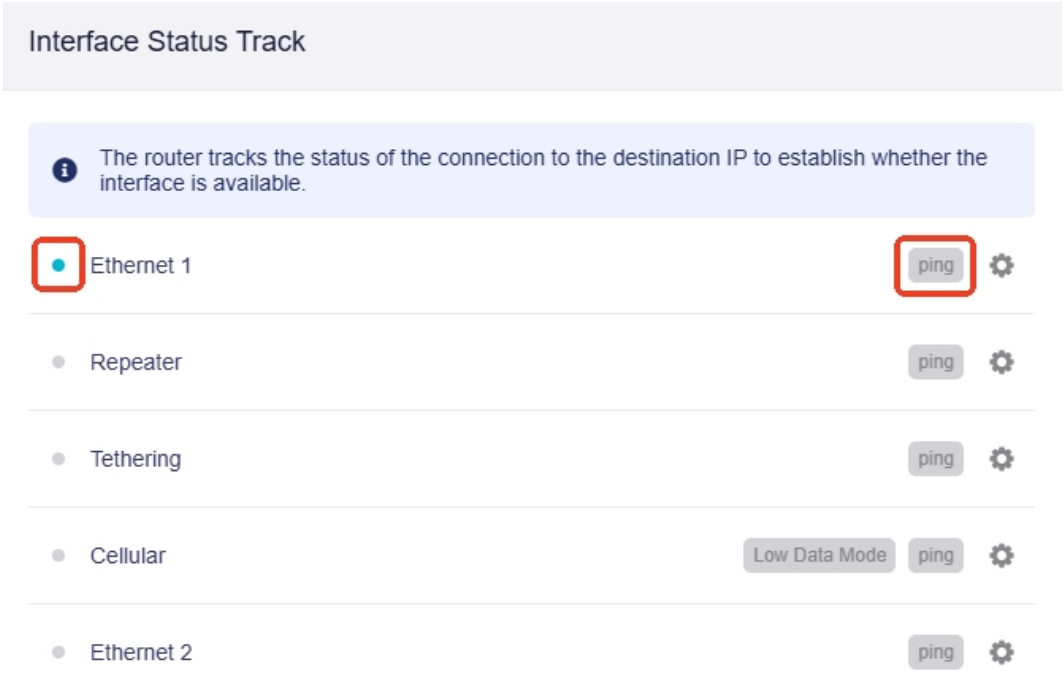
Multi-WAN ermöglicht die gleichzeitige Nutzung mehrerer Internetzugangsarten und bietet unterschiedliche Verbindungsoptionen auf dem Router. Es stehen zwei Betriebsmodi zur Verfügung:

- **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.

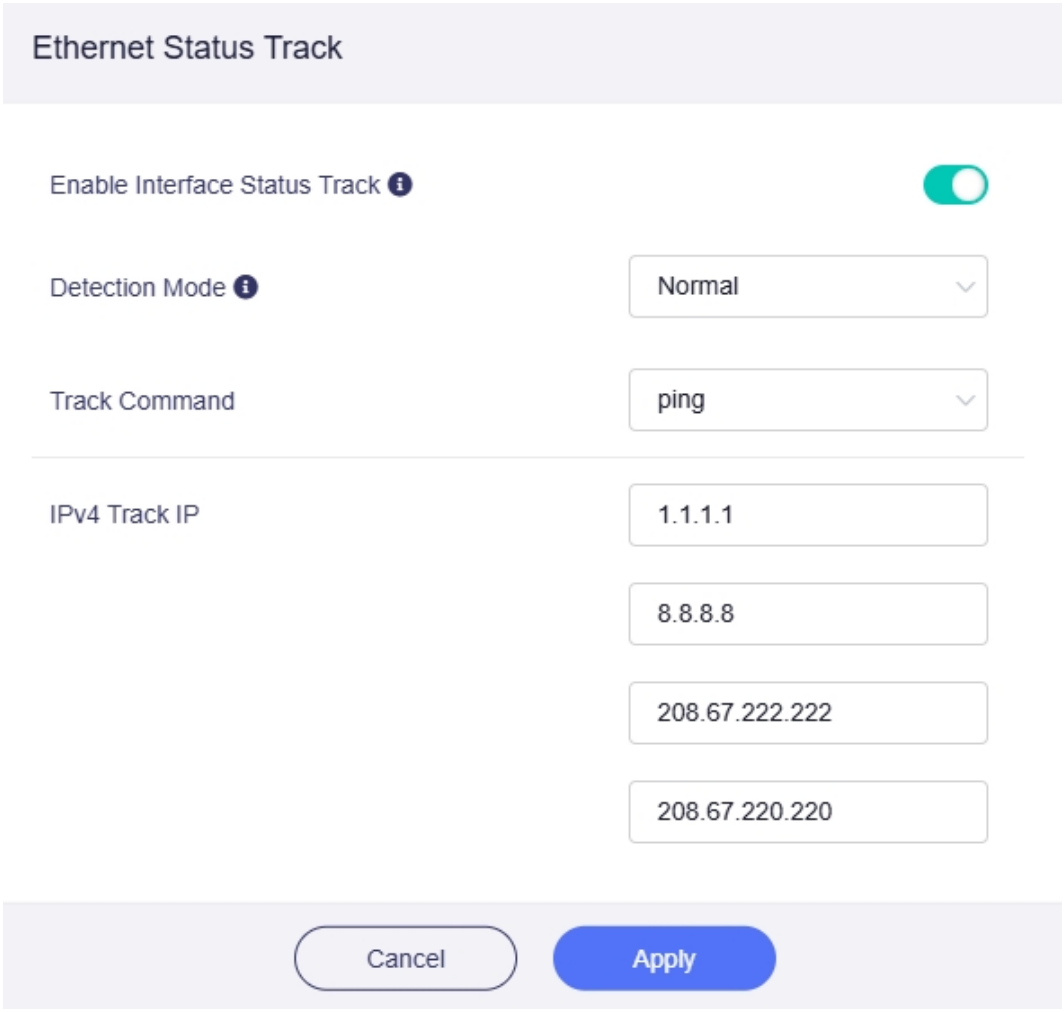
Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Multi-WAN**. Die Seite enthält die Abschnitte Interface Status Track und Multi-WAN Mode.

14.2.1 Schnittstellenstatus überwachen

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



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



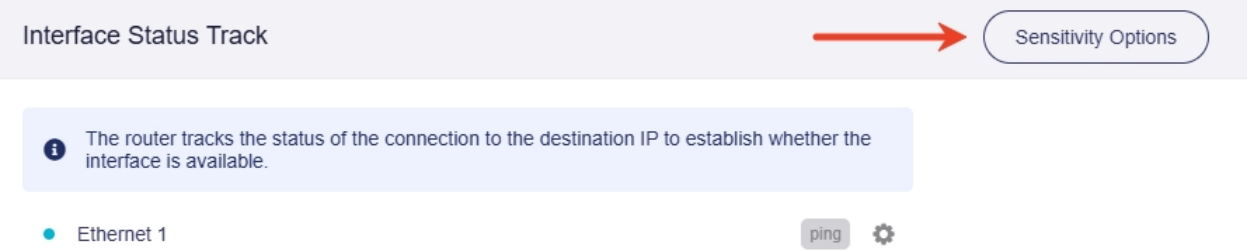
- **Enable Interface Status Track**: Standardmäßig aktiviert. Bei deaktivierter Überwachung beurteilt der Router den Schnittstellenstatus anhand physischer Merkmale, etwa ob ein Ethernetkabel angeschlossen ist.
- **Detection Mode**: Diese Funktion wurde in Firmware v4.5 als Low Data Mode eingeführt und in Firmware v4.7 in Detection Mode umbenannt. Es stehen drei Modi zur Verfügung: Normal Mode, Low Data Mode und Strict Mode.
  - **Normal**: Dieser Modus wird standardmäßig verwendet.
  - **Low Data**: Die Verbindungsüberwachung wird nur ausgelöst, wenn an der Netzwerkschnittstelle ein Netzwerkfehler auftritt. Verwenden Sie diesen Modus bei einem Tarif mit begrenztem Datenvolumen. Nach einer Unterbrechung kann der

erneute Verbindungsaufbau etwas länger dauern als im Modus Normal. Dieser Modus ist nur für die Mobilfunkschnittstelle standardmäßig aktiviert.

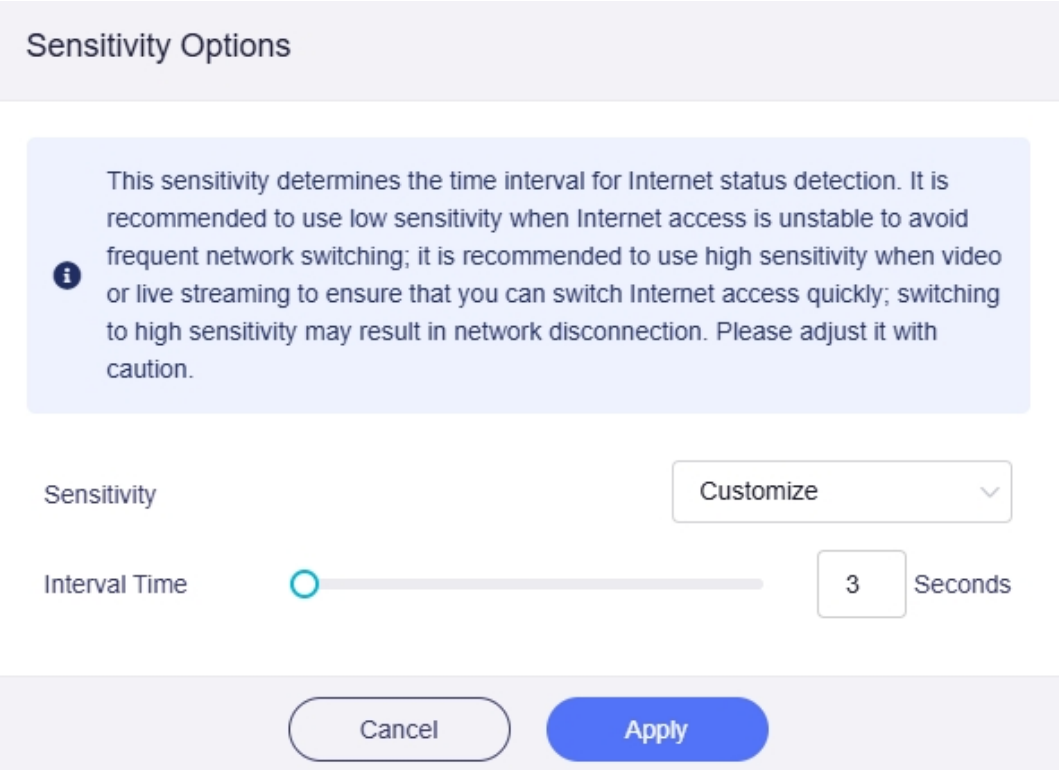
- **Strict**: Der Schnittstellenstatus wird ausschließlich anhand der Ergebnisse eines Prüfbefehls ermittelt, der an eine öffentliche IP-Adresse gesendet wird.

- **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 zur 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.

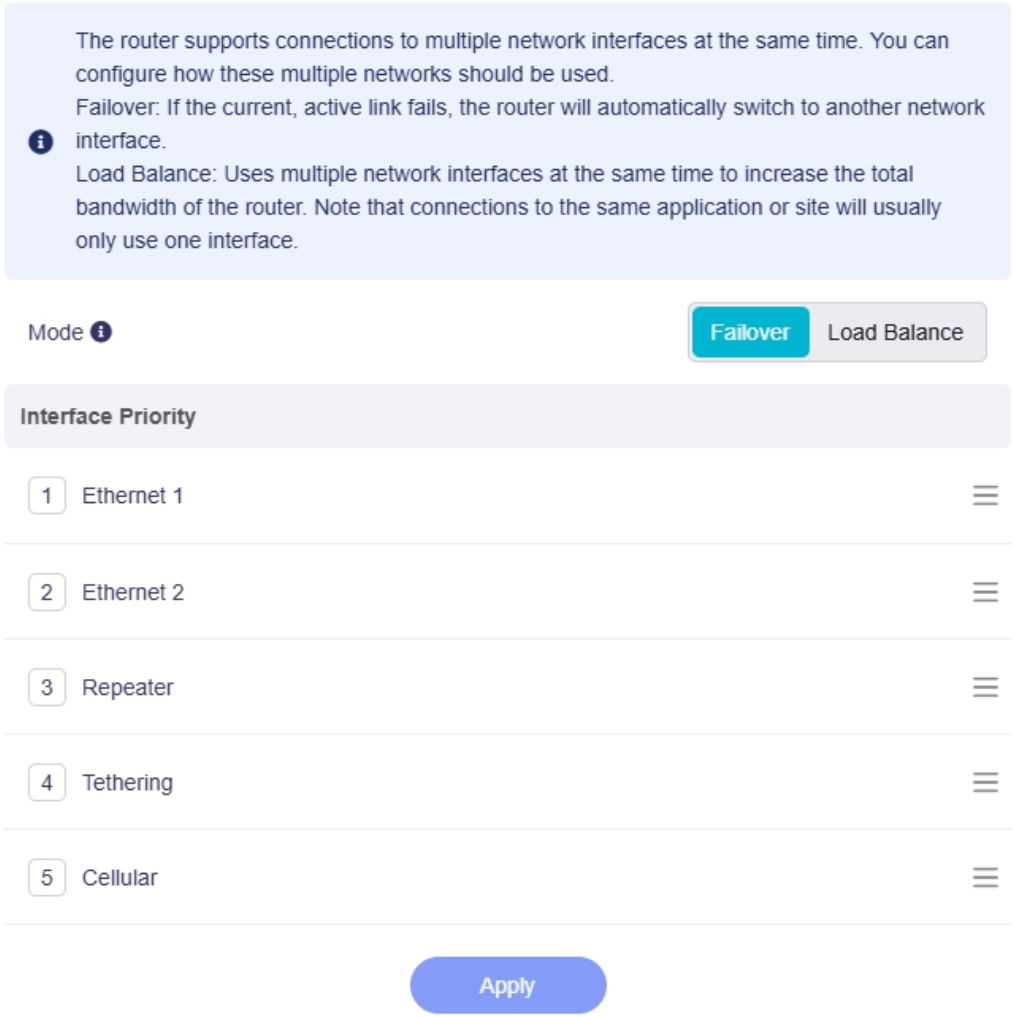


14.2.2 Multi-WAN-Modus

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

Ausfallsicherung

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

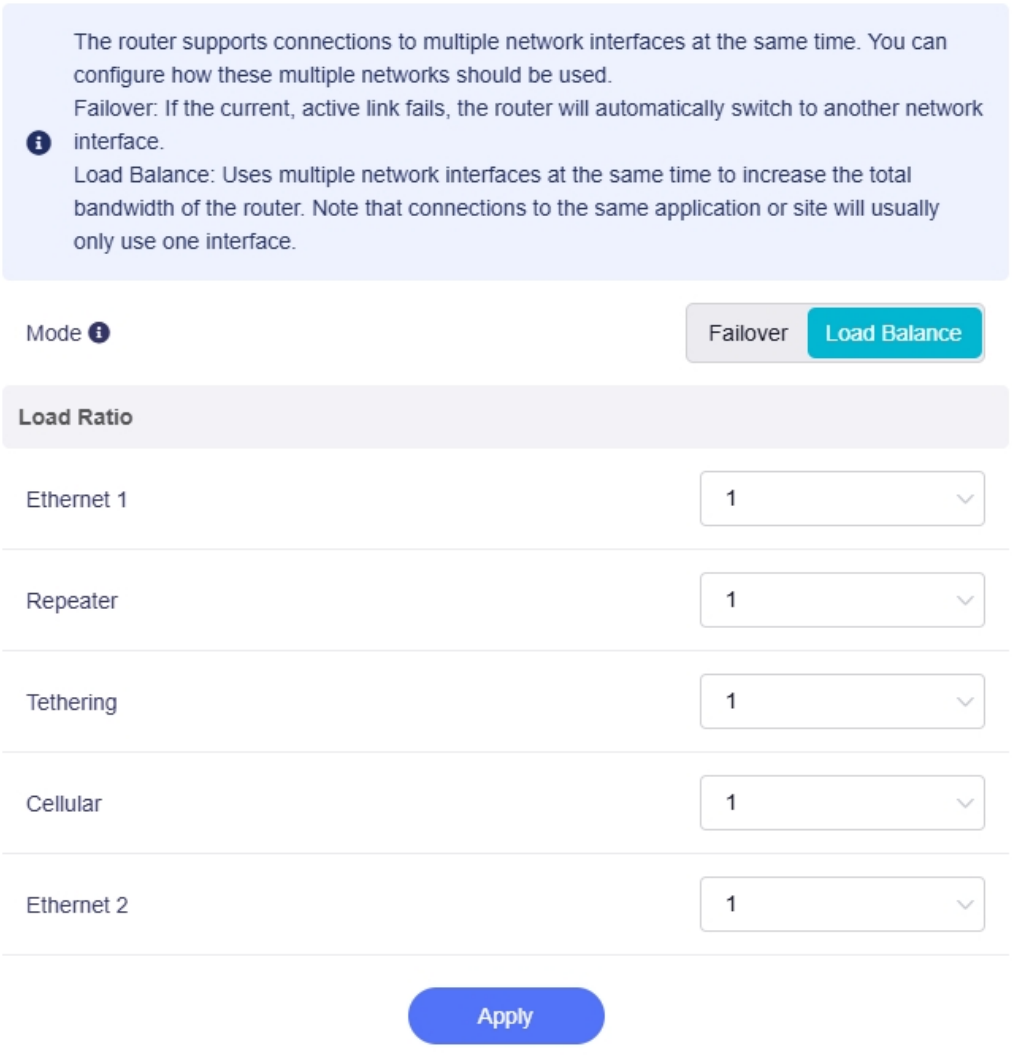


Sie können jeder Schnittstelle eine Priorität zuweisen. Fällt die verwendete Schnittstelle aus, wechselt der Router zur verfügbaren Schnittstelle mit der nächsthöheren Priorität. Sobald eine Verbindung mit höherer Priorität wieder verfügbar ist, wechselt er automatisch zurück.

Lastverteilung

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

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



Ist der Router beispielsweise gleichzeitig mit vier Netzwerken verbunden (Ethernet, Repeater, Tethering und Mobilfunk), die alle Internetzugang bieten, teilen sich bei aktivierter Lastverteilung und einem Verhältnis von 1:1:1:1 alle vier Schnittstellen die Netzwerklast gleichmäßig. Das System verteilt neue Verbindungen entsprechend diesem Verhältnis auf die vier Schnittstellen.

