GL·iNet



Manuale utente

GL-AX1800 / Flint

Router domestico Wi-Fi 6

Versione firmware 4.8.3

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 11

Capitolo 2 Collegamenti hardware 12

2.1 Scelta della posizione 13

2.2 Collegamento del router 13

Capitolo 3 Accesso al router 14

Capitolo 4 Configurazione della connessione Internet 16

4.1 Configurazione guidata rapida 17

4.2 Configurazione manuale della connessione Internet 18

4.2.1 Connessione a Internet tramite cavo Ethernet 19

4.2.2 Connessione a Internet tramite una rete Wi-Fi esistente 23

4.2.3 Connessione a Internet tramite tethering USB 30

4.2.4 Connessione a Internet tramite modem USB 34

Capitolo 5 Wireless 36

5.1 Visualizzazione dello stato Wi-Fi 37

5.2 Impostazioni wireless 38

5.2.1 5 GHz Wi-Fi 38

5.2.2 2.4 GHz Wi-Fi 40

5.2.3 BSSID casuale 42

Capitolo 6 Client 44

6.1 Dettagli del dispositivo 46

6.2 Azione 48

6.3 Rimozione dei client 51

6.4 Ordinamento 52

Capitolo 7 Servizi cloud 53

7.1 GoodCloud 54

7.1.1 Attivazione di GoodCloud 55

7.1.2 Gestione del router 57
7.1.3 Dissociazione del dispositivo 61
7.1.4 Disabilita GoodCloud 61
7.2 AstroWarp 62
Capitolo 8 Conoscere le VPN 63
8.1 Introduzione 64
8.2 Scenari di utilizzo 65
Capitolo 9 Dashboard VPN 68
9.1 Configurazione guidata VPN 69
9.2 Modalità VPN 72
9.2.1 Modalità globale 73
9.2.2 Modalità delle policy 74
Capitolo 10 Configurazione del server VPN 85
10.1 Configurazione del server OpenVPN 86
10.1.1 Preparazione 86
10.1.2 Procedura di configurazione 87
10.1.3 Risoluzione dei problemi 89
10.2 Configurazione del server WireGuard 90
10.2.1 Preparazione 90
10.2.2 Procedura di configurazione 91
10.2.3 Risoluzione dei problemi 94
Capitolo 11 Configurazione del client VPN 95
11.1 Configurazione del client OpenVPN 96
11.1.1 Preparazione 96
11.1.2 Configurazione di NordVPN 96
11.1.3 Configurazione manuale del client OpenVPN (altri provider) 102
11.2 Configurazione del client WireGuard 105
11.2.1 Preparazione 105
11.2.2 Configurazione di AzireVPN 106
11.2.3 Configurazione di Hide.me 110
11.2.4 Configurazione di IPVanish 113
11.2.5 Configurazione di Mullvad 117
11.2.6 Configurazione di NordVPN 121
11.2.7 Configurazione di PIA (Private Internet Access) 126

11.2.8 Configurazione di Surfshark 130
11.2.9 Configurazione manuale del client WireGuard (altri provider) 134
Capitolo 12 Rete 140
12.1 Multi-WAN 141
12.1.1 Monitoraggio dello stato dell’interfaccia 141
12.1.2 Modalità Multi-WAN 144
12.2 LAN 147
12.2.1 Impostazioni di base 147
12.2.2 Server DHCP 149
12.2.3 Prenotazione indirizzi 151
12.3 Rete ospiti 152
12.3.1 Impostazioni di base 152
12.3.2 Server DHCP 153
12.4 DNS 155
12.4.1 Impostazioni del server DNS 156
12.4.2 Modifica del file hosts 158
12.5 Porta Ethernet 160
12.6 IPv6 161
12.6.1 Modalità IPv6 162
12.6.2 Metodo di acquisizione DNS 162
12.7 IGMP Snooping 163
12.8 Modalità di rete 164
12.9 Gateway drop-in 167
Capitolo 13 Controllo del traffico 169
13.1 Controllo parentale 170
13.1.1 Configurazione rapida 170
13.1.2 Risoluzione dei problemi 178
Capitolo 14 Sicurezza 179
14.1 Port forwarding 180
14.1.1 DMZ 180
14.1.2 Port forwarding 181
14.2 Controllo di gestione 183
14.2.1 Controllo degli accessi 183
14.2.2 Controllo dell'accesso remoto 186

14.2.3 Apertura delle porte sul router 187
14.3 Modalità NAT 189
Capitolo 15 Applicazioni 190
15.1 Plug-in 191
15.2 DNS dinamico 192
15.2.1 Abilita DDNS 192
15.2.2 Verifica del funzionamento del DDNS 195
15.2.3 Accesso remoto HTTPS 197
15.2.4 Accesso remoto SSH 199
15.3 Archiviazione di rete 201
15.3.1 Collegamento del dispositivo di archiviazione 201
15.3.2 Configurazione di Samba 202
15.3.3 Configurazione di WebDAV 205
15.3.4 Configurazione di DLNA 208
15.4 AdGuard Home 209
15.5 Tailscale 211
15.5.1 Configurazione di Tailscale 212
15.5.2 Consenti accesso remoto WAN 215
15.5.3 Consenti accesso remoto LAN 216
13.5.4 Nodi di uscita personalizzati 217
15.6 ZeroTier 219
15.6.1 Configurazione di ZeroTier 220
15.6.2 Consenti accesso remoto WAN 224
15.6.3 Consenti accesso remoto LAN 225
15.7 Tor 226
Capitolo 16 Sistema 227
16.1 Panoramica 228
16.2 Password amministratore 229
16.3 Aggiornamento 230
16.3.1 Aggiornamento online 230
16.3.2 Aggiornamento locale 231
16.4 Attività pianificate 233
16.4.1 Programmazione del LED 233
16.4.2 Riavvio pianificato 234

16.4.3 Programmazione del Wi-Fi a 5 GHz 235
16.4.4 Programmazione del Wi-Fi a 2,4 GHz 237
16.5 Fuso orario 240
16.6 Ripristino del firmware 241
16.7 Registro 242
16.8 Impostazioni avanzate 244

Capitolo 1

Conoscere il router

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

1.1 Panoramica del prodotto

Flint (GL-AX1800) è un router dual-band Wi-Fi 6 con velocità di connessione fino a 600Mbps (2.4GHz) + 1200Mbps (5GHz). La sua velocità di crittografia VPN arriva fino a 667Mbps e può essere utilizzata per ospitare server VPN. Flint è perfetto per la trasmissione di dati pesanti, la connettività di dispositivi di massa o i giochi a latenza ultra-bassa.

1.1.1 Aspetto

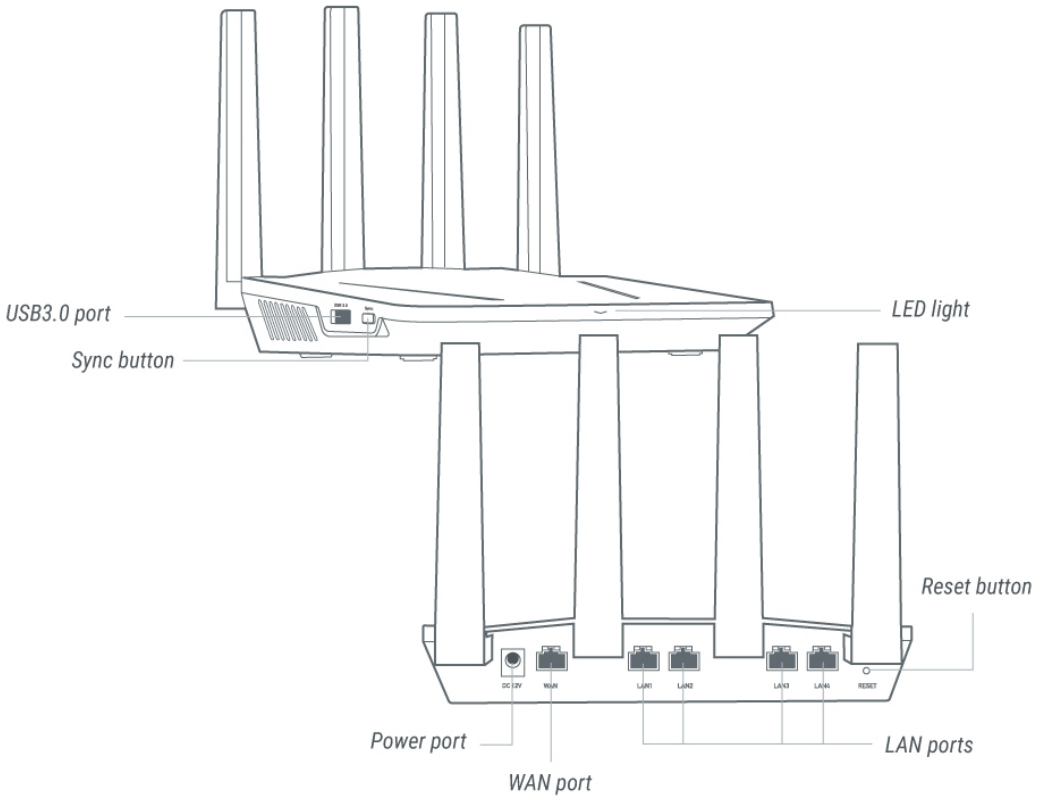








1.1.2 Interfacce e pulsanti



Voce	Descrizione
Porta di alimentazione	Consente di collegare l'alimentatore.
Porta WAN	Consente di collegare un modem o una presa Ethernet per accedere a Internet.
Porta LAN	Consente di collegare dispositivi cablati, se necessario.
Porta USB 3.0	Per dispositivi di archiviazione USB, tethering USB del telefono e modem cellulari USB compatibili.
Pulsante di ripristino	Tieni premuto per **4 secondi** per riparare la tua rete.
	Tenere premuto per **10 secondi,** quindi rilasciare per ripristinare router alle impostazioni di fabbrica.

1.1.3 LED

Stato	Indicazione
Blu fisso	Avvio
Blu pulsante lento	Avviato, senza connessione Internet
Bianco fisso	Connesso a Internet
Blu lampeggiante rapido	Ripristino

1.2 Specifiche tecniche

Interfaccia	1 x porta Ethernet WAN 4 x porte Ethernet LAN 1 x USB 3.0 (Tipo A) 1 x LED 1 x Pulsante di sincronizzazione 1 x Pulsante di ripristino 1 x 12V/1.5A Ingresso CC
CPU	Processore Arm quad-core IPQ6000 @1.2GHz
Memoria/Archiviazione	DDR3L 512MB / NAND Flash 128MB
Protocollo	IEEE 802.11a/b/g/n/ac/ax
Velocità Wi-Fi	600Mbps (2.4GHz), 1200Mbps(5GHz)
Antenne	4 x antenne esterne
Velocità Ethernet	10/100/1000Mbps
Ingresso alimentazione	DC5521, 12V/1.5A (5.5*2.1mm)
Consumo energetico	< 18W
Temperatura di esercizio	0 ~ 40°C (32 ~ 104°F)
Temperatura di conservazione	-20 ~ 70°C (-4 ~ 149°F)

Dimensioni/Peso	210 x 120 x 36.8mm / 445 g
Altri strumenti	Scheda tecnica / Firmware / App / Unboxing

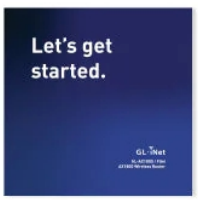
*Le velocità wireless si basano sugli standard IEEE 802.11 (ad esempio, 802.11ax per Wi-Fi 6). La velocità effettiva e la portata potrebbero essere inferiori a causa di ostacoli ambientali (muri, metallo), congestione della rete o funzionalità del dispositivo client.
*L'uso di Wi-Fi 6 (802.11ax) e le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

1.3 Contenuto della confezione

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

La confezione include:

- 1 x Selce (GL-AX1800)
- 1 x Manuale utente
- 1 x cavo Ethernet
- 1 x Biglietto di ringraziamento
- 1 x Scheda di garanzia
- 1 x Adattatore di alimentazione
- 1 x Convertitore (in base al Paese di spedizione)



1 x User manual



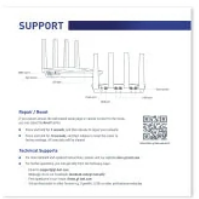
1 x Flint (GL-AX1800)



1 x Ethernet cable



1 x Thank you card



1 x Warranty card



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.
- **Evita le interferenze elettromagnetiche**: tieni il router lontano da dispositivi Bluetooth e forni a microonde per ridurre le interferenze sul segnale.

2.2 Collegamento del router

1. **Accendi**
   Monta insieme l'alimentatore in due pezzi. Collegalo al router e collegalo a una presa. Si avvierà automaticamente.
2. **Connetti un dispositivo al router**
   Collega un dispositivo (ad esempio, laptop o smartphone) al router tramite Wi-Fi o cavo Ethernet.
   - **Wi-Fi**: sul tuo dispositivo, vai su Impostazioni > WLAN, individua il nome della rete Wi-Fi del router nell'elenco delle reti disponibili e inserisci la password. Puoi trovare il nome della rete e la password predefiniti stampati sull'etichetta del router.
   - **Ethernet**: collega il tuo dispositivo alla porta LAN del router tramite un cavo Ethernet.
3. **Accedi al router**
   Internet non è disponibile quando ci si connette al router per la prima volta. Accedi al router come indicato nel capitolo 3 per completare la configurazione iniziale prima di accedere a Internet.

Capitolo 3

Accesso al router

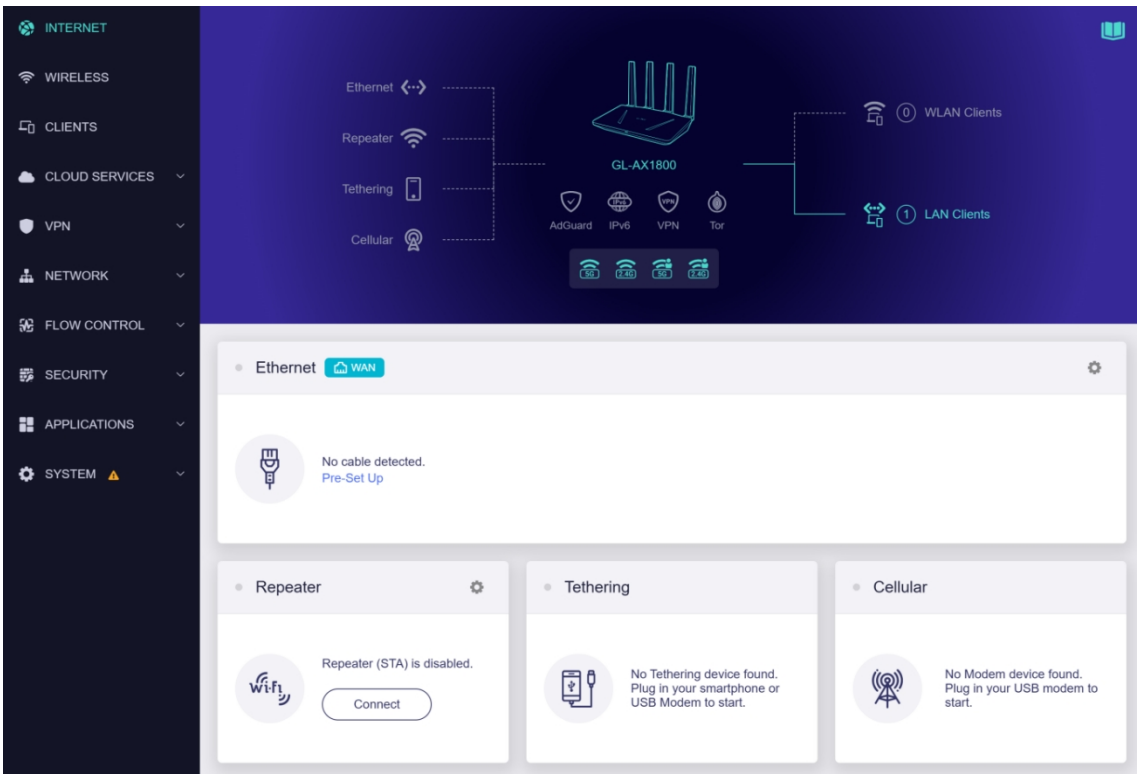
Questo capitolo ti guida ad accedere al router tramite pannello di amministrazione web.

