GL·iNet



# Manuale utente

GL-B3000 / Marble

Router domestico dual-band Wi-Fi 6

Versione firmware 4.5.22

# Informazioni sul manuale

Questo manuale è la tua risorsa di riferimento per iniziare a utilizzare il tuo dispositivo e copre informazioni di base sul prodotto, connessioni hardware, accesso all'interfaccia di gestione web, configurazione iniziale e istruzioni dettagliate per tutte le funzionalità software del pannello di amministrazione web.

### Con questa guida sarai in grado di:

- Comprendere le caratteristiche principali del prodotto
- Scegliere una posizione adatta per il dispositivo
- Effettuare i collegamenti hardware seguendo le istruzioni passo passo
- Accedere facilmente all'interfaccia di gestione web
- Configura le impostazioni iniziali e padroneggia tutte le funzionalità del software nel pannello di amministrazione web

### Convenzioni tipografiche

Questi simboli e colori aiutano a seguire più facilmente le istruzioni.

| Convenzione | Significato |
|---|---|
| Testo verde acqua sottolineato | Collegamento cliccabile a una pagina web o a una sezione specifica |
| Testo in grassetto | Evidenzia informazioni importanti, come titoli, collegamenti ipertestuali e nomi esatti di menu e voci dell'interfaccia web del dispositivo |
| > | Percorso per aprire la pagina corrispondente (ad esempio, Sistema > Firmware) |
| Nota | Informazioni essenziali per la configurazione, il funzionamento e la sicurezza. Ignorarle può causare errori di configurazione, malfunzionamenti o danni al dispositivo |
| Suggerimenti | Consigli per aiutarti a utilizzare meglio il tuo dispositivo |

### Nota:

- Le funzionalità del dispositivo possono variare in base al modello e alla versione del firmware.
- La disponibilità del prodotto è soggetta a differenze regionali o specifiche dell'ISP.
- Tutte le immagini, le procedure e le descrizioni presenti in questa guida sono solo a scopo illustrativo e potrebbero differire dalla tua effettiva esperienza di utilizzo.

## Hai bisogno di ulteriore aiuto o informazioni?

- Aggiornamento firmware: Centro download firmware GL.iNet | Router
- Community: discuti i nostri prodotti e condividi approfondimenti nel forum della community GL.iNet
- Supporto tecnico: contatta il nostro supporto tecnico alla pagina dei contatti

**Copyright © 2026 GL.iNet Technology (HK) Ltd. Tutti i diritti riservati.**
Nessuna parte di questo manuale può essere riprodotta, trascritta, tradotta o distribuita in qualsiasi forma o con qualsiasi mezzo, senza il previo consenso scritto di GL.iNet Technology (HK) Ltd. GL.iNet è un marchio registrato di GL.iNet Technology (Hong Kong) Ltd. in Cina e/o altri paesi e regioni. Tutti gli altri marchi e nomi di prodotti qui menzionati sono marchi o marchi registrati dei rispettivi proprietari.
Il contenuto di questo documento è soggetto a modifiche senza preavviso a causa degli aggiornamenti della versione del prodotto o per altri motivi. Salvo diversamente concordato, il presente documento viene fornito solo a scopo informativo e tutte le dichiarazioni, informazioni e raccomandazioni in esso contenute non costituiscono alcuna forma di garanzia.

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

# Indice


**Capitolo 1 Conoscere il router ..... 8**

1.1 Panoramica del prodotto ..... 9

1.1.1 Aspetto ..... 9

1.1.2 Interfacce e pulsanti ..... 10

1.1.3 LED ..... 11

1.2 Specifiche tecniche ..... 11

1.3 Contenuto della confezione ..... 13

**Capitolo 2 Collegamenti hardware ..... 14**

2.1 Scelta della posizione ..... 15

2.2 Collegamento del router ..... 15

**Capitolo 3 Accesso al router ..... 16**

**Capitolo 4 Configurazione della connessione Internet ..... 19**

4.1 Connessione a Internet tramite cavo Ethernet ..... 21

4.1.1 Configurazione di base ..... 21

4.1.2 Protocollo ..... 22

4.2 Connessione a Internet tramite una rete Wi-Fi esistente ..... 25

4.2.1 Configurazione di base ..... 25

4.2.2 Opzioni Ripetitore ..... 28

**Capitolo 5 Wireless ..... 29**

5.1 5 GHz Wi-Fi ..... 30

5.2 2.4 GHz Wi-Fi ..... 32

**Capitolo 6 Client ..... 34**

6.1 Dettagli del dispositivo ..... 36

6.2 Azione ..... 38

6.3 Rimozione dei client ..... 40

6.4 Ordinamento ..... 41

**Capitolo 7 Conoscere le VPN ..... 42**

7.1 Introduzione ..... 43

7.2 Scenari di utilizzo ..... 44

**Capitolo 8 Dashboard VPN ..... 47**

8.1 Client VPN ..... 48

8.1.1 Opzioni client ..... 49
8.1.2 Modalità delle policy ..... 51
8.1.3 Opzioni globali ..... 52
8.2 Server VPN ..... 55
8.2.1 Opzioni server ..... 56
8.2.2 Regola di routing del server ..... 57
8.2.3 Opzioni globali ..... 59
**Capitolo 9 Configurazione del server VPN ..... 60**
9.1 Configurazione del server OpenVPN ..... 61
9.1.1 Preparazione ..... 61
9.1.2 Procedura di configurazione ..... 62
9.1.3 Risoluzione dei problemi ..... 64
9.2 Configurazione del server WireGuard ..... 66
9.2.1 Preparazione ..... 66
9.2.2 Procedura di configurazione ..... 67
9.2.3 Risoluzione dei problemi ..... 70
**Capitolo 10 Configurazione del client VPN ..... 71**
10.1 Configurazione del client OpenVPN ..... 72
10.1.1 Preparazione ..... 72
10.1.2 Configurazione di NordVPN ..... 72
10.1.3 Configurazione manuale del client OpenVPN (altri provider) ..... 78
10.2 Configurazione del client WireGuard ..... 81
10.2.1 Preparazione ..... 81
10.2.2 Configurazione di AzireVPN ..... 82
10.2.3 Configurazione di Mullvad ..... 85
10.2.4 Configurazione manuale del client WireGuard (altri provider) ..... 89
**Capitolo 11 Tor ..... 93**
**Capitolo 12 Applicazioni ..... 95**
12.1 Plug-in ..... 96
12.2 DNS dinamico ..... 97
12.2.1 Abilita DDNS ..... 97
12.2.2 Verifica del funzionamento del DDNS ..... 100
12.2.3 Accesso remoto HTTPS ..... 102
12.2.4 Accesso remoto SSH ..... 104

12.3 GoodCloud ..... 106
12.3.1 Attivazione di GoodCloud ..... 107
12.3.2 Gestione del router ..... 111
12.3.3 Dissociazione del dispositivo ..... 116
12.4 AdGuard Home ..... 118
12.5 Controllo parentale ..... 120
12.5.1 Configurazione rapida ..... 120
12.5.2 Risoluzione dei problemi ..... 128
12.6 ZeroTier ..... 129
12.6.1 Configurazione di ZeroTier ..... 130
12.6.2 Consenti accesso remoto WAN ..... 134
12.6.3 Consenti accesso remoto LAN ..... 135
12.7 Tailscale ..... 136
12.7.1 Configurazione di Tailscale ..... 137
12.7.2 Consenti accesso remoto WAN ..... 140
12.7.3 Consenti accesso remoto LAN ..... 141
12.7.4 Nodi di uscita personalizzati ..... 142
**Capitolo 13 Rete ..... 144**
13.1 Firewall ..... 145
13.1.1 Port forwarding ..... 145
13.1.2 Apertura delle porte sul router ..... 147
13.1.3 DMZ ..... 148
13.2 Multi-WAN ..... 149
13.2.1 Monitoraggio dello stato dell'interfaccia ..... 149
13.2.2 Modalità Multi-WAN ..... 152
13.3 LAN ..... 155
13.3.1 Impostazioni di base ..... 155
13.3.2 Server DHCP ..... 156
13.3.3 Prenotazione indirizzi ..... 158
13.4 Rete ospiti ..... 159
13.4.1 Impostazioni di base ..... 159
13.4.2 Server DHCP ..... 160
13.5 DNS ..... 162
13.5.1 Impostazioni generali ..... 162

13.5.2 Impostazioni del server DNS ..... 163
13.5.3 Modifica del file hosts ..... 165
13.6 Modalità di rete ..... 167
13.7 IPv6 ..... 170
13.7.1 Modalità IPv6 ..... 170
13.7.2 Metodo di acquisizione DNS ..... 171
13.8 Indirizzo MAC ..... 172
13.9 Gateway drop-in ..... 174
13.10 IGMP Snooping ..... 176
13.11 Accelerazione di rete ..... 177
13.12 Impostazioni NAT ..... 178
**Capitolo 14 Sistema ..... 179**
14.1 Panoramica ..... 180
14.2 Aggiornamento ..... 181
14.2.1 Aggiornamento online ..... 181
14.2.2 Aggiornamento locale ..... 182
14.3 Attività pianificate ..... 184
14.3.1 Programmazione del LED ..... 184
14.3.2 Riavvio pianificato ..... 185
14.3.3 Programmazione del Wi-Fi a 5 GHz ..... 186
14.3.4 Programmazione del Wi-Fi a 2,4 GHz ..... 188
14.4 Fuso orario ..... 191
14.5 Registro ..... 193
14.6 Sicurezza ..... 194
14.6.1 Password amministratore ..... 194
14.6.2 Controllo dell'accesso locale ..... 195
14.6.3 Controllo dell'accesso remoto ..... 197
14.7 Ripristino del firmware ..... 199
14.8 Impostazioni avanzate ..... 200

Capitolo 1

# Conoscere il router

Questo capitolo tratta la panoramica del router, le specifiche e il contenuto della confezione.

## 1.1 Panoramica del prodotto

Il router Marble (GL-B3000) è un'arte a sé stante, sapientemente esposta come una cornice per foto per ospitare la tua opera d'arte preferita ed elevare il tuo spazio abitativo. Non solo un piacere visivo per gli occhi, il router Marble (GL-B3000) offre prestazioni di prim'ordine grazie alla funzionalità Wi-Fi 6 e al supporto delle funzionalità VPN.

### 1.1.1 Aspetto



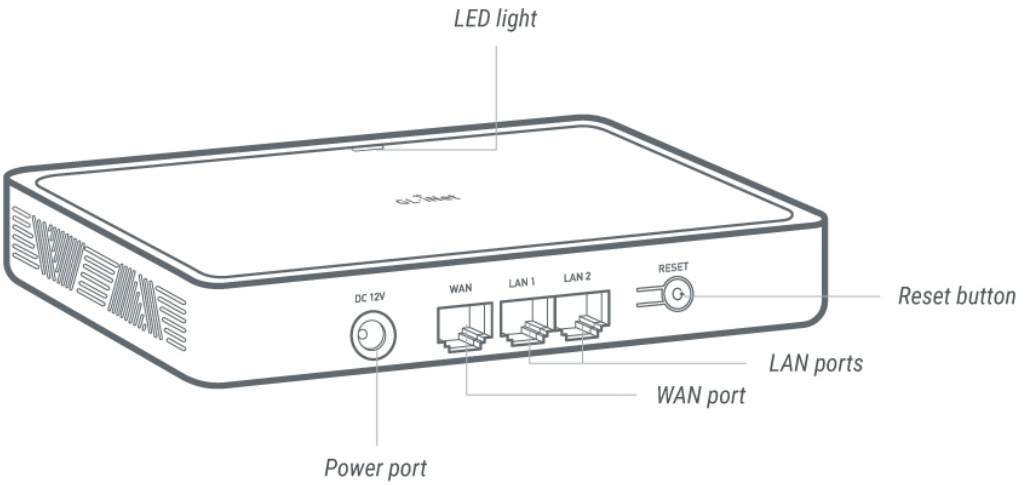








## 1.1.2 Interfacce e pulsanti




| Voce | Descrizione |
|---|---|
| Porta di alimentazione | Consente di collegare l'alimentatore. |
| Porta WAN | Consente di collegare un modem o una presa Ethernet per accedere a Internet. |
| Porta LAN | Consente di collegare dispositivi cablati, se necessario. |
| Pulsante di ripristino | Tieni premuto per **4 secondi** per riparare la tua rete;<br>Tenere premuto per **10 secondi,** quindi rilasciare per ripristinare router alle impostazioni di fabbrica. |

### 1.1.3 LED

| Stato | Indicazione |
|---|---|
| Blu fisso | Avvio del sistema |
| Blu lampeggiante lentamente | Ricerca rete |
| Blu lampeggiante rapidamente | Aggiornamento del firmware |
| Bianco fisso | Funziona normalmente |

## 1.2 Specifiche tecniche

| | |
|---|---|
| Interfaccia | 1 x porta Ethernet WAN<br>2 x porta Ethernet LAN<br>1 x 12V/1.5A Ingresso CC<br>1 pulsante di ripristino |
| CPU | Qualcomm Dual-core, @1GHz |
| Memoria/Archiviazione | DDR3L 512MB / NAND Flash 128MB |
| Protocollo | IEEE 802.11a/b/g/n/ac/ax |
| Velocità Wi-Fi | 574Mbps (2.4GHz), 2402Mbps (5GHz) |
| Antenne | 4 x Antenne Interne |
| Velocità Ethernet | 10/100/1000Mbps |
| Ingresso alimentazione | DC5521, 12V/1.5A (5.5*2.1mm) |
| Consumo energetico | < 13W |
| Temperatura di esercizio | 0 ~ 40°C (32 ~ 104°F) |
| Temperatura di conservazione | -20 ~ 70°C (-4 ~ 158°F) |
| Dimensioni/Peso | Router: 155 x 120 x 23mm / 275 g |

| | |
|---|---|
| | Cornice per foto: 235 x 197 x 32mm (adatta per una foto 8 in pollici) |
| Altri strumenti | Scheda tecnica / Firmware / App / Unboxing / Tutorial |

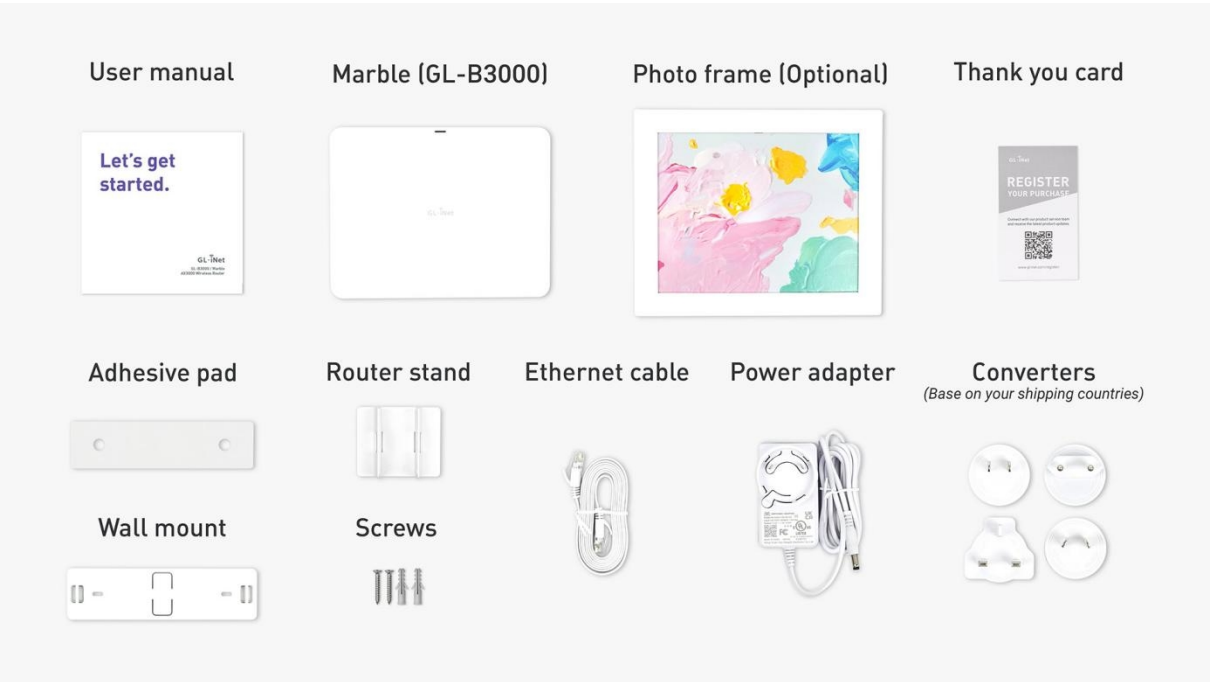
*Le velocità wireless si basano sugli standard IEEE 802.11 (ad esempio, 802.11ax per Wi-Fi 6). La velocità effettiva e la portata potrebbero essere inferiori a causa di ostacoli ambientali (muri, metallo), congestione della rete o funzionalità del dispositivo client.
*L'uso di Wi-Fi 6 (802.11ax) e le sue funzionalità (OFDMA, MU-MIMO, 1024-QAM, HT160) richiede che i dispositivi client supportino le tecnologie corrispondenti.

## 1.3 Contenuto della confezione

Tieni presente che l'adattatore all'interno del pacchetto dipende dal paese di spedizione.

La confezione include:

- 1 x Marmo (GL-B3000)
- 1 x Manuale utente
- 1 x Biglietto di ringraziamento
- 1 x cavo Ethernet
- 1 Kit di montaggio a parete
- 1 x Cuscinetto adesivo
- 1 x Supporto per router
- 1 x Cornice per foto (opzionale)
- 1 x Adattatore di alimentazione
- 1 x Convertitore (in base al Paese di spedizione)



Capitolo 2

# Collegamenti hardware

Questo capitolo tratta la selezione della posizione del router e i passaggi di connessione.

## 2.1 Scelta della posizione

Segui questi suggerimenti per scegliere una posizione per ottenere le migliori prestazioni.

- **Evita umidità e calore**: non posizionare il router vicino ad acqua, in ambienti umidi o esposti a temperature elevate (ad esempio accanto a lavelli o radiatori).
- **Ventilazione e raffreddamento**: posizionare il router in un'area fresca e ben ventilata per una corretta dissipazione del calore.-
- **Posizionamento centrale**: posiziona il router in un punto in cui possa collegarsi facilmente all'alimentazione e a più dispositivi (ad esempio, nella zona centrale del soggiorno).
- **Comodità dei cavi**: posiziona i cavi e il cavo di alimentazione in modo sicuro per evitare rischi di inciampo.
- **Posizionamento**: posiziona il router su una superficie piana e stabile (mensola, scrivania) oppure montalo a parete utilizzando il kit di montaggio a parete incluso.
- **Evita le interferenze elettromagnetiche**: tieni il router lontano da dispositivi Bluetooth e forni a microonde per ridurre le interferenze sul segnale.

## 2.2 Collegamento del router

1. **Accendi**

   Monta insieme l'alimentatore in due pezzi. Collegalo al router e collegalo a una presa. Si avvierà automaticamente.
2. **Connetti un dispositivo al router**

   Collega un dispositivo (ad esempio, laptop o smartphone) al router tramite Wi-Fi o cavo Ethernet.
   - **Wi-Fi**: sul tuo dispositivo, vai su Impostazioni > WLAN, individua il nome della rete Wi-Fi del router nell'elenco delle reti disponibili e inserisci la password. Puoi trovare il nome della rete e la password predefiniti stampati sull'etichetta del router.
   - **Ethernet**: collega il tuo dispositivo alla porta LAN del router tramite un cavo Ethernet.
3. **Accedi al router**

   Internet non è disponibile quando ci si connette al router per la prima volta. Accedi al router come indicato nel capitolo 3 per completare la configurazione iniziale prima di accedere a Internet.

Capitolo 3

# Accesso al router

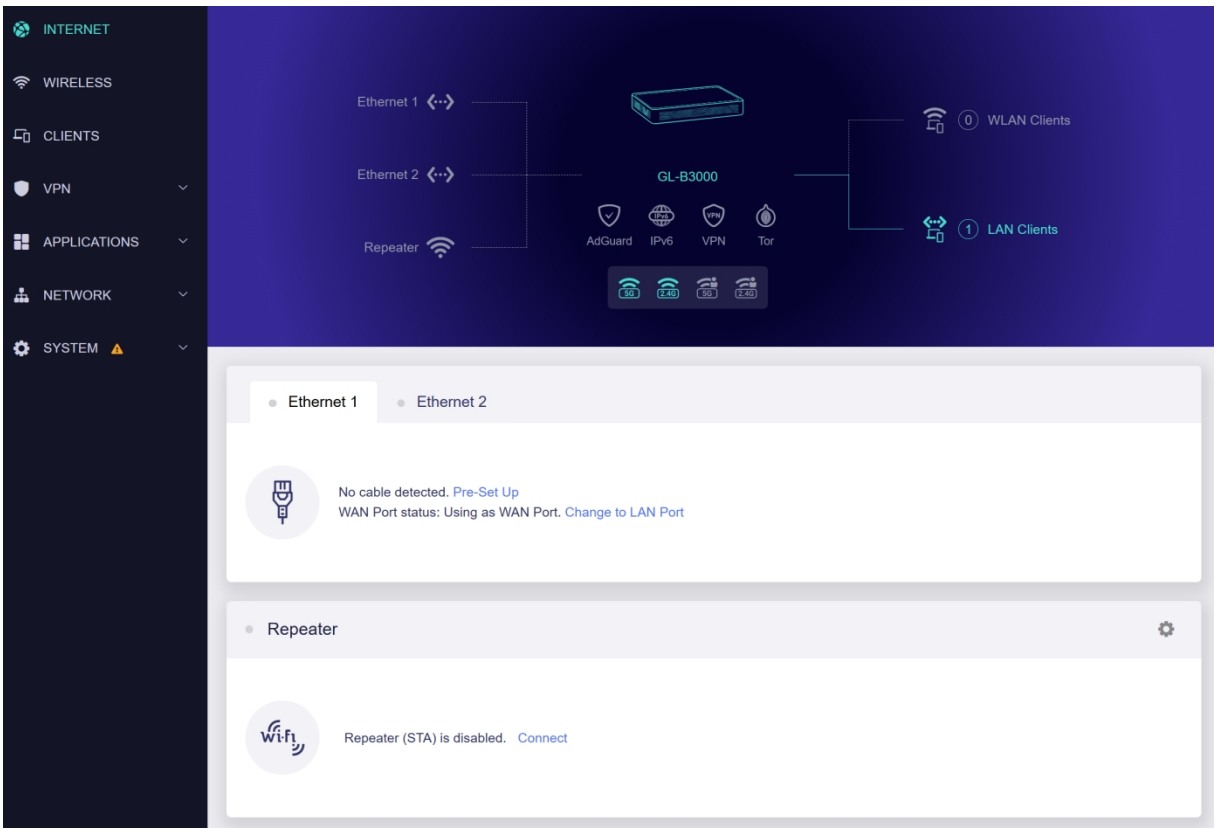
Questo capitolo ti guida ad accedere al router tramite pannello di amministrazione web.

Configura e gestisci il tuo router tramite un'interfaccia di gestione basata sul Web, a cui è possibile accedere su qualsiasi sistema operativo Windows, Mac OS o Linux con un browser Web, come Microsoft Edge, Google Chrome, Mozilla Firefox o Apple Safari.

**Nota**: se preferisci utilizzare l'app GL.iNet anziché pannello di amministrazione web, scarica l'app e segui le istruzioni visualizzate.

**Segui i passaggi seguenti per accedere al router tramite pannello di amministrazione web**.

1. Collega un dispositivo (ad esempio un computer o un laptop) al router tramite Wi-Fi o un cavo Ethernet.
2. Apri un browser web (si consiglia Chrome e Edge) e visita http://192.168.8.1. Verrai indirizzato alla pagina di accesso di pannello di amministrazione web. Se non riesci ad accedere al pannello di amministrazione web, vedi qui per la risoluzione dei problemi.
3. Imposta la tua password di amministratore. Si consiglia una password complessa per la sicurezza. Quindi fai clic su **Avanti** per continuare.
4. Inserirai quindi il codice pannello di amministrazione web del router.



Capitolo 4

# Configurazione della connessione Internet

Questo capitolo introduce diversi metodi di connessione Internet per consentire al router di adattarsi a diversi ambienti di rete.

Marble supporta due metodi di connessione Internet: Ethernet e Ripetitore, scegli il metodo appropriato in base alle tue esigenze di utilizzo.

1. **Ethernet**: collega il router a una rete a banda larga utilizzando un cavo Ethernet collegato alla porta WAN. Il router in genere ottiene automaticamente un indirizzo IP tramite DHCP. Gli utenti possono anche configurare manualmente un IP statico o le impostazioni PPPoE. Questo metodo offre elevata stabilità e velocità elevata, rendendolo ideale per ambienti domestici e di ufficio con accesso a banda larga fisso.

2. **Ripetitore**: questa modalità consente al router di connettersi a una rete Wi-Fi esistente per estendere il segnale Wi-Fi e creare una rete locale separata e sicura. Si noti che la velocità di trasmissione potrebbe essere ridotta in una certa misura. È ideale per le zone morte Wi-Fi che richiedono l'estensione del segnale o per i luoghi pubblici in cui è necessaria una maggiore sicurezza della rete.

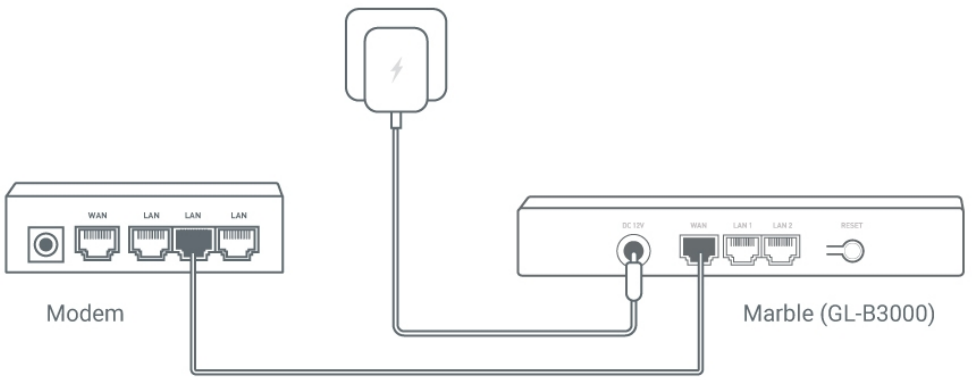
## 4.1 Connessione a Internet tramite cavo Ethernet

Collega il router a una rete a banda larga utilizzando un cavo Ethernet collegato alla porta WAN. Il router in genere ottiene automaticamente un indirizzo IP tramite DHCP. Gli utenti possono anche configurare manualmente un IP statico o le impostazioni PPPoE. Questo metodo offre elevata stabilità e velocità elevata, rendendolo ideale per ambienti domestici e di ufficio con accesso a banda larga fisso.

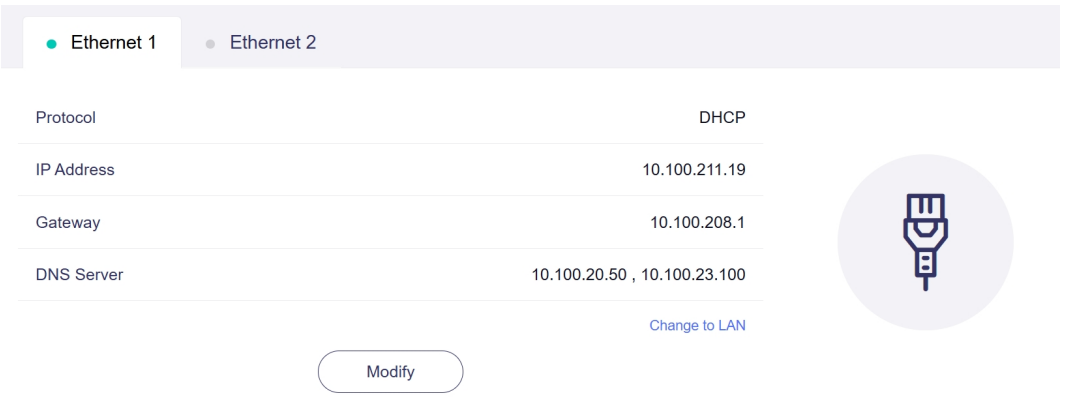
### 4.1.1 Configurazione di base

Segui i passaggi seguenti per connettere il router a Internet tramite un cavo Ethernet.

1. Collega la porta **WAN** del router al dispositivo a monte (ad esempio, un modem ISP, un router primario, uno switch di rete o un jack Ethernet) tramite un cavo Ethernet.

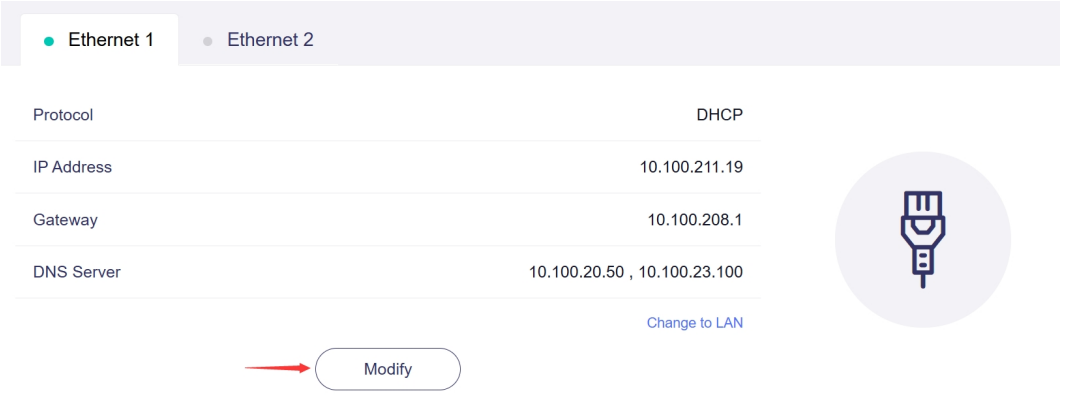



2. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Ethernet**. Se la connessione ha esito positivo, la sezione Ethernet visualizzerà i dettagli della rete, inclusi protocollo, indirizzo IP, gateway e Server DNS.



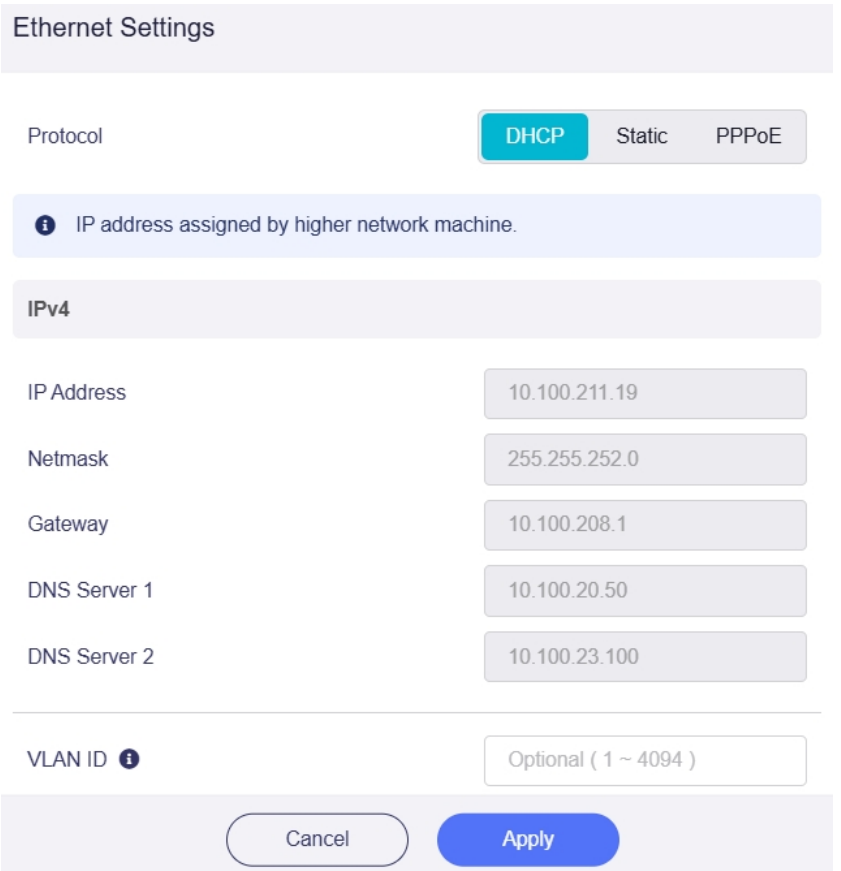
## 4.1.2 Protocollo

Esistono tre tipi di protocolli: DHCP, statico e PPPoE. Fai clic su **Modifica** per modificare.




- **DHCP**

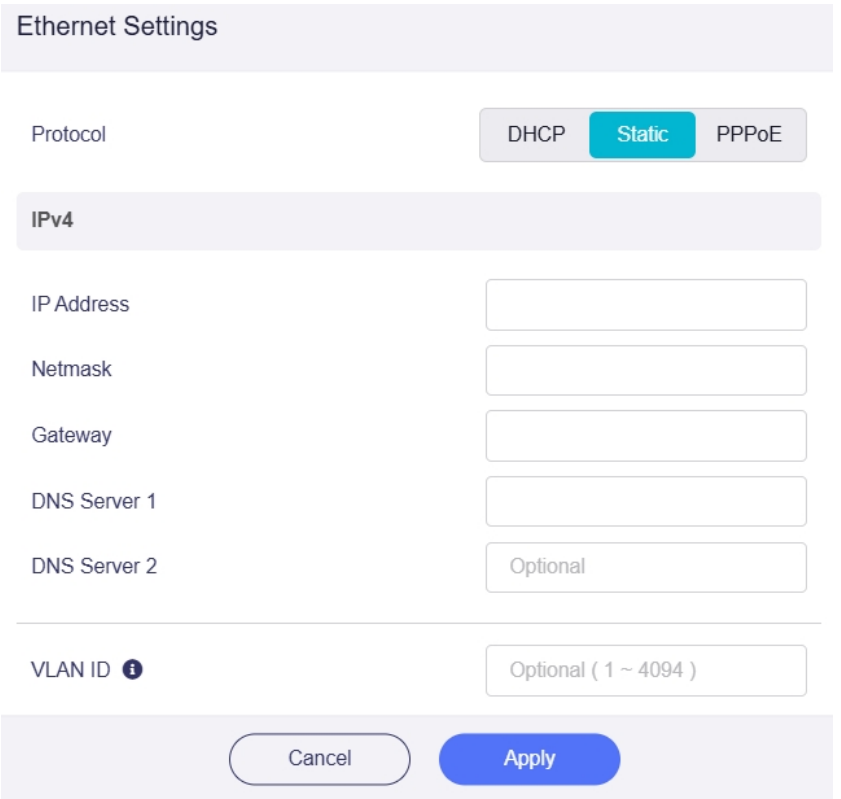
  DHCP è il protocollo di rete predefinito e più comune, che assegna automaticamente indirizzi IP e altri parametri di configurazione di rete ai dispositivi su una rete IP tramite un modello client-server.




  Puoi configurare uno **ID VLAN** se il tuo fornitore di servizi richiede che l'interfaccia utilizzi uno ID VLAN con tag specifico.

- **Statico**

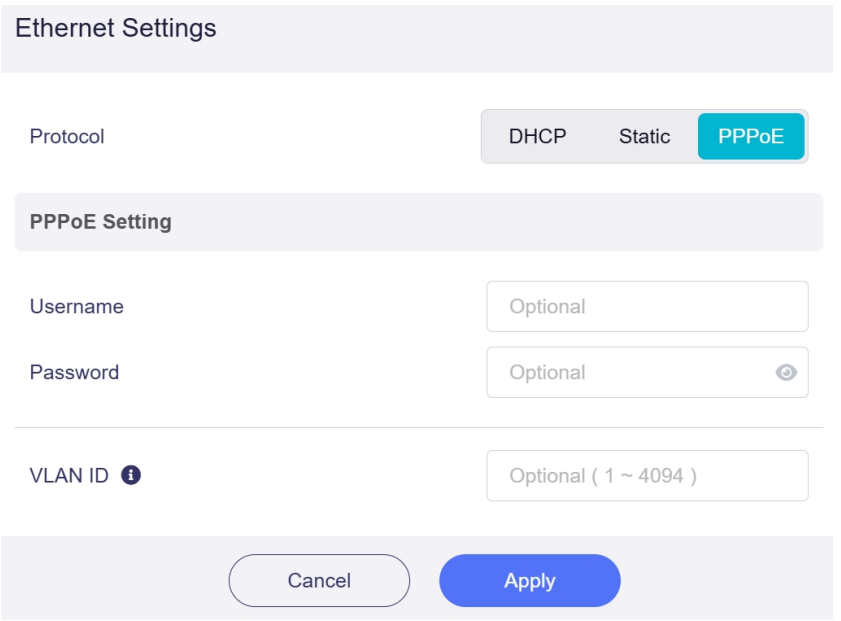
  Un indirizzo IP statico è richiesto se il tuo ISP (provider di servizi Internet) assegna un indirizzo IP pubblico fisso o se devi configurare manualmente i parametri di rete (ad esempio indirizzo IP, gateway, maschera di sottorete).




  Puoi configurare uno **ID VLAN** se il tuo fornitore di servizi richiede che l'interfaccia utilizzi uno ID VLAN con tag specifico.

- **PPPoE**

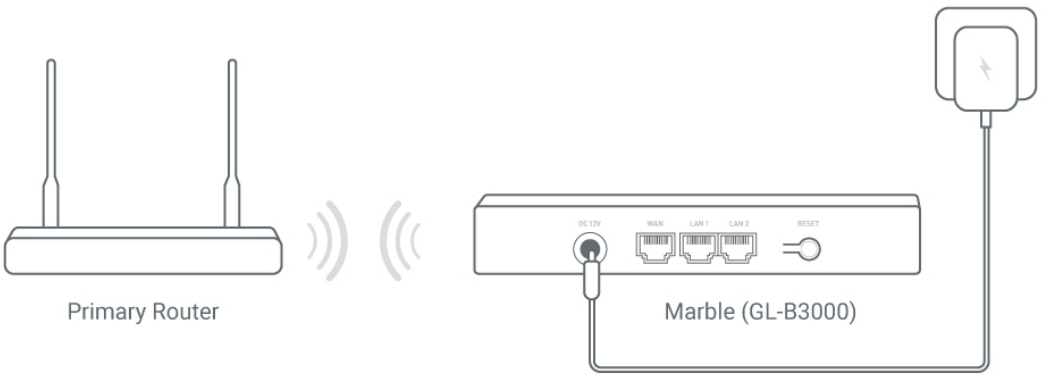
  PPPoE (Point-to-Point Protocol over Ethernet) è un protocollo di rete ampiamente utilizzato dagli ISP. In genere, forniscono un modem insieme a un nome utente e una password univoci, necessari per configurare una connessione Internet.




Puoi configurare uno **ID VLAN** se il tuo fornitore di servizi richiede che l'interfaccia utilizzi uno ID VLAN con tag specifico.

## 4.2 Connessione a Internet tramite una rete Wi-Fi esistente

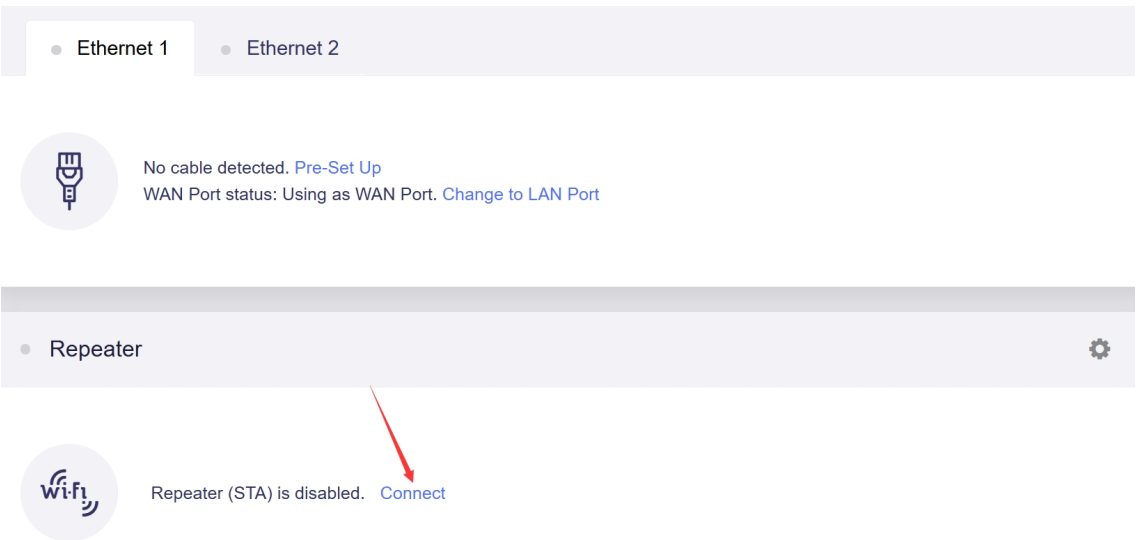
Collega il router come ripetitore alla rete wireless esistente per potenziare i segnali Wi-Fi e creare una rete locale isolata dalla rete primaria. Negli hotel o nei bar con hotspot pubblici gratuiti, l'utilizzo di un ripetitore non solo rafforza i segnali Wi-Fi, ma fornisce anche l'accesso cablato e wireless per più dispositivi e salvaguarda la sicurezza della rete.



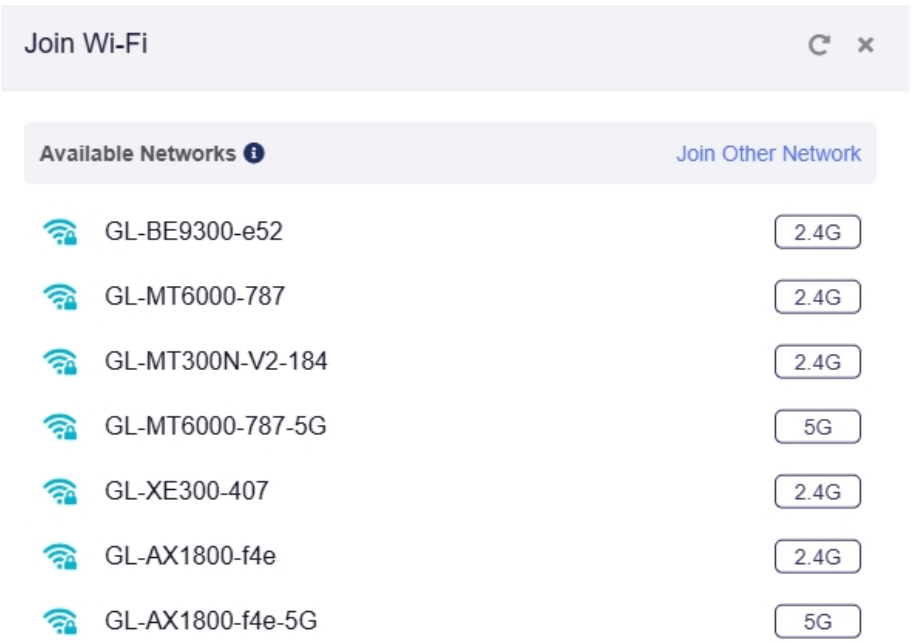

La funzione ripetitore GL.iNet funziona in modalità WISP (Wireless Internet Service Provider) per impostazione predefinita, il che significa che il router creerà la propria sottorete e fungerà da firewall per proteggerti dalla rete pubblica.

### 4.2.1 Configurazione di base

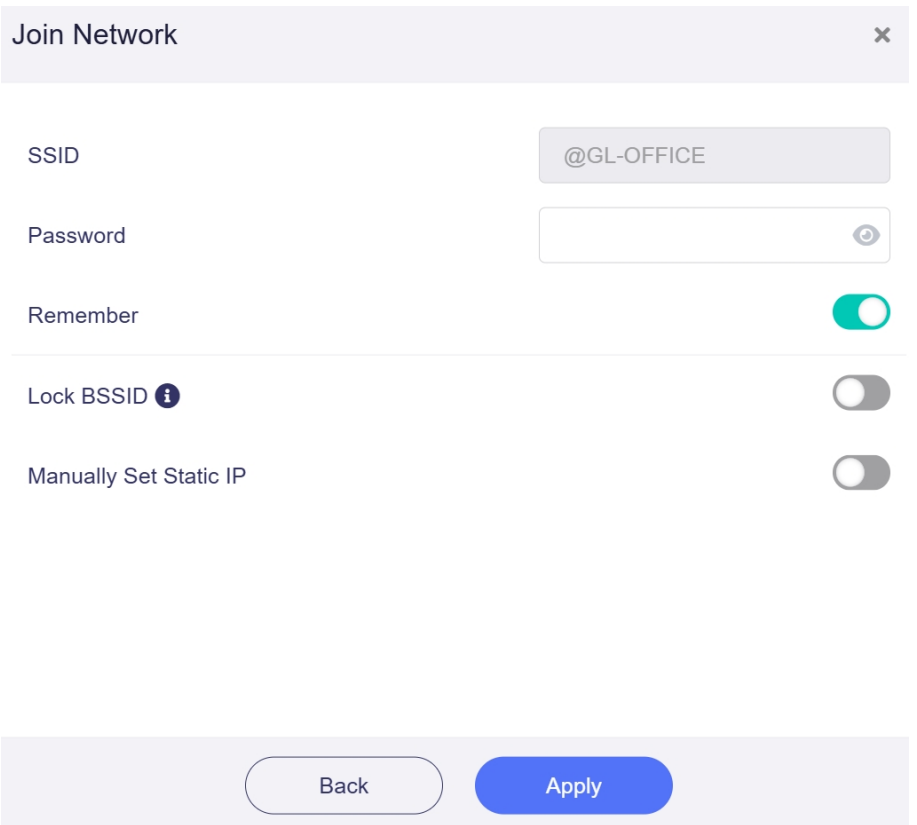
1. Accedi al pannello di amministrazione web del router e vai a **INTERNET** > **Ripetitore**. Fai clic su **Connetti**.



2. Nella finestra pop-up, scegli la rete Wi-Fi a cui desideri connetterti dall'elenco delle reti disponibili.



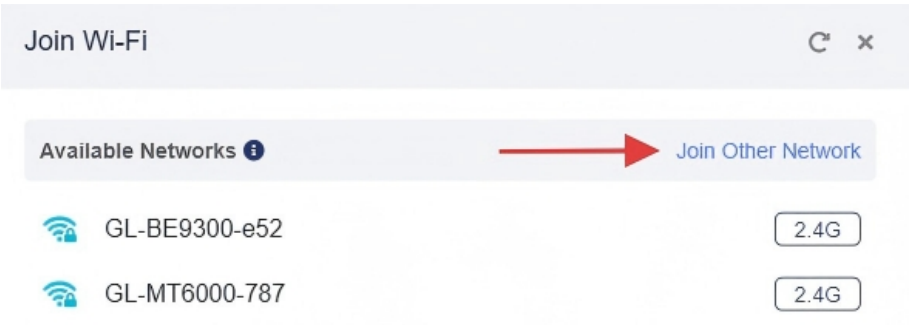

3. Inserisci la password Wi-Fi corretta e fai clic su **Applica**.



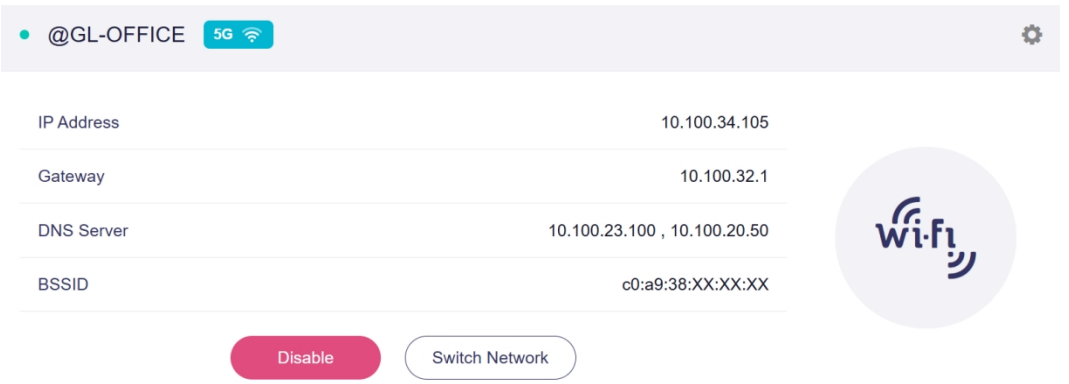

- **Ricorda**: attiva questa opzione per ricordare l'attuale rete Wi-Fi ripetuta.

- **Blocca BSSID**: se abilitato, il router si connetterà solo al punto di accesso (AP) specifico corrispondente al BSSID selezionato, anche quando altri AP condividono lo stesso SSID.
- **Imposta manualmente IP statico**: se abilitato, è possibile configurare manualmente l'indirizzo IP, la maschera di sottorete, il gateway e i server DNS, invece di ottenere automaticamente le impostazioni IP tramite DHCP.

4. Se l'SSID Wi-Fi di destinazione non è nell'elenco delle reti disponibili, fai clic su **Accedi a un'altra rete** nell'angolo in alto a destra, inserisci manualmente l'SSID Wi-Fi e altre informazioni richieste, quindi fai clic su **Applica**.

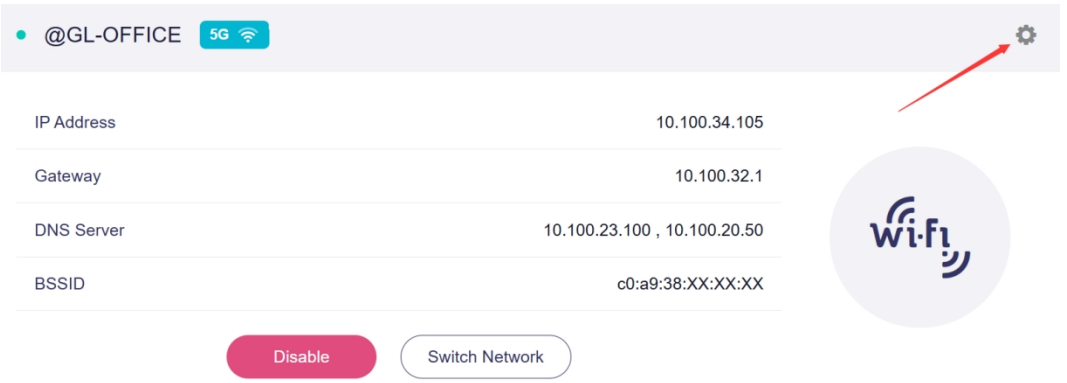



5. Attendere un minuto affinché il router si connetta. Una volta connesso, la pagina viene visualizzata come di seguito.

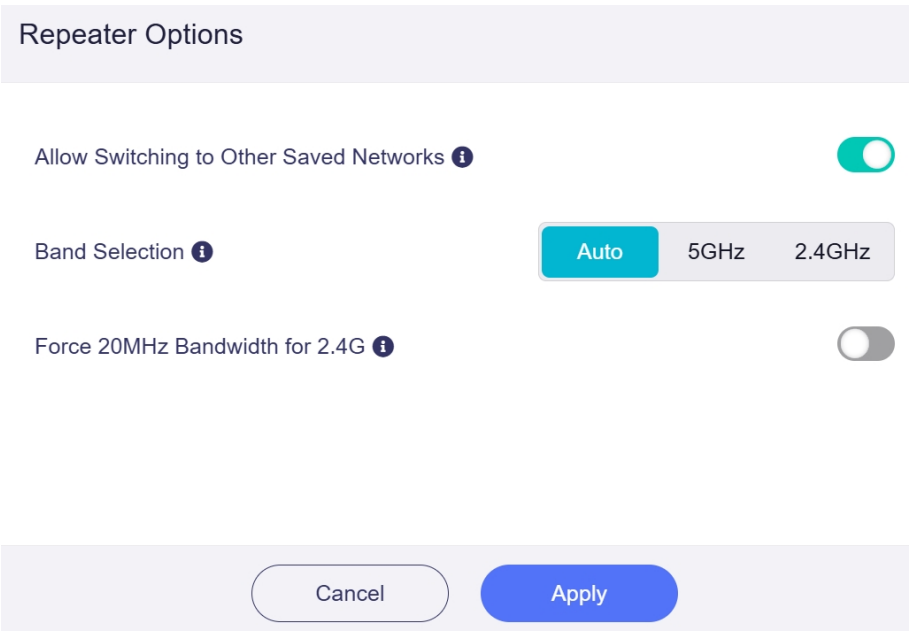


## 4.2.2 Opzioni Ripetitore

Fai clic sull'icona a forma di ingranaggio nell'angolo in alto a destra per configurare le opzioni Ripetitore.




La pagina può variare a causa delle diverse versioni del firmware.




- **Consenti il passaggio ad altre reti salvate**: se l'opzione è abilitata, il router si connetterà automaticamente ad altre reti salvate quando non è in grado di connettersi alla rete Wi-Fi corrente.
- **Selezione della banda**: se selezioni manualmente una banda, il router non eseguirà la scansione né si connetterà a qualsiasi Wi-Fi che utilizza un'altra banda.
- **Forza larghezza di banda 20MHz per 2.4G**: se questa opzione è abilitata, il dispositivo migliorerà la stabilità della connessione riducendo la velocità di connessione.
  **Nota**: funziona solo quando si ripete 2.4G Wi-Fi.

Capitolo 5

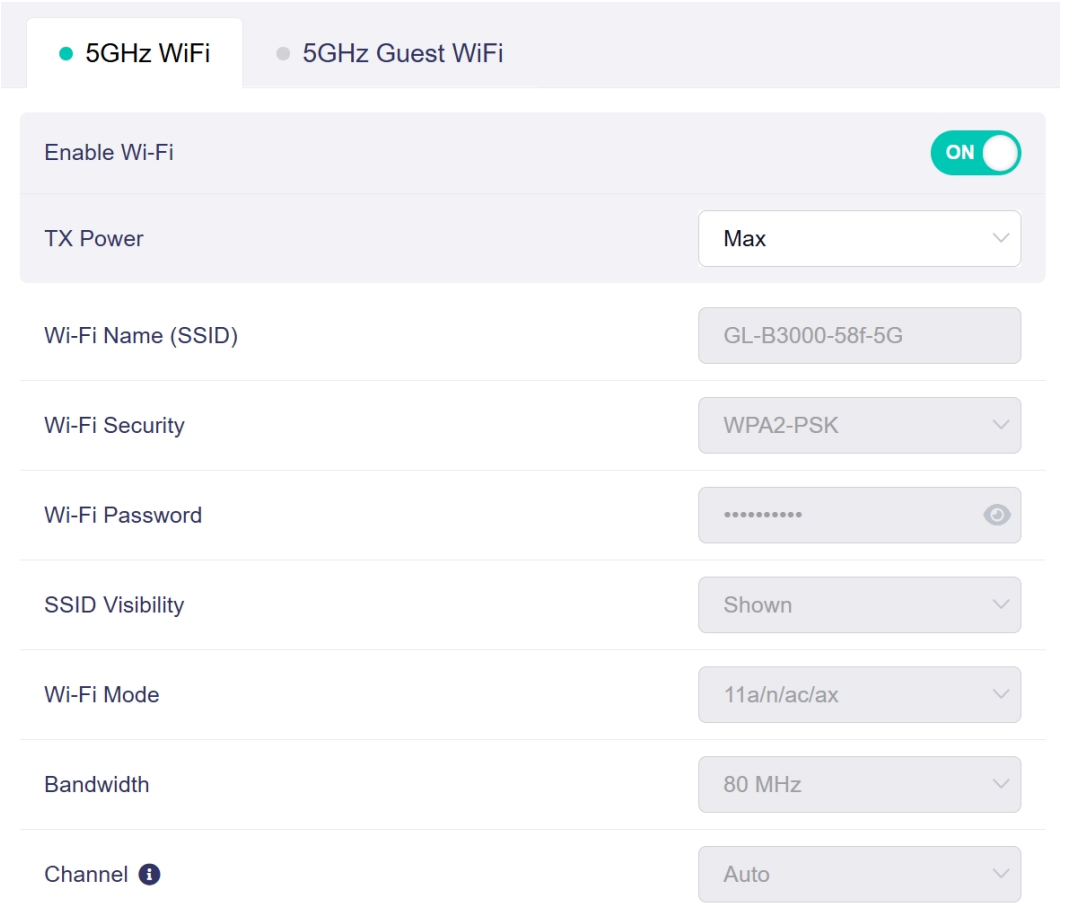
# Wireless

Questo capitolo guida l'utente a verificare lo stato del Wi-Fi e a configurare le impostazioni wireless.

Accedi al pannello di amministrazione web del router e vai a **WIRELESS**.
La pagina wireless visualizza le impostazioni 5GHz e 2.4 GHz Wi-Fi del router, ciascuna ulteriormente suddivisa in reti Wi-Fi principali e reti ospiti Wi-Fi per una gestione flessibile.

## 5.1 5 GHz Wi-Fi

Lo Wi-Fi principale 5 GHz consente di configurare più impostazioni, tra cui abilitare/disabilitare Wi-Fi, impostare la potenza TX, impostare il nome Wi-Fi (SSID), sicurezza, password, visibilità SSID, modalità, larghezza di banda e canale.

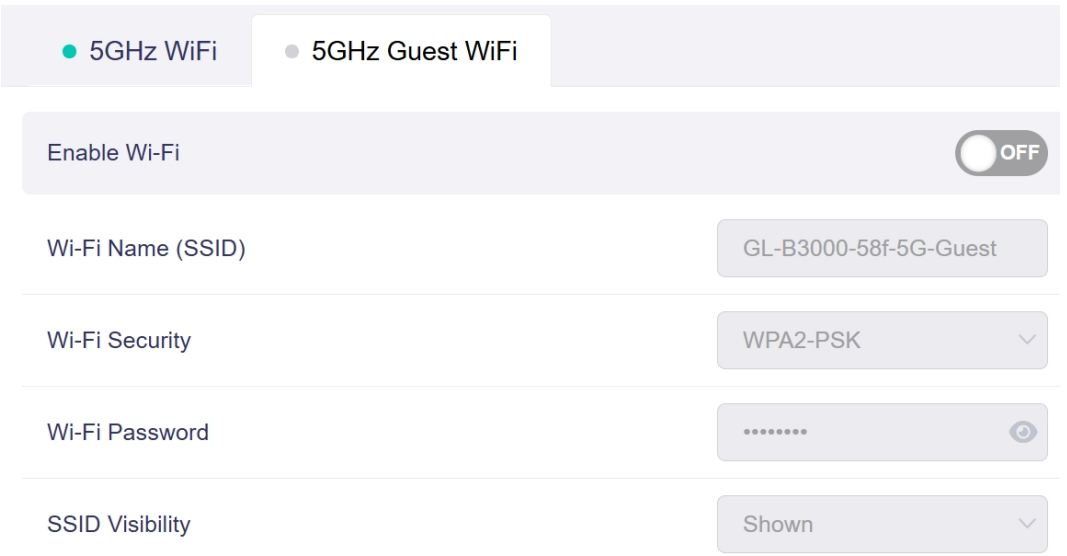



**Nota**:

1. La **larghezza di banda** e **il canale** non possono essere modificati quando il router è configurato come ripetitore, poiché seguono quello della rete ripetuta.
2. Quando **Canale** è impostato su **Automatico**, il Wi-Fi del router non passerà automaticamente al canale DFS.

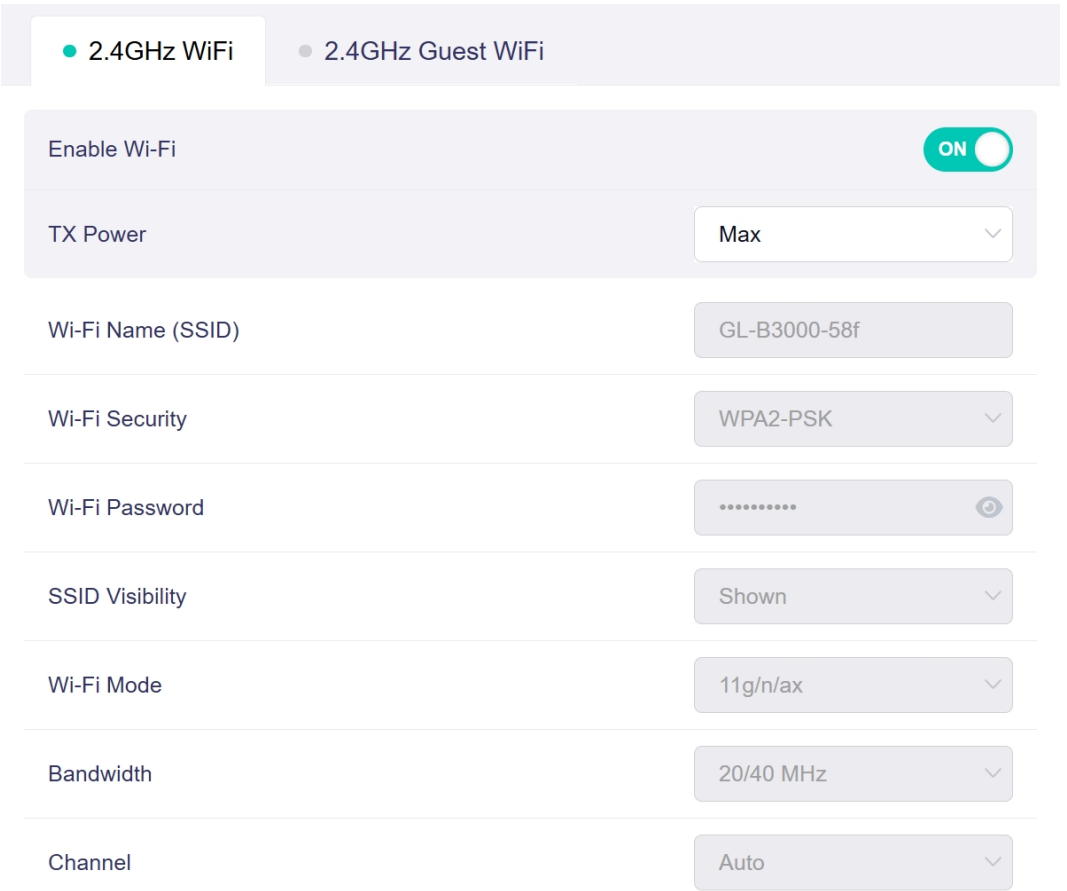
3. Quando **la larghezza di banda** è impostata su **160 MHz** (disponibile solo su alcuni modelli), Wi-Fi utilizzerà sempre il canale DFS, anche se selezioni un canale non DFS o lo imposti su Automatico.

5 GHz Guest Wi-Fi consente di configurare impostazioni semplificate, tra cui l'attivazione/disattivazione di Wi-Fi, l'impostazione del nome Wi-Fi (SSID), la sicurezza, la password e la visibilità SSID.



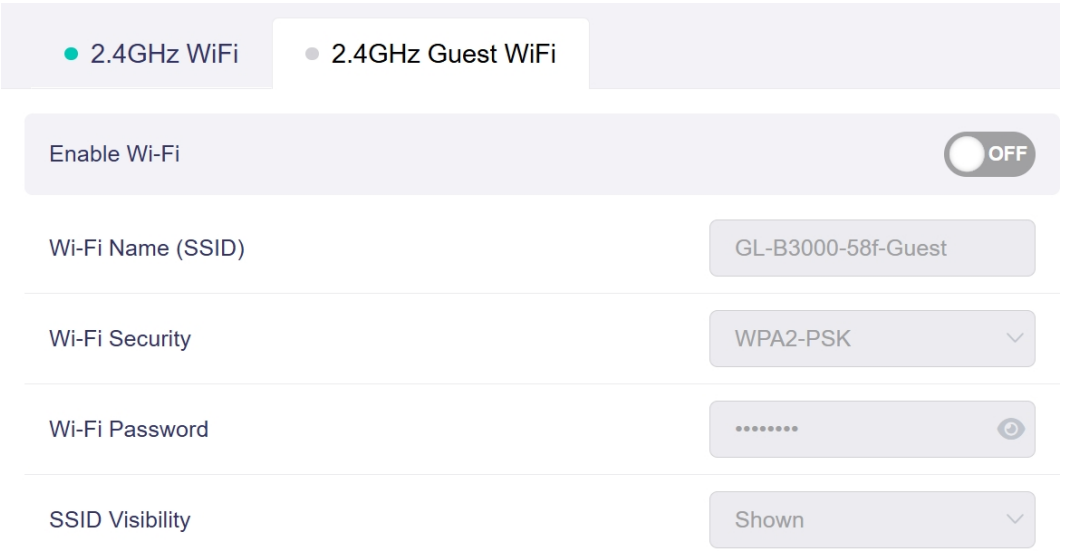
## 5.2 2.4 GHz Wi-Fi

Lo Wi-Fi principale 2.4 GHz consente di configurare più impostazioni, tra cui abilitare/disabilitare Wi-Fi, impostare la potenza TX, impostare il nome Wi-Fi (SSID), sicurezza, password, visibilità SSID, modalità, larghezza di banda e canale.




**Nota**: la **larghezza di banda** e **il canale** non possono essere modificati quando il router è configurato come ripetitore, poiché seguono quello della rete ripetuta.

2.4 GHz Guest Wi-Fi consente di configurare impostazioni semplificate, tra cui l'attivazione/disattivazione di Wi-Fi, l'impostazione del nome Wi-Fi (SSID), la sicurezza, la password e la visibilità SSID.


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

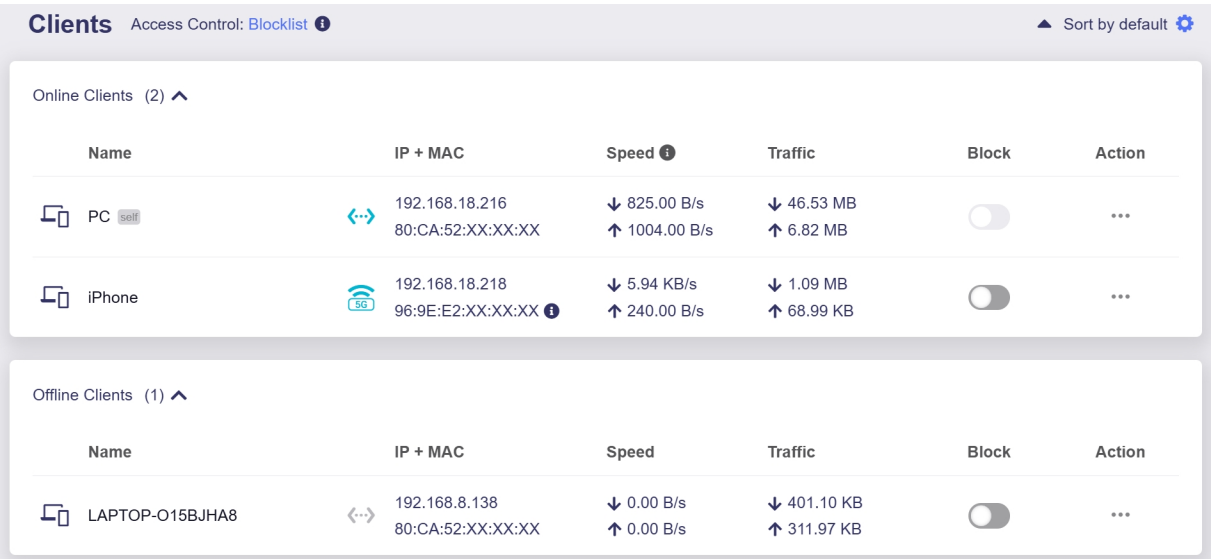
Capitolo 6

# Client

Questo capitolo ti guida a visualizzare i dettagli dei dispositivi collegati e a gestirne le connessioni.

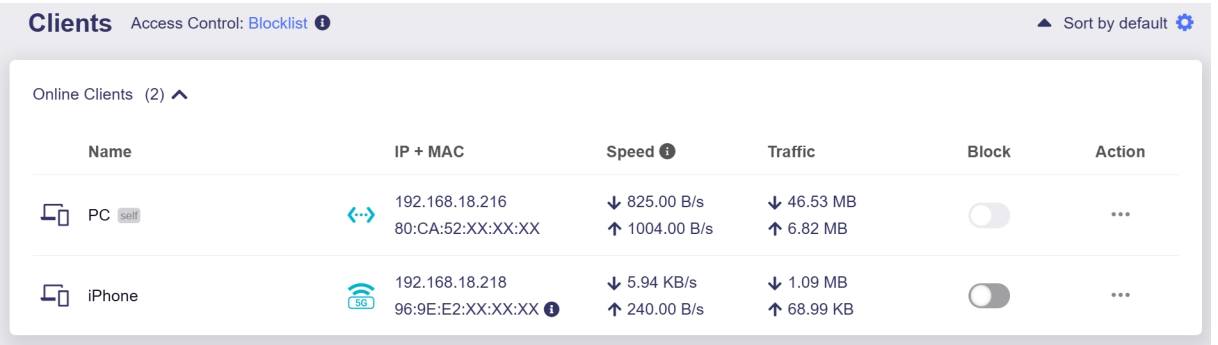
Accedi al pannello di amministrazione web del router e vai a **CLIENT**.

La pagina Client visualizza le informazioni sui dispositivi connessi, inclusi nome del dispositivo, tipo di connessione, indirizzo IP e MAC, velocità e traffico, disposti da sinistra a destra. Fornisce inoltre un accesso rapido per riservare IP, bloccare client o eseguire altre azioni.




- **Client online**: si riferisce ai dispositivi attualmente connessi alla rete del router.
- **Client offline**: si riferisce ai dispositivi che si sono precedentemente connessi al router ma che ora sono disconnessi dalla rete.

# 6.1 Dettagli del dispositivo




1. **Nome dispositivo**

   La prima colonna mostra il nome e il tipo di dispositivo, in base al nome host fornito dal dispositivo stesso. L'icona blu accanto al nome indica il tipo di connessione: in questo caso, il dispositivo è collegato al router tramite cavo Ethernet.

2. **Indirizzo IP e MAC**

   La seconda colonna elenca gli indirizzi IP e MAC del dispositivo connesso. Se i dispositivi collegati utilizzano indirizzi MAC casuali, verrà visualizzato un messaggio che indica che si tratta di un indirizzo MAC casuale.




   Se il secondo carattere dell'indirizzo MAC è 2, 6, A o E (Ignora maiuscole e minuscole), viene considerato un indirizzo MAC randomizzato. Tuttavia, alcuni dispositivi potrebbero utilizzare una regola diversa per generare un indirizzo MAC casuale, quindi questo metodo di rilevamento potrebbe non essere accurato.

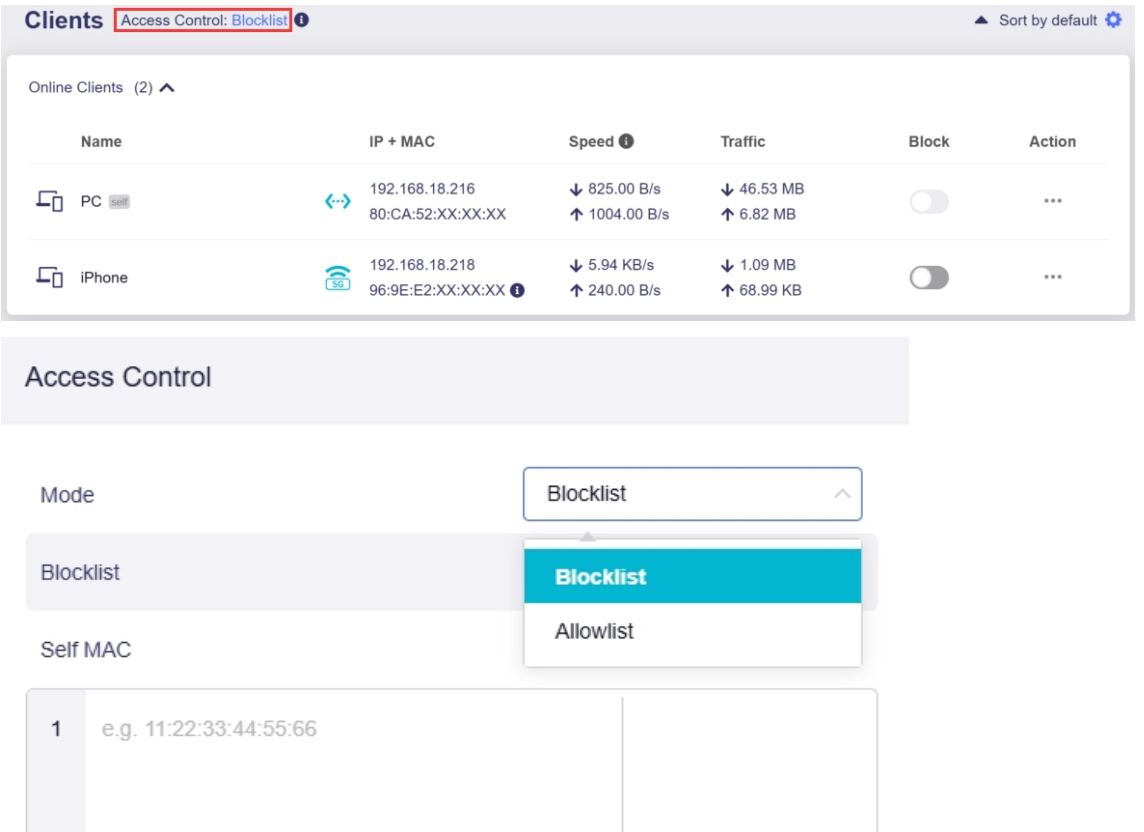
3. **Velocità**

   La terza colonna mostra la velocità Internet del dispositivo connesso. Questa velocità rappresenta la velocità media degli ultimi 3 minuti. Il sistema inizia a calcolare la velocità media quando questa pagina viene aperta (ad esempio, se la pagina è stata aperta solo per 10 secondi, la velocità media sarà basata solo su 10 secondi di dati).

