GL·iNet



Benutzerhandbuch

GL-E5800 / Mudi 7

5G-NR-Reiserouter mit Triband-Wi-Fi 7

Firmware-Version 4.8.5

Über dieses Handbuch

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

Mit diesem Handbuch können Sie:

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

Darstellungskonventionen

Diese Symbole und Farben erleichtern Ihnen das Befolgen der Anweisungen.

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

Hinweis:

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

Weitere Hilfe und Informationen

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

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

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

Inhaltsverzeichnis

Sicherheitshinweise 6

Kapitel 1 Ihren Router kennenlernen 8

1.1 Produktübersicht 9

1.1.1 Geräteansicht 9

1.1.2 Anschlüsse und Bedienelemente 10

1.1.3 Touchscreen 11

1.2 Technische Daten 12

1.3 Frequenzbänder 13

1.4 Lieferumfang 14

Kapitel 2 Ersteinrichtung des Routers 15

Kapitel 3 Am Router anmelden 17

Kapitel 4 Internetverbindung einrichten 19

4.1 Schnelleinrichtung mit dem Assistenten 20

4.2 Internetverbindung manuell einrichten 21

4.2.1 Internetverbindung über Mobilfunk herstellen 23

4.2.2 Internetverbindung über Ethernetkabel 29

4.2.3 Internetverbindung über ein vorhandenes WLAN 35

4.2.4 Internetverbindung über USB-Tethering 40

4.2.5 Internetverbindung über USB-Ethernet herstellen 42

Kapitel 5 WLAN 44

5.1 WLAN-Statusanzeige 45

5.2 WLAN-Einstellungen 46

5.2.1 5-GHz-/6-GHz-WLAN 46

5.2.2 2,4-GHz-WLAN 50

5.2.3 Zufällige BSSID 52

Kapitel 6 Verbundene Geräte 55

6.1 Gerätedetails 57

6.2 Aktionen 60

6.3 Geräte entfernen 63

6.4 Sortierung 64

Kapitel 7 Cloud-Dienste 65

7.1 GoodCloud 66
7.1.1 GoodCloud aktivieren 67
7.1.2 Router verwalten 69
7.1.3 Geräteverknüpfung aufheben 74
7.1.4 GoodCloud deaktivieren 74
7.2 AstroWarp 76
Kapitel 8 VPN kennenlernen 77
8.1 Einführung 78
8.2 Einsatzmöglichkeiten 79
Kapitel 9 VPN-Dashboard 82
9.1 VPN-Einrichtungsassistent 83
9.2 VPN-Modus 86
9.2.1 Globaler Modus 87
9.2.2 Richtlinienmodus 90
Kapitel 10 VPN-Server einrichten 101
10.1 OpenVPN-Server einrichten 102
10.1.1 Vorbereitung 102
10.1.2 Einrichtung 103
10.1.3 Fehlerbehebung 105
10.2 WireGuard-Server einrichten 106
10.2.1 Vorbereitung 106
10.2.2 Einrichtung 107
10.2.3 Fehlerbehebung 110
Kapitel 11 VPN-Client einrichten 112
11.1 OpenVPN-Client einrichten 113
11.1.1 Vorbereitung 113
11.1.2 NordVPN einrichten 113
11.1.3 OpenVPN-Client manuell einrichten (andere Anbieter) 119
11.2 WireGuard-Client einrichten 122
11.2.1 Vorbereitung 122
11.2.2 AzireVPN einrichten 123
11.2.3 Hide.me einrichten 128
11.2.4 IPVanish einrichten 131
11.2.5 Mullvad einrichten 136

11.2.6 NordVPN einrichten 140
11.2.7 PIA (Private Internet Access) einrichten 146
11.2.8 Surfshark einrichten 151
11.2.9 WireGuard-Client manuell einrichten (andere Anbieter) 156
Kapitel 12 Netzwerk 161
12.1 Multi-WAN 162
12.1.1 Schnittstellenstatus überwachen 162
12.1.2 Multi-WAN-Modus 165
12.2 LAN 168
12.2.1 Grundeinstellungen 168
12.2.2 DHCP-Server 169
12.2.3 Adressreservierung 171
12.3 Gastnetzwerk 172
12.3.1 Grundeinstellungen 172
12.3.2 DHCP-Server 173
12.4 DNS 175
12.4.1 DNS-Servereinstellungen 176
12.4.2 Hosts bearbeiten 178
12.5 Ethernetanschlüsse 181
12.6 IPv6 182
12.6.1 IPv6-Modus 183
12.6.2 DNS-Adressen beziehen 183
12.7 IGMP Snooping 184
12.8 Netzwerkmodus 185
12.9 Drop-in Gateway 187
12.10 Netzwerkbeschleunigung 189
Kapitel 13 Datenverkehr steuern 191
13.1 Kindersicherung 192
13.1.1 Schnelleinrichtung 192
13.1.2 Fehlerbehebung 201
Kapitel 14 Sicherheit 202
14.1 Portweiterleitung 203
14.1.1 DMZ 203
14.1.2 Portweiterleitung 204

14.2 Administratorzugriff 207
14.2.1 Zugriffskontrolle 207
14.2.2 Fernzugriffskontrolle 210
14.2.3 Ports am Router öffnen 211
14.3 NAT-Modus 212
Kapitel 15 Anwendungen 213
15.1 Plug-ins 214
15.2 Dynamisches DNS 215
15.2.1 DDNS aktivieren 215
15.2.2 DDNS-Funktion prüfen 218
15.2.3 HTTPS-Fernzugriff 220
15.2.4 SSH-Fernzugriff 222
15.3 Netzwerkspeicher 224
15.3.1 Speicher anschließen 224
15.3.2 Samba einrichten 225
15.3.3 WebDAV einrichten 229
15.3.4 DLNA einrichten 232
15.4 AdGuard Home 233
15.5 Tailscale 236
15.5.1 Tailscale einrichten 237
15.5.2 Fernzugriff auf WAN erlauben 240
15.5.3 Fernzugriff auf LAN erlauben 240
15.5.4 Eigene Exit-Nodes 241
15.6 ZeroTier 242
15.6.1 ZeroTier einrichten 243
15.6.2 Fernzugriff auf WAN erlauben 248
15.6.3 Fernzugriff auf LAN erlauben 249
15.7 Tor 250
Kapitel 16 System 252
16.1 Übersicht 253
16.2 Administratorpasswort 254
16.3 Aktualisierung 255
16.3.1 Online-Aktualisierung 255
16.3.2 Lokale Aktualisierung 256

16.4 Geplante Aufgaben 257
16.5 Displayverwaltung 258
16.6 USB und Stromversorgung 259
16.6.1 USB 259
16.6.2 Stromversorgung 260
16.7 Zeitzone 261
16.8 Firmware zurücksetzen 262
16.9 Protokolle 263
16.10 Erweiterte Einstellungen 265
Sicherheitshinweise zum Akku 267
Konformitätserklärung 268

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

Mudi 7 (GL-E5800) bietet ultraschnelle 5G-Verbindungen mit bis zu 4,67 Gbit/s und Triband-Wi-Fi 7 für zuverlässige, sichere Netzwerke. Eine integrierte eSIM und Dual-SIM-Dual-Standby sorgen für eine nahtlose Verbindung. Mit Touchscreen, 2,5G-Ethernetanschluss, Schnellladefunktion und langer Akkulaufzeit ist Mudi 7 Ihre Komplettlösung für leistungsstarke mobile Konnektivität.

1.1.1 Geräteansicht

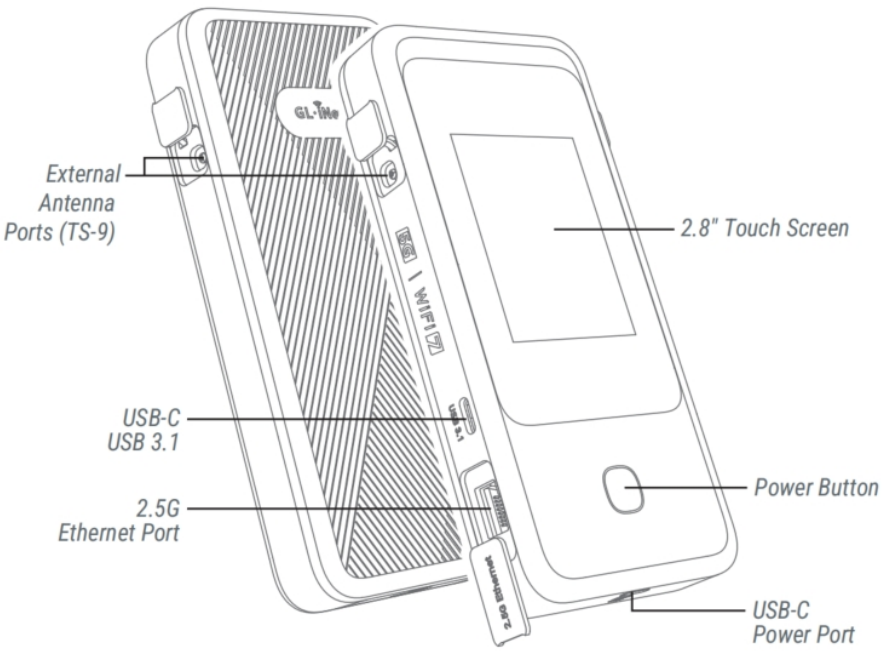






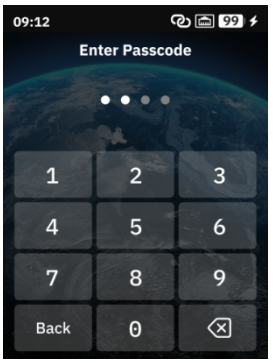
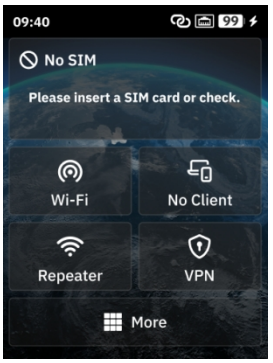
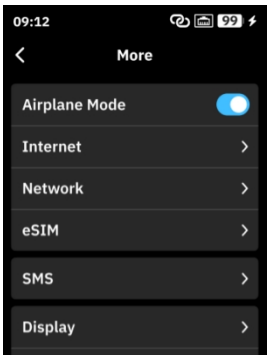


1.1.2 Anschlüsse und Bedienelemente



Element	Beschreibung
Stromanschluss	Zum Anschließen des Netzteils.
Ein-/Aus-Taste	Drücken Sie die Taste, um den Bildschirm zu aktivieren oder zur Startseite zurückzukehren.
2,5G-Ethernetanschluss	Als WAN: Verbindung mit einem Modem oder einer Ethernetdose. Als LAN: Bei Bedarf Verbindung mit kabelgebundenen Geräten.
USB-3.1-Anschluss	Für USB-Speichergeräte, USB-Tethering mit einem Smartphone und kompatible Mobilfunksticks.
2,8-Zoll-Touchscreen	Zur Statusanzeige in Echtzeit und zur umfassenden Steuerung der Funktionen.
Anschlüsse für externe Antennen (TS-9)	Zum Anschließen externer Antennen mit TS-9-Schnittstelle.

1.1.3 Touchscreen

Bildschirmanzeige	Beschreibung
	Aktivierungsbildschirm Sie können die Anzeige von Uhrzeit und Datum auf dem Aktivierungsbildschirm anpassen und bei Bedarf ein eigenes Hintergrundbild festlegen.
	Bildschirmcode eingeben Zum Entsperren des Bildschirms ist ein vierstelliger Code erforderlich. Sie können die Zeit bis zur automatischen Bildschirmsperre anpassen, damit Sie den Code seltener eingeben müssen.
	Startseite Die Startseite zeigt den Status von SIM, WLAN, verbundenen Geräten, Repeater und VPN an und bietet schnellen Zugriff auf häufig verwendete Funktionen.
	Weitere Einstellungen Tippen Sie auf der Startseite auf More, um weitere Einstellungen aufzurufen.

1.2 Technische Daten

Anschlüsse	1 × 2,5-Gbit/s-WAN/LAN-Ethernetanschluss 1 × 2,8-Zoll-LCD-Farb-Touchscreen 2 × Nano-SIM-Kartensteckplatz 1 × integrierter eSIM-Chip 1 × USB-C (nur Stromversorgung; Stromeingang und -ausgang) 1 × USB-C (10 Gbit/s; Stromeingang und -ausgang, USB OTG) 2 × TS-9-Anschluss 1 × Ein-/Aus-Taste 1 × Reset-Taste
5G-Plattform	Qualcomm Dragonwing MBB Gen 3 (X72)
CPU	Qualcomm, Quad-Core mit 2,2 GHz
Arbeitsspeicher / Speicher	2 GB LPDDR4X / 8 GB eMMC
WLAN-Geschwindigkeit	688 Mbit/s (2,4 GHz), 2882 Mbit/s (5 GHz), 5764 Mbit/s (6 GHz)
Antennen	8 × interne Antenne (6 × Mobilfunkantenne, 2 × WLAN-Antenne für 2,4 GHz, 5 GHz und 6 GHz)
Ethernet-Geschwindigkeit	100/1000/2500 Mbit/s
eSIM	1 × integrierte eSIM
Integrierter Akku	3,85 V / 5380 mAh / 20,72 Wh
Stromversorgung	USB PD/PPS, 5–12 V, max. 30 W
Leistungsaufnahme	<30W
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Abmessungen / Gewicht	157 × 75 × 22,8 mm / 300 g
Weitere Ressourcen	Datenblatt / Firmware / App / Auspacken / Anleitungen

*Die WLAN-Geschwindigkeiten basieren auf den IEEE-802.11-Standards, etwa 802.11be für Wi-Fi 7. Der tatsächliche Datendurchsatz und die Reichweite können durch Hindernisse wie

Wände oder Metall, Netzwerkauslastung und die Leistungsfähigkeit der Endgeräte geringer ausfallen.

*Für die Nutzung von Wi-Fi 7 (802.11be) und seiner Funktionen wie OFDMA, MU-MIMO, 4096-QAM und MLO müssen die Endgeräte die jeweiligen Technologien unterstützen.

1.3 Frequenzbänder

	GL-E5800NA	**GL-E5800EU**
5G-NR-Konnektivität	NSA-/SA-Betrieb gemäß 3GPP Rel-17, Sub-6 GHz	
5G NR NSA	n2 / n5 / n7 / n12 / n14 / n25 / n26 / n30 / n38 / n41 / n48 / n66 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
5G NR SA	n2 / n5 / n7 / n12 / n13 / n14 / n25 / n26 / n29 / n30 / n38 / n41 / n48 / n66 / n70 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
LTE-Kategorie	Cat 20 (DL) / Cat 18 (UL)	
LTE-FDD	B2 / B4 / B5 / B7 / B12 / B13 / B14 / B17 / B25 / B26 / B29 / B30 / B66 / B71	B1 / B3 / B5 / B7 / B8 / B20 / B28 / B32
LTE-TDD	B38 / B41 / B42 / B43 / B48	B38 / B40 / B41 / B42 / B43
WCDMA		B1 / B5 / B8

1.4 Lieferumfang

Im Lieferumfang enthalten:

- 1 × Mudi 7 (GL-E5800)
- 1 × Kurzanleitung
- 1 × Akkupack
- 1 × USB-C-Kabel für 10 Gbit/s
- 1 × Transporttasche



Kapitel 2

Ersteinrichtung des Routers

Dieses Kapitel beschreibt die Ersteinrichtung des Routers und das Verbinden Ihrer Geräte.

Gehen Sie wie folgt vor, um den Router erstmals einzurichten und Ihre Geräte zu verbinden.

1. **Einschalten**
   Halten Sie die Ein-/Aus-Taste **3 Sekunden** lang gedrückt oder schließen Sie ein Netzteil an. Mudi 7 startet automatisch.

2. **System einrichten**
   Folgen Sie den Anweisungen auf dem Bildschirm, um die Grundeinstellungen festzulegen: Bildschirmcode, Administratorpasswort, WLAN-Name, WLAN-Passwort und Frequenzbänder.
   Tipp: Das voreingestellte Administratorpasswort besteht aus den letzten 9 Zeichen der Seriennummer (S/N) des Geräts, gefolgt vom Zeichen #. Sie können dieses Passwort verwenden oder ein eigenes festlegen.

3. **Ein Gerät mit dem Router verbinden**
   Verbinden Sie ein Gerät, beispielsweise einen Laptop oder ein Smartphone, per WLAN, Ethernetkabel oder USB-Kabel mit dem Router.
   - **WLAN**: Öffnen Sie auf Ihrem Gerät Einstellungen -> WLAN, wählen Sie den WLAN-Namen von Mudi 7 in der Liste der verfügbaren Netzwerke und geben Sie das Passwort ein. Den voreingestellten Netzwerknamen und das Passwort finden Sie auf dem Bildschirm von Mudi 7. Alternativ können Sie den QR-Code auf dem Bildschirm scannen und anschließend auf „Verbinden“ tippen.
   - **Ethernet**: Verbinden Sie Ihr Gerät per Ethernetkabel mit dem Ethernetanschluss von Mudi 7. Dieser ist standardmäßig als LAN-Anschluss eingerichtet.
   - **USB**: Verbinden Sie Ihr Gerät per USB-Kabel mit dem USB-C-Anschluss von Mudi 7. Der USB-C-Anschluss unterstützt OTG, sodass Sie im nächsten Schritt auf Mudi 7 zugreifen können.

4. **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

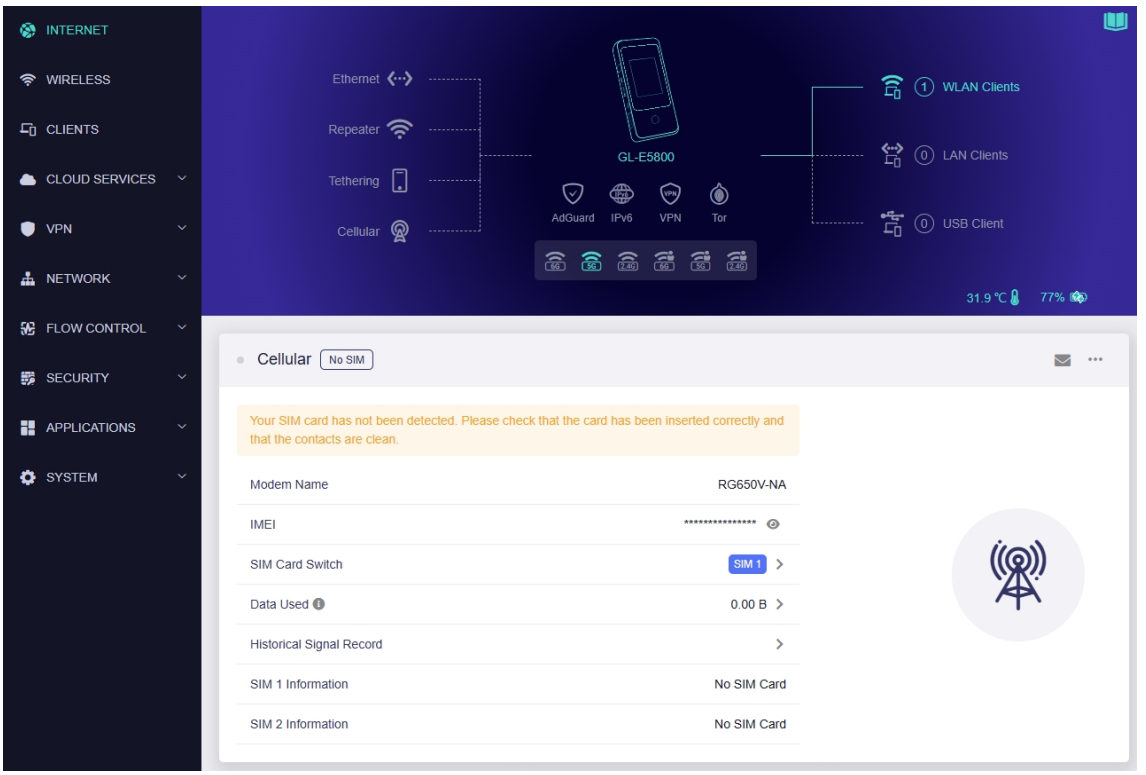
Dieses Kapitel erklärt, wie Sie sich über die Weboberfläche an Ihrem Router anmelden.

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. Aus Sicherheitsgründen empfiehlt sich ein starkes Passwort. Klicken Sie anschließend auf **Next**, um fortzufahren. Falls Sie bereits ein Administratorpasswort festgelegt haben, melden Sie sich direkt an.
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

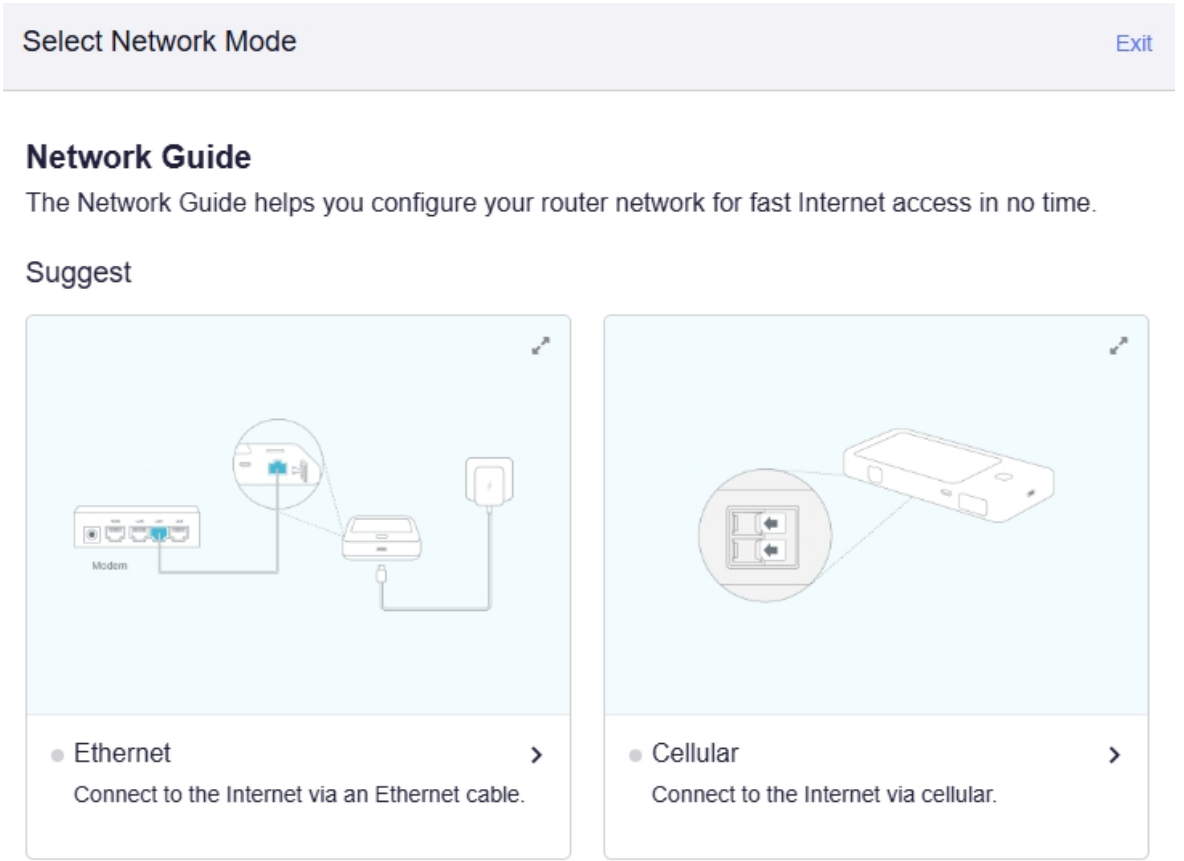
Der Einrichtungsassistent in der Weboberfläche führt Sie durch die Netzwerkkonfiguration des Routers.

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.

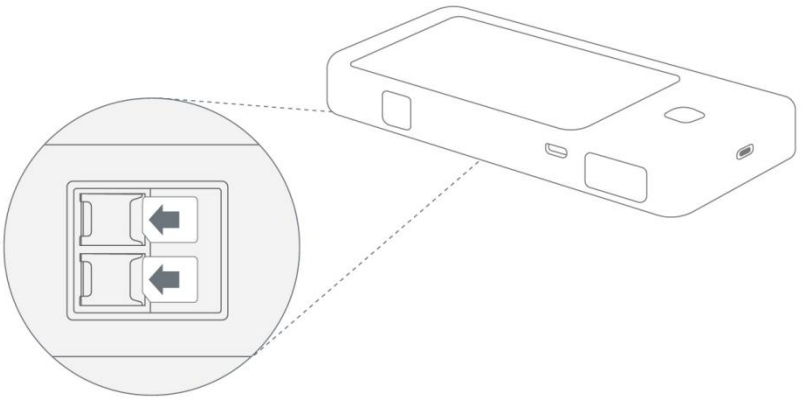
Mudi 7 unterstützt bis zu fünf Möglichkeiten für den Internetzugang: Mobilfunk, Ethernet, Repeater, USB-Tethering und USB-Ethernet. Wählen Sie die Methode, die zu Ihrem Einsatzzweck passt.

1. **Mobilfunk**: Setzen Sie eine SIM-Karte in den Router ein oder aktivieren Sie die integrierte eSIM. Der Router verbindet sich anschließend über ein 4G- oder 5G-Mobilfunknetz mit dem Internet, abhängig vom Netz Ihres Mobilfunkanbieters und den unterstützten Frequenzbändern. Diese Methode ist besonders flexibel und eignet sich beispielsweise für die Nutzung im Fahrzeug oder im Freien.

2. **Ethernet**: Verbinden Sie den WAN-Anschluss des Routers über ein Ethernetkabel mit einem Breitbandnetz. In der Regel erhält der Router automatisch per DHCP eine IP-Adresse. Sie können auch eine statische IP-Adresse oder PPPoE manuell konfigurieren. Diese Methode bietet eine besonders stabile und schnelle Verbindung und eignet sich ideal für zu Hause oder das Büro mit festem Breitbandanschluss.
   Mudi 7 verfügt außerdem über einen OTG-fähigen USB-C-Anschluss. Damit können Sie einen zweiten Ethernetanschluss für zwei Ethernet-WAN-Verbindungen hinzufügen. Hierfür benötigen Sie einen separat erhältlichen USB-C-auf-Ethernet-Adapter.
3. **Repeater**: In diesem Modus verbindet sich der Router mit einem vorhandenen WLAN, erweitert dessen Signalabdeckung und erstellt ein separates, sicheres lokales Netzwerk. Dabei kann die Übertragungsgeschwindigkeit etwas sinken. Der Modus eignet sich für Bereiche mit schwachem WLAN-Empfang und für öffentliche Orte, an denen zusätzliche Netzwerksicherheit erforderlich ist.
4. **USB-Tethering**: Verbinden Sie ein Smartphone oder ein anderes kompatibles Gerät per USB-Kabel mit dem Router, um dessen mobile Datenverbindung, etwa über 4G/5G, freizugeben. Dies ist eine praktische Lösung für einen vorübergehenden Internetzugang, besonders unterwegs oder an Orten ohne festen Breitbandanschluss.
5. **USB-Ethernet**: Mudi 7 verfügt über einen OTG-fähigen USB-C-Anschluss. Damit können Sie einen zweiten Ethernetanschluss für zwei Ethernet-WAN-Verbindungen hinzufügen. Hierfür benötigen Sie einen separat erhältlichen USB-C-auf-Ethernet-Adapter.

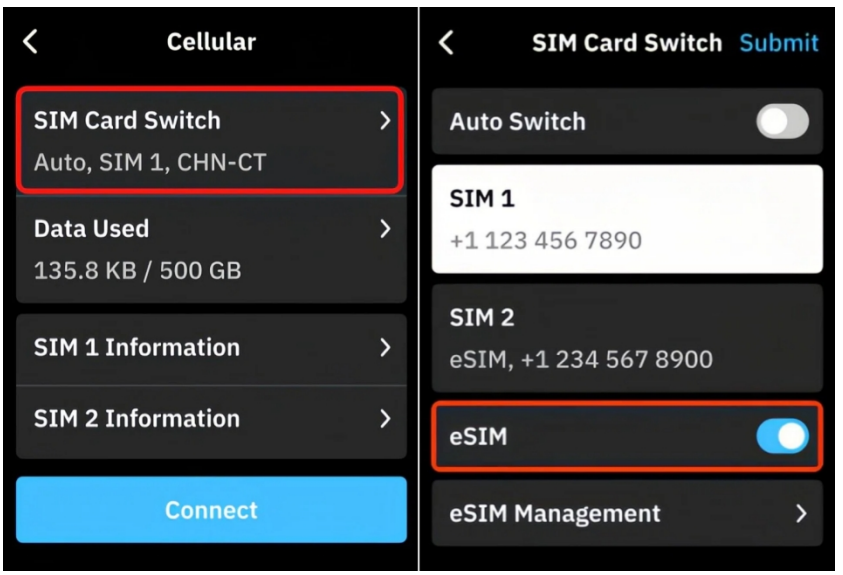
4.2.1 Internetverbindung über Mobilfunk herstellen

Mudi 7 verfügt über eine integrierte eSIM und zwei Nano-SIM-Steckplätze. Sie können ein eSIM-Datenpaket erwerben und ohne physische SIM-Karte auf das Internet zugreifen. Alternativ können Sie Nano-SIM-Karten einsetzen, um das 5G-Mobilfunknetz zu nutzen.

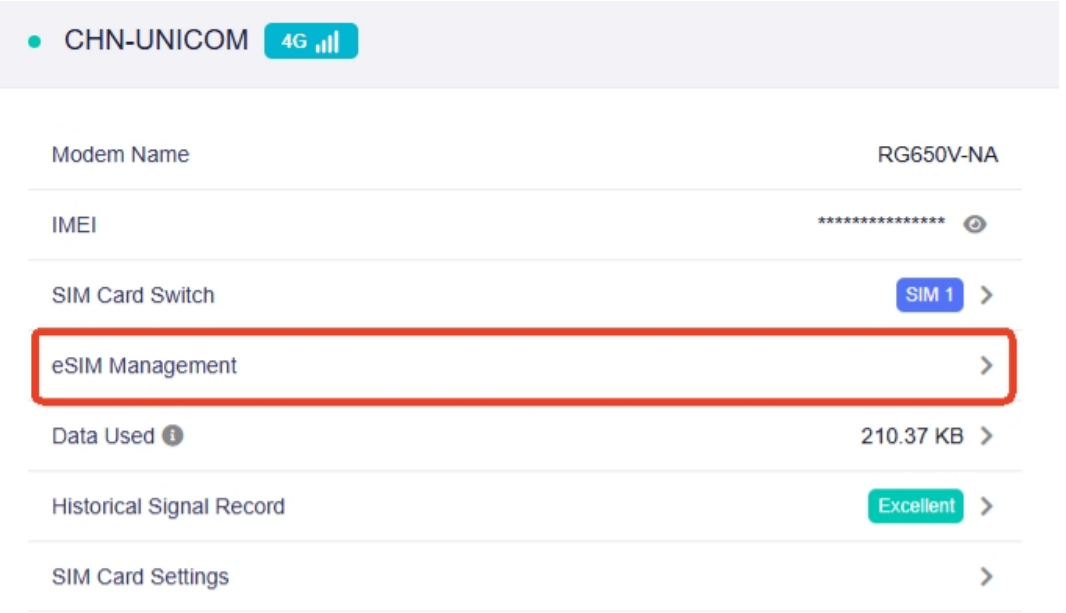


eSIM einrichten

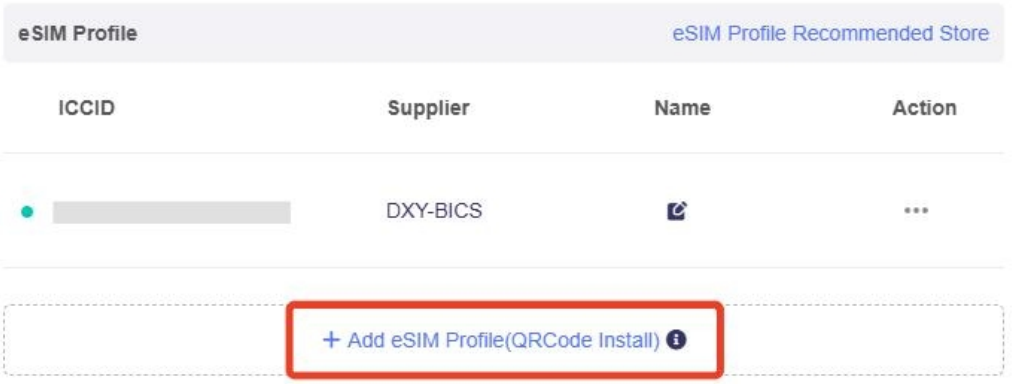
1. Öffnen Sie auf dem Touchscreen **Cellular** > **SIM Card Switch** und aktivieren Sie die eSIM mit dem Schalter.



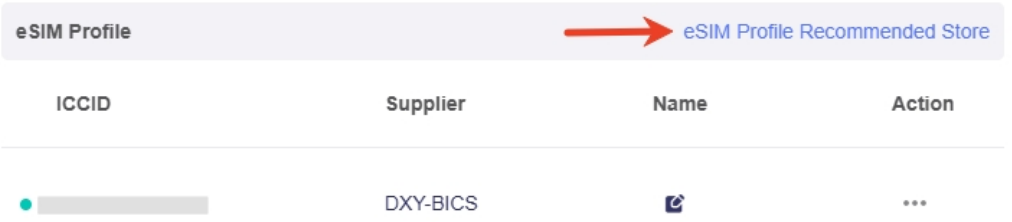
2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Cellular** > **eSIM Management**.



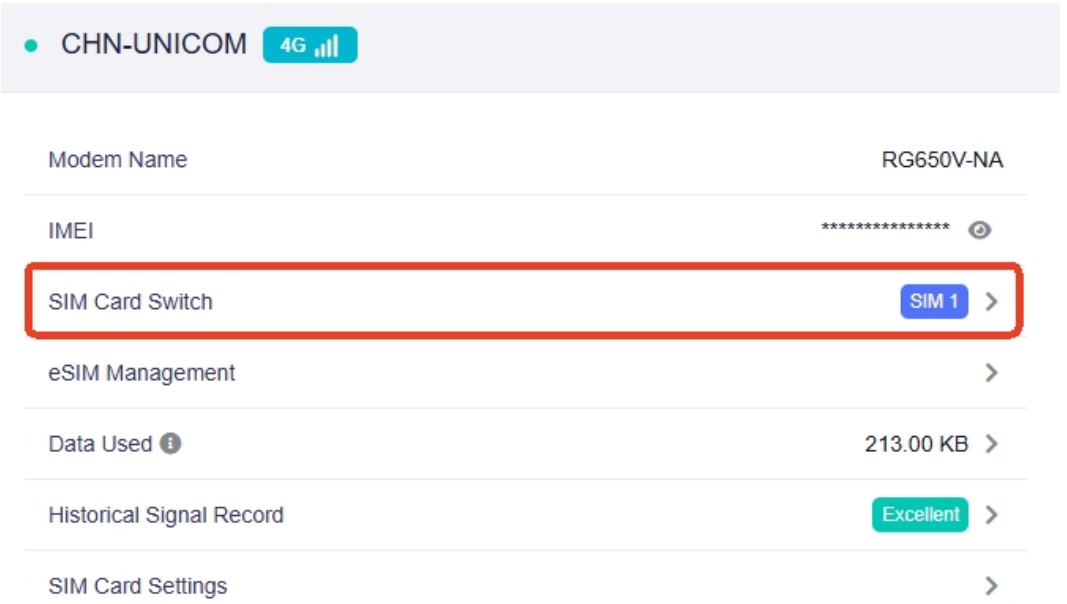
3. Klicken Sie im eingeblendeten Fenster unten auf **Add eSIM Profile**.



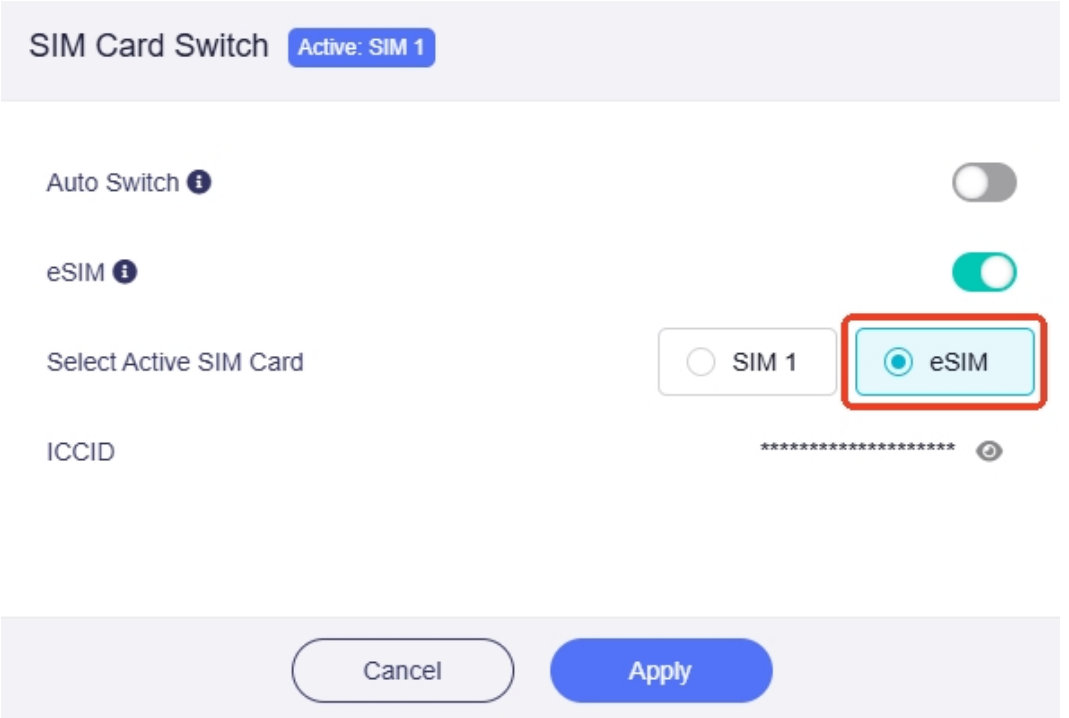
Stellen Sie vor dem Hochladen sicher, dass Ihr Gerät mit dem Internet verbunden ist. Bei einem Netzwerkfehler schlägt das Hochladen der eSIM-Konfigurationsdatei fehl.
Laden Sie Ihr eSIM-Profil per QR-Code oder Aktivierungscode hoch und klicken Sie auf **Install**. Beachten Sie, dass sich die meisten eSIM-Profile nur einmal herunterladen und hinzufügen lassen.
Tipp: Falls Sie noch kein eSIM-Profil erworben haben, können Sie eines im **eSIM Profile Recommended Store** kaufen.



4. Öffnen Sie nach dem Hochladen **Cellular** und klicken Sie auf **SIM Card Switch**.



Wählen Sie im eingeblendeten Fenster **eSIM** als aktive SIM-Karte und klicken Sie auf **Apply**.



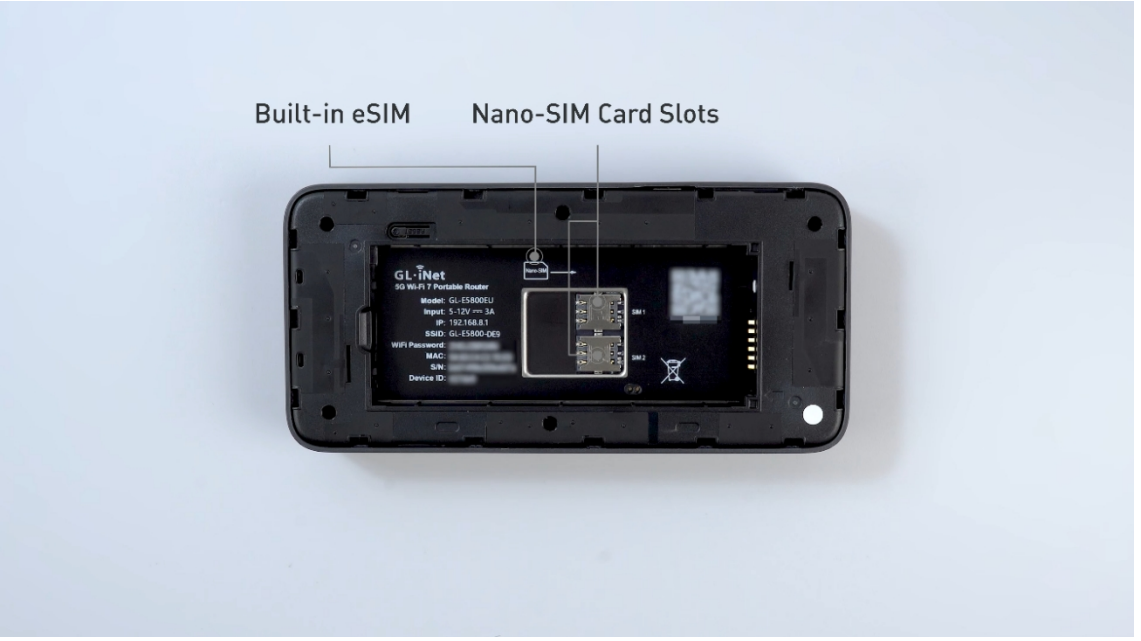
5. Der Router baut nun eine Verbindung über dieses eSIM-Profil auf. Warten Sie und prüfen Sie, ob die Verbindung erfolgreich hergestellt wurde.

Nano-SIM einrichten

1. Setzen Sie an der kleinen Aussparung unten rechts an der Rückabdeckung des Geräts an. Hebeln Sie die Abdeckung entlang der Fuge vorsichtig auf, bis ein Spalt entsteht. Öffnen Sie dann die Rückabdeckung und nehmen Sie den Akku von Mudi 7 heraus. **Warnung**: Ist der Akku aufgebläht, undicht, ungewöhnlich heiß, beschädigt oder schwer zu entnehmen, stellen Sie die Nutzung des Geräts ein und versuchen Sie nicht, den Akku herauszunehmen. Siehe Sicherheitshinweise zum Akku.



2. Setzen Sie die Nano-SIM-Karte(n) ein. Wenn Sie nur eine Karte verwenden, nutzen Sie vorzugsweise SIM 1. Setzen Sie anschließend den Akku wieder ein und bringen Sie die Abdeckung an.



3. Der Router stellt die Verbindung über die Nano-SIM-Karte automatisch her. Warten Sie und prüfen Sie, ob die Verbindung erfolgreich hergestellt wurde. Bei bestehender Verbindung erscheinen rechts oben auf dem Touchscreen die Signalbalken und der Mobilfunkstatus. Details zur Verbindung finden Sie auch in der Weboberfläche.

Hinweis:

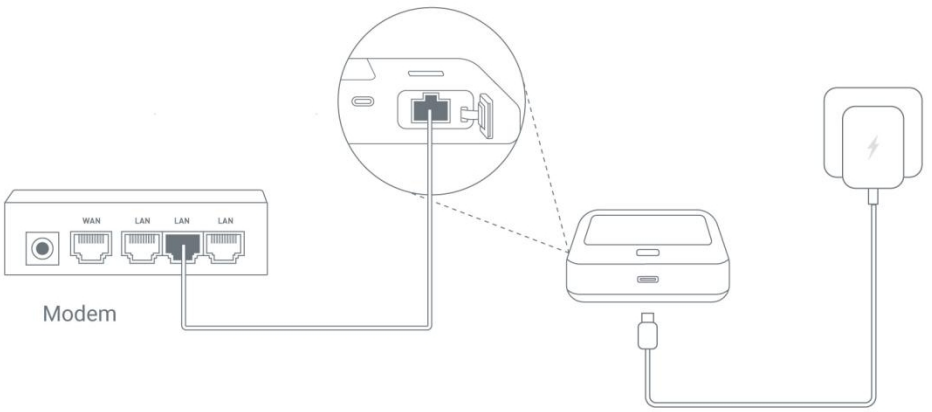
1. Die integrierte eSIM und SIM 2 schließen einander aus und können nicht gleichzeitig aktiviert werden. Die eSIM ist standardmäßig deaktiviert. Wenn Sie die eSIM aktivieren, funktioniert SIM 2 auch bei eingesetzter SIM-Karte nicht.
2. Da Mudi 7 über eine integrierte eSIM verfügt, wird eine physische SIMPoYo-eSIM-Karte auf Mudi 7 als gewöhnliche SIM-Karte ohne eSIM-Funktion erkannt.

4.2.2 Internetverbindung über Ethernetkabel

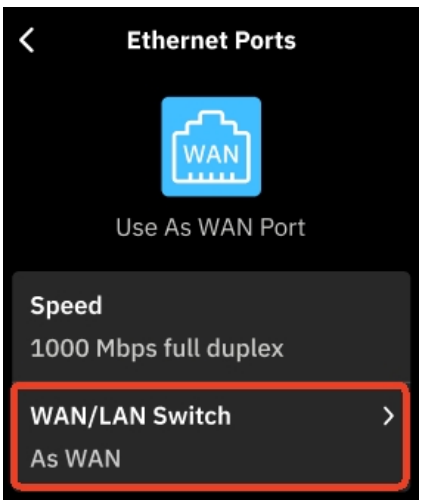
Verbinden Sie den Router per Ethernetkabel mit einem Breitbandnetz. Diese Methode bietet eine hohe Stabilität und Geschwindigkeit und eignet sich besonders für Wohnungen und Büros mit festem Breitbandanschluss.

Grundeinrichtung

1. Verbinden Sie den Ethernetanschluss von Mudi 7 per Ethernetkabel mit dem vorgeschalteten Gerät, beispielsweise einem Modem Ihres Internetanbieters, einem Hauptrouter, einem Netzwerkswitch oder einer Ethernetdose.



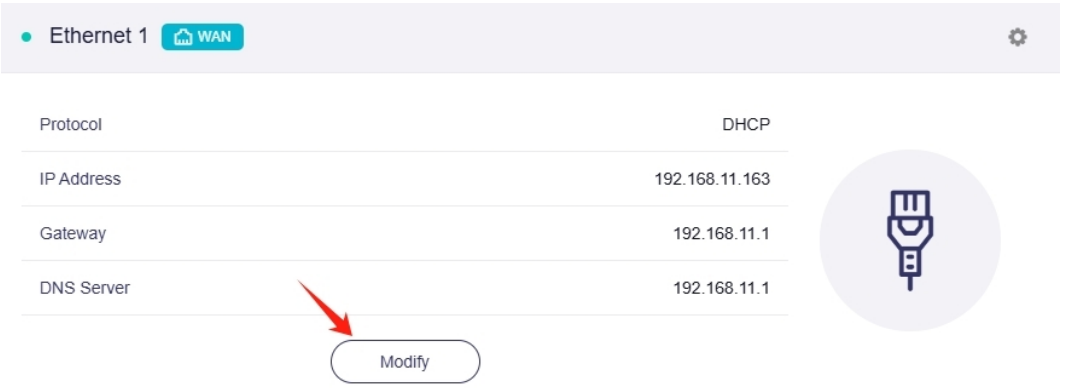
2. Öffnen Sie auf dem Touchscreen oder in der Weboberfläche **Network** > **Ethernet Ports**, stellen Sie die Anschlussfunktion auf **WAN** und klicken Sie auf **Apply**.



3. Der Router stellt die Verbindung automatisch her. Bei bestehender Verbindung erscheint rechts oben auf dem Touchscreen ein Ethernetanschlusssymbol. In der Weboberfläche können Sie zudem Verbindungsdetails prüfen und erweiterte Einstellungen vornehmen.

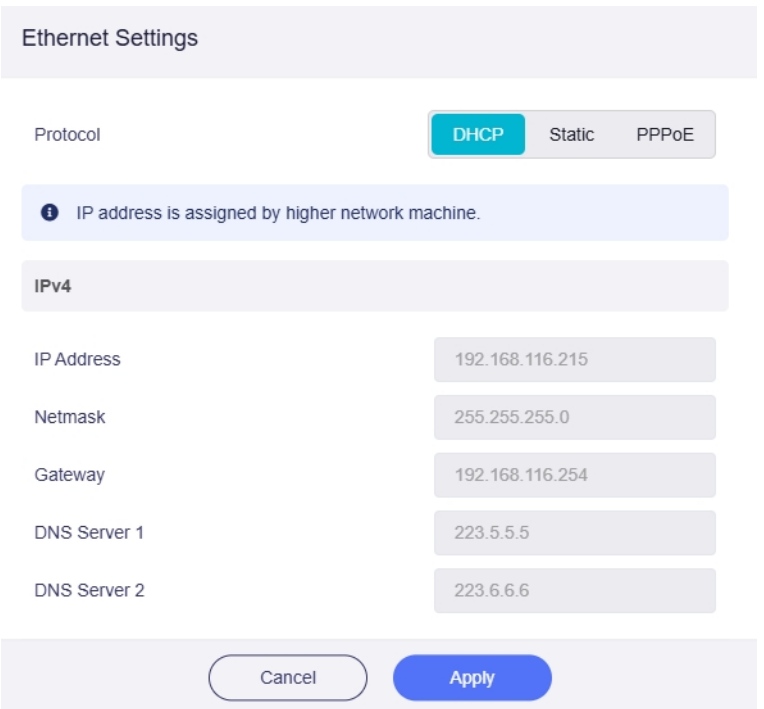
Protokoll

Für die Ethernetverbindung stehen drei Protokolle zur Verfügung: DHCP, Static und PPPoE. Klicken Sie bei Bedarf auf **Modify**, um das Protokoll zu ändern.



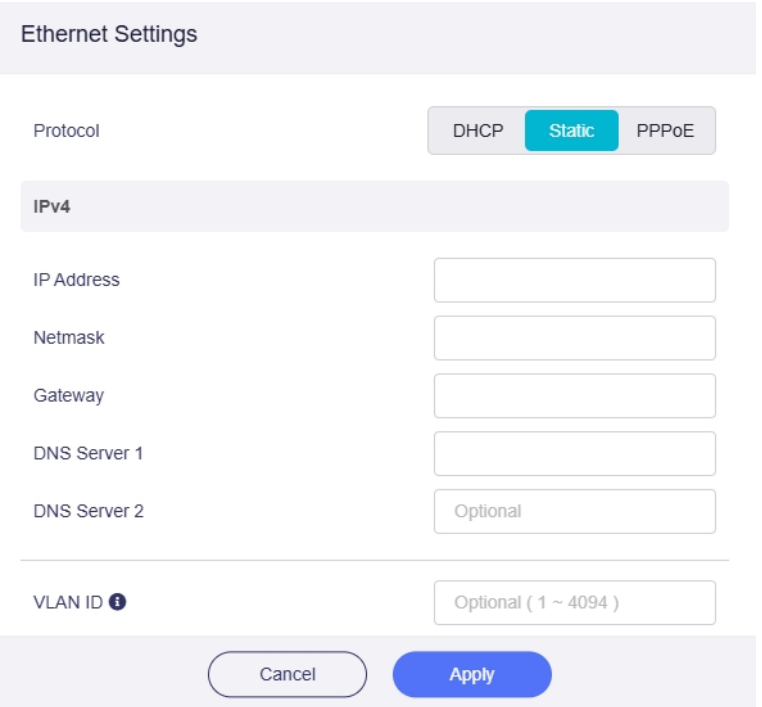
- **DHCP**

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



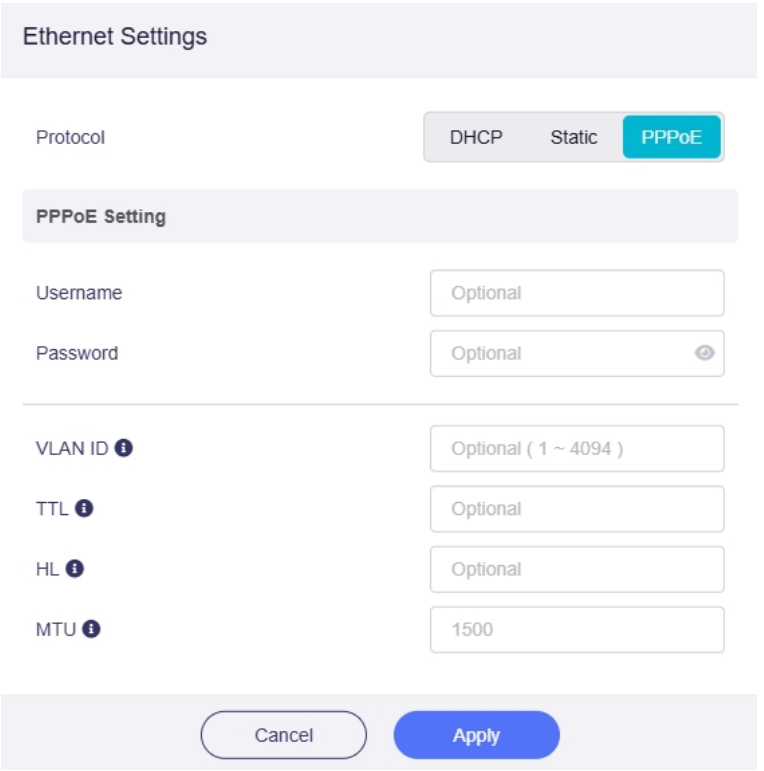
- **Statische IP-Adresse**

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



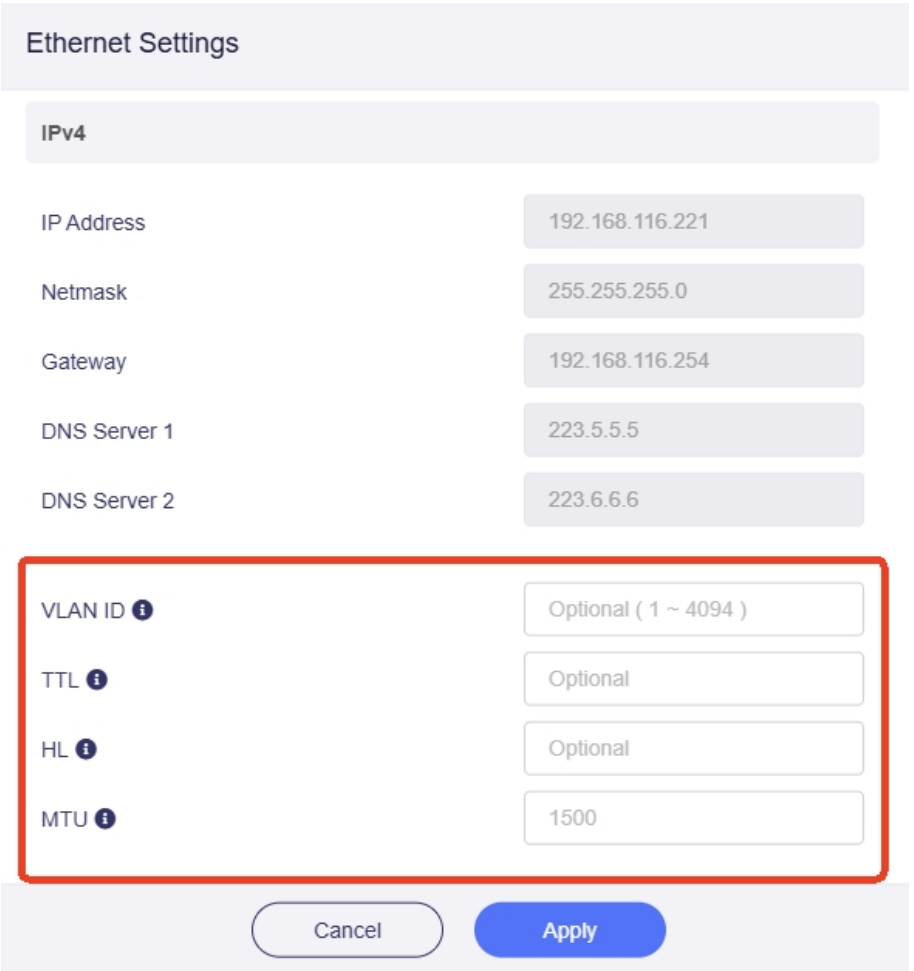
- **PPPoE**

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



Erweiterte Einstellungen

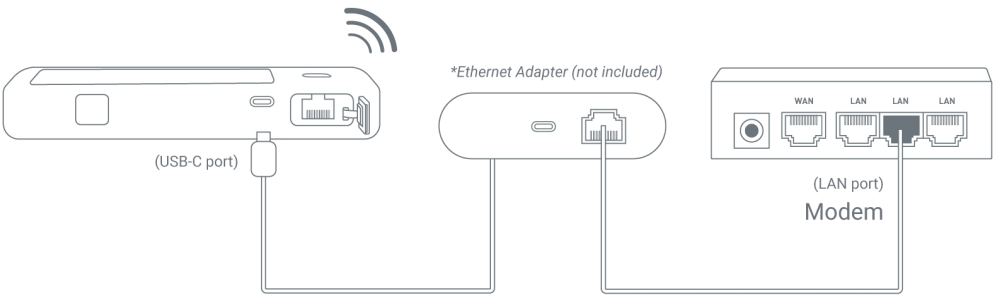
Zusätzlich zu den grundlegenden Einstellungen stehen für die drei oben genannten Protokolle optionale erweiterte Einstellungen zur Verfügung.



- **VLAN ID**: Diese Einstellung ist nur erforderlich, wenn der Server des Anbieters für die Schnittstelle eine bestimmte getaggte VLAN-ID verlangt.
- **TTL**: TTL (Time To Live) legt die maximale Lebensdauer von Paketen im Netzwerk fest. Tragen Sie den Wert gemäß den Vorgaben Ihres Anbieters ein. Um die TTL zu überschreiben oder einen anderen Wert vorzutäuschen, legen Sie hier einen festen Wert fest. Mudi 7 übernimmt den eingegebenen Wert unverändert. Die TTL-Einstellung gilt nur für IPv4.
- **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.

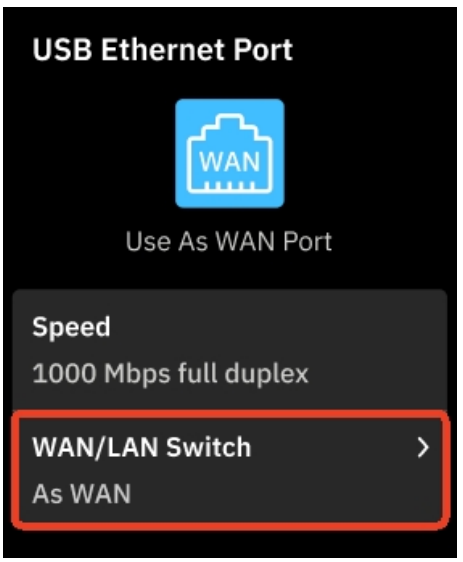
USB-Ethernet

Mudi 7 verfügt über einen **OTG-fähigen** USB-C-Anschluss. Damit können Sie einen zweiten Ethernetanschluss für zwei Ethernet-WAN-Verbindungen hinzufügen. **Hierfür benötigen Sie einen separat erhältlichen USB-C-auf-Ethernet-Adapter**.



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

1. Verbinden Sie eine vorgeschaltete Netzwerkquelle, beispielsweise ein Modem Ihres Internetanbieters, einen Netzwerkswitch oder eine Ethernet-Wanddose, über einen USB-C-auf-Ethernet-Adapter mit dem USB-C-Anschluss von Mudi 7.
2. Öffnen Sie auf dem Touchscreen oder in der Weboberfläche **Network** > **Ethernet Ports** > **USB Ethernet Port**, stellen Sie die Anschlussfunktion auf **WAN** und klicken Sie auf **Apply**.



3. Mudi 7 stellt anschließend automatisch eine Verbindung mit Ihrem Gerät her. Falls dies nicht gelingt, wiederholen Sie die obigen Schritte oder melden Sie sich an der Weboberfläche an und prüfen Sie die USB-Ethernetverbindung.
4. Bei bestehender Internetverbindung erscheinen rechts oben auf dem Touchscreen ein USB-Symbol und ein Ethernetanschlusssymbol. Details zur Verbindung finden Sie auch in der Weboberfläche.

4.2.3 Internetverbindung über ein vorhandenes WLAN

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



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

Grundeinrichtung

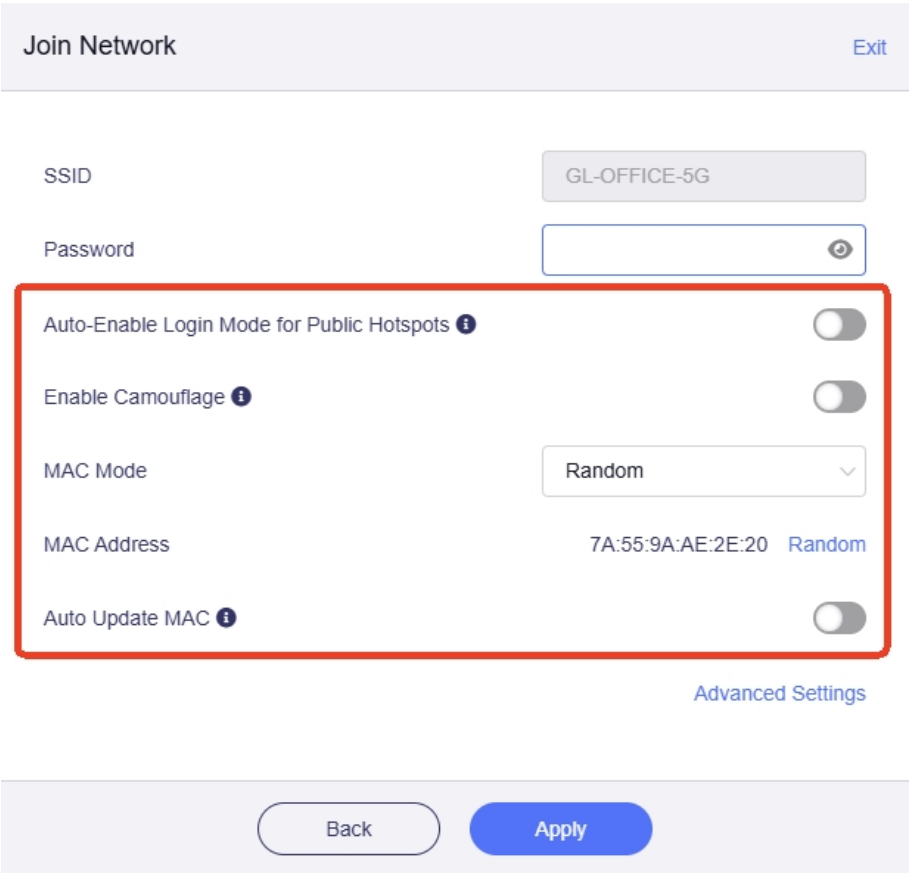
Gehen Sie wie folgt vor, um Ihren Router als Repeater mit einem vorhandenen WLAN zu verbinden.

1. Öffnen Sie auf dem Touchscreen oder in der Weboberfläche **Internet** > **Repeater** und klicken Sie auf **Connect**. Mudi 7 sucht nach verfügbaren WLAN-Netzwerken.
2. Wählen Sie das WLAN-Netzwerk, dessen Reichweite Mudi 7 erweitern soll.

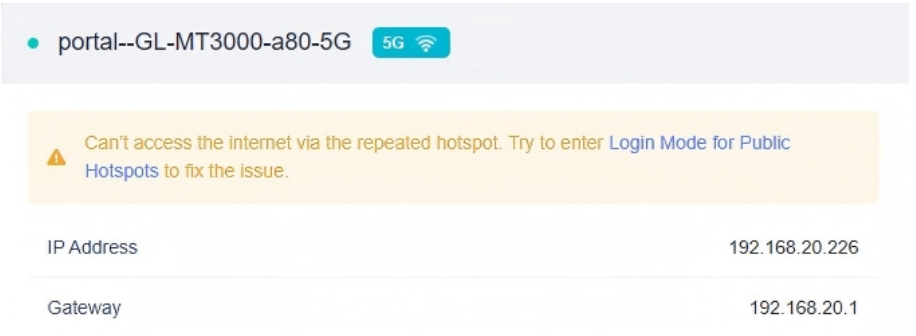
3. Geben Sie das Passwort ein und klicken Sie auf **Apply**.
4. Bei bestehender Verbindung erscheint rechts oben auf dem Touchscreen ein WLAN-Symbol. In der Weboberfläche können Sie zudem Verbindungsdetails prüfen und erweiterte Einstellungen vornehmen.

Einstellungen für öffentliche Hotspots

Wenn Sie den Router mit einem öffentlichen Hotspot mit Anmeldeseite (Captive Portal) verbinden, empfiehlt es sich, die folgenden Funktionen zu aktivieren, um die Erfolgsaussichten beim Verbindungsaufbau zu 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.

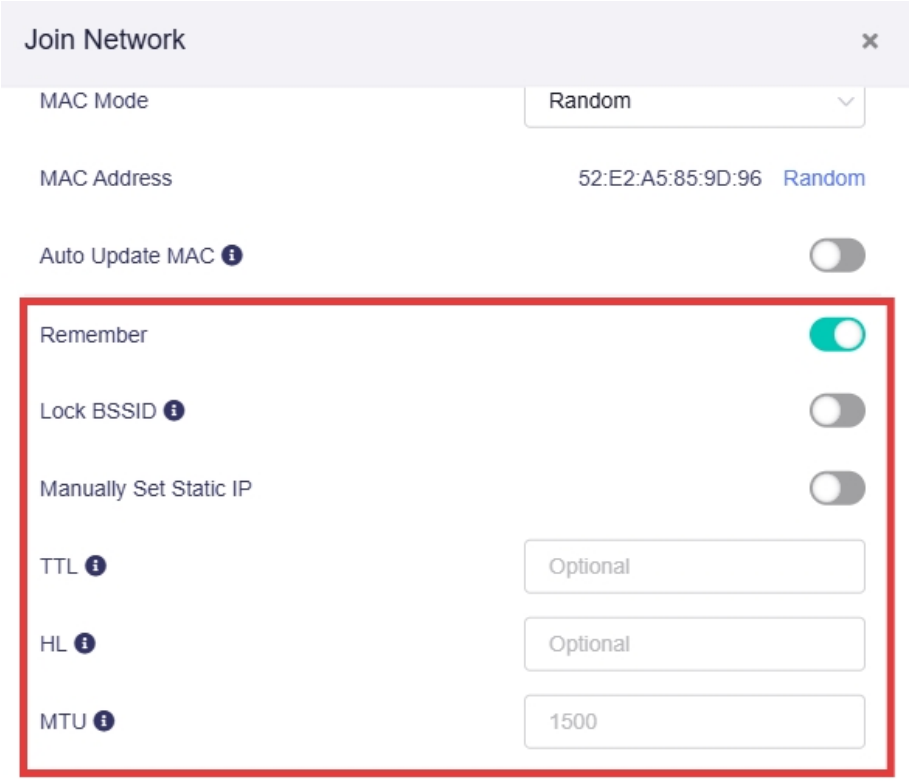


- **Tarnmodus aktivieren**
  Bei aktivierter Option gibt sich der Router als das Endgerät aus, mit dem Sie auf die Weboberfläche zugreifen, indem er dessen MAC-Adresse nachbildet.
- **MAC-Modus**
  Wählen Sie die MAC-Adresse, mit der sich der Router mit dem öffentlichen Hotspot verbindet.
  Factory: Verwendet die dem Gerät ab Werk zugewiesene MAC-Adresse.
  Clone: 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.
  Random: 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.

Erweiterte Einstellungen

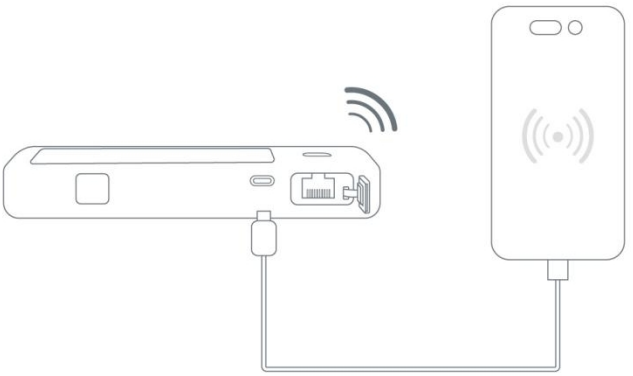
Beim Verbinden mit dem Netzwerk stehen optionale erweiterte Einstellungen zur Verfügung.



- **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 Paketen im Netzwerk fest. Tragen Sie den Wert gemäß den Vorgaben Ihres Anbieters ein. Um die TTL zu überschreiben oder einen anderen Wert vorzutäuschen, legen Sie hier einen festen Wert fest. Mudi 7 übernimmt den eingegebenen Wert unverändert. Die TTL-Einstellung 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.

4.2.4 Internetverbindung über USB-Tethering

Das Verbinden eines Smartphones mit dem Router per USB-Kabel wird als Tethering bezeichnet. Dabei wird die mobile Datenverbindung des Geräts, beispielsweise 4G oder 5G, für den Router freigegeben. Dies ist praktisch für einen vorübergehenden Internetzugang, besonders im Freien oder an Orten ohne festen Breitbandanschluss.



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

Grundeinrichtung

1. Verbinden Sie Ihr Mobilgerät, beispielsweise ein Smartphone oder einen USB-Mobilfunkstick, per USB-Kabel mit dem USB-C-Anschluss von Mudi 7.
2. Öffnen Sie auf Ihrem Mobilgerät die Einstellungen und aktivieren Sie **USB-Tethering**. Bei einem iPhone tippen Sie auf **Diesem Gerät vertrauen**, falls Sie dazu aufgefordert werden.
3. Mudi 7 stellt anschließend automatisch eine Verbindung mit Ihrem Gerät her. Falls dies nicht gelingt, wiederholen Sie die obigen Schritte oder melden Sie sich an der Weboberfläche an und prüfen Sie die Tethering-Verbindung.
4. Bei bestehender Verbindung erscheint rechts oben auf dem Touchscreen ein Kettengliedsymbol. Details zur Verbindung finden Sie auch in der Weboberfläche.

Fehlerbehebung

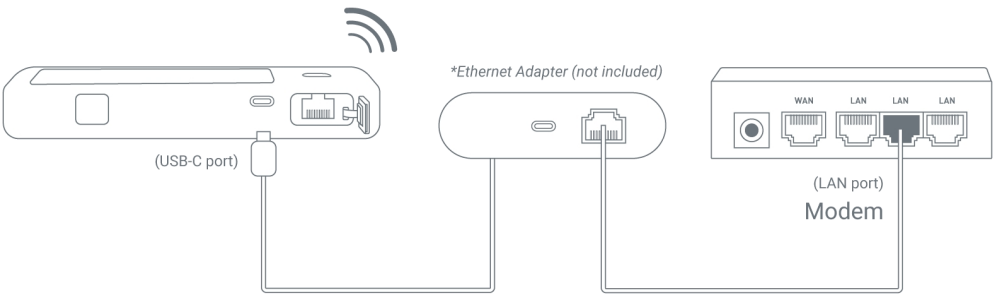
Falls die Tethering-Verbindung fehlschlägt, versuchen Sie Folgendes:

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

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

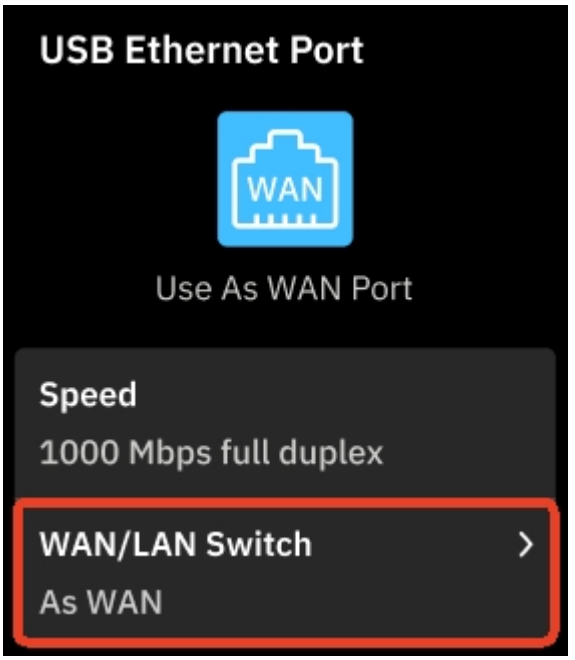
4.2.5 Internetverbindung über USB-Ethernet herstellen

USB OTG (On-The-Go) ist ein USB-Standard, mit dem kompatible Geräte wie Router zwischen der Host- und der Peripherierolle wechseln können. So sind eine direkte Datenübertragung und eine gegenseitige Stromversorgung ohne separates Hostgerät möglich. Mudi 7 verfügt über einen **OTG-fähigen USB-C-Anschluss**. Damit können Sie einen zweiten Ethernetanschluss für zwei Ethernet-WAN-Verbindungen hinzufügen. Hierfür benötigen Sie einen separat erhältlichen USB-C-auf-Ethernet-Adapter.



Gehen Sie wie folgt vor, um Mudi 7 über USB-Ethernet einzurichten.

1. Verbinden Sie eine vorgeschaltete Netzwerkquelle, beispielsweise ein Modem Ihres Internetanbieters, einen Netzwerkswitch oder eine Ethernet-Wanddose, über einen USB-C-auf-Ethernet-Adapter mit dem USB-C-Anschluss von Mudi 7.
2. Öffnen Sie auf dem Touchscreen oder in der Weboberfläche **NETWORK** -> **Ethernet Port** -> **USB Ethernet Port**, stellen Sie die Anschlussfunktion auf **WAN** und klicken Sie auf **Apply**.



3. Mudi 7 stellt anschließend automatisch eine Verbindung mit Ihrem Gerät her. Falls dies nicht gelingt, wiederholen Sie die obigen Schritte oder melden Sie sich an der Weboberfläche an und prüfen Sie auf der Seite INTERNET die **USB Ethernet**-Verbindung.
4. Bei bestehender Internetverbindung erscheinen rechts oben auf dem Touchscreen ein USB-Symbol und ein Ethernetanschlusssymbol. Details zur Verbindung finden Sie auch in der Weboberfläche.

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. Unter der Abbildung des Gerätemodells auf der Seite INTERNET leuchtet das jeweilige WLAN-Symbol.



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.



Hinweis:

1. Aufgrund von Hardwarebeschränkungen können das 5-GHz- und das 6-GHz-WLAN von Mudi 7 nicht gleichzeitig aktiviert werden. Für eine größere Gerätekompatibilität ist standardmäßig das 5-GHz-WLAN aktiviert.
2. Wenn sich Mudi 7 als Repeater mit einem vorgeschalteten WLAN verbindet, wird das vom vorgeschalteten WLAN genutzte Frequenzband auf Mudi 7 deaktiviert.
3. Wenn sich Mudi 7 als Repeater mit einem vorgeschalteten WLAN verbindet, steht das Gast-WLAN nicht zur Verfügung.

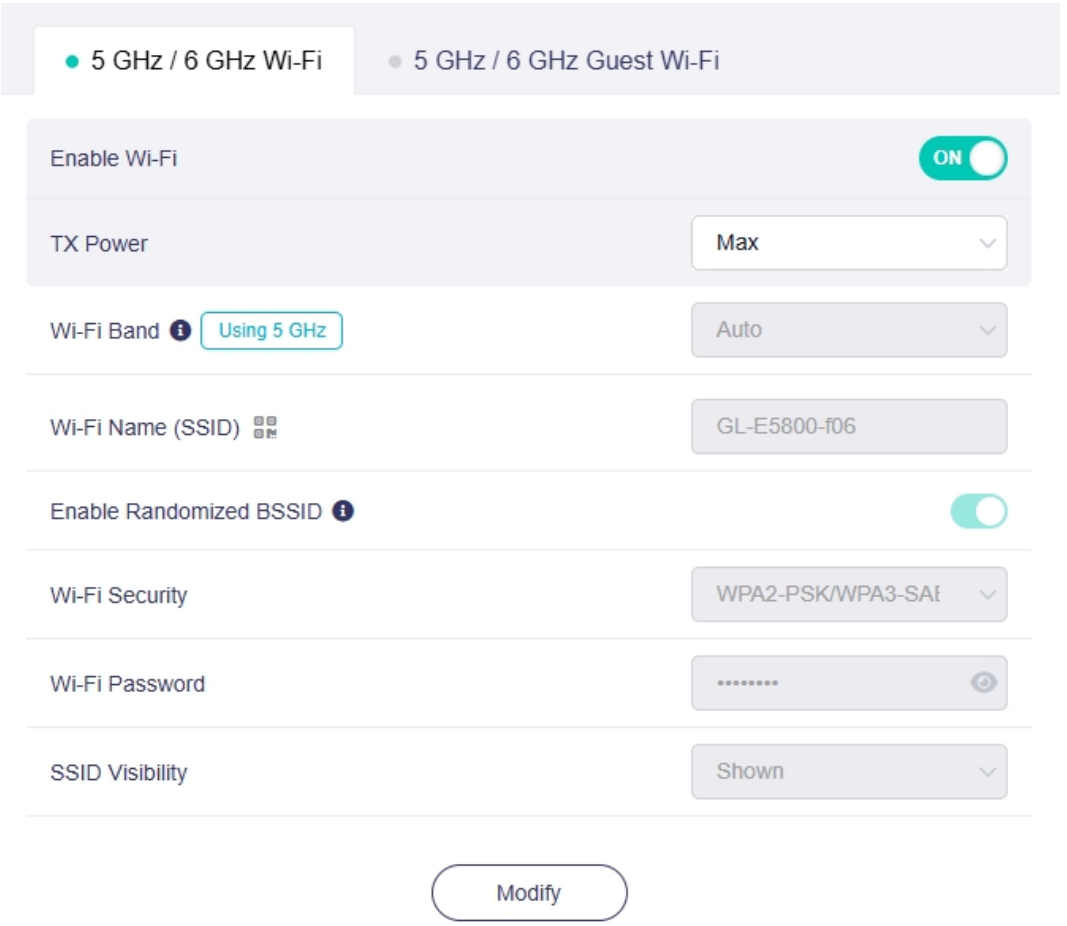
4. Gemäß den Vorschriften muss das WLAN bei der Nutzung von Mudi 7 im Freien in den Modus „Outdoor“ geschaltet werden. Dadurch kann sich die Reichweite verringern.

5.2 WLAN-Einstellungen

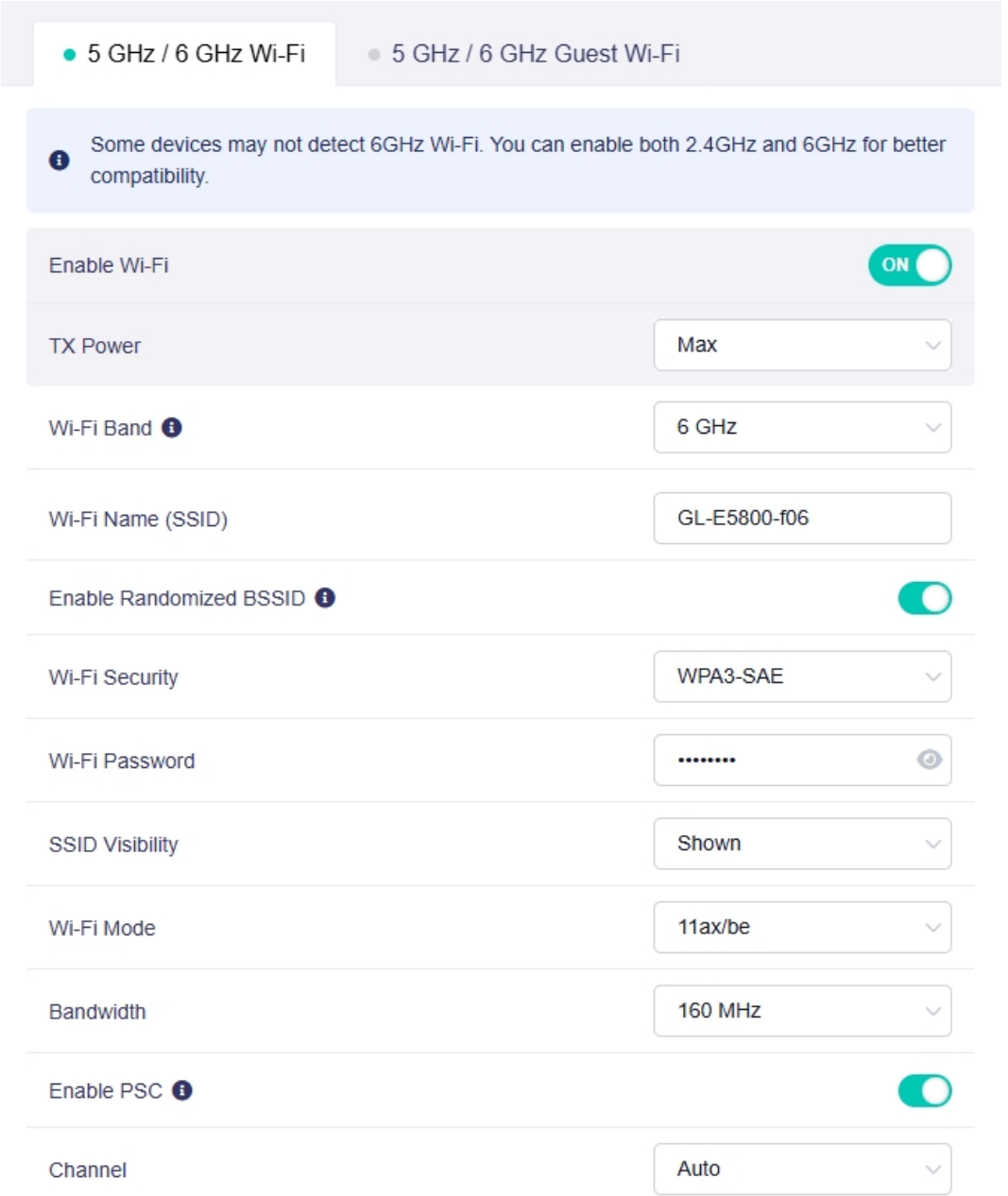
Melden Sie sich an der Weboberfläche an und öffnen Sie **WIRELESS**.
Die Seite Wireless zeigt die Einstellungen für das 2,4-GHz-, 5-GHz- und 6-GHz-WLAN des Routers.

5.2.1 5-GHz-/6-GHz-WLAN

Aufgrund von Hardwarebeschränkungen können das 5-GHz- und das 6-GHz-WLAN von Mudi 7 nicht gleichzeitig aktiviert werden. Zur einfacheren Einrichtung werden diese beiden Bänder auf der Seite Wireless als ein gemeinsames WLAN-Netzwerk dargestellt. Das WLAN-Band ist standardmäßig auf **Auto** eingestellt. Dabei wird dynamisch zwischen 5 GHz und 6 GHz gewechselt, wobei 5 GHz für eine größere Gerätekompatibilität Vorrang hat. Auf dieser Seite können Sie das WLAN ein- oder ausschalten, die Sendeleistung anpassen, eine zufällige BSSID aktivieren oder deaktivieren sowie WLAN-Namen (SSID), Sicherheit, Passwort und SSID-Sichtbarkeit festlegen. Wenn das WLAN-Band auf Auto eingestellt ist, lassen sich Kanal und Bandbreite nicht manuell konfigurieren.



Klicken Sie bei Bedarf auf **Modify** und stellen Sie das WLAN-Band auf ausschließlich 5 GHz oder ausschließlich 6 GHz ein. Sobald ein festes Band ausgewählt ist, können Sie neben den Grundeinstellungen auch WLAN-Kanal, Bandbreite und weitere zugehörige Parameter anpassen.



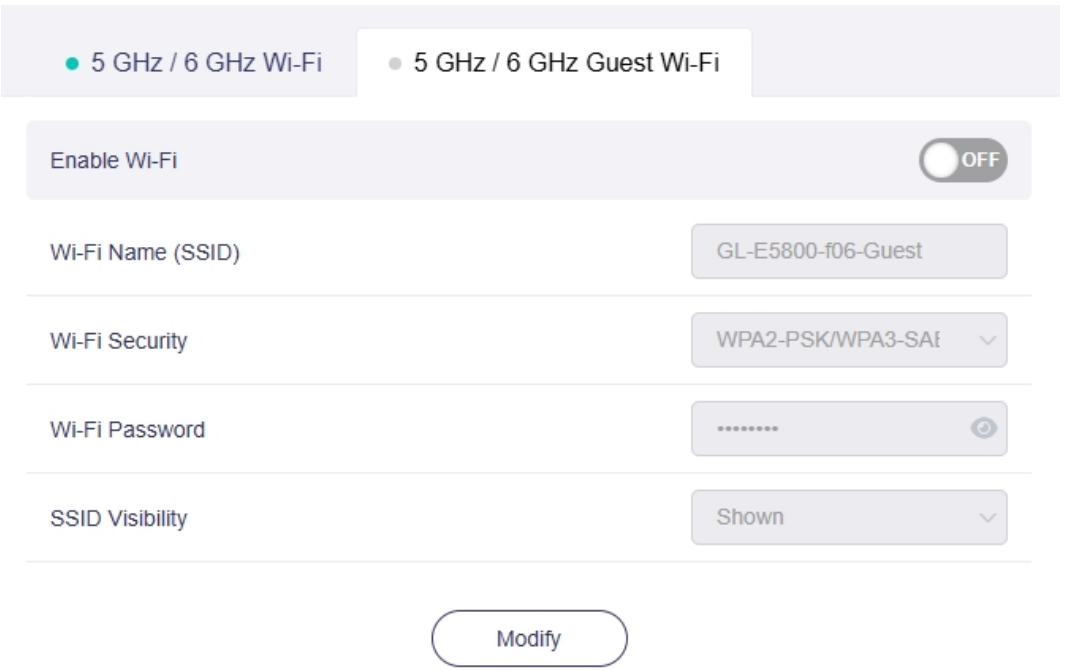
Hinweis:

1. Einige Geräte unterstützen kein 6-GHz-WLAN. Für eine größere Gerätekompatibilität können Sie das 2,4-GHz- und das 6-GHz-Band gleichzeitig aktivieren.
2. **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.

