GL·iNet



Benutzerhandbuch

GL-MG1300/Mango 2

Dual-Band Mini-Reiserouter

Firmware Version 4.10.0

Über dieses Handbuch

Dieses Handbuch ist Ihre Anlaufstelle für den Einstieg in Ihr Gerät und umfasst grundlegende Produktinformationen, Hardwareverbindungen, die Anmeldung der Webmanagementschnittstelle, die Ersteinrichtung und detaillierte Anweisungen für alle Softwarefunktionen im Web-Admin-Panel.

Mit diesem Leitfaden können Sie:

- Verstehen Sie die wichtigsten Produktdetails
- Wählen Sie einen geeigneten Ort für das Gerät
- Komplette Hardware-Anbindungen über Schritt-für-Schritt-Anleitung
- Melden Sie sich mit Leichtigkeit in die Web-Management-Schnittstelle ein
- Konfigurieren Sie die Anfangseinstellungen und beherrschen Sie alle Softwarefunktionen im Web-Admin-Panel

Formatvereinbarungen

Diese Symbole/Farben helfen Ihnen, Schritte schneller zufolgen.

Übereinkommen	Was es bedeutet
HervorgehobenerTeal-Text	Klicken Sie auf einen Link, der eine Webseite oder einen bestimmten Abschnitt öffnet.
FetterText	Hebt wichtige Informationen in diesem Dokument hervor, beispielsweise Titel, Hyperlinks sowie genaue Menü- / Elementnamen auf der Weboberfläche des Geräts.
>	Der Pfad zum Laden der entsprechenden Seite (z.B. System > Firmware)
Hinweis:	Wichtige Informationen für Einrichtung, Betrieb und Sicherheit: Das Ignorieren dieser Hinweise kann zu einem fehlgeschlagenen Aufbau, einer Geräte- Fehlfunktion oder zu Beschädigungen führen.
Tipps	Ratschläge, die Ihnen helfen, Ihr Gerät besser zu nutzen

Hinweis:

- Die Gerätemerkmale können je nach Modell und Firmware-Version variieren.
- Die Verfügbarkeit der Produkte unterliegt regionalen Unterschieden oder ISP-Spezifikationen.
- Alle Bilder, Verfahren und Beschreibungen in diesem Handbuch dienen nur zur Veranschaulichung und können von Ihrer tatsächlichen Nutzungserfahrung abweichen.

Brauchen Sie mehr Hilfe oder Info?

- Firmware Update: GL.iNet Firmware Download Center | Router
- Community: Diskutieren Sie unsere Produkte und teilen Sie Einblickeauf dem GL.iNet Community Forum.
- Support: Kontaktieren Sie unseren technischen Support auf der Kontaktseite.

Copyright © 2026 GL.iNet Technology (HK) Ltd. Alle Rechte vorbehalten.
Kein Teil dieses Handbuchs darf ohne vorherige schriftliche Genehmigung von GL.iNet Technology (HK) Ltd. reproduziert, transkribiert, übersetzt oder in irgendeiner Form oder auf irgendeine Weise verteilt werden. GL.iNet ist eine eingetragene Marke von GL.iNet Technology (Hong Kong) Ltd. in China und/oder anderen Ländern und Regionen. Alle anderen hierin genannten Marken- und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer.
Der Inhalt dieses Dokuments kann sich ohne vorherige Ankündigung aufgrund von Produktversions- Upgrades oder aus anderen Gründen ändern. Sofern nicht anders vereinbart, wird dieses Dokument nur zu Informationszwecken zur Verfügung gestellt, und alle hierin enthaltenen Erklärungen, Informationen und Empfehlungen stellen keine 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 Aussehen 11

1.1.2 Anschlüsse und Taste 12

1.1.3 LED 13

1.2 Spezifikationen 13

1.3 Inhalt der Verpackung 14

Kapitel 2 Hardware-Verbindung 15

2.1 Auswahl eines Standorts 16

2.2 Anschluss des Routers 16

Kapitel 3 An Ihrem Router anmelden 17

Kapitel 4 Internetverbindung einrichten 19

4.1 Schneller Setup-Assistent 20

4.2 Manuelles Einrichten der Internetverbindung 21

4.2.1 Internet über Ethernet-Kabel 22

4.2.2 Internet über vorhandenes Wi-Fi 26

4.2.3 Internet über USB-Tethering 32

4.2.4 Internet über USB-Modem 37

Kapitel 5 WLAN 39

5.1 Wi-Fi Statusanzeige 40

5.2 WLAN Einstellungen 41

5.2.1 Hauptnetz 41

5.2.2 Gastnetzwerk 42

5.2.3 IoT-Netzwerk 44

Kapitel 6 Clients 46

6.1 Gerätedetails 48

6.2 Aktion 50

6.3 Entfernen von Clients 53

6.4 Sortieren 54

Kapitel 7 Cloud Dienst 55

7.1 GL.iNet Konto 56

7.1.1 GL.iNet-Konto aktivieren 56
7.1.2 GL.iNet-Konto freigeben 58
7.2 GoodCloud 59
7.2.1 GoodCloud aktivieren 60
7.2.2 Verwalten Sie Ihren Router 63
7.2.3 Entbindungseinrichtung 66
7.3 GoodPAS 67
7.3.1 Schnelles Setup 67
7.3.2 Konnektivitätsprüfung 71
7.3.3 Upgrade-Plan 72
Kapitel 8 VPN 73
8.1 VPN Grundlagen 74
8.2 Einsatzszenarien 75
8.3 VPN Dashboard 77
8.4 OpenVPN Client 78
8.5 OpenVPN Server 79
8.6 WireGuard Client 80
8.7 WireGuard Server 81
Kapitel 9 Netzwerk 82
9.1 Multi WAN 83
9.1.1 Schnittstellen Statusüberwachung 83
9.1.2 Multi-WAN-Modus 86
9.2 Subnetz 89
9.2.1 Hauptnetzwerk 89
9.2.2 Gastnetzwerk 95
9.2.3 IoT-Netzwerk 99
9.2.4 VLAN-Netze 103
9.3 Ethernet-Port 107
9.3.1 WAN 108
9.3.2 LAN 109
9.3.3 Dual-Ethernet WAN 111
9.4 DNS 113
9.4.1 Einstellungen DNS-Server 114
9.4.2 Hosts-Datei bearbeiten 116

9.5 IPv6 118
9.5.1 IPv6-Modus 119
9.5.2 DNS-Erfassungsverfahren 119
9.6 IGMP Snooping 120
9.7 Netzwerkmodus 121
9.8 Netzwerk-Beschleunigung 124
Kapitel 10 Flusskontrolle 126
10.1 Kindersicherung 127
Kapitel 11 Sicherheit 133
11.1 Port Weiterleitung 134
11.1.1 DMZ 134
11.1.2 Port Weiterleitung 135
11.2 Verwaltungssteuerung 137
11.2.1 Zugangskontrolle 137
11.2.2 Berechtigung des Fernzugriff 139
11.2.3 Öffnen Sie die Ports am Router 140
11.3 NAT-Modus 142
Kapitel 12 Anwendungen 143
12.1 Softwarepakete 144
12.2 Dynamisches DNS 145
12.2.1 DDNS aktivieren 145
12.2.2 Prüfen Sie, ob DDNS funktioniert 148
12.2.3 HTTPS Fernzugriff 150
12.2.4 SSH Fernzugriff 152
12.3 Netzwerk-Speicher 154
12.3.1 Speicher verbinden 154
12.3.2 Setup von Samba 155
12.4 Tailscale 158
12.4.1 Tailscale einrichten 159
12.4.2 WAN-Subnetze bekanntgeben 162
12.4.3 LAN-Subnetze bekanntgeben 163
12.4.4 Manueller Ausgangspunkt 164
12.4.5 Exit-Knoten ausführen 165
Kapitel 13 System 172

13.1 Übersicht 173
13.2 Administrator-Kennwort 174
13.3 Aktualisierung 175
13.3.1 Online-Firmware-Upgrade 175
13.3.2 Lokales Firmware-Upgrade 177
13.4 Geplante Aufgaben 178
13.4.1 LED Display Zeitplan 178
13.4.2 Zeitplan-Neustart 179
13.4.3 5 GHZ Zeitplan 179
13.4.4 2,4 GHZ Zeitplan 181
13.5 Zeitzone 184
13.6 Konfiguration des Schalters 185
13.7 Firmware zurücksetzen 186
13.8 Protokoll 187
13.9 Erweiterte Einstellungen 189
Konformitätserklärung 191

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 behandelt die Routerübersicht, Spezifikationen und Paketinhalte.

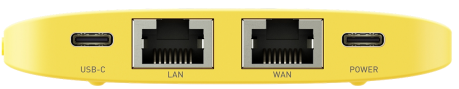
1.1 Produktübersicht

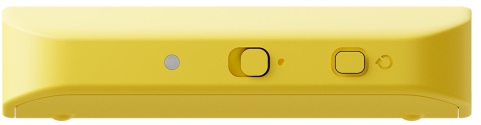
Mango 2 ist der erste Dual-Band-Wi-Fi-5-Mini-Reiserouter von GL.iNet mit ultradünnem, tragbarem Design. Er erreicht theoretische Geschwindigkeiten von 400 Mbps (2.4 GHz) und 866 Mbps (5 GHz) per 2×2-MIMO. OpenVPN und WireGuard sind vorinstalliert; er unterstützt über 30 VPN-Dienste, verschlüsselt den Netzwerkverkehr automatisch und erlaubt die Fernverwaltung über GoodCloud. Er vereint Leistung, Praktikabilität und Sicherheit.

1.1.1 Aussehen

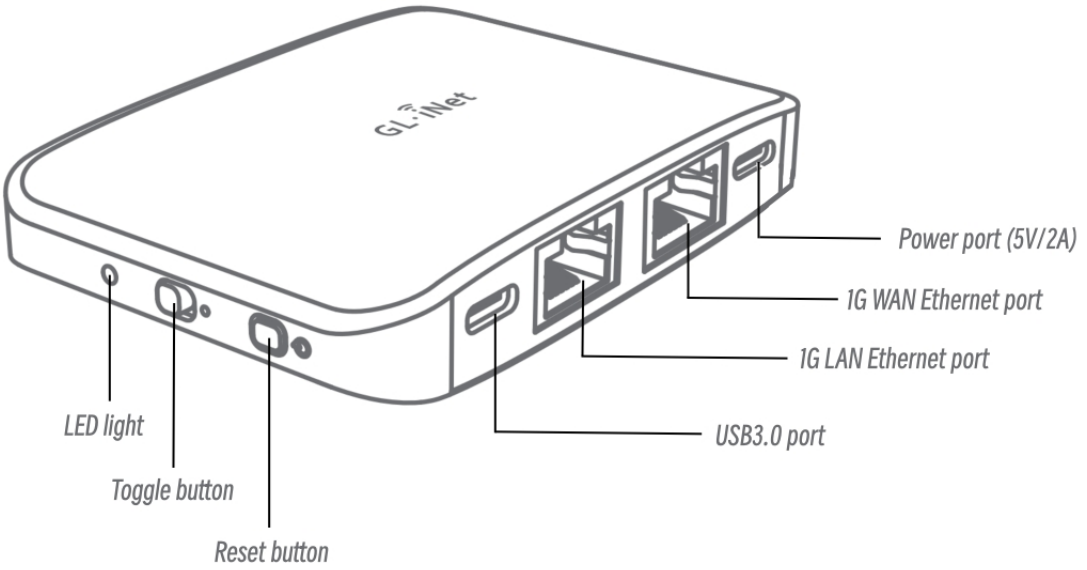








1.1.2 Anschlüsse und Taste



Element	Beschreibung
Power-Port	Verbindet sich mit dem Netzteil.
1G WAN Port	Verbindet sich mit einem Modem oder einer Ethernet-Steckdose für das Internet.
1G LAN Port	Verbindet sich bei Bedarf mit kabelgebundenen Geräten.
USB 3.0 Port	für USB-Speichergeräte, Telefon-USB-Tethering und kompatible zellulare Dongles.
Reset-Taste	Drücken und halten Sie für **3 Sekunden** und lassen Sie dann los, um Ihre Reparatur zu reparieren Netz.
	Drücken und halten Sie für **8 Sekunden** und dann loslassen, um die Zurücksetzung Router zum Factory Default.
Umschaltknopf	Ein physischer Switch, der ausgewählte Routereinstellungen mit einem flip. Sie können es im Web-Admin-Panelkonfigurieren, um es zu aktivieren Ein-Klick-Schalten von spezifischen Funktionen.

1.1.3 LED

Status	Angabe
Festblau	Anlauf
Blau pulsieren langsam	Start, aber keine Internetverbindung
Vollständig weiß	Angebunden an das Internet
Blau blinken schnell	Rücksetzung

1.2 Spezifikationen

Schnittstelle	1 x1G WAN Ethernet Port 1 x1G Ethernet Port 1 x USB 3.0 Port 1 x Typ-C Power Port 1 xReset-Taste 1 xToggle-Button
CPU	MediaTek, Dual-Core @880MHz
Speicher/Speicher	DDR3 128MB / NOR 2MB + NAND 128MB
Protokoll	IEEE 802.11a/b/g/n/ac
Wi-Fi-Geschwindigkeit	400Mbps (2,4 GHZ),866Mbps (5 GHZ)
Antennen	2 x Interne Wi-Fi-Antennen
Ethernet-Geschwindigkeit	10/100/1000Mbps
Leistungseingang	TypC,5V/2A
Stromverbrauch	<5W (ohne USB-Last)
Betriebstemperatur	0 ~ 40°C (32 ~ 104°F)
Lagertemperatur	-20 ~ 70°C (-4 ~ 158°F)
Abmessungen/Gewicht	89 x63 x15 mm /100g
WeitereInstrumente	Datenblatt / Firmware / App / Tutorials

* Die Geschwindigkeiten für drahtlose Geräte basieren auf den IEEE 802.11-Standards (z. B. 802.11ac für Wi-Fi 5). Der tatsächliche Durchsatz und die Reichweite können aufgrund von Umwelthindernissen (Wände, Metall), Netzwerküberlastung oder den Fähigkeiten der Client- Geräte niedriger ausfallen.
* Die Verwendung von Wi-Fi 5 (802.11ac) und dessen Funktionen (DLMU-MIMO, 256-QAM) erfordert, dass die Client-Geräte die entsprechenden Technologien unterstützen.

1.3 Inhalt der Verpackung

Das Paket umfasst:

- 1 x Mango 2(GL-MG1300)
- 1 x USB-C zu USB-C Power C
- 1 x Benutzerhandbuch
- 1 x Dankeschönkarte

Kapitel 2

Hardware-Verbindung

Dieses Kapitel behandelt Router Standortauswahl undVerbindungsschritte.

2.1 Auswahl eines Standorts

Befolgen Sie diese Tipps, um einen Standort für die beste Leistung zu wählen.

- **Vermeiden Sie Feuchtigkeit und Hitze**: Stellen Sie den Router nicht in Bereichen auf, die Wasser, Feuchtigkeit oder hohen Temperaturen ausgesetzt sind (z. B. Waschbecken, Heizkörper).
- **Lüftung und Kühlung**: Platzieren Sie den Router in einem kühlen, gut belüfteten Bereich für die richtige Wärmeabfuhr.
- **Zentrale Platzierung**: Positionieren Sie den Router, wo er leicht mit Strom und mehreren Geräten verbunden werden kann (z. B. in der zentralen Zone des Wohnzimmers).
- **Kabelbequemlichkeit**: Routenkabel und das Netzkabel sicher, um das Auslösen von Gefahren zu verhindern.
- **Stabile Oberfläche**: Platzieren Sie den Router auf einer horizontalen, flachen Oberfläche (Regal, Desktop) für Stabilität.
- **EMI-Vermeidung**: Halten Sie den Router von elektromagnetischen Störquellen (Bluetooth-Geräte, Mikrowellen) fern, um Signalstörungen zu minimieren.

2.2 Anschluss des Routers

1. **Einschalten**
   Setzen Sie den zweiteiligen Netzteil zusammen. Verbinden Sie ihn mit dem Router und stecken Sie ihn an eine Steckdose. Er startet automatisch.
2. **Ein Gerät mit dem Router verbinden**
   Verbinden Sie ein Gerät (z. B. Laptop oder Smartphone) mit dem Router über Wi-Fi oder ein Ethernet-Kabel.
   - **Wi-Fi**: Gehen Sie auf Ihrem Gerät zu Einstellungen > Wi-Fi, suchen Sie den Netzwerknamen des Routers Wi-Fi in der Liste der verfügbaren Netzwerke und geben Sie das Passwort ein.
   - **Ethernet**: Verbinden Sie Ihr Gerät über ein Ethernet-Kabel mit dem LAN-Port des Routers.
3. **Am Router anmelden**
   Das Internet ist nicht verfügbar, wenn Sie sich zum ersten Mal mit dem Router verbinden, melden Sie sich bitte gemäß den Anweisungen in Kapitel 3 an, um die Ersteinrichtung abzuschließen, bevor Sie auf das Internet zugreifen.

Kapitel 3

An Ihrem Router anmelden

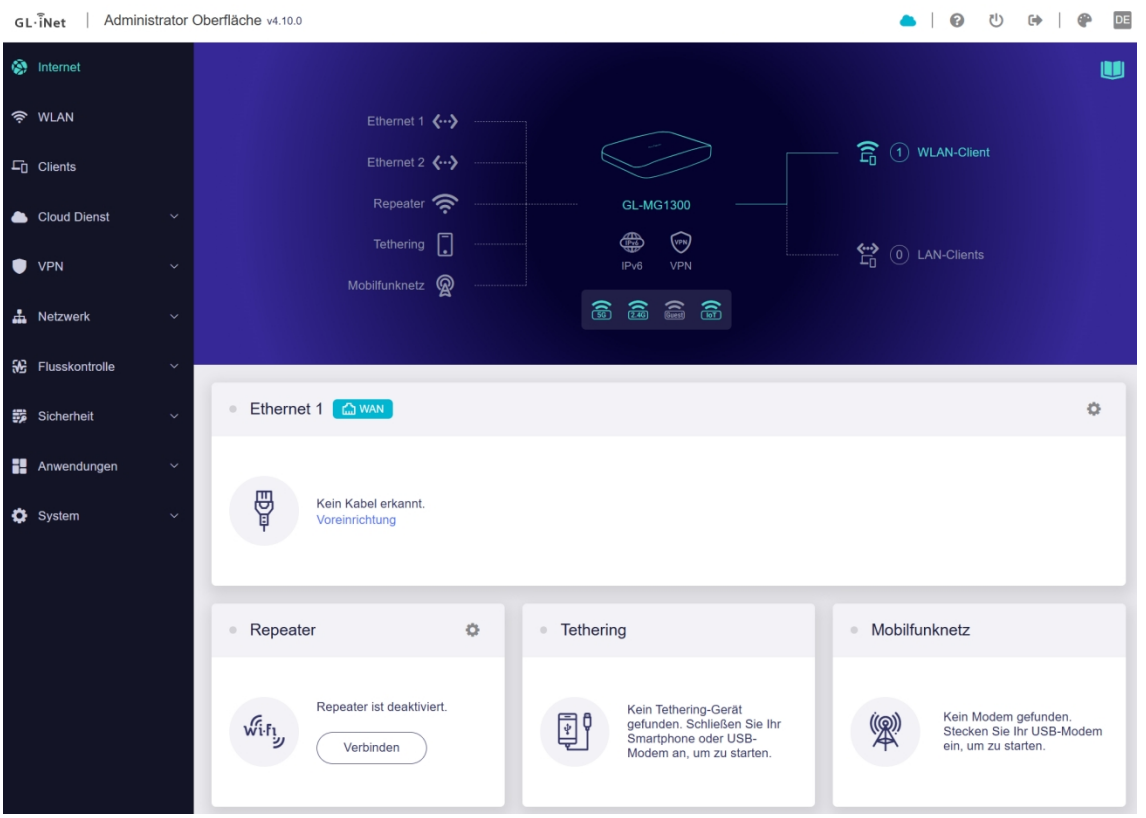
In diesem Kapitel erfahren Sie, wie Sie sich über das Web-Admin-Panelbei Ihrem Router anmelden.

Konfigurieren und verwalten Sie Ihren Router über eine webbasierte Verwaltungsoberfläche, auf die unter jedem Windows-, Mac- oder Linux-Betriebssystem mit einem Webbrowser wie Microsoft Edge, Google Chrome, Mozilla Firefoxoder Apple Safari zugegriffen werden kann.

Hinweis*:* Wenn Sie die GL.iNet-App anstelle des Web-Admin-Panels bevorzugen, laden Sie die App herunter und folgen Sie den Anweisungen auf demBildschirm.

Folgen Sie den folgenden Schritten, umsich über das Web-Admin-Panel bei Ihrem Router anzumelden.

1. Verbinden Sie ein Gerät (z. B. einen Computer oder Laptop) mit dem Router über Wi-Fi oder ein Ethernet-Kabel.
2. Öffnen Sie einen Webbrowser (Chrome undEdge werden empfohlen) undrufen Sie http://192.168.8.1. Sie werden zur Anmeldeseite des Web-Admin-Panels weitergeleitet.Falls Sie nicht auf das Web-Admin-Panel zugreifen können, finden Sie hier Hinweise zur Fehlerbehebung.
3. Legen Sie Ihr Administrator- Passwort fest. Aus Sicherheitsgründen wird ein sicheres Passwort empfohlen. Klicken Sie anschließend auf **Weite**r, um fortzufahren.
4. Sie werden dann das Web-Admin-Panel des Routers betreten.



Kapitel 4

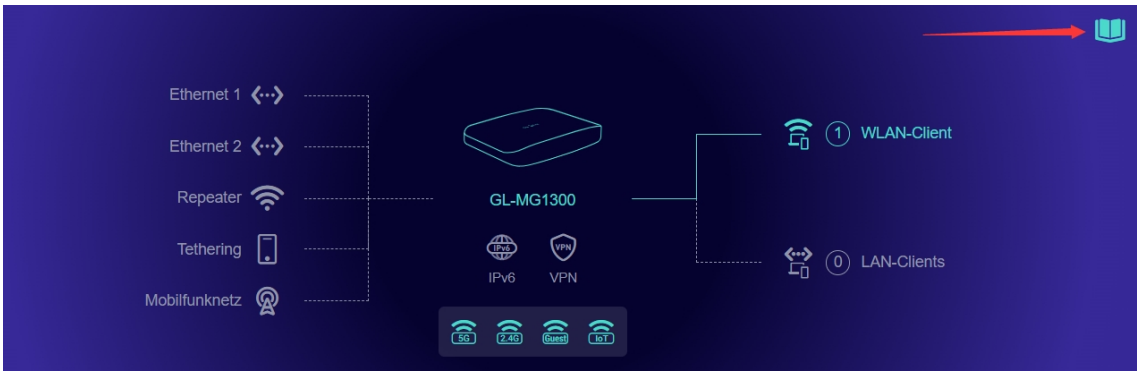
Internetverbindung einrichten

In diesem Kapitel werden verschiedene Methoden zur Herstellung einer Internetverbindung vorgestellt, damit der Router an unterschiedliche Netzwerkumgebungen angepasst werden kann.

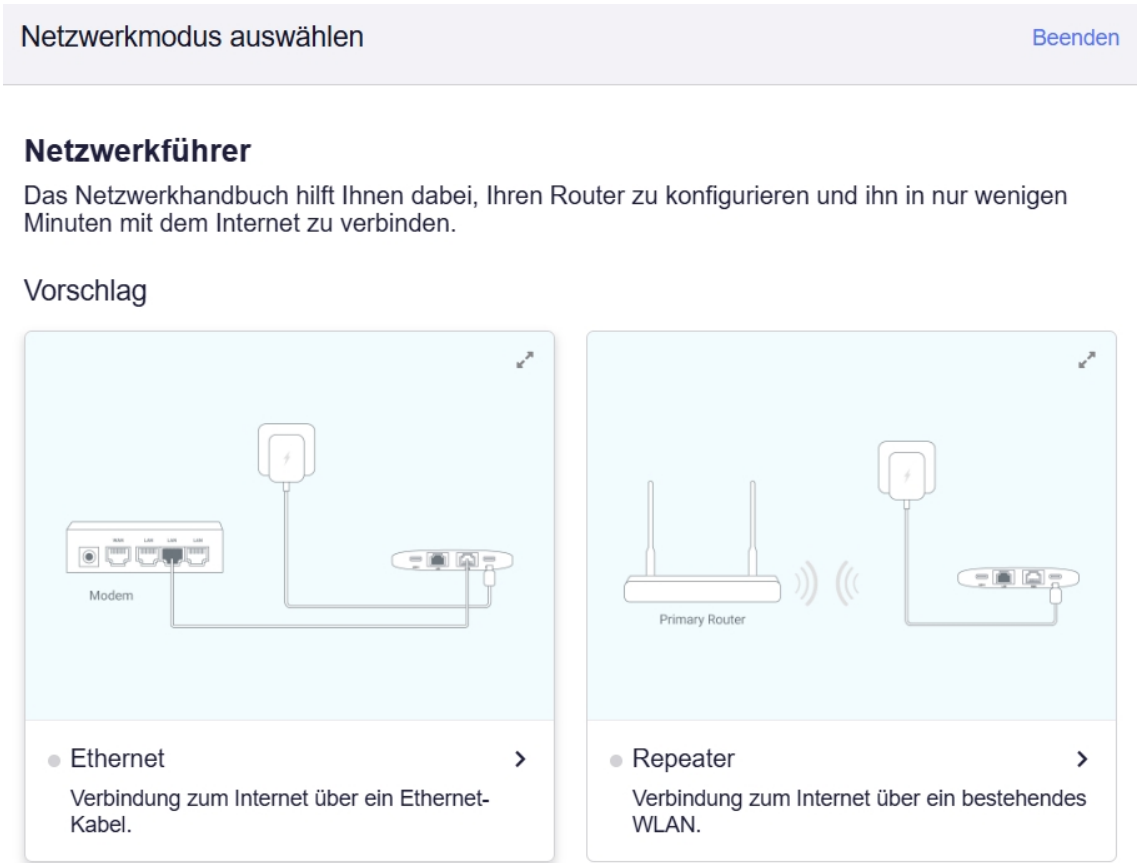
4.1 Schneller Setup-Assistent

Der webbasierte Setup-Assistent führt Sie durch die Netzwerkkonfiguration des Routers. Befolgen Sie die Schritte unten, um den Assistenten zu starten.

1. Melden Sie sich im Web-Admin-Panel des Routers gemäß den Anweisungen in Kapitel 3 an.
2. Klicken Sie auf der Homepage auf das Buchsymbol in der oberen rechten Ecke.



3. Folgen Sie dem Setup-Assistenten, um Ihren Router zu konfigurieren und eine Internetverbindung herzustellen.



4.2 Manuelles Einrichten der Internetverbindung

Während der Setup-Assistent für die schnelle Netzwerkeinrichtung geeignet ist, können Sie mit der manuellen Einrichtung erweiterte Netzwerkeinstellungen für bestimmte Anforderungen anpassen und bei Bedarf vorhandene Verbindungen überprüfen oder ändern.

Mango 2 unterstützt vier Internetverbindungsmethoden: Ethernet, Repeater, USB-Tethering und USB-Modem. Wählen Sie die geeignete Methode basierend auf Ihren Nutzungsanforderungen.

1. **Ethernet**: Verbinden Sie den Router mit einem Breitbandnetzwerk über in Ethernet-Kabel, das an den WAN-Port angeschlossen ist. Der Router erhält in der Regel automatisch eine IP-Adresse über DHCP. Benutzer können auch statische IP- oder PPPoE-Einstellungen manuell konfigurieren. Diese Methode bietet hohe Stabilität und schnelle Geschwindigkeit und eignet sich somit ideal für Heim- und Büroumgebungen mit festem Breitbandzugang.

2. **Repeater**: Dieser Modus ermöglicht es dem Router, sich mit einem vorhandenen Wi-Fi-Netzwerk zu verbinden, um das Wi-Fi-Signal zu erweitern und ein separates, sicheres lokales Netzwerk zu erstellen. Beachten Sie, dass die Übertragungsgeschwindigkeiten bis zu einem gewissen Grad reduziert werden können. Es ist ideal für Wi-Fi-Totzonen, die eine Signalerweiterung erfordern, oder öffentliche Orte, an denen eine verbesserte Netzwerksicherheit erforderlich ist.

3. **USB-Tethering**: Verbinden Sie ein Smartphone oder ein anderes kompatibles Gerät über ein USB-Kabel mit dem Router, um die mobile Datenverbindung des Geräts (z. B. 4G/5G) mit dem Router zu teilen. Dies ist eine bequeme Lösung für einen vorübergehenden Internetzugang, insbesondere im Freien oder in Bereichen ohne festes Breitband.

4. **USB-Modem**: Ein USB-Mobilfunkmodem mit vorinstallierter SIM-Karte wird in den Router eingesetzt. Der Router wird dann über 4G/5G-Mobilfunknetze mit dem Internet verbunden, wodurch eine vom Festnetz-Breitband unabhängige Konnektivität gewährleistet wird. Diese Methode bietet eine hohe Mobilität und eignet sich für Szenarien wie die Nutzung im Fahrzeug oder Outdoor-Aktivitäten.

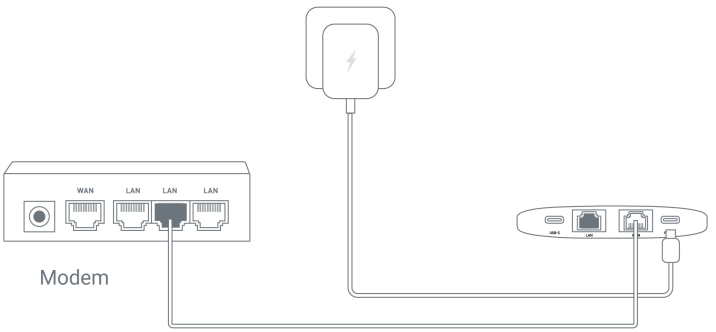
4.2.1 Internet über Ethernet-Kabel

Verbinden Sie den Router über ein Ethernet-Kabel mit einem Breitbandnetzwerk, indem Sie das Kabel an den WAN-Port anschließen. Der Router erhält in der Regel automatisch eine IP- Adresse über DHCP. Benutzer können auch statische IP- oder PPPoE-Einstellungen manuell konfigurieren. Diese Methode bietet hohe Stabilität und hohe Geschwindigkeit und eignet sich somit ideal für Heim- und Büroumgebungen mit festem Breitbandzugang.

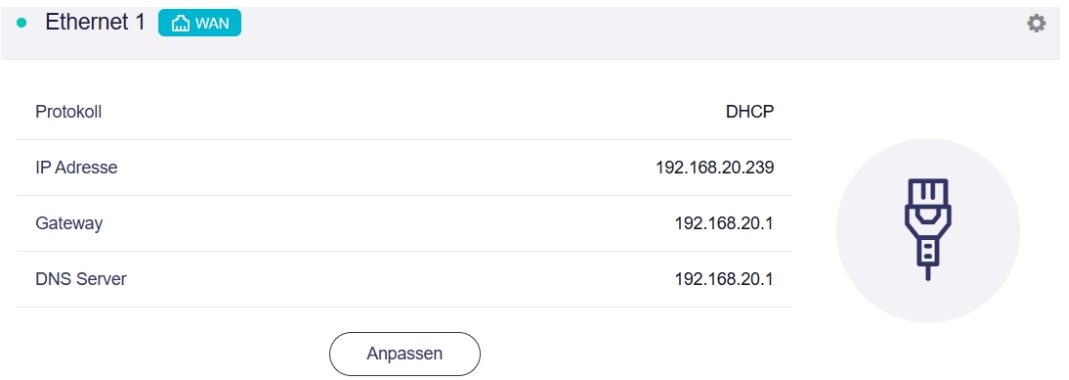
Grundkonfiguration

Folgen Sie den folgenden Schritten, um Ihren Router über ein Ethernet-Kabel mit dem Internet zu verbinden.

1. Verbinden Sie den WAN-Port Ihres Routers über ein Ethernet-Kabel mit dem vorgelagerten Gerät (z. B. einem ISP- Modem, primären Router, Netzwerkswitch oder einer Ethernet-Buchse).



2. Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **Internet** > **Ethernet**. Wenn die Verbindung erfolgreich ist, werden im Ethernet-Bereich Netzwerkdetails angezeigt, einschließlich Protokoll, IP- Adresse, Gateway und DNS-Server.



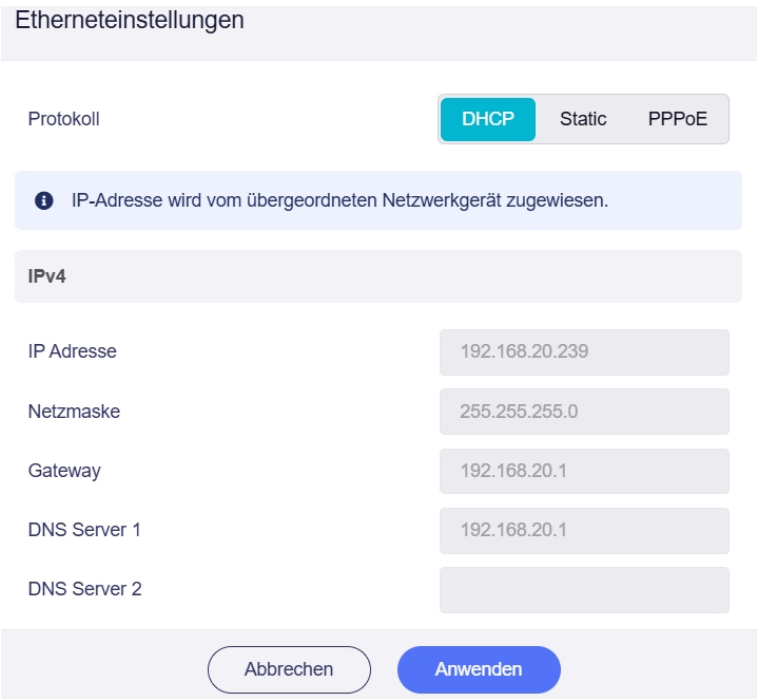
Protokoll

Es gibt drei Arten von Protokollen: DHCP, Statisch und PPPoE. Klicken Sie auf Ändern, um die Einstellungen zu bearbeiten.



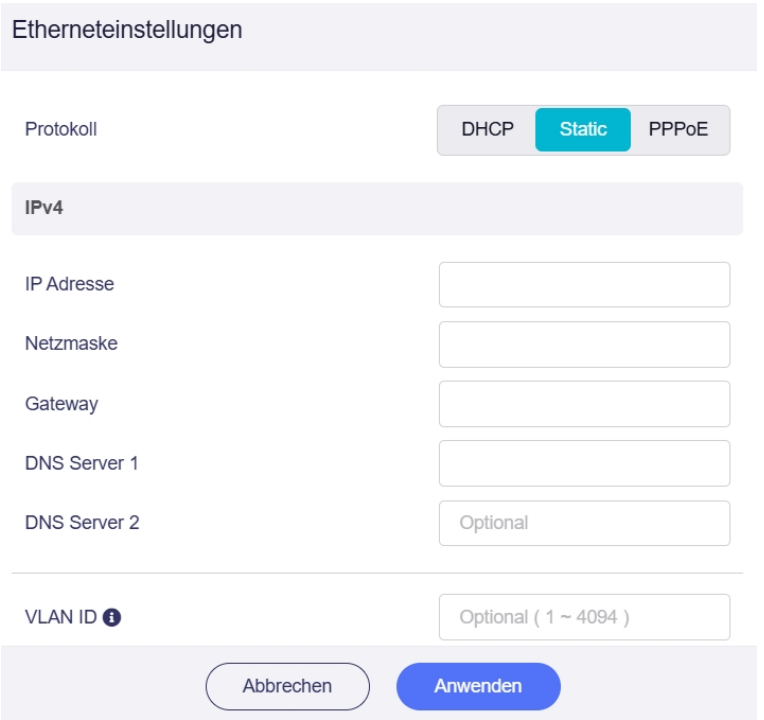
- **DHCP**

  DHCP ist das standardmäßige und häufigste Netzwerkprotokoll, das automatisch IP-Adressen und andere Netzwerkkonfigurationsparameter über ein Client-Server-Modell Geräten in einem IP-Netzwerk zuweist.



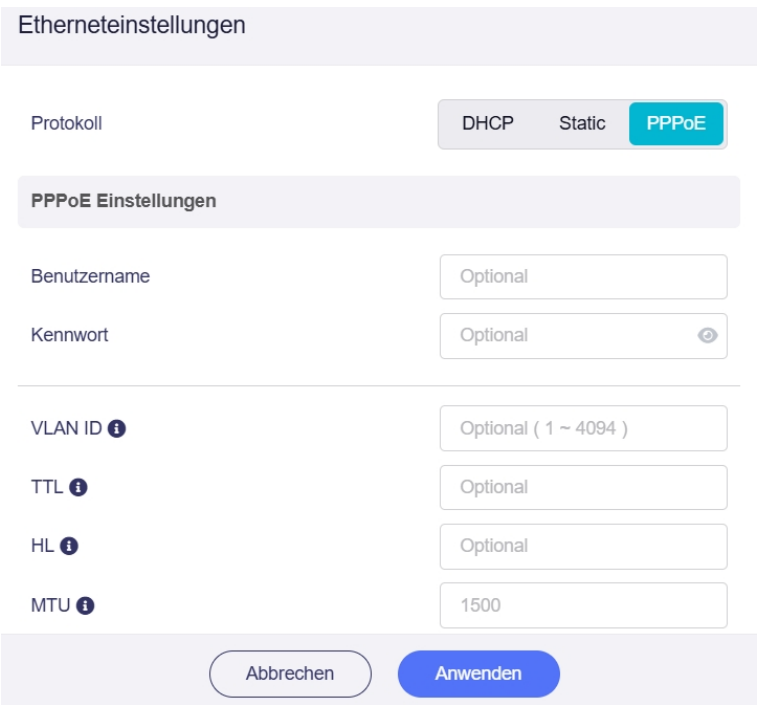
- **Statisc**

  Eine statische IP-Adresse ist erforderlich, wenn Ihr ISP (Internet Service Provider) eine feste öffentliche IP-Adresse zuweist oder wenn Sie Netzwerkparameter manuell konfigurieren müssen (z. B. IP-Adresse, Gateway, Subnetzmaske).



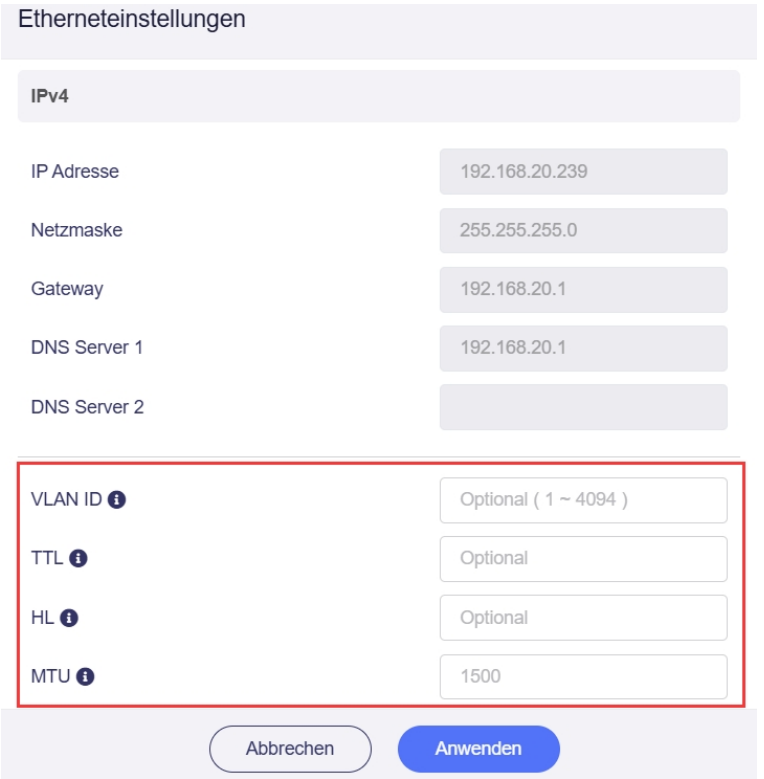
- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) ist ein von ISPs weit verbreitetes Netzwerkprotokoll. In der Regel stellen die Anbieter ein Modem sowie eindeutige Zugangsdaten (Benutzername und Passwort) bereit, die für den Aufbau einer Internetverbindung erforderlich sind.



Erweiterte Einstellungen

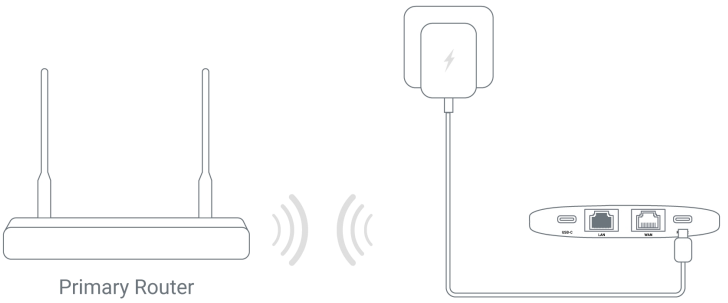
Zusätzlich zu den wesentlichen Einstellungen gibt es auch einige optionale erweiterte Einstellungen für die oben genannten drei Protokolle.



- **VLAN-ID**
  Diese Einstellung ist nur erforderlich, wenn der Server des Anbieters die Verwendung einer bestimmten, mit einem Tag versehenen VLAN-ID durch die Schnittstelle erfordert.
- **TTL**
  TTL (Time To Live) definiert die maximale Zeit, die Pakete im Netzwerk überleben können. Standardmäßig reduziert der Router die TTL der eingehenden Pakete von Client-Geräten um 1 vor der Weiterleitung. Wenn Sie es überschreiben müssen, können Sie hier einen festen Wert festlegen. Die TTL-Einstellung gilt nur für IPv4.
- **HL**
  In IPv6 begrenzt das Feld HL (Hop Limit) die Anzahl der Übertragungssprünge für Datenpakete im Netzwerk und dient als Äquivalent zu TTL in IPv4.
- **MTU**
  Der Standard-MTU-Wert ist 1500 Bytes.

4.2.2 Internet über vorhandenes Wi-Fi

Verbinden Sie den Router als Repeater mit dem vorhandenen drahtlosen Netzwerk, um Wi-Fi-Signale zu steigern und ein lokales Netzwerk zu erstellen, das vom primären Netzwerk isoliert ist. Wenn Sie in Hotels oder Cafés mit kostenlosen öffentlichen Hotspots sind, stärkt ein Repeater nicht nur Wi-Fi-Signale, sondern bietet auch kabelgebundenen und drahtlosen Zugriff für mehrere Geräte und schützt Ihre Netzwerksicherheit.

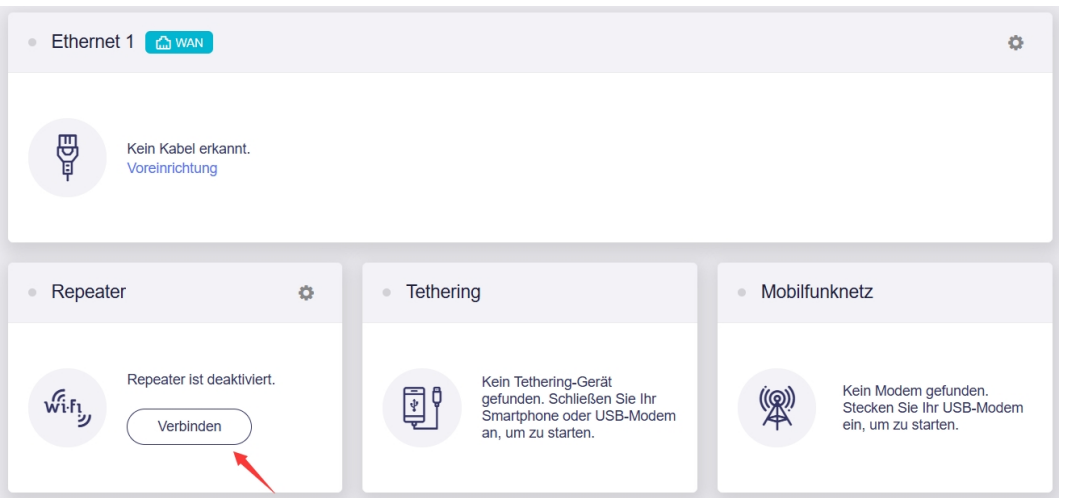


Die Funktion GL.iNet Repeater funktioniert standardmäßig im WISP-Modus (Wireless Internet Service Provider), was bedeutet, dass der Router ein eigenes Subnetz erstellt und als Firewall fungiert, um Sie vor dem öffentlichen Netzwerk zu schützen.

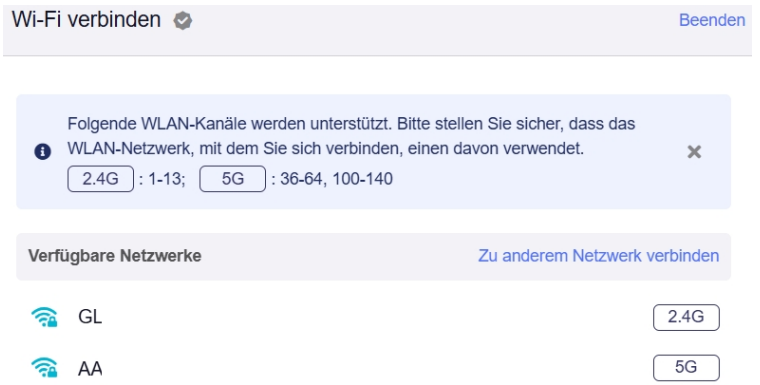
Grundeinstellungen

Folgen Sie den folgenden Schritten, um Ihren Router mit einem vorhandenen Wi-Fi als Repeater zu verbinden.

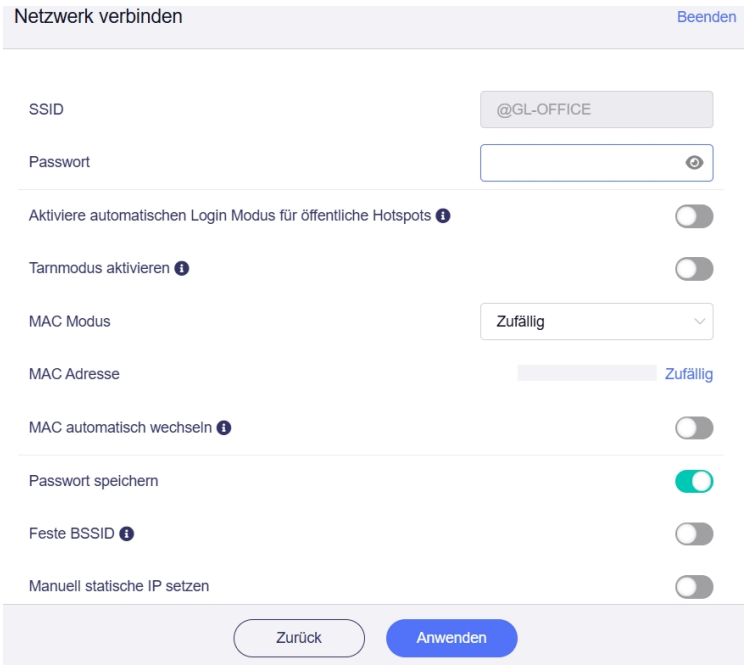
1. Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **Internet** > **Repeater**. Klicken Sie auf **Verbinden**.



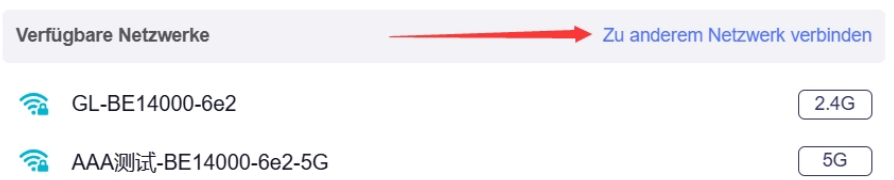
2. Wählen Sie im Popup-Fenster das Wi-Fi-Netzwerk aus, das Sie aus der Liste des verfügbaren Netzwerks verbinden möchten.



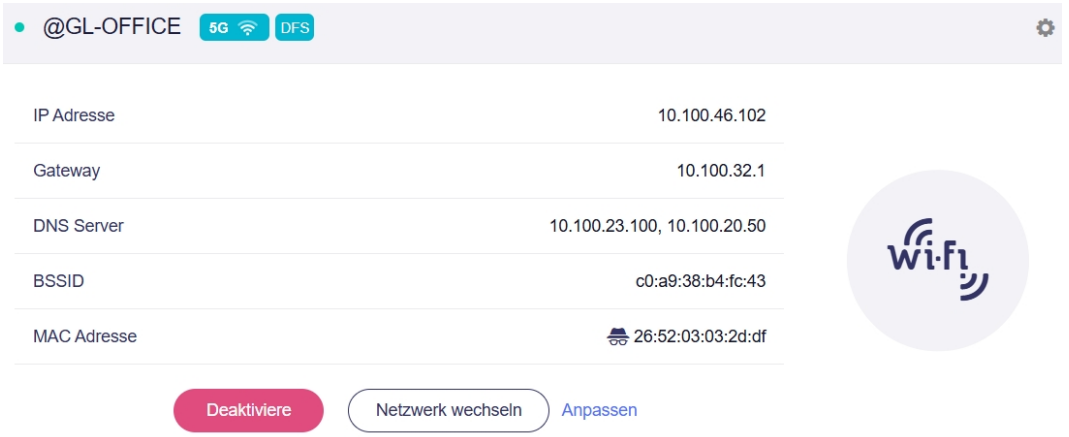
3. Geben Sie dasrichtige Wi-Fi-Passwort ein und klicken Sie auf **Anwenden**.



Wenn die Ziel-Wi-Fi-SSID nicht in der Liste Verfügbares Netzwerk enthalten ist, klicken Sie oben rechts auf **zu Anderes Netzwerk beitreten**, geben Sie manuell die Wi-Fi-SSID und andere erforderliche Informationen ein und klicken Sie auf Anwenden.

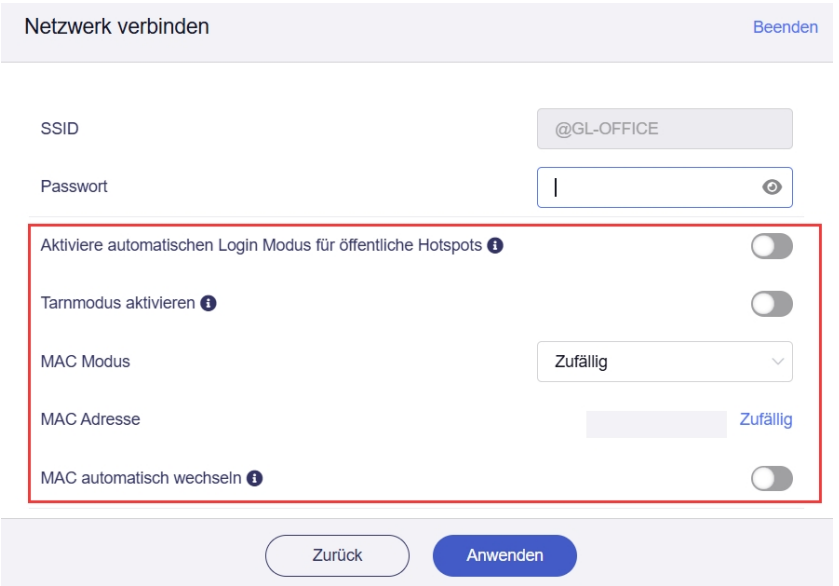


4. Warten Sie eine Minute, bis der Router eine Verbindung herstellt. Sobald die Verbindung hergestellt ist, wird die Seite wie unten angezeigt.


@GL-OFFICE
5G
DFS
IP Adresse
10.100.46.102
Gateway
10.100.32.1
DNS Server
10.100.23.100, 10.100.20.50
BSSID
c0:a9:38:b4:fc:43
MAC Adresse
26:52:03:03:2d:df
Deaktiviere
Netzwerk wechseln
Anpassen

Öffentliche Hotspot-Einstellungen

Beim Anschluss des Routers an einen öffentlichen Hotspot mit einem Captive-Portal wird empfohlen, die folgenden Funktionen zu aktivieren, um die Verbindungserfolgsrate zu verbessern.



- **Aktiviere automatischen Login Modus für öffentliche Hotspots**
  Wenn diese Option aktiviert ist, wechselt der Router automatisch in den Anmeldemodus für öffentliche Hotspots, wenn er zwar mit einem Hotspot, aber nicht mit dem Internet verbunden ist. In diesem Modus werden einige Dienste gesperrt und der DNS-Modus wird automatisch umgestellt; dadurch kann Ihre Netzwerkanfrage an den Netzwerkanbieter weitergeleitet werden (z. B. an ein Hotel oder Einkaufszentrum). Auch wenn die Option deaktiviert ist, fordert der Router Sie zum Wechsel in diesen Modus auf, sobald er ein Captive Portal erkennt oder keine Anmeldung möglich ist.
- **Tarnung aktivieren**
  Wenn aktiviert, wird der Router als Client-Gerät maskiert, das Sie verwenden, um auf das Admin-Panel zuzugreifen, indem Sie die MAC-Adresse dieses Geräts emulieren.
- **MAC Modus**
  Wählen Sie aus, welche MAC-Adresse der Router verwendet, um sich mit dem öffentlichen Hotspot zu verbinden.
  Echte MAC Adresse: Verwendet die ursprünglich werkseitig zugewiesene MAC-Adresse des Geräts.
  Klonen: Klont die MAC-Adresse eines Clientgeräts für die Verbindung.

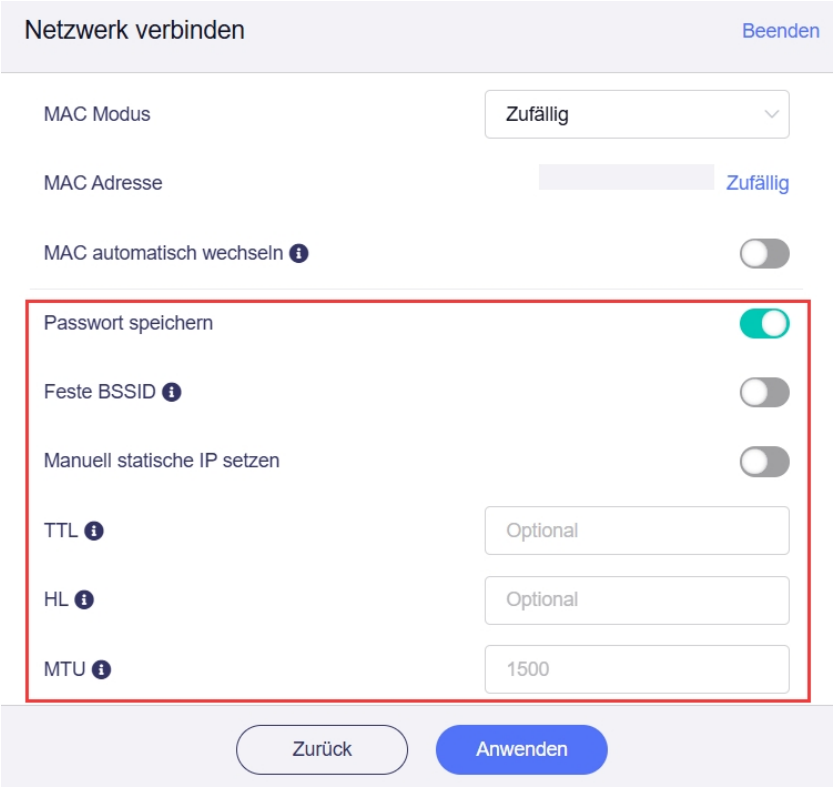
Wenn der gewünschte MAC nicht aufgeführt ist, geben Sie manuell die MAC-Adresse ein, die Sie klonen möchten. Hinweis: Viele Geräte verwenden randomisierte MAC-Adressen(oft als private Wi-Fi-Adresse oder zufällige Hardware-Adresse bezeichnet), wenn Sie sich mit Wi-Fi-Netzwerken verbinden.
Zufällig: Erzeugt automatisch eine zufällige MAC-Adresse für die Verbindung.

- **MAC automatisch wechseln**
  Wenn diese Option aktiviert ist, wird die MAC-Adresse automatisch aktualisiert.

Beim Speichern der Netzwerkkonfiguration wird der MAC-Modus, einschließlich einer geklonten oder randomisierten MAC-Adresse, an die spezifische SSID gebunden, die Sie speichern.

Erweiterte Einstellungen

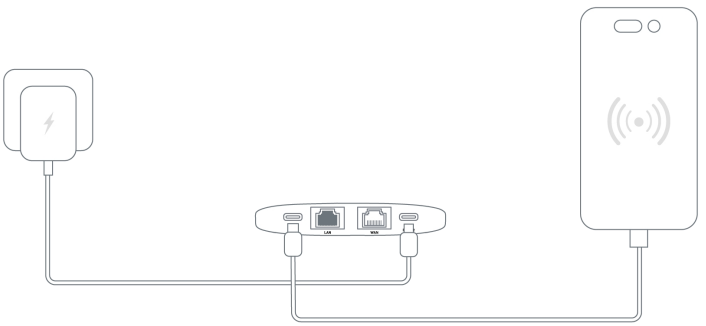
Beim Beitritt zum Netzwerk gibt es einige optionale erweiterte Einstellungen.



- **Passwort speichern**: Aktivieren Sie dies, um sich an das aktuelle wiederholte Wi-Fi-Netzwerk zu erinnern.
- **Feste BSSID**: Wenn diese Option aktiviert ist, stellt der Router nur eine Verbindung zu dem AP her, der der BSSID entspricht, die Sie beim Wechsel zu einem Netzwerk mit dieser SSID ausgewählt haben.
- **Manuell statische IP setzen**: Diese ist in Firmware v4.7 und höher verfügbar.
- **TTL**(Time To Live): Legt die maximale Lebensdauer von Paketen im Netzwerk fest und wird entsprechend den Anforderungen des Betreibers eingestellt. Standardmäßig leitet der Router die TTL eingehender Pakete von Client-Geräten um eins reduziert weiter. Bei Bedarf können Sie hier einen festen Wert festlegen. Die TTL-Einstellung gilt nur für IPv4.
- **HL**: In IPv6 wird das Feld HL (Hop Limit) verwendet, um die Anzahl der Übertragungssprünge von Datenpaketen im Netzwerk zu begrenzen, was der TTL in IPv4 entspricht.
- **MTU**: Der Standardwert ist 1500.

4.2.3 Internet über USB-Tethering

Das Verbinden eines Smartphones mit dem Router über ein USB-Kabel wird als Tethering bezeichnet, das das mobile Datennetzwerk des Geräts (z. B. 4G/5G) mit dem Router teilen kann. Dies ist eine bequeme Methode für einen vorübergehenden Internetzugang, insbesondere im Freien oder in Bereichen ohne festes Breitband.



Ein hostloses Modem kann während der Modemeinrichtung ebenfalls im Tethering-Modus verwendet werden.

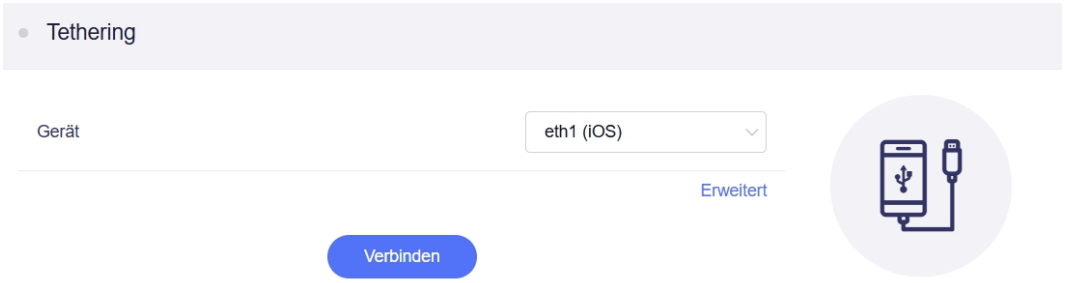
Hinweis: Einige Mobilfunkanbieter begrenzen oder berechnen extra für das Anbinden.

iPhone Tethering

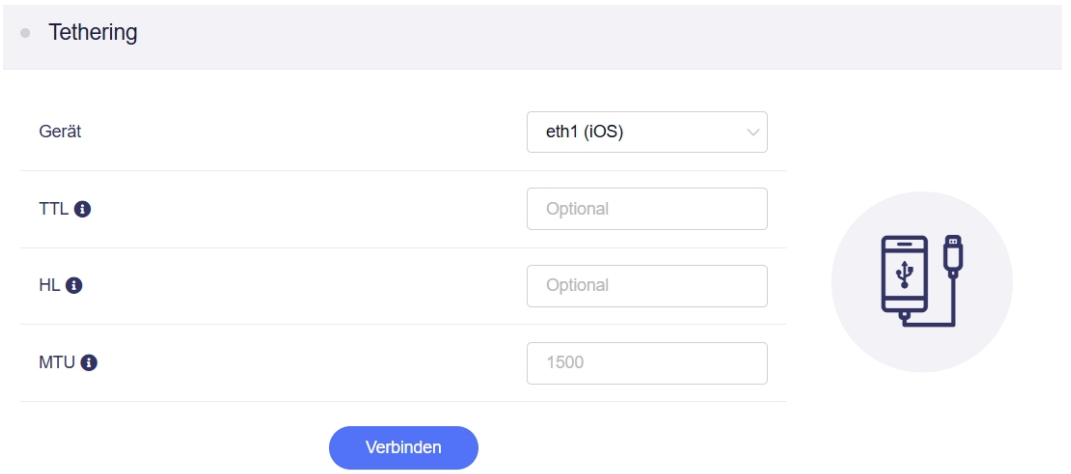
1. Verbinden Sie ein iPhone mit dem USB-Anschluss des Routers über ein USB-Kabel.
2. Gehen Sie zu **iPhone-Einstellungen** > **Persönlicher Hotspot**. Aktivieren Sie die Funktion Persönlicher Hotspot.



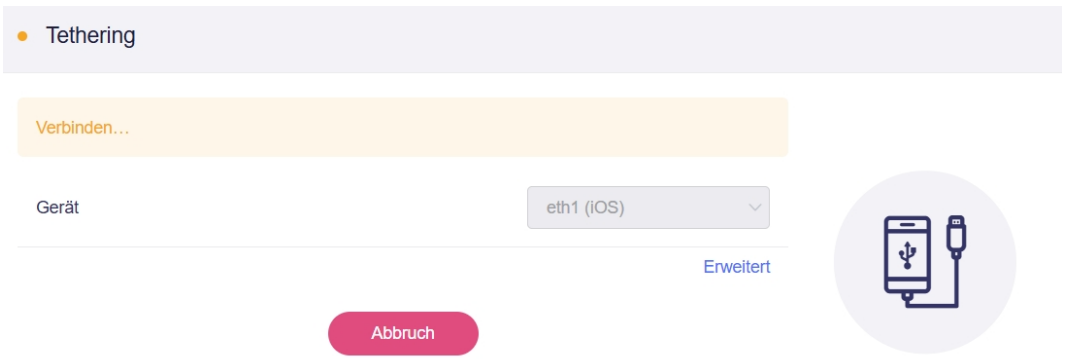
3. Schließen Sie einen Computer oder ein anderes Telefon an den Router an. Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **Internet** > **Tethering**, und klicken Sie dann auf **Verbinden**.



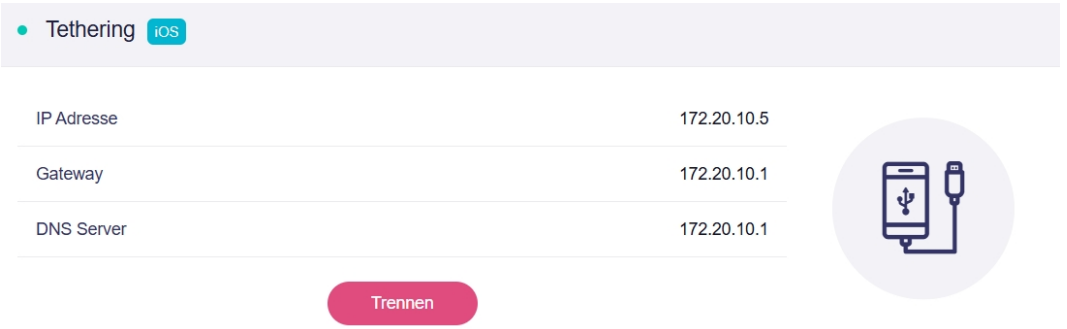
Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU festlegen müssen, klicken Sie auf **Erweitert**, umdieseEinstellungen anzupassen, und klicken Sie dann auf **Verbinden**.



4. Es wird anfangen, sich zu verbinden.

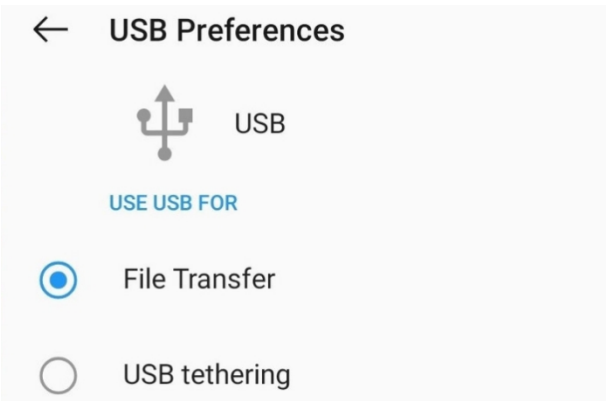


Sobald verbunden, zeigt diese Seite die Tethering-Verbindungsdetails an.

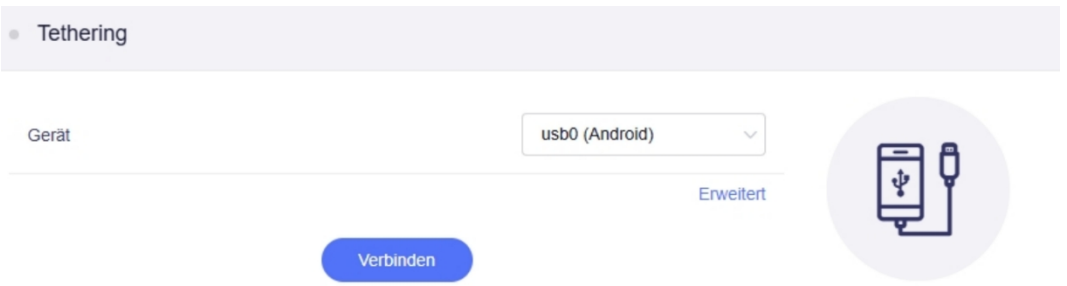


Android Tethering

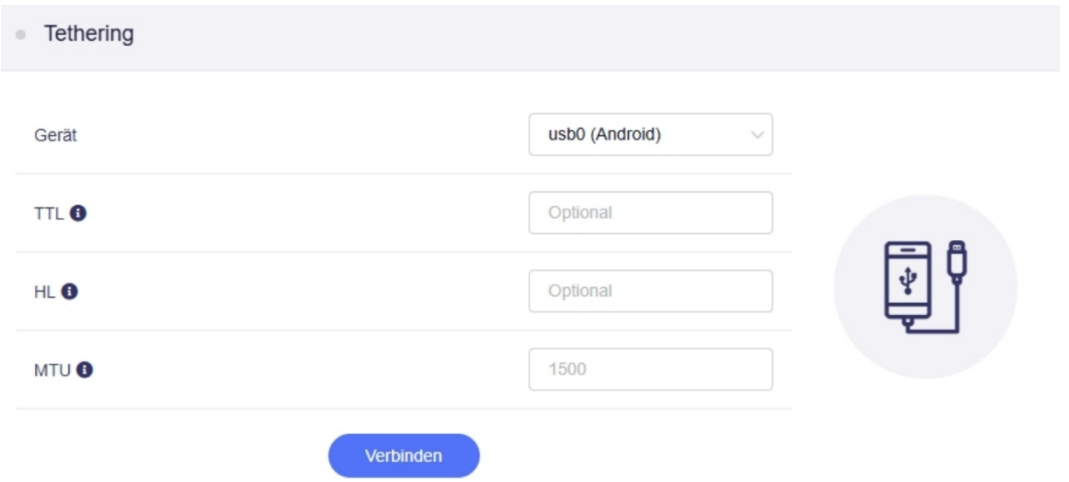
1. Verbinden Sie ein Android-Handy mit dem USB-Anschluss des Routers über ein USB-Kabel. Ein Systemdialog erscheint möglicherweise mit USB-Einstellungen. Wählen Sie **USB Tethering** oder **File Transfer**, wenn Sie dazu aufgefordert werden.



