

Manuale utente

GL-MT5000 / Brume 3

Gateway di sicurezza

Versione firmware 4.9.0

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 6
1.1 Panoramica del prodotto 7
1.1.1 Aspetto 7
1.1.2 Interfacce e pulsanti 8
1.1.3 LED 9
1.2 Specifiche tecniche 9
1.3 Contenuto della confezione 10
Capitolo 2 Collegamenti hardware 11
2.1 Scelta della posizione 12
2.2 Collegamento del router 12
Capitolo 3 Accesso al router 13
Capitolo 4 Configurazione della connessione Internet 15
4.1 Utilizza la procedura guidata di configurazione rapida 16
4.2 Configurazione manuale della connessione Internet 17
4.2.1 Connessione a Internet tramite cavo Ethernet 18
4.2.2 Connessione a Internet tramite tethering USB 22
4.2.3 Connessione a Internet tramite modem USB 27
Capitolo 5 Client 29
5.1 Dettagli del dispositivo 31
5.2 Azione 33
5.3 Rimozione dei client 36
5.4 Ordinamento 37
Capitolo 6 Servizi cloud 38
6.1 GoodCloud 39
6.1.1 Attivazione di GoodCloud 40
6.1.2 Gestione del router 42
6.1.3 Dissociazione del dispositivo 47
6.1.4 Disabilita GoodCloud 47
6.2 AstroWarp 48
6.2.1 Configurazione rapida 48
6.2.2 Verifica della connettività 52
6.2.3 Passaggio a un piano superiore 53

Capitolo 7 Conoscere le VPN 54
7.1 Introduzione 55
7.2 Scenari di utilizzo 56
Capitolo 8 Dashboard VPN 58
8.1 Caricamento di un profilo VPN 59
8.2 Aggiunta di un tunnel VPN 62
8.2.1 Procedura generale 62
8.2.2 Esempi di configurazione 65
8.3 Kill Switch 81
8.4 Tutto il resto del traffico 82
8.5 Opzioni del tunnel 83
8.6 Priorità dei tunnel 85
Capitolo 9 Configurazione del server VPN 87
9.1 Configurazione del server OpenVPN 88
9.1.1 Preparazione 88
9.1.2 Procedura di configurazione 89
9.1.3 Risoluzione dei problemi 91
9.2 Configurazione del server WireGuard 92
9.2.1 Preparazione 92
9.2.2 Procedura di configurazione 93
9.2.3 Risoluzione dei problemi 96
Capitolo 10 Configurazione del client VPN 97
10.1 Configurazione del client OpenVPN 98
10.1.1 Preparazione 98
10.1.2 Configurazione di NordVPN 98
10.1.3 Configurazione manuale del client OpenVPN (altri provider) 104
10.2 Configurazione del client WireGuard 107
10.2.1 Preparazione 107
10.2.2 Configurazione di AzireVPN 108
10.2.3 Configurazione di Hide.me 112
10.2.4 Configurazione di IPVanish 115
10.2.5 Configurazione di Mullvad 119
10.2.6 Configurazione di NordVPN 123
10.2.7 Configurazione di PIA (Private Internet Access) 128

10.2.8 Configurazione di PureVPN 132
10.2.9 Configurazione di Surfshark 135
10.2.10 Configurazione di Windscribe 139
10.2.11 Configurazione manuale del client WireGuard (altri provider) 143
Capitolo 11 Rete 148
11.1 Multi-WAN 149
11.1.1 Monitoraggio dello stato dell'interfaccia 149
11.1.2 Modalità Multi-WAN 153
11.2 LAN 156
11.2.1 Impostazioni di base 156
11.2.2 Server DHCP 157
11.2.3 Prenotazione indirizzi 159
11.3 DNS 160
11.3.1 Impostazioni del server DNS 161
11.3.2 Modifica del file hosts 165
11.4 Porta Ethernet 166
11.5 IPv6 167
11.5.1 Modalità IPv6 168
11.5.2 Metodo di acquisizione DNS 168
11.6 IGMP Snooping 169
11.7 Modalità di rete 170
11.8 Gateway drop-in 172
11.9 Accelerazione di rete 174
Capitolo 12 Controllo del traffico 176
12.1 Motore DPI 177
12.2 Statistiche dei dati 179
12.2.1 Configurazione rapida 179
12.2.2 Regole di archiviazione dei dati 181
12.2.3 Cambia intervallo di tempo 181
12.2.4 Cancella statistiche 182
12.3 Filtro dei contenuti 183
12.4 QoS 185
12.5 SQM 187
12.6 Controllo parentale 189

Capitolo 13 Sicurezza 195
13.1 Port forwarding 196
13.1.1 DMZ 196
13.1.2 Port forwarding 197
13.2 ACL 199
13.3 Accesso amministratore 201
13.3.1 Controllo degli accessi 201
13.3.2 Controllo dell'accesso remoto 204
13.3.3 Apertura delle porte sul router 205
13.4 Modalità NAT 206
Capitolo 14 Applicazioni 207
14.1 Plug-in 208
14.2 DNS dinamico 209
14.2.1 Abilita DDNS 209
14.2.2 Verifica del funzionamento del DDNS 212
14.2.3 Accesso remoto HTTPS 214
14.2.4 Accesso remoto SSH 216
14.3 Archiviazione di rete 218
14.3.1 Collegamento del dispositivo di archiviazione 218
14.3.2 Configurazione di Samba 219
14.3.3 Configurazione di WebDAV 222
14.3.4 Configurazione di DLNA 225
14.4 AdGuard Home 226
14.5 Tailscale 228
14.5.1 Configurazione di Tailscale 229
14.5.2 Annuncio delle sottoreti WAN 232
14.5.3 Annuncio delle sottoreti LAN 233
14.5.4 Nodi di uscita personalizzati 234
14.5.5 Esegui nodo di uscita 235
14.6 ZeroTier 242
14.6.1 Configurazione di ZeroTier 243
14.6.2 Consenti accesso remoto WAN 247
14.6.3 Consenti accesso remoto LAN 248
14.7 Tor 249

Capitolo 15 Sistema 250
15.1 Panoramica 251
15.2 Password amministratore 252
15.3 Aggiornamento 253
15.3.1 Aggiornamento online 253
15.3.2 Aggiornamento locale 254
15.4 Attività pianificate 255
15.4.1 Programmazione del LED 255
15.4.2 Riavvio pianificato 256
15.5 Fuso orario 257
15.6 Ripristino del firmware 258
15.7 Registro 259
15.8 Impostazioni avanzate 261

Capitolo 1

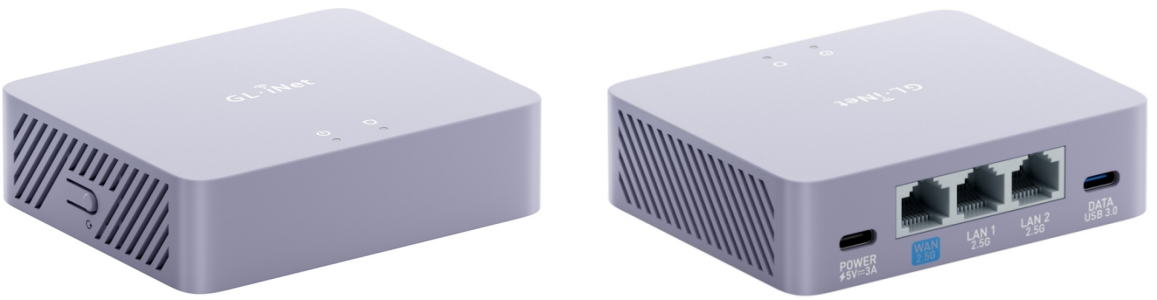
Conoscere il router

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

1.1 Panoramica del prodotto

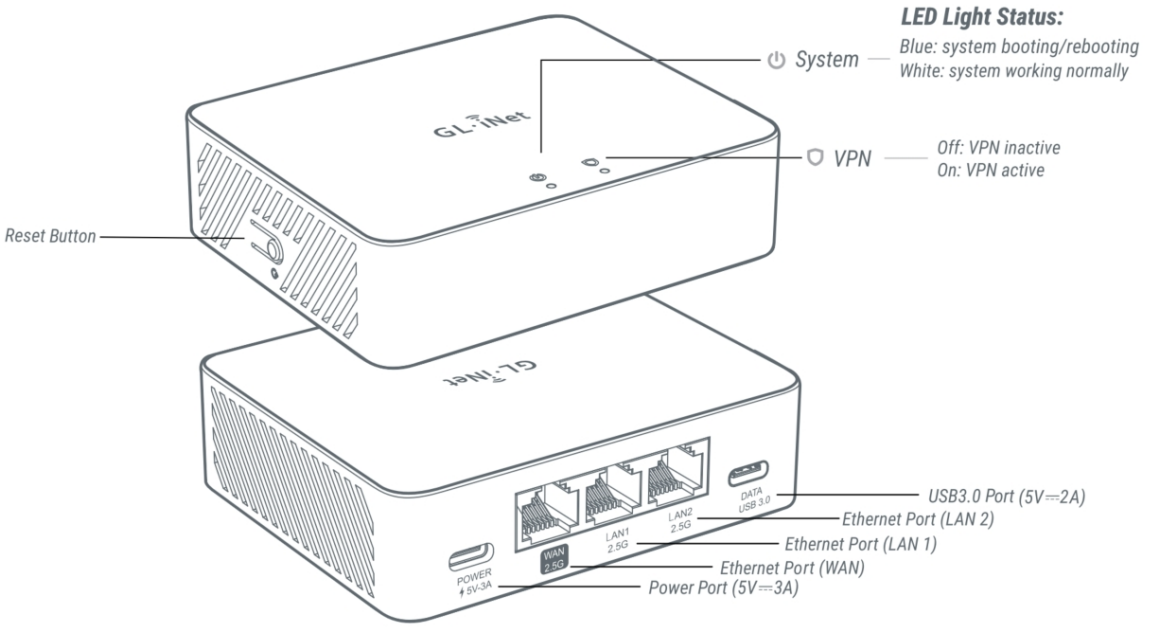
Brume 3 (GL-MT5000) è un gateway di sicurezza ad alte prestazioni, dotato di CPU quad-core MediaTek, RAM 1GB e memoria eMMC 8GB. Presenta un design compatto, ideale per implementazioni con vincoli di spazio e supporta l'hosting VPN domestico nonché 30 servizi VPN. Inoltre, viene fornito con la funzionalità DPI di GL.iNet, Controllo parentale e AdGuard Home, che soddisfa le diverse esigenze degli appassionati di tecnologia e degli utenti aziendali.

1.1.1 Aspetto





1.1.2 Interfacce e pulsanti



Voce	Descrizione
Porta di alimentazione	Consente di collegare l'alimentatore.
Porta WAN 2.5G	Consente di collegare un modem o una presa Ethernet per accedere a Internet.
Porta LAN 2.5G	Consente di collegare dispositivi cablati, se necessario.
Porta USB 3.0	Per dispositivi di archiviazione USB, tethering USB da smartphone e modem cellulari USB compatibili.
Pulsante di ripristino	Tieni premuto per **4 secondi,** quindi rilascia per riparare il tuo rete. Il LED diventerà blu e lampeggerà lentamente fino al tuo la rete è stata ripristinata.
	Tenere premuto per **10 secondi,** quindi rilasciare per ripristinare router alle impostazioni di fabbrica. Il LED diventerà blu e lampeggerà rapidamente. Tutti i dati verranno cancellati quando il LED diventa fisso blu.

1.1.3 LED

LED	Stato
Sistema	Blu: avvio del sistema
	Bianco: connesso a Internet
VPN	Off: VPN inattiva
	On: VPN attiva

1.2 Specifiche tecniche

Interfaccia	1 x 2.5G Porta Ethernet WAN 2 x 2.5G Porte Ethernet LAN 1 x porta USB 3.0 tipo C 1 x porta di alimentazione di tipo C 1 pulsante di ripristino
CPU	MediaTek, quad-core @2.0GHz
Memoria/Archiviazione	DDR4 1GB / eMMC 8GB
Velocità Ethernet	10/100/1000/2500Mbps
Ingresso alimentazione	Tipo C, 5V/3A
Consumo energetico	< 5W
Temperatura di esercizio	0 ~ 40°C (32 ~ 104°F)
Temperatura di conservazione	-20 ~ 70°C (-4 ~ 158°F)
Dimensioni/Peso	75 x 92 x 25mm / 148 g
Altri strumenti	Scheda tecnica / Firmware / App / Unboxing / Tutorial

1.3 Contenuto della confezione

La confezione include:

- 1 x Brume 3 (GL-MT5000)
- 1 x Manuale utente (Guida rapida)
- 1 cavo Ethernet
- 1 biglietto di ringraziamento
- 1 Adattatore di alimentazione
- 1 x Convertitore (a seconda del paese di spedizione)



1 x User manual



1 x Thank you card



1 x Brume 3 (GL-MT5000)



1 x Ethernet cable



1 x Power adapter



Converters
(*Base on your shipping countries*)

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.
- **Superficie stabile**: posiziona il router su una superficie piana e orizzontale (mensola, scrivania) per stabilità.

2.2 Collegamento del router

1. **Accendi**

   Monta insieme l'alimentatore in due pezzi. Collegalo al tuo Brume 3 e collegalo a una presa. Si avvierà automaticamente.
2. **Connetti un dispositivo al router**

   Collega un dispositivo cablato (ad esempio un computer o laptop) alla porta LAN di Brume 3 con un cavo Ethernet.
3. **Accedi al router**

   Internet non sarà 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

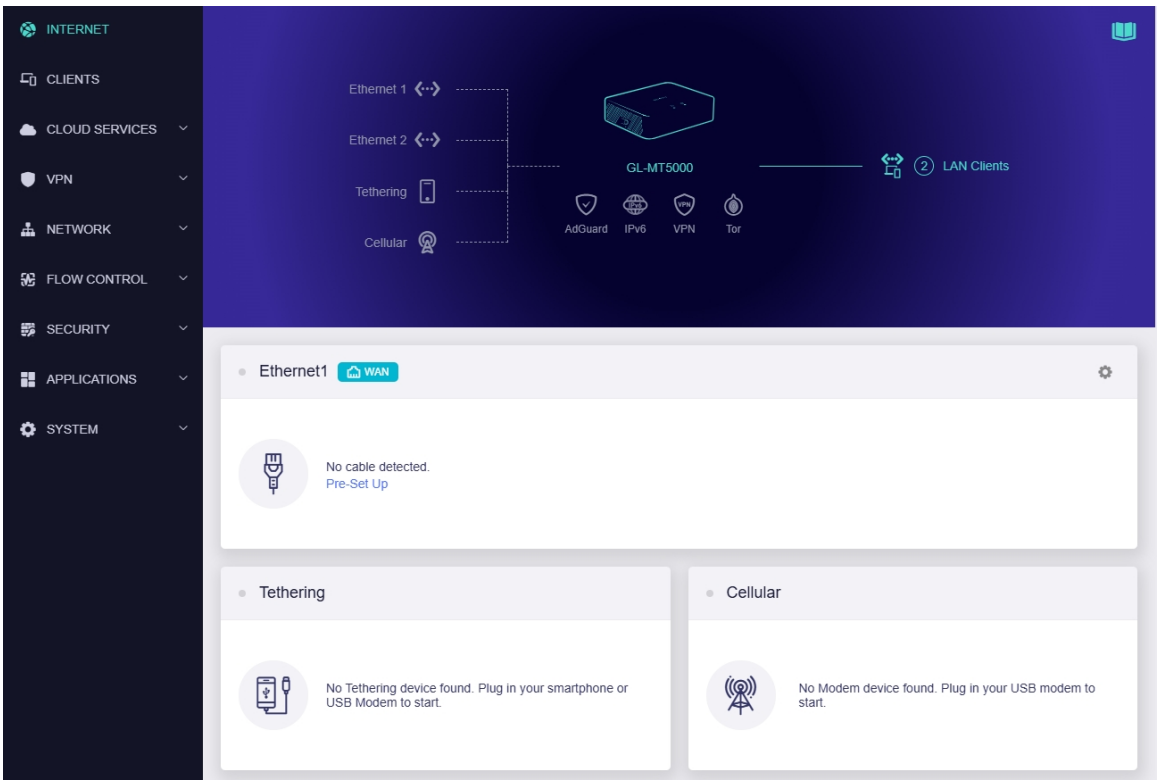
Accesso al router

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.

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

1. Collega un dispositivo (ad esempio un computer o un laptop) alla porta LAN del Brume 3 con 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. Entrerai quindi nel pannello di amministrazione web di Brume 3.



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.

4.1 Utilizza la procedura guidata di configurazione rapida

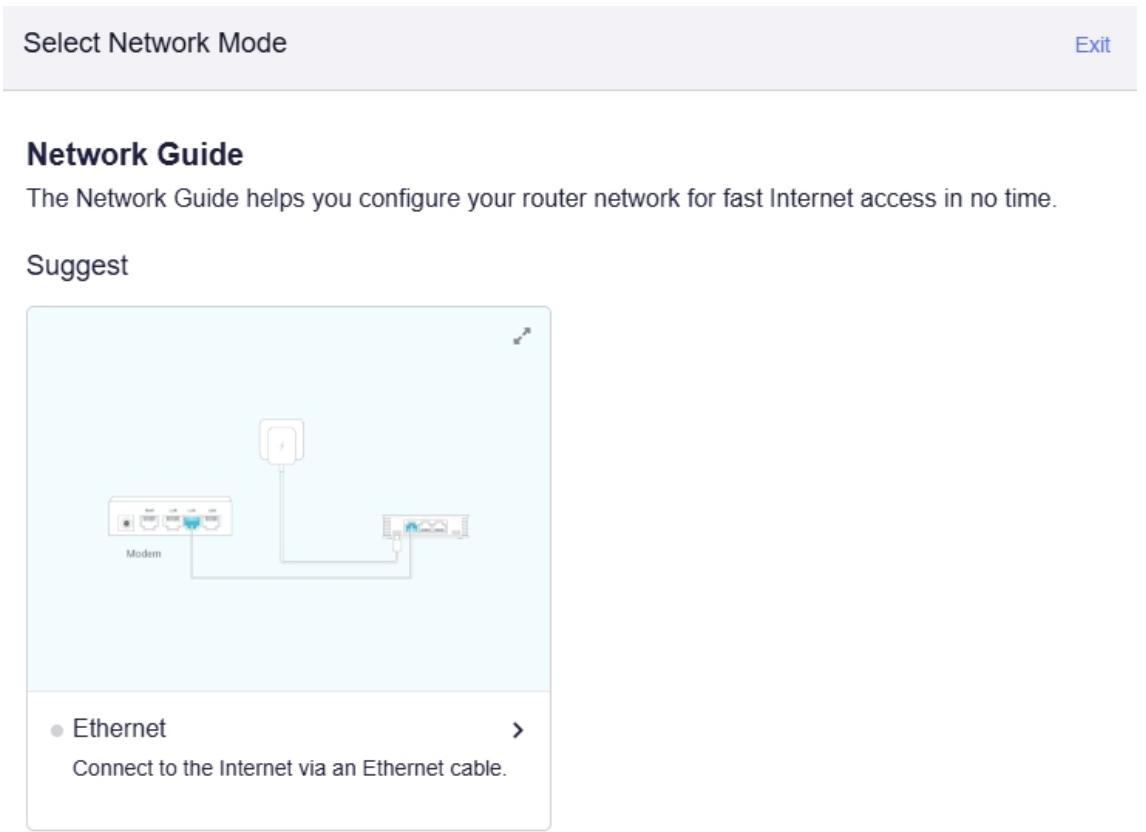
La configurazione guidata basata sul Web ti guiderà attraverso la configurazione della rete del router.

Segui i passaggi seguenti per avviare la procedura guidata.

1. Accedi al pannello di amministrazione web del router come indicato nel capitolo 3.
2. Nella home page, fai clic sull'icona del libro nell'angolo in alto a destra.



3. Segui la procedura guidata **di installazione** per configurare il router e stabilire una connessione Internet.



4.2 Configurazione manuale della connessione Internet

Mentre la configurazione guidata è utile per una rapida configurazione della rete, la configurazione manuale consente di regolare le impostazioni di rete avanzate per requisiti specifici e di controllare o modificare le connessioni esistenti secondo necessità.

Brume 3 supporta tre metodi di connessione Internet: Ethernet, Tethering USB e Modem USB/Cellulare. 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. **Tethering USB**: collega uno smartphone o un altro dispositivo compatibile al router tramite un cavo USB per condividere la connessione dati mobile del dispositivo (ad esempio, 4G/5G) con il router. Si tratta di una soluzione conveniente per l'accesso temporaneo a Internet, soprattutto all'aperto o in aree senza banda larga fissa.

3. **Modem USB/Cellulare**: inserire nel router un modem cellulare USB con una scheda SIM preinstallata. Il router si connetterà quindi a Internet tramite reti mobili 4G/5G, fornendo connettività indipendente dalla banda larga fissa. Questo metodo offre un'elevata mobilità ed è adatto a scenari come l'uso a bordo di un veicolo o attività all'aperto.

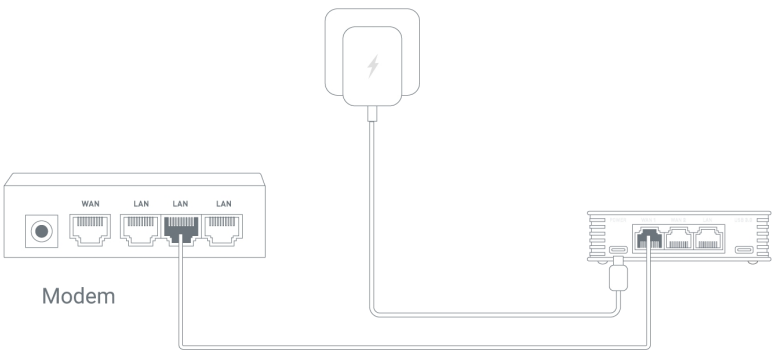
4.2.1 Connessione a Internet tramite cavo Ethernet

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.

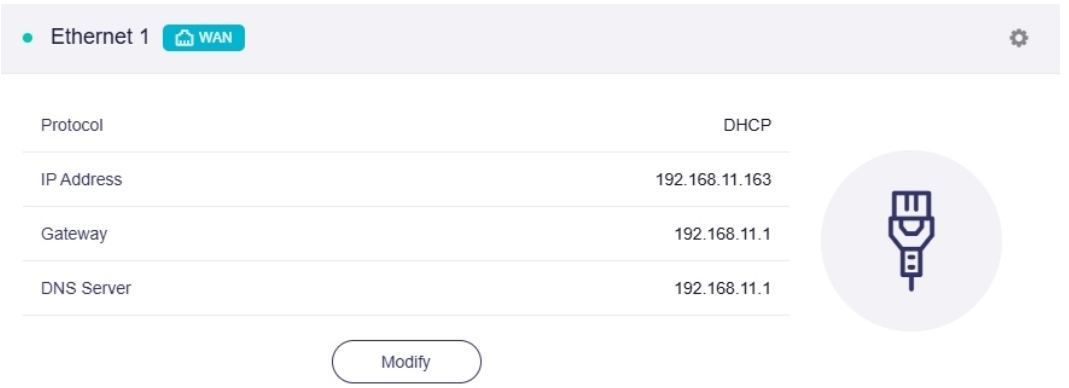
Configurazione di base

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.

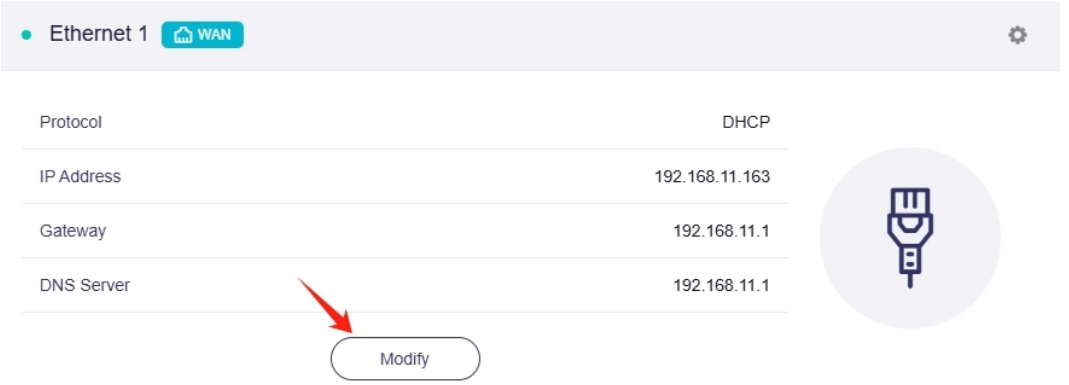


2. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Ethernet**. Se la connessione ha esito positivo, la sezione Ethernet visualizzerà i dettagli della rete, inclusi protocollo, indirizzo IP, gateway e Server DNS.



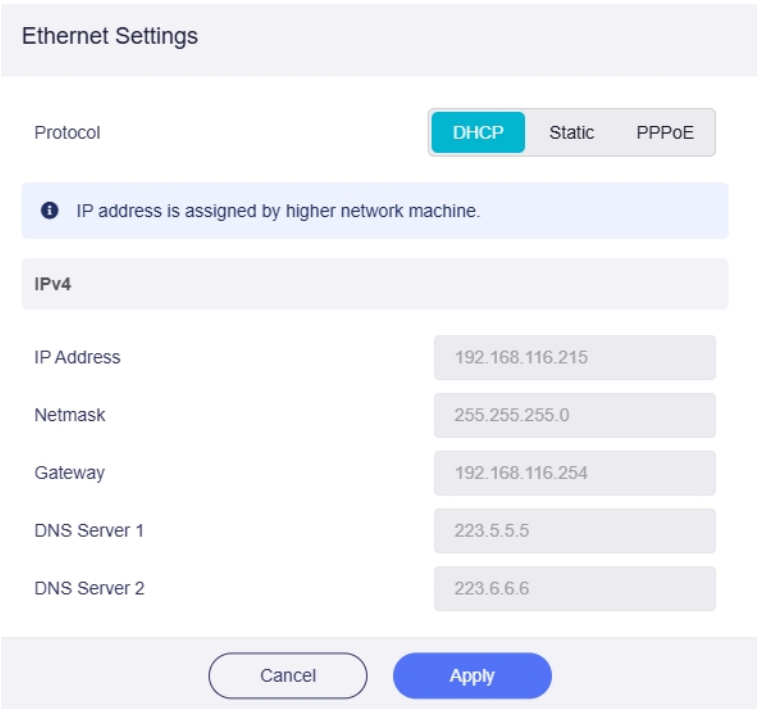
Protocollo

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



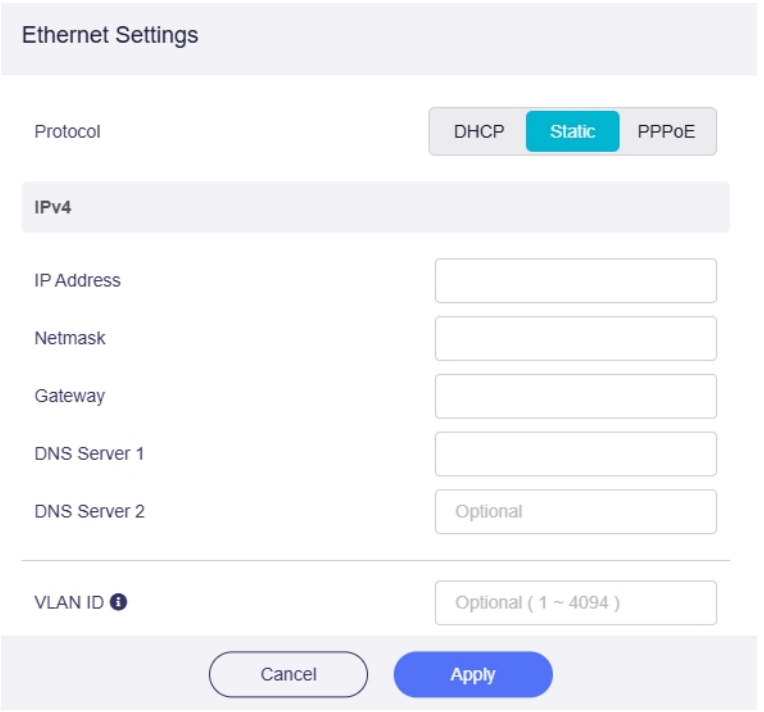
- **DHCP**

  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.



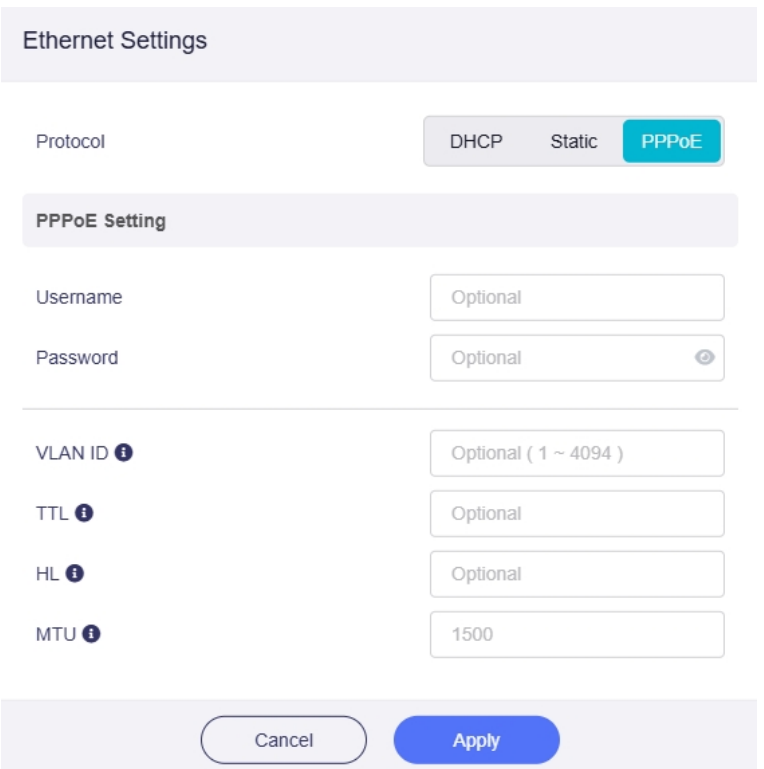
- **Statico**

  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).



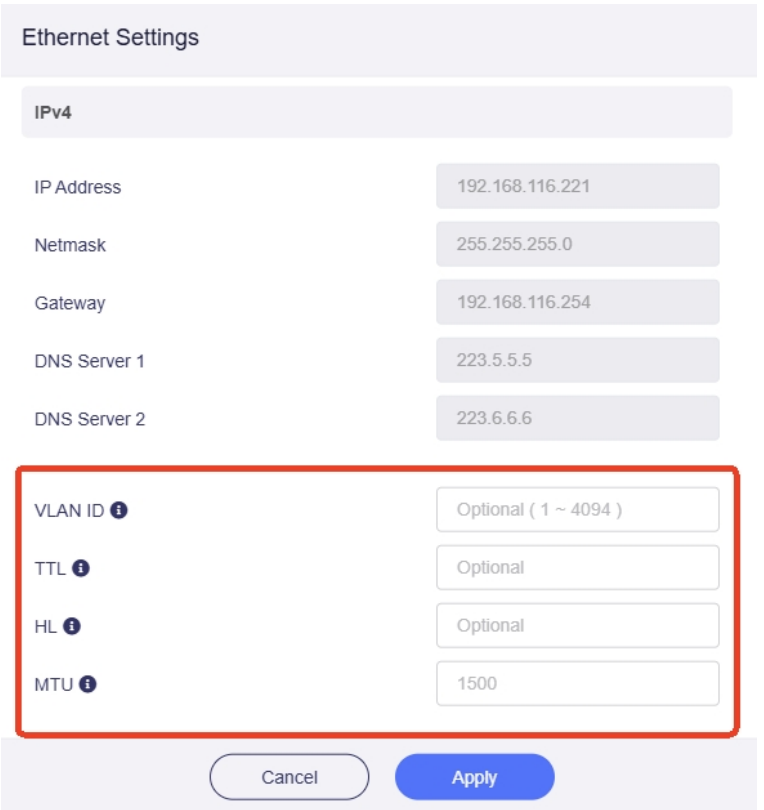
- **PPPoE**

  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.



Impostazioni avanzate

Oltre alle impostazioni essenziali, ci sono anche alcune impostazioni avanzate facoltative per i tre protocolli precedenti.



- **ID VLAN**

  Questa impostazione è necessaria solo se il server del provider richiede che l'interfaccia utilizzi uno specifico ID VLAN con tag.
- **TTL**

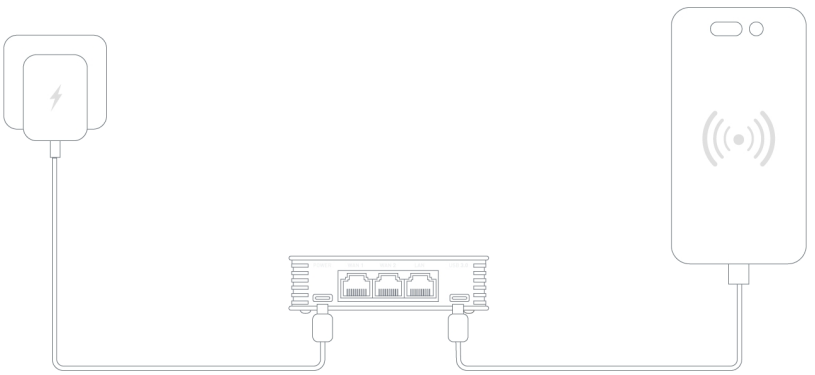
  TTL (Durata To Live) definisce il tempo massimo in cui i pacchetti possono sopravvivere nella rete. Per impostazione predefinita, il router diminuisce di 1 il TTL dei pacchetti in entrata dai dispositivi client prima di inoltrarli. Se è necessario sovrascriverlo, è possibile impostare un valore fisso qui. L'impostazione TTL è valida solo per IPv4.
- **HL**

  In IPv6, il campo HL (Hop Limit) limita il numero di hop di trasmissione per i pacchetti di dati nella rete, fungendo da equivalente di TTL in IPv4.
- **MTU**

  Il valore MTU predefinito è 1500 byte.

4.2.2 Connessione a Internet tramite tethering USB

Il collegamento di uno smartphone al router tramite un cavo USB si chiama Tethering, che può condividere la rete dati mobile del dispositivo (ad esempio 4G/5G) con il router. Questo è un metodo conveniente per l'accesso temporaneo a Internet, soprattutto all'aperto o in aree senza banda larga fissa.

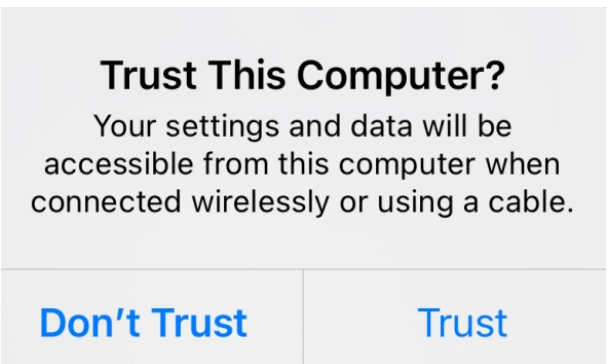


Il modem host-less funziona anche in Tethering durante la configurazione del modem.

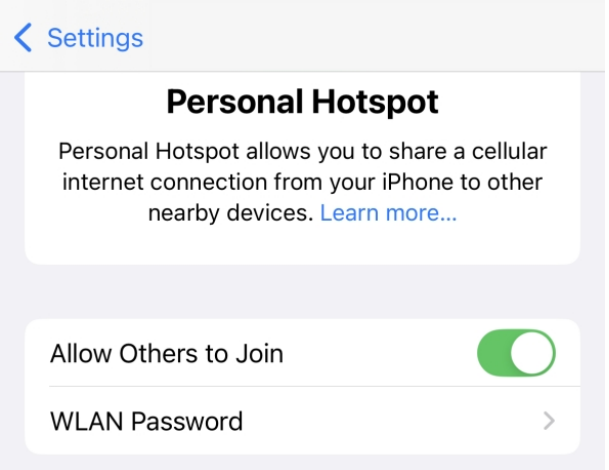
Nota: alcuni operatori di telefonia mobile limitano o addebitano costi aggiuntivi per il tethering. Ti consigliamo di verificare con il tuo operatore.

Tethering dell'iPhone

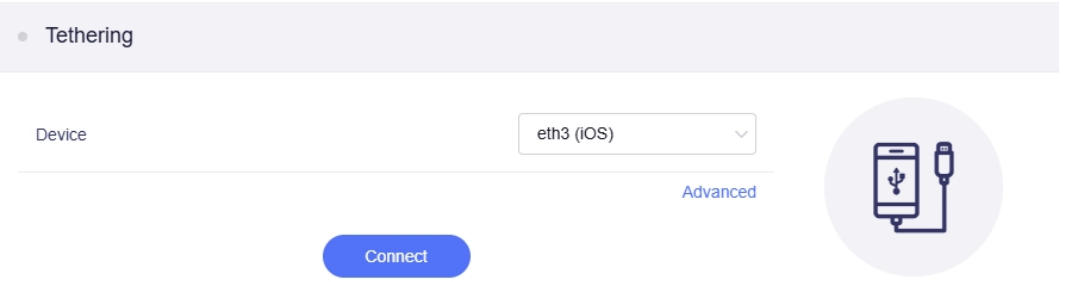
1. Collega un iPhone alla porta USB del router con un cavo USB. Quando viene chiesto se autorizzare il dispositivo, tocca **Autorizza** per continuare.



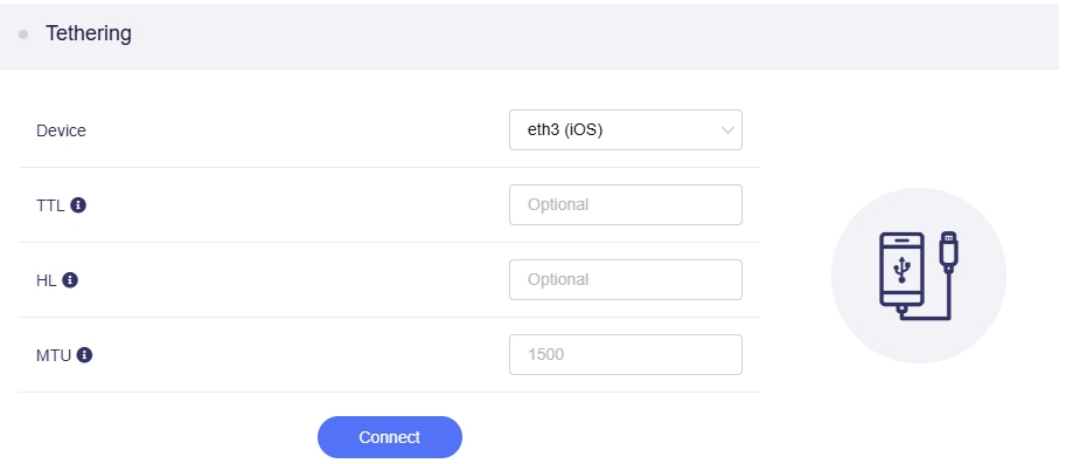
2. Su iPhone, vai in **Impostazioni** > **Hotspot personale** e attiva **Consenti agli altri di accedere**.



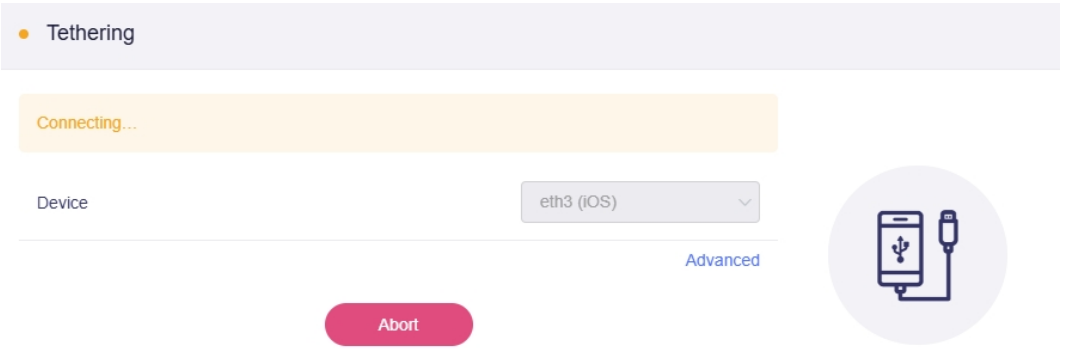
3. Collega un computer o un altro telefono al router. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Tethering**, quindi fai clic su **Connetti**.



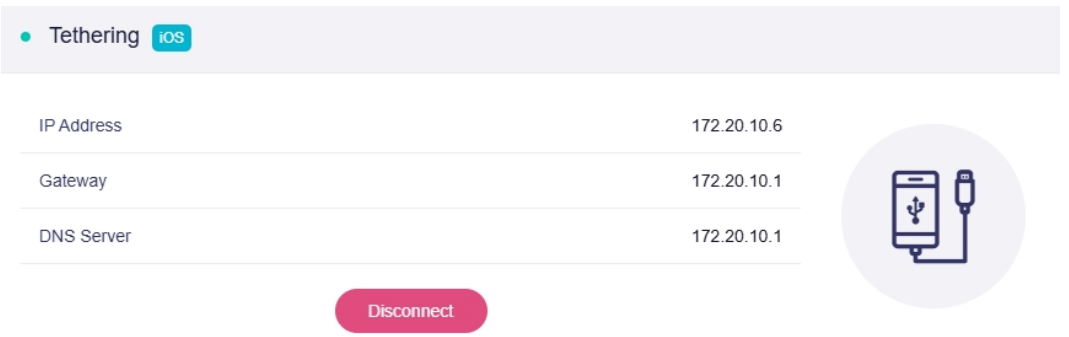
Se è necessario configurare impostazioni avanzate, come TTL, HL e MTU, fai clic su **Avanzate** per personalizzare queste impostazioni prima di fare clic su **Connetti**.



4. Inizierà la connessione.

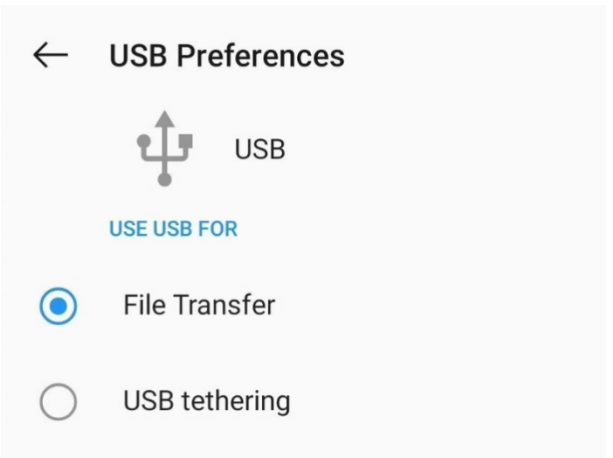


Una volta connesso, questa pagina visualizzerà i dettagli della connessione Tethering.

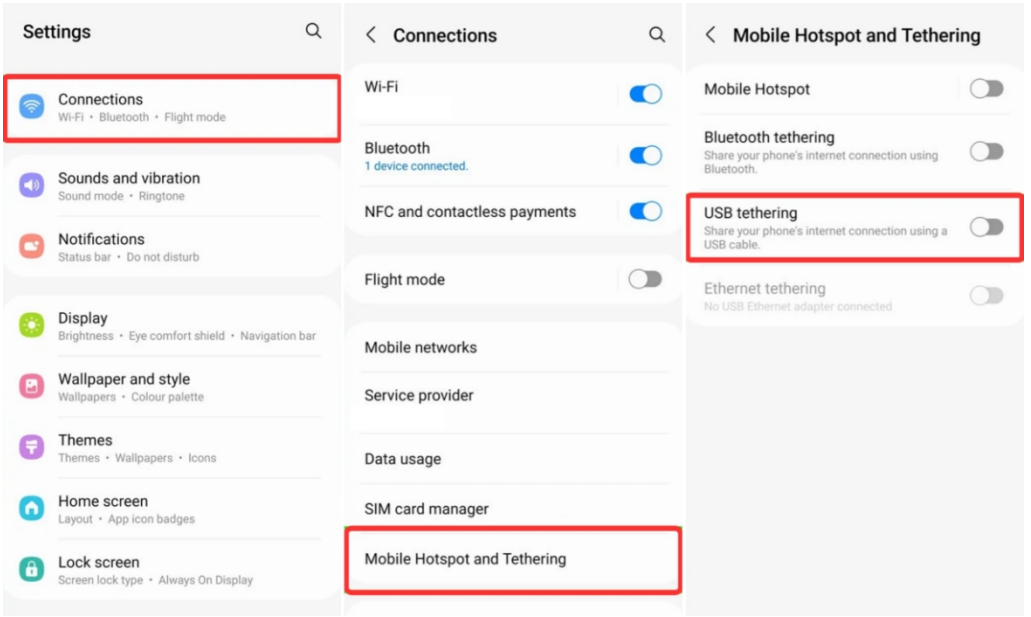


Tethering Android

1. Collega un telefono Android alla porta USB del router utilizzando un cavo USB. Potrebbe apparire una finestra di dialogo di sistema che richiede le preferenze USB. Seleziona **Tethering USB** o **Trasmissione file**, se richiesto.

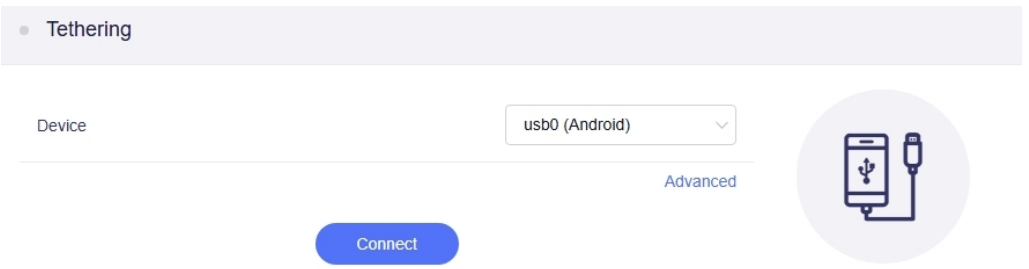


2. Vai alle **Impostazioni** del tuo telefono > **Rete e Internet** > **Hotspot personale**. Abilita **hotspot personale** o **tethering USB**.

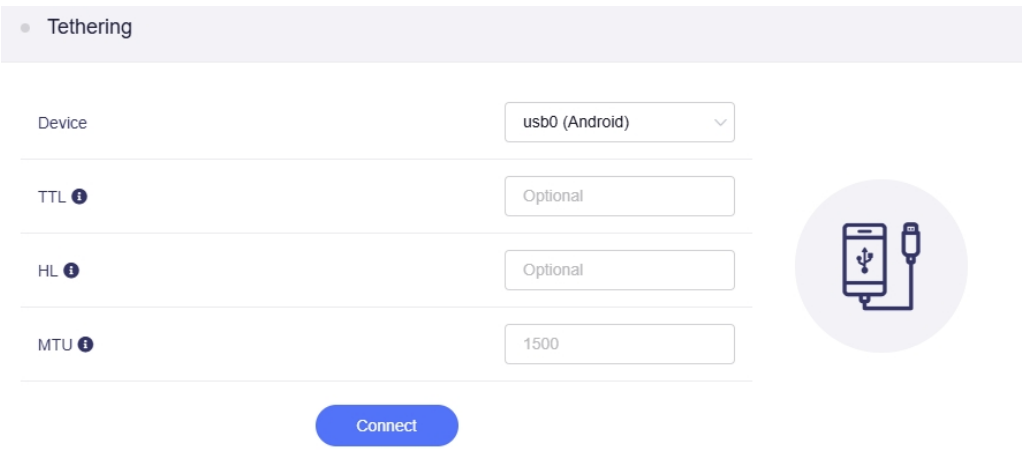


(I passaggi per abilitare Tethering USB variano in base alla marca. Controlla le impostazioni del tuo dispositivo per la posizione esatta e, se necessario, contatta l'assistenza del produttore.)

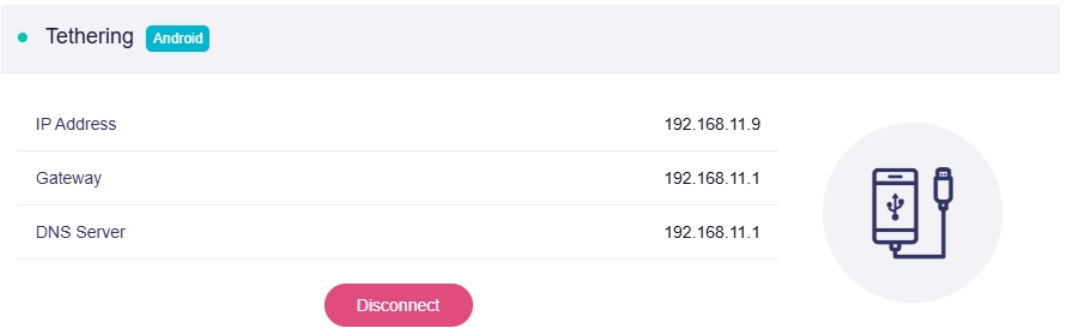
3. Collega un computer o un altro telefono al router, quindi accedi al pannello di amministrazione web del router, vai su **INTERNET** > **Tethering**. Fai clic su **Connetti**.



Se è necessario configurare impostazioni avanzate come TTL, HL e MTU, fai clic su **Avanzate** per personalizzare queste impostazioni prima di fare clic su **Connetti**.



4. Inizierà la connessione. Una volta connesso, questa pagina visualizzerà lo stato della connessione Tethering.



Risoluzione dei problemi

Se la connessione tethering non riesce, prova questi passaggi per la risoluzione dei problemi:

- Utilizzare l'alimentatore originale del router.
- Scollega e ricollega il cavo USB.
- Utilizza un altro cavo USB. Assicurati che supporti il trasferimento dei dati (non solo la ricarica).
- Spegni e attiva "Tethering USB" per alcune volte (per telefoni Android).
- Disattiva e riattiva più volte “Consenti agli altri di accedere” (su iPhone).
- Riavvia lo smartphone e riprova.

Se il problema persiste, contatta il nostro supporto tecnico all'indirizzo support@gl-inet.com.

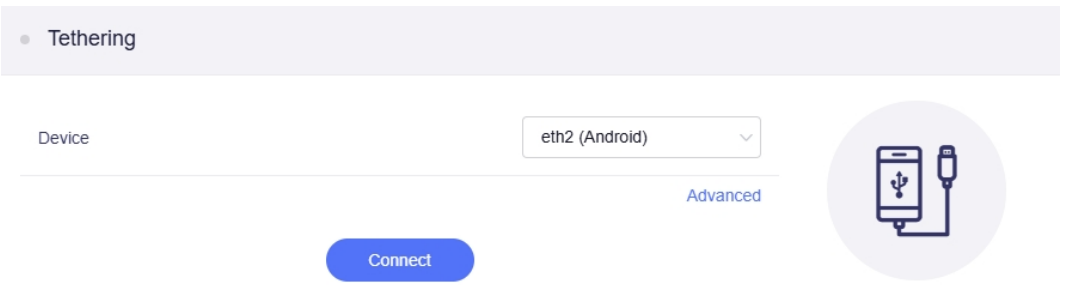
4.2.3 Connessione a Internet tramite modem USB

Connetti il router a Internet inserendo un modem USB abilitato per la rete cellulare nella sua porta USB. Ciò consente al router di connettersi a Internet tramite reti 4G/5G, fornendo connettività senza fare affidamento sulla banda larga su linea fissa. È adatto per l'uso nel veicolo o per attività all'aperto. Tieni presente che questa connessione viene implementata tramite l'interfaccia Tethering o Cellulare del router.

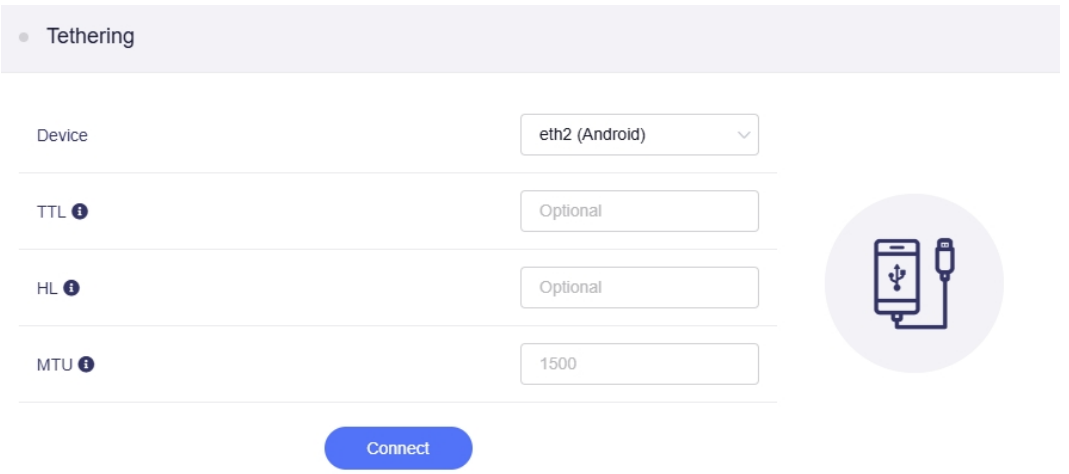
Per Brume 3, è necessario un **adattatore aggiuntivo da USB-C a USB-A** per collegare un modem USB.

Segui i passaggi seguenti per connettere il router a Internet tramite un modem USB.

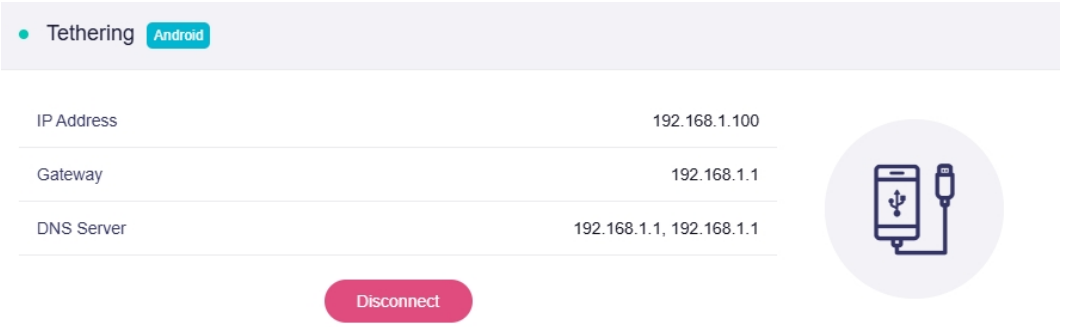
1. Collega un modem USB con una scheda SIM preinstallata alla porta USB del router prima di accenderlo.
2. Accedi al pannello di amministrazione web del router, vai su **INTERNET** > **Tethering**, quindi fai clic su **Connetti**.



Se è necessario configurare impostazioni avanzate, come TTL, HL e MTU, fai clic su **Avanzate** per personalizzare queste impostazioni, quindi fai clic su **Connetti**.

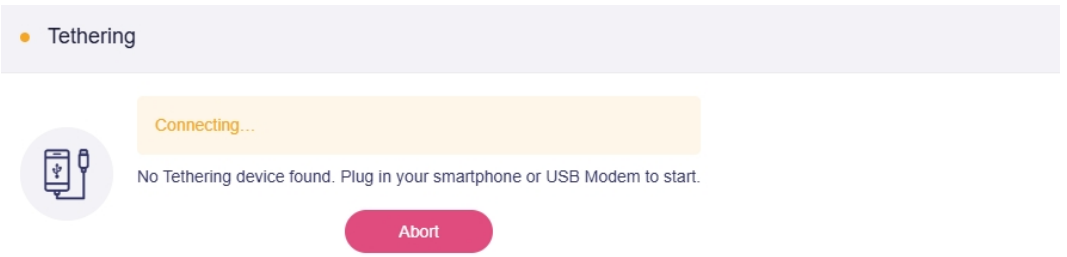


3. Inizierà la connessione. Una volta connesso, questa pagina mostrerà i dettagli della rete.



Suggerimenti:

1. Dopo la configurazione iniziale, se si riavvia il router con il modem USB ancora collegato o si reinserisce il modem nel router, il modem USB verrà riconosciuto automaticamente e verrà stabilita una connessione di rete senza fare nuovamente clic su "Connetti".
2. Se scolleghi il modem USB, la pagina visualizzerà lo stato mostrato di seguito, indicando "Nessun dispositivo Tethering trovato", mentre l'interfaccia Tethering rimarrà nello stato "Connessione in corso".



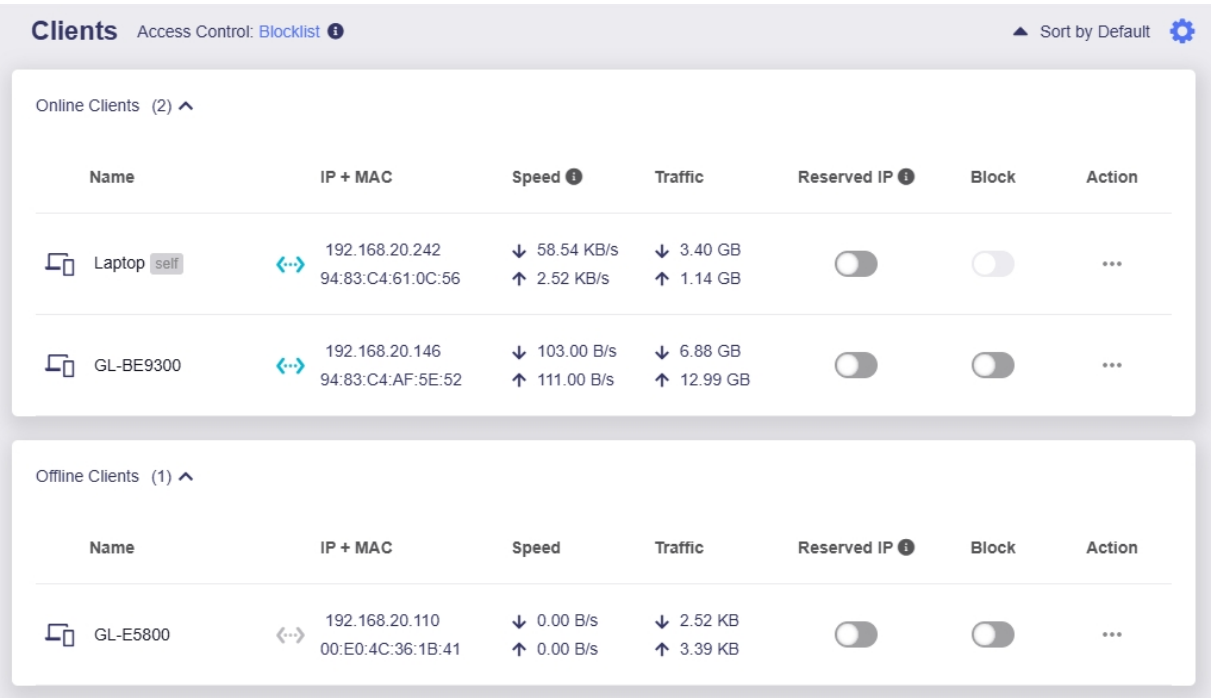
Capitolo 5

Client

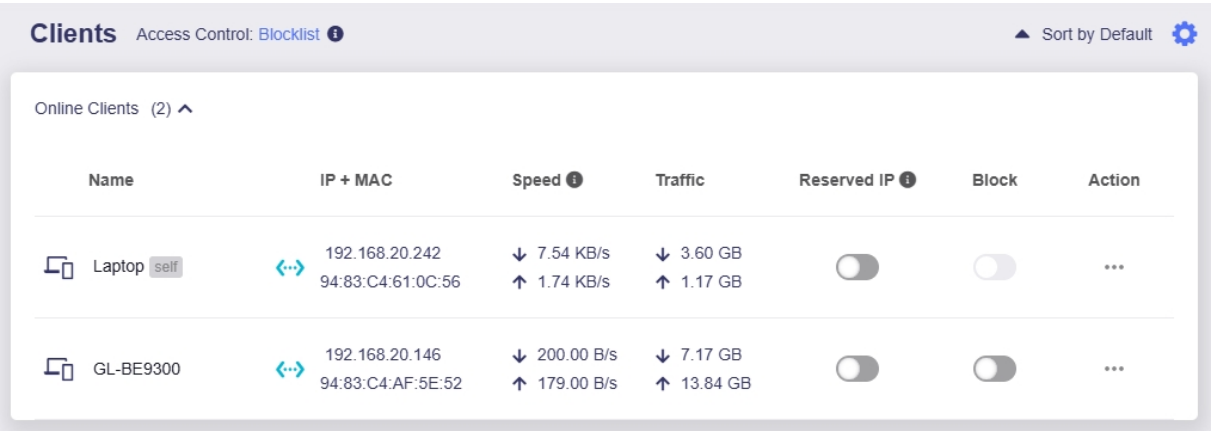
Questo capitolo ti guida a visualizzare i dettagli dei dispositivi collegati e a gestirne le connessioni.

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.



5.1 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.

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).

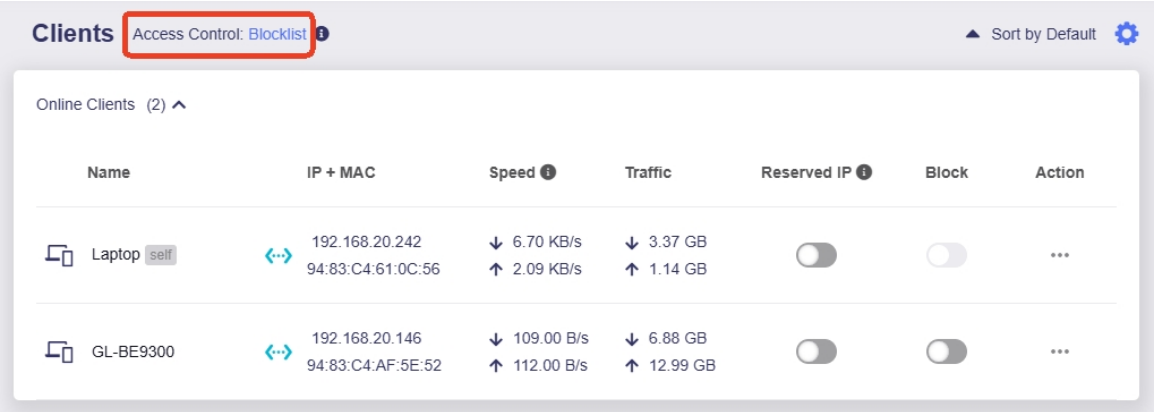
4. **Traffico**: la quarta colonna mostra il traffico Internet del dispositivo connesso.

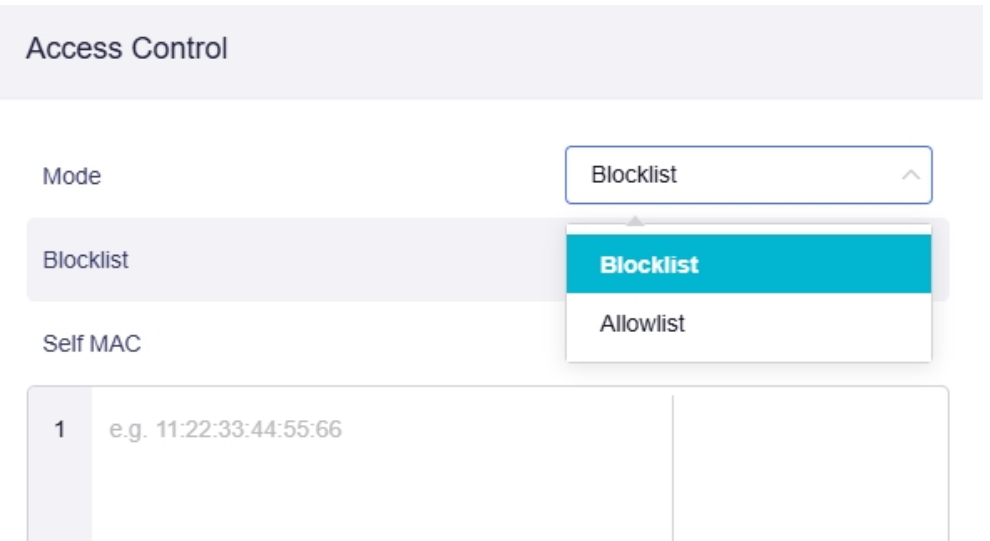
5. **Prenota IP**

   Nella quinta colonna, puoi riservare l'indirizzo IP per il dispositivo connesso con un clic. Quando specifichi un indirizzo IP riservato per un client all'interno della rete locale, riceverà sempre lo stesso indirizzo IP ogni volta che si connette al router.

6. **Lista bloccata**

   Nella sesta colonna puoi bloccare specifici dispositivi collegati con un clic.
   La regola Controllo degli accessi è Blocklist per impostazione predefinita e puoi cambiarla in Lista consentita dall'alto secondo necessità.



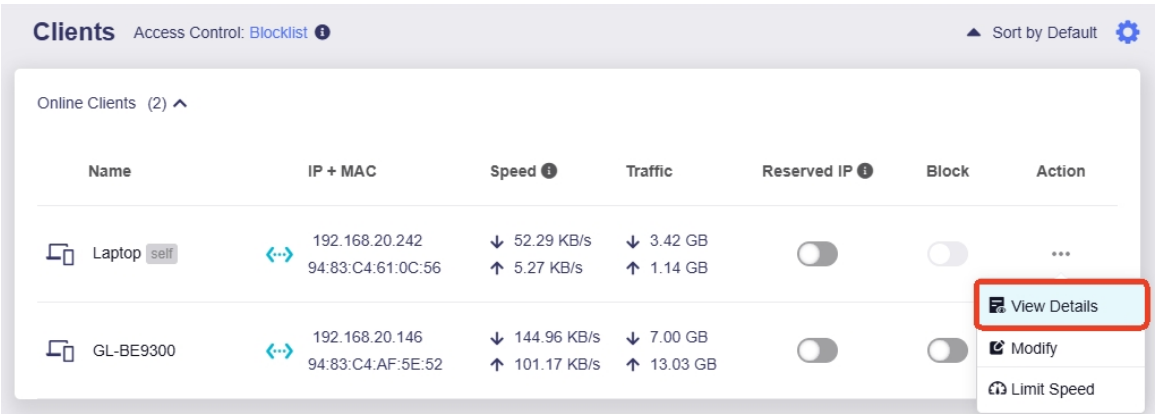


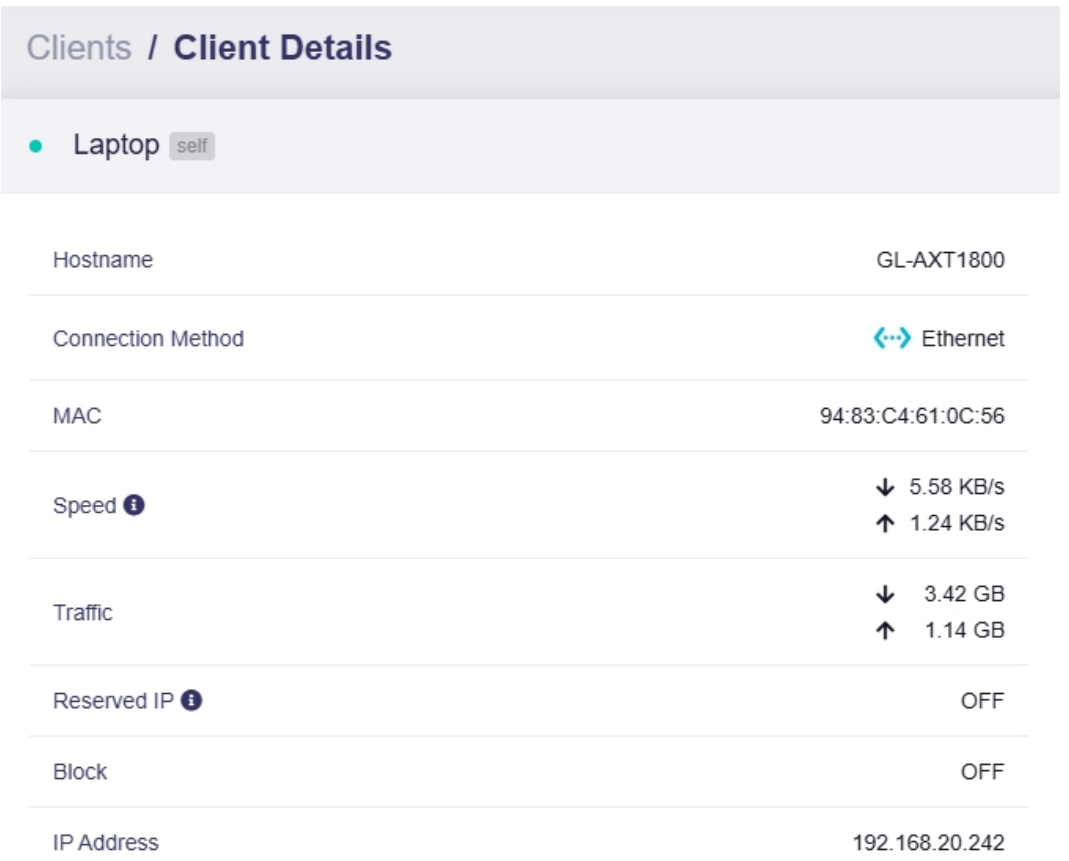
- **Lista nera**: i dispositivi con indirizzi MAC nella lista nera non possono connettersi a questo router. Tieni presente che il blocco del client si basa sull'indirizzo MAC del dispositivo. Se la prossima volta il dispositivo bloccato utilizza un indirizzo MAC diverso, può comunque riuscire a connettersi 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.

5.2 Azione

1. **Visualizzazione dettagli**

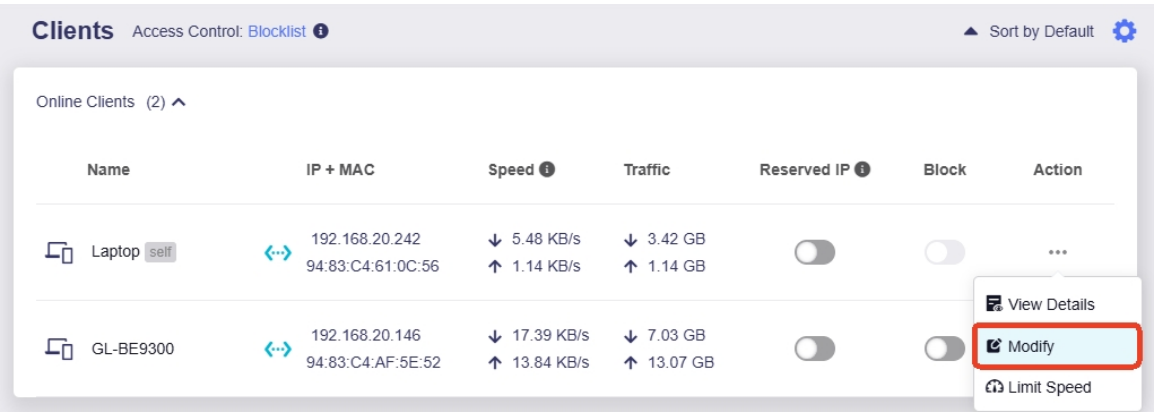
   Fai clic sull'icona a tre punti nella colonna **Azione**, quindi su **Visualizzazione dettagli** dal menu a discesa per visualizzare i dettagli del dispositivo in un'unica pagina.

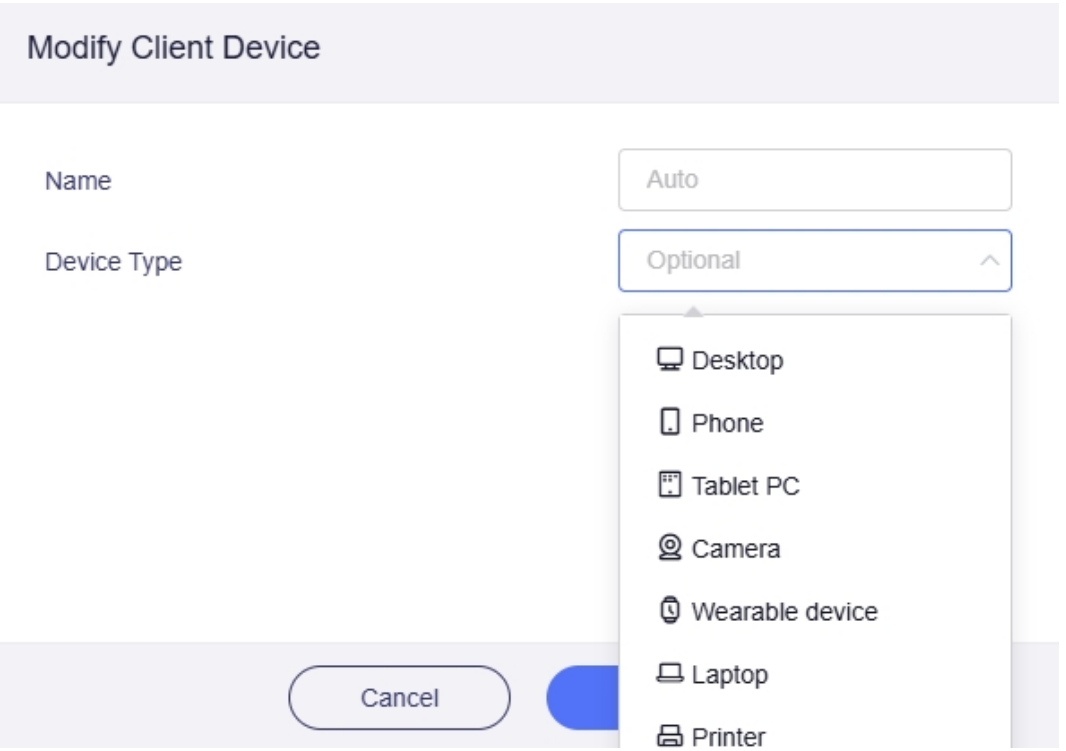




2. **Modifica**

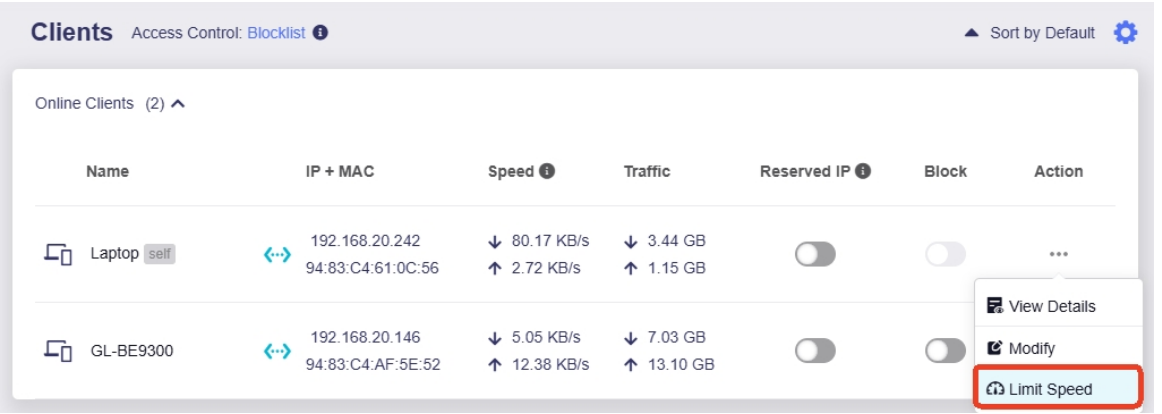
Fai clic sull'icona a tre punti nella colonna **Azione**, quindi su **Modifica** dal menu a discesa per modificare il nome e il tipo del dispositivo.



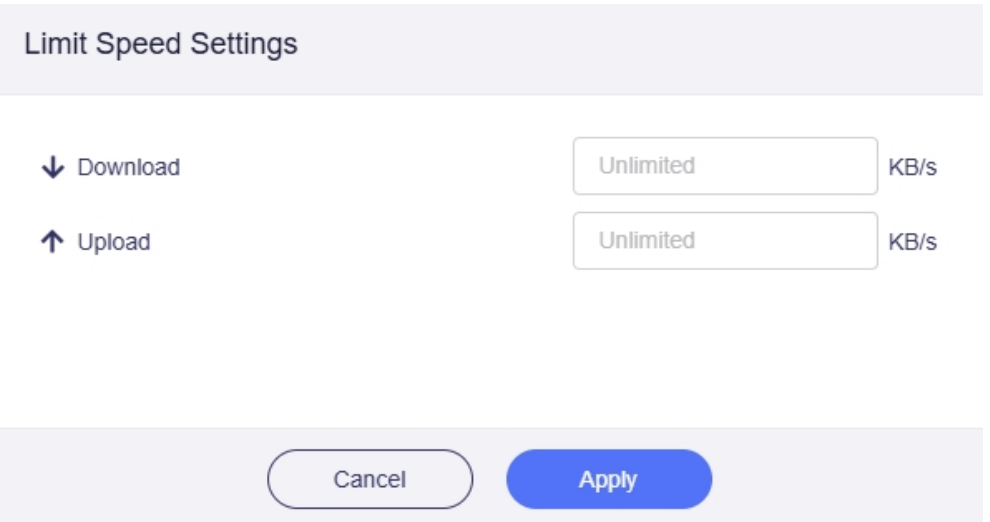


3. **Limita velocità**

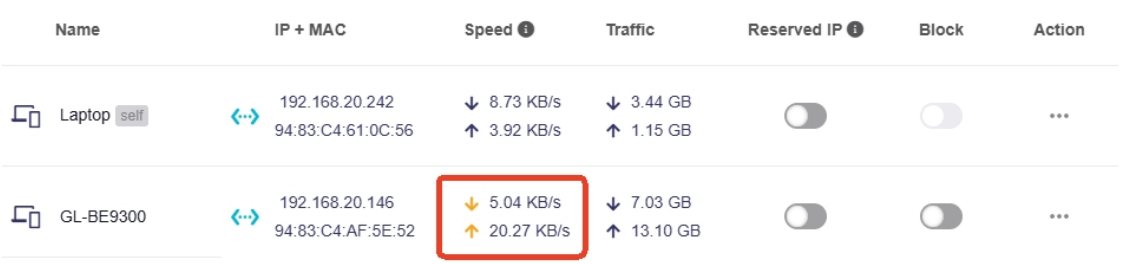
Fai clic sull'icona a tre punti nella colonna **Azione** e fai clic su **Limita velocità** dal menu a discesa.



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



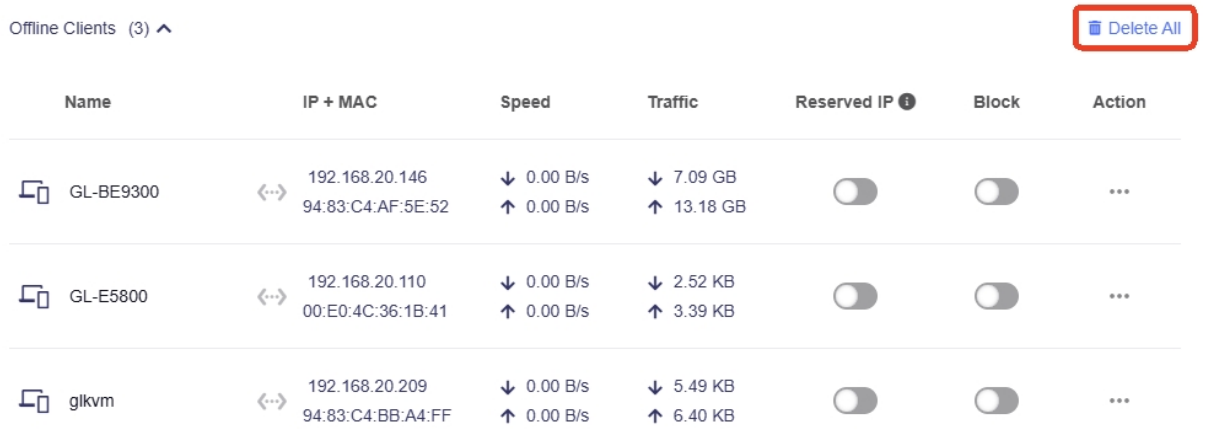
Se a un dispositivo è stata applicata una limitazione di velocità, le frecce della velocità di caricamento/download diventeranno gialle.



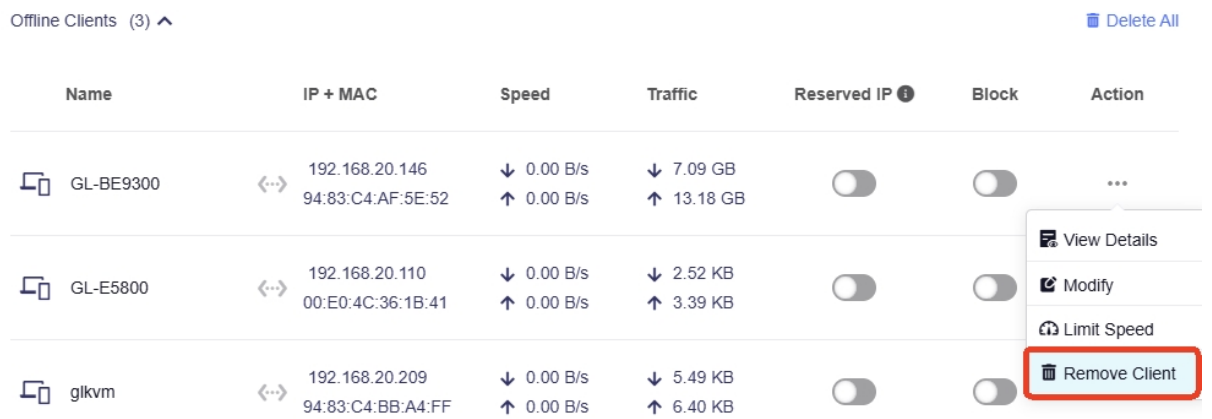
Suggerimento: se l'opzione Limita velocità non è visibile, vai in **RETE** > **Accelerazione di rete** e disattiva l'accelerazione. L'opzione Limita velocità diventerà disponibile.

5.3 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.

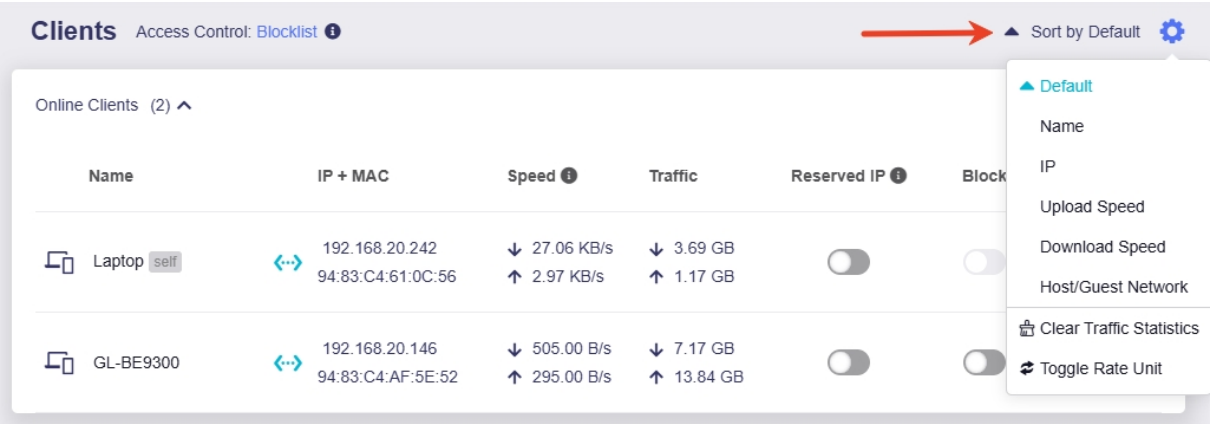


Per rimuovere un client specifico, fai clic sull'icona a tre punti nella colonna **Azione**, quindi seleziona **Rimuovi client** dal menu a discesa.



5.4 Ordinamento

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



Le regole di ordinamento predefinite sono le seguenti:

- Il dispositivo personale (ovvero il dispositivo utilizzato per accedere al pannello di amministrazione web del router) è sempre elencato per primo.
- 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.

Capitolo 6

Servizi cloud

Questo capitolo presenta due servizi cloud: GoodCloud e AstroWarp.

6.1 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.

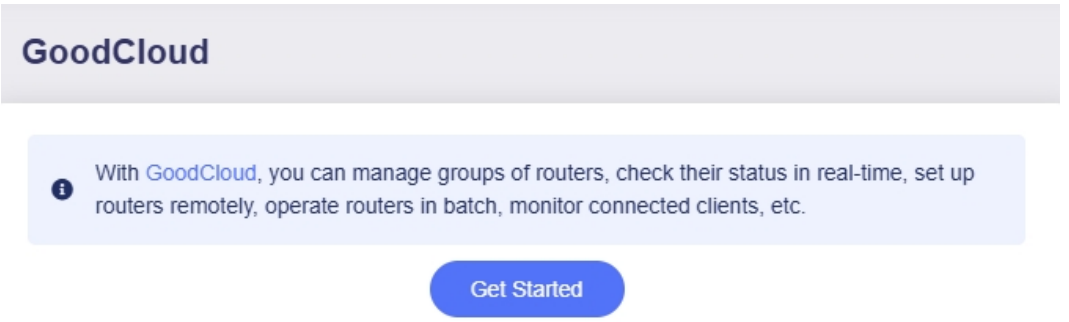
Con GoodCloud puoi:

- 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

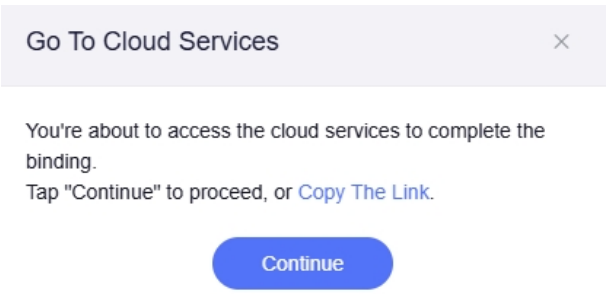
Alcune funzionalità sono disponibili nel piano Enterprise e nel piano VAR (rivenditore a valore aggiunto). Vedi qui per i dettagli.

6.1.1 Attivazione di GoodCloud

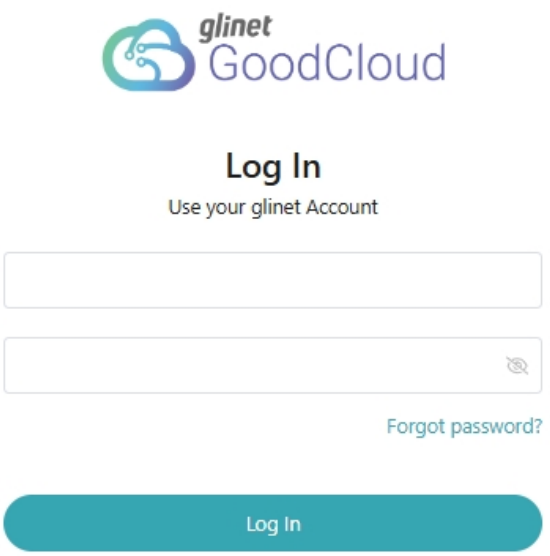
1. Accedi al pannello di amministrazione web del tuo router, vai a **SERVIZI CLOUD** > **GoodCloud** e fai clic su **Inizia.**



2. Nella finestra pop-up, fai clic su **Continua**.



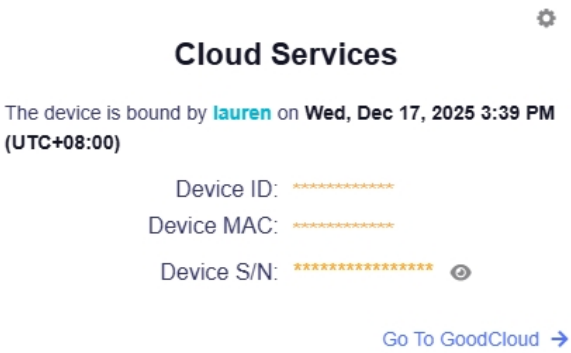
3. Verrai reindirizzato alla pagina di accesso GoodCloud. Accedi con il tuo account GL.iNet. Se non disponi di un account, fai clic su **Iscriviti per registrarti** e accedere. Una volta effettuato l'accesso, conferma le informazioni sul dispositivo e collegalo al tuo account.



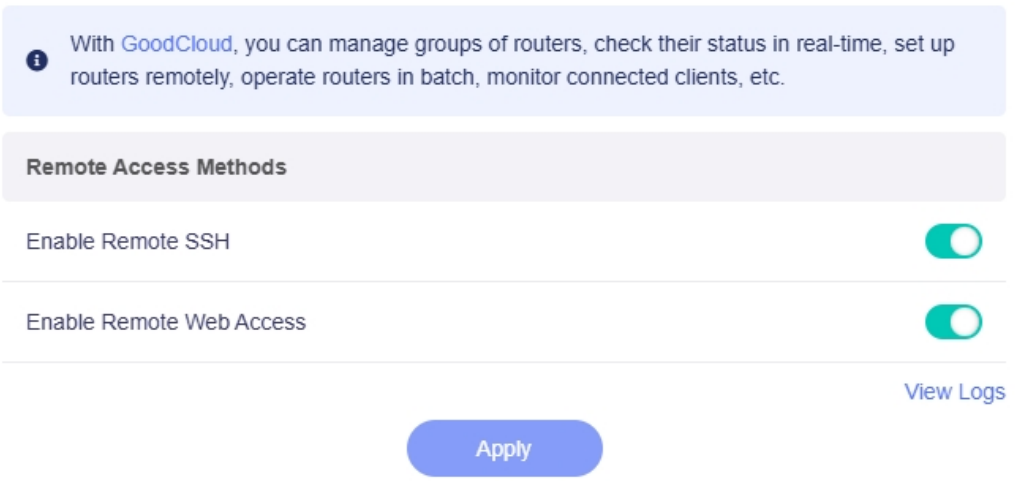
Suggerimenti:

- 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.

4. Dopo aver eseguito correttamente l'associazione, fare clic **sull'icona Cloud** nell'angolo in alto a destra del pannello di amministrazione web. Verranno quindi visualizzati i dettagli del dispositivo associato, inclusi l'account associato, la data di associazione, l'ID dispositivo, il MAC del dispositivo e il S/N del dispositivo.



5. Vai a **SERVIZI CLOUD** > **GoodCloud** e abilita accesso remoto.
GoodCloud abilita accesso remoto al pannello di amministrazione web e al terminale del router associato. Ciò è particolarmente utile per la gestione remota, la configurazione della rete e la risoluzione dei problemi. Puoi abilitare o disabilitare accesso remoto per il tuo router qui.



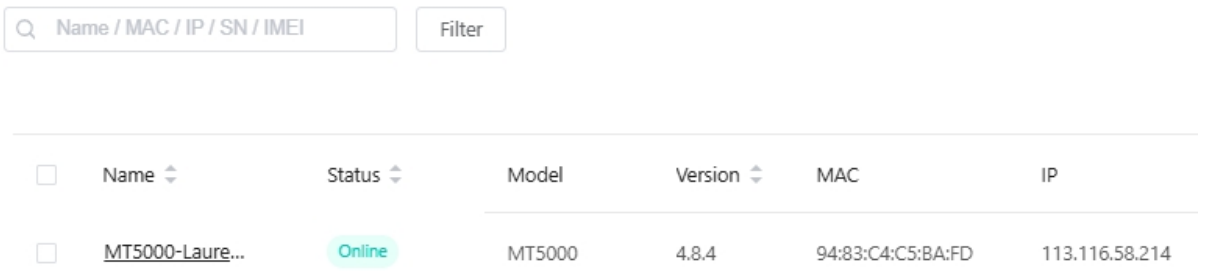
- **SSH remoto**: accedi in remoto al terminale del router da GoodCloud utilizzando SSH.

- **Accesso web remoto**: accesso remoto al pannello di amministrazione web del router da GoodCloud tramite HTTP/HTTPS.
- **Visualizza registri**: reindirizza alla pagina Registro e visualizza il registro Cloud.

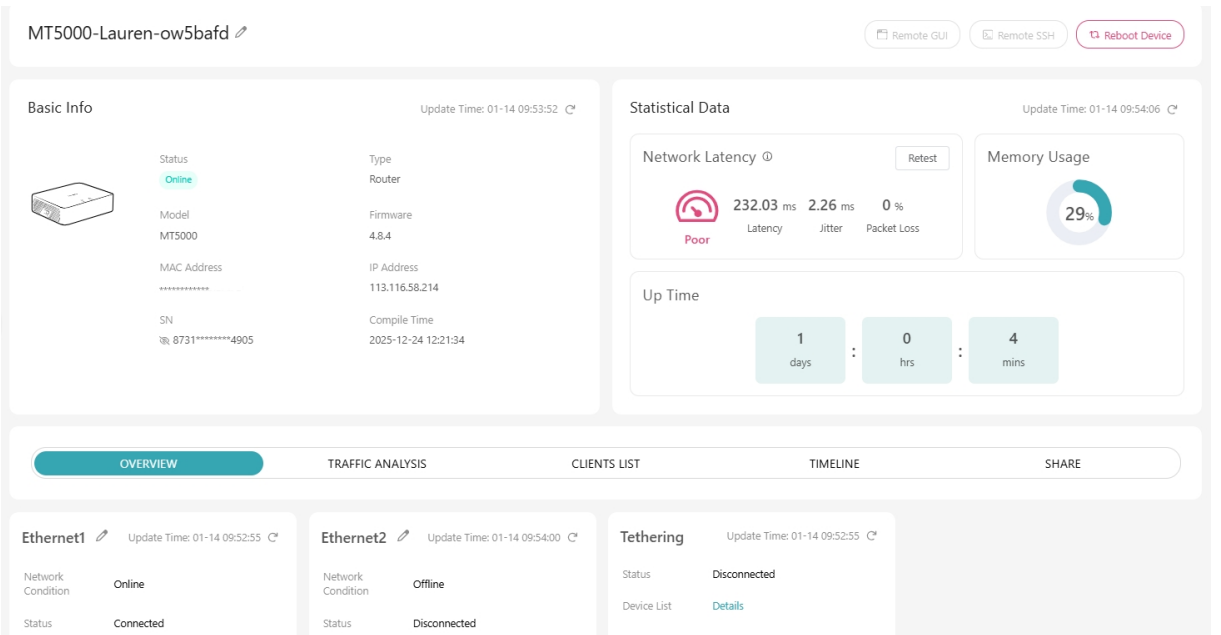
6.1.2 Gestione del router

Controlla i dettagli del dispositivo

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

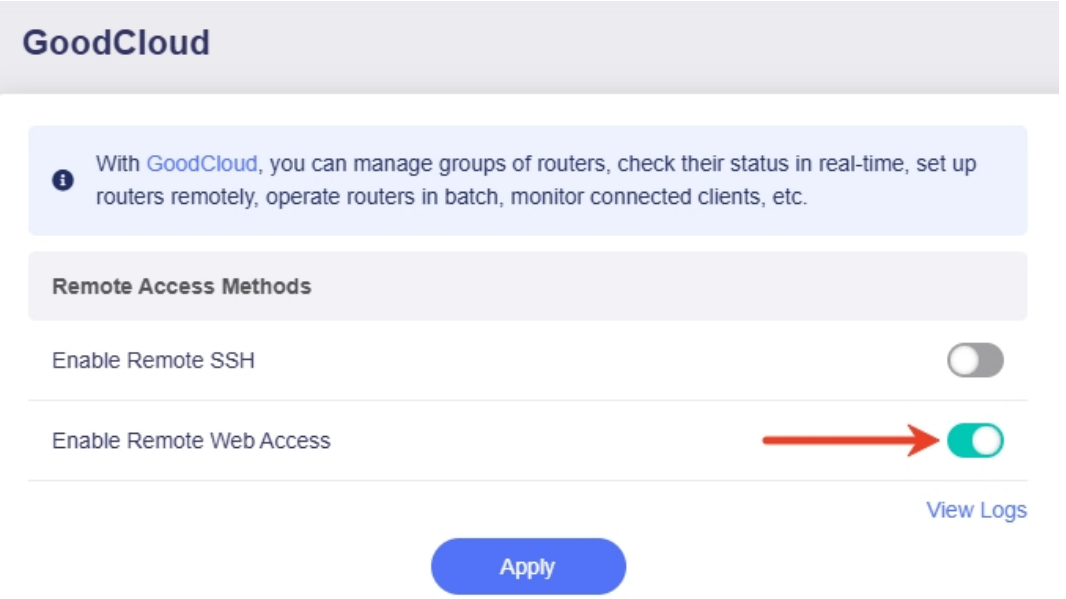


Fare clic sul nome del dispositivo per accedere alla pagina dei dettagli del dispositivo, che visualizza informazioni di base, dati statistici, panoramica della rete, elenco client e sequenza temporale. Puoi anche eseguire operazioni avanzate, come l'accesso remoto al router e il riavvio del dispositivo.

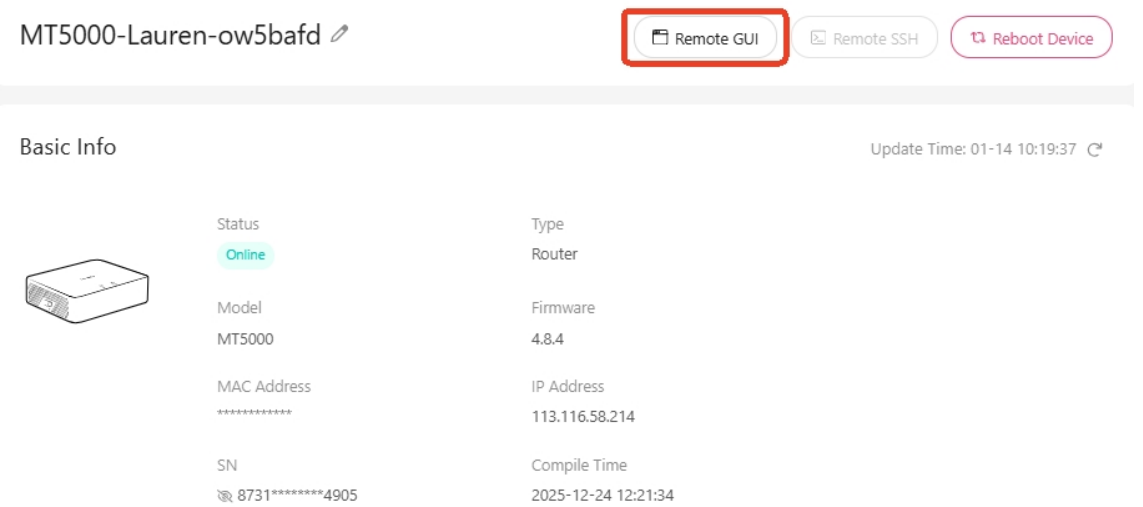


Accesso remoto all’interfaccia web

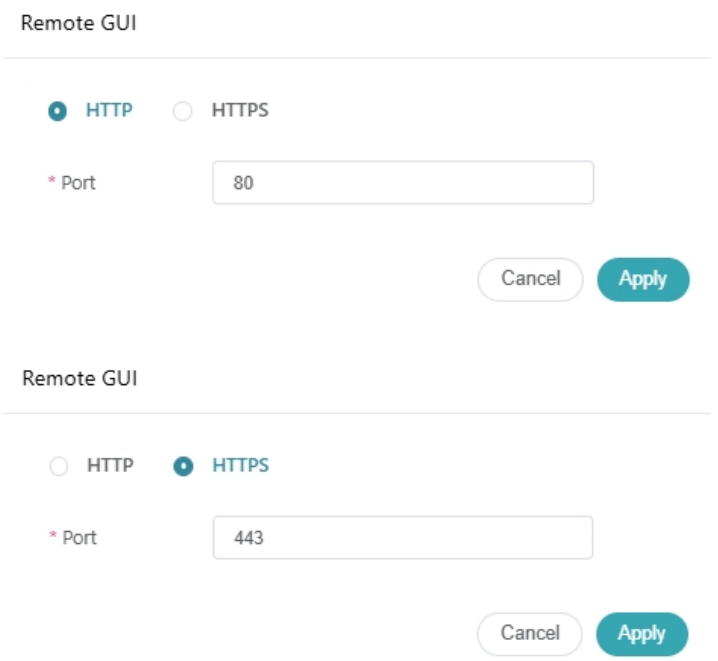
1. Accedi al pannello di amministrazione web del router, vai a **SERVIZI CLOUD** > **GoodCloud**, abilita **Accesso web remoto**, quindi fai clic su **Applica**.



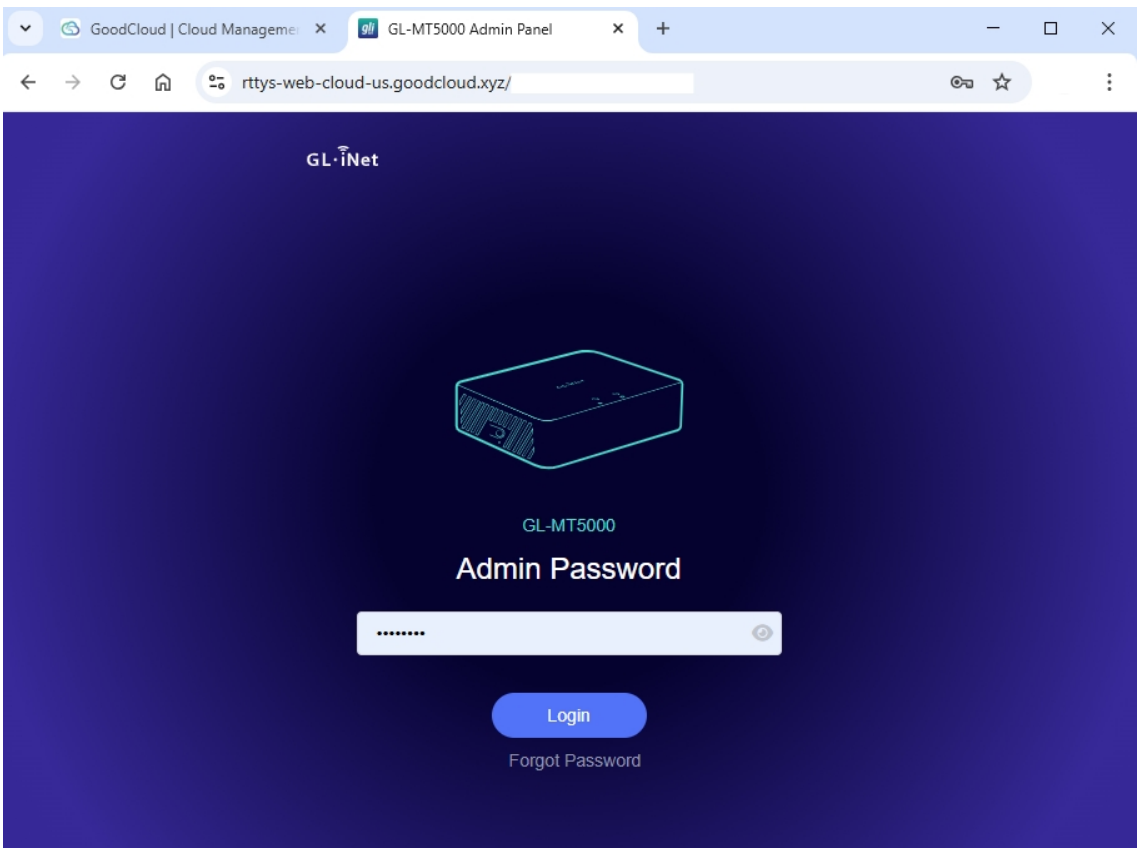
2. Accedi alla piattaforma GoodCloud e vai a **Dispositivo** > **Dispositivi associati**. Fai clic sul dispositivo a cui desideri accedere e accederai alla pagina dei dettagli del dispositivo.
3. Nella pagina dei dettagli del dispositivo, fai clic sul pulsante **GUI remota** nell'angolo in alto a destra.