4. **Traffico**: la quarta colonna mostra il traffico Internet del dispositivo connesso.

5. **Lista bloccata**

   Nella quinta colonna, puoi bloccare specifici dispositivi connessi con un clic.
   La regola di controllo dell'accesso è Blocklist per impostazione predefinita e, se necessario, puoi cambiarla in Lista consentita dall'alto.

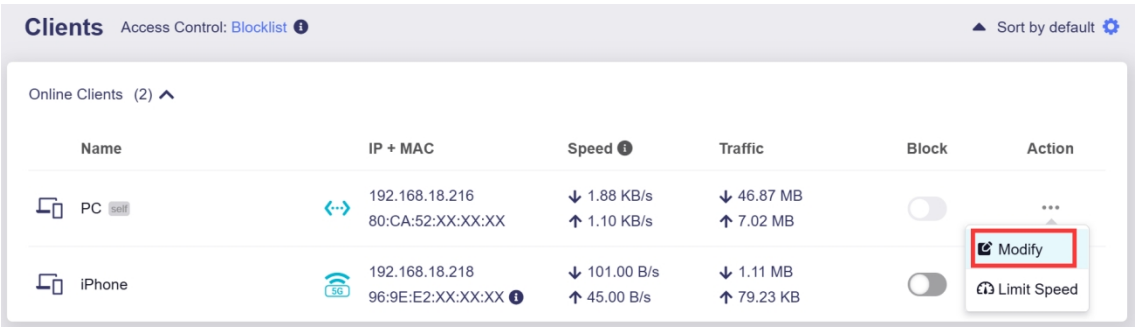


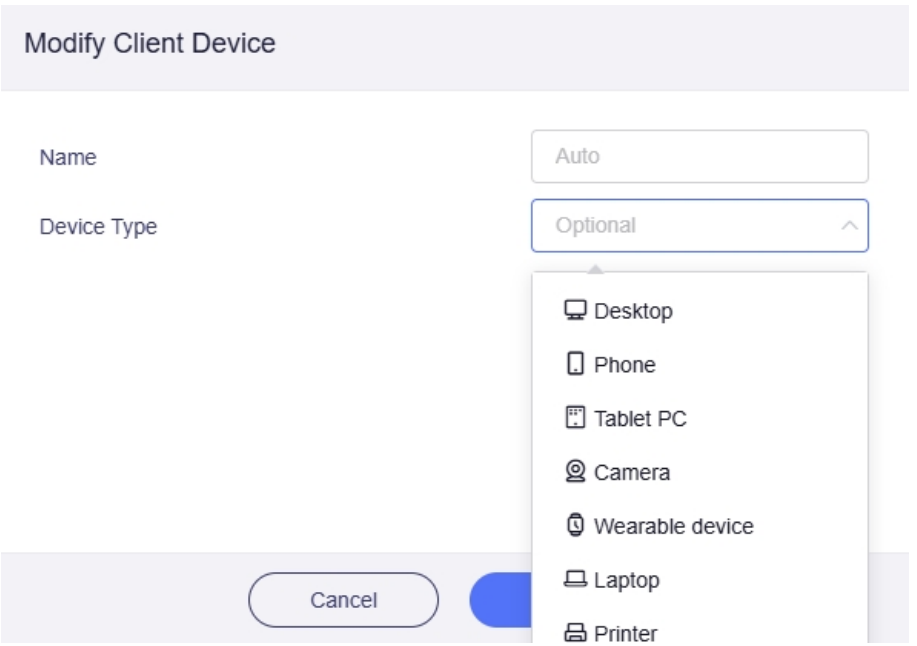

- **Lista nera**: i dispositivi con indirizzi MAC nella lista nera non possono connettersi a questo router. Tieni presente che il blocco del client si basa sull'indirizzo MAC del dispositivo. Se la prossima volta il dispositivo bloccato utilizza un indirizzo MAC diverso, può comunque riuscire a connettersi al router.
- **Lista consentita**: solo i dispositivi con indirizzi MAC specifici possono connettersi a questo router, adatto per dispositivi IoT e gestione della rete aziendale.

## 6.2 Azione

1. **Modifica**

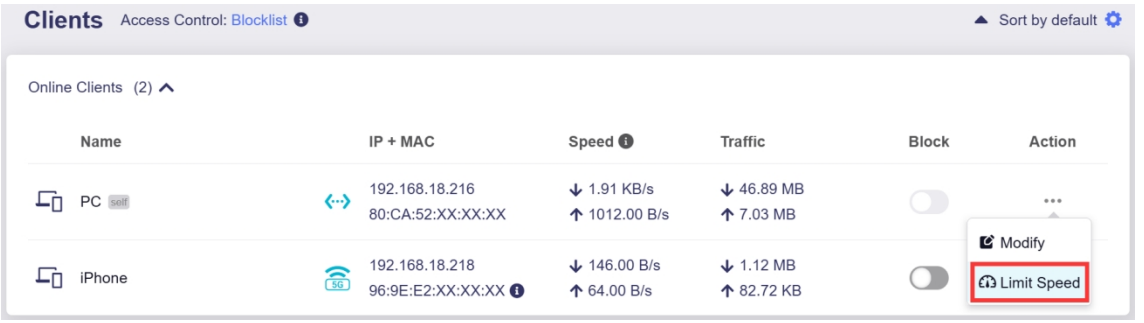
   Fai clic sull'icona a tre punti nella colonna **Azione**, quindi su **Modifica** dal menu a discesa per modificare il nome e il tipo del dispositivo.



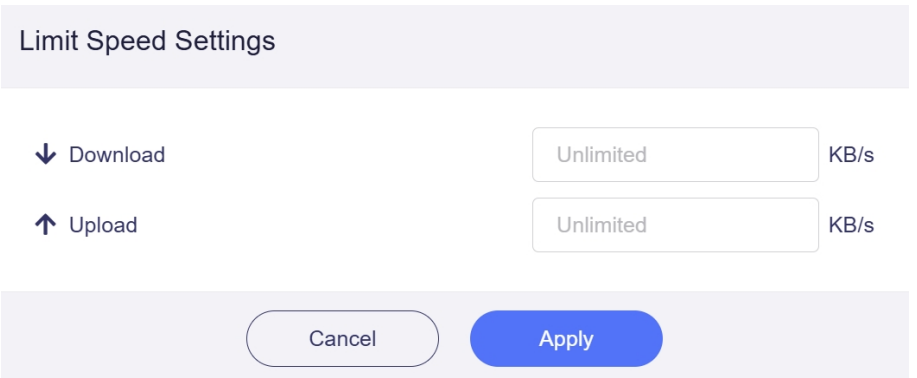



2. **Limita velocità**

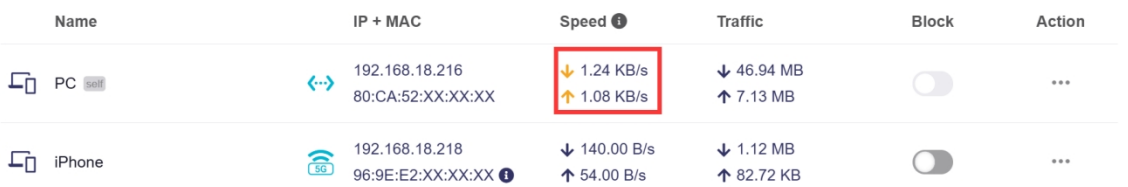
Fai clic sull'icona a tre punti nella colonna **Azione** e fai clic su **Limita velocità** dal menu a discesa.




Sarai in grado di limitare la velocità di un dispositivo connesso, con l'unità impostata su KB/s.

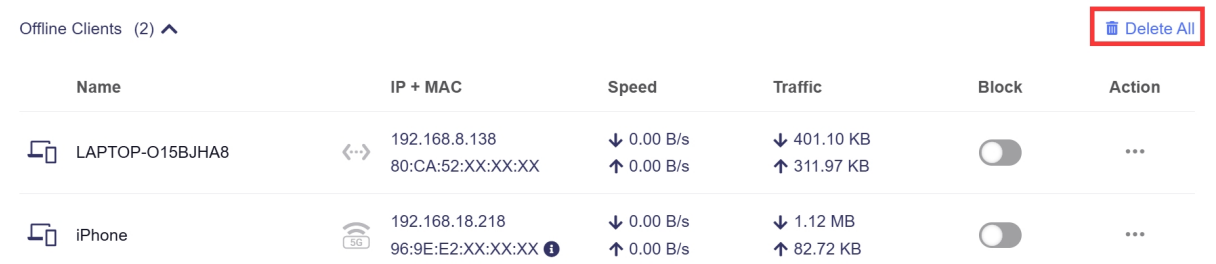



Se a un dispositivo è stata applicata una limitazione di velocità, le frecce della velocità di caricamento/download diventeranno gialle.

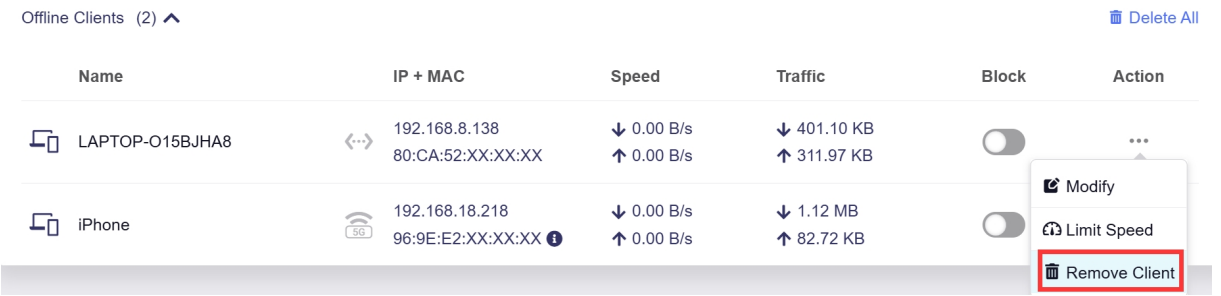


## 6.3 Rimozione dei client

Nella sezione **Client offline**, puoi fare clic su **Elimina tutto** nell'angolo in alto a destra per eliminare tutti i client offline.

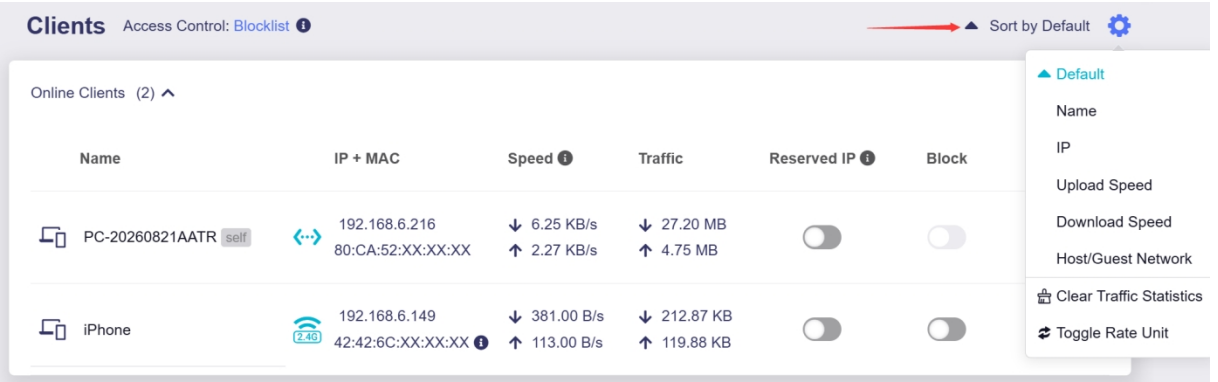



Per rimuovere un client specifico, fai clic sull'icona a tre punti nella colonna **Azione**, quindi seleziona **Rimuovi client** dal menu a discesa.



## 6.4 Ordinamento

Puoi impostare la regola di ordinamento dei dispositivi per la pagina Client nell'angolo in alto a destra.




L'ordinamento predefinito è il seguente:

- Il dispositivo personale (ovvero il dispositivo che stai utilizzando per accedere al pannello di amministrazione del router) appare sempre in alto.
- Nella sezione **Client online**, i dispositivi vengono elencati più in alto se si sono connessi in precedenza.
- Nella sezione **Client offline**, i dispositivi vengono elencati più in alto se si sono disconnessi in precedenza.

Oltre alle regole di ordinamento, il menu a discesa fornisce anche le seguenti funzioni:

- **Cancella statistiche sul traffico**: cancella le statistiche sul traffico per tutti i client online con un clic. Una volta applicata, la colonna delle statistiche del traffico verrà azzerata e quindi riavviate le statistiche.




- **Cambia unità di velocità**: cambia l'unità di velocità per la colonna della velocità tra **KB/s** e **Kbps**.

Capitolo 7

# Conoscere le VPN

Questo capitolo introduce i concetti della VPN e gli scenari di utilizzo comune.

# 7.1 Introduzione

## VPN

VPN, abbreviazione di Virtual Private Network, stabilisce un tunnel privato e crittografato tra un dispositivo e un server remoto, proteggendo la trasmissione dei dati e consentendo un accesso sicuro a reti private o riservate.

## Router VPN

Un router VPN presenta funzionalità VPN preinstallate, proteggendo tutti i dispositivi connessi tramite VPN. A differenza della configurazione della VPN sui singoli dispositivi, la configurazione del router come client VPN instrada tutto il traffico attraverso un tunnel crittografato, senza necessità di configurazione separata per dispositivo. Ciò protegge più dispositivi contemporaneamente, fa risparmiare tempo e garantisce configurazioni VPN coerenti, riducendo i rischi derivanti da impostazioni individuali non corrette.

I router GL.iNet supportano oltre 30 popolari servizi commerciali OpenVPN e WireGuard VPN. Carica i file di configurazione VPN per attivare la connessione VPN per una rete sicura. Vedi qui per l'elenco completo dei provider VPN di terze parti.

## OpenVPN

OpenVPN è un protocollo VPN open source che utilizza la sicurezza basata su SSL/TLS per connessioni da punto a sito o da sito a sito. Supporta più metodi di crittografia, TCP/UDP e un facile bypass firewall/NAT.

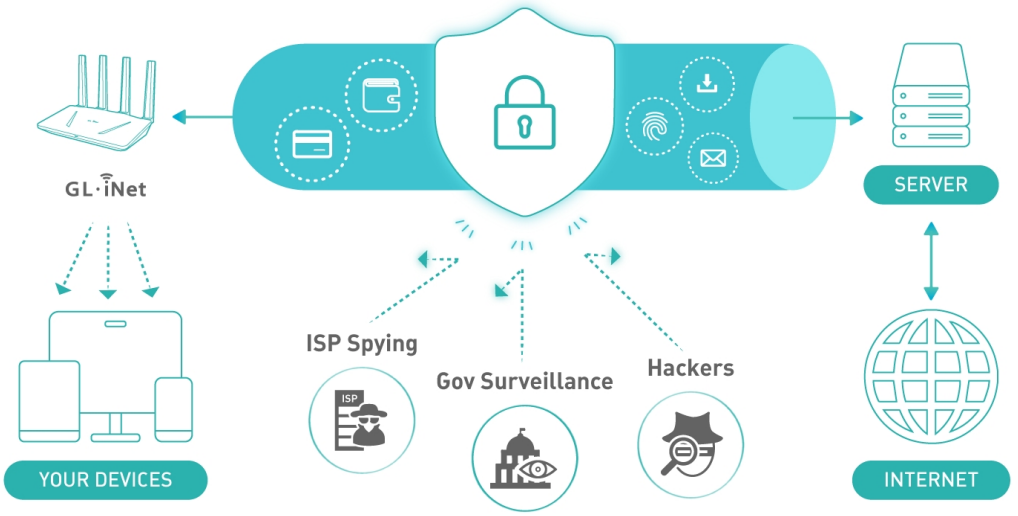
## WireGuard

WireGuard è un protocollo VPN leggero e veloce, più semplice ed efficiente di OpenVPN. È dotato di crittografia moderna per garantire efficienza, una piccola base di codice per un controllo e una sicurezza più semplici e algoritmi all'avanguardia (ChaCha20/Poly1305) per la crittografia e l'integrità dei dati.

## 7.2 Scenari di utilizzo

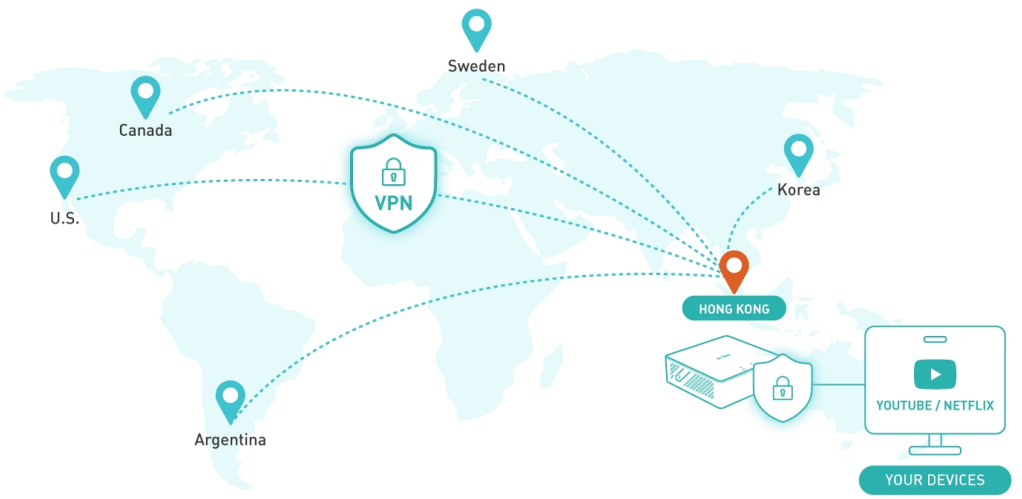
1. **Privacy dei dati personali**

   Il servizio VPN è compatibile con un'ampia gamma di dispositivi tramite il nostro router, inclusi non solo laptop, telefoni e tablet, ma anche console di gioco, TV e dispositivi di streaming. I tuoi dati saranno protetti sia tramite connessioni wireless che cablate. Puoi anche personalizzare le policy VPN per ottenere una protezione flessibile per determinati dispositivi.



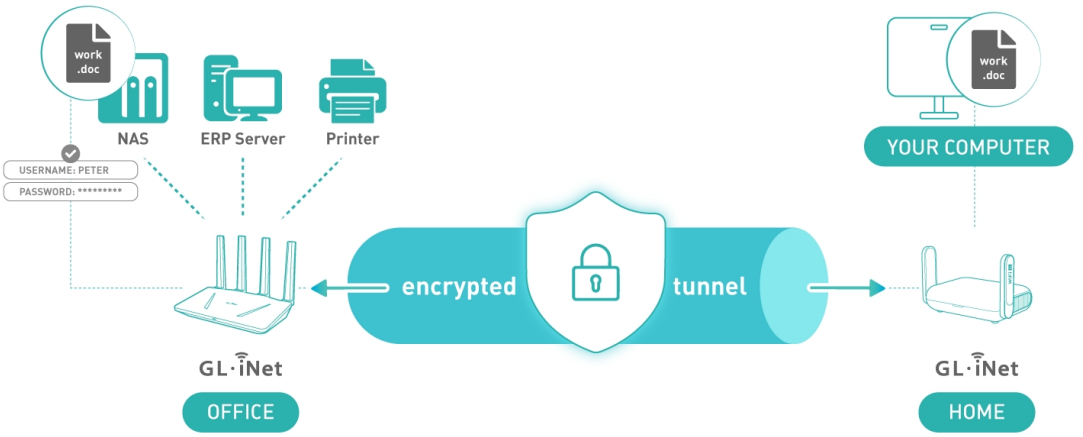

2. **Accesso illimitato in tutto il mondo**

   L'accesso ad alcuni siti potrebbe essere limitato in base alla posizione. Con la VPN abilitata, puoi sbloccare qualsiasi sito quando necessario. Collegandoti a diversi server di terze parti, ti verranno assegnati indirizzi IP diversi per la navigazione o l'accesso a siti bloccati per regione.



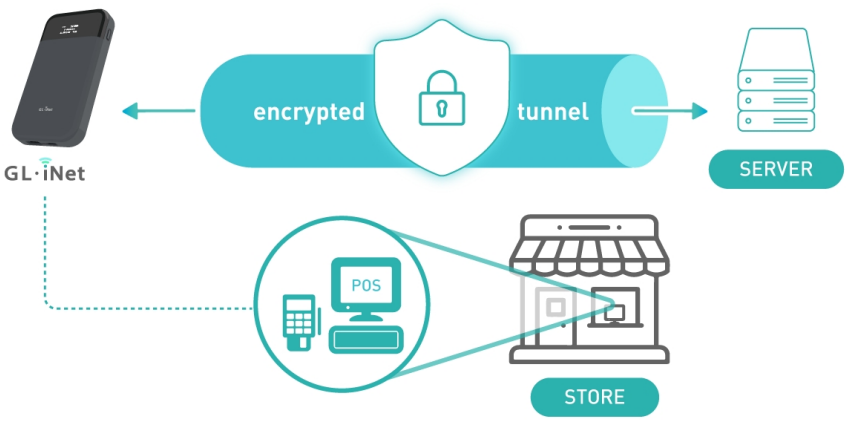
3. **Sicurezza dei dati delle piccole imprese**

Molte persone lavorano in spazi di coworking o bar e si affidano al Wi-Fi pubblico gratuito. Tali reti sono vulnerabili agli attacchi dei criminali informatici. Configurando il tuo router da viaggio come client VPN, puoi usufruire di una connettività sicura per lavorare ovunque.




4. **Infrastruttura di pagamento sicura**

I piccoli proprietari di negozi al dettaglio devono gestire le credenziali di pagamento dei client quando svolgono attività in loco. Utilizzando un router VPN, i loro terminali POS possono caricare i dati della carta di credito tramite un tunnel VPN crittografato per garantire la sicurezza dei pagamenti.



Capitolo 8

# Dashboard VPN

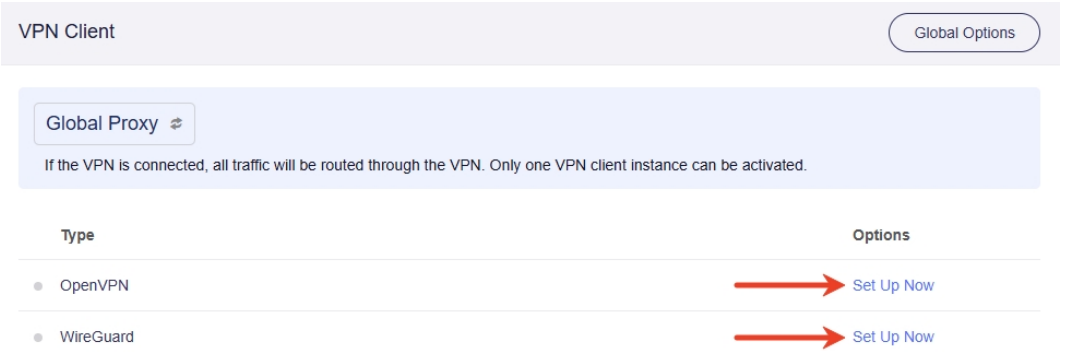
Questo capitolo introduce come gestire le connessioni VPN tramite pannello di amministrazione web.

Accedi al pannello di amministrazione web del router e vai a **VPN** > **Dashboard VPN**.

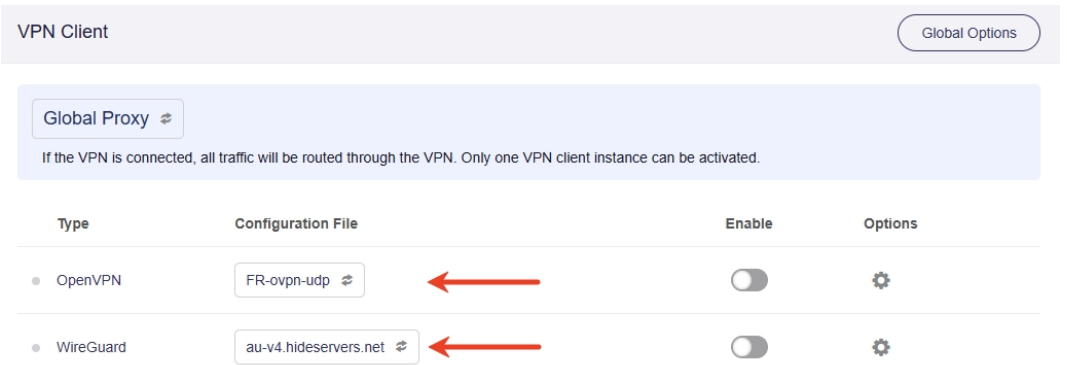
Quando il router è impostato come client VPN attiva, il dashboard VPN visualizza i dettagli della connessione VPN, come indirizzo del server, statistiche sul traffico, IP virtuale client e registro della connessione. Ti consente inoltre di configurare impostazioni avanzate come Blocca traffico non VPN, Consenti accesso WAN e Usa la VPN per i servizi GL.iNet.

## 8.1 Client VPN

Quando si accede a **Dashboard VPN** per la prima volta e non sono disponibili file di configurazione OpenVPN o WireGuard, la pagina viene visualizzata come segue. Fai clic su **Configura ora** e verrai indirizzato alla pagina **Client OpenVPN** o **Client WireGuard** per caricare i file di configurazione VPN.

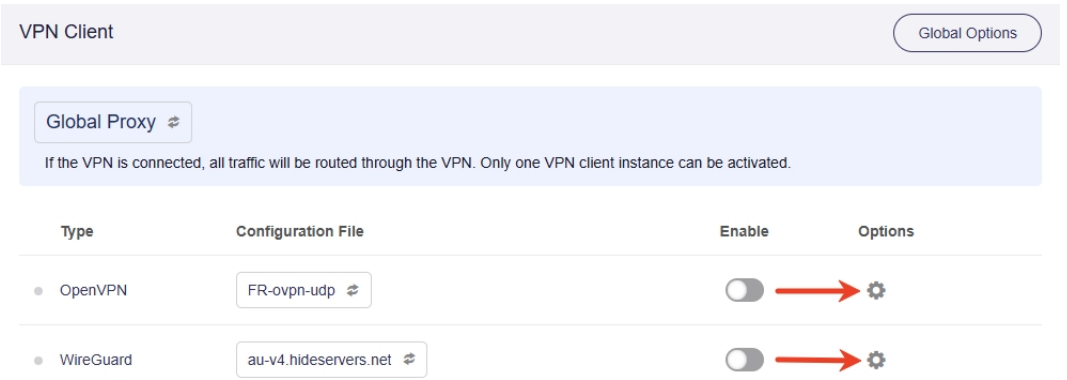



Una volta caricata, la tua configurazione verrà mostrata nella colonna **File di configurazione**. Se hai caricato più file di configurazione, puoi cambiare file facendo clic sulla casella.

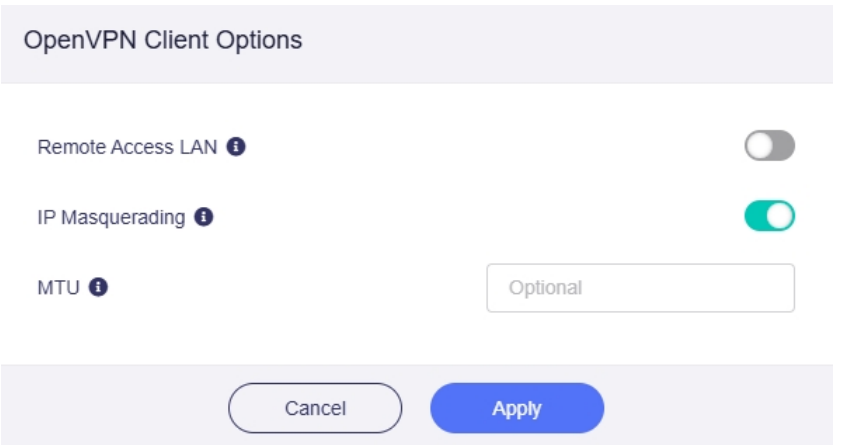


## 8.1.1 Opzioni client

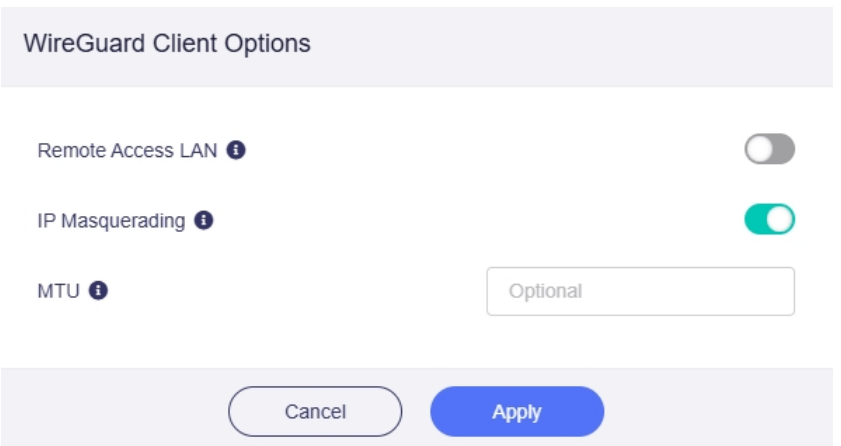
Fai clic sull'icona a forma di ingranaggio a destra per accedere alle opzioni OpenVPN o WireGuard client.



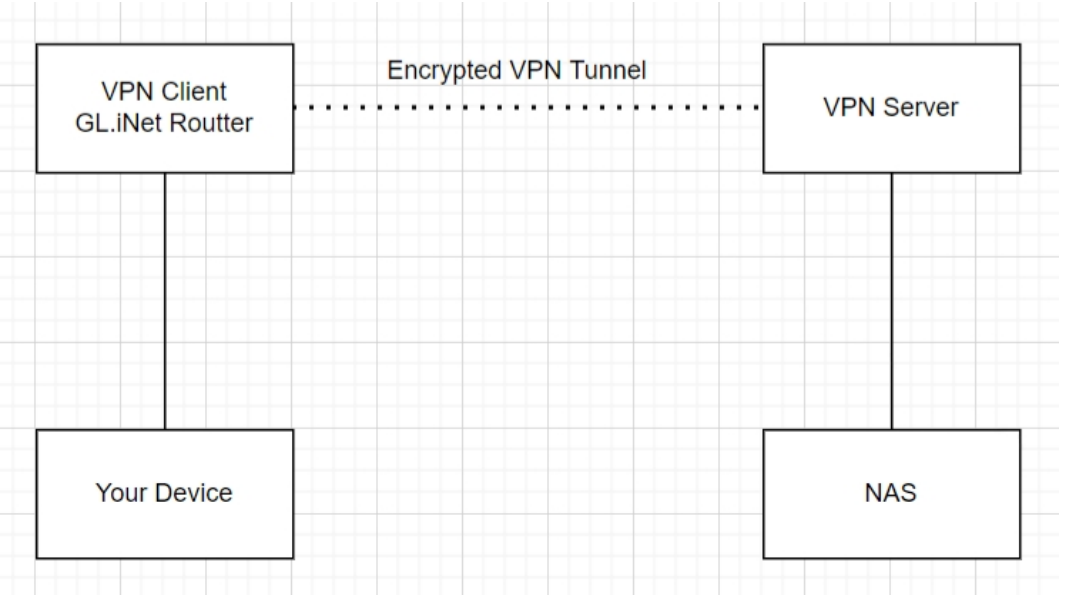

Le opzioni Client OpenVPN vengono visualizzate come segue.




Le opzioni Client WireGuard vengono visualizzate come segue.



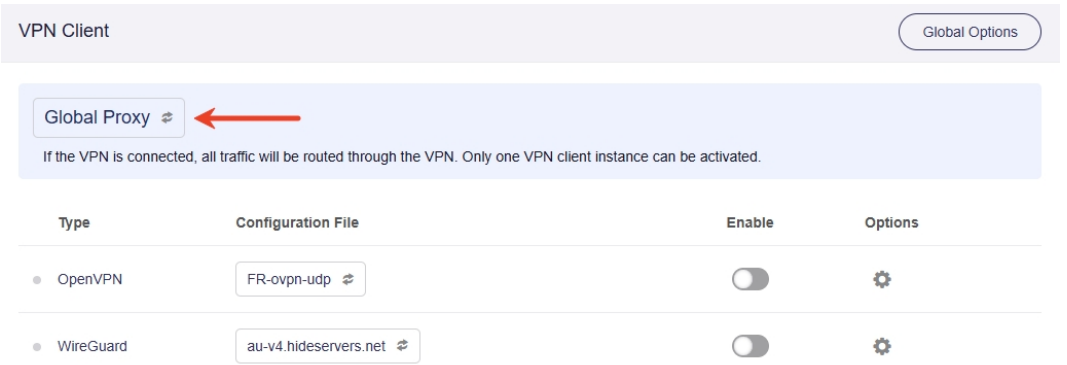
- **Accesso remoto alla LAN**: se abilitato, sarà consentito accesso remoto a questo router e ai suoi dispositivi LAN tramite VPN. Il server VPN deve pubblicizzare un percorso verso la sottorete LAN di questo router.
  Ad esempio, come mostrato nel diagramma seguente, il router GL.iNet funziona come client VPN e si connette a un server VPN tramite il tunnel VPN. Quando questa opzione è abilitata, sia il router GL.iNet che i suoi dispositivi lato LAN sono accessibili dai dispositivi lato server VPN (ad esempio NAS). Ciò richiede l'aggiunta di una regola di routing sul server VPN per raggiungere la sottorete LAN del router GL.iNet.




- **Masquerading IP**: se abilitato, gli indirizzi IP di origine dei client LAN verranno riscritti nell'IP del tunnel VPN del router. Disabilitalo solo per le configurazioni da sito a sito in cui il peer remoto conosce le tue sottoreti LAN.
- **MTU**: abbreviazione di Maximum Transmission Unit. Questa impostazione facoltativa ti consente di personalizzare il tunnel VPN MTU, che sovrascrive il valore definito nel file di configurazione.

## 8.1.2 Modalità delle policy

La modalità proxy predefinita per la connessione VPN è **Proxy globale**. Puoi fare clic sulla casella in alto a destra per passare ad altre modalità proxy.




Sono disponibili tre modalità proxy: proxy globale, modalità delle policy e modalità di routing.

1. **Proxy globale**

   In questa modalità, tutto il traffico verrà instradato attraverso la VPN. È possibile attivare una sola istanza client VPN.

2. **Modalità delle policy**

   Questa modalità può essere ulteriormente suddivisa in tre politiche.

   - **In base al dominio o IP di destinazione**

     In questa modalità, solo il traffico di determinati siti Web identificati dall'indirizzo IP o dal nome di dominio verrà instradato tramite VPN. È possibile attivare una sola istanza client VPN.

   - **In base al dispositivo client**

     In questa modalità, solo il traffico di determinati dispositivi LAN identificati da indirizzi MAC verrà instradato tramite VPN. È possibile attivare una sola istanza client VPN.

   - **Basato sulla VLAN**

     In questa modalità, solo il traffico di determinate VLAN verrà instradato tramite VPN. È possibile attivare una sola istanza client VPN.

3. **Modalità di routing**

   - **Rilevamento automatico**

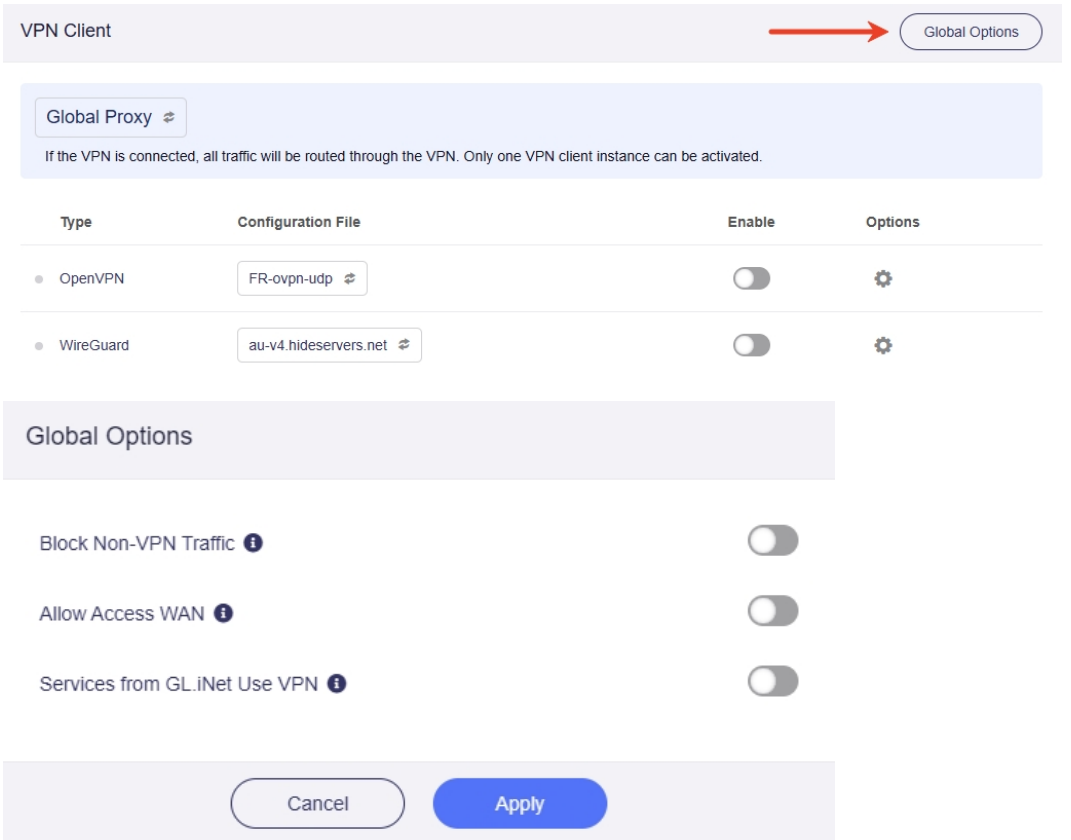
     Verranno utilizzate le regole di instradamento definite in ciascun file di configurazione client VPN o emesse dal server VPN.

   - **Personalizza le regole di routing**

     Puoi configurare manualmente le regole di routing per ciascuna istanza client VPN.

## 8.1.3 Opzioni globali

Fai clic su **Opzioni globali** nell'angolo in alto a destra per configurare le impostazioni avanzate per la tua client VPN.



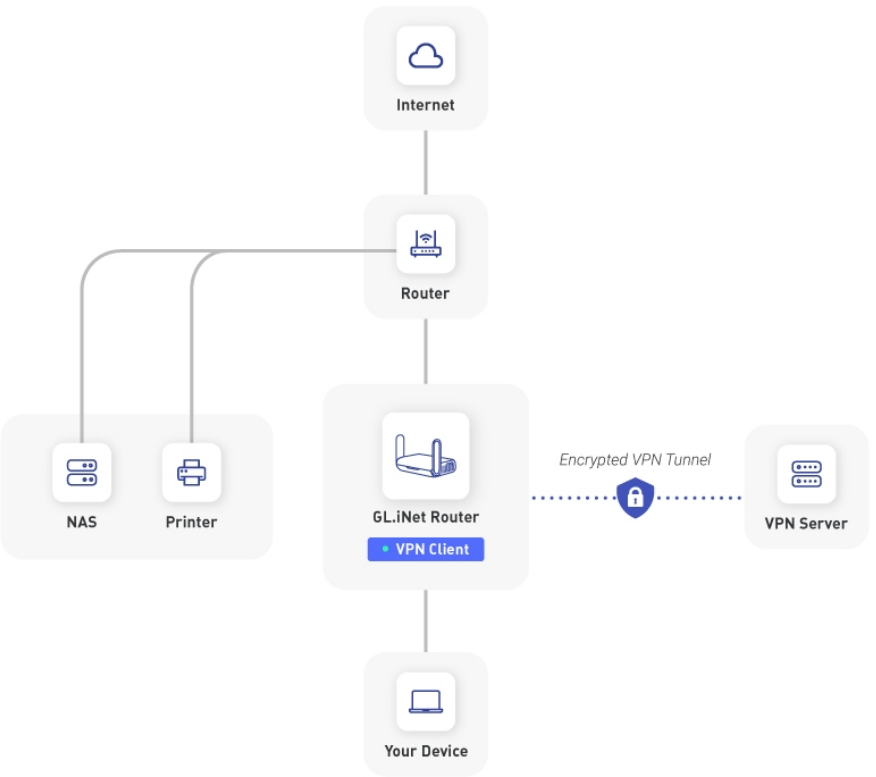

- **Blocca traffico non VPN**: se abilitato, tutto il traffico Internet è costretto a passare esclusivamente attraverso il tunnel VPN e non può essere instradato tramite altre interfacce come la WAN dell'ISP locale. Se la connessione VPN si interrompe inaspettatamente, tutto il traffico Internet viene completamente bloccato per impedire il fallback alla normale WAN. Ciò evita perdite VPN causate da errori VPN, impostazioni DNS client errate e problemi simili.

  Questa funzionalità è nota anche come VPN Kill Switch. Impedisce che i dati dell'utente vengano esposti online. Un tipico Kill Switch interrompe automaticamente l'accesso a Internet quando la connessione VPN fallisce. La funzionalità Blocca traffico non VPN sui router GL.iNet fornisce una protezione più ampia dalle perdite e copre i seguenti scenari:

  a. Perdita DNS
  b. Perdita IPv6
  c. Perdita WebRTC

d. Interruzione della connessione VPN
e. Applicazioni lanciate prima dell'istituzione della VPN
f. Perdite di traffico per applicazione

- **Consenti accesso WAN**: se abilitato, i dispositivi client locali possono comunque accedere ai servizi lato WAN (ad esempio stampanti, NAS e altri dispositivi nella sottorete upstream) mentre la VPN è attiva.



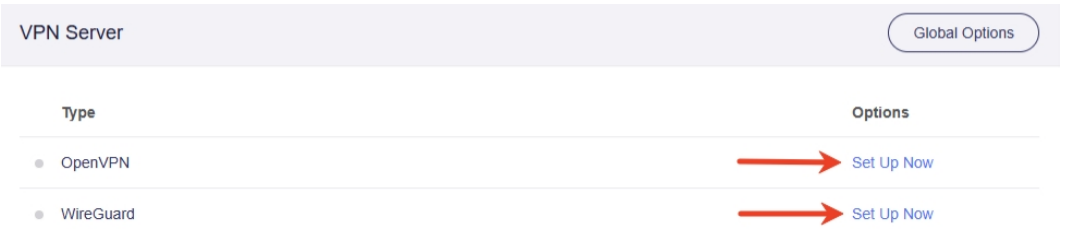

Come mostrato nel diagramma sopra, l'abilitazione di questa funzione consente ai dispositivi locali di raggiungere gli host sulla sottorete upstream, come stampanti e NAS.

Questa opzione è progettata principalmente per consentire ai client di accedere ai dispositivi all'interno della sottorete upstream. Tuttavia, il router non è in grado di distinguere il traffico della sottorete upstream dal normale traffico Internet. Se i dispositivi client accedono alle risorse direttamente tramite IP pubblici, esiste un potenziale rischio di perdita di traffico. Per questo motivo, **Consenti accesso WAN** e **Blocca traffico non VPN** si escludono a vicenda e non possono essere abilitati contemporaneamente.

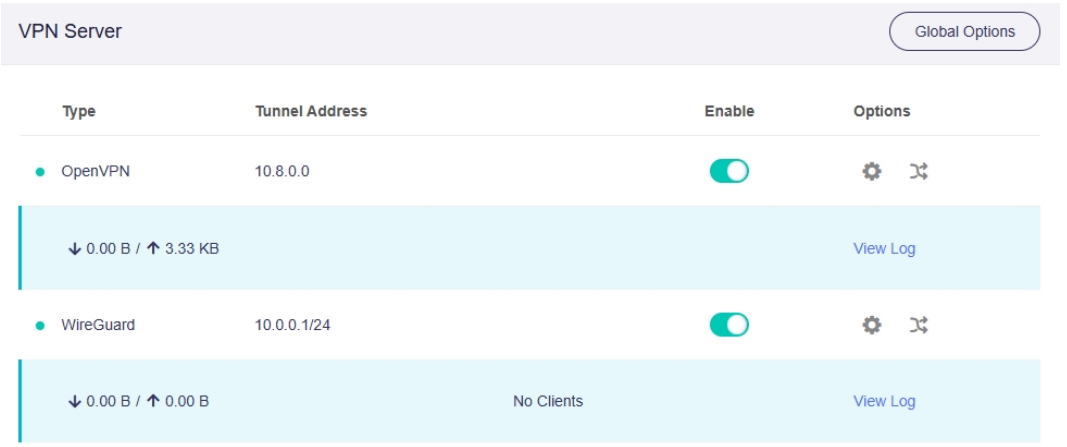
- **Usa la VPN per i servizi GL.iNet**: se abilitati, GoodCloud, DDNS e i servizi rtty trasmetteranno i pacchetti attraverso tunnel VPN. Questa opzione è disabilitata per impostazione predefinita, poiché questi servizi normalmente richiedono l'indirizzo IP reale del dispositivo per funzionare correttamente.

## 8.2 Server VPN

Se il router non è mai stato configurato come server OpenVPN o WireGuard, la pagina apparirà come mostrato di seguito. Fai clic su **Configura ora** e verrai indirizzato **alla pagina Server OpenVPN** o **Server WireGuard** per inizializzare il tuo server VPN.

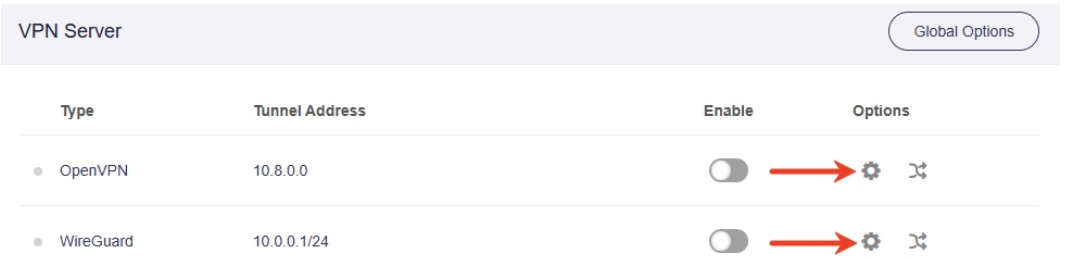



Dopo aver abilitato Server OpenVPN o Server WireGuard, la pagina visualizzerà lo stato del server come segue.

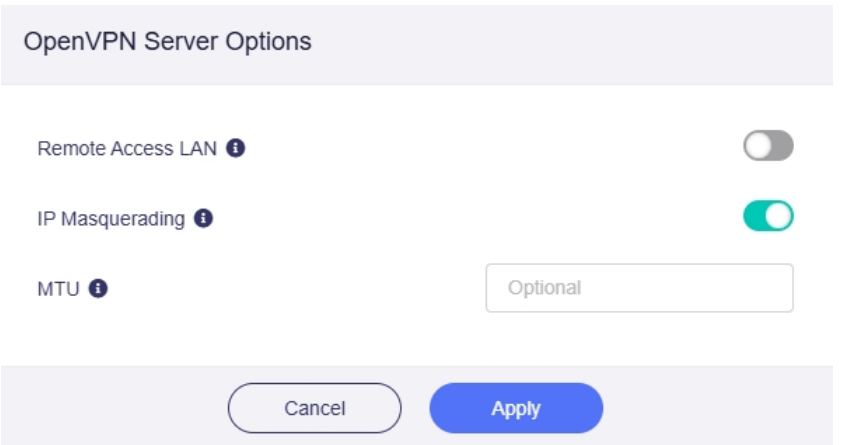


## 8.2.1 Opzioni server

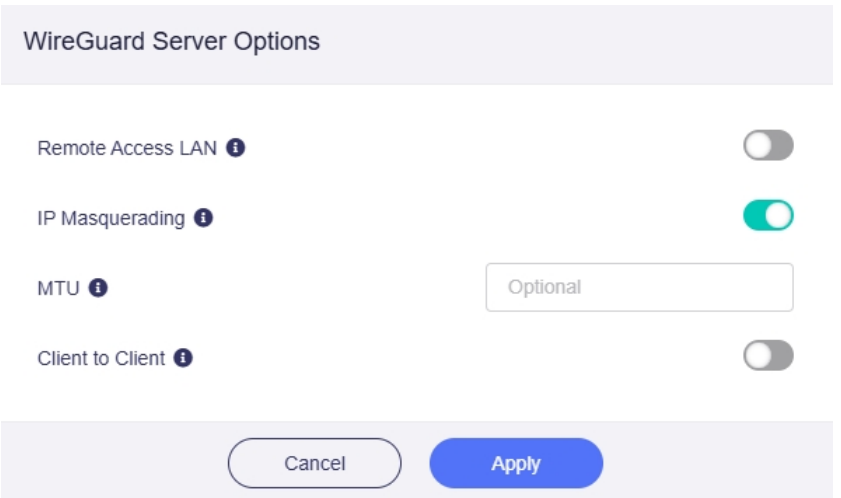
Fai clic sull'icona a forma di ingranaggio a destra per accedere alle opzioni del server OpenVPN o WireGuard.




Le opzioni Server OpenVPN vengono visualizzate come segue.




Le opzioni Server WireGuard vengono visualizzate come segue.

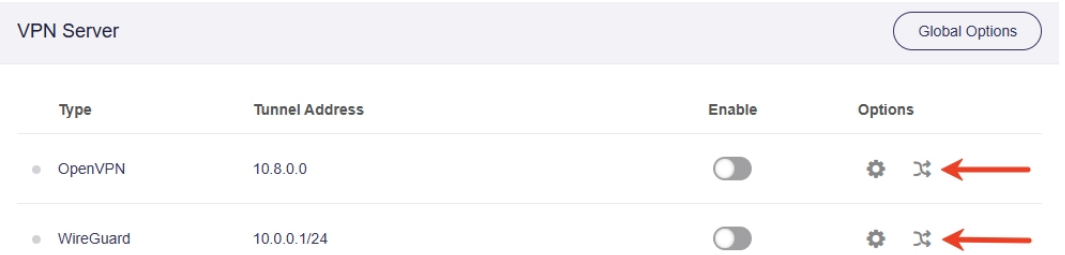



- **Accesso remoto alla LAN**: se abilitato, è possibile accedere alle risorse all'interno della sottorete LAN del server tramite il tunnel VPN.

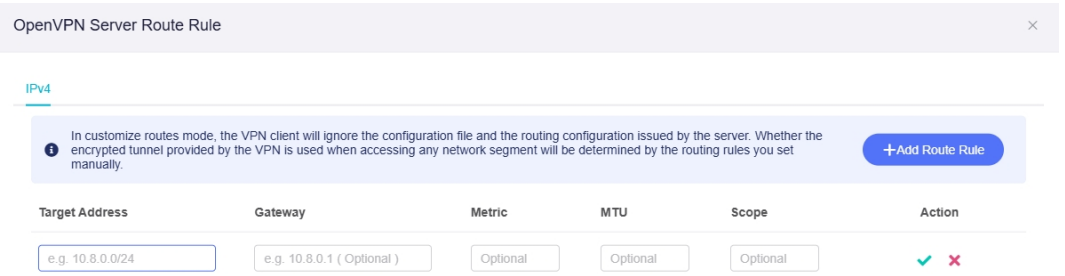
- **Masquerading IP**: se abilitato, gli indirizzi IP di origine dei client LAN verranno riscritti nell'IP del tunnel VPN del router. Disabilitalo solo per le configurazioni da sito a sito in cui il peer remoto conosce le tue sottoreti LAN.
- **MTU**: abbreviazione di Maximum Transmission Unit. Il valore MTU impostato per il tunnel sovrascriverà le impostazioni MTU nel file di configurazione.
- **Da client a client**: se abilitato, i client VPN connessi a questo server possono accedersi tra loro tramite i propri IP tunnel VPN. Se desideri consentire ai client di accedere anche alle sottoreti LAN degli altri, devi aggiungere regole di routing sul server VPN per pubblicizzare tali sottoreti LAN remote.

## 8.2.2 Regola di routing del server

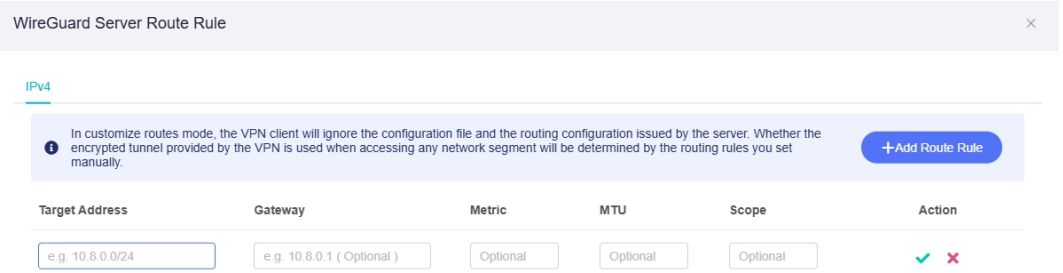
Fai clic sull'icona del percorso a destra per personalizzare le regole del percorso OpenVPN o WireGuard secondo necessità.




La regola di percorso Server OpenVPN viene visualizzata come segue. Fai clic su **Aggiungi regola di percorso**, inserisci **l'indirizzo di destinazione** e **il gateway**, quindi fai clic sull'icona di controllo verde per applicare.



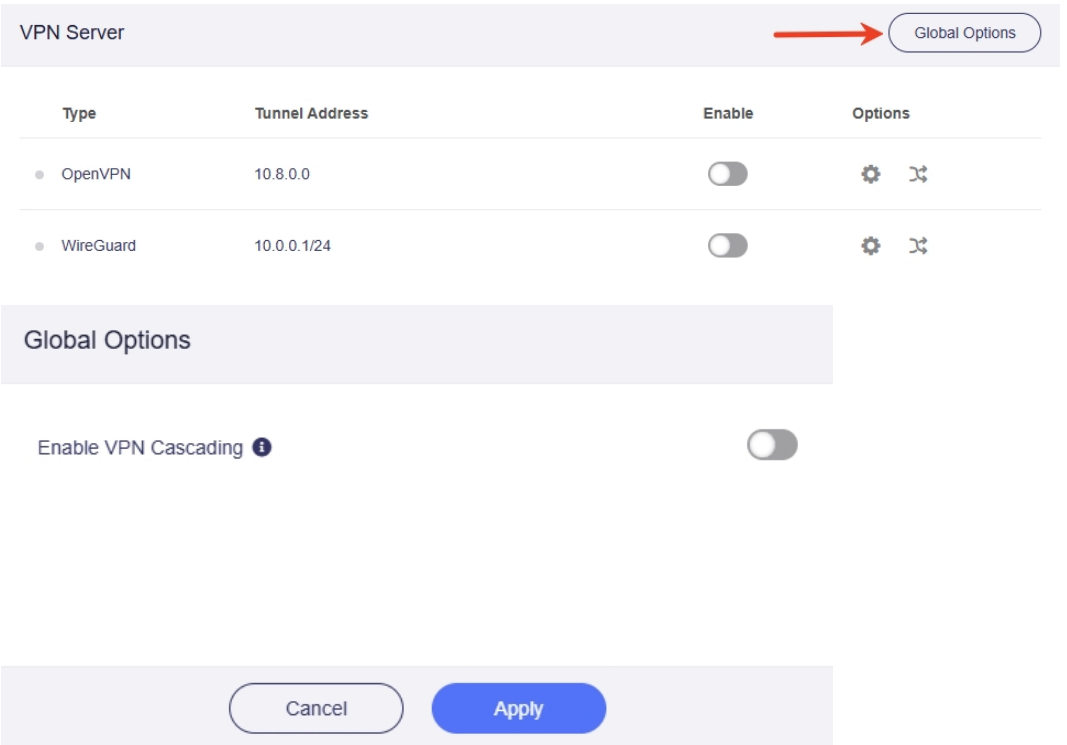

La regola di percorso Server WireGuard viene visualizzata come segue. Fai clic su **Aggiungi regola di percorso**, inserisci **l'indirizzo di destinazione** e **il gateway**, quindi fai clic sull'icona di controllo verde per applicare.




**Nota**: nella modalità di personalizzazione dei percorsi, la client VPN ignorerà il file di configurazione e la configurazione del routing emessa dal server. L'utilizzo o meno del tunnel crittografato VPN quando si accede a qualsiasi segmento di rete è determinato dalle regole di instradamento impostate manualmente.

## 8.2.3 Opzioni globali

Fai clic su **Opzioni globali** nell'angolo in alto a destra per configurare le impostazioni avanzate per il tuo server VPN.




Se **VPN in cascata** è abilitato, quando questo router funge contemporaneamente da server VPN e client VPN, i client VPN remoti connessi al server VPN di questo router avranno il loro traffico instradato attraverso il tunnel VPN upstream che questo router utilizza come client VPN. Ulteriori informazioni sul VPN in cascata.

Capitolo 9

# Configurazione del server VPN

Questo capitolo introduce come configurare un router GL.iNet come server OpenVPN o WireGuard.

## 9.1 Configurazione del server OpenVPN

OpenVPN è un protocollo VPN open source che utilizza la crittografia SSL/TLS per connessioni sicure punto a punto e da sito a sito. Per configurare il server OpenVPN su un router GL.iNet, guarda questo video o fai riferimento ai passaggi seguenti.

### 9.1.1 Preparazione

1. **Assicurati di avere un indirizzo IP pubblico**

   Fai clic qui per verificare se il tuo provider di servizi Internet (ISP) ti ha assegnato un indirizzo IP pubblico.

   In caso contrario, il router non può essere impostato come server OpenVPN.

   Metodi alternativi:

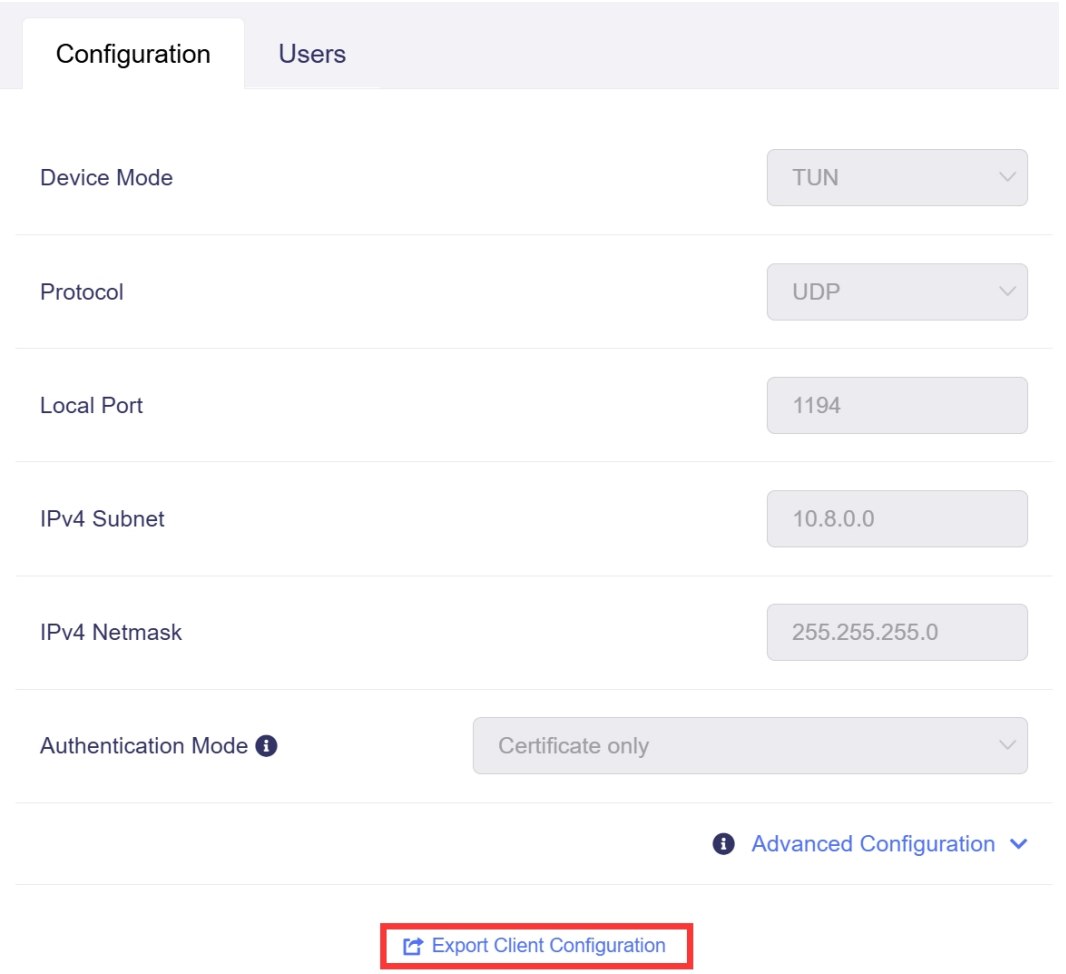
   - Se disponi di un router primario a monte del tuo router GL.iNet, accedi ad esso e verifica che abbia un indirizzo IP pubblico assegnato dal tuo ISP.
   - Chiedi al tuo ISP un indirizzo IP pubblico. Ciò potrebbe comportare un costo aggiuntivo.

2. **Conferma se è richiesto il port forwarding**

   - Se il tuo router GL.iNet è il router principale della tua rete, non è richiesta alcuna configurazione di port forwarding. Procedi al passaggio successivo.
   - Se un router primario è già in uso e il tuo router GL.iNet è configurato come router secondario, dovrai configurare il port forwarding sul router primario.
   - Se il tuo router GL.iNet si trova su più livelli a valle del router primario, configura il port forwarding su ciascun dispositivo intermedio.

## 9.1.2 Procedura di configurazione

1. Accedi al pannello di amministrazione web del router, vai a **VPN** > **Server OpenVPN**, quindi fai clic su **Genera configurazione** (solo per la configurazione iniziale del server VPN).
2. Applica la configurazione.
   La configurazione predefinita funziona nella maggior parte dei casi. Fai clic su **Esporta configurazione client** in basso e procedi al passaggio 3. Se hai modificato la configurazione, fai clic su **Applica** prima di esportarla.



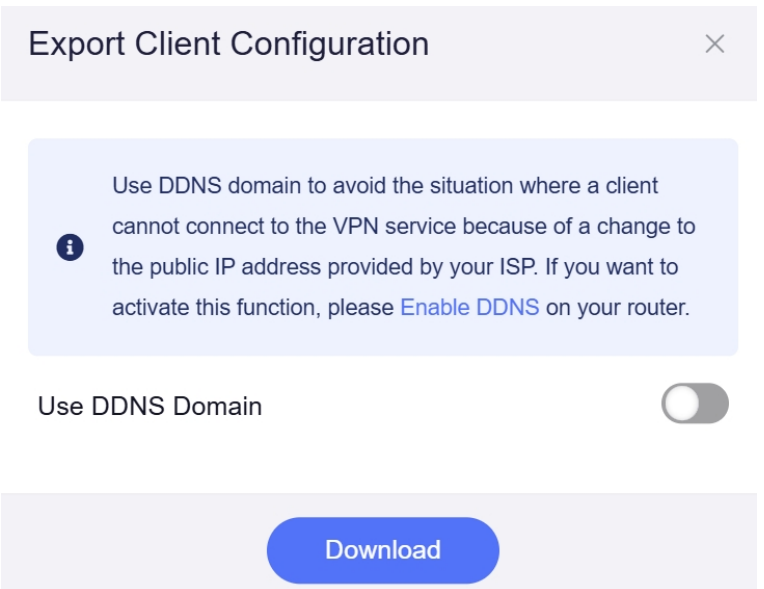

- **Modalità dispositivo**: TAP-S2S o Tun. Vedi qui per le differenze.
- **Protocollo**: UDP o TCP. Vedi qui per le differenze.
- **Modalità di autenticazione**: determina il metodo di autenticazione utilizzato quando il client si connette al server. Sono disponibili tre opzioni:

- **Solo certificato**: se selezionato, il router genererà automaticamente chiavi di certificato server e client e le incorporerà nel file di configurazione. Quando carichi la configurazione sul client, non sono richieste credenziali aggiuntive.
- **Solo nome utente/password**: se selezionato, il router genererà la configurazione del client senza chiavi di certificato. È necessario aggiungere un nome utente e una password nella scheda **Utenti** prima di esportare la configurazione del client. Quando carichi la configurazione sul client, inserisci queste credenziali per l'autenticazione.
- **Nome utente/password e certificato**: se selezionato, è necessario aggiungere prima un nome utente e una password nella scheda **Utenti** prima di esportare la configurazione del client; in secondo luogo, il router genererà automaticamente le chiavi dei certificati server e client e le incorporerà nel file di configurazione. Quando si carica la configurazione sul client, verrà verificata prima la chiave del certificato, seguita dall'autenticazione con nome utente/password per la sicurezza 2FA.

- **Configurazione avanzata**: personalizza più impostazioni del server, se necessario.

3. Esporta configurazione client.

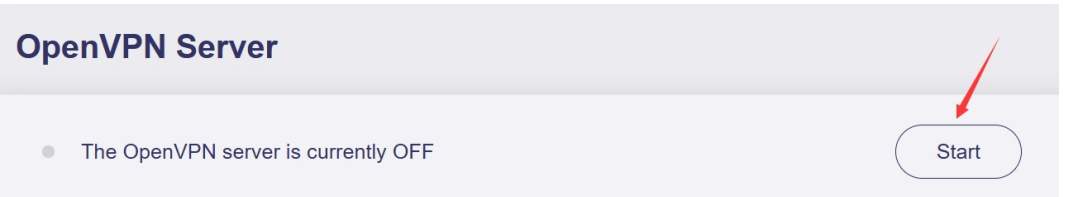
   Dopo aver fatto clic su **Esporta configurazione client** nella parte inferiore della scheda Configurazione (o dopo aver applicato la configurazione modificata), verrà visualizzata una finestra come segue. Fai clic su **Scarica** per esportare la configurazione.



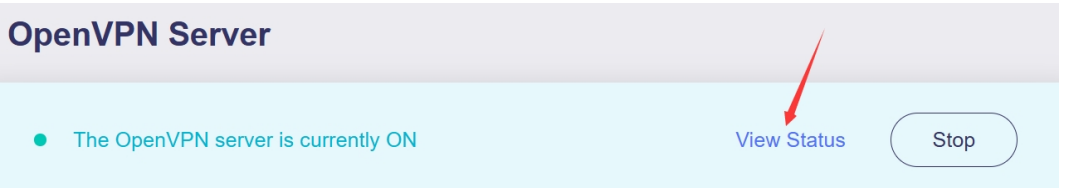
**Suggerimento**: se il tuo indirizzo IP pubblico cambia frequentemente, vai su **APPLICAZIONI** > **DNS dinamico** e abilita DDNS. Puoi quindi utilizzare il dominio DDNS come indirizzo del server.

4. Avvia il server OpenVPN.

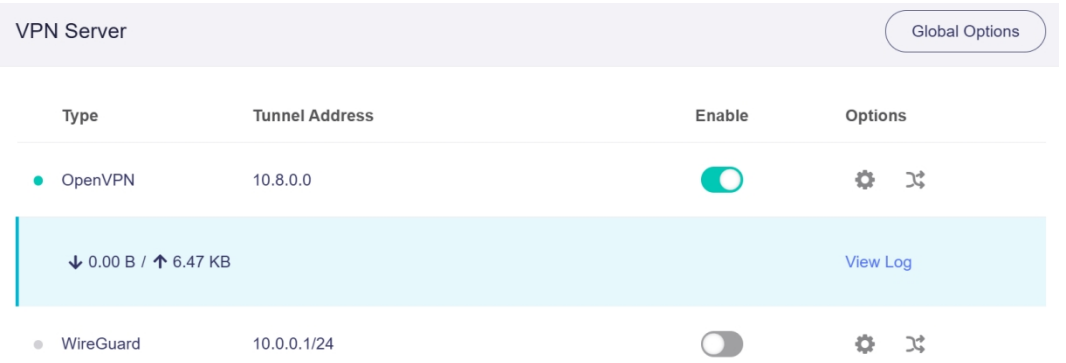
   Nella pagina **del server OpenVPN**, fai clic sul pulsante **Avvia** nell'angolo in alto a destra per avviare il server.




   Se desideri visualizzare lo stato della connessione al server, fai clic su **Visualizzazione stato**.




   Verrai reindirizzato allo Dashboard VPN. Se in questa pagina vengono visualizzate le statistiche sul traffico di caricamento e download, il server OpenVPN è in esecuzione.




## 9.1.3 Risoluzione dei problemi

Se la connessione fallisce, ci sono diversi motivi comuni:

- Il server VPN non ha un indirizzo IP pubblico. Vedi qui per la risoluzione dei problemi.
- Potrebbe essere necessario impostare il port forwarding. Vedi qui per la risoluzione dei problemi.

- La porta utilizzata per il server OpenVPN è bloccata dal tuo provider di servizi Internet. Passa a un'altra porta o contatta il tuo ISP per assistenza.
- La connessione VPN potrebbe essere bloccata in alcuni paesi o regioni.

## 9.2 Configurazione del server WireGuard

WireGuard® è una VPN semplice, veloce e moderna che utilizza tecniche crittografiche all'avanguardia. È progettata per essere più veloce, semplice e pratica di IPsec, evitando configurazioni complesse, e per offrire prestazioni sensibilmente superiori a OpenVPN. Per configurare un server WireGuard su un router GL.iNet, guarda questo video oppure segui le istruzioni riportate di seguito.

### 9.2.1 Preparazione

1. **Assicurati di avere un indirizzo IP pubblico**

   Fai clic qui per verificare se il tuo provider di servizi Internet ti assegna un indirizzo IP pubblico.

   In caso contrario, il router non può essere impostato come server WireGuard.

   Metodi alternativi:

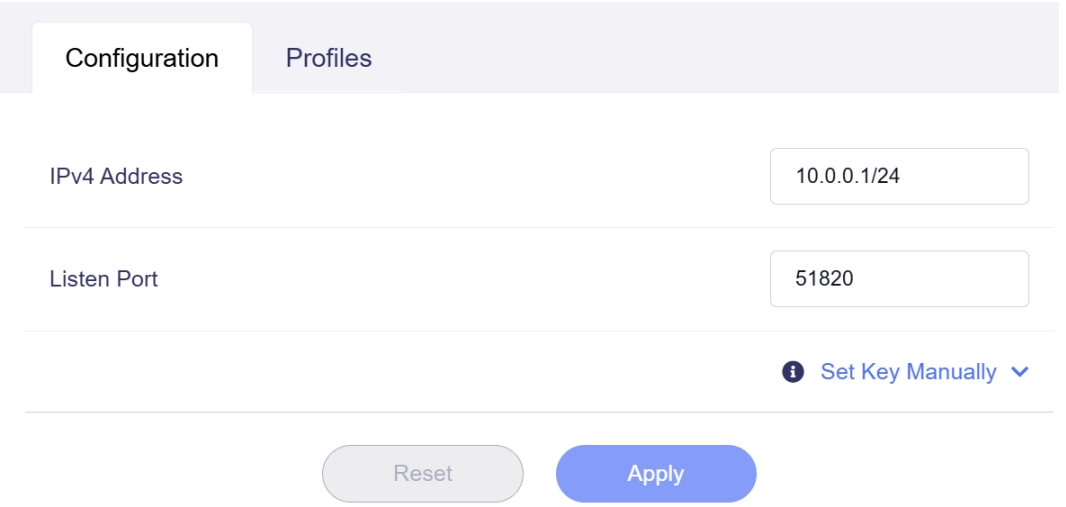
   - Se disponi di un router primario a monte del tuo router GL.iNet, accedi ad esso e verifica che abbia un indirizzo IP pubblico assegnato dal tuo ISP.
   - Chiedi al tuo ISP un indirizzo IP pubblico. Ciò potrebbe comportare un costo aggiuntivo.