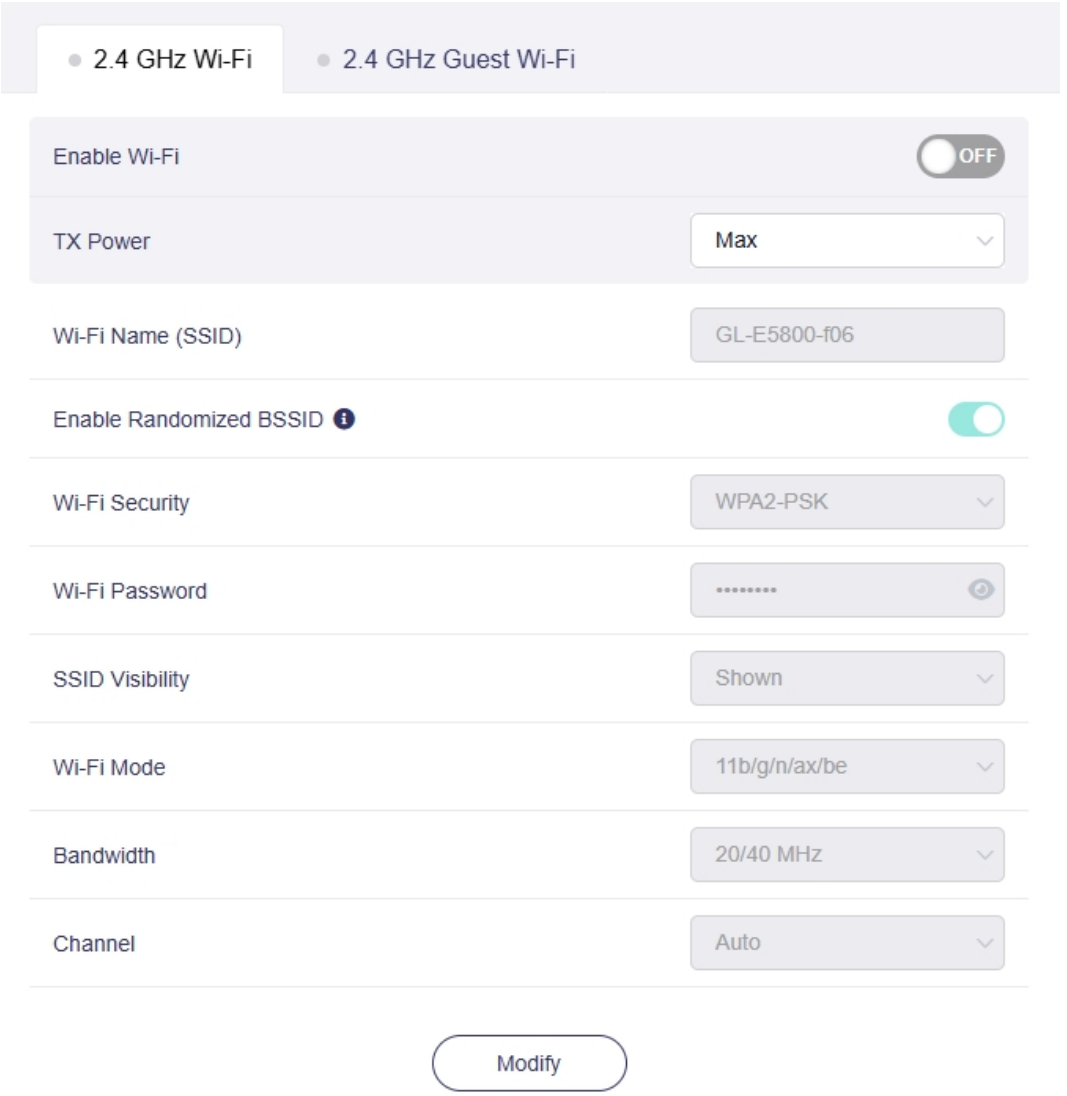
3. Die Einstellungen **Bandwidth** und **Channel** lassen sich nicht ändern, wenn der Router als Repeater eingerichtet ist, da sie vom übergeordneten WLAN übernommen werden.
4. Wenn das 5-GHz-WLAN aktiviert und **Bandwidth** auf **160 MHz** eingestellt ist, verwendet das WLAN standardmäßig einen DFS-Kanal. Dies gilt auch dann, wenn Sie manuell einen Kanal ohne DFS wählen oder den Kanal auf Auto einstellen.
5. Bei aktiviertem 6-GHz-WLAN ist **PSC** (Preferred Scanning Channel) standardmäßig eingeschaltet, um hochwertige Kanäle vorzuhalten und stabile Verbindungen für 6-GHz-Geräte sicherzustellen.

Für das 5-GHz-/6-GHz-Gast-WLAN stehen vereinfachte Einstellungen zur Verfügung: WLAN ein- oder ausschalten sowie WLAN-Namen (SSID), Sicherheit, Passwort und SSID-Sichtbarkeit festlegen.



5.2.2 2,4-GHz-WLAN

Für das 2,4-GHz-Haupt-WLAN können Sie das WLAN ein- oder ausschalten, die Sendeleistung festlegen, eine zufällige BSSID aktivieren oder deaktivieren sowie WLAN-Namen (SSID), Sicherheit, Passwort, SSID-Sichtbarkeit, WLAN-Modus (Standard), Bandbreite und Kanal einstellen.



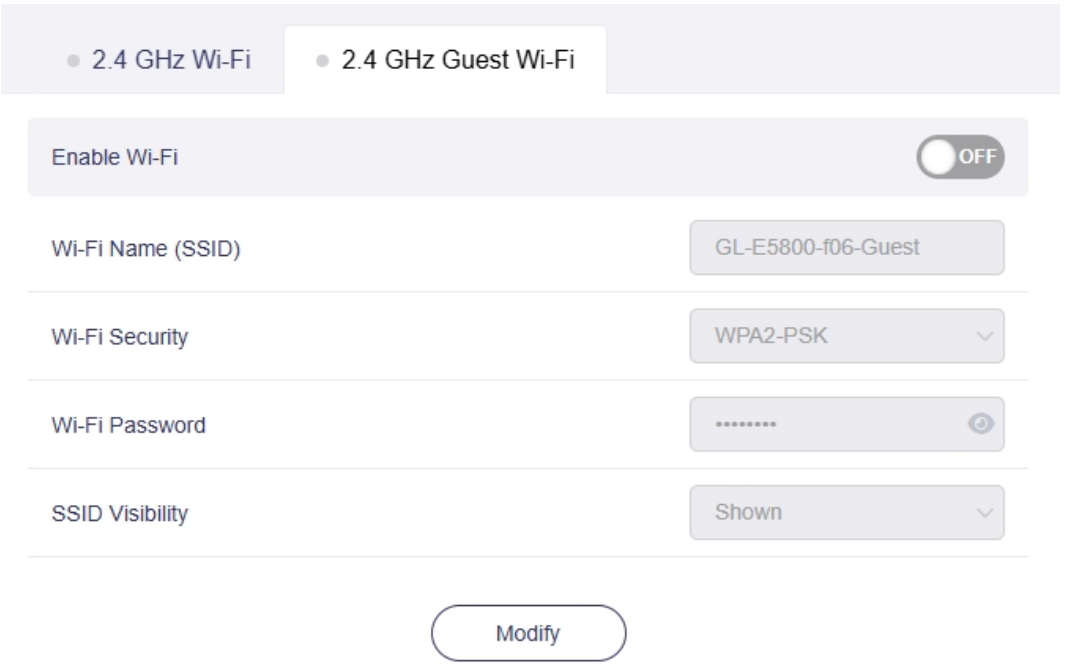
Hinweis:

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-Gast-WLAN können Sie das WLAN ein- oder ausschalten sowie WLAN-Namen (SSID), Sicherheit, Passwort und SSID-Sichtbarkeit festlegen.



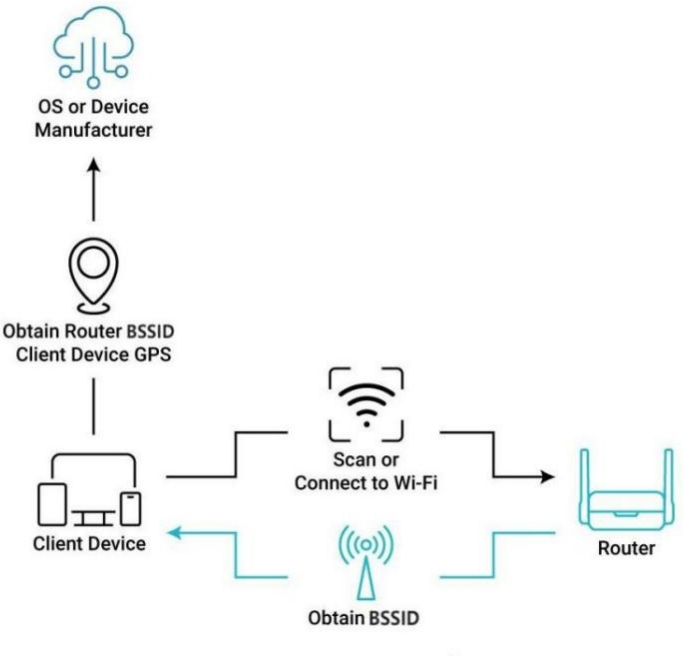
5.2.3 Zufällige BSSID

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.

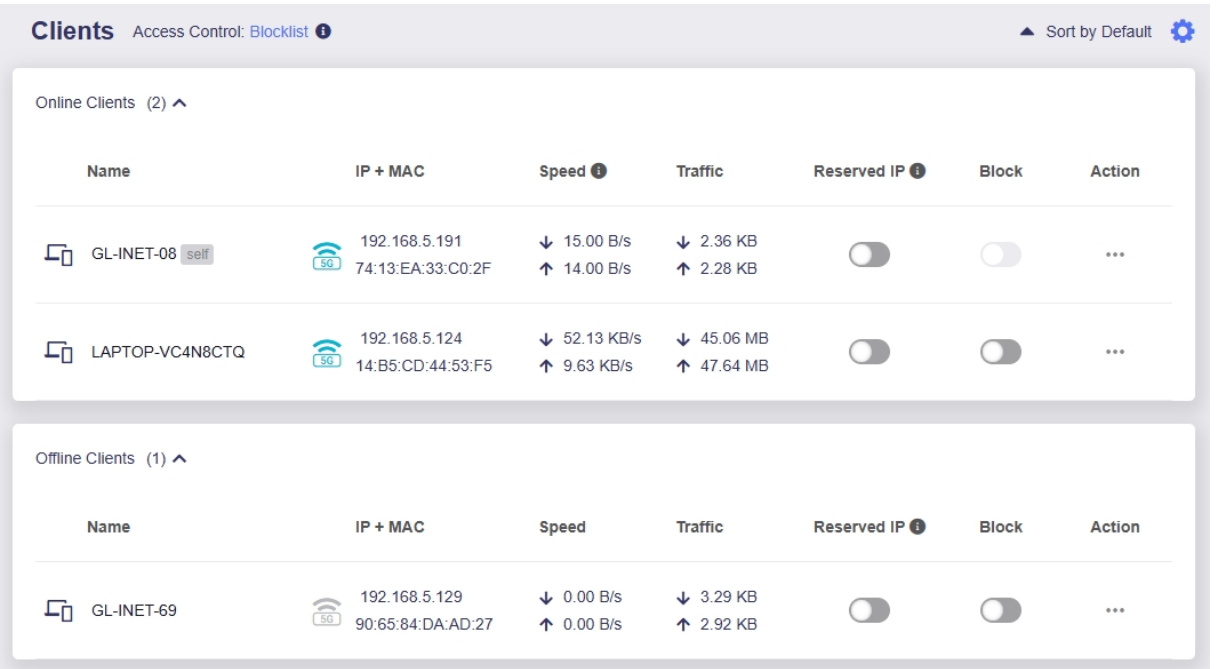
Kapitel 6

Verbundene Geräte

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

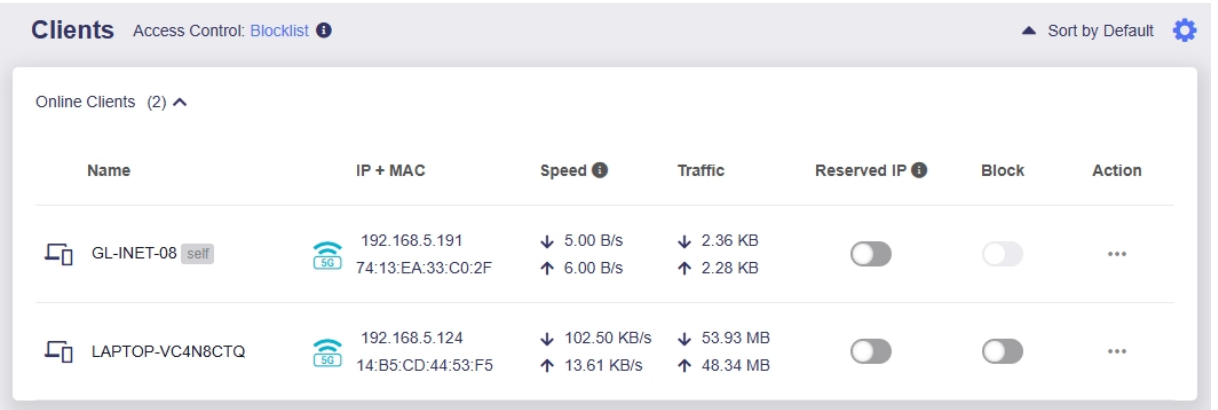
Melden Sie sich an der Weboberfläche an und öffnen Sie **CLIENTS**.

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



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

6.1 Gerätedetails



1. **Gerätename**

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

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

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



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

3. **Geschwindigkeit**

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

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

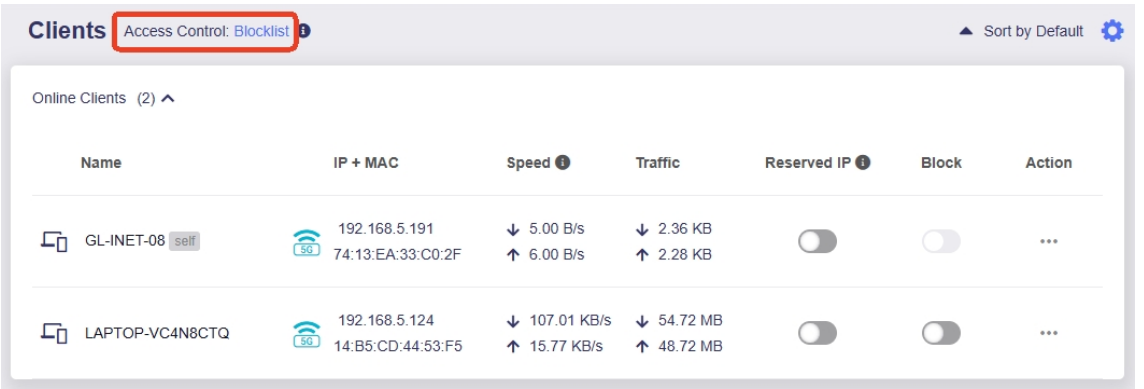
5. **IP-Adresse reservieren**

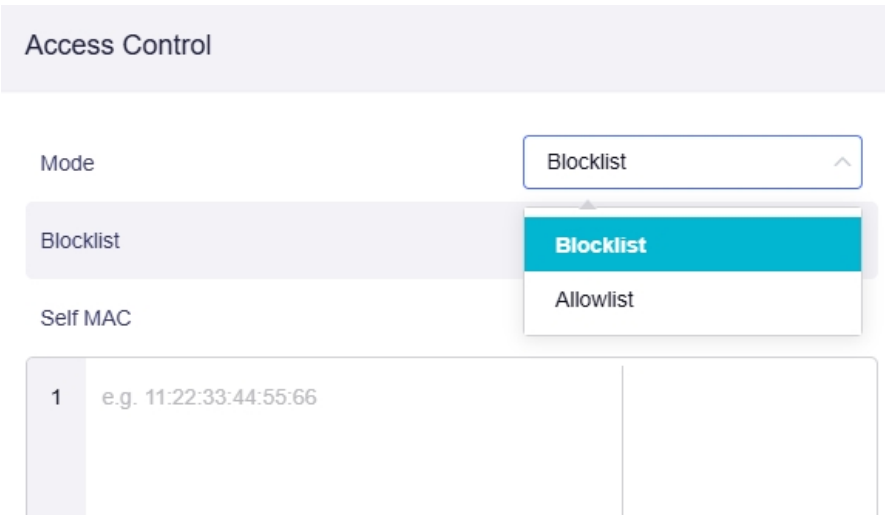
   In der fünften Spalte können Sie mit einem Klick eine IP-Adresse für ein verbundenes Gerät reservieren. Wenn Sie einem Endgerät im lokalen Netzwerk eine reservierte IP-Adresse zuweisen, erhält es bei jeder Verbindung mit dem Router dieselbe IP-Adresse.

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 eine Freigabeliste (Allowlist) wechseln.





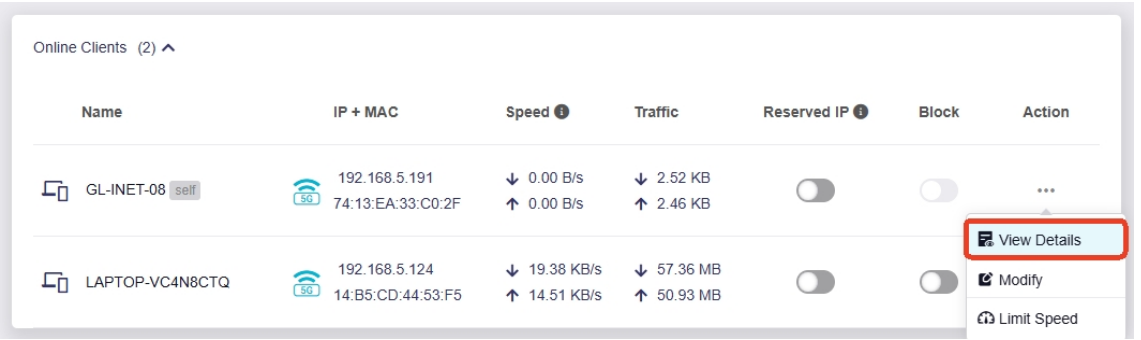
- **Blacklist**: Geräte, deren MAC-Adressen auf der Sperrliste stehen, dürfen sich nicht mit diesem Router verbinden. Die Sperre basiert auf der MAC-Adresse des Geräts. Verwendet ein gesperrtes Gerät beim nächsten Verbindungsversuch eine andere MAC-Adresse, kann es sich dennoch verbinden.

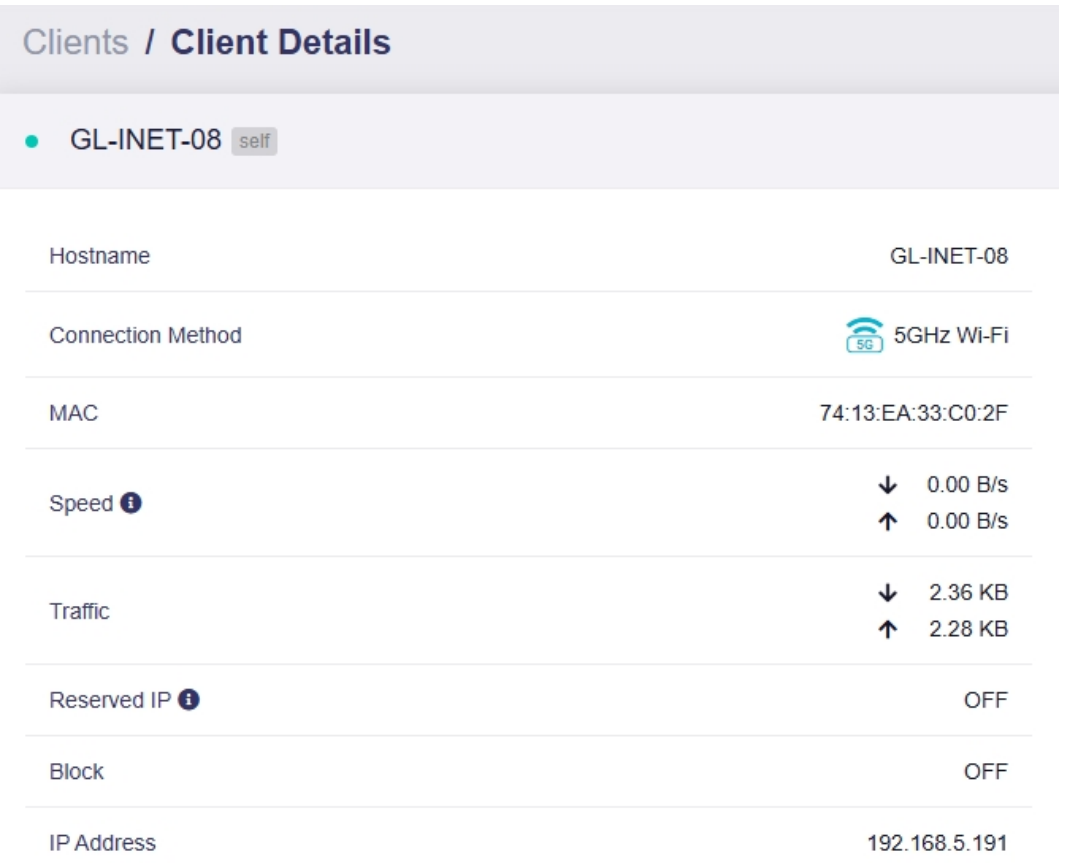
- **Allowlist**: Nur Geräte mit den festgelegten MAC-Adressen dürfen sich mit dem Router verbinden. Dies eignet sich für IoT-Geräte und die Verwaltung von Unternehmensnetzwerken.

6.2 Aktionen

1. **Details anzeigen**

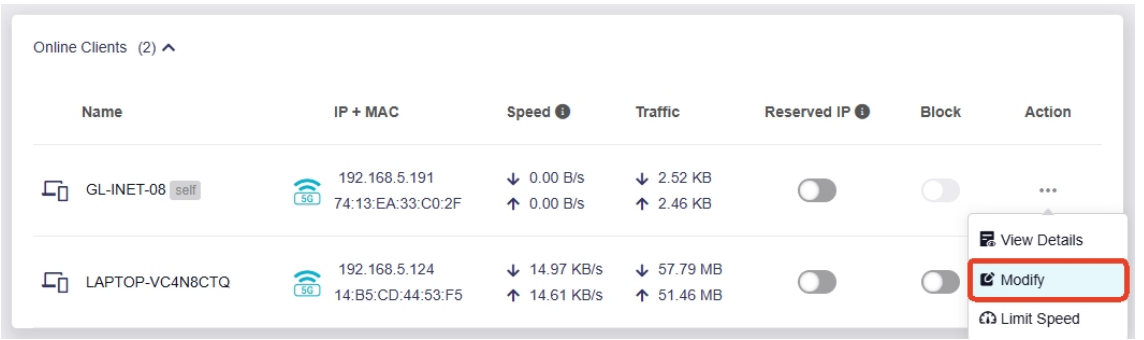
   Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Dropdown-Menü **View Details**, um die Gerätedetails auf einer eigenen Seite anzuzeigen.

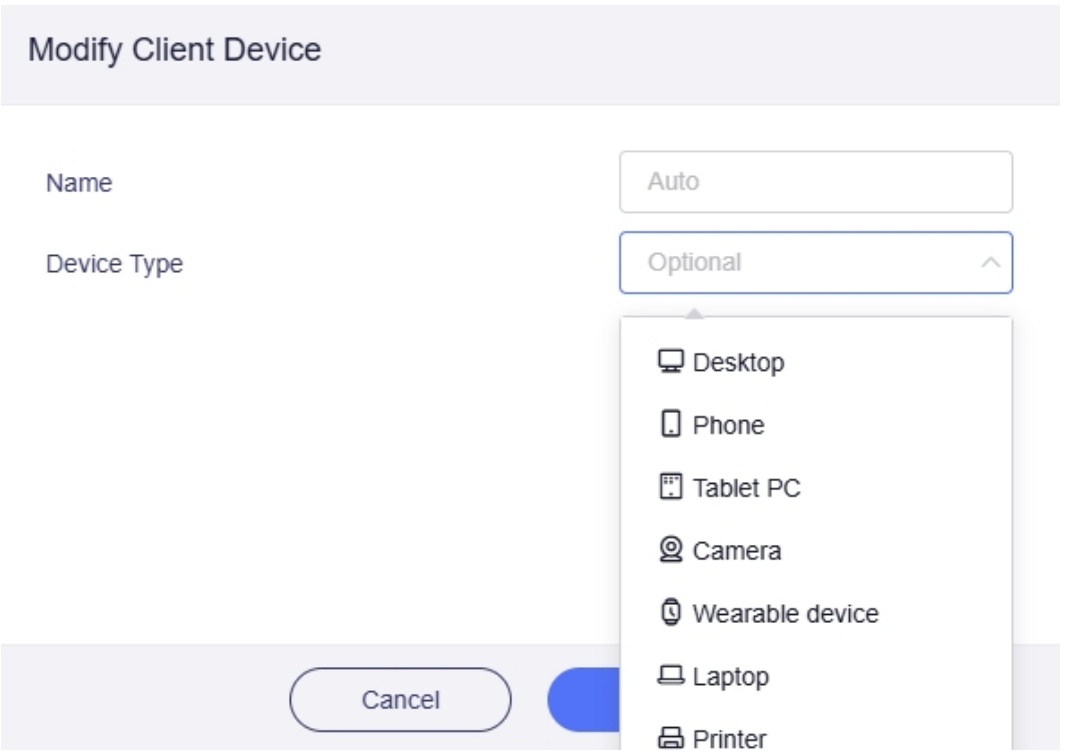




2. **Gerät bearbeiten**

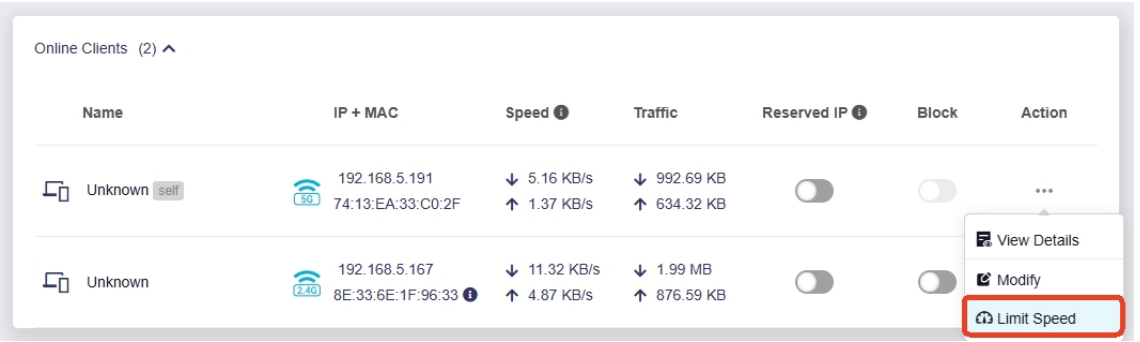
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Modify**, um den Gerätenamen und -typ zu ändern.



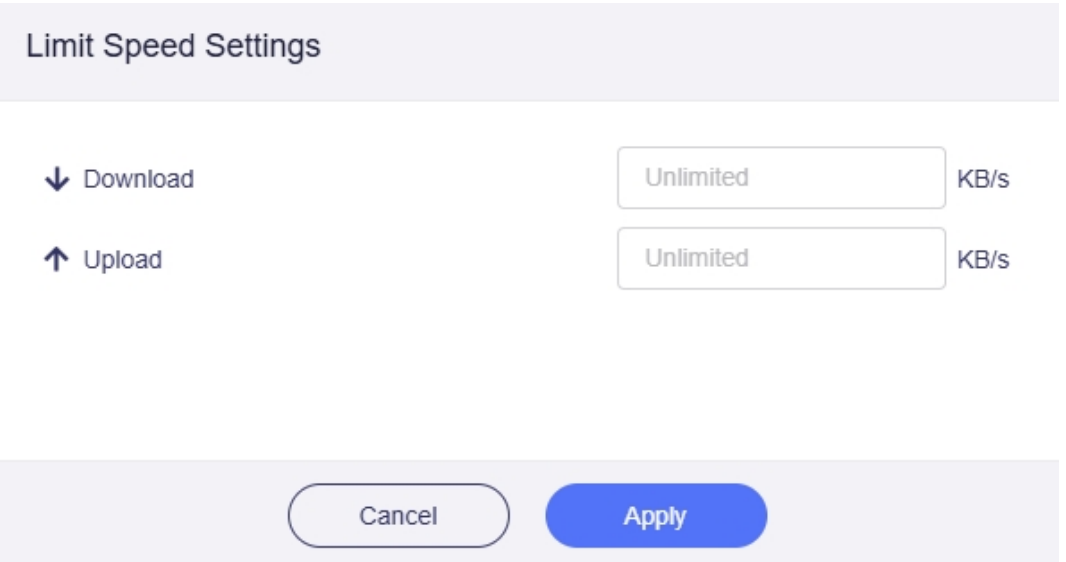


3. **Geschwindigkeit begrenzen**

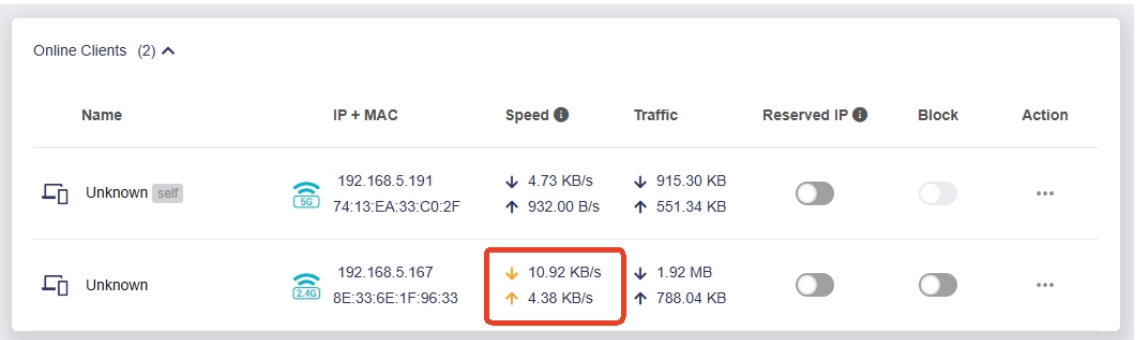
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Limit Speed**.



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



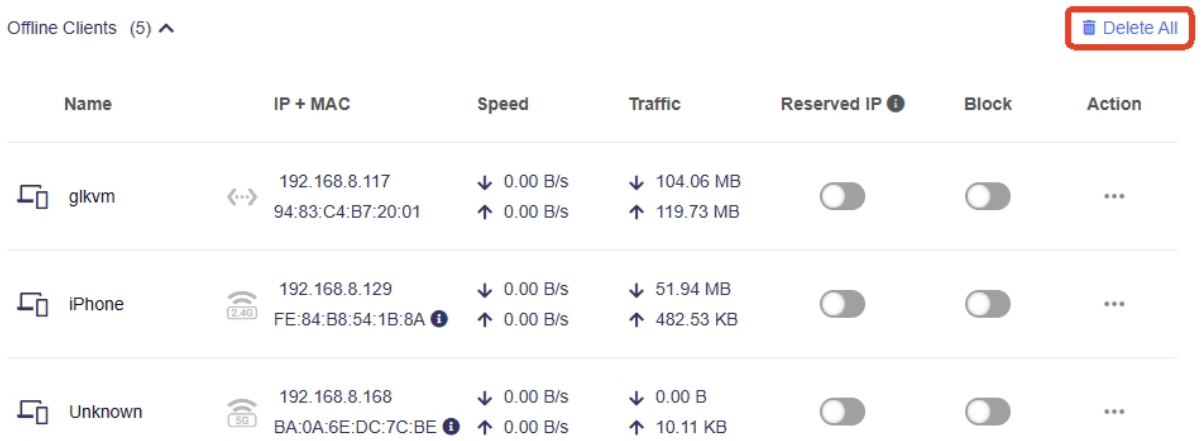
Bei Geräten mit aktivierter Geschwindigkeitsbegrenzung werden die Pfeile für die Upload- und Downloadgeschwindigkeit gelb angezeigt.



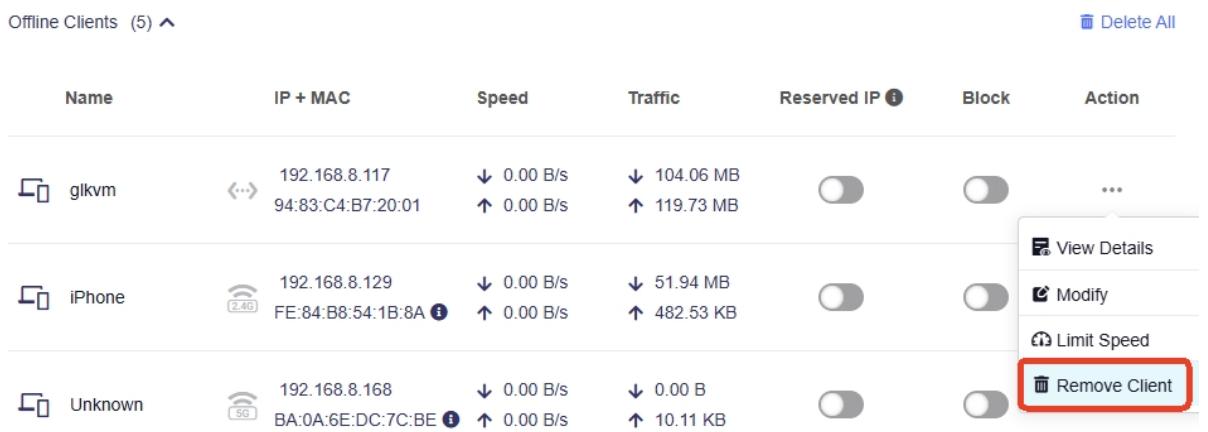
Tipp: Falls die Option Limit Speed fehlt, öffnen Sie **NETWORK** > **Network Acceleration** und deaktivieren Sie die Netzwerkbeschleunigung. Danach ist die Option Limit Speed verfügbar.

6.3 Geräte entfernen

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

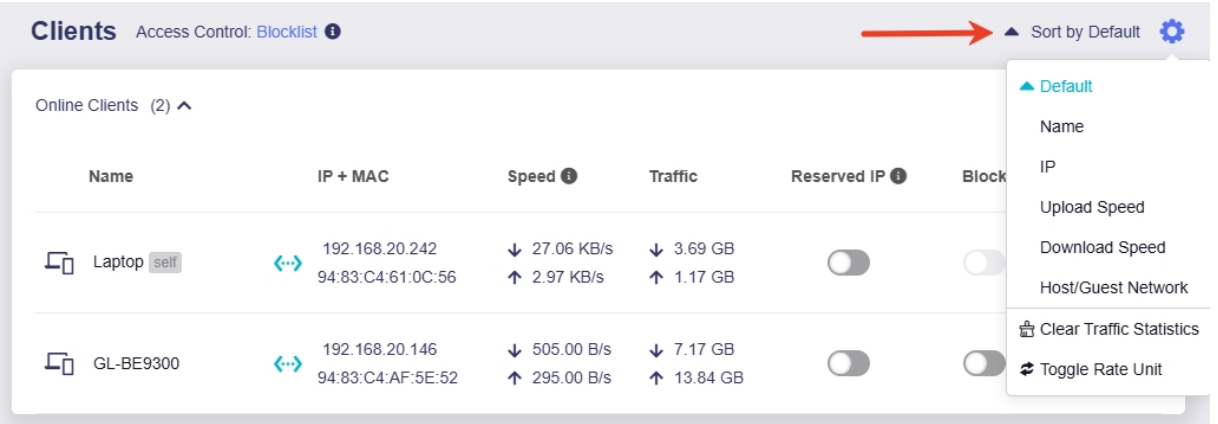


Um ein einzelnes Gerät zu entfernen, klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Remove Client**.



6.4 Sortierung

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



Standardmäßig gilt folgende 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.

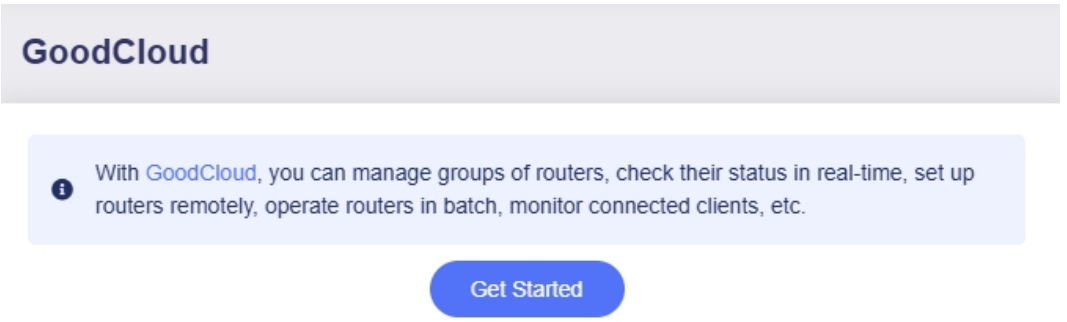
Mit GoodCloud können Sie:

- 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

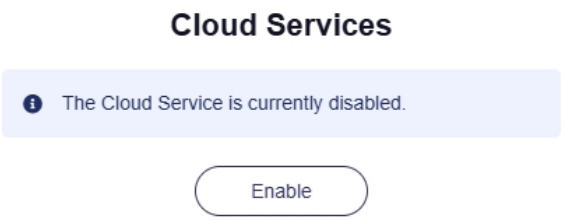
Einige Funktionen sind im Enterprise-Tarif und im VAR-Tarif (Value Added Reseller) verfügbar. Weitere Informationen finden Sie hier.

7.1.1 GoodCloud aktivieren

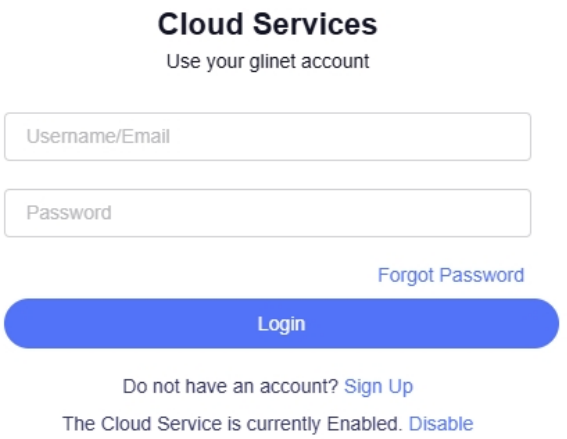
1. Melden Sie sich an der Weboberfläche Ihres Routers an, öffnen Sie **CLOUD SERVICE** > **GoodCloud** und klicken Sie auf **Get Started.**



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.

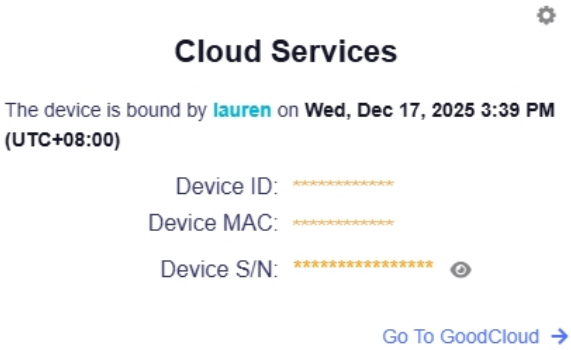


Tipps:

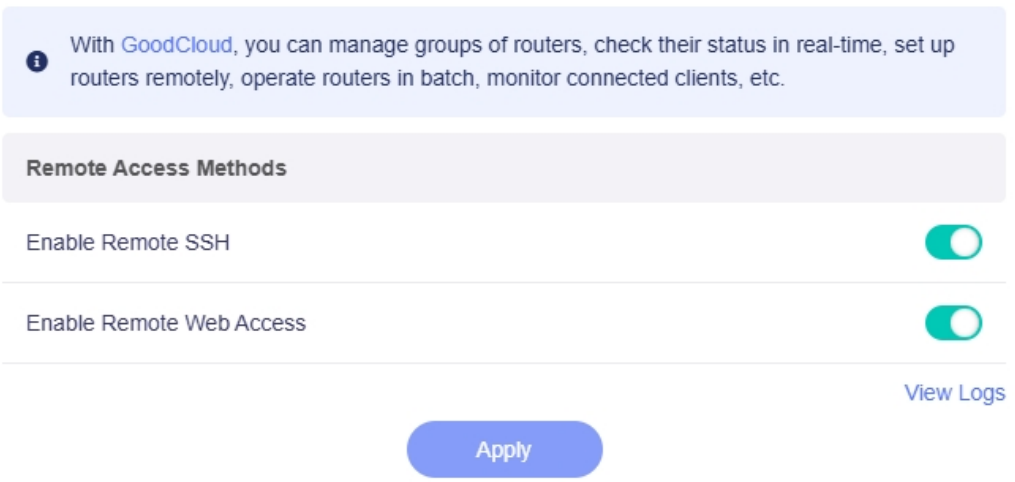
- Die Schritte zur Verknüpfung mit GoodCloud unterscheiden sich je nach Firmwareversion.

- Falls Sie bei der Registrierung keine Bestätigungs-E-Mail erhalten, prüfen Sie Ihren Spamordner oder versuchen Sie es später erneut. Bei Fragen erreichen Sie uns unter support@gl-inet.c om.

4. Nach erfolgreicher Verknüpfung werden oben rechts in der Weboberfläche die Angaben zum verknüpften Gerät angezeigt, darunter Konto, Verknüpfungsdatum, Device ID, Device MAC und Device S/N.



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

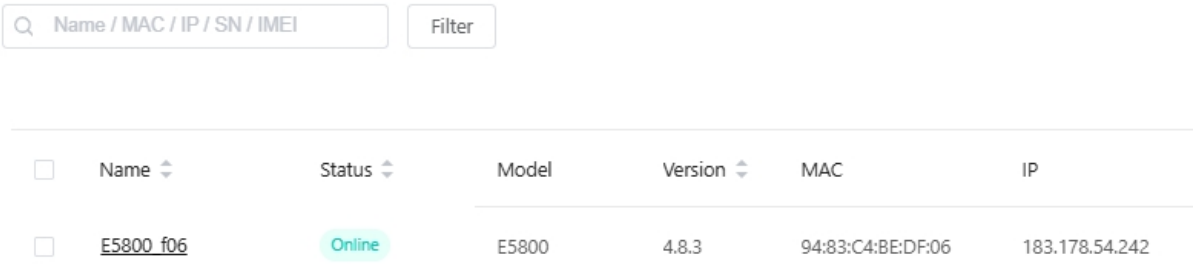


- **Remote SSH**: Fernzugriff auf das Terminal des Routers über GoodCloud per SSH.
- **Remote Web Access**: Fernzugriff auf die Weboberfläche des Routers über GoodCloud per HTTP/HTTPS.
- **View Logs**: Öffnet die Protokollseite und zeigt das Cloud-Protokoll an.

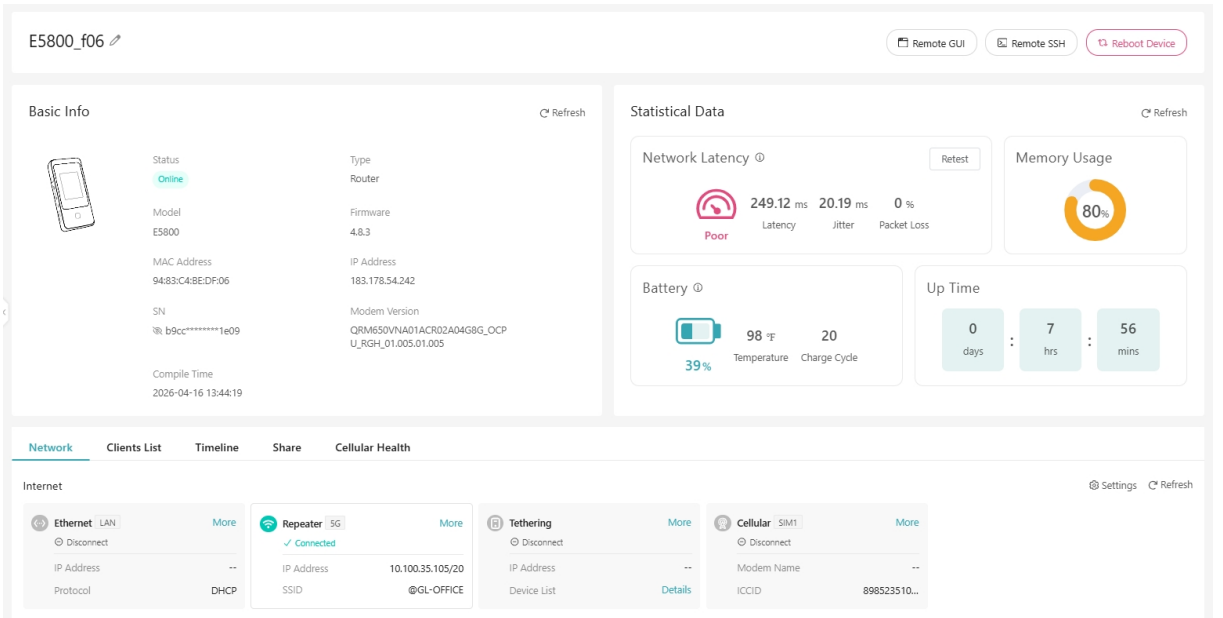
7.1.2 Router verwalten

Gerätedetails prüfen

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

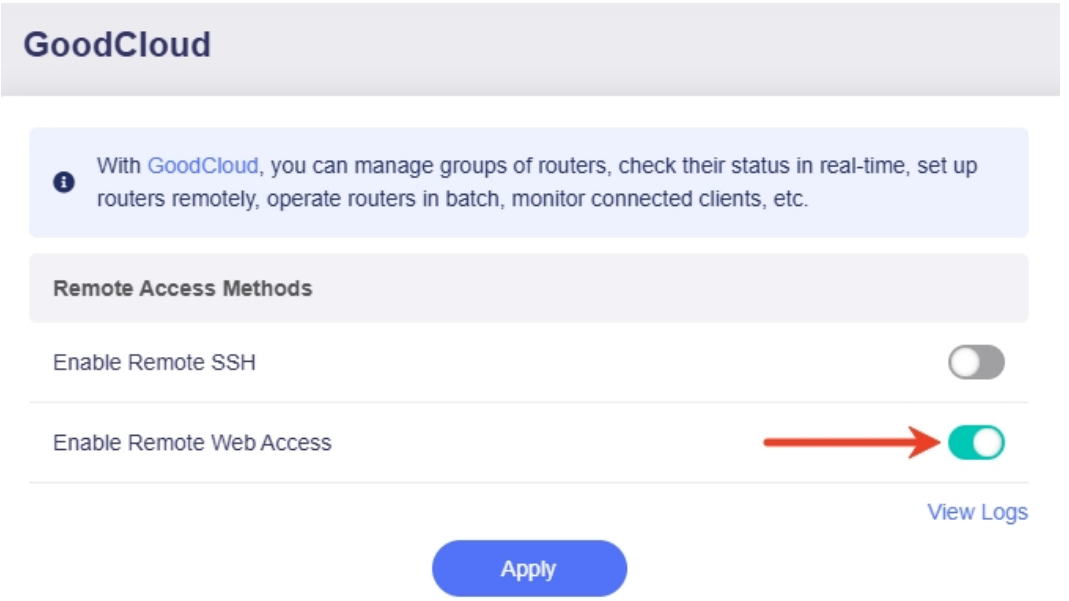


Klicken Sie auf den Gerätenamen, um die Detailseite zu öffnen. Diese enthält grundlegende Informationen, Statistiken, eine Netzwerkübersicht, die Geräteliste und eine Zeitleiste. Außerdem können Sie erweiterte Aktionen ausführen, etwa aus der Ferne auf den Router zugreifen oder ihn neu starten.

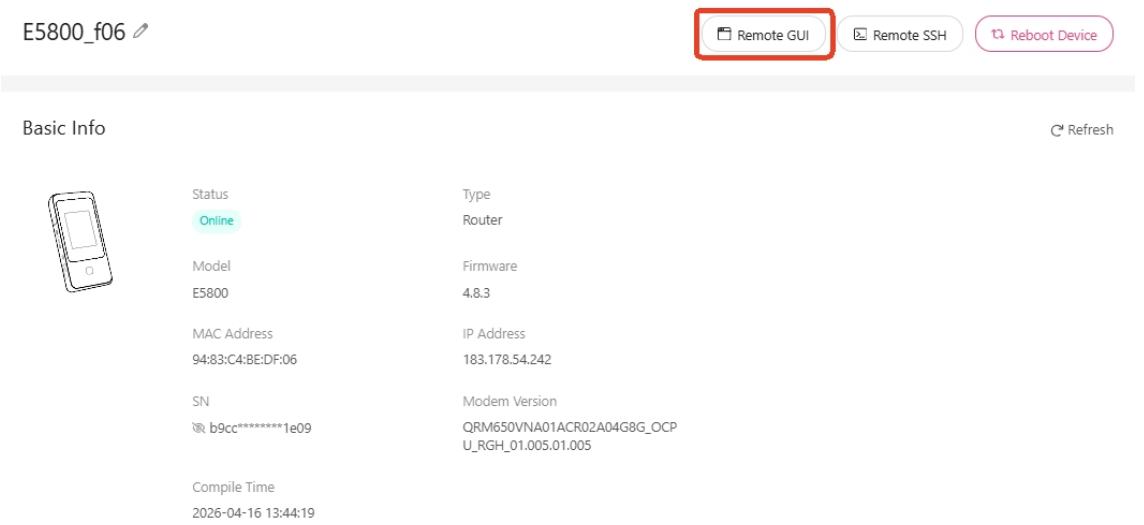


Fernzugriff auf die Weboberfläche

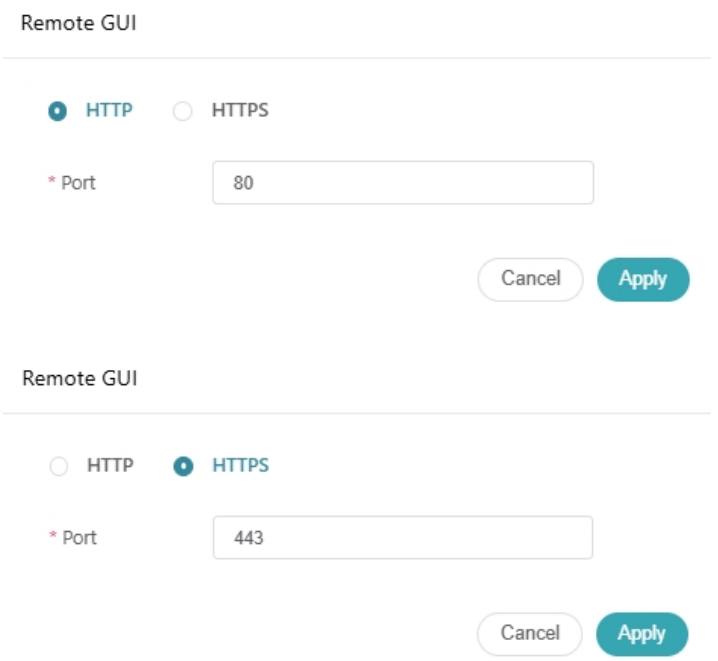
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote Web Access** und klicken Sie auf **Apply**.



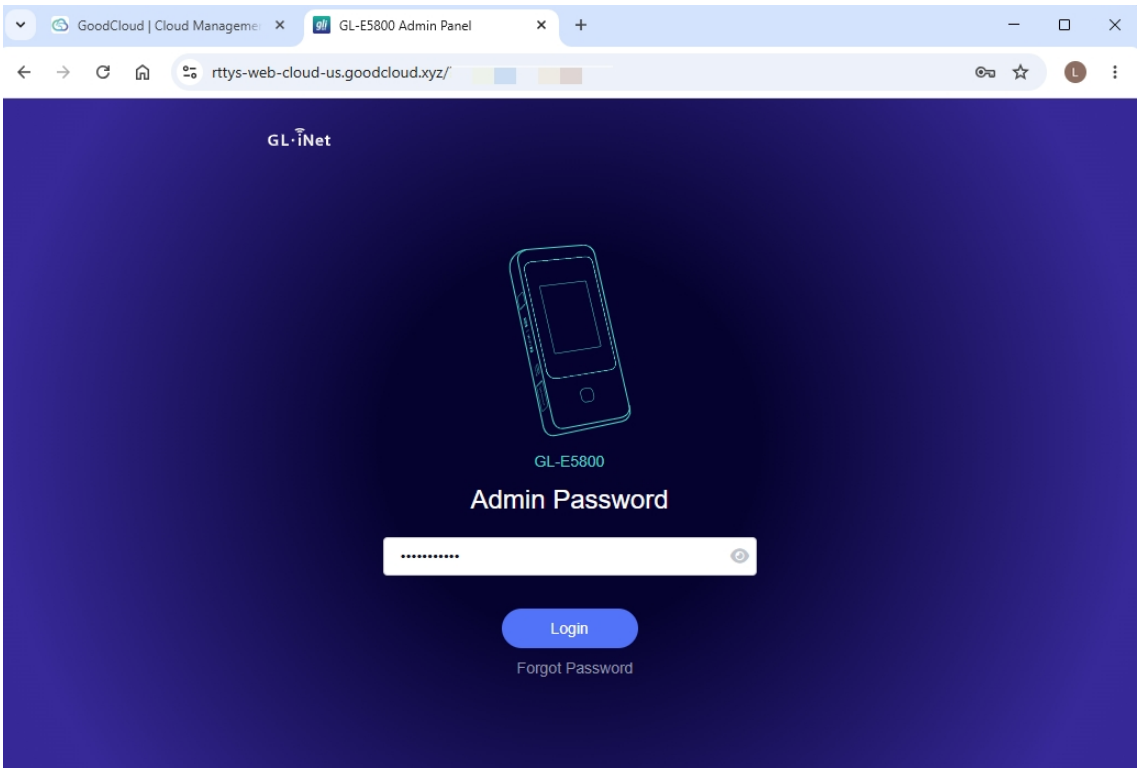
2. Melden Sie sich bei GoodCloud an und öffnen Sie **Device** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote GUI**.



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

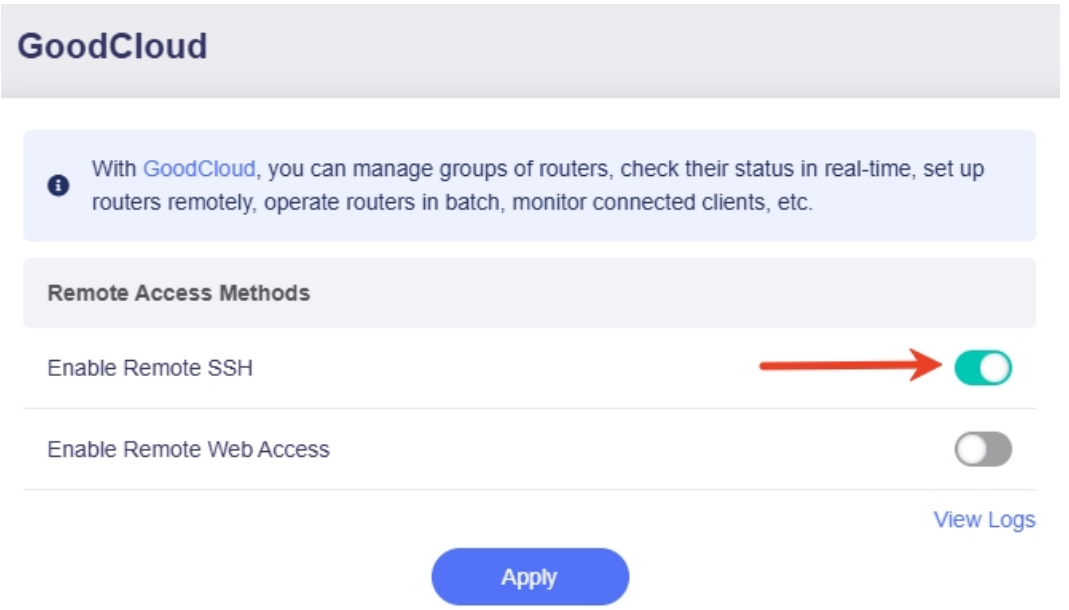


5. Sie werden zur Anmeldeseite des Routers weitergeleitet. Geben Sie das Administratorpasswort ein, um aus der Ferne auf die Weboberfläche zuzugreifen.

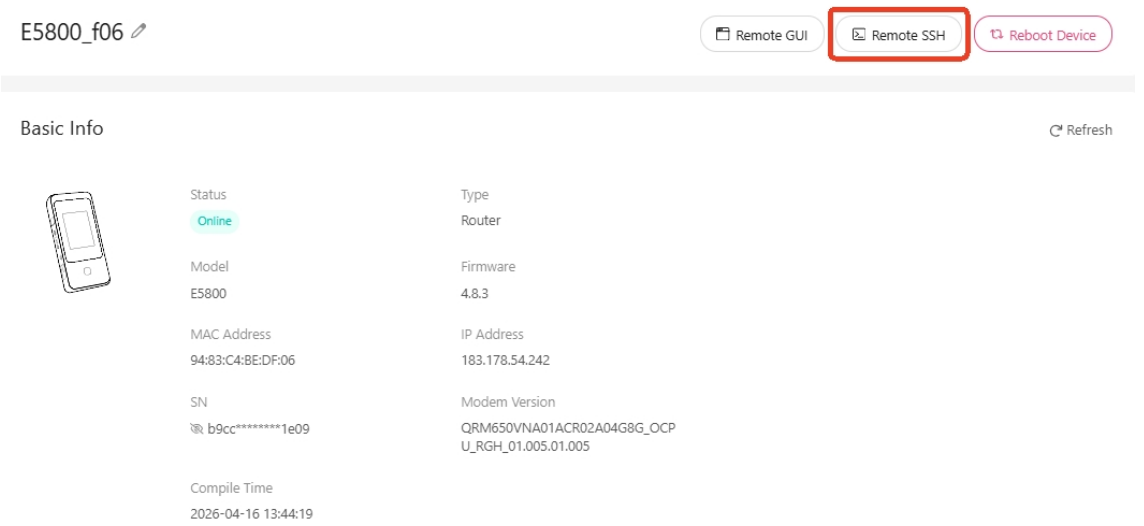


Fernzugriff auf das Terminal

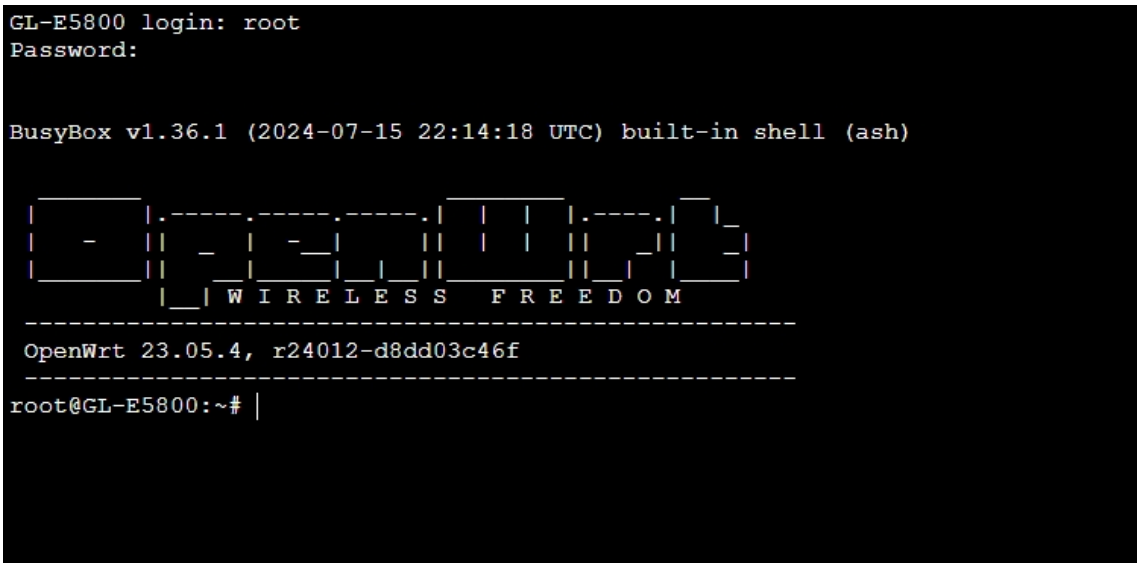
1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **CLOUD SERVICES** > **GoodCloud**. Aktivieren Sie **Remote SSH** und klicken Sie auf **Apply**.



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

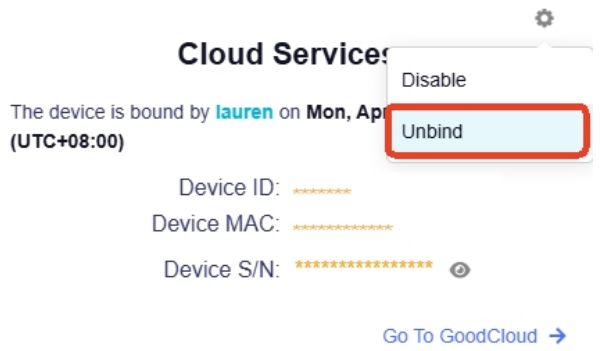


4. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

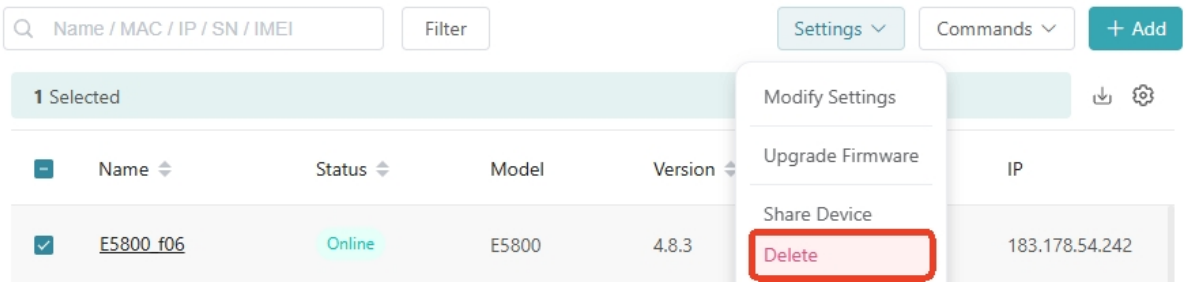

GL-E5800 login: root
Password:
BusyBox v1.36.1 (2024-07-15 22:14:18 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 23.05.4, r24012-d8dd03c46f
root@GL-E5800:~#

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.

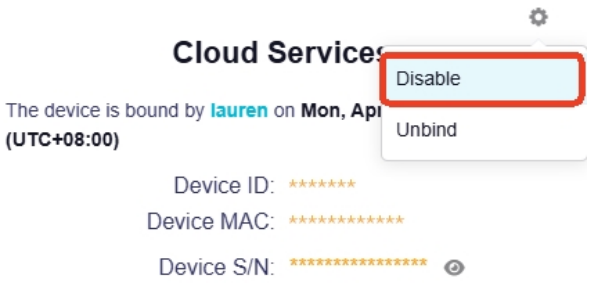


Alternativ können Sie sich an der Cloud-Plattform anmelden und **Device** > **Bound Devices** öffnen. Wählen Sie das Gerät aus, dessen Verknüpfung Sie aufheben möchten. Klicken Sie oben rechts auf **Settings** und wählen Sie **Delete**. Die Verknüpfung Ihres Geräts mit Ihrem GoodCloud-Konto wird daraufhin 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 leistungsfähige Netzwerkplattform für den nahtlosen Fernzugriff auf Netzwerke und die Fernverwaltung von Geräten.

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

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

Weitere Informationen finden Sie unter astrowarp.net.

Kapitel 8

VPN kennenlernen

Dieses Kapitel erläutert die Grundlagen von VPN und typische Einsatzmöglichkeiten.

8.1 Einführung

VPN

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

VPN-Router

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

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

OpenVPN

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

WireGuard

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

8.2 Einsatzmöglichkeiten

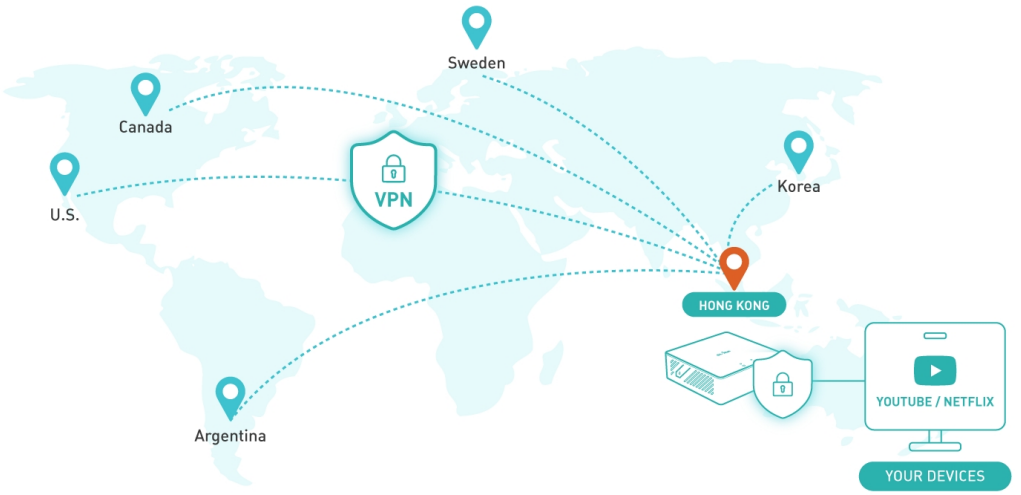
1. **Schutz persönlicher Daten**

   Der VPN-Dienst dieses Routers unterstützt zahlreiche kabelgebundene und drahtlose Geräte, darunter Laptops, Tablets, Smartphones, Spielkonsolen und Smart-TVs. Sämtliche über Kabel und WLAN übertragenen Daten werden durch das VPN geschützt. Mit individuellen VPN-Regeln können Sie den Schutz für bestimmte Geräte flexibel anpassen.



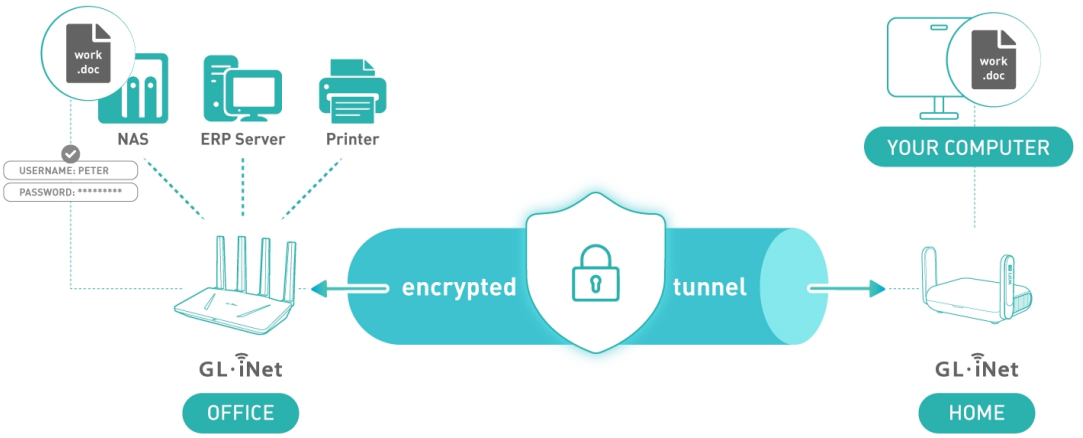
2. **Weltweiter Zugriff ohne Einschränkungen**

   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

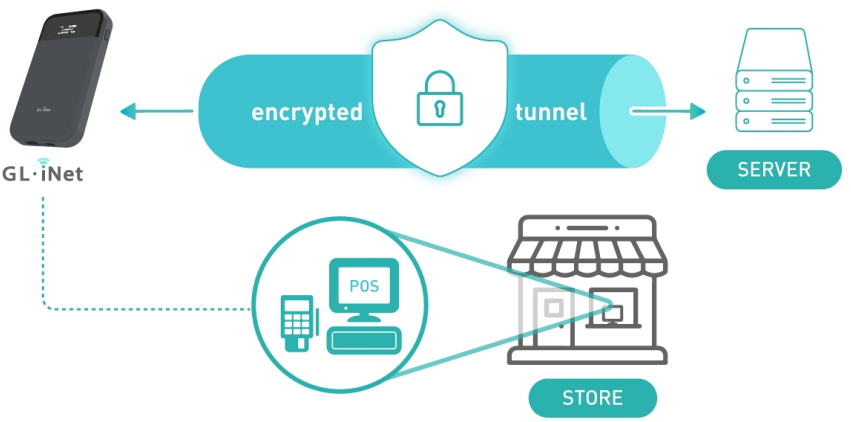
3. **Datensicherheit für kleine Unternehmen**

   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

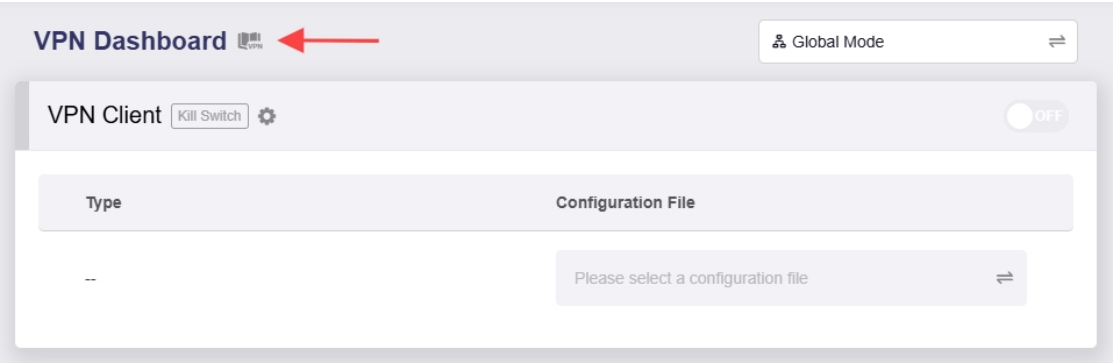
Dieses Kapitel beschreibt die Verwaltung von VPN-Verbindungen über die Weboberfläche.

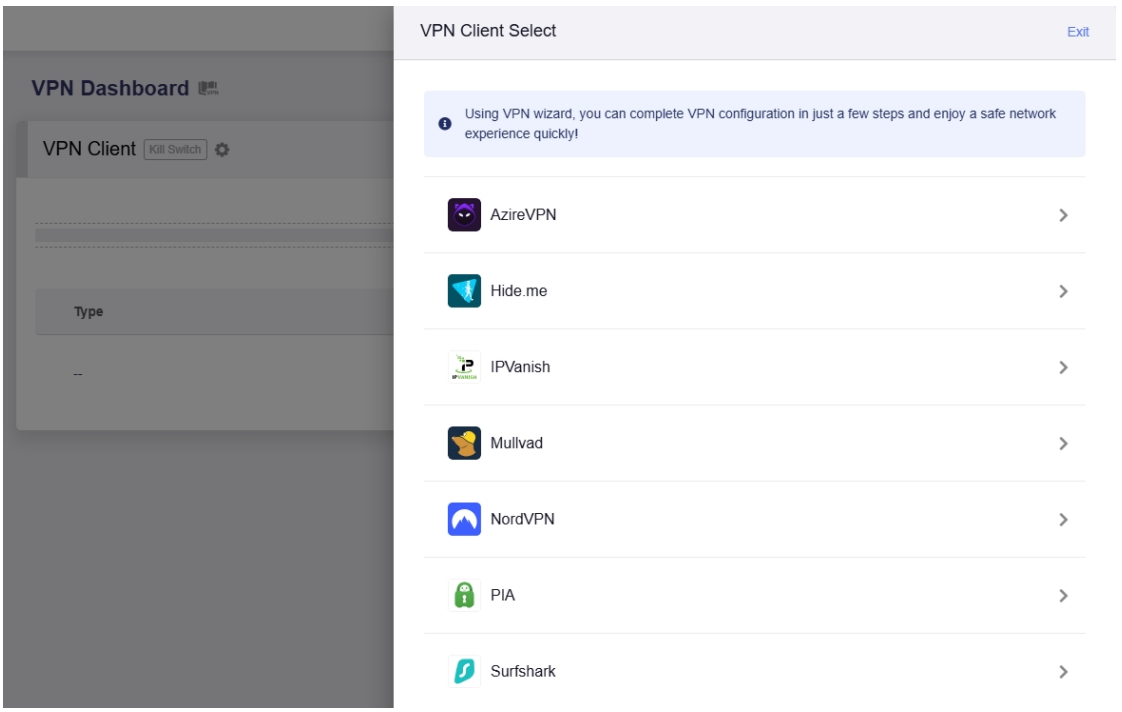
Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **VPN Dashboard**.

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.



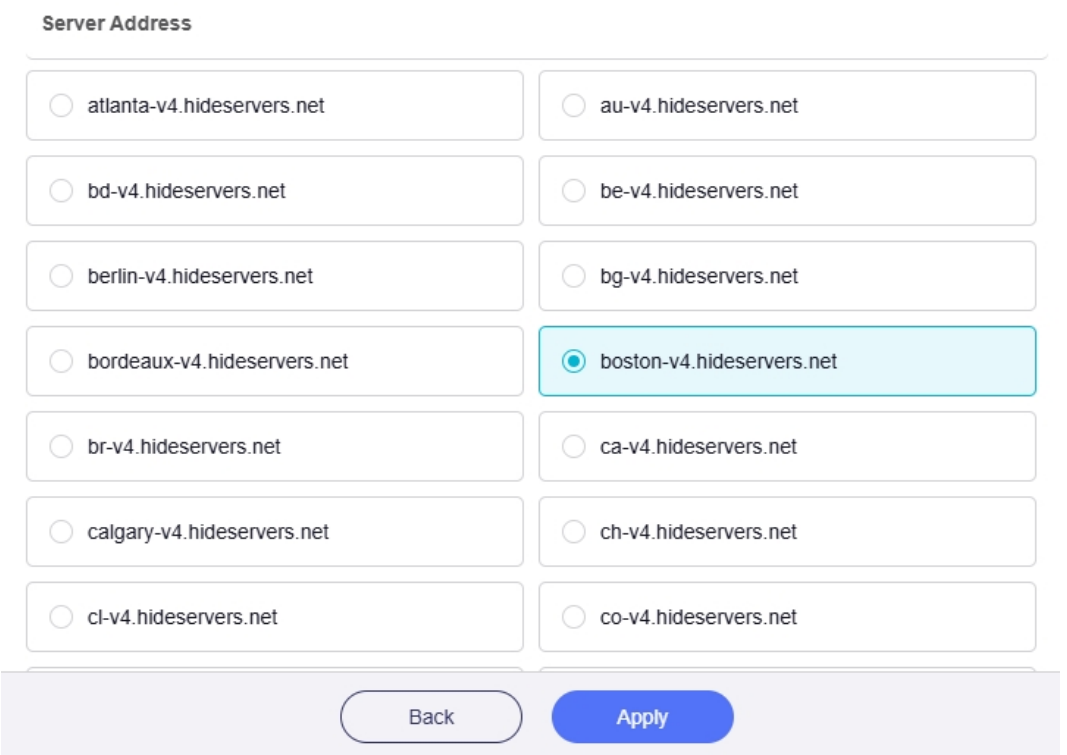


Hinweis: Der VPN-Einrichtungsassistent unterstützt nur die integrierten VPN-Dienste AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA und Surfshark. Bei anderen VPN-Anbietern überspringen Sie den Assistenten und öffnen **VPN** > **OpenVPN Client** oder **WireGuard Client**, um das VPN manuell einzurichten.

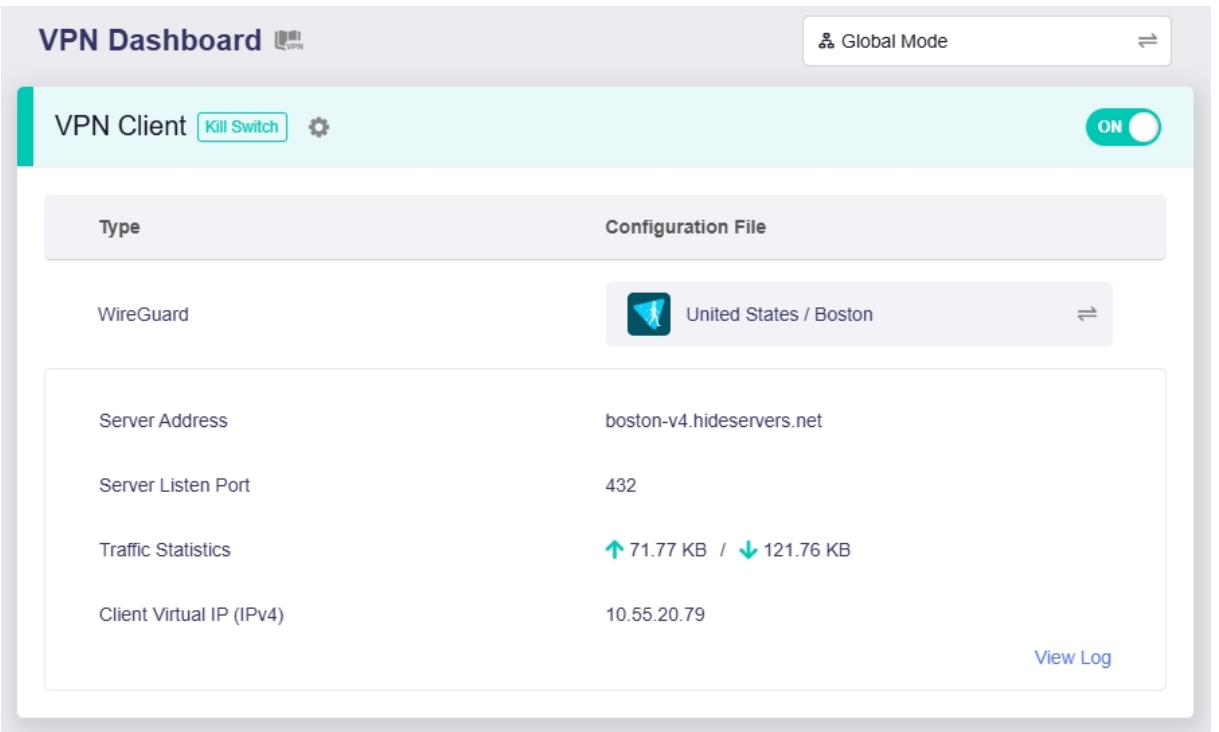
Das folgende Beispiel verwendet **Hide.me**. Melden Sie sich mit Ihren Hide.me-Zugangsdaten an.



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.

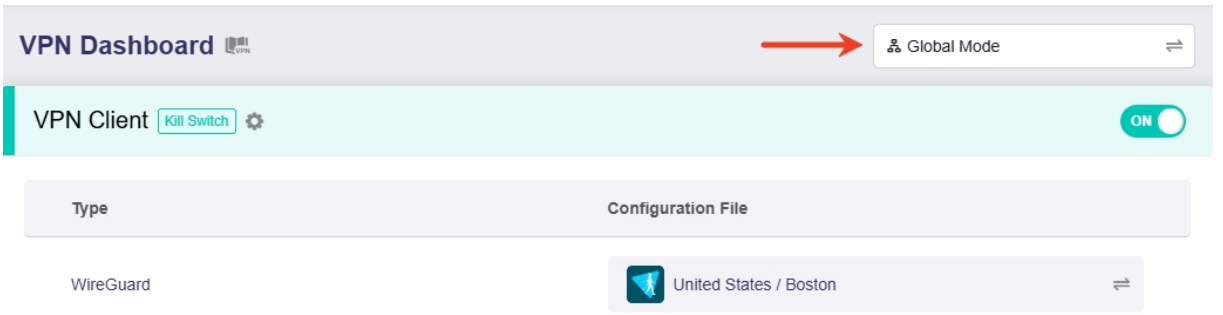


Die Verbindung wird automatisch hergestellt. Öffnen Sie anschließend das **VPN Dashboard**. Dort sehen Sie den aktivierten VPN-Tunnel mit Angaben zu VPN-Protokoll (z. B. WireGuard), Konfigurationsdatei, Serveradresse, Serverport, Datenverkehrsstatistiken und virtueller Client-IP-Adresse. Unten rechts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

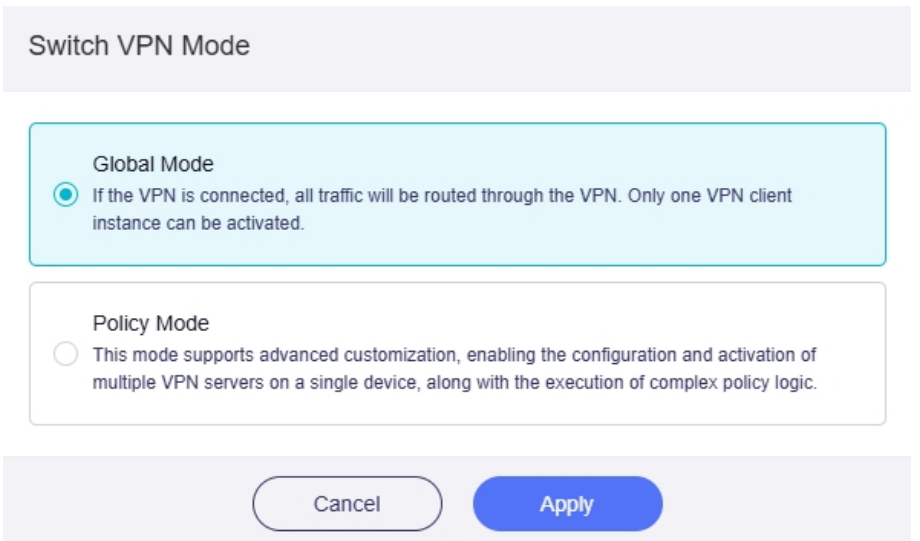


9.2 VPN-Modus

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



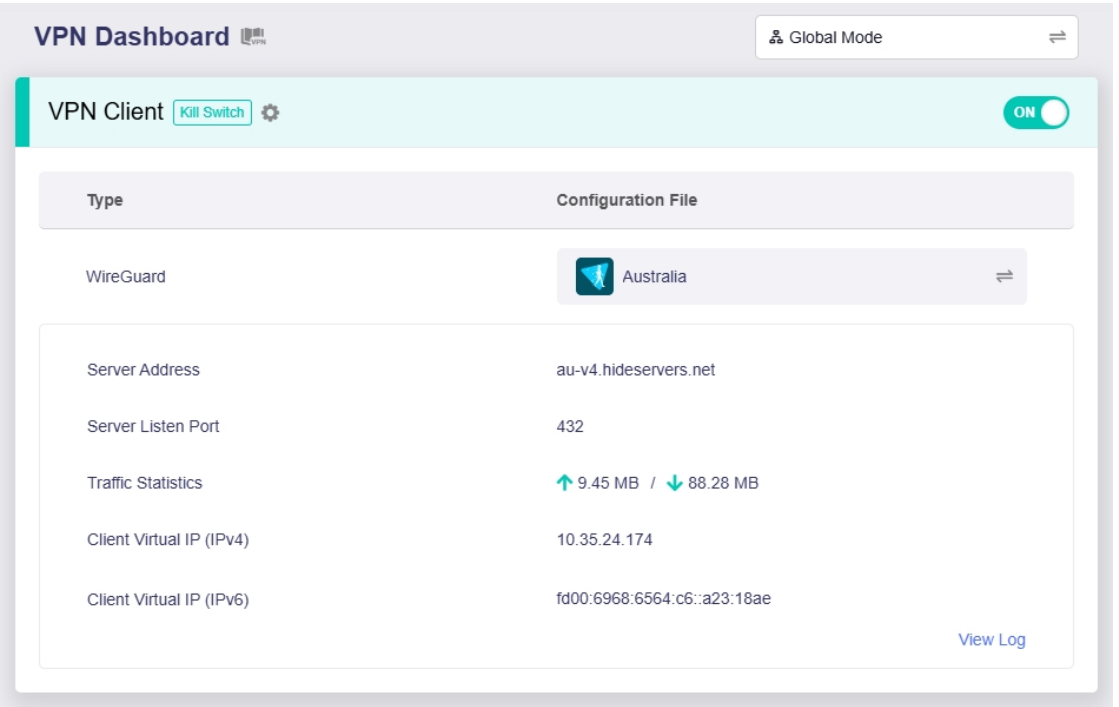
Es stehen zwei Modi zur Verfügung: **Global Mode** und **Policy Mode**.



9.2.1 Globaler Modus

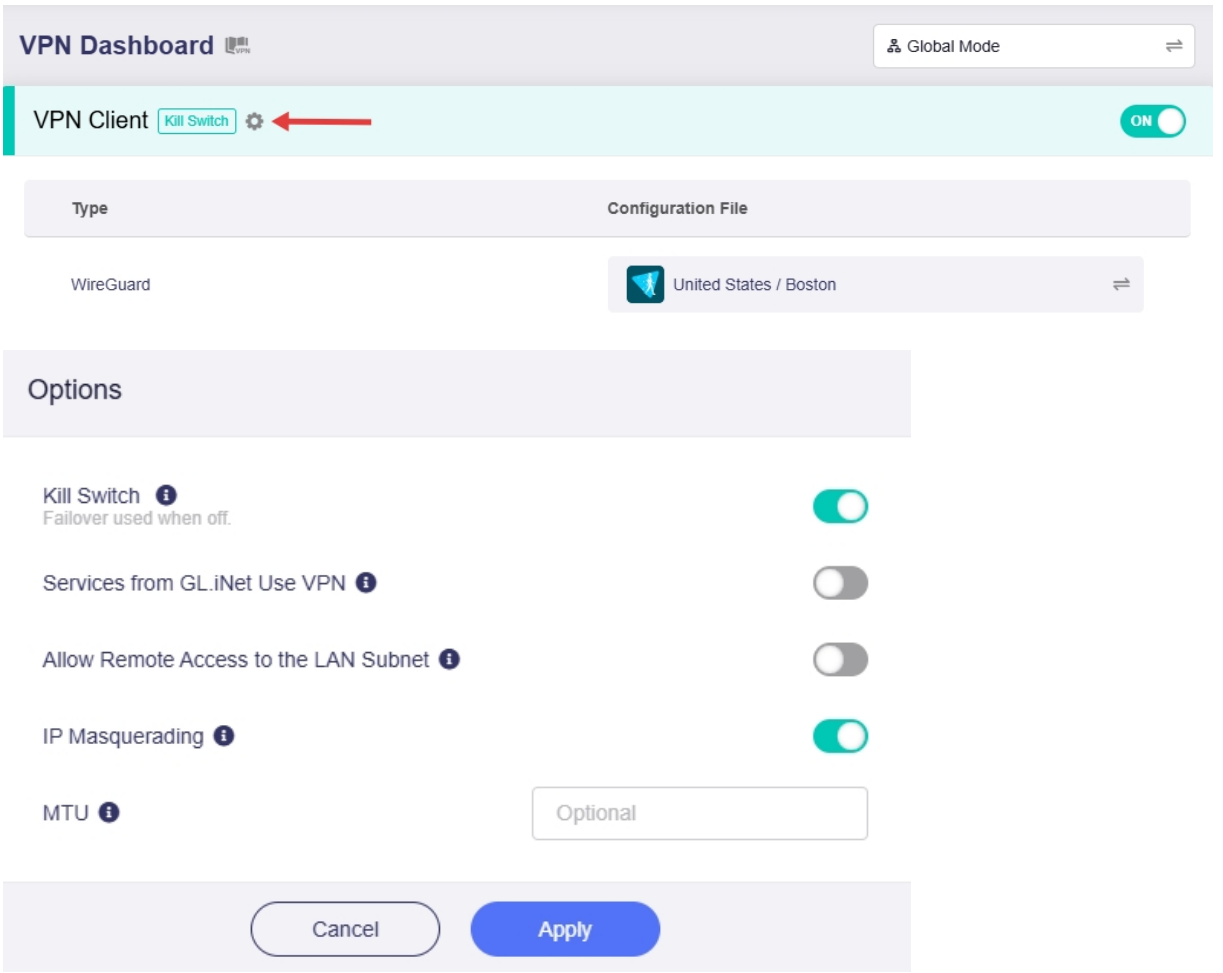
In diesem Modus wird der gesamte Datenverkehr durch den VPN-Tunnel geleitet. Es kann nur eine VPN-Client-Instanz aktiviert werden. Dieser Modus eignet sich, wenn der gesamte Geräteverkehr einen einzigen VPN-Server nutzen soll, beispielsweise für einheitliche Netzwerksicherheit oder den Zugriff auf regionsgebundene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



Tunneloptionen

Sie können erweiterte Einstellungen für Ihren VPN-Tunnel vornehmen, beispielsweise VPN-Kill-Switch, IP-Masquerading und MTU. Klicken Sie rechts oben auf das Zahnradsymbol.



