GL·iNet



Benutzerhandbuch

GL-B3000 / Marble

Dualband-Heimrouter mit Wi-Fi 6

Firmware-Version 4.5.22

Über dieses Handbuch

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

Mit diesem Handbuch können Sie:

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

Darstellungskonventionen

Diese Symbole und Farben erleichtern Ihnen das Befolgen der Anweisungen.

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

Hinweis:

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

Weitere Hilfe und Informationen

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

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

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

Inhaltsverzeichnis

Sicherheitshinweise 8

Kapitel 1 Ihren Router kennenlernen 10

1.1 Produktübersicht 11

1.1.1 Geräteansicht 11

1.1.2 Anschlüsse und Bedienelemente 12

1.1.3 LED-Anzeige 13

1.2 Technische Daten 13

1.3 Lieferumfang 14

Kapitel 2 Hardware anschließen 16

2.1 Standort auswählen 17

2.2 Router anschließen 17

Kapitel 3 Am Router anmelden 19

Kapitel 4 Internetverbindung einrichten 21

4.1 Internetverbindung über Ethernetkabel 23

4.1.1 Grundeinrichtung 23

4.1.2 Protokoll 25

4.2 Internetverbindung über ein vorhandenes WLAN 28

4.2.1 Grundeinrichtung 28

4.2.2 Repeater-Optionen 32

Kapitel 5 WLAN 33

5.1 5-GHz-WLAN 34

5.2 2,4-GHz-WLAN 36

Kapitel 6 Verbundene Geräte 38

6.1 Gerätedetails 40

6.2 Aktionen 42

6.3 Geräte entfernen 44

6.4 Sortierung 45

Kapitel 7 VPN kennenlernen 46

7.1 Einführung 47

7.2 Einsatzmöglichkeiten 48

Kapitel 8 VPN-Dashboard 51

8.1 VPN-Client 52
8.1.1 Client-Optionen 53
8.1.2 Richtlinienmodus 55
8.1.3 Globale Optionen 56
8.2 VPN-Server 59
8.2.1 Server-Optionen 60
8.2.2 Server-Routingregeln 61
8.2.3 Globale Optionen 63
Kapitel 9 VPN-Server einrichten 64
9.1 OpenVPN-Server einrichten 65
9.1.1 Vorbereitung 65
9.1.2 Einrichtung 66
9.1.3 Fehlerbehebung 68
9.2 WireGuard-Server einrichten 70
9.2.1 Vorbereitung 70
9.2.2 Einrichtung 71
9.2.3 Fehlerbehebung 74
Kapitel 10 VPN-Client einrichten 75
10.1 OpenVPN-Client einrichten 76
10.1.1 Vorbereitung 76
10.1.2 NordVPN einrichten 76
10.1.3 OpenVPN-Client manuell einrichten (andere Anbieter) 82
10.2 WireGuard-Client einrichten 85
10.2.1 Vorbereitung 85
10.2.2 AzireVPN einrichten 86
10.2.3 Mullvad einrichten 89
10.2.4 WireGuard-Client manuell einrichten (andere Anbieter) 93
Kapitel 11 Tor 98
Kapitel 12 Anwendungen 100
12.1 Plug-ins 101
12.2 Dynamisches DNS 102
12.2.1 DDNS aktivieren 102
12.2.2 DDNS-Funktion prüfen 105
12.2.3 HTTPS-Fernzugriff 107

12.2.4 SSH-Fernzugriff 109
12.3 GoodCloud 111
12.3.1 GoodCloud aktivieren 112
12.3.2 Router verwalten 117
12.3.3 Geräteverknüpfung aufheben 123
12.4 AdGuard Home 124
12.5 Kindersicherung 127
12.5.1 Schnelleinrichtung 127
12.6.2 Fehlerbehebung 136
12.7 ZeroTier 137
12.7.1 ZeroTier einrichten 138
12.7.2 Fernzugriff auf WAN erlauben 142
12.7.3 Fernzugriff auf LAN erlauben 144
12.8 Tailscale 145
12.8.1 Tailscale einrichten 146
12.8.2 Fernzugriff auf WAN erlauben 149
12.8.3 Fernzugriff auf LAN erlauben 150
12.8.4 Eigene Exit-Nodes 151
Kapitel 13 Netzwerk 153
13.1 Firewall 154
13.1.1 Portweiterleitungen 154
13.1.2 Ports am Router öffnen 156
13.1.3 DMZ 157
13.2 Multi-WAN 158
13.2.1 Schnittstellenstatus überwachen 158
13.2.2 Multi-WAN-Modus 161
13.3 LAN 164
13.3.1 Grundeinstellungen 164
13.3.2 DHCP-Server 165
13.3.3 Adressreservierung 167
13.4 Gastnetzwerk 168
13.4.1 Grundeinstellungen 168
13.4.2 DHCP-Server 169
13.5 DNS 171

13.5.1 Allgemeine Einstellungen 171
13.5.2 DNS-Servereinstellungen 172
13.5.3 Hosts bearbeiten 174
13.6 Netzwerkmodus 176
13.7 IPv6 178
13.7.1 IPv6-Modus 178
13.7.2 DNS-Adressen beziehen 179
13.8 MAC-Adresse 180
13.9 Drop-in Gateway 182
13.10 IGMP Snooping 185
13.11 Netzwerkbeschleunigung 186
13.12 NAT-Einstellungen 187
Kapitel 14 System 188
14.1 Übersicht 189
14.2 Aktualisierung 190
14.2.1 Online-Aktualisierung 190
14.2.2 Lokale Aktualisierung 191
14.3 Geplante Aufgaben 192
14.3.1 LED-Zeitplan 192
14.3.2 Geplanter Neustart 193
14.3.3 Zeitplan für das 5-GHz-WLAN 194
14.3.4 Zeitplan für das 2,4-GHz-WLAN 197
14.4 Zeitzone 200
14.5 Protokolle 201
14.6 Sicherheit 202
14.6.1 Administratorpasswort 202
14.6.2 Lokale Zugriffskontrolle 203
14.6.3 Fernzugriffskontrolle 205
14.7 Firmware zurücksetzen 206
14.8 Erweiterte Einstellungen 207

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

Der Router Marble (GL-B3000) ist selbst ein kleines Kunstwerk: Als Bilderrahmen gestaltet, bietet er Platz für Ihr Lieblingsmotiv und setzt einen besonderen Akzent in Ihrem Wohnraum. Neben seinem ansprechenden Design überzeugt der Marble (GL-B3000) mit hoher Leistung dank Wi-Fi 6 und VPN-Unterstützung.

1.1.1 Geräteansicht

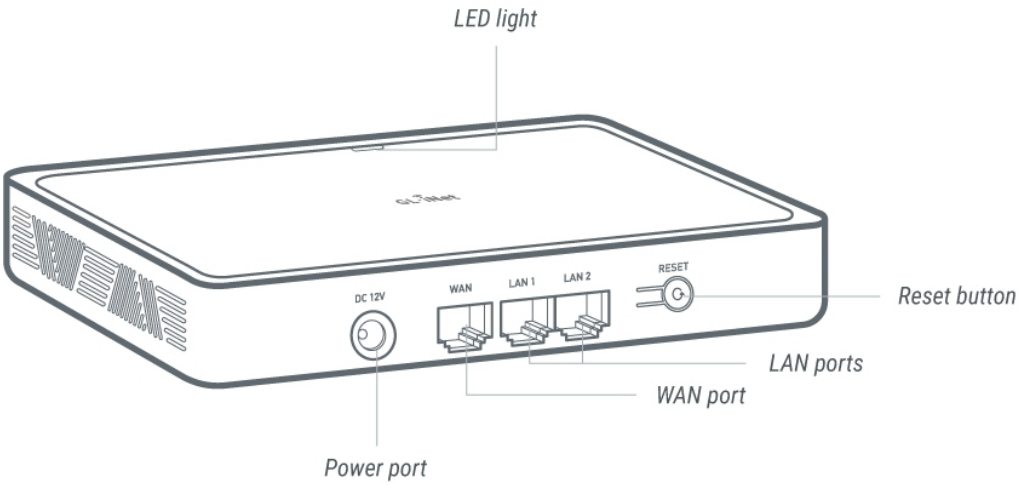








1.1.2 Anschlüsse und Bedienelemente



Element	Beschreibung
Stromanschluss	Zum Anschließen des Netzteils.
WAN-Anschluss	Zum Anschließen eines Modems oder einer Ethernetdose für den Internetzugang.
LAN-Anschluss	Zum Anschließen kabelgebundener Geräte bei Bedarf.
Reset-Taste	Halten Sie die Taste **4 Sekunden** gedrückt, um Ihr Netzwerk zu reparieren. Halten Sie die Taste **10 Sekunden** gedrückt und lassen Sie sie dann los, um den Router auf die Werkseinstellungen zurückzusetzen.

1.1.3 LED-Anzeige

Status	Bedeutung
Leuchtet blau	System startet
Blinkt langsam blau	Netzwerksuche läuft
Blinkt schnell blau	Firmware wird aktualisiert
Leuchtet weiß	Normaler Betrieb

1.2 Technische Daten

Anschlüsse	1 × WAN-Ethernetanschluss 2 × LAN-Ethernetanschluss 1 × Gleichstromeingang, 12 V/1,5 A 1 × Reset-Taste
CPU	Qualcomm, Zweikernprozessor mit 1 GHz
Arbeitsspeicher / Speicher	512 MB DDR3L / 128 MB NAND-Flash
Protokoll	IEEE 802.11a/b/g/n/ac/ax
WLAN-Geschwindigkeit	574 Mbit/s (2,4 GHz), 2402 Mbit/s (5 GHz)
Antennen	4 × interne Antenne
Ethernet-Geschwindigkeit	10/100/1000 Mbit/s
Stromversorgung	DC5521, 12 V/1,5 A (5,5 × 2,1 mm)
Leistungsaufnahme	< 13W
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Lagertemperatur	-20 ~ 70°C (-4 ~ 158°F)
Abmessungen / Gewicht	Router: 155 × 120 × 23 mm / 275 g Bilderrahmen: 235 × 197 × 32 mm (für ein Foto mit 8 Zoll)

Weitere Ressourcen	Datenblatt / Firmware / App / Auspacken / Anleitungen

*Die WLAN-Geschwindigkeiten basieren auf den IEEE-802.11-Standards (z. B. 802.11ax für Wi-Fi 6). Der tatsächliche Datendurchsatz und die Reichweite können durch Hindernisse wie Wände oder Metall, Netzwerkauslastung sowie die Leistungsfähigkeit der Endgeräte geringer ausfallen.

*Für die Nutzung von Wi-Fi 6 (802.11ax) und seinen Funktionen (OFDMA, MU-MIMO, 1024-QAM, HT160) müssen die Endgeräte die jeweiligen Technologien unterstützen.

1.3 Lieferumfang

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

Im Lieferumfang enthalten:

- 1 × Marble (GL-B3000)
- 1 × Benutzerhandbuch
- 1 × Dankeskarte
- 1 × Ethernetkabel
- 1 × Wandmontageset
- 1 × Klebepad
- 1 × Routerständer
- 1 × Bilderrahmen (optional)
- 1 × Netzteil
- 1 × Steckeradapter (je nach Lieferland)

User manual



Marble (GL-B3000)



Photo frame (Optional)



Thank you card



Adhesive pad

Router stand



Ethernet cable



Power adapter



Converters

(Base on your shipping countries)



Wall mount



Screws



Kapitel 2

Hardware anschließen

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

2.1 Standort auswählen

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

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

2.2 Router anschließen

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

3. **Am Router anmelden**

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

Kapitel 3

Am Router anmelden

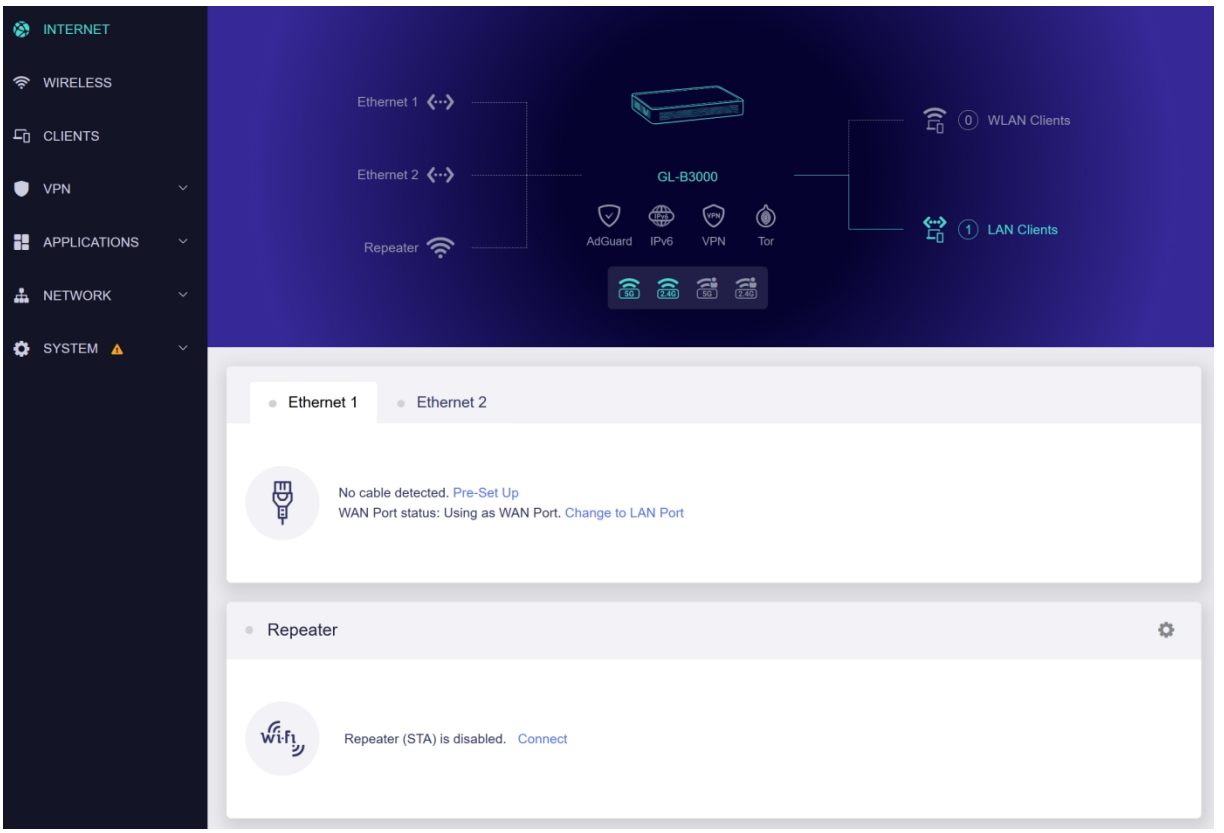
Dieses Kapitel erklärt, wie Sie sich über die Weboberfläche an Ihrem Router anmelden.

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

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

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

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



Kapitel 4

Internetverbindung einrichten

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

Marble unterstützt zwei Methoden für den Internetzugang: Ethernet und Repeater. Wählen Sie die für Ihren Einsatz passende Methode.

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

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

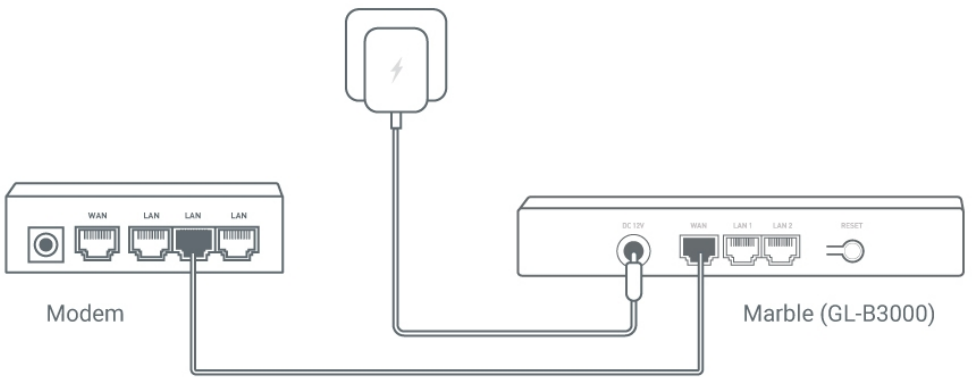
4.1 Internetverbindung über Ethernetkabel

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

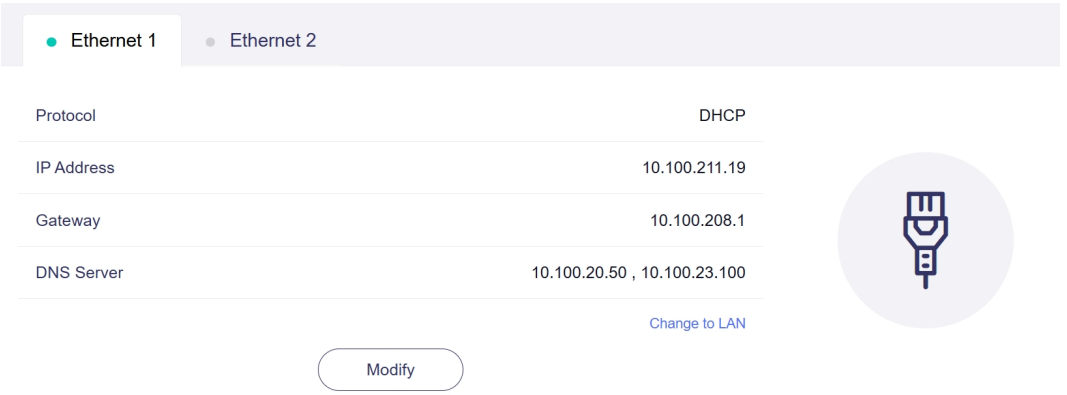
4.1.1 Grundeinrichtung

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

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

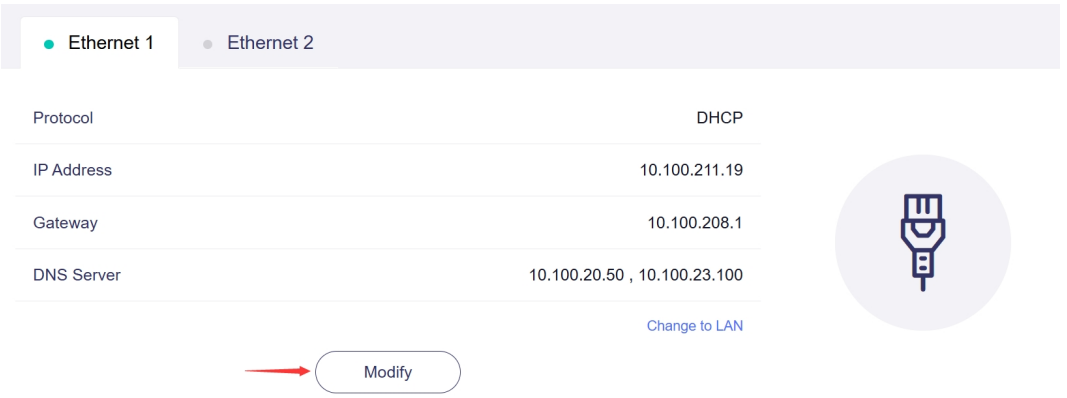


2. Melden Sie sich an der Weboberfläche des Routers an und öffnen Sie **INTERNET** > **Ethernet**. Bei erfolgreicher Verbindung werden im Abschnitt Ethernet die Netzwerkdaten angezeigt, darunter Protokoll, IP-Adresse, Gateway und DNS-Server.


Ethernet 1
Ethernet 2
Protocol
DHCP
IP Address
10.100.211.19
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Change to LAN
Modify

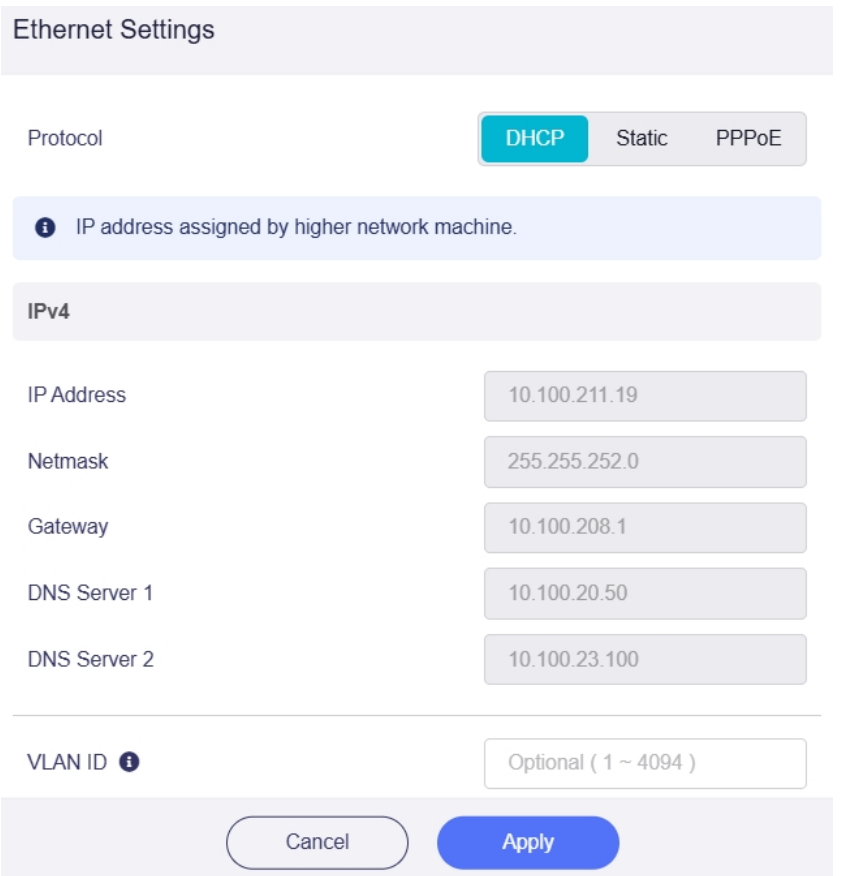
4.1.2 Protokoll

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



- **DHCP**

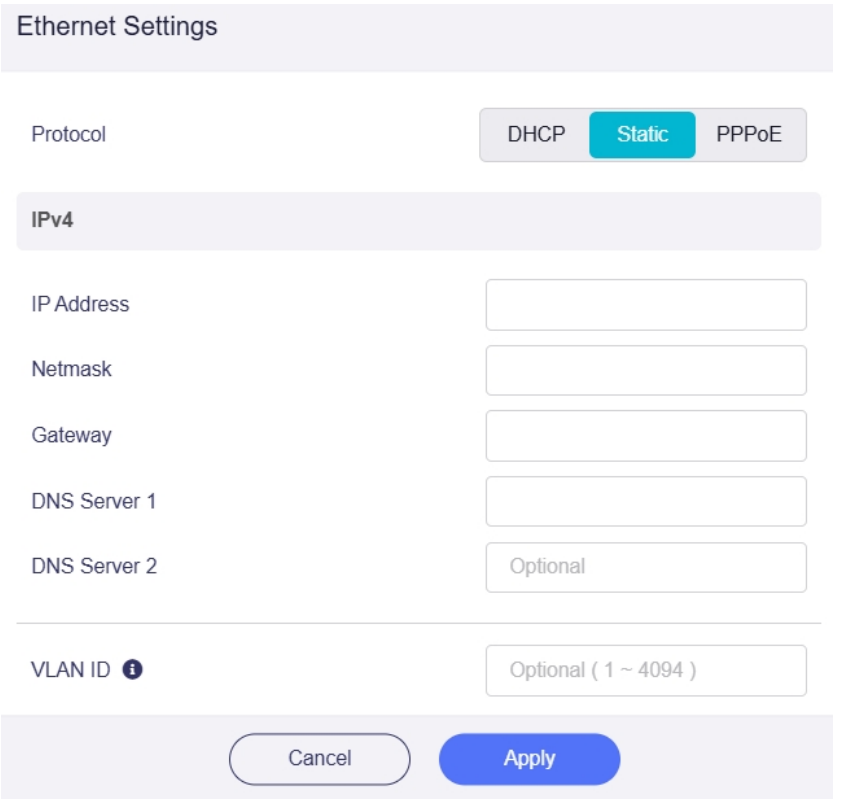
  DHCP ist das voreingestellte und am häufigsten verwendete Netzwerkprotokoll. Es weist Geräten in einem IP-Netzwerk nach dem Client-Server-Prinzip automatisch IP-Adressen und weitere Netzwerkeinstellungen zu.



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

- **Statische IP-Adresse**

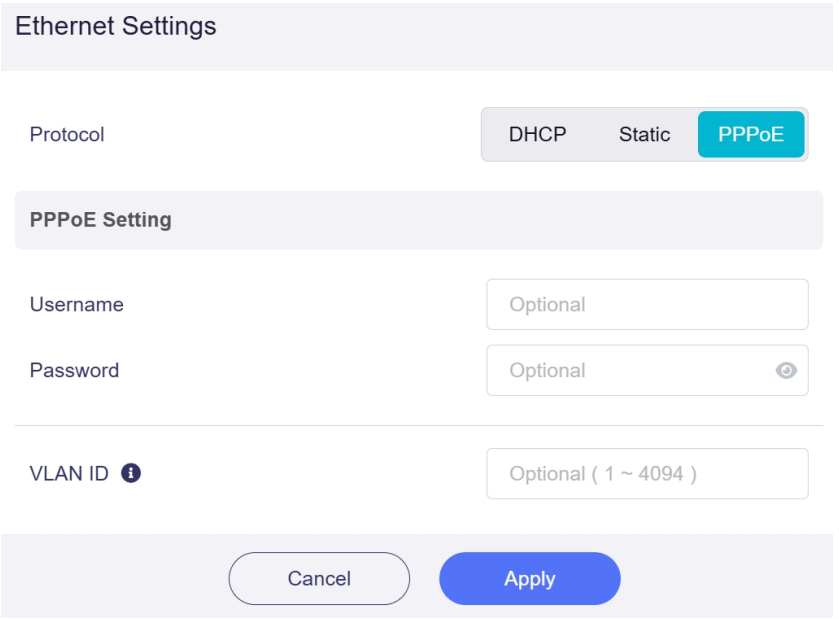
  Eine statische IP-Adresse ist erforderlich, wenn Ihr Internetanbieter Ihnen eine feste öffentliche IP-Adresse zuweist oder wenn Sie Netzwerkparameter wie IP-Adresse, Gateway und Subnetzmaske manuell festlegen müssen.



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

- **PPPoE**

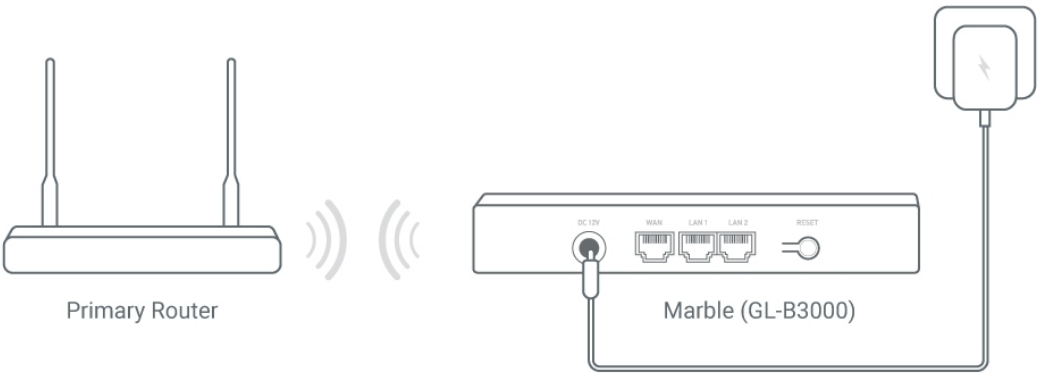
  PPPoE (Point-to-Point Protocol over Ethernet) ist ein von Internetanbietern häufig verwendetes Netzwerkprotokoll. In der Regel stellt der Anbieter ein Modem sowie einen individuellen Benutzernamen und ein Passwort bereit, die Sie zur Einrichtung der Internetverbindung benötigen.



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

4.2 Internetverbindung über ein vorhandenes WLAN

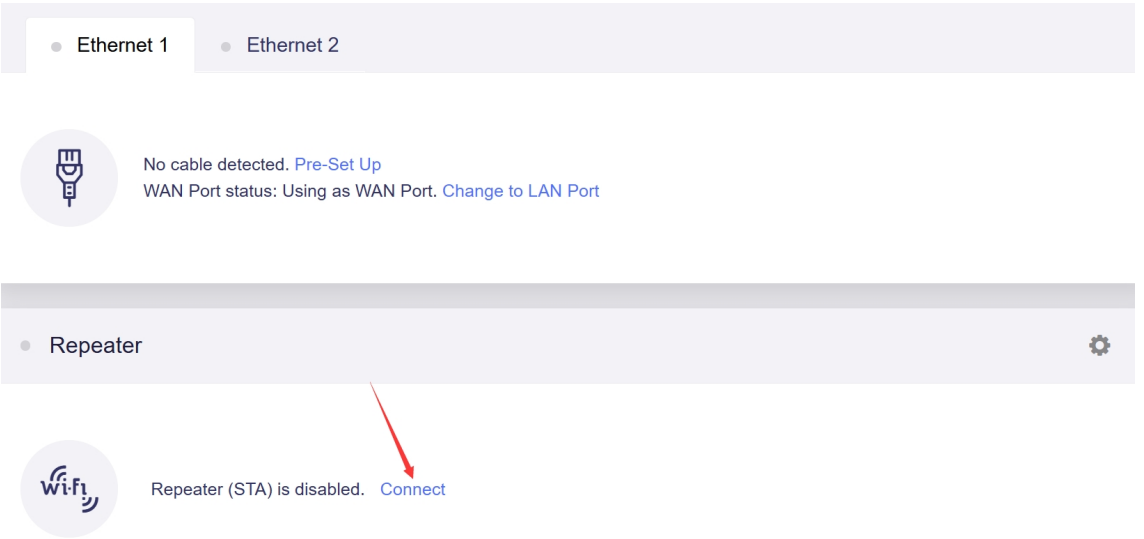
Verbinden Sie den Router als Repeater mit einem vorhandenen WLAN, um die Signalabdeckung zu erweitern und ein vom Hauptnetzwerk getrenntes lokales Netzwerk aufzubauen. An Orten mit kostenlosen öffentlichen Hotspots, etwa Hotels oder Cafés, verbessert der Repeater die WLAN-Abdeckung, ermöglicht mehreren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



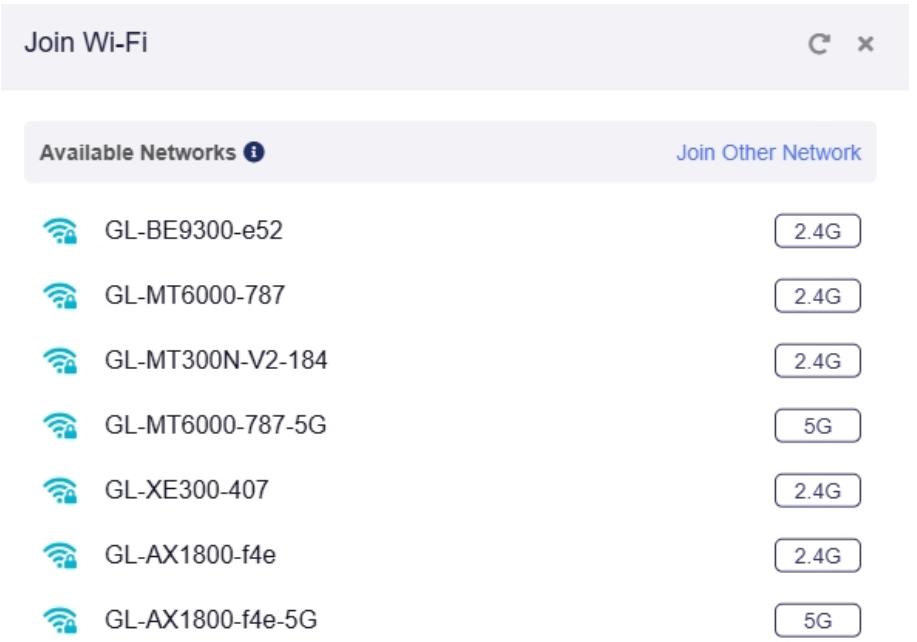
Die Repeater-Funktion von GL.iNet arbeitet standardmäßig im WISP-Modus (Wireless Internet Service Provider). Dabei erstellt der Router ein eigenes Subnetz und schützt Sie durch seine Firewall vor dem öffentlichen Netzwerk.

4.2.1 Grundeinrichtung

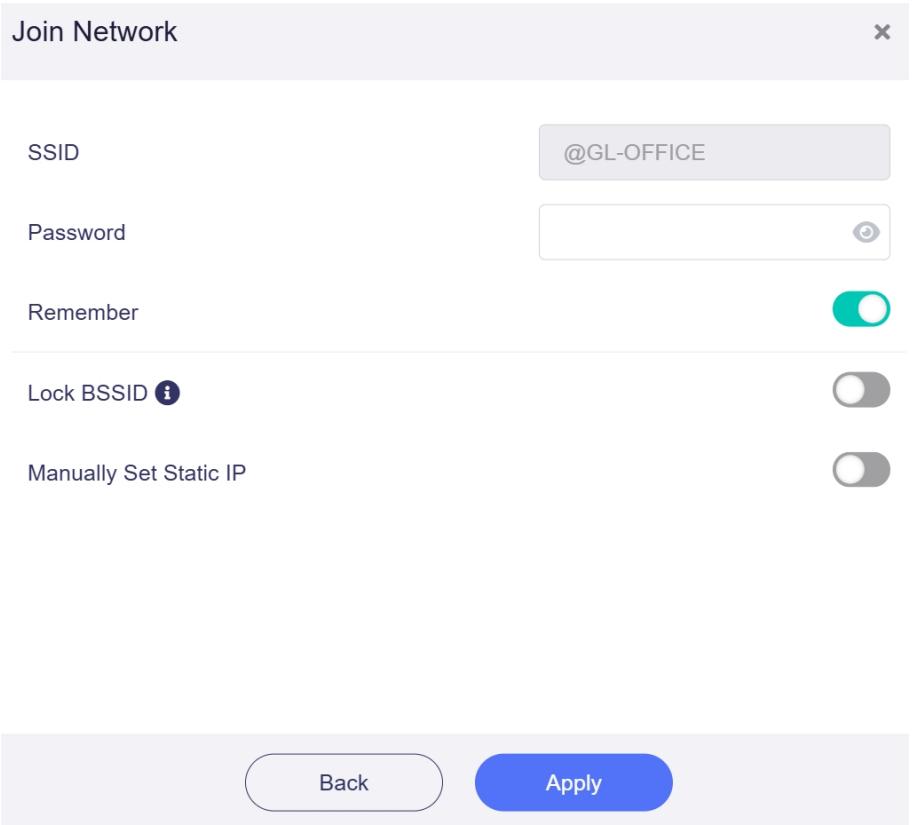
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **INTERNET** > **Repeater**. Klicken Sie auf **Connect**.



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

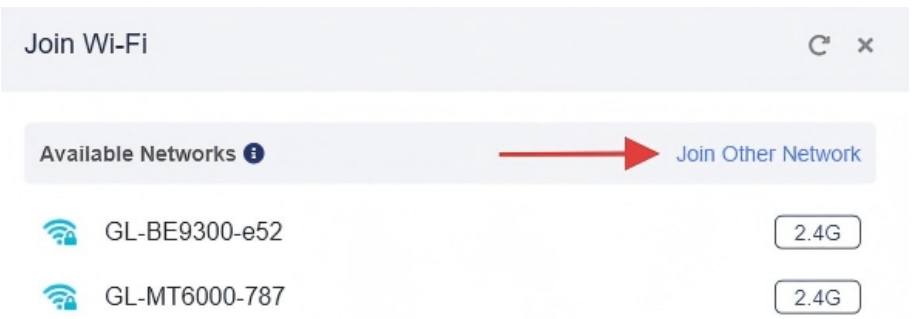


3. Geben Sie das richtige WLAN-Passwort ein und klicken Sie auf **Apply**.

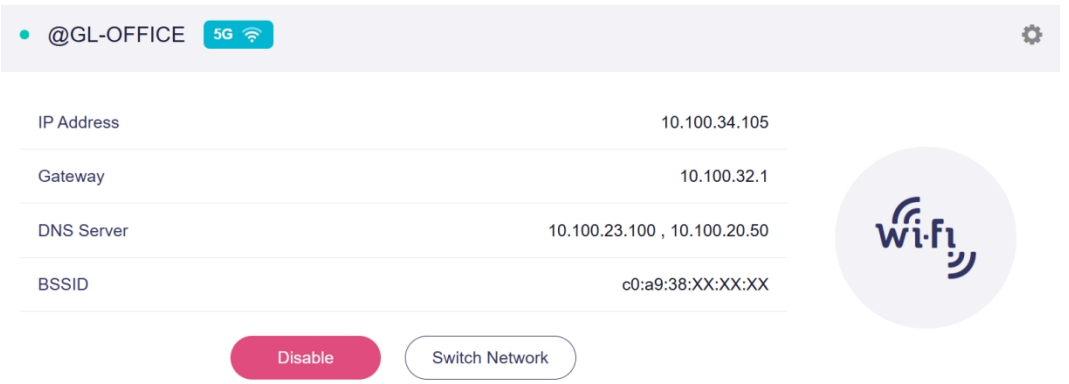


- **Remember**: Aktivieren Sie diese Option, um das aktuell als Repeater genutzte WLAN zu speichern.
- **Lock BSSID**: Wenn diese Option aktiviert ist, verbindet sich der Router ausschließlich mit dem Zugangspunkt (AP) der ausgewählten BSSID, auch wenn andere Zugangspunkte dieselbe SSID verwenden.
-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

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

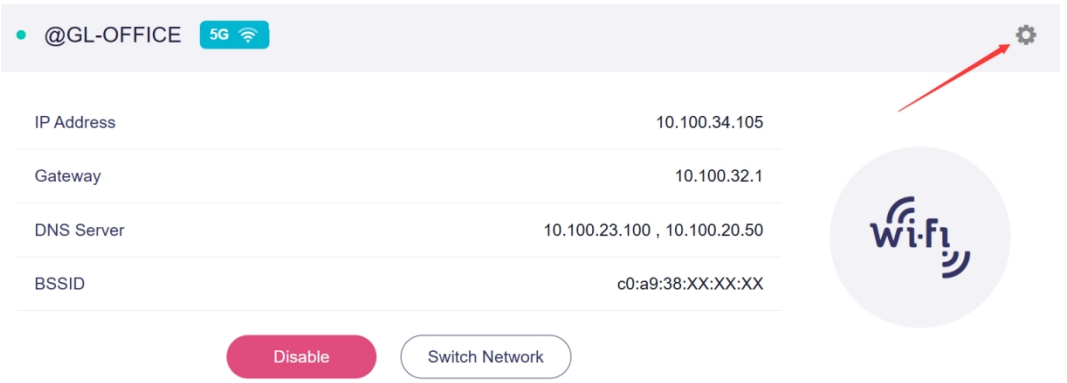


5. Warten Sie etwa eine Minute, bis der Router verbunden ist. Nach erfolgreicher Verbindung erscheint die folgende Ansicht.

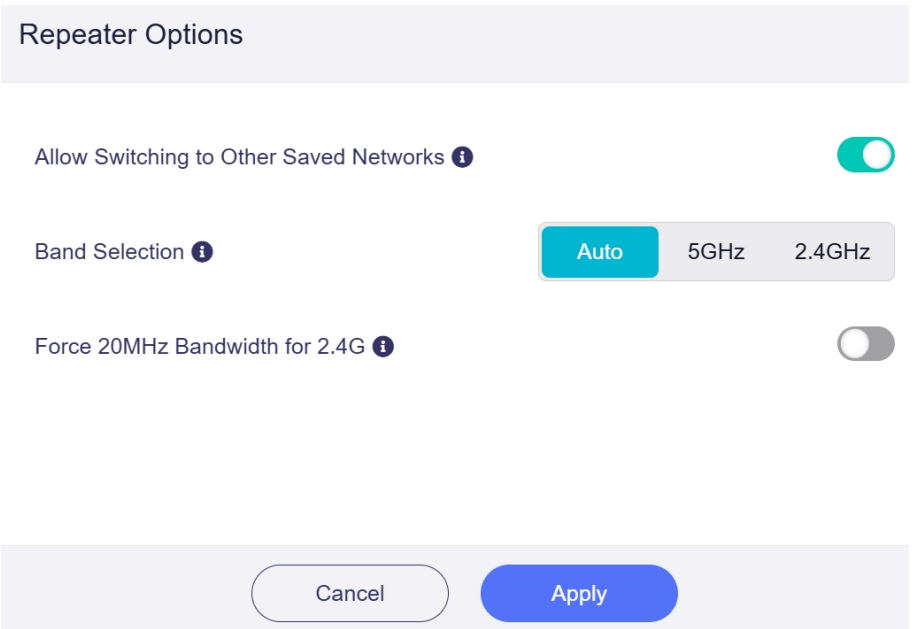


4.2.2 Repeater-Optionen

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



Die Ansicht kann je nach Firmwareversion abweichen.



- **Allow Switching to Other Saved Networks**: Wenn diese Option aktiviert ist, verbindet sich der Router automatisch mit anderen gespeicherten Netzwerken, sobald er keine Verbindung zum aktuellen WLAN herstellen kann.
- **Band Selection**: Wenn Sie ein Frequenzband manuell auswählen, sucht der Router nicht nach WLANs in anderen Frequenzbändern und stellt auch keine Verbindung zu ihnen her.
- **Force 20MHz Bandwidth for 2.4G**: Diese Option verbessert die Verbindungsstabilität, indem sie die Übertragungsrate reduziert.
  Hinweis: Dies funktioniert nur bei einer Repeater-Verbindung mit einem 2,4-GHz-WLAN.

Kapitel 5

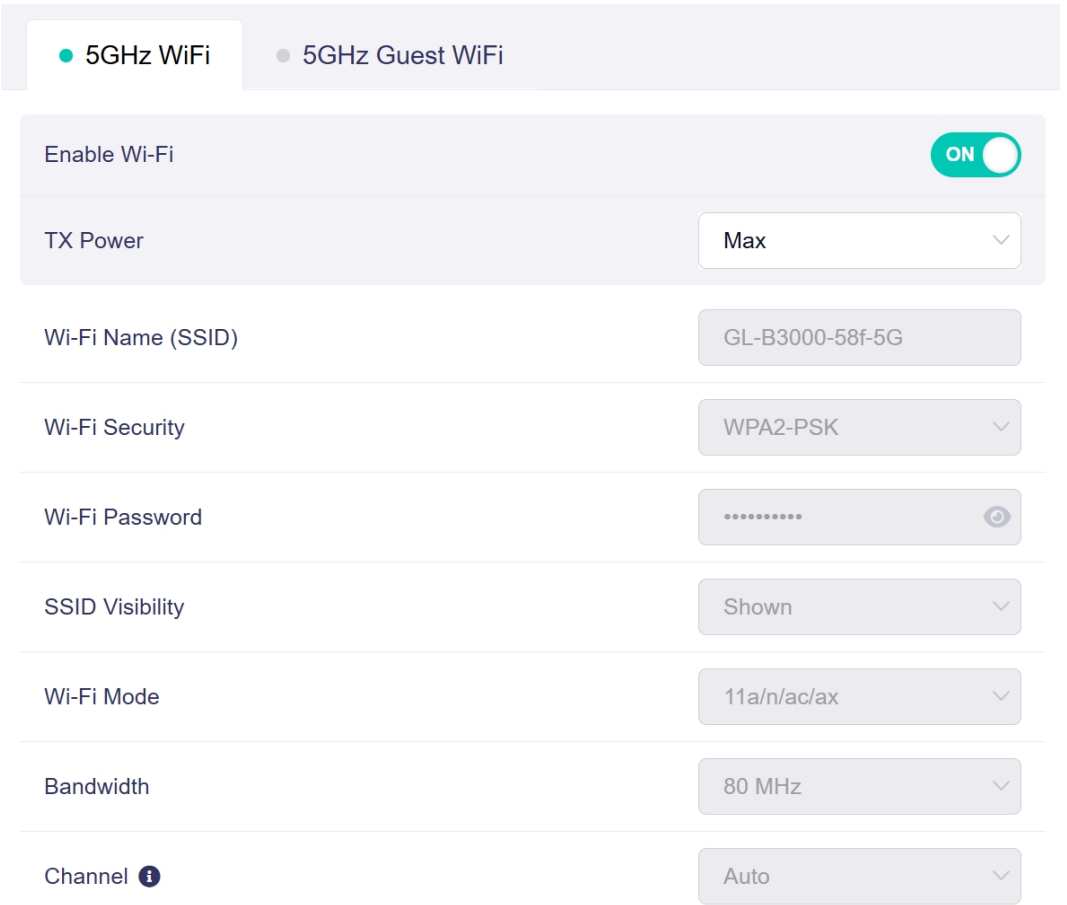
WLAN

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

Melden Sie sich an der Weboberfläche an und öffnen Sie **WIRELESS**.
Die WLAN-Seite zeigt die Einstellungen für das 5-GHz- und das 2,4-GHz-WLAN des Routers. Beide Frequenzbänder sind jeweils in ein Hauptnetzwerk und ein Gastnetzwerk unterteilt und lassen sich flexibel verwalten.

5.1 5-GHz-WLAN

Für das 5-GHz-Hauptnetzwerk können Sie das WLAN ein- und ausschalten sowie Sendeleistung, WLAN-Namen (SSID), Sicherheitsverfahren, Passwort, Sichtbarkeit der SSID, Modus, Bandbreite und Kanal festlegen.

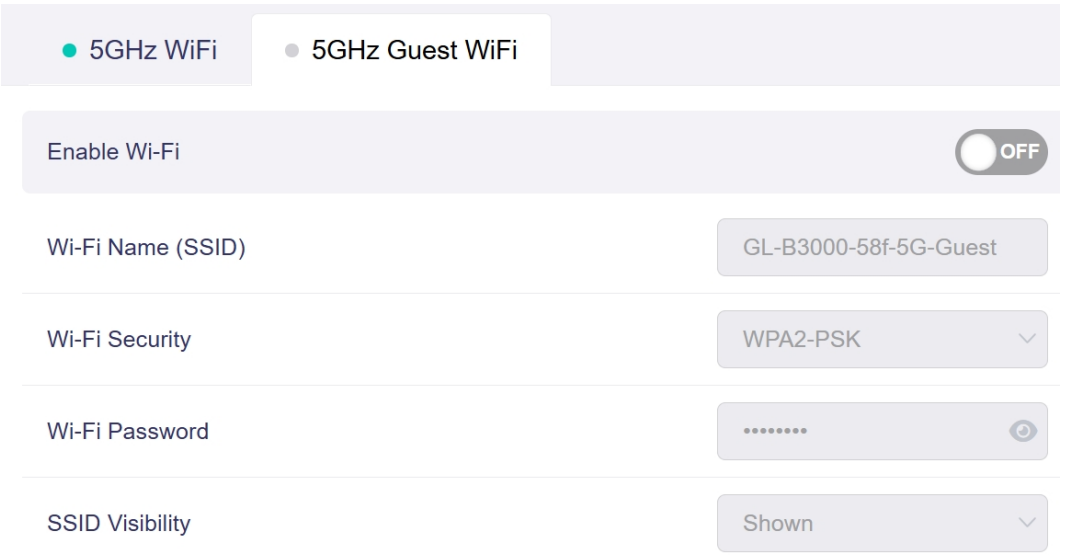


Hinweis:

1. Die Einstellungen **Bandwidth** und **Channel** lassen sich nicht ändern, wenn der Router als Repeater eingerichtet ist, da sie vom übergeordneten WLAN übernommen werden.
2. Wenn **Channel** auf **Auto** eingestellt ist, wechselt das WLAN des Routers nicht automatisch auf einen DFS-Kanal.

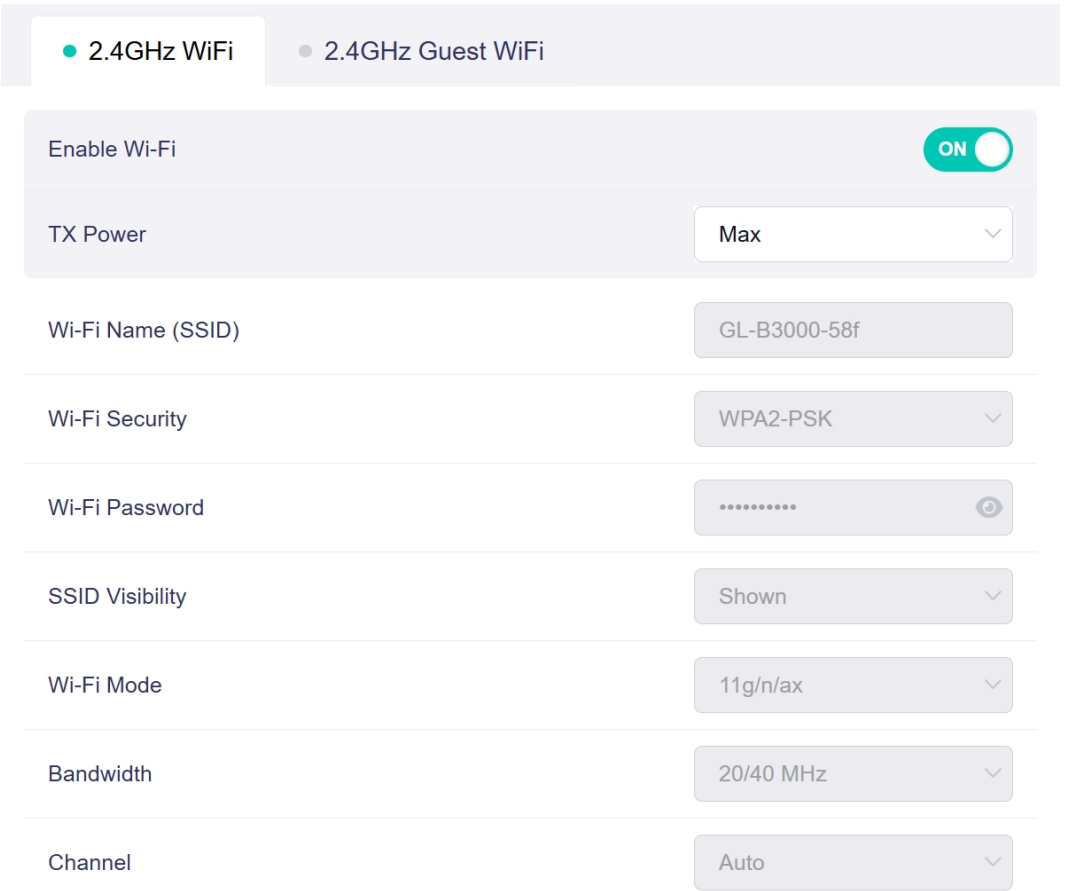
3. Wenn **Bandwidth** auf **160 MHz** eingestellt ist (nur bei einigen Modellen verfügbar), verwendet das WLAN immer einen DFS-Kanal, auch wenn Sie einen Kanal ohne DFS oder Auto auswählen.

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



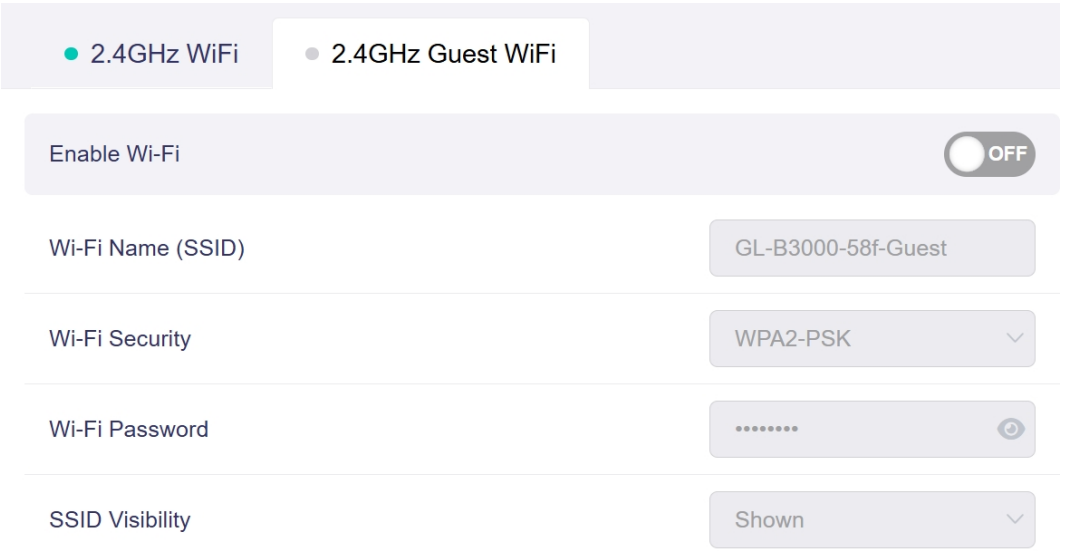
5.2 2,4-GHz-WLAN

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



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

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


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
OFF
Wi-Fi Name (SSID)
GL-B3000-58f-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
SSID Visibility
Shown

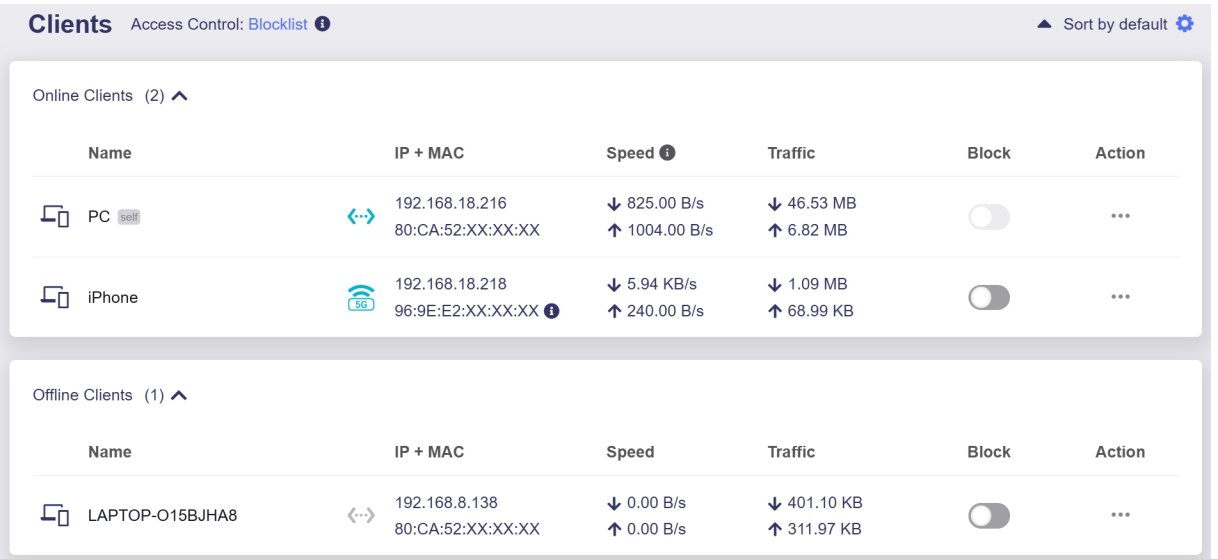
Kapitel 6

Verbundene Geräte

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

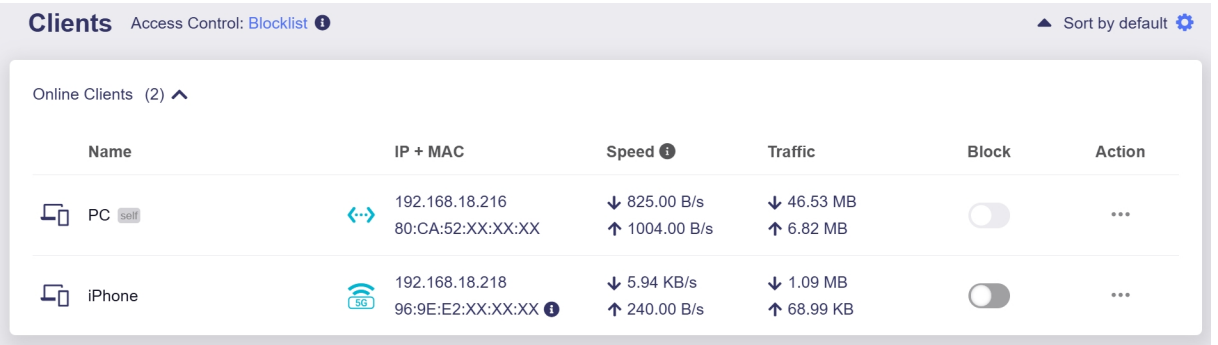
Melden Sie sich an der Weboberfläche an und öffnen Sie **CLIENTS**.

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



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

6.1 Gerätedetails



1. **Gerätename**

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

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

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



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

3. **Geschwindigkeit**

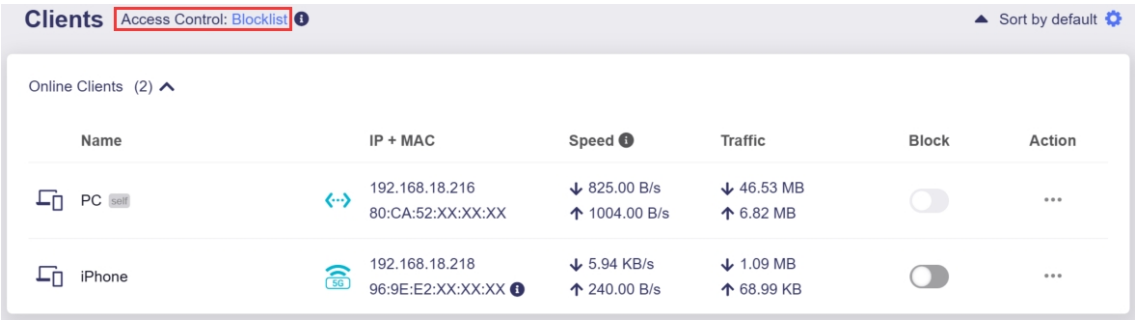
   Die dritte Spalte zeigt die durchschnittliche Internetgeschwindigkeit des Geräts während der letzten drei Minuten. Die Berechnung beginnt beim Öffnen dieser Seite. Ist die Seite beispielsweise erst seit zehn Sekunden geöffnet, basiert der Durchschnitt nur auf den Daten dieser zehn Sekunden.

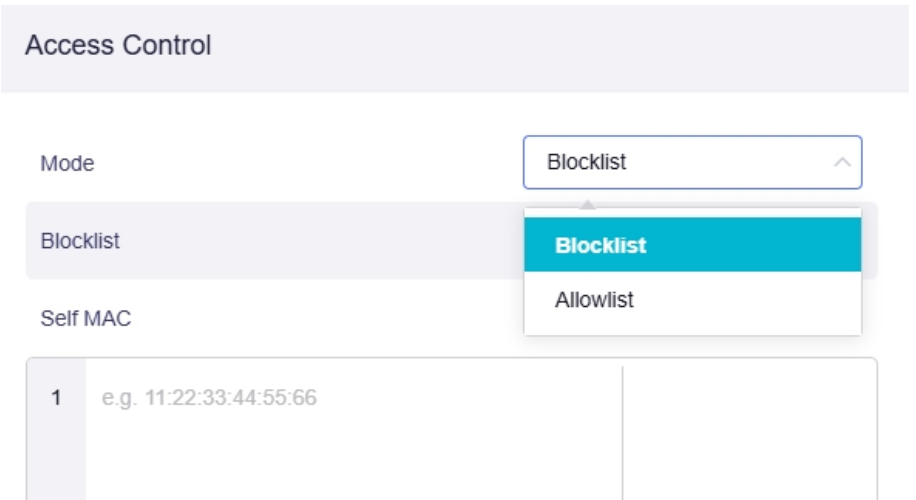
4. **Datenverkehr**: Die vierte Spalte zeigt das übertragene Internetdatenvolumen des Geräts an.

5. **Sperrliste**

   In der fünften Spalte können Sie einzelne verbundene Geräte mit einem Klick sperren.

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



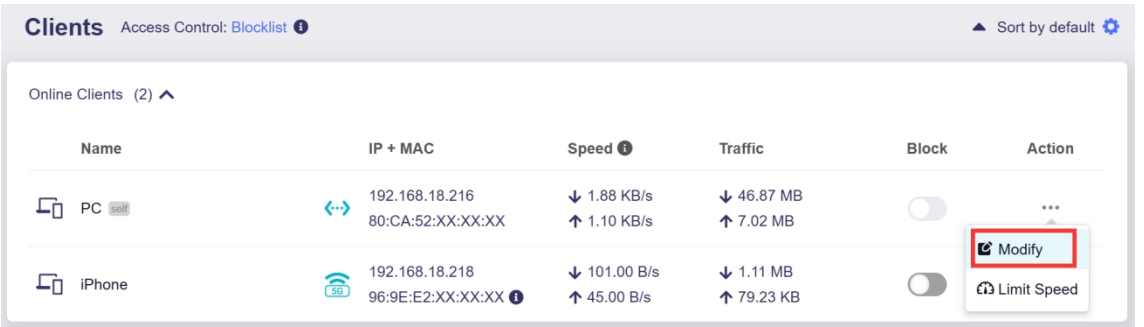


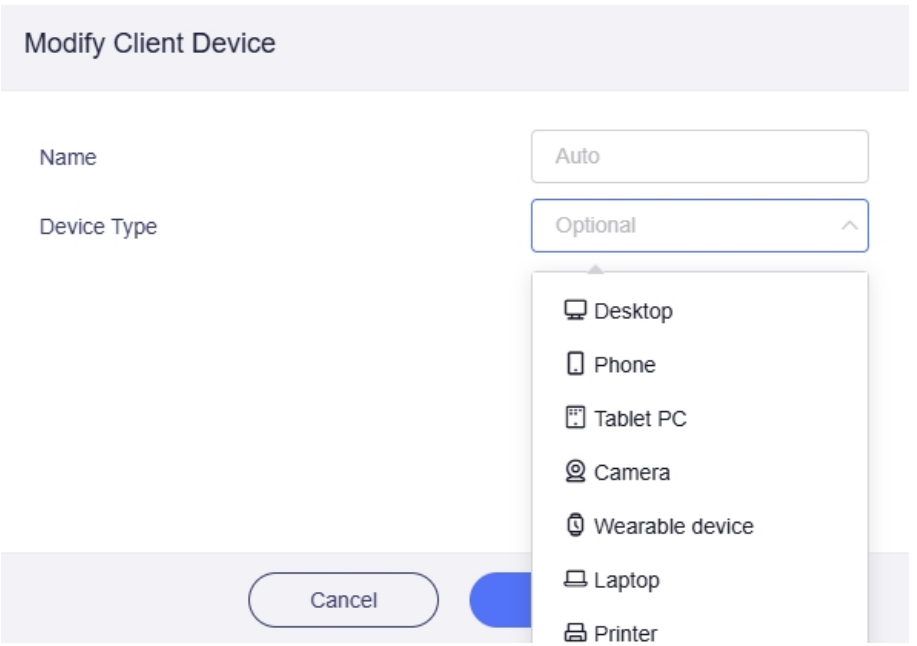
- **Blacklist**: Geräte, deren MAC-Adressen auf der Sperrliste stehen, dürfen sich nicht mit diesem Router verbinden. Die Sperre basiert auf der MAC-Adresse des Geräts. Verwendet ein gesperrtes Gerät beim nächsten Verbindungsversuch eine andere MAC-Adresse, kann es sich dennoch verbinden.
- **Allowlist**: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

6.2 Aktionen

1. **Gerät bearbeiten**

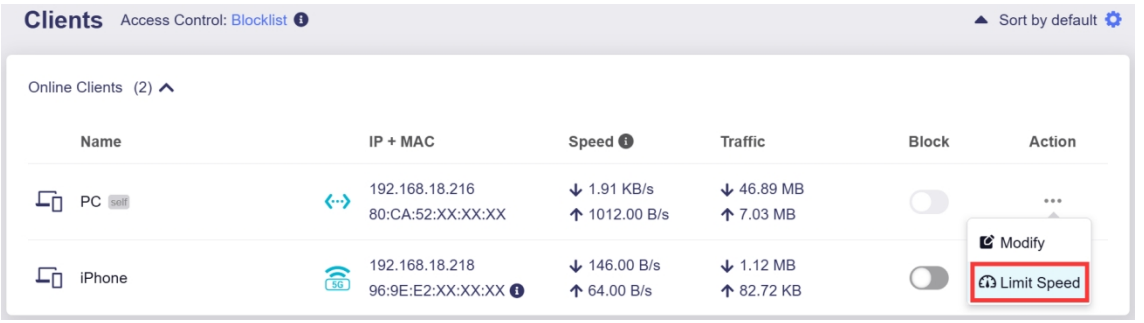
   Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Modify**, um den Gerätenamen und -typ zu ändern.