2. **Conferma se è richiesto il port forwarding**

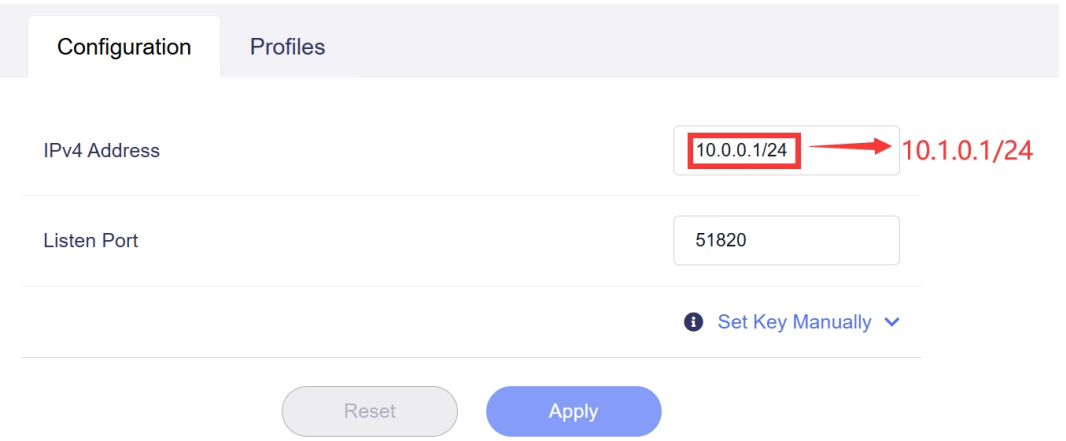
   - Se il tuo router GL.iNet è il router principale della tua rete, non è richiesta alcuna configurazione di port forwarding. Procedi al passaggio successivo.
   - Se un router primario è già in uso e il tuo router GL.iNet è configurato come router secondario, dovrai configurare il port forwarding sul router primario.
   - Se il tuo router GL.iNet si trova su più livelli a valle del router primario, configura il port forwarding su ciascun dispositivo intermedio.

## 9.2.2 Procedura di configurazione

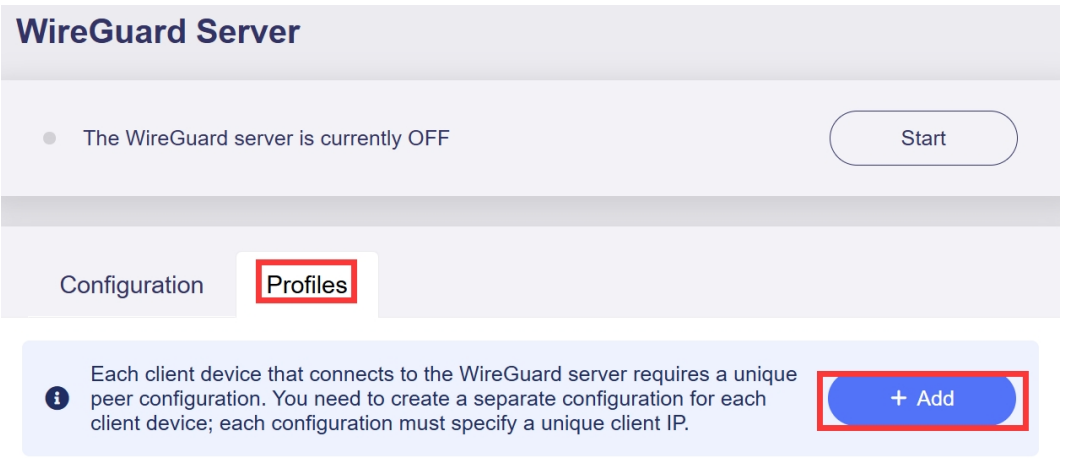
1. Accedi al pannello di amministrazione web del router, vai a **VPN** > **Server WireGuard**, quindi fai clic su **Genera configurazione** (solo per la configurazione iniziale del server VPN).
2. Applica la configurazione.
   La configurazione predefinita funziona nella maggior parte dei casi. Non è necessario modificare l'indirizzo IPv4 a meno che non sia in conflitto con il gateway del router upstream.



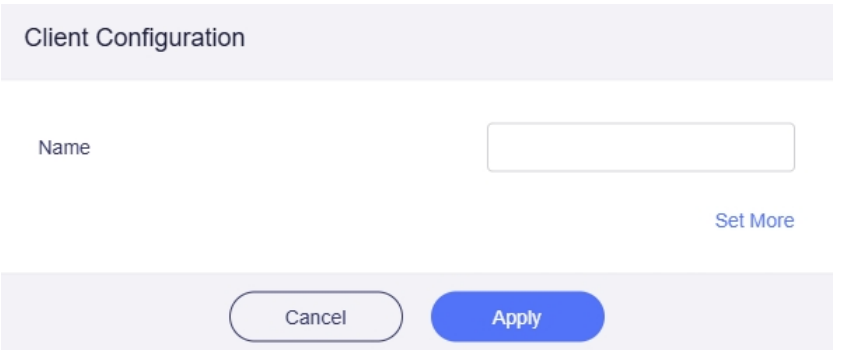

   Se l'indirizzo IPv4 è in conflitto con il gateway del router upstream, modifica l'indirizzo IPv4 con un altro (ad esempio, **10.1.0.1/24**) e fai clic su **Applica**. Assicurati che la notazione CIDR "/24" sia inclusa per evitare problemi di connettività.




3. Aggiungi un profilo.
   Passa alla scheda **Profili**, fai clic sul pulsante **Aggiungi** per generare un profilo per il tuo dispositivo.



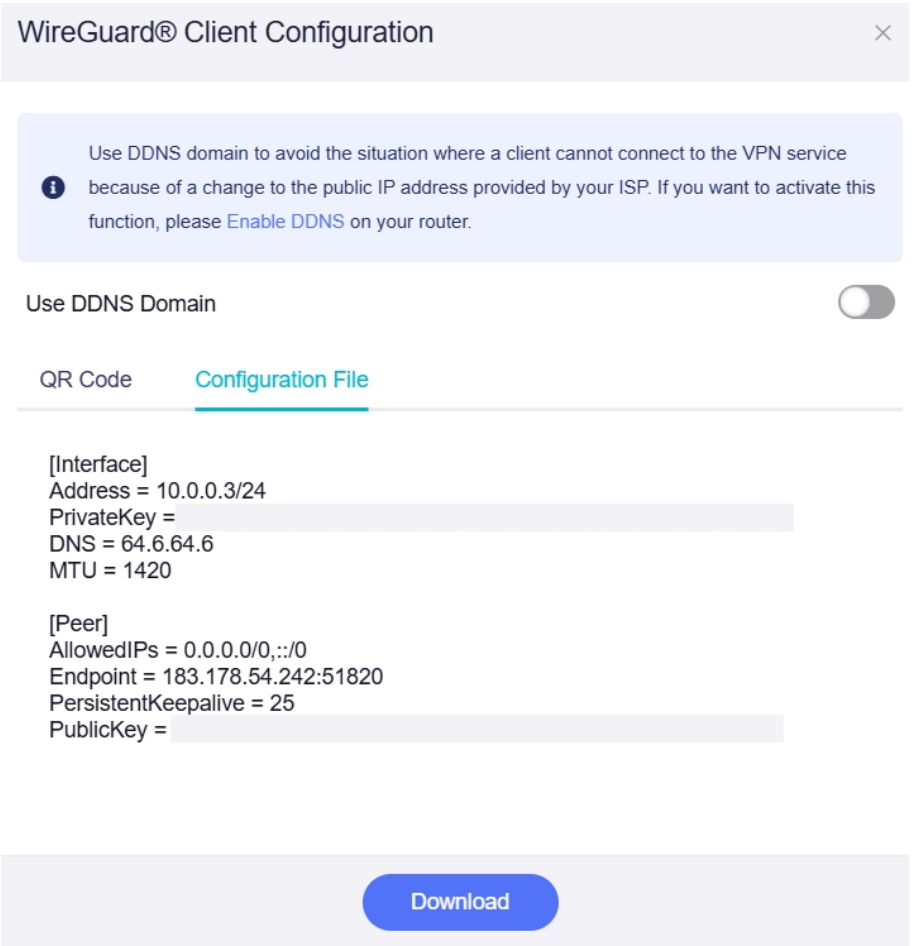

Imposta un nome descrittivo e fai clic su **Applica** per continuare.




4. Scarica configurazione.

   Dopo aver aggiunto un profilo, il router genererà un file di configurazione in tre formati: codice QR, testo normale e file.conf. Scegli il tuo metodo preferito per ottenere il file di configurazione.

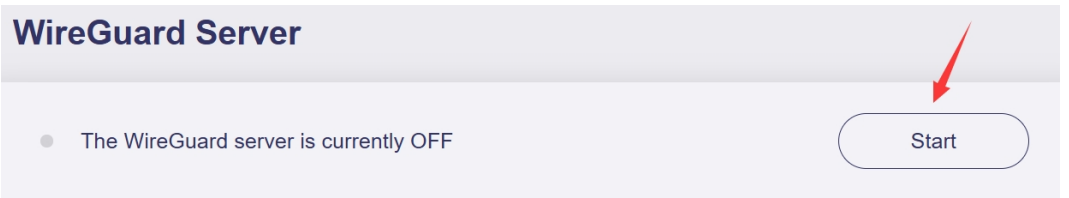
   - **Codice QR**: adatto per dispositivi (ad esempio smartphone, tablet, laptop) con l'app WireGuard installata. Se desideri impostare un dispositivo specifico come client WireGuard, apri semplicemente l'app WireGuard e scansiona il codice QR per importare un file di configurazione.
   - **Testo normale**: in formato testo normale, puoi rivedere i dettagli di configurazione e copiarli e incollarli comodamente altrove per la configurazione manuale, come l'app WireGuard o un router GL.iNet.
   - **File.conf**: fai clic sul pulsante **Scarica** per salvare il file.conf sul tuo dispositivo locale. È anche comodo e può essere caricato direttamente sull'app WireGuard o su un router GL.iNet.



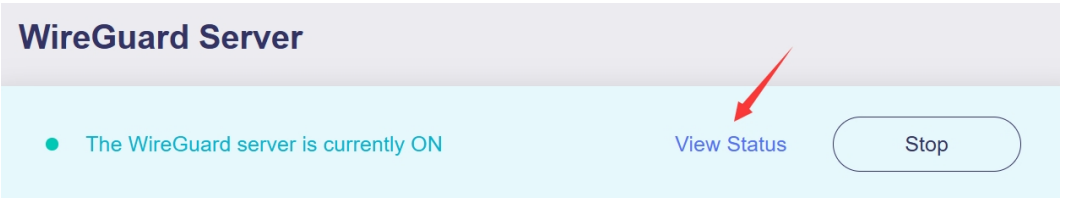

**Suggerimento**: se il tuo indirizzo IP pubblico cambia frequentemente, vai su **APPLICAZIONI** > **DNS dinamico** e abilita DDNS. Puoi quindi utilizzare il dominio DDNS come indirizzo del server.

5. Avvia il server WireGuard.

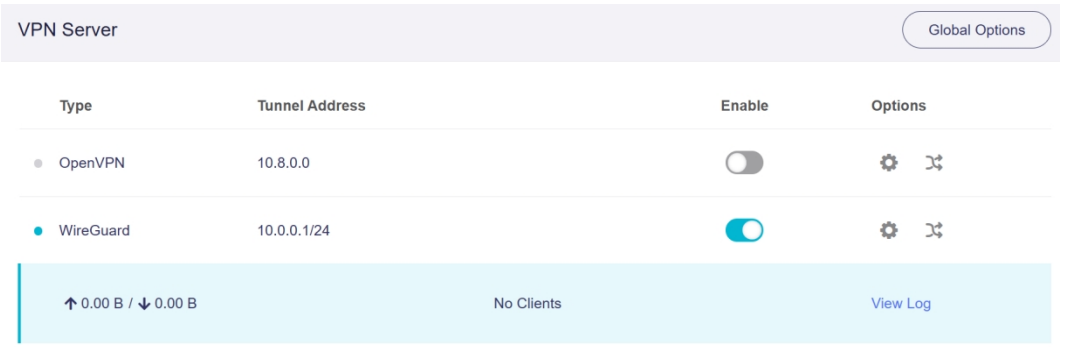
   Nella pagina **del server WireGuard**, fai clic sul pulsante **Avvia** nell'angolo in alto a destra per avviare il server.




   Se desideri visualizzare lo stato della connessione al server, fai clic su **Visualizzazione stato**.




Verrai reindirizzato allo Dashboard VPN. Se in questa pagina vengono visualizzate le statistiche sul traffico di caricamento e download, il server OpenVPN è in esecuzione.




## 9.2.3 Risoluzione dei problemi

Se la connessione fallisce, ci sono diversi motivi comuni:

- Il server VPN non ha un indirizzo IP pubblico. Vedi qui per la risoluzione dei problemi.
- Potrebbe essere necessario impostare il port forwarding. Vedi qui per la risoluzione dei problemi.
- La porta utilizzata per il server WireGuard è bloccata dal tuo provider di servizi Internet. Passa a un'altra porta o contatta il tuo ISP per assistenza.
- La connessione VPN potrebbe essere bloccata in alcuni paesi o regioni.

Capitolo 10

# Configurazione del client VPN

Questo capitolo introduce come configurare un router GL.iNet come client OpenVPN o WireGuard.

# 10.1 Configurazione del client OpenVPN

## 10.1.1 Preparazione

Innanzitutto, assicurati di avere un abbonamento attivo con un fornitore di servizi VPN che supporti la configurazione manuale di OpenVPN. Vedi qui per i provider OpenVPN compatibili con GL.iNet.

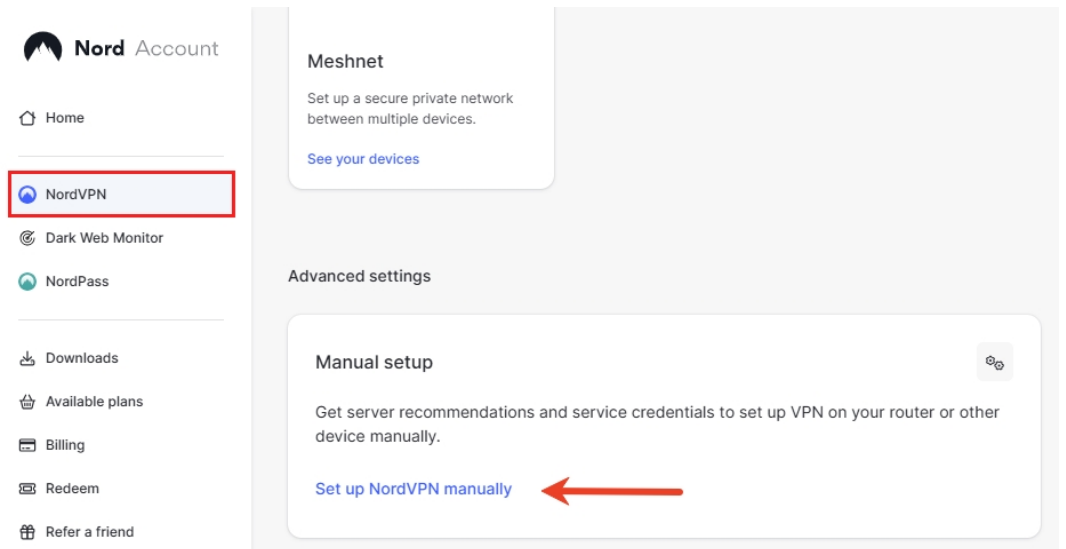
Successivamente, visita il sito Web ufficiale del fornitore di servizi VPN a cui sei iscritto e ottieni le credenziali del servizio o il file di configurazione. Se non sai come ottenere il file di configurazione, fai riferimento a questo collegamento o contatta il loro supporto.

## 10.1.2 Configurazione di NordVPN

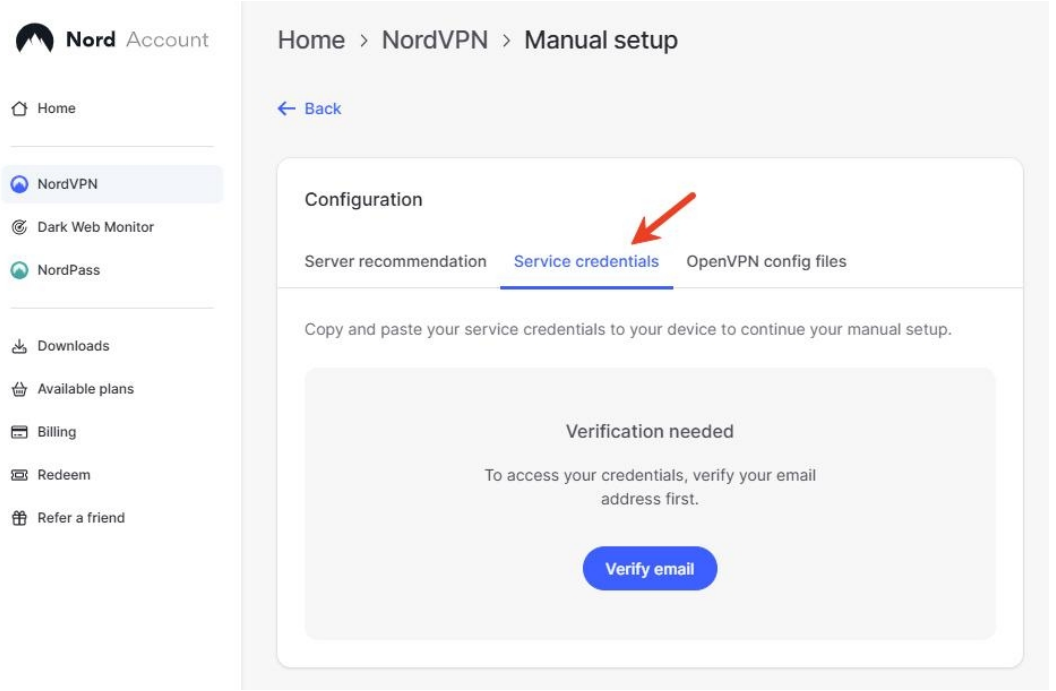
NordVPN è integrato in GL.iNet pannello di amministrazione web. Puoi acquisire file di configurazione per tutti i server NordVPN inserendo le credenziali del tuo account (ottenute dalla dashboard NordVPN) nell'app mobile pannello di amministrazione web o GL.iNet del router, eliminando la necessità di caricamenti manuali dei file.

Segui i passaggi seguenti per impostare il router come client NordVPN.

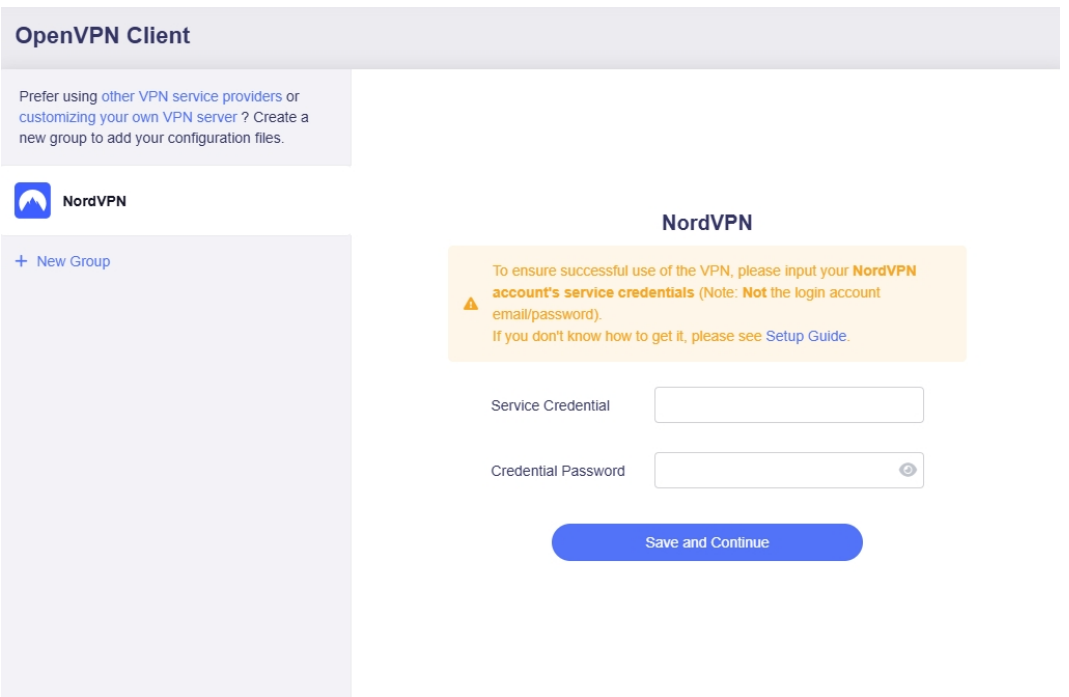
1. Accedi al tuo account web NordVPN qui.
2. Nella Nord Dashboard, fai clic su **NordVPN**, quindi su **Configura NordVPN manualmente**.



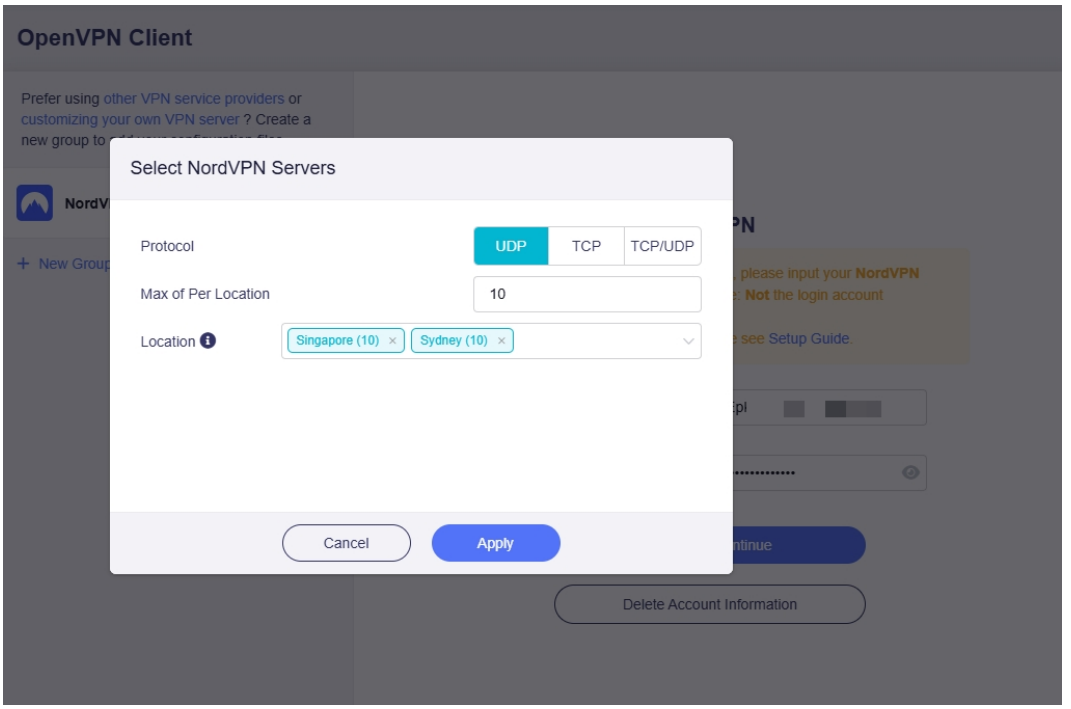

Troverai le **credenziali del servizio**. Copiali per un uso successivo.



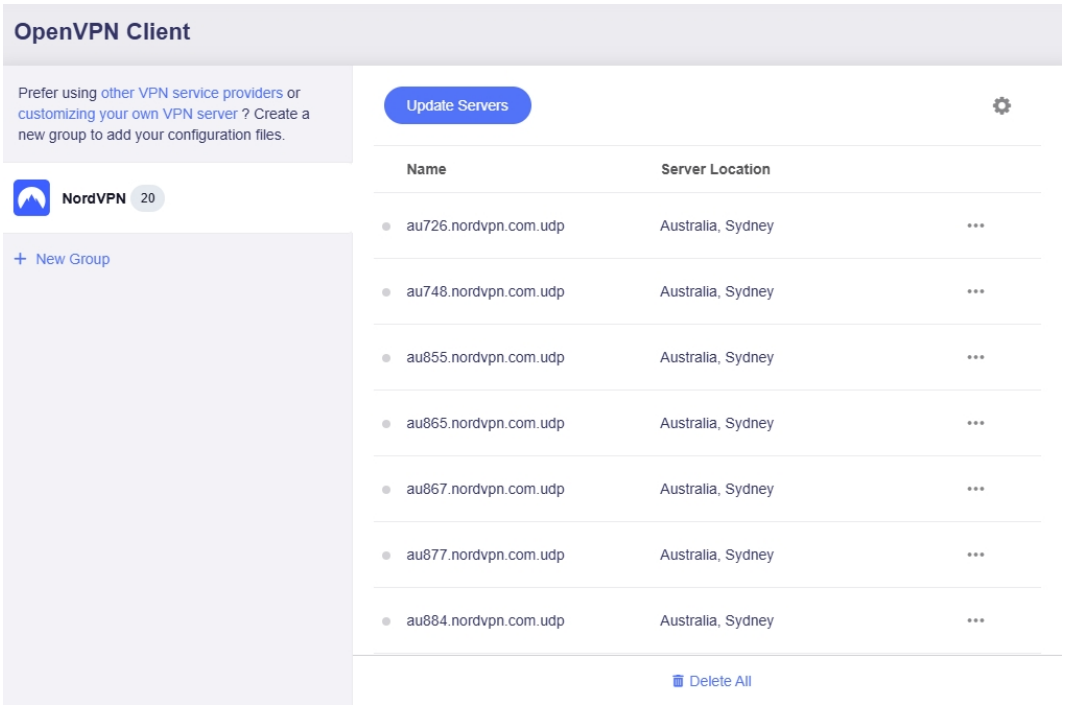

3. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client OpenVPN** > **NordVPN**. Inserisci le credenziali del servizio (Nota: NON è l'e-mail/password dell'account di accesso), quindi fai clic su **Salva e continua**.




4. Seleziona il protocollo, il numero massimo di server per ciascuna posizione e posizioni, quindi fai clic su **Applica**.

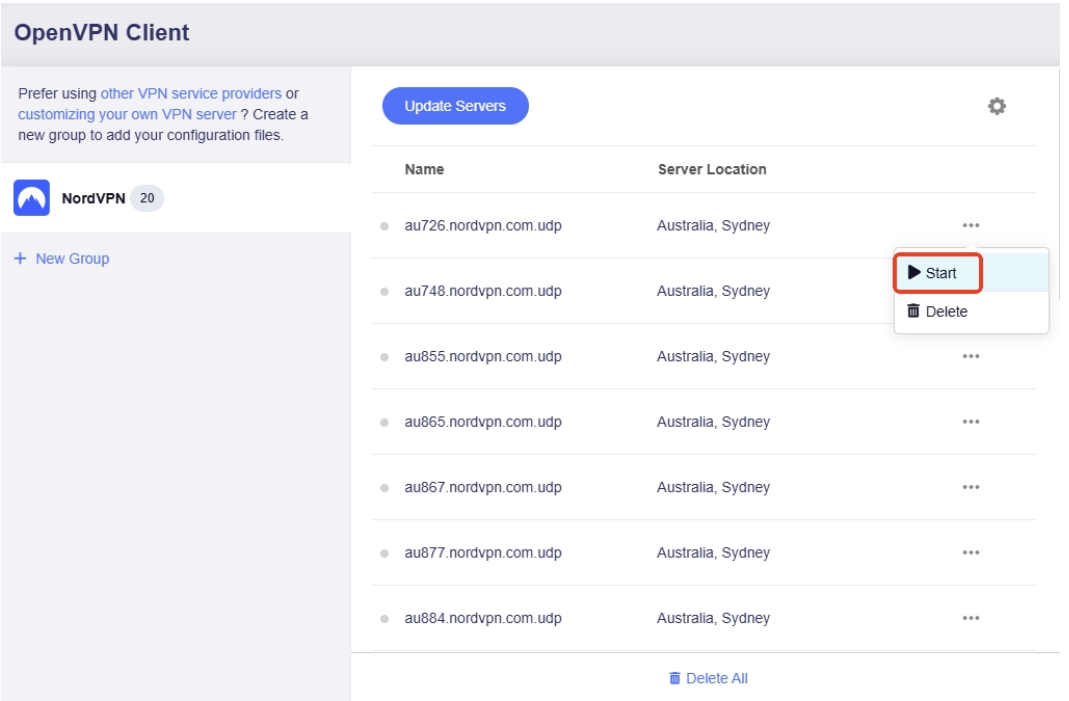



Scaricherà i file di configurazione.

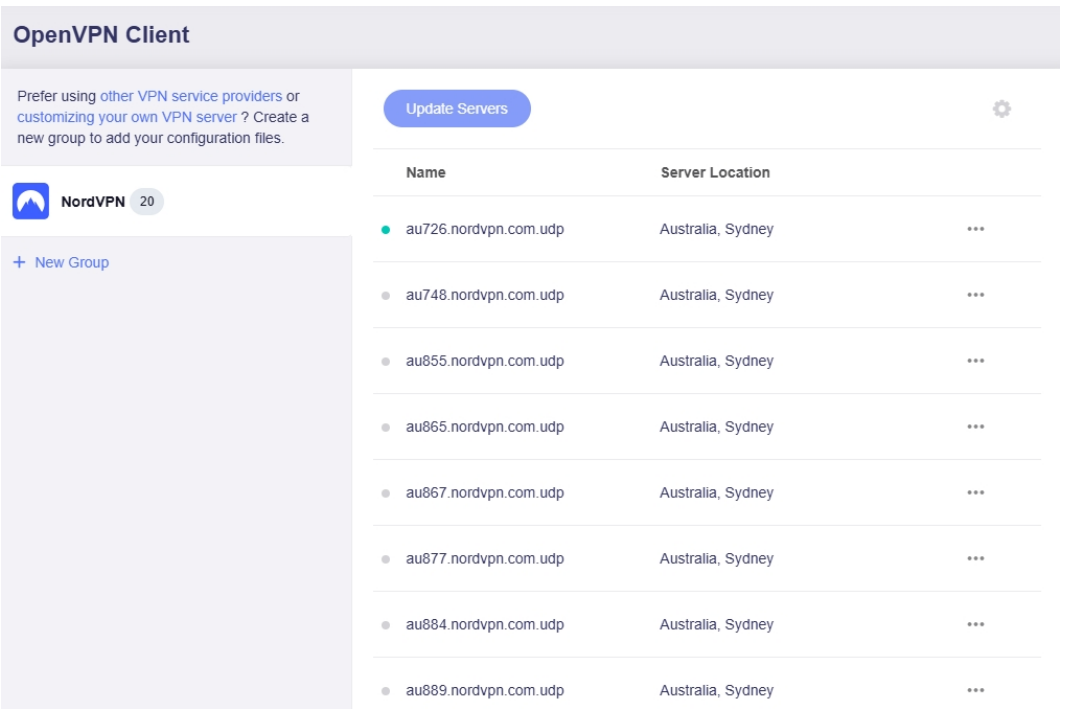



5. Avvia una connessione.

   Seleziona un server e fai clic sull'icona a tre punti a destra per avviare una connessione.



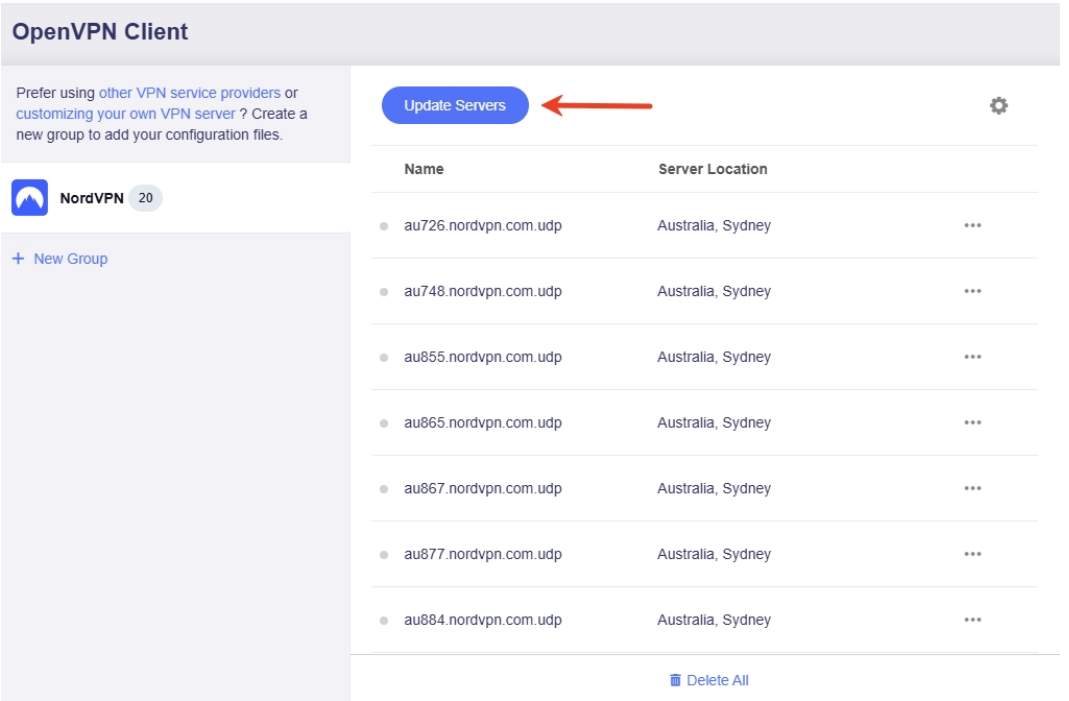

6. Una volta connesso, apparirà un punto verde accanto al file di configurazione.




Puoi anche controllare i dettagli della connessione VPN sulla **dashboard VPN**.

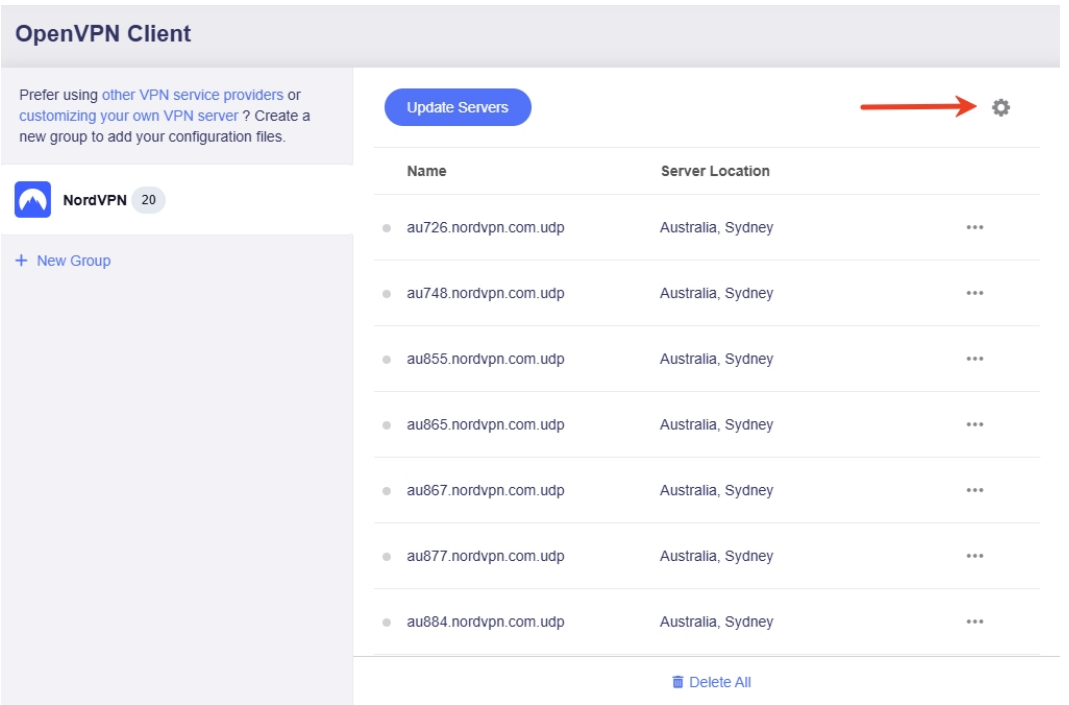
7. Aggiorna server.

   Puoi fare clic su **Aggiorna server** per ottenere l'elenco dei server disponibili più recente, evitando errori di connessione causati dalla manutenzione o dall'arresto del server.



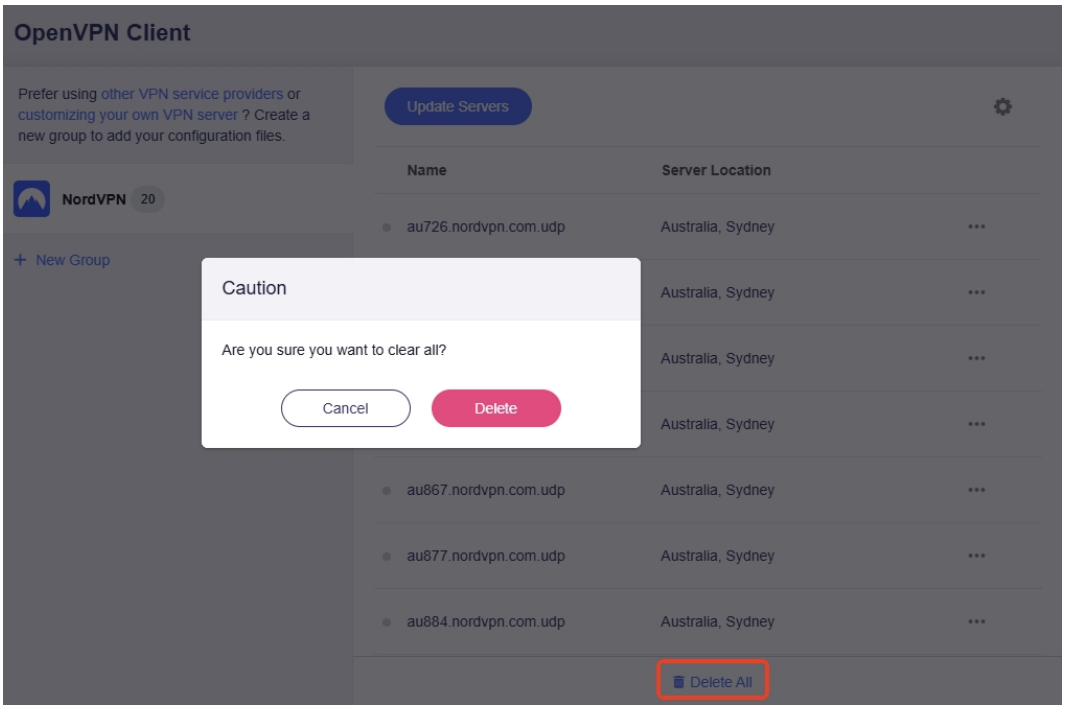

8. Modifica credenziali.

   Fai clic sull'icona a forma di ingranaggio per modificare le tue credenziali di accesso.




9. Elimina tutti i file.

   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic.

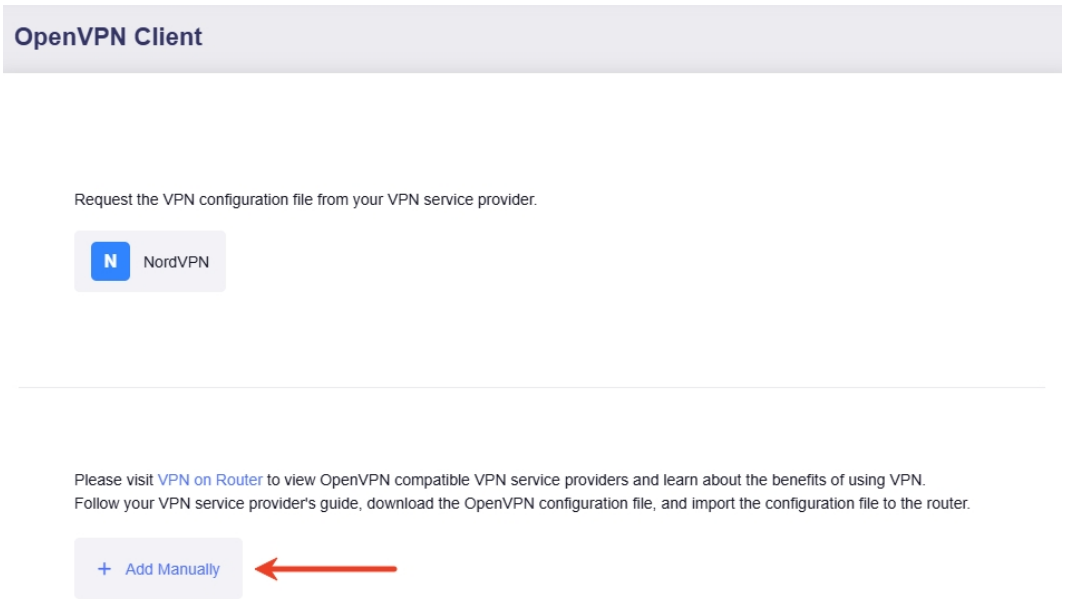

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

## 10.1.3 Configurazione manuale del client OpenVPN (altri provider)

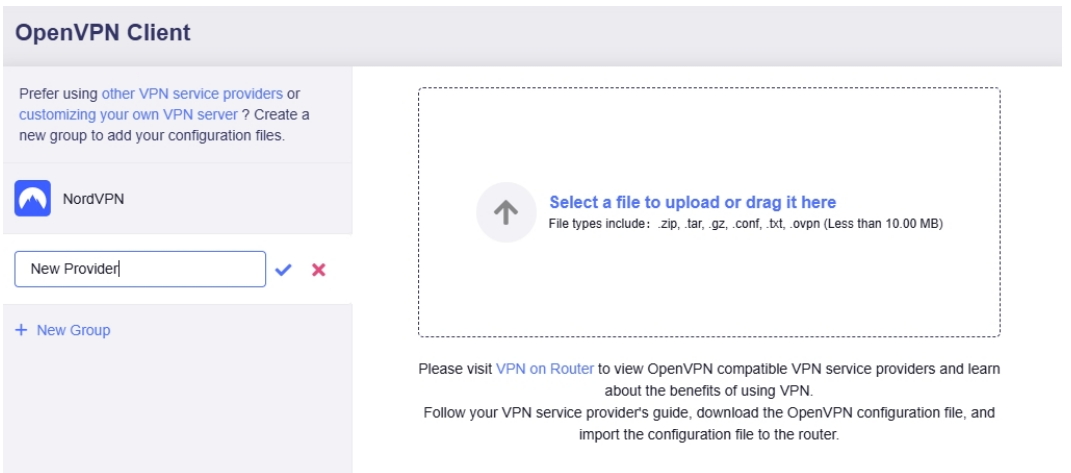
Se il tuo fornitore di servizi OpenVPN non è integrato nel nostro pannello di amministrazione, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare un client OpenVPN.

Nei passaggi seguenti, utilizzeremo PIA (Private Internet Access) come esempio.

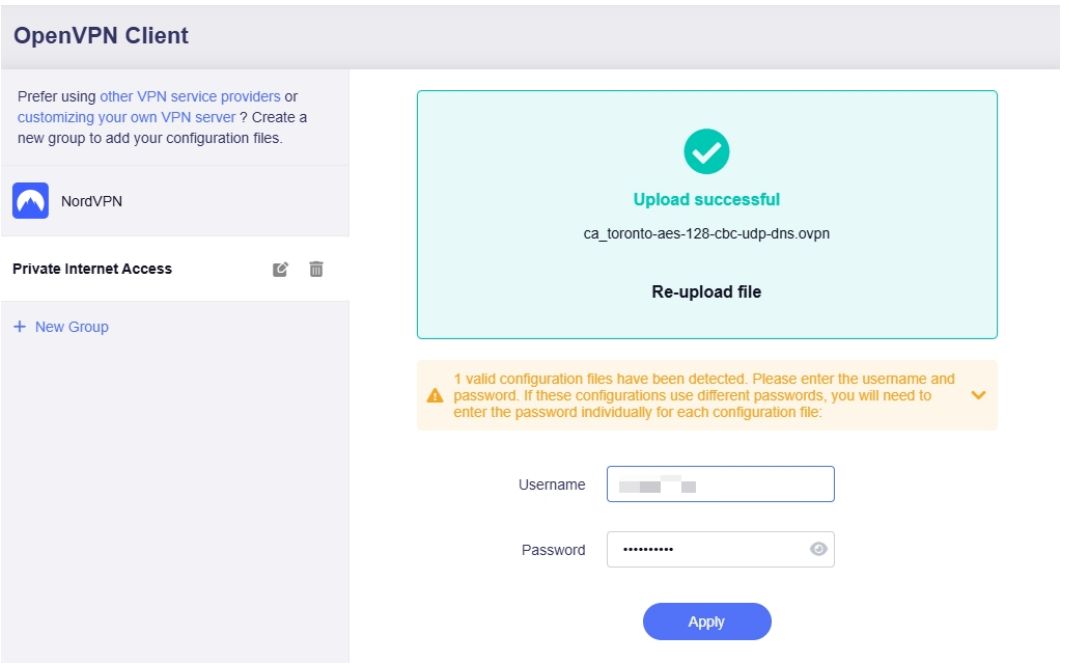
1. Scarica un file di configurazione dal sito Web ufficiale di Private Internet Access.
2. Accedi al pannello di amministrazione web del tuo router, vai a **VPN** > **Client OpenVPN** e fai clic su **Aggiungi manualmente**.



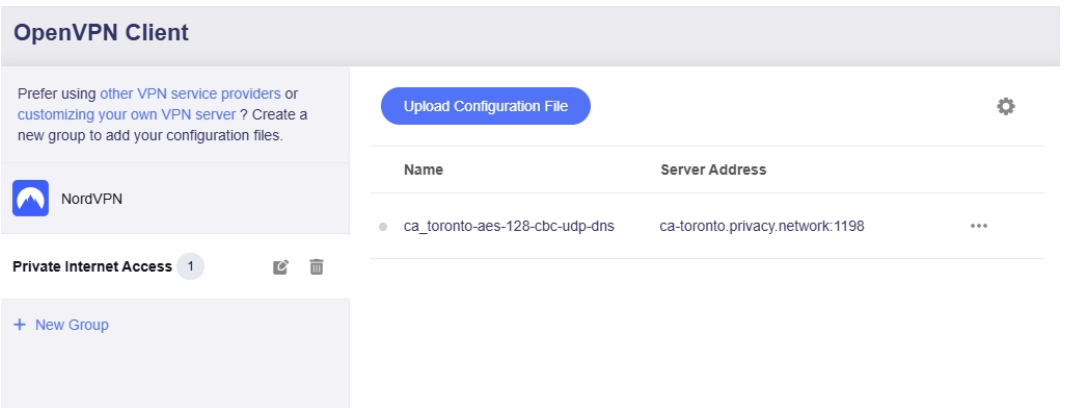

3. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.



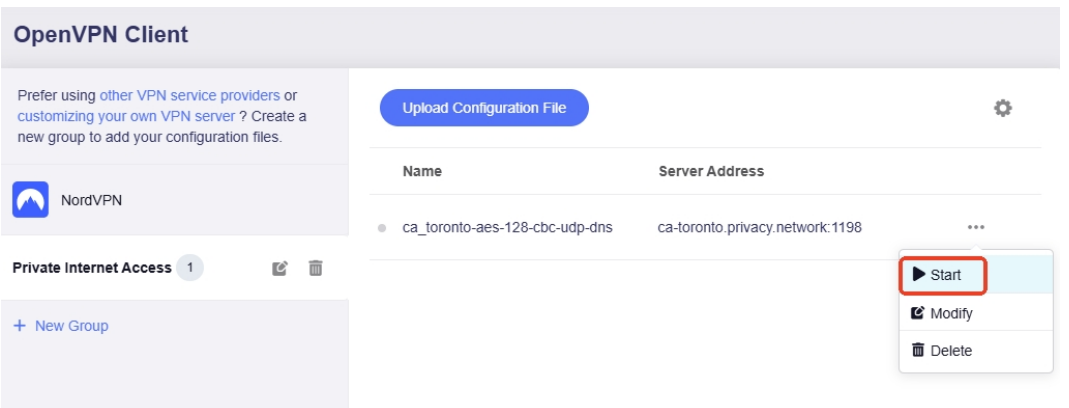
4. Carica il tuo file di configurazione OpenVPN. Inserisci le credenziali, se richieste, quindi fai clic su **Applica**.



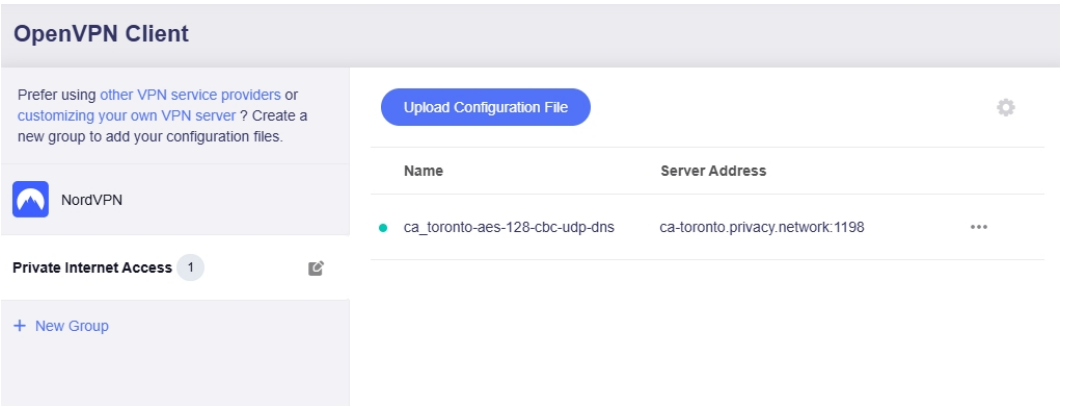

Vedrai il file di configurazione caricato.




5. Fai clic sull'icona con tre punti a destra per avviare una connessione.



6. Una volta connesso, apparirà un punto verde accanto al file di configurazione.




Puoi anche controllare i dettagli della connessione VPN sulla **dashboard VPN**.

## 10.2 Configurazione del client WireGuard

Puoi configurare Client WireGuard tramite l'app mobile GL.iNet o pannello di amministrazione web.

- L'app mobile integra alcuni fornitori di servizi WireGuard, come AzireVPN, Mullvad VPN, OVPN, StrongVPN, PIA VPN. Puoi configurarlo facilmente inserendo le credenziali di accesso del servizio WireGuard a cui sei iscritto. Apri l'app e segui le istruzioni visualizzate sullo schermo per la configurazione.
- pannello di amministrazione web non solo integra alcuni fornitori di servizi WireGuard, ma fornisce anche una voce per la configurazione manuale. Puoi inserire le credenziali del servizio WireGuard a cui sei iscritto per una configurazione rapida oppure caricare manualmente un file di configurazione per completare la configurazione.

### 10.2.1 Preparazione

Innanzitutto, assicurati di avere un abbonamento attivo con un fornitore di servizi VPN che supporti la configurazione manuale di WireGuard. Vedi qui per i provider WireGuard compatibili con GL.iNet.

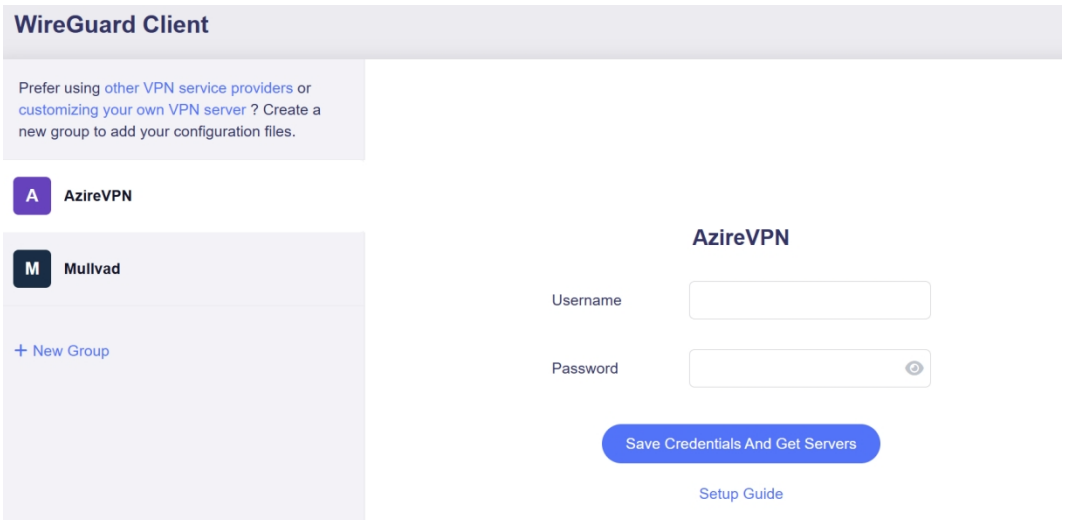
Successivamente, seleziona il fornitore di servizi WireGuard corrispondente di seguito per individuare rapidamente le istruzioni dettagliate.

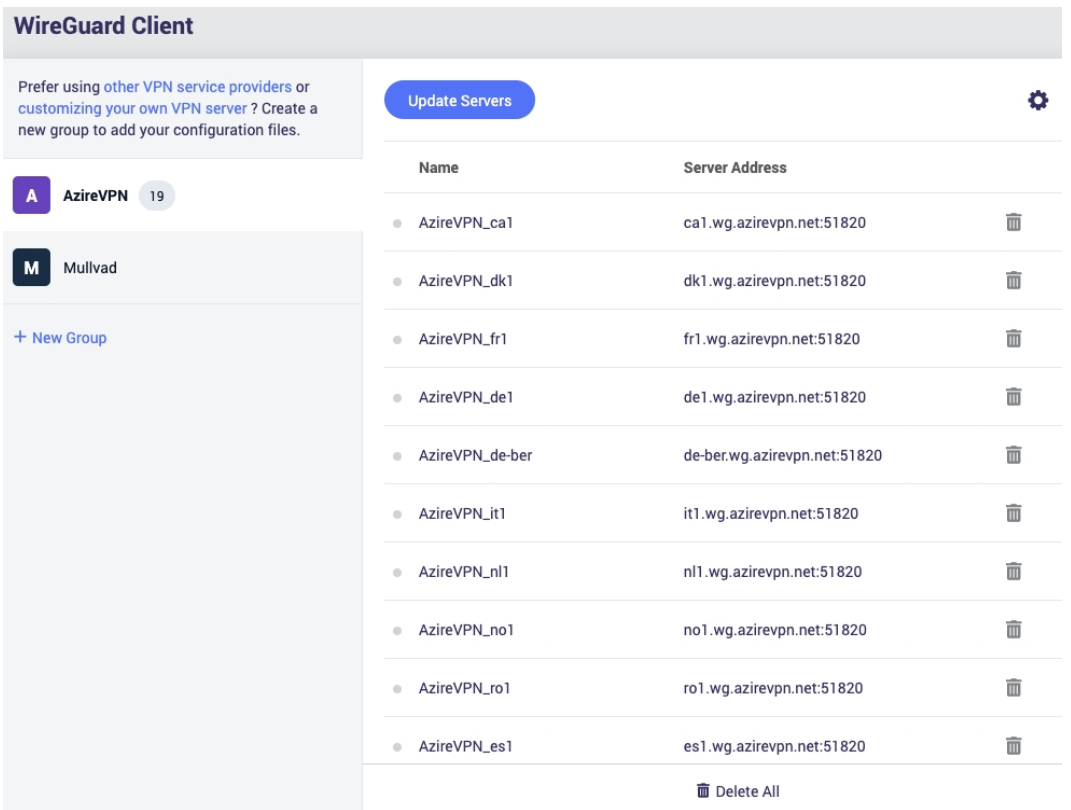
- Configurazione di AzireVPN
- Configurazione di Mullvad
- Configurazione manuale del client WireGuard (altri provider)

## 10.2.2 Configurazione di AzireVPN

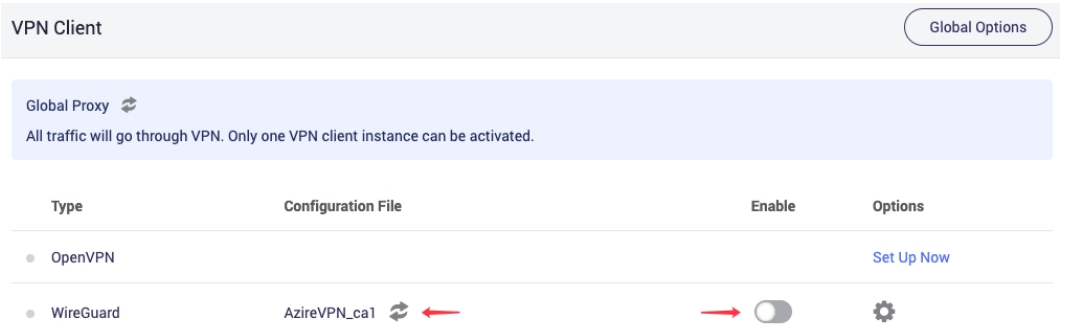
Segui i passaggi seguenti per impostare il router come client AzireVPN.

1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **AzireVPN**.
2. Inserisci nome utente e password, quindi fai clic su **Salva credenziali e ottieni server**. Genererà file di configurazione per ciascun server.

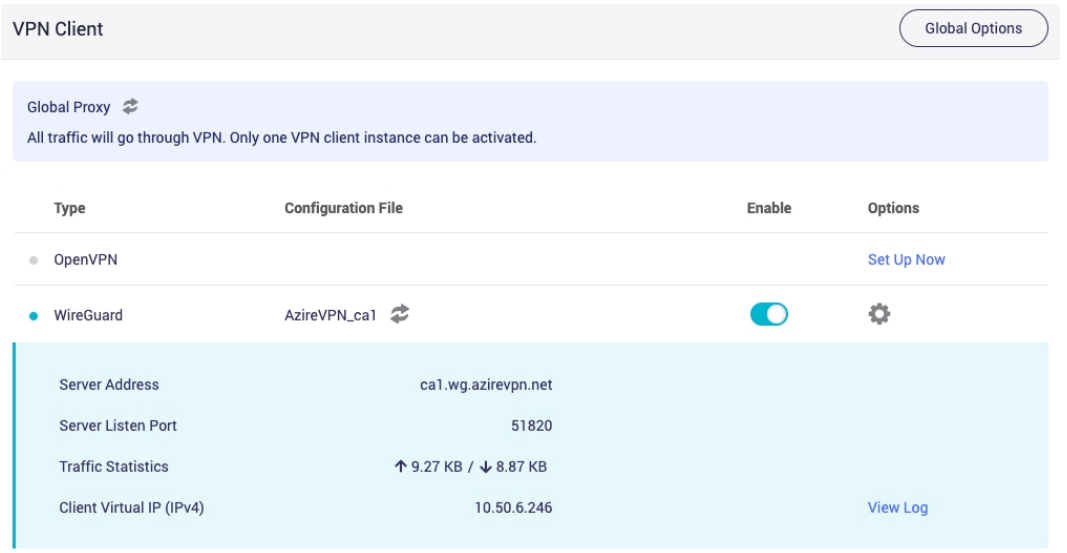



3. Vai a Dashboard VPN per abilitare la connessione.

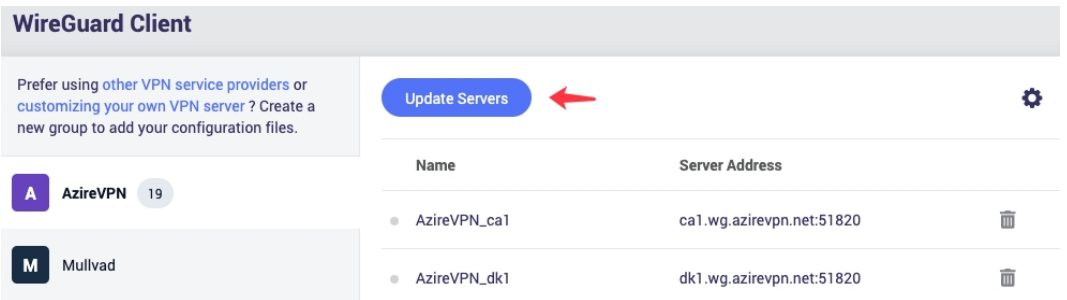



Una volta connesso, dovresti vedere il tuo indirizzo IP utente e il numero di byte inviati/ricevuti.



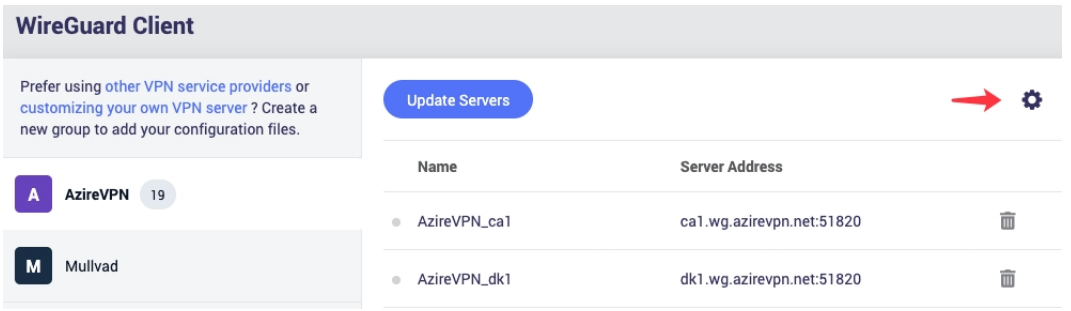

4. Aggiorna server.

   AzireVPN potrebbe mantenere o arrestare alcuni server, farà fallire la connessione, puoi **aggiornare i server** per ottenere gli ultimi server disponibili.



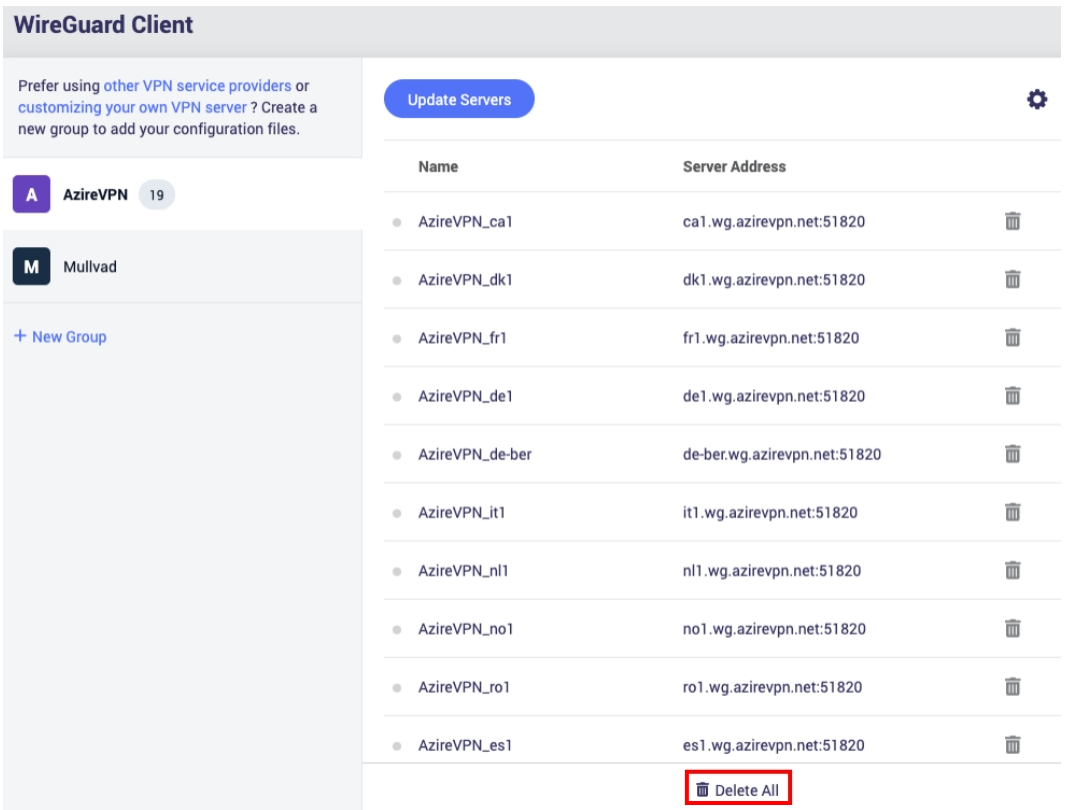

5. Modifica credenziali.

   Fai clic sull'icona a forma di ingranaggio per modificare la credenziale.




6. Elimina tutti i file.

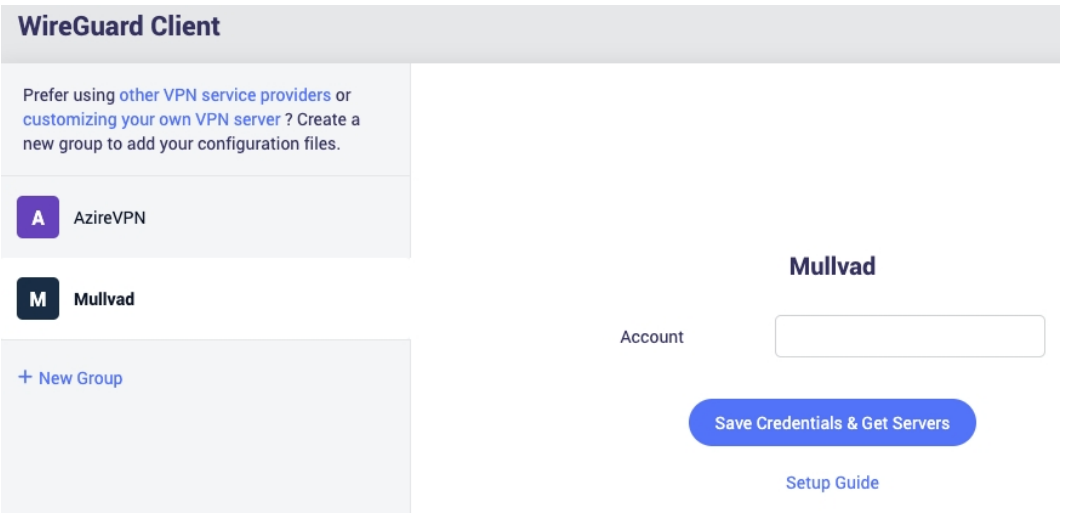
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic.



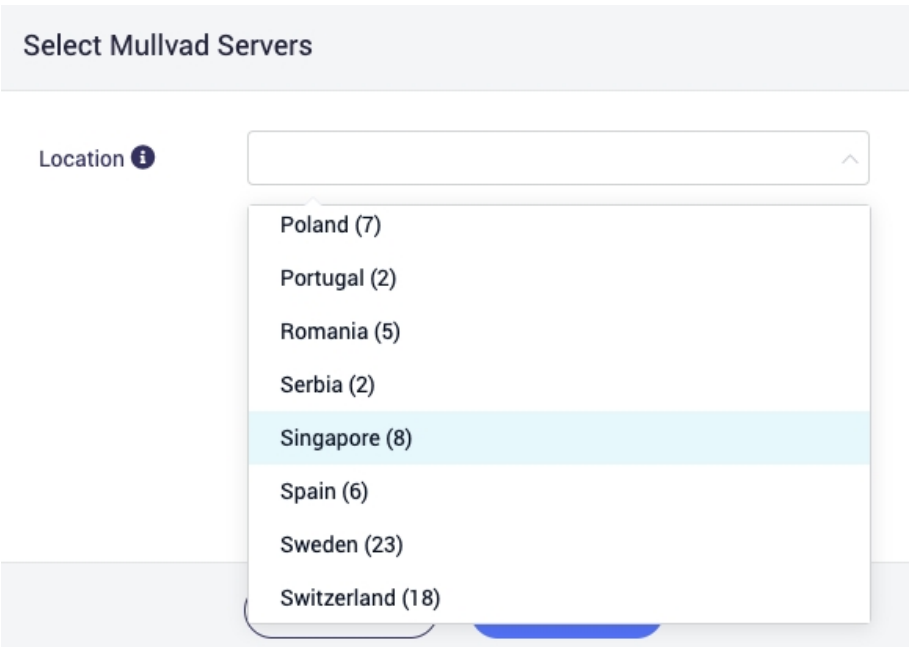
## 10.2.3 Configurazione di Mullvad

Segui i passaggi seguenti per impostare il router come client Mullvad.

1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Mullvad**.
2. Inserisci il tuo account Mullvad (numero di cifre 16), quindi fai clic su **Salva credenziali e ottieni server**.

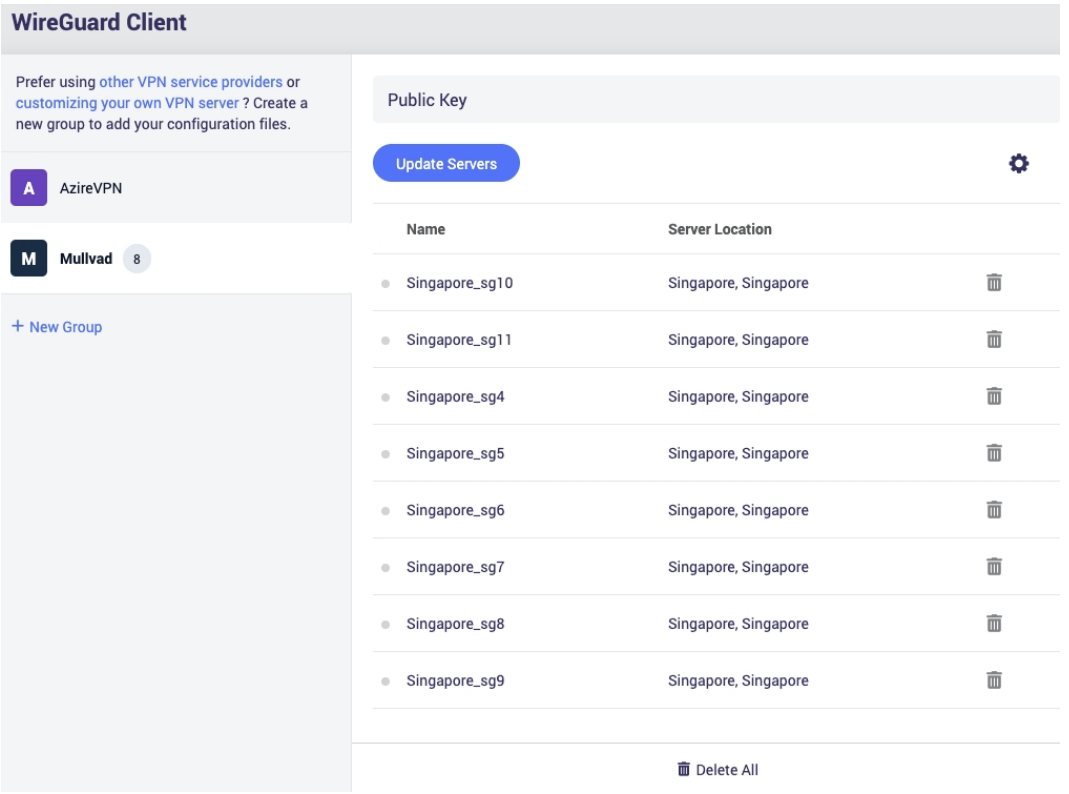



Apparirà una finestra di dialogo per selezionare una posizione.