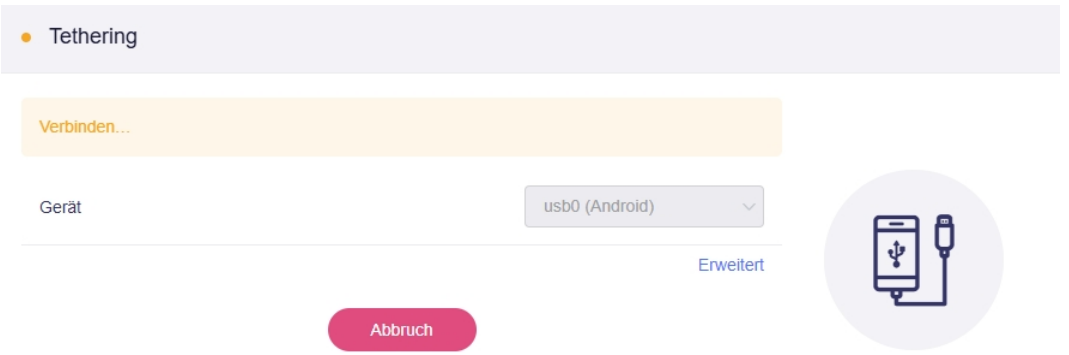
2. Gehen Sie zu den **Einstellungen** Ihres Telefons **> Netzwerk & Internet > Persönlicher Hotspot**.Aktivieren Sie den **persönlichen Hotspot** oder **USB-Tethering**.
3. Schließen Sie einen Computer oder ein anderes Telefon an den Router an, melden Sie sich dann im Web-Admin-Panel des Routers an, navigieren Sie zu **Internet** > **Tethering**. Klicken Sie auf **Verbinden**.



Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU festlegen müssen, klicken Sie auf **Erweitert**, um diese Einstellungen anzupassen, bevor Sie auf **Verbinden** klicken.



4. Es wird beginnen, sich zu verbinden.



5. Sobald die Verbindung hergestellt ist, zeigt diese Seite den Status der Tethering-Verbindung an.



Fehlerbehebung

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

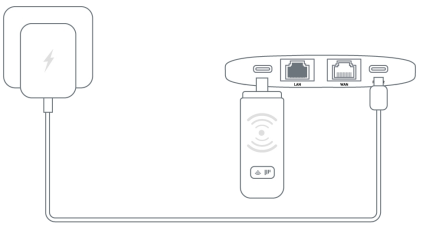
- Verwenden Sie die ursprüngliche Stromversorgung für den Router.
- Ziehen Sie das USB-Kabel heraus und stecken Sie es erneut ein.
- Verwenden Sie ein anderes USB-Kabel. Stellen Sie sicher, dass es die Datenübertragung unterstützt (nicht nur das Laden).
- Schalten Sie "USB Tethering" für einige Male aus und schalten Sie es ein (für Android Phone).
- Schalten Sie "Andere zulassen" für einige Male aus und schalten Sie "Andere beitreten" ein (für iPhone).
- Starten Sie Ihr Smartphone neu und versuchen Sie es erneut.

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

4.2.4 Internet über USB-Modem

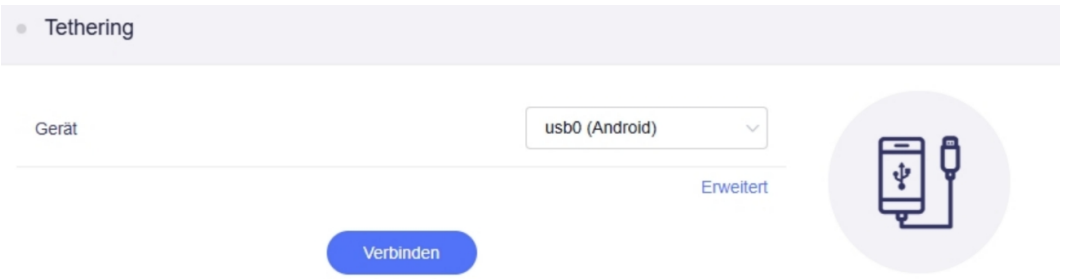
Verbinden Sie den Router mit dem Internet, indem Sie ein Mobilfunk-USB-Modem in seinen USB-Anschluss einsetzen. Dadurch kann der Router über 4G-/5G-Netze eine Internetverbindung herstellen, ohne auf einen Festnetz-Breitbandanschluss angewiesen zu sein. Diese Methode eignet sich für die Nutzung im Fahrzeug oder im Freien. Die Verbindung wird über die Tethering- oder Mobilfunk-Schnittstelle des Routers hergestellt.

Für die Mango 2 können Sie ein USB-C-Modem direkt anschließen oder einen USB-C-zu-USB-A-Adapter verwenden, um ein USB-A-Modem anzuschließen.

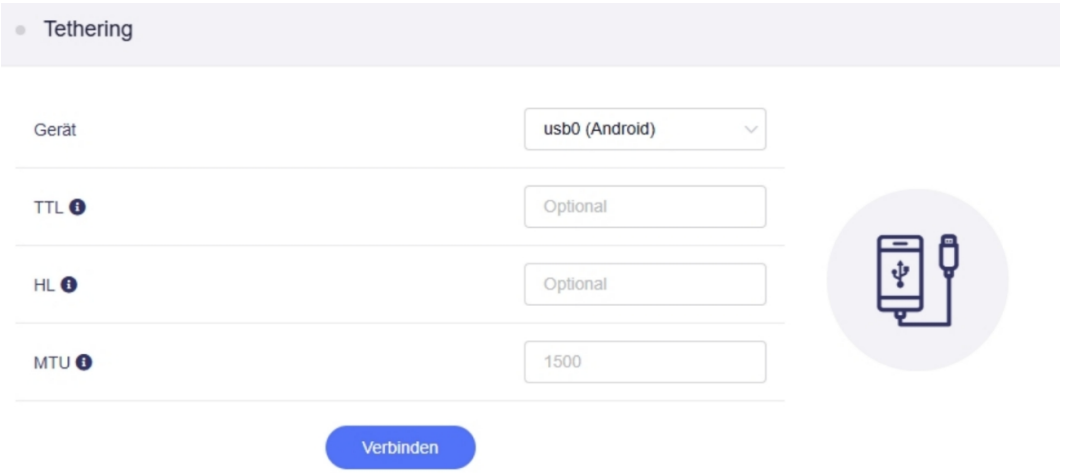


Folgen Sie den folgenden Schritten, um Ihren Router über ein USB-Modem mit dem Internet zu verbinden.

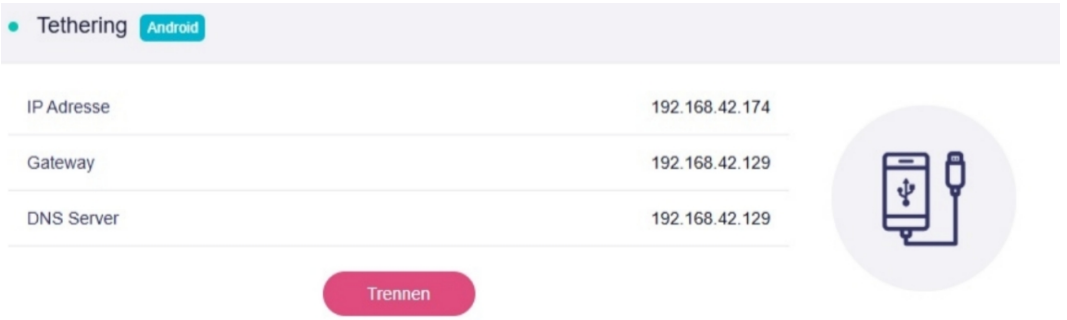
1. Schließen Sie ein USB-Modem mit einer vorinstallierten SIM-Karte an den USB-Anschluss des Routers an, bevor Sie es einschalten.
2. Melden Sie sich im Web-Admin-Panel des Routers an, navigieren Sie zu **Internet** > **Tethering** und klicken Sie dann auf **Verbinden**.



Wenn Sie erweiterte Einstellungen wie TTL, HL und MTU festlegen müssen, klicken Sie auf **Erweitert**, um diese Einstellungen anzupassen, und klicken Sie dann auf **Verbinden**.

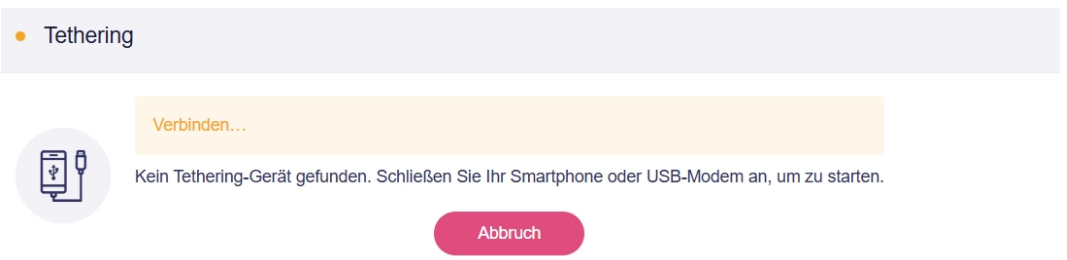


3. Sobald die Verbindung hergestellt ist, werden auf dieser Seite die Netzwerkdetails angezeigt.



Tipps:

1. Wenn Sie den Router nach der Ersteinrichtung mit weiterhin angeschlossenem USB-Modem neustarten oder das Modem erneut einsetzen, wird das USB-Modem automatisch erkannt und die Netzwerkverbindung hergestellt, ohne dass Sie erneut auf Verbinden klicken müssen.
2. Wenn Sie das USB-Modem ausziehen, wird auf der Seite der unten gezeigte Status angezeigt, der angibt, dass "Kein Tethering-Gerät gefunden" wird, während die Tethering-Schnittstelle im Zustand "Verbindung" bleibt.



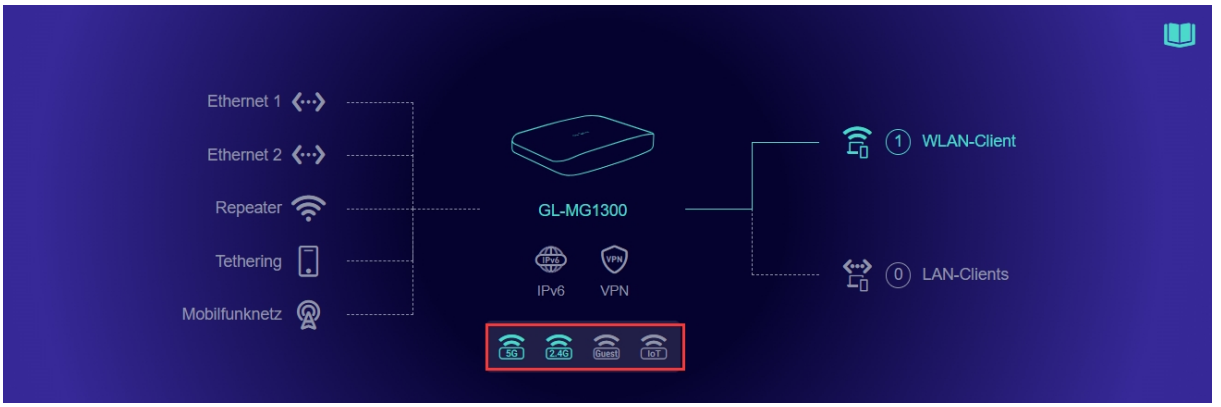
Kapitel 5

WLAN

In diesem Kapitel werden Sie aufgefordert, den Wi-Fi-Status zu überprüfen und die drahtlosen Einstellungen zu konfigurieren.

5.1 Wi-Fi Statusanzeige

Die Wi-Fi-Netzwerke des Routers sind standardmäßig aktiviert, und das entsprechende Wi-Fi-Symbol leuchtet unterhalb des Gerätemodellbildes auf der Internet-Seite auf.



Wenn der Cursor über dem aktivierten WLAN-Symbol schwebt, wird ein WLAN-QR-Code angezeigt. Sie können den WLAN-QR-Code scannen, um sich schnell mit dem entsprechenden WLAN zu verbinden.



5.2 WLAN Einstellungen

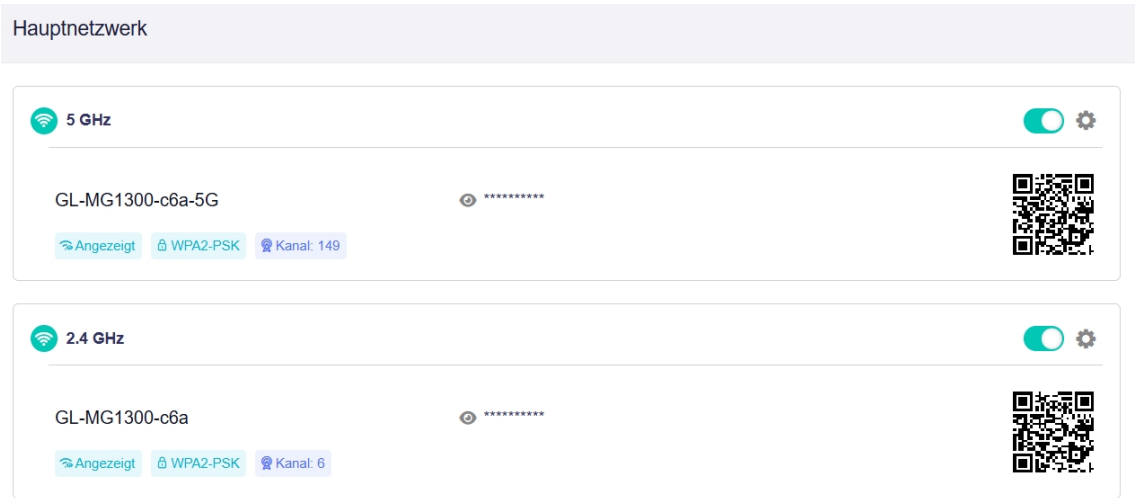
WLAN-Frequenzbänder variieren je nach Modell. Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu WLAN. Auf der Seite WLAN können Sie verschiedene WLAN-Netzwerke konfigurieren, darunter Hauptnetzwerk, Gastnetzwerk und IoT-Netzwerk. Die unterstützten WLAN-Frequenzbänder variieren je nach Modell.

5.2.1 Hauptnetz

Das Hauptnetzwerk ist Ihr primäres Wi-Fi-Netzwerk und unterstützt gleichzeitige Übertragungen über verschiedene Funkbänder, die alle standardmäßig aktiviert sind.

Klicken Sie auf das Zahnrad-Symbol auf der rechten Seite, um die Wi-Fi-Einstellungen für jedes Band anzuzeigen oder zu ändern, z. B. Wi-Fi SSID, Sicherheit, Passwort, randomisierte BSSID, TX-Leistung, Bandbreite und Wi-Fi-Kanal.

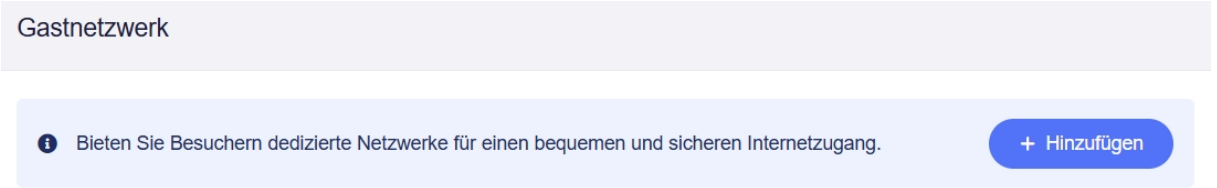
Hinweis: Die verfügbaren Wi-Fi-Bänder variieren je nach Modell.



5.2.2 Gastnetzwerk

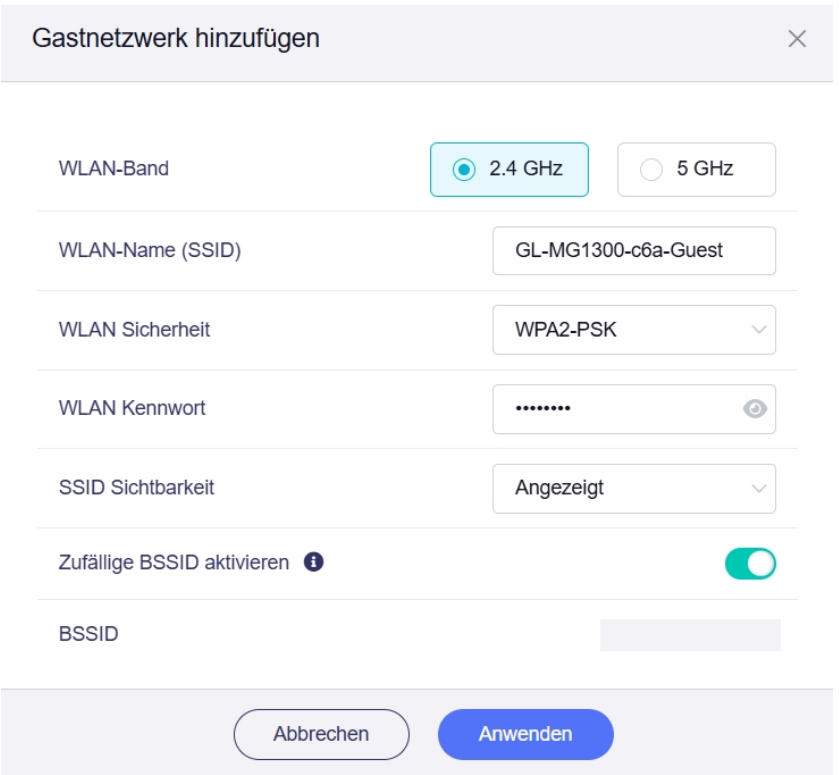
Das Gastnetzwerk ist ein dediziertes Wi-Fi-Netzwerk für Besucher, wobei alle Bänder standardmäßig deaktiviert sind. Sie können grundlegende Netzwerkeinstellungen für jedes Band aktivieren und konfigurieren, z. B. die Wi-Fi SSID, den Sicherheitsmodus, das Passwort und die randomisierte BSSID.

Um ein Gast-Wi-Fi-Netzwerk zu erstellen, klicken Sie auf die Schaltfläche Hinzufügen rechts.

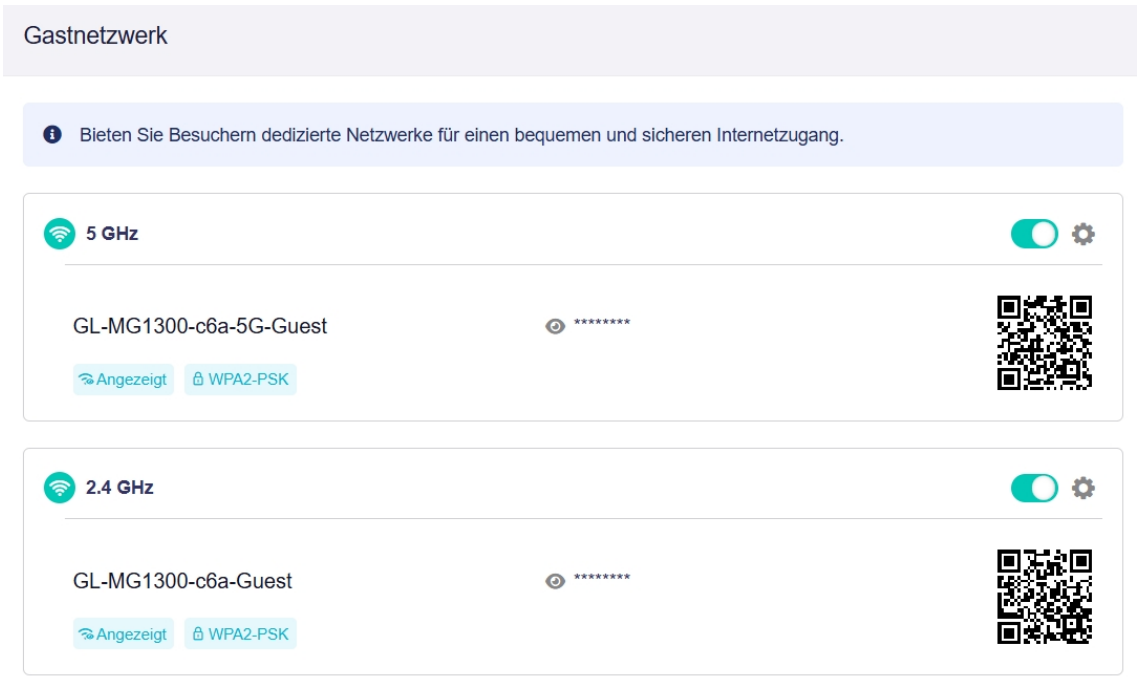


Wählen Sie ein Wi-Fi-Band aus, konfigurieren Sie Wi-Fi-Details und klicken Sie dann auf **Anwenden**.

Hinweis: Die verfügbaren Wi-Fi-Bänder variieren je nach Modell.



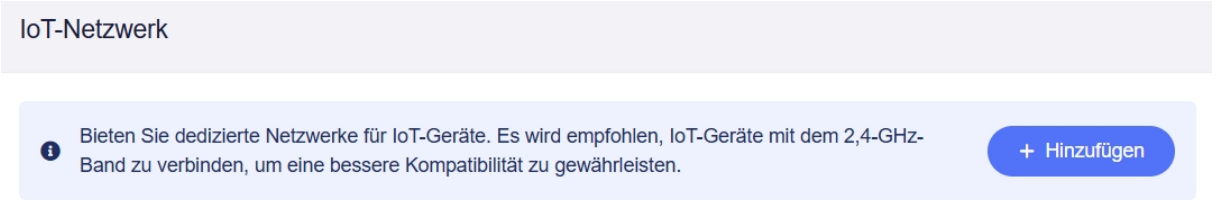
Nachdem die Seite aktiviert ist, wird sie wie unten dargestellt angezeigt.


Gastnetzwerk
Bieten Sie Besuchern dedizierte Netzwerke für einen bequemen und sicheren Internetzugang.
5 GHz
GL-MG1300-c6a-5G-Guest
****
Angezeigt
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-Guest
****
Angezeigt
WPA2-PSK

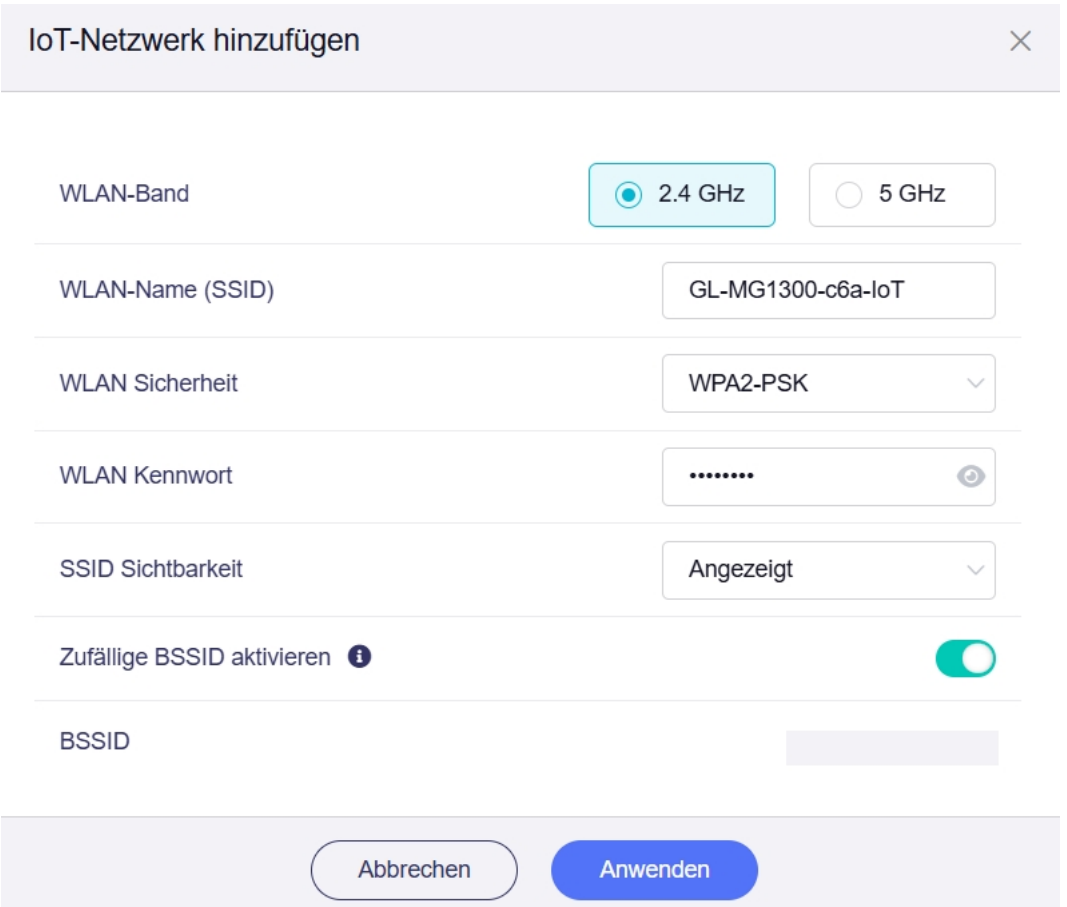
5.2.3 IoT-Netzwerk

Das IoT-Netzwerk ist ein dediziertes Wi-Fi-Netzwerk für intelligente Geräte, bei dem alle Bänder standardmäßig deaktiviert sind. Sie können grundlegende Netzwerkeinstellungen für jedes Band aktivieren und konfigurieren, z. B. die Wi-Fi SSID, den Sicherheitsmodus, das Passwort und die randomisierte BSSID.

Um ein IoT Wi-Fi-Netzwerk zu erstellen, klicken Sie auf die Schaltfläche Hinzufügen rechts.



Wählen Sie ein Wi-Fi-Band aus, konfigurieren Sie Wi-Fi-Details und klicken Sie dann auf Anwenden.



Nachdem die Seite aktiviert ist, wird sie wie unten dargestellt angezeigt.


IoT-Netzwerk
Bieten Sie dedizierte Netzwerke für IoT-Geräte. Es wird empfohlen, IoT-Geräte mit dem 2,4-GHz-Band zu verbinden, um eine bessere Kompatibilität zu gewährleisten.
5 GHz
GL-MG1300-c6a-5G-IoT
****
Angezeigt
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-IoT
****
Angezeigt
WPA2-PSK

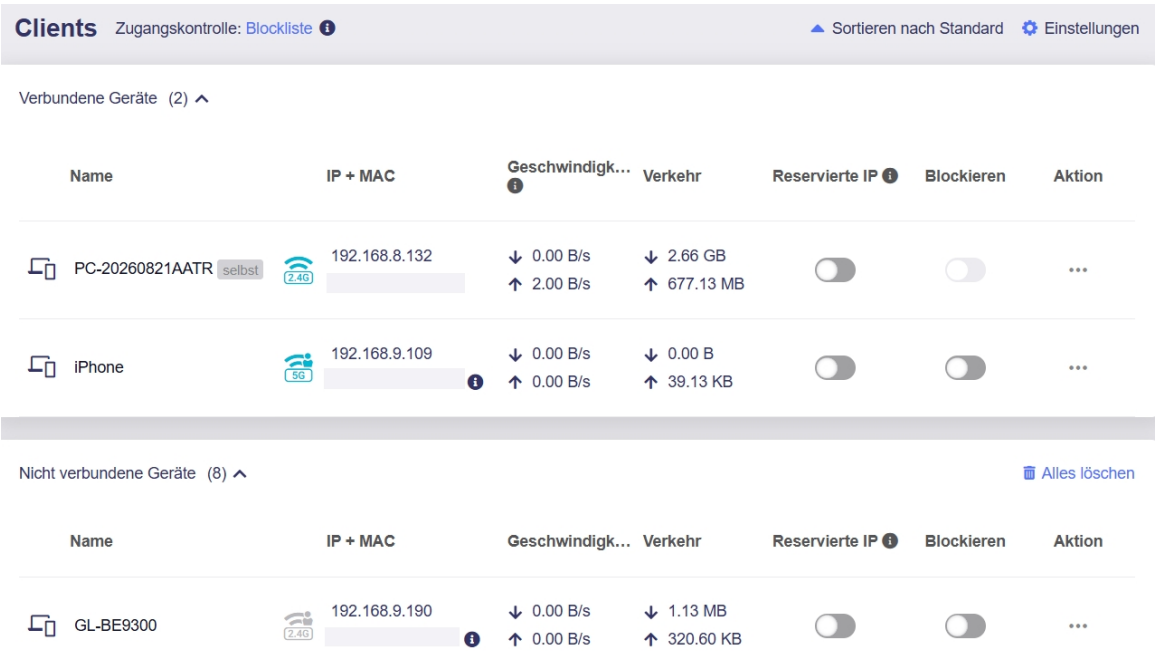
Kapitel 6

Clients

In diesem Kapitel erfahren Sie, wie Sie Details der verbundenen Geräte anzeigen und deren Verbindungen verwalten können.

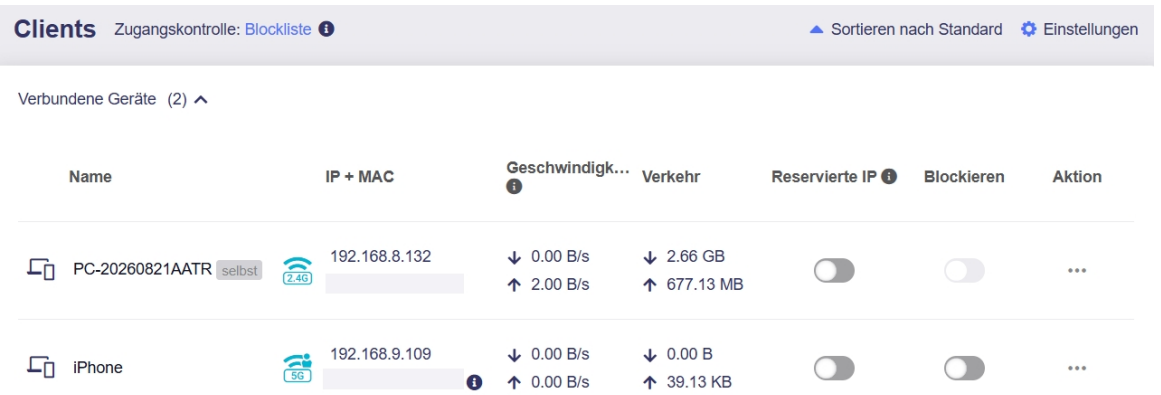
Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **Clients**.

Die Clients-Seite zeigt Informationen über verbundene Geräte an, einschließlich Gerätename, Verbindungstyp, IP- und MAC-Adresse, Geschwindigkeit und Datenverkehr, die von links nach rechts angeordnet sind. Es bietet auch schnellen Zugriff auf IP-Reserve, Block-Client oder andere Aktionen.



- **Verbundene Geräte**: Es bezieht sich auf Geräte, die derzeit mit dem Netzwerk des Routers verbunden sind.
- **Nicht verbundene Geräte**: Es bezieht sich auf Geräte, die zuvor mit dem Router verbunden waren, aber jetzt vom Netzwerk getrennt sind.

6.1 Gerätedetails



1. **Name**

   In der ersten Spalte werden der Gerätename und der Gerätetyp angezeigt; beide richten sich nach dem Hostnamen des Gerätebetreibers. Das blaue Symbol neben dem Gerätenamen kennzeichnet die Verbindungsart und zeigt an, dass das Gerät über ein Ethernet-Kabel mit dem Router verbunden ist.

2. **IP + MAC**

   In der zweiten Spalte werden die IP- und MAC-Adressen des angeschlossenen Geräts aufgeführt, und wenn die angeschlossenen Geräte randomisierte MAC-Adressen verwenden, wird eine Aufforderung angezeigt, die anzeigt, dass es sich um eine randomisierte MAC-Adresse handelt.



   Wenn das zweite Zeichen der MAC-Adresse 2, 6, A oder E ist (Fall ignorieren), wird es als randomisierte MAC-Adresse betrachtet, jedoch können einige Geräte eine andere Regel verwenden, um eine randomisierte MAC-Adresse zu erzeugen, so dass dieses Erkennungsverfahren möglicherweise nicht genau ist.

3. **Geschwindigkeit**

   In der dritten Spalte wird die Internetgeschwindigkeit des angeschlossenen Geräts angezeigt, die die Durchschnittsgeschwindigkeit der letzten 3 Minuten darstellt. Das System beginnt mit der Berechnung der Durchschnittsgeschwindigkeit, wenn diese Seite geöffnet wird (z. B. wenn die Seite nur 10 Sekunden geöffnet war, basiert die Durchschnittsgeschwindigkeit auf nur 10 Sekunden Daten).

4. **Verkehr**

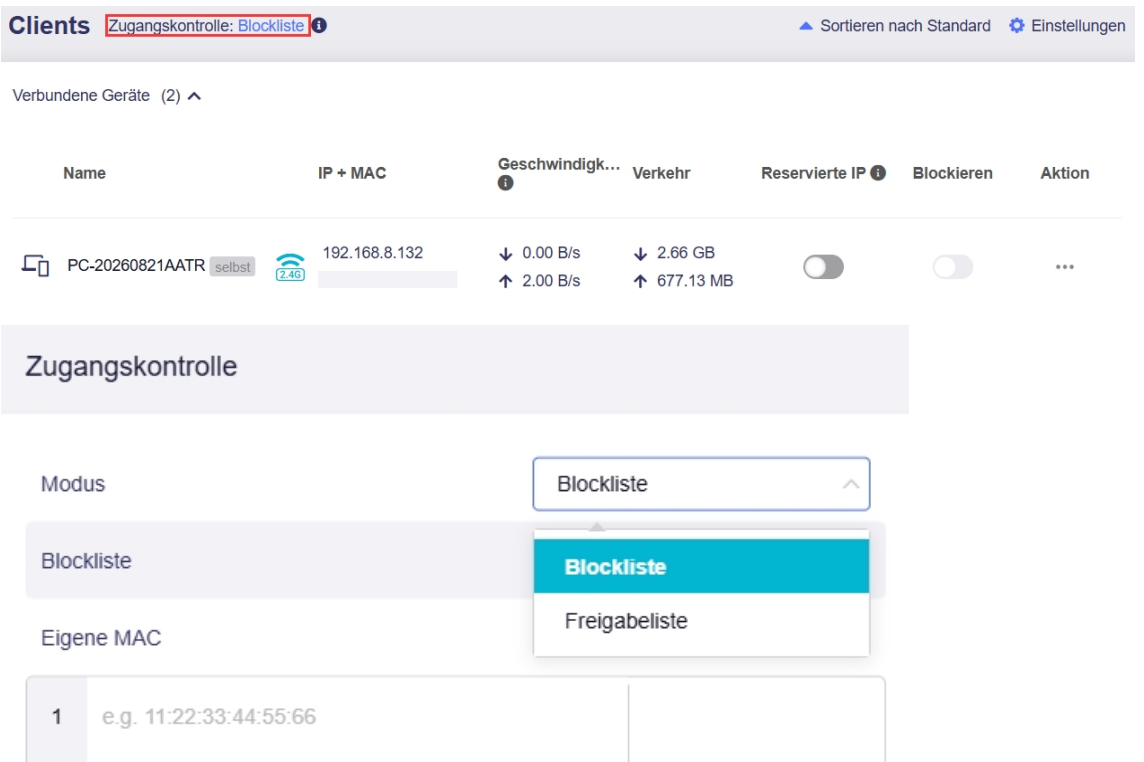
In der vierten Spalte wird der Internetverkehr des angeschlossenen Geräts angezeigt.

5. **Reservierte IP**

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

6. **Blockieren**

   In der sechsten Spalte können Sie bestimmte angeschlossene Geräte mit einem Klick blockieren. Die Access Control-Regel ist standardmäßig Blocklist, und Sie können sie bei Bedarf von oben in Allowlist umschalten.

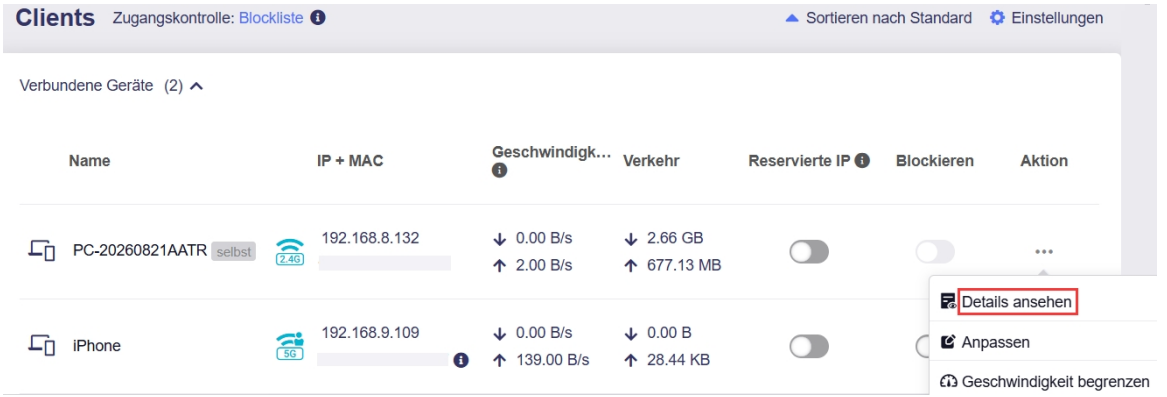


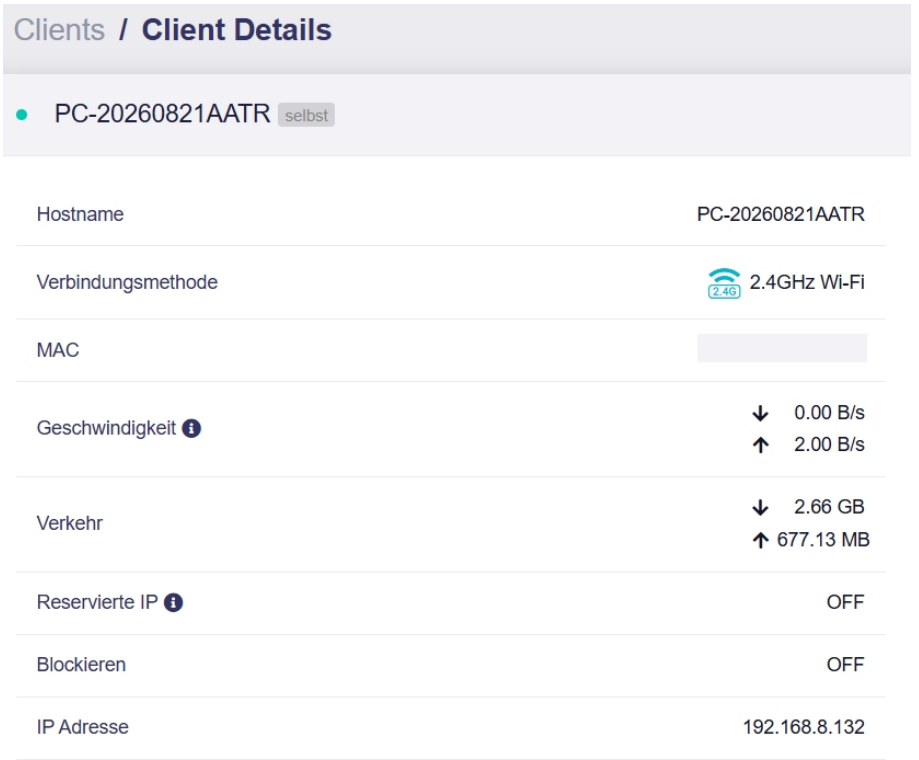
- **Blockliste**: Geräte, deren MAC-Adressen in der Sperrliste stehen, dürfen keine Verbindung zu diesem Router herstellen. Beachten Sie, dass die Sperre auf der MAC-Adresse des Geräts basiert. Verwendet das gesperrte Gerät beim nächsten Mal eine andere MAC-Adresse, kann es weiterhin eine Verbindung zum Router herstellen.
- **Freigabeliste**: Nur Geräte mit spezifischen MAC-Adressen dürfen sich mit diesem Router verbinden, der für IoT-Geräte und das Unternehmensnetzwerkmanagement geeignet ist.

6.2 Aktion

1. **Details ansehen**

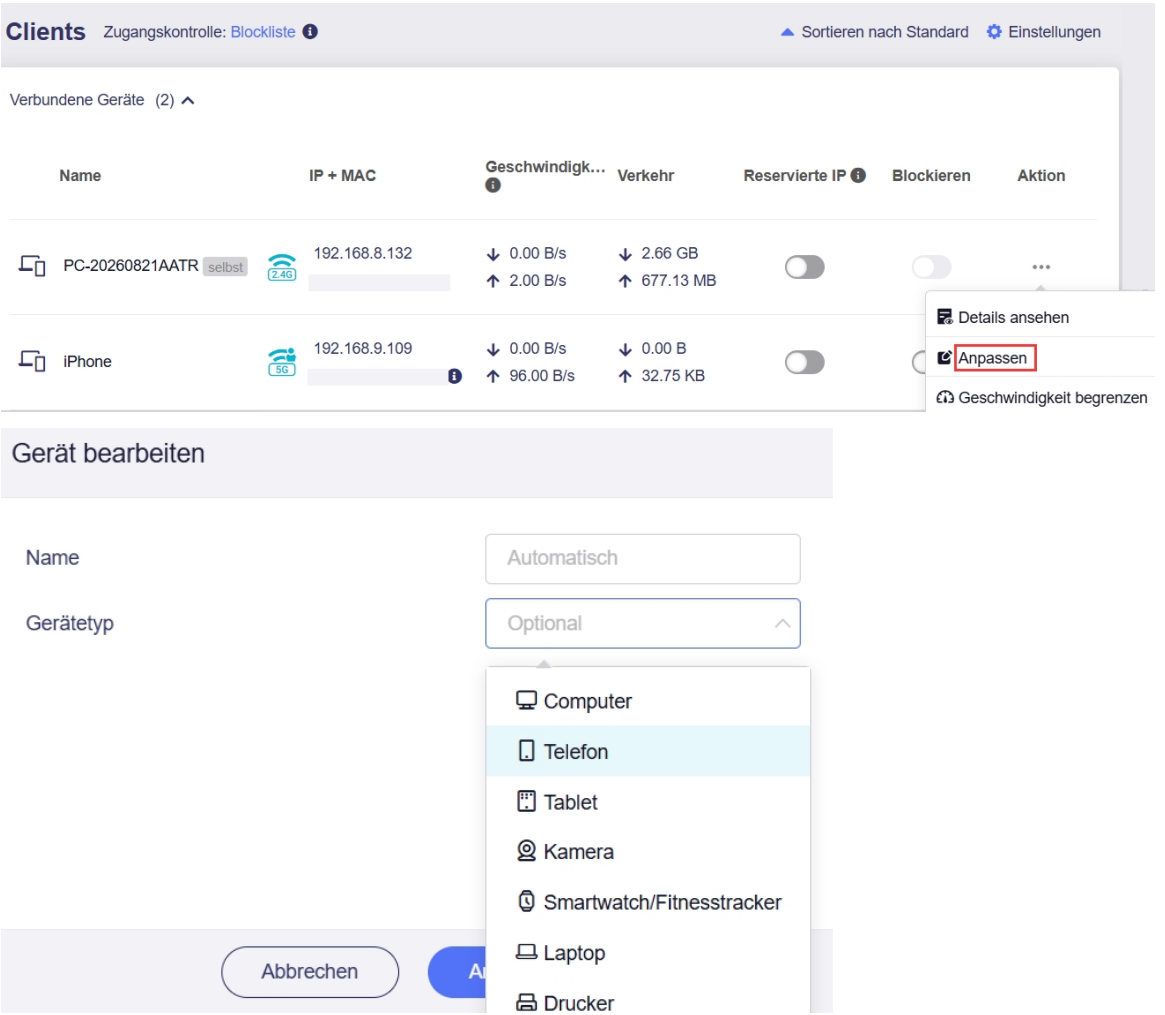
   Klicken Sie auf das Drei-Punkt-Symbol in der Aktionsspalte und klicken Sie auf **Details ansehen** aus dem Dropdown-Menü anzeigen, um die Gerätedetails auf einer einzelnen Seite anzuzeigen.





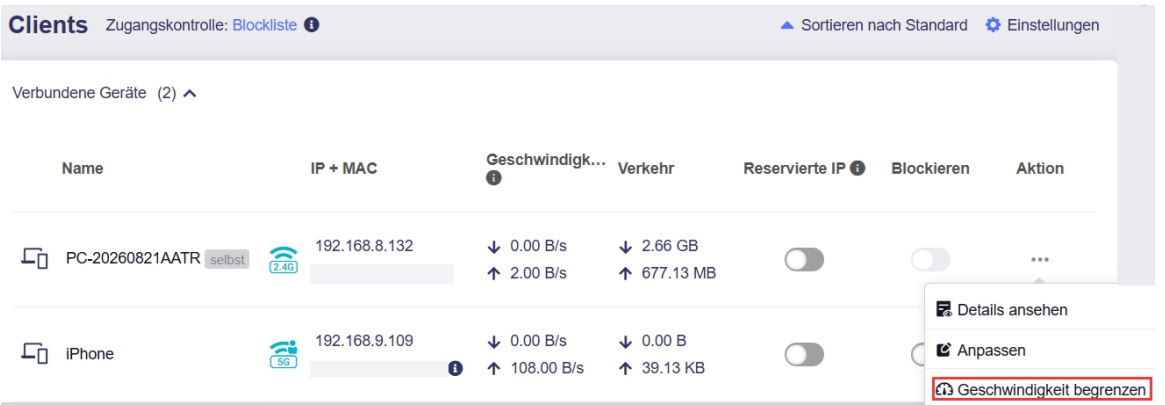
2. **Anpassen**

   Klicken Sie auf das Dre-Punkt-Symbol in der Aktionsspalte und klicken Sie auf **Anpassen** aus dem Dropdown-Menü, um den Gerätenamen und -typ zu ändern.



3. **Geschwindigkeit begrenzen**

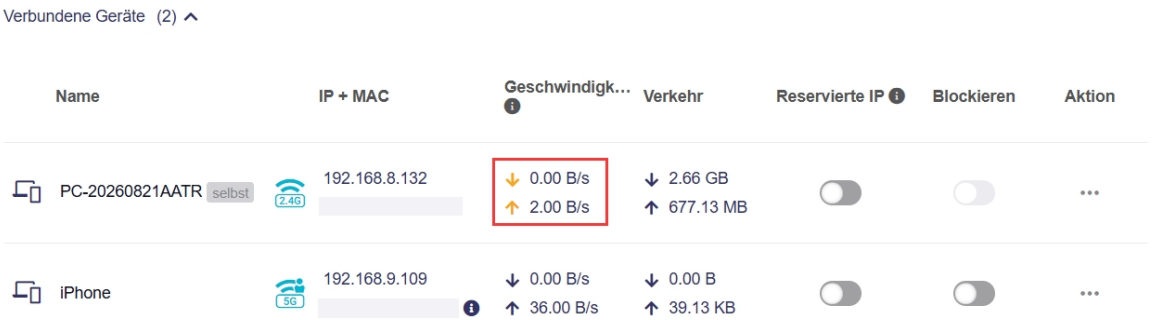
   Klicken Sie auf das Drei-Punkt-Symbol in der Aktionsspalte und klicken Sie auf **Geschwindigkeit begrenzen** aus dem Dropdown-Menü.





Sie können die Geschwindigkeit eines angeschlossenen Geräts begrenzen, wobei das Gerät auf KB/s eingestellt ist.

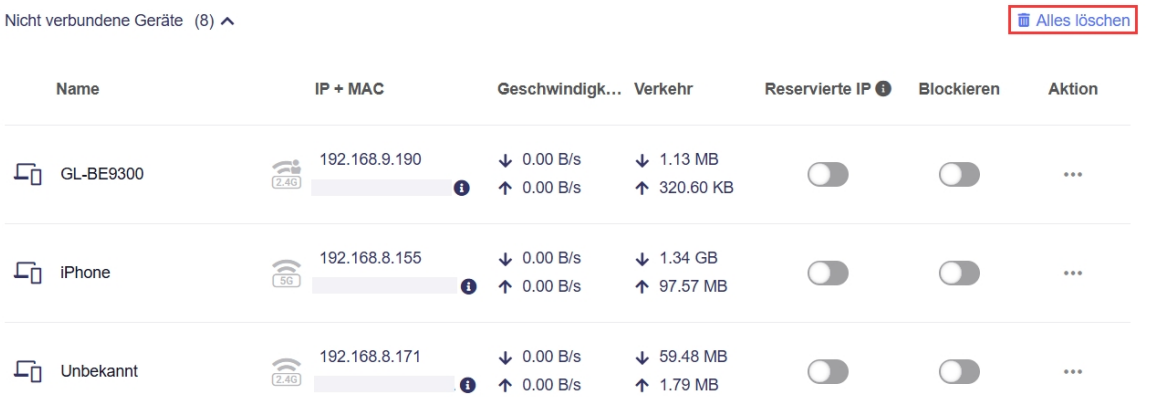
Wenn die Geschwindigkeitsbegrenzung auf ein Gerät angewendet wurde, werden die Upload-/Download-Geschwindigkeitspfeile gelb.



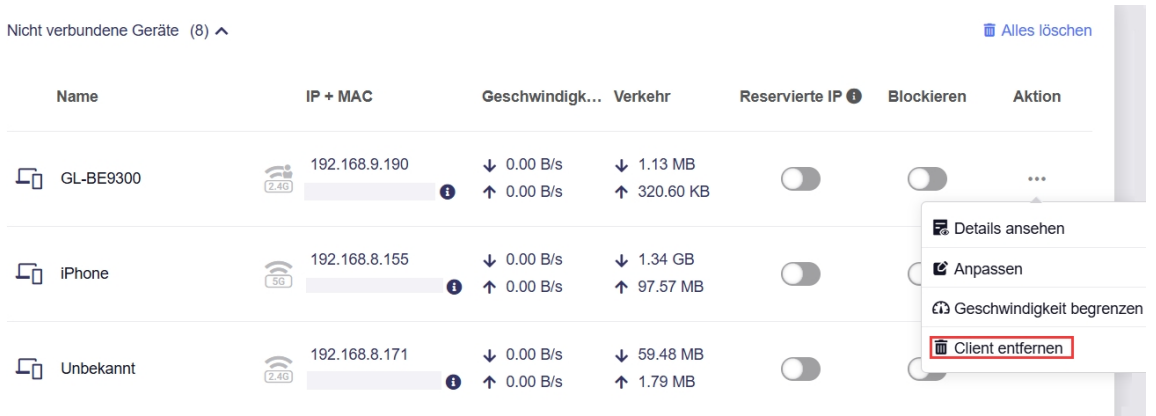
Tipp: Wenn die Option „Limit Speed“ nicht sichtbar ist, wechseln Sie zu **Netzwerk** > **Netzwerk-Beschleunigung** und deaktivieren Sie diese Funktion.

6.3 Entfernen von Clients

Im Bereich **Nicht verbundene Geräte** können Sie in der oberen rechten Ecke auf **Alles löschen** klicken, um alle Offline-Clients zu löschen.

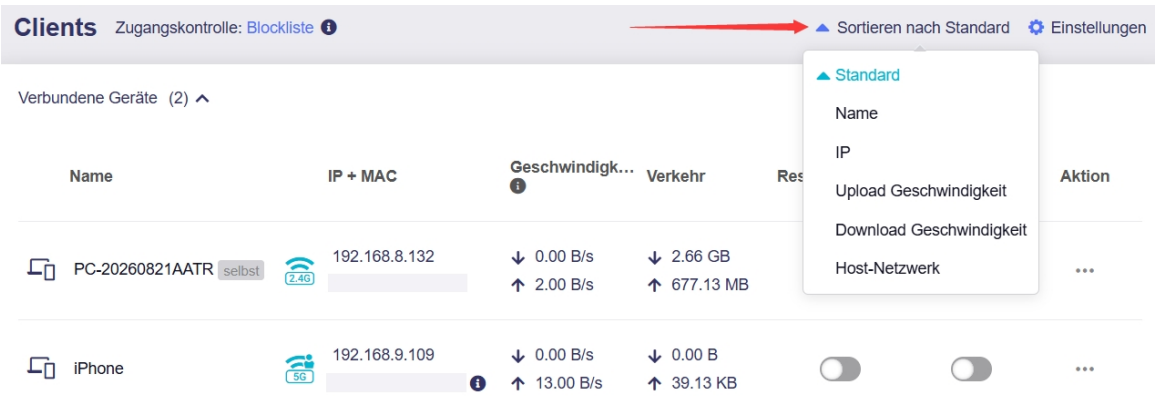


Wenn Sie einen bestimmten Client entfernen möchten, klicken Sie auf das Drei-Punkt-Symbol in der **Aktion** und klicken Sie dann auf **Clients entfernen** aus dem Dropdown-Menü.



6.4 Sortieren

Sie können die Gerätesortierungsregel für die Client-Seite in der oberen rechten Ecke festlegen.



Die Standard-Sortierregeln lauten wie folgt:

- Das Self-Gerät (d.h. das Gerät, mit dem auf das Web-Admin-Panel des Routers zugegriffen wird) wird immer zuerst aufgeführt.
- In dem Bereich **Verbundene Geräte** werden Geräte weiter oben angezeigt, wenn sie sich früher verbunden haben.
- In dem Bereich **Nicht verbundene Geräte** werden Geräte weiter oben angezeigt, wenn sie sich früher getrennt haben.

Kapitel 7

Cloud Dienst

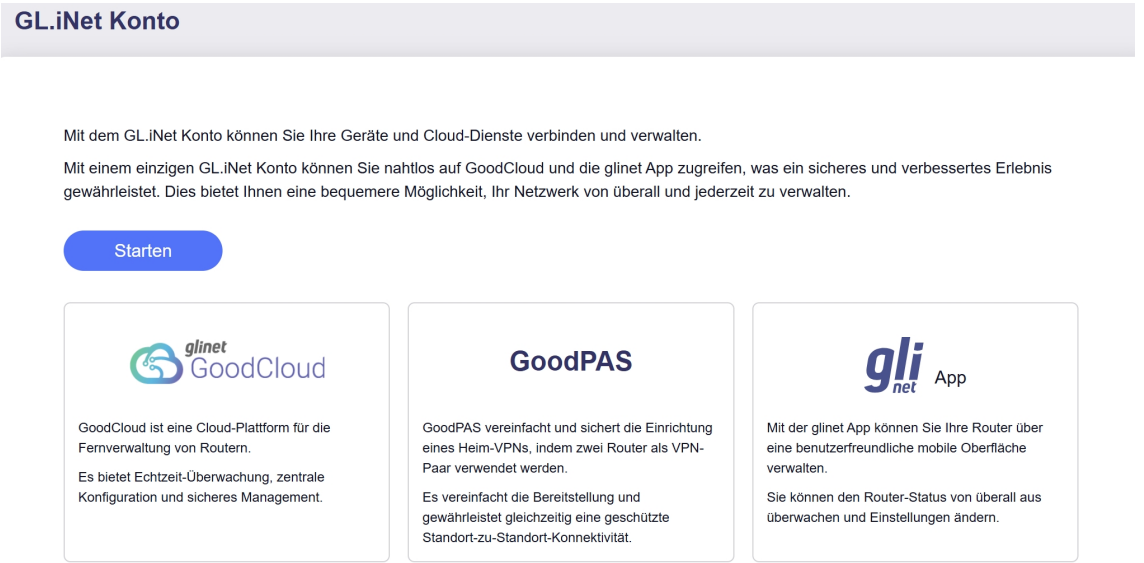
In diesem Kapitel werden drei Cloud Dienste vorgestellt: GL.iNet Konto, GoodCloud und GoodPAS.

7.1 GL.iNet Konto

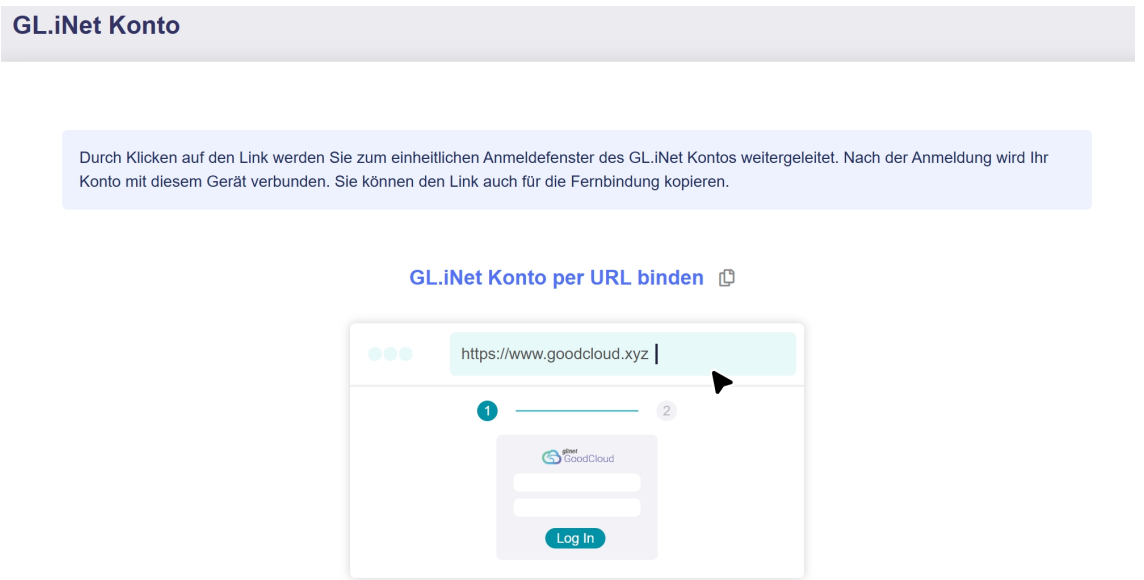
Mit dem GL.iNet-Konto können Sie Ihre Geräte und Cloud-Dienste verbinden und verwalten. Sie können anschließend auf Cloud-Funktionen und -Dienste zugreifen, darunter GoodCloud, GoodPAS und die GL.iNet-App.

7.1.1 GL.iNet-Konto aktivieren

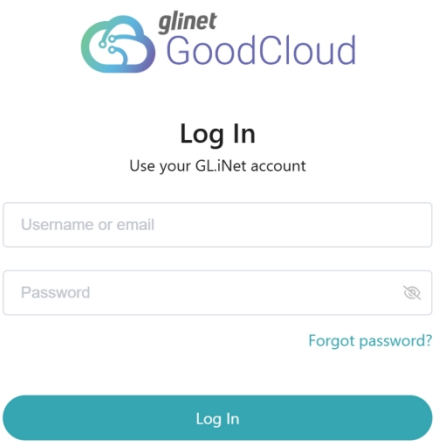
1. Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Cloud Dienst** > **GL.iNet Konto** und klicken Sie auf **Starten.**



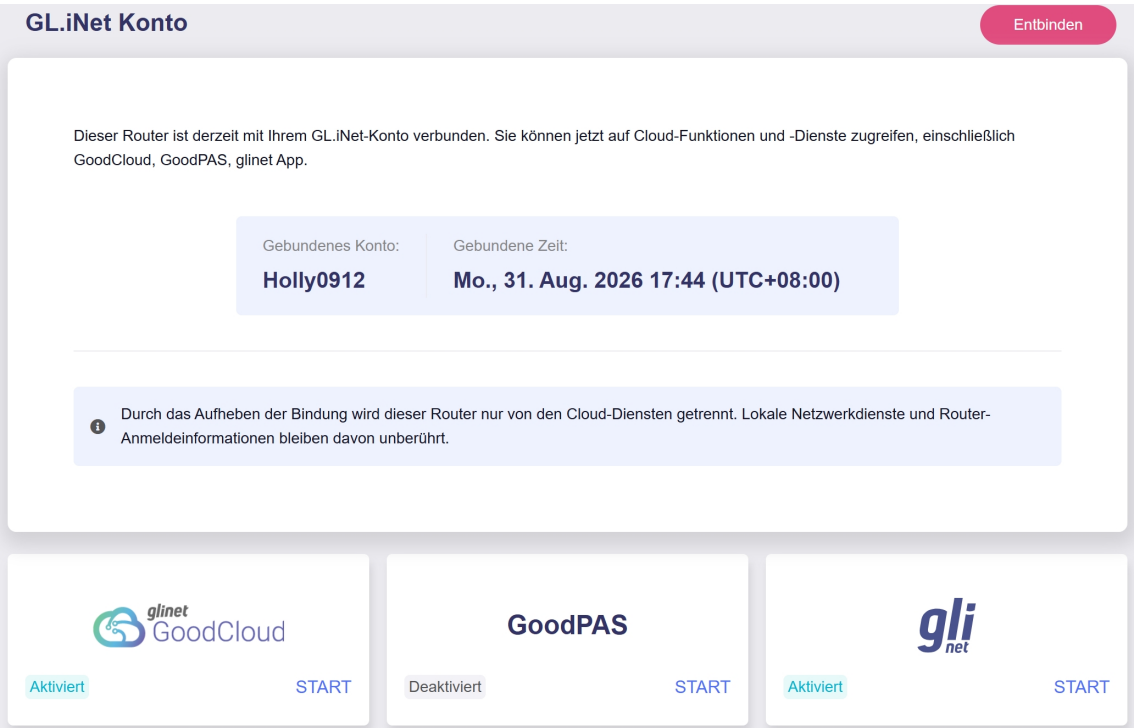
2. Eine URL wird dann auf der Seite angezeigt. Klicken Sie auf den **Link,** um sich über die Seite GL.iNet Konto anzumelden, oder kopieren Sie sie zur Fernbindung.



3. Melden Sie sich mit Ihrem GL.iNet-Konto an. Wenn Sie kein Konto haben, melden Sie sich für eines an und melden Sie sich an.



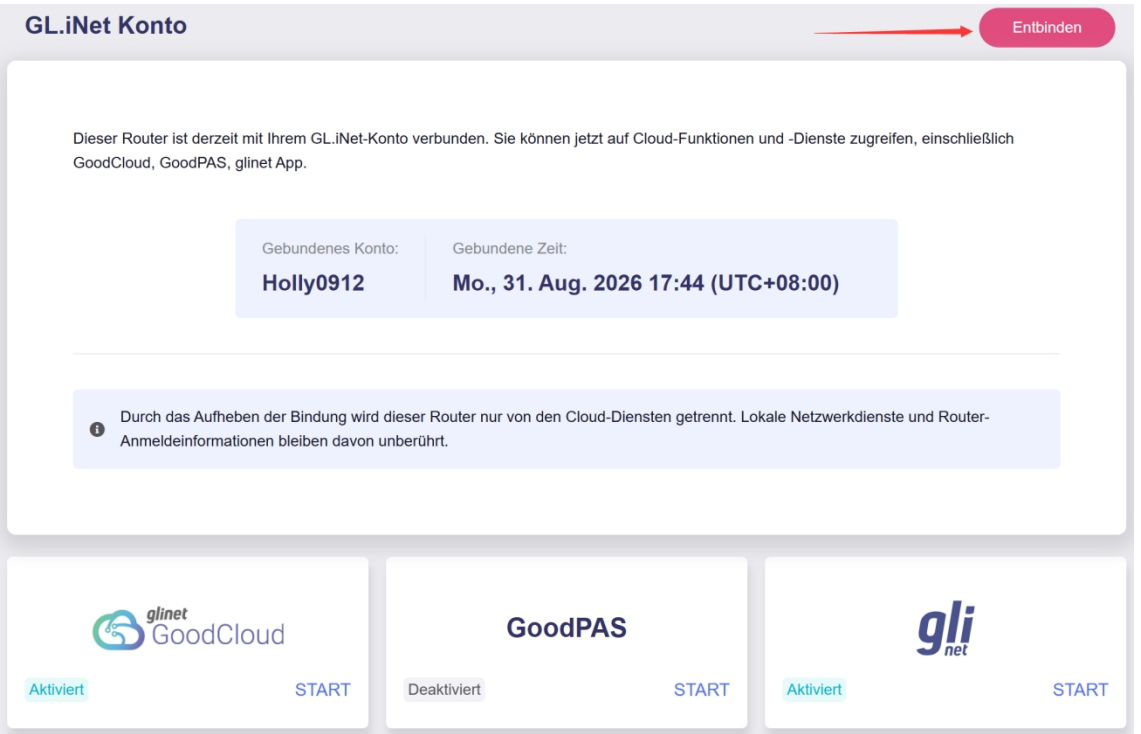
4. Nach der Anmeldung zeigt die Seite das verknüpfte Konto und den Zeitpunkt der Verknüpfung an. Auf dieser Seite können Sie die Verbindung zwischen dem Router und Ihrem GL.iNet-Konto verwalten. Prüfen Sie einfach die Kennzeichnung „Aktiviert“ bzw. „Deaktiviert“ unten links bei jedem Cloud-Dienst, um dessen aktuellen Status zu sehen. Klicken Sie neben dem jeweiligen Dienst auf „START“, um die zugehörige Funktionsseite zu öffnen.



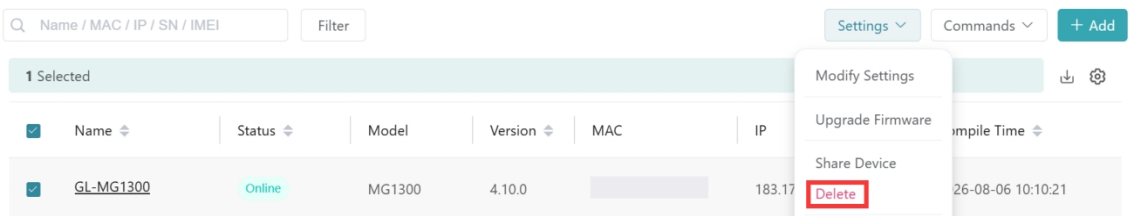
5. GoodPAS ist standardmäßig deaktiviert. Informationen zur Aktivierung finden Sie in Kapitel 7.3 GoodPAS.

7.1.2 GL.iNet-Konto freigeben

Navigieren Sie im Web-Admin-Panel des Routers zu **Cloud Dienst** > **GL.iNet Konto** und klicken Sie auf **Entbinden**. Ihr Gerät ist dann von Ihrem GoodCloud-Konto ungebunden.



Alternativ melden Sie sich bei der Cloud-Plattform an und navigieren Sie zu **Devices** > **Bound Devices**. Wählen Sie das Gerät aus, das Sie trennen möchten, klicken Sie oben rechts auf **Settings** und wählen Sie anschließend **Delete**. Ihr Gerät wird daraufhin von Ihrem GoodCloud-Konto getrennt.



7.2 GoodCloud

GL.iNet GoodCloud ist eine Plattform, die die Fernbereitstellung und Verwaltung verbundener Geräte vereinfacht. Sie bietet eine einfache Möglichkeit, aus der Ferne auf GL.iNet-Router zuzugreifen und sie zu verwalten. Durch die Zentralisierung von Netzwerkgeräten in der Cloud können Benutzer Verwaltungsaufgaben im Stapel effizient ausführen, etwa Netzwerkkonfigurationen bereitstellen und Software aktualisieren. Sie können auch aus der Ferne auf das Web-Admin-Panel des Routers zugreifen oder sich per SSH mit dem Terminal des Routers verbinden. GoodCloud unterstützt damit ein standortübergreifendes End-to-End-Management von Netzwerkgeräten.