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

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

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

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



Capitolo 4

Configurazione della connessione Internet

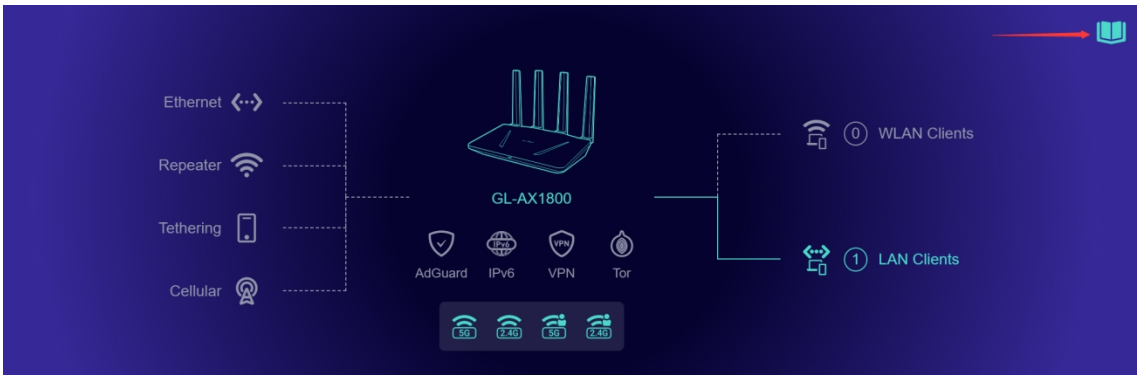
Questo capitolo introduce diversi metodi di connessione Internet per consentire al router di adattarsi a diversi ambienti di rete.

4.1 Configurazione guidata rapida

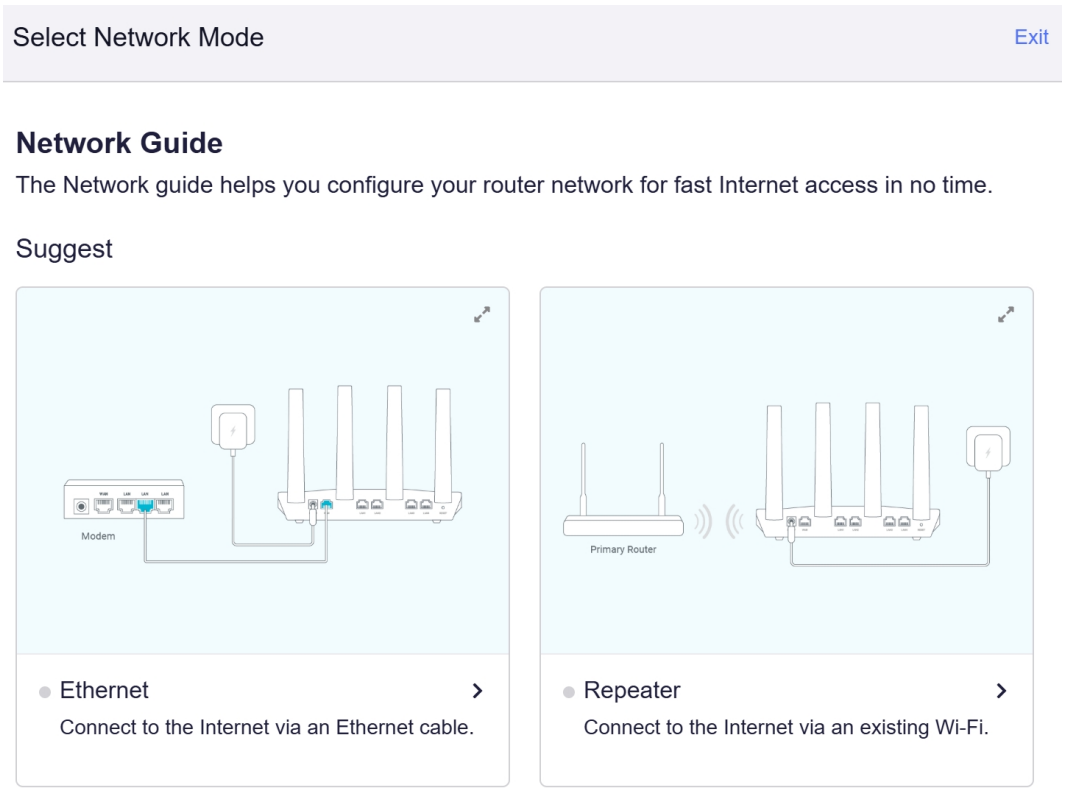
La configurazione guidata basata sul Web ti guiderà attraverso la configurazione della rete del router.

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.



Se utilizzi l'app GL.iNet, segui le istruzioni visualizzate sullo schermo per configurare l'accesso a 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 se necessario.

Flint supporta quattro metodi di connessione Internet: Ethernet, Ripetitore, Tethering USB e Modem USB. Scegli il metodo appropriato in base alle tue esigenze di utilizzo.

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

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

3. **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.

4. **Modem USB**: inserisci 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.

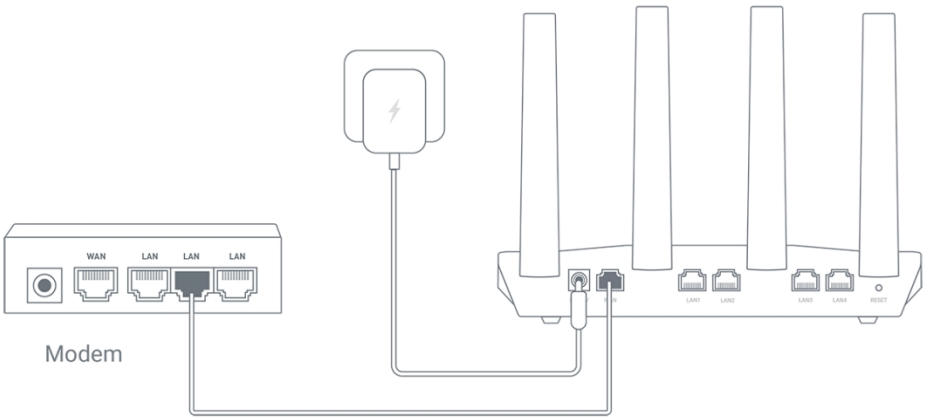
4.2.1 Connessione a Internet tramite cavo Ethernet

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.

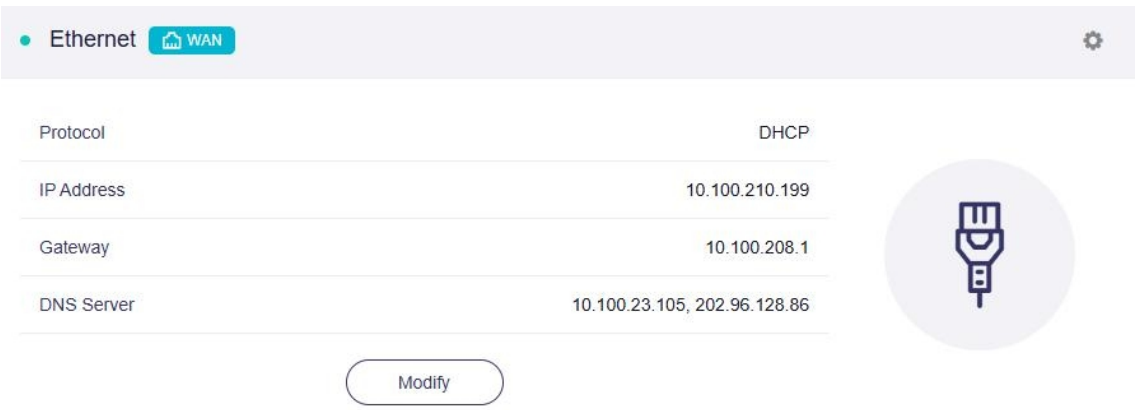
Configurazione di base

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.

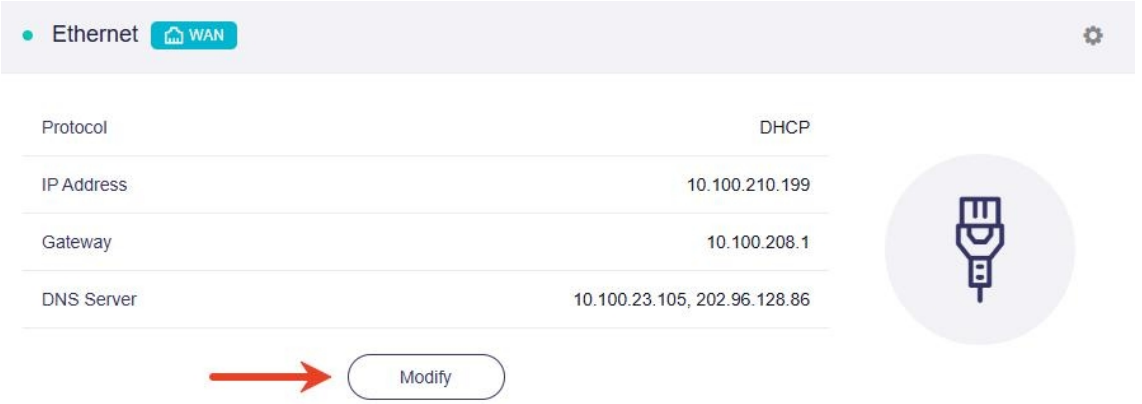


2. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Ethernet**. Se la connessione ha esito positivo, la sezione Ethernet visualizzerà i dettagli della rete, inclusi protocollo, indirizzo IP, gateway e Server DNS.



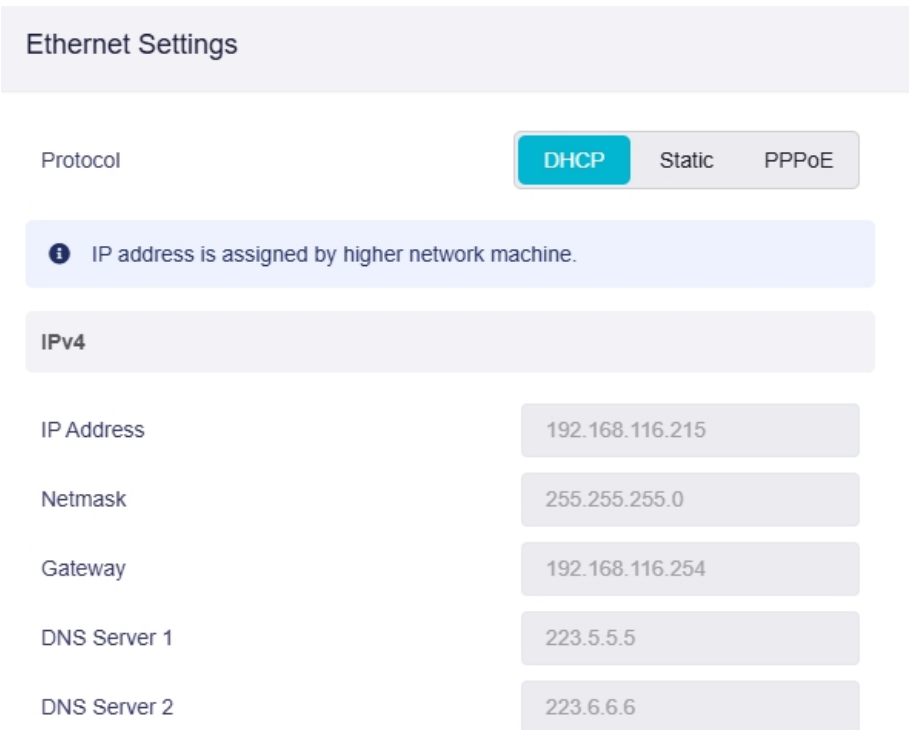
Protocollo

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



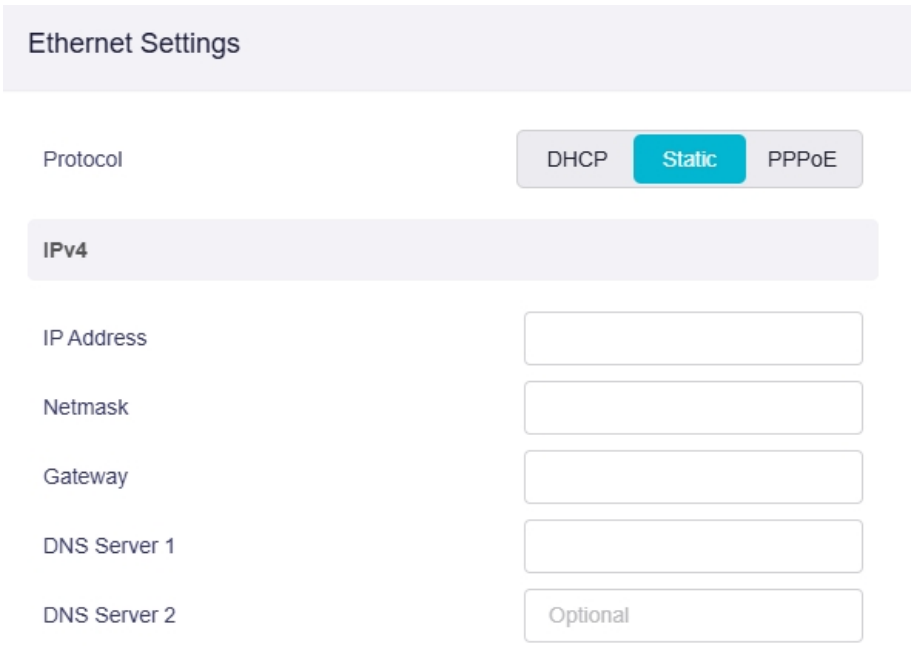
- **DHCP**

  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.



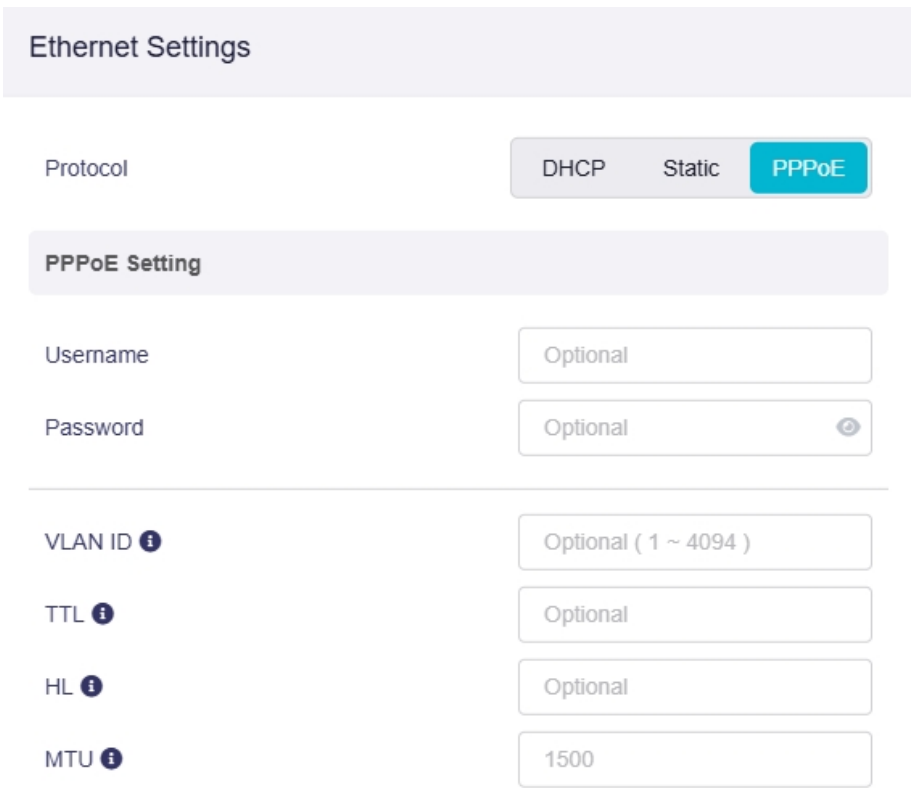
- **Statico**

  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).