Sie können das Lastverhältnis bei Bedarf anpassen. Verfügt Ethernet beispielsweise über 100 Mbit/s und der Repeater über 200 Mbit/s und sind keine Tethering- oder Mobilfunkverbindungen aktiv, stellen Sie für Ethernet den Wert 1, für den Repeater den Wert 2 und für Tethering und Mobilfunk jeweils den Wert 0 ein. Das System verteilt neue Verbindungen dann im Verhältnis 1:2 auf die Schnittstellen. Ethernet übernimmt somit halb so viele Verbindungen wie der Repeater. 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.

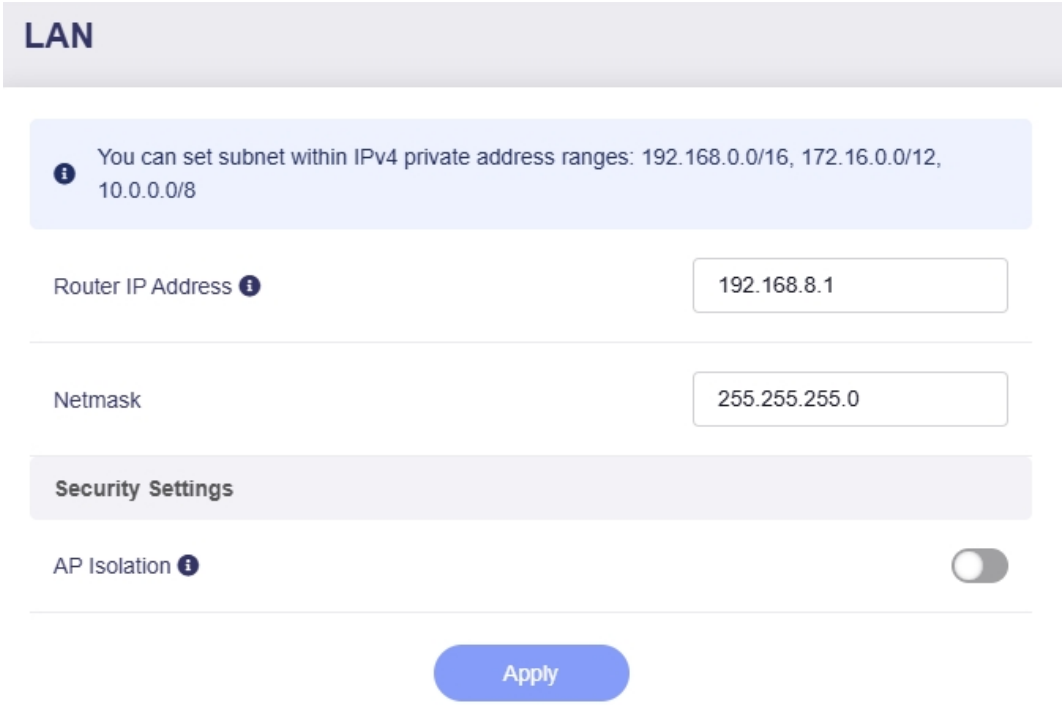
14.3 LAN

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.

14.3.1 Grundeinstellungen

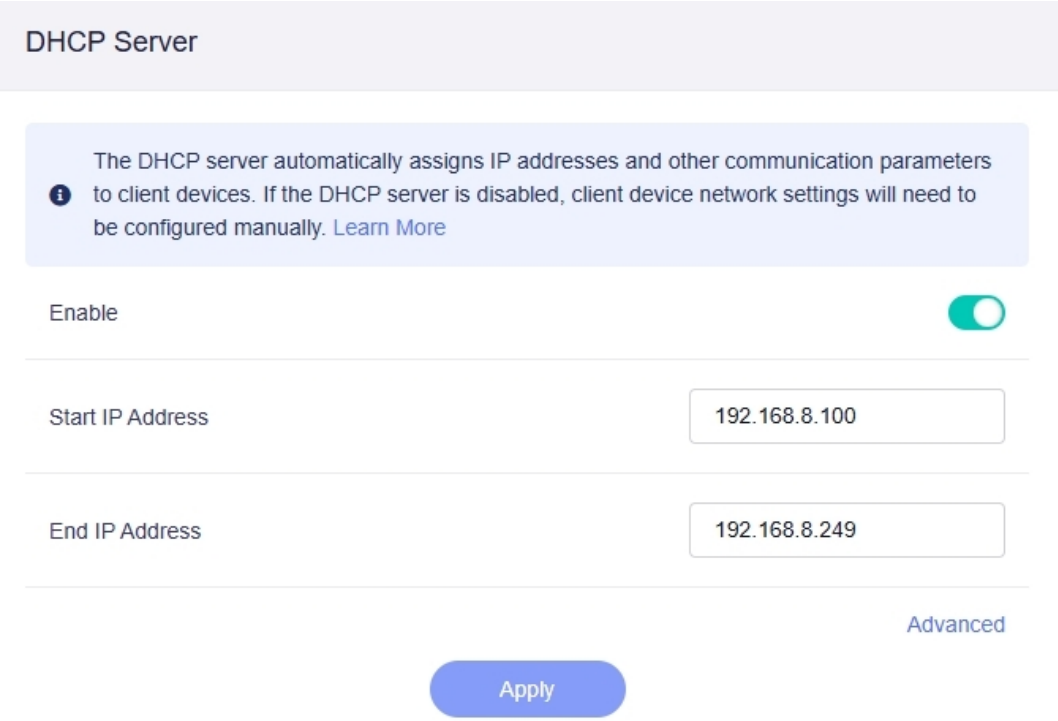
Zu den Grundeinstellungen gehören die IP-Adresse des Routers und die Netzmaske. Sie können ein Subnetz innerhalb der privaten IPv4-Adressbereiche 192.168.0.0/16, 172.16.0.0/12 oder 10.0.0.0/8 festlegen.



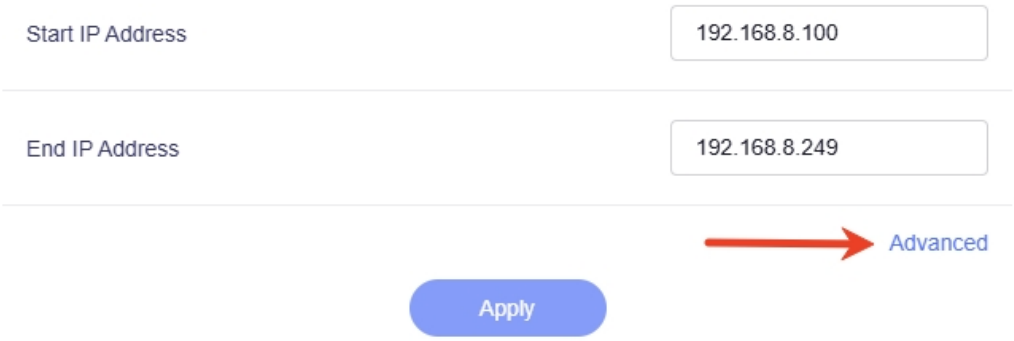
- **Router IP Address**: Über diese Adresse rufen Sie die Weboberfläche im Browser auf. Standardmäßig lautet sie 192.168.8.1. Bei einem Konflikt mit dem vorgeschalteten Netzwerk können Sie sie ändern.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.
- **AP Isolation**: Isoliert die Clientgeräte Ihres Netzwerks in einem separaten Netzwerkbereich. Diese Geräte können nicht mit anderen Geräten im Netzwerk kommunizieren.

14.3.2 DHCP-Server

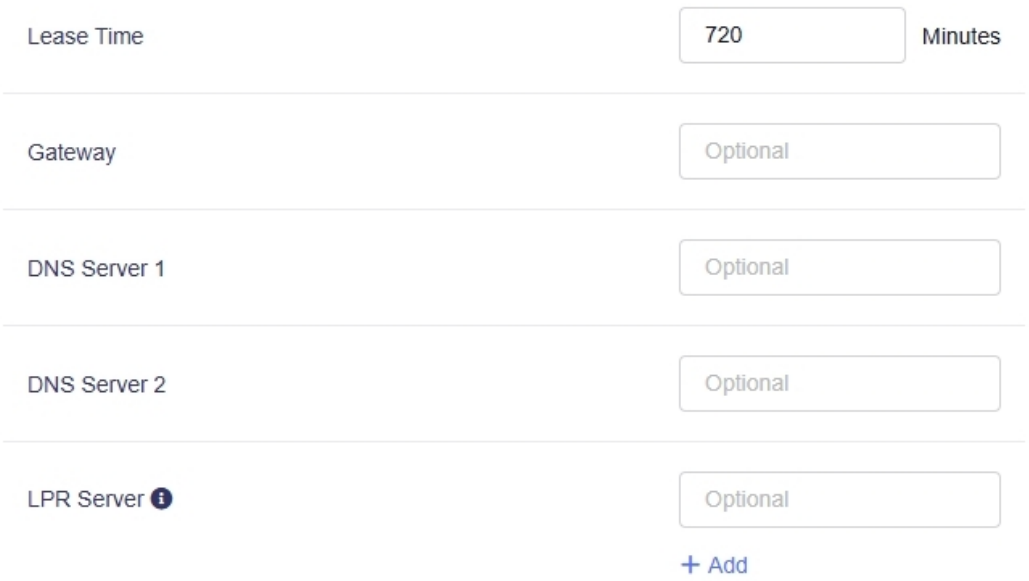
Der DHCP-Server weist jedem verbundenen Gerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Auf GL.iNet-Routern ist er standardmäßig aktiviert und verwendet den Adressbereich 192.168.8.100 bis 192.168.8.249. Diesen Bereich können Sie bei Bedarf anpassen.



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.

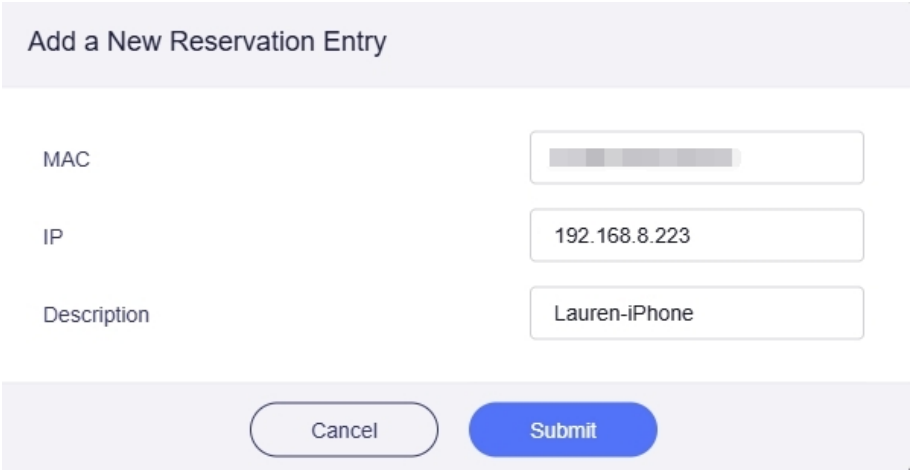
Hinweis: Bei deaktiviertem DHCP-Server müssen Sie für jedes Gerät eine statische IP-Adresse und weitere Kommunikationsparameter manuell festlegen. Einzelheiten finden Sie hier.

14.3.3 Adressreservierung

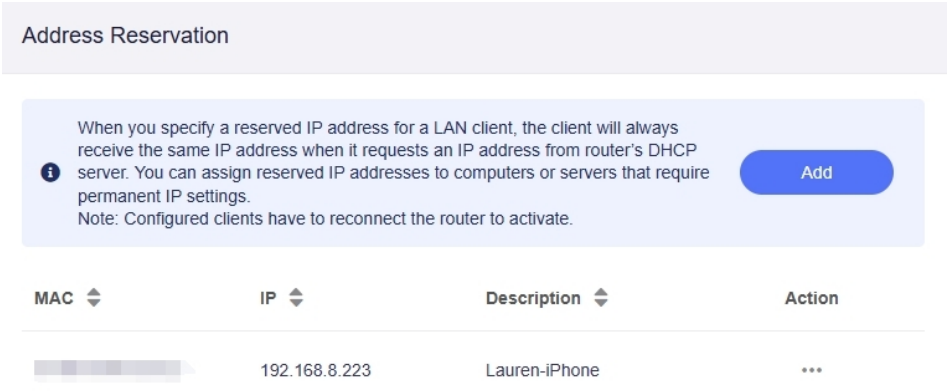
Mit der Adressreservierung weisen Sie einem LAN-Gerät eine feste IP-Adresse zu, die es bei jeder Anfrage an den DHCP-Server des Routers erneut erhält. Dies eignet sich für Computer oder Server, die dauerhaft dieselbe IP-Adresse benötigen. Damit eine neue Reservierung wirksam wird, muss sich das betreffende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



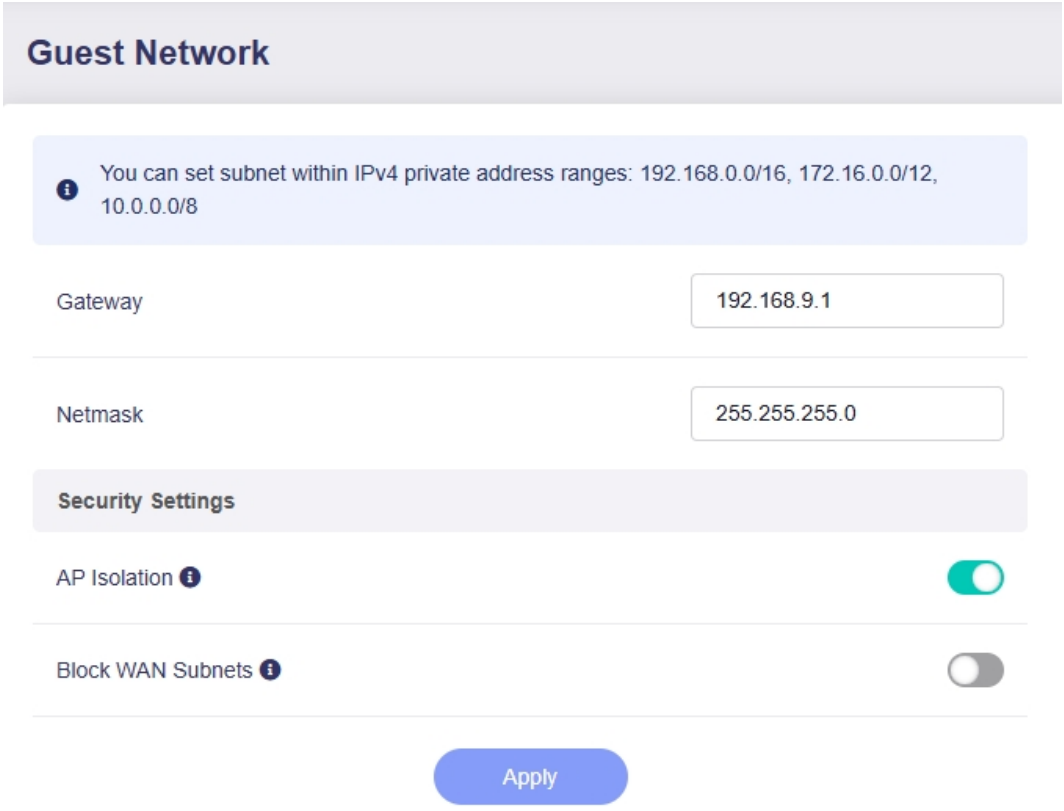
14.4 Gastnetzwerk

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

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Guest Network**. Hier konfigurieren Sie das Gastnetzwerk einschließlich der grundlegenden Einstellungen und des DHCP-Servers.

14.4.1 Grundeinstellungen

Zu den grundlegenden Einstellungen gehören Gateway, Netmask, AP Isolation und Block WAN Subnets.



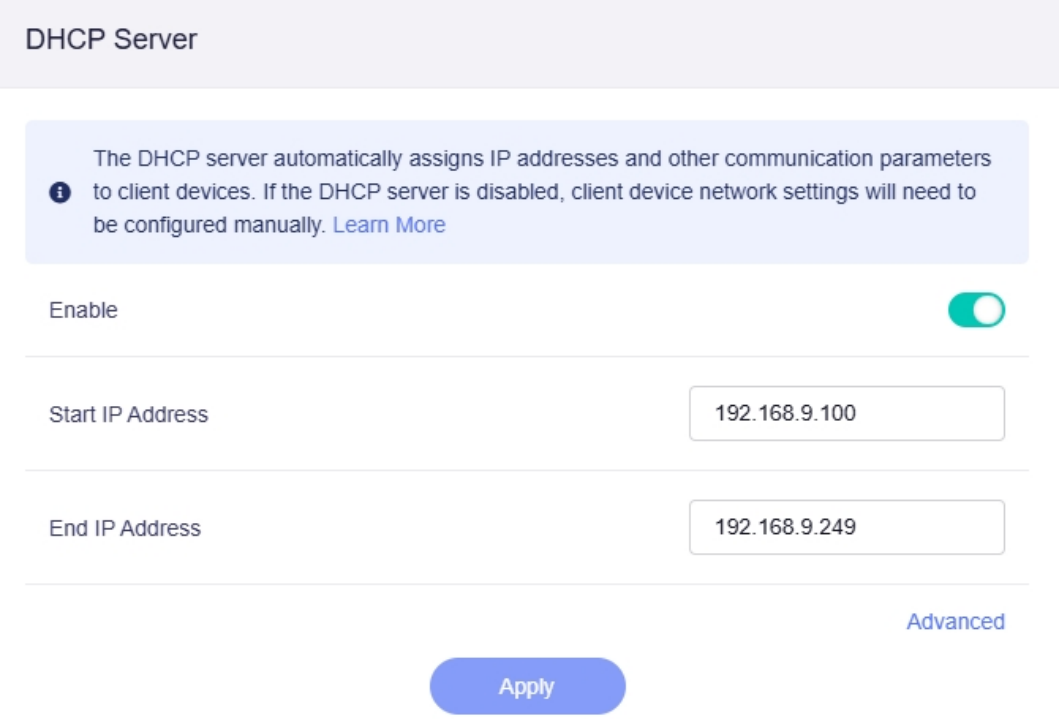
- **Gateway**: Standardmäßig 192.168.9.1. Sie können diese Adresse ändern, sie darf jedoch nicht mit dem Gateway des Hauptnetzwerks kollidieren.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.
- **AP Isolation**: Isoliert Geräte im Gastnetzwerk voneinander, damit sie nicht mit anderen Geräten im selben Netzwerk kommunizieren können.

- **Block WAN Subnets**: Bei aktivierter Option kann das Gastnetzwerk nicht auf das übergeordnete Netzwerk oder dessen Netzwerksegment zugreifen.