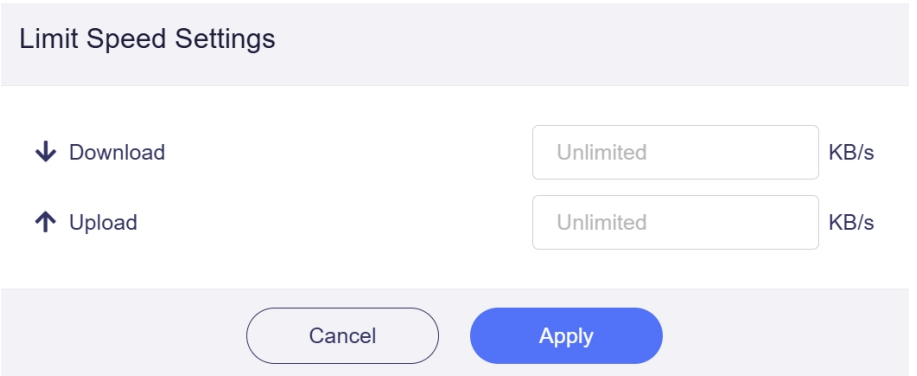


2. **Geschwindigkeit begrenzen**

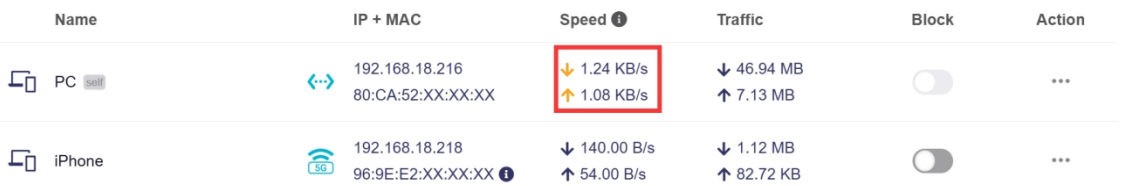
Klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Limit Speed**.



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

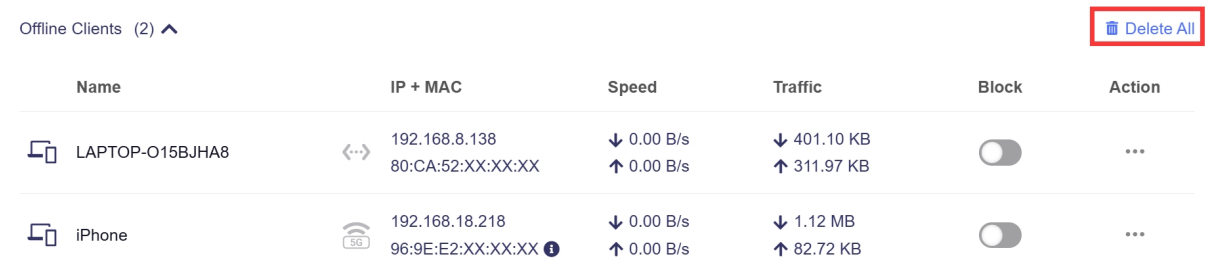


Bei Geräten mit aktivierter Geschwindigkeitsbegrenzung werden die Pfeile für die Upload- und Downloadgeschwindigkeit gelb angezeigt.

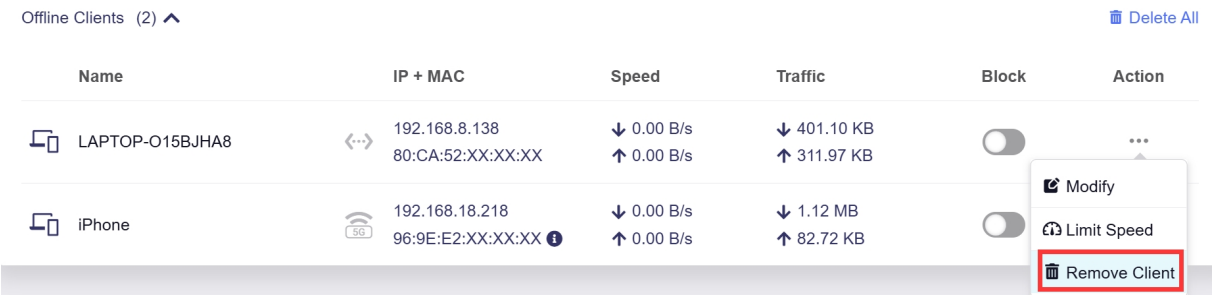


6.3 Geräte entfernen

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

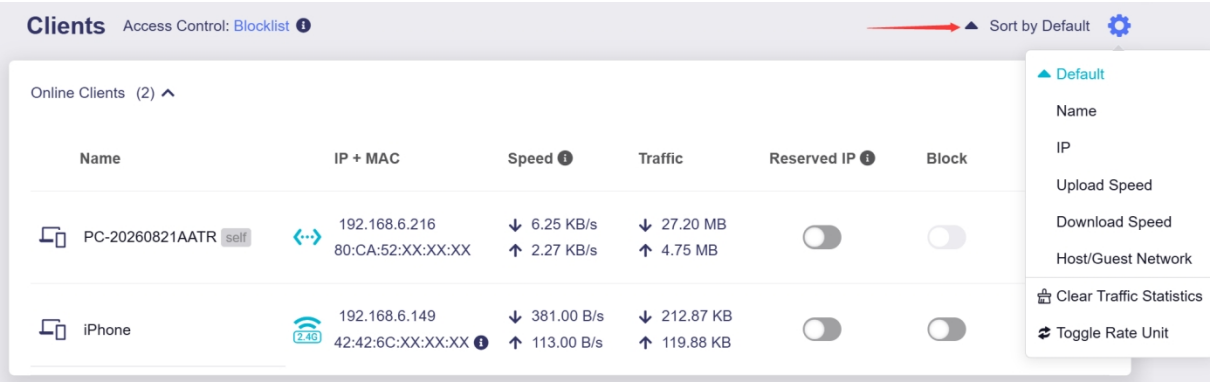


Um ein einzelnes Gerät zu entfernen, klicken Sie in der Spalte **Action** auf das Dreipunktsymbol und wählen Sie im Menü **Remove Client**.



6.4 Sortierung

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



Standardmäßig gilt folgende Reihenfolge:

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

Neben der Sortierung bietet das Auswahlmenü folgende Funktionen:

- **Clear Traffic Statistics**: Setzt die Datenverkehrsstatistiken aller verbundenen Geräte mit einem Klick zurück. Die Werte in der Statistikspalte werden auf null gesetzt und anschließend neu erfasst.



- **Toggle Rate Unit**: Wechselt die Einheit in der Geschwindigkeitsspalte zwischen **KB/s** und **Kbps**.

Kapitel 7

VPN kennenlernen

Dieses Kapitel erläutert die Grundlagen von VPN und typische Einsatzmöglichkeiten.

7.1 Einführung

VPN

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

VPN-Router

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

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

OpenVPN

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

WireGuard

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

7.2 Einsatzmöglichkeiten

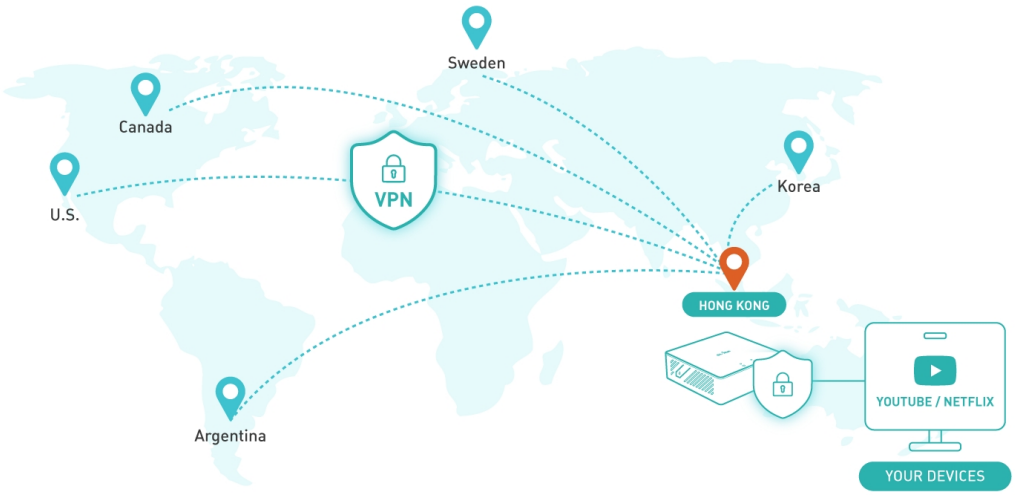
1. **Schutz persönlicher Daten**

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



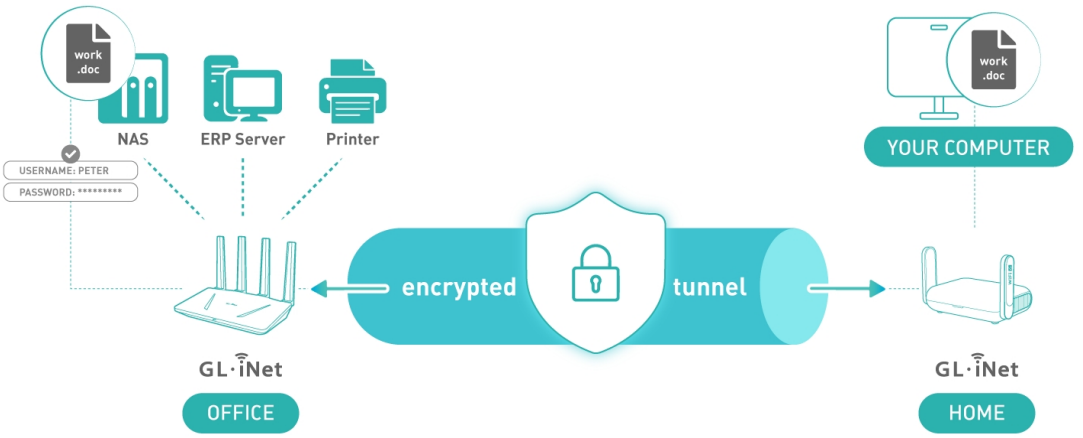
2. **Weltweiter Zugriff ohne Einschränkungen**

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


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

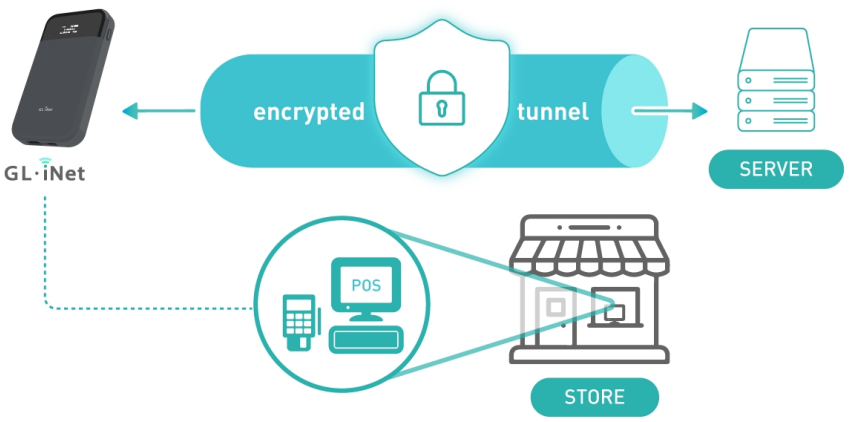
3. **Datensicherheit für kleine Unternehmen**

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



4. **Sichere Zahlungsabwicklung**

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



Kapitel 8

VPN-Dashboard

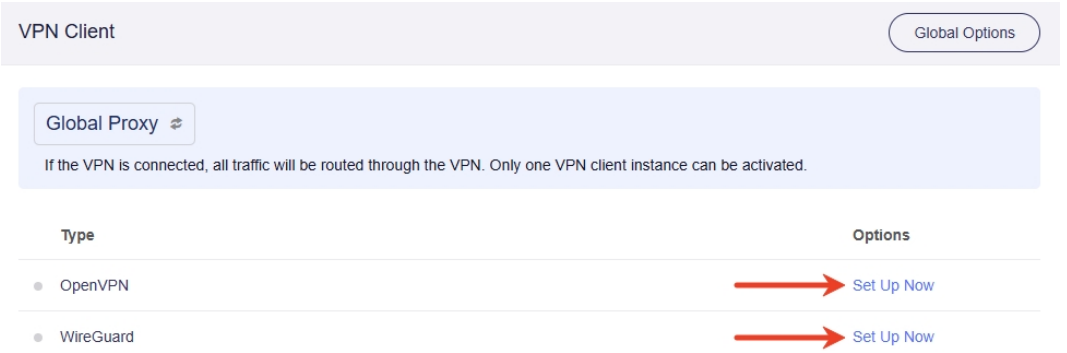
Dieses Kapitel beschreibt die Verwaltung von VPN-Verbindungen über die Weboberfläche.

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

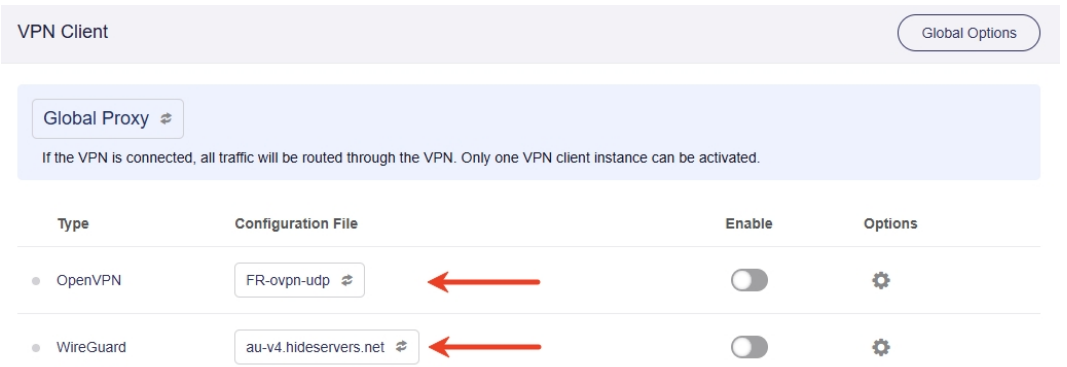
Wenn der Router als aktiver VPN-Client eingerichtet ist, zeigt das VPN-Dashboard Verbindungsdetails wie Serveradresse, Datenverkehrsstatistik, virtuelle Client-IP-Adresse und Verbindungsprotokoll an. Sie können außerdem erweiterte Optionen wie Block non-VPN traffic, Allow Access WAN und Services from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

8.1 VPN-Client

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

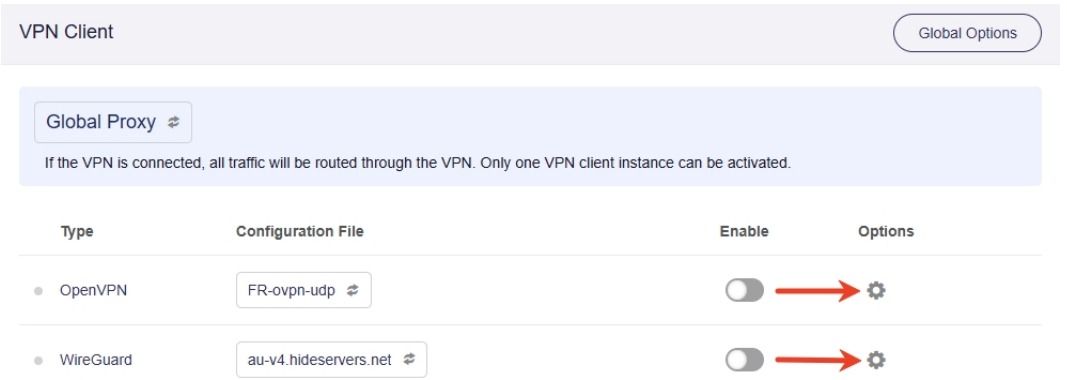


Nach dem Hochladen wird Ihre Konfiguration in der Spalte **Configuration File** angezeigt. Wenn mehrere Konfigurationsdateien vorhanden sind, können Sie über das Auswahlfeld zwischen ihnen wechseln.

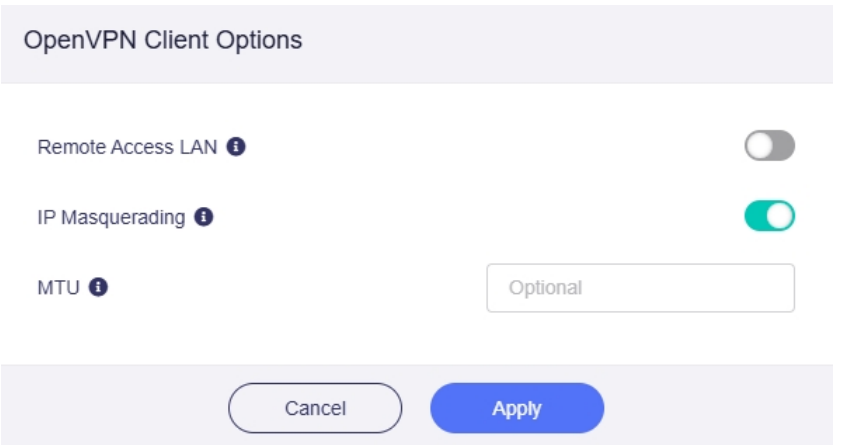


8.1.1 Client-Optionen

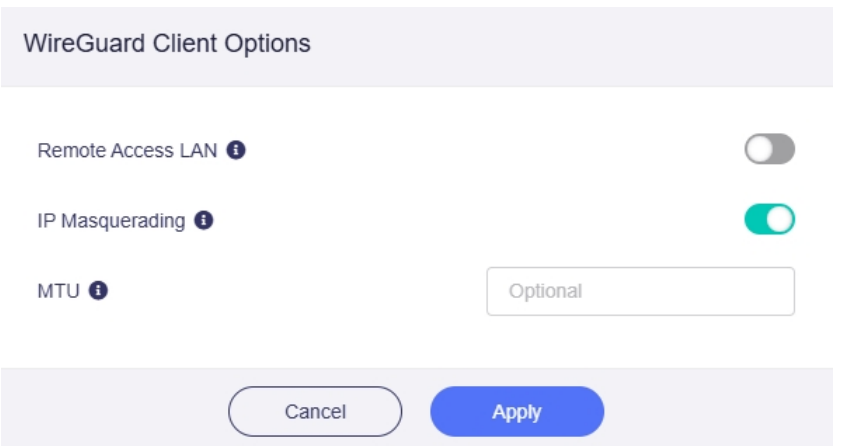
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Clients zu öffnen.



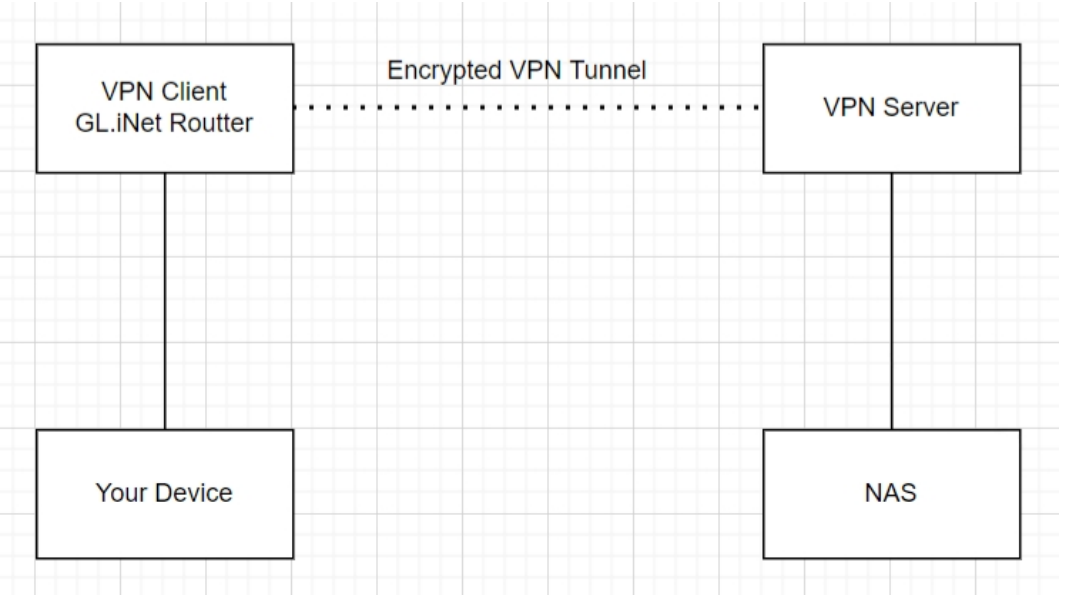
Die Optionen des OpenVPN-Clients werden wie folgt angezeigt.



Die Optionen des WireGuard-Clients werden wie folgt angezeigt.



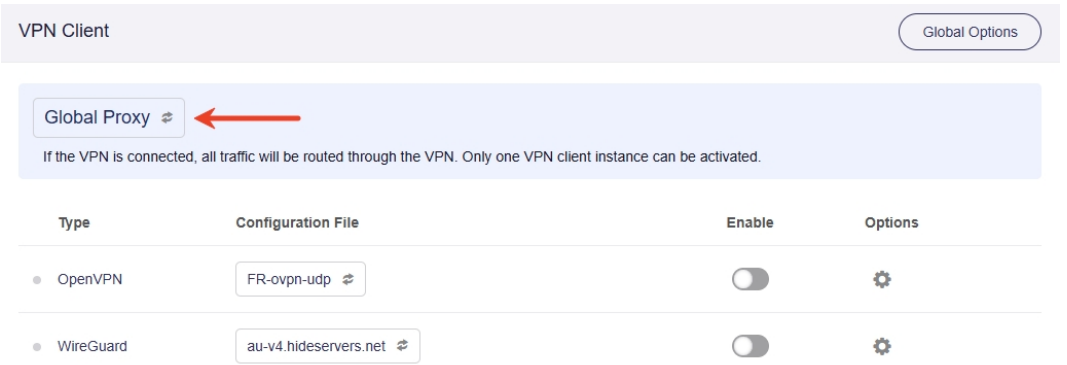
- **Remote Access LAN**: Erlaubt den Fernzugriff über VPN auf diesen Router und seine LAN-Geräte. Der VPN-Server muss eine Route zum LAN-Subnetz dieses Routers bekannt geben.
  Im folgenden Beispiel arbeitet der GL.iNet-Router als VPN-Client und ist über einen VPN-Tunnel mit einem VPN-Server verbunden.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



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

8.1.2 Richtlinienmodus

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



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

1. **Globaler Proxy**

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

2. **Richtlinienmodus**

   Dieser Modus bietet drei Arten von Richtlinien.

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

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

   - **Nach Endgerät**

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

   - **Nach VLAN**

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

3. **Routenmodus**

   - **Automatische Erkennung**

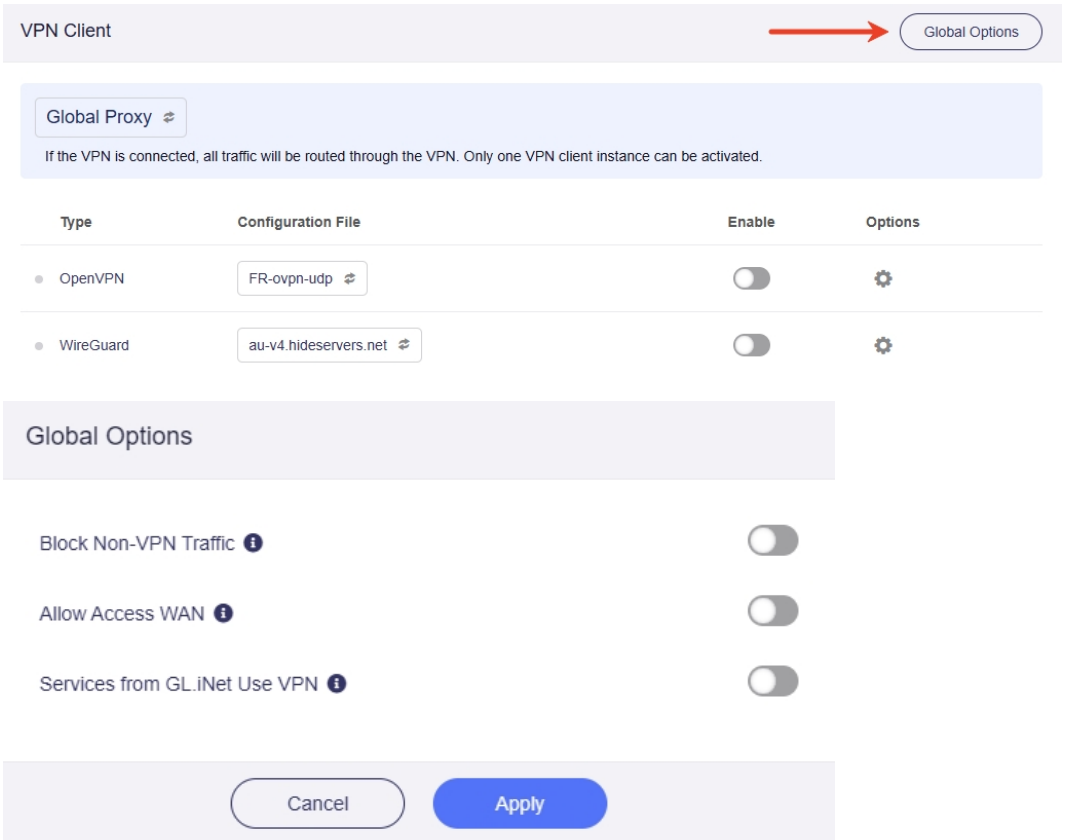
     Verwendet die Routingregeln aus der jeweiligen VPN-Client-Konfigurationsdatei oder die vom VPN-Server übermittelten Regeln.

   - **Eigene Routingregeln**

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

8.1.3 Globale Optionen

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



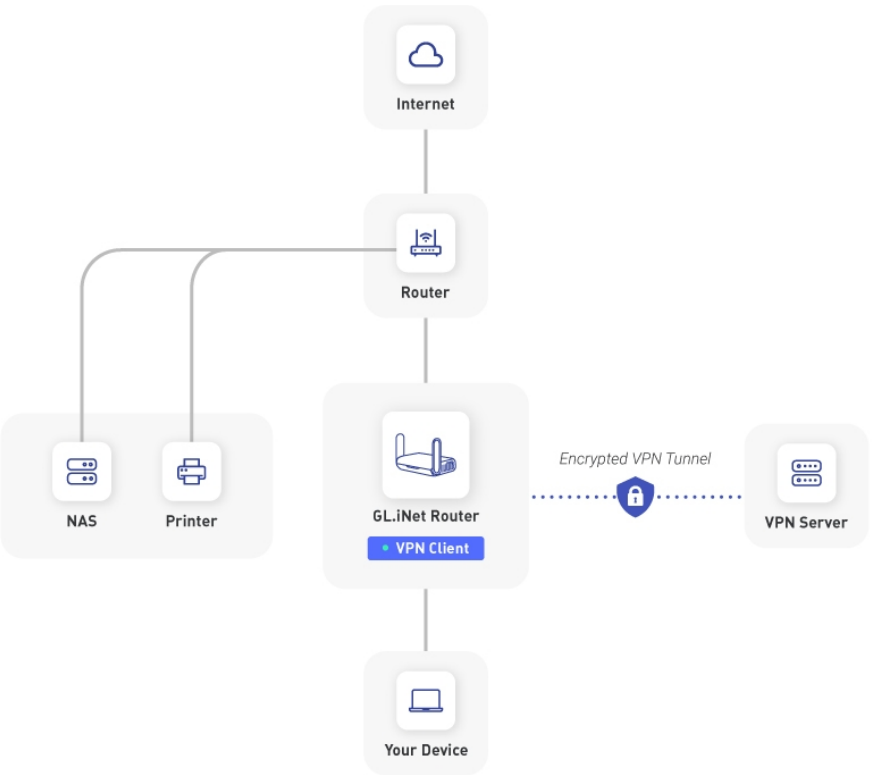
- **Block Non-VPN Traffic**: Erzwingt, dass sämtlicher Internetdatenverkehr ausschließlich durch den VPN-Tunnel geleitet wird. Andere Schnittstellen wie die WAN-Verbindung zum lokalen Internetanbieter können nicht verwendet werden. Bei einem unerwarteten Abbruch der VPN-Verbindung wird der gesamte Internetdatenverkehr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

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

  a. DNS-Lecks
  b. IPv6-Lecks

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

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



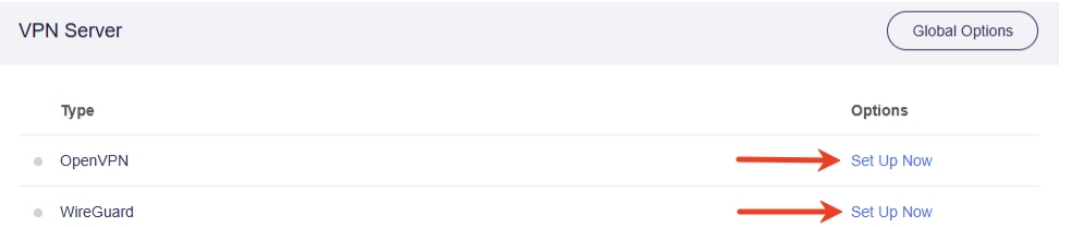
Wie im obigen Diagramm dargestellt, können Ihre lokalen Geräte nach Aktivierung dieser Funktion auf Geräte im vorgeschalteten Subnetz zugreifen, etwa Drucker und NAS.

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

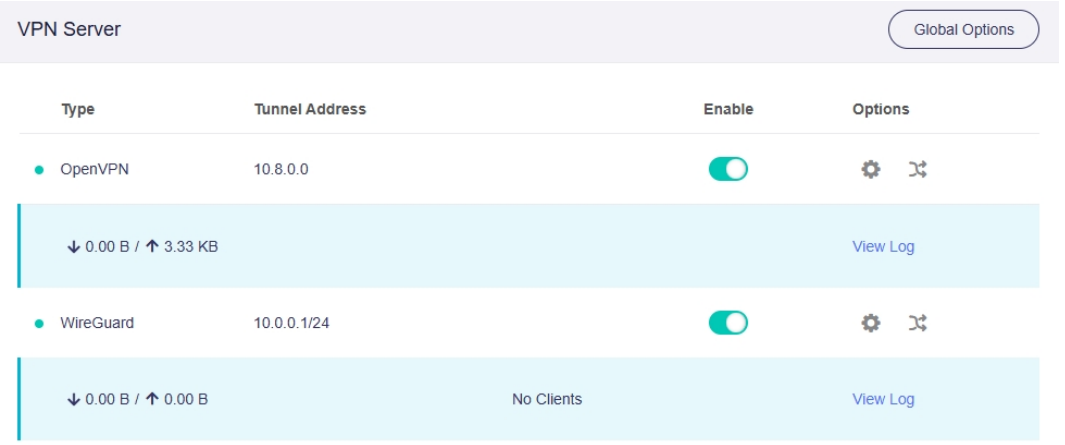
- **Services From GL.iNet Use VPN**: Leitet die Datenpakete von GoodCloud, DDNS und rtty durch die VPN-Tunnel. Diese Option ist standardmäßig deaktiviert, da diese Dienste für den ordnungsgemäßen Betrieb normalerweise die tatsächliche IP-Adresse des Geräts benötigen.

8.2 VPN-Server

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

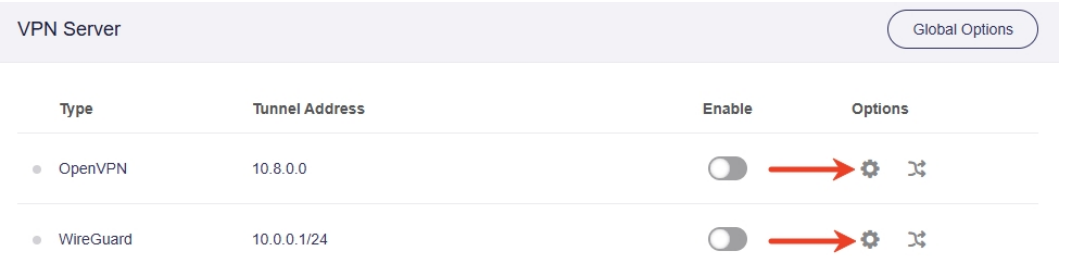


Nach dem Aktivieren des OpenVPN- oder WireGuard-Servers wird dessen Status wie folgt angezeigt.

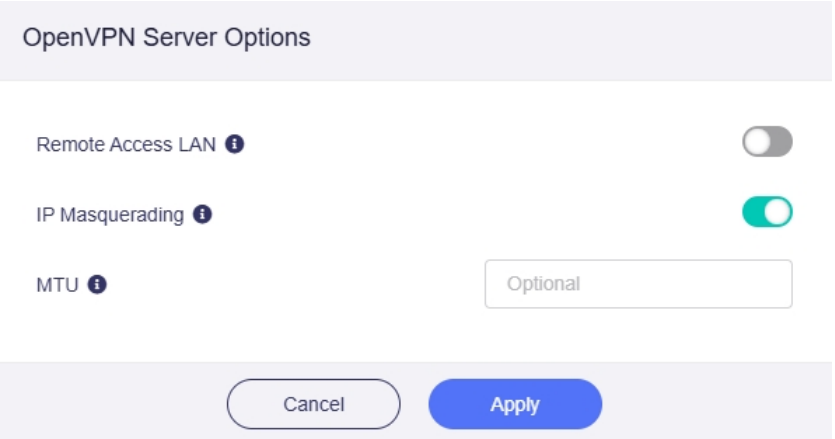


8.2.1 Server-Optionen

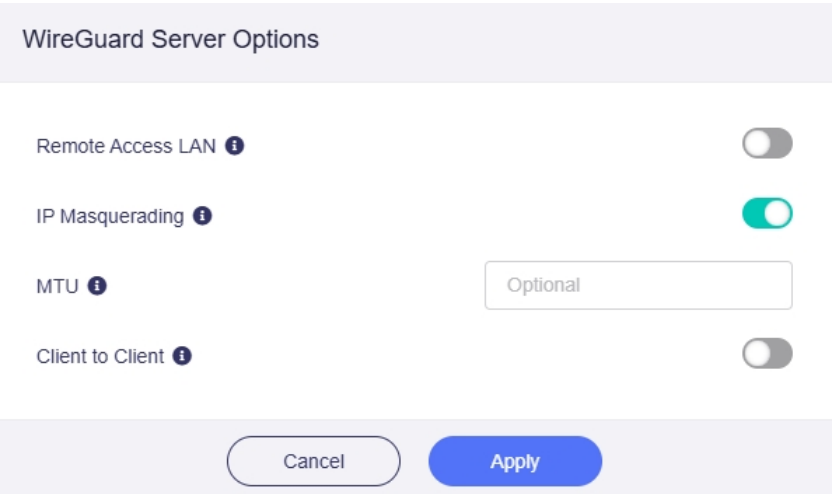
Klicken Sie rechts auf das Zahnradsymbol, um die Optionen des OpenVPN- oder WireGuard-Servers zu öffnen.



Die Optionen des OpenVPN-Servers werden wie folgt angezeigt.



Die Optionen des WireGuard-Servers werden wie folgt angezeigt.

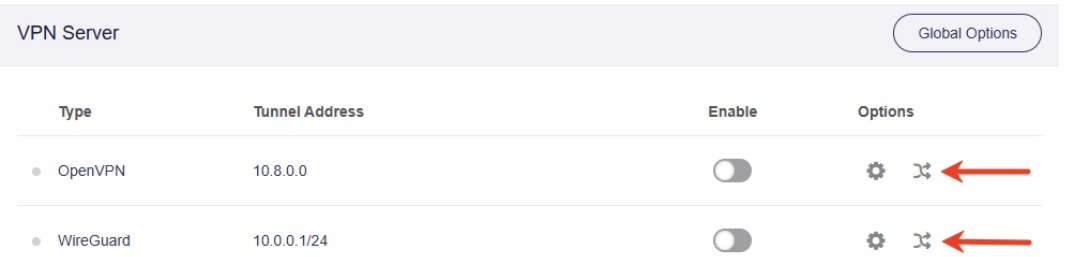


- **Remote Access LAN**: Erlaubt den Zugriff über den VPN-Tunnel auf Ressourcen im LAN-Subnetz des Servers.

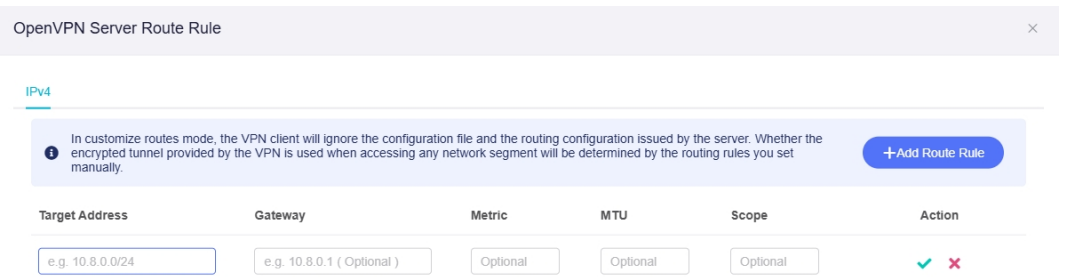
- **IP Masquerading**: Ersetzt die Quell-IP-Adressen der LAN-Geräte durch die VPN-Tunnel-IP-Adresse des Routers. Deaktivieren Sie diese Option nur bei Standortvernetzungen, bei denen die Gegenstelle Ihre LAN-Subnetze kennt.
- **MTU**: Steht für Maximum Transmission Unit, die maximale Paketgröße. Der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

8.2.2 Server-Routingregeln

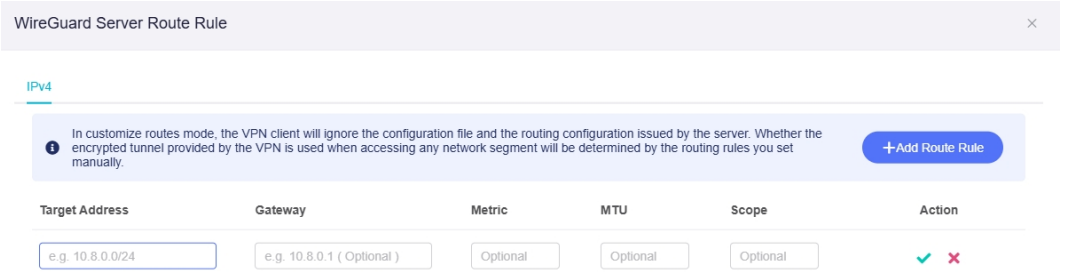
Klicken Sie rechts auf das Routensymbol, um die Routingregeln für OpenVPN oder WireGuard nach Bedarf anzupassen.



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



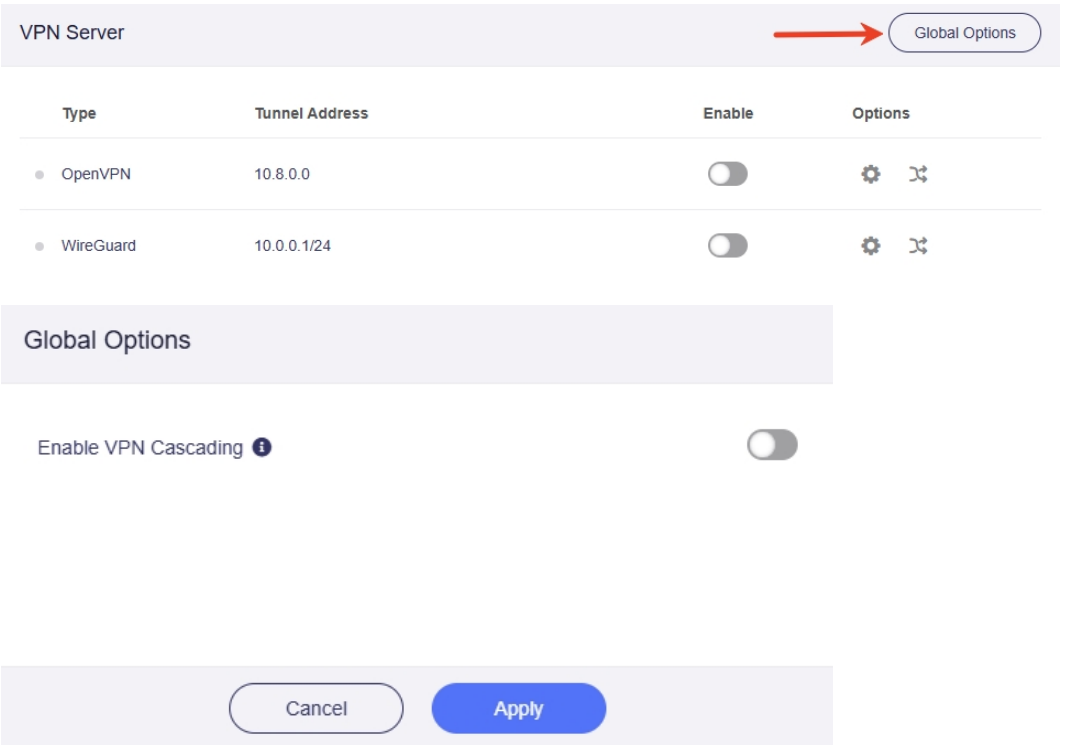
Die WireGuard-Server-Routingregeln werden wie folgt angezeigt. Klicken Sie auf **Add Route Rule**, geben Sie **Target Address** und **Gateway** ein und klicken Sie zum Übernehmen auf das grüne Häkchen.



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

8.2.3 Globale Optionen

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



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

Kapitel 9

VPN-Server einrichten

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

9.1 OpenVPN-Server einrichten

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

9.1.1 Vorbereitung

1. **Öffentliche IP-Adresse sicherstellen**

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

   Alternativen:

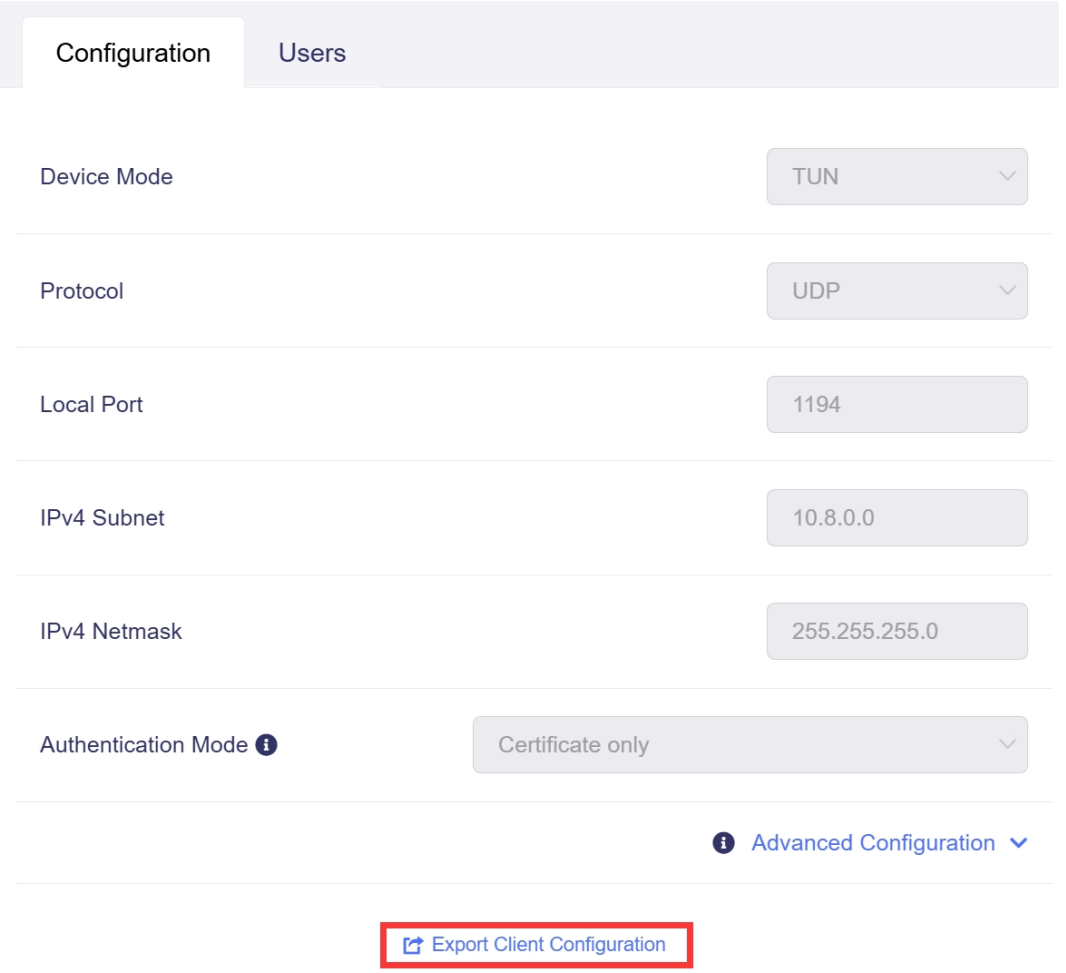
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.

2. **Erforderliche Portweiterleitung prüfen**

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

9.1.2 Einrichtung

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



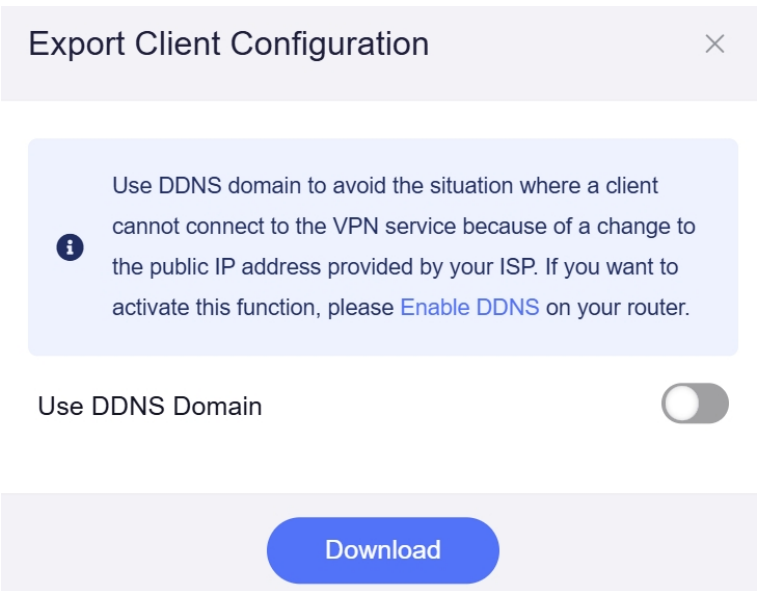
- **Device Mode**: TAP-S2S oder Tun. Die Unterschiede werden hier erläutert.
- **Protocol**: UDP oder TCP. Die Unterschiede werden hier erläutert.
- **Authentication Mode**: Legt fest, wie sich der Client beim Verbinden mit dem Server authentifiziert. Es gibt drei Optionen:
  - **Certificate Only**: Der Router erzeugt automatisch die Zertifikate und Schlüssel für Server und Client und bettet sie in die Konfigurationsdatei ein. Nach dem

Hochladen der Konfiguration auf den Client sind keine weiteren Zugangsdaten erforderlich.

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

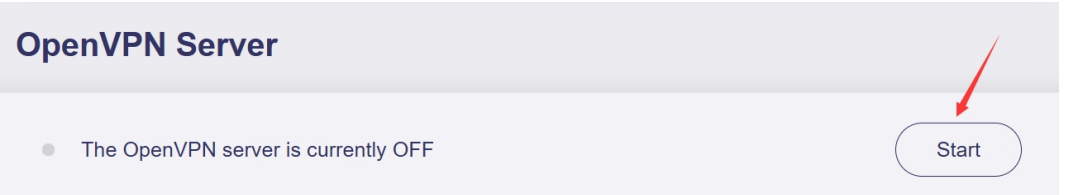
- **Advanced Configuration**: Hier können Sie bei Bedarf weitere Servereinstellungen anpassen.

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

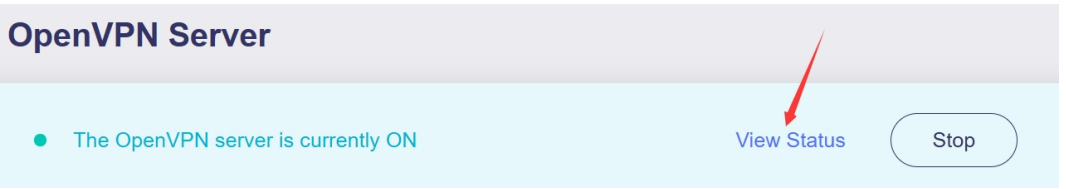


Tipp: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Sie können dann den DDNS-Domainnamen als Serveradresse verwenden.

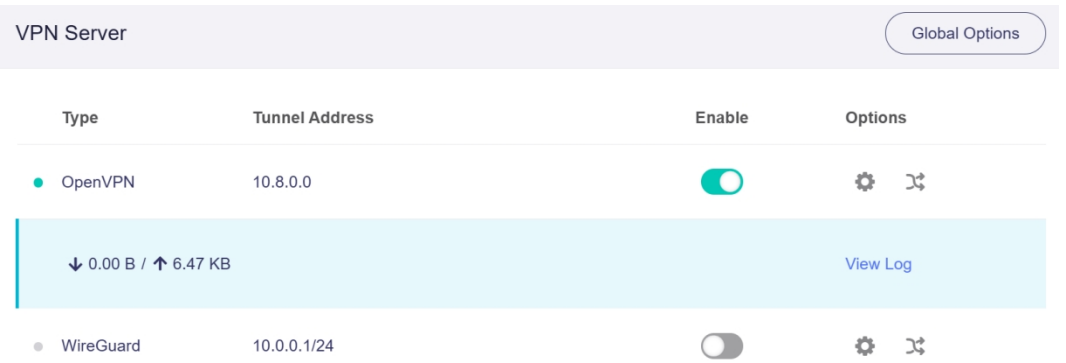
4. OpenVPN-Server starten.
   Klicken Sie auf der Seite **OpenVPN Server** oben rechts auf **Start**, um den Server zu starten.



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



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



9.1.3 Fehlerbehebung

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

- Der VPN-Server hat keine öffentliche IP-Adresse. Hinweise zur Fehlerbehebung finden Sie hier.

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

9.2 WireGuard-Server einrichten

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

9.2.1 Vorbereitung

1. **Öffentliche IP-Adresse sicherstellen**

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

   Alternativen:

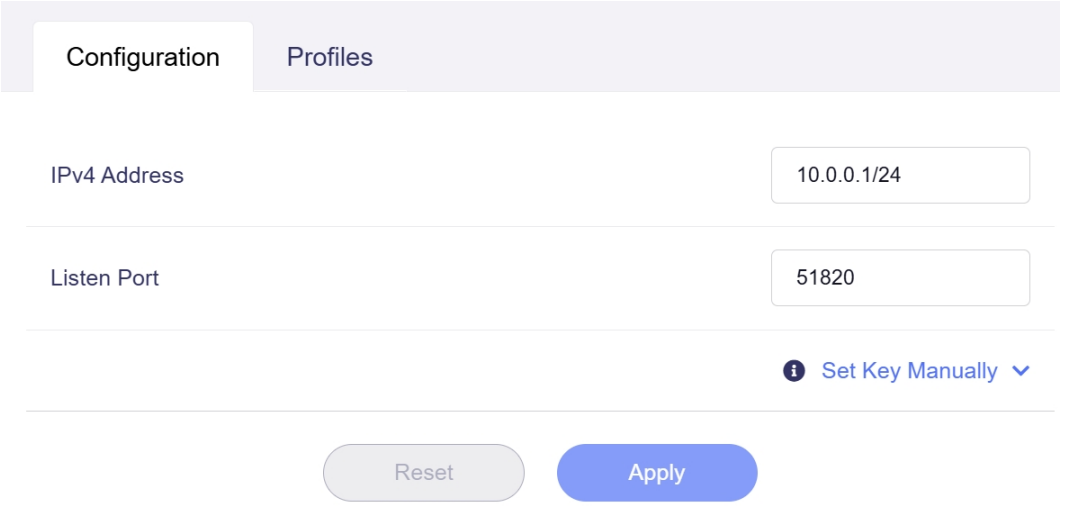
   - Wenn Ihrem GL.iNet-Router ein Hauptrouter vorgeschaltet ist, melden Sie sich an diesem an und prüfen Sie, ob er eine öffentliche IP-Adresse vom Internetanbieter erhalten hat.
   - Bitten Sie Ihren Internetanbieter um eine öffentliche IP-Adresse. Dafür können zusätzliche Gebühren anfallen.

2. **Erforderliche Portweiterleitung prüfen**

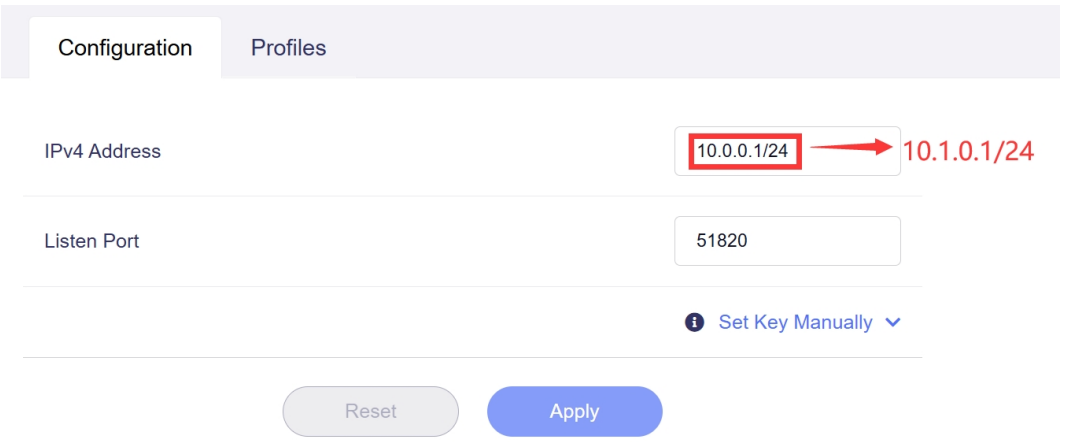
   - Wenn Ihr GL.iNet-Router der Hauptrouter Ihres Netzwerks ist, benötigen Sie keine Portweiterleitung. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn bereits ein Hauptrouter vorhanden ist und Ihr GL.iNet-Router als nachgeschalteter Router arbeitet, müssen Sie auf dem Hauptrouter eine Portweiterleitung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

9.2.2 Einrichtung

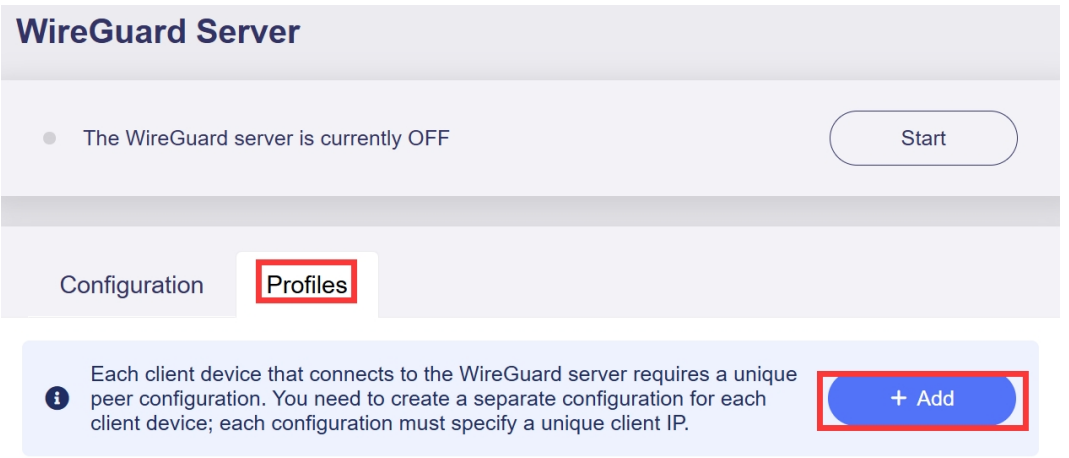
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **WireGuard Server** und klicken Sie auf **Generate Configuration** (nur bei der Ersteinrichtung des VPN-Servers).
2. Konfiguration übernehmen.
   Die Standardkonfiguration eignet sich für die meisten Fälle. Die IPv4-Adresse müssen Sie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



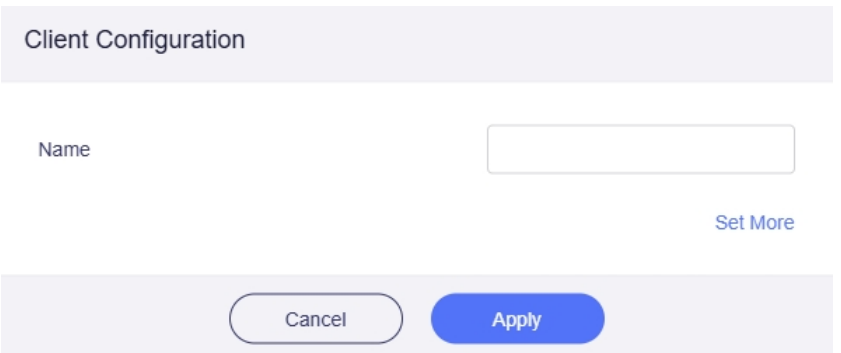
   Bei einem solchen Adresskonflikt wählen Sie eine andere IPv4-Adresse, etwa **10.1.0.1/24**, und klicken Sie auf **Apply**. Achten Sie darauf, die CIDR-Angabe „/24“ beizubehalten, um Verbindungsprobleme zu vermeiden.



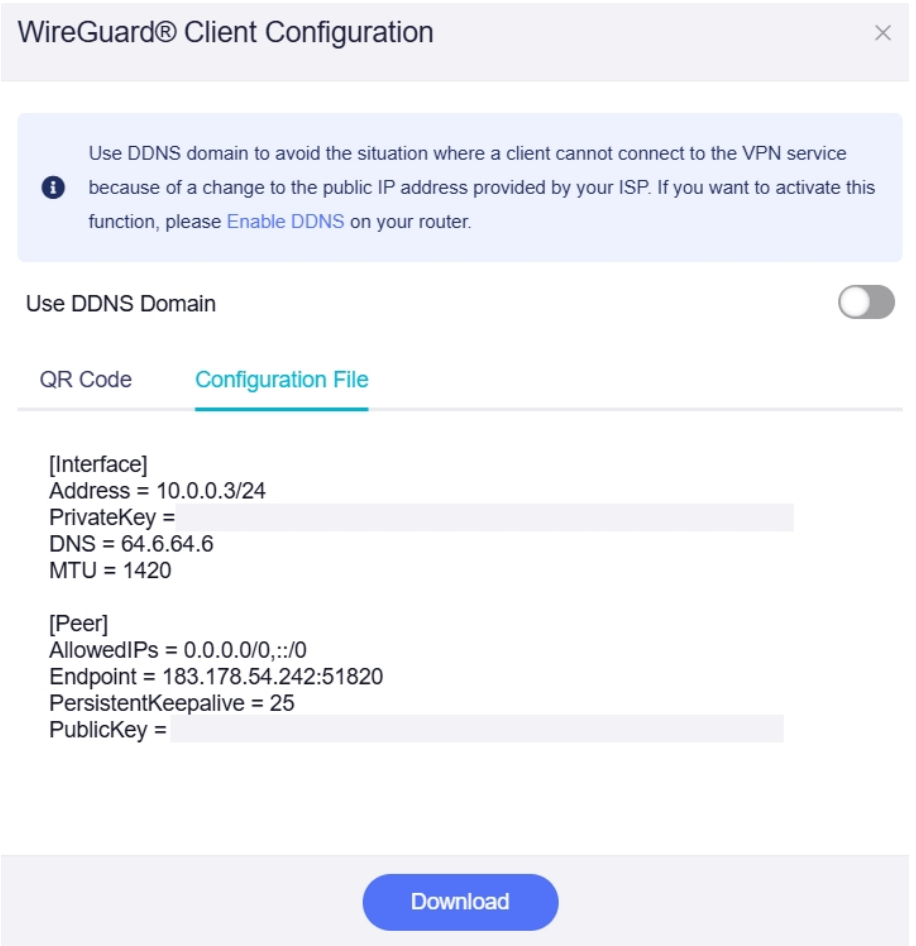
3. Profil hinzufügen.
   Wechseln Sie zur Registerkarte **Profiles** und klicken Sie auf **Add**, um ein Profil für Ihr Gerät zu erzeugen.



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

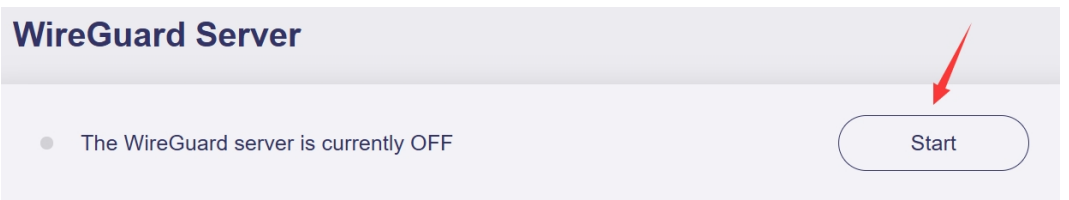


4. Konfiguration herunterladen.
   Nach dem Hinzufügen eines Profils stellt der Router die Konfiguration in drei Formen bereit: als QR-Code, als Klartext und als .conf-Datei. Wählen Sie die gewünschte Form aus.
   - **QR-Code**: Geeignet für Geräte wie Smartphones, Tablets oder Laptops mit installierter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

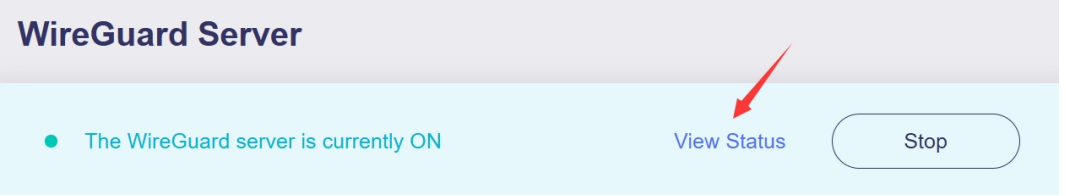


Tipp: Wenn sich Ihre öffentliche IP-Adresse häufig ändert, öffnen Sie **APPLICATIONS** > **Dynamic DNS** und aktivieren Sie DDNS. Sie können dann den DDNS-Domainnamen als Serveradresse verwenden.