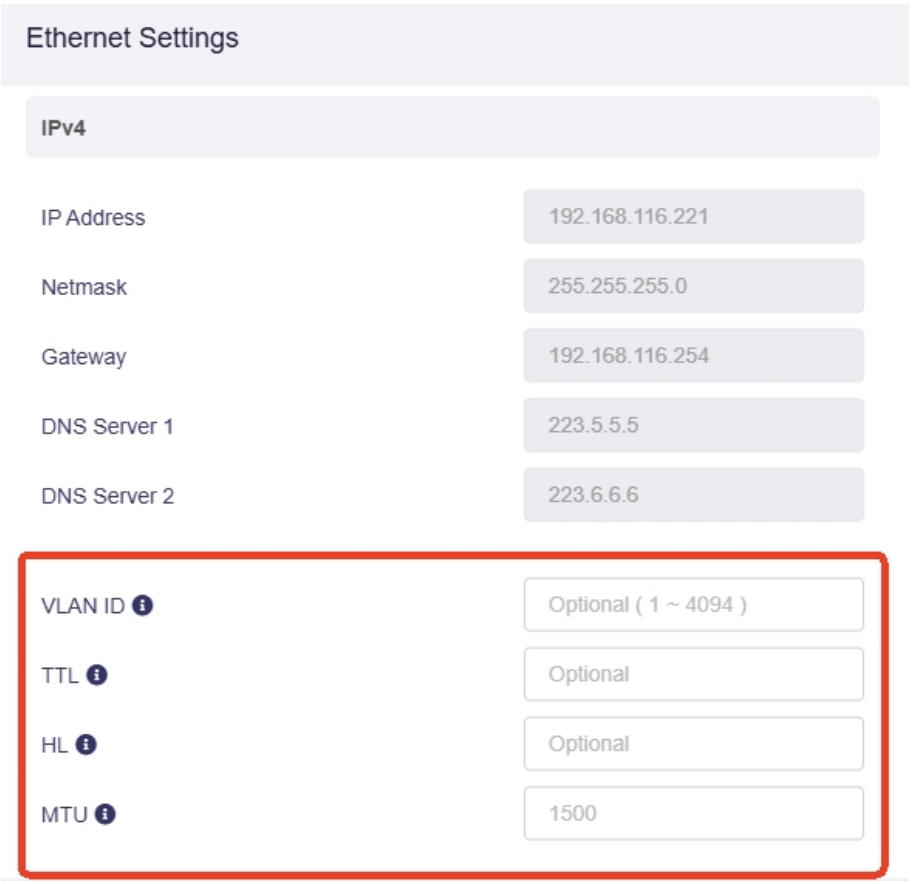
- **PPPoE**

  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**

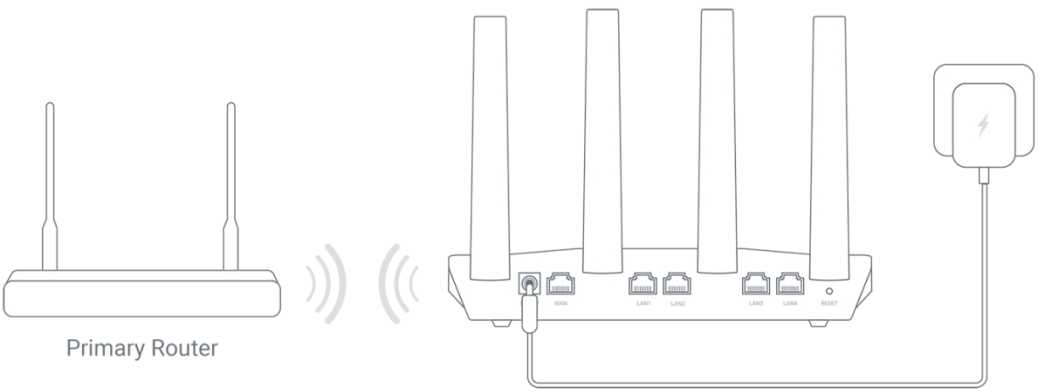
  In IPv6, il campo HL (Hop Limit) limita il numero di hop di trasmissione per i pacchetti di dati nella rete, fungendo da equivalente di TTL in IPv4.

- **MTU**

  Il valore MTU predefinito è 1500 byte.

4.2.2 Connessione a Internet tramite una rete Wi-Fi esistente

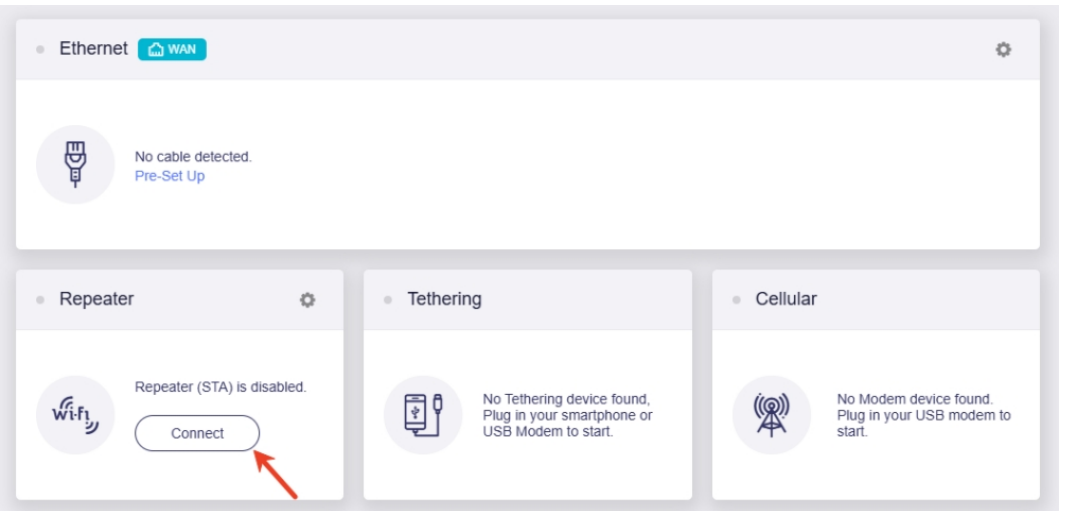
Collega il router come ripetitore alla rete wireless esistente per potenziare i segnali Wi-Fi e creare una rete locale isolata dalla rete primaria. Negli hotel o nei bar con hotspot pubblici gratuiti, l'utilizzo di un ripetitore non solo rafforza i segnali Wi-Fi, ma fornisce anche l'accesso cablato e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



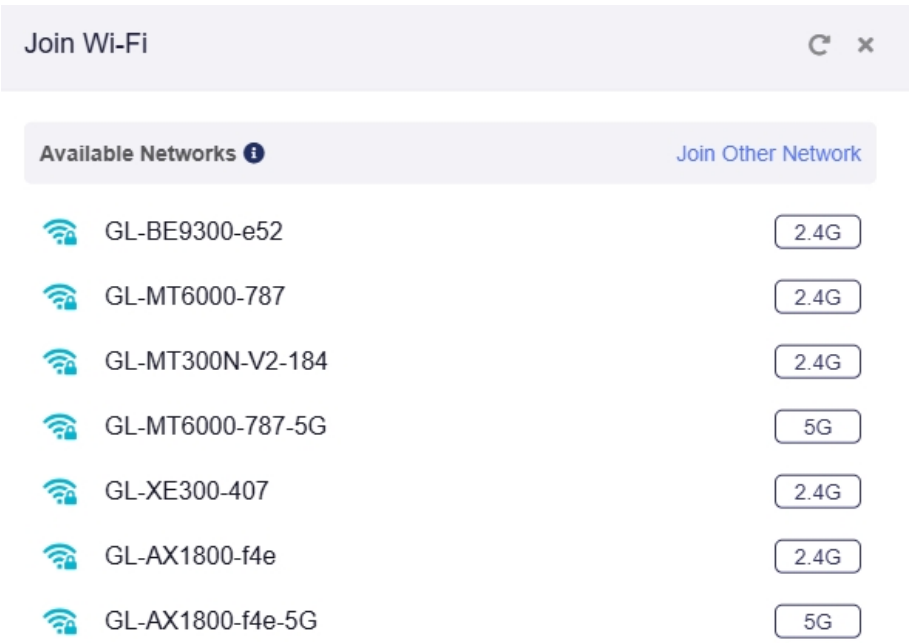
La funzione ripetitore GL.iNet funziona in modalità WISP (Wireless Internet Service Provider) per impostazione predefinita, il che significa che il router creerà la propria sottorete e fungerà da firewall per proteggerti dalla rete pubblica.

Configurazione di base

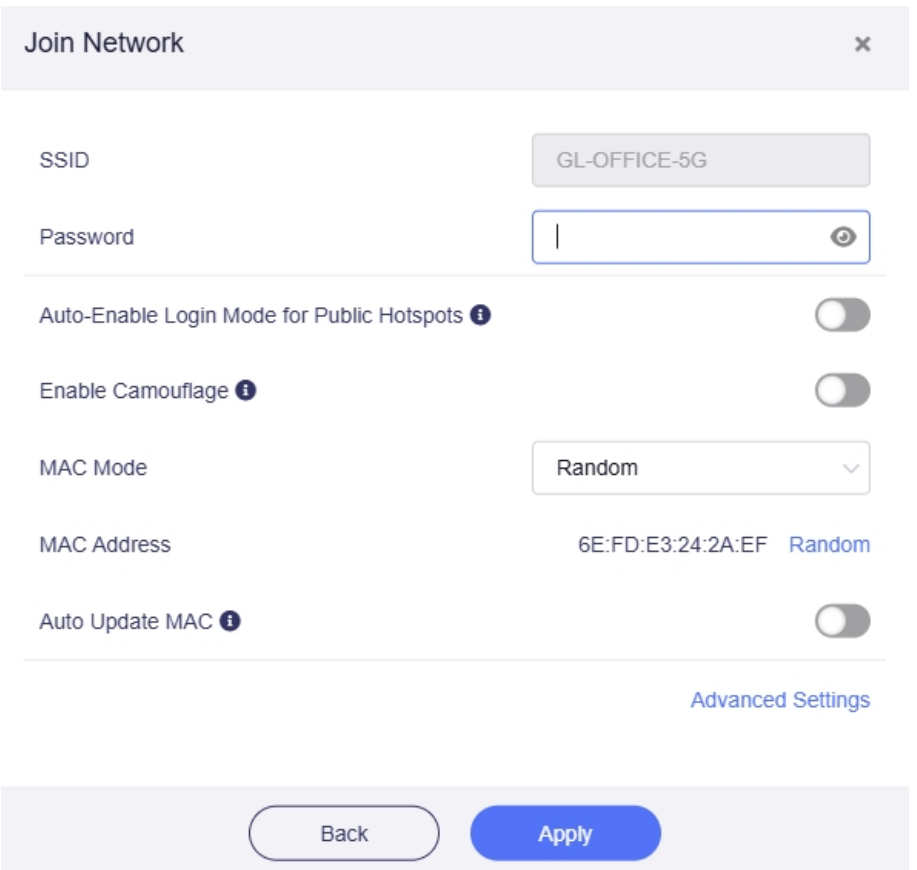
1. Accedi al pannello di amministrazione web del router e vai a **INTERNET** > **Ripetitore**. Fai clic su **Connetti**.



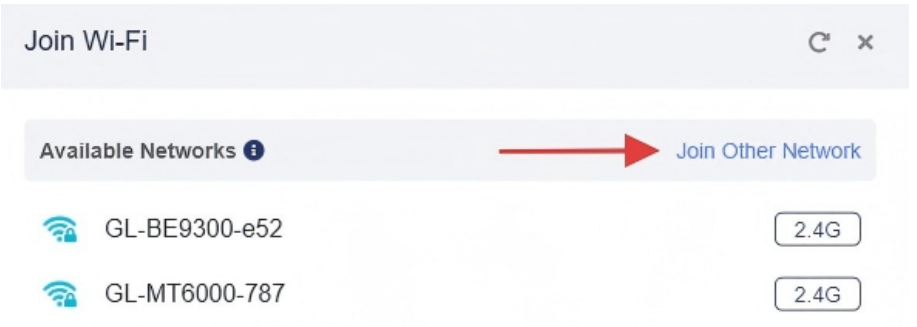
2. Nella finestra pop-up, scegli la rete Wi-Fi a cui desideri connetterti dall'elenco delle reti disponibili.



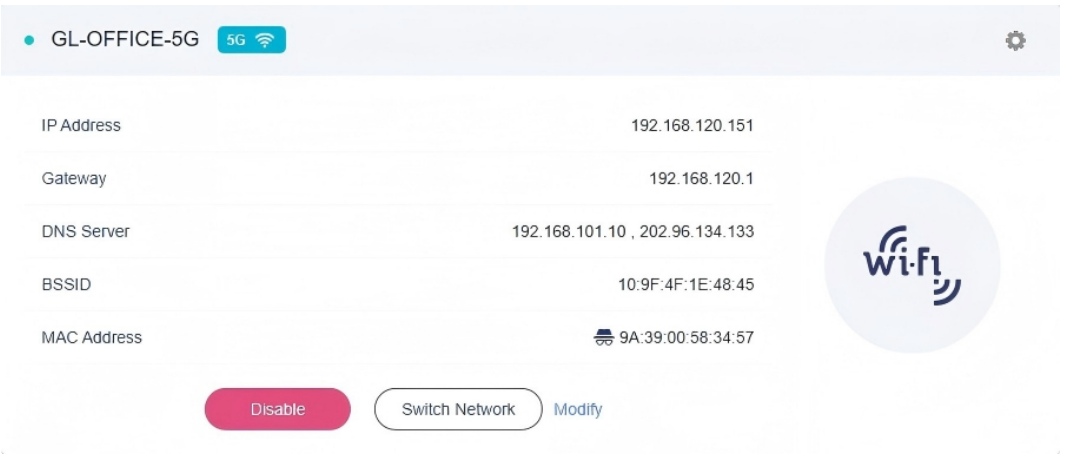
3. Inserisci la password Wi-Fi corretta e fai clic su **Applica**.



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

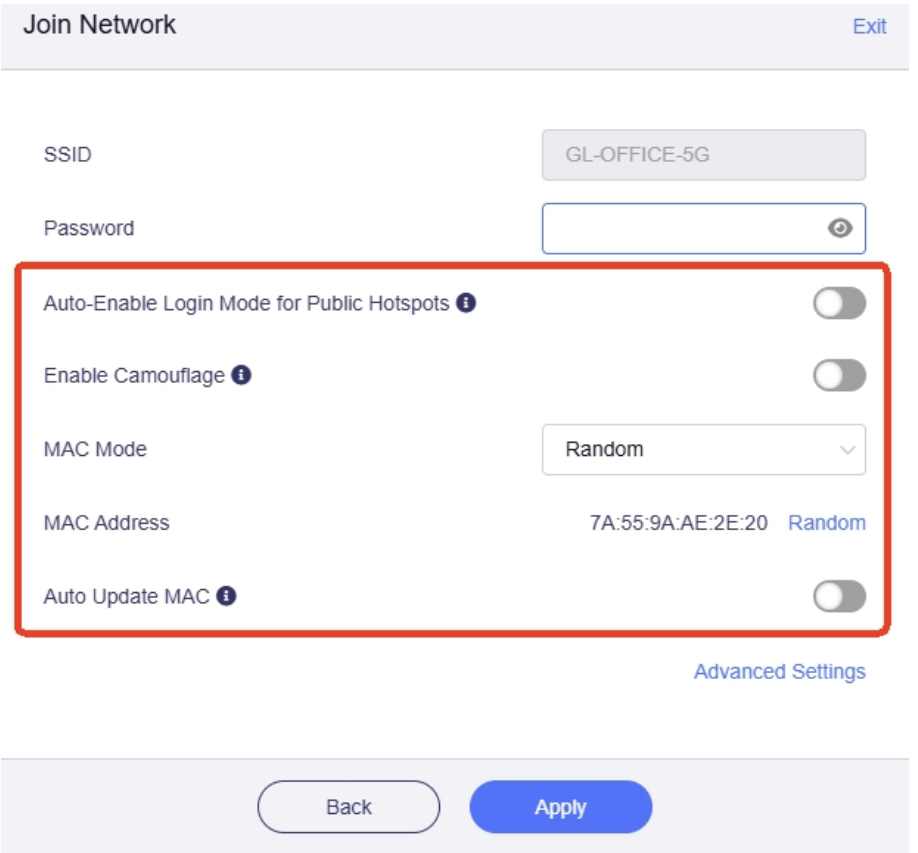


4. Attendere un minuto affinché il router si connetta. Una volta connesso, la pagina viene visualizzata come di seguito.

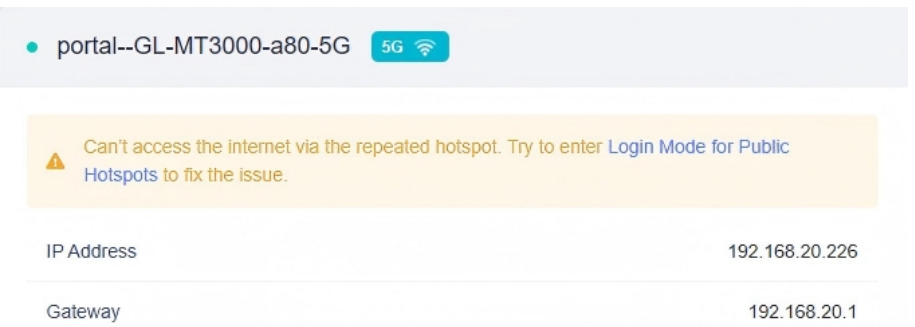


Impostazioni hotspot pubblico

Quando si connette il router a un hotspot pubblico con un captive portal, si consiglia di abilitare le seguenti funzionalità per migliorare la percentuale di successo della connessione.