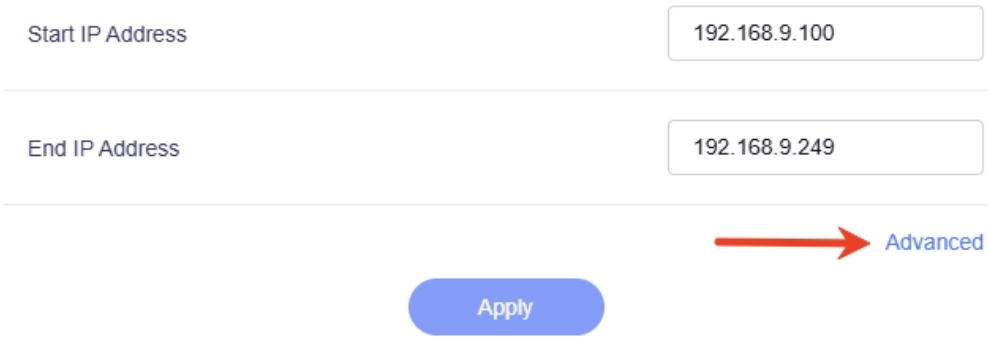
14.4.2 DHCP-Server

Das Gastnetzwerk ist standardmäßig deaktiviert. Sein DHCP-Server bleibt ebenfalls deaktiviert und ausgeblendet, bis Sie das Gastnetzwerk manuell aktivieren.

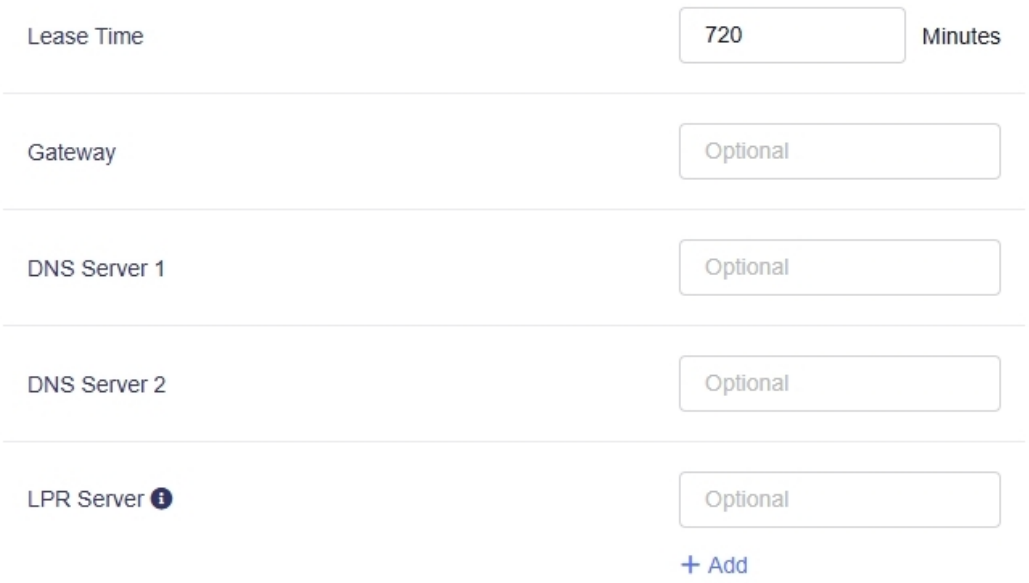
Nach der Aktivierung weist der DHCP-Server jedem verbundenen Gerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Im Gastnetzwerk reicht der Adresspool von 192.168.9.100 bis 192.168.9.249. Diesen Bereich können Sie anpassen.



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 vom DHCP-Server des Gastnetzwerks zugewiesene IP-Adresse verwenden darf.
- **Gateway**: Die Routerkomponente, die Datenverkehr zwischen dem Gastnetzwerk 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.

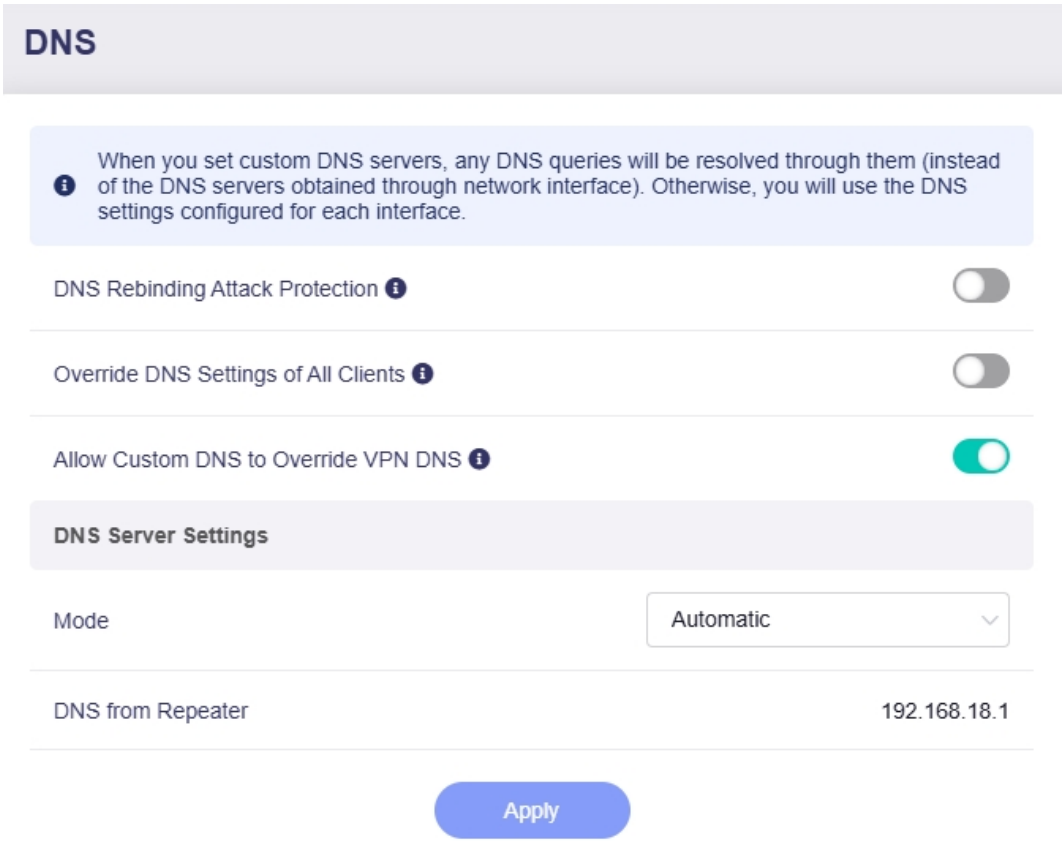
14.5 DNS

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

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

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

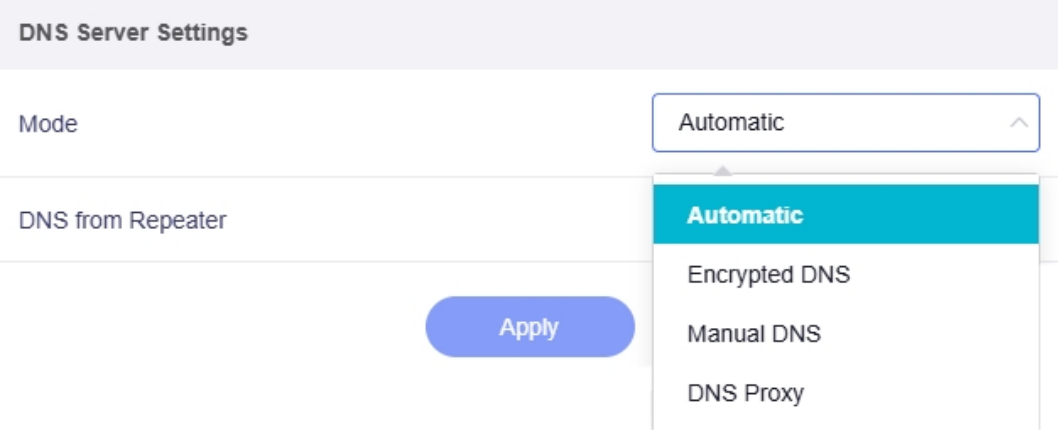
14.5.1 Allgemeine Einstellungen



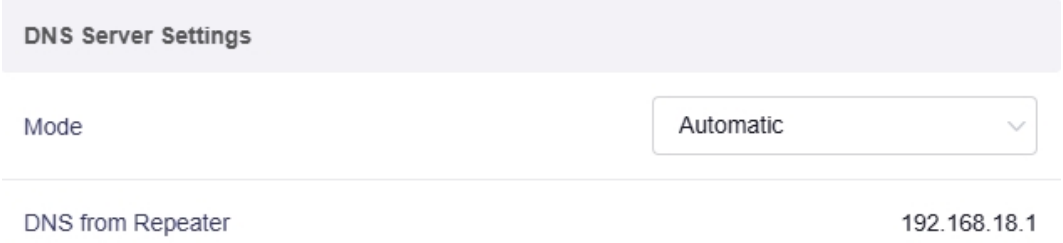
- **DNS Rebinding Attack Protection**: Schützt vor DNS-Rebinding-Angriffen, indem bösartige Namensauflösungen blockiert werden. Dadurch kann die Auflösung privater Adressen fehlschlagen. Deaktivieren Sie die Option, wenn Ihr Netzwerk ein Captive Portal verwendet, etwa eine Anmeldeseite in einem öffentlichen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

14.5.2 DNS-Servereinstellungen

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

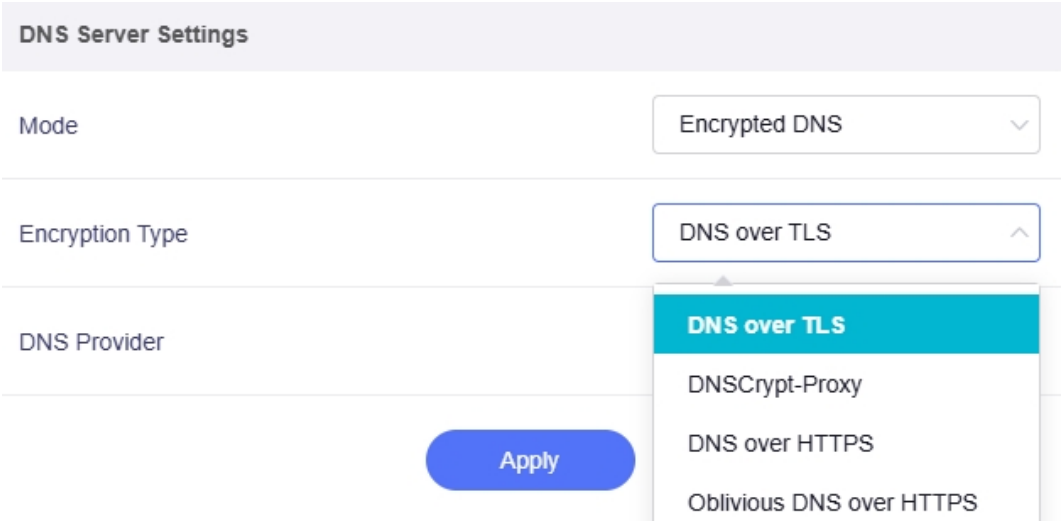


1. **Automatic**: Der Router bezieht die DNS-Serveradressen automatisch aus dem vorgeschalteten Netzwerk und verwendet sie für alle verbundenen Geräte.



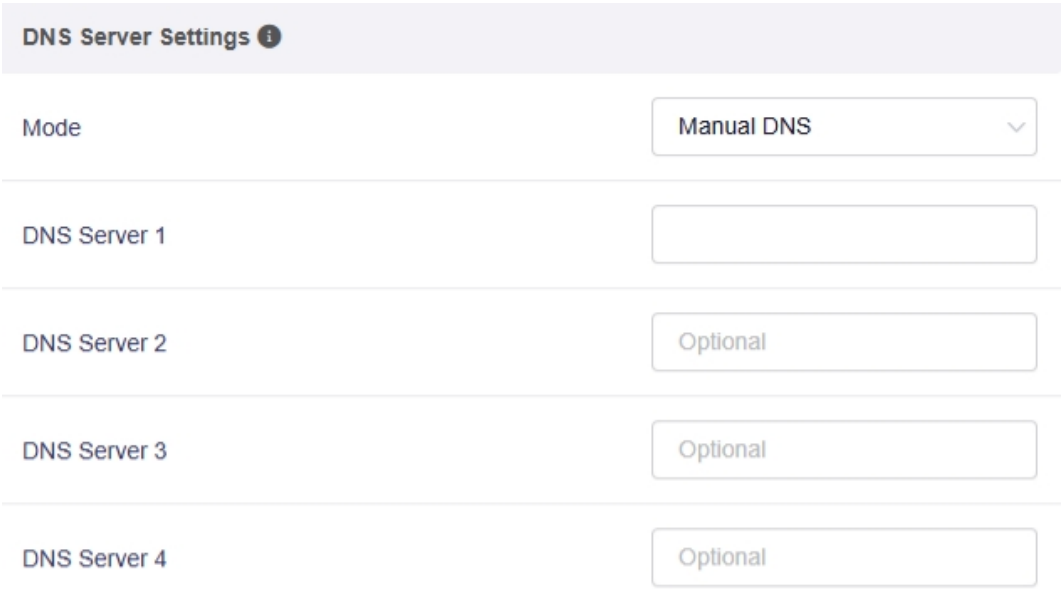
2. **Encrypted DNS**: Der Router verarbeitet DNS-Anfragen über verschlüsselte Protokolle und schützt die Auflösungsdaten so vor Abhören und Manipulation.

Es stehen vier Verfahren zur Auswahl: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS.



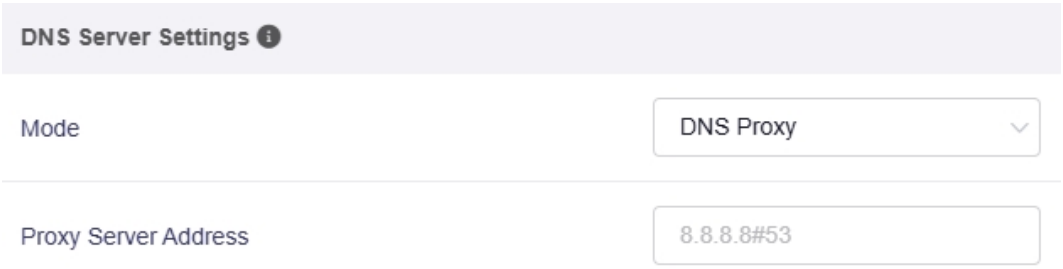
- Bei DNS over TLS wählen Sie Control D, NextDNS oder Cloudflare als DNS-Anbieter aus.
- Bei den drei anderen Verfahren wählen Sie mindestens einen DNS-Server aus dem Verzeichnis aus. Es sind bis zu acht Server möglich. Bei mehreren ausgewählten Servern verwendet der Router automatisch den schnellsten.

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.

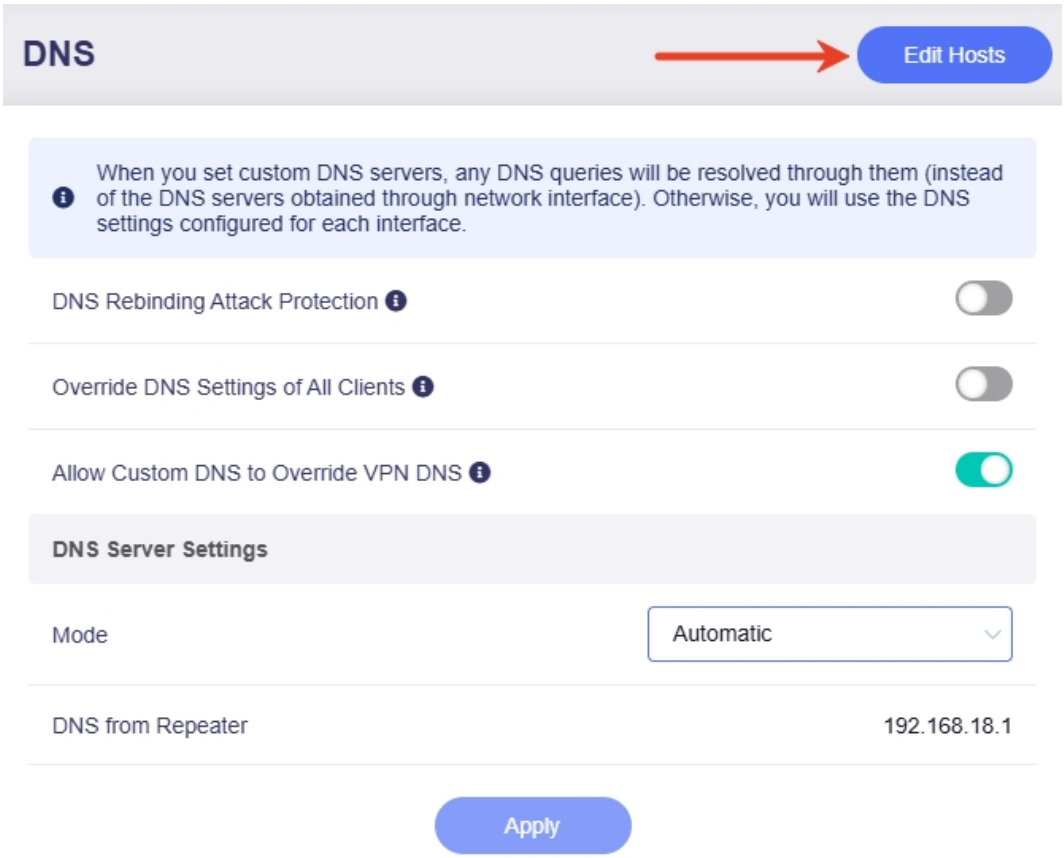
4. **DNS Proxy**: Der Router leitet alle DNS-Anfragen über einen Proxyserver weiter. Die Namensauflösung erfolgt in dessen Netzwerkumgebung, um besondere Zugriffsanforderungen zu erfüllen.