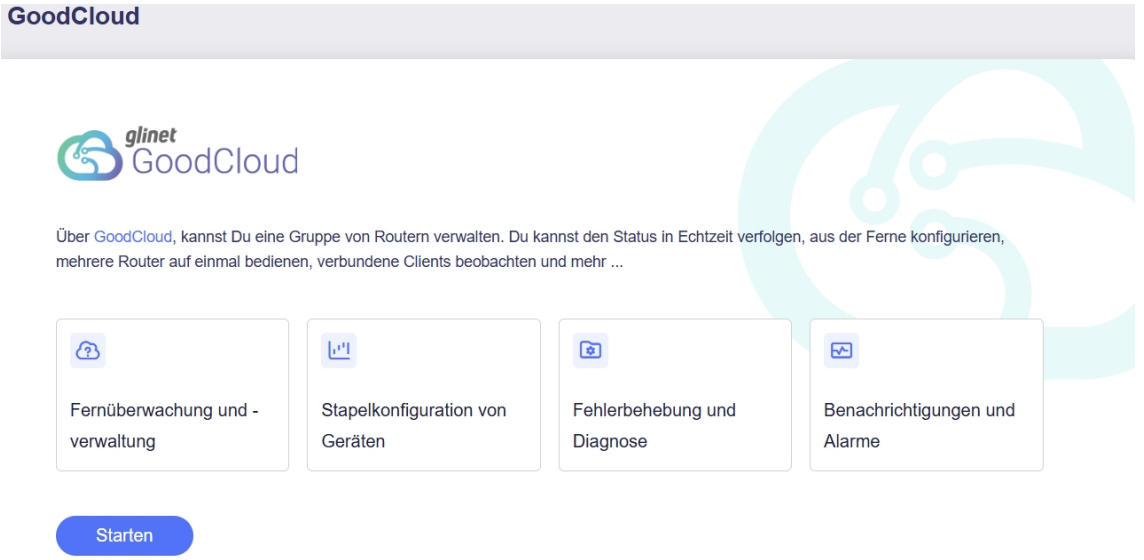
Mit GoodCloud können Sie:

- Überprüfen Sie den Status Ihres Routers in Echtzeit
- Verwalten von Routergruppen
- Router aus der Ferne einrichten
- Überwachen Sie angeschlossene Clients
- Router im Batch betreiben
- Aufbau einer Site-to-Site-Verbindung

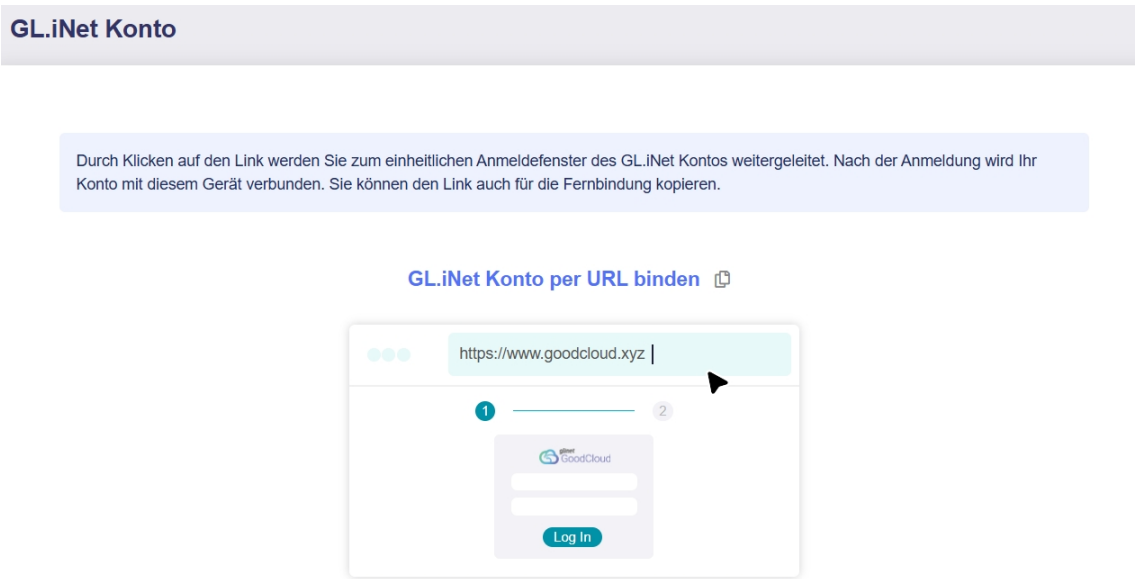
Einige Funktionen sind im Enterprise- und VAR-Plan (Value Added Reseller) verfügbar. Einzelheiten finden Sie hier.

7.2.1 GoodCloud aktivieren

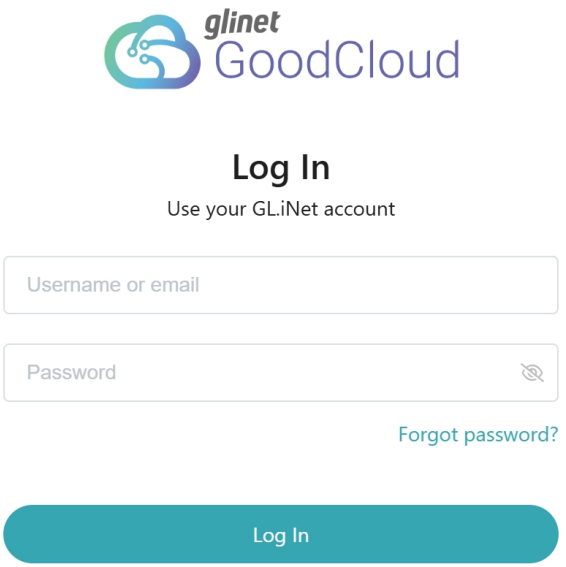
1. Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Cloud Dienst** > **GoodCloud** und klicken Sie auf **Starten.**



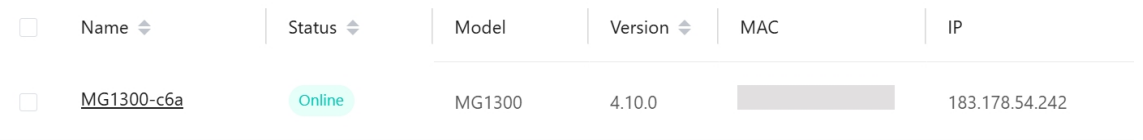
2. Eine URL wird dann auf der Seite angezeigt. Klicken Sie auf den **Link,** um sich über die Seite GL.iNet Konto anzumelden, oder kopieren Sie sie zur Fernbindung.



3. Melden Sie sich mit Ihrem GL.iNet-Konto an. Wenn Sie kein Konto haben, melden Sie sich für eines an und melden Sie sich an.



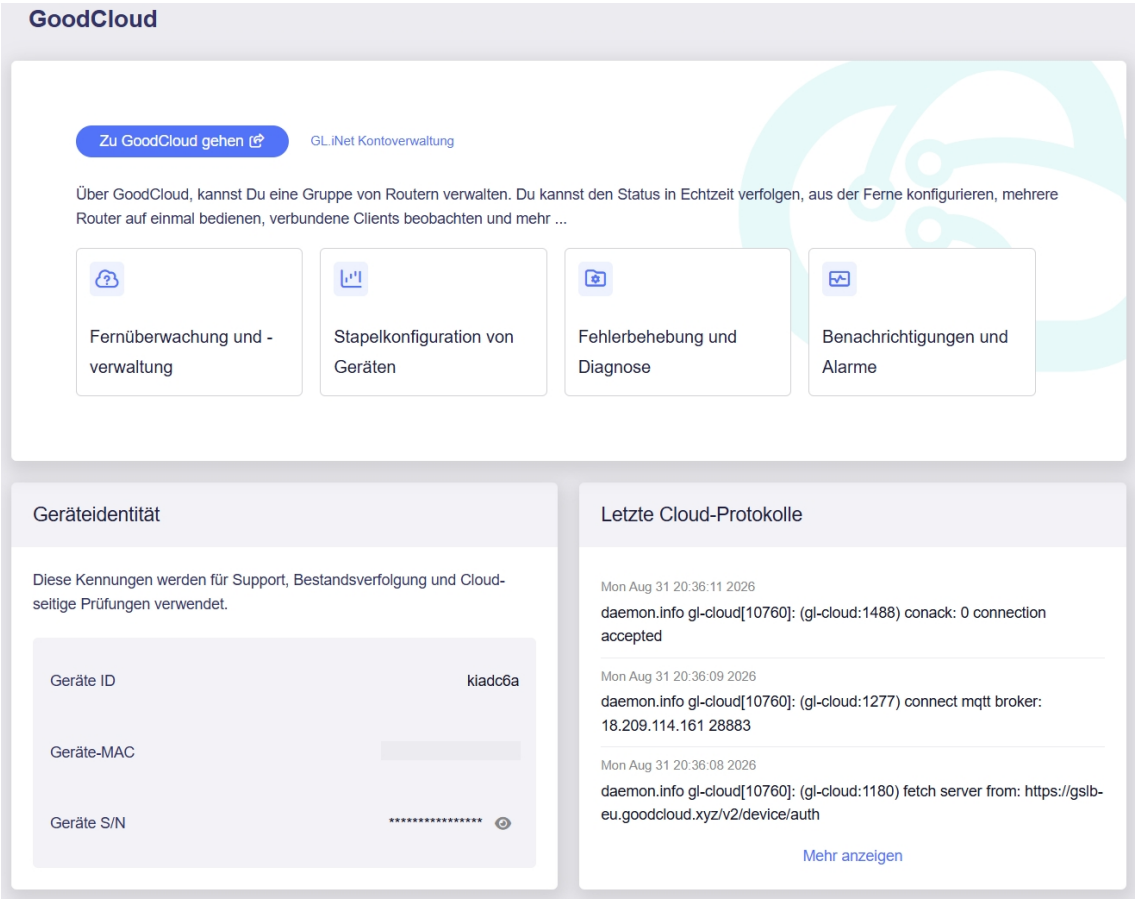
4. Bestätigen Sie im nächsten Schritt Ihr Konto und Ihre Geräteinformationen und klicken Sie dann auf **Bind**. Sie werden dann zur GoodCloud-Plattform weitergeleitet, wo Sie überprüfen können, ob Ihr Router an Ihr Konto gebunden ist.



Tipps:

- Die GoodCloud-Bindungsschritte unterscheiden sich je nach Firmware-Version.
- Wenn Sie die Bestätigungs-E-Mail während der Anmeldung nicht erhalten, überprüfen Sie Ihren Spam-Ordner oder versuchen Sie es später erneut. Für weitere Hilfe kontaktieren Sie uns unter support@gl-inet.com.

5. Nach erfolgreicher Verknüpfung kehren Sie zur Cloud-Service-Seite im Web-Admin-Panel zurück. Dort sehen Sie die gebundene Geräteidentität und die zuletzt verwendeten Cloud-Protokolle, einschließlich Geräte-ID, Geräte-MAC und Geräte-S/N.

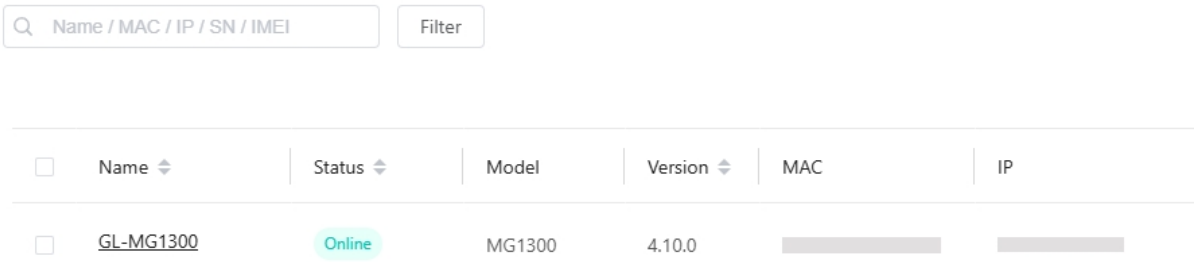


6. Sobald Sie sich bei GoodCloud angemeldet haben, sind auch Web-Fernzugriff aktivieren und SSH-Fernzugriff aktivieren, was besonders für die Fernverwaltung und Fehlersuche nützlich ist.
   - **Web-Fernzugriff aktivieren**: Remote Zugriff auf das Web-Admin-Panel des Routers von GoodCloud über HTTP/HTTPS.
   - **SSH-Fernzugriff aktivieren**: Fernzugriff auf das Terminal des Routers von GoodCloud aus mit SSH.

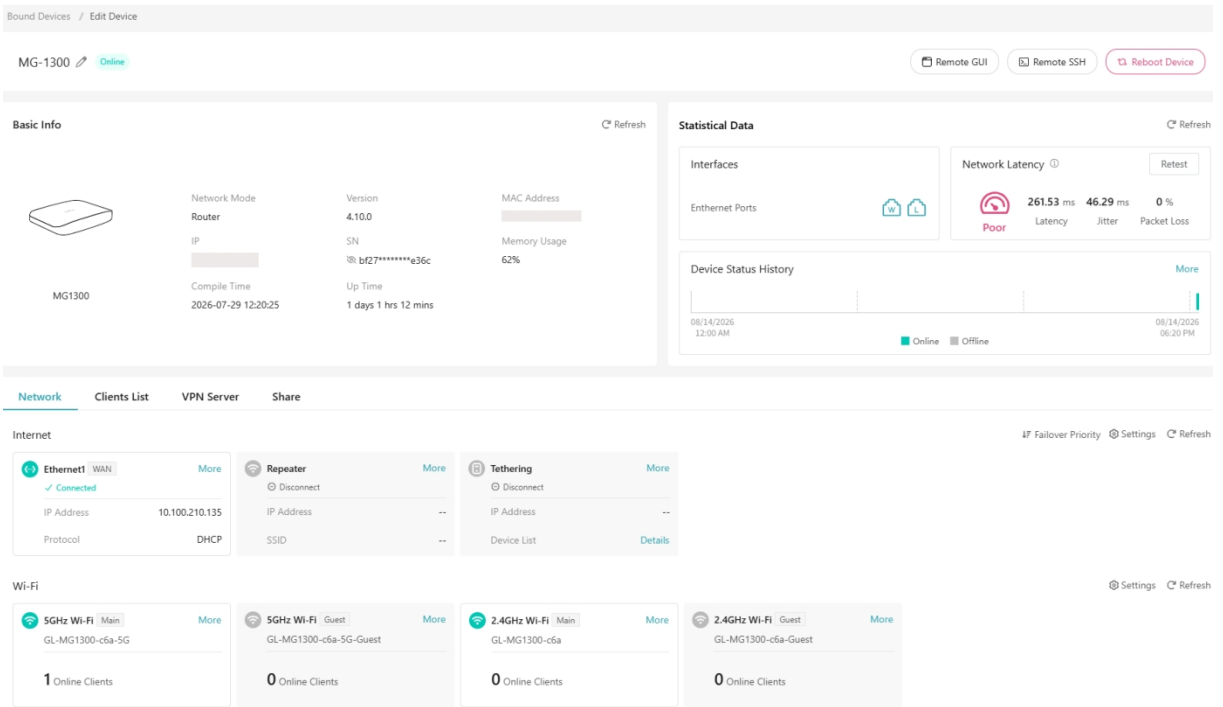
7.2.2 Verwalten Sie Ihren Router

Angaben zum Prüfgerät

Melden Sie sich bei der GoodCloud-Plattform an und navigieren Sie zu **Devices** > **Bound Devices**. Sie können die grundlegenden Informationen des Geräts wie Hostname, Status (online/offline), Modell, Firmware-Version und MAC-Adresse anzeigen.

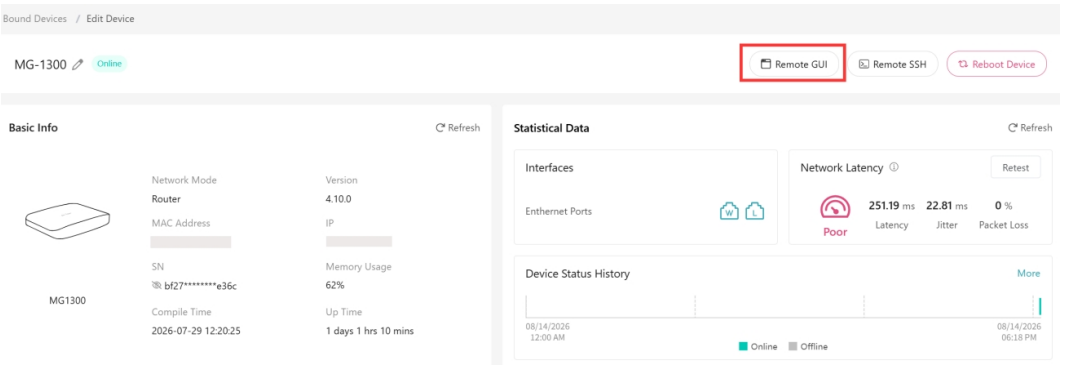


Klicken Sie auf den Gerätenamen, um die Gerätedetailseite zu betreten, auf der grundlegende Informationen, statistische Daten, Netzwerkübersicht, Clientliste und Zeitleiste angezeigt werden. Sie können auch erweiterte Operationen ausführen, wie z. B. den Fernzugriff auf den Router und das Neustarten des Geräts.

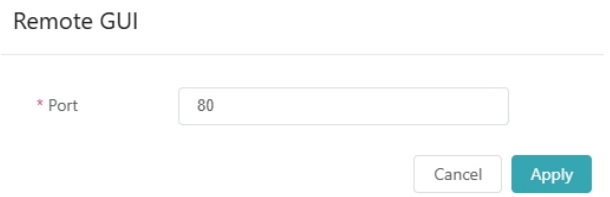


Web-Fernzugriff

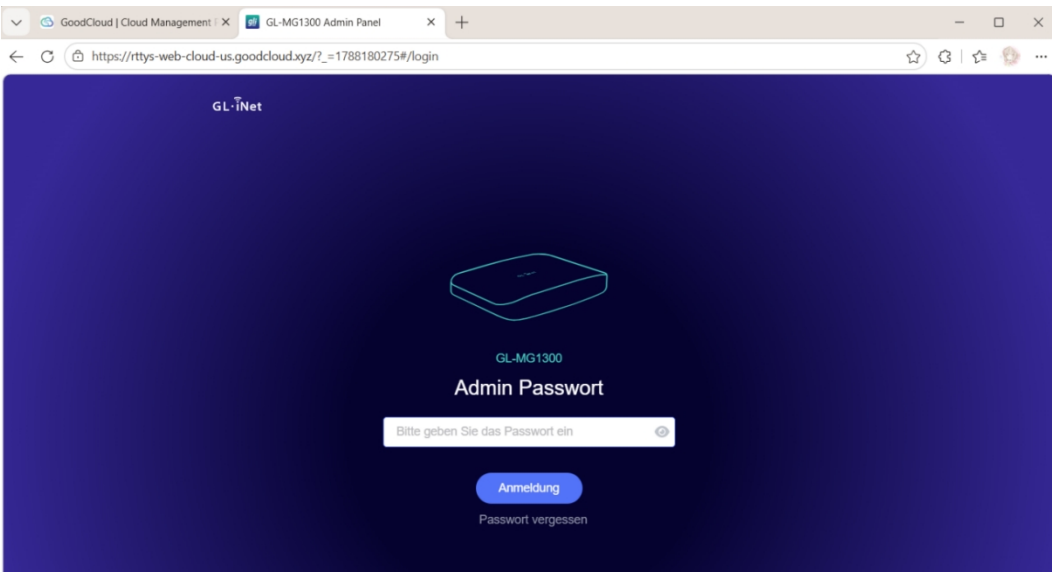
1. Melden Sie sich bei der GoodCloud-Plattform an und navigieren Sie zu **Devices** > **Bound Devices**. Klicken Sie auf das Gerät, auf das Sie zugreifen möchten; daraufhin wird die Seite mit den Gerätedetails angezeigt. Klicken Sie dort oben rechts auf die Schaltfläche „ **Remote GUI**“.



2. Wählen Sie das Übertragungsprotokoll und den Port aus. Die Standardwerte sind HTTP und Port 80. Sie können das Protokoll bei Bedarf auf HTTPS umschalten, und der Port wechselt automatisch zu 443.

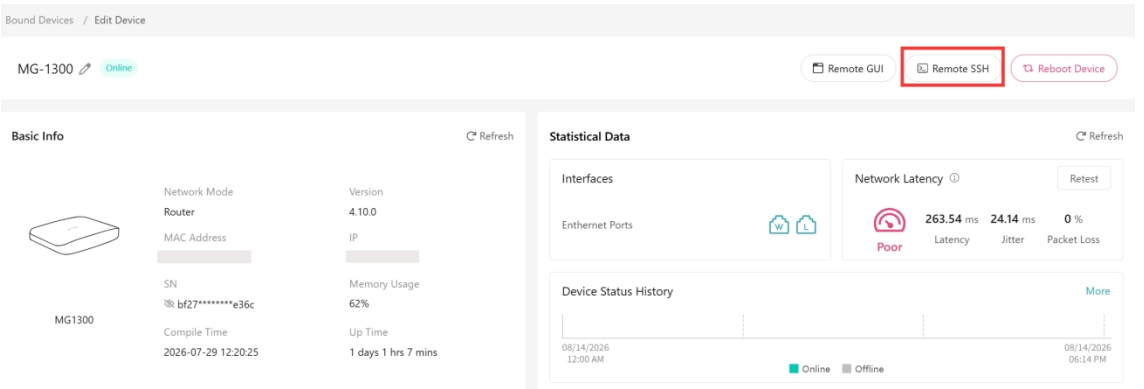


3. Sie werden auf die Anmeldeseite des Routers weitergeleitet. Geben Sie das Admin-Passwort ein, um aus der Ferne auf das Web-Admin-Panel des Routers zuzugreifen.



SSH-Fernzugriff

1. Melden Sie sich bei der GoodCloud-Plattform an und navigieren Sie zu **Devices** > **Bound Devices**. Klicken Sie auf das Gerät, auf das Sie zugreifen möchten, und Sie werden die Gerätedetails-Seite eingeben.
2. Auf der Gerätedetailseite klicken Sie oben rechts auf die Schaltfläche **Remote SSH**.

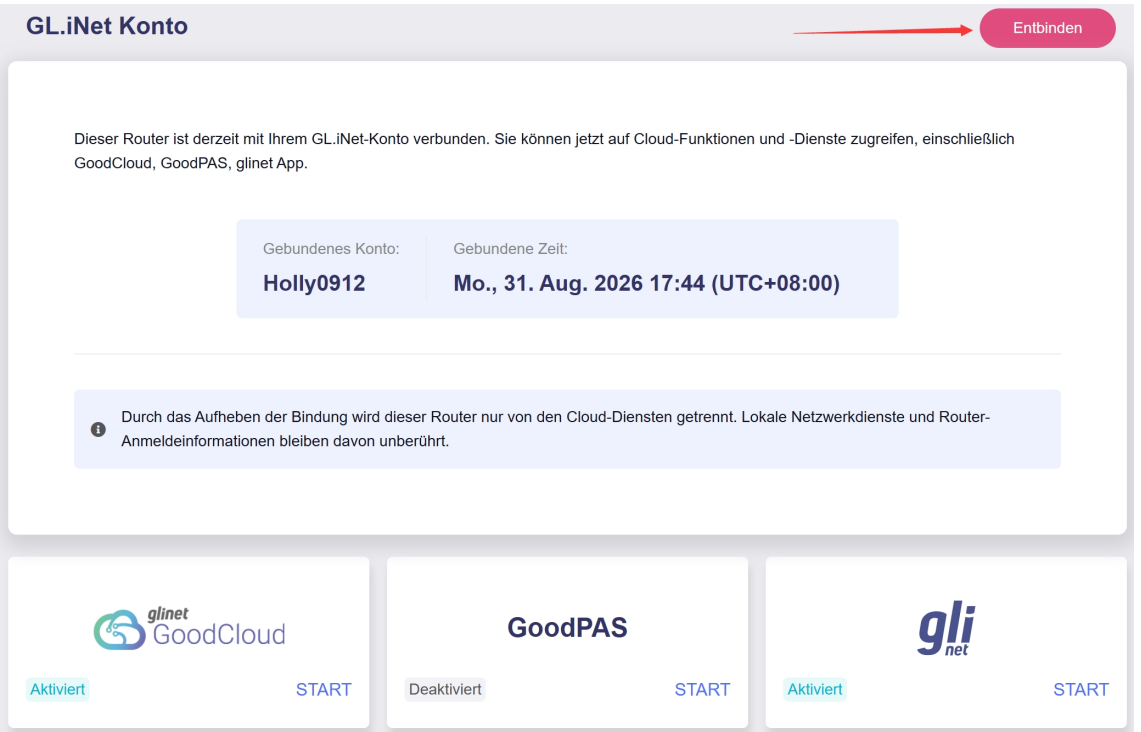


3. Melden Sie sich als **root** an und geben Sie das Passwort ein, um auf das Terminal Ihres Routers zuzugreifen.

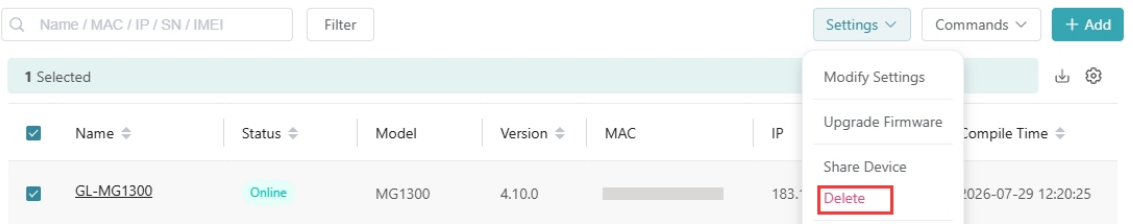


7.2.3 Entbindungseinrichtung

Navigieren Sie im Web-Admin-Panel des Routers zu **Cloud Dienste** > **GL.iNet Konto** und klicken Sie auf **Entbinden**. Ihr Gerät ist dann von Ihrem GoodCloud-Konto ungebunden.



Alternativ können Sie sich bei der Cloud-Plattform anmelden und zu **Devices** > **Bound Devices** navigieren. Wählen Sie das Gerät aus, das Sie trennen möchten, klicken Sie oben rechts auf **Settings** und wählen Sie anschließend **Delete**. Ihr Gerät wird daraufhin von Ihrem GoodCloud- Konto getrennt.



7.3 GoodPAS

GoodPAS ist eine erweiterte Netzwerkfunktion für GL.iNet-Router, die einen nahtlosen Fernzugriff und eine einfache Geräteverwaltung ermöglicht. GoodPAS ist in das GL.iNet-Router-SDK integriert, verwendet das AmneziaWG-Protokoll mit integrierter Datenverkehrsverschleierung und stellt stabile, sichere Verbindungen für zuverlässigen Fernzugriff jederzeit und überall bereit.

Diese Funktion ermöglicht einen nahtlosen Fernzugriff auf Ihr Heimnetzwerk. Sie können Geräte direkt über einen dynamischen Zugangscode im Web-Admin-Panel einrichten und koppeln, wodurch schnell eine sichere Verbindung zwischen Ihrem Reiserouter und Ihrem Heimnetzwerk in nur wenigen Sekunden hergestellt wird, ohne dass eine Registrierung oder Anmeldung erforderlich ist.

Hinweis:

1. Es wird nicht empfohlen, GoodPAS gleichzeitig mit einer der folgenden Funktionen zu verwenden, da dies zu Routing-Konflikten führen kann: GoodCloud Site to Site, ZeroTier, Tailscale, Tor.
2. Wenn GoodPAS aktiviert ist, kann der Netzwerkmodus nicht verwendet werden.

7.3.1 Schnelles Setup

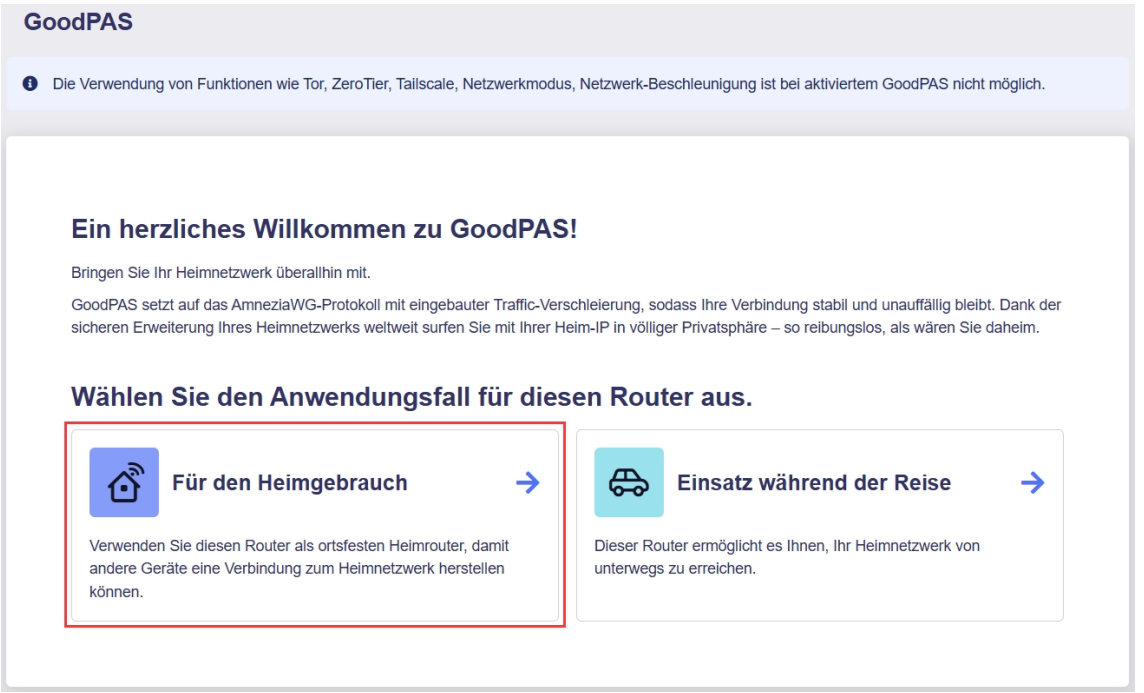
Im Folgenden finden Sie ein Beispiel für die Verwendung von Mango 2 (GL-MG1300) und Flint 3 (GL-BE9300), um ein GoodPAS-Netzwerk einzurichten. Flint 3 ist der Heimrouter, während Mango 2 der Reiserouter ist, der den Netzwerkverkehr zurück zu Flint 3 für den Internetzugang leitet.

Tipp: Jeder GL.iNet-Router umfasst **monatlich 10 GB kostenlose** Daten für GoodPAS-Netzwerke. Geräte in einem GoodPAS-Netzwerk nutzen die Daten des Heimrouters für den Internetzugriff. Bei Bedarf können Sie auf den GoodPAS+-Tarif mit unbegrenztem Datenvolumen upgraden.

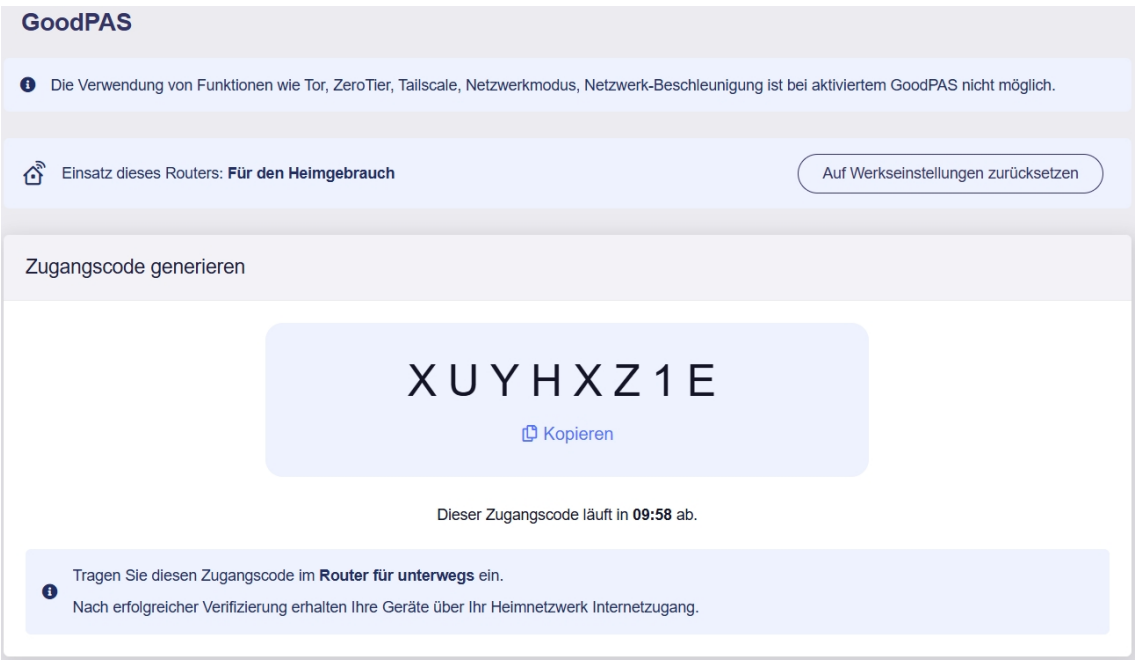
1. Konfigurieren Sie Flint 3 für das Internet.

Melden Sie sich im Web-Admin-Panel von Flint 3 an und navigieren Sie zur Internet-Seite. Verbinden Sie es mit dem Internet mit einer der unterstützten Internetverbindungsmethoden: Ethernet, Repeater, Tethering und Mobilfunknetz.

2. Navigieren Sie im Web-Admin-Panel von Flint 3 zu **Cloud Dienst** > **GoodPAS**. Klicken Sie auf Verwenden zu Hause.



Es erzeugt einen Zugangscode. Kopieren Sie diesen Code für die spätere Verwendung.

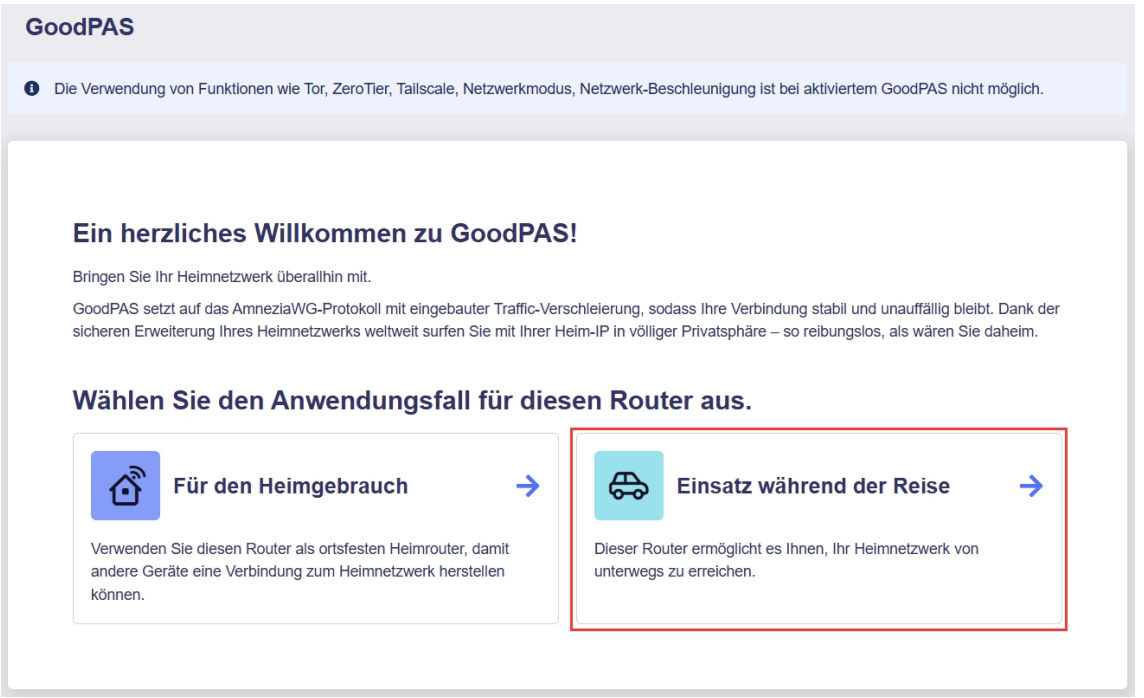


3. Konfigurieren Sie Mango 2 für das Internet.

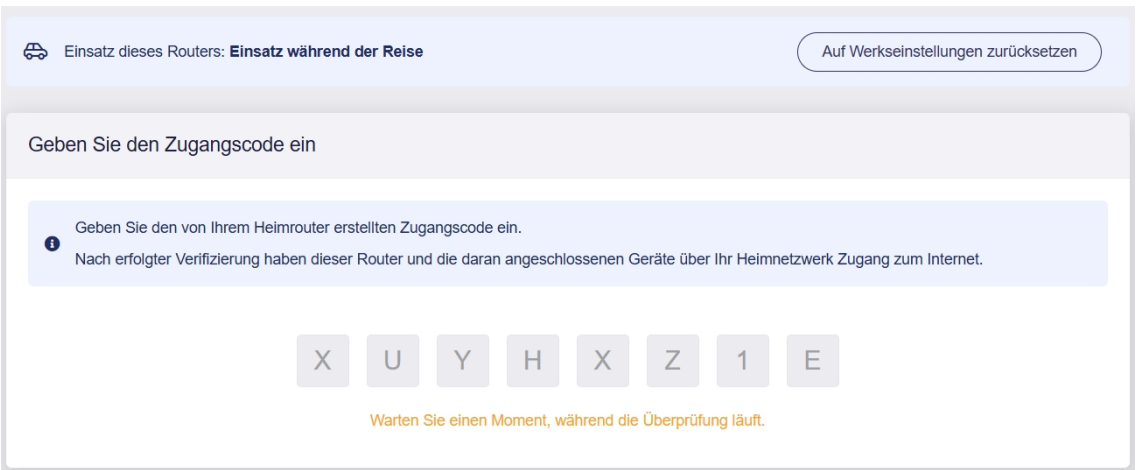
Melden Sie sich im Mango 2 Web Admin Panel an und navigieren Sie zur internet-Seite. Verbinden Sie es mit dem Internet mit einer der unterstützten Internetverbindungsmethoden: Ethernet, Repeater, Tethering und Mobilfunknetz.

4. Zugangscode eingeben.

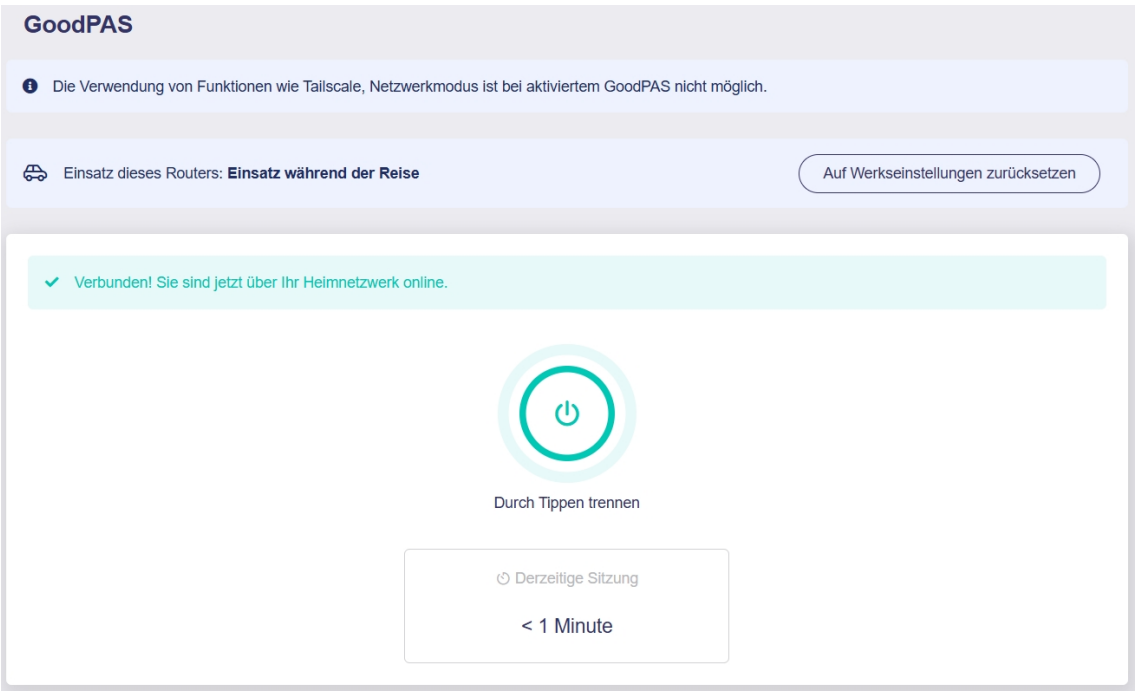
   Navigieren Sie im Web-Admin-Panel von Mango 2 zu **Cloud Dienst** > **GoodPAS.** Klicken Sie auf Verwenden während der Reise.



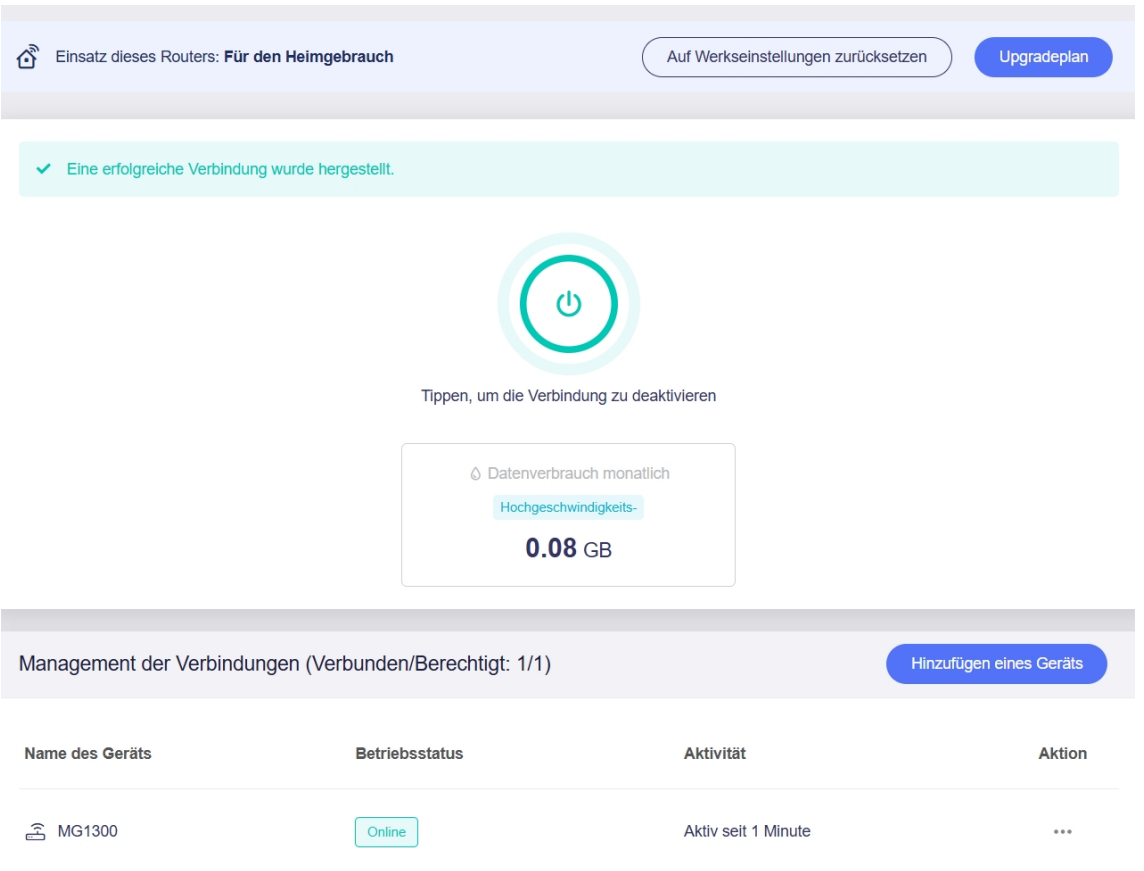
Geben Sie den in Schritt 2 erhaltenen Zugangscode ein und warten Sie, bis die Überprüfung abgeschlossen ist.



Es wird dann erfolgreich mit dem Flint 3 Home Router verbunden.

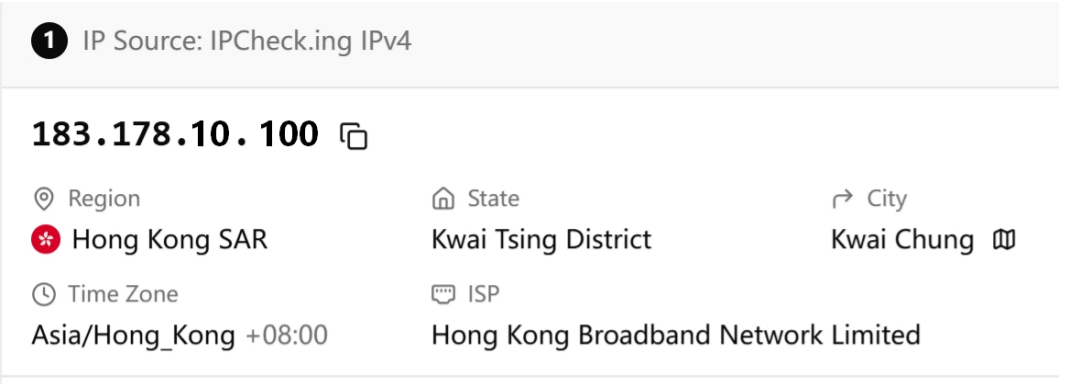


5. Im Web-Admin-Panel des Flint 3 wird auch der Verbindungsstatus angezeigt, wie unten gezeigt.

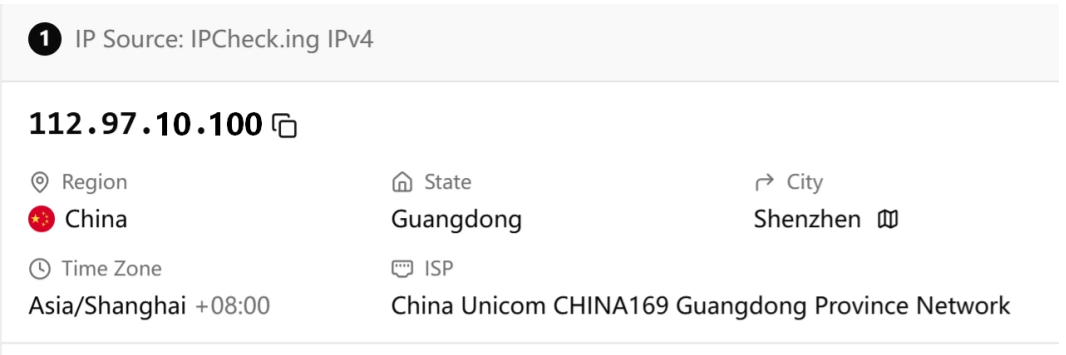


7.3.2 Konnektivitätsprüfung

1. Verbinden Sie einen Laptop oder ein Smartphone mit dem WLAN des Mango 2 Reiserouters.
2. Öffnen Sie einen Browser und besuchen Sie die Website ipcheck.ing oder eine andere IP-Adresse, auf der die öffentliche IP-Adresse von Flint 3 angezeigt wird, was darauf hinweist, dass Mango 2 über Ihren Flint 3-Home-Router auf das Internet zugreift.

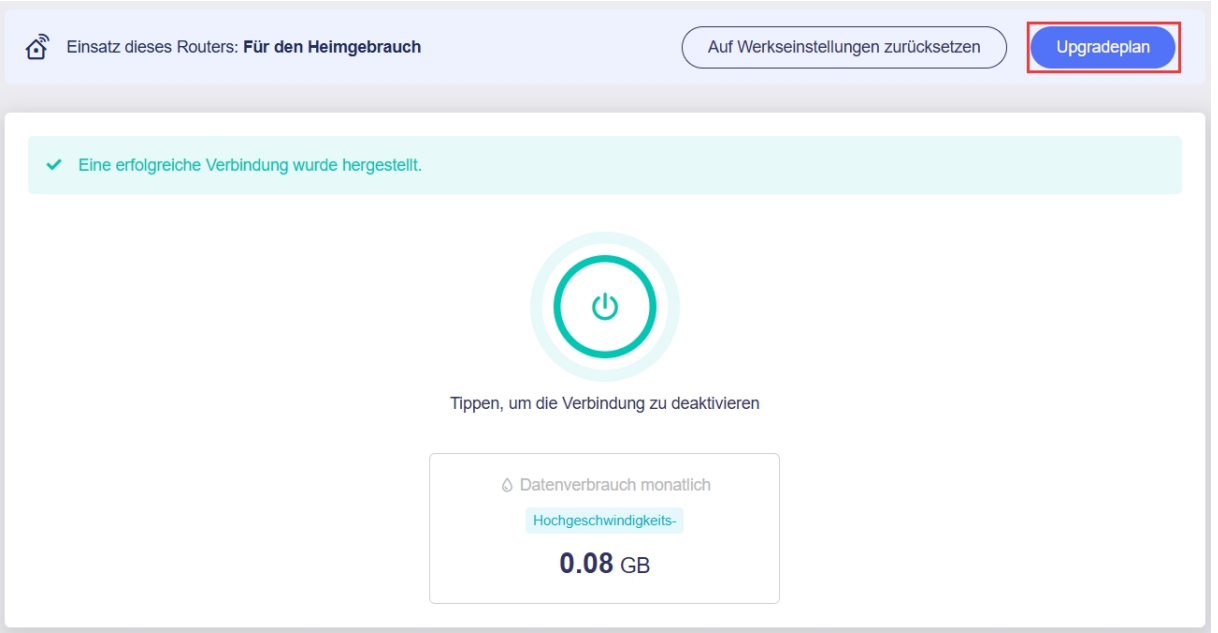


3. Trennen Sie die GoodPAS-Verbindung auf Mango 2, aktualisieren Sie dann die Webseite, um die IP-Abfrage erneut zu senden. Es wird die öffentliche IP-Adresse von Mango 2 angezeigt, was darauf hinweist, dass Mango 2 über sein lokales Netzwerk auf das Internet zugreift.



7.3.3 Upgrade-Plan

Jeder GL.iNet-Router umfasst **monatlich 10 GB kostenlose** Daten für GoodPAS-Netzwerke. Geräte in einem GoodPAS-Netzwerk nutzen die Daten des Heimrouters für den Internetzugriff. Bei Bedarf können Sie auf den GoodPAS+-Tarif mit unbegrenztem Datenvolumen upgraden.



Kapitel 8

VPN

Dieses Kapitel behandelt VPN-Grundlagen und häufige Anwendungsfälle; es erläutert, wie man einen GL.iNet-Router entweder als OpenVPN- oder WireGuard- Client oder -Server konfiguriert, und stellt das VPN-Dashboard vor.

8.1 VPN Grundlagen

VPN

Vpn, kurz für virtual private network, stellt einen verschlüsselten und privaten tunnel zwischen einem gerät und einem entfernten server her, schützt die datenübertragung und ermöglicht einen sicheren zugriff auf private oder eingeschränkte netzwerke.

VPN Router

Ein vpn-router verfügt über vorinstallierte vpn-funktionalität, die alle verbundenen geräte über vpn schützt im gegensatz zum einrichten von vpn auf einzelnen geräten, leitet die konfiguration des routers als vpn-client den gesamten verkehr durch einen verschlüsselten tunnel, ohne separate einrichtung pro gerät.

GL.iNet-Router unterstützen über 30 beliebte kommerzielle OpenVPN- und WireGuard-VPN-Dienste. Laden Sie Ihre VPN-Konfigurationsdateien hoch, um die VPN-Verbindung für sichere Netzwerke zu aktivieren. Sehen Sie hier die vollständige Liste der VPN-Anbieter von Drittanbietern.

OpenVPN

OpenVPN ist ein Open-Source-VPN-Protokoll, das SSL/TLS-basierte Sicherheit für Point-to-Site- oder Site-to-Site-Verbindungen verwendet. Es unterstützt mehrere Verschlüsselungsmethoden, TCP/UDP und eine einfache Firewall/NAT-Umgehung.

WireGuard

WireGuard ist ein leichtes, schnelles VPN-Protokoll, das einfacher und effizienter ist als OpenVPN. Es verfügt über moderne Kryptographie für Effizienz, eine kleine Codebasis für einfachere Auditierung und Sicherheit sowie modernste Algorithmen (ChaCha20 / Poly1305) für Verschlüsselung und Datenintegrität.

8.2 Einsatzszenarien

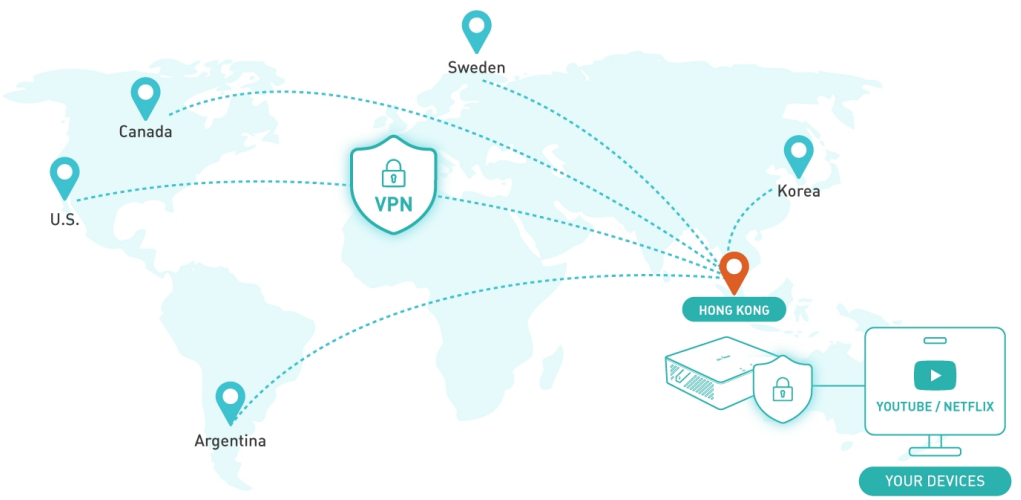
1. **Datenschutz personenbezogener Daten**

   Der vpn-dienst ist mit einer vielzahl von geräten über unseren router kompatibel, einschließlich nicht nur laptops, telefone und tablets, sondern auch spielkonsolen, fernseher und streaming-geräte. ihre daten werden geschützt, ob über drahtlose oder kabelgebundene verbindungen. sie können sogar vpn-richtlinien anpassen, um flexiblen schutz für bestimmte geräte zu erreichen.



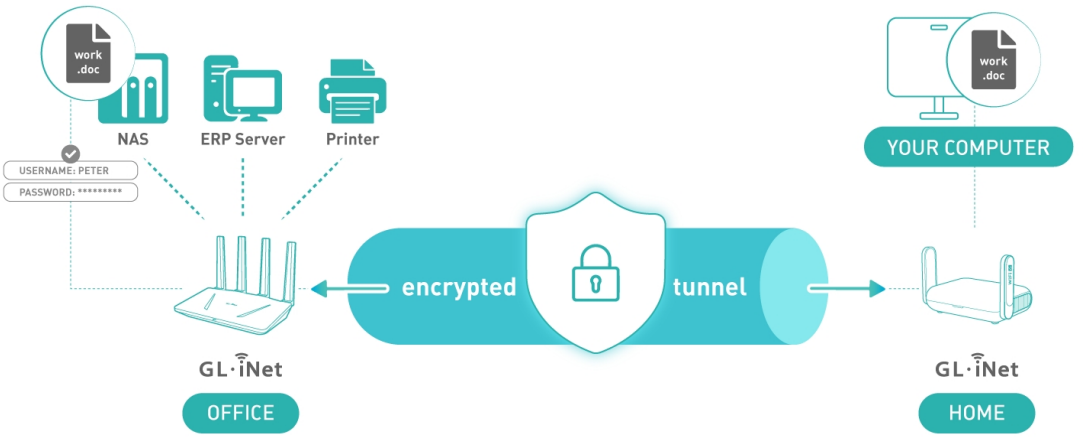
2. **Uneingeschränkter Zugang weltweit**

   Der zugriff auf einige websites kann durch den standort eingeschränkt sein wenn vpn aktiviert ist, können sie bei bedarf alle websites entsperren wenn sie sich mit verschiedenen servern von drittanbietern verbinden, erhalten sie verschiedene ip-adressen für das surfen oder den zugriff auf regionenblockierte websites.



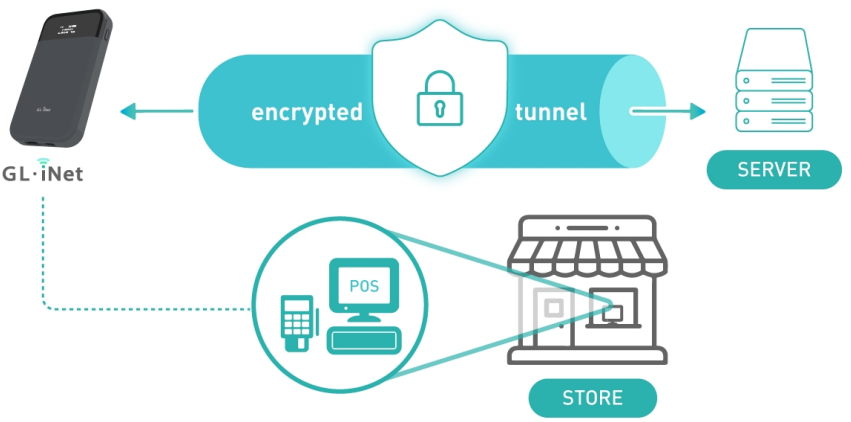
3. **Datensicherheit für kleine Unternehmen**

Viele Menschen arbeiten in Coworking Spaces oder Cafés und verlassen sich auf kostenloses öffentliches Wi-Fi. Solche Netzwerke sind anfällig für cyberkriminelle Angriffe. Durch die Konfiguration Ihres Reiserouters als VPN-Client können Sie überall eine sichere Konnektivität für die Arbeit genießen.



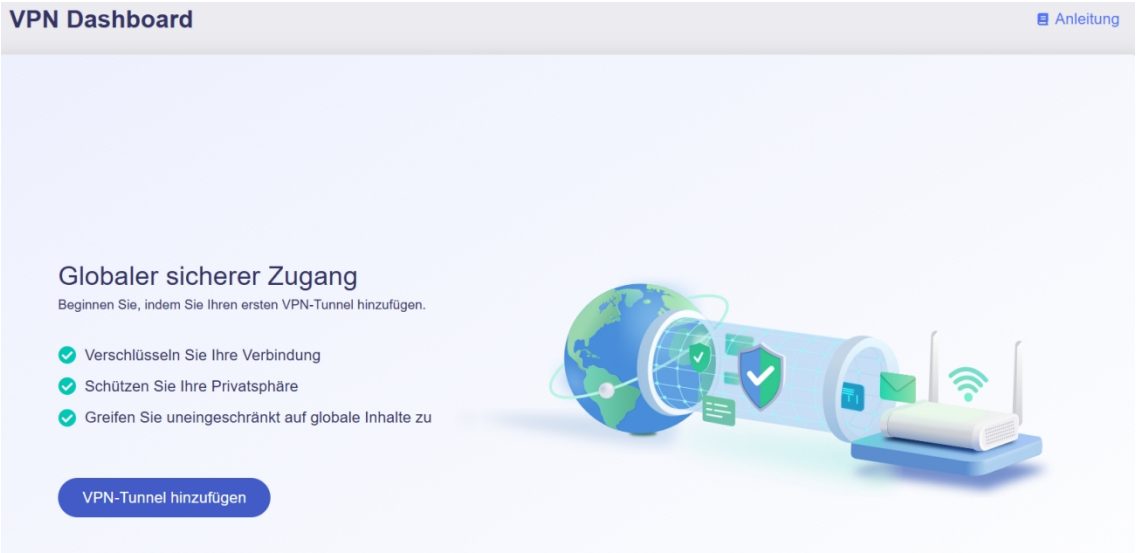
4. **Sichere Zahlungsinfrastruktur**

Kleine Einzelhandelsbesitzer müssen die Zahlungsinformationen der Kunden bei der Durchführung von Geschäften vor Ort behandeln. Mit einem VPN-Router können ihre POS-Maschinen Kreditkarteninformationen über einen verschlüsselten VPN-Tunnel hochladen, um die Zahlungssicherheit zu gewährleisten.



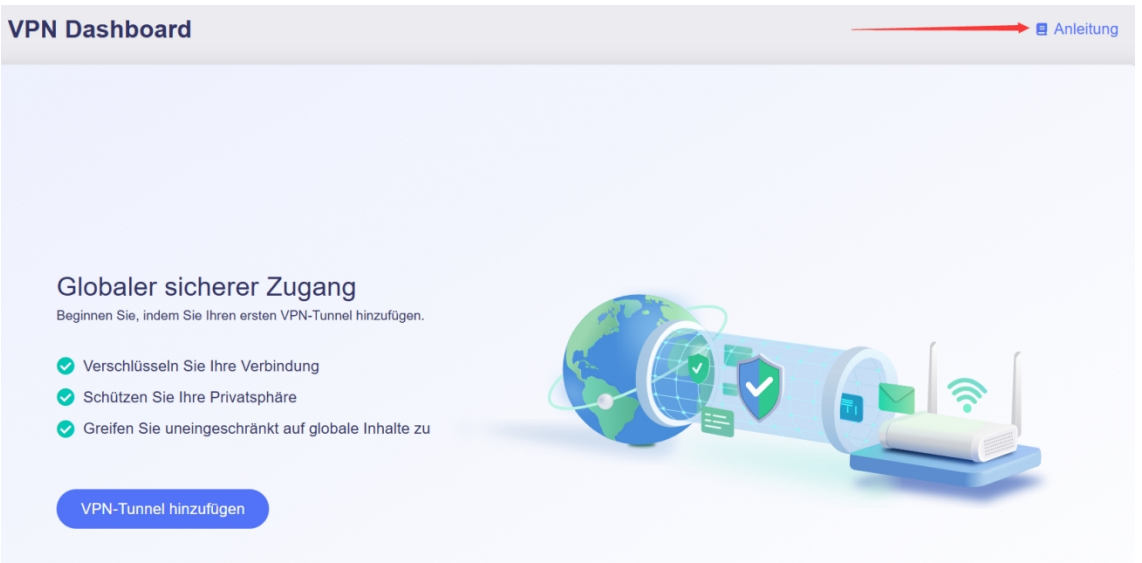
8.3 VPN Dashboard

Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **VPN** > **VPN Dashboard**.



Das VPN-Dashboard zeigt in der Regel VPN-Verbindungsdetails an, wie Tunnelregeln, Serveradresse, Verkehrsstatistiken, virtuelle Client-IP und Verbindungsprotokoll, und ermöglicht es Benutzern, erweiterte Einstellungen wie den VPN-Kill-Switch, IP-Masquerading und MTU zu konfigurieren. Sie können auch mehrere VPN-Verbindungen aktivieren und verschiedene VPN-Richtlinien für Multi-Tunnel-Szenarien konfigurieren.

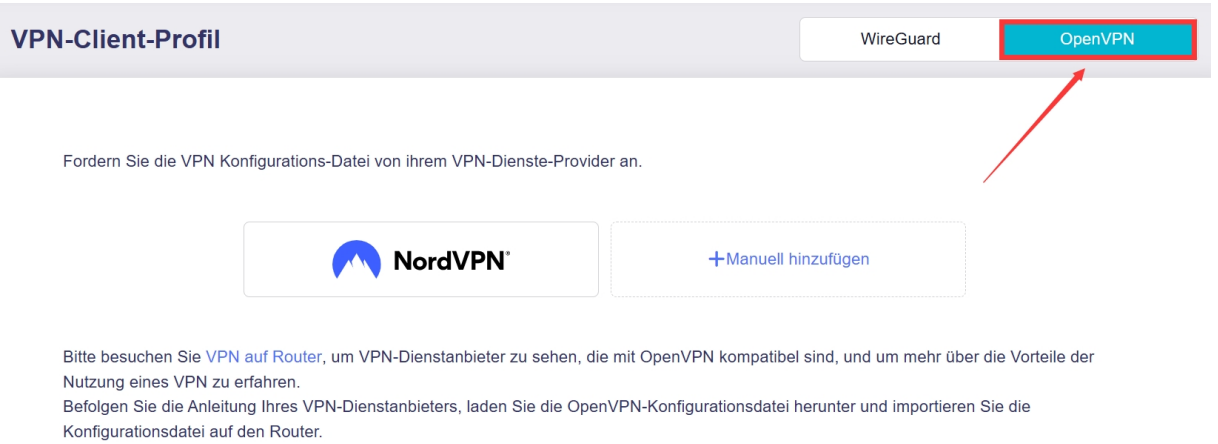
Klicken Sie auf das Buch-Symbol oben links und folgen Sie dem VPN-Setup-Assistenten, um Ihre VPN-Konfiguration schnell abzuschließen. Bitte lesen Sie dieses Tutorial für Details.



8.4 OpenVPN Client

OpenVPN ist ein Open-Source-VPN-Protokoll, das SSL/TLS-Verschlüsselung verwendet, um sichere Punkt-zu-Punkt- und Site-to-Site-Verbindungen herzustellen.

Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **VPN** > **VPN-Client-Profil** > **OpenVPN Client**.

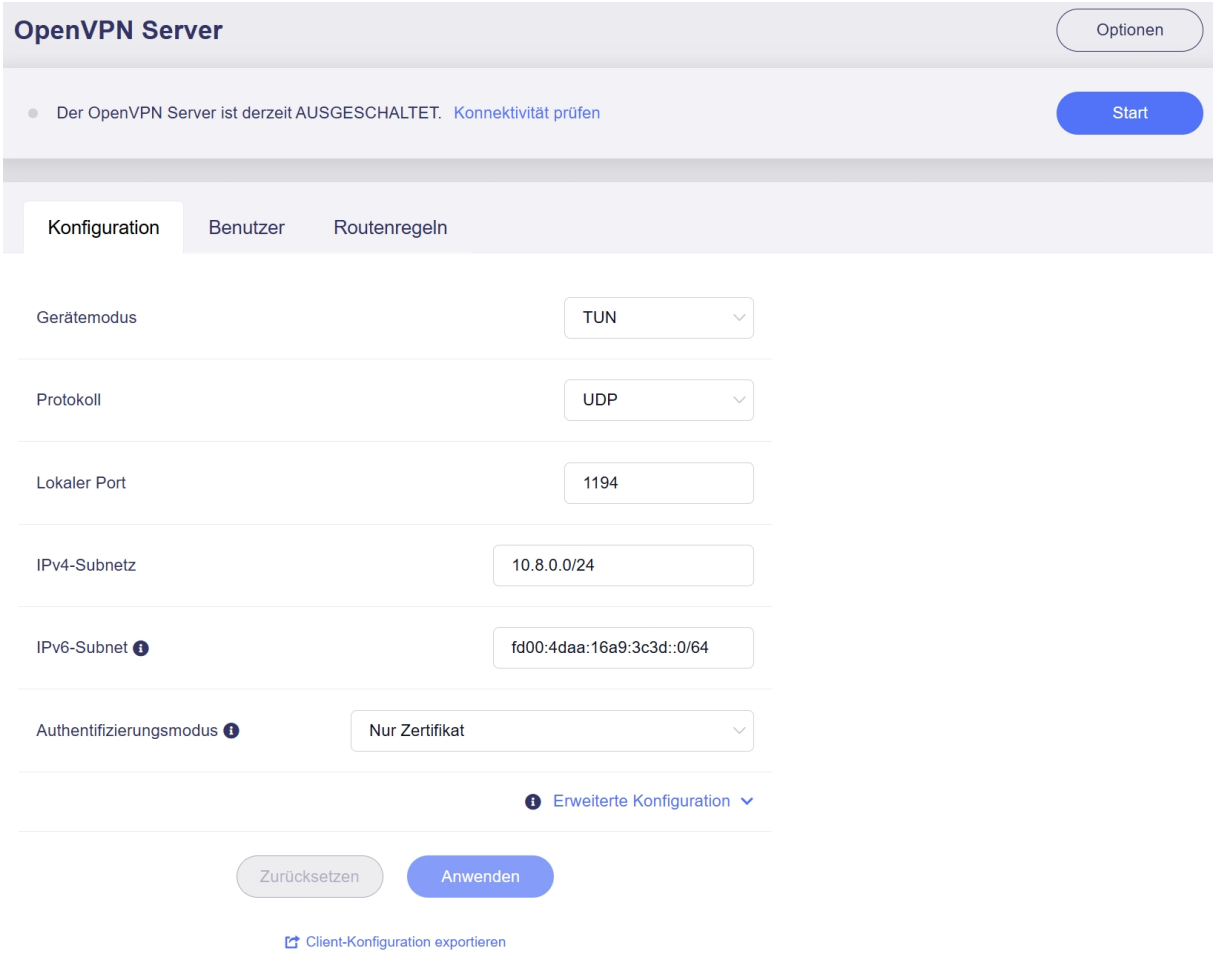


Einrichten Sie Ihren GL.iNet-Router als OpenVPN-Client, um den gesamten LAN-Verkehr zu verschlüsseln und über einen VPN-Tunnel zu routieren. Sie können auch mehrere VPN-Verbindungen aktivieren und verschiedene VPN-Richtlinien für Multi-Tunnel-Bereitstellungen einrichten.