- **Abilita automaticamente la modalità di accesso per gli hotspot pubblici**
  Se abilitato, il router entra automaticamente nella modalità di accesso all'hotspot pubblico quando è connesso a un hotspot ma non a Internet. In questa modalità, alcuni servizi verranno sospesi mentre la modalità DNS passa ad automatica, il che potrebbe far trapelare la tua attività di rete al provider di rete (ad esempio, hotel, centro commerciale). Anche se disabilitato, il router ti chiederà di accedere a questa modalità se rileva un captive portal hotspot o non riesce ad accedere.



- **Abilita mimetizzazione**

  Se abilitato, il router si maschererà come il dispositivo client che utilizzi per accedere al pannello di amministrazione emulando l'indirizzo MAC di quel dispositivo.
- **Modalità MAC**

  Scegli quale indirizzo MAC utilizza il router per connettersi all'hotspot pubblico.

Fabbrica	Utilizza l'indirizzo MAC originale assegnato in fabbrica al dispositivo.
Clona	Clona l'indirizzo MAC di un dispositivo client per la connessione. Se il MAC desiderato non è elencato, inserisci manualmente l'indirizzo MAC che desideri clonare. Nota: molti dispositivi utilizzano indirizzi MAC casuali (spesso chiamati indirizzi Wi-Fi privati o indirizzi hardware casuali) quando si connettono alle reti Wi-Fi. Di conseguenza, l'indirizzo MAC visualizzato qui potrebbe non corrispondere al MAC fisico effettivo del dispositivo.
Casuale	Genera automaticamente un indirizzo MAC casuale per la connessione.

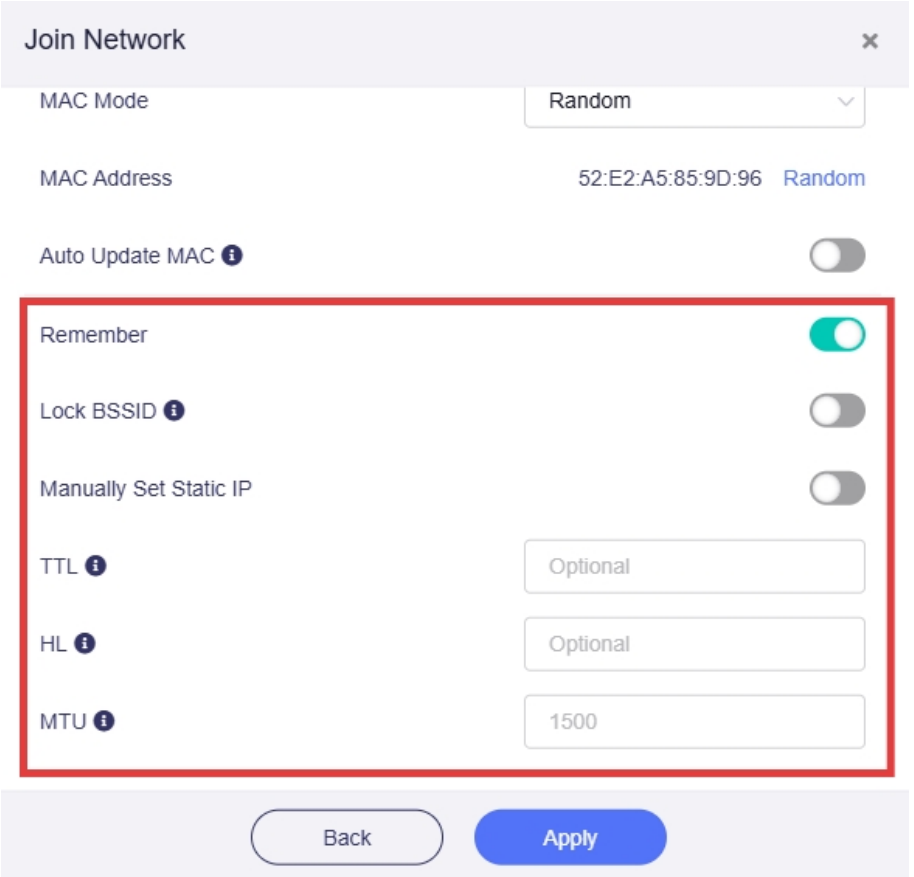
- **Aggiornamento automatico MAC**

  Se questa opzione è abilitata, l'indirizzo MAC verrà aggiornato automaticamente.

Quando si salva la configurazione di rete, la modalità MAC, incluso qualsiasi indirizzo MAC clonato o randomizzato, sarà legata allo specifico SSID salvato. Puoi modificare manualmente queste impostazioni per ciascun SSID in qualsiasi momento.

Impostazioni avanzate

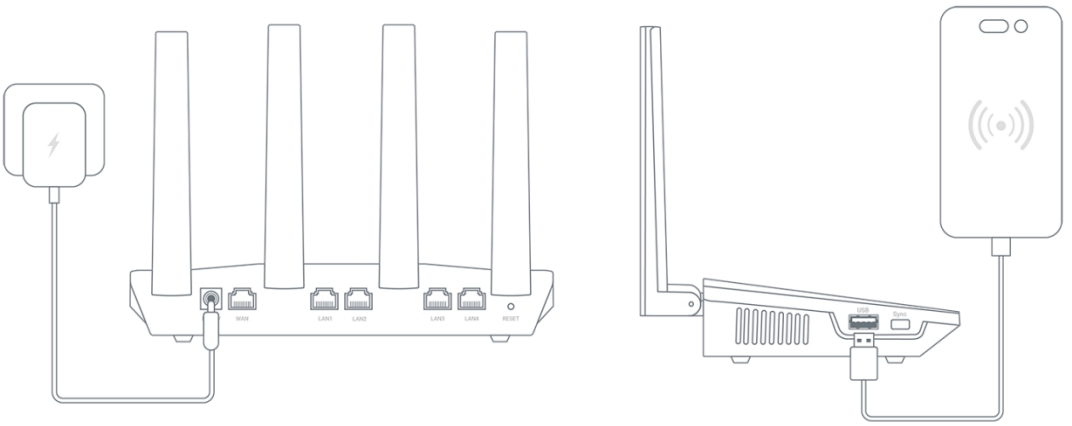
Quando ti unisci alla rete, ci sono alcune impostazioni avanzate facoltative.



- **Ricorda**: attiva questa opzione per ricordare l'attuale rete Wi-Fi ripetuta.
- **Blocca BSSID**: se abilitato, il router si connetterà solo al punto di accesso (AP) specifico corrispondente al BSSID selezionato, anche quando altri AP condividono lo stesso SSID.
- **Imposta manualmente IP statico**: se abilitato, puoi configurare manualmente un indirizzo IPv4 fisso, maschera di rete, gateway e server DNS per la connessione del ripetitore del router, invece di ottenere queste impostazioni automaticamente.
- **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 sovrascrivere/falsificare il TTL, immettere il TTL effettivo desiderato più 1 per compensare il decremento automatico. TTL è valido solo per IPv4.
- **HL**: In IPv6, il campo HL (Hop Limit) viene utilizzato per limitare il numero di salti di trasmissione dei pacchetti di dati nella rete, che è equivalente al TTL in IPv4.
- **MTU**: il valore predefinito è 1500.

4.2.3 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.

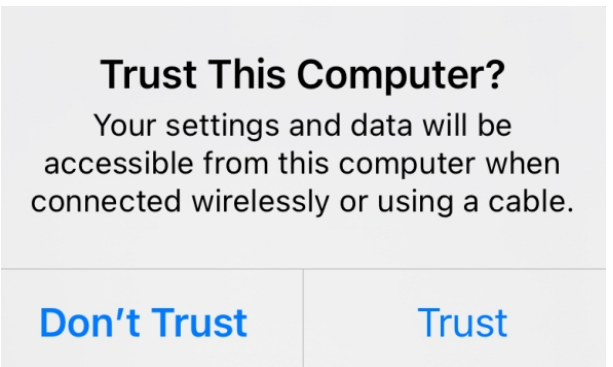


Il modem host-less funziona anche in Tethering durante la configurazione del modem.

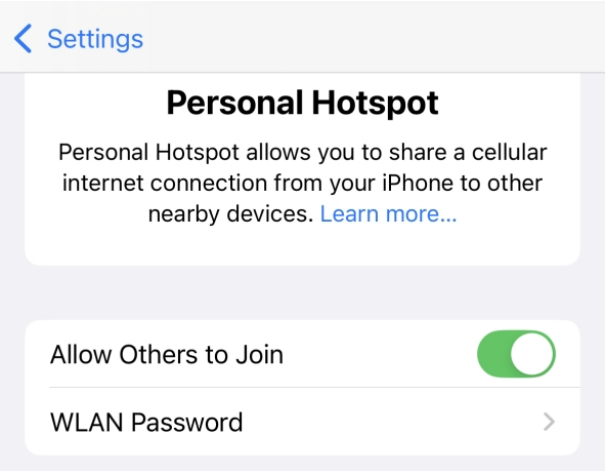
Nota: alcuni operatori di telefonia mobile limitano o addebitano costi aggiuntivi per il tethering. Ti consigliamo di verificare con il tuo operatore.

Tethering dell'iPhone

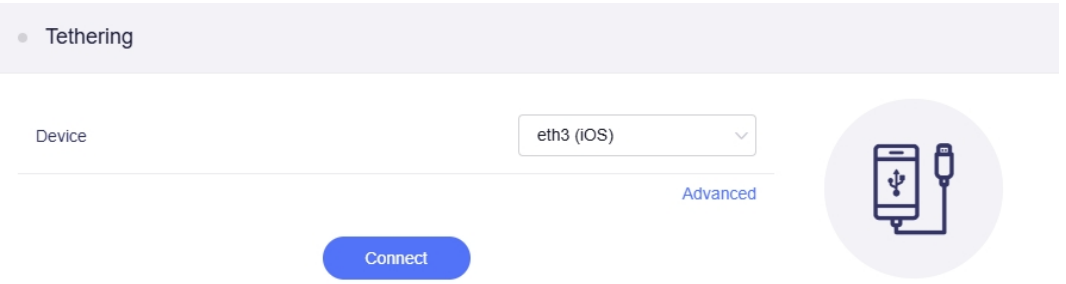
1. Collega un iPhone alla porta USB del router con un cavo USB. Quando viene chiesto se autorizzare il dispositivo, tocca **Autorizza** per continuare.



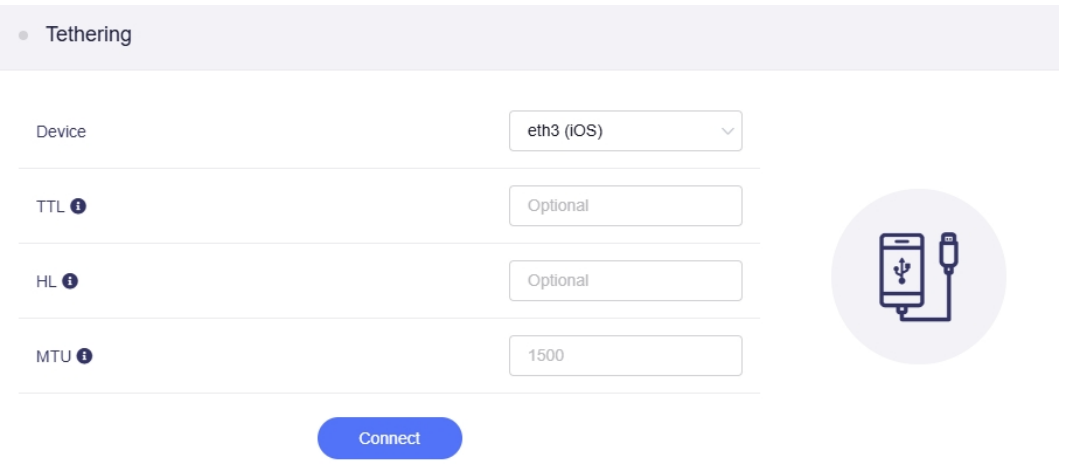
2. Su iPhone, vai in **Impostazioni** > **Hotspot personale** e attiva **Consenti agli altri di accedere**.



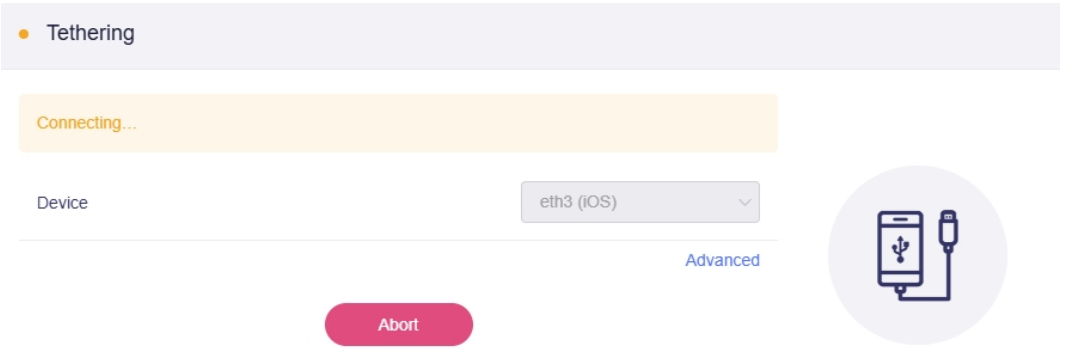
3. Collega un computer o un altro telefono al router. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Tethering**, quindi fai clic su **Connetti**.



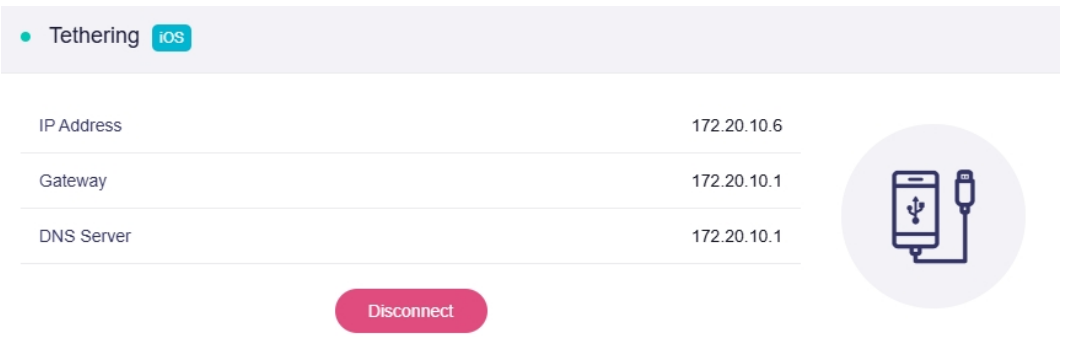
Se è necessario configurare impostazioni avanzate, come TTL, HL e MTU, fai clic su **Avanzate** per personalizzare queste impostazioni, quindi fai clic su **Connetti**.



4. Inizierà la connessione.

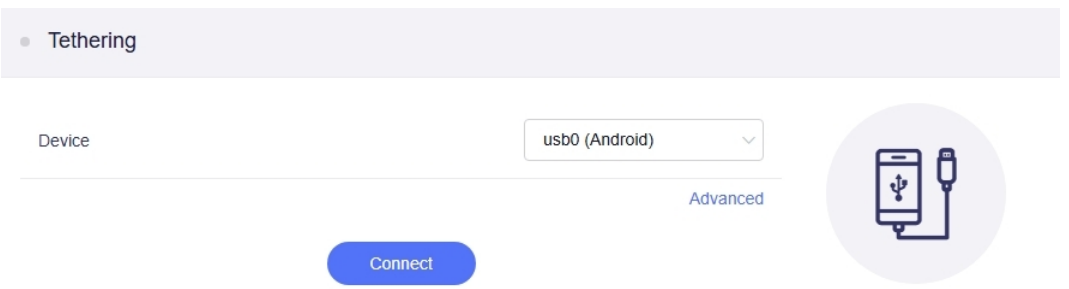


Una volta connesso, questa pagina visualizzerà i dettagli della connessione Tethering.