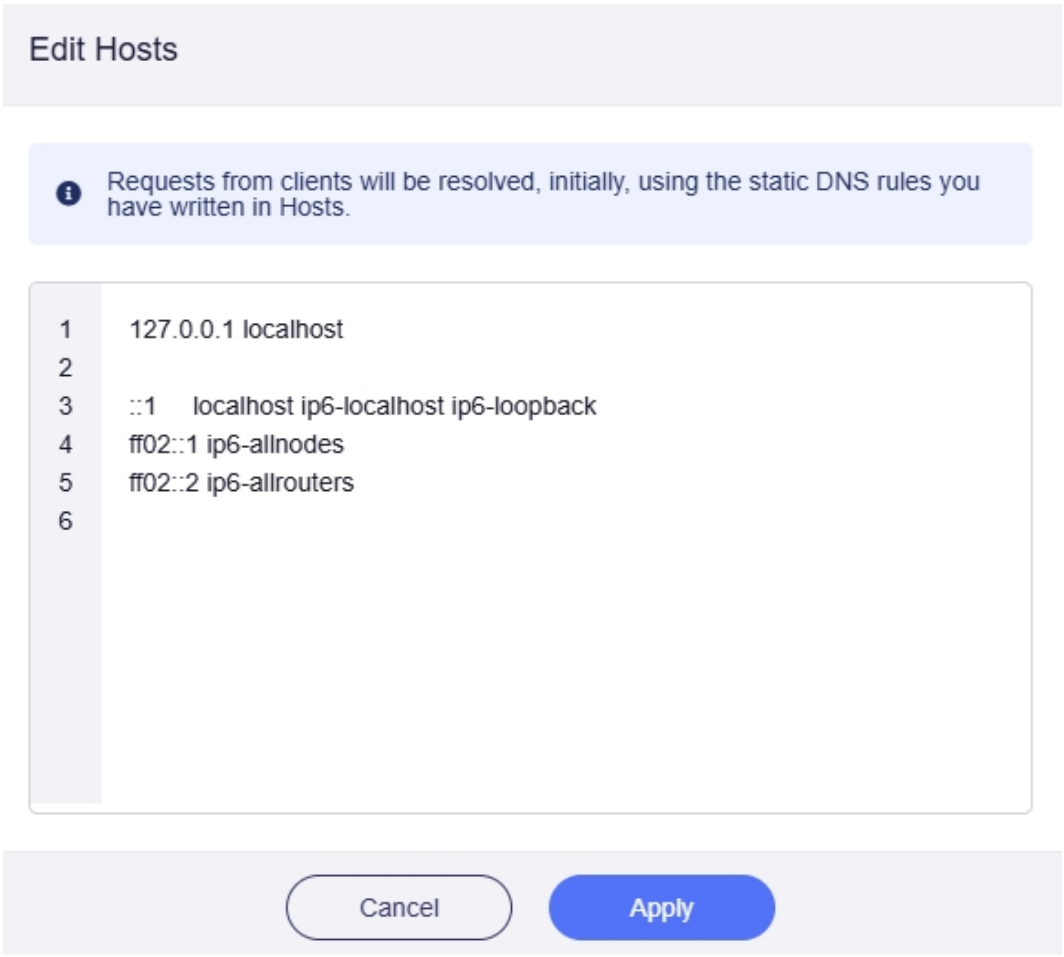
14.5.3 Hosts bearbeiten

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

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



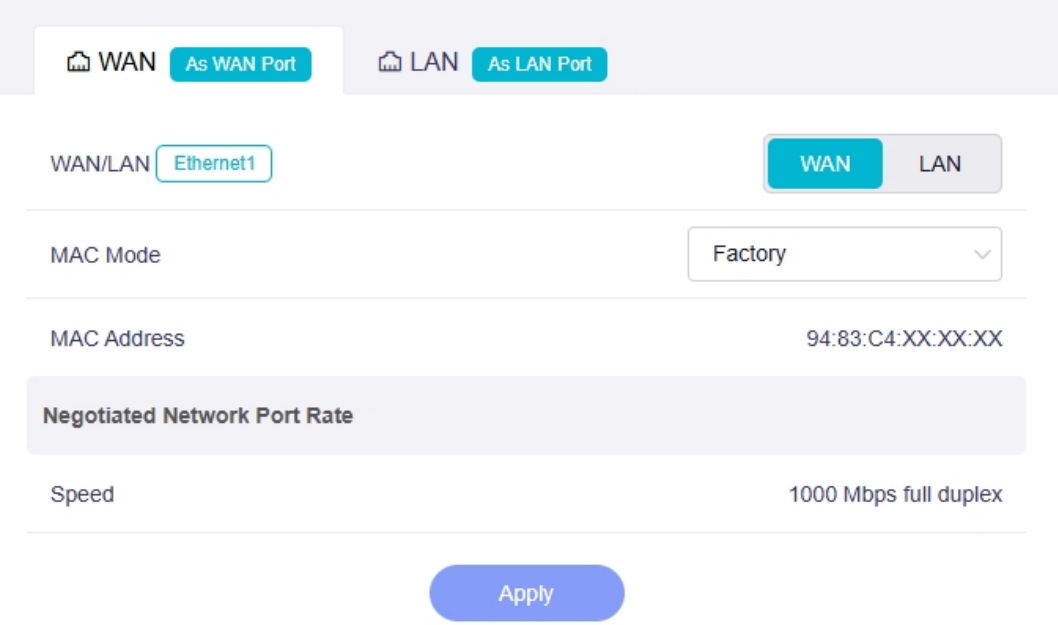
Anfragen von Endgeräten werden vorrangig anhand der hier eingetragenen statischen DNS-Regeln aufgelöst. Sie können Hostnamen manuell IP-Adressen zuordnen und so die Namensauflösung gezielt steuern. Ein Beispiel ist der Standardeintrag „127.0.0.1 localhost“ für die lokale Loopback-Adresse.



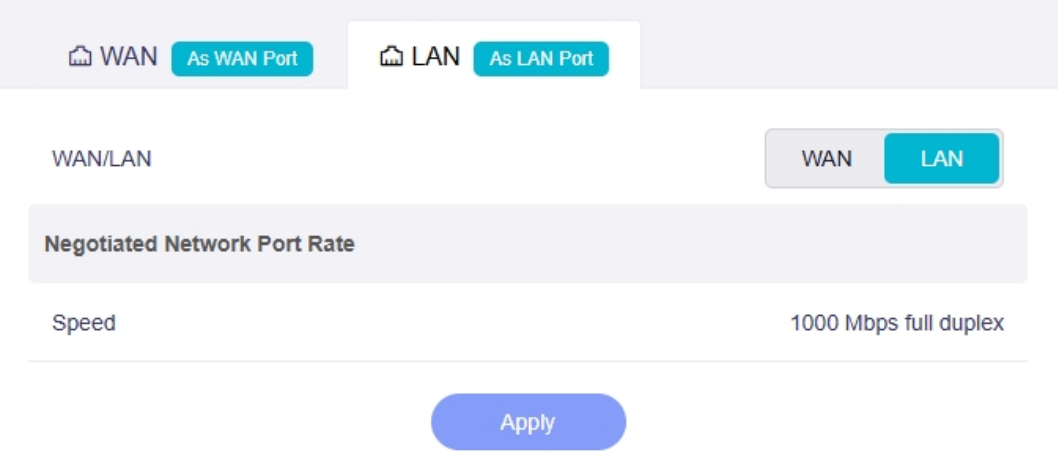
14.6 Ethernetanschlüsse

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Ethernet Port**. 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.

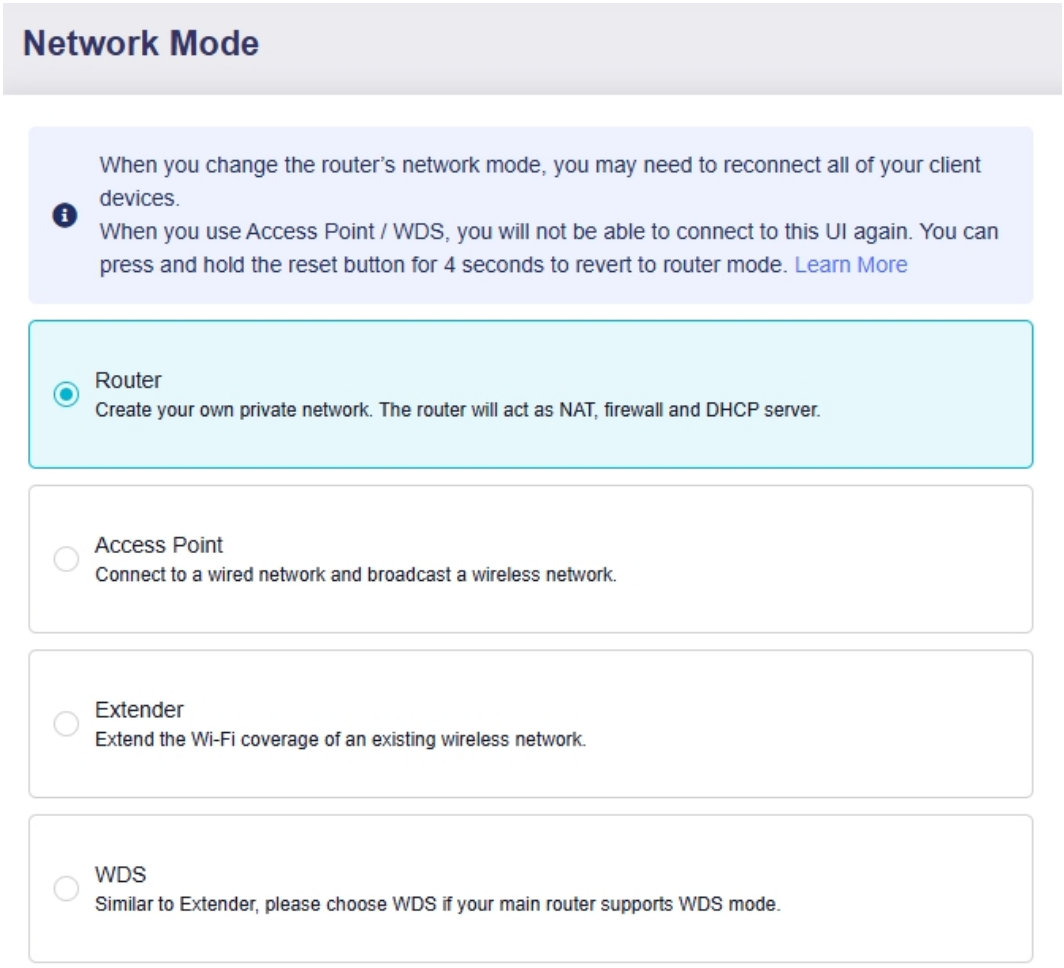


Hinweis: Die ausgehandelte Verbindungsgeschwindigkeit der WAN- und LAN-Anschlüsse wird nur bei angeschlossenem Ethernetkabel angezeigt. Sie hängt sowohl vom Ethernetanschluss als auch vom Ethernetkabel ab.

14.7 Netzwerkmodus

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

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



- **Router**: Der Standardmodus der meisten Router für zu Hause und kleine Büros. Er erstellt ein privates lokales Netzwerk und dient als Gateway zwischen dem öffentlichen Internet und den verbundenen Geräten. NAT, DHCP und die integrierte Firewall sind aktiv. Der

Router verbindet sich mit einem vorgeschalteten Anschluss, etwa Glasfaser, weist Endgeräten automatisch private IP-Adressen zu und schützt das gesamte private Netzwerk.

- **Access Point**: In diesem Modus wird der Router per LAN-Kabel mit einem kabelgebundenen Netzwerk verbunden und stellt WLAN bereit. Dadurch vergrößert sich die WLAN-Abdeckung, und weitere Geräte können auf das Netzwerk zugreifen. NAT und DHCP sind deaktiviert. Der Router arbeitet ausschließlich als WLAN-Zugangspunkt und Switch, nicht als eigenständiges Gateway.
- **Extender**: Dieser Modus erweitert die Reichweite eines vorhandenen WLANs und versorgt Bereiche mit schlechtem Empfang. Der Router empfängt das Signal des Hauptrouters drahtlos und sendet es erneut aus. Anders als im Access-Point-Modus ist keine Kabelverbindung zum Hauptrouter nötig. Da das Gerät gleichzeitig empfangen und senden muss, kann sich die verfügbare Bandbreite halbieren.
- **WDS**: Wireless Distribution System erweitert wie der Extender-Modus die WLAN-Abdeckung drahtlos, unterstützt jedoch zusätzlich WLAN-Brücken zwischen mehreren kompatiblen Routern. Dieser Modus wird empfohlen, wenn der vorgeschaltete Router WDS unterstützt.

  WDS eignet sich etwa für mehrstöckige Gebäude oder kleine Bürogelände, in denen mehrere Router gemeinsam ein einheitliches WLAN bilden sollen. Während im Extender-Modus ein Hauptrouter mit einem einzelnen Extender kommuniziert, können in WDS miteinander verbundene Router Signale sowohl senden als auch empfangen. Mehrere Funkknoten ermöglichen so eine durchgängige Abdeckung größerer Bereiche.

Hinweis:

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

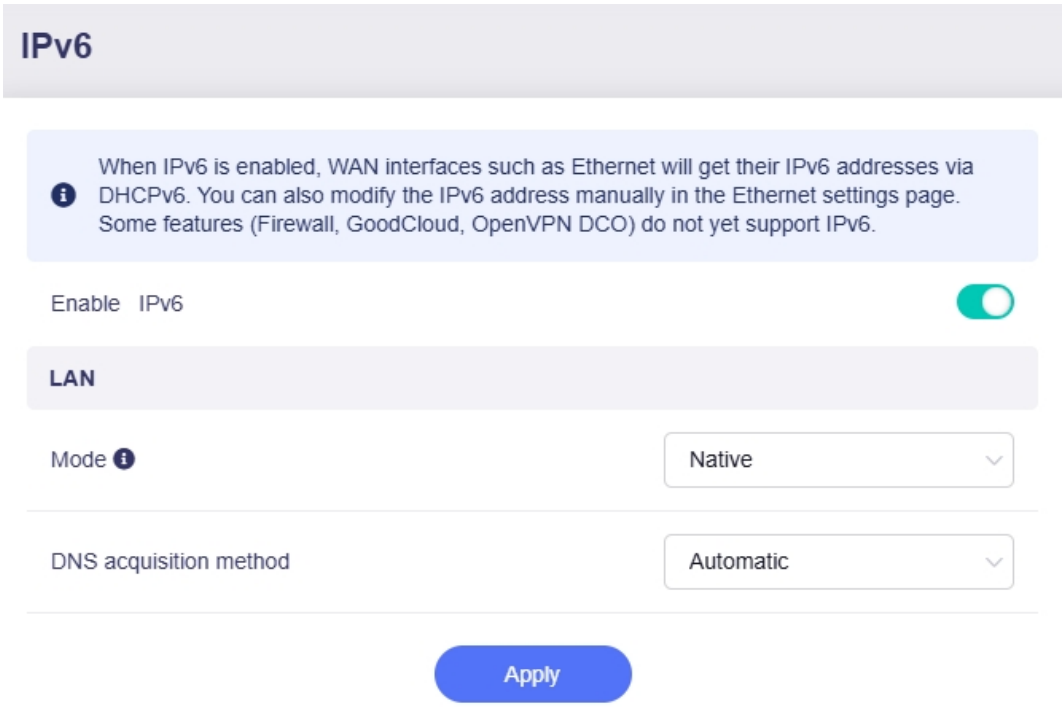
Adressreservierung, Gastnetzwerk, DNS, Ethernetanschluss, IPv6, Drop-in Gateway, IGMP Snooping, Netzwerkbeschleunigung und NAT-Einstellungen.

14.8 IPv6

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

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

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



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.

14.8.1 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.

14.8.2 DNS-Adressen beziehen

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

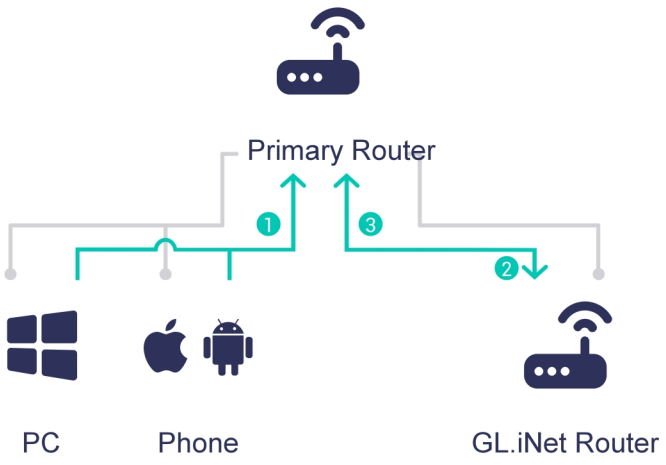
- **Automatic**: Der Router bezieht die IPv6-DNS-Serveradressen dynamisch, etwa über DHCPv6.
- **Manual**: Geben Sie eigene IPv6-DNS-Serveradressen ein. Da DNS Domainnamen in die zugehörigen IP-Adressen auflöst, kann eine manuelle Konfiguration zu Fehlern bei der Namensauflösung führen. Verwenden Sie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

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



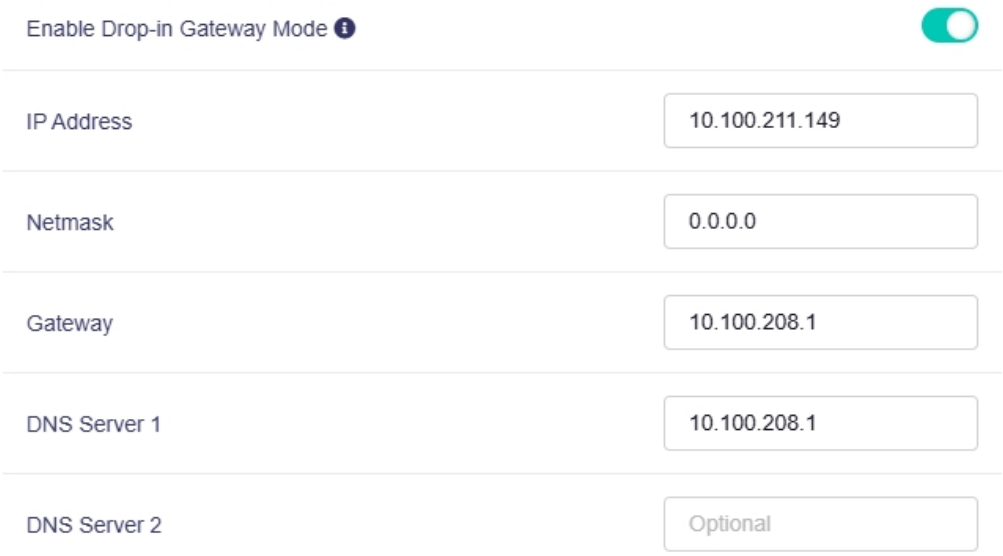
Das obige Diagramm enthält graue Linien sowie grüne Linien mit drei nummerierten Pfeilen.