Bitte lesen Sie dieses Tutorial, um Ihren GL.iNet-Router als OpenVPN-Client zu konfigurieren.

8.5 OpenVPN Server

Melden Sie sich im Webadmin-Panel des Routers an und navigieren Sie zu **VPN** > **OpenVPN Server**. Auf dieser Seite können Sie Ihren eigenen OpenVPN-Server einrichten.

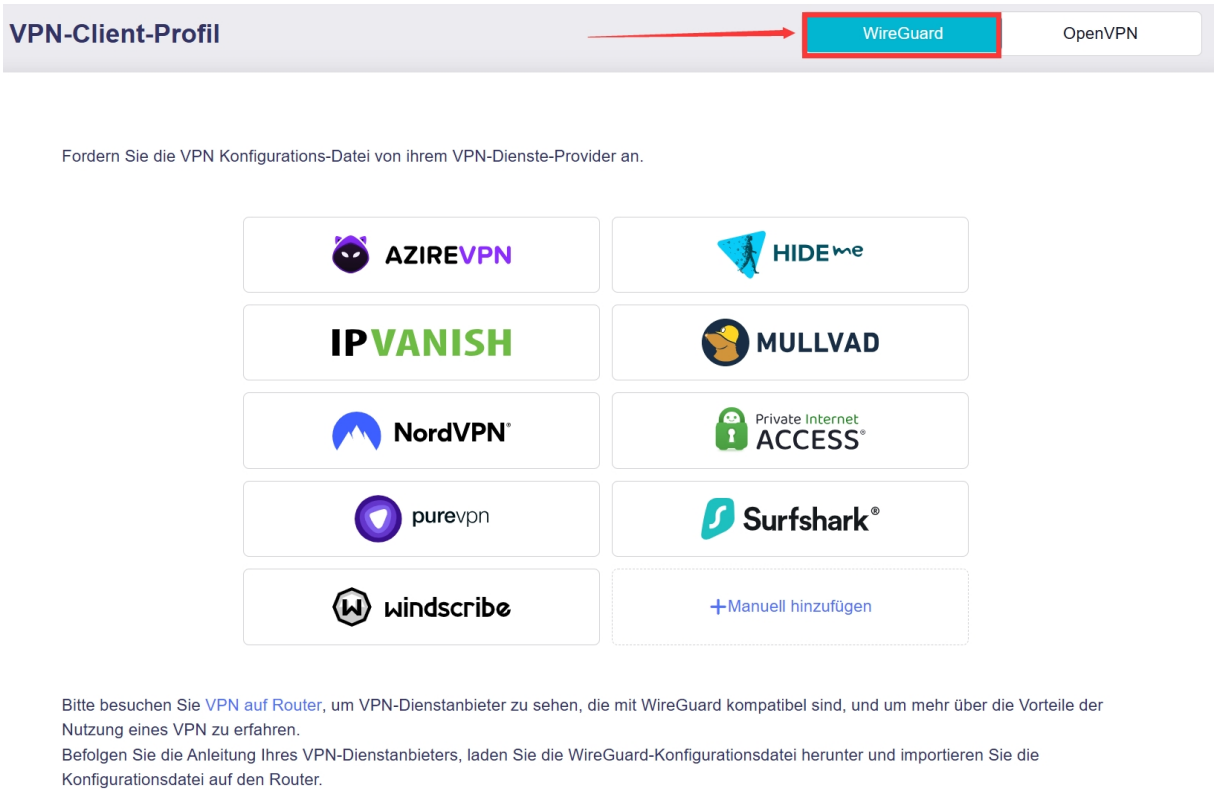


Generieren Sie die OpenVPN-Konfigurationsdatei und importieren Sie sie dann auf das Gerät, das Sie als OpenVPN-Client konfigurieren möchten, um eine Verbindung herzustellen. Sobald der OpenVPN-Server verbunden ist, sichert er den gesamten Datenverkehr, der vom OpenVPN-Client stammt. Bitte lesen Sie dieses Tutorial für weitere Details.

8.6 WireGuard Client

WireGuard® ist ein besonders einfaches, schnelles und modernes VPN, das modernste Kryptografie verwendet. Es wurde entwickelt, um schneller, einfacher, schlanker und praktischer als IPSec zu sein, ohne den damit üblicherweise verbundenen hohen Aufwand. Darüber hinaus bietet es eine deutlich höhere Leistung als OpenVPN.

Melden Sie sich im Web-Admin-Panel des Routers an und navigieren Sie zu **VPN** > **VPN-Client-Profil** > **WireGuard Client**.

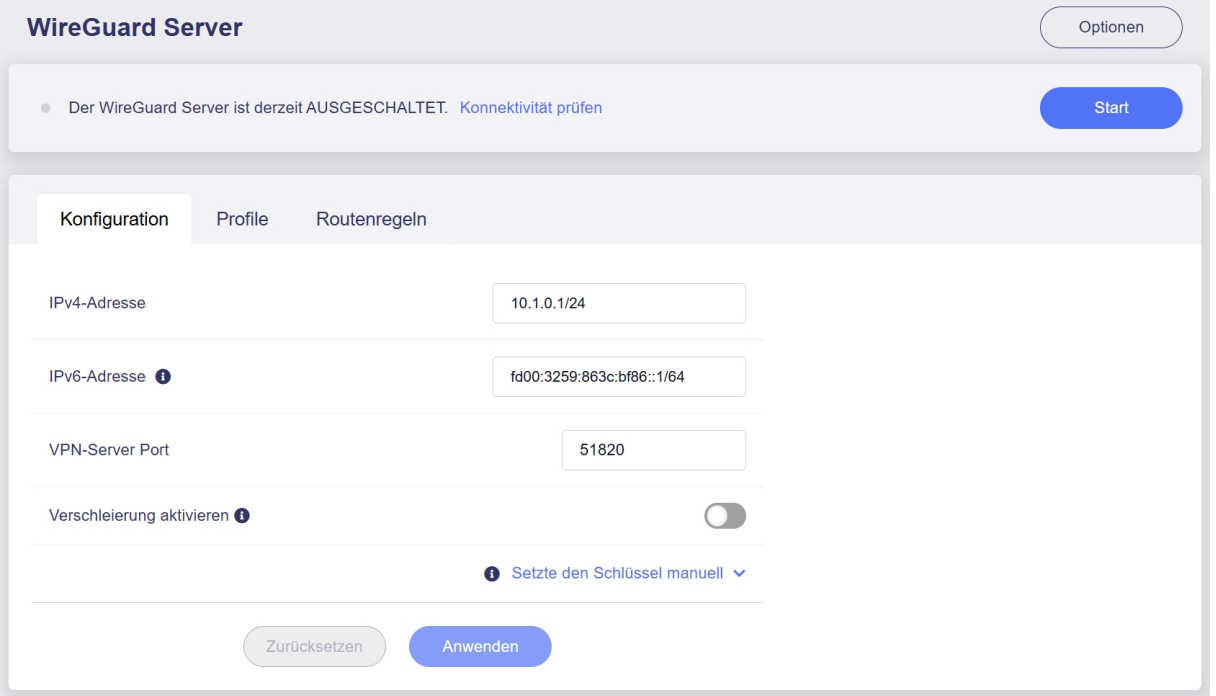


Einrichten Sie Ihren GL.iNet-Router als WireGuard-Client, um den gesamten LAN-Verkehr zu verschlüsseln und über einen VPN-Tunnel zu routieren. Sie können auch mehrere VPN-Verbindungen aktivieren und verschiedene VPN-Richtlinien für Multi-Tunnel-Bereitstellungen einrichten.

Bitte lesen Sie dieses Tutorial, um Ihren GL.iNet-Router als OpenVPN-Client zu konfigurieren.

8.7 WireGuard Server

Melden Sie sich im Webadmin-Panel des Routers an und navigieren Sie zu **VPN** > **WireGuard Server**. Auf dieser Seite können Sie Ihren eigenen WireGuard-Server einrichten.



Generieren Sie die WireGuard-Konfigurationsdatei und importieren Sie sie dann auf das Gerät, das Sie als WireGuard-Client konfigurieren möchten, um eine Verbindung herzustellen. Sobald der WireGuard-Server verbunden ist, sichert er den gesamten Datenverkehr, der vom WireGuard-Client stammt. Bitte lesen Sie dieses Tutorial für weitere Details.

Kapitel 9

Netzwerk

In diesem Kapitel werden netzwerkbezogene Einstellungen für Konfiguration und Verwaltung wie Subnetz, DNS und IPv6 vorgestellt.

9.1 Multi WAN

Multi-WAN ermöglicht die gleichzeitige Nutzung mehrerer Internetzugangsmethoden, wodurch verschiedene Konnektivitätsoptionen auf dem Router konfiguriert werden können.

- **Ausfallsicherung**: Wechselt automatisch innerhalb kurzer Zeit zu einer alternativen Verbindung, wenn die primäre Verbindung ausfällt, wodurch ein ununterbrochener Netzwerkzugriff gewährleistet ist.
- **Lastverteilung**: Verteilt den Netzwerkverkehr auf alle verfügbaren Verbindungen in einem festgelegten Verhältnis für die gleichzeitige Mehrfachverbindungsnutzung und optimiert die Bandbreitenauslastung.

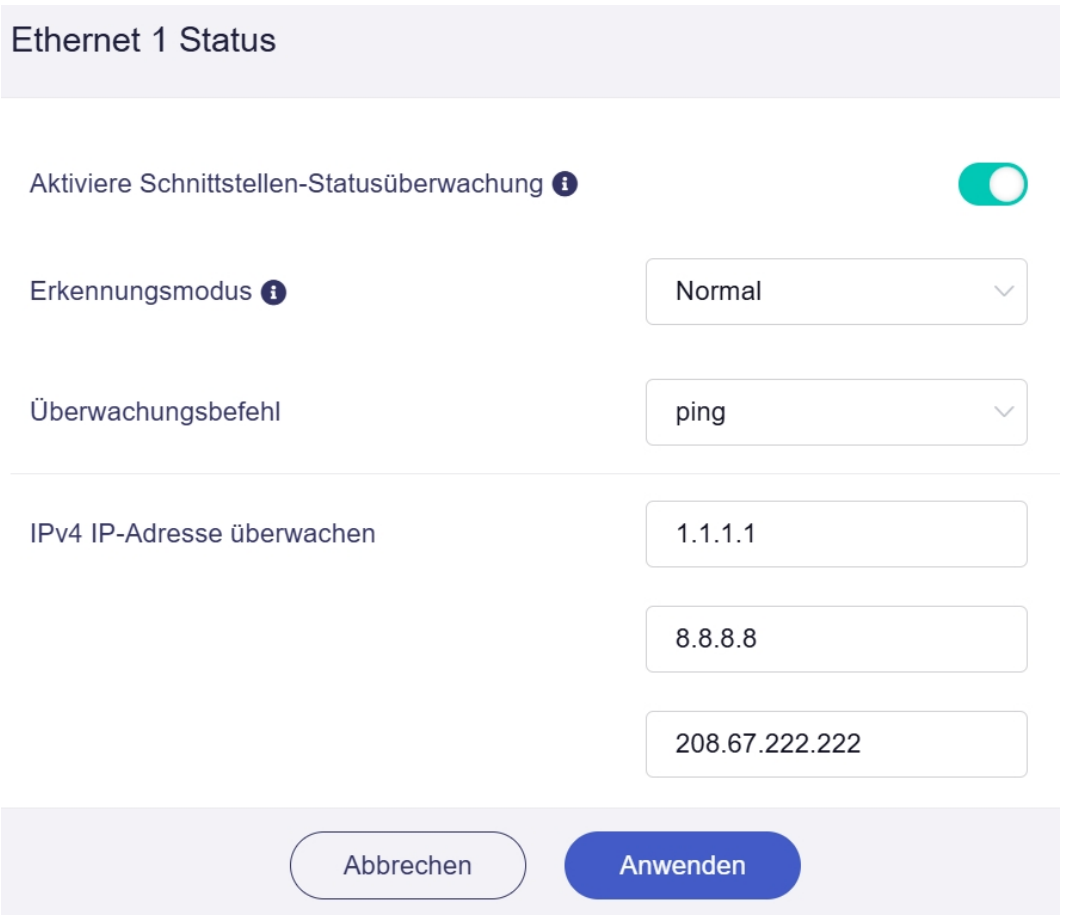
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **Multi WAN**. Diese Seite enthält zwei Abschnitte: Interface Status Track und goodlife12 Multi-WAN-Modus.

9.1.1 Schnittstellen Statusüberwachung

GL.iNet-Router überwachen mit dem Ping-Befehl den Verbindungsstatus zur Ziel-IP und ermitteln, ob die Schnittstelle verfügbar ist. Ist die Schnittstelle verfügbar, wird links ein grüner Punkt angezeigt, ansonsten ist er grau.



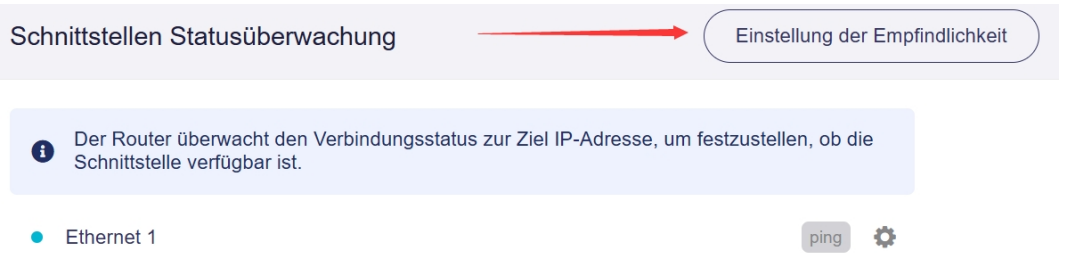
Klicken Sie im Abschnitt Interface Status Track auf das Zahnradsymbol rechts, um auf die Statusverfolgungseinstellungen für jede Netzwerkschnittstelle zuzugreifen.



- **Aktiviere Schnittstellen-Statusüberwachung**: Standardmäßig aktiviert; falls deaktiviert, bestimmt der Router den Schnittstellenstatus basierend auf den physikalischen Bedingungen (z. B. ob das Ethernet-Kabel eingesteckt ist).
- **Erkennungsmodus**: Diese Funktion wurde mit Firmware-Version 4.5 als „Low Data Mode“ eingeführt und mit Firmware-Version 4.7 in „Detection Mode“ umbenannt. Es stehen drei Modi zur Verfügung: „Normal Mode“, „Low Data Mode“ und „Strict Mode“.
  - **Normaler Modus**: Er wird standardmäßig verwendet.
  - **Datenarm:** Er löst nur Tracking aus, wenn ein Netzwerkfehler auf der Netzwerkschnittstelle auftritt. Verwenden Sie diesen Modus, wenn Sie einen begrenzten Datenplan haben. Beachten Sie, dass die Wiederverbindung nach einer Trennung möglicherweise etwas langsamer ist als im Normalmodus und standardmäßig nur für die Mobilfunkschnittstelle aktiviert ist.
  - **Streng**: Er bestimmt den Schnittstellenstatus ausschließlich auf der Grundlage der Ergebnisse eines Erkennungsbefehls, der an eine öffentliche IP gesendet wird.

- **Überwachungsbefehl**: Der Ping-Befehl wird verwendet, um den Verbindungsstatus zur Ziel-IP zu überwachen und die Verfügbarkeit der Schnittstelle zu überprüfen.
- **IPv4 IP-Adresse überwachen**: Passen Sie die IPv4 Track IP-Adressen an, wenn Sie sie benötigen.

Klicken Sie auf **Einstellung der Empfindlichkeit** in der oberen rechten Ecke.



Sie können das Zeitintervall für die Internetstatuserkennung auf Niedrig, Mittel, Hoch einstellen oder es anpassen. Die einstellbare Intervallzeit reicht von 0,5 Sekunden bis 90 Sekunden.



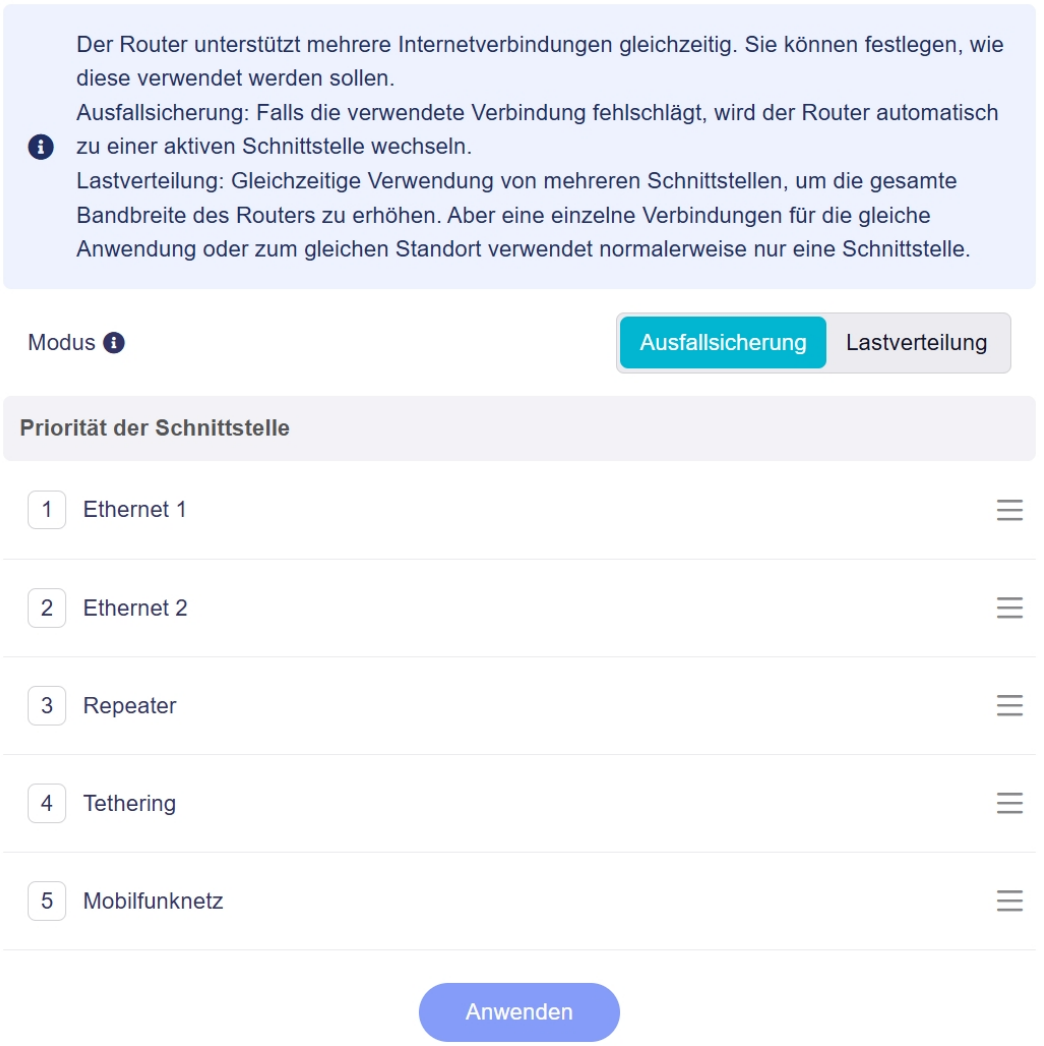
9.1.2 Multi-WAN-Modus

Für Multi-WAN stehen zwei Modi zur Verfügung: Ausfallsicherung und Lastverteilung.

Ausfallsicherung

Ausfallsicherung ist der Standardmodus, wenn mehrere Verbindungen konfiguriert sind. Fällt die aktive Verbindung aus, wechselt der Router automatisch zu einer anderen Netzwerkschnittstelle für den Internetzugang.

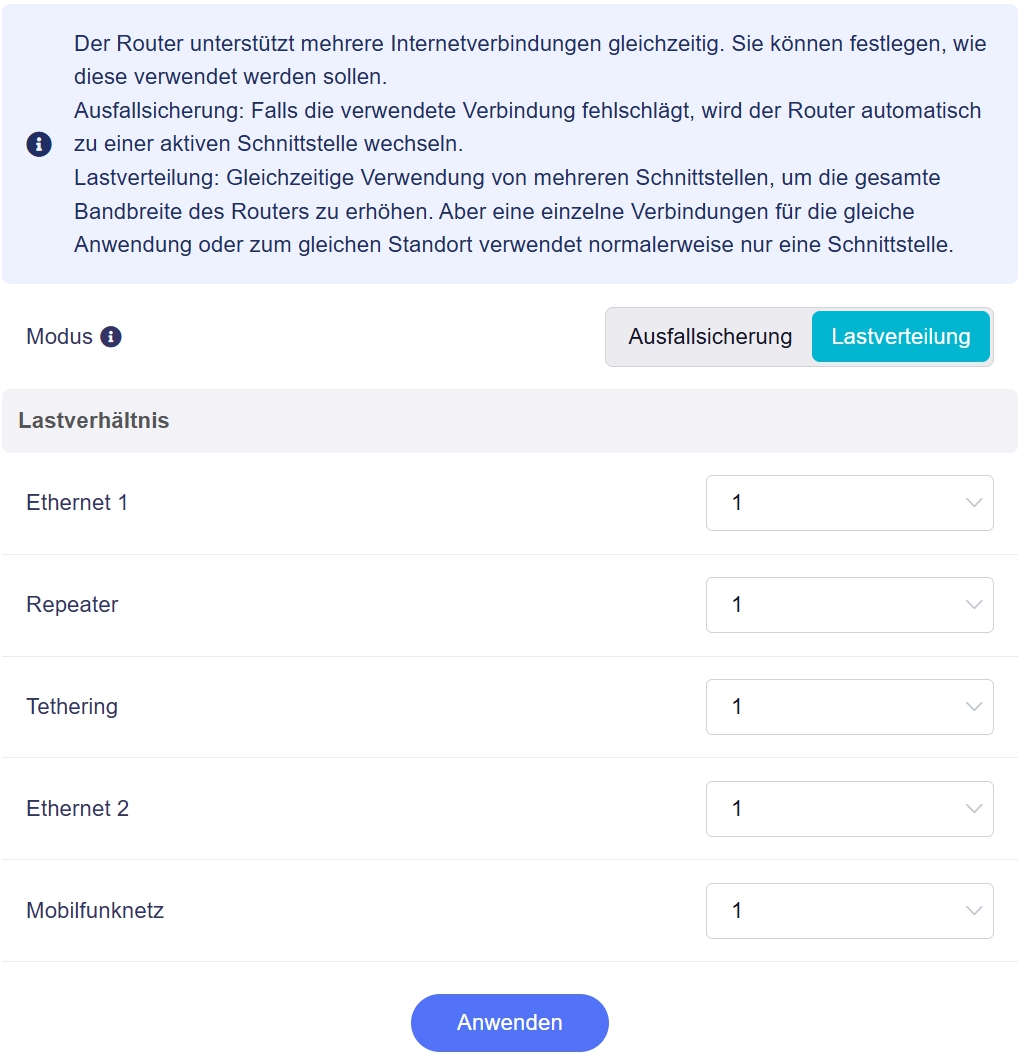
Sie können für jede Schnittstelle Prioritätsstufen festlegen: Wenn die aktuell genutzte Schnittstelle ausfällt, wechselt der Router zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität. Sobald eine höher priorisierte Verbindung wiederhergestellt ist, wechselt der Router automatisch wieder zu ihr.



Lastverteilung

Der Lastverteilung-Modus verwendet mehrere Netzwerkschnittstellen gleichzeitig, um die Gesamtbandbreite des Routers zu erhöhen, wobei das System neue Verbindungen nach einem konfigurierten Lastverhältnis über Schnittstellen verteilt.

Das Lastverhältnis beschreibt das Verhältnis zwischen den einzelnen Netzwerkschnittstellen. Das System ordnet neue Verbindungen anhand dieses konfigurierten Verhältnisses den Schnittstellen zu. Wenn der Router beispielsweise gleichzeitig mit fünf Netzwerken verbunden ist (z. B. Ethernet 1, Repeater, Tethering, Mobilfunknetz und Ethernet 2) und alle Schnittstellen für den Internetzugang verfügbar sind, bedeutet ein Verhältnis von 1:1:1:1:1, dass die fünf Schnittstellen die Netzwerkbandbreite gleichmäßig teilen. Das System verteilt neue Verbindungen entsprechend dem konfigurierten Lastverhältnis auf diese Schnittstellen.



Wenn Ethernet 1 eine Bandbreite von 100 Mbit/s und der Repeater eine Bandbreite von 200 Mbit/s hat und keine anderen Verbindungen aktiv sind, legen Sie die Lastverhältnisse auf 1 für Ethernet 1, 2 für den Repeater und 0 für Tethering, Mobilfunknetz und Ethernet 2 fest. Das System verteilt neue Verbindungen dann gemäß dem Verhältnis 1:2; Ethernet 1 verarbeitet somit halb so viele Verbindungen wie der Repeater. Im Unterschied zum Ausfallsicherung-Modus optimiert dieser Modus den Gesamtdurchsatz durch einen Ausgleich der Verkehrslast über alle verfügbaren Schnittstellen.

Hinweis: Bestehende Verbindungen oder Verkehr sind nicht garantiert, um mit dem Lastverhältnis auszurichten. die tatsächliche Verteilung wird sich allmählich dem konfigurierten Verhältnis mit längerer Nutzung annähern.

9.2 Subnetz

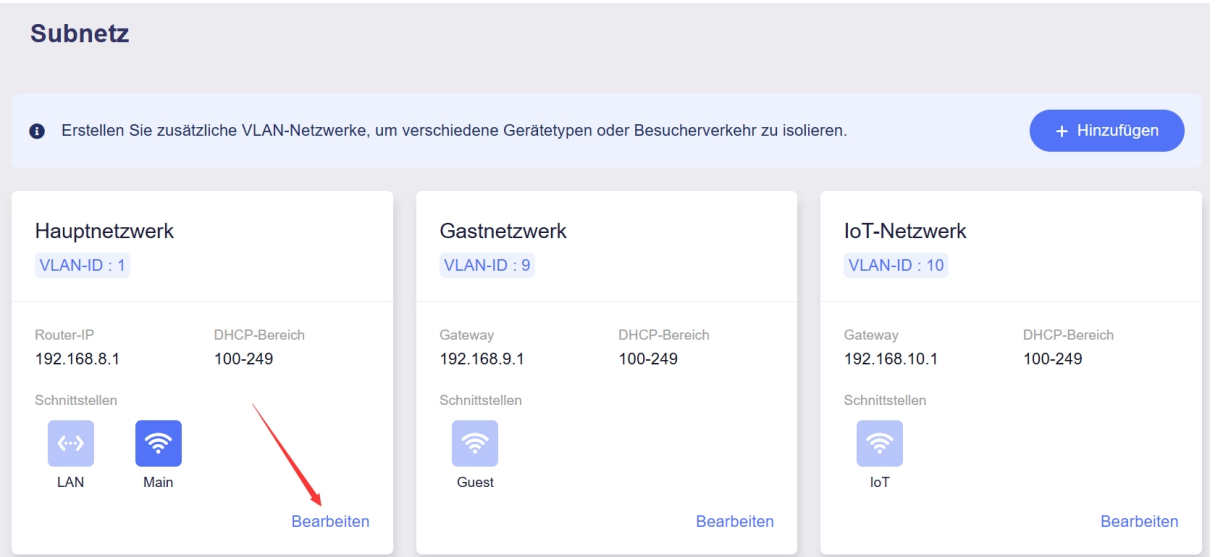
Subnetz bezieht sich auf eine logische Unterteilung eines Netzwerks, die verwendet wird, um Geräte innerhalb verschiedener Netzwerksegmente zu organisieren und zu isolieren.

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **Subnetz**. Hier können Sie Hauptnetzwerk, Gastnetzwerk, IoT-Netzwerk und benutzerdefinierte VLAN-Netzwerke konfigurieren.

9.2.1 Hauptnetzwerk

Das Hauptnetzwerk bezieht sich auf die über Ihr primäres WLAN oder Ethernet hergestellte Verbindung. Es bietet Einblick in alle Schnittstellenzustände, VLAN-ID, Router-IP-Adresse und DHCP-Bereich.

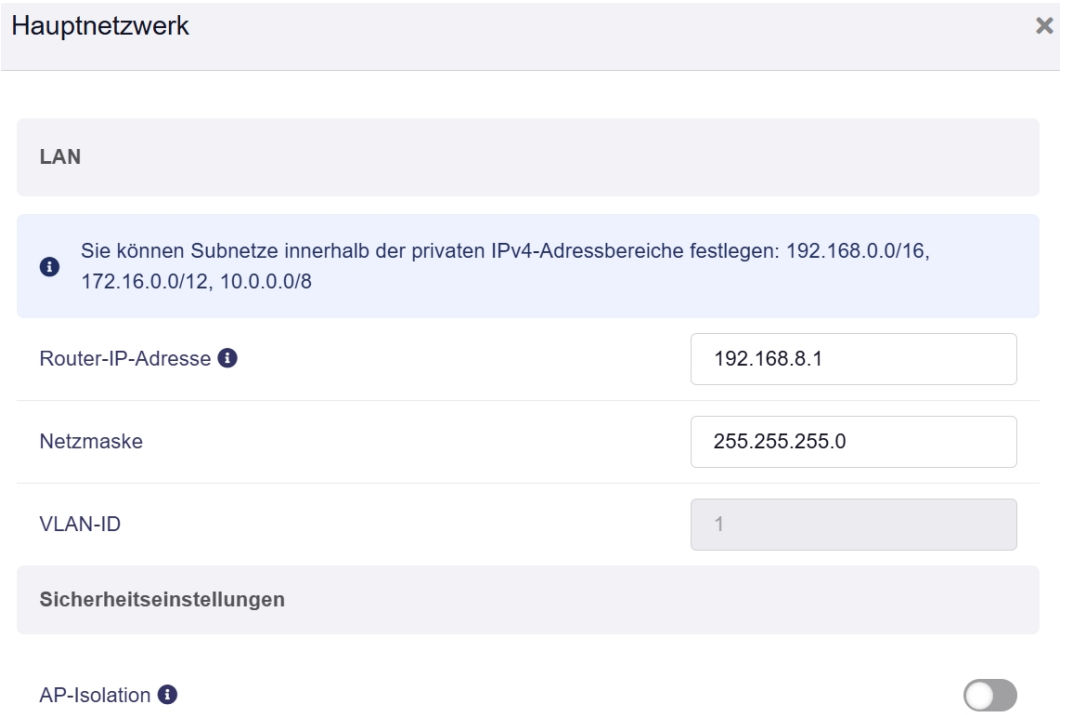
Klicken Sie auf **Bearbeiten** in der unteren rechten Ecke, um das Hauptnetzwerk zu konfigurieren.



Die Konfigurationsseite enthält Grundeinstellungen, DHCP-Server-Einstellungen und Adressreservierung.

Grundeinstellungen

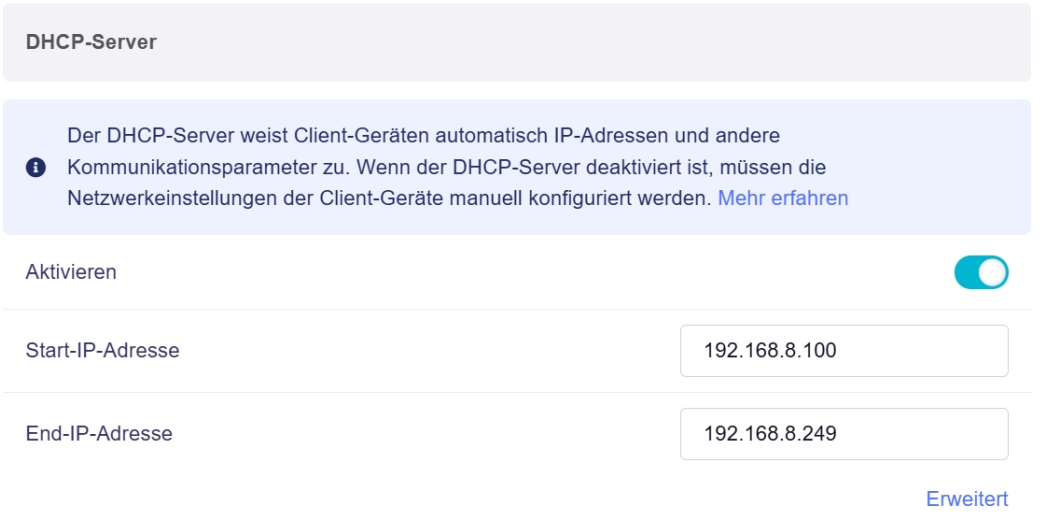
Die Grundeinstellungen umfassen Router IP-Adresse, Netzmaske und VLAN ID. Sie können Subnetz innerhalb der privaten IPv4-Adressbereiche einstellen: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



- **Router-IP-Adresse**: Dies ist die Adresse, die in die Adressleiste eines Browsers eingegeben wird, um auf das Admin-Panel des Routers zuzugreifen. Sie ist standardmäßig 192.168.8.1 und kann geändert werden, wenn sie mit dem vorgelagerten Netzwerk kollidiert.
- **Netzmaske**: Es stehen zwei Optionen zur Verfügung: 255.255.255.0 und 255.255.0.0.
- **VLAN-ID**: Die Standard-VLAN ID des Hauptnetzwerks ist 1, die nicht geändert werden kann.
- **AP-Isolation:** Sie können Client-Geräte in einem separaten Netzwerksegment isolieren, da diese Geräte nicht mit anderen Geräten im selben Netzwerk kommunizieren können.

DHCP-Server

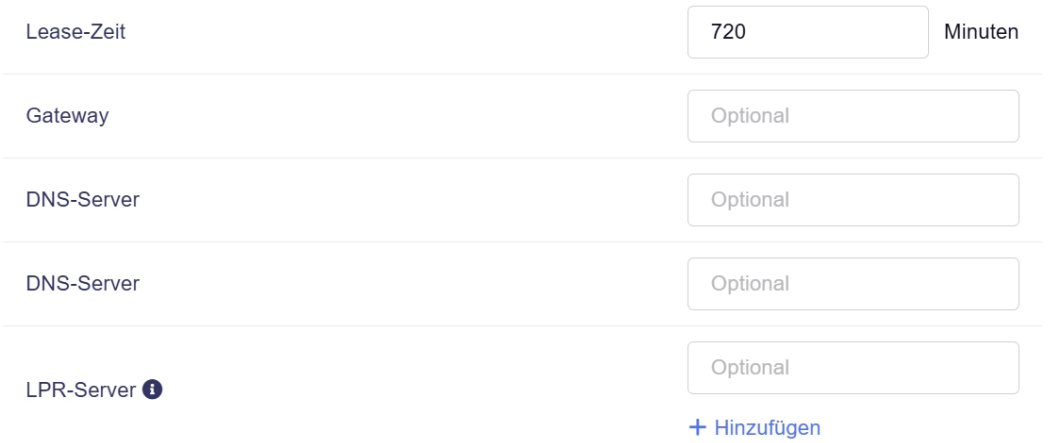
Der DHCP-Server weist jedem angeschlossenen Client automatisch IP-Adressen und andere Kommunikationsparameter zu. Der DHCP-Server des GL.iNet-Routers ist standardmäßig aktiviert, und der IP-Adresspool des DHCP-Servers reicht von 192.168.8.100 bis 192.168.8.249. Sie können den Adressbereich bei Bedarf anpassen.



Klicken Sie auf **Erweitert** in der unteren rechten Ecke.



Sie können erweiterte Einstellungen konfigurieren, einschließlich Lease-Zeit, Gateway, DNS Server und LPR-Server.



- **Lease-Zeit**: Die Dauer, für die ein Gerät eine über DHCP zugewiesene IP-Adresse verwenden kann.
- **Gateway**: Die Routerkomponente, die den Datenverkehr zwischen dem lokalen Netzwerk und externen Netzwerken (z. B. dem Internet) leitet.
- **DNS-Server**: Zwei DNS Server Felder stehen zur Konfiguration des primären und sekundären Resolvers zur Verfügung. Das primäre DNS wird im oberen Feld und das sekundäre im unteren Feld eingegeben. Im Falle der Nichtverfügbarkeit des primären Servers werden Client-Geräte automatisch auf den sekundären Resolver ausfallen, wodurch die Kontinuität der Domainnamenauflösung gewährleistet wird.
- **LPR-Server** (Line Printer Remote Server): Ein Dienst, der Druckaufträge verwaltet und es vernetzten Geräten ermöglicht, Druckanforderungen an entfernte Drucker zu senden.

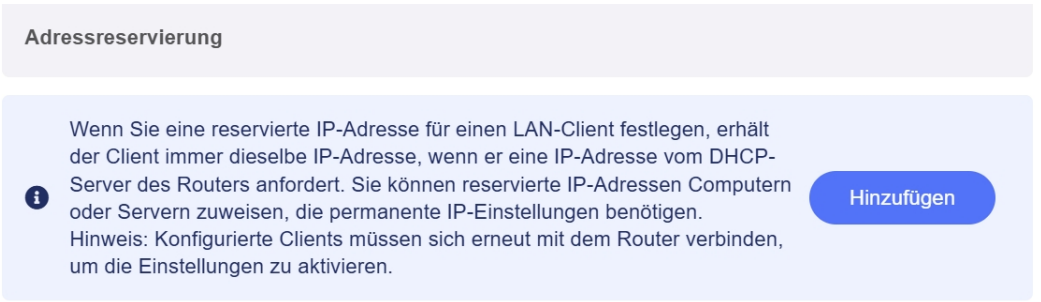
Hinweis: Wenn der DHCP-Server deaktiviert ist, müssen Sie statische IP- und andere Kommunikationsparameter manuell für jeden Client konfigurieren.

Adressreservierung

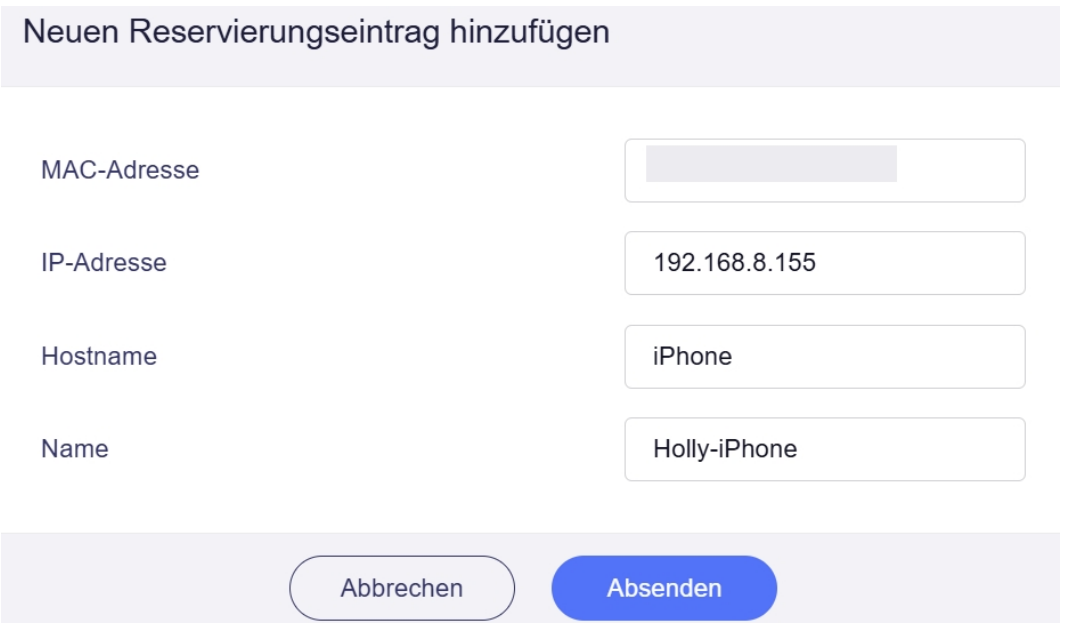
Adressreservierung ermöglicht es Ihnen, eine feste IP-Adresse für einen LAN-Client anzugeben, so dass der Client immer die gleiche IP-Adresse erhält, wenn er auf den DHCP-Server des Routers zugreift. Sie können reservierte IP-Adressen Computern oder Servern zuweisen, die permanente IP-Einstellungen erfordern. Beachten Sie, dass Clients mit konfigurierter Adressreservierung sich wieder mit dem Router verbinden müssen, um die Einstellung zu aktivieren.

Folgen Sie den Schritten unten, um die Adressreservierung bei Bedarf zu konfigurieren.

1. Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Subnetz** > **Hauptnetzwerk** > **Adressreservierung** und klicken Sie auf **Hinzufügen**.



2. Wählen Sie im Popup-Fenster die MAC-Adresse aus der Dropdown-Liste aus, dann wird die entsprechende IP-Adresse für den ausgewählten MAC automatisch ausgefüllt. Geben Sie einen Hostnamen und einen benutzerdefinierten Namen zur einfachen Identifizierung ein.



3. Nach dem Hinzufügen einer neuen IP-Adressreservierung wird auf der Seite der reservierte Eintrag angezeigt, wie unten gezeigt.

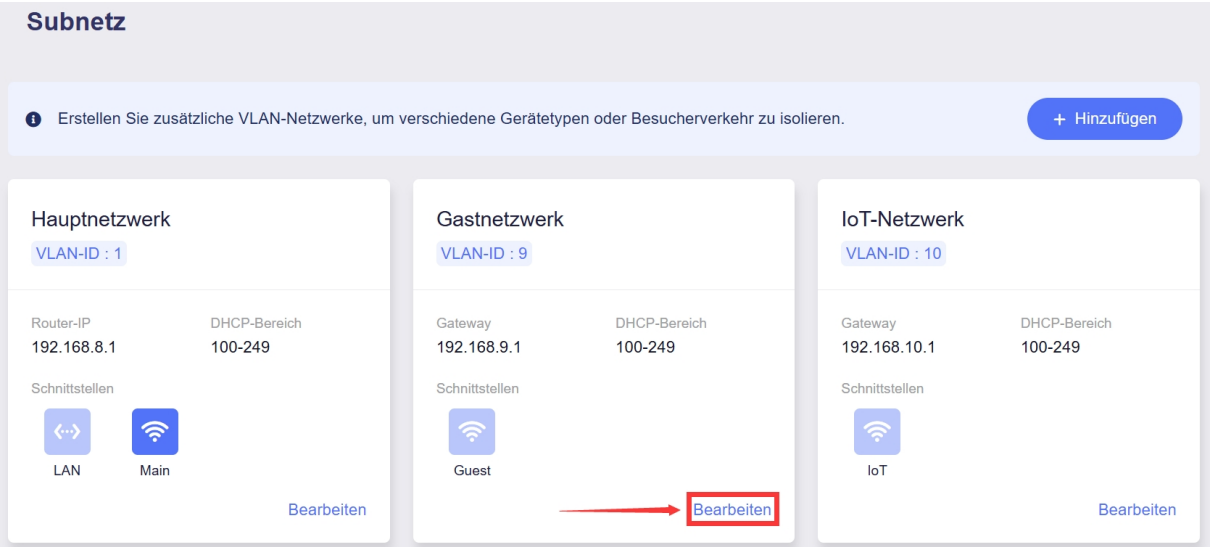


9.2.2 Gastnetzwerk

Gastnetzwerk bezieht sich auf ein dediziertes Netzwerk für Besucher, mit dem sie sich verbinden können, und isoliert sie von Ihrem Haupt-LAN, um die Sicherheit Ihres privaten Netzwerks zu schützen.

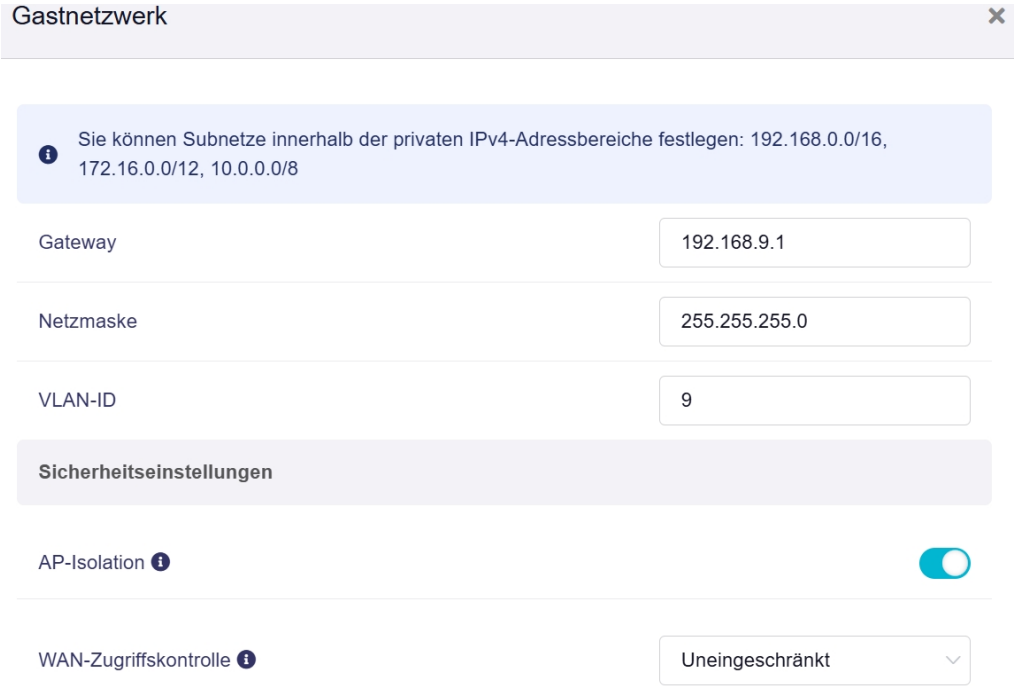
Melden Sie sich im Web-Admin-Panel Ihres Routers an und gehen Sie zu **Netzwerk** > **Subnetz** > **Gastnetzwerk**. Diese Seite ermöglicht es Ihnen, die Gastnetzwerk-Einstellungen einschließlich der Grundeinstellungen und des DHCP-Servers zu konfigurieren.

Klicken Sie unten rechts auf Bearbeiten, um das Gastnetzwerk zu konfigurieren.



Grundeinstellungen

Die Grundeinstellungen umfassen Gateway, Netzmaske, AP-Isolation, VLAN-ID und WAN-Zugriffskontrolle .

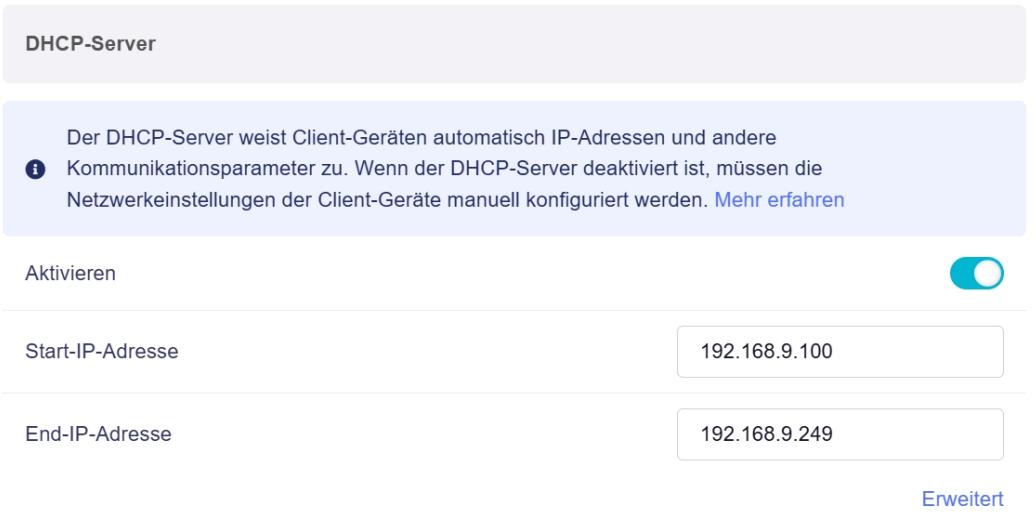


- **Gateway:** Es ist standardmäßig 192.168.9.1 und kann bei Bedarf geändert werden, darf jedoch nicht mit dem Gateway des Hauptnetzwerks in Konflikt stehen.
- **Netzmaske:** Es stehen zwei Optionen zur Verfügung: 255.255.255.0 und 255.255.0.0.
- **VAN-ID:** Die standardmäßige VLAN ID des Gastnetzwerks ist 9, die bei Bedarf geändert werden kann.
- **AP-Isolation:** Es wird verwendet, um Gastnetzwerk-Clients in separate Segmente zu isolieren, so dass sie nicht mit anderen Geräten im selben Netzwerk kommunizieren können.
- **WAN-Zugriffskontrolle**: WAN-Zugriffskontrolle verwaltet den lokalen Subnetzzugang zu WAN-seitigen Netzwerken, einschließlich des Internets und anderer WAN-Subnetze.
  Es stehen drei WAN-Zugriffskontrollmodi zur Verfügung:
  - **Uneingeschränkt**: Ermöglicht diesem Subnetz den Zugriff auf das Internet und andere WAN-seitige Subnetze ohne Einschränkungen.
  - **WAN-Subnetz blockieren**: Blockiert den Zugriff auf andere WAN-seitige Subnetze. Internetzugang bleibt verfügbar.
  - **Internetzugriff blockierenl**: Blockiert alle ausgehenden Zugriffe, einschließlich des Internets und der WAN-seitigen Subnetze.

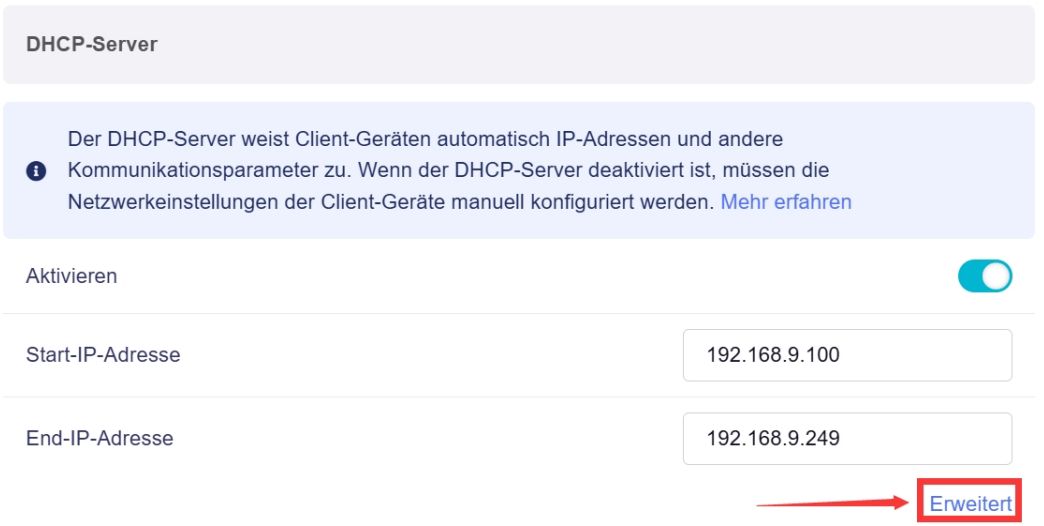
DHCP-Server

Da das Gastnetzwerk standardmäßig deaktiviert ist, ist der DHCP-Server deaktiviert und ausgeblendet, bis er manuell aktiviert ist.

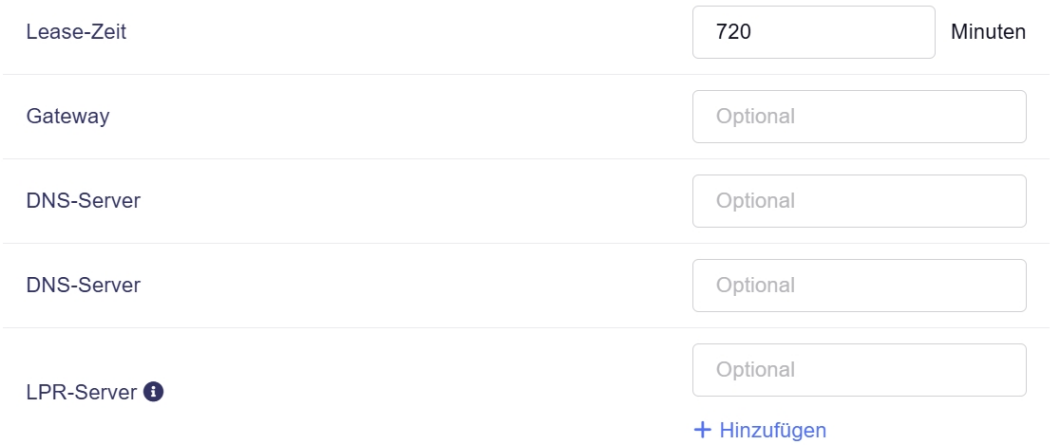
Wenn aktiviert, weist der DHCP-Server automatisch IP-Adressen und andere Kommunikationsparameter jedem angeschlossenen Client zu. Der IP-Adresspool des DHCP-Servers für das Gastnetzwerk reicht von 192.168.9.100 bis 192.168.9.249. Sie können den Adressbereich bei Bedarf anpassen.



Klicken Sie auf **Erweitert** in der unteren rechten Ecke.



Sie können erweiterte Einstellungen konfigurieren, einschließlich Lease-Zeit, Gateway, DNS-Server und LPR-Server.



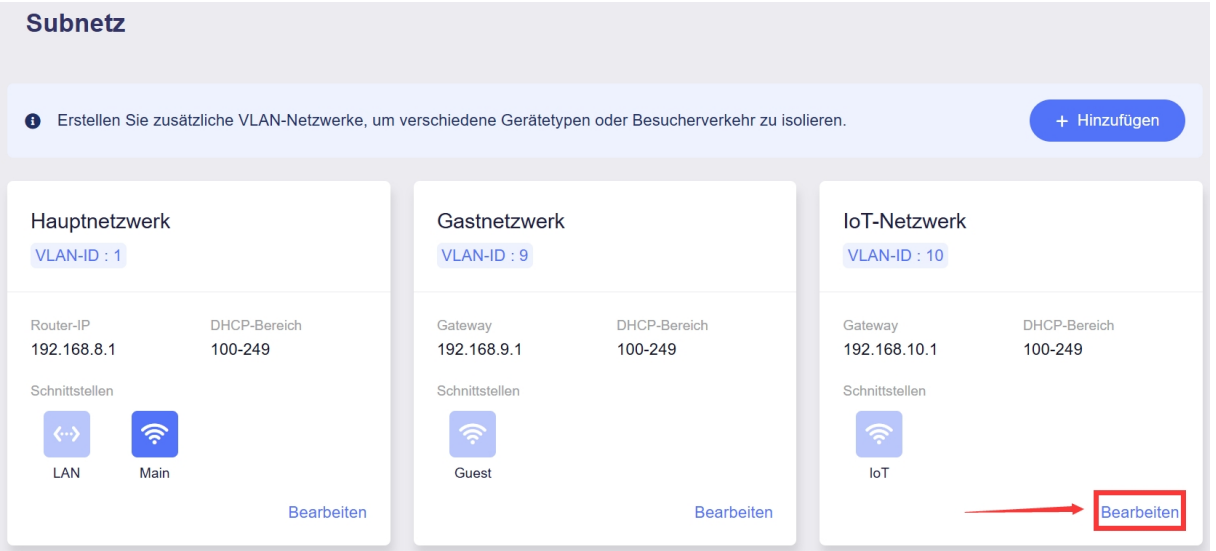
- **Lease-Zeit**: Die Dauer, für die ein Gerät eine IP-Adresse verwenden kann, die über die DHCP des Gastnetzwerks zugewiesen wird.
- **Gateway**: Die Routerkomponente, die den Datenverkehr zwischen dem Gastnetzwerk und externen Netzwerken (z. B. dem Internet) weiterleitet.
- **DNS-Server**: Zwei DNS Server Felder stehen zur Konfiguration des primären und sekundären Resolvers zur Verfügung. Das primäre DNS wird im oberen Feld und das sekundäre im unteren Feld eingegeben. Im Falle der Nichtverfügbarkeit des primären Servers werden Client-Geräte automatisch auf den sekundären Resolver ausfallen, wodurch die Kontinuität der Domainnamenauflösung gewährleistet wird.
- **LPR-Server** (Line Printer Remote Server): Ein Dienst, der Druckaufträge verwaltet und es vernetzten Geräten ermöglicht, Druckanforderungen an entfernte Drucker zu senden.

9.2.3 IoT-Netzwerk

IoT-Network erstellt ein dediziertes Wi-Fi-Netzwerk für IoT-Geräte. Vom primären Netzwerk isoliert, bietet es eine bessere Kompatibilität und verbesserte Sicherheit. Sie können direkt den Schnittstellenstatus, die VLAN-ID, das Gateway und die DHCP-Reichweite anzeigen.

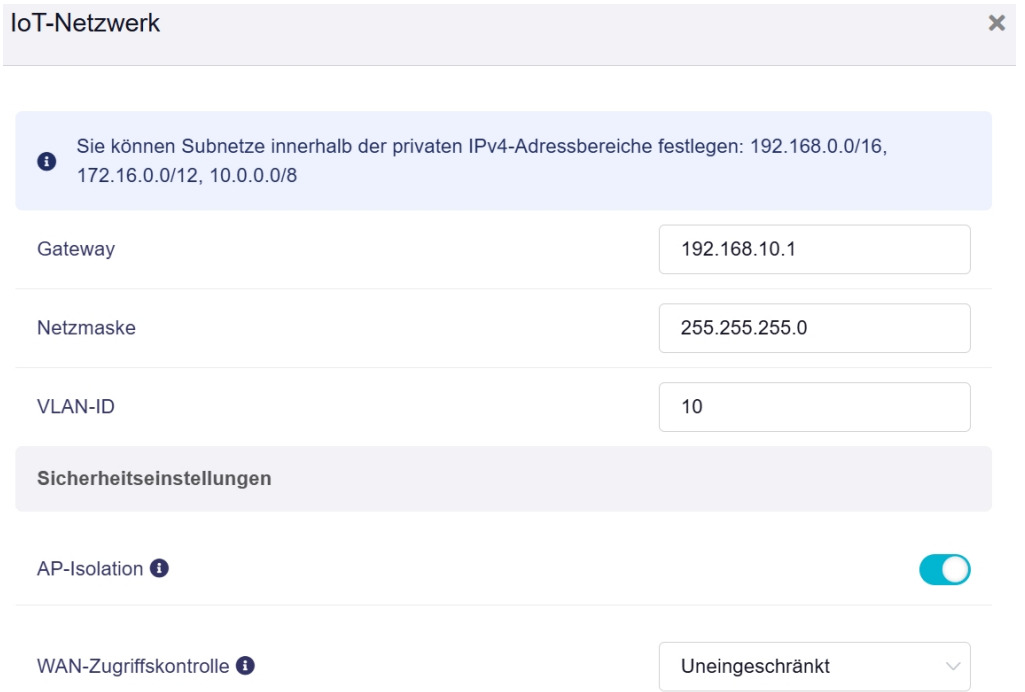
Melden Sie sich im Web-Admin-Panel Ihres Routers an und gehen Sie zum Abschnitt **Netzwerk** > **Subnetz**> **IoT-Netzwerk**. Diese Seite ermöglicht es Ihnen, IoT-Netzwerk-Einstellungen zu konfigurieren, einschließlich grundlegender Einstellungen und DHCP-Server.

Klicken Sie unten rechts auf Bearbeiten, um das Gastnetzwerk zu konfigurieren.



Grundeinstellungen

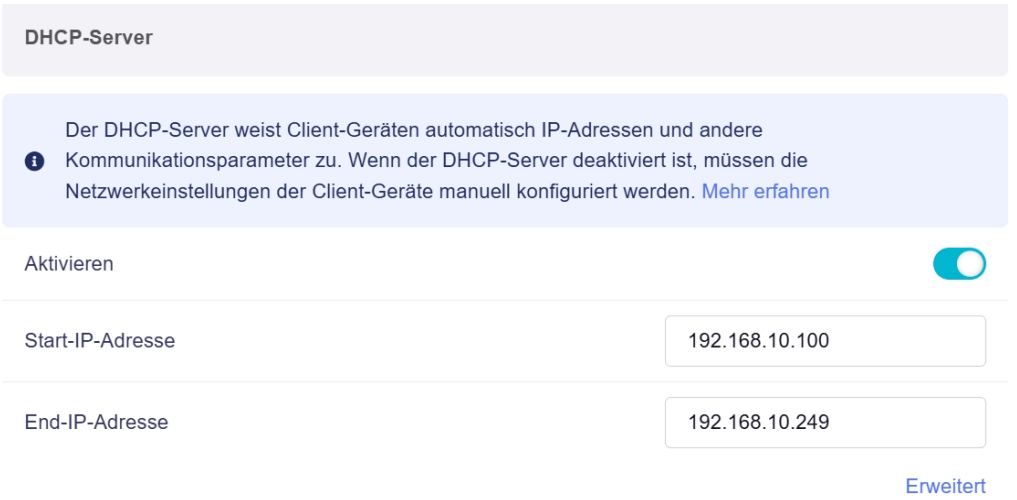
Die Grundeinstellungen umfassen Gateway, Netzmaske, AP-Isolation, VLAN-ID und WAN-Zugriffskontrolle.



- **Gateway:** Es ist standardmäßig 192.168.10.1 und kann bei Bedarf geändert werden, darf jedoch nicht mit dem Gateway des Hauptnetzwerks in Konflikt stehen.
- **Netzmaske**: Es stehen zwei Optionen zur Verfügung: 255.255.255.0 und 255.255.0.0.
- **VAN-ID:** Die Standard-VLAN ID des Gastnetzwerks ist 10, die bei Bedarf geändert werden kann.
- **AP-Isolation**: Es wird verwendet, um Gastnetzwerk-Clients in separate Segmente zu isolieren, so dass sie nicht mit anderen Geräten im selben Netzwerk kommunizieren können.
- **WAN-Zugriffskontrolle**: WAN-Zugriffskontrolle verwaltet den lokalen Subnetzzugang zu WAN-seitigen Netzwerken, einschließlich des Internets und anderer WAN-Subnetze.
  Es stehen drei WAN-Zugriffskontrollmodi zur Verfügung:
  - **Uneingeschränkt**: Ermöglicht diesem Subnetz den Zugriff auf das Internet und andere WAN-seitige Subnetze ohne Einschränkungen.
  - **WAN-Subnetz blockieren**: Blockiert den Zugriff auf andere WAN-seitige Subnetze. Internetzugang bleibt verfügbar.
  - **Internetzugriff blockieren**: Blockiert alle ausgehenden Zugriffe, einschließlich des Internets und der WAN-seitigen Subnetze.

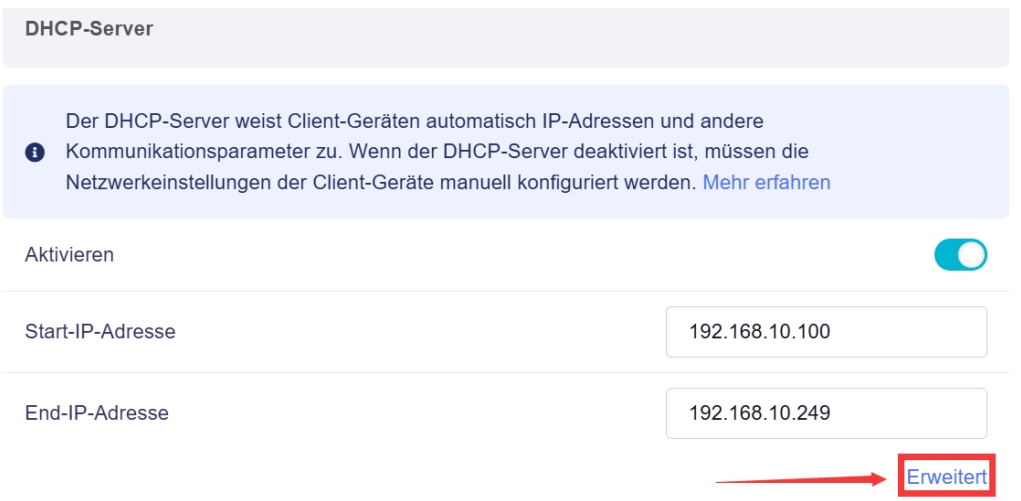
DHCP-Server

Da das IoT-Netzwerk standardmäßig deaktiviert ist, ist der DHCP-Server deaktiviert und ausgeblendet, bis er manuell aktiviert ist.

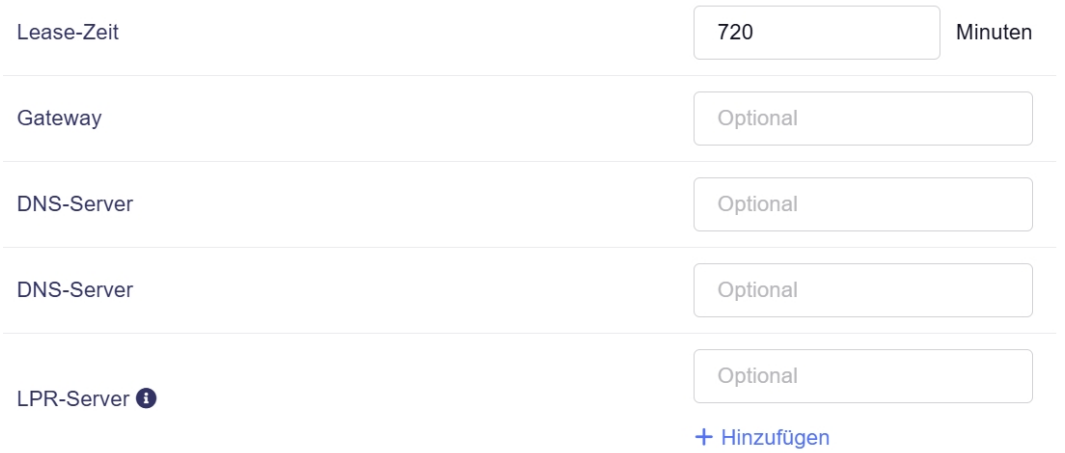


Wenn aktiviert, weist der DHCP-Server automatisch IP-Adressen und andere Kommunikationsparameter jedem angeschlossenen Client zu. Der IP-Adresspool des DHCP-Servers für das IoT-Netzwerk reicht von 192.168.10.100 bis 192.168.10.249. Sie können den Adressbereich bei Bedarf anpassen.

Klicken Sie auf **Erweitert** in der unteren rechten Ecke.



Sie können erweiterte Einstellungen konfigurieren, einschließlich Lease-Zeit, Gateway, DNS Server und LPR-Server.

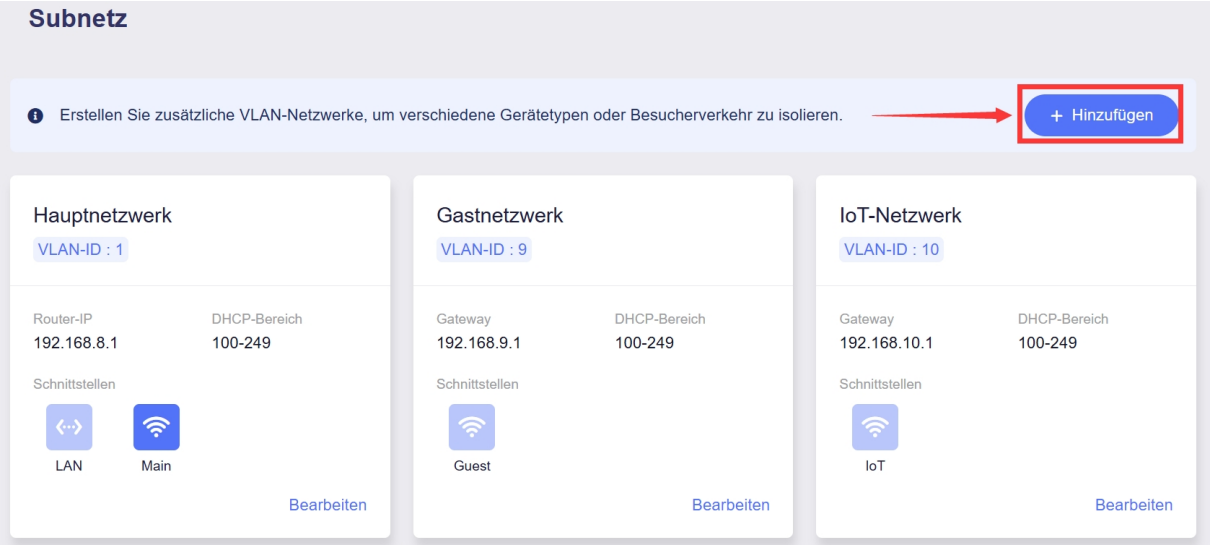


- **Lease-Zeit**: Die Dauer, für die ein Gerät eine IP-Adresse verwenden kann, die über die DHCP des Gastnetzwerks zugewiesen wird.
- **Gateway**: Die Routerkomponente, die den Datenverkehr zwischen dem Gastnetzwerk und externen Netzwerken (z. B. dem Internet) weiterleitet.
- **DNS-Server**: Zwei DNS Server Felder stehen zur Konfiguration des primären und sekundären Resolvers zur Verfügung. Das primäre DNS wird im oberen Feld und das sekundäre im unteren Feld eingegeben. Im Falle der Nichtverfügbarkeit des primären Servers werden Client-Geräte automatisch auf den sekundären Resolver ausfallen, wodurch die Kontinuität der Domainnamenauflösung gewährleistet wird.
- **LPR-Server** (Line Printer Remote Server): Ein Dienst, der Druckaufträge verwaltet und es vernetzten Geräten ermöglicht, Druckanforderungen an entfernte Drucker zu senden.