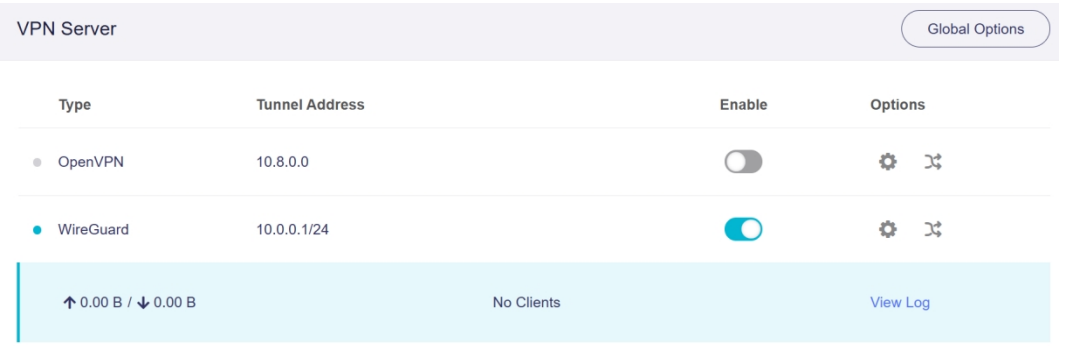
5. WireGuard-Server starten.
   Klicken Sie auf der Seite **WireGuard Server** oben rechts auf **Start**, um den Server zu starten.



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



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



9.2.3 Fehlerbehebung

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

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

Kapitel 10

VPN-Client einrichten

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

10.1 OpenVPN-Client einrichten

10.1.1 Vorbereitung

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

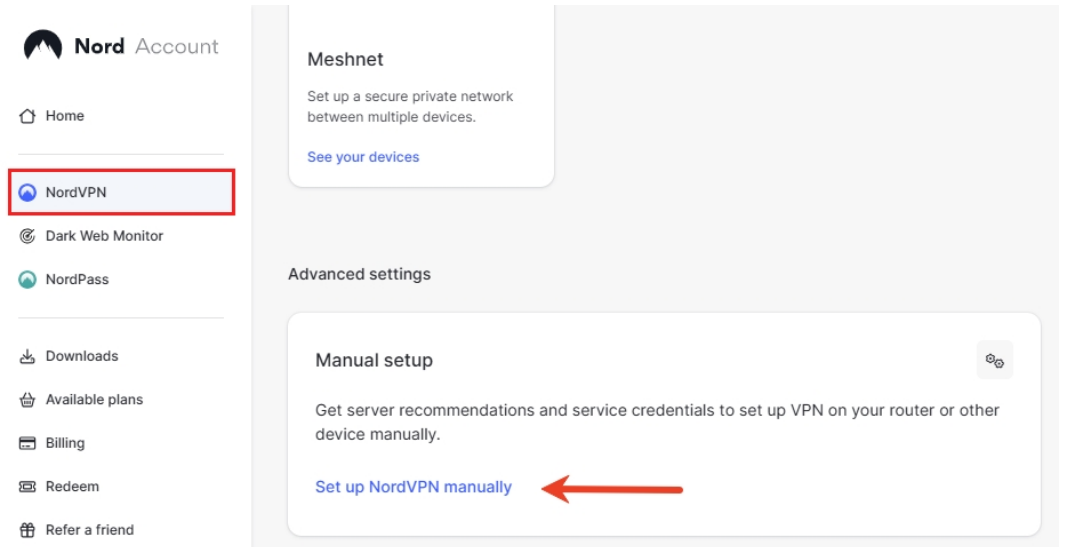
Rufen Sie anschließend die offizielle Webseite Ihres VPN-Anbieters auf und beschaffen Sie die Dienstzugangsdaten oder eine Konfigurationsdatei. Falls Sie nicht wissen, wie Sie die Datei erhalten, folgen Sie diesem Link oder wenden Sie sich an den Support des Anbieters.

10.1.2 NordVPN einrichten

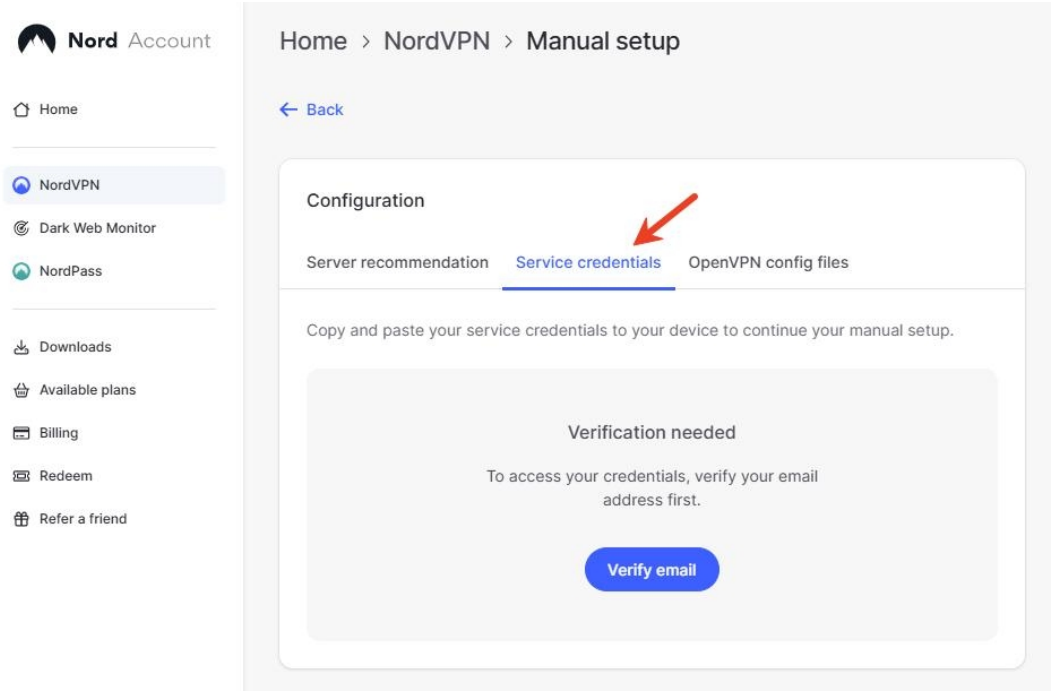
NordVPN ist in die GL.iNet-Weboberfläche integriert. Geben Sie Ihre im NordVPN-Dashboard erhältlichen Zugangsdaten in der Weboberfläche des Routers oder in der GL.iNet-App ein, um die Konfigurationsdateien aller NordVPN-Server abzurufen. Ein manuelles Hochladen der Dateien ist dadurch nicht erforderlich.

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

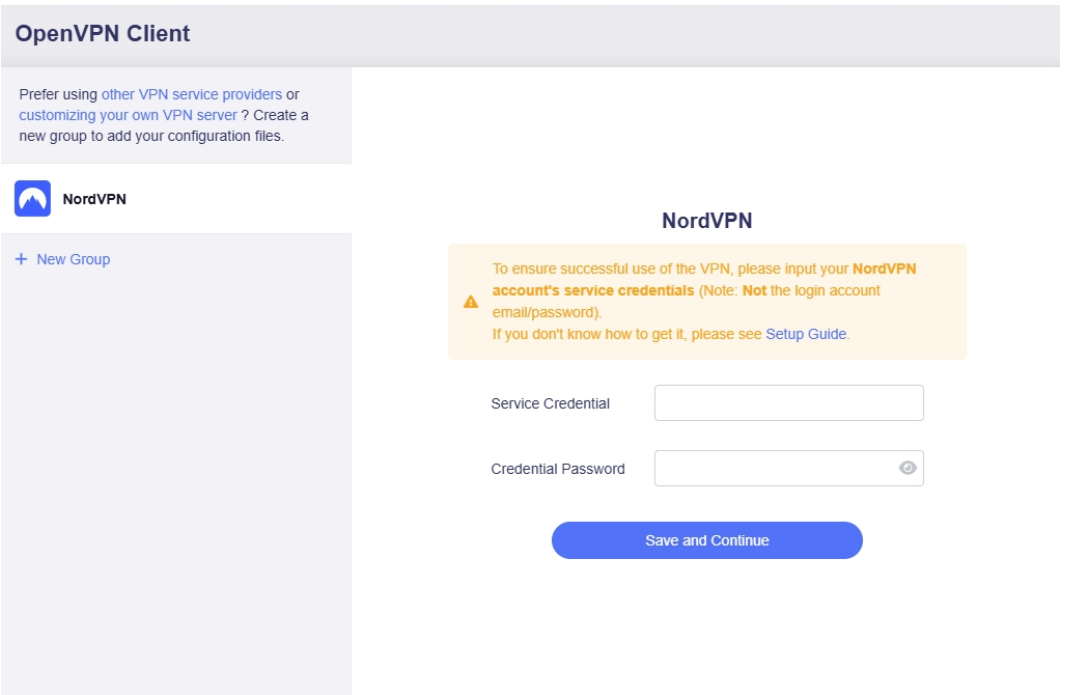
1. Melden Sie sich hier bei Ihrem NordVPN-Webkonto an.
2. Klicken Sie im Nord-Dashboard auf **NordVPN** und anschließend auf **Set up NordVPN manually**.



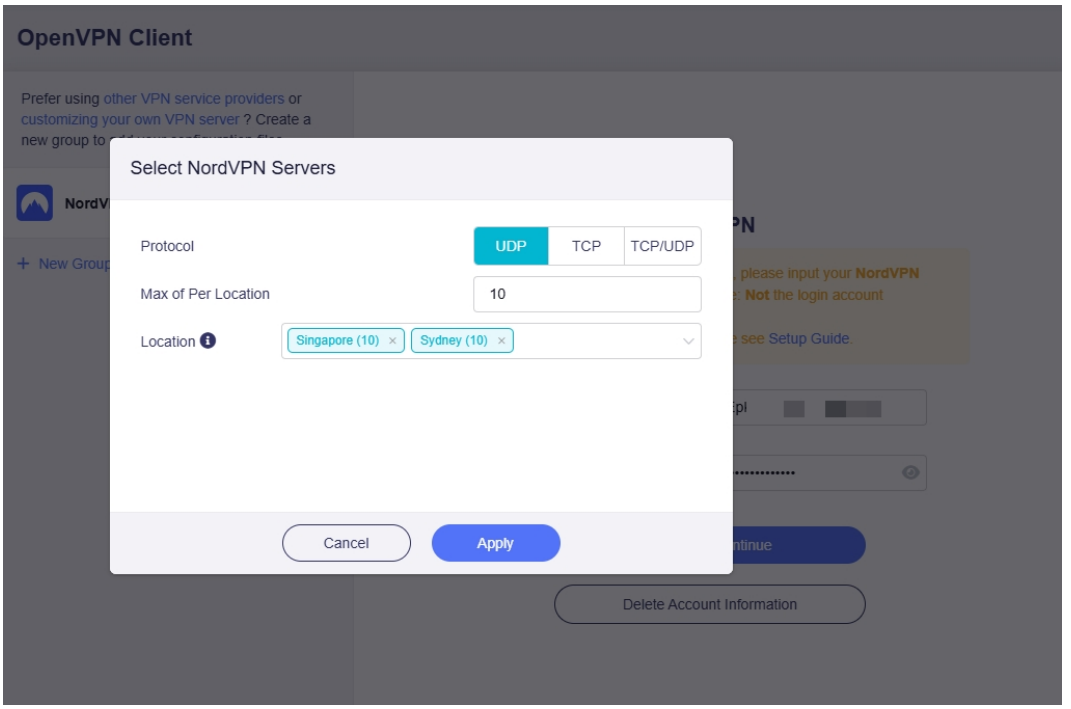
Dort finden Sie die **Dienstzugangsdaten**. Kopieren Sie diese für die spätere Verwendung.



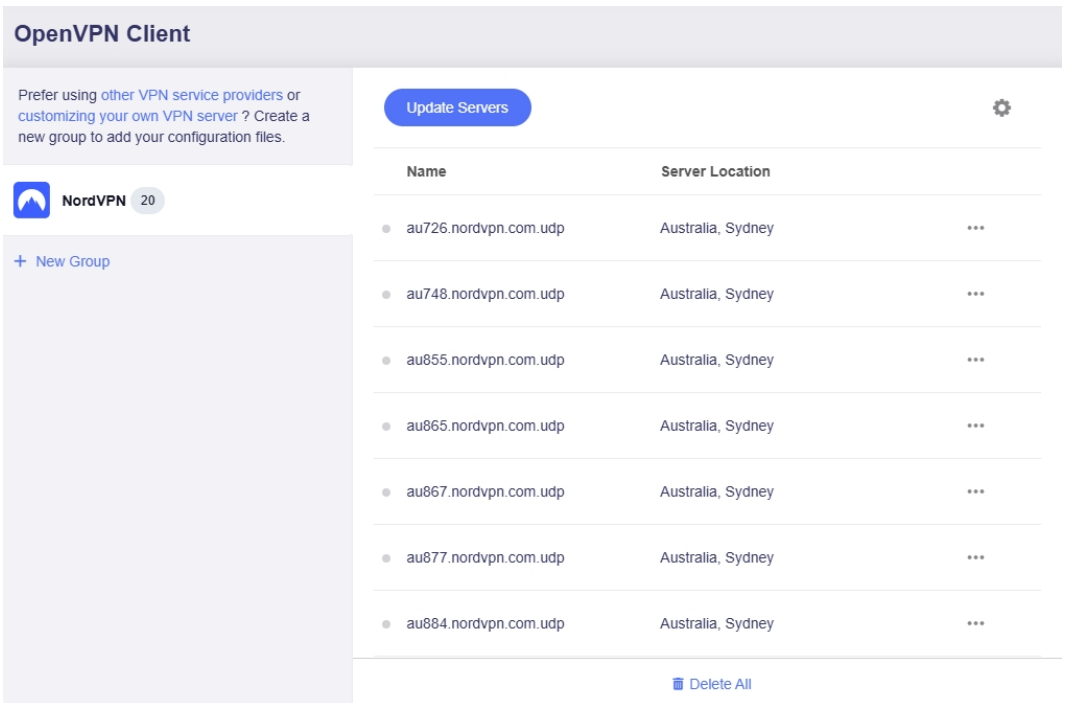
3. Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **VPN** > **OpenVPN Client** > **NordVPN**. Geben Sie die Dienstzugangsdaten ein. Hinweis: Dies sind NICHT die E-Mail-Adresse und das Passwort Ihres Benutzerkontos. Klicken Sie anschließend auf **Save and Continue**.



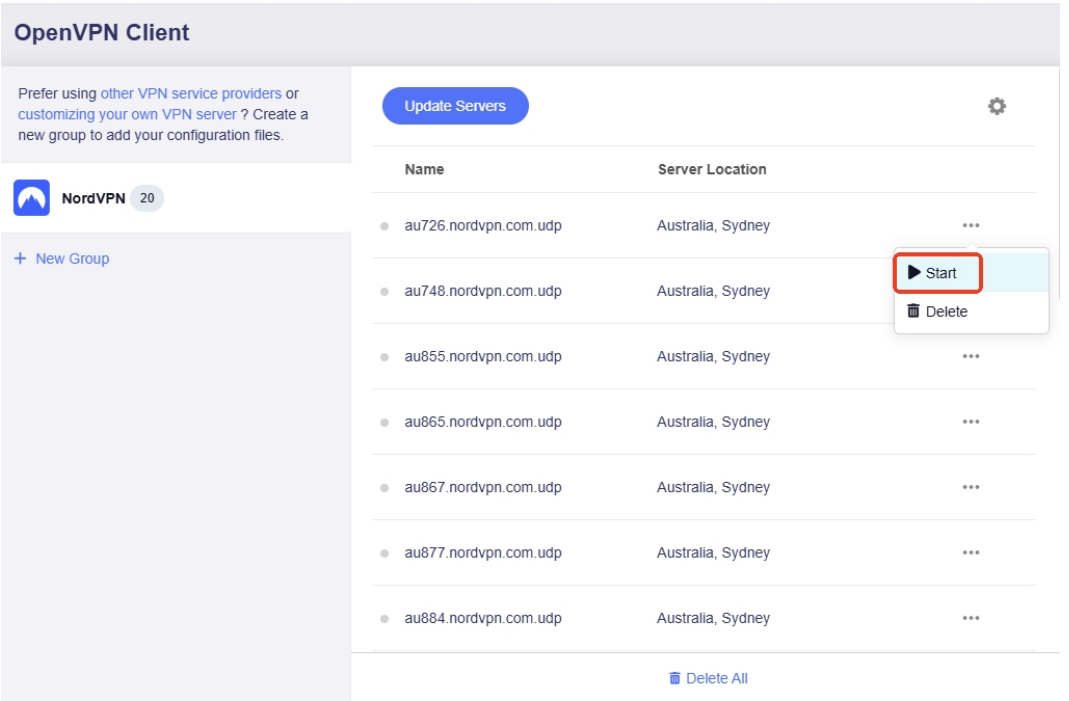
4. Wählen Sie das Protokoll, die maximale Serveranzahl pro Standort und die Standorte aus. Klicken Sie anschließend auf **Apply**.



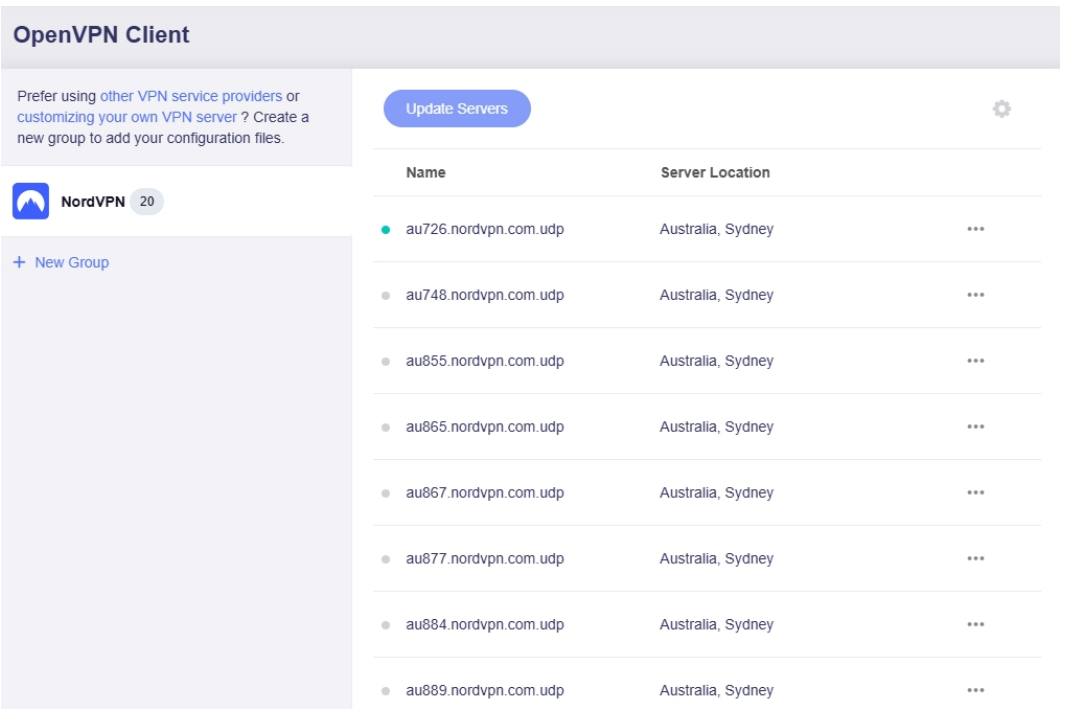
Die Konfigurationsdateien werden heruntergeladen.



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



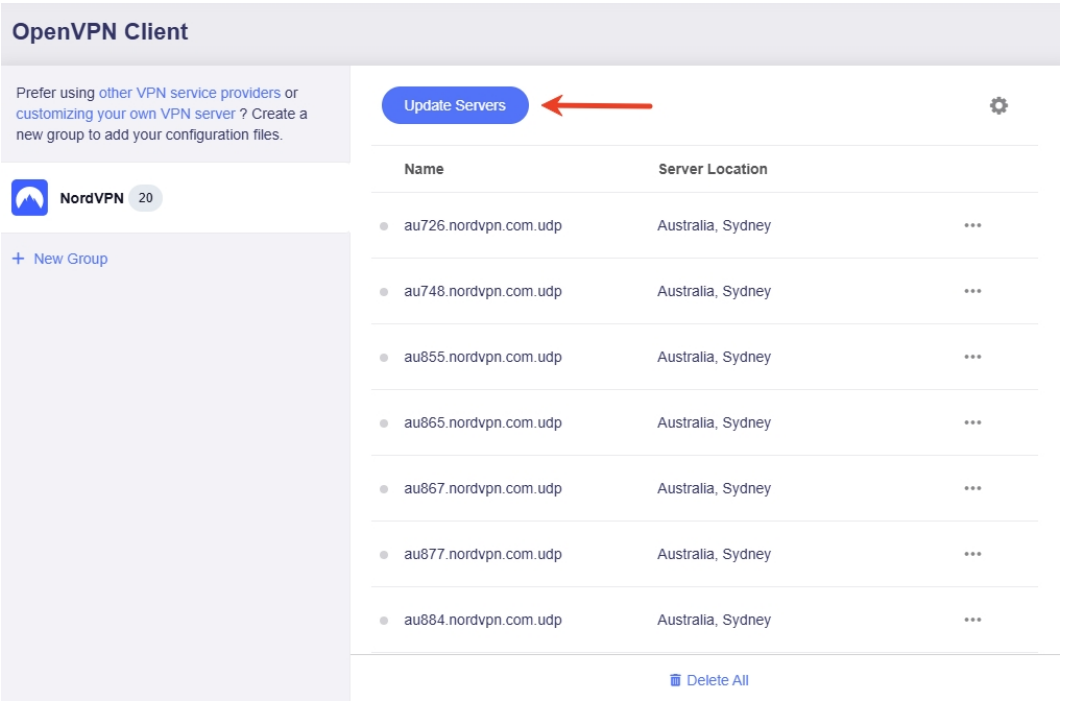
6. Bei erfolgreicher Verbindung erscheint neben der Konfigurationsdatei ein grüner Punkt.



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

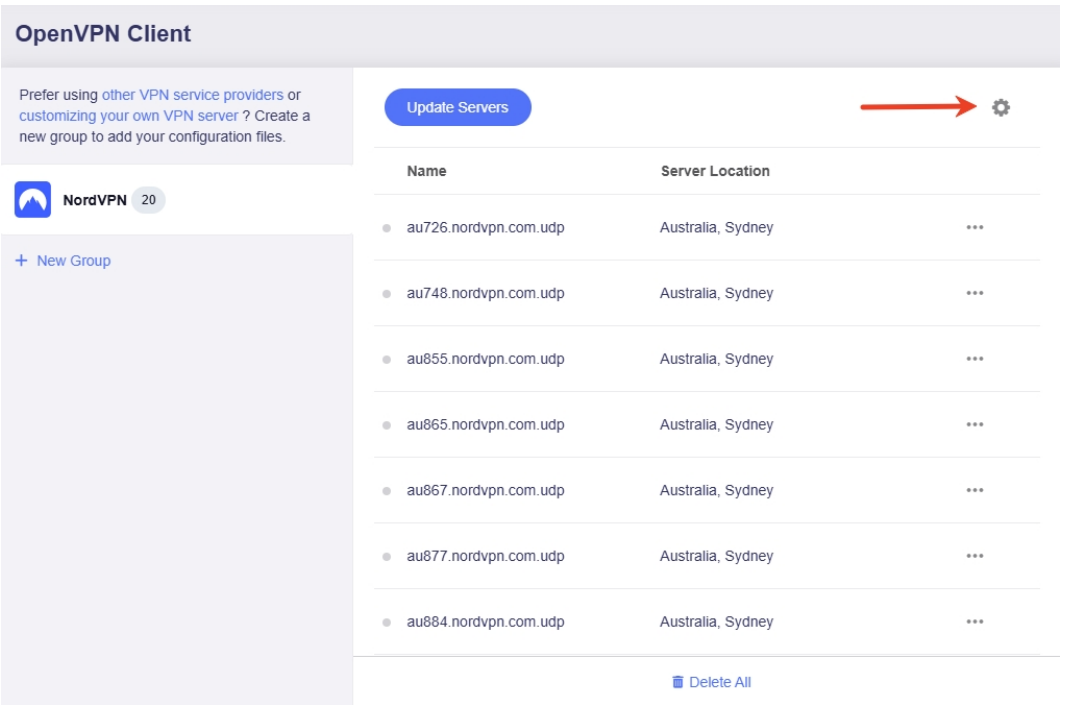
7. Server aktualisieren.

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



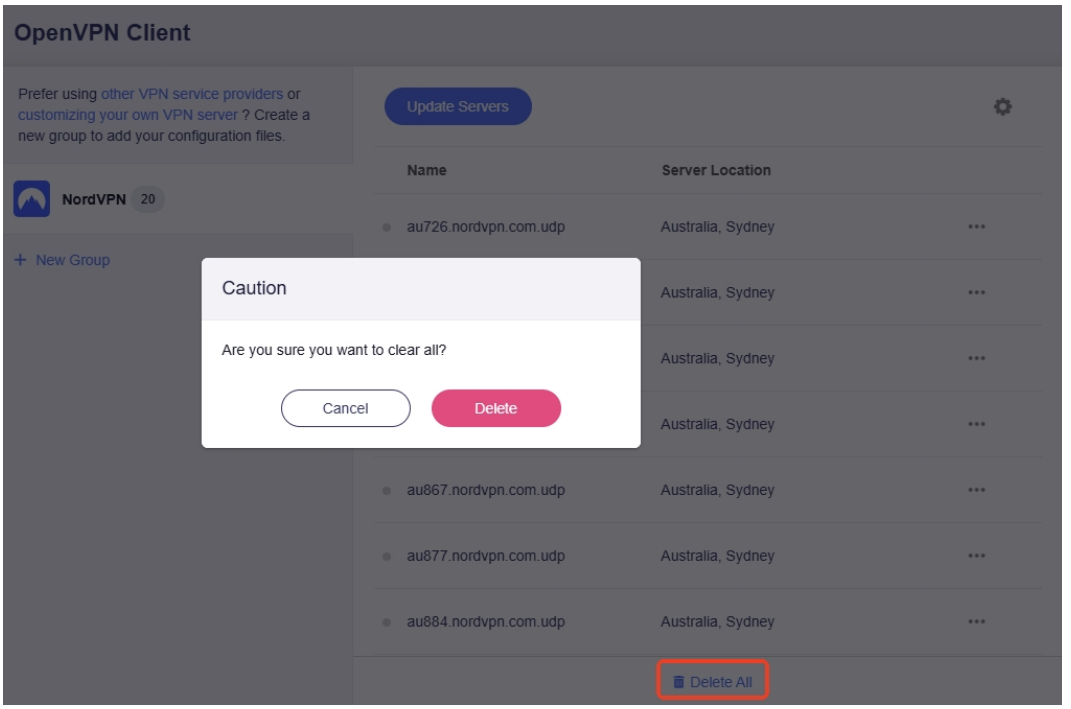
8. Zugangsdaten bearbeiten.

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



9. Alle Dateien löschen.

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

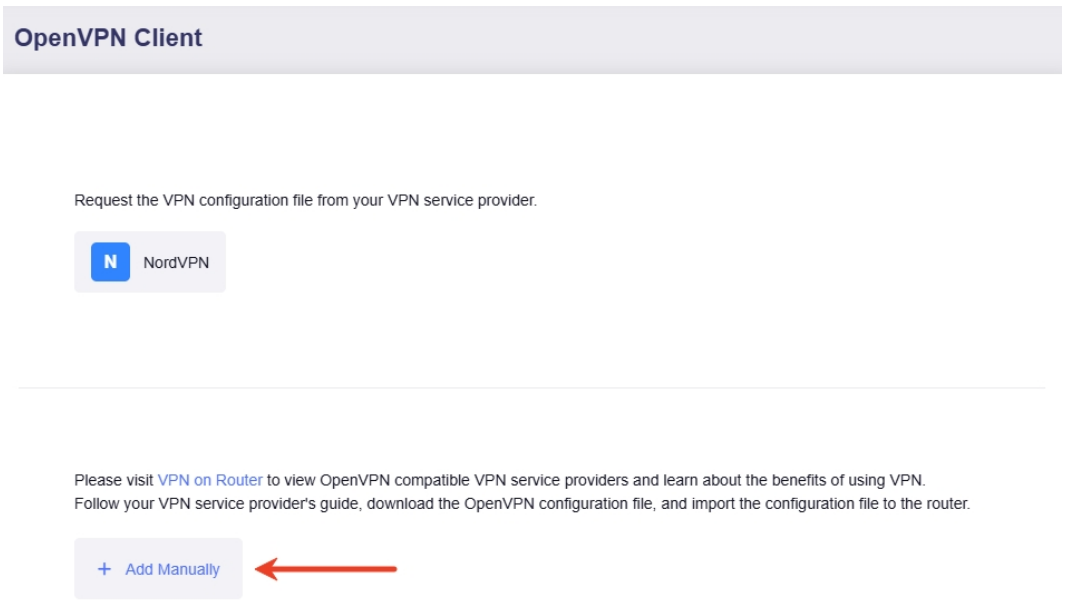

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

10.1.3 OpenVPN-Client manuell einrichten (andere Anbieter)

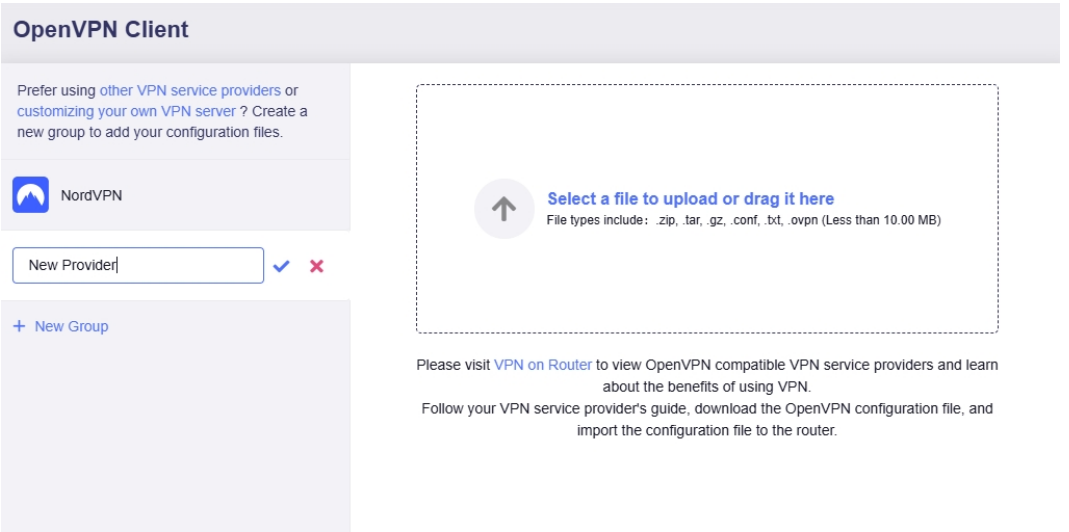
Wenn Ihr OpenVPN-Anbieter nicht in unsere Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den OpenVPN-Client einzurichten.

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

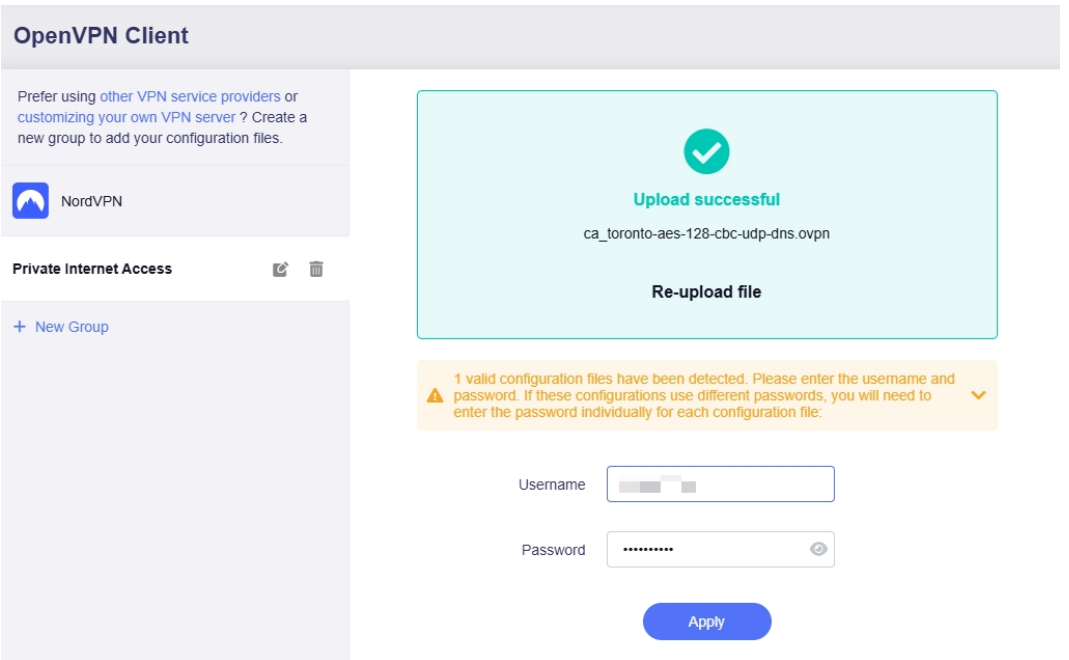
1. Laden Sie eine Konfigurationsdatei von der offiziellen Webseite von Private Internet Access herunter.
2. Melden Sie sich an der Weboberfläche an, öffnen Sie **VPN** > **OpenVPN Client** und klicken Sie auf **Add Manually**.



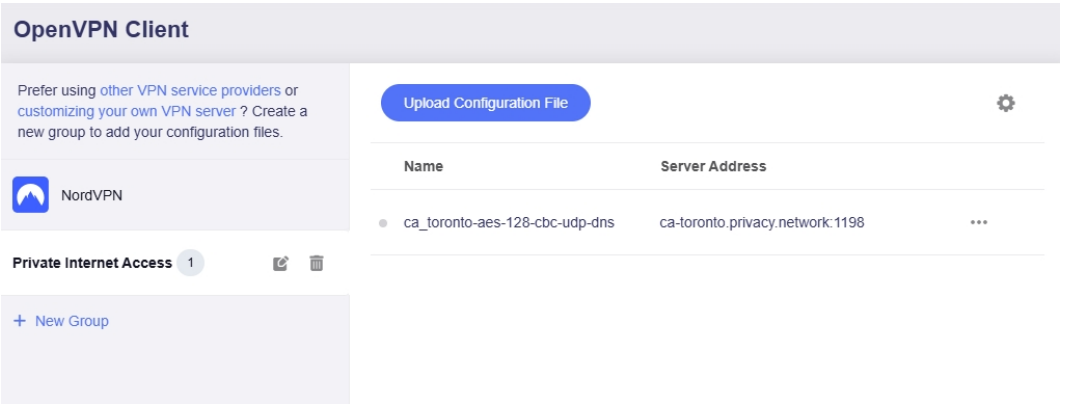
3. In der linken Seitenleiste wird eine Gruppe erstellt. Vergeben Sie einen aussagekräftigen Namen.



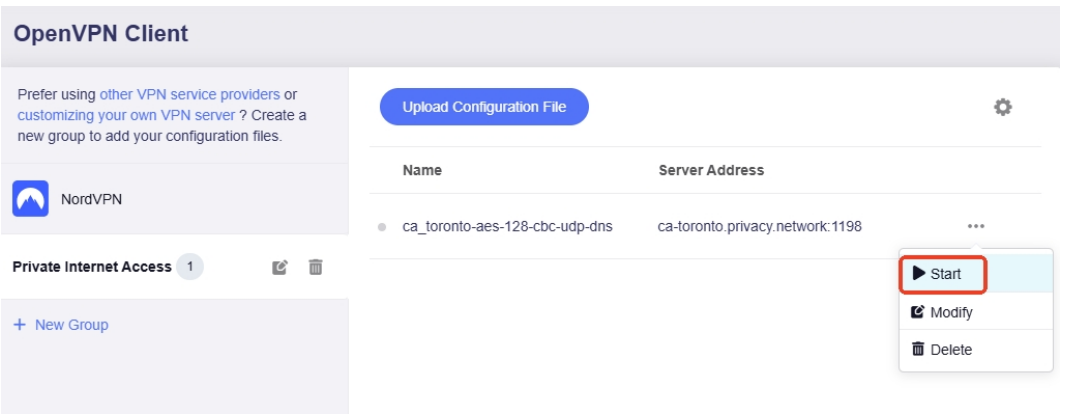
4. Laden Sie Ihre OpenVPN-Konfigurationsdatei hoch. Geben Sie bei Bedarf die Zugangsdaten ein und klicken Sie auf **Apply**.



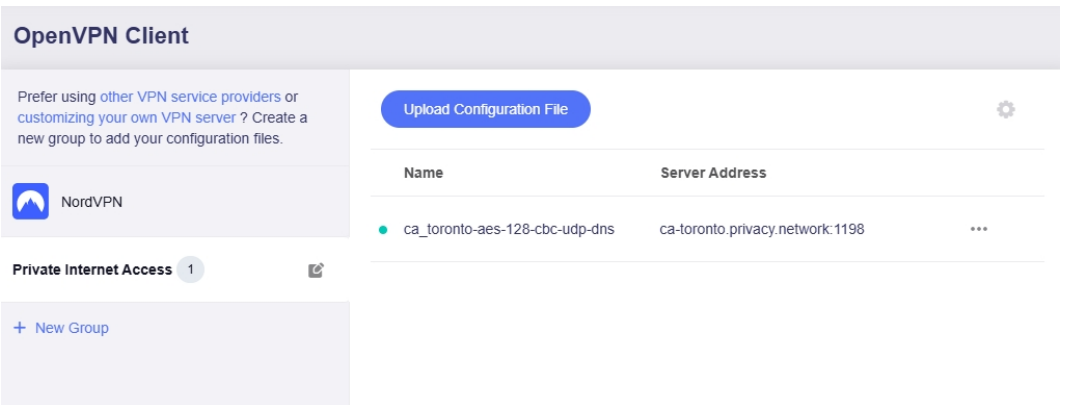
Die hochgeladene Konfigurationsdatei wird angezeigt.



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



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



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

10.2 WireGuard-Client einrichten

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

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

10.2.1 Vorbereitung

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

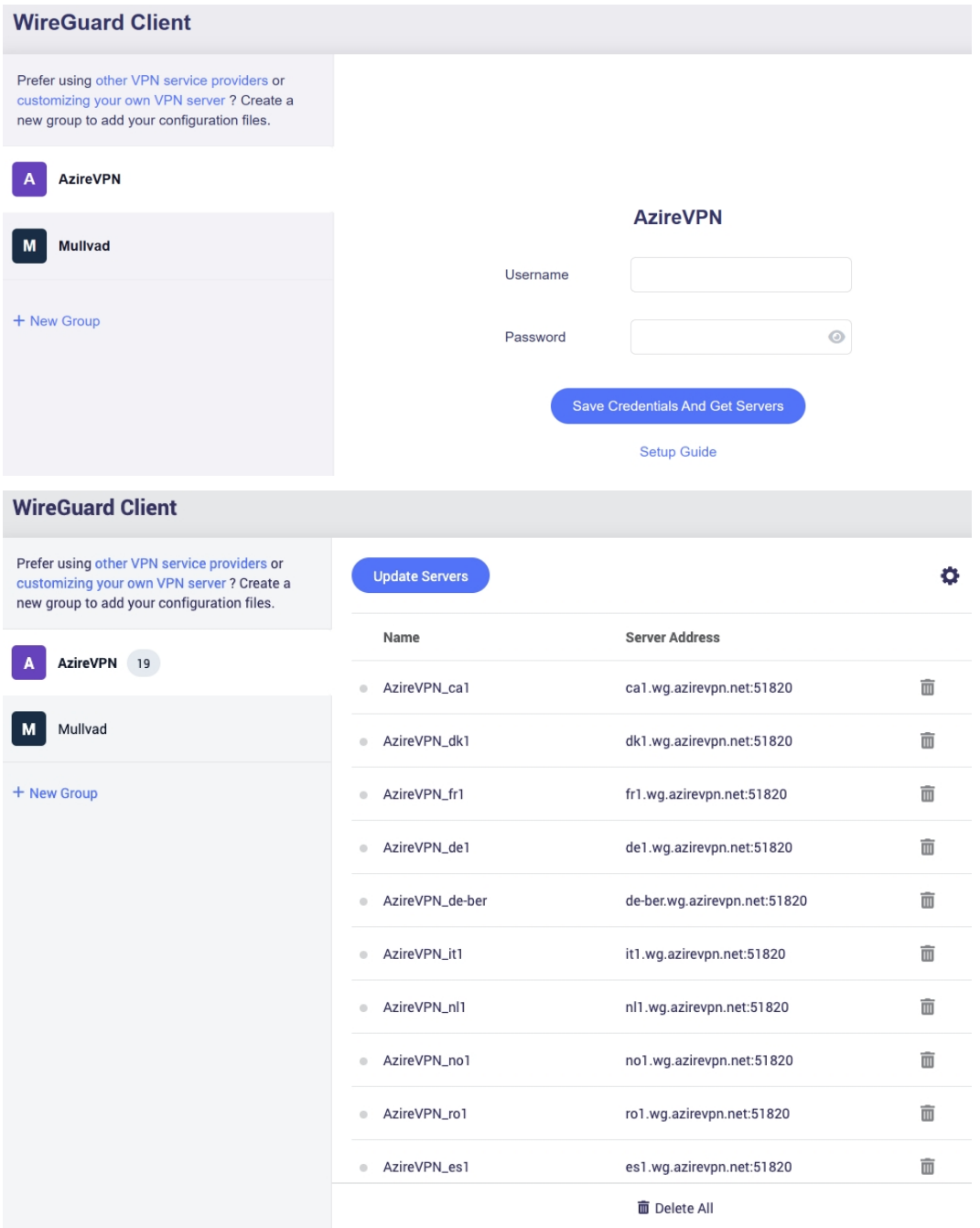
Wählen Sie nachstehend Ihren WireGuard-Anbieter aus, um direkt zur passenden Schritt-für-Schritt-Anleitung zu gelangen.

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

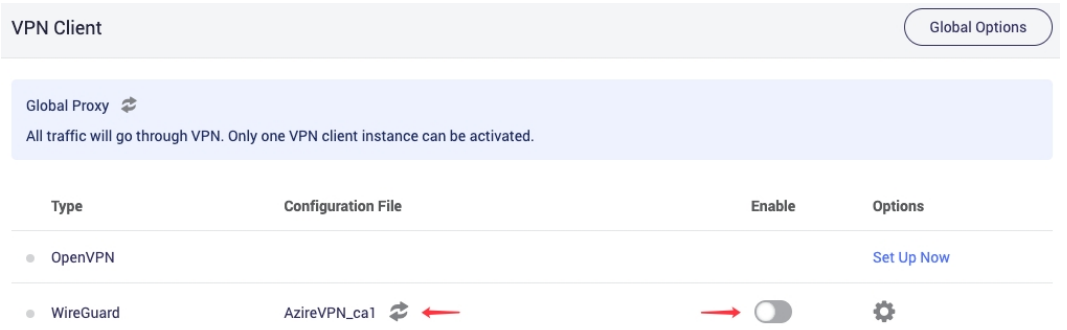
10.2.2 AzireVPN einrichten

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

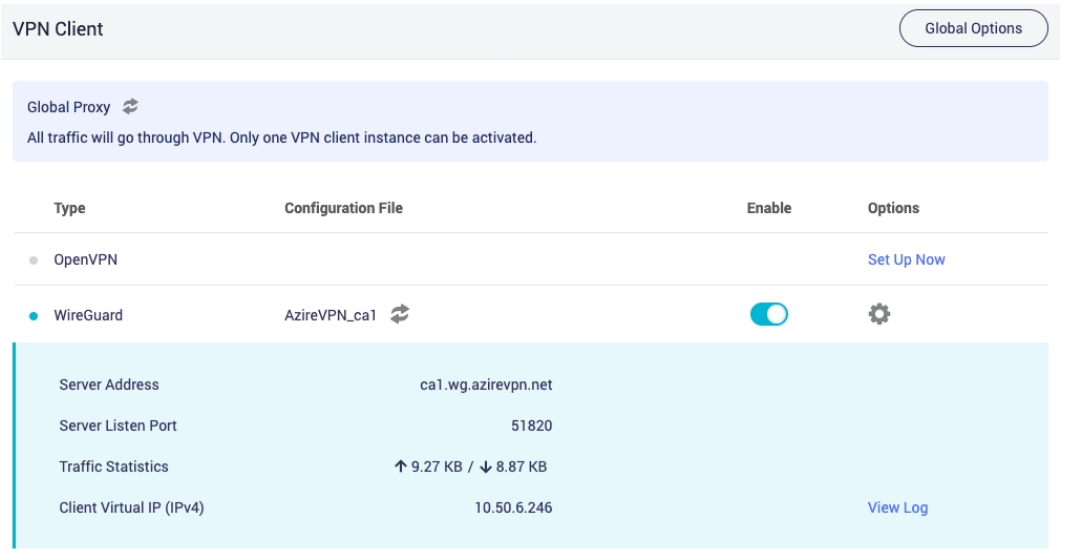
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **AzireVPN**.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Save Credentials And Get Servers**. Für jeden Server wird eine Konfigurationsdatei erzeugt.



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

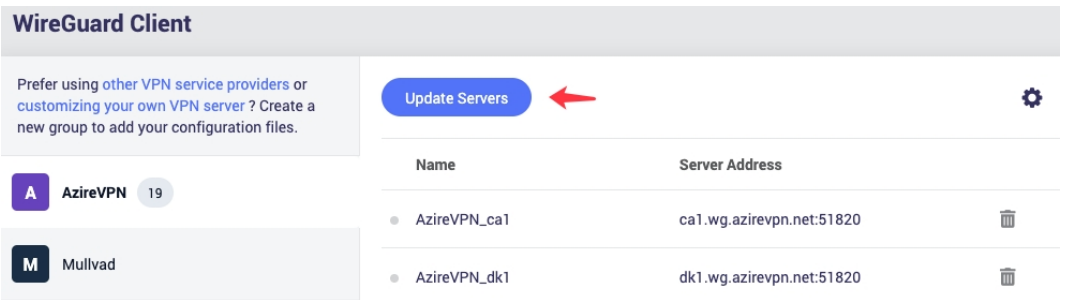


Nach erfolgreicher Verbindung werden Ihre Benutzer-IP-Adresse sowie die Anzahl der gesendeten und empfangenen Bytes angezeigt.



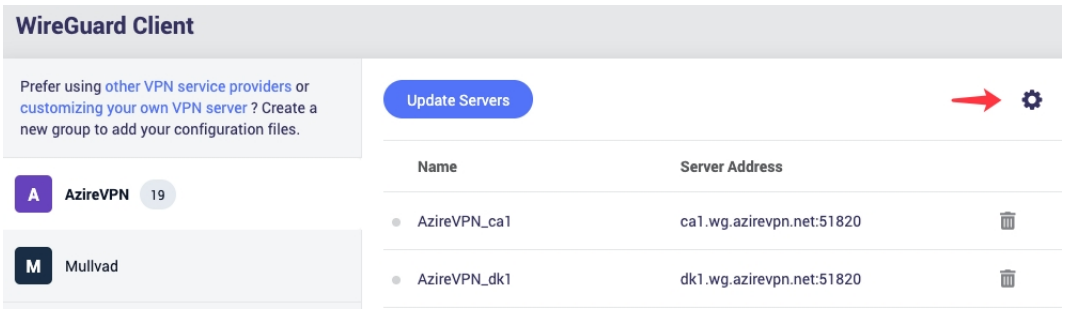
4. Server aktualisieren.

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



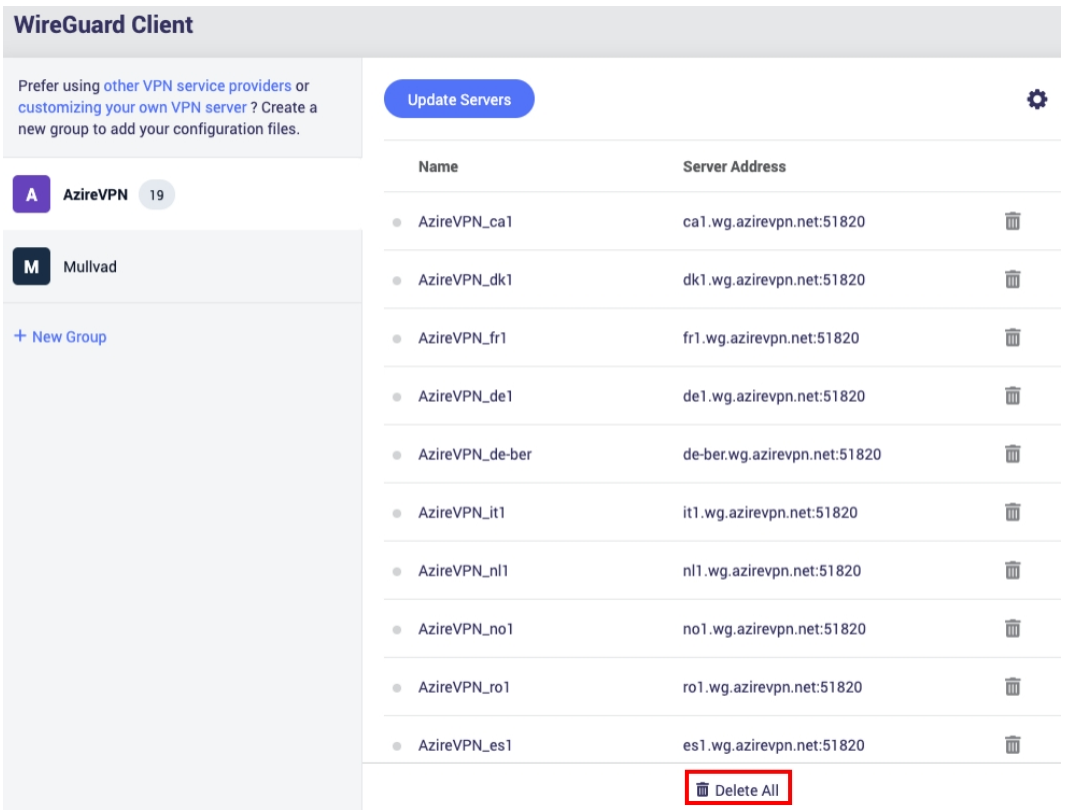
5. Zugangsdaten bearbeiten.

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



6. Alle Dateien löschen.

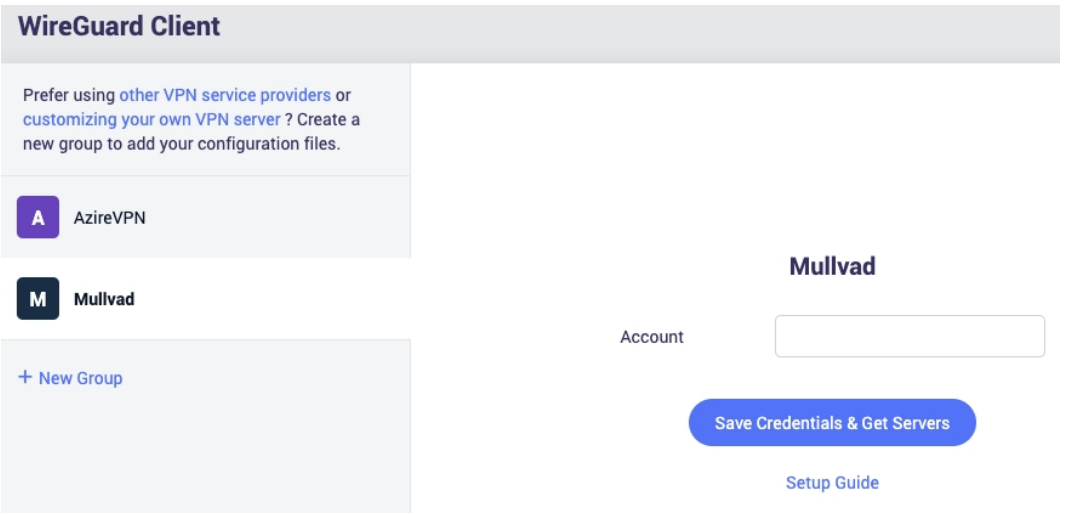
   Klicken Sie auf **Delete All**, um alle Konfigurationsdateien mit einem Klick zu löschen.



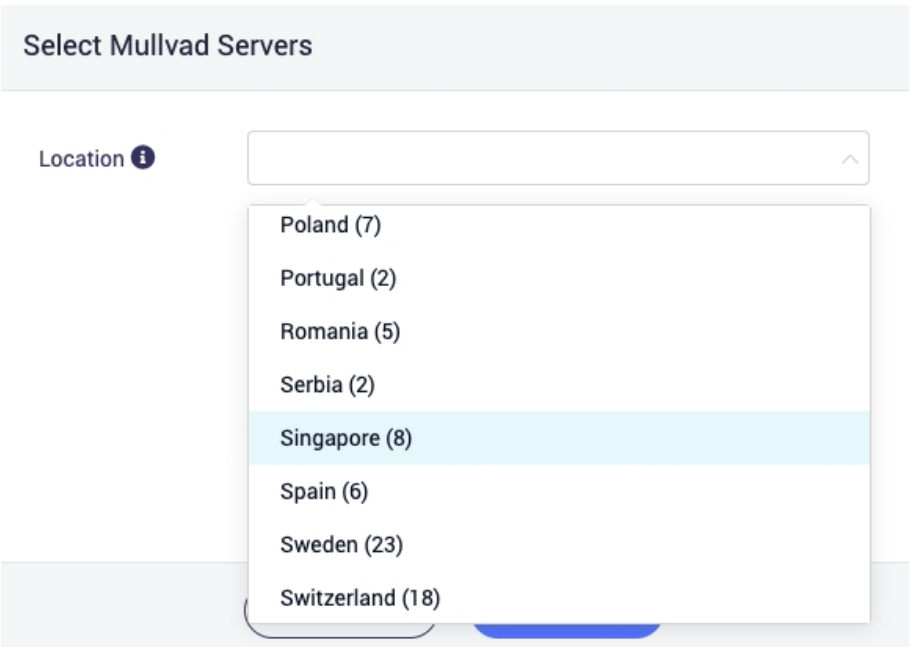
10.2.3 Mullvad einrichten

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

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

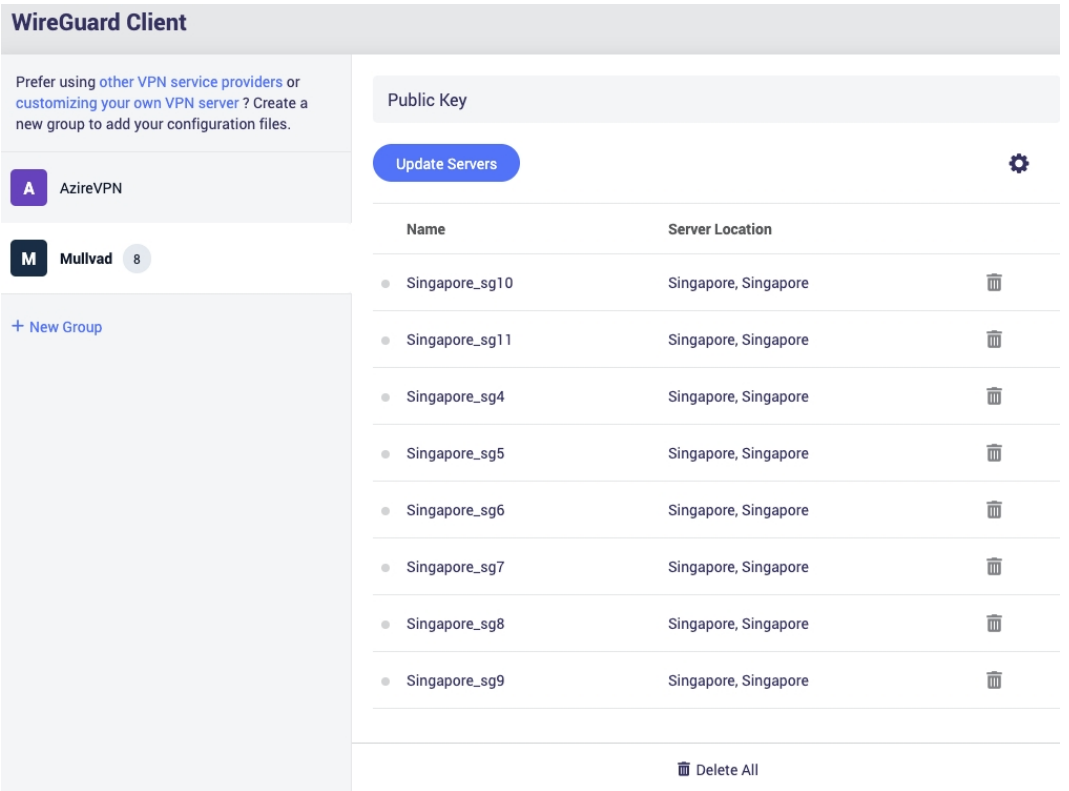


Es erscheint ein Dialog zur Standortauswahl.

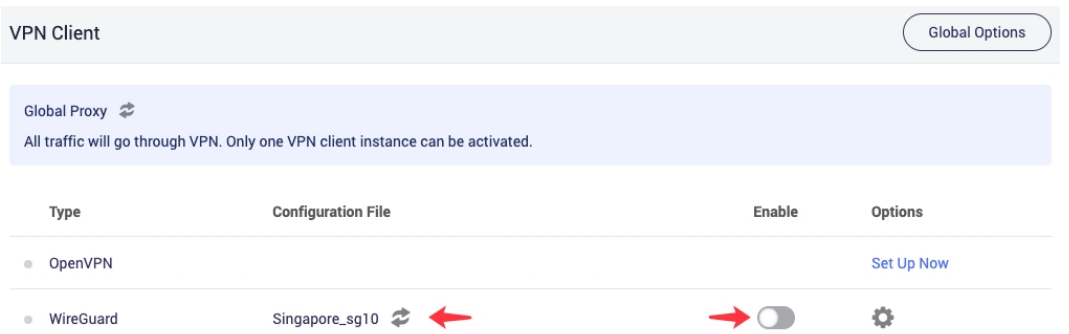


Anschließend werden die Konfigurationsdateien für den Server am ausgewählten Standort erzeugt.

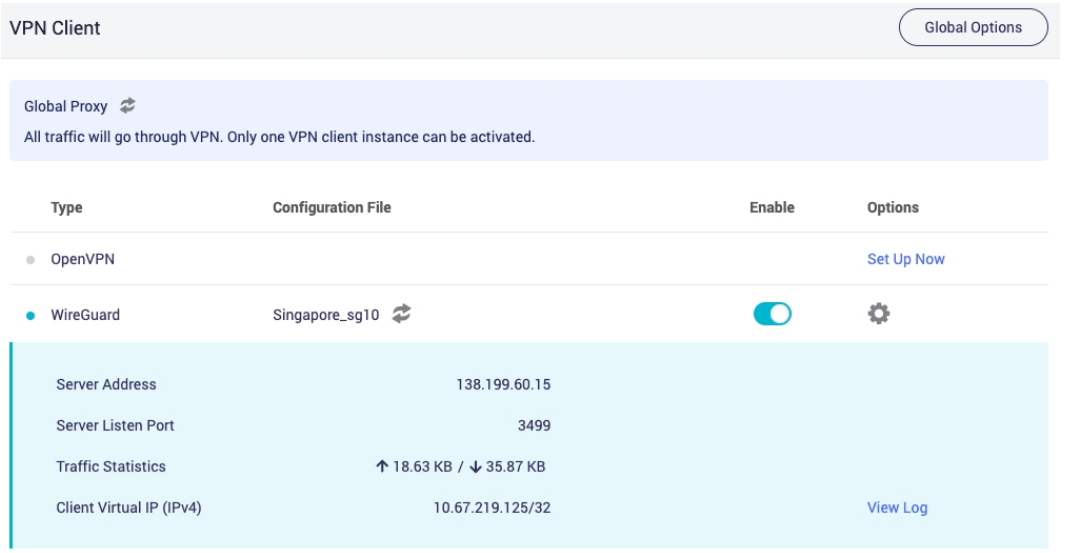
Der **Public Key** ist der öffentliche WireGuard-Schlüssel, der an den Mullvad-Server gesendet wird. Sie können bis zu fünf Schlüssel gleichzeitig verwenden und diese auf Ihrer Mullvad-Kontoseite verwalten.



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

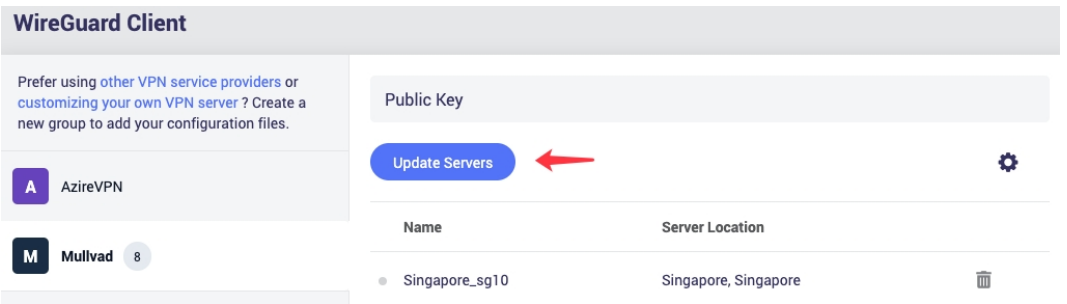


Nach erfolgreicher Verbindung werden Ihre Benutzer-IP-Adresse sowie die Anzahl der gesendeten und empfangenen Bytes angezeigt.



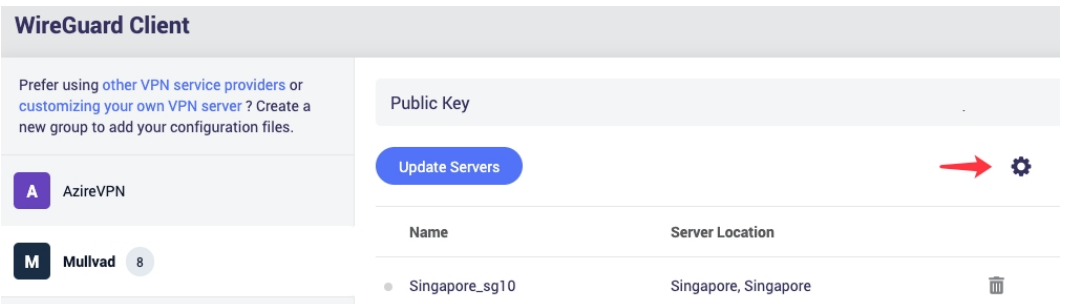
4. Server aktualisieren.