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

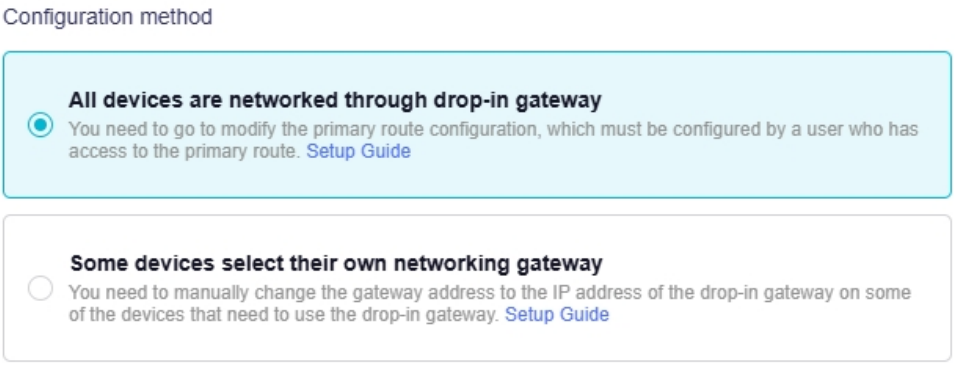
1. Der Datenverkehr der Endgeräte gelangt zunächst zum Hauptrouter.
2. Der Hauptrouter leitet ihn zur Verarbeitung an den GL.iNet-Router weiter, etwa zum Filtern von Werbung oder zur VPN-Verschlüsselung.
3. Nach der Verarbeitung gelangt der Datenverkehr zurück zum Hauptrouter. Dieser übermittelt die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

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

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



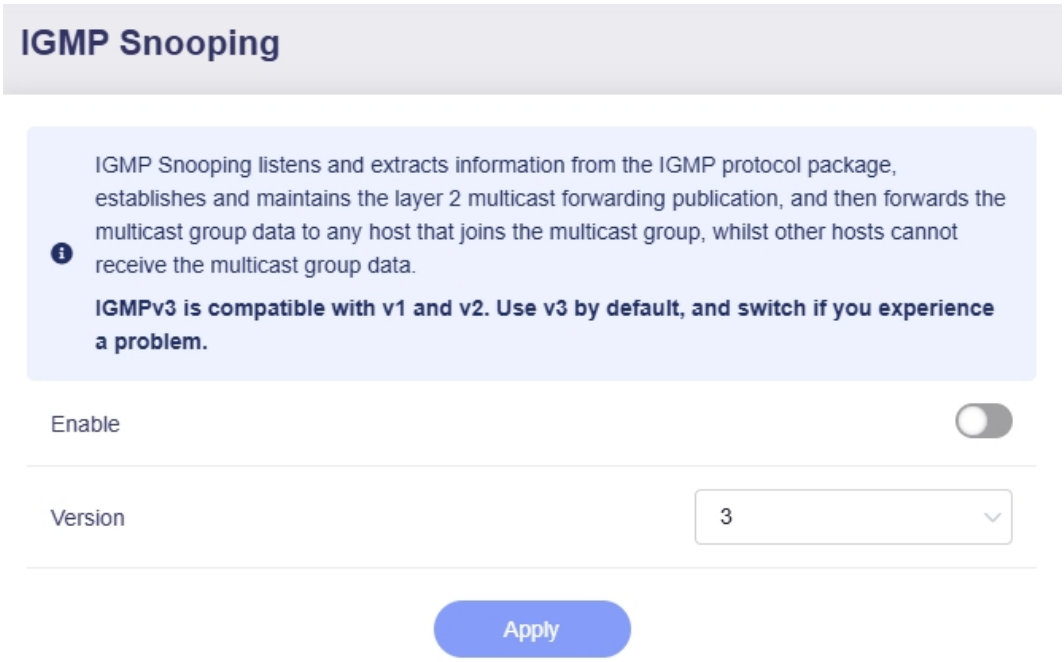
2. Wählen Sie die Konfigurationsmethode aus und klicken Sie auf **Apply**. Einzelheiten finden Sie in dieser Anleitung.



14.10 IGMP Snooping

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

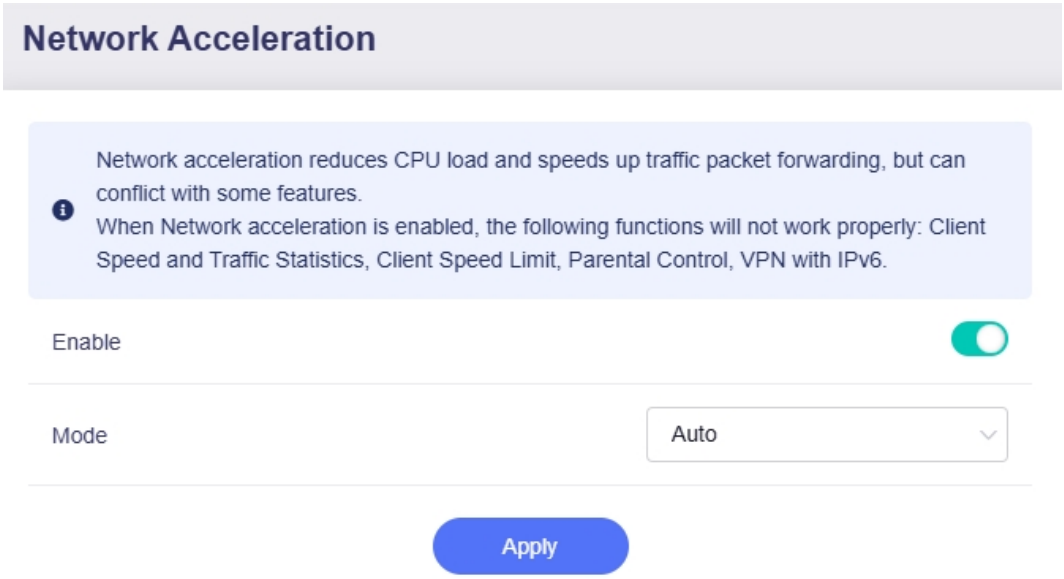
Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **IGMP Snooping**. Aktivieren Sie die Funktion bei Bedarf, um Multicast auf Ihrem Router zu nutzen.



14.11 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.

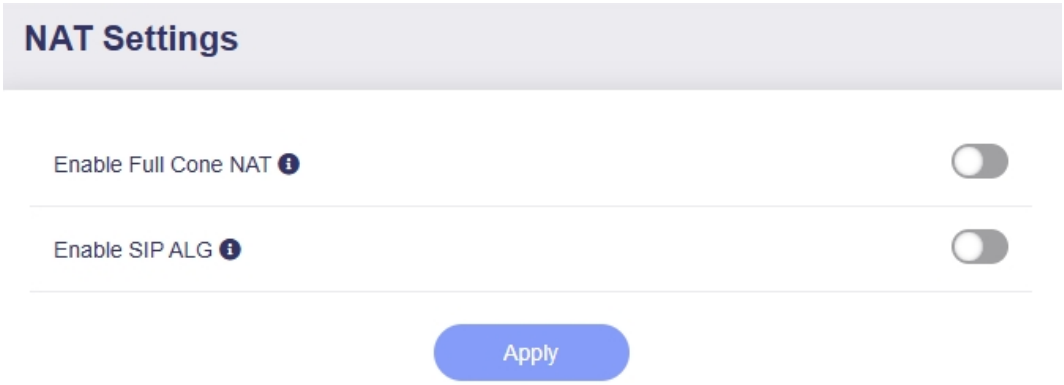


- **Auto**: Wechselt je nach tatsächlicher Nutzung automatisch zwischen den beiden Beschleunigungsmodi.
- **Hardware Acceleration**: Dieser Modus lagert häufig anfallende Netzwerkaufgaben wie NAT, Paketweiterleitung und Prüfsummenprüfung auf spezielle Hardware wie NPUs oder HWNAT-Chips aus. Er arbeitet mit Ethernet- und Repeater-Verbindungen. Bei festen Übertragungswegen und einfachen Regeln ermöglicht er einen hohen Durchsatz, geringe Latenzen und eine minimale CPU-Auslastung bei Datenübertragung mit voller Leitungsgeschwindigkeit.
- **Software Acceleration**: Dieser Modus nutzt die allgemeine CPU des Routers zusammen mit optimierten Kerneln oder Treibern, etwa SWNAT. Er funktioniert beim Mobilfunkzugang über 4G/5G, einem typischen Einsatzfall, in dem keine Hardwarebeschleunigung verfügbar ist. Er bietet hohe Kompatibilität und unterstützt komplexe Protokolle. Bei hoher Bandbreitenauslastung können jedoch Engpässe an der CPU auftreten, insbesondere bei der Nutzung erweiterter Funktionen.

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

14.12 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 15

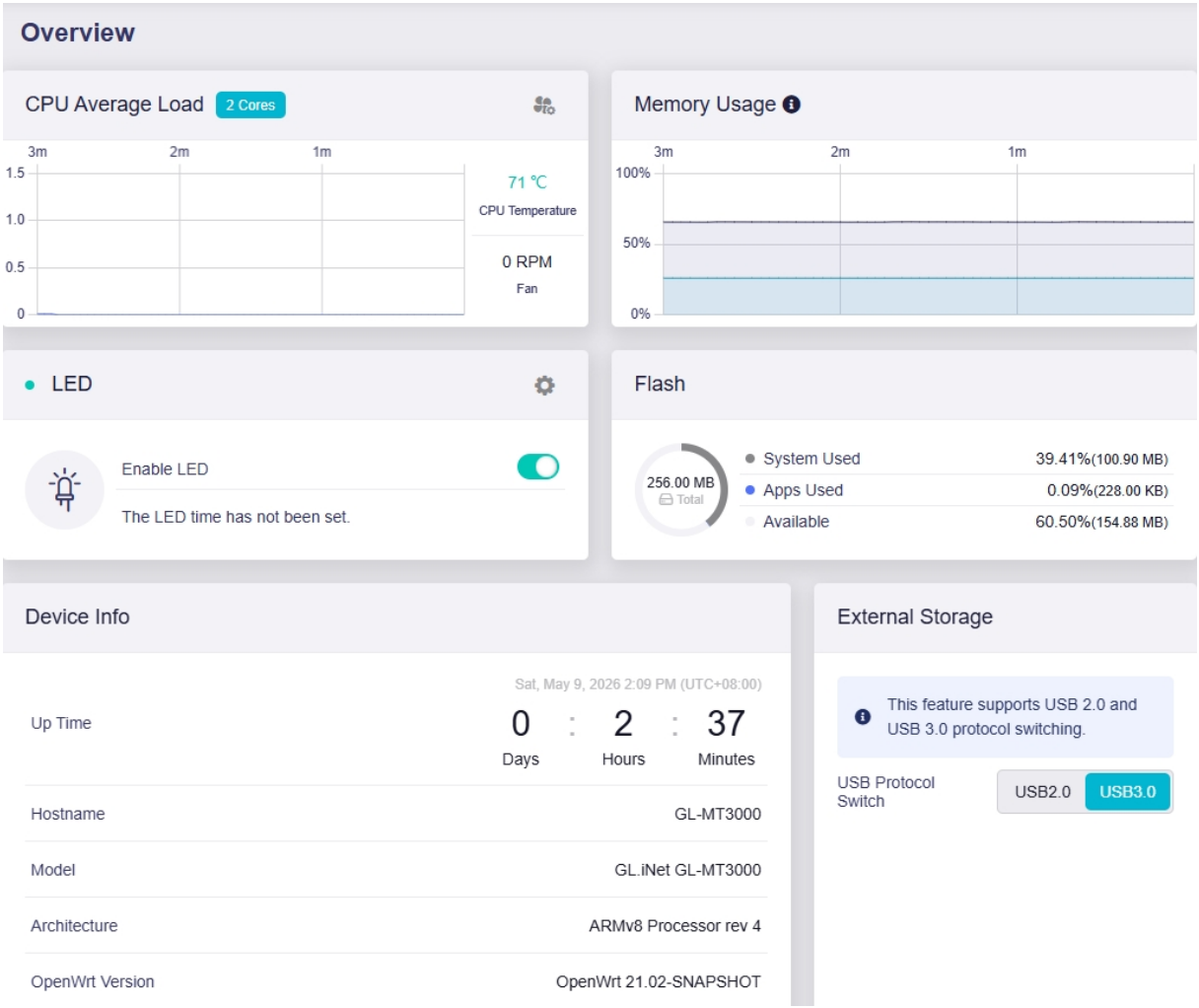
System

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

15.1 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

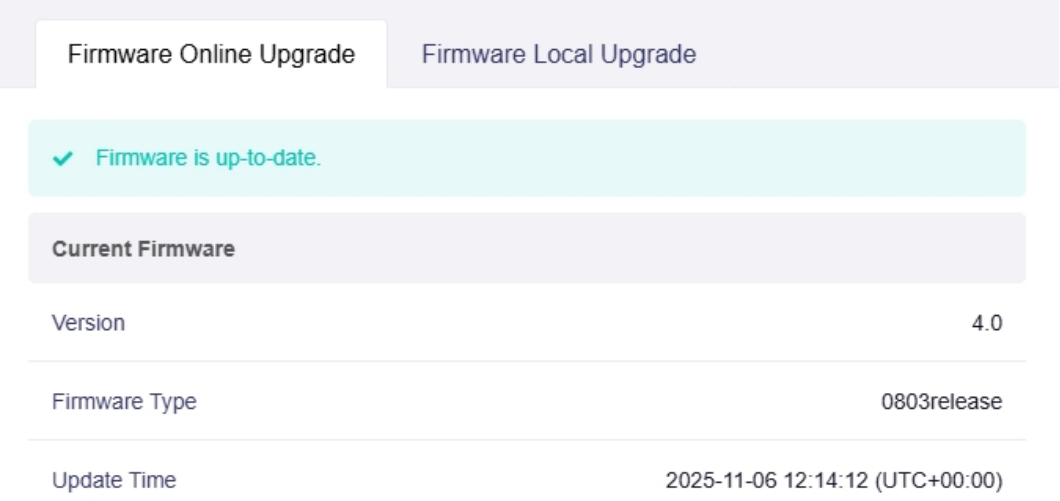


15.2 Aktualisierung

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

15.2.1 Firmware online aktualisieren

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

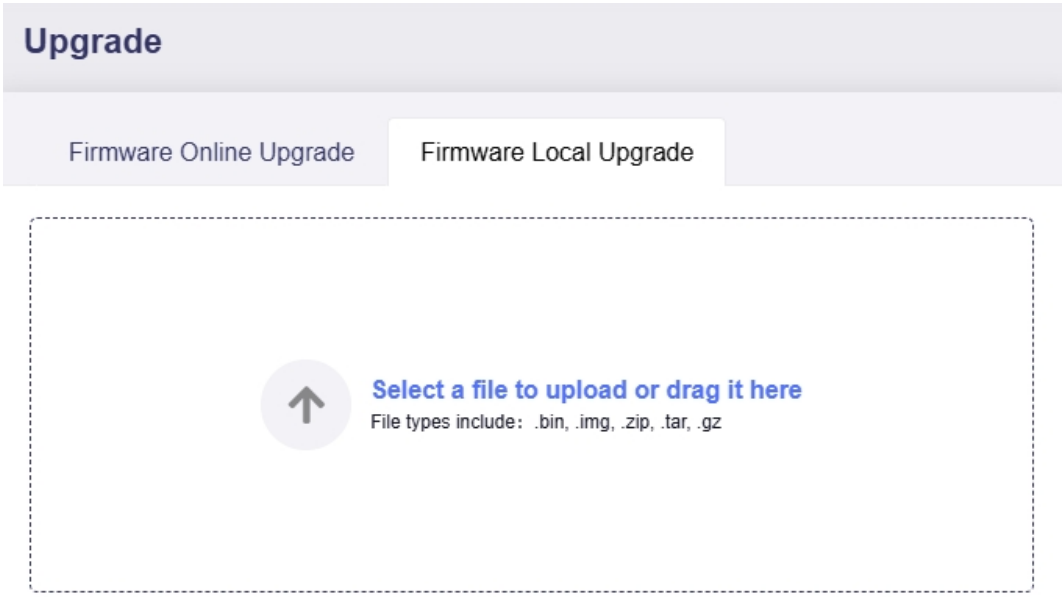


Tipp: Wenn bei einer Online-Aktualisierung **Download Failed** angezeigt wird, öffnen Sie **SYSTEM** > **Time Zone** und korrigieren Sie die Zeitzone durch Synchronisieren mit dem Browser.

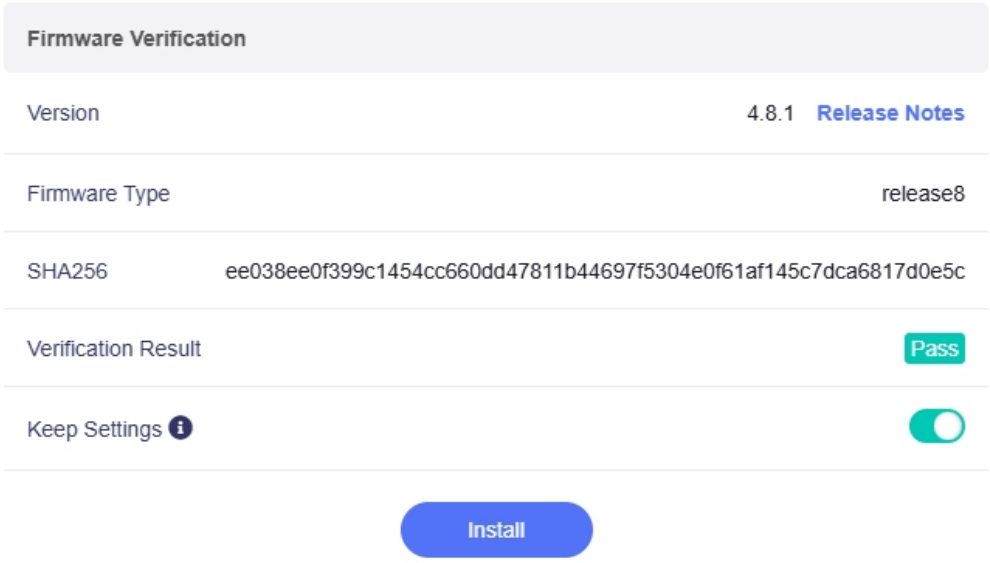
15.2.2 Firmware lokal aktualisieren

Für die lokale Aktualisierung benötigt der Router keine Internetverbindung.

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



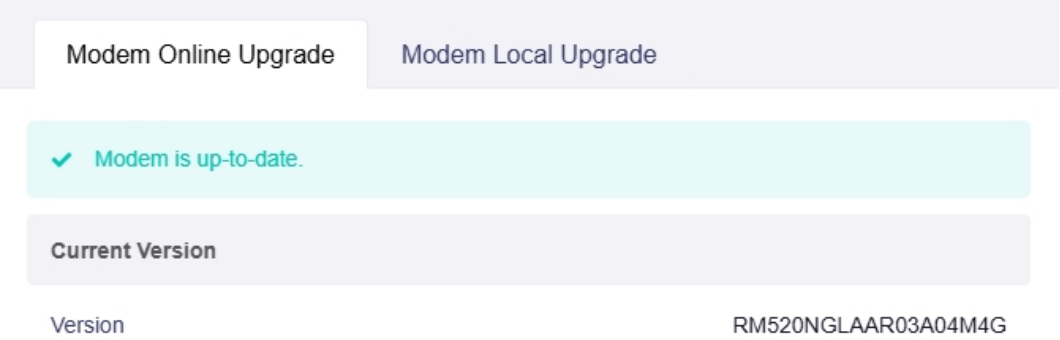
Die Firmwaredetails werden angezeigt. Prüfen Sie diese, bevor Sie auf **Install** klicken.



- **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.