4. Seleziona il protocollo di trasferimento e la porta. Le impostazioni predefinite sono **HTTP** e Porta **80**. È possibile modificare il protocollo in HTTPS secondo necessità e la porta cambierà automaticamente in 443. Quindi fare clic su **Applica**.

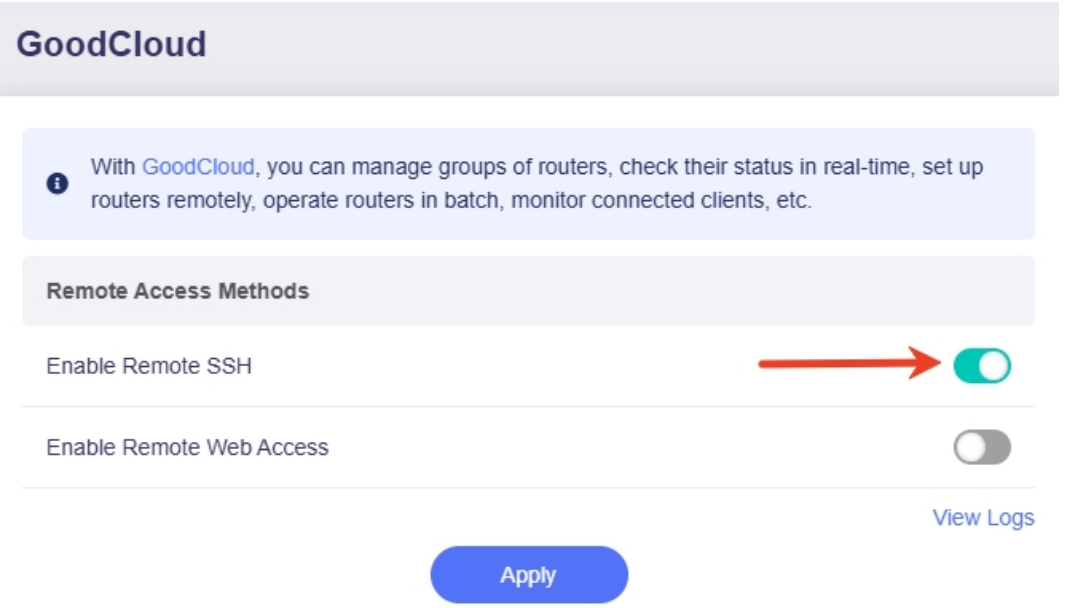


5. Verrai reindirizzato alla pagina di accesso del router. Inserisci la password dell'amministratore per accedere da remoto al pannello di amministrazione web del router.

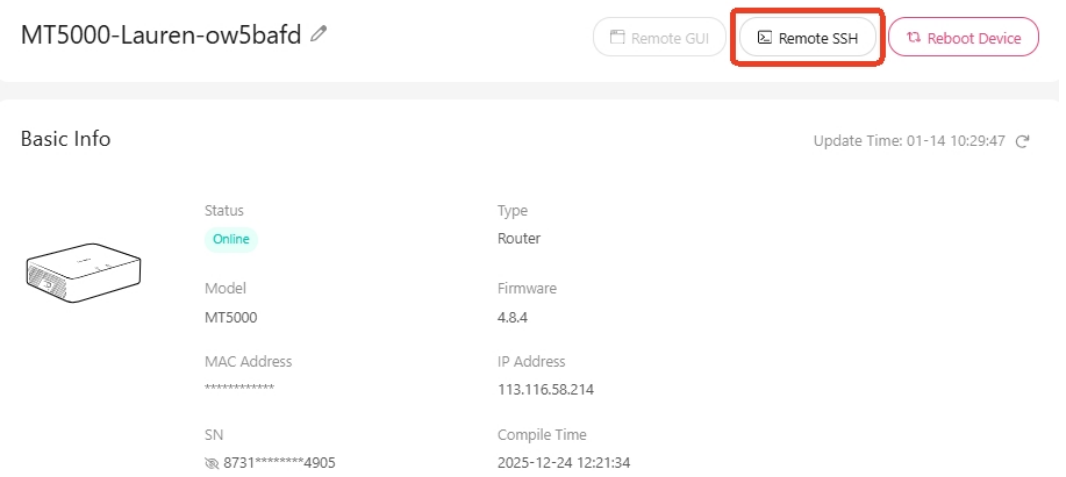


Accesso remoto al terminale

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



2. Accedi alla piattaforma GoodCloud e vai a **Dispositivo** > **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.

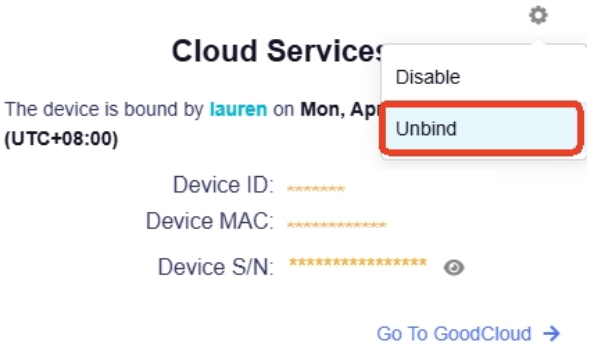


4. Registro come **root** e inserisci la password per accedere al terminale del tuo router.

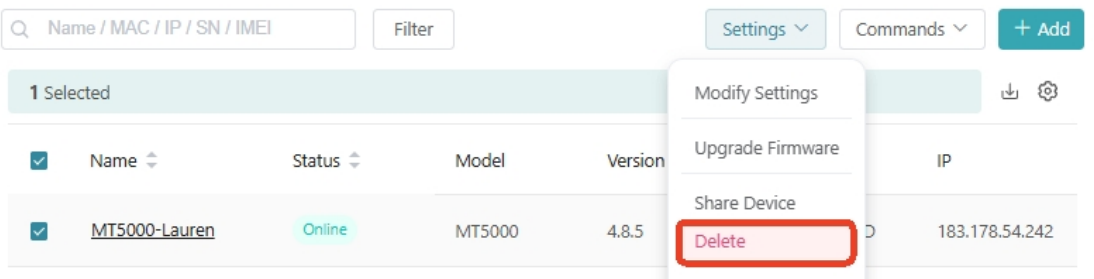

GL-MT5000 login: root
Password:
BusyBox v1.33.2 (2025-12-24 12:15:29 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-MT5000:~#

6.1.3 Dissociazione del dispositivo

Nel pannello di amministrazione web del router, fai clic sull'icona Cloud nell'angolo in alto a destra. Nel menu a discesa, fai clic sull'icona a forma di ingranaggio e seleziona **Dissocia**. Il tuo dispositivo verrà quindi scollegato dal tuo account GoodCloud.

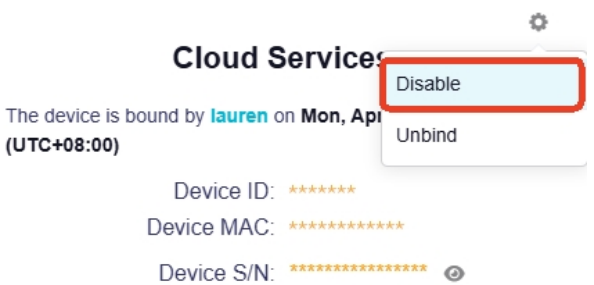


In alternativa, accedi alla piattaforma cloud e vai a **Dispositivo** > **Dispositivi associati**. Seleziona il dispositivo che desideri scollegare, fai clic su **Impostazioni** nell'angolo in alto a destra, quindi seleziona **Elimina**. Il tuo dispositivo verrà quindi scollegato dal tuo account GoodCloud.



6.1.4 Disabilita GoodCloud

Se non desideri più che il dispositivo sia connesso al Cloud, fai clic sull'icona Cloud nell'angolo in alto a destra. Nel menu a discesa, fai clic sull'icona a forma di ingranaggio e seleziona **Disabilita**. Il servizio Cloud verrà quindi disabilitato.



6.2 AstroWarp

AstroWarp è una funzionalità di rete avanzata progettata per i router GL.iNet per fornire reti remote e gestione dei dispositivi senza soluzione di continuità. Integrato nell'SDK del router GL.iNet, adotta il protocollo AmneziaWG con offuscamento del traffico integrato, offrendo connessioni stabili e sicure per accesso remoto affidabile sempre e ovunque.

Questa funzionalità consente l'accesso remoto senza interruzioni alla rete domestica. Puoi configurare e accoppiare direttamente i dispositivi tramite un codice di accesso dinamico nel pannello di amministrazione web, stabilendo rapidamente una connessione sicura tra il tuo router da viaggio e la rete domestica in pochi secondi, senza registrazione o accesso richiesto.

Nota:

1. Non è consigliabile utilizzare AstroWarp con una qualsiasi delle seguenti funzionalità contemporaneamente, poiché ciò potrebbe causare conflitti di routing: GoodCloud da sito a sito, ZeroTier, Tailscale, Tor.
2. Quando AstroWarp è abilitato, non è possibile utilizzare Modalità di rete.

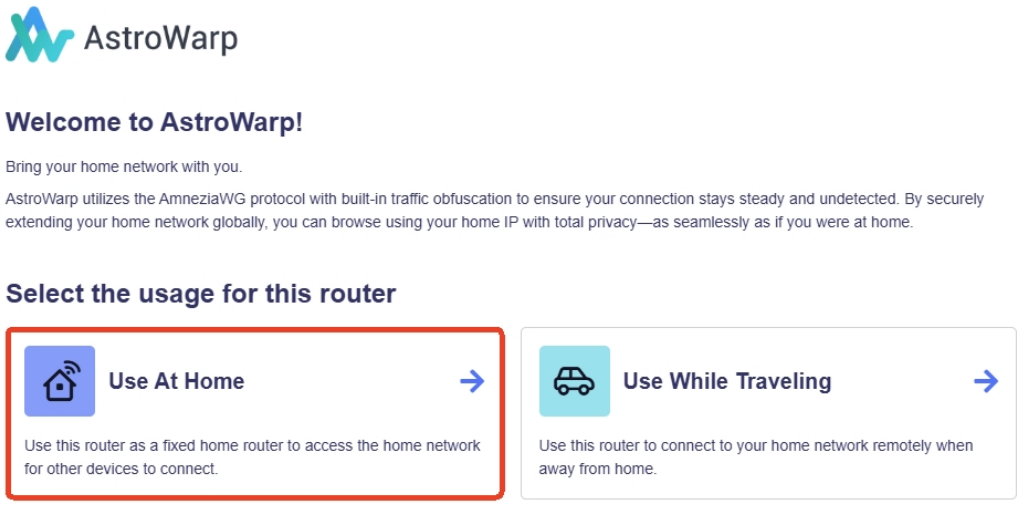
6.2.1 Configurazione rapida

Nell'esempio seguente, verranno utilizzati due router per configurare una rete AstroWarp: Brume 3 fungerà da router domestico, mentre un router da viaggio GL.iNet instraderà il traffico di rete a Brume 3 per l'accesso a Internet. Suggeriamo di configurare la rete AstroWarp prima della partenza.

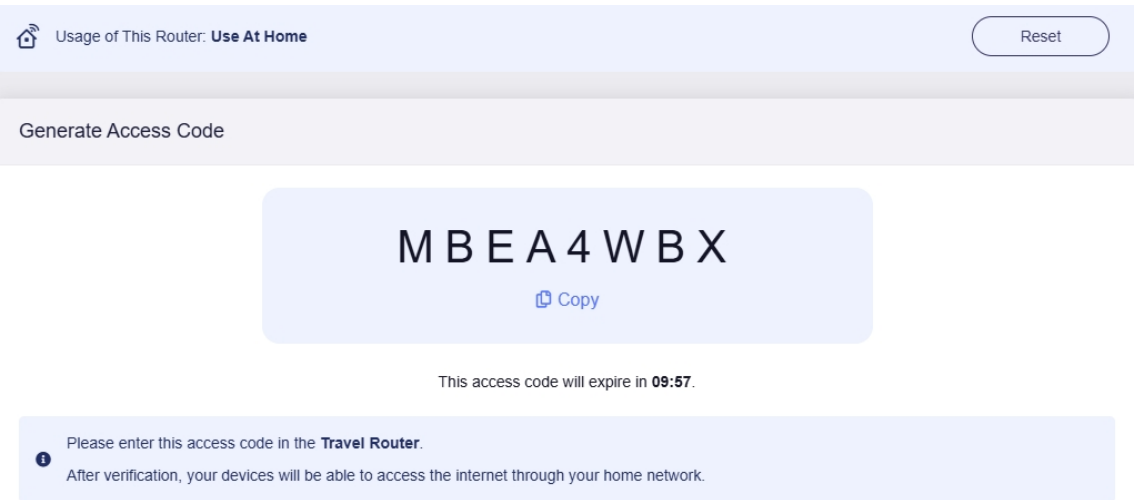
Suggerimento: ogni router GL.iNet viene fornito con **10 GB dati gratuiti al mese** per la rete AstroWarp. I dispositivi in una rete AstroWarp utilizzeranno i dati del router domestico per accedere a Internet. Se necessario, puoi eseguire l'aggiornamento al piano AstroWarp+ per dati illimitati.

1. Configura Brume 3 per Internet.
   Accedi al pannello di amministrazione web di Brume 3 e vai alla pagina INTERNET. Collegalo a Internet utilizzando uno dei metodi di connessione Internet supportati: Ethernet, tethering e cellulare.

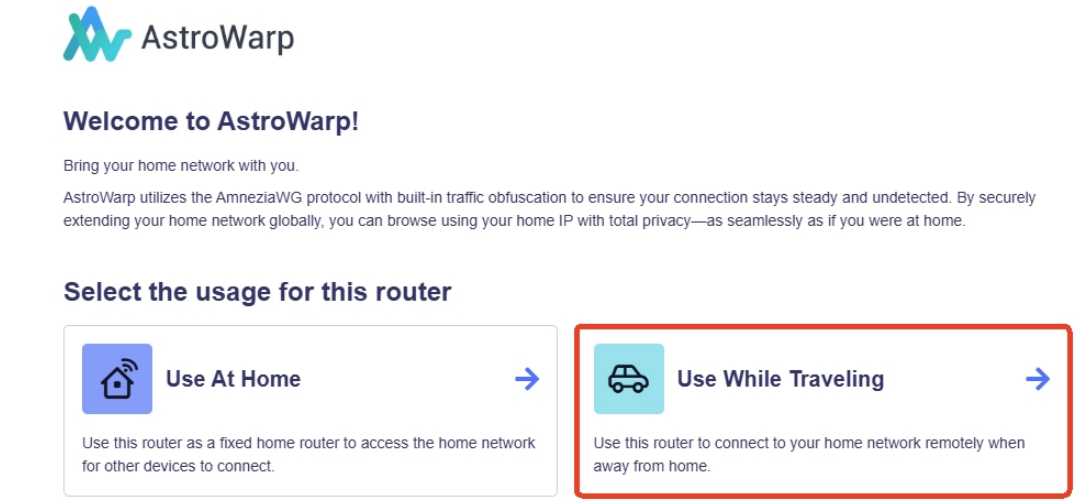
2. Nel pannello di amministrazione web di Brume 3, vai a **SERVIZI CLOUD** > **AstroWarp**. Fai clic su **Usa a casa**.



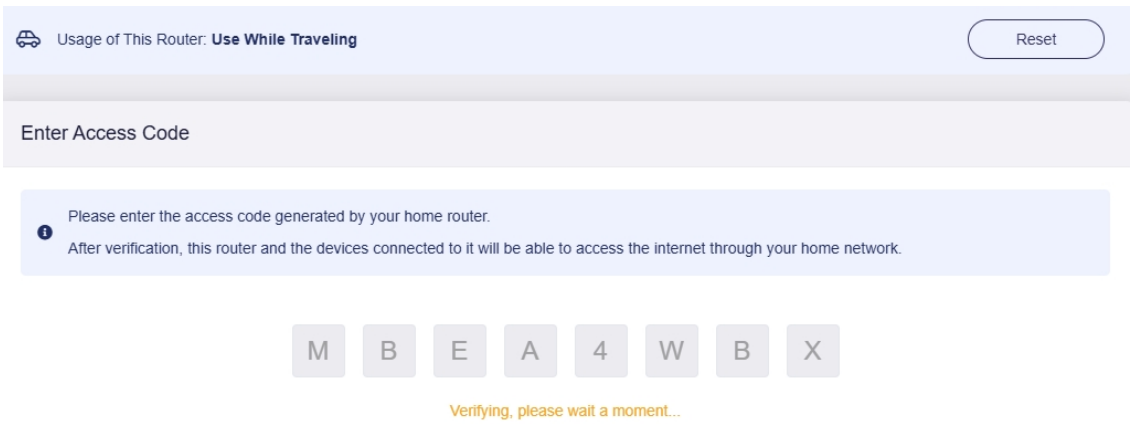
Genera un **codice di accesso**. Copia questo codice per un uso successivo.



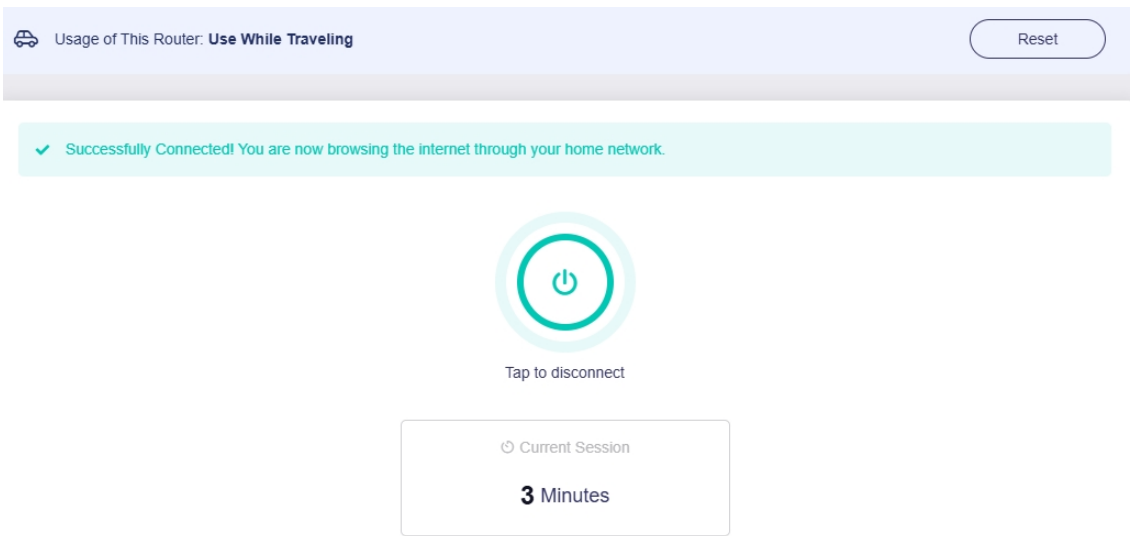
3. Configura il router da viaggio per Internet.
   Accedi al pannello di amministrazione web del router da viaggio e vai alla pagina INTERNET. Collegalo a Internet utilizzando uno dei metodi di connessione Internet supportati: Ethernet, Ripetitore, Tethering e Cellulare.
4. Inserisci il codice di accesso.
   Nel pannello di amministrazione web del router da viaggio, vai a **SERVIZI CLOUD** > **AstroWarp**. Fai clic su **Usa durante il viaggio**.



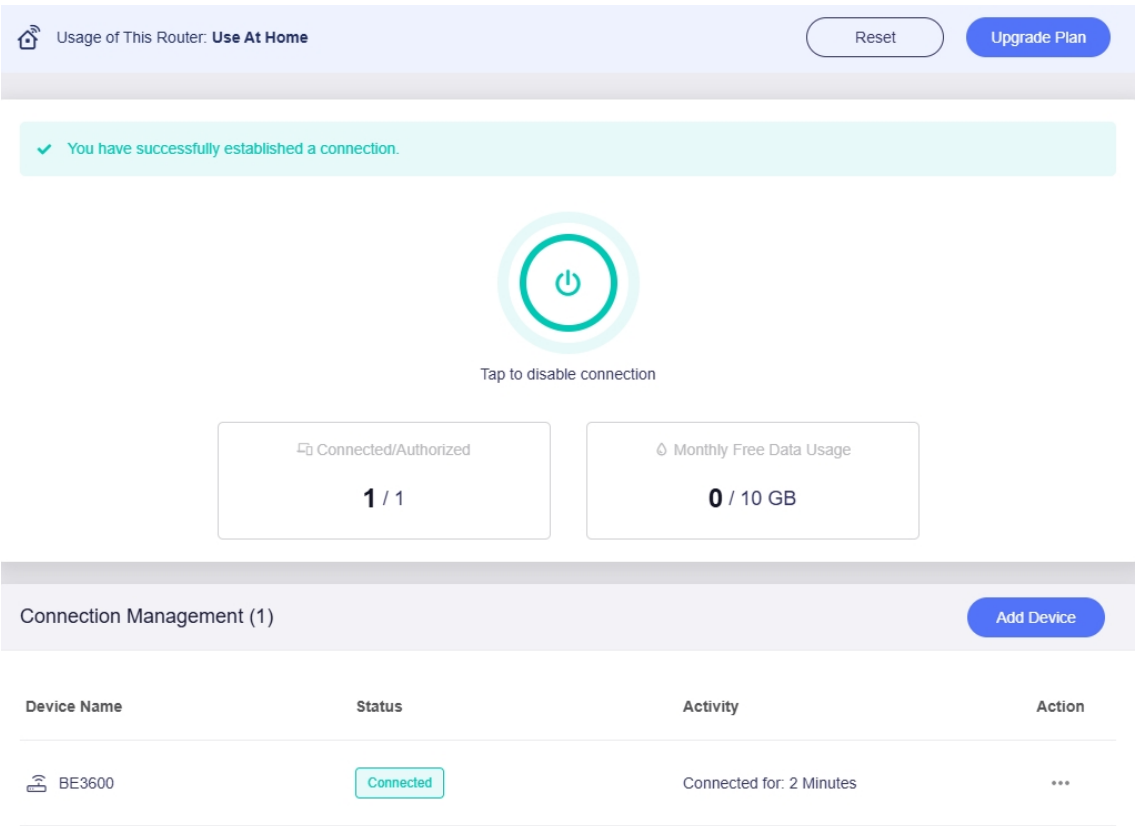
Inserisci il codice di accesso ottenuto nel passaggio 2 e attendi il completamento della verifica.



Si collegherà quindi correttamente a Brume 3. Ora puoi navigare in Internet attraverso la tua rete domestica in tutta sicurezza.



5. Nel pannello di amministrazione web di Brume 3, visualizza anche lo stato della connessione come segue.



6.2.2 Verifica della connettività

1. Collega un laptop o uno smartphone al Wi-Fi del router da viaggio.
2. Apri un browser e visita ipcheck.ing o qualsiasi altro sito Web di ricerca di indirizzi IP. Mostrerà l'indirizzo IP pubblico di Brume 3, indicando che il router da viaggio sta accedendo a Internet tramite Brume 3.

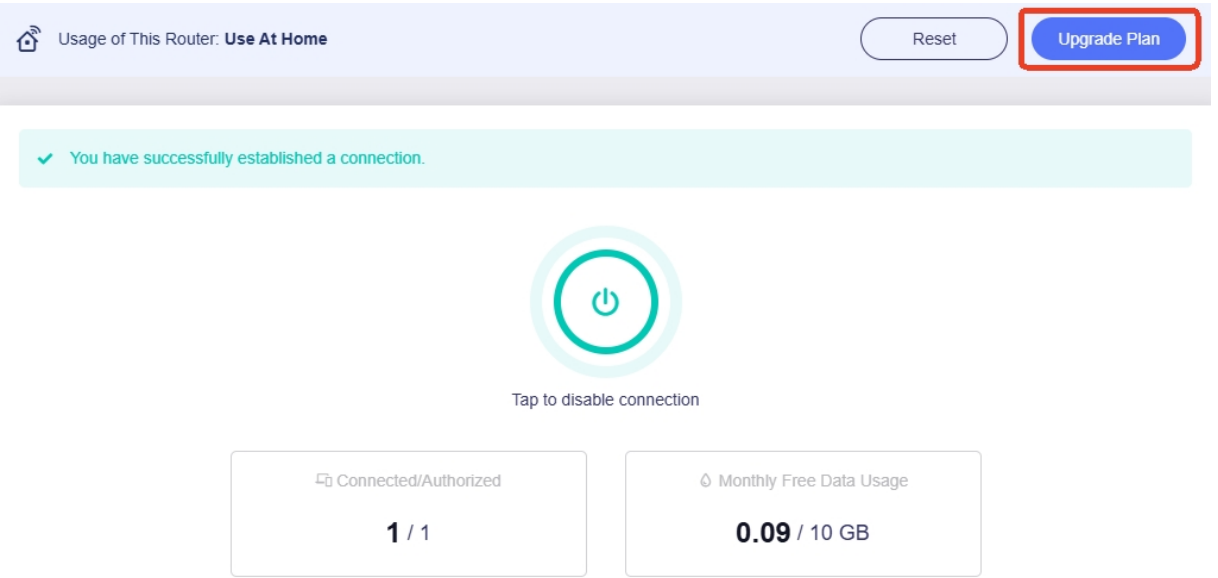


3. Disconnetti la connessione AstroWarp sul router da viaggio, quindi aggiorna la pagina web per inviare nuovamente la richiesta di query IP. Mostrerà l'indirizzo IP pubblico locale del router da viaggio, indicando che sta accedendo a Internet attraverso la sua rete locale.



6.2.3 Passaggio a un piano superiore

Ogni router GL.iNet viene fornito con **10 GB dati gratuiti al mese** per la rete AstroWarp. I dispositivi in una rete AstroWarp utilizzeranno i dati del router domestico per accedere a Internet. Se necessario, puoi eseguire l'aggiornamento al piano **AstroWarp+** per dati illimitati.



Fai clic qui per visualizzare ulteriori dettagli e domande frequenti su AstroWarp.

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

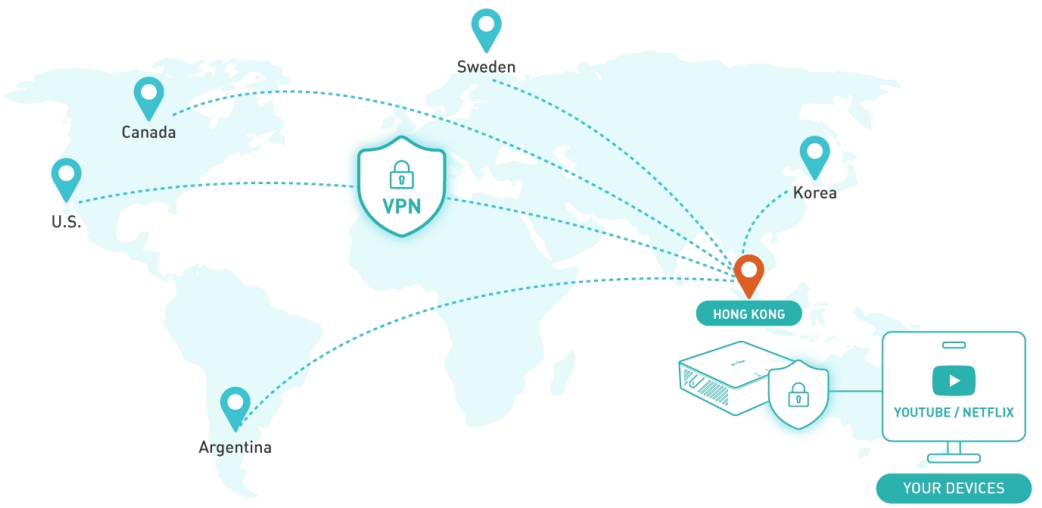
1. **Privacy dei dati personali**

   Il servizio VPN su questo router funziona con una gamma completa di dispositivi cablati, inclusi desktop, laptop, console di gioco, smart TV e dispositivi di streaming. Tutti i tuoi dati trasmessi tramite connessioni cablate sono protetti dalla VPN. Puoi anche personalizzare le policy VPN per abilitare una protezione flessibile per dispositivi specifici.



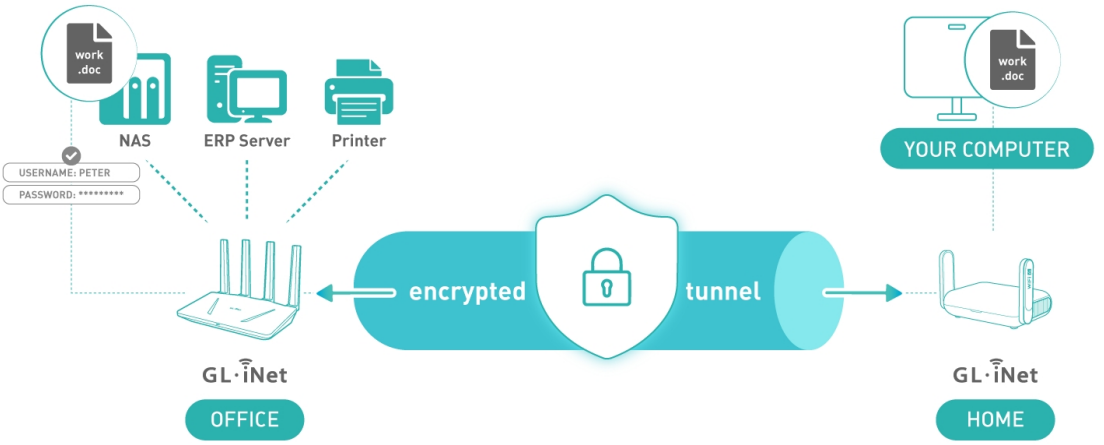
2. **Accesso illimitato in tutto il mondo**

   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.



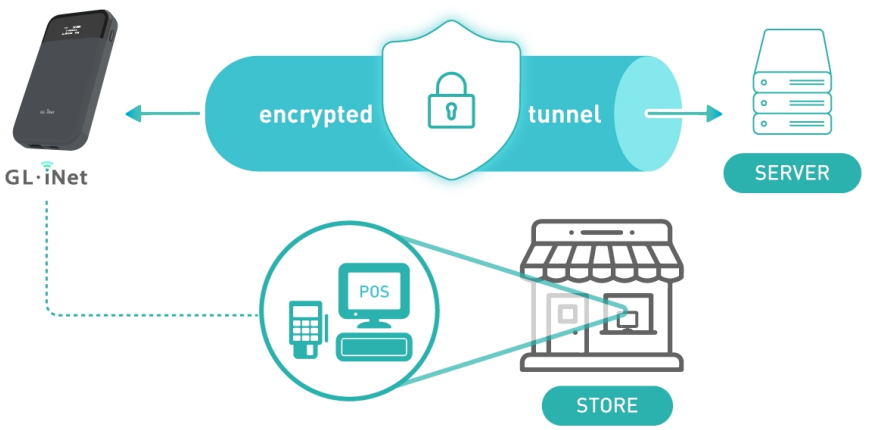
3. **Sicurezza dei dati delle piccole imprese**

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

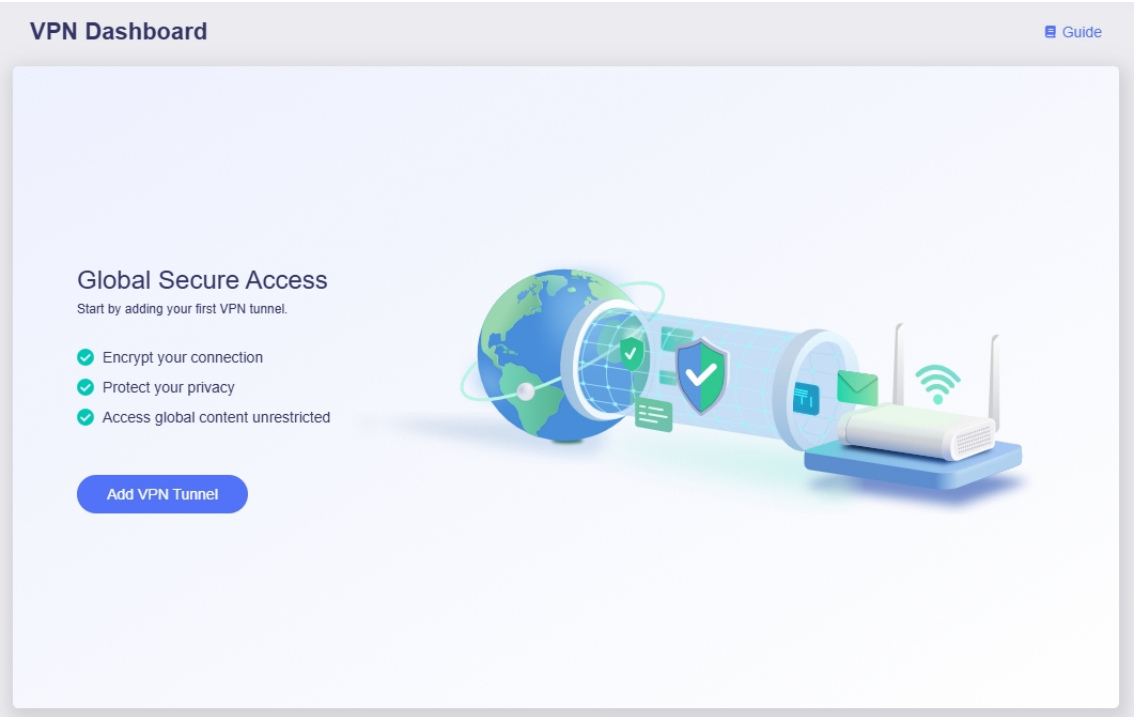
Questo capitolo introduce come gestire le connessioni VPN tramite pannello di amministrazione web.

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

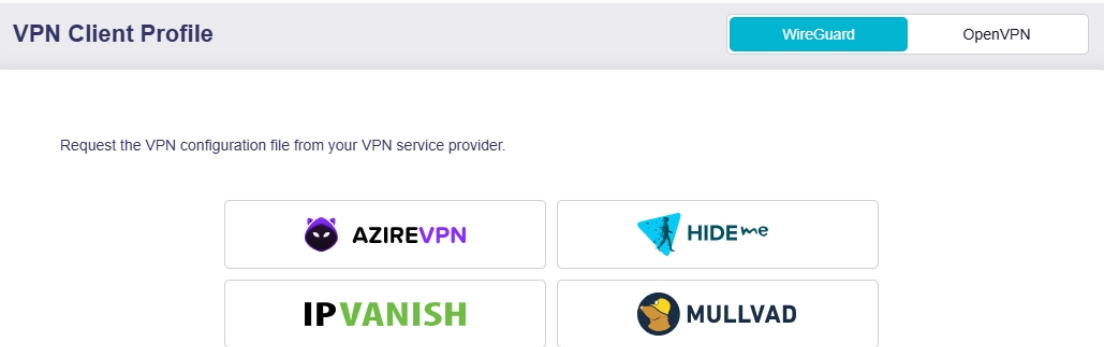
Il dashboard VPN mostra i dettagli della connessione VPN, come regole di routing, server connesso, statistiche sul traffico, IP virtuale del client e registro delle connessioni e consente agli utenti di configurare impostazioni avanzate come Kill Switch VPN, mascheramento IP e MTU.

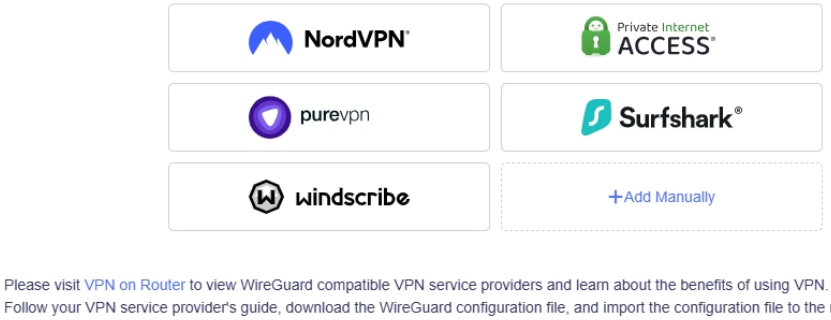
8.1 Caricamento di un profilo VPN

Quando si accede a questa pagina per la prima volta, se non sono stati creati tunnel, la pagina appare come segue. Fai clic su Aggiungi tunnel VPN per iniziare.



Verrai indirizzato alla pagina Profilo client VPN. Seleziona un provider VPN ed effettua l'accesso.

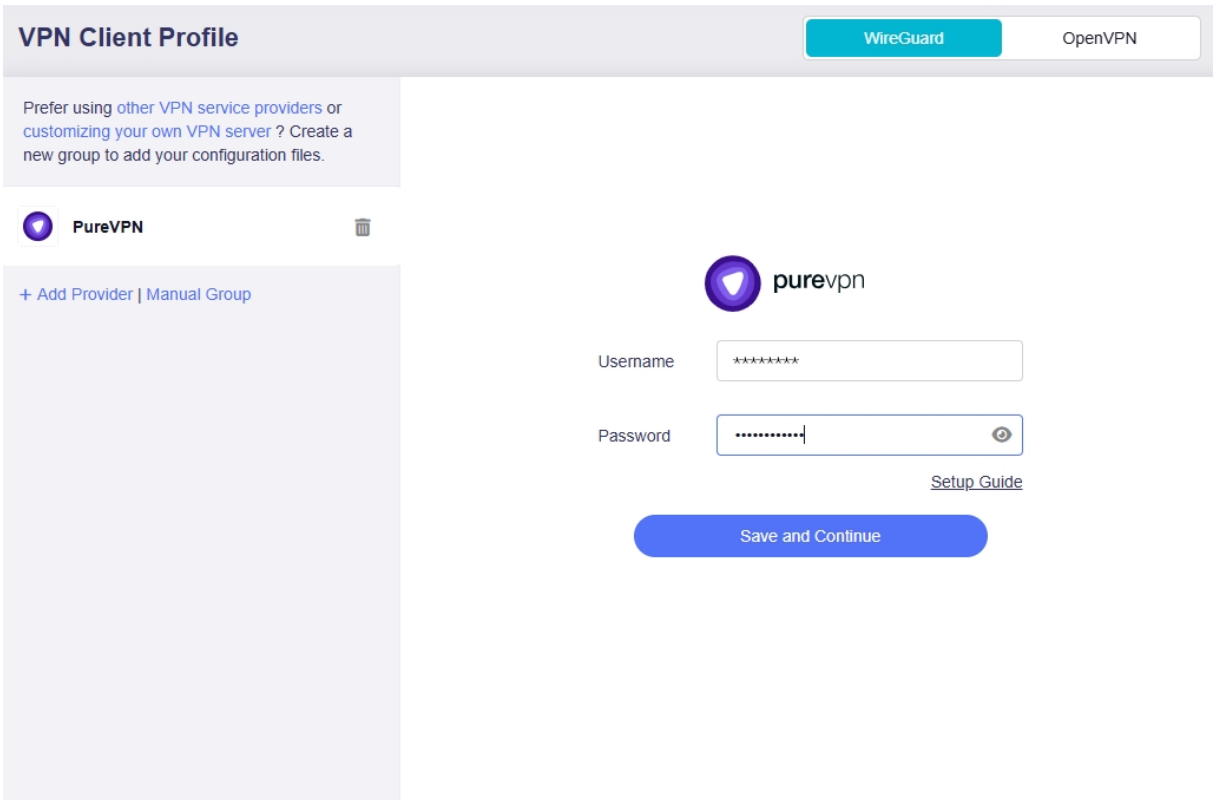




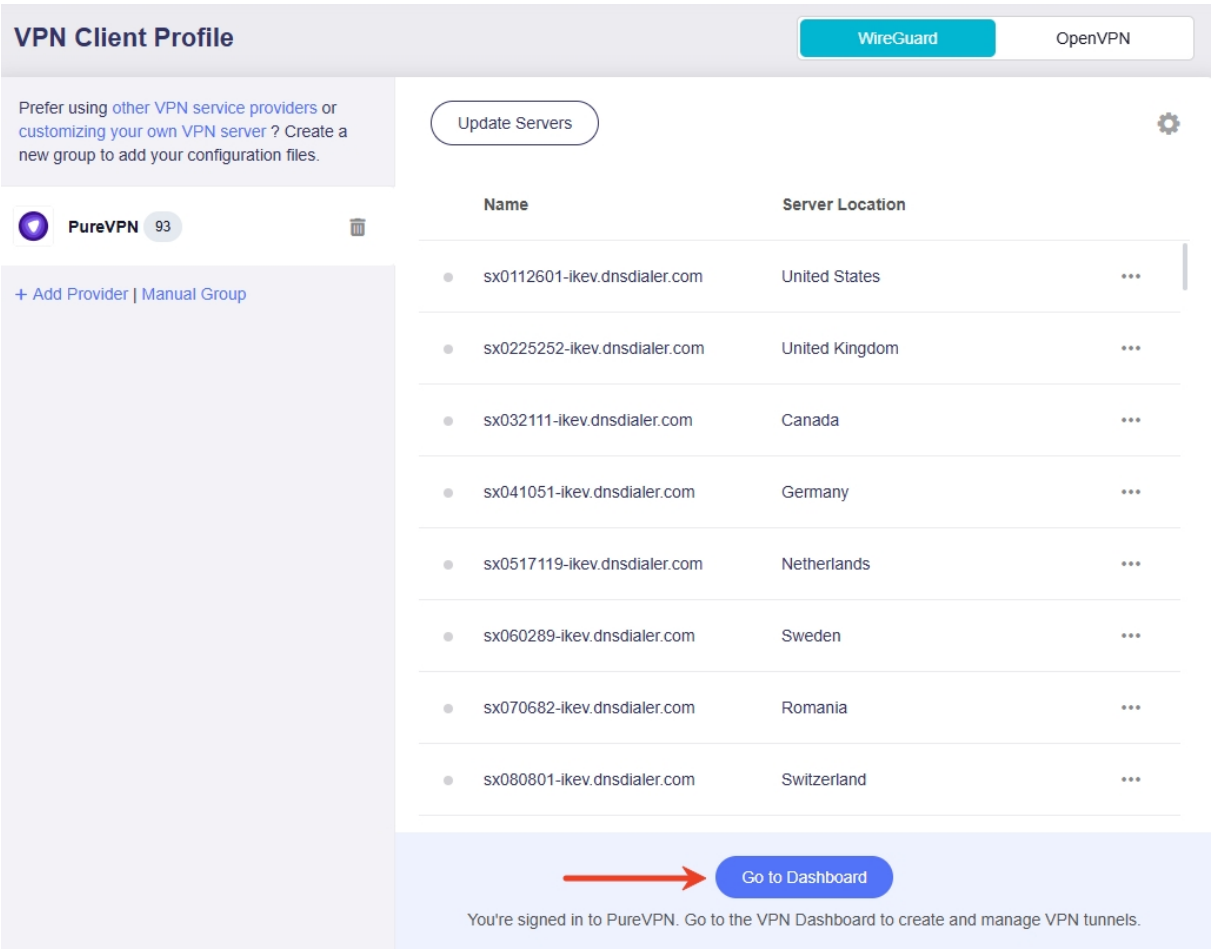
Suggerimenti:

1. I provider VPN elencati sono integrati nel pannello di amministrazione web del router GL.iNet. Con un abbonamento attivo, gli utenti inseriscono semplicemente le proprie credenziali per accedere istantaneamente e ottenere file di configurazione per le connessioni VPN.
2. Se sei abbonato ad altri provider VPN o se desideri caricare le tue configurazioni VPN personali, fai clic su Aggiungi manualmente e carica le tue configurazioni.

Prendiamo PureVPN come esempio. Fai clic su PureVPN e accedi con credenziali valide.



Otterrai un elenco di profili VPN, come mostrato di seguito. Fai clic su Vai alla dashboard in basso, quindi verrai indirizzato alla dashboard VPN per configurare il tunnel VPN e i criteri VPN.



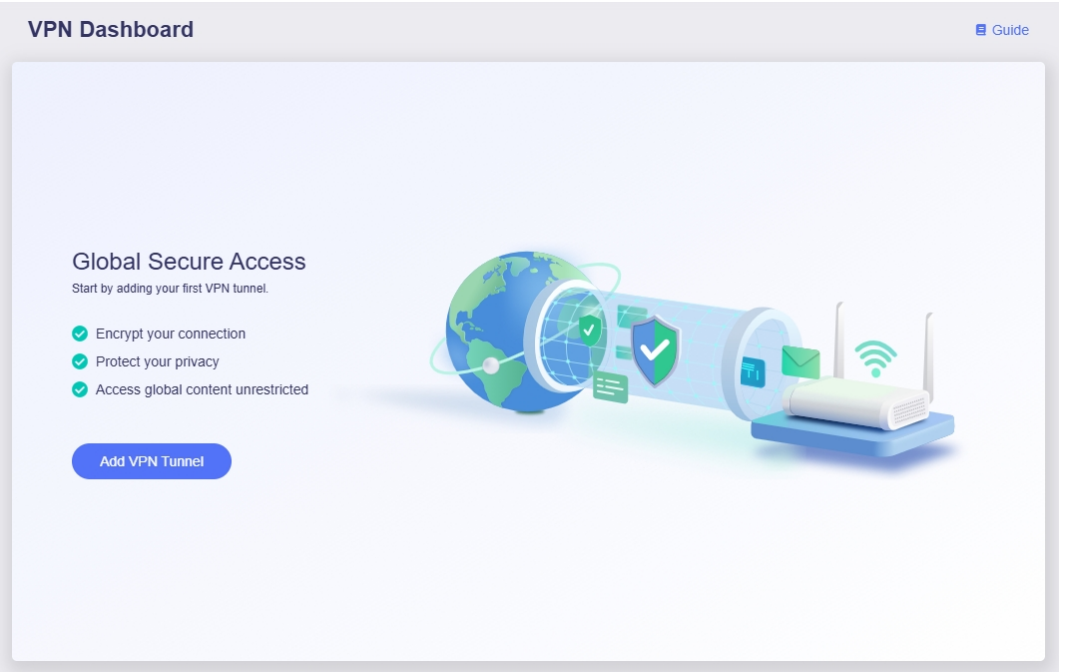
Suggerimento: per alcuni fornitori di servizi VPN, potrebbe essere necessario selezionare un protocollo VPN o server/città preferiti prima che venga visualizzato l'elenco dei profili.

8.2 Aggiunta di un tunnel VPN

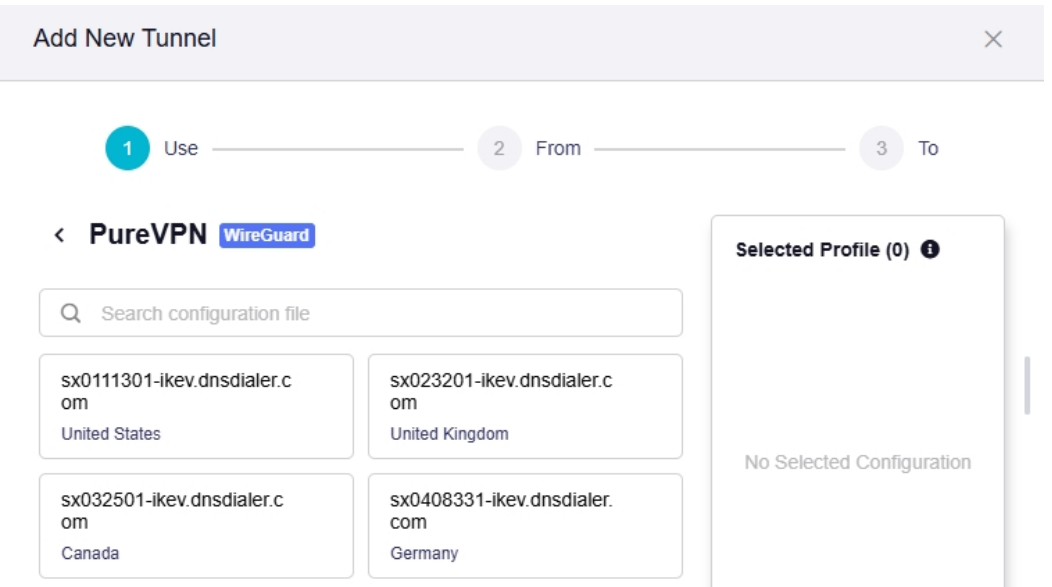
8.2.1 Procedura generale

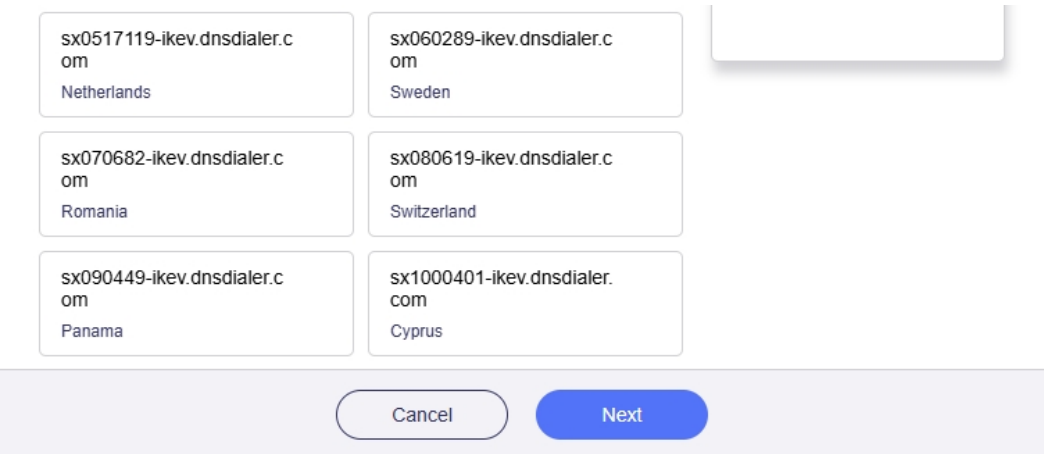
Segui i passaggi seguenti per aggiungere il tuo tunnel VPN e configurare i criteri VPN. Vedi Esempi di configurazione se necessario.

1. Nella dashboard VPN, fai clic su Aggiungi tunnel VPN. Sulla destra apparirà una procedura guidata di configurazione.



2. Seleziona uno o più profili e, se necessario, regola la loro priorità a destra, quindi fai clic su Avanti.





Nota: quando vengono selezionati più profili, il tunnel tenterà di connettersi utilizzando ciascun profilo in ordine di priorità finché non viene stabilita correttamente una connessione. Se tutti i profili all'interno di un singolo tunnel non riescono a connettersi, il sistema determinerà se passare alla rete locale (WAN) del router in base allo stato del Kill Switch nelle impostazioni Opzioni tunnel e Tutto il resto del traffico.

3. Seleziona l'origine client, quindi fai clic su Avanti. Sono disponibili quattro opzioni:
   - Tutti i client: se selezionato, il traffico proveniente da tutti i dispositivi corrisponderà a questa regola.
   - Tipi di connessione specificati: se selezionato, il traffico proveniente dai tipi di connessione specificati (ad esempio, sottorete LAN, gateway drop-in, rete ospiti) corrisponderà a questa regola.
   - Dispositivi specificati: se selezionato, il traffico proveniente dai dispositivi specificati (identificati dall'indirizzo MAC) corrisponderà a questa regola.
   - Escludi dispositivi specificati: se selezionato, il traffico proveniente da dispositivi specificati (identificati dall'indirizzo MAC) non corrisponderà a questa regola.
4. Seleziona la destinazione del traffico, quindi fai clic su Applica. Sono disponibili tre opzioni:
   - Tutti i target: se selezionato, il traffico corrispondente a questa regola verrà instradato a tutti i target.
   - Dominio specificato/Elenco IP: se selezionato, il traffico corrispondente a questa regola verrà instradato ai domini o agli indirizzi IP specificati. È necessario inserirli manualmente.
   - Escludi domini/elenco IP specificati: se selezionato, il traffico corrispondente a questa regola non verrà instradato ai domini o agli indirizzi IP specificati. È necessario inserirli manualmente.

5. Un tunnel VPN è stato aggiunto correttamente. Verrai indirizzato alla dashboard della VPN. Aggiungi altri tunnel VPN se necessario. Per motivi di sicurezza, vai su Tutto il resto del traffico e Opzioni tunnel per verificare lo stato del Kill Switch prima di abilitare il tunnel VPN.

8.2.2 Esempi di configurazione

Ecco due casi tipici di configurazione dei criteri VPN con istruzioni dettagliate come riferimento.

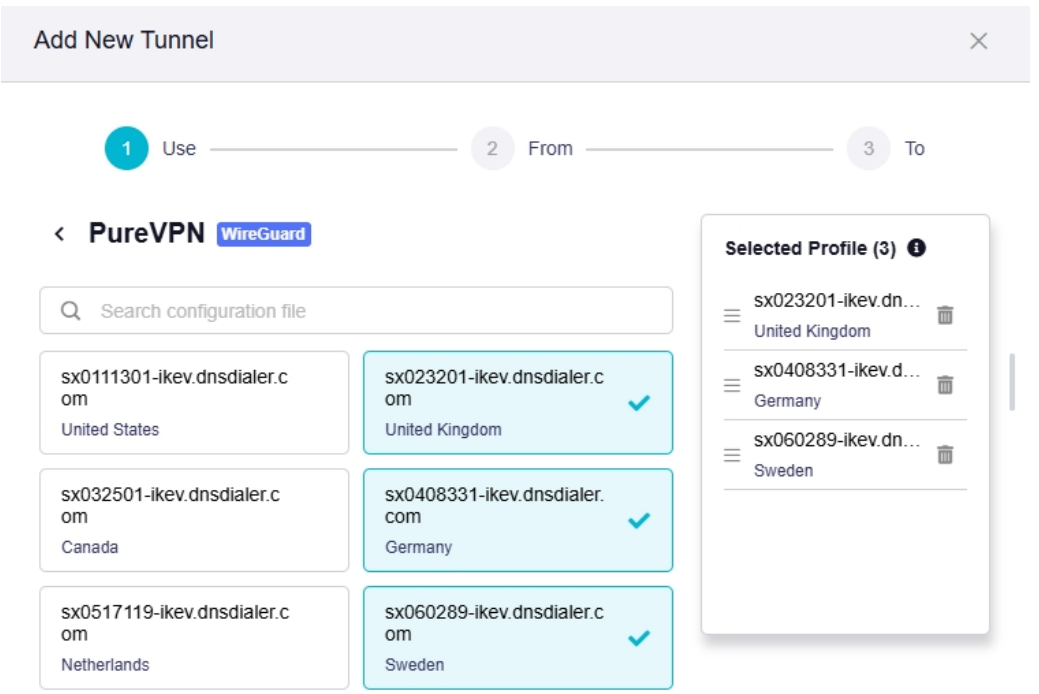
Caso 1: instrada solo i dispositivi specificati tramite VPN

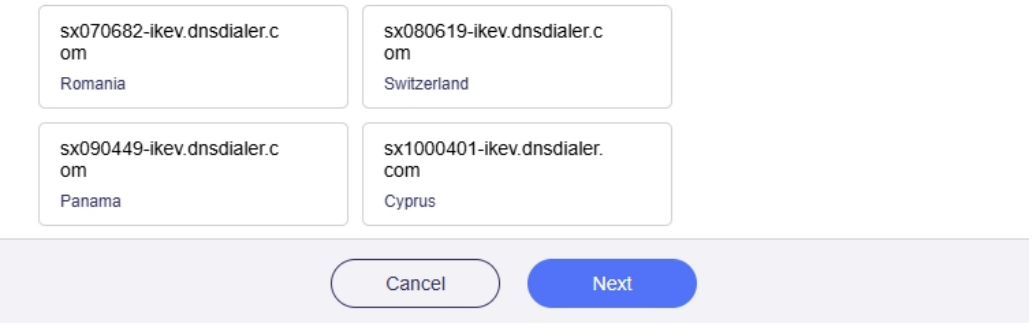
Requisiti:

1. Solo dispositivi specifici collegati a questo router accedono a Internet tramite la VPN. Tutti gli altri dispositivi accedono a Internet tramite la WAN locale.
2. I dispositivi selezionati devono utilizzare solo la connessione VPN. Se la VPN si disconnette inaspettatamente, l'accesso a Internet per questi dispositivi verrà bloccato per prevenire perdite DNS e tracciamento IP.

Passaggi di configurazione:

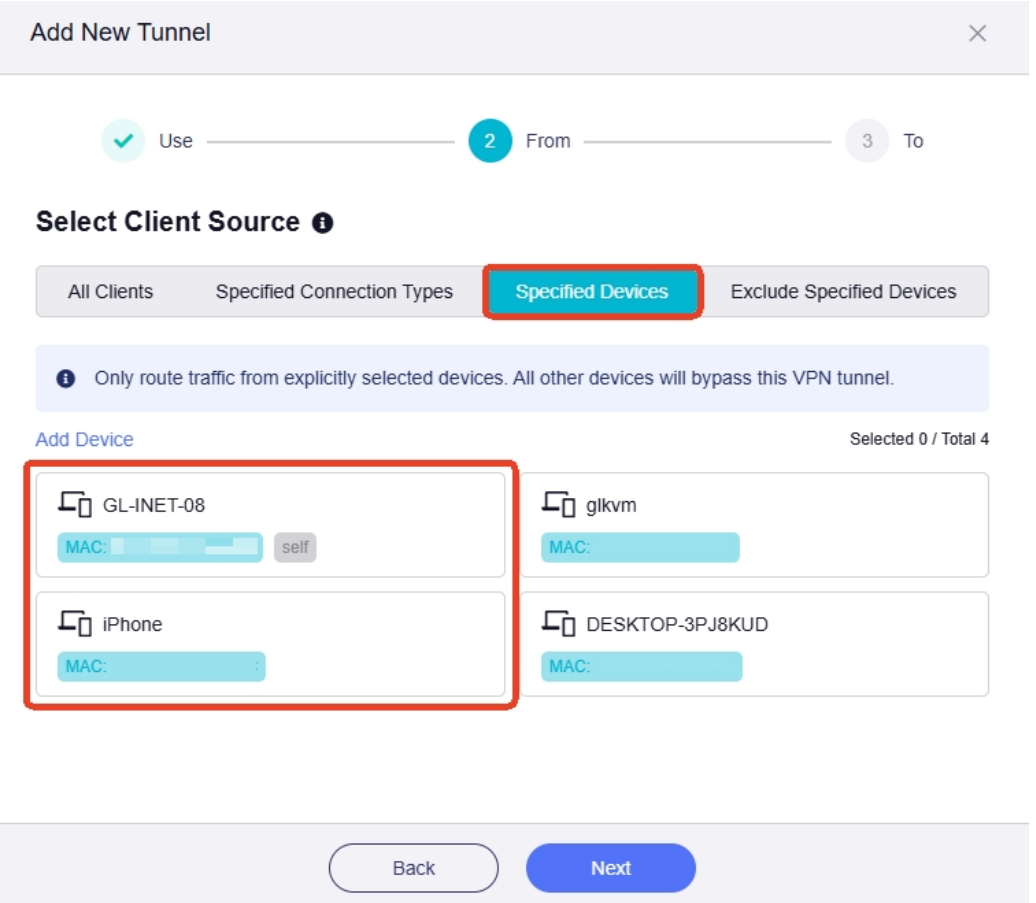
1. Seleziona il profilo VPN.
   Se hai effettuato l'accesso con le credenziali del servizio VPN integrato o hai caricato un file di configurazione, i profili disponibili verranno elencati qui. Altrimenti, vai su **Profilo client VPN** per accedere con le tue credenziali o carica manualmente un file di configurazione.
   Prendiamo PureVPN come esempio. Seleziona uno o più profili e, se necessario, regola la loro priorità sulla destra.





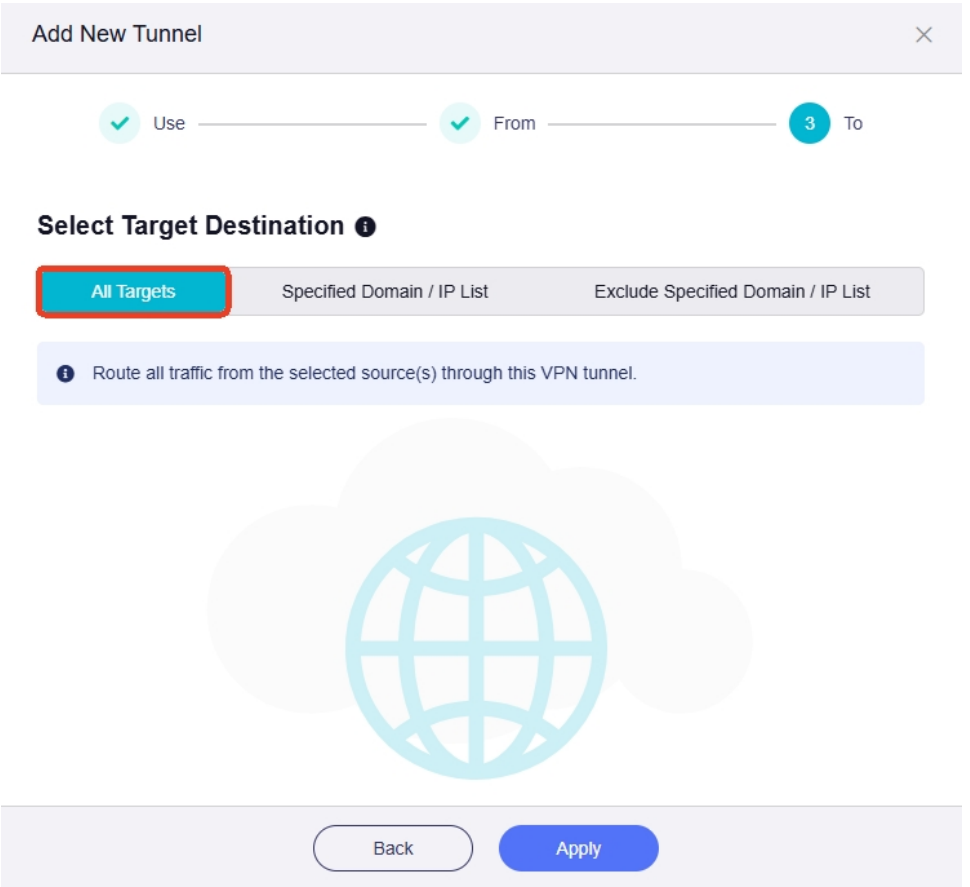
2. Seleziona l'origine del client.

   Fai clic sulla scheda **Dispositivi specificati**, seleziona i dispositivi che utilizzeranno la VPN, quindi fai clic su **Avanti**.

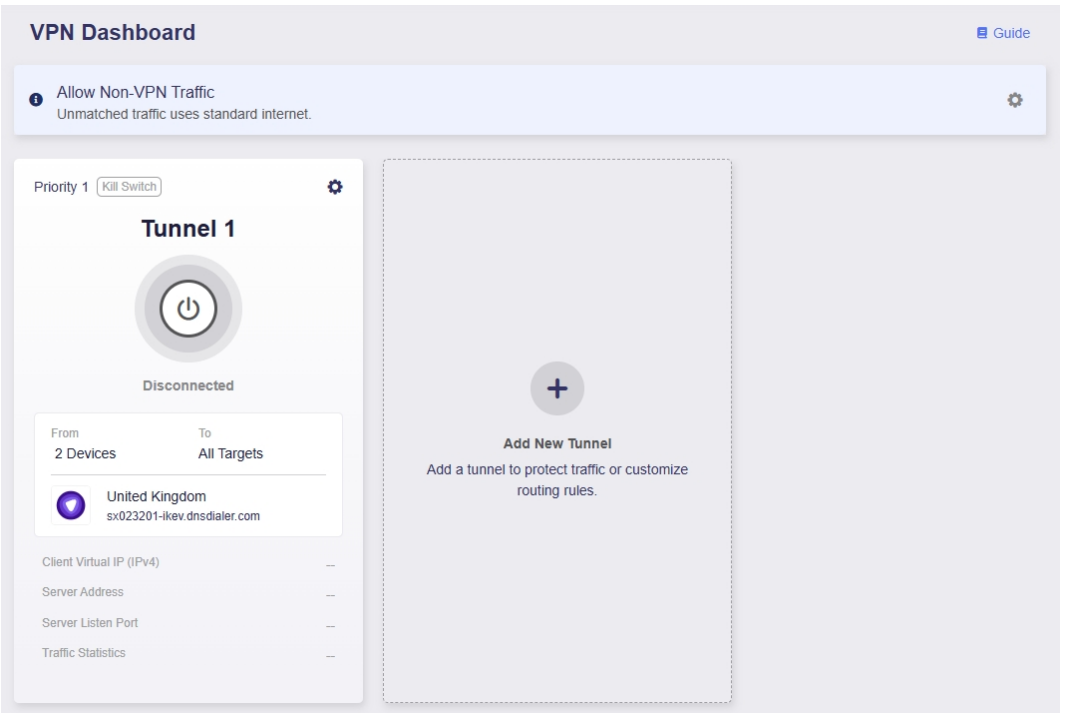


3. Seleziona la destinazione del traffico.

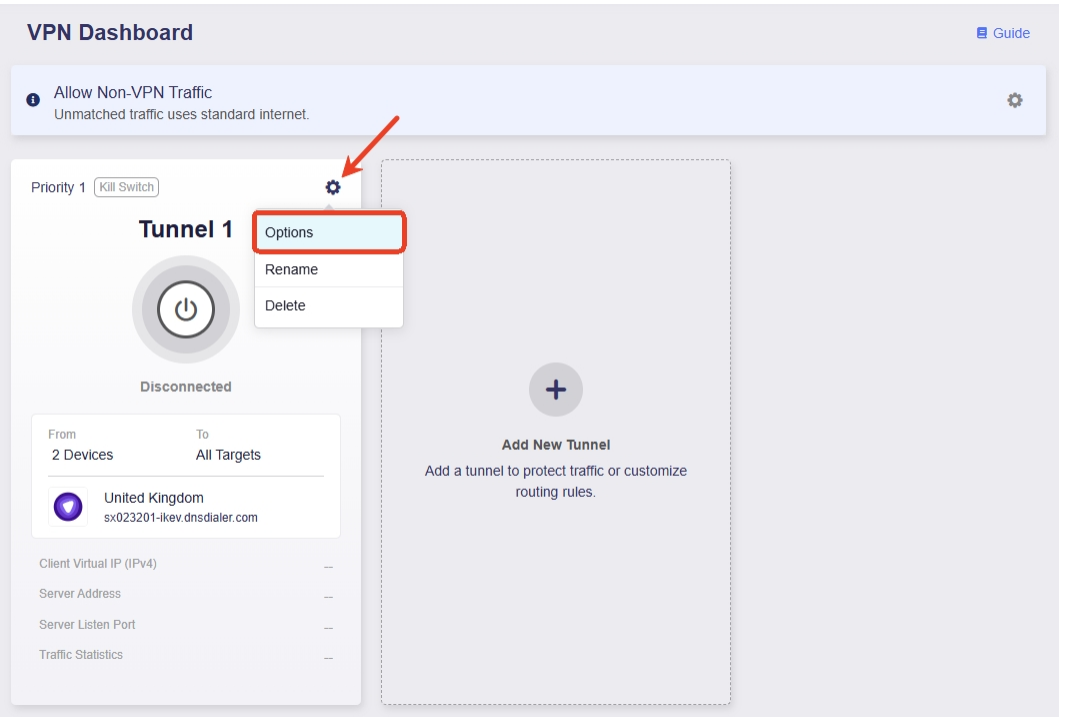
   Fai clic sulla scheda **Tutti i target**, impostala come destinazione del traffico, quindi fai clic su **Applica**.

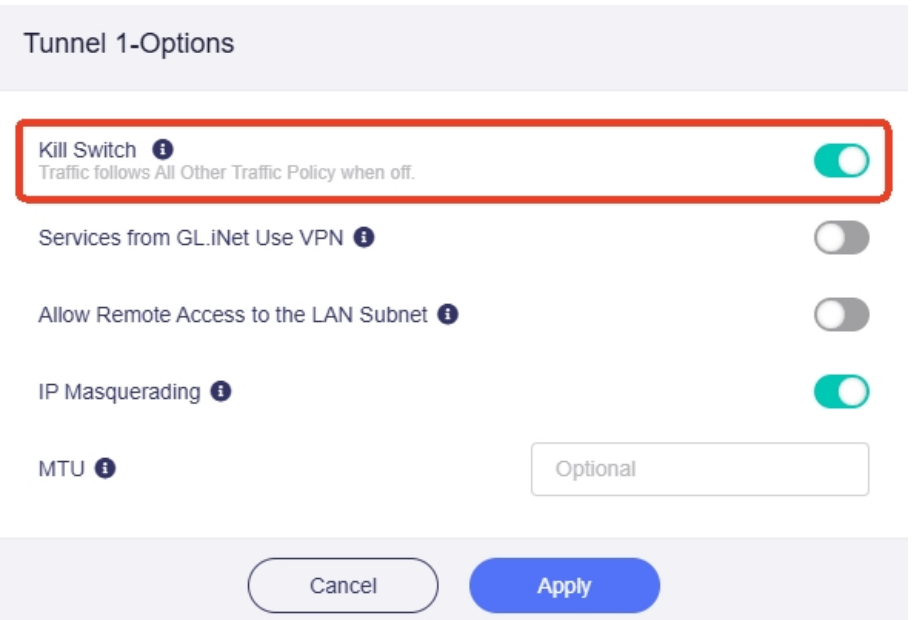


4. Verrai indirizzato alla dashboard VPN. Ora un tunnel VPN è stato aggiunto correttamente, come mostrato di seguito.

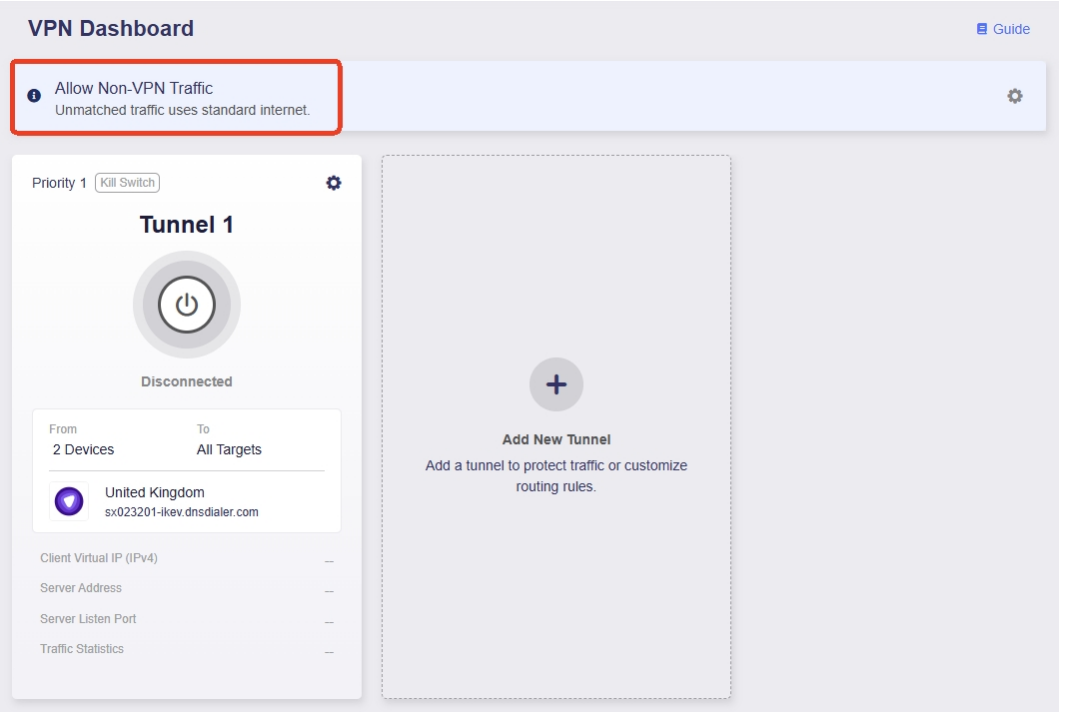


5. Assicurati che il **Kill Switch** per questo tunnel sia abilitato. Se la VPN si disconnette inaspettatamente, l'accesso a Internet per il traffico corrispondente a questo tunnel verrà bloccato per impedire perdite DNS e tracciamento IP.

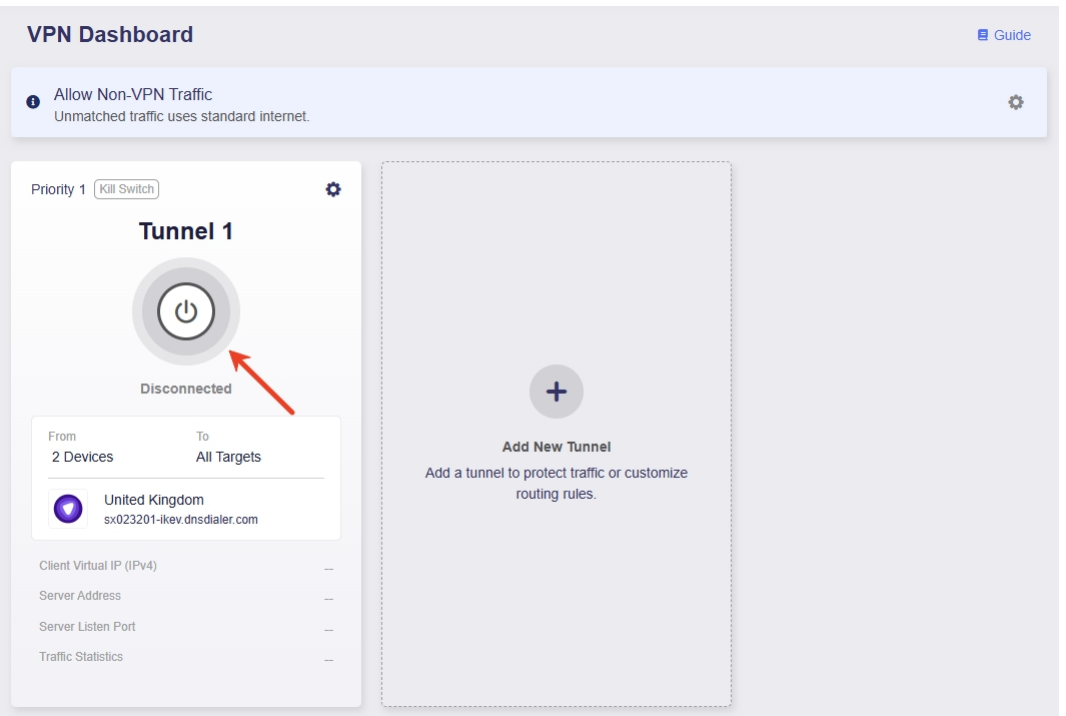




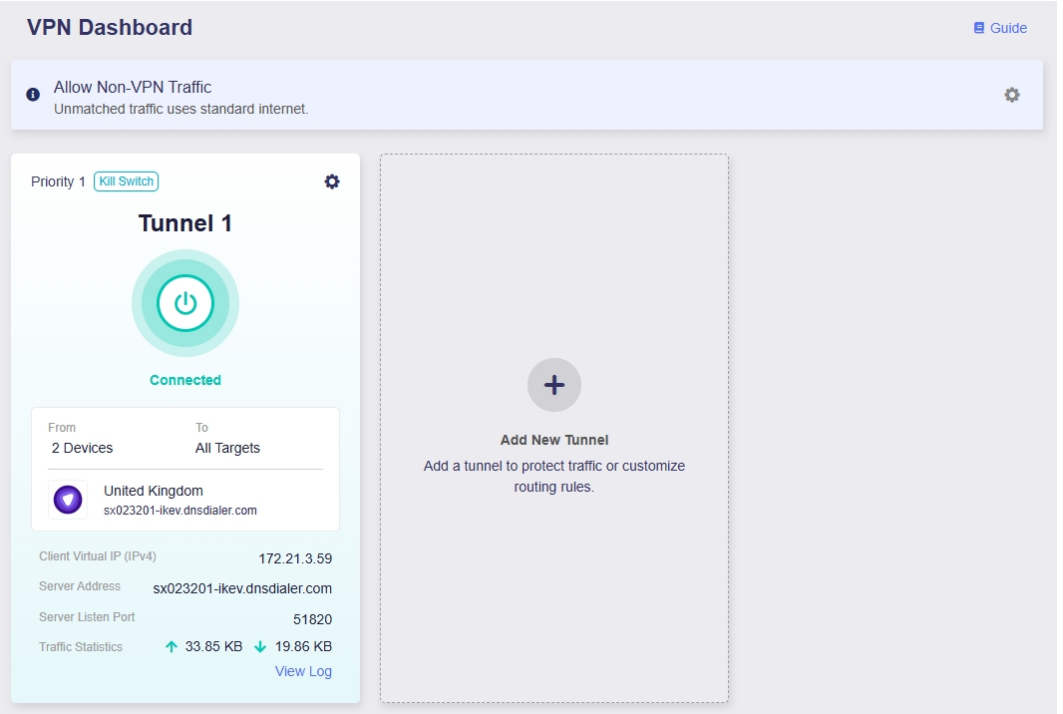
6. Assicurati che **Consenti traffico non VPN** sia abilitato. Questa opzione è abilitata per impostazione predefinita per garantire che il traffico che non corrisponde al tunnel VPN possa comunque accedere a Internet tramite la WAN locale.



7. Fai clic sul pulsante centrale per attivare questo tunnel.



8. Una volta connesso, la pagina visualizzerà i dettagli della connessione VPN, inclusi criteri VPN, statistiche sul traffico, indirizzo del server, porta di ascolto e indirizzo IP virtuale.



Ora solo due dispositivi specificati accedono a Internet tramite VPN. Se la VPN si disconnette inaspettatamente, l'accesso a Internet per questi dispositivi verrà bloccato per prevenire perdite DNS e tracciamento IP. Tutti gli altri dispositivi accederanno invece a Internet tramite la WAN locale.

Caso 2: instrada tutti i dispositivi sulla VPN 1 per siti Web specifici e instrada tutto il traffico rimanente sulla VPN 2.

Requisiti:

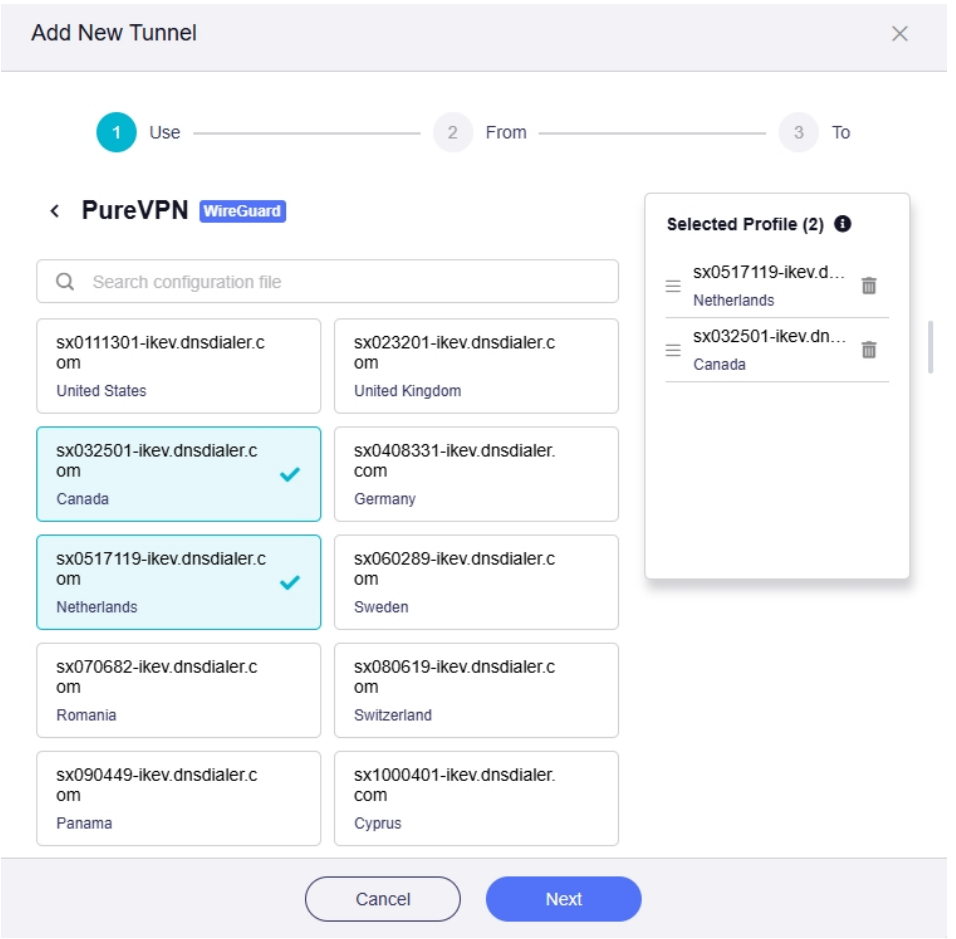
1. Tutti i dispositivi utilizzano il Tunnel VPN 1 quando accedono a domini di social media e servizi di streaming specifici e utilizzano il Tunnel VPN 2 per tutti gli altri accessi a Internet.
2. Se i tunnel VPN si disconnettono inaspettatamente, l'accesso a Internet per tutti i dispositivi verrà bloccato per prevenire perdite DNS e tracciamento IP.

Passaggi di configurazione:

1. Seleziona il profilo VPN per Tunnel 1.
   Se hai effettuato l'accesso con le credenziali del servizio VPN integrato o hai caricato un file di configurazione, i profili disponibili verranno elencati qui. Altrimenti, vai su **Profilo**

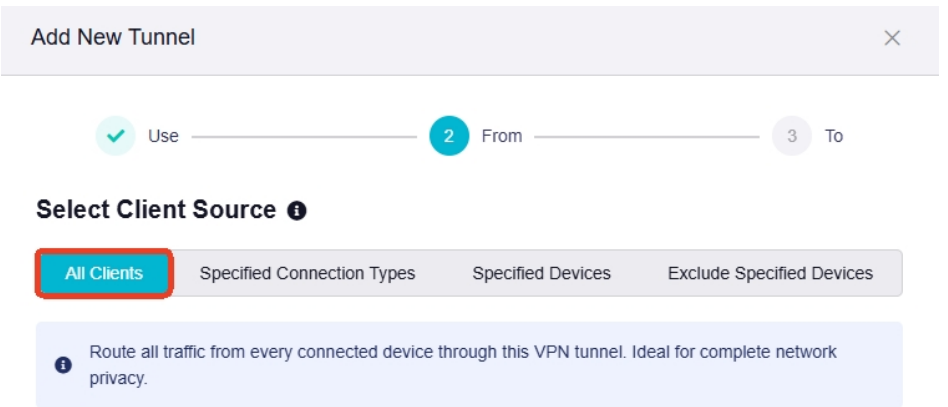
client VPN per accedere con le tue credenziali o carica manualmente un file di configurazione.

Prendiamo PureVPN come esempio. Seleziona uno o più profili e, se necessario, regola la loro priorità a destra, quindi fai clic su **Avanti**.

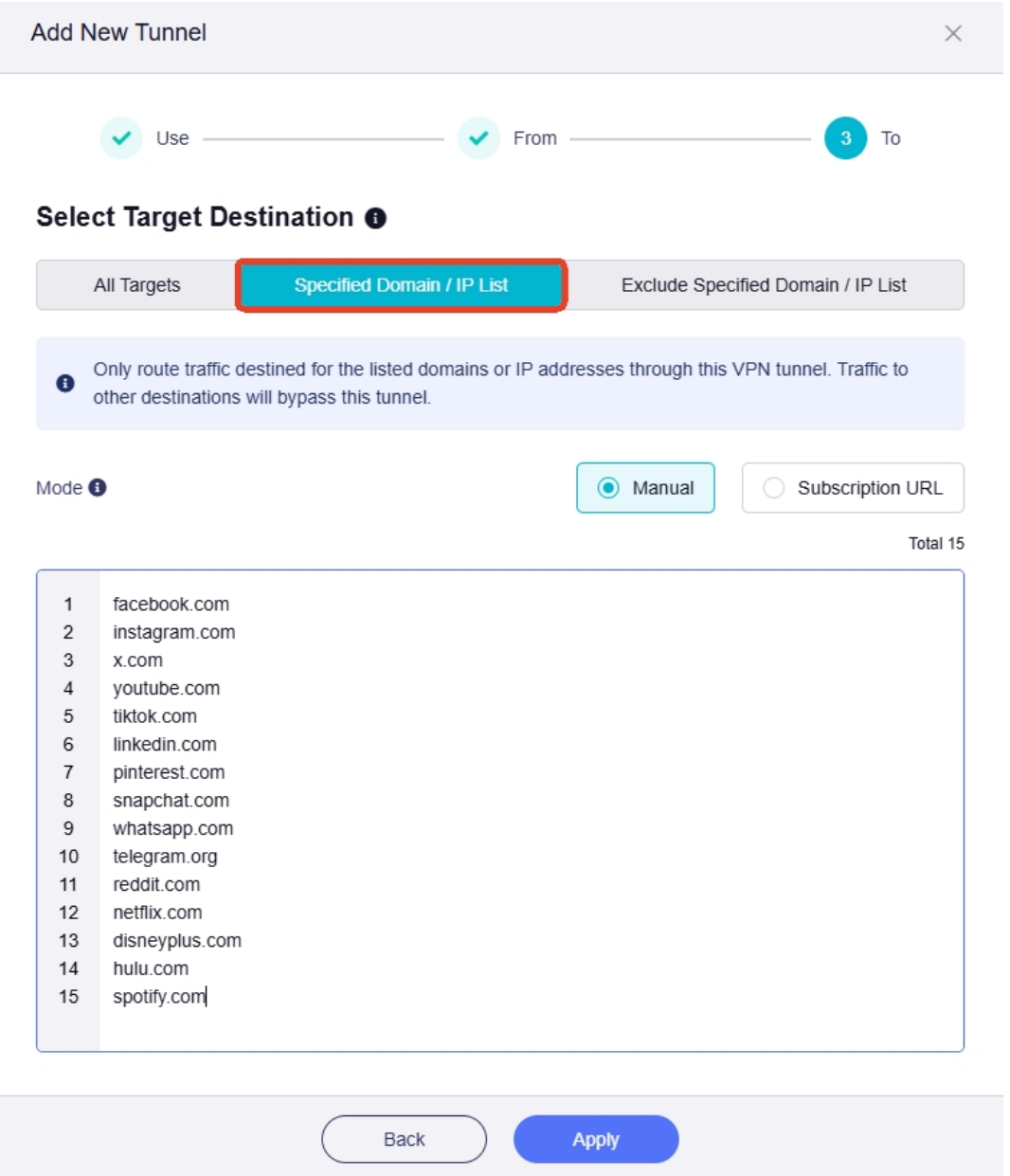


2. Seleziona l'origine del client.

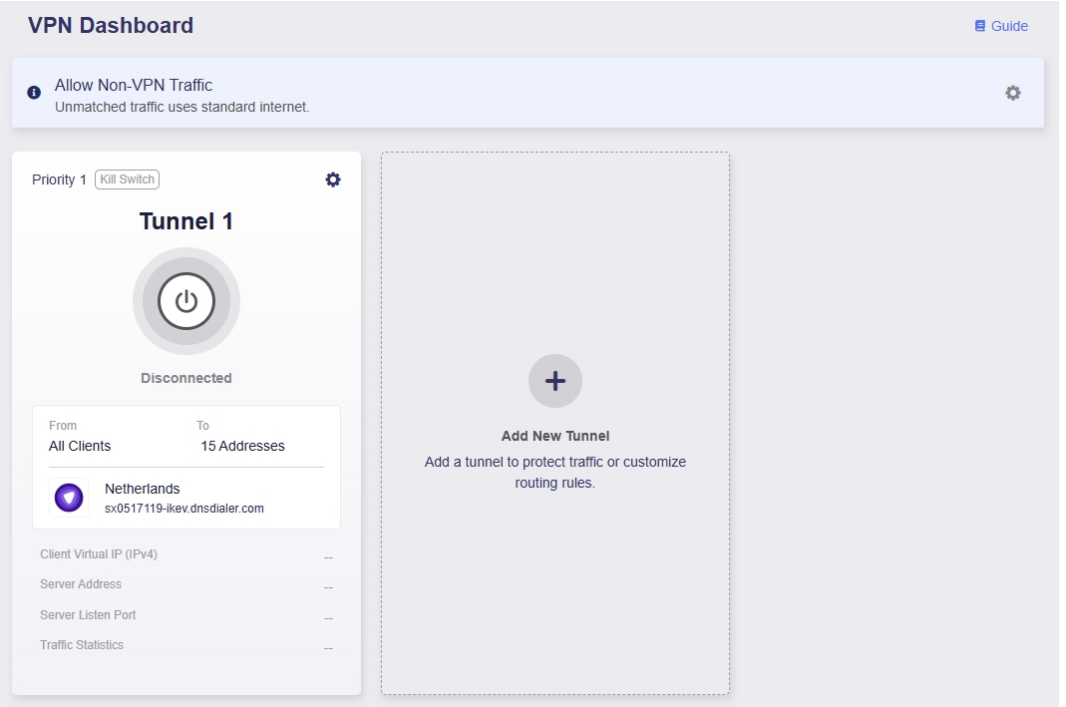
   Fai clic sulla scheda **Tutti i client**, impostala come origine client per il Tunnel 1, quindi fai clic su **Avanti**.



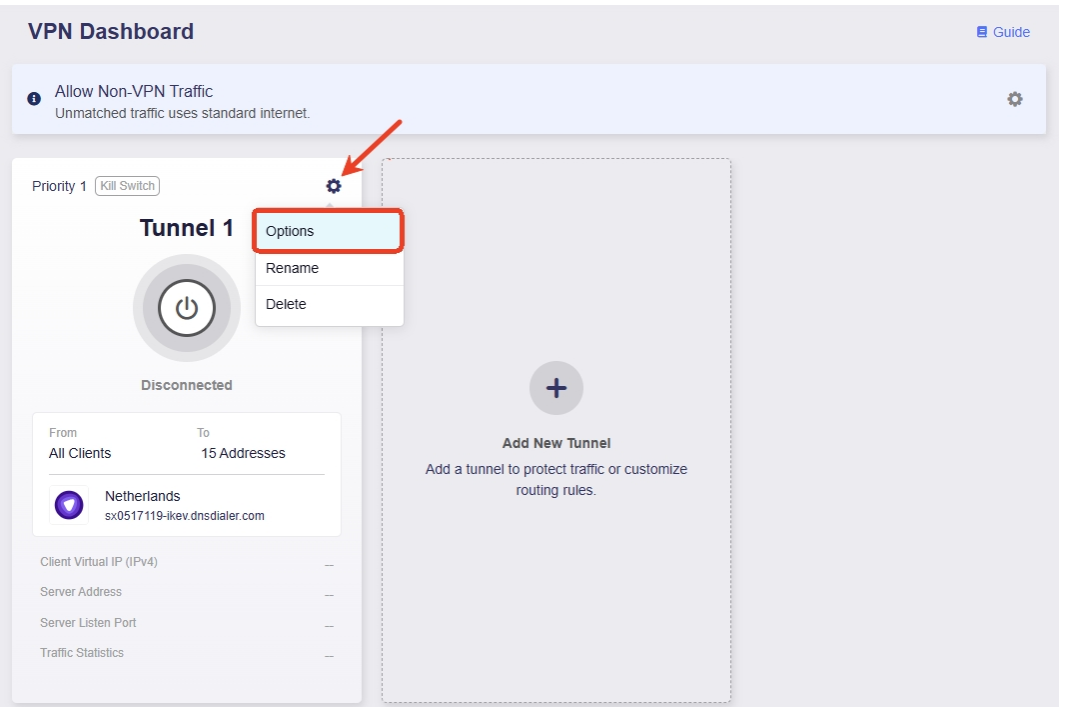
3. Seleziona la destinazione del traffico.
   Fai clic sulla scheda **Dominio specificato/Elenco IP**, inserisci i domini di alcuni social media e servizi di streaming comuni, come mostrato di seguito, quindi fai clic su **Applica**.

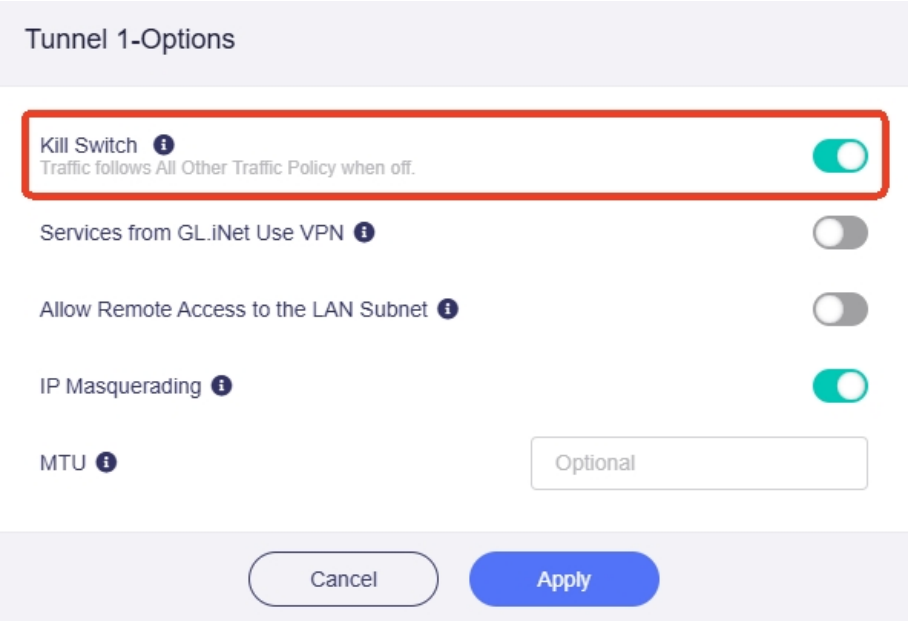


4. Verrai indirizzato alla dashboard della VPN. Ora il tunnel VPN 1 è stato aggiunto con successo.

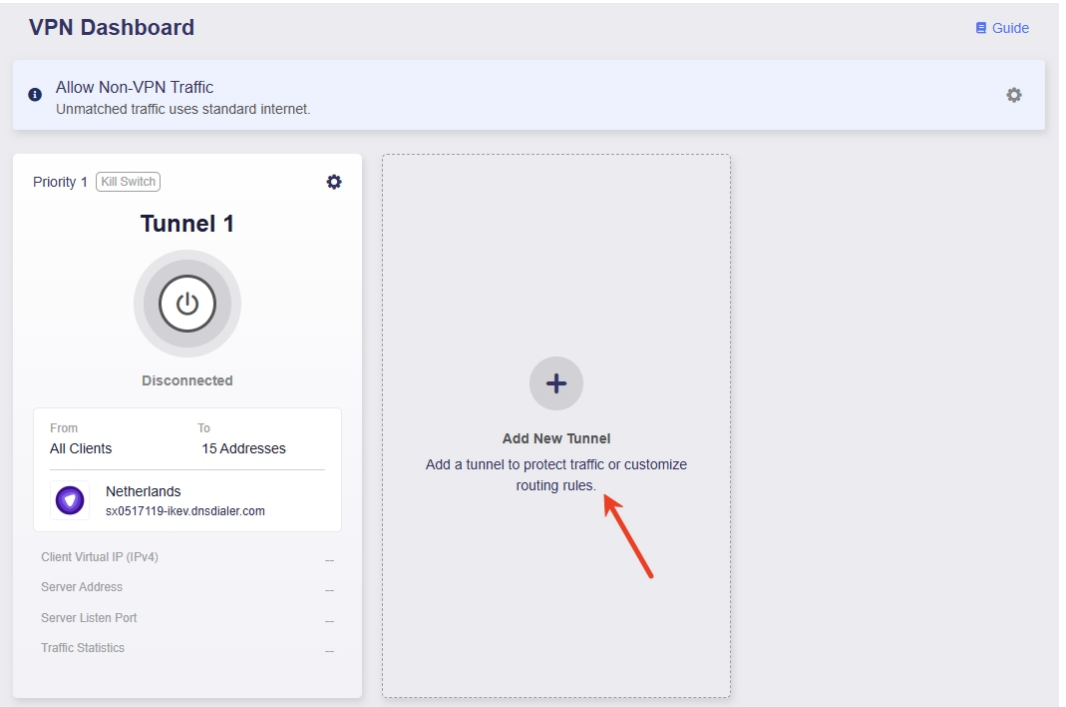


5. Assicurati che il **Kill Switch** per il Tunnel 1 sia abilitato. Se la VPN si disconnette inaspettatamente, l'accesso a Internet per il traffico corrispondente a questo tunnel verrà bloccato per impedire perdite DNS e tracciamento IP.



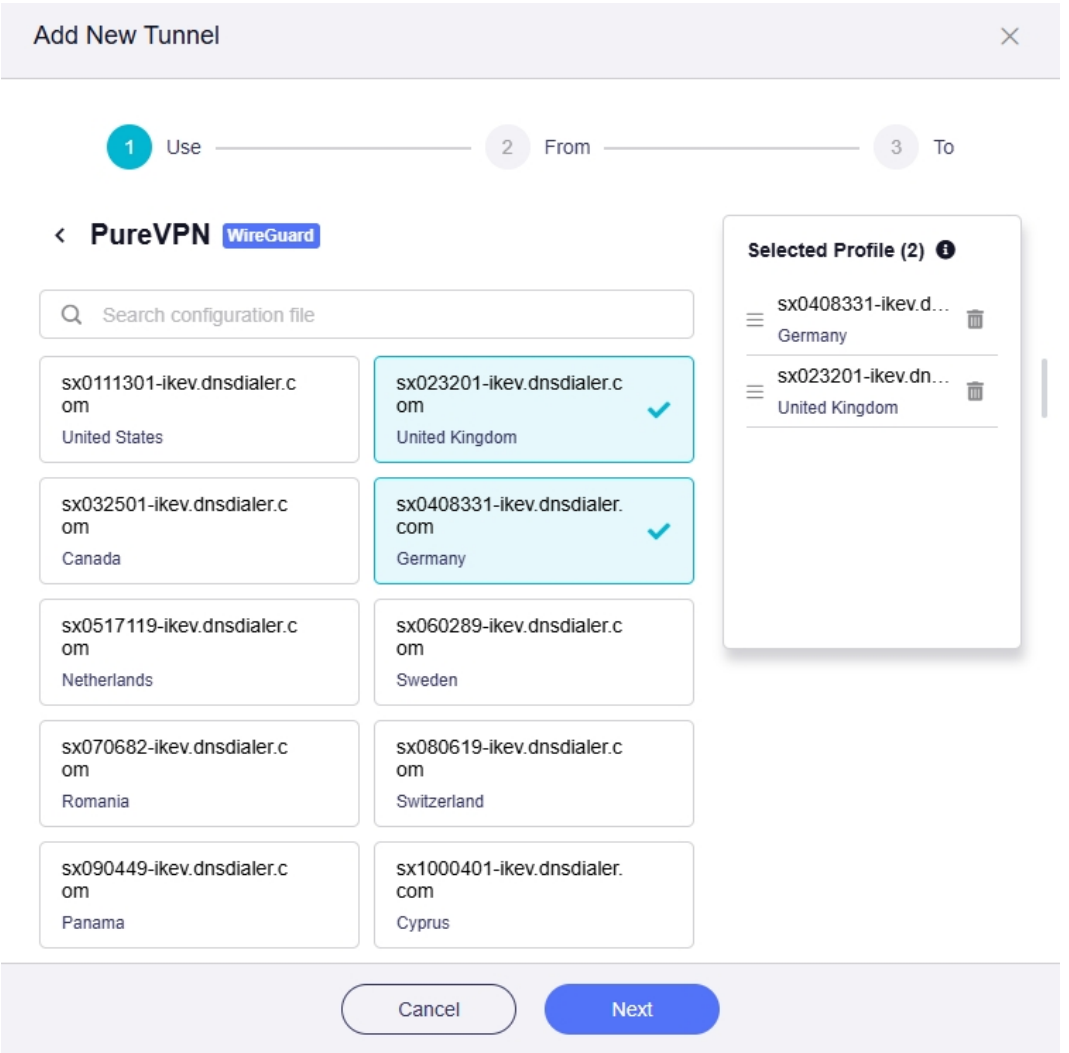


6. Fai clic su **Aggiungi nuovo tunnel** per aggiungere il tunnel 2.



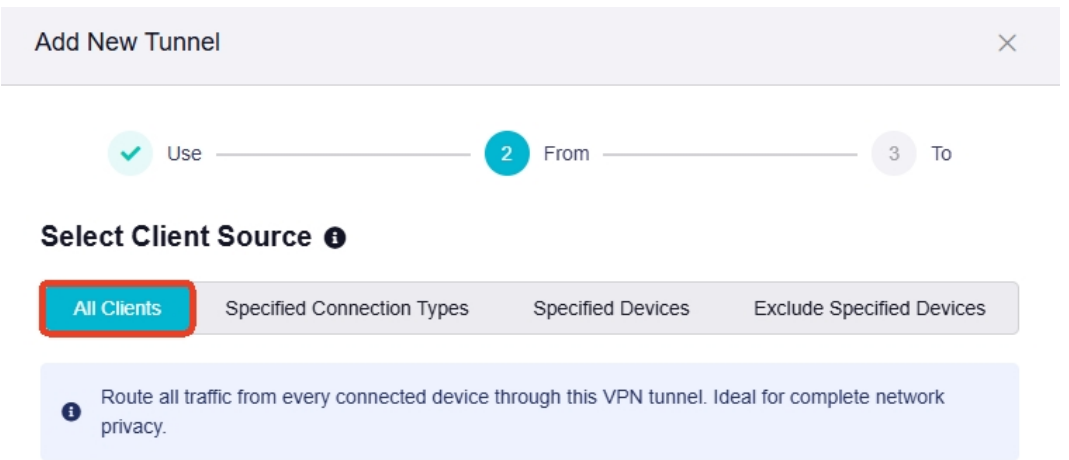
7. Seleziona il profilo VPN per Tunnel 2.