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



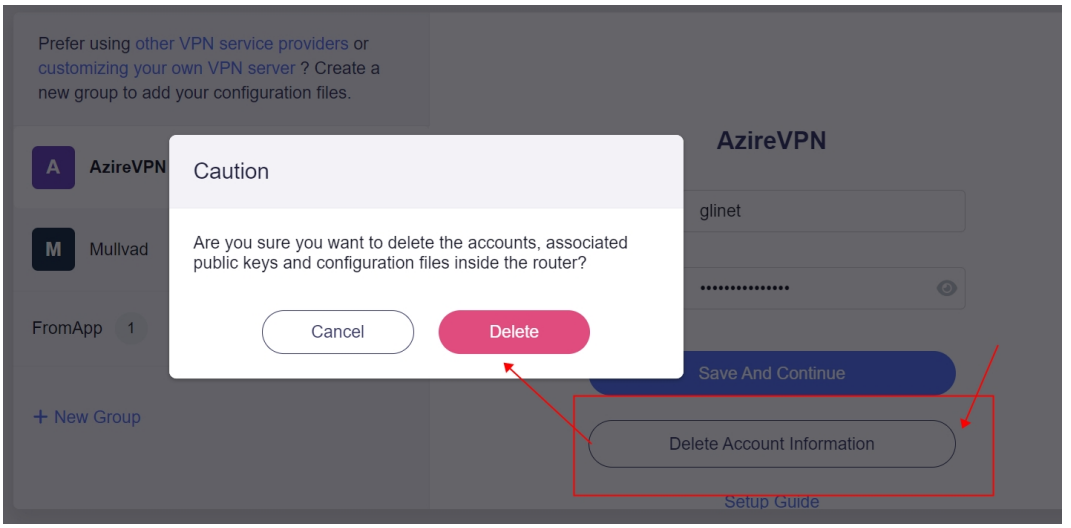
5. Zugangsdaten bearbeiten

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



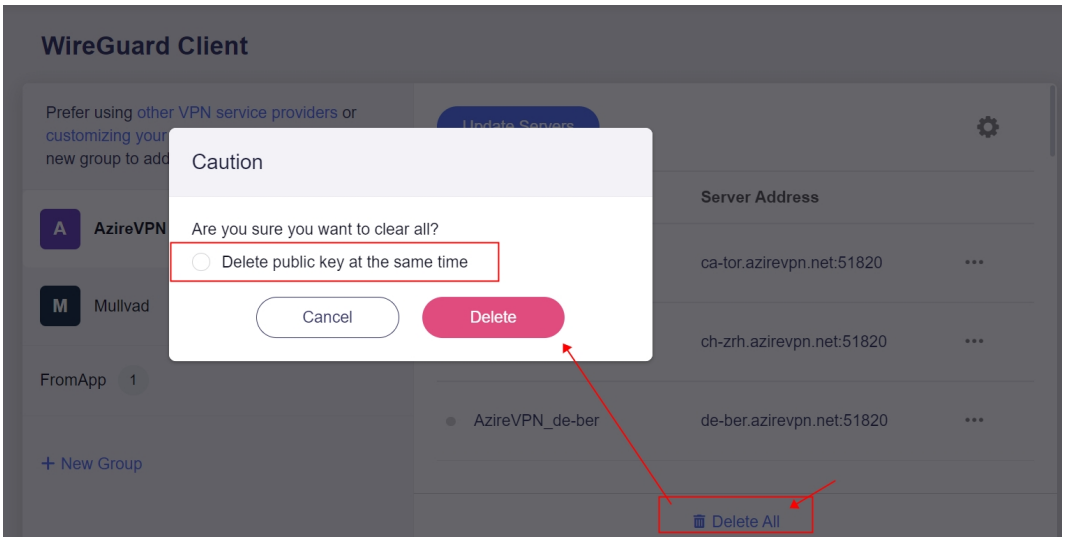
6. Kontoinformationen löschen

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



7. Löschen

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

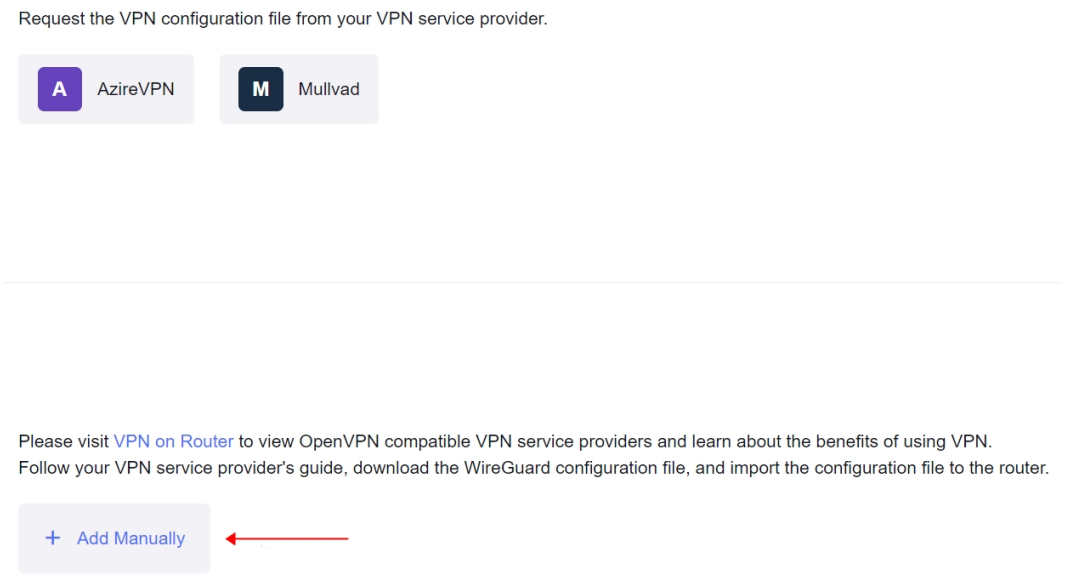


10.2.4 WireGuard-Client manuell einrichten (andere Anbieter)

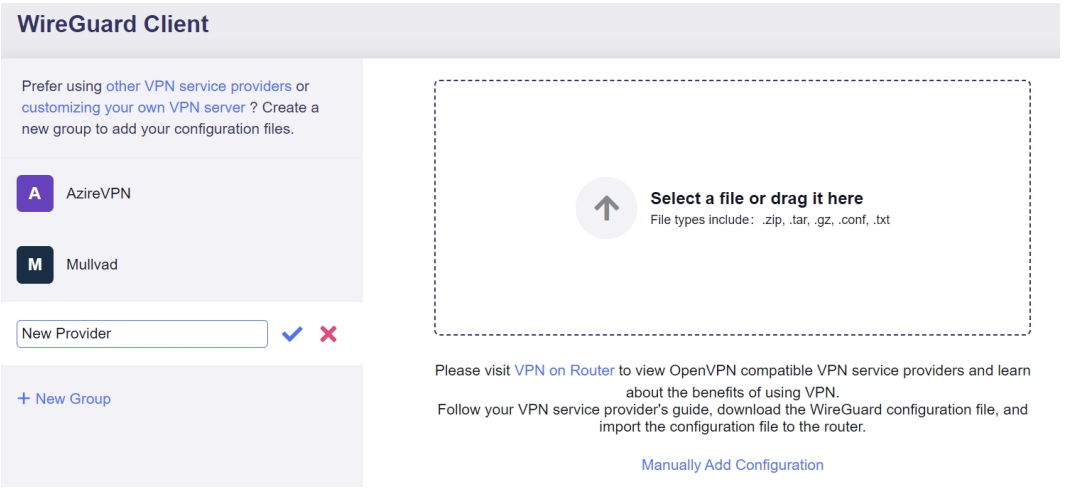
Wenn Ihr WireGuard-Anbieter nicht in die Weboberfläche integriert ist, laden Sie zunächst eine Konfigurationsdatei von seiner offiziellen Webseite herunter. Laden Sie diese anschließend auf den Router hoch, um den WireGuard-Client einzurichten. Falls Sie nicht wissen, wie Sie die Dateien herunterladen,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

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

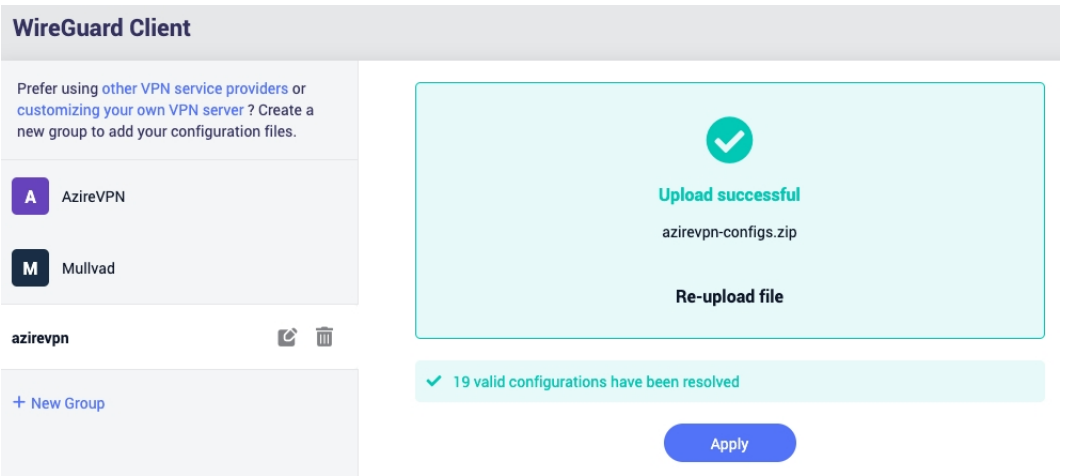
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **VPN** > **WireGuard Client** > **Add Manually**.



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

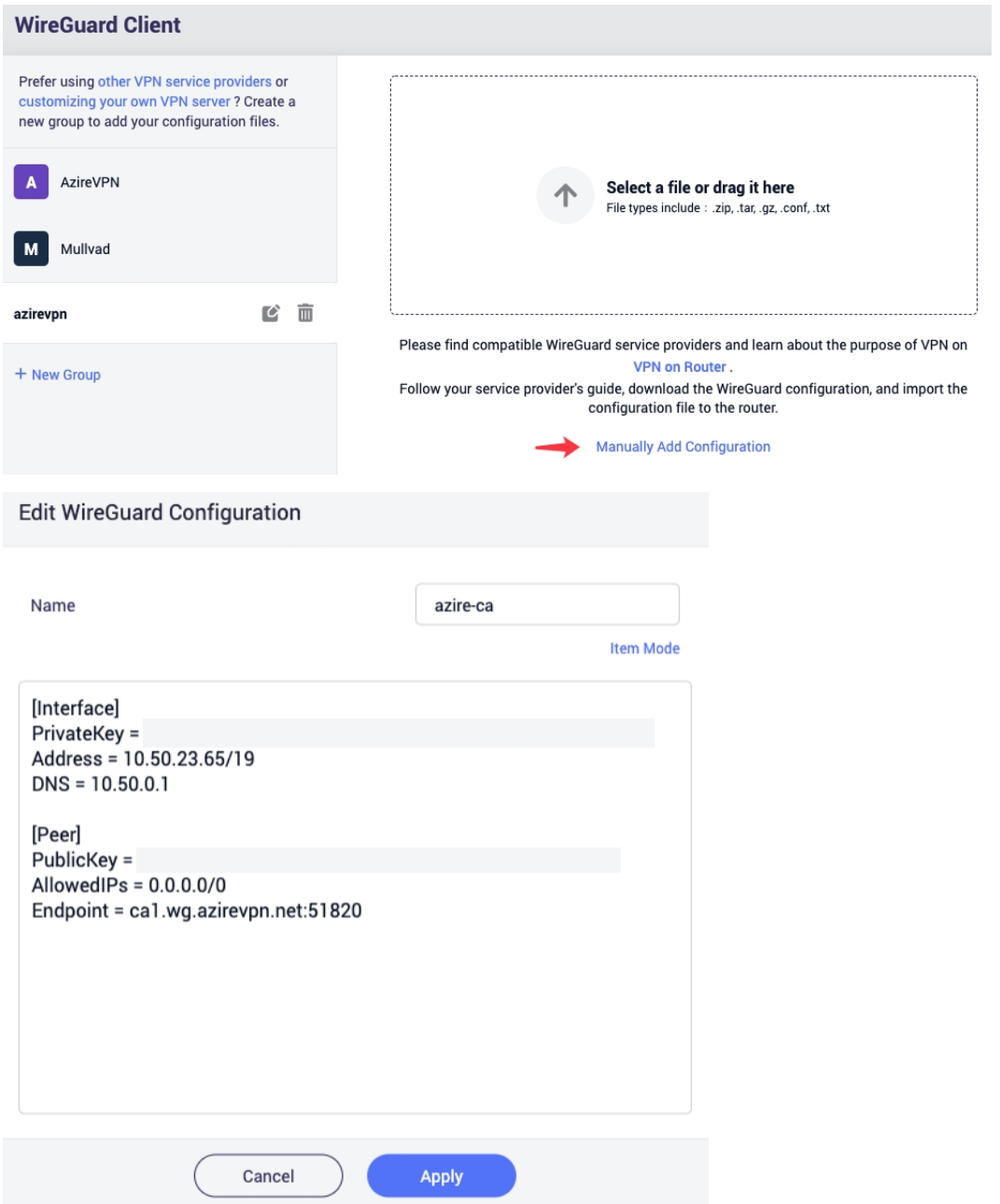


3. Klicken Sie auf den Upload-Bereich, laden Sie Ihre WireGuard-Konfigurationsdatei hoch und klicken Sie auf **Apply**. Unterstützte Formate: zip, tar, gz, conf und txt.

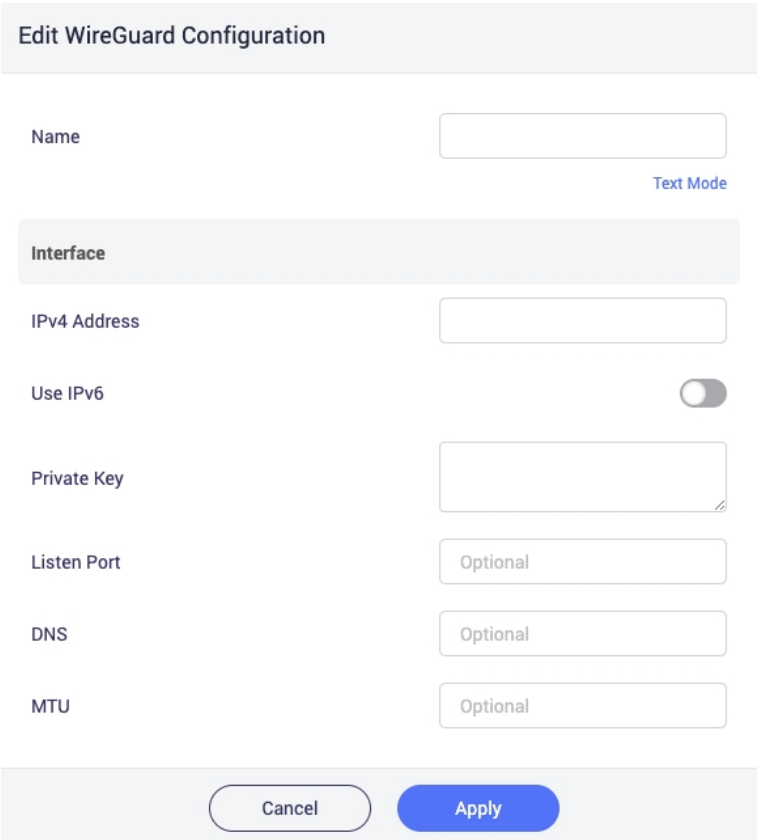


Wenn Sie ein Archiv mit mehreren Konfigurationsdateien hochladen, wird es automatisch entpackt.

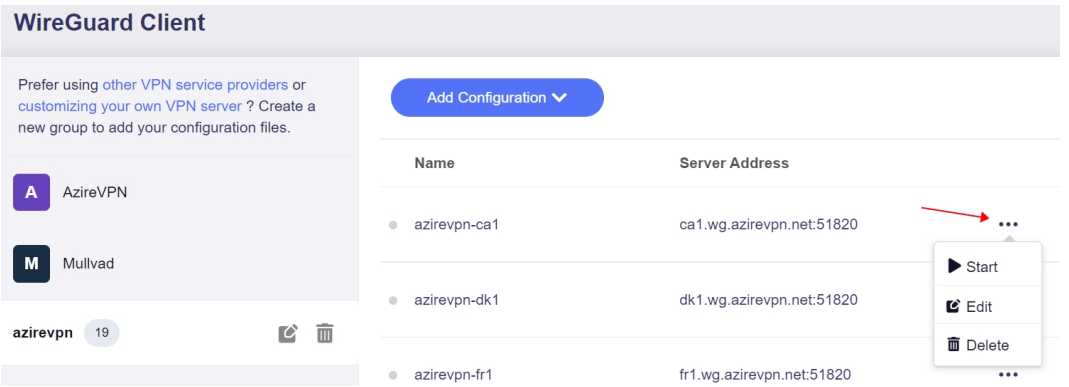
Alternativ klicken Sie unten im Upload-Bereich auf **Manually Add Configuration**, geben die Konfiguration als Text ein und klicken auf **Apply**.



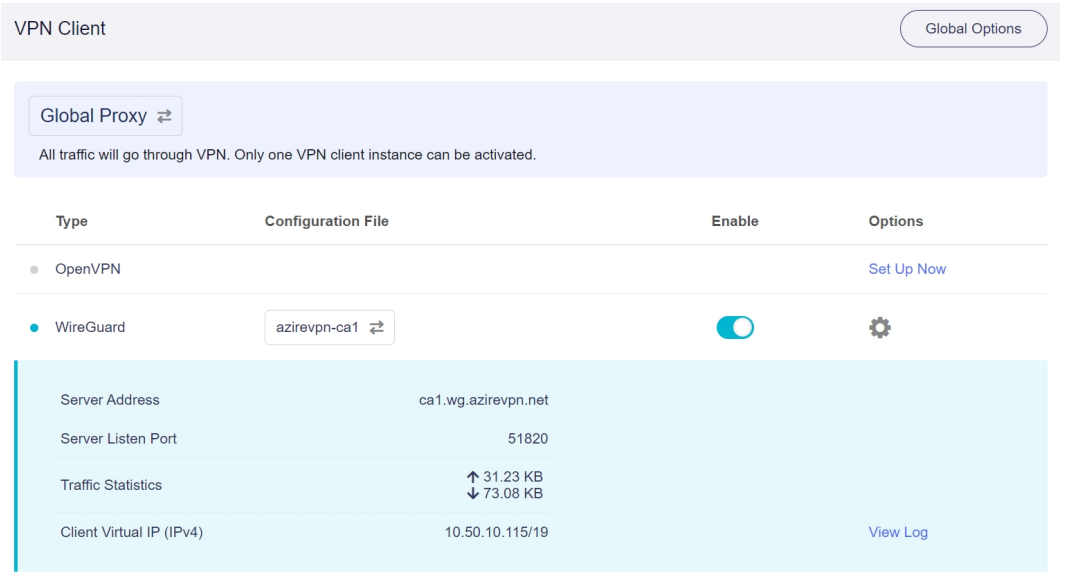
Um die einzelnen Einträge zu prüfen, wechseln Sie in den Modus Item und kontrollieren Sie die Konfigurationsdetails. Klicken Sie anschließend auf **Apply**.



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



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


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

Kapitel 11

Tor

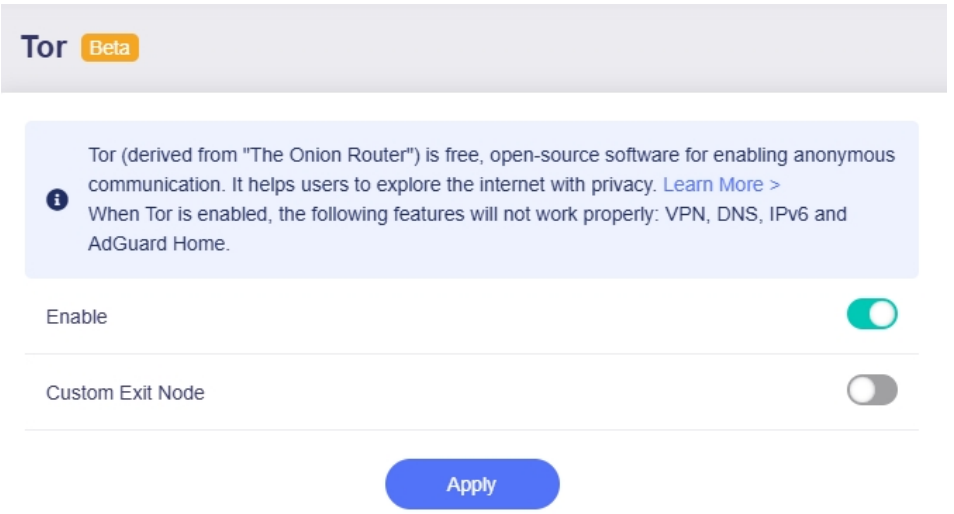
Dieses Kapitel stellt Tor (The Onion Router) vor, eine freie, quelloffene Software für anonyme Kommunikation.

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

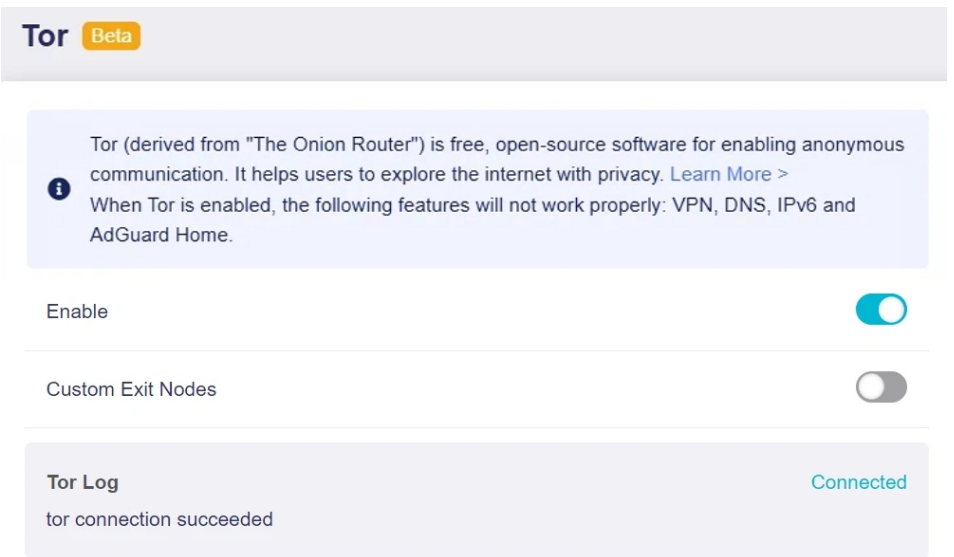
Bei aktiviertem Tor funktionieren VPN, DNS, IPv6 und AdGuard Home nicht ordnungsgemäß.

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

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



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



Kapitel 12

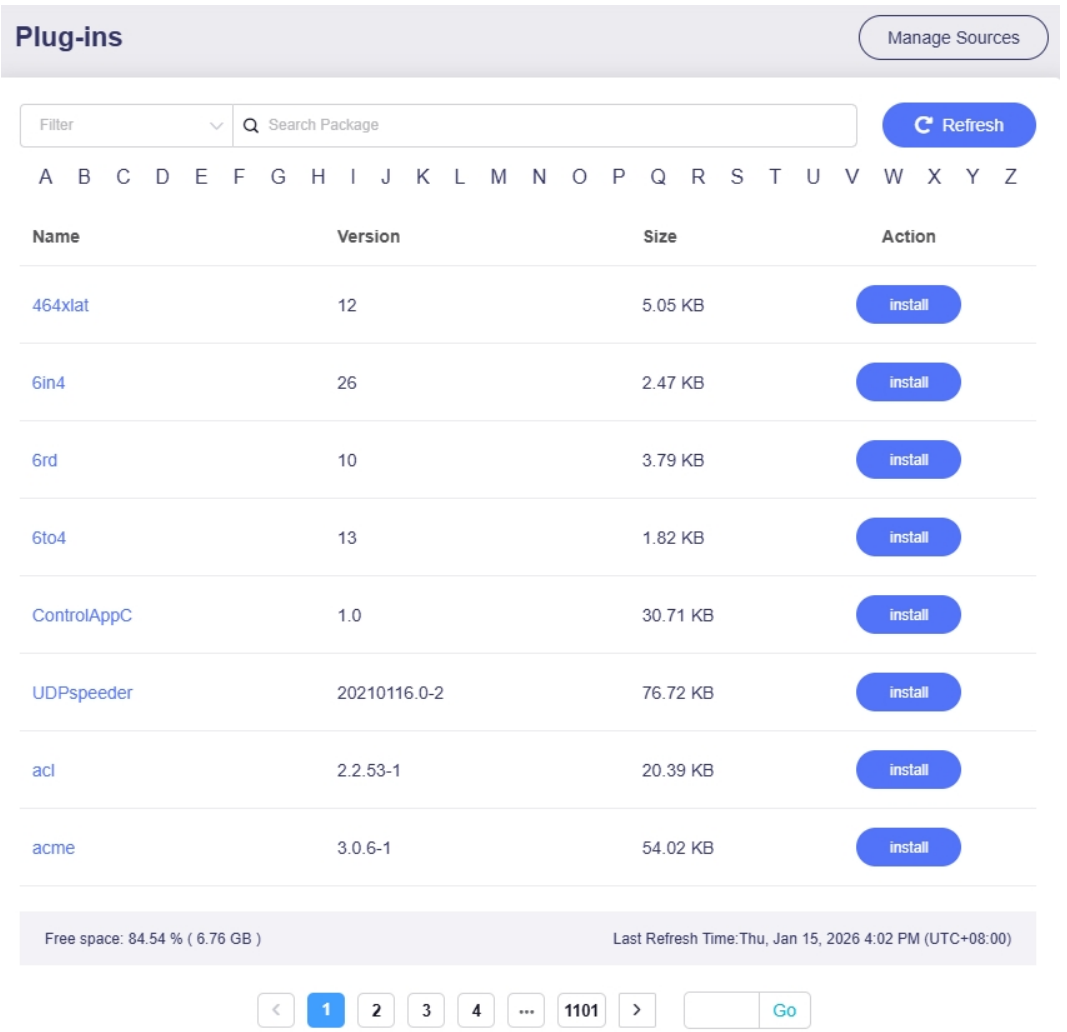
Anwendungen

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

12.1 Plug-ins

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

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



Hinweis:

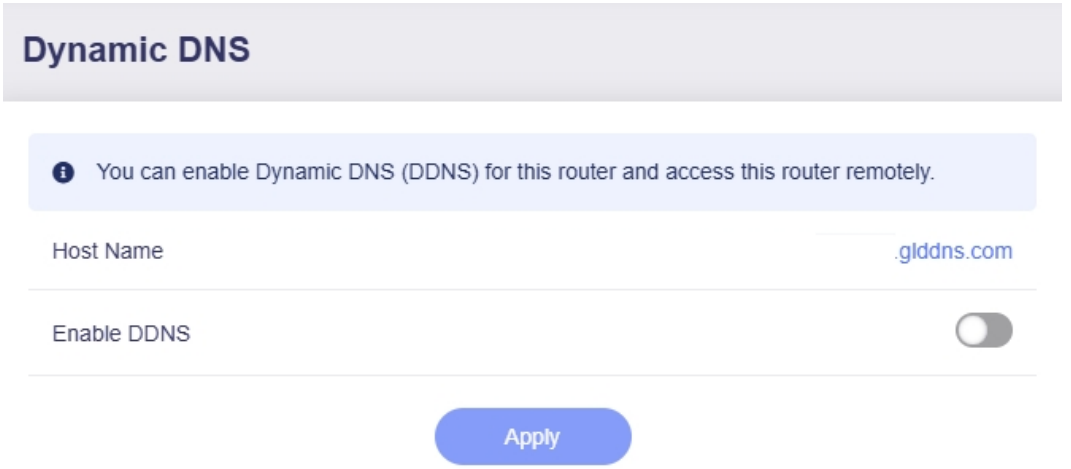
1. Es wird davon abgeraten, in der offiziellen GL.iNet-Firmware vorinstallierte Plug-ins wie nginx, AdGuard Home oder Tailscale zu aktualisieren.
2. Manuell installierte Plug-ins von Drittanbietern können aktualisiert werden. GL.iNet haftet jedoch nicht für Sicherheitsprobleme durch solche Plug-ins.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

12.2 Dynamisches DNS

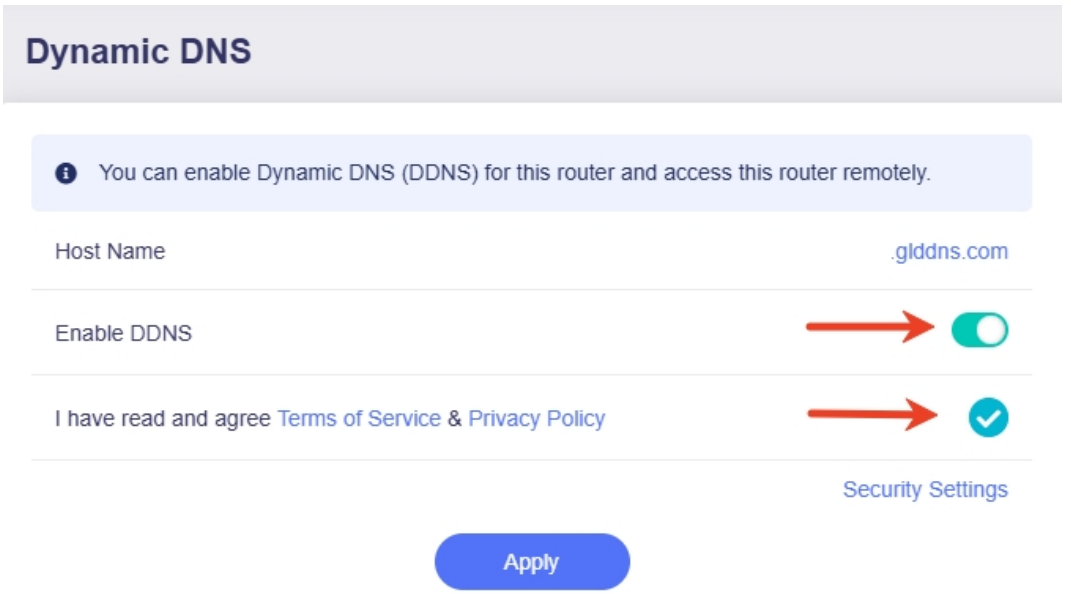
Dynamic DNS (DDNS) ordnet einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zu. Damit können Sie aus der Ferne auf Ihren Router zugreifen. Für diese Funktion ist eine öffentliche IP-Adresse erforderlich.

12.2.1 DDNS aktivieren

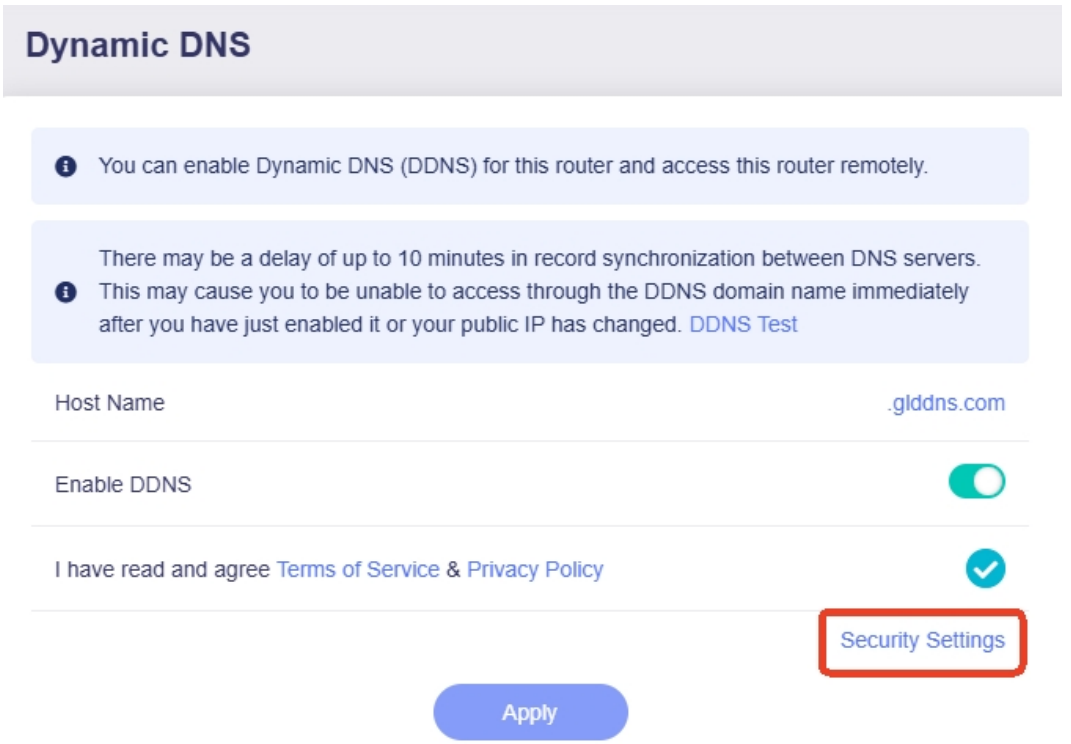
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **Dynamic DNS**. Die folgende Seite wird angezeigt.



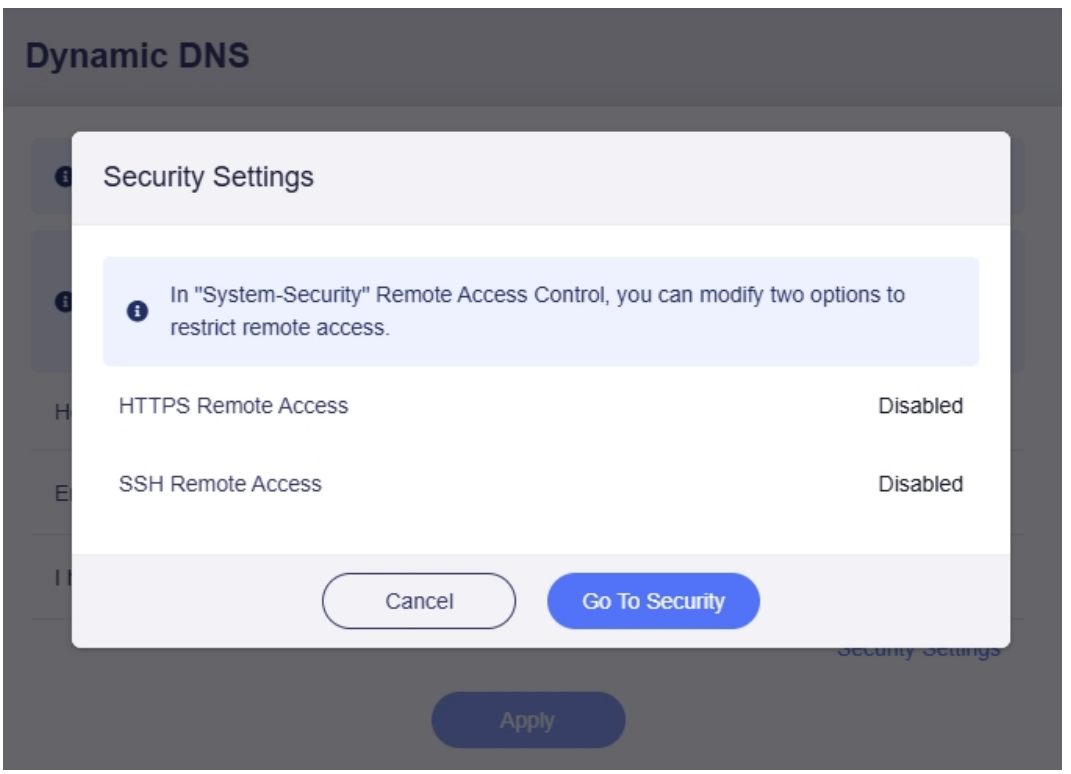
2. Aktivieren Sie **Enable DDNS**, lesen und akzeptieren Sie die **Terms of Services & Privacy Policy** und klicken Sie auf **Apply**.



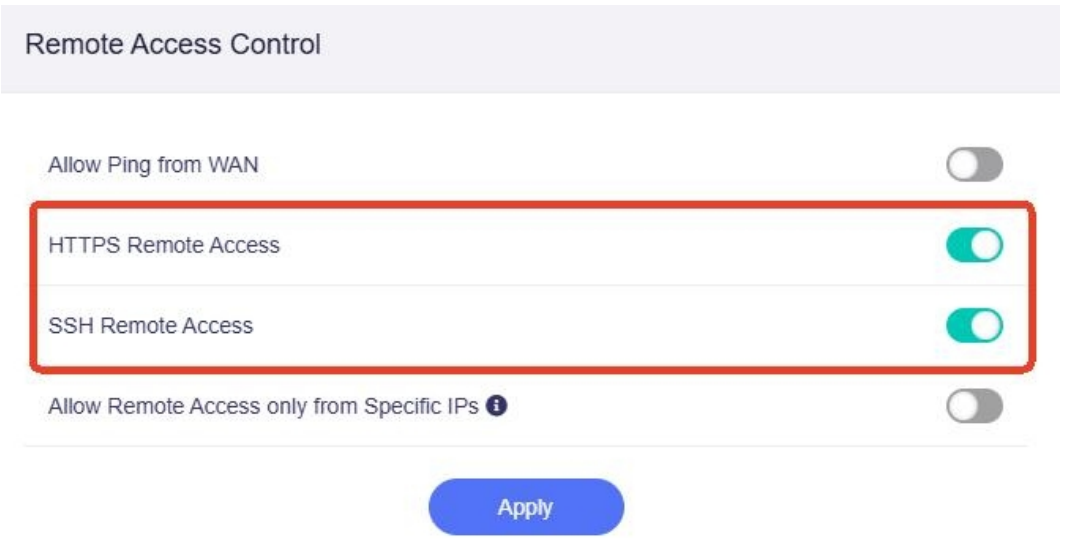
3. Klicken Sie unten rechts auf **Security Settings**.



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



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



Hinweis:

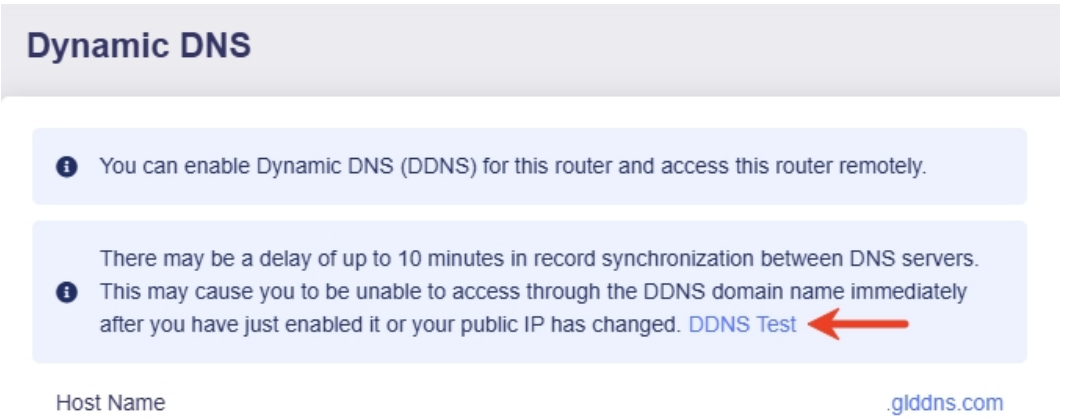
1. Die Synchronisierung der Einträge zwischen DNS-Servern kann bis zu zehn Minuten dauern. Deshalb kann der Zugriff über den DDNS-Domainnamen direkt nach der Aktivierung oder nach einer Änderung Ihrer öffentlichen IP-Adresse vorübergehend nicht möglich sein.
2. Wenn Sie DDNS und einen VPN-Client gleichzeitig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

12.2.2 DDNS-Funktion prüfen

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

Methode 1: DDNS-Testwerkzeug verwenden

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



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



Methode 2: Befehle verwenden

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



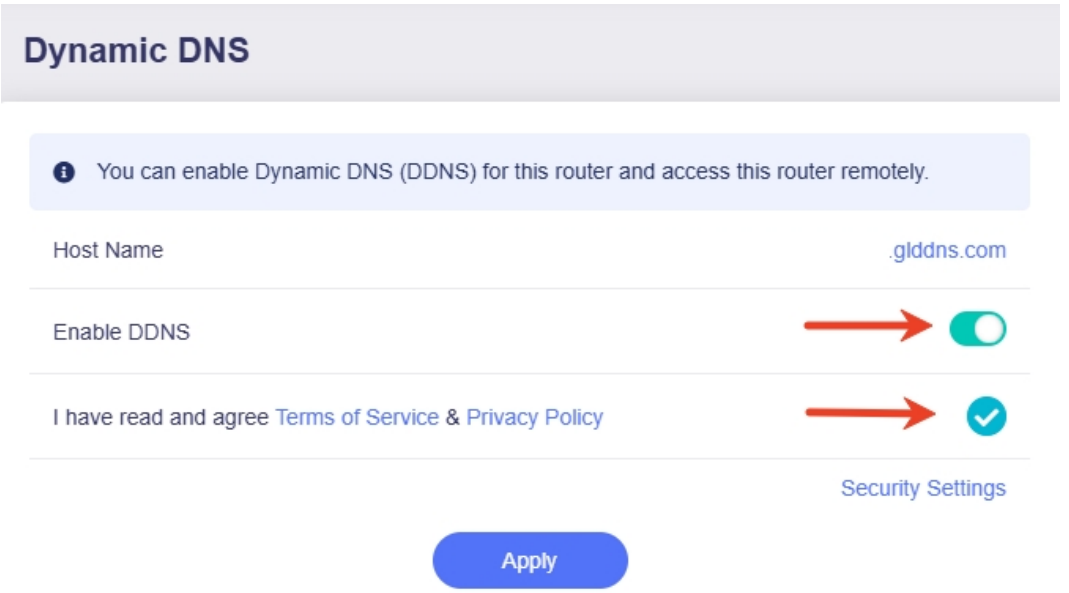
   - Ersetzen Sie „xxxxxxx.glddns.com“ in der obigen Abbildung durch Ihren Hostnamen.
   - „8.8.8.8“ ist ein DNS-Server von Google. Verwenden Sie diesen oder ersetzen Sie ihn durch einen anderen DNS-Server und drücken Sie die Eingabetaste.
2. Wenn eine öffentliche IP-Adresse wie „183.178.10.100“ in der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

12.2.3 HTTPS-Fernzugriff

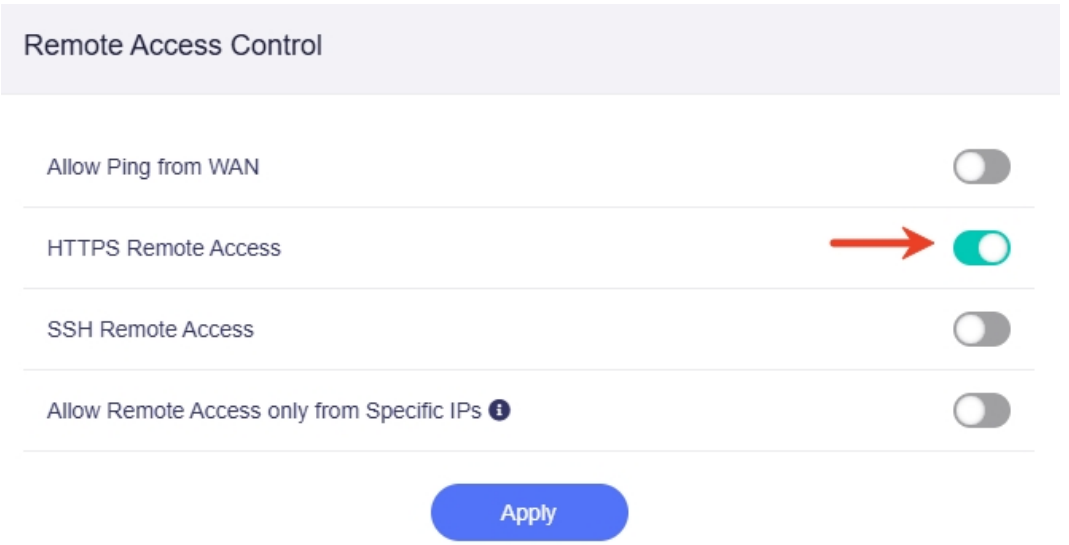
Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 443** ein.

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

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

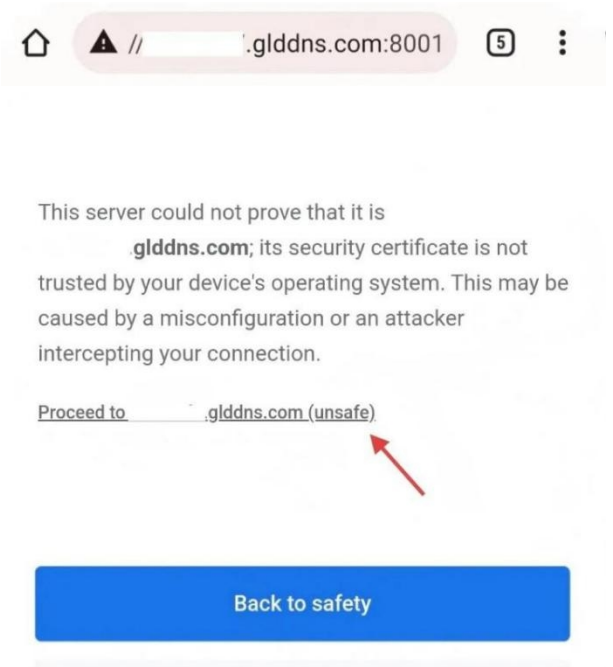


2. Öffnen Sie in der Weboberfläche **SYSTEM** > **Security** > **Remote Access Control**. Aktivieren Sie **HTTPS Remote Access** und klicken Sie auf **Apply**.



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.



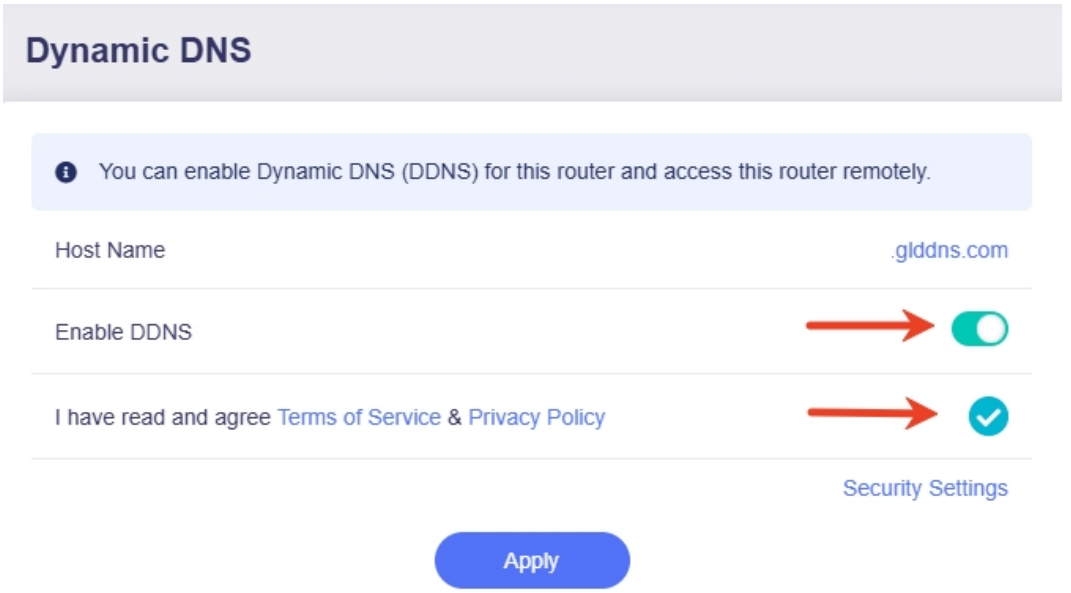
Sie können nun über den DDNS-Hostnamen per **HTTPS** auf die Weboberfläche des Routers zugreifen.

12.2.4 SSH-Fernzugriff

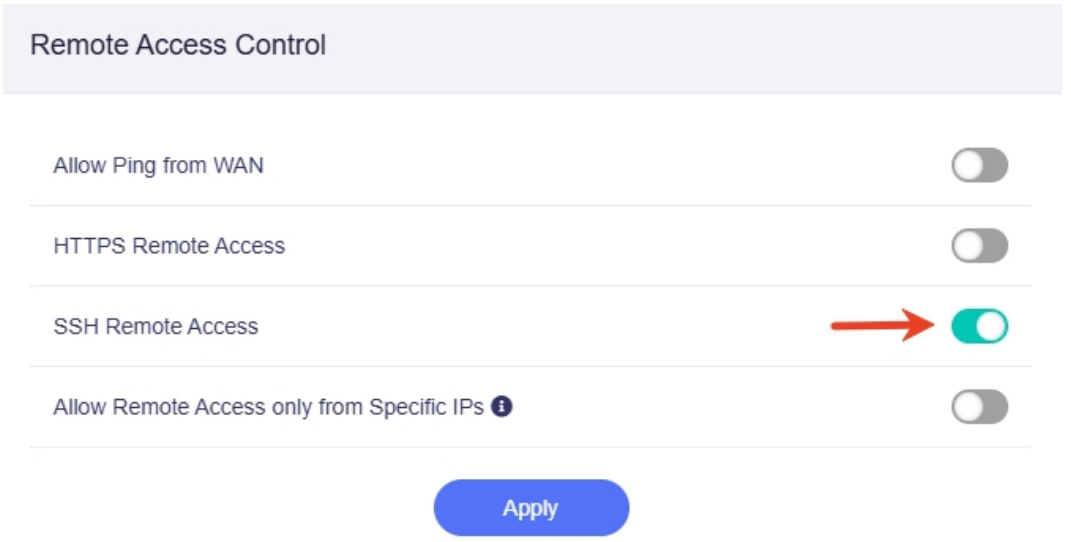
Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Prüfen Sie hier, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Falls sich Ihr Router hinter NAT befindet, richten Sie auf dem vorgeschalteten Router eine Portweiterleitung für **Port 22** ein.

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

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



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



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

12.3 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.

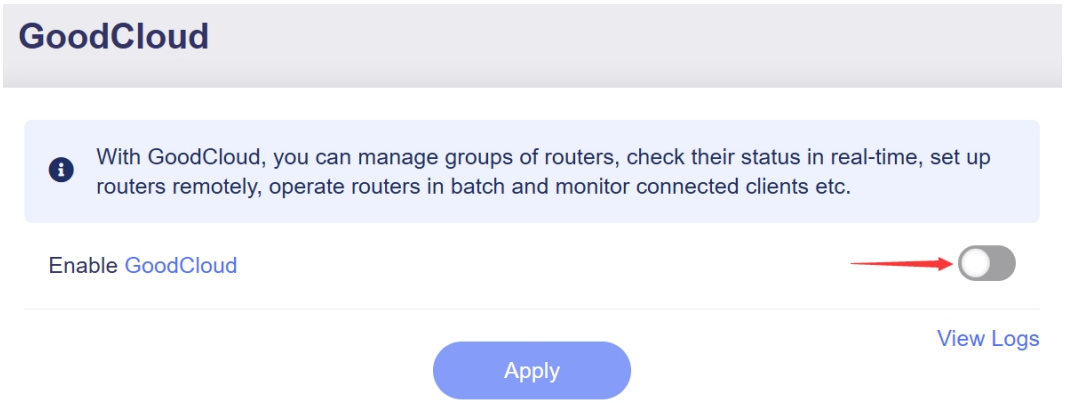
Mit GoodCloud können Sie:

- 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

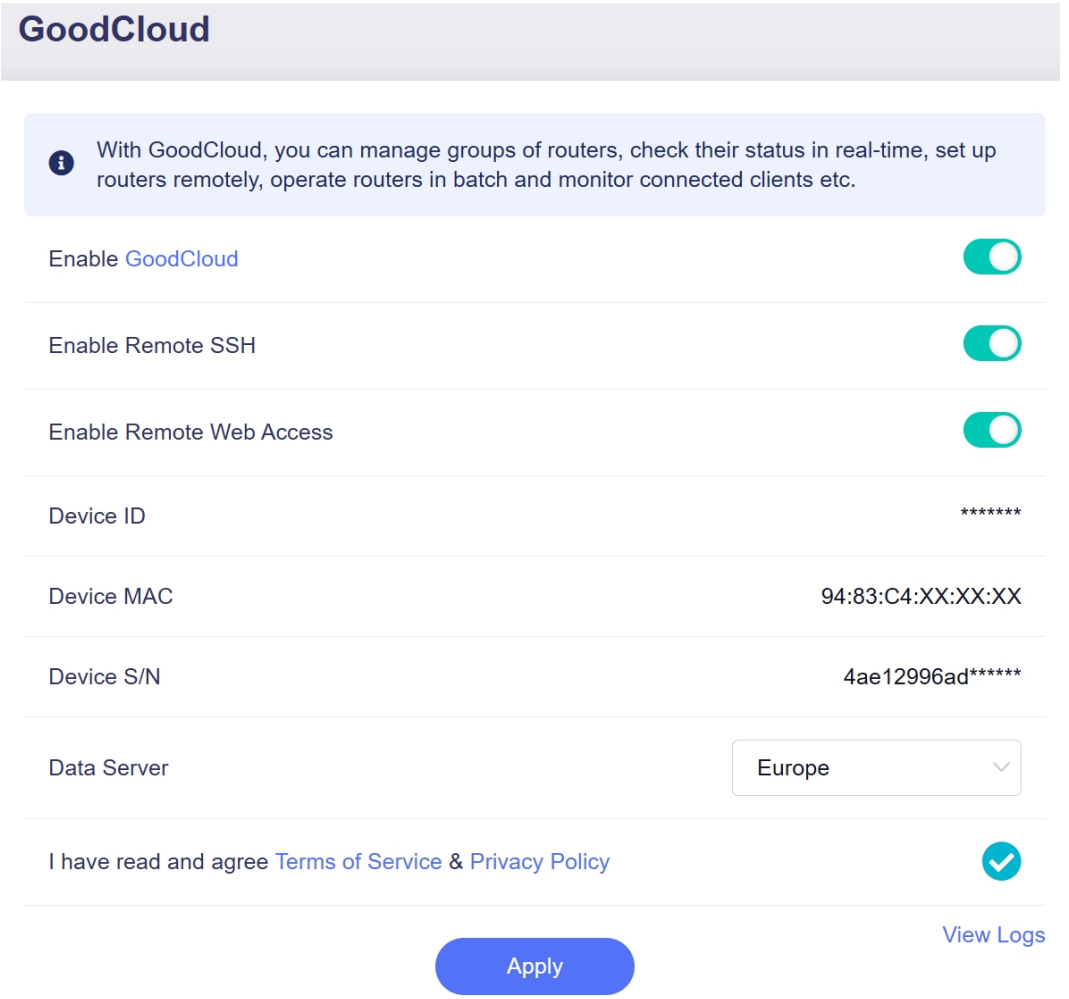
Einige Funktionen sind im Enterprise-Tarif und im VAR-Tarif (Value Added Reseller) verfügbar. Weitere Informationen finden Sie hier.

12.3.1 GoodCloud aktivieren

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

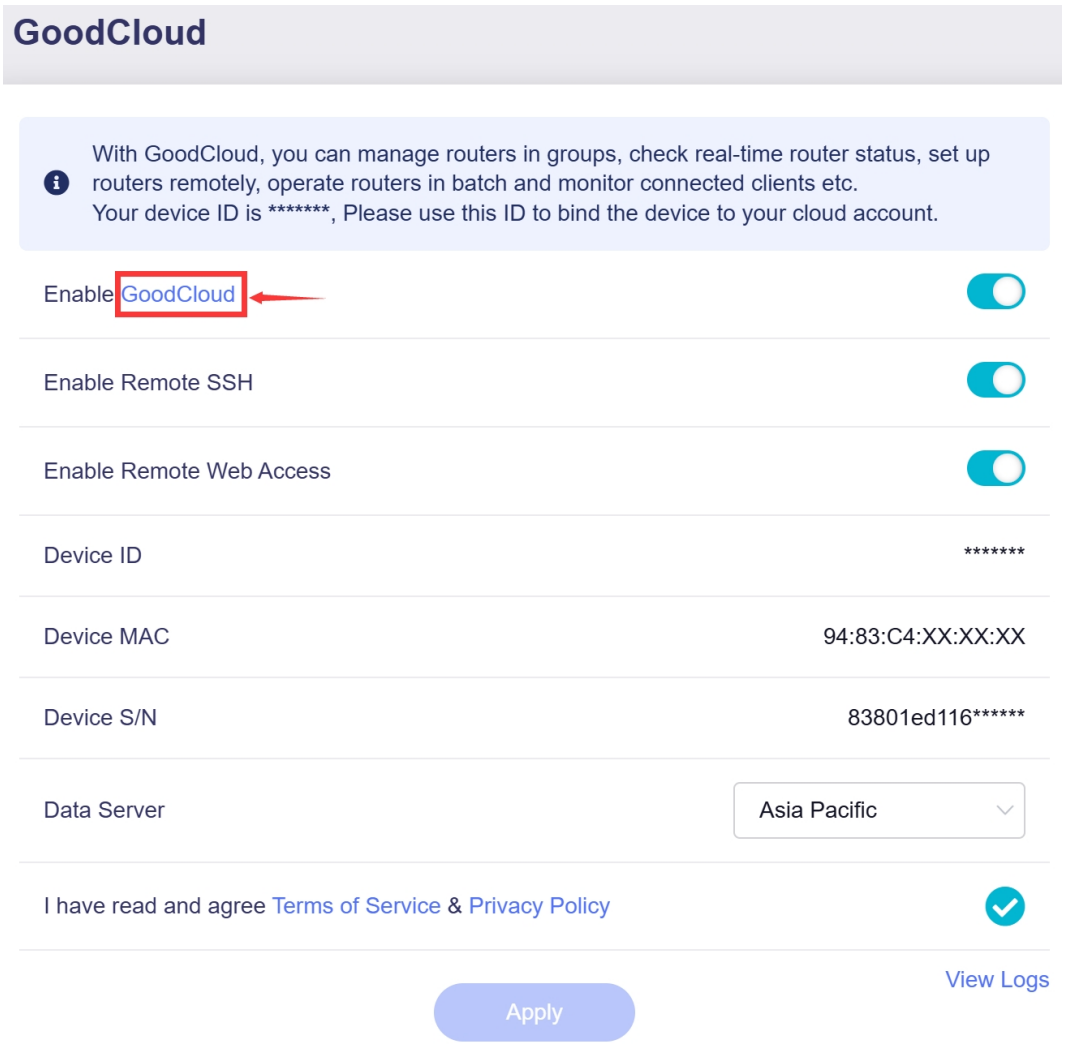


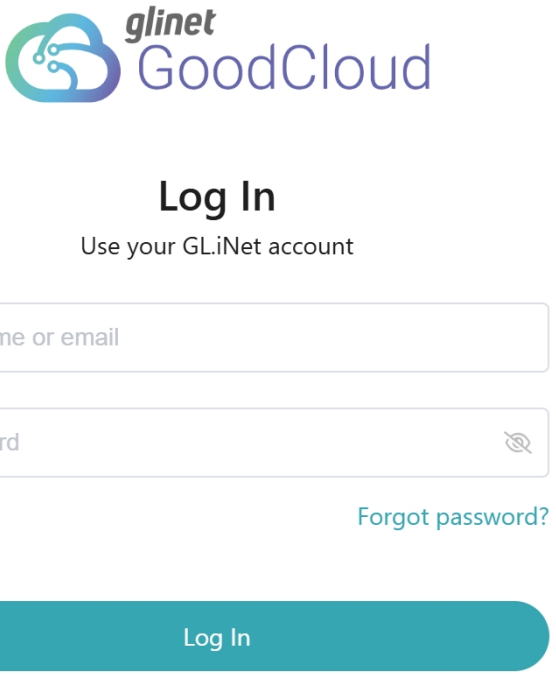
   Aktivieren Sie bei Bedarf **Remote SSH** und **Remote Web Access**. Wählen Sie den nächstgelegenen Server aus, lesen und akzeptieren Sie die **Terms of Service & Privacy Policy** und klicken Sie auf **Apply**.



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

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

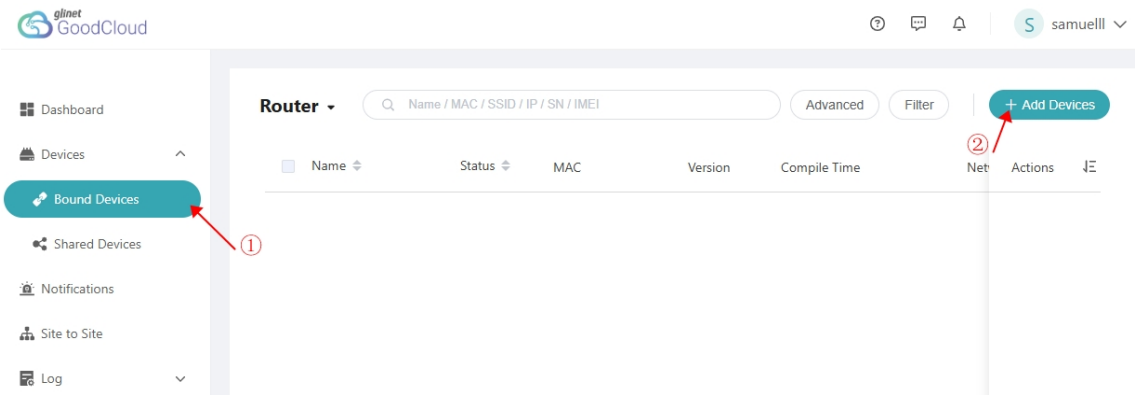

GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is *******, Please use this ID to bind the device to your cloud account.
Enable GoodCloud
Enable Remote SSH
Enable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



Tipps:

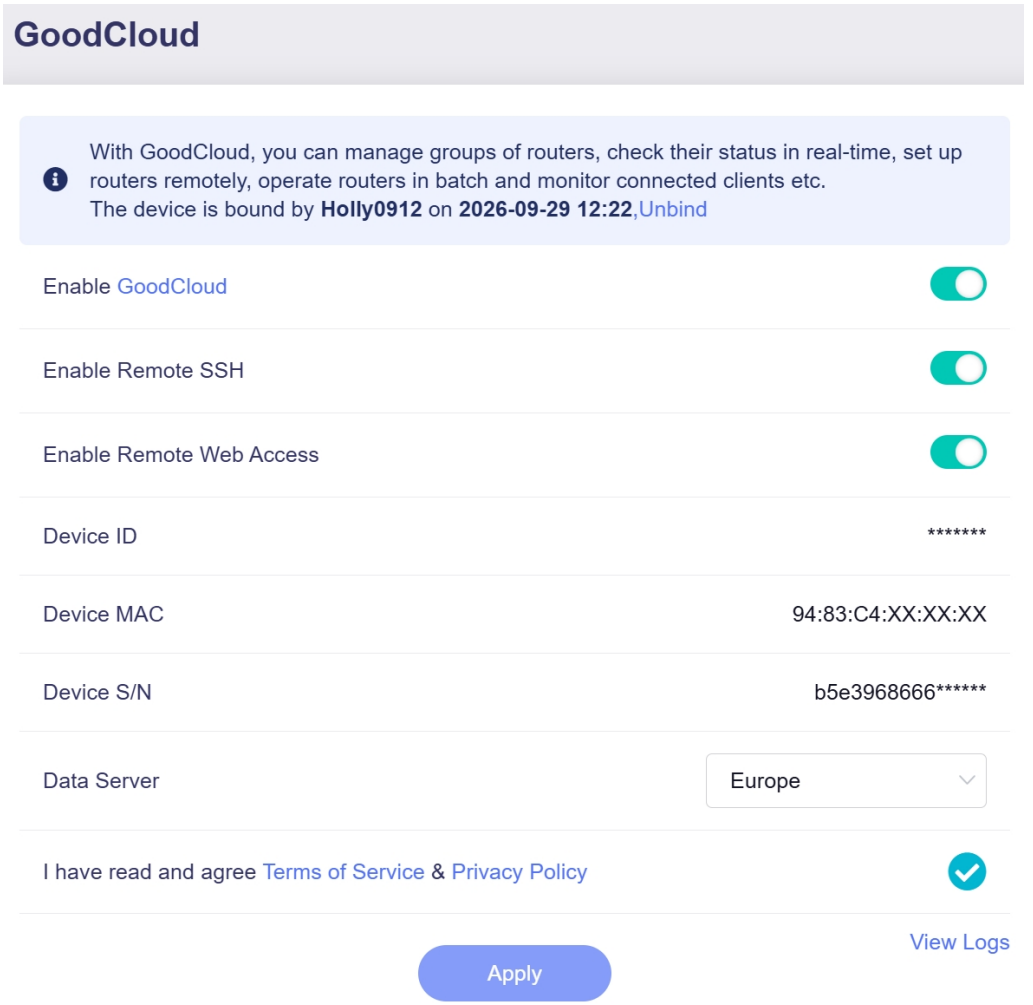
- Die Schritte zur Verknüpfung mit GoodCloud unterscheiden sich je nach Firmwareversion.
- Falls Sie keine Bestätigungs-E-Mail erhalten, prüfen Sie Ihren Spamordner oder versuchen Sie es später erneut. Weitere Unterstützung erhalten Sie unter support@gl-inet.com.