9.2.4 VLAN-Netze

VLAN Networks ermöglicht die Erstellung zusätzlicher VLAN-Netzwerke, um bei Bedarf verschiedene Gerätetypen oder Besucherdaten zu isolieren.

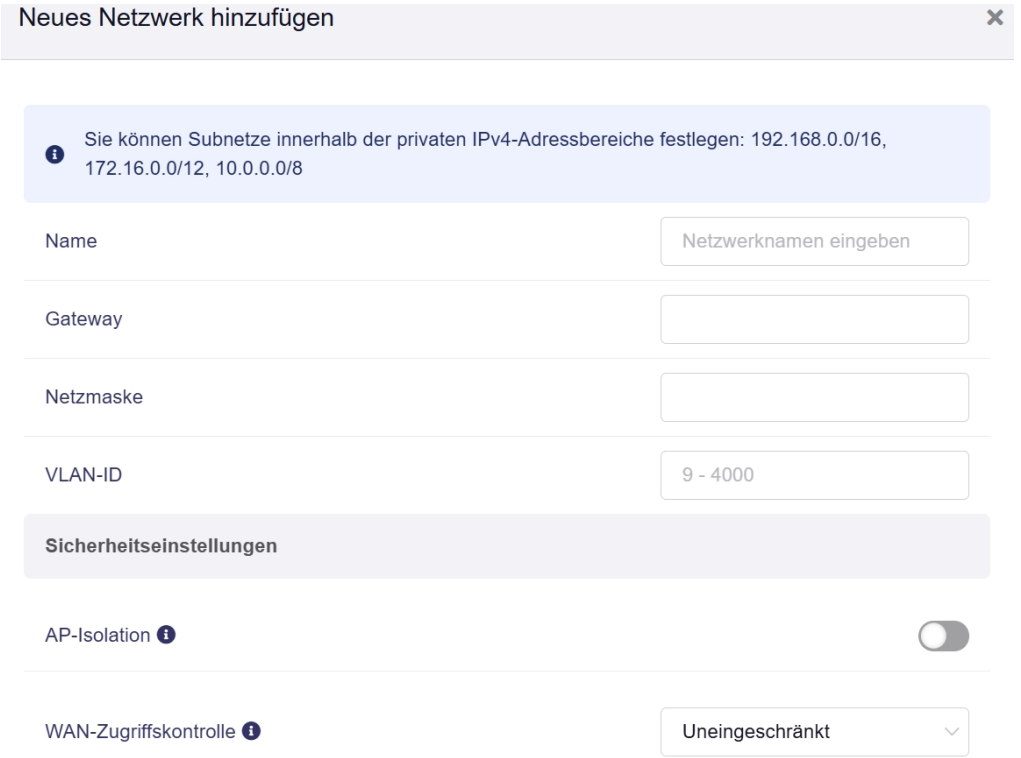
Klicken Sie auf die **+ Hinzufügen** e auf der rechten Seite der Seite, um ein neues Netzwerk zu konfigurieren.



Auf dieser Seite können Sie die Einstellungen von VLAN Networks konfigurieren, einschließlich der Grundeinstellungen und des DHCP-Servers.

Grundeinstellungen

Sie können die grundlegenden VLAN-Netzwerkinformationen auf dieser Seite konfigurieren.

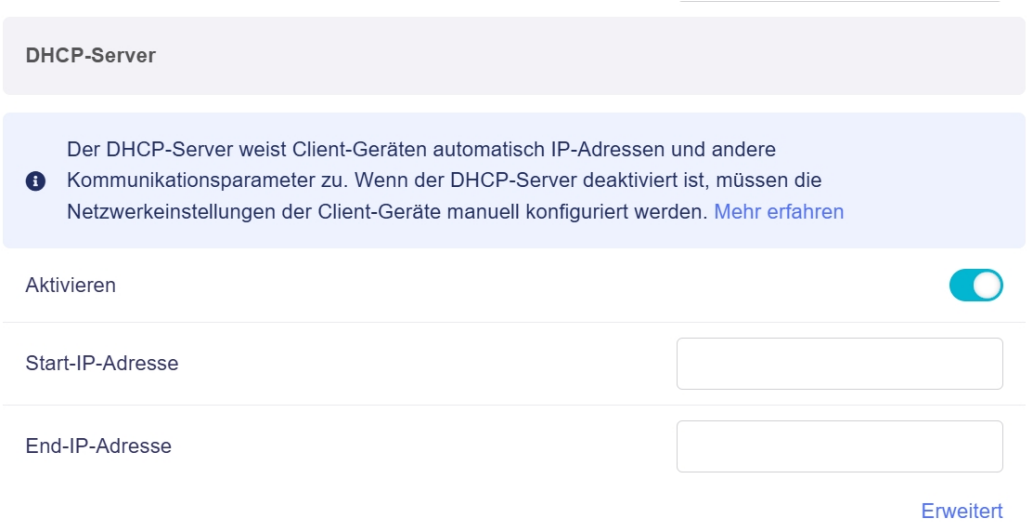


- **Name*:*** Passen Sie einen Namen für Ihr neu erstelltes Subnetz zur Identifizierung an.
- **Gateway**: Es ist standardmäßig 192.168.10.1 und kann bei Bedarf geändert werden, darf jedoch nicht mit dem Gateway des Hauptnetzwerks in Konflikt stehen.
- **Netzmaske**: Es stehen zwei Optionen zur Verfügung: 255.255.255.0 und 255.255.0.0.
- **VAN-ID:** Beim Erstellen eines Subnetzes müssen Sie eine VLAN ID zwischen 9 und 4000 zuweisen.
- **AP-Isolation**: Es wird verwendet, um Gastnetzwerk-Clients in separate Segmente zu isolieren, so dass sie nicht mit anderen Geräten im selben Netzwerk kommunizieren können.
- **WAN-Zugriffskontrolle**: WAN-Zugriffskontrolle verwaltet den lokalen Subnetzzugang zu WAN-seitigen Netzwerken, einschließlich des Internets und anderer WAN-Subnetze.
  Es stehen drei WAN-Zugriffskontrollmodi zur Verfügung:
  - **Unbeschränkt**: Ermöglicht diesem Subnetz den Zugriff auf das Internet und andere WAN-seitige Subnetze ohne Einschränkungen.
  - **WAN-Subnetz blockieren**: Blockiert den Zugriff auf andere WAN-seitige Subnetze. Internetzugang bleibt verfügbar.

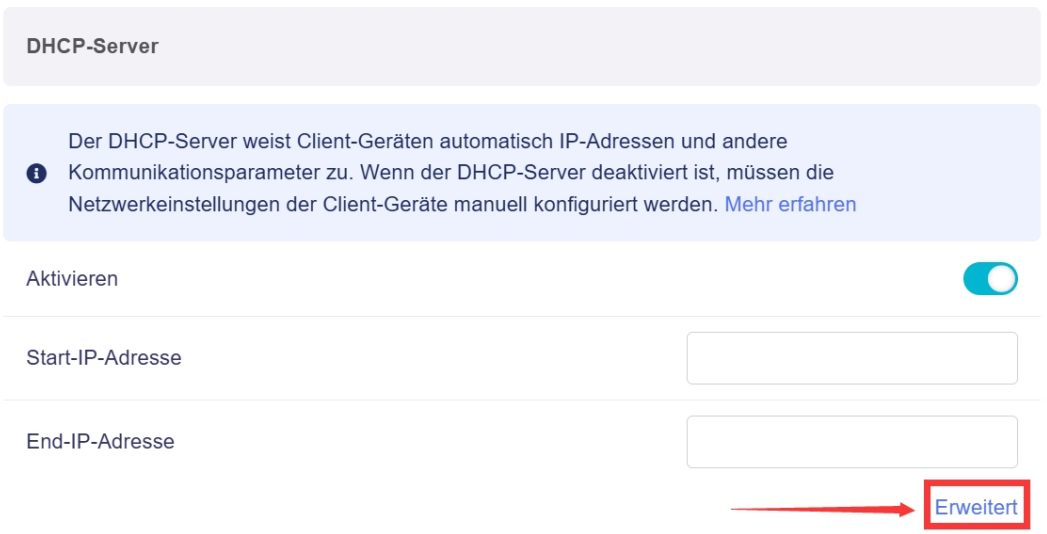
- **Internetzugang blockieren**: Blockiert alle ausgehenden Zugriffe, einschließlich des Internets und der WAN-seitigen Subnetze.

DHCP-Server

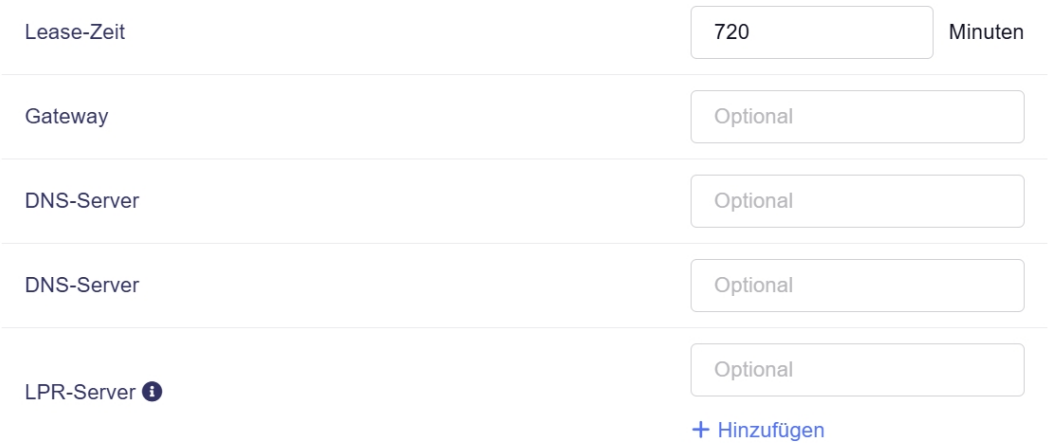
Wenn aktiviert, weist der DHCP-Server automatisch IP-Adressen und andere Kommunikationsparameter jedem angeschlossenen Client zu.



Klicken Sie auf **Erweitert** für weitere Konfiguration, falls erforderlich.



Sie können erweiterte Einstellungen konfigurieren, einschließlich Lease-Zeit, Gateway, DNS-Server und LPR-Server.



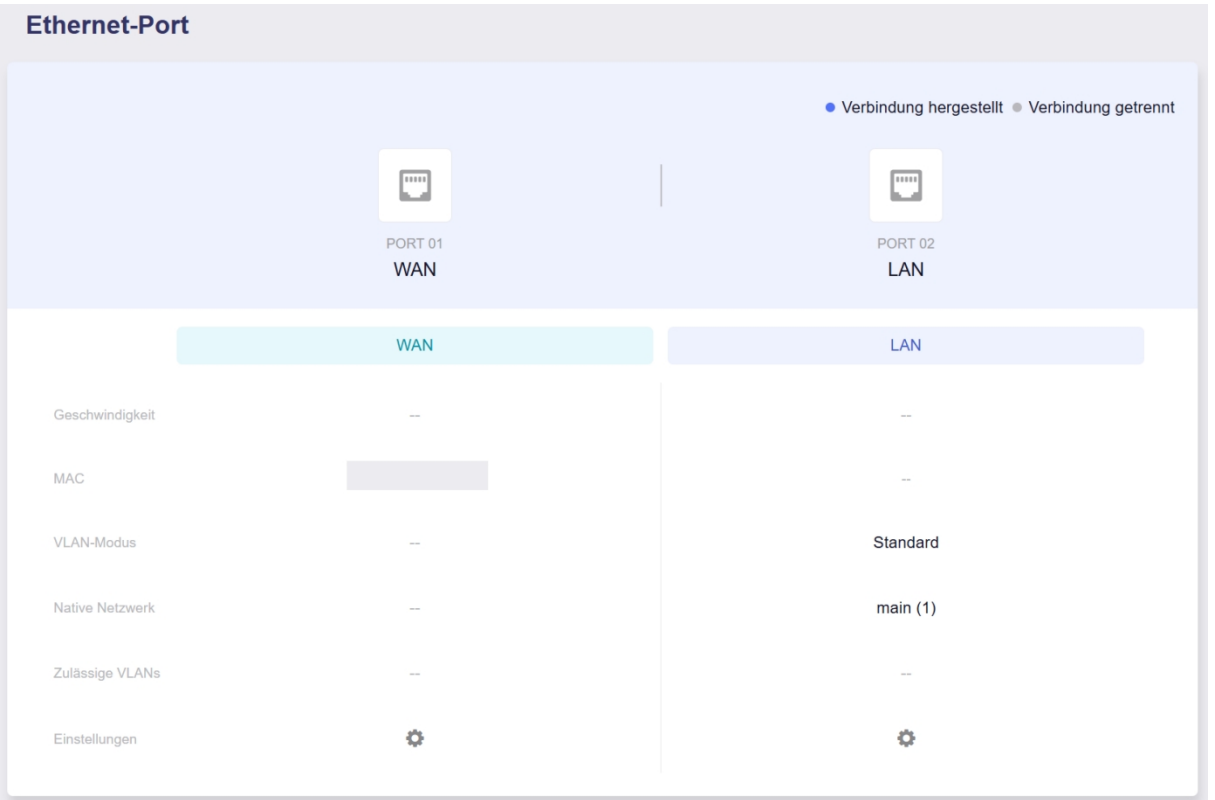
- **Lease-Zeit**: Die Dauer, für die ein Gerät eine IP-Adresse verwenden kann, die über die DHCP des Gastnetzwerks zugewiesen wird.
- **Gateway**: Die Routerkomponente, die den Datenverkehr zwischen dem Gastnetzwerk und externen Netzwerken (z. B. dem Internet) weiterleitet.
- **DNS-Server**: Zwei DNS Server Felder stehen zur Konfiguration des primären und sekundären Resolvers zur Verfügung. Das primäre DNS wird im oberen Feld und das sekundäre im unteren Feld eingegeben. Im Falle der Nichtverfügbarkeit des primären Servers werden Client-Geräte automatisch auf den sekundären Resolver ausfallen, wodurch die Kontinuität der Domainnamenauflösung gewährleistet wird.
- **LPR-Server** (Line Printer Remote Server): Ein Dienst, der Druckaufträge verwaltet und es vernetzten Geräten ermöglicht, Druckanforderungen an entfernte Drucker zu senden.

Nach der Konfiguration können Sie sehen, dass das neue VLAN-Netzwerk auf der aktuellen Seite erscheint und die Subnetzinformationen anzeigt.

9.3 Ethernet-Port

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **Ethernet-Port**. Diese Seite ermöglicht es Ihnen, die Ethernet-Ports des Routers zu verwalten.

Ethernet-Port-Seite zeigt alle Router-Schnittstellen an. Sie können den Verbindungsstatus jeder Schnittstelle anzeigen, Ethernet-Portrollen (WAN oder LAN) verwalten und Portdetails wie MAC-Adresse, ausgehandelte Geschwindigkeit und aktuellen Linkstatus anzeigen. Darüber hinaus können Sie physische Schnittstellen zu allen von Ihnen erstellten Subnetzen zuweisen.

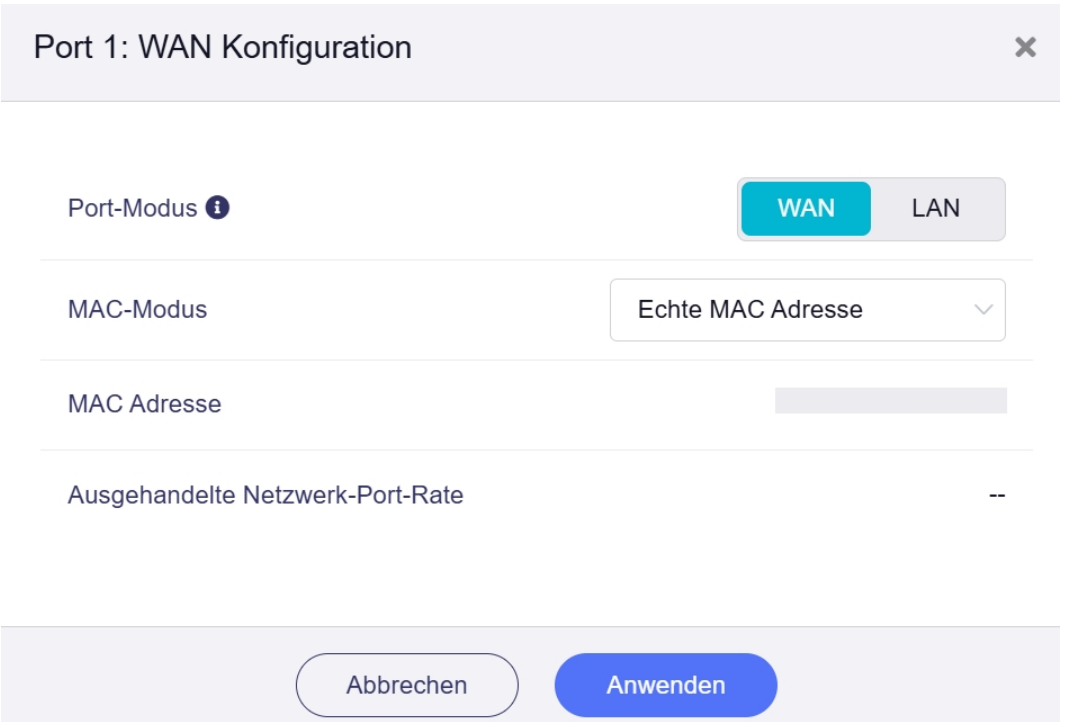


- **Verbindung hergestellt**: Wenn das Port-Icon blau hervorgehoben ist, ist der physische Link aktiv.
- **Verbindung getrennt**: Wenn das Port-Icon grau ist, ist der physische Link inaktiv.
- **Geschwindigkeit**: Verhandelte Übertragungsrate des Ethernet-Ports.
- **MAC:** MAC-Adresse des Ports.
- **VLAN-Modus**: Der Arbeitsmodus von LAN-Ports kann entweder auf den Standard- oder den Multiple-VLAN-Modus eingestellt werden.

- **Native Netzwerk:** Standardmäßig untaggtes Subnetz, das dem LAN-Port zugewiesen ist.
- **Zulässige VLANs**: Gibt markierte VLANs an, die diesen Port im Modus für mehrere VLANs passieren dürfen.
- **Einstellungen**: Klicken Sie, um auf die Konfigurationsseite für jeden einzelnen Port zuzugreifen.

9.3.1 WAN

Im WAN-Bereich werden die Portrolle (WAN oder LAN), die MAC-Adresse und die Verhandlungsrate angezeigt.

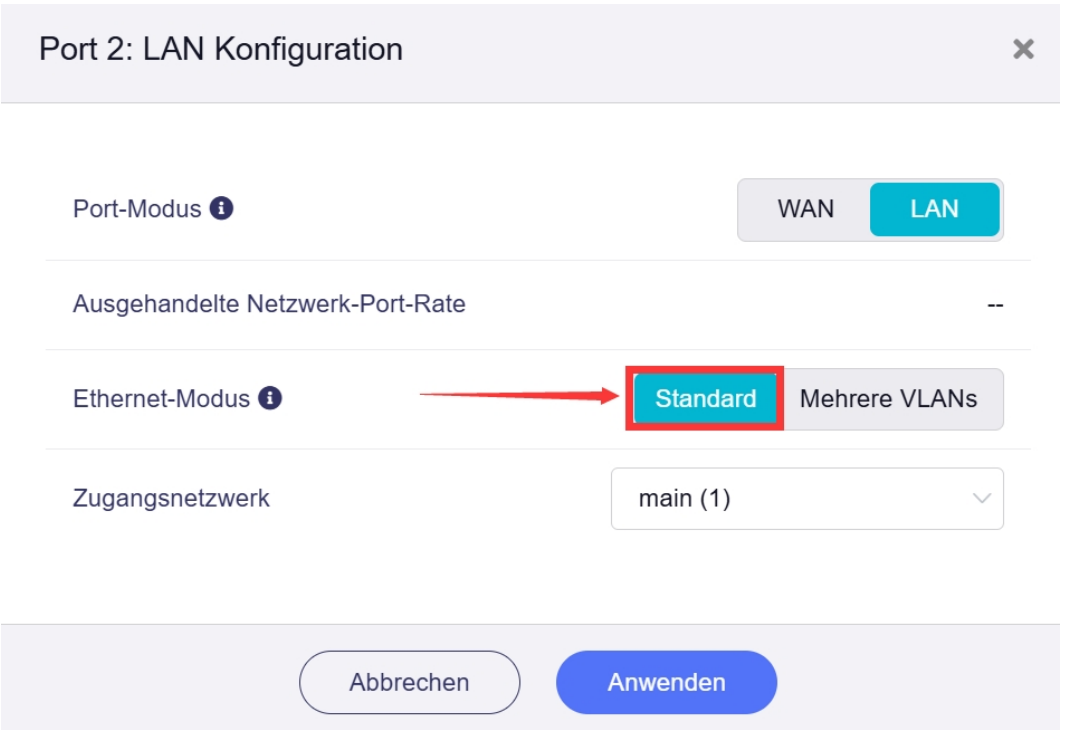


- **Port-Modus**: Der aktuelle Betriebsmodus des physischen WAN-Ports. Sie können ihn bei Bedarf auf LAN einstellen.
- **MAC-Modus**: Standardmäßig im Werksmodus. Sie können ihn in Klonmodus oder Zufallsmodus umschalten.
- **MAC Adresse**: Die MAC Adresse der WAN-Schnittstelle.
- **Ausgehandelte Netzwerk-Port-Rate**: Die ausgehandelte Linkgeschwindigkeit der WAN-Schnittstelle, die nur angezeigt wird, wenn eine gültige Verbindung erkannt wird.

9.3.2 LAN

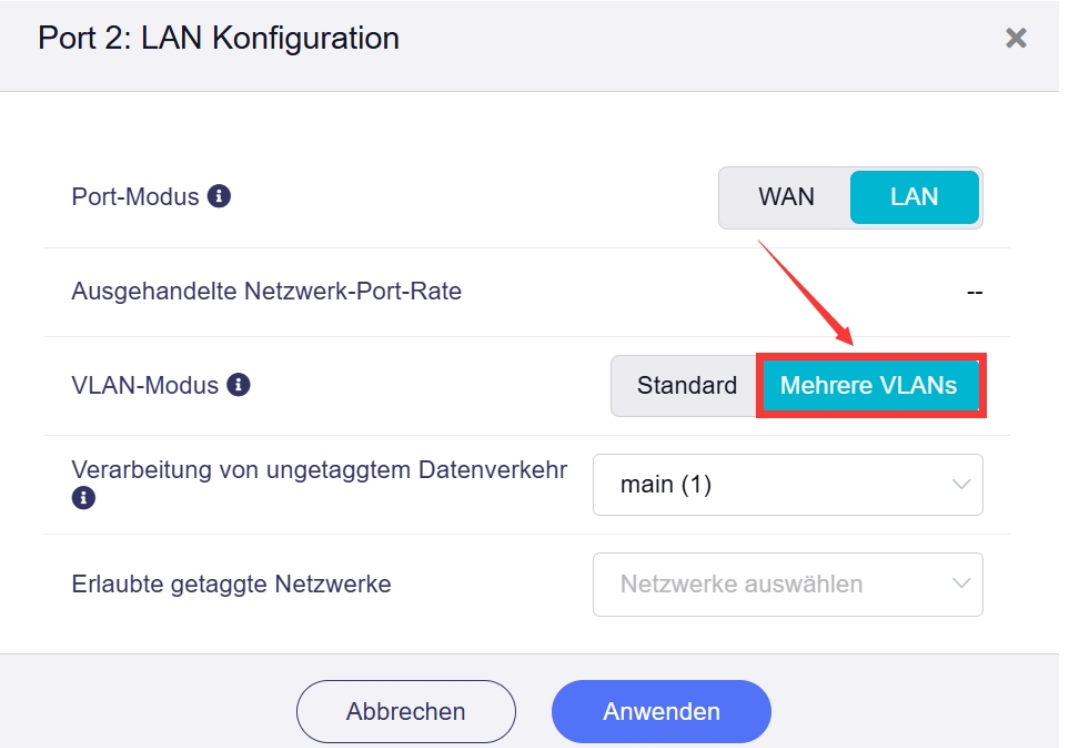
Der LAN-Bereich zeigt die LAN-Port-Konfiguration an. Sie können die Portrolle zwischen LAN und WAN wechseln, den Ethernet-Modus (Standard oder mehrere VLANs) für den LAN-Port auswählen und die ausgehandelte Linkrate anzeigen.

1. Standardmodus
   Der Standardmodus erlaubt nur ein VLAN (Untagged), das zum Anschluss von Endgeräten verwendet wird.



- **Ausgehandelte Netzwerk-Port-Rate**: Die ausgehandelte Linkgeschwindigkeit der LAN-Schnittstelle, die nur angezeigt wird, wenn eine gültige Verbindung erkannt wird.
- **Ethernet-Modus**: Standardmäßig im Standard-Modus.
- **Zugriffsnetzwerk**: Mit dem Zugriffsnetzwerk können Sie eine Netzwerkisolierung erreichen, indem Sie LAN-Ports unterschiedlichen Subnetzen zuweisen.

2. Mehrfach-VLAN-Modus
   Der Modus mit mehreren VLANs ermöglicht mehrere VLANs (Tagged) an einem Port, typischerweise zum Anschluss von APs oder anderen Switches.



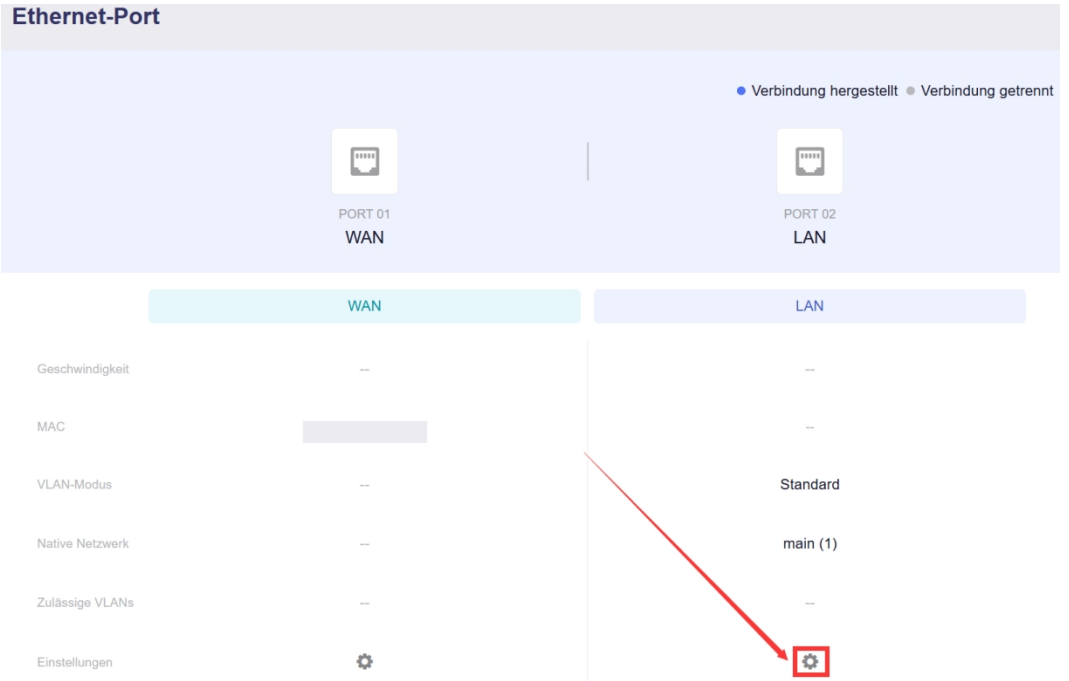
- **Ausgehandelte Netzwerk-Port-Rate**: Die ausgehandelte Linkgeschwindigkeit der LAN-Schnittstelle, die nur angezeigt wird, wenn eine gültige Verbindung erkannt wird.
- **VLAN-Modus**: Um in den Modus Mehrere VLANs zu wechseln, klicken Sie auf die Registerkarte Mehrere VLANs.
- **Verarbeitung von ungetaggtem Datenverkehr**: Konfigurieren Sie die untagged Pakethandling für den Port. Sie können auswählen, ob Sie solche Pakete direkt ablegen oder an ein anderes Subnetz als das native PVID-Netzwerk weiterleiten möchten.
- **Erlaubte getaggte Netzwerke**: Gibt die VLANs an, die im markierten Modus durch diesen Port geleitet werden dürfen. Sie können VLAN-Netzwerke aus der Liste auswählen, und nur der übereinstimmende Datenverkehr wird weitergeleitet.

Hinweis: Die ausgehandelte Rate für den WAN- und LAN-Port wird nur angezeigt, wenn ein Ethernet-Kabel verbunden. Es hängt sowohl vom Ethernet-Port als auch vom Ethernet-Kabel ab.

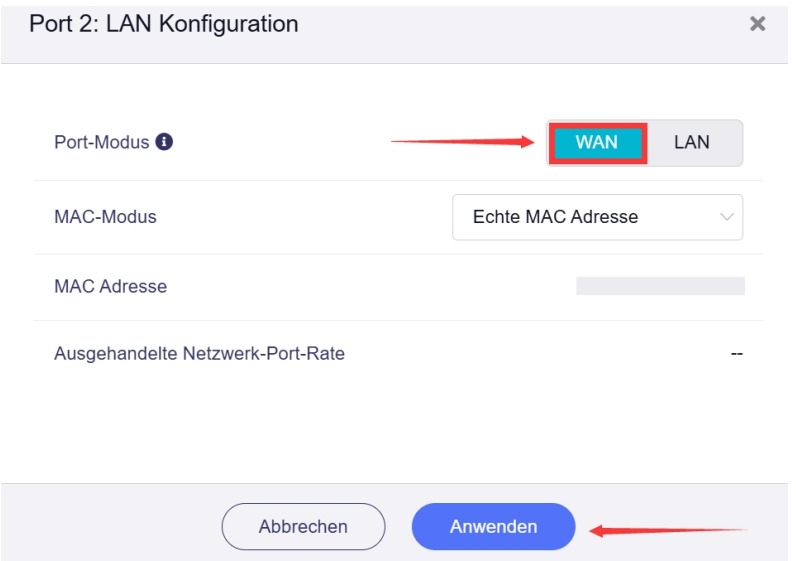
9.3.3 Dual-Ethernet WAN

Mit der Dual-Ethernet-WAN-Funktion können Sie einen Standard-LAN-Ethernet-Port auf einen sekundären WAN-Port für den Dual-Ethernet-Internetzugang umschalten. es können Sie sich auch mit zwei unabhängigen Netzwerken (z. B. arbeits- und privat) gleichzeitig verbinden, was die Flexibilität ohne zusätzliche Hardware erhöht.

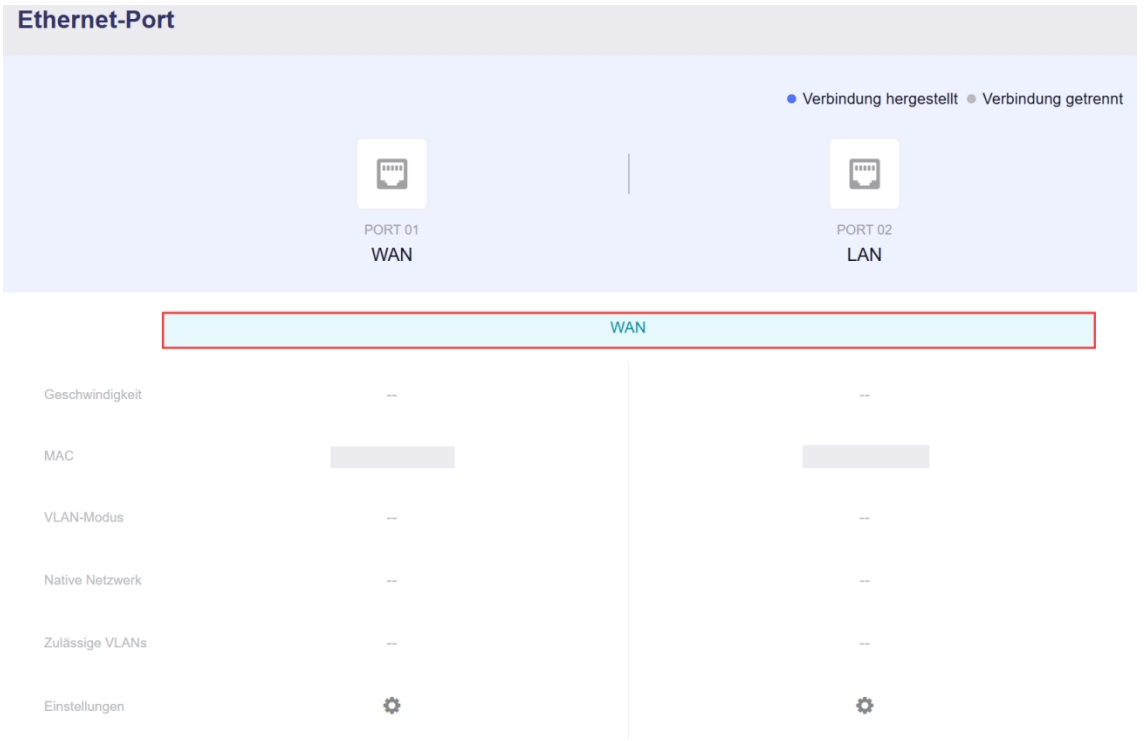
1. Klicken Sie auf der Ethernet-Port-Seite auf die LAN-Einstellung, um die Konfigurationsseite einzugeben.



2. Wechseln Sie die Portrolle zu WAN und klicken Sie auf **Anwenden**.



3. Sie können zur Ethernet-Port-Seite zurückkehren, um zu überprüfen, ob die Portrolle auf WAN umgestellt ist, und der LAN-Port wird dann als WAN-Port betrieben.

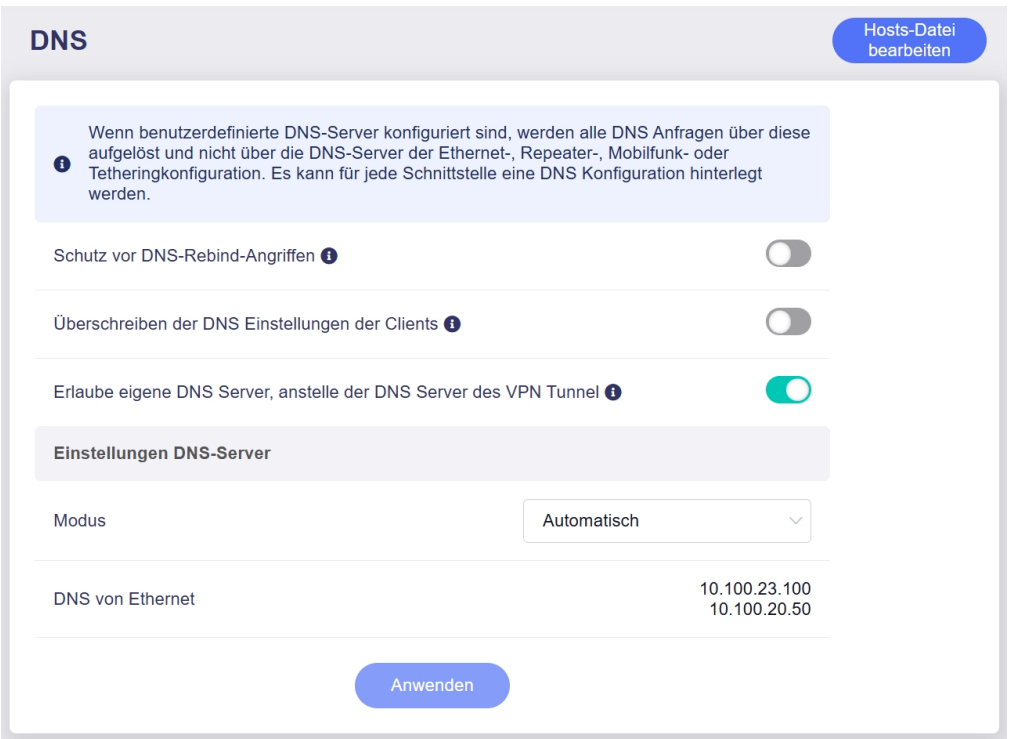


9.4 DNS

DNS (Domain Name System) ist ein Netzwerkdienst, der von Menschen lesbare Domainnamen (z. B. www.google.com) in maschinenerkennbare IP-Adressen (z. B. 142.250.185.142) übersetzt, wodurch Geräte mit Zielwebsites oder -diensten verbunden werden können.

Router DNS Server bezeichnet den in den Router integrierten DNS-Dienst, der für alle verbundenen Geräte Domainnamen in IP-Adressen auflöst. Er funktioniert in der Regel auf zwei Arten: Erstens bezieht er automatisch DNS-Adressen aus dem vorgelagerten Netzwerk, um die Standard-Namensauflösung bereitzustellen. Zweitens können Benutzer im Web-Admin-Panel des Routers benutzerdefinierte öffentliche DNS-Adressen (z. B. 8.8.8.8) festlegen, um den Netzwerkzugriff zu optimieren oder die Sicherheit zu erhöhen. Standardmäßig verwenden die verbundenen Geräte diesen einheitlichen DNS-Server, sodass keine separate DNS-Konfiguration auf jedem Gerät erforderlich ist.

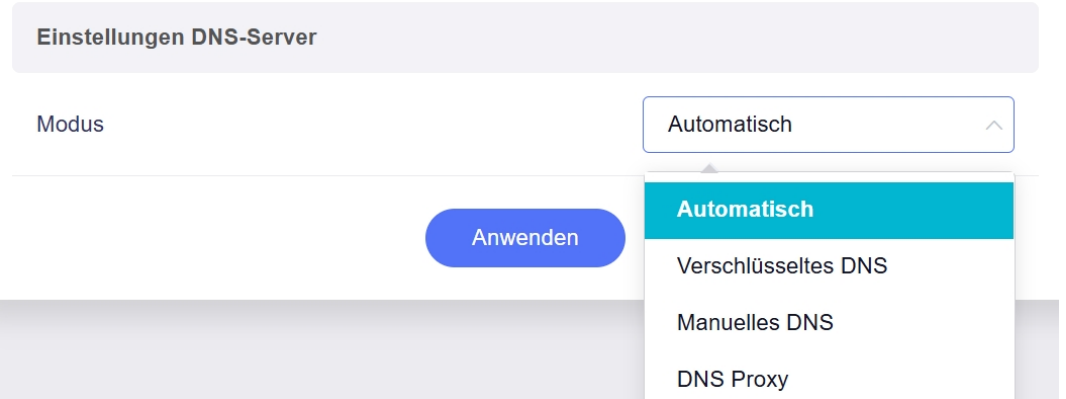
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **DNS**. Diese Seite ermöglicht es Ihnen, DNS-bezogene Einstellungen zu konfigurieren, einschließlich Sicherheitsoptionen, Servermodi und DNS-Prioritätsregeln für verschiedene Netzwerkszenarien.



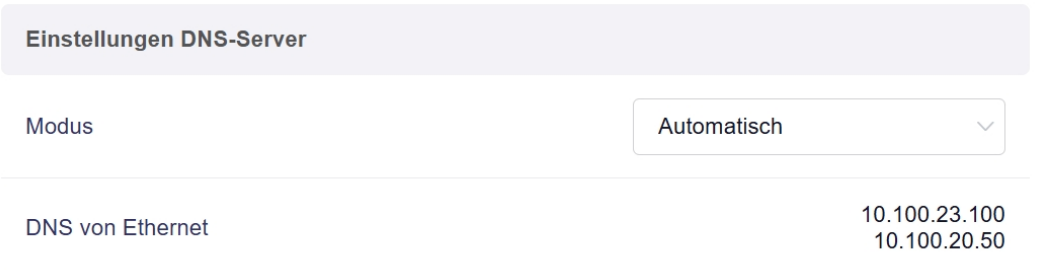
- **Schutz vor DNS-Rebind-Angriffen**: Schützt vor DNS Rebinding Attacken, indem es bösartige DNS-Auflösungsversuche blockiert. Beachten Sie, dass die Aktivierung dazu führen kann, dass private DNS-Lookup-Fehler fehlschlagen; deaktivieren, wenn Ihr Netzwerk ein Captive-Portal verwendet (z. B. öffentliche Wi-Fi-Anmeldeseiten).
- **Überschreiben der DNS Einstellungen der Clients**: Wenn diese aktiviert sind, werden alle angeschlossenen Geräte gezwungen, die auf dem Router konfigurierten DNS-Server zu verwenden, wobei ihre eigenen ursprünglichen DNS-Einstellungen ignoriert werden.
- **Erlaube eigene DNS Server, anstelle der DNS Server des VPN Tunnel**: Wenn Sie aktiviert sind, wenn Sie benutzerdefinierte DNS festgelegt haben, verwenden Pakete, die durch den VPN-Tunnel übertragen werden, das benutzerdefinierte DNS zur Auflösung anstelle der DNS-Server aus der VPN-Verbindung.

9.4.1 Einstellungen DNS-Server

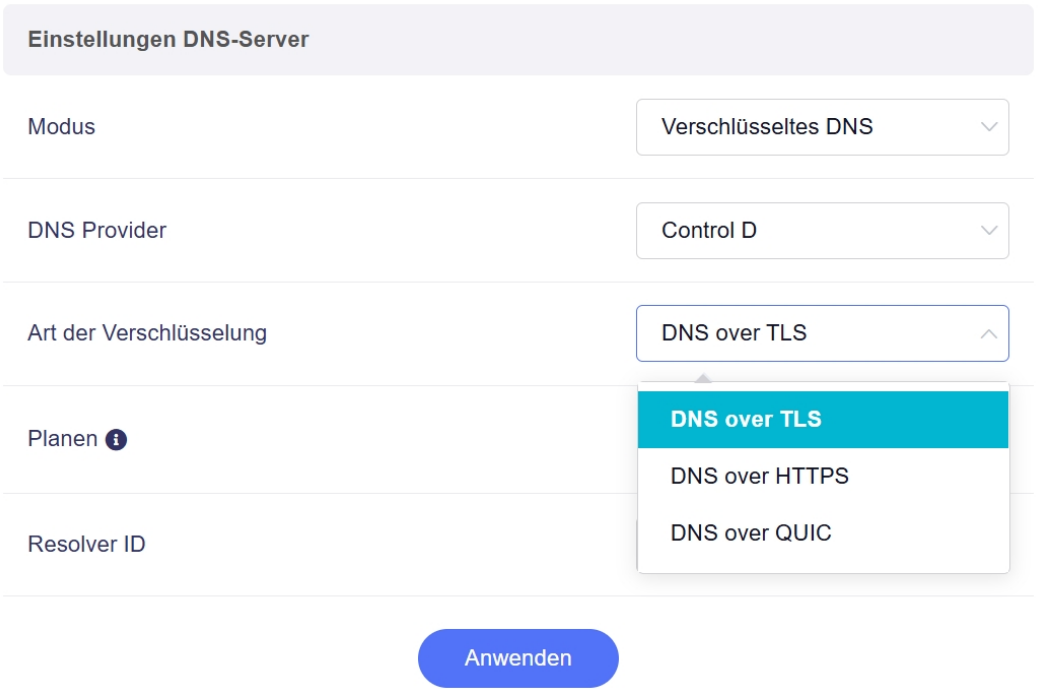
Es gibt vier Modi für den DNS-Server: Automatisch, Verschlüsseltes DNS, Manuelles DNS und DNS Proxy.



1. **Automatisch**: Wenn der Router ausgewählt ist, erhält er automatisch DNS-Serveradressen aus dem vorgelagerten Netzwerk und wendet sie auf alle angeschlossenen Geräte an.

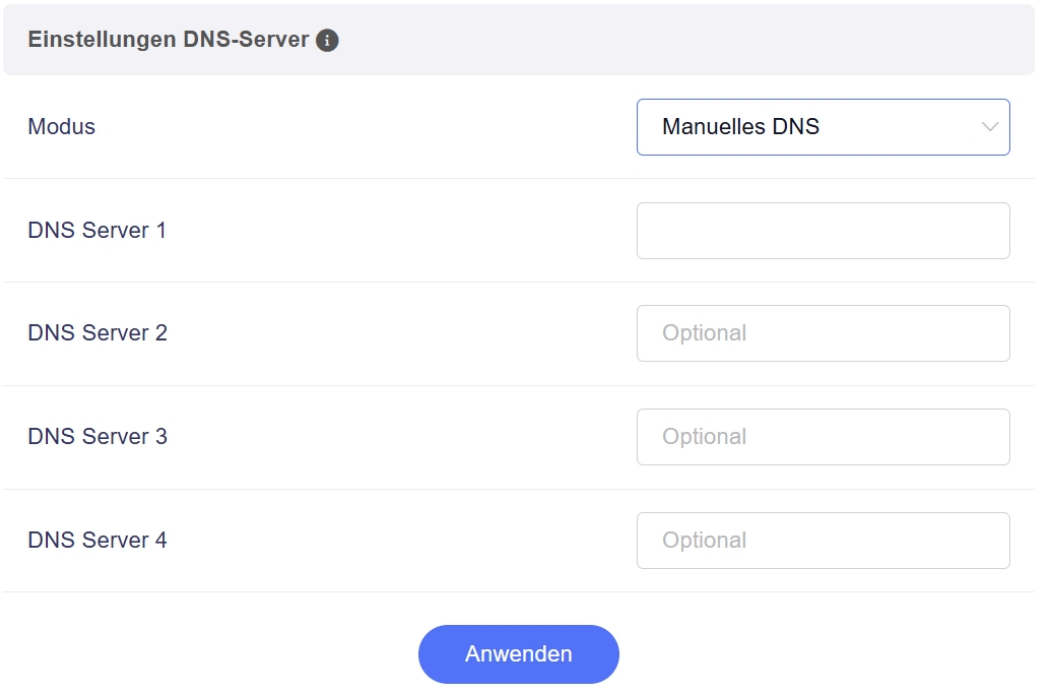


2. **Verschlüsseltes DNS**: Wenn der Router ausgewählt wird, verwendet er verschlüsselte Protokolle, um DNS-Abfragen zu verarbeiten und die Auflösungsdaten gegen Abhören oder Manipulation zu sichern.
   Es hat vier Verschlüsselungstypen: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS.



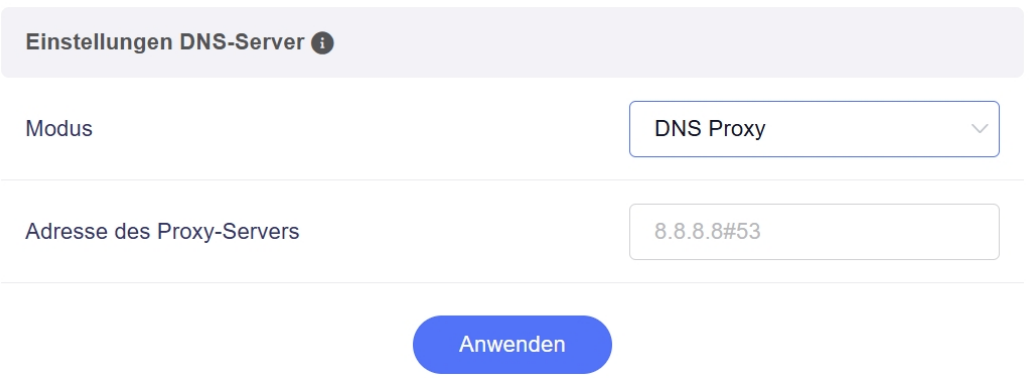
   - Wählen Sie für DNS over TLS einen DNS-Anbieter unter Control D, NextDNS und Cloudflare aus.
   - Für die anderen drei (DNSCrypt-Proxy, DNS over HTTPS und Oblivious DNS over HTTPS) wählen Sie mindestens einen DNS-Server aus dem Repository. Bis zu 8 Server können ausgewählt werden. Wenn mehrere Server ausgewählt werden, verwendet der Router automatisch den schnellsten.

3. **Manuelles DNS**: Wenn Sie ausgewählt sind, können Sie die DNS-Server Ihres Routers anpassen. Klicken Sie auf DNS Server 1 und wählen Sie einen DNS-Server aus der Dropdown-Liste. Die verbleibenden DNS-Felder werden automatisch aktualisiert.



Hinweis: Wenn Sie IPv6-Adressen für manuelles DNS verwenden müssen, aktivieren Sie zuerst IPv6 auf Ihrem Router.

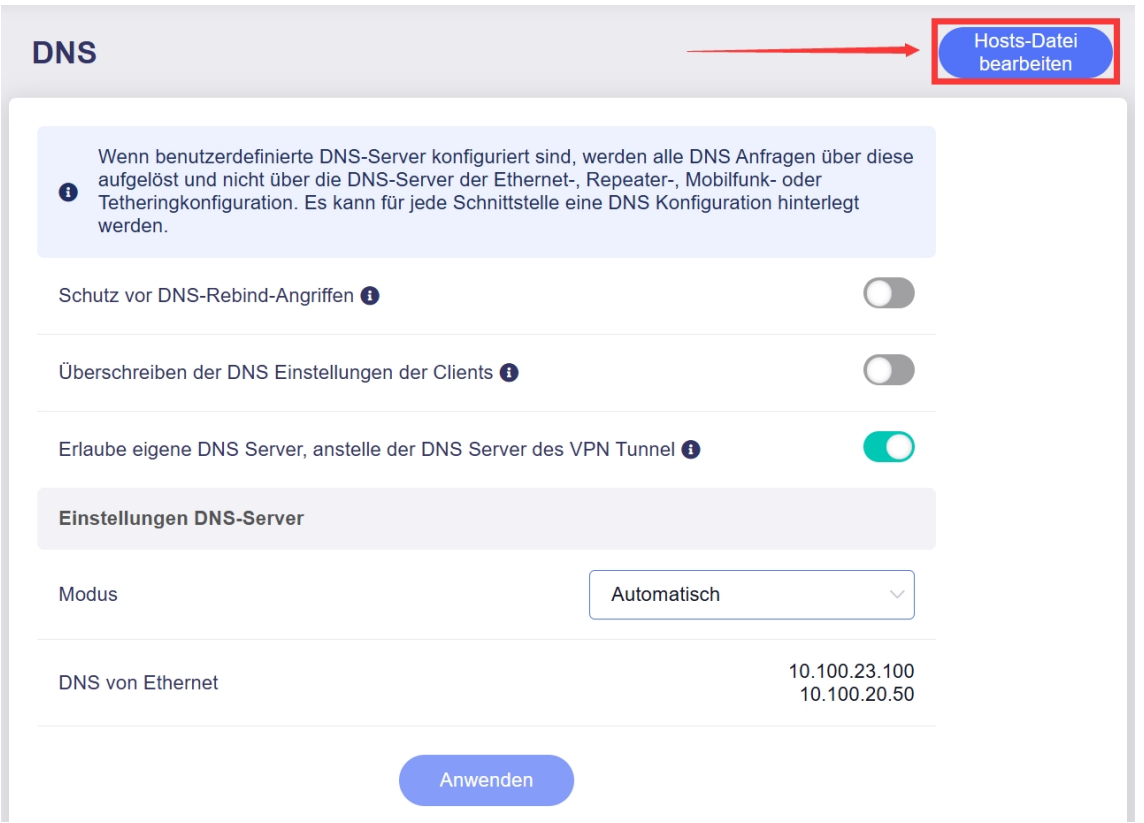
4. **DNS-Proxy**: Bei der Auswahl leitet der Router alle DNS-Abfragen über einen Proxy-Server weiter, wodurch eine Auflösung über die Netzwerkumgebung des Proxys für bestimmte Zugriffsanforderungen ermöglicht wird.



9.4.2 Hosts-Datei bearbeiten

Sie können bei Bedarf statische DNS-Auflösungsregeln definieren.

Klicken Sie auf der DNS-Seite auf **Hosts-Datei bearbeiten** in der oberen rechten Ecke.



Anfragen von Clients werden vorzugsweise mit den hier geschriebenen statischen DNS-Regeln gelöst, so dass Sie IP-Adressen manuell Hostnamen zuordnen können (z. B. die Standardeinträge wie 127.0.0.1 localhost für Local Loopback) für eine angepasste Domänennamenauflösungskontrolle.

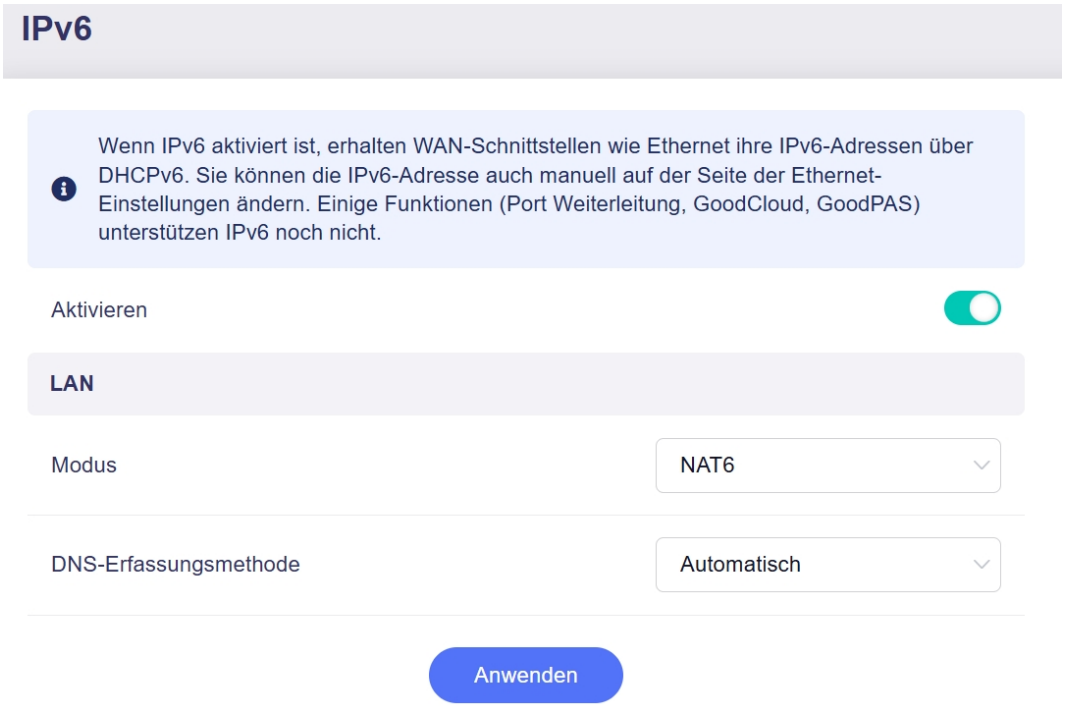


9.5 IPv6

IPv6 (Internet Protocol Version 6) ist das neueste Internet Protocol, das IPv4 ersetzen soll. Es bietet einen größeren Pool an einzigartigen IPs, löst das Problem der Adresserschöpfung von IPv4 und unterstützt die wachsende Zahl von angeschlossenen Geräten weltweit.

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **IPv6**. Diese Seite ermöglicht es Ihnen, IPv6 auf Ihrem Router zu aktivieren und zu konfigurieren. Wenn IPv6 aktiviert ist, erhalten WAN-Schnittstellen wie Ethernet ihre IPv6-Adressen über DHCPv6.

Wechseln Sie auf **Aktivieren**, wählen Sie den Modus für Ihr Hauptnetzwerk und Ihre DNS-Erfassungsmethode aus und klicken Sie dann auf **Anwenden.**



Hinweis: Einige Funktionen (z. B. Firewall, GoodCloud, OpenVPN DCO) unterstützen IPv6 noch nicht. Wenn Sie diese Funktionen und IPv6 gleichzeitig aktivieren, ist es wahrscheinlich, dass es zu Verbindungsproblemen kommt.

9.5.1 IPv6-Modus

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

- **Native**: Dieser Modus eignet sich, wenn der Router direkt eine öffentliche IPv6-Adresse erhält. Der Router weist den verbundenen Geräten automatisch IPv6-Adressen zu; damit werden die IPv6-Zugriffsanforderungen der meisten Benutzer erfüllt.
- **Passthrough**: Dieser Modus ist anwendbar, wenn IPv6-Pakete direkt ohne Verarbeitung oder Konvertierung durchlaufen werden müssen. Beispielsweise können bestimmte Anwendungen oder Dienste die vollständige Aufbewahrung von IPv6-Paketinhalten für die weitere Verarbeitung oder Analyse erfordern. Dieser Modus wird von technischem Personal für das Netzwerk-Debugging oder die Sicherheitsanalyse verwendet.
- **NAT6**: Dieser Modus eignet sich für Szenarien, in denen ein Router als Gateway verwendet wird, um jedem Gerät im Netzwerk dynamische interne IPv6-Adressen zuzuweisen. In diesem Modus verbinden sich Endgeräte über ein optisches Netzabschlussgerät und erhalten eine IPv6-Adresse im lokalen Netzwerk.
- **Static IPv6**: Dieser Modus eignet sich für Geräte oder Dienste, die eine feste IPv6-Adresse benötigen, wie Server oder Netzwerkdrucker. Dieser Modus stellt sicher, dass das Gerät immer die gleiche IPv6-Adresse verwendet, was die Verwaltung und den Zugriff erleichtert.

9.5.2 DNS-Erfassungsverfahren

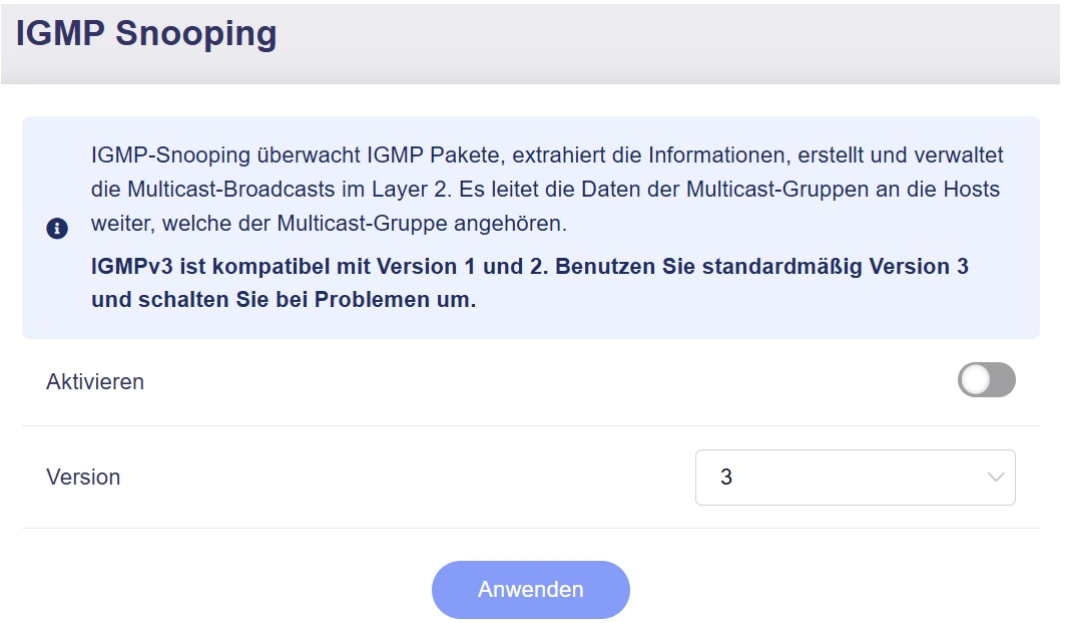
Es bestimmt, wie der Router IPv6-DNS-Serveradressen erhält. Es gibt zwei Optionen: Automatisch und Manuell.

- **Automatisch**: Der Router erhält die IPv6-DNS-Serveradressen dynamisch (z. B. über DHCPv6).
- **Manuelles DNS**: Eingabe benutzerdefinierter IPv6-DNS-Serveradressen. Da DNS jedoch verwendet wird, um Domainnamen auf die entsprechenden IP-Adressen aufzulösen, kann die manuelle DNS-Serverkonfiguration zu DNS-Lookup-Ausfällen führen.

9.6 IGMP Snooping

IGMP Snooping hört das IGMP-Protokollpaket, extrahiert die entsprechenden Informationen, erstellt und pflegt die Multicast-Weiterleitungstabelle für Schicht 2 und leitet dann die Multicast-Gruppendaten an den Host weiter, der der Multicast-Gruppe beitritt, während andere Hosts die Multicast-Gruppendaten nicht empfangen können.

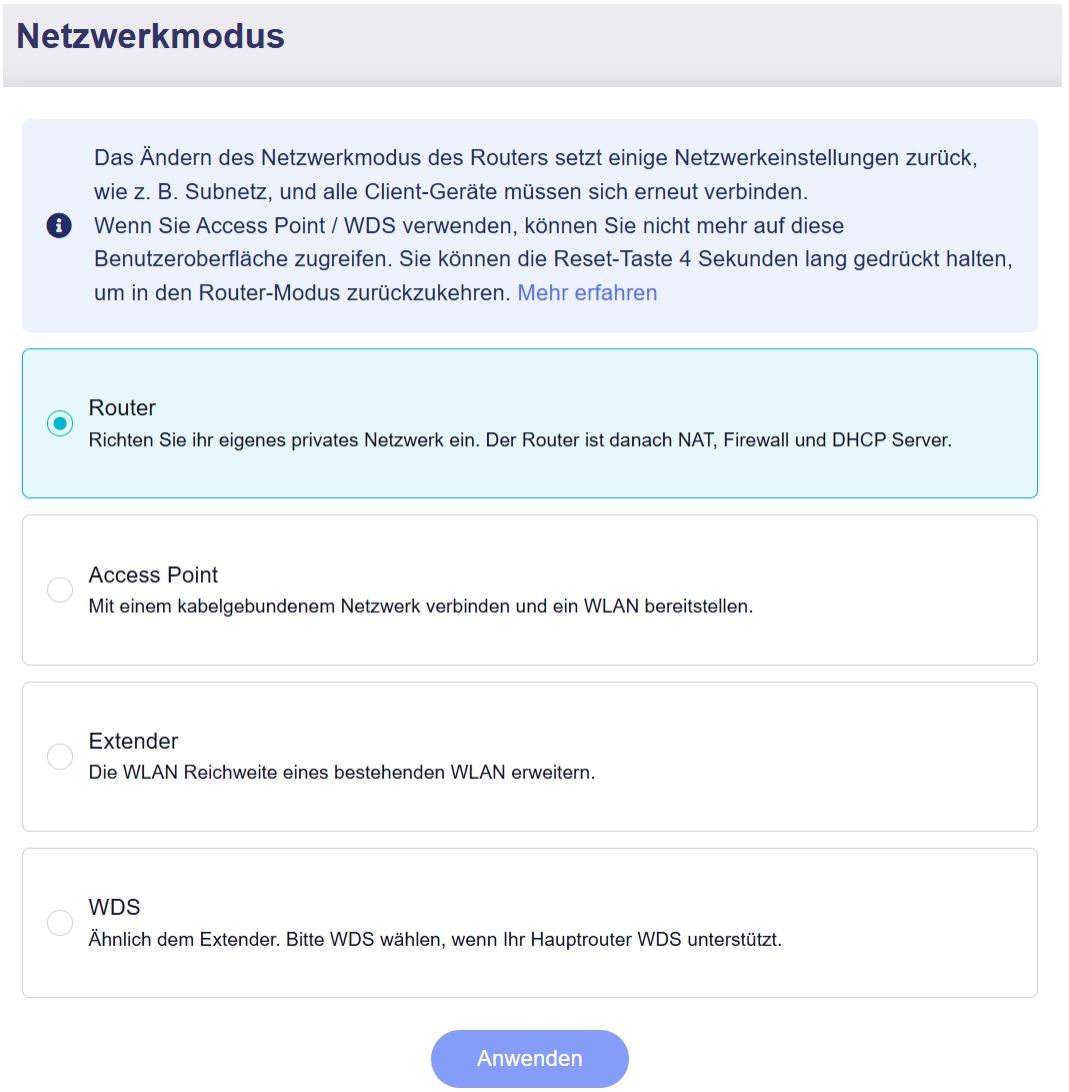
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **IGMP Snooping.** Sie können es aktivieren, um die Multicast-Funktion auf Ihrem Router zu verwenden, wenn Sie es benötigen.



9.7 Netzwerkmodus

Der Netzwerkmodus bezieht sich auf die verschiedenen operativen Rollen und Funktionen, die ein Router übernehmen kann, um verschiedene Netzwerkbereitstellungsanforderungen zu erfüllen.

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zum **Netzwerk** > **Netzwerkmodus**. Sie können den Netzwerkmodus Ihres Routers ändern.



- **Router**: Dies ist der Standardbetriebsmodus für die meisten Heim- und Bürorouter. Er dient dazu, ein privates lokales Netzwerk (LAN) einzurichten und als dediziertes Gateway zwischen dem öffentlichen Internet und verbundenen Geräten zu fungieren. In diesem Modus stellt der Router Kernfunktionen wie NAT, DHCP und eine integrierte Firewall

bereit. Er verbindet sich mit einer vorgelagerten Leitung, etwa einem Breitbandfaseranschluss, weist verbundenen Geräten automatisch private IP-Adressen zu und schützt das gesamte private Netzwerk.

- **Access Point**: In diesem Modus kann sich ein Router über ein LAN-Kabel mit einem kabelgebundenen Netzwerk verbinden und drahtlose Signale senden. Dadurch wird die WLAN-Abdeckung in großen Bereichen erweitert, sodass mehr Geräte auf das Netzwerk zugreifen können. Der Router deaktiviert dabei seine NAT- und DHCP-Funktionen und arbeitet ausschließlich als drahtloser Sender und Switch, nicht als eigenständiges Gateway.
- **Extender**: Dieser Modus erweitert die WLAN-Abdeckung eines bestehenden drahtlosen Netzwerks und beseitigt Funklöcher in Bereichen mit schlechter Verbindung. Der Router empfängt die Signale des Hauptrouters drahtlos, verstärkt sie und sendet sie erneut. Im Unterschied zum Access-Point-Modus ist keine kabelgebundene Verbindung zum Hauptrouter erforderlich; die Bandbreite kann sich jedoch halbieren, da das Gerät gleichzeitig Signale empfangen und senden muss.
- **WDS**: Der Modus des Wireless Distribution System (WDS) ähnelt dem Extender-Modus, da er die WLAN-Abdeckung drahtlos erweitert, aber er unterstützt die drahtlose Überbrückung zwischen mehreren kompatiblen Routern.
  Dieser Modus ist ideal für Szenarien wie die Abdeckung von mehrstöckigen Gebäuden oder kleinen Bürocampussen, wo mehrere Router zusammenarbeiten müssen, um ein einheitliches drahtloses Netzwerk zu bilden. Im Gegensatz zum Extender-Modus, der nur Signale von einem Hauptrouter an einen einzigen Extender überträgt, ermöglicht der WDS-Modus miteinander verbundenen Routern, Signale zu senden und zu empfangen, was eine nahtlose Abdeckung über größere Bereiche mit mehreren Signalknoten ermöglicht.