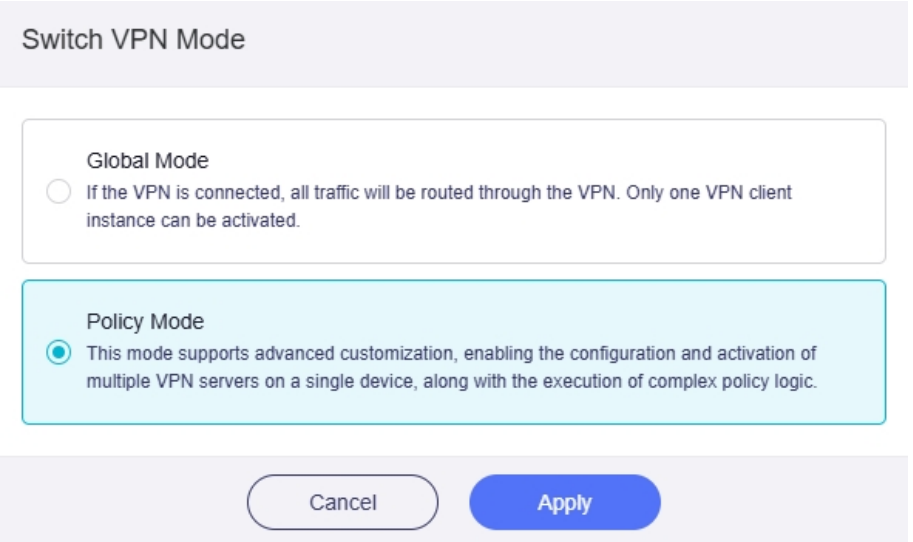
- **Kill Switch**: Bei aktivierter Option wird sämtlicher über diesen VPN-Tunnel geleiteter Datenverkehr automatisch gesperrt, wenn die VPN-Verbindung ausfällt. Bei deaktivierter Option wird der Datenverkehr auf das lokale WAN umgeleitet und greift ohne VPN-Tunnel auf das Internet zu.
- **Services from 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 auf diesen Router und seine LAN-Geräte über VPN erlaubt. Der VPN-Server muss eine Route zum LAN-Subnetz dieses Routers bekannt geben.
- **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**: Abkürzung für Maximum Transmission Unit, die maximale Übertragungseinheit. Der für den Tunnel festgelegte MTU-Wert überschreibt den in der Konfigurationsdatei definierten Wert.

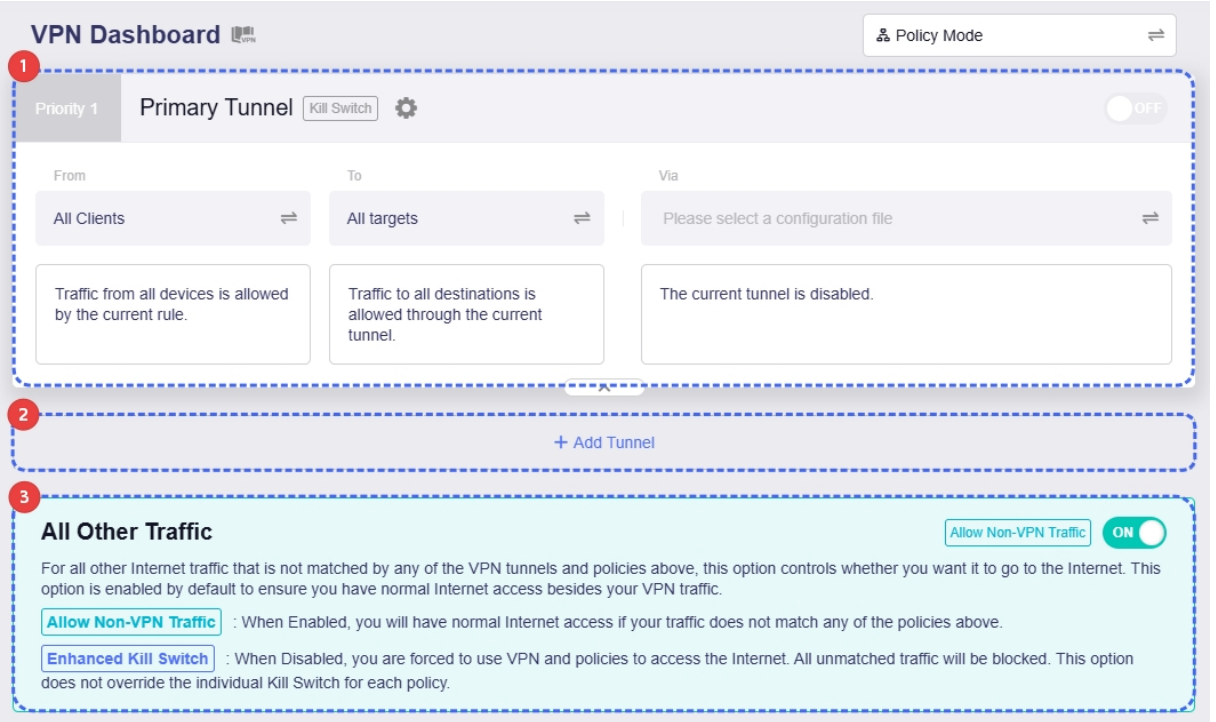
9.2.2 Richtlinienmodus

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**.

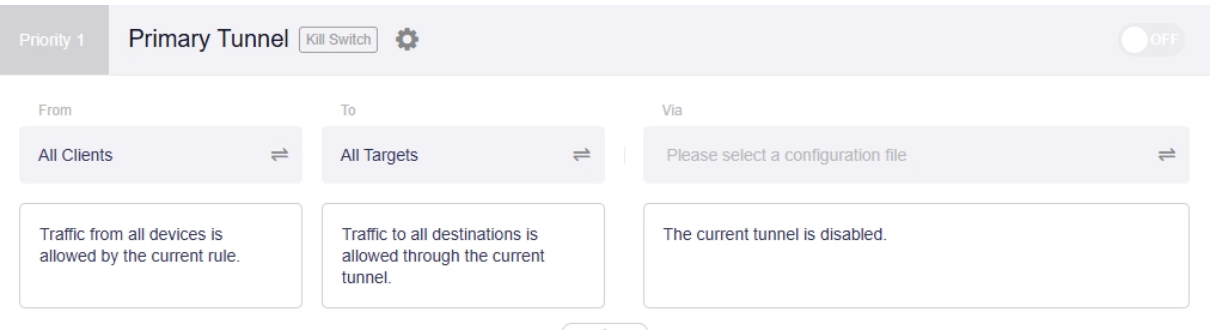


Primärer Tunnel

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

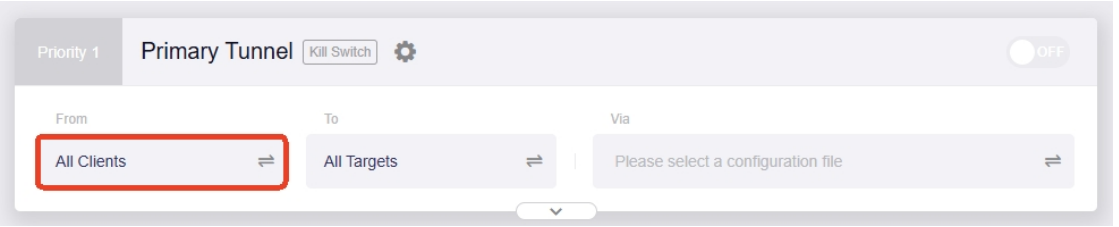
Für die Tunnelregel können Sie drei Merkmale festlegen:

- **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.

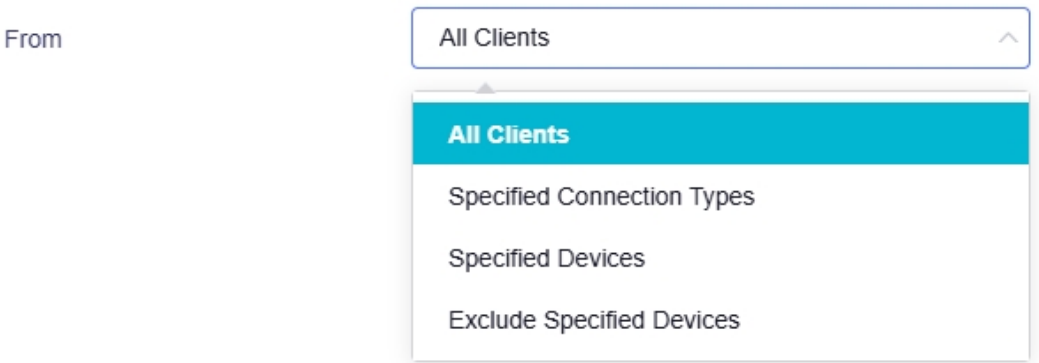


Gehen Sie wie folgt vor, um die Tunnelregel zu konfigurieren.

1. Klicken Sie auf das linke ausgegraute Feld.

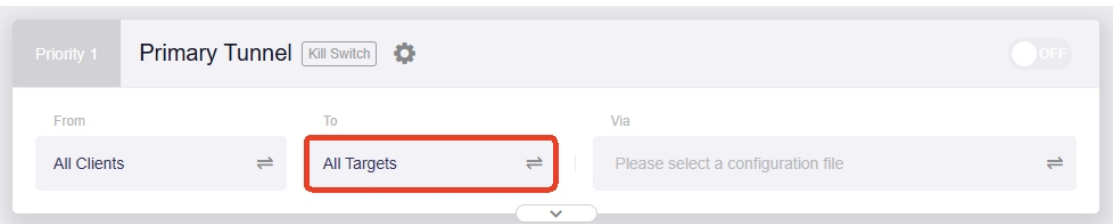


2. Wählen Sie die Geräte aus, auf die diese Regel zutreffen soll, und klicken Sie auf **Apply**.

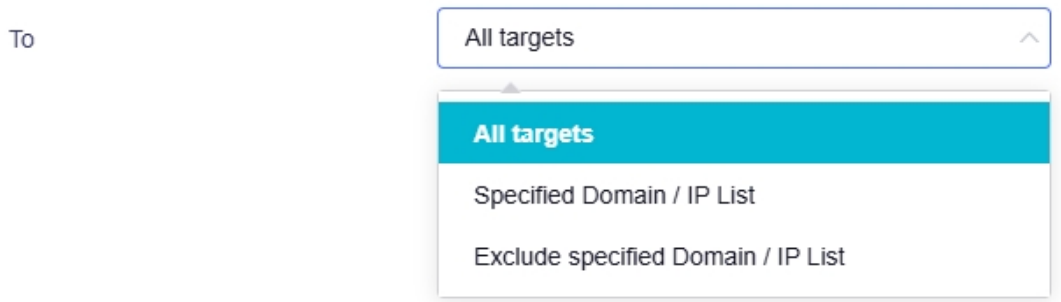


- **All Clients**: Die Regel gilt für den Datenverkehr aller Geräte.
- **Specified Connection Types**: Die Regel gilt für den Datenverkehr bestimmter Verbindungstypen, beispielsweise LAN-Subnetz, Drop-in Gateway oder Gastnetzwerk.
- **Specified Devices**: Die Regel gilt für den Datenverkehr bestimmter, 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.



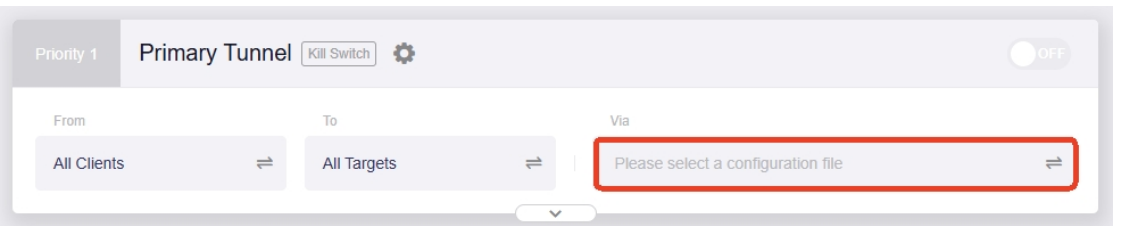
4. Wählen Sie das Ziel aus, an das der Datenverkehr durch diesen Tunnel geleitet werden soll, und klicken Sie auf **Apply**.



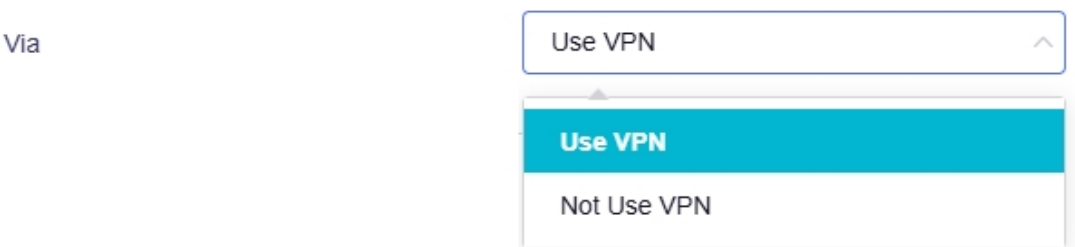
- **All Targets**: Der dieser Regel entsprechende Datenverkehr wird an alle Ziele geleitet.
- **Specified Domain / IP List**: Der dieser Regel entsprechende Datenverkehr wird an die angegebenen Domains bzw. IP-Adressen geleitet. Geben Sie die Domains/IP-Adressen manuell ein oder tragen Sie die Abonnement-URL 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.

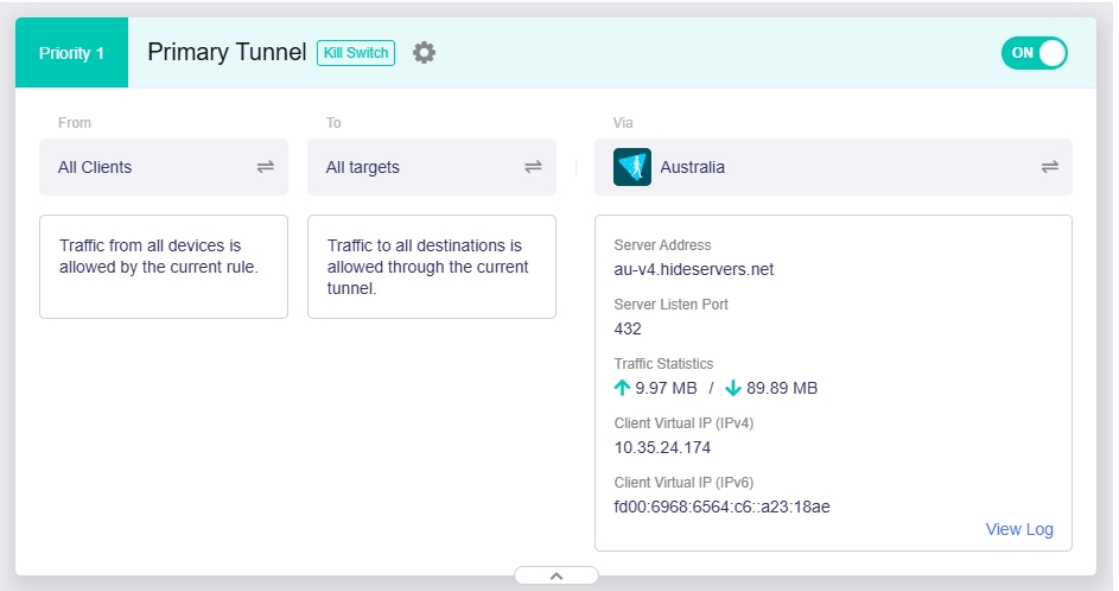


6. Wählen Sie die Weiterleitungsmethode für diesen Tunnel: **Use VPN** oder **Not Use VPN**.



- **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.



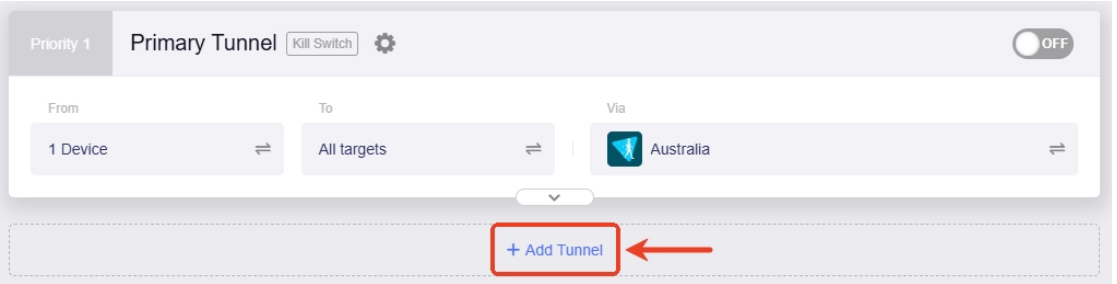
Hinweis: Prüfen Sie vor der Aktivierung dieses Tunnels aus Sicherheitsgründen die weiteren Einstellungen unter All Other Traffic und Tunnel Options.

Tunnel hinzufügen

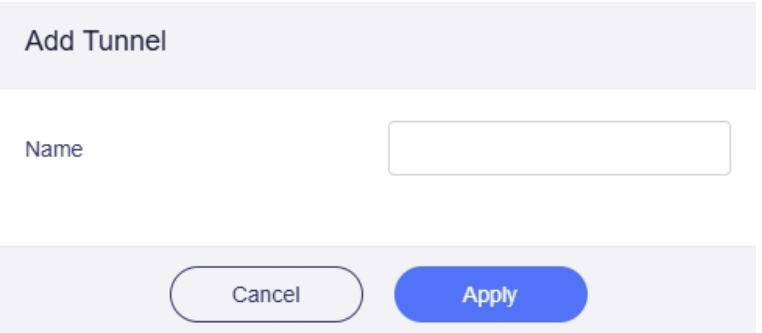
Fügen Sie weitere Tunnel hinzu, wenn Sie den Datenverkehr verschiedener Geräte an unterschiedliche Ziele leiten möchten.

Gehen Sie wie folgt vor, um einen Tunnel hinzuzufügen.

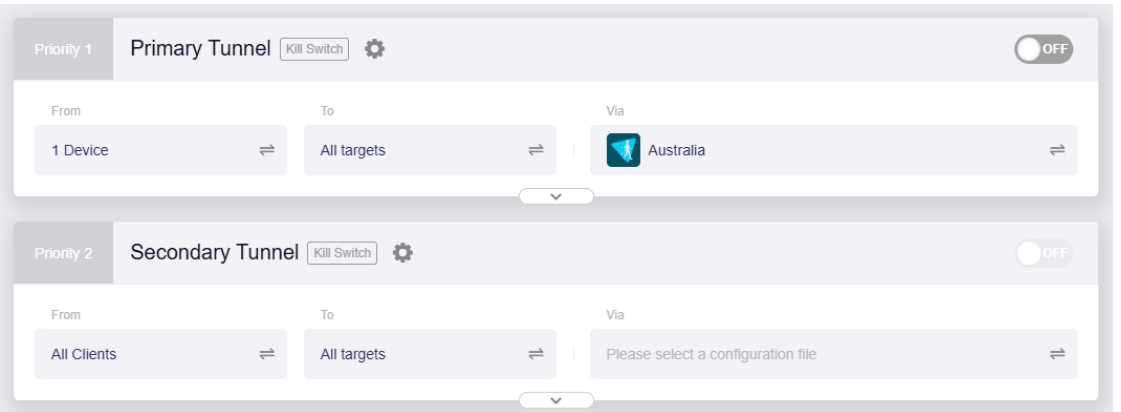
1. Klicken Sie unter dem primären Tunnel auf **Add Tunnel**.



2. Geben Sie dem Tunnel einen Namen.



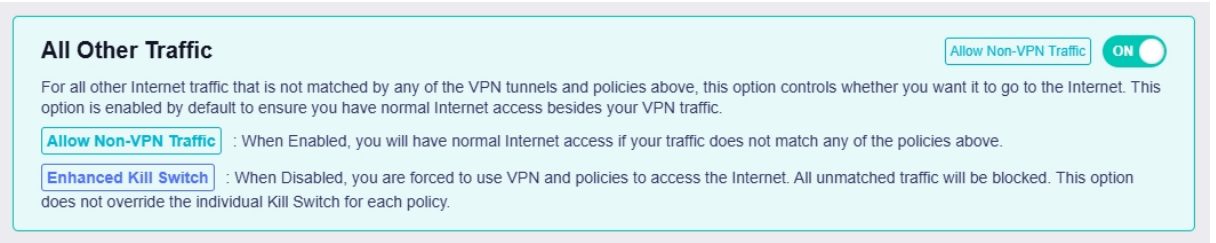
3. Im VPN-Dashboard wird ein weiterer Tunnel angezeigt. Sie können bis zu fünf Tunnel einschließlich des vorgegebenen primären Tunnels erstellen.



4. Legen Sie für die Tunnelregeln Quelle, Ziele und Weiterleitungsmethode fest. Prüfen Sie anschließend aus Sicherheitsgründen die weiteren Einstellungen unter All Other Traffic und Tunnel Options, bevor Sie die Tunnel aktivieren.

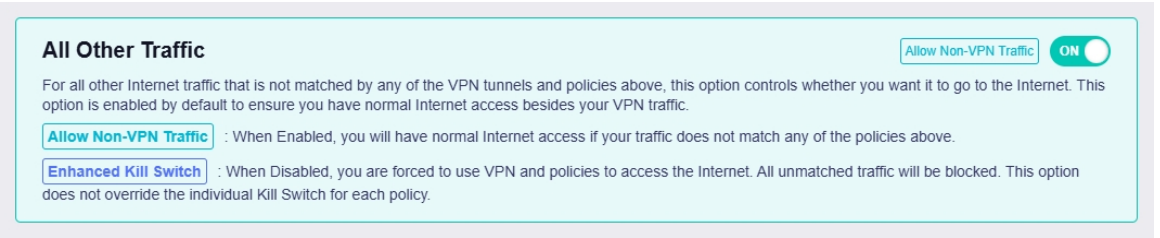
Sonstiger Datenverkehr

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

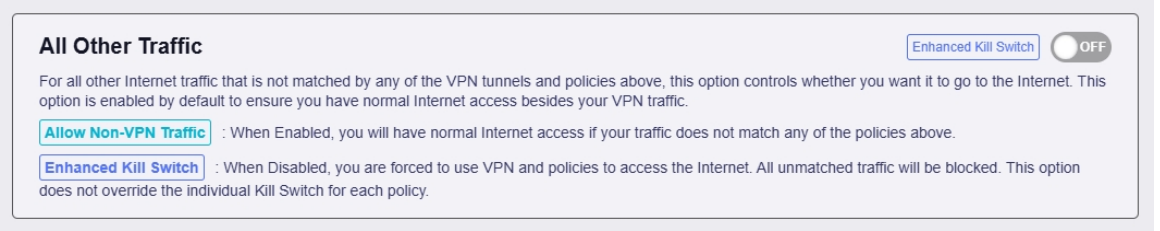


Dieser Tunnel steuert, ob Datenverkehr, auf den keine der darüberstehenden VPN-Tunnelgruppen zutrifft, auf das Internet zugreifen darf. Er ist standardmäßig aktiviert, um den normalen Internetzugang für Datenverkehr außerhalb des VPN zu gewährleisten.

- 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.

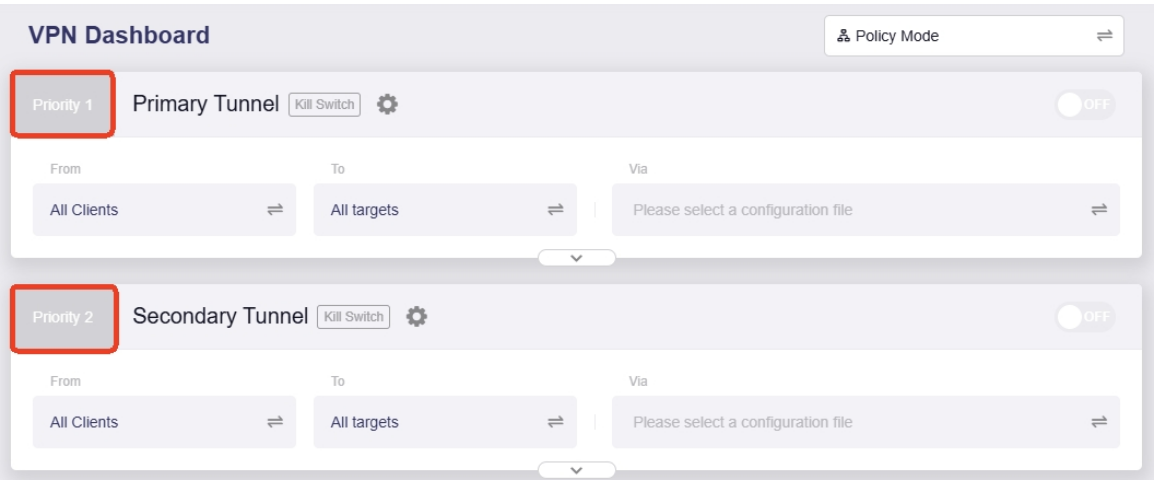


Tunnelpriorität

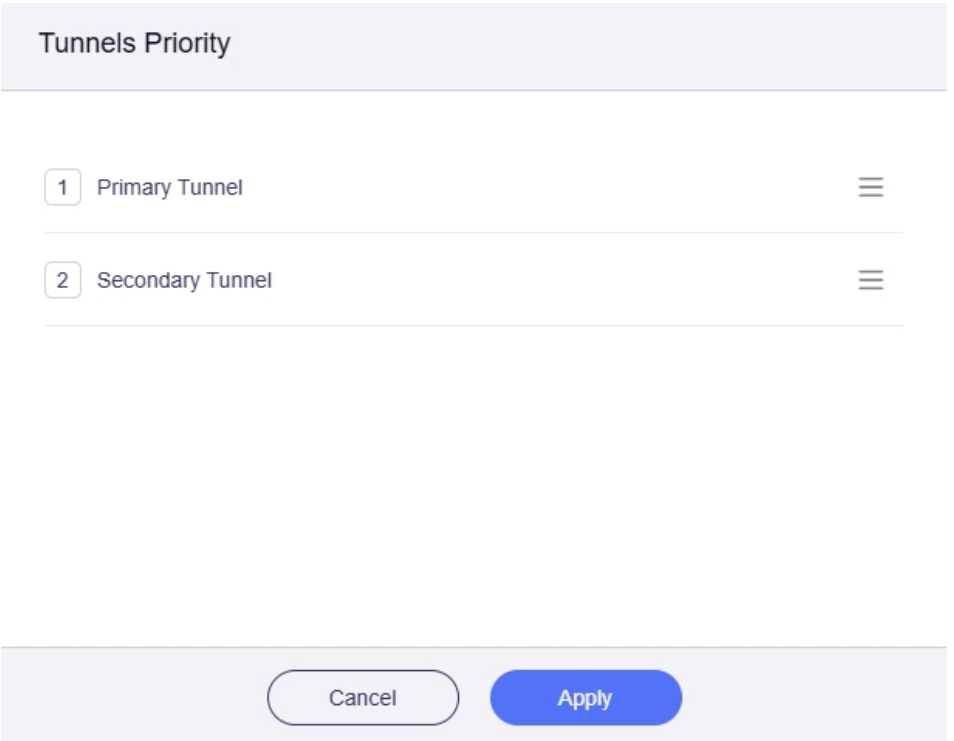
Standardmäßig hat der vorgegebene primäre Tunnel die höchste Priorität. Darauf folgen gegebenenfalls manuell hinzugefügte Tunnel und zuletzt der vorgegebene Tunnel „All Other Traffic“, der die Verbindung über das lokale Netz des Internetanbieters (WAN) sicherstellt.

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**.

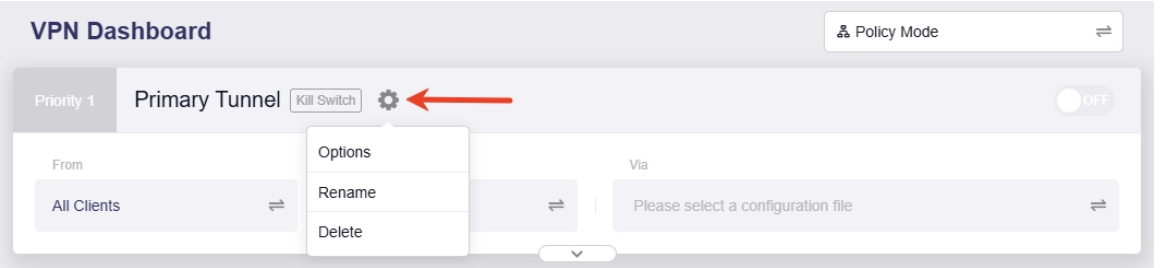


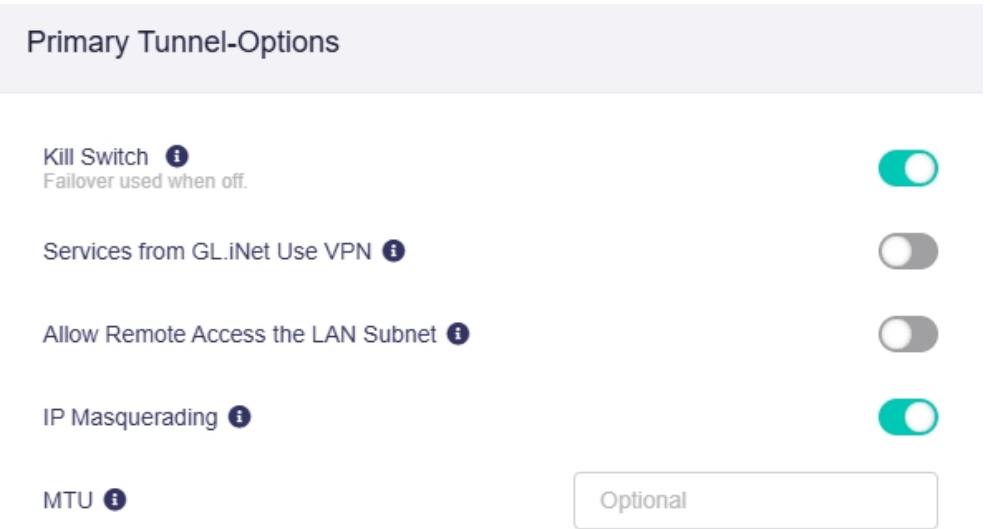
Wenn mehrere Tunnel aktiviert sind, leitet der Router den Datenverkehr in folgender Reihenfolge weiter:

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.

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 sämtlicher über diesen VPN-Tunnel geleiteter Datenverkehr automatisch gesperrt, wenn die VPN-Verbindung ausfällt. Bei deaktivierter Option wird auf den nächsten Tunnel in der Prioritätsreihenfolge oder auf das lokale WAN ausgewichen.
- **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 auf diesen Router und seine LAN-Geräte über VPN erlaubt. Der VPN-Server muss eine Route zum LAN-Subnetz dieses Routers bekannt geben.

- **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**: Der für den Tunnel festgelegte MTU-Wert überschreibt den Wert in der Konfigurationsdatei.

Kapitel 10

VPN-Server einrichten

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

10.1 OpenVPN-Server einrichten

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

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:

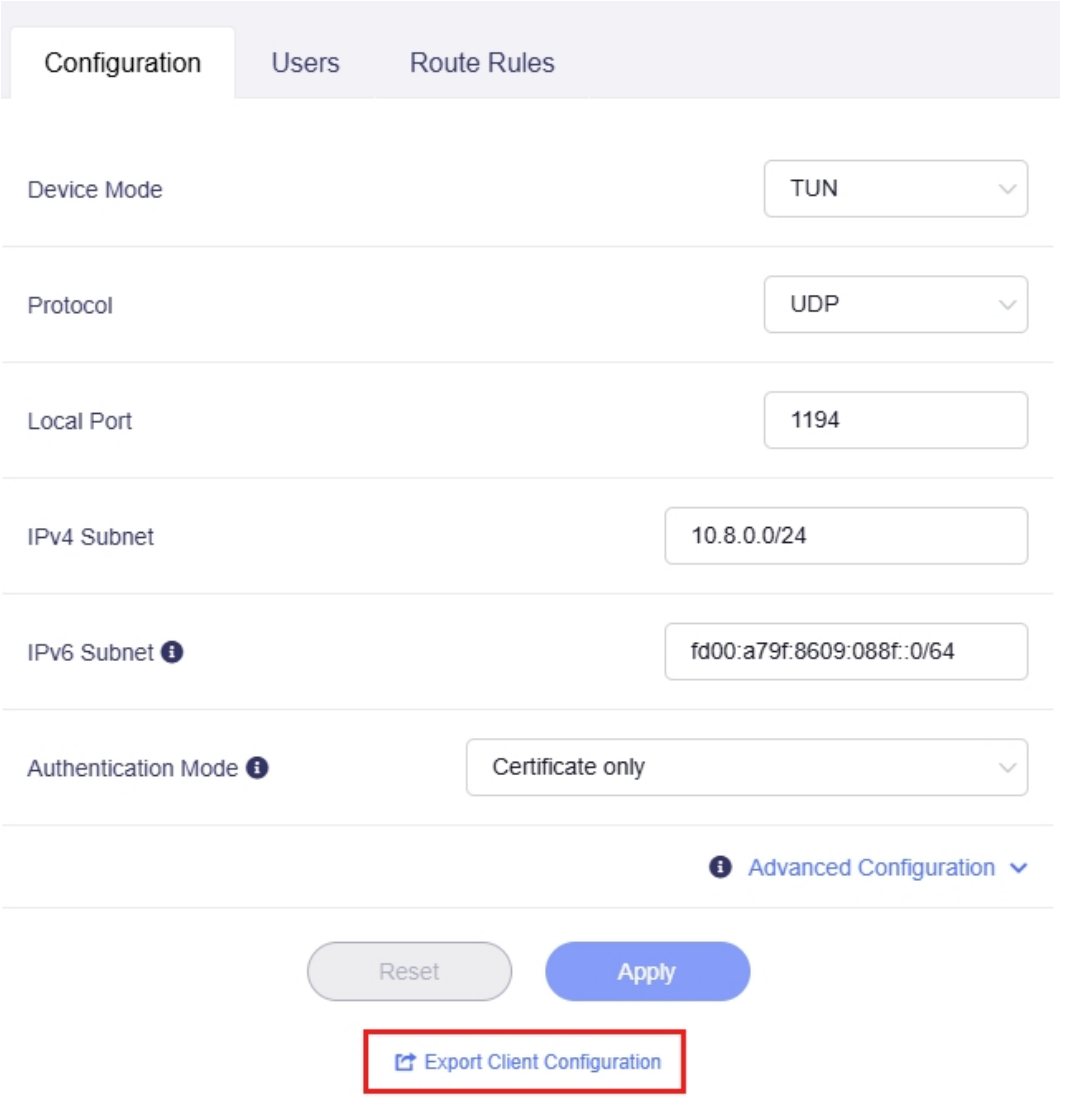
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.
   - Wenn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

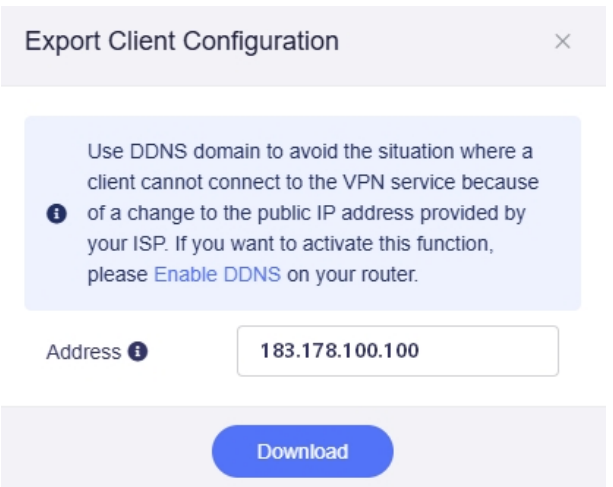


- **Device Mode**: TAP-S2S oder Tun. Die Unterschiede werden hier erläutert.
- **Protocol**: UDP oder TCP. Die Unterschiede werden hier erläutert.
- **Authentication Mode**: Legt fest, wie sich der Client beim Verbinden mit dem Server authentifiziert. Es gibt drei Optionen:

- **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.

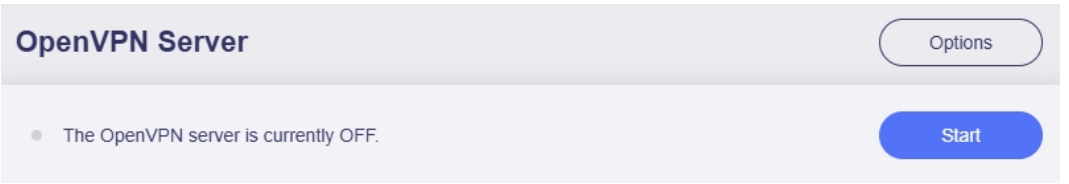
3. Client-Konfiguration exportieren.
   Nach einem Klick auf **Export Client Configuration** unten auf der Registerkarte Configuration oder nach dem Übernehmen einer geänderten Konfiguration erscheint das folgende Fenster. Klicken Sie auf **Download**, um die Konfiguration zu exportieren.



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 Fehlerbehebung

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

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

10.2 WireGuard-Server einrichten

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

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:

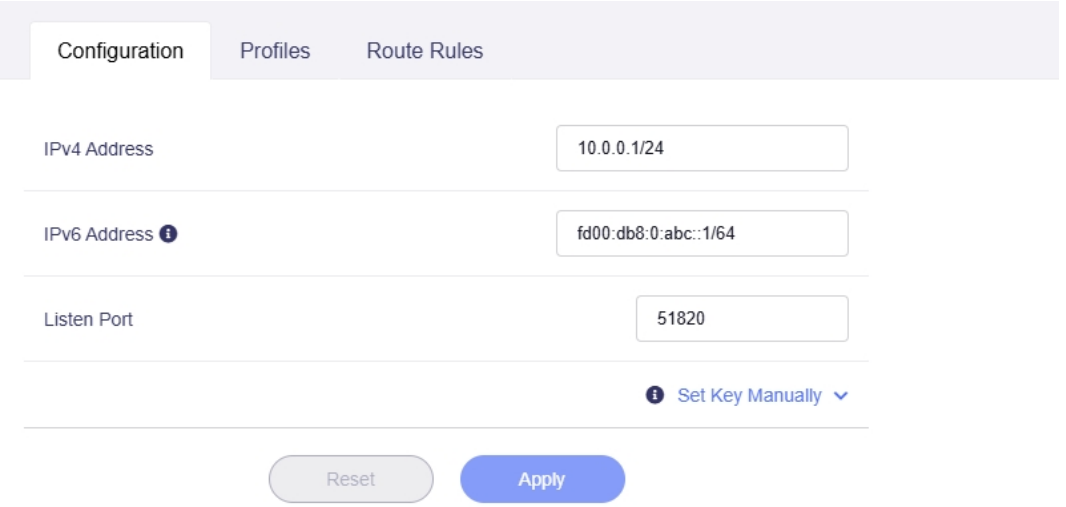
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.
   - Wenn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

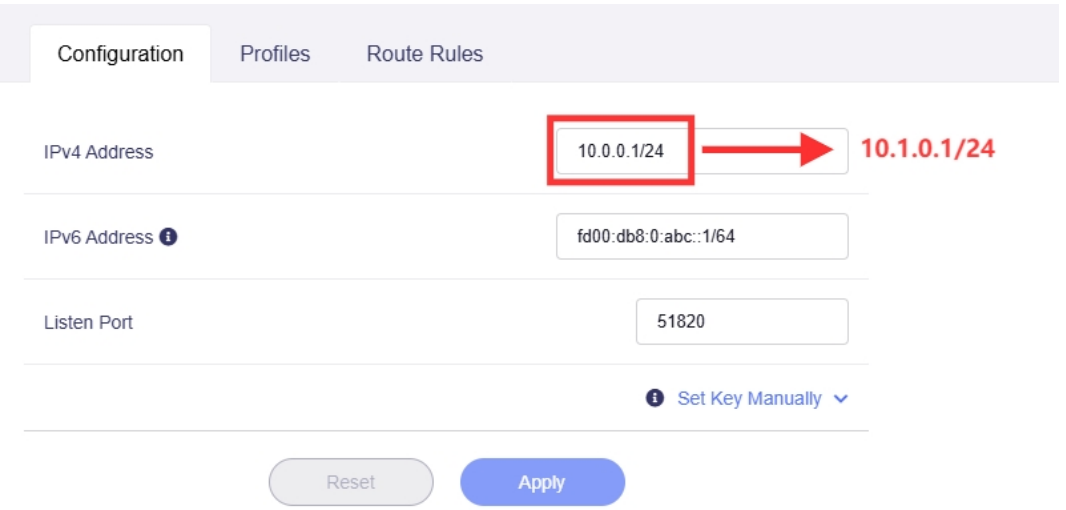
   - Wenn Ihr GL.iNet-Router der Hauptrouter Ihres Netzwerks ist, benötigen Sie keine Portweiterleitung. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn bereits ein Hauptrouter vorhanden ist und Ihr GL.iNet-Router als nachgeschalteter Router arbeitet, müssen Sie auf dem Hauptrouter eine Portweiterleitung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

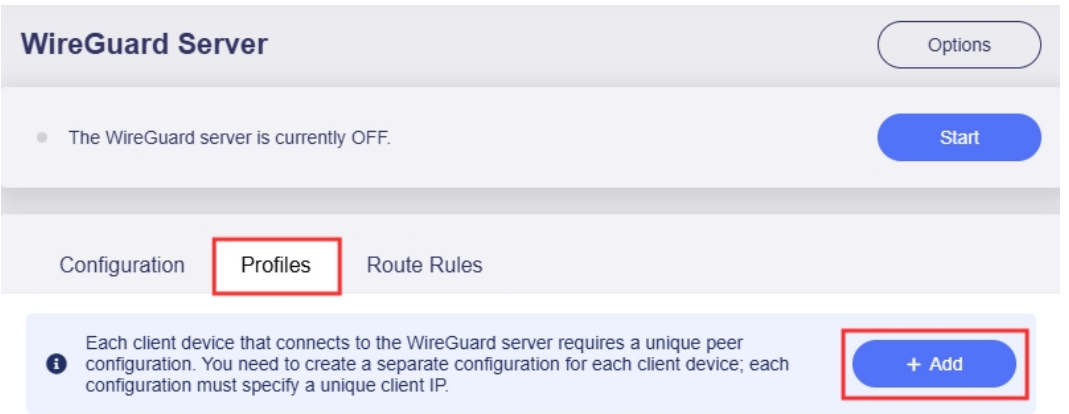


   Bei einem solchen Adresskonflikt wählen Sie eine andere IPv4-Adresse, etwa **10.1.0.1/24**, und klicken Sie auf **Apply**. Achten Sie darauf, die CIDR-Angabe „/24“ beizubehalten, um Verbindungsprobleme zu vermeiden.

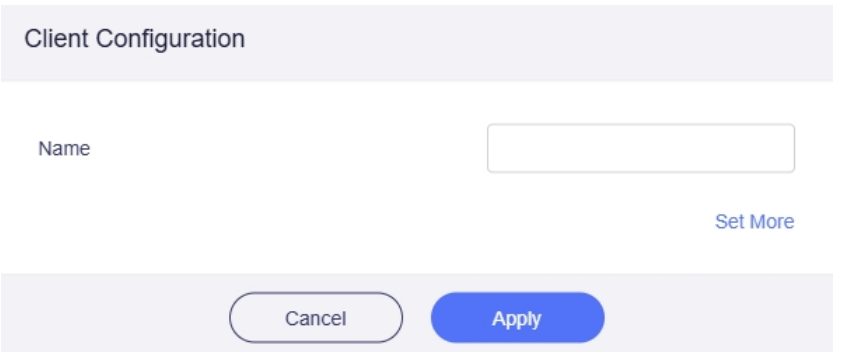


3. Profil hinzufügen.

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



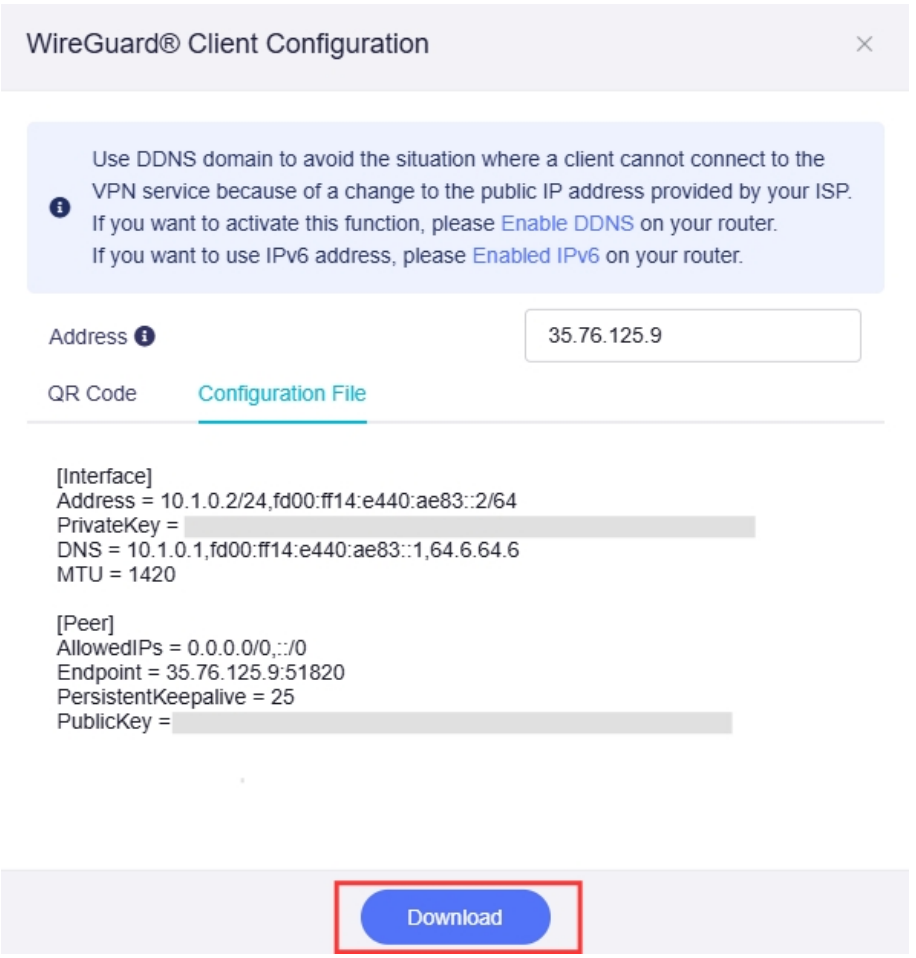
Vergeben Sie einen aussagekräftigen Namen und klicken Sie auf **Apply**, um fortzufahren.



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.

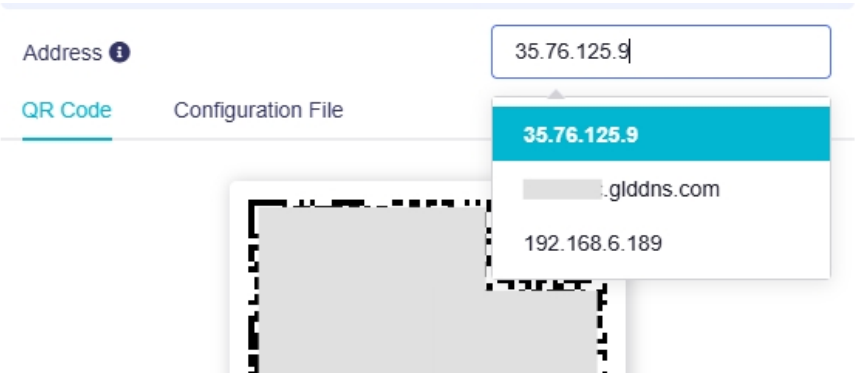
4. Konfiguration herunterladen.
   Nach dem Hinzufügen eines Profils stellt der Router die Konfiguration in drei Formen bereit: als QR-Code, als Klartext und als .conf-Datei. Wählen Sie die gewünschte Form aus.
   - **QR-Code**: Geeignet für Geräte wie Smartphones, Tablets oder Laptops mit installierter 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.

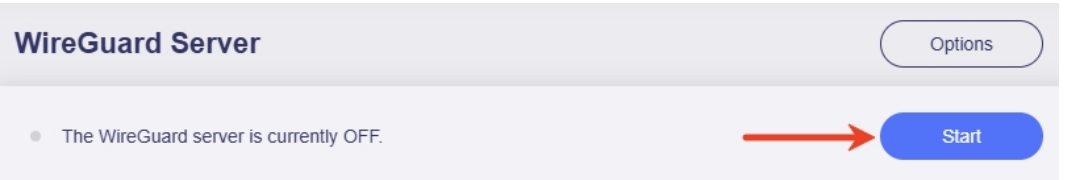


Tipps:

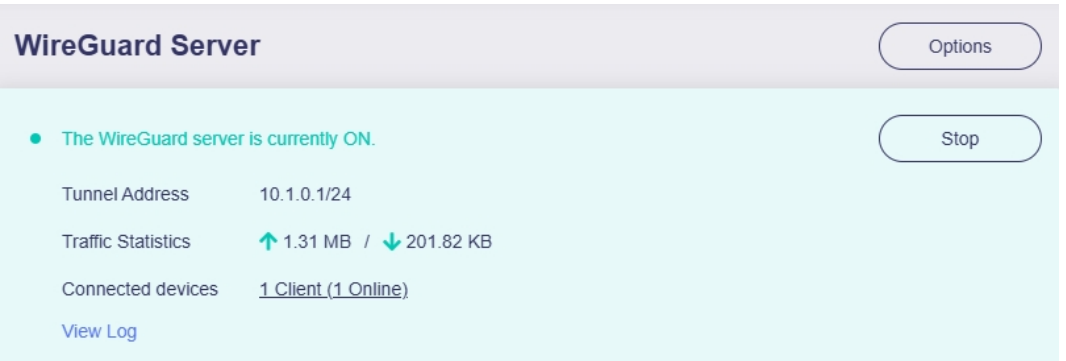
- Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Anschließend können Sie die DDNS-Domain als Serveradresse verwenden.
- Seit Firmware v4.8 können Sie die Serveradresse vor dem Export der Konfigurationsdatei aus einer Dropdown-Liste 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 Fehlerbehebung

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

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

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

Kapitel 11

VPN-Client einrichten

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

11.1 OpenVPN-Client einrichten

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.

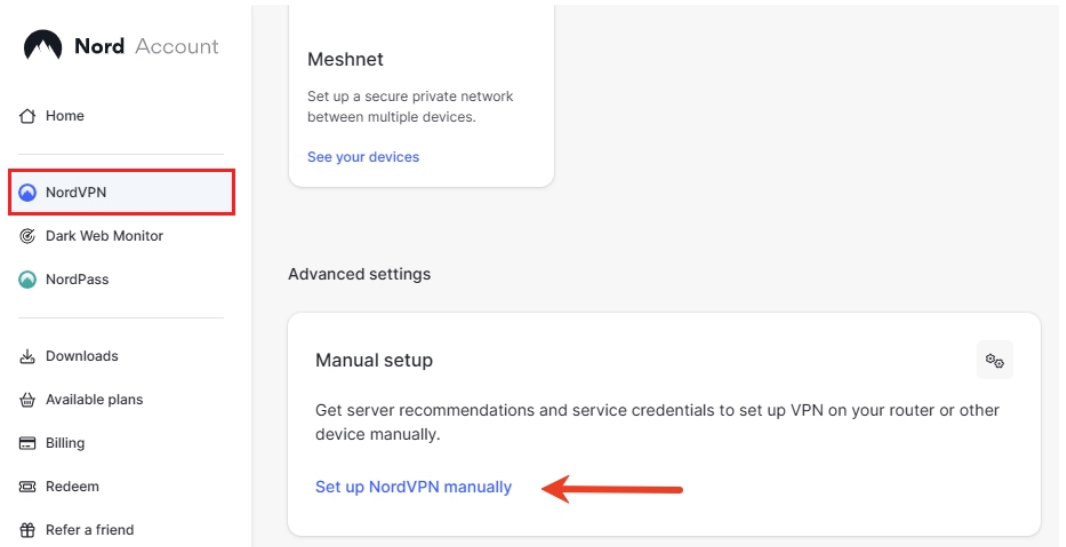
Rufen Sie anschließend die offizielle Webseite Ihres VPN-Anbieters auf und beschaffen Sie die Dienstzugangsdaten oder eine Konfigurationsdatei. Falls Sie nicht wissen, wie Sie die Datei erhalten, folgen Sie diesem Link oder wenden Sie sich an den Support des Anbieters.

11.1.2 NordVPN einrichten

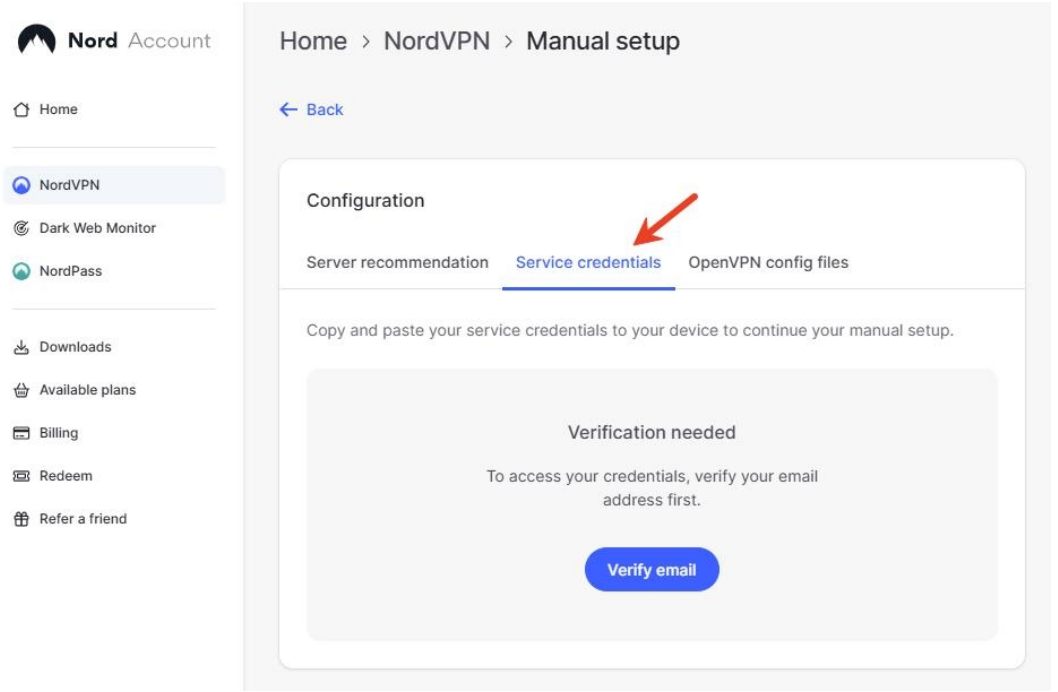
NordVPN ist in die GL.iNet-Weboberfläche integriert. Geben Sie Ihre im NordVPN-Dashboard erhältlichen Zugangsdaten in der Weboberfläche des Routers oder in der GL.iNet-App ein, um die Konfigurationsdateien aller NordVPN-Server abzurufen. Ein manuelles Hochladen der Dateien ist dadurch nicht erforderlich.

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

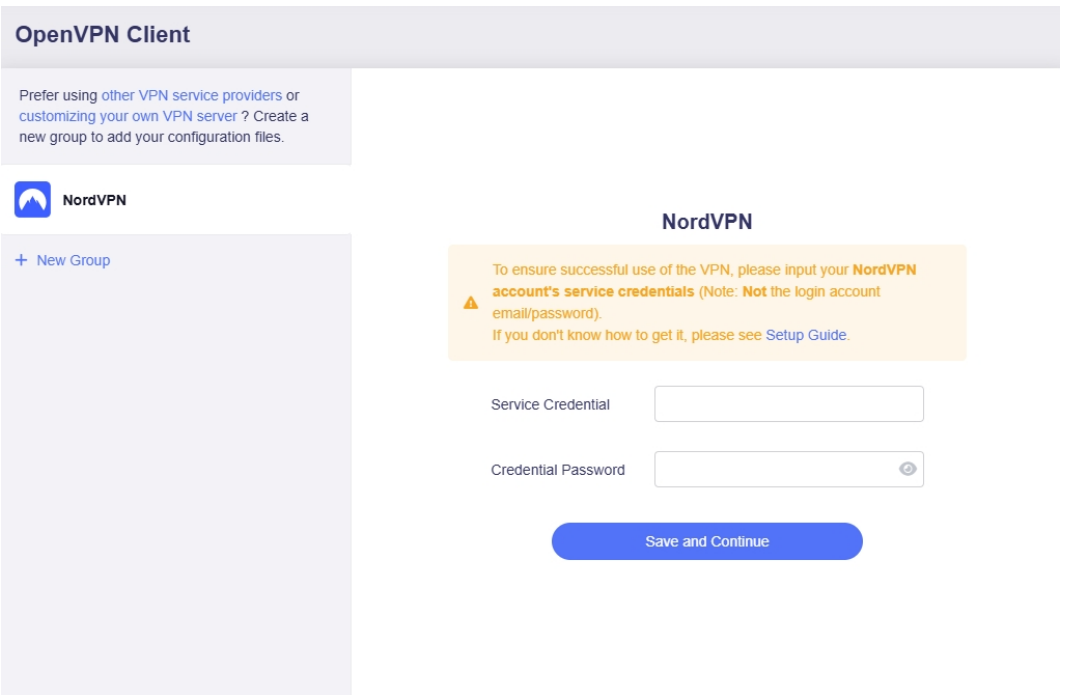
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



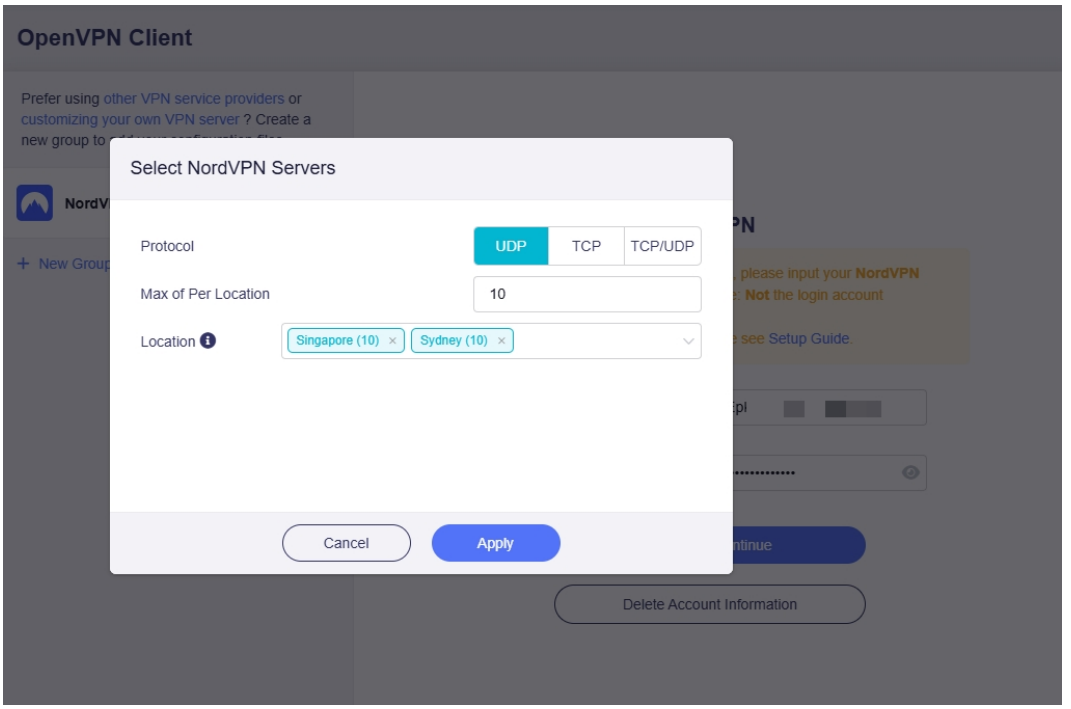
Dort finden Sie die **Dienstzugangsdaten**. Kopieren Sie diese für die spätere Verwendung.



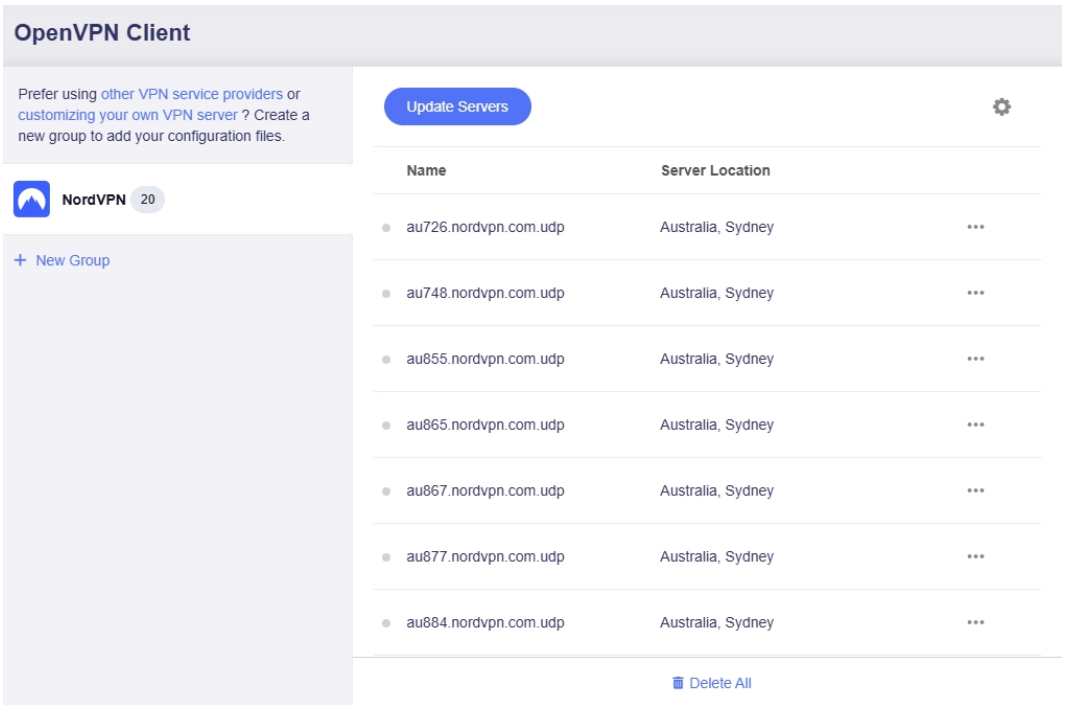
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **OpenVPN Client** > **NordVPN**. Geben Sie die Dienstzugangsdaten ein. Hinweis: Dies sind NICHT die E-Mail-Adresse und das Passwort Ihres Benutzerkontos. Klicken Sie anschließend auf **Save and Continue**.



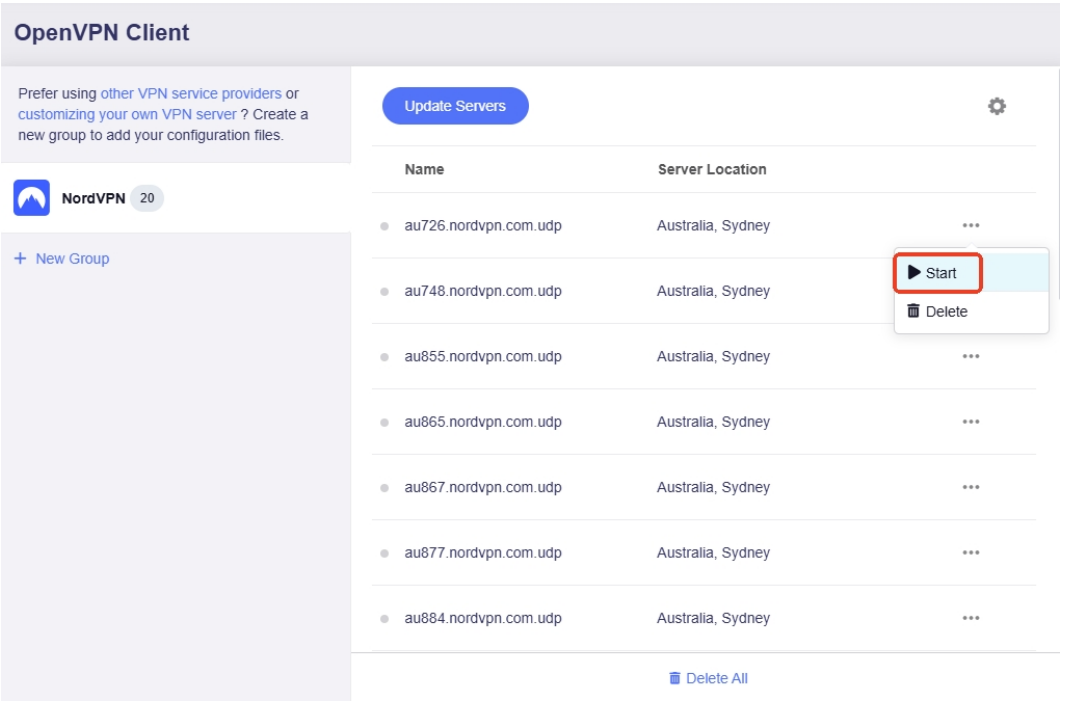
4. Wählen Sie das Protokoll, die maximale Serveranzahl pro Standort und die Standorte aus. Klicken Sie anschließend auf **Apply**.



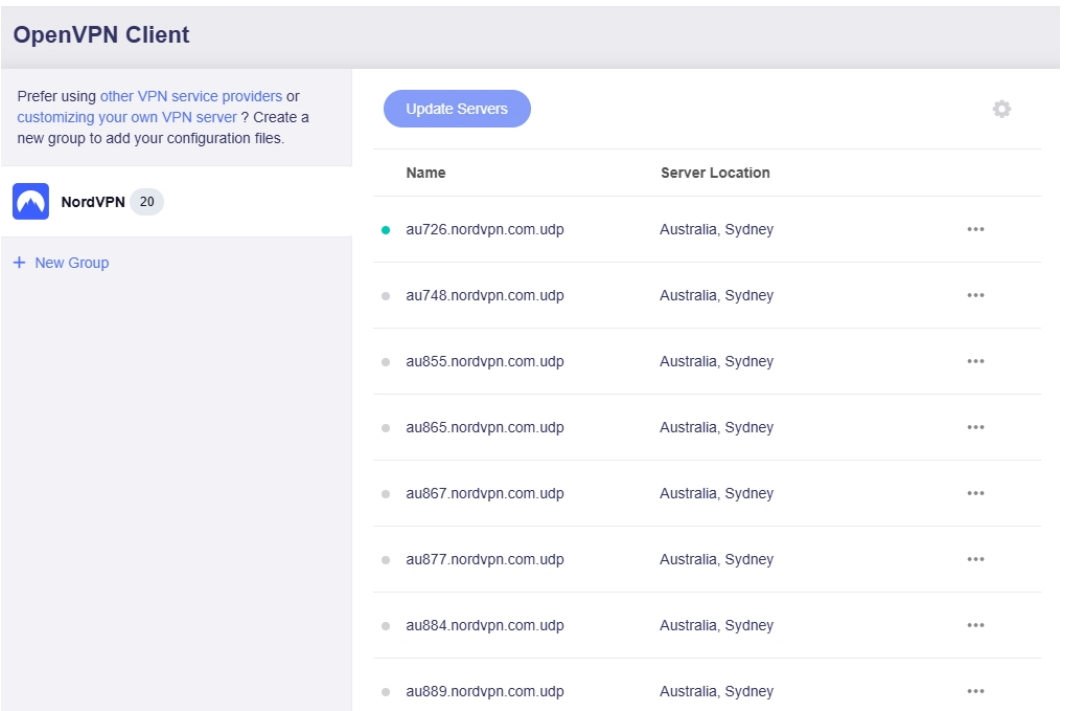
Die Konfigurationsdateien werden heruntergeladen.



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



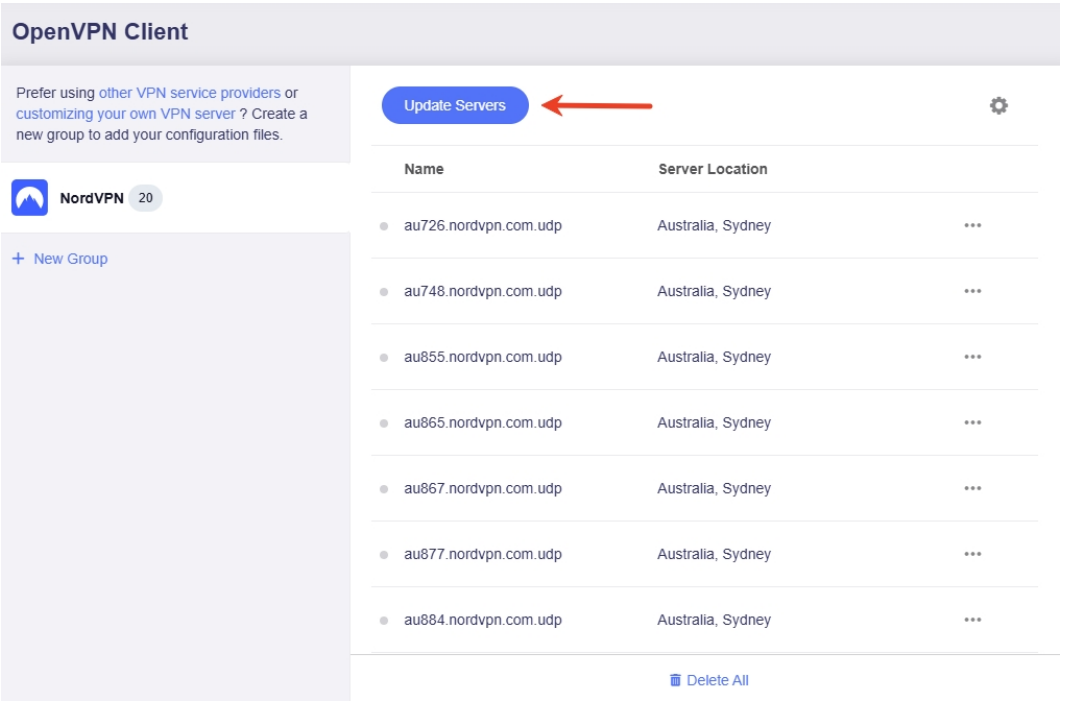
6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

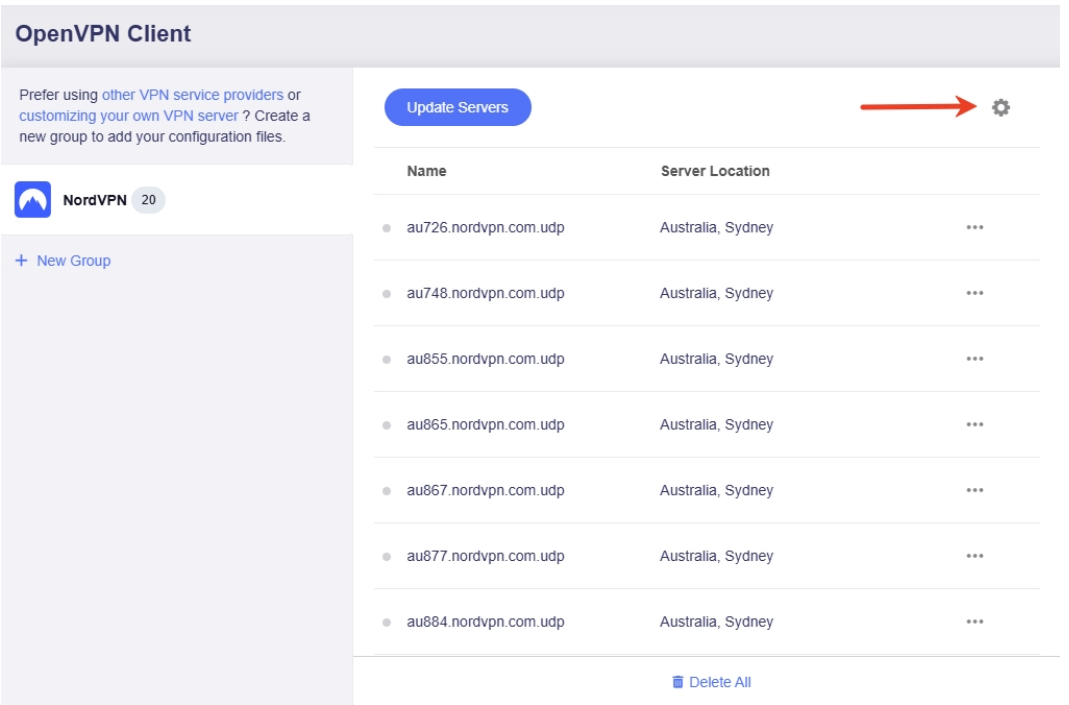
7. Server aktualisieren.

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



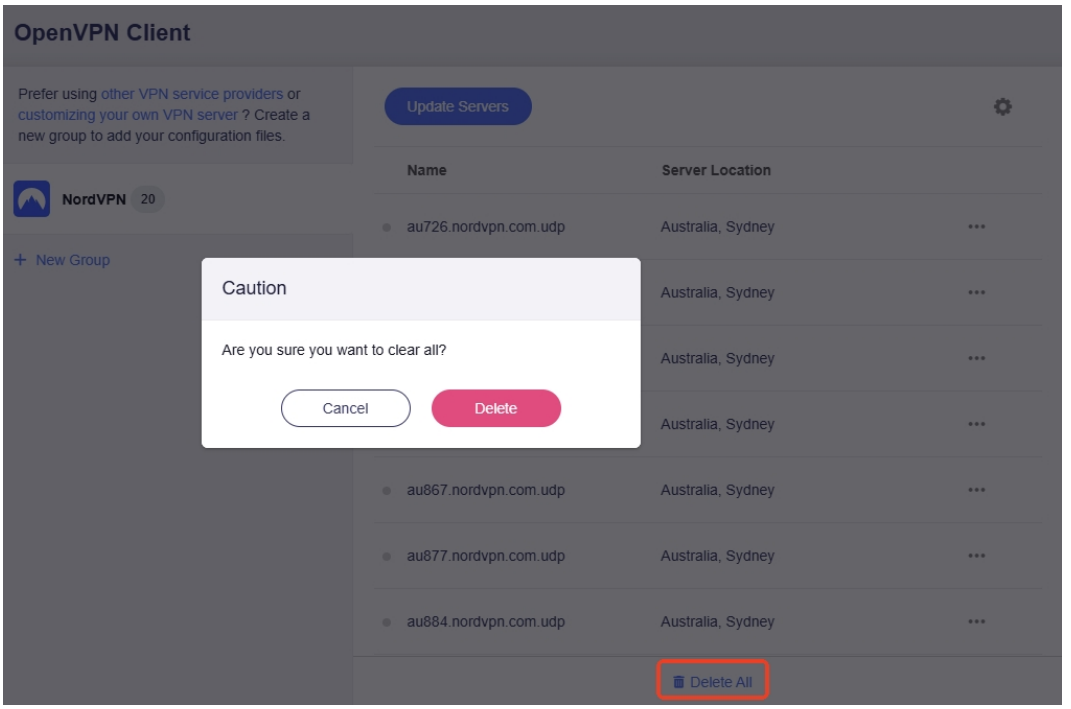
8. Zugangsdaten bearbeiten.

   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.

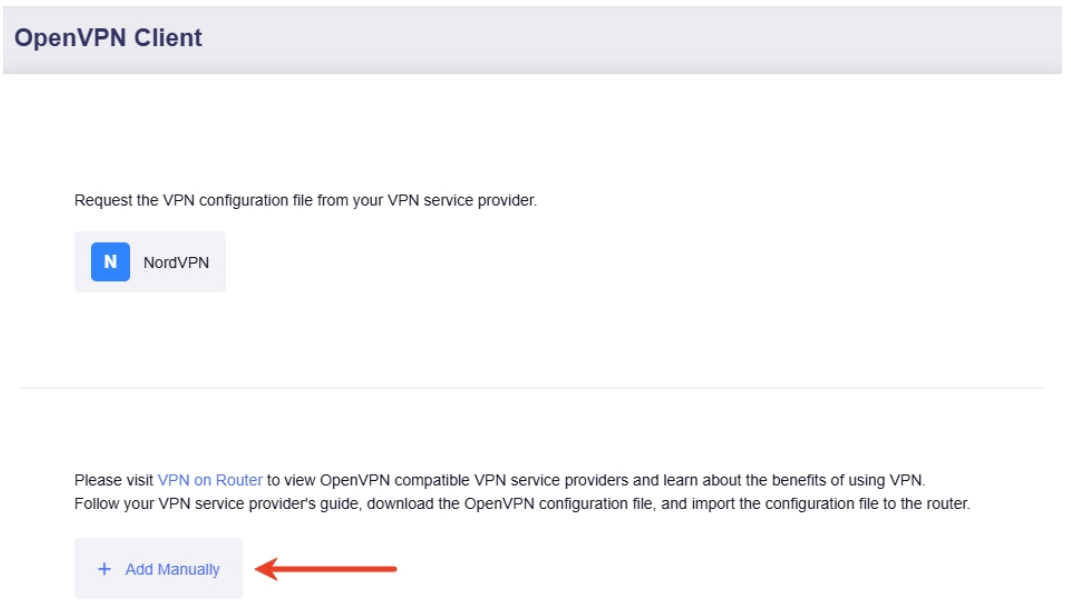

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

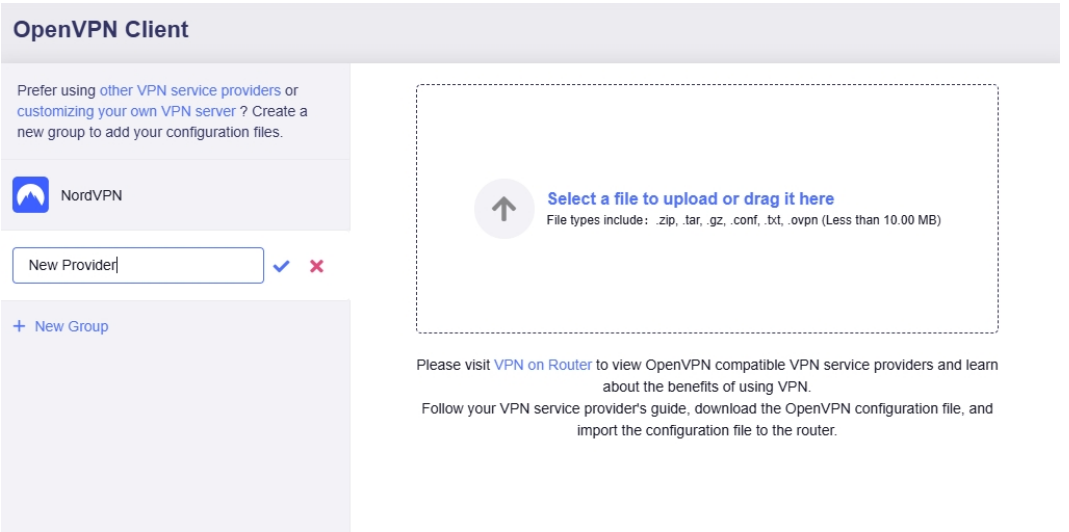
Wenn Ihr OpenVPN-Anbieter nicht in unsere Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den OpenVPN-Client einzurichten.

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

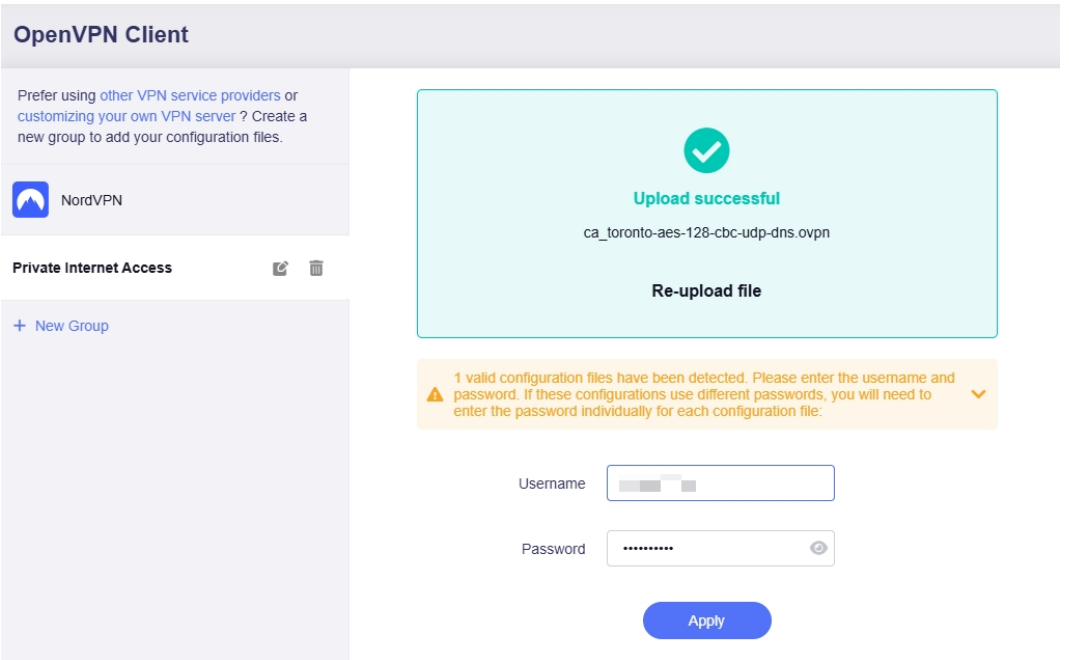
1. Laden Sie eine Konfigurationsdatei von der offiziellen Webseite von Private Internet Access herunter.
2. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Client** und klicken Sie auf **Add Manually**.



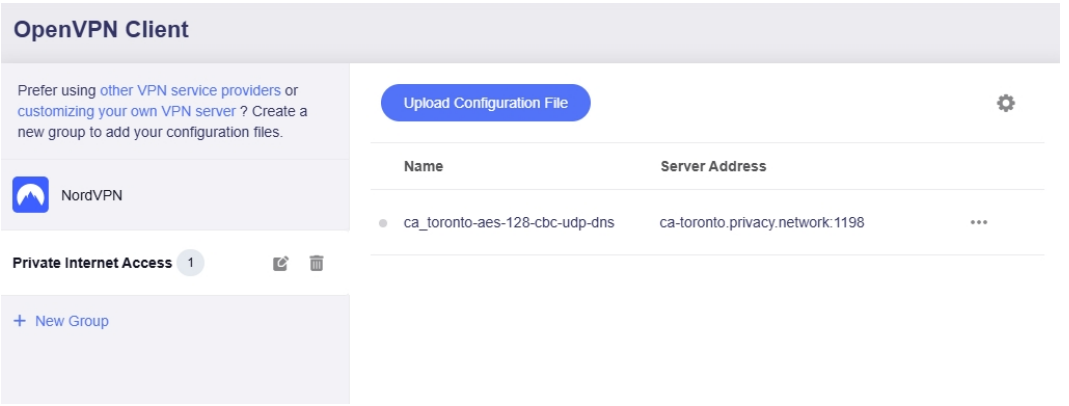
3. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



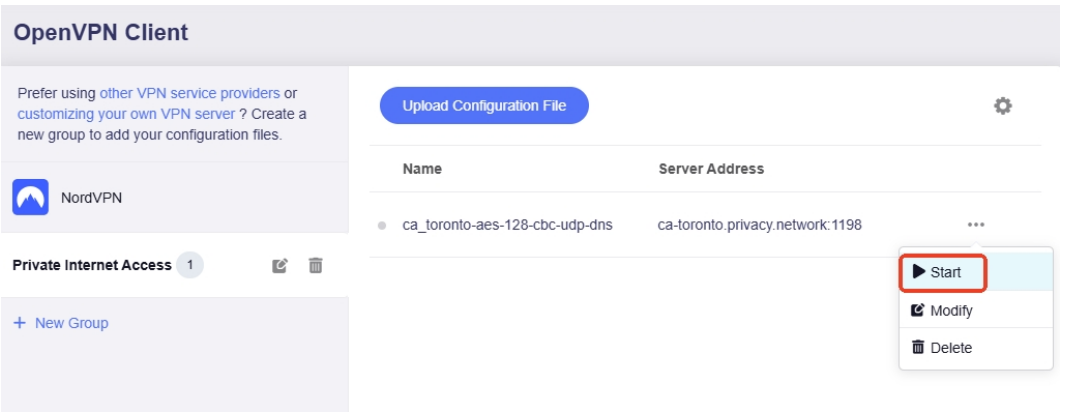
4. Laden Sie Ihre OpenVPN-Konfigurationsdatei hoch. Geben Sie bei Bedarf die Zugangsdaten ein und klicken Sie auf **Apply**.



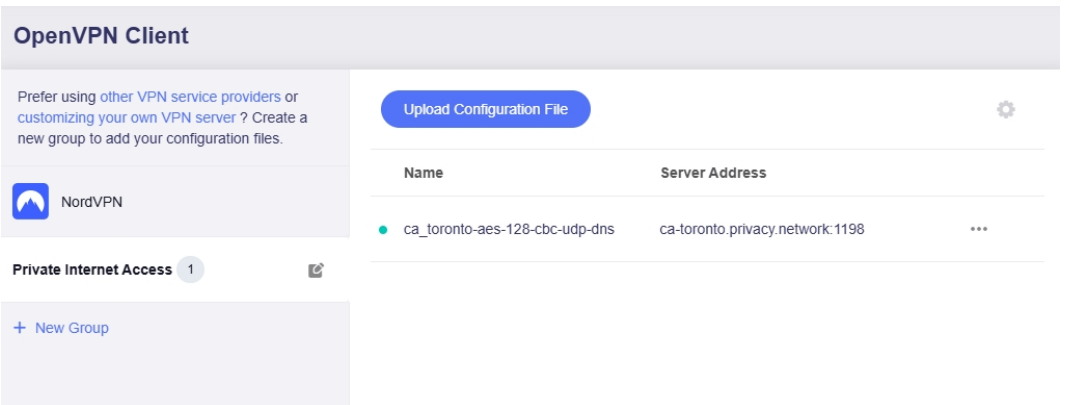
Die hochgeladene Konfigurationsdatei wird angezeigt.



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.

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.

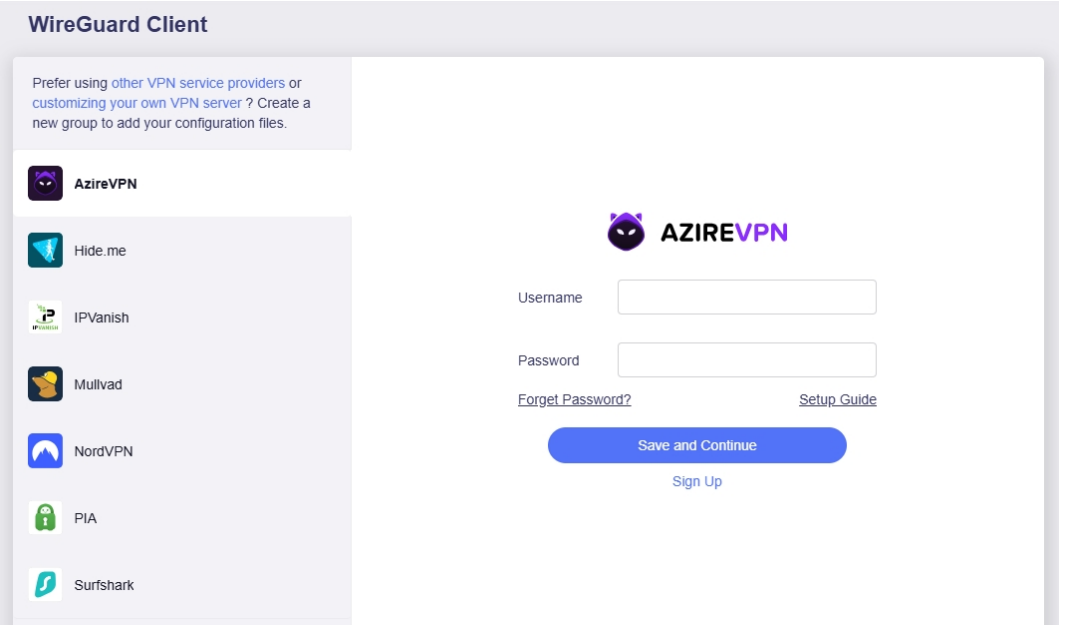
Wählen Sie nachstehend Ihren WireGuard-Anbieter aus, um direkt zur passenden Schritt-für-Schritt-Anleitung zu gelangen.