   Seleziona uno o più profili e, se necessario, regola la loro priorità sulla destra. Quindi fai clic su **Avanti**.



8. Seleziona l'origine del client.

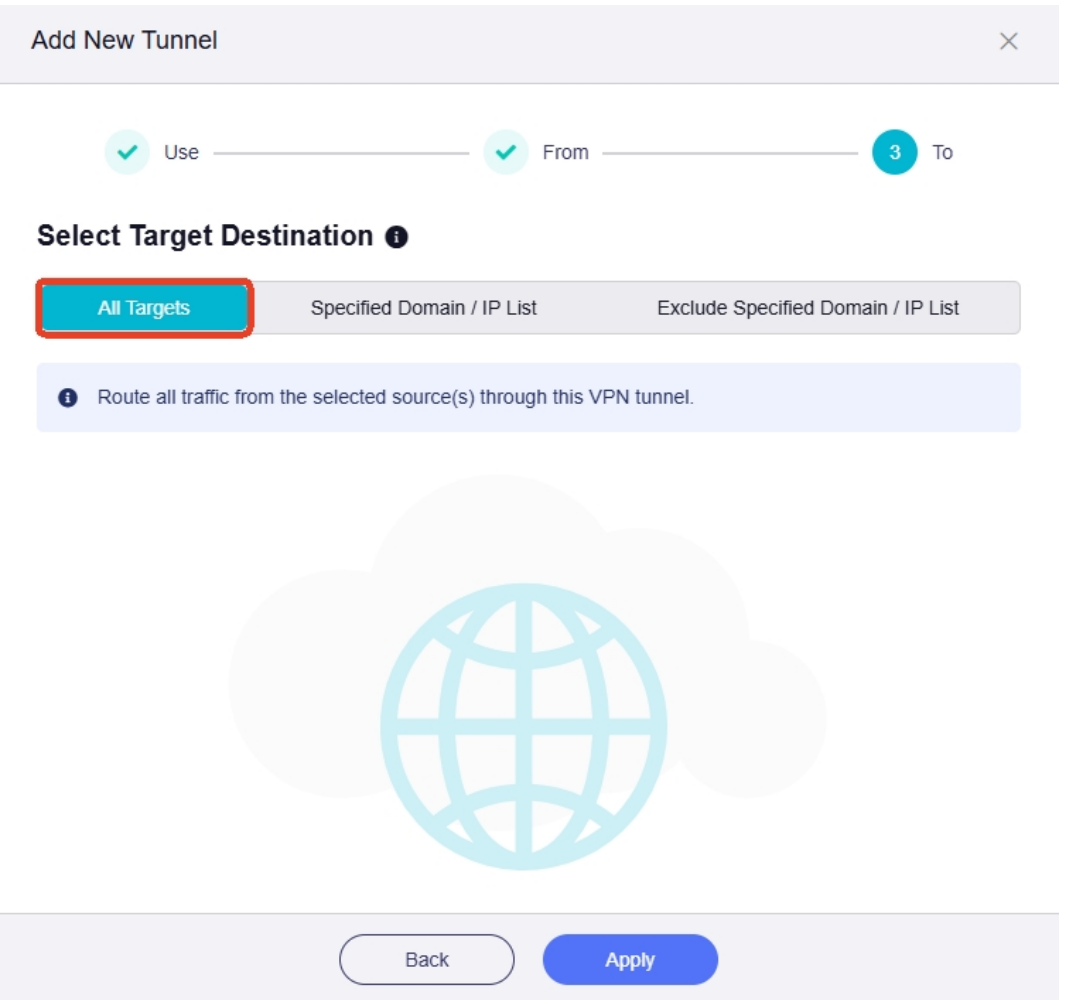
   Fai clic sulla scheda **Tutti i client**, impostala come origine client per Tunnel 2, quindi fai clic su **Avanti**.



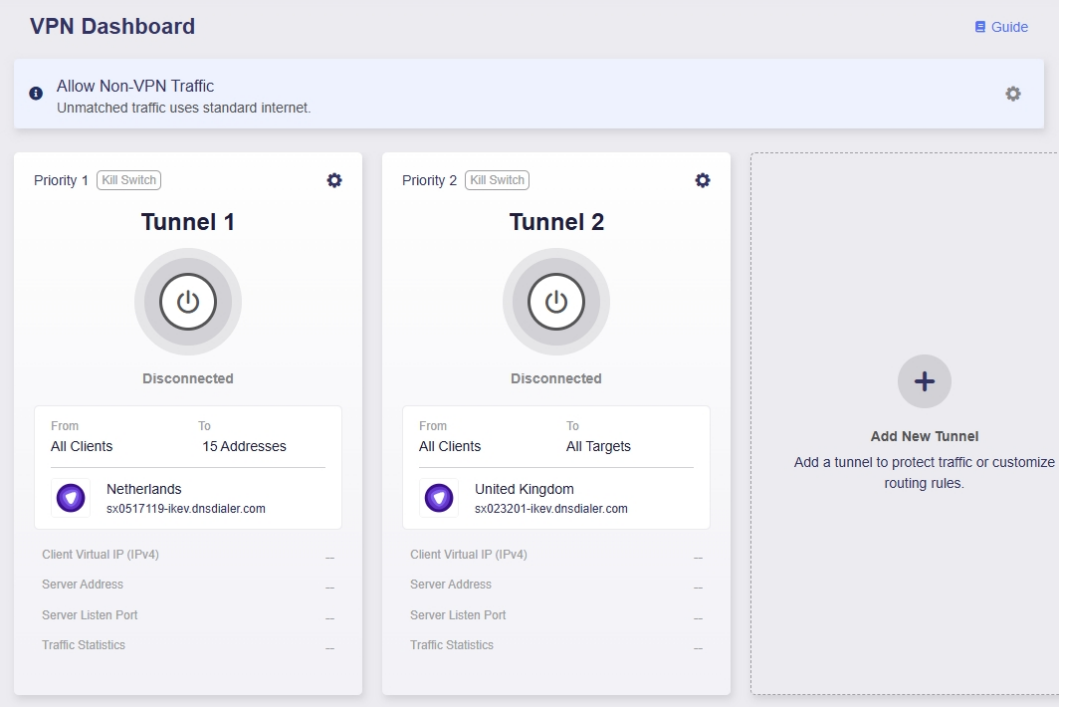


9. Seleziona la destinazione del traffico.

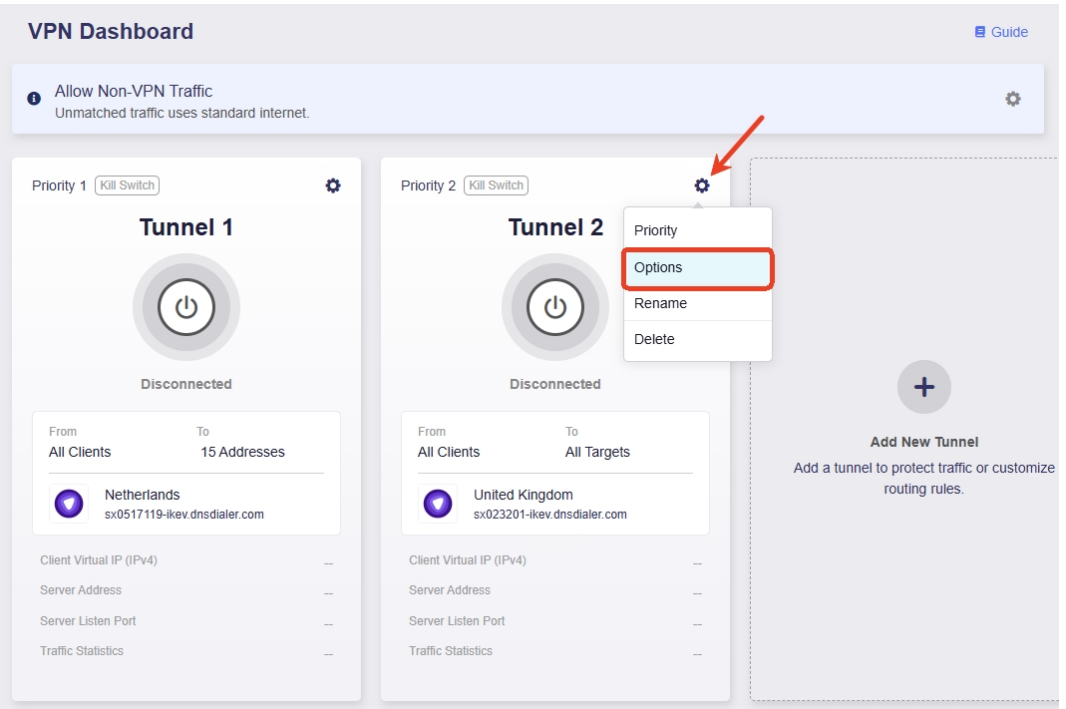
   Fai clic sulla scheda **Tutti i target**, impostala come destinazione del traffico per il Tunnel 2, quindi fai clic su **Applica**.

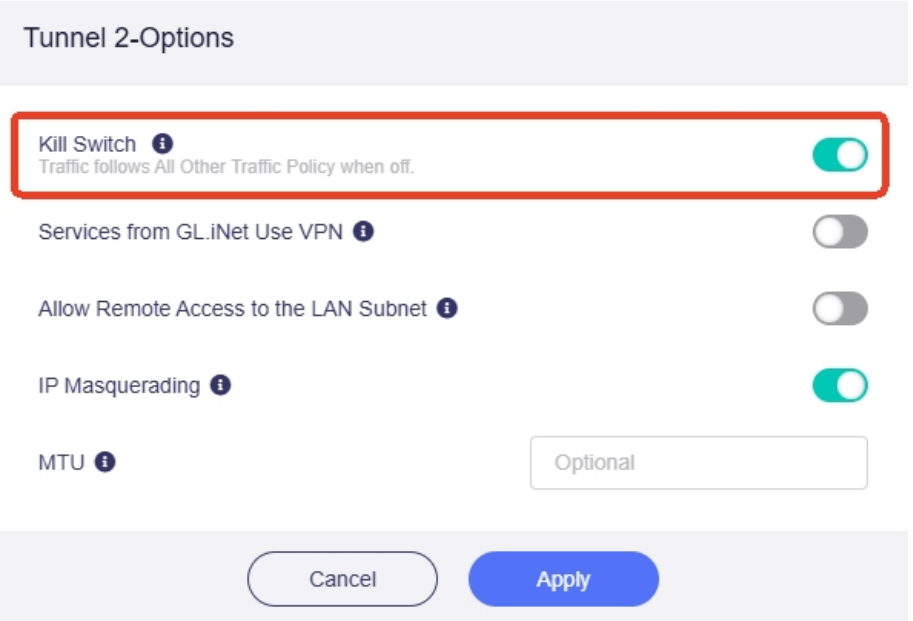


10. Verrai indirizzato alla dashboard della VPN. Ora il tunnel VPN 2 è stato aggiunto con successo.

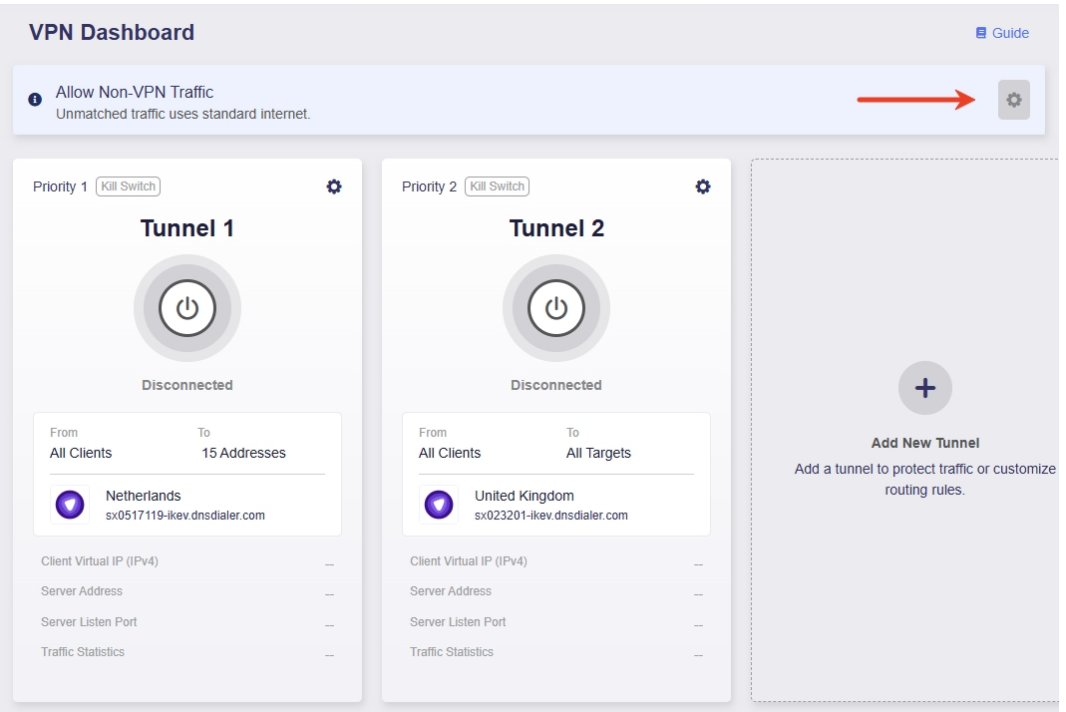


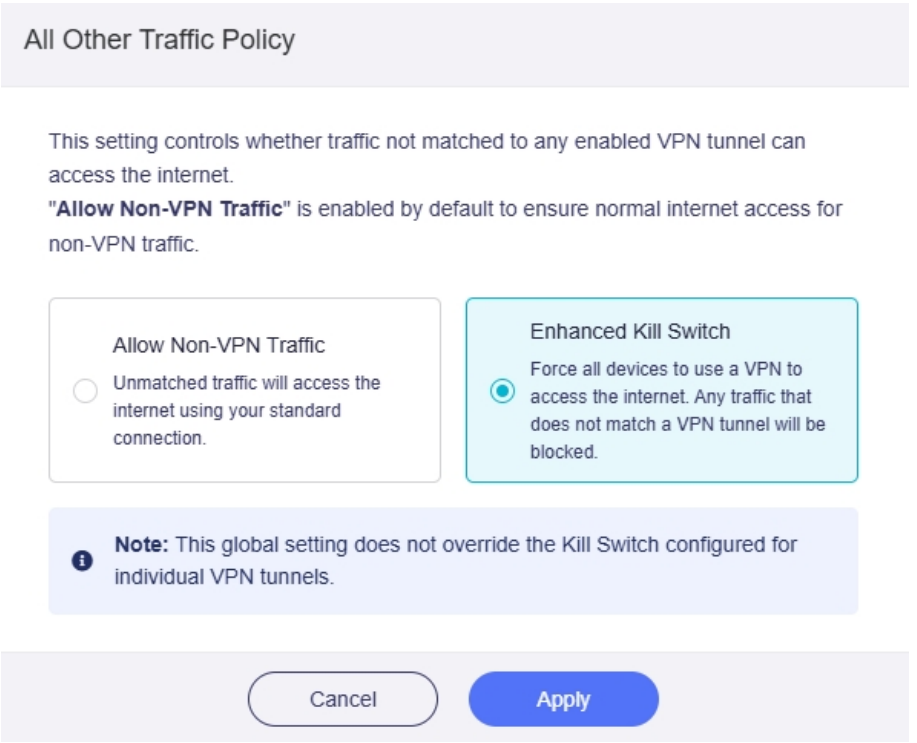
11. Assicurati che il **Kill Switch** per Tunnel 2 sia abilitato. Se la VPN si disconnette inaspettatamente, l'accesso a Internet per il traffico corrispondente a questo tunnel verrà bloccato per impedire perdite DNS e tracciamento IP.



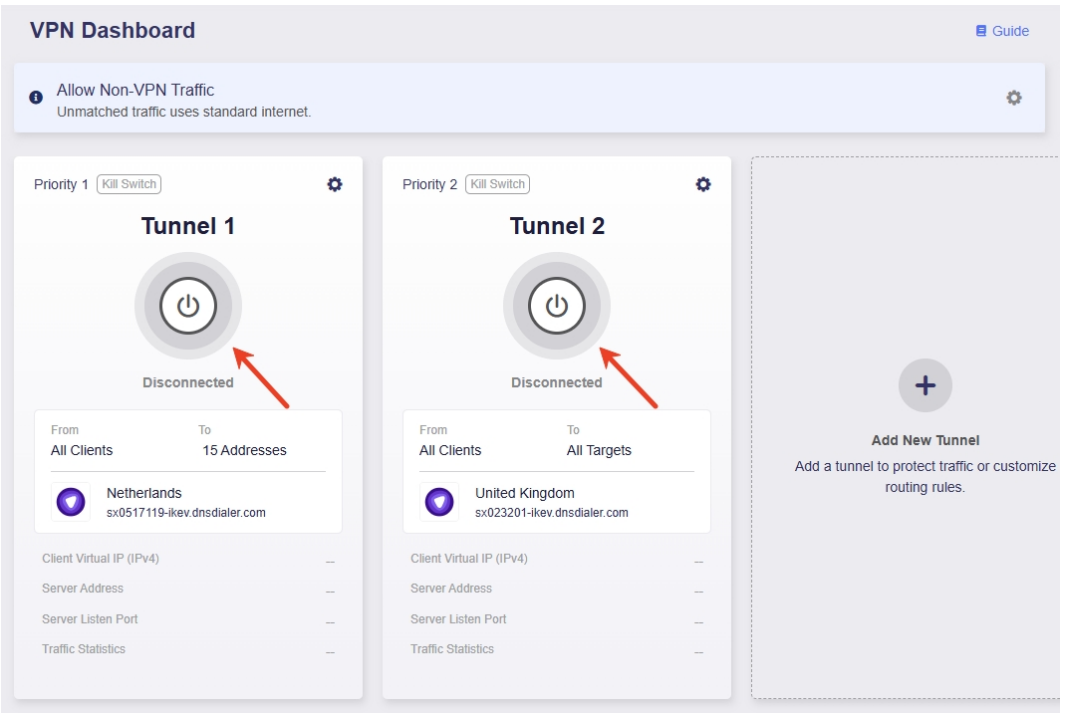


12. Fai clic sull'icona a forma di ingranaggio in alto a destra per abilitare il **Kill Switch avanzato**. Ciò garantisce che tutto il traffico debba accedere a Internet tramite VPN.

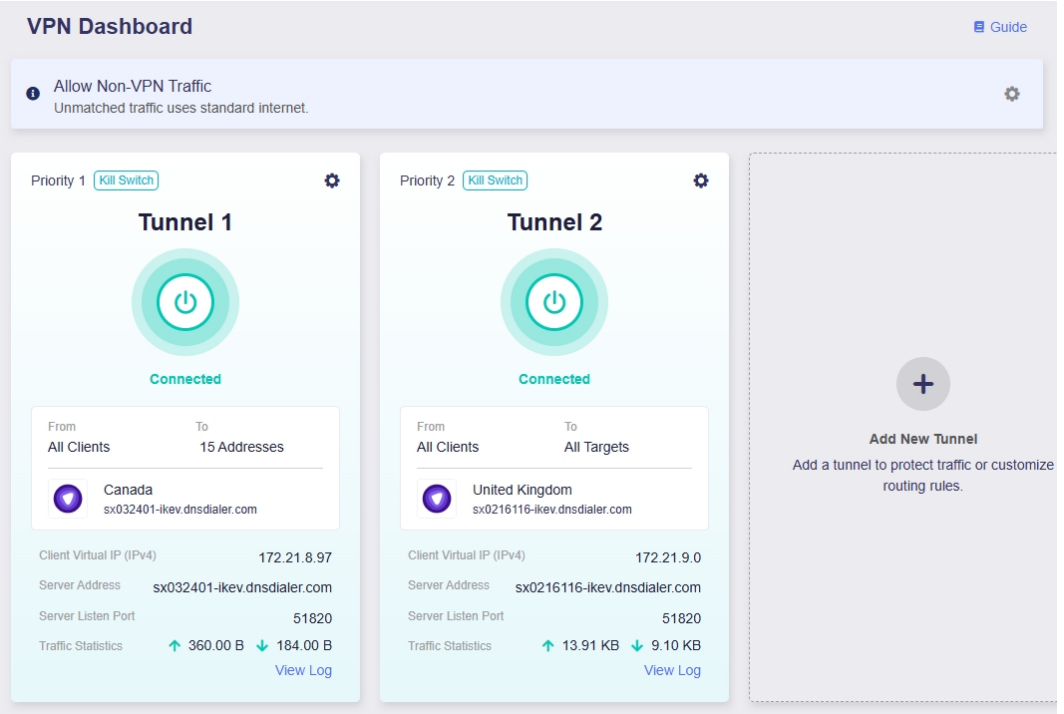




13. Fai clic sul pulsante centrale per attivare Tunnel 1 e Tunnel 2.



14. Una volta connesso, la pagina visualizzerà i dettagli della connessione VPN, inclusi criteri VPN, statistiche sul traffico, indirizzo del server, porta di ascolto e indirizzo IP virtuale.



Ora tutti i dispositivi utilizzeranno il Tunnel VPN 1 per l'accesso a domini specifici e utilizzeranno il Tunnel VPN 2 per tutti gli altri accessi a Internet. Se i tunnel VPN si disconnettono inaspettatamente, l'accesso a Internet per tutti i dispositivi verrà bloccato per impedire perdite DNS e tracciamento IP.

8.3 Kill Switch

Kill Switch è una funzionalità di sicurezza per le connessioni VPN. Interrompe automaticamente tutti gli accessi a Internet per la tua rete locale se la connessione VPN si interrompe inaspettatamente, impedendo che il tuo indirizzo IP reale e i tuoi dati online vengano esposti e garantendo privacy e sicurezza continue. Questa funzionalità è particolarmente utile per mantenere un accesso a Internet sicuro e anonimo, ad esempio quando si utilizzano reti pubbliche, si elaborano dati sensibili o si nasconde il proprio indirizzo IP reale.

Se abilitato, blocca qualsiasi traffico client che tenta di bypassare il tunnel VPN, bloccando efficacemente le perdite VPN causate da problemi di configurazione DNS, disconnessioni impreviste, richieste IP dirette e altri scenari simili.

A partire dal firmware v4.8, i router GL.iNet supportano la configurazione Kill Switch per la connessione VPN globale, nonché per ogni singolo tunnel VPN.

- Per configurare Kill Switch per la connessione VPN globale, fai riferimento a Tutto il resto del traffico.
- Per configurare Kill Switch per ogni singolo tunnel VPN, fai riferimento alle Opzioni tunnel.

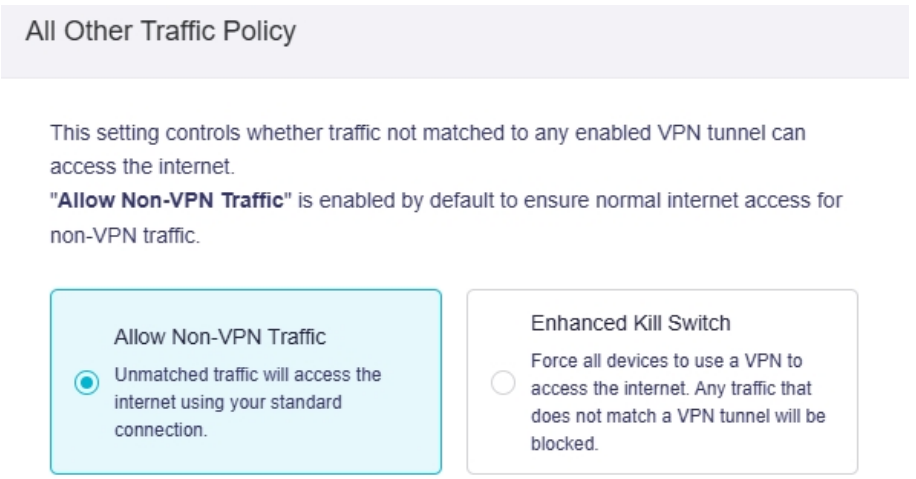
8.4 Tutto il resto del traffico

Fai clic sull'icona a forma di ingranaggio in alto a destra per impostare la politica per il traffico che non corrisponde al tunnel VPN.

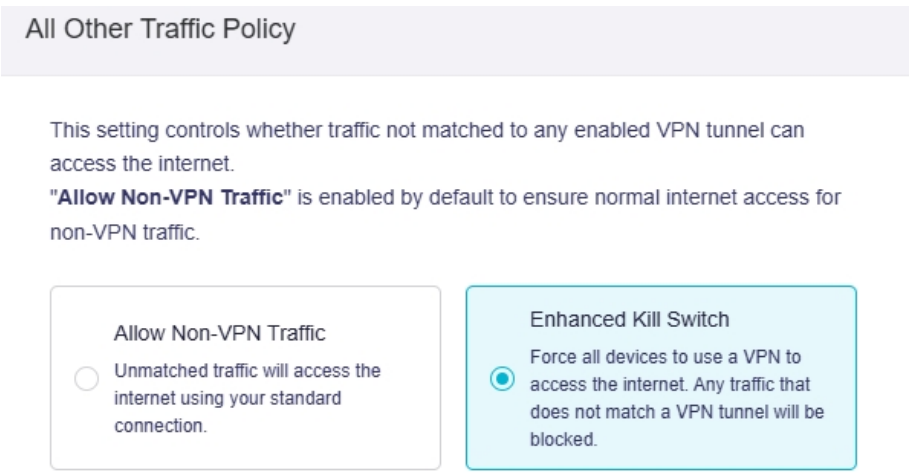


Questa policy controlla se il traffico che non corrisponde a nessuno dei tuoi gruppi di tunnel VPN può accedere o meno a Internet. Ha due opzioni:

- **Consenti traffico non VPN**: abilitato per impostazione predefinita per garantire il normale accesso a Internet per il traffico non VPN.



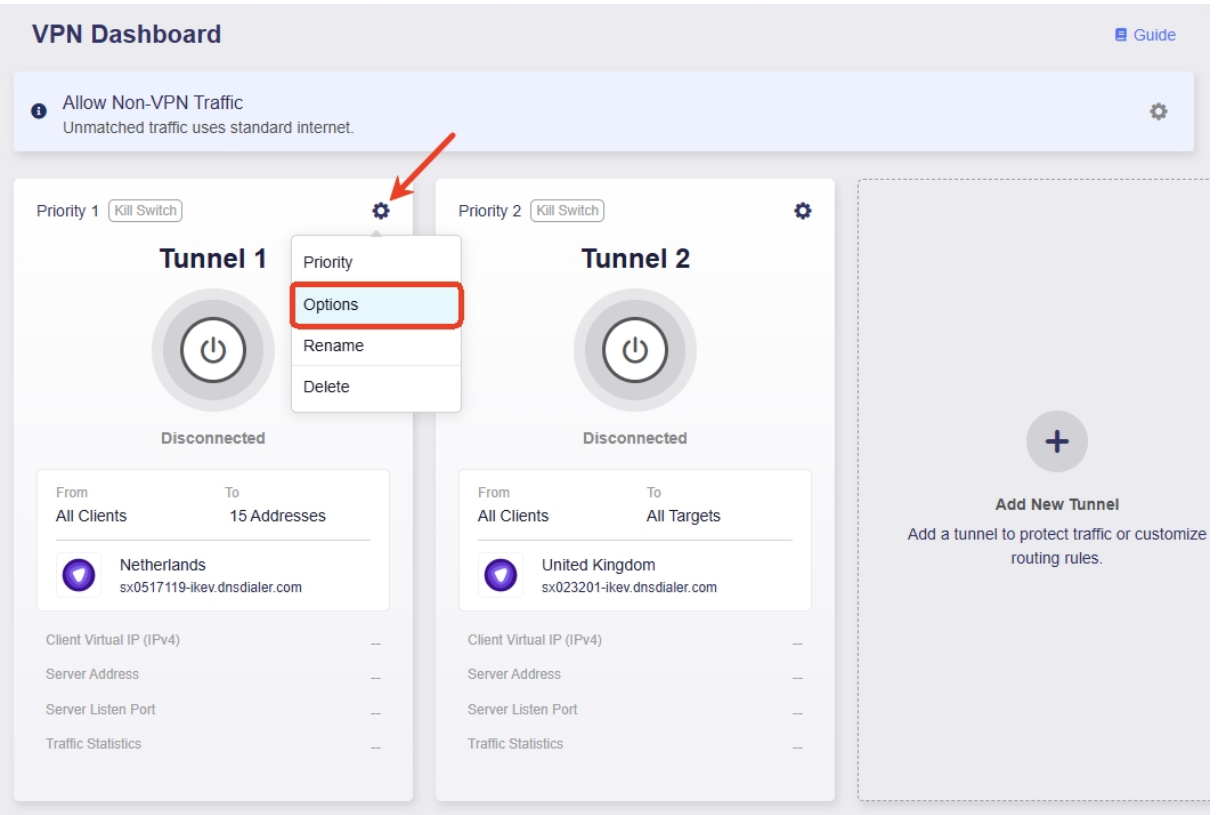
- **Kill Switch avanzato**: forza tutti i dispositivi ad accedere a Internet tramite una VPN. Tutto il traffico che non corrisponde a un tunnel VPN verrà bloccato. Questa impostazione globale non sovrascrive il Kill Switch configurato per i singoli tunnel VPN.

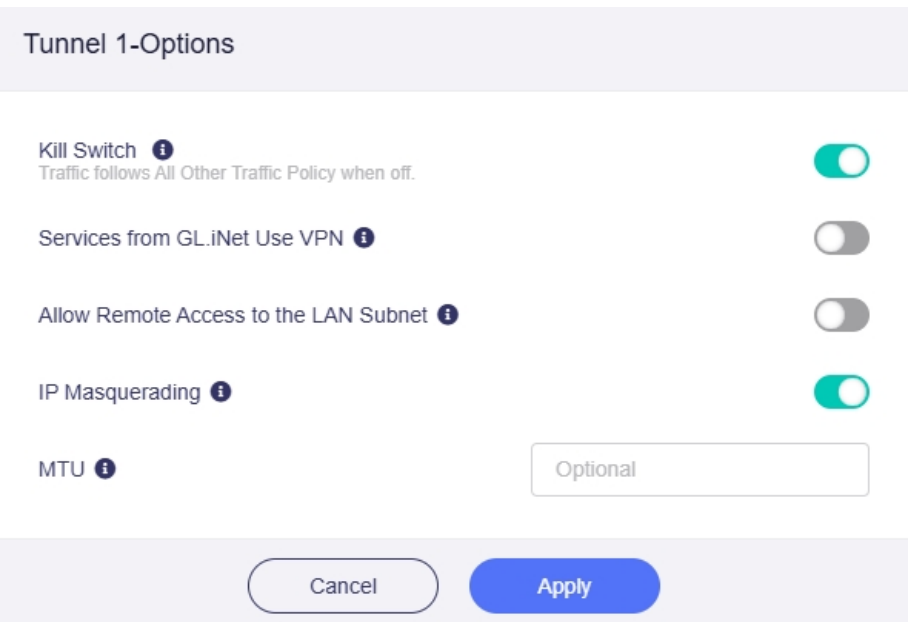


8.5 Opzioni del tunnel

Puoi configurare impostazioni avanzate per ciascun tunnel VPN, come VPN Kill Switch, Masquerading IP e MTU.

Fai clic sull'icona a forma di ingranaggio in un gruppo di tunnel e seleziona **Opzioni**.

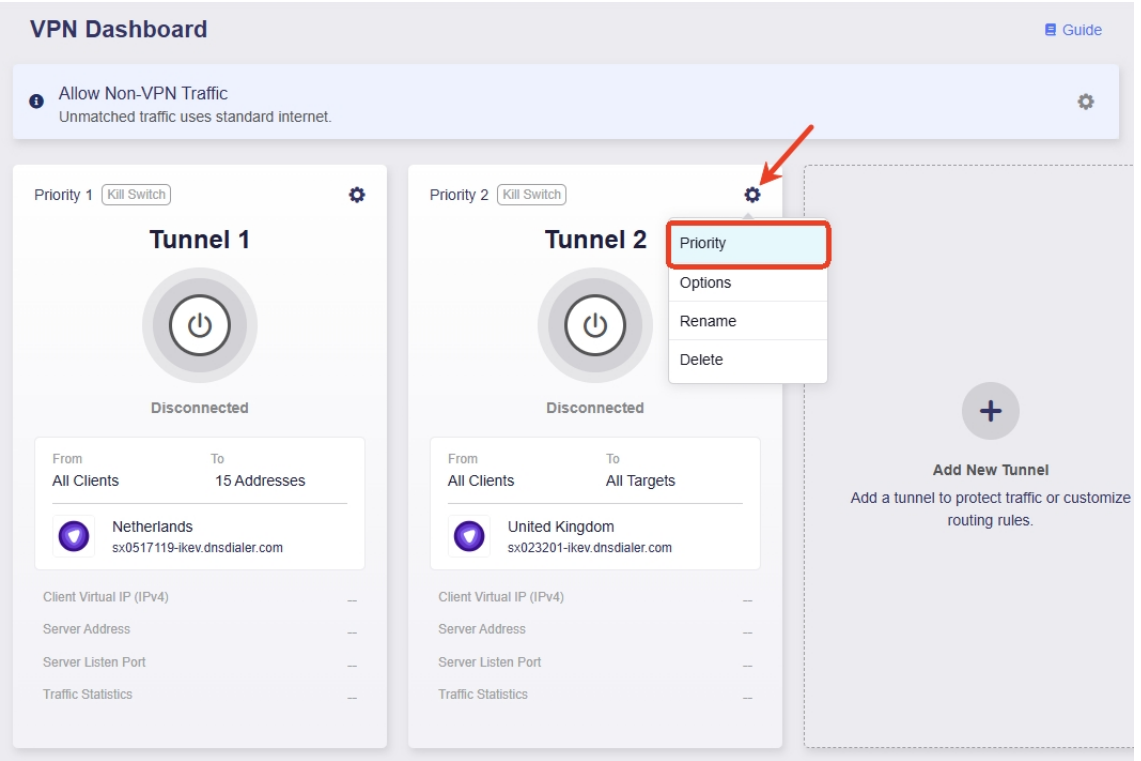




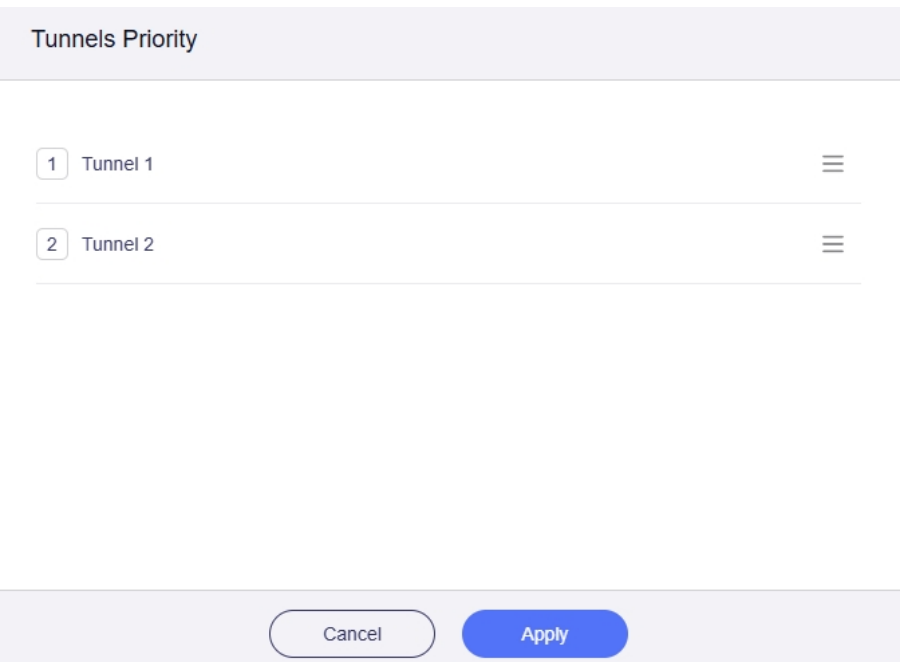
- **Kill Switch**: se abilitato, il traffico corrispondente a questo tunnel VPN verrà bloccato se la connessione VPN fallisce inaspettatamente. Se disabilitato, tale traffico eseguirà il failover nel tunnel Tutto il resto del traffico.
- **Usa la VPN per i servizi GL.iNet**: se abilitati, i servizi GoodCloud, DDNS e 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.
- **Consenti accesso remoto alla sottorete LAN**: se abilitato, sarà consentito l'accesso remoto a questo router e ai suoi dispositivi LAN tramite la VPN. Richiede che il server VPN pubblicizzi un percorso di ritorno alla sua sottorete LAN.
- **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**: il valore MTU impostato per il tunnel sovrascriverà le impostazioni MTU nel file di configurazione.

8.6 Priorità dei tunnel

Per regolare la priorità del tunnel, fai clic sull'icona a forma di ingranaggio in un gruppo di tunnel e seleziona **Priorità**.



Fai clic e tieni premuta l'icona a tre righe a destra per riordinare i tunnel, quindi fai clic su **Applica**.



Quando sono abilitati più tunnel, il router instrada il traffico secondo le seguenti regole:

1. Il traffico tenterà innanzitutto di soddisfare la regola del tunnel con la priorità più alta. Se abbinato, verrà instradato attraverso quel tunnel; altrimenti proverà il tunnel con priorità successiva e così via.
2. Ogni gruppo di tunnel funziona in modo indipendente. Una volta che il traffico corrisponde a una regola del tunnel, verrà instradato attraverso quel tunnel e non verrà eseguito il failover tra i gruppi di tunnel.
3. È possibile selezionare più profili all'interno di ciascun gruppo di tunnel per abilitare il failover intra-tunnel. Quando il profilo con la priorità più alta in un gruppo di tunnel viene interrotto, il tunnel si connetterà automaticamente utilizzando il secondo profilo con la priorità più alta e così via.
4. Se un tunnel VPN si disconnette inaspettatamente, il sistema determinerà se eseguire il failover del traffico verso il tunnel Tutto il resto del traffico in base al fatto che il **Kill Switch** di questo tunnel sia abilitato.
    - Se il Kill Switch è abilitato, il traffico verrà bloccato e non verrà eseguito il failover sul tunnel Tutto il resto del traffico.
    - Se il Kill Switch è disabilitato, il traffico eseguirà il failover nel tunnel Tutto il resto del traffico.
5. Nel tunnel **Tutto il resto del traffico**, diverse modalità determinano se il traffico che non corrisponde al tunnel VPN può accedere a Internet.
    - **Consenti traffico non VPN**: è abilitato per impostazione predefinita per garantire che il traffico che non corrisponde ai tunnel VPN possa comunque accedere a Internet tramite WAN locale.

- **Kill Switch avanzato**: forza tutti i dispositivi ad accedere a Internet tramite una VPN. Tutto il traffico che non corrisponde a un tunnel VPN verrà bloccato. Questa impostazione globale non sovrascrive il Kill Switch configurato per i singoli tunnel VPN. In breve, rafforza il Kill Switch e blocca l'accesso regolare a Internet per prevenire perdite di IP.

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:

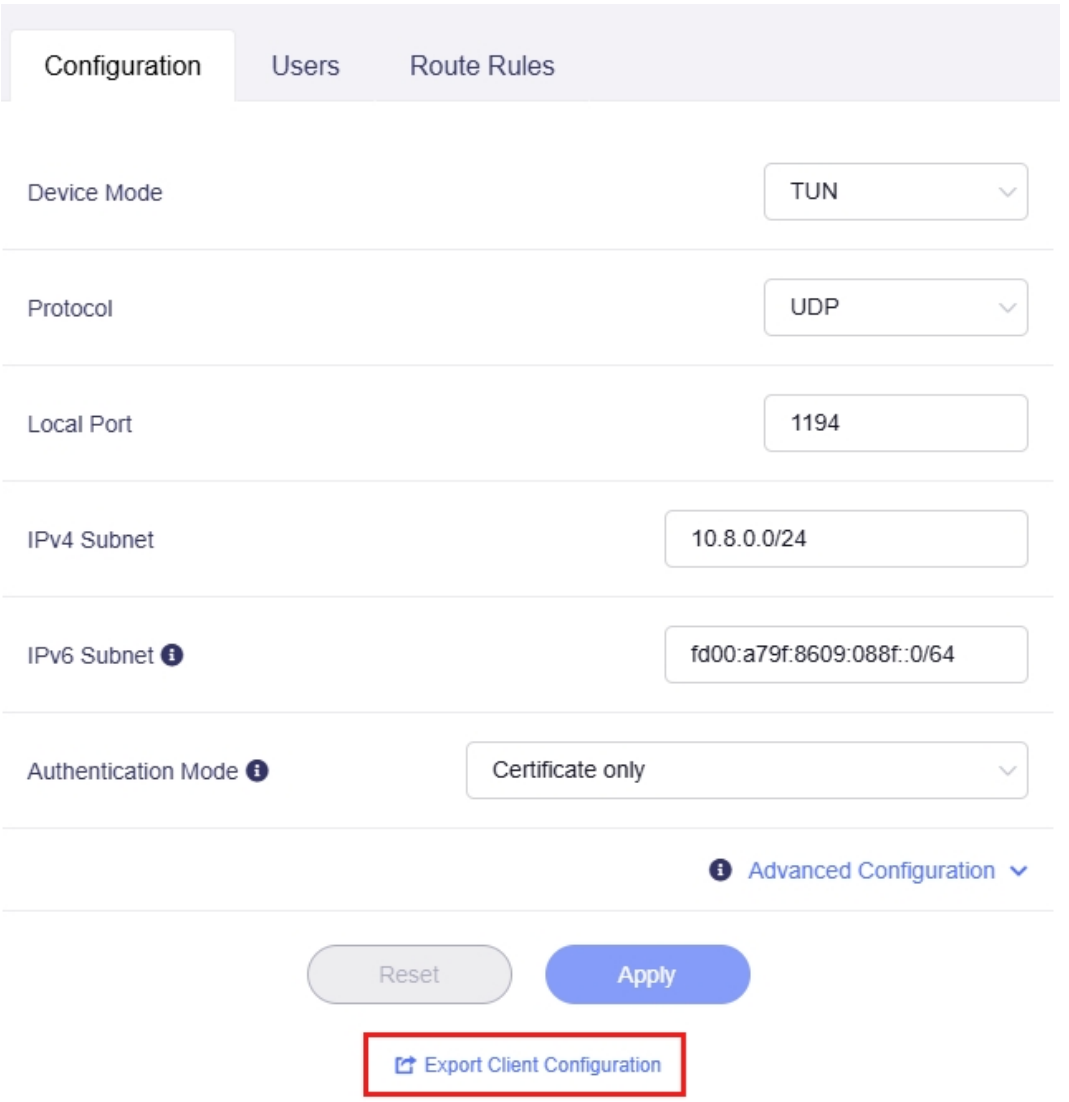
   - Se disponi di un router primario a monte del tuo router GL.iNet, accedi ad esso e verifica che abbia un indirizzo IP pubblico assegnato dal tuo ISP.
   - Chiedi al tuo ISP un indirizzo IP pubblico. Ciò potrebbe comportare un costo aggiuntivo.
   - Se i due metodi precedenti non funzionano (ad esempio, se la tua rete è dietro CGNAT), puoi provare la nostra soluzione SD-WAN AstroWarp.

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

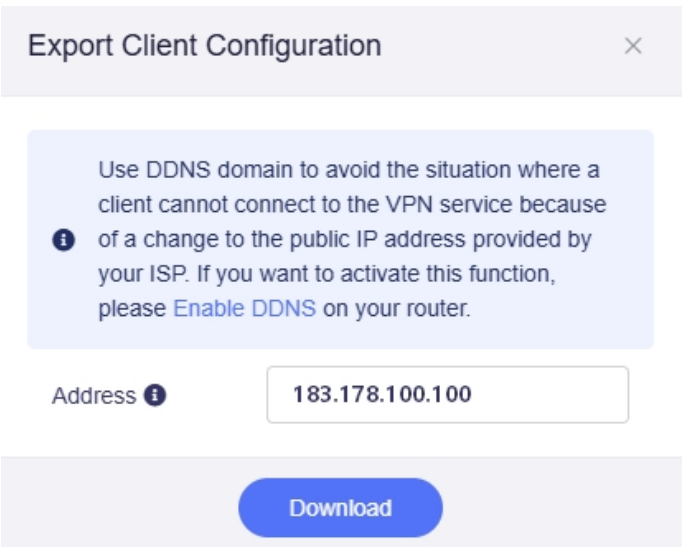
1. Accedi al pannello di amministrazione web del router, vai a **VPN** > **Server OpenVPN**, quindi fai clic su **Genera configurazione** (solo per la configurazione iniziale del server VPN).
2. Applica la configurazione.
   La configurazione predefinita funziona nella maggior parte dei casi. Fai clic 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 secondo necessità.

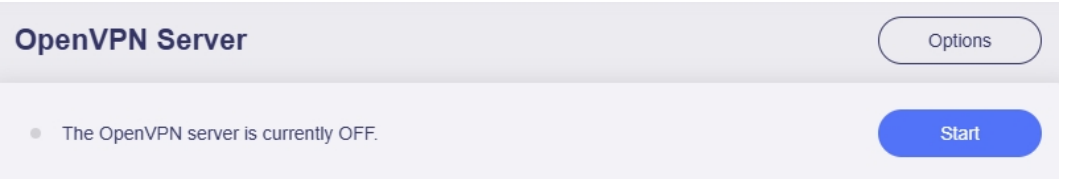
3. Esporta configurazione client.
   Dopo aver fatto clic su **Esporta configurazione client** nella parte inferiore della scheda Configurazione (o dopo aver applicato la configurazione modificata), verrà visualizzata una finestra come segue. Fai clic su **Scarica** per esportare la configurazione.



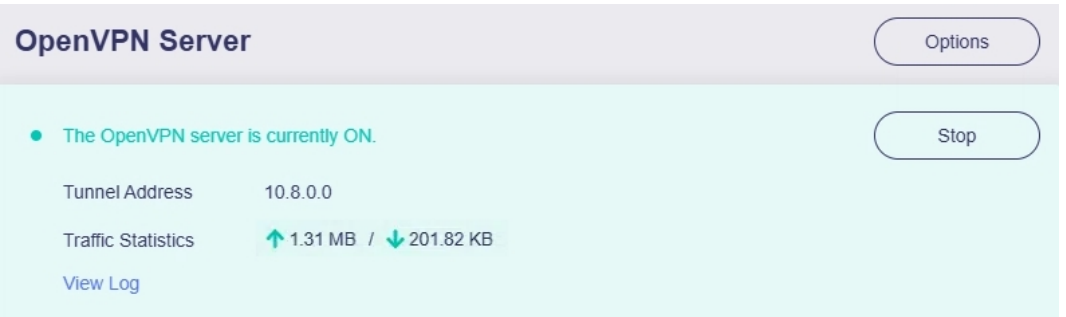
Suggerimenti:

- Se il tuo indirizzo IP pubblico cambia frequentemente, vai su **APPLICAZIONI** > **DNS dinamico** e attiva DDNS. Puoi quindi utilizzare il dominio DDNS come indirizzo del server.
- A partire dal firmware v4.8, è possibile selezionare l'indirizzo del server da un elenco a discesa prima di esportare il file di configurazione: IP pubblico, dominio DDNS e indirizzo IP WAN corrente. Una volta selezionato, l'indirizzo del server nel file di configurazione verrà aggiornato automaticamente. Scaricare nuovamente il file di configurazione se l'indirizzo del server viene modificato.

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.



   Lo stato della connessione al server viene visualizzato in alto. Se mostra le statistiche sul traffico di caricamento e download, significa che 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.
   - Se i due metodi precedenti non funzionano (ad esempio, se la tua rete è dietro CGNAT), puoi provare la nostra soluzione SD-WAN AstroWarp.

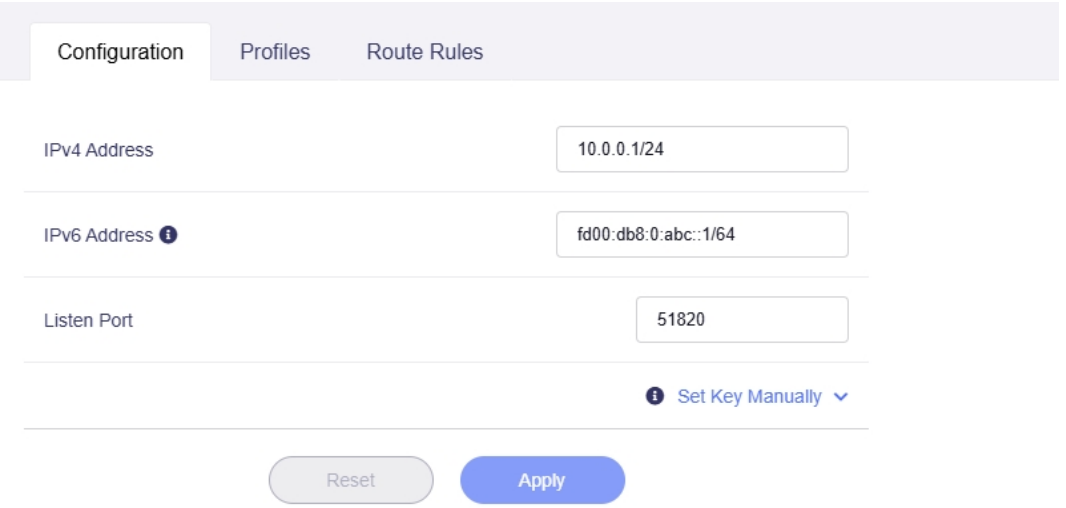
2. **Conferma se è richiesto il port forwarding**

   - 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.

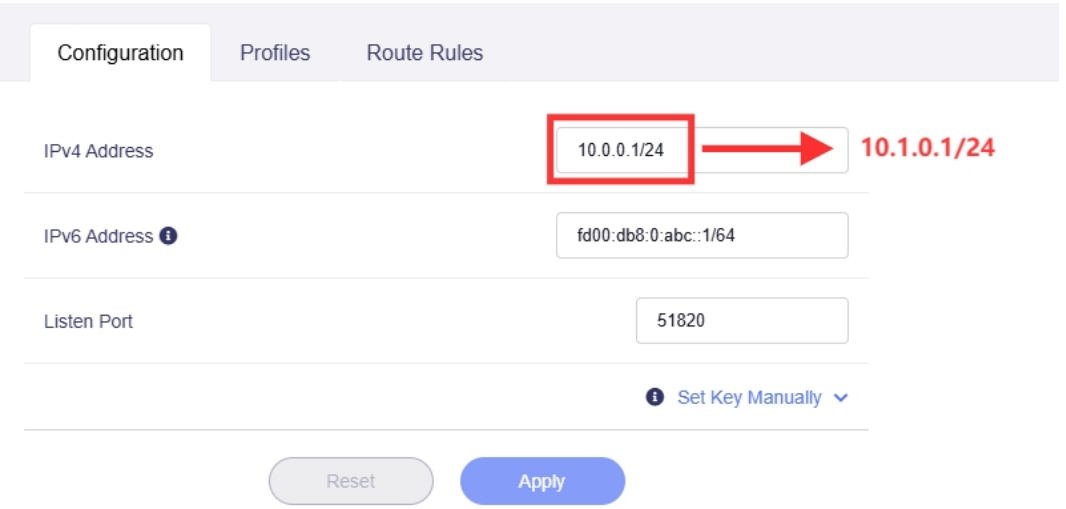
9.2.2 Procedura di configurazione

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.

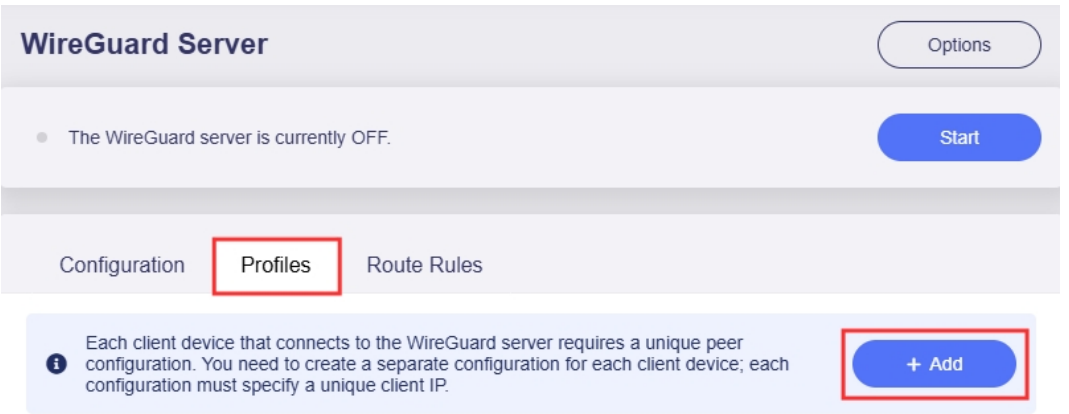


   Se l'indirizzo IPv4 è in conflitto con il gateway del router upstream, modifica l'indirizzo IPv4 con un altro (ad esempio, **10.1.0.1/24**) e fai clic su **Applica**. Assicurati che la notazione CIDR "/24" sia inclusa per evitare problemi di connettività.

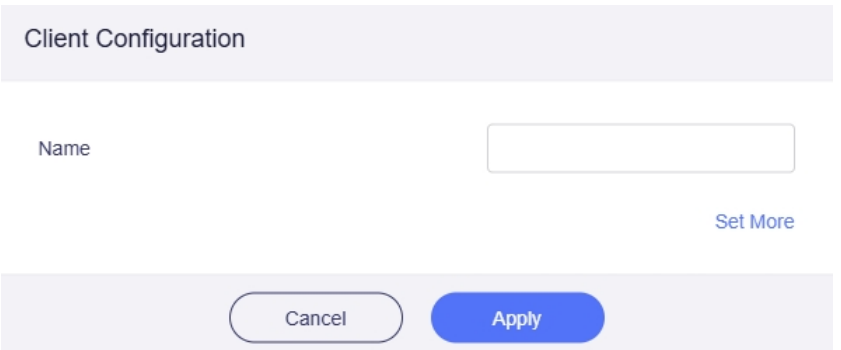


3. Aggiungi un profilo.

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.



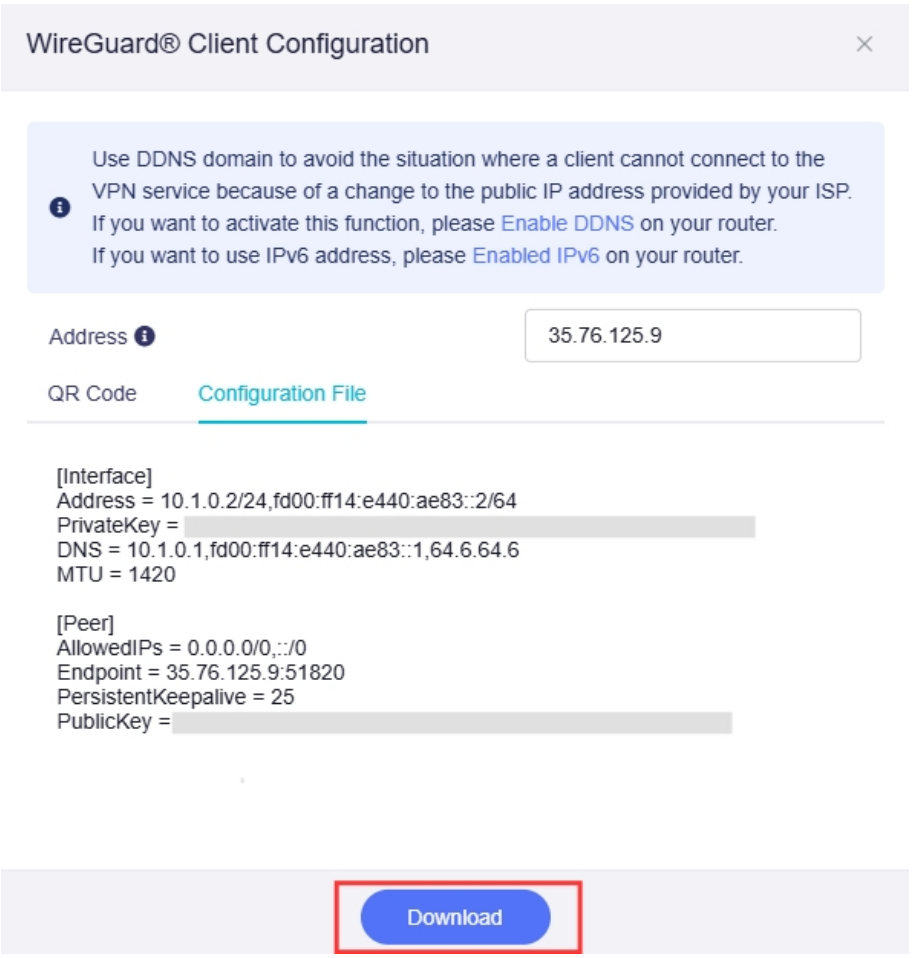
Suggerimento: se desideri accedere ai dispositivi LAN del client WireGuard dal tuo server WireGuard, passa alla scheda **Regole di routing** per configurare le regole di routing. Vedi qui per i dettagli.

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.

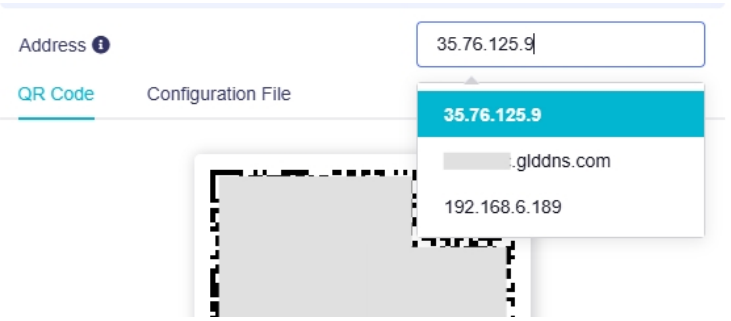
   - **Codice QR**: adatto per dispositivi (ad esempio smartphone, tablet, laptop) con l'app WireGuard installata. Se desideri impostare un dispositivo specifico come client WireGuard, apri semplicemente l'app WireGuard e scansiona il codice QR per importare un file di configurazione.
   - **Testo normale**: 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.



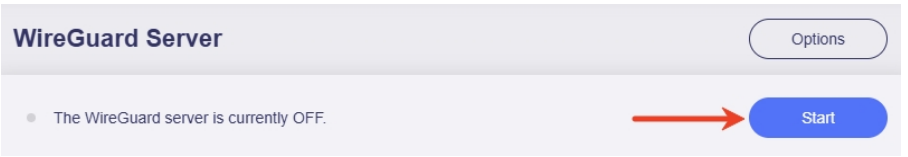
Suggerimenti:

- Se il tuo indirizzo IP pubblico cambia frequentemente, vai su **APPLICAZIONI** > **DNS dinamico** e attiva DDNS. Puoi quindi utilizzare il dominio DDNS come indirizzo del server.
- A partire dal firmware v4.8, è possibile selezionare l'indirizzo del server da un elenco a discesa prima di esportare il file di configurazione: IP pubblico, dominio DDNS e indirizzo IP WAN corrente. Una volta selezionato, l'indirizzo del server nel file di configurazione verrà aggiornato automaticamente. Scaricare nuovamente il file di configurazione se l'indirizzo del server viene modificato.

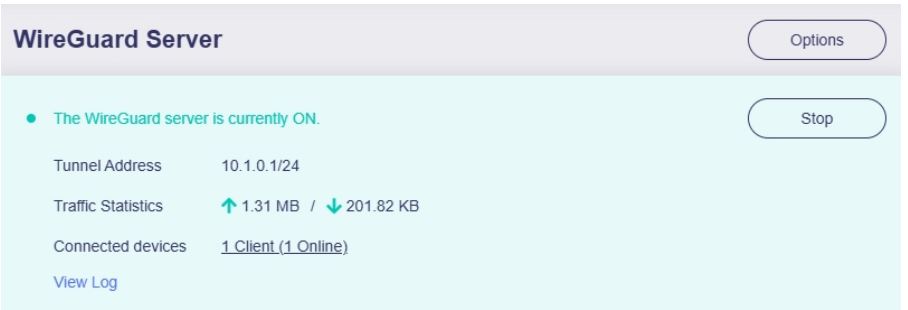


5. Avvia il server WireGuard.

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



   Lo stato della connessione al server viene visualizzato in alto. Se mostra le statistiche sul traffico di caricamento, download e dispositivi connessi online, significa che il server WireGuard 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.

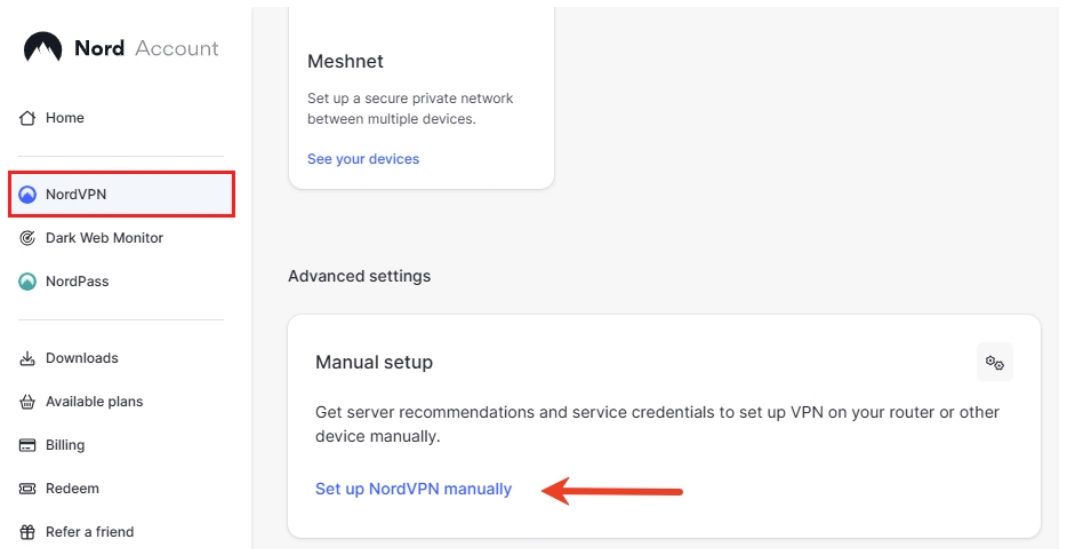
Successivamente, visita il sito Web ufficiale del fornitore di servizi VPN a cui sei iscritto e ottieni le credenziali del servizio o il file di configurazione. Se non sai come ottenere il file di configurazione, fai riferimento a questo collegamento o contatta il loro supporto.

10.1.2 Configurazione di NordVPN

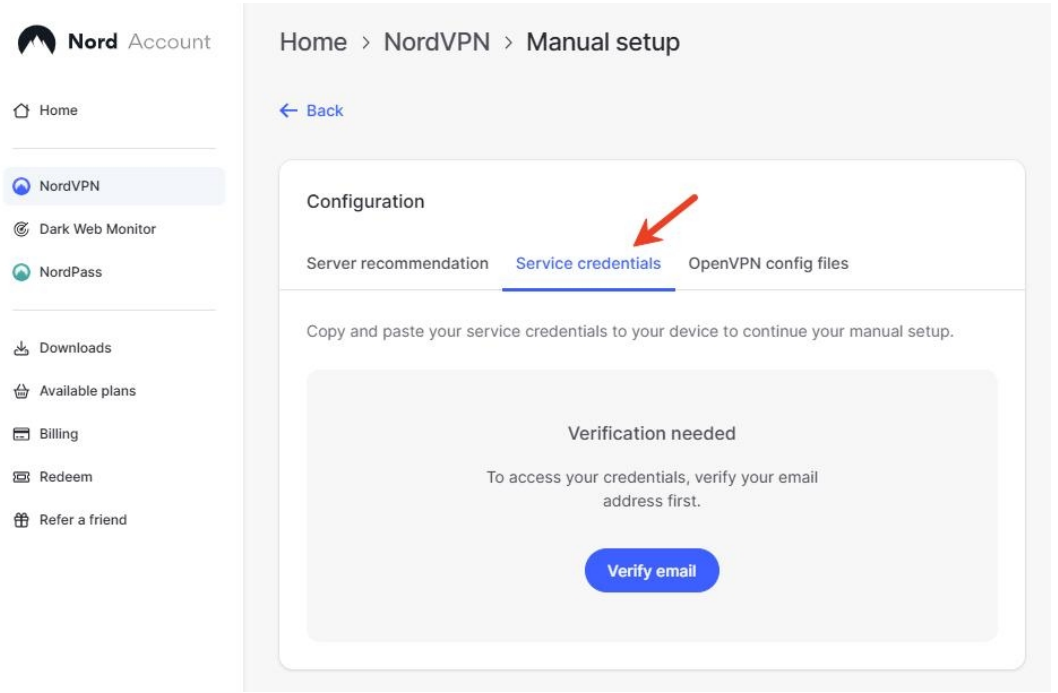
NordVPN è integrato in GL.iNet pannello di amministrazione web. Puoi acquisire file di configurazione per tutti i server NordVPN inserendo le credenziali del tuo account (ottenute dalla dashboard NordVPN) nell'app mobile pannello di amministrazione web o GL.iNet del router, eliminando la necessità di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

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

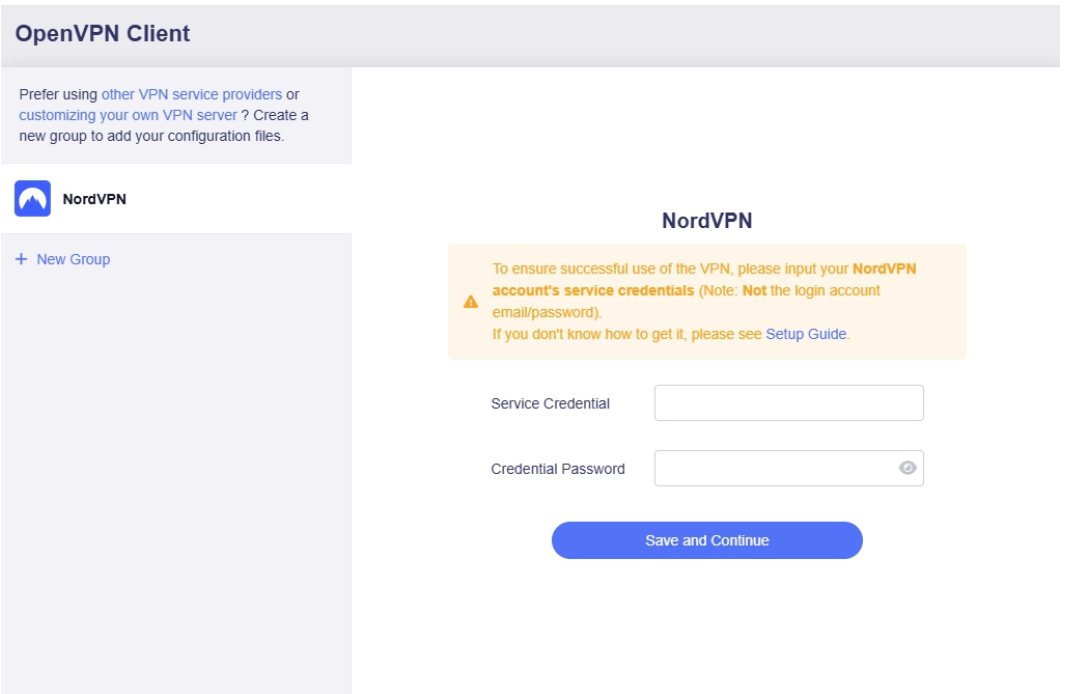
1. Accedi al tuo account web NordVPN qui.
2. Nella Nord Dashboard, fai clic su **NordVPN**, quindi su **Configura NordVPN manualmente**.



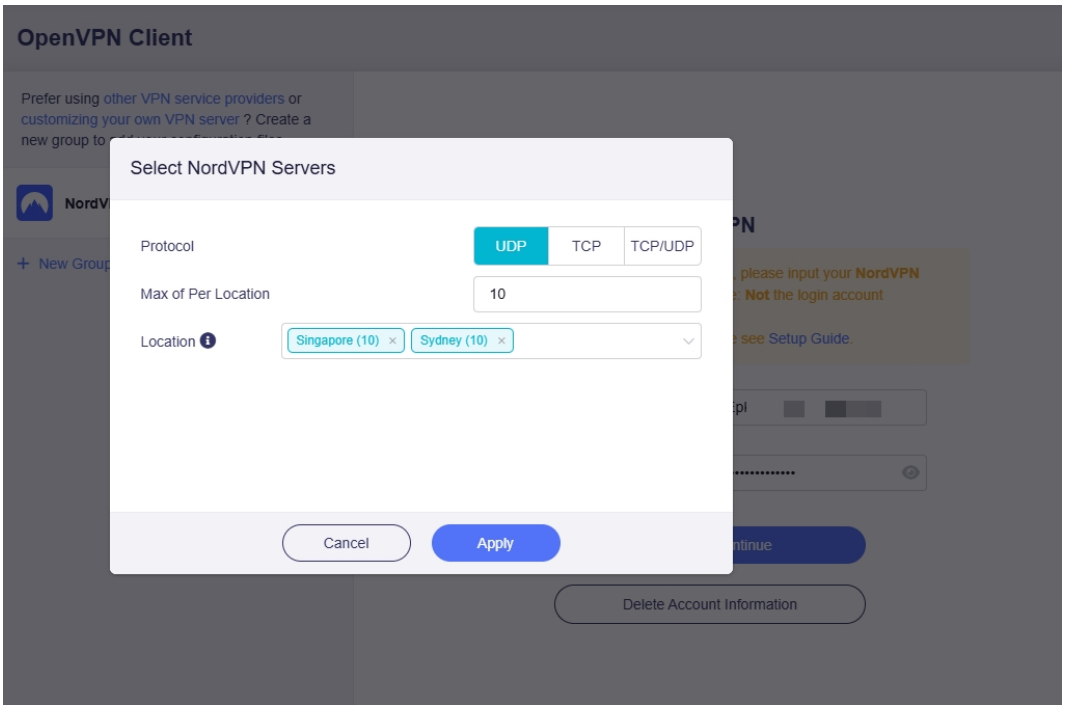
Troverai le **credenziali del servizio**. Copiali per un uso successivo.



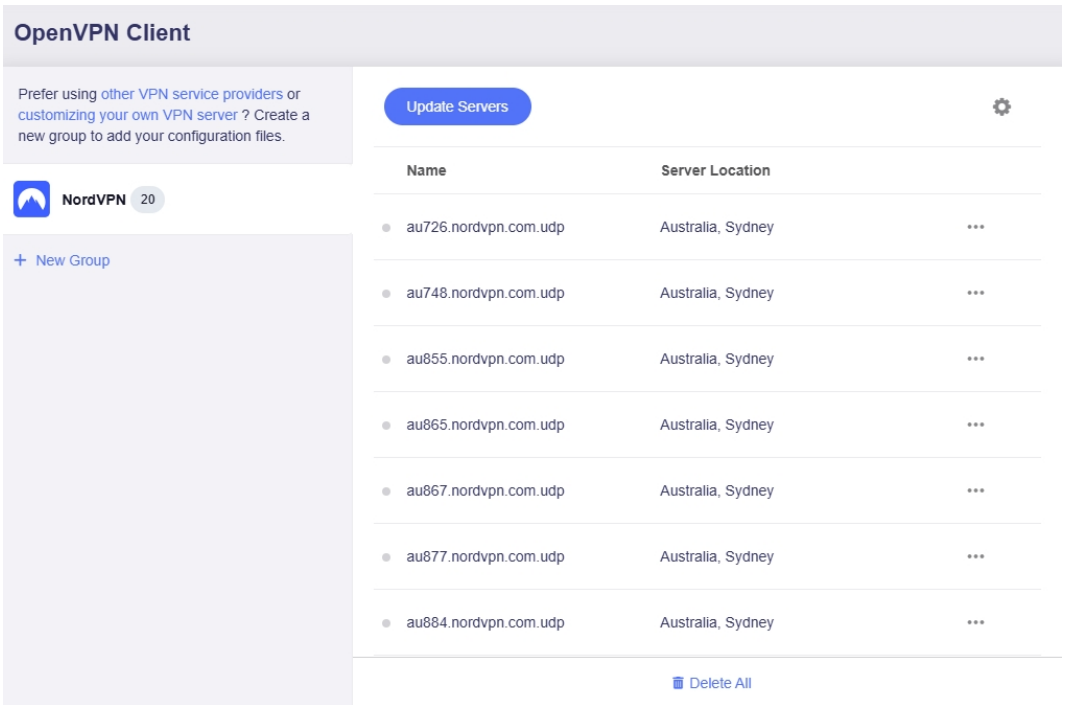
3. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client OpenVPN** > **NordVPN**. Inserisci le credenziali del servizio (Nota: NON è l'e-mail/password dell'account di accesso), quindi fai clic su **Salva e continua**.



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

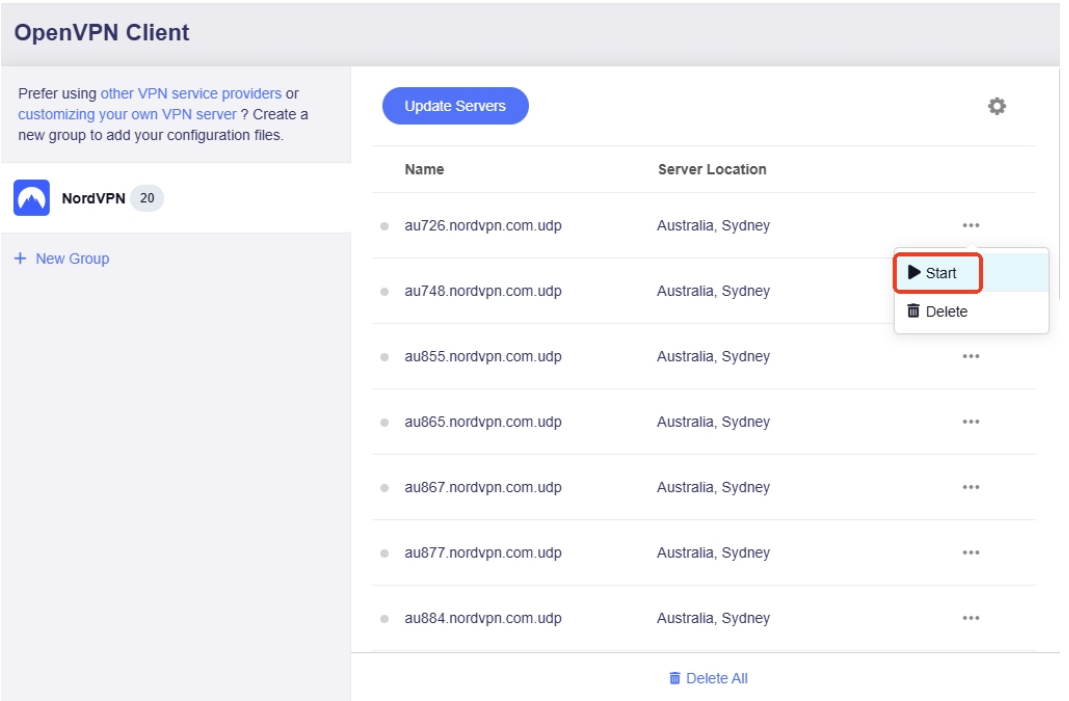


Scaricherà i file di configurazione.

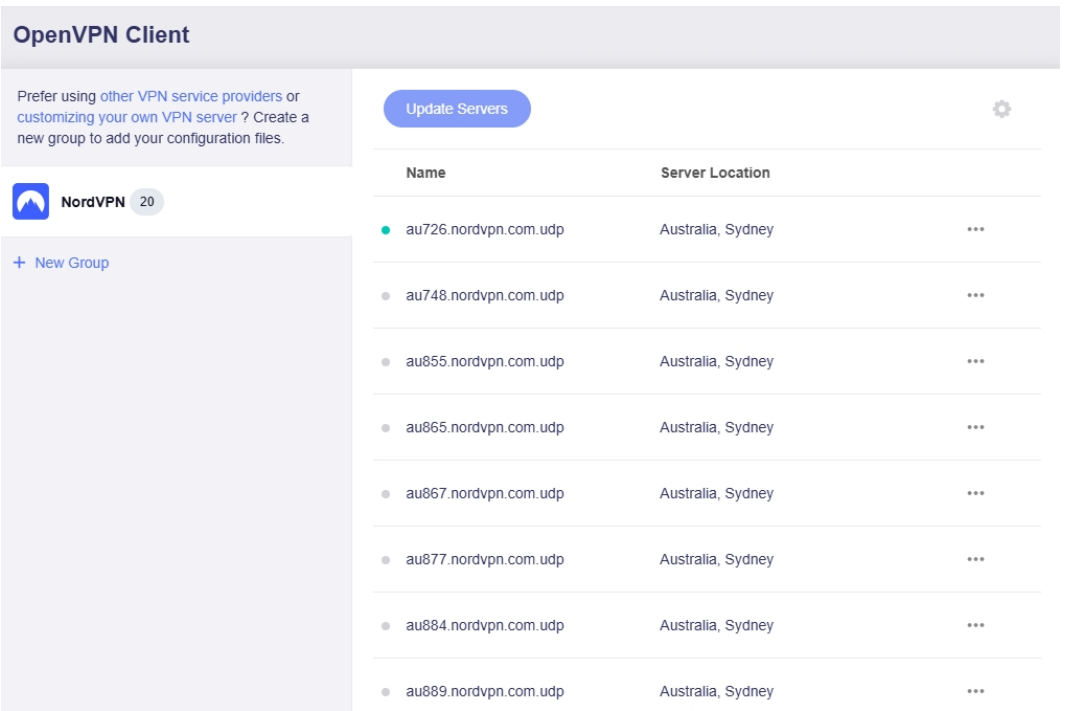


5. Avvia una connessione.

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



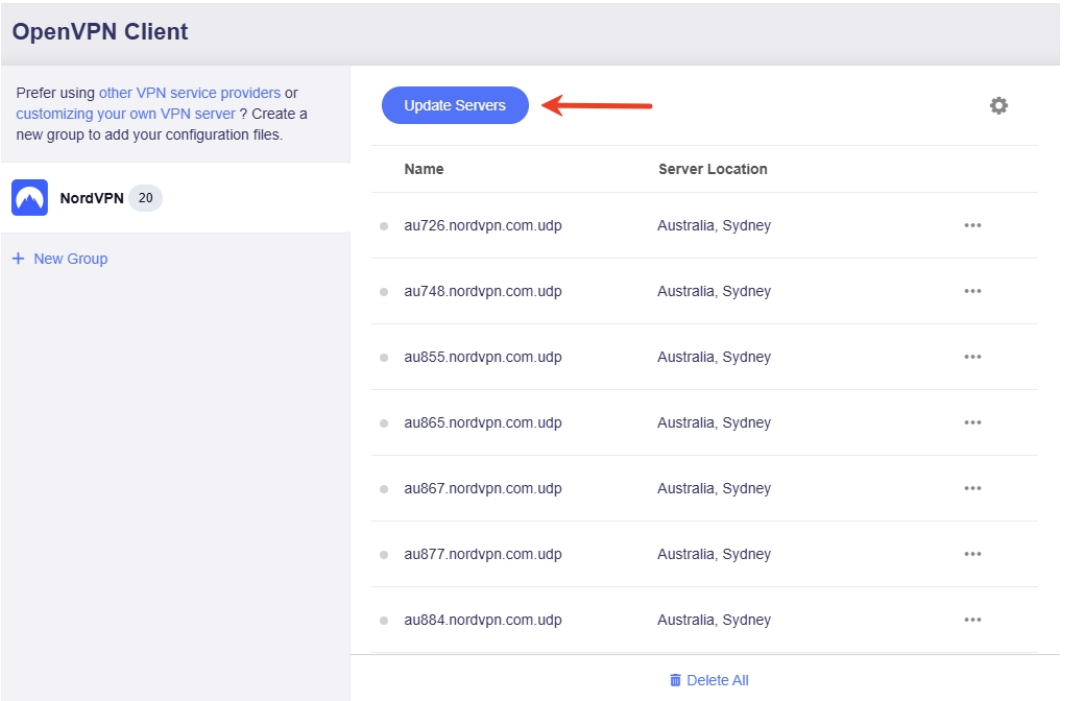
6. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

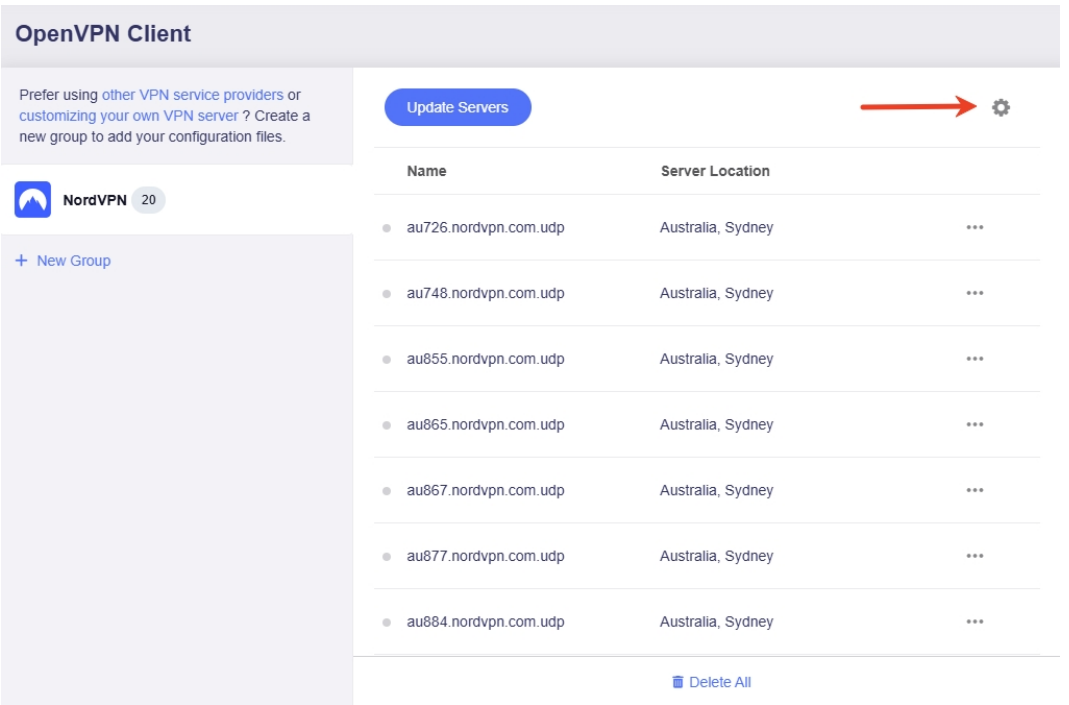
7. Aggiorna server.

   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.



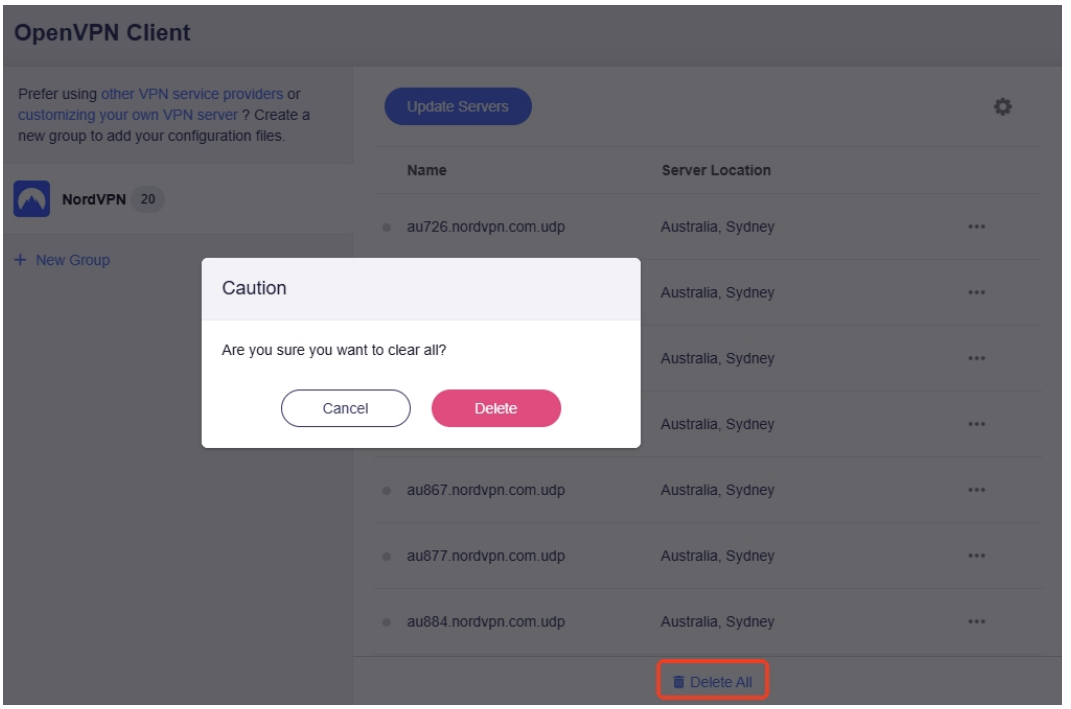
8. Modifica credenziali.

   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.

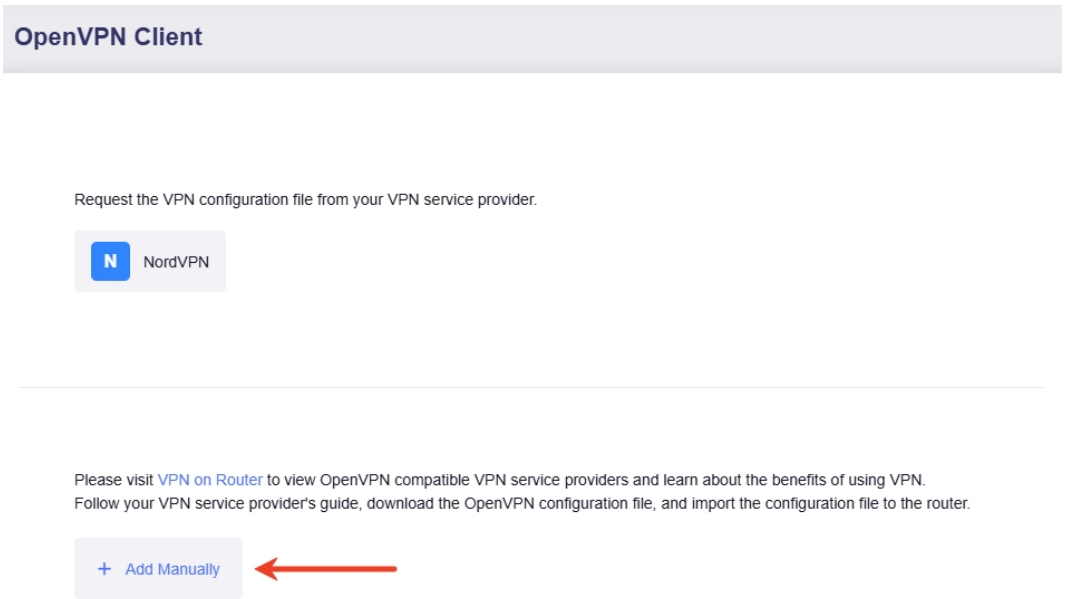

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

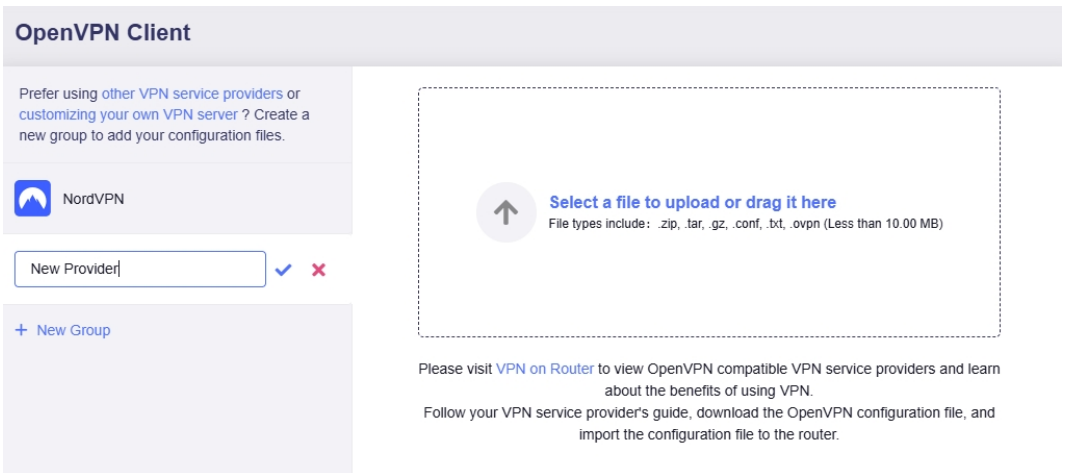
Se il tuo fornitore di servizi OpenVPN non è integrato nel nostro pannello di amministrazione, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare un client OpenVPN.

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

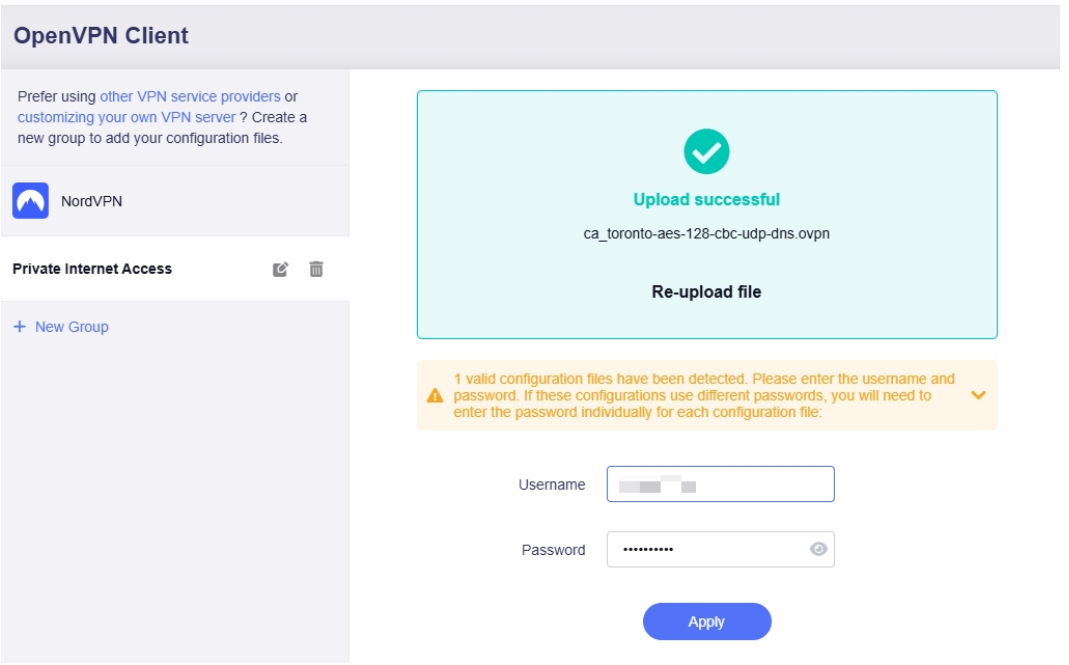
1. Scarica un file di configurazione dal sito Web ufficiale di Private Internet Access.
2. Accedi al pannello di amministrazione web del tuo router, vai a **VPN** > **Client OpenVPN** e fai clic su **Aggiungi manualmente**.



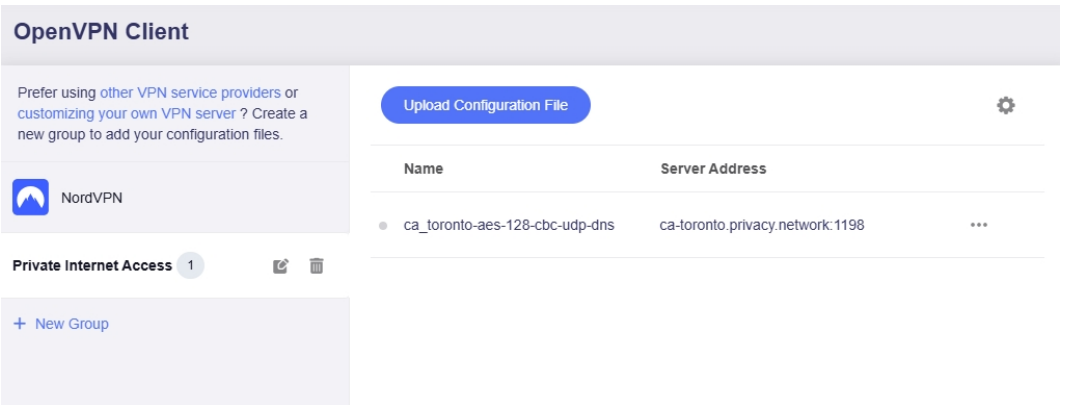
3. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.



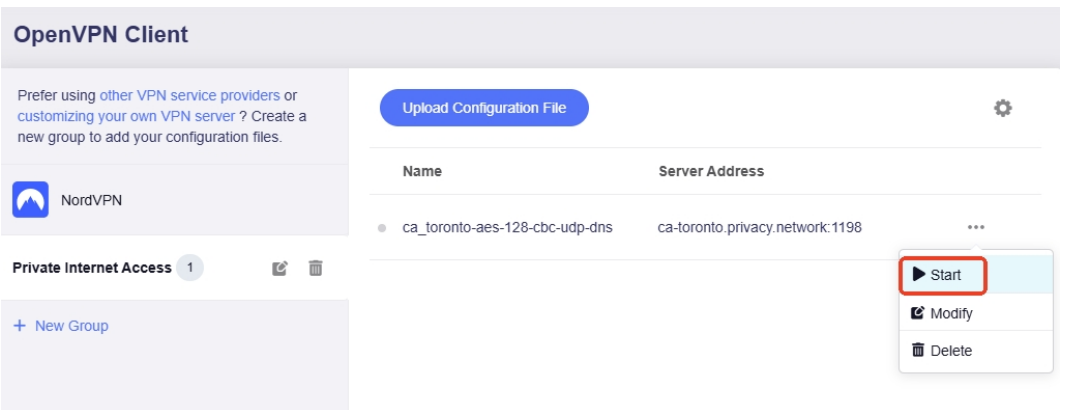
4. Carica il tuo file di configurazione OpenVPN. Inserisci le credenziali, se richieste, quindi fai clic su **Applica**.



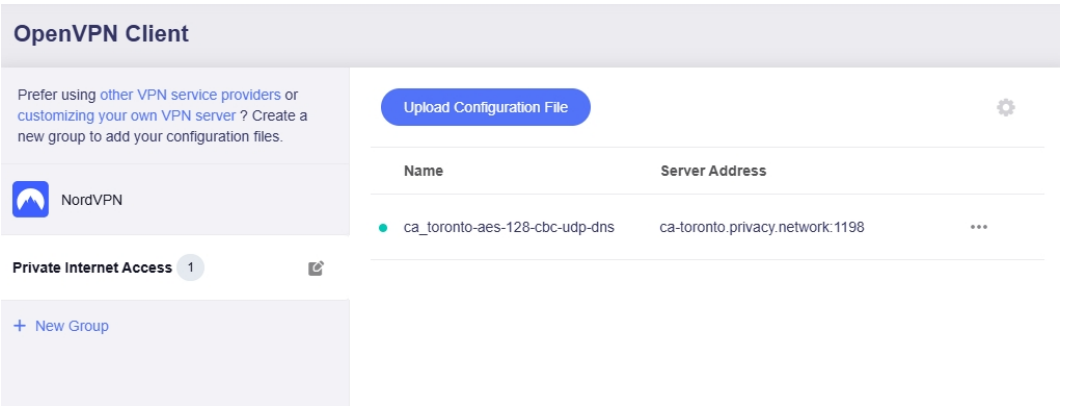
Vedrai il file di configurazione caricato.



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.

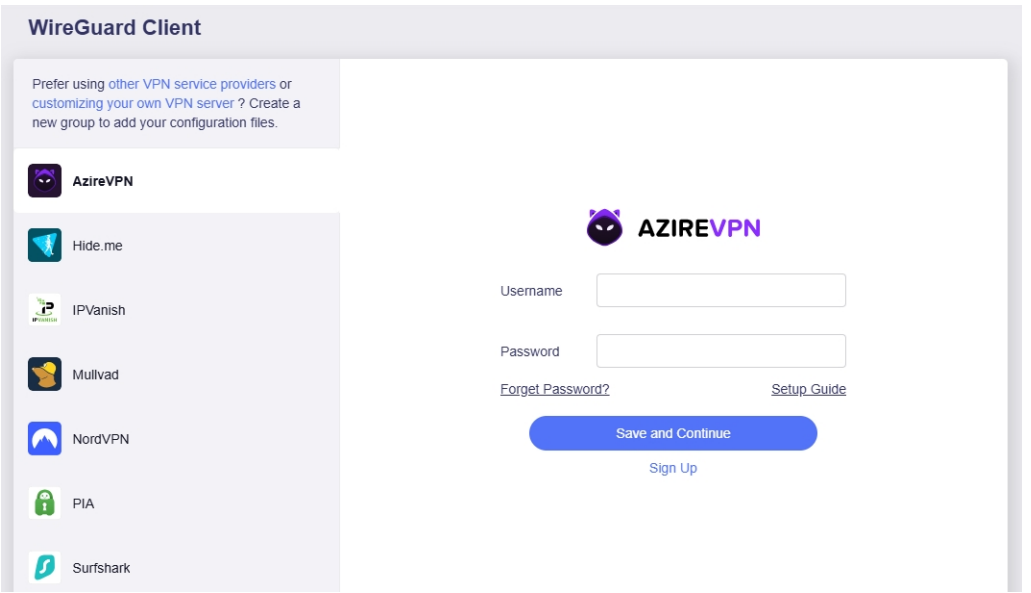
Successivamente, seleziona il fornitore di servizi WireGuard corrispondente di seguito per individuare rapidamente le istruzioni dettagliate.