Hinweis:

1. Wenn der Netzwerkmodus geändert wird, müssen sich alle Clientgeräte wieder mit dem Router verbinden, um eine stabile Netzwerkverbindung zu gewährleisten.
2. **Im Modus Access Point / WDS können Sie nicht über die ursprüngliche IP-Adresse auf das Web-Admin-Panel zugreifen.** Melden Sie sich stattdessen am vorgelagerten Router an, um die diesem Router zugewiesene IP-Adresse zu ermitteln, und verwenden Sie diese Adresse für den Zugriff auf das Web-Admin-Panel. Haben Sie keinen Zugriff

auf den vorgelagerten Router, halten Sie die Reset-Taste 4 Sekunden lang gedrückt, um zum Standardmodus „Router“ zurückzukehren.

3. **Im Modus Access Point / Extender / WDS sind folgende Funktionen nicht verfügbar**: Zugangskontrolle(Allowlist und Blocklist), GoodPAS, VPN, AdGuard Home, Kindersicherung, ZeroTier, Tailscale, Port Weiterleitung, Multi WAN, DHCP-Server, Adressreservierung, Gastnetzwerk, DNS, Ethernet-Port, IPv6, Drop-in Gateway, IGMP Snooping, Netzwerk-Beschleunigung und Netzwerkmodus.

9.8 Netzwerk-Beschleunigung

Die Netzwerk-Beschleunigung reduziert die CPU-Auslastung und beschleunigt die Datenverkehrspaketweiterleitung, kann jedoch mit einigen Funktionen in Konflikt geraten.

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Netzwerk** > **Netzwerk-Beschleunigung**. Diese Seite ermöglicht es Ihnen, die Netzwerkbeschleunigung zu aktivieren und den Modus zwischen Hardware Acceleration und Software Acceleration auszuwählen.



- **Hardware-Beschleunigun**: Es lädt hochfrequente Netzwerkaufgaben (z. B. NAT, Paketweiterleitung, Prüfsummenverifizierung) auf dedizierte Hardware wie NPUs oder HWNAT-Chips. Es funktioniert speziell auf Ethernet- und Repeater-Verbindungen, was sich in diesen Szenarien mit festen Pfaden und einfachen Regeln auszeichnet, um einen hohen Durchsatz, eine geringe Latenz und eine minimale CPU-Last für die Datenübertragung mit Drahtgeschwindigkeit zu liefern.
- **Software-Beschleunigung**: Es basiert auf der allgemeinen CPU eines Routers, gepaart mit optimierten Kerneln oder Treibern (z. B. SWNAT). Es funktioniert mit dem Zugang zu Mobilfunk (4G/5G), typischerweise dem primären Szenario, in dem keine Hardwarebeschleunigung verfügbar ist, und bietet eine starke Kompatibilität und Unterstützung für komplexe Protokolle.

Hinweis: Wenn die Netzwerkbeschleunigung aktiviert ist, funktionieren die folgenden Funktionen nicht ordnungsgemäß: Client-Geschwindigkeitsstatistik, Verkehrsstatistik, Geschwindigkeitsbegrenzung, Kindersicherung und VPN mit IPv6.

Kapitel 10

Flusskontrolle

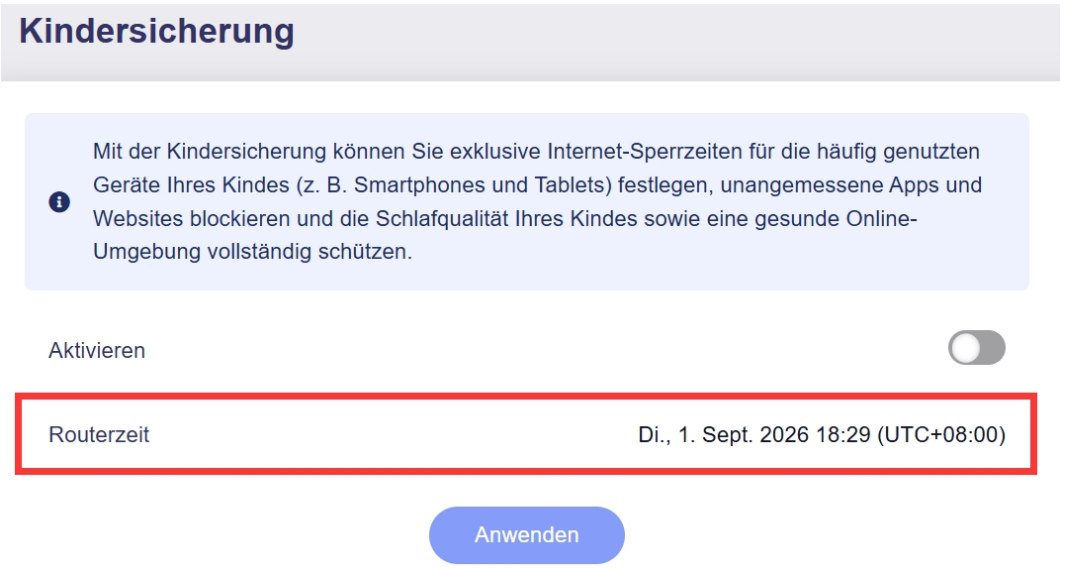
In diesem Kapitel wird die Kindersicherung vorgestellt, die ein spezielles Tool zum Filtern von Websites und zum Festlegen von Nutzungsbeschränkungen bietet.

10.1 Kindersicherung

Die elterliche Kontrolle ist eine Möglichkeit, Kinder online zu schützen, indem sie unangemessene Websites blockiert und die Nutzungsdauer von Geräten begrenzt. Sie hilft, den Zugang zu schädlichen Inhalten zu verhindern, die Bildschirmzeit zu verwalten und sicherzustellen, dass Kinder das Internet verantwortungsvoll nutzen.

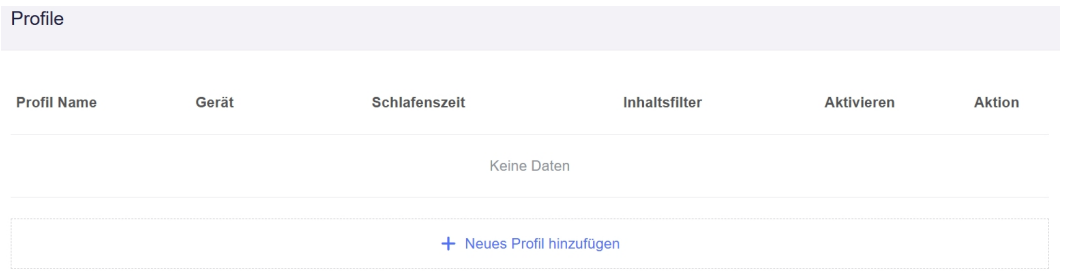
Befolgen Sie die folgenden Schritte, um Ihre elterliche Kontrolle einzurichten.

1. Melden Sie sich im Web-Admin-Panel des Routers an und gehen Sie zu **Flusskontrolle** > **Kindersicherung**.

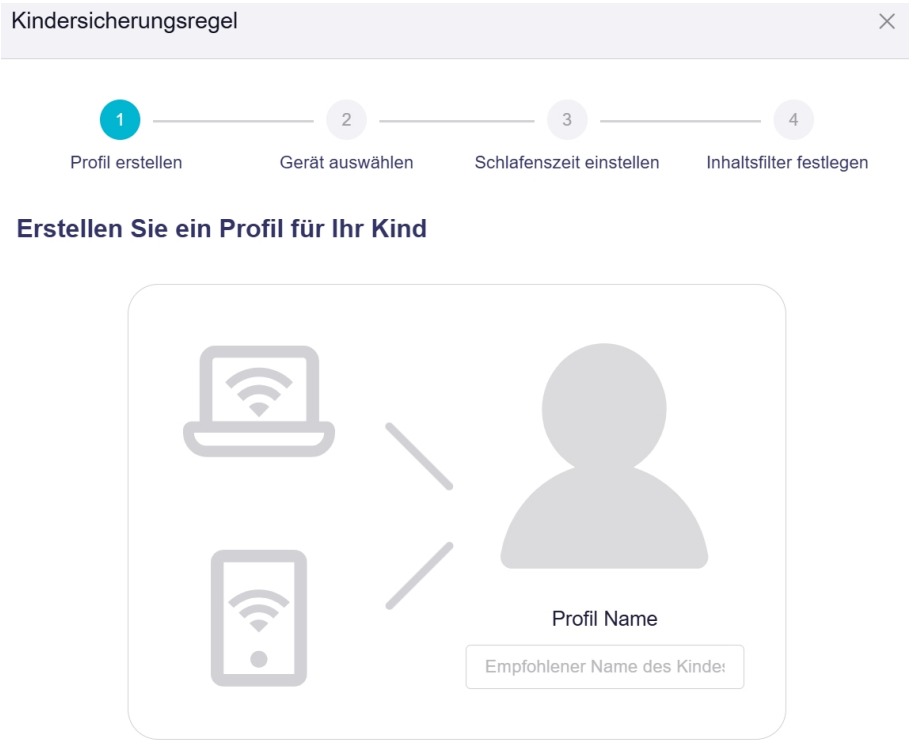


   Wenn nicht, gehen Sie zu **System** > **Zeitzone,** um es zuerst zu synchronisieren.

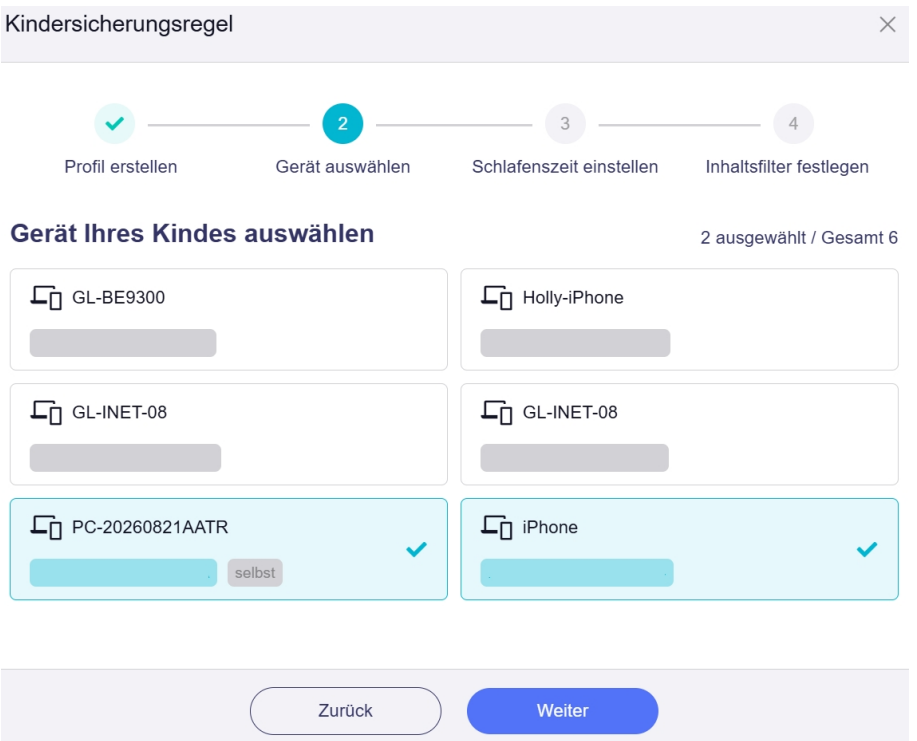
2. Aktivieren Sie die elterliche Kontrolle und klicken Sie auf **Anwenden**.
3. Sie sehen eine Regelliste wie folgt. Klicken Sie auf **Neues Profil hinzufügen**.



4. Erstellen Sie im Popup-Fenster eine Regel und legen Sie einen benutzerdefinierten Namen fest, und klicken Sie dann auf **Weiter**.

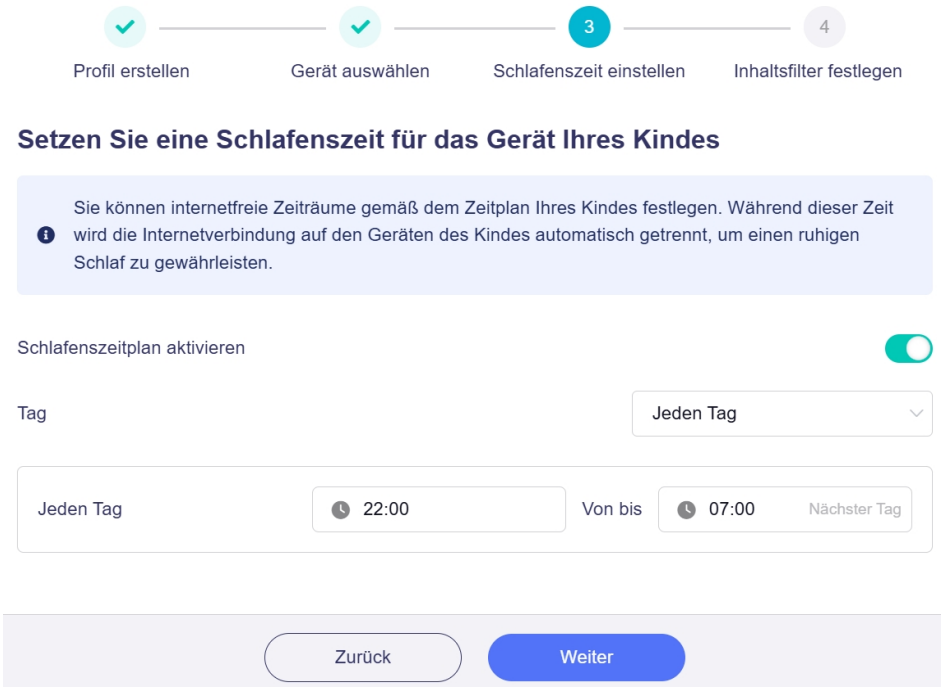


5. Wählen Sie das Gerät Ihres Kindes und klicken Sie dann auf **Weiter**.
   Geräte werden nur auf dieser Seite angezeigt, wenn sie über WLAN oder Ethernet mit dem Router verbunden sind. Cyan zeigt den Online-Status an, während Grau den Offline-Status anzeigt.



Tipp: Wenn Sie die verbundenen Geräte voneinander unterscheiden möchten, wechseln Sie zur Seite **Clients** und passen Sie die Gerätenamen individuell an.

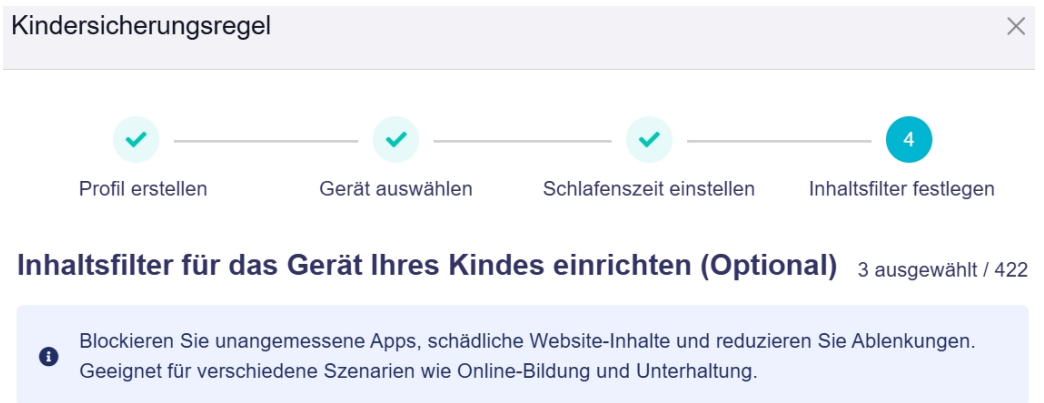
6. Legen Sie die Schlafenszeit für das Gerät Ihres Kindes fest und klicken Sie dann auf **Weiter**. Das Internet auf dem ausgewählten Gerät ist während dieses Zeitraums nicht verfügbar. Die Schlafenszeit ist standardmäßig für jeden Tag gleich.

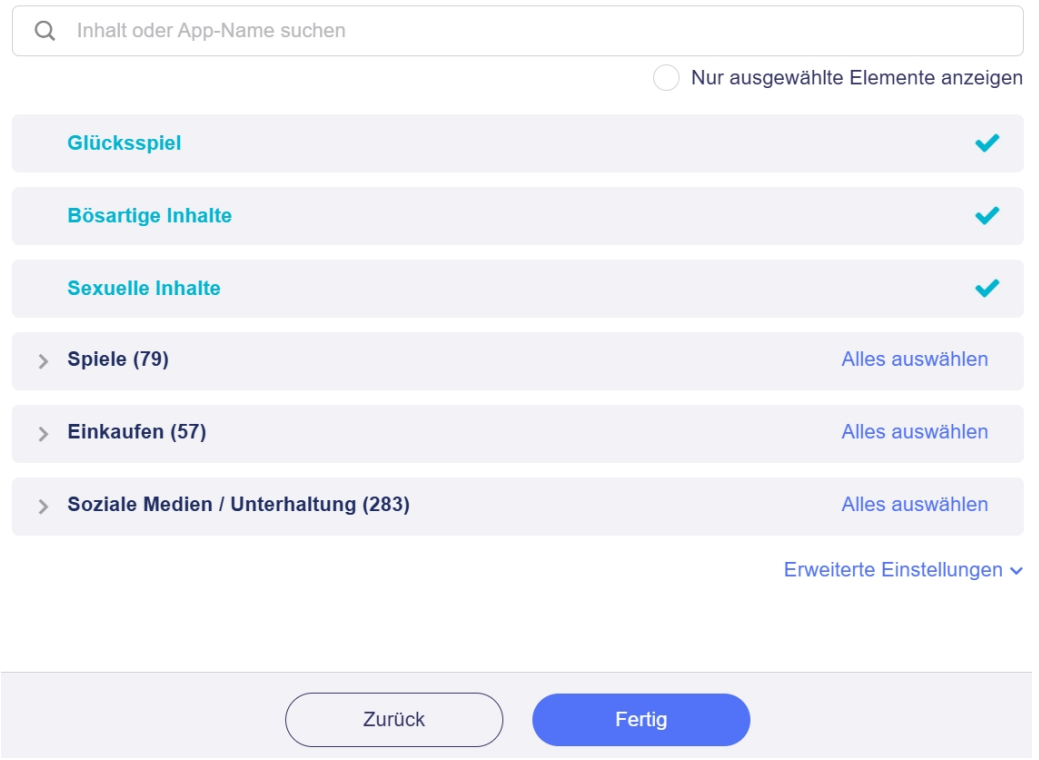


Wenn Sie für jeden Tag der Woche unterschiedliche Schlafenszeiten festlegen möchten, wählen Sie **Tage anpassen** und verschiedene Schlafenszeiten festlegen, und klicken Sie auf **Weiter**.

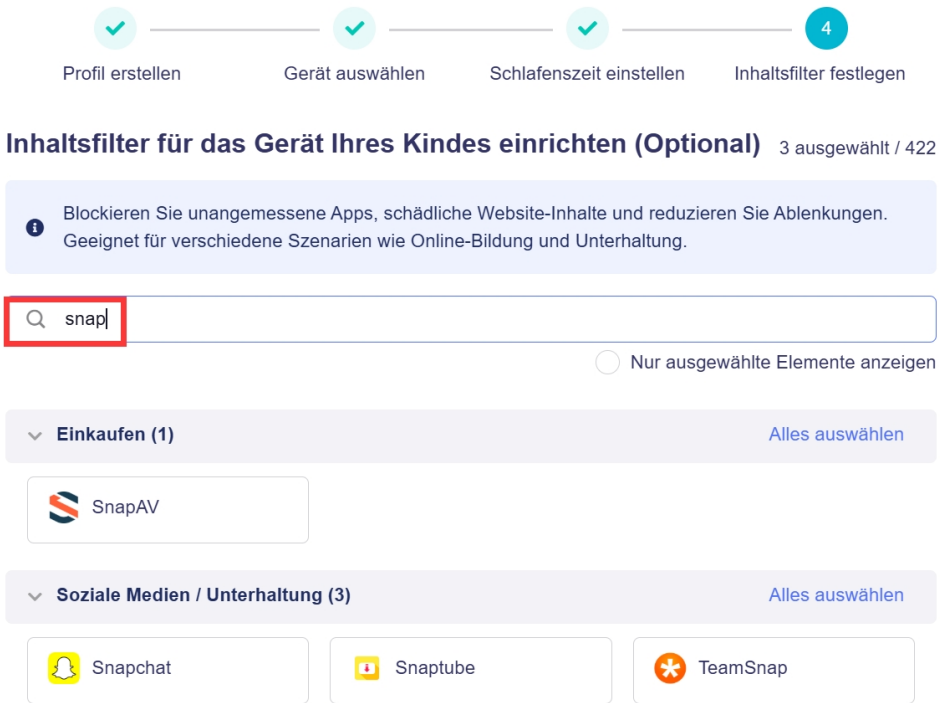
7. Wählen Sie Inhaltsfilter.

   Standardmäßig wurden drei Kategorien ausgewählt: **Glücksspiel, bösartige Inhalte** und **sexuelle Inhalte**. Sie können bei Bedarf andere Kategorien auswählen, z. B. **Spiele, Einkaufen**, **Social Media**, **Unterhaltung** usw.

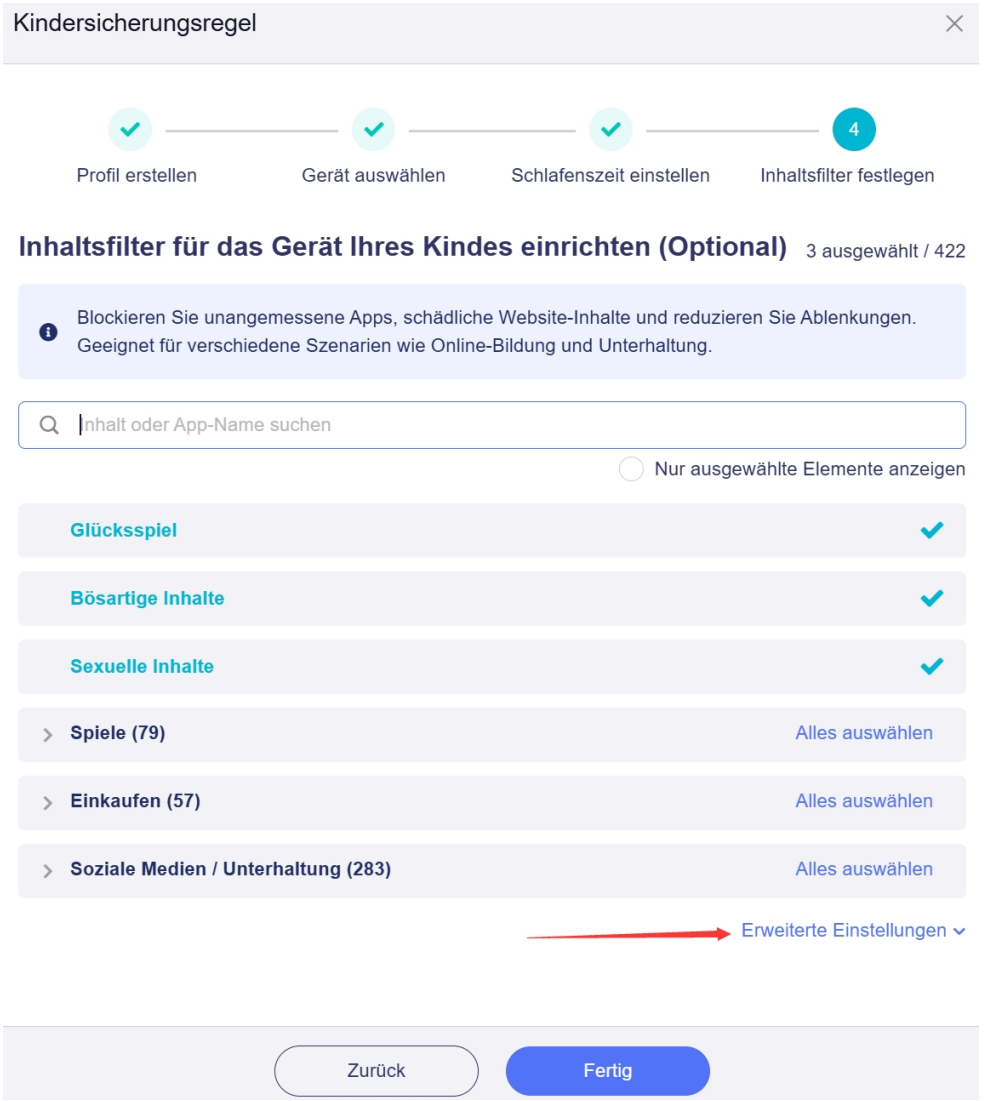




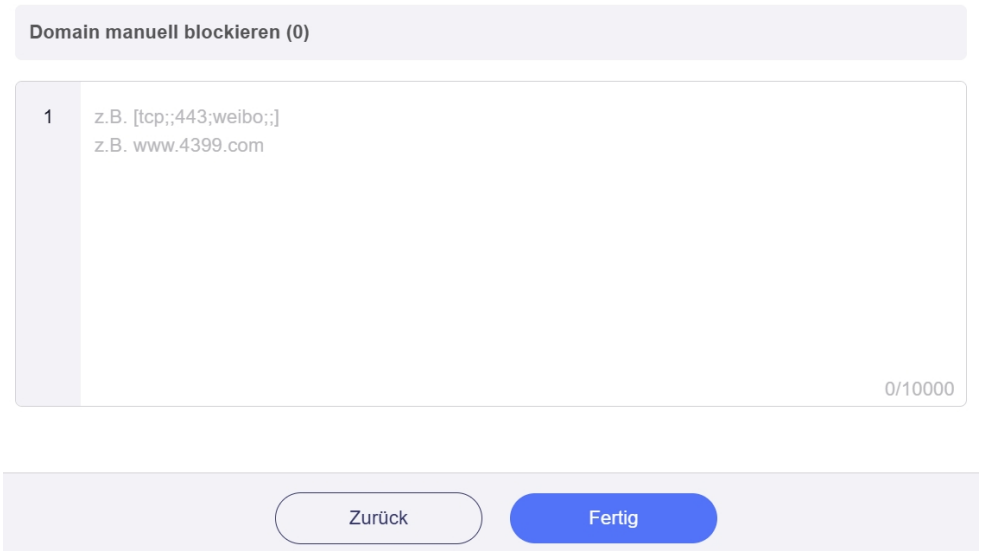
Wenn eine bestimmte App, die Sie blockieren möchten, schwer herauszufinden ist, können Sie sie oben suchen.



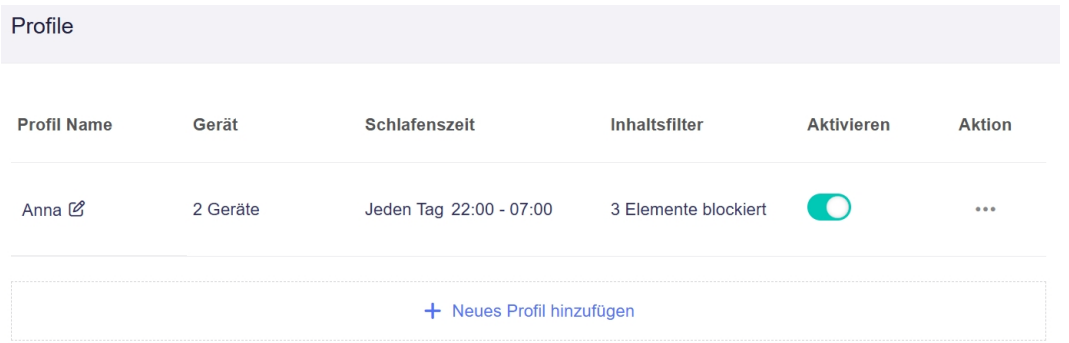
8. Wenn Sie bestimmte Domains blockieren müssen, klicken Sie unten rechts auf **Erweiterte Einstellungen**.



Geben Sie Domains manuell ein und klicken Sie dann auf **Fertig**.



9. Die Liste zeigt den Regelnamen, die Anzahl der angeschlossenen Geräte, den Schlafenszeitplan, den gefilterten Inhalt und den Regelstatus (aktiviert/deaktiviert).



Kapitel 11

Sicherheit

Dieses Kapitel verwaltet die Netzwerksicherheit, wie Port-Weiterleitung, Verwaltungssteuerungn und NAT-Modus.

11.1 Port Weiterleitung

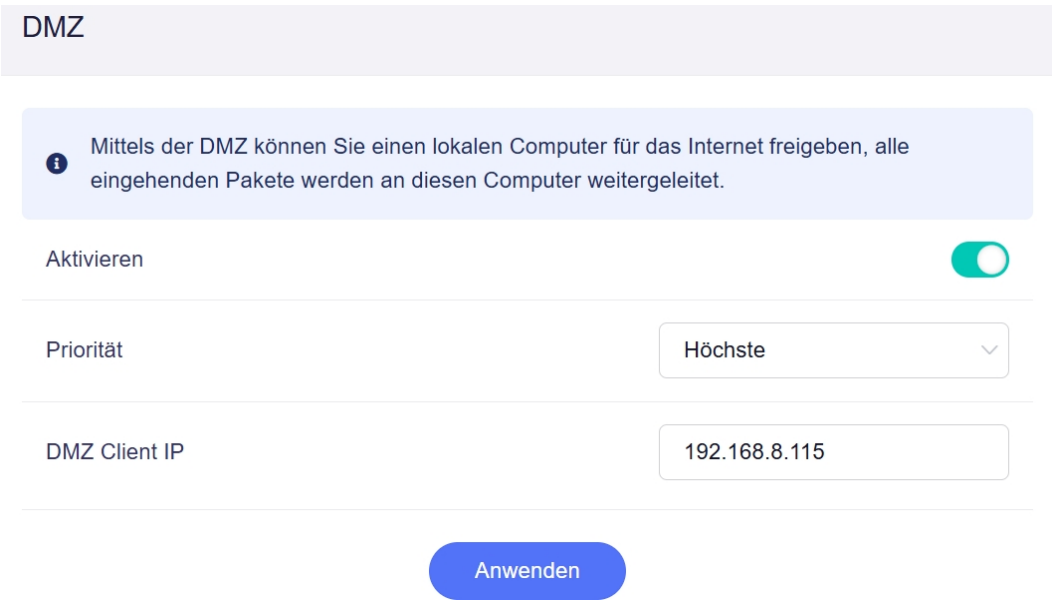
Port-Weiterleitung ist eine Netzwerkfunktion, die externe Anfragen an bestimmte Geräte in Ihrem lokalen Netzwerk weiterleitet. Die Port-Weiterleitungsseite enthält zwei Schlüsselfunktionen: **DMZ** (für direkten Vollzugriff auf ein einzelnes Gerät) und **Port Weiterleitung** (für gezielten Zugriff auf bestimmte Ports von Geräten).

11.1.1 DMZ

DMZ ermöglicht es Ihnen, einen Computer dem Internet auszusetzen, so dass alle eingehenden Pakete auf diesen Computer umgeleitet werden.

Befolgen Sie die folgenden Schritte, um DMZ bei Bedarf zu aktivieren.

1. Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zum **Sicherheit** > **Port weiterleitung** > **DMZ**.
2. Wechseln Sie auf DMZ aktivieren. Wählen Sie die Priorität und DMZ Host IP aus der Dropdown-Liste und klicken Sie auf Anwenden.



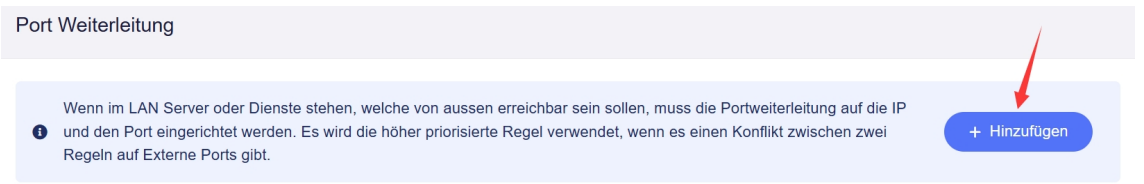
- **Priorität**: Setzen Sie sie als Höchste oder Niedrigste fest. Ist die Priorität der DMZ höher als die Portweiterleitungsregeln, werden alle Portweiterleitungsregeln ungültig. Andernfalls werden Anforderungen nur dann an das DMZ-Clientgerät weitergeleitet, wenn der aufgerufene Port keine entsprechende Portweiterleitungsregel hat.
- **DMZ Client IP**: Wählen Sie die interne IP-Adresse des Geräts aus, das alle eingehenden Pakete empfängt.

11.1.2 Port Weiterleitung

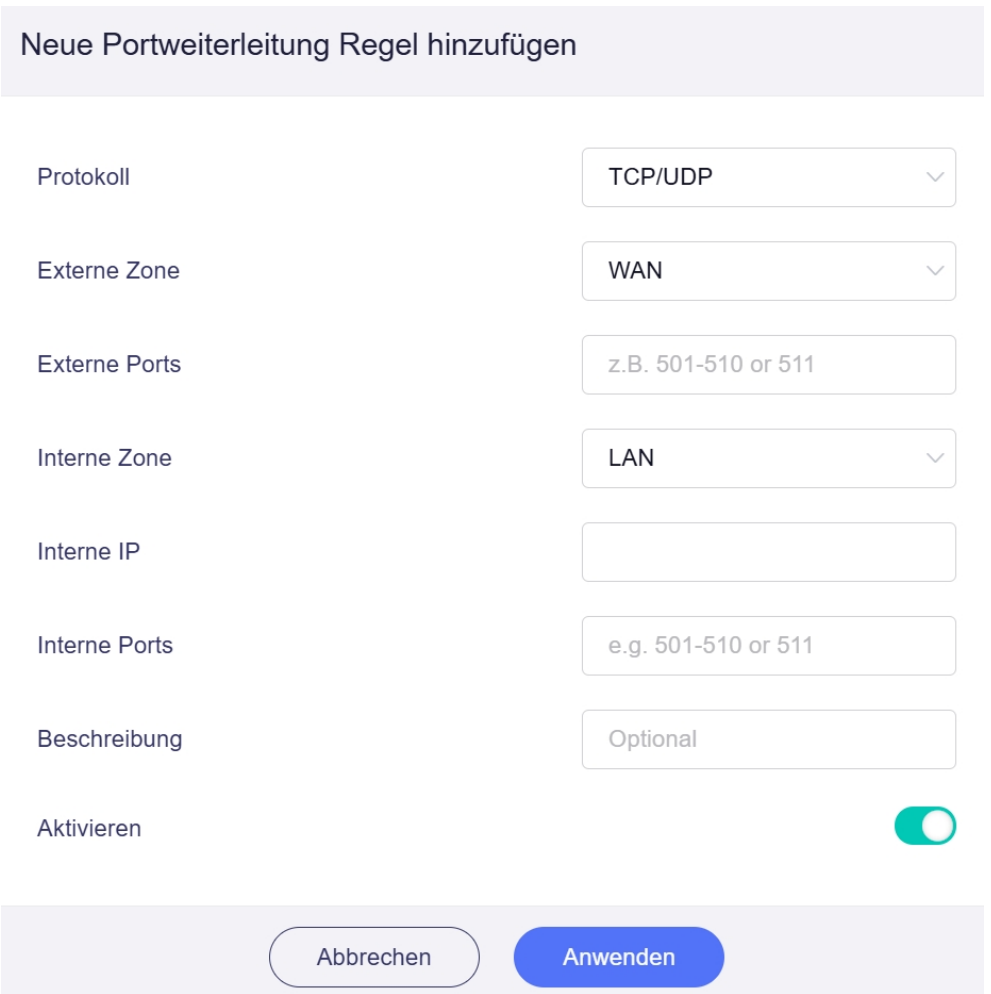
Port Weiterleitung ermöglicht es Remotecomputern, sich mit einem lokalen Computer oder Server hinter der LAN-Firewall zu verbinden (z. B. Webserver, FTP-Server).

Folgen Sie den Schritten unten, um die Portweiterleitung einzurichten, falls erforderlich.

1. Melden Sie sich im Web-Admin-Panel Ihres Routers an, gehen Sie zu **Sicherheit** > **Port Weiterleitung** > **Port Weiterleitung** und klicken Sie auf **Hinzufügen**.



2. Im Popup-Fenster geben Sie die erforderlichen Parameter aus der Dropdown-Liste ein oder wählen Sie sie aus, um eine Portweiterleitungsregel hinzuzufügen, und klicken Sie dann auf **Anwenden**.



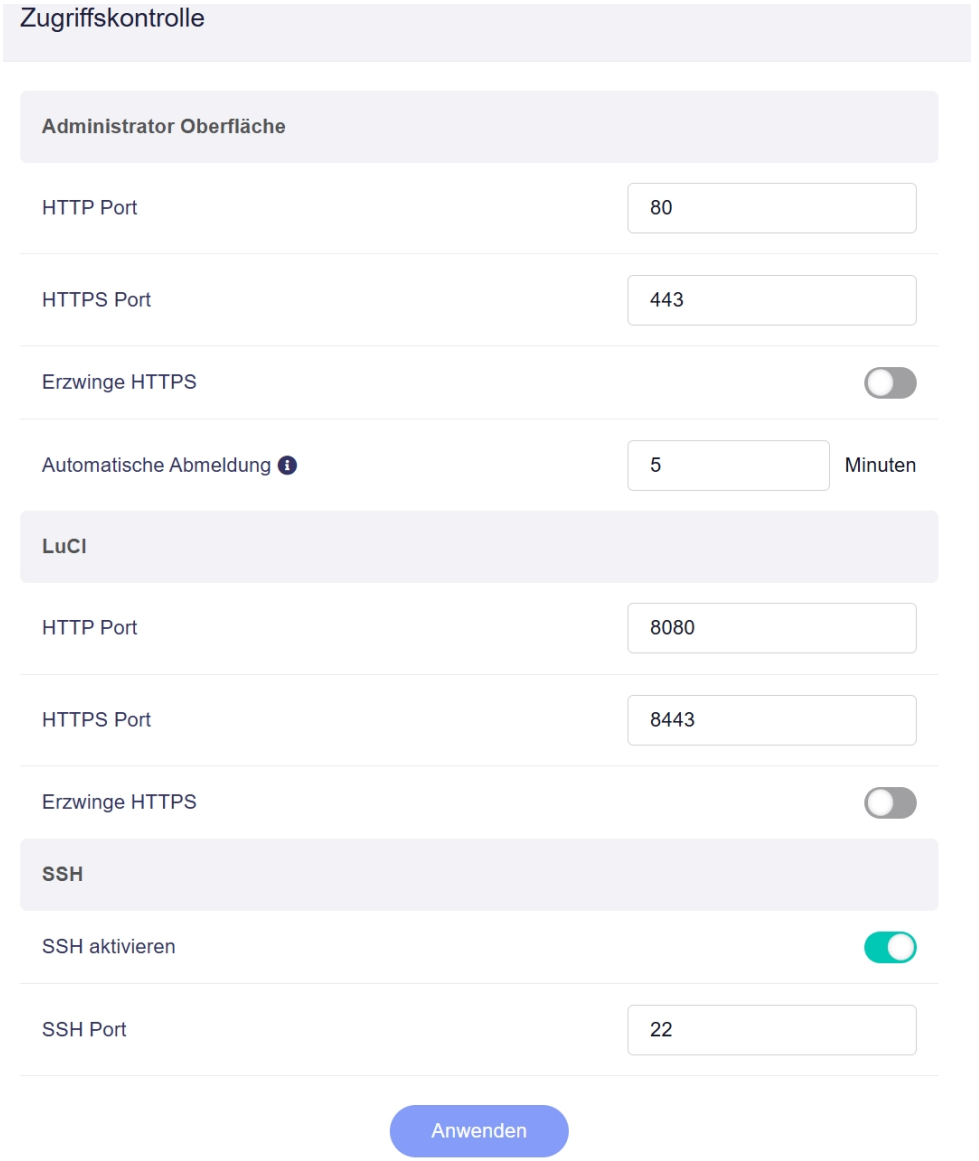
- **Protokoll**: Das verwendete Protokoll. Sie können TCP, UDP oder sowohl TCP als auch UDP wählen.
- **Externe Zone**: Verfügbare Optionen sind WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server und LAN.
- **Externer Ports**: Die Anzahl der externen Ports. Geben Sie hier eine bestimmte Portnummer ein. Der Portbereich ist 1–65535. Sie können einen einzelnen Port oder einen Portbereich festlegen, indem Sie die erste und letzte Portnummer mit einem Bindestrich verknüpfen (z. B. 501-510).
- **Interne Zone**: Verfügbare Optionen sind LAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server und WAN.
- **Interne IP**: Die IP-Adresse, die der Router dem Gerät zuweist, das Fernzugriff benötigt. Wenn Sie unter „External Port“ einen einzelnen Port festlegen, geben Sie hier ebenfalls einen einzelnen Port an. Wenn Sie unter „External Port“ einen Portbereich festlegen, geben Sie hier den entsprechenden Portbereich an.
- **Interner Ports**: Die interne Portnummer des Geräts. Geben Sie eine bestimmte Portnummer ein. Lassen Sie sie leer, wenn sie mit dem externen Port übereinstimmt.
- **Beschreibung**: Legen Sie einen Namen fest oder fügen Sie eine Beschreibung für die Portweiterleitungsregel hinzu (optional).
- **Aktivieren**: Aktivieren oder Deaktivieren dieser Regel.

11.2 Verwaltungssteuerung

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Sicherheit** > **Verwaltungssteuerung**. Auf dieser Seite können Sie den lokalen Routerzugriff, den HTTPS-/SSH-Fernzugriff und offene Ports konfigurieren bzw. verwalten, um Router und Netzwerk vor unbefugtem Zugriff zu schützen.

11.2.1 Zugangskontrolle

Dieser Abschnitt verwaltet den Zugriff auf die mehreren Schnittstellen des Routers (Admin Panel, LuCI und SSH), kann Scan- und Eindringversuche am Standard-Port verhindern und Netzwerkprobleme vermeiden, die durch Portkonflikte verursacht werden.



Admin-Panel

- **HTTP Port**: Standardmäßig 80, verwendet für unverschlüsselten HTTP-Zugriff auf das Web-Admin-Panel.
- **HTTPS Port**: Standardmäßig 443, verwendet für den sicheren HTTPS-Zugriff auf das Web-Admin-Panel.
- **Erzwinge HTTPS**: Wenn aktiviert, wird der Zugriff auf das Web-Admin-Panel erzwungen, um eine sichere HTTPS-Verbindung zu verwenden.
- **Automatische Abmeldung**: Standardmäßig auf 5 Minuten eingestellt, protokolliert es aus Sicherheitsgründen automatisch im Leerlauf befindliche Admin-Sitzungen.

LuCI

Bitte installieren Sie LuCI in den Erweiterten Einstellungen, bevor Sie die Zugriffskontrolle dafür einstellen.

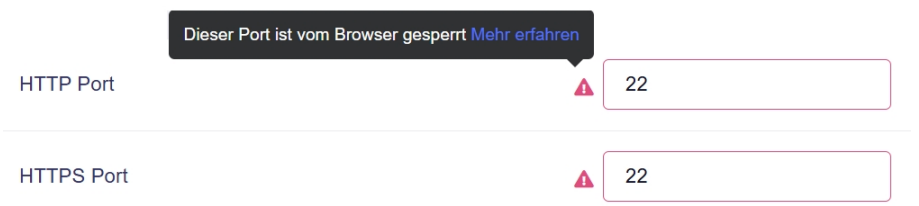
- **HTTP Port**: Standardmäßig 8080 für unverschlüsselten HTTP-Zugriff auf die LuCI-Schnittstelle.
- **HTTPS Port**: Standardmäßig 8443 für sicheren HTTPS-Zugriff auf die LuCI-Schnittstelle.
- **Erzwinge HTTPS**: Wenn aktiviert, wird der Zugriff auf die LuCI-Schnittstelle erzwungen, um eine sichere HTTPS-Verbindung zu verwenden.

SSH

- **SSH aktivieren**: Standardmäßig aktiviert, steuert es, ob der SSH-Zugriff auf den Router erlaubt ist.
- **SSH Port**: Standardmäßig 22, der Port, der für den SSH-Zugriff auf den Router verwendet wird.

Hinweis:

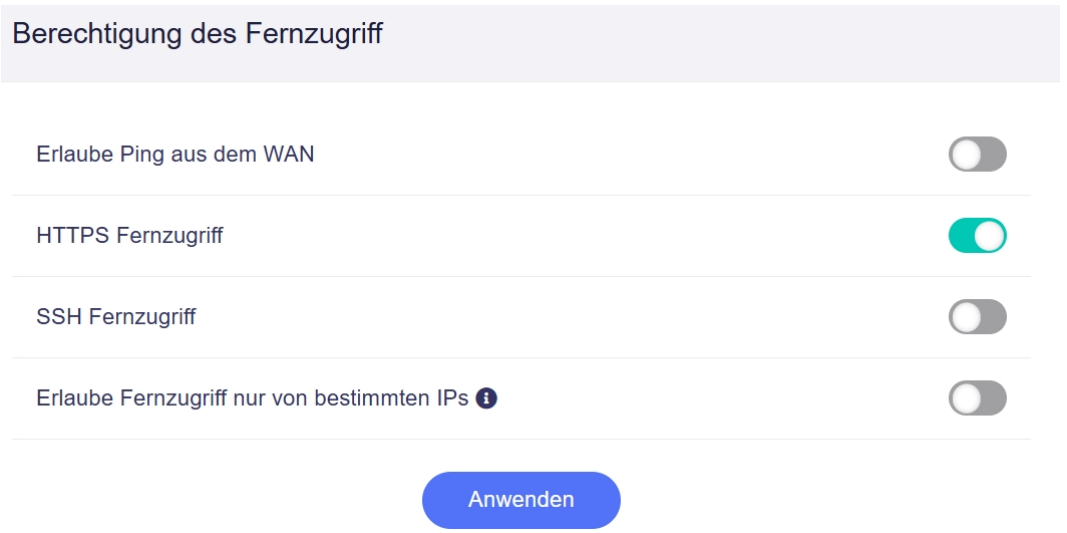
1. Wenn Sie eine Portnummer zuweisen, die mit einem reservierten Port kollidiert (oder einer, die für bestimmte Dienste von Browsern / Netzwerkkonventionen reserviert ist), wird eine Aufforderung mit der Aufschrift "Dieser Port ist vom Browser verboten" angezeigt.



2. Wenn die Portnummer in der Firmware geändert wurde, müssen Sie die richtige Portnummer eingeben, um auf das Admin-Panel zuzugreifen.

11.2.2 Berechtigung des Fernzugriff

Dieser Abschnitt verwaltet den Fernzugriff auf Router-Schnittstellen, einschließlich HTTPS, SSH und WAN-seitigem Ping. Er ermöglicht es Ihnen auch, den Zugriff von bestimmten IP-Adressen aus zu beschränken und ein Gleichgewicht zwischen Fernzugriff und Netzwerksicherheit herzustellen.

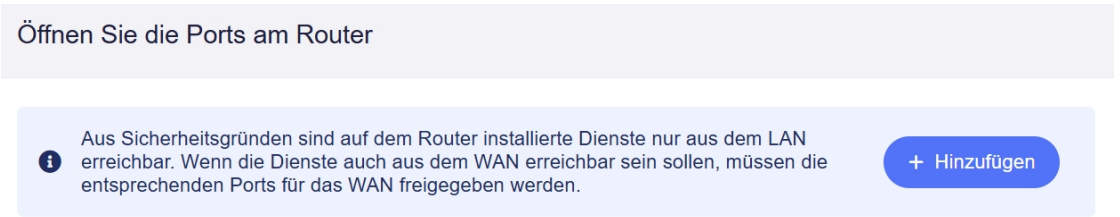


- **Erlaube Ping aus dem WAN**: Das Ermöglichen von Ping von der WAN-Seite des Routers kann Benutzern helfen, zu überprüfen, ob der Router über das WAN erreichbar ist, wenn ein Netzwerkproblem vorliegt, sowie die Netzwerklatenz und den Paketverlust zu bestimmen.
- **HTTPS Fernzugriff**: HTTPS Remote Access ermöglicht einen sicheren Fernzugriff auf das Web-Admin-Panel des Routers über das HTTPS-Protokoll. Es gewährleistet eine verschlüsselte Datenübertragung bei der Fernverwaltung des Routers über einen Webbrowser.
- **SSH Fernzugriff**: Diese Funktion ermöglicht einen sicheren Zugriff auf das Router-Terminal. Benutzer können den Router über SSH aus der Ferne verwalten und für ihre Aufgaben einen verschlüsselten Tunnel aufbauen.
- **Erlaube Fernzugriff nur von bestimmten IPs**: Diese Funktion ist nur verfügbar, wenn eine der drei oben genannten Funktionen aktiviert ist. Sie können mehrere IP-Adressen hinzufügen, damit der Router nur von Geräten mit diesen IP-Adressen aus fernverwaltet werden kann.

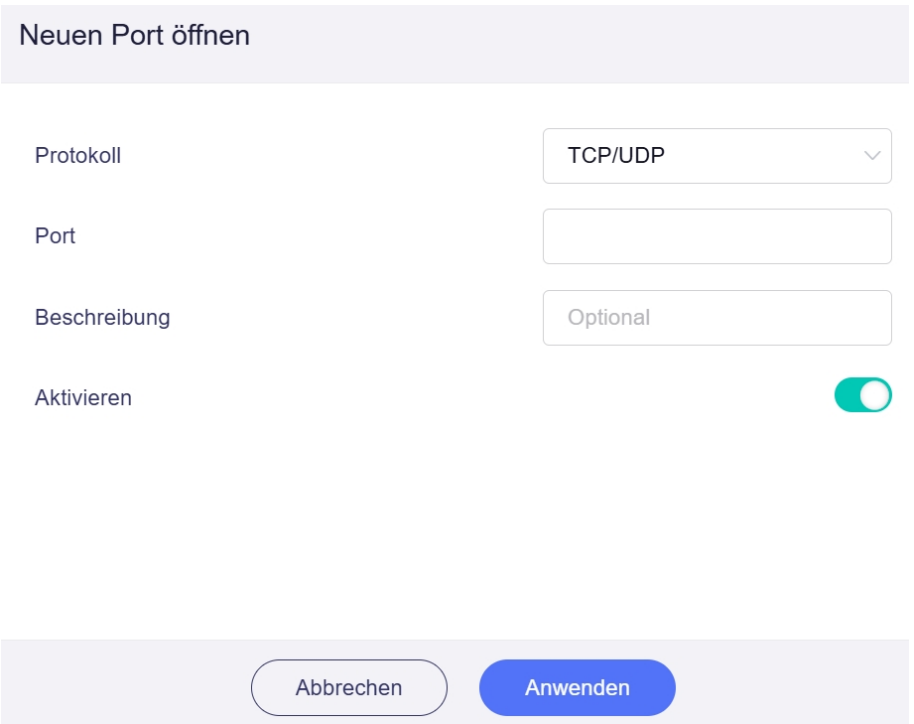


11.2.3 Öffnen Sie die Ports am Router

In diesem Abschnitt wird die Portweiterleitung für Dienste auf Ihrem Router verwaltet. Einige Dienste, wie Web und FTP, erfordern, dass ihre jeweiligen Ports auf dem Router geöffnet werden, um vom WAN-Netzwerk aus öffentlich erreichbar zu sein. Aus Sicherheitsgründen sind auf dem Gerät installierte Dienste standardmäßig nur im LAN zugänglich. Wenn Sie einen solchen WAN-Zugriff aktivieren müssen, können Sie bestimmte Ports hier öffnen.



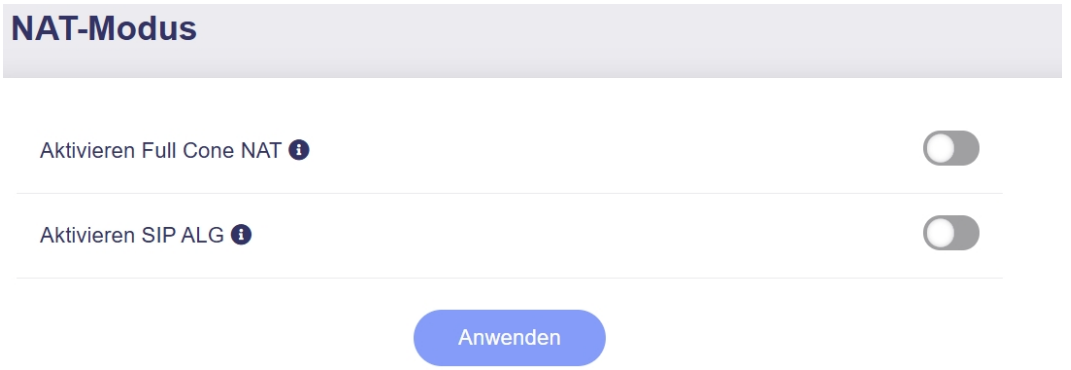
Um einen Port zu öffnen, klicken Sie auf **Hinzufügen** und geben Sie die erforderlichen Informationen im Popup-Fenster ein.



- **Protokoll**: Wählen Sie das Netzwerkprotokoll (TCP, UDP oder TCP/UDP) für den Port aus, das bestimmt, wie Daten für den mit dem Port verbundenen Dienst übertragen werden.
- **Port**: Geben Sie die spezifische Portnummer ein, die Sie öffnen möchten.
- **Beschreibung** (optional): Fügen Sie eine kurze Notiz hinzu, um den Zweck dieses offenen Ports (z. B. "Web Server" oder "FTP Service") für eine einfachere Verwaltung zu beschreiben.
- **Aktivieren**: Umschalten dieses Schalters, um die Port-Weiterleitungsregel zu aktivieren oder zu deaktivieren.

11.3 NAT-Modus

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zum **Sicherheit** > **NAT-Modus**. Diese Seite ermöglicht es Ihnen, zwei wichtige NAT-bezogene Funktionen zu konfigurieren: Full Cone NAT und SIP ALG.



- **Aktivieren Full Cone NAT**: Es kann verwendet werden, um die Latenzzeit von Spielen zu reduzieren und die Reaktionsfähigkeit von Online-Spielen zu verbessern, aber die Aktivierung von Full Cone NAT ist möglicherweise weniger sicher, da es uneingeschränkte eingehende Verbindungen ermöglicht.
- **Aktivieren SIP ALG**: Es soll die Auswirkungen mehrerer NATs auf den SIP-Datenverkehr (Session Initiation Protocol) mildern, in den meisten Fällen hilft es jedoch nicht und kann sogar VoIP-Anrufe beeinflussen, was zu Problemen wie Einweg-Audio, Telefone, die nicht klingeln, unerwartete Anrufe oder Anrufe führt direkt an Voicemail.

Kapitel 12

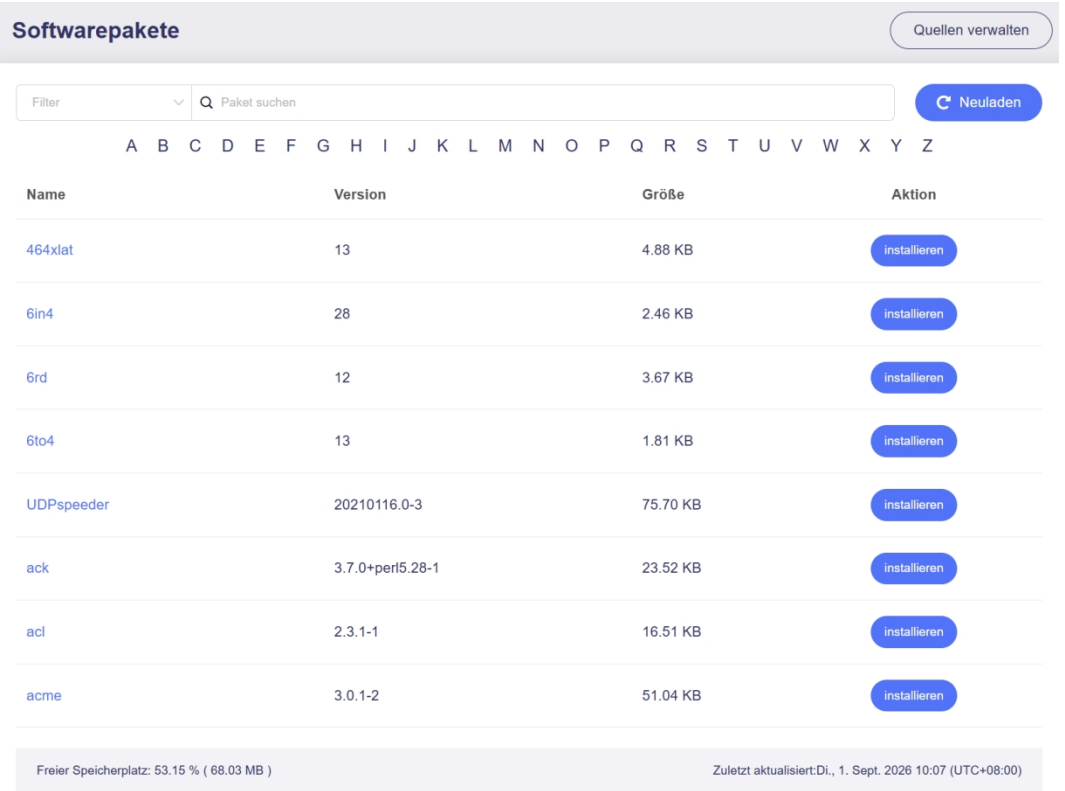
Anwendungen

In diesem Kapitel werden einige Anwendungen in GL.iNet-Routern vorgestellt, z. B. Softwarepakete, Dynamisches DNS, Netzwerk-Speicher und Tailscale.

12.1 Softwarepakete

Die Softwarepakete-Seite ermöglicht es Ihnen, OpenWrt-Pakete zu verwalten.

Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Anwendungen** > **Softwarepakete**. Sie können jedes im Repository verfügbare Paket installieren oder entfernen. Klicken Sie vor der Installation von Plug- ins auf die Schaltfläche **Neuladen**, um die Paketliste zu aktualisieren.



Hinweis:

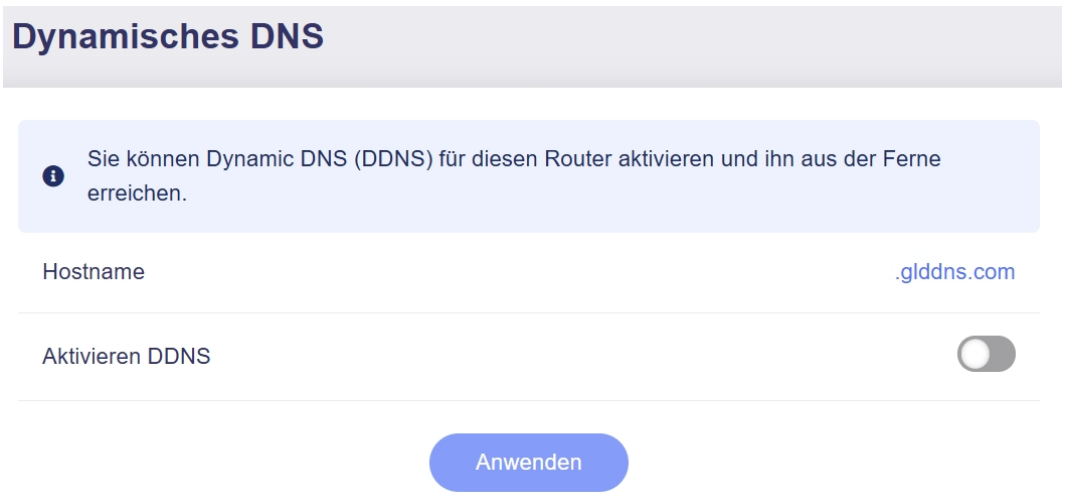
1. Es wird nicht empfohlen, vorinstallierte Softwarepakete in der offiziellen Firmware von GL.iNet zu aktualisieren, wie z. B. nginx, adguard home, tailscale usw.
2. Von Nutzern manuell installierte Plugins von Drittanbietern können aktualisiert werden; GL.iNet haftet jedoch nicht für Sicherheitsprobleme von Drittanbieter-Plugins.

12.2 Dynamisches DNS

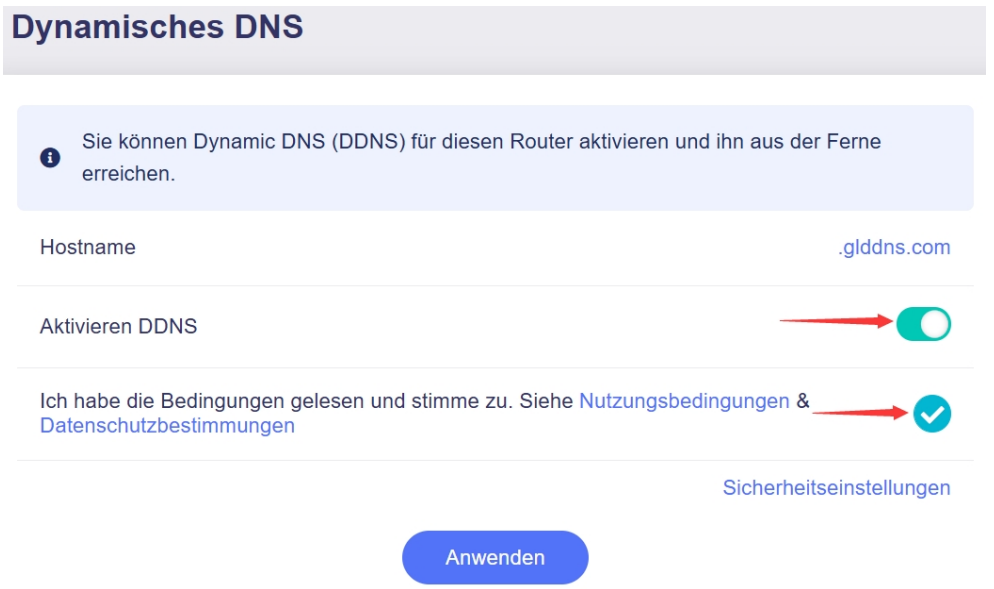
Dynamischer Domain Name Service (DDNS oder Dynamisches DNS) ist ein Dienst, der verwendet wird, um einen Domainnamen der dynamischen IP-Adresse eines Netzwerkgeräts zuzuordnen. Mit Dynamischem DNS können Sie aus der Ferne auf Ihren Router zugreifen. Eine öffentliche IP-Adresse ist für diese Funktionalität erforderlich.

12.2.1 DDNS aktivieren

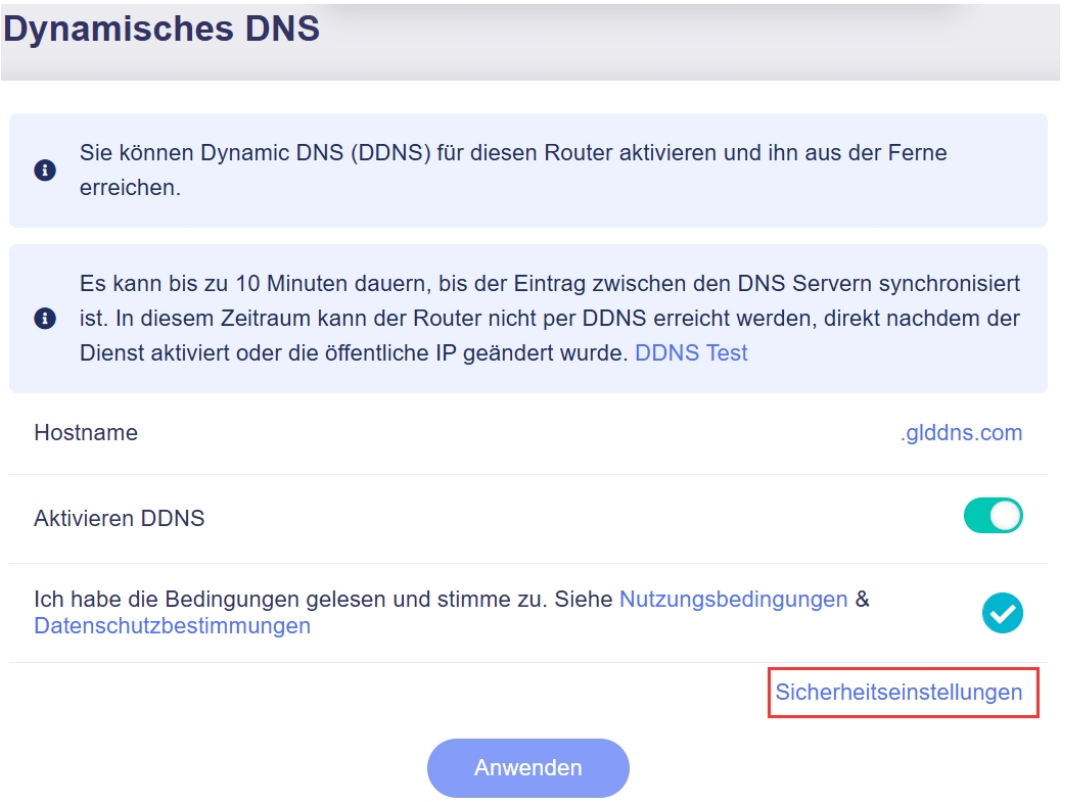
1. Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Anwendungen** > **Dynamisches DNS**, die Seite wird wie unten angezeigt.



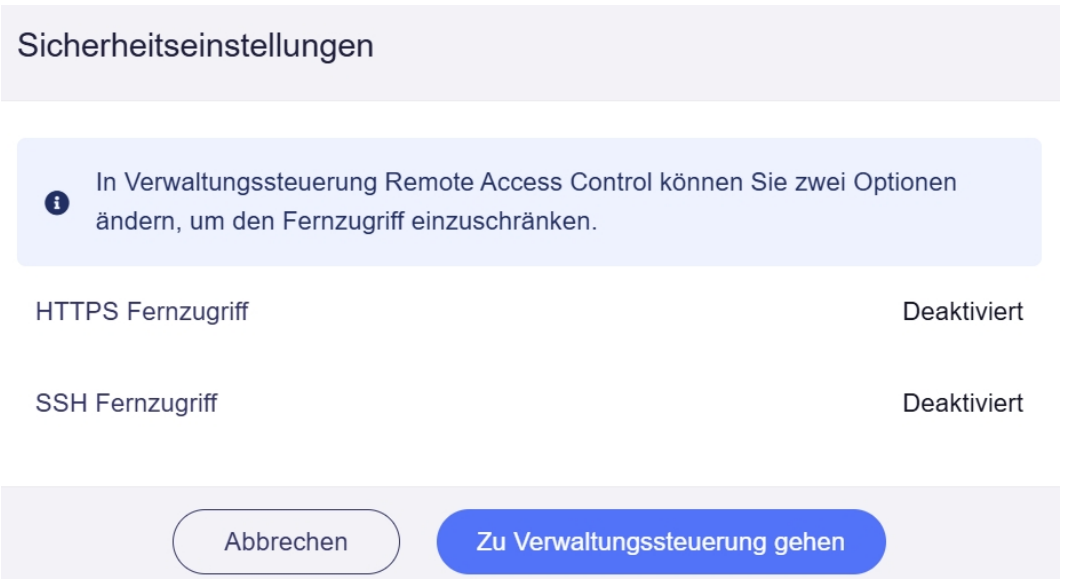
2. Umschalten auf DDNS aktivieren, lesen und stimmen Sie die **Nutzungsbedingungen & Datenschutzbestimmungen,** und klicken Sie dann auf **Anwenden**.



3. Klicken Sie auf **Sicherheitseinstellungen** in der unteren rechten Ecke.



4. Überprüfen Sie im Popup-Fenster, ob der Fernzugriff, den Sie verwenden möchten, aktiviert ist.



Wenn nicht, gehen Sie zu **Sicherheit** > **Verwaltungssteuerung** > **Berechtigung des Fernzugriff**, um es zu aktivieren, und klicken Sie auf Anwenden.