15.2.3 Modem online aktualisieren

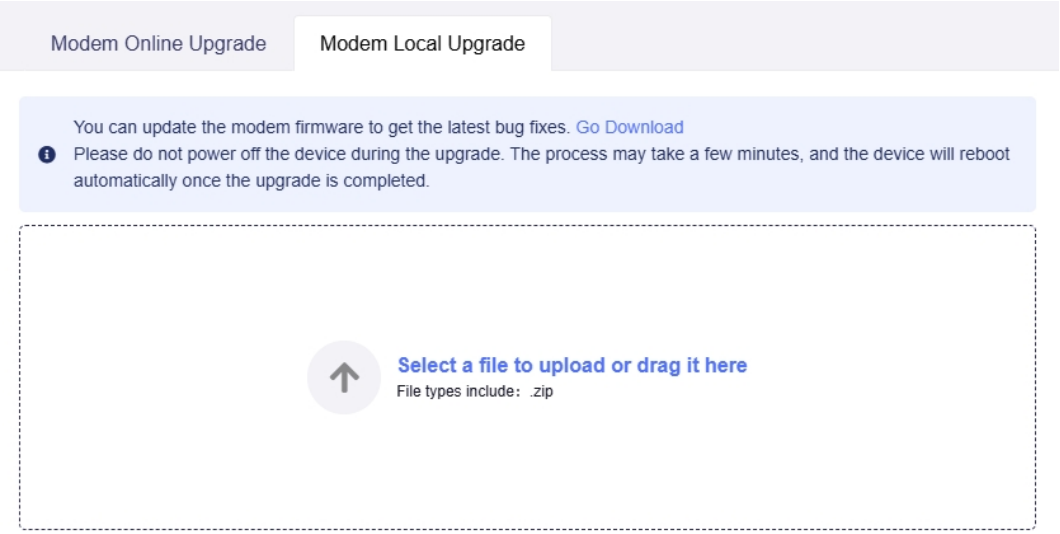
Bei GL.iNet-Mobilfunkroutern können Sie die Firmware des Mobilfunkmodems über die Weboberfläche anzeigen und aktualisieren.
Hier sehen Sie die aktuelle Version des Mobilfunkmodems. Wenn Ihr Router mit dem Internet verbunden ist, prüft er automatisch auf dem Server des Herstellers, ob eine neuere Modemversion verfügbar ist. Das vereinfacht die Aktualisierung.



15.2.4 Modem lokal aktualisieren

Wenn die Mobilfunkverbindung ausfällt oder instabil ist, können Sie versuchen, das Mobilfunkmodul zu aktualisieren. Wir empfehlen, vor der Modemaktualisierung den technischen Support zur Fehlerbehebung zu kontaktieren.

Laden Sie bei Bedarf manuell eine Modem-Firmwaredatei hoch, um das Mobilfunkmodem zu aktualisieren.



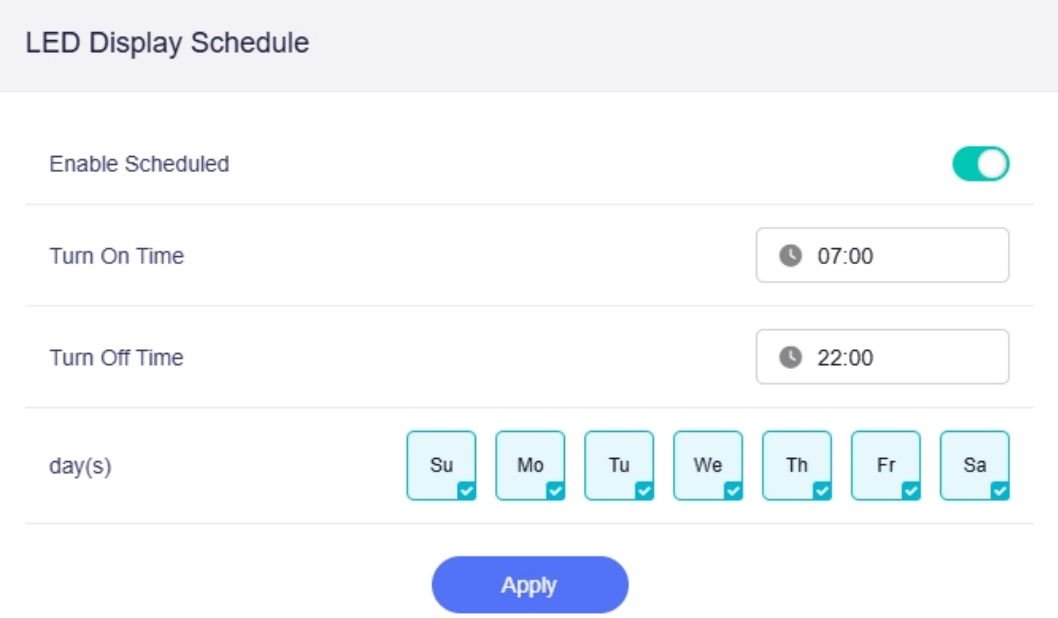
15.3 Geplante Aufgaben

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

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

15.3.1 LED-Zeitplan

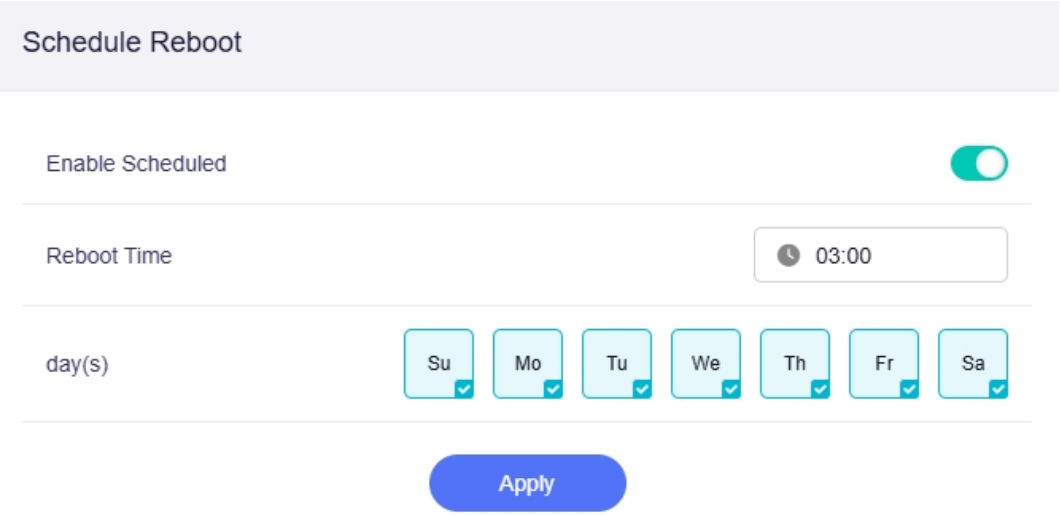
Legen Sie bei Bedarf einen Zeitplan für die Router-LED fest und klicken Sie auf **Apply**.



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

15.3.2 Geplanter Neustart

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



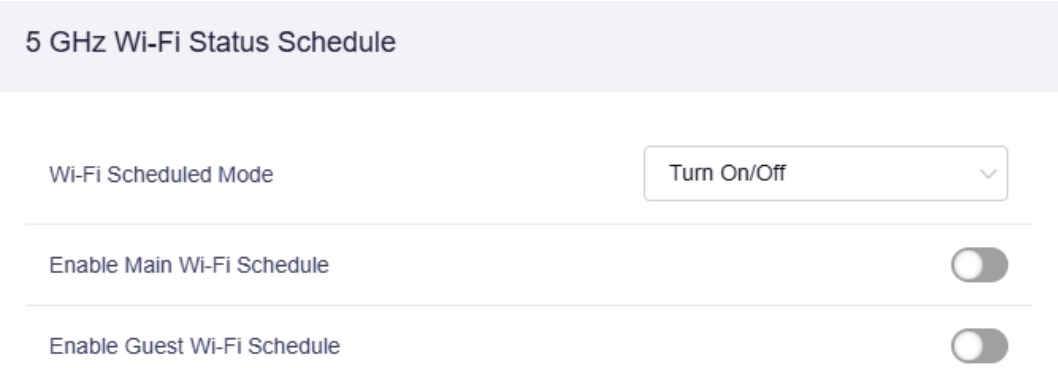
- **Enable Scheduled**: Aktiviert den geplanten Neustart.
- **Reboot Time**: Uhrzeit des Routerneustarts, etwa 03:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

15.3.3 Zeitplan für das 5-GHz-WLAN

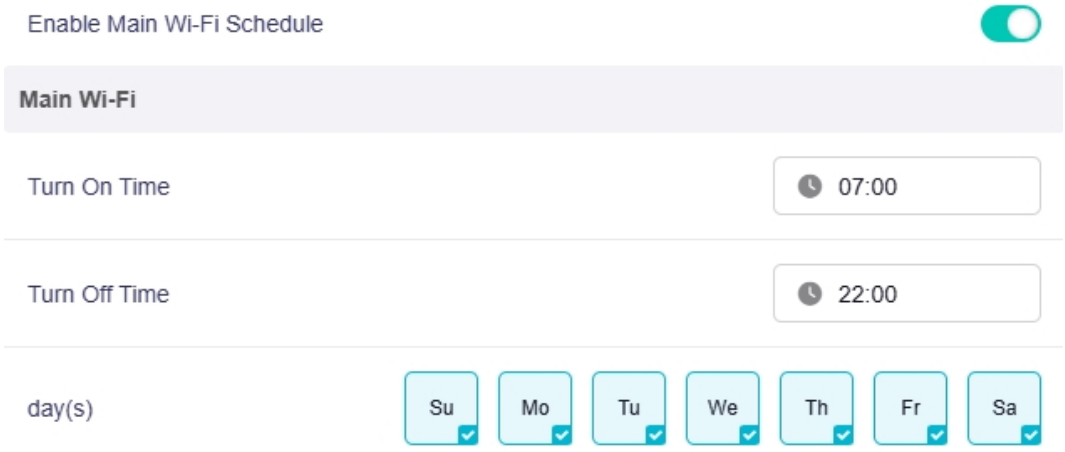
Hier legen Sie einen Zeitplan für Ihr 5-GHz-WLAN fest. Es gibt zwei Modi: Ein-/Ausschalten und Sendeleistung umschalten.

Modus 1: Ein-/Ausschalten

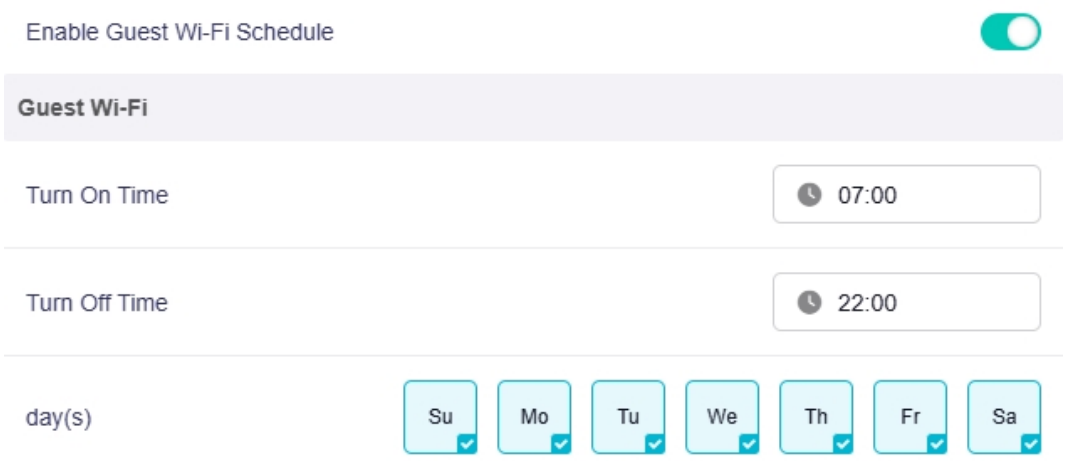
Sie können den Ein-/Ausschaltzeitplan sowohl für das 5-GHz-Hauptnetzwerk als auch für das Gastnetzwerk aktivieren.



- **Main Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 5-GHz-Hauptnetzwerk fest.

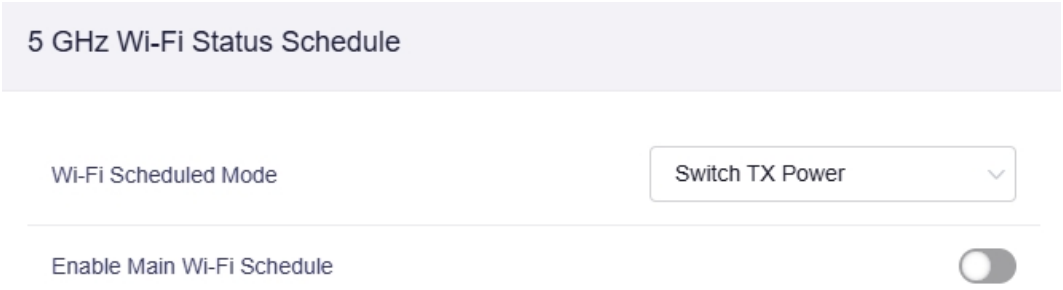


- **Guest Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 5-GHz-Gastnetzwerk fest.

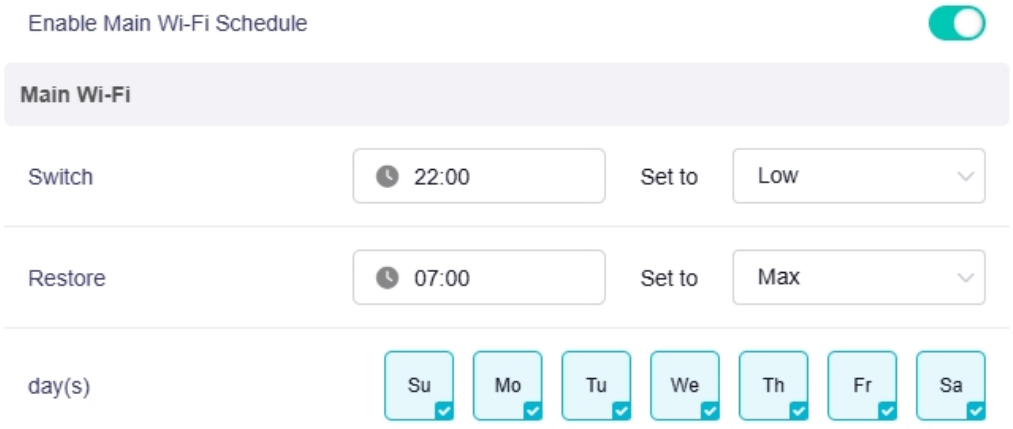


Modus 2: Sendeleistung umschalten

Für das 5-GHz-Hauptnetzwerk können Sie einen Zeitplan zum Umschalten der Sendeleistung aktivieren.



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



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

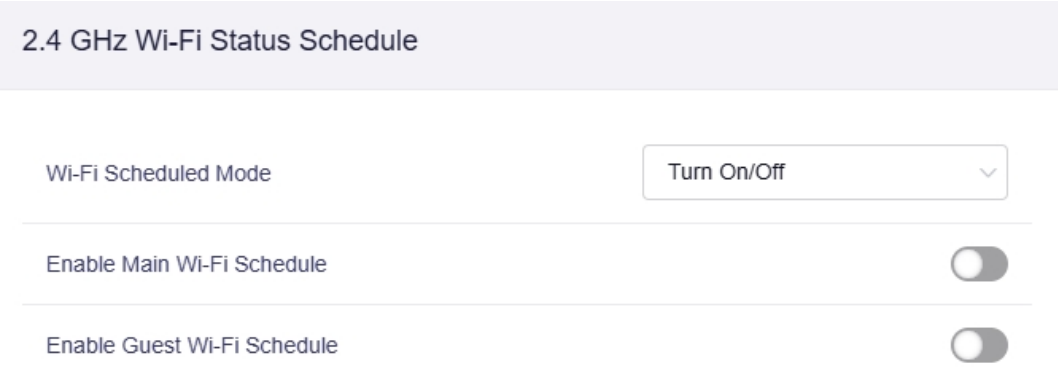
- **Restore**: Setzt die Sendeleistung zu einer anderen Uhrzeit, etwa 07:00 Uhr, auf eine andere Stufe wie Max zurück.
- **days**: Wochentage, an denen die Einstellungen gelten.

15.3.4 Zeitplan für das 2,4-GHz-WLAN

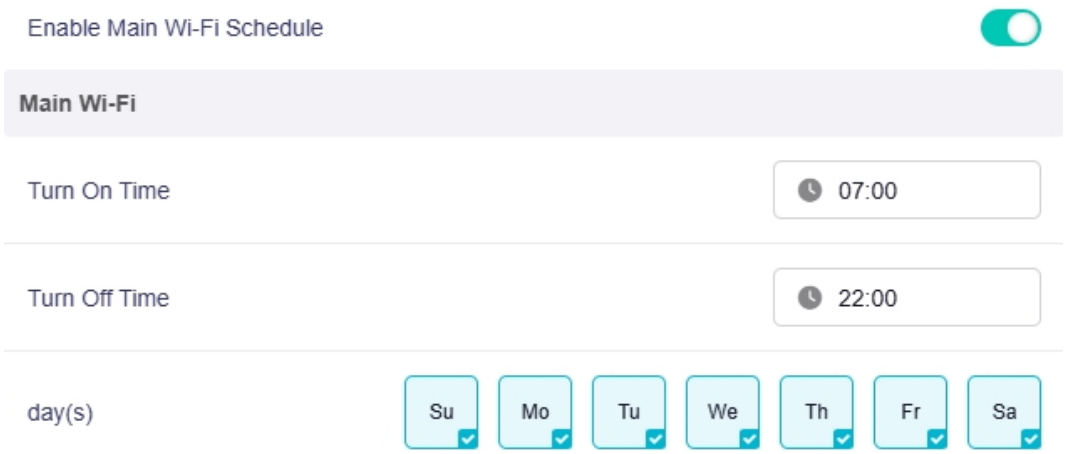
Hier legen Sie einen Zeitplan für Ihr 2,4-GHz-WLAN fest. Es gibt zwei Modi: Ein-/Ausschalten und Sendeleistung umschalten.