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



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

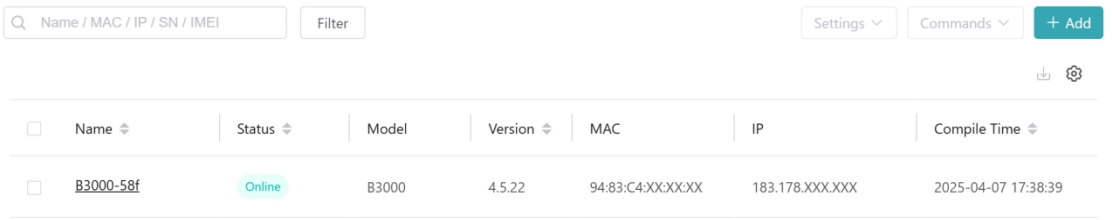
4. Kehren Sie nach erfolgreicher Verknüpfung zur Weboberfläche des Routers zurück und öffnen Sie **APPLICATIONS** > **GoodCloud**. Auf dieser Seite erscheinen die Verknüpfungsdaten, darunter Benutzername und Zeitpunkt.



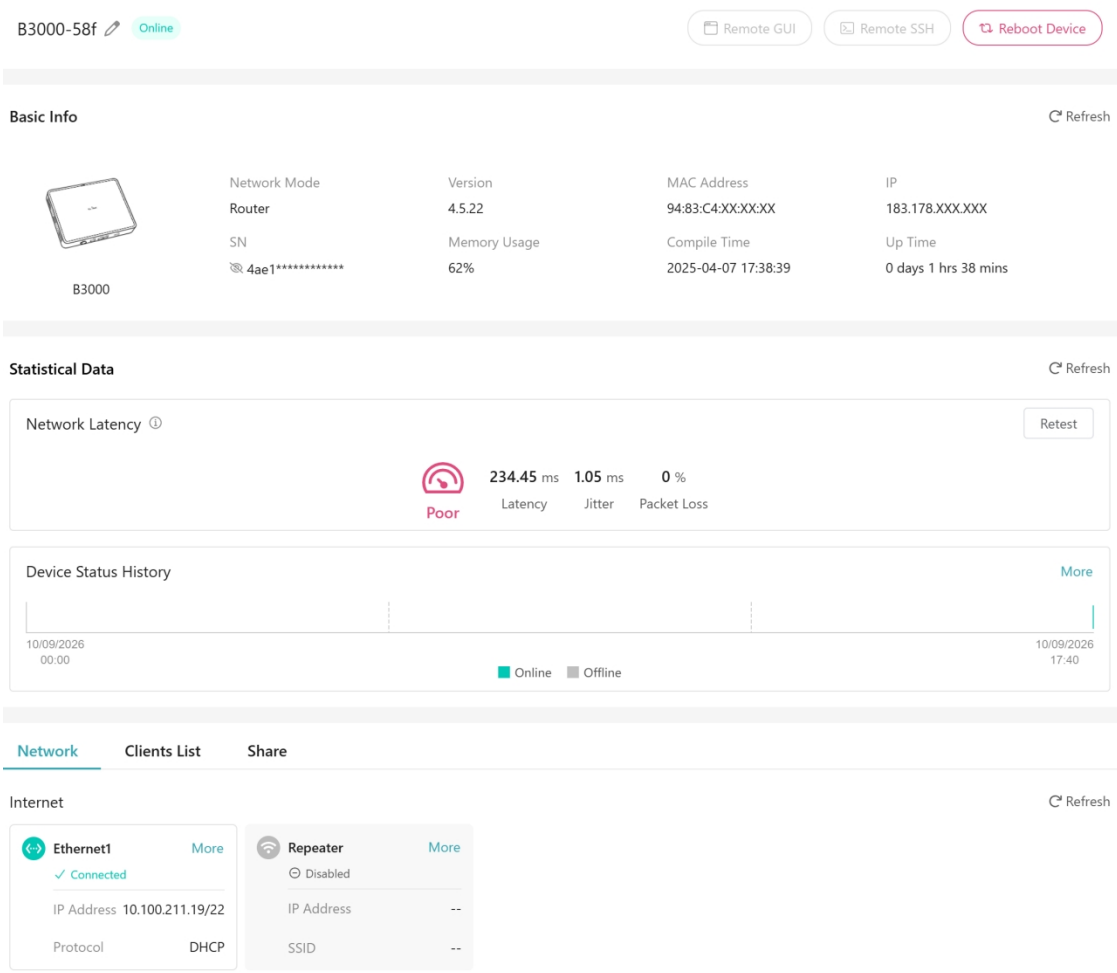
12.3.2 Router verwalten

Gerätedetails prüfen

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

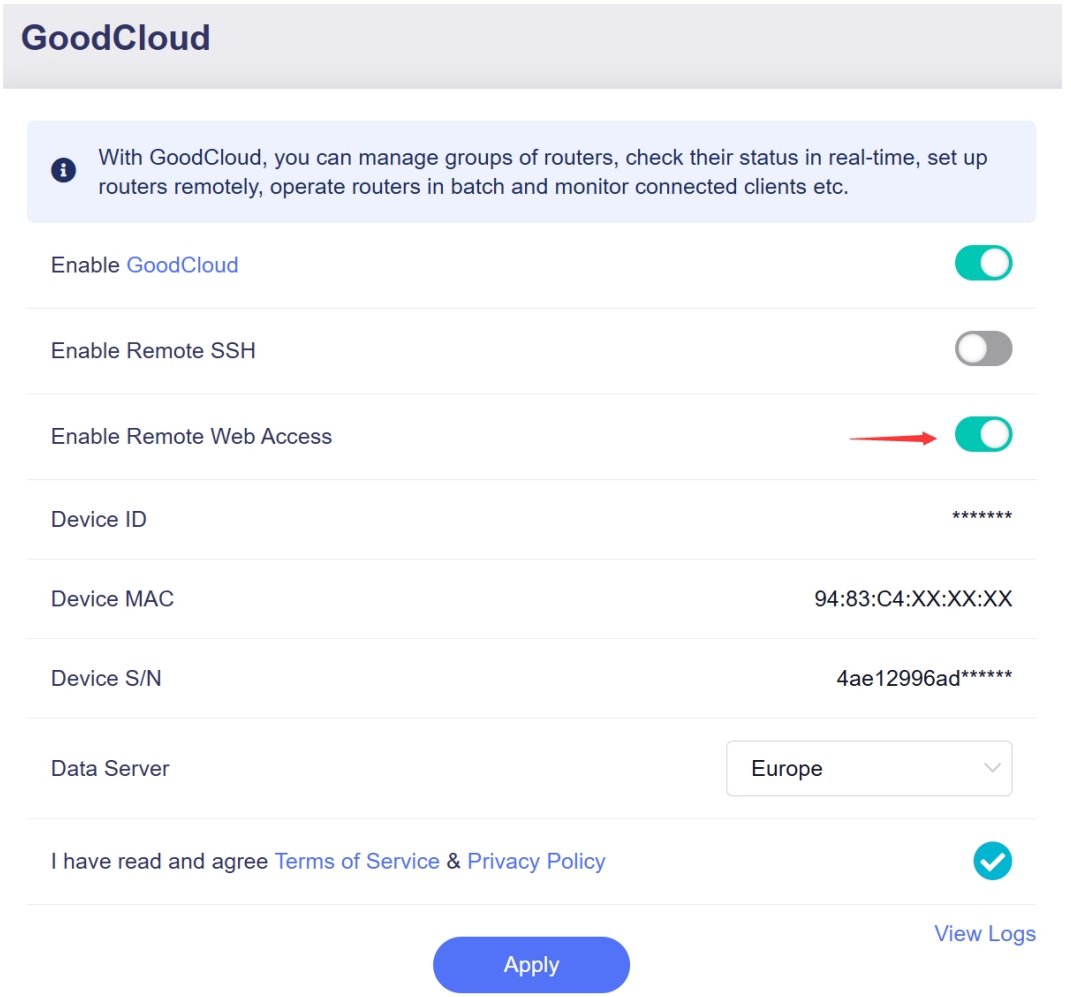


Klicken Sie auf den Gerätenamen, um die Detailseite zu öffnen. Diese enthält grundlegende Informationen, Statistiken, eine Netzwerkübersicht, die Geräteliste und eine Zeitleiste. Außerdem können Sie erweiterte Aktionen ausführen, etwa aus der Ferne auf den Router zugreifen oder ihn neu starten.

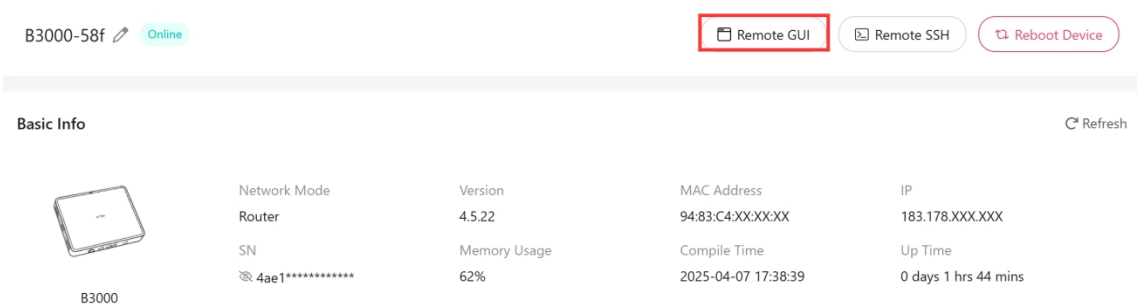

B3000-58f
Online
Remote GUI
Remote SSH
Reboot Device
Basic Info
Refresh
B3000
Network Mode
Router
Version
4.5.22
MAC Address
94:83:C4:XX:XX:XX
IP
183.178.XXX.XXX
SN
4ae1**********
Memory Usage
62%
Compile Time
2025-04-07 17:38:39
Up Time
0 days 1 hrs 38 mins
Statistical Data
Refresh
Network Latency
Retest
Poor
234.45 ms
Latency
1.05 ms
Jitter
0 %
Packet Loss
Device Status History
More
10/09/2026
00:00
10/09/2026
17:40
Online
Offline
Network
Clients List
Share
Internet
Refresh
Ethernet1
More
Connected
IP Address 10.100.211.19/22
Protocol DHCP
Repeater
More
Disabled
IP Address --
SSID --

Fernzugriff auf die Weboberfläche

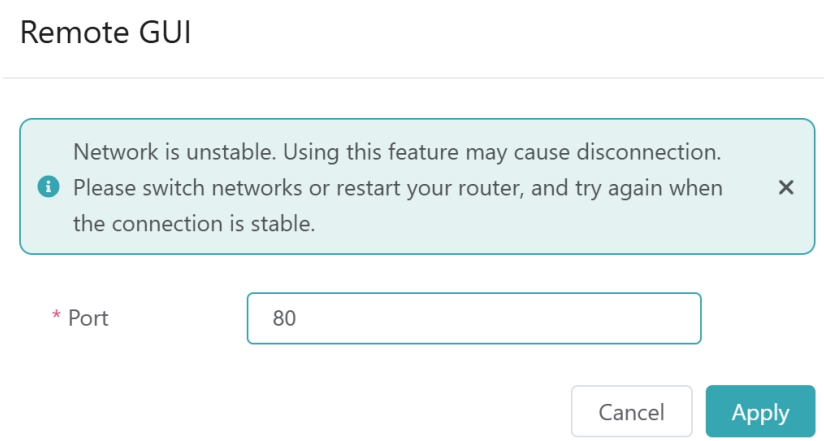
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **APPLICATIONS** > **GoodCloud**, aktivieren Sie **Remote Web Access** und klicken Sie auf **Apply**.



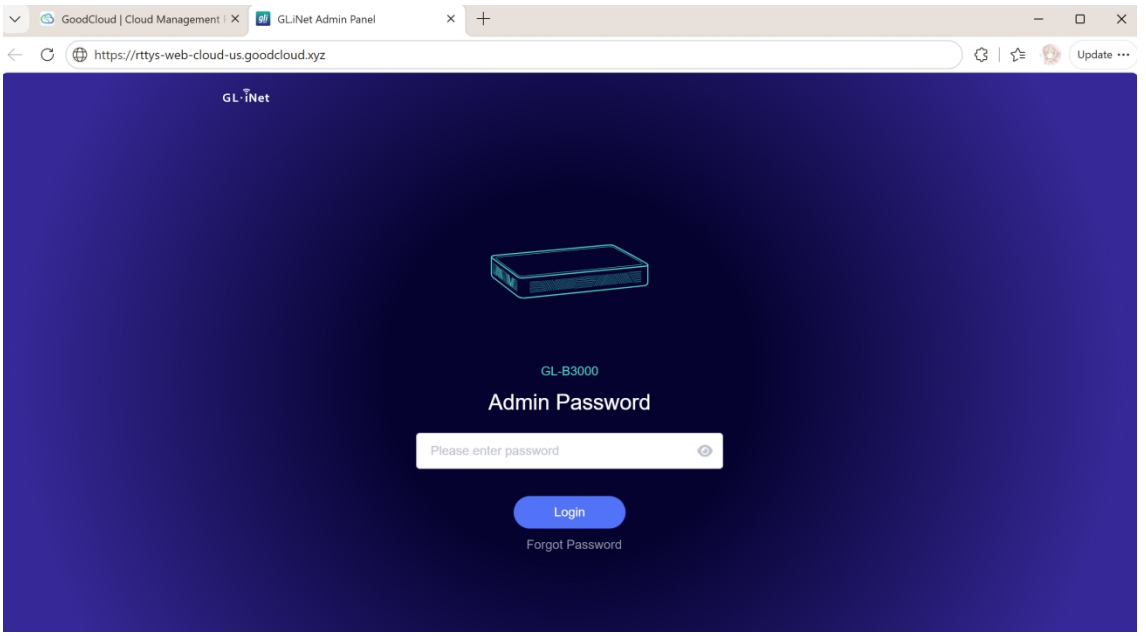
2. Melden Sie sich bei GoodCloud an und öffnen Sie **Devices** > **Bound Devices**. Klicken Sie auf das gewünschte Gerät, um dessen Detailseite zu öffnen.
3. Klicken Sie auf der Gerätedetailseite oben rechts auf **Remote GUI**.



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

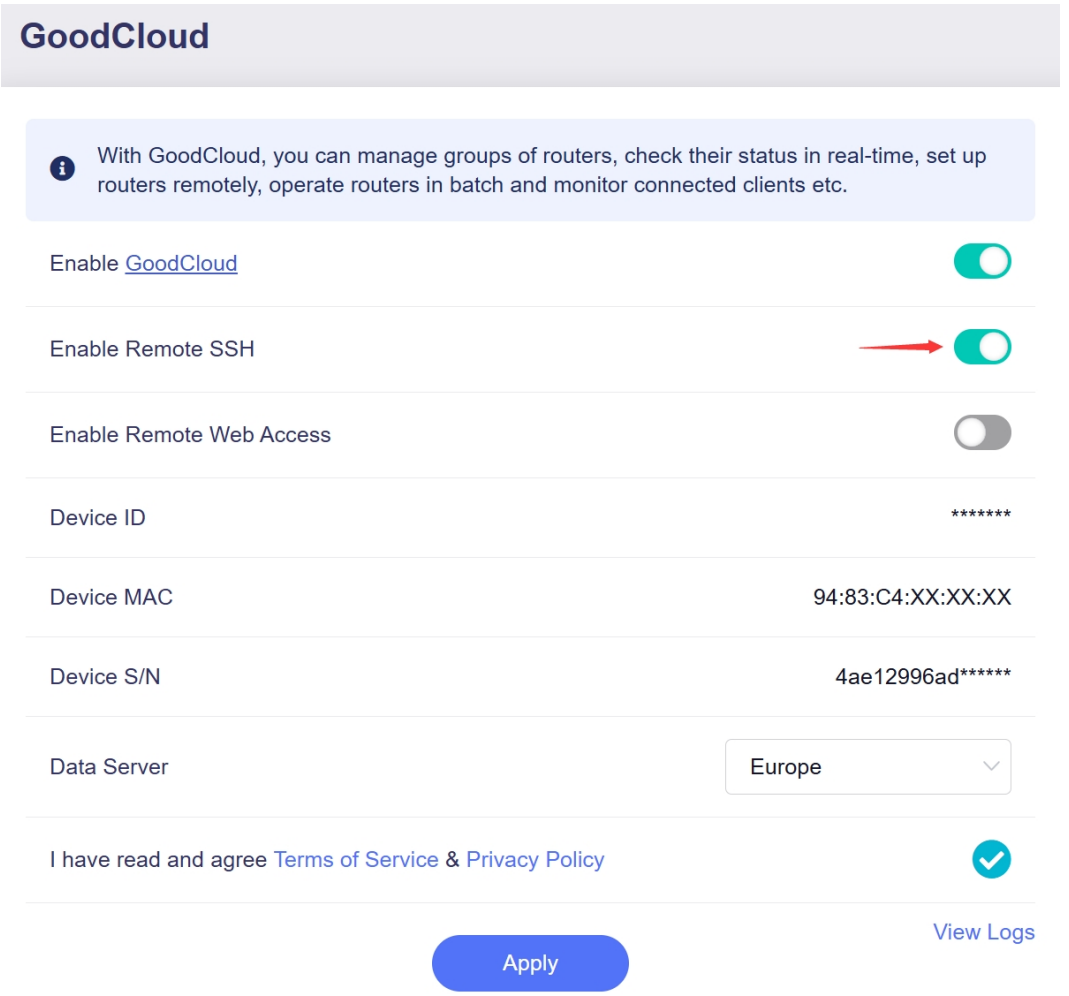


5. Sie werden zur Anmeldeseite des Routers weitergeleitet. Geben Sie das Administratorpasswort ein, um aus der Ferne auf die Weboberfläche zuzugreifen.

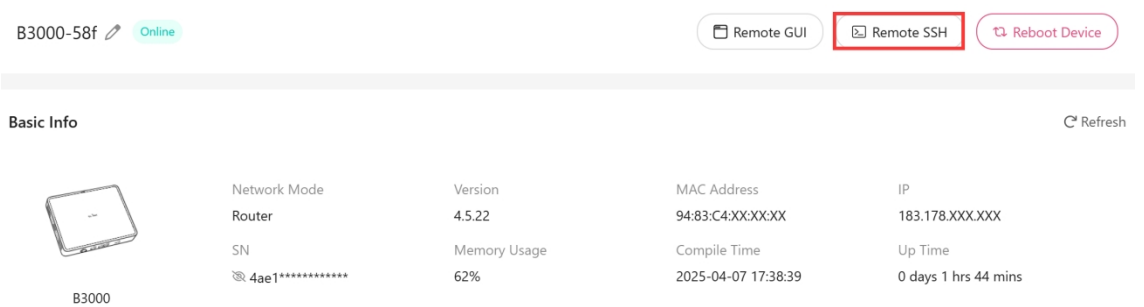


SSH-Fernzugriff

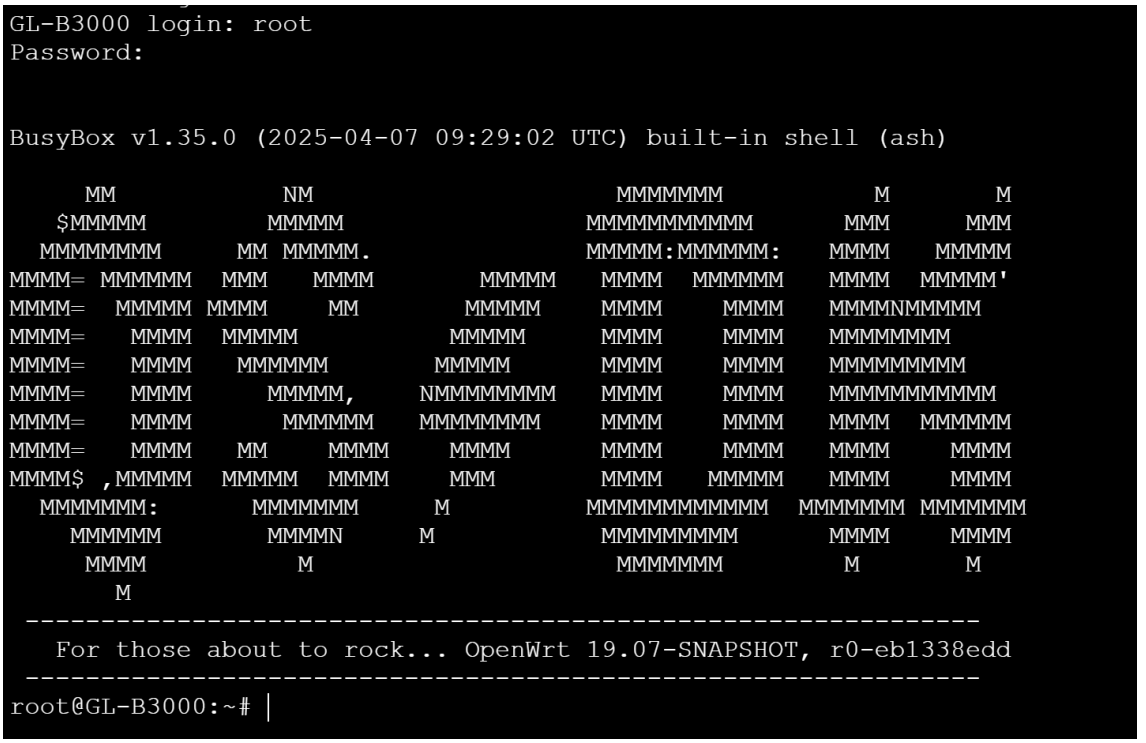
1. Melden Sie sich an der Weboberfläche an, öffnen Sie **APPLICATIONS** > **GoodCloud**, aktivieren Sie **Remote SSH** und klicken Sie auf **Apply**.



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

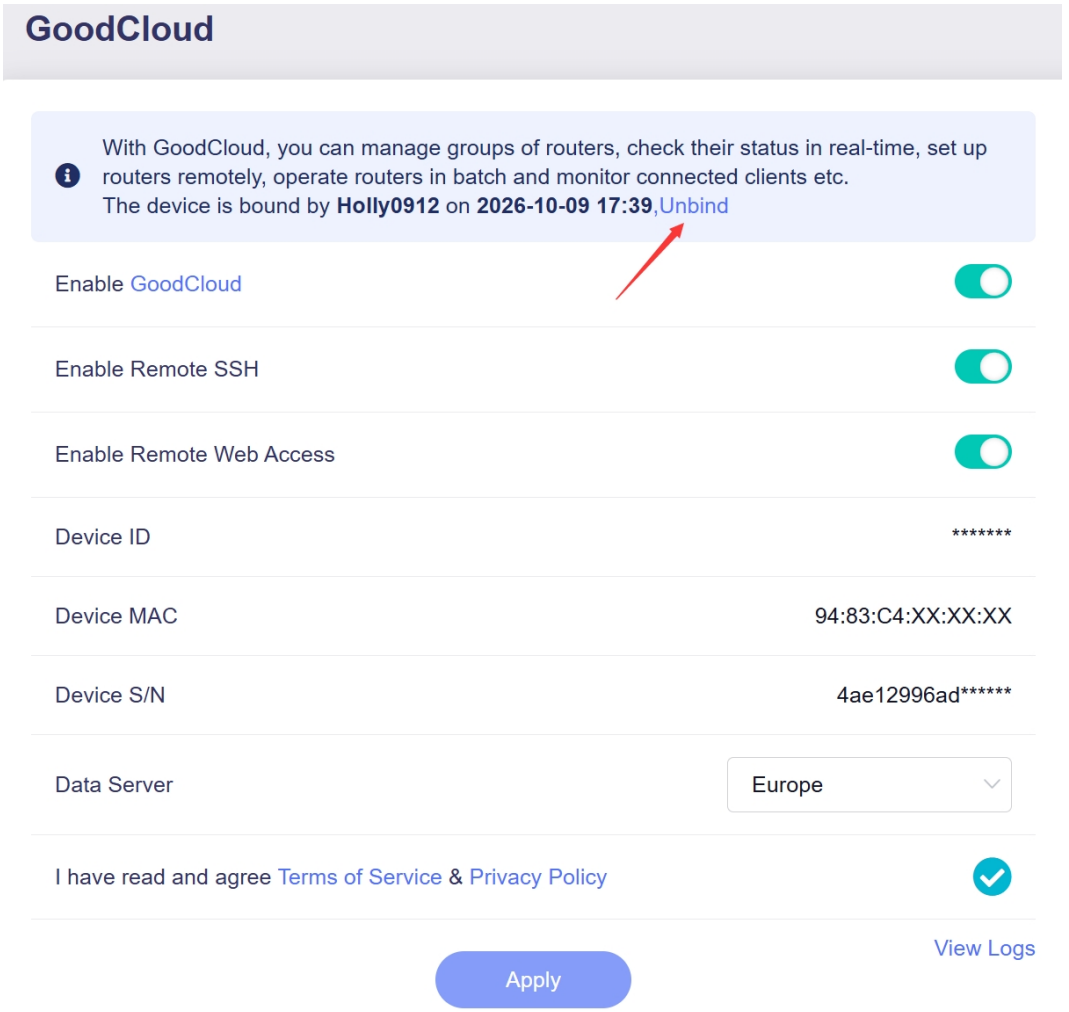


4. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

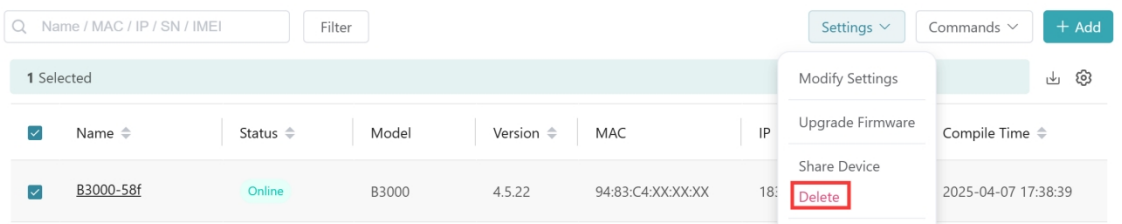


12.3.3 Geräteverknüpfung aufheben

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



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

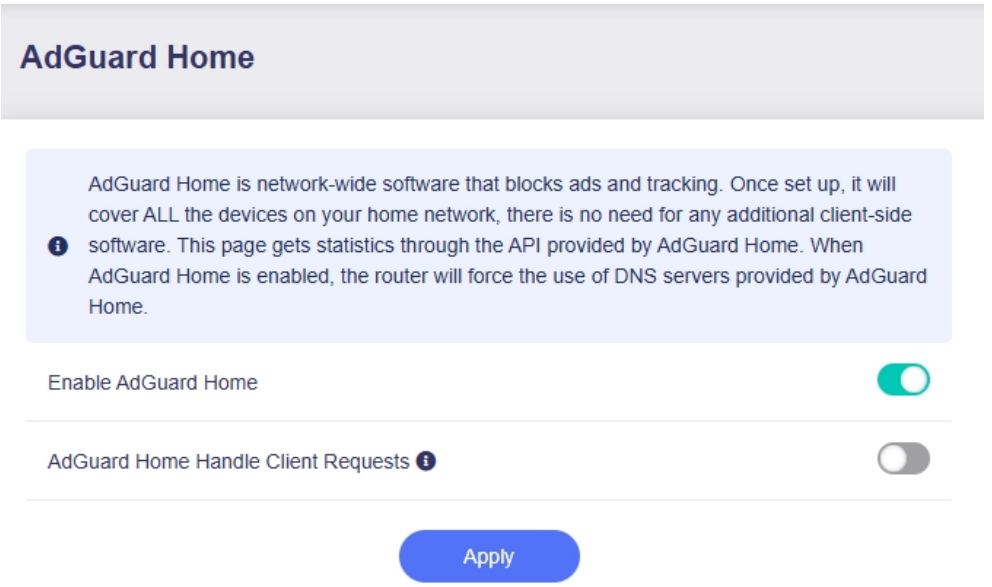


12.4 AdGuard Home

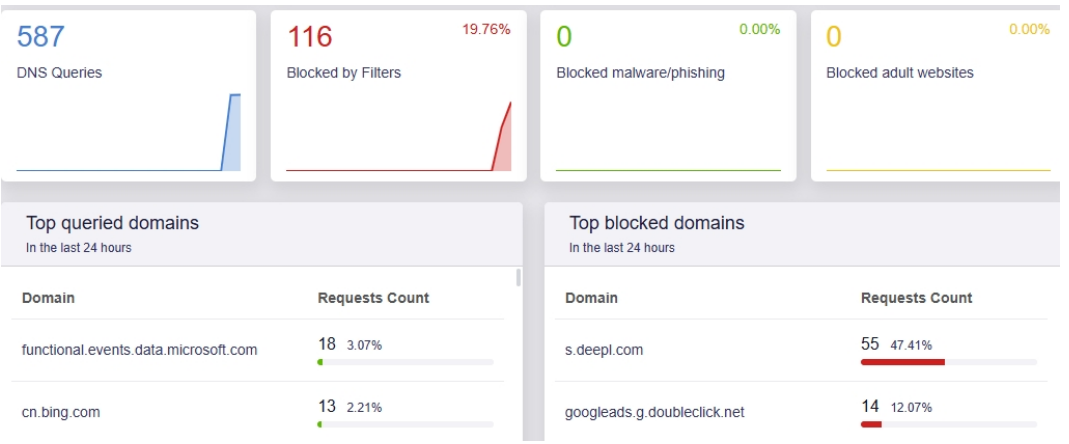
AdGuard Home blockiert Werbung und Tracking im gesamten Netzwerk. Nach der Einrichtung schützt die Software alle Endgeräte, ohne dass auf diesen zusätzliche Software installiert werden muss.

Gehen Sie wie folgt vor, um AdGuard Home einzurichten.

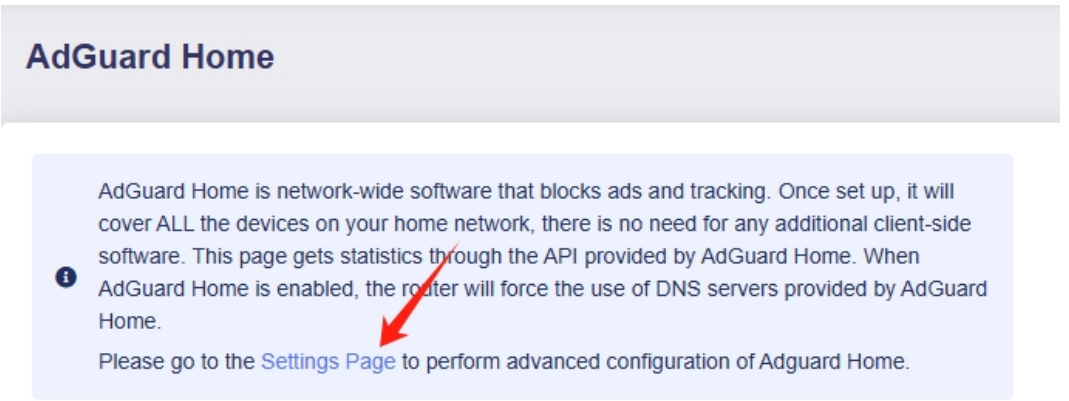
1. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **AdGuard Home**. Aktivieren Sie **Enable AdGuard Home** und klicken Sie auf **Apply**.



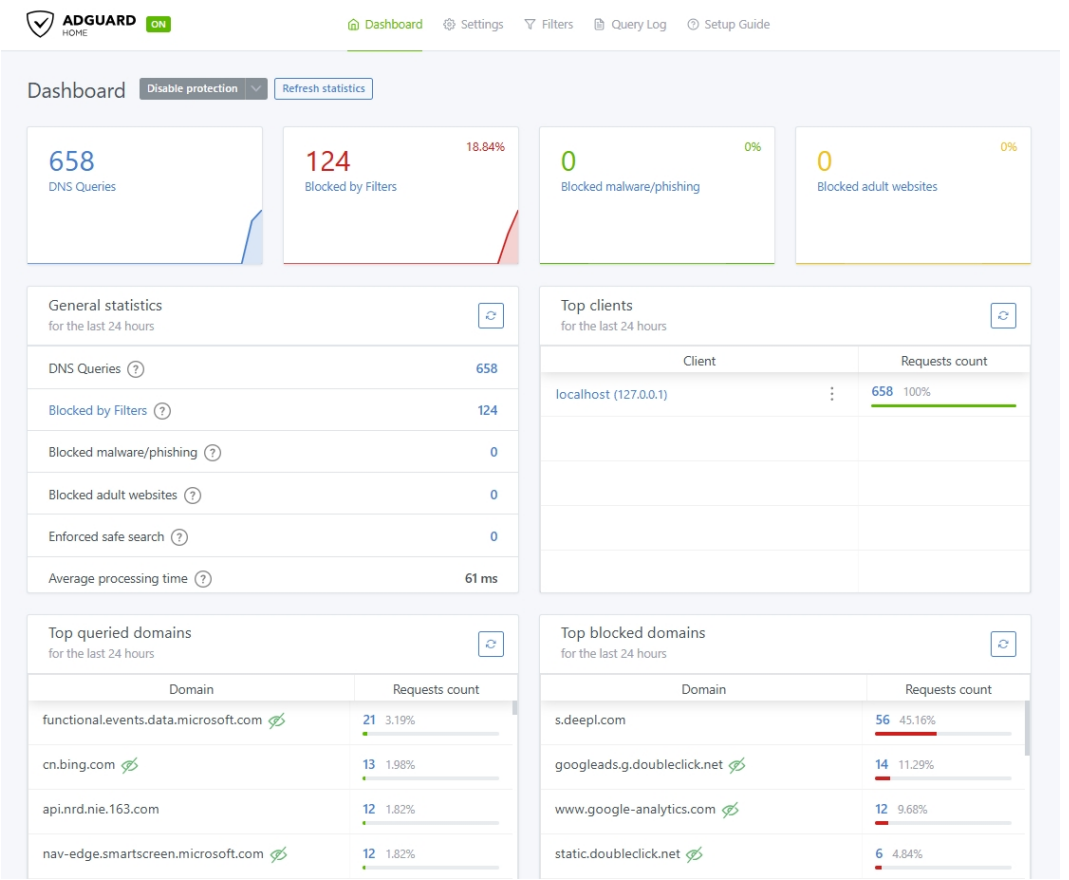
   - **AdGuard Home Handles Client Requests**: Leitet DNS-Anfragen der Endgeräte direkt an AdGuard Home weiter. Dadurch funktionieren jedoch domainbasierte VPN-Richtlinien nicht mehr.
2. Die Seite lädt automatisch DNS-Statistiken wie Anfragen und blockierte Domains über die API von AdGuard Home.



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



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


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

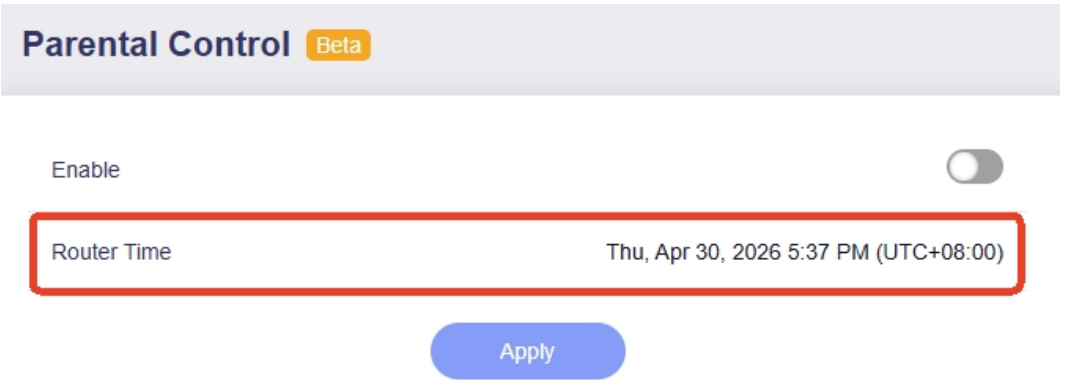
12.5 Kindersicherung

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

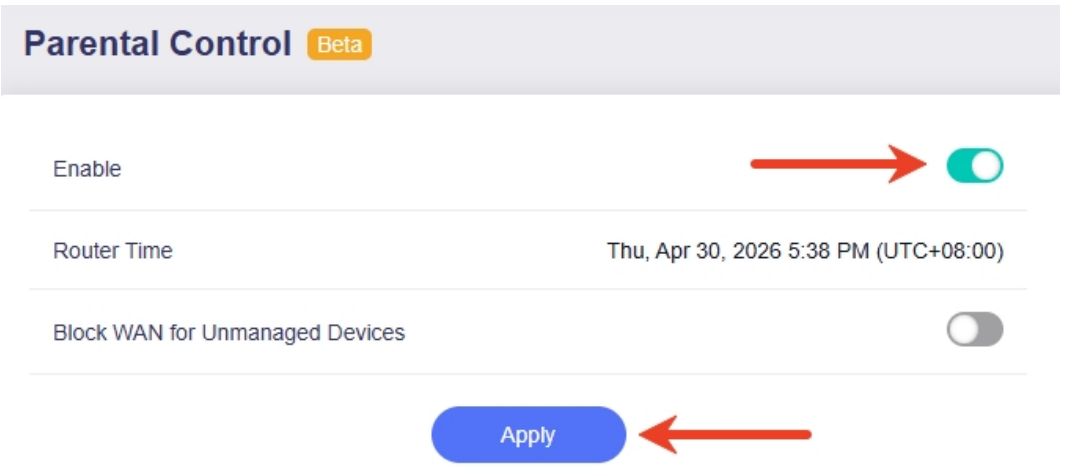
12.5.1 Schnelleinrichtung

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

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



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



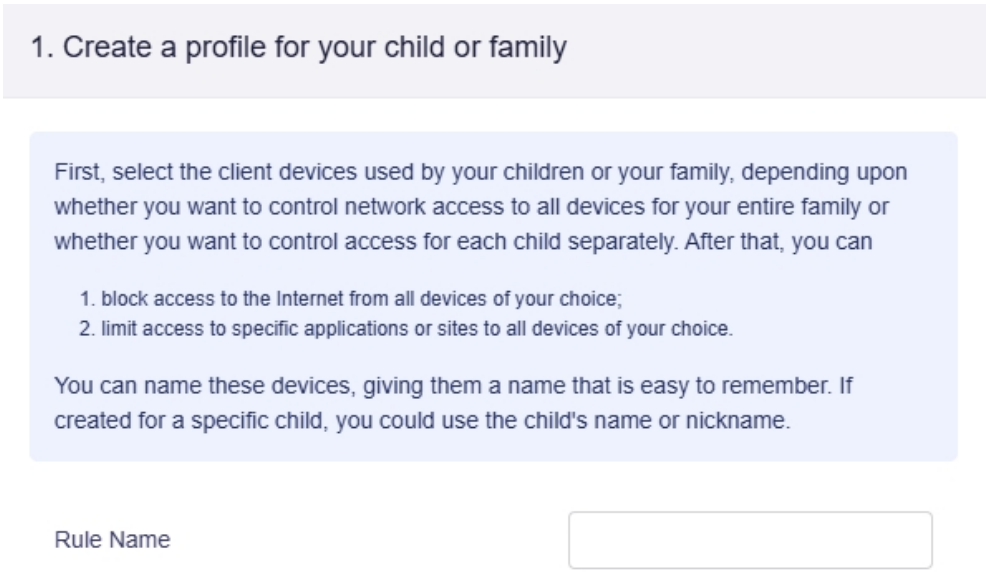
- **Block WAN for Unmanaged Devices**: Sperrt den Internetzugang für alle Geräte, die nicht in der Kindersicherungsliste stehen.

Das folgende Beispiel zeigt eine mögliche Anwendung.

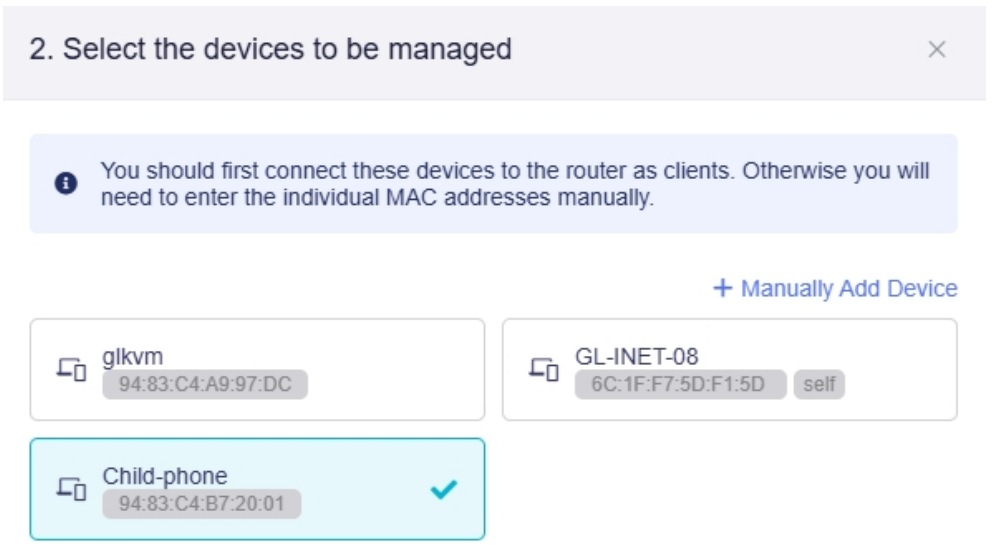
Szenario: Geräte in diesem Profil dürfen an Wochentagen von 08:00 bis 11:00 Uhr zum Lernen und am Wochenende von 18:00 bis 20:00 Uhr zum Spielen auf das Internet zugreifen. Zu allen anderen Zeiten ist der Internetzugang standardmäßig gesperrt.

Einrichtung:

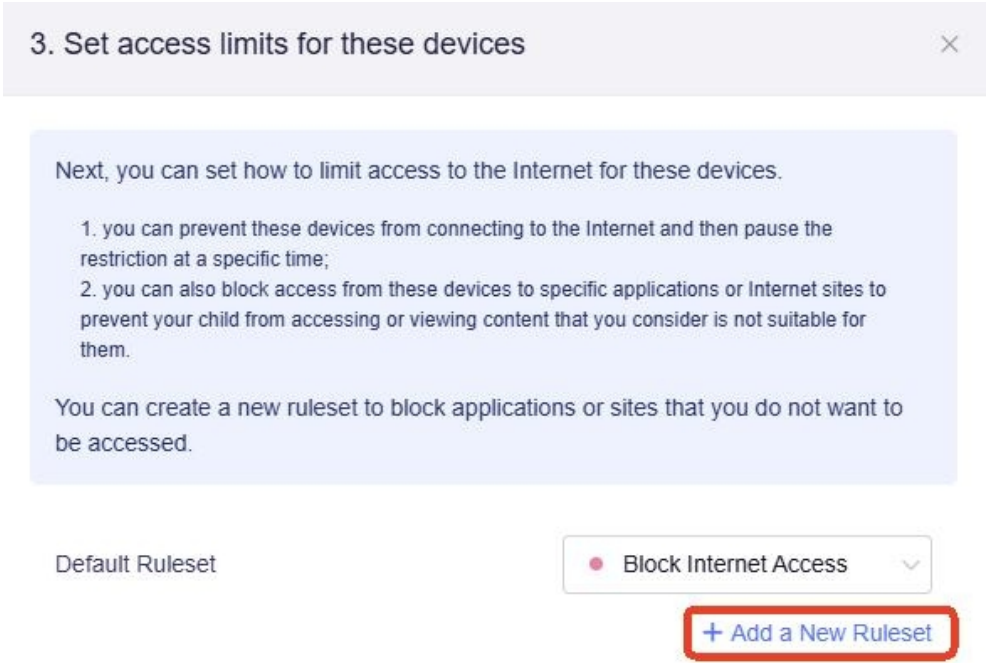
1. Erstellen Sie ein Profil und vergeben Sie einen Namen.



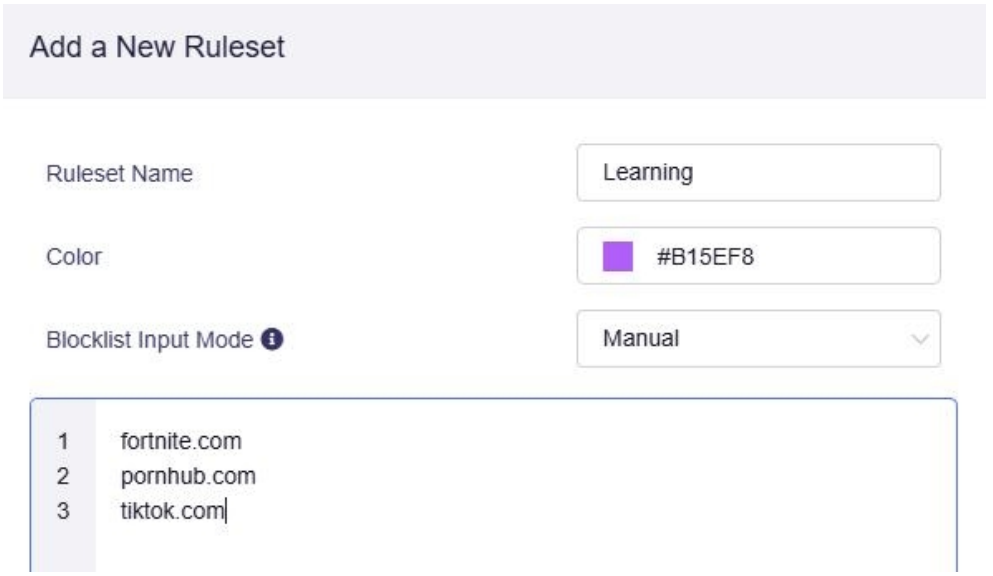
2. Wählen Sie die zu verwaltenden Geräte aus. Verbinden Sie diese zunächst mit dem Router. Noch nicht verbundene Geräte können Sie durch Eingabe ihrer MAC-Adressen manuell hinzufügen.



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

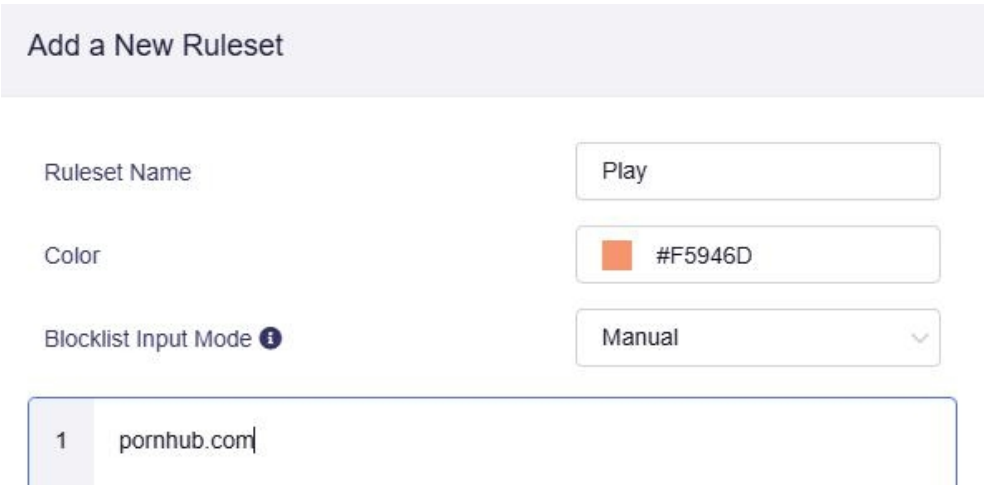


   Legen Sie Namen, etwa Learning, und Farbe des Regelsatzes fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.

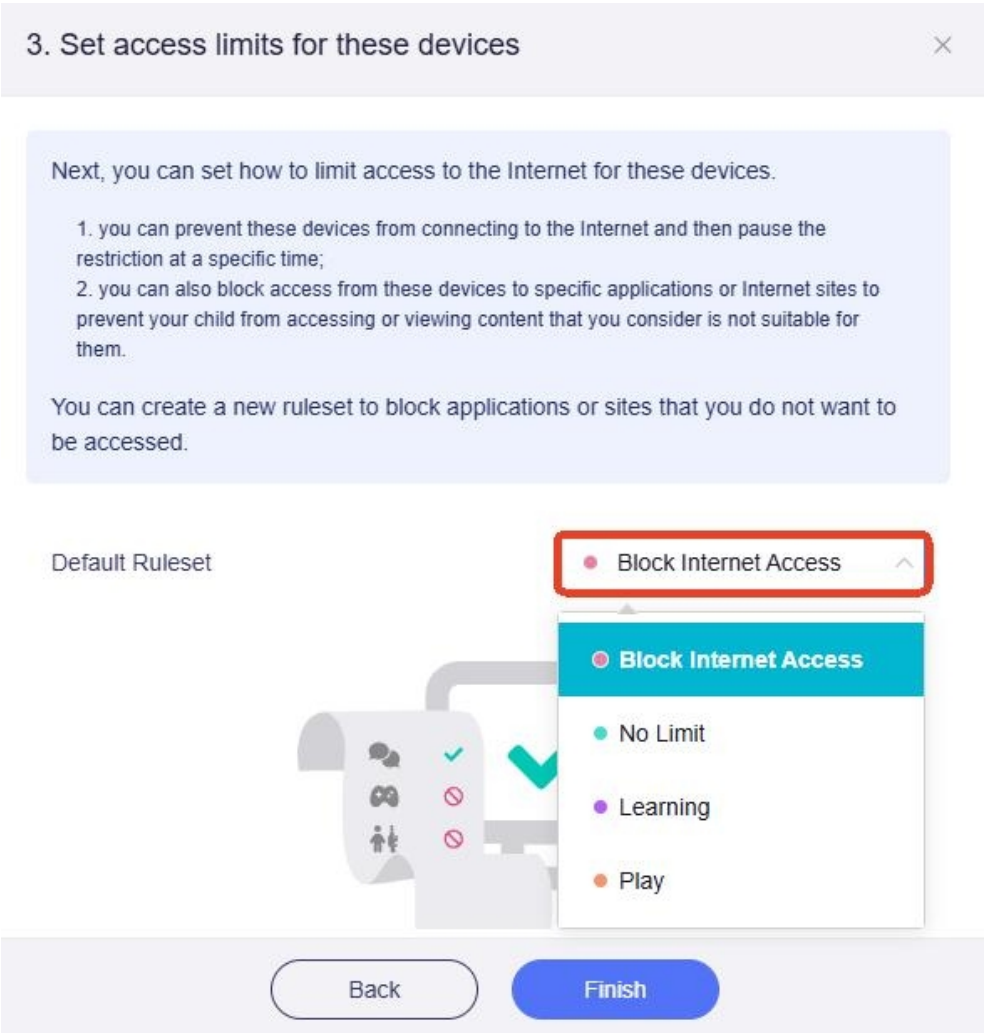


   Hinweis: Die Domainnamen auf der Sperrliste umfassen auch ihre Subdomains. Der Eintrag „example.com“ schließt beispielsweise „subdomain.example.com“ und alle weiteren Subdomains ein.

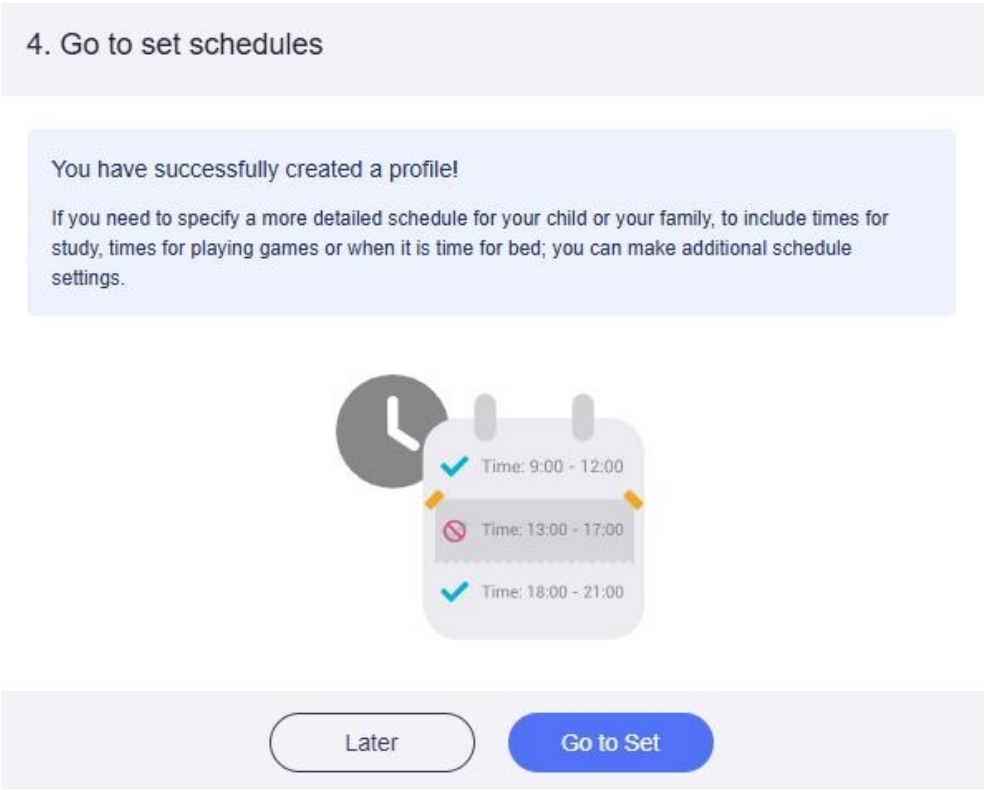
Erstellen Sie auf dieselbe Weise den zweiten Regelsatz. Legen Sie Namen, etwa Play, und Farbe fest, geben Sie die zu sperrenden Webseiten ein und klicken Sie auf **Apply**.



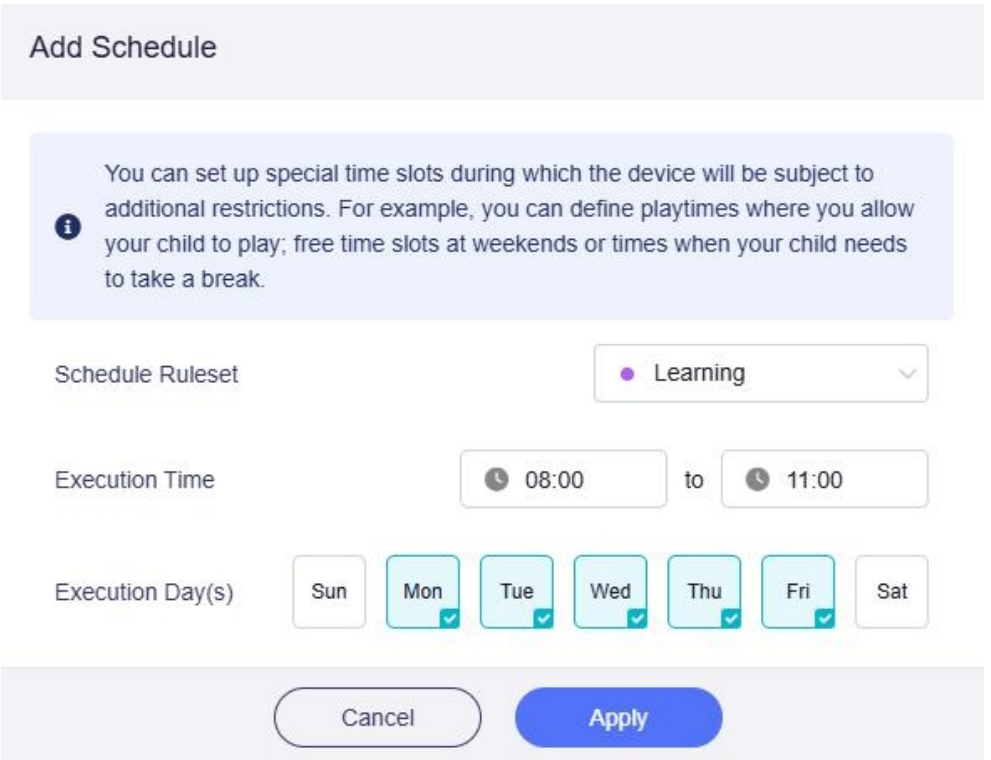
Nun sind insgesamt vier Regelsätze vorhanden. Wählen Sie **Block Internet Access** als **Default Ruleset** aus und klicken Sie auf **Finish**.



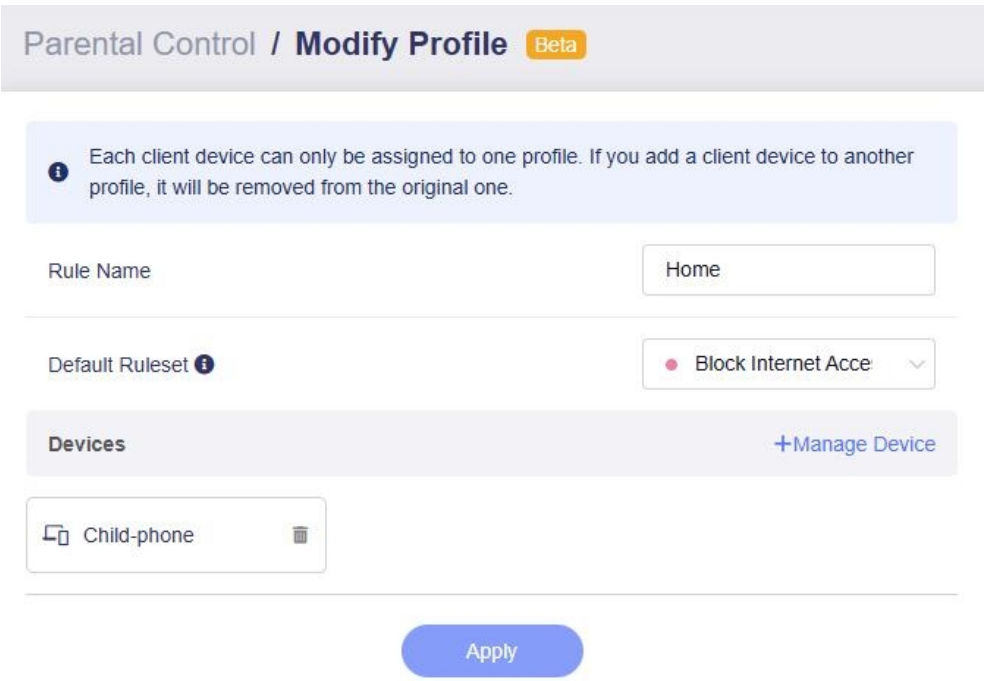
4. Erstellen Sie anschließend einen Zeitplan für Ihr Profil. Klicken Sie auf **Go to Set**.



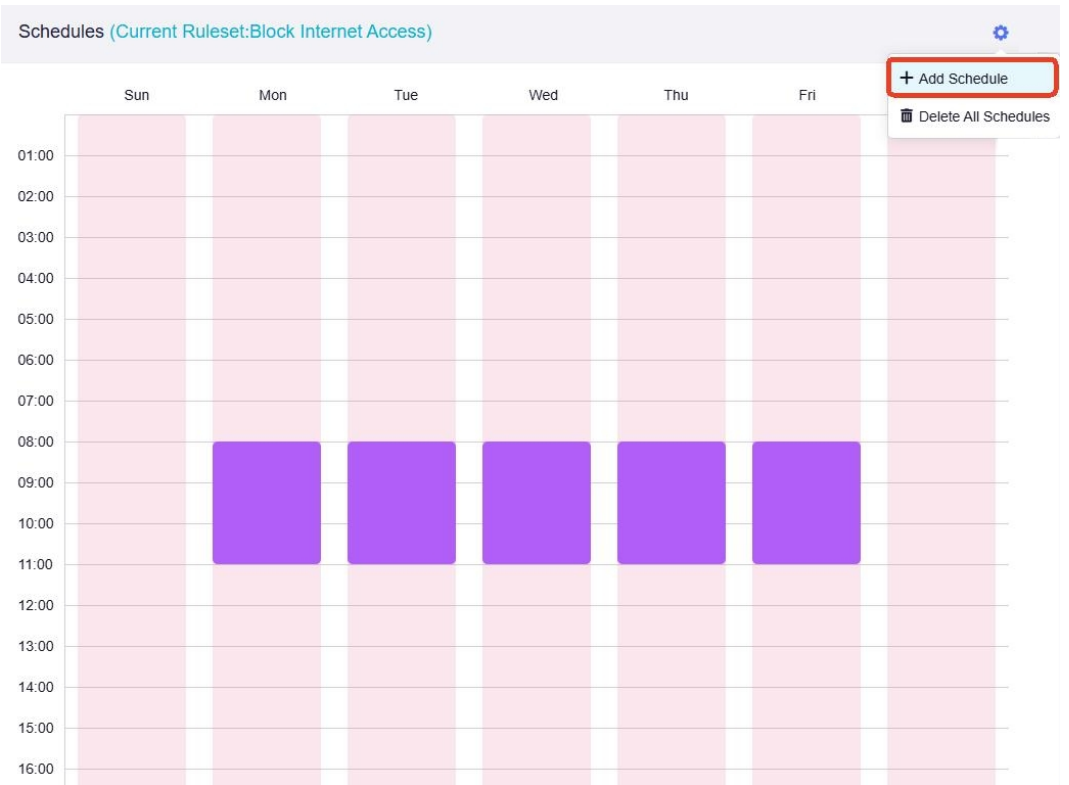
Fügen Sie den Regelsatz **Learning** zum Zeitplan hinzu. Legen Sie unter **Execution Time** an Wochentagen 08:00 bis 11:00 Uhr fest und klicken Sie auf **Apply**.



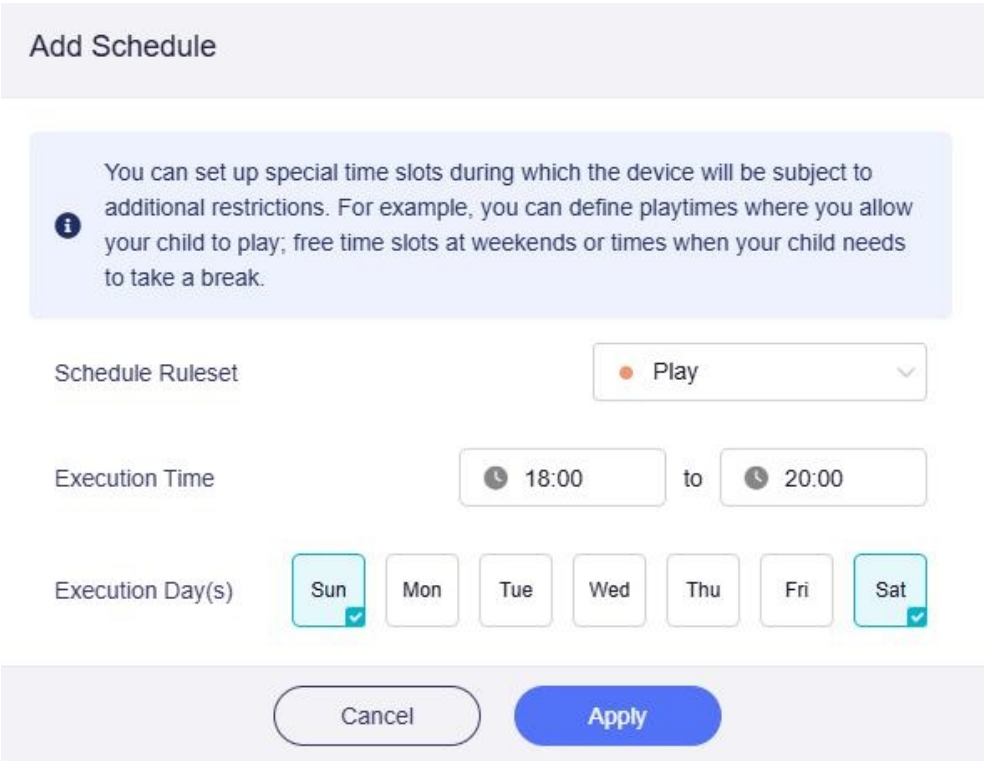
5. Sie gelangen zur Bearbeitungsseite des angelegten Profils.