Hinweis:

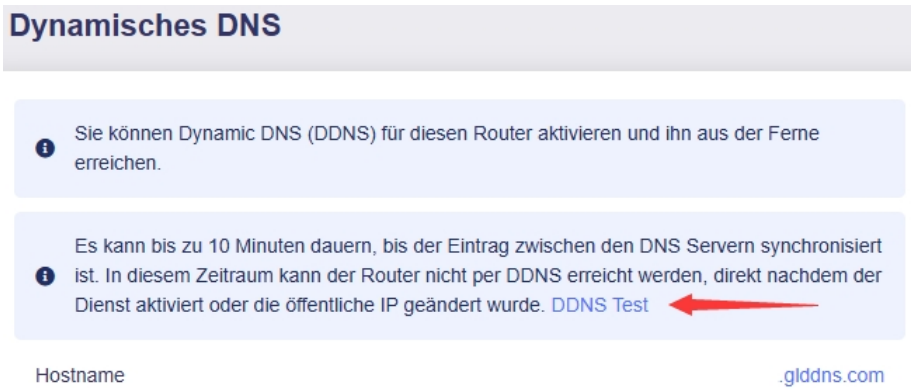
1. Es kann zu einer Verzögerung von bis zu 10 Minuten bei der Datensatzsynchronisation zwischen DNS-Servern kommen, was Sie möglicherweise daran hindert, unmittelbar nach der Aktivierung oder bei Änderungen Ihrer öffentlichen IP über den DDNS-Domänennamen zuzugreifen.
2. Wenn Sie DDNS und VPN Client gleichzeitig aktivieren, stellen Sie sicher, dass Services From GL.iNet Use VPN deaktiviert ist.

12.2.2 Prüfen Sie, ob DDNS funktioniert

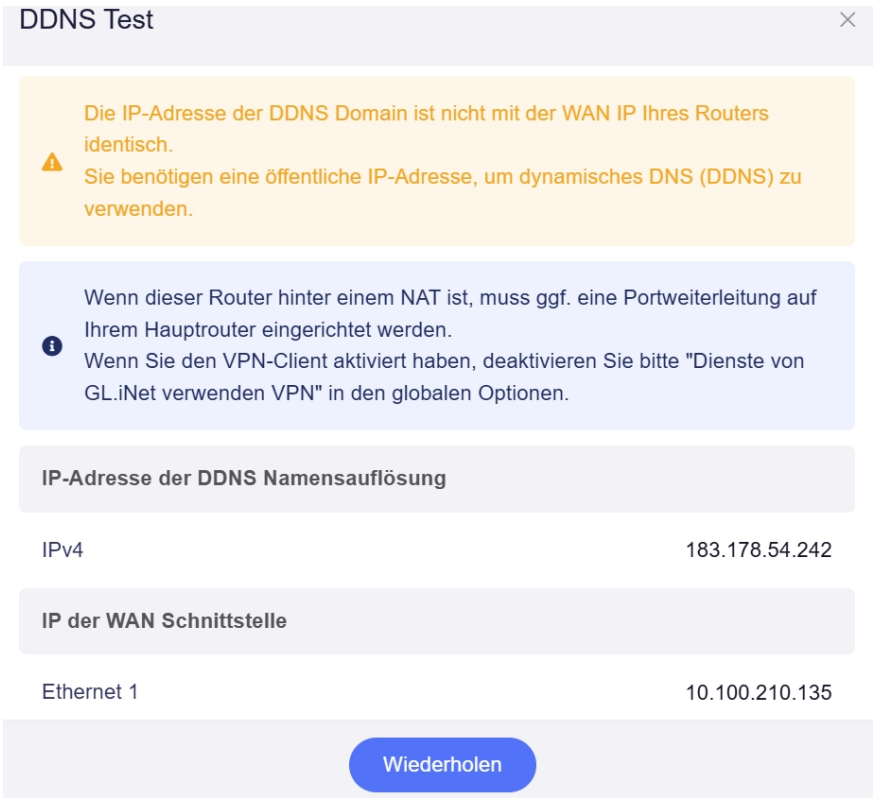
Ob DDNS funktioniert, können Sie mit dem DDNS-Testtool oder manuell über Befehle überprüfen.

Methode 1. DDNS-Test-Tool verwenden

1. Klicken Sie auf der Seite Dynamisches DNS auf den **DDNS Test**.



2. Stellen Sie sicher, dass die IP-Adresse von DDNS-Domänenauflösung mit der WAN-IP des Routers übereinstimmt. Wenn nicht, wird oben eine gelbe Eingabeaufforderung angezeigt, die anzeigt, dass der Router möglicherweise hinter NAT liegt, und Sie müssen die Portweiterleitung auf dem vorgelagerten Router einrichten.



Methode 2. Befehle verwenden

1. Verwenden Sie den Befehl *nslookup nslookup* xxxxxxx.glddns.com 8.8.8.8, um die Zuordnung zwischen Domainname und IP-Adresse zu erhalten.



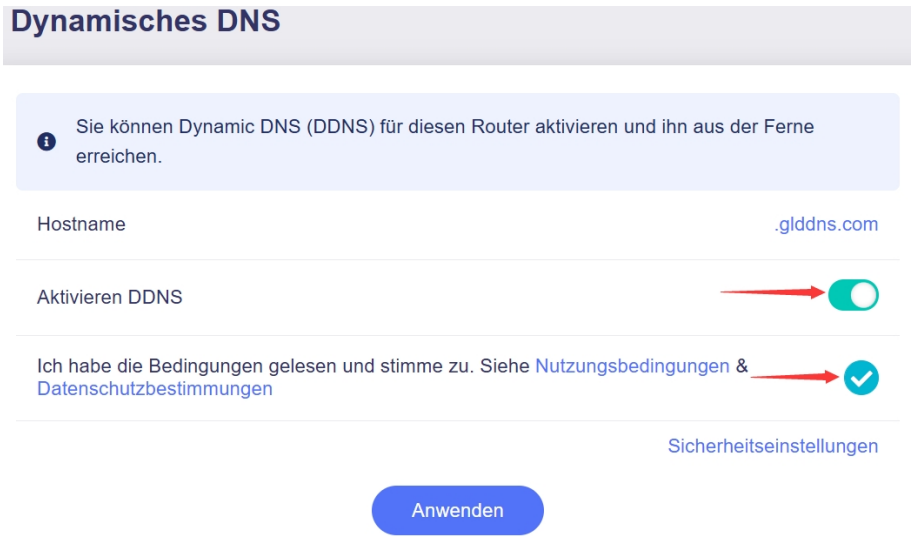
   - Ersetzen Sie "xxxxxxx.glddns.com" im Bild oben mit Ihrem Host-Namen.
   - Das „8.8.8.8 ist das Google DNS. Verwenden Sie es oder ersetzen Sie es durch andere, und drücken Sie dann Enter.
2. Wenn Sie eine öffentliche IP-Adresse wie „183.178.10.100“ im obigen Bild erhalten, zeigt dies an, dass Ihre DDNS-Domäne erfolgreich einer öffentlichen IP-Adresse zugeordnet wurde. Wenn Sie eine Nachricht wie „Server kann xxxxxxx.glddns.com nicht finden“ erhalten, kann dies darauf hinweisen, dass die Domänenauflösung fehlgeschlagen ist und Ihre DDNS-Domäne nicht erfolgreich einer öffentlichen IP-Adresse zugeordnet wurde.
3. Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zum Internet. Finden Sie die WAN-IP-Adresse Ihres Routers in der aktuellen aktiven Benutzeroberfläche. Vergleichen Sie diese IP-Adresse mit der oben erhaltenen öffentlichen IP-Adresse. Wenn sie gleich sind, ist das DDNS in Kraft, andernfalls ist es nicht.

12.2.3 HTTPS Fernzugriff

Für den HTTPS-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Klicken Sie hier, um zu prüfen, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Befindet sich Ihr Router hinter NAT, richten Sie für den HTTPS-Zugriff auf dem vorgelagerten Router eine Portweiterleitung für **Port 443** ein.

Befolgen Sie die folgenden Schritte, um den HTTPS-Fernzugriff für Ihren Router zu aktivieren.

1. Auf der Dynamischen DNS-Seite wechseln Sie auf **Aktivieren DDNS,** stimmen den **Nutzungsbedingungen & Datenschutzbestimmungen,** und klicken Sie dann auf **Anwenden**.

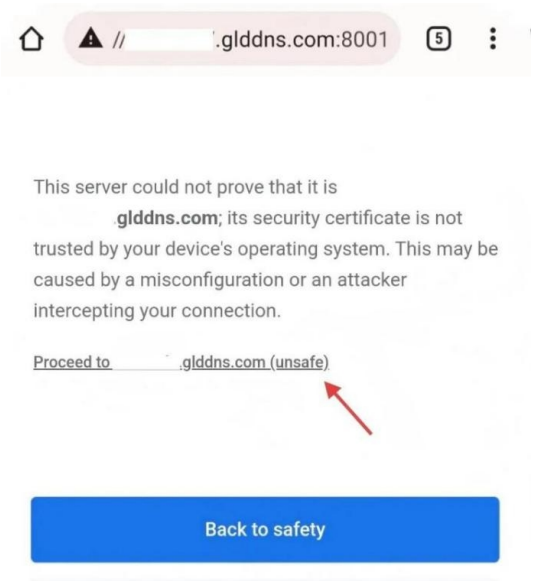


2. Gehen Sie im Web-Admin-Panel zu **Sicherheit** > **Verwaltungssteuerung** > **Berechtigung des Fernzugriff**. Aktivieren Sie **HTTPS Fernzugriff** und klicken Sie auf **Anwenden**.



Sobald die Funktion aktiviert ist, können Sie von überall über HTTPS und den DDNS-Hostnamen auf das Admin-Panel des Routers zugreifen, z. B. über **https://xxxxxxx.glddns.com**. Wenn eine Portweiterleitung eingerichtet ist, verwenden Sie **https://xxxxxxx.glddns.com:external_port** und ersetzen external_port durch Ihre tatsächliche Portnummer.

Hinweis: Diese Funktion verwendet selbstsignierte Zertifikate; Daher zeigen Browser "Ihre Verbindung ist nicht privat" an, wenn Sie über den DDNS-Hostnamen über HTTPS auf das Administrator-Panel des Routers zugreifen. Um mit dem HTTPS-Fernzugriff fortzufahren, klicken Sie unten auf **Advanced** und anschließend auf Proceed to **xxxxxxx.glddns.com**, um fortzufahren.



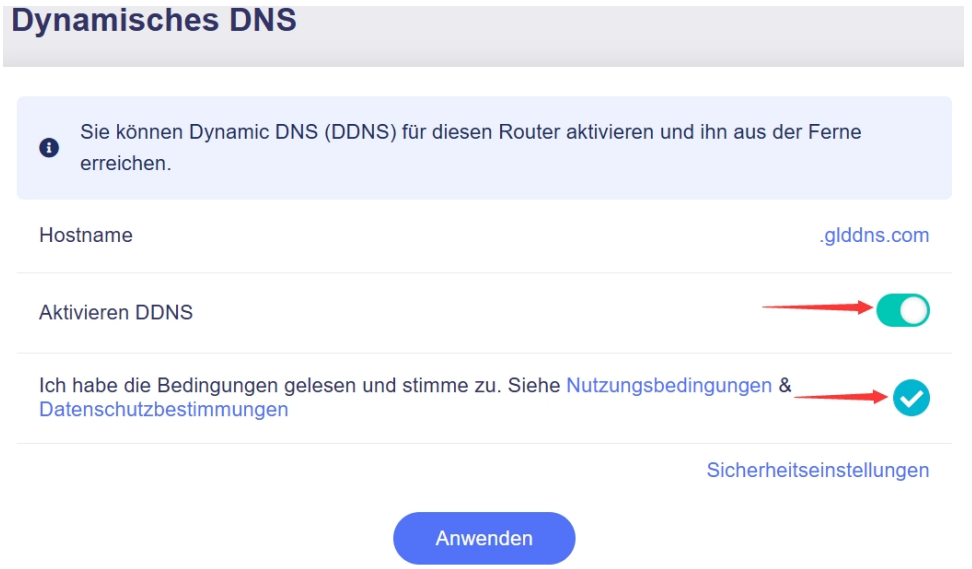
Sie können dann mit dem DDNS-Hostnamen über **HTTPS** auf das Web-Admin-Panel des Routers zugreifen.

12.2.4 SSH Fernzugriff

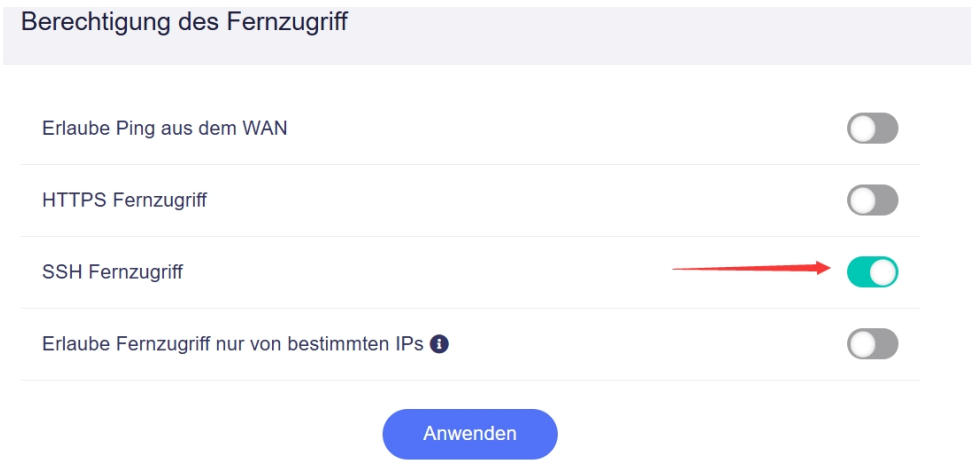
Für den SSH-Fernzugriff ist eine **öffentliche IP-Adresse** erforderlich. Klicken Sie hier, um zu prüfen, ob Ihr Internetanbieter Ihnen eine öffentliche IP-Adresse zuweist. Befindet sich Ihr Router hinter NAT, richten Sie für den SSH-Fernzugriff auf dem vorgelagerten Router eine Portweiterleitung für **Port 22** ein.

Befolgen Sie die folgenden Schritte, um den SSH-Fernzugriff für Ihren Router zu aktivieren.

1. Auf der Dynamischen DNS-Seite wechseln Sie auf **Aktivieren DDNS,** stimmen den **Nutzungsbedingungen & Datenschutzbestimmungen,** und klicken Sie dann auf **Anwenden**.



2. Gehen Sie im Web-Admin-Panel zu **Sicherheit** > **Verwaltungssteuerung** > **Berechtigung des Fernzugriff**. Aktivieren Sie **SSH-Fernzugriff** und klicken Sie auf **Anwenden**.



Einmal aktiviert, können Sie von überall aus mit dem DDNS-Hostnamen über SSH auf das Administrator-Panel des Routers zugreifen, z. B. **ssh root@xxxxxxxxx.glddns.com**. Wenn die Portweiterleitung konfiguriert ist, greifen Sie als ssh **root@xxxxxxxxx.glddns.com:external_port** zu (ersetzen Sie den externen_port durch Ihre tatsächliche Portnummer).

12.3 Netzwerk-Speicher

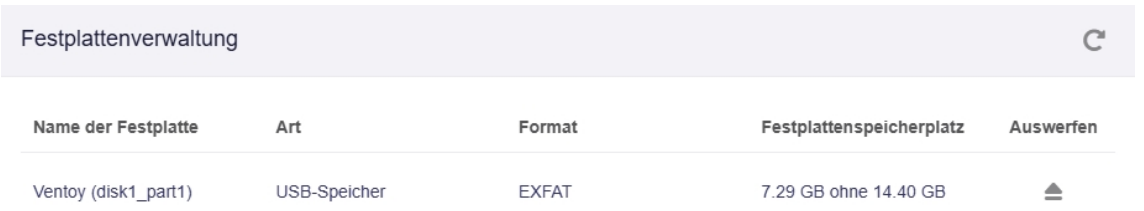
Netzwerk-Speicher ermöglicht die drahtlose Dateifreigabe über Geräte hinweg, indem ein USB-Laufwerk oder eine SD-Karte an Ihren Router angeschlossen wird. Der Router wandelt das Speichergerät in ein gemeinsames Netzwerklaufwerk um, auf das alle mit Wi-Fi verbundenen Geräte zugreifen können.

Mango 2 ist mit einem USB-Anschluss ausgestattet, der mit USB-Sticks und tragbaren externen Festplatten kompatibel ist. Sie können Samba für diese Speichergeräte mit gängigen Formaten wie NTFS, FAT32 und EXT4 konfigurieren.

Hinweis: Der Stromverbrauch der USB-Festplatte ist recht hoch. Verwenden Sie sie mit einem externen Netzteil, da sonst eine Fehlfunktion auftreten kann.

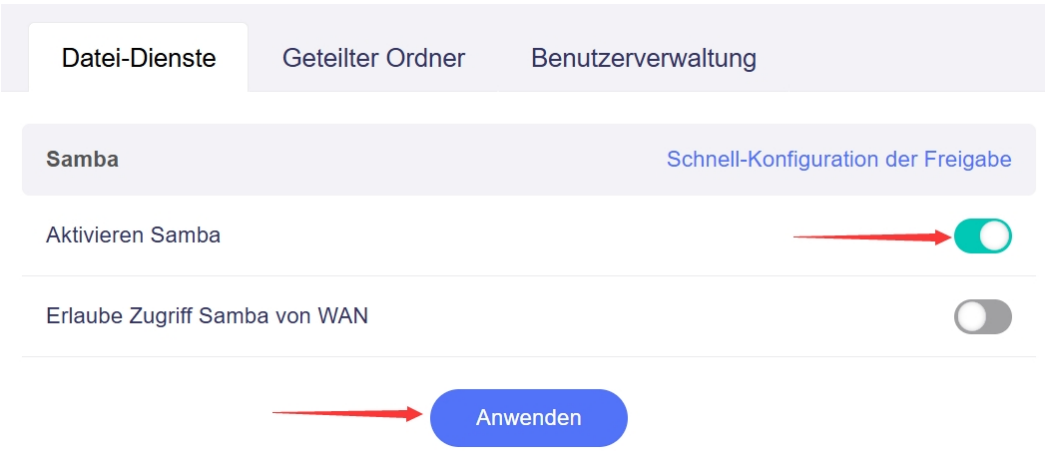
12.3.1 Speicher verbinden

1. Verbinden Sie Ihr Speichergerät mit dem Router.
   - Für ein USB-Laufwerk: Schließen Sie es direkt an den USB-Anschluss an.
   - Für eine externe Festplatte: Verbinden Sie sie mit einem separaten Netzteil (falls erforderlich), und schließen Sie sie dann an den Router an.
2. Melden Sie sich im Web-Admin-Panel Ihres Routers an, navigieren Sie zu **Anwendungen** > **Netzwerk-Speicher**. Sie können Dateiübertragungsdienste aktivieren und den freigegebenen Ordner hier verwalten.
3. Wenn das Speichergerät erkannt wird, wird die Datenträgerverwaltung wie folgt angezeigt.



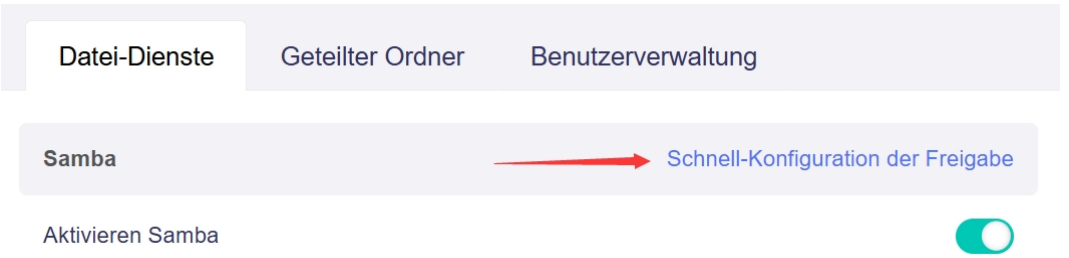
12.3.2 Setup von Samba

1. Aktivieren Sie im Bereich **Datei-Dienste** die Option Aktivieren Samba und klicken Sie auf **Anwenden**.



   - **Erlaube Zugriff Samba von WAN**: Aktivieren Sie es, wenn Sie möchten, dass vorgelagerte Geräte auf den Samba-Dienst zugreifen können.

2. Klicken Sie auf **Schnell-Konfiguration der Freigabe**, um den freigegebenen Link festzulegen.



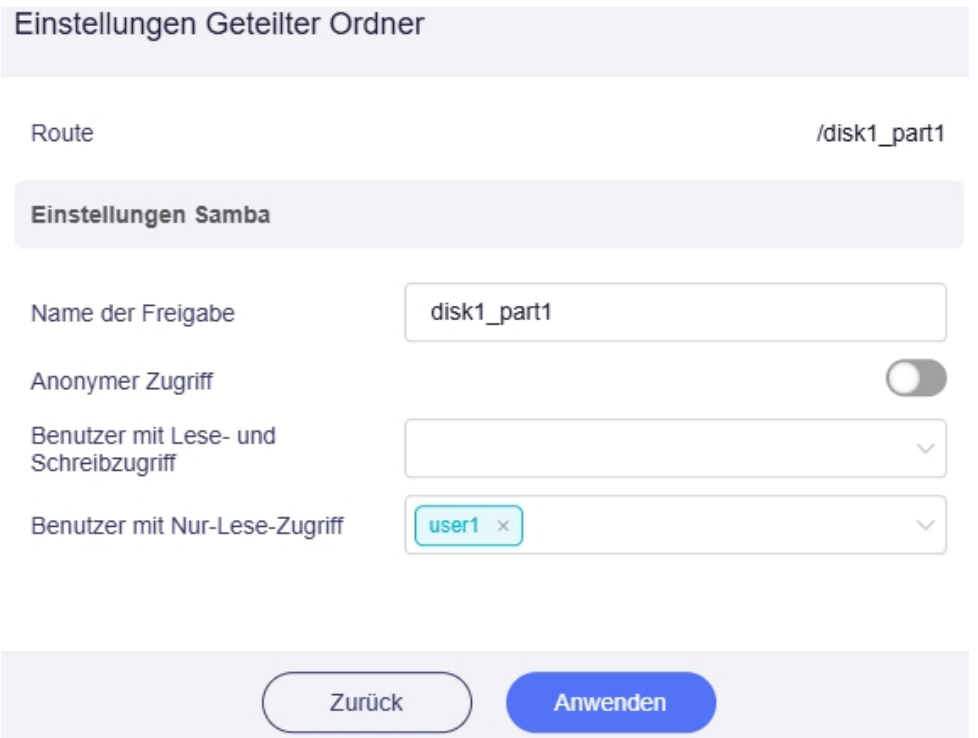
3. Fügen Sie einen Benutzer hinzu und klicken Sie auf Weiter. Dieser Schritt wird übersprungen, wenn Sie bereits ein Konto haben.



4. Klicken Sie auf das Dreieckssymbol, um alle Ordner anzuzeigen. Wählen Sie einen Ordner zum Teilen aus, und klicken Sie auf **Weiter**. Wenn Sie die gesamte Festplatte teilen möchten, klicken Sie auf den Festplattennamen (z. B. disk1_part1).

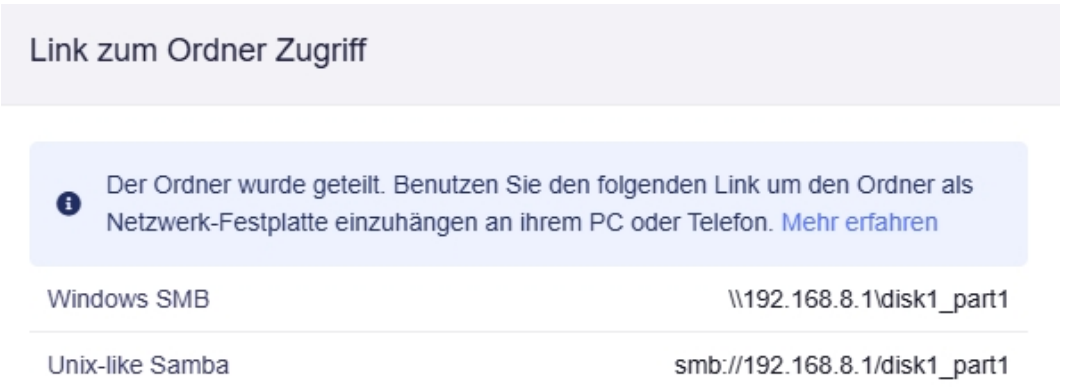


5. Richten Sie den freigegebenen Ordner ein.
   Aus Sicherheitsgründen ist es nicht empfehlenswert, Anonymous Access zu aktivieren. Der im vorherigen Schritt erstellte Benutzer wird standardmäßig zu **Benutzer mit Nur-Lese-Zugriff** hinzugefügt. Wenn Sie möchten, dass dieser Benutzer Dateien schreiben oder löschen kann, entfernen Sie sie aus Benutzer mit Nur-Lese-Zugriff und fügen Sie sie zu **Benutzer mit Lese- und Schreibzugriff** hinzu, und klicken Sie dann auf **Anwenden**.



Tipp: Aus Sicherheitsgründen wird es nicht empfohlen, Anonymous Access zu aktivieren.

6. Besorgen Sie sich den Ordner-Zugriffslink.
   Die Seite zeigt die Links für Windows und Unix-ähnliches Betriebssystem an. Das Unix-ähnliche System umfasst Android, iOS, macOS, Ubuntu usw. Jetzt können Sie über diesen Link über den Samba-Dienst auf Ihren freigegebenen Ordner zugreifen.



Hinweis: Wenn Sie **Erlaube Zugriff Samba von WAN** zulassen und über ein vorgelagertes Netzwerk auf den freigegebenen Ordner zugreifen, ersetzen Sie die Router-IP (Standard: 192.168.8.1) im Zugriffslink mit der WAN-IP Ihres Routers, die auf der internet-Seite des Web-Admin-Panels zu finden ist.

12.4 Tailscale

Tailscale ist ein VPN-Dienst, der Ihre persönlichen Geräte und Anwendungen weltweit sicher und mühelos zugänglich macht.

Die Tailscale-Funktion auf GL.iNet-Routern ermöglicht es dem Router, einem virtuellen Tailscale-Netzwerk beizutreten, was den Fernzugriff auf den Router selbst sowie seine WAN- und LAN-seitigen Ressourcen ermöglicht.

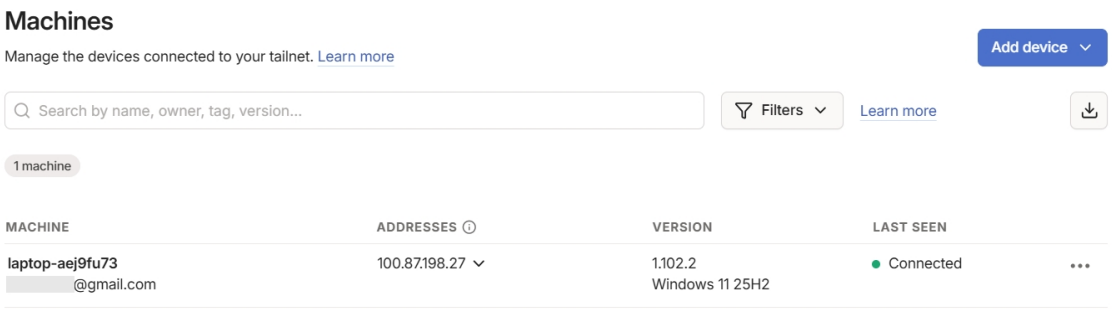
Hinweis:

1. Da Tailscale auf WireGuard basiert, wird es nicht empfohlen, Tailscale mit einer der folgenden Funktionen oder Dienste gleichzeitig zu verwenden, da dies zu Routing-Konflikten führen kann: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier, GoodPAS.
2. Diese Funktion befindet sich derzeit in der Beta und kann einige Bugs haben.

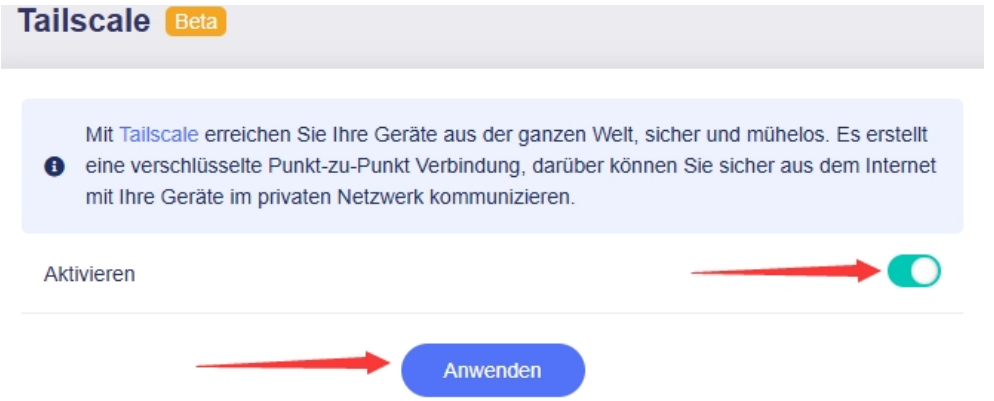
12.4.1 Tailscale einrichten

Hier ist ein Beispiel für die Verwendung von GL-MG1300 zum Einrichten des Tailscale-Netzwerks.

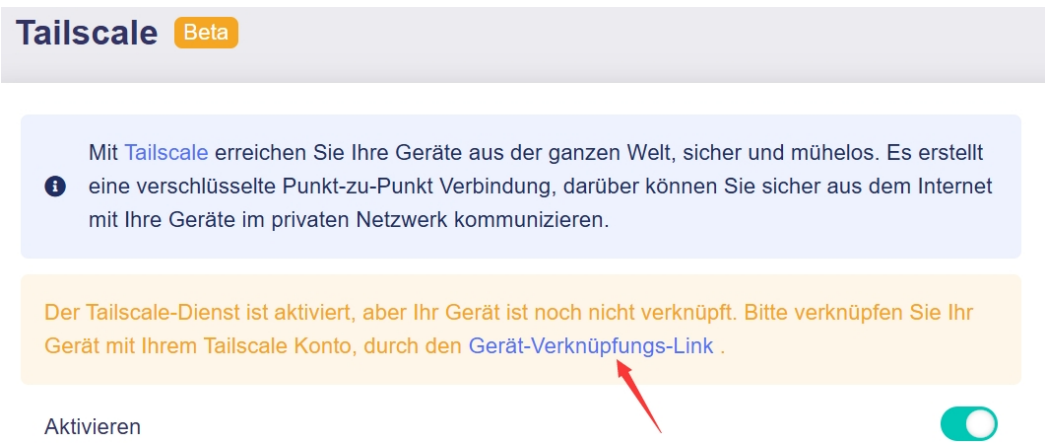
1. Registrieren Sie zuerst ein Tailscale-Konto und binden Sie ein oder zwei Geräte zu Testzwecken an Ihr Tailscale-Konto.



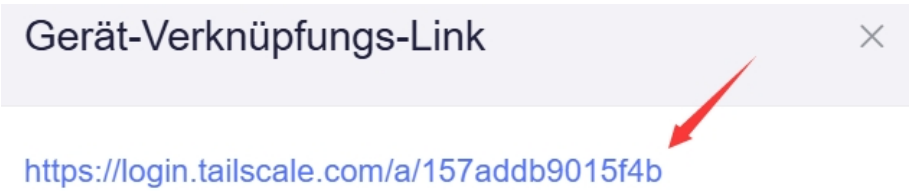
2. Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **Anwendungen** > **Tailscale**. Wechseln Sie auf Tailscale aktivieren und klicken Sie auf **Anwenden**.



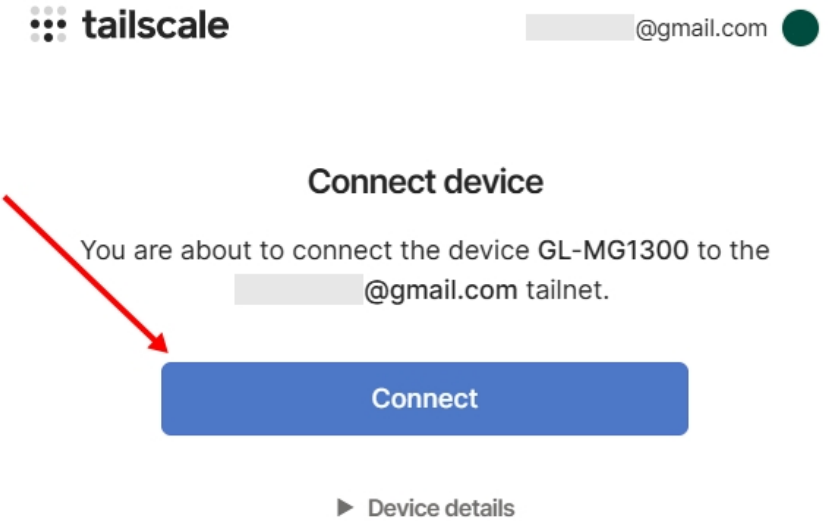
3. Auf der Seite werden Sie aufgefordert, das Gerät zu binden. Klicken Sie auf **Gerät-Verknüpfungs-Link**.



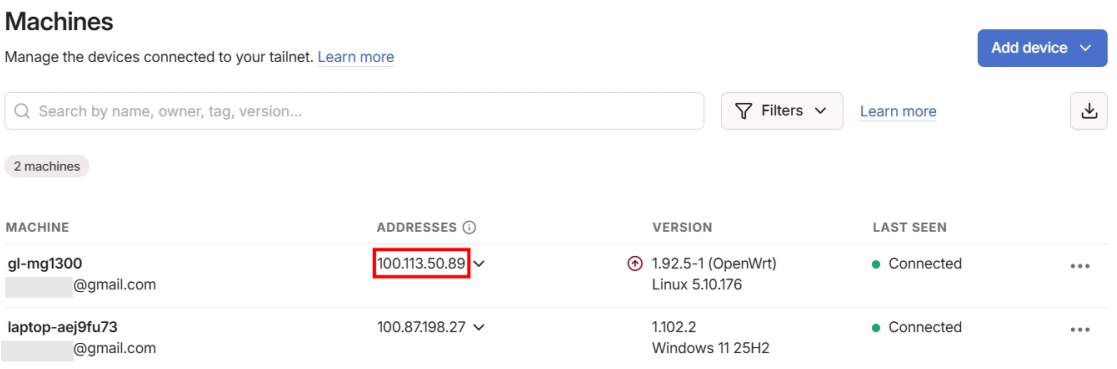
4. Klicken Sie im Popup-Fenster auf den Link und melden Sie sich mit Ihrem Tailscale-Konto an.



5. Nach der Anmeldung werden Sie aufgefordert, das Gerät zu bestätigen. Klicken Sie auf **Connect**.



6. Sie werden anschließend zur Tailscale-Adminkonsole weitergeleitet. Der Router wurde nun zum virtuellen Tailscale-Netzwerk hinzugefügt und kann über die virtuelle Tailscale-IP-Adresse 100.113.50.89 aus der Ferne aufgerufen werden.



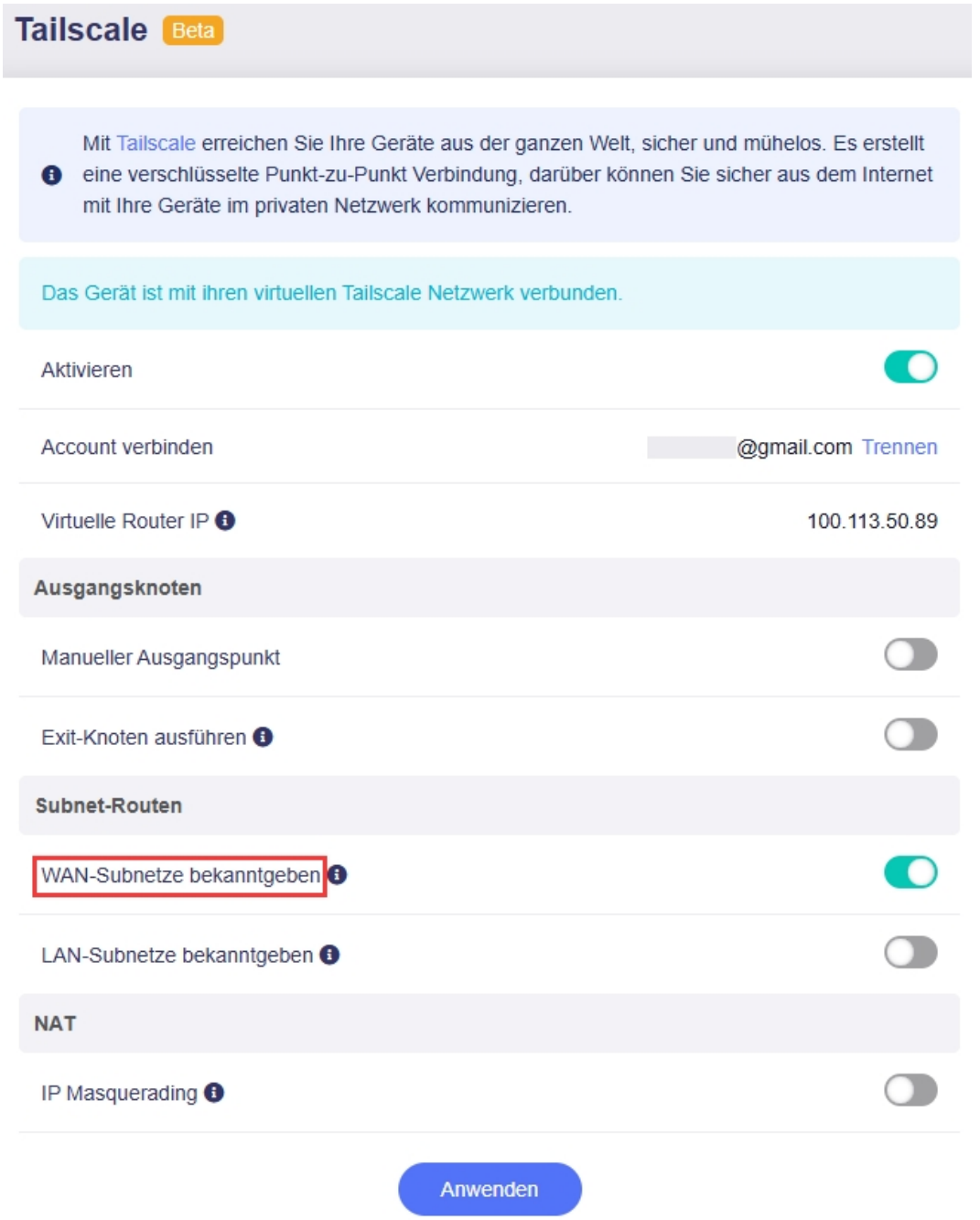
7. Konnektivität testen.

   Auf einem anderen Gerät, das mit demselben Tailscale-Netzwerk verbunden ist, öffnen Sie einen Webbrowser und geben Sie die virtuelle IP des Routers in die Adressleiste ein.

Wenn Sie auf das Web-Admin-Panel des Routers zugreifen können, bedeutet dies, dass Tailscale funktioniert. Sie können sich auch mit dem Ping-Befehl oder SSH-Anmeldung am Terminal des Routers über seine virtuelle IP anmelden, um die Konnektivität zu testen.

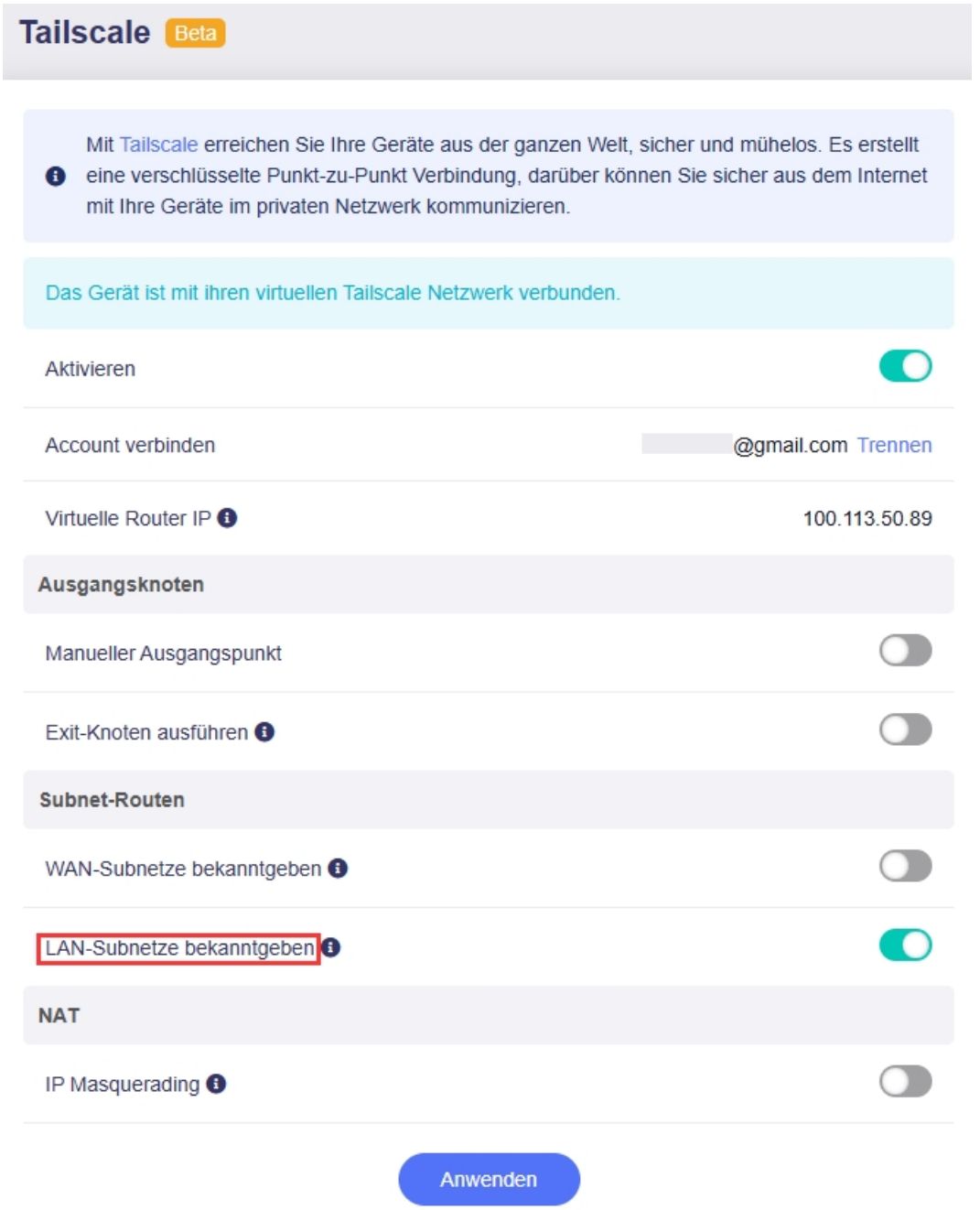
12.4.2 WAN-Subnetze bekanntgeben

Wenn diese Option aktiviert ist, können Ressourcen auf der WAN-Seite des Geräts über das virtuelle Tailscale-Netzwerk aufgerufen werden.



12.4.3 LAN-Subnetze bekanntgeben

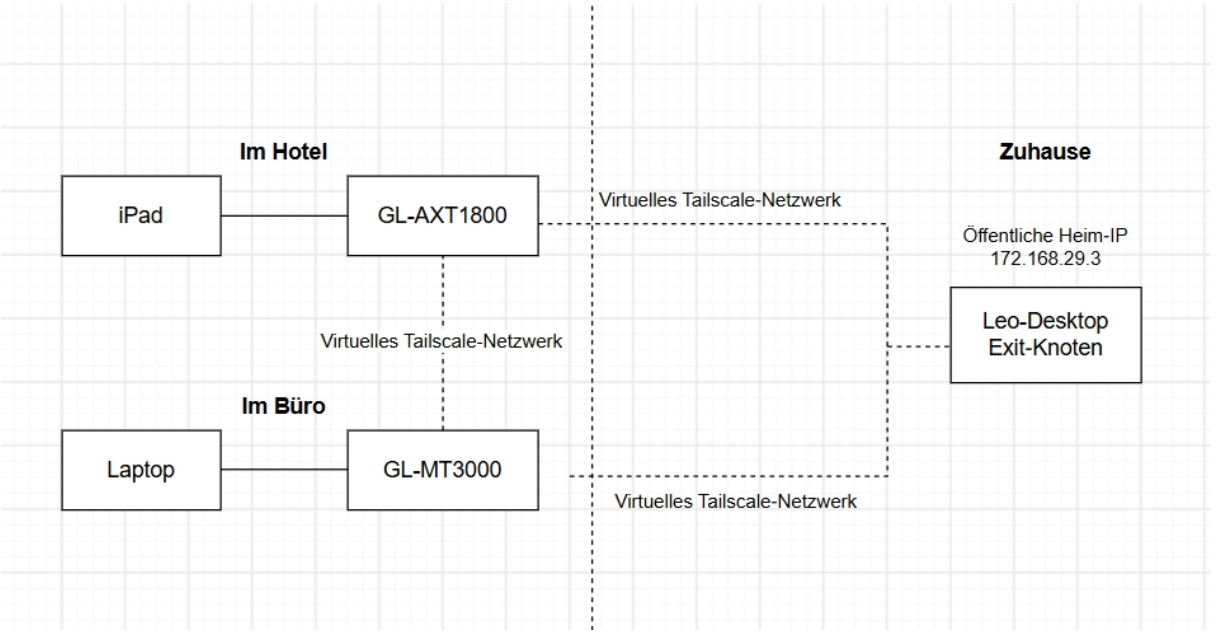
Wenn diese Option aktiviert ist, können Ressourcen auf der LAN-Seite des Geräts über das virtuelle Netzwerk Tailscale aufgerufen werden.



12.4.4 Manueller Ausgangspunkt

Standardmäßig fungiert Tailscale als Overlay-Netzwerk: Es leitet nur den Datenverkehr zwischen Geräten mit Tailscale und verarbeitet nicht Ihren öffentlichen Internetverkehr - beispielsweise beim Durchsuchen von Websites wie Google.

Es kann jedoch vorkommen, dass Sie Ihren öffentlichen Internet-Datenverkehr über Tailscale leiten möchten. Wenn Sie beispielsweise nicht zu Hause sind oder ins Ausland reisen und auf Online-Dienste wie Bankgeschäfte zugreifen müssen, die nur in Ihrem Heimatland verfügbar sind, können Sie Ihren Heimcomputer mit öffentlicher IP-Adresse als Exit-Knoten einrichten und andere Geräte im selben Tailnet – etwa GL-AXT1800 und GL-MT3000 im folgenden Bild – so konfigurieren, dass sie ihren Datenverkehr darüber senden. Ihr öffentlicher Internetverkehr wird dann über den Exit-Knoten weitergeleitet.



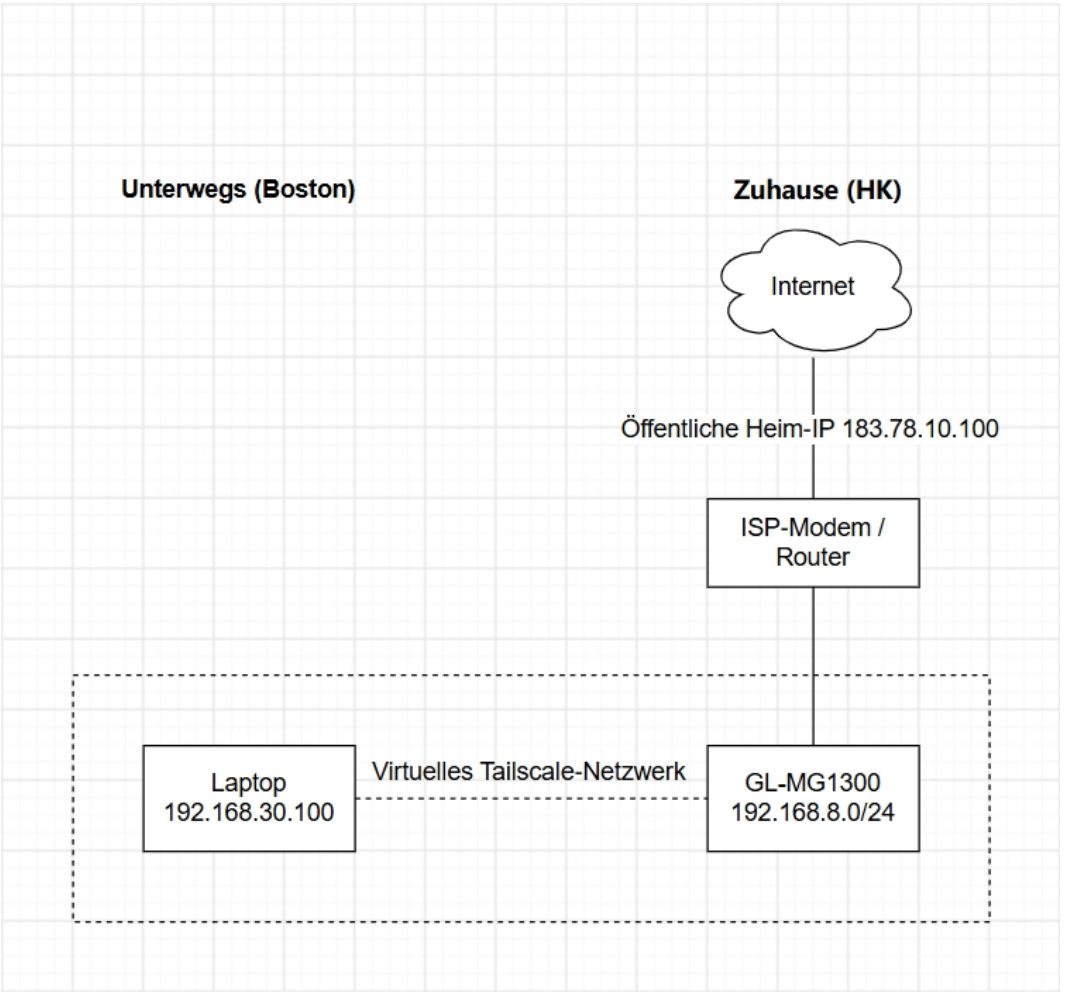
Zusammenfassend leitet ein Exit-Knoten ausgehenden Internet-Datenverkehr von Ihren Tailnet-Geräten, effektiv als VPN-Server. Wenn Sie mit einem Exit-Knoten verbunden sind, scheint der gesamte nicht-Tailscale-Internet-Datenverkehr von seinem Standort aus zu stammen, was Ihnen den Zugriff auf geo-eingeschränkte Inhalte und die Verbesserung Ihrer Online-Privatsphäre erleichtert. Das Gerät, das diese Datenverkehrsweiterleitung verarbeitet, wird als "Exit-Knoten" bezeichnet.

Hinweis: Wenn der DNS-Server des Routers eine private IP-Adresse ist, auf die nur im lokalen Netzwerk zugegriffen werden kann, können Sie beim Ausführen der Exit-Knoten den Internetzugang verlieren.

12.4.5 Exit-Knoten ausführen

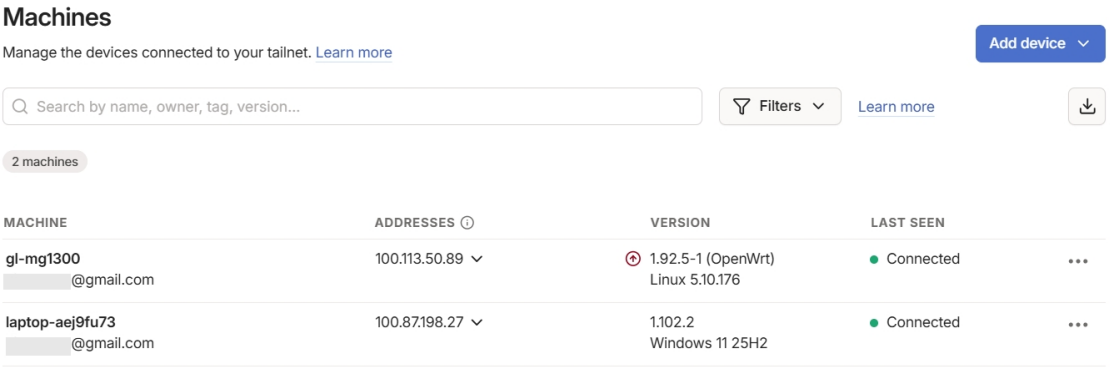
Durch das Ausführen eines Exit-Knotens auf Ihrem Router können andere Geräte in Ihrem Tailnet den gesamten ausgehenden Internetverkehr über die öffentliche IP dieses Routers leiten.

In der folgenden Topologie befindet sich ein Laptop in Boston und ein Router GL-MG1300 in Hongkong. Beide wurden demselben Tailscale-Netzwerk hinzugefügt. Wenn Sie den GL-MG1300 als Exit-Knoten festlegen, wird der gesamte ausgehende Datenverkehr des Laptops über diesen Router ins Internet geleitet. Die öffentliche IP-Adresse des Laptops wird dann als Hongkonger statt als Bostoner IP-Adresse aufgelöst.

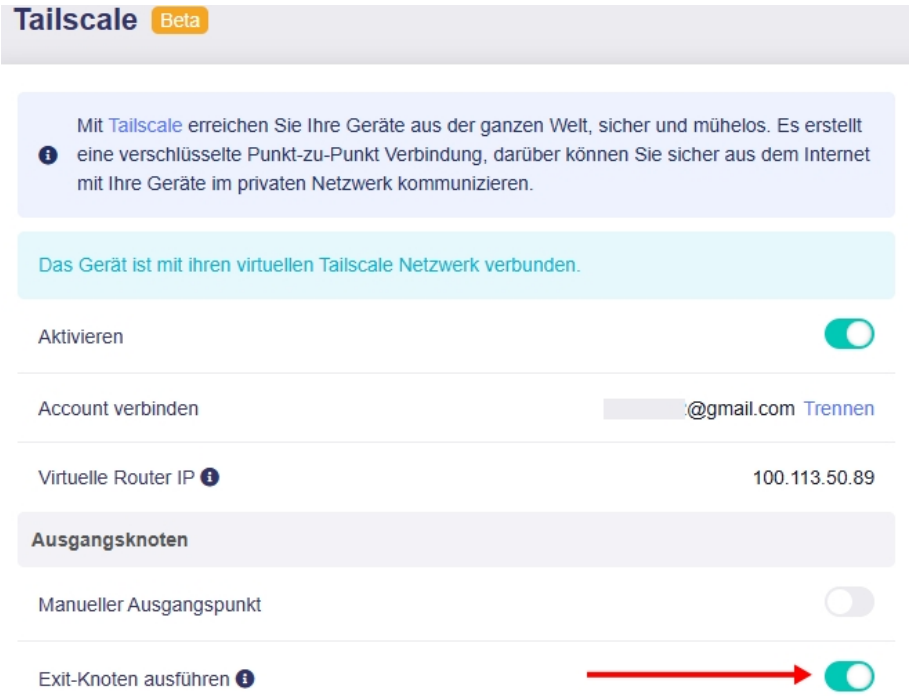


Hier sind die Schritte, um den GL-MG1300 als Exit-Knoten einzurichten.

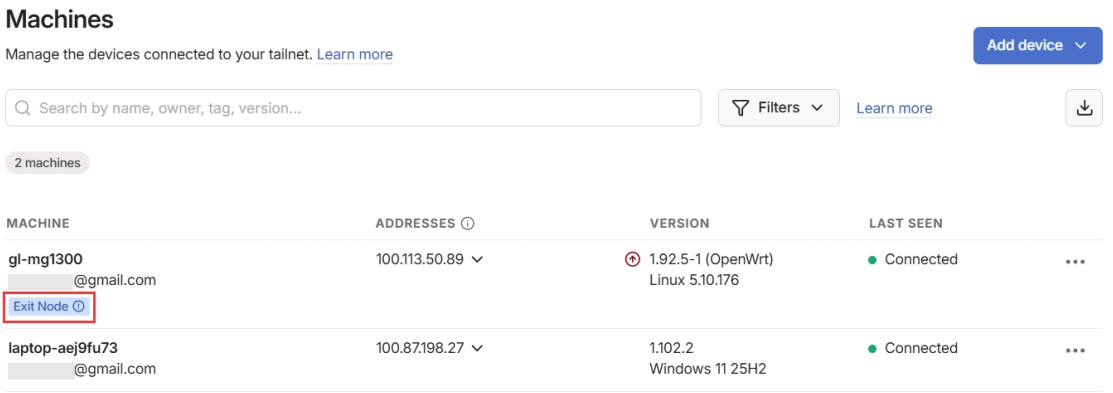
1. Melden Sie sowohl den Router GL-MG1300 als auch den Reise-Laptop an demselben Tailscale-Tailnet an.



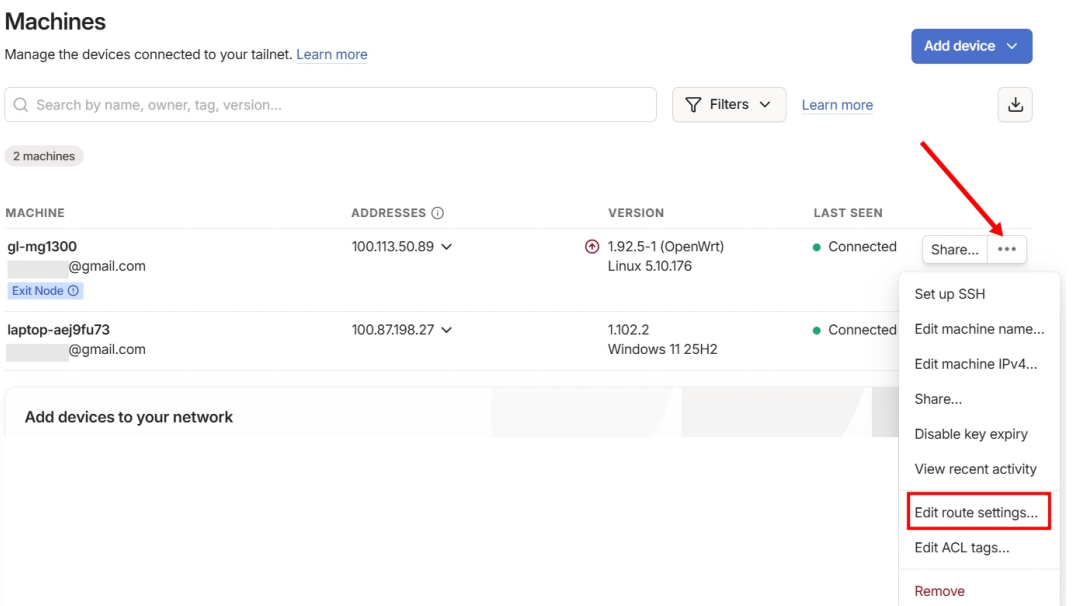
2. Gehen Sie im GL-MG1300 Webadministratorfeld zu **Anwendungen** > **Tailscale.** aktivieren Sie Exit-Knoten ausführen und klicken Sie auf **Anwenden**.



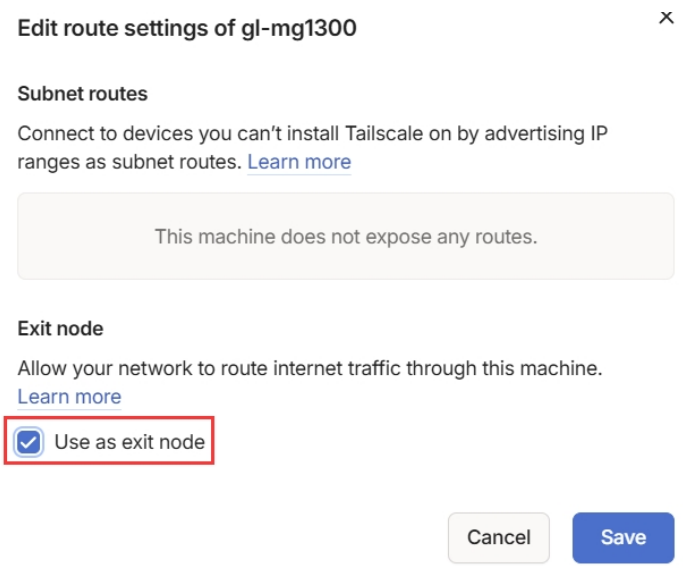
3. Gehen Sie zur Tailscale Admin Console und Sie sehen ein Tag "Exit Node" unter dem GL-MG1300.



4. Klicken Sie auf das Drei-Punkt-Symbol rechts von GL-MG1300 und wählen Sie **Edit route settings**.



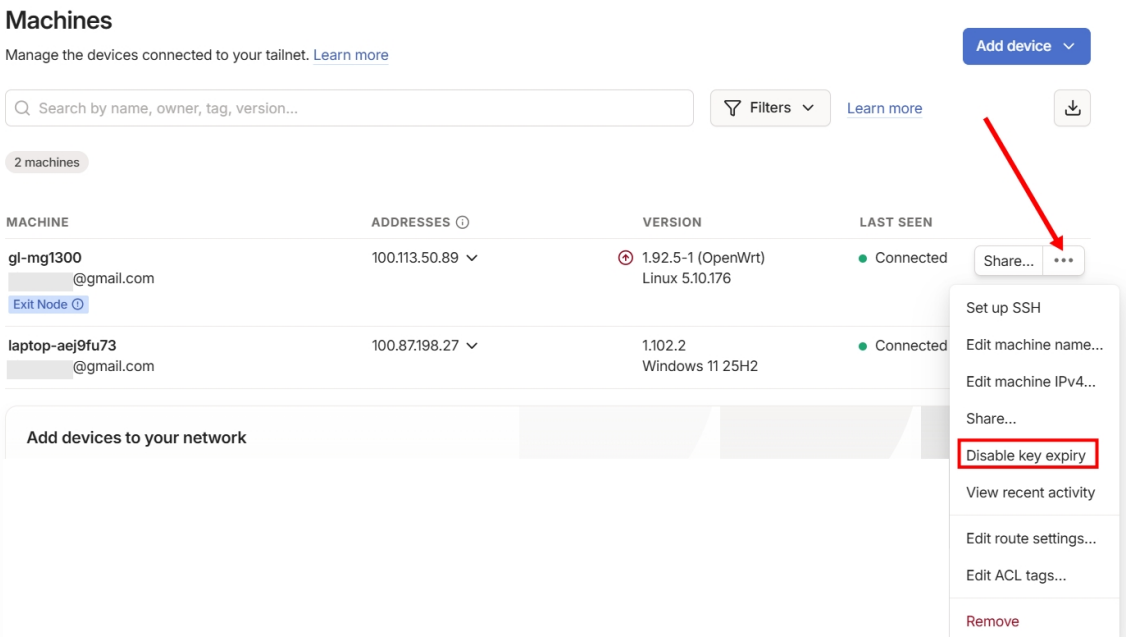
5. Aktivieren Sie im Pop-up-Fenster die Option **Use as exit node** und klicken Sie auf **Save**.



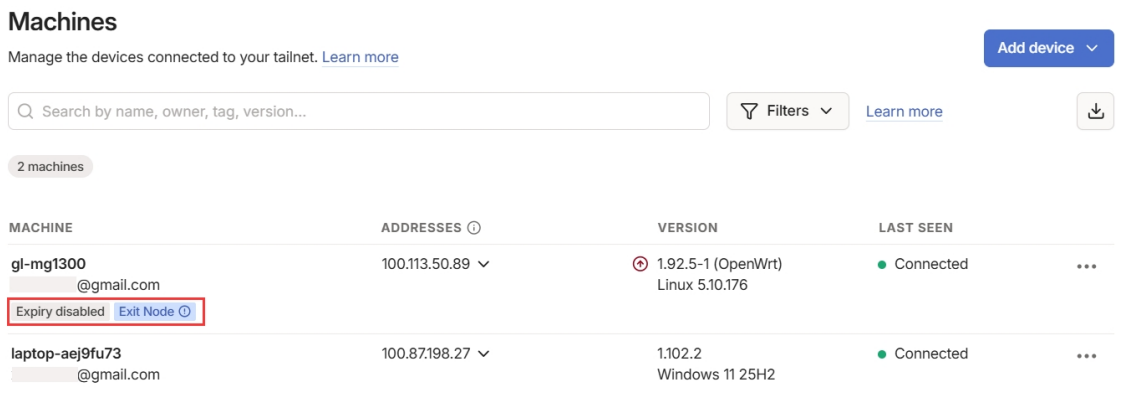
6. Deaktivieren Sie den Schlüsselablauf.

   Als Sicherheitsfunktion müssen Benutzer sich regelmäßig auf jedem ihrer Geräte neu authentifizieren. Um Unterbrechungen beim Ablauf des Authentifizierungsschlüssels für den Ausgangsknoten zu vermeiden, empfehlen wir, den Ablauf des Schlüssels für den Ausgangsknoten zu deaktivieren. Klicken Sie hier für weitere Details zum Ablauf des Schlüssels.

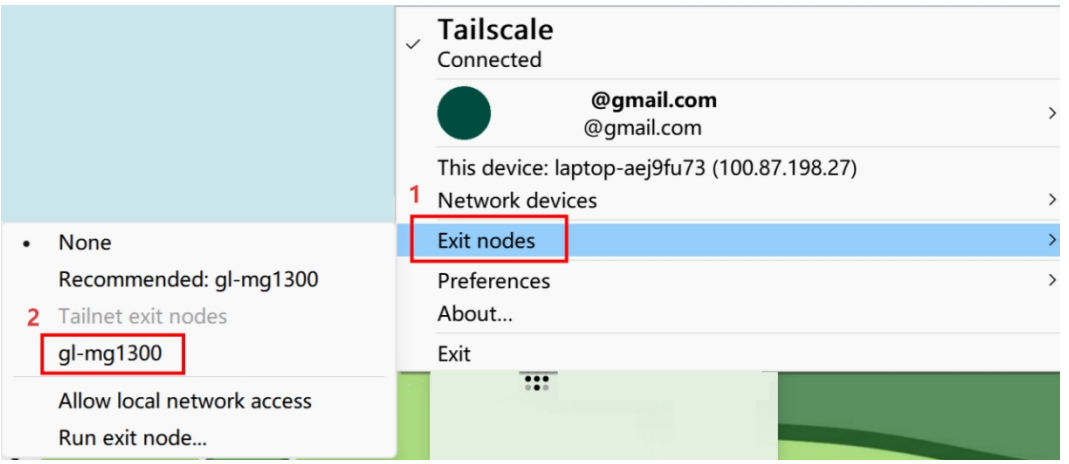
   Klicken Sie auf das Drei-Punkt-Symbol rechts von GL-MG1300 und wählen Sie den Ablauf der Tasten deaktivieren.



   Einmal angewendet, erscheint ein Tag "Ablauf deaktiviert" unter dem GL-MG1300.



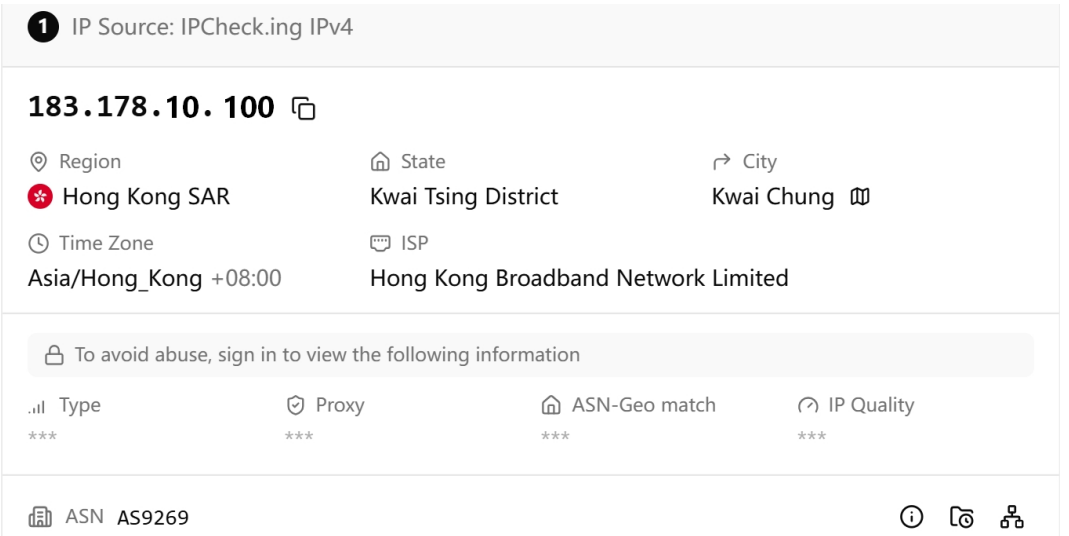
7. Führen Sie Tailscale auf Ihrem Reise-Laptop aus. Das Tailscale-Symbol erscheint im Infobereich unten rechts. Klicken Sie mit der rechten Maustaste auf das Symbol, wählen Sie **„Exit nodes“** und anschließend **„gl-mg1300“**.