- Configurazione di AzireVPN
- Configurazione di Hide.me
- Configurazione di IPVanish
- Configurazione di Mullvad
- Configurazione di NordVPN
- Configurazione di PIA (Private Internet Access)
- Configurazione di PureVPN
- Configurazione di Surfshark
- Configurazione di Windscribe
- Configurazione manuale del client WireGuard (altri provider)

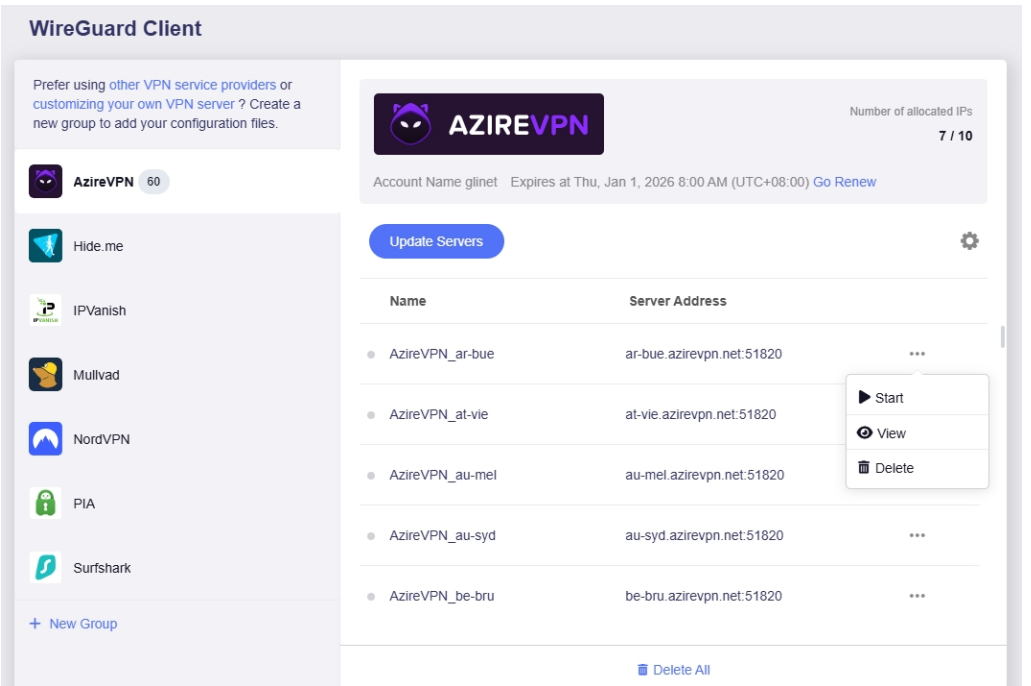
10.2.2 Configurazione di AzireVPN

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

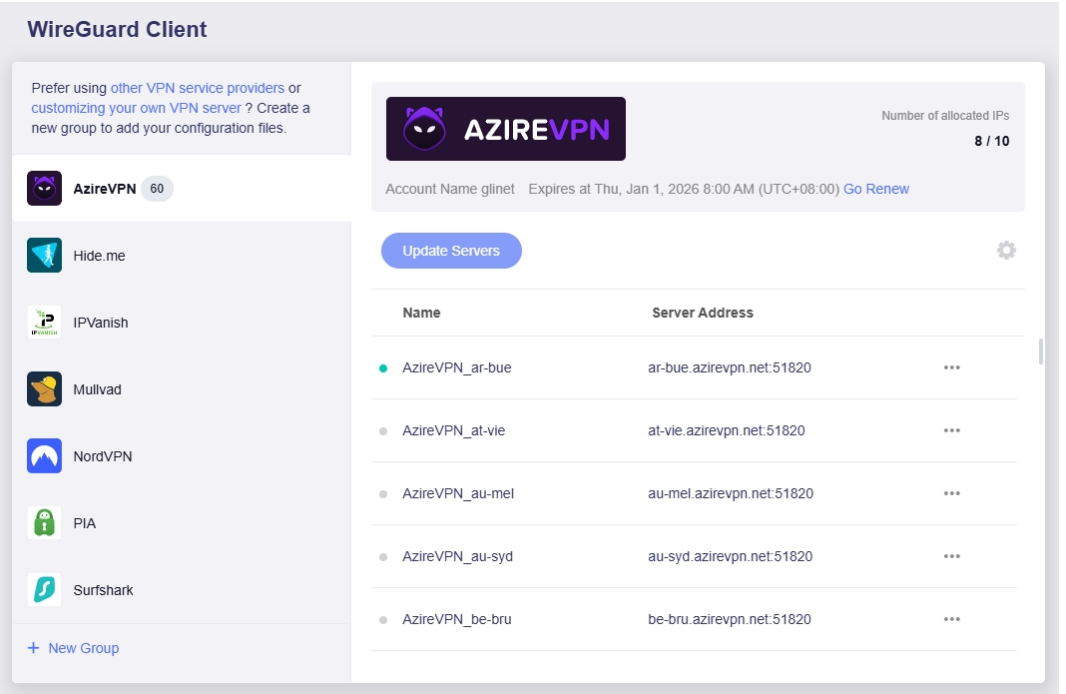
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **AzireVPN**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



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



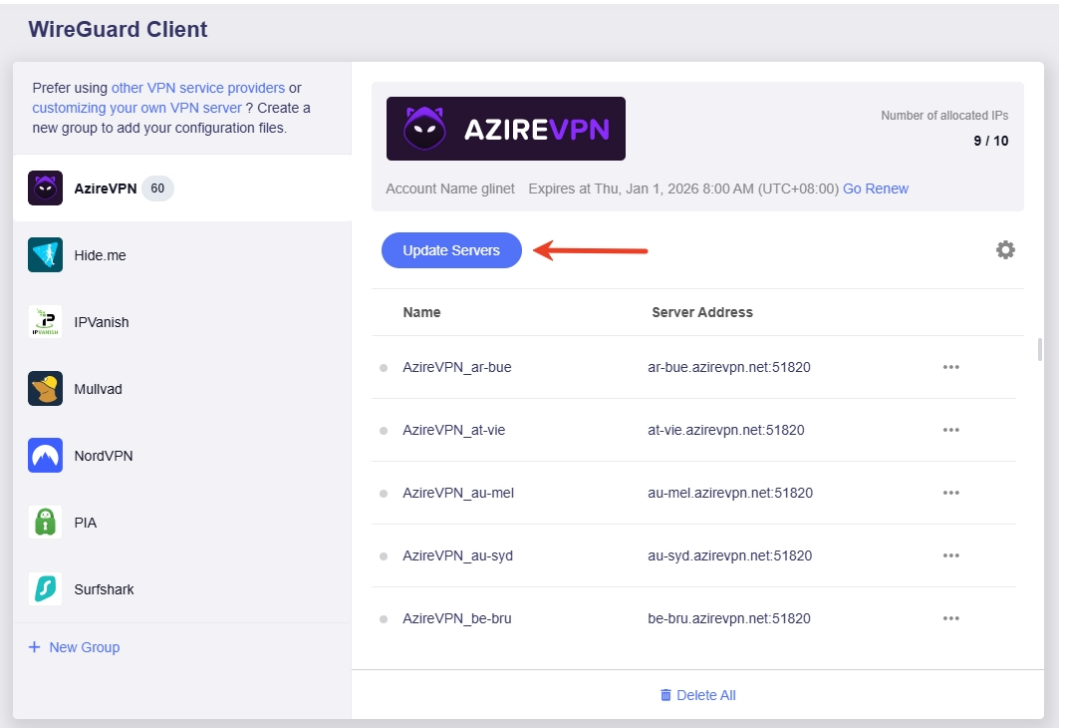
4. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

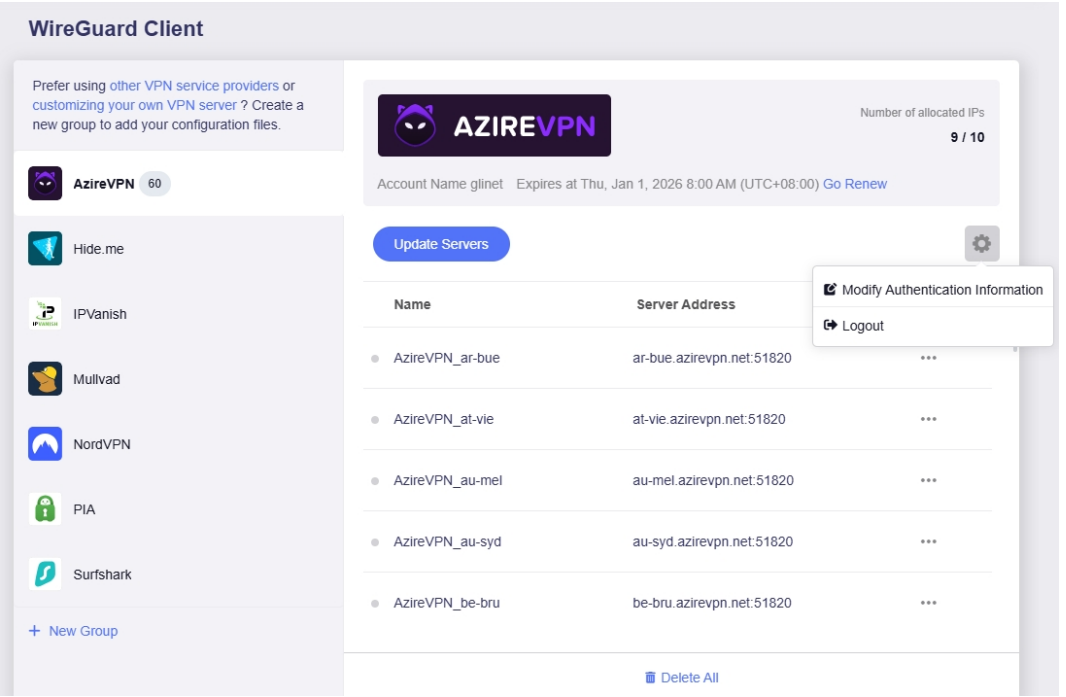
5. Aggiorna server.

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.



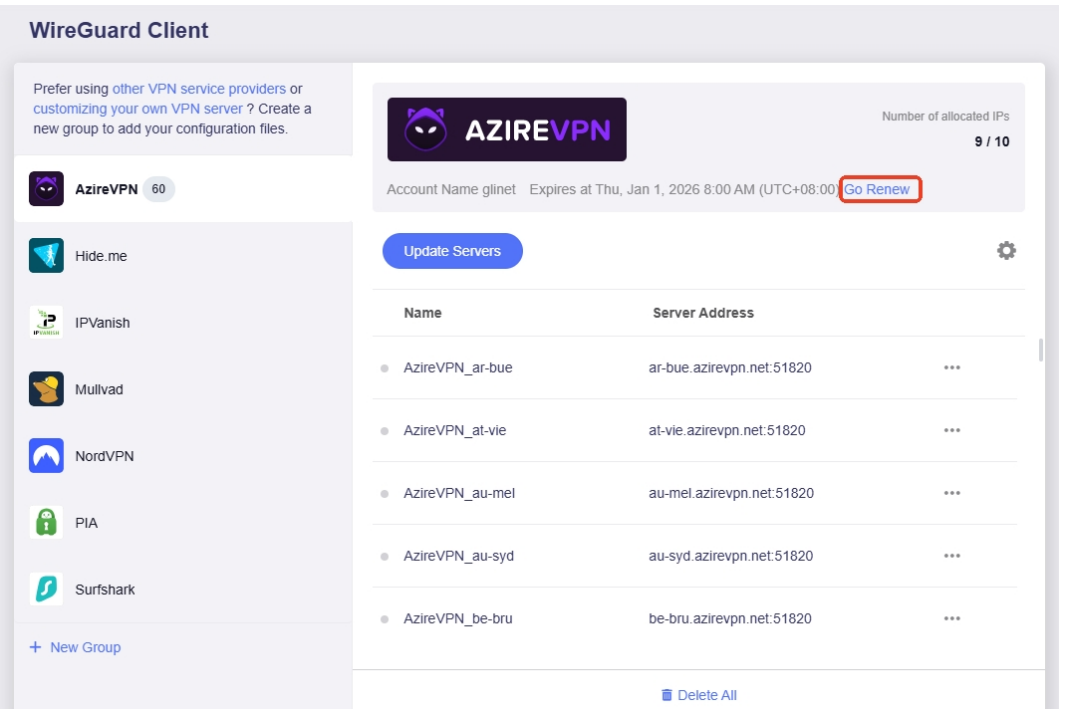
6. Modifica credenziali o esci.

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



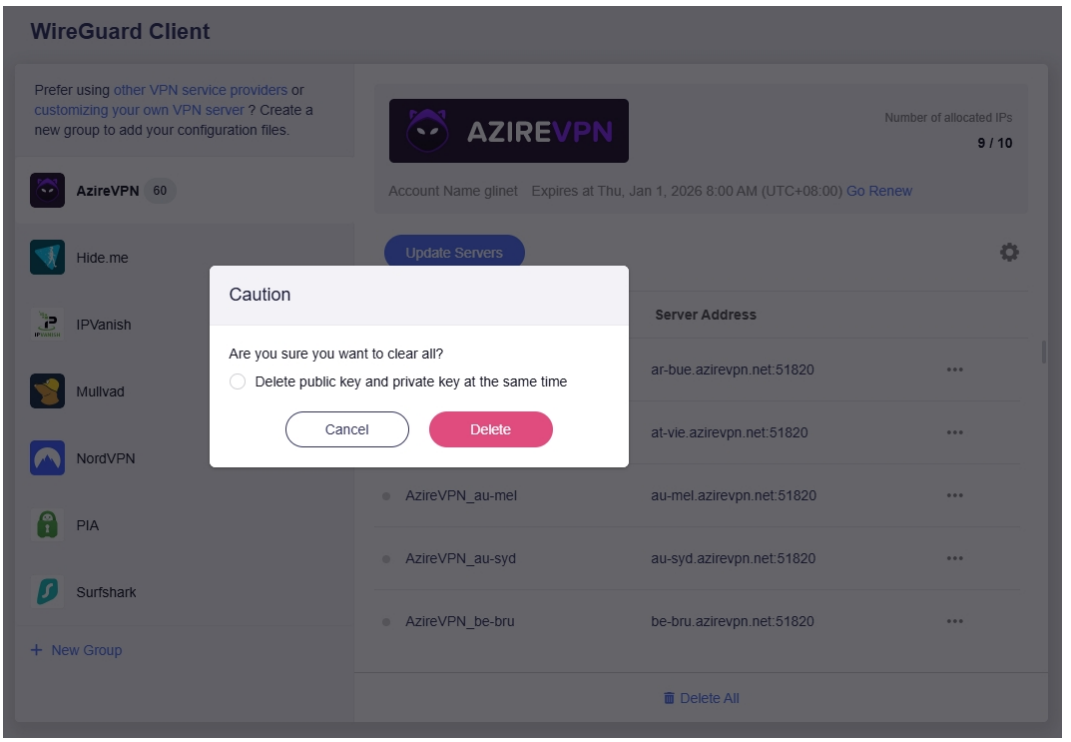
7. Rinnova.

   Se fai clic su **Rinnova**, verrai reindirizzato al sito Web ufficiale per rinnovare l'abbonamento.



8. Elimina tutti i file.

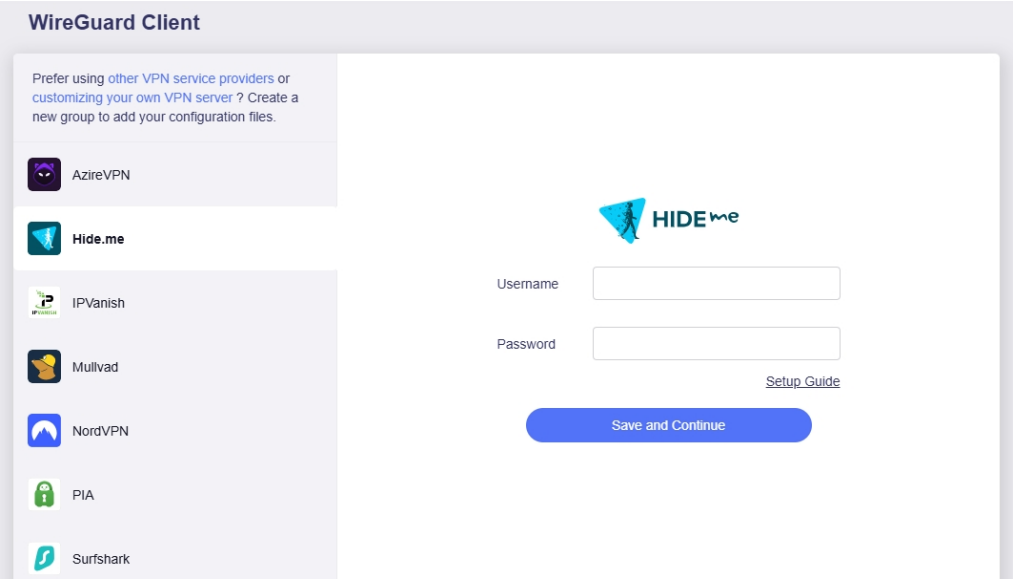
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



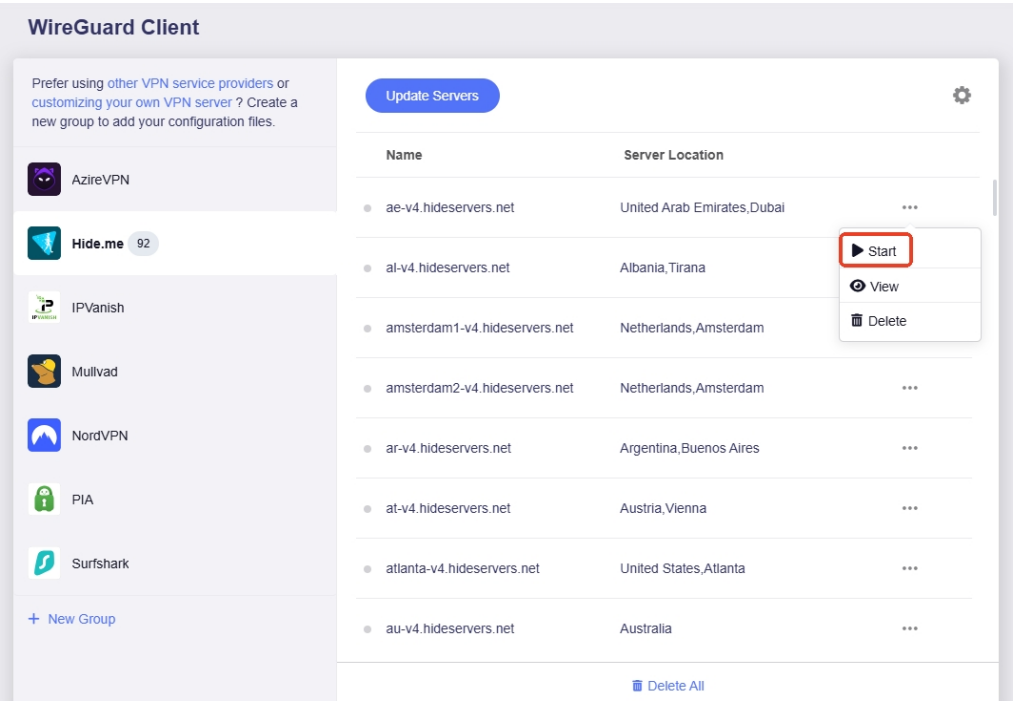
10.2.3 Configurazione di Hide.me

Segui i passaggi seguenti per impostare il router come client Hide.me.

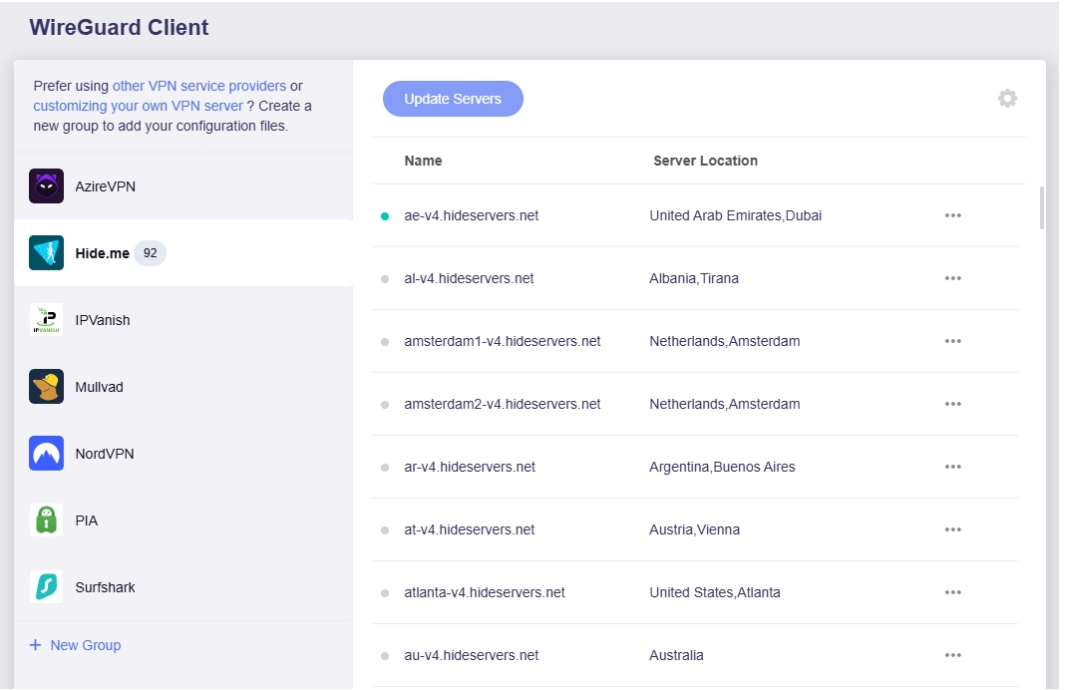
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Hide.me**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



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



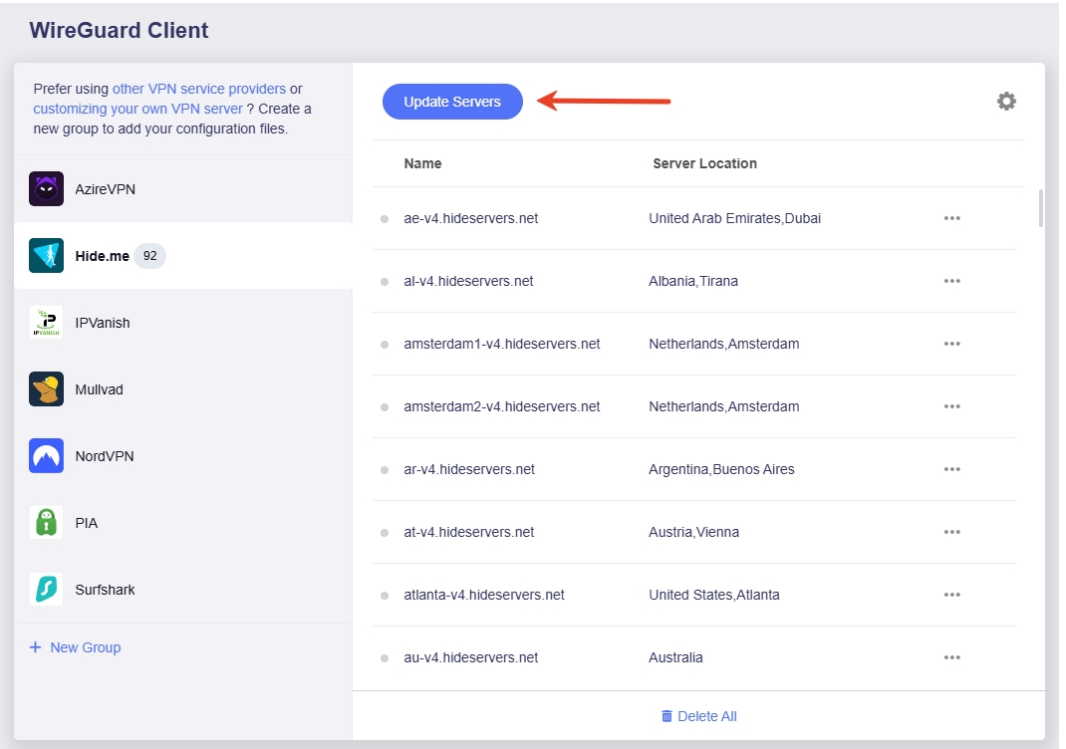
4. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

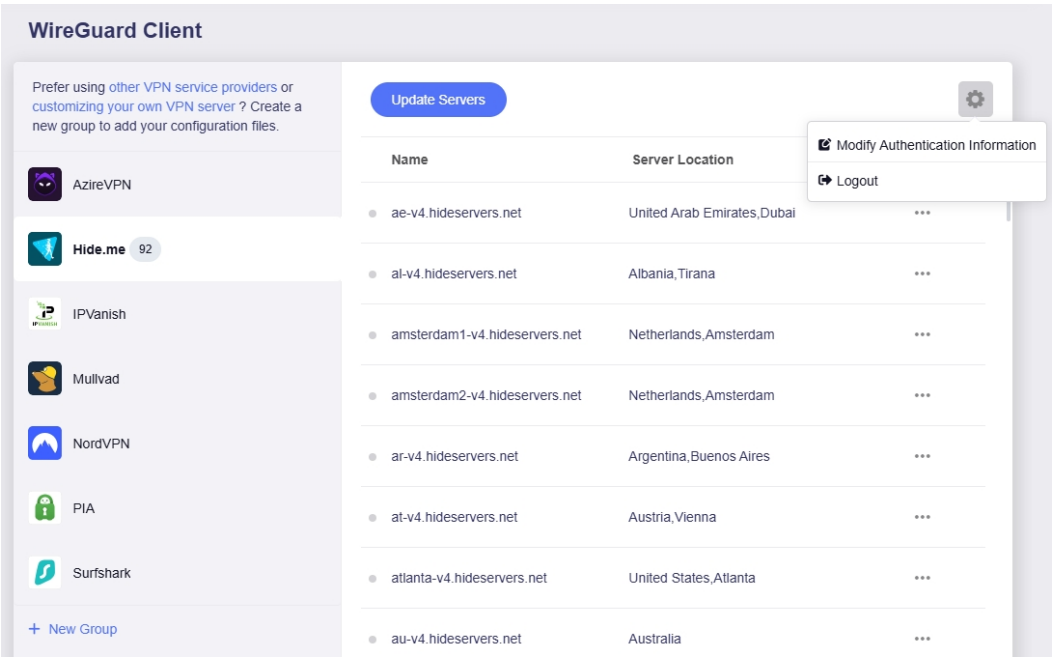
5. Aggiorna server.

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.



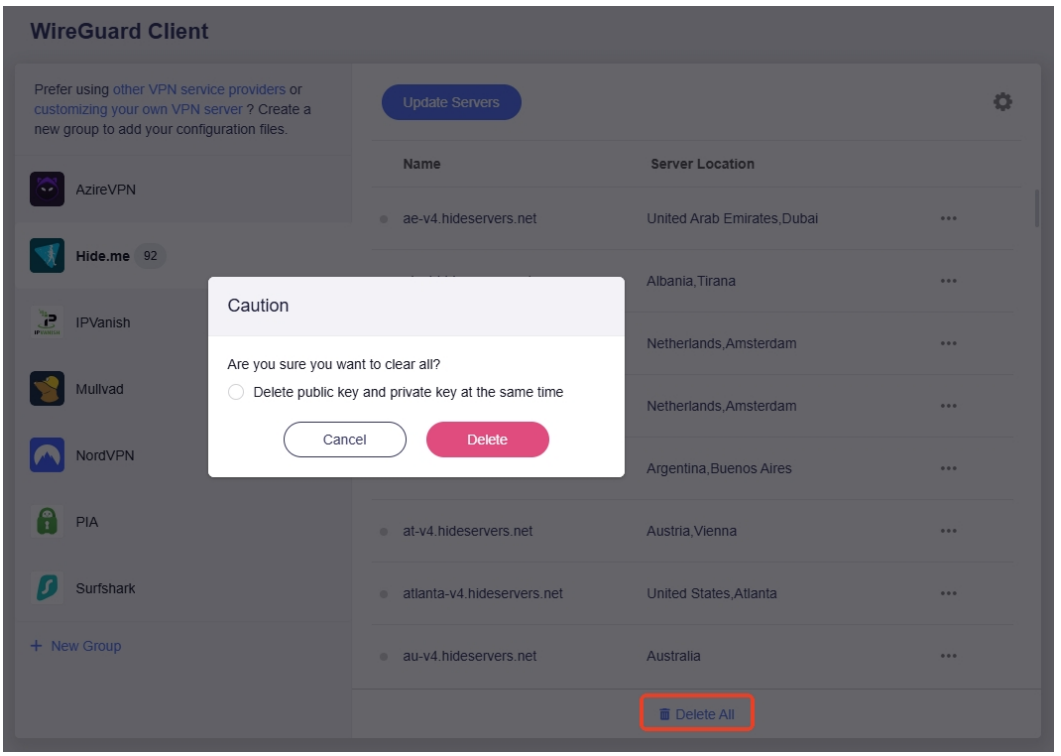
6. Modifica credenziali o esci.

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



7. Elimina tutti i file.

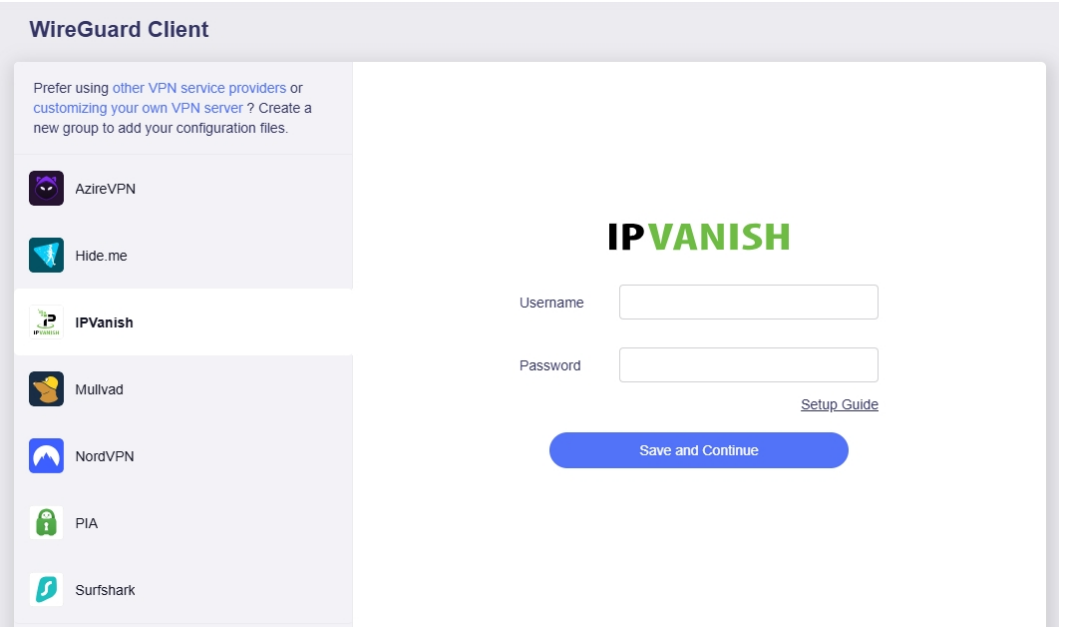
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



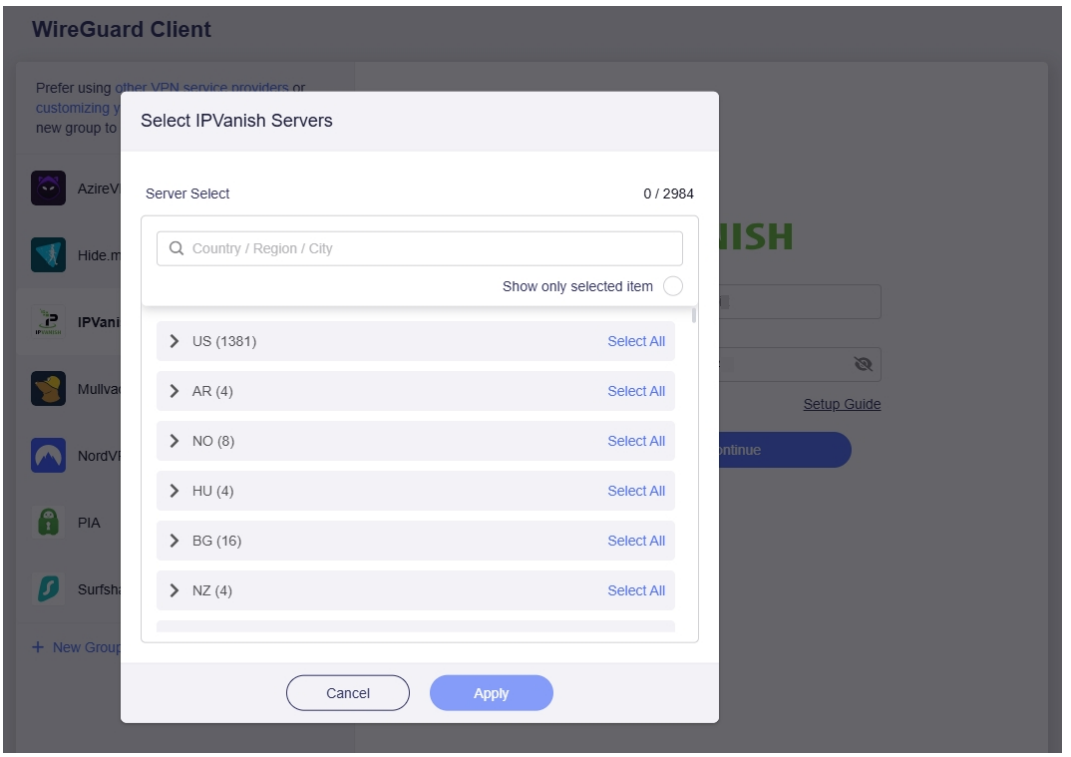
10.2.4 Configurazione di IPVanish

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

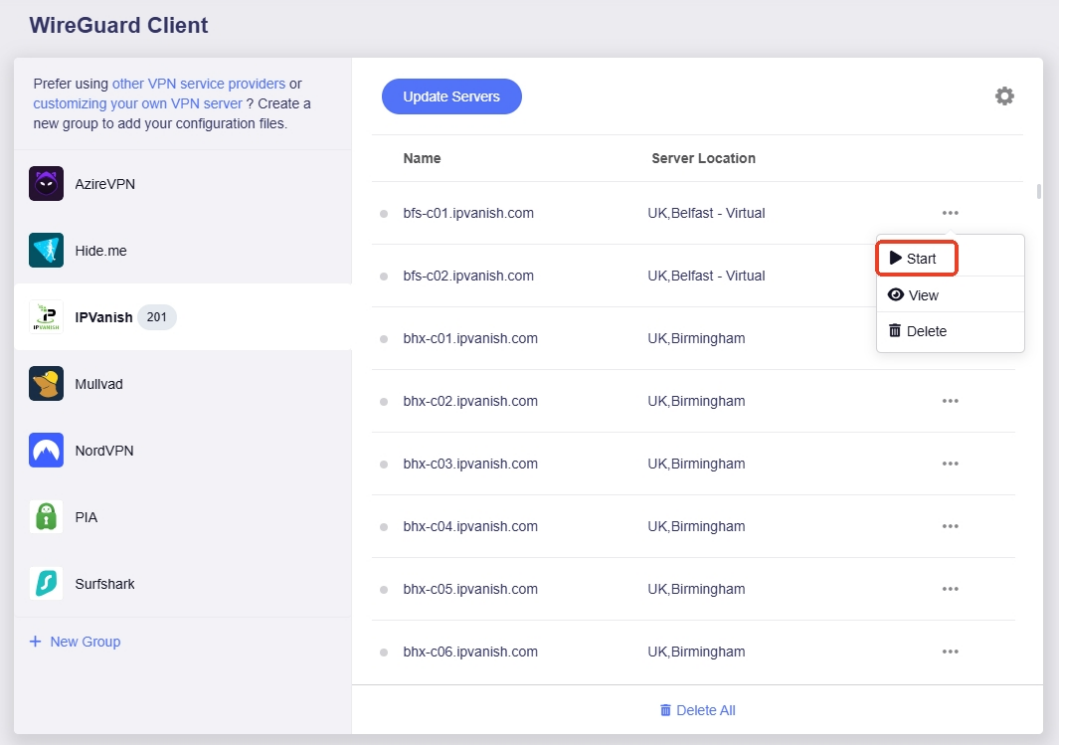
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **IPVanish**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



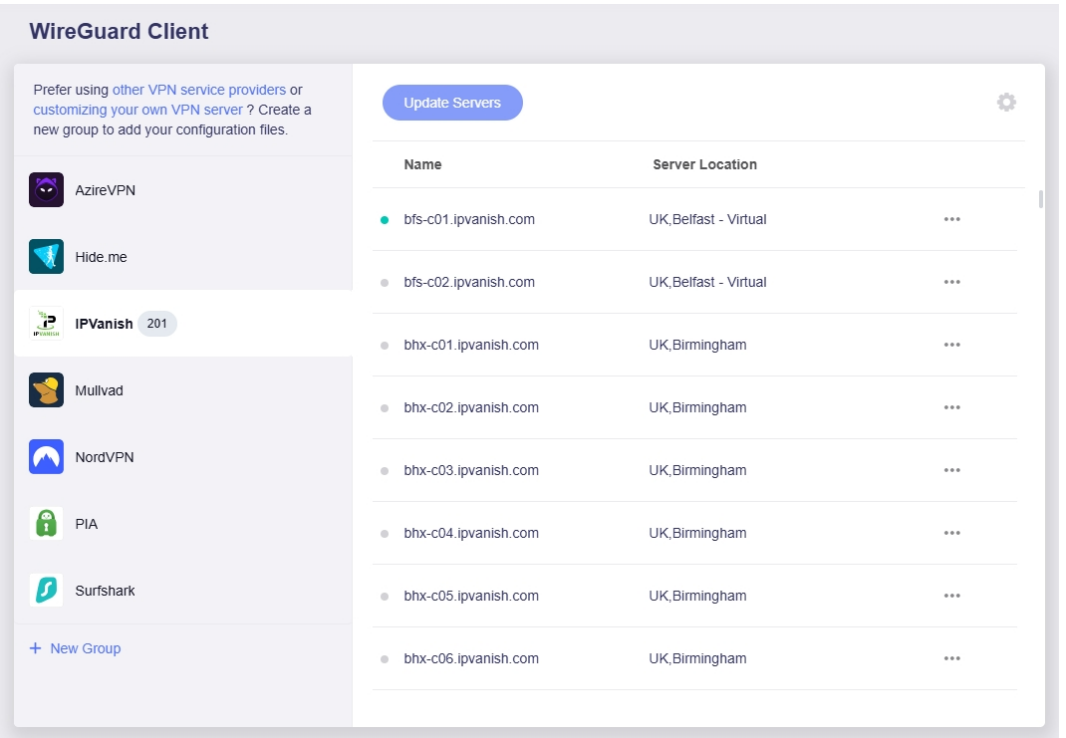
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



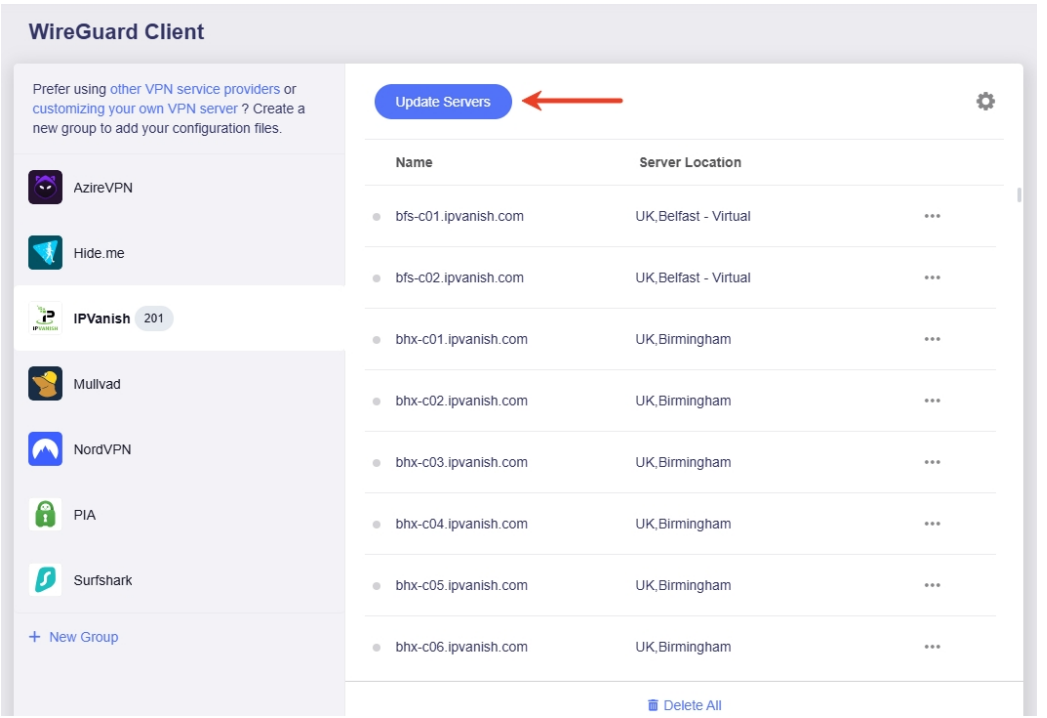
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

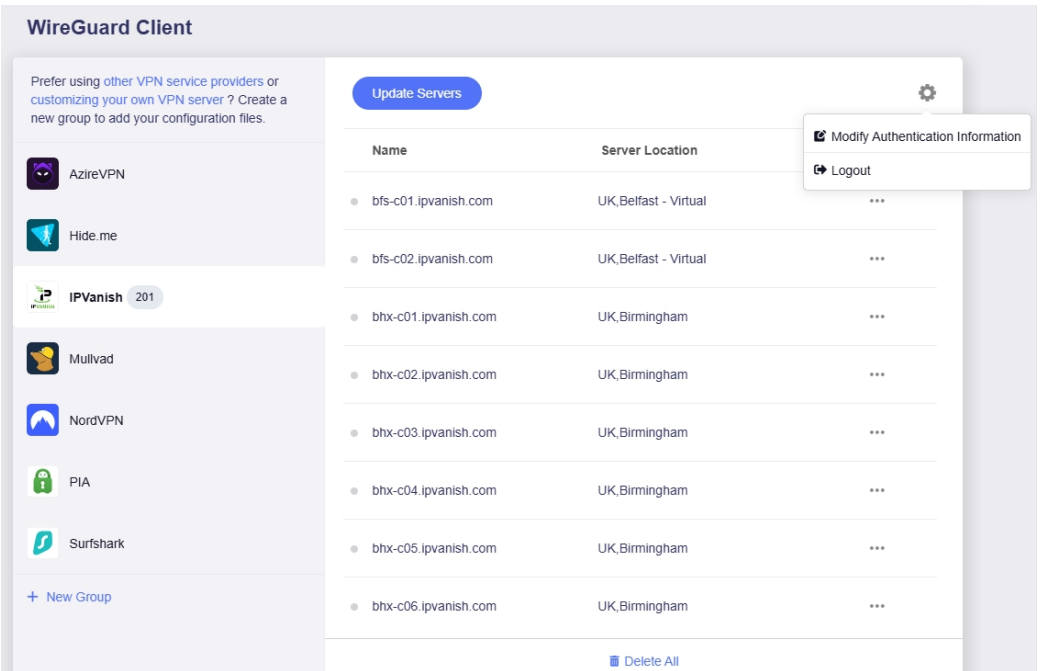
6. Aggiorna server.

   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.



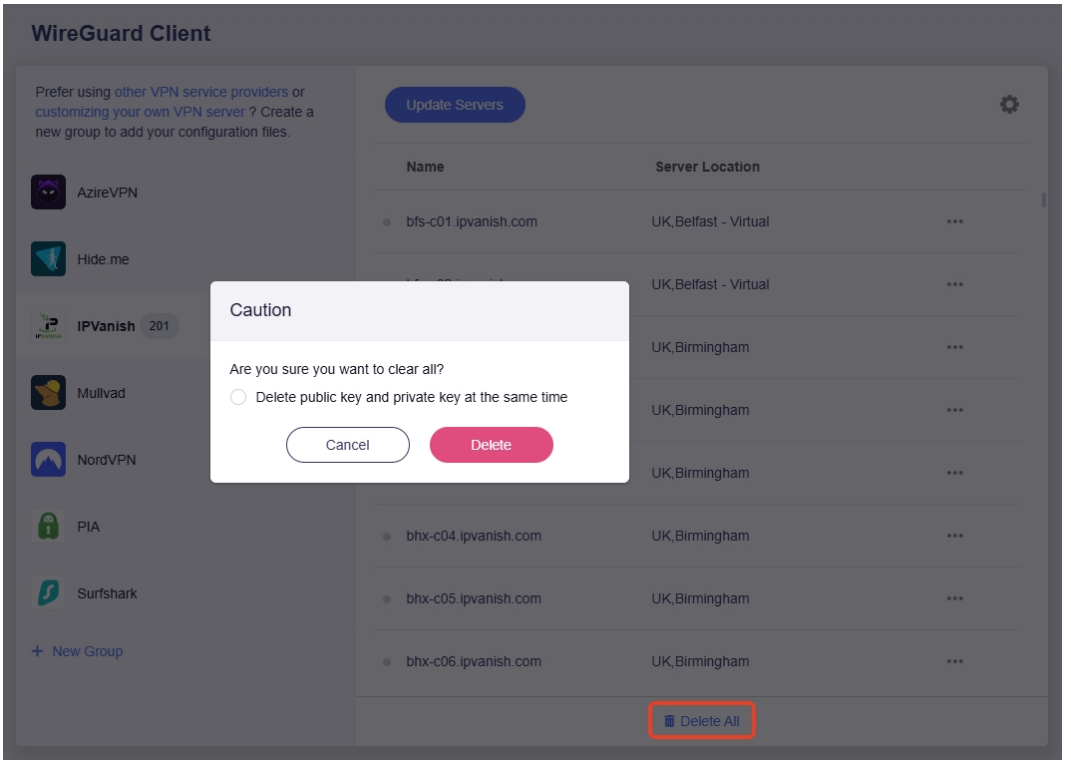
7. Modifica credenziali o esci.

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



8. Elimina tutti i file.

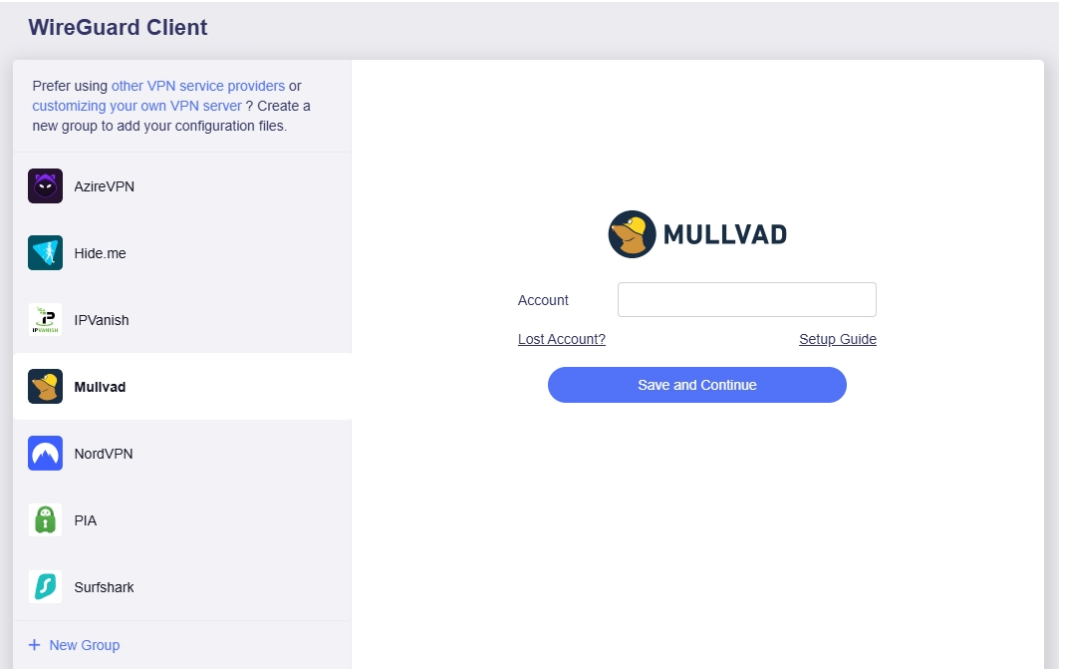
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



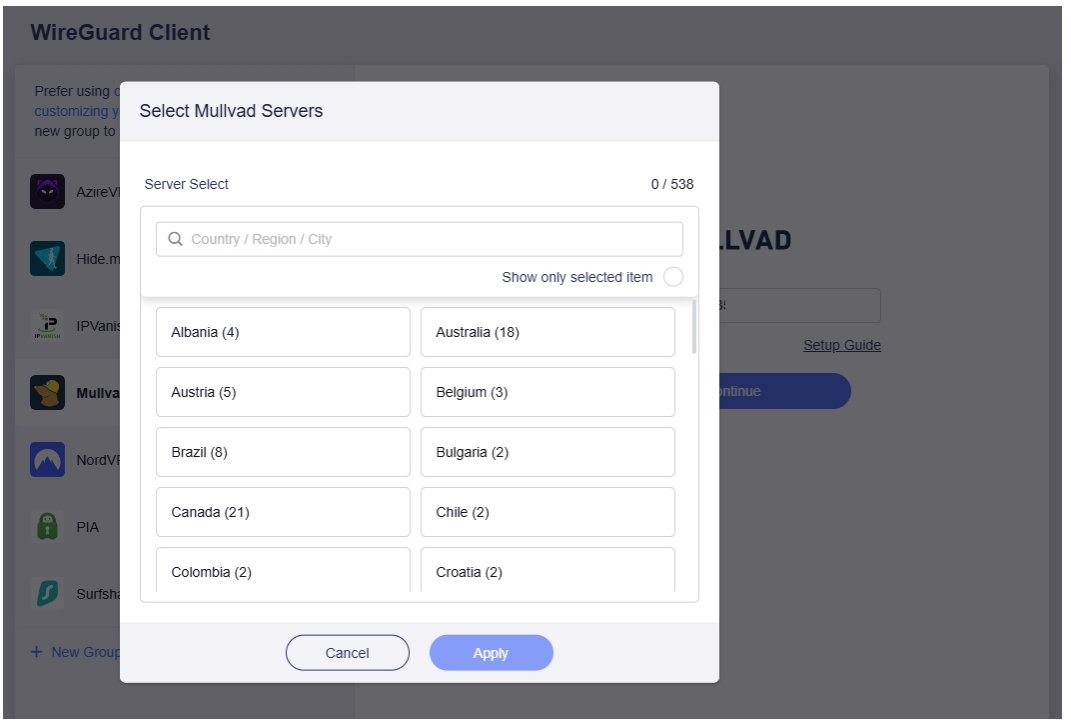
10.2.5 Configurazione di Mullvad

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

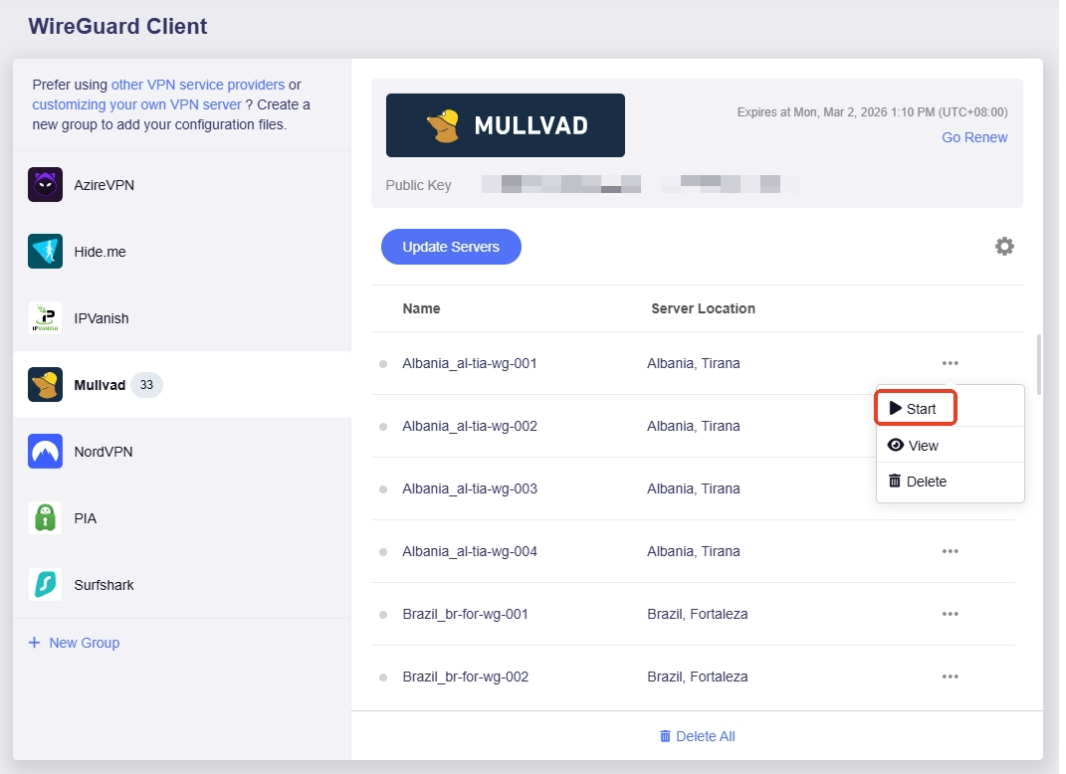
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Mullvad**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



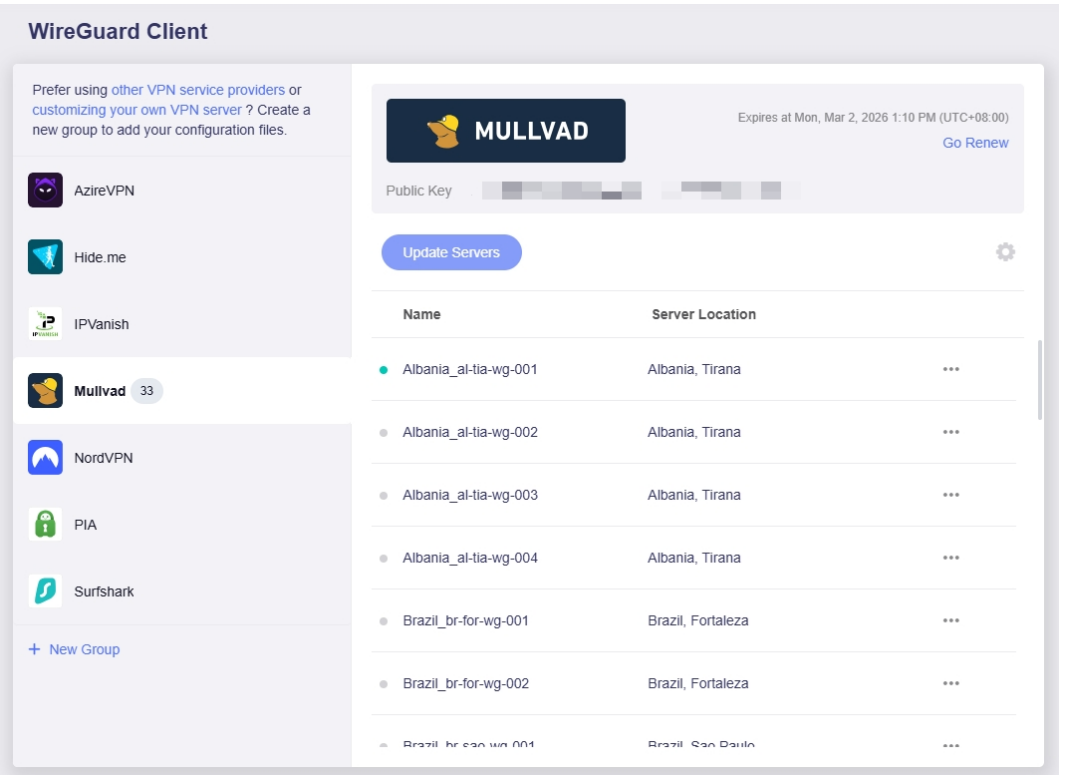
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



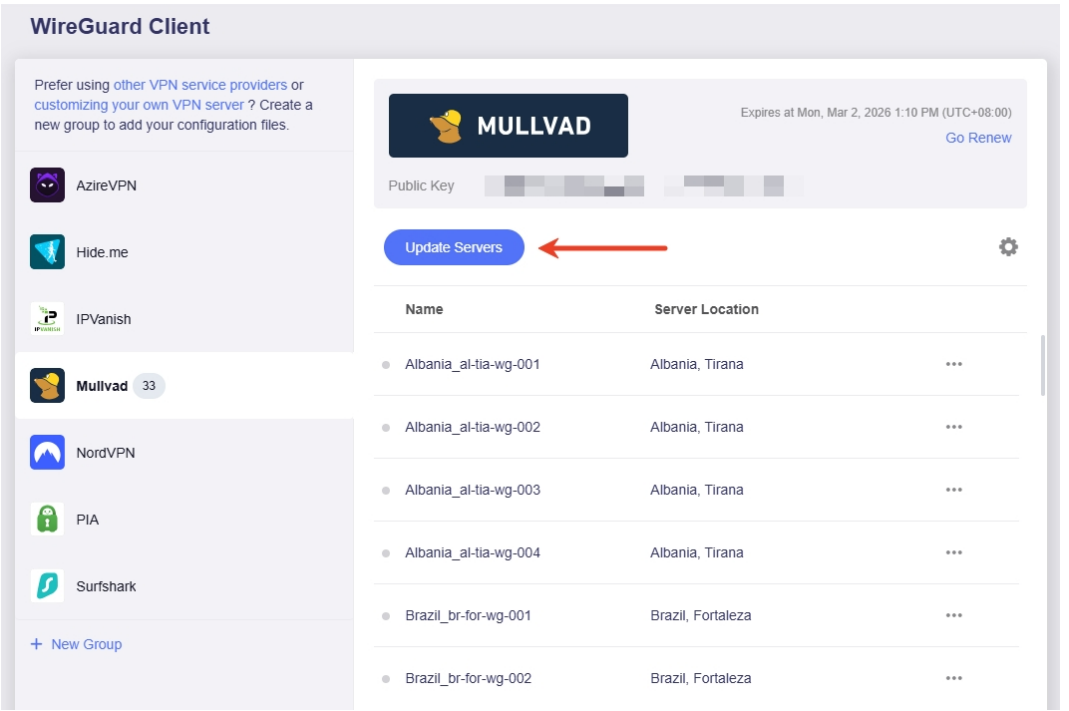
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

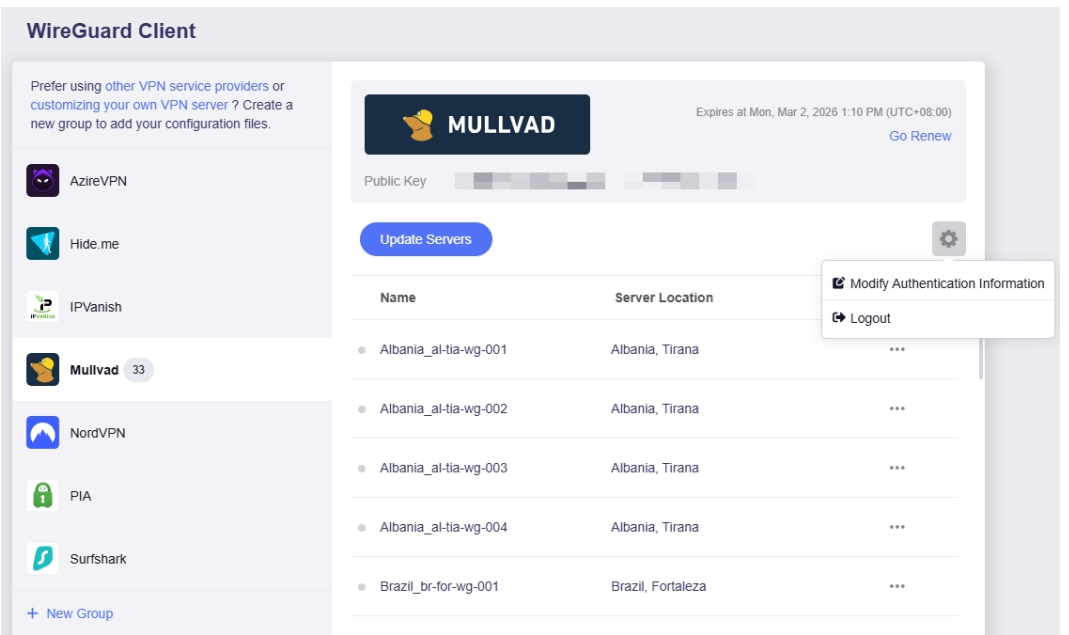
6. Aggiorna server.

   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.



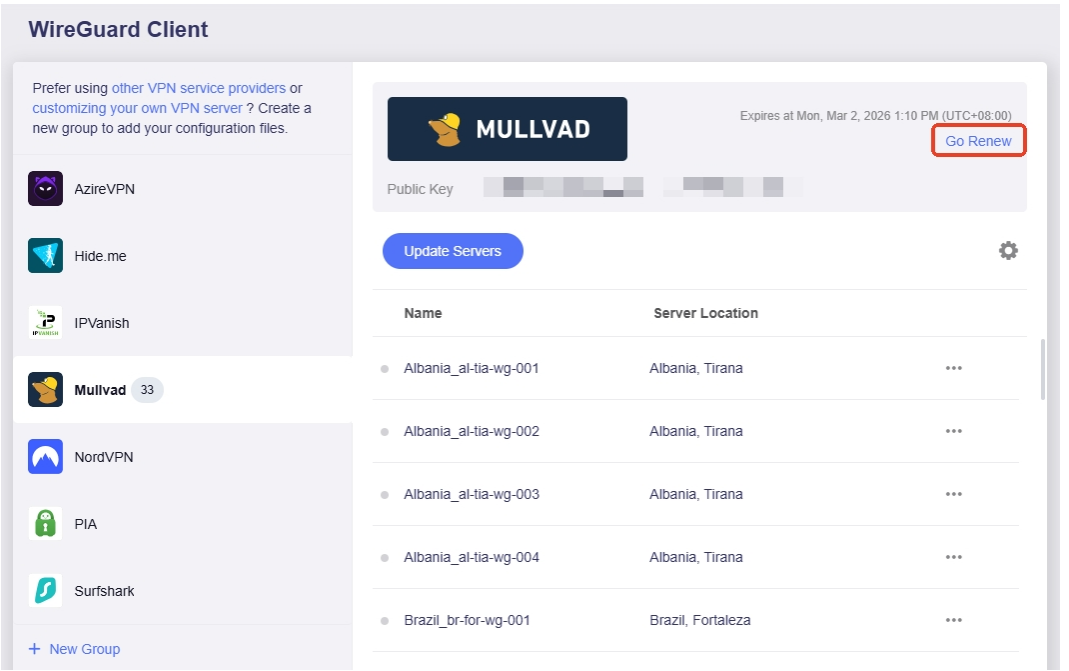
7. Modifica credenziali o esci.

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



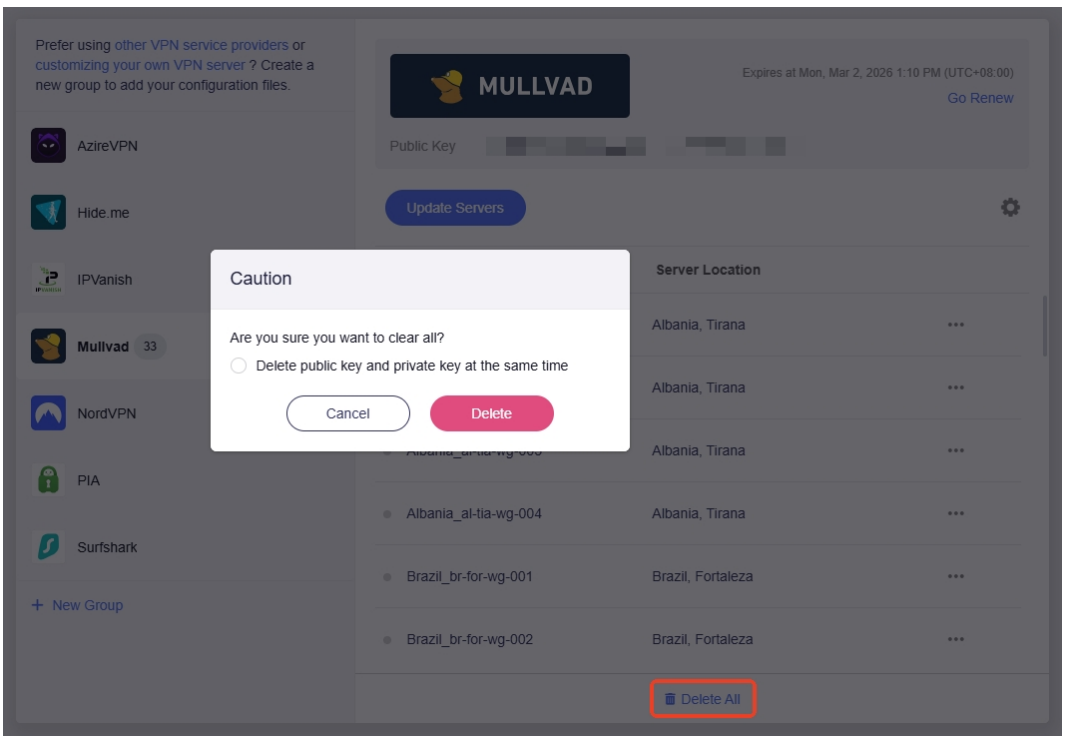
8. Rinnova.

   Se fai clic su **Rinnova**, verrai reindirizzato al sito Web ufficiale per rinnovare l'abbonamento.



9. Elimina tutti i file.

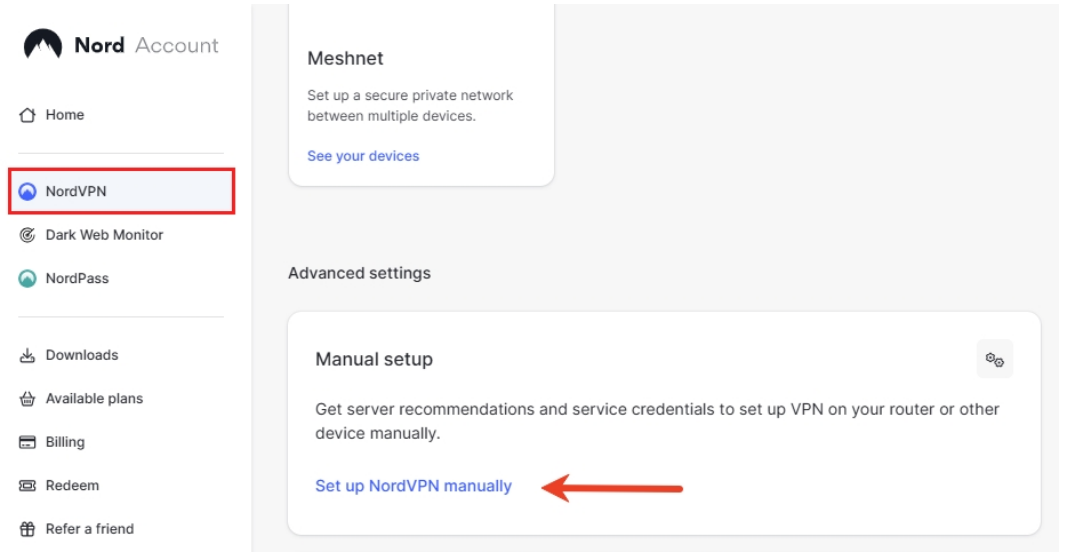
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



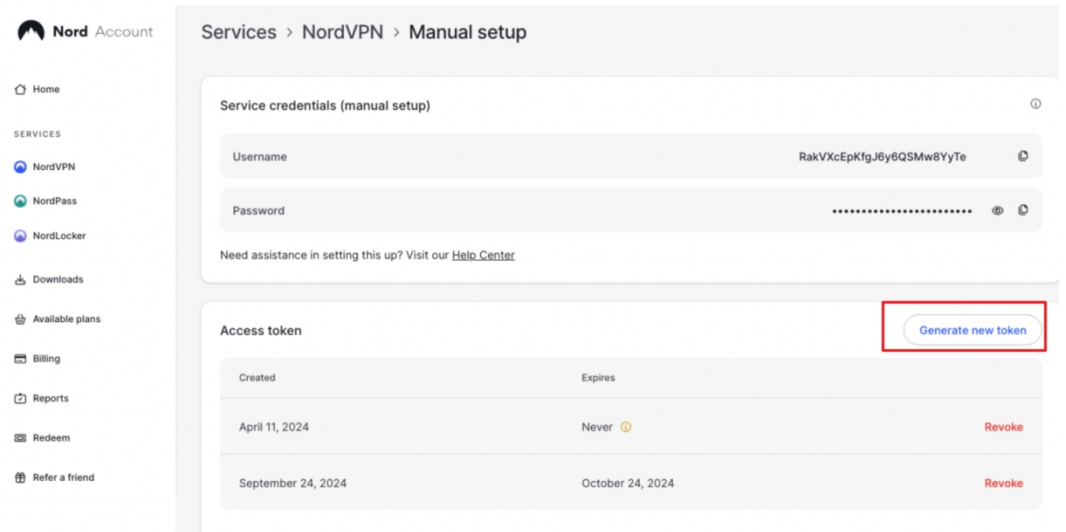
10.2.6 Configurazione di NordVPN

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

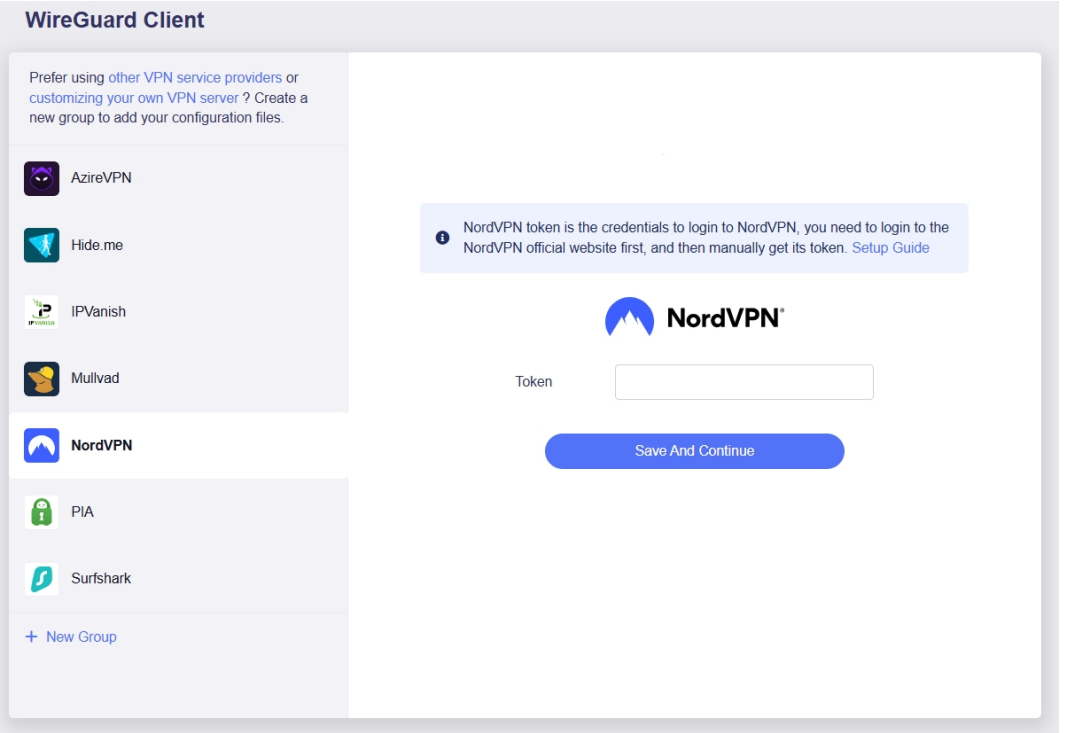
1. Accedi al tuo account web NordVPN qui.
2. Nella Nord Dashboard, fai clic su **NordVPN**, quindi su **Configura NordVPN manualmente**.



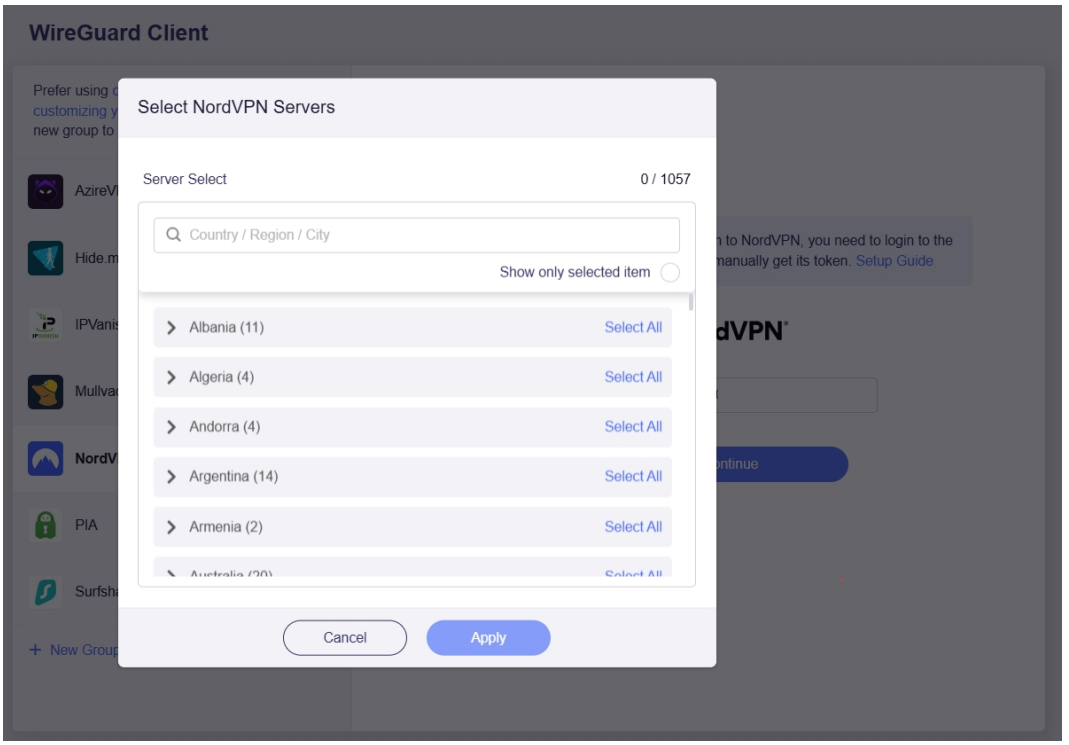
Troverai il **Token di accesso**. Crea un token di accesso e copialo per un uso successivo.



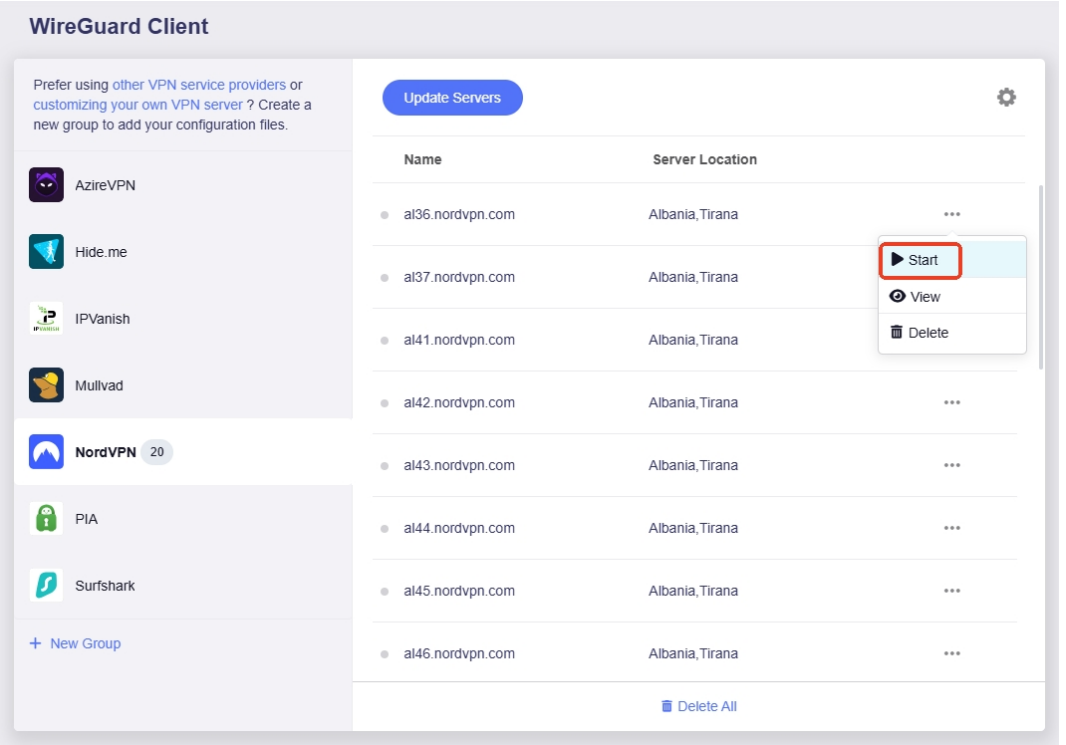
3. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **NordVPN**.
4. Inserisci il token e fai clic su **Salva e continua**.



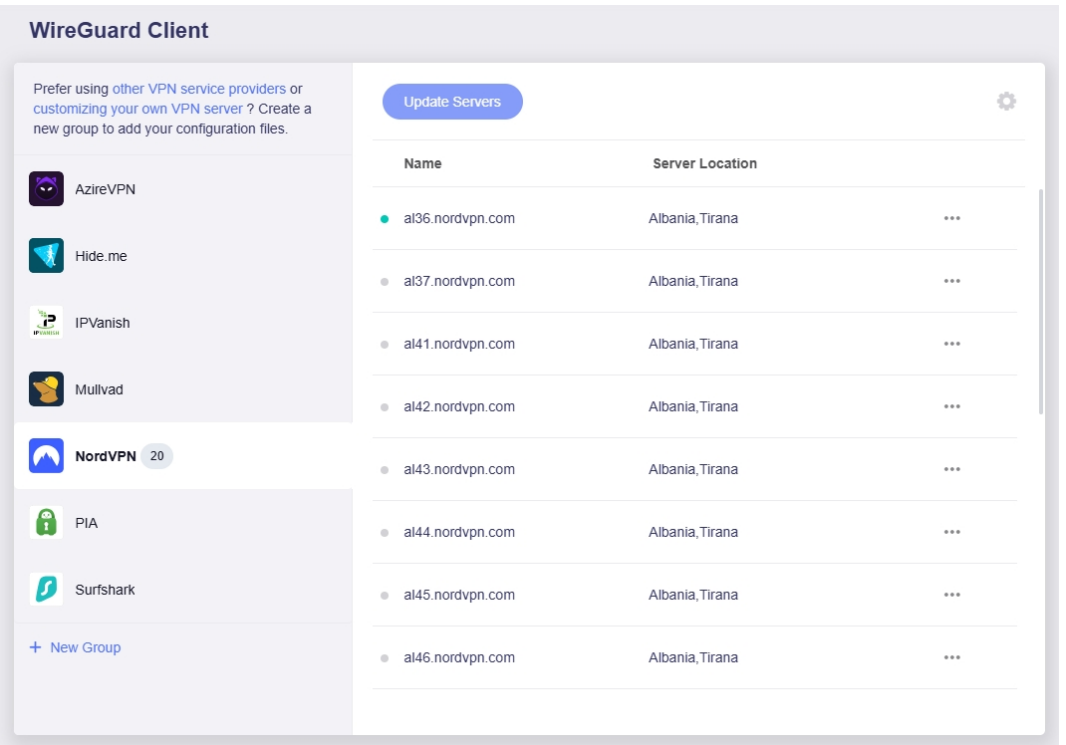
5. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



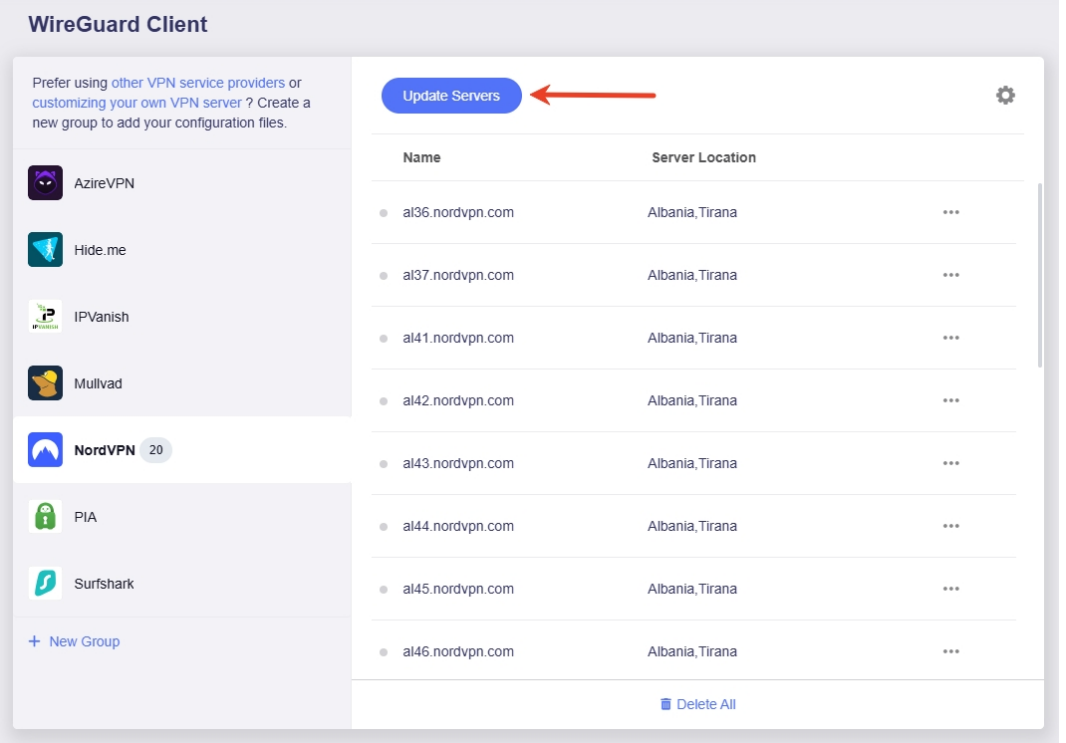
7. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



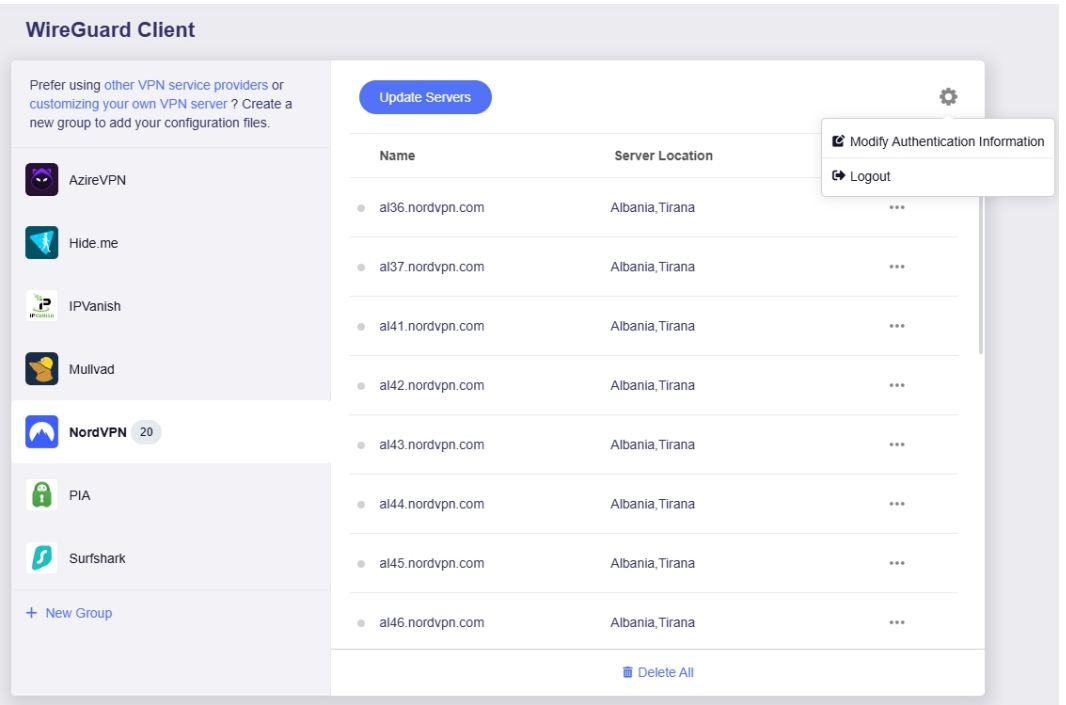
Puoi anche controllare i dettagli della connessione VPN sulla **dashboard VPN**.

8. 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.

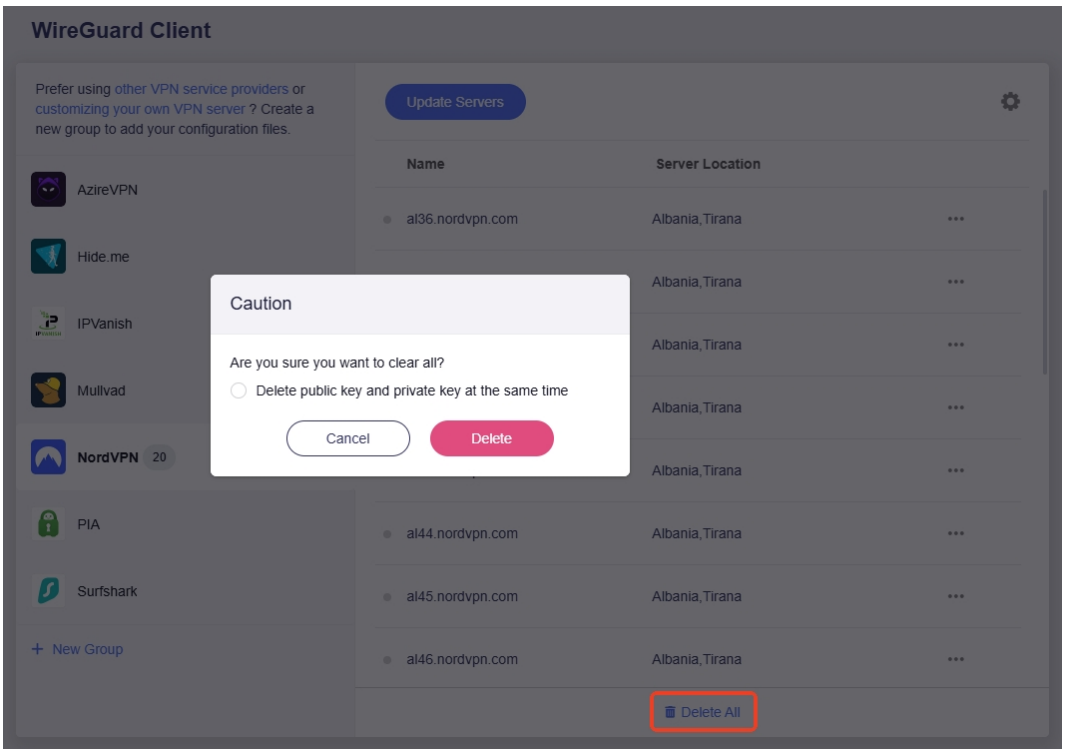


9. Modifica credenziali o esci.
   Fai clic sull'icona a forma di ingranaggio per modificare le tue credenziali di accesso o disconnetterti.



10. Elimina tutti i file.

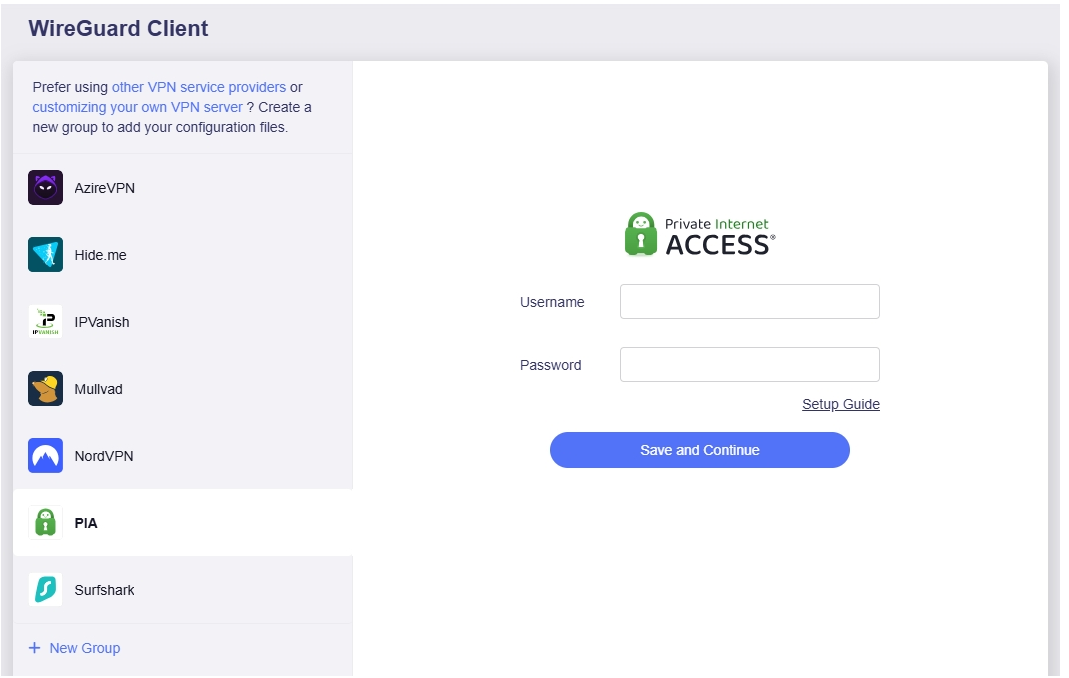
    Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



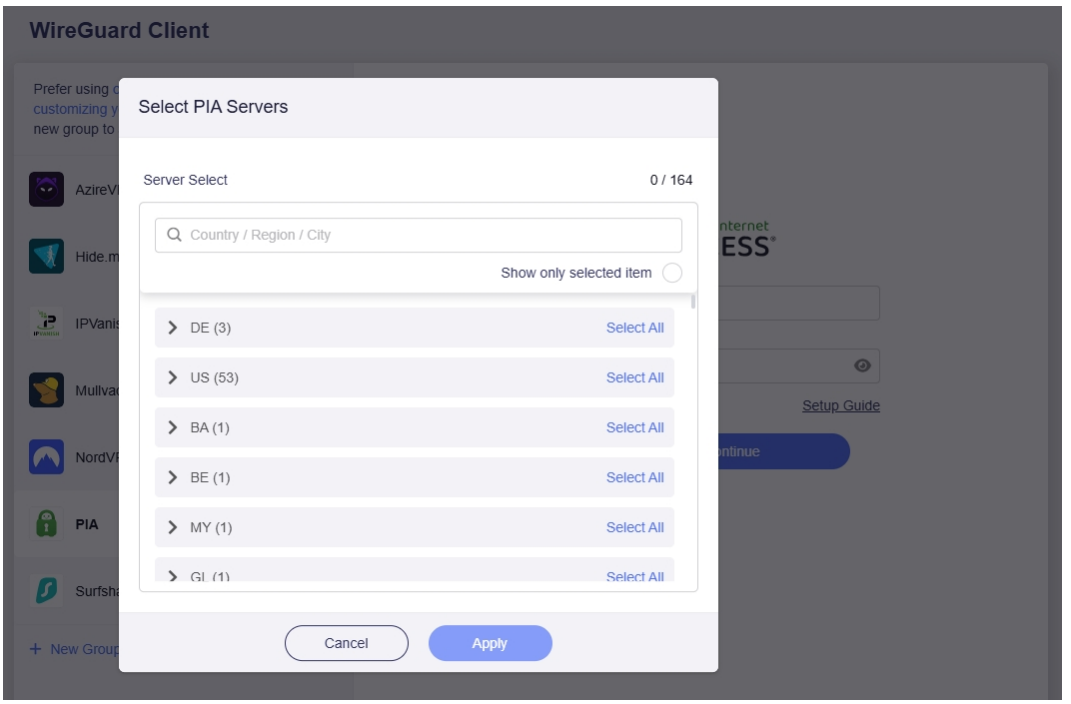
10.2.7 Configurazione di PIA (Private Internet Access)

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

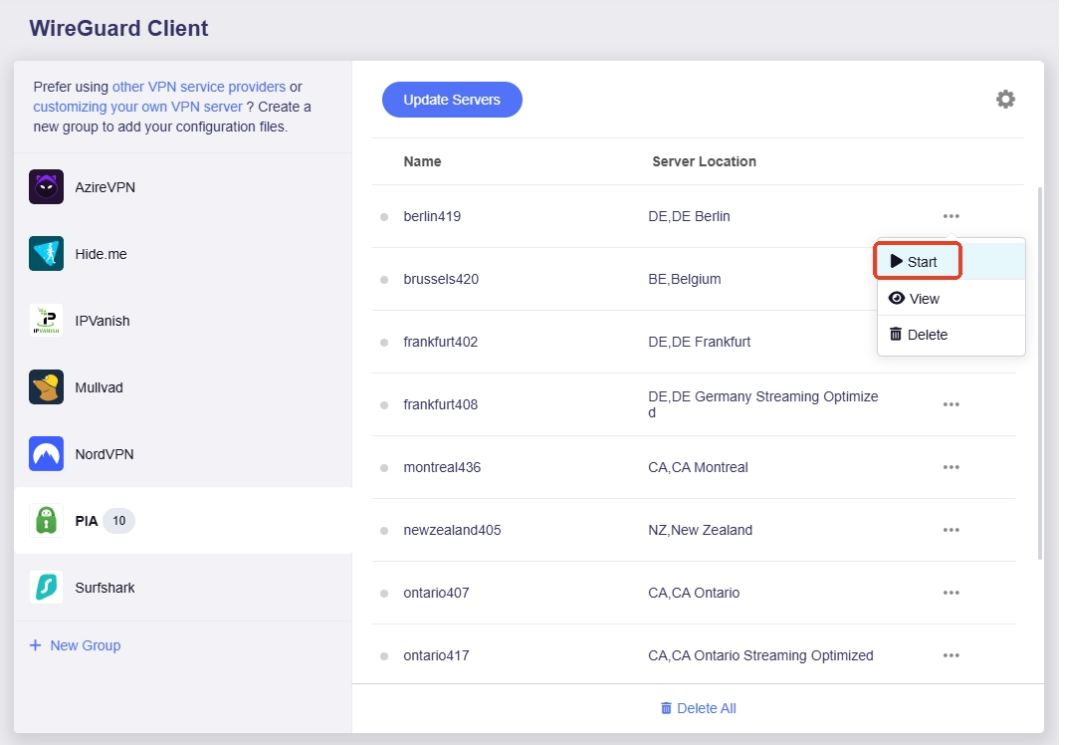
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **PIA**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



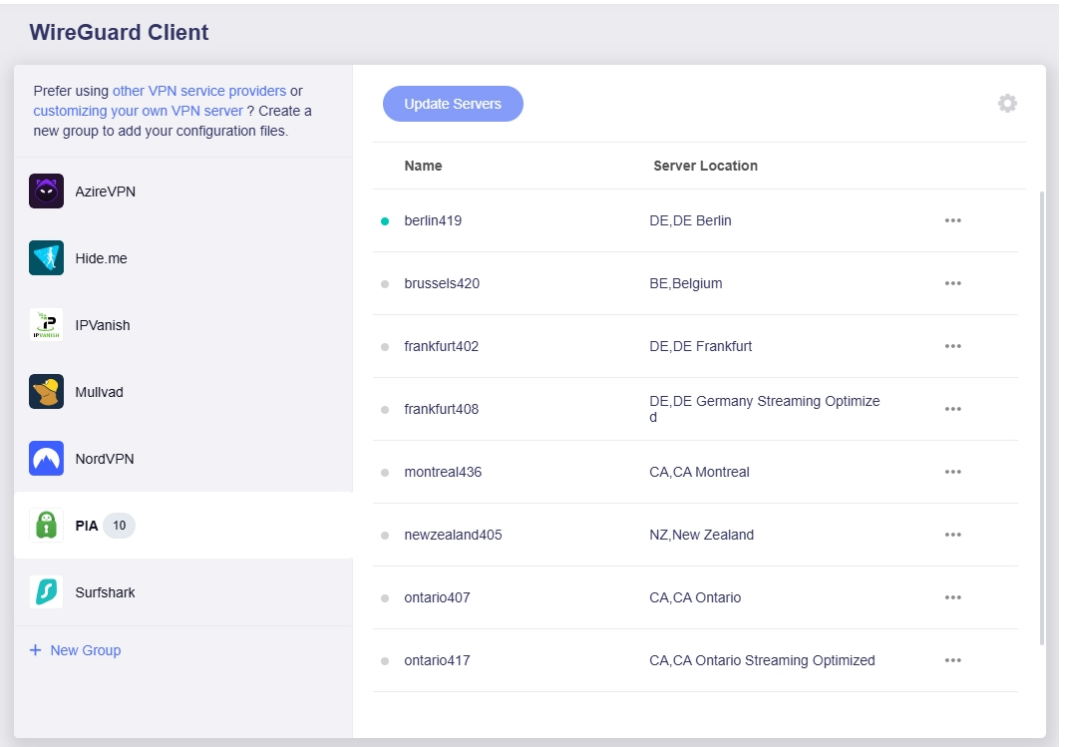
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



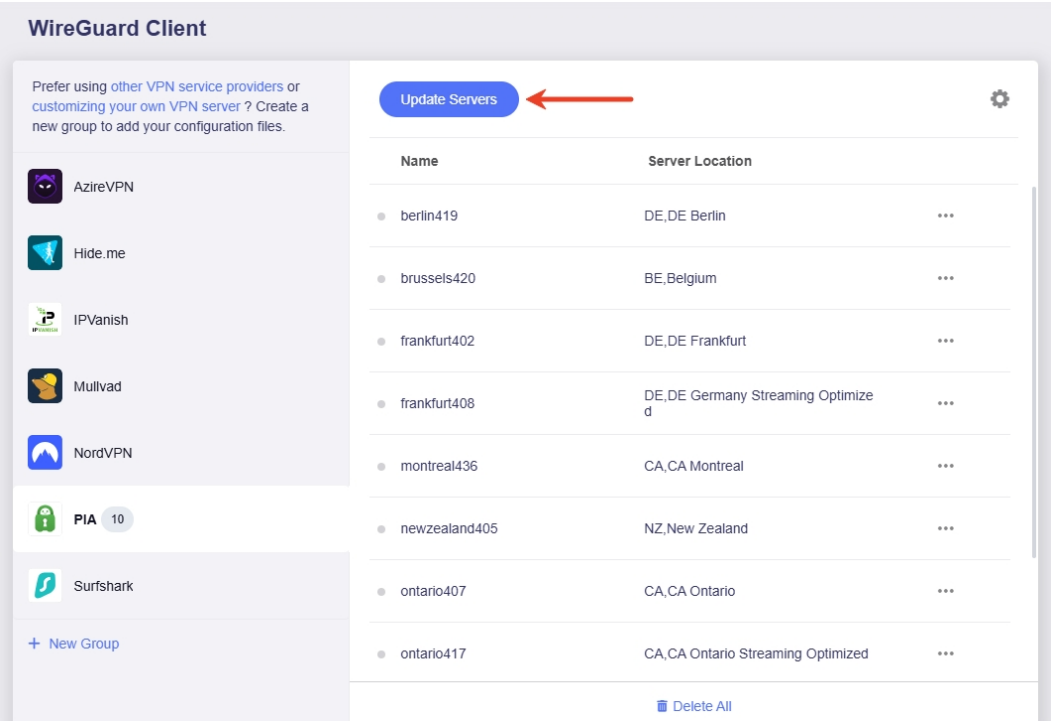
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

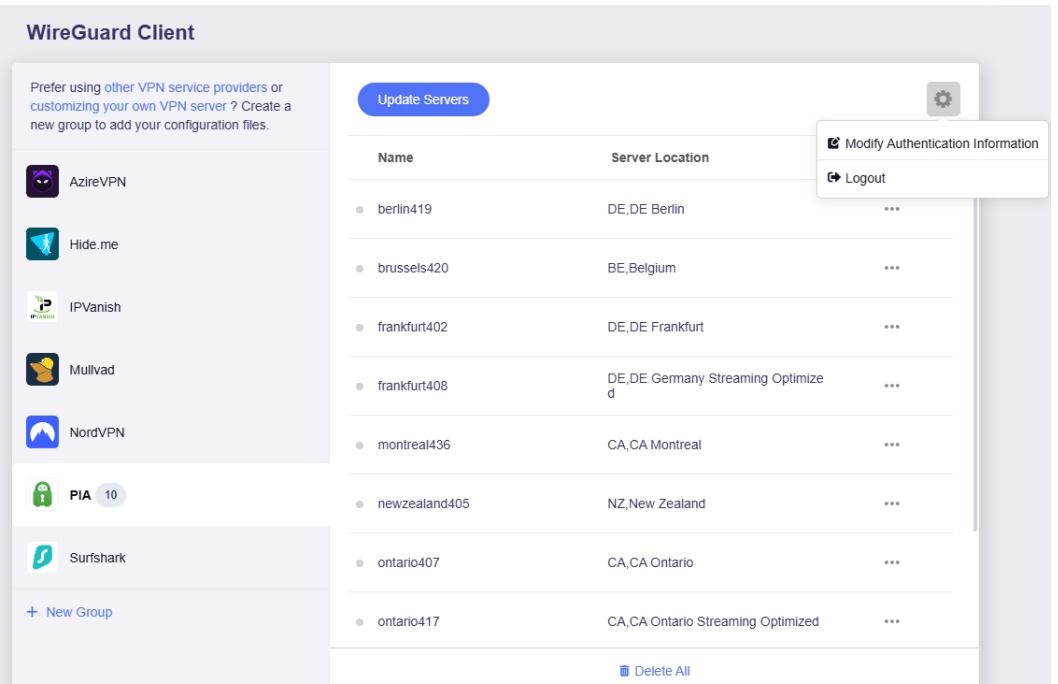
6. Aggiorna server.

   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.



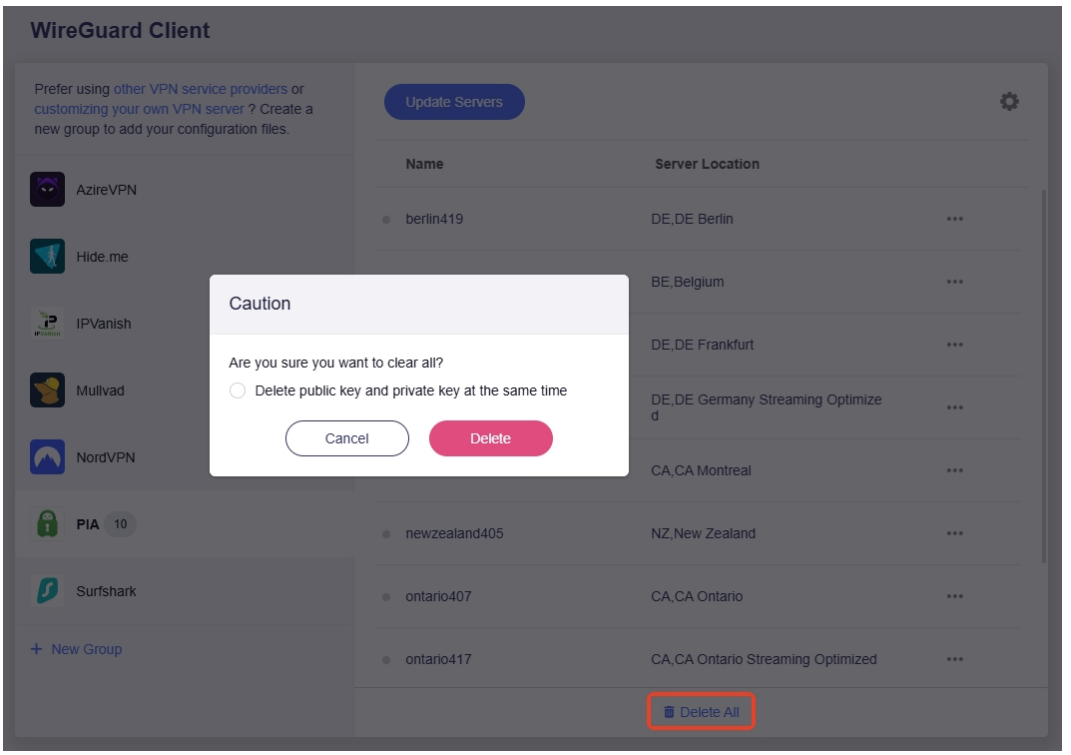
7. Modifica credenziali o esci.