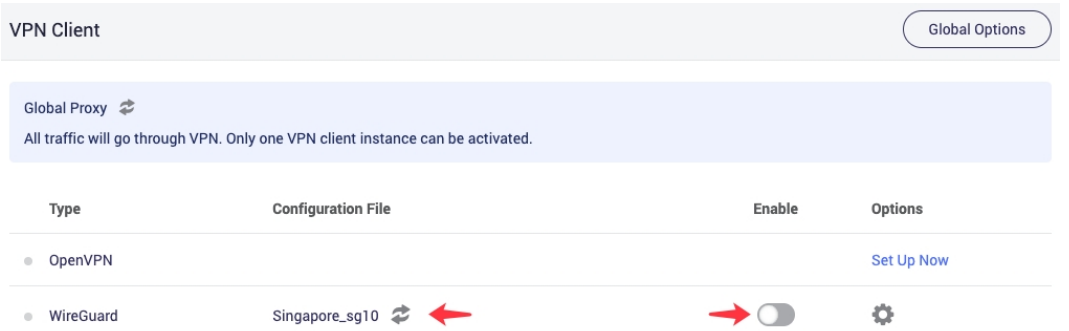



Quindi genererà i file di configurazione del server di posizione selezionato.

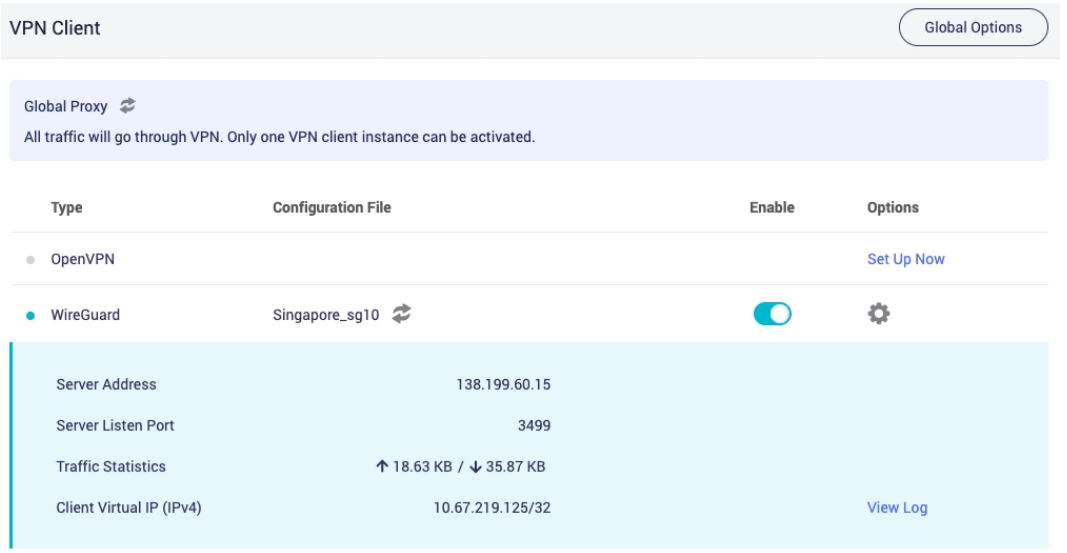
La **chiave pubblica** è la chiave pubblica WireGuard da inviare al server Mullvad. Puoi avere fino a cinque chiavi contemporaneamente e gestire le chiavi WireGuard nella pagina del tuo account Mullvad.




3. Vai a Dashboard VPN per abilitare la connessione.

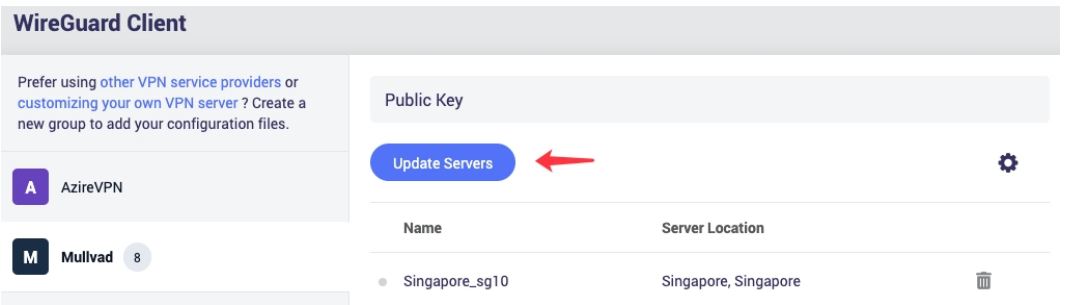



Una volta connesso, dovresti vedere il tuo indirizzo IP utente e il numero di byte inviati/ricevuti.



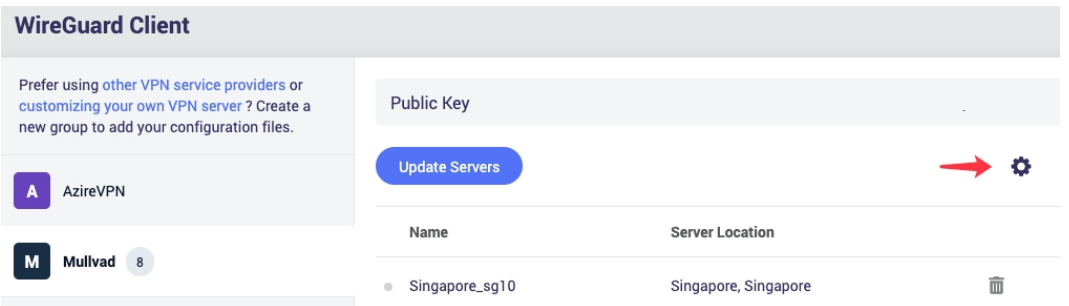

4. Aggiorna server.

   Mullvad potrebbe mantenere o arrestare alcuni server, farà fallire la connessione, puoi **aggiornare i server** per ottenere gli ultimi server disponibili.



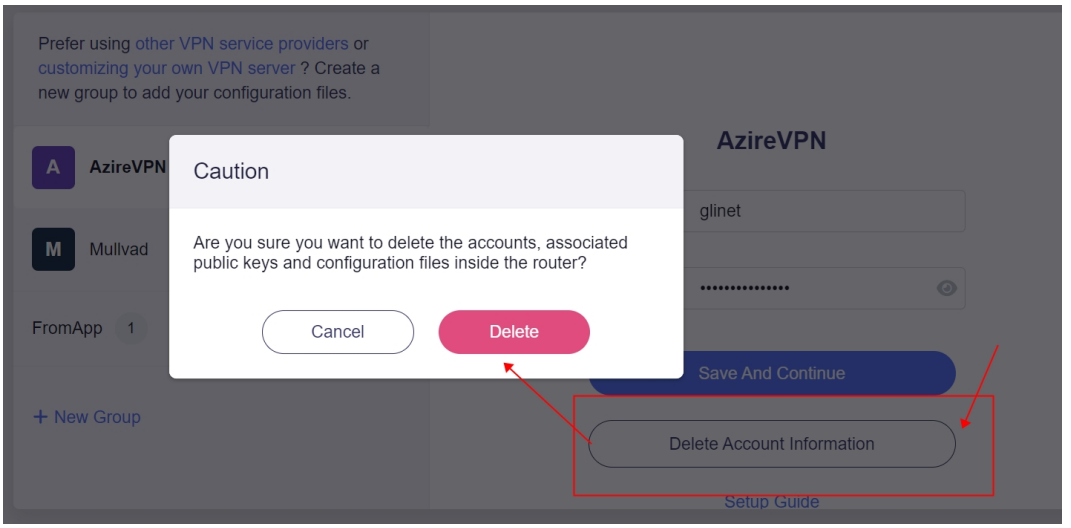

5. Modifica credenziali

   Fai clic sull'icona a forma di ingranaggio per modificare le tue credenziali di accesso.



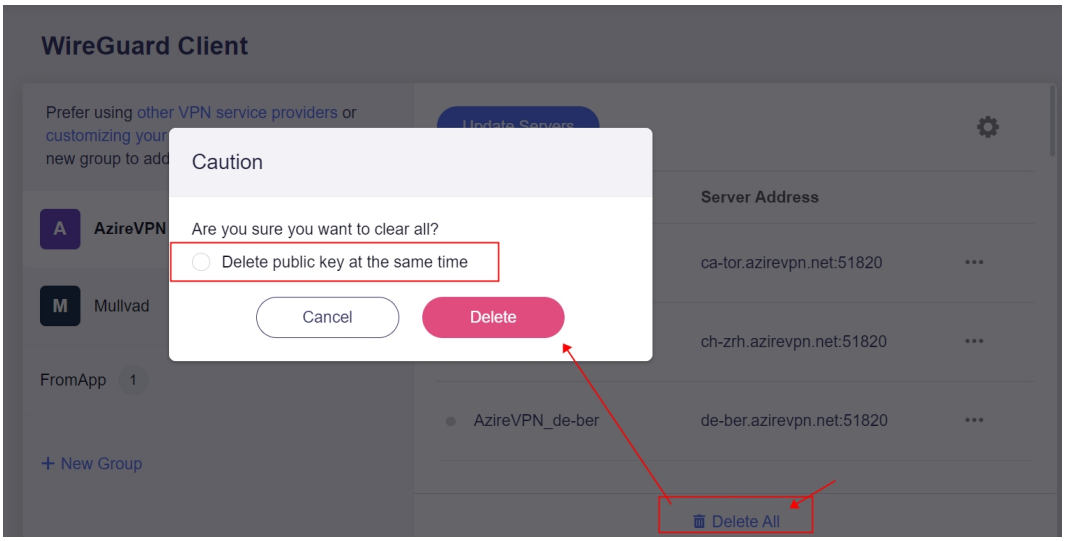

6. Elimina le informazioni dell'account

   Se fai clic su **Elimina**, verranno eliminate le credenziali dell'account, la chiave privata, la chiave pubblica e i file di configurazione **nel router**.




7. Elimina

   Consente di eliminare tutti i file di configurazione con un clic e fornisce una richiesta per eliminare anche la chiave privata e la chiave pubblica.

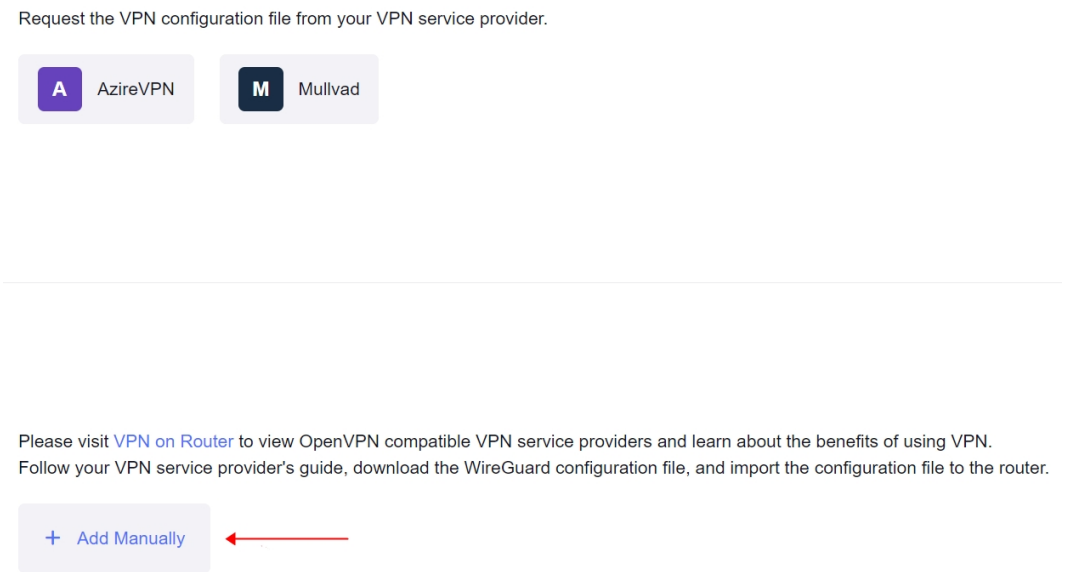


## 10.2.4 Configurazione manuale del client WireGuard (altri provider)

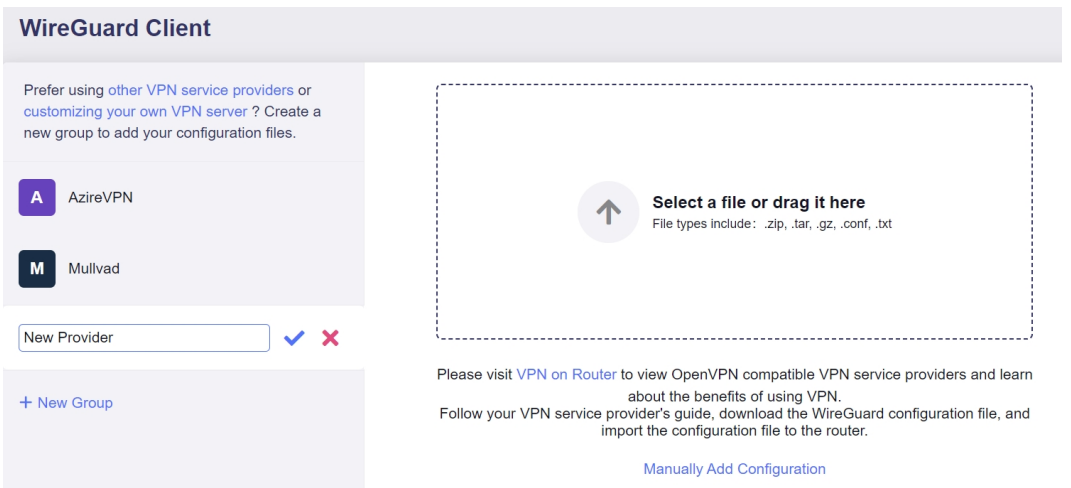
Se il tuo fornitore di servizi WireGuard non è integrato nel pannello di amministrazione web, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare uno WireGuard client. Se non sai come scaricare i file di configurazione, consulta questa guida o contatta il loro supporto.

Di seguito sono riportati i passaggi per caricare il file di configurazione sul router per configurare un client WireGuard.

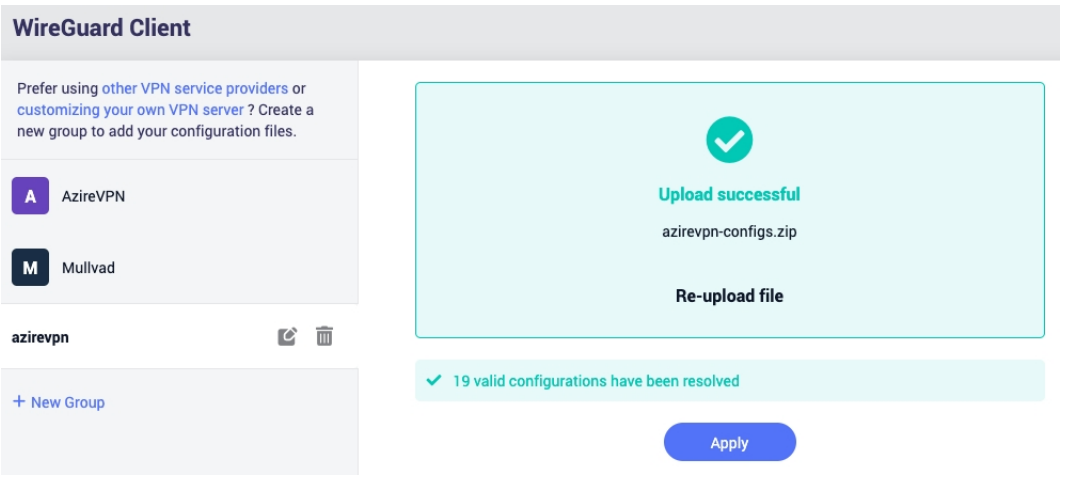
1. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client WireGuard** > **Aggiungi manualmente**.




2. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.

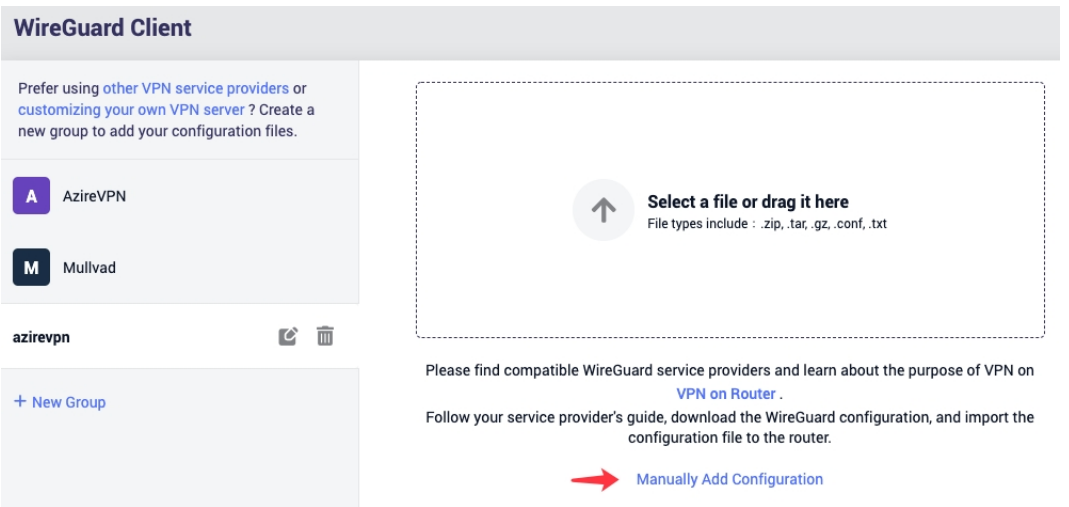


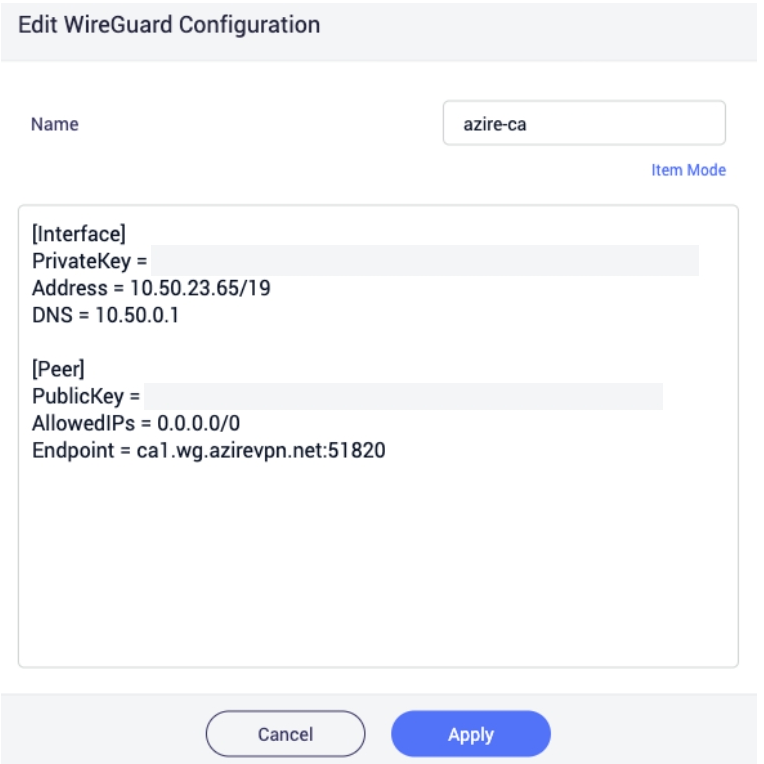
3. Fai clic sull'area di caricamento per caricare il file di configurazione WireGuard (formati supportati: zip, tar, gz, conf, txt) e fai clic su **Applica**.



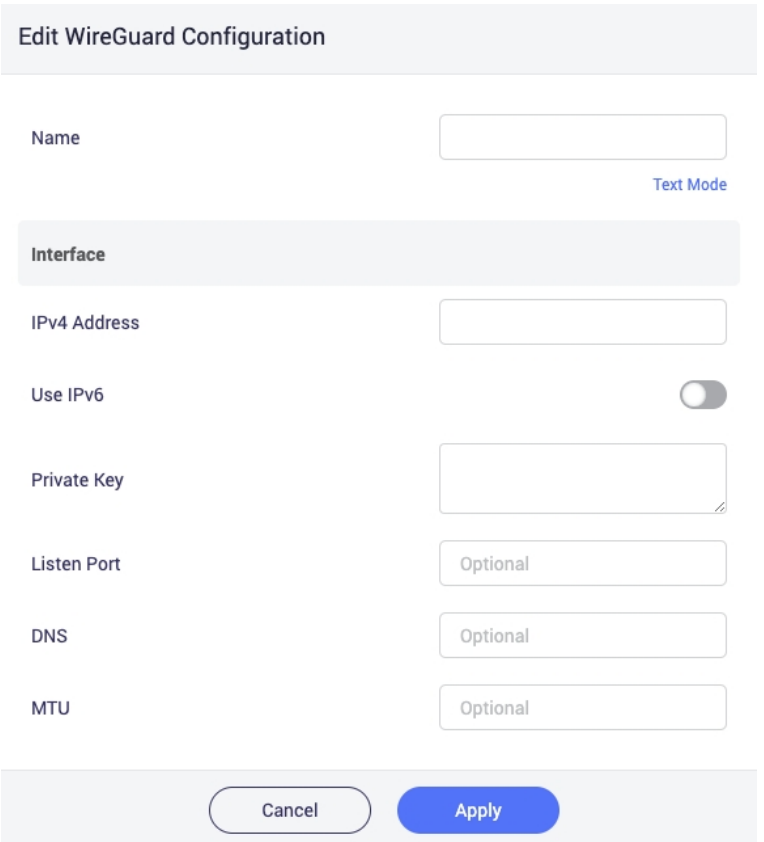

Se carichi un file compresso contenente più file di configurazione, verrà decompresso automaticamente.

In alternativa, puoi fare clic su **Aggiungi manualmente la configurazione** nella parte inferiore dell'area di caricamento, aggiungere i dettagli della configurazione in formato testo e fare clic su **Applica**.

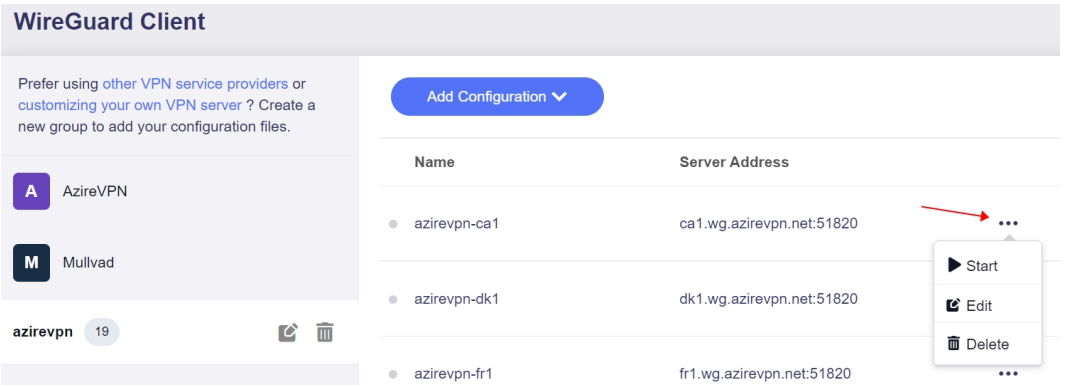




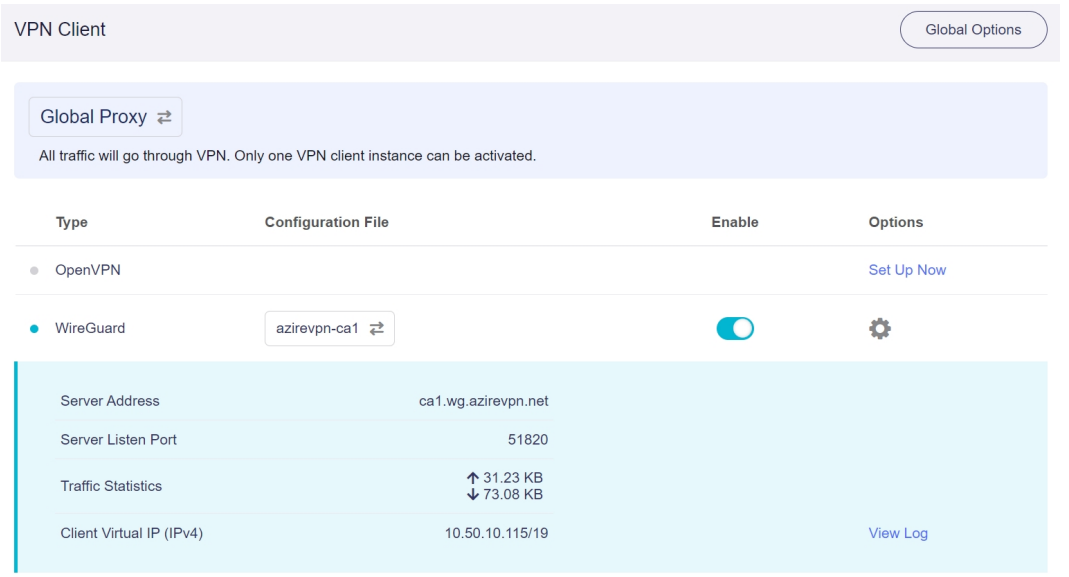

Per verificare ogni parametro, passa alla modalità Voce e controlla i dettagli della configurazione, quindi fai clic su **Applica**.



4. Fai clic sull'icona a tre punti sul lato destro per avviare la connessione.




5. Una volta connesso, apparirà un punto verde accanto al file di configurazione. Puoi controllare i dettagli della connessione VPN sulla **dashboard VPN**.



Capitolo 11

# Tor

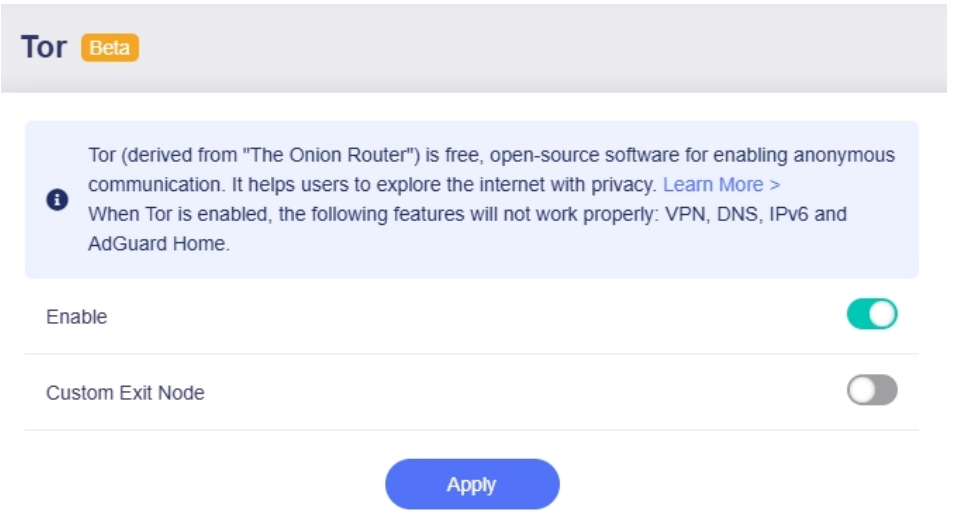
Questo capitolo fornisce una breve introduzione a Tor (The Onion Router), un software gratuito e open source per consentire la comunicazione anonima.

Tor (derivato da **The Onion Router**) è un software gratuito e open source per consentire la comunicazione anonima. Aiuta gli utenti a esplorare Internet con privacy. Tieni presente che questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug.

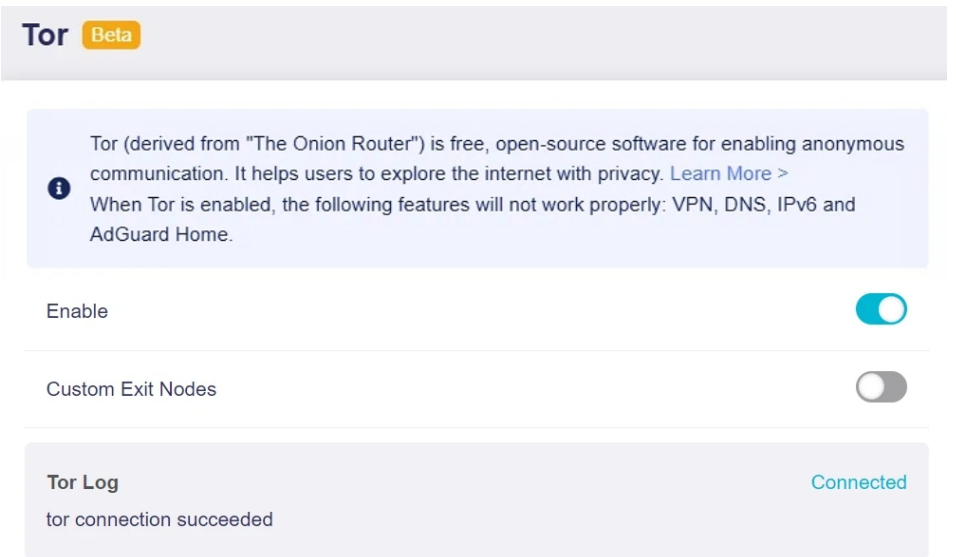
Quando Tor è abilitato, le seguenti funzionalità non funzioneranno correttamente: VPN, DNS, IPv6 e AdGuard Home.

Segui i passaggi seguenti per configurare Tor se necessario.

1. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Tor**. Attiva l'interruttore per abilitarlo, abilita i nodi di uscita personalizzati se necessario e fai clic su **Applica**.




2. Inizierà a connettersi. Se la tua rete soddisfa i requisiti, verrà visualizzata connessa.



Capitolo 12

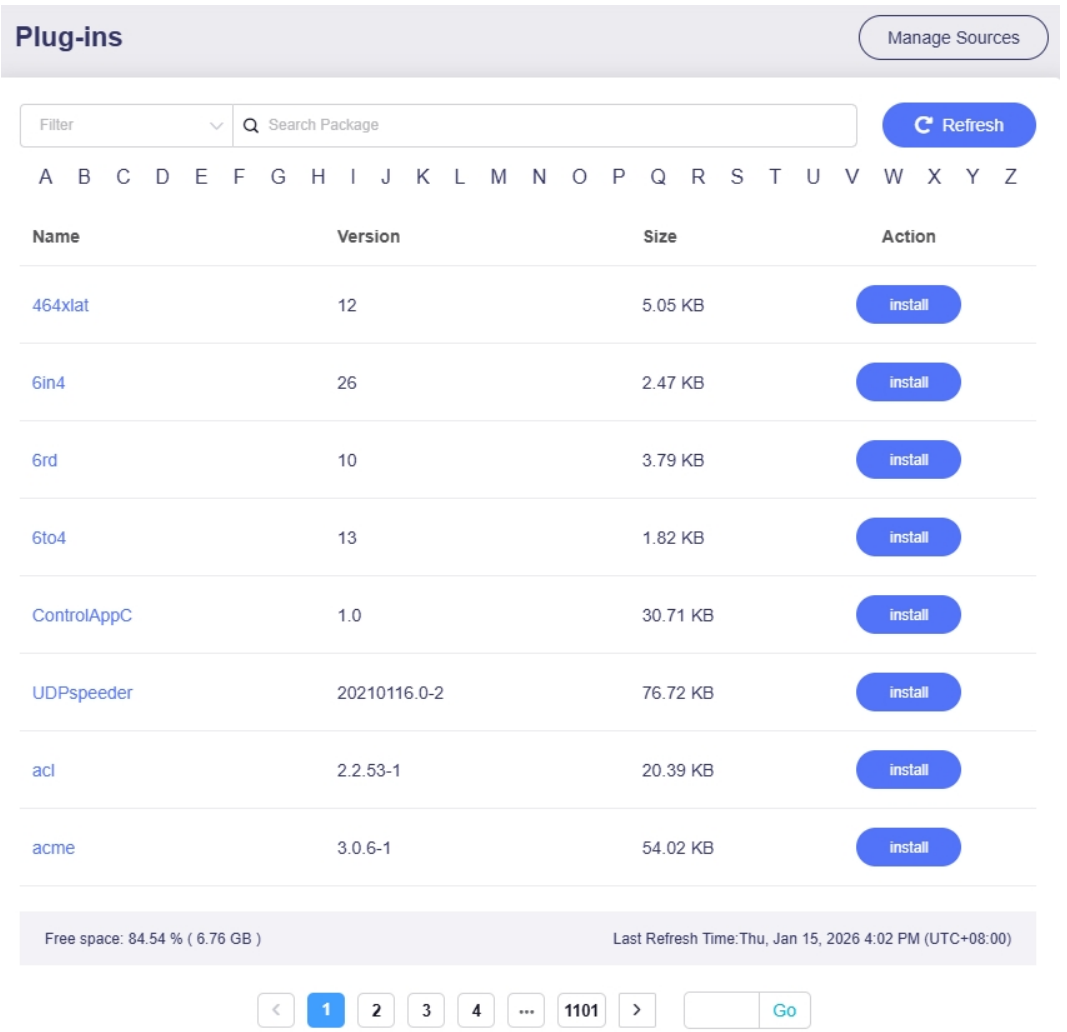
# Applicazioni

Questo capitolo introduce alcune applicazioni nei router GL.iNet, ad esempio plug-in, DNS dinamico, GoodCloud, AdGuard Home, Controllo parentale, ZeroTier e Tailscale.

## 12.1 Plug-in

La pagina Plug-in ti consente di gestire i pacchetti OpenWrt.

Accedi al pannello di amministrazione web del tuo router, vai su **APPLICAZIONI** > **Plug-in.** È possibile installare o rimuovere qualsiasi pacchetto disponibile nel repository. Fare clic sul pulsante **Aggiorna** per aggiornare l'elenco dei pacchetti prima di installare i plug-in.




**Nota**:

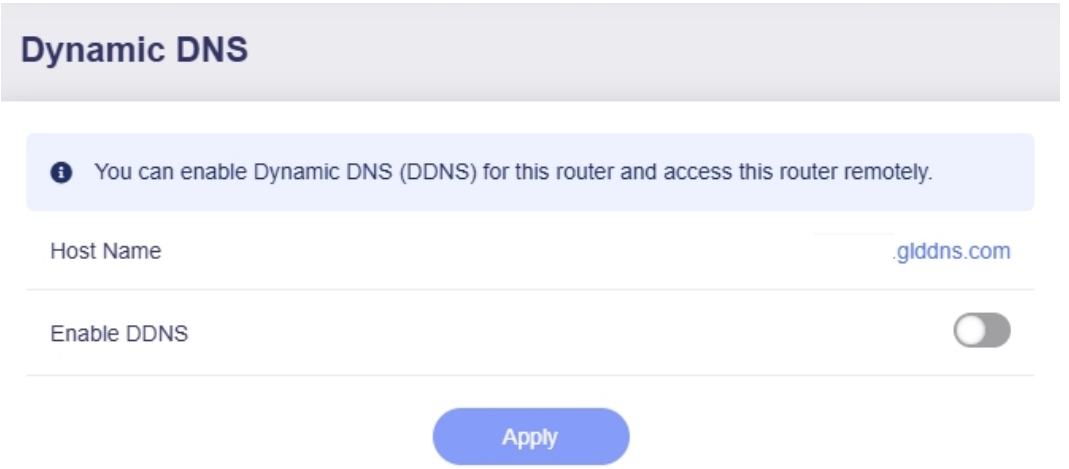
1. Non è consigliabile aggiornare i plug-in preinstallati nel firmware ufficiale GL.iNet, come nginx, adguard home, tailscale, ecc.
2. I plugin di terze parti installati manualmente dagli utenti possono essere aggiornati; tuttavia, GL.iNet non è responsabile per eventuali problemi di sicurezza derivanti da plug-in di terze parti. Per domande, contattare i rispettivi autori di plug-in di terze parti.

## 12.2 DNS dinamico

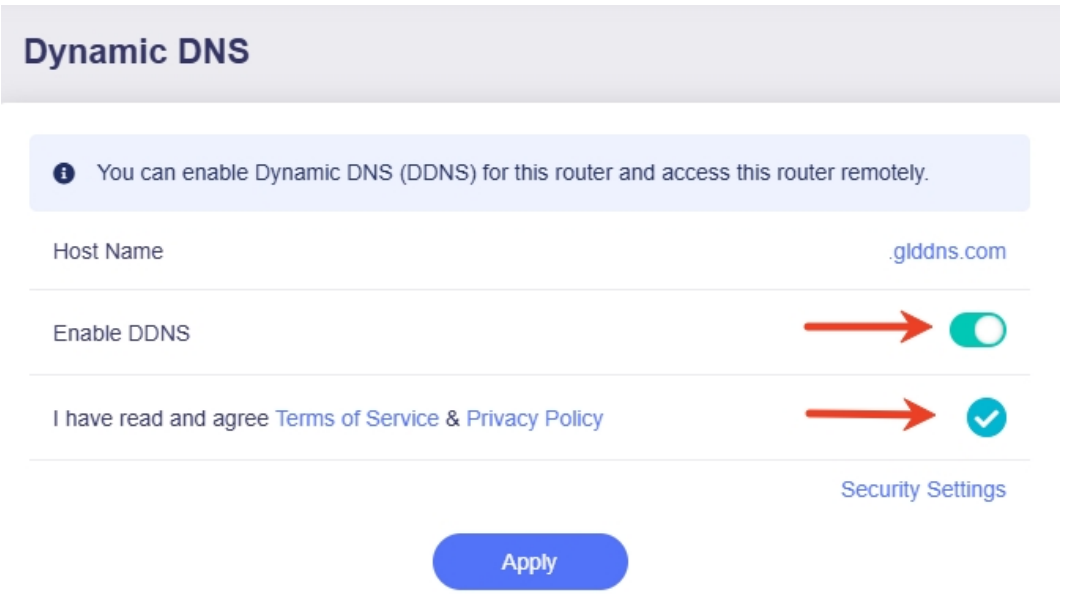
Dynamic Domain Name Service (DDNS o DNS dinamico) è un servizio utilizzato per mappare un nome di dominio all'indirizzo IP dinamico di un dispositivo di rete. Con DNS dinamico puoi accedere al tuo router da remoto. Per questa funzionalità è richiesto un indirizzo IP pubblico.

### 12.2.1 Abilita DDNS

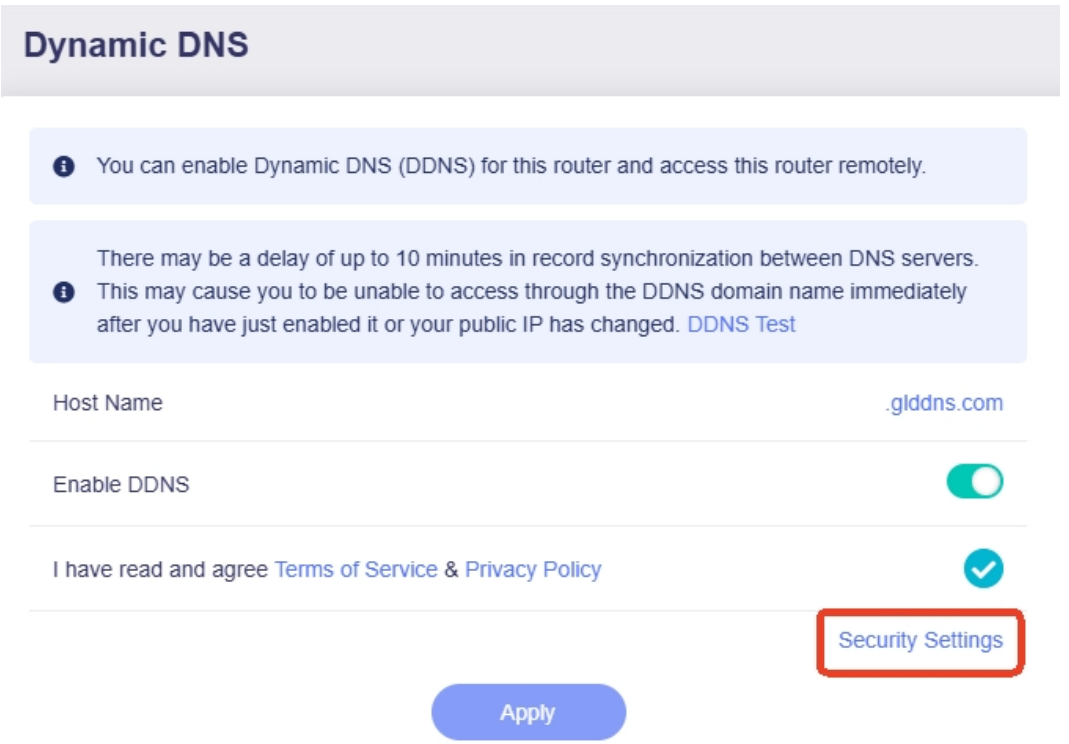
1. Accedi al pannello di amministrazione web del tuo router, vai su **APPLICAZIONI** > **DNS dinamico**, la pagina viene visualizzata come di seguito.



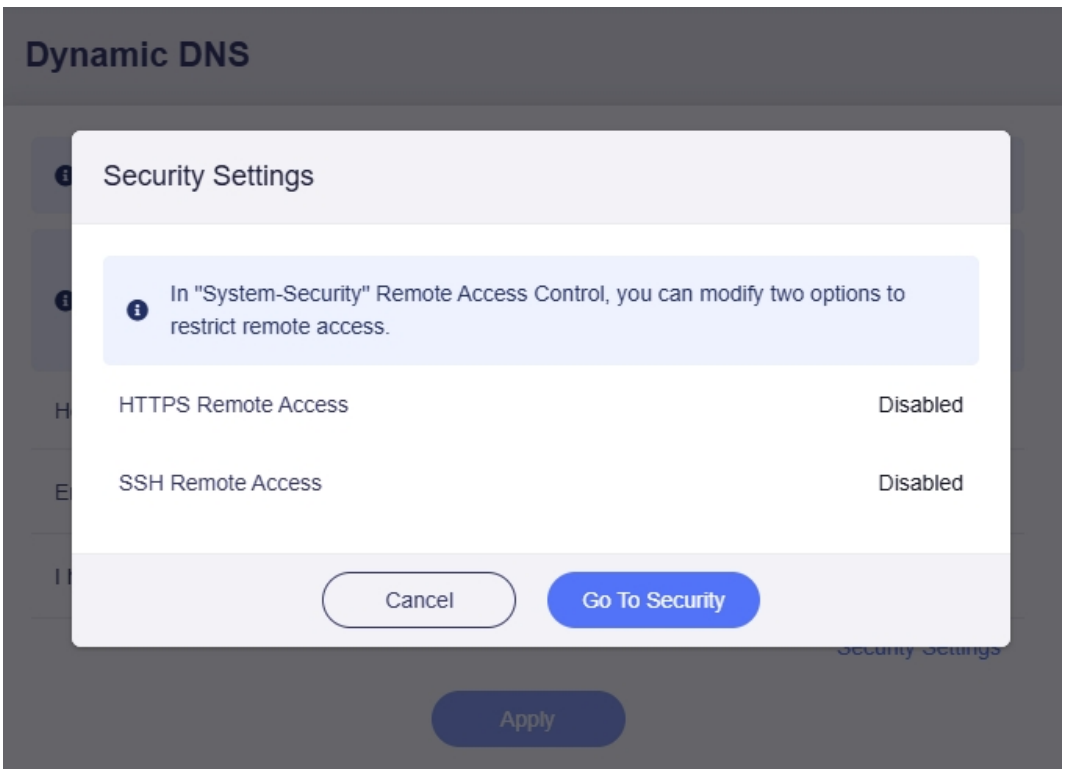

2. Attiva **Abilita DDNS**, leggi e accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.



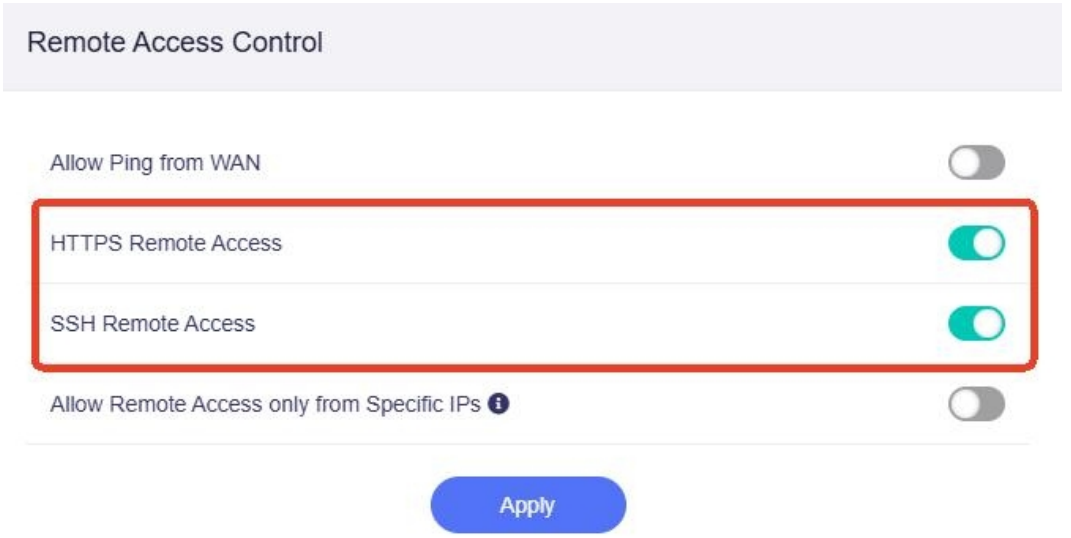

3. Fai clic su **Impostazioni di sicurezza** nell'angolo in basso a destra.




4. Nella finestra pop-up, controlla se l'accesso remoto che desideri utilizzare è abilitato.




In caso contrario, vai su **SISTEMA** > **Sicurezza** > **Controllo dell'accesso remoto** per abilitarlo, quindi fai clic su **Applica**.




**Nota**:

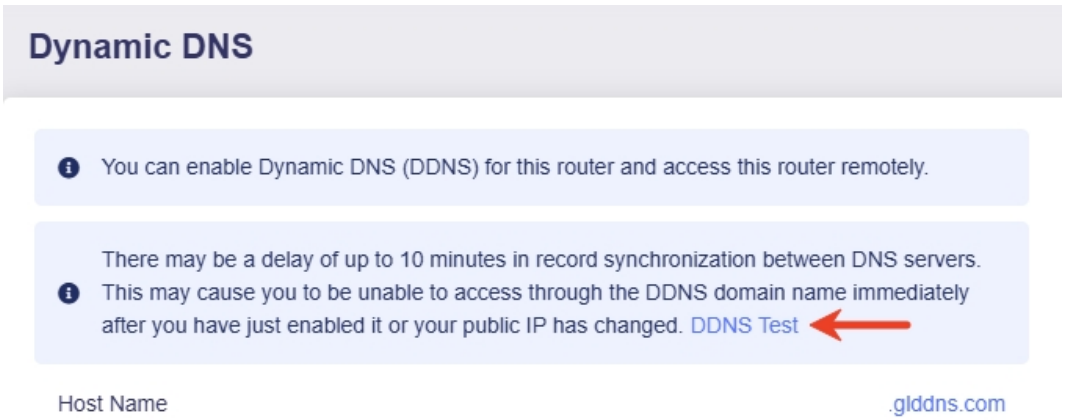
1. Potrebbe verificarsi un ritardo fino a 10 minuti nella sincronizzazione dei record tra i server DNS. Ciò potrebbe impedirti di accedere tramite il nome di dominio DDNS immediatamente dopo averlo abilitato o quando il tuo IP pubblico cambia.
2. Se abiliti DDNS e client VPN contemporaneamente, assicurati che Usa la VPN per i servizi GL.iNet siano disabilitati.

## 12.2.2 Verifica del funzionamento del DDNS

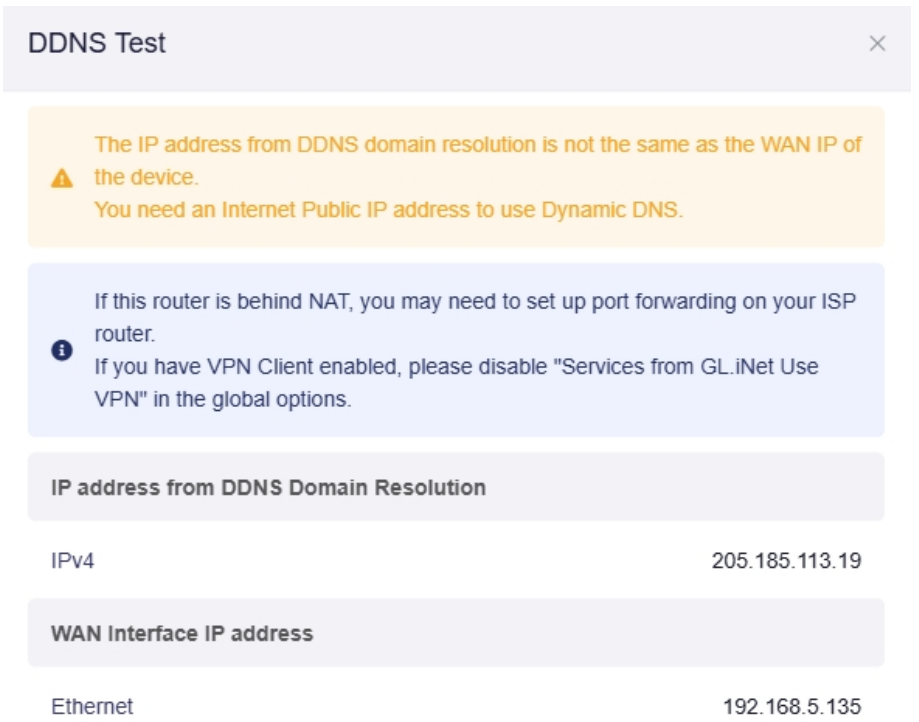
Puoi verificare se DDNS funziona utilizzando lo strumento di test DDNS o manualmente tramite comandi.

**Metodo 1. Utilizzo dello strumento di verifica DDNS**

1. Nella pagina DNS dinamico, fai clic su **Test DDNS**.




2. Assicurati che l'indirizzo IP dalla risoluzione del dominio DDNS corrisponda all'IP WAN del router. In caso contrario, verrà visualizzato un messaggio giallo in alto, che indica che il router potrebbe trovarsi dietro NAT e che è necessario impostare il port forwarding sul router upstream.



**Metodo 2. Utilizza i comandi**

1. Utilizzare il comando nslookup *nslookup xxxxxxx.glddns.com 8.8.8.8* per ottenere la mappatura tra nome di dominio e indirizzo IP, come mostrato di seguito.



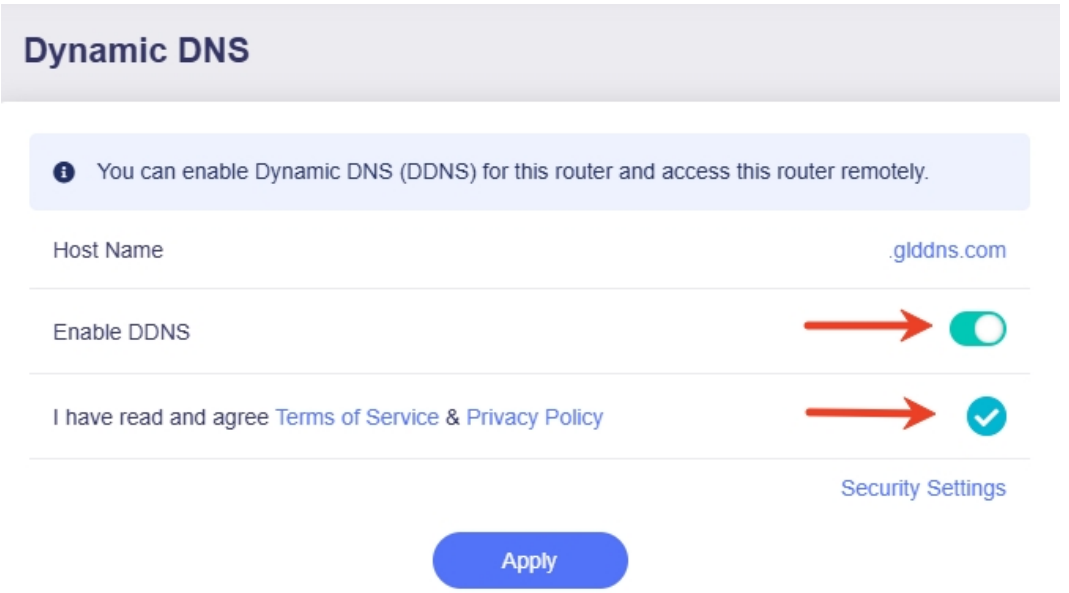

   - Sostituisci "xxxxxxx.glddns.com" nell'immagine sopra con il tuo nome host.
   - "8.8.8.8" è il DNS di Google. Usalo o sostituiscilo con altri, quindi premi Invio.
2. Se ottieni un indirizzo IP pubblico come "183.178.10.100" nell'immagine sopra, indica che il tuo dominio DDNS è stato mappato correttamente su un indirizzo IP pubblico. Se ricevi un messaggio del tipo "il server non riesce a trovare xxxxxxx.glddns.com", potrebbe indicare che la risoluzione del dominio non è riuscita e che il tuo dominio DDNS non è stato mappato correttamente su un indirizzo IP pubblico. Procedi al passaggio successivo per verificare.
3. Accedi al pannello di amministrazione web del tuo router e vai su **INTERNET**. Trova l'indirizzo IP WAN del tuo router nell'interfaccia attualmente attiva. Confronta questo indirizzo IP con l'indirizzo IP pubblico ottenuto sopra. Se sono uguali, è in vigore il DDNS, altrimenti no.

## 12.2.3 Accesso remoto HTTPS

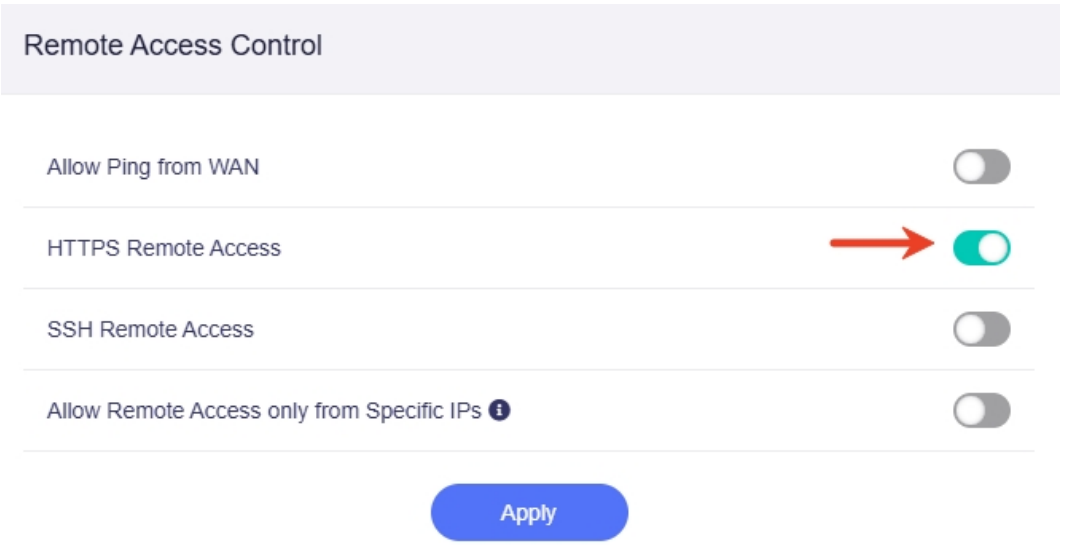
**Per l'accesso remoto HTTPS è richiesto un indirizzo IP pubblico**. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 443**) sul router upstream per l'accesso HTTPS.

Segui i passaggi seguenti per abilitare l'accesso remoto HTTPS per il tuo router.

1. Nella pagina DNS dinamico, attiva **Abilita DDNS**, accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.

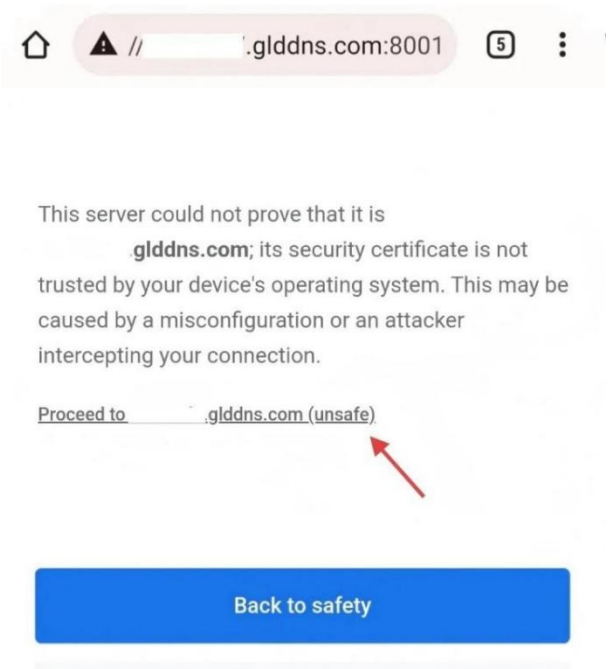



2. Nel pannello di amministrazione web, vai su **SISTEMA** > **Sicurezza** > **Controllo dell'accesso remoto**. Abilita **Accesso remoto HTTPS** e fai clic su **Applica**.



3. Una volta abilitato, puoi accedere al pannello di amministrazione del router da qualsiasi luogo utilizzando il nome host DDNS su HTTPS, ad esempio **https://xxxxxxx.glddns.com**. Se è configurato il port forwarding, accedi come **https://xxxxxxx.glddns.com:external_port** (sostituisci external_port con il numero di porta effettivo).

**Nota**: questa funzione utilizza certificati autofirmati; pertanto, i browser indicheranno "La tua connessione non è privata" quando accedi al pannello di amministrazione del router tramite il nome host DDNS su HTTPS. Per procedere con l'accesso remoto HTTPS, fai clic su **Avanzate** in basso, quindi fai clic su **Procedi a xxxxxxx.glddns.com** per continuare.



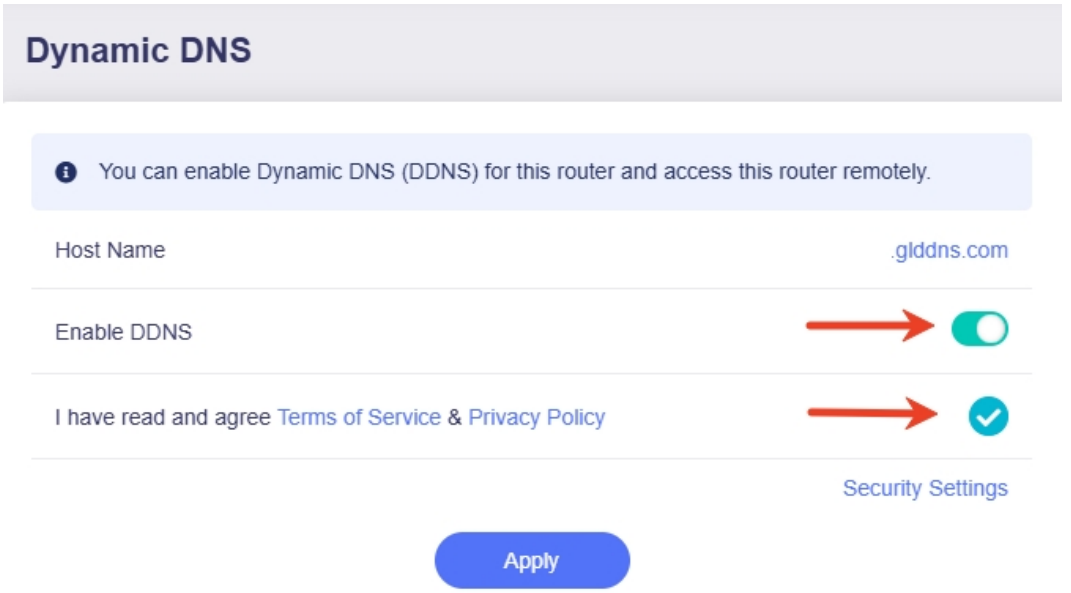

Sarai quindi in grado di accedere al pannello di amministrazione web del router utilizzando il nome host DDNS su **HTTPS**.

## 12.2.4 Accesso remoto SSH

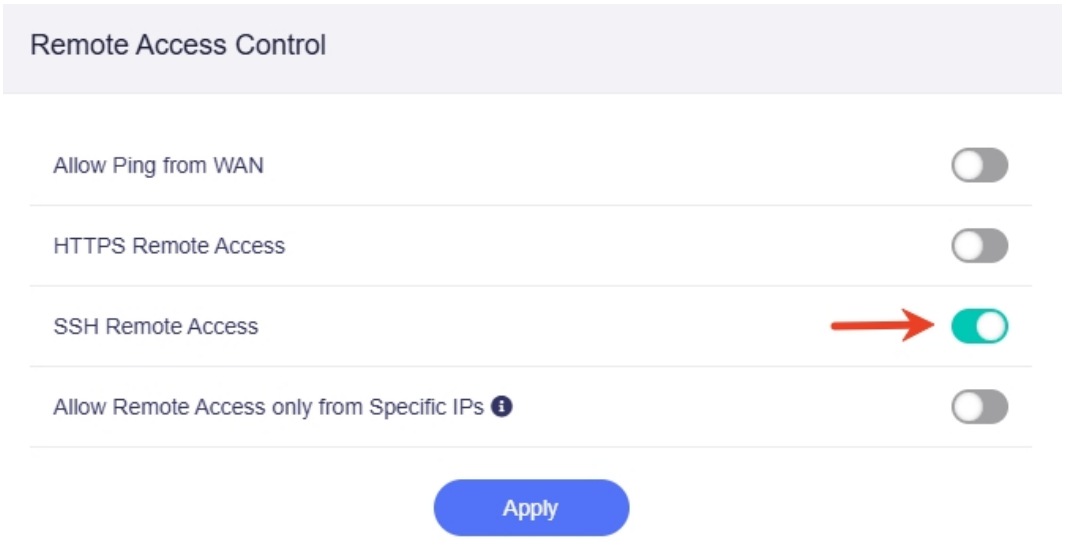
Per l'accesso remoto SSH è richiesto un **indirizzo IP pubblico**. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 22**) sul router upstream per l'accesso remoto SSH.

Segui i passaggi seguenti per abilitare l'accesso remoto SSH per il tuo router.

1. Nella pagina DNS dinamico, attiva **Abilita DDNS**, accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.




2. Nel pannello di amministrazione web, vai su **SISTEMA** > **Sicurezza** > **Controllo dell'accesso remoto**. Abilita **Accesso remoto SSH** e fai clic su **Applica**.



Una volta abilitato, puoi accedere al pannello di amministrazione del router da qualsiasi luogo utilizzando il nome host DDNS su SSH, ad esempio **ssh root@xxxxxxx.glddns.com**. Se è configurato il port forwarding, accedi come **ssh root@xxxxxxx.glddns.com:external_port** (sostituisci external_port con il numero di porta effettivo).

## 12.3 GoodCloud

GL.iNet GoodCloud è una piattaforma progettata per semplificare l'implementazione e la gestione remota dei dispositivi connessi. Fornisce un modo semplice per accedere e gestire in remoto i router GL.iNet. Centralizzando i dispositivi di rete sul cloud, gli utenti possono eseguire in modo efficiente attività di gestione in blocco, come la distribuzione di configurazioni di rete e l'esecuzione di aggiornamenti software. Possono anche accedere in remoto al pannello di amministrazione web del router o connettersi al terminale del router tramite SSH, ottenendo la gestione dei dispositivi di rete interregionali ed end-to-end.

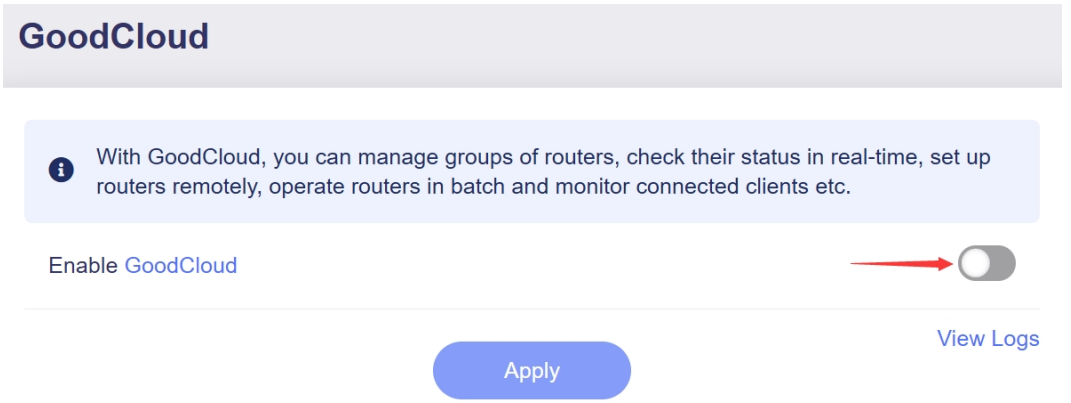
Con GoodCloud puoi:

- Controllare lo stato del router in tempo reale
- Gestire gruppi di router
- Configurare i router da remoto
- Monitorare i client connessi
- Gestire più router contemporaneamente
- Stabilire una connessione site-to-site

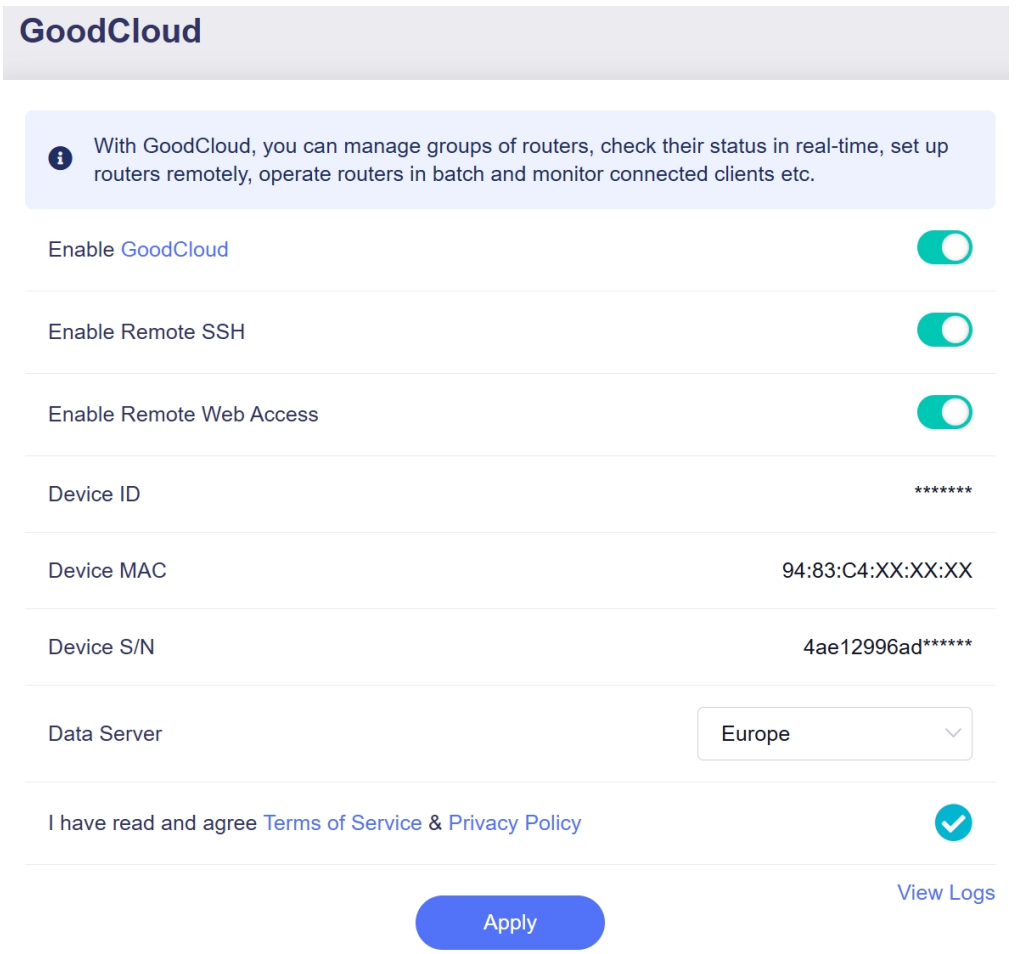
Alcune funzionalità sono disponibili nel piano Enterprise e nel piano VAR (rivenditore a valore aggiunto). Vedi qui per i dettagli.

## 12.3.1 Attivazione di GoodCloud

1. Accedi al pannello di amministrazione web del tuo router e vai su **APPLICAZIONI** > **GoodCloud**. Attiva l'interruttore per abilitare GoodCloud.

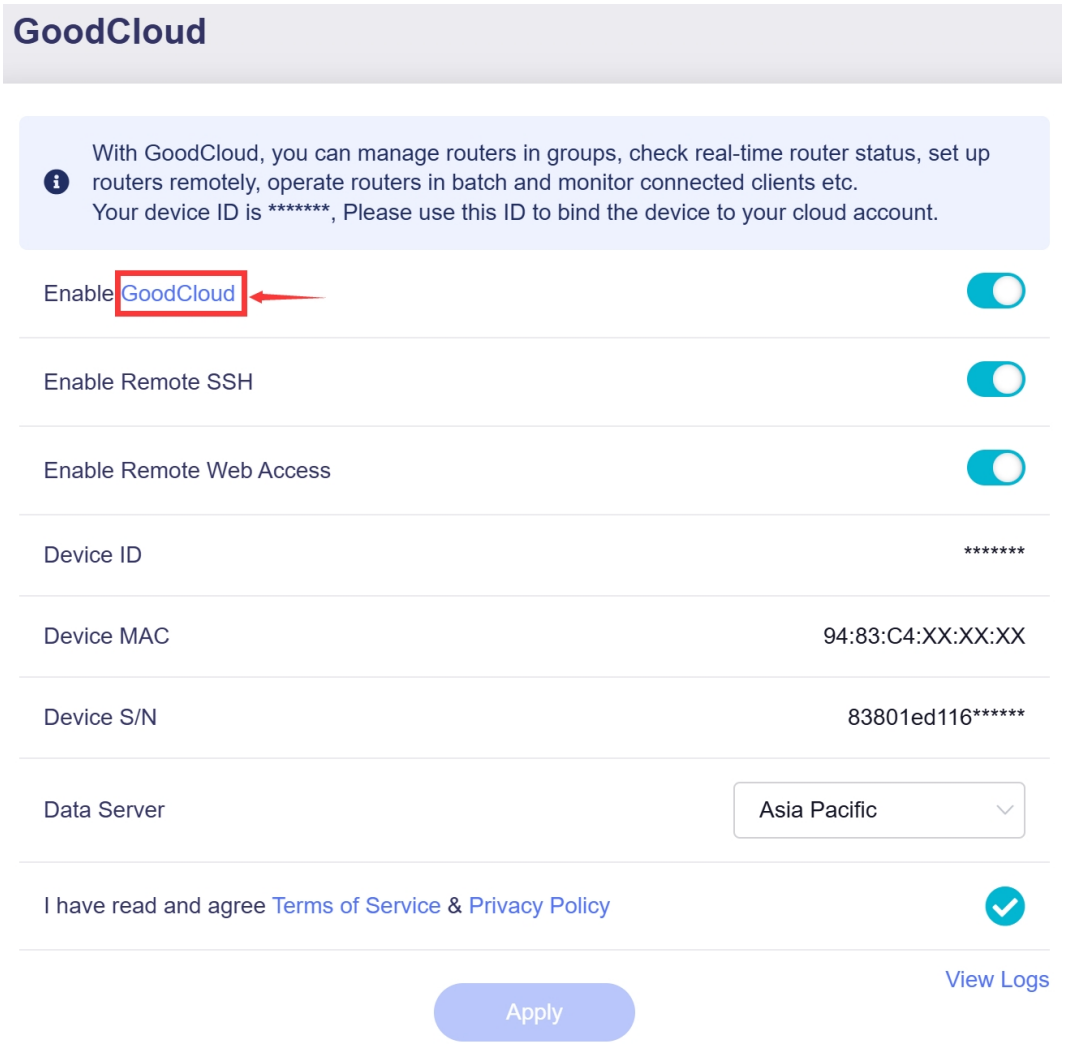


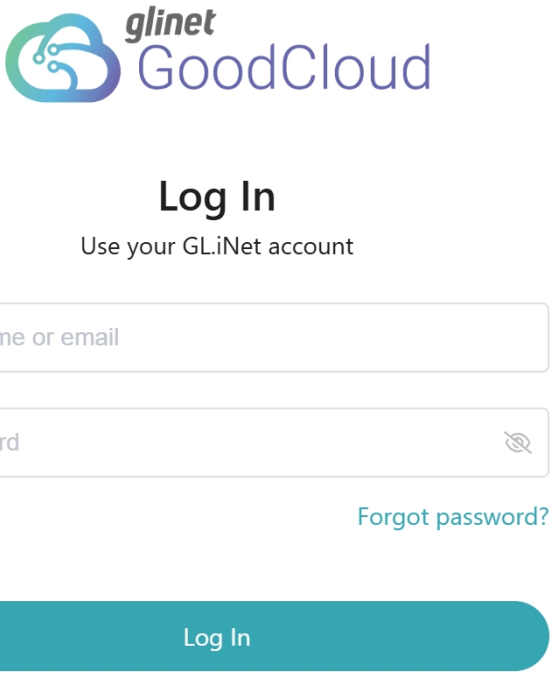

Abilita **SSH remoto** e **Accesso web remoto** se necessario, seleziona il server più vicino, leggi e accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.