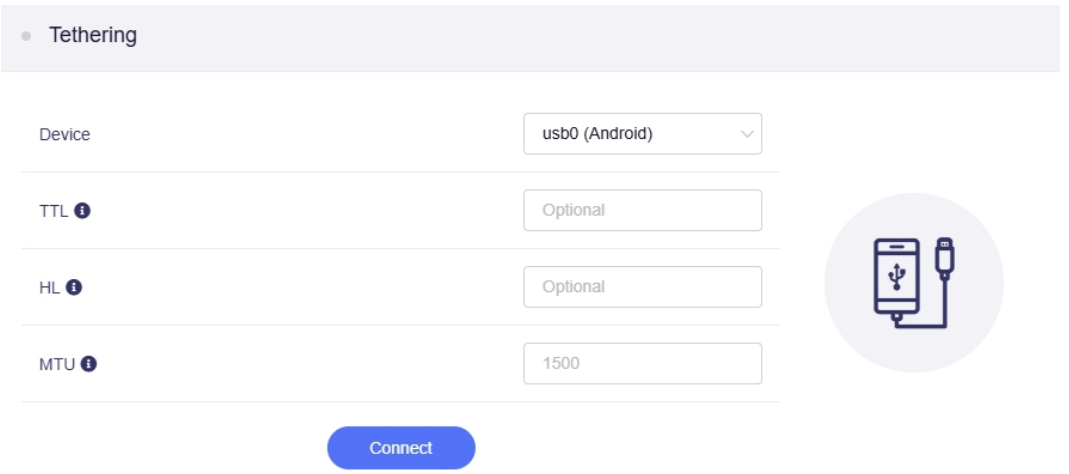


Tethering Android

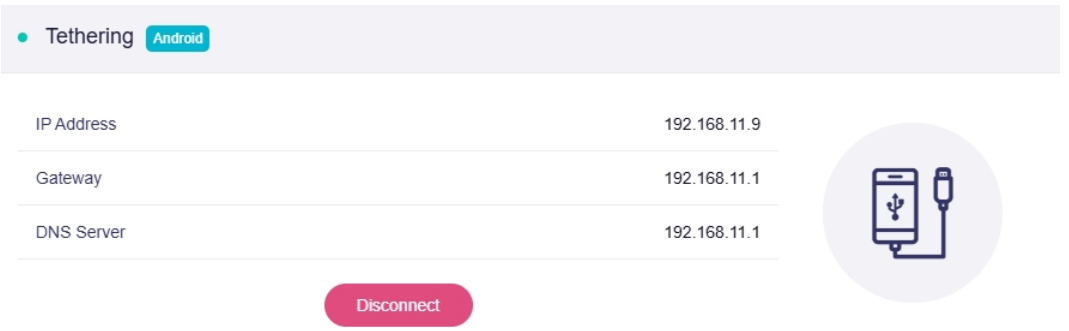
1. Collega un telefono Android alla porta USB del router utilizzando un cavo USB. Potrebbe apparire una finestra di dialogo di sistema che richiede le preferenze USB. Seleziona **Tethering USB** o **Trasmissione file**, se richiesto.
2. Vai alle **Impostazioni** del tuo telefono > **Rete e Internet** > **Hotspot personale**. Abilita **Hotspot personale** o **Tethering USB**.
   (I passaggi per abilitare il 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, fare clic su **Avanzate** per personalizzare queste impostazioni, quindi fare clic su **Connetti**.



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



Risoluzione dei problemi

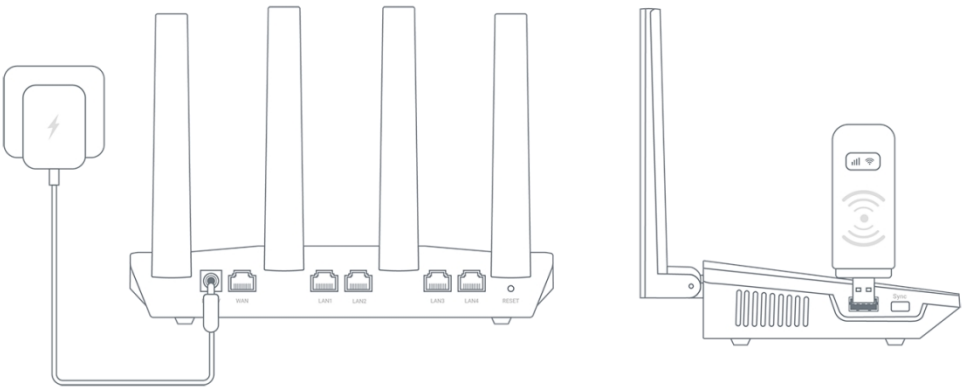
Se la connessione tethering non riesce, prova questi passaggi per la risoluzione dei problemi:

- 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.

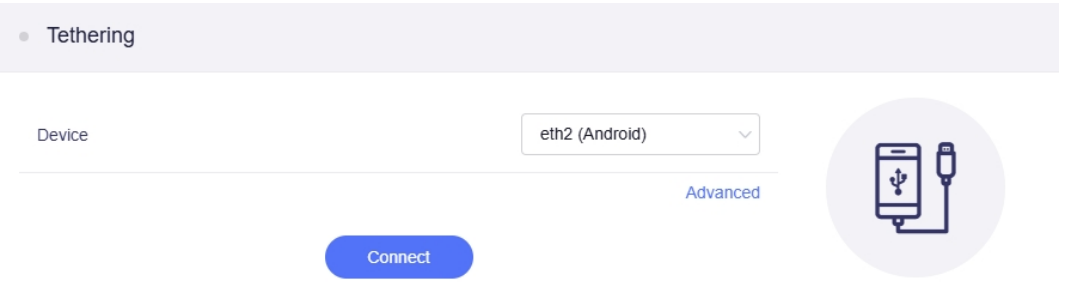
4.2.4 Connessione a Internet tramite modem USB

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.

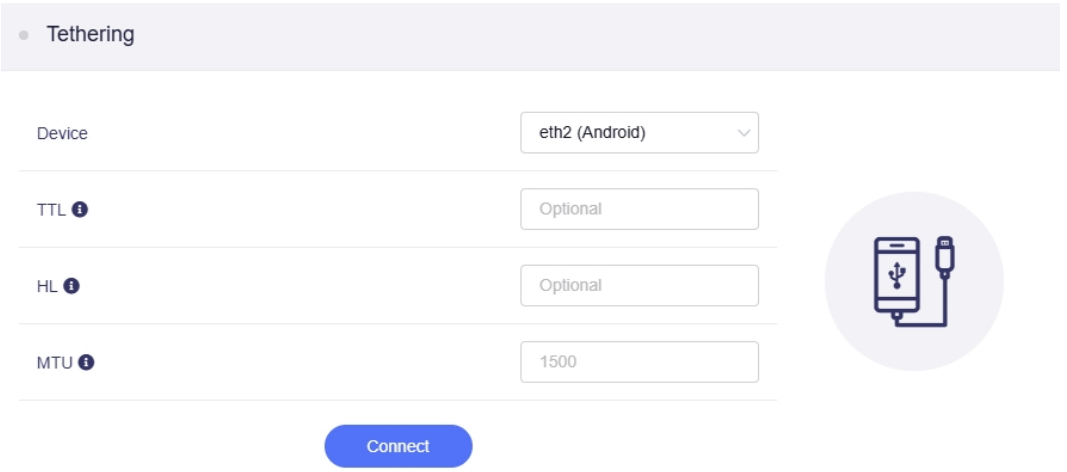


Segui i passaggi seguenti per connettere il router a Internet tramite un modem USB.

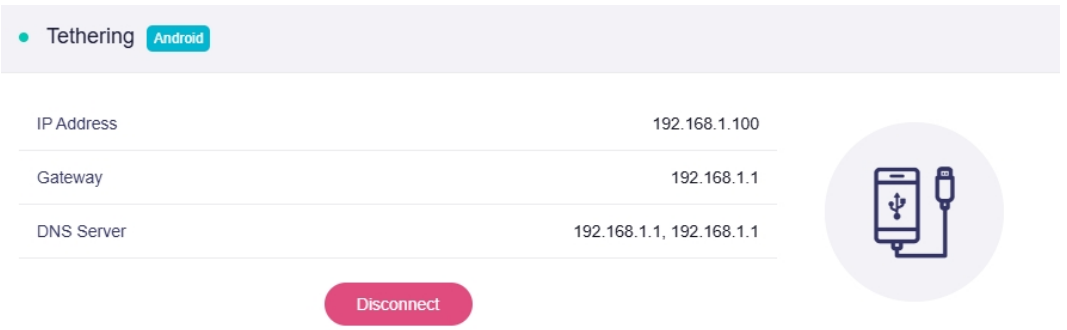
1. Collega un modem USB con una scheda SIM preinstallata alla porta USB del router prima di accenderlo.
2. Accedi al pannello di amministrazione web del router e vai su **INTERNET** > **Tethering**. Fai clic su **Connetti**.



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**.



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



Suggerimento: 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".

Capitolo 5

Wireless

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

5.1 Visualizzazione dello stato Wi-Fi

Le reti Wi-Fi del router sono abilitate per impostazione predefinita e l'icona Wi-Fi corrispondente si illuminerà sotto l'immagine del modello del dispositivo nella pagina INTERNET.



Se il cursore passa sopra l'icona Wi-Fi abilitata, verrà visualizzato un codice QR Wi-Fi come segue. Puoi scansionare il codice QR Wi-Fi per connetterti rapidamente al Wi-Fi corrispondente.

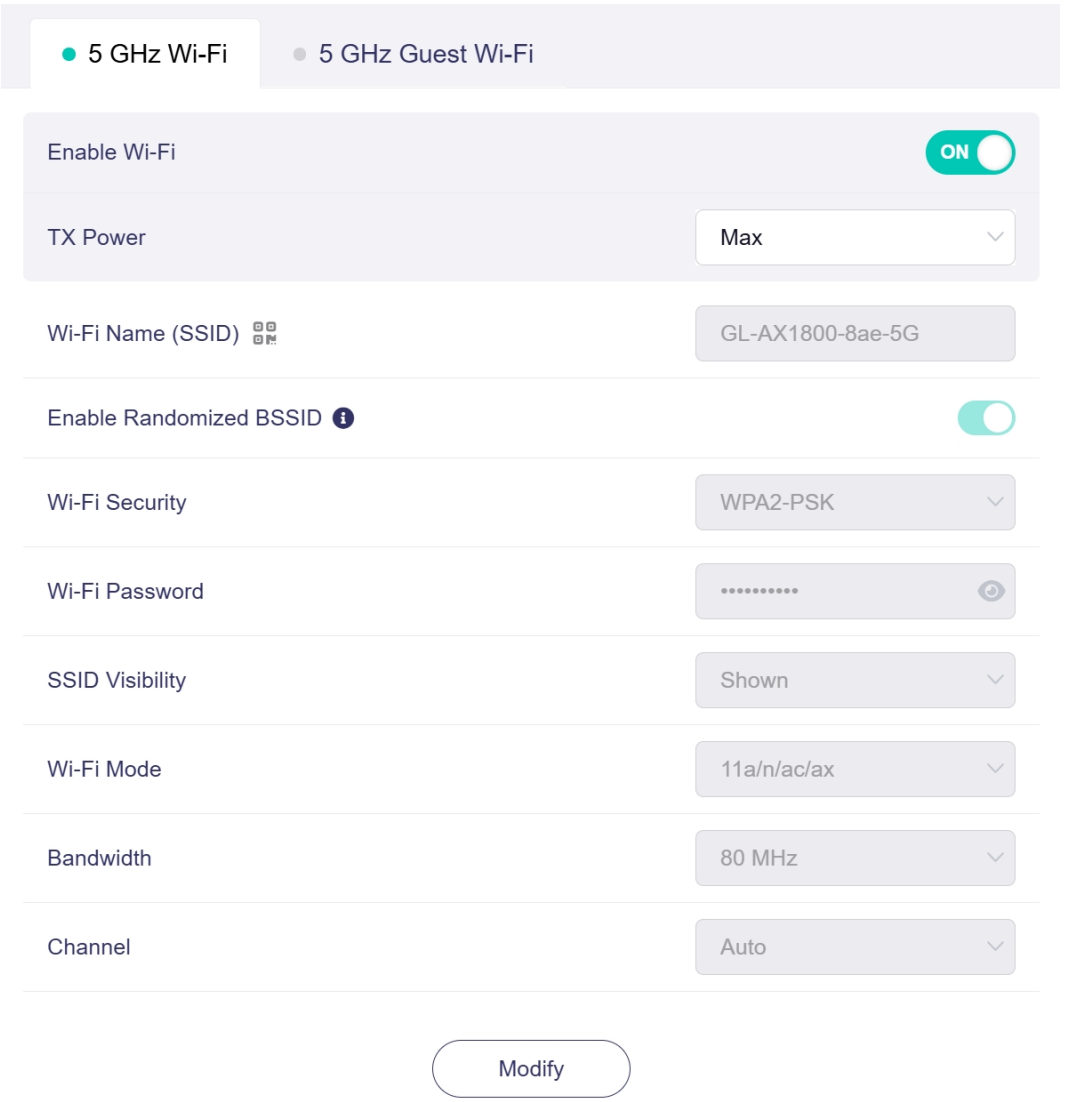


5.2 Impostazioni wireless

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

5.2.1 5 GHz Wi-Fi

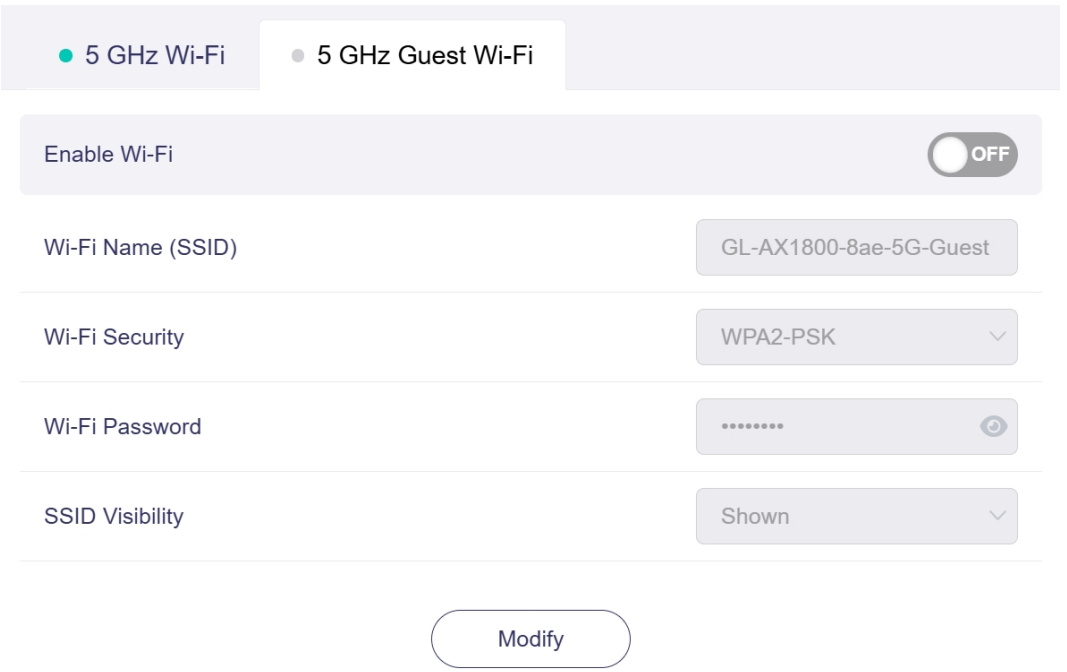
Lo Wi-Fi principale 5 GHz consente di configurare più impostazioni, tra cui abilitare/disabilitare Wi-Fi, impostare la potenza TX, abilitare/disabilitare BSSID randomizzato, impostare il nome Wi-Fi (SSID), sicurezza, password, SSID visibilità, modalità, larghezza di banda e canale.