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



8. Elimina tutti i file.

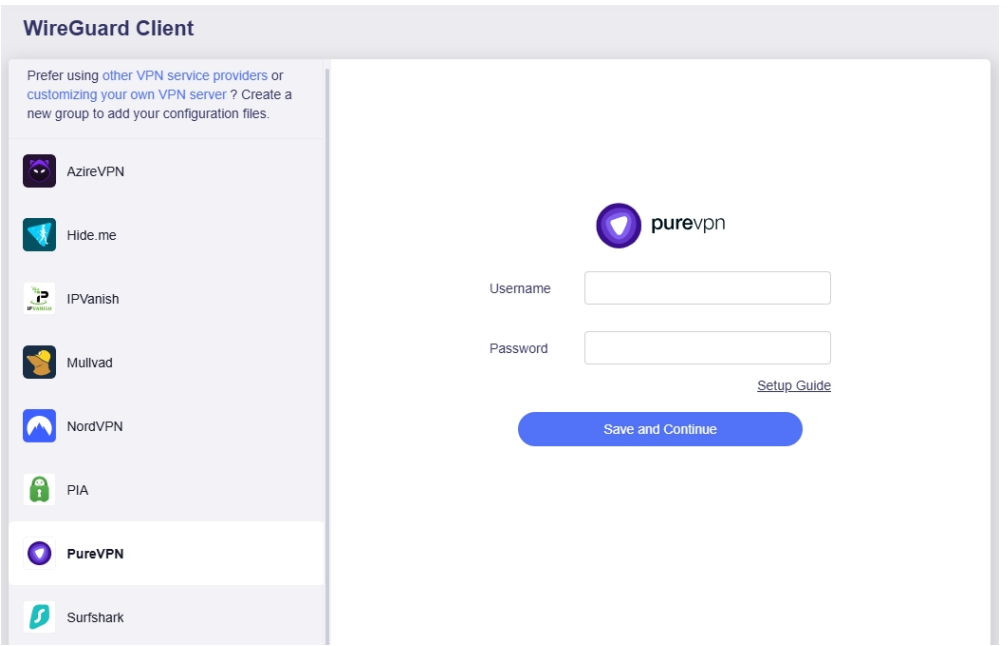
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



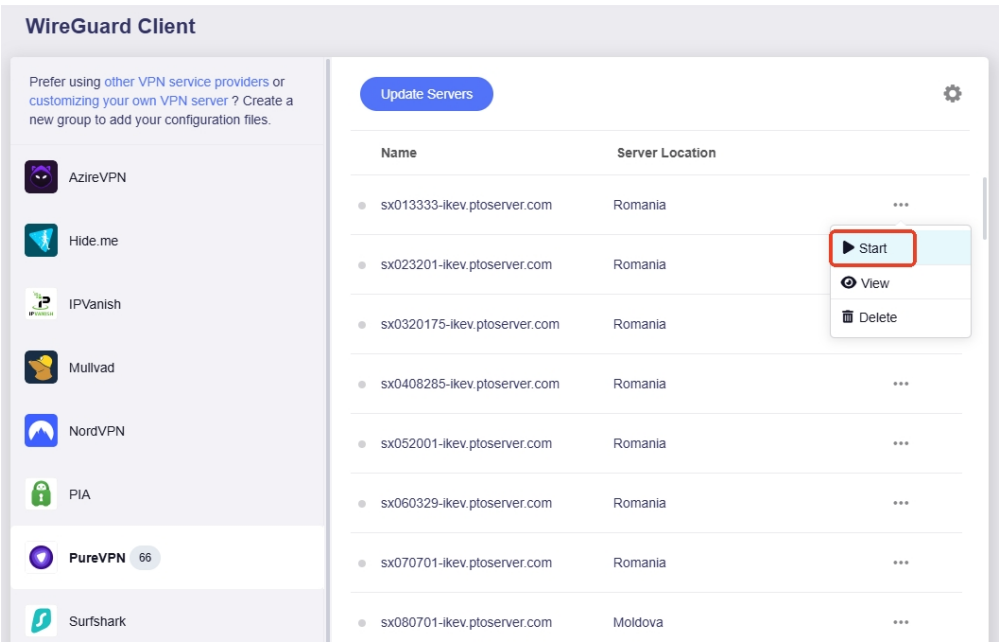
10.2.8 Configurazione di PureVPN

Segui i passaggi seguenti per impostare il tuo router come Pureclient VPN.

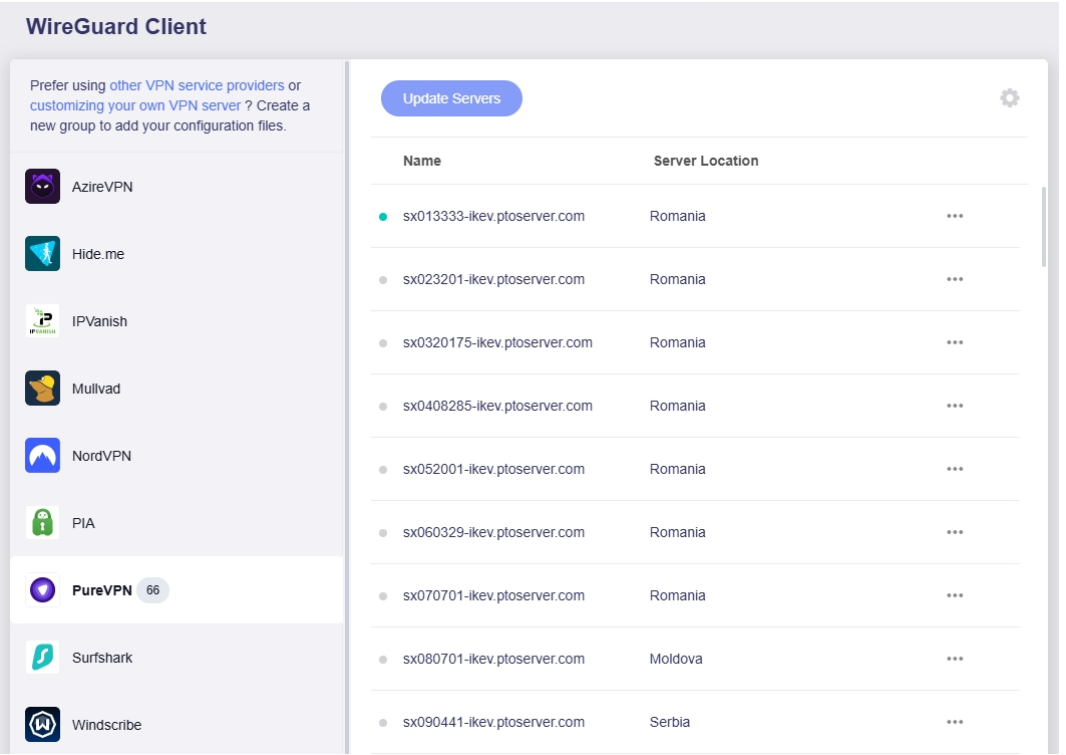
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **PureVPN**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



3. Seleziona il tuo server preferito e fai clic sull'icona a tre punti sulla destra per avviare una connessione.



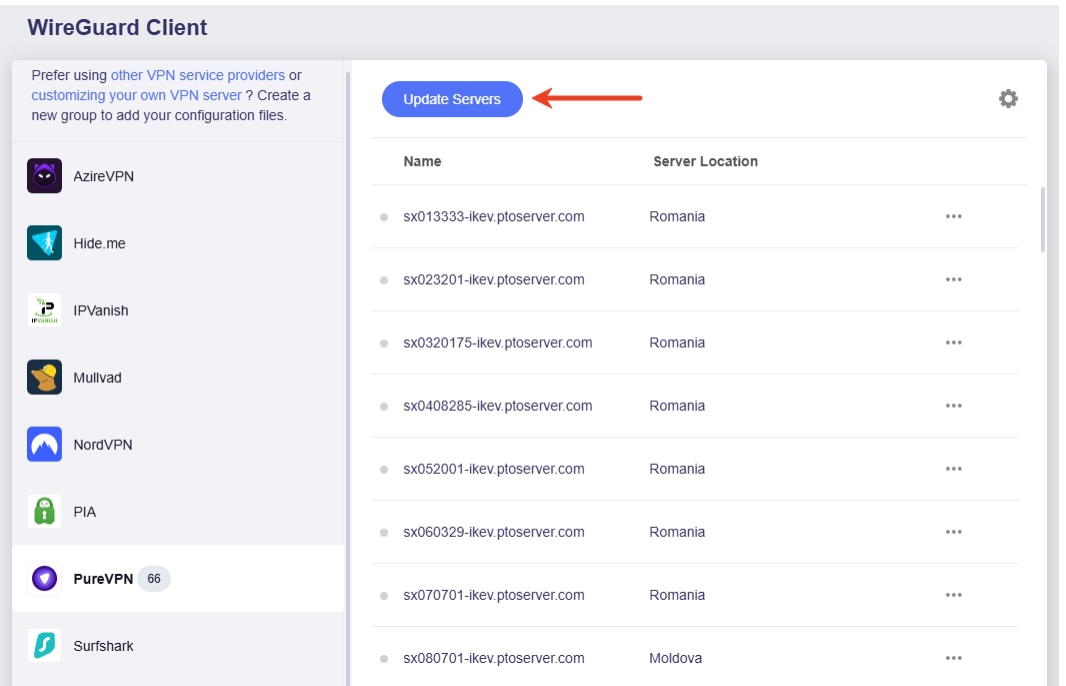
4. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

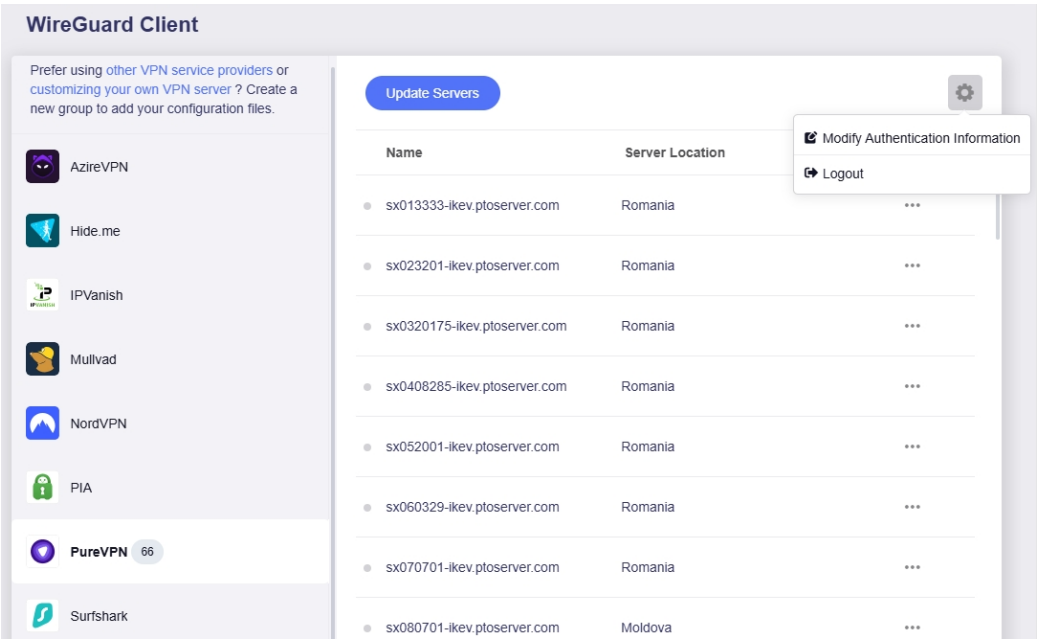
5. Aggiorna server.

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.



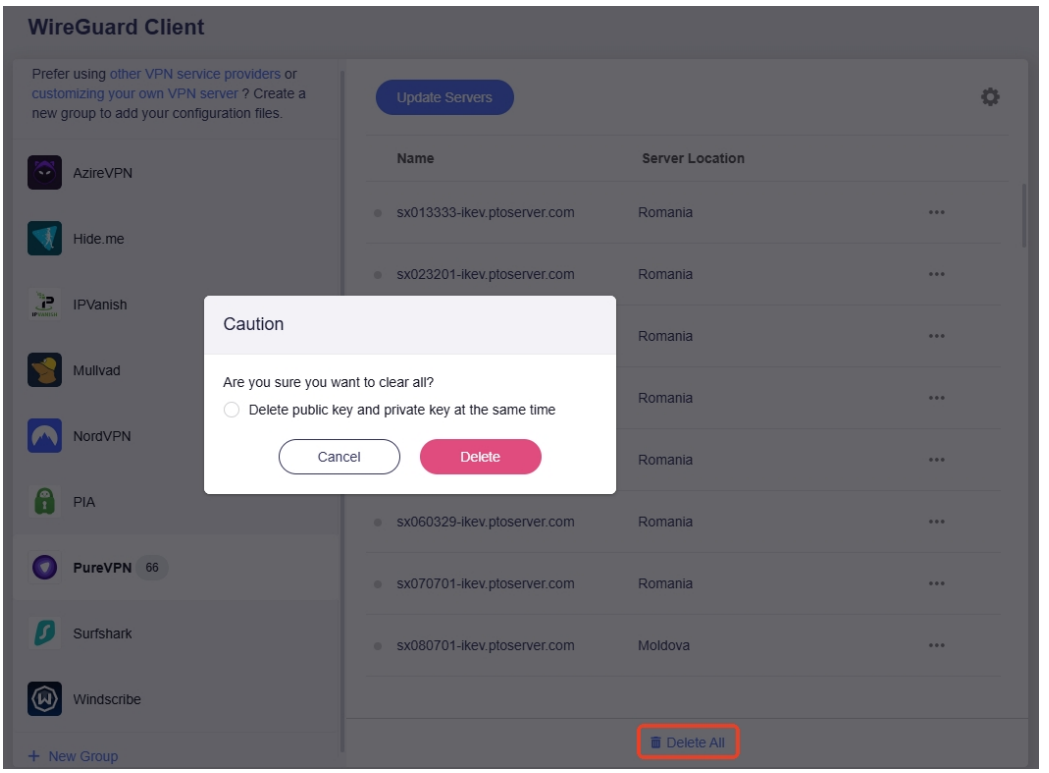
6. Modifica credenziali o esci.

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



7. Elimina tutti i file.

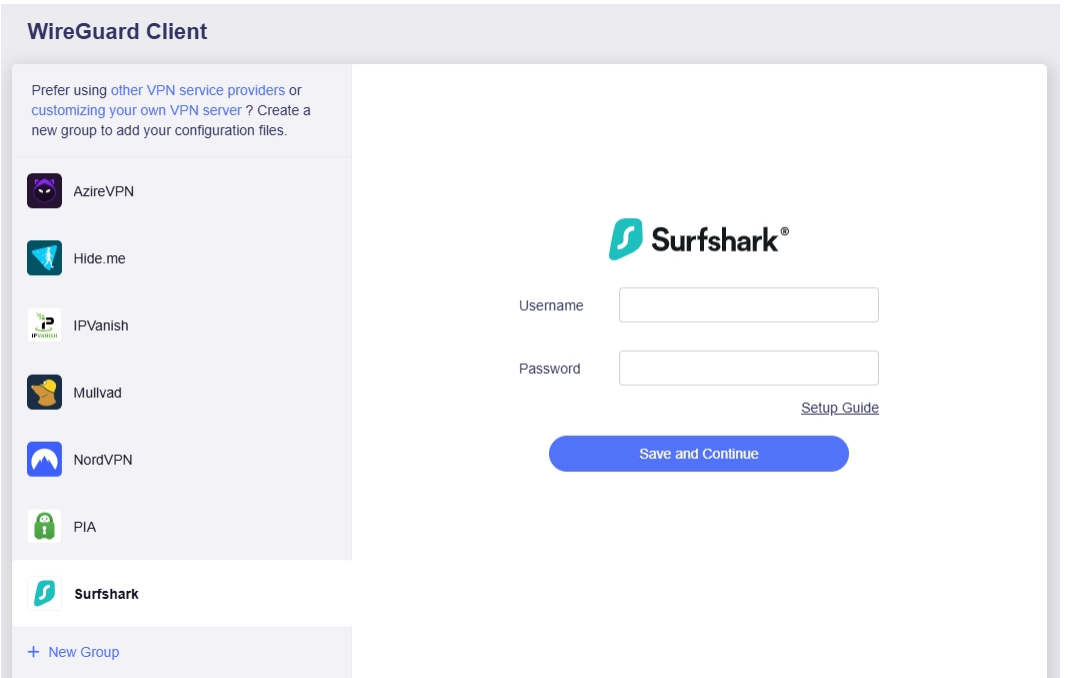
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



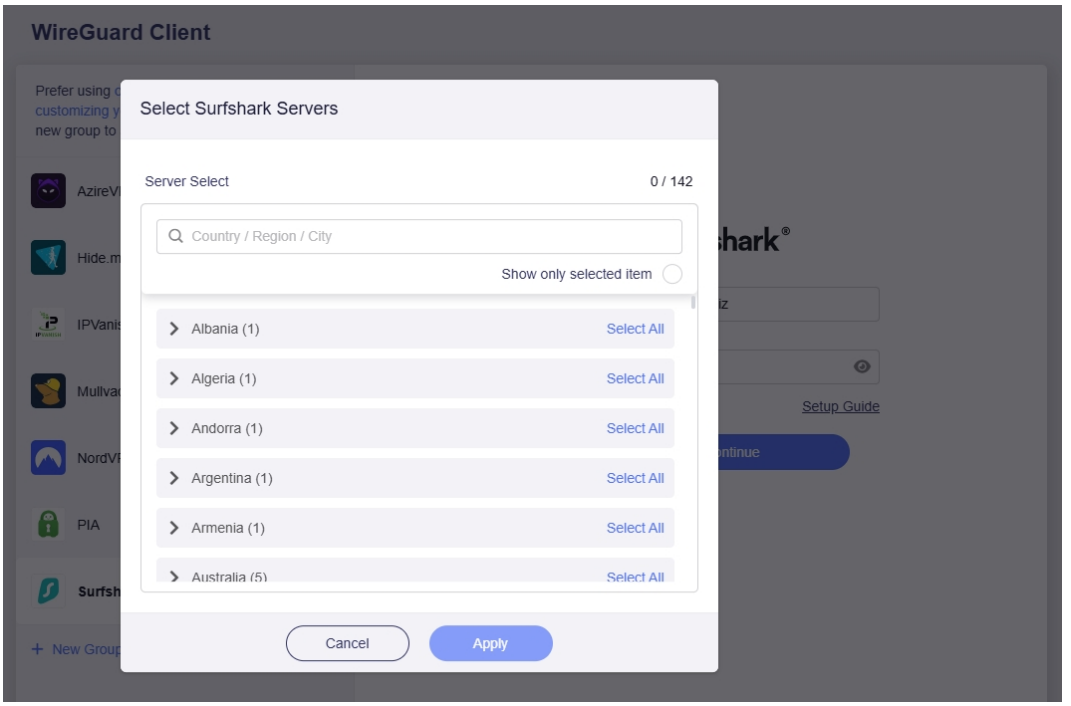
10.2.9 Configurazione di Surfshark

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

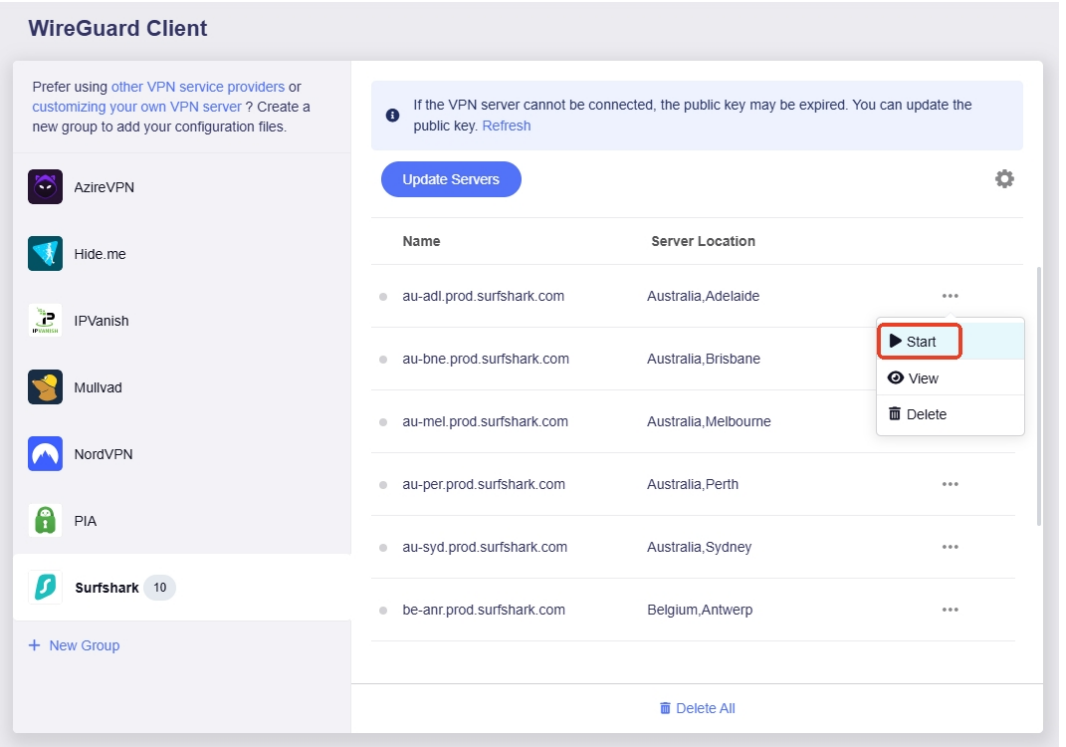
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Surfshark**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



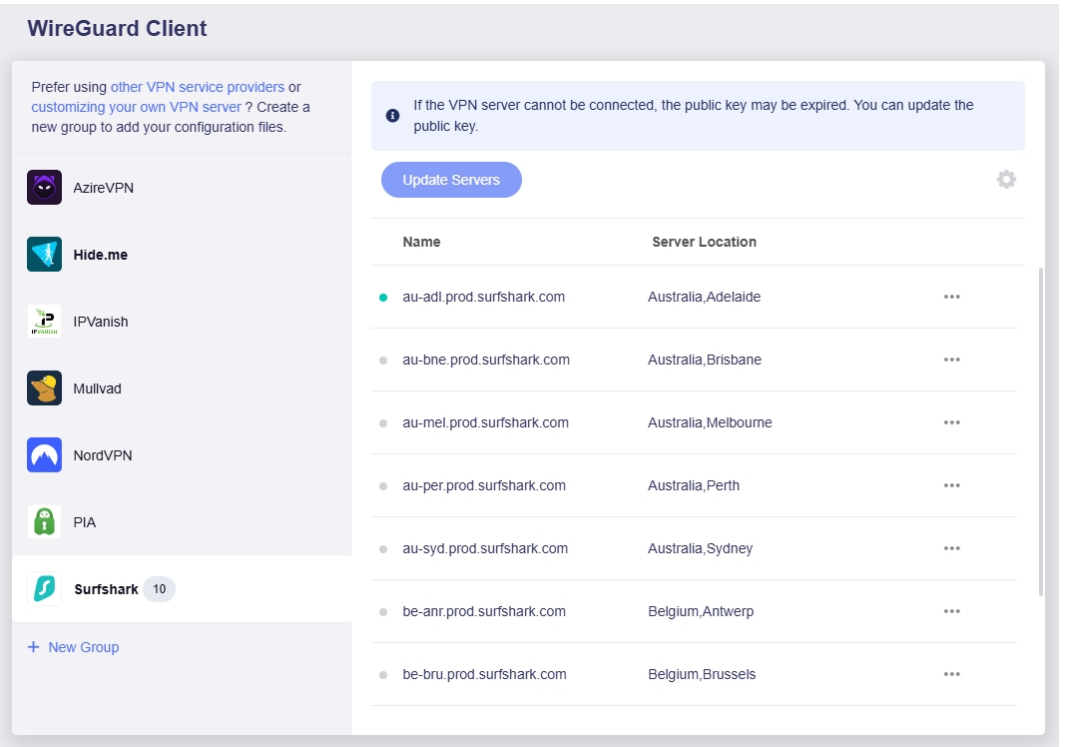
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



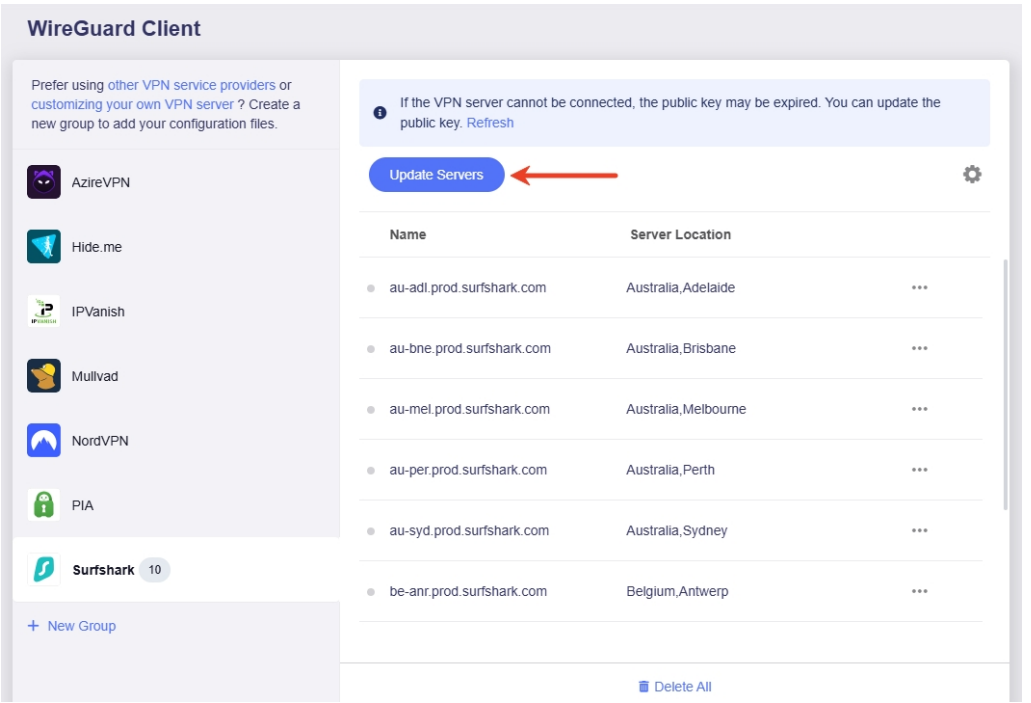
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

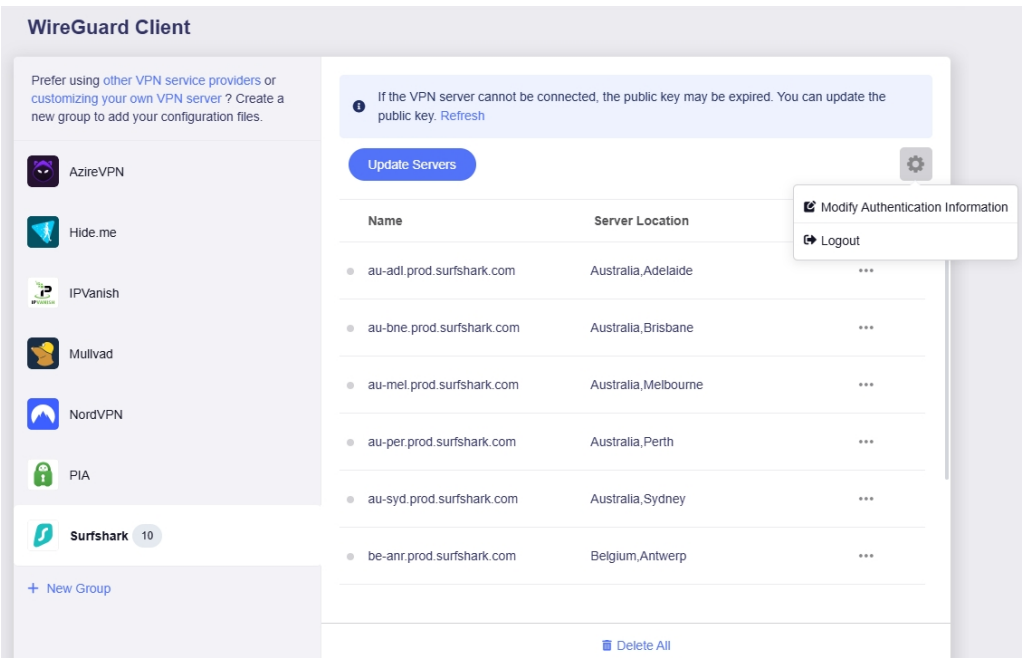
6. Aggiorna server.

   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.



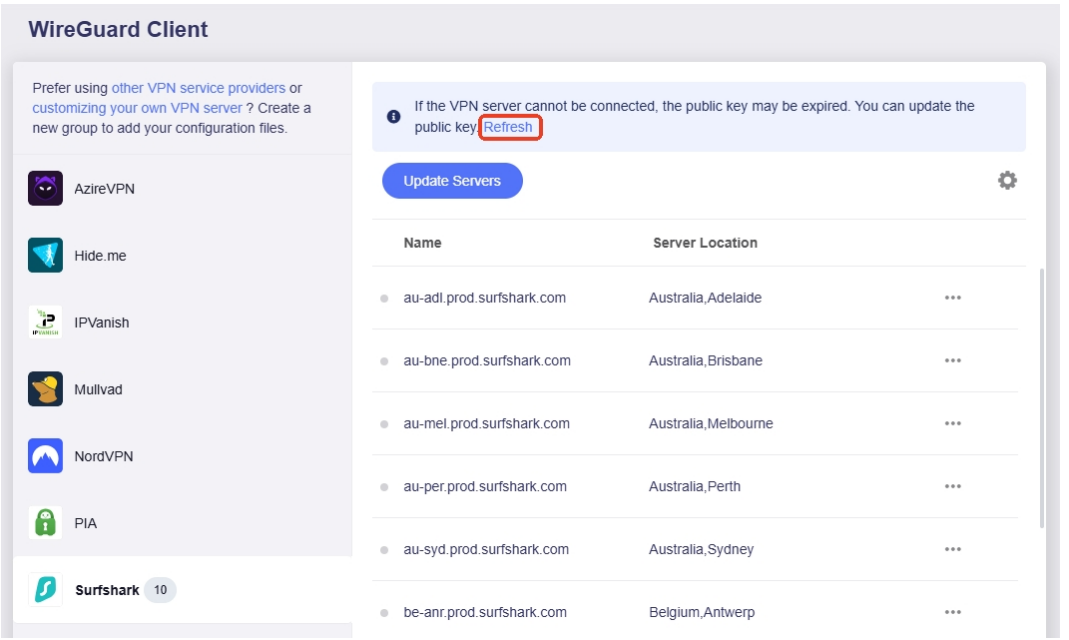
7. Modifica credenziali o esci.

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



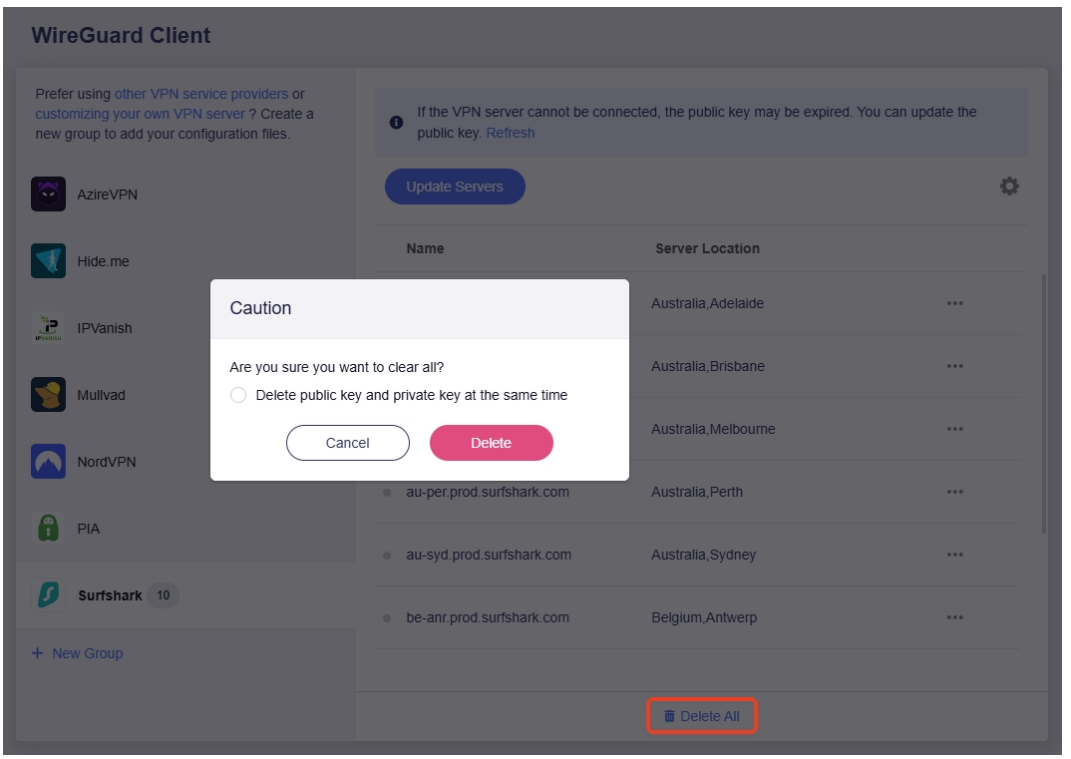
8. Aggiorna.

   Puoi fare clic su **Aggiorna** per aggiornare la chiave pubblica quando non è possibile connettere il server VPN.



9. Elimina tutti i file.

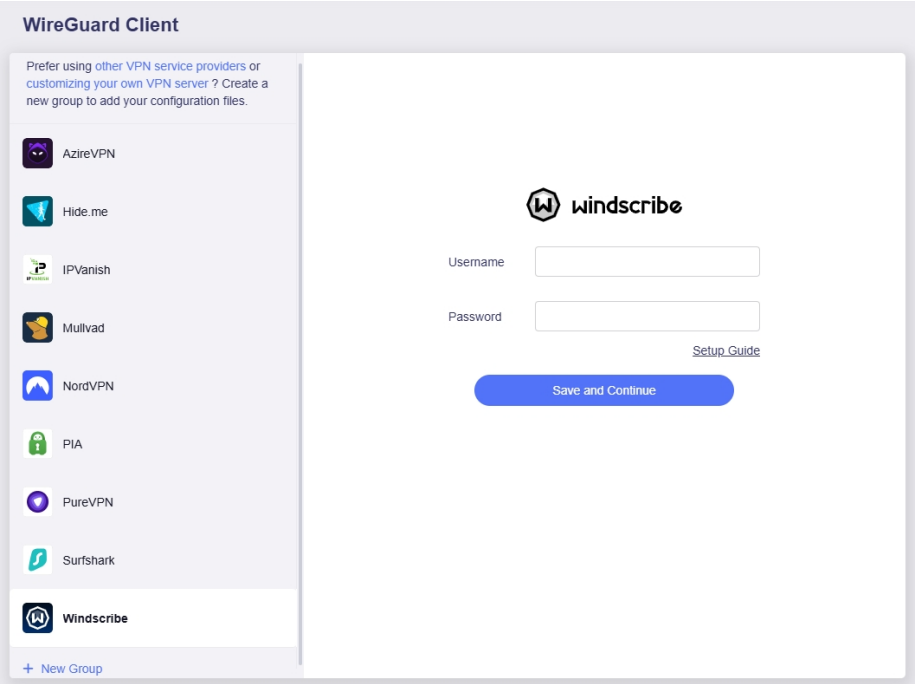
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



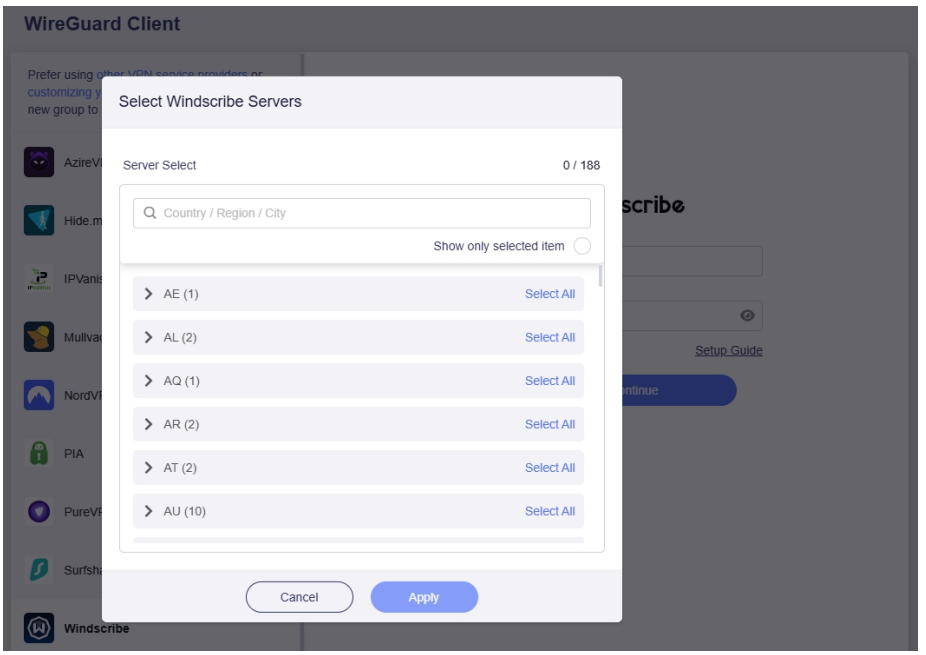
10.2.10 Configurazione di Windscribe

Segui i passaggi seguenti per impostare il tuo router come Windscribe client.

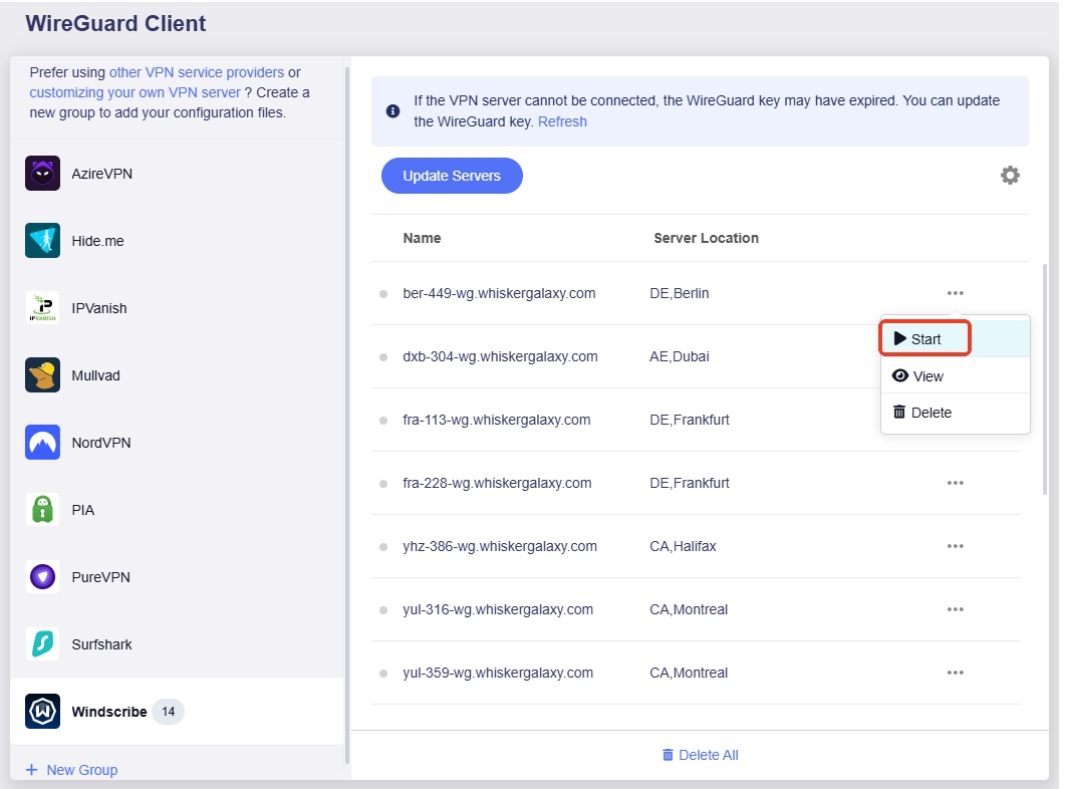
1. Accedi a pannello di amministrazione web e vai su **VPN** > **Client WireGuard** > **Windscribe**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



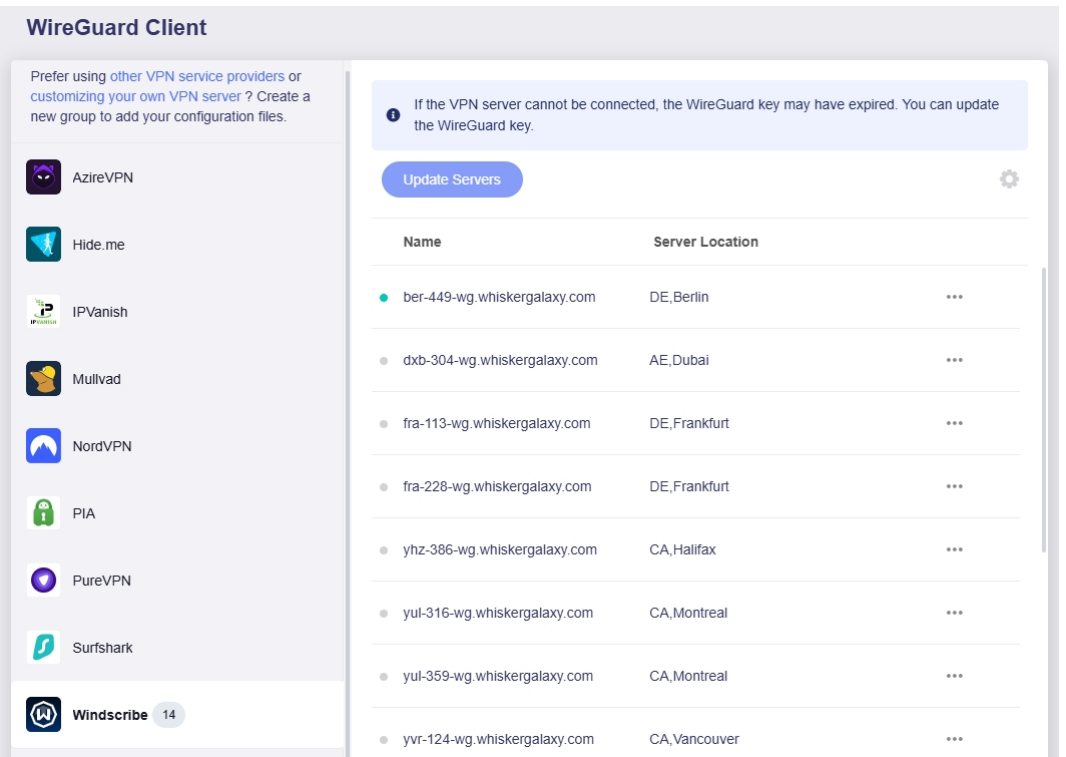
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



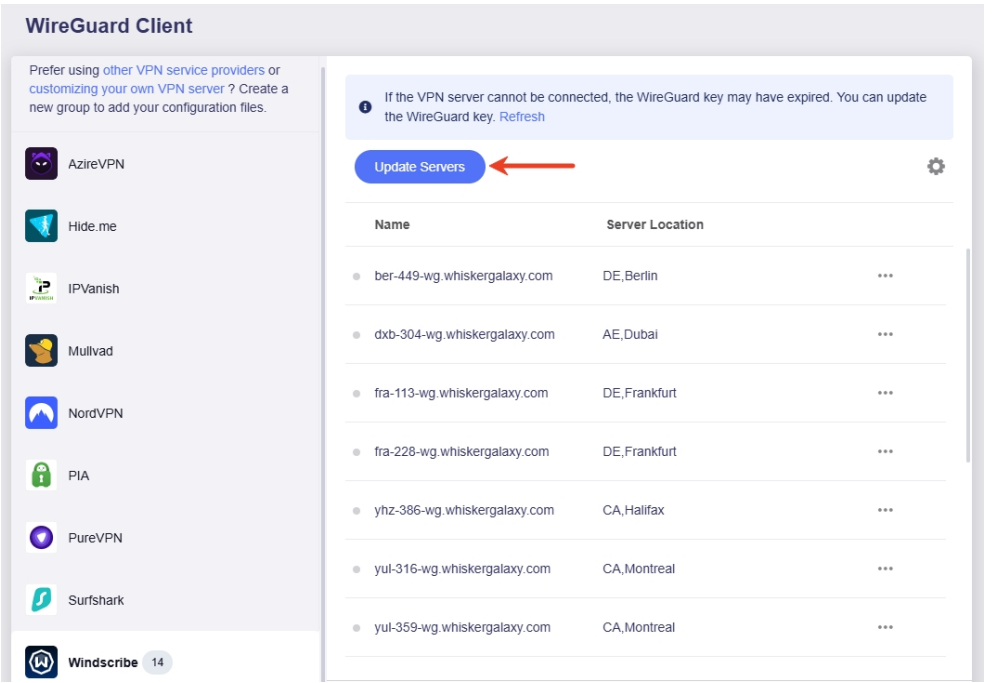
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

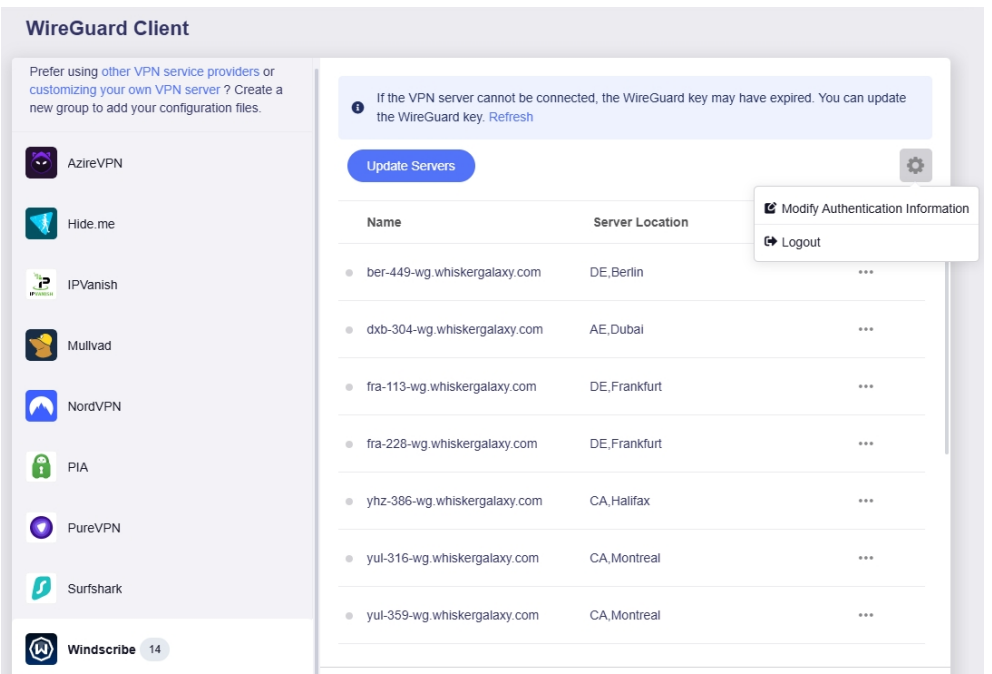
6. Aggiorna server.

   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.



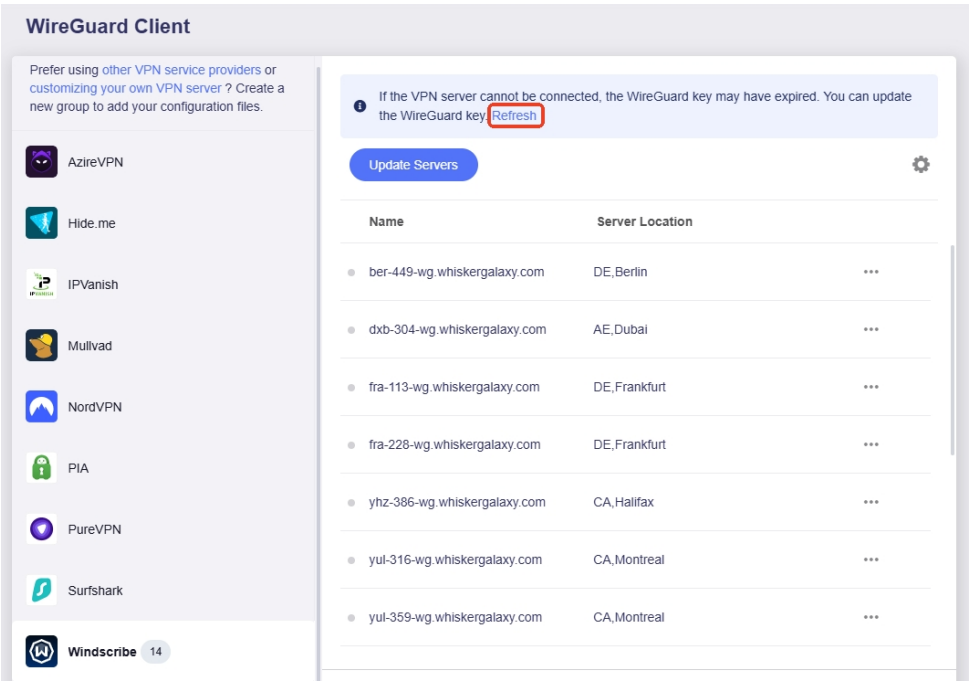
7. Modifica credenziali o esci.

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



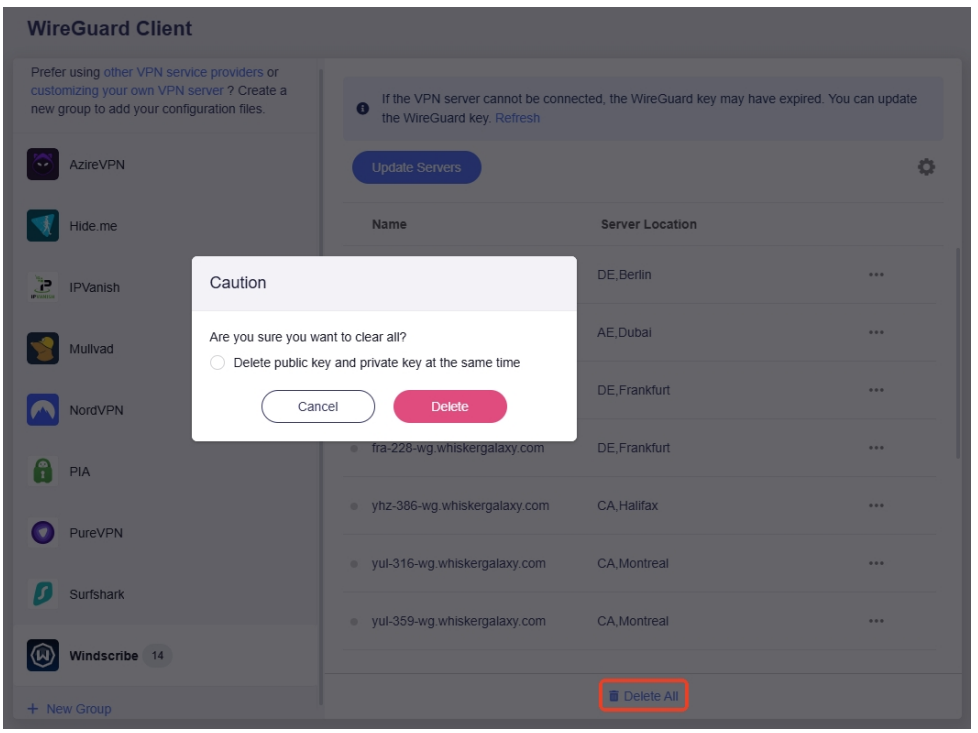
8. Aggiorna.

   È possibile fare clic su **Aggiorna** per aggiornare la chiave pubblica quando non è possibile connettere la VPN.



9. Elimina tutti i file.

   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.

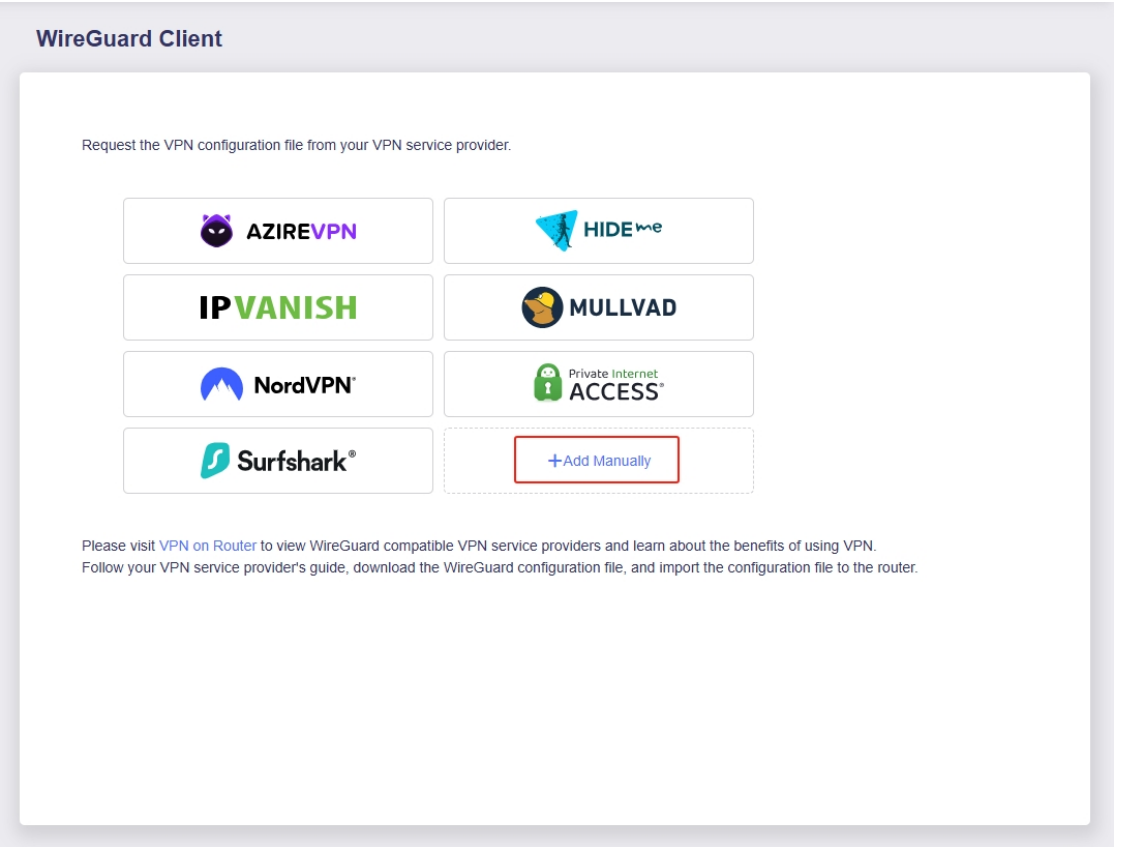


10.2.11 Configurazione manuale del client WireGuard (altri provider)

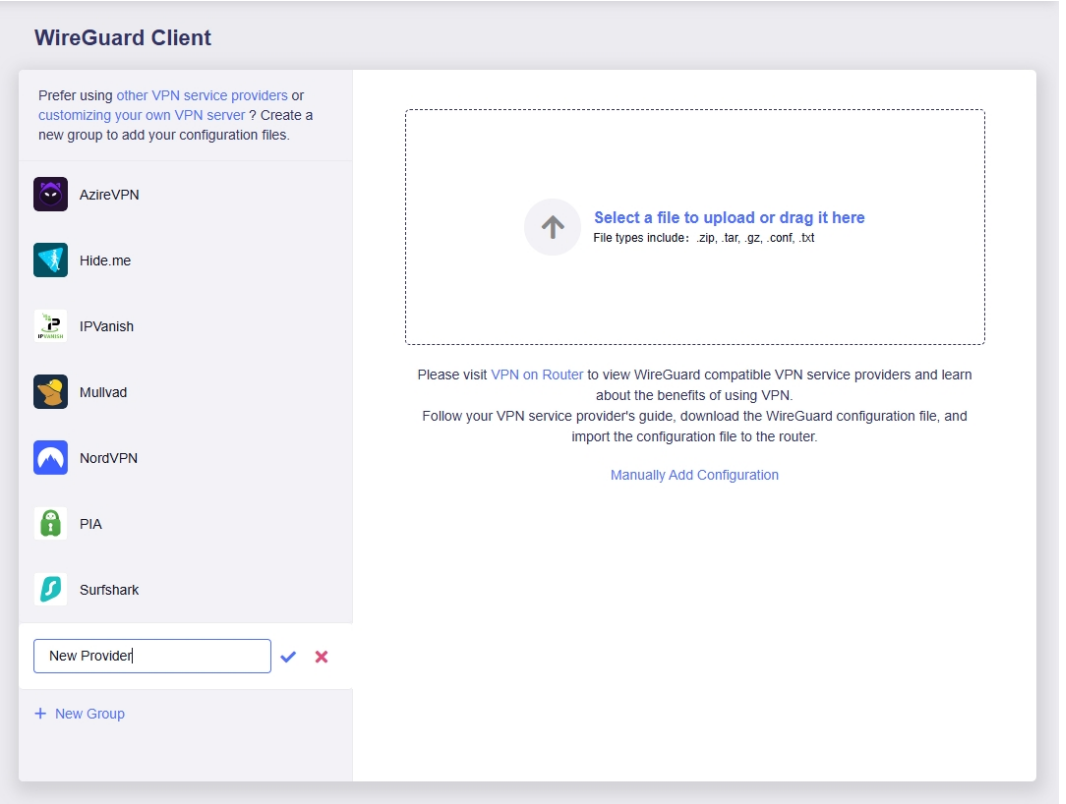
Se il tuo fornitore di servizi WireGuard non è integrato nel pannello di amministrazione web, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare uno WireGuard client. Se non sai come scaricare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

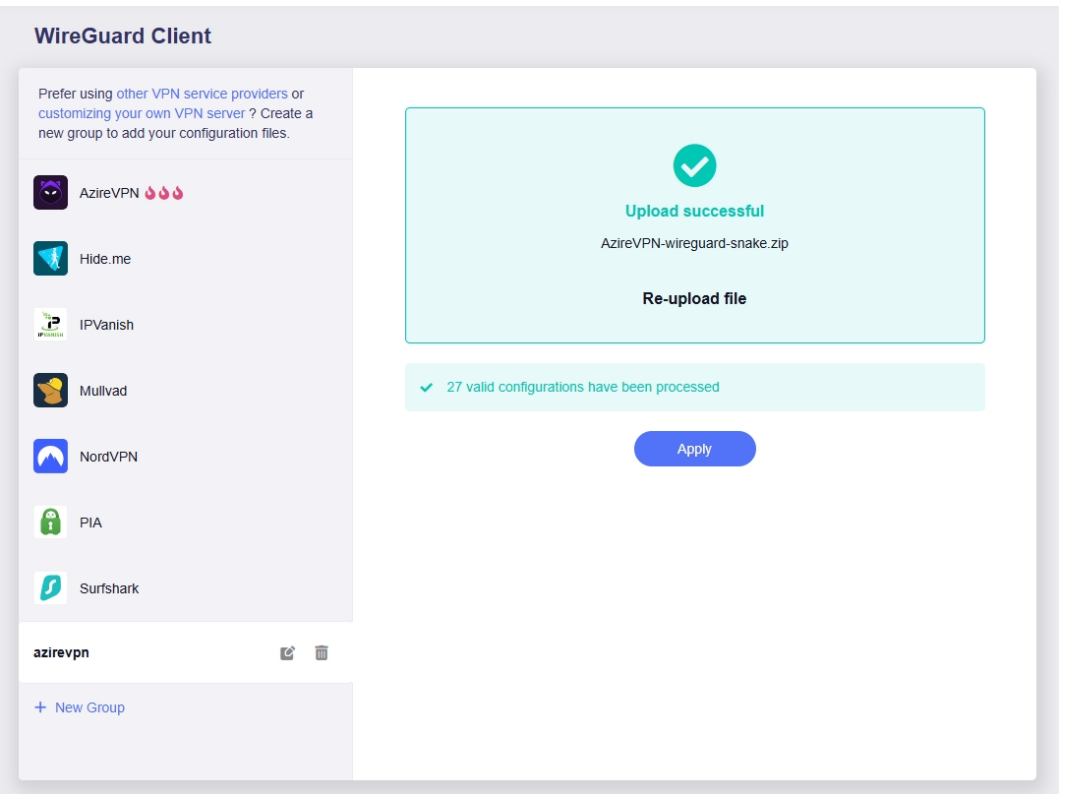
1. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client WireGuard** > **Aggiungi manualmente**.



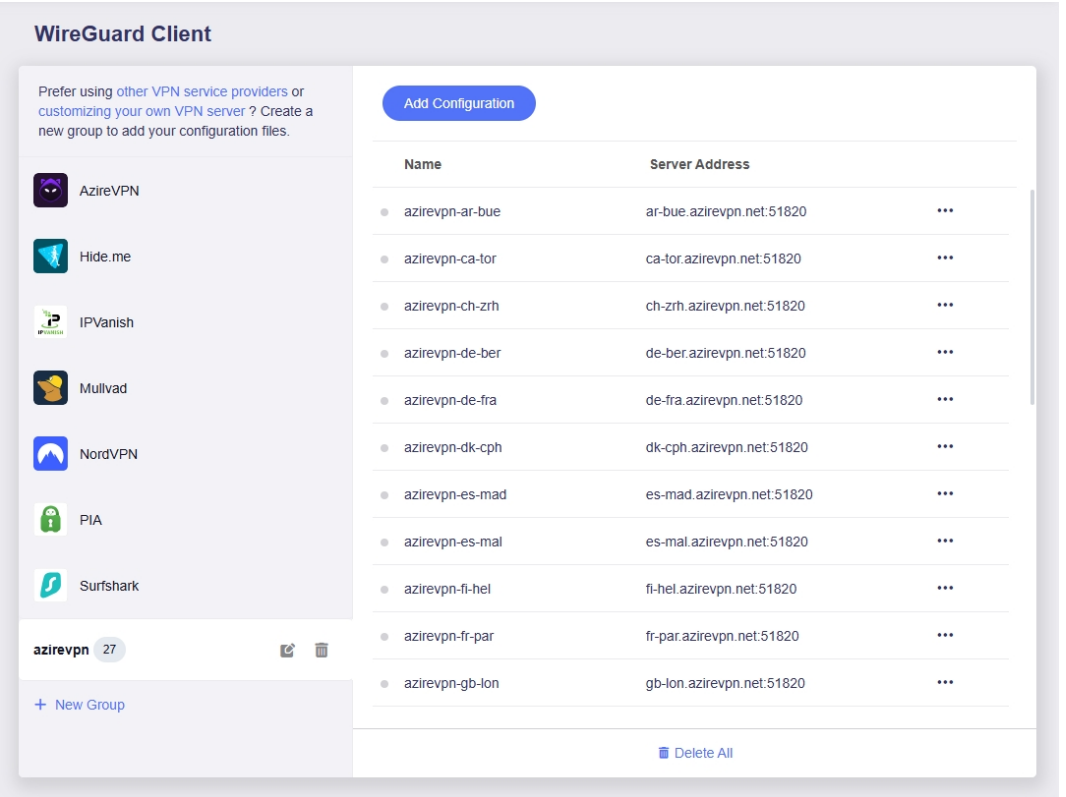
2. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.



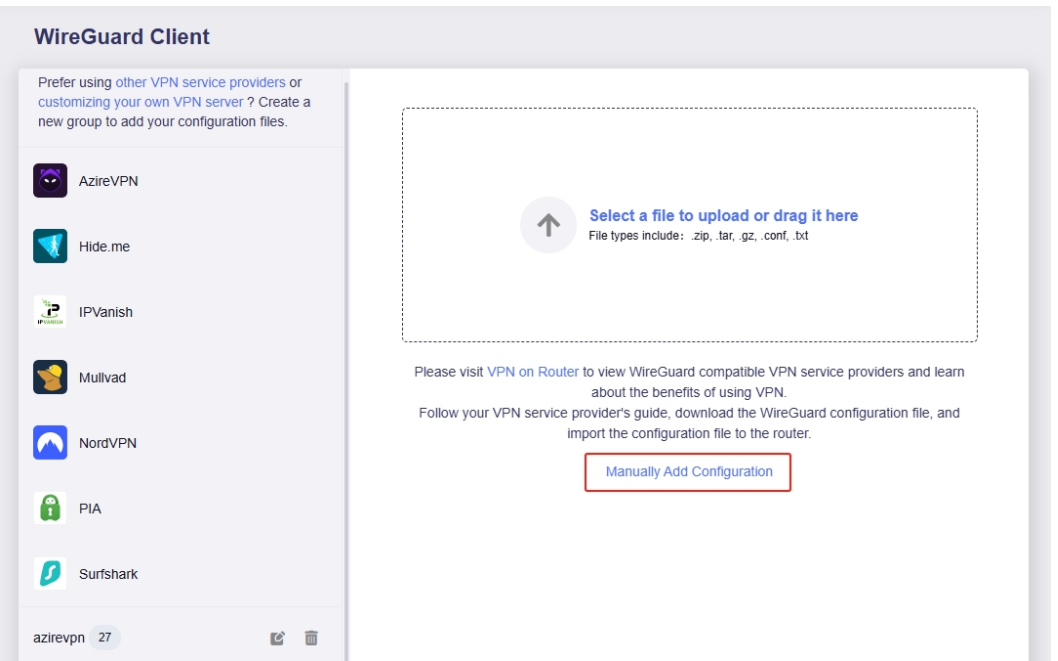
3. Fai clic sull'area di caricamento per caricare il file di configurazione WireGuard (formati supportati: zip, tar, gz, conf, txt) e fai clic su **Applica**.

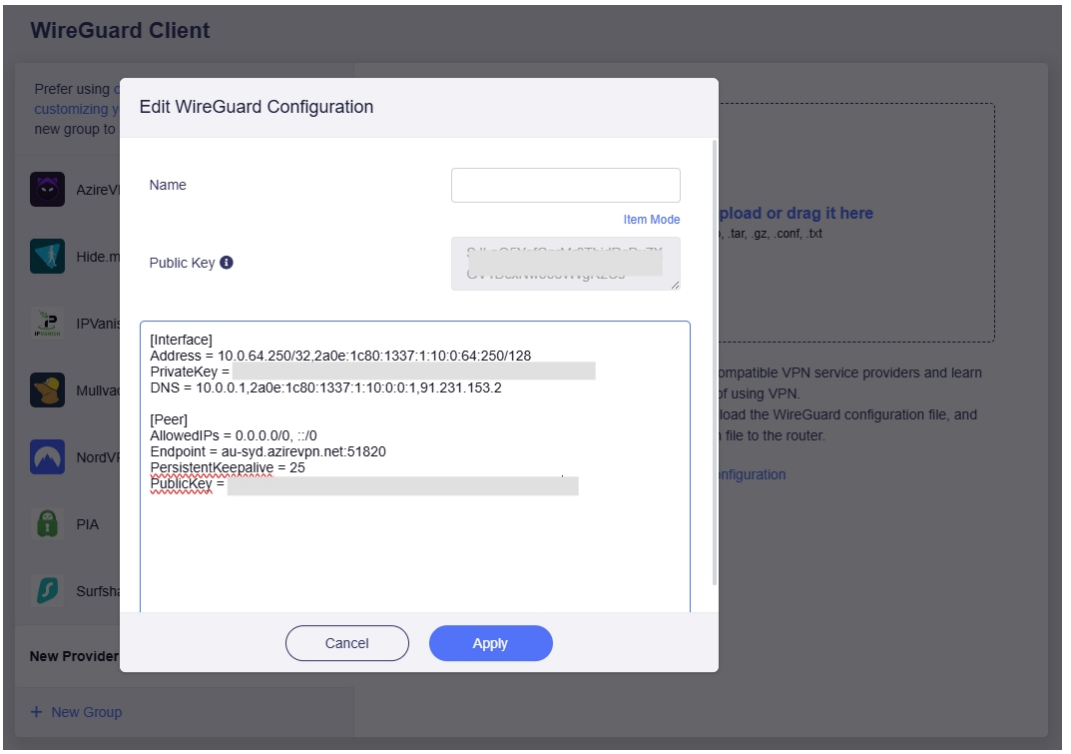


Se carichi un file compresso contenente più file di configurazione, verrà decompresso automaticamente, come mostrato di seguito.

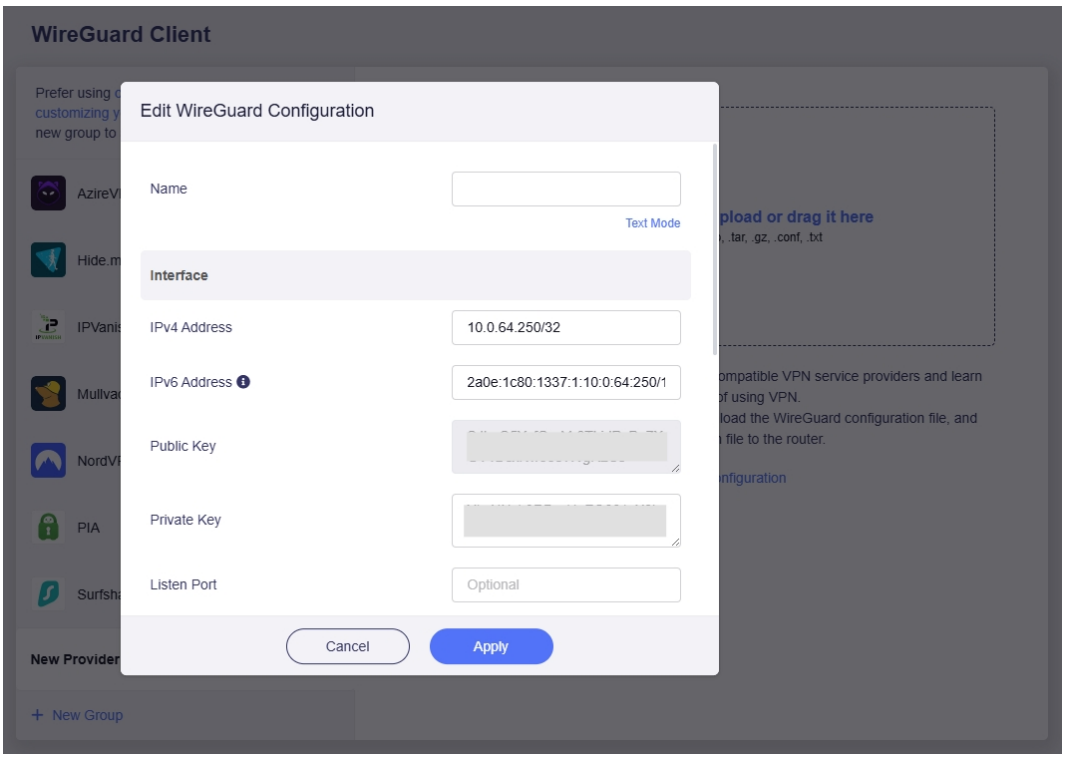


In alternativa, puoi fare clic su **Aggiungi manualmente la configurazione** nella parte inferiore dell'area di caricamento, aggiungere i dettagli della configurazione in formato testo e fare clic su **Applica**.

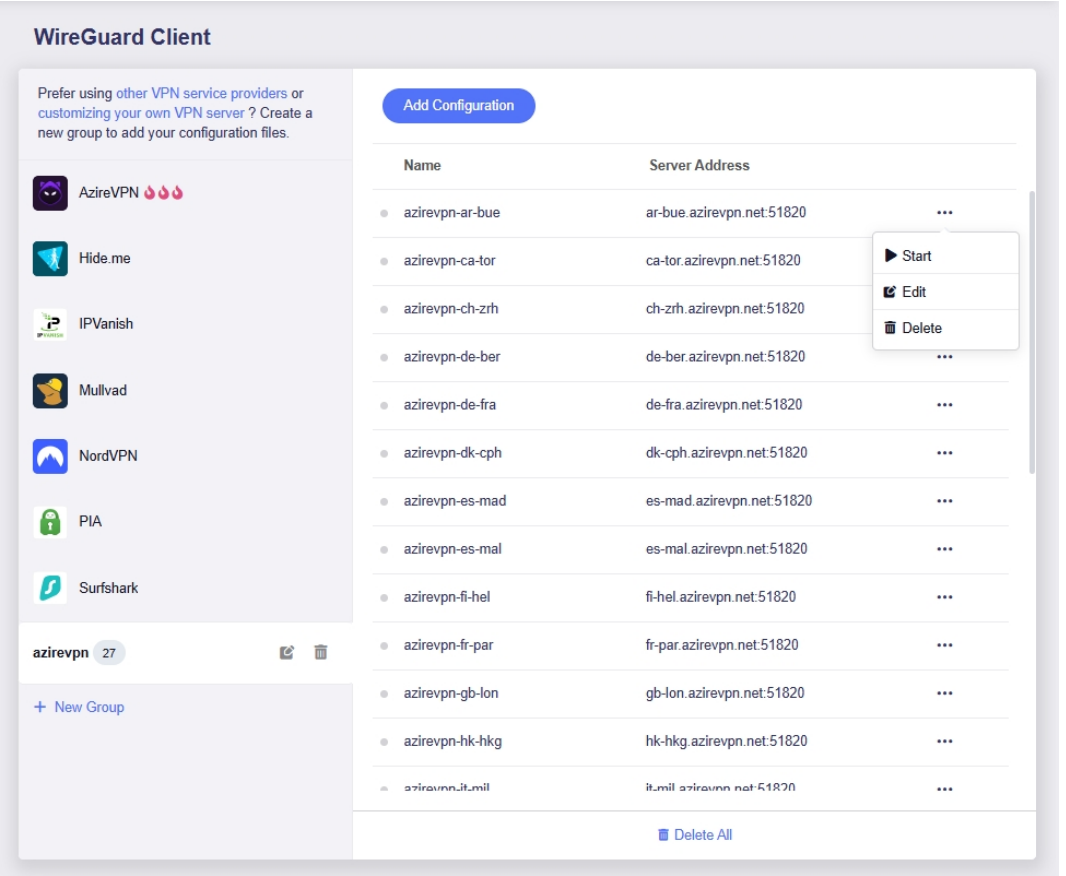




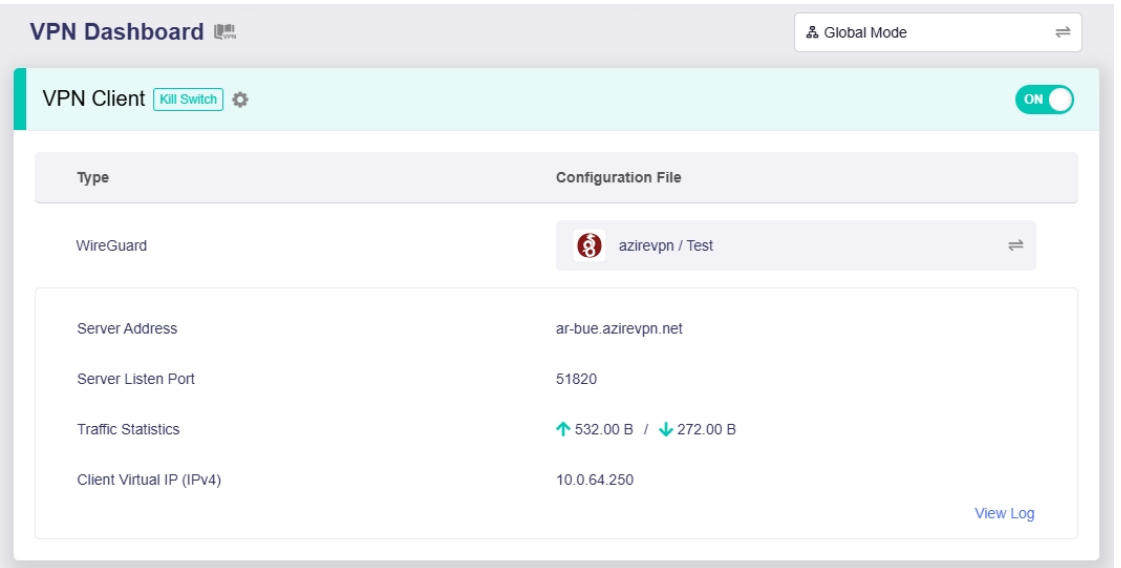
Per verificare ogni parametro, passa alla modalità Voce e controlla i dettagli della configurazione, quindi fai clic su **Applica**.



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

Rete

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

11.1 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:

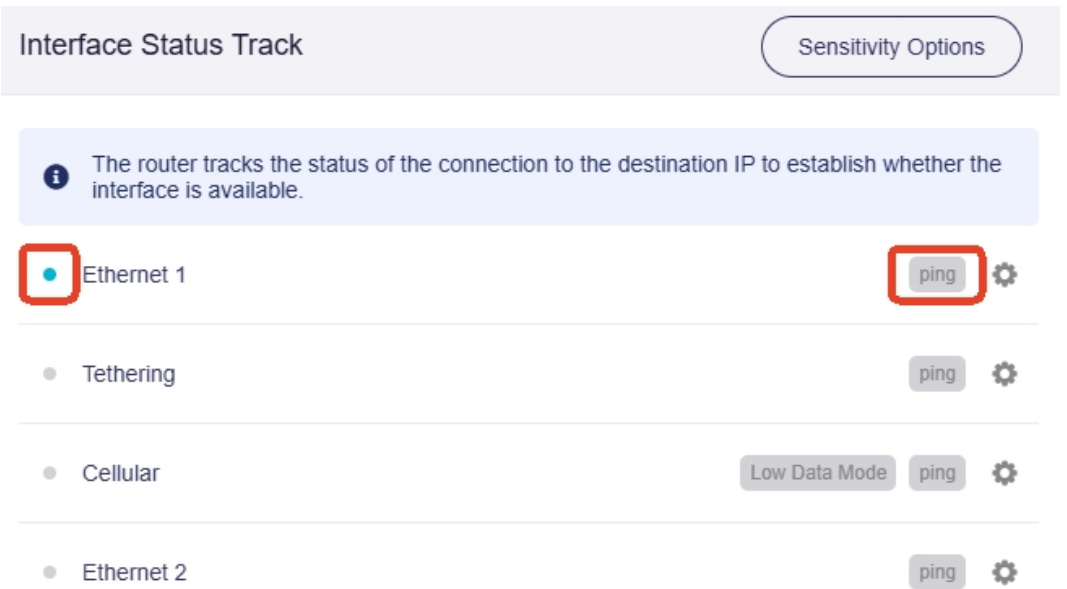
- **Failover**: passa automaticamente a una connessione alternativa in breve tempo se la connessione primaria fallisce, garantendo un accesso alla rete ininterrotto.
- **Bilanciamento del carico**: distribuisce il traffico di rete su tutte le connessioni disponibili con un rapporto prestabilito per l'utilizzo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

Brume 3 supporta tre tipi di metodi di connessione Internet, tra cui Ethernet, Tethering e Cellulare, ciascuno dei quali serve una funzione di rete distinta in configurazioni definite dal software.

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.

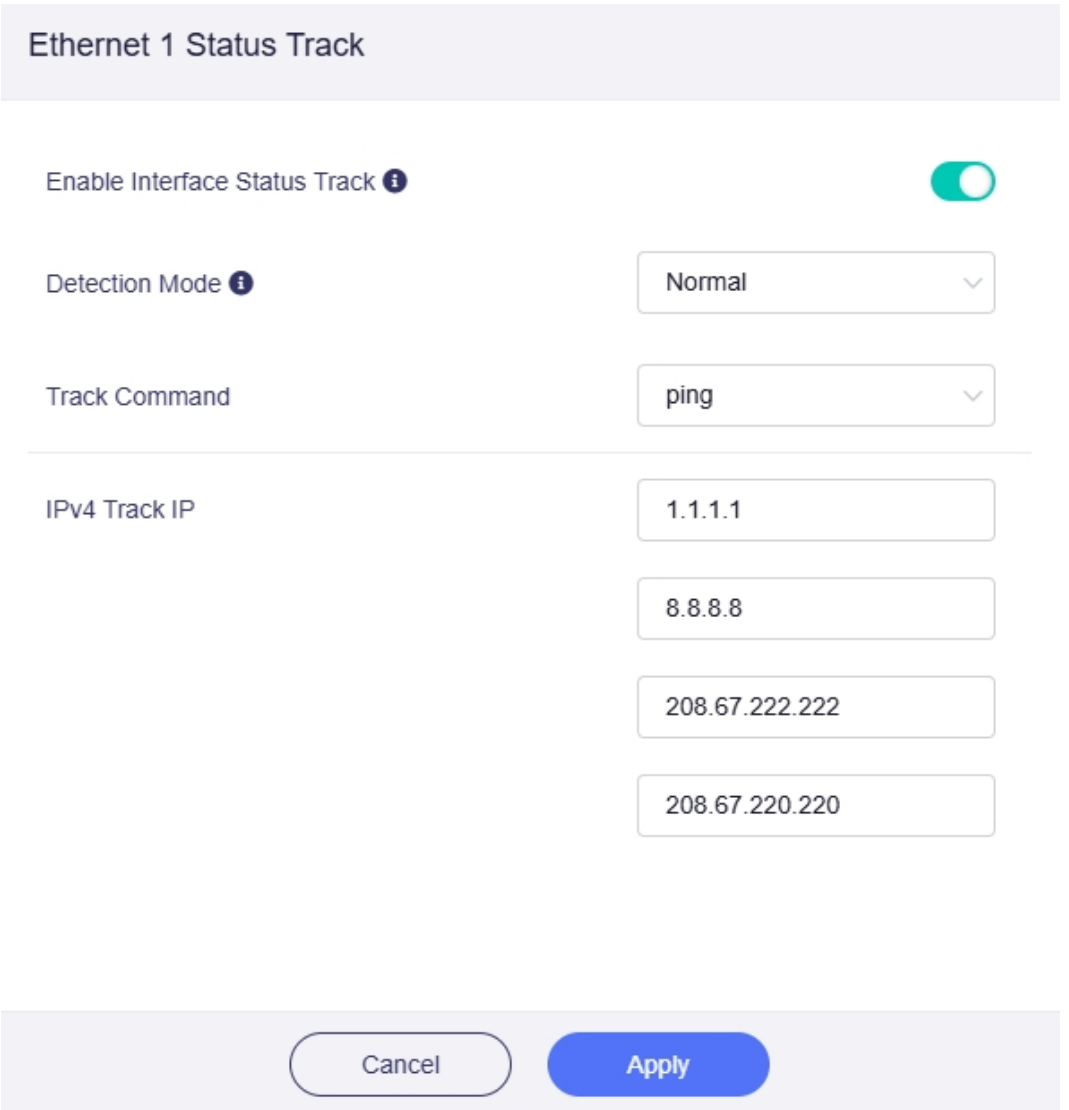
11.1.1 Monitoraggio dello stato dell’interfaccia

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.

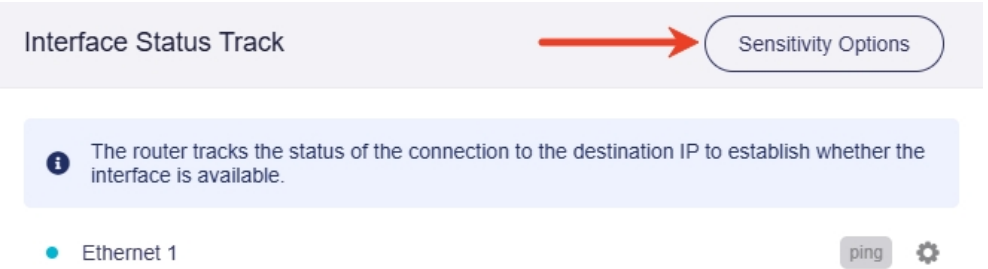


- **Abilita monitoraggio dello stato dell'interfaccia**: è abilitato per impostazione predefinita. Se disabilitato, il router determinerà lo stato dell'interfaccia in base alle condizioni fisiche (ad esempio, se il cavo Ethernet è collegato).
- **Modalità di rilevamento**: questa funzionalità è stata 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.

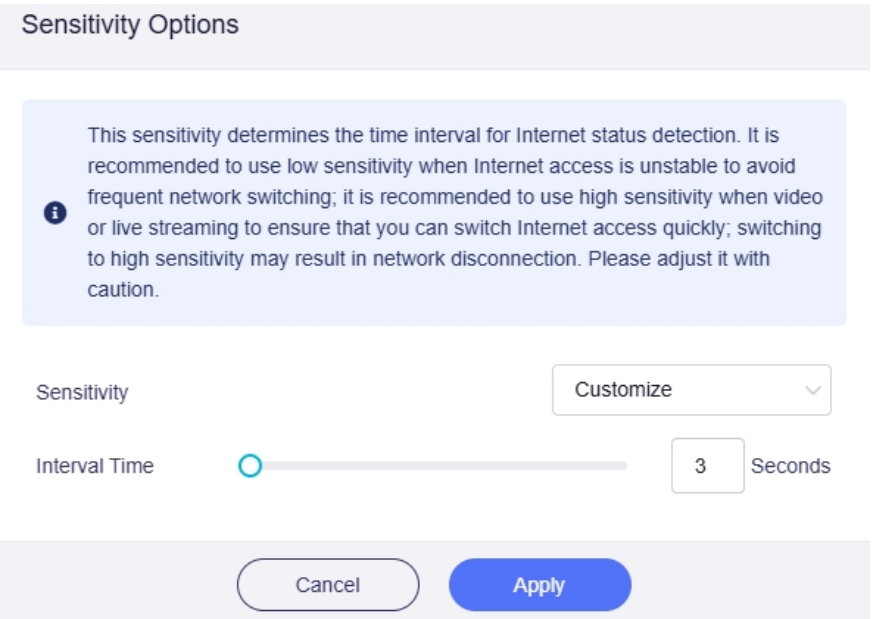
- **Modalità normale**: viene utilizzata per impostazione predefinita.
- **Modalità dati ridotti**: attiva il monitoraggio solo quando si verifica un errore di rete sull'interfaccia di rete. Utilizza questa modalità se hai un piano dati limitato. Tieni presente che la riconnessione dopo una disconnessione potrebbe essere leggermente più lenta rispetto alla modalità normale ed è abilitata per impostazione predefinita solo per l'interfaccia cellulare.
- **Modalità rigorosa**: 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 IP di traccia IPv4 secondo necessità.

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.



Suggerimenti: se la rete è stabile, si consiglia un'elevata sensibilità per una commutazione rapida in caso di disconnessione della rete. Questo è adatto per scenari come guardare video, streaming live o giocare. Se la rete è instabile, si consiglia una sensibilità bassa per evitare frequenti cambi di rete e connessioni non riuscite. Questo vale per scenari come il download di file memorizzati nella cache.

Nota: il passaggio alla sensibilità elevata può causare disconnessioni di rete occasionali durante il processo. Si prega di adeguarsi con cautela.

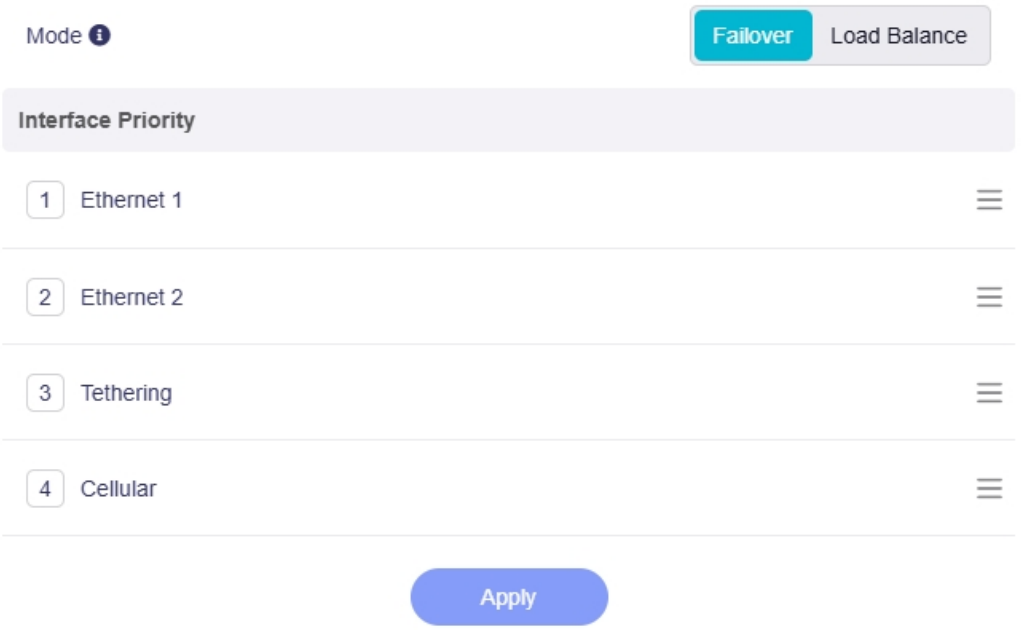
11.1.2 Modalità Multi-WAN

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.

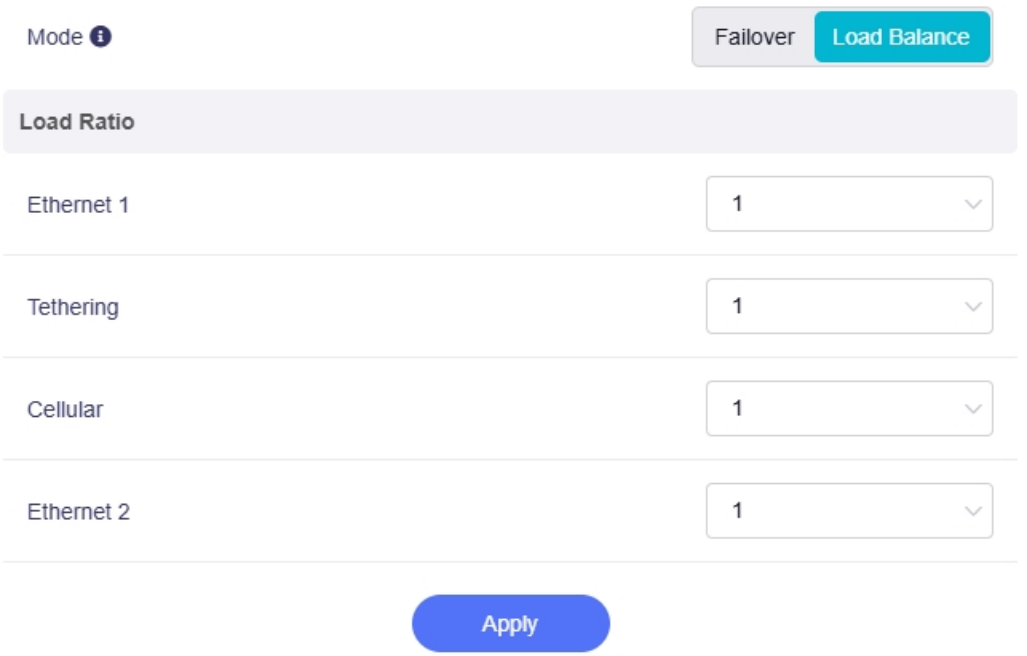


Bilanciamento del carico

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



Personalizza il rapporto di carico secondo necessità. Ad esempio, se Ethernet 1 ha una larghezza di banda di 100 Mbps, Ethernet 2 ha 200 Mbps e non sono attive connessioni tethering o cellulare, impostare i rapporti di carico su 1 per Ethernet 1, 2 per Ethernet 2, e 0

per tethering e cellulare. 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 Ethernet 2. 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.

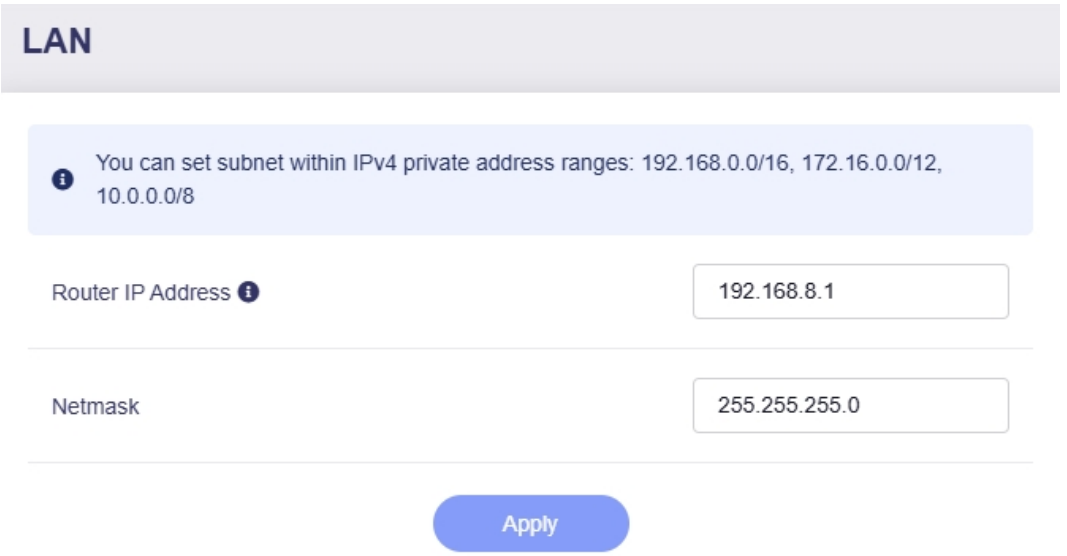
11.2 LAN

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.

11.2.1 Impostazioni di base

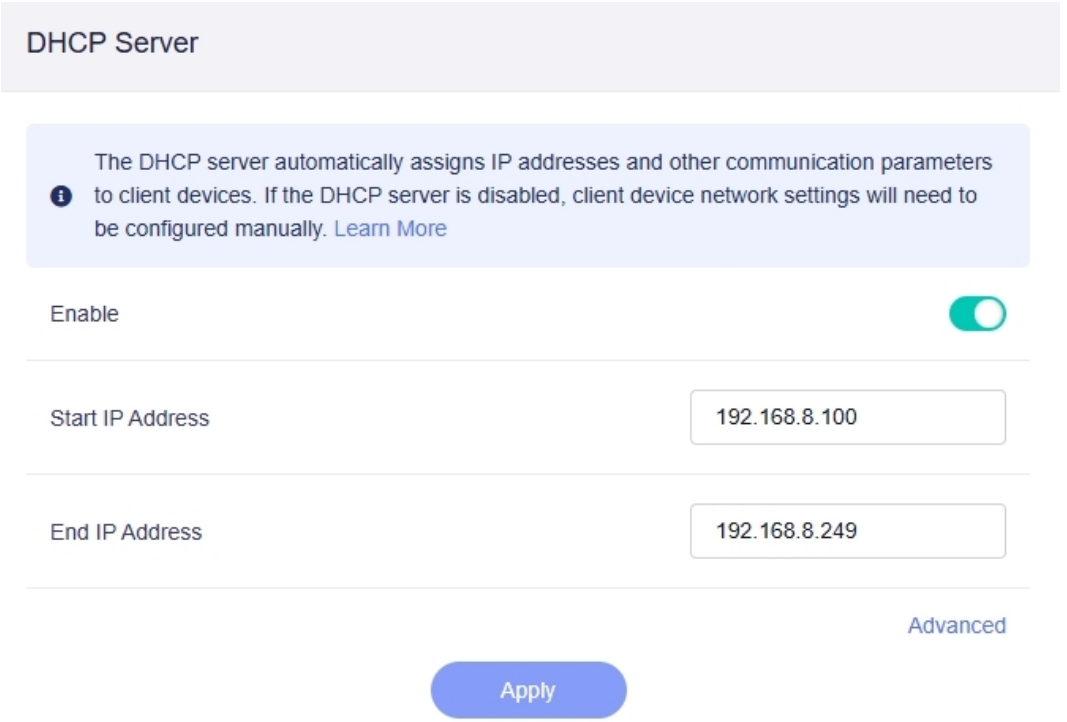
Le impostazioni di base includono l'indirizzo IP del router e Maschera di rete. È possibile impostare la sottorete all'interno degli intervalli di indirizzi privati IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



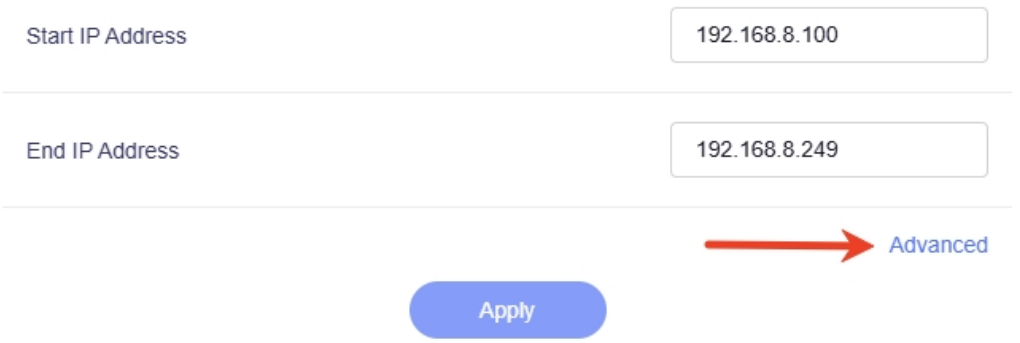
- **Indirizzo IP del router**: questo è l'indirizzo inserito nella barra degli indirizzi del browser per accedere al pannello di amministrazione del router. Per impostazione predefinita è 192.168.8.1 e può essere modificato se è in conflitto con la rete upstream.
- **Maschera di rete**: sono disponibili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

11.2.2 Server DHCP

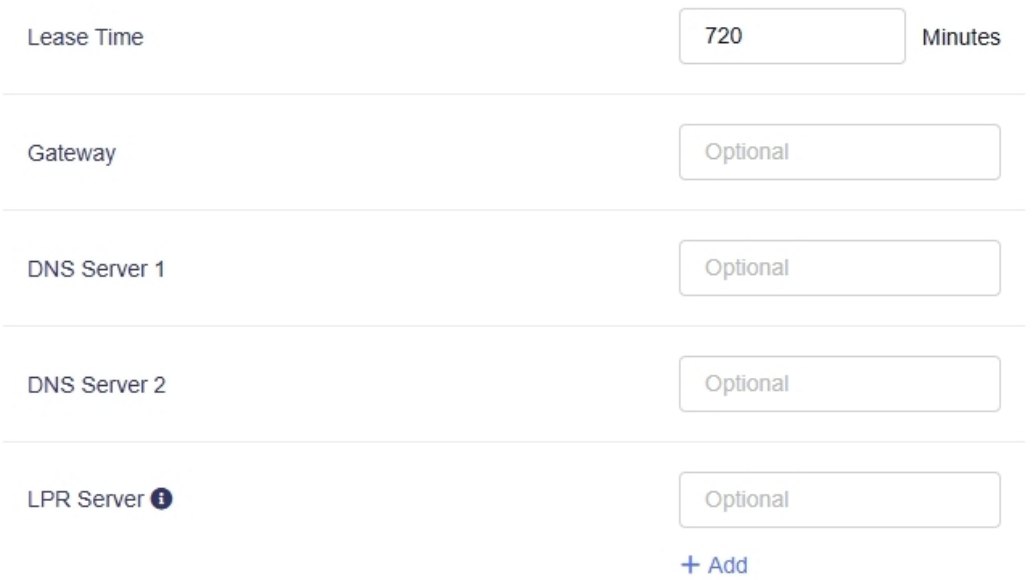
Il server DHCP assegna automaticamente indirizzi IP e altri parametri di comunicazione a ciascuno client connesso. Il server DHCP del router GL.iNet è abilitato per impostazione predefinita e il pool di indirizzi IP del server DHCP varia da 192.168.8.100 a 192.168.8.249. Puoi personalizzare l'intervallo di indirizzi secondo necessità.



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.

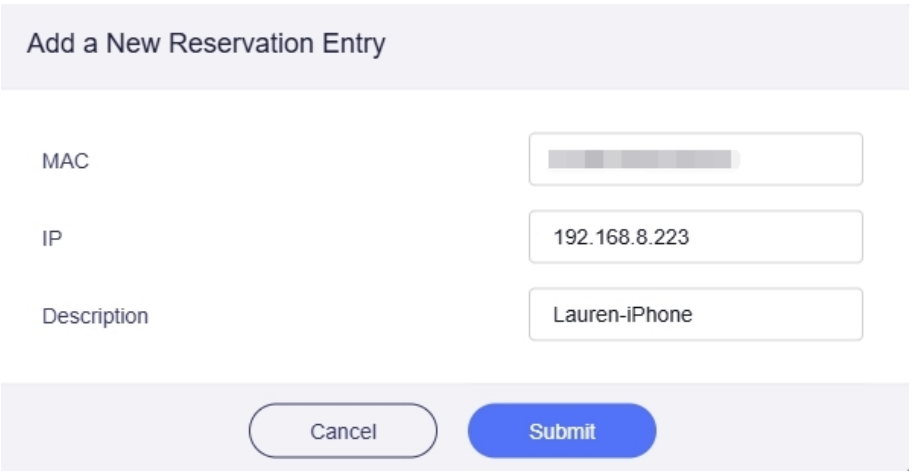
Nota: se il server DHCP è disabilitato, è necessario configurare manualmente l'IP statico e altri parametri di comunicazione per ciascun client. Vedi qui per i dettagli.

11.2.3 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 secondo necessità.

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.

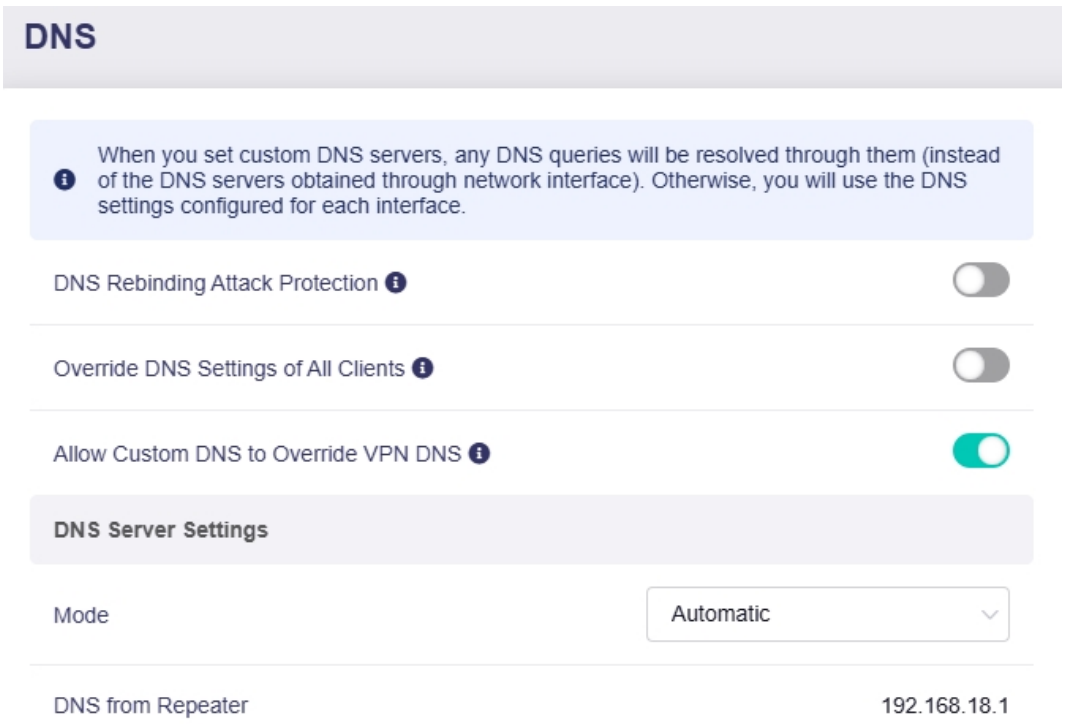


11.3 DNS

DNS (Domain Name System) è un servizio di rete che traduce nomi di dominio leggibili dall'uomo (ad esempio, www.google.com) in indirizzi IP riconoscibili dalle macchine (ad esempio, 142.250.185.142), consentendo ai dispositivi di connettersi a siti Web o servizi di destinazione.