- SSH remoto: per accedere in remoto al terminale del router tramite SSH dalla piattaforma GoodCloud.
- Accesso web remoto: per accedere in remoto al pannello di amministrazione web del router tramite HTTP/HTTPS dalla piattaforma GoodCloud.
- Server dati: scegli il server più vicino alla posizione del tuo dispositivo. Sono disponibili tre opzioni: Asia Pacifico (Giappone), America (Oregon) ed Europa (Irlanda).
- **Visualizza registri**: reindirizza alla pagina Registro e visualizza il registro Cloud.

2. Fai clic su GoodCloud per andare alla pagina di accesso e accedi con il tuo account GL.iNet Cloud. Se non disponi di un account, creane uno ed effettua l'accesso. Una volta effettuato l'accesso, il router verrà associato automaticamente al tuo account.

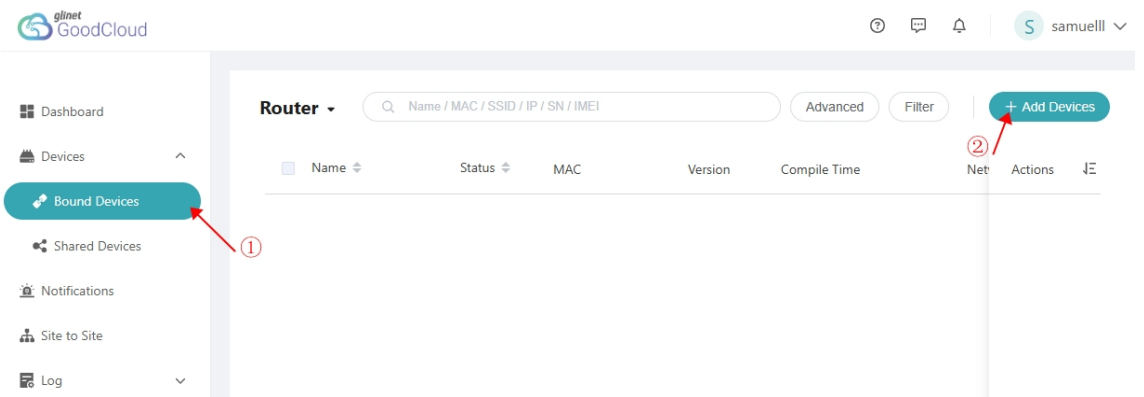





**Suggerimenti**:

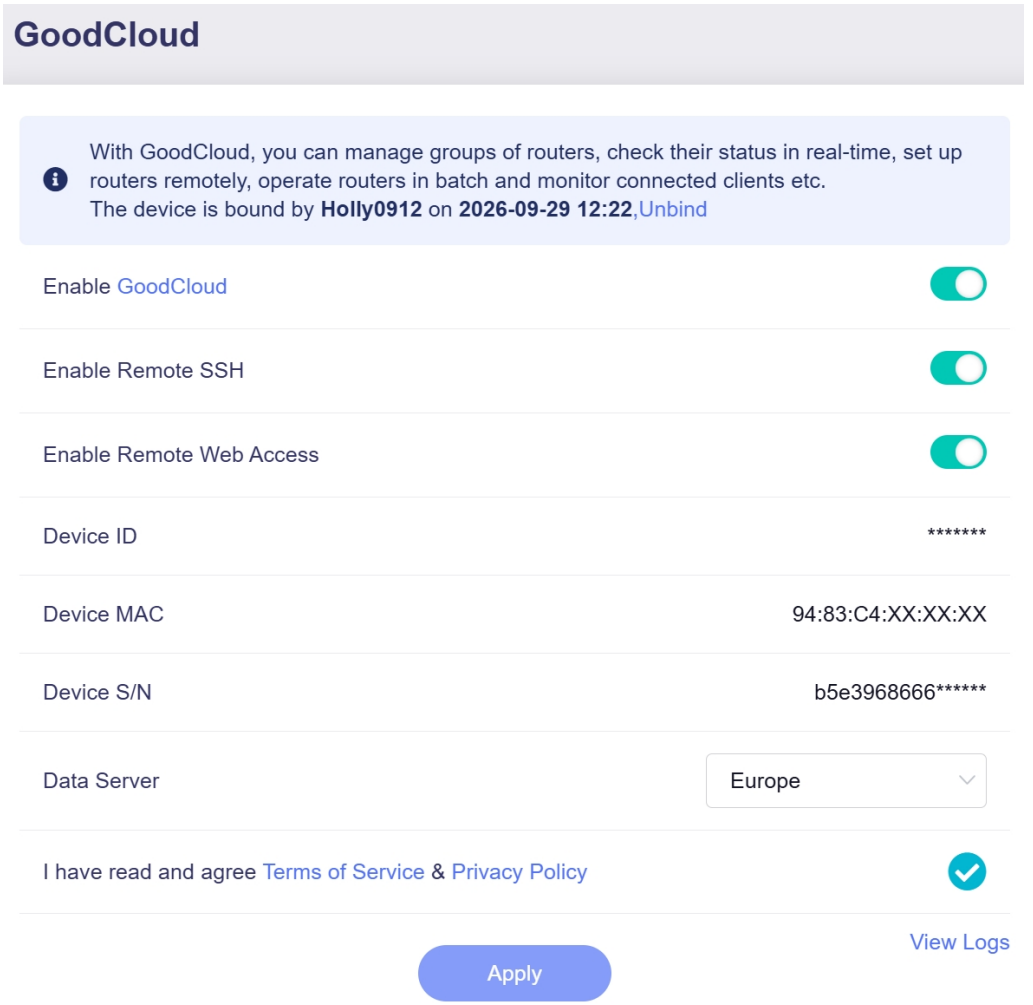
- I passaggi di associazione di GoodCloud differiscono in base alla versione del firmware.
- Se non ricevi l'e-mail di verifica, controlla la cartella spam o riprova più tardi. Per ulteriore assistenza, contattaci all'indirizzo support@gl-inet.com.

3. Sulla piattaforma cloud, vai a **Dispositivi > Dispositivi associati** > **Aggiungi dispositivi**.




Esistono tre metodi per associare il dispositivo al tuo account GoodCloud: rilevamento automatico, aggiunta manuale e importazione in blocco. Fai clic qui per maggiori dettagli.

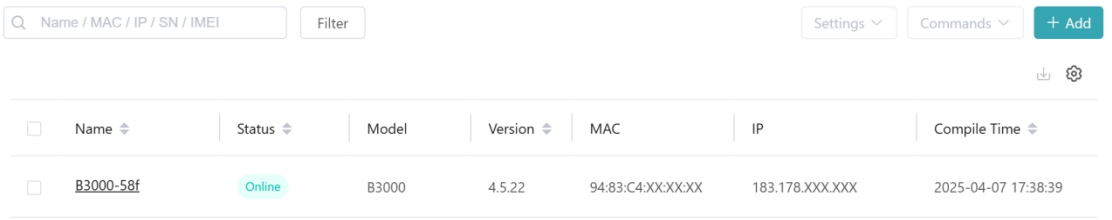
4. Dopo aver eseguito correttamente l'associazione, torna al pannello di amministrazione web del router e vai a **APPLICAZIONI** > **GoodCloud**. Questa pagina mostra i dettagli di associazione, inclusi nome utente e tempo di associazione.



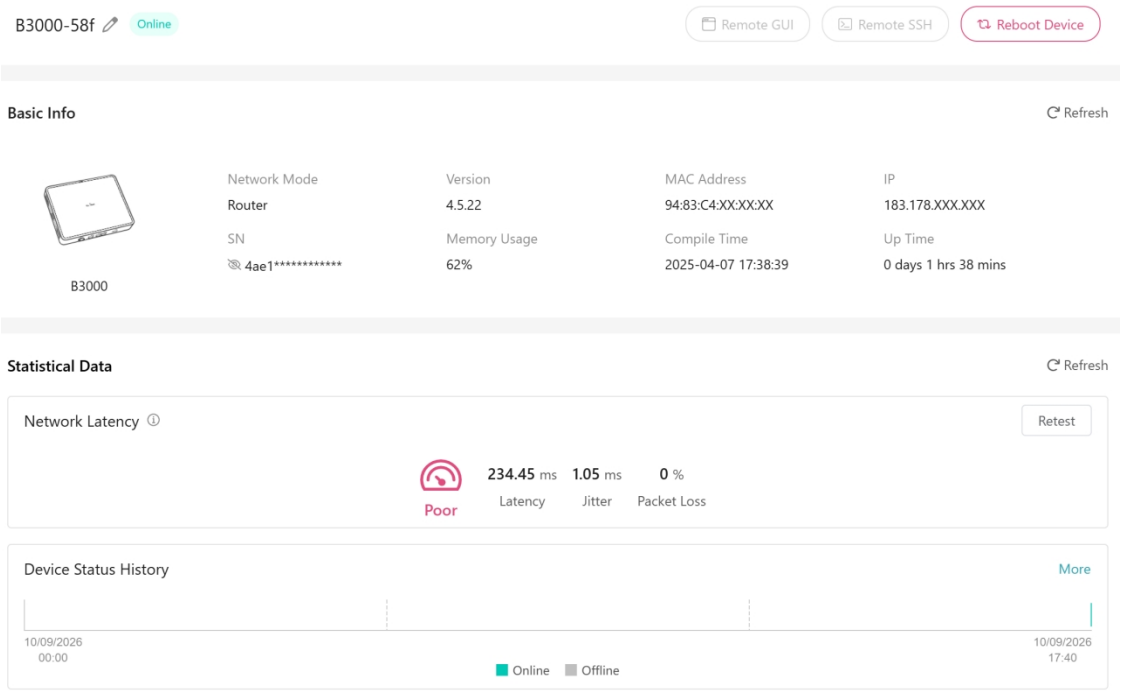
## 12.3.2 Gestione del router

### Controlla i dettagli del dispositivo

Accedi alla piattaforma GoodCloud e vai a **Dispositivi > Dispositivi associati**. **Puoi** visualizzare le informazioni di base del dispositivo, come nome host, stato (online/offline), modello, versione firmware e indirizzo MAC.

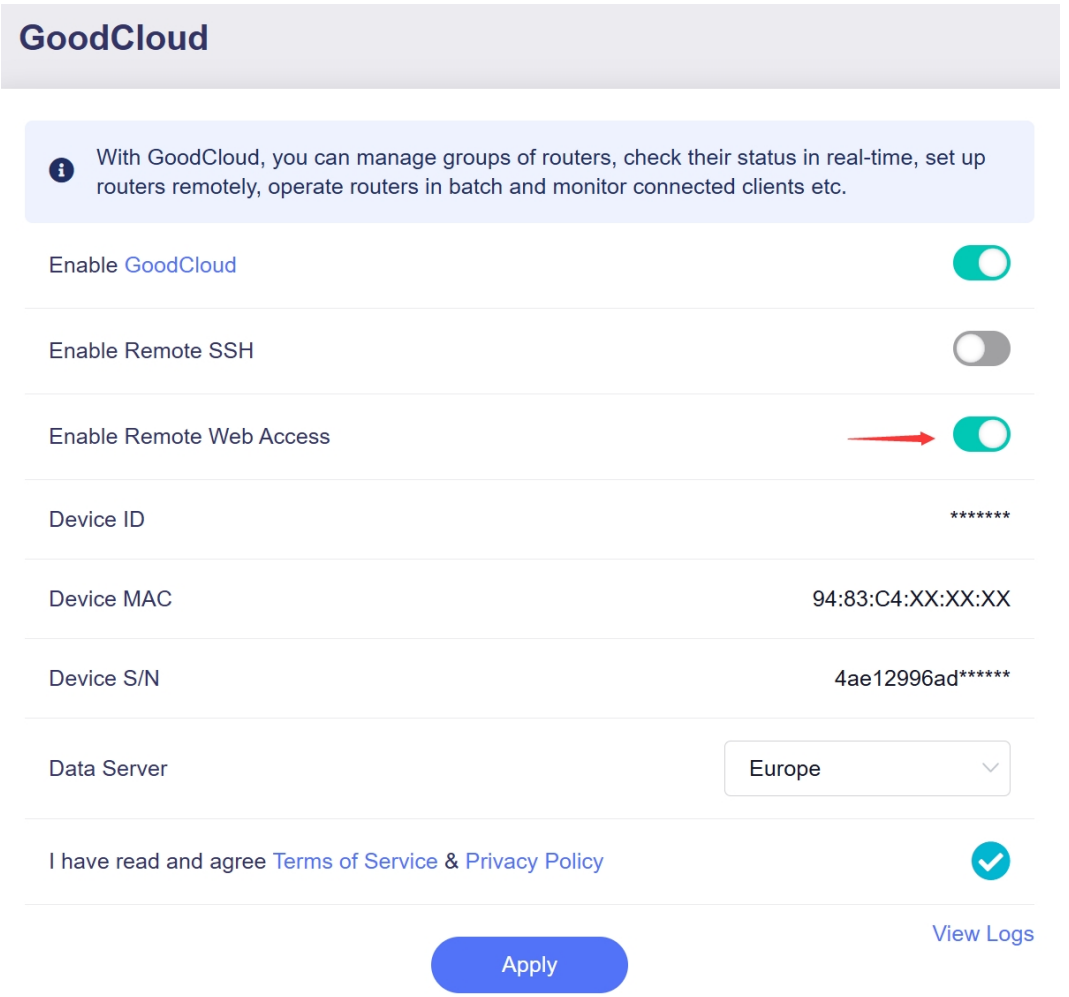



Fare clic sul nome del dispositivo per accedere alla pagina dei dettagli del dispositivo, che visualizza informazioni di base, dati statistici, panoramica della rete, elenco client e sequenza temporale. Puoi anche eseguire operazioni avanzate, come l'accesso remoto al router e il riavvio del dispositivo.

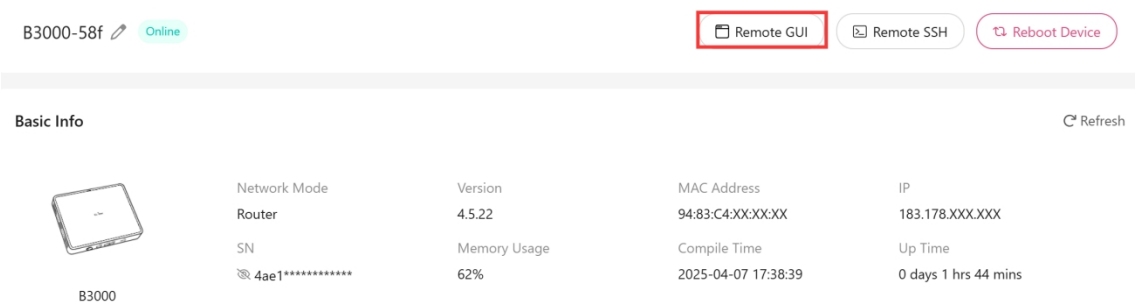


## Accesso web remoto

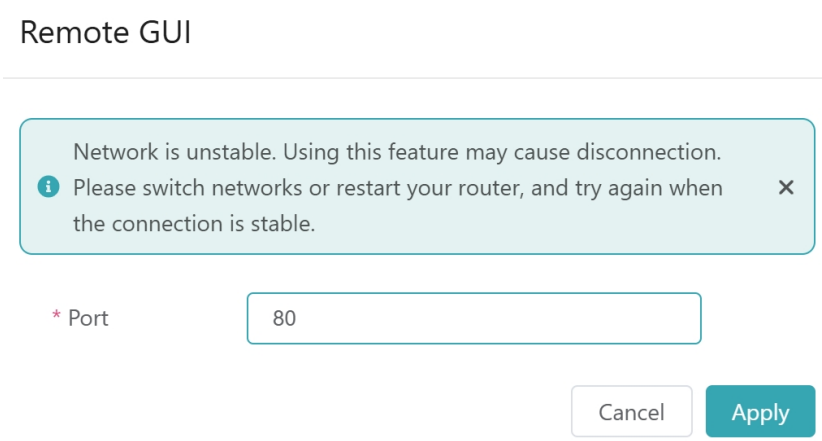
1. Accedi al pannello di amministrazione web del router, vai su **APPLICAZIONI** > **GoodCloud**, abilita **Accesso web remoto**, quindi fai clic su **Applica**.



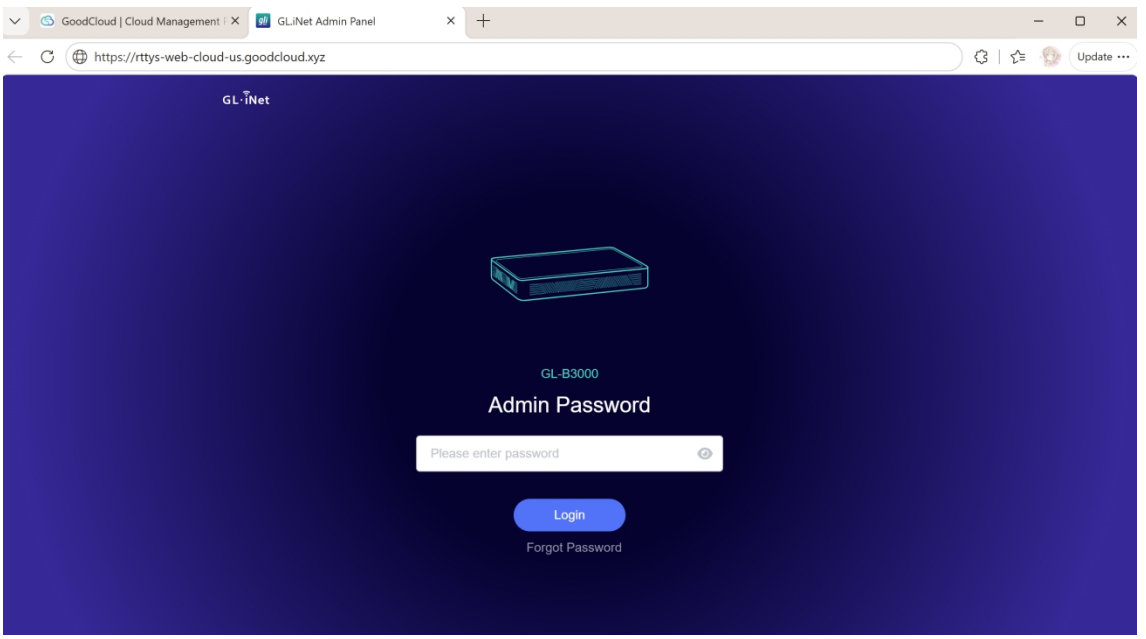

2. Accedi alla piattaforma GoodCloud e vai a **Dispositivi > Dispositivi associati**. Fai clic sul dispositivo a cui desideri accedere e accederai alla pagina dei dettagli del dispositivo.
3. Nella pagina dei dettagli del dispositivo, fai clic sul pulsante **GUI remota** nell'angolo in alto a destra.



4. Seleziona il protocollo di trasferimento e la porta. Le impostazioni predefinite sono **HTTP** e Porta **80**. Se necessario, è possibile cambiare il protocollo in HTTPS e la porta cambierà automaticamente in 443. Quindi fare clic su **Applica**.

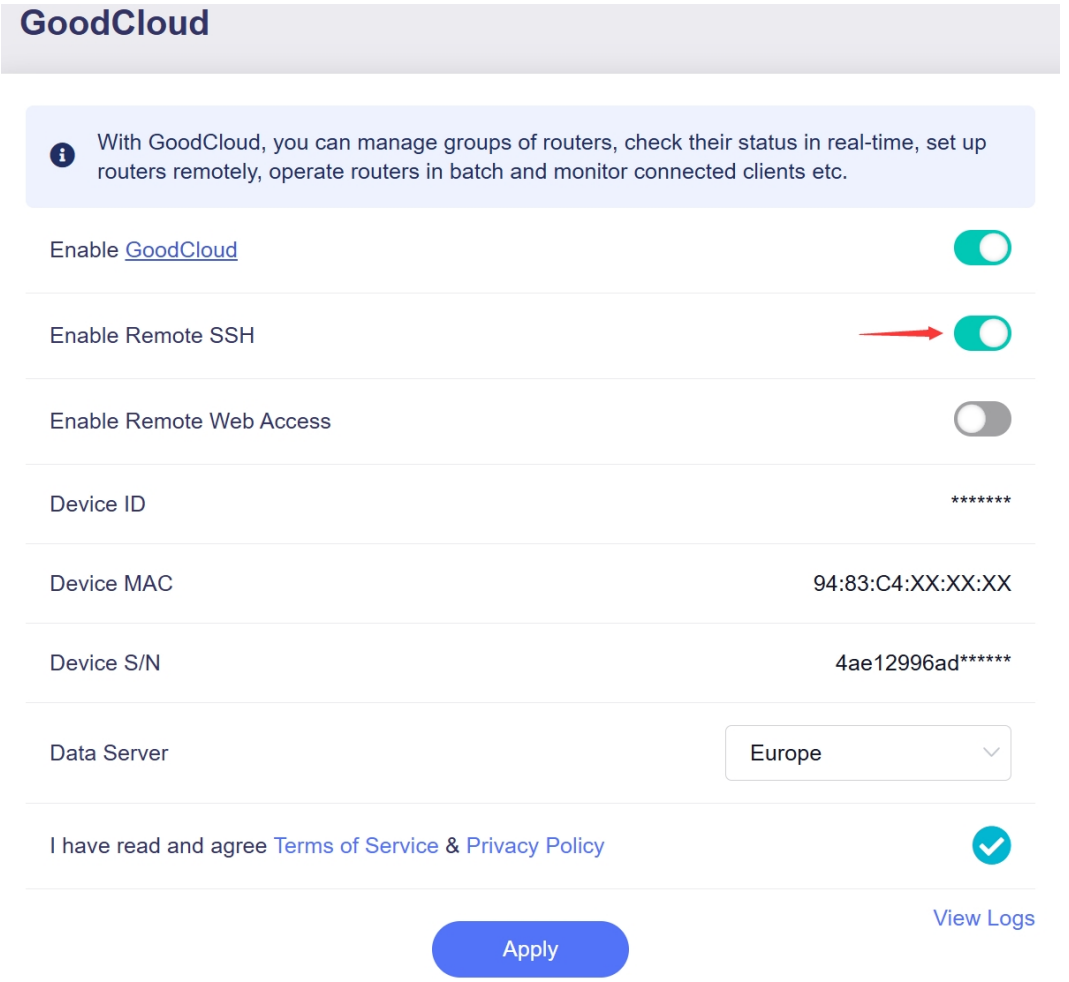



5. Verrai reindirizzato alla pagina di accesso del router. Inserisci la password dell'amministratore per accedere da remoto al pannello di amministrazione web del router.

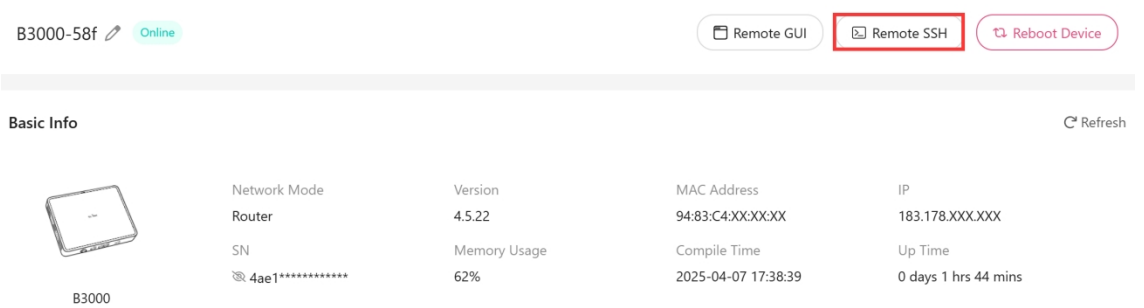


## SSH remoto

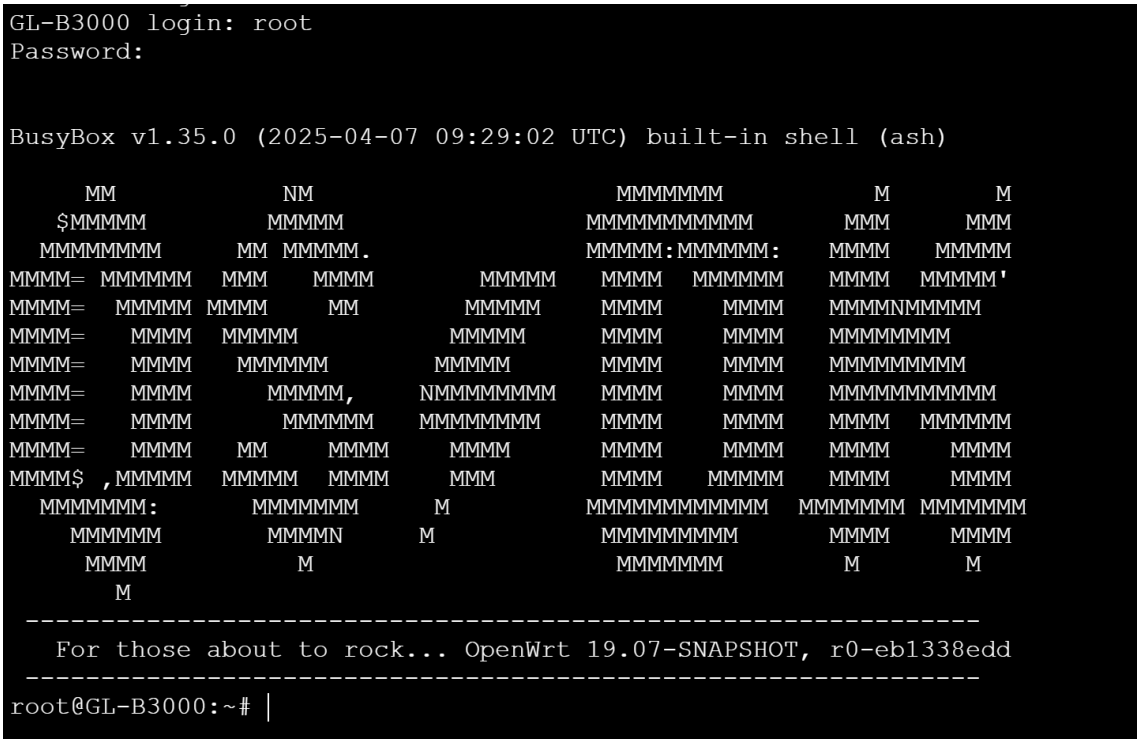
1. Accedi al pannello di amministrazione web del router, vai su **APPLICAZIONI** > **GoodCloud**, abilita **SSH remoto**, quindi fai clic su **Applica**.




2. Accedi alla piattaforma GoodCloud e vai a **Dispositivi > Dispositivi associati**. Fai clic sul dispositivo a cui desideri accedere e accederai alla pagina dei dettagli del dispositivo.
3. Nella pagina dei dettagli del dispositivo, fai clic sul pulsante **SSH remoto** nell'angolo in alto a destra.

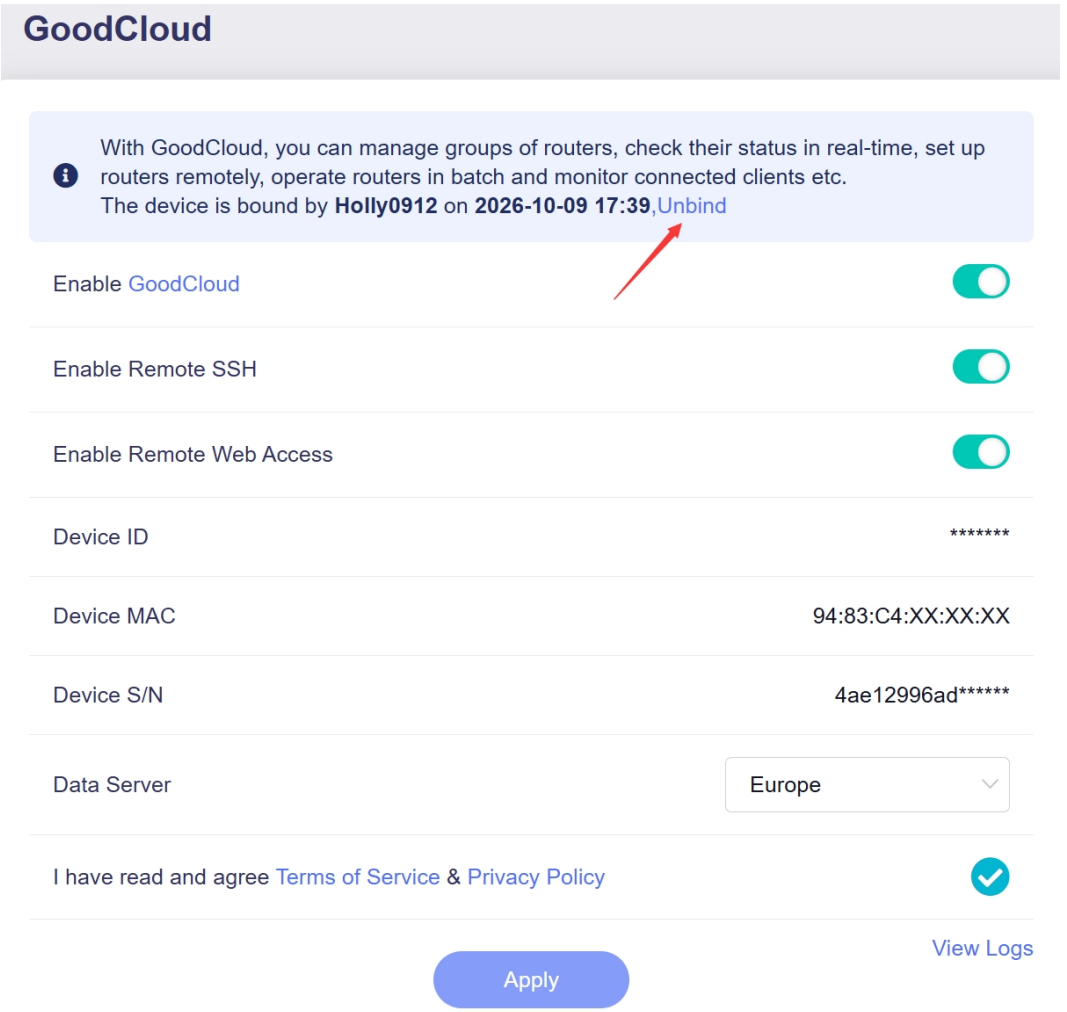


4. Registro come **root** e inserisci la password per accedere al terminale del tuo router.

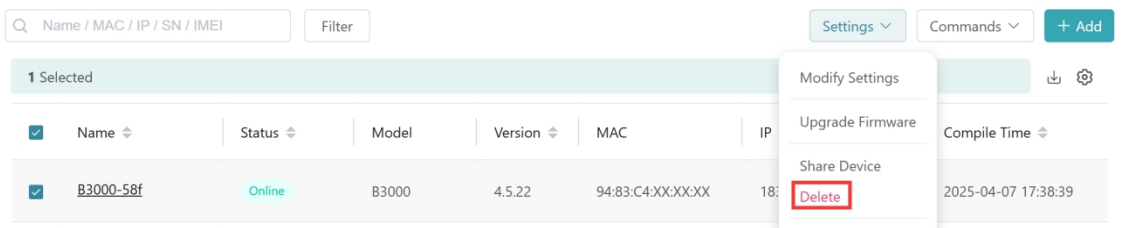


## 12.3.3 Dissociazione del dispositivo

Nel pannello di amministrazione web del router, fai clic su **Dissocia**. Il tuo dispositivo verrà quindi scollegato dal tuo account GoodCloud.




In alternativa, accedi alla piattaforma cloud e vai a **Dispositivi > Dispositivi associati**. Seleziona il dispositivo che desideri scollegare, fai clic su **Impostazioni** nell'angolo in alto a destra, quindi seleziona **Elimina**. Il tuo dispositivo verrà quindi scollegato dal tuo account GoodCloud.

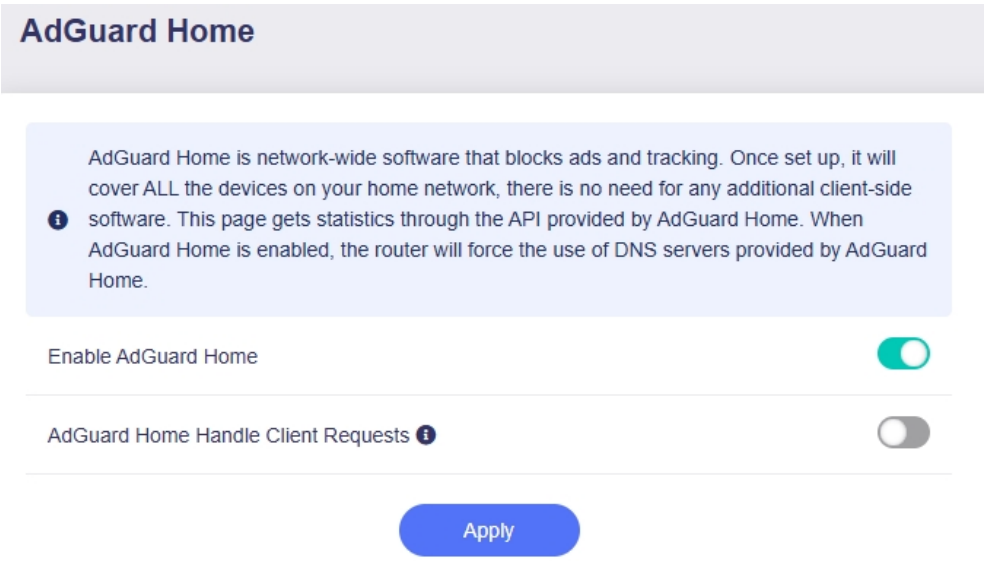


## 12.4 AdGuard Home

AdGuard Home è un software di blocco degli annunci pubblicitari e di prevenzione del tracciamento a livello di rete. Una volta configurato, coprirà tutti i dispositivi client senza la necessità di software aggiuntivo sul lato client.

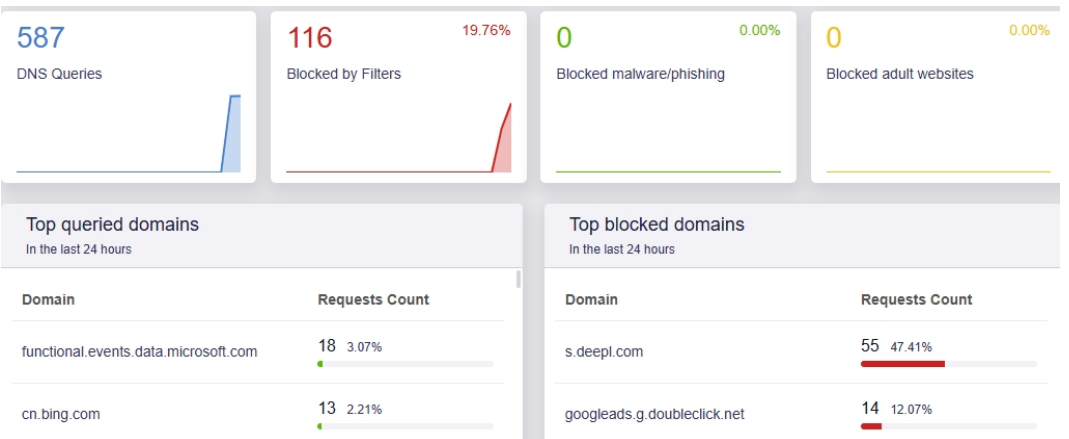
Segui questi passaggi per configurare AdGuard Home.

1. Accedi al pannello di amministrazione web del router, vai su **APPLICAZIONI** > **AdGuard Home**. Attiva **Abilita AdGuard Home** e fai clic su **Applica**.

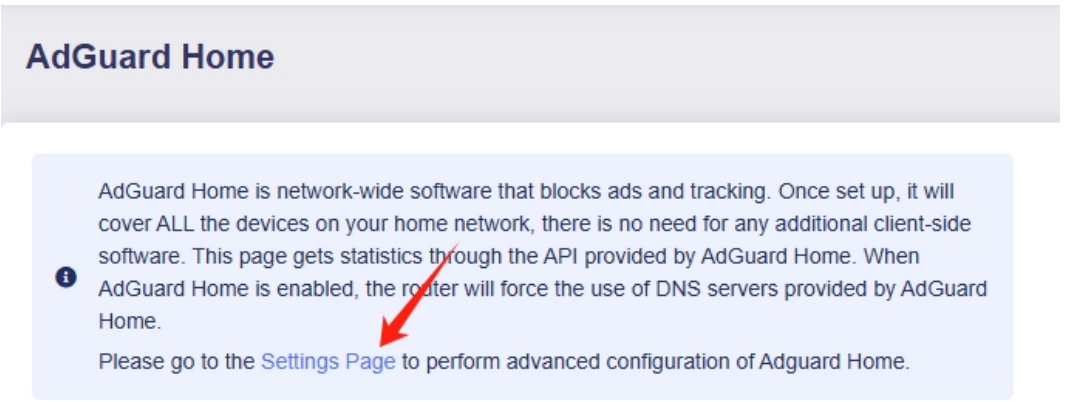



   - **AdGuard Home gestisce le richieste dei client**: se abilitato, le query DNS dai dispositivi client verranno gestite direttamente da AdGuard Home, ma ciò causerà il fallimento delle policy VPN basate sui domini.

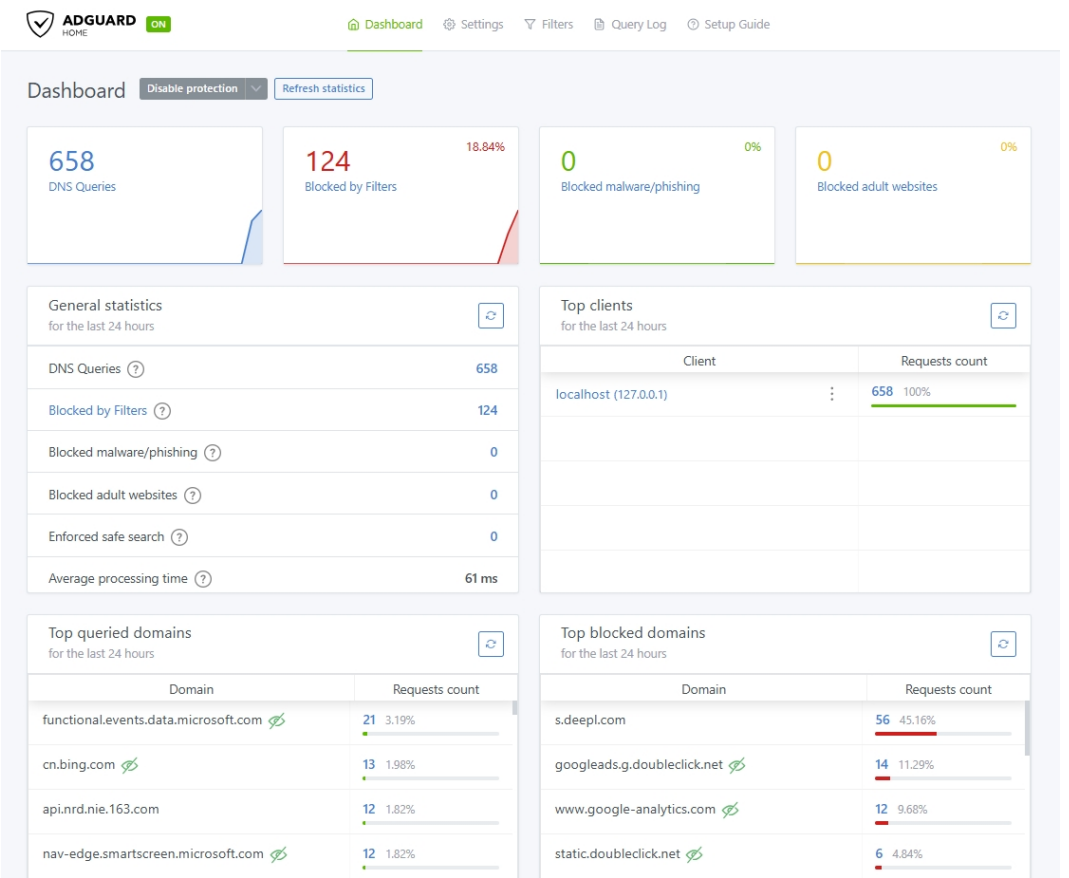
2. La pagina caricherà automaticamente le statistiche DNS (query, domini bloccati, ecc.) tramite l'API fornita da AdGuard Home.



3. Fai clic sulla **pagina Impostazioni** per configurare le impostazioni avanzate per AdGuard Home.




4. Verrai reindirizzato alla pagina delle impostazioni di AdGuard Home. Per assistenza, visitare il Centro assistenza AdGuard Home.



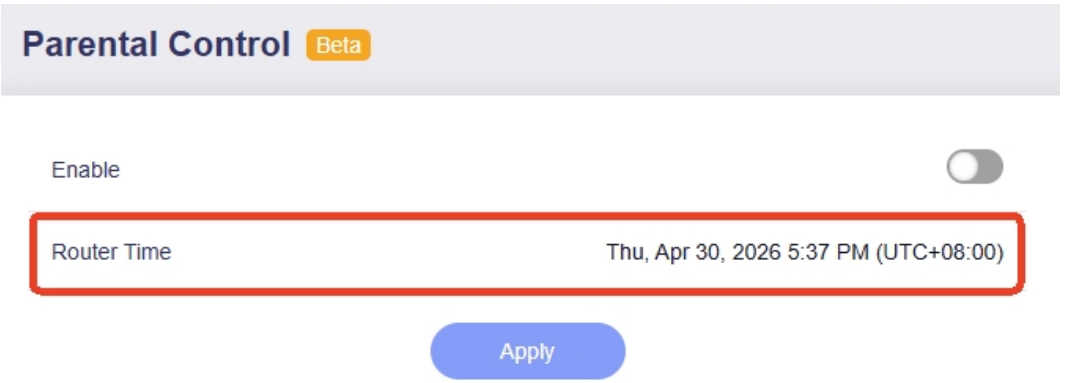
## 12.5 Controllo parentale

Il controllo parentale è un modo per garantire la sicurezza dei bambini online bloccando i siti Web inappropriati e limitando il tempo di utilizzo dei dispositivi. Aiuta a prevenire l'accesso a contenuti dannosi, a gestire il tempo di utilizzo e a garantire che i bambini utilizzino Internet in modo responsabile.

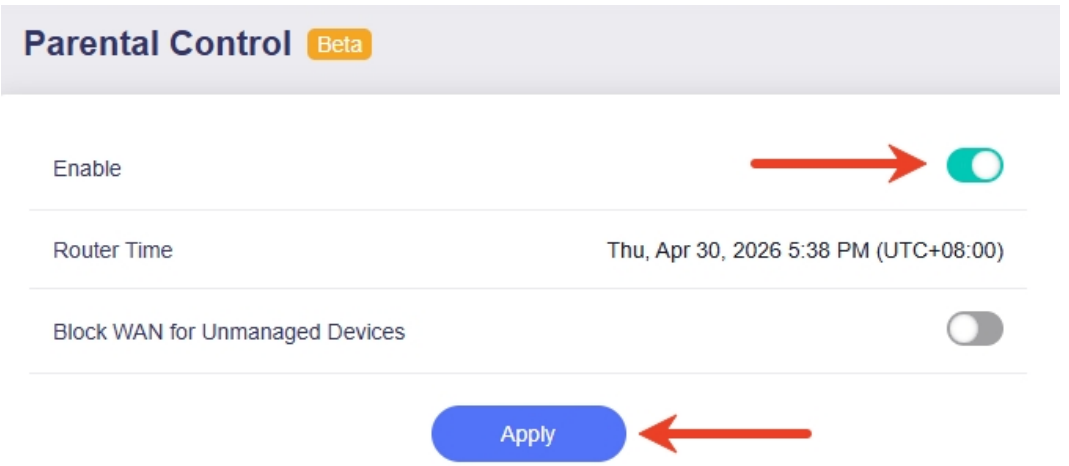
### 12.5.1 Configurazione rapida

Segui questi passaggi per configurare Controllo parentale sui router GL.iNet.

1. Accedi al pannello di amministrazione web del router e vai su **APPLICAZIONI** > **Controllo parentale.** Assicurarsi che l'orario del router sia accurato. In caso contrario, vai su **SISTEMA** > **Fuso orario** per sincronizzarlo prima.




2. Abilita Controllo parentale e fai clic su **Applica**. Quindi seguire la procedura guidata di configurazione per configurare Controllo parentale. Puoi anche guardare il video di configurazione qui.



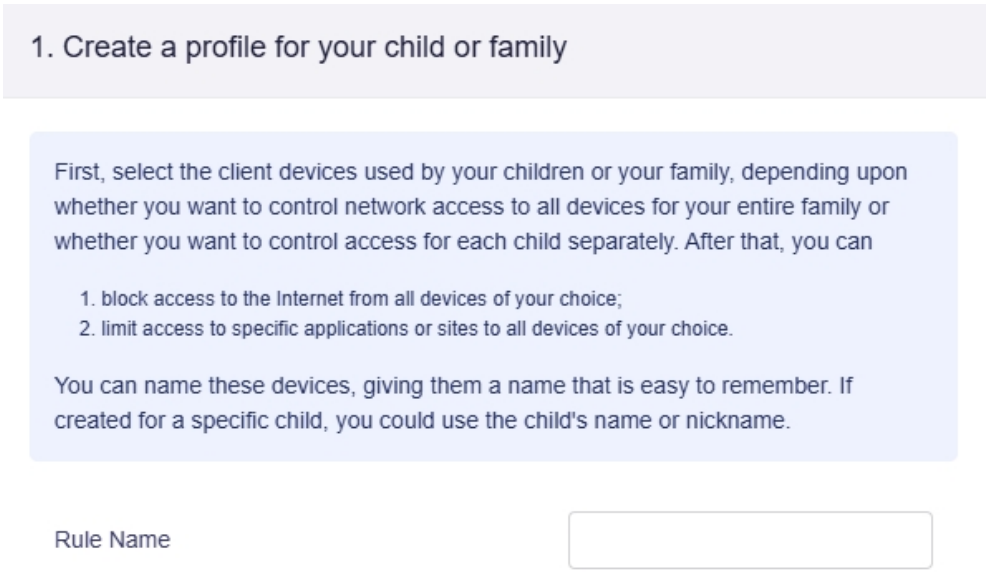
- **Blocca WAN per dispositivi non gestiti**: blocca l'accesso a Internet per tutti i dispositivi che non sono presenti nell'elenco Controllo parentale.

Ecco un caso d'uso come riferimento.

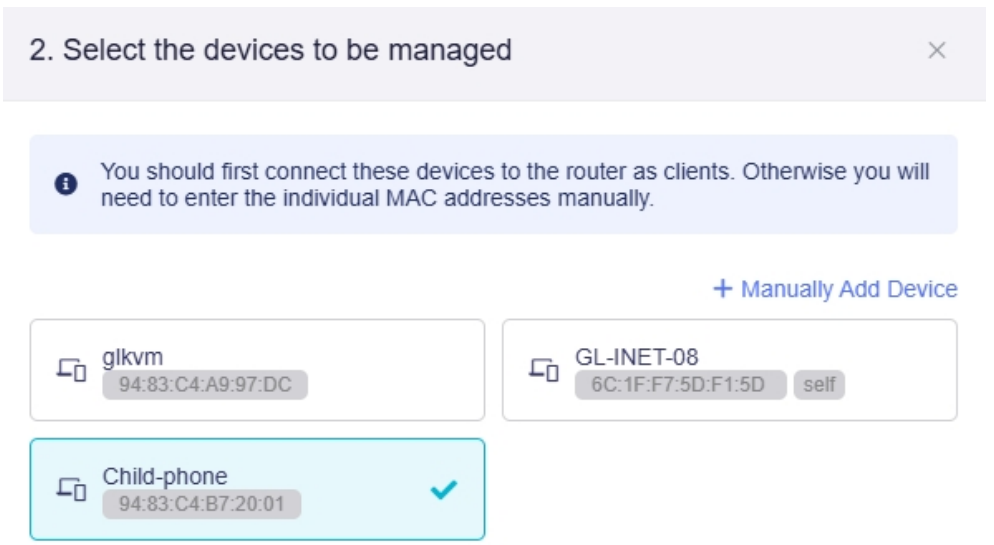
**Scenario:** i dispositivi in questo profilo possono accedere a Internet solo per studiare da 8 AM a 11 AM nei giorni feriali e per giocare da 6 PM a 8 PM nei fine settimana. L'accesso a Internet è bloccato per impostazione predefinita in tutti gli altri momenti.

**Procedura di configurazione:**

1. Crea un profilo e personalizza un nome.

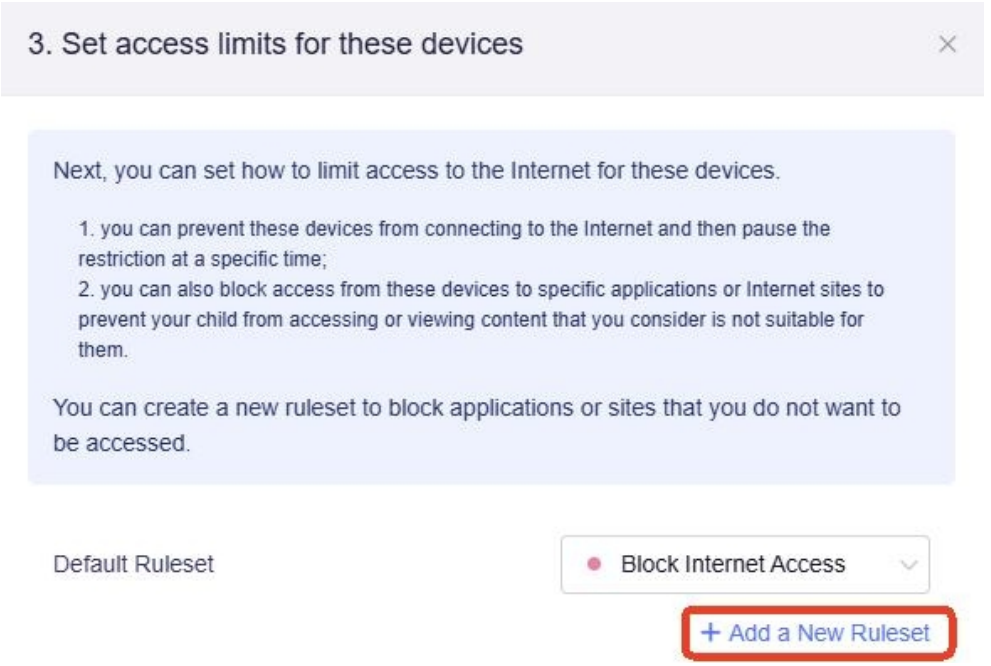



2. Seleziona i dispositivi che desideri gestire. Collegali prima al router. Se non sono stati collegati al router, aggiungili manualmente inserendo i loro indirizzi MAC.

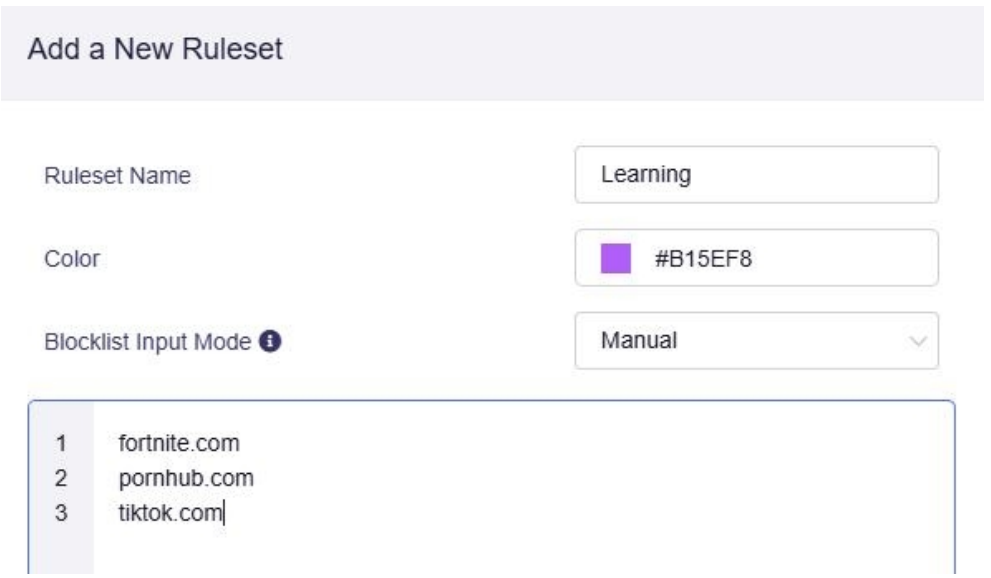


3. Imposta limite di accesso.

   Esistono due set di regole predefinite: **Blocca l'accesso a Internet** e **Nessun limite**. Fai clic su **Aggiungi un nuovo set di regole** per creare altri due set di regole da utilizzare in seguito: **Apprendimento** e **Gioco**.

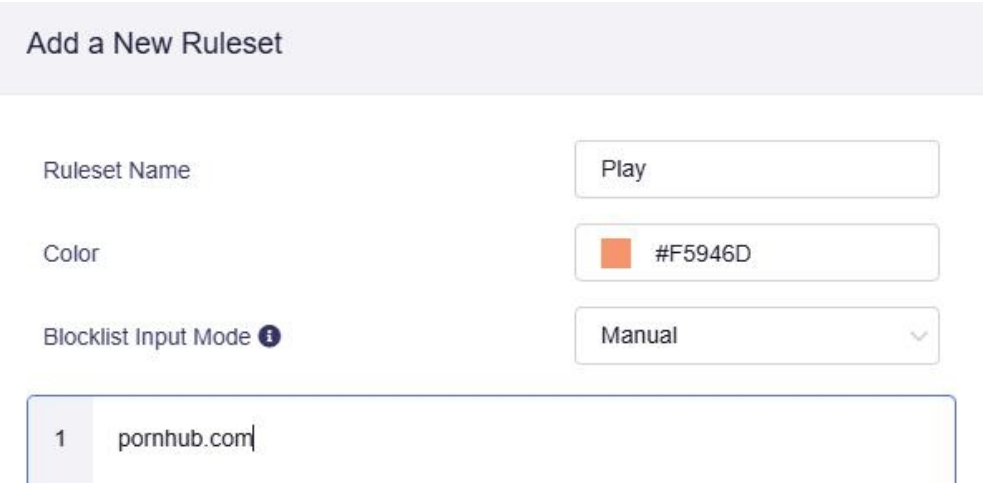



   Specifica il nome del set di regole (ad esempio, Apprendimento) e il colore, inserisci i siti Web da bloccare, quindi fai clic su **Applica**.

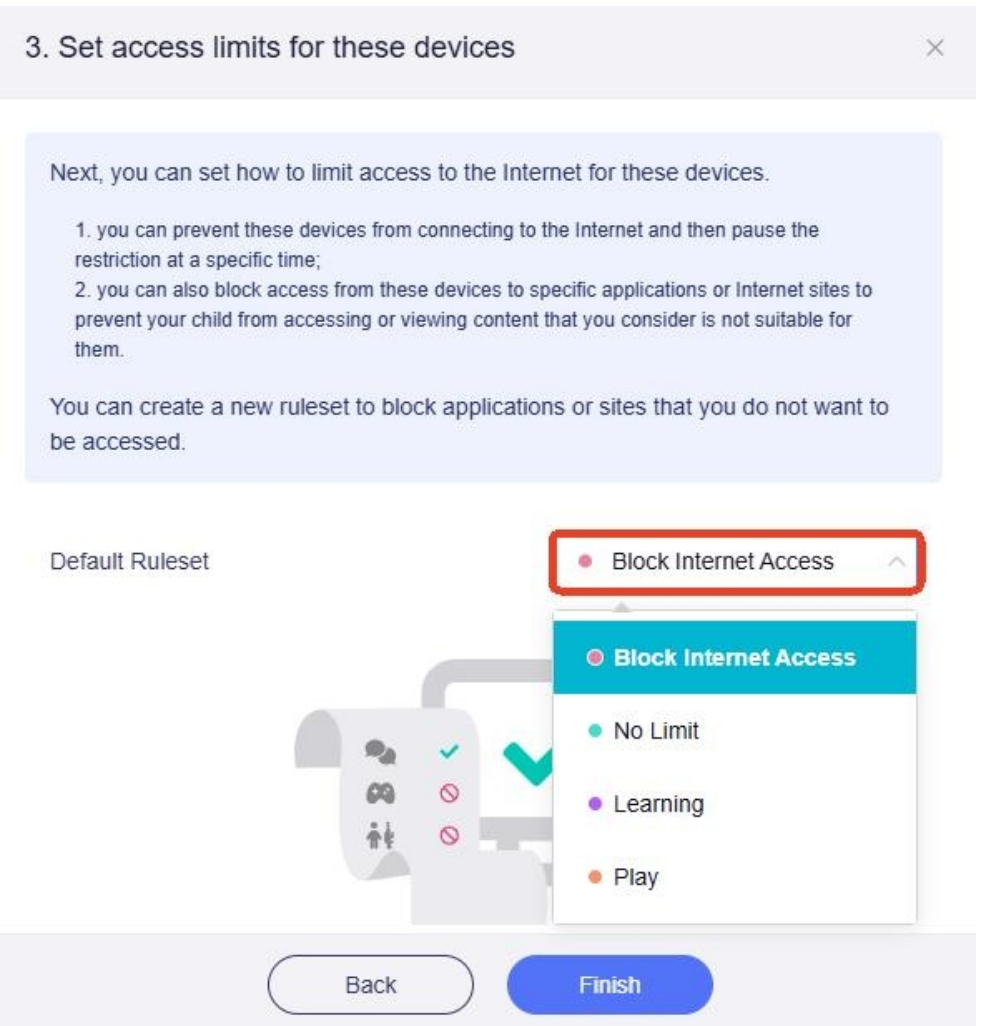



   **Nota**: i nomi di dominio inseriti nella blocklist devono includere i relativi sottodomini. Ad esempio, se viene inserito "esempio.com", include anche qualsiasi sottodominio, come "sottodominio.esempio.com".

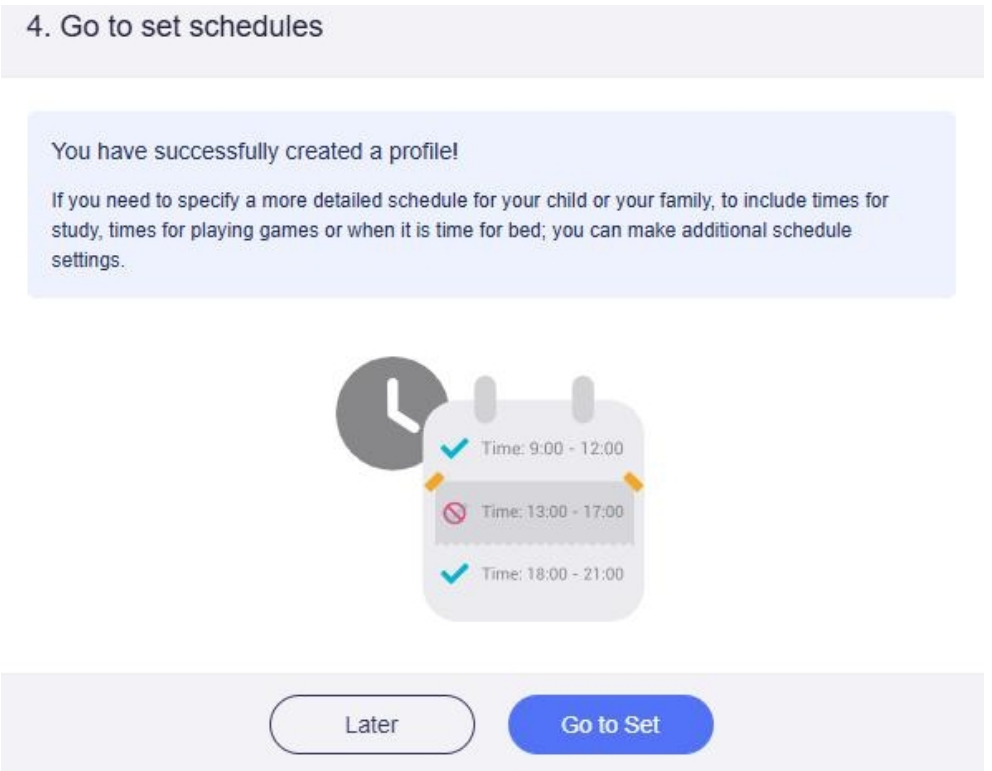
Allo stesso modo, crea un altro set di regole. Specifica il nome del set di regole (ad esempio, Gioco) e il colore, inserisci i siti Web da bloccare, quindi fai clic su **Applica**.



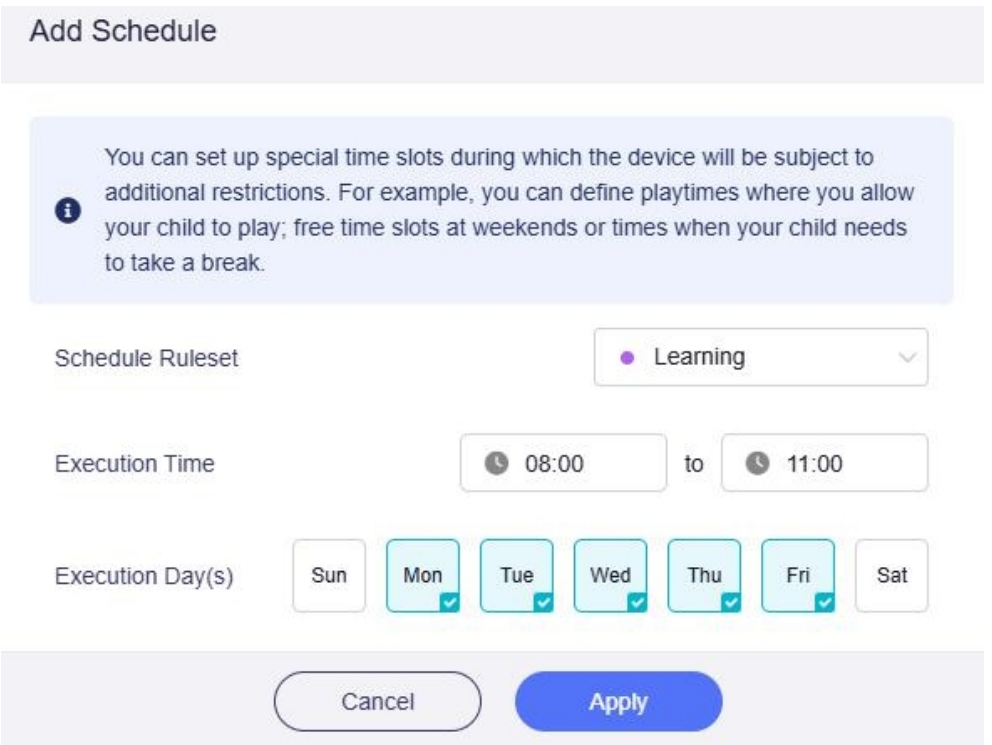

Una volta applicate, ci saranno un totale di quattro set di regole. Seleziona **Blocca l'accesso a Internet** come **set di regole predefinito** e fai clic su **Fine**.



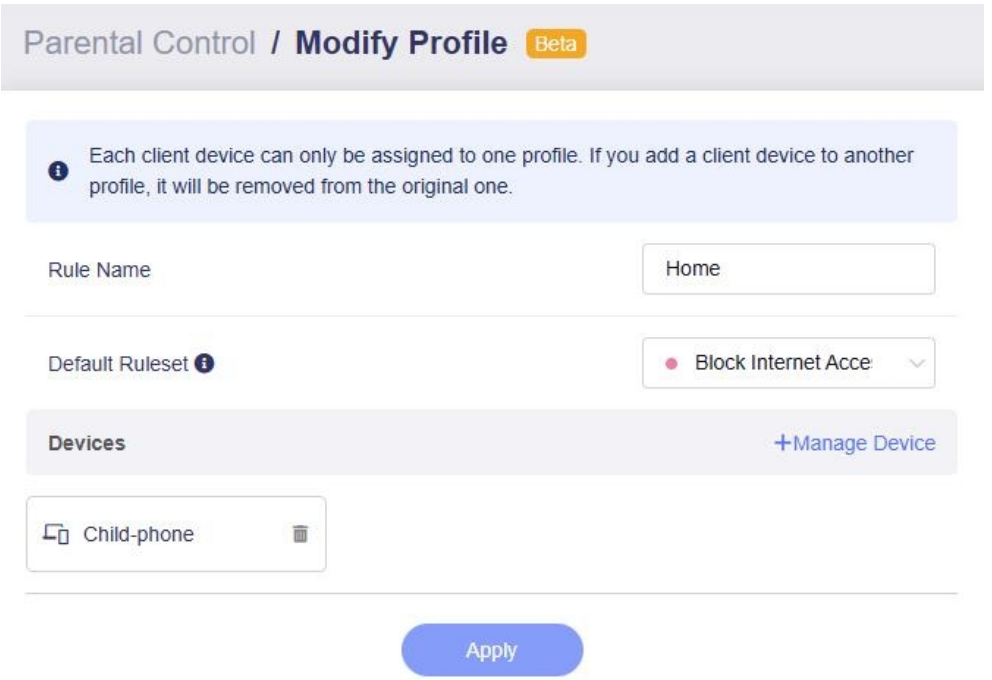
4. Successivamente, imposta la pianificazione per il tuo profilo. Fai clic su **Vai alla configurazione**.



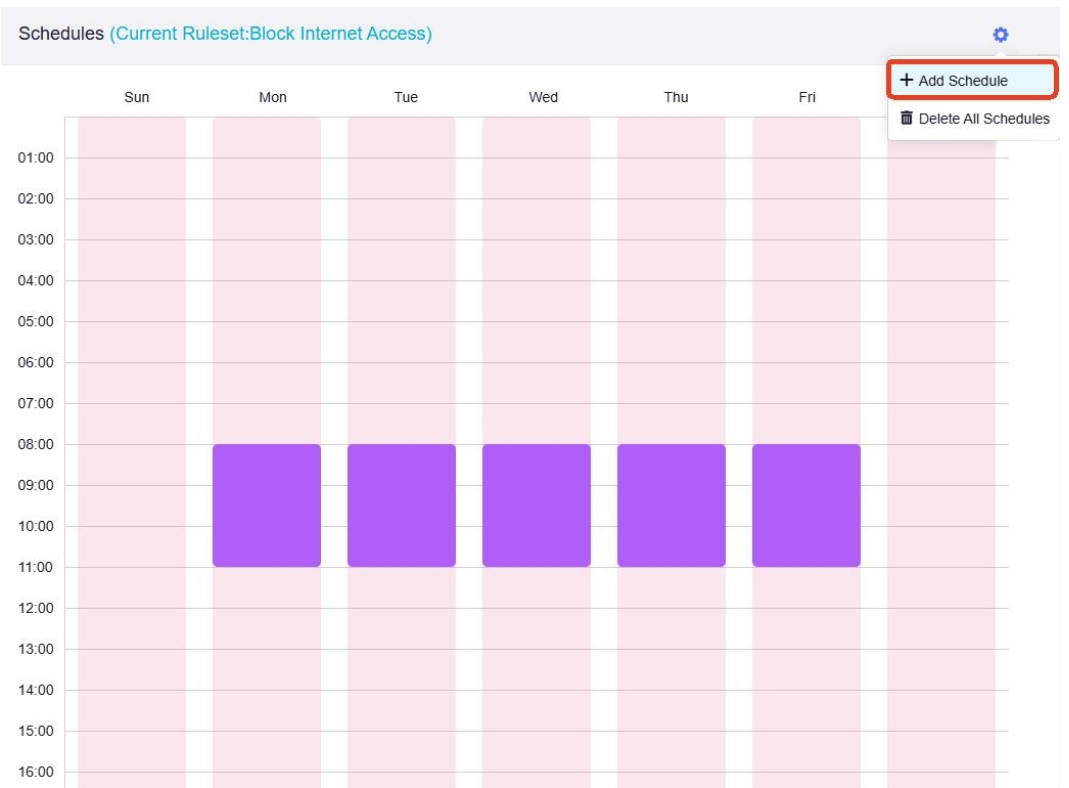

Aggiungi il set di regole di **apprendimento** al programma. Imposta l'**orario di esecuzione** da 8 AM a 11 AM nei giorni feriali, quindi fai clic su **Applica**.



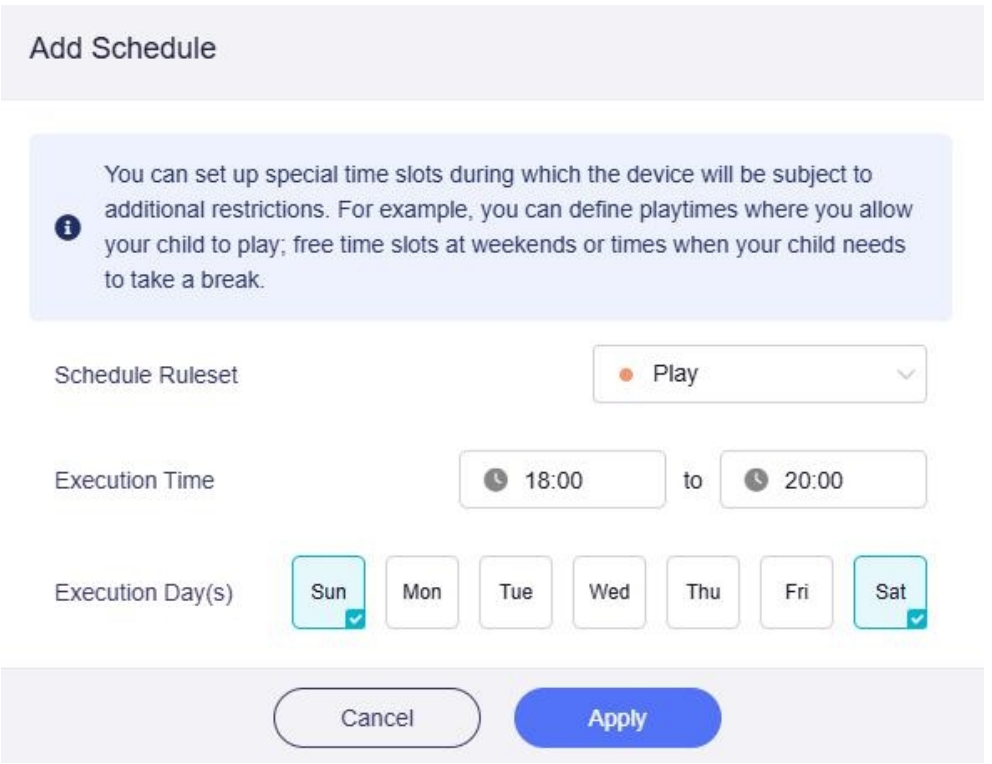
5. Verrai reindirizzato alla pagina di modifica del profilo creato.