Nota:

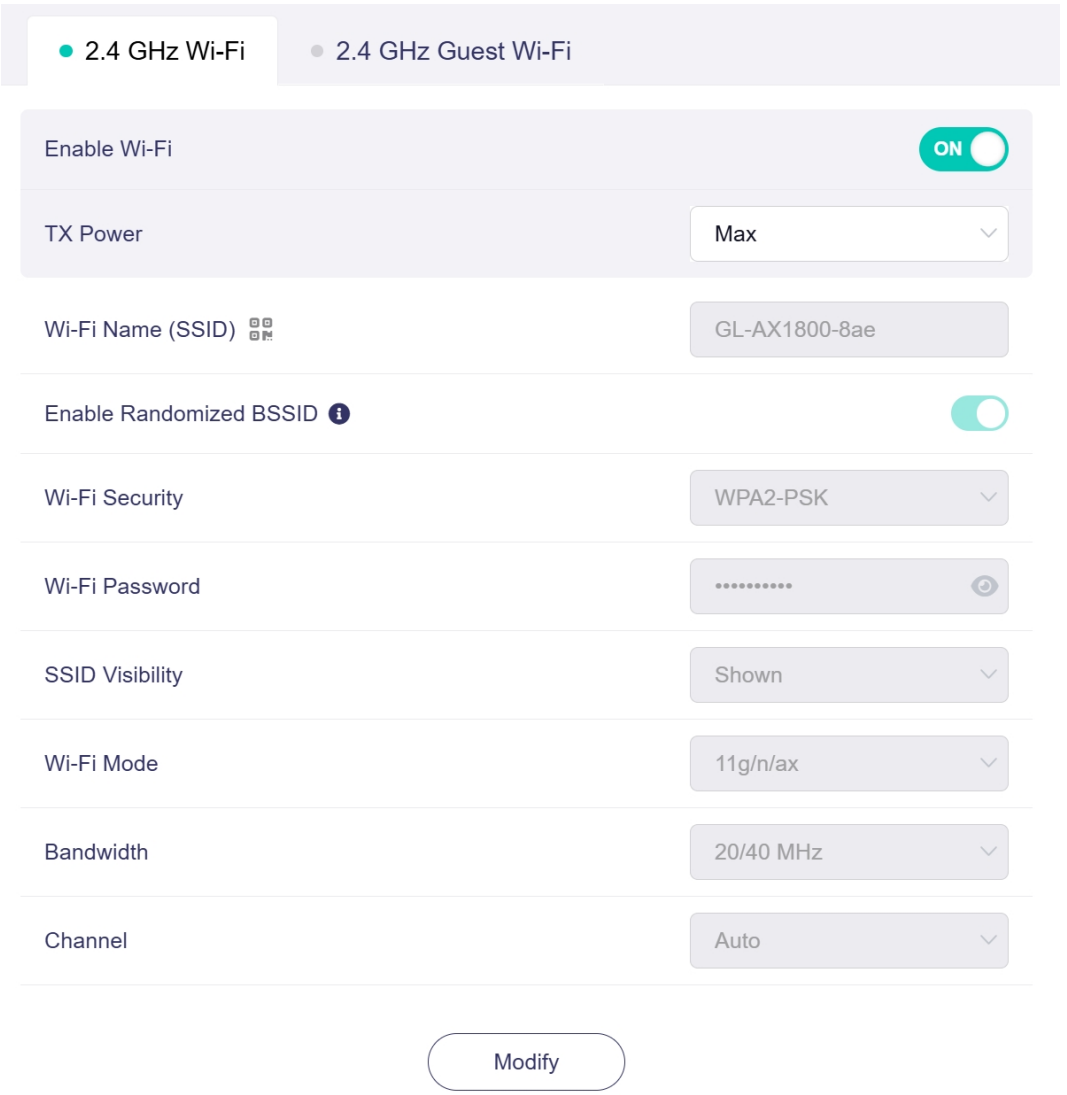
1. **BSSID casuale** è abilitato per impostazione predefinita. Aiuta a impedire che il router venga tracciato attraverso un BSSID fisso, poiché i dispositivi client potrebbero segnalare i BSSID vicini e i propri dati sulla posizione ai fornitori di sistemi operativi/dispositivi, che li utilizzano per creare un database da BSSID alla posizione. Quando è abilitato, il router utilizza uno BSSID generato casualmente e lo rinnova ad ogni riavvio, quindi BSSID non può essere collegato a una posizione fissa.
2. La **larghezza di banda** e **il canale** non possono essere modificati quando il router è configurato come ripetitore, poiché seguono quello della rete ripetuta.
3. Quando **Canale** è impostato su **Automatico**, il Wi-Fi del router non passerà automaticamente al canale DFS.

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



5.2.2 2.4 GHz Wi-Fi

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



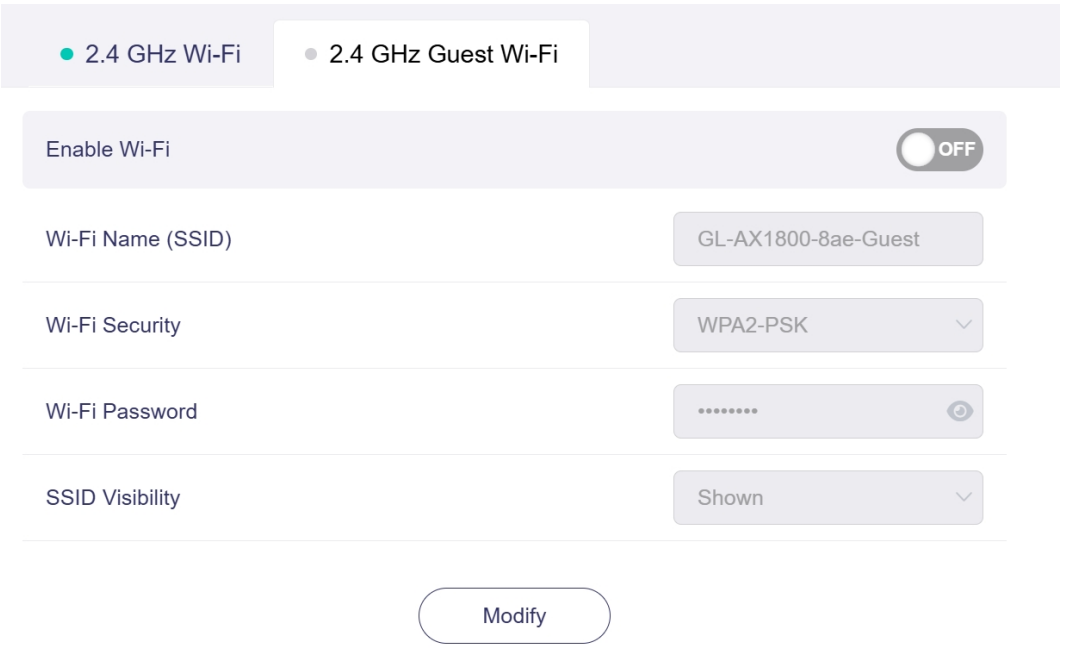
Nota:

1. **BSSID casuale** è abilitato per impostazione predefinita. Aiuta a impedire che il router venga tracciato attraverso un BSSID fisso, poiché i dispositivi client potrebbero segnalare i BSSID vicini e i propri dati sulla posizione ai fornitori di sistemi operativi/dispositivi, che li utilizzano per creare un database da BSSID alla posizione. Quando è abilitato, il router

utilizza uno BSSID generato casualmente e lo rinnova ad ogni riavvio, quindi BSSID non può essere collegato a una posizione fissa.

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

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



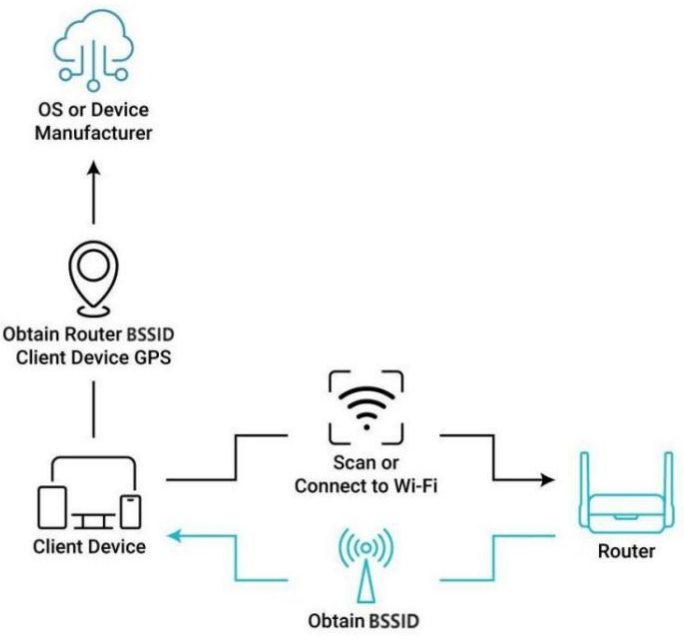
5.2.3 BSSID casuale

BSSID casuale è una funzionalità di privacy disponibile a partire dal firmware v4.6 e abilitata per impostazione predefinita. Impedisce che il router venga localizzato e monitorato tramite un Wi-Fi BSSID fisso (l'indirizzo MAC dell'interfaccia wireless del router).

Perché un BSSID fisso rappresenta un rischio per la privacy

I sistemi operativi mobili (ad esempio Android e iOS) si affidano al posizionamento Wi-Fi di crowdsourcing per fornire servizi di localizzazione:

1. I dispositivi client (telefoni, laptop) caricano periodicamente i BSSID che possono vedere, insieme alla propria posizione derivata dal GPS, sul server del fornitore del sistema operativo/dispositivo.
2. I fornitori aggregano questi dati in un database globale BSSID-to-location.
3. Qualsiasi dispositivo con Wi-Fi abilitato, anche senza GPS, può interrogare quel database per stimare la sua posizione dai BSSID circostanti.
4. Di conseguenza, un router con BSSID fisso agisce come un segnale di posizione stazionario: può essere geolocalizzato da remoto e i suoi movimenti (ad esempio, quando viaggi con lui) possono essere tracciati nel tempo. Gli aggressori possono anche interrogare tali database per individuare i router o rilevarne le impronte digitali tramite le informazioni sul fornitore (OUI) dello BSSID.



Come ti protegge Randomized BSSID

Quando questa funzione è abilitata, il router genera uno BSSID casuale e lo rinnova ad ogni avvio. Poiché BSSID continua a cambiare, non può più essere legato a una posizione fissa nei database dei fornitori, interrompendo l'associazione della posizione BSSID utilizzata per il monitoraggio.

Stato	Comportamento
Abilitato (predefinito)	Un nuovo BSSID casuale viene generato e rinnovato ad ogni avvio
Disabilitato	Il router utilizza il suo vero indirizzo MAC di fabbrica come BSSID

Note:

1. Lo BSSID cambia solo quando il router si riavvia; rimane lo stesso durante una sessione di corsa.
2. Per Guest Wi-Fi, BSSID rimane coerente con Main Wi-Fi BSSID sulla stessa banda di frequenza.
3. BSSID casuale blocca il tracciamento tramite BSSID del router, ma non impedisce ai dispositivi client di segnalare la propria posizione e non è una soluzione completa per la privacy: è ancora possibile osservare le caratteristiche di SSID, del canale e del segnale.

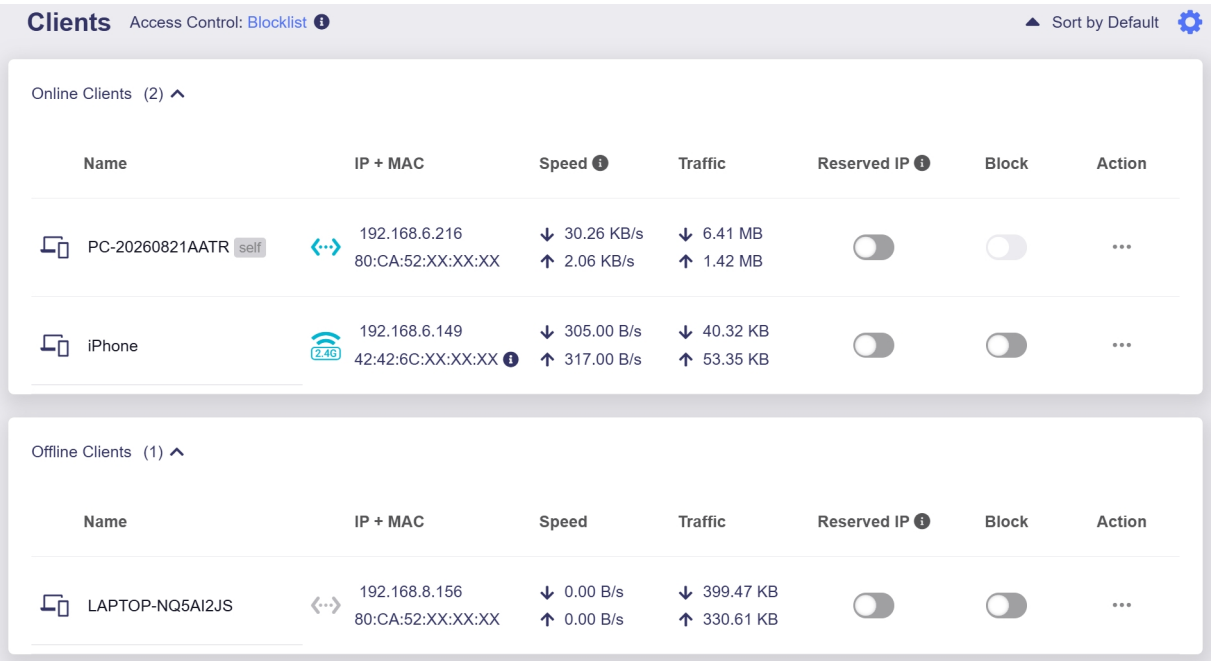
Capitolo 6

Client

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

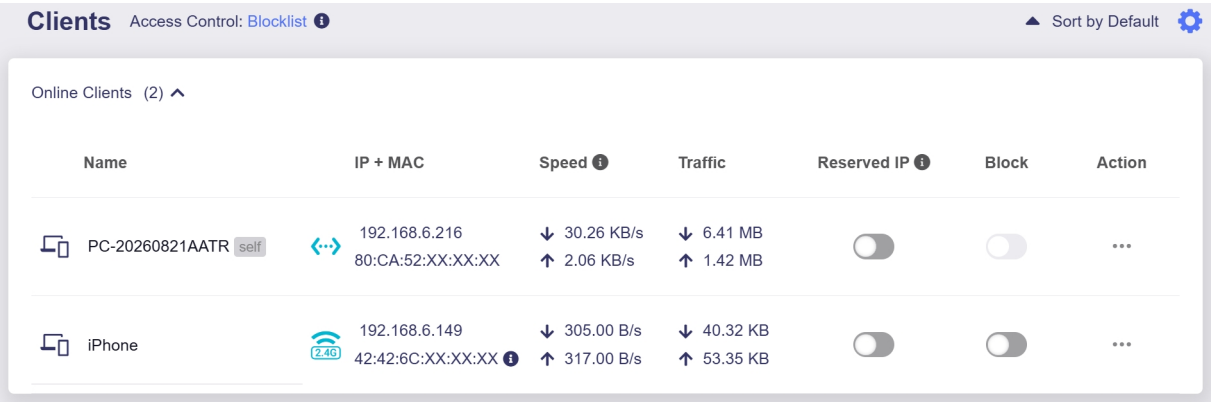
Accedi al pannello di amministrazione web del router e vai a **CLIENT**.