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

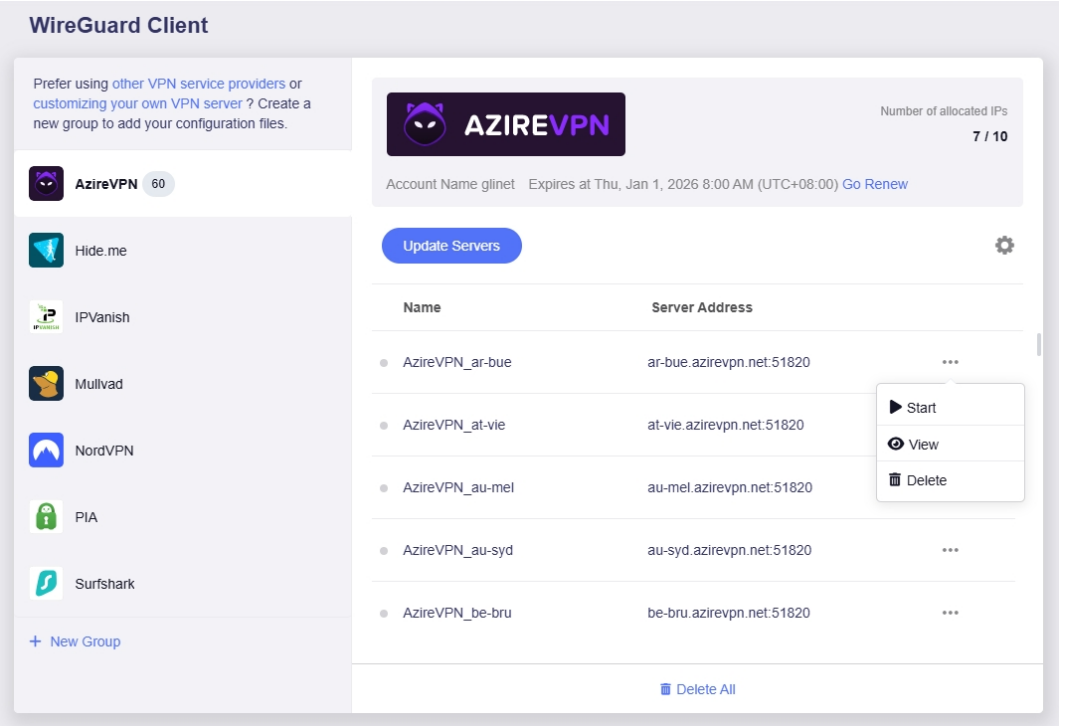
11.2.2 AzireVPN einrichten

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

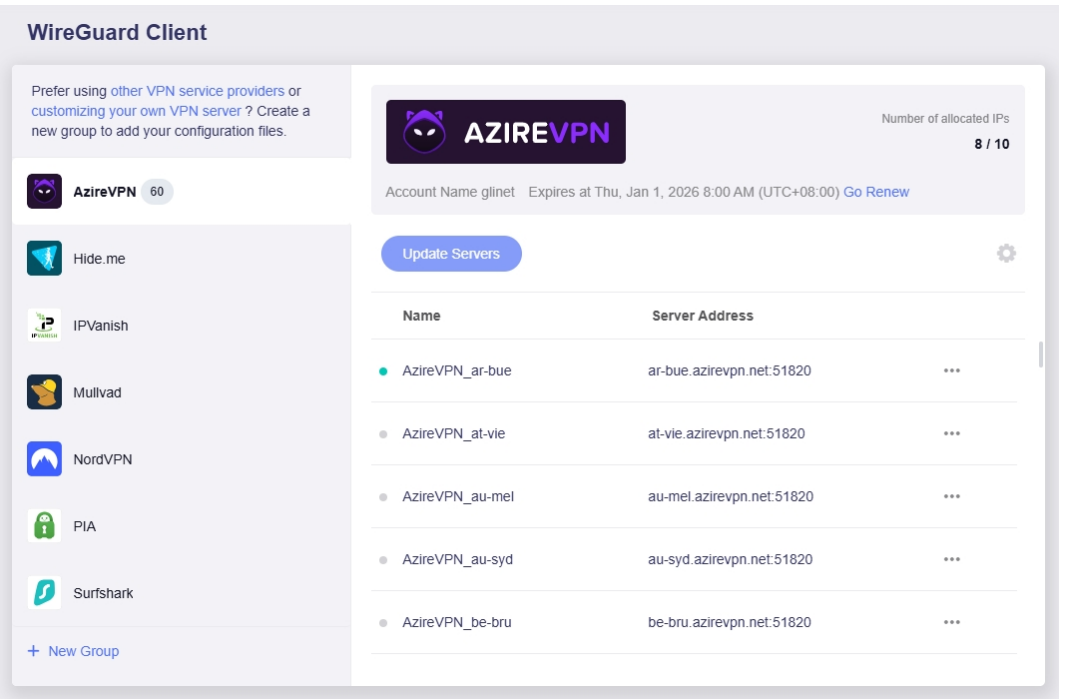
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **AzireVPN**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



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



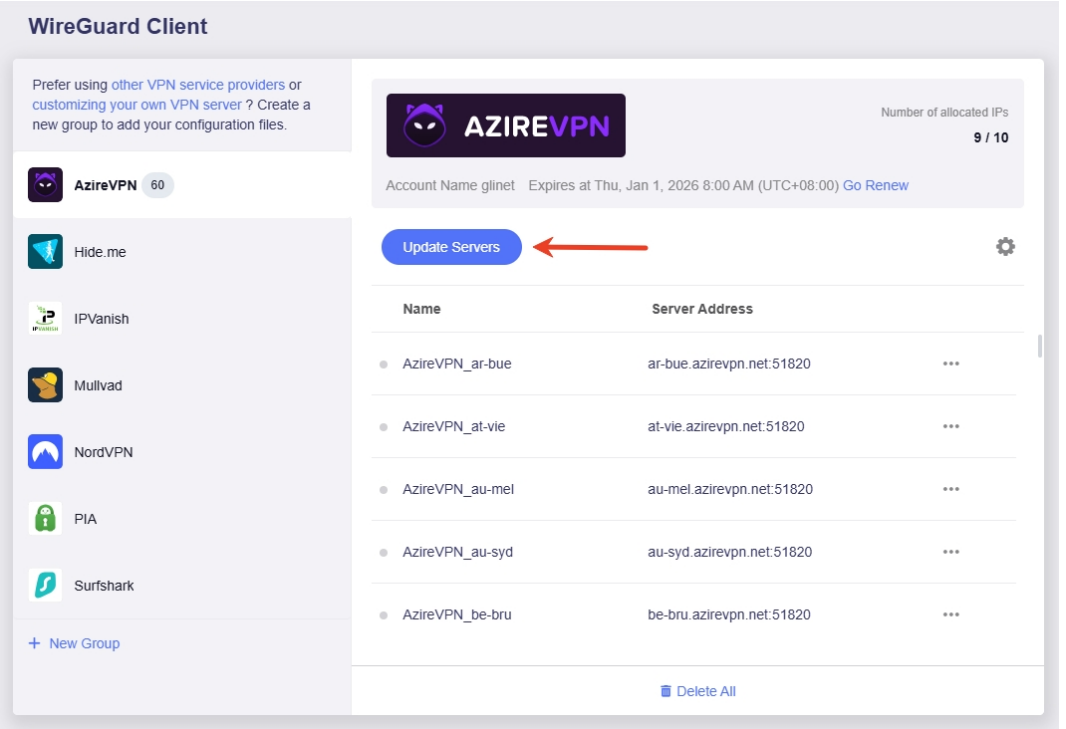
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

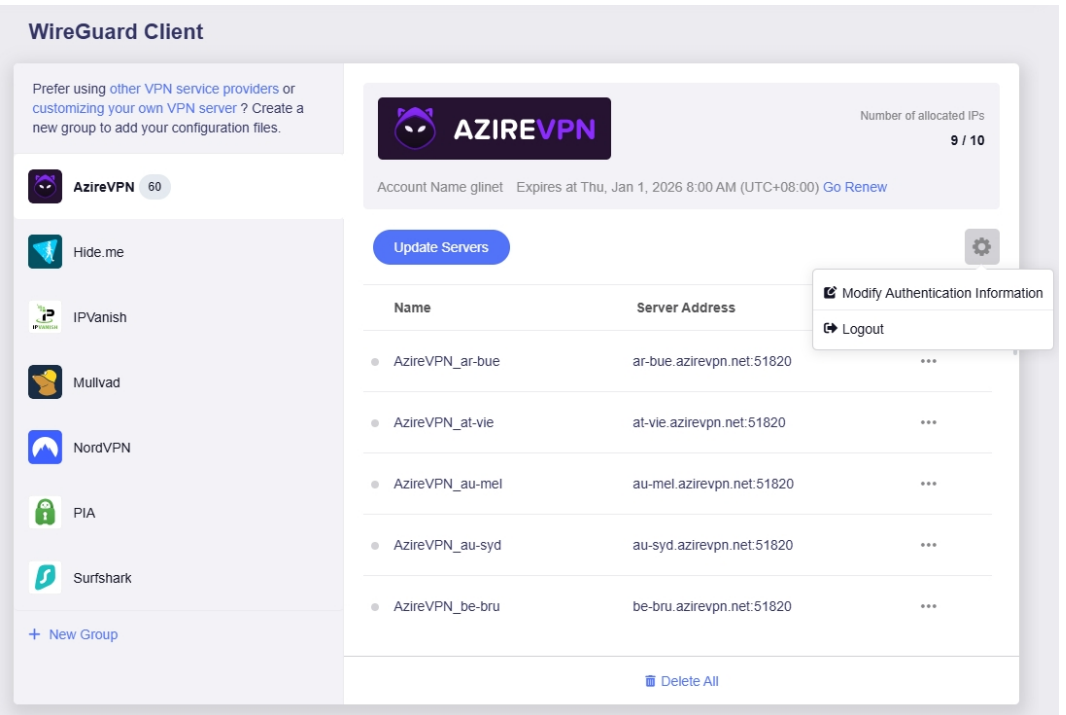
5. Server aktualisieren.

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



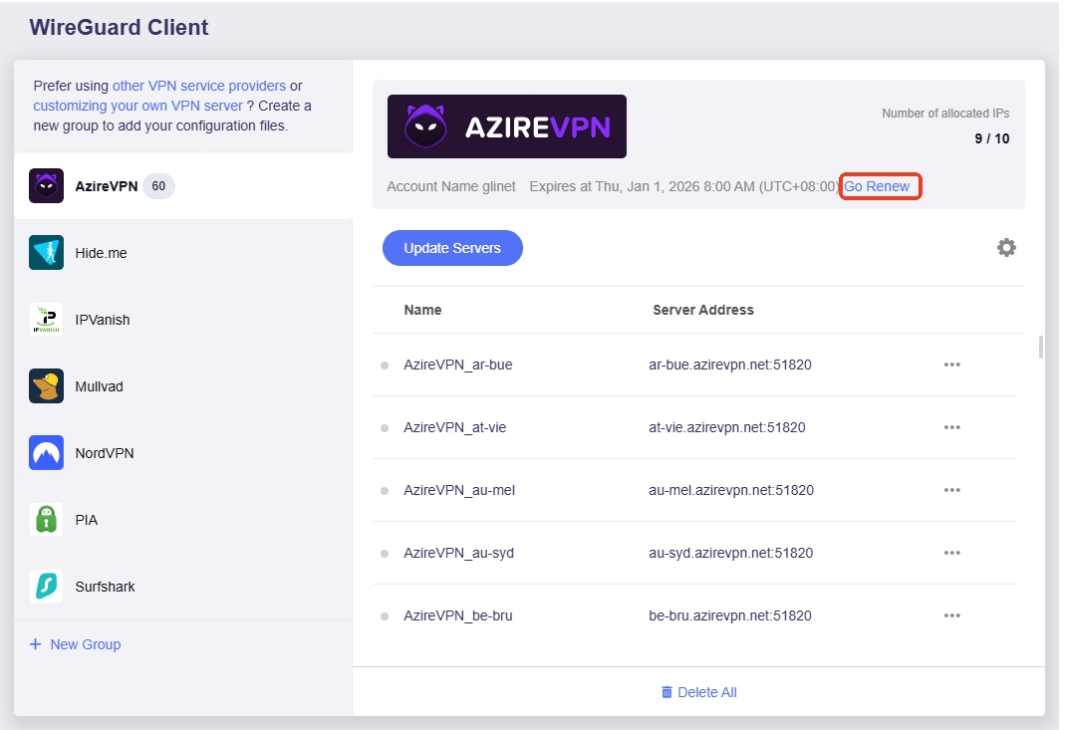
6. Zugangsdaten bearbeiten oder abmelden.

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

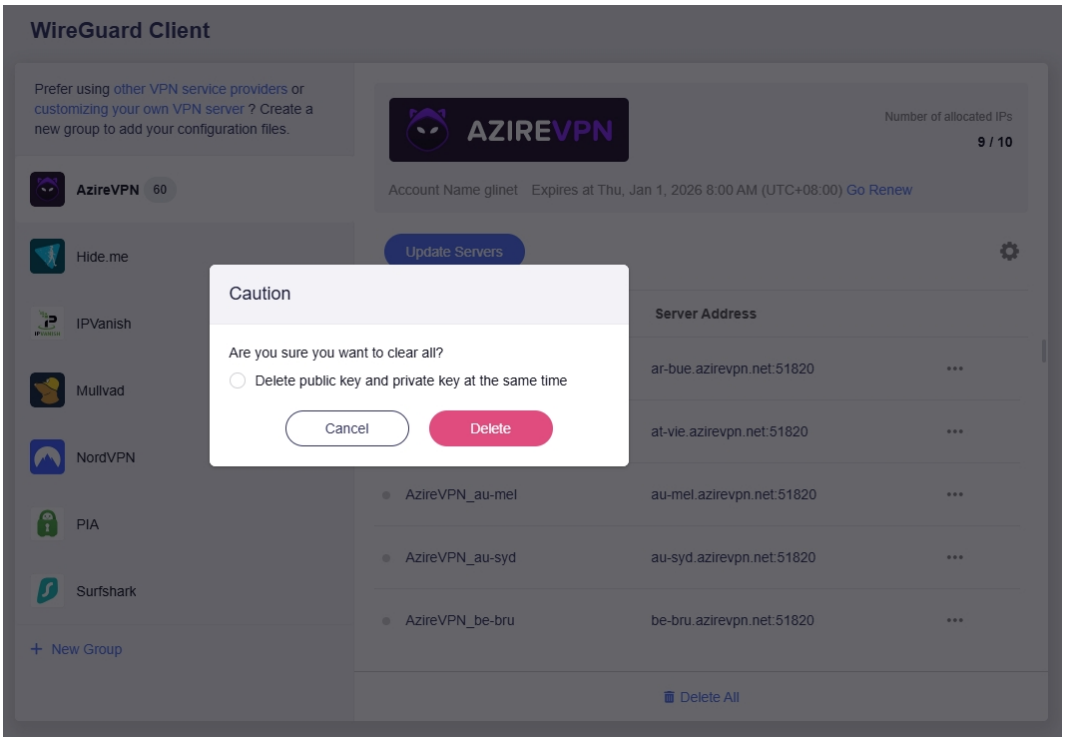


7. Abonnement verlängern.

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



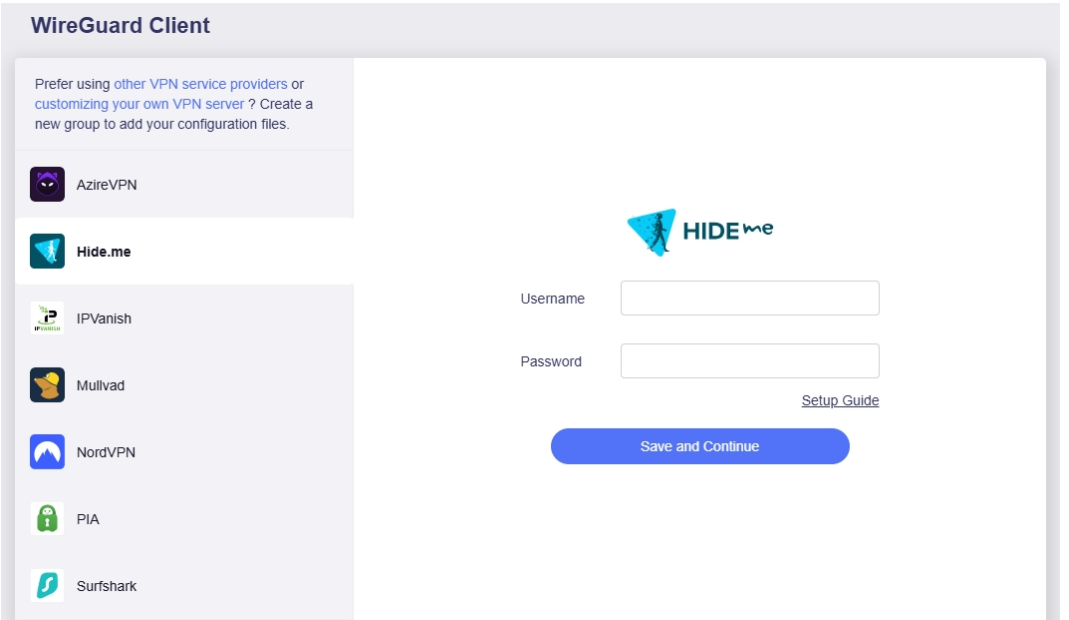
8. Alle Dateien löschen.
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


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

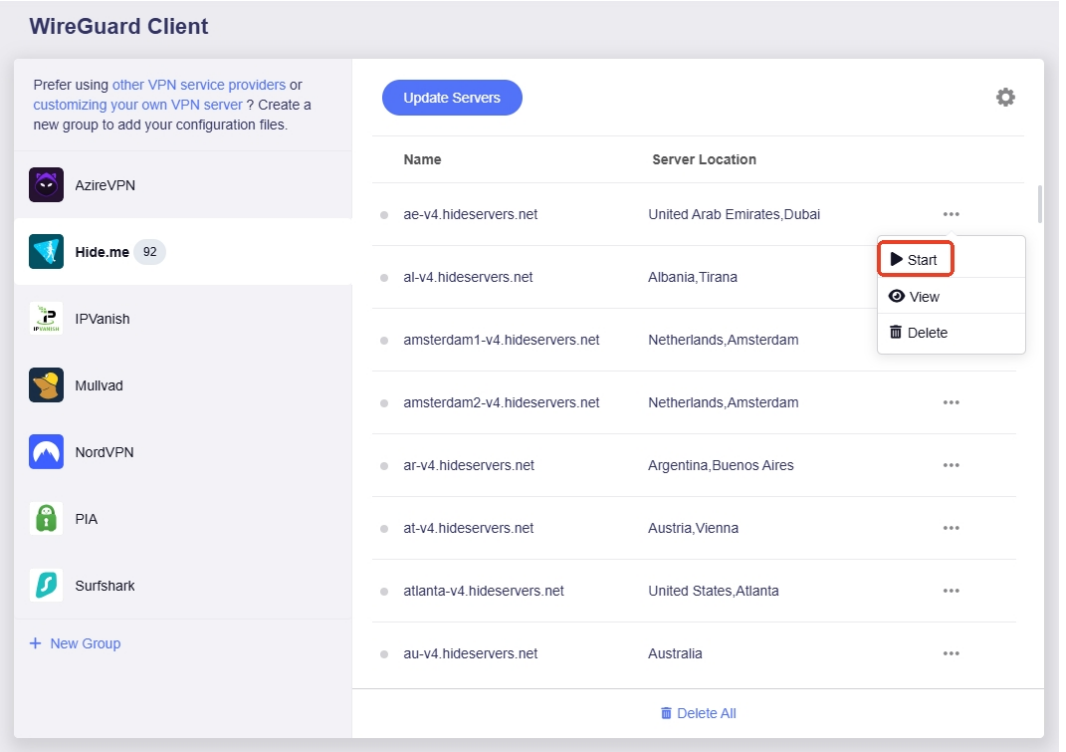
11.2.3 Hide.me einrichten

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

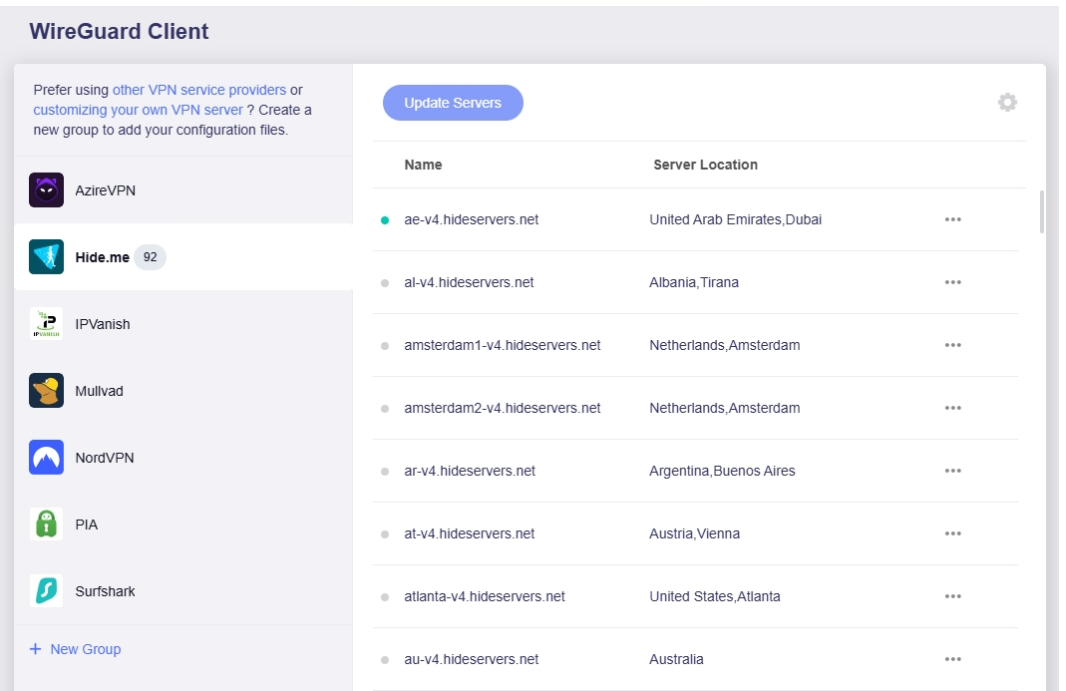
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Hide.me**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**. Für jeden Server werden Konfigurationsdateien erzeugt.



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



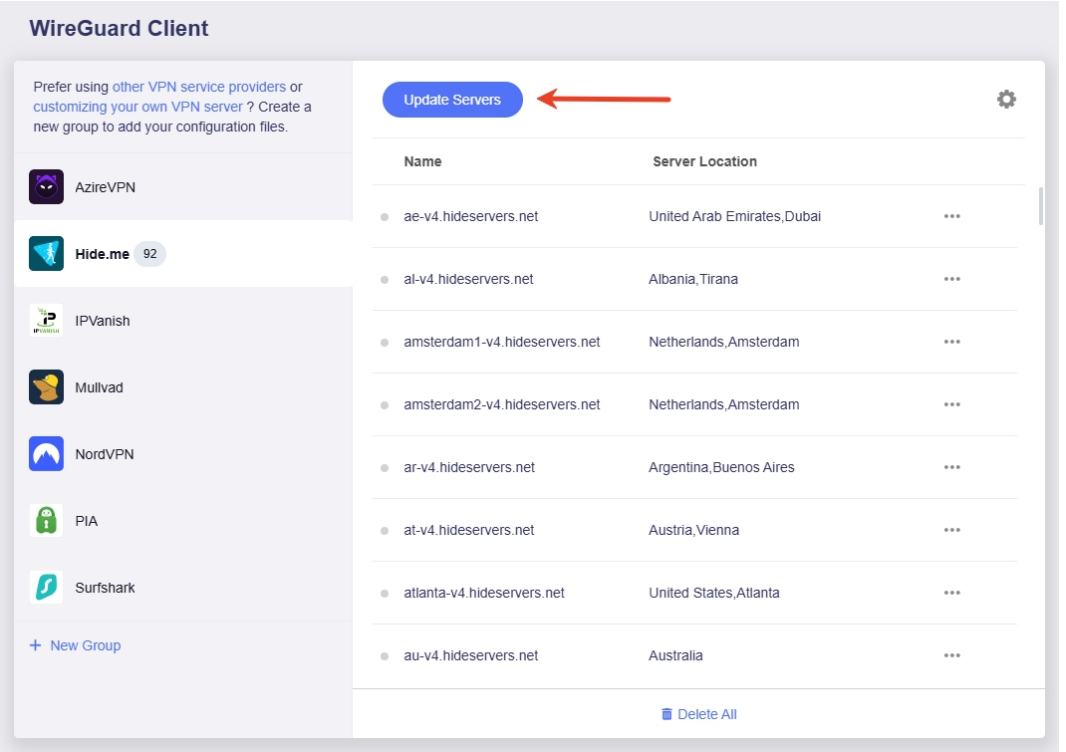
4. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

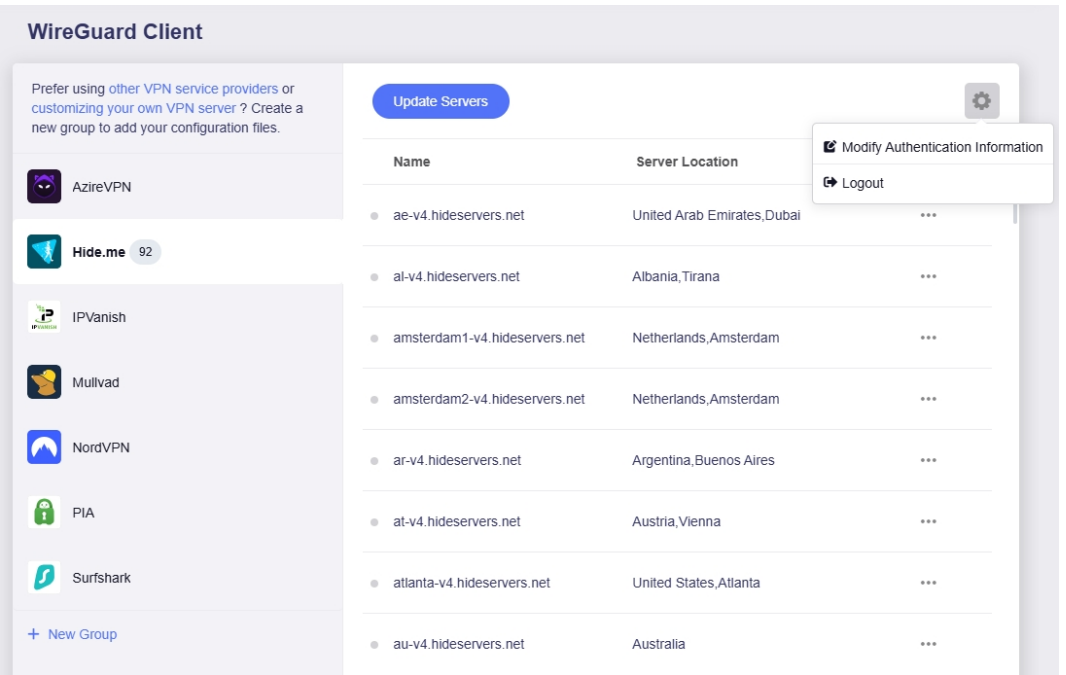
5. Server aktualisieren.

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



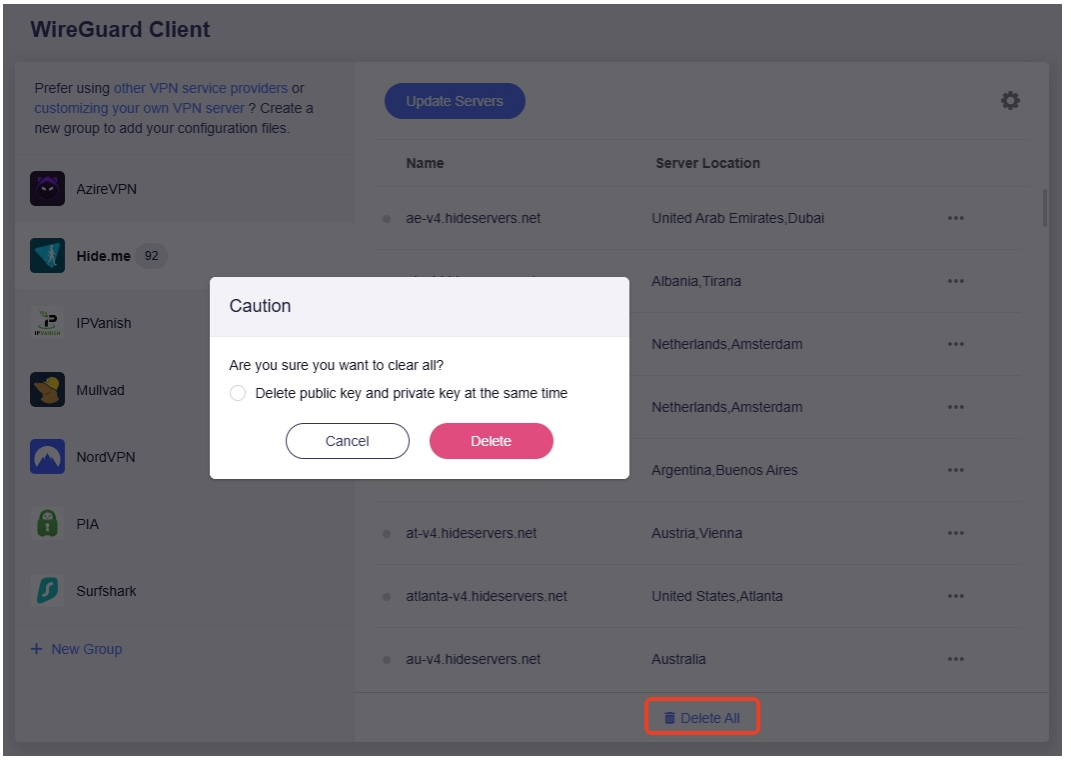
6. Zugangsdaten bearbeiten oder abmelden.

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



7. Alle Dateien löschen.

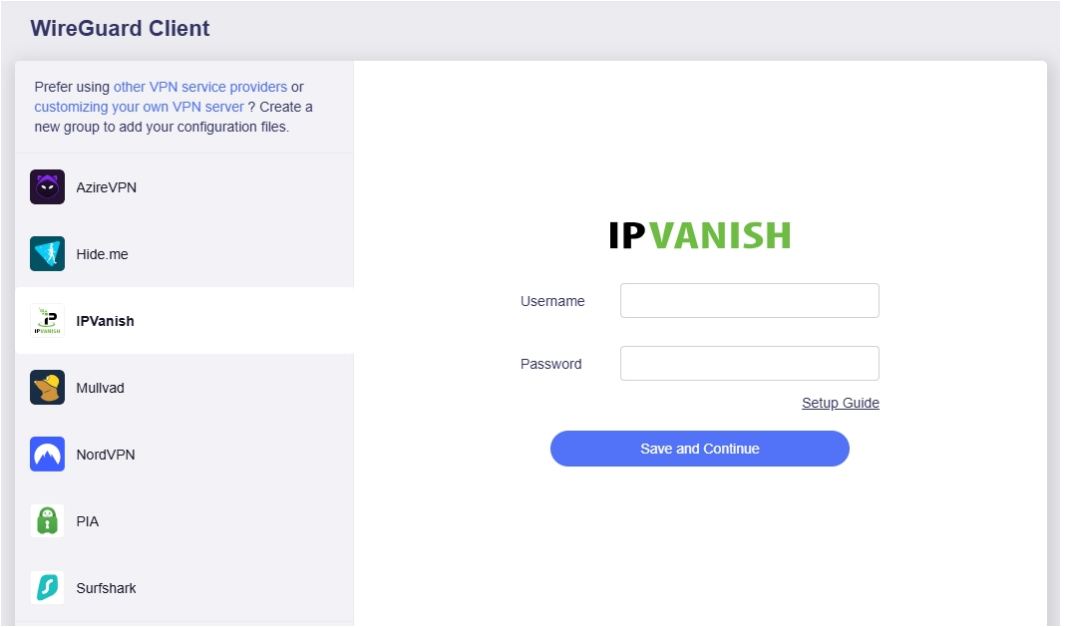
Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



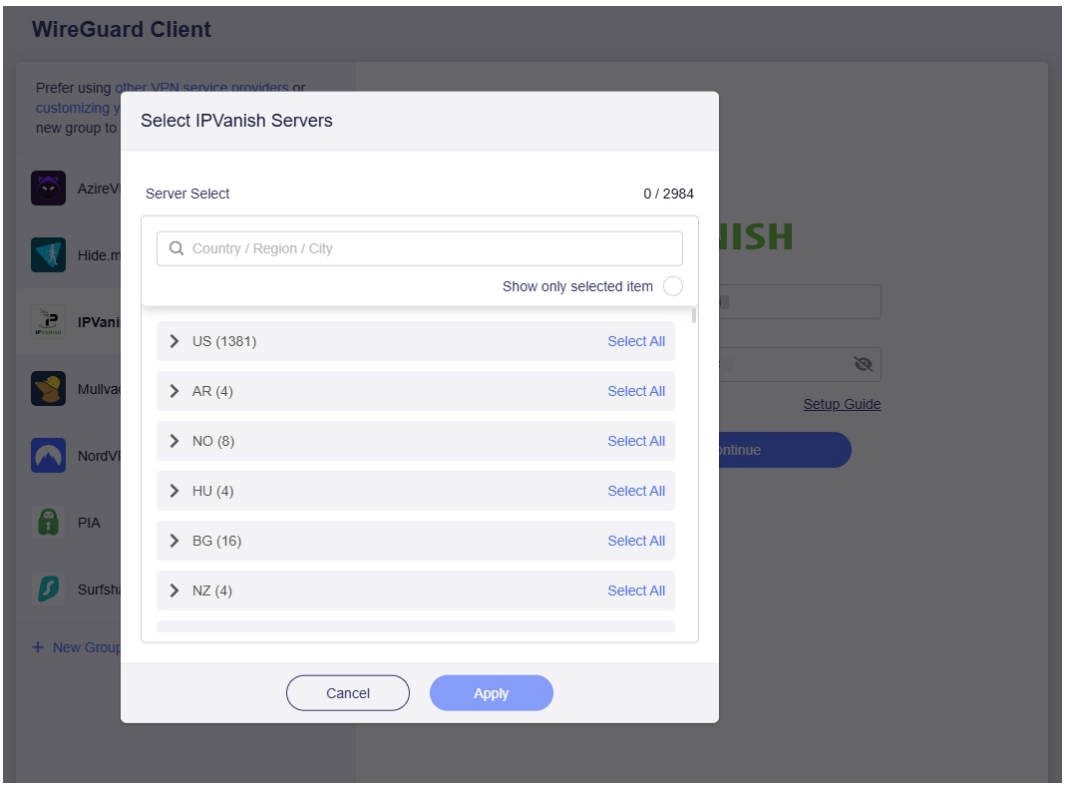
11.2.4 IPVanish einrichten

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

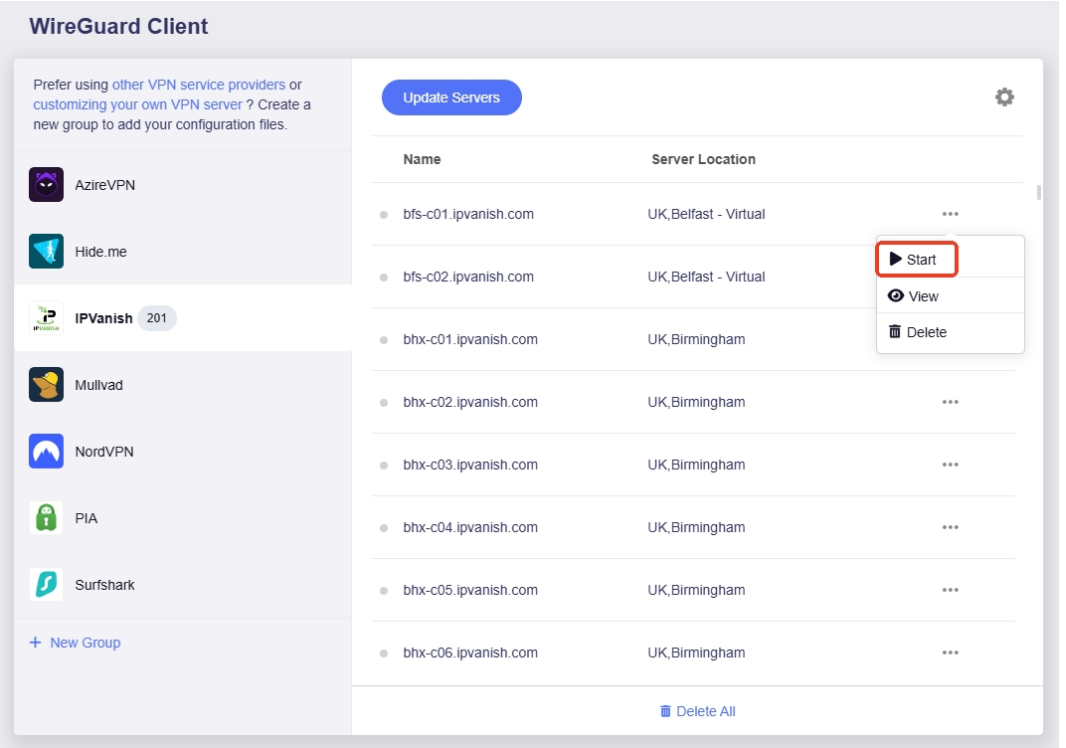
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **IPVanish**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



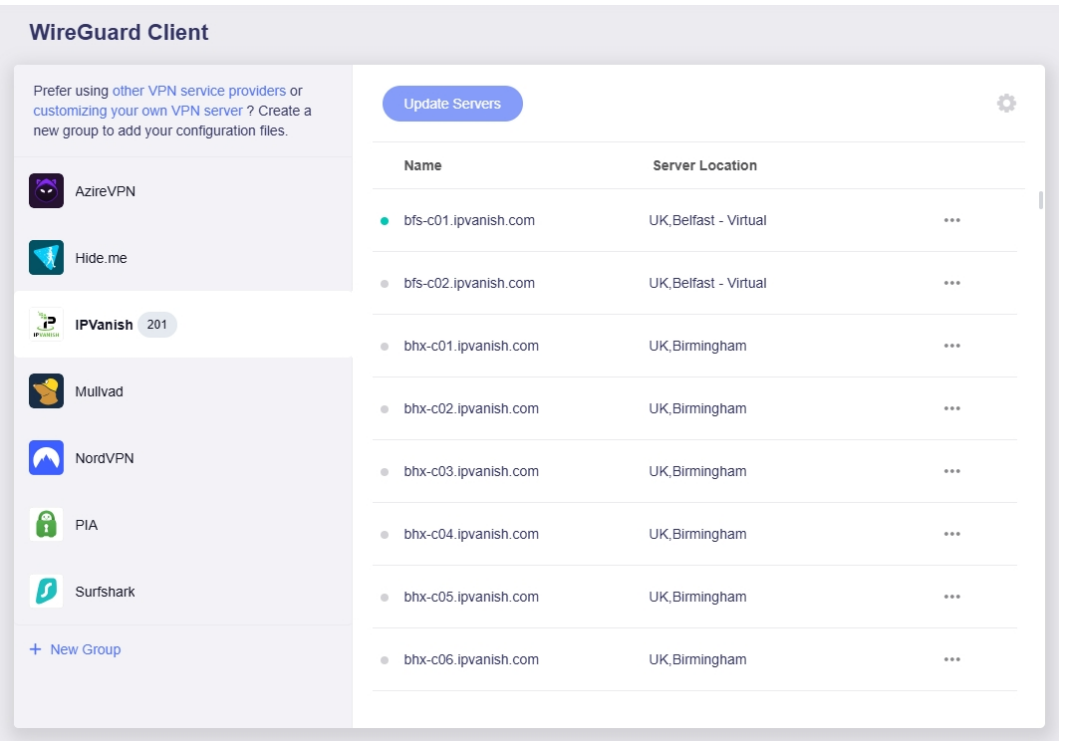
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



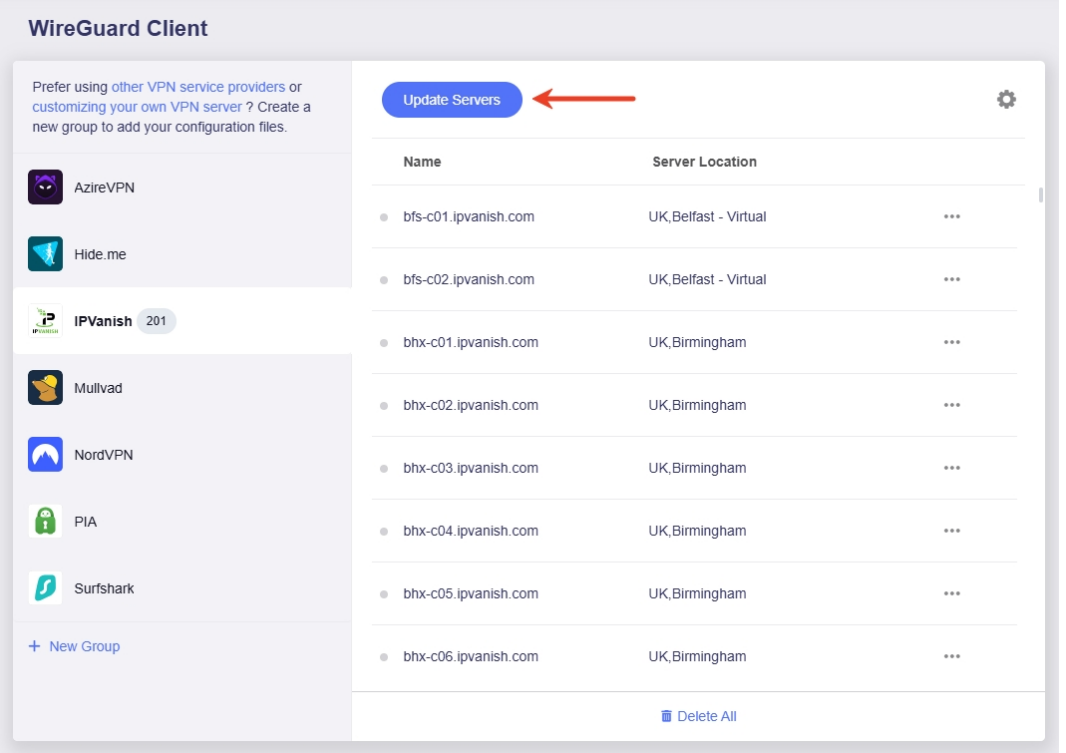
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



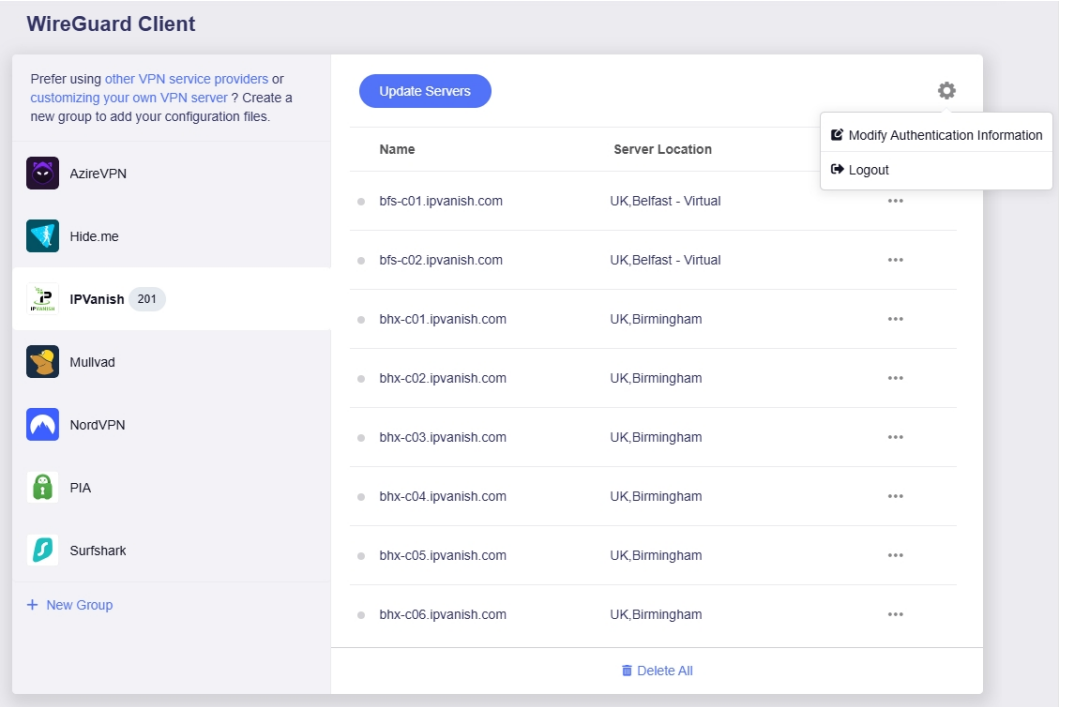
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

6. Server aktualisieren.

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

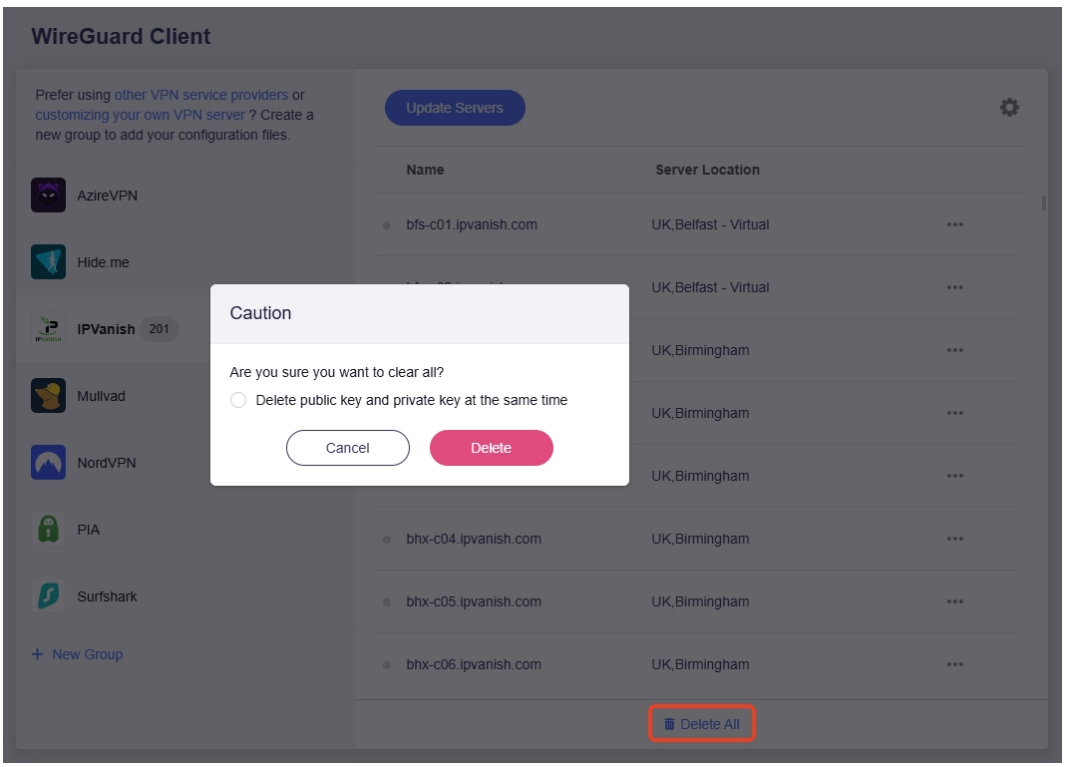


7. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



8. Alle Dateien löschen.

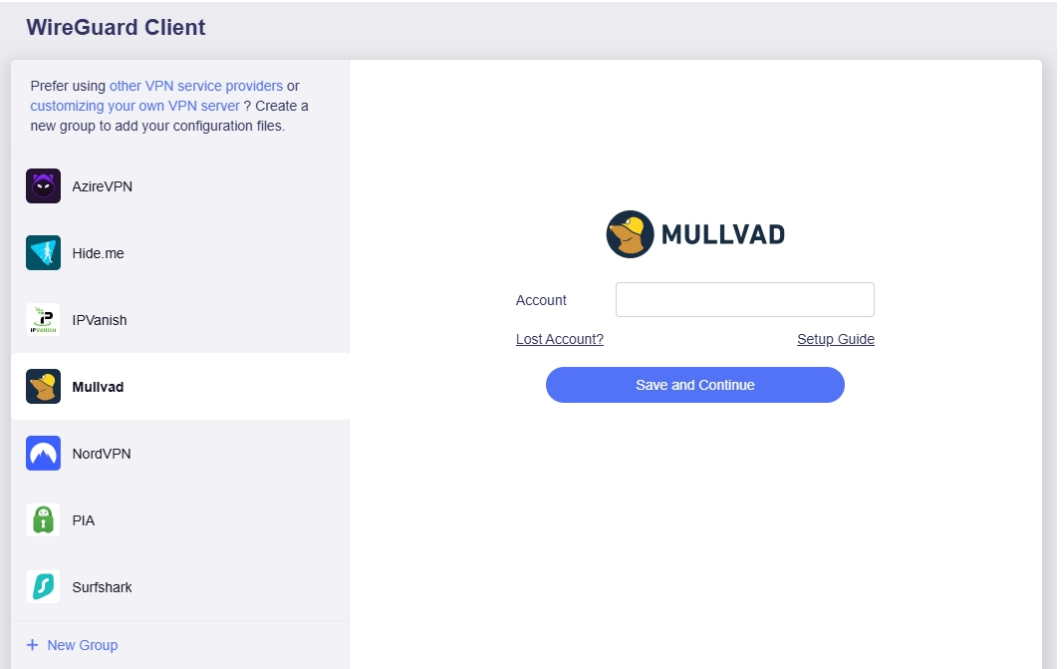
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



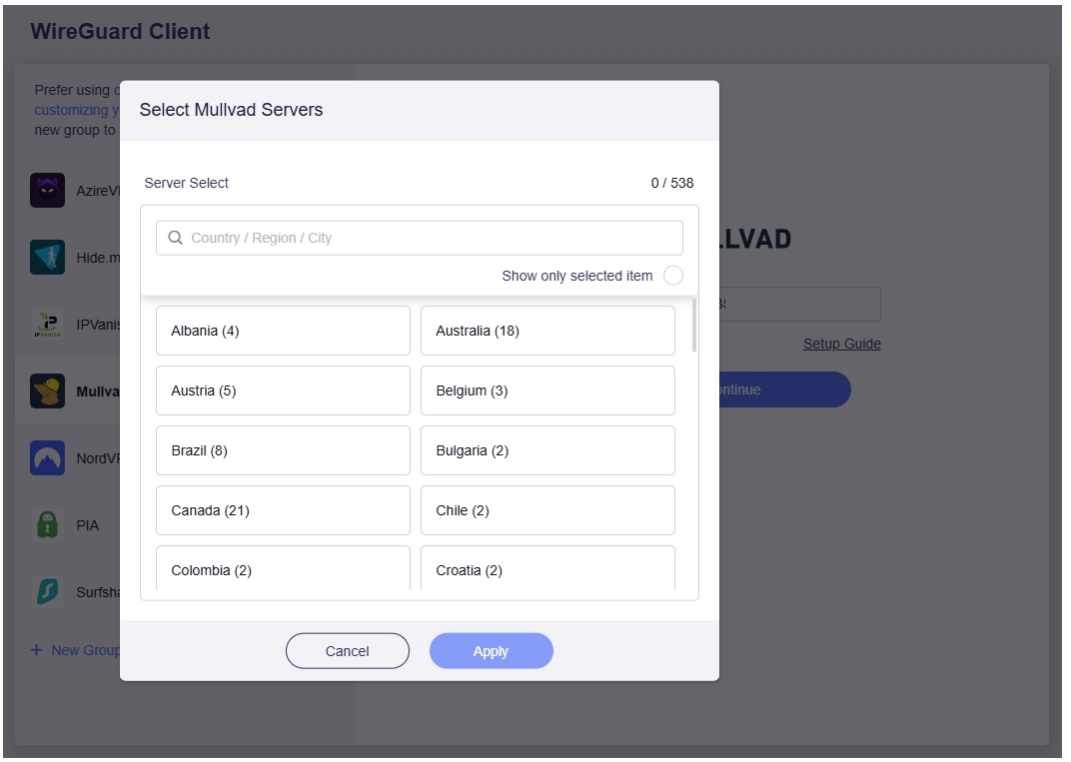
11.2.5 Mullvad einrichten

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

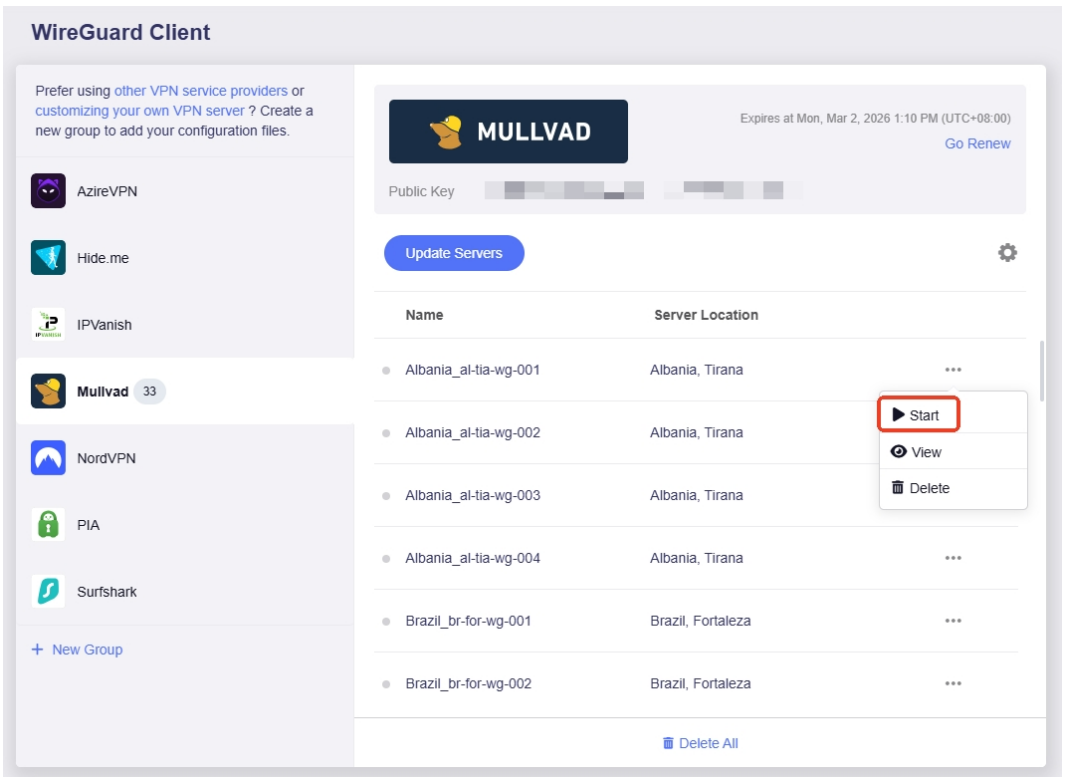
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Mullvad**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



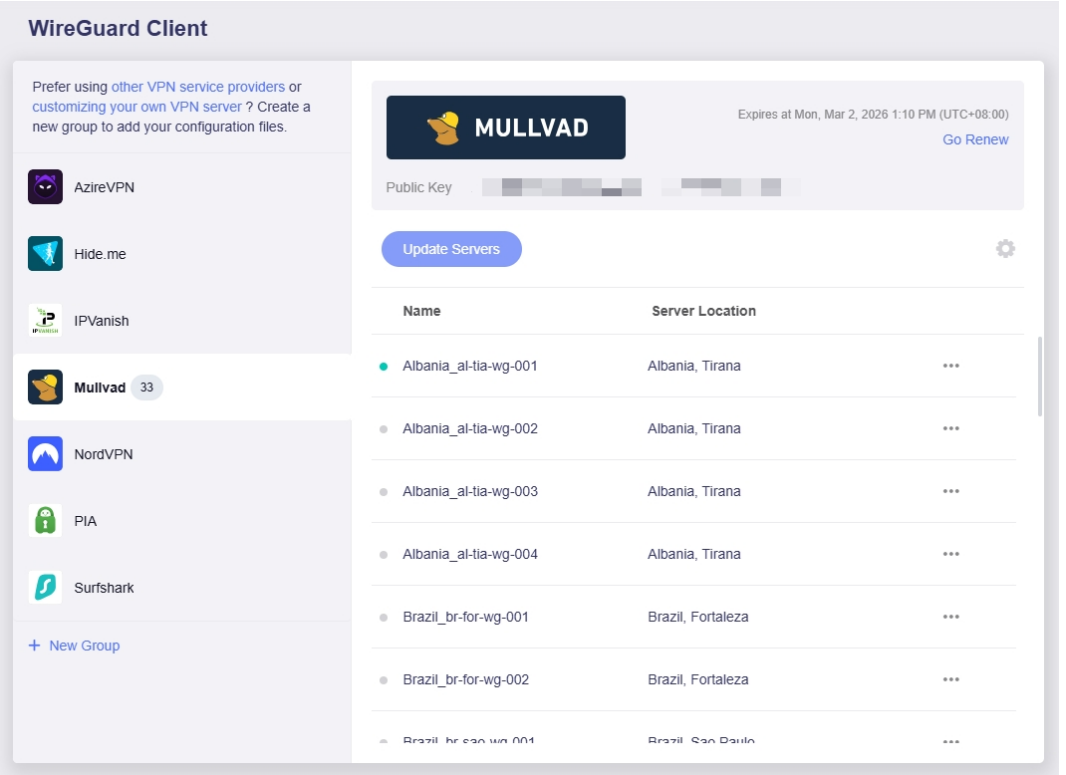
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



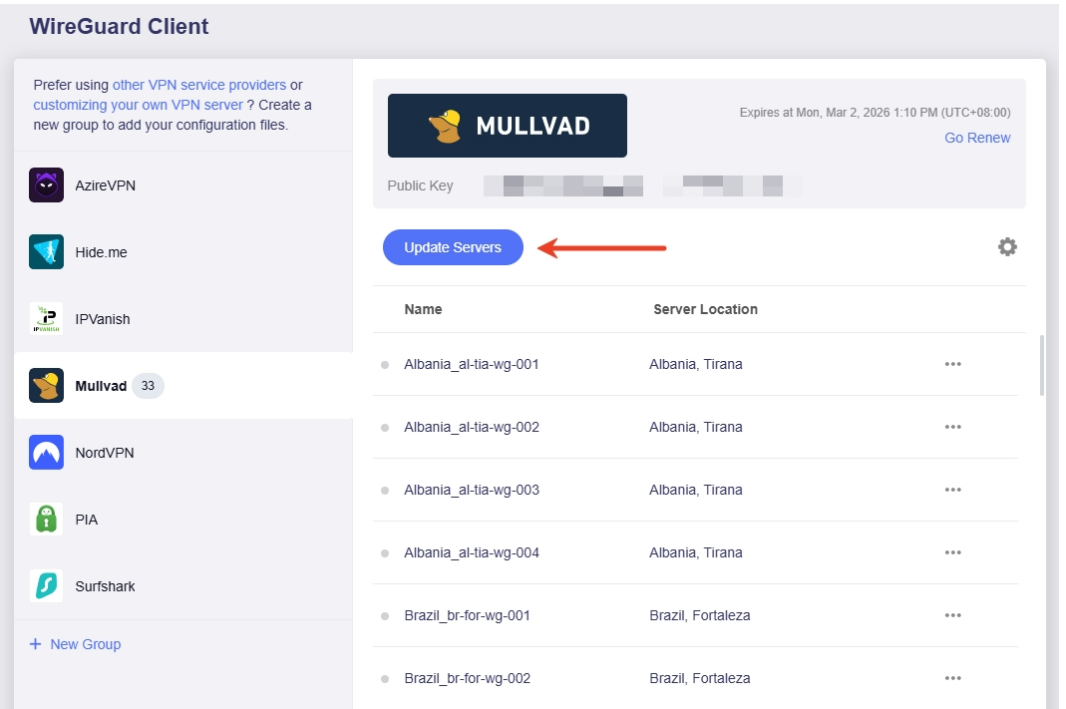
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

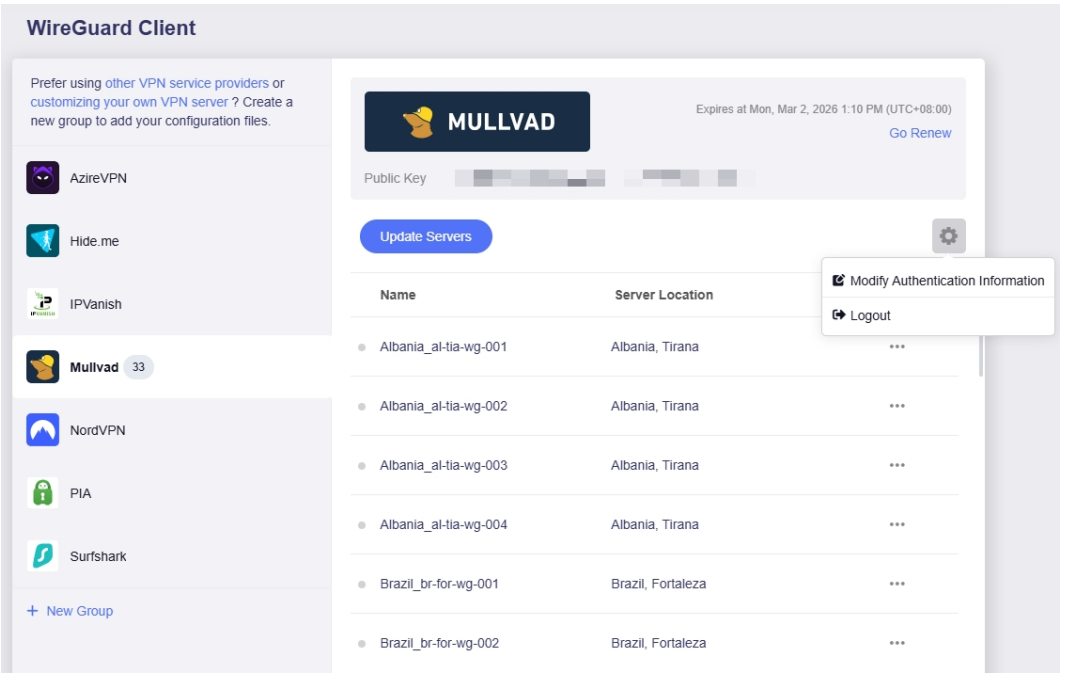
6. Server aktualisieren.

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



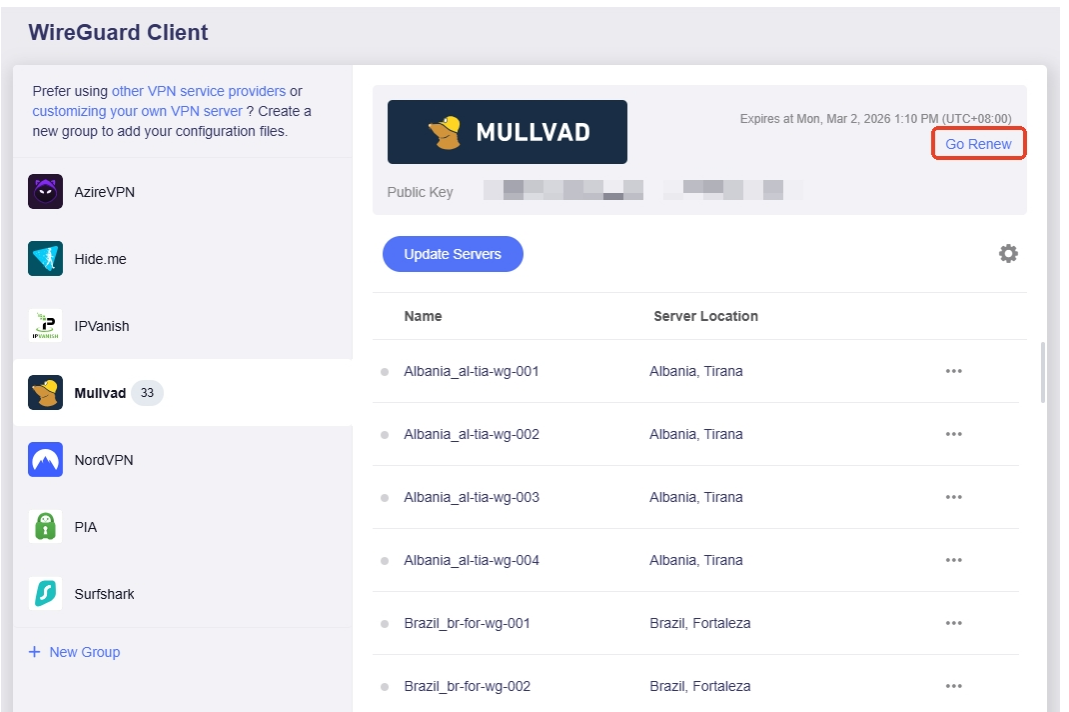
7. Zugangsdaten bearbeiten oder abmelden.

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



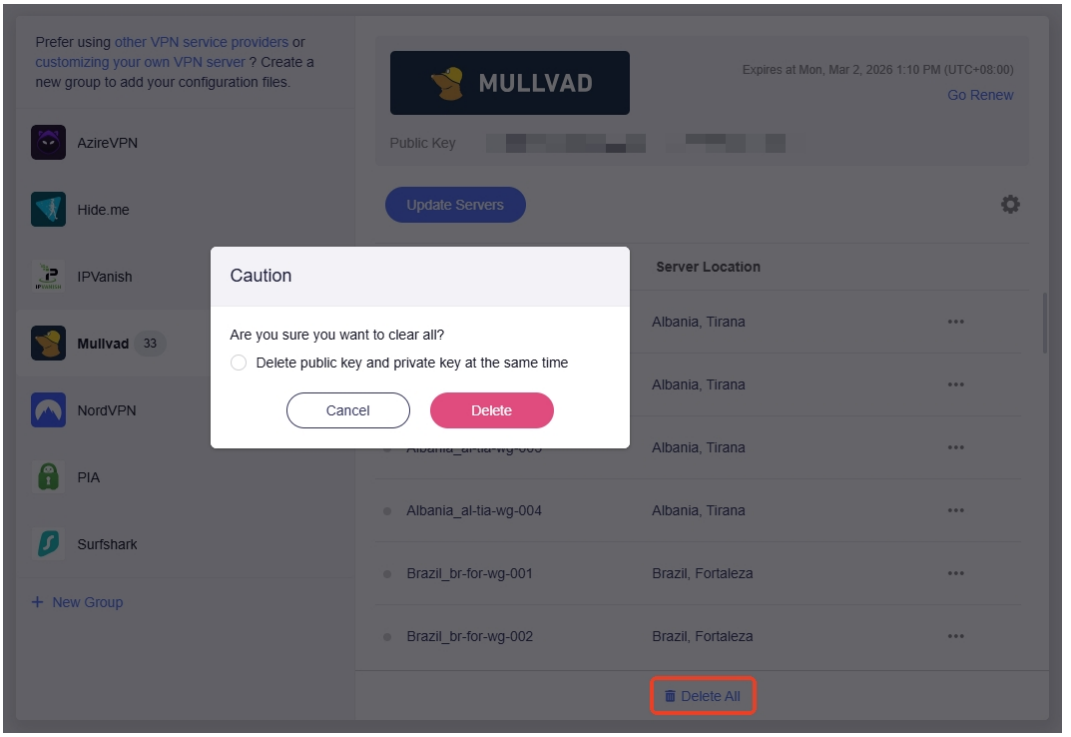
8. Abonnement verlängern.

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



9. Alle Dateien löschen.

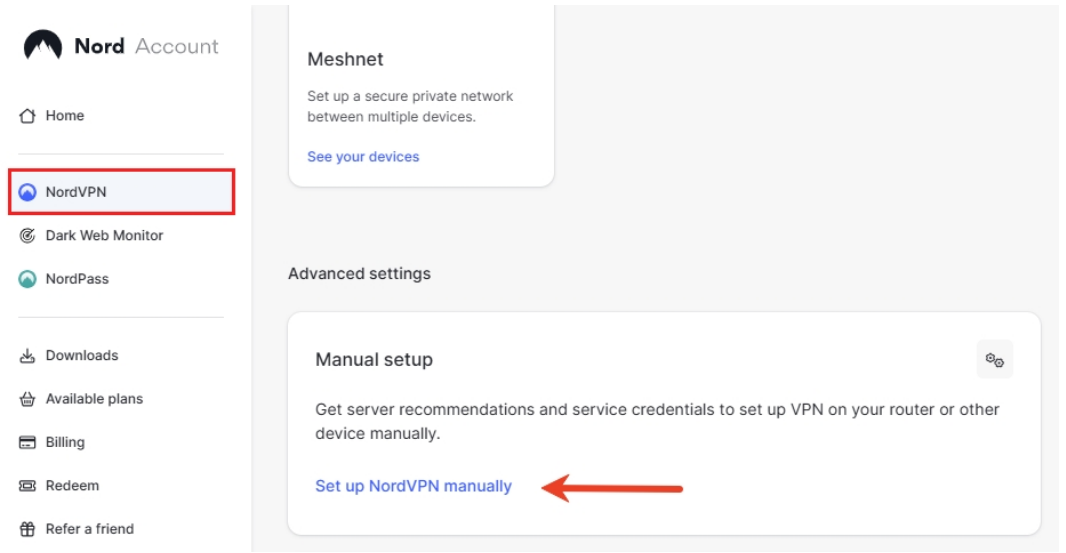
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



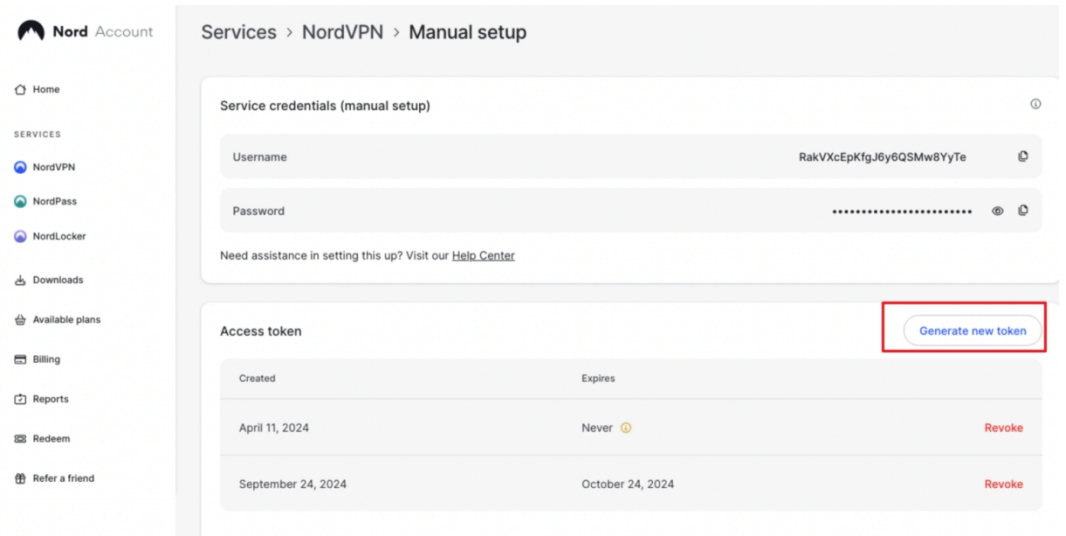
11.2.6 NordVPN einrichten

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

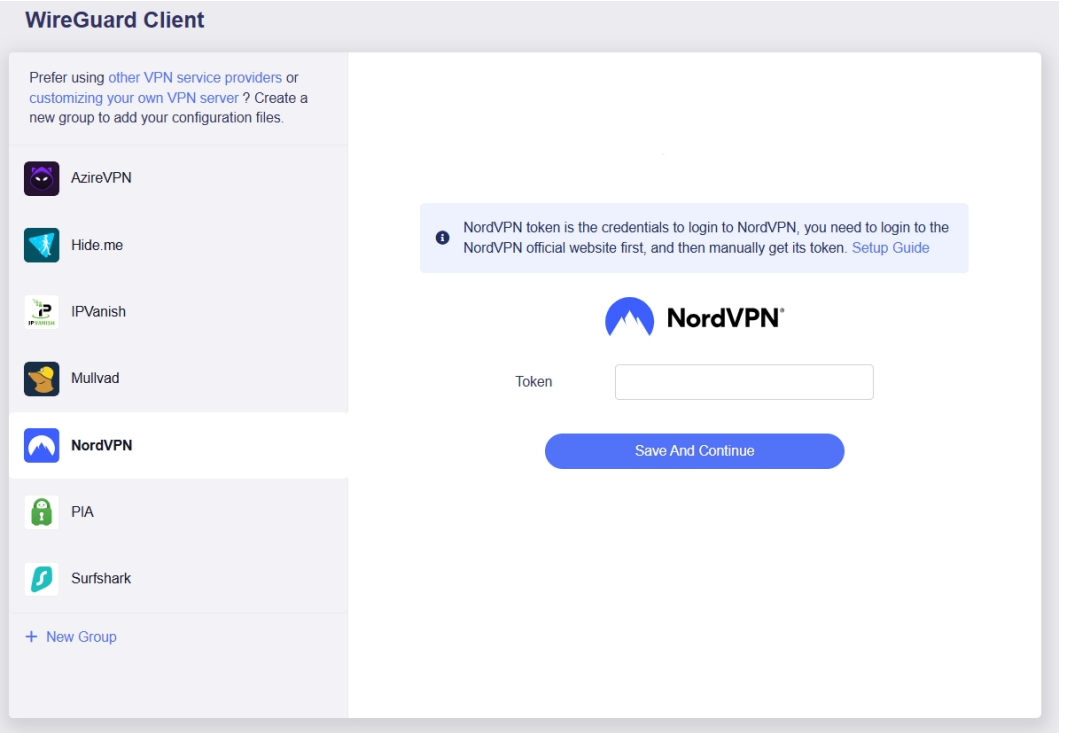
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



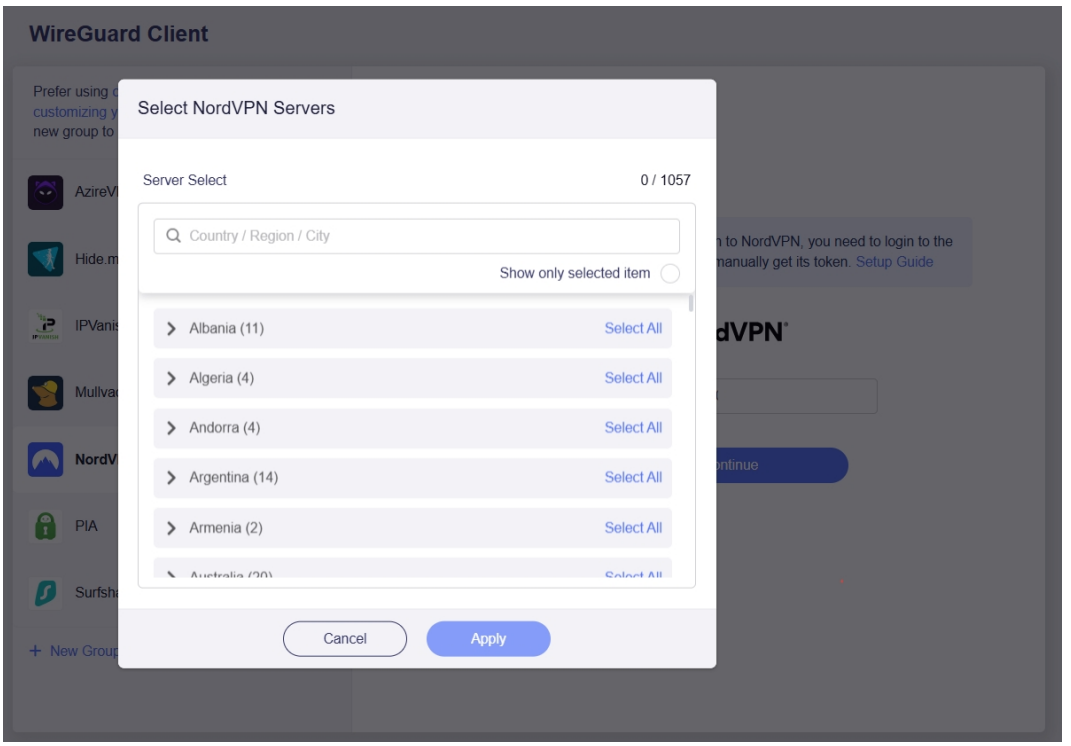
Dort finden Sie den Bereich **Access Token**. Erstellen Sie ein Zugriffstoken und kopieren Sie es zur späteren Verwendung.



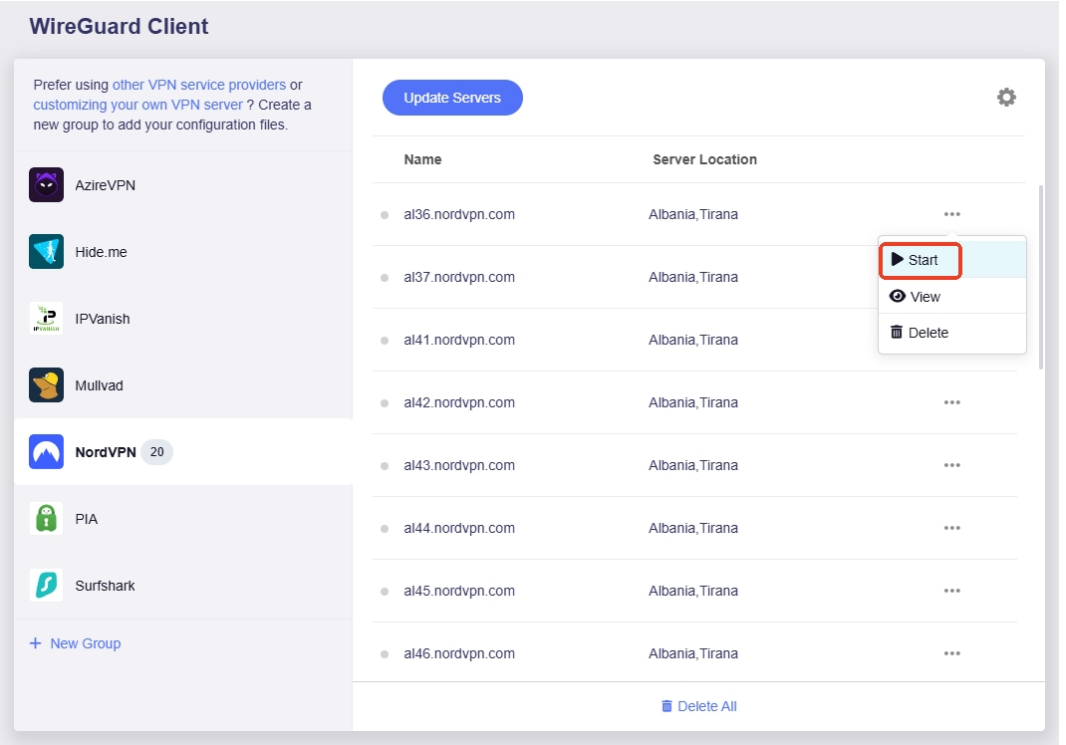
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **NordVPN**.
4. Geben Sie das Token ein und klicken Sie auf **Save and Continue**.



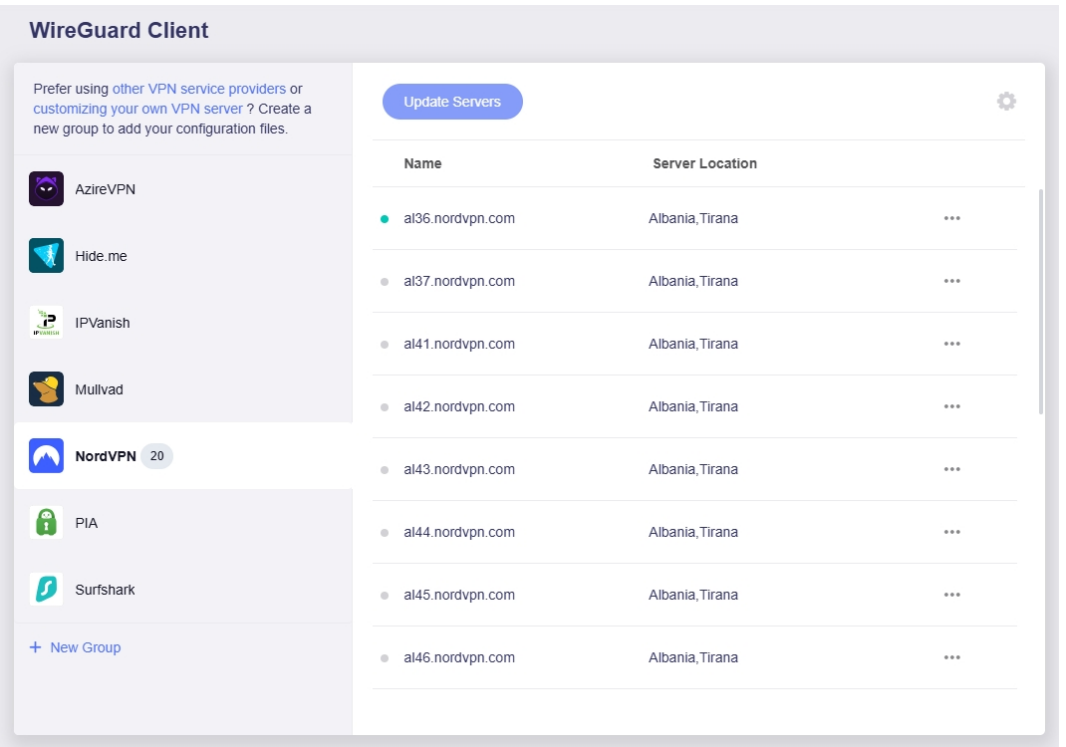
5. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



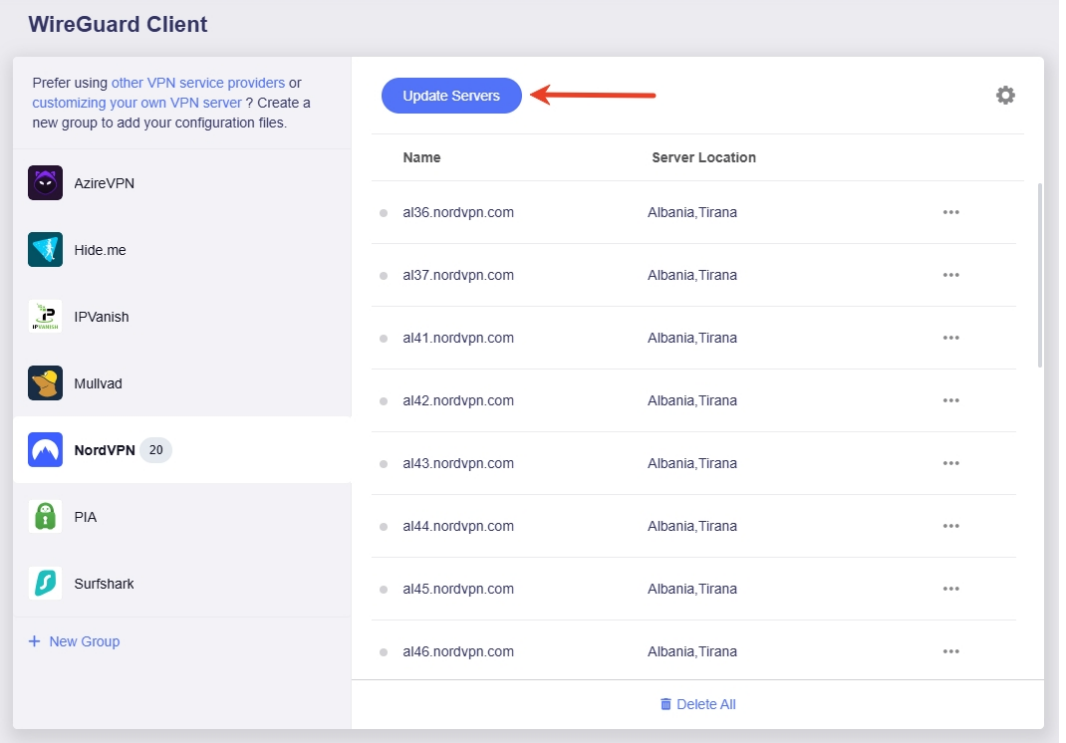
7. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



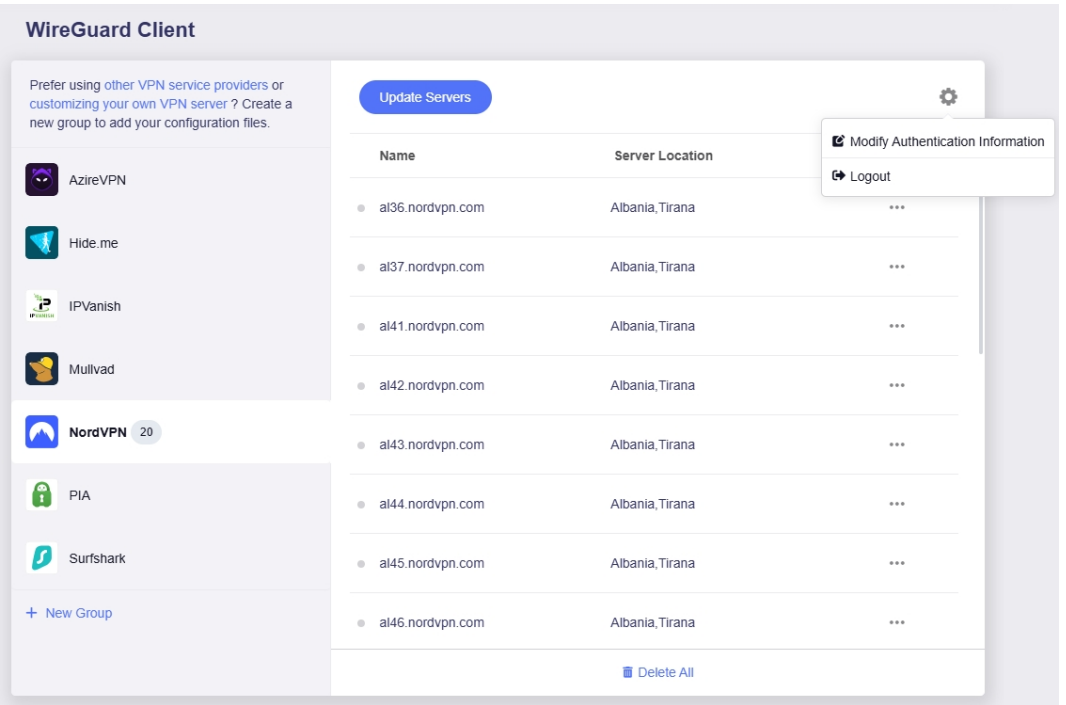
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

8. Server aktualisieren.

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

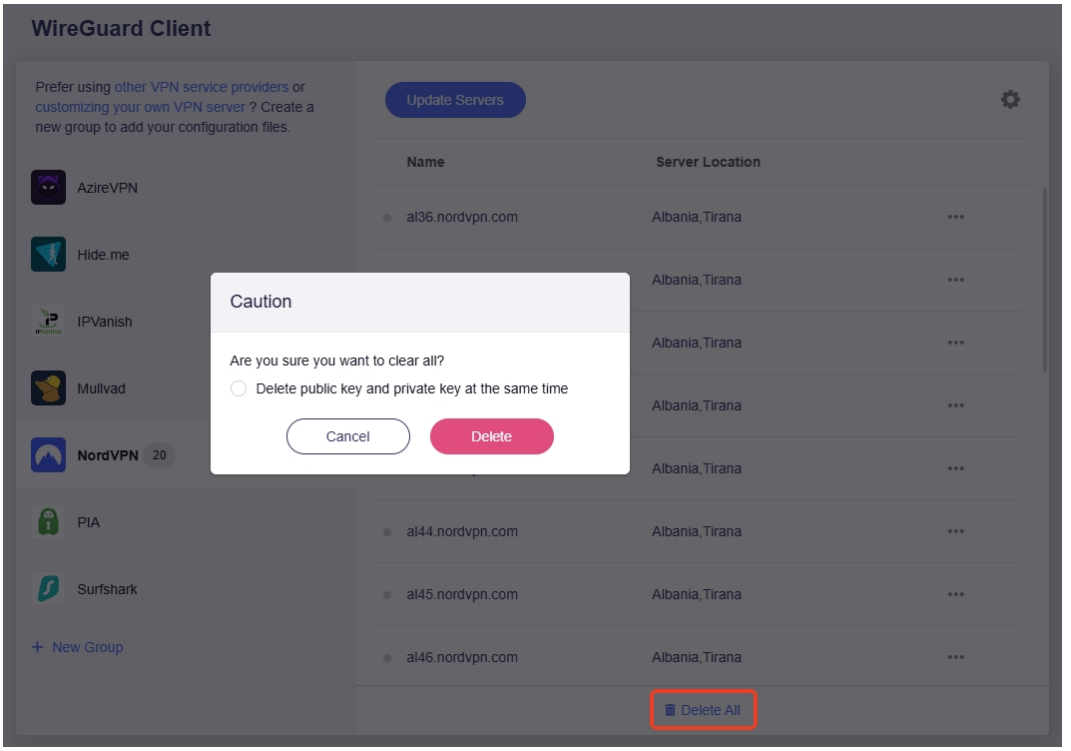


9. Zugangsdaten bearbeiten oder abmelden.
   Klicken Sie auf das Zahnradsymbol, um Ihre Zugangsdaten zu bearbeiten oder sich abzumelden.