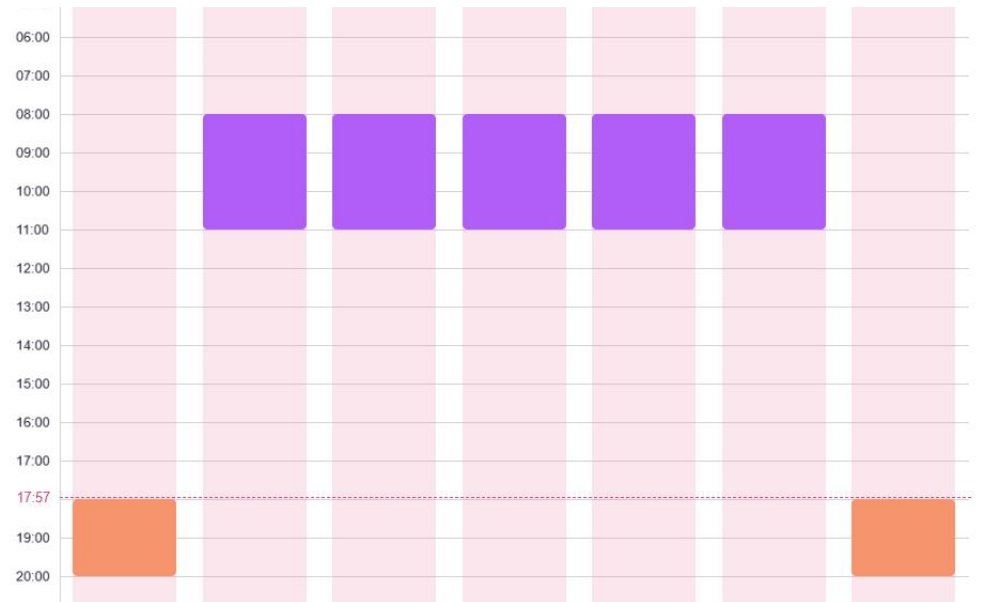

Sposta in fondo e vedrai che è stata creata una pianificazione. Fai clic sull'icona a forma di ingranaggio in alto a destra e seleziona **Aggiungi pianificazione**.



6. Aggiungi un altro set di regole **Gioco** al programma. Imposta l'**orario di esecuzione** da 6 PM a 8 PM nei fine settimana, quindi fai clic su **Applica**.




Le regole di gioco verranno quindi aggiunte al programma.

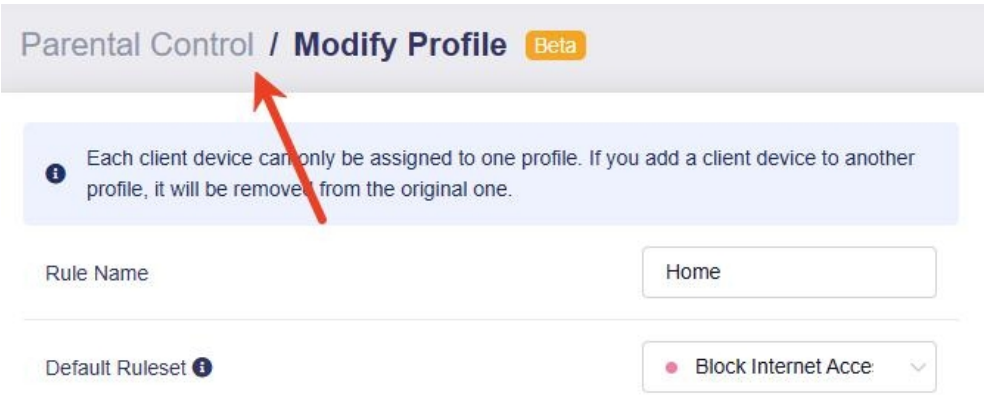



**Suggerimenti**:

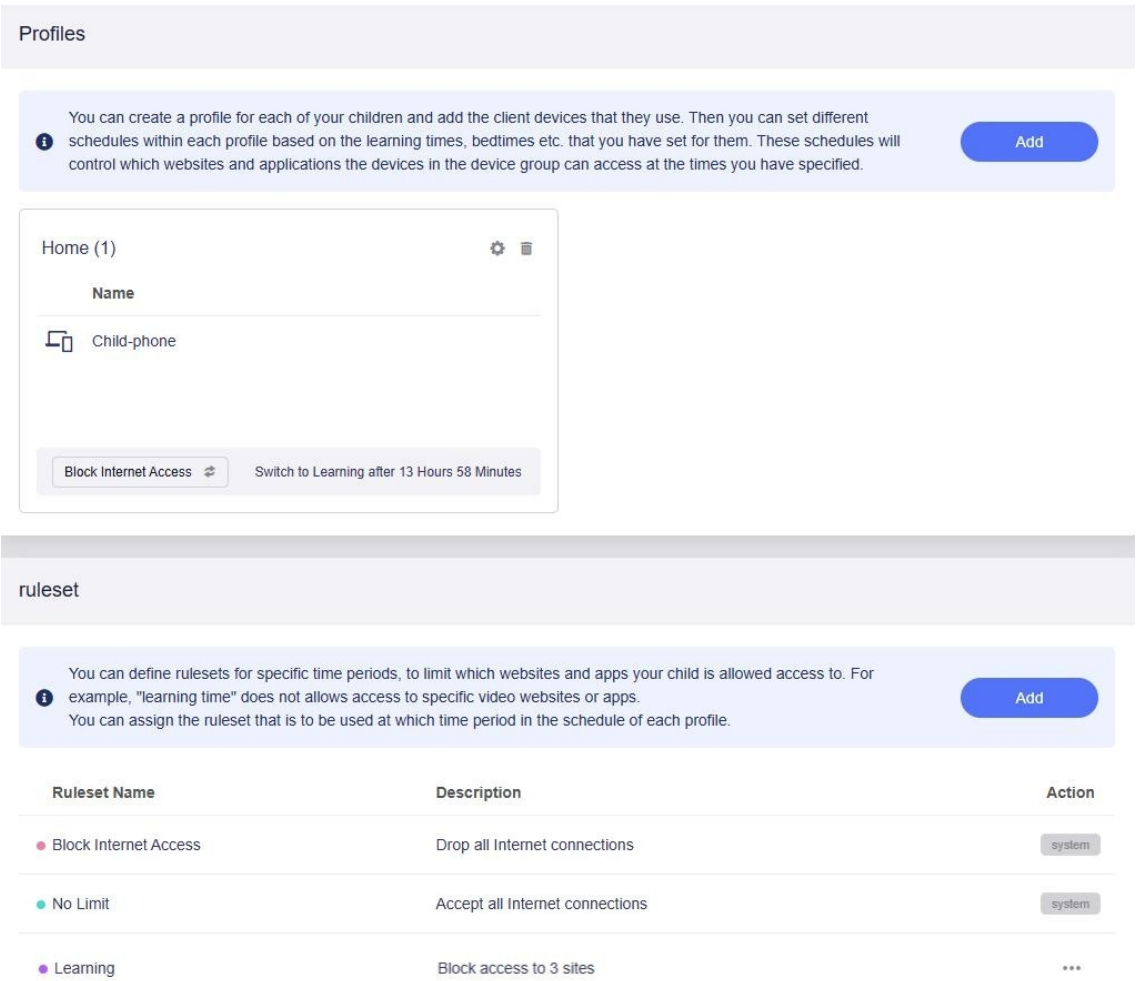
- La linea rossa tratteggiata indica l'ora corrente.

- Puoi modificare il tempo di esecuzione facendo clic su un determinato set di regole nel programma.

7. Fai clic su **Controllo parentale** in alto per tornare alla pagina Controllo parentale.




Vedrai la configurazione finale. Controllo parentale sta ora entrando in vigore secondo il programma. Puoi modificare profili e set di regole esistenti o aggiungerne di nuovi se necessario.



## 12.5.2 Risoluzione dei problemi

Se le impostazioni configurate non hanno effetto, controlla le seguenti possibili cause.

1. Problema con la cache DNS.
   Browser e sistemi operativi mantengono cache DNS, il che potrebbe ritardare l'applicazione delle modifiche alla configurazione. Svuota la cache DNS per applicare immediatamente le modifiche.
2. La pianificazione del profilo non è ancora iniziata.
3. Il nome di dominio inserito potrebbe essere errato.
   Mentre il dominio pubblico di un sito web è facile da trovare, i domini API utilizzati dalle app spesso non sono disponibili pubblicamente. Per individuare il dominio corretto, utilizza uno strumento di acquisizione di pacchetti come Wireshark o cerca le informazioni sul dominio pertinenti.
   Ad esempio, quando si blocca "www.google.com”, entrando in "google.com" si ottengono risultati migliori rispetto a "www.google.com”.
4. Il dispositivo di destinazione utilizza un indirizzo MAC casuale per ogni connessione di rete, il che impedisce alle regole di accesso di avere effetto. Disabilita l'indirizzo MAC casuale sul dispositivo di destinazione, quindi aggiungi nuovamente il dispositivo al tuo profilo.

## 12.6 ZeroTier

ZeroTier è una rete privata virtuale (VPN) basata su software che consente comunicazioni sicure e crittografate tra dispositivi su Internet. Crea una rete virtuale privata che consente ai dispositivi di comunicare come se fossero sulla stessa rete locale, indipendentemente dalla loro posizione fisica o topologia di rete. ZeroTier è progettato per essere facile da configurare e utilizzare e offre funzionalità come crittografia end-to-end, segmentazione della rete e funzionalità di bridging di rete.

La funzione ZeroTier sui router GL.iNet consente al router di unirsi a una rete virtuale ZeroTier, abilitando accesso remoto al router stesso, nonché alle sue risorse lato WAN e LAN.

**Nota**:

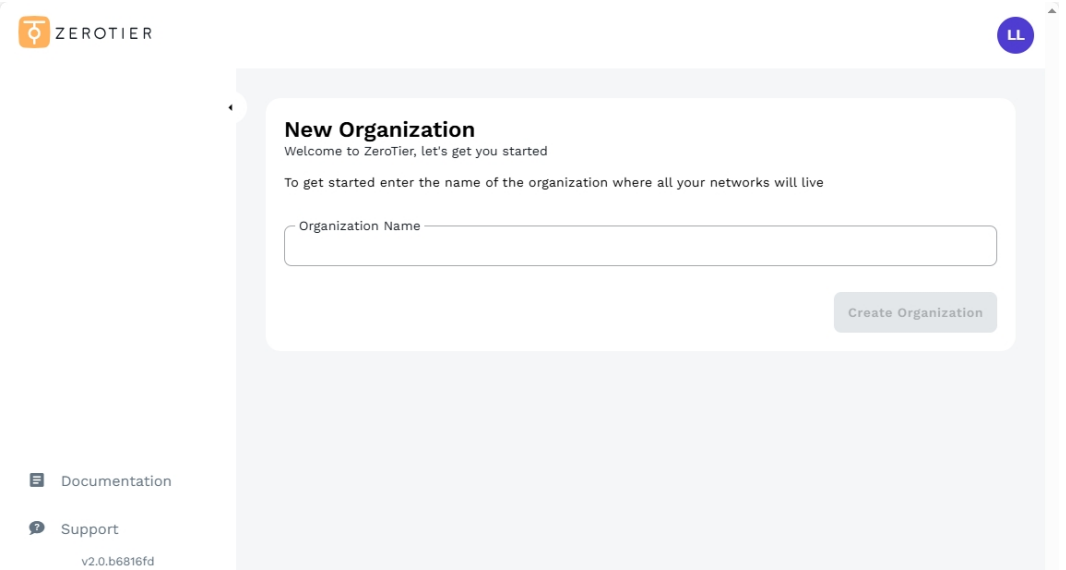
1. Non è consigliabile utilizzare ZeroTier contemporaneamente a una qualsiasi delle seguenti funzionalità o servizi, poiché ciò potrebbe causare conflitti di routing: Client OpenVPN, Client WireGuard, GoodCloud da sito a sito e Tailscale.
2. Questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug.

## 12.6.1 Configurazione di ZeroTier

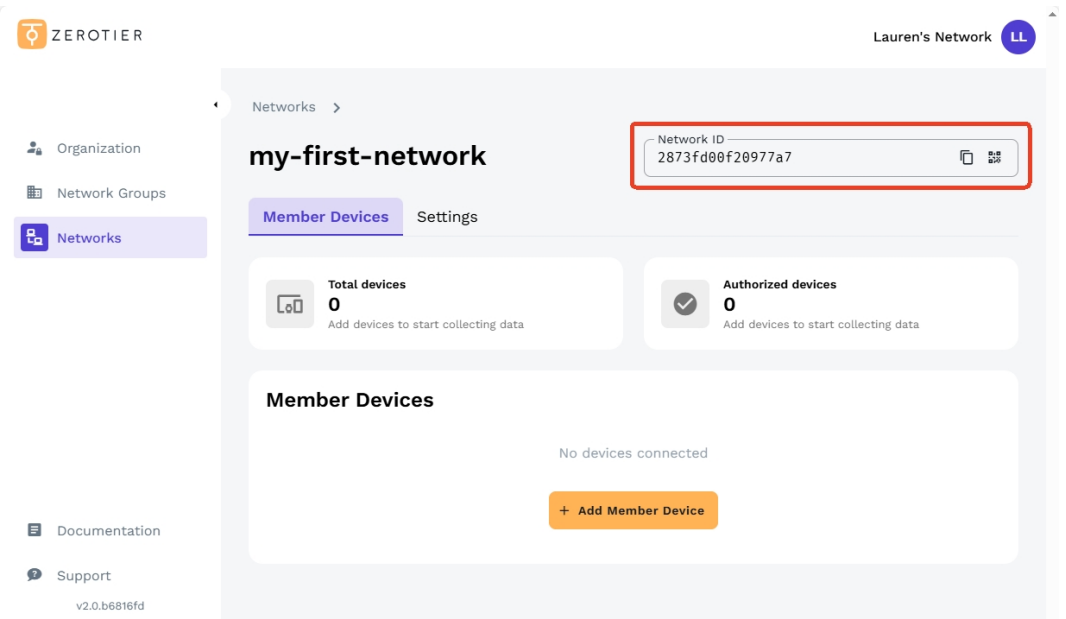
Sono disponibili due versioni di ZeroTier Central: New Central e Legacy Central.

I passaggi seguenti utilizzano New Central come esempio.

1. Visita il [sito web ufficiale ZeroTier] e accedi con il tuo account.
2. Crea un'organizzazione.

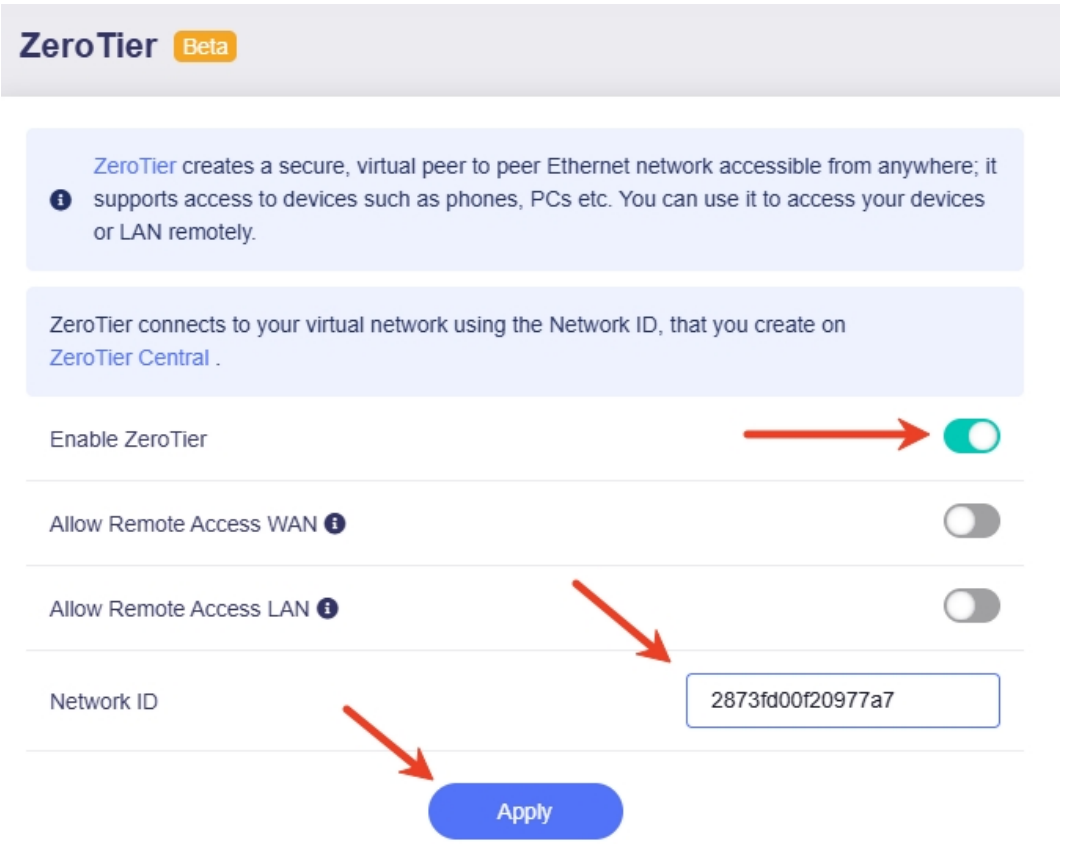



3. Seleziona un piano. Qui scegliamo **come esempio il piano Personal**, che include i dispositivi 10, l'amministratore di rete 1 e la rete 1. Se devi creare più reti, aggiungere più dispositivi o aggiungere percorsi e DNS personalizzati, scegli un altro piano a pagamento.
4. Ora la tua rete ZeroTier è stata creata.

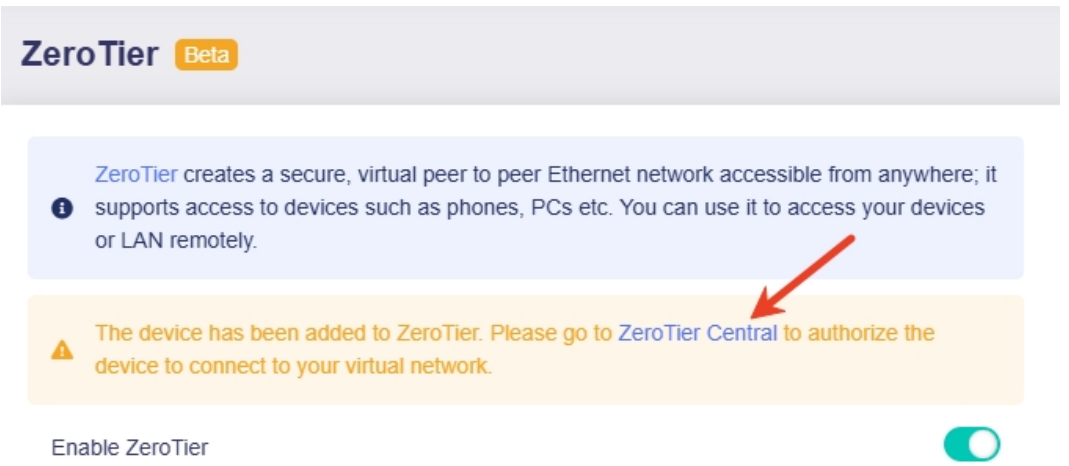


Usa nota **dell'ID di rete**, che è una combinazione alfanumerica di caratteri 16 nell'angolo in alto a destra, poiché sarà richiesto quando connetterai altri dispositivi in seguito.

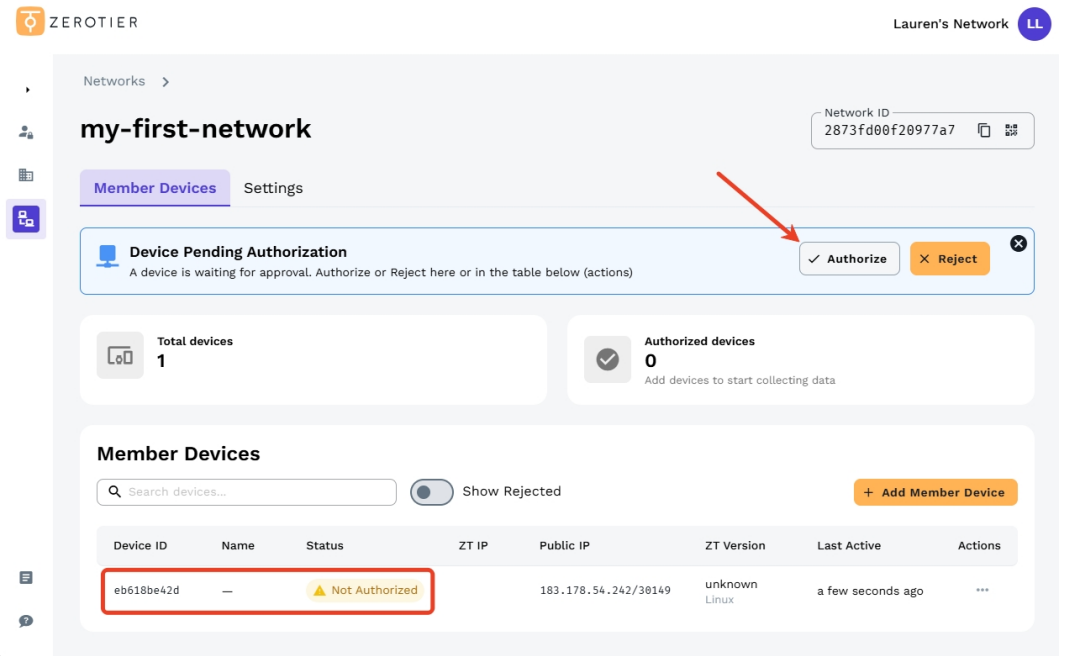
5. Accedi al pannello di amministrazione web del tuo router e vai su **APPLICAZIONI** > **ZeroTier**. Abilita ZeroTier, inserisci **l'ID di rete**, quindi fai clic su **Applica**.



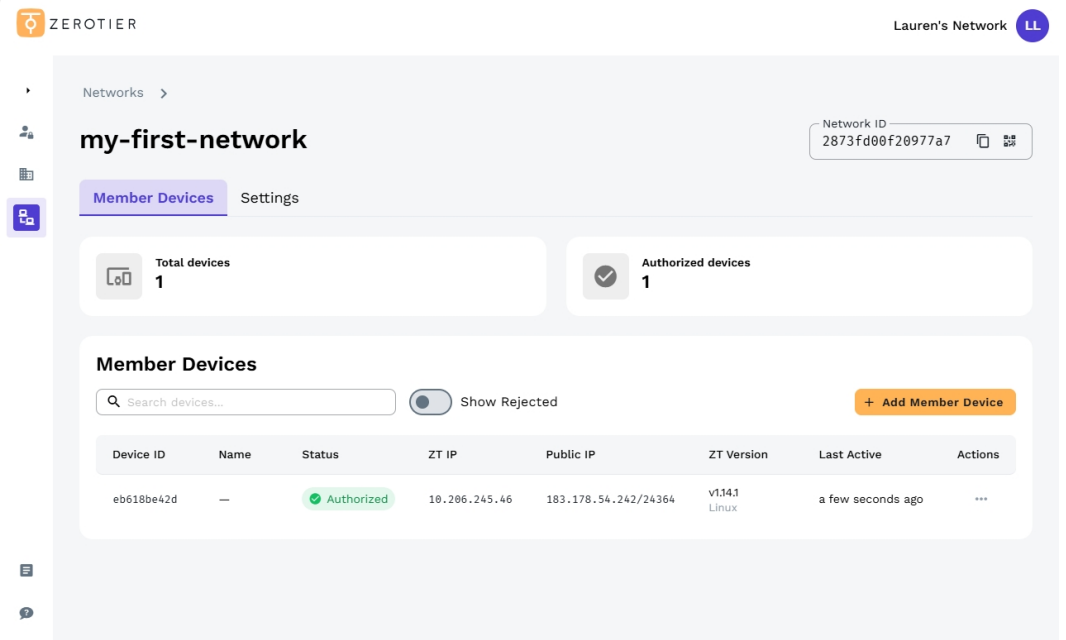

Dopo poco, la pagina indicherà che è necessaria l'autorizzazione. Fare clic **sul collegamento ipertestuale ZeroTier Central** per reindirizzare allo ZeroTier Central.



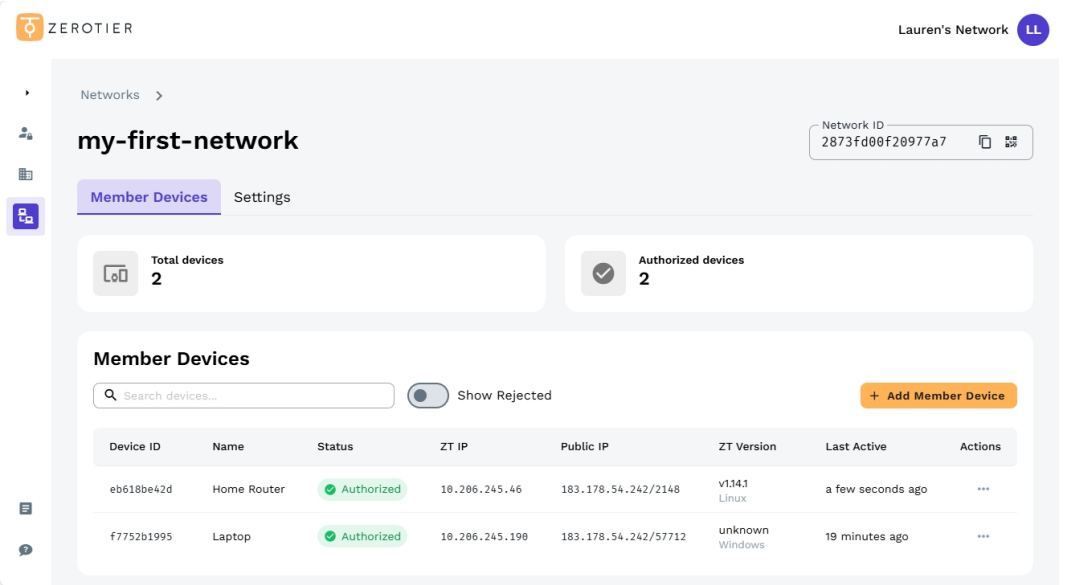

6. Sul ZeroTier Central, individua il dispositivo in sospeso e autorizzalo.




Una volta autorizzata, la pagina viene visualizzata come segue.

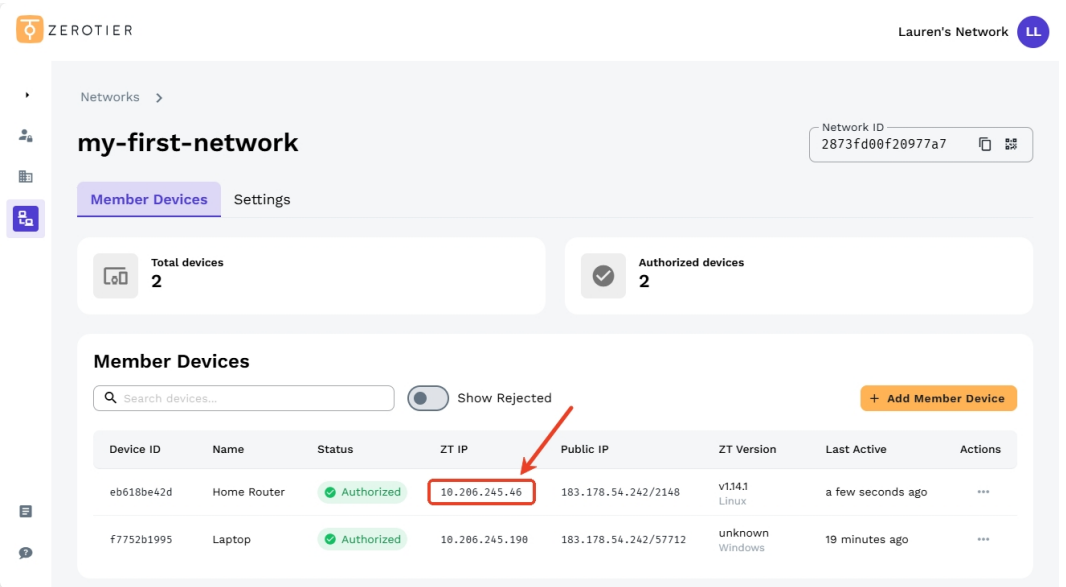



7. Aggiungi un altro dispositivo (come un computer o uno smartphone) alla stessa rete ZeroTier seguendo questa guida. Una volta aggiunta correttamente, la pagina viene visualizzata come segue. Vedrai i dettagli dei dispositivi membri, come ID dispositivo, nome, stato, IP gestito e IP pubblico.




Suggerimento: puoi fare clic sull'icona con tre punti a destra per modificare le impostazioni del dispositivo membro, inclusi il nome del dispositivo, gli IP gestiti e le impostazioni avanzate.

8. Fai clic sull'IP gestito del router per copiarlo.

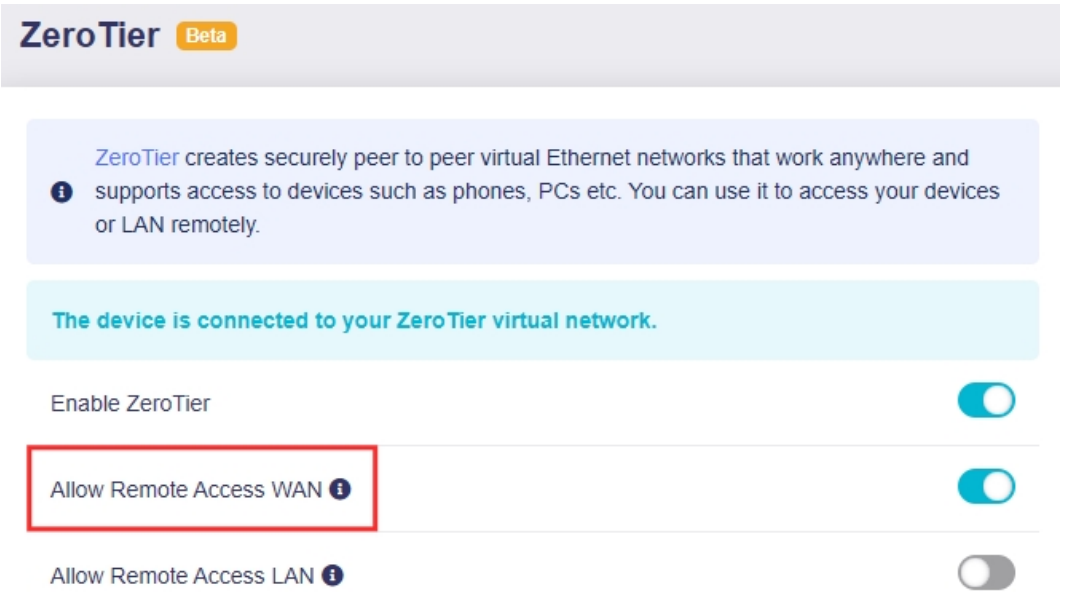



Puoi quindi utilizzare questo IP gestito per accedere al router dal tuo laptop che si trova sulla stessa rete ZeroTier.

9. Verifica connettività.
   Sul laptop connesso alla stessa rete ZeroTier, aprire un browser Web e inserire l'IP gestito del router ottenuto nel passaggio precedente. Se riesci ad accedere al pannello di amministrazione web del router, la connessione ZeroTier ha avuto esito positivo.

## 12.6.2 Consenti accesso remoto WAN

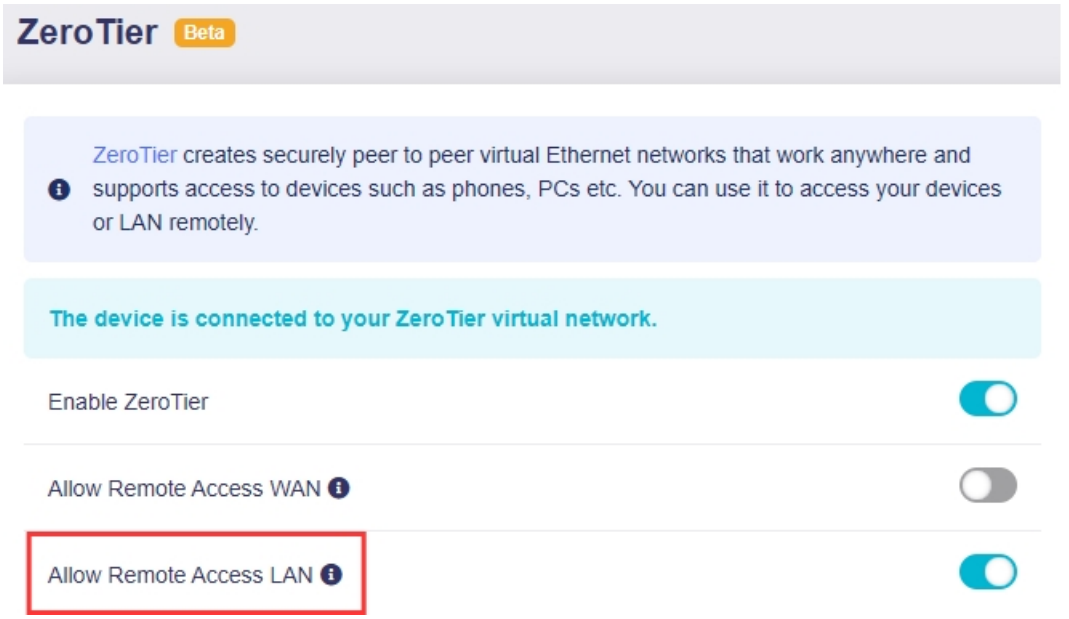
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato WAN del dispositivo tramite la rete virtuale ZeroTier. Vedi qui per maggiori dettagli.




Nota: questa funzionalità richiede l'aggiunta di regole di routing alla rete ZeroTier per avere effetto. È possibile aggiungere gratuitamente un percorso personalizzato in Legacy Central, mentre in New Central puoi configurare percorsi personalizzati solo con un piano Essential o superiore. Vedi qui per i dettagli sui prezzi.

## 12.6.3 Consenti accesso remoto LAN

Se questa opzione è abilitata, è possibile accedere alle risorse sul lato LAN del dispositivo tramite la rete virtuale ZeroTier. Vedi qui per maggiori dettagli.




Nota: questa funzionalità richiede l'aggiunta di regole di routing alla rete ZeroTier per avere effetto. È possibile aggiungere gratuitamente un percorso personalizzato in Legacy Central, mentre in New Central puoi configurare percorsi personalizzati solo con un piano Essential o superiore. Vedi qui per i dettagli sui prezzi.

## 12.7 Tailscale

Tailscale è un servizio VPN che rende i tuoi dispositivi e le tue applicazioni personali accessibili in tutto il mondo, in modo sicuro e semplice.

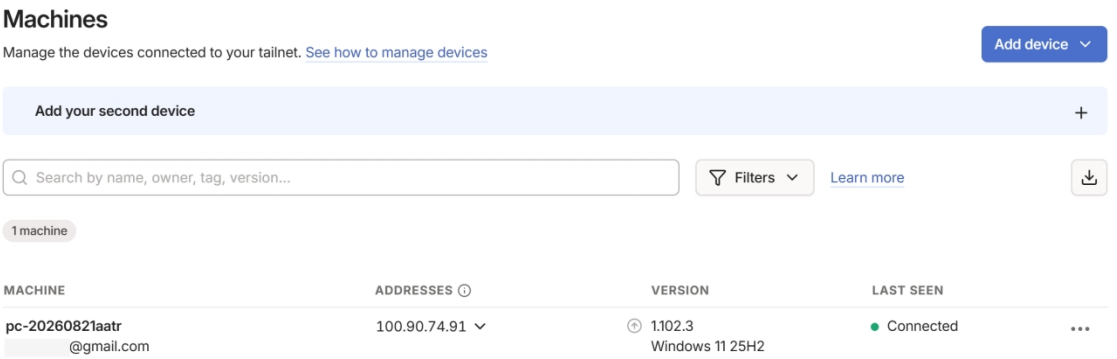
La funzionalità Tailscale sui router GL.iNet consente al router di unirsi a una rete virtuale Tailscale, consentendo l'accesso remoto al router stesso, nonché alle sue risorse lato WAN e LAN.

**Nota**:

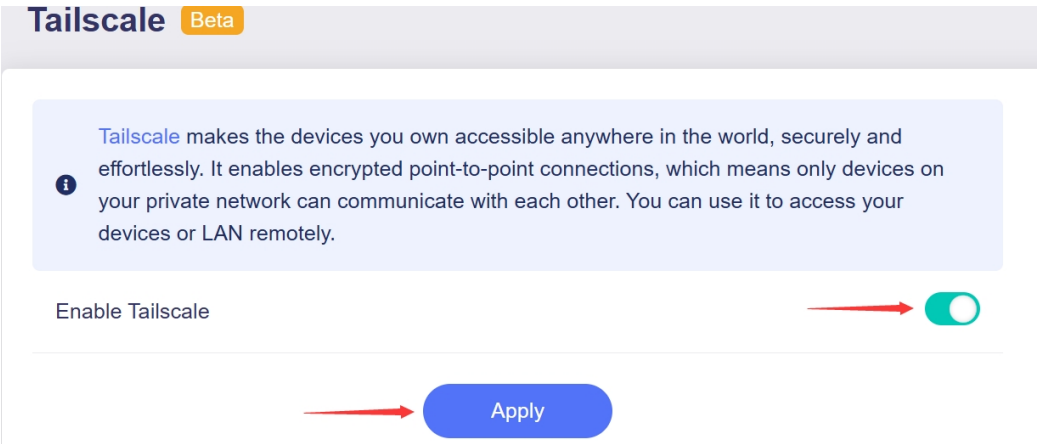
1. Poiché Tailscale è basato su WireGuard, non è consigliabile utilizzare Tailscale con una qualsiasi delle seguenti funzionalità o servizi contemporaneamente, poiché ciò potrebbe causare conflitti di routing: Client OpenVPN, Client WireGuard, GoodCloud da sito a sito, ZeroTier.
2. Questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug.

## 12.7.1 Configurazione di Tailscale

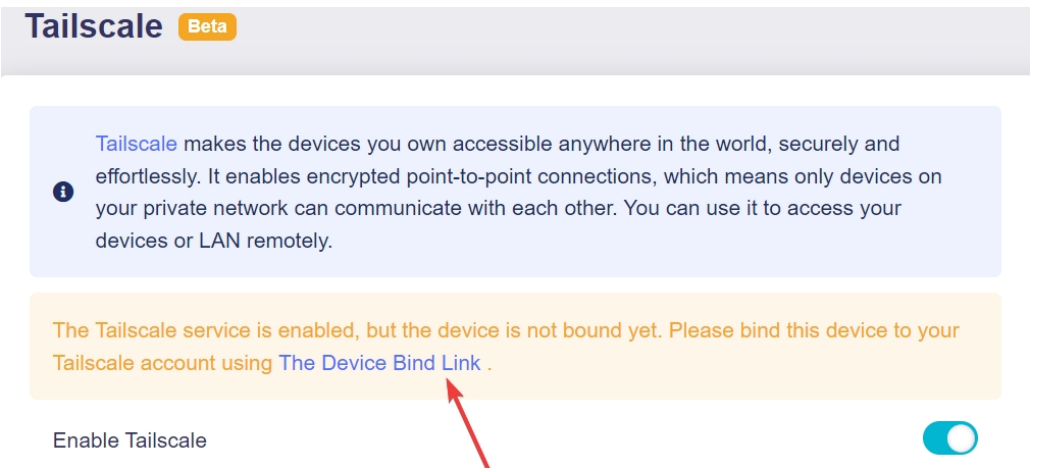
1. Registra prima un account Tailscale e associa uno o due dispositivi al tuo account Tailscale a scopo di test. Dopo l'associazione, vedrai i tuoi dispositivi nella console Tailscale.




2. Accedi al pannello di amministrazione web del tuo router e vai su **APPLICAZIONI** > **Tailscale**. Attiva **Abilita Tailscale** e fai clic su Applica.



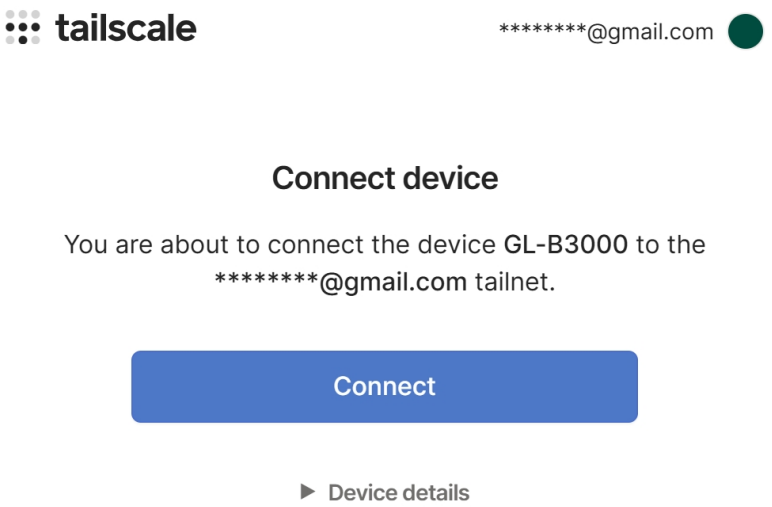

3. La pagina ti chiederà di associare il dispositivo. Fai clic su **Link di associazione del dispositivo**.



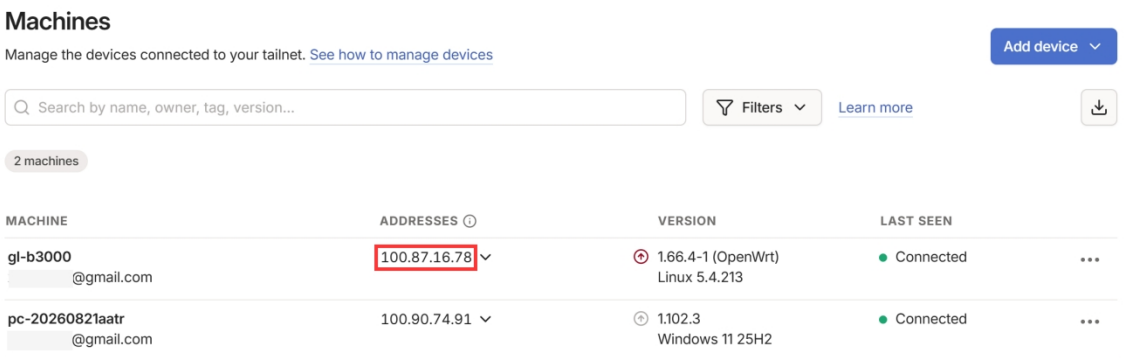
4. Nella finestra pop-up, fai clic sul collegamento e accedi con il tuo account Tailscale.




5. Una volta effettuato l'accesso ti verrà chiesto di confermare il dispositivo. Fai clic su **Connetti**.



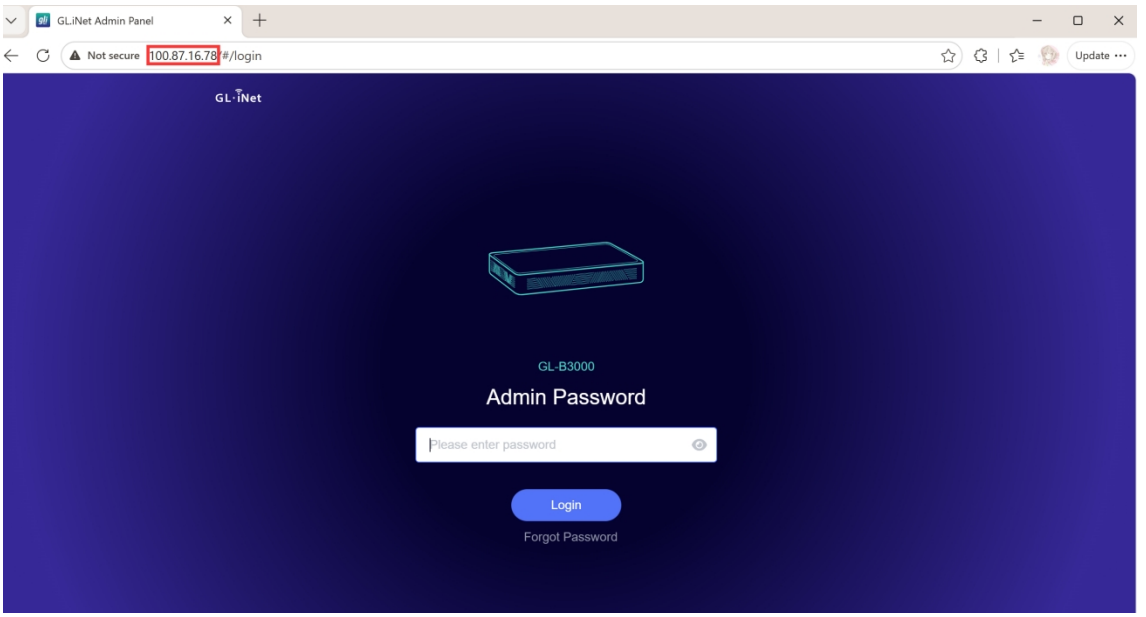

6. Verrai quindi reindirizzato alla console di amministrazione Tailscale. Ora il router è stato aggiunto alla rete virtuale Tailscale ed è possibile accedervi in remoto tramite l'IP virtuale Tailscale **100.87.16.78**.




7. Verifica connettività.

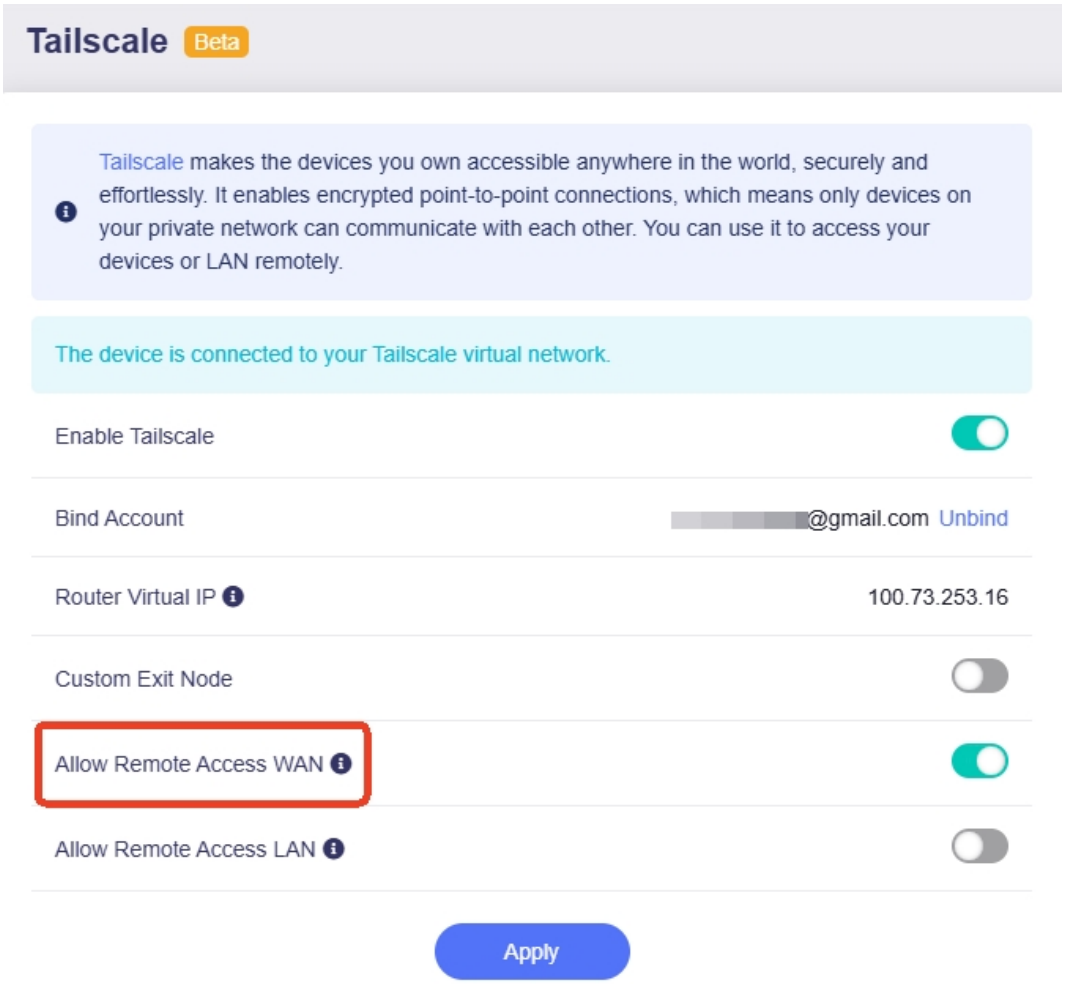
   Su un altro dispositivo connesso alla stessa rete Tailscale, apri un browser web e inserisci l'IP virtuale del router nella barra degli indirizzi. Se riesci ad accedere al pannello di amministrazione web del router, significa che Tailscale funziona. Puoi anche utilizzare

il comando ping o SSH accedere al terminale del router tramite il suo IP virtuale per testare la connettività.



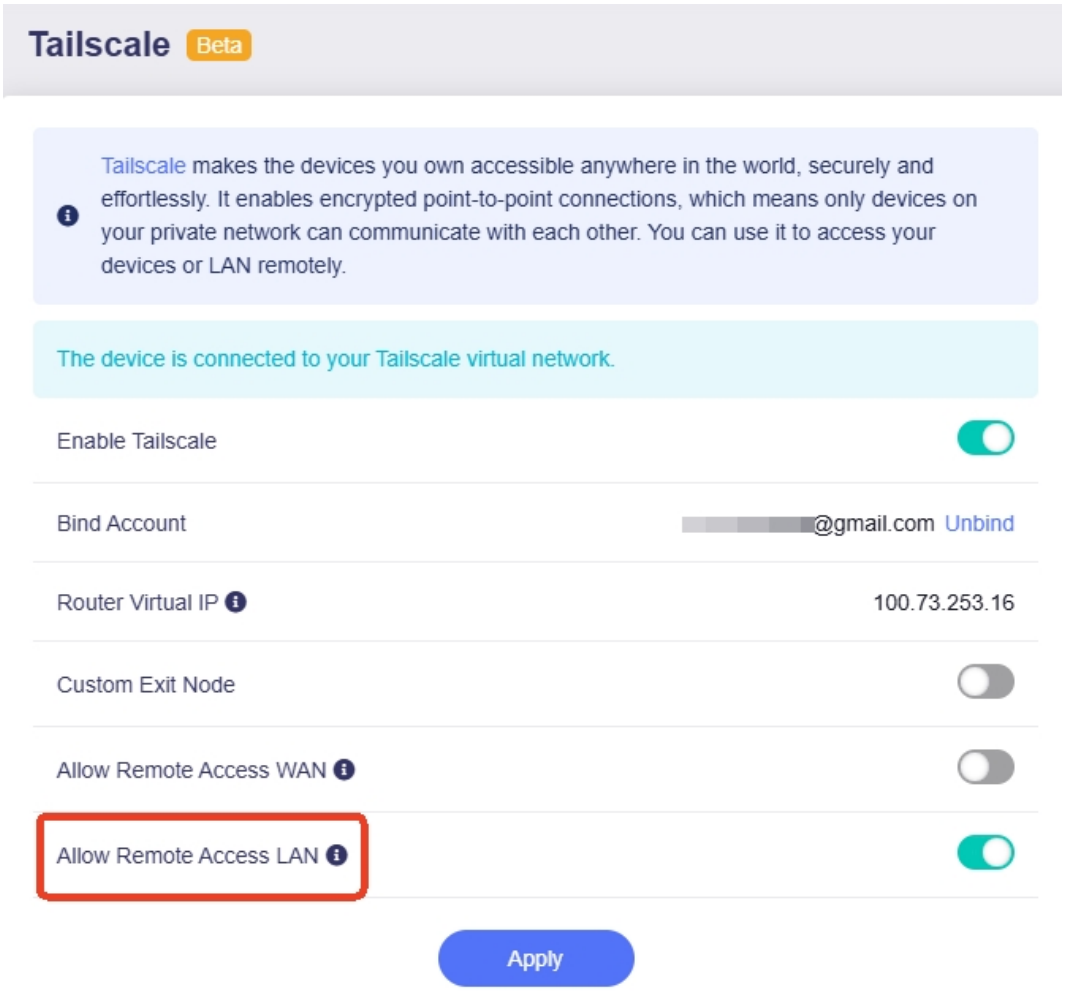
## 12.7.2 Consenti accesso remoto WAN

Se questa opzione è abilitata, è possibile accedere alle risorse sul lato WAN del dispositivo tramite la rete virtuale Tailscale. Vedi qui per ulteriori dettagli.



## 12.7.3 Consenti accesso remoto LAN

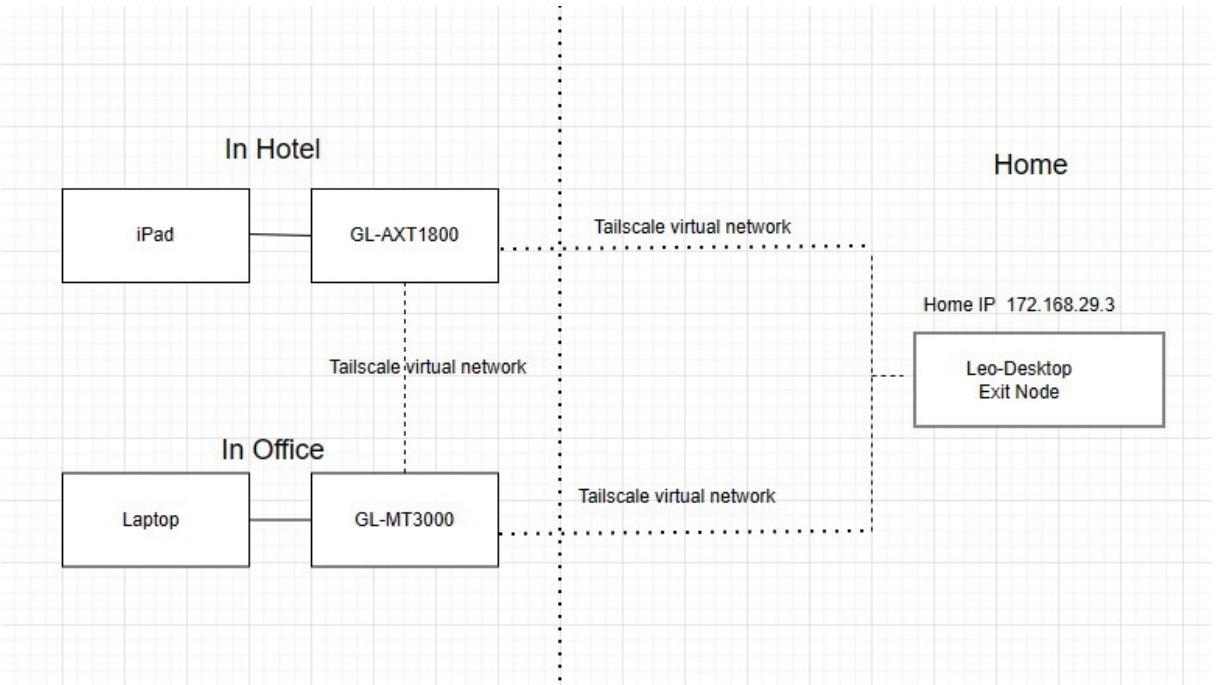
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato LAN del dispositivo tramite la rete virtuale Tailscale. Vedi qui per ulteriori dettagli.



## 12.7.4 Nodi di uscita personalizzati

Per impostazione predefinita, Tailscale agisce come una rete overlay: instrada il traffico solo tra i dispositivi che eseguono Tailscale e non elabora il traffico Internet pubblico, ad esempio quando navighi su siti Web come Google.

Tuttavia, potrebbero esserci momenti in cui desideri che Tailscale instradi il tuo traffico Internet pubblico. Ad esempio, quando sei lontano da casa o viaggi all'estero, se hai bisogno di accedere a servizi online (come quelli bancari) che sono disponibili solo nel tuo Paese, puoi impostare il tuo desktop di casa con un IP pubblico come nodo di uscita e configurare altri dispositivi sulla stessa Tailnet, come GL-AXT1800 e GL-MT3000 nell'immagine seguente, per inviare il loro traffico attraverso di essa. Ciò consente a tutto il traffico Internet pubblico di essere inoltrato tramite il nodo di uscita.




In sintesi, un nodo di uscita instrada il traffico Internet in uscita dai tuoi dispositivi Tailnet, agendo effettivamente come server VPN. Quando sei connesso a un nodo di uscita, tutto il tuo traffico Internet non Tailscale sembra provenire dalla sua posizione, aiutandoti ad accedere a contenuti con restrizioni geografiche e a migliorare la tua privacy online. Il dispositivo che gestisce questo inoltro del traffico viene definito "nodo di uscita". Per configurare il nodo di uscita personalizzato sui router GL.iNet, fare riferimento a questo tutorial.

**Nota**: se il server DNS del router è un indirizzo IP privato a cui è possibile accedere solo nella rete locale, potresti perdere l'accesso a Internet durante l'esecuzione dei nodi di uscita. Per evitare ciò, imposta manualmente un server DNS pubblico (ad esempio 8.8.8.8) per il tuo router.

Capitolo 13

# Rete

Questo capitolo introduce le impostazioni relative alla rete per la configurazione e la gestione, come LAN, DNS e IPv6.

## 13.1 Firewall

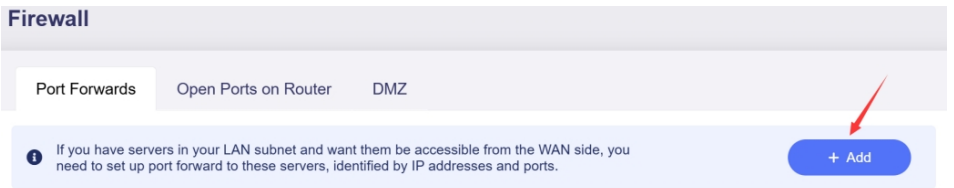
Il firewall è una funzionalità di rete che instrada le richieste esterne a dispositivi specifici sulla tua rete locale. La pagina Firewall include tre funzioni chiave: **Port forwarding** (per l'accesso mirato a porte specifiche di dispositivi), **Apertura delle porte sul router** (per l'accesso ai servizi in esecuzione sul router stesso) e **DMZ** (per l'accesso completo diretto a un singolo dispositivo).

### 13.1.1 Port forwarding

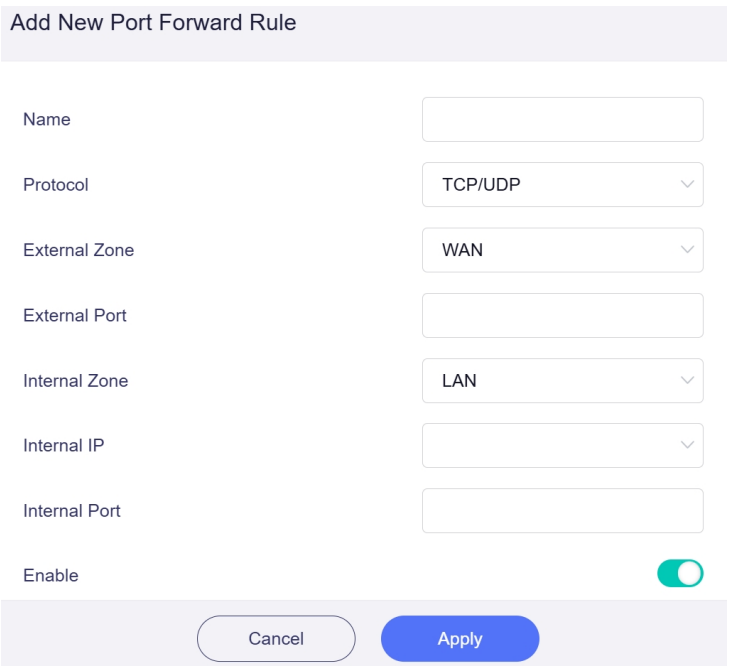
Port forwarding consente ai computer remoti di connettersi a un computer locale o a un server dietro il firewall LAN (ad esempio server Web, server FTP).

Se è necessario impostare il port forwarding, seguire i passaggi seguenti.

1. Accedi al pannello di amministrazione web del tuo router, vai su **RETE** > **Firewall** > **sezione Port forwarding** e fai clic su **Aggiungi**.




2. Nella finestra pop-up, inserisci o seleziona i parametri richiesti dall'elenco a discesa per aggiungere una regola di port forwarding, quindi fai clic su **Applica**.

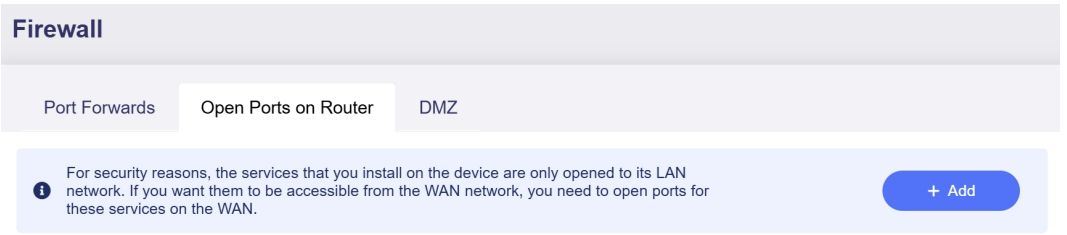


- **Nome**: il nome della regola che può essere specificato dall'utente.
- **Protocollo**: il protocollo utilizzato. Puoi scegliere TCP, UDP o sia TCP che UDP.
- **Zona esterna**: le opzioni disponibili sono WAN, Client WireGuard, Server WireGuard, Client OpenVPN, Server OpenVPN, LAN e Guest.
- **Porta esterna**: il numero o i numeri di porte esterne. Inserisci qui un numero di porta specifico. L'intervallo di porte è 1–65535. Puoi impostare una singola porta o un intervallo di porte concatenando il primo e l'ultimo numero di porta con un trattino (ad esempio, 501-510).
- **Zona interna**: le opzioni disponibili sono LAN, Ospite, Client WireGuard, Server WireGuard, Client OpenVPN, Server OpenVPN e WAN.
- **IP interno**: l'indirizzo IP assegnato dal router al dispositivo che necessita dell'accesso remoto. Se imposti una porta singola in Porta esterna, imposta una porta singola qui. Se imposti un intervallo di porte in Porta esterna, imposta qui l'intervallo di porte corrispondente.
- **Porta interna**: il numero della porta interna del dispositivo. Immettere un numero di porta specifico. Lascialo vuoto se corrisponde alla porta esterna.
- **Abilita**: abilita o disabilita questa regola.

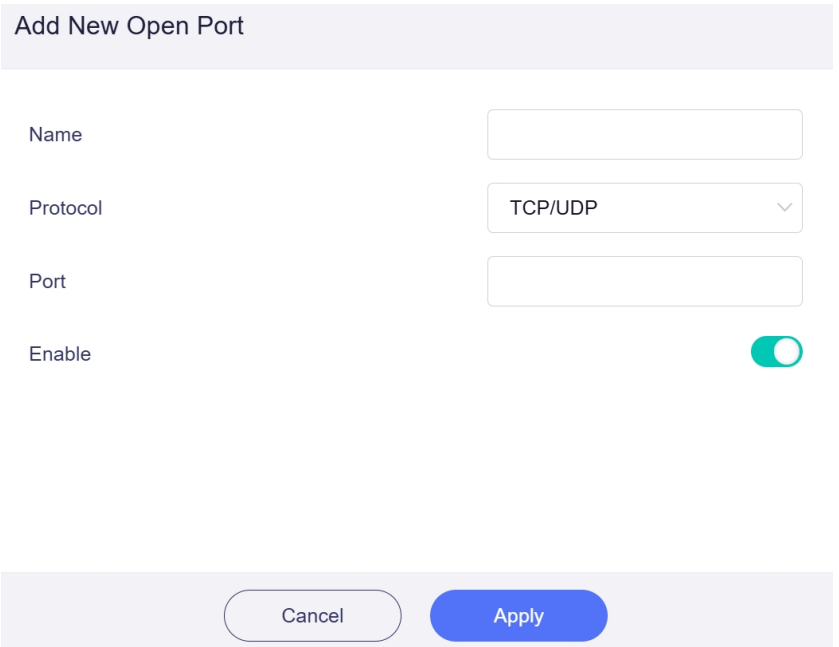
## 13.1.2 Apertura delle porte sul router

I servizi del router, come web e FTP, richiedono che le rispettive porte siano aperte sul router per essere raggiungibili pubblicamente.

Per aprire una porta, passa alla scheda Apri porte sul router, quindi fai clic su Aggiungi.




Nella finestra pop-up, apri una nuova porta e fai clic su Applica.



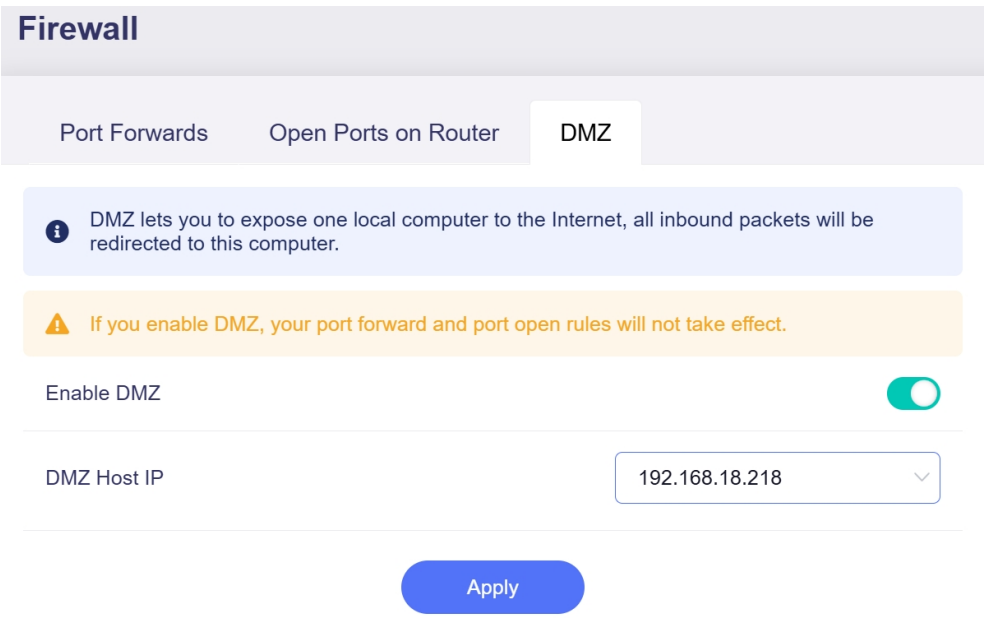

- **Nome**: il nome della regola che può essere specificato dall'utente.
- **Protocollo**: il protocollo utilizzato, puoi scegliere TCP, UDP o entrambi TCP e UDP.
- **Porta**: il numero di porta che desideri aprire.

## 13.1.3 DMZ

DMZ ti consente di esporre un computer a Internet, quindi tutti i pacchetti in entrata verranno reindirizzati a questo computer.

Segui i passaggi seguenti per abilitare DMZ, se necessario.

1. Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **Firewall** > **sezione DMZ**.
2. Attiva **Abilita DMZ**, quindi seleziona **l'IP host DMZ** dall'elenco a discesa. Il dispositivo selezionato riceve tutti i pacchetti in entrata. Fai clic su **Applica** per salvare le impostazioni.



## 13.2 Multi-WAN

Multi-WAN consente l'uso simultaneo di più metodi di accesso a Internet, consentendo la configurazione di diverse opzioni di connettività sul router. Offre due modalità di lavoro:

- **Failover**: passa automaticamente a una connessione alternativa in breve tempo se la connessione primaria fallisce, garantendo un accesso alla rete ininterrotto.
- **Bilanciamento del carico**: distribuisce il traffico di rete su tutte le connessioni disponibili con un rapporto prestabilito per l'utilizzo simultaneo di più connessioni, ottimizzando l'utilizzo della larghezza di banda.

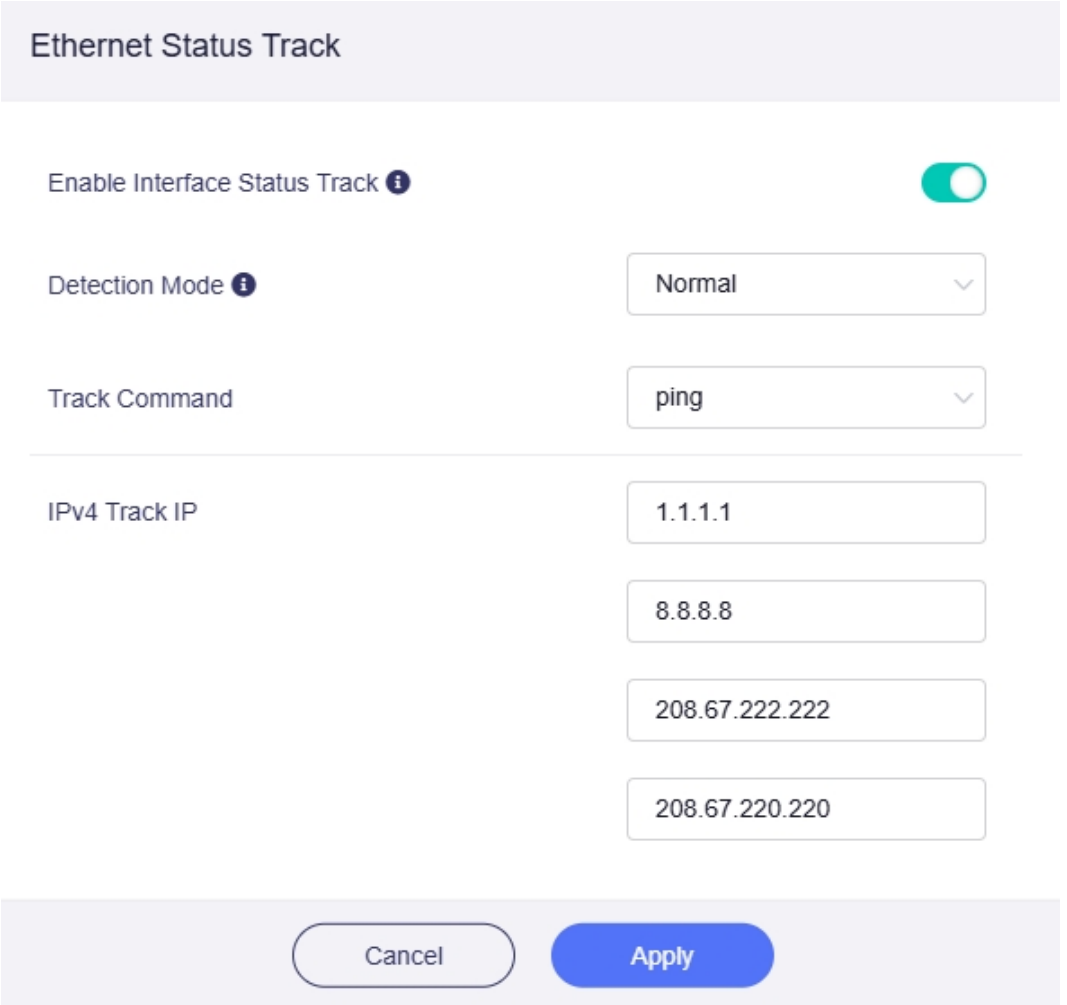
Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Multi-WAN**. Questa pagina include due sezioni: Monitoraggio dello stato dell'interfaccia e Modalità Multi-WAN.

### 13.2.1 Monitoraggio dello stato dell’interfaccia

I router GL.iNet utilizzano il comando **ping** per monitorare lo stato della connessione all'IP di destinazione e determinare se l'interfaccia è disponibile. Se l'interfaccia è disponibile verrà visualizzato un punto verde sulla sinistra; altrimenti sarà grigio.