Router Server DNS si riferisce al servizio DNS integrato nel router, che fornisce la traduzione del nome di dominio in IP per tutti i dispositivi collegati. Solitamente funziona in due modi: in primo luogo, ottiene automaticamente gli indirizzi DNS dalla rete upstream per fornire servizi di traduzione predefiniti; in secondo luogo, gli utenti possono configurare manualmente indirizzi DNS pubblici personalizzati (ad esempio, 8.8.8.8) sul pannello di amministrazione web del router per ottimizzare l'accesso alla rete o migliorare la sicurezza. Una volta configurato, tutti i dispositivi connessi utilizzeranno questo server DNS unificato per impostazione predefinita, eliminando la necessità di una configurazione DNS separata su ciascun dispositivo.

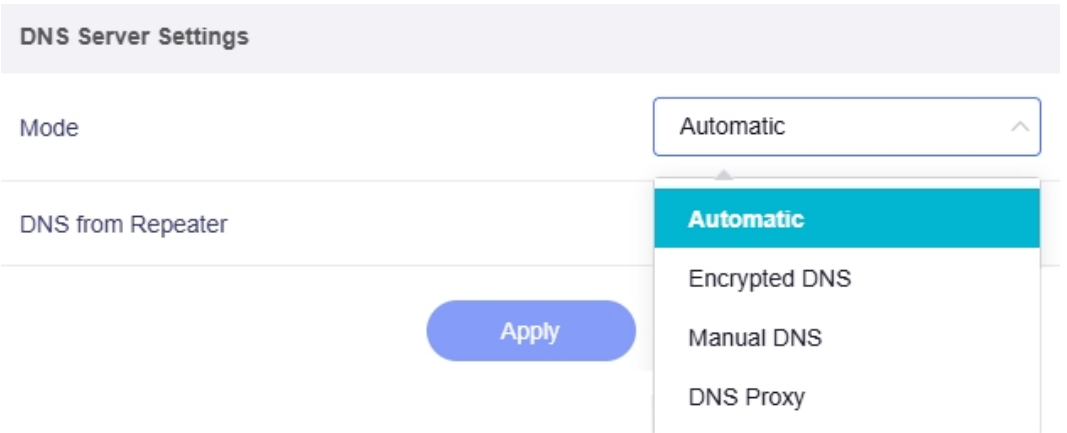
Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **DNS**. Questa pagina ti consente di configurare le impostazioni relative al DNS, incluse le opzioni di sicurezza, le modalità server e le regole di priorità DNS per diversi scenari di rete.



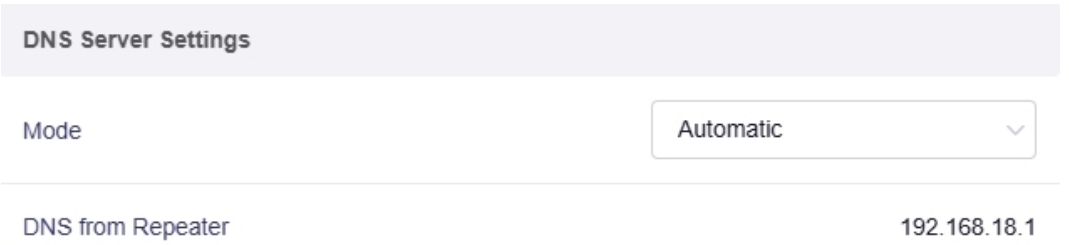
- **Protezione dagli attacchi di riassociazione DNS**: protegge dagli attacchi di rebinding DNS bloccando i tentativi dannosi di risoluzione DNS. Tieni presente che abilitarlo potrebbe causare un errore di ricerca DNS privato.
- **Sostituisci le impostazioni DNS di tutti i client**: se abilitato, tutti 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.
- **Consenti al DNS personalizzato di sovrascrivere il DNS VPN**: se abilitato, se hai impostato il DNS personalizzato, i pacchetti trasmessi attraverso il tunnel VPN utilizzeranno il DNS personalizzato per la risoluzione, anziché i server DNS dalla connessione VPN. Ciò garantisce che le regole di risoluzione DNS personalizzate vengano applicate normalmente quando si utilizza la VPN.

11.3.1 Impostazioni del server DNS

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

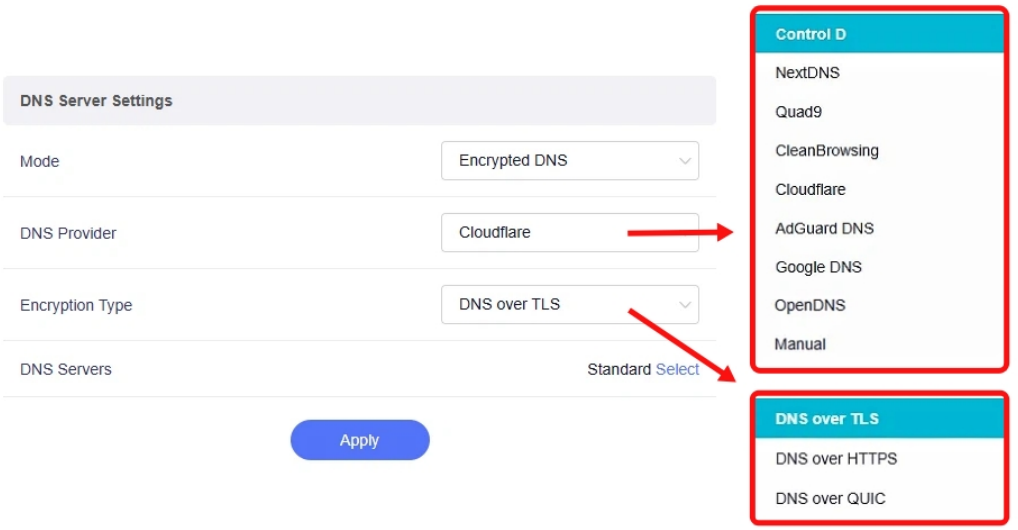


1. **Automatico**: se selezionato, il router otterrà automaticamente gli indirizzi del server DNS dalla rete upstream e li applicherà a tutti i dispositivi collegati.

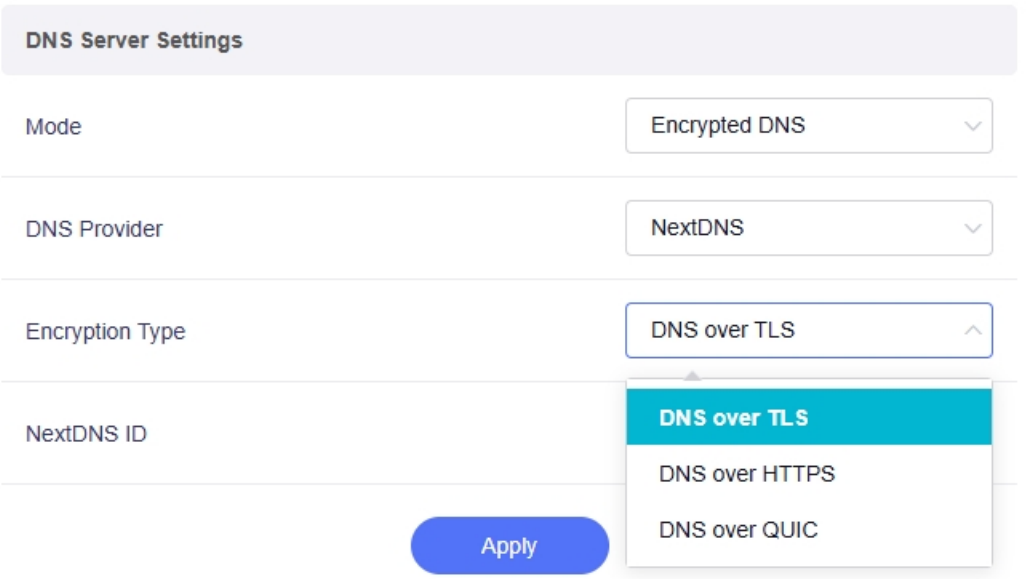


2. **DNS crittografato**: se selezionato, il router utilizzerà protocolli crittografati per elaborare le query DNS, proteggendo i dati di risoluzione da intercettazioni o manomissioni.

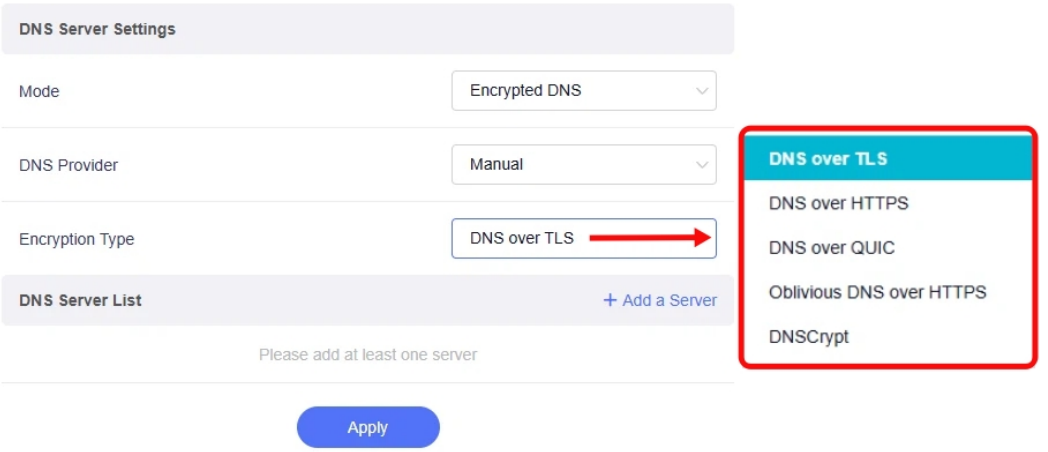
Supporta più provider DNS per la modalità DNS crittografato, inclusi Control D, NextDNS, Cloudflare,Quad9, CleanBrowsing, AdGuard DNS, Google DNS e OpenDNS. Seleziona prima il provider DNS. Le restanti opzioni cambieranno in base alla tua selezione.



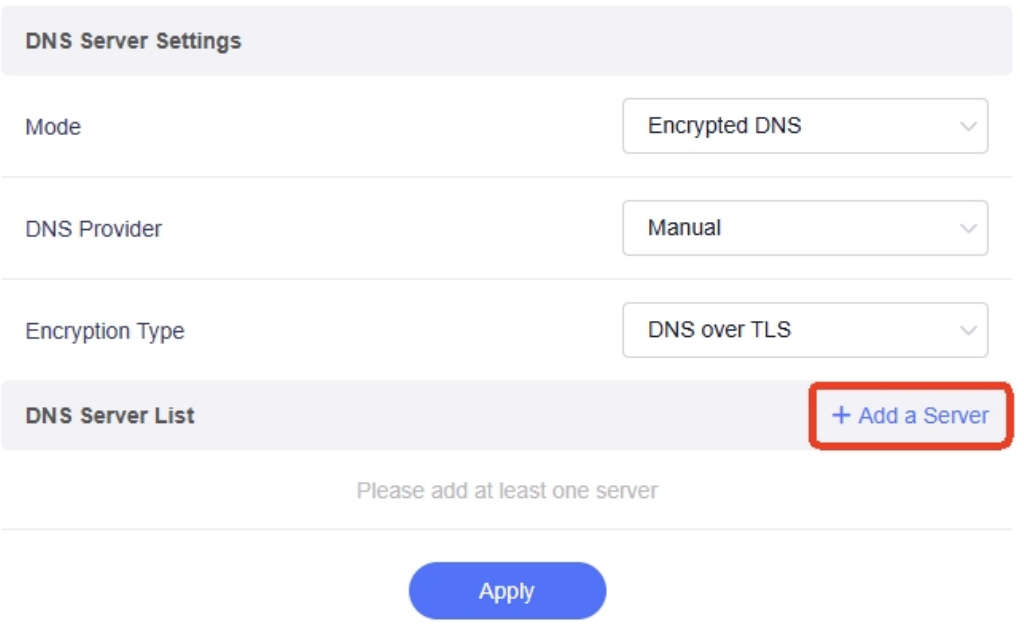
- Se selezioni un provider DNS specifico (ad esempio, NextDNS), scegli un tipo di crittografia tra DNS su TLS (DoT), DNS su HTTPS (DoH) e DNS su QUIC (DoQ). Tieni presente che DNS over QUIC (DoQ) è stato introdotto nel firmware v4.9 ed è disponibile solo quando si utilizza Control D, NextDNS o AdGuard DNS come provider DNS.



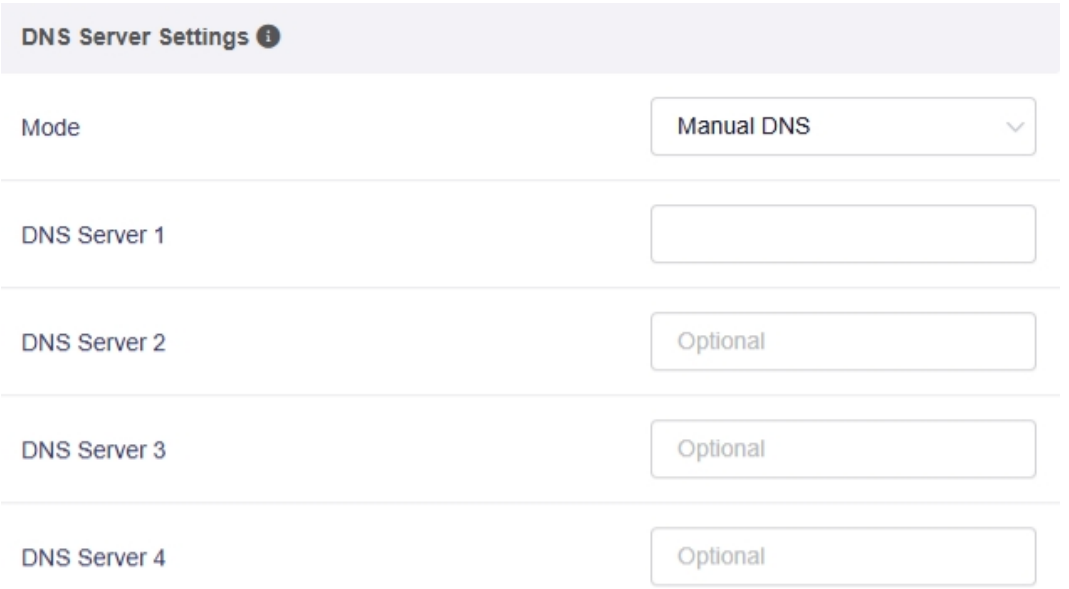
- Se selezioni Manuale come provider DNS, scegli un tipo di crittografia tra DNS su TLS (DoT), DNS su HTTPS (DoH), DNS su QUIC (DoQ), DNS inconsapevole su HTTPS e DNSCrypt.



Successivamente, fai clic su Aggiungi un server per aggiungere almeno un server DNS. Puoi inserire direttamente l'URL o il formato timbro del DNS crittografato. Per un elenco dei server pubblici, fare riferimento a https://dnscrypt.info/public-servers.

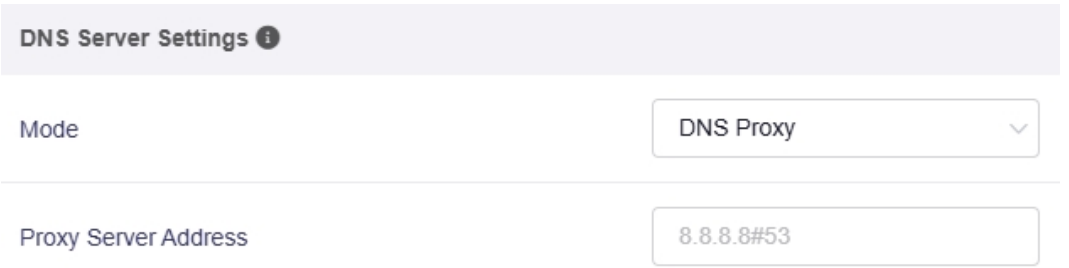


3. **DNS manuale**: se selezionato, puoi personalizzare i server DNS del router. Fare clic su Server DNS 1 e scegliere un server DNS dall'elenco a discesa. I restanti campi DNS verranno aggiornati automaticamente.



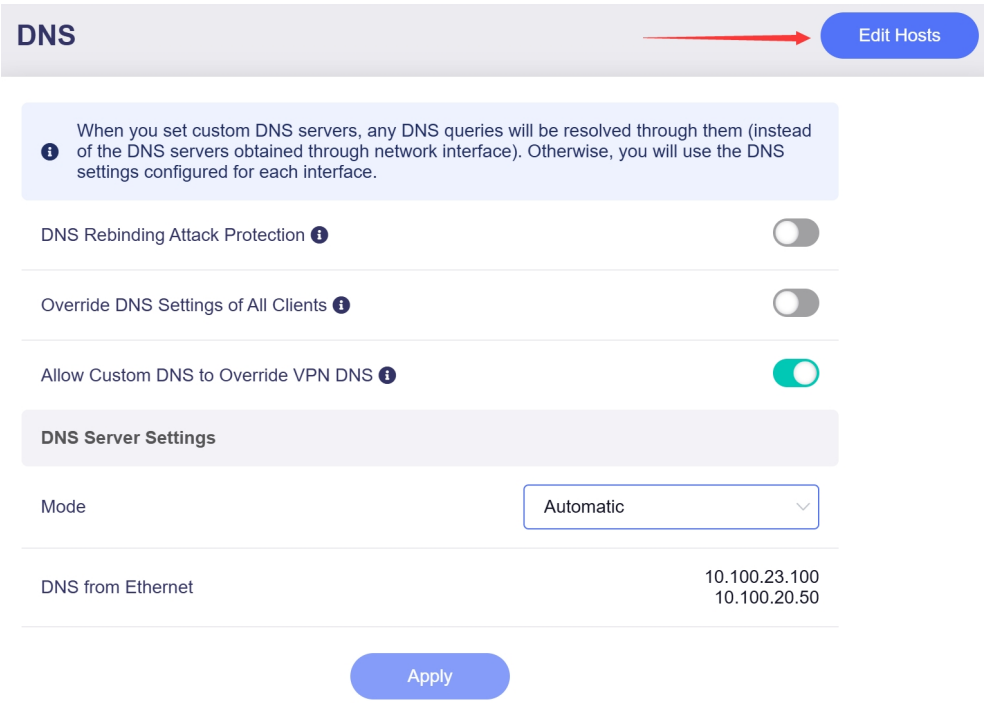
Nota: se è necessario utilizzare indirizzi IPv6 per il DNS manuale, abilitare prima IPv6 sul router.

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.

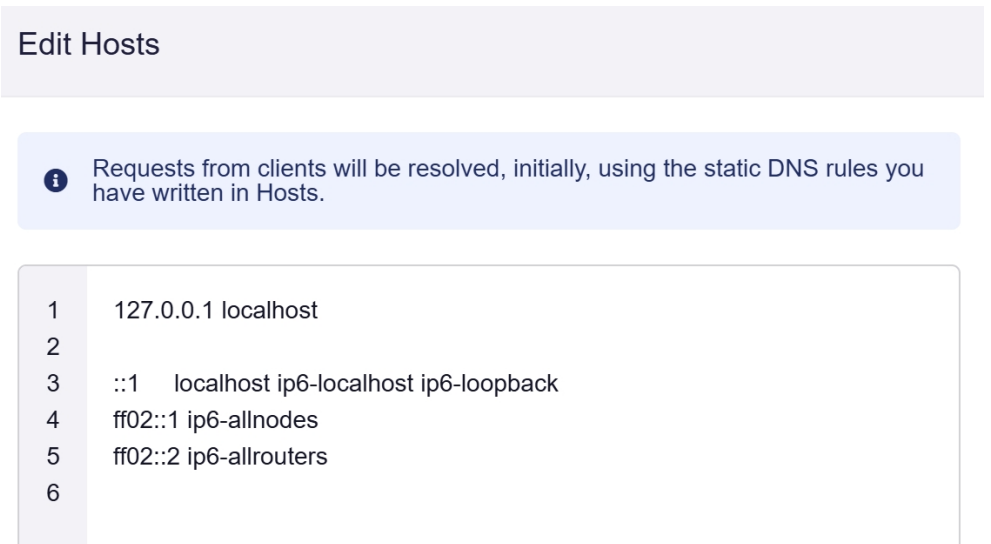


11.3.2 Modifica del file hosts

Se necessario, è possibile definire regole di risoluzione DNS statiche. Nella pagina DNS, fai clic su **Modifica del file hosts** nell'angolo in alto a destra.



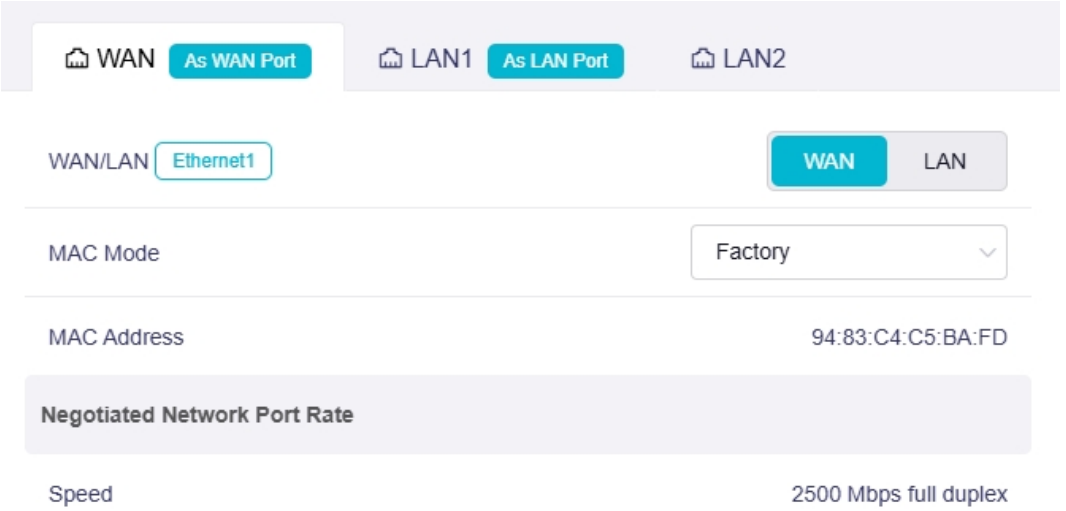
Le richieste dei client verranno risolte preferenzialmente utilizzando le regole DNS statiche scritte qui, consentendoti di mappare manualmente gli indirizzi IP sui nomi host (ad esempio, le voci predefinite come 127.0.0.1 localhost per il loopback locale) per il controllo personalizzato della risoluzione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



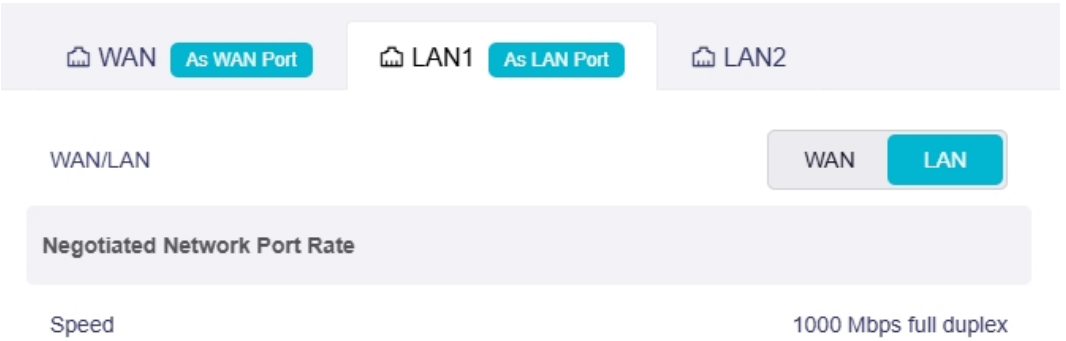
11.4 Porta Ethernet

Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Porta Ethernet**. Questa pagina ti consente di gestire le porte Ethernet del router.

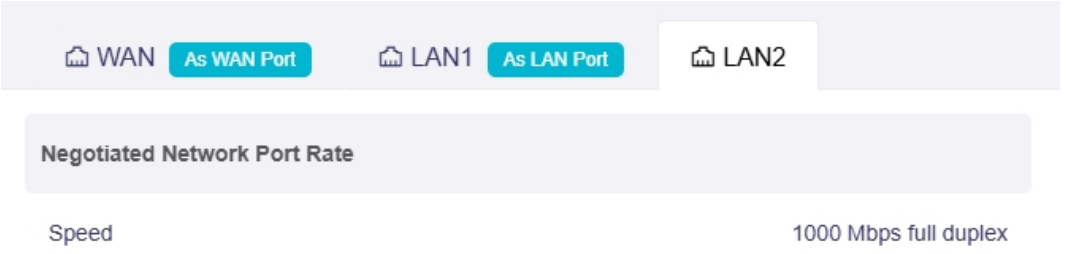
La sezione **WAN** mostra il ruolo della porta (WAN o LAN), l’ indirizzo MAC e la velocità negoziata.



La sezione **LAN 1** consente di passare dalla LAN 1 alla WAN. Puoi cambiare il ruolo della porta e controllare la velocità negoziata qui.



La sezione **LAN 2** mostra la velocità negoziata per la porta LAN.



Nota: la velocità negoziata per le porte WAN e LAN viene visualizzata solo quando è collegato un cavo Ethernet.

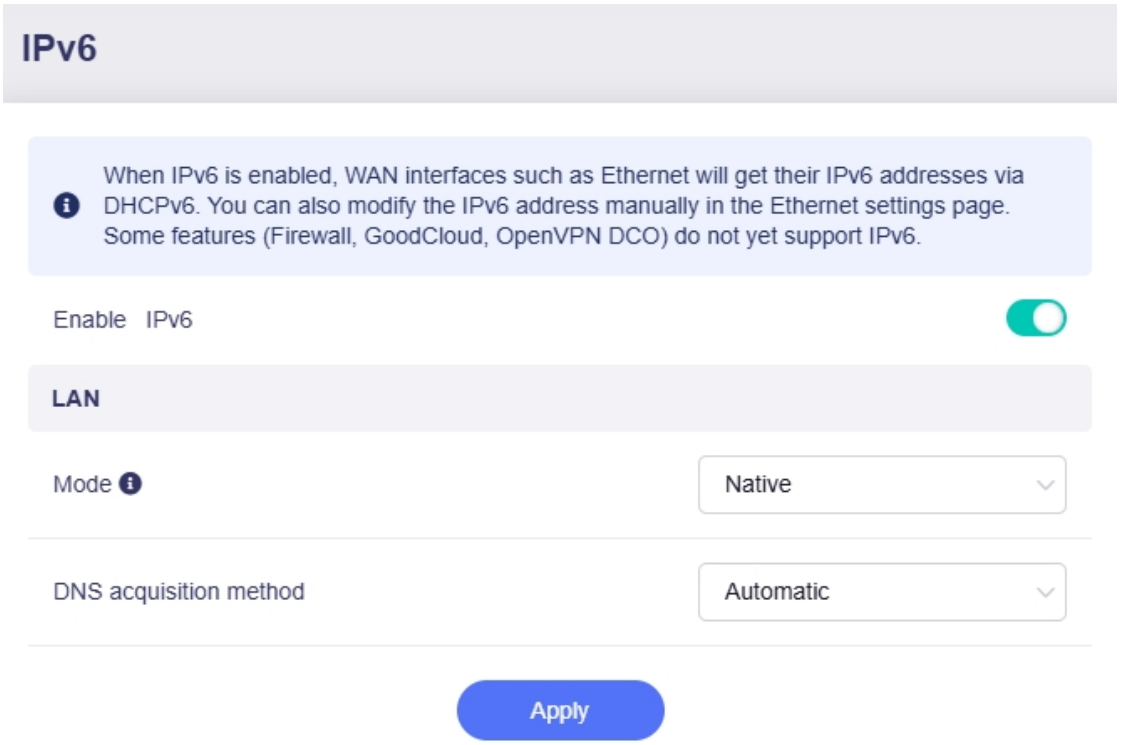
11.5 IPv6

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.

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

Attiva **Abilita IPv6**, seleziona la modalità per la rete principale e il metodo di acquisizione DNS, quindi fai clic su **Applica.**



11.5.1 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.

11.5.2 Metodo di acquisizione DNS

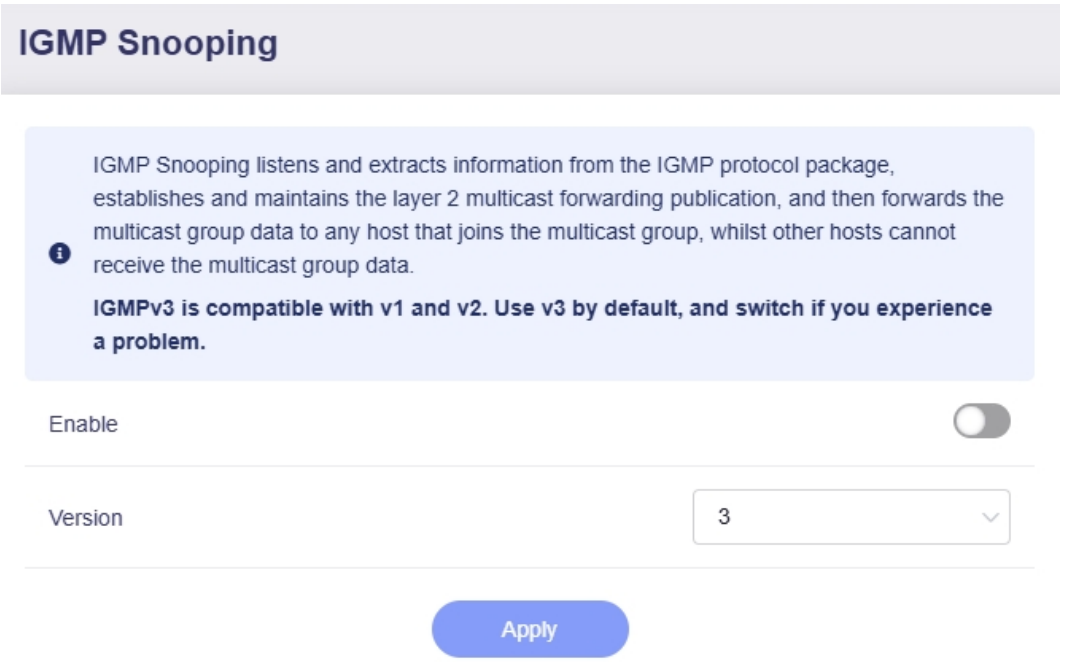
Determina il modo in cui il router ottiene gli indirizzi del server DNS IPv6. Sono disponibili due opzioni: Automatico e Manuale.

- **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.

11.6 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.

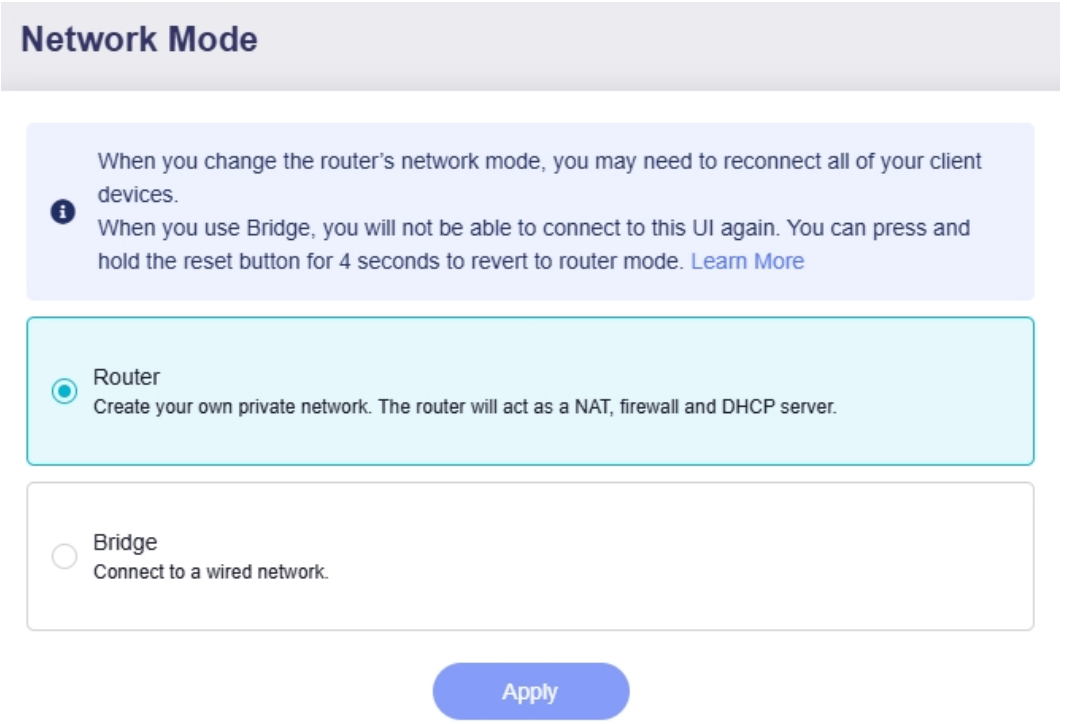
Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **IGMP Snooping**. Puoi abilitarlo per utilizzare la funzione multicast sul tuo router secondo necessità.



11.7 Modalità di rete

La modalità di rete si riferisce ai diversi ruoli operativi e funzionalità che un router può assumere per soddisfare le varie esigenze di implementazione 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. Brume 3 supporta due modalità: modalità Router e Bridge.



- **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.
- **Bridge**: consente al router di connettersi a una rete cablata e di funzionare come bridge tra i dispositivi di rete. In questa modalità, il router funziona essenzialmente come uno switch, inoltrando i dati tra i dispositivi connessi senza eseguire servizi NAT, firewall o DHCP. Ciò consente una comunicazione continua tra i dispositivi sulla stessa rete agendo come un semplice punto di connessione anziché come un gateway di rete.

Nota:

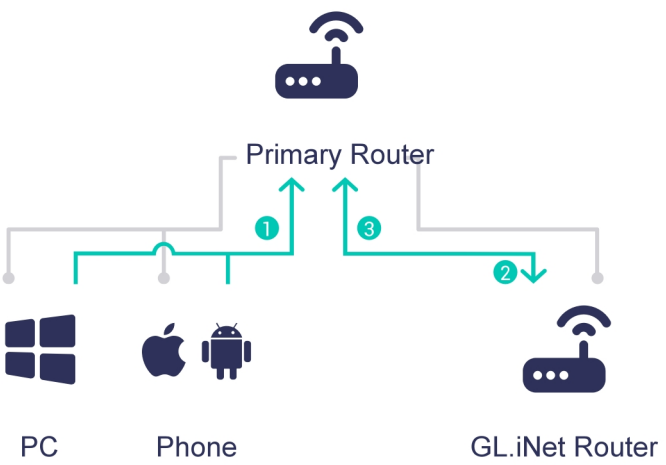
1. Quando la modalità di rete viene modificata, i dispositivi devono riconnettersi al router per garantire una connessione stabile.
2. **In modalità Bridge, non sarai in grado di accedere al pannello di amministrazione web utilizzando l'indirizzo IP originale**. È invece necessario accedere al router 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 Bridge, le seguenti funzionalità non saranno disponibili**: Controllo degli accessi (Lista consentita e Blocklist), AstroWarp, VPN, AdGuard Home, Controllo parentale, ZeroTier, Tailscale, Port forwarding, Multi-WAN, Server DHCP, Prenotazione indirizzi, DNS, Porta Ethernet, IPv6, Gateway drop-in, IGMP Snooping, Accelerazione di rete, Impostazioni NAT.

11.8 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 secondo necessità.



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.

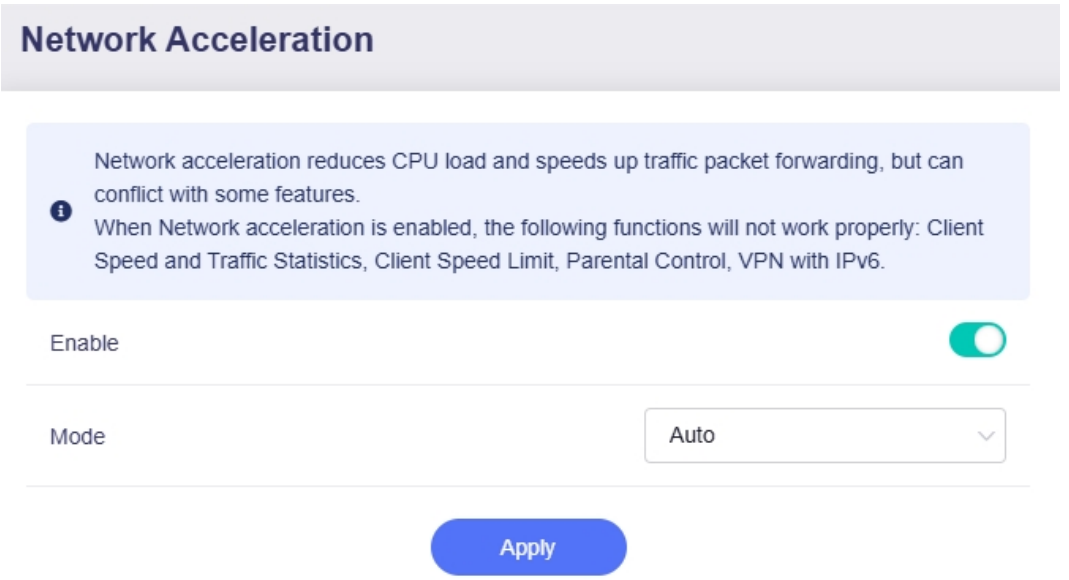
- **Le linee verdi** rappresentano il percorso sequenziale di trasmissione dei dati quando Gateway drop-in è attivo, con le frecce numerate che indicano l'ordine del flusso di traffico:
    1. Il traffico dai dispositivi client viene prima instradato al router primario;
    2. Il router primario inoltra 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.

Puoi abilitare Gateway drop-in per tutti o dispositivi specifici collegati al router principale. Fare riferimento a questo collegamento per ulteriori istruzioni.

11.9 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 l'accelerazione di rete e selezionare la modalità di accelerazione tra Automatico, Accelerazione hardware e Accelerazione software.



- **Automatico**: passa automaticamente tra le due modalità di accelerazione in base all'utilizzo effettivo.
- **Accelerazione hardware**: questa modalità solitamente funziona su Ethernet e Ripetitore (quest'ultimo non è disponibile su Brume 3). 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 (WAN/LAN cablate) 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.
- **Accelerazione software**: questa modalità funziona su cellulare. Si basa sulla CPU generale del router abbinata a kernel o driver ottimizzati (ad esempio SWNAT). Funziona sull'accesso cellulare (4G/5G), in genere lo scenario principale in cui l'accelerazione hardware non è disponibile, offrendo una forte compatibilità e supporto per protocolli complessi. Sebbene flessibile, potrebbe riscontrare colli di bottiglia della CPU in caso di

carichi con larghezza di banda elevata, soprattutto quando si eseguono funzionalità avanzate come DPI, QoS o port forwarding.

Nota: quando l'accelerazione di rete è abilitata, le seguenti funzioni non funzioneranno correttamente: statistiche sulla velocità del client, statistiche sul traffico, limite di velocità, Controllo parentale, VPN con IPv6, statistiche dei dati, filtro dei contenuti, QoS e SQM.

Capitolo 12

Controllo del traffico

Questo capitolo introduce le funzionalità di controllo del flusso, fornendo strumenti dedicati per il traffico di rete e la gestione dei contenuti.

12.1 Motore DPI

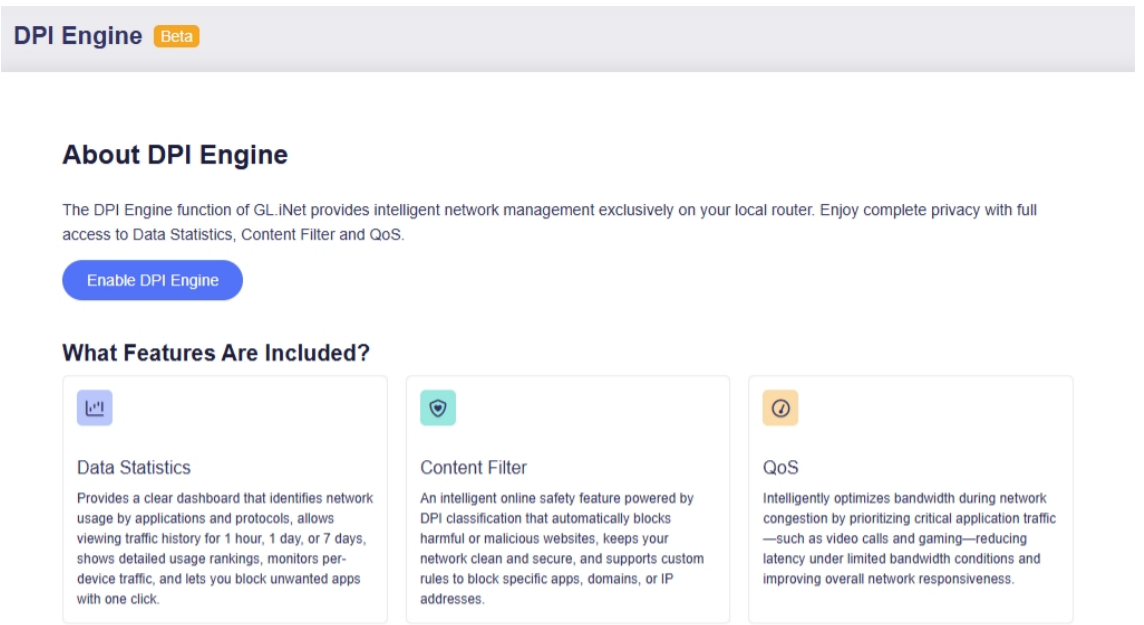
DPI (Deep Packet Inspection) è una tecnologia fondamentale per la gestione intelligente della rete. A differenza dei router tradizionali che identificano solo gli indirizzi di origine e di destinazione, DPI esegue un'analisi approfondita dei carichi utili dei pacchetti e identifica accuratamente applicazioni e siti Web utilizzando una libreria di corrispondenza delle funzionalità, consentendo la classificazione e il controllo granulari del traffico.

GL.iNet DPI Engine viene eseguito localmente sul tuo router per offrire una gestione della rete intelligente con completa privacy. Fornisce accesso completo alle statistiche del traffico, al filtraggio dei contenuti e alla QoS per un controllo completo del traffico. Integrato con Netify, GL.iNet DPI utilizza il database delle firme online aggiornato automaticamente per fornire un controllo della rete affidabile, accurato ed efficiente.

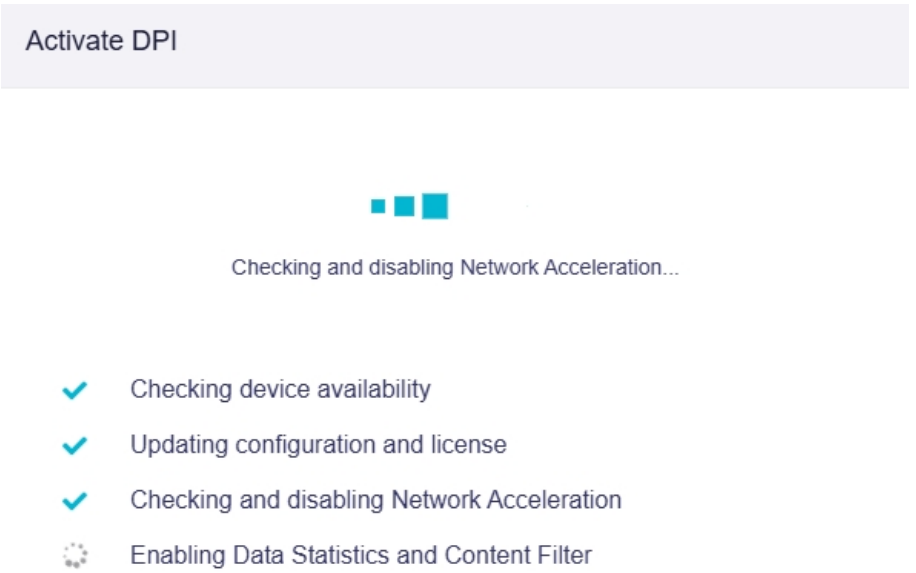
Nota:

1. Quando il router è in modalità Gateway drop-in, le funzionalità DPI (incluse statistiche dei dati, filtro contenuti e QoS) e SQM non avranno effetto.
2. Quando DPI è abilitato, Accelerazione di rete verrà disabilitato automaticamente per garantire prestazioni stabili.

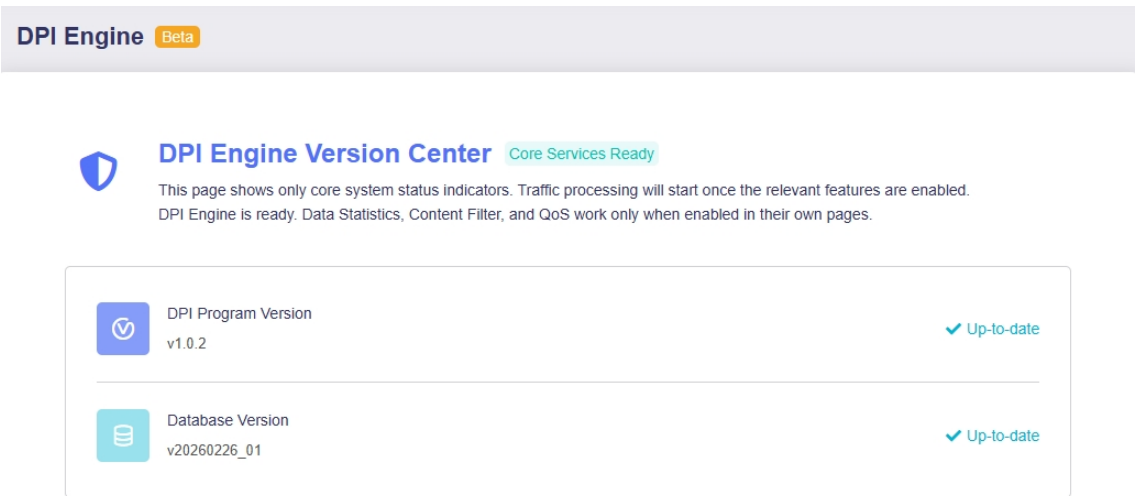
Accedi al pannello di amministrazione web del router e vai a **CONTROLLO TRAFFICO** > **DPI Engine. Fai clic su Abilita motore DPI**.



Nella finestra pop-up, leggi e accetta i Termini di servizio e l'Informativa sulla privacy, quindi fai clic su **Applica**. Il router avvierà quindi l'inizializzazione DPI. Disabiliterà Accelerazione di rete, abilitando al contempo **le statistiche dei dati** e **il filtro dei contenuti**.



Una volta attivato, verrai indirizzato al **Centro versioni del motore DPI**, dove potrai visualizzare la versione del programma DPI e la versione del database. Puoi aggiornare il database qui quando è disponibile una versione più recente del database.



Nota: questa pagina visualizza solo gli indicatori di stato del sistema principale. L'elaborazione del traffico inizierà una volta abilitate le funzionalità pertinenti.

12.2 Statistiche dei dati

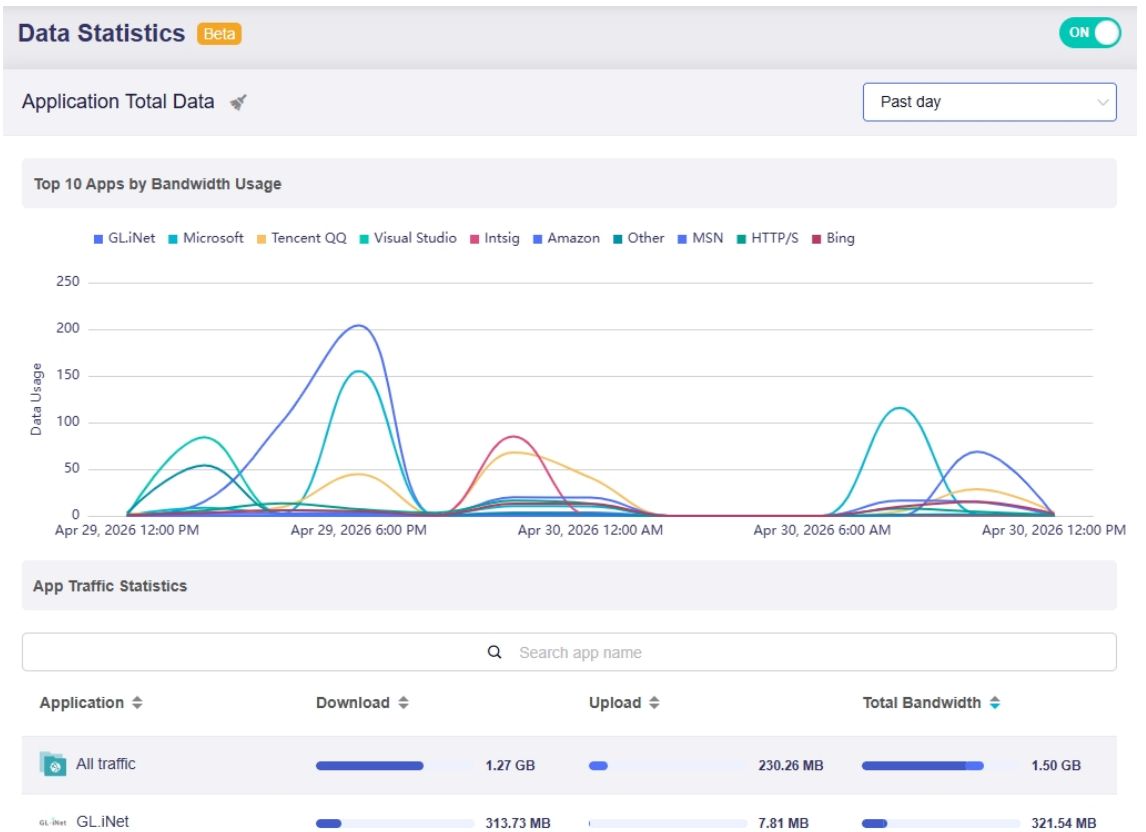
Statistiche dei dati offre una dashboard intuitiva del traffico che identifica l'utilizzo della rete per applicazione e protocollo. Consente di visualizzare l'andamento storico nell'ultima ora, nell'ultimo giorno e negli ultimi 7 giorni, mostra le classifiche di utilizzo, monitora il traffico di ciascun dispositivo e permette di bloccare le app indesiderate con un clic.

Nota:

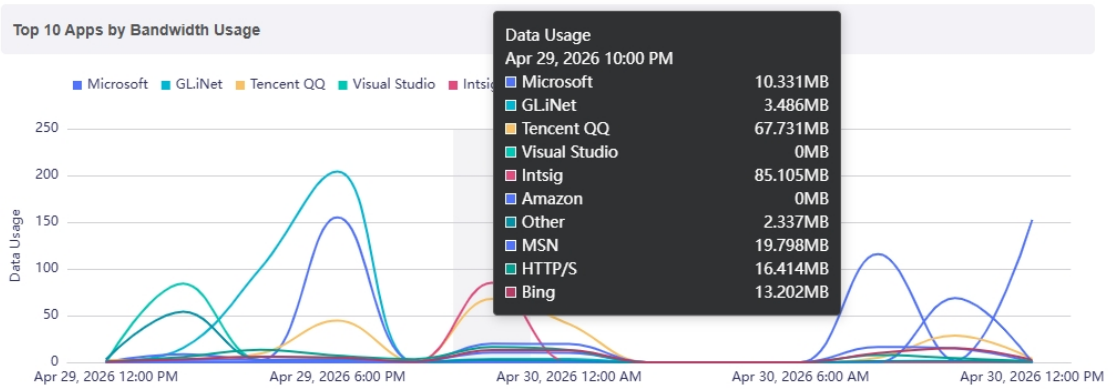
1. Le statistiche dei dati non avranno effetto quando il router è in modalità Gateway drop-in.
2. Le statistiche dei dati non possono funzionare con Accelerazione di rete. L'abilitazione delle statistiche dei dati disabiliterà automaticamente Accelerazione di rete per garantire prestazioni stabili.

12.2.1 Configurazione rapida

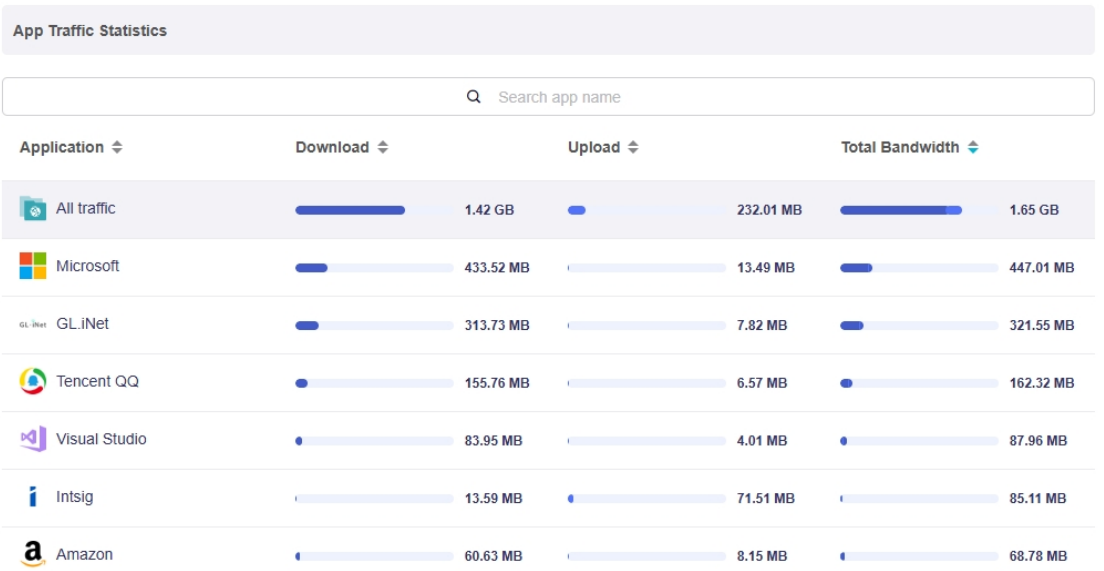
Accedi al pannello di amministrazione web del router e vai a **CONTROLLO TRAFFICO** > **Statistiche dati**. Attiva l'interruttore in alto a destra per visualizzare **i dati totali dell'applicazione**.



- **Le 10 app con il maggiore utilizzo della larghezza di banda**: presenta un grafico di tendenza basato sul tempo (ad esempio, per l'ultimo giorno) per mostrare il consumo di larghezza di banda delle principali applicazioni 10 nel periodo selezionato. Passa il mouse sul grafico per visualizzare l'utilizzo dei dati delle principali app 10 che consumano larghezza di banda in un momento specifico.



- **Statistiche sul traffico delle app**: visualizza metriche dettagliate sul traffico per ciascuna applicazione, inclusi i dati di download, caricamento e larghezza di banda totale. Cerca app specifiche nella barra di ricerca, se necessario. Puoi fare clic sulla freccia di ordinamento accanto all'intestazione della colonna per ordinare l'elenco in ordine crescente o decrescente.

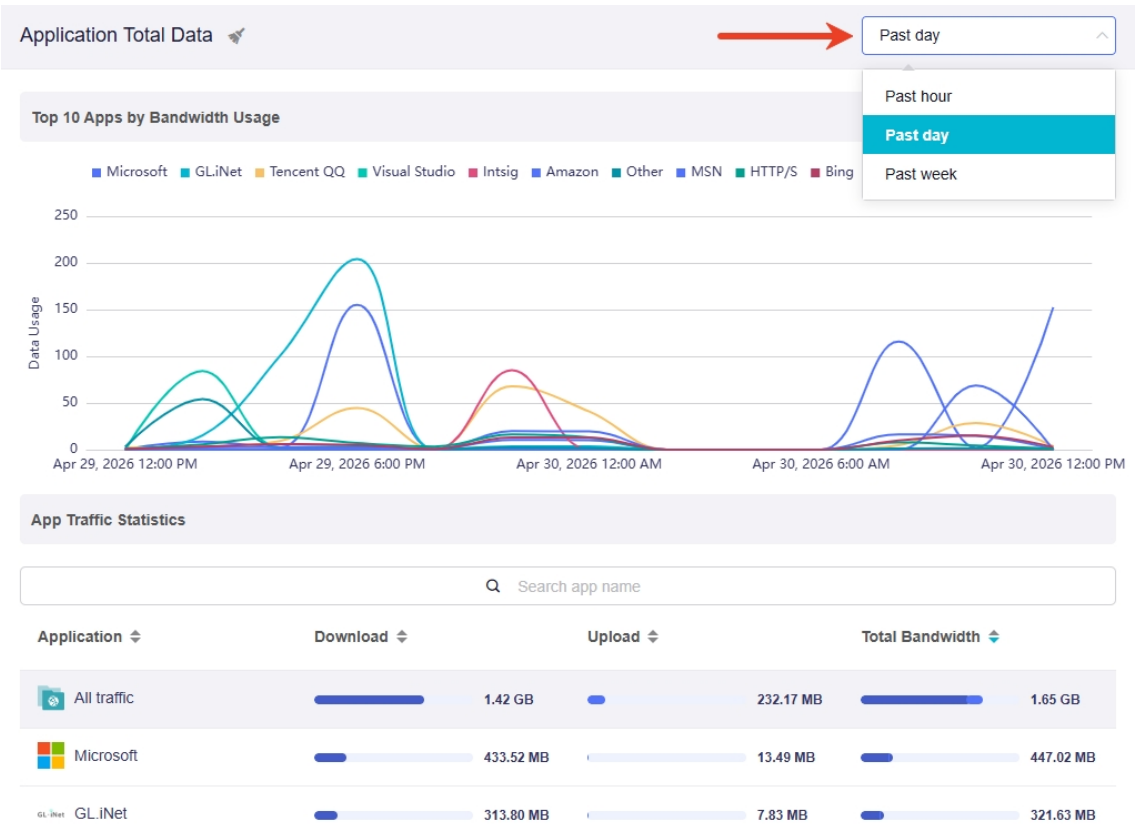


12.2.2 Regole di archiviazione dei dati

1. Le statistiche sul traffico vengono salvate nella RAM ogni 15 secondi e archiviate nella flash ogni 1 ora. Vengono evitate frequenti scritture flash per proteggere la durata della memoria flash.
2. Un riavvio graduale non causerà la perdita di dati. Il sistema scrive innanzitutto i dati dalla RAM alla memoria flash prima di riavviarsi.
3. Un riavvio forzato (scollegamento e ricollegamento dell'alimentazione) o un aggiornamento del firmware (mantenimento delle impostazioni) può comportare la perdita di dati fino all'ora più recente.

12.2.3 Cambia intervallo di tempo

Puoi cambiare l'intervallo di tempo tra Ultima ora, Ultimo giorno e Ultima settimana, se necessario.

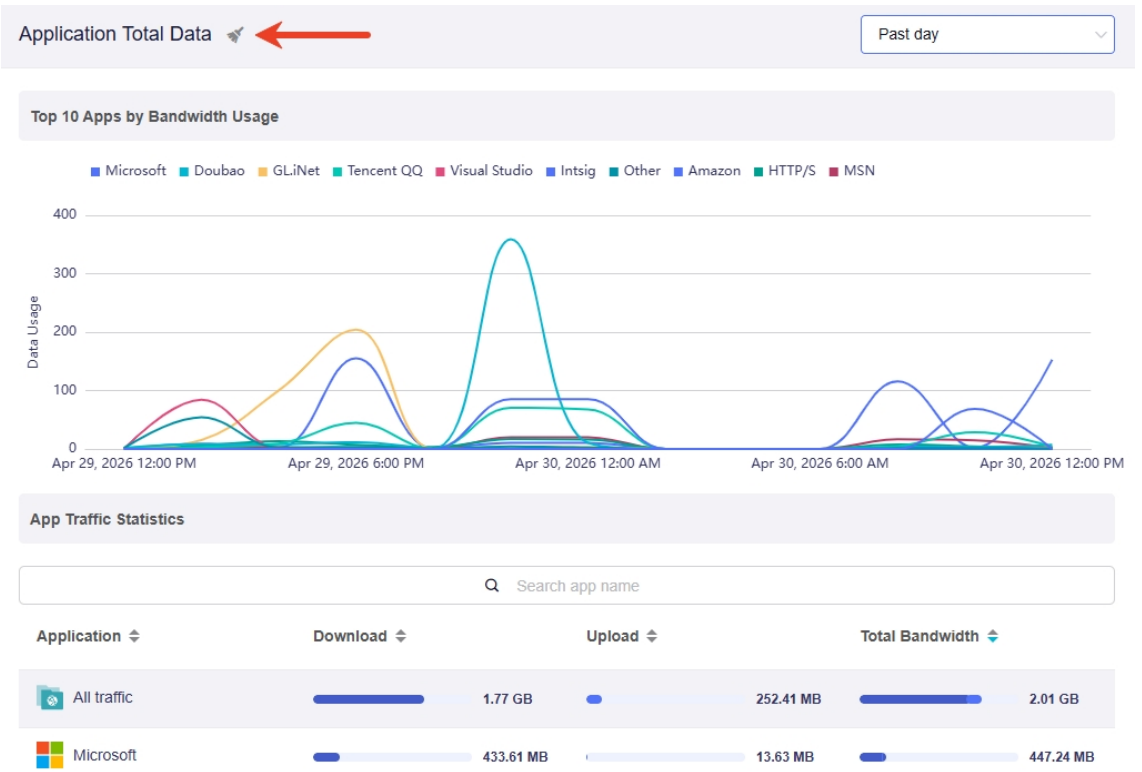


L'intervallo di tempo scelto determina la modalità di visualizzazione dei dati:

- **Per uno sguardo più attento (ad esempio, l'ora passata)**: il grafico mostra fluttuazioni dettagliate e in tempo reale. I picchi sono più alti e i cali più ripidi, rendendo facile individuare picchi improvvisi nell'utilizzo della larghezza di banda.
- **Per una panoramica ampia (ad es. Giorno passato o Settimana passata)**: il grafico condensa i dati in una sequenza temporale più lunga. Le curve diventano più morbide, mostrando l'andamento generale del traffico piuttosto che ogni piccolo cambiamento.

12.2.4 Cancella statistiche

Fai clic sull'icona della scopa nell'angolo in alto a sinistra per cancellare le statistiche, se necessario.



Dopo la cancellazione, la pagina non visualizzerà alcun dato. Attendi un attimo affinché le nuove statistiche vengano compilate.

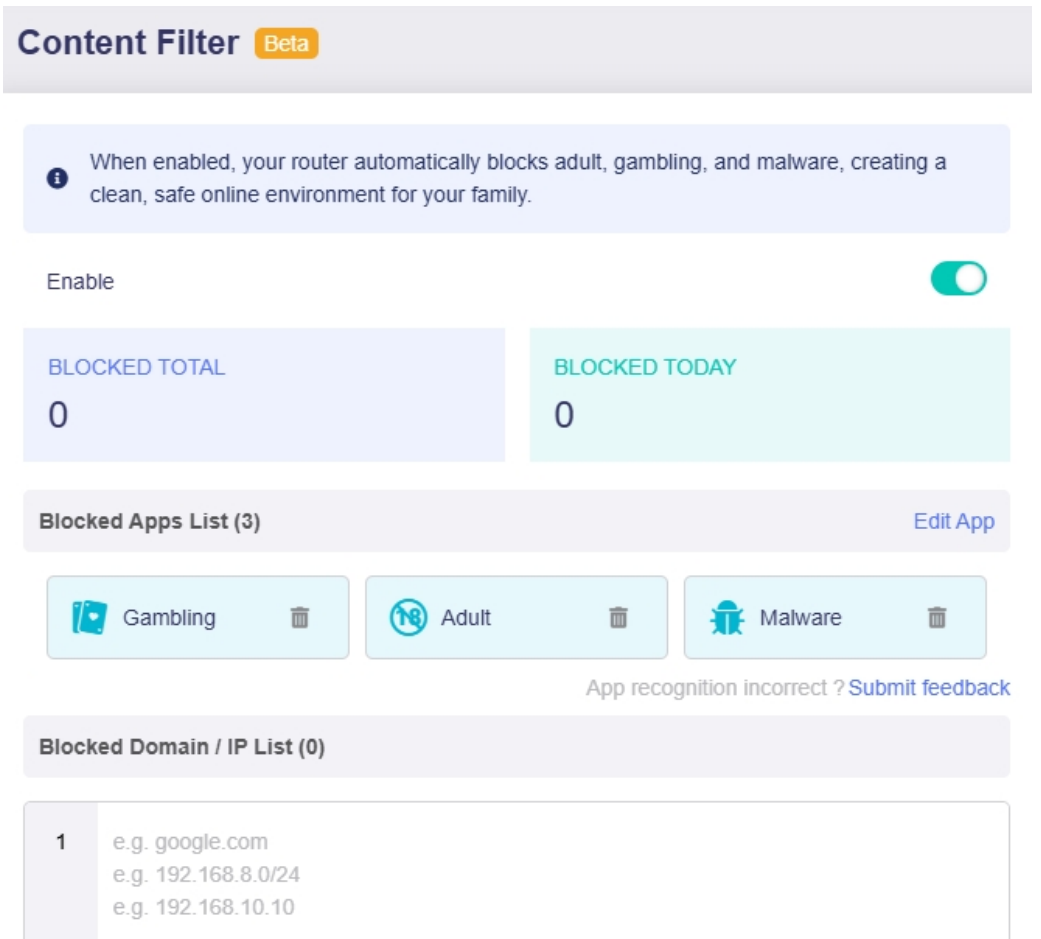
12.3 Filtro dei contenuti

Il filtro contenuti è una funzionalità di sicurezza online intelligente basata sulla classificazione DPI. Blocca automaticamente i siti Web dannosi per mantenere la tua rete pulita e sicura e supporta anche regole personalizzate per bloccare app, domini o indirizzi IP specifici.

Nota:

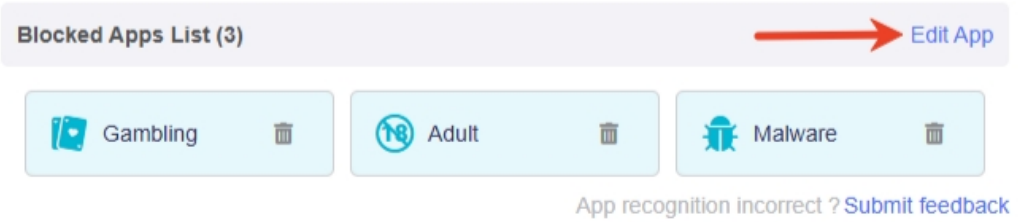
1. Il filtro dei contenuti non avrà effetto quando il router è in modalità Gateway drop-in.
2. Il filtro contenuti non può funzionare con Accelerazione di rete. L'abilitazione del filtro contenuti disabiliterà automaticamente Accelerazione di rete per garantire prestazioni stabili.

Accedi al pannello di amministrazione web del router e vai a **CONTROLLO TRAFFICO** > **Filtro dei contenuti**.
Attiva l'interruttore nell'angolo in alto a destra, personalizza il contenuto bloccato, quindi fai clic su **Applica**.

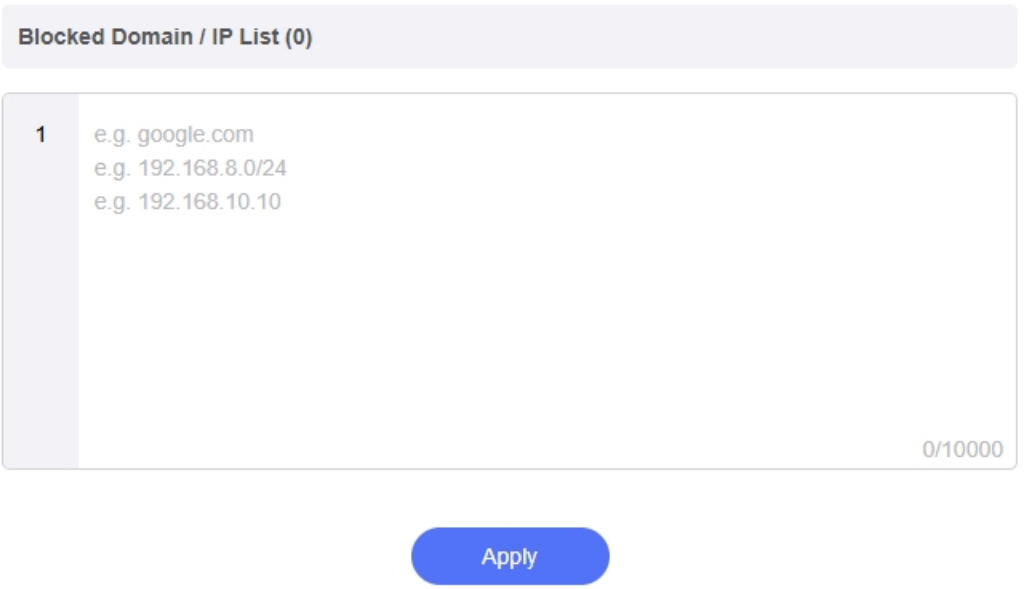


Questa pagina è composta da due parti:

- **Elenco delle app bloccate**: questa sezione include tre categorie preselezionate: giochi a distanza, per adulti e malware. Se abilitato, qualsiasi sito Web, servizio o app relativo a queste tre categorie verrà bloccato. Se necessario, puoi fare clic su **Modifica app** per aggiungere altre categorie (ad esempio Giochi, Social media, Shopping).



- **Elenco domini/IP bloccati**: questa sezione consente di inserire manualmente domini specifici (ad esempio google.com), intervallo CIDR (ad esempio 192.168.8.0/24) o indirizzi IP (ad esempio 192.168.10.10) per bloccarne l'accesso. L'elenco supporta fino a voci 10000.
  Inserisci i domini o gli indirizzi IP che desideri bloccare, quindi fai clic su **Applica**.



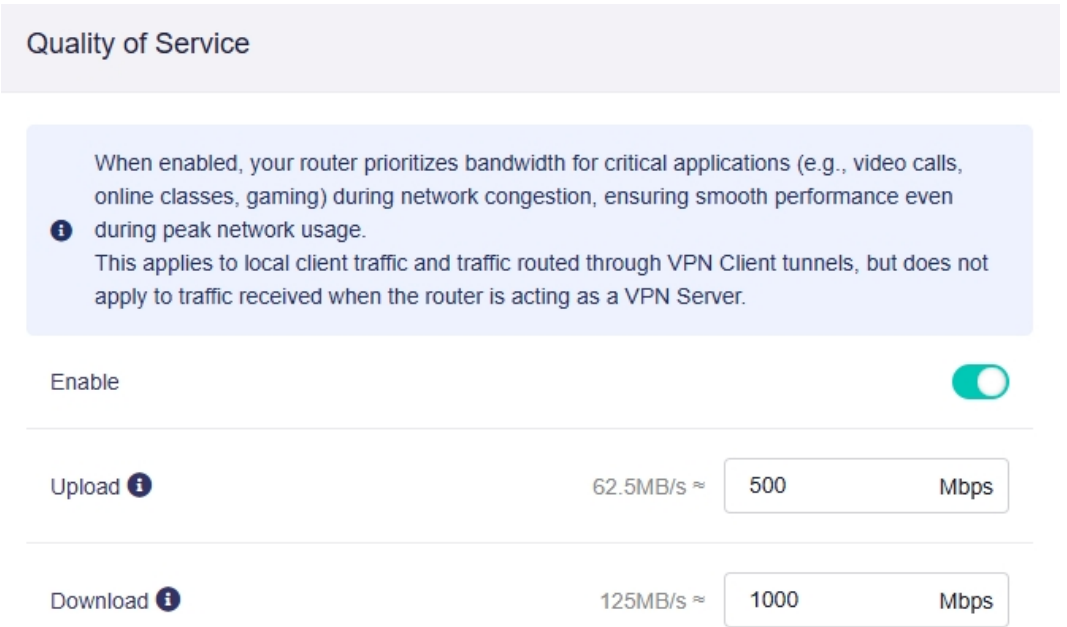
12.4 QoS

QoS (Quality of Service) ottimizza l'allocazione della larghezza di banda dando priorità al traffico sensibile alla latenza come videochiamate e giochi durante la congestione della rete, riducendo la latenza e migliorando le prestazioni complessive della rete.

Nota:

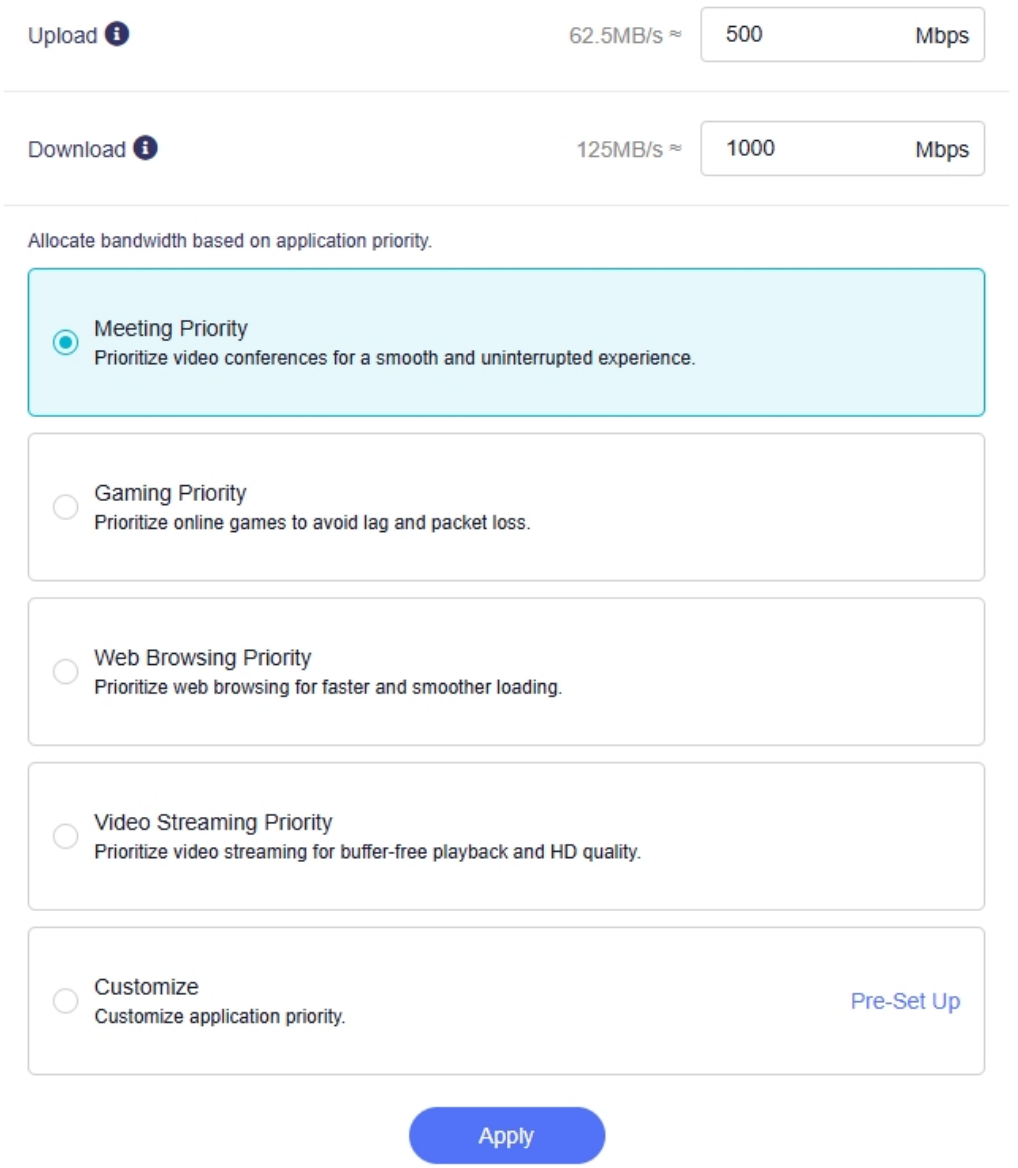
1. Questa funzionalità influisce solo sul traffico che passa attraverso il router quando funziona come gateway, incluso il traffico locale client e il traffico client VPN. Non si applica al traffico in entrata quando il router funge da server VPN.
2. QoS non avrà effetto quando il router è in modalità Gateway drop-in.
3. QoS e SQM non possono essere abilitati contemporaneamente.
4. QoS non può funzionare con Accelerazione di rete. L'abilitazione di QoS disabiliterà automaticamente Accelerazione di rete per garantire prestazioni stabili.

Accedi al pannello di amministrazione web del router, vai su **CONTROLLO TRAFFICO** > **QoS** e abilitalo. Imposta le velocità massime di upload e download (intervallo di input: 1-10000) per la pianificazione del traffico. Abbinali alla tua effettiva larghezza di banda Internet per ottenere i migliori risultati.



Suggerimento: i valori immessi nel campo di immissione sono in **Mbps** (megabit al secondo). I MB/s equivalenti (megabyte al secondo) vengono visualizzati come riferimento.

Quindi imposta le priorità per le diverse applicazioni. Il router allocherà la larghezza di banda di conseguenza.



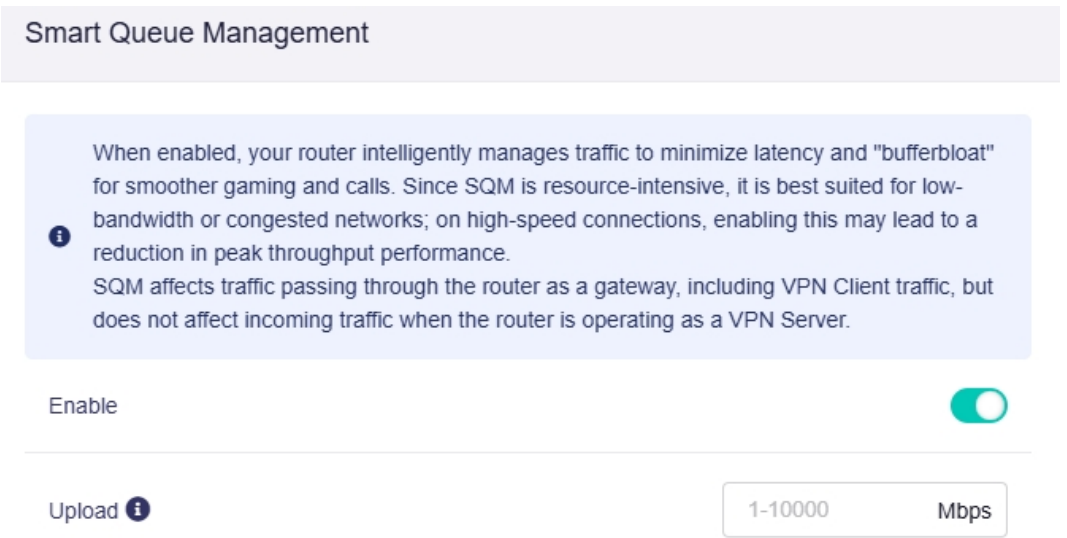
12.5 SQM

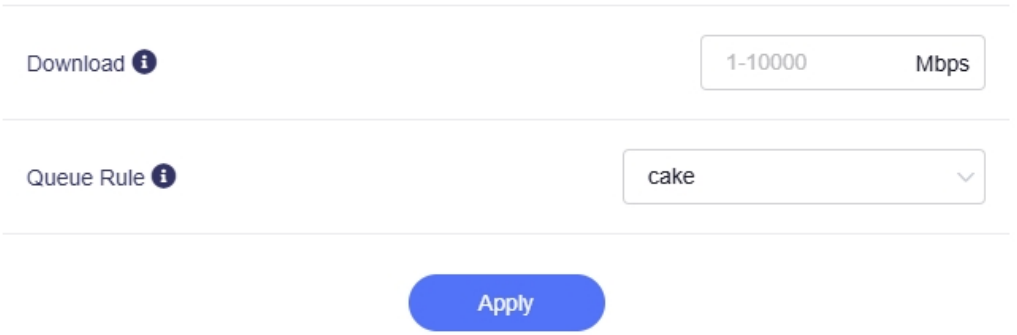
SQM (Smart Queue Management) gestisce in modo intelligente il traffico di rete del router per ridurre al minimo la latenza e il "bufferbloat", garantendo giochi e chiamate vocali più fluidi.

Nota:

1. Questa funzionalità influisce solo sul traffico che passa attraverso il router quando funziona come gateway, incluso il traffico locale client e il traffico client VPN. Non si applica al traffico in entrata quando il router funge da server VPN.
2. Poiché SQM richiede molte risorse, funziona meglio per reti con larghezza di banda ridotta o congestionate. Abilitarlo su connessioni ad alta velocità può ridurre il picco di throughput.
3. SQM non avrà effetto quando il router è in modalità Gateway drop-in.
4. SQM e QoS non possono essere abilitati contemporaneamente.
5. SQM non può funzionare con Accelerazione di rete. L'abilitazione di SQM disabiliterà automaticamente Accelerazione di rete per garantire prestazioni stabili.

Accedi al pannello di amministrazione web del router, vai su **CONTROLLO TRAFFICO** > **SQM** e abilitalo. Imposta prima la velocità massima di upload e download (intervallo di input: 1-10000) per la pianificazione del traffico. Abbinali alla tua effettiva larghezza di banda Internet per ottenere i migliori risultati.





Per **la regola di accodamento** sono disponibili due opzioni:

- **cake**: modellazione del traffico intelligente e automatica con controllo generale della latenza superiore (consigliato).
- **fq_codel**: accodamento semplice ed efficiente con riduzione della latenza di base.

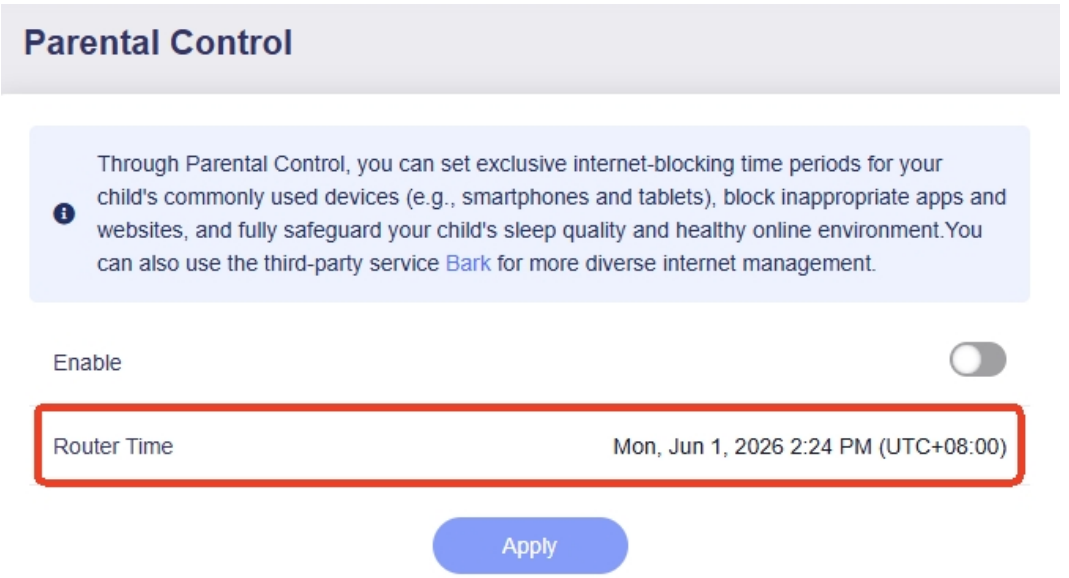
Suggerimento: una differenza tra le impostazioni QoS e SQM è che QoS consente di impostare le priorità dell'applicazione, con il router che alloca la larghezza di banda di conseguenza; mentre SQM ti consente di selezionare una regola di coda.

12.6 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.

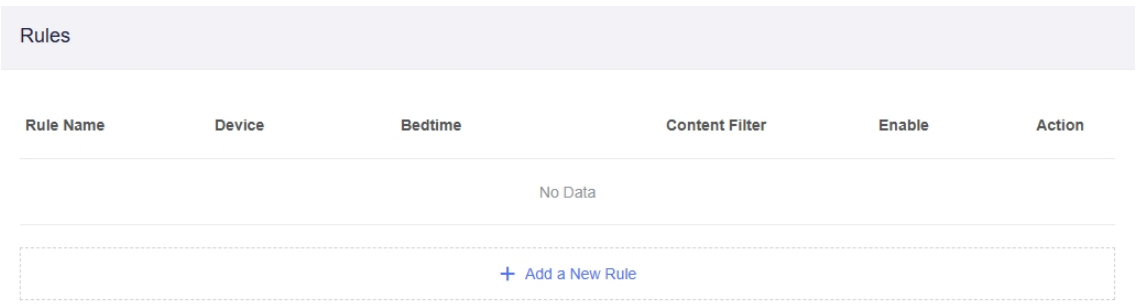
Segui i passaggi seguenti per impostare il controllo parentale.

1. Accedi al pannello di amministrazione web del router e vai su **CONTROLLO TRAFFICO** -> **Controllo parentale**. Assicurati che l'orario del router sia accurato.

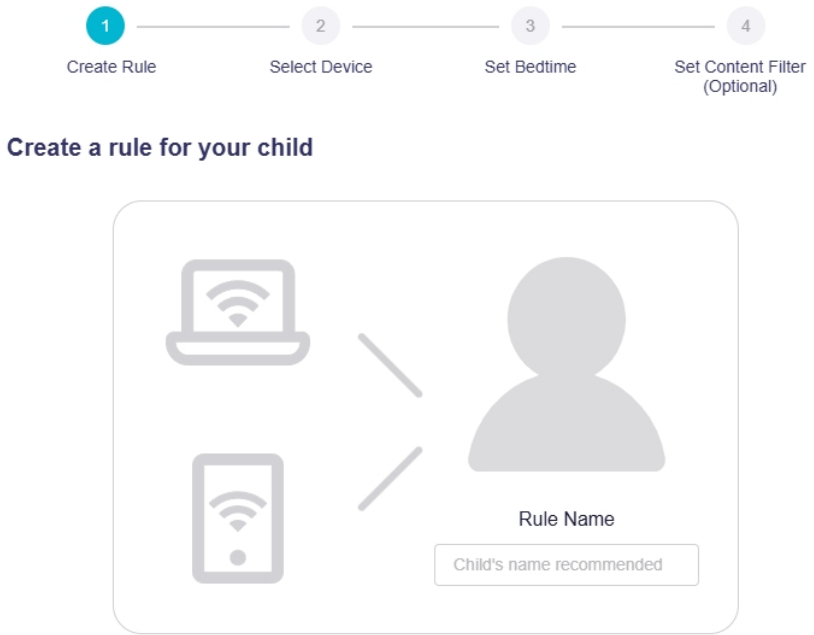


   In caso contrario, vai su **SISTEMA** -> **Fuso orario** per sincronizzarlo prima.

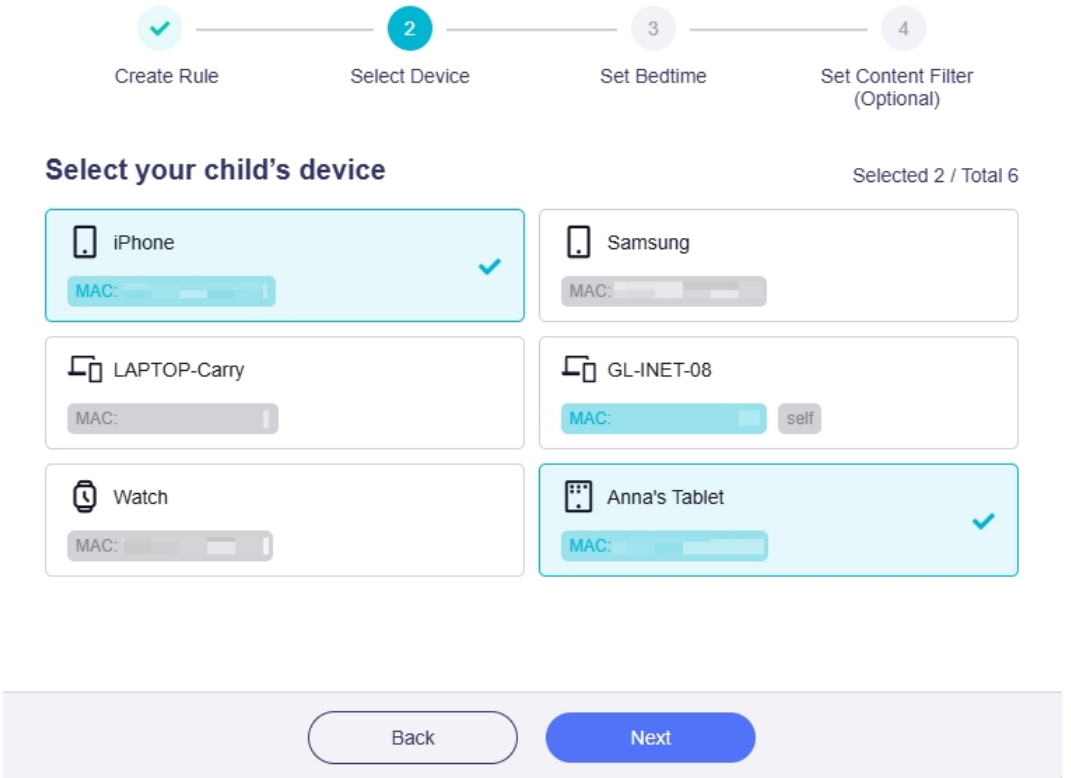
2. Abilita il controllo parentale e fai clic su **Applica**.
3. Vedrai un elenco di regole come segue. Fai clic su **Aggiungi una nuova regola**.



4. Nella finestra pop-up, crea una regola e imposta un nome personalizzato, quindi fai clic su **Avanti**.

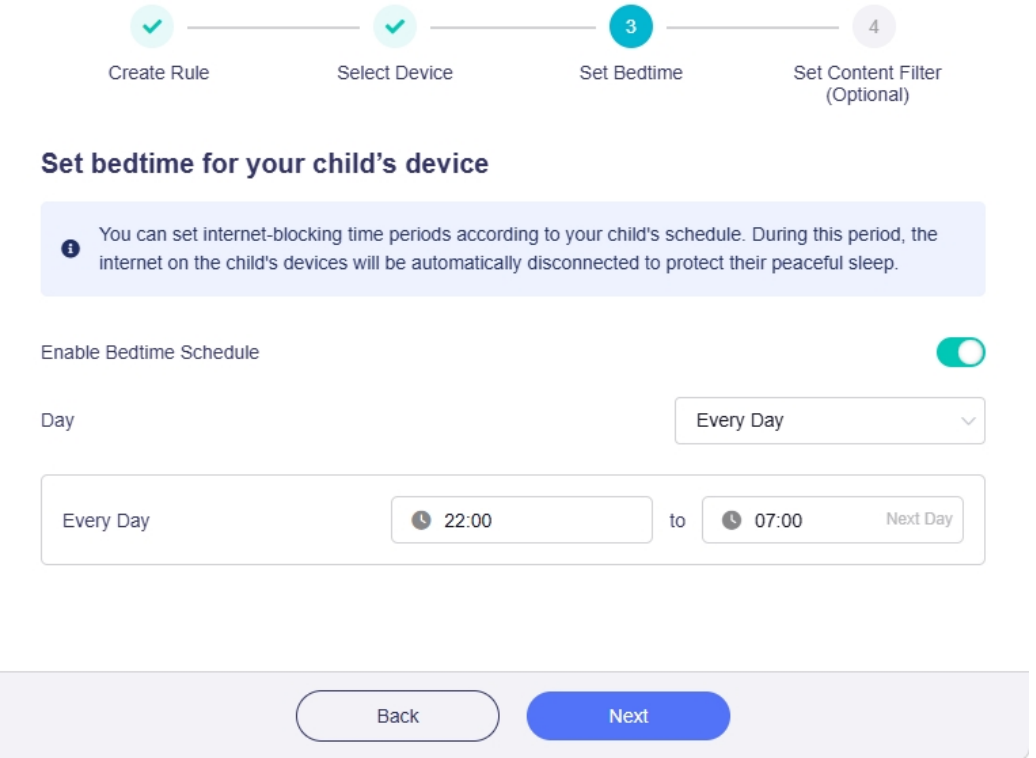


5. Seleziona il dispositivo di tuo figlio, quindi fai clic su **Avanti**.
   I dispositivi verranno visualizzati in questa pagina solo se sono collegati al router. Il ciano indica lo stato online, mentre il grigio indica lo stato offline.



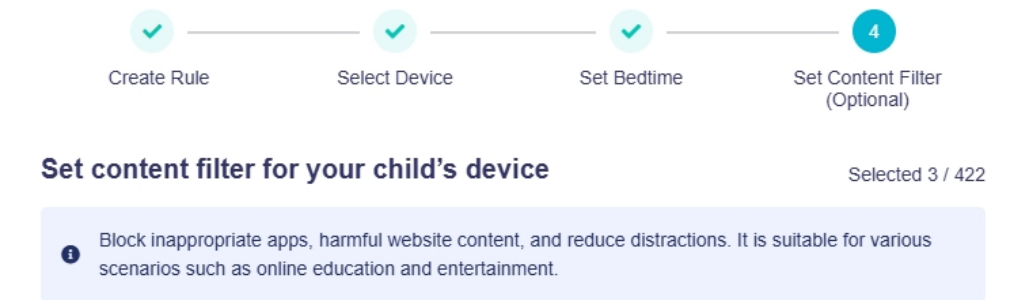
Suggerimento: se desideri distinguere i dispositivi collegati, vai alla pagina **CLIENT** e personalizza i nomi dei dispositivi.

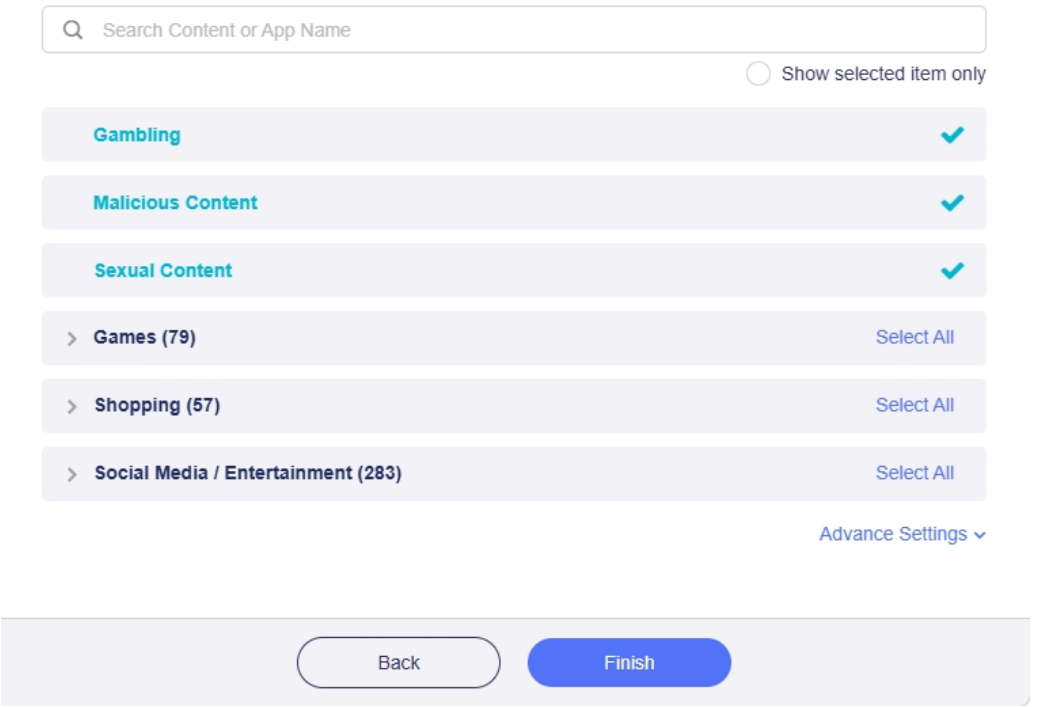
6. Imposta l'ora di andare a dormire per il dispositivo di tuo figlio, quindi fai clic su **Avanti**. Durante questo periodo Internet sui dispositivi selezionati non sarà disponibile. Per impostazione predefinita, l'ora di andare a dormire è la stessa tutti i giorni.



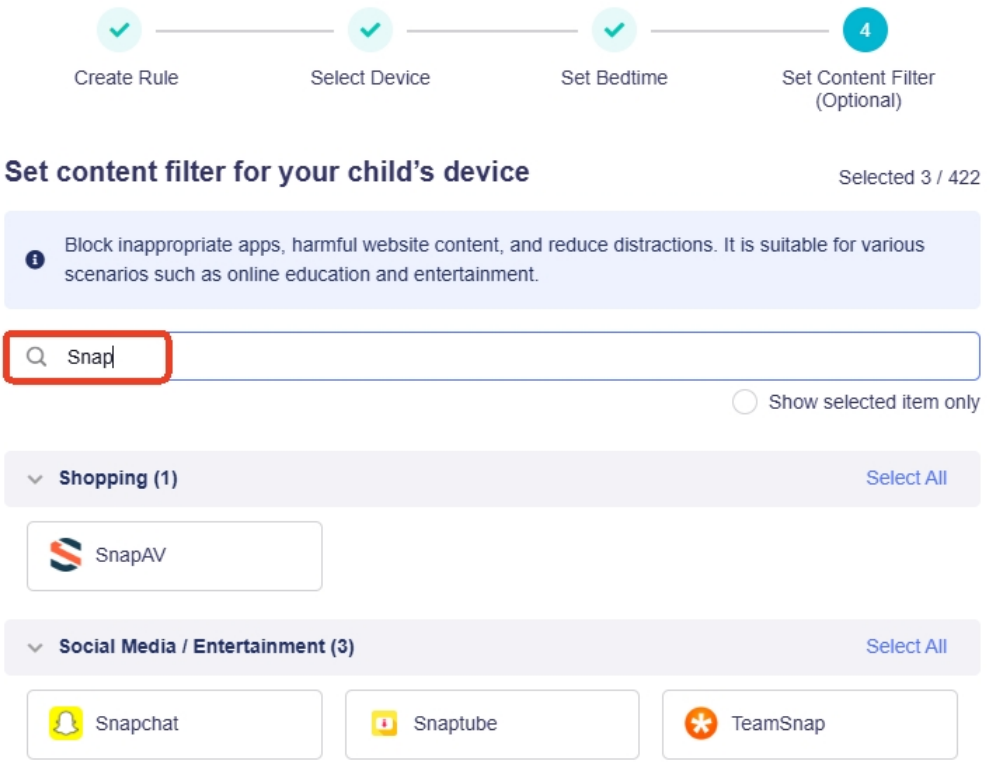
Se desideri impostare orari di andare a dormire diversi per ogni giorno della settimana, seleziona **Personalizza giorni** e imposta orari di andare a dormire diversi, quindi fai clic su **Avanti**.

7. Seleziona il filtro dei contenuti.
   Tre categorie sono state selezionate per impostazione predefinita: **Giochi d'azzardo**, **Contenuti dannosi** e **Contenuti di natura sessuale**. Se necessario, puoi selezionare altre categorie, come **Giochi**, **Shopping**, **Social media**, **Intrattenimento**, ecc.

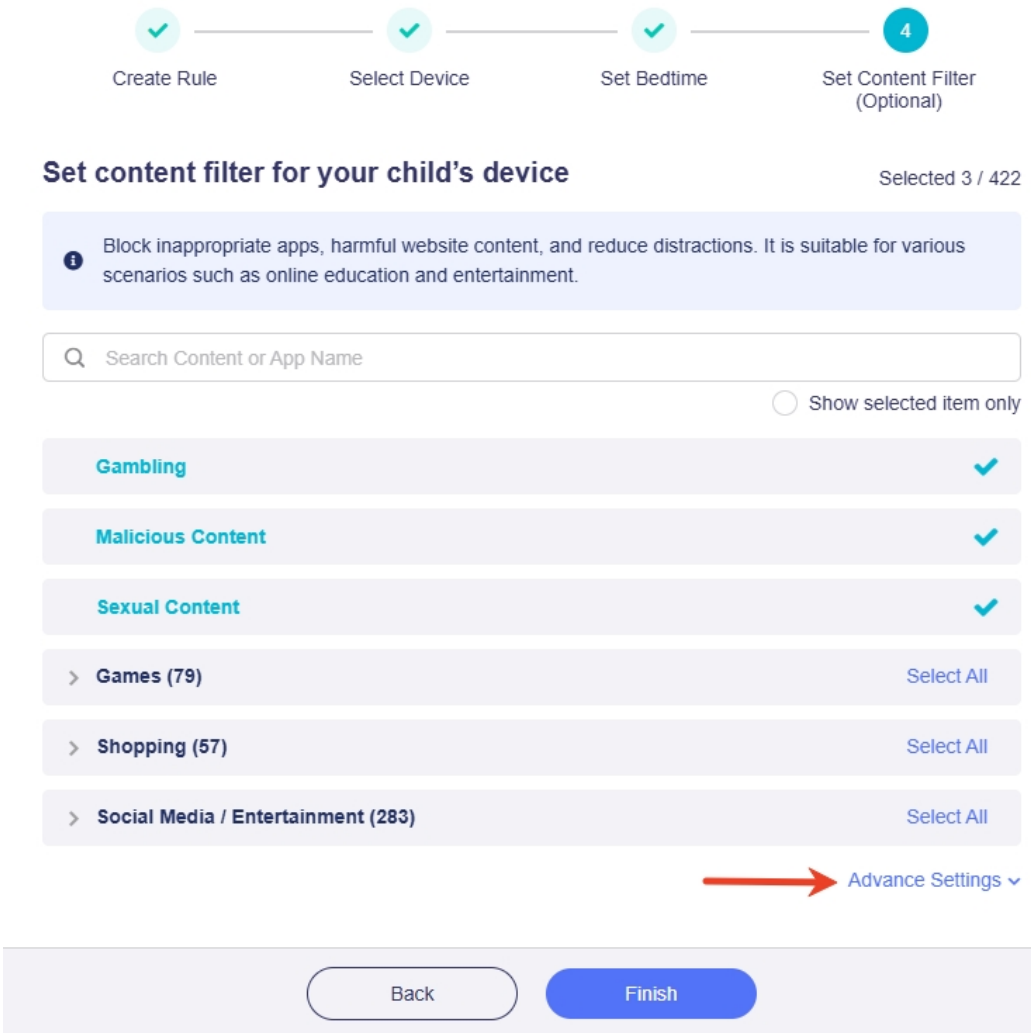




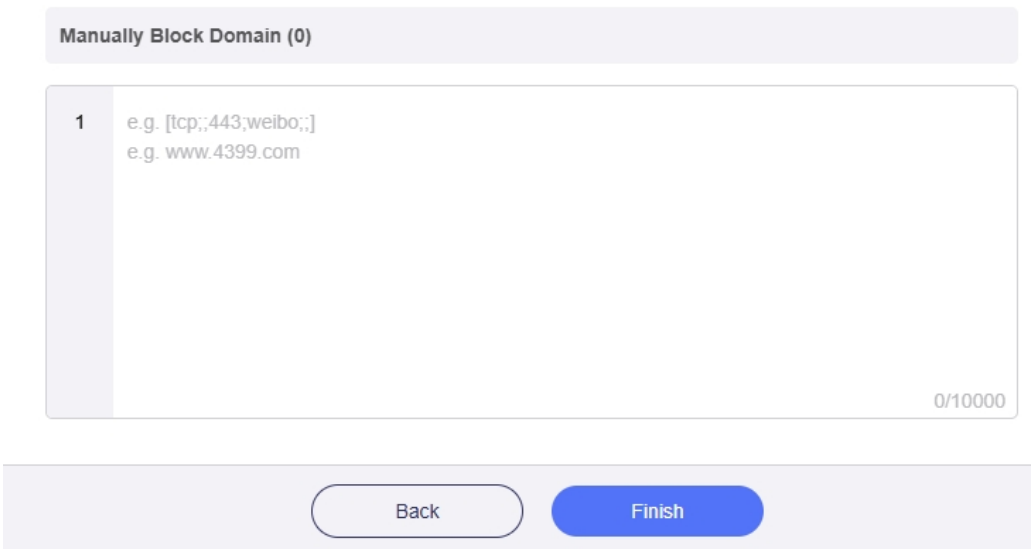
Se una determinata app che desideri bloccare è difficile da trovare, puoi cercarla in alto.