10. Alle Dateien löschen.

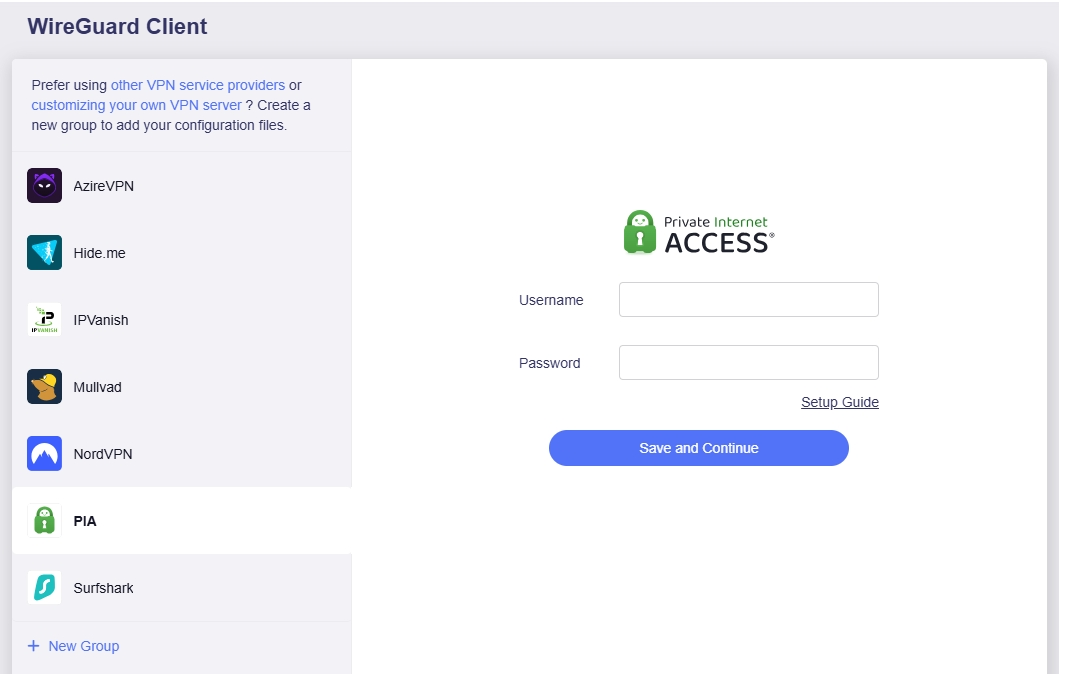
    Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.



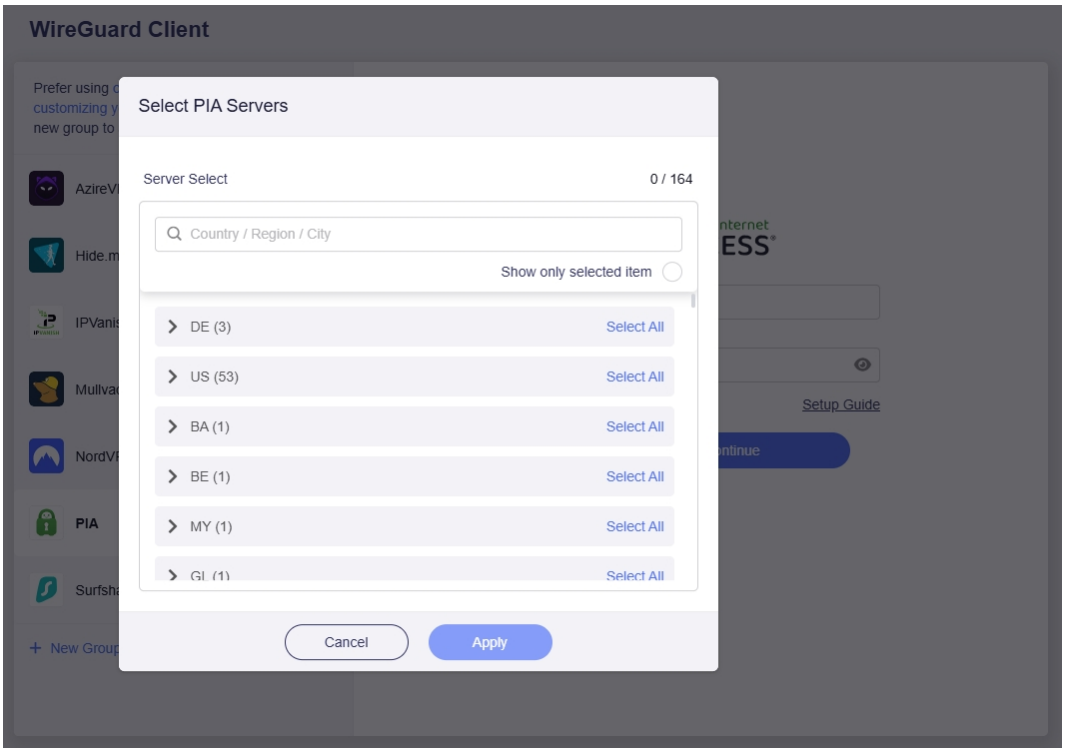
11.2.7 PIA (Private Internet Access) einrichten

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

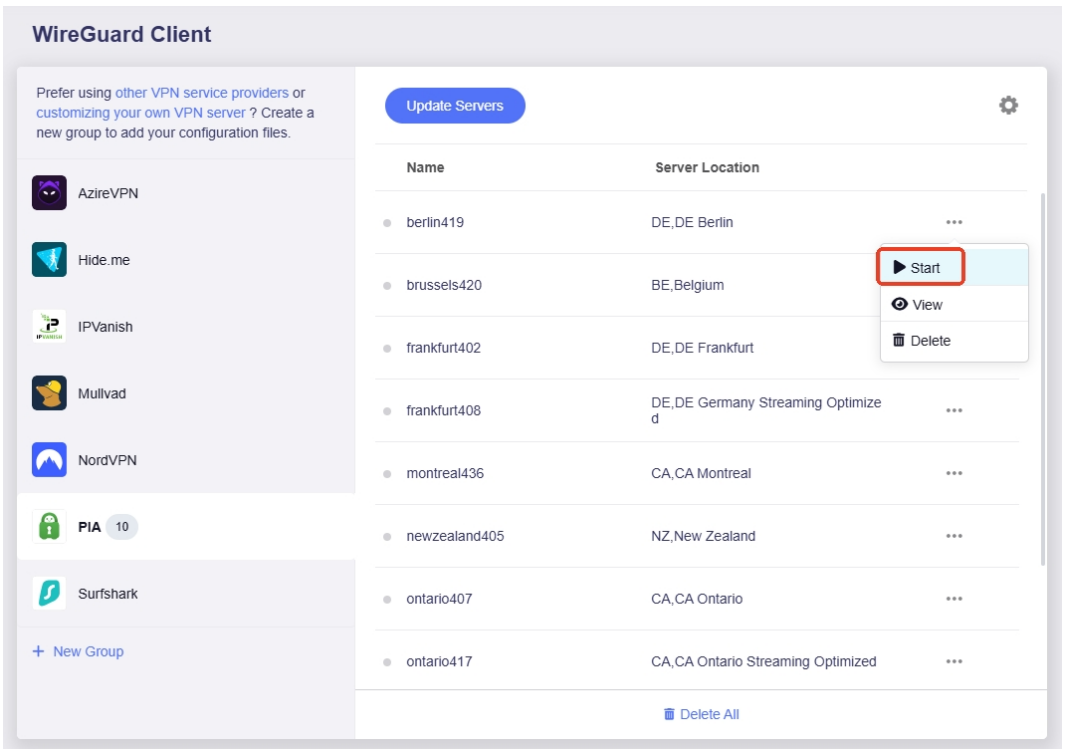
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **PIA**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



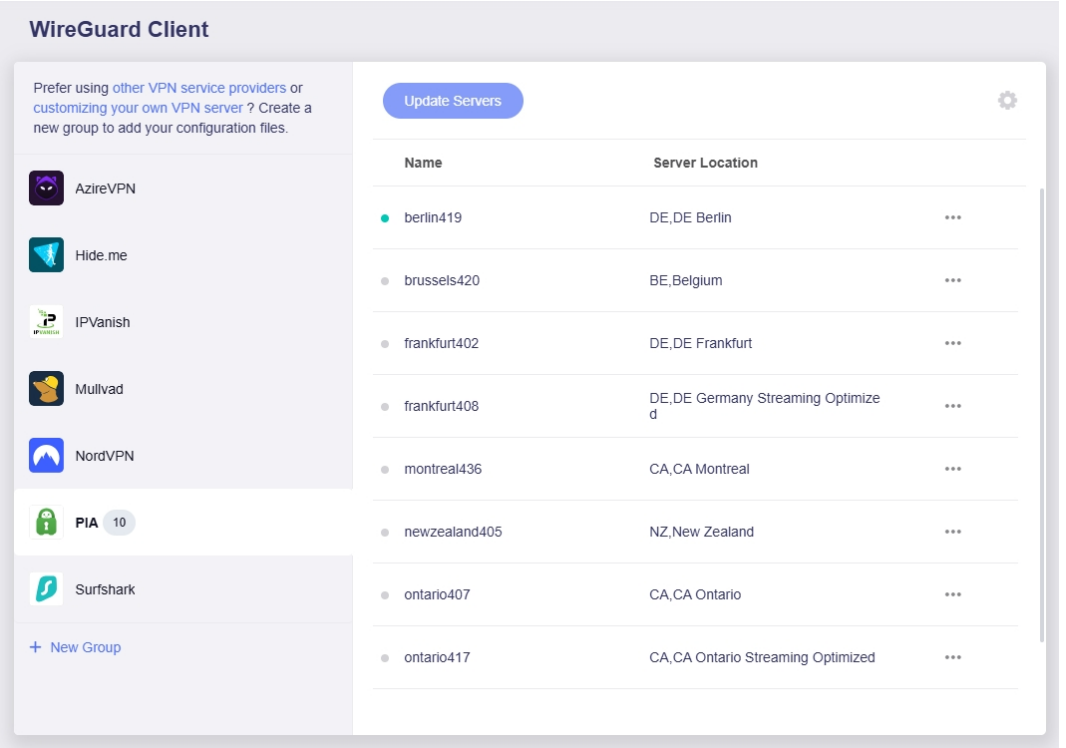
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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



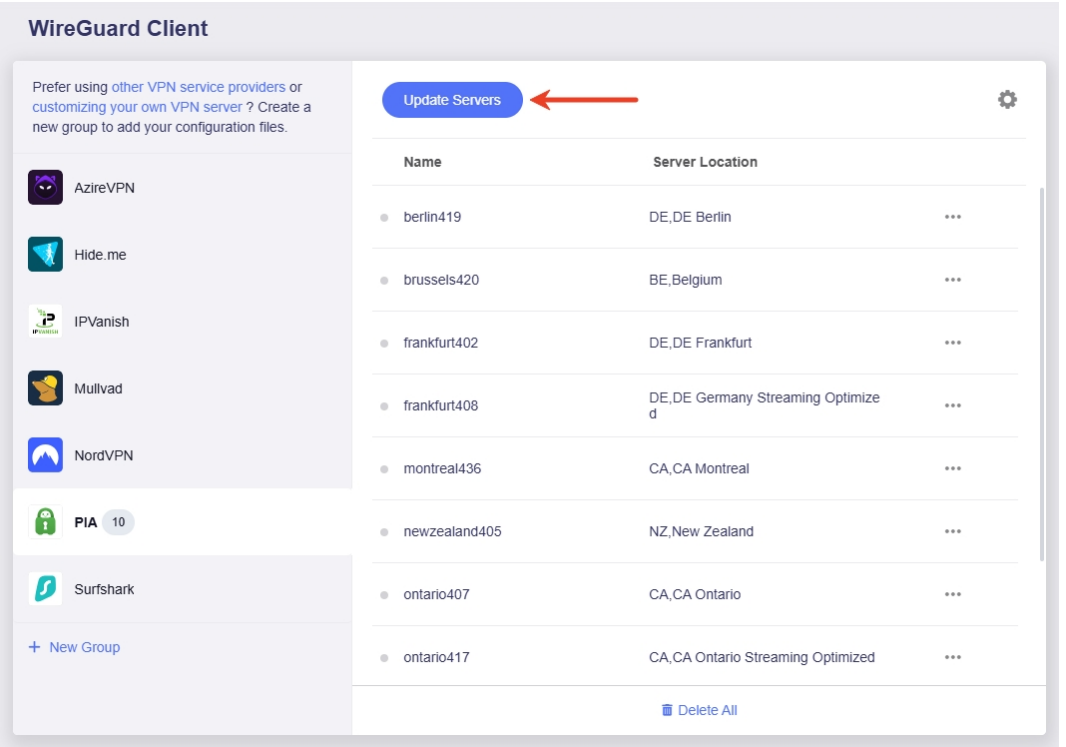
5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



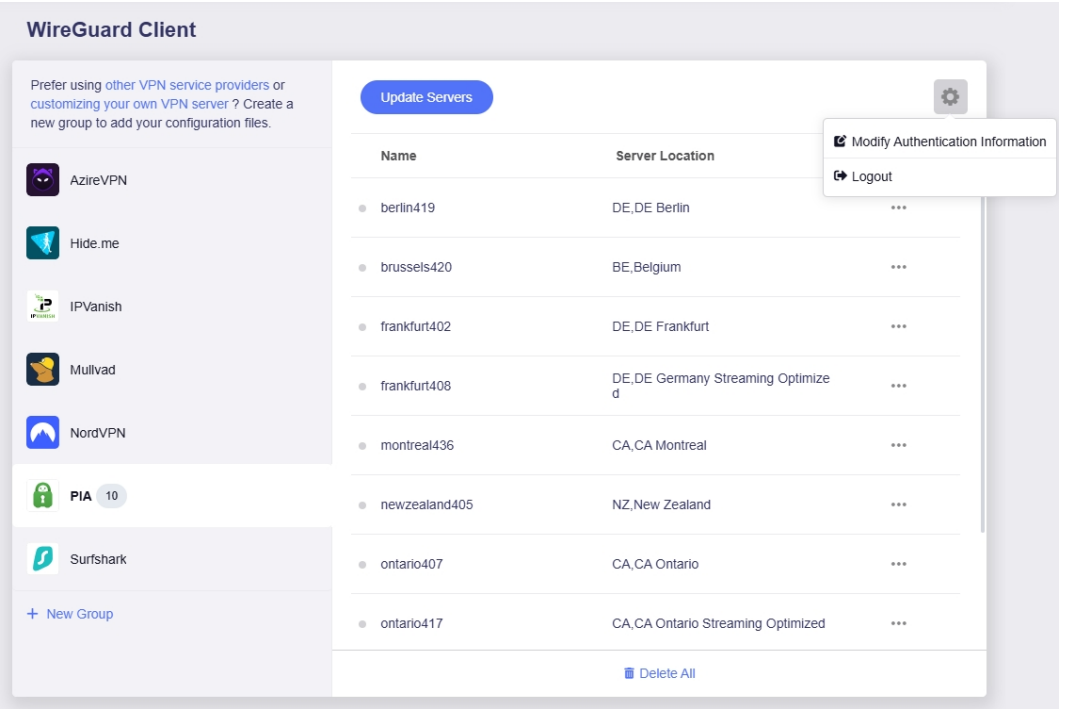
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

6. Server aktualisieren.

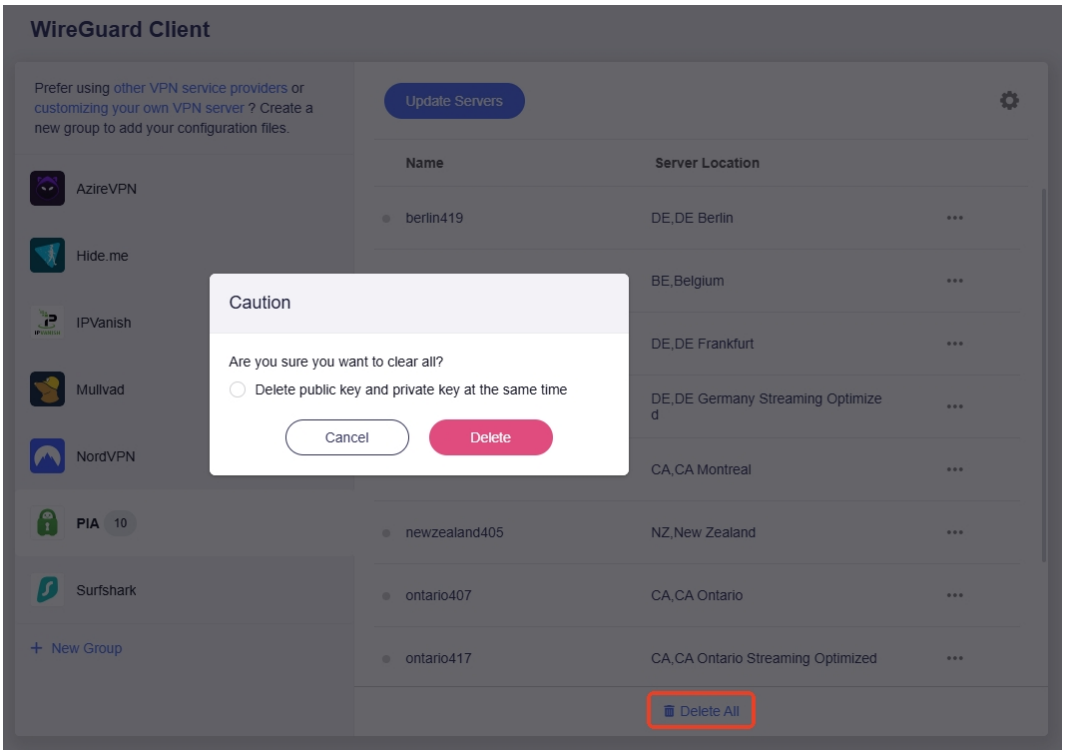
   Klicken Sie auf **Update Servers**, um die aktuelle Liste verfügbarer Server abzurufen. So vermeiden Sie Verbindungsfehler durch Serverwartung oder abgeschaltete Server.



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



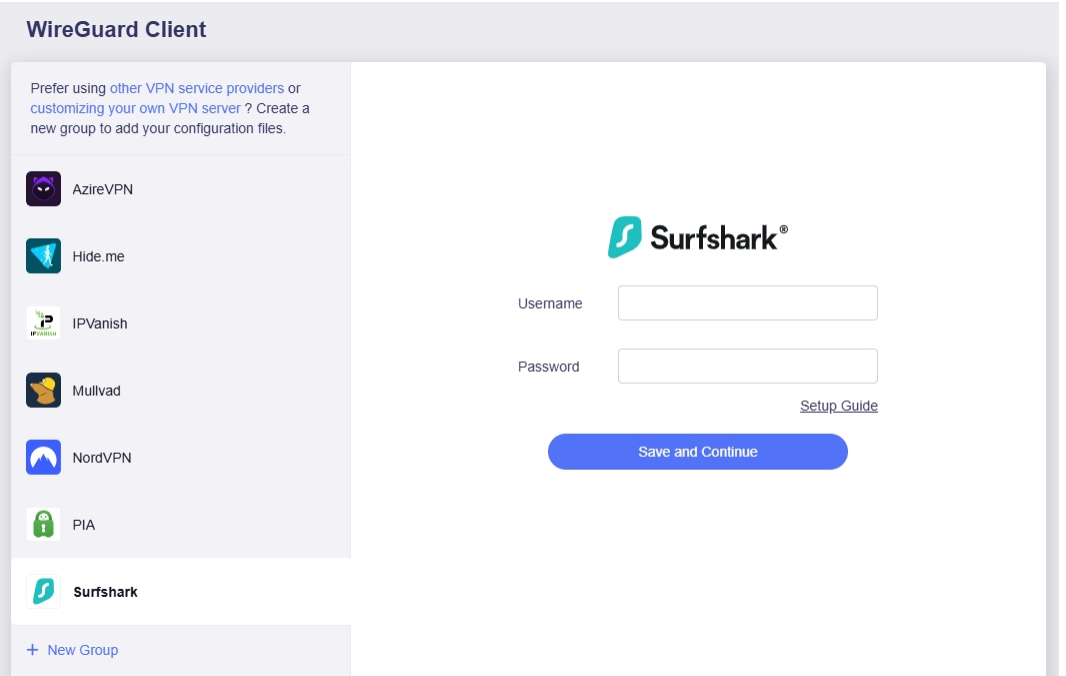
8. Alle Dateien löschen.
   Mit **Delete All** können Sie sämtliche Konfigurationsdateien mit einem Klick löschen und wählen, ob gleichzeitig auch die privaten und öffentlichen Schlüssel gelöscht werden sollen.


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

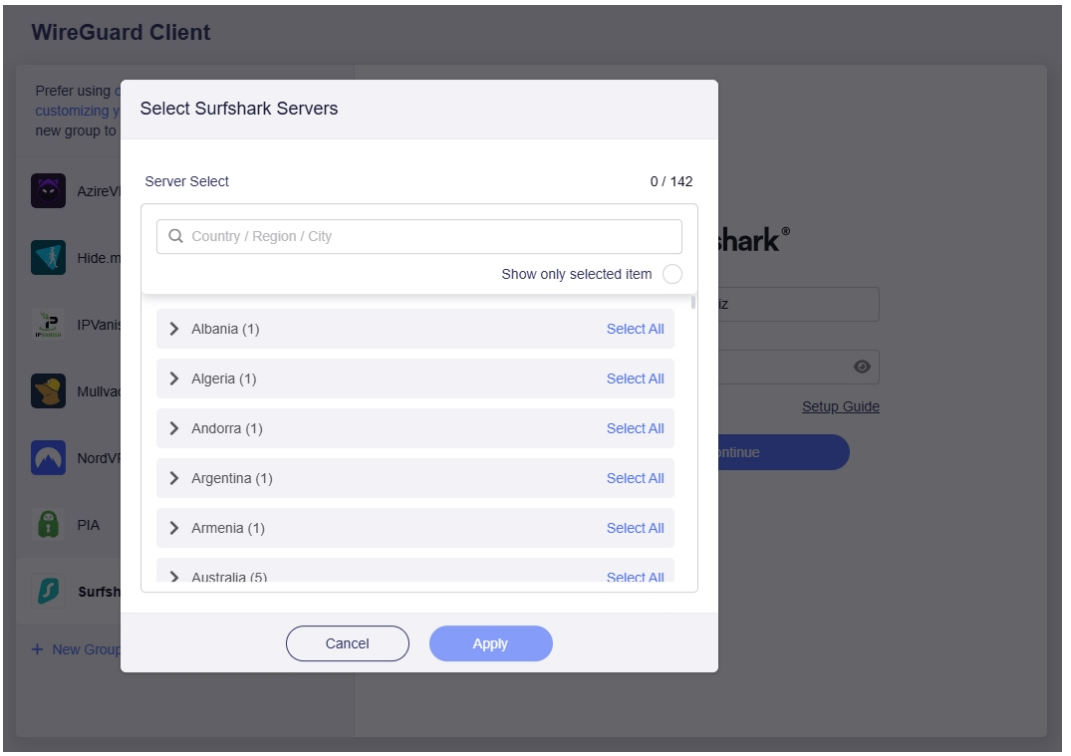
11.2.8 Surfshark einrichten

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

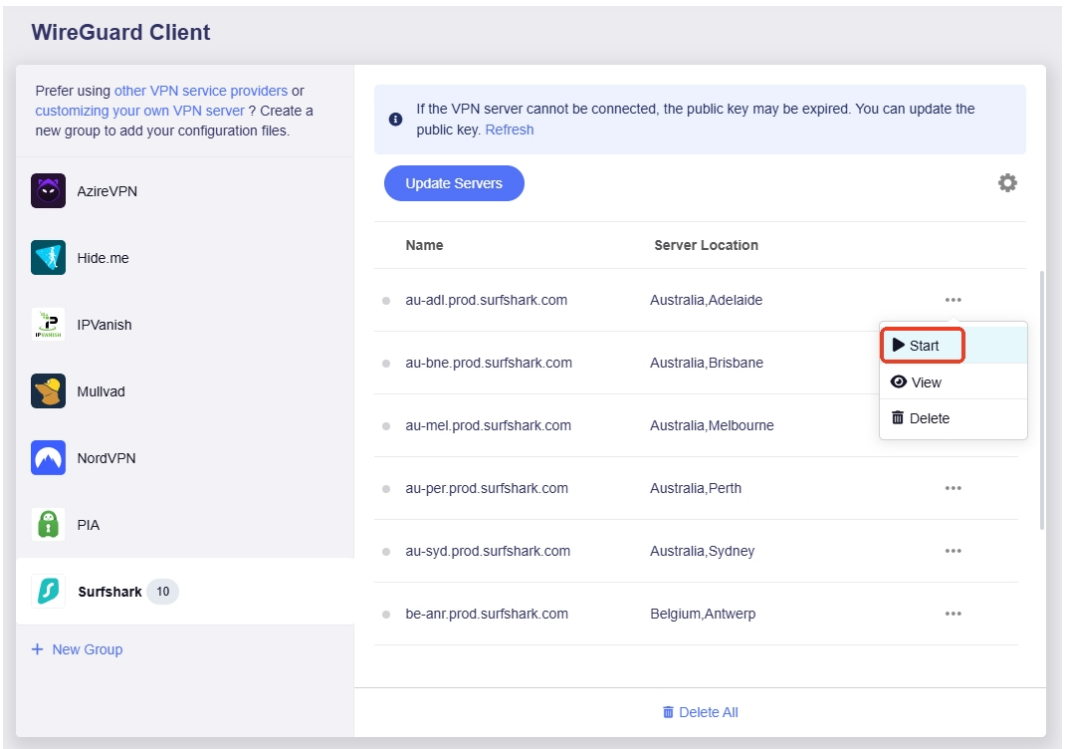
1. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **WireGuard Client** > **Surfshark**.
2. Geben Sie Benutzername und Passwort ein und klicken Sie auf **Save and Continue**.



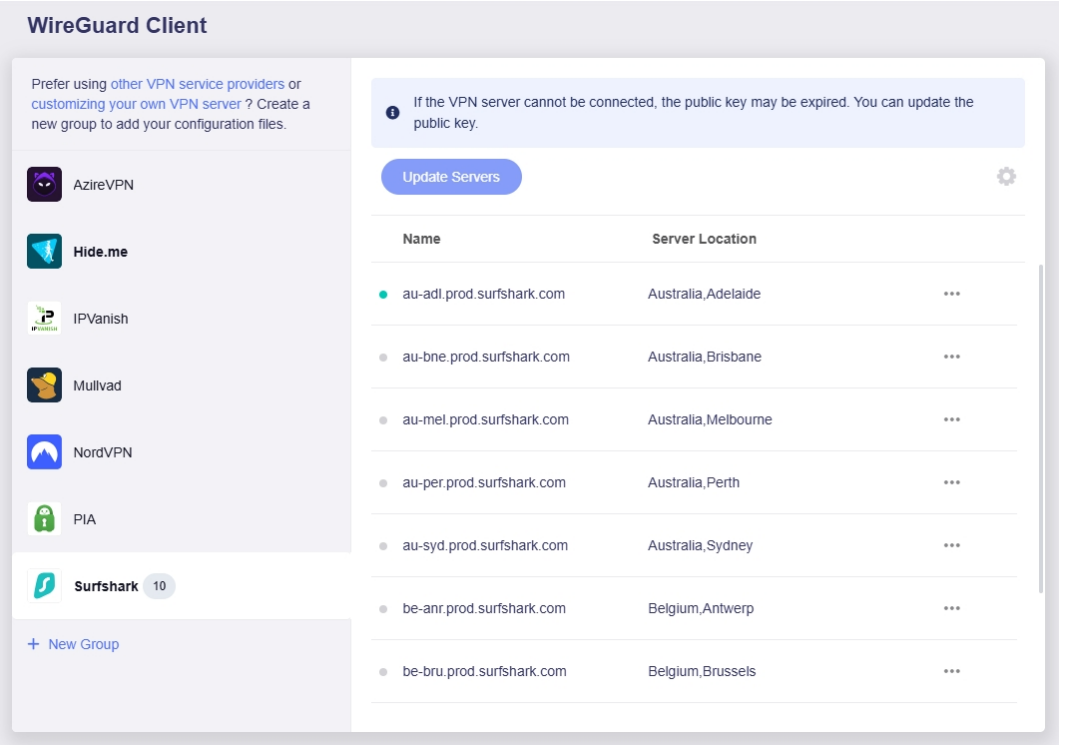
3. Wählen Sie die Server aus, zu denen Sie eine Verbindung herstellen möchten, und klicken Sie auf **Apply**.



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

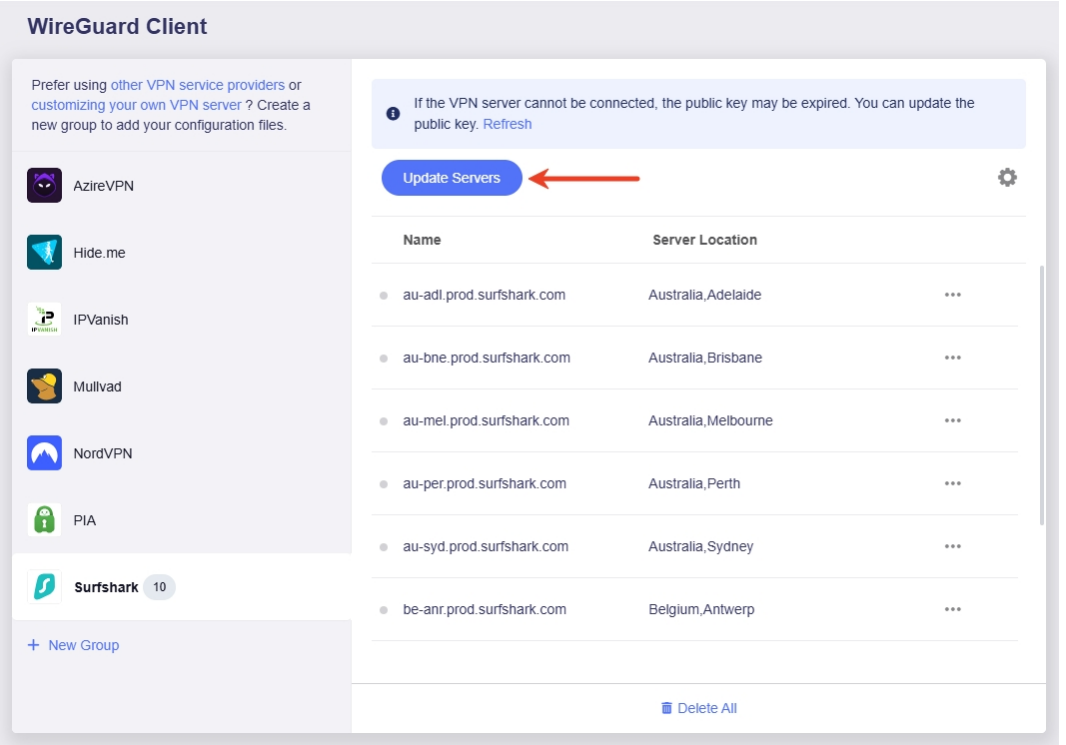


5. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



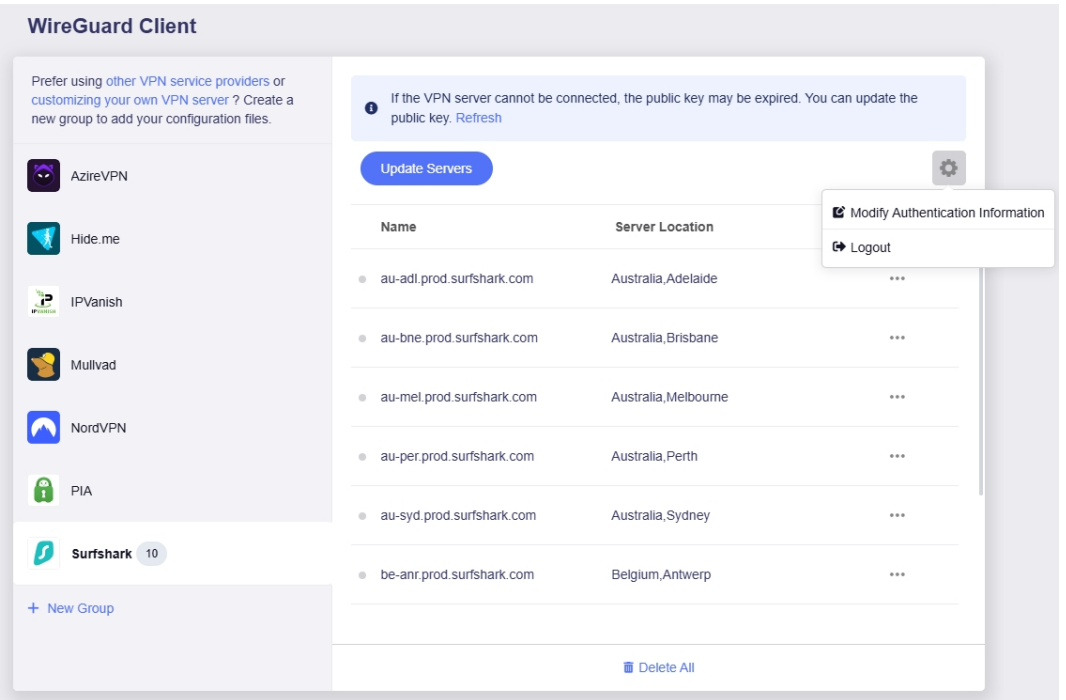
Sie können die Details der VPN-Verbindung auch im **VPN Dashboard** prüfen.

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



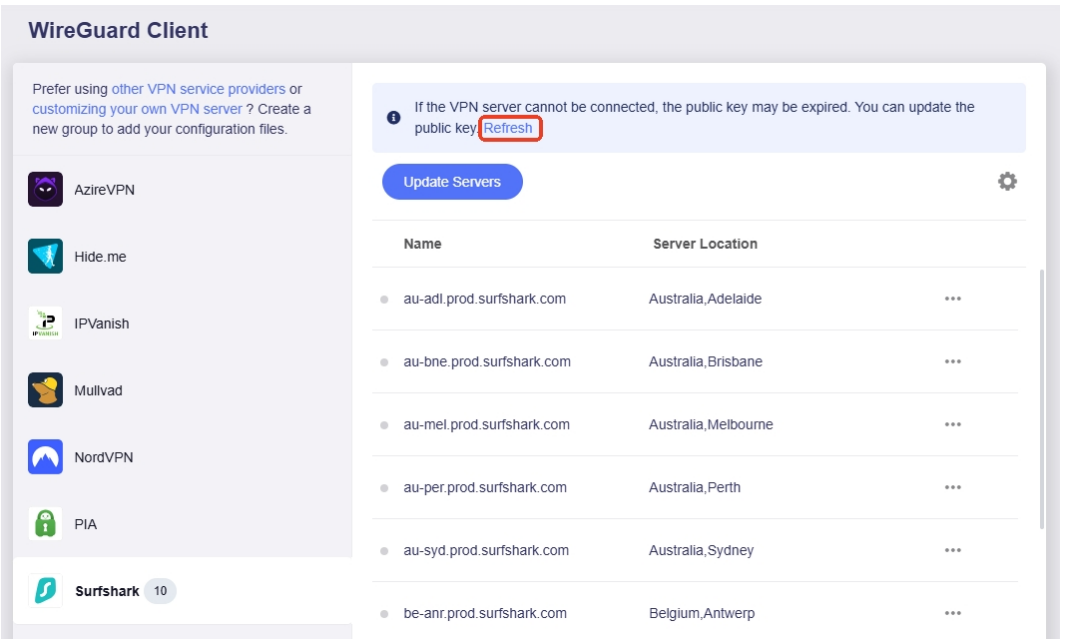
7. Zugangsdaten bearbeiten oder abmelden.

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



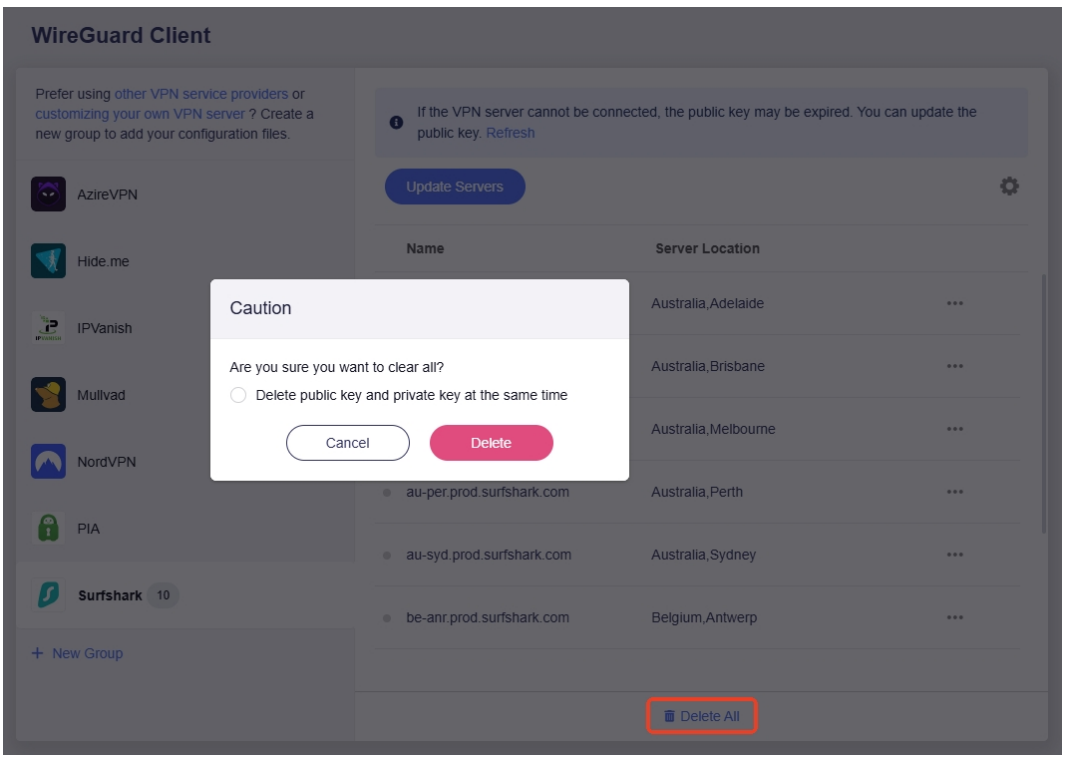
8. Aktualisieren.

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.

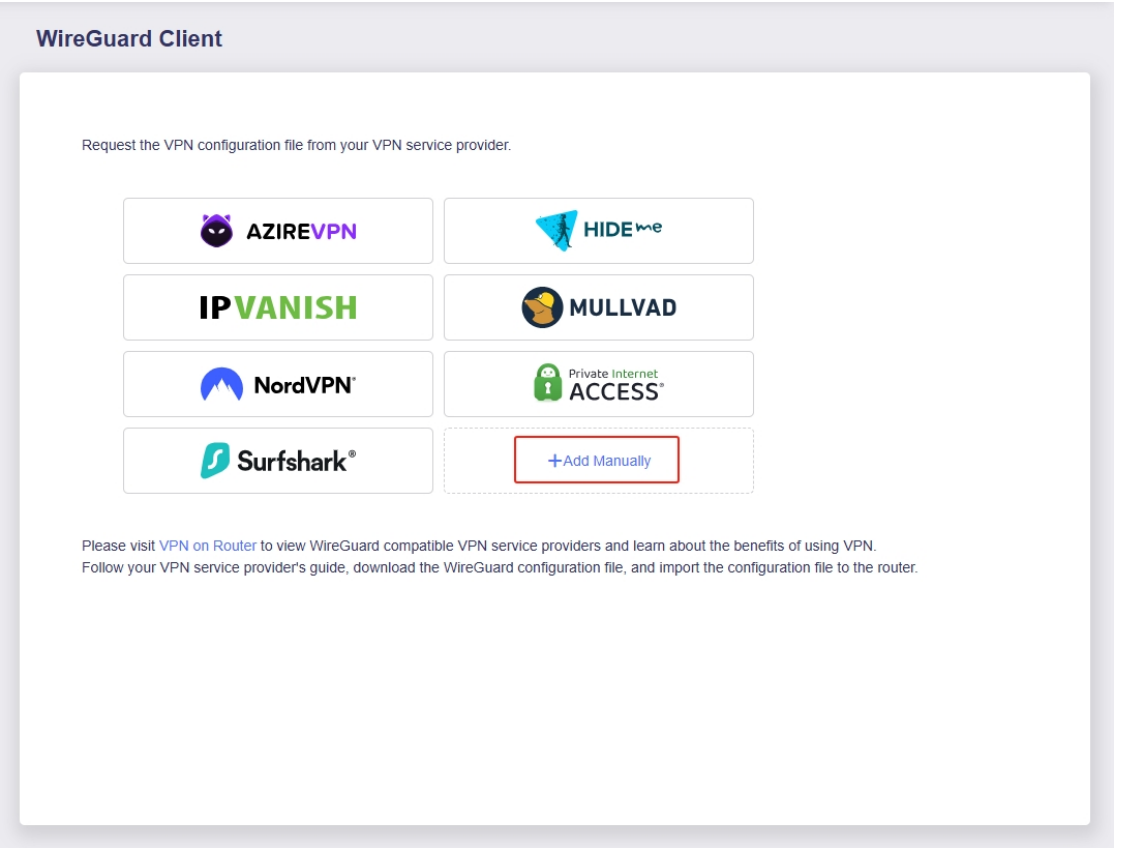


11.2.9 WireGuard-Client manuell einrichten (andere Anbieter)

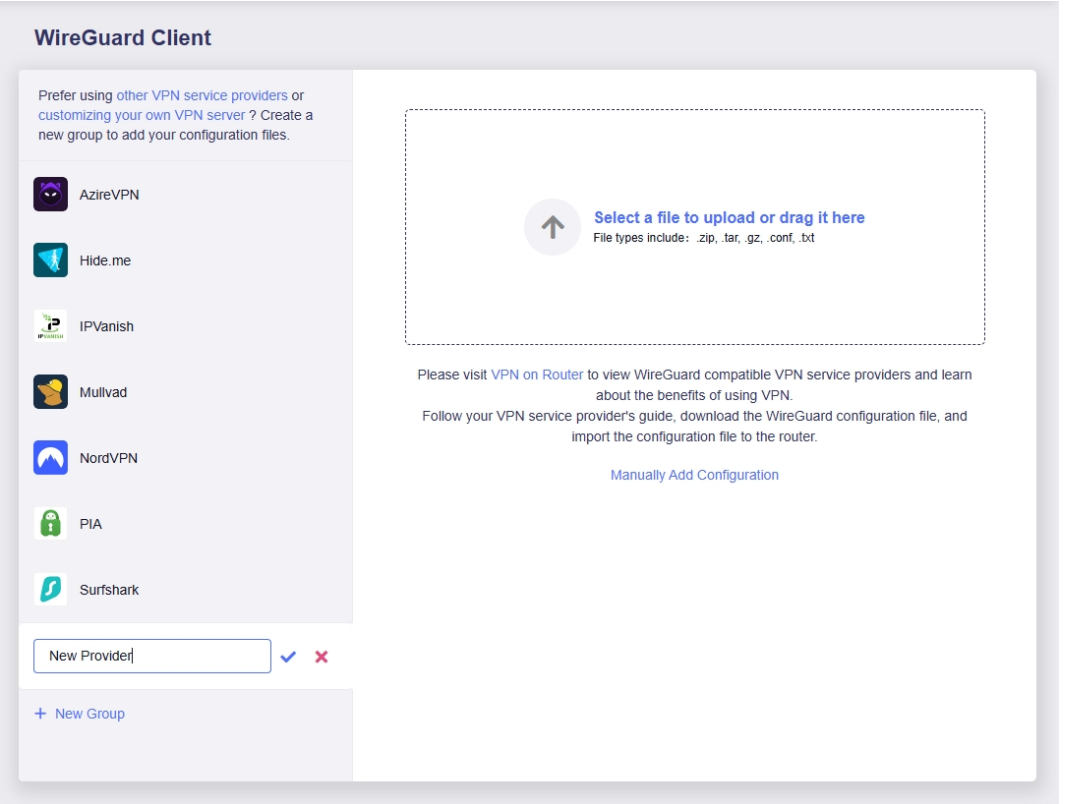
Wenn Ihr WireGuard-Anbieter nicht in die Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den WireGuard-Client einzurichten. Falls Sie nicht wissen, wie Sie die Dateien herunterladen,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

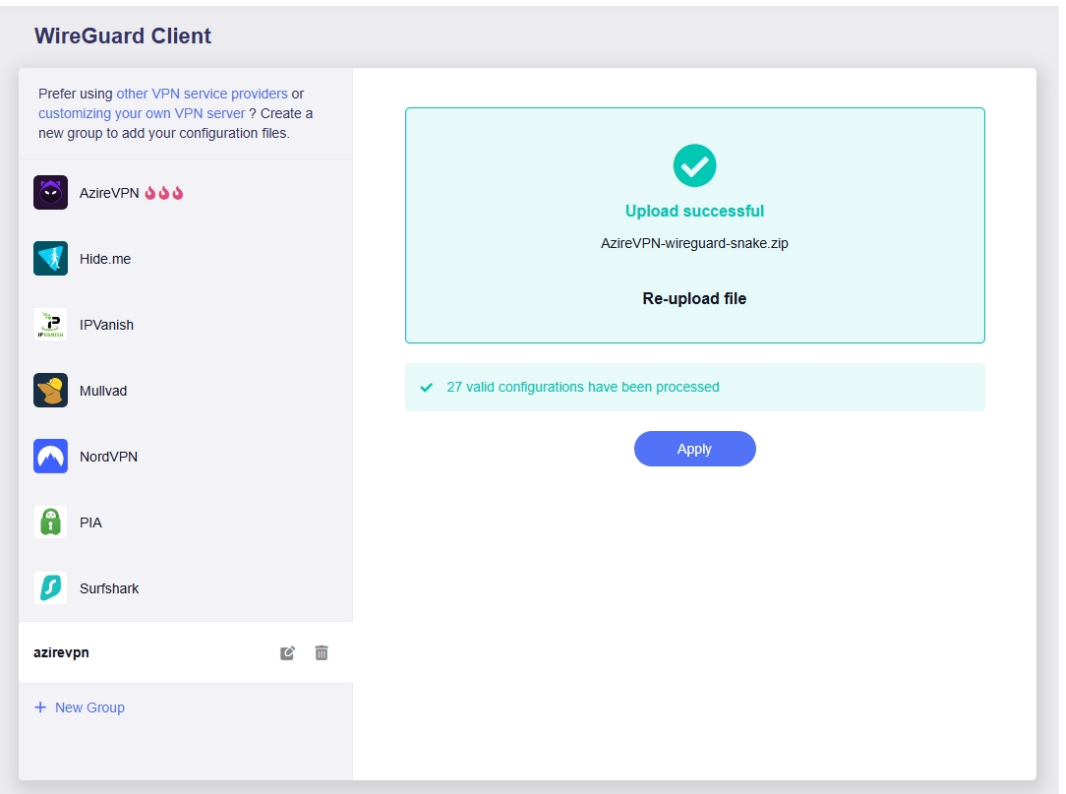
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Add Manually**.



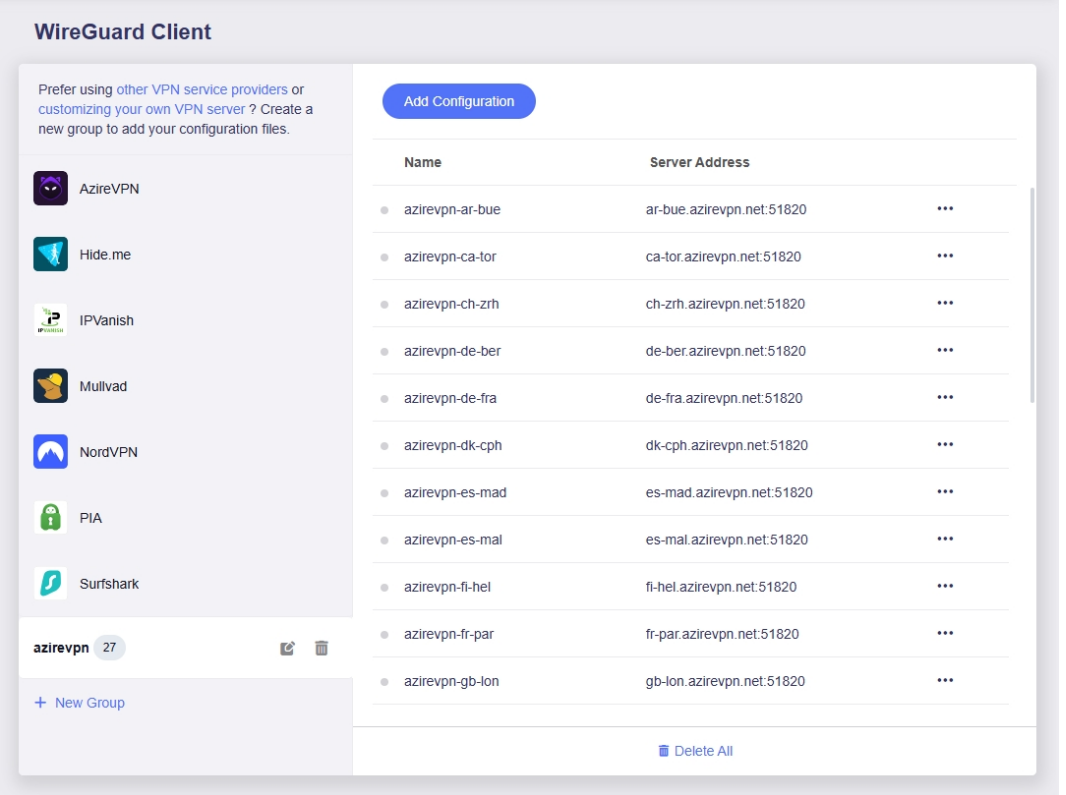
2. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



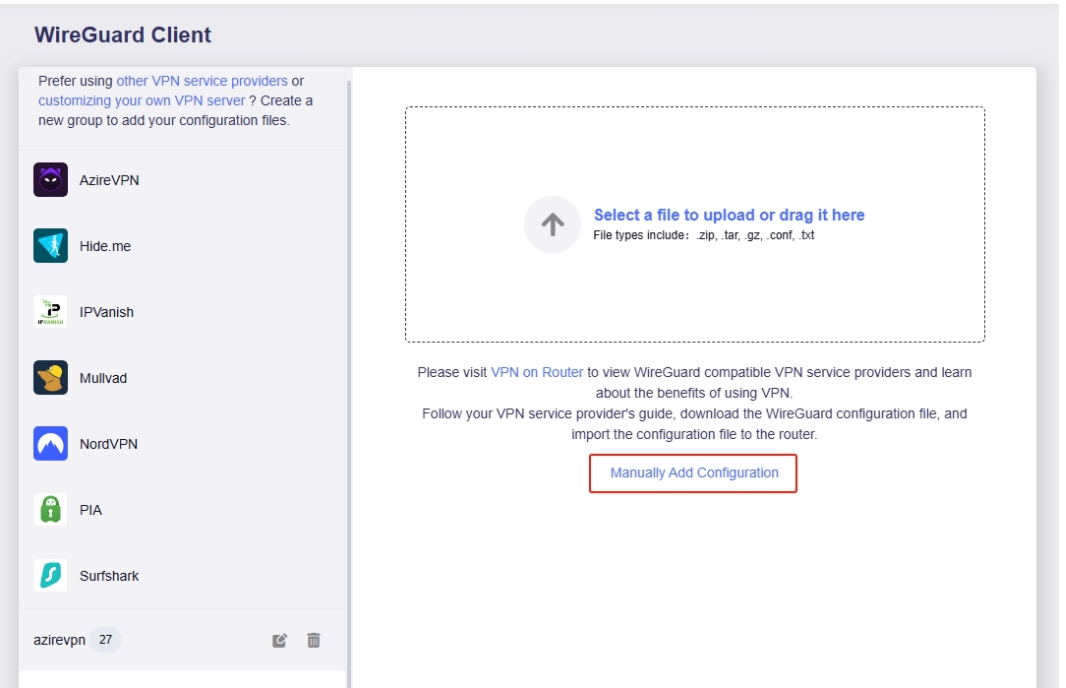
3. Klicken Sie auf den Upload-Bereich, laden Sie Ihre WireGuard-Konfigurationsdatei hoch und klicken Sie auf **Apply**. Unterstützte Formate: zip, tar, gz, conf und txt.

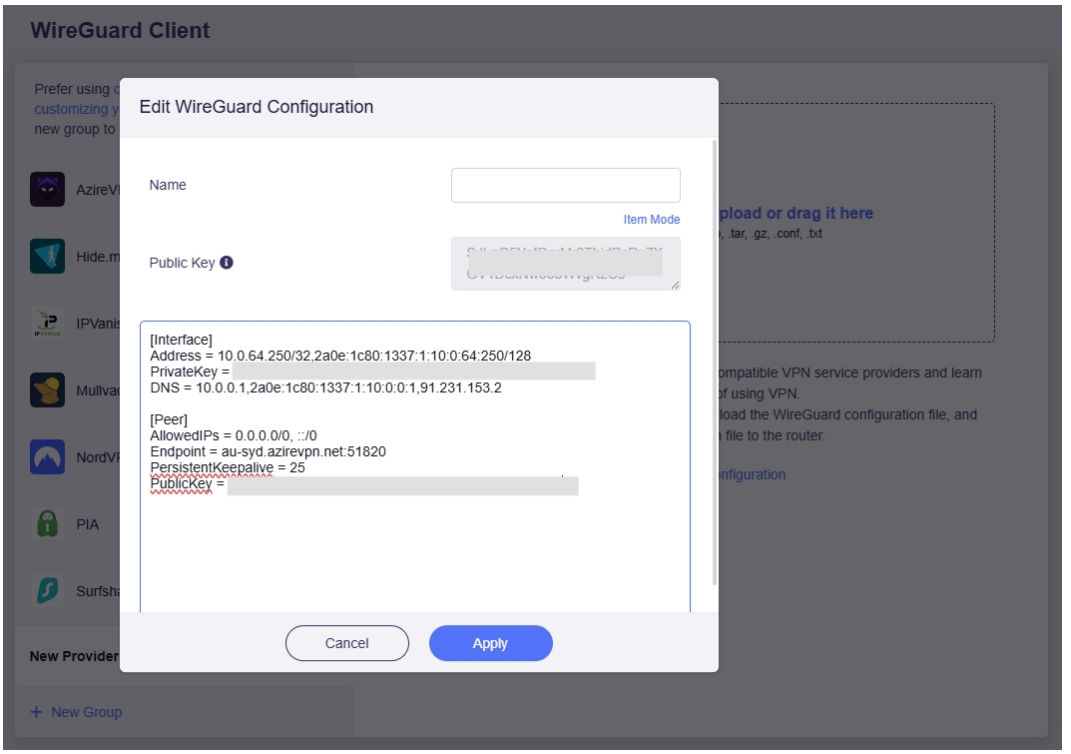


Wenn Sie eine komprimierte Datei mit mehreren Konfigurationsdateien hochladen, wird sie wie unten gezeigt automatisch entpackt.

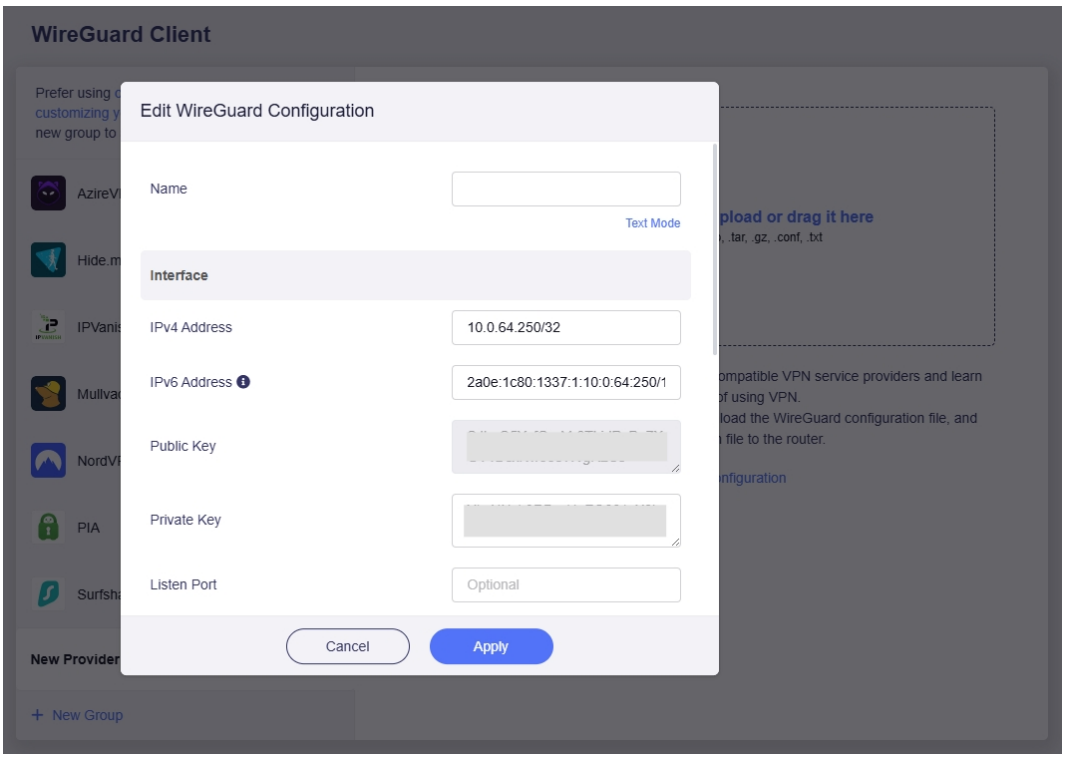


Alternativ klicken Sie unten im Upload-Bereich auf **Manually Add Configuration**, geben die Konfiguration als Text ein und klicken auf **Apply**.

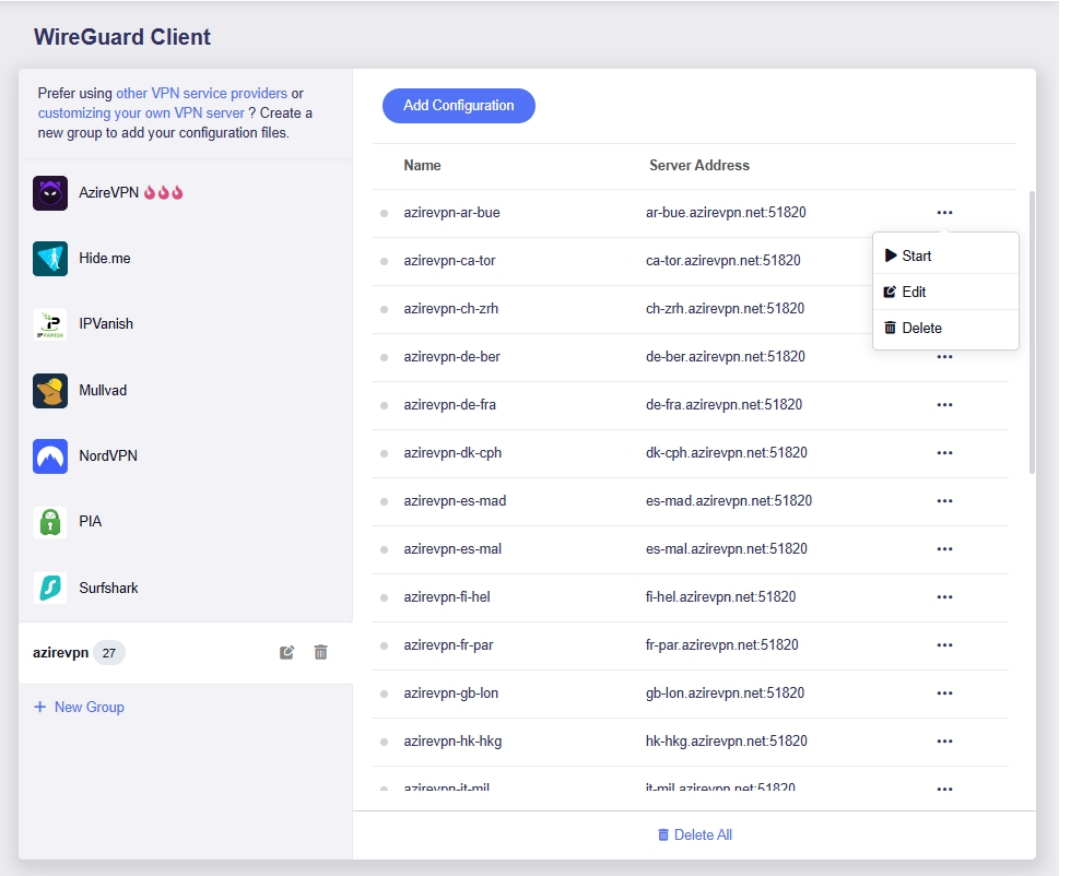




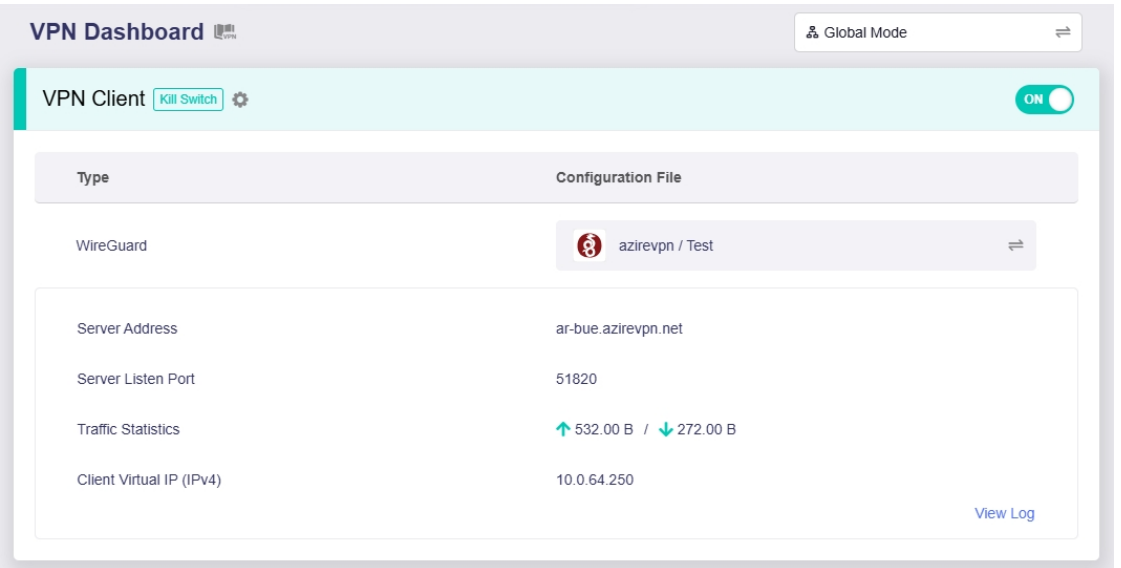
Um die einzelnen Einträge zu prüfen, wechseln Sie in den Modus Item und kontrollieren Sie die Konfigurationsdetails. Klicken Sie anschließend auf **Apply**.



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

Netzwerk

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

12.1 Multi-WAN

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

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

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

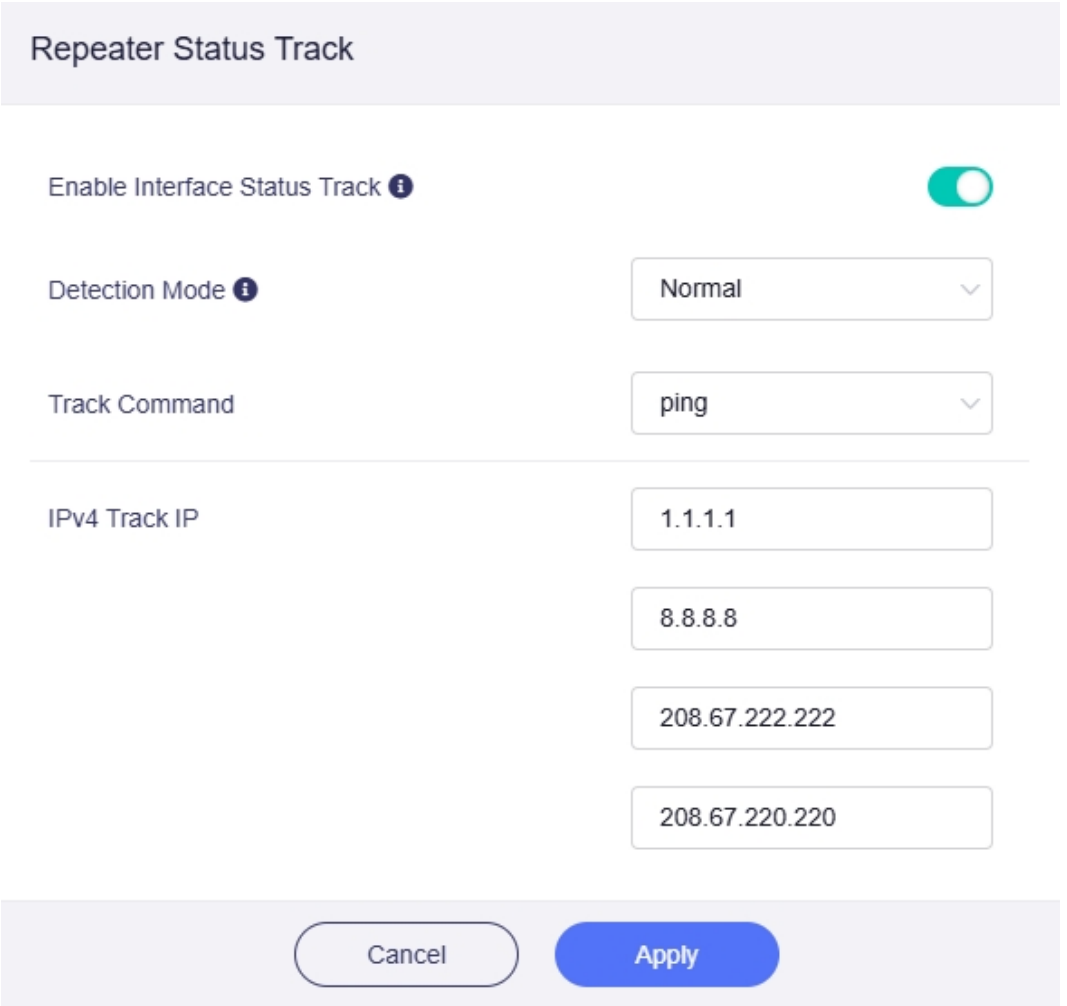
12.1.1 Schnittstellenstatus überwachen

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 Einstellungen zur Statusüberwachung der jeweiligen Netzwerkschnittstelle zu öffnen.

Nachfolgend sind die Einstellungen für die Repeater-Schnittstelle dargestellt. Die anderen Schnittstellen werden nach demselben Prinzip konfiguriert.



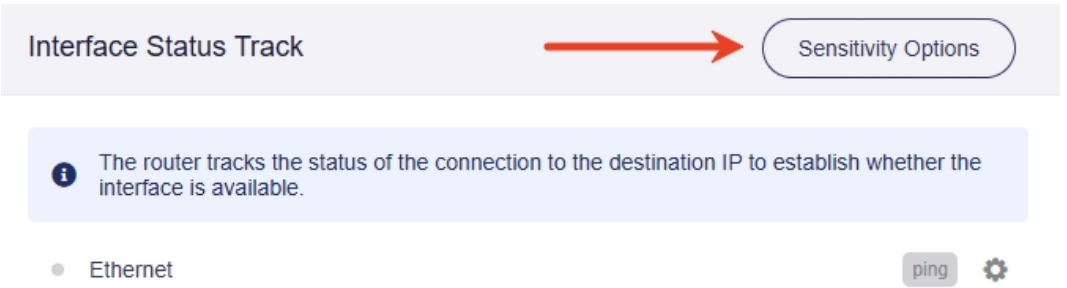
- **Enable Interface Status Track**: Standardmäßig aktiviert. Bei deaktivierter Option geht das Gerät von einer bestehenden Internetverbindung aus, sobald die Schnittstelle verbunden ist, beispielsweise wenn ein Kabel eingesteckt und eine IP-Adresse bezogen wurde.
- **Detection Mode**: Diese Funktion wurde in Firmware v4.5 als Low Data Mode eingeführt und in Firmware v4.7 in Detection Mode umbenannt. Es stehen drei Modi zur Verfügung: Normal Mode, Low Data Mode und Strict Mode.
  - **Normal Mode**: Dieser Modus wird standardmäßig verwendet.
  - **Low Data Mode**: Die Verbindungsüberwachung wird nur bei einem Netzwerkfehler an der Schnittstelle ausgelöst. Verwenden Sie diesen Modus bei einem Tarif mit begrenztem Datenvolumen. Beachten Sie, dass der erneute Verbindungsaufbau

nach einem Ausfall etwas länger dauern kann als im Normalmodus. Standardmäßig ist dieser Modus nur für die Mobilfunkschnittstelle aktiviert.

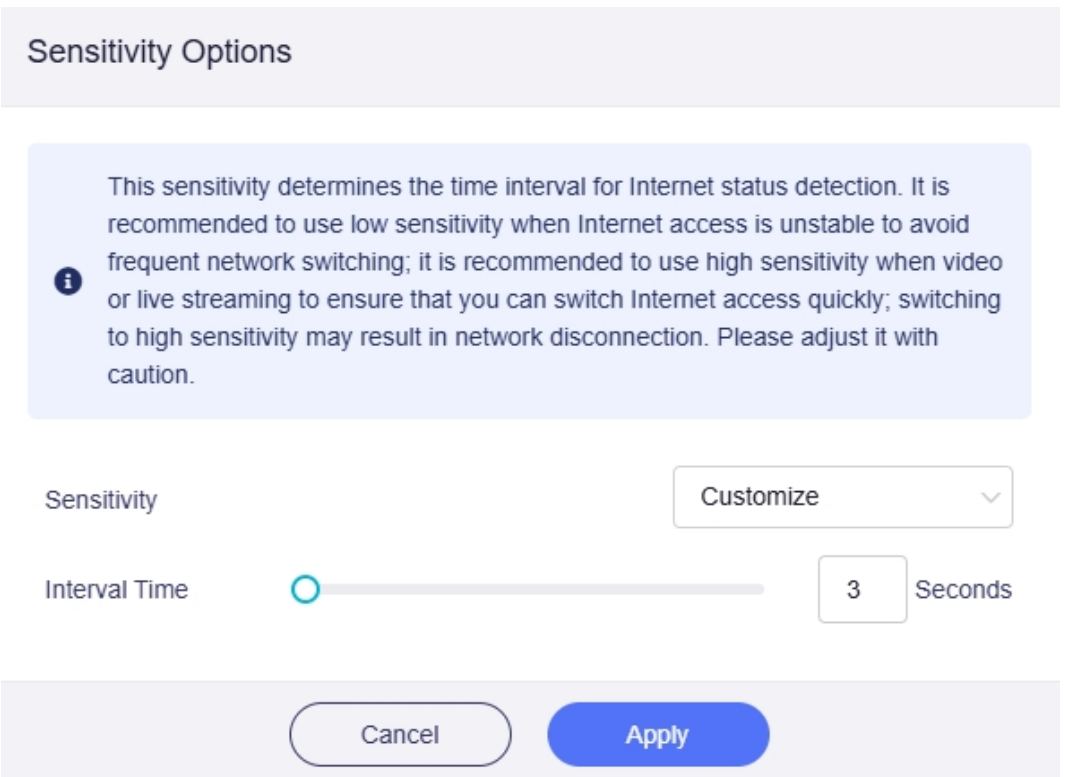
- **Strict Mode**: Der Schnittstellenstatus wird ausschließlich anhand der Ergebnisse eines an eine öffentliche IP-Adresse gesendeten Prüfbefehls bestimmt.

- **Track Command**: Der Befehl ping prüft die Verbindung zur Ziel-IP-Adresse und damit die Verfügbarkeit der Schnittstelle.
- **IPv4 Track IP**: Passen Sie bei Bedarf die für die Überwachung verwendeten IPv4-Adressen an.

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



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



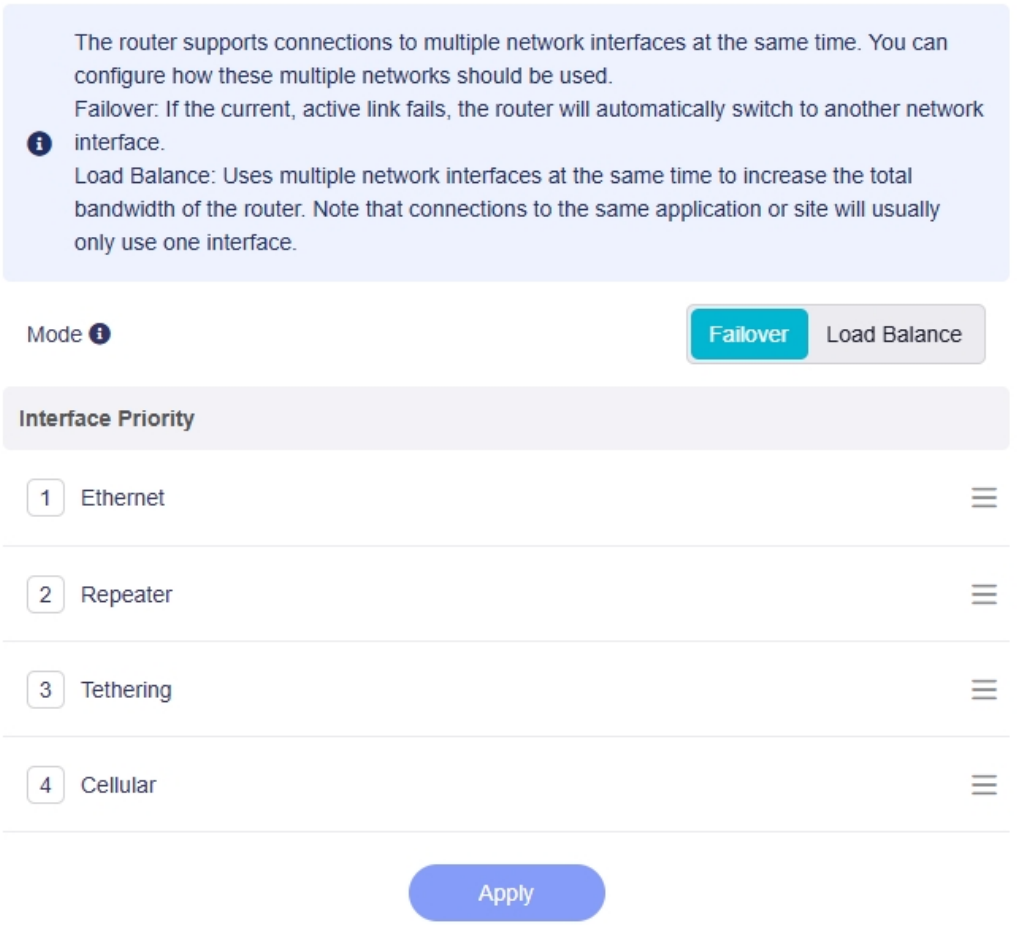
12.1.2 Multi-WAN-Modus

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.

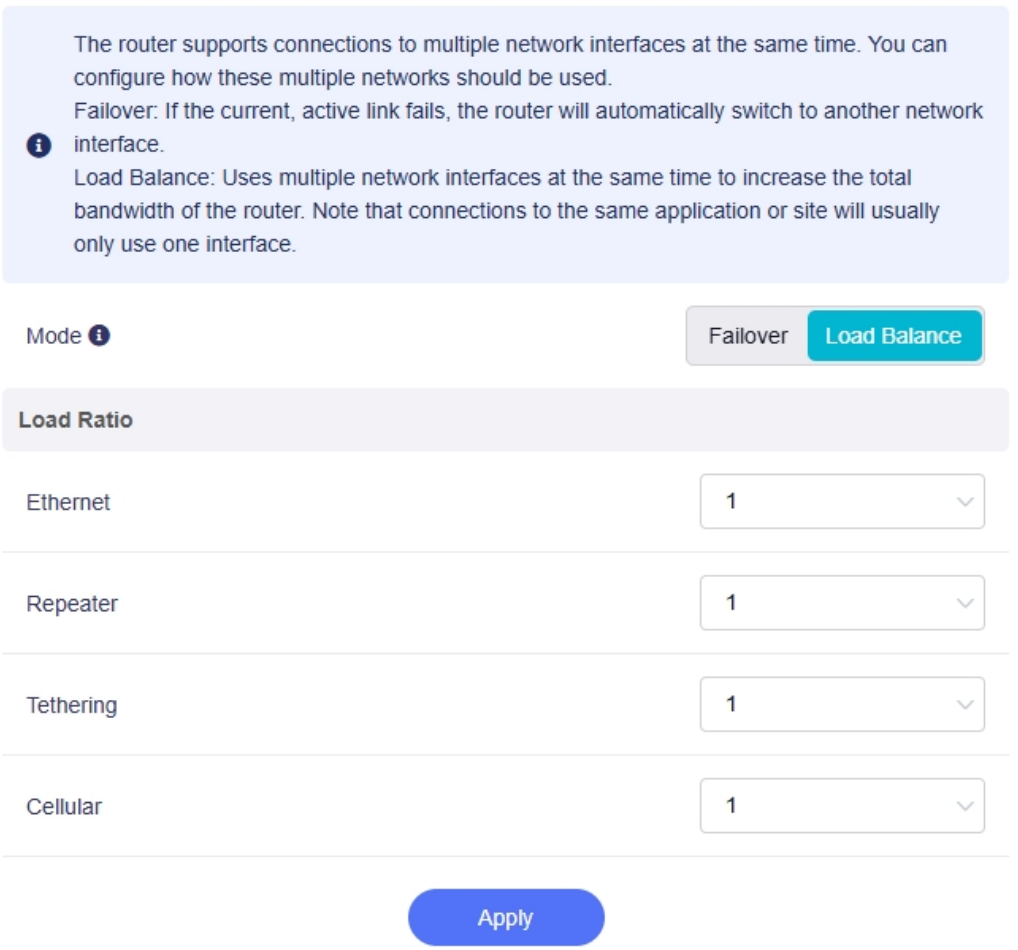
Sie können jeder Schnittstelle eine Priorität zuweisen. Fällt die verwendete Schnittstelle aus, wechselt der Router zur verfügbaren Schnittstelle mit der nächsthöheren Priorität. Sobald eine Verbindung mit höherer Priorität wieder verfügbar ist, wechselt er automatisch zurück.



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 bestimmt das Verhältnis zwischen den einzelnen Netzwerkschnittstellen. Anhand dieses Verhältnisses weist das System neue Verbindungen den Schnittstellen zu. Ist der Router beispielsweise gleichzeitig mit vier Netzwerken verbunden, etwa Ethernet, Repeater, Tethering und Mobilfunk, und haben alle Schnittstellen Internetzugang, teilen sie bei aktiviertem Load Balance und einem Verhältnis von 1:1:1:1 die Netzwerkbandbreite gleichmäßig untereinander auf. Das System verteilt neue Verbindungen gemäß dem festgelegten Lastverhältnis auf diese Schnittstellen.



Sie können das Lastverhältnis bei Bedarf anpassen. Hat Ethernet beispielsweise eine Bandbreite von 100 Mbit/s und der Repeater 200 Mbit/s und sind keine anderen Verbindungen aktiv, setzen Sie das Verhältnis für Ethernet auf 1, für den Repeater auf 2 sowie für Tethering und Mobilfunk auf 0. Das System verteilt neue Verbindungen dann im Verhältnis 1:2 auf diese Schnittstellen. Ethernet übernimmt also halb so viele Verbindungen wie der Repeater. Anders als bei der Ausfallsicherung wird hier der Gesamtdurchsatz durch die Verteilung der Datenverkehrslast auf alle verfügbaren Schnittstellen optimiert.

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

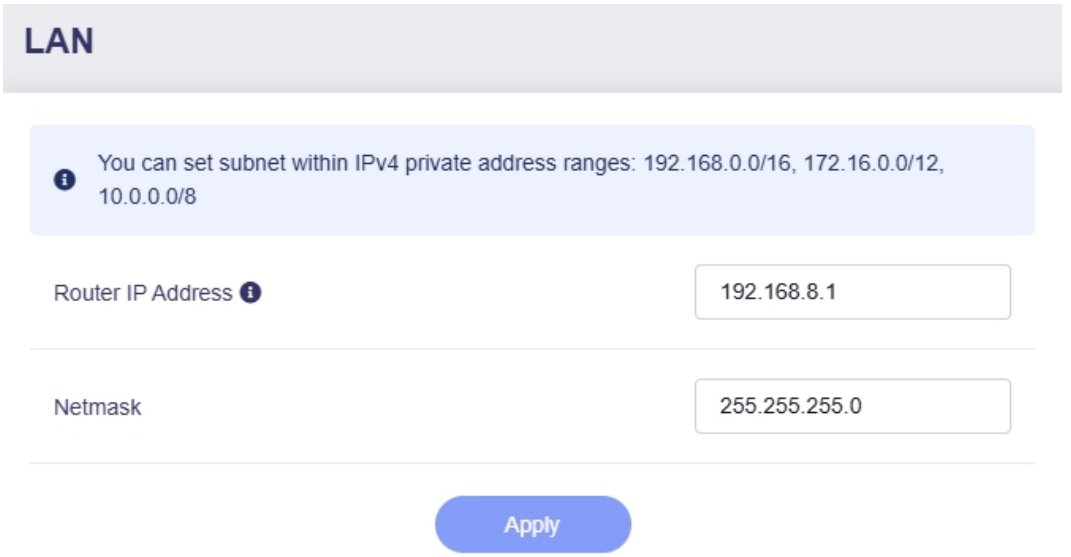
12.2 LAN

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.

12.2.1 Grundeinstellungen

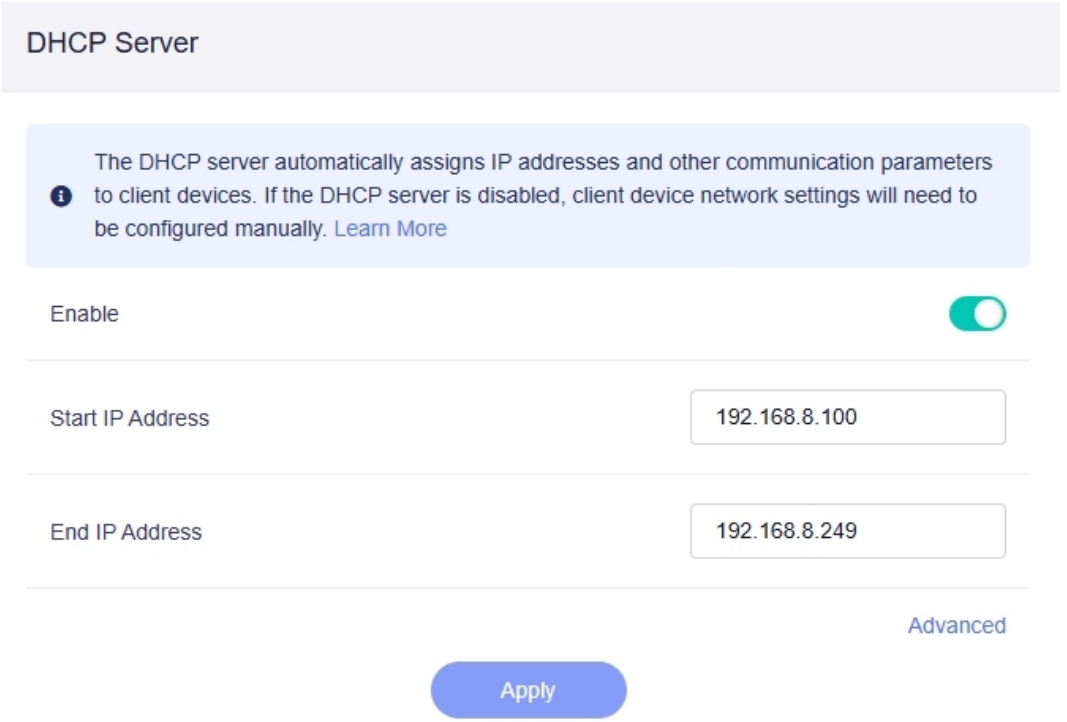
Zu den Grundeinstellungen gehören die IP-Adresse des Routers und die Netzmaske. Sie können ein Subnetz innerhalb der privaten IPv4-Adressbereiche 192.168.0.0/16, 172.16.0.0/12 oder 10.0.0.0/8 festlegen.



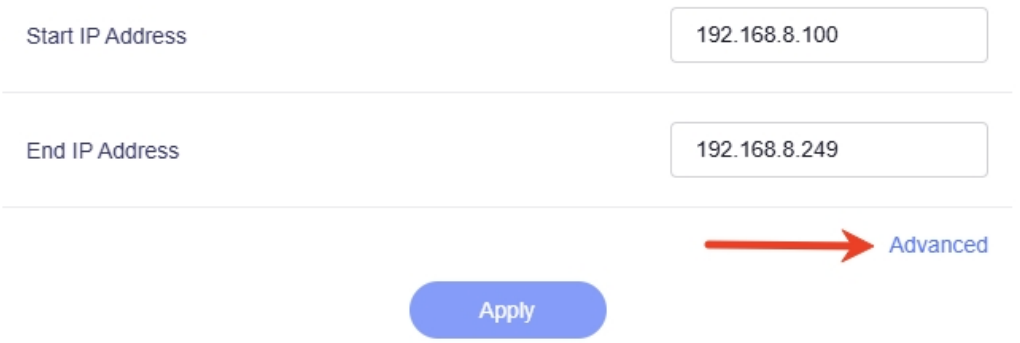
- **Router IP Address**: Über diese Adresse rufen Sie die Weboberfläche im Browser auf. Standardmäßig lautet sie 192.168.8.1. Bei einem Konflikt mit dem vorgeschalteten Netzwerk können Sie sie ändern.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.