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



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

6.1 Dettagli del dispositivo



1. **Nome dispositivo**

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

2. **Indirizzo IP e MAC**

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



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

3. **Velocità**

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

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

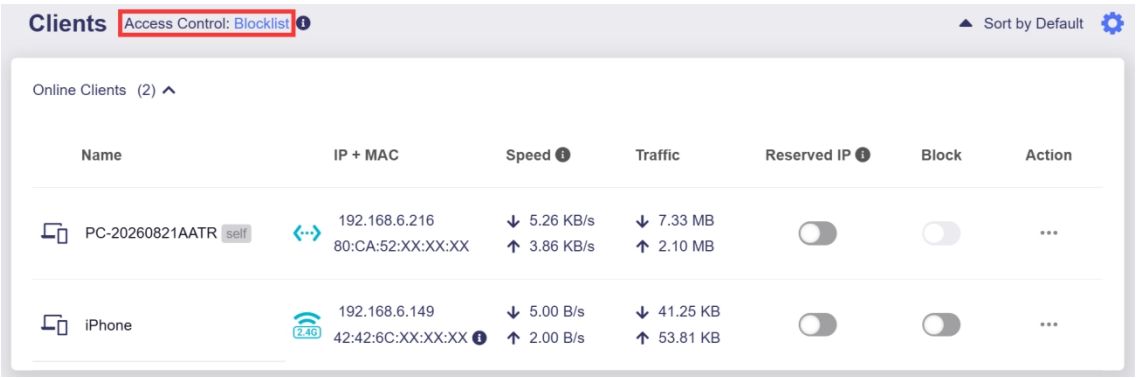
5. **Prenota IP**

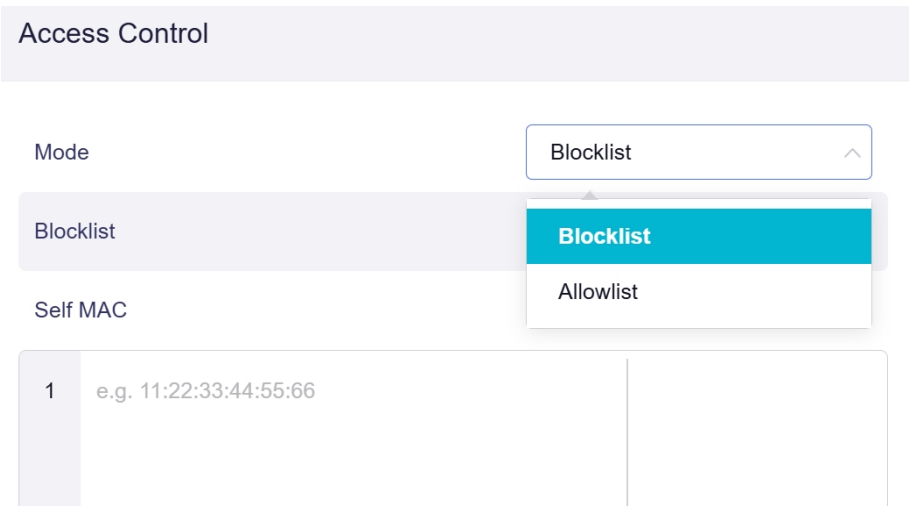
Nella quinta colonna, puoi riservare l'indirizzo IP per il dispositivo connesso con un clic. Quando specifichi un indirizzo IP riservato per un client all'interno della rete locale, riceverà sempre lo stesso indirizzo IP ogni volta che si connette al router.

6. **Lista bloccata**

Nella sesta colonna puoi bloccare specifici dispositivi collegati con un clic.

La regola di controllo dell'accesso è Blocklist per impostazione predefinita e, se necessario, puoi cambiarla in Lista consentita dall'alto.



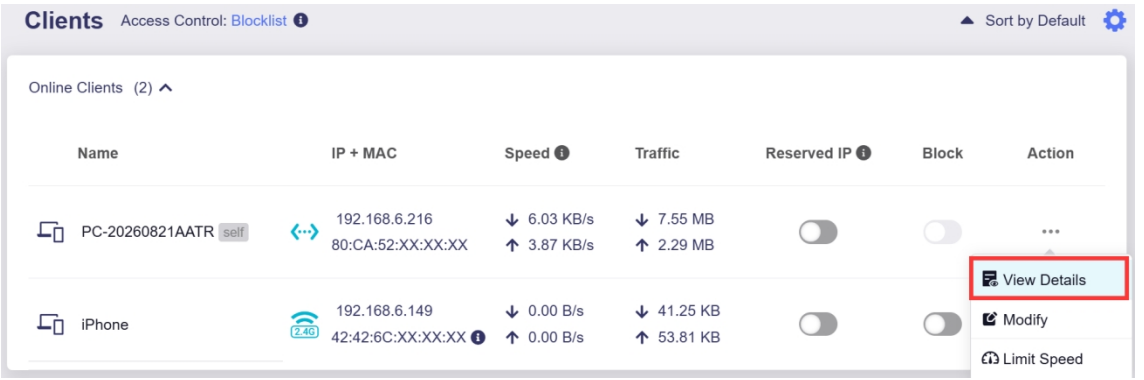


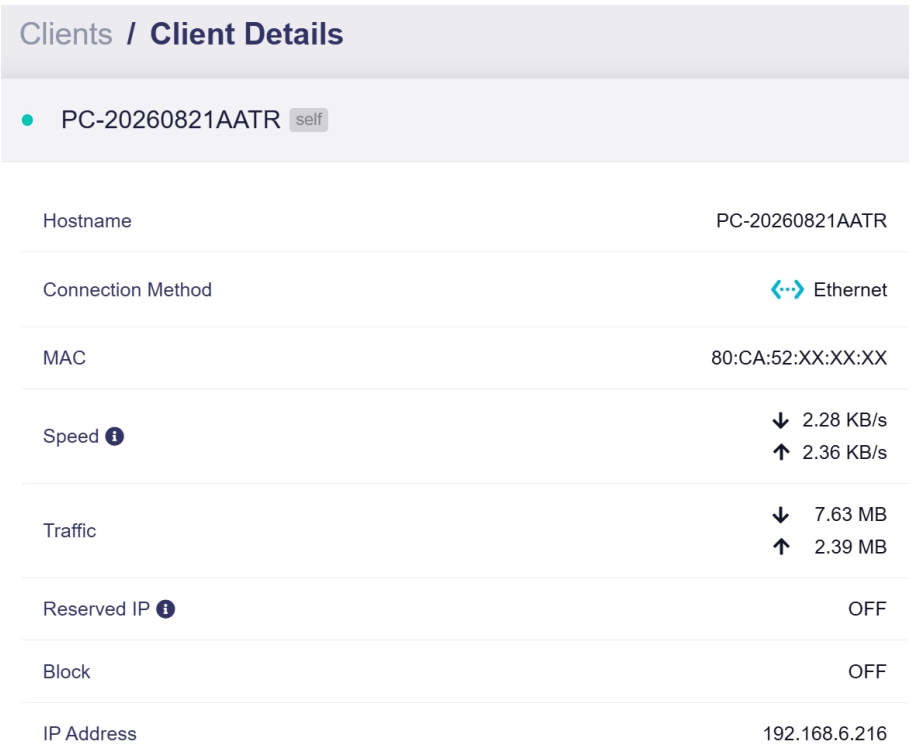
- **Lista nera**: i dispositivi con indirizzi MAC nella lista nera non possono connettersi a questo router. Tieni presente che il blocco del client si basa sull'indirizzo MAC del dispositivo. Se la prossima volta il dispositivo bloccato utilizza un indirizzo MAC diverso, può comunque riuscire a connettersi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

6.2 Azione

1. **Visualizzazione dettagli**

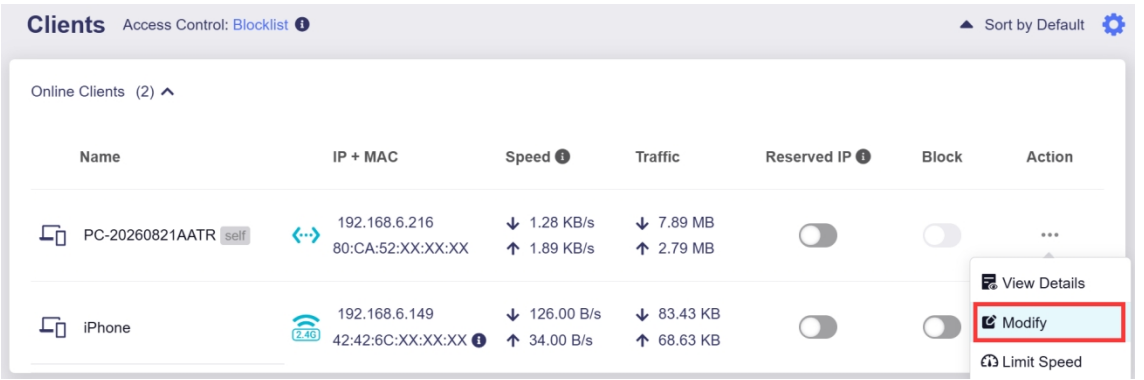
   Fai clic sull'icona a tre punti nella colonna **Azione**, quindi su **Visualizzazione dettagli** dal menu a discesa per visualizzare i dettagli del dispositivo in un'unica pagina.

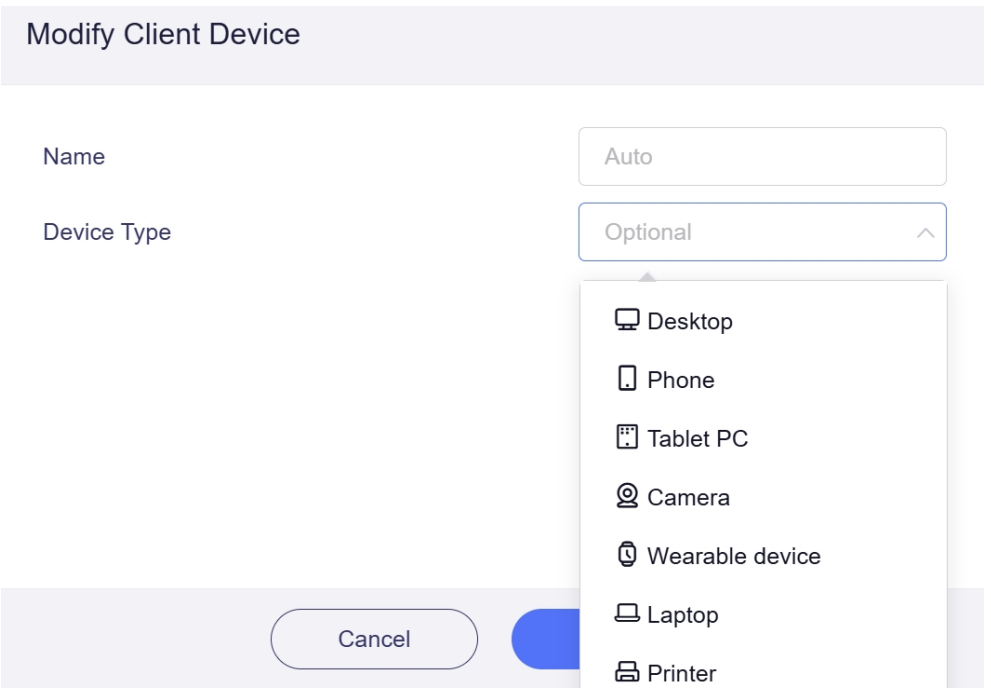




2. **Modifica**

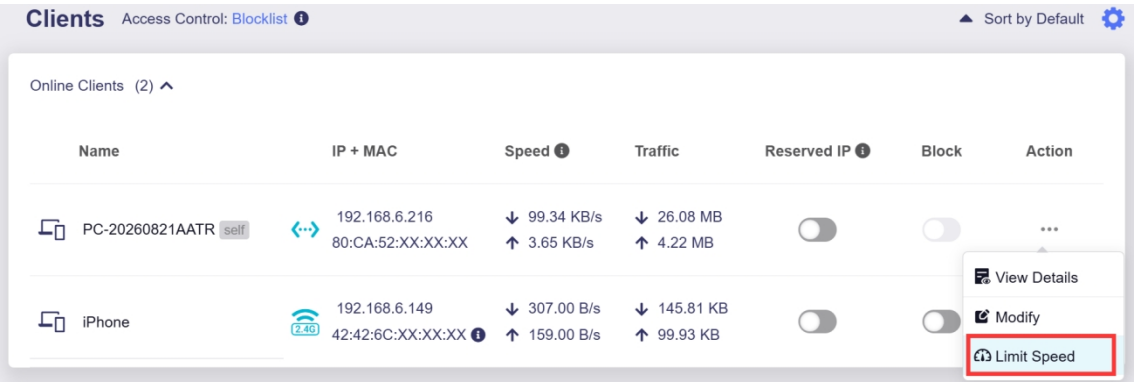
Fai clic sull'icona a tre punti nella colonna **Azione**, quindi su **Modifica** dal menu a discesa per modificare il nome e il tipo del dispositivo.



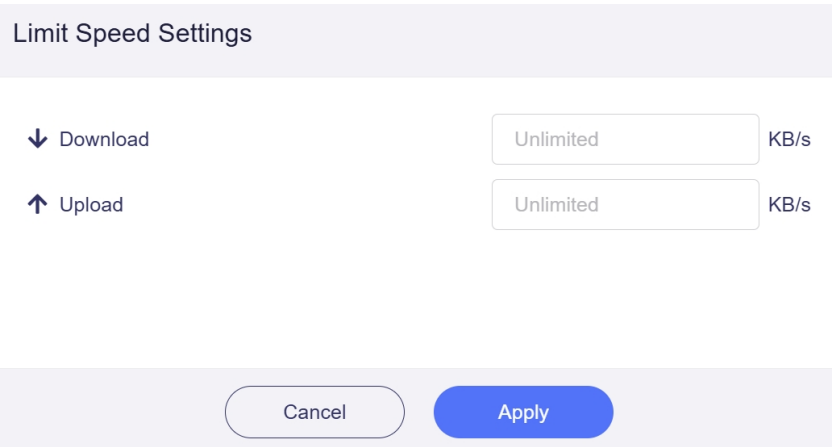


3. **Limita velocità**

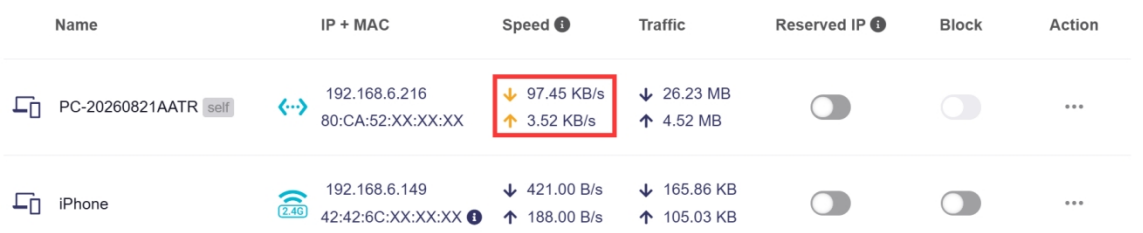
Fai clic sull'icona a tre punti nella colonna **Azione** e fai clic su **Limita velocità** dal menu a discesa.



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

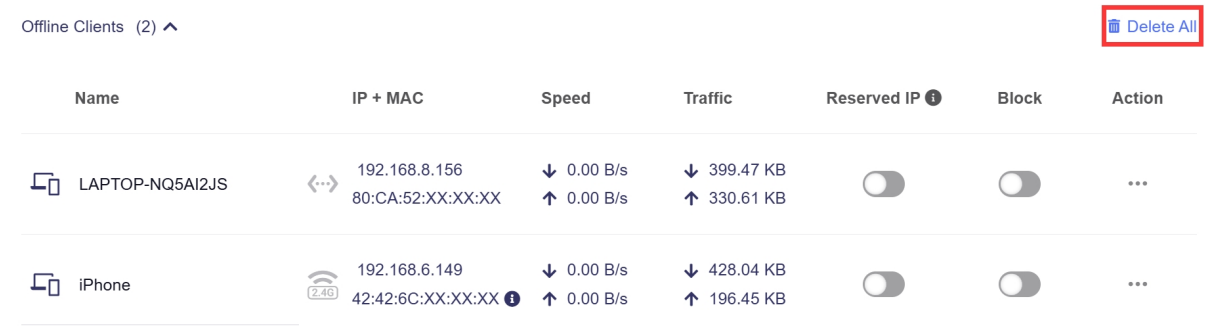


Se a un dispositivo è stata applicata una limitazione di velocità, le frecce della velocità di caricamento/download diventeranno gialle.