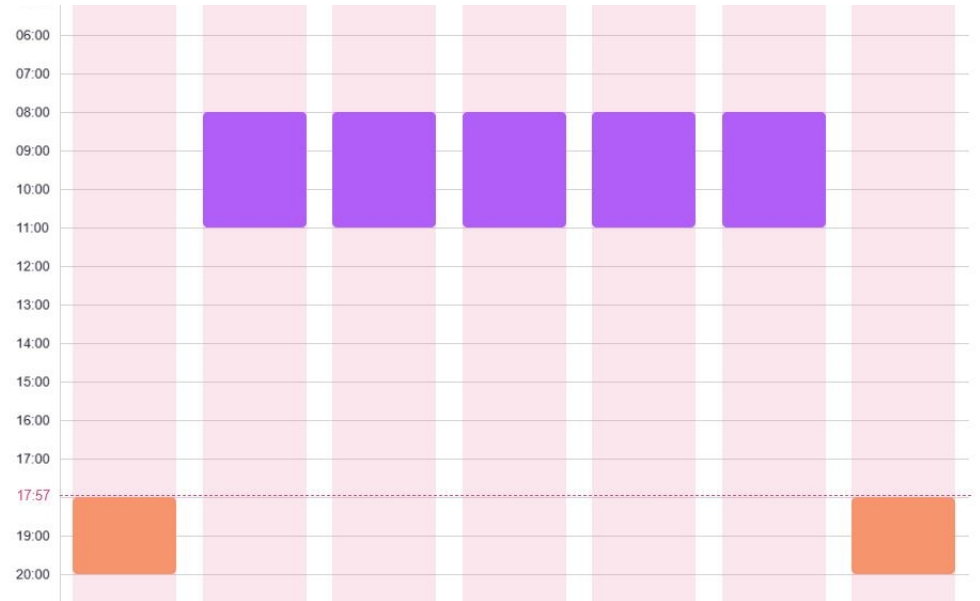
Unten sehen Sie den angelegten Zeitplan. Klicken Sie oben rechts auf das Zahnradsymbol und wählen Sie **Add Schedule**.



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



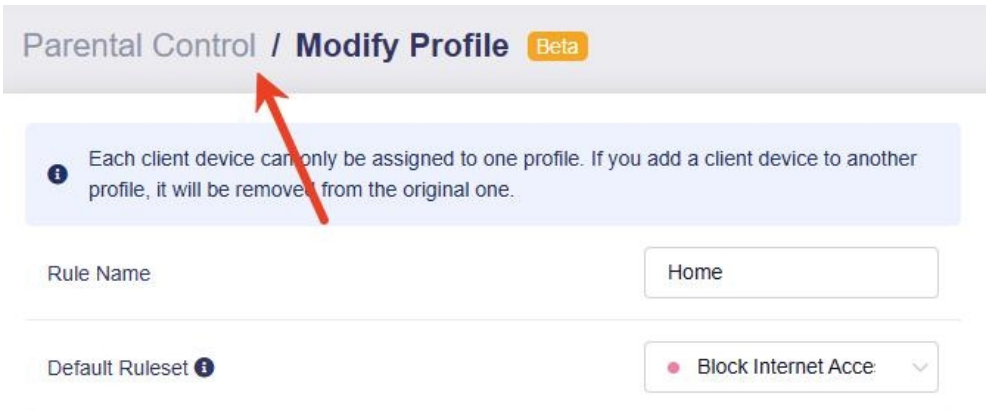
Der Regelsatz Play wird in den Zeitplan aufgenommen.



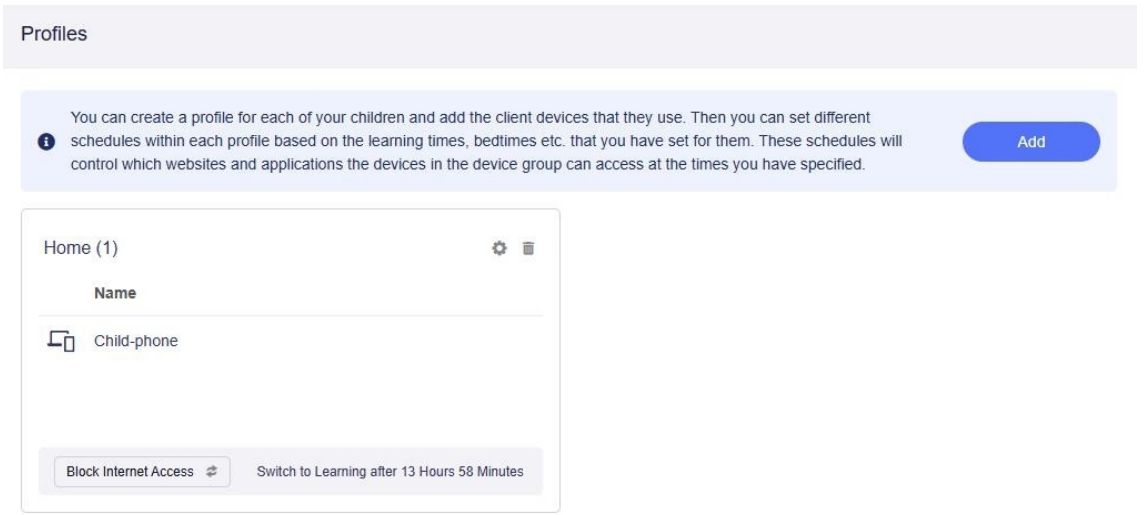
Tipps:

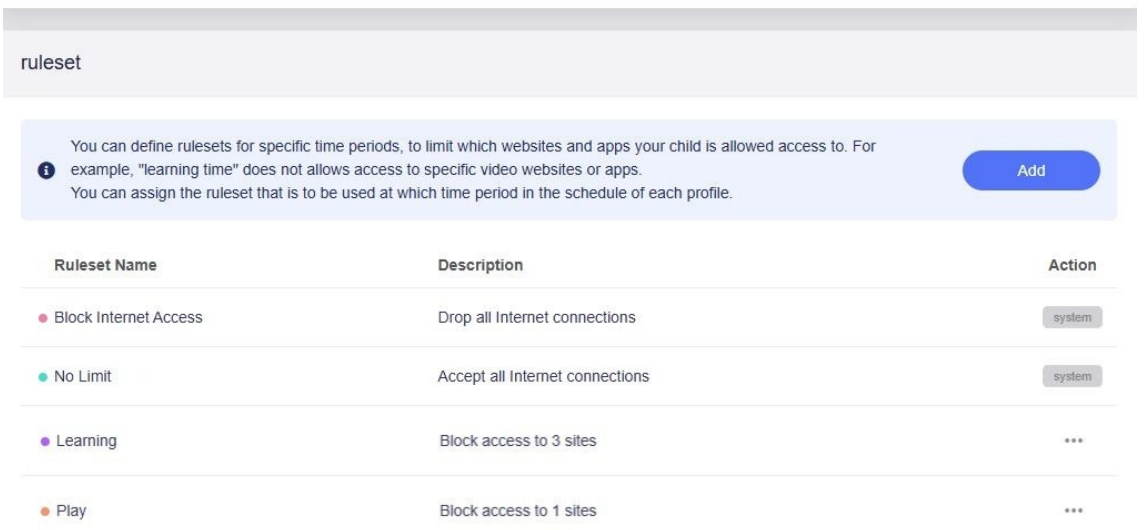
- Die rote gestrichelte Linie zeigt die aktuelle Uhrzeit an.
- Klicken Sie im Zeitplan auf einen Regelsatz, um seine Ausführungszeit zu ändern.

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



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





12.6.2 Fehlerbehebung

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

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

12.7 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:

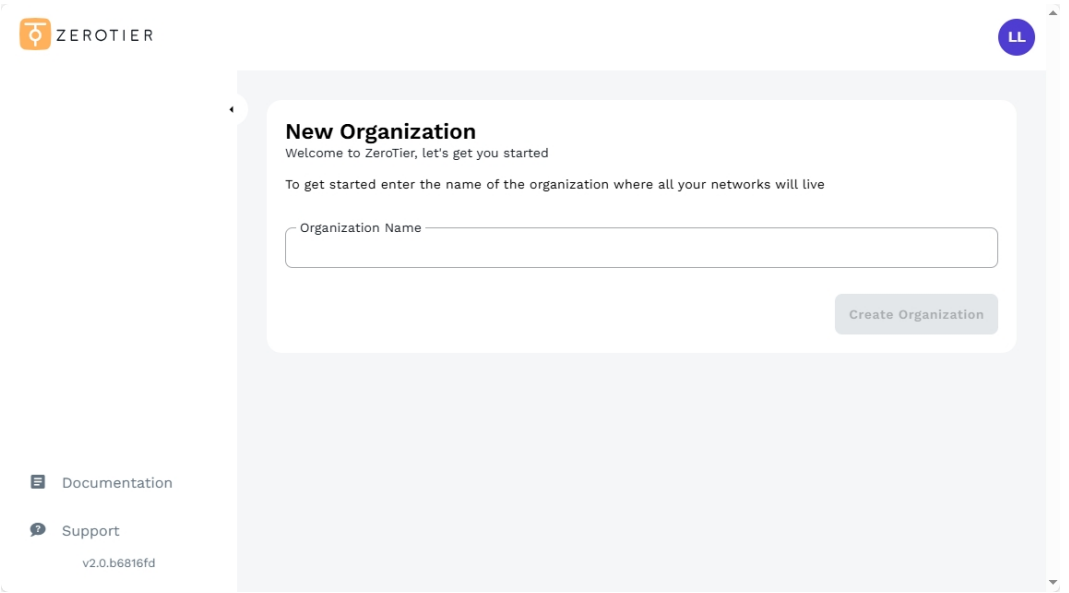
1. Die gleichzeitige Verwendung von ZeroTier mit OpenVPN Client, WireGuard Client, GoodCloud Site to Site oder Tailscale wird nicht empfohlen, da Routingkonflikte auftreten können.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

12.7.1 ZeroTier einrichten

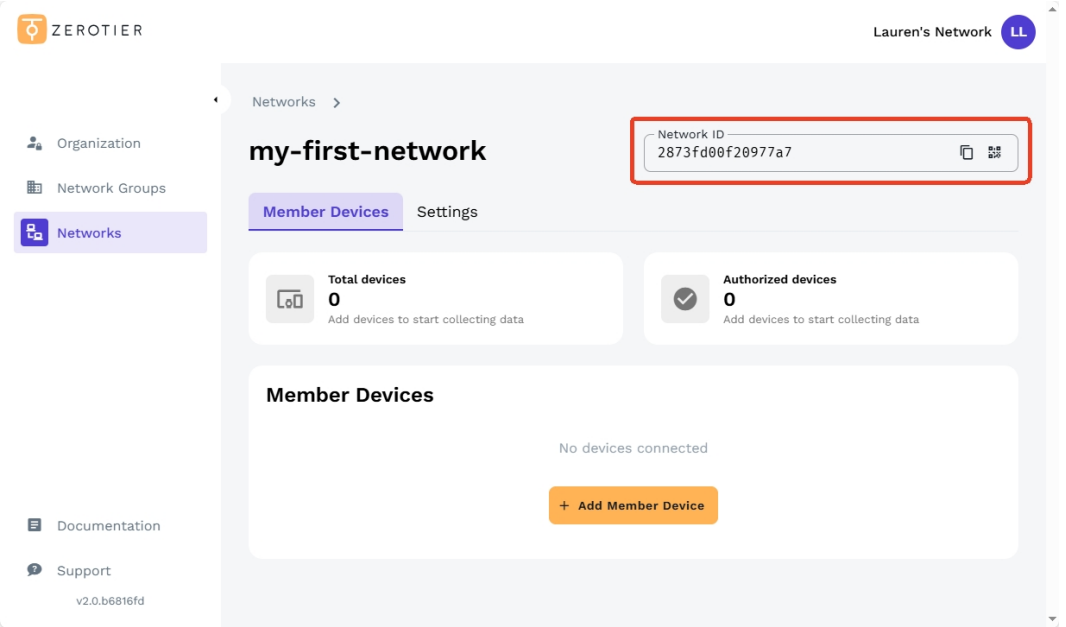
ZeroTier Central ist in zwei Versionen verfügbar: New Central und Legacy Central.

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.

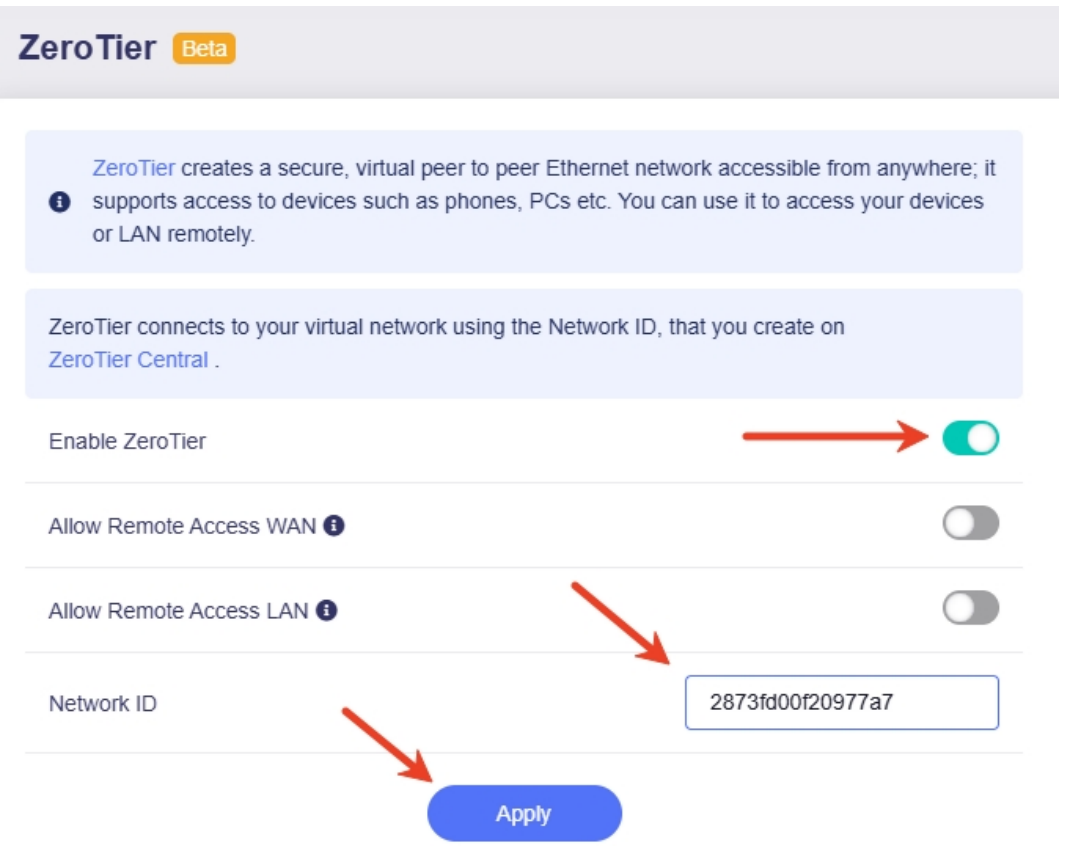


3. Wählen Sie einen Tarif aus. In diesem Beispiel verwenden wir den **Personal-Tarif** mit zehn Geräten, einem Netzwerkadministrator und einem Netzwerk. Wenn Sie mehr Netzwerke, zusätzliche Geräte, eigene Routen oder DNS-Einstellungen benötigen, wählen Sie einen kostenpflichtigen Tarif.
4. Ihr ZeroTier-Netzwerk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

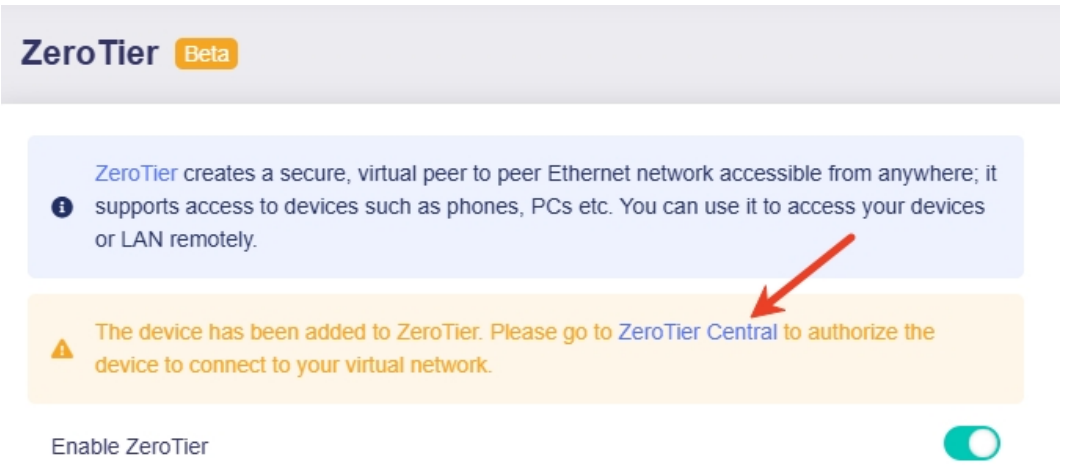


Notieren Sie die **Network ID** oben rechts. Diese besteht aus 16 Buchstaben und Ziffern und wird später benötigt, um weitere Geräte zu verbinden.

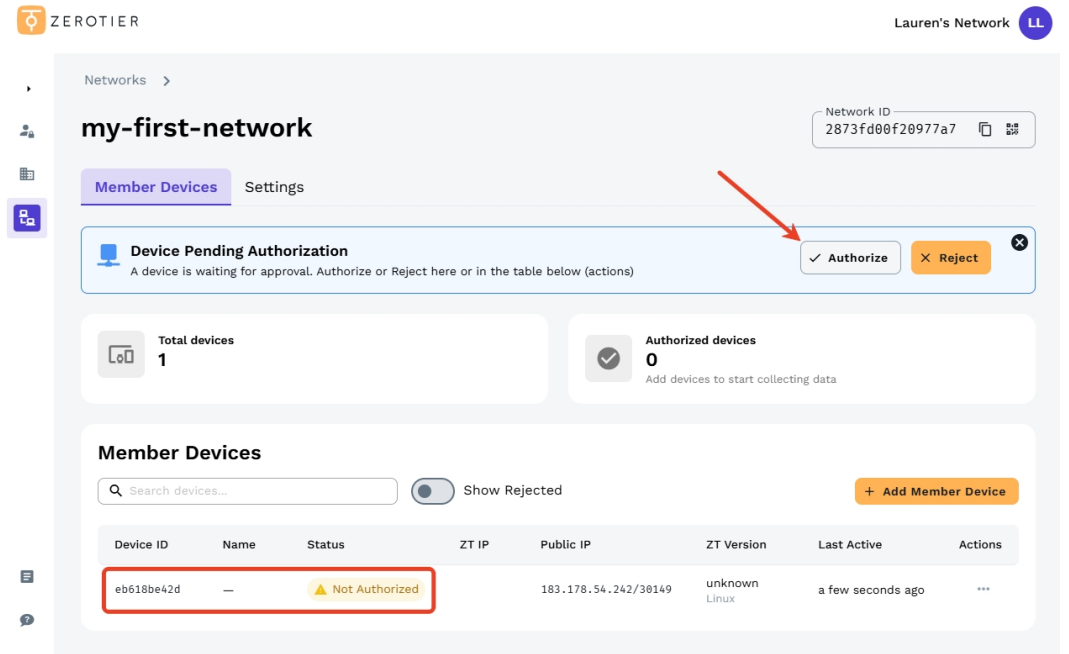
5. Melden Sie sich an der Weboberfläche an und öffnen Sie **APPLICATIONS** > **ZeroTier**. Aktivieren Sie ZeroTier, geben Sie die **Network ID** ein und klicken Sie auf **Apply**.



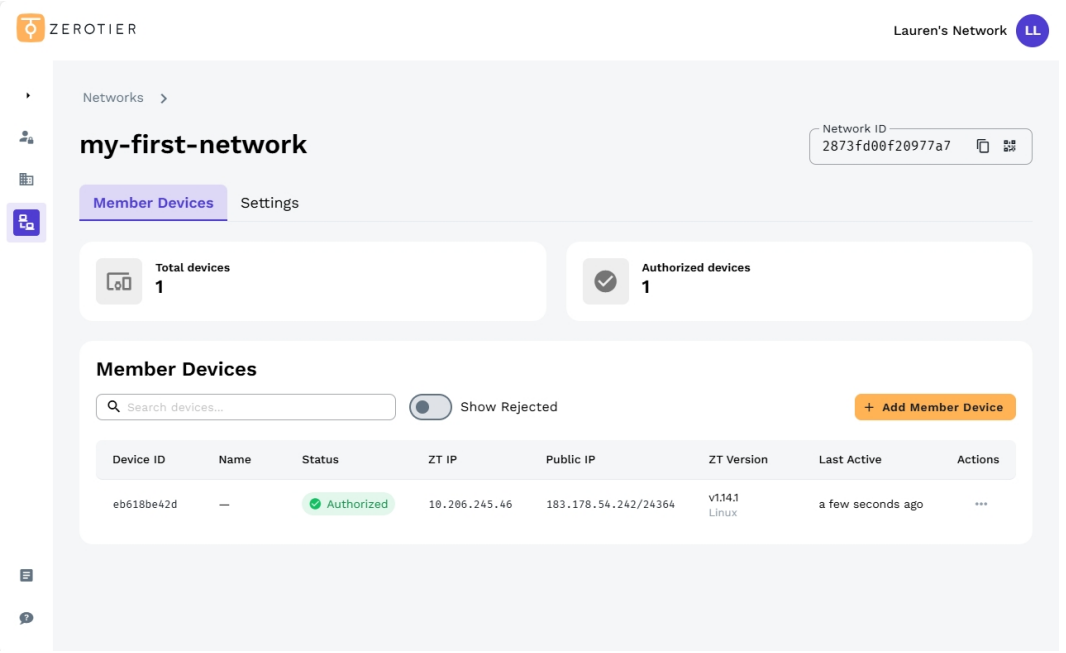
Nach kurzer Zeit erscheint der Hinweis, dass eine Autorisierung erforderlich ist. Klicken Sie auf den Link **ZeroTier Central**, um ZeroTier Central zu öffnen.



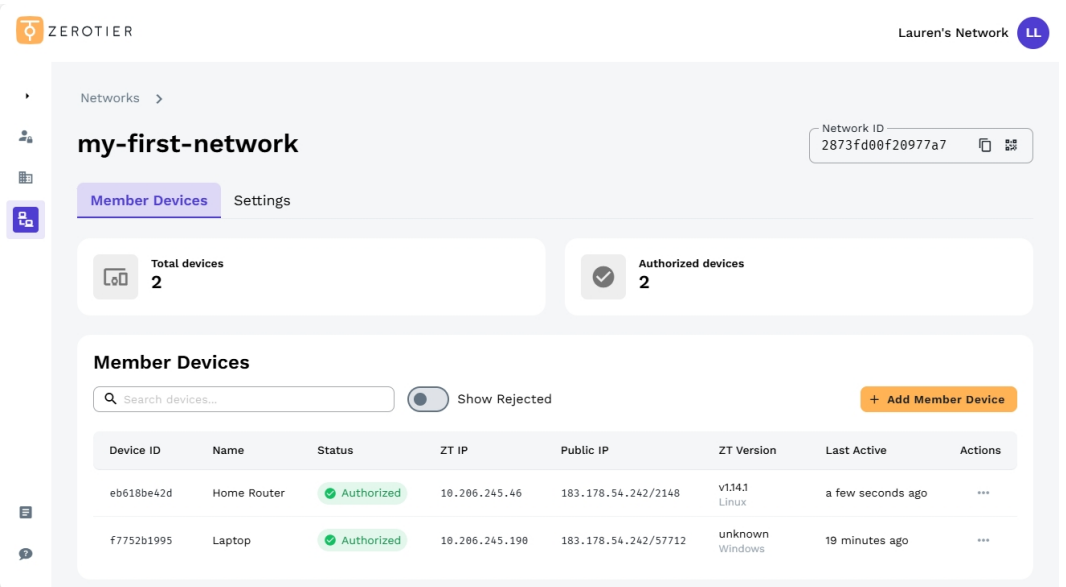
6. Suchen Sie in ZeroTier Central das ausstehende Gerät unter Pending und autorisieren Sie es.



Nach der Autorisierung erscheint die folgende Ansicht.

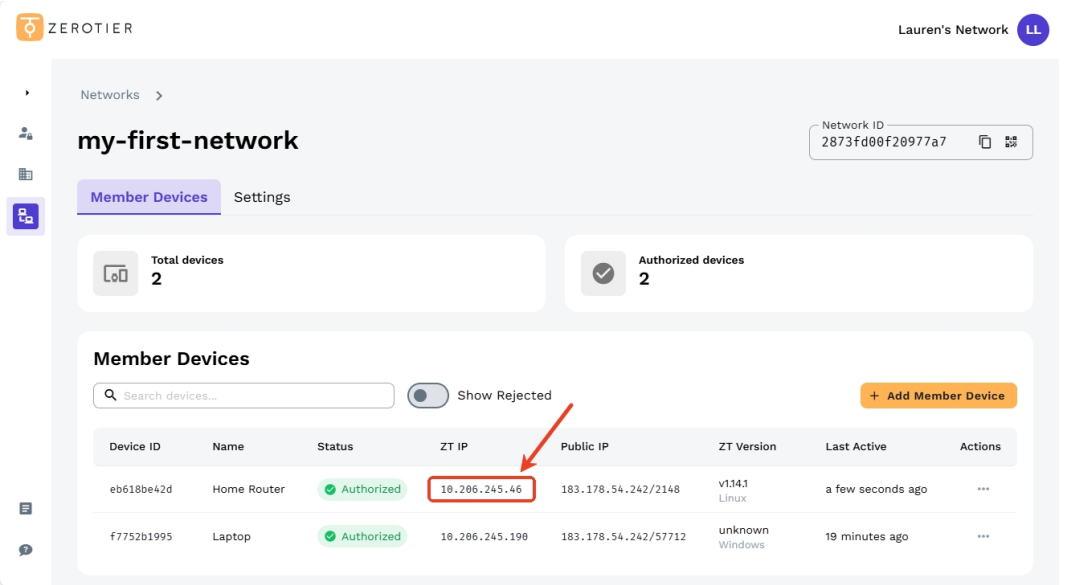


7. Fügen Sie anhand dieser Anleitung ein weiteres Gerät, etwa einen Computer oder ein Smartphone, zum selben ZeroTier-Netzwerk hinzu. Nach erfolgreichem Hinzufügen erscheint die folgende Ansicht **mit Gerätedetails wie Device ID, Name, Status, Managed IP und Public IP**.



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

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



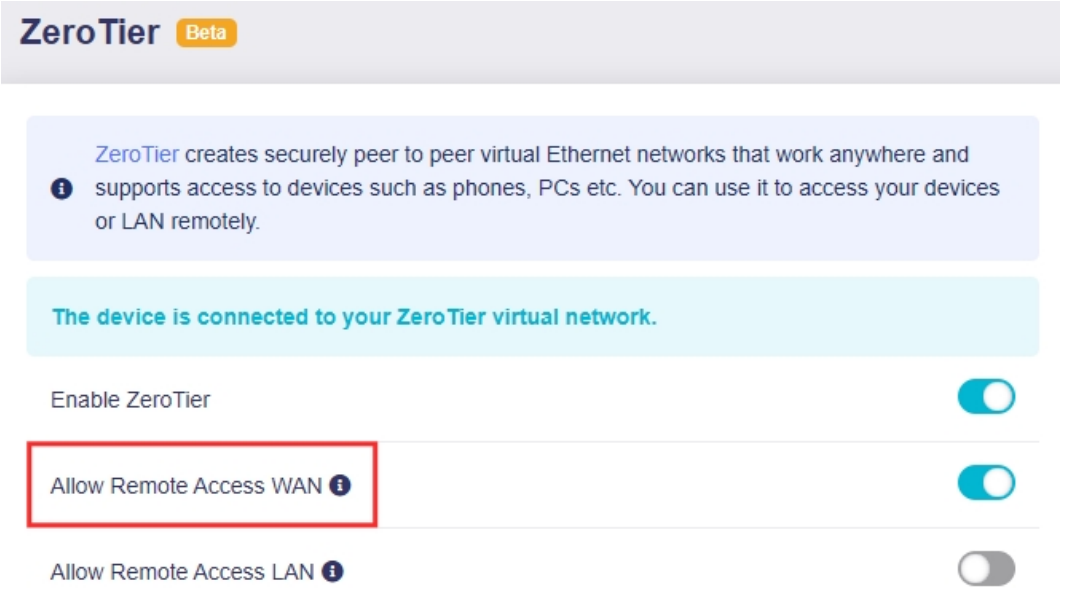
Über diese verwaltete IP-Adresse können Sie von einem Laptop im selben ZeroTier-Netzwerk auf den Router zugreifen.

9. Verbindung prüfen.

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

12.7.2 Fernzugriff auf WAN erlauben

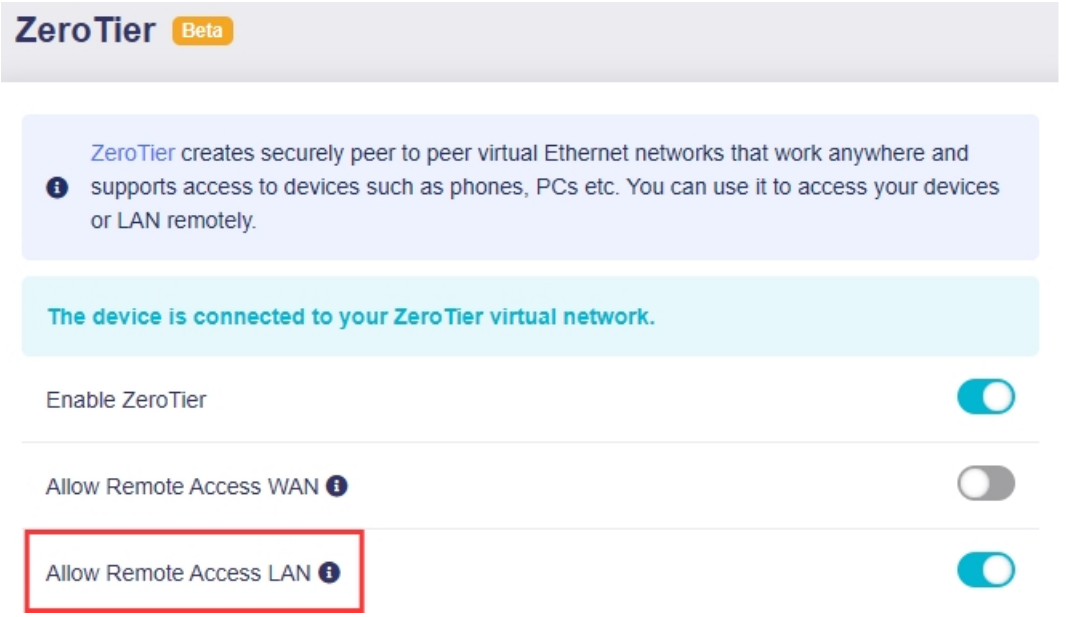
Diese Option erlaubt den Zugriff auf Ressourcen auf der WAN-Seite des Geräts über das virtuelle ZeroTier-Netzwerk. Weitere Informationen finden Sie hier.



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

12.7.3 Fernzugriff auf LAN erlauben

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



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

12.8 Tailscale

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

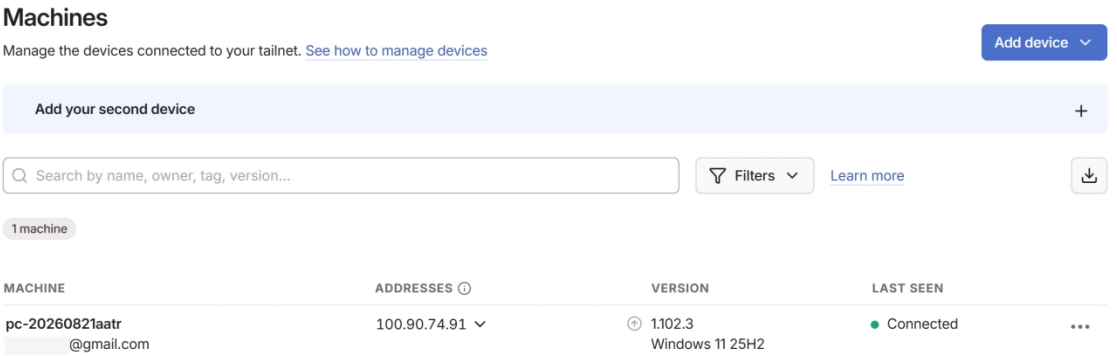
Mit der Tailscale-Funktion kann Ihr GL.iNet-Router einem virtuellen Tailscale-Netzwerk beitreten. Dadurch wird der Fernzugriff auf den Router sowie auf Ressourcen auf seiner WAN- und LAN-Seite möglich.

Hinweis:

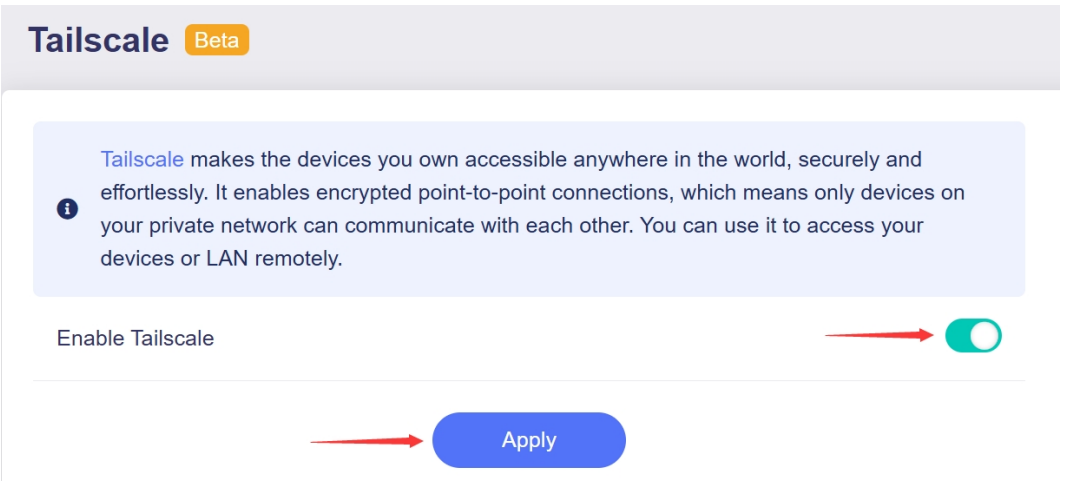
1. Tailscale basiert auf WireGuard. Die gleichzeitige Nutzung mit OpenVPN Client, WireGuard Client, GoodCloud Site to Site oder ZeroTier wird nicht empfohlen, da Routingkonflikte auftreten können.
2. Diese Funktion befindet sich derzeit in der Betaphase und kann noch Fehler enthalten.

12.8.1 Tailscale einrichten

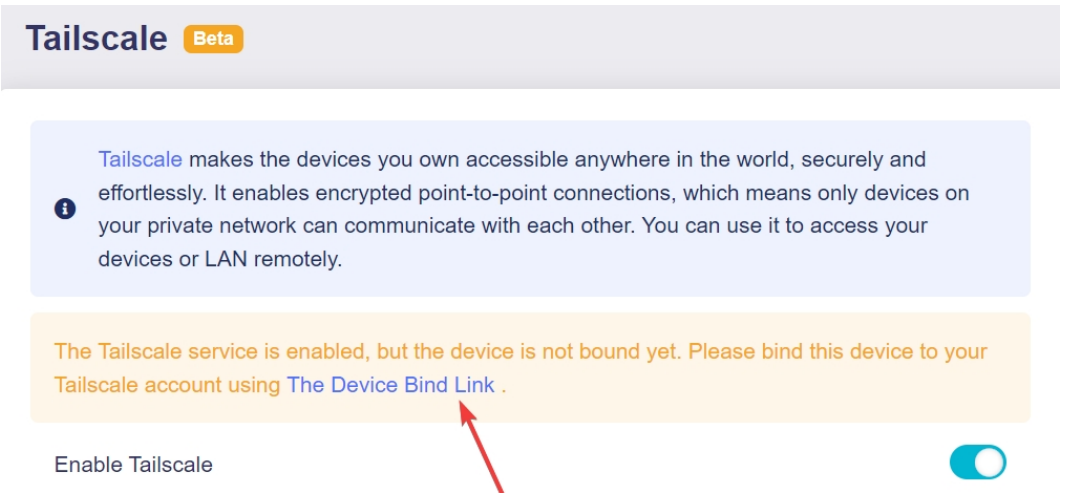
1. Registrieren Sie zunächst ein Tailscale-Konto und verknüpfen Sie zu Testzwecken ein oder zwei Geräte damit. Anschließend werden diese in der Tailscale-Konsole angezeigt.



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



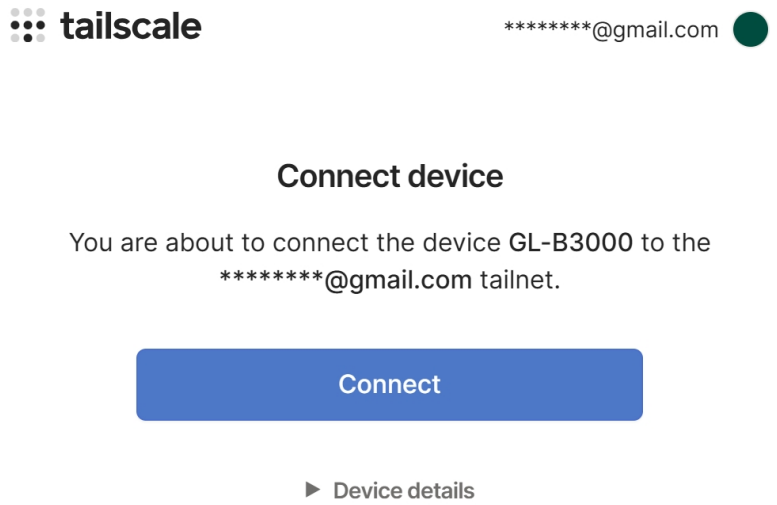
3. Sie werden aufgefordert, das Gerät zu verknüpfen. Klicken Sie auf **Device Bind Link**.



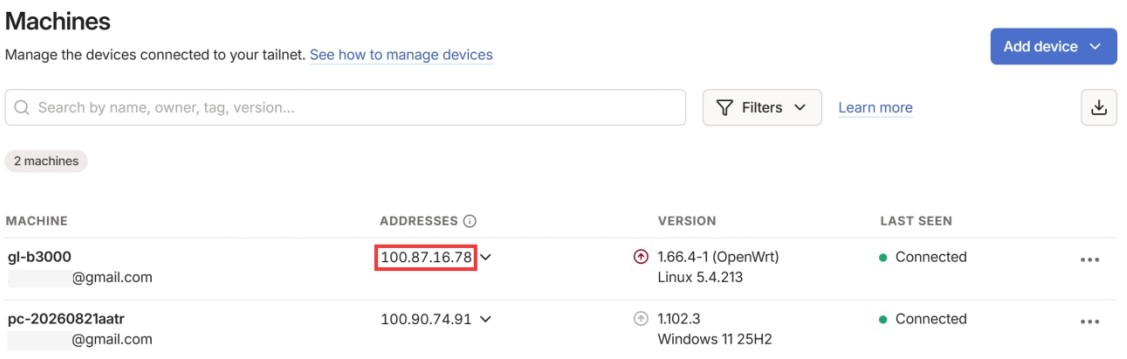
4. Klicken Sie im eingeblendeten Fenster auf den Link und melden Sie sich mit Ihrem Tailscale-Konto an.



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

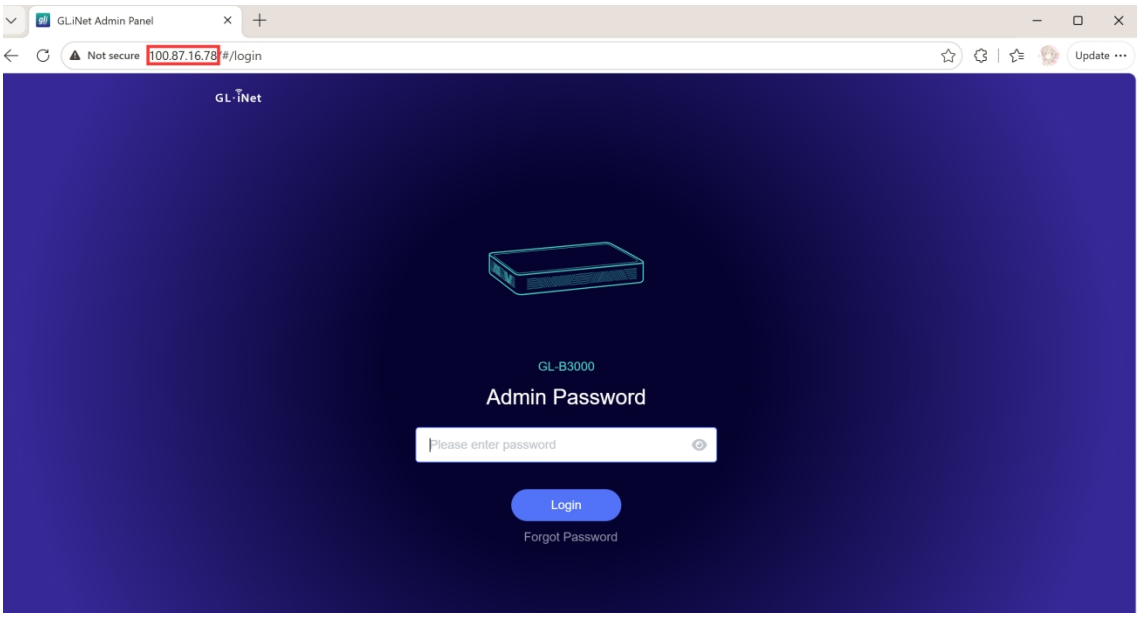


6. Sie werden anschließend zur Tailscale-Verwaltungskonsole weitergeleitet. Der Router wurde nun zum virtuellen Tailscale-Netzwerk hinzugefügt und ist über die virtuelle Tailscale-IP-Adresse **100.87.16.78** aus der Ferne erreichbar.



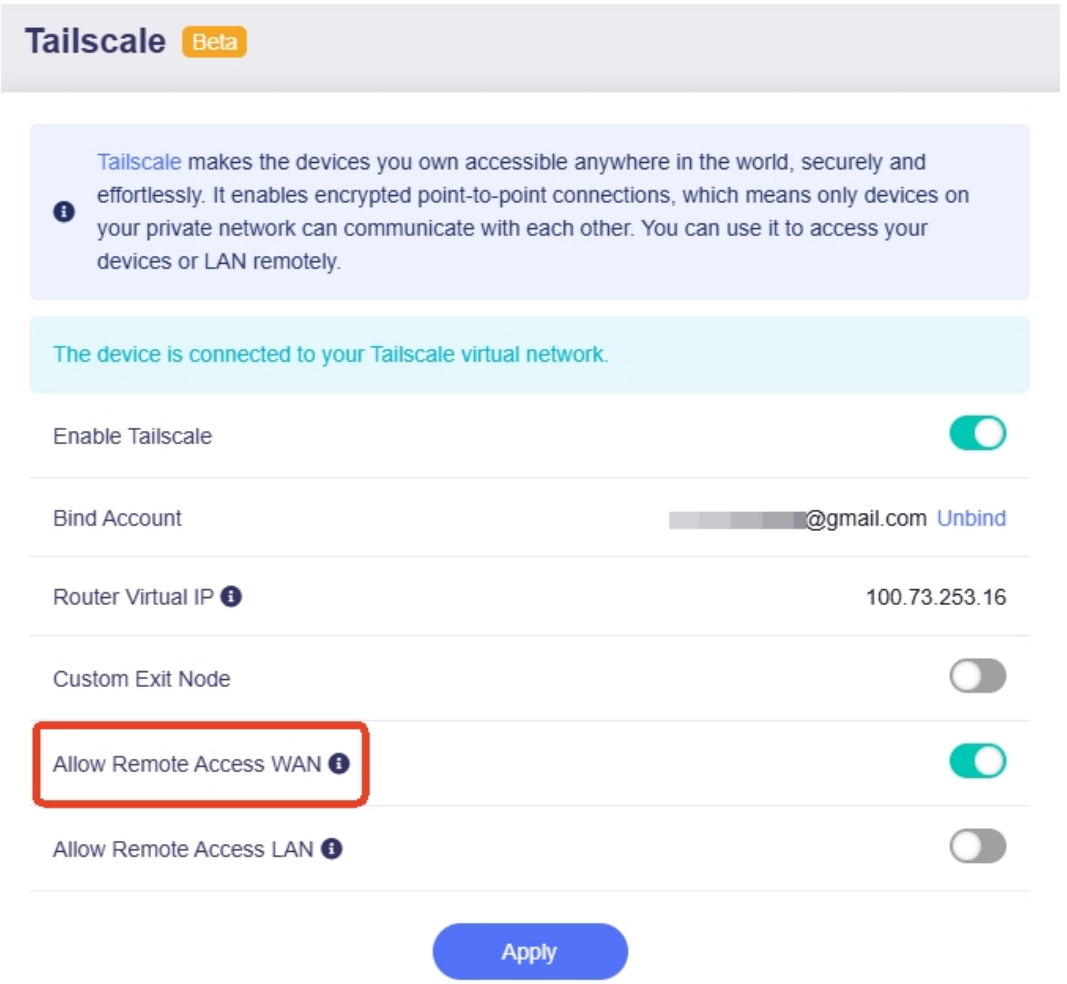
7. Verbindung prüfen.
   Öffnen Sie auf einem anderen Gerät im selben Tailscale-Netzwerk einen Webbrowser und geben Sie die virtuelle IP-Adresse des Routers ein. Wenn Sie seine Weboberfläche

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



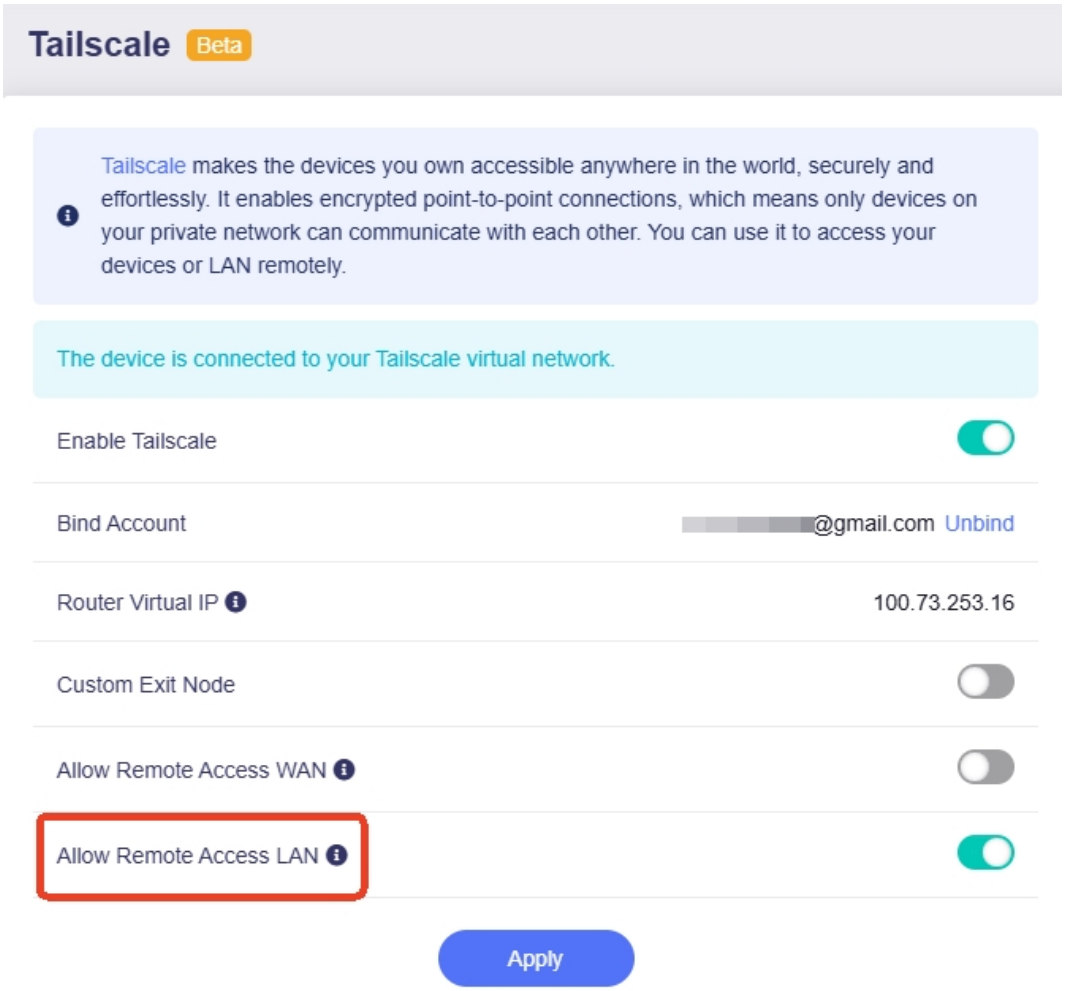
12.8.2 Fernzugriff auf WAN erlauben

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



12.8.3 Fernzugriff auf LAN erlauben

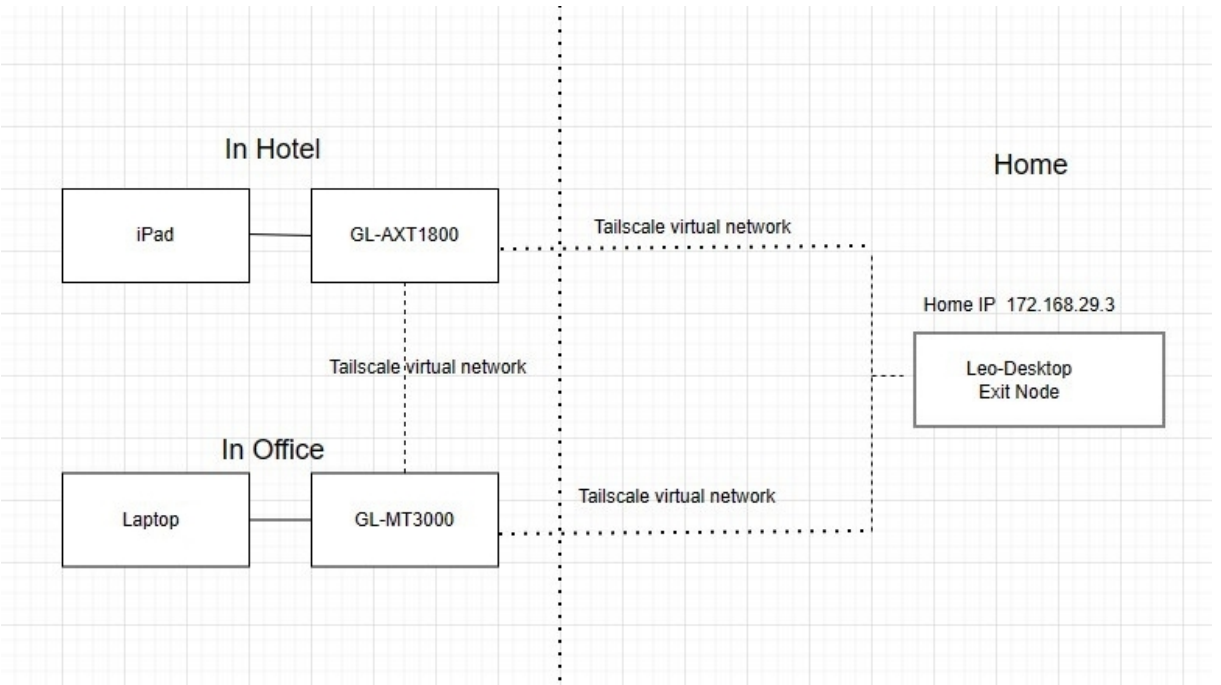
Diese Option erlaubt den Zugriff auf Ressourcen auf der LAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk. Weitere Informationen finden Sie hier.



12.8.4 Eigene Exit-Nodes

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

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



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

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

Kapitel 13

Netzwerk

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

13.1 Firewall

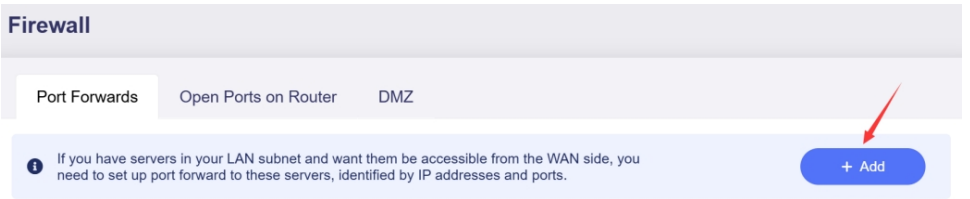
Über die Firewall-Einstellungen lassen sich externe Anfragen an bestimmte Geräte im lokalen Netzwerk weiterleiten. Die Firewall-Seite bietet drei zentrale Funktionen: **Port Forwards** für den gezielten Zugriff auf bestimmte Geräteports, **Open Ports on Router** für den Zugriff auf Dienste des Routers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

13.1.1 Portweiterleitungen

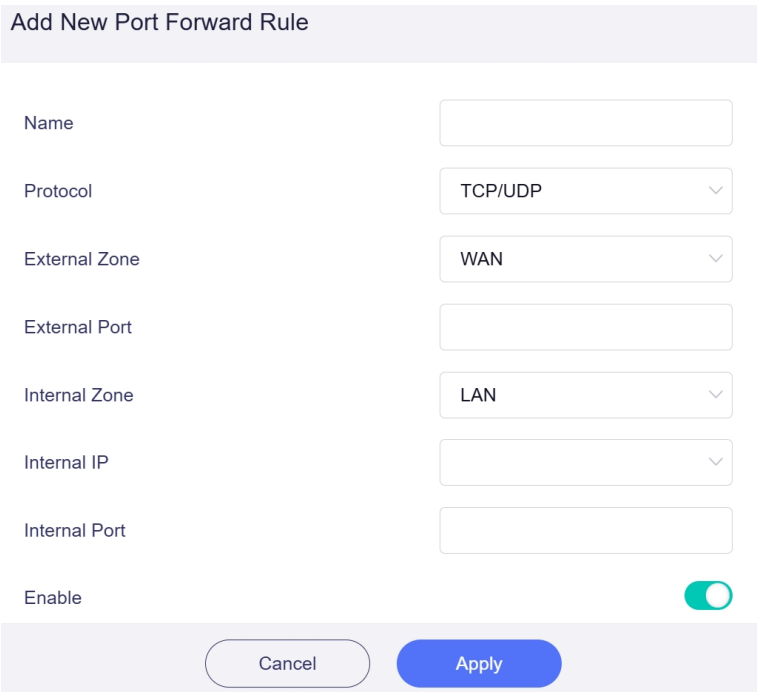
Portweiterleitungen ermöglichen entfernten Computern den Zugriff auf einen lokalen Computer oder Server hinter der LAN-Firewall, etwa einen Web- oder FTP-Server.

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

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



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

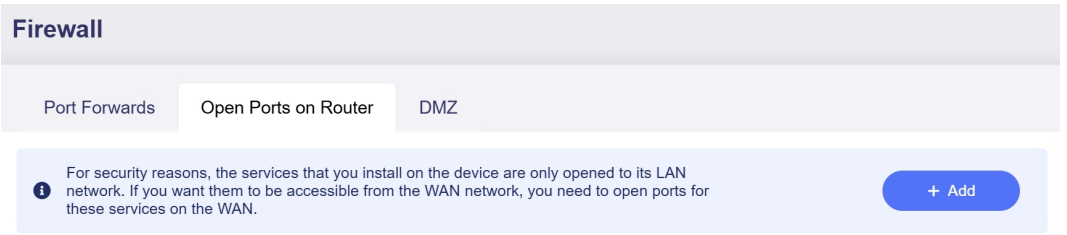


- **Name**: Ein frei wählbarer Name für die Regel.
- **Protocol**: Das verwendete Protokoll. Sie können TCP, UDP oder beide auswählen.
- **External Zone**: Zur Auswahl stehen WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN und Guest.
- **External Port**: Die externe Portnummer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

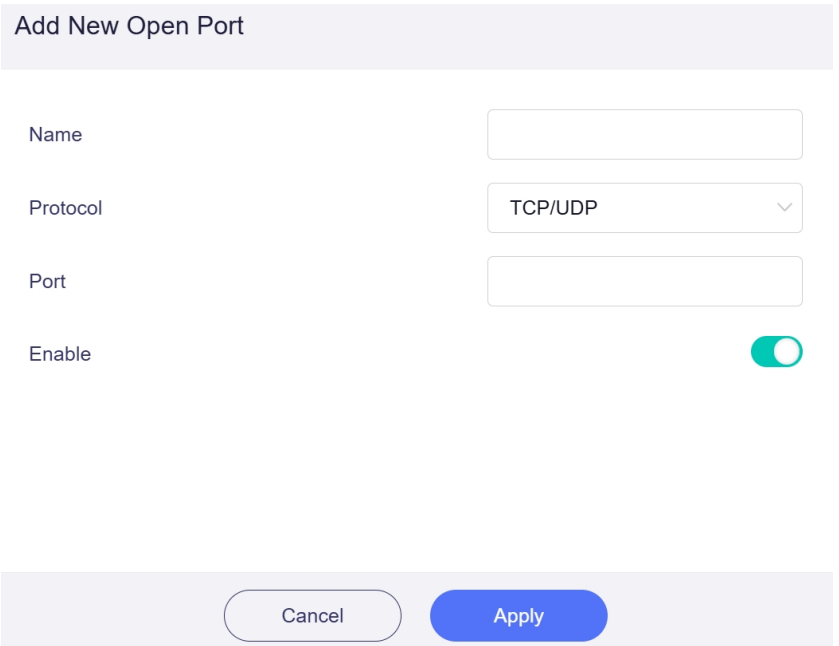
13.1.2 Ports am Router öffnen

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

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



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



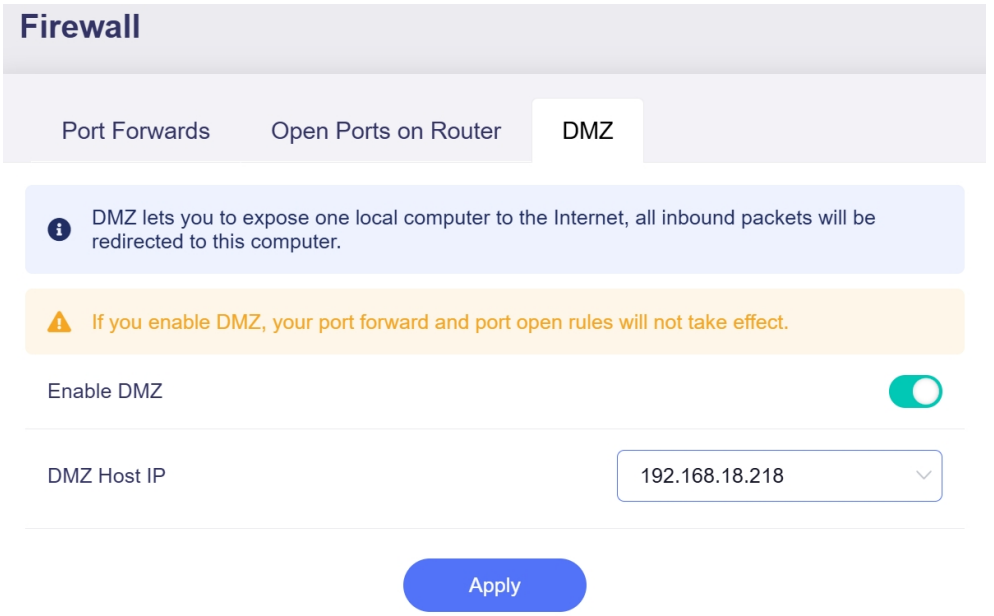
- **Name**: Ein frei wählbarer Name für die Regel.
- **Protocol**: Das verwendete Protokoll. Sie können TCP, UDP oder beide auswählen.
- **Port**: Die Nummer des Ports, den Sie öffnen möchten.

13.1.3 DMZ

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

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

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



13.2 Multi-WAN

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

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

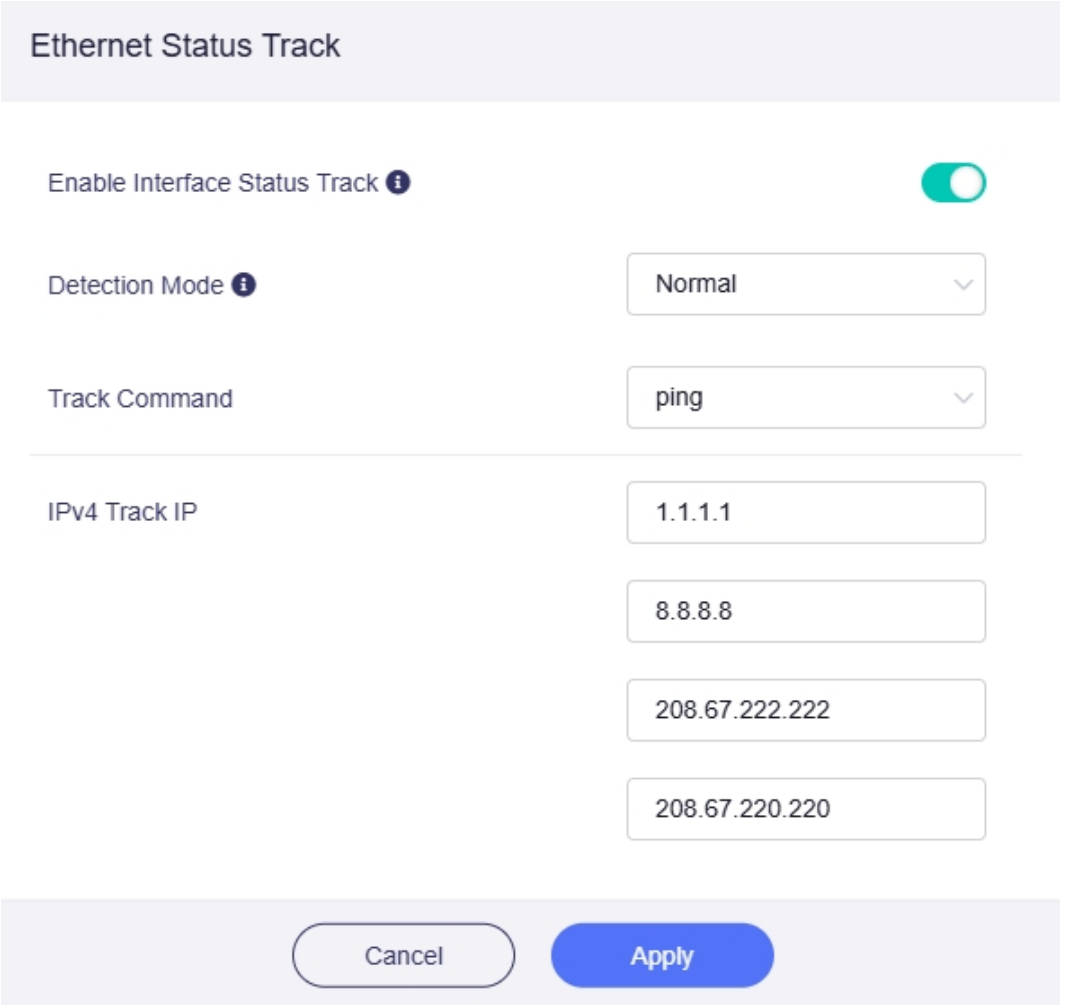
Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Multi-WAN**. Die Seite enthält die Abschnitte Interface Status Track und Multi-WAN Mode.