12.2.2 DHCP-Server

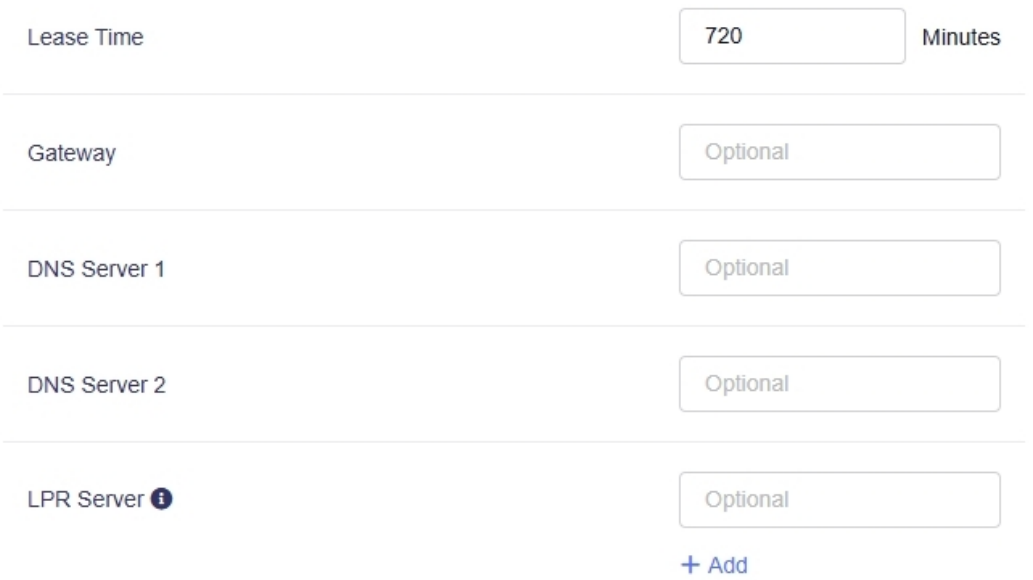
Der DHCP-Server weist jedem verbundenen Endgerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Auf GL.iNet-Routern ist er standardmäßig aktiviert und vergibt Adressen von 192.168.8.100 bis 192.168.8.249. Diesen Adressbereich können Sie bei Bedarf anpassen.



Klicken Sie unten rechts auf **Advanced**.



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



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

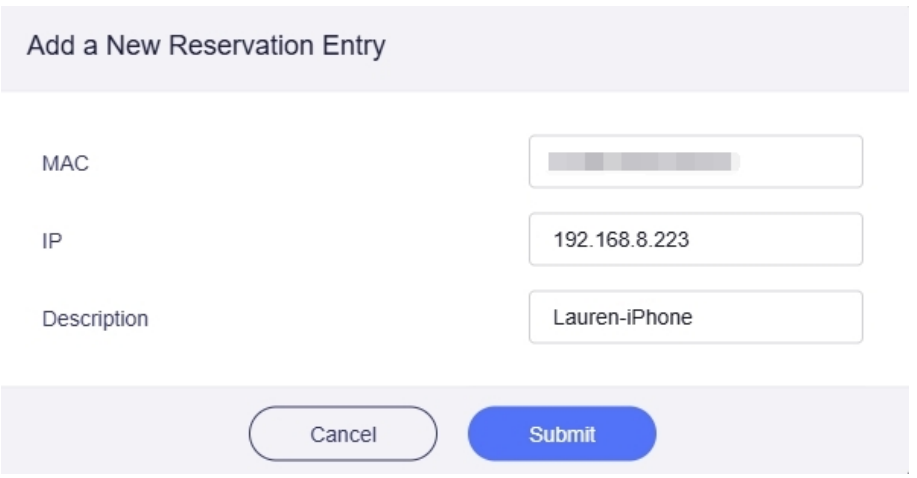
Hinweis: Bei deaktiviertem DHCP-Server müssen Sie für jedes Gerät eine statische IP-Adresse und weitere Kommunikationsparameter manuell festlegen. Einzelheiten finden Sie hier.

12.2.3 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.



12.3 Gastnetzwerk

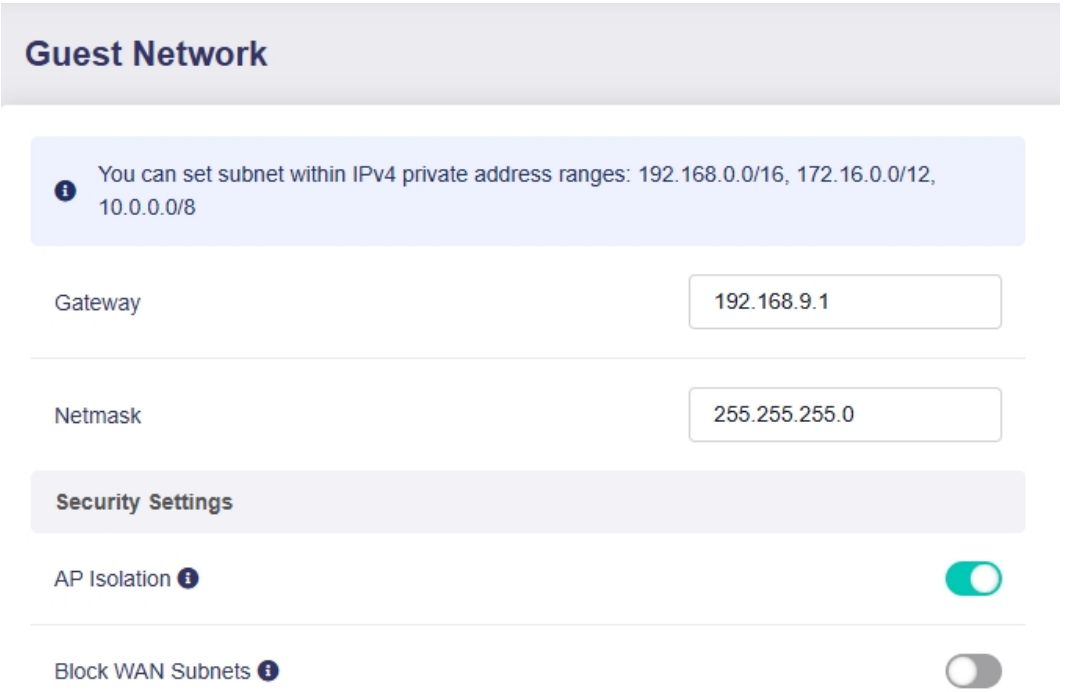
Ein Gastnetzwerk ist ein separates Netzwerk für Besucher. Es ist vom Haupt-LAN getrennt und schützt so Ihr privates Netzwerk.

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.

Hinweis: Das Gast-WLAN steht nicht zur Verfügung, wenn Mudi 7 als Repeater arbeitet.

12.3.1 Grundeinstellungen

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

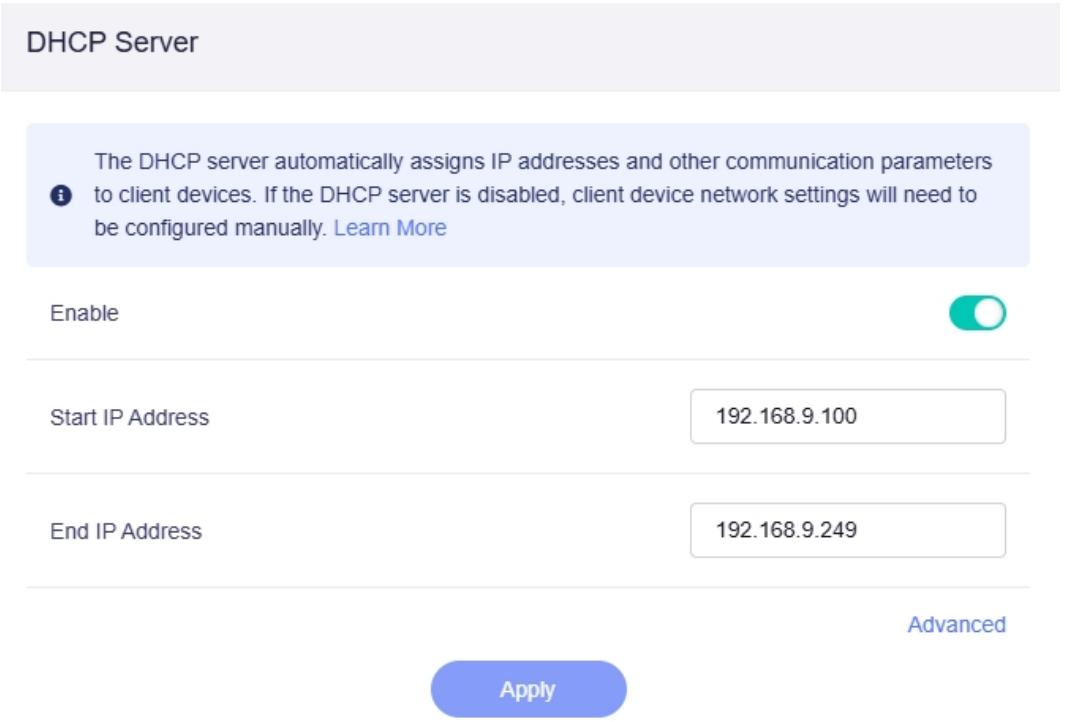


- **Gateway**: Standardmäßig 192.168.9.1. Sie können diese Adresse bei Bedarf ändern, sie darf jedoch nicht mit dem Gateway des Hauptnetzwerks kollidieren.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.
- **AP Isolation**: Isoliert Geräte im Gastnetzwerk voneinander, damit sie nicht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

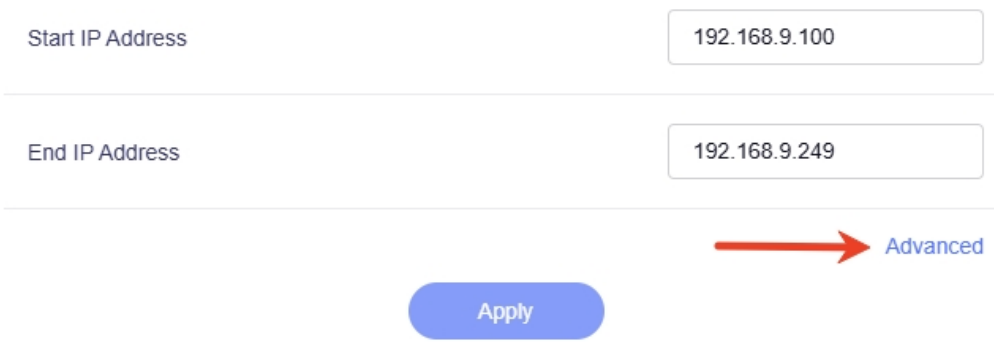
- **Block WAN Subnets**: Bei aktivierter Option kann das Gastnetzwerk nicht auf das übergeordnete Netzwerk oder dessen Netzwerksegment zugreifen.

12.3.2 DHCP-Server

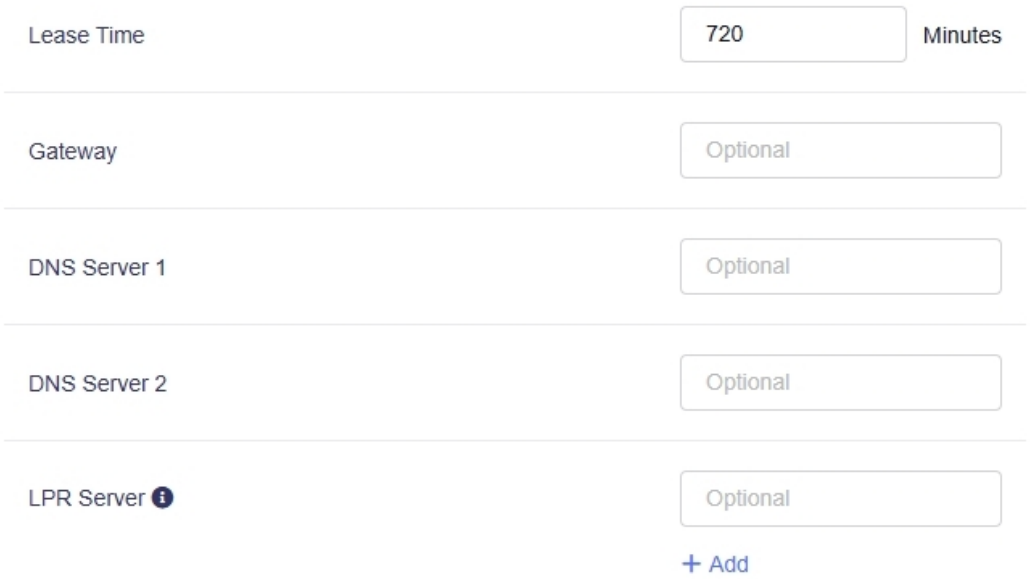
Das Gastnetzwerk ist standardmäßig deaktiviert. Sein DHCP-Server bleibt ebenfalls deaktiviert und ausgeblendet, bis Sie das Gastnetzwerk manuell aktivieren.
Bei aktiviertem DHCP-Server erhält jedes verbundene Endgerät automatisch eine IP-Adresse und weitere Kommunikationsparameter. Im Gastnetzwerk vergibt der DHCP-Server Adressen von 192.168.9.100 bis 192.168.9.249. Diesen Adressbereich können Sie bei Bedarf anpassen.



Klicken Sie unten rechts auf **Advanced**.



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



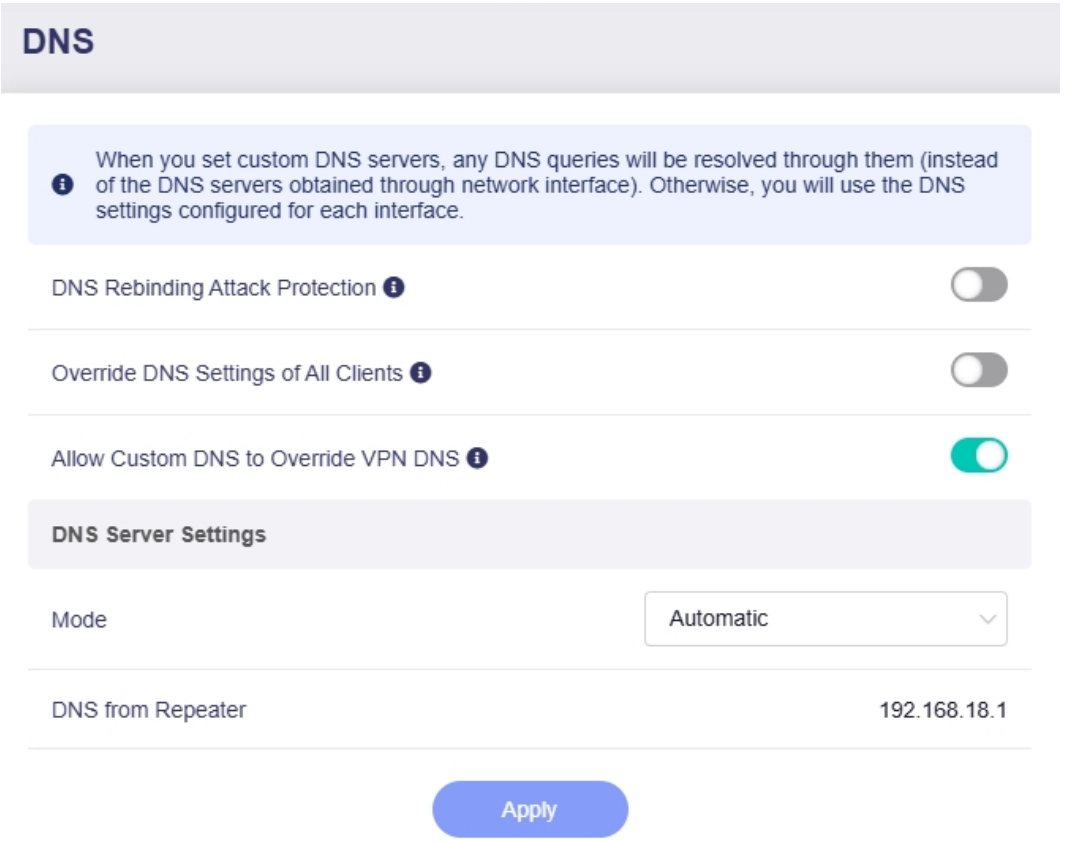
- **Lease Time**: Die Zeitspanne, für die ein Gerät eine vom DHCP-Server des Gastnetzwerks zugewiesene IP-Adresse verwenden darf.
- **Gateway**: Die Routerkomponente, die Datenverkehr zwischen dem Gastnetzwerk und externen Netzwerken wie dem Internet weiterleitet.
- **DNS Server 1**: Der primäre Server, 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.

12.4 DNS

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

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

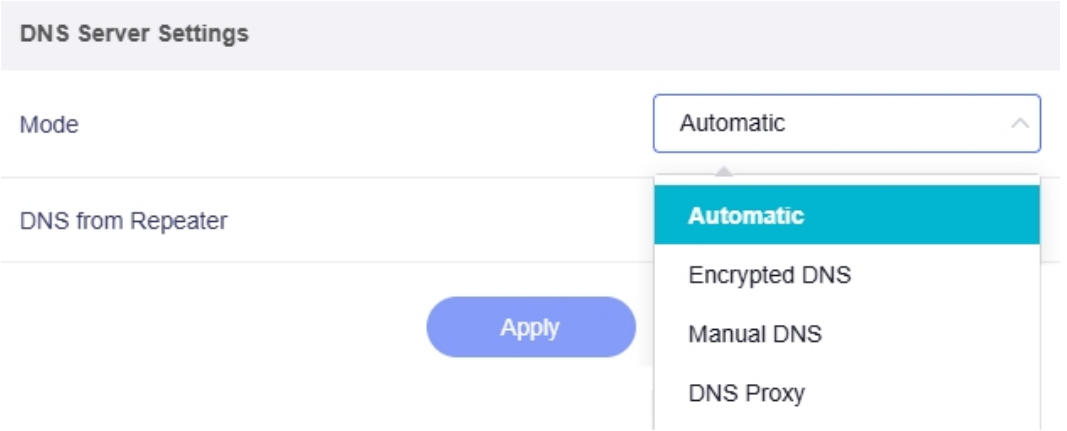
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **DNS**. Hier können Sie DNS-Einstellungen wie Sicherheitsoptionen, Servermodi und DNS-Prioritätsregeln für unterschiedliche Netzwerkszenarien konfigurieren.



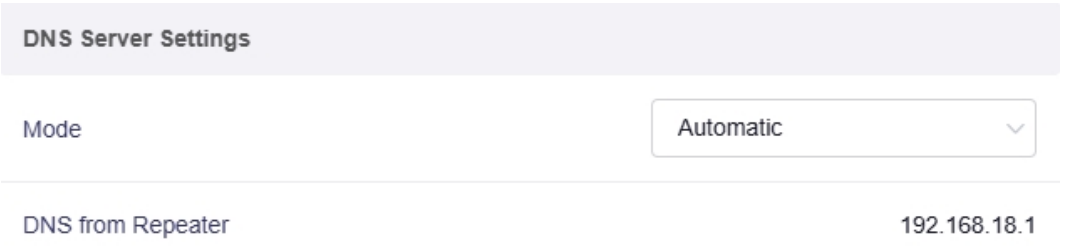
- **DNS Rebinding Attack Protection**: Schützt vor DNS-Rebinding-Angriffen, indem bösartige Namensauflösungen blockiert werden. Dadurch kann die Auflösung privater Adressen fehlschlagen. Deaktivieren Sie die Option, wenn Ihr Netzwerk ein Captive Portal verwendet, etwa eine Anmeldeseite in einem öffentlichen 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.

12.4.1 DNS-Servereinstellungen

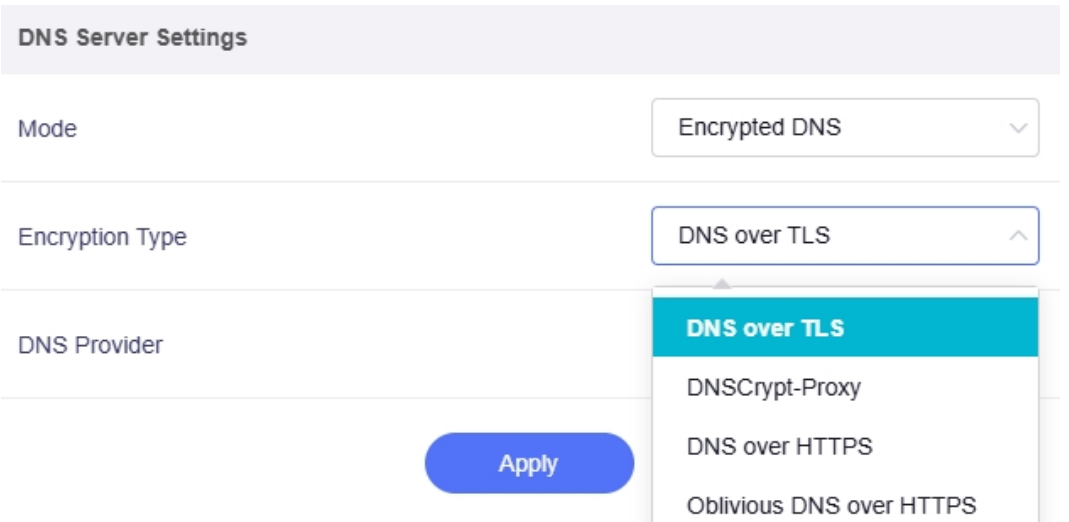
Für den DNS-Server stehen vier Modi zur Verfügung: Automatic, Encrypted DNS, Manual DNS und DNS Proxy.



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



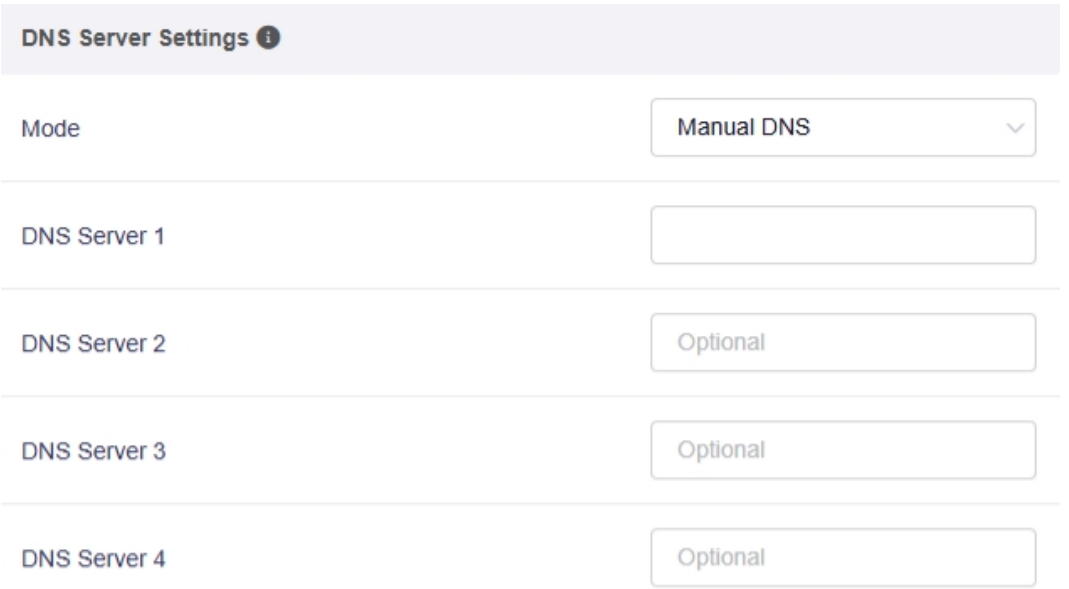
2. **Encrypted DNS**: Der Router verarbeitet DNS-Anfragen über verschlüsselte Protokolle und schützt die Auflösungsdaten so vor Abhören und Manipulation.
   Es stehen vier Verfahren zur Auswahl: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS.



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

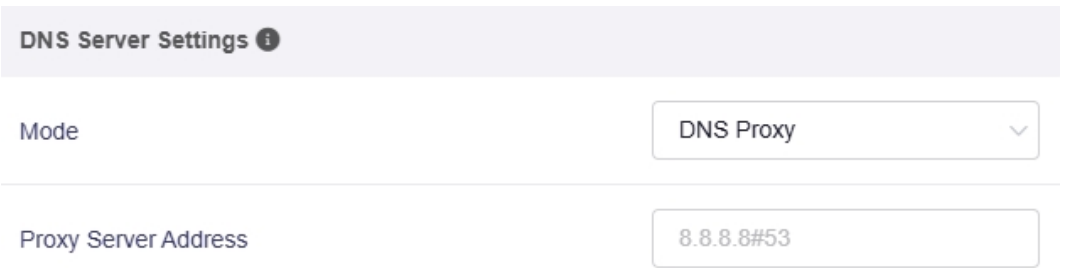
- Bei den drei anderen Verfahren wählen Sie mindestens einen DNS-Server aus dem Verzeichnis aus. Es sind bis zu acht Server möglich. Bei mehreren ausgewählten Servern verwendet der Router automatisch den schnellsten.

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



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

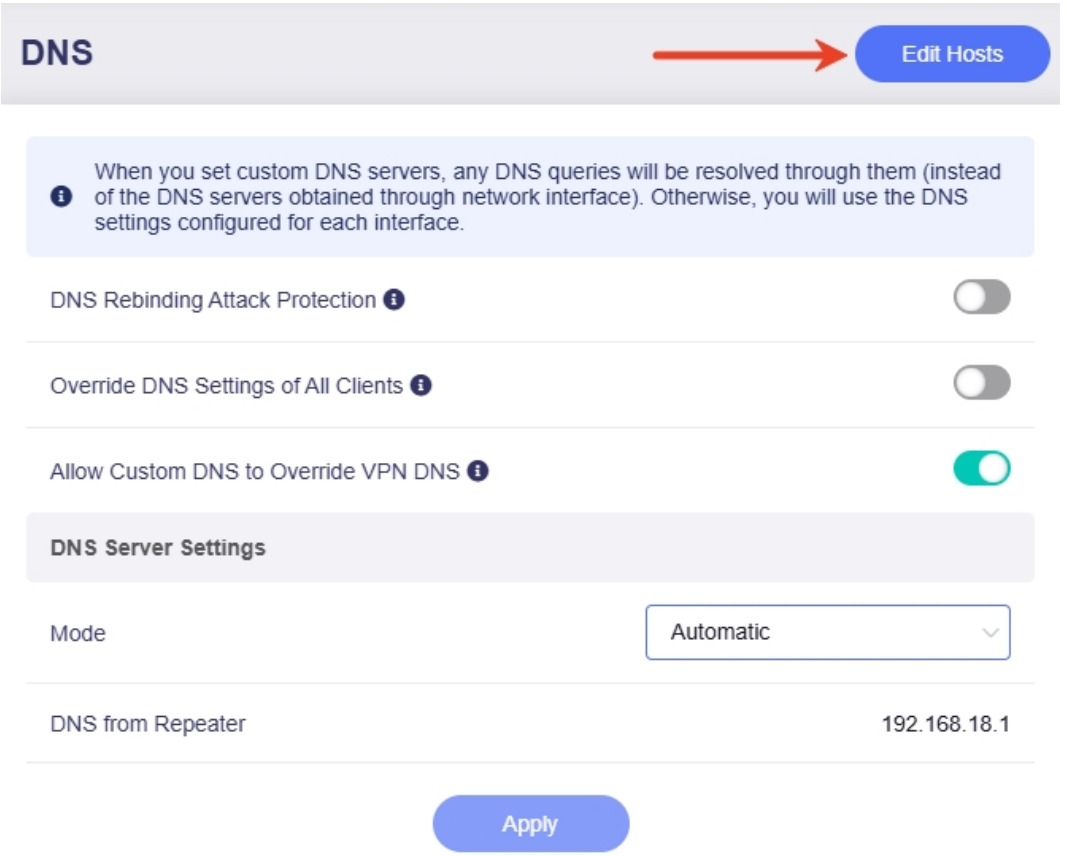
4. **DNS Proxy**: Der Router leitet alle DNS-Anfragen über einen Proxyserver weiter. Die Namensauflösung erfolgt in dessen Netzwerkumgebung, um besondere Zugriffsanforderungen zu erfüllen.



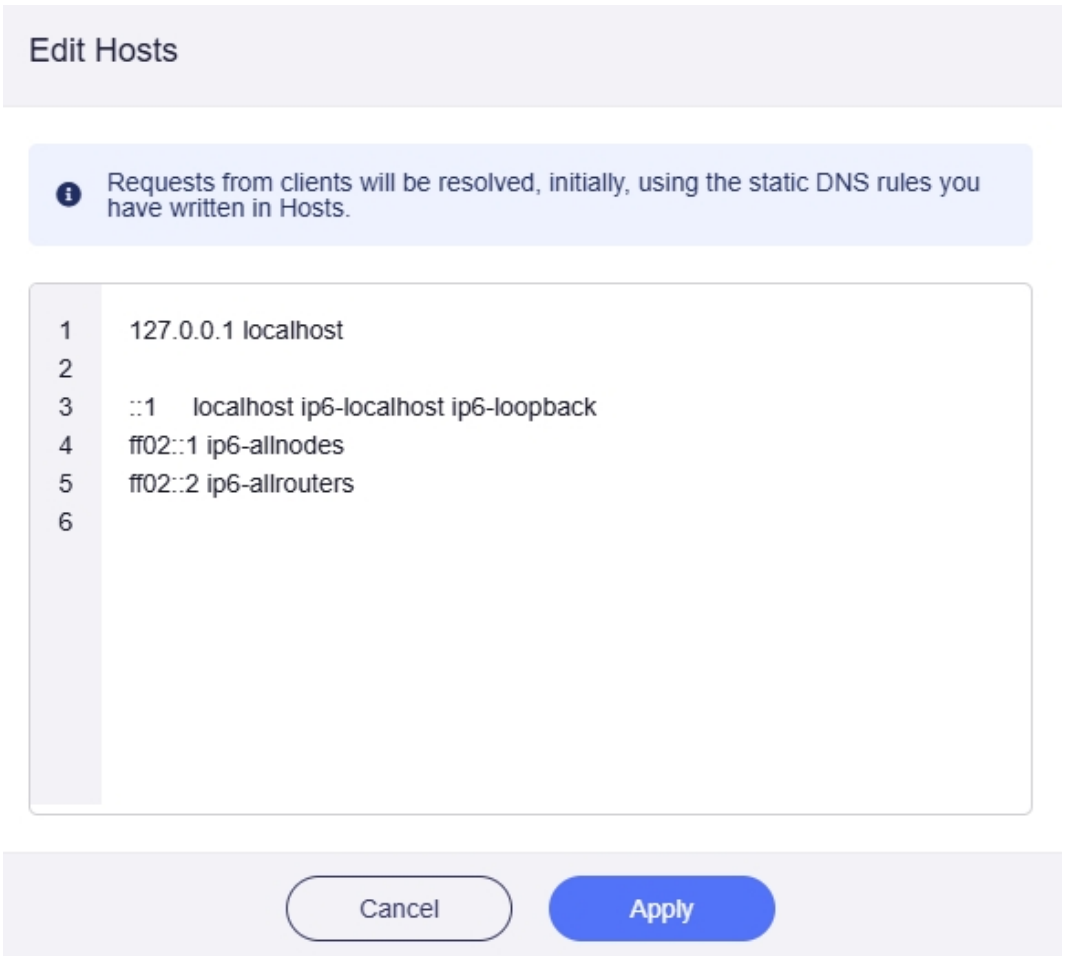
12.4.2 Hosts bearbeiten

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

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



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

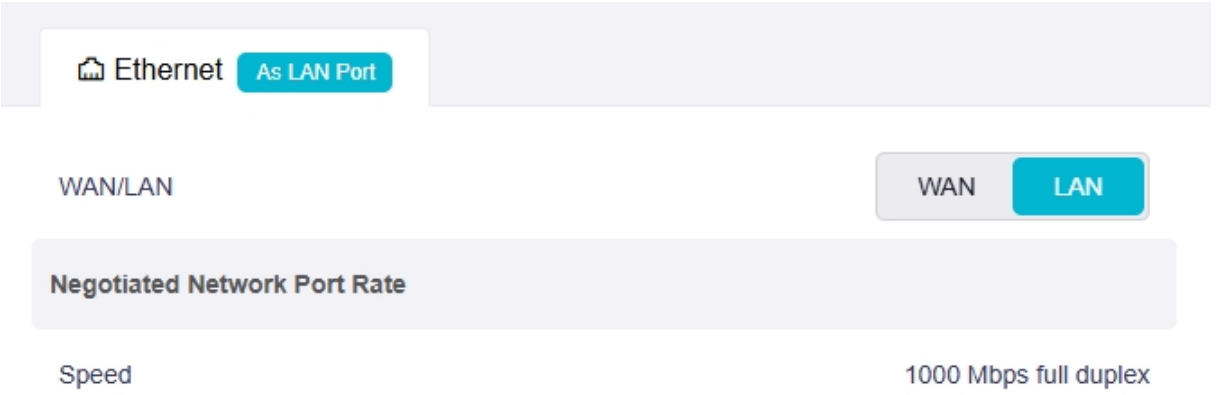

Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 Ethernetanschlüsse

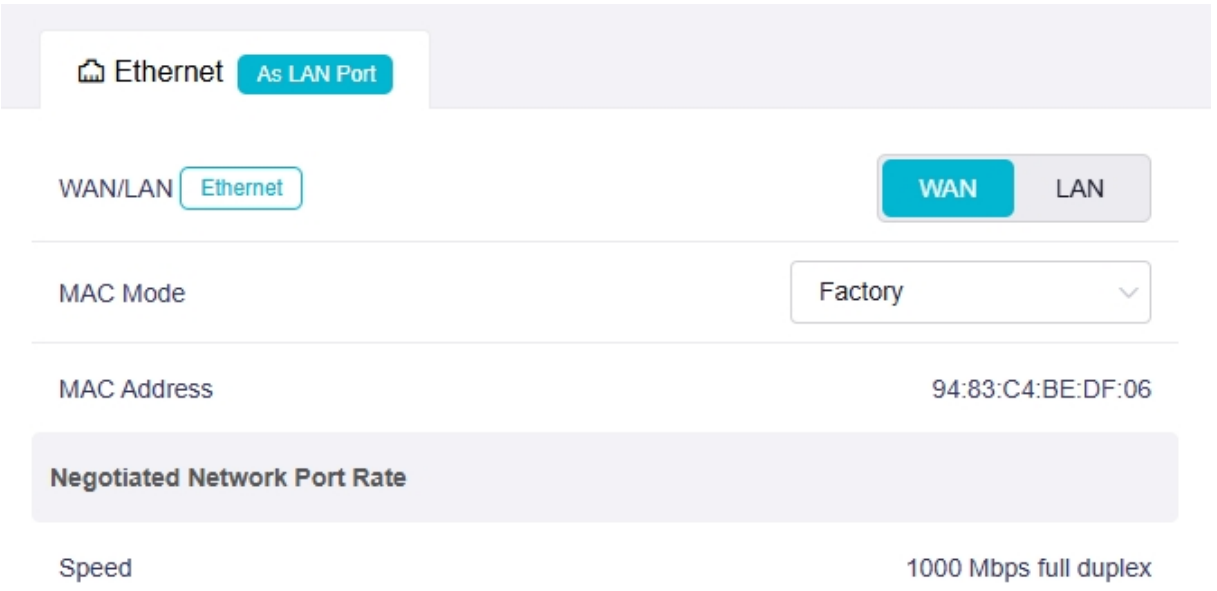
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Ethernet Port**. Auf dieser Seite verwalten Sie die Ethernetanschlüsse des Routers.

Mudi 7 verfügt über einen Ethernetanschluss. Dieser ist standardmäßig als LAN-Anschluss eingerichtet. Sie können seine Funktion zwischen WAN und LAN umschalten.

Bei der Funktion **LAN** zeigt die Seite die Anschlussfunktion und die ausgehandelte Verbindungsgeschwindigkeit an.



Bei der Funktion **WAN** zeigt die Seite die Anschlussfunktion, den MAC-Modus, die MAC-Adresse und die ausgehandelte Verbindungsgeschwindigkeit an.



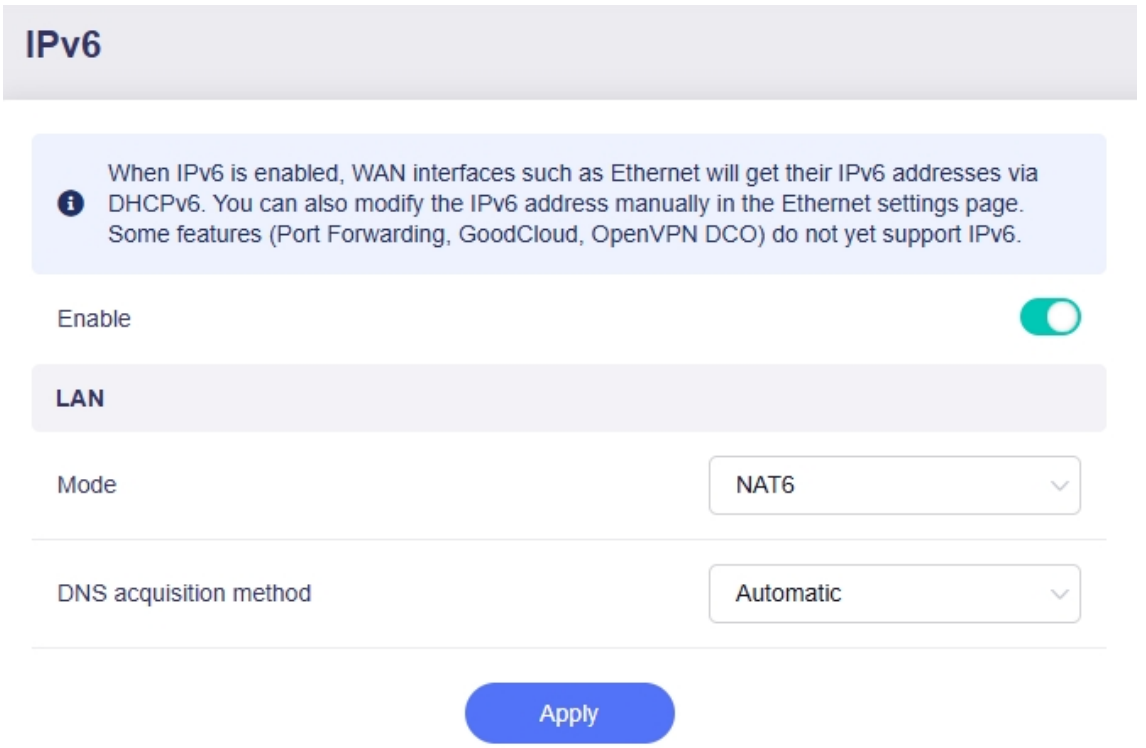
Hinweis: Die ausgehandelte Verbindungsgeschwindigkeit wird nur bei angeschlossenem Ethernetkabel angezeigt. Sie hängt sowohl vom Ethernetanschluss als auch vom Ethernetkabel ab.

12.6 IPv6

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

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

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



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

12.6.1 IPv6-Modus

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

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

12.6.2 DNS-Adressen beziehen

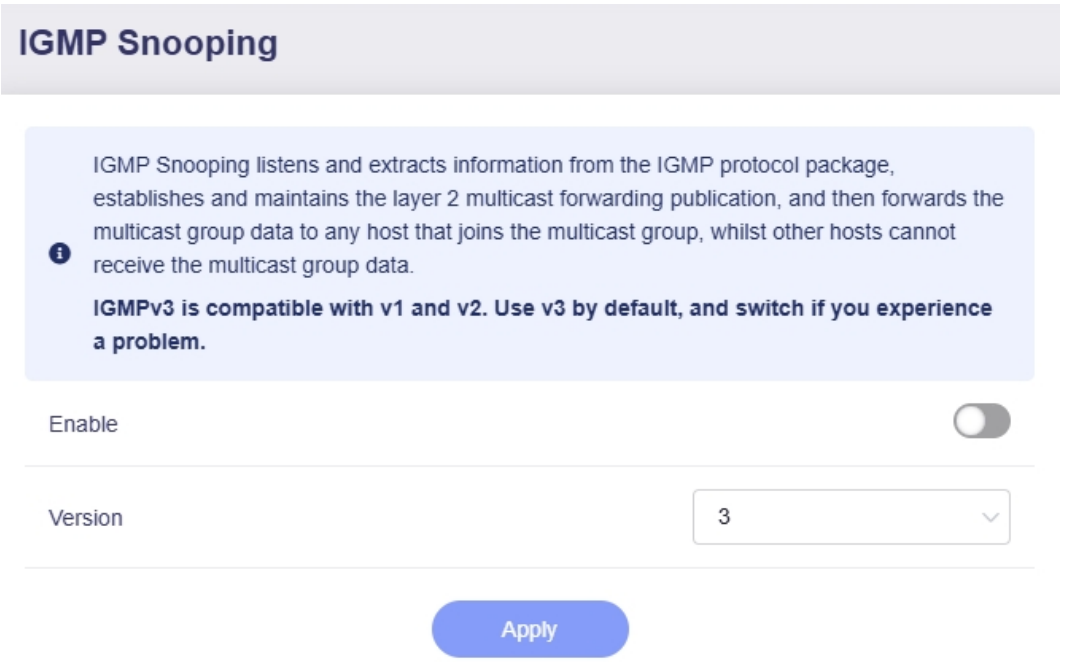
Diese Einstellung bestimmt, wie der Router IPv6-DNS-Serveradressen erhält. Zur Auswahl stehen Automatic und Manual.

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

12.7 IGMP Snooping

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

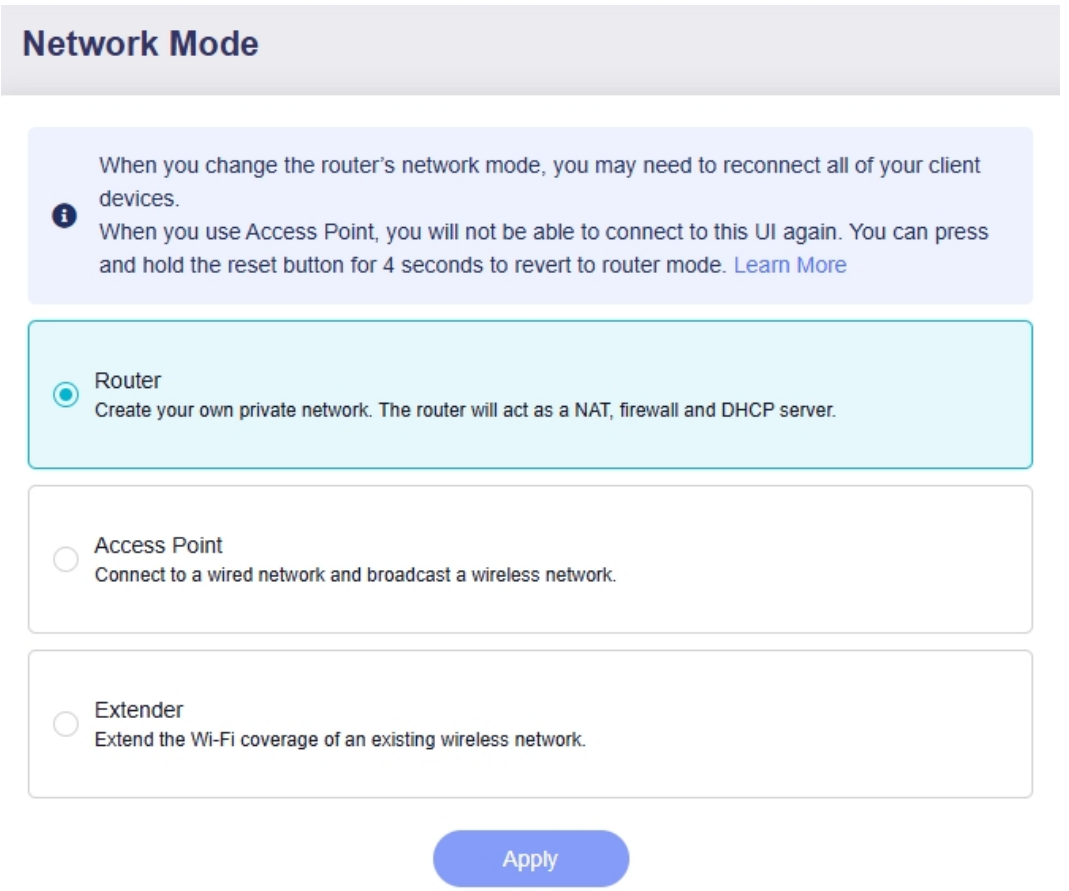
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **IGMP Snooping**. Aktivieren Sie die Funktion bei Bedarf, um Multicast auf Ihrem Router zu nutzen.



12.8 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.

Hinweis:

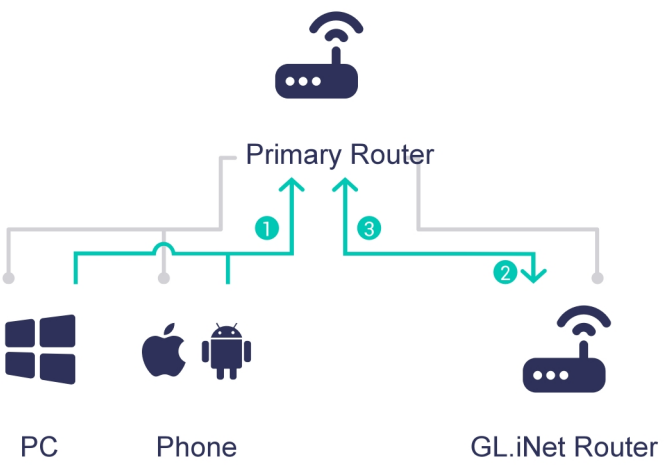
1. Nach einer Änderung des Netzwerkmodus sollten sich alle Endgeräte erneut mit dem Router verbinden, um eine stabile Verbindung sicherzustellen.
2. **Im Access-Point-Modus ist die Weboberfläche nicht mehr über die ursprüngliche IP-Adresse erreichbar**. Melden Sie sich am vorgeschalteten Router an und ermitteln Sie die IP-Adresse, die er diesem Router zugewiesen hat. Öffnen Sie die Weboberfläche anschließend über diese Adresse. Haben Sie keinen Zugriff auf den vorgeschalteten Router, halten Sie die Reset-Taste 4 Sekunden lang gedrückt, um zum standardmäßigen Router-Modus zurückzukehren.
3. **Im Access-Point- und Extender-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.

12.9 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 Netzwerksystem. Der Datenverkehr der Endgeräte wird zur Verarbeitung durch den GL.iNet-Router und anschließend über den Hauptrouter weitergeleitet. Die vorhandenen Netzwerkeinstellungen bleiben erhalten, damit alle verbundenen Geräte weiterhin unterbrechungsfrei arbeiten. Gleichzeitig können Sie den Datenverkehr aller oder ausgewählter Endgeräte nach Bedarf verwalten.



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

- **Graue Linien** zeigen die physischen Verbindungen: Endgeräte wie Computer und Laptops sind mit dem Hauptrouter verbunden. Dessen LAN-Anschluss ist per Ethernetkabel mit dem WAN-Anschluss des GL.iNet-Routers verbunden, auf dem Drop-in Gateway aktiviert ist.

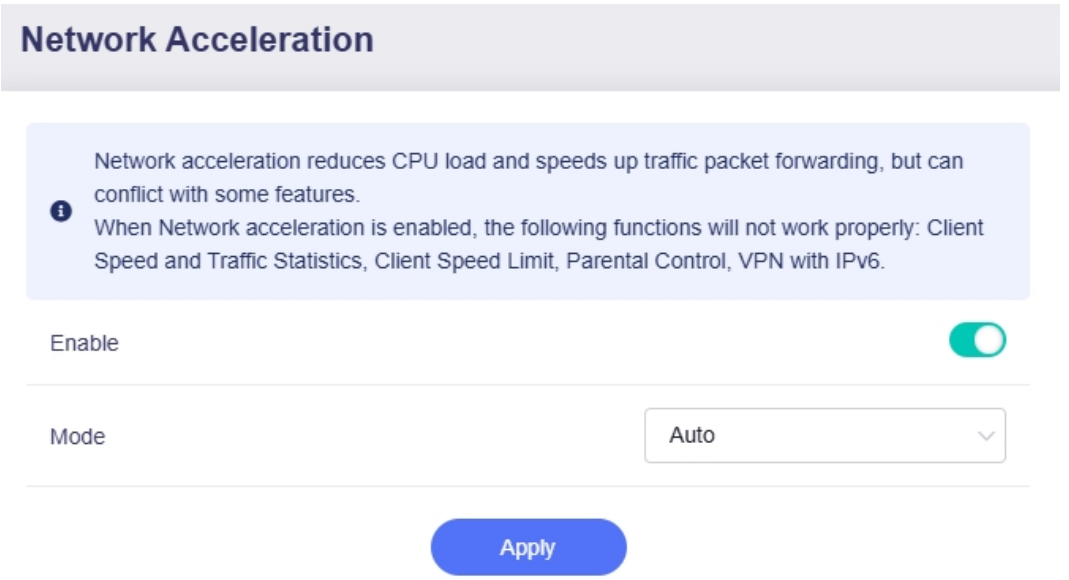
- **Grüne Linien** zeigen den Datenweg bei aktiviertem Drop-in Gateway. Die nummerierten Pfeile geben die Reihenfolge an:
    1. Der Datenverkehr der Endgeräte gelangt zunächst zum Hauptrouter.
    2. Der Hauptrouter leitet ihn zur Verarbeitung an den GL.iNet-Router weiter, etwa zum Filtern von Werbung oder zur VPN-Verschlüsselung.
    3. Nach der Verarbeitung gelangt der Datenverkehr zurück zum Hauptrouter. Dieser übermittelt die Daten an die ursprünglichen Endgeräte oder leitet sie ins Internet weiter.

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

12.10 Netzwerkbeschleunigung

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

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



- **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.

Kapitel 13

Datenverkehr steuern

Dieses Kapitel stellt die Kindersicherung als Funktion zur Steuerung des Datenverkehrs vor.

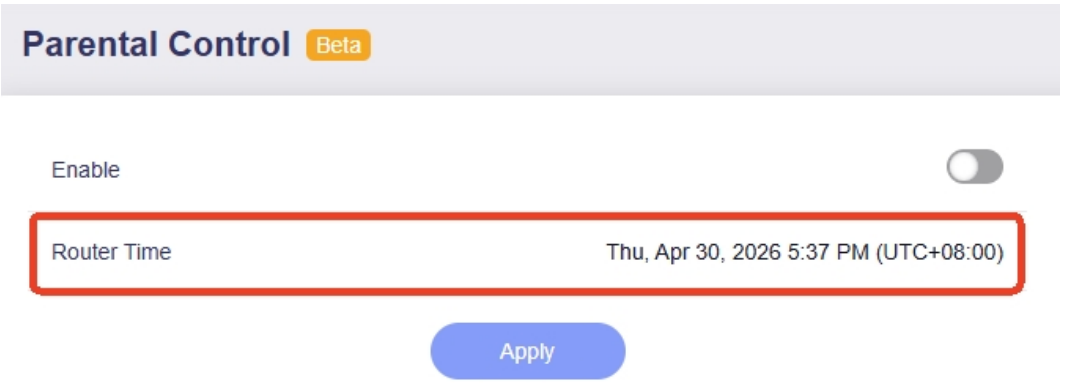
13.1 Kindersicherung

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.

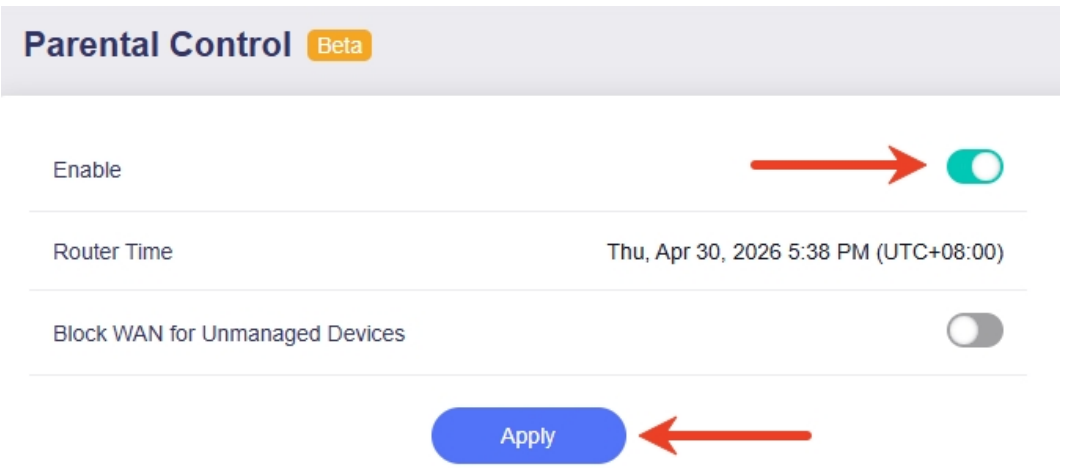
13.1.1 Schnelleinrichtung

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

1. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **FLOW CONTROL** > **Parental Control.** Stellen Sie sicher, dass die Uhrzeit des Routers korrekt ist. Synchronisieren Sie sie bei Bedarf 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.



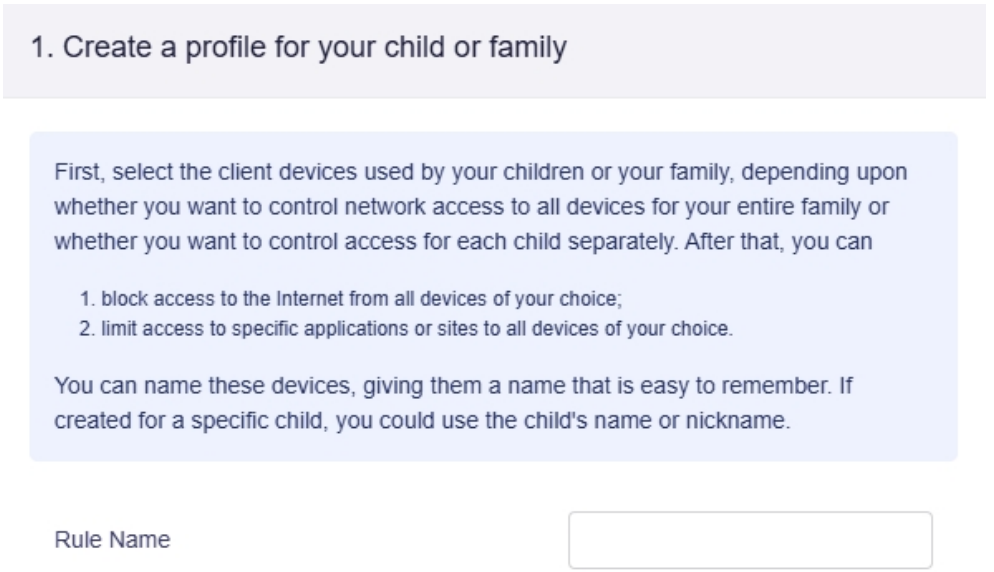
- **Block WAN for Unmanaged Devices**: Sperrt den Internetzugang für alle Geräte, die nicht in der Kindersicherungsliste stehen.

Das folgende Beispiel zeigt eine mögliche Anwendung.

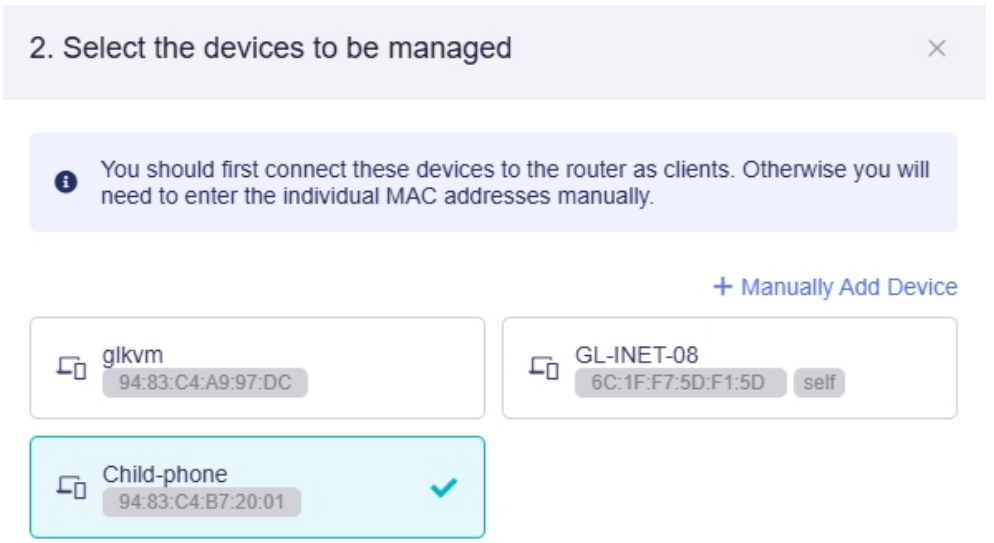
Szenario: Geräte in diesem Profil dürfen an Wochentagen von 08:00 bis 11:00 Uhr zum Lernen und am Wochenende von 18:00 bis 20:00 Uhr zum Spielen auf das Internet zugreifen. Zu allen anderen Zeiten ist der Internetzugang standardmäßig gesperrt.

Einrichtung:

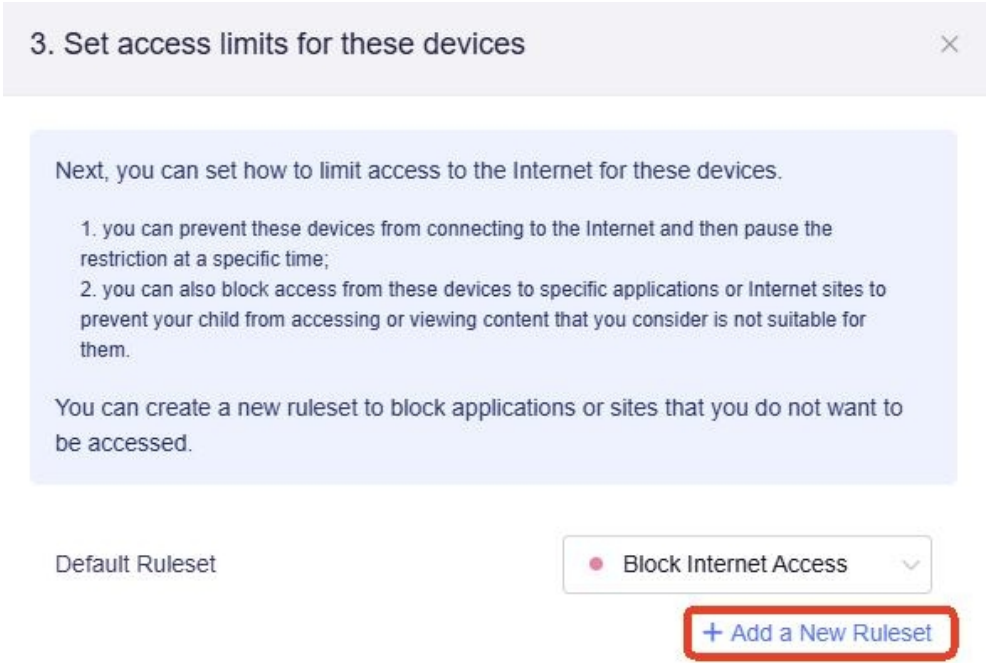
1. Erstellen Sie ein Profil und vergeben Sie einen Namen.



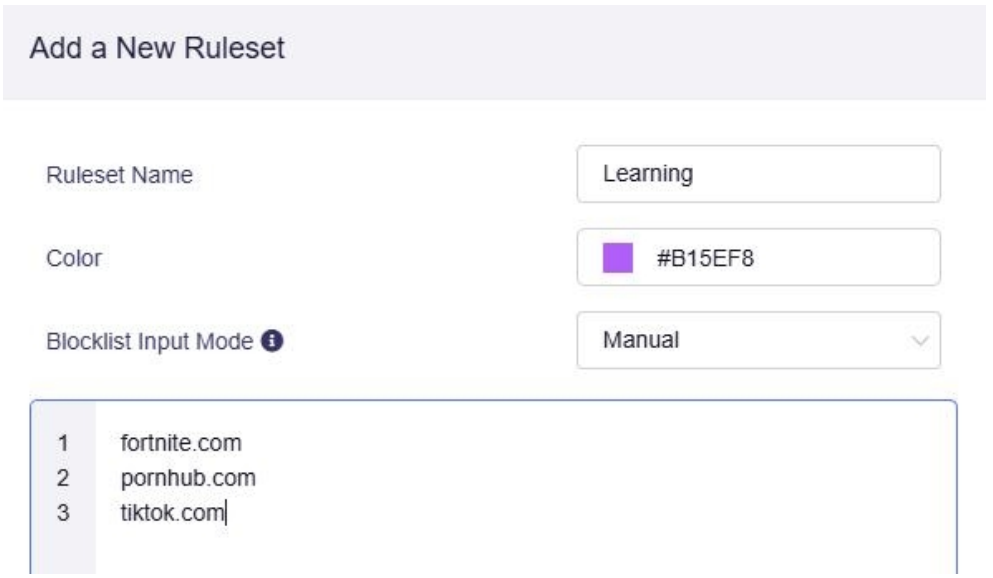
2. Wählen Sie die zu verwaltenden Geräte aus. Verbinden Sie diese zunächst mit dem Router. Noch nicht verbundene Geräte können Sie durch Eingabe ihrer MAC-Adressen manuell hinzufügen.



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**.

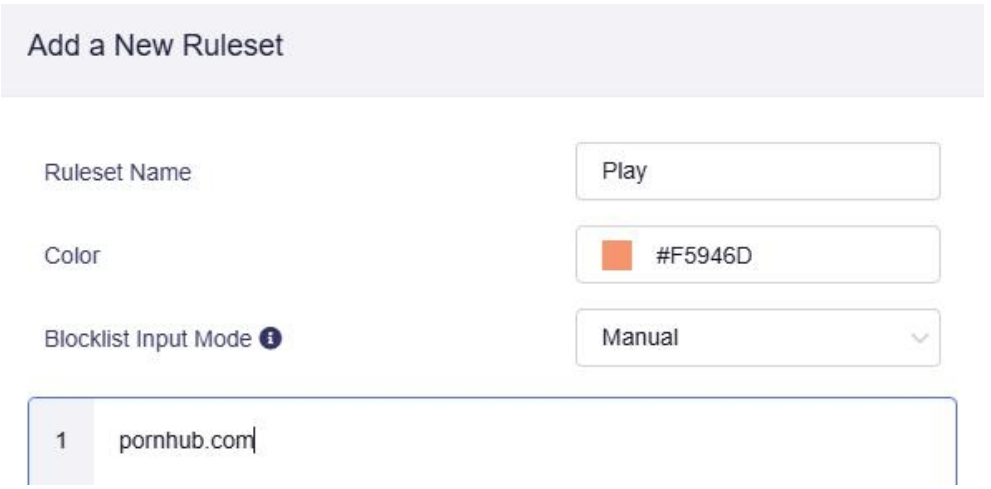


   Legen Sie Namen, etwa Learning, und Farbe des Regelsatzes fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.

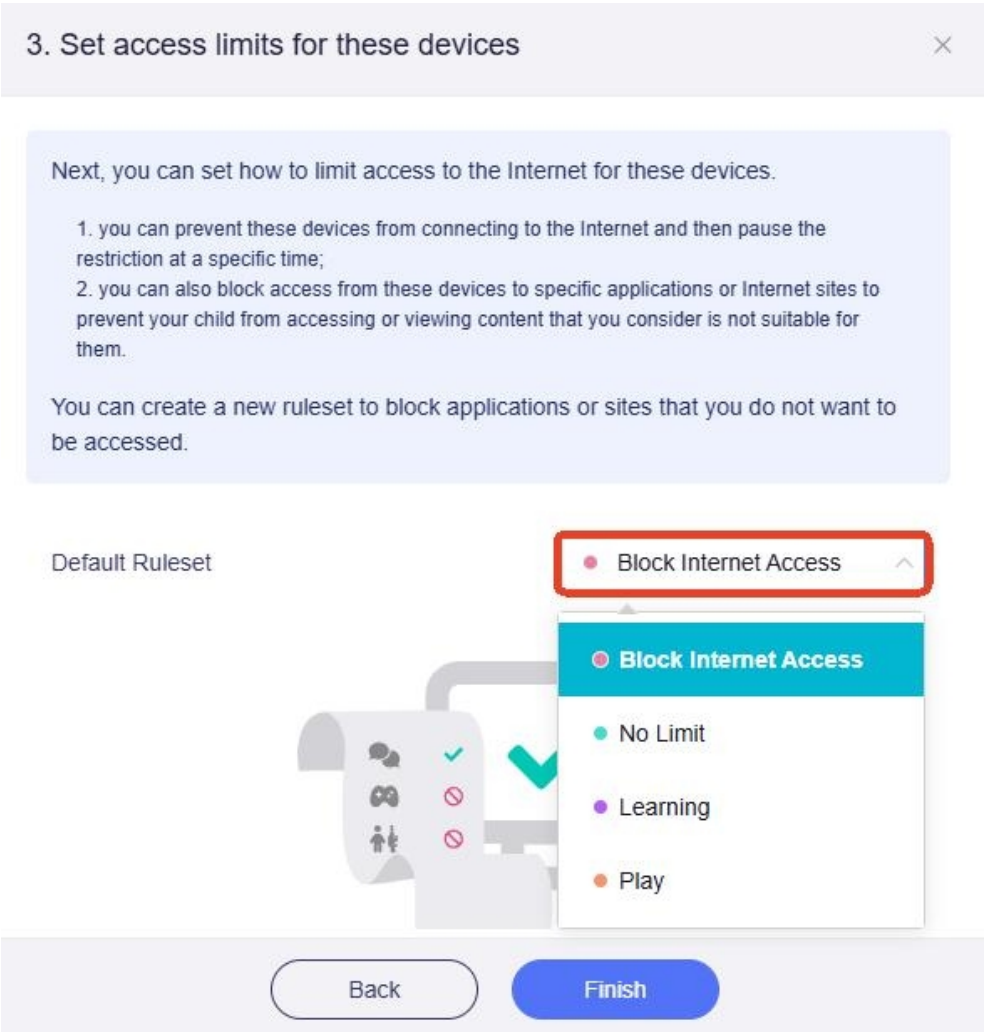


   Hinweis: Die Domainnamen auf der Sperrliste umfassen auch ihre Subdomains. Der Eintrag „example.com“ schließt beispielsweise „subdomain.example.com“ und alle weiteren Subdomains ein.

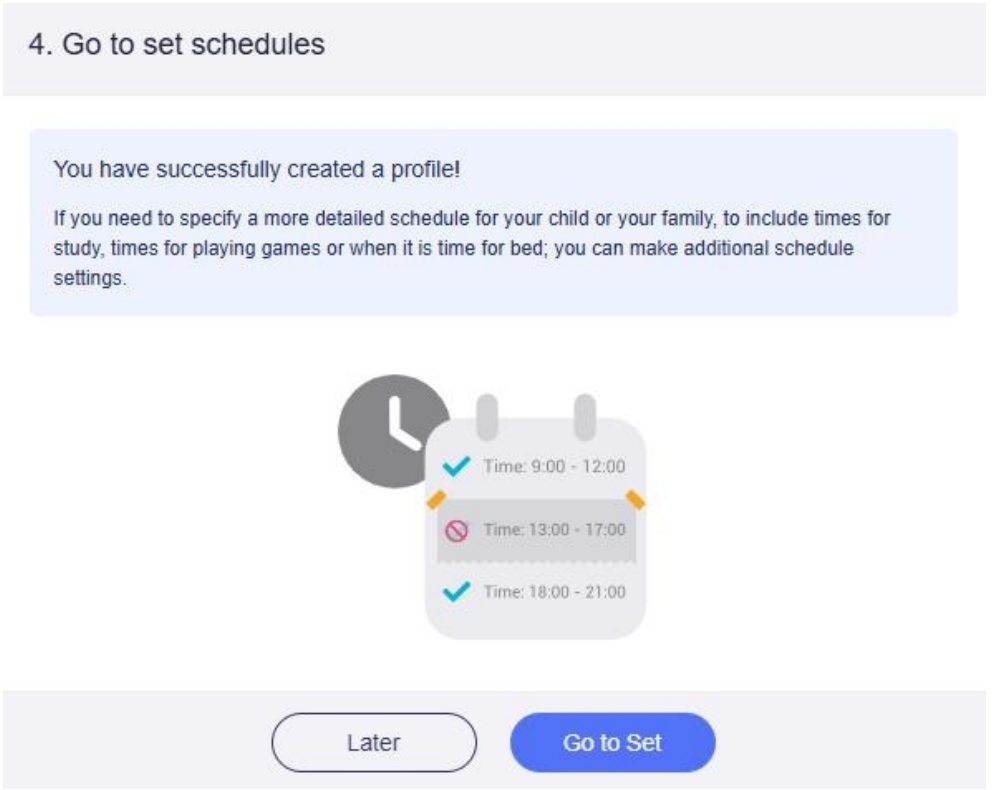
Erstellen Sie auf dieselbe Weise den zweiten Regelsatz. Legen Sie Namen, etwa Play, und Farbe fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.



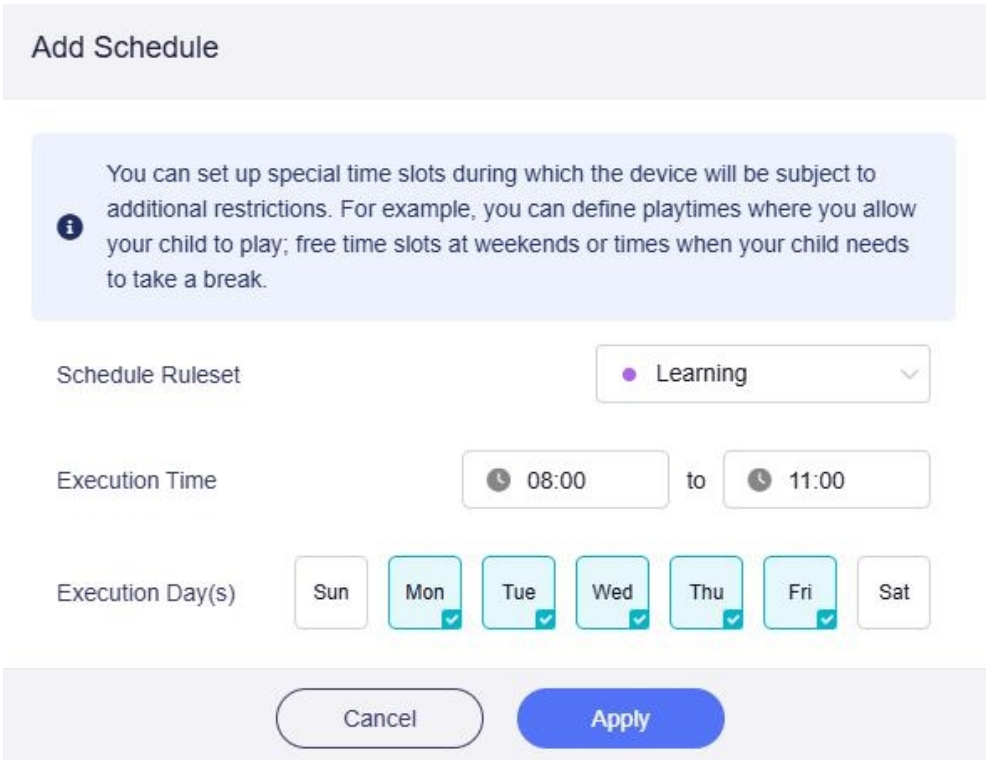
Nun sind insgesamt vier Regelsätze vorhanden. Wählen Sie **Block Internet Access** als **Default Ruleset** aus und klicken Sie auf **Finish**.



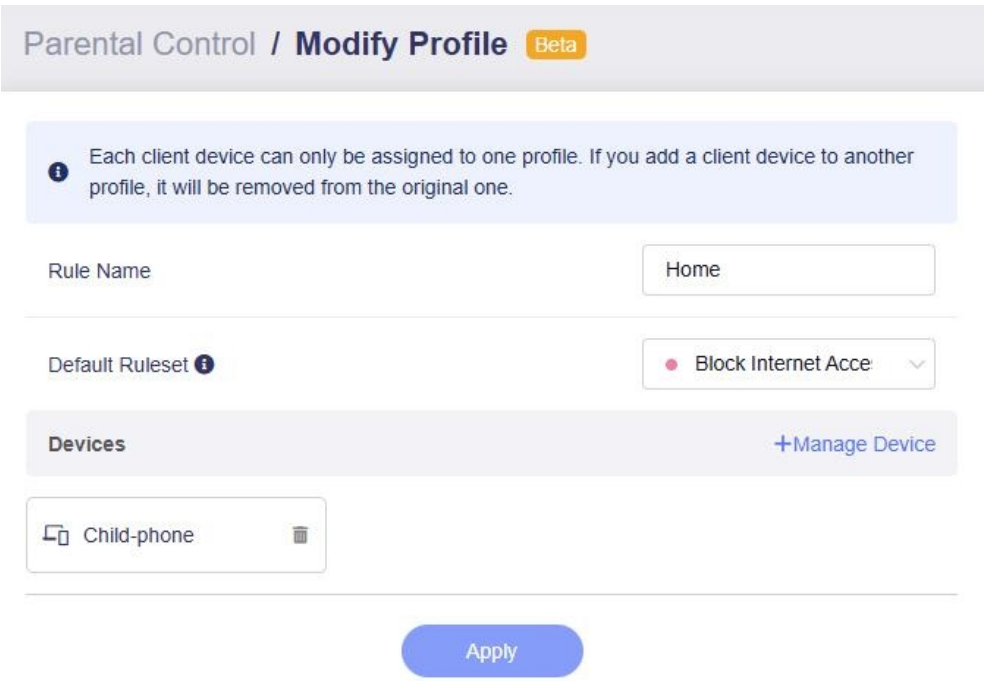
4. Erstellen Sie anschließend einen Zeitplan für Ihr Profil. Klicken Sie auf **Go to Set**.



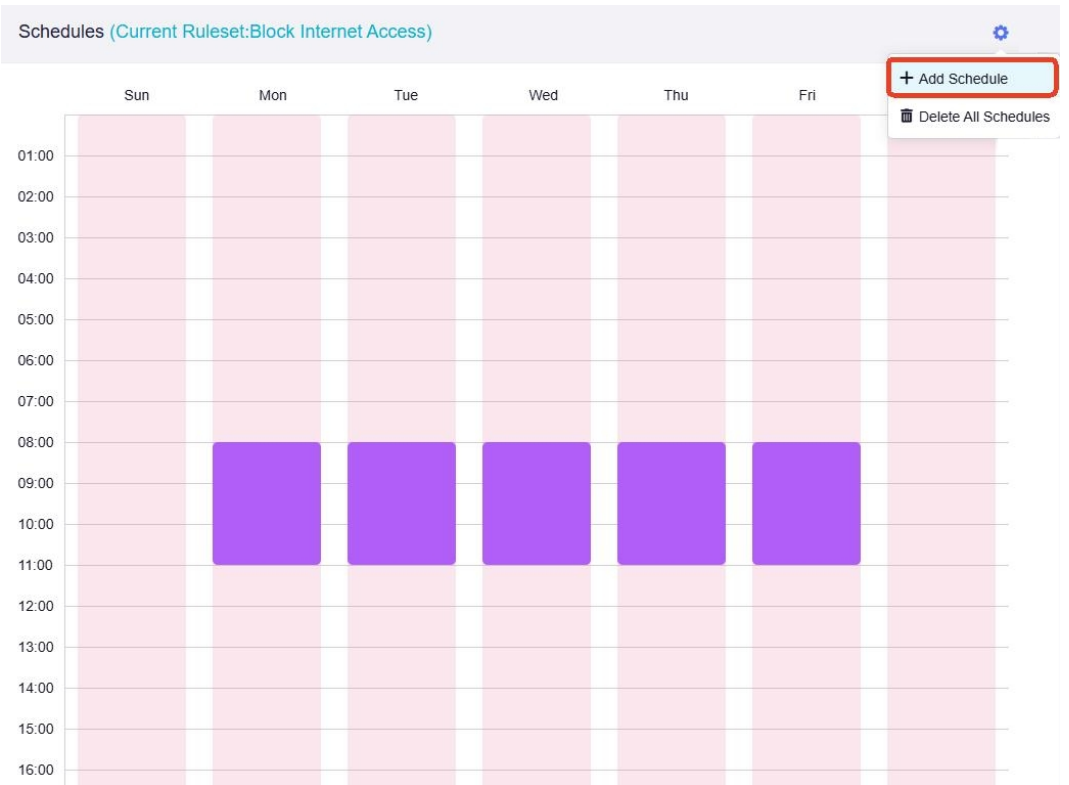
Fügen Sie den Regelsatz **Learning** zum Zeitplan hinzu. Legen Sie unter **Execution Time** an Wochentagen 08:00 bis 11:00 Uhr fest und klicken Sie auf **Apply**.



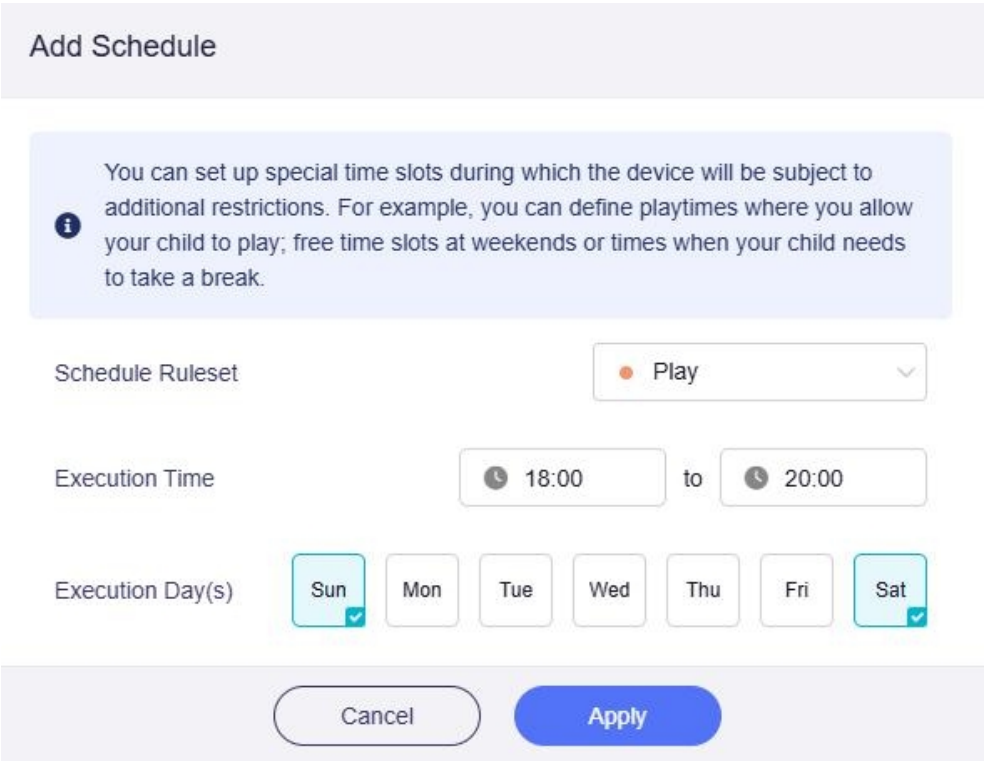
5. Sie gelangen zur Bearbeitungsseite des angelegten Profils.



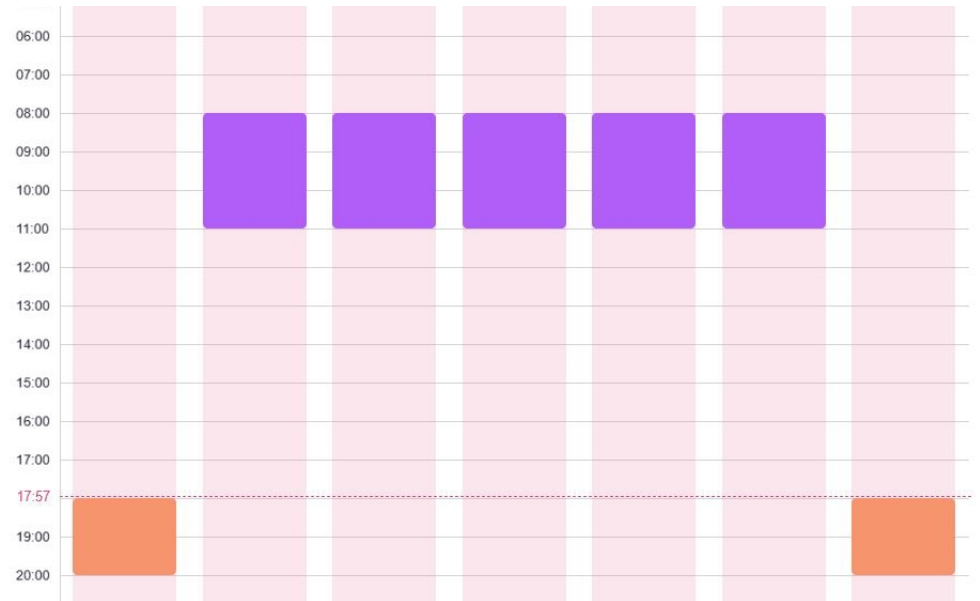
Unten sehen Sie den angelegten Zeitplan. Klicken Sie oben rechts auf das Zahnradsymbol und wählen Sie **Add Schedule**.



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**.



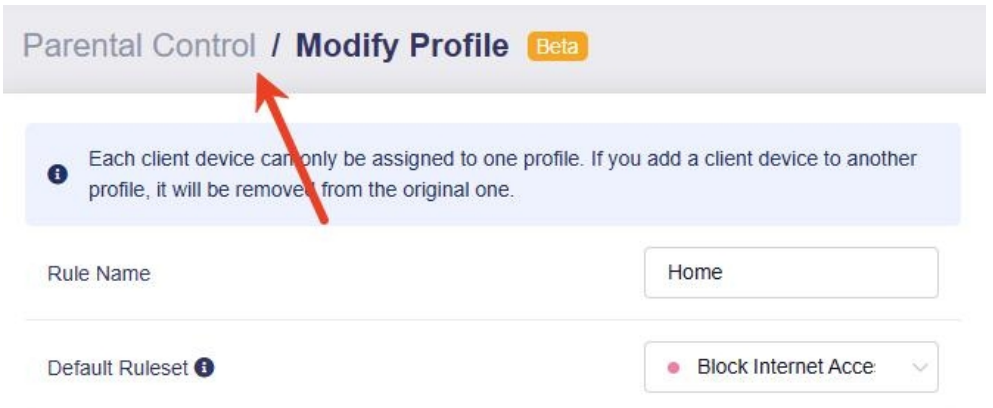
Der Regelsatz Play wird in den Zeitplan aufgenommen.



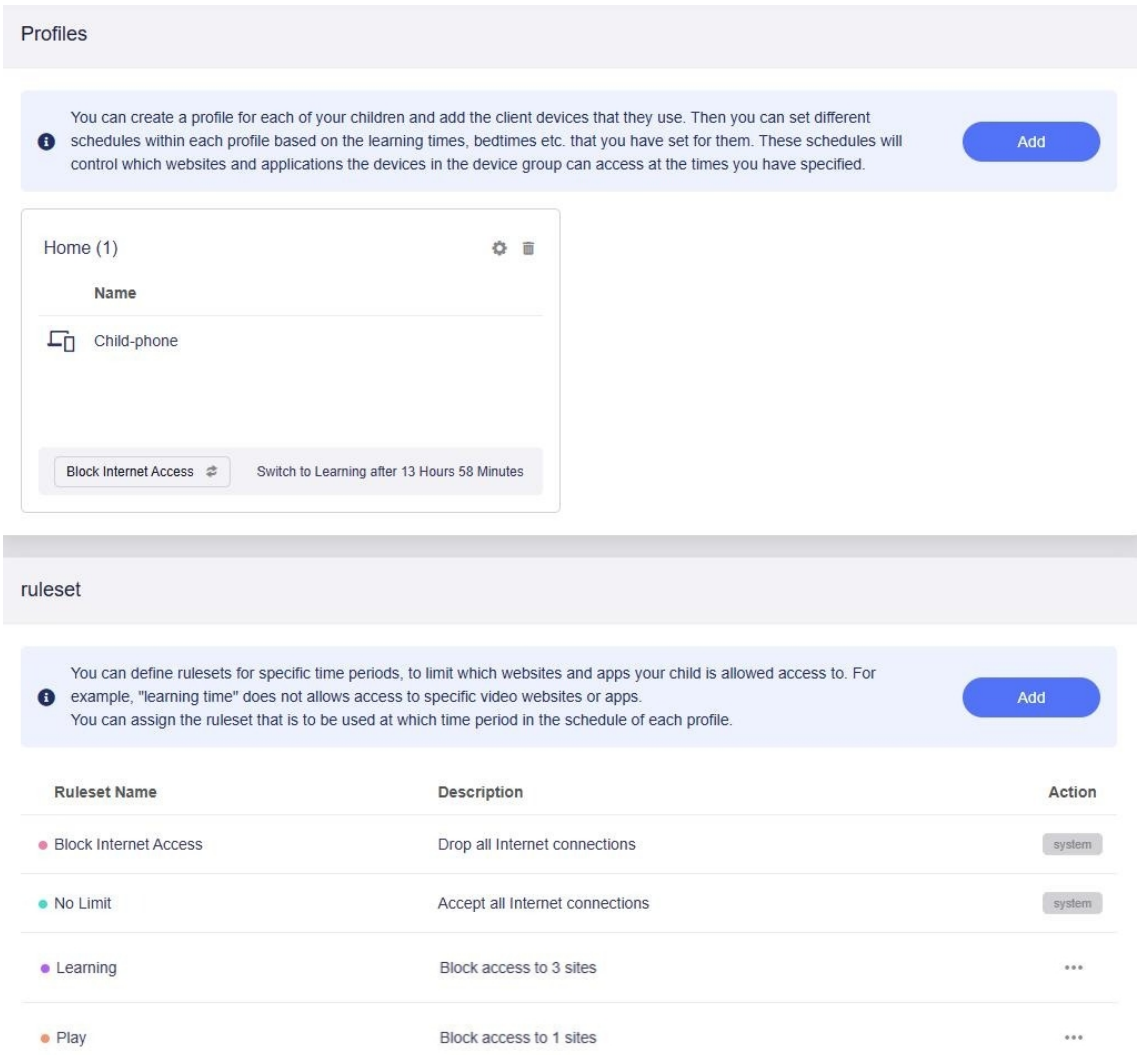
Tipps:

- 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.



13.1.2 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.

Kapitel 14

Sicherheit

Dieses Kapitel beschreibt die Netzwerksicherheit, darunter Portweiterleitung, Administratorzugriff und NAT-Modus, um Netzwerkzugriff und Sicherheit aufeinander abzustimmen.