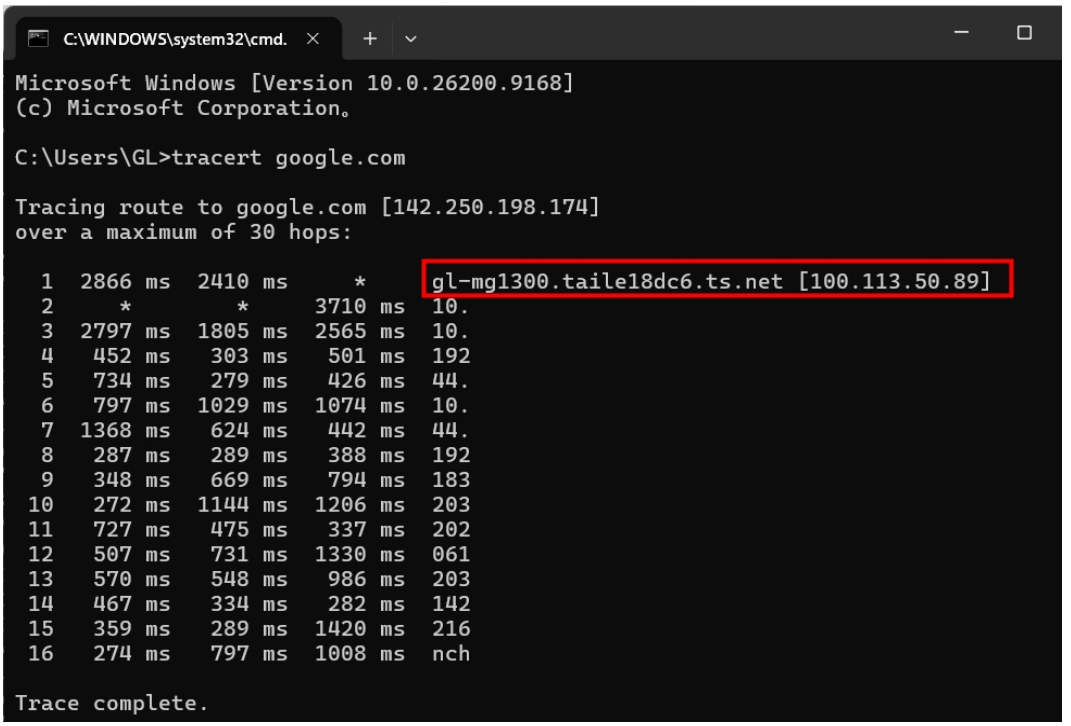
Jetzt wird der gesamte ausgehende Verkehr von diesem Reise-Laptop über GL-BMG1300 verlassen, um auf das Internet zuzugreifen.

8. Konnektivität testen.

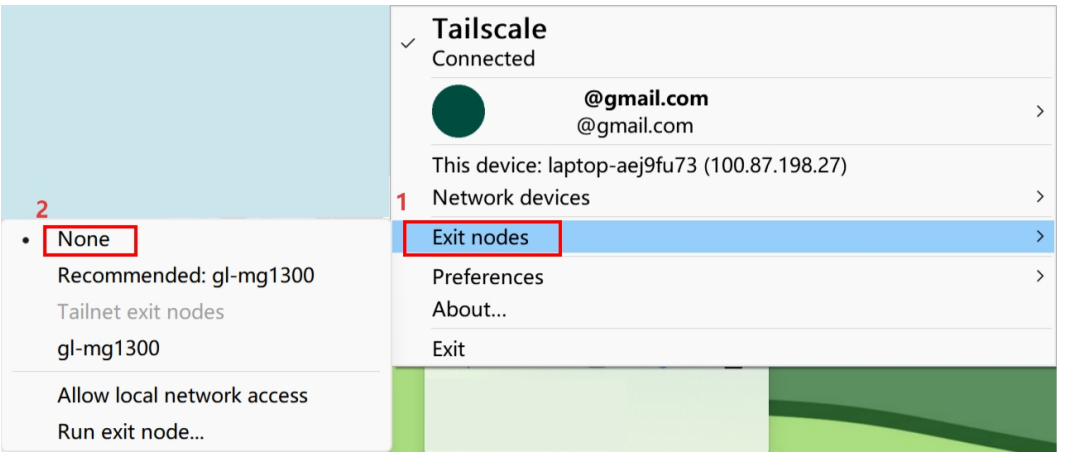
(1) Öffnen Sie auf Ihrem Reise-Laptop einen Webbrowser und rufen Sie ipcheck.ing oder eine andere Website zur IP-Überprüfung auf. Die Seite zeigt die öffentliche IP-Adresse Ihres Tailscale-Exit-Knotens an und bestätigt damit, dass der Laptop über diesen Exit-Knoten – in diesem Beispiel den GL-MG1300 in Hongkong – auf das Internet zugreift.



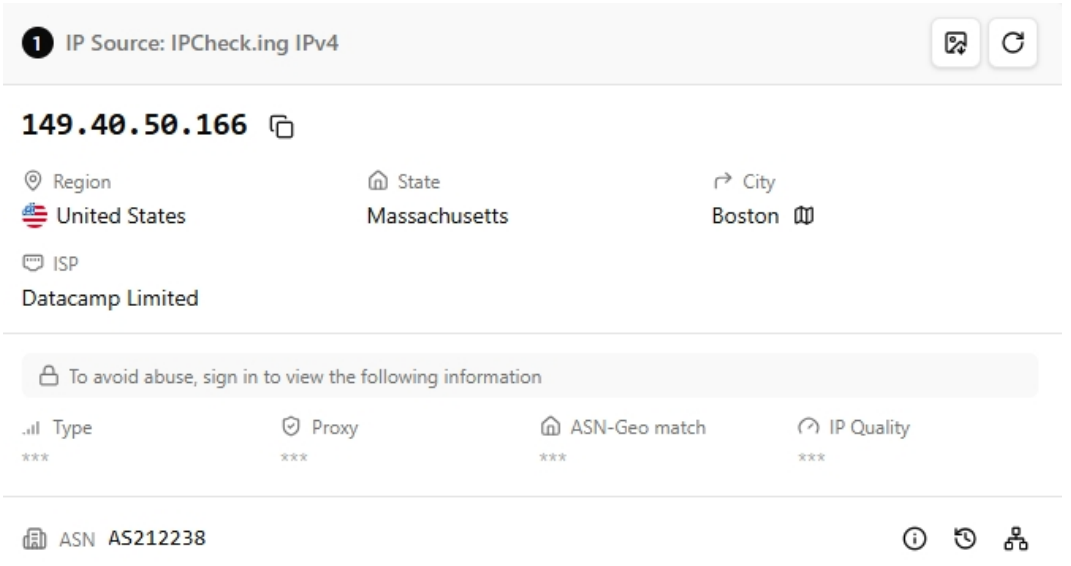
(2) Drücken *Sie* Win + R, *geben* Sie cmd ein, um die Eingabeaufforderung zu *starten, und führen* Sie dann tracert google.com aus, um die ausgehenden Verkehrsrouten zu verfolgen. Die Befehlsausgabe listet alle Routing-Hops für Ihren Internetverkehr auf. Wenn korrekt konfiguriert, wird der erste externe Hop durch den Exit-Knoten geleitet, wie unten gezeigt, und überprüft alle ausgehenden Internetverkehr geht über diesen Router aus.



(3) Trennen Sie den Exit-Knoten für einen Vergleichstest. Klicken Sie mit der rechten Maustaste auf das Tailscale-Symbol im Infobereich unten rechts, klicken Sie auf **Exit nodes** und wählen Sie „**None**“, um die Nutzung des Exit-Knotens zu beenden.



(4) Öffnen Sie eine neue Browser-Registerkarte und besuchen Sie ipcheck.ing oder einen IP-Lookup-Service. Es zeigt nun die native öffentliche IP-Adresse Ihres Laptops an und beweist, dass das Gerät stattdessen Ihre lokale Internetverbindung verwendet (in diesem Beispiel Boston).


1 IP Source: IPCheck.ing IPv4
149.40.50.166
Region
United States
State
Massachusetts
City
Boston
ISP
Datacamp Limited
To avoid abuse, sign in to view the following information
Type
***
Proxy
***
ASN-Geo match
***
IP Quality
***
ASN AS212238

Kapitel 13

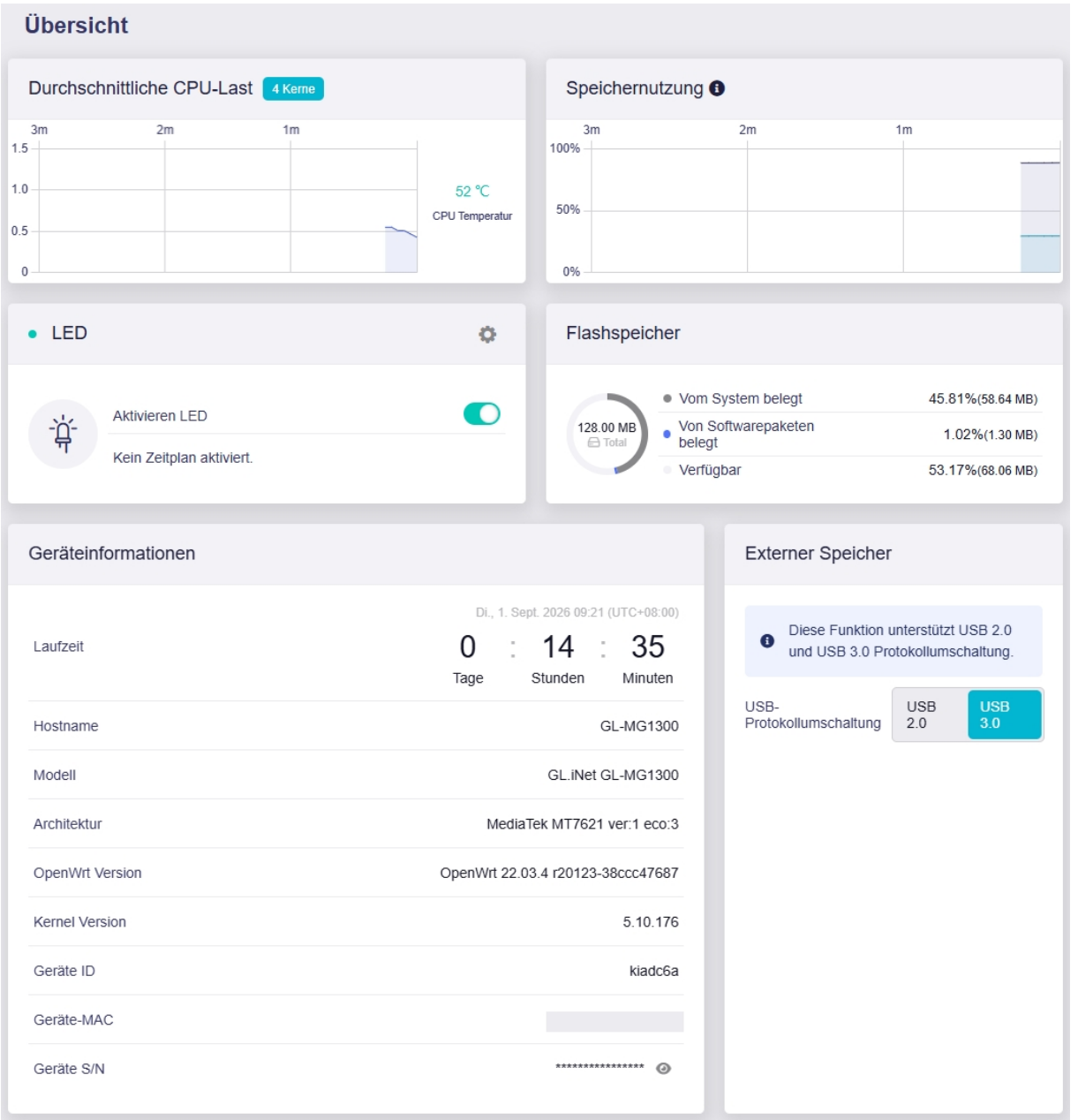
System

Dieses Kapitel behandelt Systemverwaltungstools für das Gerät, wie Systemübersicht, Upgrade, geplante Aufgaben, Zeitzone, Protokoll, Firmware-Reset und erweiterte Einstellungen.

13.1 Übersicht

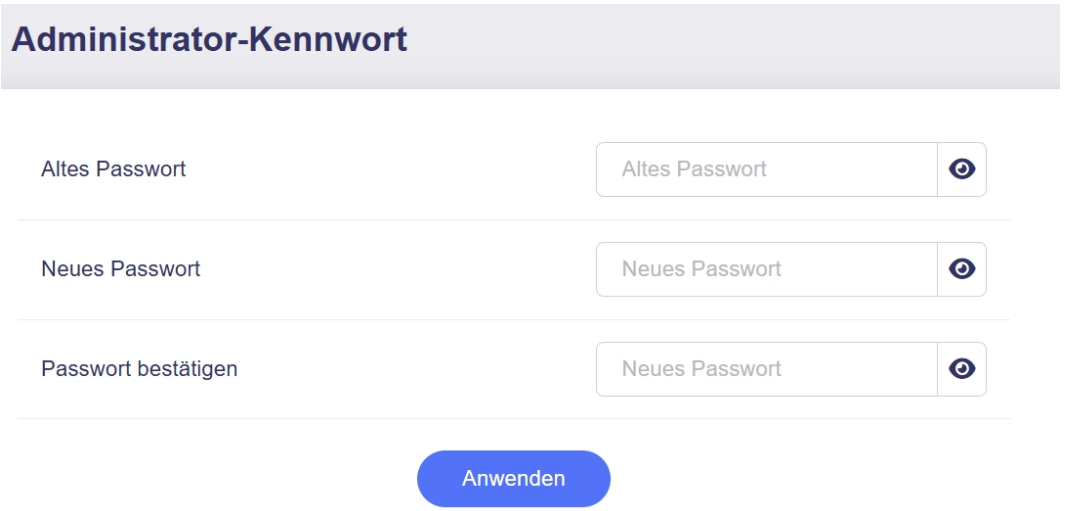
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Übersicht**. Diese Seite zeigt den Hardware-Status an und unterstützt einige einfache Bedienelemente, darunter:

- CPU, Speicher und Flash-Status
- LED-Steuerung
- Geräteinformationen
- externer Speicherprotokollschalter



13.2 Administrator-Kennwort

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Administrator-Kennwort**. Auf dieser Seite können Sie das Anmeldepasswort des Web-Admin-Panels ändern.



Die Anforderungen an das Admin-Passwort lauten wie folgt:

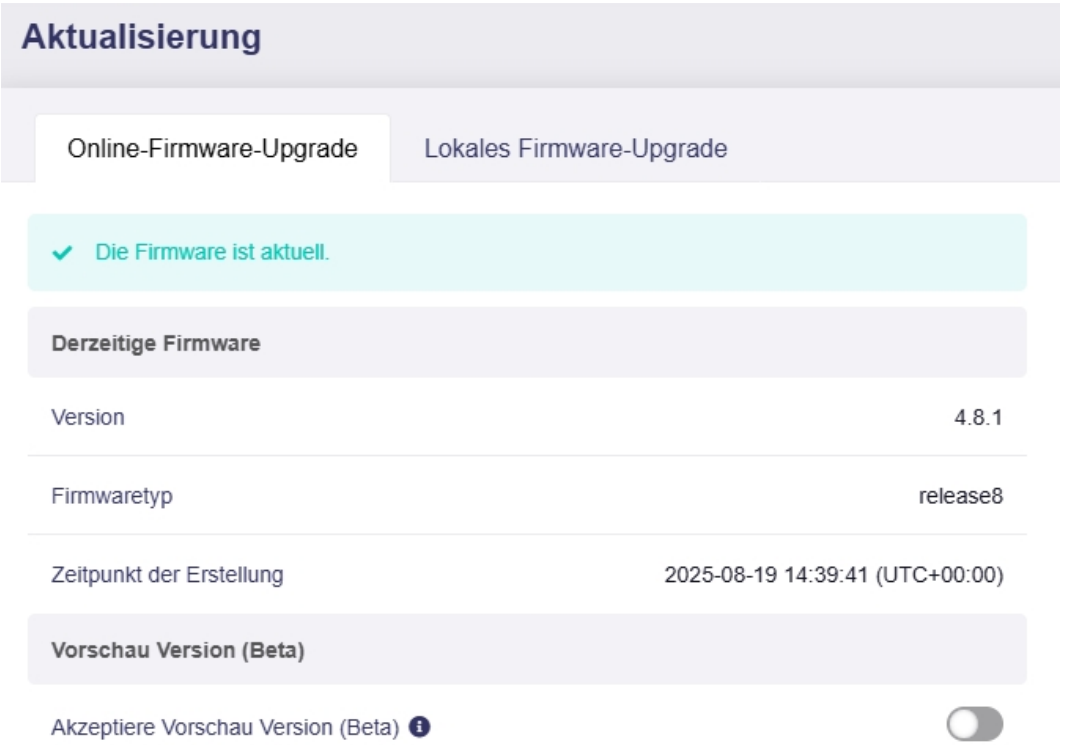
1. Mindestens 10 Zeichen und maximal 63 Zeichen in der Länge.
2. Buchstaben (fallsensibel), Zahlen und Symbole (z. B. ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ' ~) sind erlaubt.
3. Es sind mindestens zwei Typen (Oberbuchstaben, Kleinbuchstaben, Zahlen und Symbole) erforderlich.

13.3 Aktualisierung

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Aktualisierung.** Sie können die Firmware-Version des Routers per Online-Firmware-Upgrade oder lokalem Upgrade aktualisieren.

13.3.1 Online-Firmware-Upgrade

Sie können die aktuellen Firmware-Details hier finden, einschließlich Firmware-Version, Firmware-Typ (z. B. Release, Beta) und Update-Zeit.



- **Akzeptiere Vorschau Version (Beta)**: Wenn diese Option aktiviert ist, können Sie neue Funktionen ausprobieren, bevor die endgültige Version veröffentlicht wird, und uns Feedback geben. Stellen Sie sie einmal ein und sie bleibt eingeschaltet. Beachten Sie, dass diese Upgrades möglicherweise nicht stabil sind.

Wenn Ihr Router mit dem Internet verbunden ist, wird er nach der neueren Firmware-Version suchen, die zum Download zur Verfügung steht.

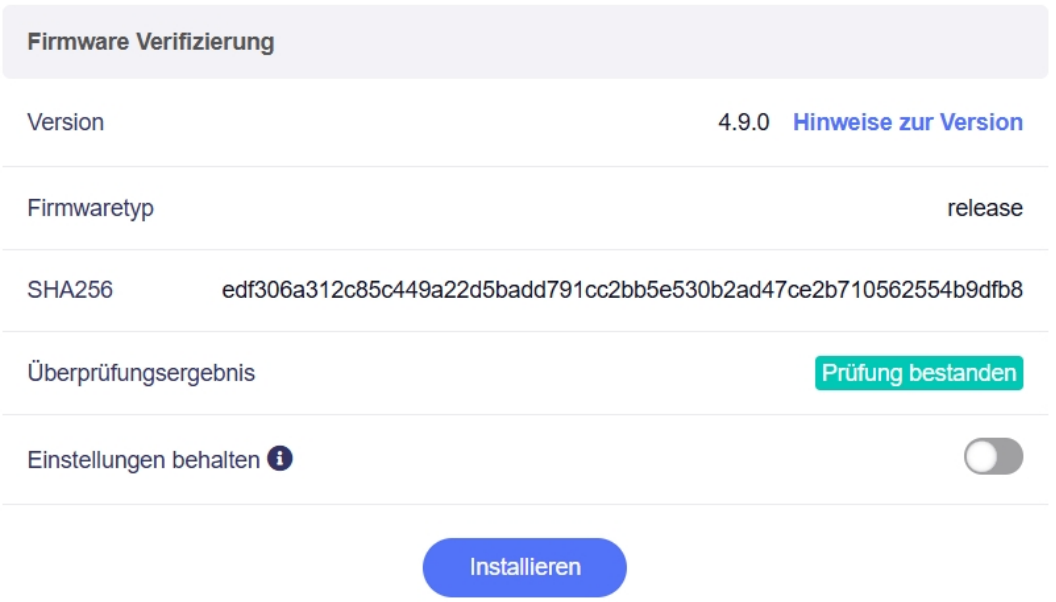
Tipp: Wenn Sie versuchen, ein Online-Upgrade durchzuführen, wenn es den Download Failed anzeigt**,** navigieren Sie bitte zu **System** > **Zeitzone** und beheben Sie den Zeitzonenfehler (Synchronisierung mit dem Browser).

13.3.2 Lokales Firmware-Upgrade

Lokales Upgrade ist nicht auf eine Internetverbindung für den Router angewiesen. Laden Sie das richtige Firmware-Paket (zu Ihrem Routermodell passend) vom offiziellen Download Center auf Ihr lokales Gerät herunter. Dann melden Sie sich im Web-Admin-Panel des Routers an, navigieren Sie zum Abschnitt **System** > **Aktualisierung** > **Lokales Firmware-Upgrade** und laden Sie das Firmware-Paket hoch.



Die Seite zeigt die Firmware-Details an. Überprüfen Sie diese Details, bevor Sie auf **Installieren** klicken.



- **Einstellungen beibehalten**: Wenn aktiviert, bleiben die aktuellen Einstellungen erhalten. Alle manuell installierten Pakete müssen jedoch nach Abschluss des Upgrades neu installiert werden. Aktivieren Sie diese Option nicht, wenn Sie die Firmware herunterstufen.

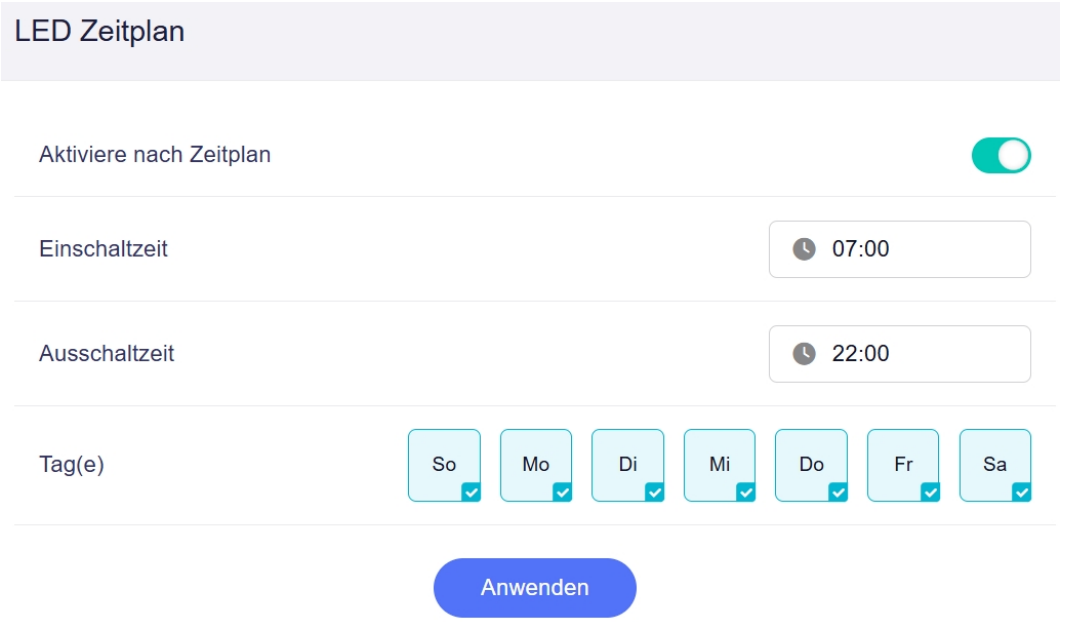
13.4 Geplante Aufgaben

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Geplante Aufgaben**. Diese Seite ermöglicht es Ihnen, einen täglichen Zeitplan für einige grundlegende Aktionen einzurichten, einschließlich des Ein- und Ausschaltens von LED-Licht und des Neustartens des Routers.

Hinweis: Bitte synchronisieren Sie die Zeit in der Zeitzone, bevor Sie diese Funktion verwenden. Wenn das Gerät zum geplanten Zeitpunkt heruntergefahren wird, wird die Aufgabe nicht ausgeführt.

13.4.1 LED Display Zeitplan

Legen Sie bei Bedarf einen Zeitplan für das LED-Licht Ihres Routers fest.

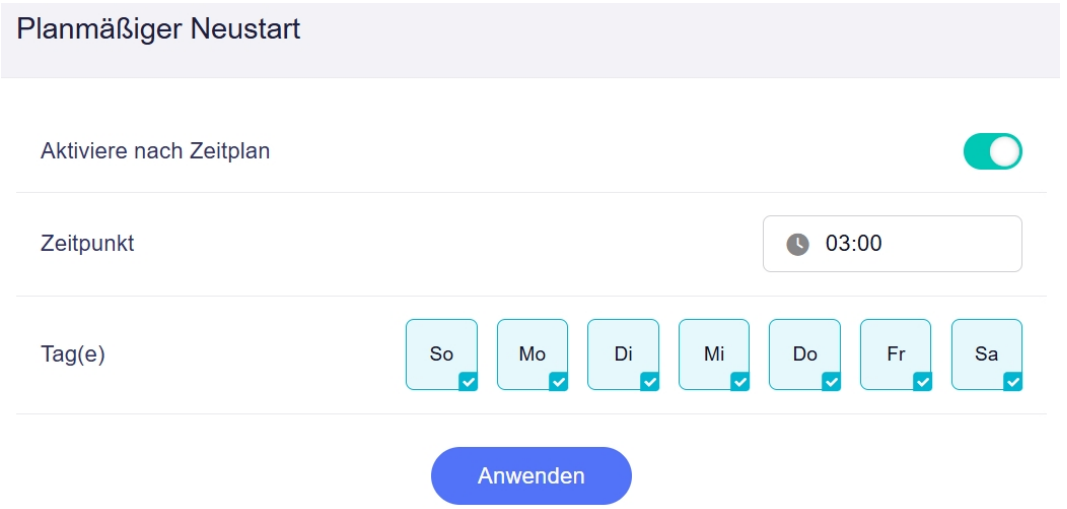


- **Aktiviere nach Zeitplan**: Schalten Sie diesen Schalter um, um den LED-Anzeigeplan zu aktivieren.
- **Einschaltzeit**: Stellen Sie die Zeit (z. B. 07:00 Uhr) ein, zu der das LED-Licht eingeschaltet wird.
- **Ausschaltzeit**: Stellen Sie die Zeit (z. B. 22:00 Uhr) ein, zu der das LED-Licht ausgeschaltet wird.
- **Tag(e)**: Wählen Sie die effektiven Tage der Woche für diese Einstellungen.

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

13.4.2 Zeitplan-Neustart

Legen Sie einen Zeitplan für den automatischen Neustart Ihres Routers fest, falls erforderlich.



- **Aktiviere nach Zeitplan**: Schalten Sie diesen Schalter um, um den geplanten Neustart zu aktivieren.
- **Zeitpunkt**: Legen Sie die bestimmte Zeit fest (z. B. 03:00), wenn der Router neu gestartet wird.
- **Tag(e)**: Wählen Sie die effektiven Tage der Woche für diese Einstellungen.

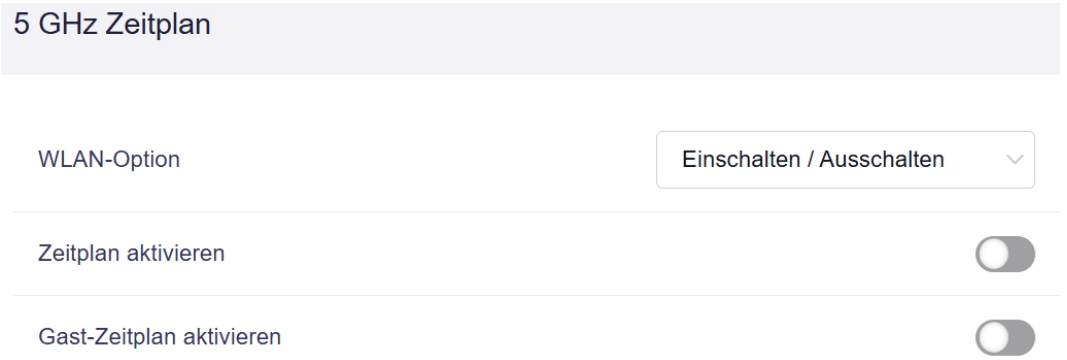
Klicken Sie nach der Konfiguration auf **Anwenden,** um Ihre Einstellungen zu speichern.

13.4.3 5 GHZ Zeitplan

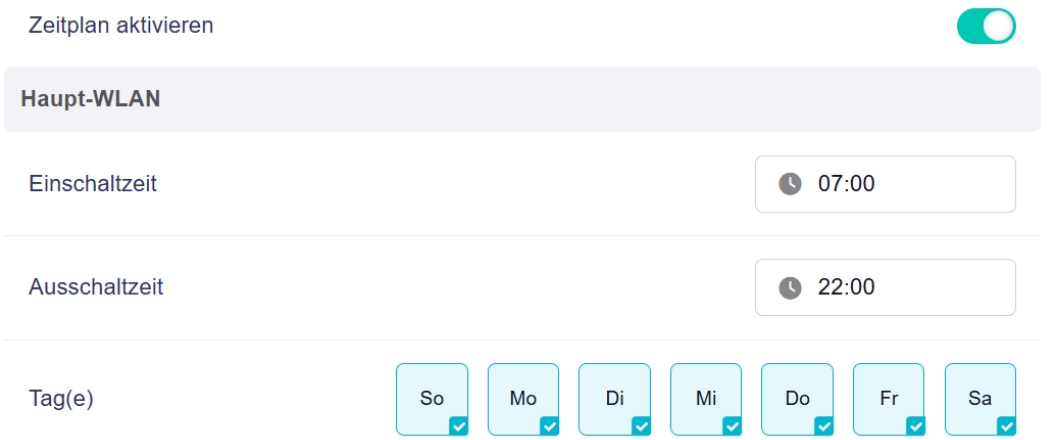
Mit dieser Funktion legen Sie einen Zeitplan für Ihr 5 GHZ-WLAN fest. Zur Auswahl stehen zwei WLAN-Optionen: Ein-/Ausschalten und WLAN-Sendeleistung.

WLAN-Option 1: Einschalten / Ausschalten

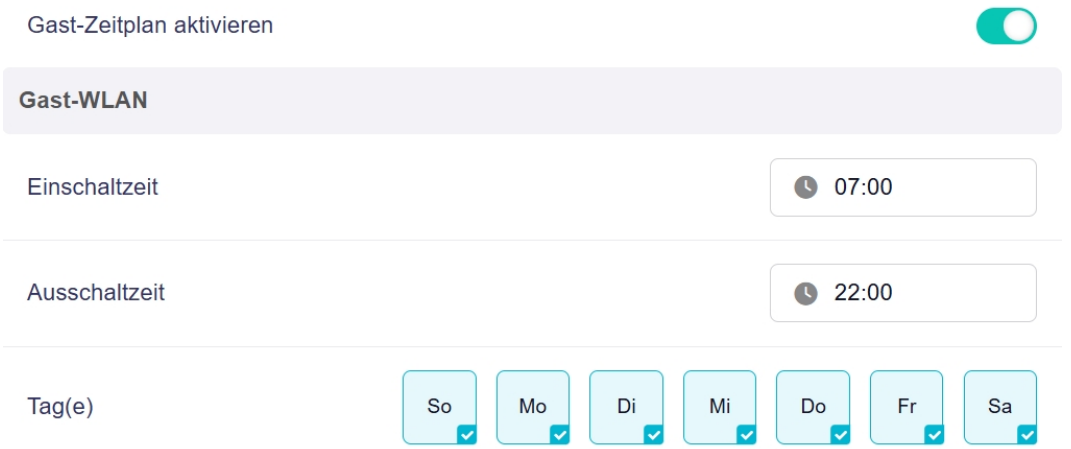
Sie können den Ein/Aus-Zeitplan sowohl für das 5 GHZ-Haupt-WLAN als auch für das Gast-WLAN aktivieren.



- **Zeitplan aktivieren**: Wenn Sie aktiviert sind, legen Sie die Ein- und Ausschaltzeiten für Ihr 5 GHz Haupt-WLAN fest und wählen Sie ein effektives Datum für die Woche.



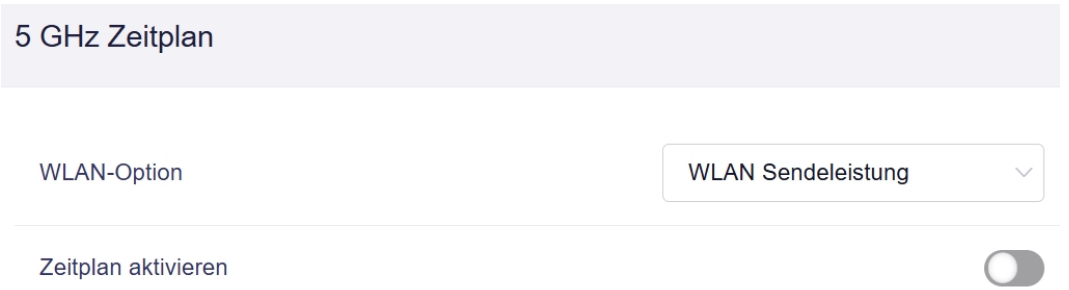
- **Gast-Zeitplan aktivieren**: Wenn Sie aktiviert sind, legen Sie die Ein- und Ausschaltzeiten für Ihr 5 GHz Gast-WLAN fest und wählen Sie ein effektives Datum für die Woche.



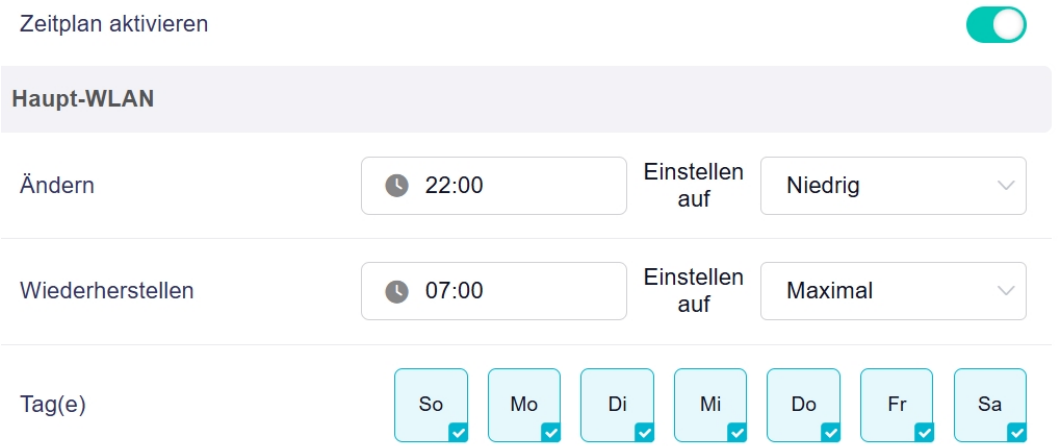
Klicken Sie nach der Konfiguration auf **Anwenden,** um Ihre Einstellungen zu speichern.

WLAN-Option 2: WLAN-Sendeleistung

Sie können den TX-Power-Schaltplan für das 5 GHz Main Wi-Fi aktivieren.



Wenn aktiviert, legen Sie zwei zeitgesteuerte Aktionen für Ihr 5 GHz Main Wi-Fi fest, um die TX-Leistung zu wechseln, und wählen Sie ein effektives Datum für die Woche.



- **Ändern**: Setzen Sie TX Power auf einen bestimmten Pegel (z. B. Low) zu einem bestimmten Zeitpunkt (z. B. 22: 00).
- **Wiederherstellen:** Wiederherstellen Sie TX Power zu einem anderen Zeitpunkt (z. B. 07: 00) auf ein anderes Niveau (z. B. Max).
- **Tag(e)**: Wählen Sie die effektiven Tage der Woche für diese Einstellungen.

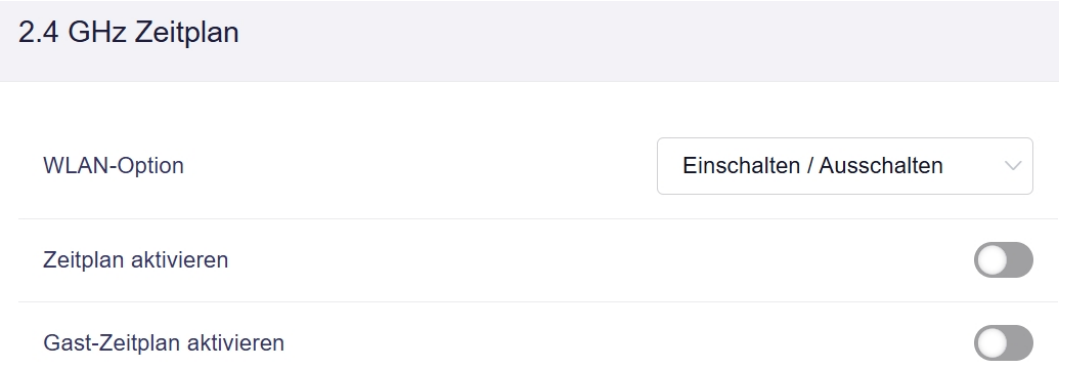
Klicken Sie nach der Konfiguration auf **Anwenden,** um Ihre Einstellungen zu speichern.

13.4.4 2,4 GHZ Zeitplan

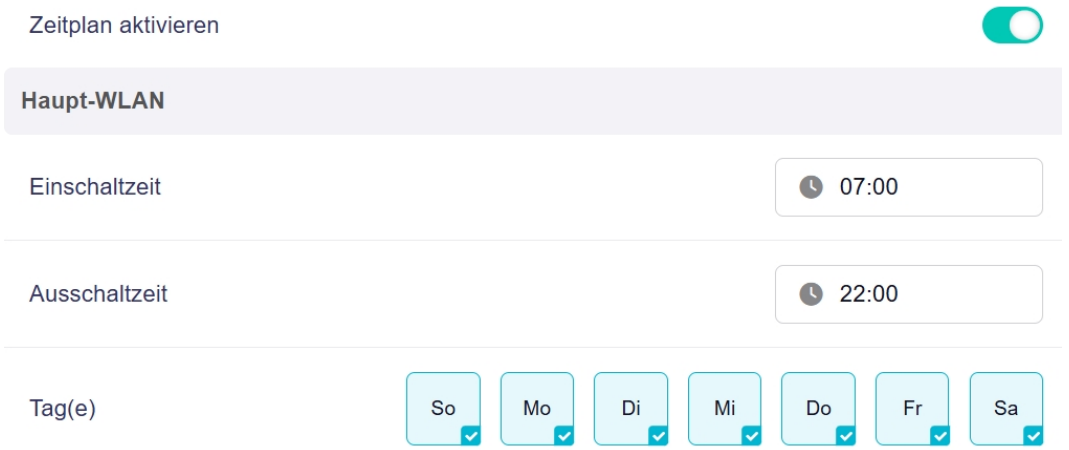
Mit dieser Funktion können Sie einen Zeitplan für Ihr 2,4 GHZ Wi-Fi festlegen. Es gibt zwei Modi: Ein-/Ausschalten und Switch TX Power.

WLAN-Option 1: Einschalten / Ausschalten

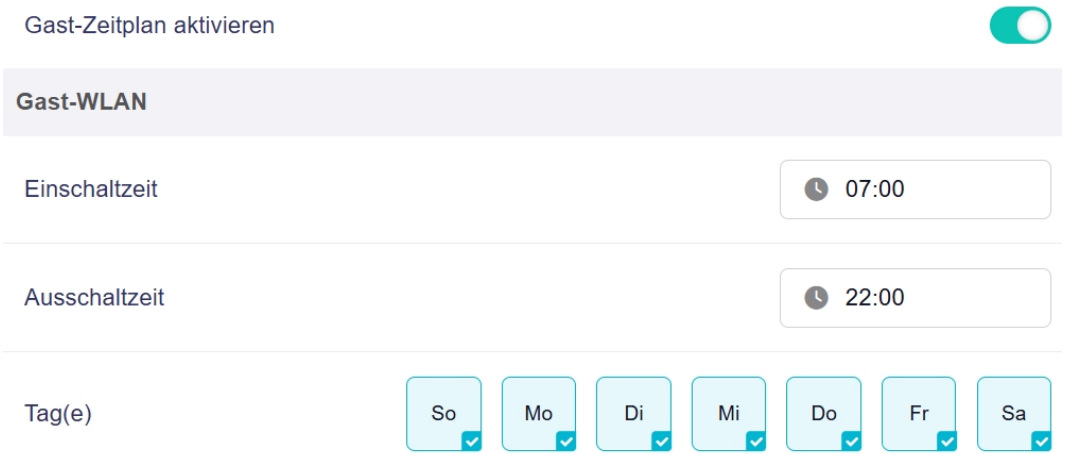
Sie können den On/Off-Zeitplan sowohl für das 2,4 GHZ Main Wi-Fi als auch für das Guest Wi-Fi aktivieren.



- **Zeitplan aktivieren**: Wenn aktiviert, legen Sie die Ein- und Ausschaltzeiten für Ihr 2,4 GHZ Main Wi-Fi fest und wählen Sie ein effektives Datum für die Woche.



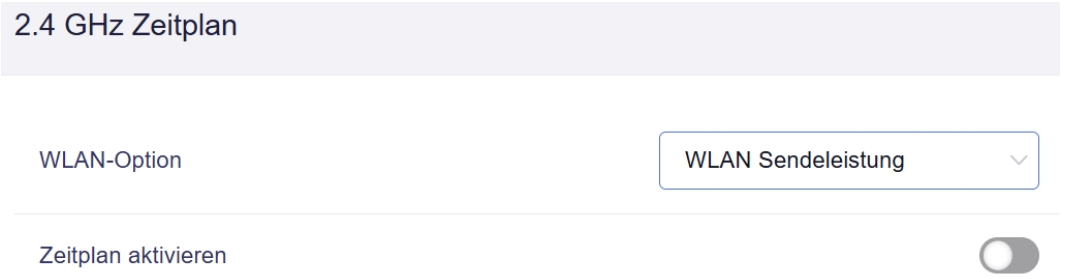
- **Gast-Zeitplan aktivieren**: Wenn aktiviert, legen Sie die Ein- und Ausschaltzeiten für Ihr 2,4 GHZ Gast-WLAN fest und wählen Sie ein effektives Datum für die Woche.



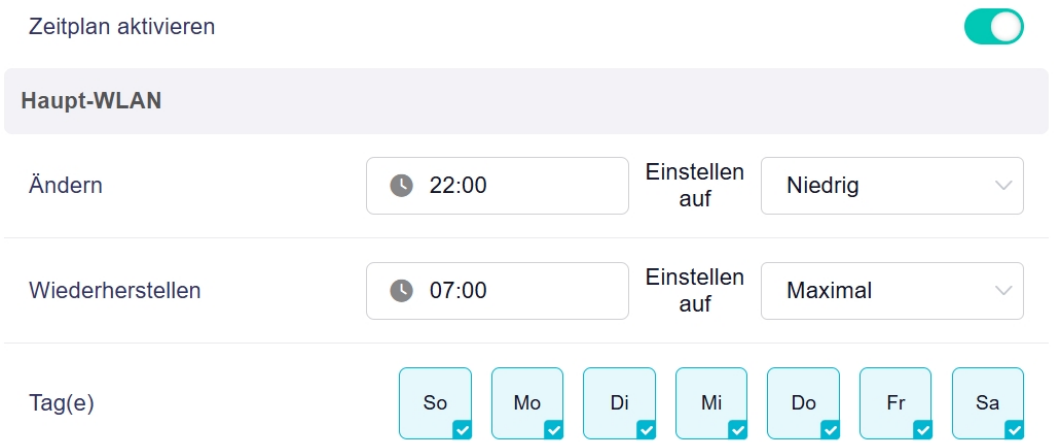
Klicken Sie nach der Konfiguration auf **Anwenden,** um Ihre Einstellungen zu speichern.

WLAN-Option 2: WLAN-Sendeleistung

Sie können den TX-Power-Schaltplan für das 2,4 GHZ Main Wi-Fi aktivieren.



Wenn aktiviert, legen Sie zwei zeitgesteuerte Aktionen für Ihr 2,4 GHZ Main Wi-Fi fest, um die TX-Leistung zu wechseln, und wählen Sie ein effektives Datum für die Woche.

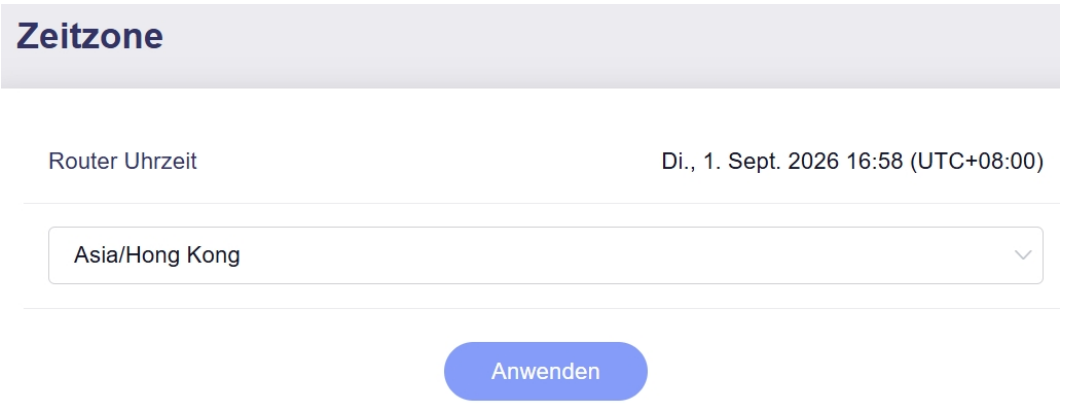


- **Ändern**: Setzen Sie TX Power auf einen bestimmten Pegel (z. B. Low) zu einem bestimmten Zeitpunkt (z. B. 22: 00).
- **Wiederherstellen**: Wiederherstellen Sie TX Power zu einem anderen Zeitpunkt (z. B. 07: 00) auf ein anderes Niveau (z. B. Max).
- **Tag(e)**: Wählen Sie die effektiven Tage der Woche für diese Einstellungen.

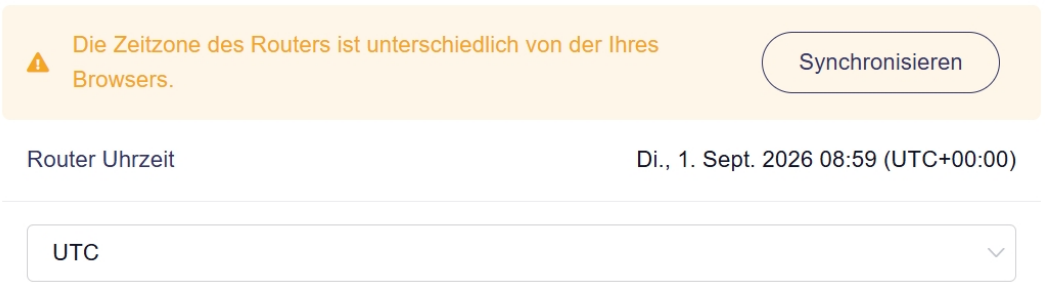
Klicken Sie nach der Konfiguration auf **Anwenden,** um Ihre Einstellungen zu speichern.

13.5 Zeitzone

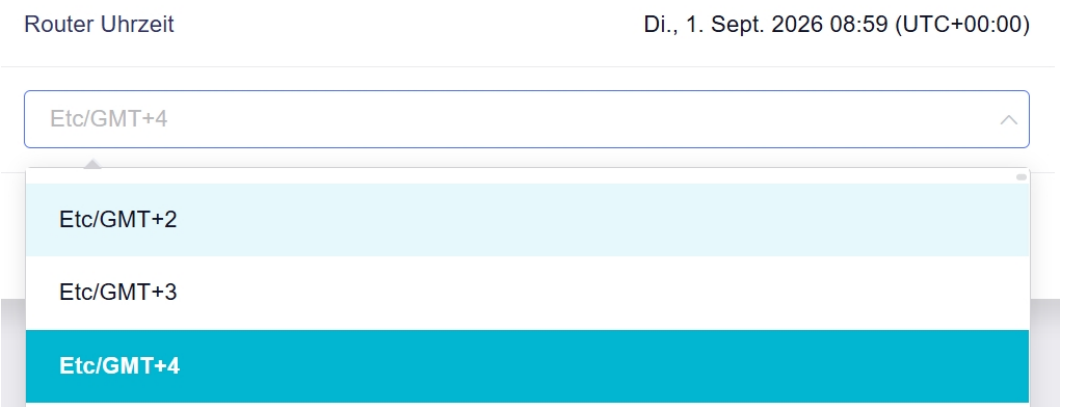
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Zeitzone.** Diese Seite zeigt die Systemzeit Ihres Routers an und zeigt den Datums-, Zeit- und entsprechenden Zeitzonenversatz an.



Einige Funktionen sind auf die Systemzeit des Routers angewiesen, um wirksam zu werden. Bitte stellen Sie daher sicher, dass die richtige Zeitzone richtig synchronisiert ist. Wenn die Zeitzone des Routers sich von der Ihres Browsers unterscheidet, wird eine Aufforderung wie folgt angezeigt. Klicken Sie auf die Schaltfläche Synchronisieren, um die Zeitzone zu synchronisieren.



Um die Zeitzone zu wechseln, wählen Sie die entsprechende Zeitzone aus der Liste aus, um sicherzustellen, dass die Systemzeit des Routers mit Ihrer lokalen Zeit übereinstimmt.



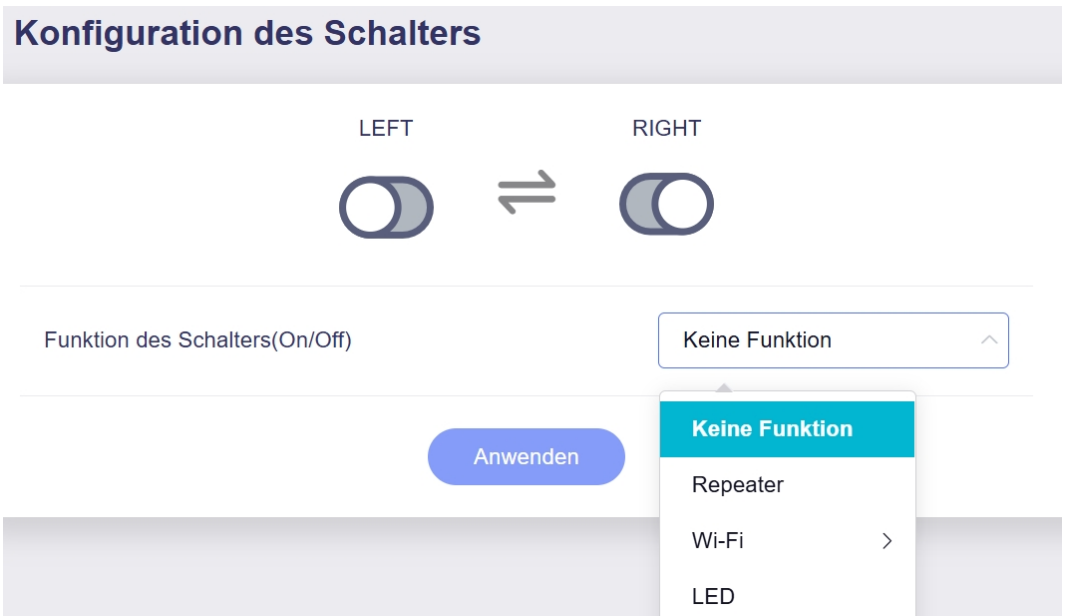
13.6 Konfiguration des Schalters

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Konfiguration des Schalters**.

Diese Seite ermöglicht es Ihnen, die Funktion des physischen Umschalters des Routers anzupassen (lokalisiert) an der Seite) für eine einfachere Verwendung



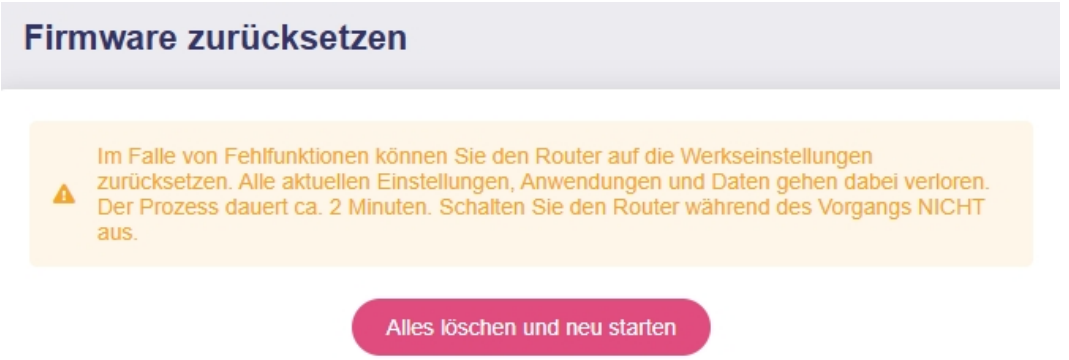
Standardmäßig sind dem Umschalter keine Funktionen zugewiesen. Schalten Sie bestimmte Funktionen mit einem einzigen Flip ein oder aus.



13.7 Firmware zurücksetzen

Wenn der Router eine Fehlfunktion aufweist, können Sie versuchen, das Problem zu beheben, indem Sie die Firmware zurücksetzen.

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Firmware zurücksetzen**. Klicken Sie auf **Alle löschen und neu starten,** um die Firmware bei Bedarf zurückzusetzen.

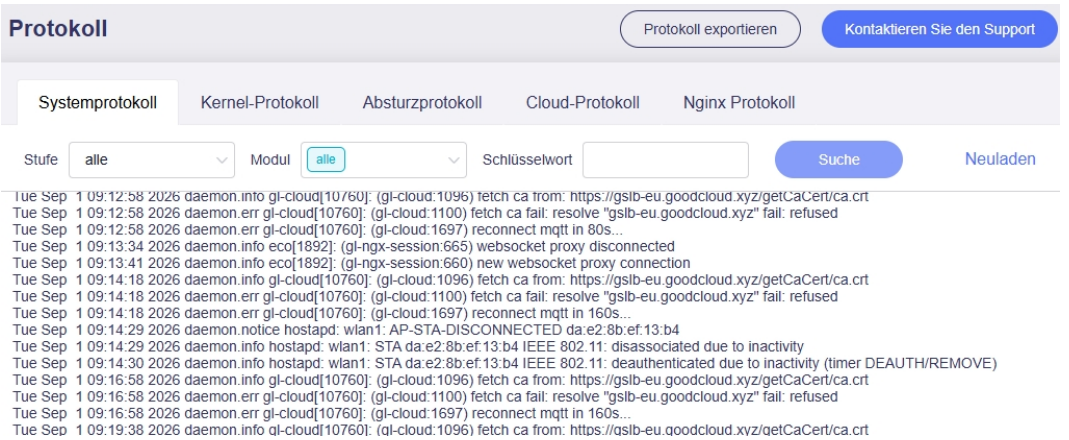


Hinweis: Alle Ihre aktuellen Einstellungen, Anwendungen und Daten werden gelöscht. Der Vorgang dauert ca. 2 Minuten. Schalten Sie den Router während dieses Vorgangs nicht aus.

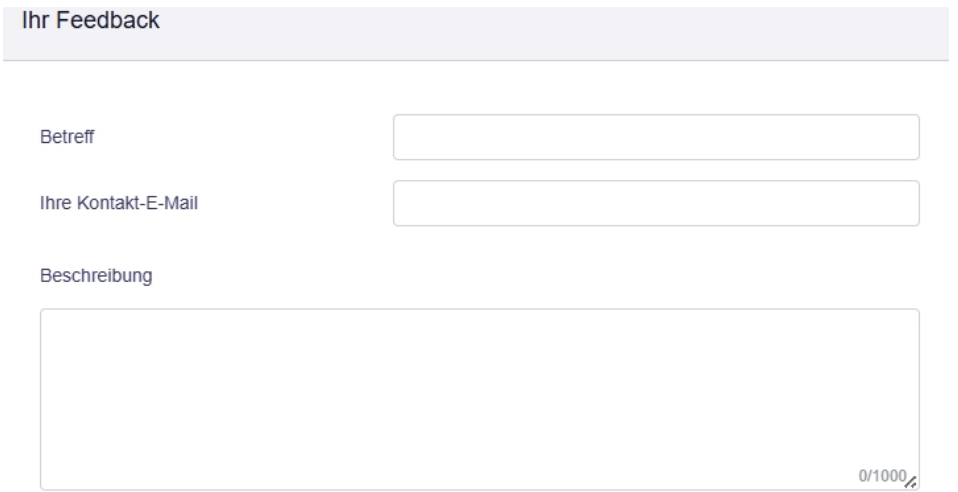
Wenn Sie nicht auf das Web-Admin-Panel des Routers zugreifen können, versuchen Sie, Ihren Router mit der physischen Reset-Taste an der Seite zurückzusetzen.

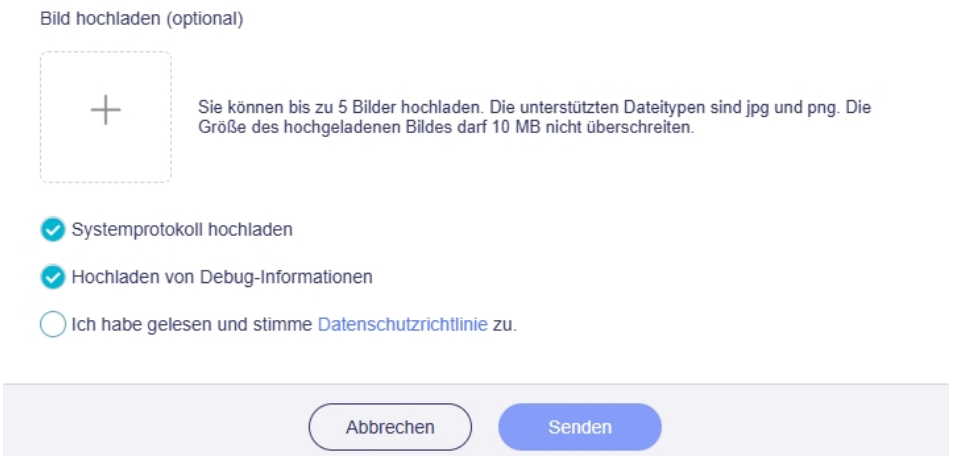
13.8 Protokoll

Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System > Protokol**l. Diese Seite ermöglicht es Ihnen, Protokolle von System, Kernel, Crash, Cloud und Nginx zur Analyse und Fehlerbehebung anzuzeigen. Darüber hinaus bieten einige Mobilfunkmodelle, die eSIM unterstützen, auch eSIM-Protokoll.



- **Suche:** Die Systemlogseite bietet Filterung für die schnelle Suche. Sie können die Log-Ebene (z. B. alle, Informationen, Fehler) oder das Modul (z. B. IPv6, Tethering, Mobilfunknetz) aus der Dropdown-Liste auswählen oder Schlüsselwörter eingeben, um Protokolle schnell abzufragen.
- **Neuladen**: Klicken Sie auf diese Schaltfläche, um die Protokolle zu aktualisieren.
- **Protokoll exportieren**: Klicken Sie auf diese Schaltfläche, um Debug-Informationen zusammen mit den Protokollen zu exportieren.
- **Kontaktieren Sie den Support**: Klicken Sie auf diese Schaltfläche, füllen Sie detaillierte Informationen im Popup-Fenster auf der rechten Seite, dann auf Senden. Ihr Feedback wird direkt an GL.iNet Technical Support gesendet.



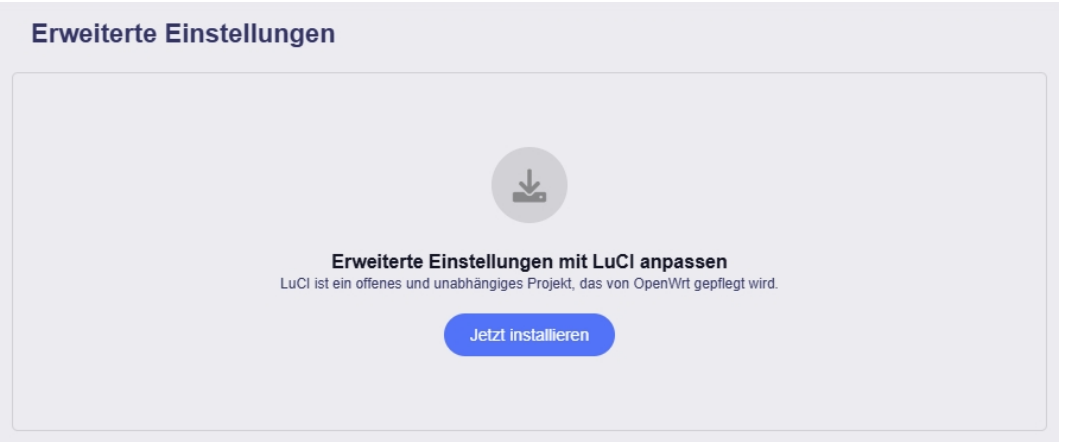

Bild hochladen (optional)
Sie können bis zu 5 Bilder hochladen. Die unterstützten Dateitypen sind jpg und png. Die Größe des hochgeladenen Bildes darf 10 MB nicht überschreiten.
Systemprotokoll hochladen
Hochladen von Debug-Informationen
Ich habe gelesen und stimme Datenschutzrichtlinie zu.
Abbrechen
Senden

13.9 Erweiterte Einstellungen

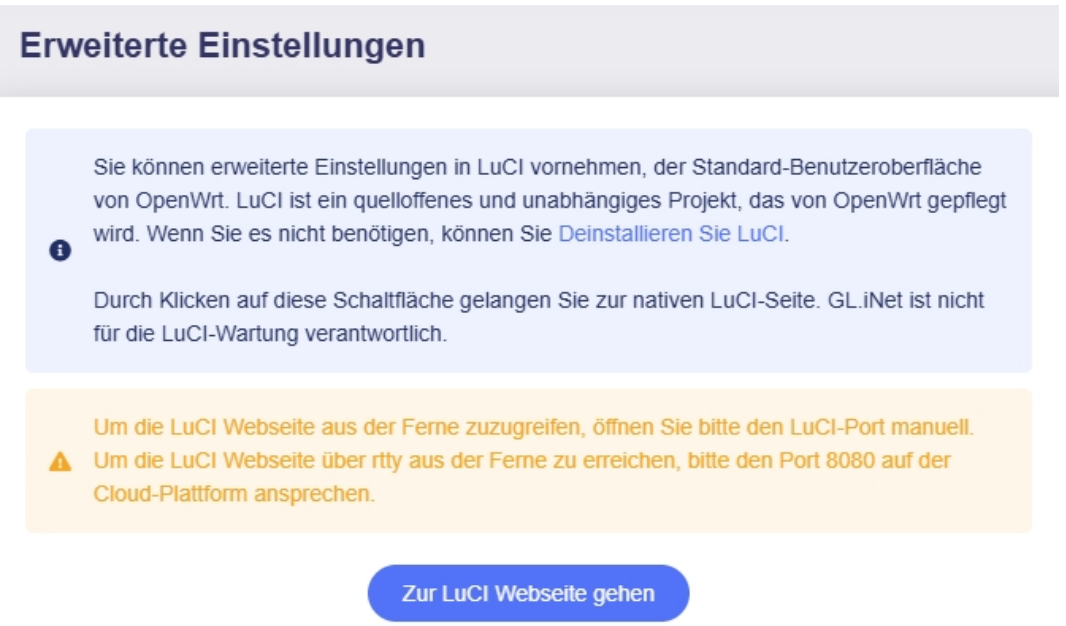
Melden Sie sich im Web-Admin-Panel Ihres Routers an und navigieren Sie zu **System** > **Erweiterte Einstellungen**. Diese Seite ermöglicht es Ihnen, erweiterte Einstellungen in LuCI zu ändern, der Standard-Web-Benutzeroberfläche von OpenWrt. Als offenes und unabhängiges Projekt, das von OpenWrt gepflegt wird, wird LuCI wie vorgesehen bereitgestellt. GL.iNet ist nicht für die Wartung von LuCI verantwortlich.

Folgen Sie den Schritten unten, um sich bei der LuCI-Schnittstelle anzumelden.

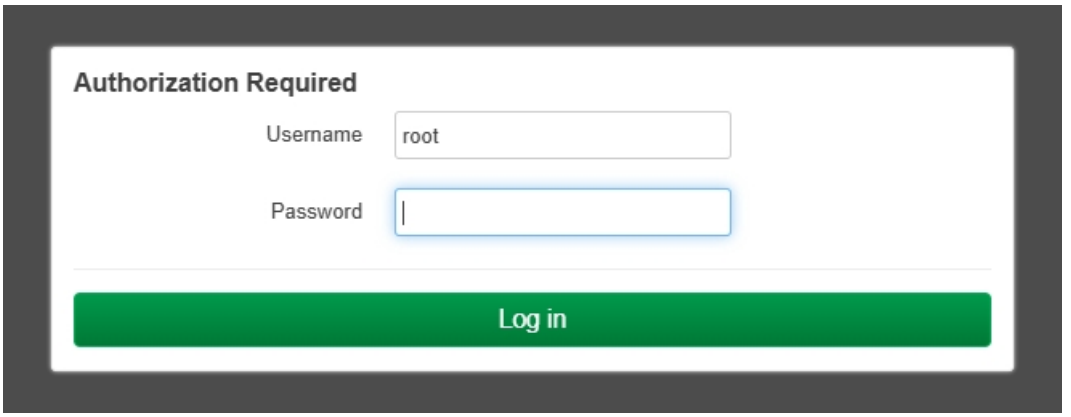
1. Klicken Sie auf **Jetzt Installieren**, und es wird die Installation LuCI-Schnittstelle.



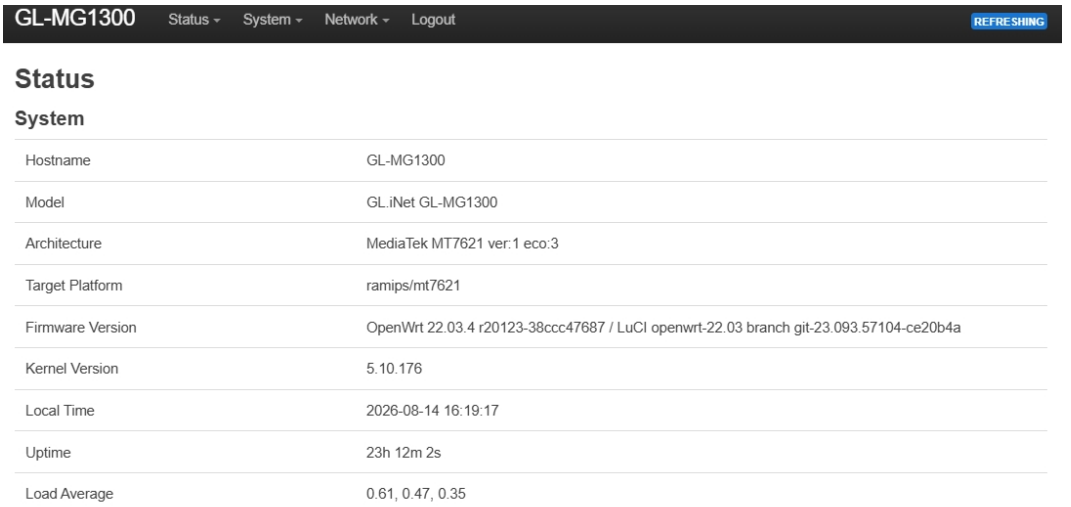
2. Klicken Sie auf **Zur LuCI Webseite gehen**, und Sie werden auf die LuCI-Anmeldeseite weitergeleitet.



3. Geben Sie das Anmeldekennwort ein, das mit dem Kennwort des Web-Admin-Panels identisch ist.



Sie werden sich dann in die LuCI-Schnittstelle einloggen.



Konformitätserklärung

Hiermit erklärt GL TECHNOLOGIES (HONG KONG) LIMITED, dass der Funkanlagentyp [Dualband-Mini-Reise-Router, GL-MG1300] den grundlegenden Anforderungen und anderen einschlägigen Bestimmungen der Richtlinie 2014/53/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: https://www.gl-inet.com/products/certificate.