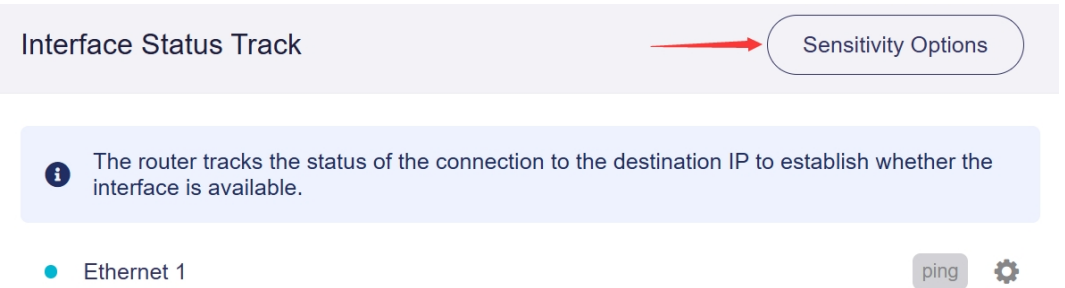

Nella sezione **Monitoraggio dello stato dell'interfaccia**, fai clic sull'icona a forma di ingranaggio a destra per accedere alle impostazioni di monitoraggio dello stato per ciascuna interfaccia di rete. Di seguito sono riportate le impostazioni di monitoraggio dello stato per l'interfaccia Ethernet. La stessa logica di configurazione si applica ad altre interfacce.



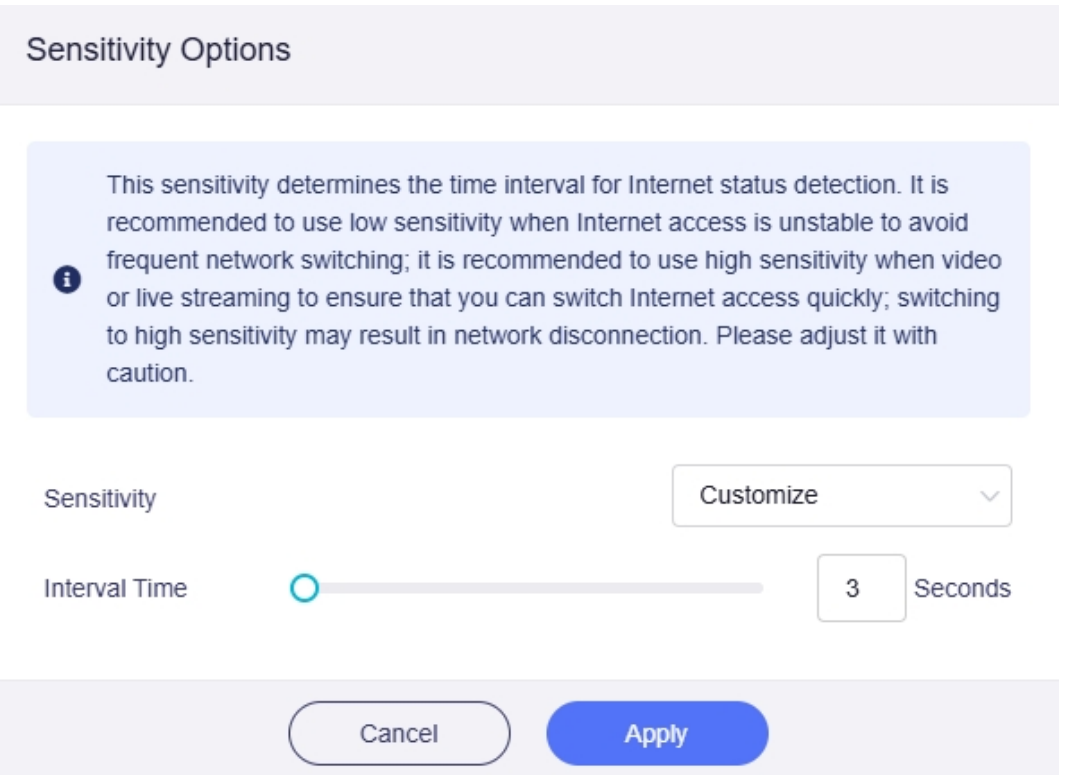

- **Abilita monitoraggio dello stato dell'interfaccia**: è abilitato per impostazione predefinita. Se disabilitato, il router determinerà lo stato dell'interfaccia in base alle condizioni fisiche (ad esempio, se il cavo Ethernet è collegato).
- **Modalità di rilevamento**: questa funzionalità è stata introdotta come Modalità dati ridotti nel firmware v4.5, quindi rinominata Modalità di rilevamento nel firmware v4.7. Sono disponibili tre modalità: modalità normale, modalità dati ridotti e modalità rigorosa.
  - **Normale**: viene utilizzato per impostazione predefinita.
  - **Dati bassi**: attiva il monitoraggio solo quando si verifica un errore di rete sull'interfaccia di rete. Utilizza questa modalità se hai un piano dati limitato. Tieni presente che la riconnessione dopo una disconnessione potrebbe essere leggermente più lenta rispetto alla modalità normale ed è abilitata per impostazione predefinita solo per l'interfaccia cellulare.
  - **Rigoroso**: determina lo stato dell'interfaccia esclusivamente in base ai risultati di un comando di rilevamento inviato a un IP pubblico.

- **Comando di monitoraggio**: il comando ping viene utilizzato per monitorare lo stato della connessione all'IP di destinazione e verificare la disponibilità dell'interfaccia.
- **IP di monitoraggio IPv4**: personalizza gli indirizzi IPv4 da monitorare, se necessario.

Fai clic su **Opzioni sensibilità** nell'angolo in alto a destra.




È possibile impostare l'intervallo di tempo per il rilevamento dello stato di Internet su Basso, Medio, Alto oppure personalizzarlo. L'intervallo di tempo regolabile varia da 0,5 secondi a 90 secondi.



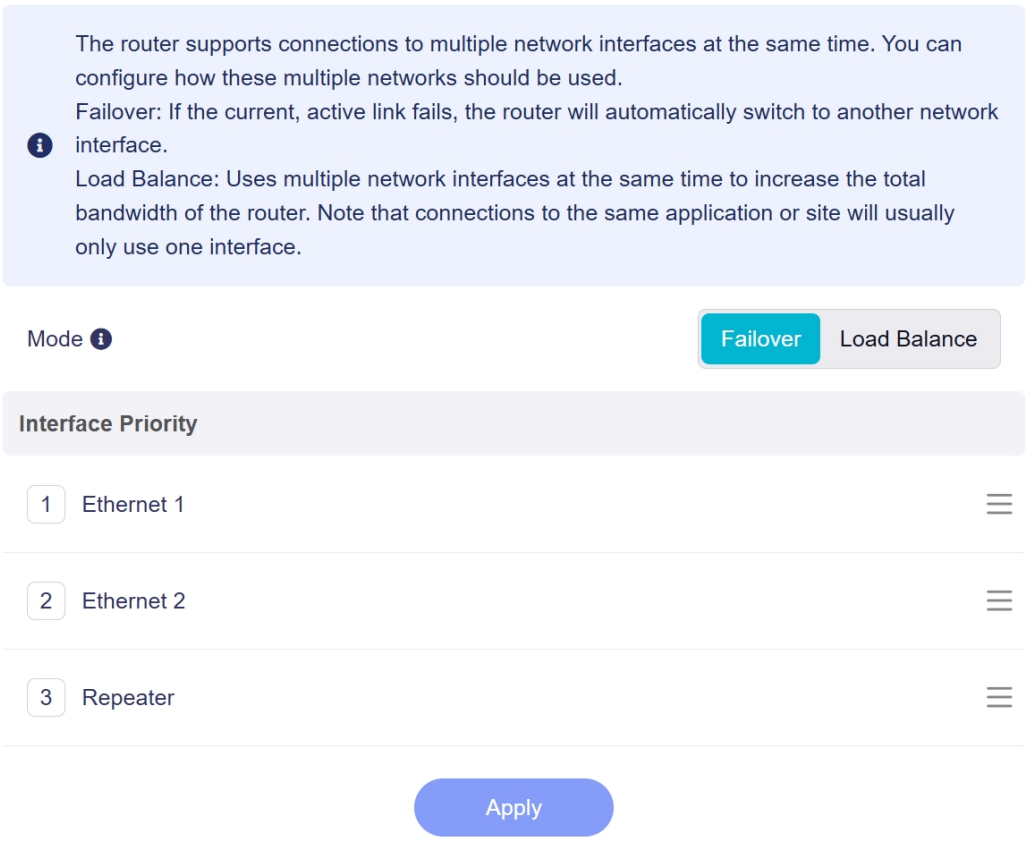
## 13.2.2 Modalità Multi-WAN

Sono disponibili due modalità per Multi-WAN: **Failover** e **Bilanciamento del carico**. Tieni presente che queste modalità si escludono a vicenda.

## Failover

Il failover è la modalità predefinita quando sono configurate più connessioni. Se il collegamento attivo fallisce, il router passerà automaticamente a un'altra interfaccia di rete per l'accesso a Internet.

Puoi impostare livelli di priorità per ciascuna interfaccia: quando l'interfaccia attualmente utilizzata fallisce, il router passa alla successiva interfaccia disponibile con la priorità più alta. Una volta ripristinata una connessione con priorità più alta, il router tornerà automaticamente ad essa.

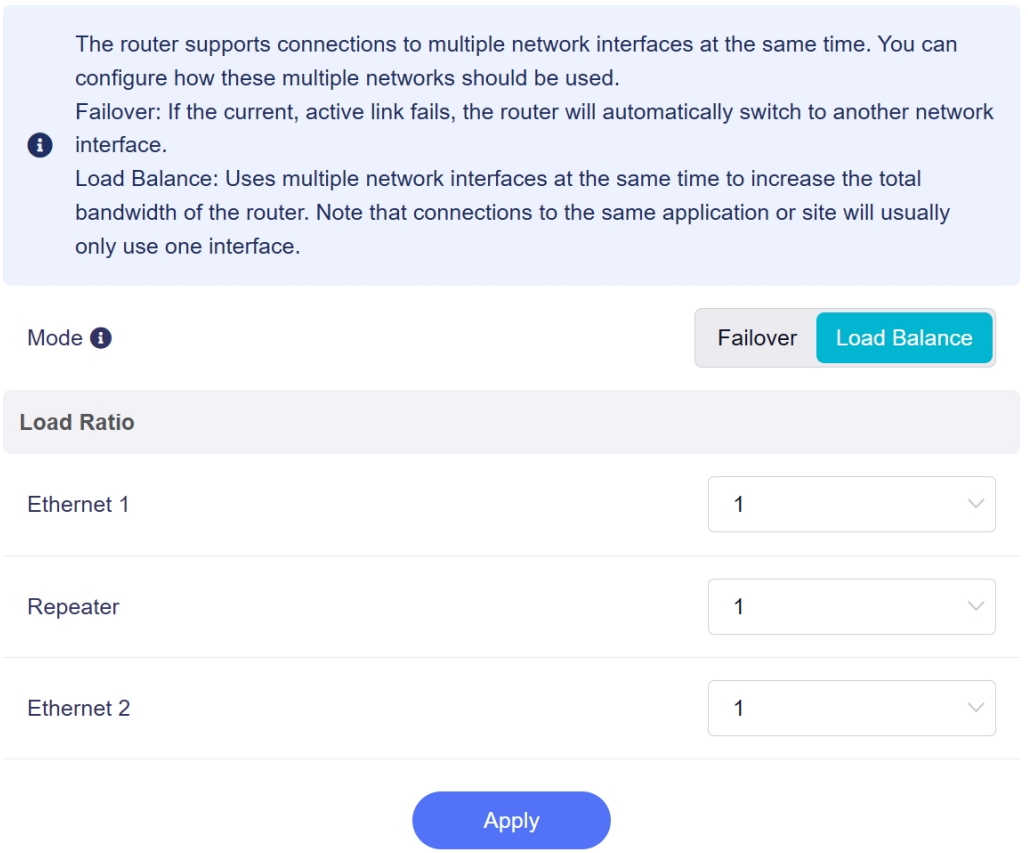


## Bilanciamento del carico

La modalità Bilanciamento del carico utilizza più interfacce di rete contemporaneamente per aumentare la larghezza di banda totale del router, con il sistema che distribuisce le nuove connessioni tra le interfacce in base a un rapporto di carico configurato. Tieni presente che le connessioni alla stessa applicazione o sito Web utilizzeranno in genere una sola interfaccia.

Il rapporto di carico si riferisce alla proporzione tra ciascuna interfaccia di rete. Il sistema assegnerà le interfacce per gestire le nuove connessioni in base a questo rapporto configurato.

Ad esempio, se il router è collegato a tre reti (ad esempio, Ethernet 1, Ripetitore ed Ethernet 2) contemporaneamente e tutte le interfacce sono disponibili per l'accesso a Internet, abilitando Bilanciamento del carico e impostando un Il rapporto 1:1:1 significa che le tre interfacce condivideranno equamente la larghezza di banda della rete. Il sistema distribuirà le nuove connessioni su queste interfacce in base al rapporto di carico 1:1:1 configurato.



Puoi anche personalizzare il rapporto di carico, se necessario. Ad esempio, se Ethernet 1 ha una larghezza di banda di 100 Mbps, Ripetitore ha 200 Mbps e nessun'altra connessione è attiva, impostare i rapporti di carico su 1 per Ethernet 1, 2 per Ripetitore r e 0 per Ethernet 2. Il sistema distribuirà quindi le nuove connessioni su queste interfacce in base al rapporto 1:2 configurato, il che significa che Ethernet 1 gestirà la metà delle connessioni rispetto a Ripetitore. A differenza della modalità Failover, questa modalità ottimizza l'efficienza complessiva del throughput bilanciando il carico del traffico su tutte le interfacce disponibili.

**Nota**: non è garantito che le connessioni o il traffico esistenti siano in linea con il rapporto di carico. La distribuzione effettiva si avvicinerà gradualmente al rapporto configurato con un uso prolungato.

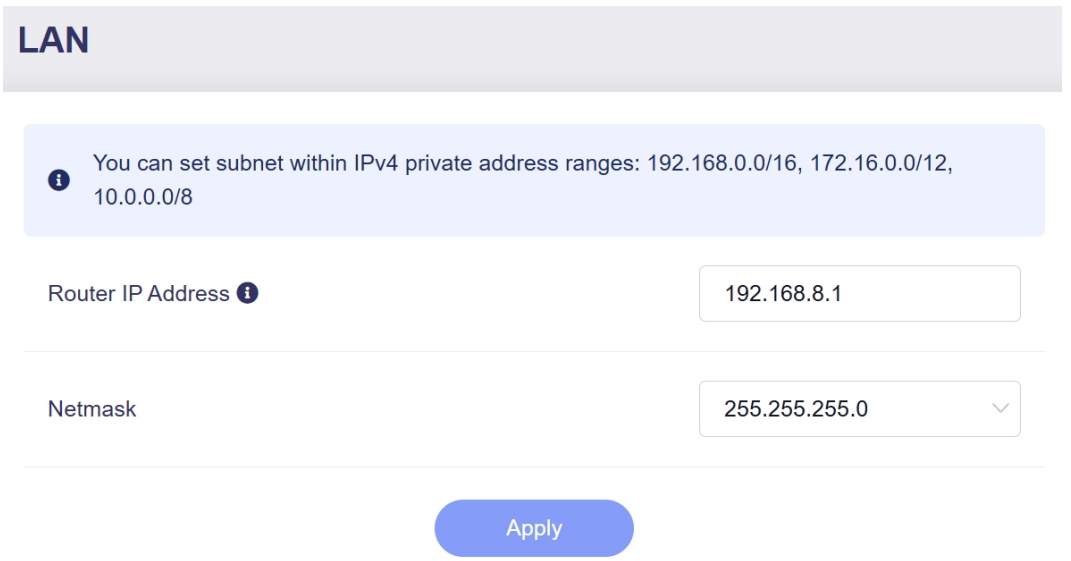
## 13.3 LAN

LAN (Local Area Network) si riferisce alla rete locale privata, alla quale i tuoi dispositivi si collegano tramite cavi Ethernet.

Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **LAN**. Qui puoi configurare le impostazioni LAN, comprese le impostazioni di base, il server DHCP e la prenotazione degli indirizzi.

### 13.3.1 Impostazioni di base

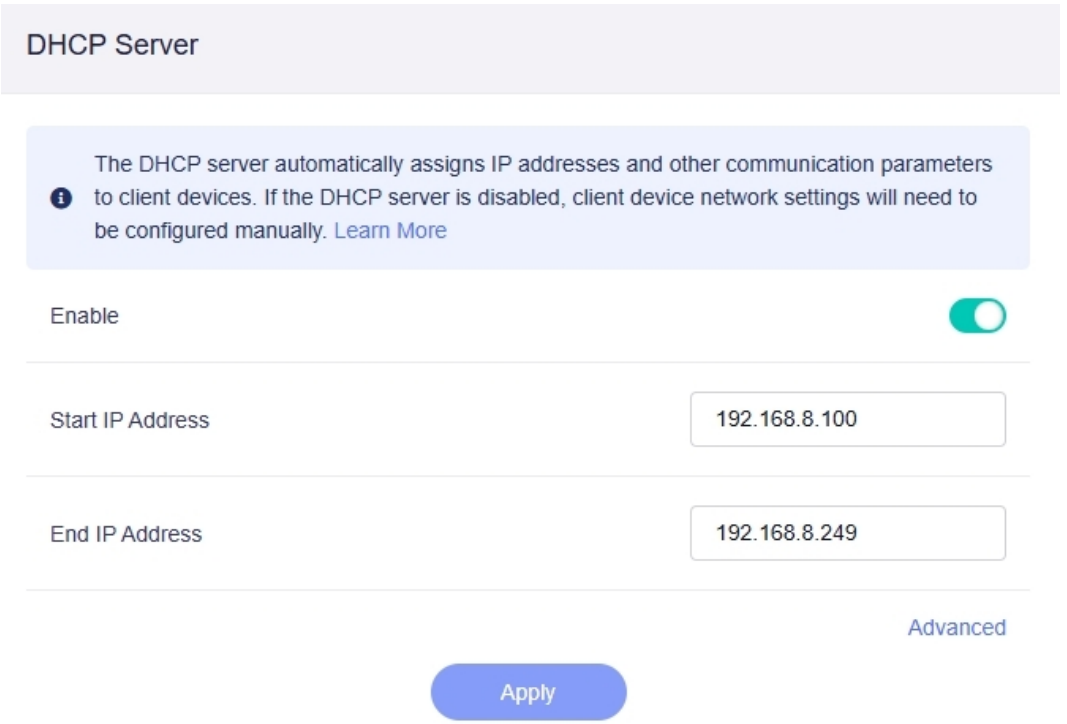
Le impostazioni di base includono l'indirizzo IP del router e Maschera di rete. È possibile impostare la sottorete all'interno degli intervalli di indirizzi privati IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



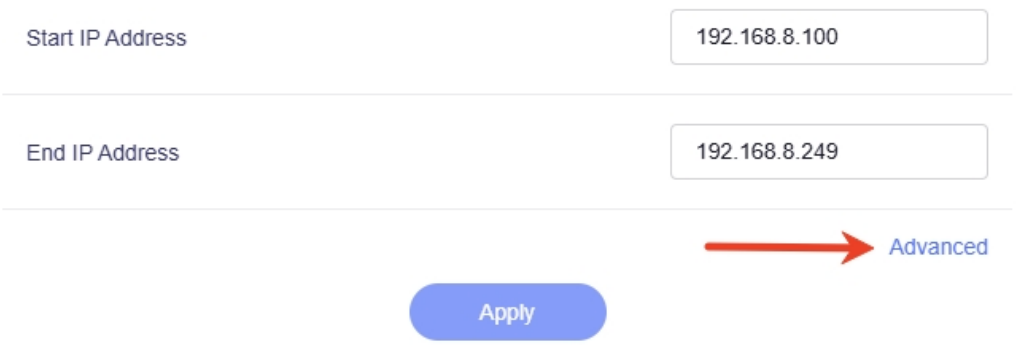

- **Indirizzo IP del router**: questo è l'indirizzo inserito nella barra degli indirizzi del browser per accedere al pannello di amministrazione del router. Per impostazione predefinita è 192.168.8.1 e può essere modificato se è in conflitto con la rete upstream.
- **Maschera di rete**: sono disponibili due opzioni: 255.255.255.0 e 255.255.0.0.

## 13.3.2 Server DHCP

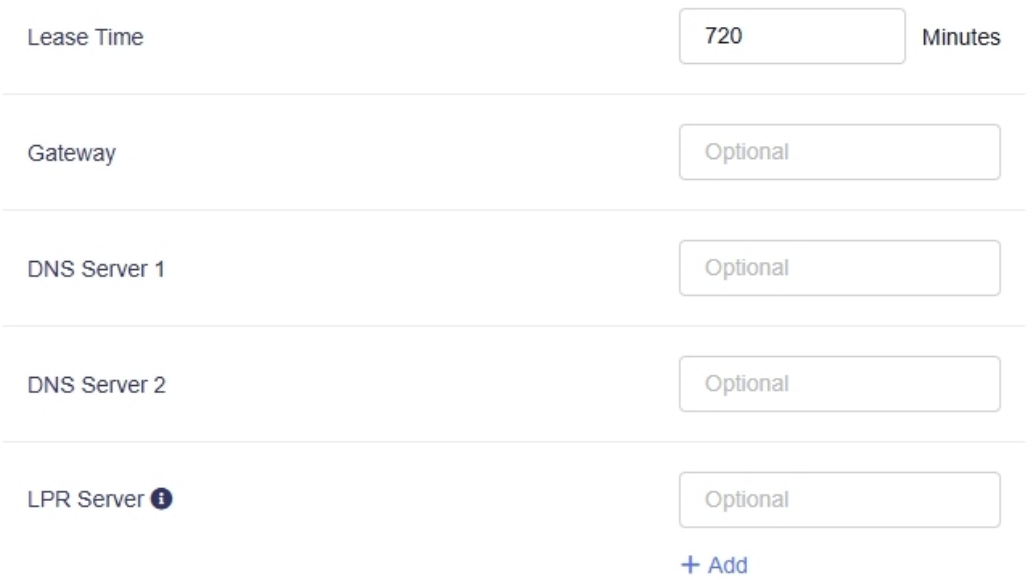
Il server DHCP assegna automaticamente indirizzi IP e altri parametri di comunicazione a ciascun client connesso. Il server DHCP del router GL.iNet è abilitato per impostazione predefinita e il pool di indirizzi IP del server DHCP varia da 192.168.8.100 a 192.168.8.249. Se necessario, è possibile personalizzare l'intervallo di indirizzi.




Fai clic su **Avanzate** nell'angolo in basso a destra.




Sarai in grado di configurare impostazioni avanzate, tra cui durata del lease, gateway, server DNS e server LPR.




- **Durata del lease**: la durata per la quale un dispositivo può utilizzare un indirizzo IP assegnato tramite DHCP.
- **Gateway**: il componente router che instrada il traffico tra la rete locale e le reti esterne (ad esempio Internet).
- **Server DNS 1**: il server primario responsabile della traduzione dei nomi di dominio in indirizzi IP.
- **Server DNS 2**: un server di backup utilizzato per risolvere i nomi di dominio se il server DNS primario fallisce.
- **Server LPR**: (Line Printer Remote Server) un servizio che gestisce i lavori di stampa e consente ai dispositivi in rete di inviare richieste di stampa a stampanti remote. È possibile configurare più porte LPR per stampanti.

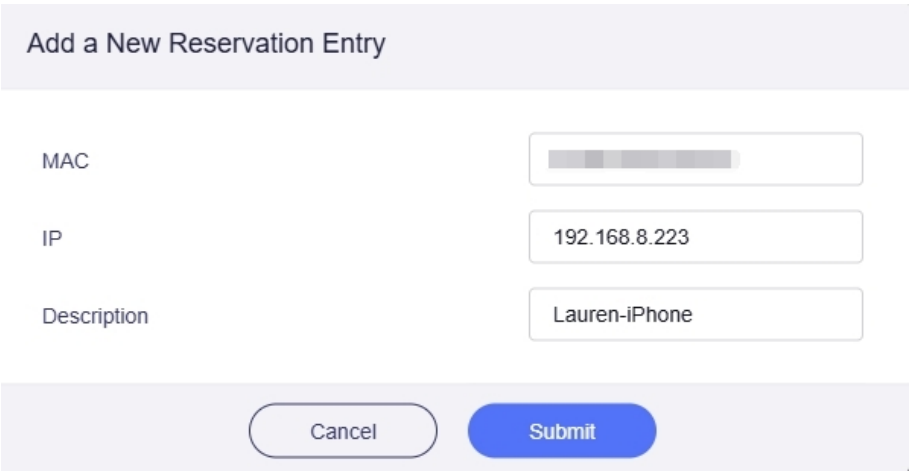
**Nota**: se il server DHCP è disabilitato, è necessario configurare manualmente l'IP statico e altri parametri di comunicazione per ciascun client. Vedi qui per i dettagli.

## 13.3.3 Prenotazione indirizzi

La prenotazione dell'indirizzo consente di specificare un indirizzo IP fisso per un client LAN, in modo che il client riceva sempre lo stesso indirizzo IP ogni volta che accede al server DHCP del router. È possibile assegnare indirizzi IP riservati a computer o server che richiedono impostazioni IP permanenti. Tieni presente che i client con la prenotazione dell'indirizzo configurata devono riconnettersi al router per attivare l'impostazione.

Segui i passaggi seguenti per configurare la prenotazione degli indirizzi, se necessario.

1. Accedi al pannello di amministrazione web del tuo router, vai su **RETE** > **LAN** > **Prenotazione indirizzi** e fai clic su **Aggiungi**.
2. Nella finestra pop-up, seleziona l'indirizzo MAC dall'elenco a discesa, quindi l'indirizzo IP corrispondente per il MAC selezionato verrà compilato automaticamente. Inserisci un nome descrittivo e fai clic su **Invia**.




3. Dopo aver aggiunto una nuova prenotazione dell'indirizzo IP, la pagina visualizzerà la voce riservata, come mostrato di seguito.



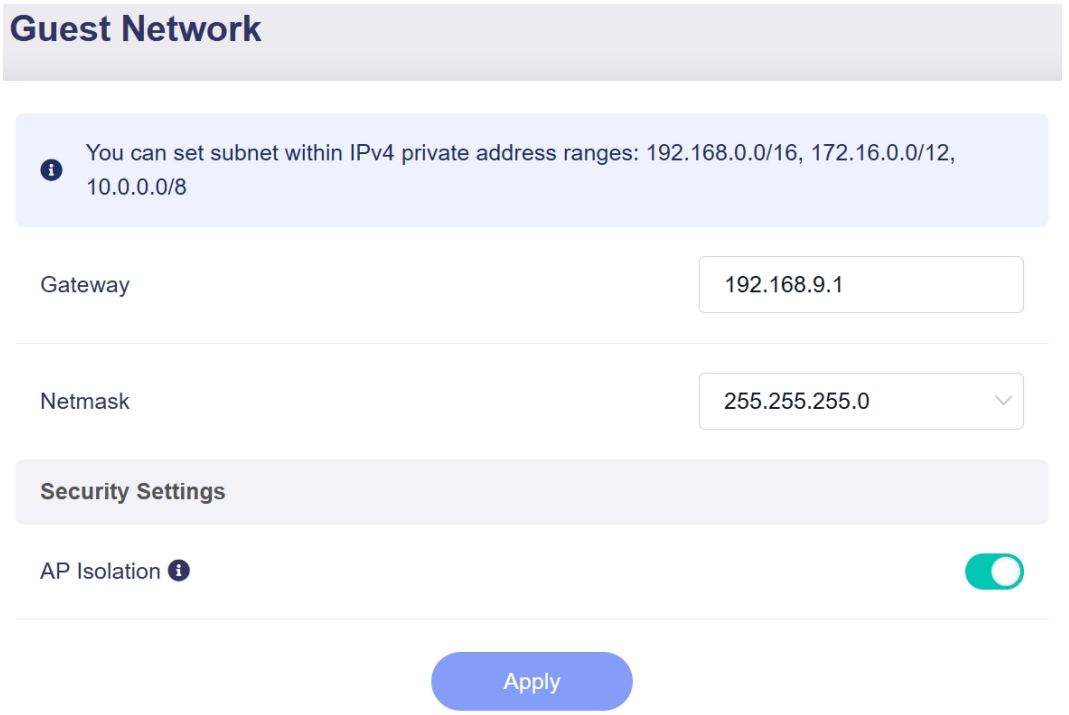
## 13.4 Rete ospiti

La rete ospiti si riferisce a una rete dedicata a cui i visitatori possono connettersi, isolandoli dalla tua LAN principale per proteggere la sicurezza della tua rete privata.

Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **Rete ospiti**. Questa pagina consente di configurare le impostazioni di Rete ospiti, incluse le impostazioni di base e il server DHCP.

### 13.4.1 Impostazioni di base

Le impostazioni di base includono Gateway, Maschera di rete e Isolamento AP.

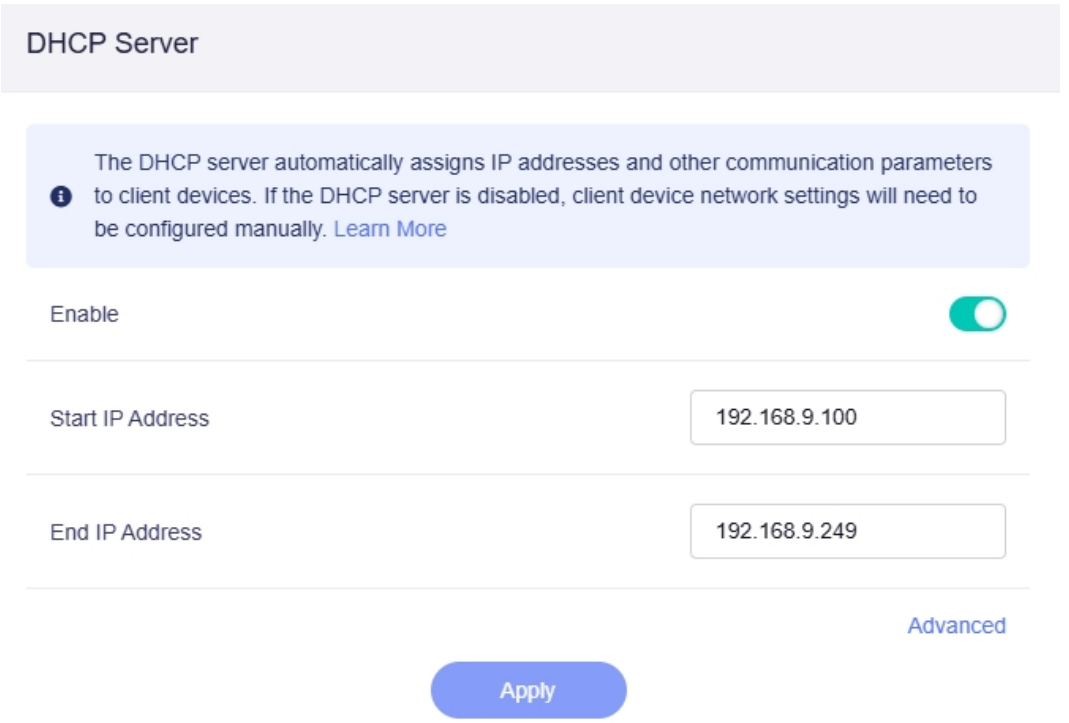



- **Gateway**: di default è 192.168.9.1 e può essere modificato se necessario, ma non deve entrare in conflitto con il gateway della rete principale.
- **Maschera di rete**: sono disponibili due opzioni: 255.255.255.0 e 255.255.0.0.
- **Isolamento AP**: viene utilizzato per isolare i client della rete ospiti in segmenti separati in modo che non possano comunicare con altri dispositivi sulla stessa rete.

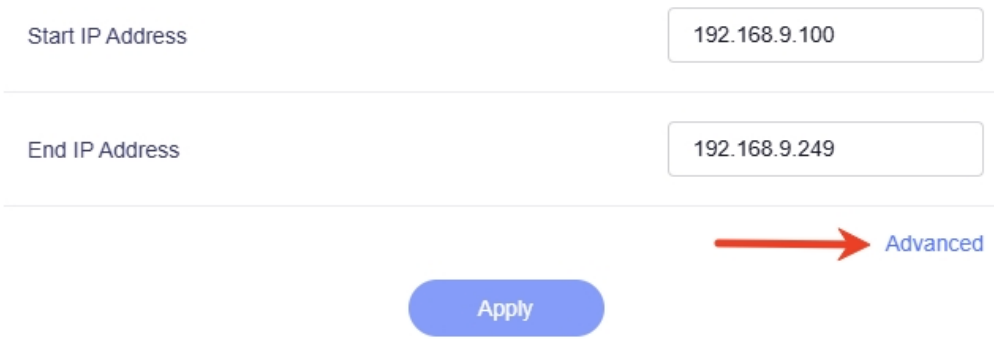
## 13.4.2 Server DHCP

Poiché la rete ospiti è disabilitata per impostazione predefinita, il suo server DHCP è disabilitato e nascosto finché non viene abilitato manualmente.

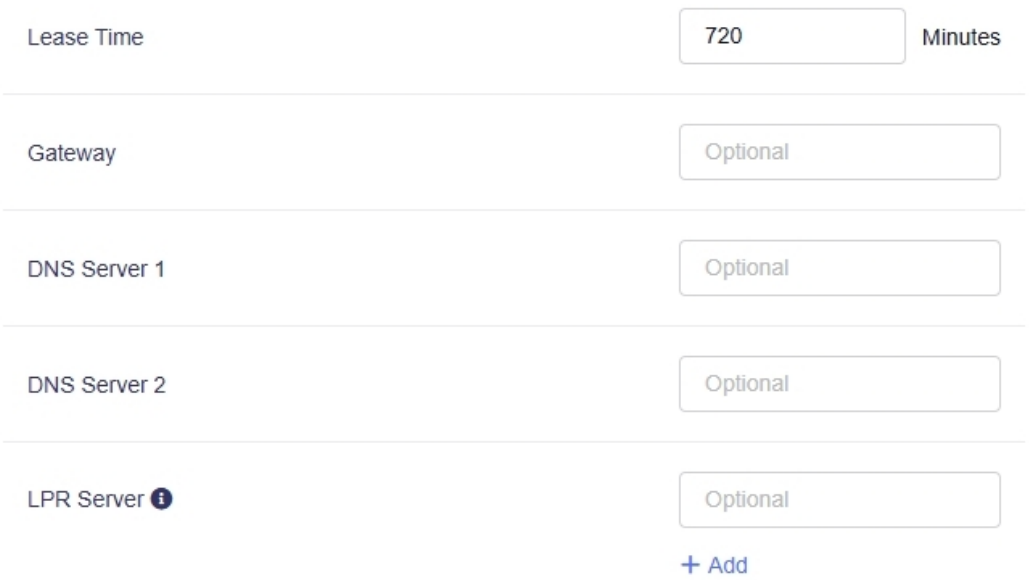
Se abilitato, il server DHCP assegna automaticamente indirizzi IP e altri parametri di comunicazione a ciascun client connesso. Il pool di indirizzi IP del server DHCP per la rete ospiti varia da 192.168.9.100 a 192.168.9.249. Se necessario, puoi personalizzare l'intervallo di indirizzi.




Fai clic su **Avanzate** nell'angolo in basso a destra.




Sarai in grado di configurare impostazioni avanzate, tra cui durata del lease, gateway, server DNS e server LPR.




- **Durata del lease**: la durata durante la quale un dispositivo può utilizzare un indirizzo IP assegnato tramite DHCP della rete ospiti.
- **Gateway**: il componente router che instrada il traffico tra la rete ospiti e le reti esterne (ad esempio Internet).
- **Server DNS 1**: il server primario responsabile della traduzione dei nomi di dominio in indirizzi IP.
- **Server DNS 2**: un server di backup utilizzato per risolvere i nomi di dominio se il server DNS primario fallisce.
- **Server LPR**: (Line Printer Remote Server) un servizio che gestisce i lavori di stampa e consente ai dispositivi in rete di inviare richieste di stampa a stampanti remote. È possibile configurare più porte LPR per stampanti.

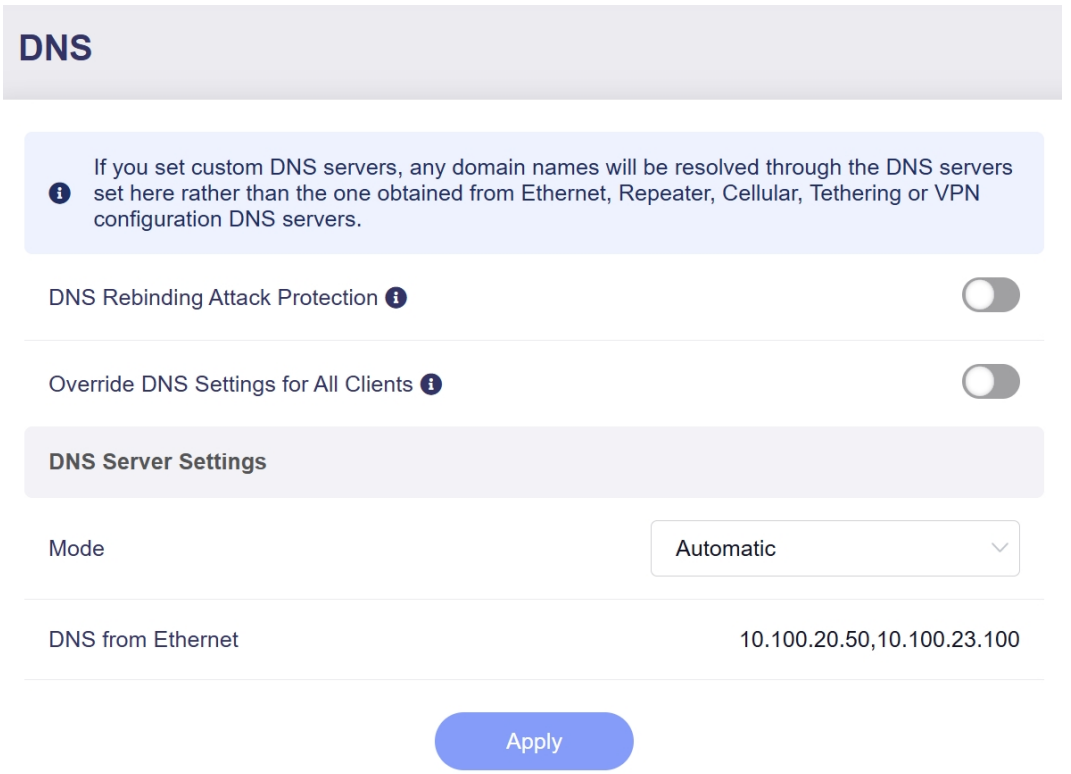
## 13.5 DNS

DNS (Domain Name System) è un servizio che traduce nomi di dominio leggibili dall'uomo, come www.google.com, in indirizzi IP in modo che i dispositivi possano individuare e connettersi a siti Web e servizi online.

Su un router, le impostazioni DNS solitamente determinano quali server DNS vengono utilizzati dai dispositivi connessi. Nella maggior parte dei casi, il router ottiene automaticamente gli indirizzi dei server DNS dall'ISP o dalla rete upstream oppure consente agli utenti di specificare manualmente i server DNS pubblici, come 8.8.8.8, nell'interfaccia di gestione web. Una volta configurate, queste impostazioni DNS vengono generalmente distribuite automaticamente ai dispositivi collegati, quindi non è necessario configurare il DNS separatamente su ciascun dispositivo.

Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **DNS**. Questa pagina ti consente di configurare le impostazioni relative al DNS.

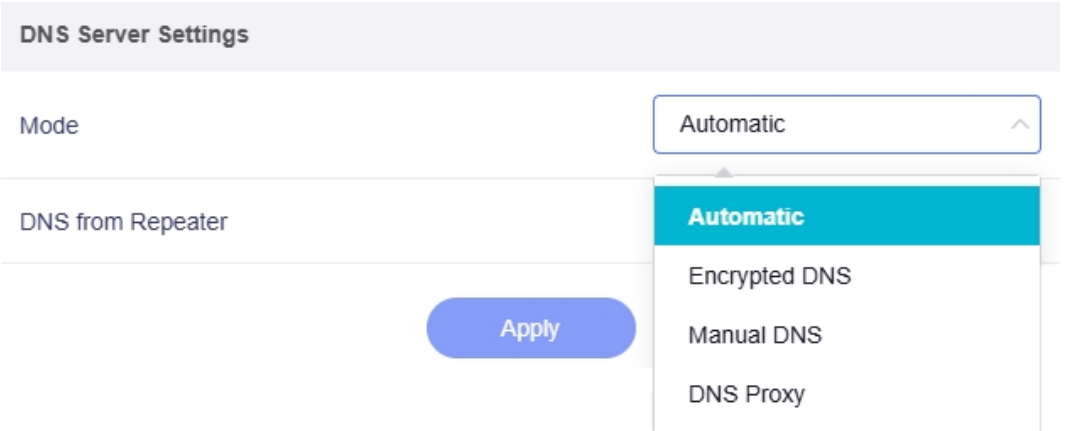
### 13.5.1 Impostazioni generali



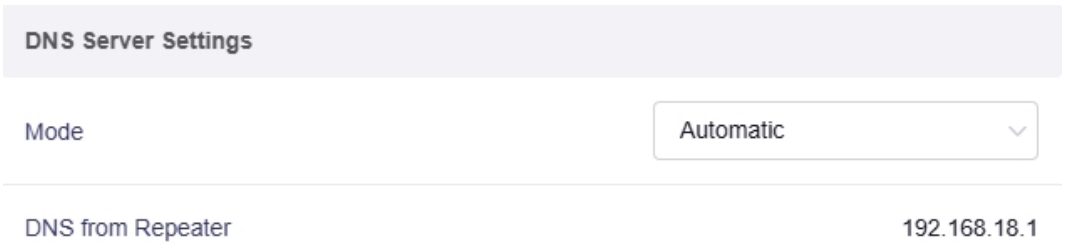
- **Protezione dagli attacchi di riassociazione DNS**: protegge dagli attacchi di riassociazione DNS bloccando i tentativi dannosi di risoluzione DNS. Tieni presente che abilitarlo potrebbe causare un errore di ricerca DNS privato; disabilitalo se la tua rete utilizza un captive portal (ad esempio, pagine di accesso Wi-Fi pubbliche).
- **Sostituisci le impostazioni DNS di tutti i client**: se abilitato, tutti i dispositivi connessi saranno costretti a utilizzare i server DNS configurati sul router, ignorando le proprie impostazioni DNS originali. Abilita la configurazione DNS unificata per tutti i dispositivi.

## 13.5.2 Impostazioni del server DNS

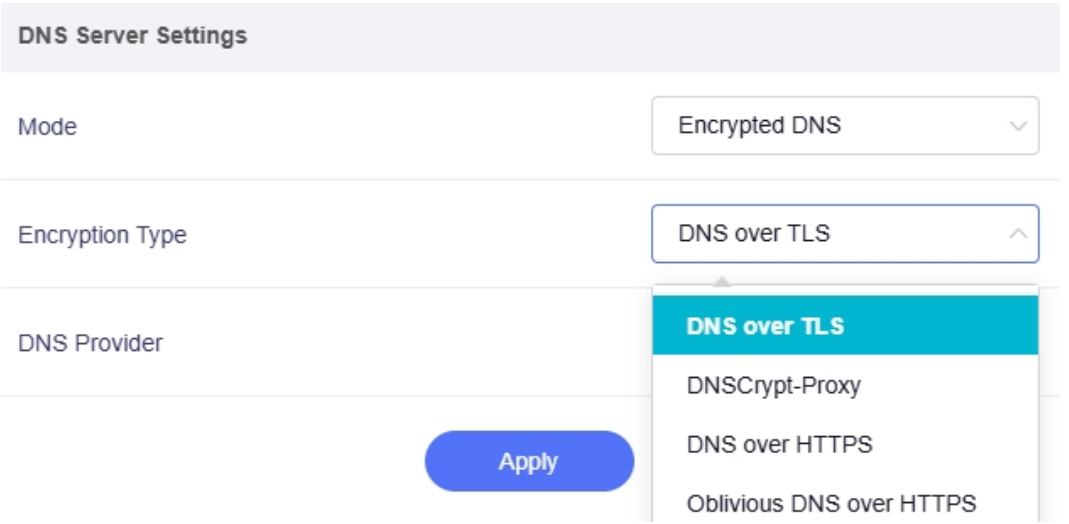
Esistono quattro modalità per il server DNS: automatico, DNS crittografato, DNS manuale e proxy DNS.




1. **Automatico**: se selezionato, il router otterrà automaticamente gli indirizzi del server DNS dalla rete upstream e li applicherà a tutti i dispositivi collegati.

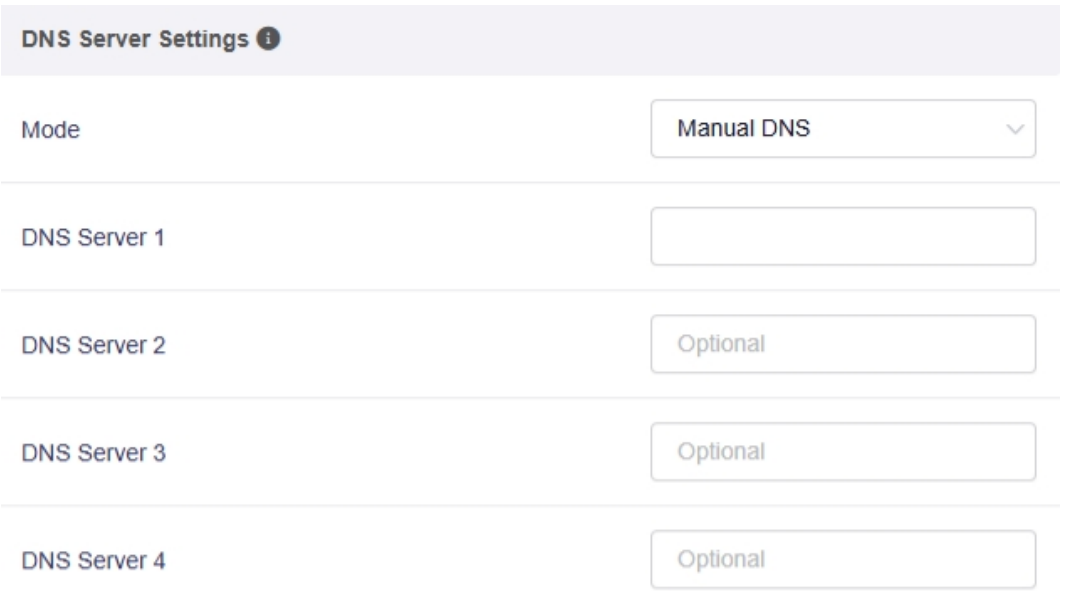



2. **DNS crittografato**: se selezionato, il router utilizzerà protocolli crittografati per elaborare le query DNS, proteggendo i dati di risoluzione da intercettazioni o manomissioni.
   Ha quattro tipi di crittografia: DNS su TLS, DNSCrypt-Proxy, DNS su HTTPS e Oblivious DNS su HTTPS.



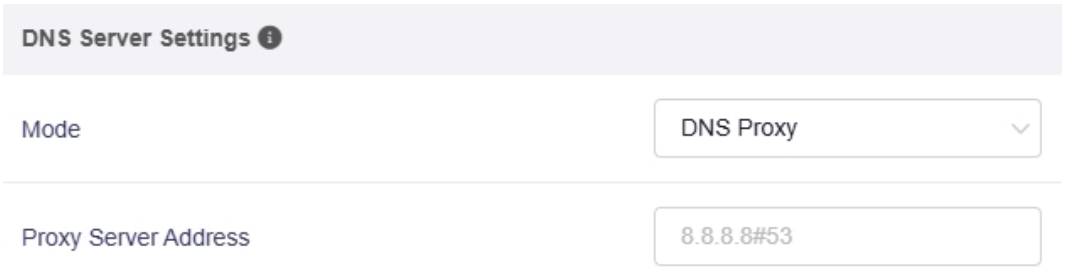

- Per DNS su TLS, seleziona un provider DNS tra Control D, NextDNS e Cloudflare.
- Per gli altri tre (ovvero DNSCrypt-Proxy, DNS over HTTPS e Oblivious DNS over HTTPS), seleziona almeno un server DNS dal repository. È possibile selezionare fino a server 8. Quando vengono selezionati più server, il router utilizzerà automaticamente quello più veloce.

3. **DNS manuale**: se selezionato, puoi personalizzare i server DNS del router. Fare clic su Server DNS 1 e scegliere un server DNS dall'elenco a discesa. I restanti campi DNS verranno aggiornati automaticamente.




**Nota**: se è necessario utilizzare indirizzi IPv6 per il DNS manuale, abilitare prima IPv6 sul router.

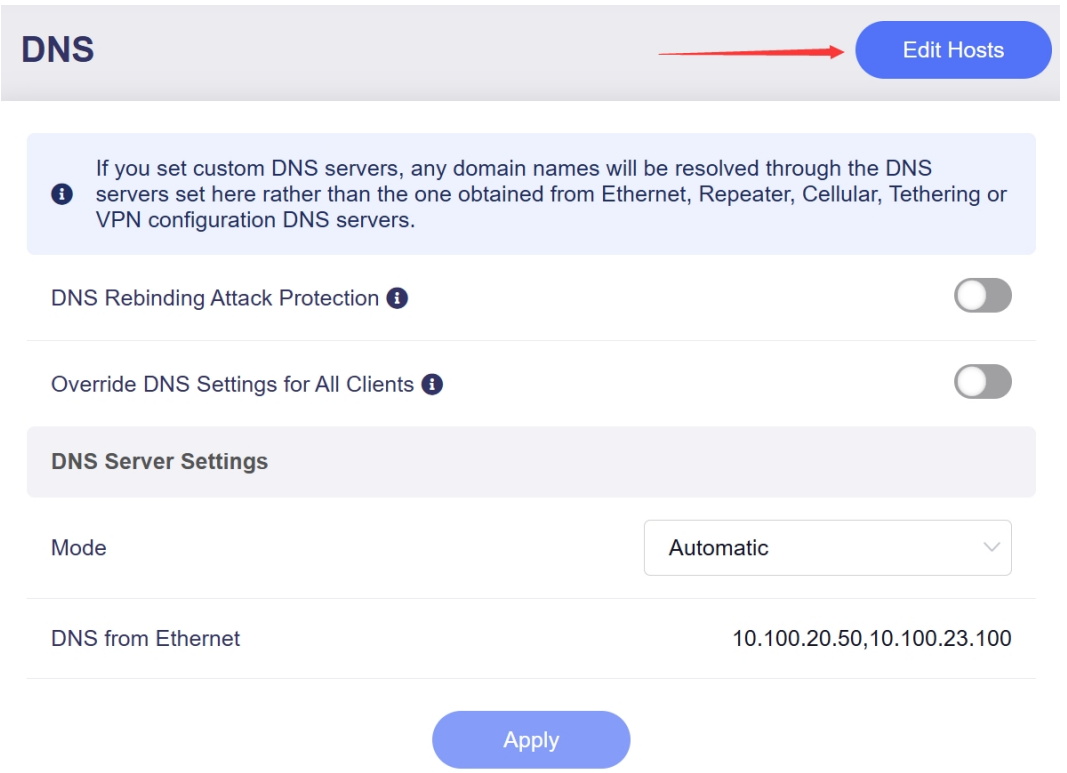
4. **Proxy DNS**: se selezionato, il router inoltra tutte le query DNS tramite un server proxy, consentendo la risoluzione tramite l'ambiente di rete del proxy per esigenze di accesso specifiche.



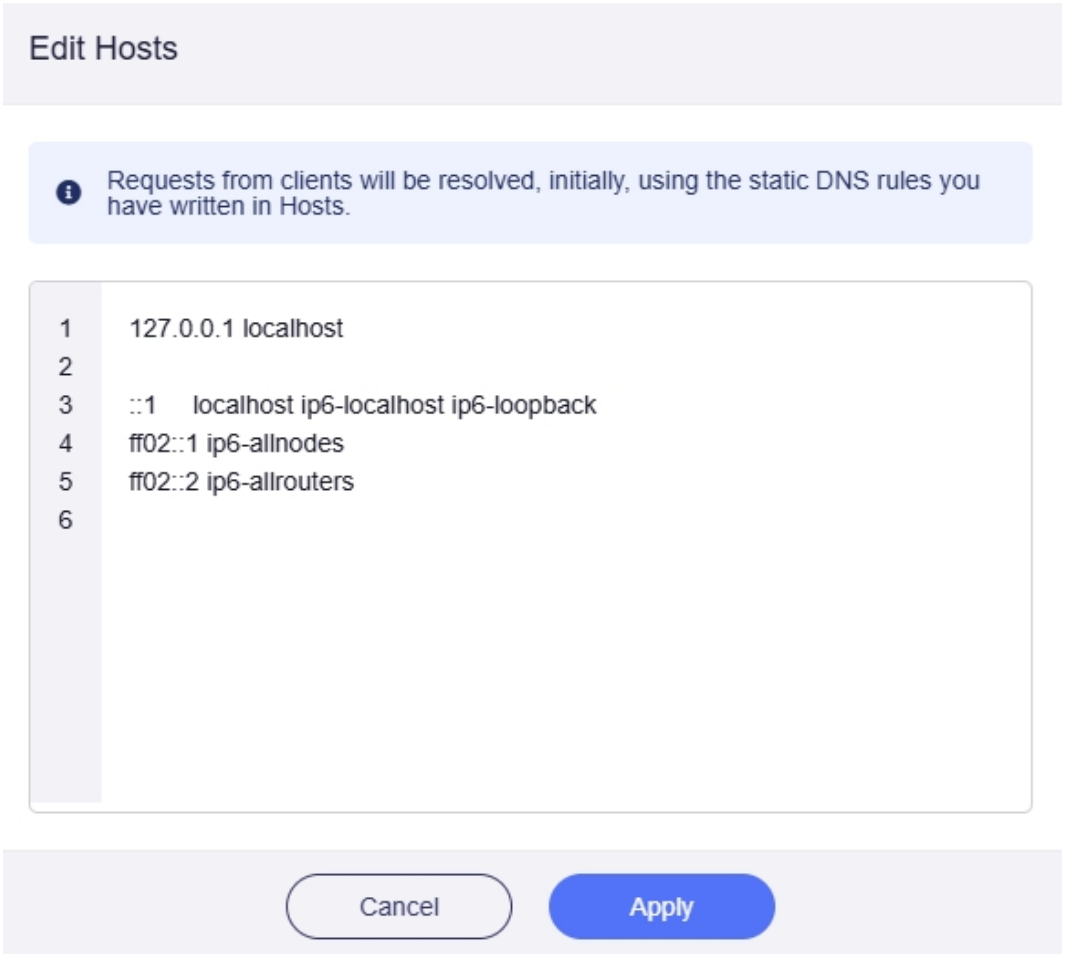

## 13.5.3 Modifica del file hosts

Puoi definire regole di risoluzione DNS statiche, se necessario.

Nella pagina DNS, fai clic su **Modifica del file hosts** nell'angolo in alto a destra.



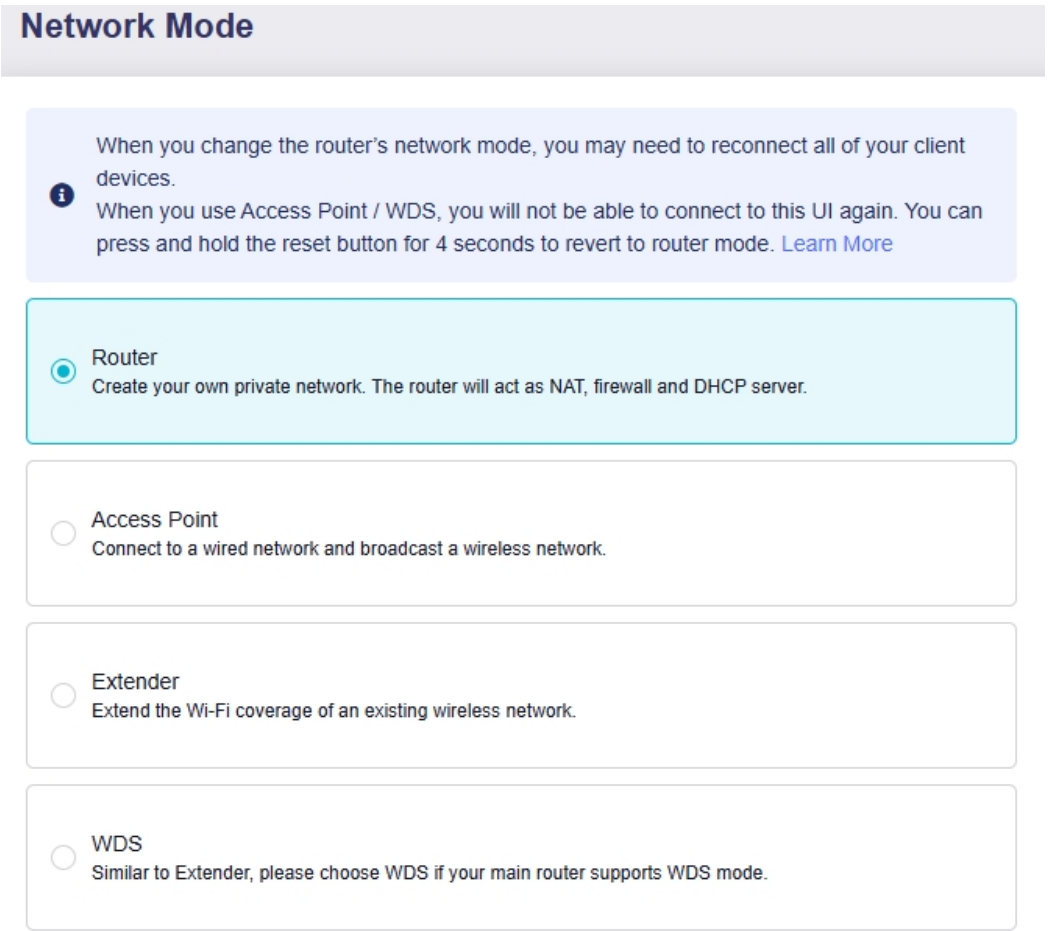

Le richieste dei client verranno risolte preferenzialmente utilizzando le regole DNS statiche scritte qui, consentendoti di mappare manualmente gli indirizzi IP sui nomi host (ad esempio, le voci predefinite come 127.0.0.1 localhost per il loopback locale) per il controllo personalizzato della risoluzione dei nomi di dominio.


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

## 13.6 Modalità di rete

La modalità di rete si riferisce ai diversi ruoli operativi e funzioni che un router può assumere per soddisfare le varie esigenze di distribuzione della rete.

Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Modalità di rete**. Puoi modificare la modalità di rete del tuo router.




- **Router**: questa è la modalità operativa predefinita per la maggior parte dei router domestici e di piccoli uffici, progettata per creare una rete locale privata (LAN) e fungere da gateway dedicato tra Internet pubblica e i dispositivi connessi. In questa modalità, il router abilita le funzioni principali tra cui NAT, DHCP e un firewall integrato. Si collega a una linea a monte come la fibra a banda larga, assegna automaticamente indirizzi IP privati ai dispositivi collegati e fornisce sicurezza di rete per l'intera rete privata.
- **Punto di accesso**: questa modalità consente a un router di connettersi a una rete cablata tramite un cavo LAN e trasmettere segnali wireless, espandendo la copertura Wi-Fi in ampi spazi per consentire a più dispositivi di accedere alla rete. In questa

modalità, il router disabilita le funzioni NAT e DHCP, funzionando esclusivamente come trasmettitore e switch di segnale wireless anziché come gateway autonomo.

- **Extender**: questa modalità è progettata per estendere la copertura Wi-Fi di una rete wireless esistente ed eliminare le zone senza segnale nelle aree con scarsa connettività. Consente al router di ricevere segnali in modalità wireless dal router principale, amplificarli e ritrasmettere il segnale potenziato. A differenza della modalità Punto di accesso, non richiede una connessione cablata al router principale, ma può portare al dimezzamento della larghezza di banda, poiché il dispositivo deve gestire la ricezione e la trasmissione simultanea del segnale.
- **WDS**: la modalità Wireless Distribution System (WDS) è simile alla modalità Extender poiché estende la copertura Wi-Fi in modalità wireless, ma supporta il bridging wireless tra più router compatibili. È consigliato per l'espansione della rete wireless quando il router upstream dispone della funzionalità WDS.

  Questa modalità è ideale per scenari come la copertura di edifici a più piani o piccoli uffici in cui più router devono lavorare insieme per formare una rete wireless unificata. A differenza della modalità Extender, che trasmette segnali solo da un router principale a un singolo extender, la modalità WDS consente ai router interconnessi di inviare e ricevere segnali, consentendo una copertura continua su aree più grandi con più nodi di segnale.

**Nota**:

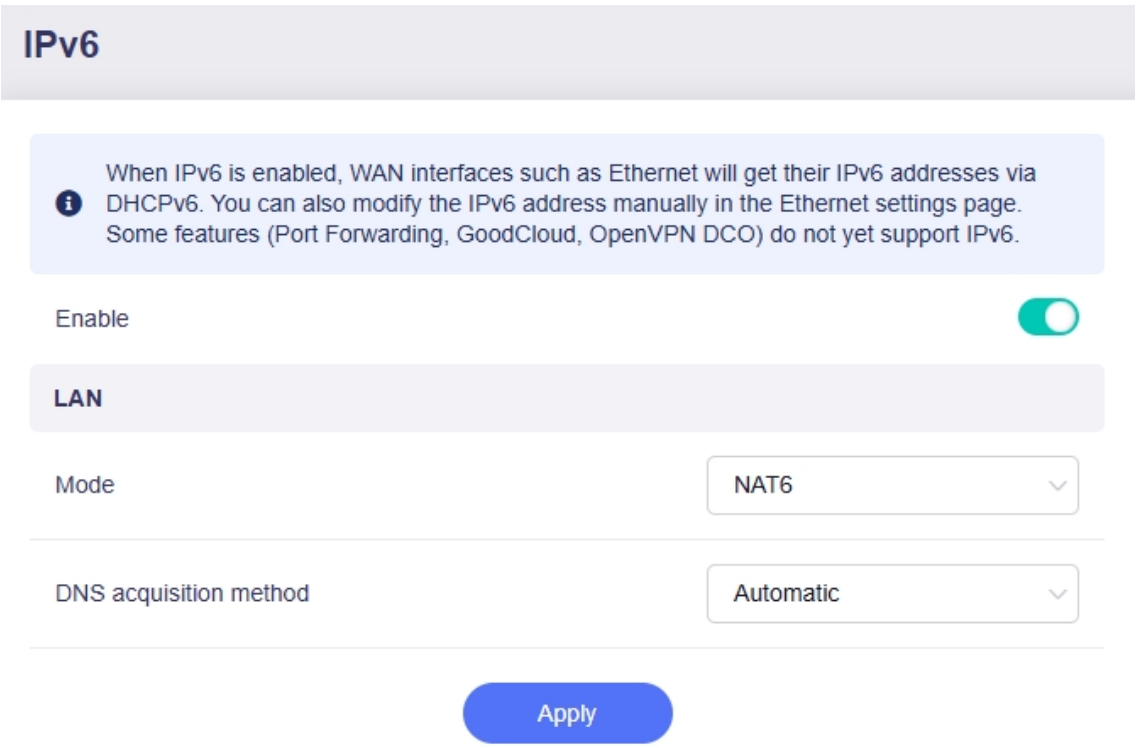
1. Quando la modalità di rete viene modificata, tutti i dispositivi client devono riconnettersi al router per una connettività di rete stabile.
2. **In modalità Punto di accesso / WDS, non sarai in grado di accedere al pannello di amministrazione web utilizzando l'indirizzo IP originale**. È invece necessario accedere al router upstream per trovare l'indirizzo IP assegnato a questo router, quindi utilizzare questo indirizzo IP per accedere al pannello di amministrazione web. Se non hai accesso al router upstream, tieni premuto il pulsante di ripristino per 4 secondi per ripristinare la modalità router predefinita.
3. **In modalità Punto di accesso / Extender / WDS, le seguenti funzionalità non saranno disponibili**: Controllo degli accessi (Lista consentita e Blocklist), VPN, AdGuard Home, Controllo parentale, ZeroTier, Tailscale, Firewall, Multi-WAN, Server DHCP, Prenotazione indirizzi, Rete ospiti, DNS, IPv6, Gateway drop-in, IGMP Snooping, Impostazioni NAT.

## 13.7 IPv6

IPv6 (protocollo Internet versione 6) è l'ultimo protocollo Internet progettato per sostituire IPv4. Offre un pool più ampio di IP univoci, risolvendo il problema dell'esaurimento degli indirizzi di IPv4 e supportando il numero crescente di dispositivi connessi a livello globale.

Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **IPv6**. Questa pagina ti consente di abilitare e configurare IPv6 sul tuo router. Quando IPv6 è abilitato, le interfacce WAN come Ethernet otterranno i propri indirizzi IPv6 tramite DHCPv6.

Attiva **Abilita**, seleziona la modalità per la rete principale e il metodo di acquisizione DNS, quindi fai clic su **Applica.**




**Nota**: alcune funzionalità (ad esempio firewall, GoodCloud) non supportano ancora IPv6. Se abiliti queste funzionalità e IPv6 contemporaneamente, è probabile che si verifichino problemi di connettività.

### 13.7.1 Modalità IPv6

Sono disponibili quattro modalità: Nativo, Passthrough, NAT6 e IPv6 statico.

- **Nativo**: questa modalità è applicabile quando il router ottiene direttamente un indirizzo IPv6 pubblico e assegna automaticamente gli indirizzi IPv6 ai dispositivi online. Questa modalità può soddisfare le esigenze di accesso IPv6 della maggior parte degli utenti.
- **Passthrough**: questa modalità è applicabile quando i pacchetti IPv6 devono essere passati direttamente senza alcuna elaborazione o conversione. Ad esempio, alcune applicazioni o servizi specifici potrebbero richiedere la completa conservazione del contenuto del pacchetto IPv6 per ulteriori elaborazioni o analisi. Questa modalità viene utilizzata dal personale tecnico per il debug della rete o l'analisi della sicurezza.
- **NAT6**: questa modalità è adatta per scenari in cui un router viene utilizzato come gateway per assegnare indirizzi IPv6 interni dinamici a ciascun dispositivo sulla rete. In questa modalità, i dispositivi terminali si connettono tramite un terminale di rete ottica e ottengono un indirizzo IPv6 di rete locale.
- **IPv6 statico**: questa modalità è adatta per dispositivi o servizi che richiedono un indirizzo IPv6 fisso, come server o stampanti di rete. Questa modalità garantisce che il dispositivo utilizzi sempre lo stesso indirizzo IPv6, facilitandone la gestione e l'accesso.

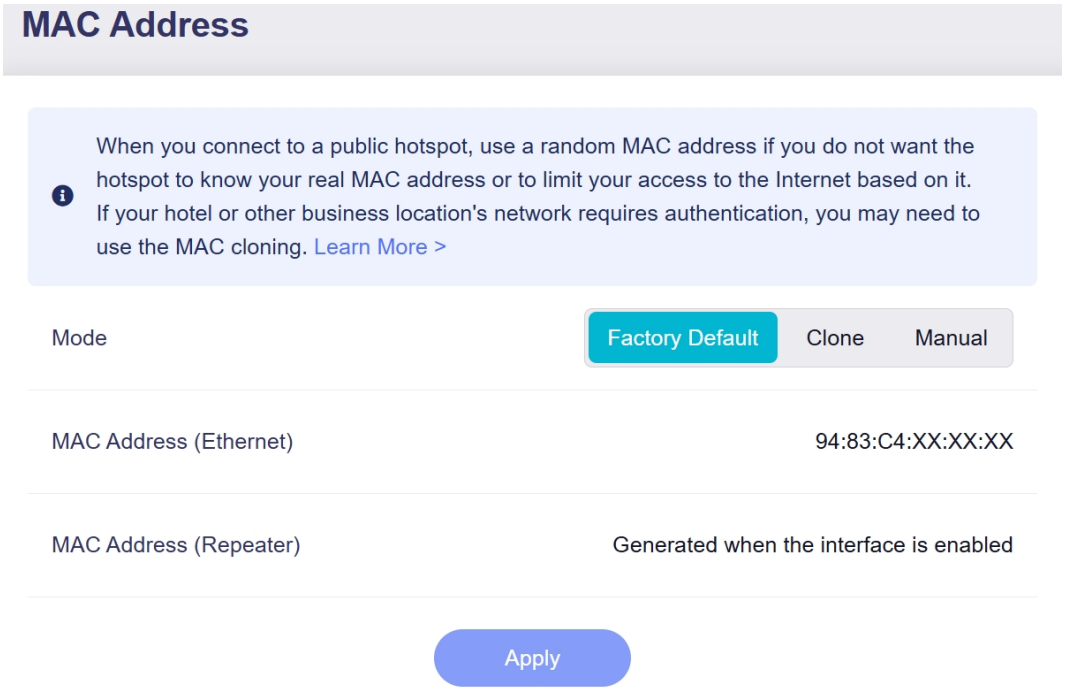
### 13.7.2 Metodo di acquisizione DNS

Determina il modo in cui il router ottiene gli indirizzi del server DNS IPv6. Sono disponibili due opzioni: Automatico e Manuale.

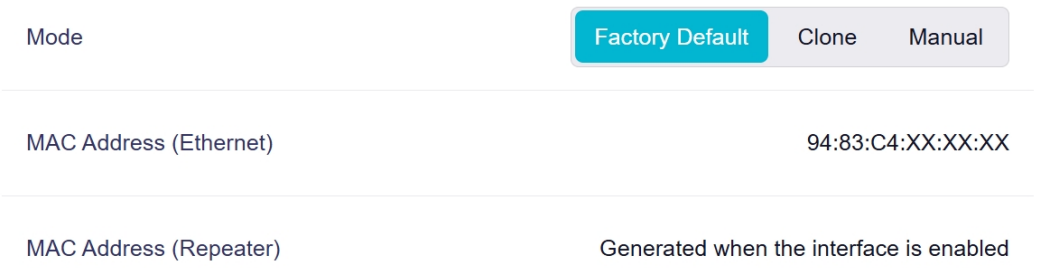
- **Automatico**: il router otterrà gli indirizzi del server DNS IPv6 in modo dinamico (ad esempio tramite DHCPv6).
- **Manuale**: inserisci gli indirizzi del server DNS IPv6 personalizzati. Tuttavia, poiché il DNS viene utilizzato per risolvere i nomi di dominio negli indirizzi IP corrispondenti, la configurazione manuale del server DNS potrebbe causare errori di ricerca DNS. Si prega di utilizzarlo con cautela.

## 13.8 Indirizzo MAC

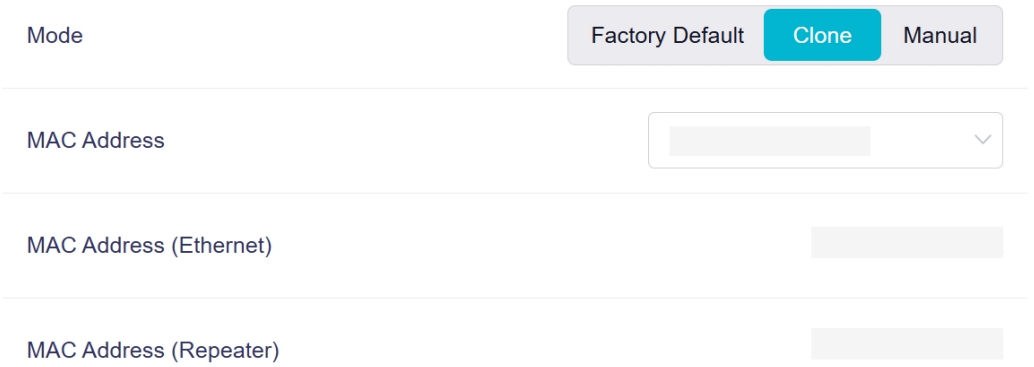
La pagina Indirizzo MAC visualizza l'indirizzo MAC predefinito del router, clona l'indirizzo MAC di uno client, immetti manualmente un indirizzo MAC o genera un indirizzo MAC casuale. Se il dispositivo supporta l'impostazione di più porte Ethernet da utilizzare come porte WAN, è possibile impostare l'indirizzo MAC per ciascuna porta separatamente. Tieni presente che l'impostazione dell'indirizzo MAC è valida solo quando la porta Ethernet viene utilizzata come porta WAN.