Modus 1: Ein-/Ausschalten

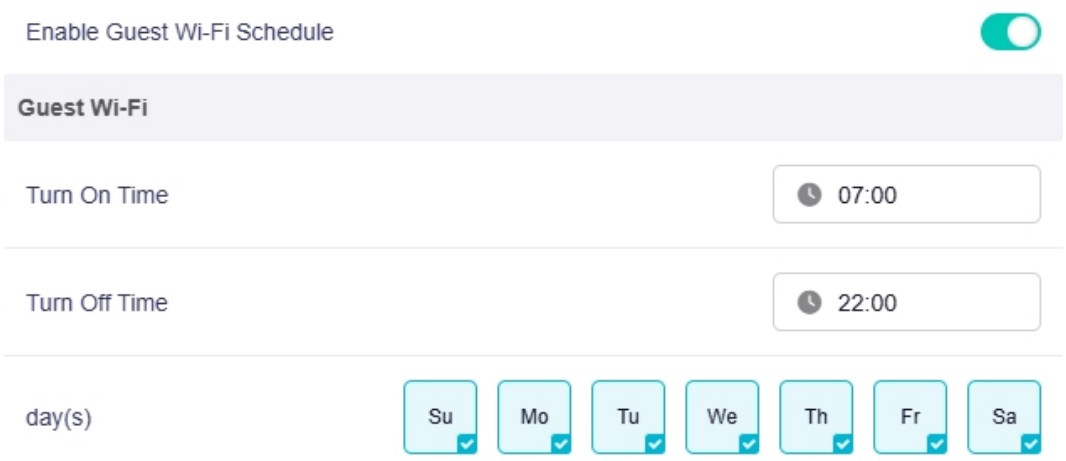
Sie können den Ein-/Ausschaltzeitplan sowohl für das 2,4-GHz-Hauptnetzwerk als auch für das Gastnetzwerk aktivieren.



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

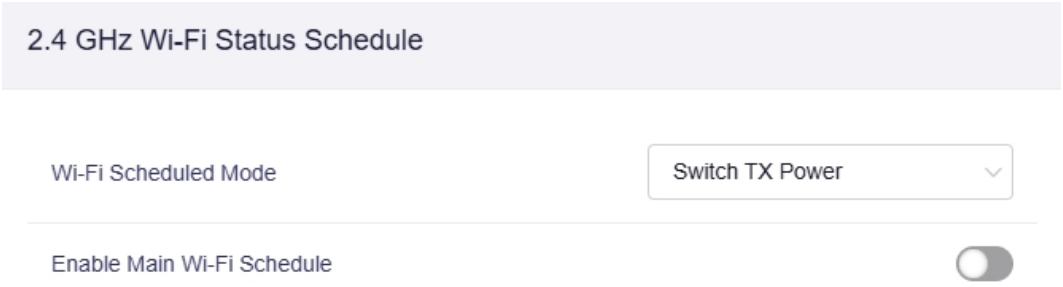


- **Guest Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 2,4-GHz-Gastnetzwerk fest.

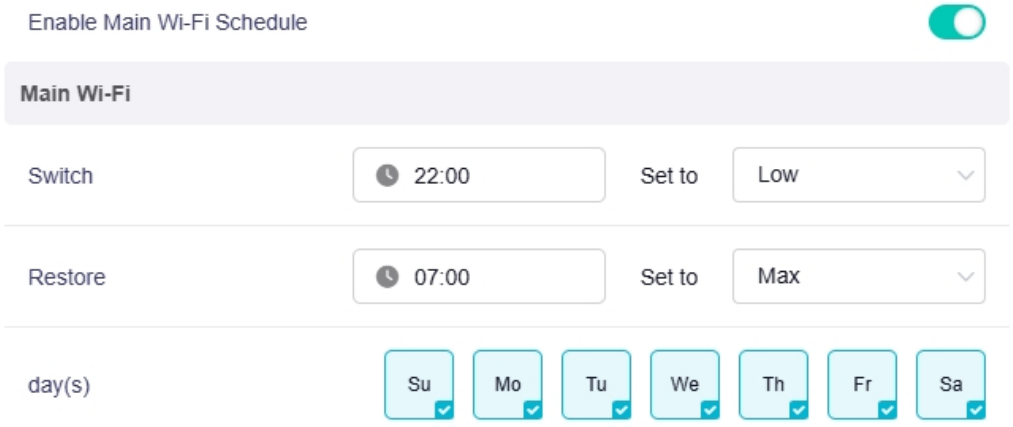


Modus 2: Sendeleistung umschalten

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



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

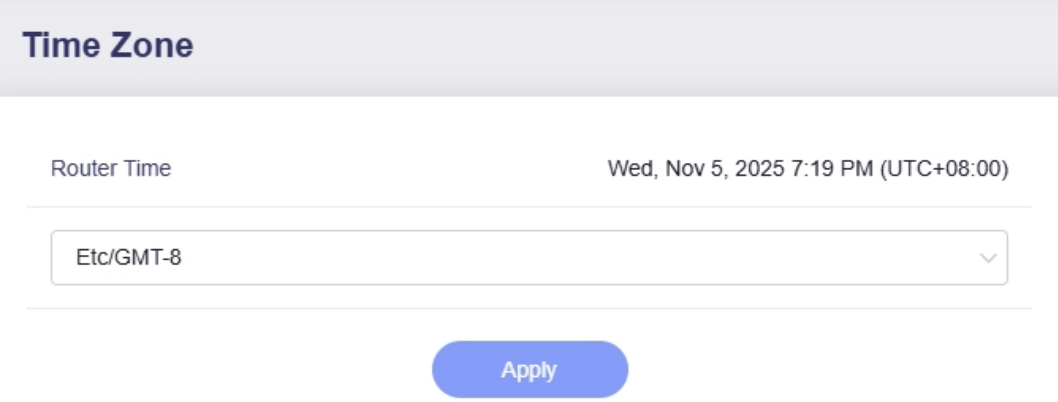


- **Switch**: Stellt die Sendeleistung zu einer bestimmten Uhrzeit, etwa 22:00 Uhr, auf eine festgelegte Stufe wie Low.

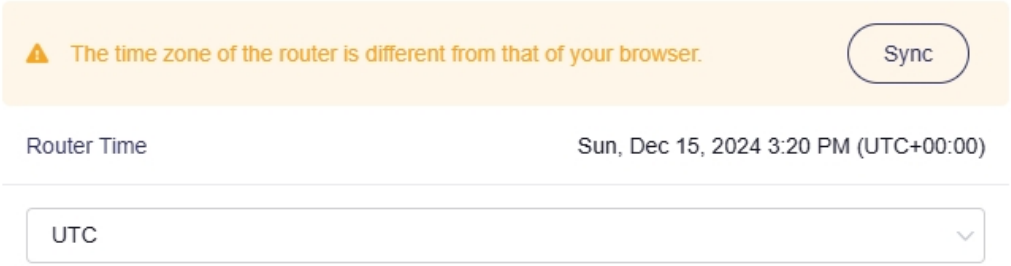
- **Restore**: Setzt die Sendeleistung zu einer anderen Uhrzeit, etwa 07:00 Uhr, auf eine andere Stufe wie Max zurück.
- **days**: Wochentage, an denen die Einstellungen gelten.

15.4 Zeitzone

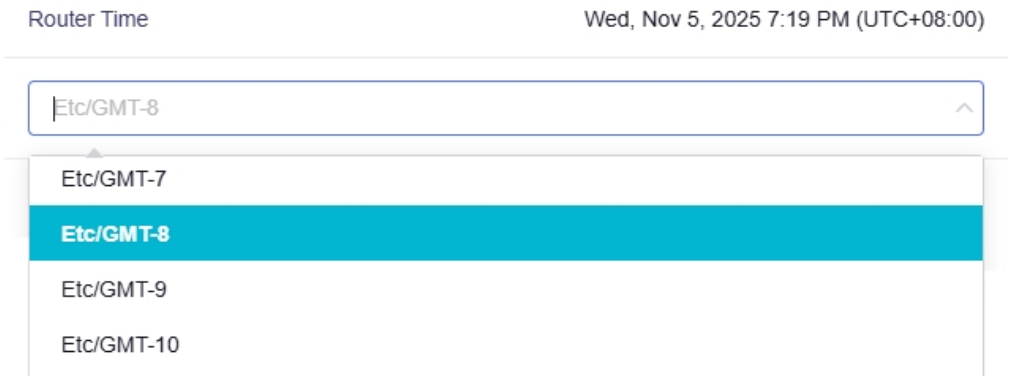
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Time Zone**. Die Seite zeigt die Systemzeit Ihres Routers mit Datum, Uhrzeit und Zeitzonenversatz an.



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

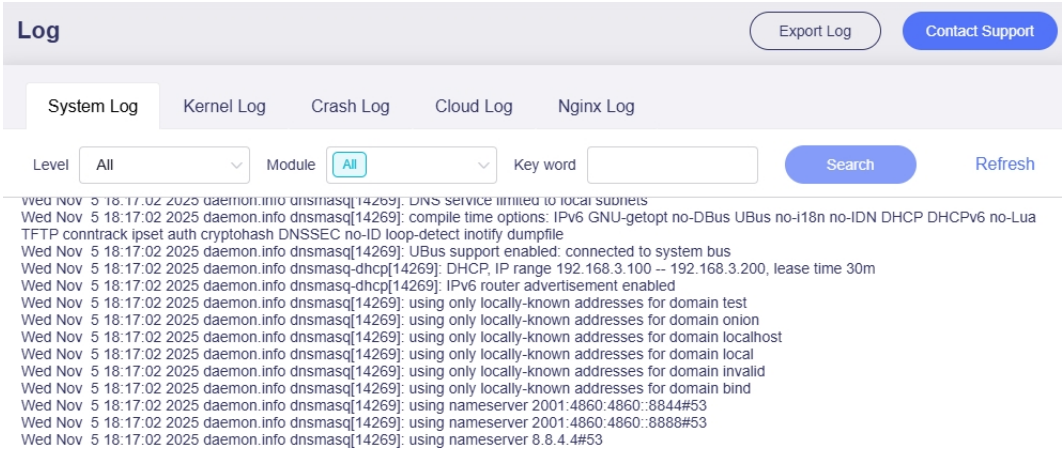


Wählen Sie zum Ändern der Zeitzone den passenden Eintrag aus der Liste, damit die Routerzeit Ihrer Ortszeit entspricht.

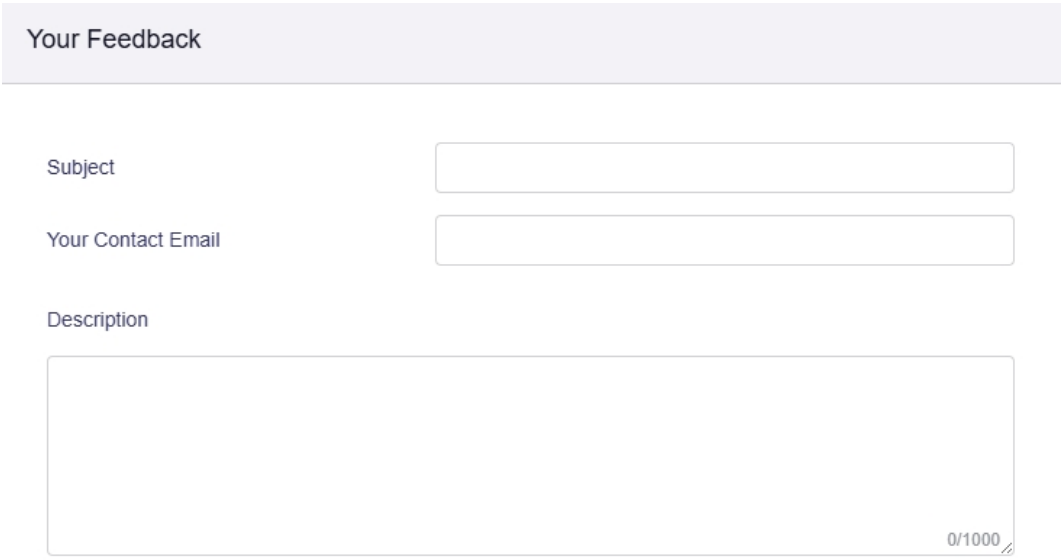

Router Time
Wed, Nov 5, 2025 7:19 PM (UTC+08:00)
Etc/GMT-8
Etc/GMT-7
Etc/GMT-8
Etc/GMT-9
Etc/GMT-10

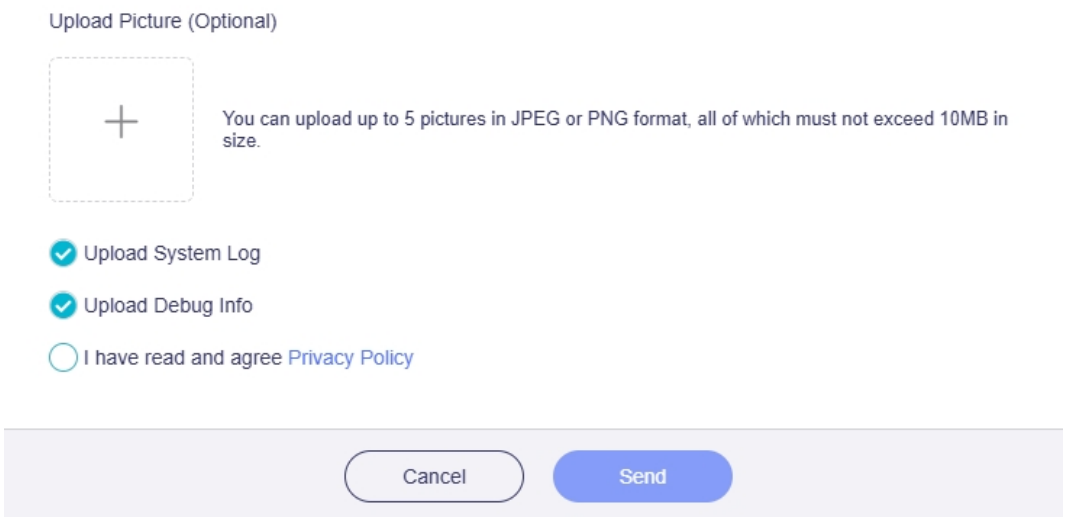
15.5 Protokolle

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



- **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.




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

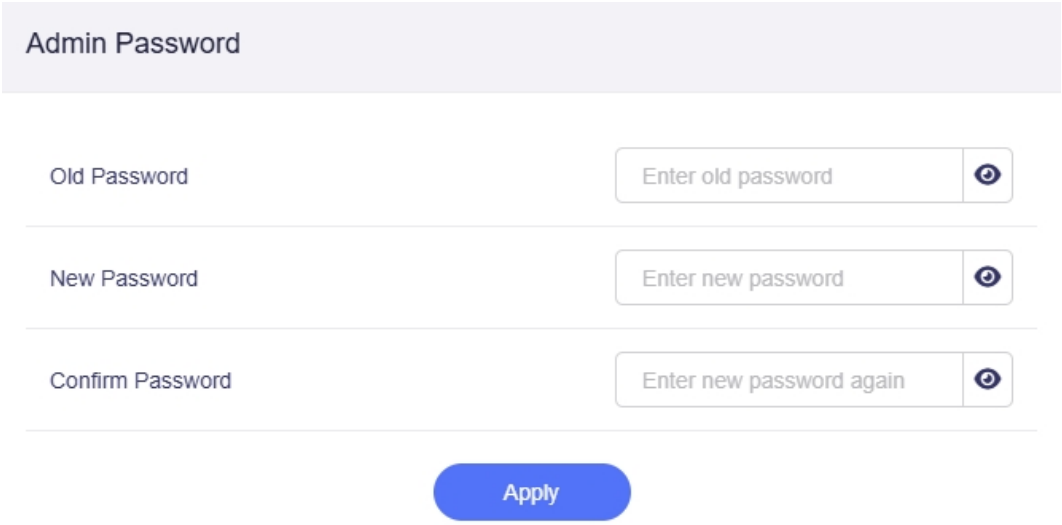
15.6 Sicherheit

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 am Router

15.6.1 Administratorpasswort

In diesem Abschnitt ändern Sie das Anmeldepasswort der Weboberfläche.

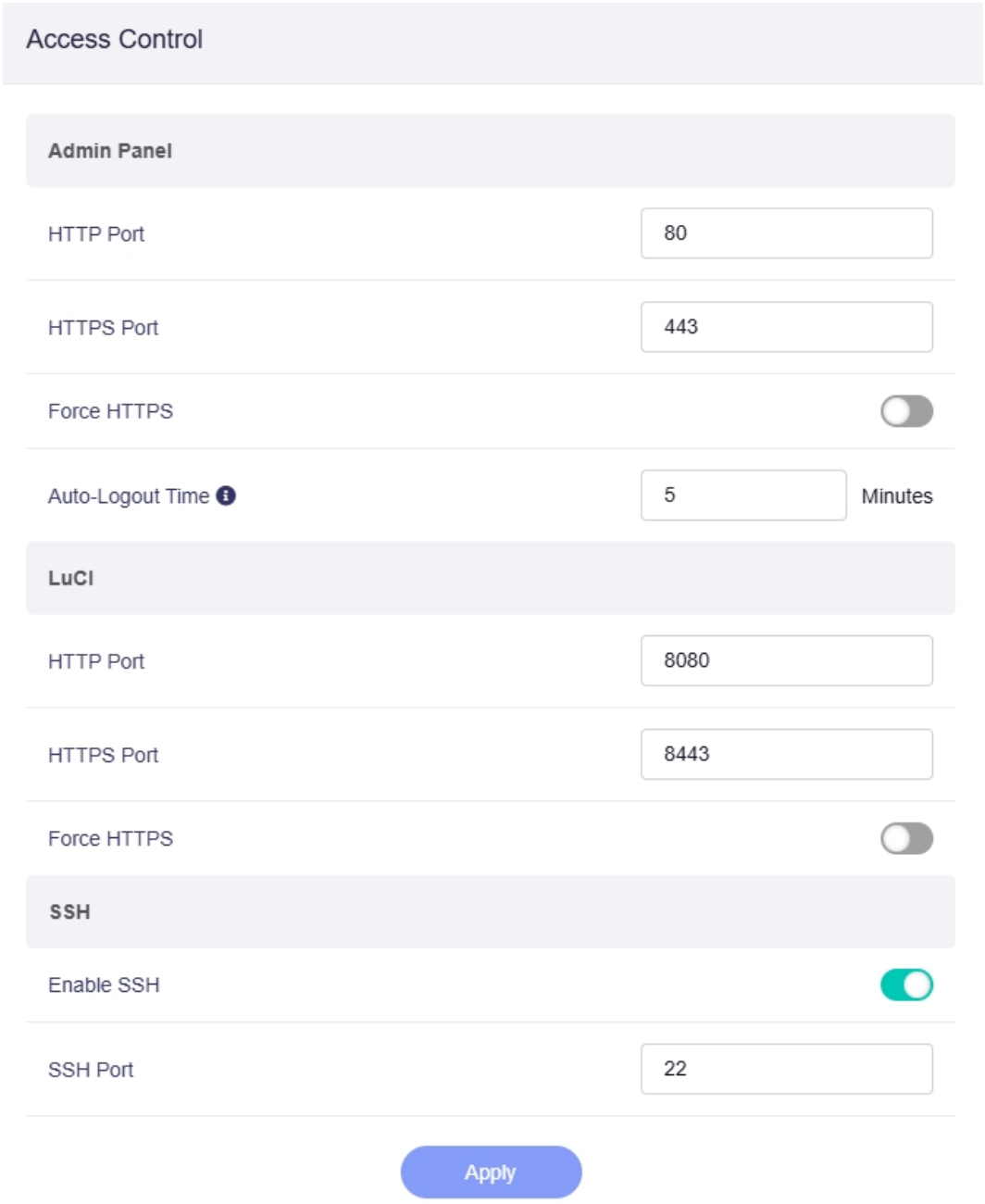


Für das Administratorpasswort gelten folgende Anforderungen:

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.