13.2.1 Schnittstellenstatus überwachen

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



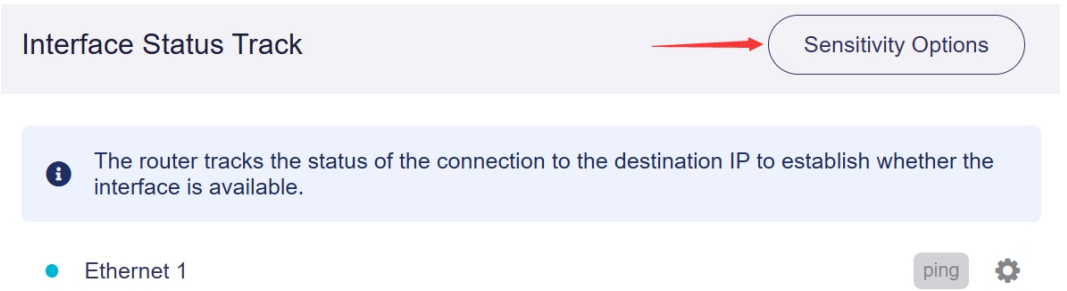
Klicken Sie im Abschnitt **Interface Status Track** rechts auf das Zahnradsymbol, um die Überwachung für die jeweilige Schnittstelle einzustellen. Nachfolgend sind die Einstellungen für Ethernet abgebildet. Für andere Schnittstellen gilt dieselbe Vorgehensweise.



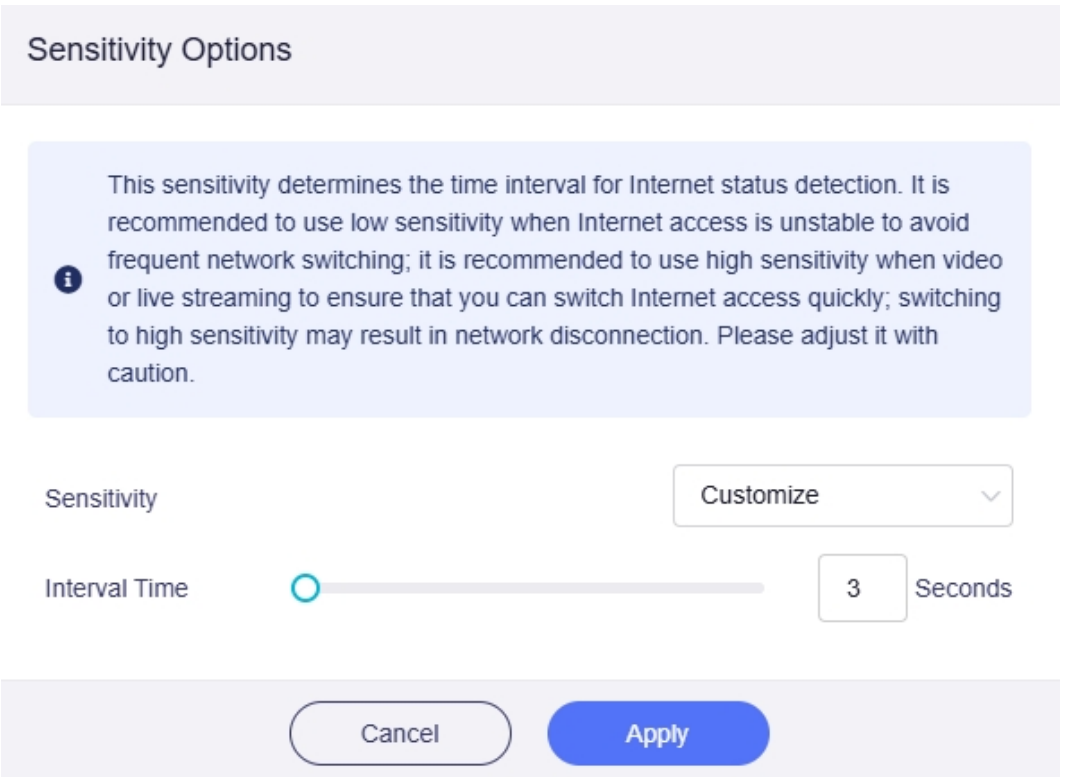
- **Enable Interface Status Track**: Standardmäßig aktiviert. Bei deaktivierter Überwachung beurteilt der Router den Schnittstellenstatus anhand physischer Merkmale, etwa ob ein Ethernetkabel angeschlossen ist.
- **Detection Mode**: Diese Funktion wurde in Firmware v4.5 als Low Data Mode eingeführt und in Firmware v4.7 in Detection Mode umbenannt. Es stehen drei Modi zur Verfügung: Normal Mode, Low Data Mode und Strict Mode.
  - **Normal**: Dieser Modus wird standardmäßig verwendet.
  - **Low Data**: Die Verbindungsüberwachung wird nur ausgelöst, wenn an der Netzwerkschnittstelle ein Netzwerkfehler auftritt. Verwenden Sie diesen Modus bei einem Tarif mit begrenztem Datenvolumen. Nach einer Unterbrechung kann der erneute Verbindungsaufbau etwas länger dauern als im Modus Normal. Dieser Modus ist nur für die Mobilfunkschnittstelle standardmäßig aktiviert.
  - **Strict**: Der Schnittstellenstatus wird ausschließlich anhand der Ergebnisse eines Prüfbefehls ermittelt, der an eine öffentliche IP-Adresse gesendet wird.

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

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



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



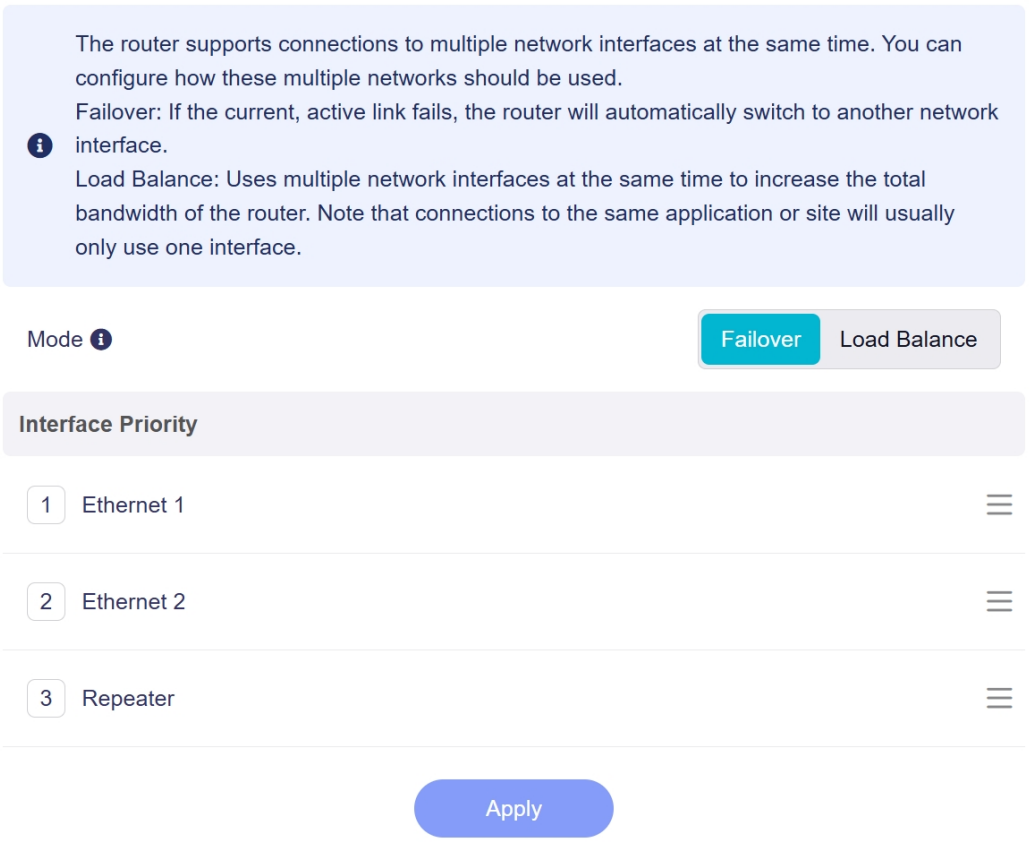
13.2.2 Multi-WAN-Modus

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

Ausfallsicherung

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

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

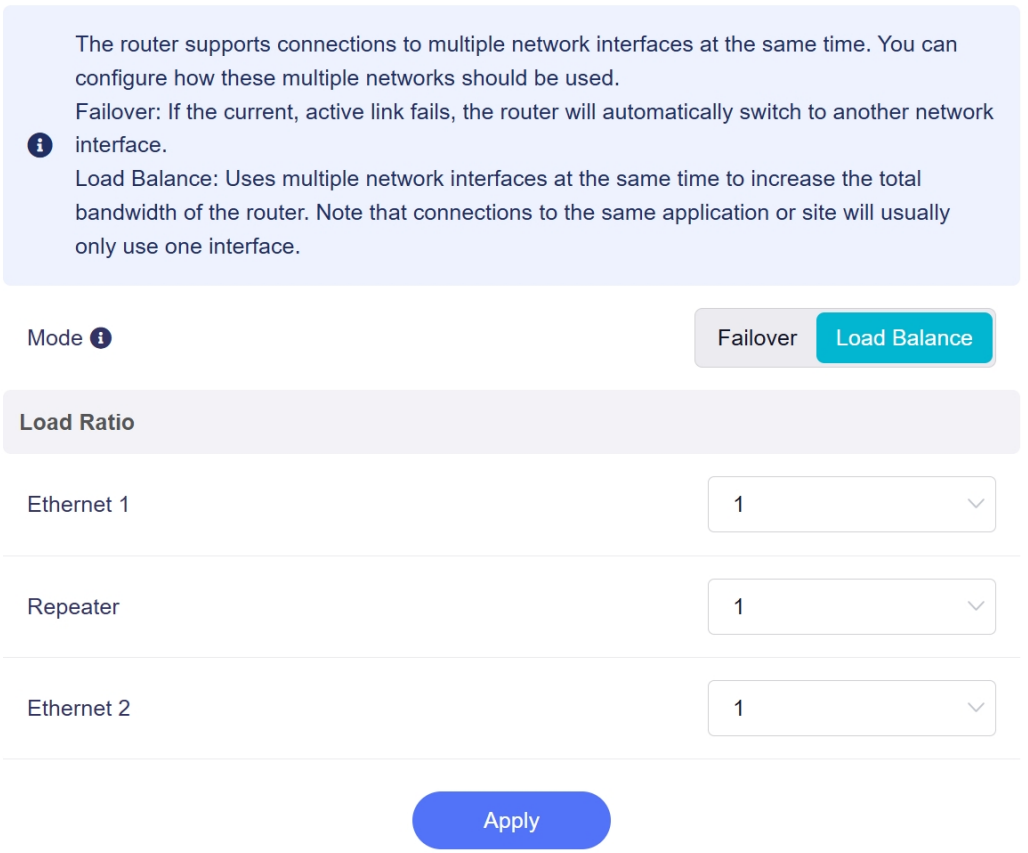


Lastverteilung

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

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

Ist der Router beispielsweise gleichzeitig mit drei Netzwerken verbunden (etwa Ethernet 1, Repeater und Ethernet 2) und bieten alle Schnittstellen Internetzugang, wird bei aktivierter Lastverteilung mit dem Verhältnis 1:1:1 die Netzwerklast gleichmäßig auf die drei Schnittstellen verteilt. Das System weist neue Verbindungen diesen Schnittstellen entsprechend dem eingestellten Lastverhältnis 1:1:1 zu.



Sie können das Lastverhältnis bei Bedarf anpassen. Hat beispielsweise Ethernet 1 eine Bandbreite von 100 Mbit/s und Repeater eine Bandbreite von 200 Mbit/s und sind keine

weiteren Verbindungen aktiv, stellen Sie das Lastverhältnis für Ethernet 1 auf 1, für Repeater auf 2 und für Ethernet 2 auf 0 ein. Das System verteilt neue Verbindungen dann im Verhältnis 1:2 auf diese Schnittstellen. Ethernet 1 übernimmt somit halb so viele Verbindungen wie Repeater. Während die Ausfallsicherung nur bei einem Verbindungsausfall umschaltet, optimiert dieser Modus den Gesamtdurchsatz durch die Verteilung der Datenlast auf alle verfügbaren Schnittstellen.

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

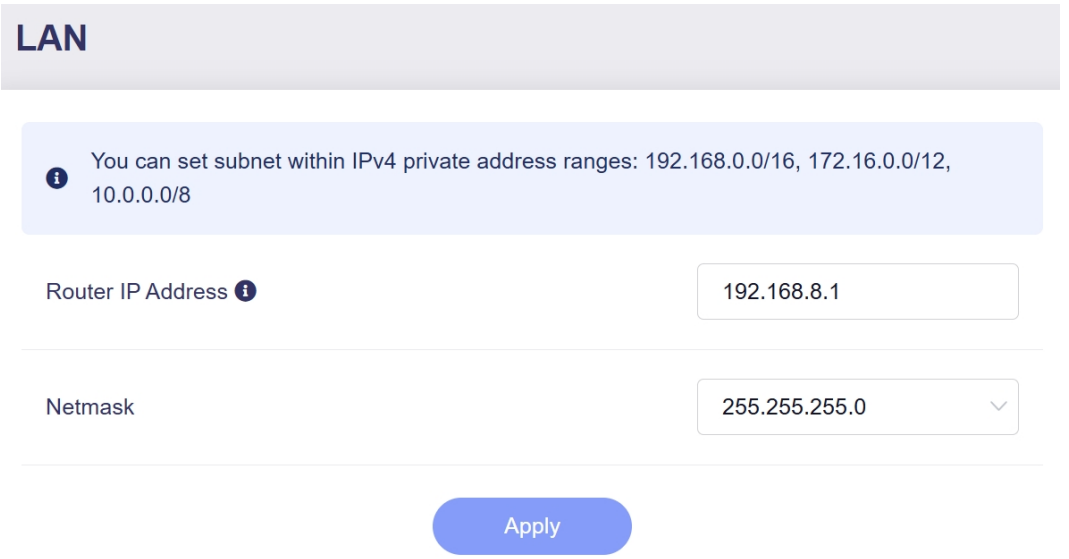
13.3 LAN

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

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **LAN**. Hier konfigurieren Sie die Grundeinstellungen, den DHCP-Server und die Adressreservierung.

13.3.1 Grundeinstellungen

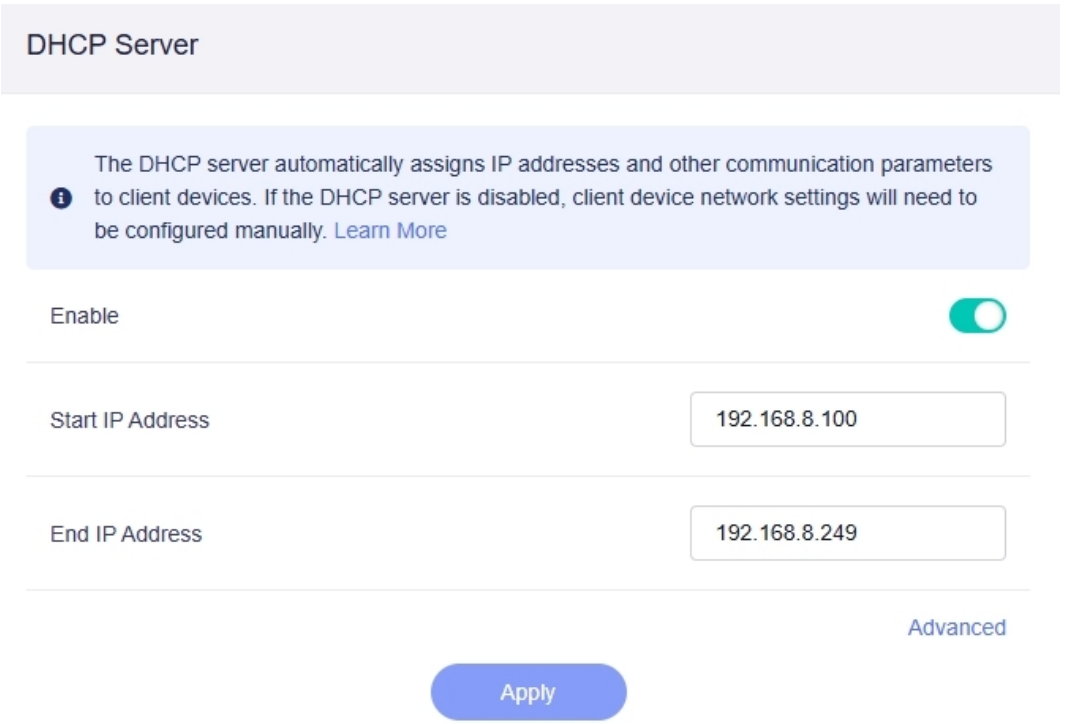
Zu den Grundeinstellungen gehören die IP-Adresse des Routers und die Netzmaske. Sie können ein Subnetz innerhalb der privaten IPv4-Adressbereiche 192.168.0.0/16, 172.16.0.0/12 oder 10.0.0.0/8 festlegen.



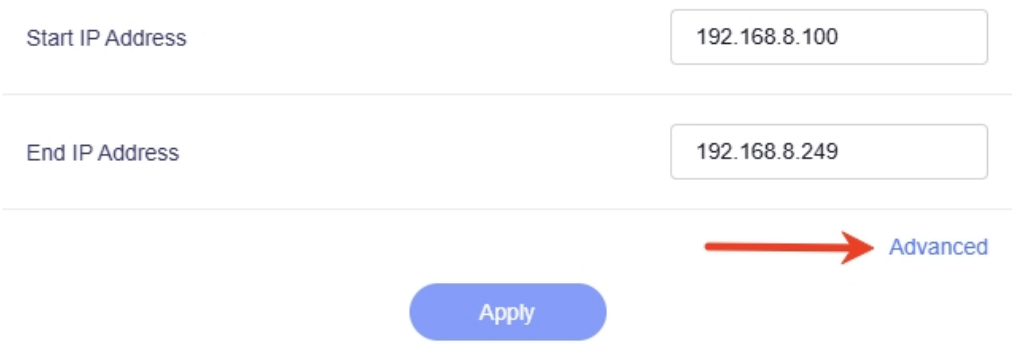
- **Router IP Address**: Über diese Adresse rufen Sie die Weboberfläche im Browser auf. Standardmäßig lautet sie 192.168.8.1. Bei einem Konflikt mit dem vorgeschalteten Netzwerk können Sie sie ändern.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.

13.3.2 DHCP-Server

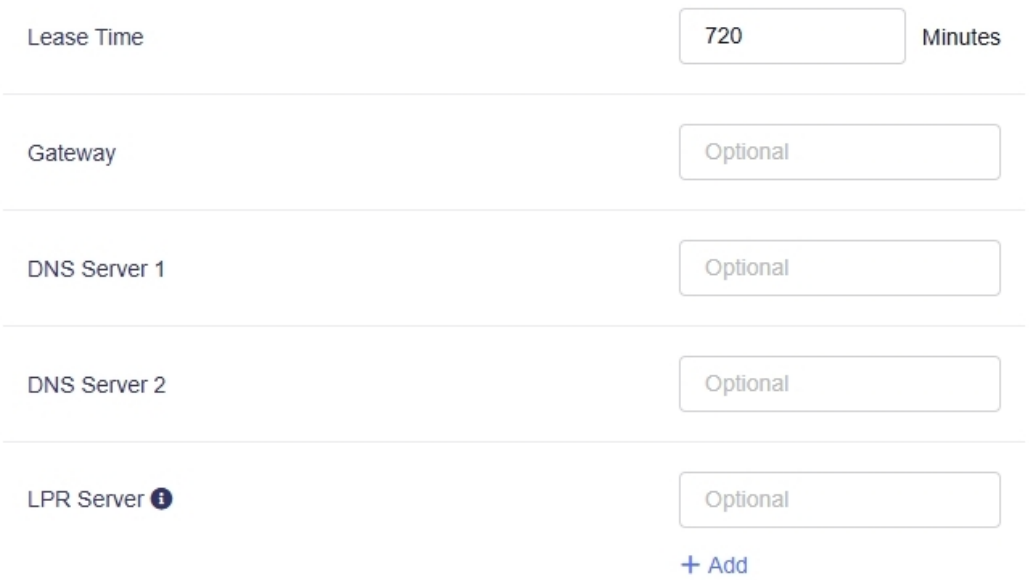
Der DHCP-Server weist jedem verbundenen Gerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Auf GL.iNet-Routern ist er standardmäßig aktiviert und verwendet den Adressbereich 192.168.8.100 bis 192.168.8.249. Diesen Bereich können Sie bei Bedarf anpassen.



Klicken Sie unten rechts auf **Advanced**.



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



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

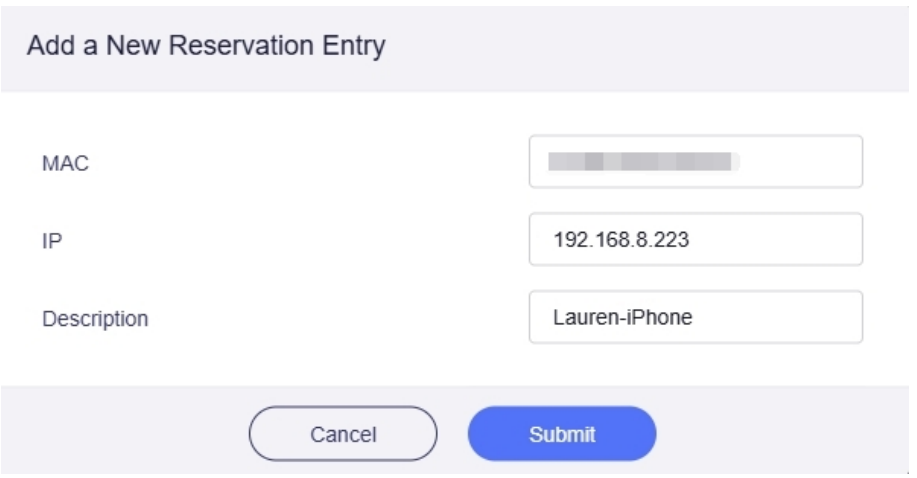
Hinweis: Bei deaktiviertem DHCP-Server müssen Sie für jedes Gerät eine statische IP-Adresse und weitere Kommunikationsparameter manuell festlegen. Einzelheiten finden Sie hier.

13.3.3 Adressreservierung

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

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

1. Melden Sie sich an der Weboberfläche an, öffnen Sie **NETWORK** > **LAN** > **Address Reservation** und klicken Sie auf **Add**.
2. Wählen Sie im eingeblendeten Fenster die MAC-Adresse aus. Die zugehörige IP-Adresse wird automatisch eingetragen. Geben Sie einen aussagekräftigen Namen ein und klicken Sie auf **Submit**.



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



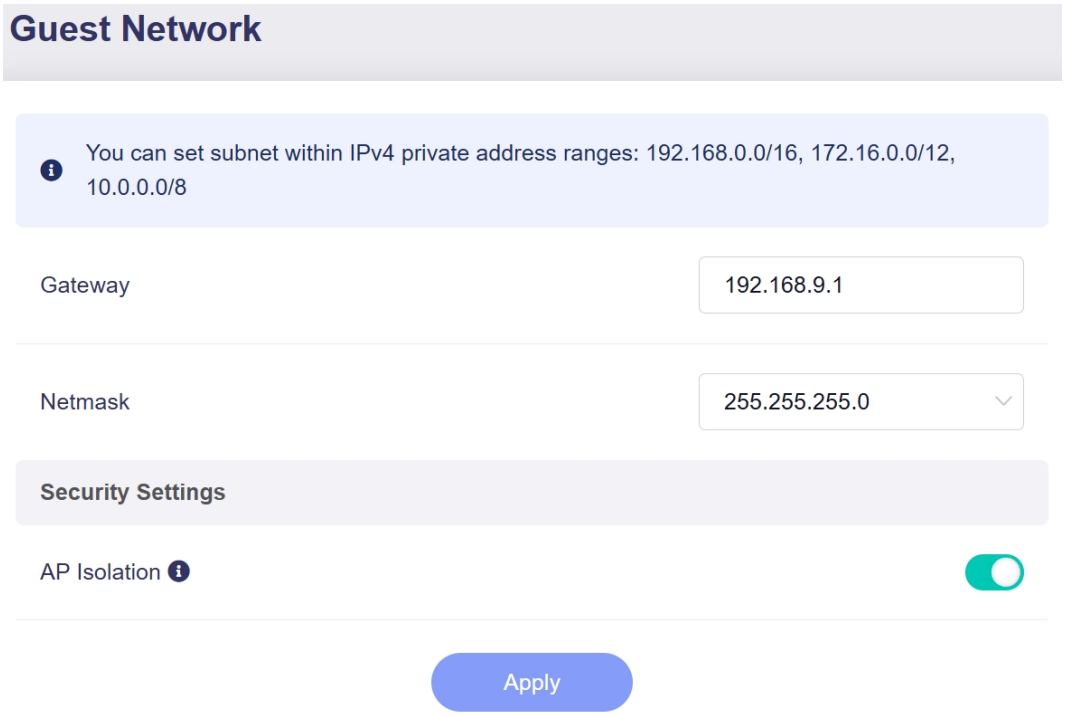
13.4 Gastnetzwerk

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

Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **Guest Network**. Hier konfigurieren Sie die Grundeinstellungen und den DHCP-Server des Gastnetzwerks.

13.4.1 Grundeinstellungen

Zu den Grundeinstellungen gehören Gateway, Netzmaske und AP-Isolierung.

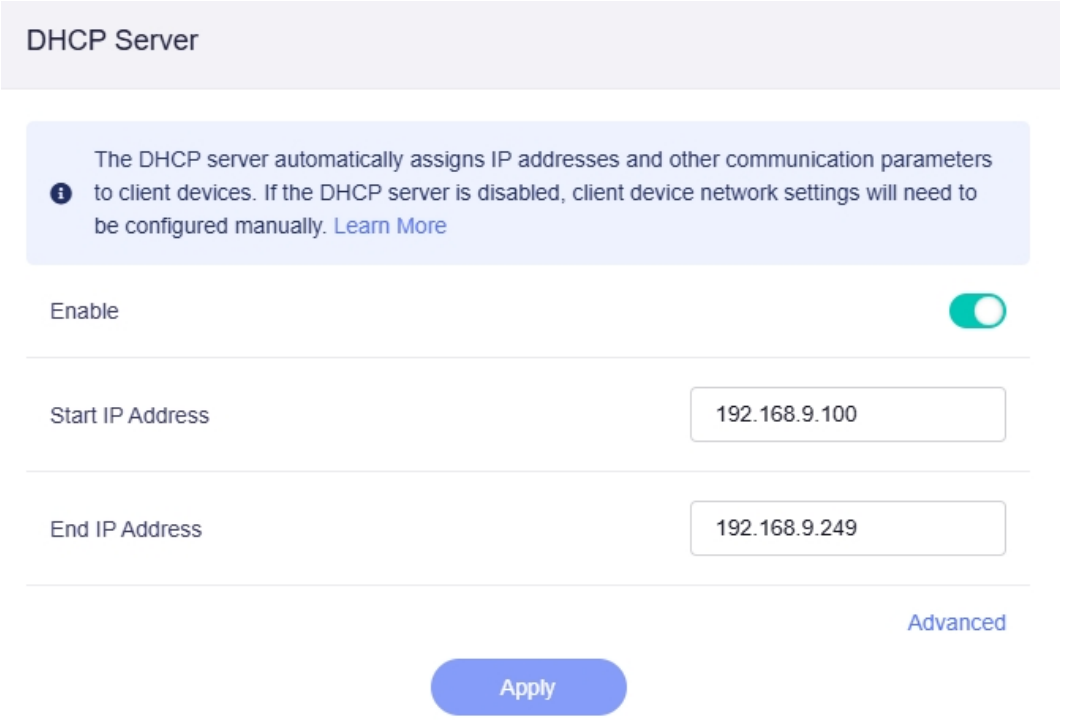


- **Gateway**: Standardmäßig 192.168.9.1. Sie können diese Adresse ändern, sie darf jedoch nicht mit dem Gateway des Hauptnetzwerks kollidieren.
- **Netmask**: Zur Auswahl stehen 255.255.255.0 und 255.255.0.0.
- **AP Isolation**: Isoliert Geräte im Gastnetzwerk voneinander, damit sie nicht mit anderen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

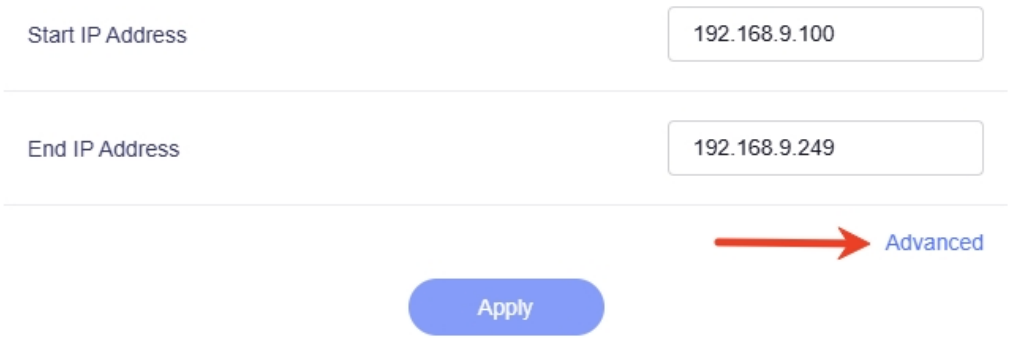
13.4.2 DHCP-Server

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

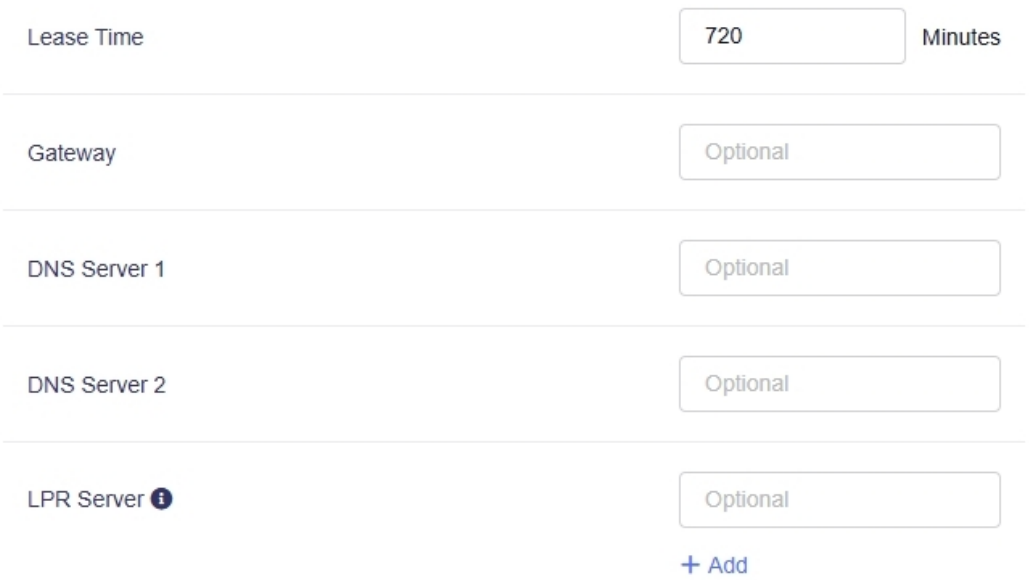
Nach der Aktivierung weist der DHCP-Server jedem verbundenen Gerät automatisch eine IP-Adresse und weitere Kommunikationsparameter zu. Im Gastnetzwerk reicht der Adresspool von 192.168.9.100 bis 192.168.9.249. Diesen Bereich können Sie anpassen.



Klicken Sie unten rechts auf **Advanced**.



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



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

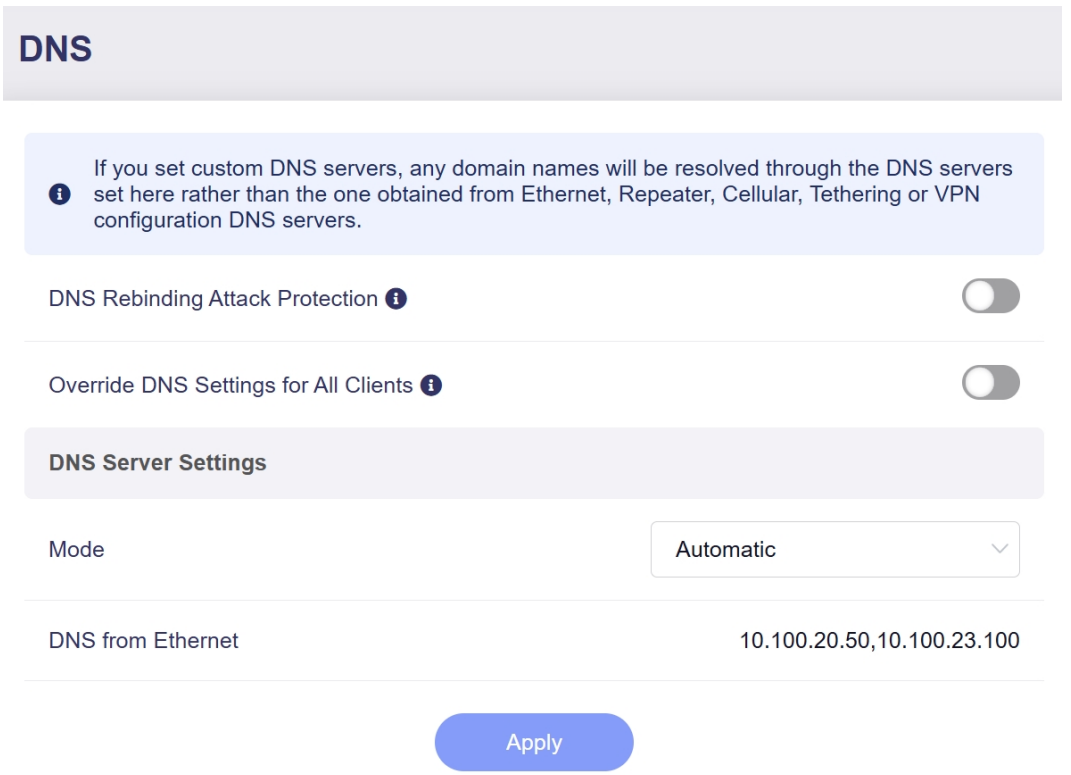
13.5 DNS

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

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

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

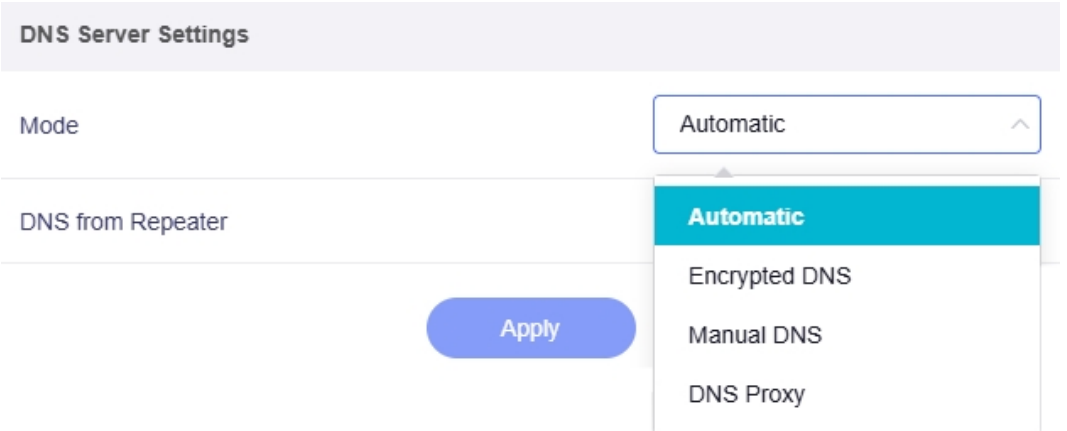
13.5.1 Allgemeine Einstellungen



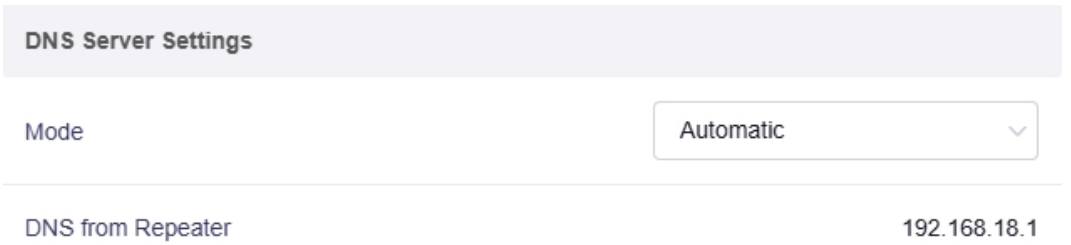
- **DNS Rebinding Attack Protection**: Schützt vor DNS-Rebinding-Angriffen, indem bösartige Namensauflösungen blockiert werden. Dadurch kann die Auflösung privater Adressen fehlschlagen. Deaktivieren Sie die Option, wenn Ihr Netzwerk ein Captive Portal verwendet, etwa eine Anmeldeseite in einem öffentlichen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

13.5.2 DNS-Servereinstellungen

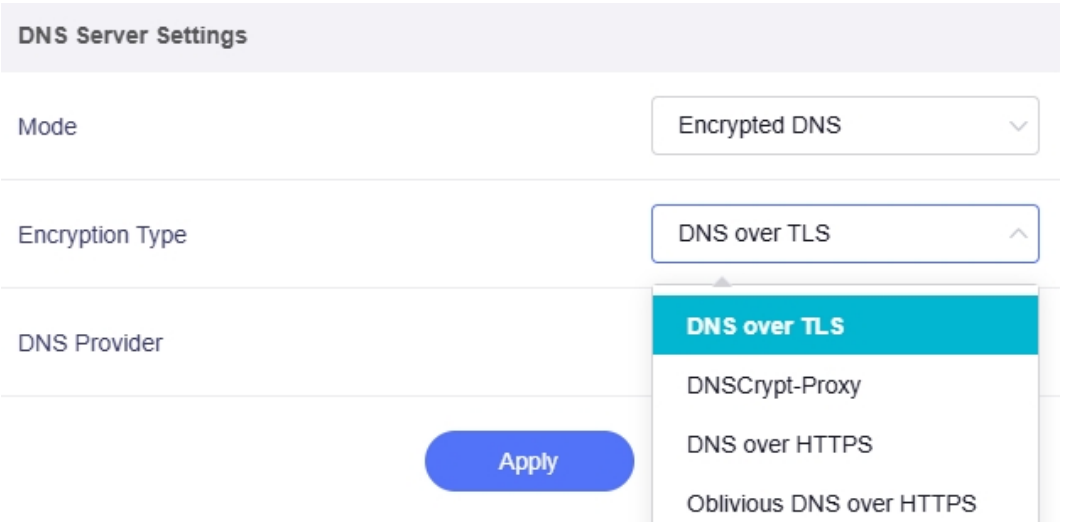
Für den DNS-Server stehen vier Modi zur Verfügung: Automatic, Encrypted DNS, Manual DNS und DNS Proxy.



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

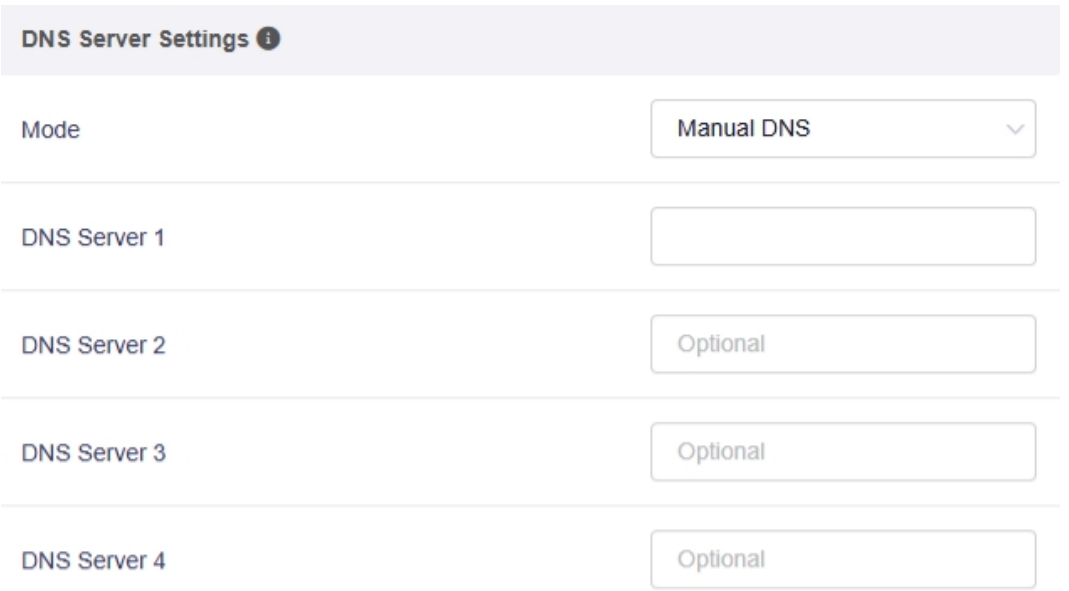


2. **Encrypted DNS**: Der Router verarbeitet DNS-Anfragen über verschlüsselte Protokolle und schützt die Auflösungsdaten so vor Abhören und Manipulation.
   Es stehen vier Verfahren zur Auswahl: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS.



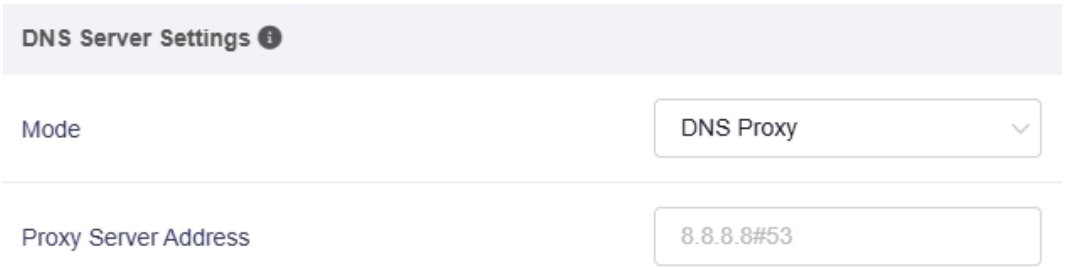
- Bei DNS over TLS wählen Sie Control D, NextDNS oder Cloudflare als DNS-Anbieter aus.
- Bei den drei anderen Verfahren wählen Sie mindestens einen DNS-Server aus dem Verzeichnis aus. Es sind bis zu acht Server möglich. Bei mehreren ausgewählten Servern verwendet der Router automatisch den schnellsten.

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



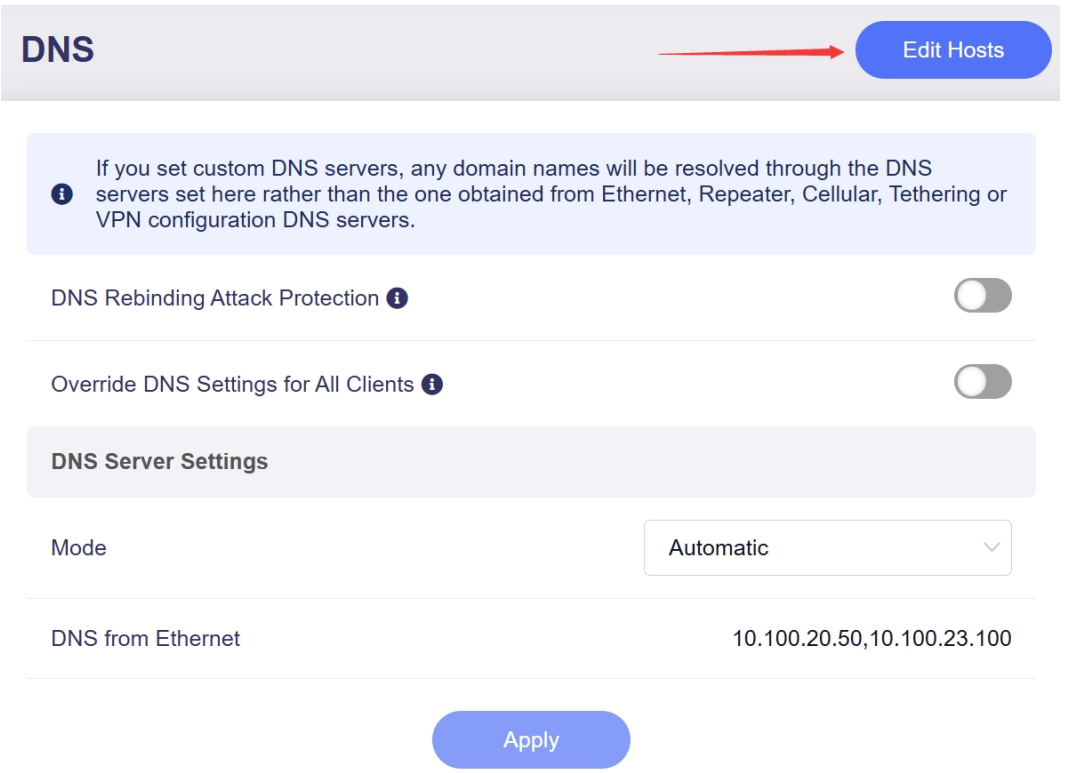
Hinweis: Wenn Sie IPv6-Adressen für manuelles DNS verwenden möchten, aktivieren Sie zunächst IPv6 auf dem Router.

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

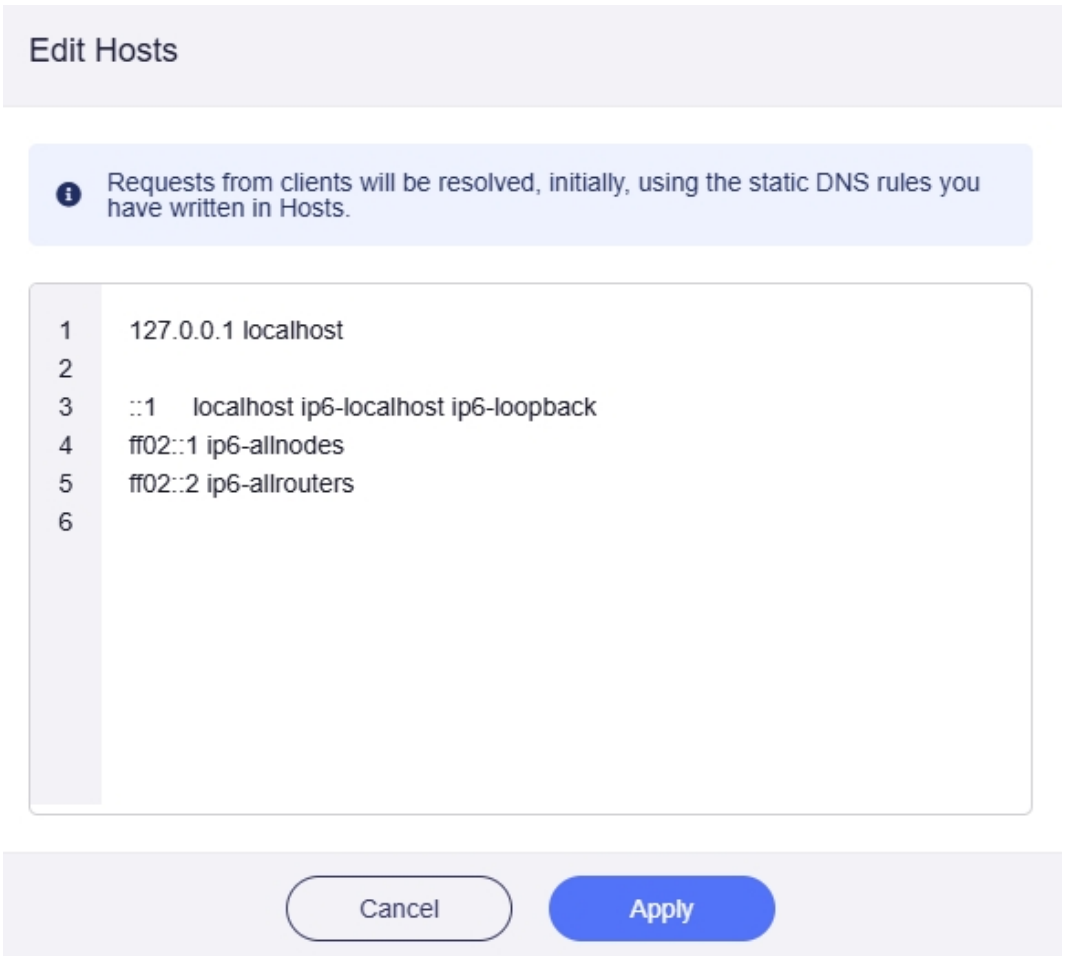


13.5.3 Hosts bearbeiten

Bei Bedarf können Sie statische Regeln für die DNS-Auflösung festlegen.
Klicken Sie auf der DNS-Seite oben rechts auf **Edit Hosts**.



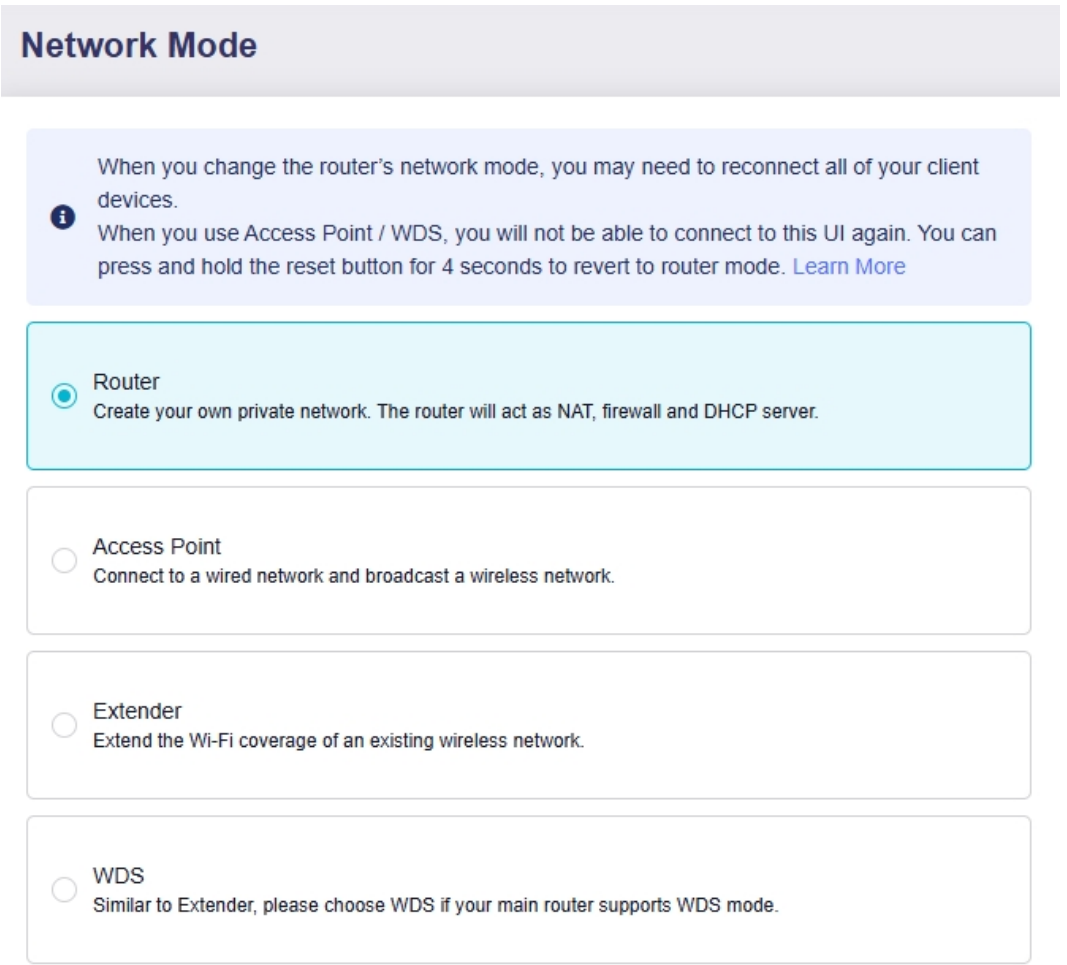
Anfragen von Endgeräten werden vorrangig anhand der hier eingetragenen statischen DNS-Regeln aufgelöst. Sie können Hostnamen manuell IP-Adressen zuordnen und so die Namensauflösung gezielt steuern. Ein Beispiel ist der Standardeintrag „127.0.0.1 localhost“ fü r die lokale Loopback-Adresse.


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

13.6 Netzwerkmodus

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

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



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

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

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

Hinweis:

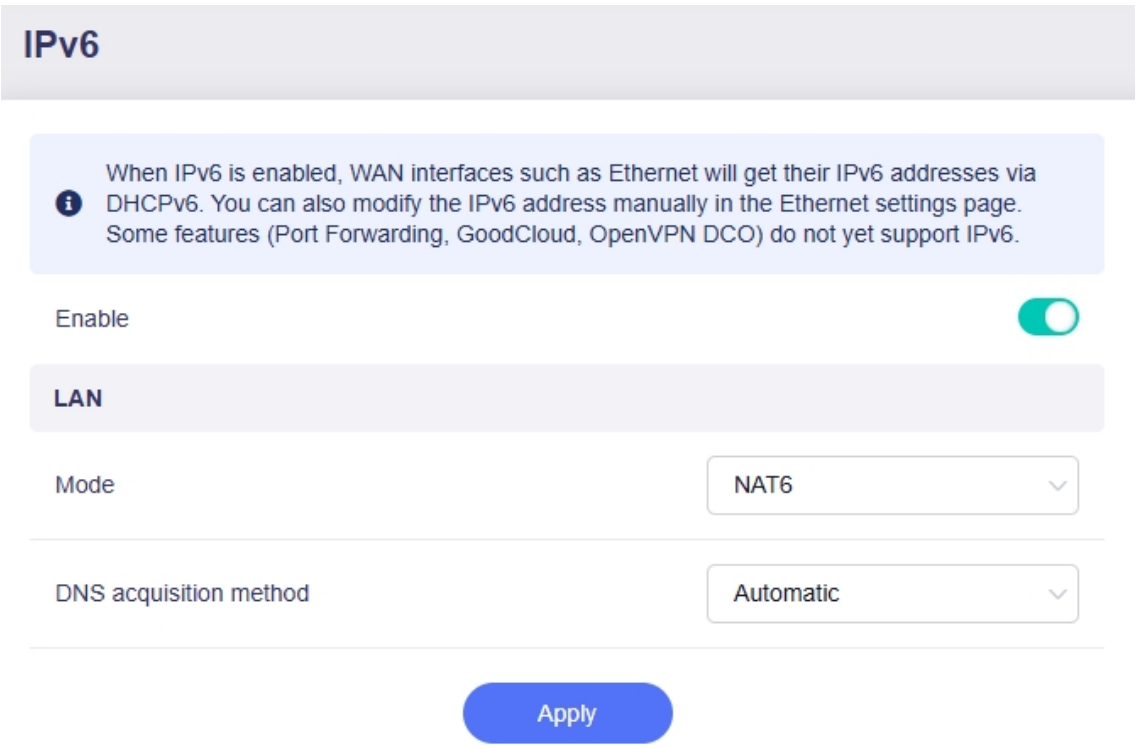
1. Nach einer Änderung des Netzwerkmodus sollten sich alle Endgeräte erneut mit dem Router verbinden, um eine stabile Verbindung sicherzustellen.
2. **Im Access-Point- und WDS-Modus ist die Weboberfläche nicht mehr über die ursprüngliche IP-Adresse erreichbar**. Melden Sie sich am vorgeschalteten Router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

13.7 IPv6

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

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

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



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

13.7.1 IPv6-Modus

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

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

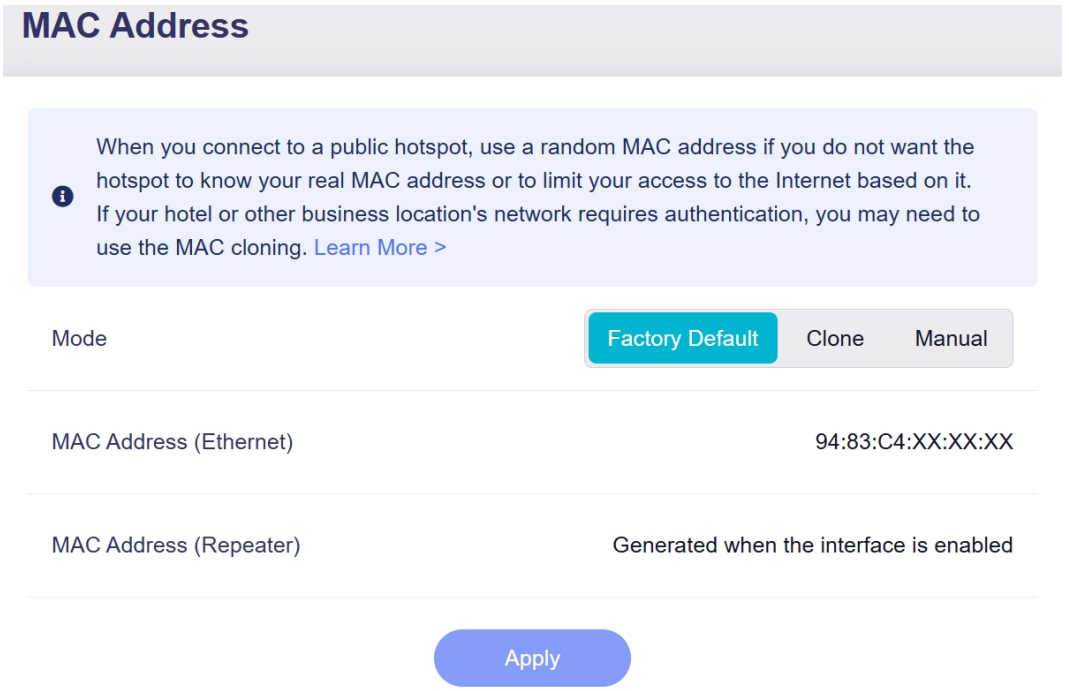
13.7.2 DNS-Adressen beziehen

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

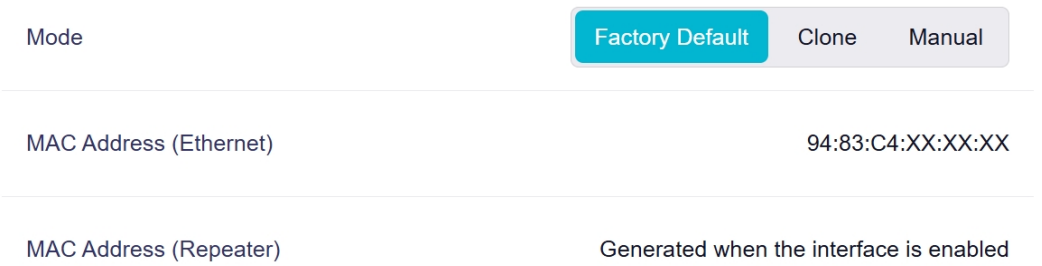
- **Automatic**: Der Router bezieht die IPv6-DNS-Serveradressen dynamisch, etwa über DHCPv6.
- **Manual**: Geben Sie eigene IPv6-DNS-Serveradressen ein. Da DNS Domainnamen in die zugehörigen IP-Adressen auflöst, kann eine manuelle Konfiguration zu Fehlern bei der Namensauflösung führen. Verwenden Sie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

13.8 MAC-Adresse

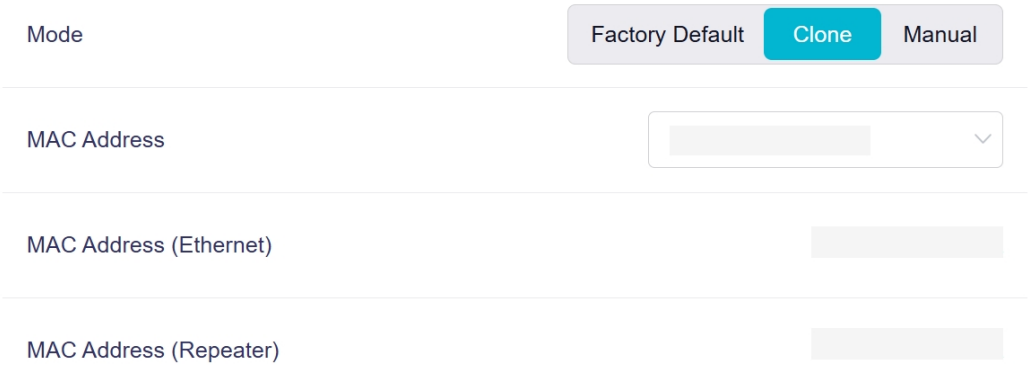
Auf der Seite MAC Address sehen Sie die voreingestellte MAC-Adresse des Routers. Sie können die MAC-Adresse eines Endgeräts klonen, eine Adresse manuell eingeben oder eine zufällige Adresse erzeugen. Unterstützt das Gerät mehrere Ethernetanschlüsse als WAN-Anschlüsse, lässt sich die MAC-Adresse jedes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



- **Werkseitig voreingestellte MAC-Adresse.**

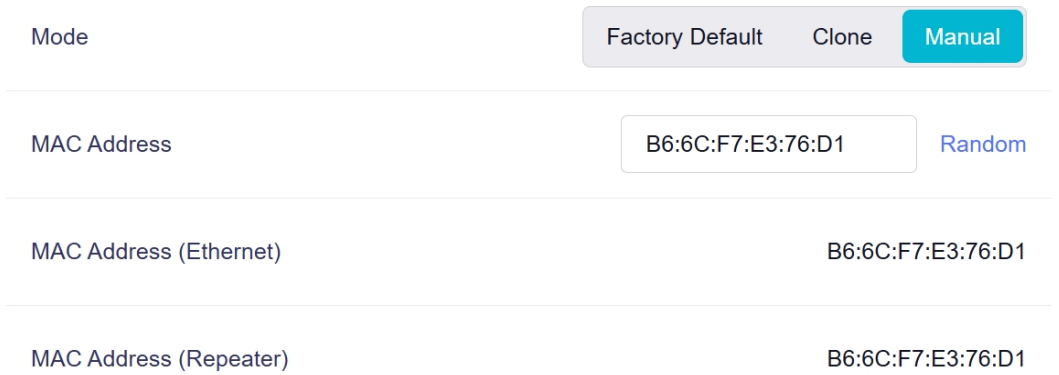


- **MAC-Adresse eines Endgeräts klonen.**



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

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

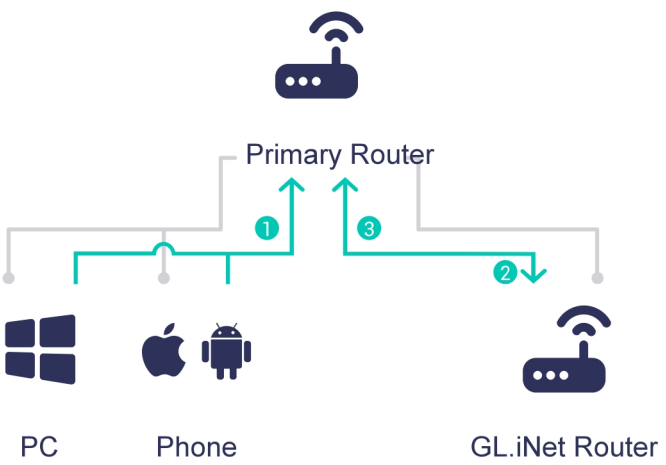


13.9 Drop-in Gateway

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

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

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



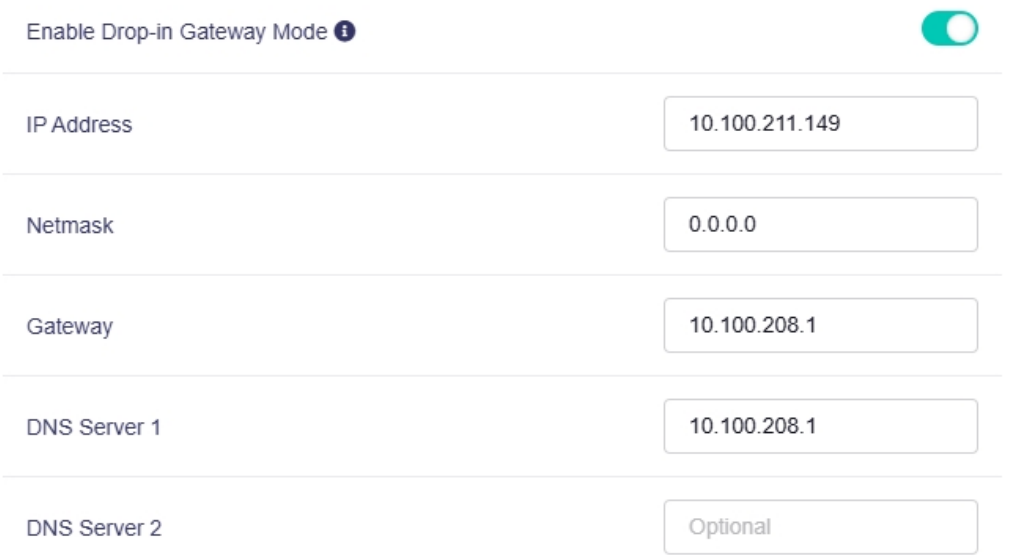
Das obige Diagramm enthält graue Linien sowie grüne Linien mit drei nummerierten Pfeilen.