- **L'indirizzo MAC predefinito di fabbrica.**

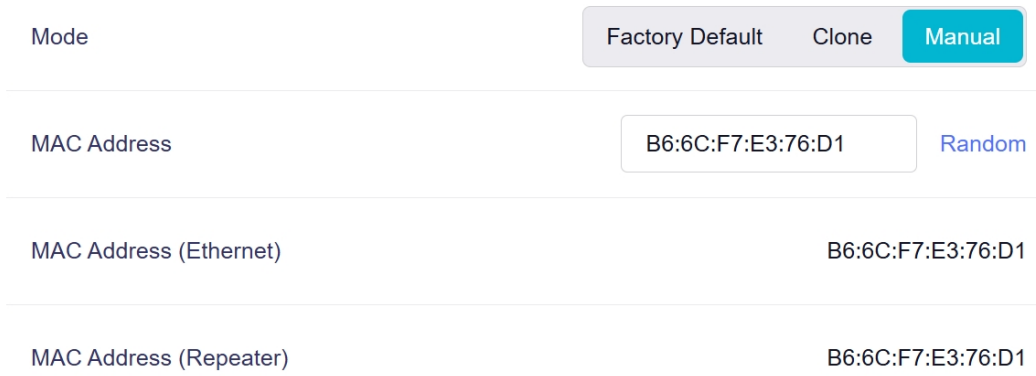



- **Clona l'indirizzo MAC di un client.**




**Nota**: molti nuovi dispositivi ora utilizzano un indirizzo MAC casuale diverso per connettersi a diversi Wi-Fi, quindi l'indirizzo MAC mostrato qui potrebbe non essere l'indirizzo MAC effettivo del dispositivo dell'utente. Il MAC randomizzato può anche essere chiamato indirizzo privato Wi-Fi o indirizzo hardware casuale su diversi dispositivi.

- **Inserimento manuale o generazione di un indirizzo MAC casuale.**

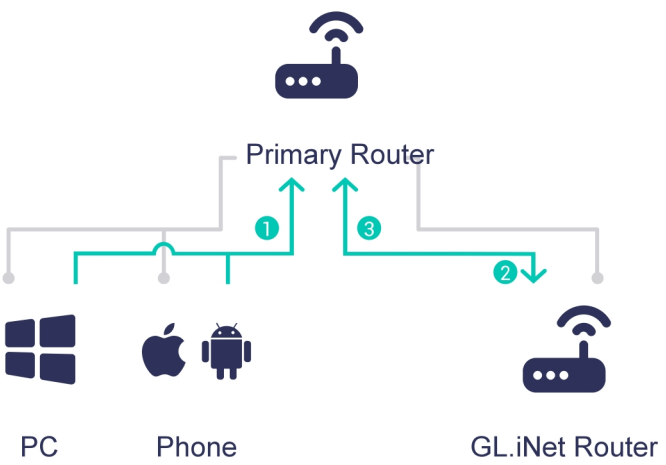


## 13.9 Gateway drop-in

Gateway drop-in è una funzione di estensione che consente l'espansione delle capacità di un router primario esistente senza sostituirlo o riconfigurarlo. Collegando il router GL.iNet al router primario tramite un cavo Ethernet, gli utenti possono aggiungere funzionalità avanzate all'infrastruttura di rete esistente, ad esempio:

- Filtra annunci tramite AdGuard Home
- Abilita client VPN
- Utilizza DNS crittografato

Gateway drop-in funziona come un sistema di rete intermedio, instradando il traffico dati dai dispositivi client attraverso il router GL.iNet per l'elaborazione prima di trasmetterlo tramite il router primario. Durante questo processo, non solo preserva le impostazioni di rete esistenti per garantire una connettività ininterrotta per tutti i dispositivi collegati, ma consente anche di gestire il traffico di rete per tutti o specifici dispositivi client, se necessario.



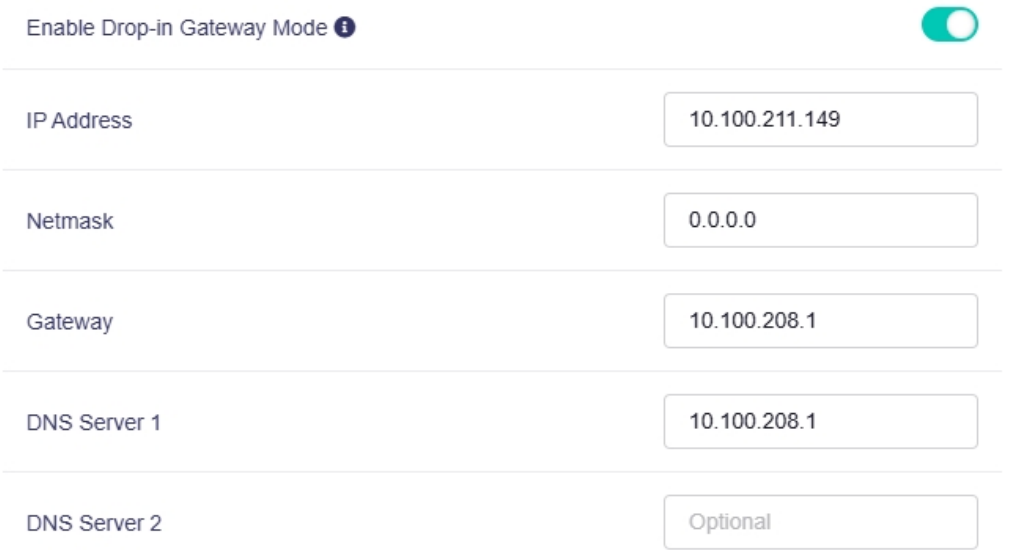

Il diagramma sopra è costituito da due tipi di linee: linee grigie e linee verdi contrassegnate da tre frecce, ciascuna etichettata con un numero corrispondente.

- **Le linee grigie** illustrano la topologia della connessione fisica: i dispositivi client (ad esempio, computer, laptop) si collegano al router principale e la porta LAN del router primario si collega alla porta WAN del router GL.iNet (con Gateway drop-in abilitato) tramite un cavo Ethernet.

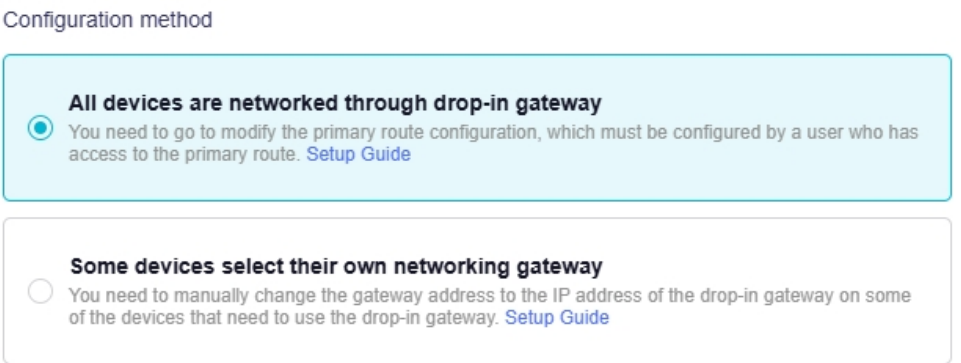
- **Le linee verdi** rappresentano il percorso sequenziale di trasmissione dei dati quando Gateway drop-in è attivo, con le frecce numerate che indicano l'ordine del flusso di traffico:
  1. Il traffico dai dispositivi client viene prima instradato al router primario;
  2. Il router primario inoltra il traffico al router GL.iNet per l'elaborazione (ad esempio, filtro degli annunci, crittografia VPN);
  3. Dopo l'elaborazione, il traffico viene rimandato al router primario, che poi consegna i dati finali ai dispositivi client originali o li instrada su Internet.

Segui i passaggi seguenti per abilitare Gateway drop-in se necessario.

1. Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Gateway drop-in**. Attiva **Abilita modalità gateway drop-in** e conferma i parametri di rete.



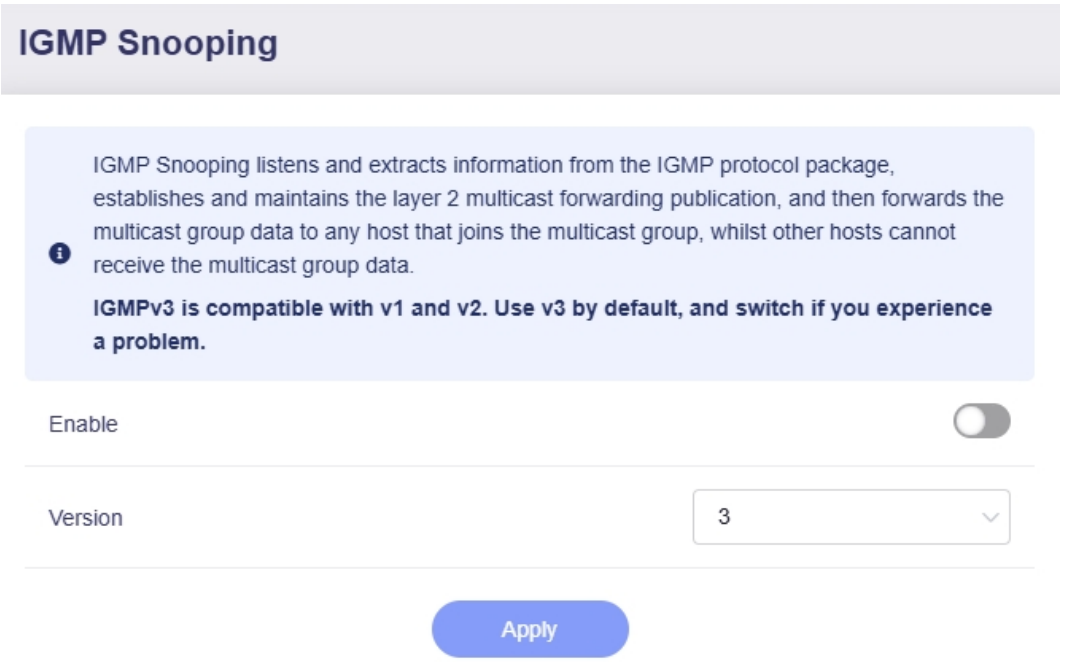

2. Seleziona il metodo di configurazione, quindi fai clic su **Applica**. Fare riferimento a questo tutorial per i dettagli.



## 13.10 IGMP Snooping

IGMP Snooping ascolta il pacchetto del protocollo IGMP, estrae le informazioni corrispondenti, stabilisce e mantiene la tabella di inoltro multicast di livello 2, quindi inoltra i dati del gruppo multicast all'host che si unisce al gruppo multicast, mentre gli altri host non possono ricevere i dati del gruppo multicast.

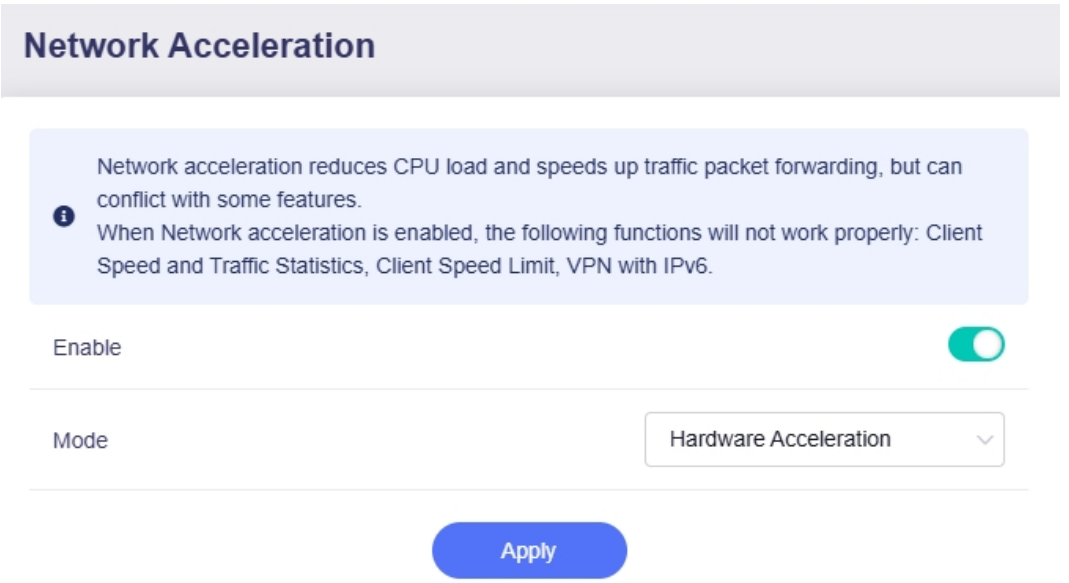
Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **IGMP Snooping**. Puoi abilitarlo per utilizzare la funzione multicast sul tuo router, se necessario.



## 13.11 Accelerazione di rete

L'accelerazione di rete riduce il carico della CPU e accelera l'inoltro dei pacchetti di traffico, ma può entrare in conflitto con alcune funzionalità.

Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Accelerazione di rete**. Questa pagina consente di abilitare Accelerazione di rete e selezionare la modalità Accelerazione hardware.

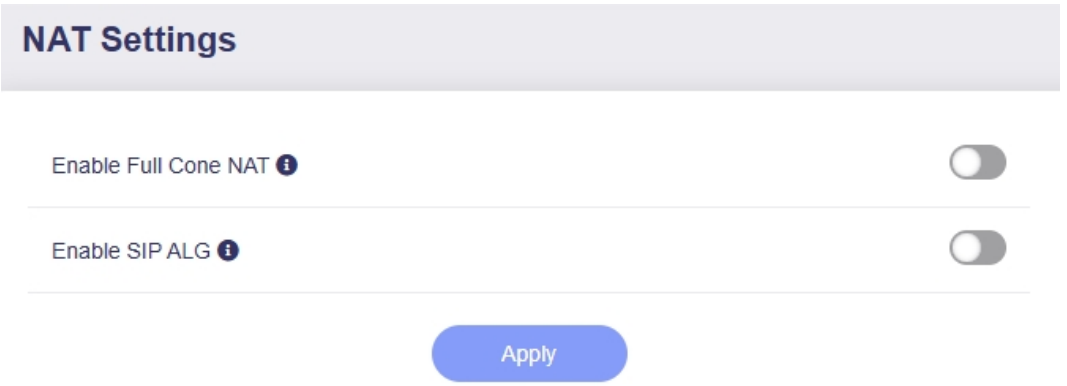



**La modalità Accelerazione hardware** scarica le attività di rete ad alta frequenza (ad esempio NAT, inoltro di pacchetti, verifica del checksum) su hardware dedicato come NPU o chip HWNAT. Funziona specificamente su connessioni Ethernet e Ripetitore, eccellendo in questi scenari con percorsi fissi e regole semplici per fornire un throughput elevato, bassa latenza e carico minimo della CPU per la trasmissione dei dati wire-speed.

**Nota**: quando Accelerazione di rete è abilitato, le seguenti funzioni non funzioneranno correttamente: statistiche sulla velocità del client, statistiche sul traffico, limite di velocità, Controllo parentale e VPN con IPv6.

## 13.12 Impostazioni NAT

Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **Impostazioni NAT**. Questa pagina ti consente di configurare due funzionalità chiave relative al NAT: Full Cone NAT e SIP ALG.




- **Full Cone NAT**: può essere utilizzato per ridurre la latenza del gioco, migliorando la reattività del gioco online. Tuttavia, abilitare Full Cone NAT potrebbe essere meno sicuro in quanto consente connessioni in entrata illimitate.
- **SIP ALG**: ha lo scopo di mitigare gli effetti di più NAT sul traffico SIP (Session Initiation Protocol). Tuttavia, nella maggior parte dei casi, non sarà di alcun aiuto e potrebbe addirittura influire sulle chiamate VoIP, causando problemi come audio unidirezionale, telefoni che non squillano, interruzioni impreviste delle chiamate o chiamate direttamente alla segreteria.

Capitolo 14

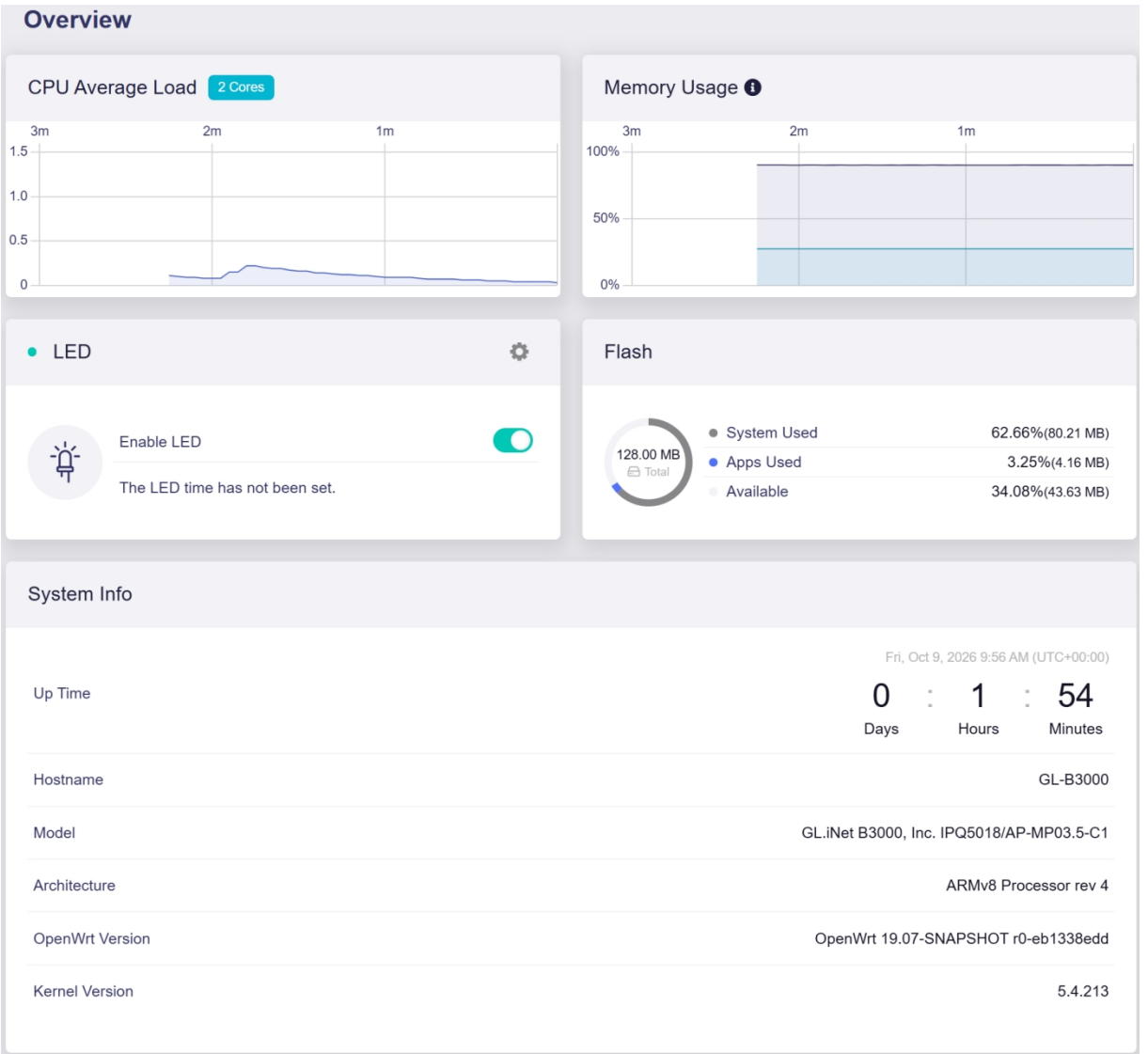
# Sistema

Questo capitolo tratta gli strumenti di gestione del sistema per il dispositivo, come panoramica del sistema, aggiornamento, attività pianificate, fuso orario, registro, ripristino del firmware e impostazioni avanzate.

# 14.1 Panoramica

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Panoramica**. Questa pagina mostra lo stato dell'hardware e supporta alcuni semplici controlli, tra cui:

- Stato CPU, memoria e flash
- Controllo LED
- Informazioni sul dispositivo

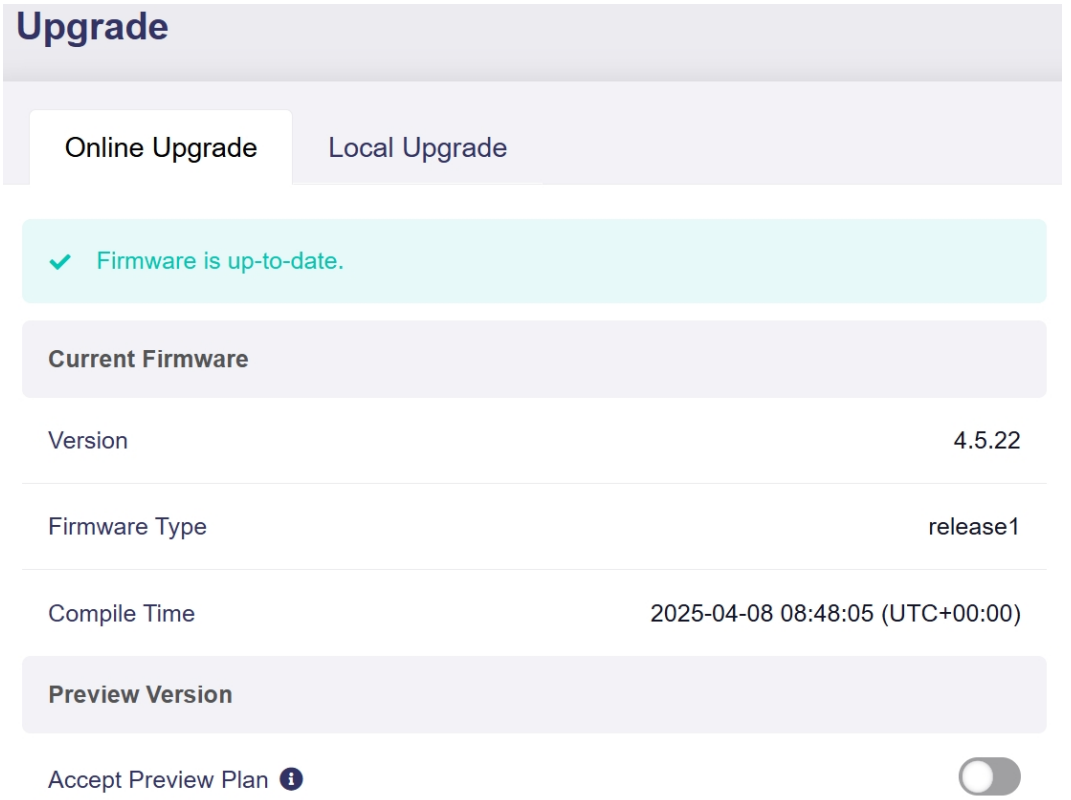


## 14.2 Aggiornamento

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Aggiorna. È possibile aggiornare la versione del firmware del router tramite aggiornamento** online o aggiornamento locale.

### 14.2.1 Aggiornamento online

Puoi trovare i dettagli del firmware corrente qui, inclusa la versione del firmware, il tipo di firmware (ad esempio, versione, beta) e l'ora dell'aggiornamento. Se il router è connesso a Internet, verificherà la presenza della versione firmware più recente disponibile per il download.



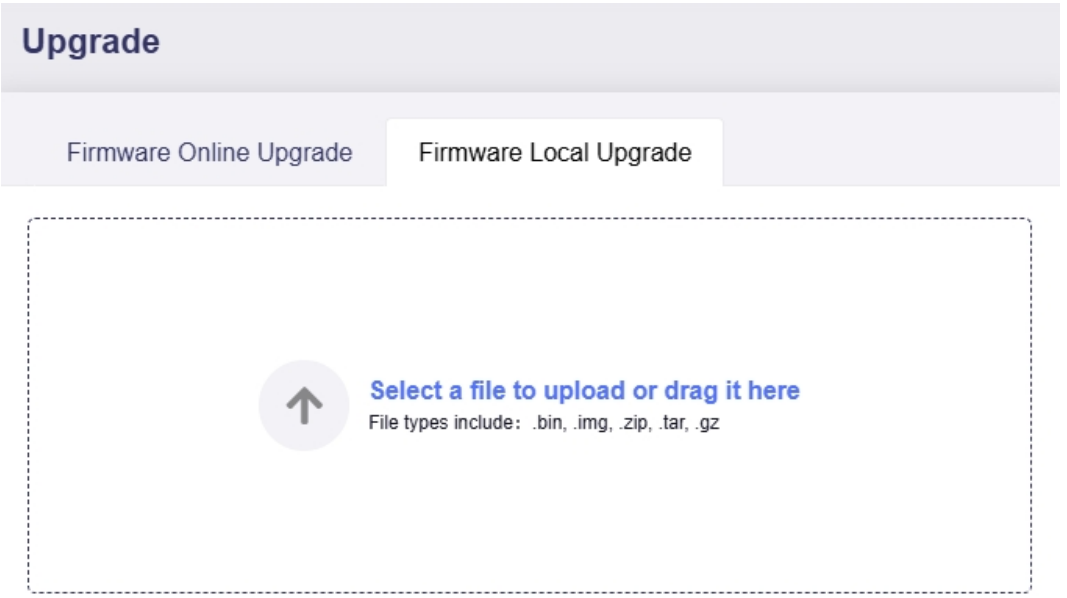

Se **Accetta piano di anteprima** è abilitato, puoi provare le nuove funzionalità prima che venga rilasciata la versione finale e fornirci feedback. Impostalo una volta e rimane acceso. Tieni presente che questi aggiornamenti potrebbero non essere stabili.

**Suggerimento**: quando provi a eseguire un aggiornamento online, se viene visualizzato **Download non riuscito**, vai a **SISTEMA** > **Fuso orario** e correggi l'errore del fuso orario (sincronizzazione con il browser).

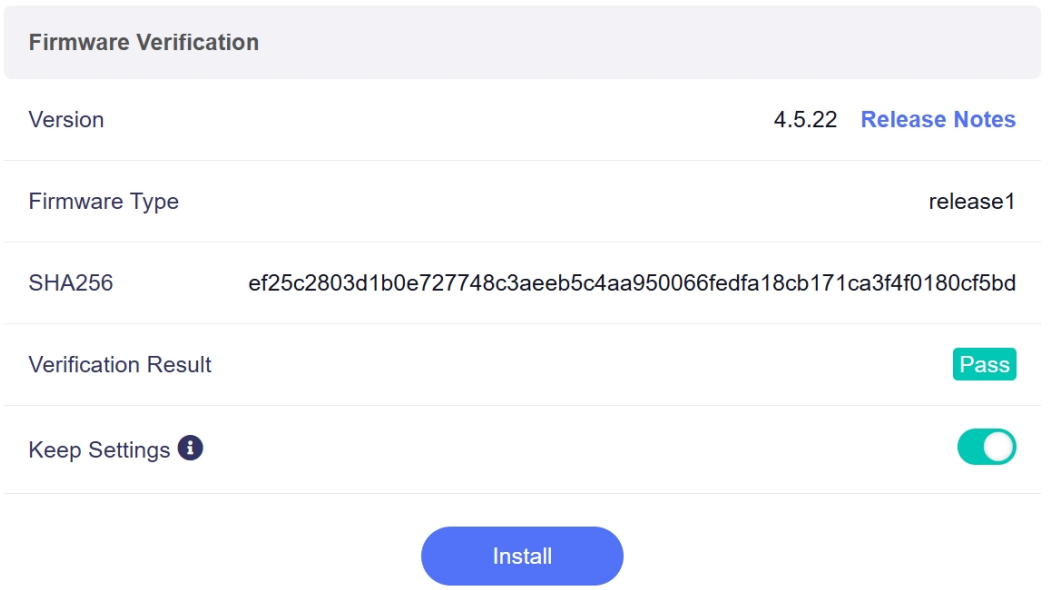
## 14.2.2 Aggiornamento locale

L'aggiornamento locale non si basa su una connessione Internet per il router.

Scarica il pacchetto firmware corretto (corrispondente al modello del tuo router) dal Centro download ufficiale sul tuo dispositivo locale. Quindi accedi al pannello di amministrazione web del router, vai alla sezione **SISTEMA** > **Aggiornamento** > **Aggiornamento locale** e carica il pacchetto firmware.




La pagina visualizzerà i dettagli del firmware. Verifica questi dettagli prima di fare clic su **Installa**.



Se **Mantieni impostazioni** è abilitato, le impostazioni correnti vengono mantenute. Tuttavia, eventuali pacchetti installati manualmente dovranno essere reinstallati al termine dell'aggiornamento. Non abilitare questa opzione durante il downgrade del firmware.

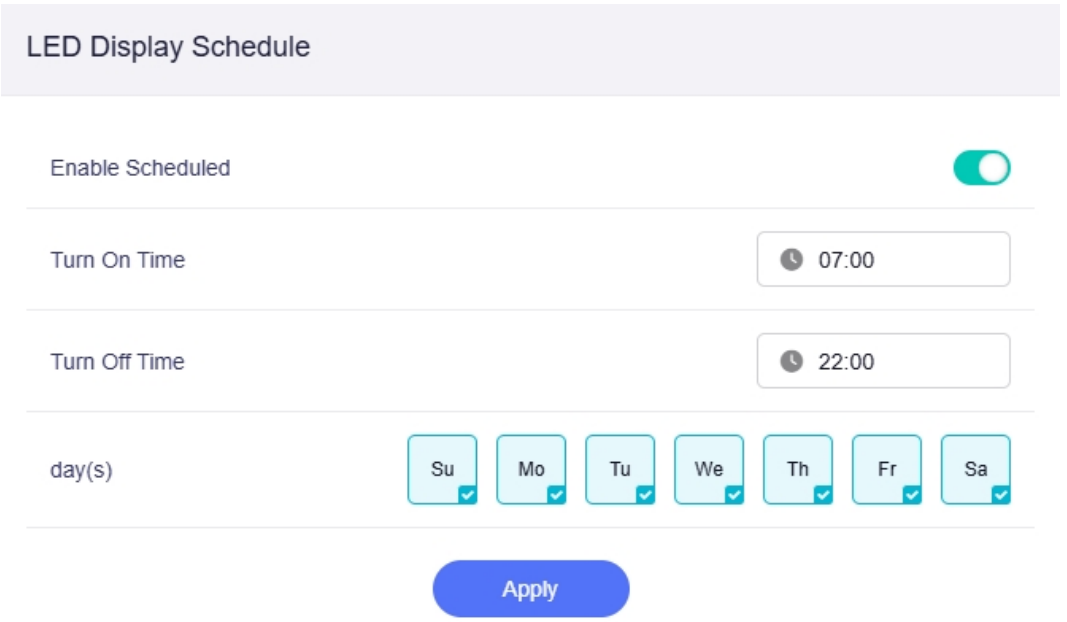
## 14.3 Attività pianificate

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Attività pianificate**. Questa pagina ti consente di impostare una pianificazione giornaliera per alcune azioni di base, tra cui l'accensione e lo spegnimento della luce LED e il riavvio del router.

**Nota**: sincronizza l'ora nella pagina Fuso orario prima di utilizzare questa funzione. Se il dispositivo è spento all'orario previsto, l'attività non verrà eseguita.

### 14.3.1 Programmazione del LED

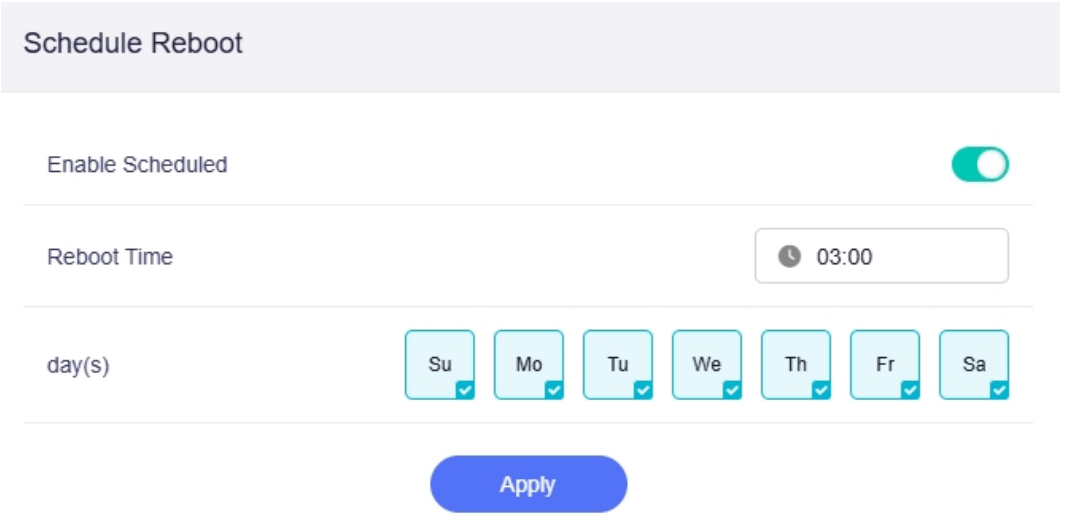
Imposta una pianificazione per la luce LED del router, se necessario, quindi fai clic su **Applica**.




- **Abilita programmazione**: attiva questo interruttore per abilitare la pianificazione del display LED.
- **Durata di accensione**: imposta l'ora (ad esempio, 07:00) in cui la luce LED si accenderà.
- **Durata di spegnimento**: imposta l'ora (ad esempio, 22:00) in cui la luce LED si spegnerà.
- **giorno(i): seleziona i giorni** effettivi della settimana per queste impostazioni.

## 14.3.2 Riavvio pianificato

Imposta una pianificazione per il riavvio automatico del router, se necessario, quindi fai clic su **Applica**.



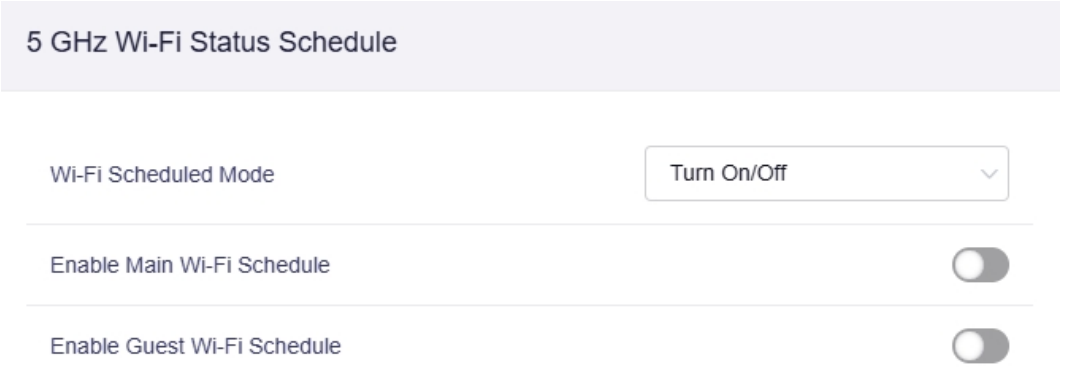

- **Abilita programmazione**: attiva questo interruttore per abilitare il riavvio pianificato.
- **Durata di riavvio**: imposta l'ora specifica (ad esempio 03:00) in cui il router si riavvierà.
- **giorno(i): seleziona i giorni** effettivi della settimana per queste impostazioni.

## 14.3.3 Programmazione del Wi-Fi a 5 GHz

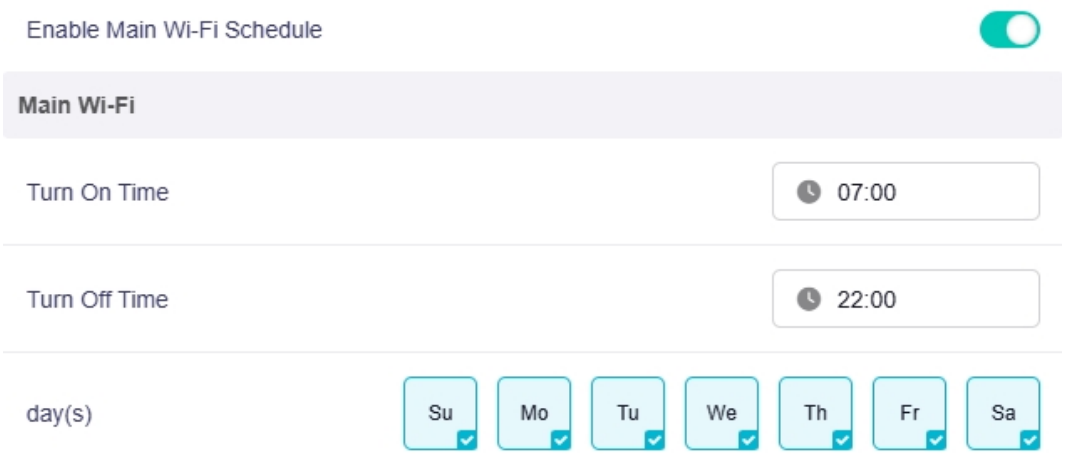
Questa funzione ti consente di impostare una pianificazione per il tuo Wi-Fi a 5 GHz. Sono disponibili due modalità: Accendi/Spegni e Cambia potenza TX.

**Modalità 1: accensione/spegnimento**

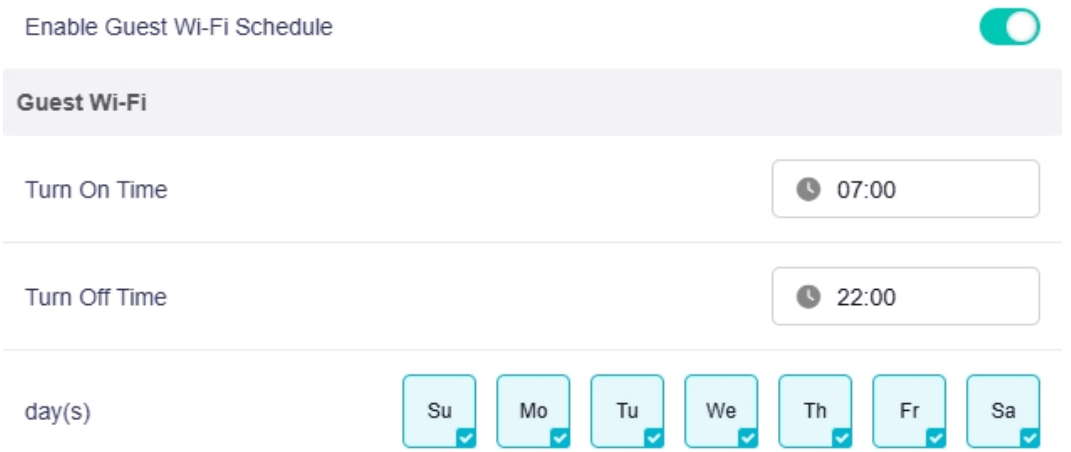
Puoi abilitare la pianificazione di accensione/spegnimento sia per il Wi-Fi principale a 5 GHz che per il Wi-Fi ospiti.




- **Programmazione del Wi-Fi principale**: se abilitato, imposta gli orari di accensione e spegnimento per il Wi-Fi principale da 5 GHz e seleziona una data di validità per la settimana.

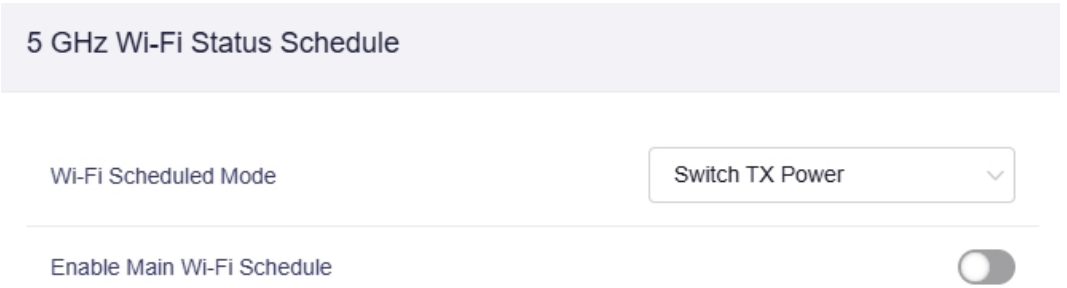



- **Programmazione del Wi-Fi ospiti**: se abilitato, imposta gli orari di accensione e spegnimento per il Wi-Fi ospiti da 5 GHz e seleziona una data effettiva per la settimana.

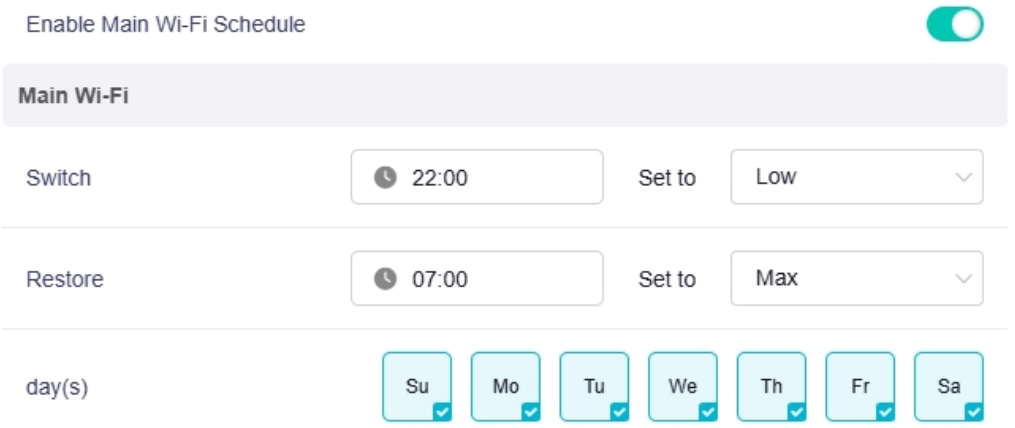



**Modalità 2: cambia potenza TX**

Puoi abilitare la pianificazione del cambio di potenza TX per il Wi-Fi principale a 5 GHz.




Se abilitato, imposta due azioni temporizzate per il tuo Wi-Fi principale da 5 GHz per cambiare la potenza TX e seleziona una data effettiva per la settimana.




- **Interruttore**: imposta la potenza TX su un determinato livello (ad esempio Basso) a un orario specifico (ad esempio 22:00).

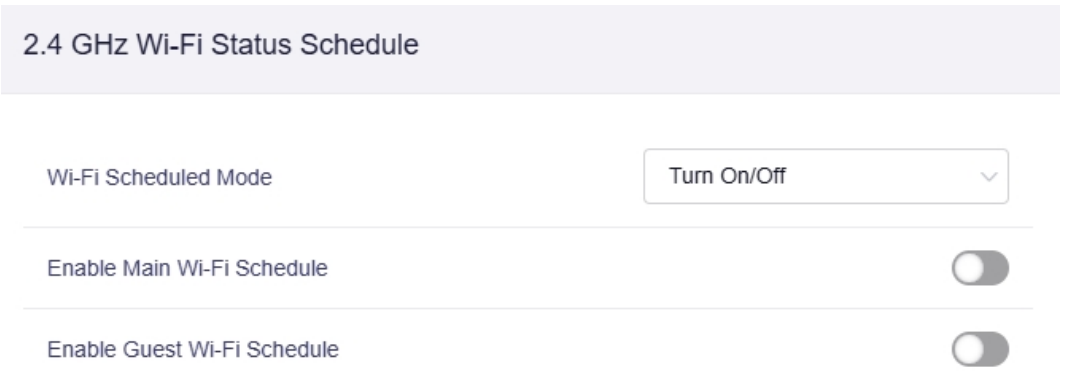
- **Ripristina**: ripristina la potenza TX a un altro livello (ad esempio Max) in un altro momento (ad esempio 07:00).
- **Giorni**: seleziona i giorni effettivi della settimana per queste impostazioni.

### 14.3.4 Programmazione del Wi-Fi a 2,4 GHz

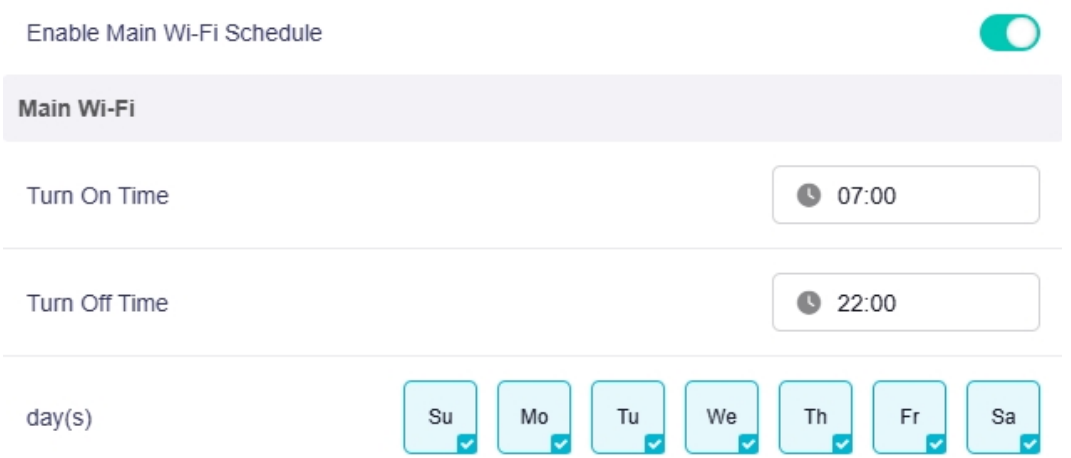
Questa funzione ti consente di impostare una pianificazione per il tuo Wi-Fi a 2,4 GHz. Sono disponibili due modalità: Accendi/Spegni e Cambia potenza TX.

**Modalità 1: accensione/spegnimento**

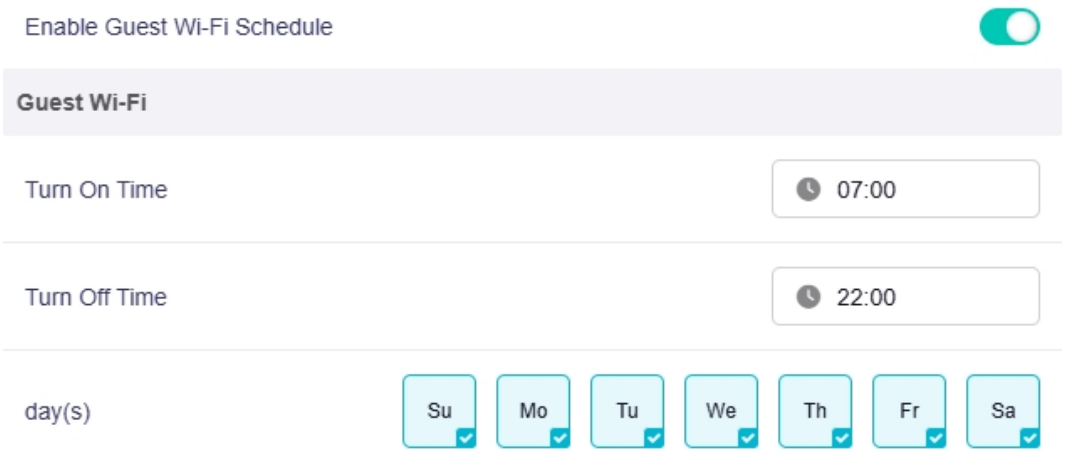
Puoi abilitare la pianificazione di accensione/spegnimento sia per il Wi-Fi principale a 2,4 GHz che per il Wi-Fi ospiti.




- **Programmazione del Wi-Fi principale**: se abilitato, imposta gli orari di accensione e spegnimento per il Wi-Fi principale a 2,4 GHz e seleziona una data di validità per la settimana.

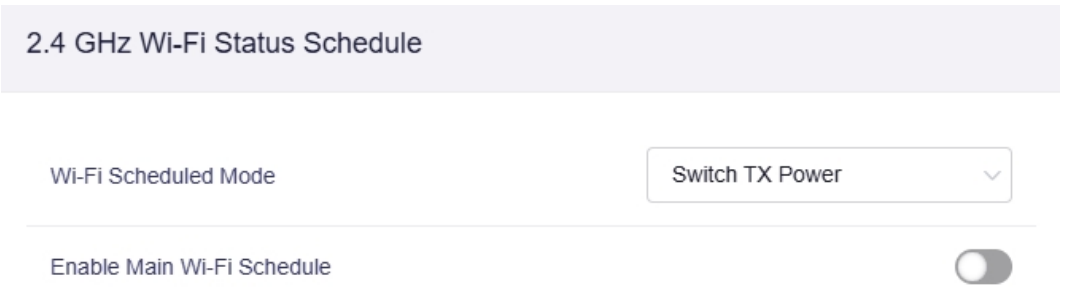


- **Programmazione del Wi-Fi ospiti**: se abilitato, imposta gli orari di accensione e spegnimento per il Wi-Fi ospiti a 2,4 GHz e seleziona una data effettiva per la settimana.

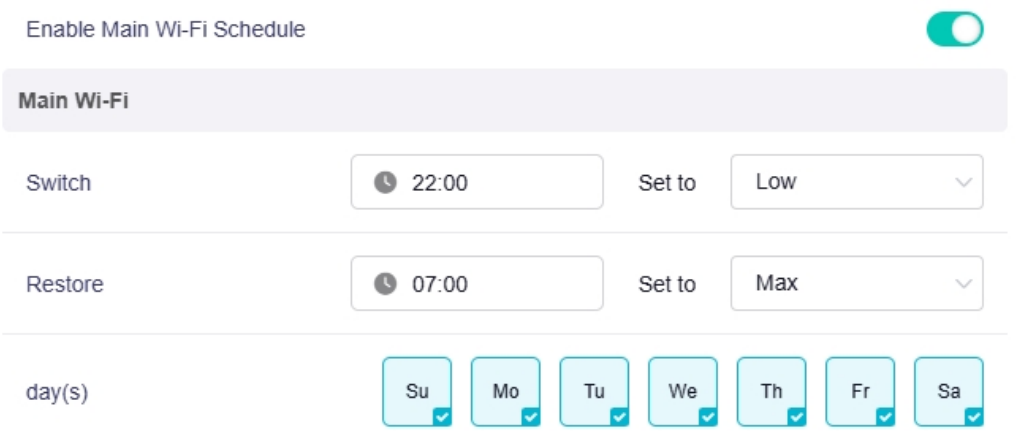



**Modalità 2: cambia potenza TX**

Puoi abilitare la pianificazione del cambio di potenza TX per il Wi-Fi principale a 2,4 GHz.




Se abilitato, imposta due azioni temporizzate per il tuo Wi-Fi principale a 2,4 GHz per cambiare la potenza TX e seleziona una data effettiva per la settimana.

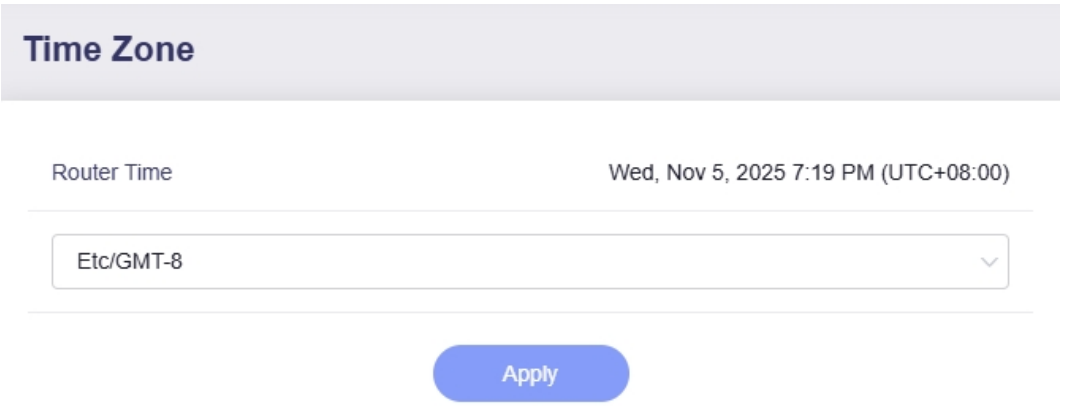



- **Interruttore**: imposta la potenza TX su un determinato livello (ad esempio Basso) a un orario specifico (ad esempio 22:00).

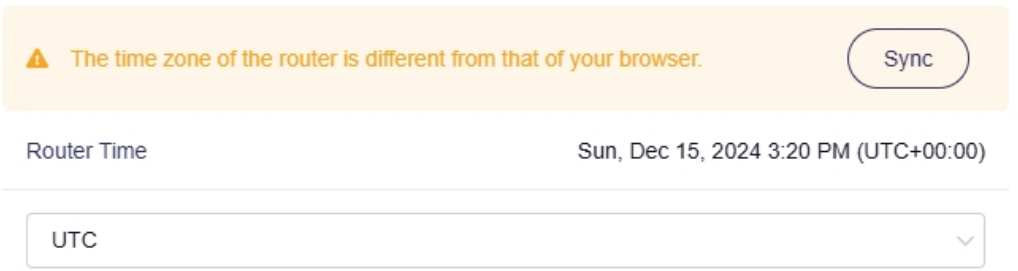
- **Ripristina**: ripristina la potenza TX a un altro livello (ad esempio Max) in un altro momento (ad esempio 07:00).
- **Giorni**: seleziona i giorni effettivi della settimana per queste impostazioni.

## 14.4 Fuso orario

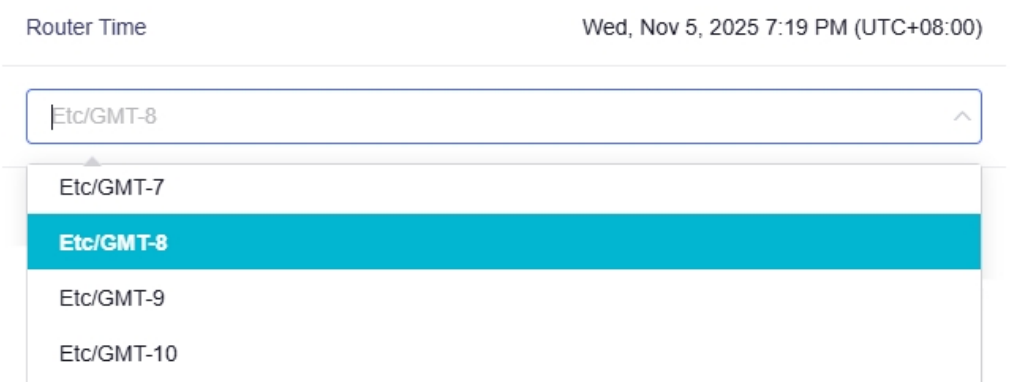
Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Fuso orario**. Questa pagina mostra l'ora di sistema del router, indicando la data, l'ora e la differenza di fuso orario corrispondente.




Alcune funzioni si basano sull'ora di sistema del router per avere effetto. Assicurati che il fuso orario corretto sia sincronizzato correttamente. Se il fuso orario del router è diverso da quello del browser, verrà visualizzato un messaggio come segue. Fai clic sul pulsante **Sincronizza** per sincronizzare il fuso orario.

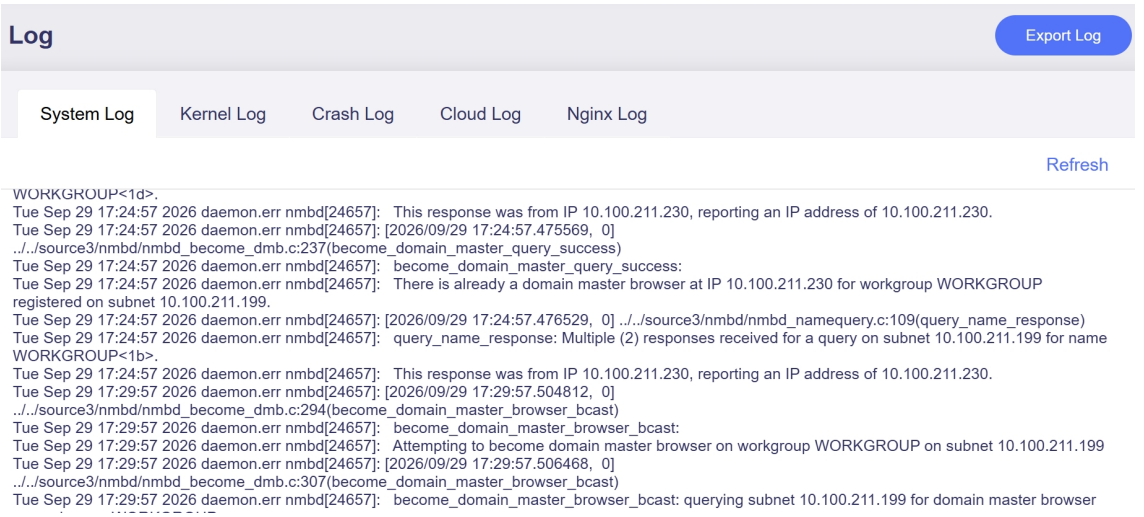



Per cambiare fuso orario, seleziona il fuso orario appropriato dall'elenco per assicurarti che l'ora di sistema del router corrisponda all'ora locale.



# 14.5 Registro

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Registro**. Questa pagina ti consente di visualizzare i log di sistema, kernel, crash, cloud e Nginx per l'analisi e la risoluzione dei problemi.




- **Aggiorna**: fai clic su questo pulsante per aggiornare i registri.
- **Esporta registro**: fai clic su questo pulsante per esportare le informazioni di debug insieme ai registri.

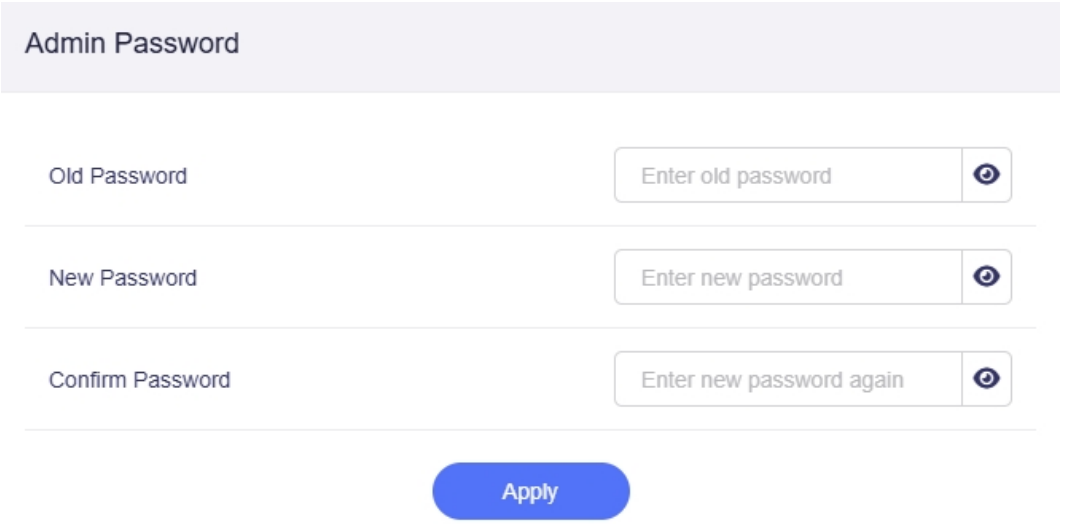
## 14.6 Sicurezza

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Sicurezza**. Questa pagina contiene le opzioni di configurazione per la gestione locale e remota del router, tra cui:

- Password amministratore
- Accesso locale per pannello di amministrazione web, LuCI e SSH
- Accesso remoto HTTPS/SSH
- Apri le porte sul router

### 14.6.1 Password amministratore

In questa sezione è possibile modificare la password di accesso del pannello di amministrazione web.

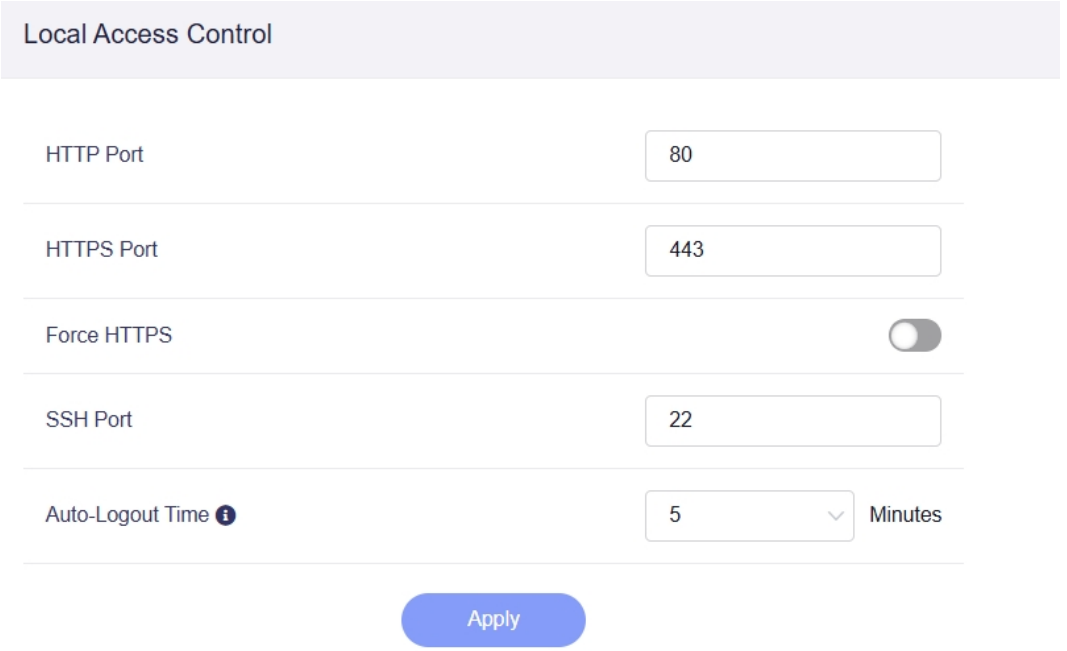



I requisiti per la password amministratore sono i seguenti:

1. Minimo 10 caratteri e massimo 63 caratteri di lunghezza.
2. Sono consentiti lettere (con distinzione tra maiuscole e minuscole), numeri e simboli (ad esempio,! @ # $ % ^ & * ( ) _ + - =,. > < |? / \ [ ] { }:; " ' ` ~ ).
3. Sono richieste almeno due delle seguenti categorie: lettere maiuscole, lettere minuscole, numeri e simboli.

## 14.6.2 Controllo dell'accesso locale

Questa sezione gestisce l'accesso alle molteplici interfacce del router (Pannello di amministrazione, SSH). Può impedire tentativi di scansione e intrusione sulla porta predefinita ed evitare problemi di rete causati da conflitti di porte.

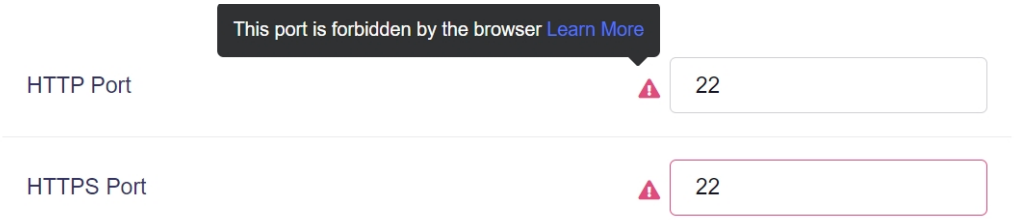



**Pannello di amministrazione**

- **Porta HTTP**: il valore predefinito è 80, utilizzato per l'accesso HTTP non crittografato al pannello di amministrazione web.
- **Porta HTTPS**: il valore predefinito è 443, utilizzato per l'accesso sicuro da HTTPS a pannello di amministrazione web.
- **Forza HTTPS**: se abilitato, l'accesso a pannello di amministrazione web viene imposto per utilizzare una connessione HTTPS sicura.
- **Porta SSH**: il valore predefinito è 22, la porta utilizzata per l'accesso SSH al router.
- **Durata di disconnessione automatica**: impostato su 5 minuti per impostazione predefinita, disconnette automaticamente le sessioni di amministrazione inattive dopo questa durata per motivi di sicurezza. Puoi personalizzare il tempo di disconnessione automatica, da 1 minuto a 3 ore.

**Nota**:

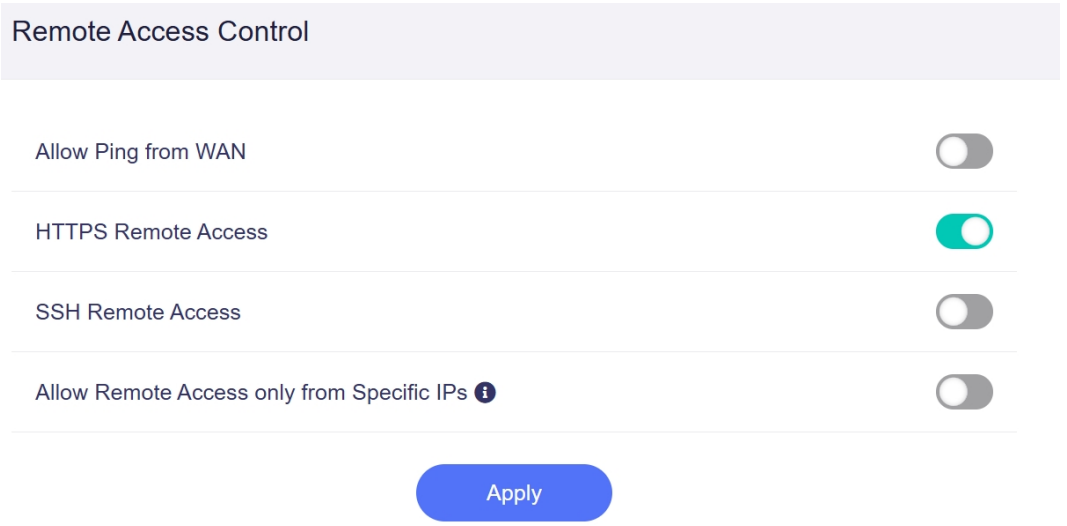
1. Se assegni un numero di porta che è in conflitto con una porta riservata (o una riservata per servizi specifici da browser/convenzioni di rete), verrà visualizzato un messaggio che indica "Questa porta è vietata dal browser".



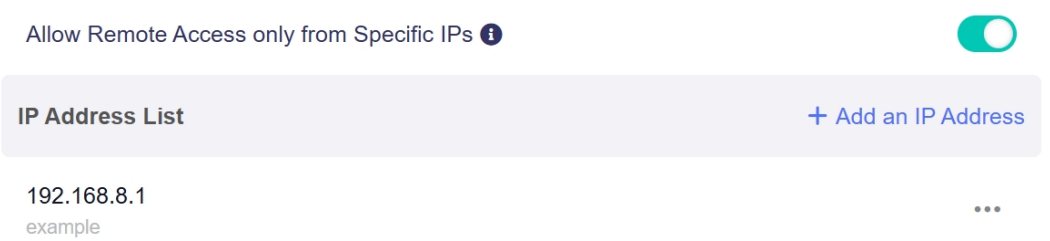

2. Se il numero di porta viene modificato nel firmware, è necessario inserire il numero di porta corretto per accedere al pannello di amministrazione. Se hai dimenticato il numero di porta, reimposta il router per ripristinare il numero di porta predefinito.

## 14.6.3 Controllo dell'accesso remoto

Questa sezione gestisce l'accesso remoto alle interfacce del router, inclusi HTTPS, SSH e ping lato WAN. Consente inoltre di limitare l'accesso da indirizzi IP specifici, trovando un equilibrio tra accessibilità remota e sicurezza della rete.



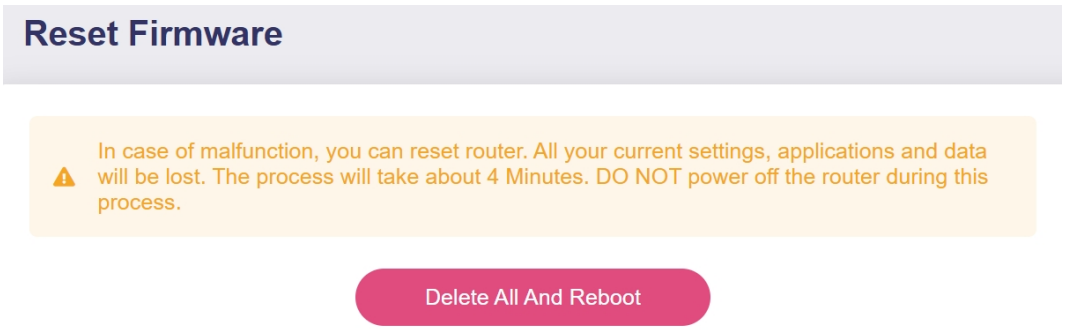

- **Consenti ping dalla WAN**: consentire il ping dal lato WAN del router può aiutare gli utenti a verificare se il router è raggiungibile tramite WAN in caso di problemi di rete, nonché a determinare la latenza di rete e la perdita di pacchetti.
- **Accesso remoto HTTPS**: Accesso remoto HTTPS abilita accesso remoto sicuro al pannello di amministrazione web del router tramite il protocollo HTTPS. Garantisce la trasmissione dei dati crittografati durante la gestione del router da remoto tramite un browser web.
- **Accesso remoto SSH**: l'accesso remoto SSH consente l'accesso sicuro al terminale del router. Consente agli utenti di gestire in remoto il router tramite SSH, stabilendo un tunnel crittografato per le attività.
- **Consenti accesso remoto da IP specifici**: questa funzione è disponibile solo quando è abilitata una delle tre funzioni precedenti. È possibile aggiungere più indirizzi IP specificati per gestire in remoto il router solo da dispositivi con questi IP.



## 14.7 Ripristino del firmware

Se il router non funziona correttamente, puoi provare a risolvere il problema reimpostando il firmware.

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Ripristino del firmware**. Fai clic su **Elimina tutto e riavvia** per ripristinare il firmware, se necessario.




**Nota**: tutte le impostazioni, le applicazioni e i dati correnti verranno cancellati. Il processo richiederà circa 2 minuti. Non spegnere il router durante questo processo.

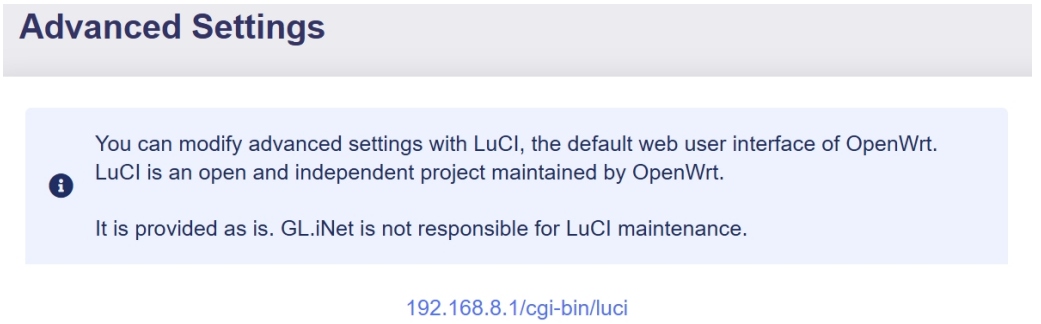
Se non riesci ad accedere al pannello di amministrazione web del router, prova a ripristinare il router utilizzando il pulsante di ripristino fisico sul lato.

## 14.8 Impostazioni avanzate

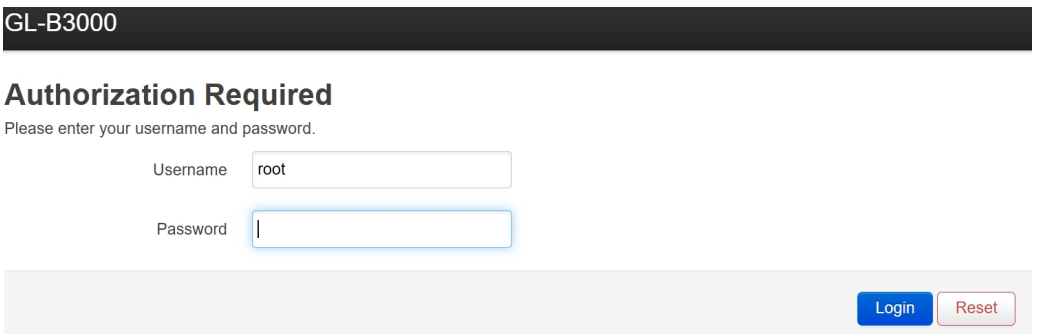
Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Impostazioni avanzate**. Questa pagina consente di modificare le impostazioni avanzate in LuCI, che è l'interfaccia utente web predefinita di OpenWrt. Essendo un progetto aperto e indipendente gestito da OpenWrt, LuCI viene fornito così com'è. GL.iNet non è responsabile della manutenzione di LuCI.

Segui i passaggi seguenti per accedere all'interfaccia LuCI.

1. Fai clic sul collegamento di accesso e verrai reindirizzato alla pagina di accesso LuCI.




2. Inserisci la password di accesso, che è la stessa della password del pannello di amministrazione web.




Quindi accederai all'interfaccia LuCI.