15.6.2 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.

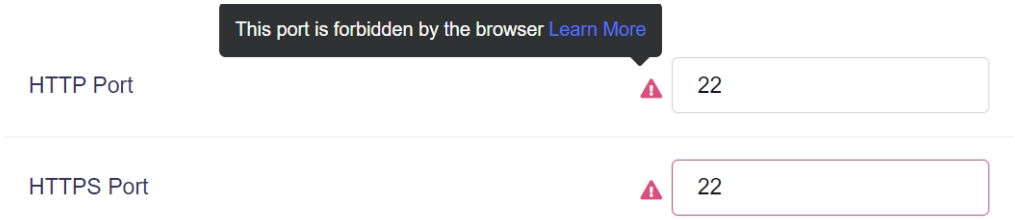
- **HTTP Port**: Standardmäßig 8080; wird für den unverschlüsselten HTTP-Zugriff auf die LuCI -Oberfläche verwendet.
- **HTTPS Port**: Standardmäßig 8443; wird für den sicheren HTTPS-Zugriff auf die LuCI-Oberfläche verwendet.
- **Force HTTPS**: Bei aktivierter Option ist der Zugriff auf die LuCI-Oberfläche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

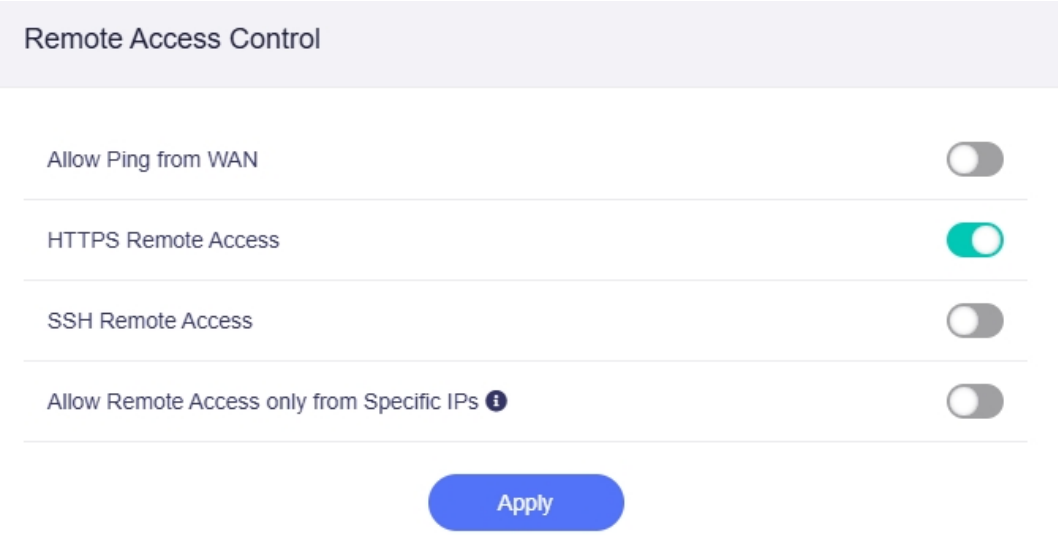


2. Nach einer Änderung der Portnummer in der Firmware müssen Sie die neue Portnummer beim Aufrufen der Weboberfläche angeben. Haben Sie sie vergessen, setzen Sie den Router zurück, um den Standardport wiederherzustellen.

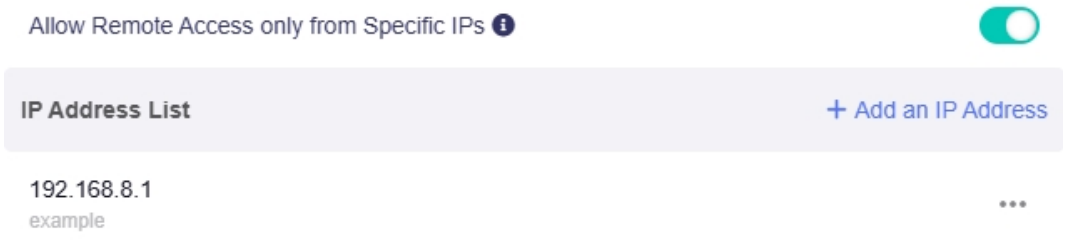
3. Die LuCI-Zugriffseinstellungen sind erst nach der Installation von LuCI verfügbar. Wenn diese Einstellungen nicht angezeigt werden, öffnen Sie **SYSTEM** > **Advanced Settings** und installieren Sie LuCI.

15.6.3 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.

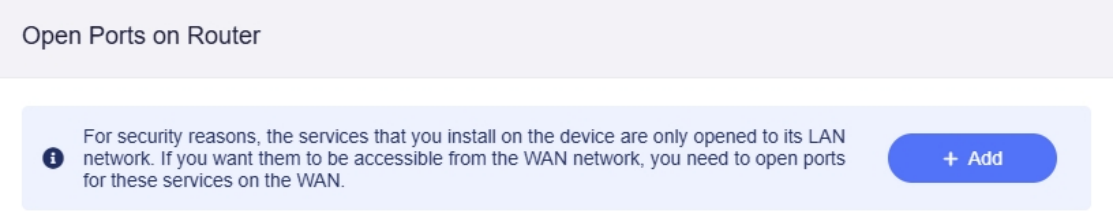


- **Allow Ping from WAN**: Erlaubt Ping-Anfragen von der WAN-Seite. Bei Netzwerkproblemen können Sie damit die Erreichbarkeit des Routers sowie Latenz und Paketverlust prüfen.
- **HTTPS Remote Access**: Ermöglicht den sicheren Fernzugriff auf die Weboberfläche über HTTPS. Die Datenübertragung bei der 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.

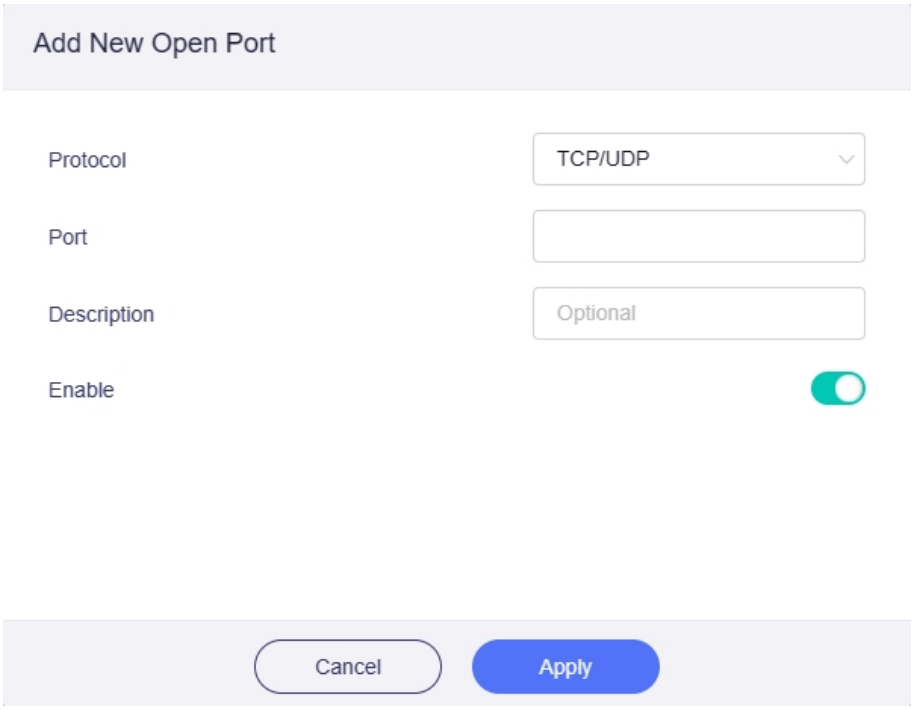


15.6.4 Ports am Router öffnen

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.

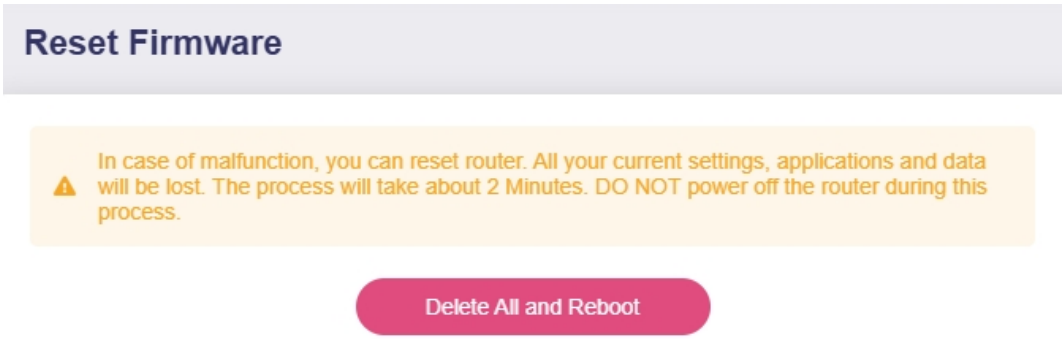


- **Protocol**: Wählen Sie das Netzwerkprotokoll für den Port aus: TCP, UDP oder TCP/UDP. Dies bestimmt die Art der Datenübertragung für den zugehörigen Dienst.
- **Port**: Geben Sie die Nummer des zu öffnenden Ports ein.
- **Description** (optional): Geben Sie zur einfacheren Verwaltung eine kurze Beschreibung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

15.7 Firmware zurücksetzen

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

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



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

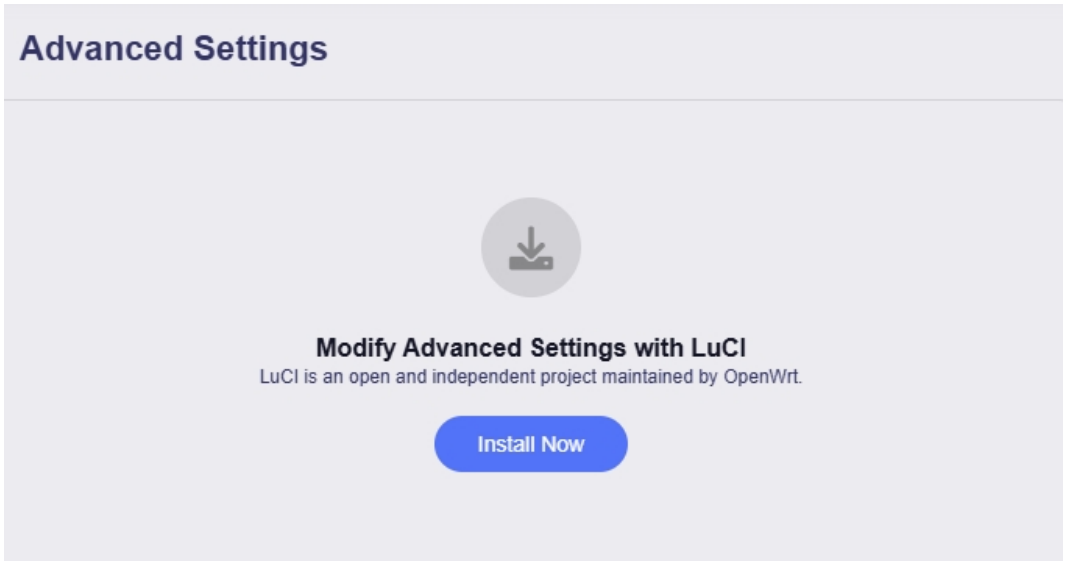
Falls Sie die Weboberfläche nicht erreichen, setzen Sie den Router mit der seitlichen Reset-Taste zurück.

15.8 Erweiterte Einstellungen

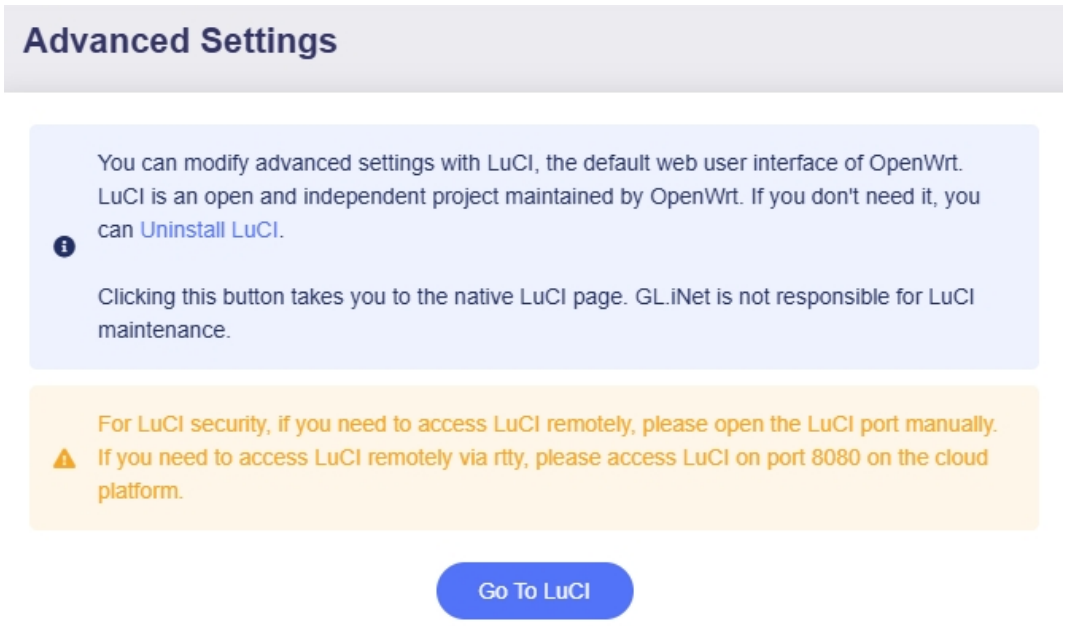
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Advanced Settings**. Hier ändern Sie erweiterte Einstellungen in LuCI, der standardmäßigen OpenWrt-Weboberfläche. LuCI ist ein offenes, unabhängiges Projekt, das von OpenWrt gepflegt und in der vorliegenden Form bereitgestellt wird.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

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

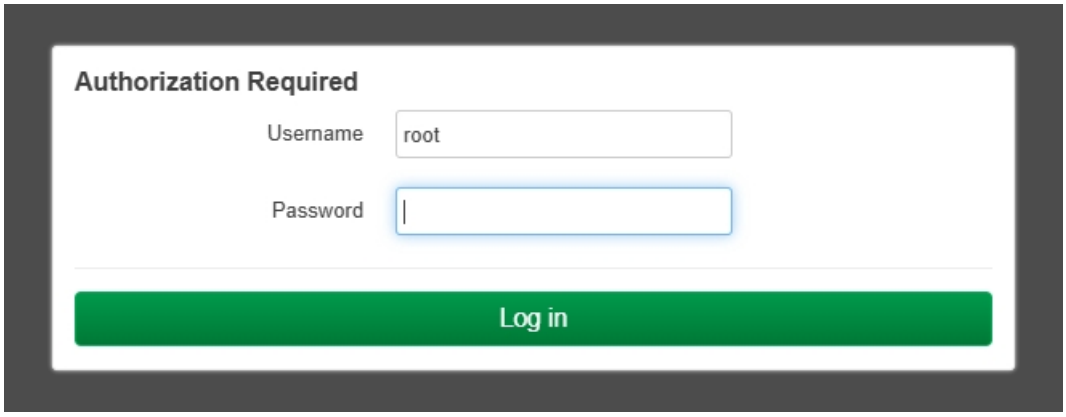
1. Klicken Sie auf **Install Now**, um die LuCI-Oberfläche zu installieren.



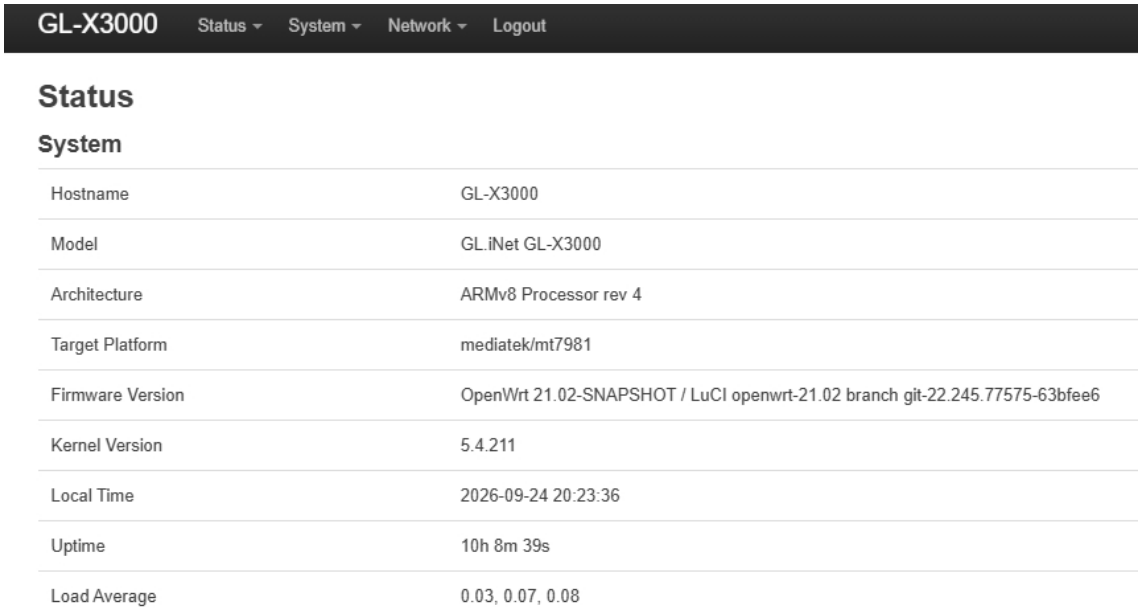
2. Klicken Sie auf **Go To LuCI**, um zur LuCI-Anmeldeseite zu gelangen.



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



Sie sind nun an der LuCI-Oberfläche angemeldet.



Konformitätserklärung

Hiermit erklärt GL TECHNOLOGIES (HONG KONG) LIMITED, dass der Funkanlagentyp [5G NR Wi-Fi 6-Router, GL-X3000NR / 4G LTE Wi-Fi 6-Router, GL-X3000C16] den grundlegenden Anforderungen und anderen relevanten Bestimmungen der Richtlinie 2014/53/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: https://www.gl-inet.com/products/certificate.