14.1 Portweiterleitung

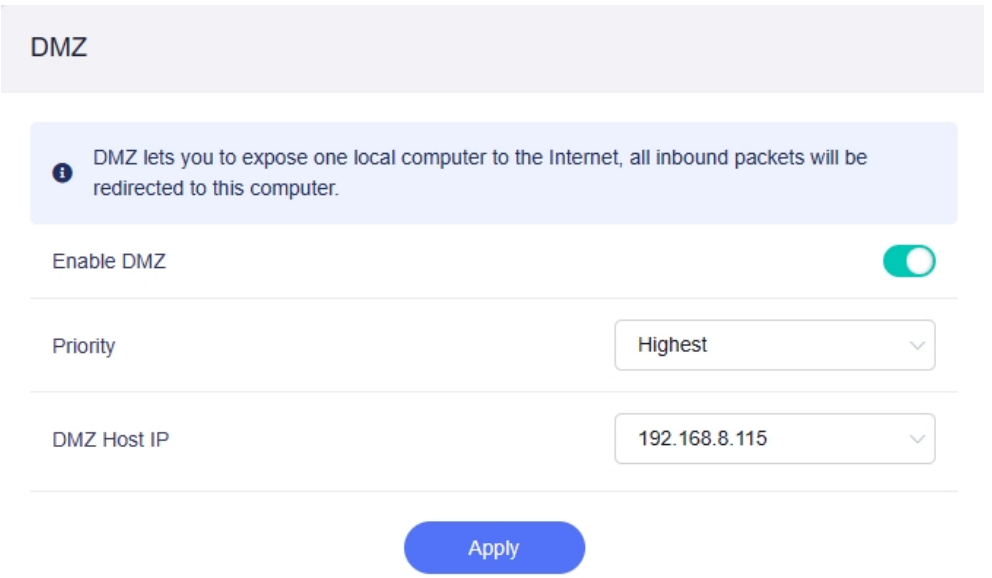
Portweiterleitung leitet externe Anfragen an bestimmte Geräte in Ihrem lokalen Netzwerk weiter. Die Seite Port Forwarding umfasst zwei zentrale Funktionen: **DMZ** für den direkten vollständigen Zugriff auf ein einzelnes Gerät und **Port Forwarding** für den gezielten Zugriff auf bestimmte Geräteports.

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 **SECURITY** > **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**.



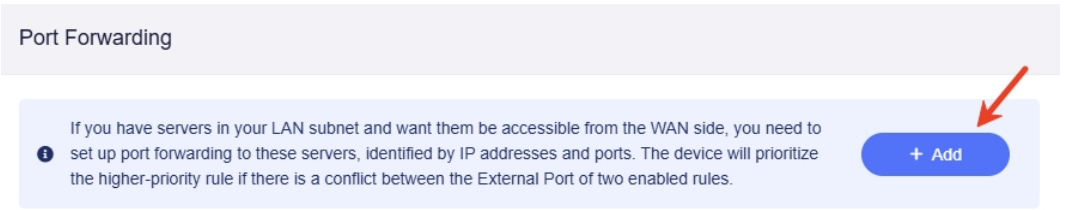
- **Priority**: Wählen Sie Highest oder Lowest. Hat DMZ eine höhere Priorität als die Portweiterleitungsregeln, werden alle Portweiterleitungsregeln außer Kraft gesetzt. Andernfalls werden Anfragen nur dann an das DMZ-Endgerät weitergeleitet, wenn für den angefragten Port keine Portweiterleitungsregel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

14.1.2 Portweiterleitung

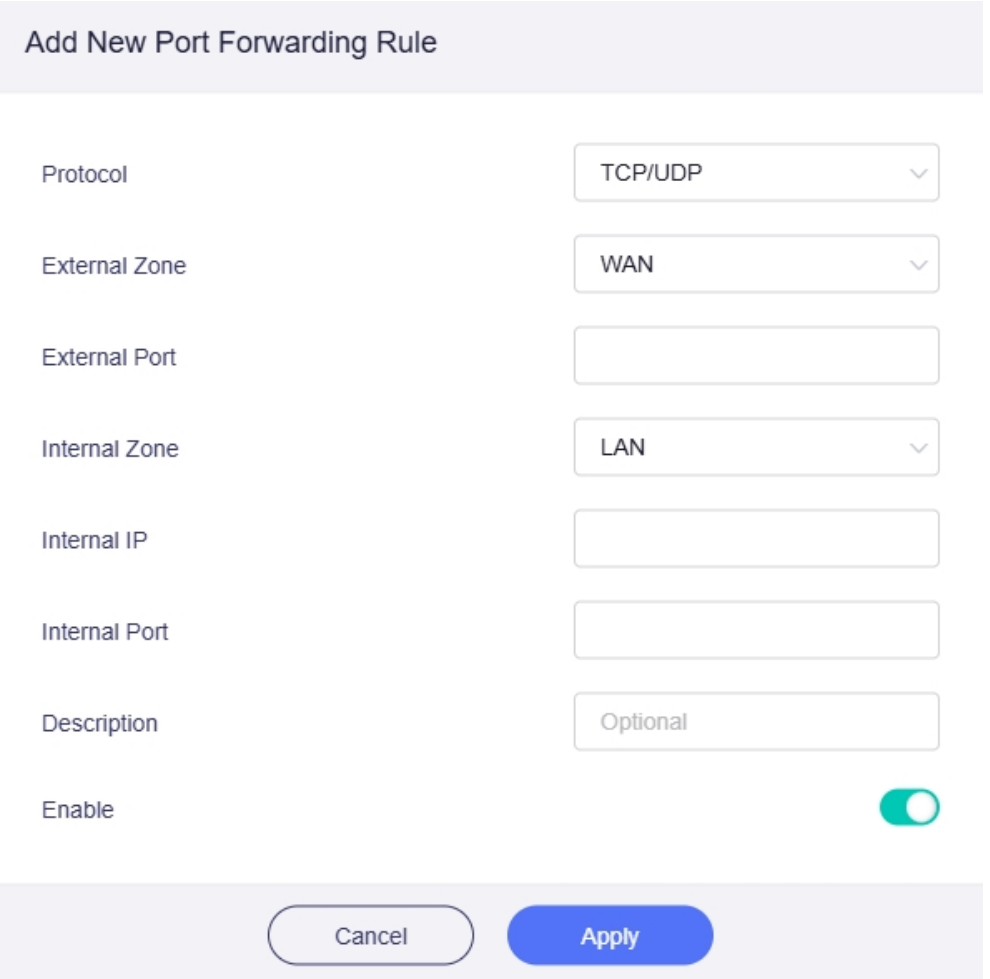
Portweiterleitungen ermöglichen entfernten Computern die Verbindung mit einem lokalen Computer oder Server hinter der LAN-Firewall, beispielsweise einem Web- oder FTP-Server.

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

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



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



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

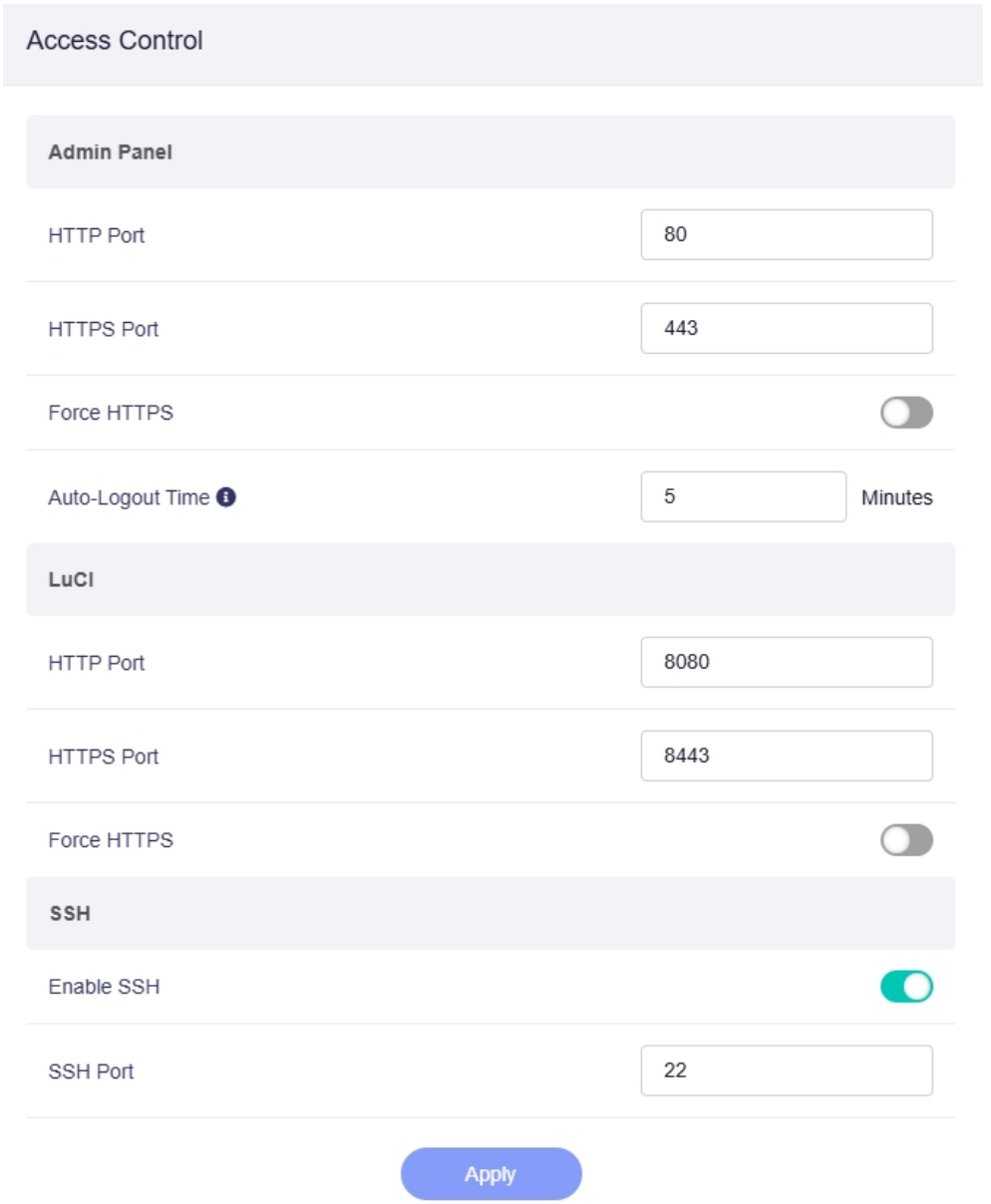
- **Description**: Legen Sie einen Namen fest oder geben Sie eine Beschreibung für die Portweiterleitungsregel ein (optional).
- **Enable**: Aktiviert oder deaktiviert diese Regel.

14.2 Administratorzugriff

Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **SECURITY** > **Admin Access**. Hier konfigurieren Sie den lokalen Zugriff, den HTTPS-/SSH-Fernzugriff und offene Ports am Router, um Ihren Router und Ihr Netzwerk zu schützen.

14.2.1 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.

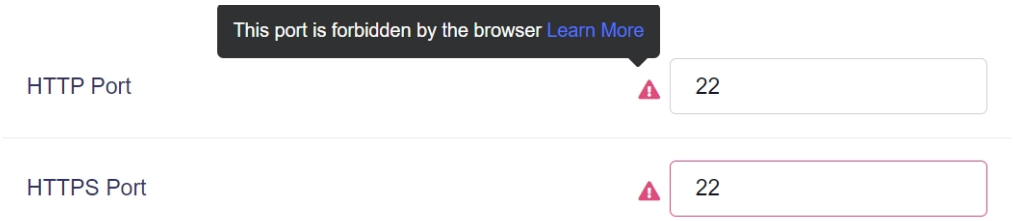
- **HTTP Port**: Standardmäßig 8080; wird für den unverschlüsselten HTTP-Zugriff auf die LuCI-Oberfläche verwendet.
- **HTTPS Port**: Standardmäßig 8443; wird für den sicheren HTTPS-Zugriff auf die LuCI-Oberfläche verwendet.
- **Force HTTPS**: Bei aktivierter Option ist der Zugriff auf die LuCI-Oberfläche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

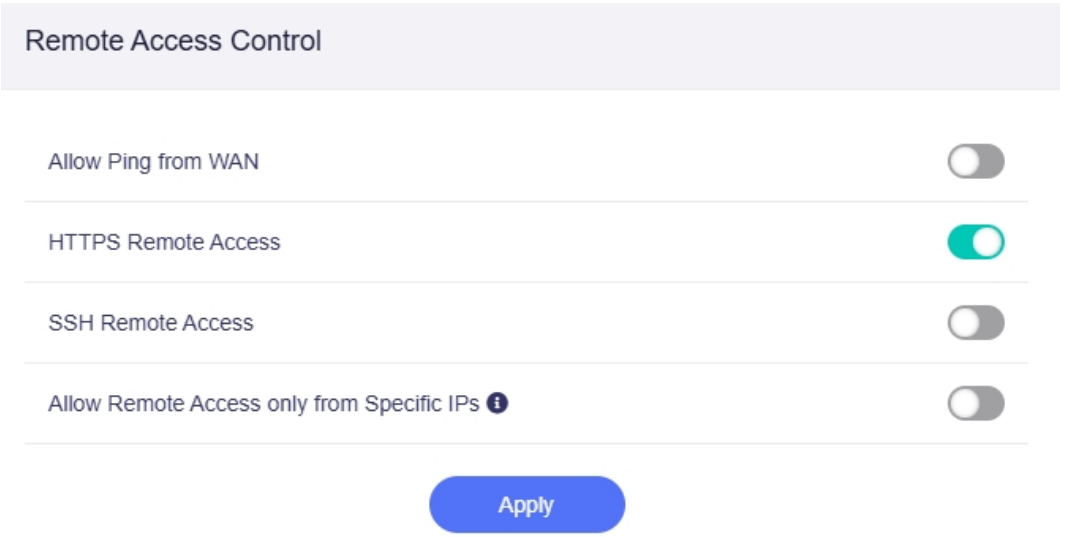
1. Wenn Sie einen reservierten Port oder einen von Browsern beziehungsweise Netzwerkkonventionen bestimmten Diensten vorbehaltenen Port auswählen, erscheint die Meldung „This port is forbidden by the browser“.



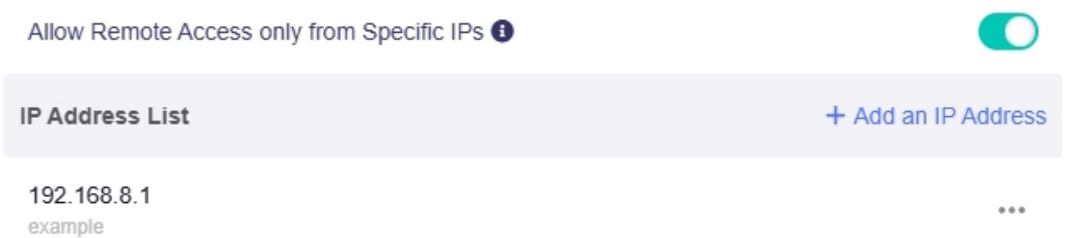
2. Nach einer Änderung der Portnummer in der Firmware müssen Sie die neue Portnummer beim Aufrufen der Weboberfläche angeben. Haben Sie sie vergessen, setzen Sie den Router zurück, um den Standardport wiederherzustellen.

14.2.2 Fernzugriffskontrolle

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

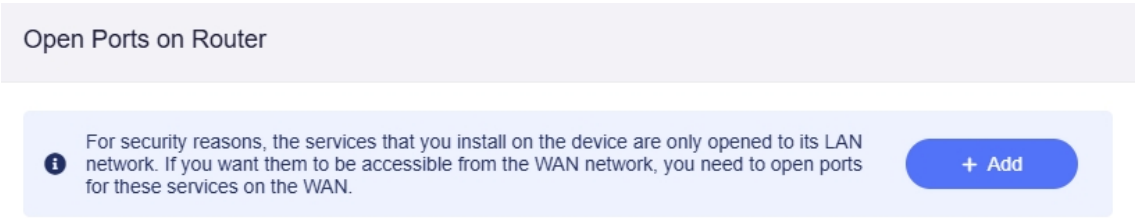


- **Allow Ping from WAN**: Erlaubt Ping-Anfragen von der WAN-Seite. Bei Netzwerkproblemen können Sie damit die Erreichbarkeit des Routers sowie Latenz und Paketverlust prüfen.
- **HTTPS Remote Access**: Ermöglicht den sicheren Fernzugriff auf die Weboberfläche über HTTPS. Die Datenübertragung bei der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

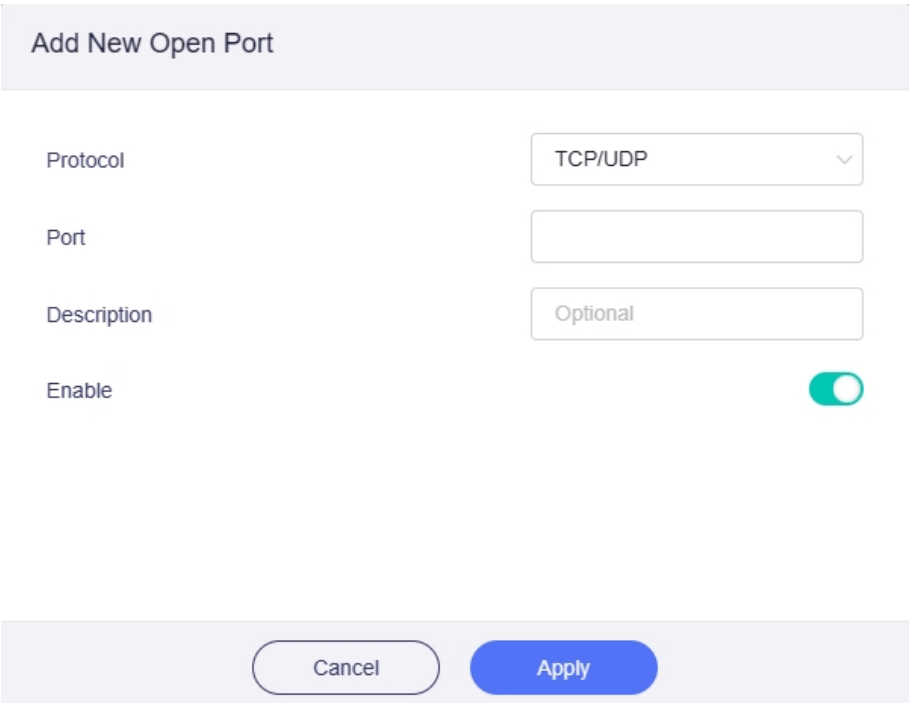


14.2.3 Ports am Router öffnen

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



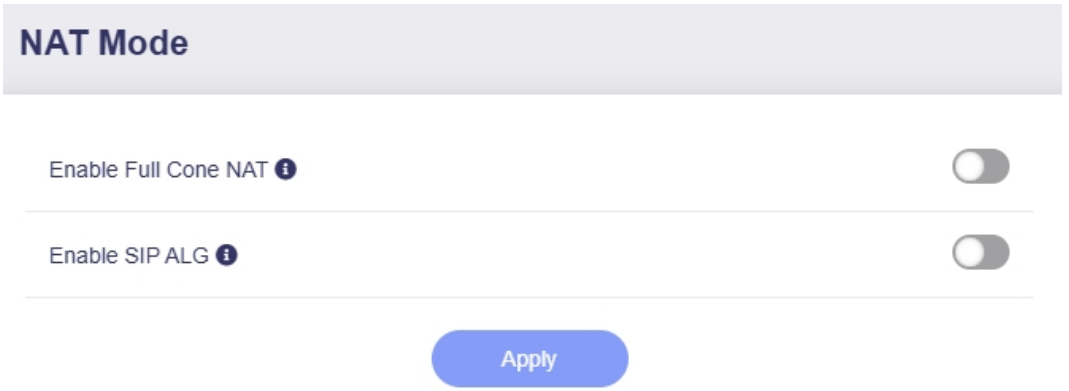
Klicken Sie auf **Add** und geben Sie im eingeblendeten Fenster die erforderlichen Angaben ein, um einen Port zu öffnen.



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

14.3 NAT-Modus

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SECURITY** > **NAT Mode**. Hier können Sie zwei zentrale NAT-Funktionen konfigurieren: 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

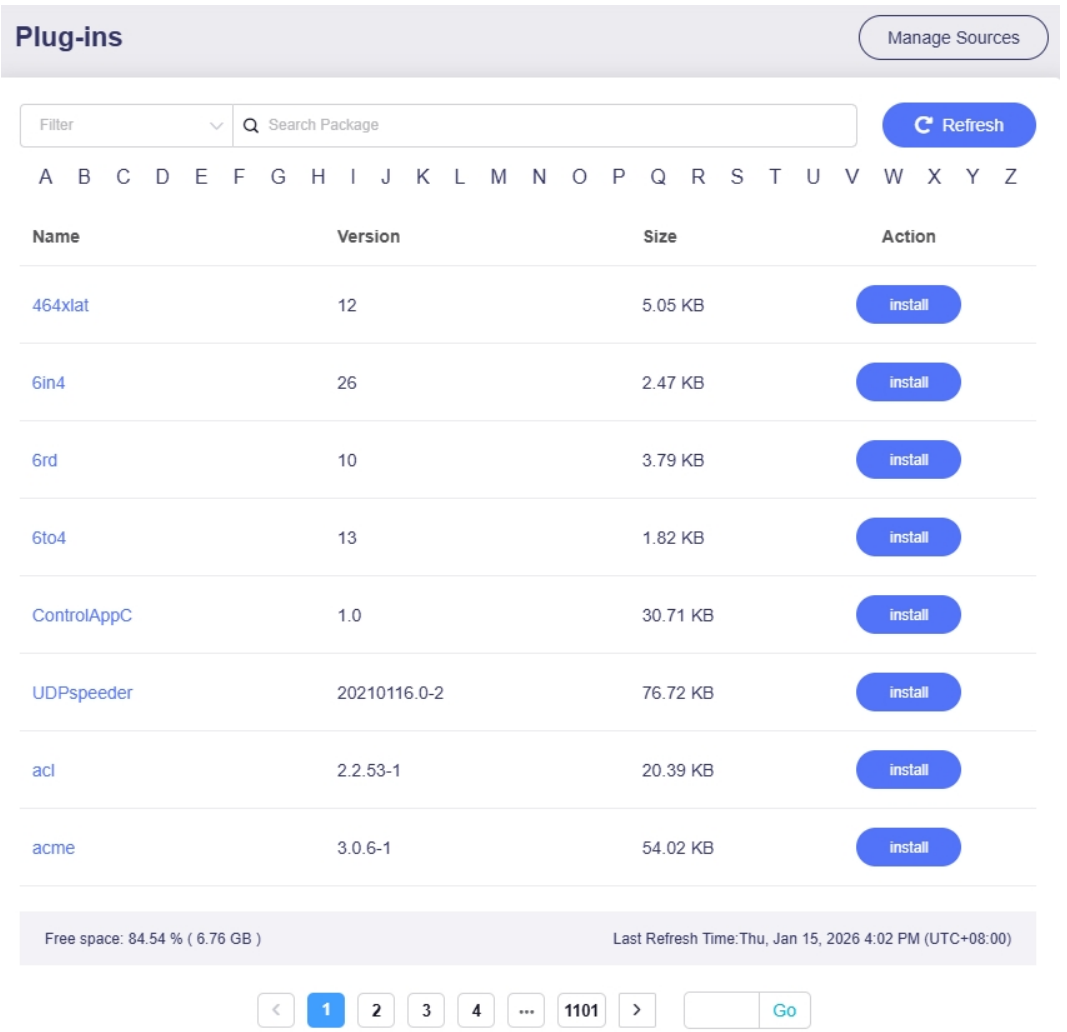
Anwendungen

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

15.1 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:

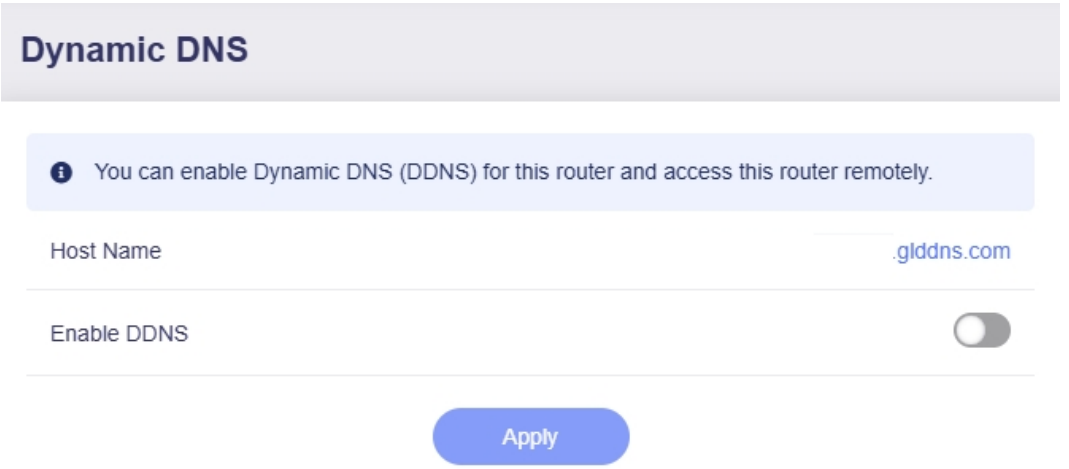
1. Es wird davon abgeraten, in der offiziellen GL.iNet-Firmware vorinstallierte Plug-ins wie nginx, AdGuard Home oder Tailscale zu aktualisieren.
2. Manuell installierte Plug-ins von Drittanbietern können aktualisiert werden. GL.iNet haftet jedoch nicht für Sicherheitsprobleme durch solche Plug-ins.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

15.2 Dynamisches DNS

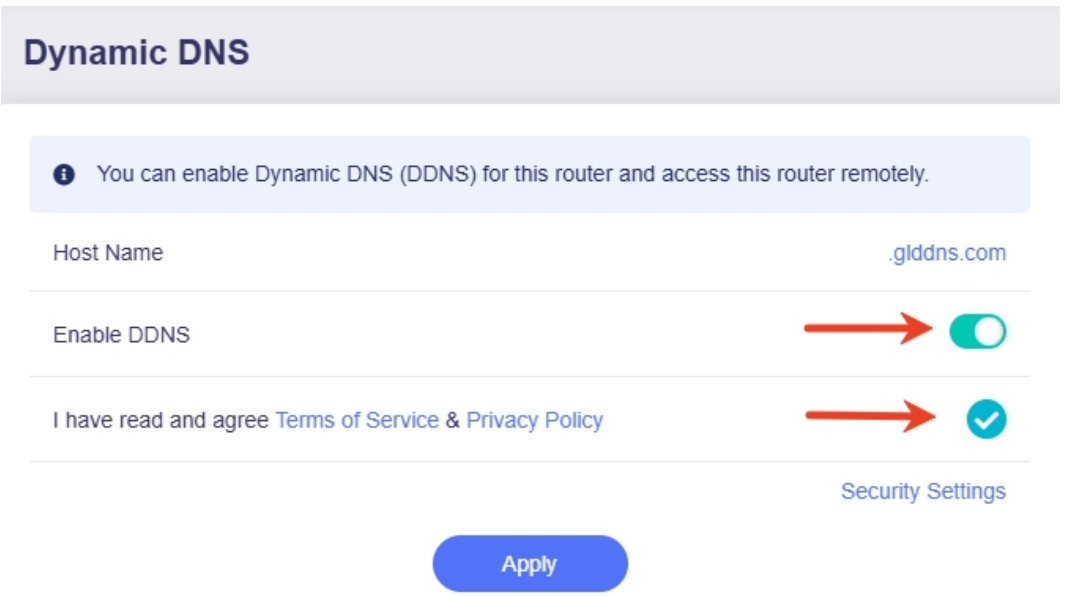
Dynamic DNS (DDNS) ordnet einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zu. Damit können Sie aus der Ferne auf Ihren Router zugreifen. Für diese Funktion ist eine öffentliche IP-Adresse erforderlich.

15.2.1 DDNS aktivieren

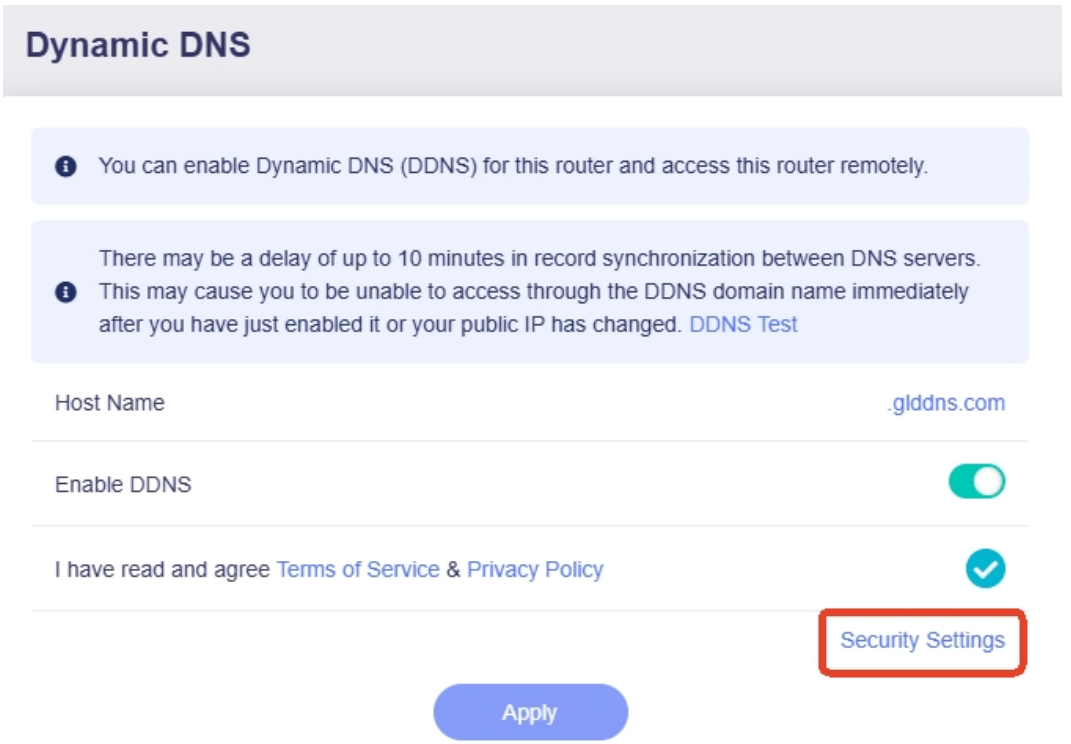
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Dynamic DNS**. Die folgende Seite wird angezeigt.



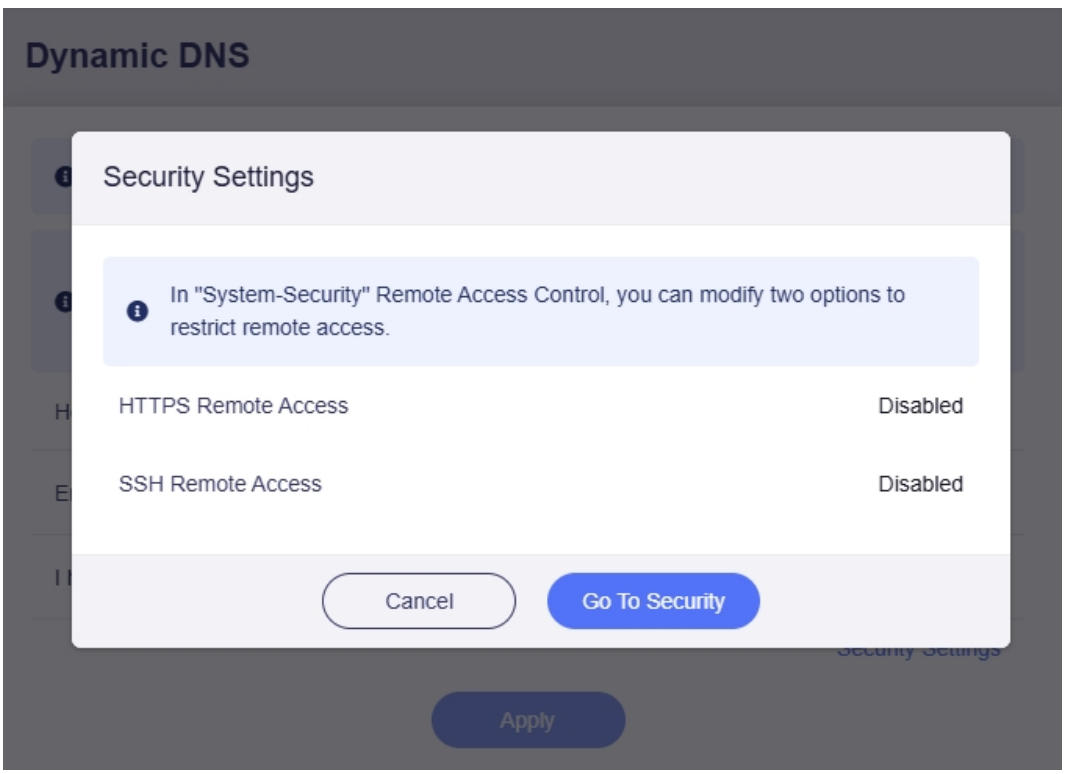
2. Aktivieren Sie **Enable DDNS**, lesen und akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



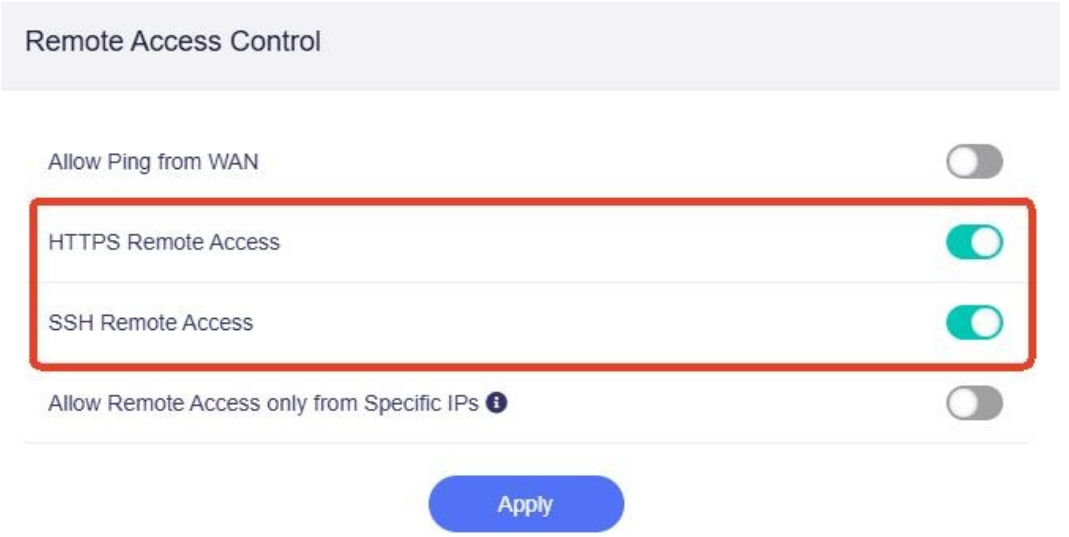
3. Klicken Sie unten rechts auf **Security Settings**.



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



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



Hinweis:

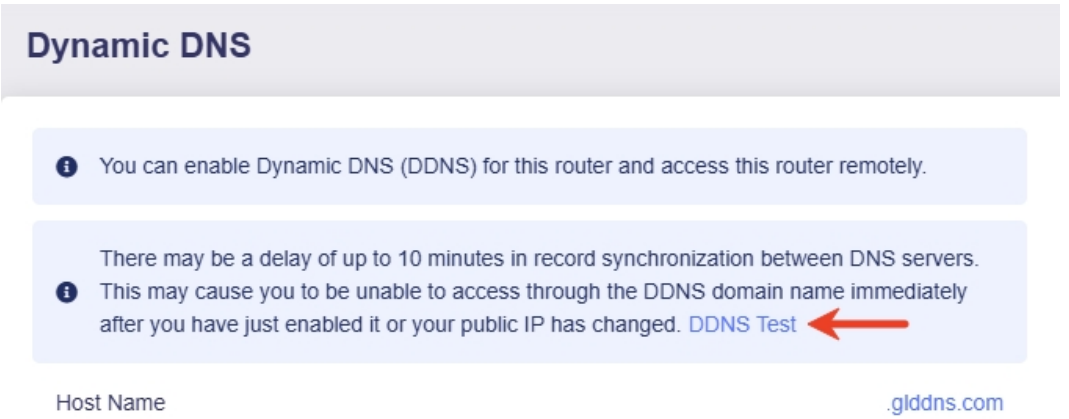
1. Die Synchronisierung der Einträge zwischen DNS-Servern kann bis zu zehn Minuten dauern. Deshalb kann der Zugriff über den DDNS-Domainnamen direkt nach der Aktivierung oder nach einer Änderung Ihrer öffentlichen IP-Adresse vorübergehend nicht möglich sein.
2. Wenn Sie DDNS und einen VPN-Client gleichzeitig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

15.2.2 DDNS-Funktion prüfen

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

Methode 1: DDNS-Testwerkzeug verwenden

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



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



Methode 2: Befehle verwenden

1. Verwenden Sie den Befehl *nslookup xxxxxxx.glddns.com 8.8.8.8*, um die Zuordnung zwischen Domainname und IP-Adresse abzufragen. Das folgende Beispiel zeigt Beryl AX GL-MT3000.



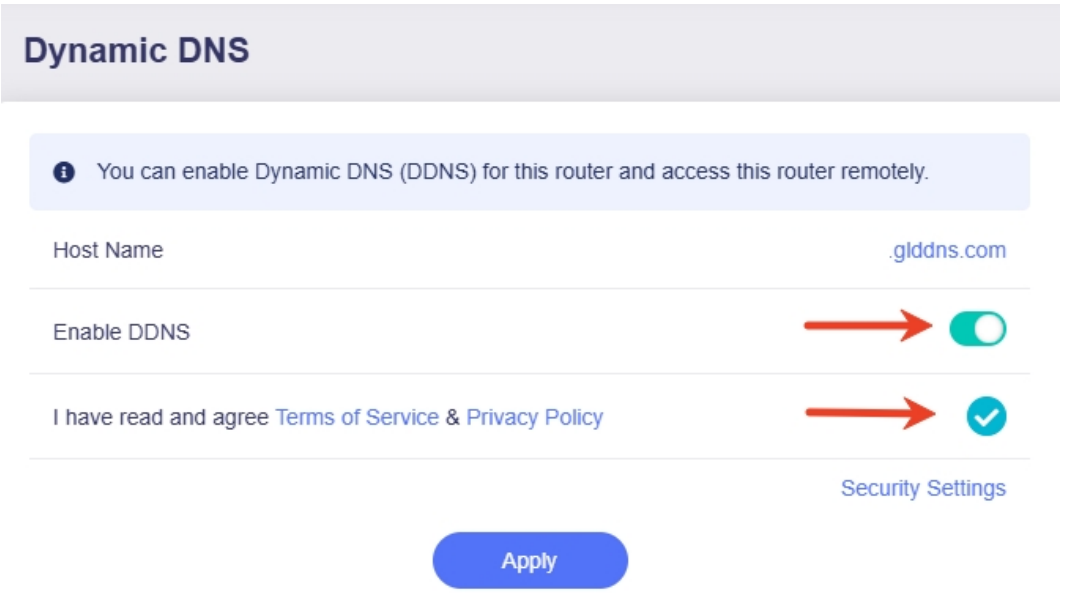
   - Ersetzen Sie „xxxxxxx.glddns.com“ in der obigen Abbildung durch Ihren Hostnamen.
   - „8.8.8.8“ ist ein DNS-Server von Google. Verwenden Sie diesen oder ersetzen Sie ihn durch einen anderen DNS-Server und drücken Sie die Eingabetaste.
2. Wenn eine öffentliche IP-Adresse wie „183.178.10.100“ in der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

15.2.3 HTTPS-Fernzugriff

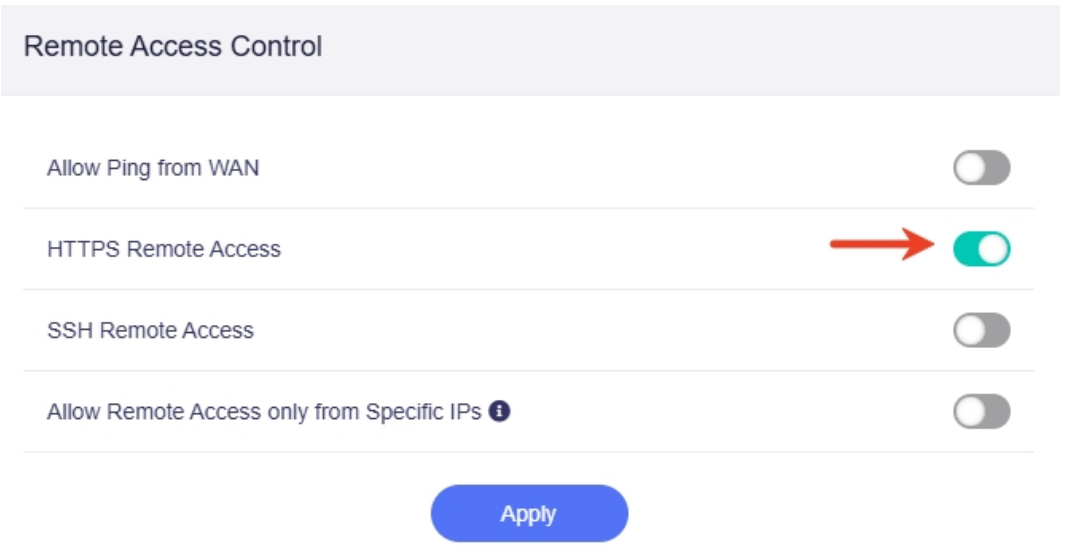
Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 443** ein.

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**.

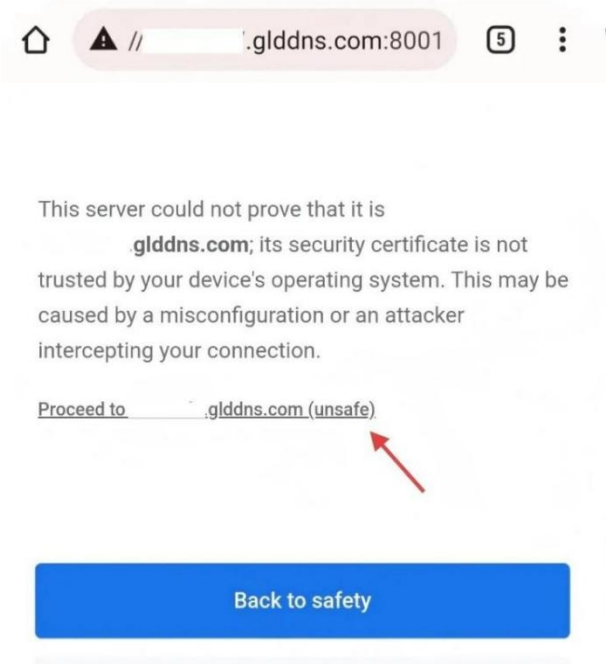


2. Öffnen Sie auf der Weboberfläche **SECURITY** > **Admin Access** > **Remote Access Control**. Aktivieren Sie **HTTPS Remote Access** und klicken Sie auf **Apply**.



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.



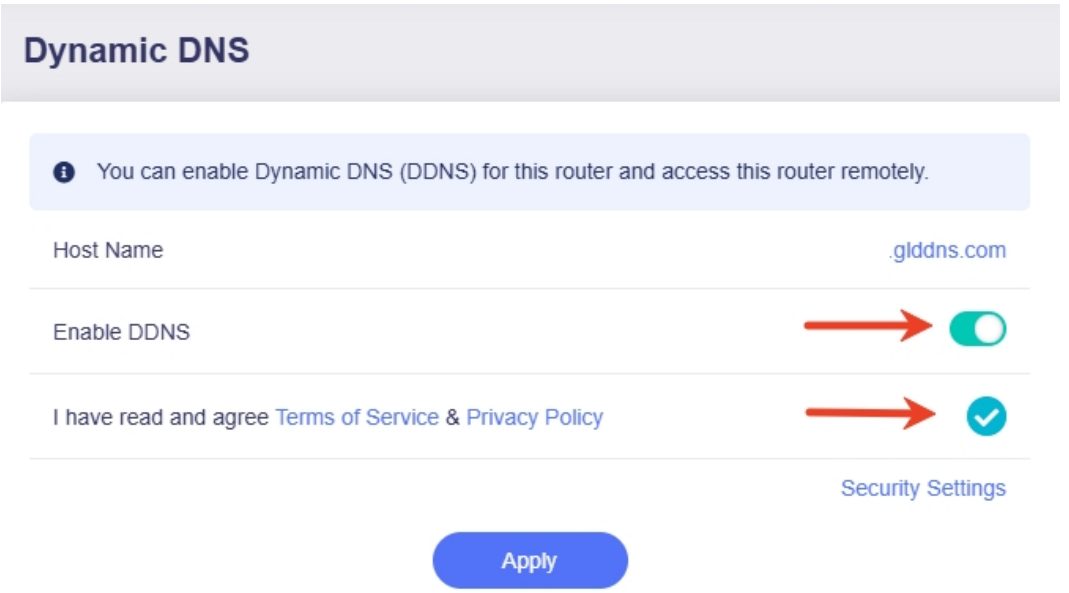
Sie können nun über den DDNS-Hostnamen per **HTTPS** auf die Weboberfläche des Routers zugreifen.

15.2.4 SSH-Fernzugriff

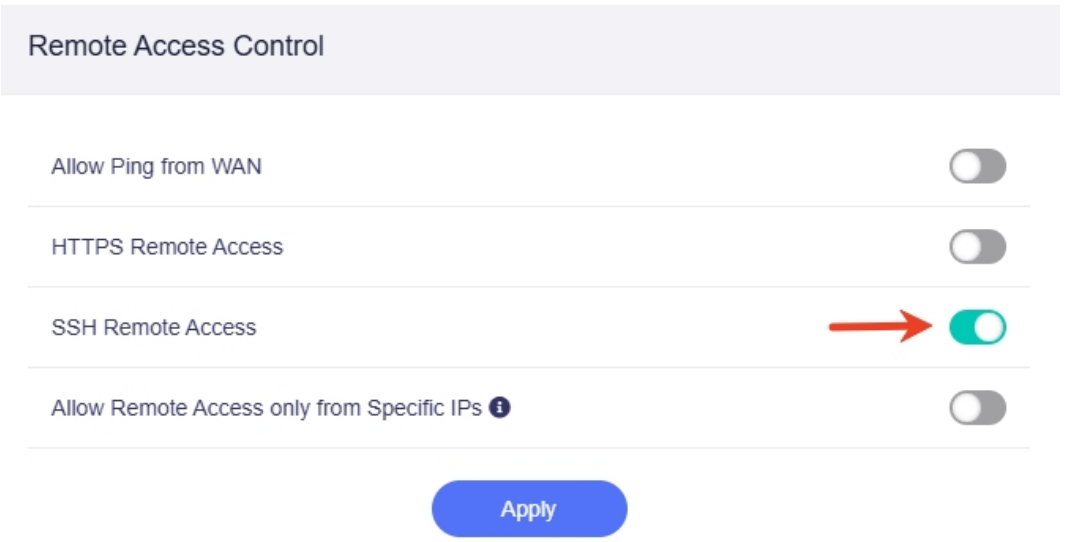
Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 22** ein.

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 auf der Weboberfläche **SECURITY** > **Admin Access** > **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.

15.3 Netzwerkspeicher

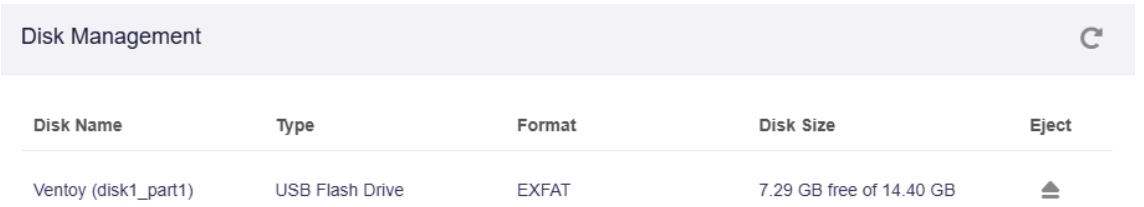
Die Netzwerkspeicherfunktion ermöglicht die drahtlose Dateifreigabe zwischen Geräten, wenn Sie ein USB-Laufwerk oder eine SD-Karte an Ihren Router anschließen. Der Router stellt den Speicher als gemeinsames Netzlaufwerk bereit, auf das alle per WLAN verbundenen Geräte zugreifen können.

Mudi 7 verfügt über einen USB-Anschluss für USB-Sticks und tragbare externe Festplatten. Für diese Speichergeräte können Sie Samba, WebDAV oder DLNA einrichten. Unterstützt werden gängige Dateisysteme wie NTFS, FAT32 und EXT4.

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

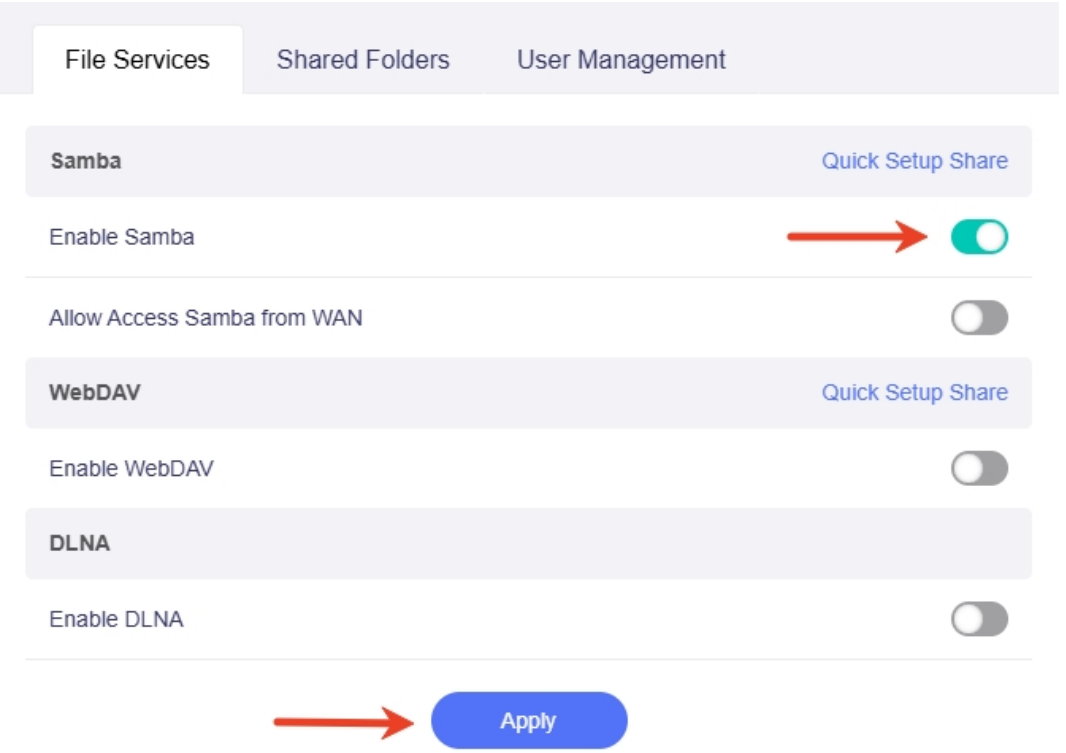
15.3.1 Speicher anschließen

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.



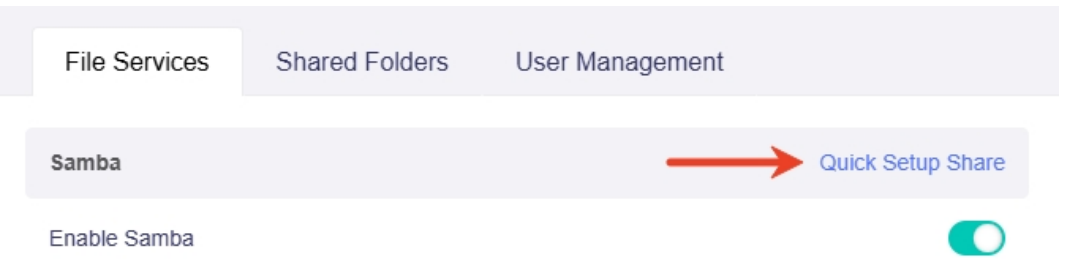
15.3.2 Samba einrichten

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

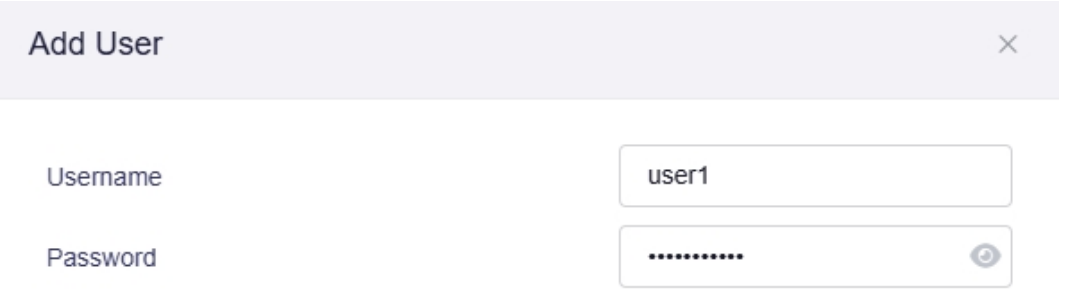


   - **Allow Access Samba from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den Samba-Dienst zugreifen sollen.

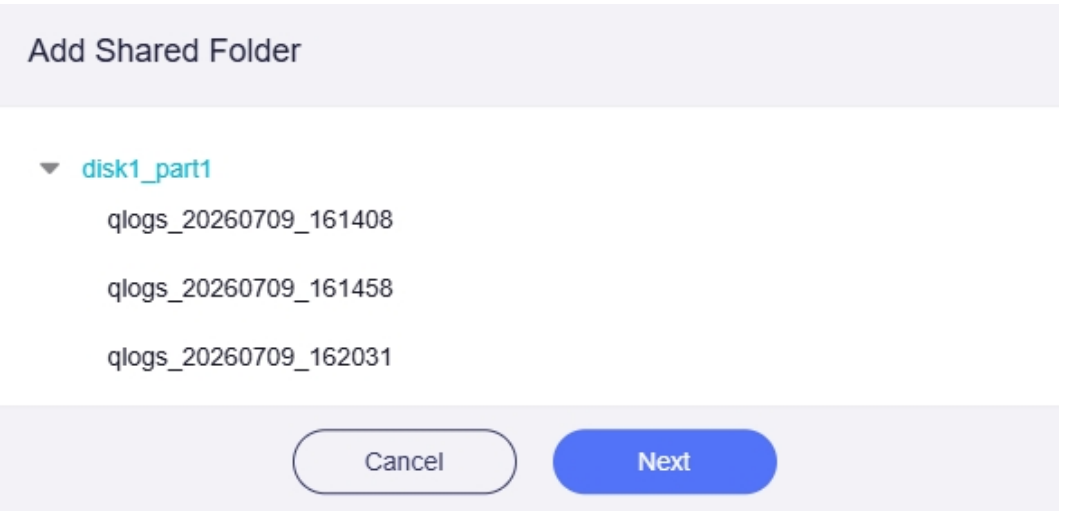
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



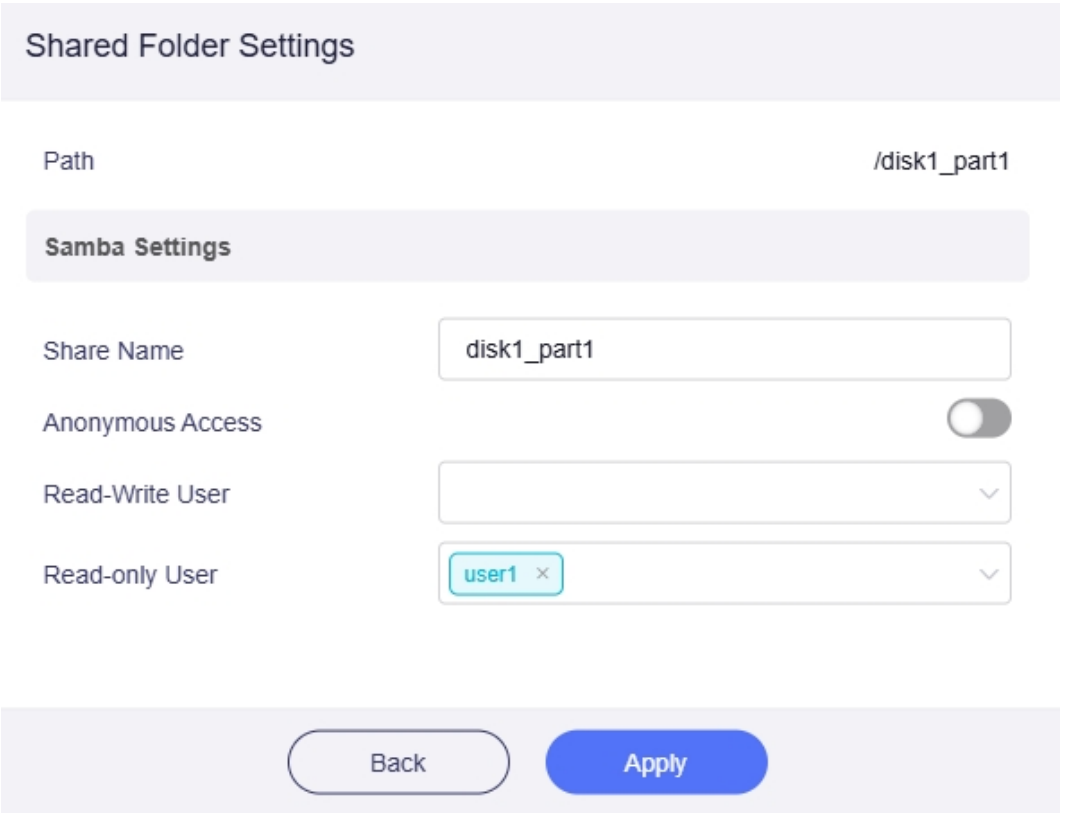
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



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.

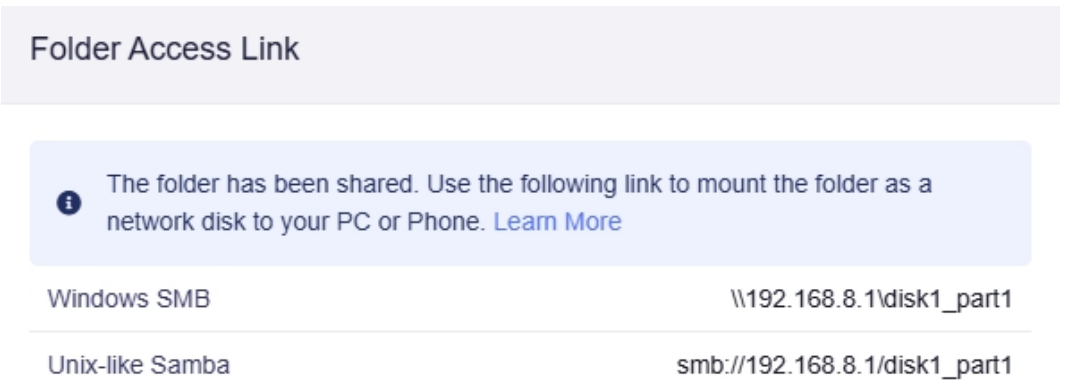


5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll er Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn dort und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend auf **Apply**.



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.

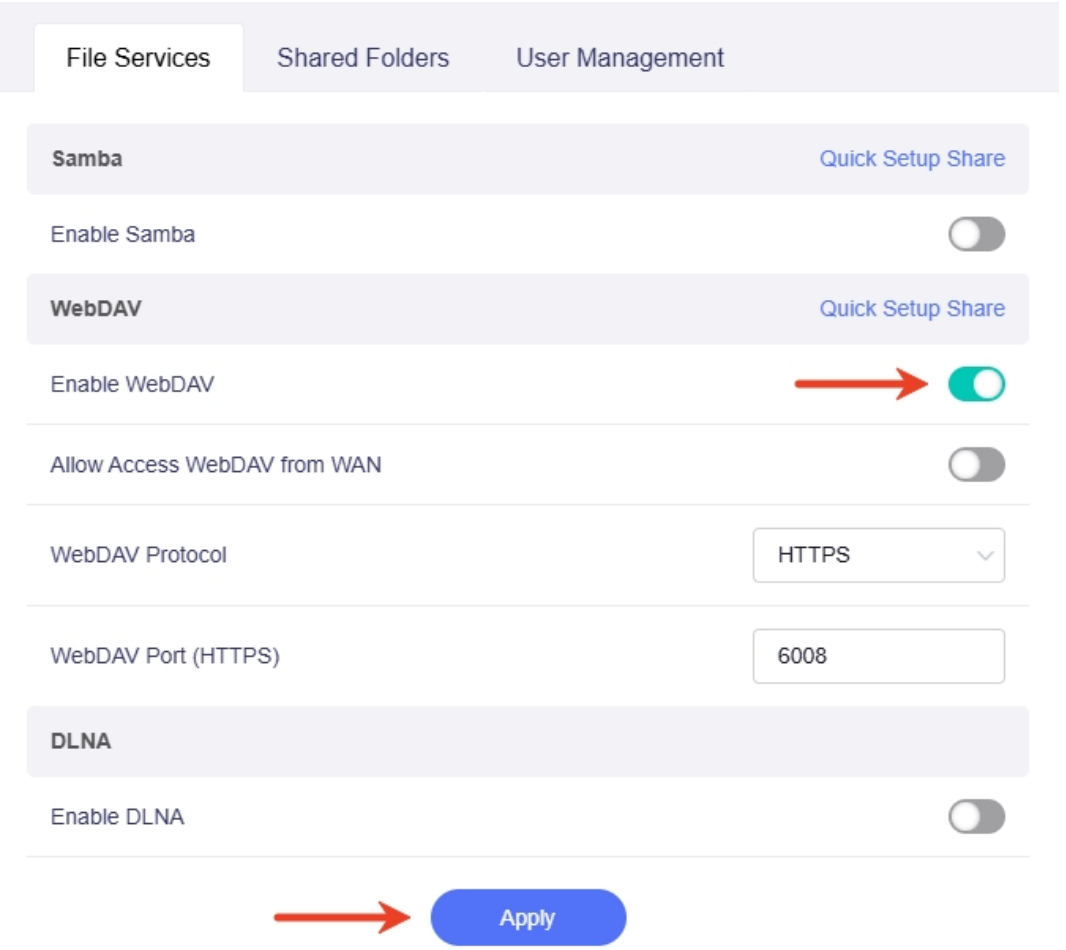


Hinweis: Wenn Sie **Allow Access Samba from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der

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

15.3.3 WebDAV einrichten

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

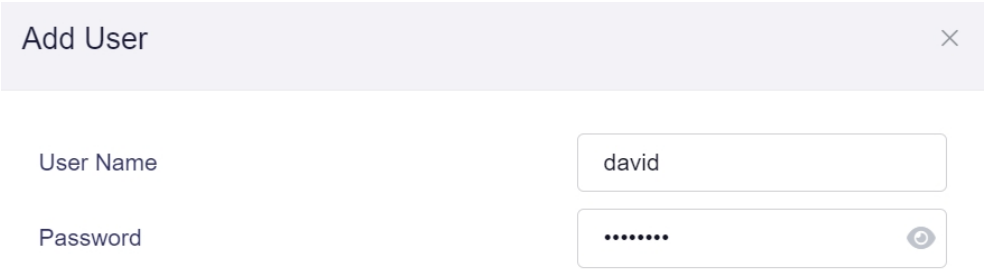


- **Allow Access WebDAV from WAN**: Aktivieren Sie diese Option, wenn Geräte im vorgeschalteten Netzwerk auf den WebDAV-Dienst zugreifen sollen.
- **WebDAV Protocol**: HTTP ist unverschlüsselt und wird auf eigenes Risiko verwendet. HTTPS ist verschlüsselt und verwendet ein selbstsigniertes Zertifikat.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

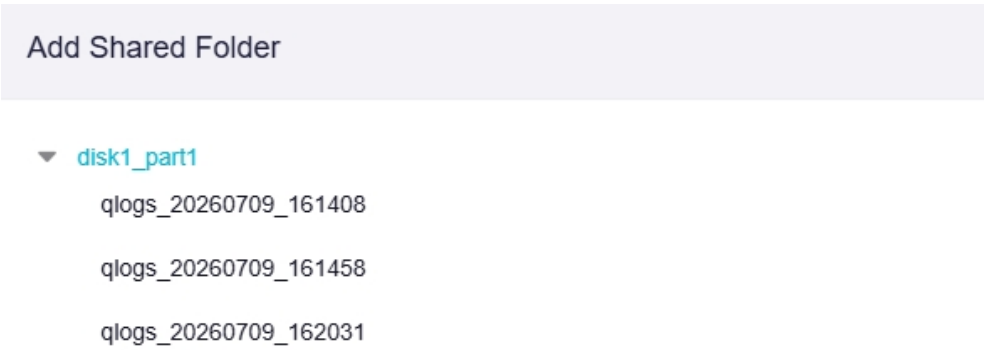
2. Klicken Sie auf **Quick Setup Share**, um die Freigabeadresse einzurichten.



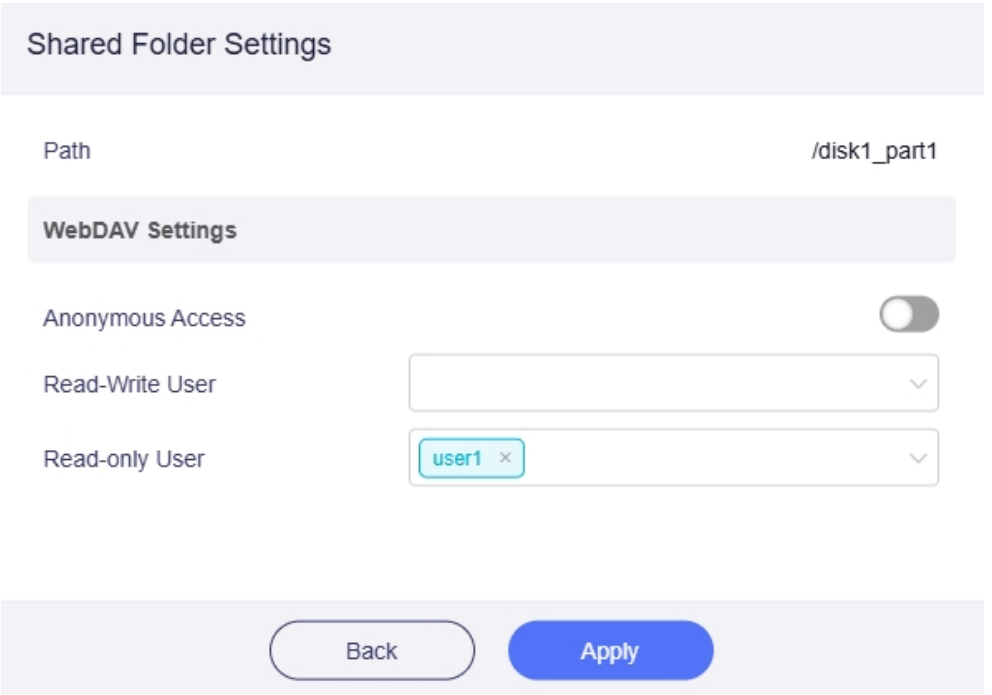
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf **Next**. Falls bereits ein Konto vorhanden ist, wird dieser Schritt übersprungen.



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.



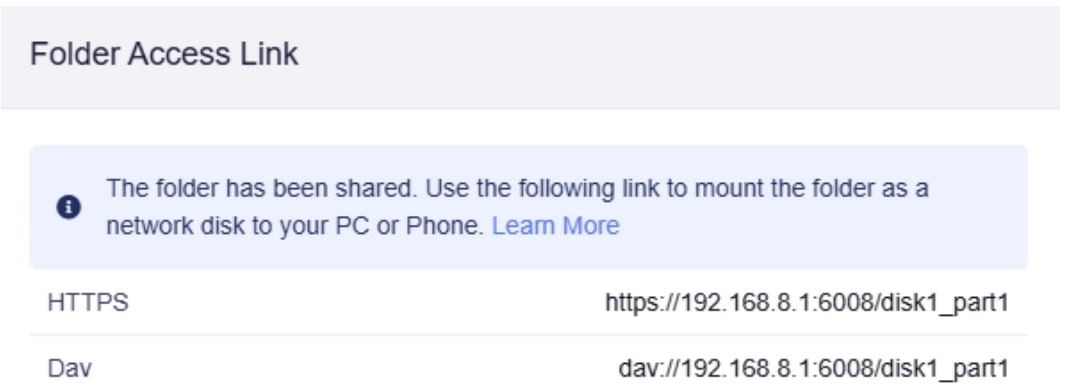
5. Freigegebenen Ordner einrichten.
   Der zuvor angelegte Benutzer wird standardmäßig unter **Read-Only User** eingetragen. Soll dieser Benutzer Dateien auch schreiben oder löschen dürfen, entfernen Sie ihn unter Read-Only User und fügen Sie ihn unter **Read-Write User** hinzu. Klicken Sie anschließend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



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

6. Zugriffsadresse des Ordners abrufen.

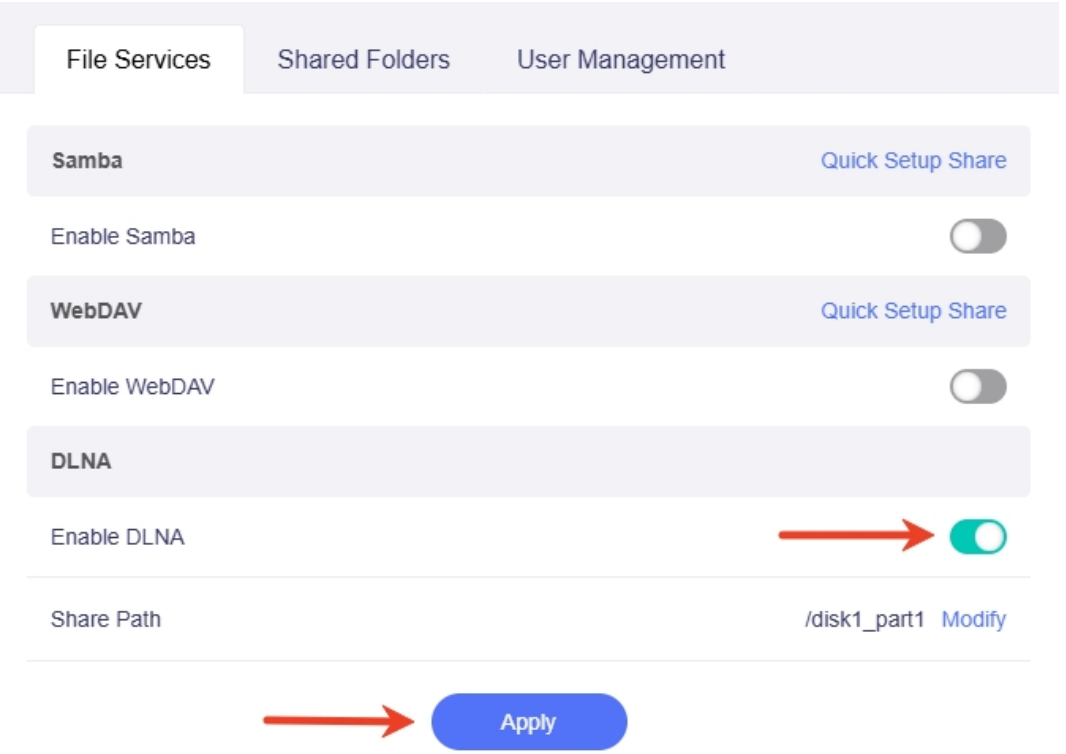
   Die Seite zeigt die Zugriffsadressen für Windows und Unix-ähnliche Betriebssysteme an. Zu Letzteren gehören Android, iOS, macOS und Ubuntu. Über diese Adressen können Sie nun per WebDAV auf den freigegebenen Ordner zugreifen.



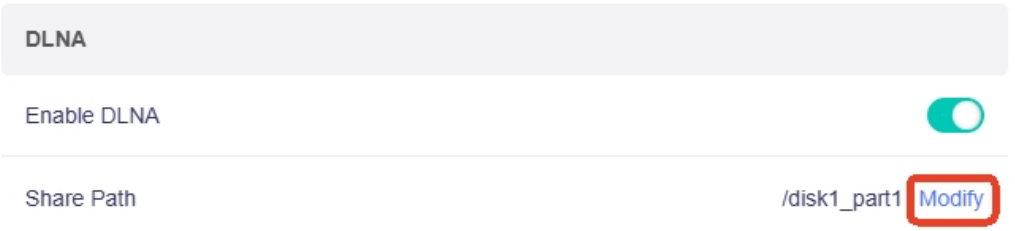
Hinweis: Wenn Sie **Allow Access WebDAV from WAN** aktivieren und aus dem vorgeschalteten Netzwerk zugreifen, ersetzen Sie die Router-IP-Adresse in der Zugriffsadresse (standardmäßig 192.168.8.1) durch die WAN-IP-Adresse des Routers. Diese finden Sie auf der Seite INTERNET der Weboberfläche.

15.3.4 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.



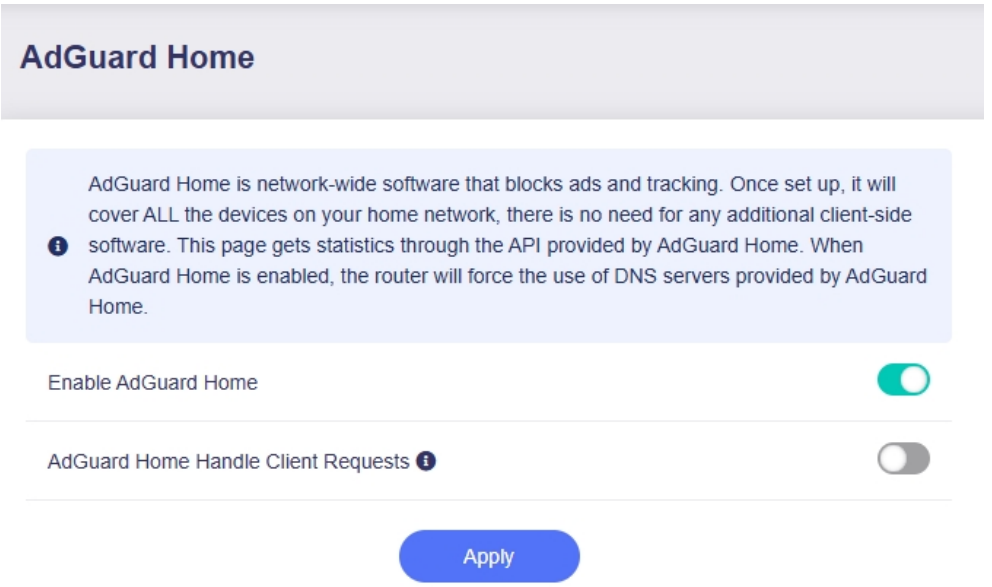
3. Verbinden Sie Ihren Smart-TV mit dem Router. Er erkennt den DLNA-Server automatisch.

15.4 AdGuard Home

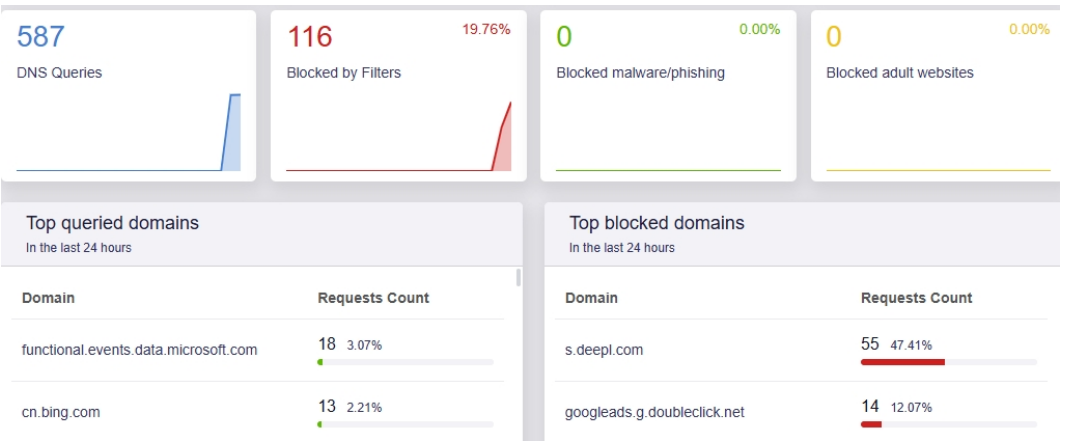
AdGuard Home blockiert Werbung und Tracking im gesamten Netzwerk. Nach der Einrichtung schützt die Software alle Endgeräte, ohne dass auf diesen zusätzliche Software installiert werden muss.

Gehen Sie wie folgt vor, um AdGuard Home einzurichten.

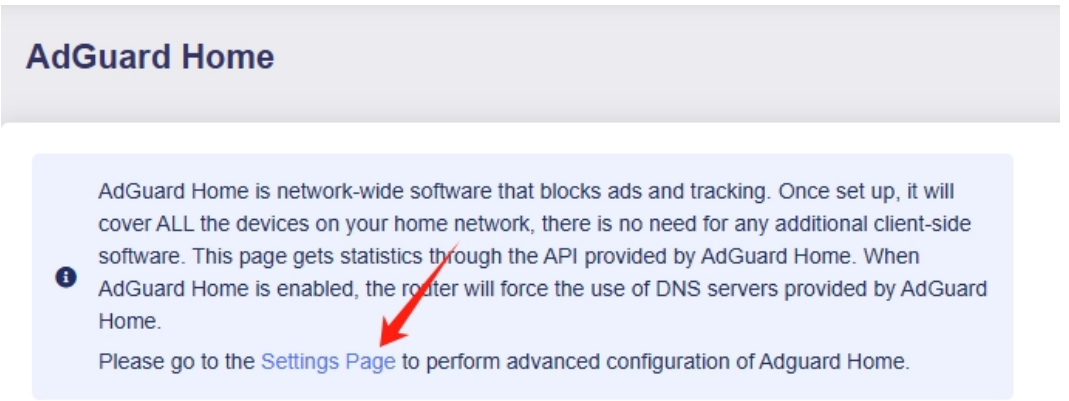
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **AdGuard Home**. Aktivieren Sie **Enable AdGuard Home** und klicken Sie auf **Apply**.



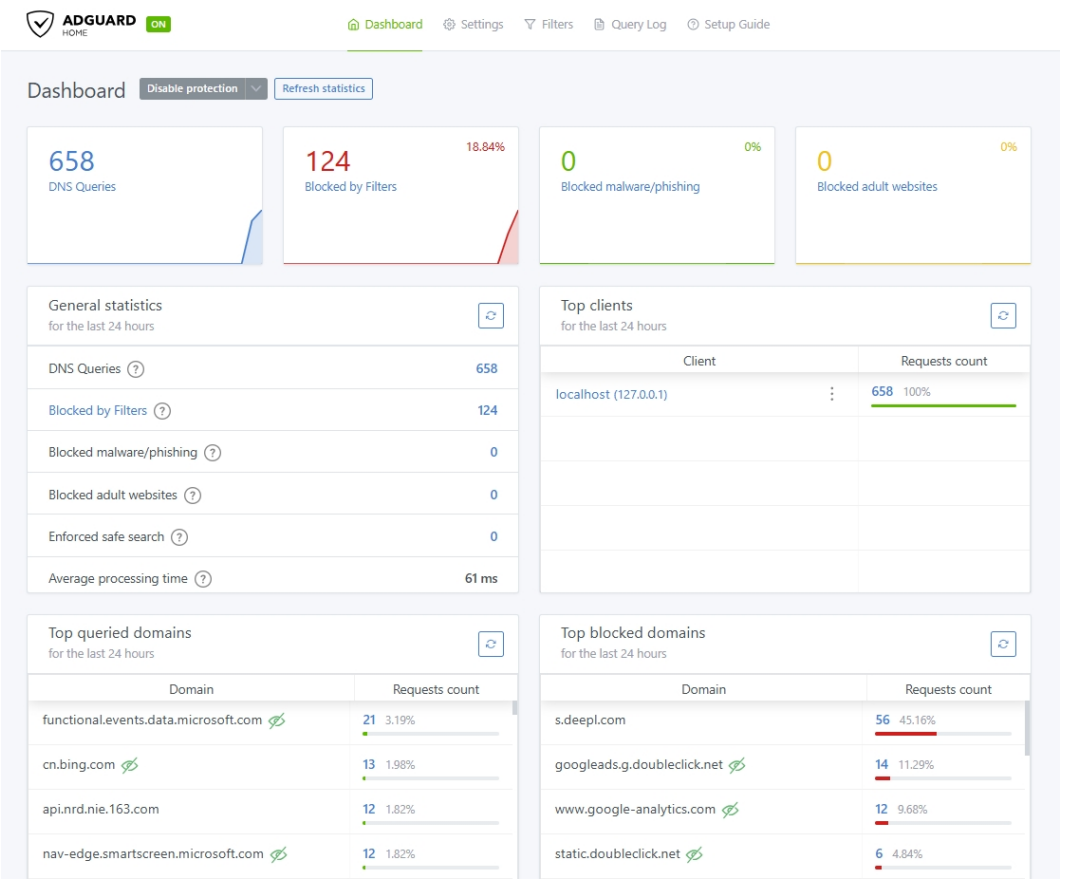
   - **AdGuard Home Handles Client Requests**: Leitet DNS-Anfragen der Endgeräte direkt an AdGuard Home weiter. Dadurch funktionieren jedoch domainbasierte VPN-Richtlinien nicht mehr.
2. Die Seite lädt automatisch DNS-Statistiken wie Anfragen und blockierte Domains über die API von AdGuard Home.



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%

15.5 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.

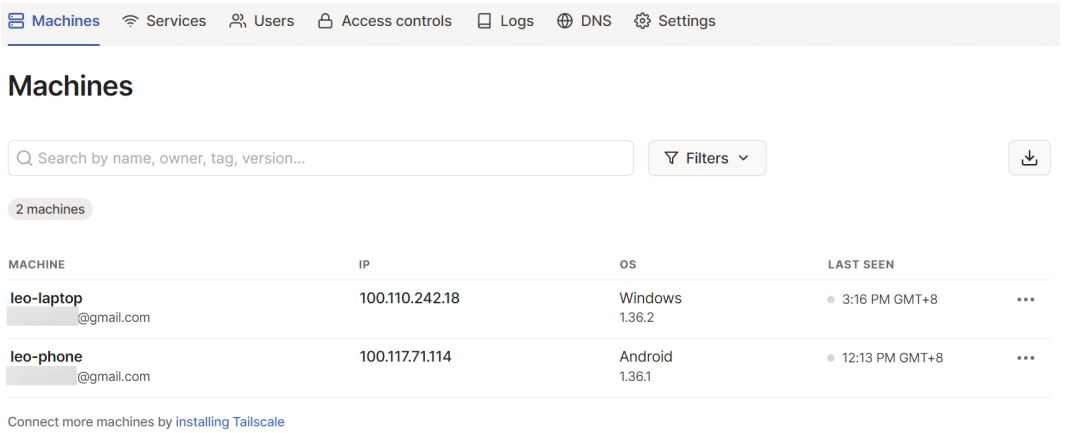
Hinweis:

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.

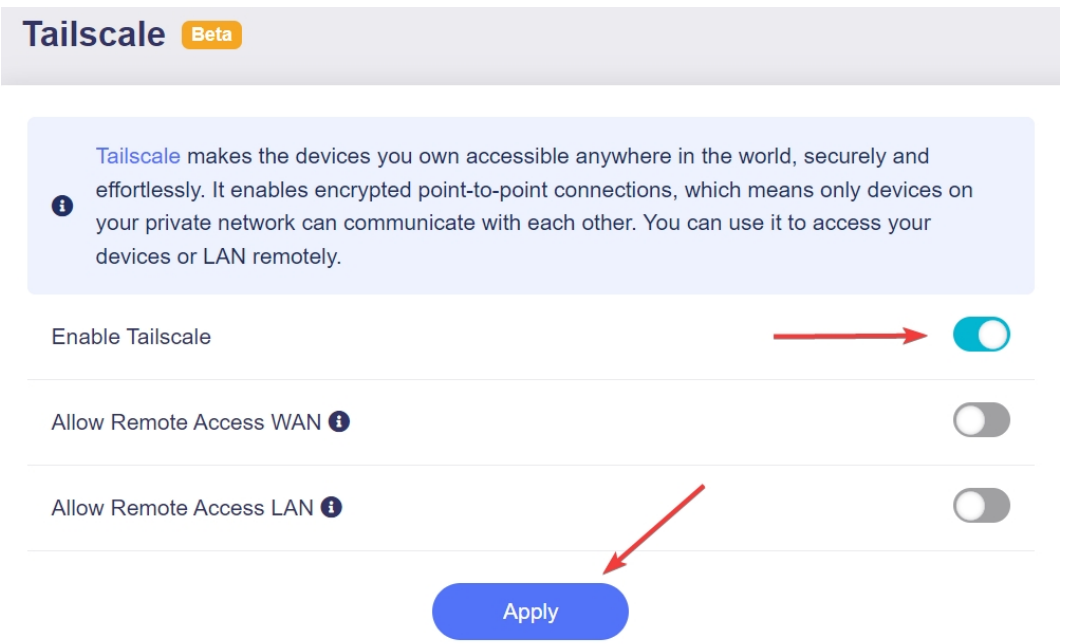
15.5.1 Tailscale einrichten

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

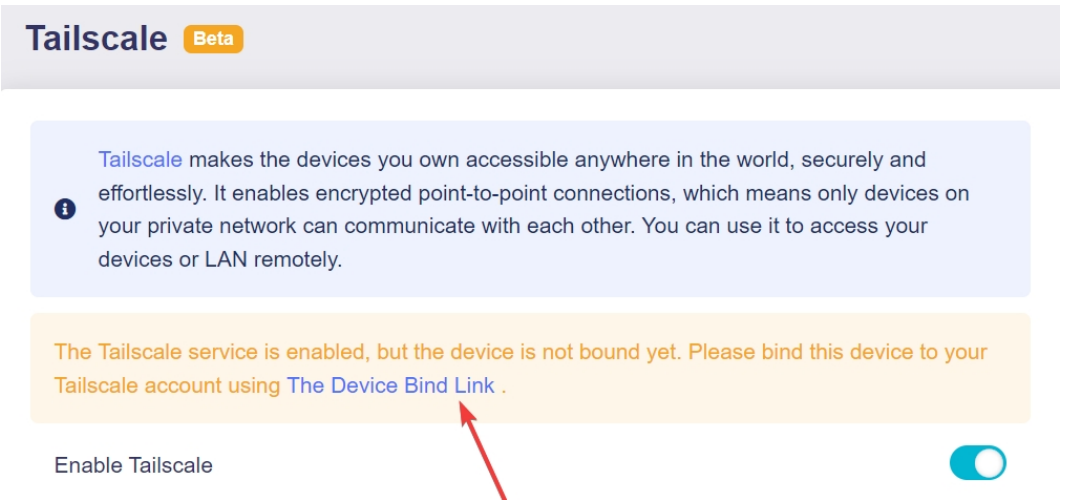
1. Registrieren Sie zunächst ein Tailscale-Konto und verknüpfen Sie zu Testzwecken ein oder zwei Geräte damit. Anschließend werden diese in der Tailscale-Konsole angezeigt.