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

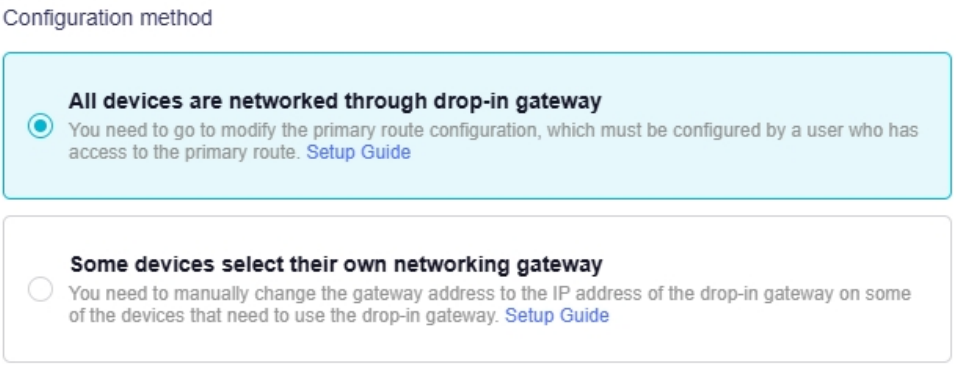
- **Grüne Linien** zeigen den Datenweg bei aktiviertem Drop-in Gateway. Die nummerierten Pfeile geben die Reihenfolge an:
  1. Der Datenverkehr der Endgeräte gelangt zunächst zum Hauptrouter.
  2. Der Hauptrouter leitet ihn zur Verarbeitung an den GL.iNet-Router weiter, etwa zum Filtern von Werbung oder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

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

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



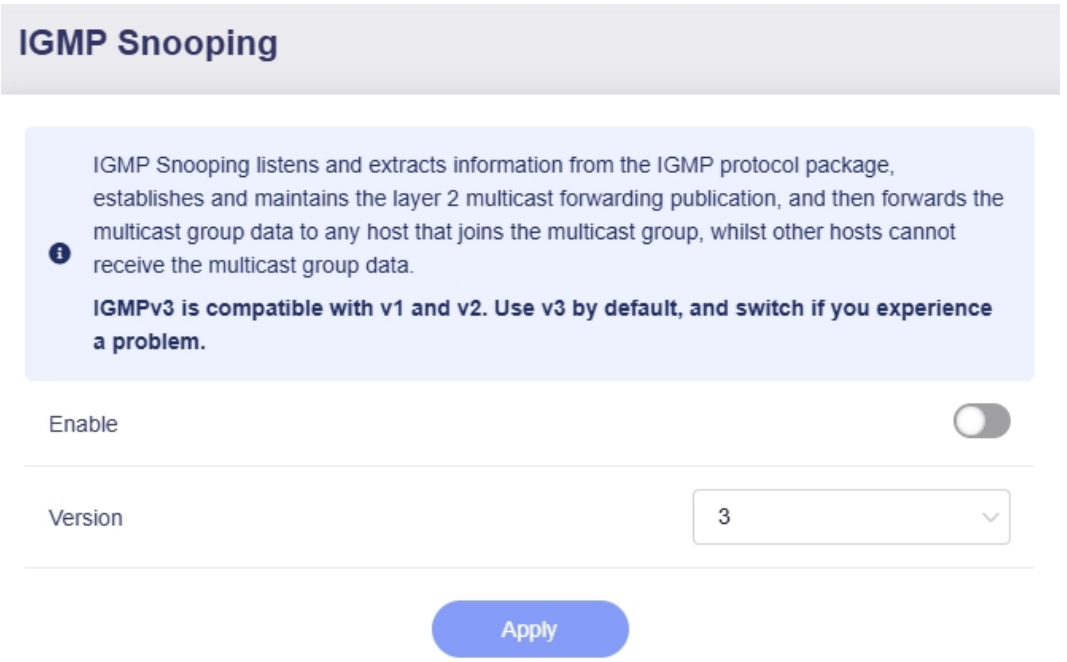
2. Wählen Sie die Konfigurationsmethode aus und klicken Sie auf **Apply**. Einzelheiten finden Sie in dieser Anleitung.


Configuration method
All devices are networked through drop-in gateway
You need to go to modify the primary route configuration, which must be configured by a user who has access to the primary route. Setup Guide
Some devices select their own networking gateway
You need to manually change the gateway address to the IP address of the drop-in gateway on some of the devices that need to use the drop-in gateway. Setup Guide

13.10 IGMP Snooping

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

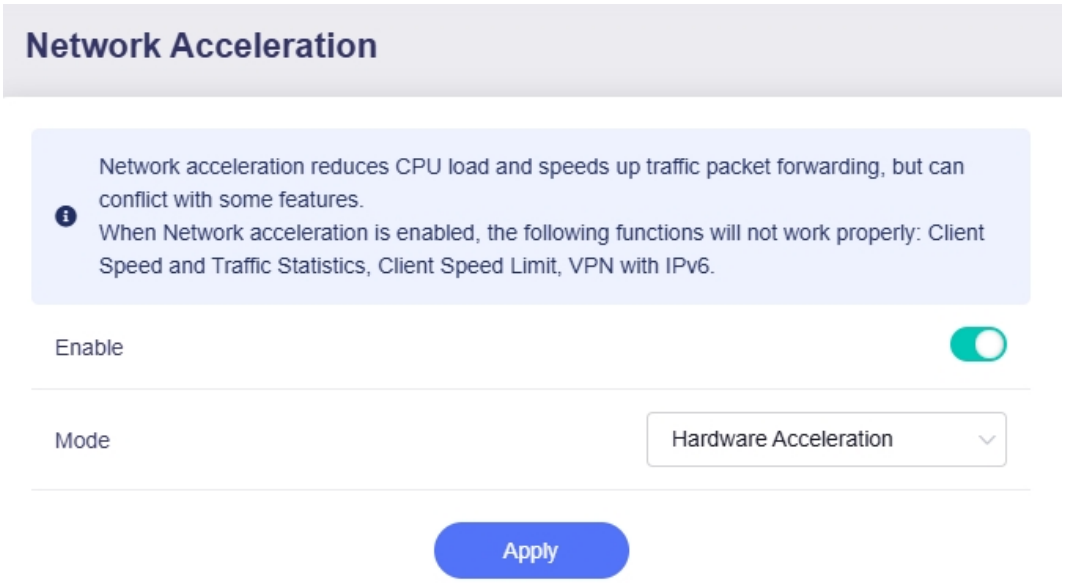
Melden Sie sich an der Weboberfläche an und öffnen Sie **NETWORK** > **IGMP Snooping**. Aktivieren Sie die Funktion bei Bedarf, um Multicast auf Ihrem Router zu nutzen.



13.11 Netzwerkbeschleunigung

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

Melden Sie sich an der Weboberfläche Ihres Routers an und öffnen Sie **NETWORK** > **Network Acceleration**. Hier können Sie die Netzwerkbeschleunigung aktivieren und den Modus Hardware Acceleration auswählen.

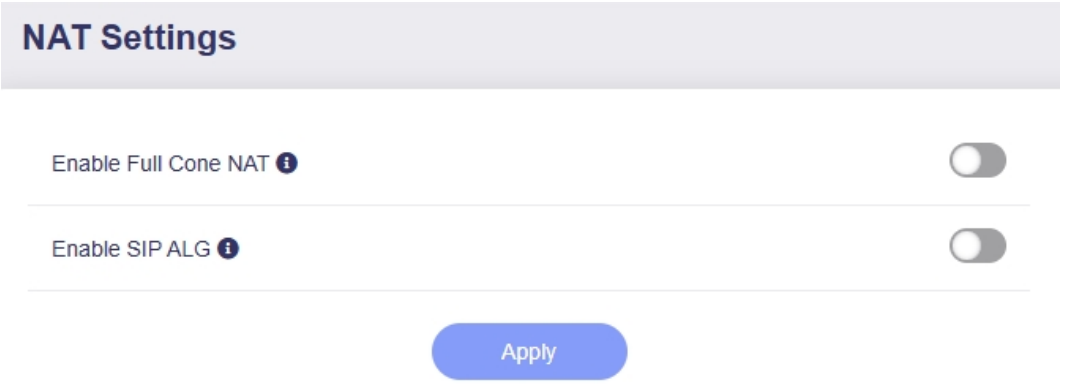


Hardware Acceleration lagert häufig anfallende Netzwerkaufgaben wie NAT, Paketweiterleitung und Prüfsummenprüfung auf spezielle Hardware wie NPUs oder HWNAT-Chips aus. Dieser Modus arbeitet mit Ethernet- und Repeater-Verbindungen. Bei festen Übertragungswegen und einfachen Regeln ermöglicht er einen hohen Durchsatz, geringe Latenzen und eine minimale CPU-Auslastung bei Datenübertragung mit voller Leitungsgeschwindigkeit.

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

13.12 NAT-Einstellungen

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



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

Kapitel 14

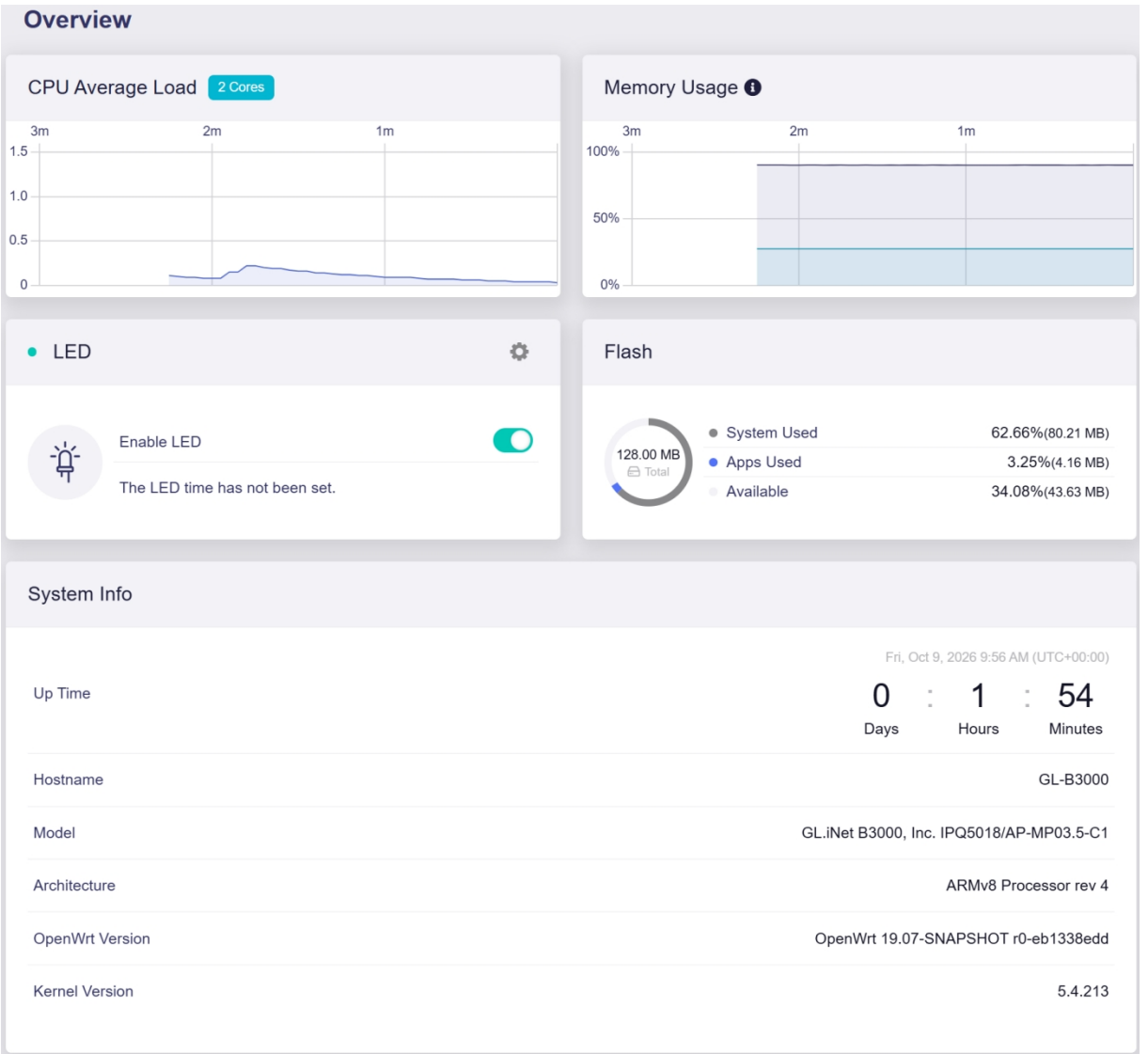
System

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

14.1 Übersicht

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

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

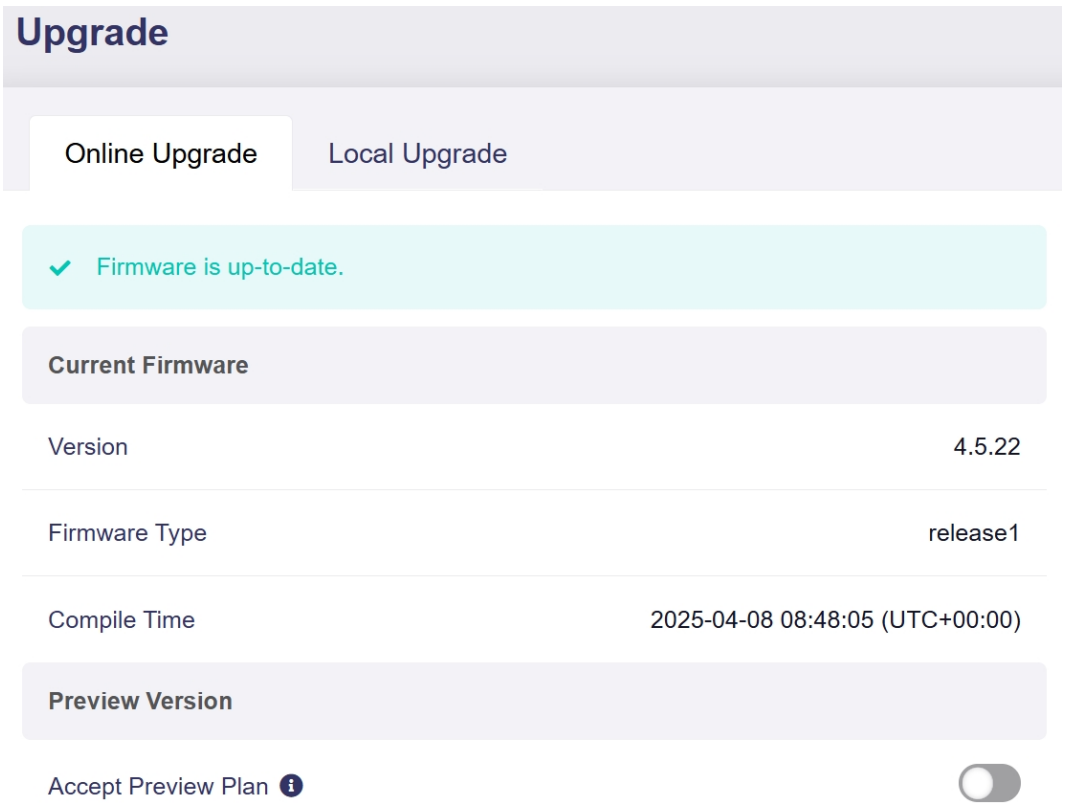


14.2 Aktualisierung

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

14.2.1 Online-Aktualisierung

Hier 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.



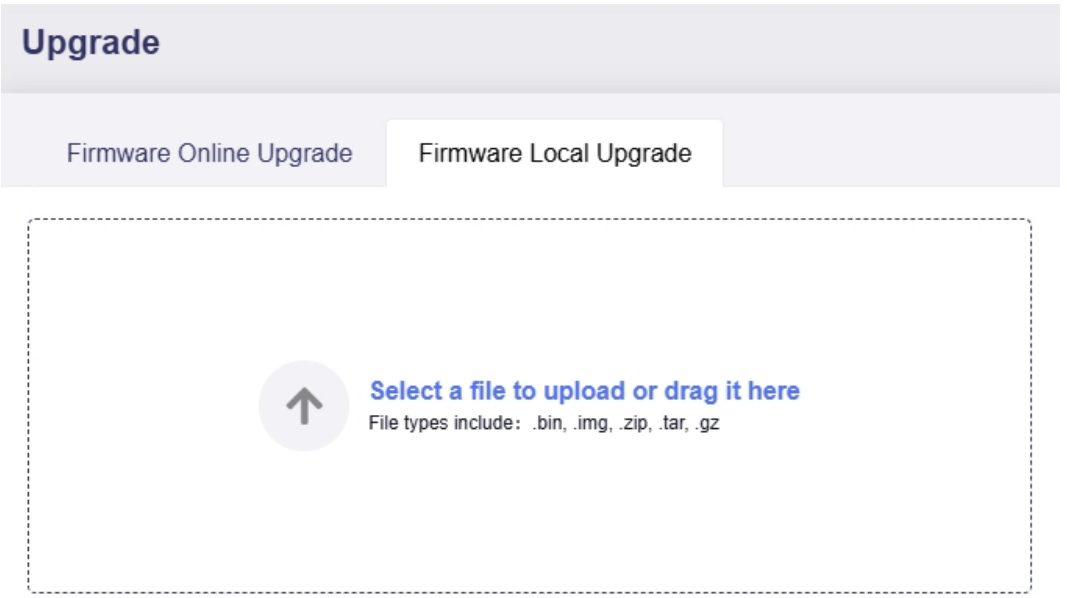
Mit **Accept Preview Plan** können Sie neue Funktionen vor der Veröffentlichung der endgültigen Version ausprobieren und uns Rückmeldung geben. Die Option bleibt nach einmaliger Aktivierung eingeschaltet. Beachten Sie, dass diese Versionen möglicherweise nicht stabil sind.

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

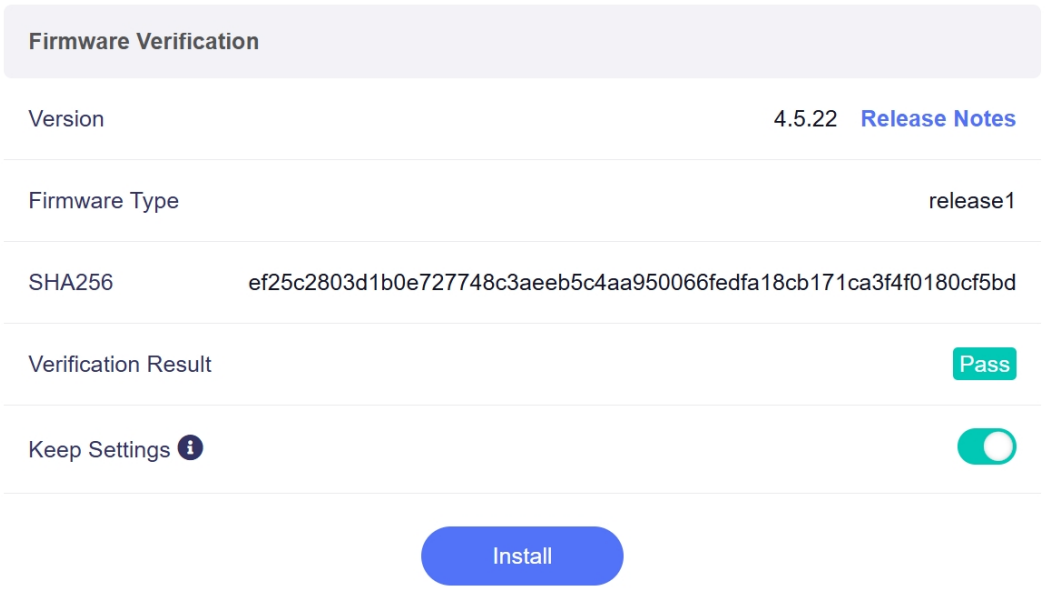
14.2.2 Lokale Aktualisierung

Für die lokale Aktualisierung benötigt der Router keine Internetverbindung.

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



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



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

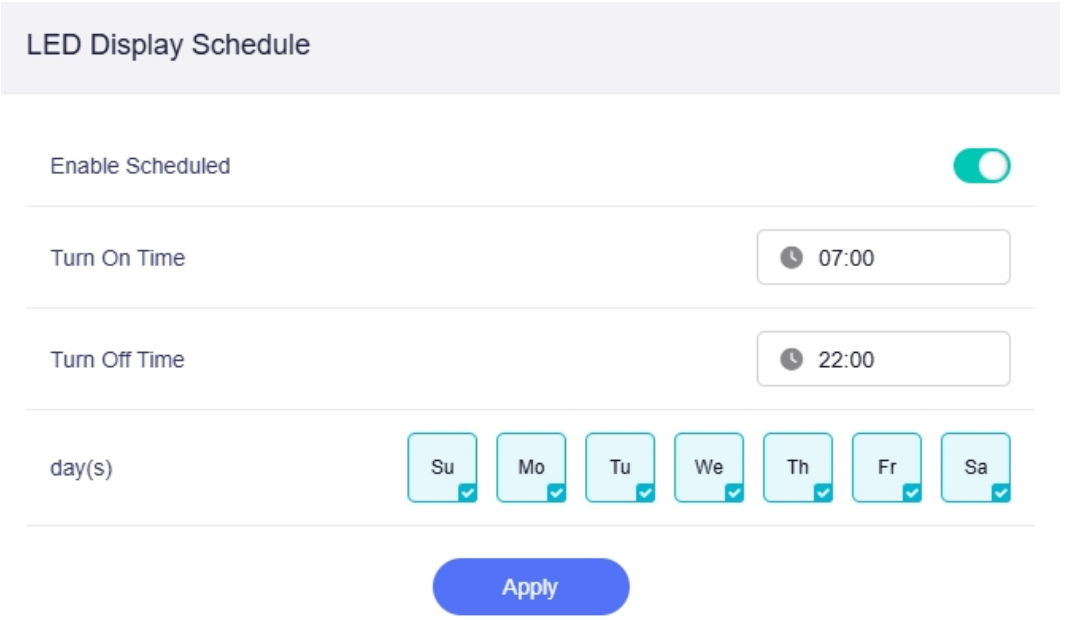
14.3 Geplante Aufgaben

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

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

14.3.1 LED-Zeitplan

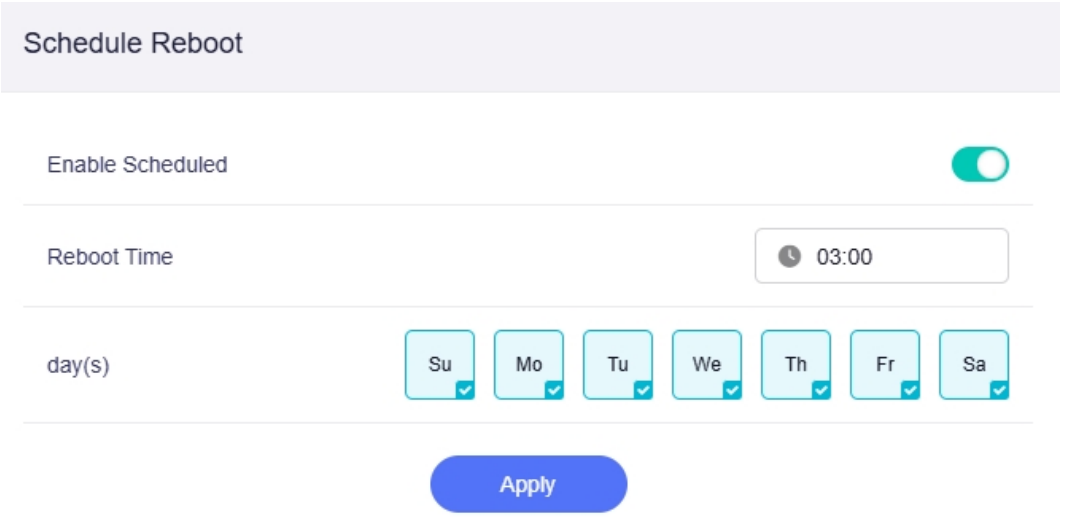
Legen Sie bei Bedarf einen Zeitplan für die Router-LED fest und klicken Sie auf **Apply**.



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

14.3.2 Geplanter Neustart

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



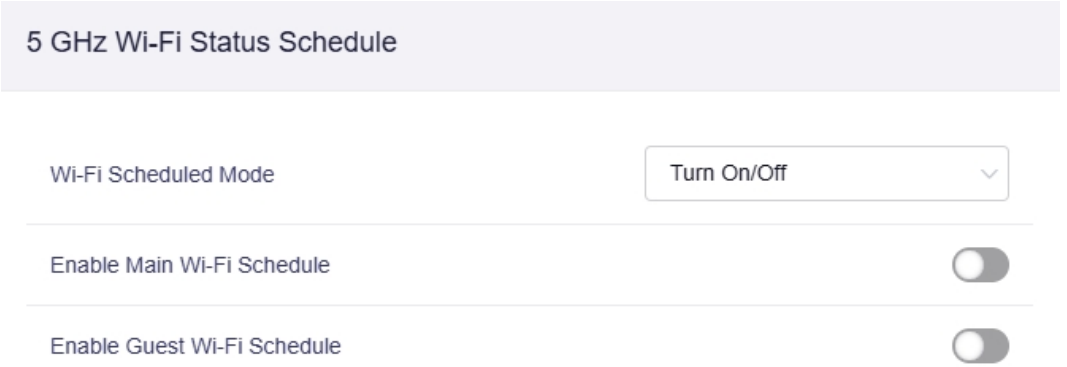
- **Enable Scheduled**: Aktiviert den geplanten Neustart.
- **Reboot Time**: Uhrzeit des Routerneustarts, etwa 03:00 Uhr.
- **day(s)**: Wochentage, an denen die Einstellungen gelten.

14.3.3 Zeitplan für das 5-GHz-WLAN

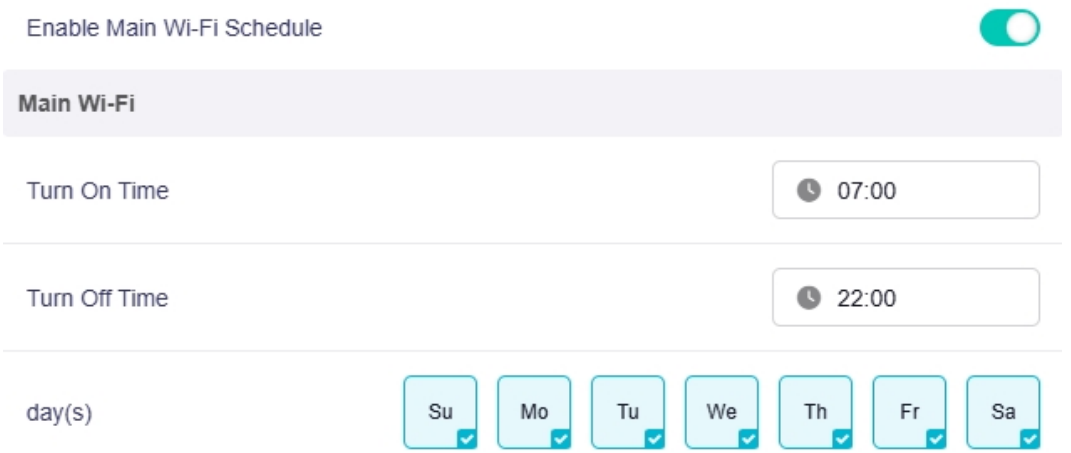
Hier legen Sie einen Zeitplan für Ihr 5-GHz-WLAN fest. Es gibt zwei Modi: Ein-/Ausschalten und Sendeleistung umschalten.

Modus 1: Ein-/Ausschalten

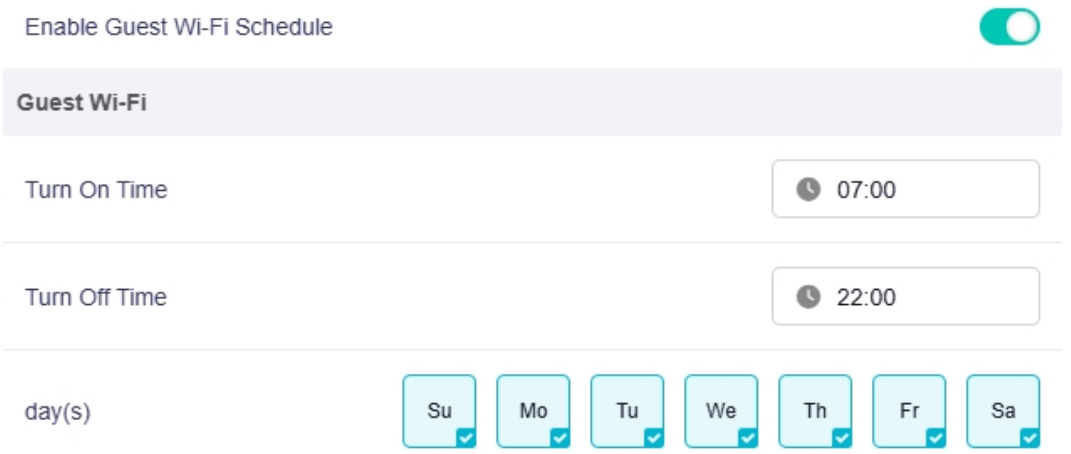
Sie können den Ein-/Ausschaltzeitplan sowohl für das 5-GHz-Hauptnetzwerk als auch für das Gastnetzwerk aktivieren.



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

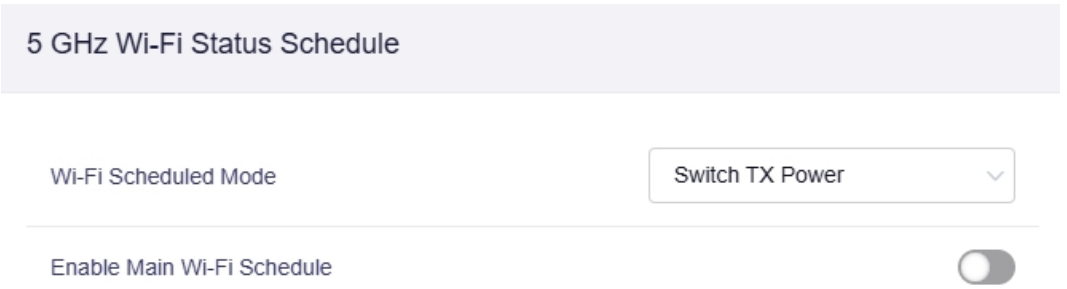


- **Guest Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 5-GHz-Gastnetzwerk fest.

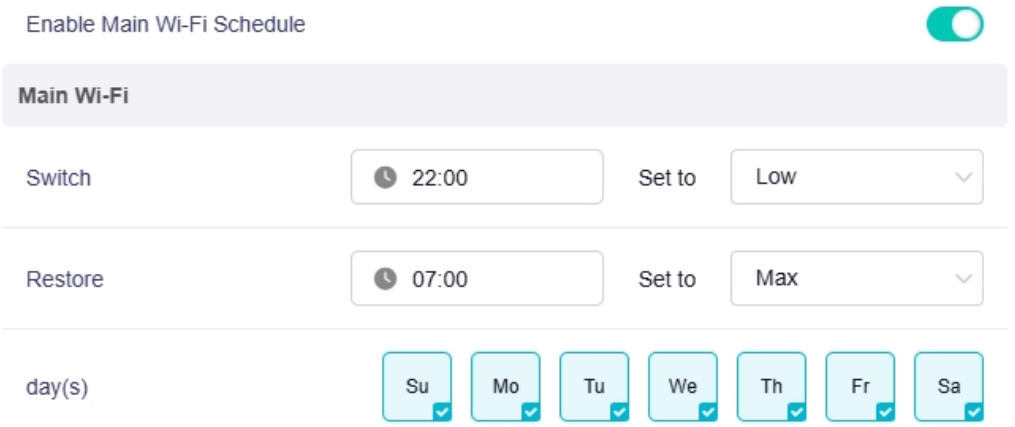


Modus 2: Sendeleistung umschalten

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



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



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

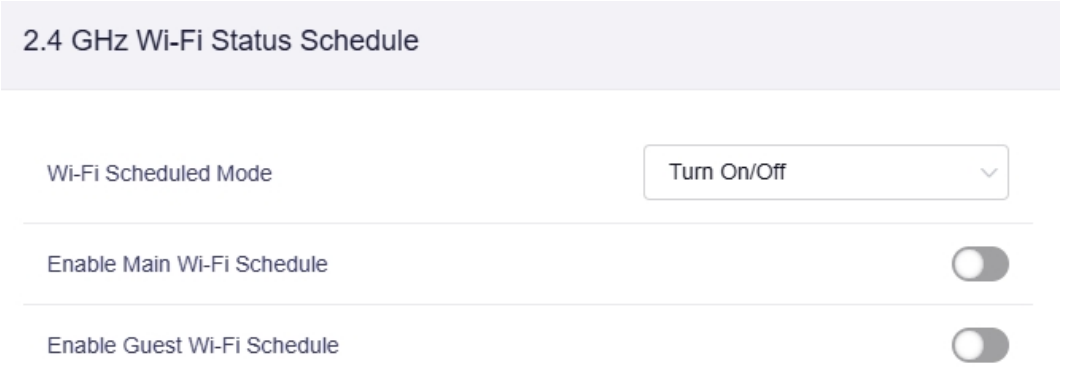
- **Restore**: Setzt die Sendeleistung zu einer anderen Uhrzeit, etwa 07:00 Uhr, auf eine andere Stufe wie Max zurück.
- **days**: Wochentage, an denen die Einstellungen gelten.

14.3.4 Zeitplan für das 2,4-GHz-WLAN

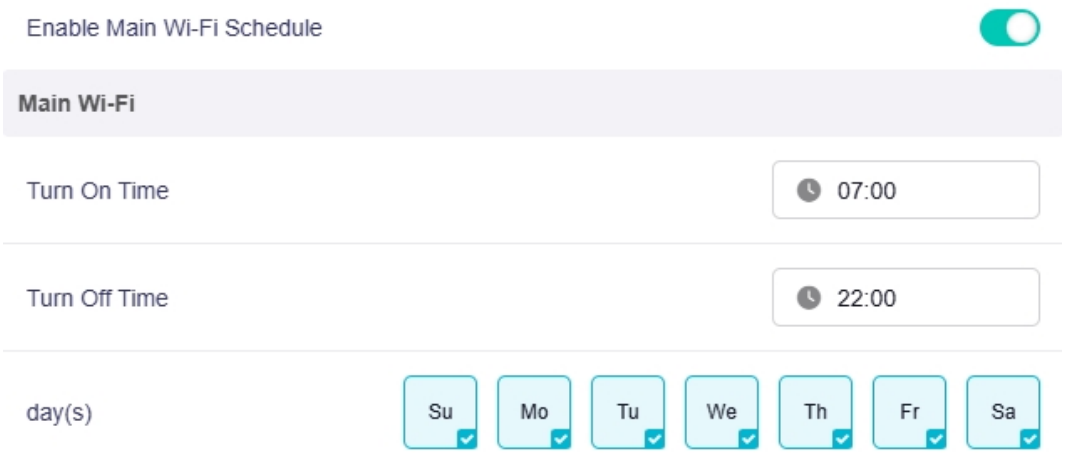
Hier legen Sie einen Zeitplan für Ihr 2,4-GHz-WLAN fest. Es gibt zwei Modi: Ein-/Ausschalten und Sendeleistung umschalten.

Modus 1: Ein-/Ausschalten

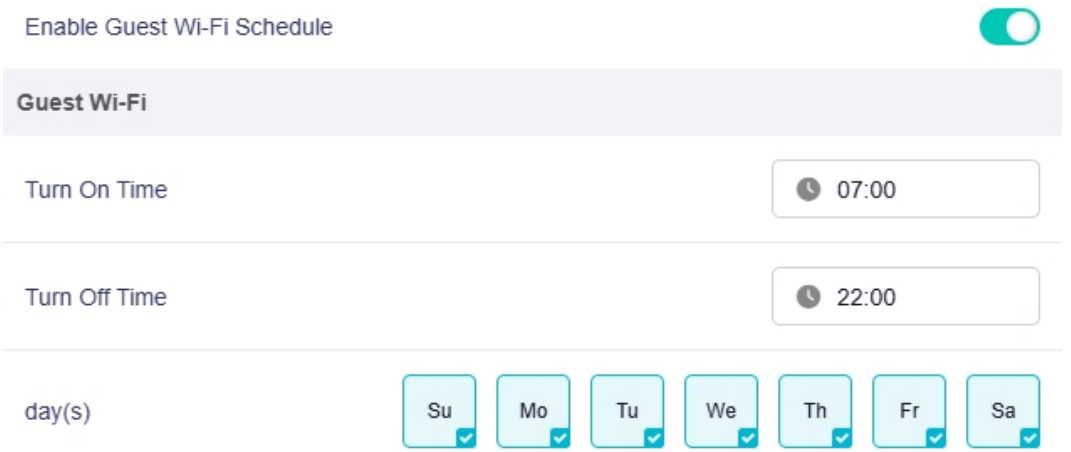
Sie können den Ein-/Ausschaltzeitplan sowohl für das 2,4-GHz-Hauptnetzwerk als auch für das Gastnetzwerk aktivieren.



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

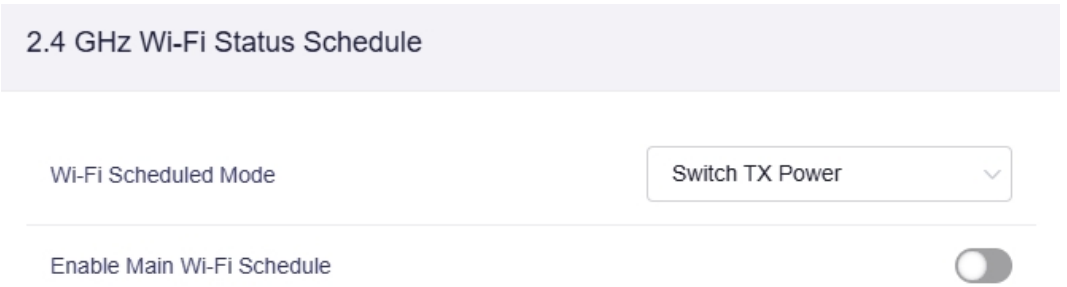


- **Guest Wi-Fi Schedule**: Legen Sie nach der Aktivierung die Ein- und Ausschaltzeiten sowie die Wochentage für Ihr 2,4-GHz-Gastnetzwerk fest.

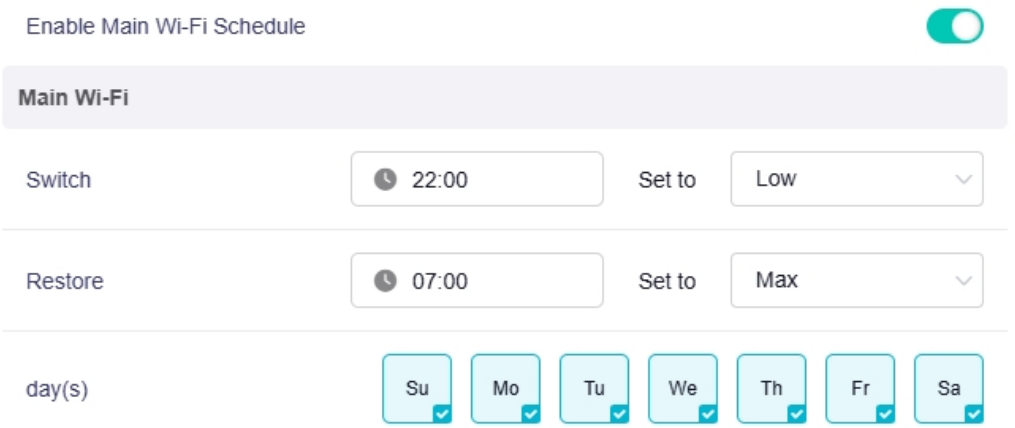


Modus 2: Sendeleistung umschalten

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



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

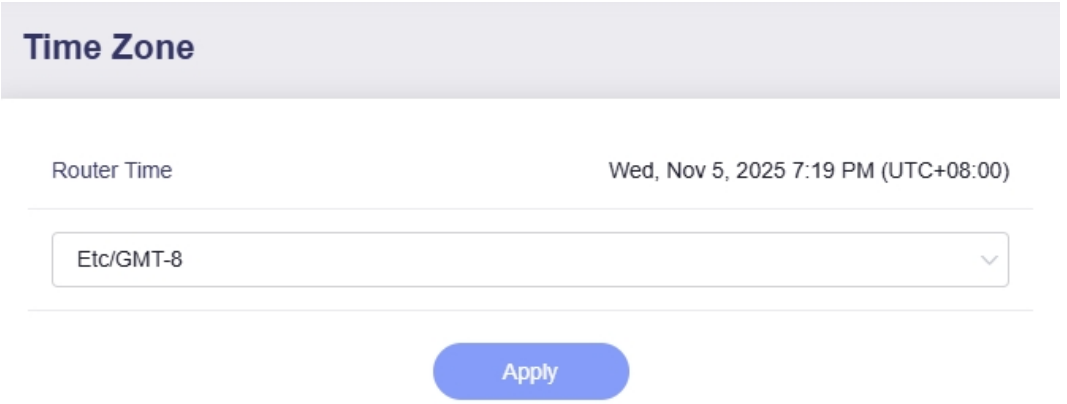


- **Switch**: Stellt die Sendeleistung zu einer bestimmten Uhrzeit, etwa 22:00 Uhr, auf eine festgelegte Stufe wie Low.

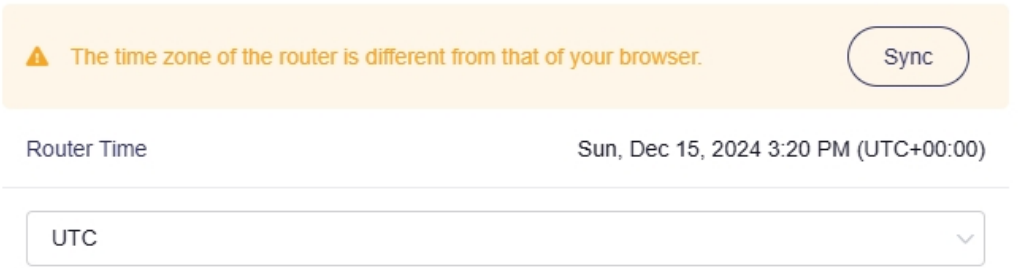
- **Restore**: Setzt die Sendeleistung zu einer anderen Uhrzeit, etwa 07:00 Uhr, auf eine andere Stufe wie Max zurück.
- **days**: Wochentage, an denen die Einstellungen gelten.

14.4 Zeitzone

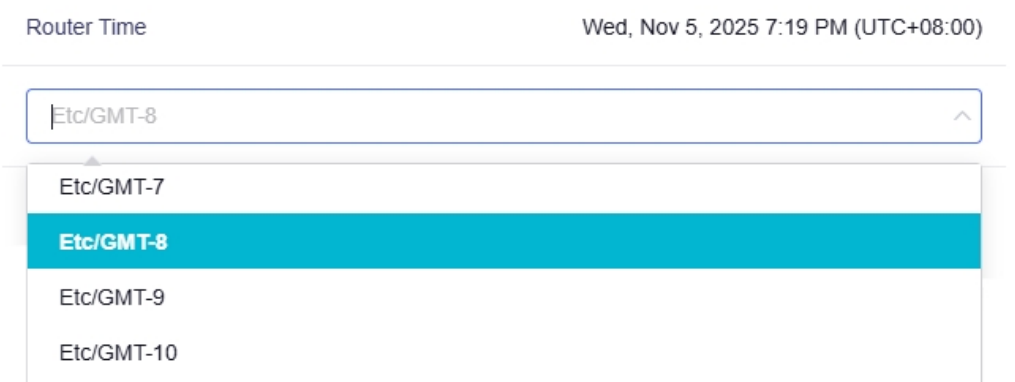
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Time Zone**. Die Seite zeigt die Systemzeit Ihres Routers mit Datum, Uhrzeit und Zeitzonenversatz an.



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

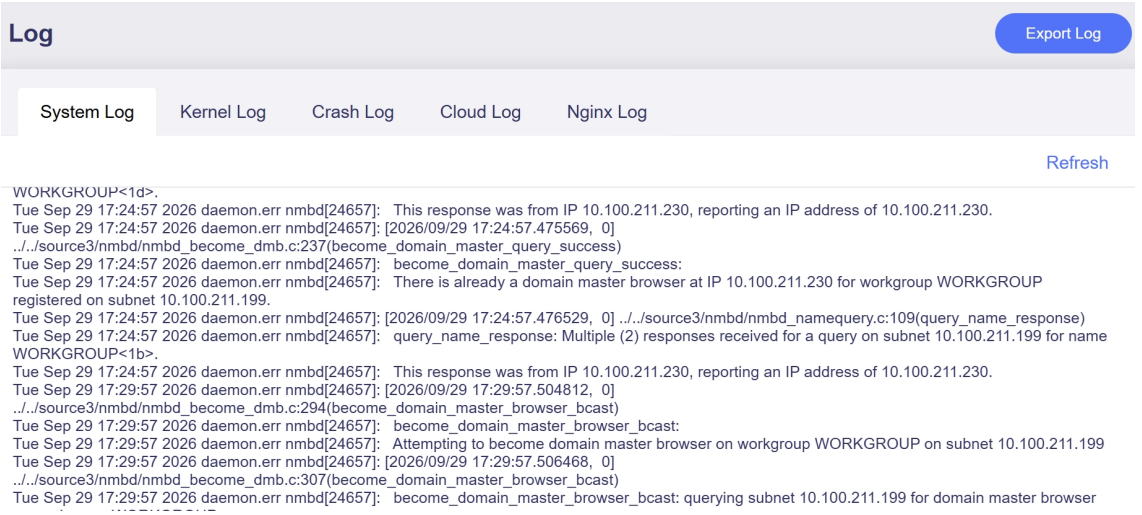


Wählen Sie zum Ändern der Zeitzone den passenden Eintrag aus der Liste, damit die Routerzeit Ihrer Ortszeit entspricht.



14.5 Protokolle

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



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

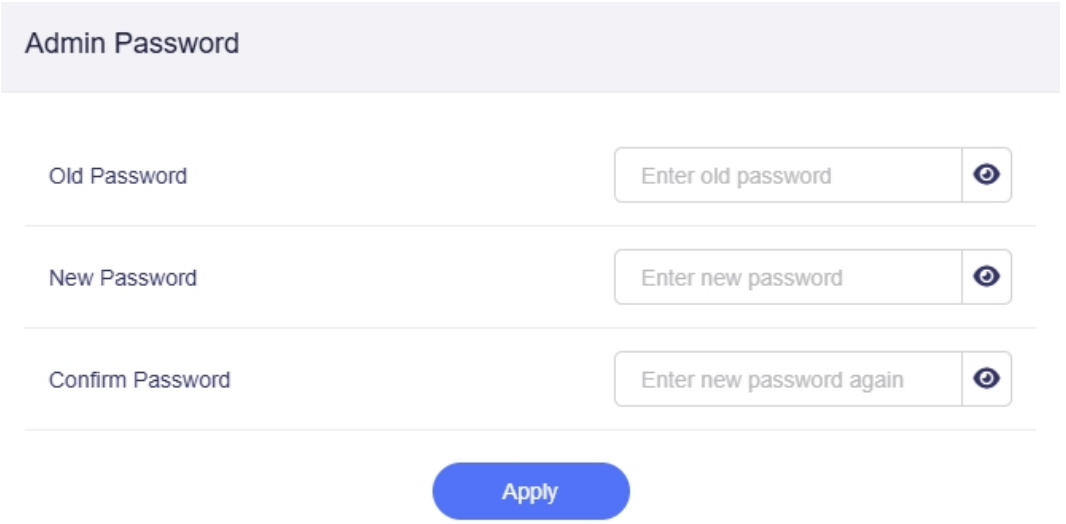
14.6 Sicherheit

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

- Administratorpasswort
- Lokaler Zugriff auf Weboberfläche, LuCI und SSH
- HTTPS-/SSH-Fernzugriff
- Offene Ports am Router

14.6.1 Administratorpasswort

In diesem Abschnitt ändern Sie das Anmeldepasswort der Weboberfläche.

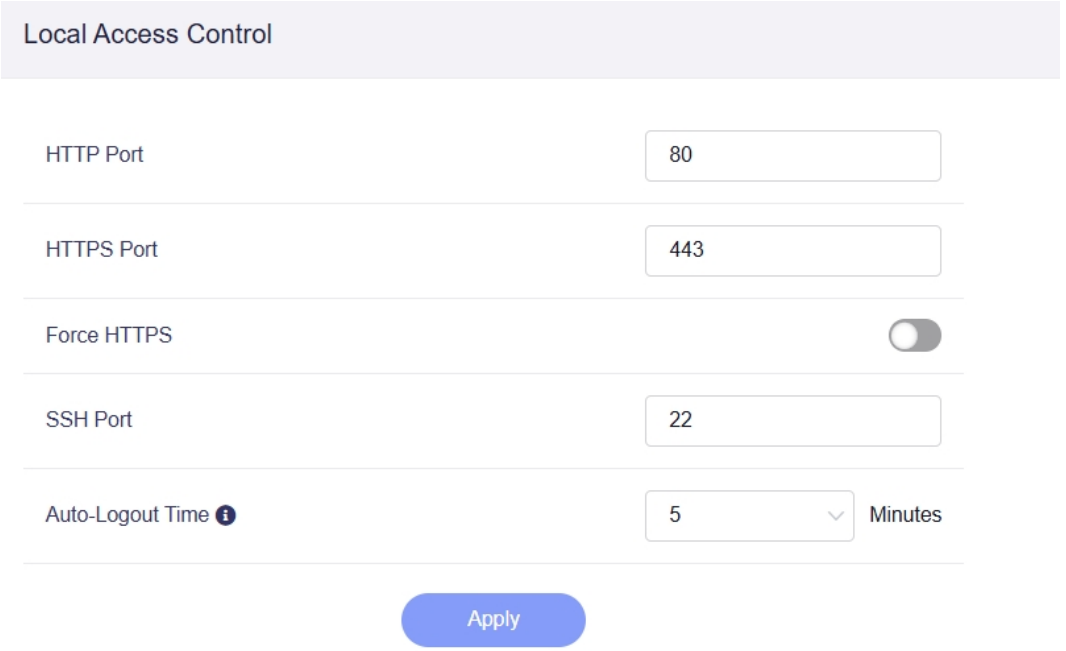


Für das Administratorpasswort gelten folgende Anforderungen:

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

14.6.2 Lokale Zugriffskontrolle

Dieser Abschnitt steuert den Zugriff auf die Verwaltungszugänge des Routers, etwa Weboberfläche und SSH. Er hilft, Scan- und Angriffsversuche auf Standardports zu verhindern und Netzwerkprobleme durch Portkonflikte zu vermeiden.

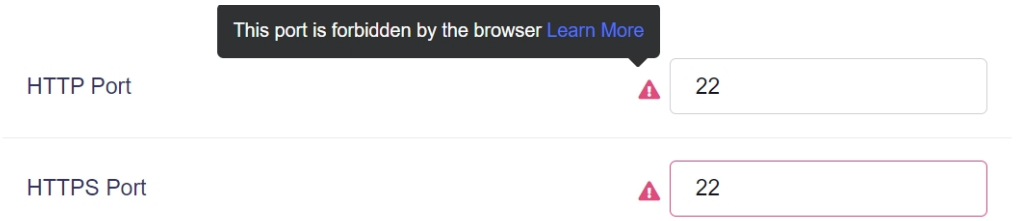


Weboberfläche

- **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.
- **SSH Port**: Standardmäßig 22; für den SSH-Zugriff auf den Router.
- **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.

Hinweis:

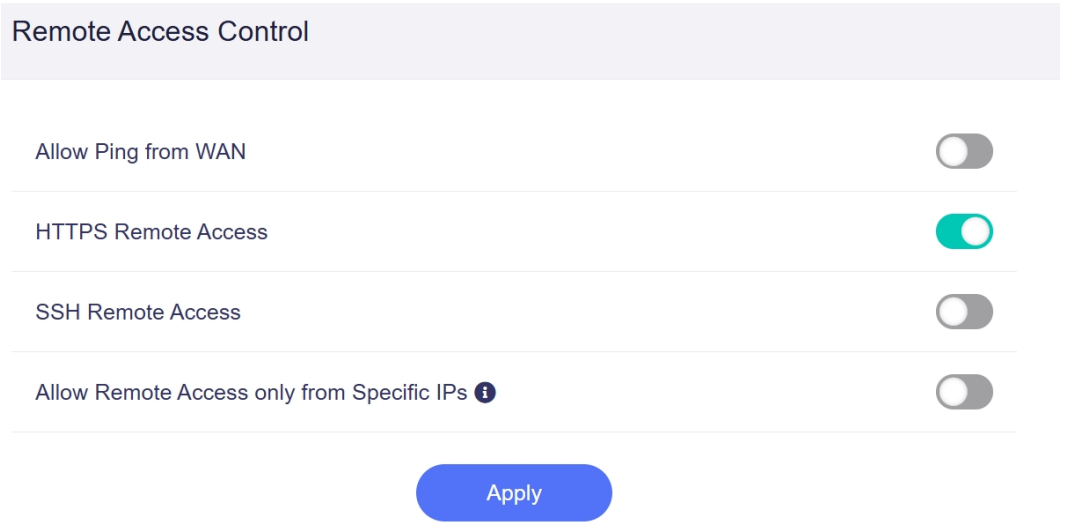
1. Wenn Sie einen reservierten Port oder einen von Browsern beziehungsweise Netzwerkkonventionen bestimmten Diensten vorbehaltenen Port auswählen, erscheint die Meldung „This port is forbidden by the browser“.



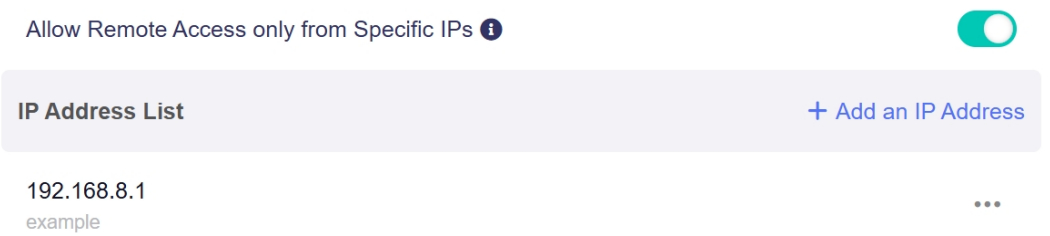
2. Nach einer Änderung der Portnummer in der Firmware müssen Sie die neue Portnummer beim Aufrufen der Weboberfläche angeben. Haben Sie sie vergessen, setzen Sie den Router zurück, um den Standardport wiederherzustellen.

14.6.3 Fernzugriffskontrolle

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



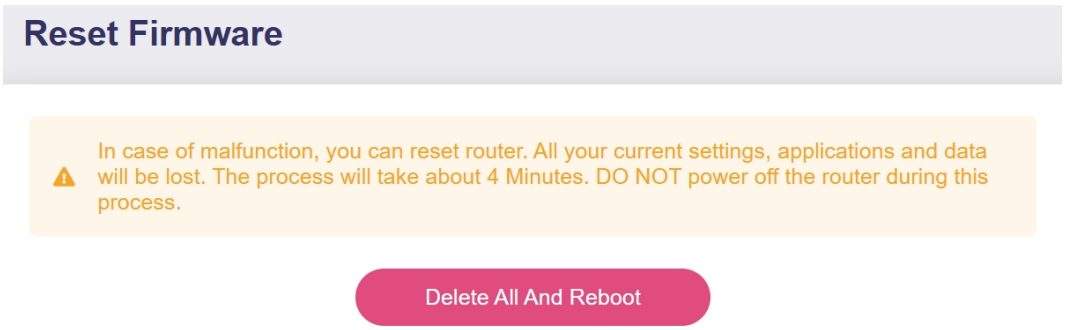
- **Allow Ping from WAN**: Erlaubt Ping-Anfragen von der WAN-Seite. Bei Netzwerkproblemen können Sie damit die Erreichbarkeit des Routers sowie Latenz und Paketverlust prüfen.
- **HTTPS Remote Access**: Ermöglicht den sicheren Fernzugriff auf die Weboberfläche über HTTPS. Die Datenübertragung bei der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



14.7 Firmware zurücksetzen

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

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



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

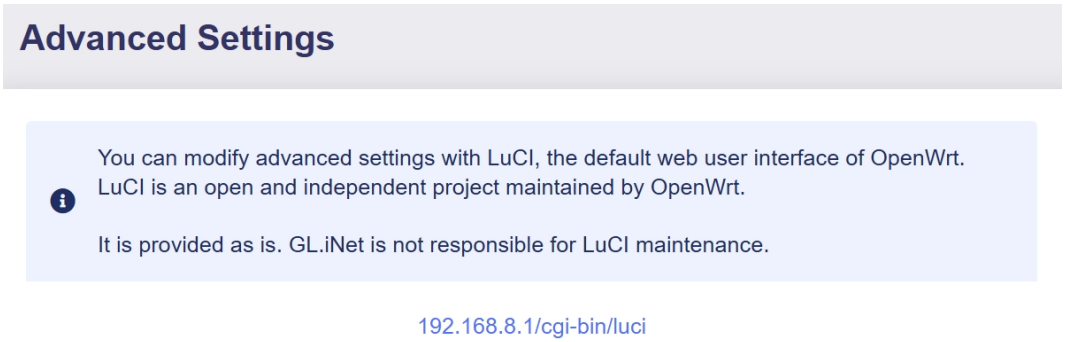
Falls Sie die Weboberfläche nicht erreichen, setzen Sie den Router mit der seitlichen Reset-Taste zurück.

14.8 Erweiterte Einstellungen

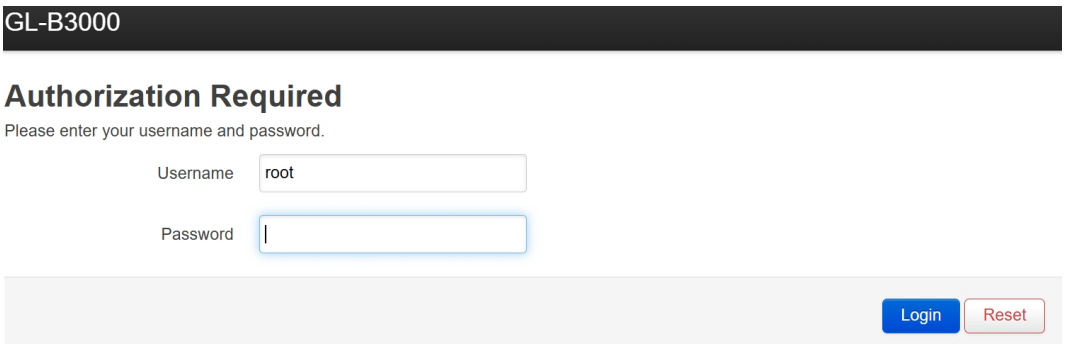
Melden Sie sich an der Weboberfläche an und öffnen Sie **SYSTEM** > **Advanced Settings**. Hier ändern Sie erweiterte Einstellungen in LuCI, der standardmäßigen OpenWrt-Weboberfläche. LuCI ist ein offenes, unabhängiges Projekt, das von OpenWrt gepflegt und in der vorliegenden Form bereitgestellt wird.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

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

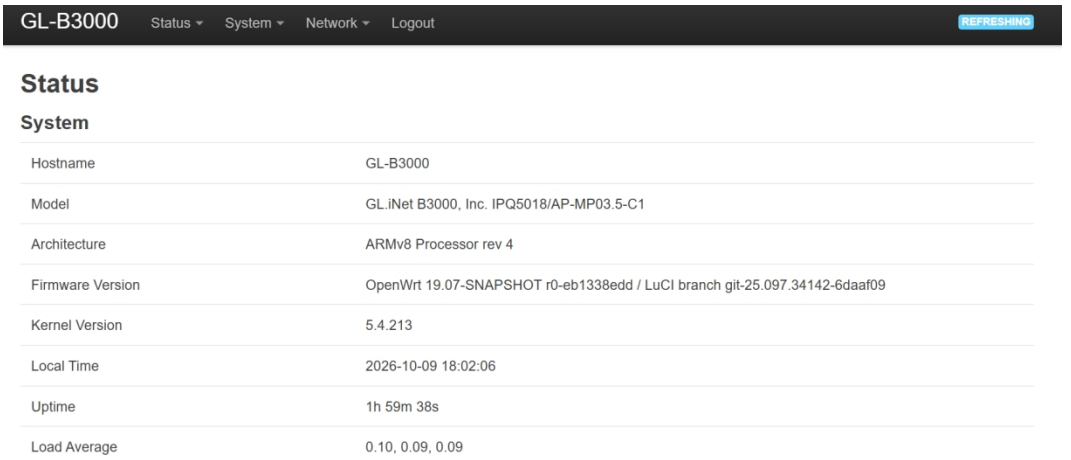
1. Klicken Sie auf den Zugriffslink, um zur LuCI-Anmeldeseite zu gelangen.



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



Sie sind nun an der LuCI-Oberfläche angemeldet.


GL-B3000
Status
System
Network
Logout
REFRESHING
Status
System
Hostname
GL-B3000
Model
GL.iNet B3000, Inc. IPQ5018/AP-MP03.5-C1
Architecture
ARMv8 Processor rev 4
Firmware Version
OpenWrt 19.07-SNAPSHOT r0-eb1338edd / LuCI branch git-25.097.34142-6daaf09
Kernel Version
5.4.213
Local Time
2026-10-09 18:02:06
Uptime
1h 59m 38s
Load Average
0.10, 0.09, 0.09