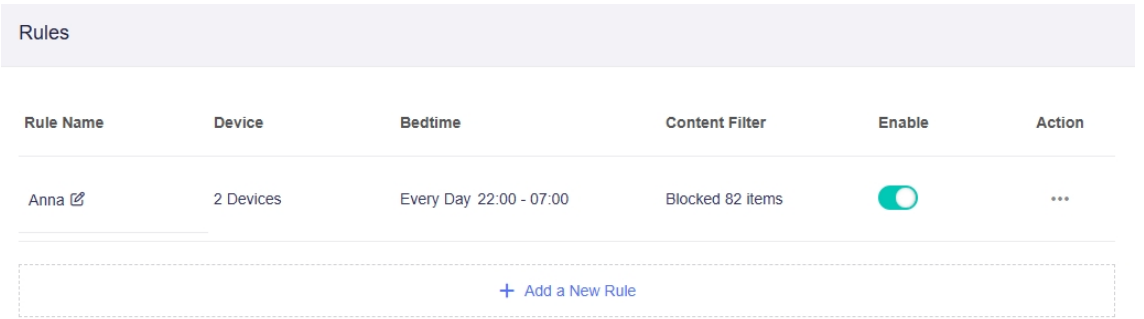
8. Se devi bloccare determinati domini, fai clic su **Impostazioni avanzate** in basso a destra.



Immetti i domini manualmente, quindi fai clic su **Fine**.



9. La regola è ora aggiunta. L'elenco mostra il nome della regola, il conteggio dei dispositivi connessi, la programmazione dell'ora di andare a dormire, i contenuti filtrati e lo stato della regola (abilitato/disabilitato).



Capitolo 13

Sicurezza

Questo capitolo gestisce la sicurezza della rete, come il port forwarding, le impostazioni di accesso dell'amministratore e la modalità NAT.

13.1 Port forwarding

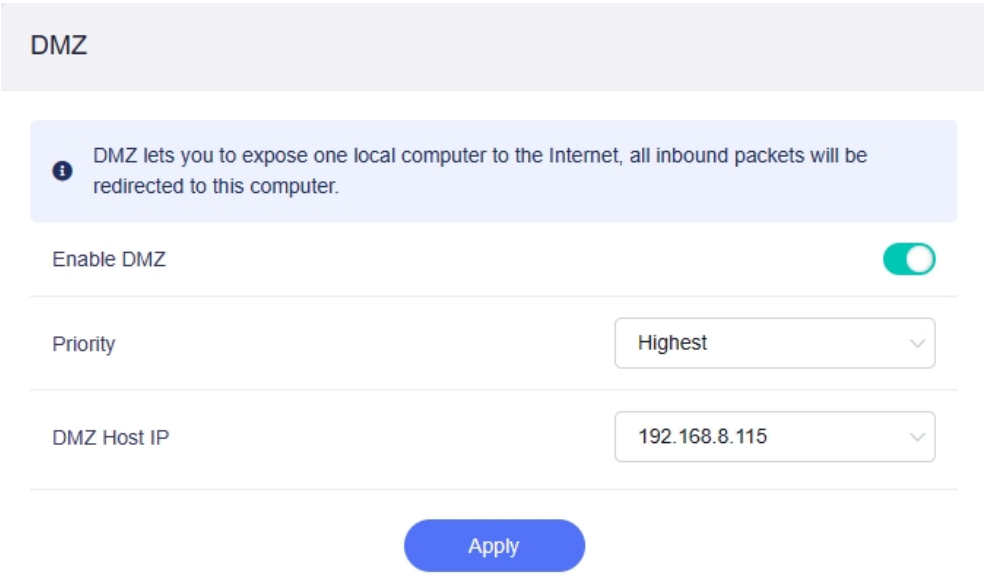
Il port forwarding è una funzionalità di rete che instrada le richieste esterne a dispositivi specifici sulla rete locale. La pagina Port forwarding include due funzioni chiave: **DMZ** (per l'accesso completo diretto a un singolo dispositivo) e **Port forwarding** (per l'accesso mirato a porte specifiche di dispositivi).

13.1.1 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 secondo necessità.

1. Accedi al pannello di amministrazione web del tuo router e vai a **SICUREZZA** > **Port forwarding** > **sezione DMZ**.
2. Attiva **Abilita DMZ**. Seleziona la priorità e l'IP host DMZ dall'elenco a discesa e fai clic su **Applica**.



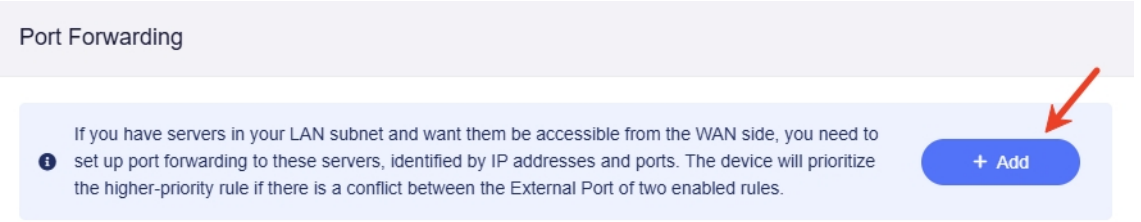
- **Priorità**: impostala su Massima o Minima. Se la priorità della DMZ è superiore alle regole di port forwarding, tutte le regole di port forwarding verranno invalidate. In caso contrario, le richieste verranno inoltrate al dispositivo client DMZ solo se la porta a cui si accede non ha una regola di port forwarding corrispondente.
- **IP host DMZ**: seleziona l'indirizzo IP interno del dispositivo che riceverà tutti i pacchetti in entrata.

13.1.2 Port forwarding

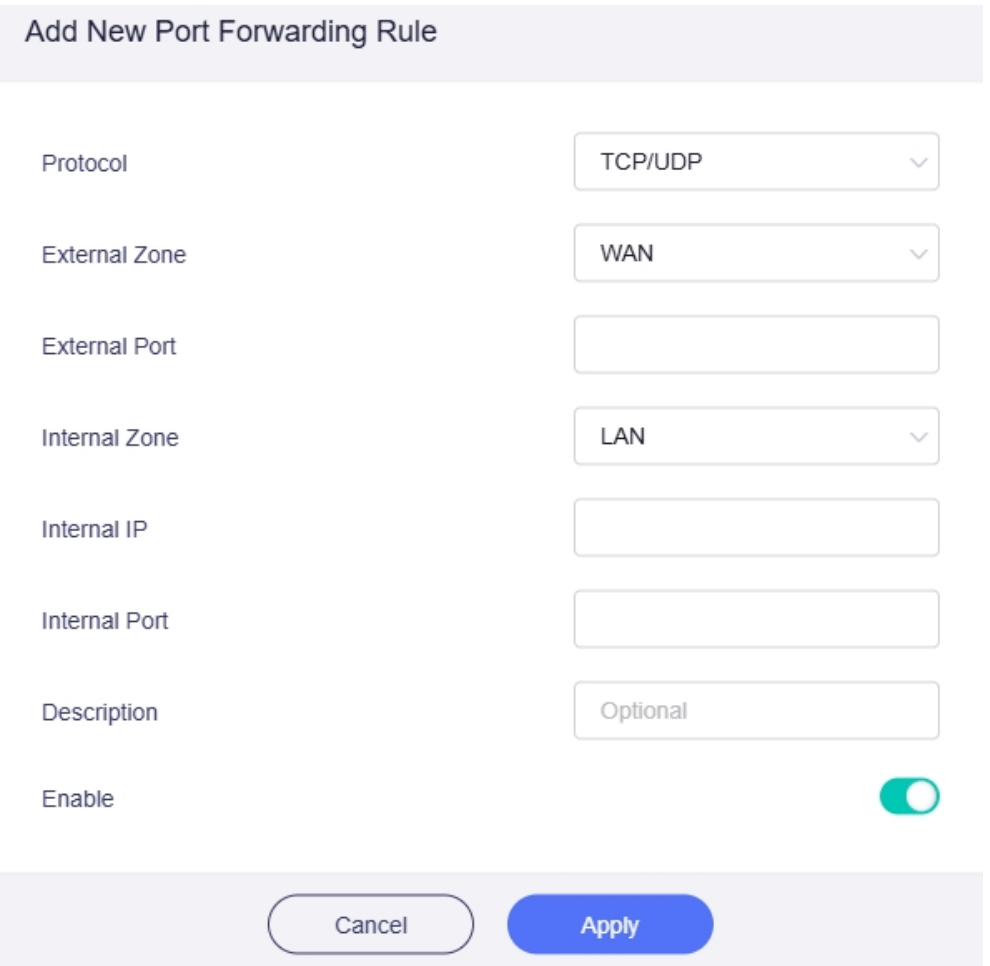
Il port forwarding consente ai computer remoti di connettersi a un computer locale o a un server dietro il firewall LAN (ad esempio server Web, server FTP).

Se è necessario configurare port forwarding, seguire i passaggi seguenti.

1. Accedi al pannello di amministrazione web del tuo router, vai alla sezione **SICUREZZA** > **Port forwarding > 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**.



- **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 e LAN.
- **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, 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.
- **Descrizione**: imposta un nome o aggiungi una descrizione per la regola di port forwarding (facoltativo).
- **Abilita**: abilita o disabilita questa regola.

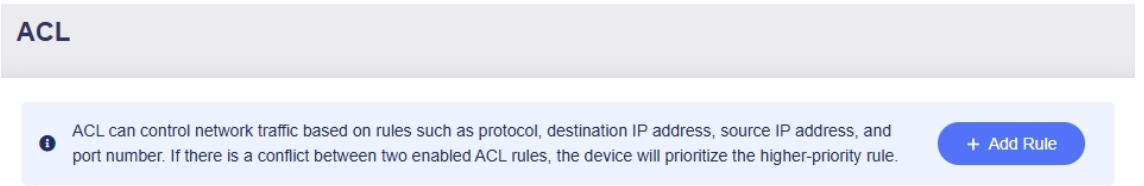
13.2 ACL

ACL, abbreviazione di Controllo degli accessi List, ti consente di creare regole per gestire il traffico di rete in base ai protocolli di connessione, agli indirizzi dei dispositivi e alle porte. Controlla se consentire o bloccare l'accesso alla rete. Se più regole ACL sono in conflitto, il sistema applica quella con priorità più alta.

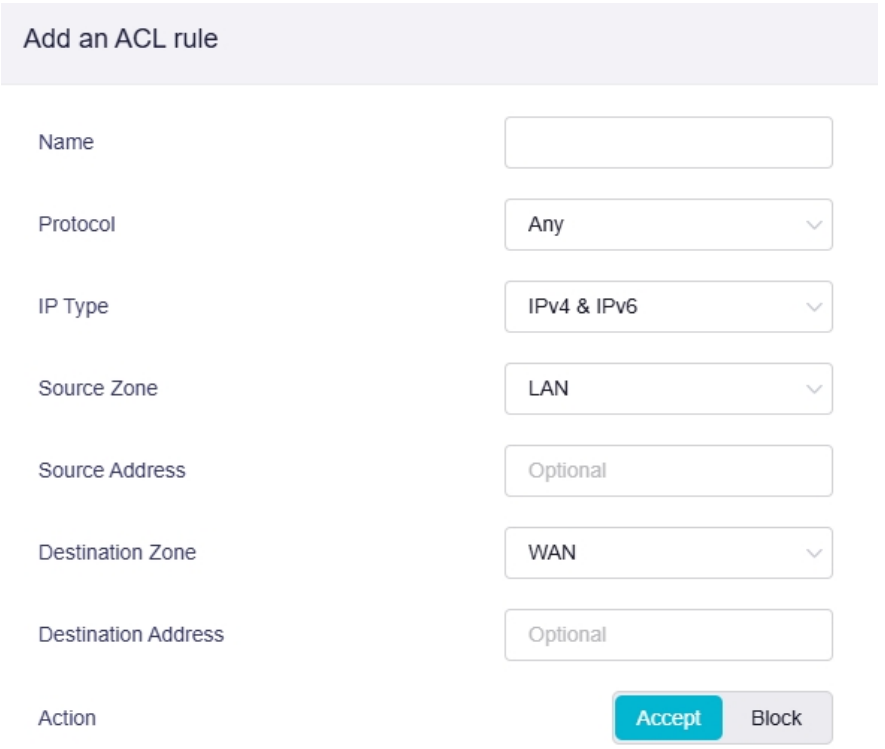
Diverso da Port forwarding, ACL consente o blocca principalmente l'accesso alla rete per motivi di sicurezza, mentre Port forwarding reindirizza il traffico esterno a dispositivi specifici sulla rete locale per abilitare accesso remoto ai servizi locali.

Segui i passaggi seguenti per configurare l'elenco Controllo degli accessi, se necessario.

1. Accedi al pannello di amministrazione web del tuo router e vai su **SICUREZZA** > **ACL**. Fai clic sul pulsante **Aggiungi regola** a destra.



2. Crea la tua regola ACL nella finestra pop-up, quindi fai clic su **Applica**.





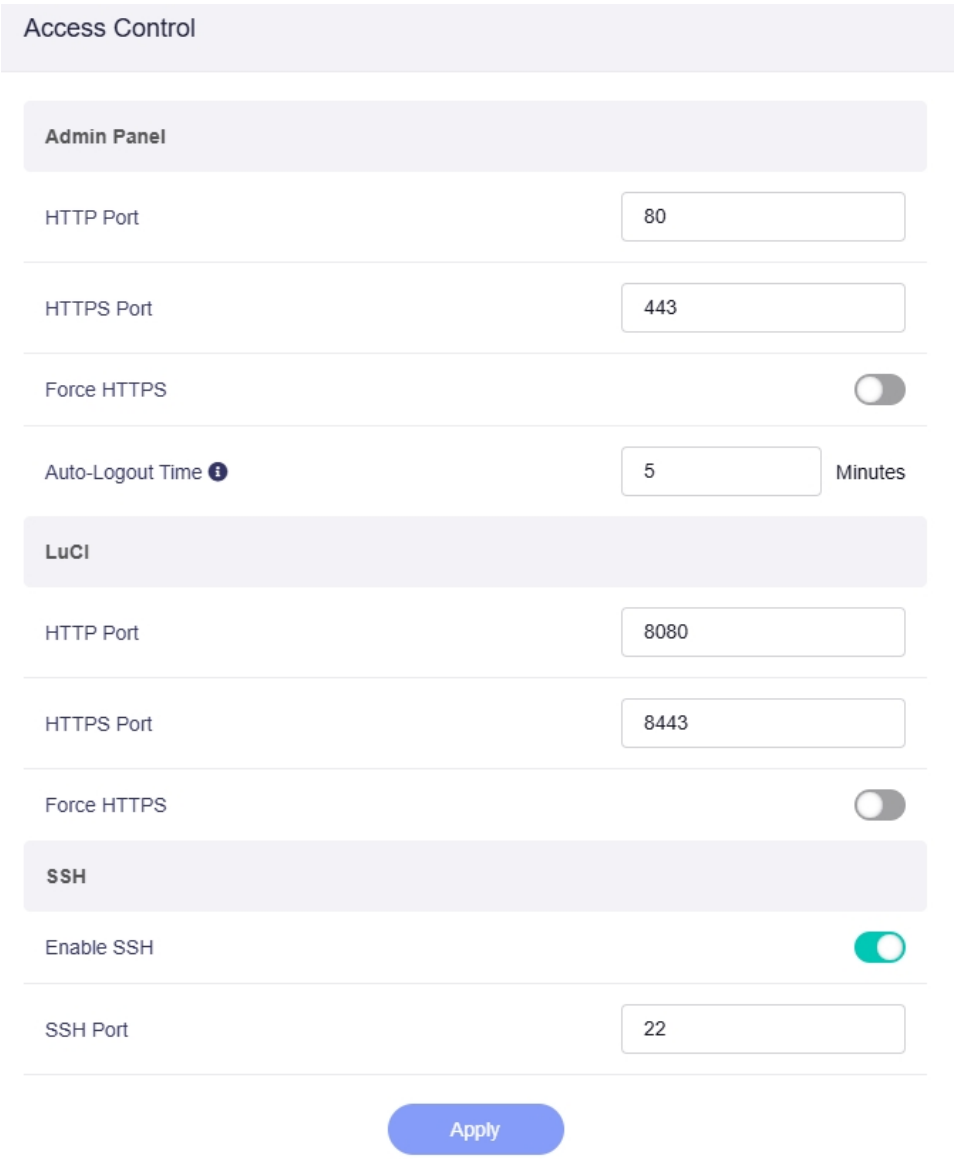
- **Nome**: inserisci un nome personalizzato per la regola.
- **Protocollo**: specifica a quale tipo di traffico di rete si applica la regola. Seleziona un protocollo di connessione tra Qualsiasi, TCP, UDP, TCP+UDP e ICMP.
- **Tipo IP**: definisce il formato dell'indirizzo IP per il traffico di rete. Seleziona il tipo IP tra IPv4 e IPv6, IPv4 e IPv6.
- **Zona sorgente**: seleziona la zona di rete da cui ha origine il traffico. Opzioni disponibili: LAN, Guest, IoT e WAN.
- **Indirizzo di origine**: (facoltativo) limita la regola a dispositivi di origine o indirizzi IP specifici. Puoi selezionare un indirizzo di origine dall'elenco a discesa.
- **Zona di destinazione**: è qui che è diretto il traffico di rete. Seleziona la zona della rete di destinazione. Opzioni disponibili: LAN, Guest, IoT e WAN.
- **Indirizzo di destinazione**: (facoltativo) limita la regola a dispositivi di destinazione o indirizzi IP specifici. Puoi selezionare un indirizzo di destinazione dall'elenco a discesa.
- **Azione**: scegli di accettare o bloccare il traffico di rete corrispondente a questa regola.
- **Abilita**: attiva o disattiva questa regola.

13.3 Accesso amministratore

Accedi al pannello di amministrazione web del tuo router e vai a **SICUREZZA** > **Accesso amministratore**. Questa pagina consente di configurare il router accesso locale, l'accesso remoto HTTPS/SSH e gestire le porte aperte sul router, proteggendo il router e la rete da accessi non autorizzati.

13.3.1 Controllo degli accessi

Questa sezione gestisce l'accesso alle molteplici interfacce del router (Pannello di amministrazione, LuCI e 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.
- **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.

LuCI

Nota: installare LuCI sullo Impostazioni avanzate prima di impostarne il controllo di accesso.

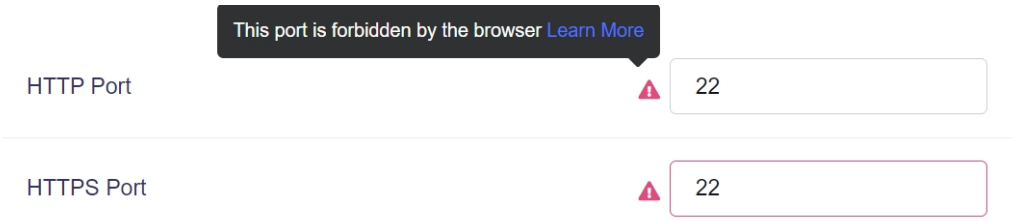
- **Porta HTTP**: predefinita su 8080, per l'accesso HTTP non crittografato all'interfaccia LuCI.
- **Porta HTTPS**: il valore predefinito è 8443, per l'accesso HTTPS sicuro all'interfaccia LuCI.
- **Forza HTTPS**: se abilitato, l'accesso all'interfaccia LuCI viene imposto per utilizzare una connessione HTTPS sicura.

SSH

- **Abilita SSH**: abilitato per impostazione predefinita, controlla se l'accesso SSH al router è consentito.
- **Porta SSH**: il valore predefinito è 22, la porta utilizzata per l'accesso SSH al router.

Nota:

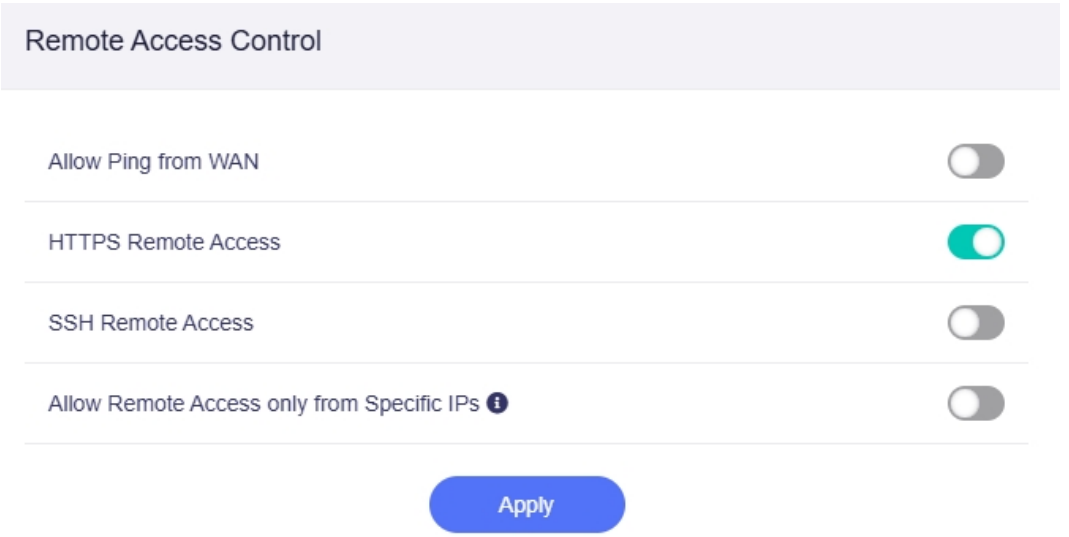
1. Se assegni un numero di porta che è in conflitto con una porta riservata (o una riservata per servizi specifici da browser/convenzioni di rete), verrà visualizzato un messaggio che indica "Questa porta è vietata dal browser".



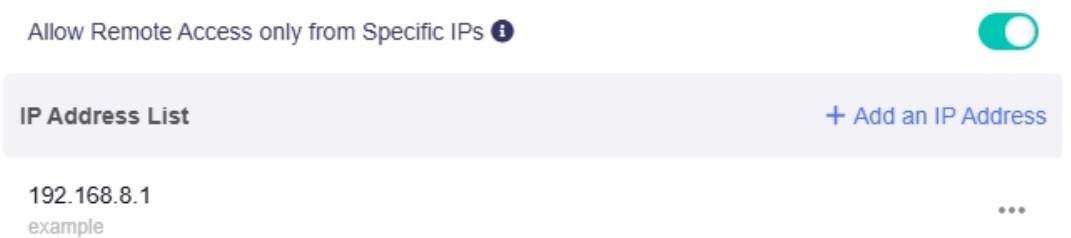
2. Se il numero di porta viene modificato nel firmware, è necessario inserire il numero di porta corretto per accedere al pannello di amministrazione. Se hai dimenticato il numero di porta, reimposta il router per ripristinare il numero di porta predefinito.

13.3.2 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.

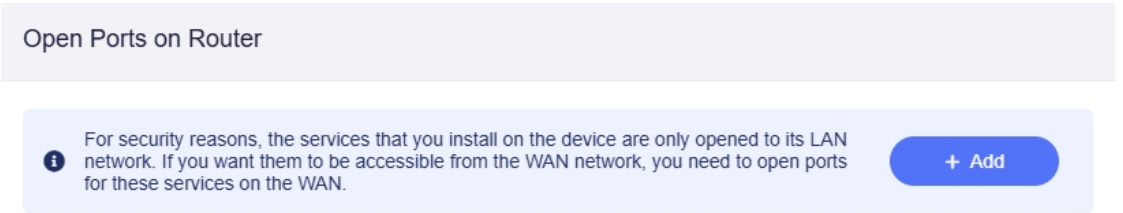


- **Consenti ping dalla WAN**: consentire il ping dal lato WAN del router può aiutare gli utenti a verificare se il router è raggiungibile tramite WAN in caso di problemi di rete, nonché a determinare la latenza di rete e la perdita di pacchetti.
- **Accesso remoto HTTPS**: Accesso remoto HTTPS abilita 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.

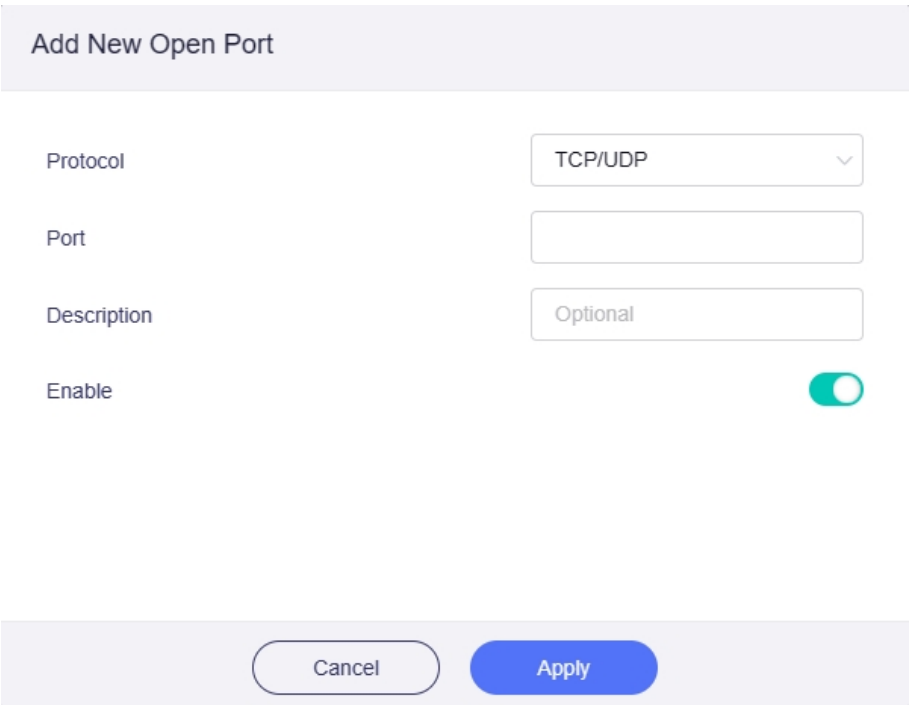


13.3.3 Apertura delle porte sul router

Questa sezione gestisce il port forwarding per i servizi sul router. Alcuni servizi, come web e FTP, richiedono che le rispettive porte siano aperte sul router per essere pubblicamente raggiungibili dalla rete WAN. Per motivi di sicurezza, per impostazione predefinita i servizi installati sul dispositivo sono accessibili solo all'interno della LAN. Se devi abilitare tale accesso WAN, puoi aprire porte specifiche qui.



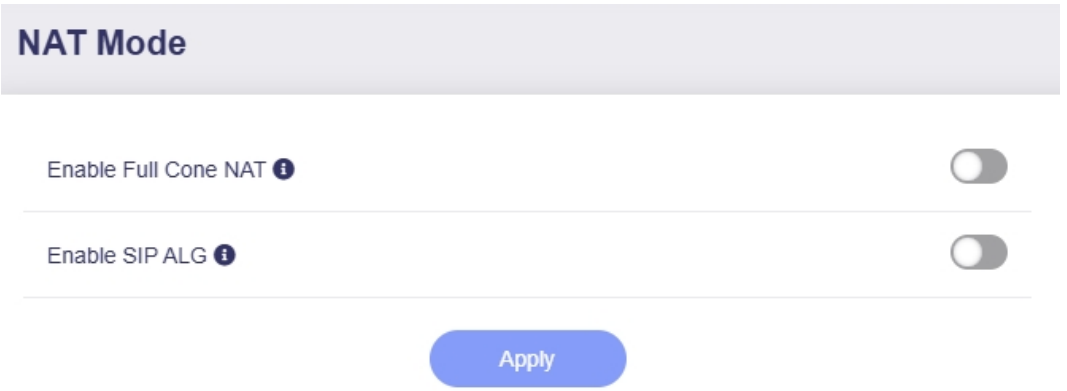
Per aprire una porta, fai clic su **Aggiungi** e inserisci le informazioni richieste nella finestra pop-up.



- **Protocollo**: selezionare il protocollo di rete (TCP, UDP o TCP/UDP) per la porta. Ciò determina la modalità di trasmissione dei dati per il servizio associato alla porta.
- **Porta**: inserisci il numero di porta specifico che desideri aprire.
- **Descrizione** (facoltativo): aggiungi una breve nota per descrivere lo scopo di questa porta aperta (ad esempio, "Server Web" o "Servizio FTP") per una gestione più semplice.
- **Abilita**: attiva questo interruttore per attivare o disattivare la regola di port forwarding.

13.4 Modalità NAT

Accedi al pannello di amministrazione web del tuo router e vai a **SICUREZZA** > **Modalità 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

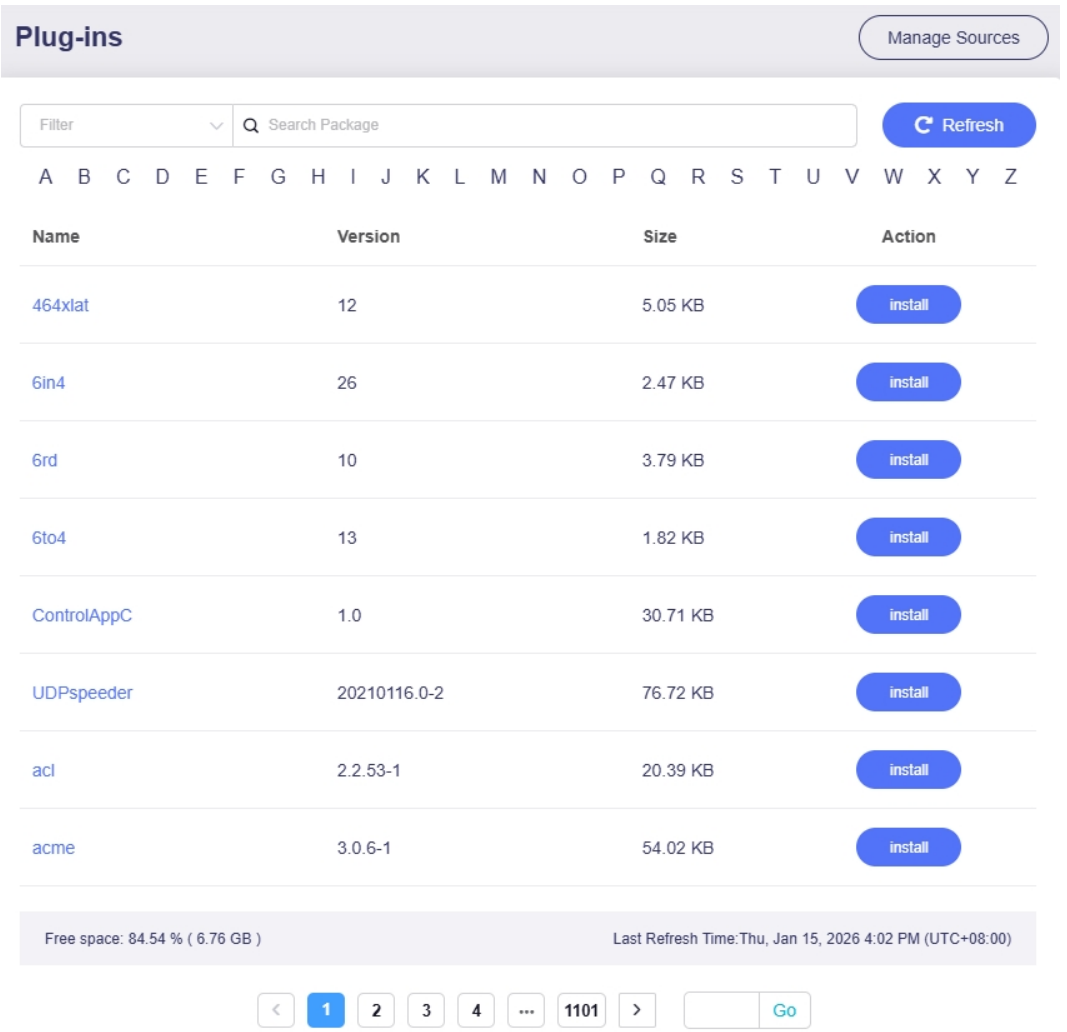
Applicazioni

Questo capitolo introduce alcune applicazioni nei router GL.iNet, ad esempio plug-in, DNS dinamico, Archiviazione di rete, AdGuard Home, Tailscale, ZeroTier e Tor.

14.1 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:

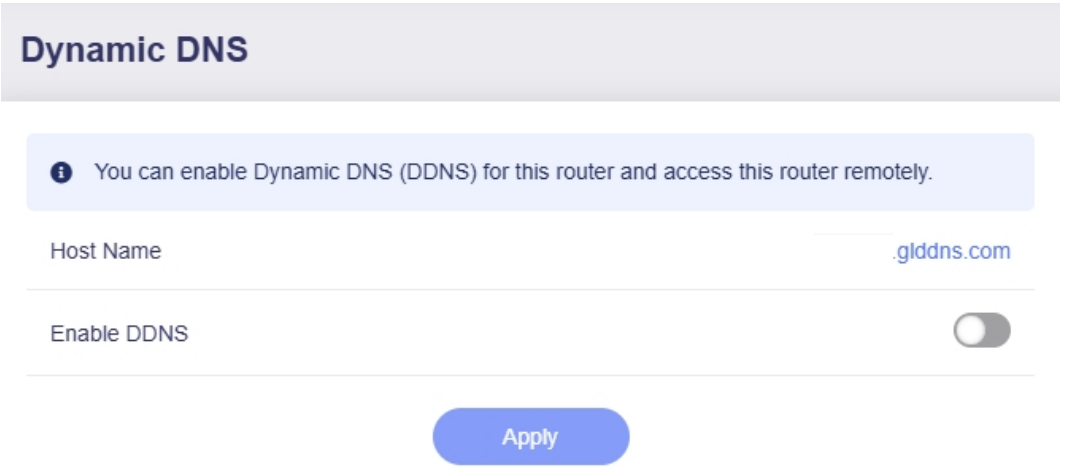
1. Non è consigliabile aggiornare i plug-in preinstallati nel firmware ufficiale GL.iNet, come nginx, adguard home, tailscale, ecc.
2. I plugin di terze parti installati manualmente dagli utenti possono essere aggiornati; tuttavia, GL.iNet non è responsabile per eventuali problemi di sicurezza derivanti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

14.2 DNS dinamico

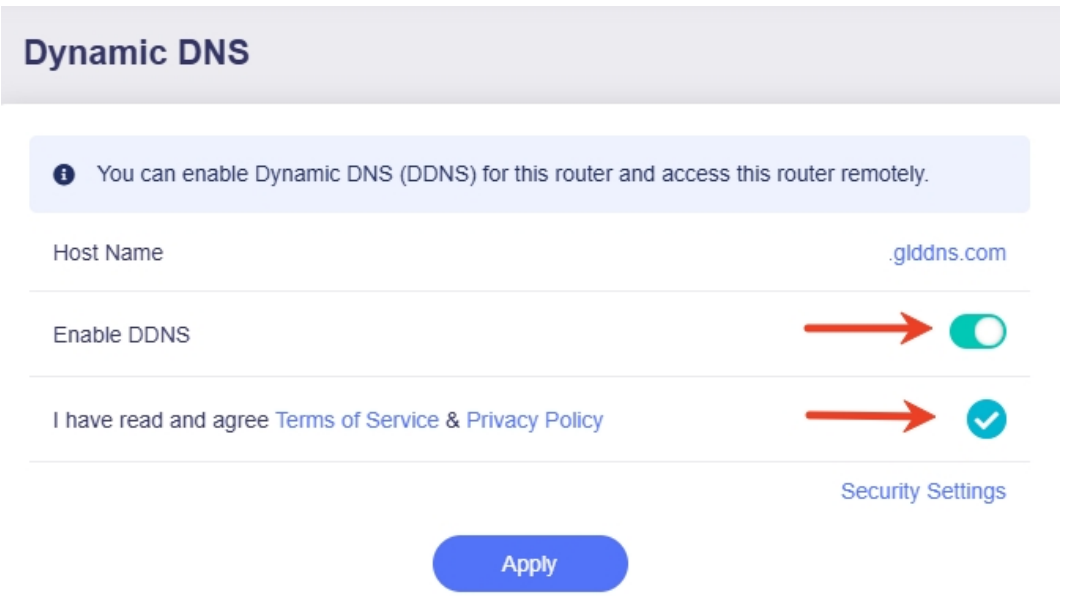
Dynamic Domain Name Service (DDNS o DNS dinamico) è un servizio utilizzato per mappare un nome di dominio all'indirizzo IP dinamico di un dispositivo di rete. Con DNS dinamico puoi accedere al tuo router da remoto. Per questa funzionalità è richiesto un indirizzo IP pubblico.

14.2.1 Abilita DDNS

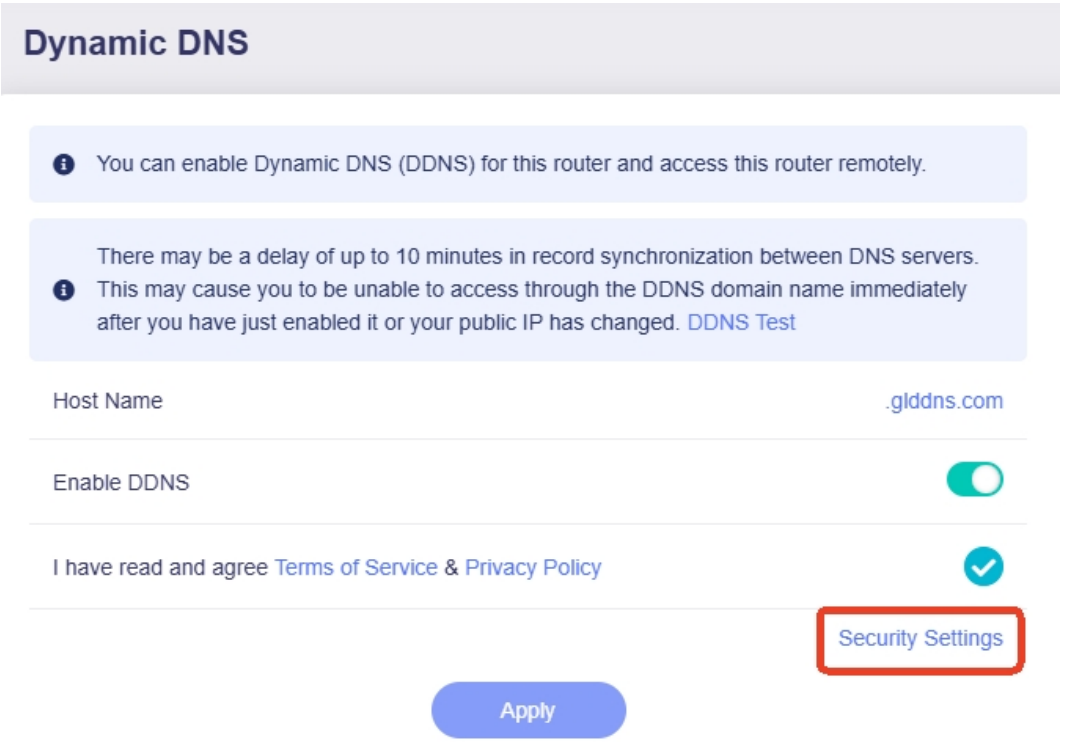
1. Accedi al pannello di amministrazione web del tuo router, vai su **APPLICAZIONI** > **DNS dinamico**, la pagina viene visualizzata come di seguito.



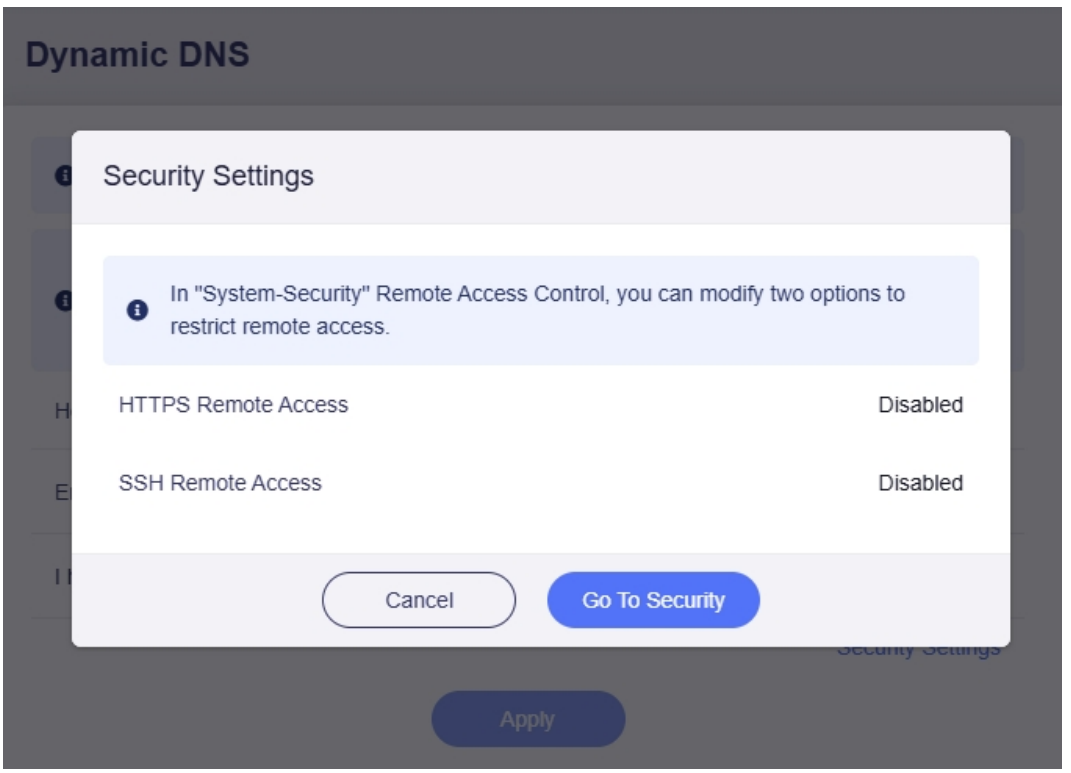
2. Attiva **Abilita DDNS**, leggi e accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.



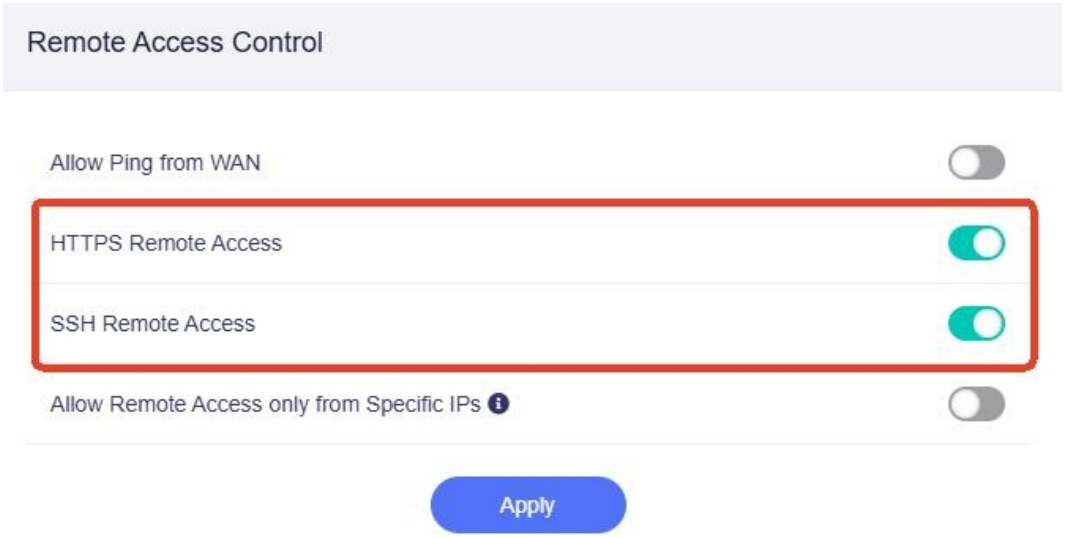
3. Fai clic su **Impostazioni di sicurezza** nell'angolo in basso a destra.



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



In caso contrario, vai su **SICUREZZA** > **Accesso amministratore** > **Controllo dell'accesso remoto** per abilitarlo e fai clic su **Applica**.



Nota:

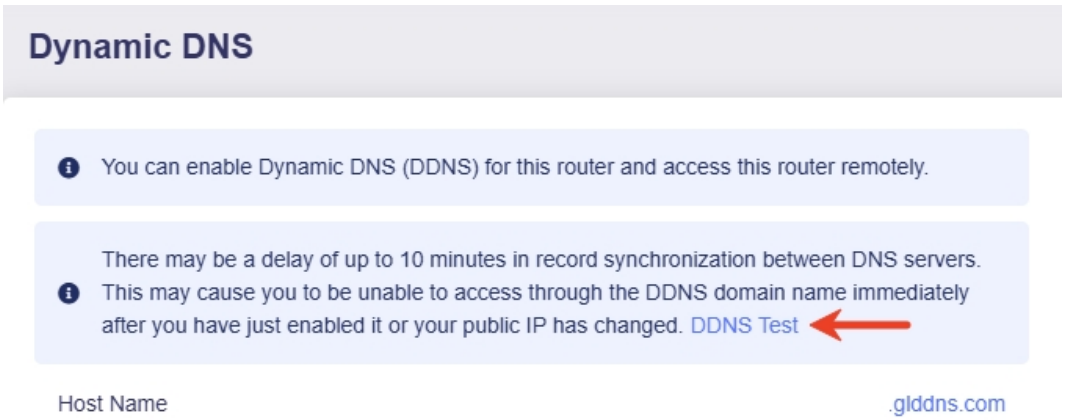
1. Potrebbe verificarsi un ritardo fino a 10 minuti nella sincronizzazione dei record tra i server DNS. Ciò potrebbe impedirti di accedere tramite il nome di dominio DDNS immediatamente dopo averlo abilitato o quando il tuo IP pubblico cambia.
2. Se abiliti DDNS e client VPN contemporaneamente, assicurati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

14.2.2 Verifica del funzionamento del DDNS

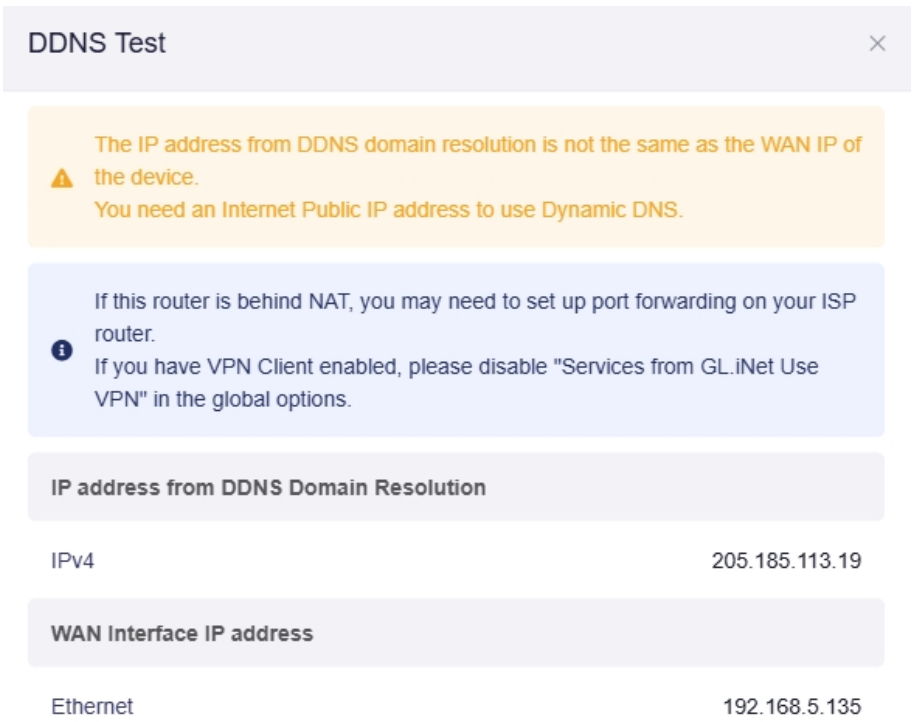
Puoi verificare se DDNS funziona utilizzando lo strumento di test DDNS o manualmente tramite comandi.

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. Usa il comando *nslookup xxxxxxx.glddns.com 8.8.8.8* per verificare la corrispondenza tra nome di dominio e indirizzo IP. Di seguito è riportato un esempio con Beryl AX GL-MT3000.



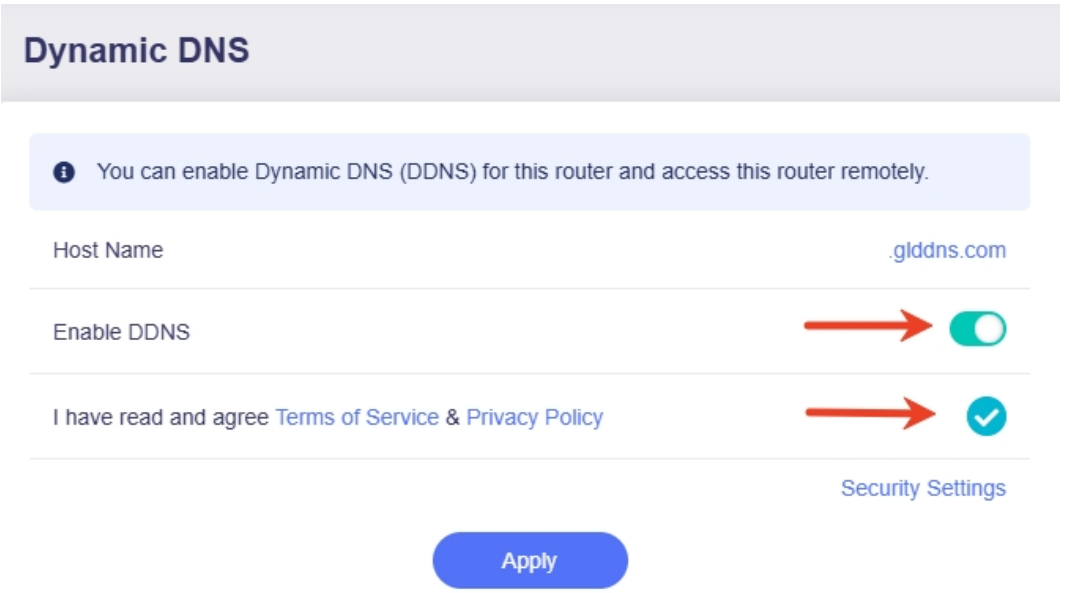
   - Sostituisci "xxxxxxx.glddns.com" nell'immagine sopra con il tuo nome host.
   - "8.8.8.8" è il DNS di Google. Usalo o sostituiscilo con altri, quindi premi Invio.
2. Se ottieni un indirizzo IP pubblico come "183.178.10.100" nell'immagine sopra, indica che il tuo dominio DDNS è stato mappato correttamente 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.

14.2.3 Accesso remoto HTTPS

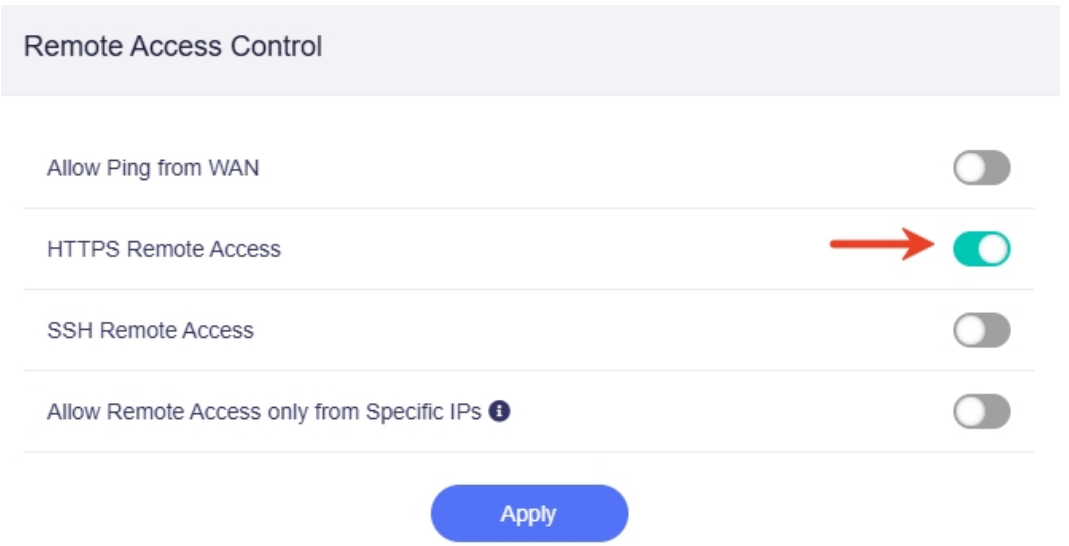
Per l'accesso remoto HTTPS è richiesto un indirizzo IP pubblico. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 443**) sul router upstream per l'accesso HTTPS.

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**.

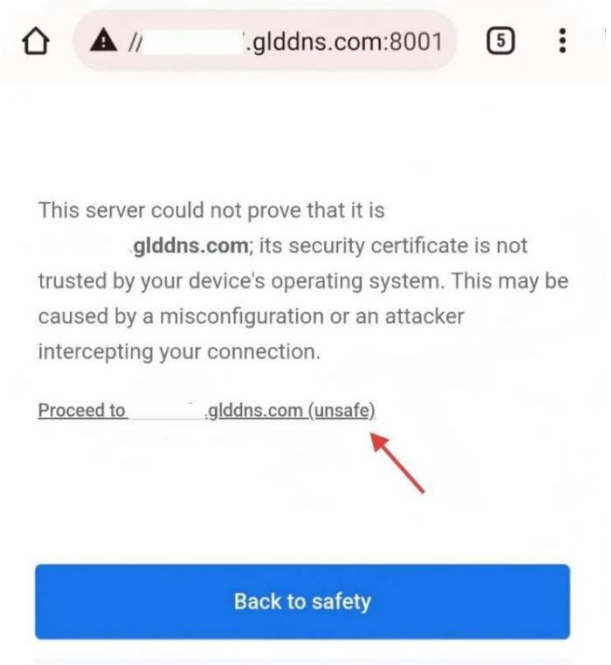


2. Nel pannello di amministrazione web, vai su **SICUREZZA** > **Accesso amministratore** > **Controllo dell'accesso remoto**. Abilita **Accesso remoto HTTPS** e fai clic su **Applica**.



Una volta abilitato, puoi accedere al pannello di amministrazione del router da qualsiasi luogo utilizzando il nome host DDNS su 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.



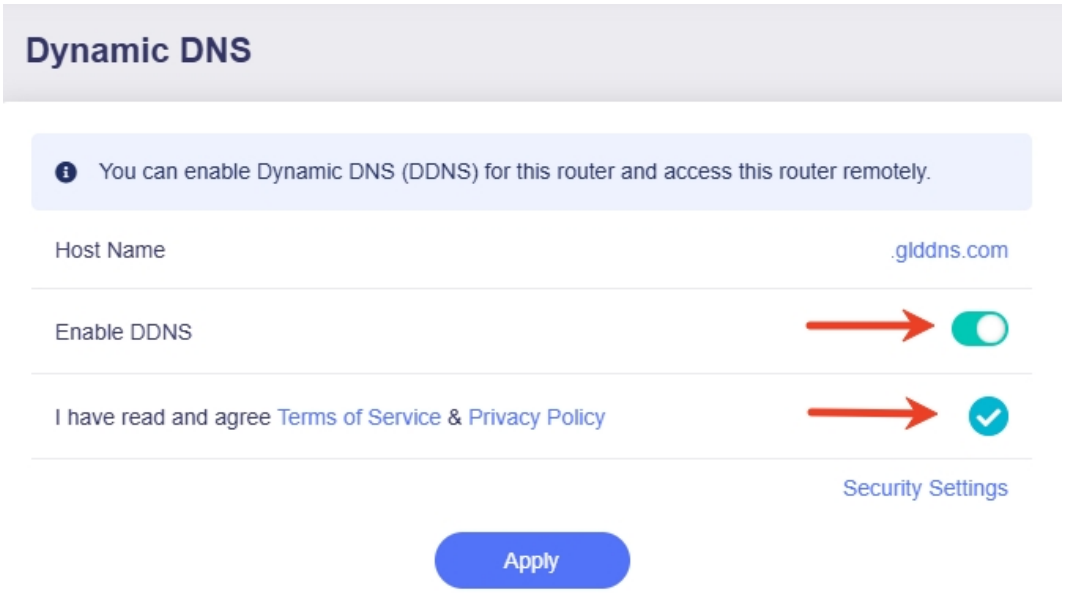
Sarai quindi in grado di accedere al pannello di amministrazione web del router utilizzando il nome host DDNS su **HTTPS**.

14.2.4 Accesso remoto SSH

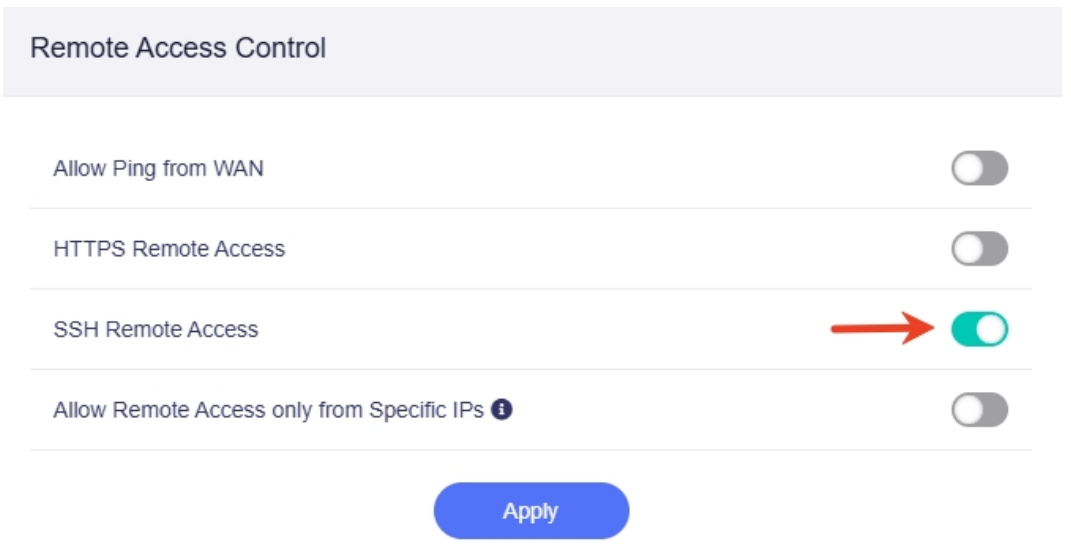
Per l'accesso remoto SSH è richiesto un **indirizzo IP pubblico**. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 22**) sul router upstream per l'accesso remoto SSH.

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 **SICUREZZA** > **Accesso amministratore** > **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).

14.3 Archiviazione di rete

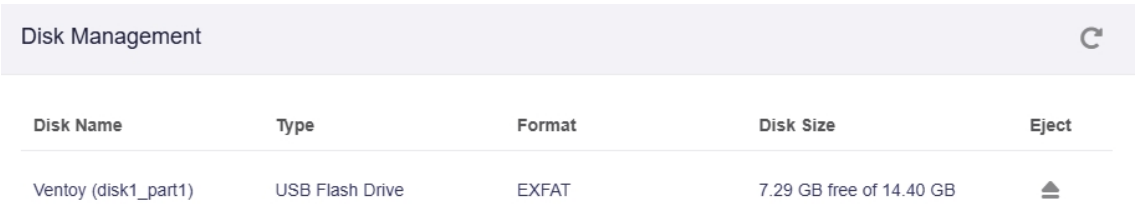
L'archiviazione di rete consente la condivisione di file tra dispositivi collegando un'unità USB o una scheda SD al router. Il router converte il dispositivo di archiviazione in un'unità di rete condivisa, accessibile a tutti i dispositivi collegati.

Brume 3 è dotato di una porta USB, compatibile con chiavette USB e hard disk esterni portatili. Puoi configurare Samba, WebDAV o DLNA per questi dispositivi di archiviazione, che supportano formati comuni come NTFS, FAT32 ed EXT4.

Nota: il consumo energetico del disco rigido USB è piuttosto elevato. Utilizzarlo con un alimentatore esterno, altrimenti potrebbe causare malfunzionamenti.

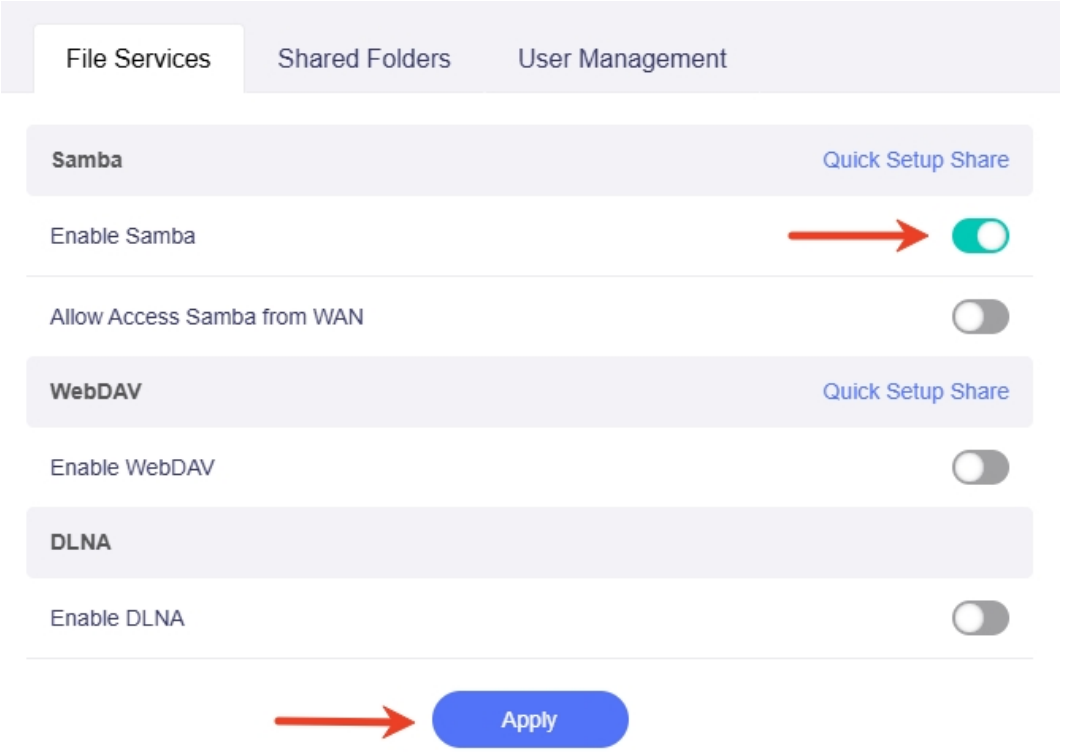
14.3.1 Collegamento del dispositivo di archiviazione

1. Collega il tuo dispositivo di archiviazione al router.
   - Per un'unità USB: collegala direttamente alla porta USB.
   - Per un disco rigido esterno: collegalo a un alimentatore separato (se necessario), quindi collegalo al router.
2. Accedi al pannello di amministrazione web del tuo router, vai su **APPLICAZIONI** > **Archiviazione di rete**. Puoi abilitare i servizi di trasferimento file e gestire la cartella condivisa qui.
3. Se il dispositivo di archiviazione viene rilevato, **Gestione disco** verrà visualizzata come segue.



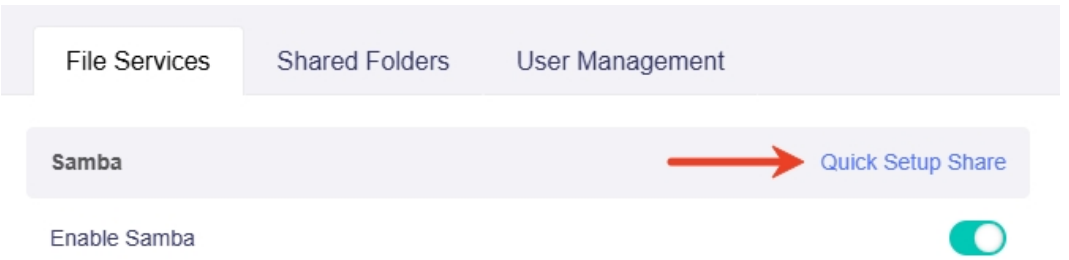
14.3.2 Configurazione di Samba

1. Nella sezione **Servizi file**, attiva **Abilita Samba** e fai clic su **Applica**.

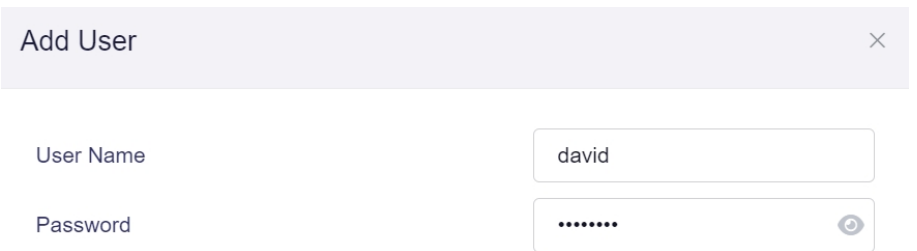


- **Consenti accesso a Samba dalla WAN**: abilitalo se desideri che i dispositivi upstream accedano al servizio Samba.

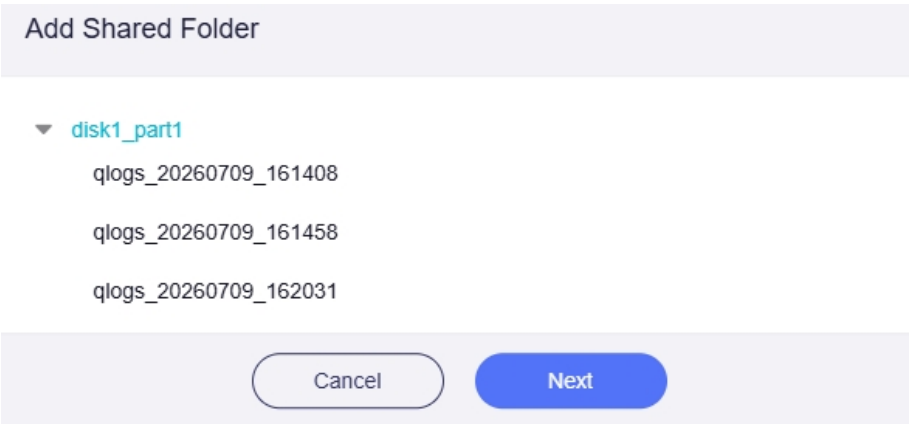
2. Fai clic su **Condivisione rapida** per impostare il collegamento condiviso.



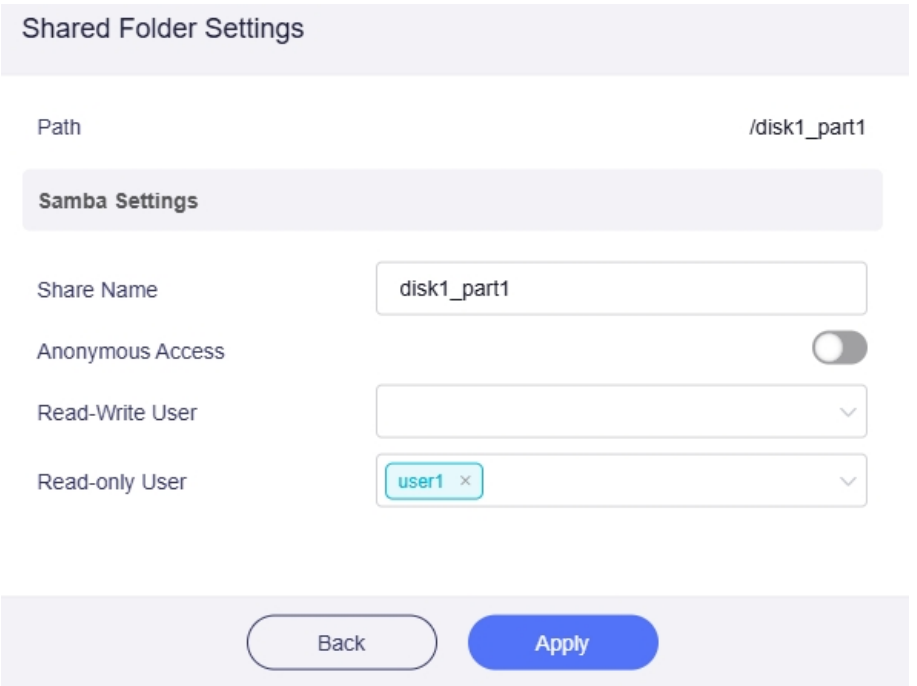
3. Aggiungi un utente e fai clic su **Avanti**. Questo passaggio verrà saltato se disponi già di un account.



4. Fai clic sull'icona del triangolo per mostrare tutte le cartelle. Seleziona una cartella da condividere, quindi fai clic su **Avanti**. Se desideri condividere l'intero disco, fai clic sul nome del disco (ad esempio, disk1_part1).

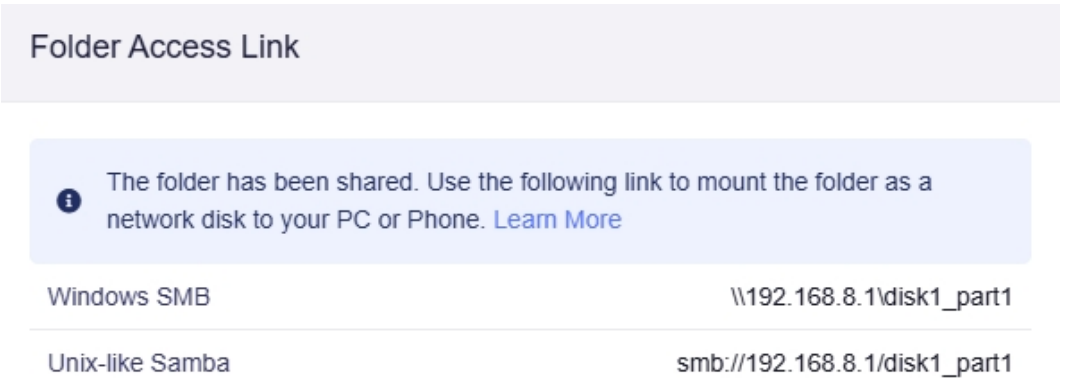


5. Imposta la cartella condivisa.
   L'utente creato nel passaggio precedente verrà aggiunto **all'utente di sola lettura** per impostazione predefinita. Se desideri che questo utente sia in grado di scrivere o eliminare file, rimuovilo da Utente di sola lettura e aggiungilo a **Utente di lettura-scrittura**, quindi fai clic su **Applica**.



   Suggerimento: per motivi di sicurezza, non è consigliabile abilitare l'accesso anonimo.
6. Ottenere il collegamento di accesso alla cartella.

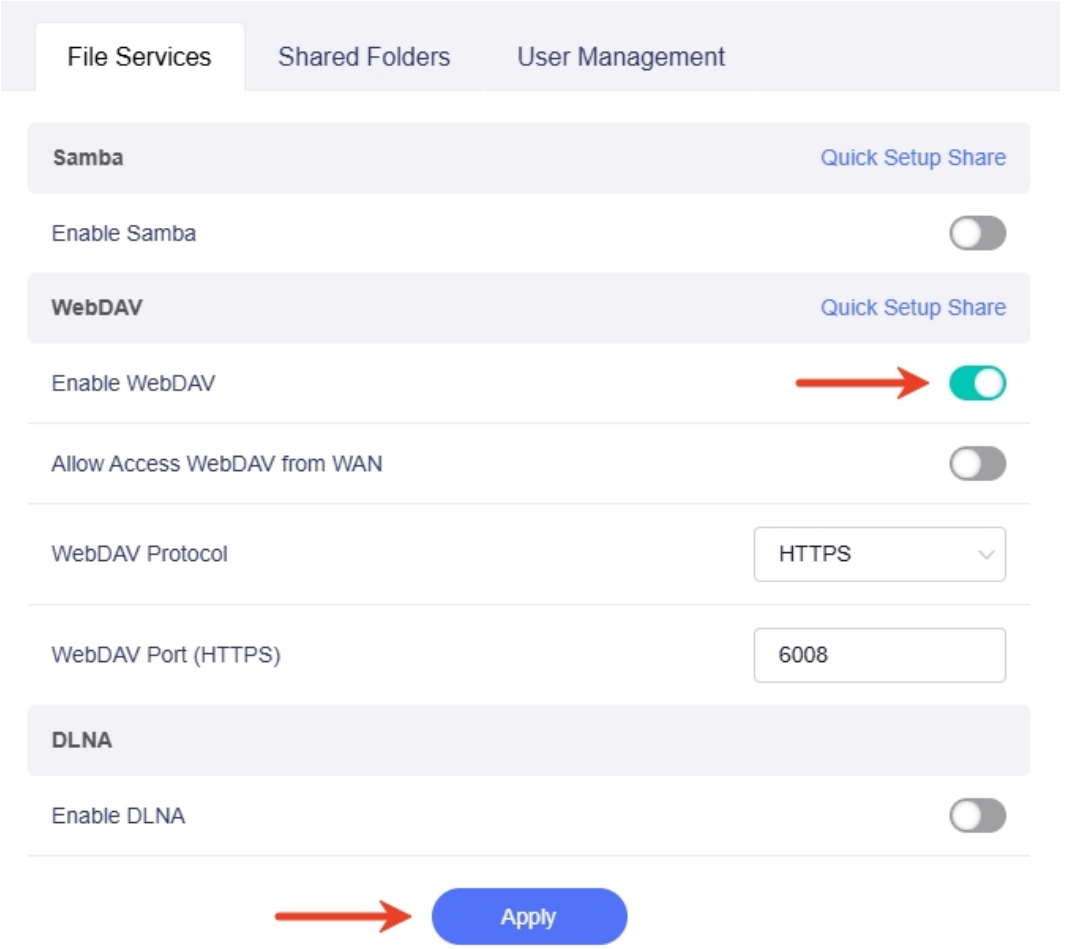
La pagina mostrerà i collegamenti per i sistemi operativi Windows e simili a Unix. Il sistema simile a Unix include Android, iOS, macOS, Ubuntu, ecc. Ora puoi accedere alla tua cartella condivisa tramite il servizio Samba tramite questi collegamenti.



Nota: se abiliti **l'accesso Samba dalla WAN** e accedi alla cartella condivisa dalla rete upstream, sostituisci l'IP del router (predefinito: 192.168.8.1) nel collegamento di accesso con l'IP WAN del router, che puoi trovare nella pagina INTERNET del pannello di amministrazione web.

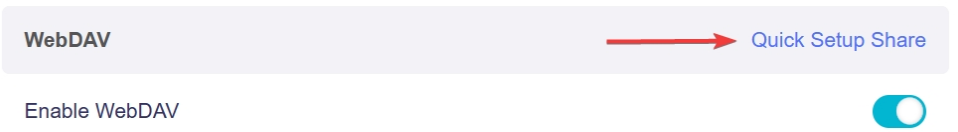
14.3.3 Configurazione di WebDAV

1. Nella sezione **Servizi file**, attiva **Abilita WebDAV** e fai clic su **Applica**.

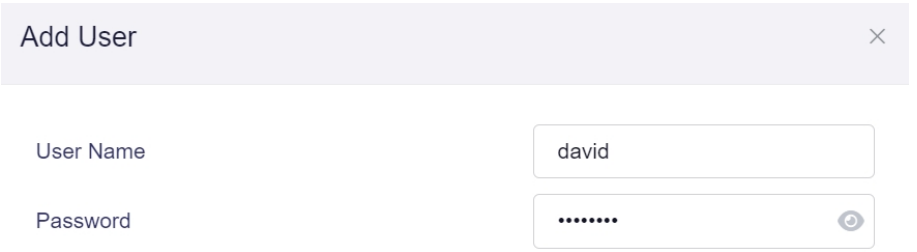


- **Consenti accesso WebDAV dalla WAN**: abilitalo se desideri che i dispositivi upstream accedano al servizio WebDAV.
- **Protocollo WebDAV**: HTTP non crittografato; utilizzarlo a proprio rischio. HTTPS è crittografato e utilizza un certificato autofirmato.
- **Porta WebDAV**: non è necessario modificare il numero di porta a meno che non ci sia un conflitto. L'intervallo di numeri di porta consigliato è 1024 - 65535.

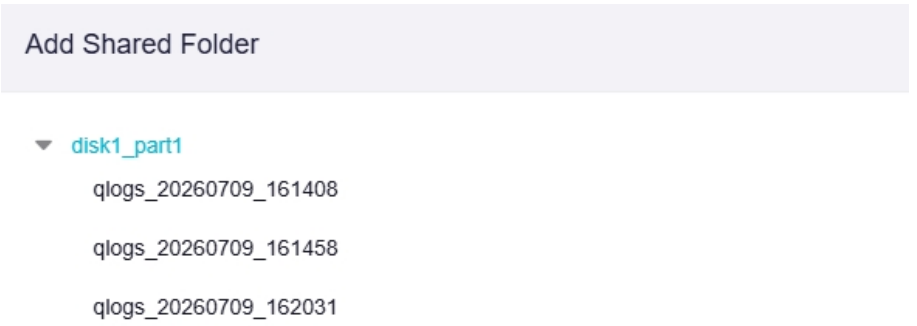
2. Fai clic su **Condivisione rapida** per impostare il collegamento condiviso.



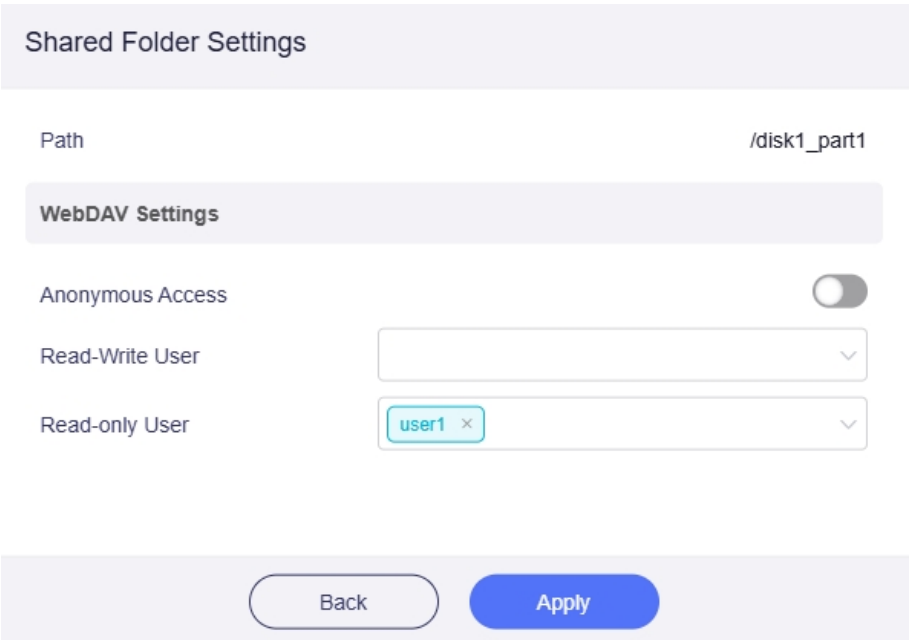
3. Aggiungi un utente e fai clic su **Avanti**. Questo passaggio verrà saltato se disponi già di un account.



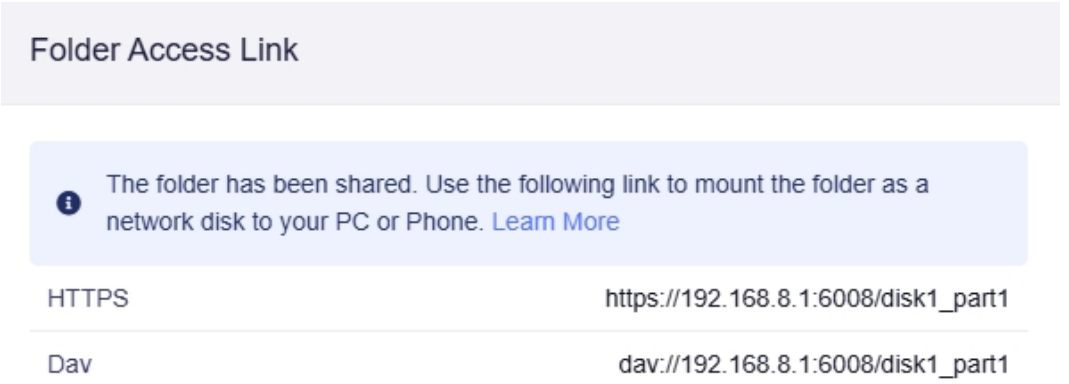
4. Fai clic sull'icona del triangolo per mostrare tutte le cartelle. Seleziona una cartella per la condivisione. Se desideri condividere l'intero disco, fai clic sul nome del disco (ad esempio, disk1_part1).



5. Imposta la cartella condivisa.
   L'utente creato nel passaggio precedente verrà aggiunto **all'utente di sola lettura** per impostazione predefinita.
   Se desideri che questo utente sia in grado di scrivere o eliminare file, rimuovilo dall'utente di sola lettura e aggiungilo **all'utente di lettura-scrittura**, quindi fai clic su **Applica**.



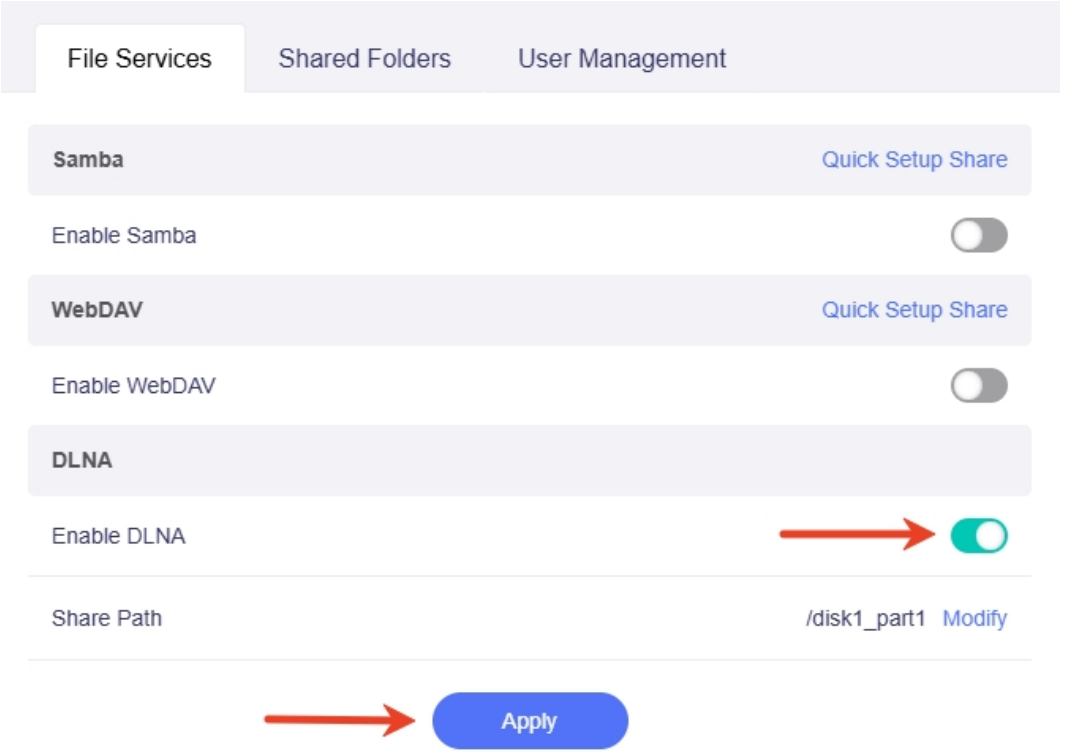
6. Ottenere il collegamento di accesso alla cartella.
   La pagina mostrerà i collegamenti per i sistemi operativi Windows e Unix-like. I sistemi simili a Unix includono Android, iOS, macOS, Ubuntu, ecc. Ora puoi accedere alla tua cartella condivisa tramite il servizio WebDAV tramite questi collegamenti.



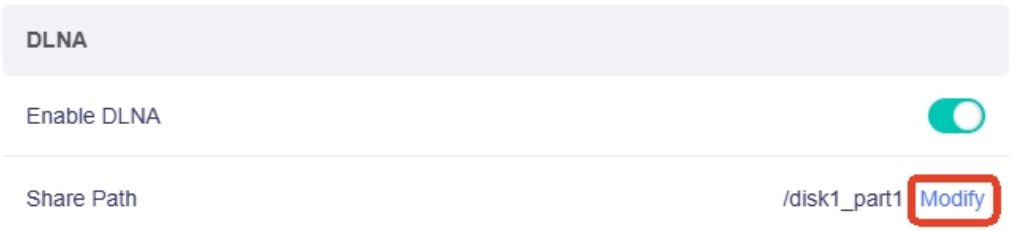
Nota: se attivi **Consenti accesso WebDAV dalla WAN** e accedi alla cartella condivisa dalla rete upstream, sostituisci l'IP del router (predefinito: 192.168.8.1) nel collegamento di accesso con l'IP WAN del router, che puoi trovare nella pagina INTERNET del pannello di amministrazione web.

14.3.4 Configurazione di DLNA

1. Nella sezione **Servizi file**, attiva **Abilita DLNA** e fai clic su **Applica**.



2. Modifica il percorso di condivisione sulla destra, se necessario.



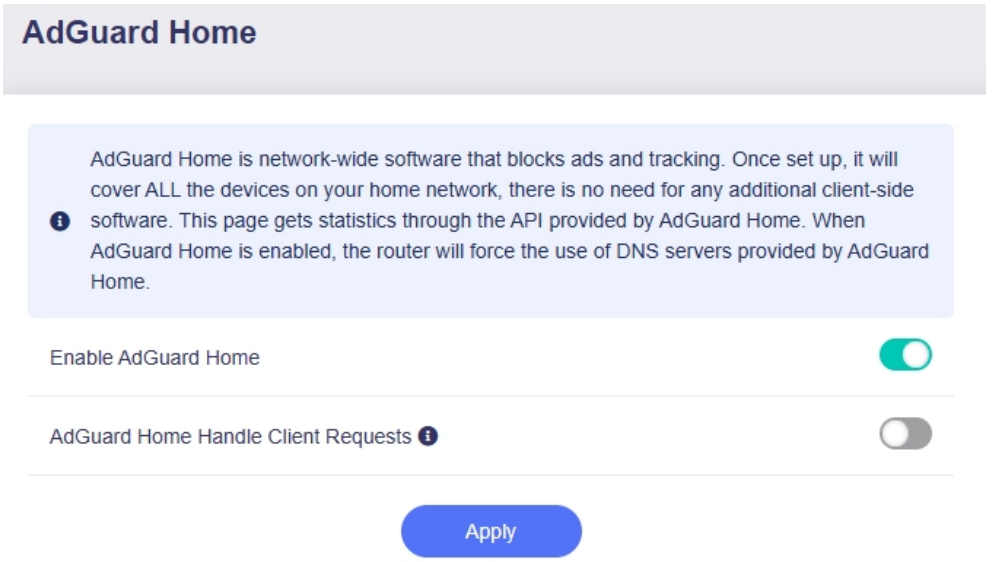
3. Collega la tua smart TV al router. Troverà automaticamente il server DLNA.

14.4 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.

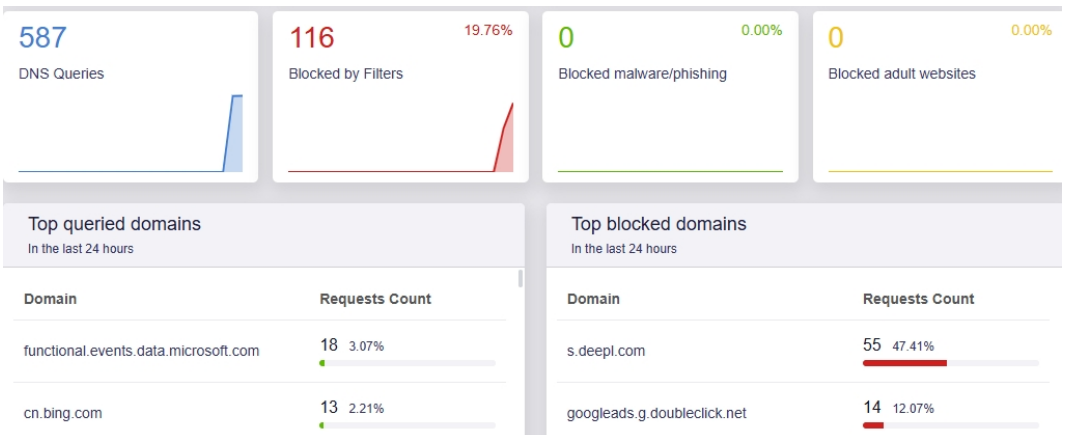
Segui questi passaggi per configurare AdGuard Home.

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

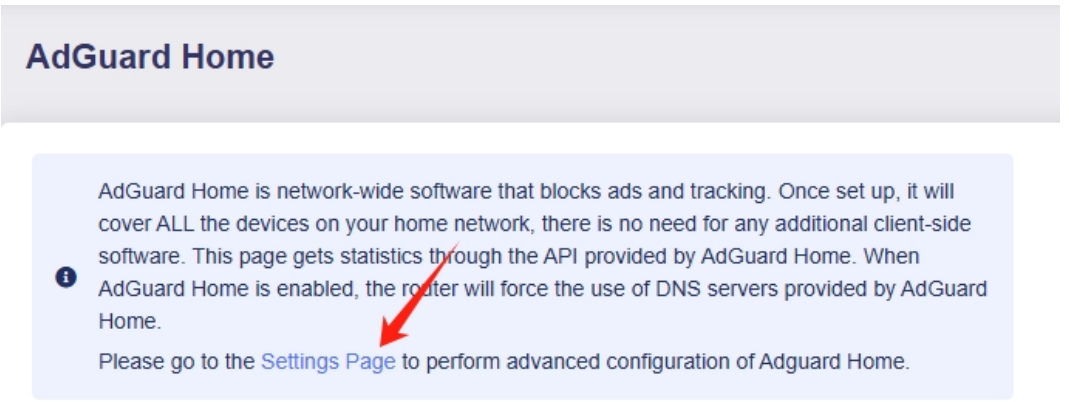


   - **AdGuard Home gestisce le richieste dei client**: se abilitato, le query DNS dai dispositivi client verranno gestite direttamente da AdGuard Home, ma ciò causerà il fallimento delle policy VPN basate sui domini.

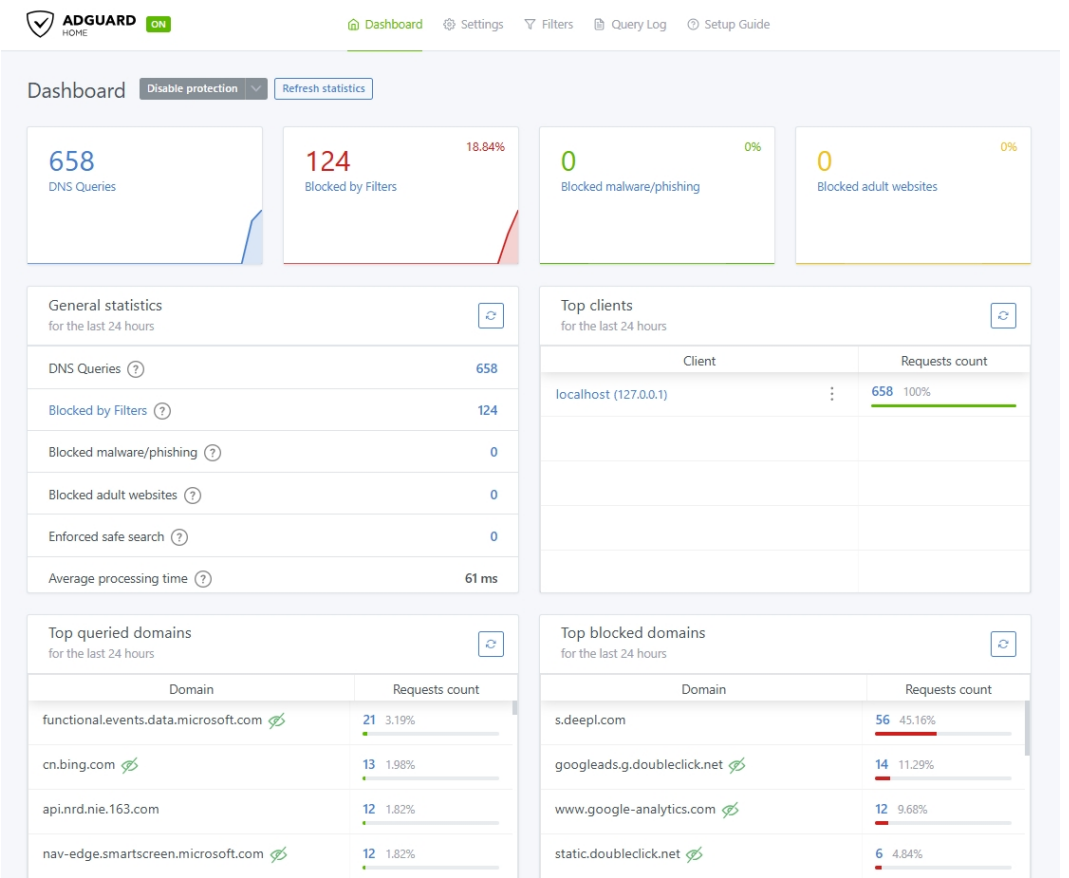
2. La pagina caricherà automaticamente le statistiche DNS (query, domini bloccati, ecc.) tramite l'API fornita da AdGuard Home.



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.



14.5 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. Vedi qui per ulteriori dettagli.

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.

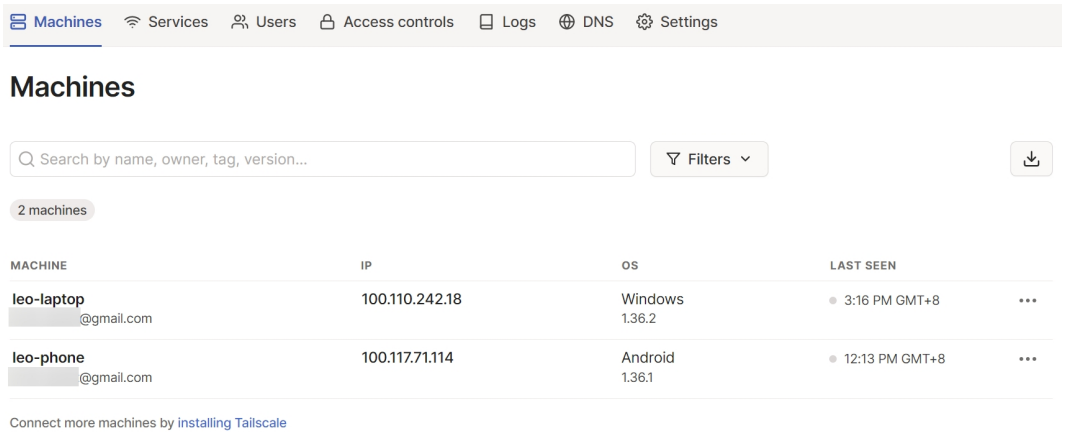
Nota:

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, AstroWarp.
2. Questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug.

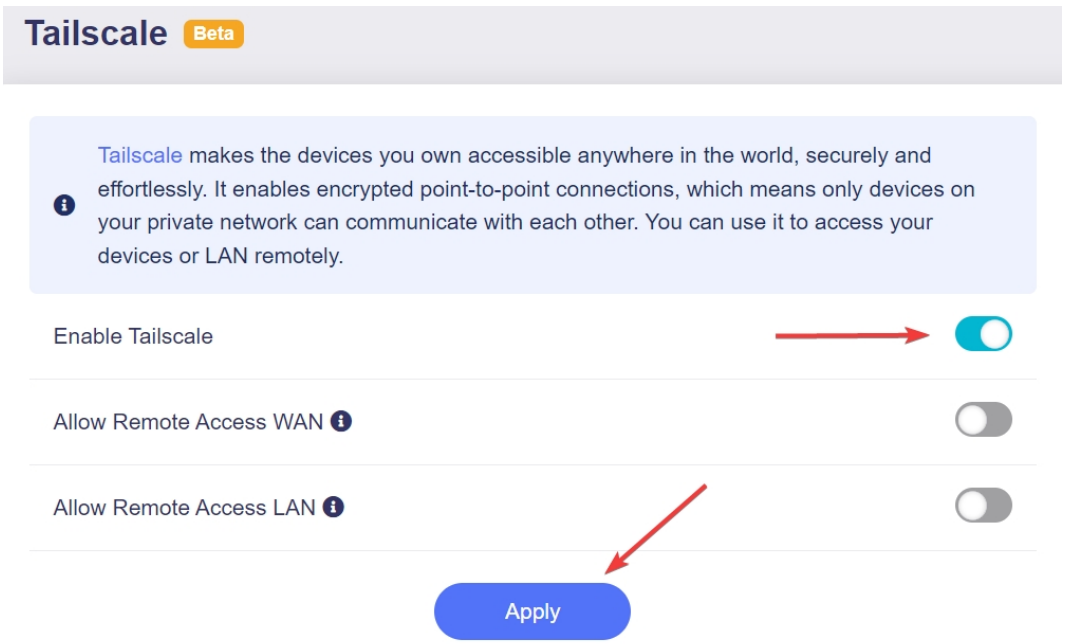
14.5.1 Configurazione di Tailscale

Ecco un esempio di utilizzo di GL-MT2500 per configurare la rete Tailscale.

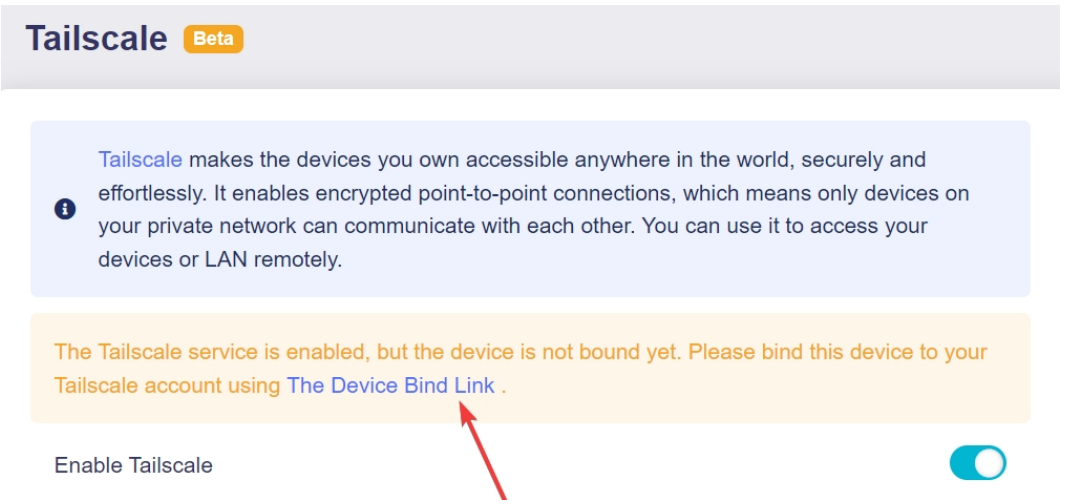
1. Registra prima un account Tailscale e associa uno o due dispositivi al tuo account Tailscale a scopo di test. Dopo l'associazione, vedrai i tuoi dispositivi nella console Tailscale.



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



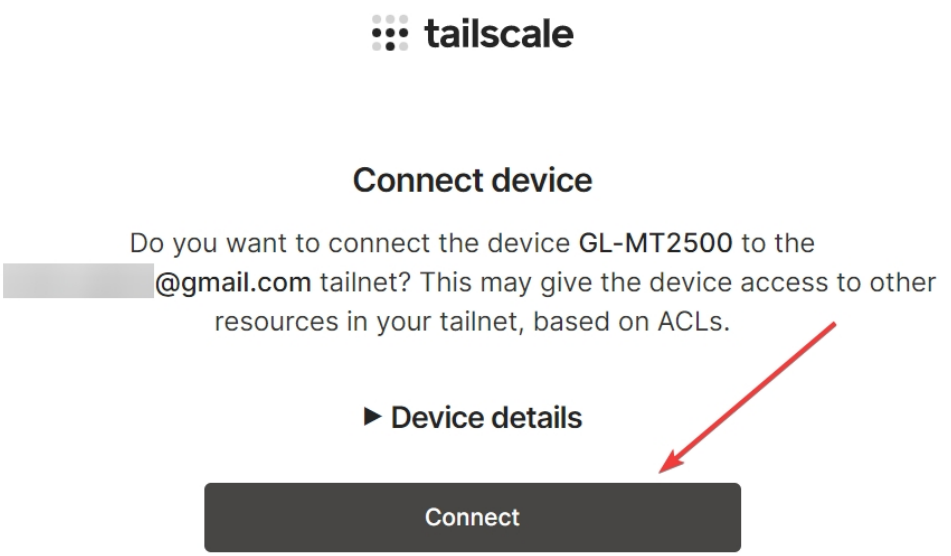
3. La pagina ti chiederà di associare il dispositivo. Fai clic su **Link di associazione del dispositivo**.