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



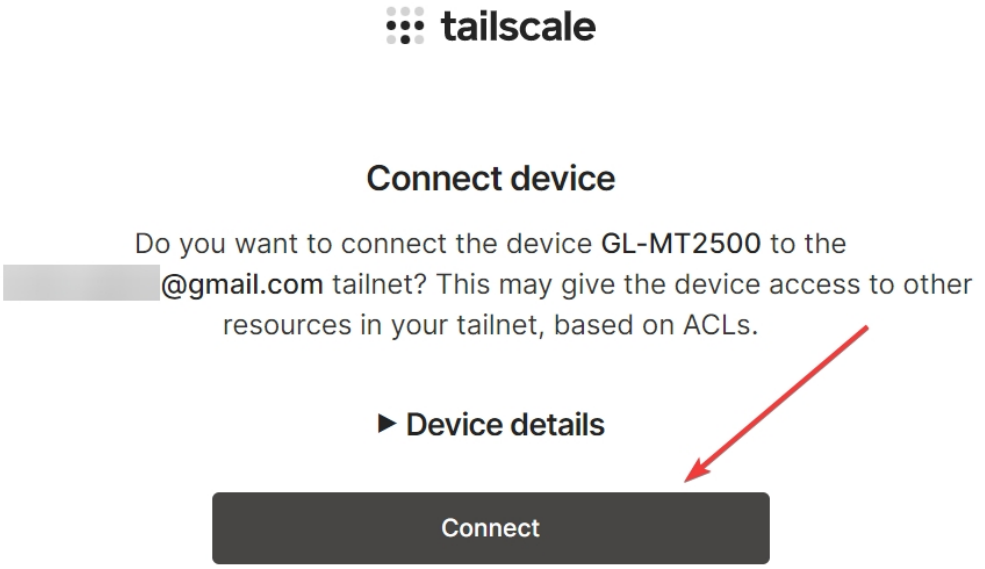
3. Sie werden aufgefordert, das Gerät zu verknüpfen. Klicken Sie auf **Device Bind Link**.



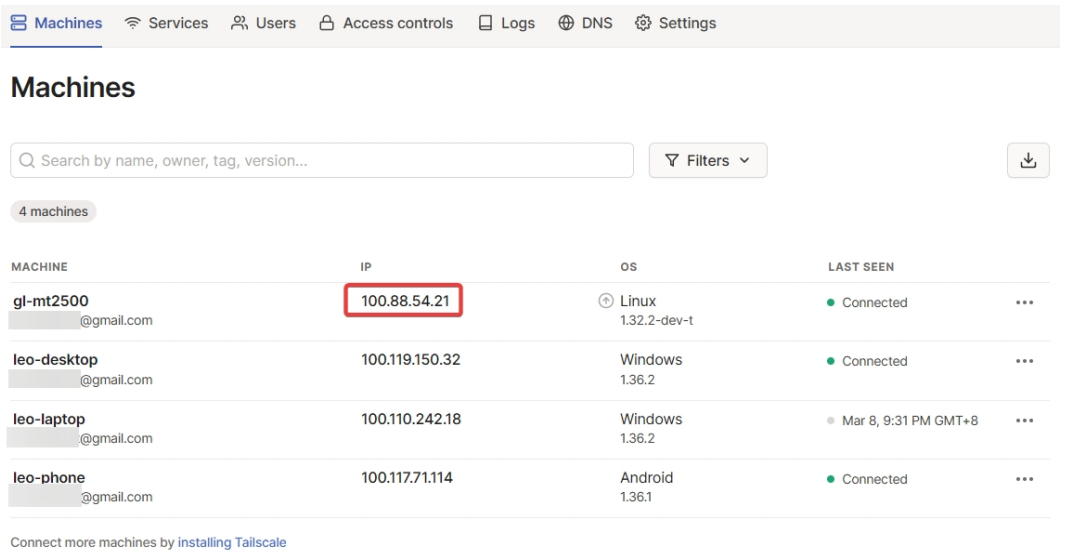
4. Klicken Sie im eingeblendeten Fenster auf den Link und melden Sie sich mit Ihrem Tailscale-Konto an.



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



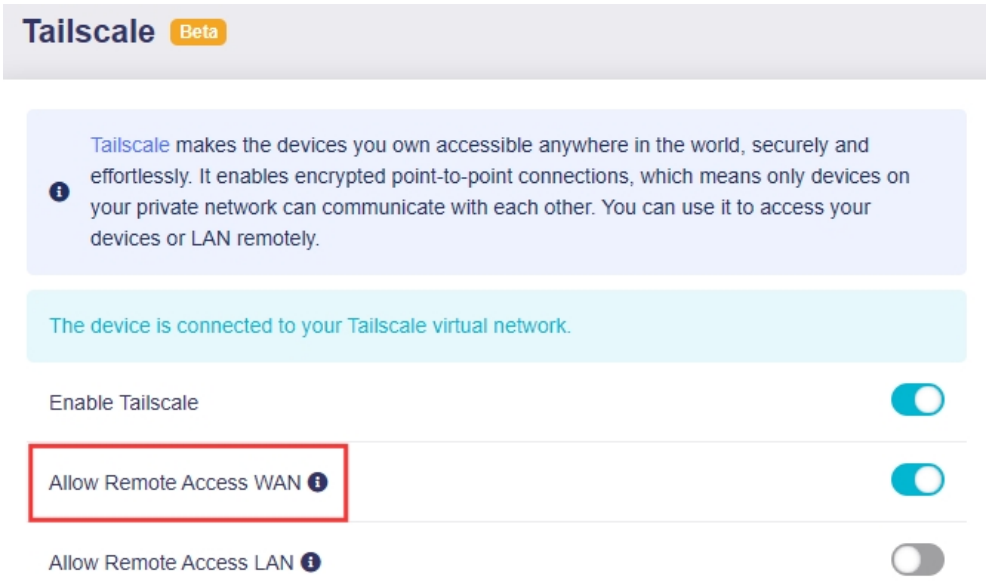
6. Sie werden anschließend zur Tailscale-Verwaltungskonsole weitergeleitet. Der Router wurde dem virtuellen Tailscale-Netzwerk hinzugefügt und ist über die virtuelle Tailscale-IP-Adresse 100.88.54.21 aus der Ferne erreichbar.



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

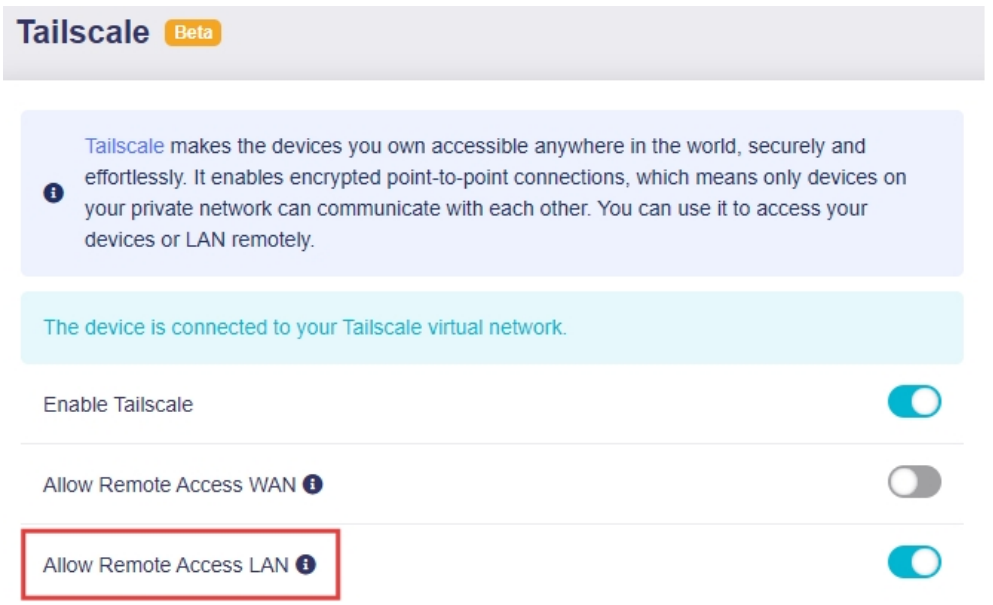
15.5.2 Fernzugriff auf WAN erlauben

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



15.5.3 Fernzugriff auf LAN erlauben

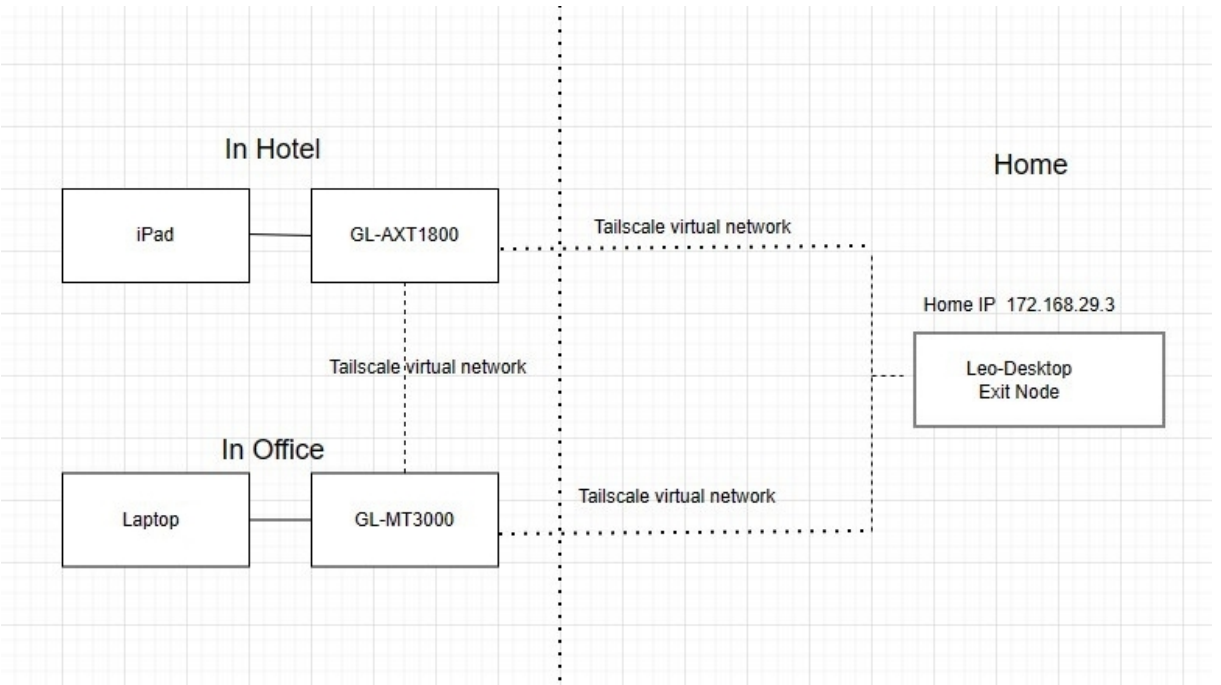
Diese Option erlaubt den Zugriff auf Ressourcen auf der LAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk. Weitere Informationen finden Sie hier.



15.5.4 Eigene Exit-Nodes

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

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



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

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

15.6 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:

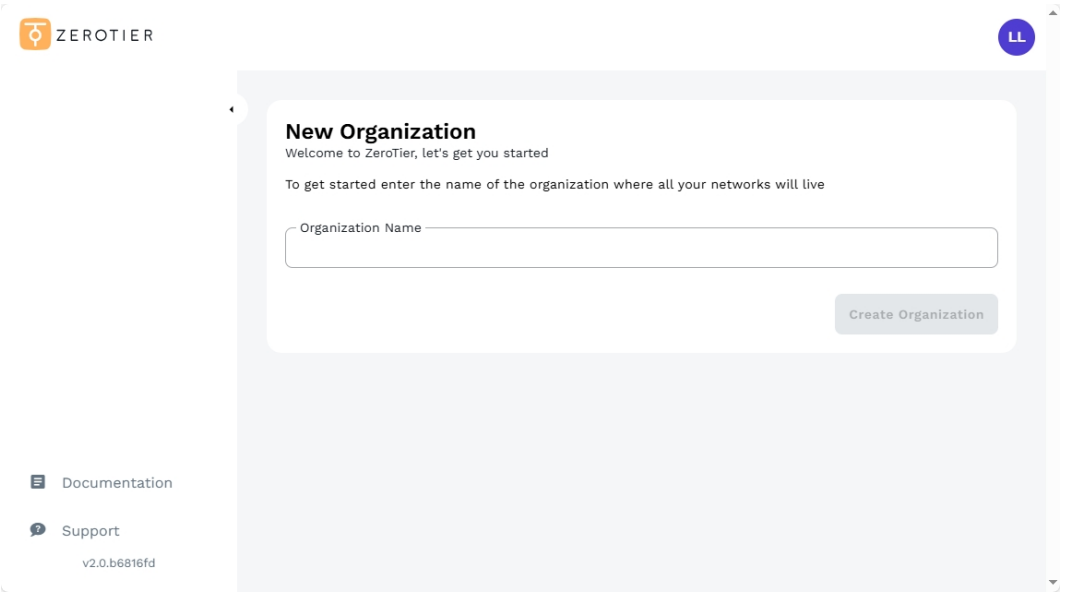
1. Die gleichzeitige Verwendung von ZeroTier mit folgenden Funktionen oder Diensten wird wegen möglicher Routingkonflikte nicht empfohlen: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale und AstroWarp.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

15.6.1 ZeroTier einrichten

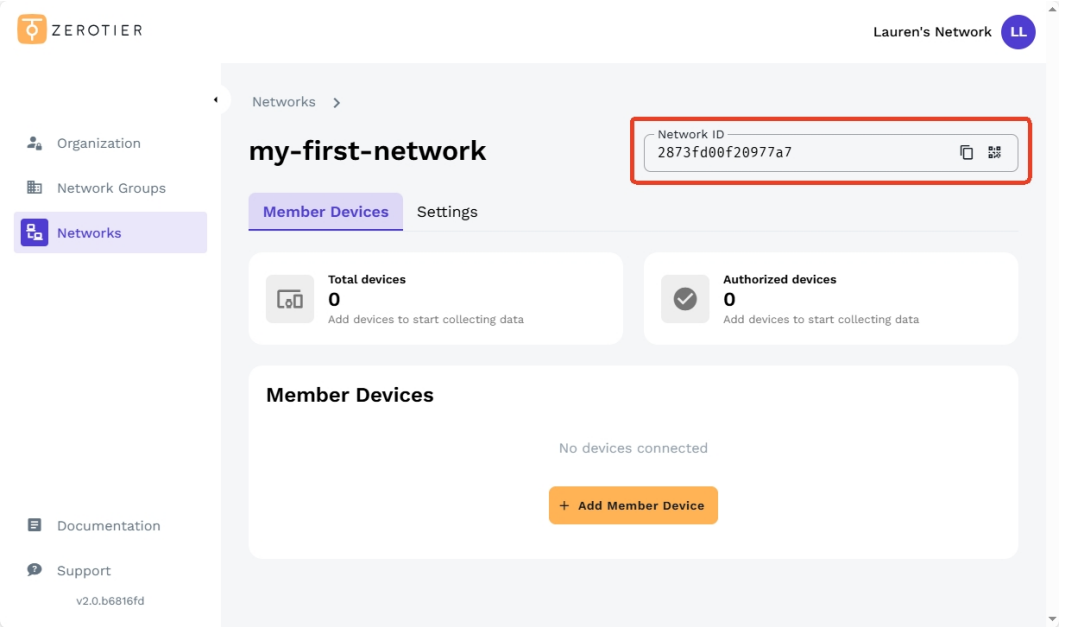
ZeroTier Central ist in zwei Versionen verfügbar: New Central und Legacy Central.

Die folgenden Schritte verwenden New Central als Beispiel.

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

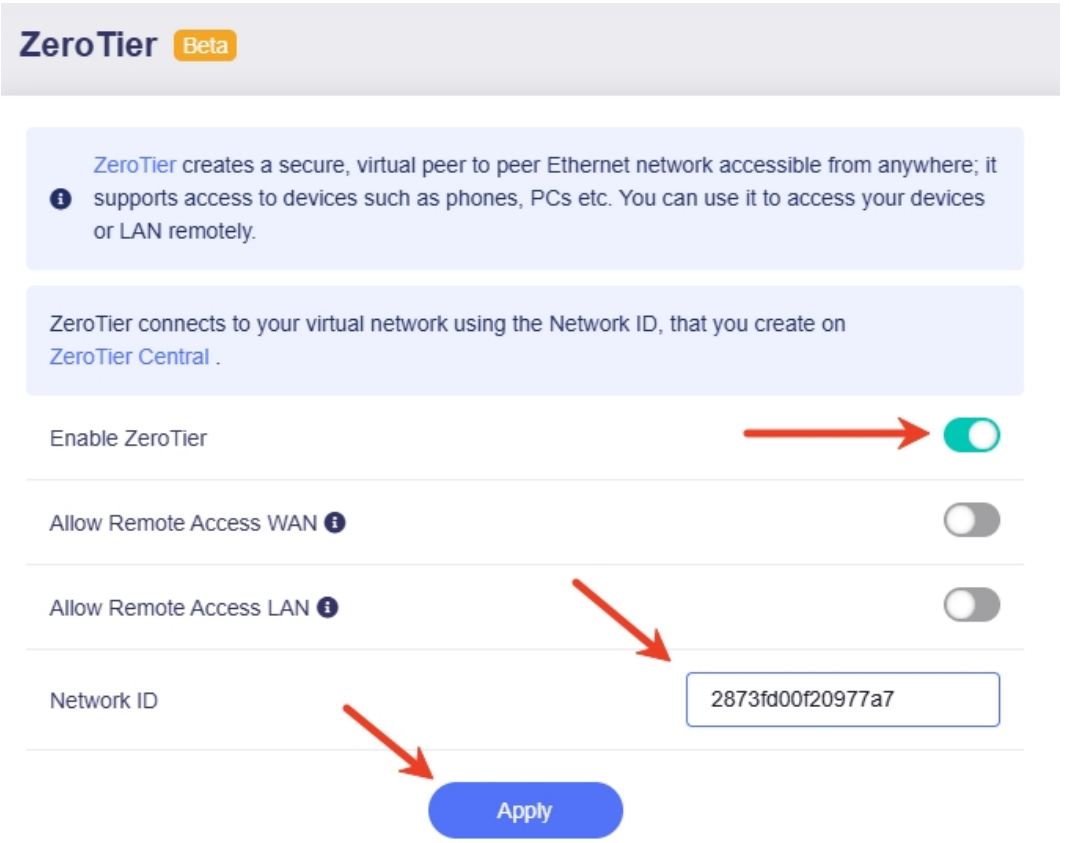


3. Wählen Sie einen Tarif aus. In diesem Beispiel verwenden wir den **Personal-Tarif** mit zehn Geräten, einem Netzwerkadministrator und einem Netzwerk. Wenn Sie mehr Netzwerke, zusätzliche Geräte, eigene Routen oder DNS-Einstellungen benötigen, wählen Sie einen kostenpflichtigen Tarif.
4. Ihr ZeroTier-Netzwerk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

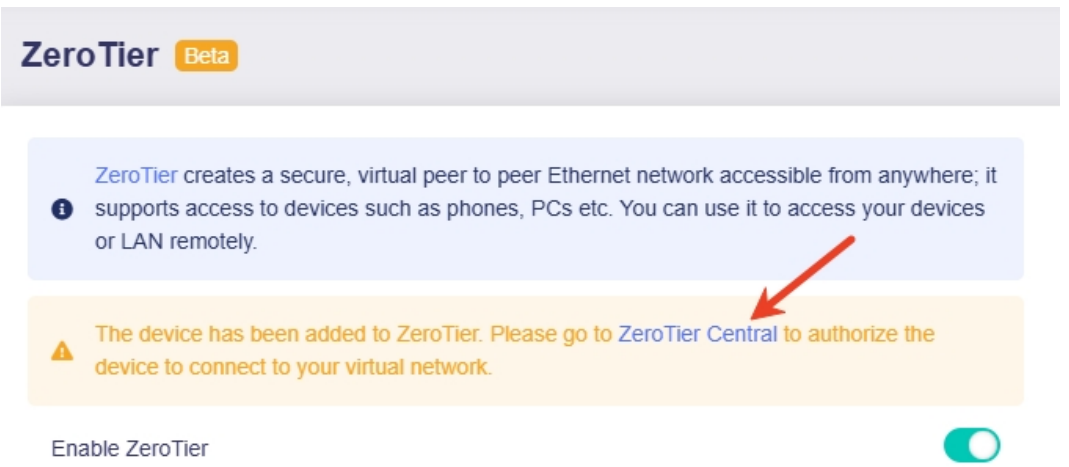


Notieren Sie die **Network ID** oben rechts. Diese besteht aus 16 Buchstaben und Ziffern und wird später benötigt, um weitere Geräte zu verbinden.

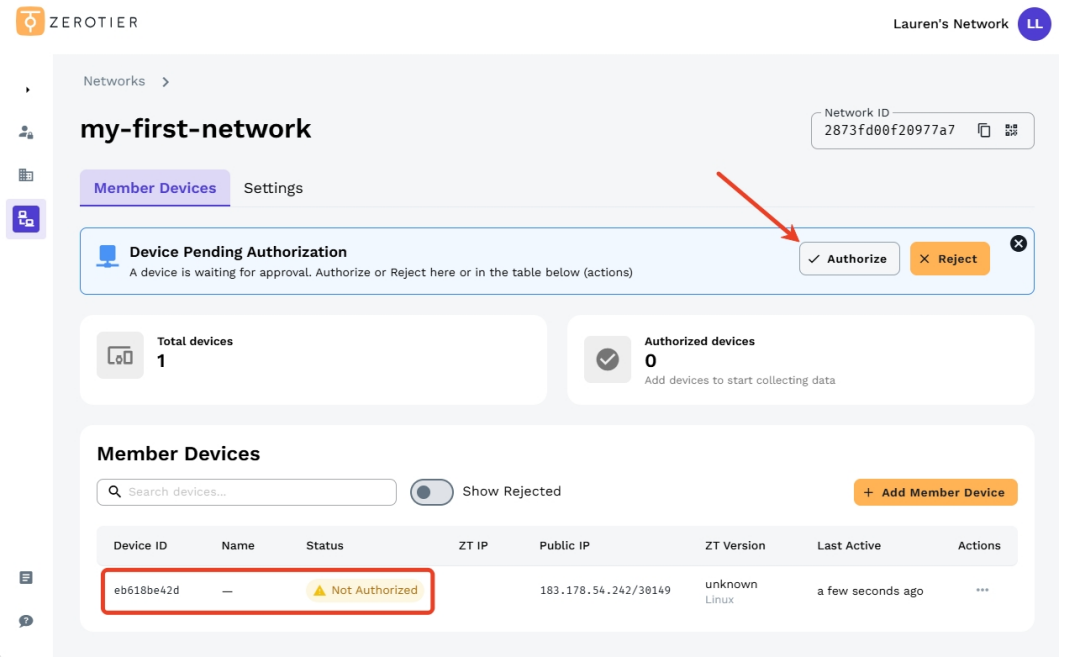
5. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **APPLICATIONS** > **ZeroTier**. Aktivieren Sie ZeroTier, geben Sie die **Network ID** ein und klicken Sie auf **Apply**.



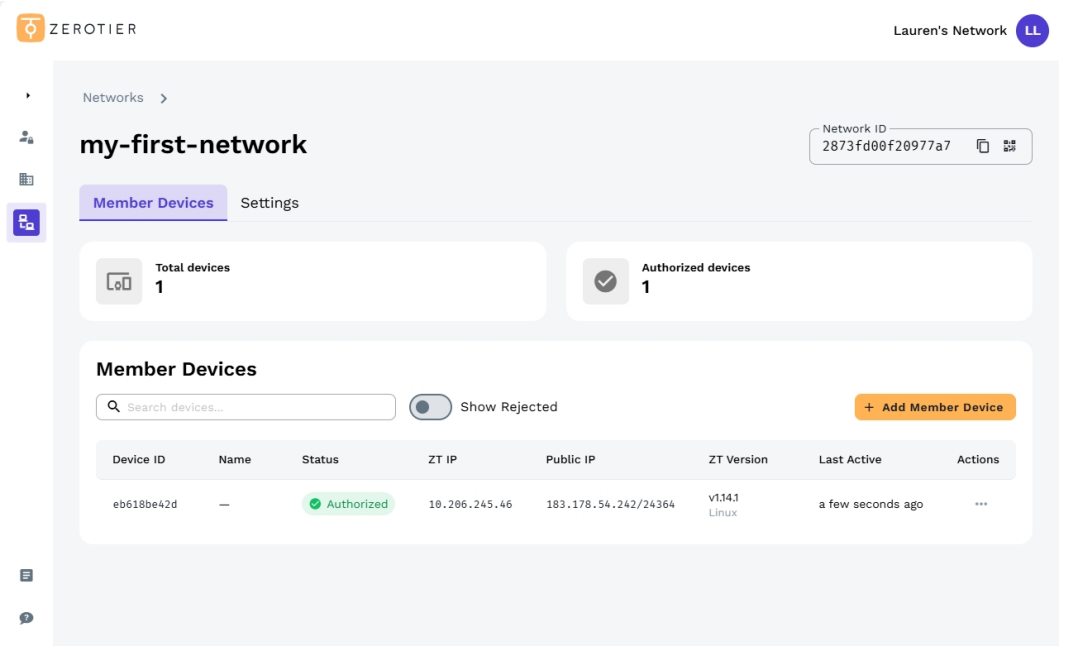
Nach kurzer Zeit erscheint der Hinweis, dass eine Autorisierung erforderlich ist. Klicken Sie auf den Link **ZeroTier Central**, um ZeroTier Central zu öffnen.



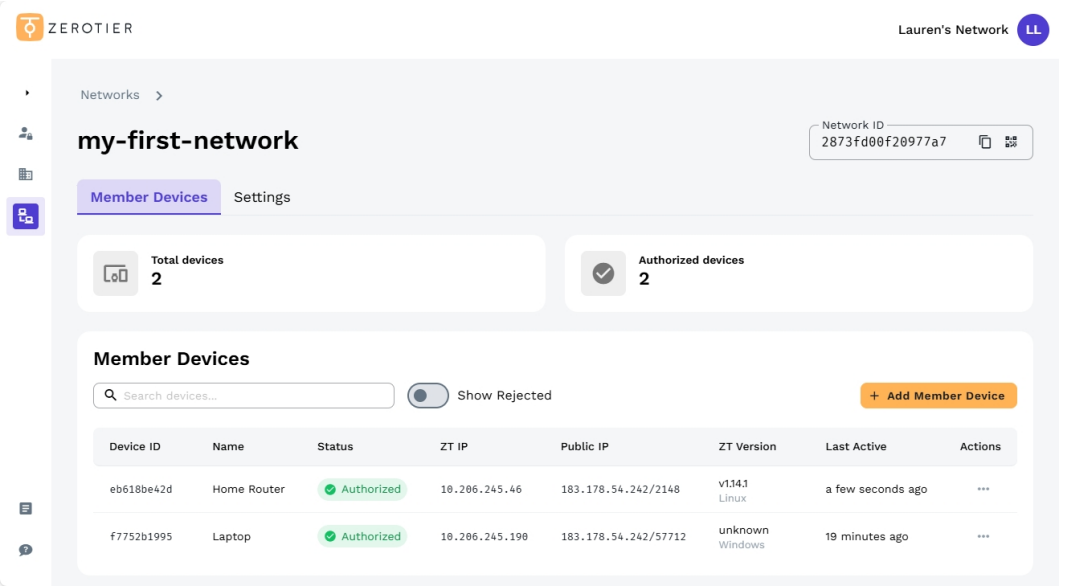
6. Suchen Sie in ZeroTier Central das ausstehende Gerät unter Pending und autorisieren Sie es.



Nach der Autorisierung erscheint die folgende Ansicht.

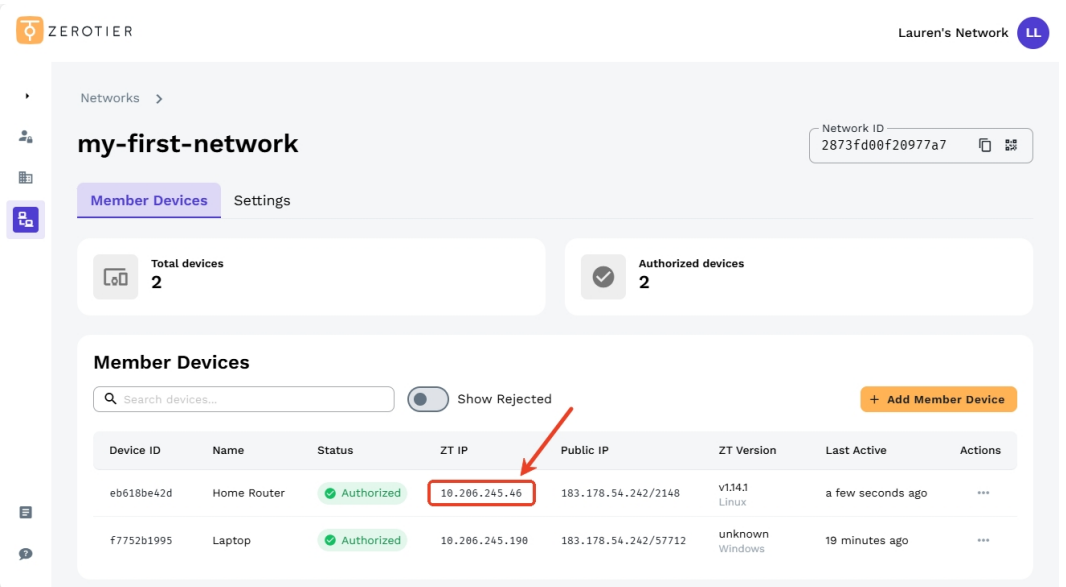


7. Fügen Sie anhand dieser Anleitung ein weiteres Gerät, etwa einen Computer oder ein Smartphone, zum selben ZeroTier-Netzwerk hinzu. Nach erfolgreichem Hinzufügen erscheint die folgende Ansicht **mit** Gerätedetails wie **Device ID, Name, Status,** Managed IP **und Public IP**.



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

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



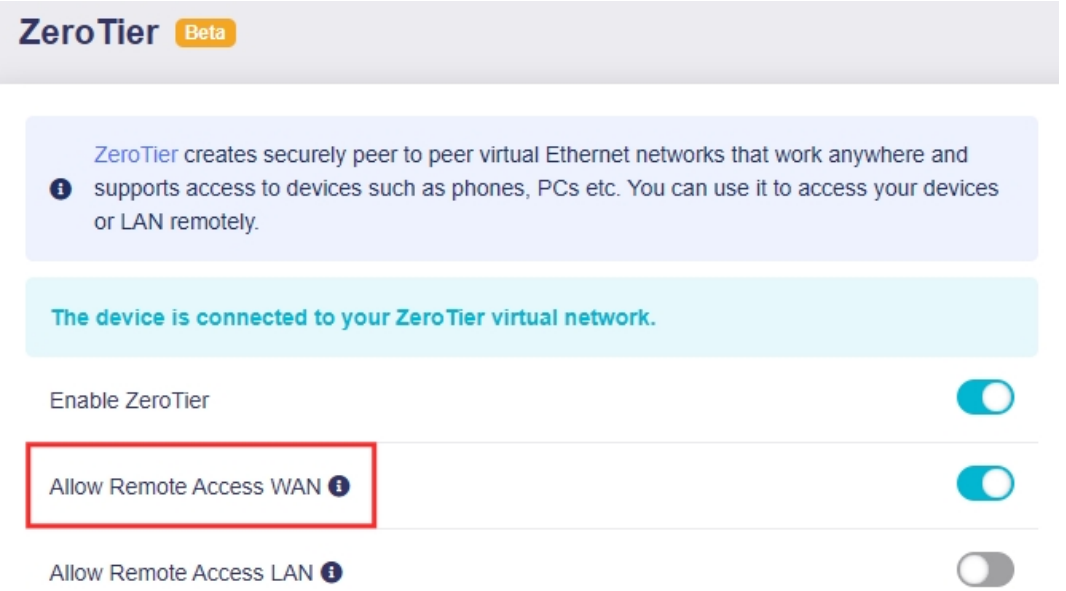
Über diese verwaltete IP-Adresse können Sie von einem Laptop im selben ZeroTier-Netzwerk auf den Router zugreifen.

9. Verbindung prüfen.

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

15.6.2 Fernzugriff auf WAN erlauben

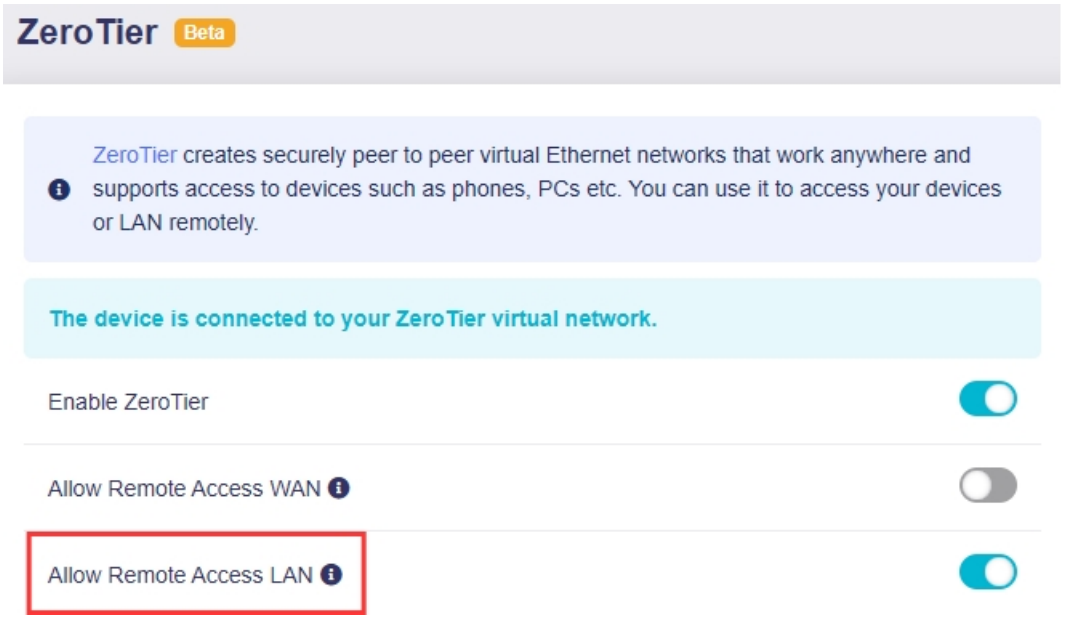
Diese Option erlaubt den Zugriff auf Ressourcen auf der WAN-Seite des Geräts über das virtuelle ZeroTier-Netzwerk. Weitere Informationen finden Sie hier.



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

15.6.3 Fernzugriff auf LAN erlauben

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



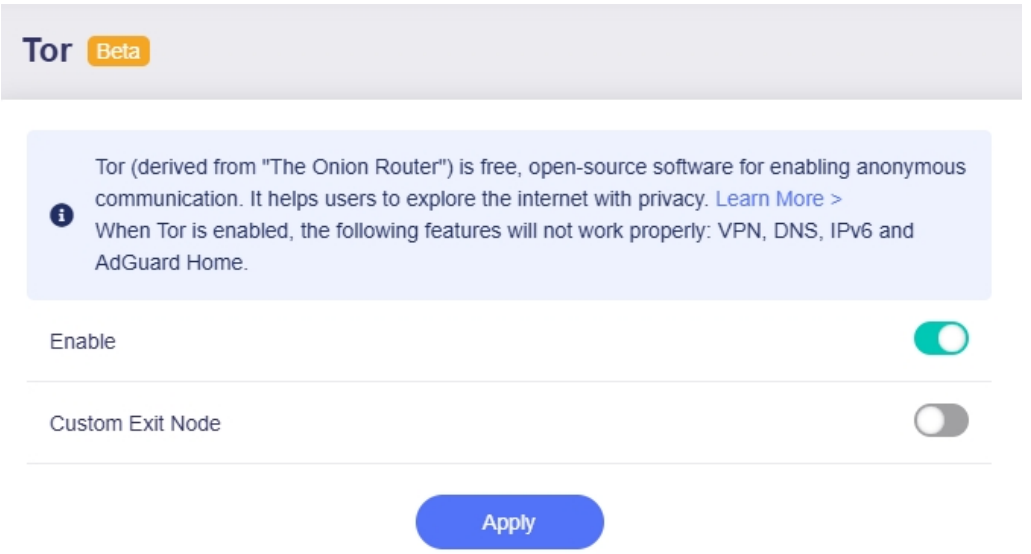
Hinweis: Damit diese Funktion wirksam wird, müssen Sie dem ZeroTier-Netzwerk Routingregeln hinzufügen. In Legacy Central lässt sich eine eigene Route kostenlos einrichten. In New Central benötigen Sie dafür mindestens den Essential-Tarif. Informationen zu den Tarifen finden Sie hier.

15.7 Tor

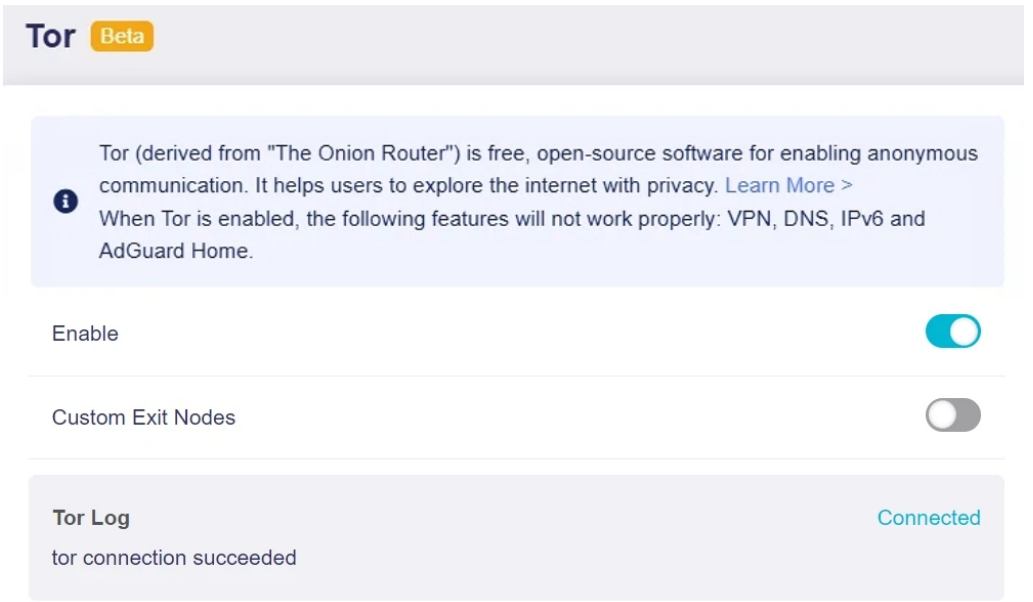
Tor, abgeleitet von **The Onion Router**, ist freie, quelloffene Software für anonyme Kommunikation. Sie unterstützt den Schutz der Privatsphäre beim Surfen im Internet. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten. Bei aktiviertem Tor funktionieren VPN, DNS, IPv6 und AdGuard Home nicht ordnungsgemäß.

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

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



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


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

Kapitel 16

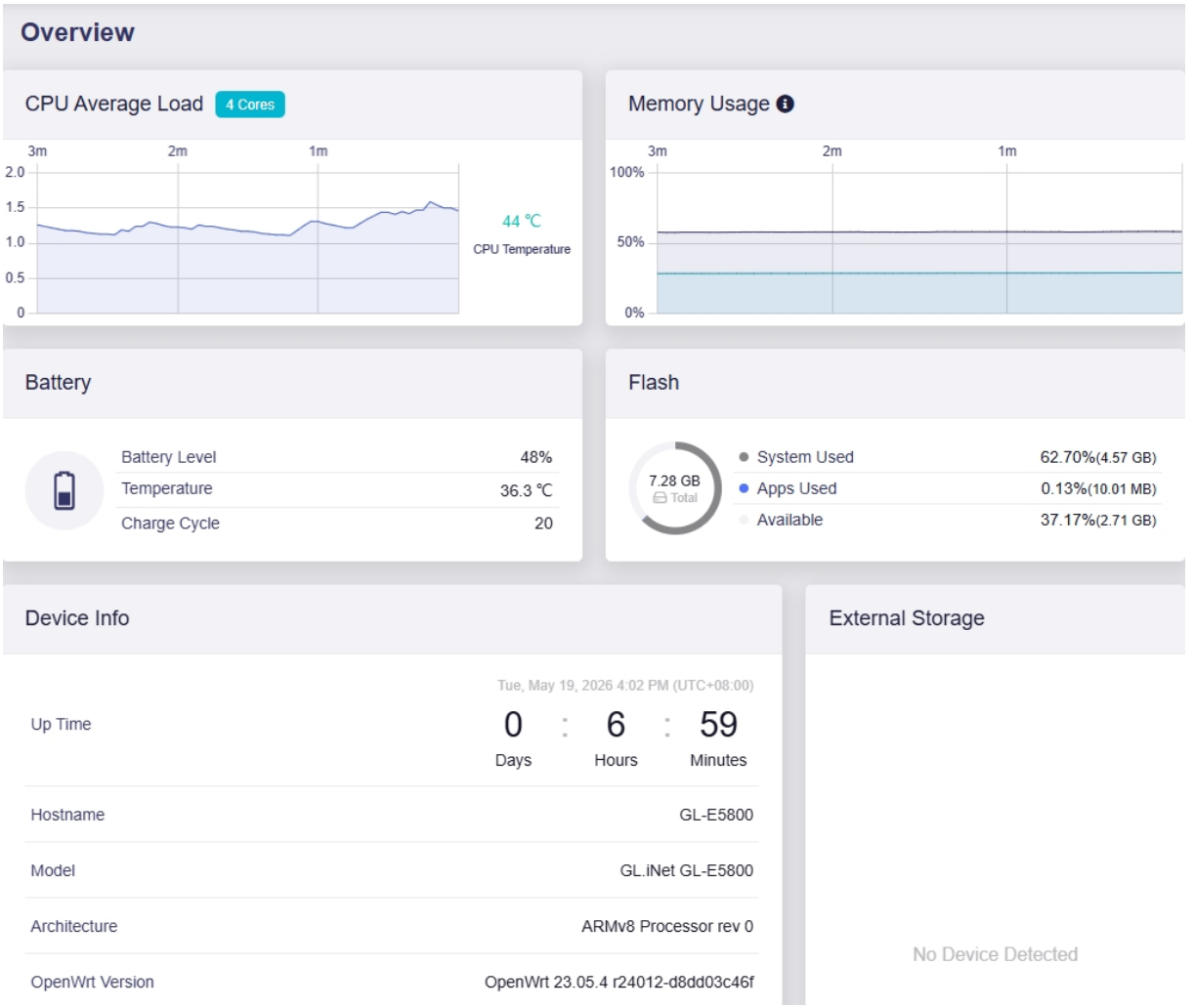
System

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

16.1 Übersicht

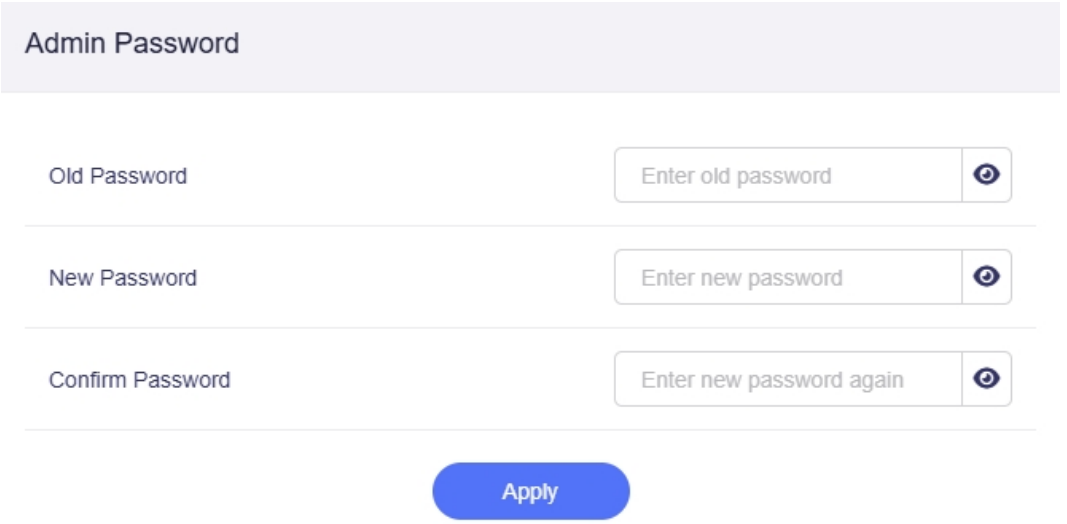
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Overview**. Die Seite zeigt den Hardwarestatus und bietet einfache Steuerungsmöglichkeiten, darunter:

- CPU-, Arbeitsspeicher- und Flash-Status
- Akkustatus
- Geräteinformationen
- Umschalten des Protokolls für externe Speicher



16.2 Administratorpasswort

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



Für das Administratorpasswort gelten folgende Anforderungen:

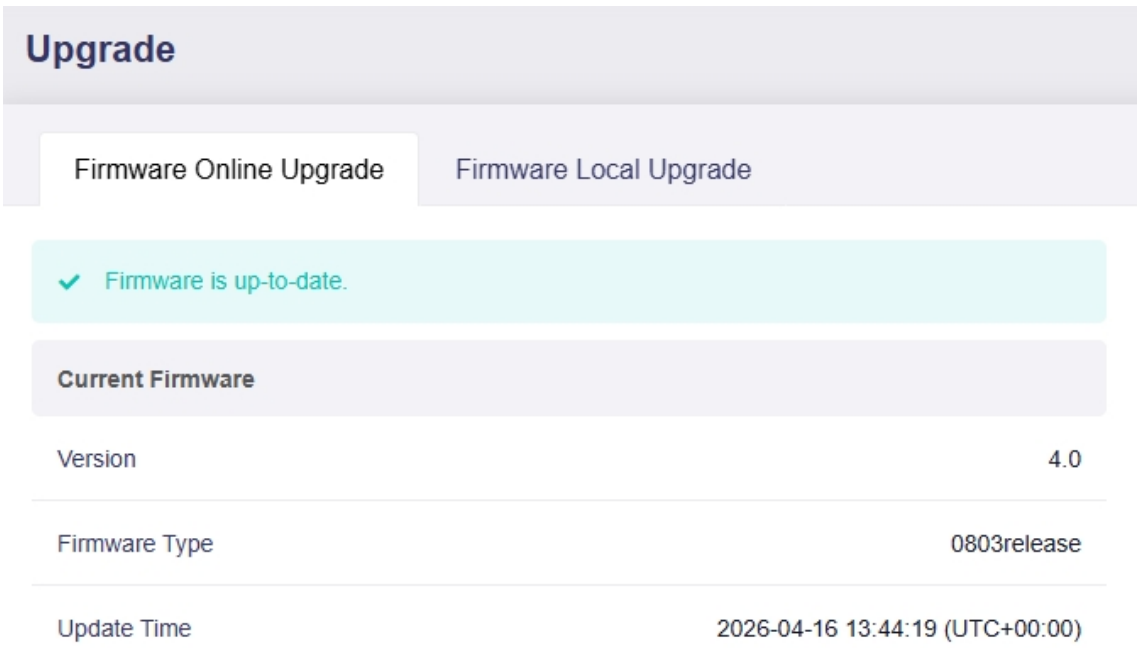
1. Mindestens 10 und höchstens 63 Zeichen.
2. Zulässig sind Buchstaben (Groß-/Kleinschreibung wird unterschieden), Ziffern und Sonderzeichen, etwa ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~ .
3. Mindestens zwei Zeichentypen aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen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

16.3 Aktualisierung

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

16.3.1 Online-Aktualisierung

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

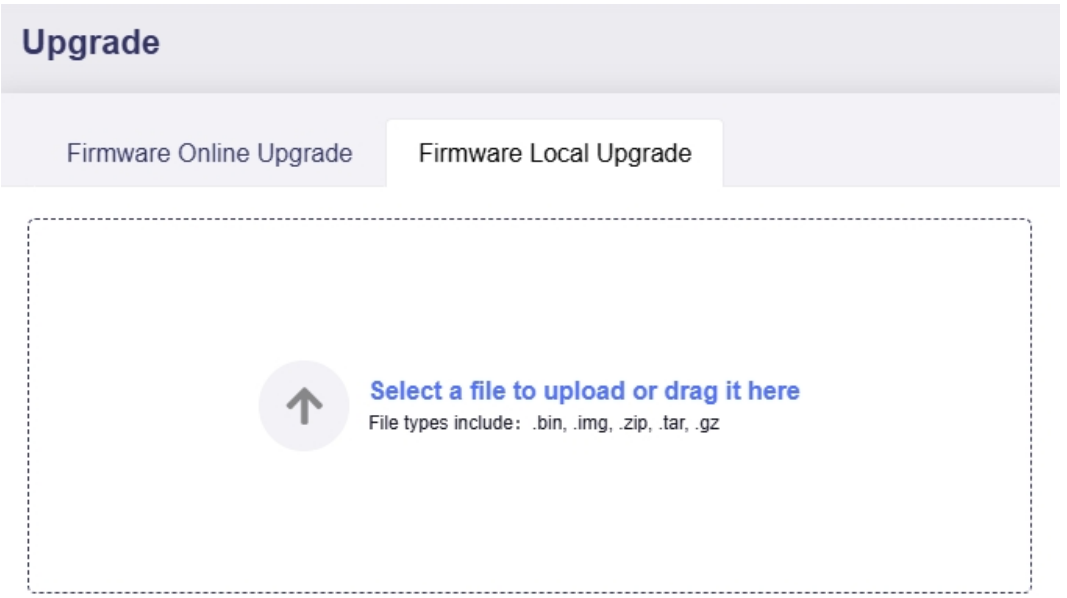


Tipp: Wenn bei einer Online-Aktualisierung **Download Failed** angezeigt wird, öffnen Sie **SYSTEM** > **Time Zone** und korrigieren Sie die Zeitzone durch Synchronisieren mit dem Browser.

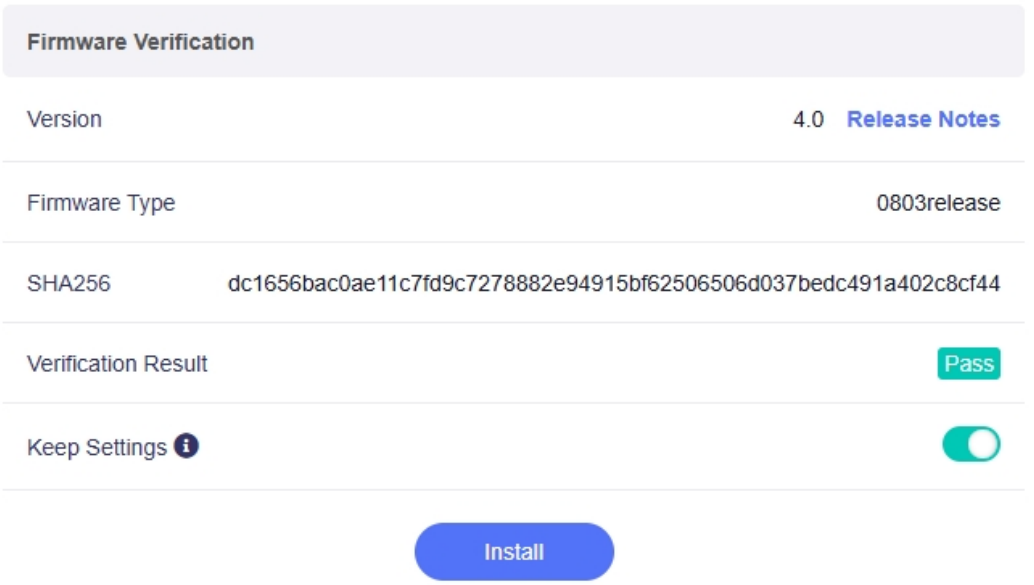
16.3.2 Lokale Aktualisierung

Für die lokale Aktualisierung benötigt der Router keine Internetverbindung.

Laden Sie das zu Ihrem Routermodell passende Firmwarepaket aus dem offiziellen Download Center auf Ihr lokales Gerät herunter. Melden Sie sich dann 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.

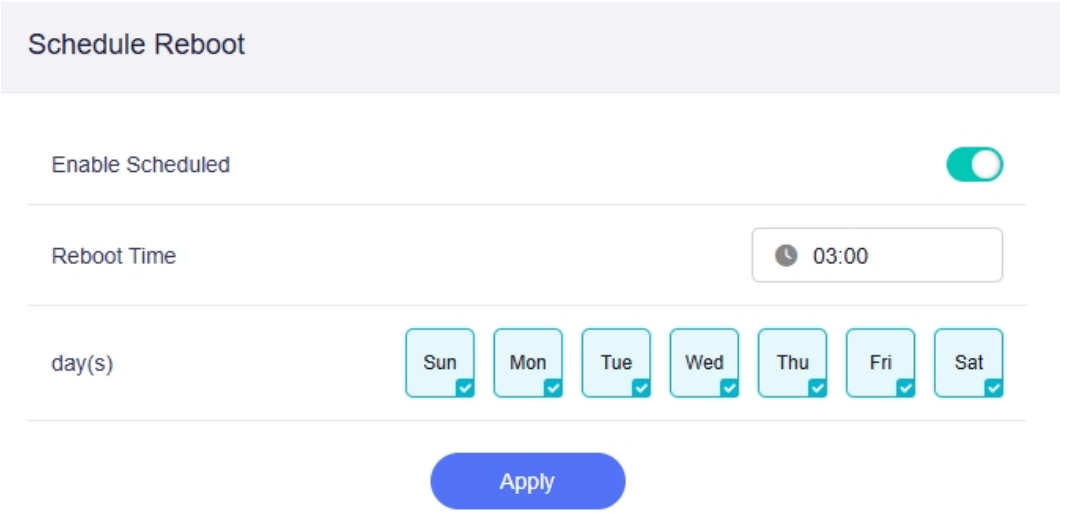


- **Keep Settings**: Bei aktivierter Option bleiben die aktuellen Einstellungen erhalten. Manuell installierte Pakete müssen nach der Aktualisierung jedoch erneut installiert werden. Aktivieren Sie diese Option nicht beim Wechsel auf eine ältere Firmwareversion.

16.4 Geplante Aufgaben

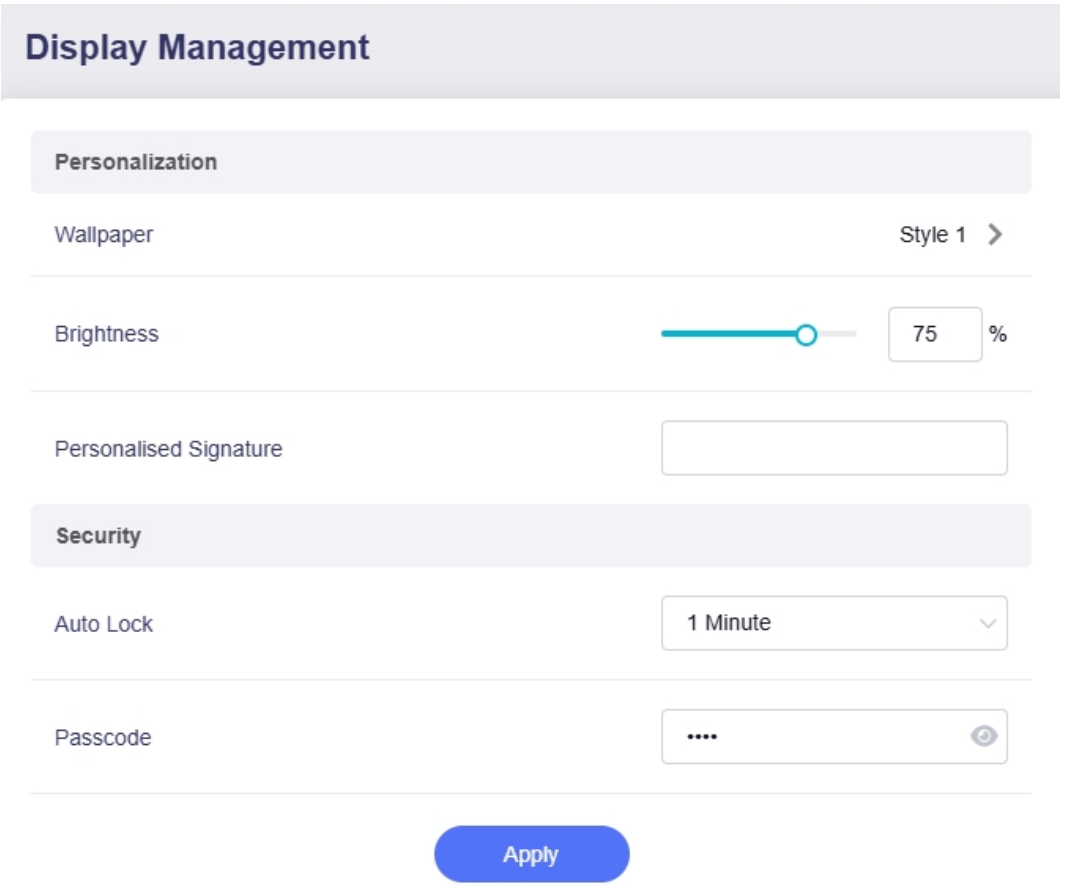
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SYSTEM** > **Scheduled Tasks**. Hier können Sie einen Zeitplan für Neustarts festlegen. Synchronisieren Sie vor der Verwendung die Uhrzeit unter Time Zone. Ist das Gerät zum geplanten Zeitpunkt ausgeschaltet, wird die Aufgabe nicht ausgeführt.

Legen Sie bei Bedarf einen Zeitplan für automatische Routerneustarts fest. Aktivieren Sie die Funktion, legen Sie die Neustartzeiten und Wochentage fest und klicken Sie auf **Apply**.



16.5 Displayverwaltung

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SYSTEM** > **Display Management**. Hier können Sie den Touchscreen und die zugehörigen Einstellungen verwalten.



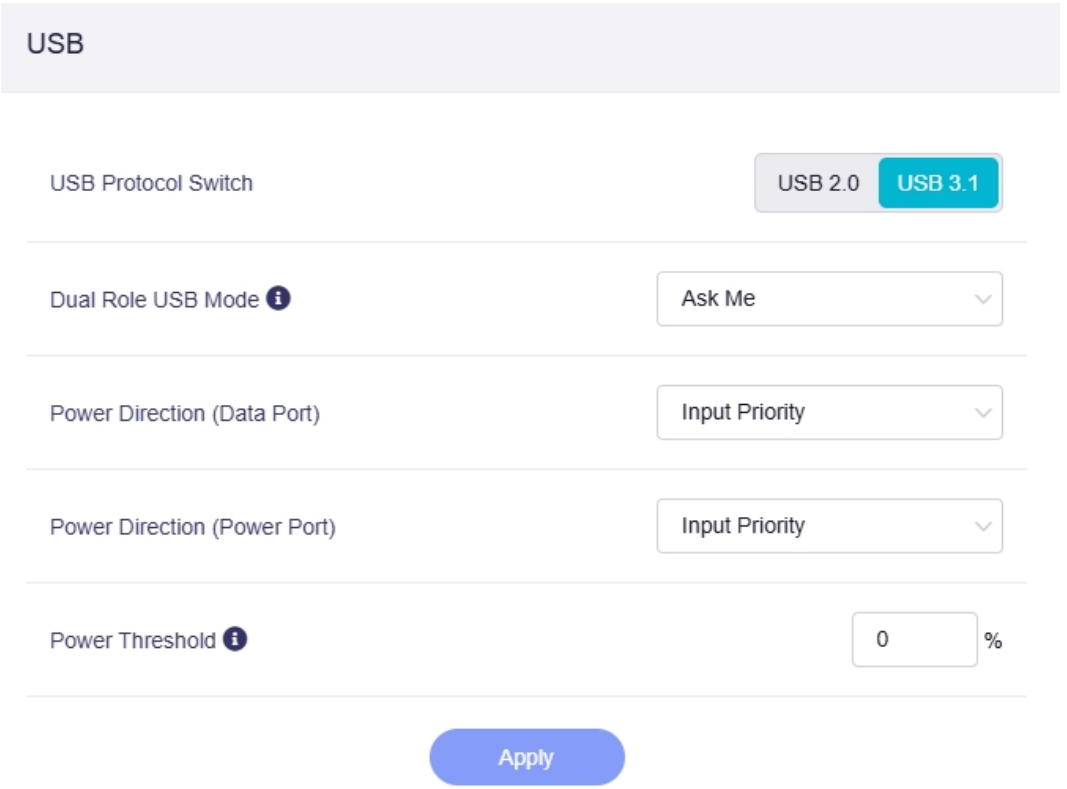
- **Wallpaper**: Passen Sie das Hintergrundbild und die Darstellung des Aktivierungsbildschirms an.
- **Brightness**: Passen Sie die Helligkeit des Touchscreens an. Verwenden Sie den Schieberegler oder geben Sie einen Prozentwert ein, um die Helligkeit an die Lichtverhältnisse anzupassen.
- **Personalised Signature**: Fügen Sie dem Touchscreen einen eigenen Text hinzu, um ihn persönlich zu gestalten oder das Gerät schnell zu erkennen.
- **Auto Lock**: Legen Sie fest, nach welcher Zeit ohne Bedienung der Bildschirm automatisch gesperrt wird. Der Bereich reicht von 15 Sekunden bis 5 Minuten.
- **Passcode**: Legen Sie für zusätzliche Sicherheit einen vierstelligen Code für den Touchscreen fest.

16.6 USB und Stromversorgung

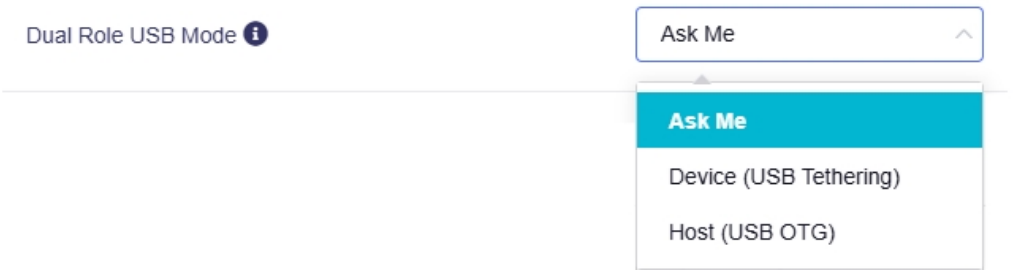
Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **SYSTEM** > **USB & Power**. Hier können Sie die USB- und Energieeinstellungen Ihres Routers konfigurieren, beispielsweise USB-Protokoll, Stromflussrichtung, Zeitlimits bei Inaktivität und Standby-Verhalten.

16.6.1 USB

In diesem Abschnitt passen Sie das Verhalten der USB-Anschlüsse Ihres Routers an.



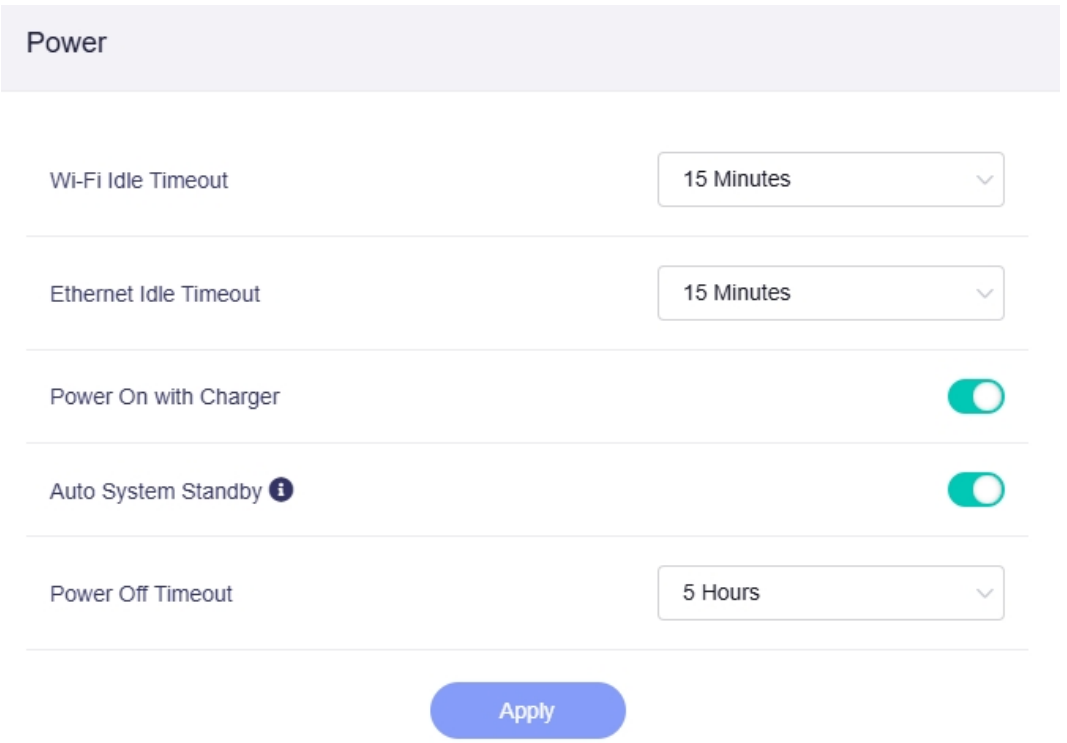
- **USB Protocol Switch**: Schalten Sie den USB-Anschluss zwischen den Protokollen USB 2.0 und USB 3.1 um.
- **Dual Role USB Mode**: Wählen Sie im Dropdown-Menü den USB-Betriebsmodus. Zur Auswahl stehen Device (Peripheriegerät) und Host.



- **Power Direction**: Wählen Sie im Dropdown-Menü die Priorität der Stromflussrichtung für den USB-Anschluss. Zur Auswahl stehen Input Priority (Eingang bevorzugen) und Output Priority (Ausgang bevorzugen).
- **Power Threshold**: Legen Sie für den USB-Anschluss einen prozentualen Akkuschwellenwert fest. Damit bestimmen Sie den Mindestladestand für den USB-Betrieb und schonen den Akku.

16.6.2 Stromversorgung

In diesem Abschnitt optimieren Sie den Energieverbrauch und das Geräteverhalten.

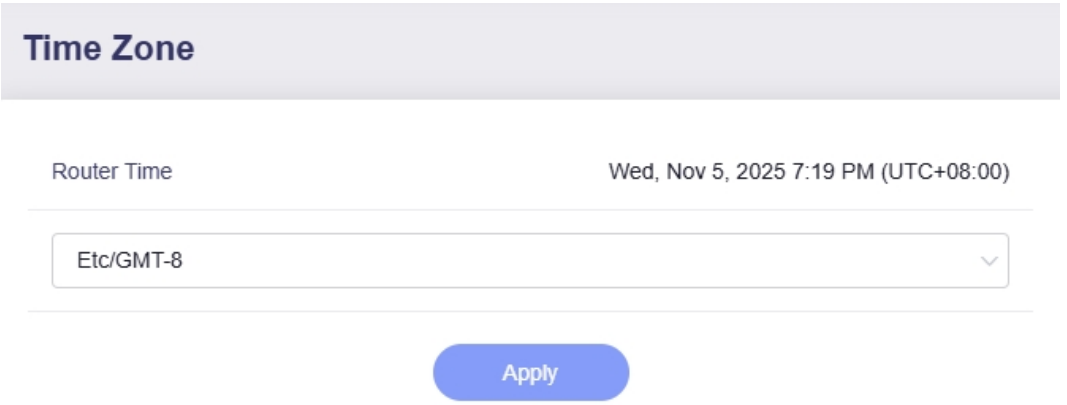


- **Wi-Fi Idle Timeout**: Legen Sie fest, nach welcher Zeit ohne Aktivität das WLAN in den Standby-Modus wechselt. Zur Auswahl stehen 10 Minuten bis 2 Stunden oder Never (nie).

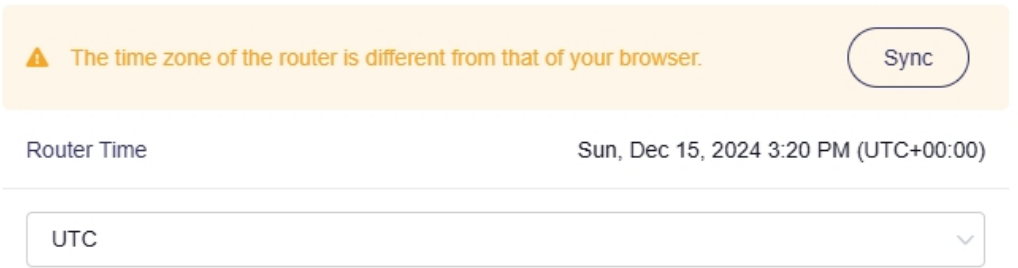
- **Ethernet Idle Timeout**: Legen Sie fest, nach welcher Zeit ohne Aktivität Ethernet in den Standby-Modus wechselt. Zur Auswahl stehen 10 Minuten bis 2 Stunden oder Never (nie).
- **Power Off Timeout**: Legen Sie fest, nach welcher Zeit ohne Aktivität sich der Router automatisch ausschaltet. Zur Auswahl stehen 1 bis 12 Stunden oder Never (nie).
- **Power On with Charger**: Aktivieren oder deaktivieren Sie das automatische Einschalten des Routers beim Anschließen eines Ladegeräts.
- **Auto Standby**: Aktivieren oder deaktivieren Sie den automatischen Standby-Modus zum Energiesparen.

16.7 Zeitzone

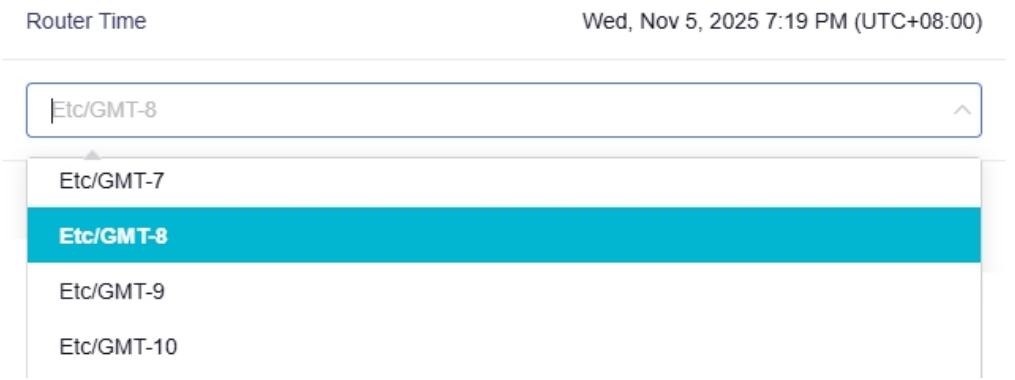
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Time Zone**. Die Seite zeigt die Systemzeit Ihres Routers mit Datum, Uhrzeit und Zeitzonenversatz an.



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



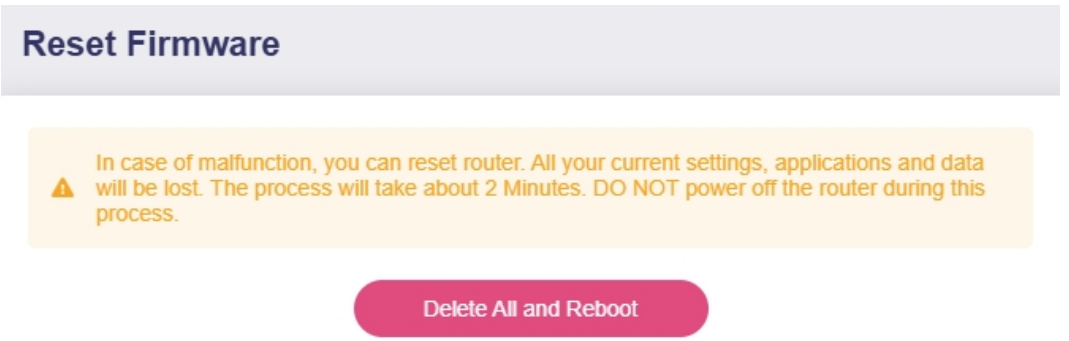
Wählen Sie zum Ändern der Zeitzone den passenden Eintrag aus der Liste, damit die Routerzeit Ihrer Ortszeit entspricht.



16.8 Firmware zurücksetzen

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

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

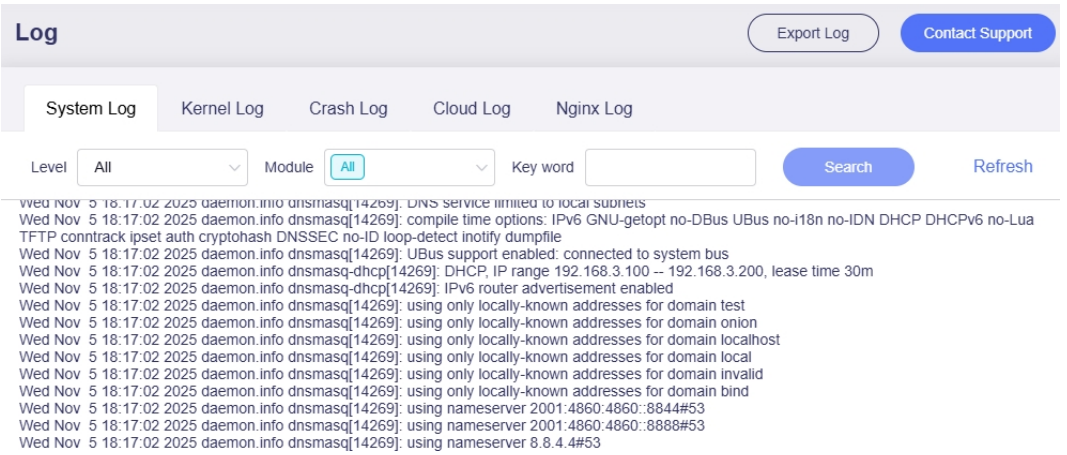


Hinweis: Alle aktuellen Einstellungen, Anwendungen und Daten werden gelöscht. Der Vorgang dauert etwa zwei Minuten. Schalten Sie den Router währenddessen nicht aus.

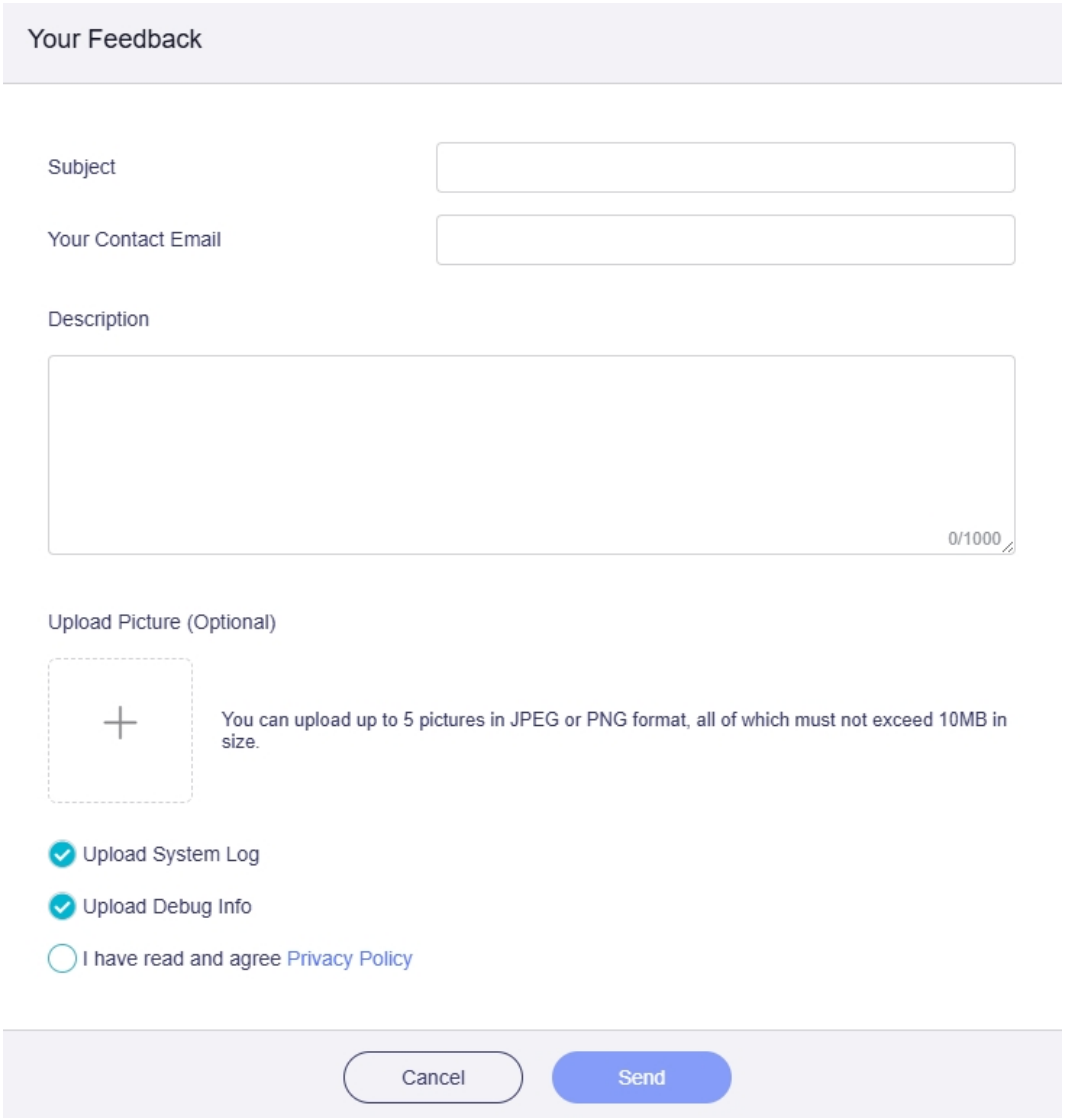
Falls Sie die Weboberfläche nicht erreichen, setzen Sie den Router mit der seitlichen Reset-Taste zurück.

16.9 Protokolle

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



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

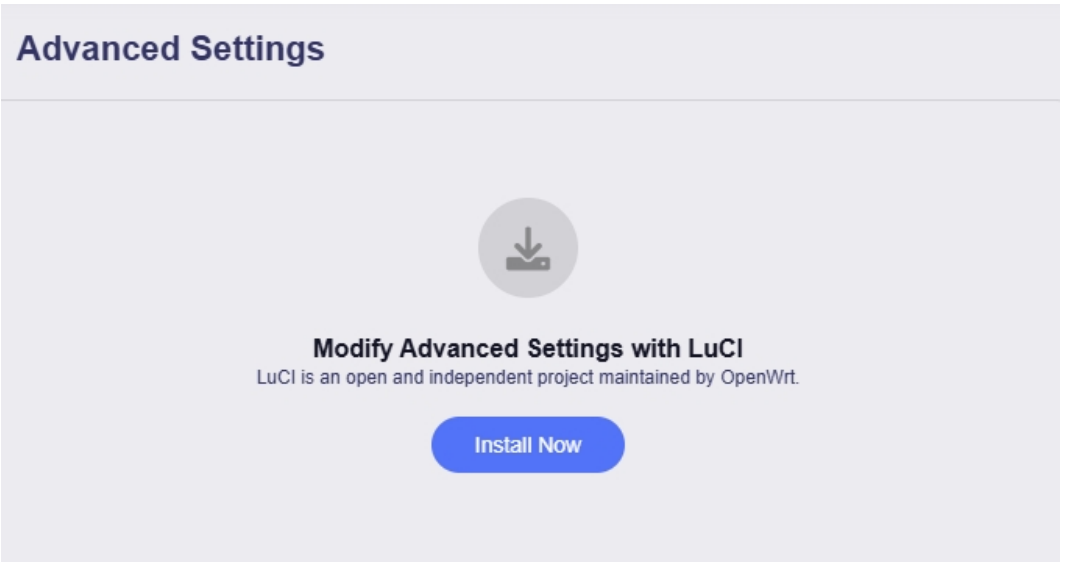

Your Feedback
Subject
Your Contact Email
Description
0/1000
Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.10 Erweiterte Einstellungen

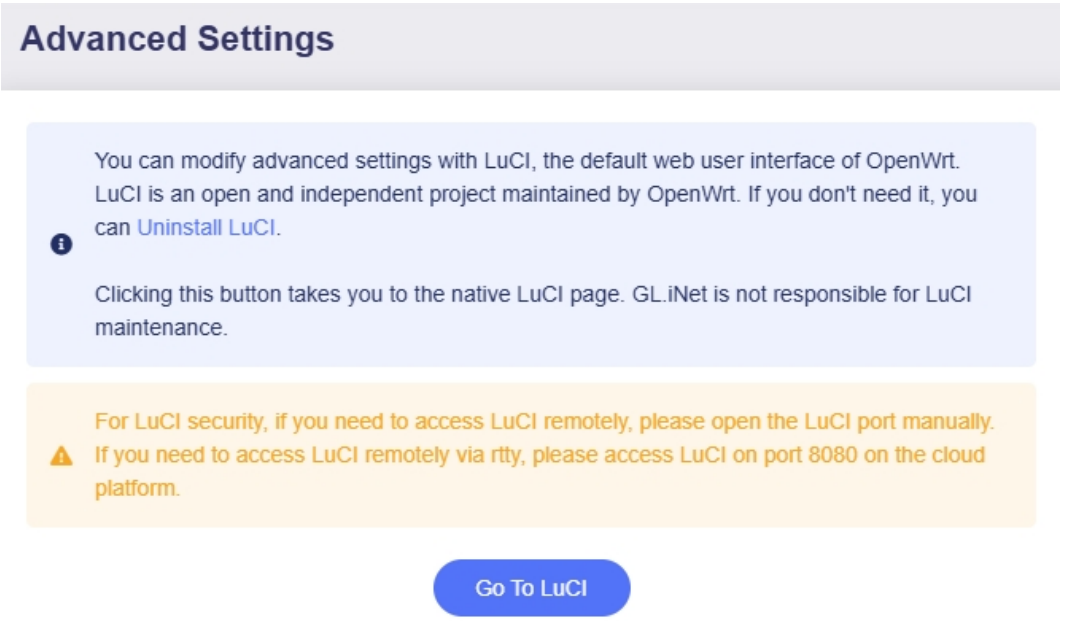
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Advanced Settings**. Hier ändern Sie erweiterte Einstellungen in LuCI, der standardmäßigen OpenWrt-Weboberfläche. LuCI ist ein offenes, unabhängiges Projekt, das von OpenWrt gepflegt und in der vorliegenden Form bereitgestellt wird.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

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

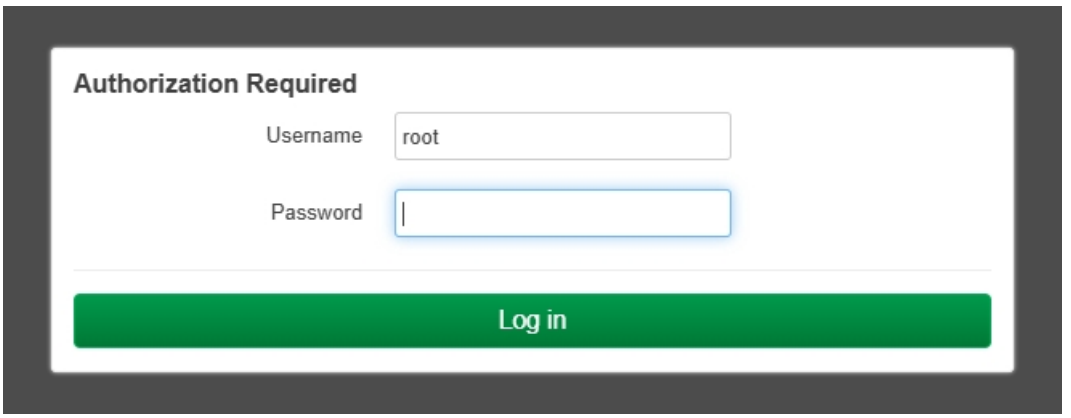
1. Klicken Sie auf **Install Now**, um die LuCI-Oberfläche zu installieren.



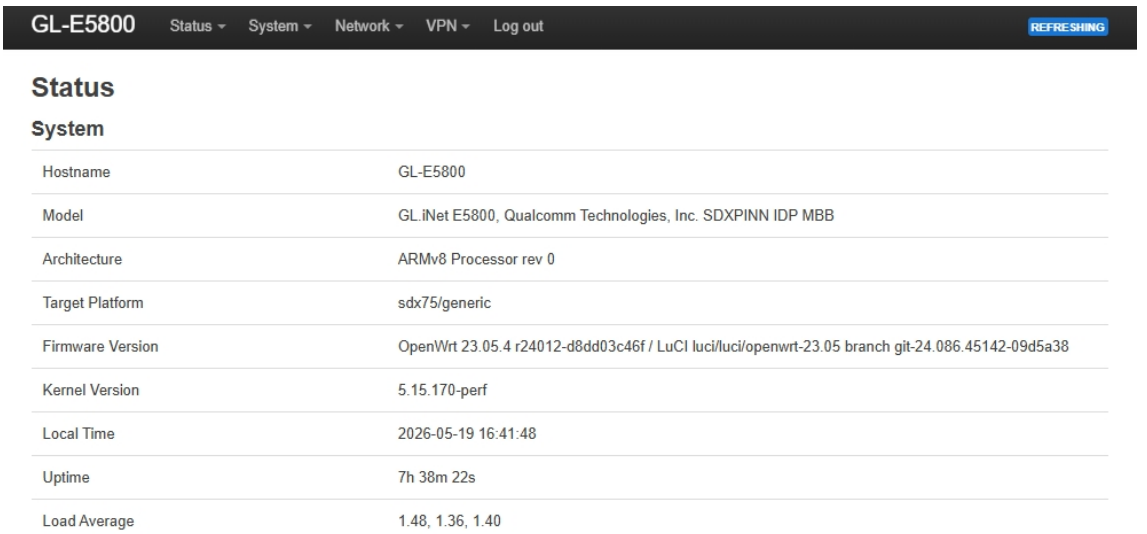
2. Klicken Sie auf **Go To LuCI**, um zur LuCI-Anmeldeseite zu gelangen.



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



Sie sind nun an der LuCI-Oberfläche angemeldet.



Sicherheitshinweise zum Akku

Verwenden und laden Sie Mudi 7 nicht weiter, wenn der Akku aufgebläht, undicht, ungewöhnlich heiß oder beschädigt ist oder einen ungewöhnlichen Geruch abgibt.

- Drücken, verbiegen, durchstechen oder zerquetschen Sie den Akku nicht und üben Sie keinen Druck darauf aus.
- Hebeln Sie einen aufgeblähten oder beschädigten Akku nicht mit Werkzeugen heraus.
- Versuchen Sie nicht, einen Akku herauszunehmen, der aufgebläht, verklemmt, undicht oder heiß ist oder sich aus anderen Gründen nicht sicher handhaben lässt.
- Entsorgen Sie einen beschädigten Lithium-Ionen-Akku weder im Hausmüll noch im gewöhnlichen Recycling.
- Versenden Sie einen aufgeblähten oder beschädigten Akku nicht mit einem gewöhnlichen Paketdienst.
- Wenden Sie sich an den GL.iNet-Support, um Unterstützung zur Garantie und zum weiteren Vorgehen zu erhalten.

Wurde der beschädigte Akku bereits entnommen, setzen Sie ihn nicht wieder ein. Wenden Sie sich an eine geeignete örtliche Batteriesammelstelle oder Schadstoffsammelstelle, die beschädigte Lithium-Ionen-Akkus annimmt.

Wenn der Akku raucht, sich schnell erhitzt, zischt, brennt oder eine andere unmittelbare Gefahr darstellt, entfernen Sie sich vom Gerät und verständigen Sie die örtlichen Rettungsdienste.

Konformitätserklärung

Hiermit erklärt GL TECHNOLOGIES (HONG KONG) LIMITED, dass der Funkanlagentyp [Tragbarer 5G NR Dreiband-Wi-Fi 7-Router, GL-E5800EU] den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: https://www.gl-inet.com/products/certificate.