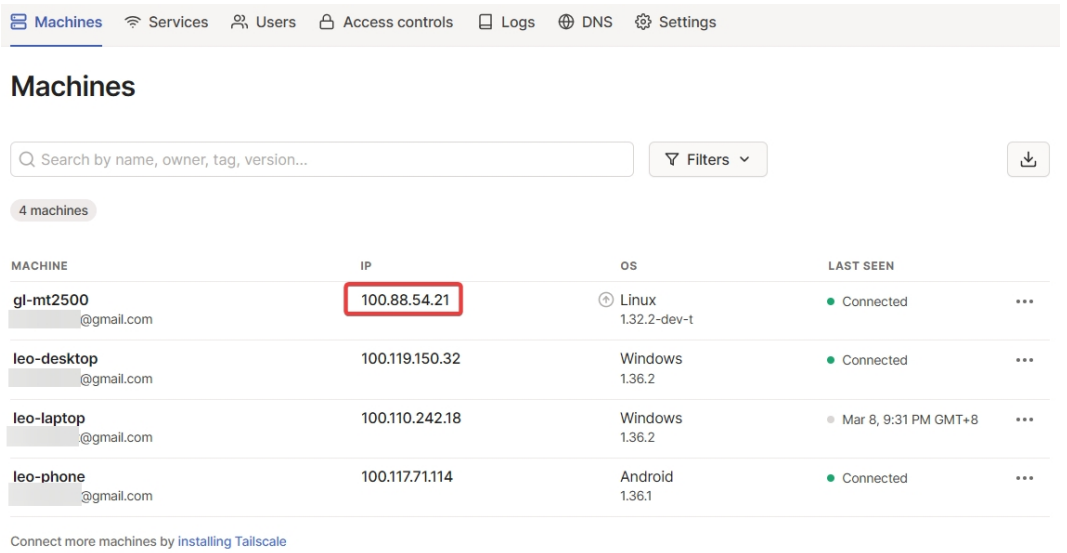
4. Nella finestra pop-up, fai clic sul collegamento e accedi con il tuo account Tailscale.



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 100.88.54.21.

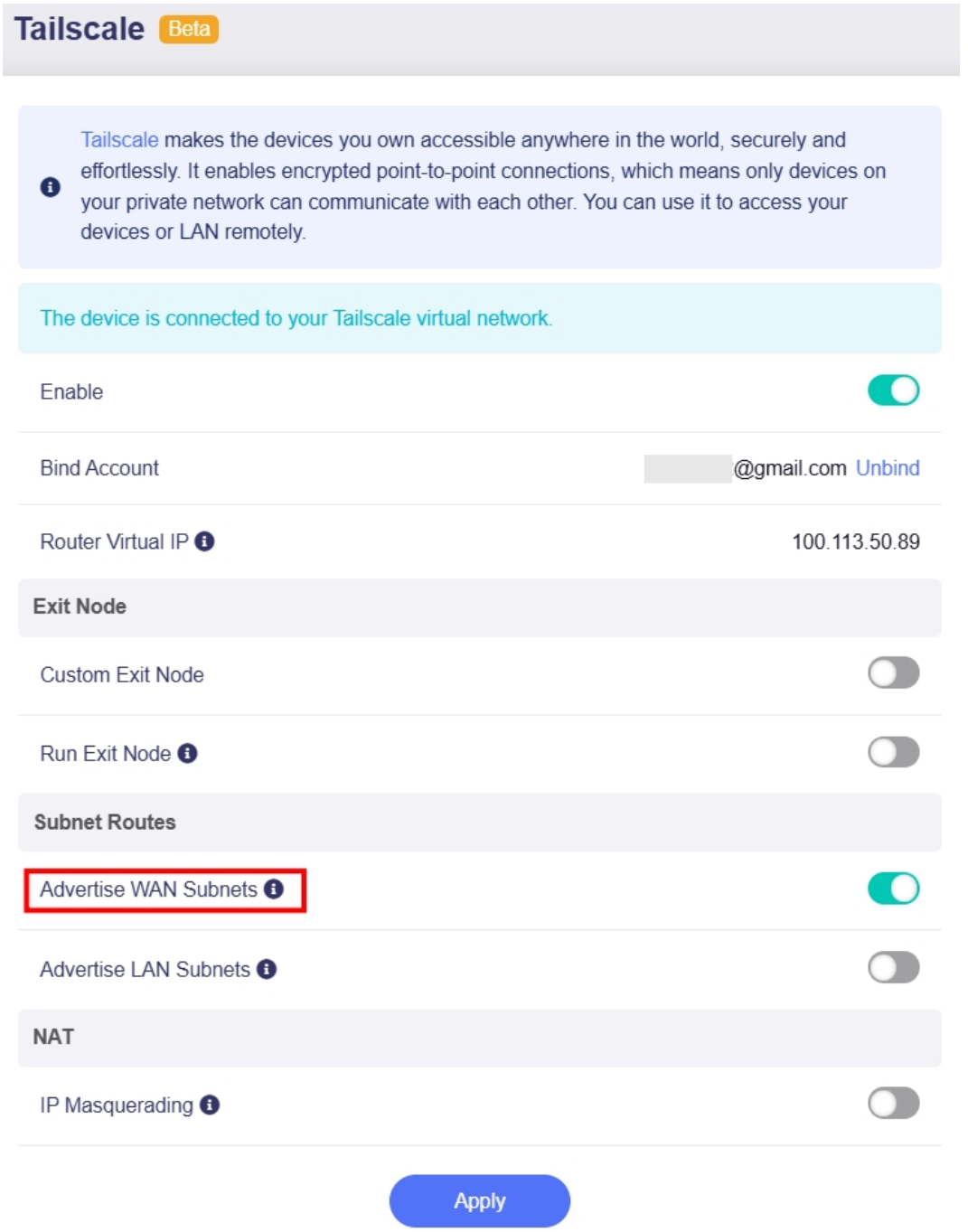


7. Verifica connettività.

   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.

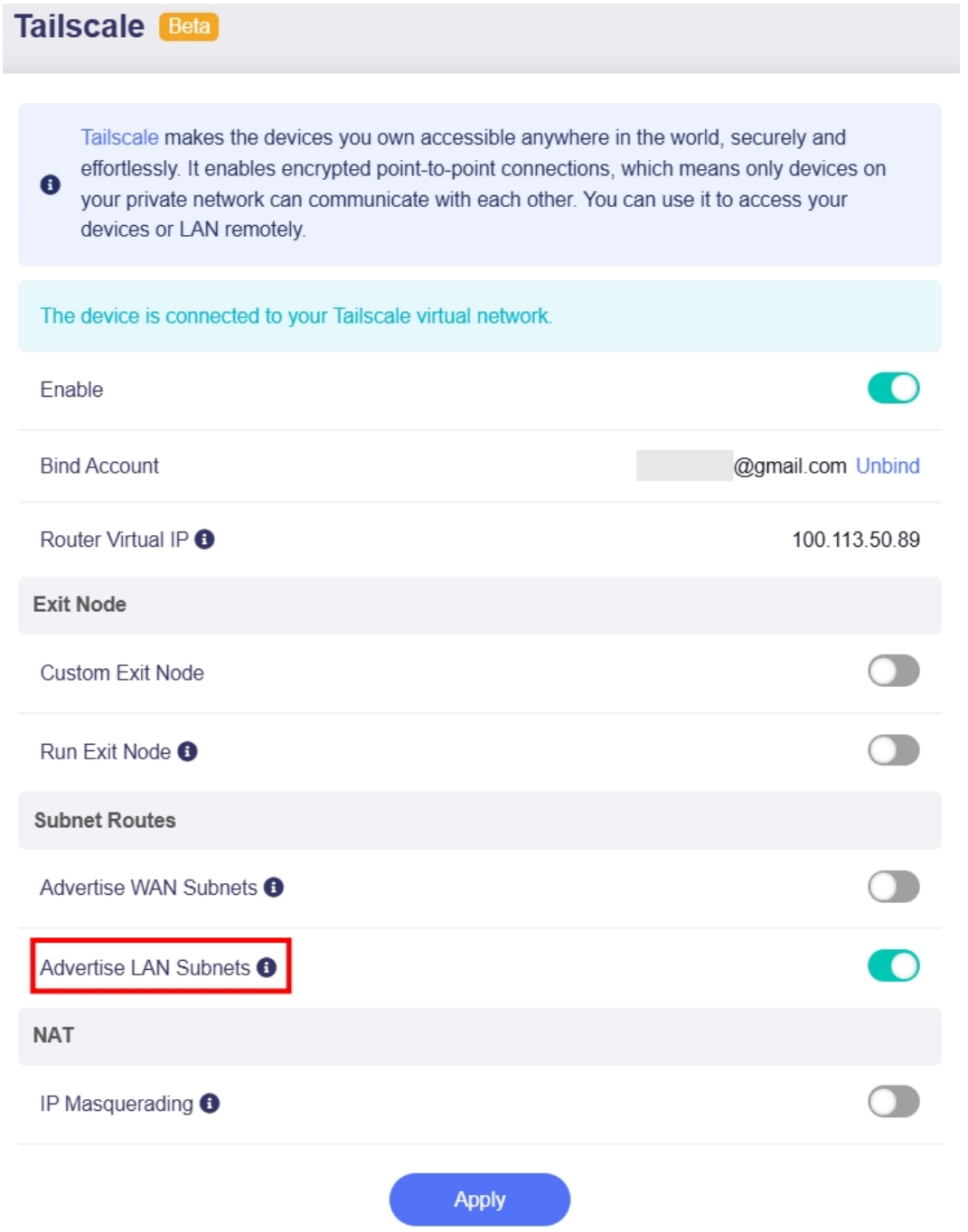
14.5.2 Annuncio delle sottoreti WAN

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.



14.5.3 Annuncio delle sottoreti LAN

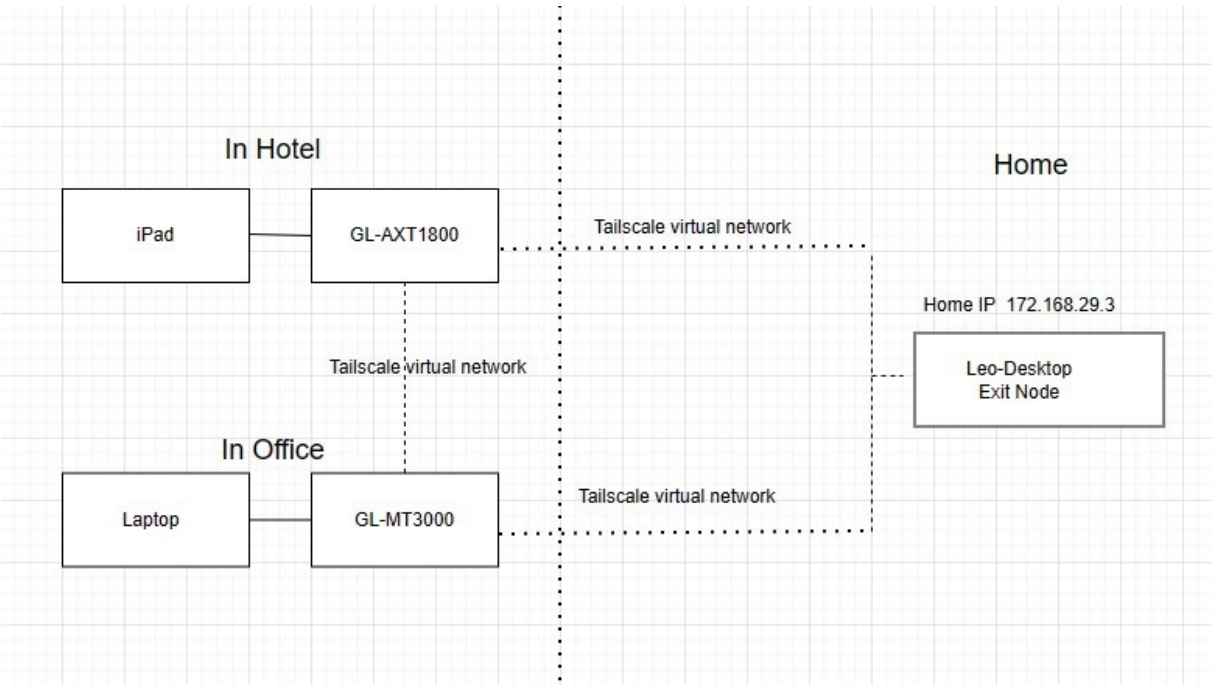
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato LAN del dispositivo tramite la rete virtuale Tailscale. Vedi qui per ulteriori dettagli.



14.5.4 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.



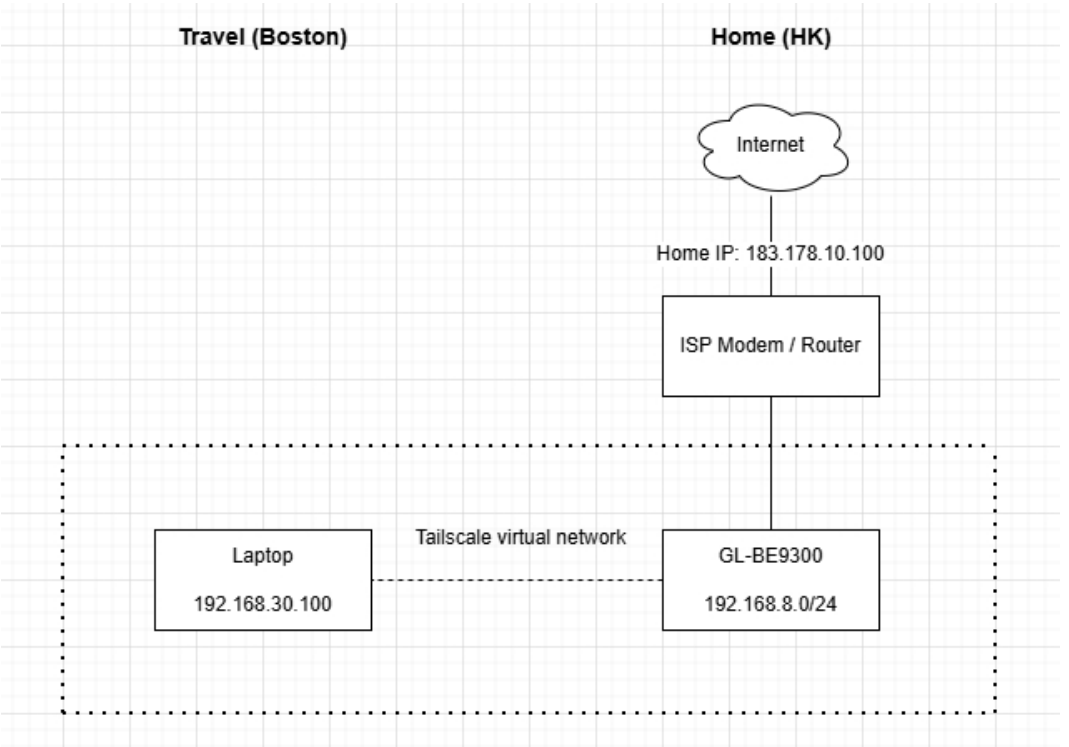
In sintesi, un nodo di uscita instrada il traffico Internet in uscita dai tuoi dispositivi Tailnet, agendo effettivamente come server VPN. Quando sei connesso a un nodo di uscita, tutto il tuo traffico Internet non Tailscale sembra provenire dalla sua posizione, aiutandoti ad accedere a contenuti con restrizioni geografiche e a migliorare la tua privacy online. Il dispositivo che gestisce questo inoltro del traffico viene definito "nodo di uscita". Vedi qui per maggiori dettagli.

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.

14.5.5 Esegui nodo di uscita

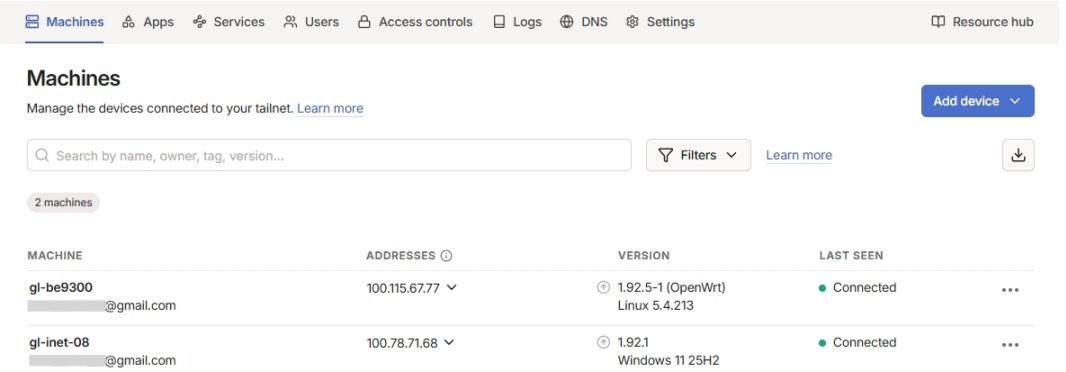
L'esecuzione di un nodo di uscita sul router consente ad altri dispositivi all'interno della tailnet di instradare tutto il traffico Internet in uscita tramite l'IP pubblico di questo router.

Nella topologia seguente, un laptop si trova a Boston, mentre un router GL-BE9300 si trova a Hong Kong. Entrambi sono stati aggiunti alla stessa rete Tailscale. Se imposti GL-BE9300 come nodo di uscita, tutto il traffico in uscita dal laptop uscirà attraverso questo router per accedere a Internet e l'IP pubblico del laptop verrà risolto in un indirizzo IP di Hong Kong anziché in uno di Boston.

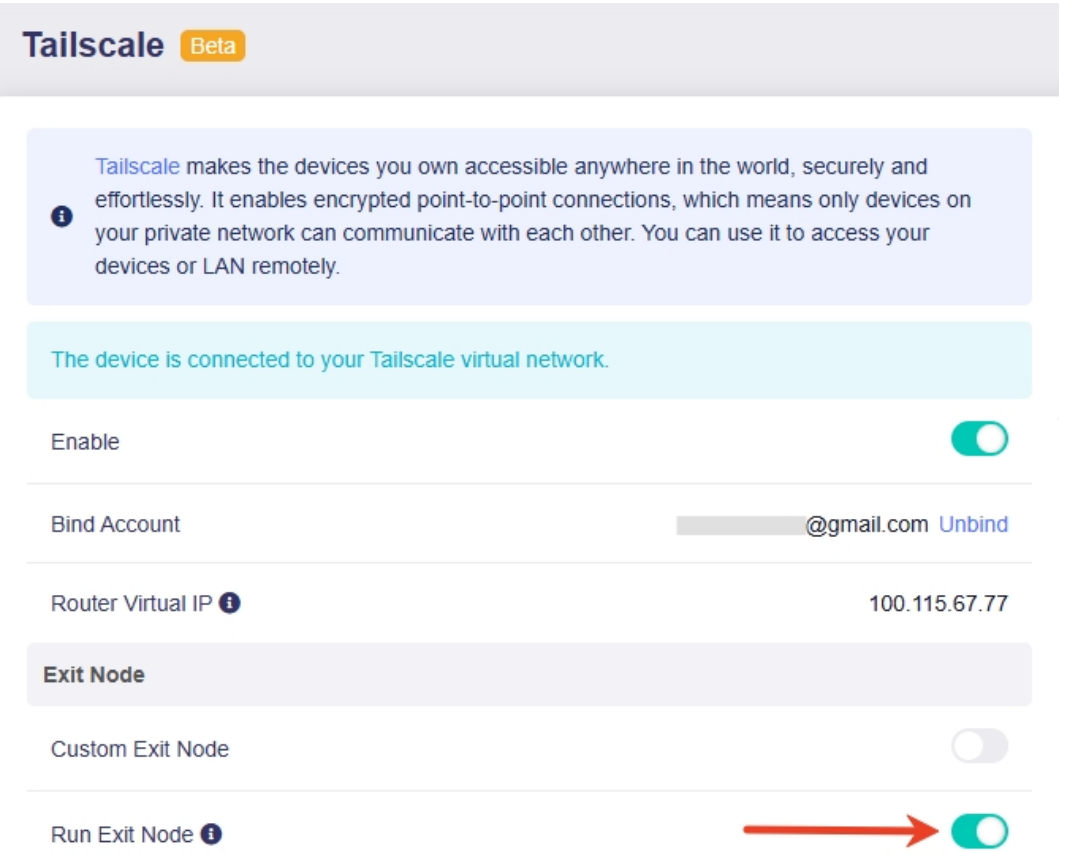


Ecco un esempio di configurazione di un router GL-BE9300 come nodo di uscita.

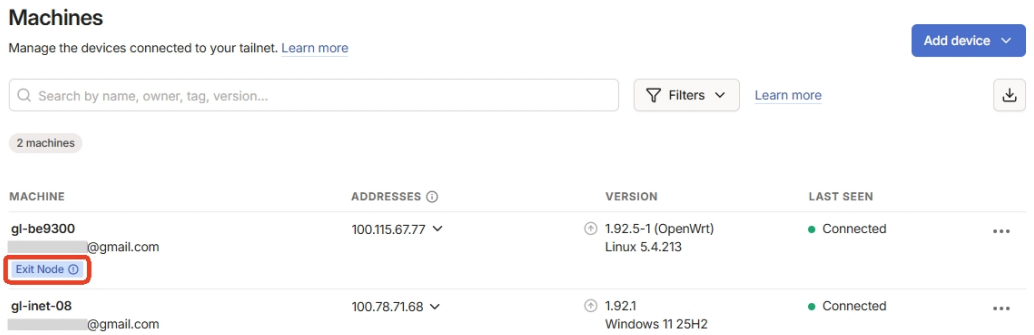
1. Registra sia GL-BE9300 che il laptop da viaggio sulla stessa rete Tailscale.



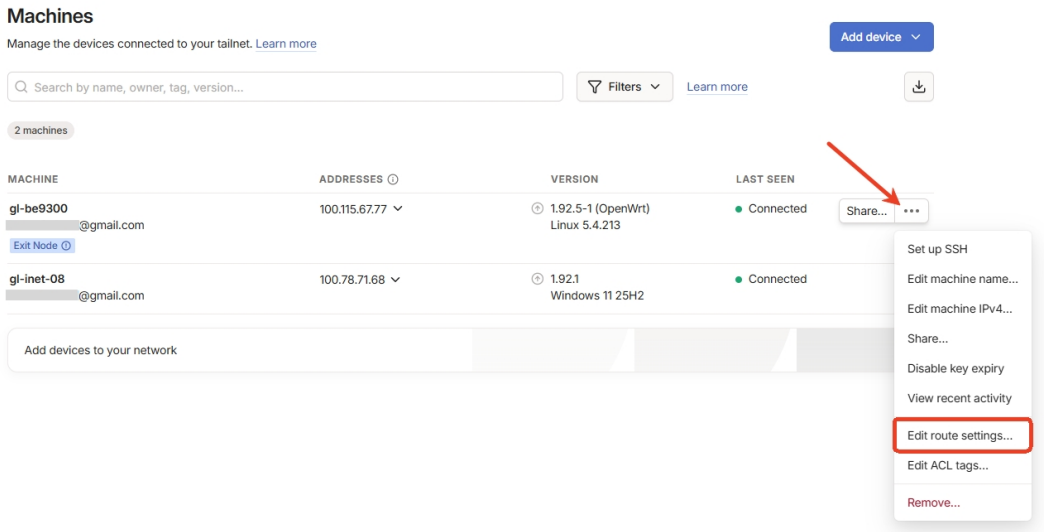
2. Nel pannello di amministrazione web di GL-BE9300, vai su APPLICAZIONI > Tailscale. abilita **Esegui nodo di uscita** e fai clic su **Applica**.



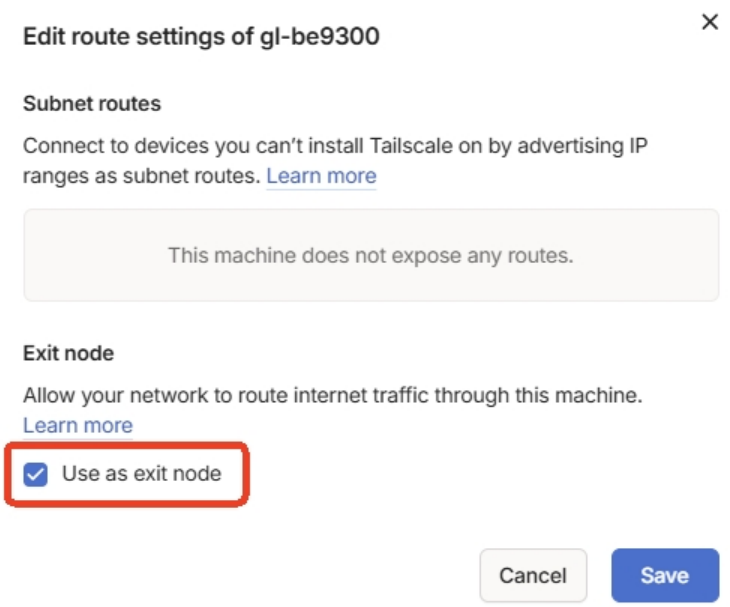
3. Vai alla console di amministrazione Tailscale e vedrai un tag "Nodo di uscita" sotto GL-BE9300.



4. Fai clic sull'icona a tre punti a destra di GL-BE9300 e seleziona **Modifica impostazioni percorso**.



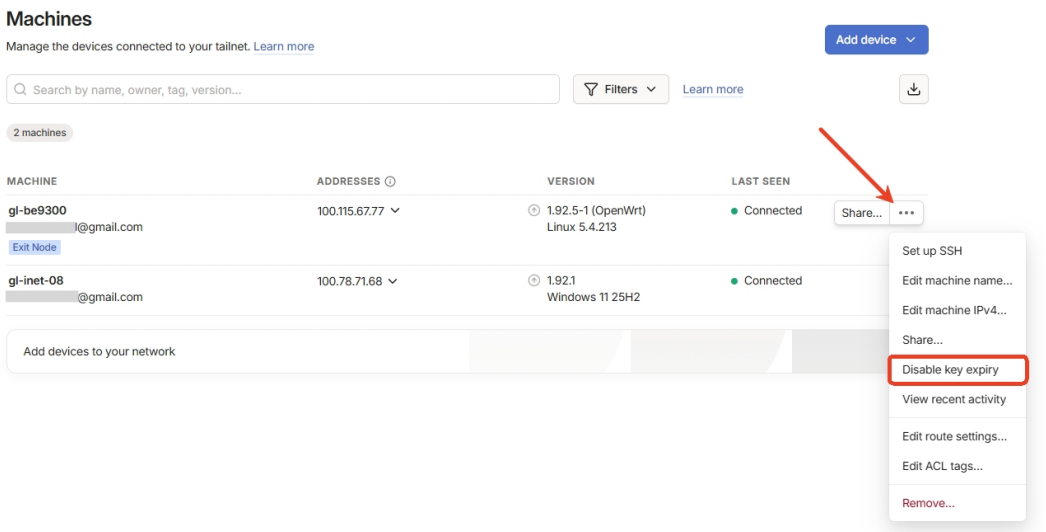
5. Nella finestra pop-up, seleziona **Utilizza come nodo di uscita** e fai clic su **Salva**.



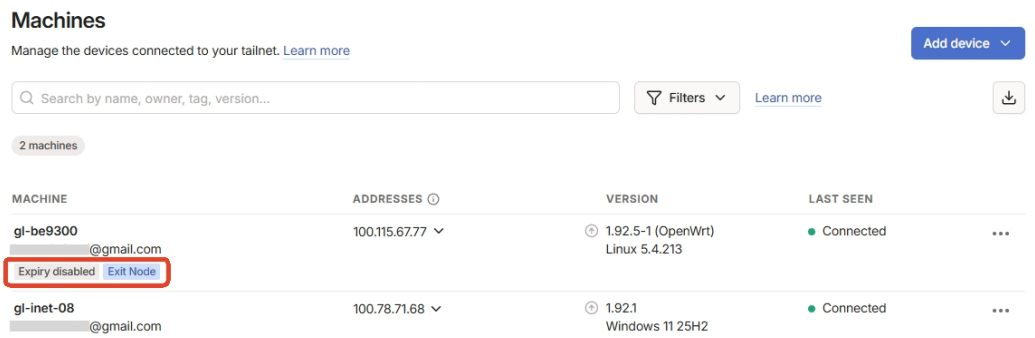
6. Disabilita scadenza chiave.

   Come funzionalità di sicurezza, gli utenti devono autenticarsi nuovamente periodicamente su ciascuno dei loro dispositivi. Per evitare disconnessioni alla scadenza della chiave di autenticazione del nodo di uscita, ti consigliamo di disabilitare la scadenza della chiave per il tuo nodo di uscita. Fai clic qui per ulteriori dettagli sulla scadenza della chiave.

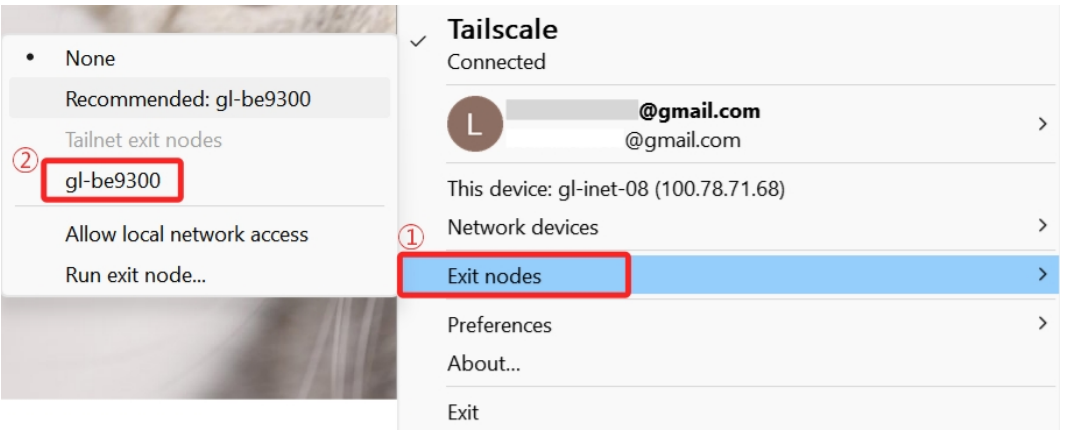
   Fai clic sull'icona a tre punti a destra di GL-BE9300 e seleziona Disabilita scadenza chiave.



   Una volta applicato, verrà visualizzato un tag "Scadenza disabilitata" sotto GL-BE9300.



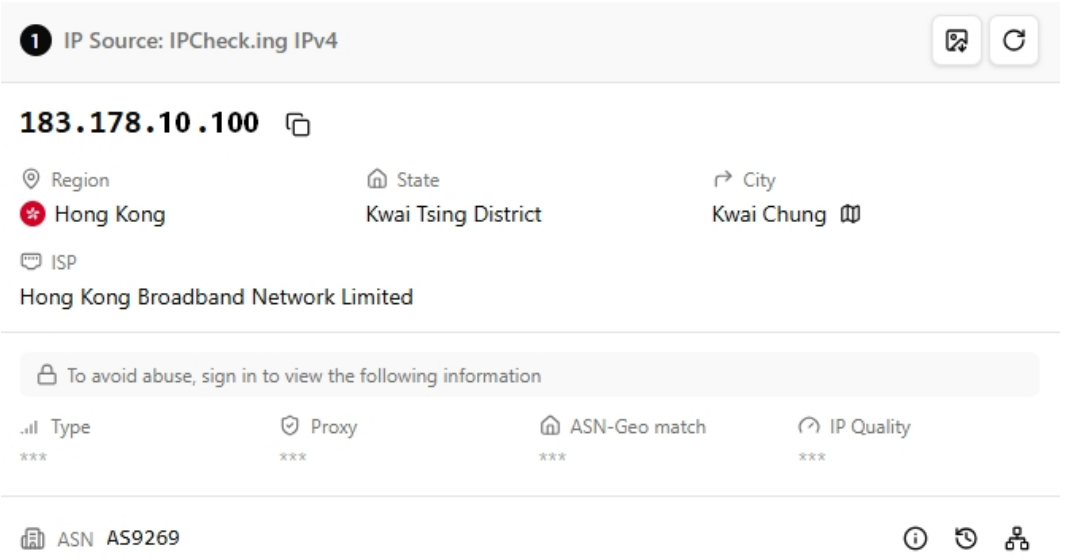
7. Esegui Tailscale sul tuo laptop da viaggio. L'icona Tailscale apparirà nella barra delle applicazioni nell'angolo in basso a destra. Fare clic con il tasto destro sull'icona, fare clic su **Nodi di uscita** e selezionare **gl-be9300**.



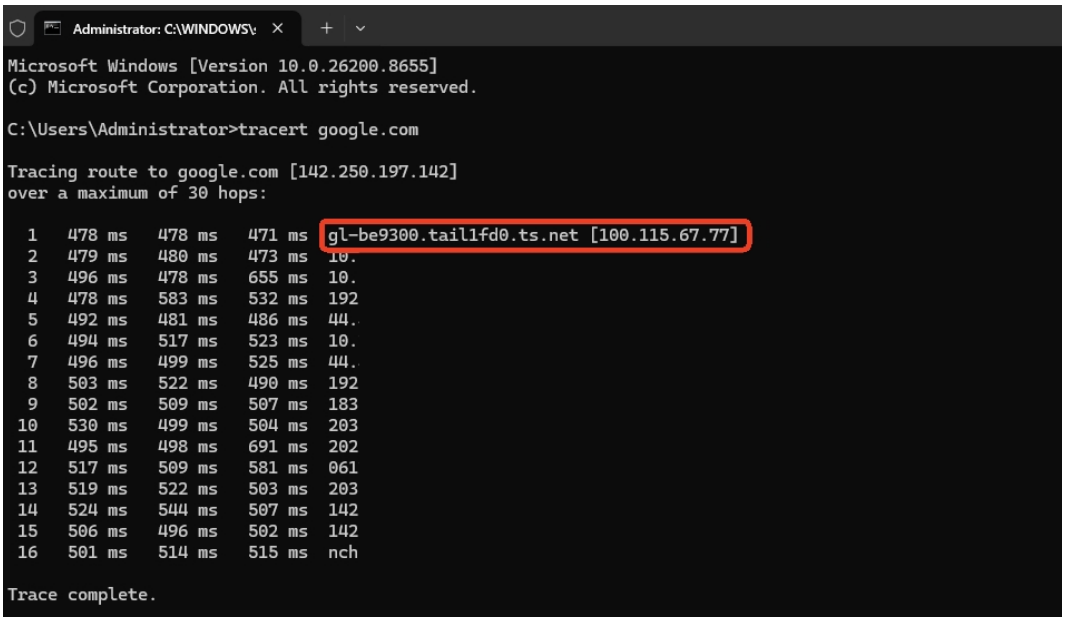
Ora, tutto il traffico in uscita da questo laptop da viaggio uscirà attraverso GL-BE9300 per accedere a Internet.

8. Verifica connettività.

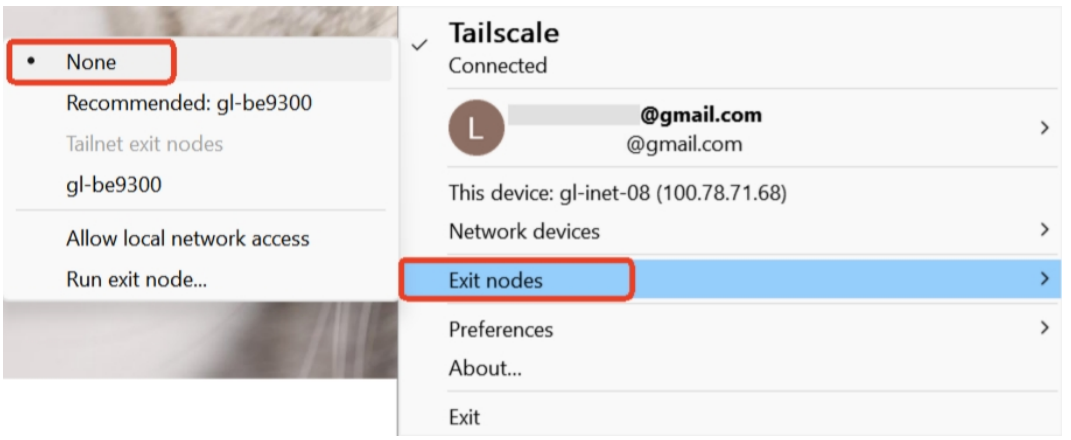
(1) Sul tuo laptop da viaggio, apri un browser web e visita ipcheck.ing o qualsiasi altro sito web di ricerca IP. La pagina visualizzerà l'indirizzo IP pubblico appartenente al tuo nodo di uscita Tailscale, confermando che il laptop sta accedendo a Internet tramite il nodo di uscita (lo GL-BE9300 situato a Hong Kong, in questo esempio).



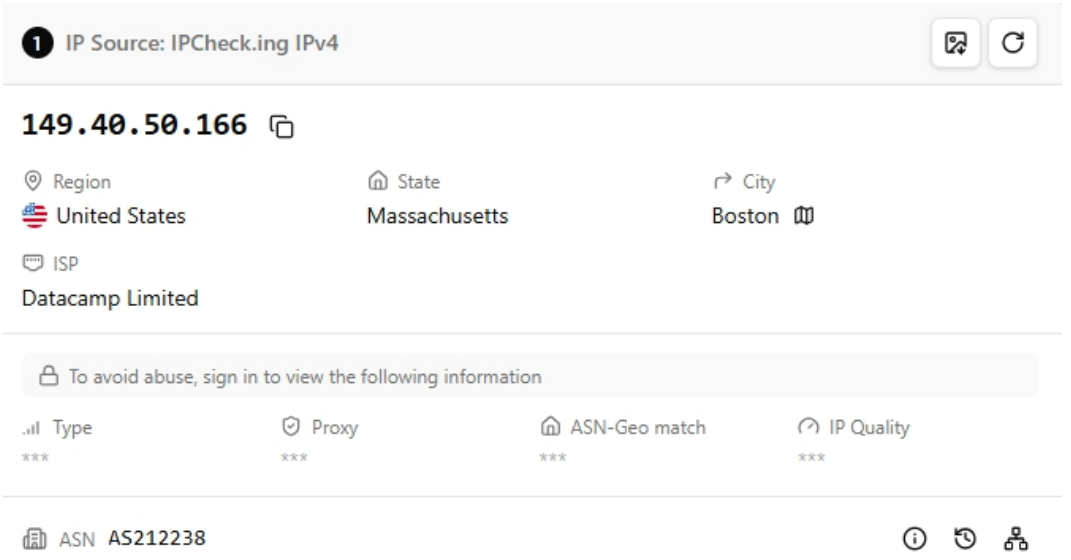
(2) Premi *Win+R*, digita *cmd* per avviare il prompt dei comandi, quindi esegui *tracert google.com* per tracciare i percorsi del traffico in uscita. L'output del comando elenca tutti gli hop di routing per il tuo traffico Internet. Se configurato correttamente, il primo hop esterno verrà instradato attraverso il nodo di uscita, come mostrato di seguito, verificando che tutto il traffico Internet in uscita esca attraverso questo router.



(3) Disconnetti il nodo di uscita per un test comparativo. Fai clic con il pulsante destro del mouse sull'icona Tailscale nella barra delle applicazioni nell'angolo in basso a destra, fai clic su **Nodi di uscita** quindi seleziona **Nessuno** per smettere di utilizzare il nodo di uscita.



(4) Apri una nuova scheda del browser e visita ipcheck.ing o qualsiasi servizio di ricerca IP. Ora mostrerà l'indirizzo IP pubblico nativo del tuo laptop, dimostrando che il dispositivo sta utilizzando invece la tua connessione Internet locale (Boston, in questo esempio).


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

14.6 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:

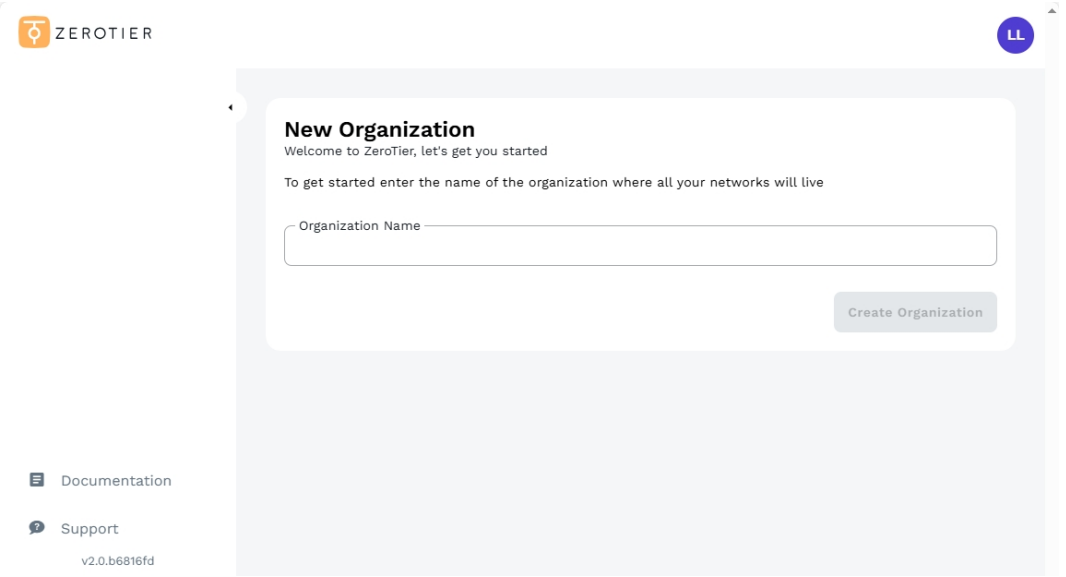
1. Non è consigliabile utilizzare ZeroTier contemporaneamente a una qualsiasi delle seguenti funzionalità o servizi, poiché ciò potrebbe causare conflitti di routing: Client OpenVPN, Client WireGuard, GoodCloud da sito a sito, Tailscale e AstroWarp.
2. Questa funzionalità è attualmente in versione beta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

14.6.1 Configurazione di ZeroTier

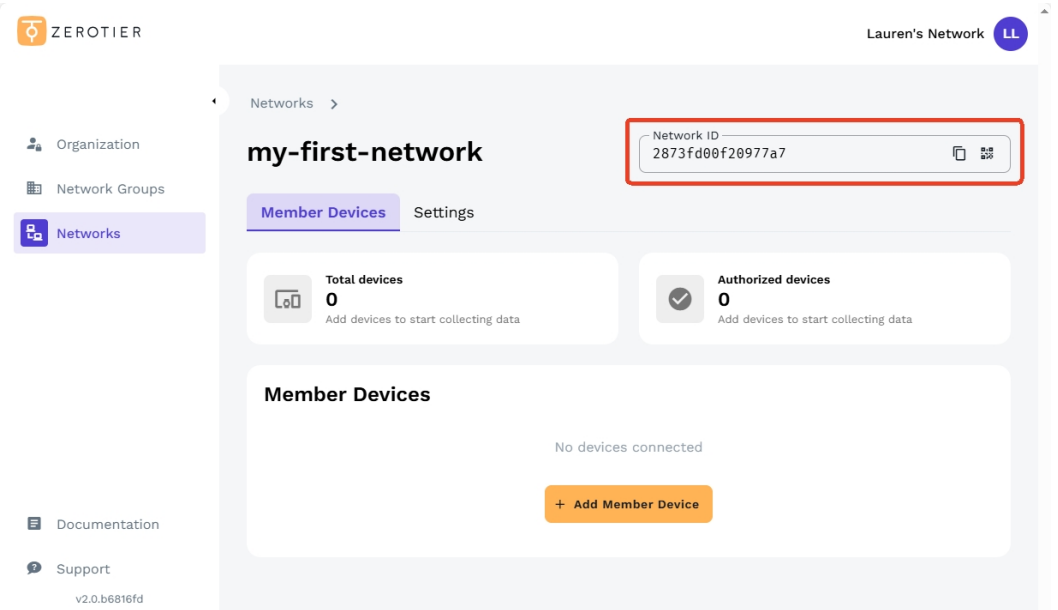
Sono disponibili due versioni di ZeroTier Central: New Central e Legacy Central.

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.

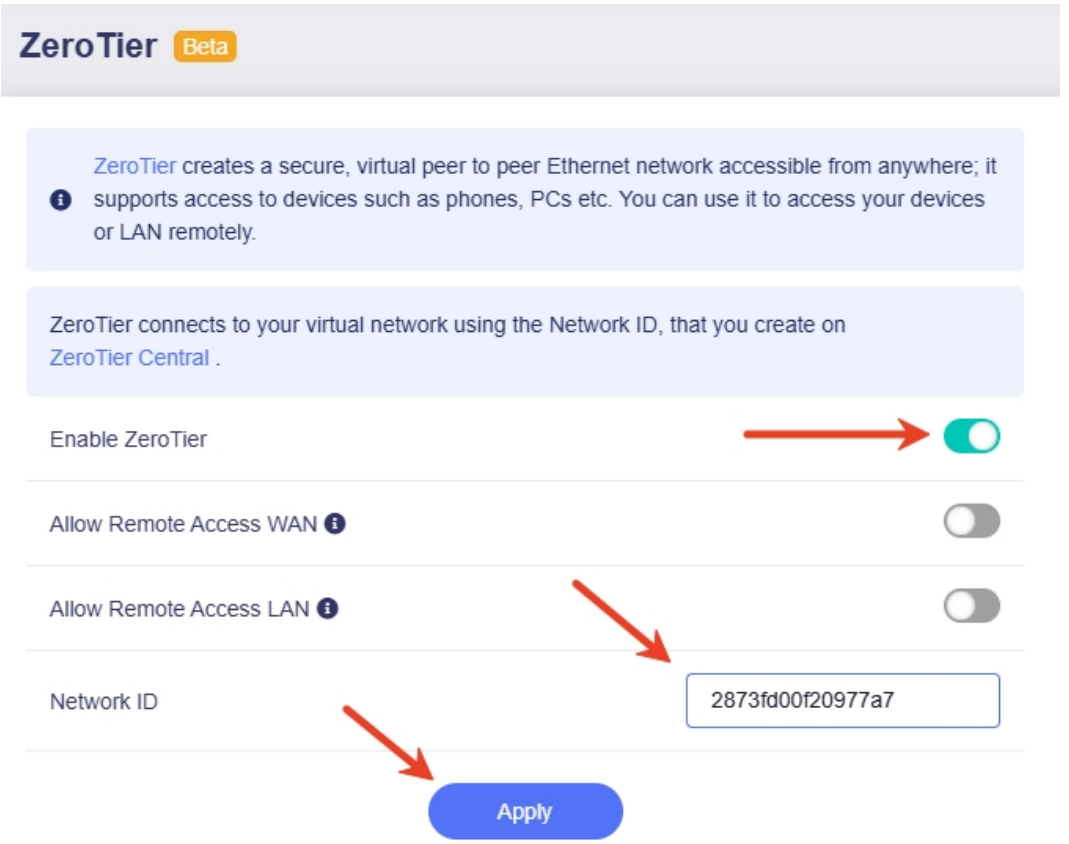


3. Seleziona un piano. Qui scegliamo **come esempio il piano Personal**, che include i dispositivi 10, l'amministratore di rete 1 e la rete 1. Se devi creare più reti, aggiungere più dispositivi o aggiungere percorsi e DNS personalizzati, scegli un altro piano a pagamento.
4. Ora la tua rete ZeroTier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

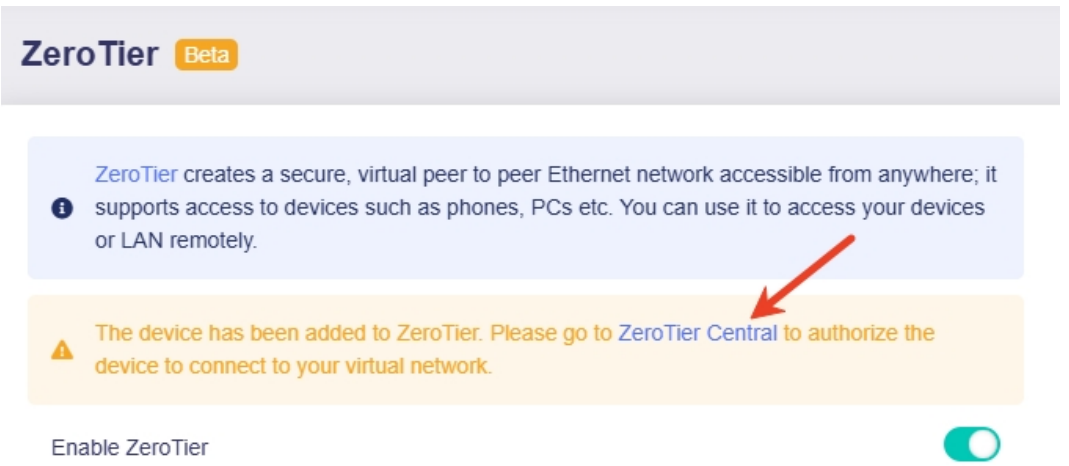


Usa nota **dell'ID di rete**, che è una combinazione alfanumerica di caratteri 16 nell'angolo in alto a destra, poiché sarà richiesto quando connetterai altri dispositivi in seguito.

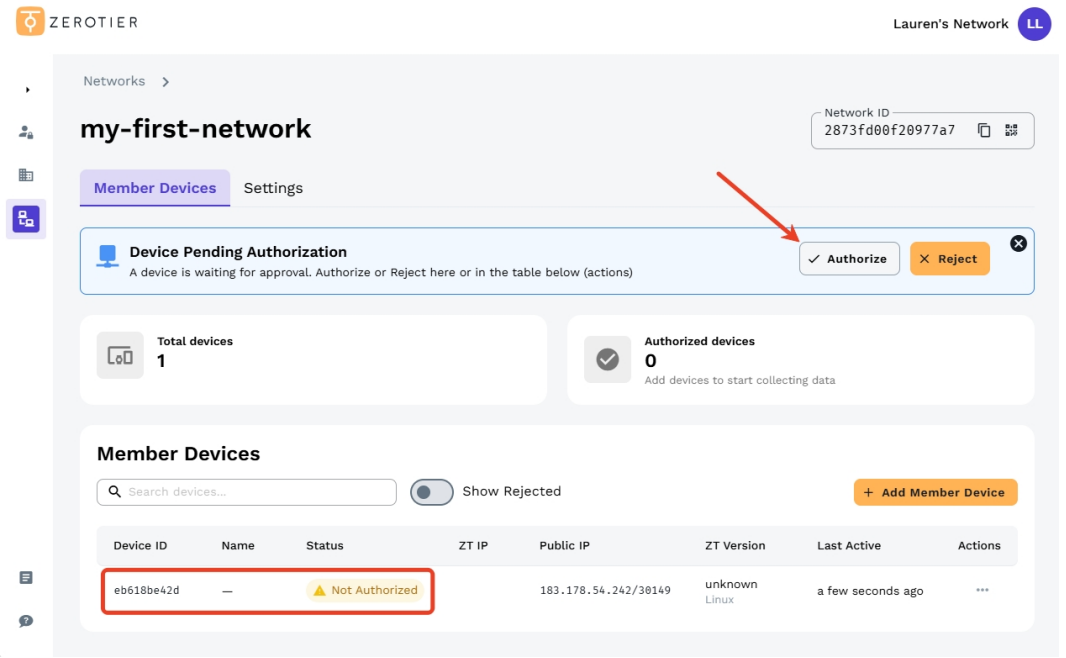
5. Accedi al pannello di amministrazione web del tuo router e vai su **APPLICAZIONI** -> **ZeroTier**. Abilita ZeroTier, inserisci **l'ID di rete**, quindi fai clic su **Applica**.



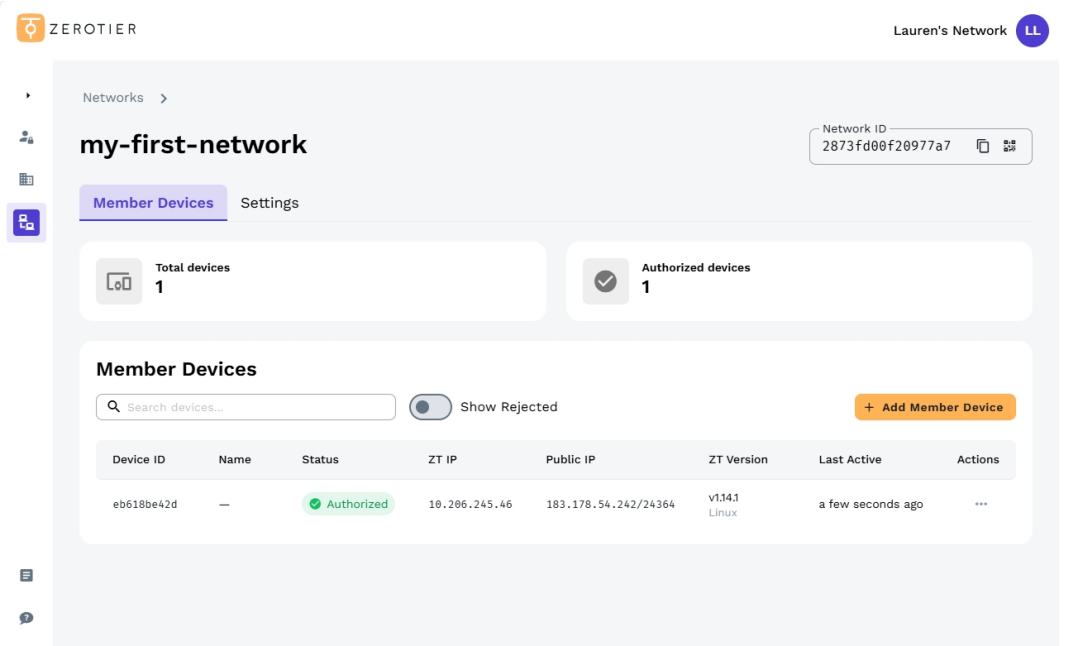
Dopo poco, la pagina indicherà che è necessaria l'autorizzazione. Fare clic **sul collegamento ipertestuale ZeroTier Central** per reindirizzare allo ZeroTier Central.



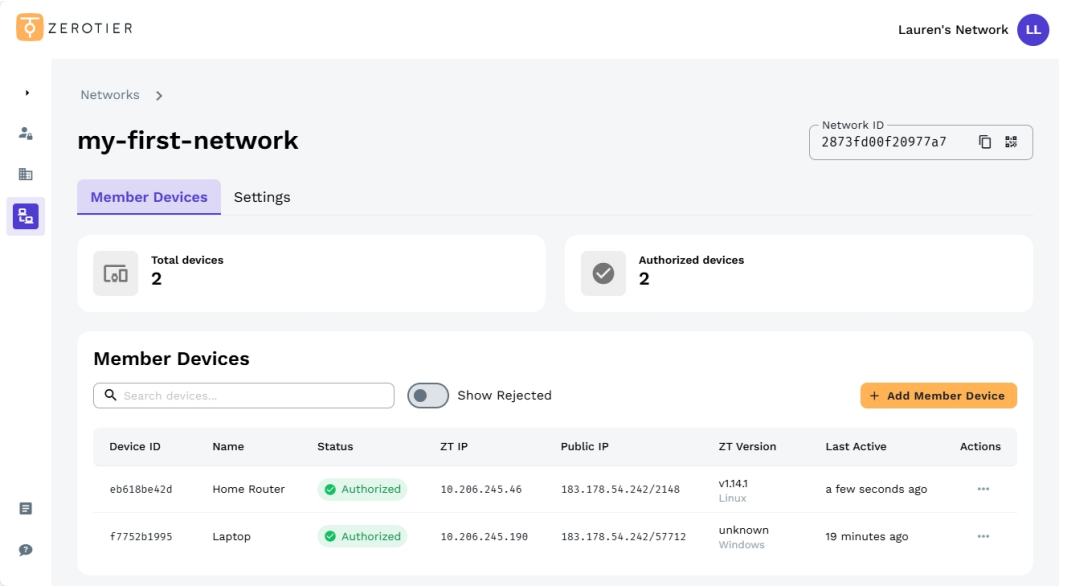
6. Sul ZeroTier Central, individua il dispositivo in sospeso e autorizzalo.



Una volta autorizzata, la pagina viene visualizzata come segue.

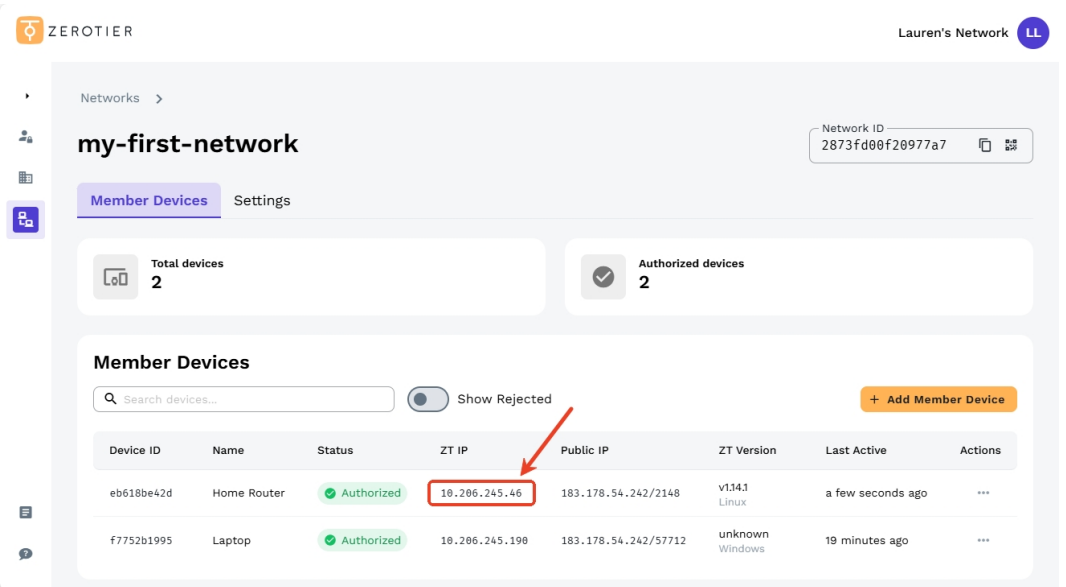


7. Aggiungi un altro dispositivo (come un computer o uno smartphone) alla stessa rete ZeroTier seguendo questa guida. Una volta aggiunta correttamente, la pagina viene visualizzata come segue. Vedrai i dettagli dei dispositivi membri, come ID dispositivo, nome, stato, IP gestito e IP pubblico.



Suggerimenti: 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.



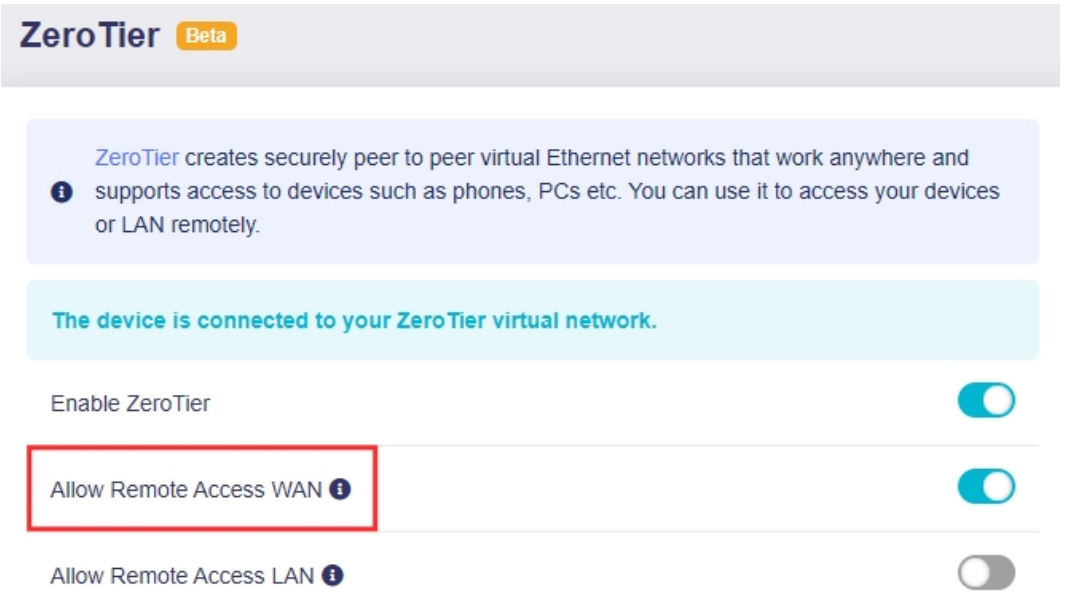
Puoi quindi utilizzare questo IP gestito per accedere al router dal tuo laptop che si trova sulla stessa rete ZeroTier.

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.

14.6.2 Consenti accesso remoto WAN

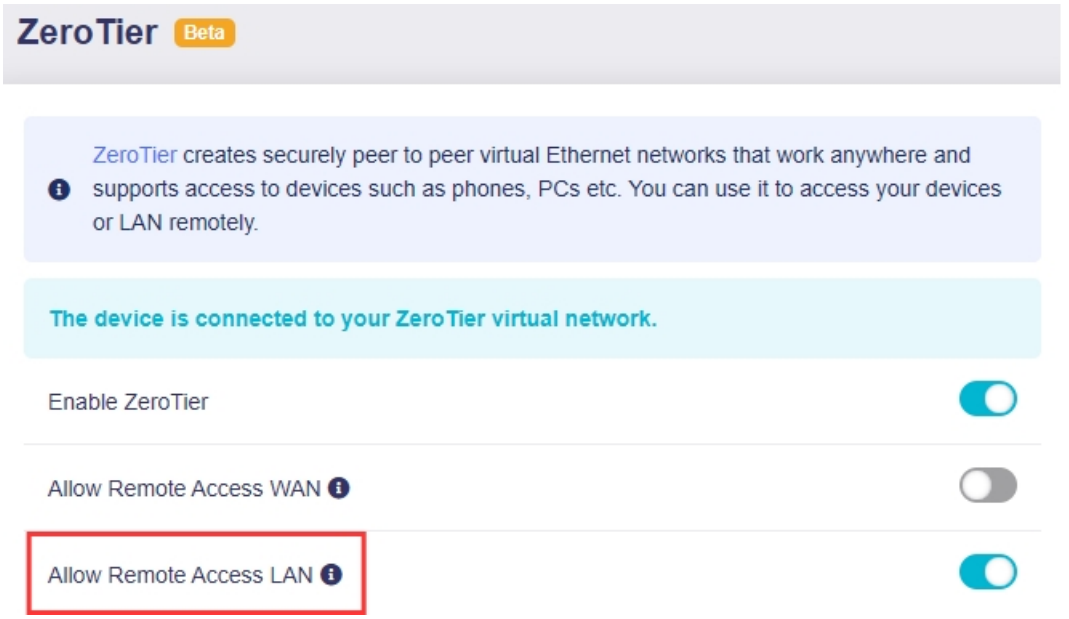
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato WAN del dispositivo tramite la rete virtuale ZeroTier. Vedi qui per maggiori dettagli.



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.

14.6.3 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.

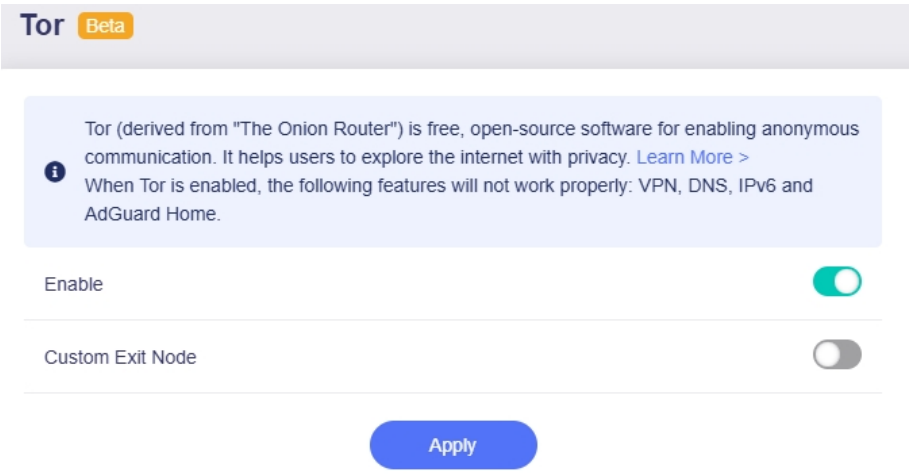
14.7 Tor

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.

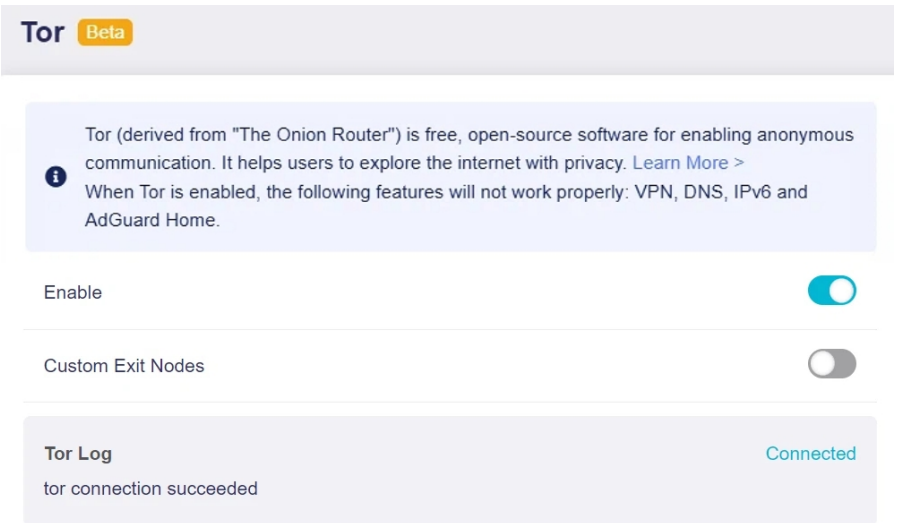
Quando Tor è abilitato, le seguenti funzionalità non funzioneranno correttamente: VPN, DNS, IPv6 e AdGuard Home.

Segui i passaggi seguenti per configurare Tor secondo necessità.

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



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



Capitolo 15

Sistema

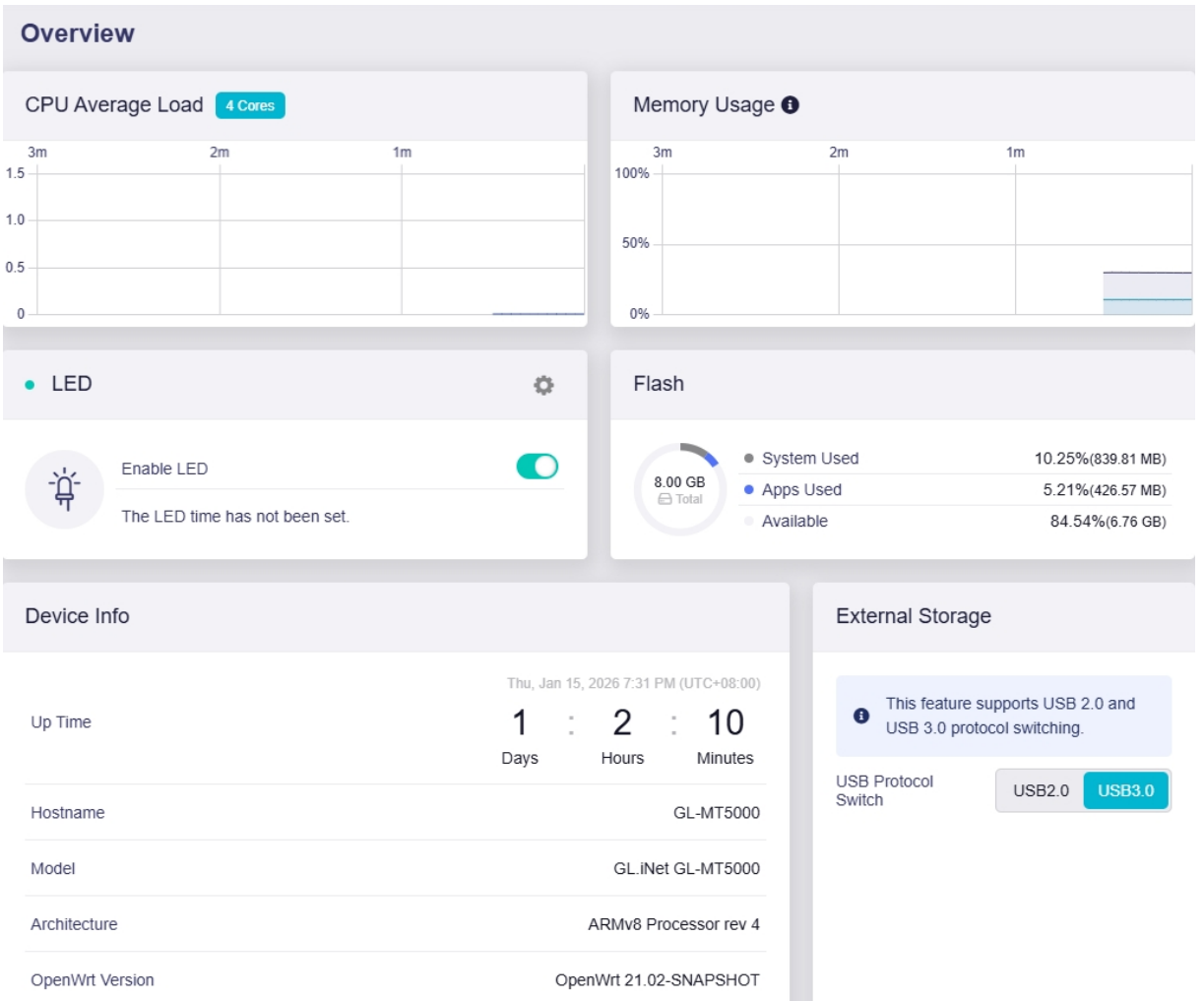
Questo capitolo tratta gli strumenti di sistema del dispositivo, tra cui panoramica del sistema, password dell'amministratore, aggiornamento, attività pianificate, fuso orario, registro, ripristino del firmware e impostazioni avanzate.

15.1 Panoramica

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Panoramica**.

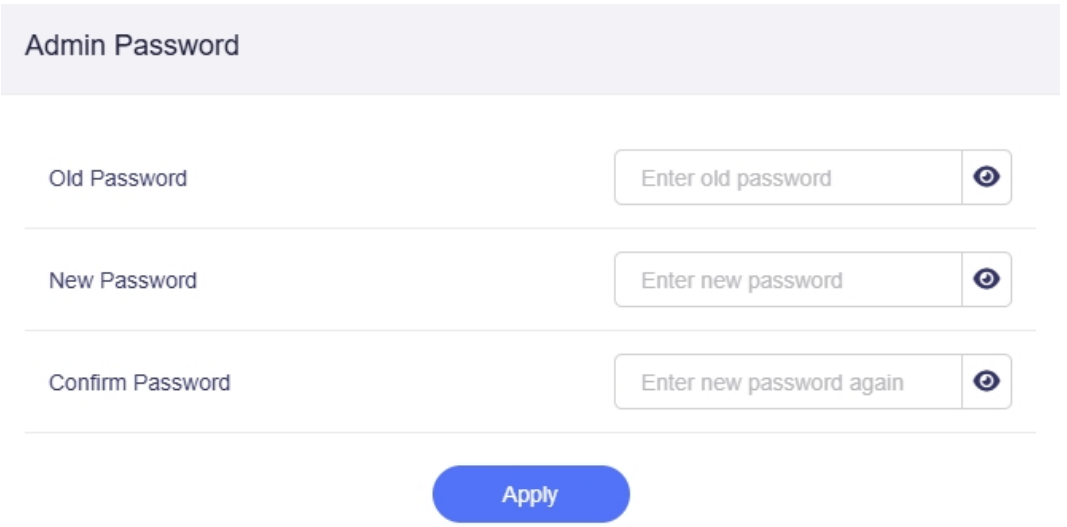
Questa pagina mostra lo stato dell'hardware e supporta alcuni semplici controlli, tra cui:

- Stato CPU, memoria, Flash e dispositivi di archiviazione esterni
- Controllo LED
- Informazioni sul dispositivo



15.2 Password amministratore

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Password amministratore**. È possibile modificare la password di accesso del pannello di amministrazione web.



I requisiti per la password amministratore sono i seguenti:

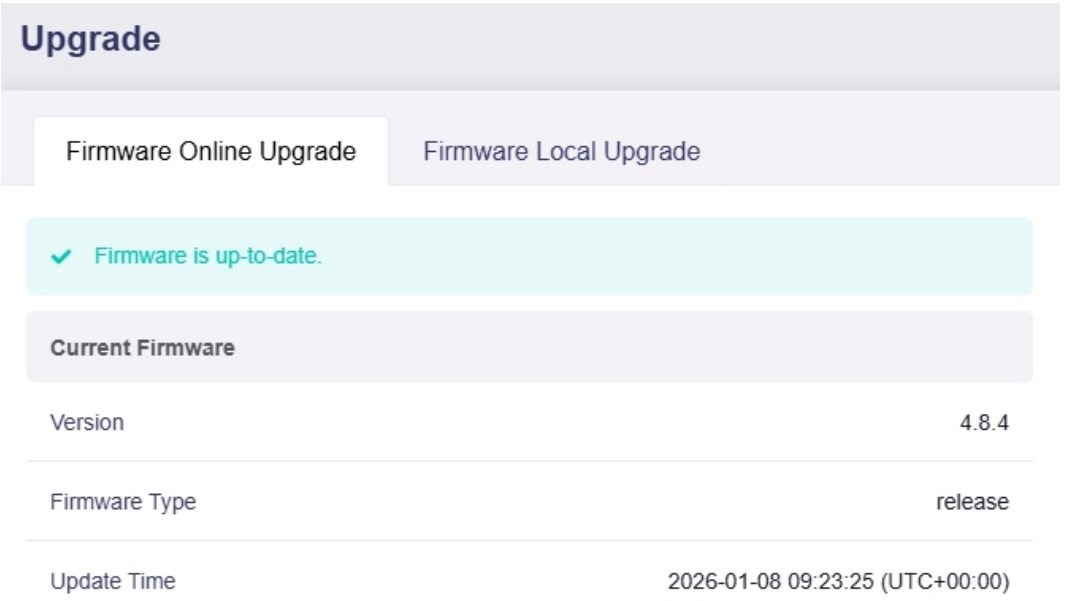
1. Minimo 10 caratteri e massimo 63 caratteri di lunghezza.
2. Sono consentiti lettere (con distinzione tra maiuscole e minuscole), numeri e simboli (ad esempio,! @ # $ % ^ & * ( ) _ + - =,. > < |? / \ [ ] { }:; " ' ` ~).
3. Sono richieste almeno due delle seguenti categorie: lettere maiuscole, lettere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

15.3 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.

15.3.1 Aggiornamento online

Puoi trovare i dettagli del firmware corrente qui, inclusi la versione del firmware, il tipo di firmware (ad esempio, versione, beta) e l'ora dell'aggiornamento.



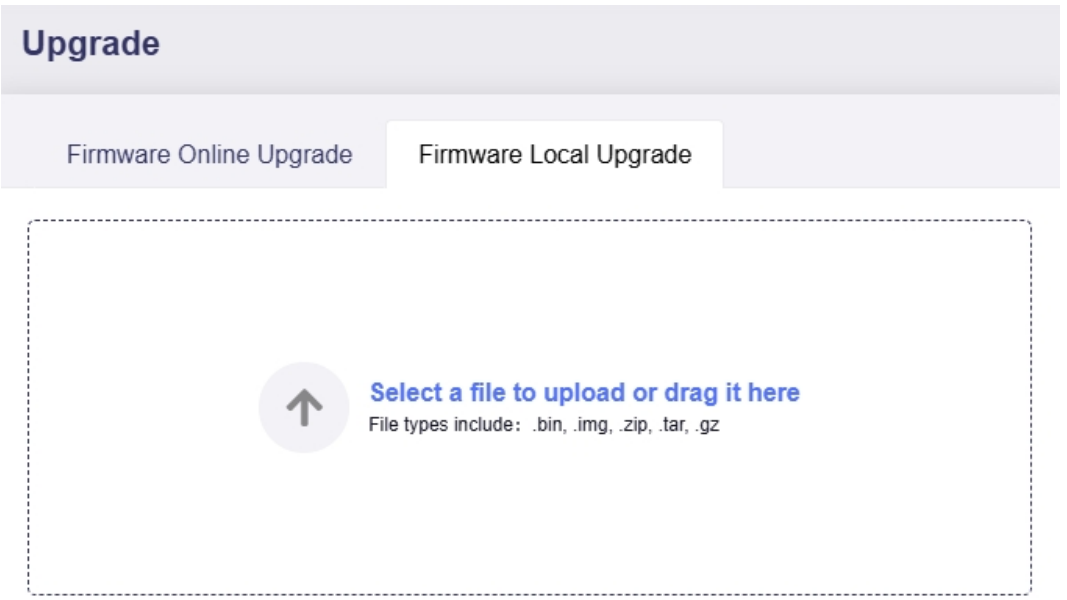
Se il router è connesso a Internet, verificherà la presenza della versione firmware più recente disponibile per il download.

Suggerimenti: quando si tenta di eseguire un aggiornamento online, se viene visualizzato **Download non riuscito**, accedere a **SISTEMA** -> **Fuso orario** e correggere l'errore del fuso orario (sincronizzazione con il browser).

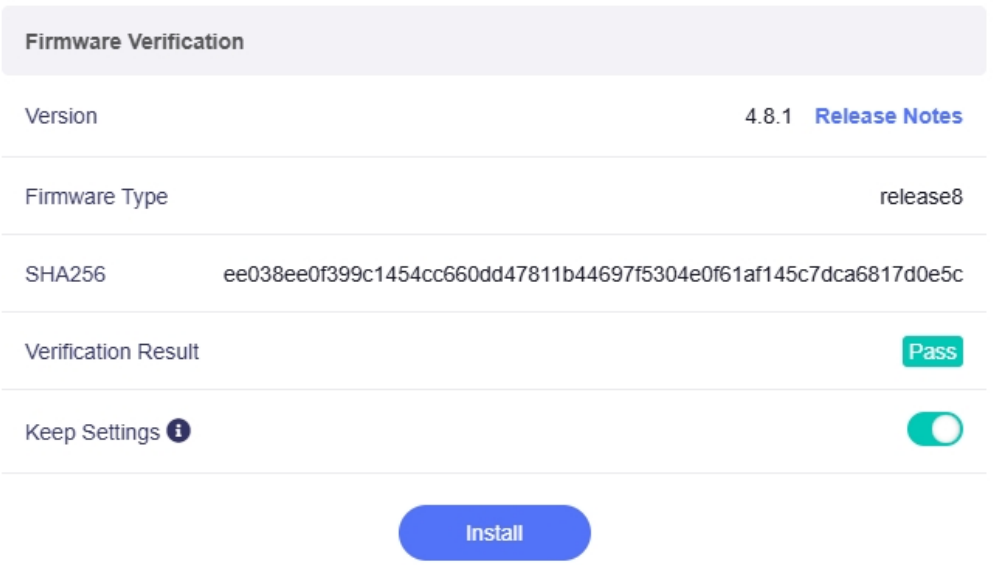
15.3.2 Aggiornamento locale

Questo metodo 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**.



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

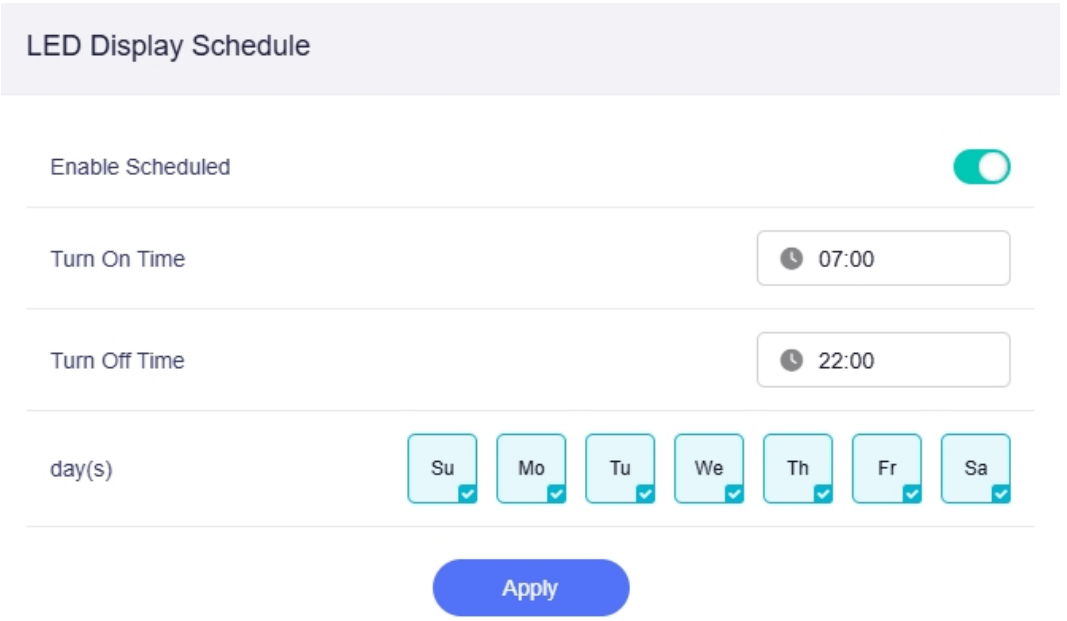
15.4 Attività pianificate

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: sincronizzare innanzitutto l'ora nello Fuso orario prima di utilizzare questa funzione. Se il dispositivo viene spento all'orario previsto, l'attività non verrà eseguita.

15.4.1 Programmazione del LED

Questa funzione ti consente di impostare una programmazione per la luce LED del tuo router.



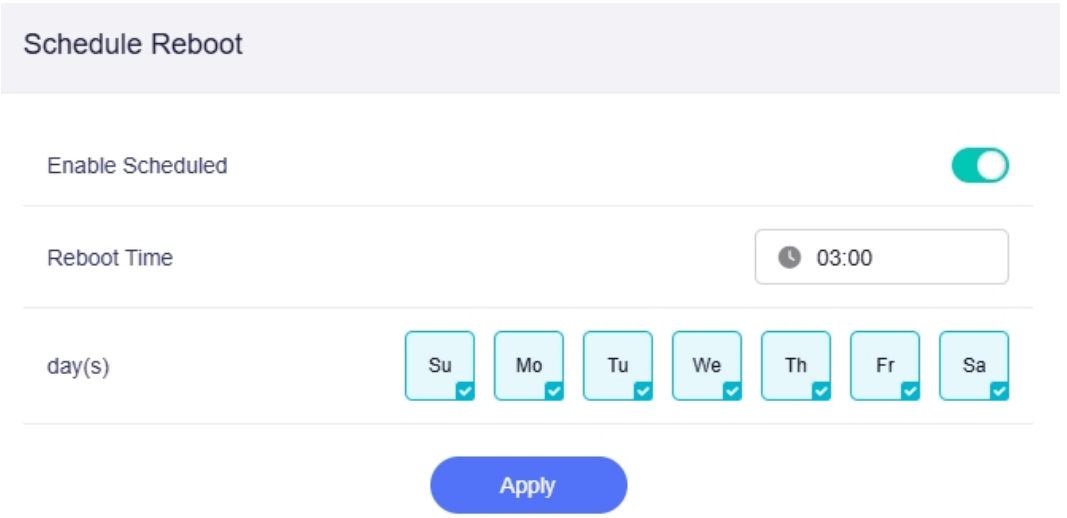
- **Abilita programmazione**: attiva questo interruttore per abilitare la pianificazione del display LED.
- **Durata di accensione**: imposta l'ora (ad esempio, 07:00) in cui la luce LED si accenderà.
- **Durata di spegnimento**: imposta l'ora (ad esempio, 22:00) in cui la luce LED si spegnerà.

- **giorno(i): seleziona i giorni** effettivi della settimana per queste impostazioni.

Dopo la configurazione, fai clic su **Applica** per salvare le impostazioni.

15.4.2 Riavvio pianificato

Questa funzione ti consente di impostare una pianificazione per il riavvio automatico del router.

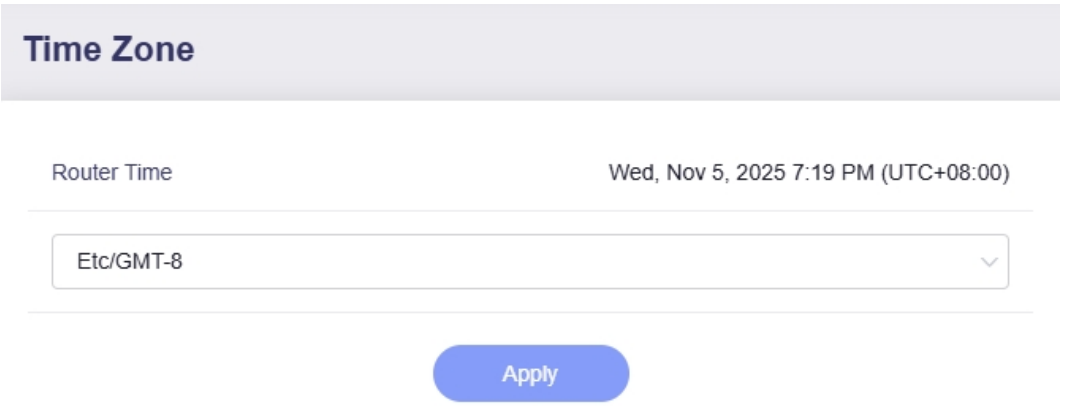


- **Abilita programmazione**: attiva questo interruttore per abilitare il riavvio pianificato.
- **Durata di riavvio**: imposta l'ora specifica (ad esempio 03:00) in cui il router si riavvierà.
- **giorno(i): seleziona i giorni** effettivi della settimana per queste impostazioni.

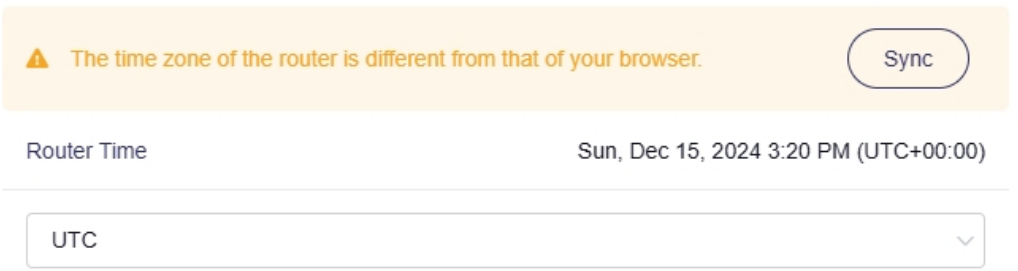
Dopo la configurazione, fai clic su **Applica** per salvare le impostazioni.

15.5 Fuso orario

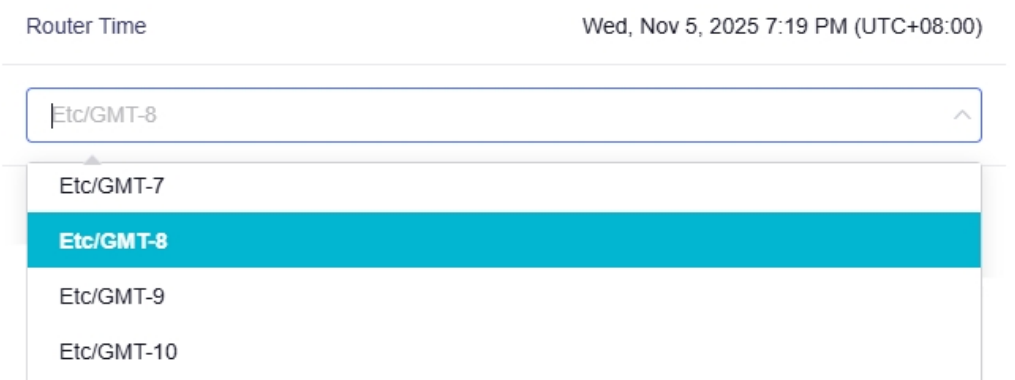
Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Fuso orario**. Questa pagina mostra l'ora di sistema del router, indicando la data, l'ora e la differenza di fuso orario corrispondente.



Alcune funzioni si basano sull'ora di sistema del router per avere effetto. Pertanto, 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.



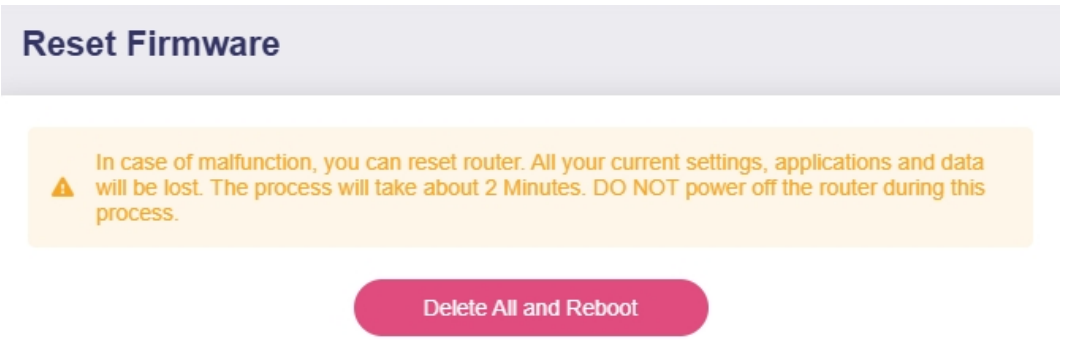
Per cambiare fuso orario, seleziona il fuso orario appropriato dall'elenco per assicurarti che l'ora di sistema del router corrisponda all'ora locale.



15.6 Ripristino del firmware

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Ripristino del firmware**. Se il router non funziona correttamente, puoi provare a risolvere il problema ripristinando il firmware.

Fai clic sul pulsante **Elimina tutto e riavvia** per ripristinare il firmware secondo necessità.

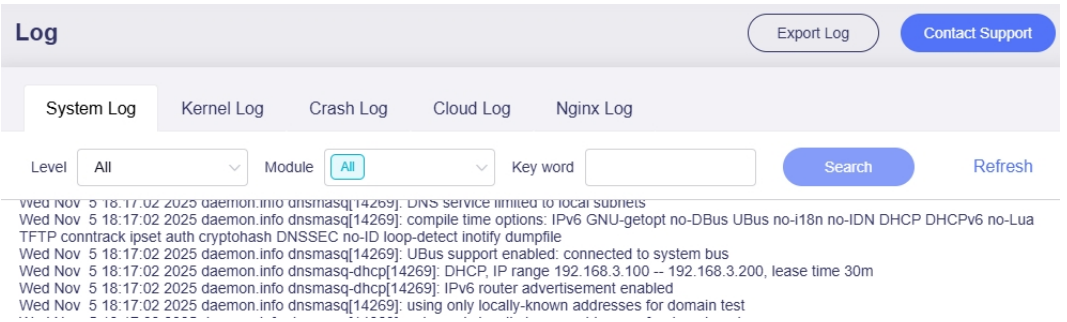


Nota: tutte le impostazioni, le applicazioni e i dati correnti verranno cancellati. Il processo richiederà circa 2 minuti. Non spegnere il router durante questo processo.

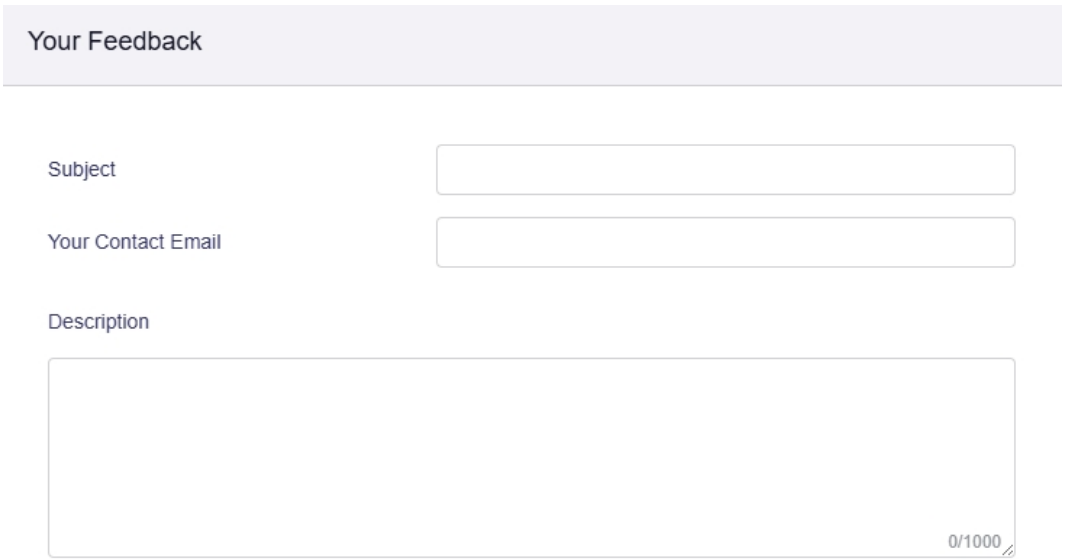
Se non riesci ad accedere al pannello di amministrazione web del router, prova a ripristinare il router utilizzando il pulsante di ripristino fisico sul lato.

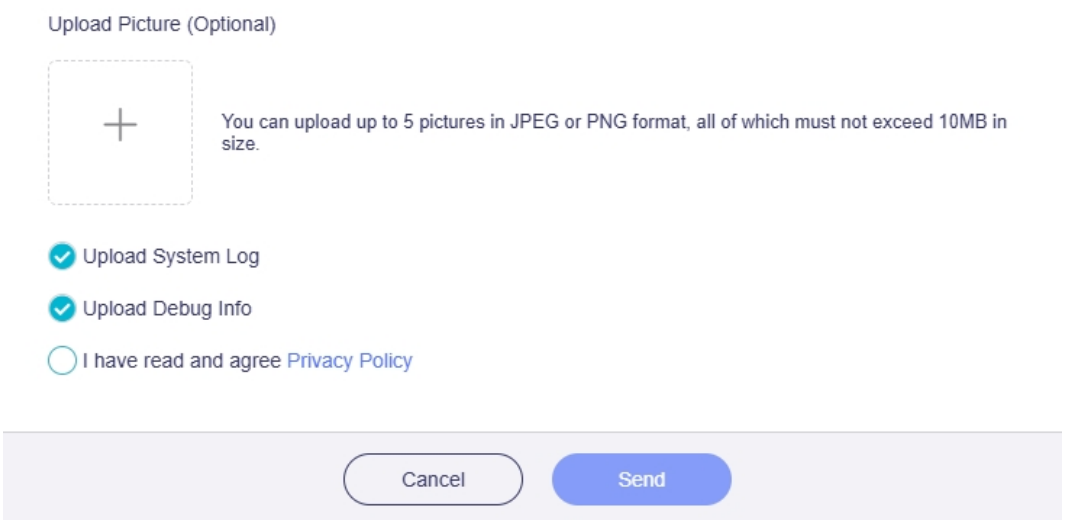
15.7 Registro

Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Registro**. Questa pagina consente di visualizzare i log di sistema, kernel, crash, cloud e Nginx per l'analisi e la risoluzione dei problemi. Inoltre, alcuni modelli cellulari che supportano eSIM forniscono anche il registro eSIM.



- **Ricerca**: la pagina del registro di sistema fornisce filtri per la ricerca rapida. Puoi selezionare il livello di log (ad esempio, tutto, informazioni, errore) o il modulo (ad esempio, IPv6, Tethering, Cellulare) dall'elenco a discesa oppure inserire parole chiave per interrogare rapidamente i log.
- **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.
- **Contatta l'assistenza**: fai clic su questo pulsante, inserisci le informazioni dettagliate nella finestra pop-up a destra, quindi fai clic su **Invia**. Il tuo feedback verrà inviato direttamente al supporto tecnico GL.iNet.

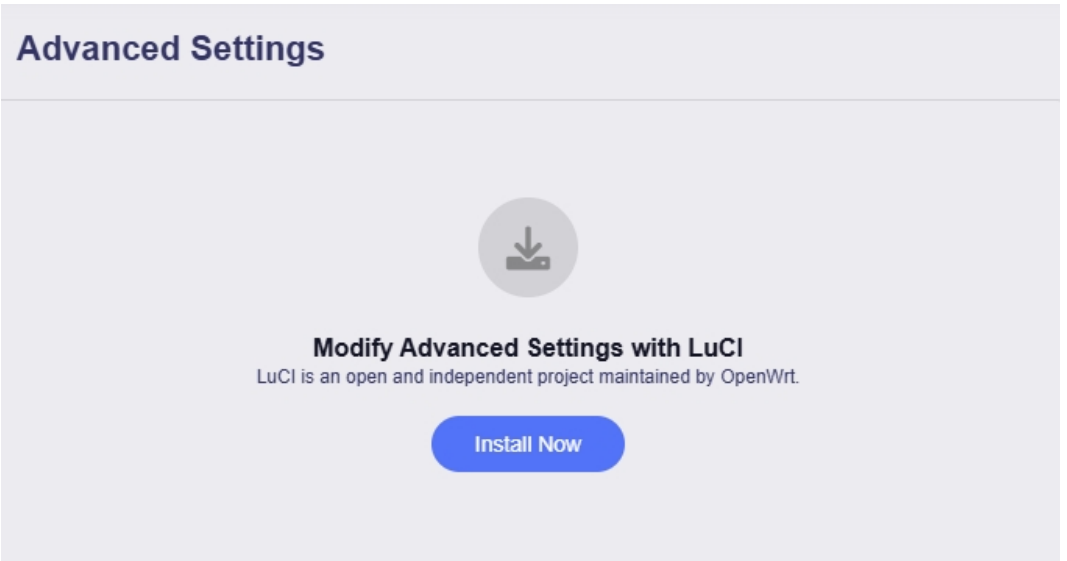



Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

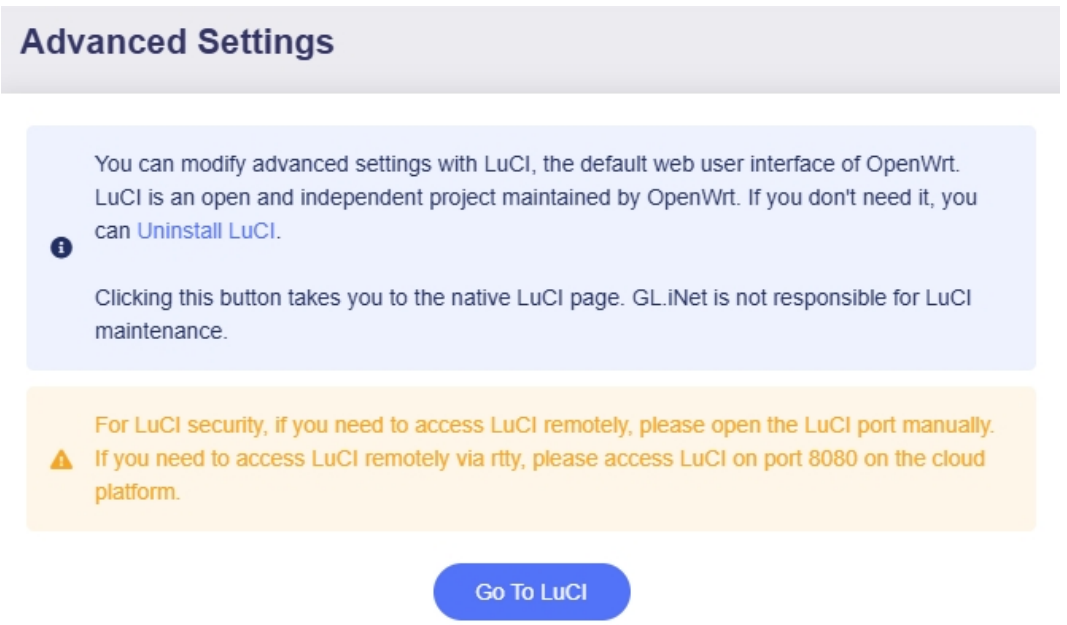
15.8 Impostazioni avanzate

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.

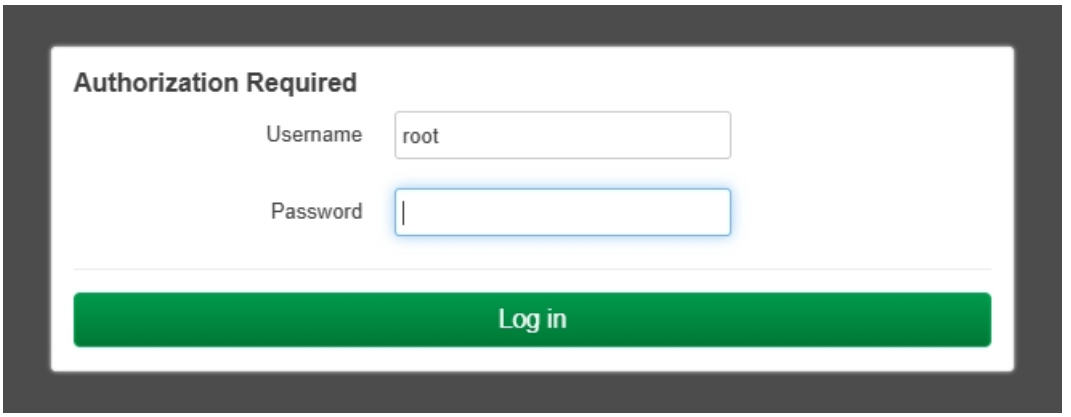
Fai clic sul pulsante **Installa ora** e verrà installata l'interfaccia LuCI.



Fai clic sul pulsante **Vai a LuCI** e verrai reindirizzato alla pagina di accesso LuCI.



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



Quindi accederai alla pagina LuCI.