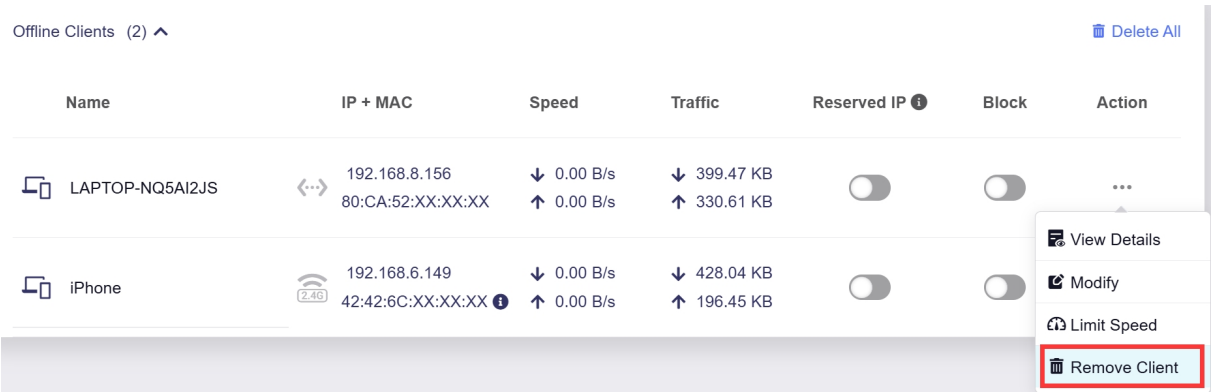


6.3 Rimozione dei client

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

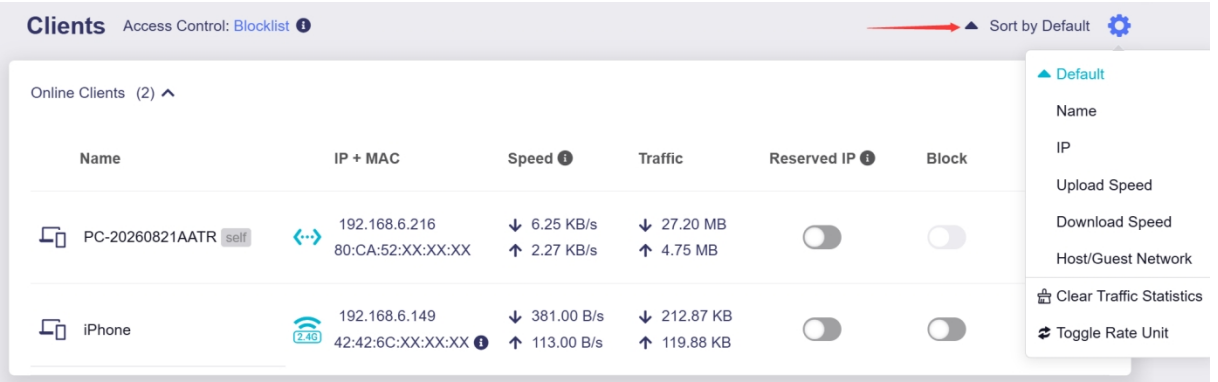


Per rimuovere un client specifico, fai clic sull'icona a tre punti nella colonna **Azione**, quindi seleziona **Rimuovi client** dal menu a discesa.



6.4 Ordinamento

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



L'ordinamento predefinito è il seguente:

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

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

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



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

Capitolo 7

Servizi cloud

Questo capitolo presenta due servizi cloud: GoodCloud e AstroWarp.

7.1 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.

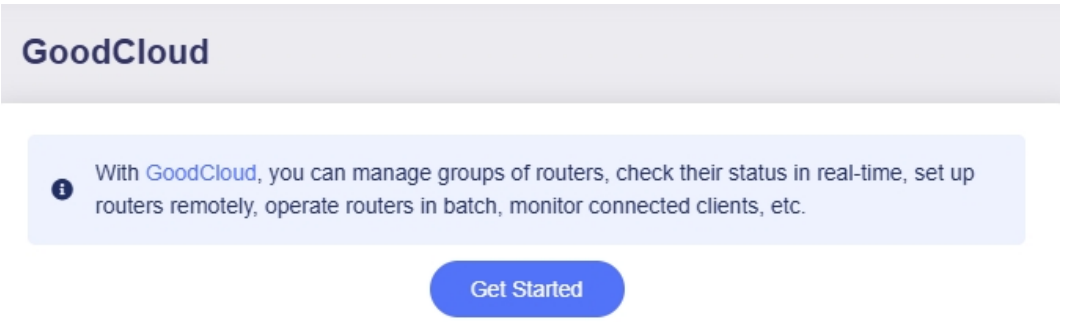
Con GoodCloud puoi:

- 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

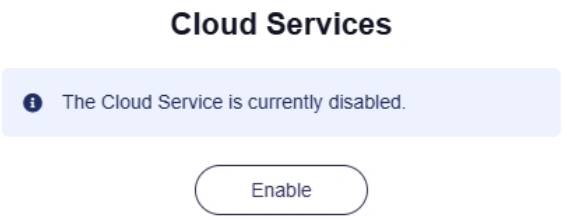
Alcune funzionalità sono disponibili nel piano Enterprise e nel piano VAR (rivenditore a valore aggiunto). Vedi qui per i dettagli.

7.1.1 Attivazione di GoodCloud

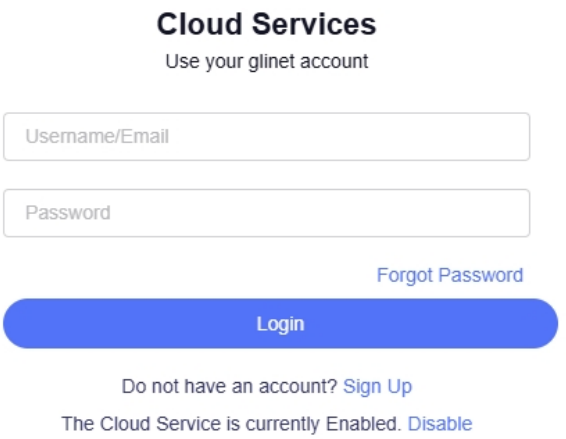
1. Accedi al pannello di amministrazione web del tuo router, vai a **SERVIZI CLOUD** > **GoodCloud** e fai clic su **Inizia.**



2. Apparirà una finestra a discesa nell'angolo in alto a destra. Fai clic su **Abilita**.



3. Accedi con il tuo account GL.iNet Cloud. Se non disponi di un account, creane uno ed effettua l'accesso. Una volta effettuato l'accesso, il router verrà associato automaticamente al tuo account.

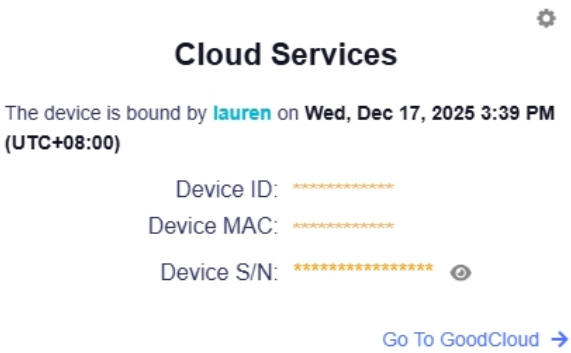


Suggerimenti:

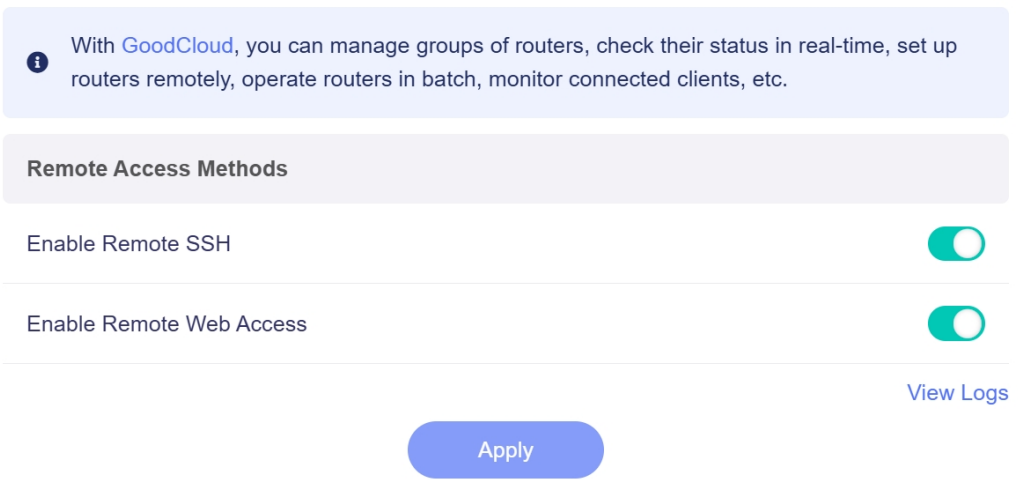
- I passaggi di associazione di GoodCloud differiscono in base alla versione del firmware.

- Se non ricevi l'e-mail di verifica, controlla la cartella spam o riprova più tardi. Per ulteriore assistenza, contattaci all'indirizzo support@gl-inet.com.

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 fornisce 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.



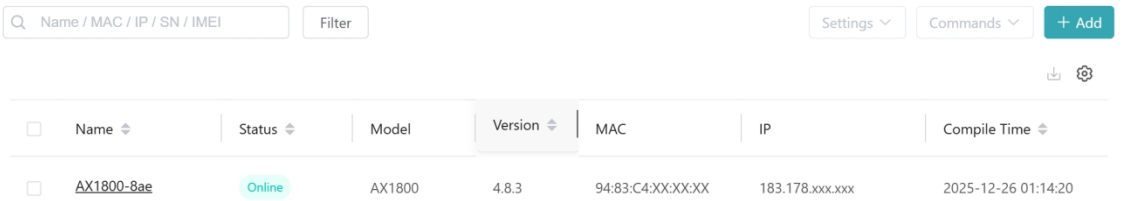
- **SSH remoto**: accedi in remoto al terminale del router da GoodCloud utilizzando SSH.
- **Accesso web remoto**: accesso remoto al pannello di amministrazione web del router da GoodCloud tramite HTTP/HTTPS.

- **Visualizza registri**: reindirizza alla pagina Registro e visualizza il registro Cloud.

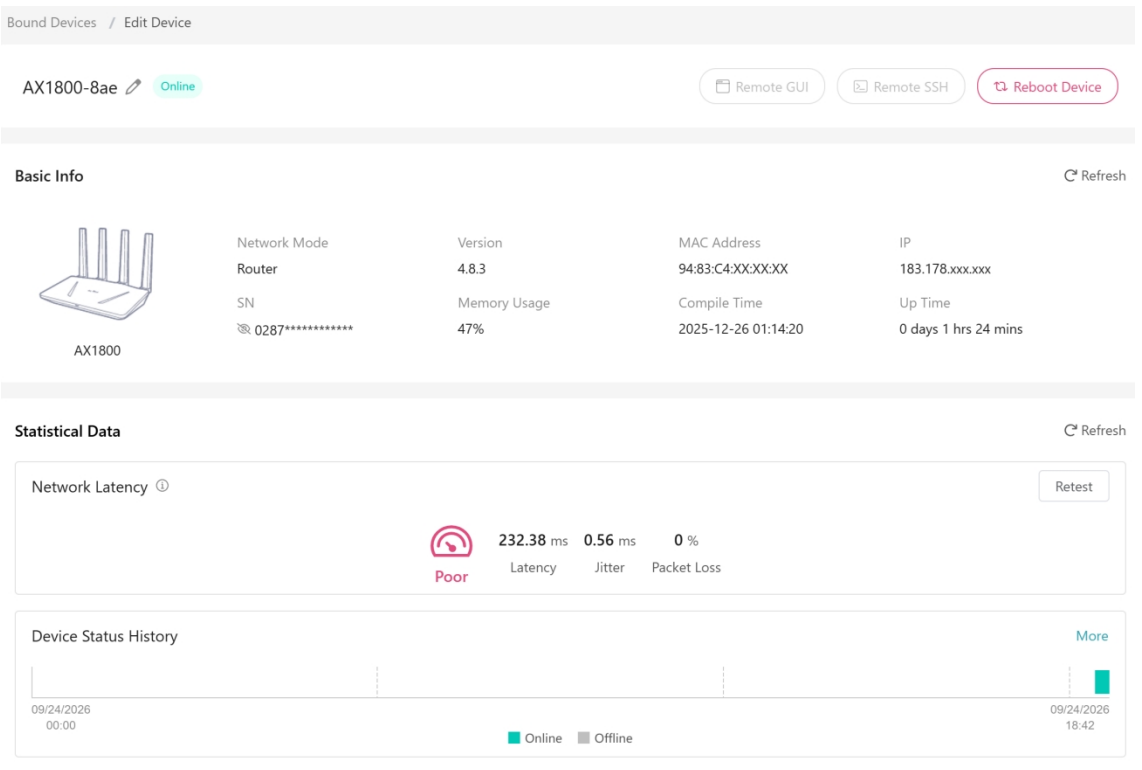
7.1.2 Gestione del router

Controlla i dettagli del dispositivo

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

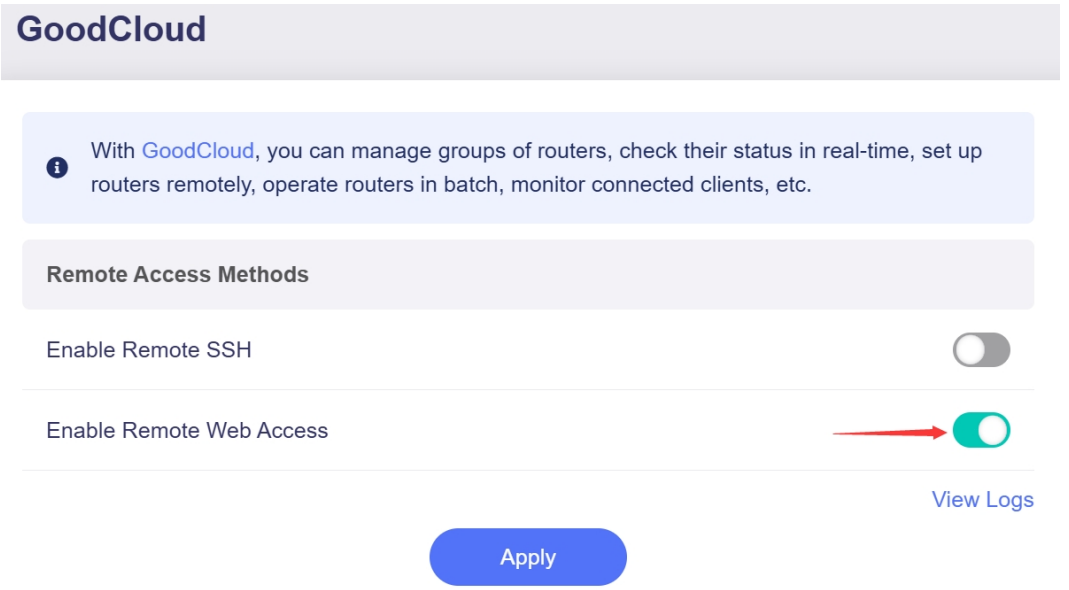


Fare clic sul nome del dispositivo per accedere alla pagina dei dettagli del dispositivo, che visualizza informazioni di base, dati statistici, panoramica della rete, elenco client e sequenza temporale. Puoi anche eseguire operazioni avanzate, come l'accesso remoto al router e il riavvio del dispositivo.

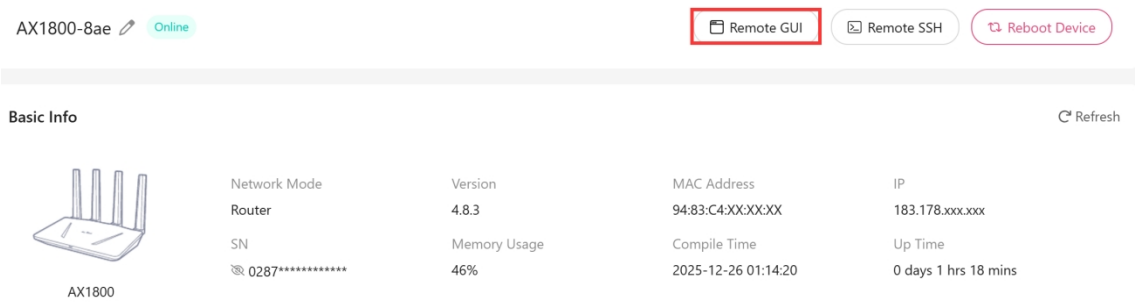


Accesso web remoto

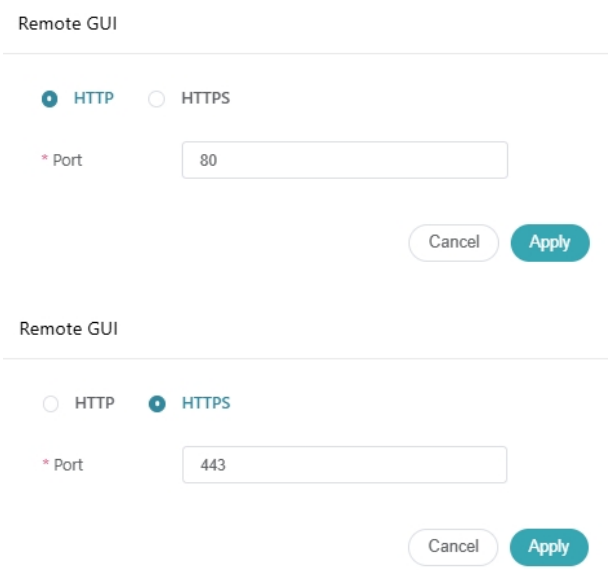
1. Accedi al pannello di amministrazione web del router, vai a **SERVIZI CLOUD** > **GoodCloud**, abilita **Accesso web remoto**, quindi fai clic su **Applica**.



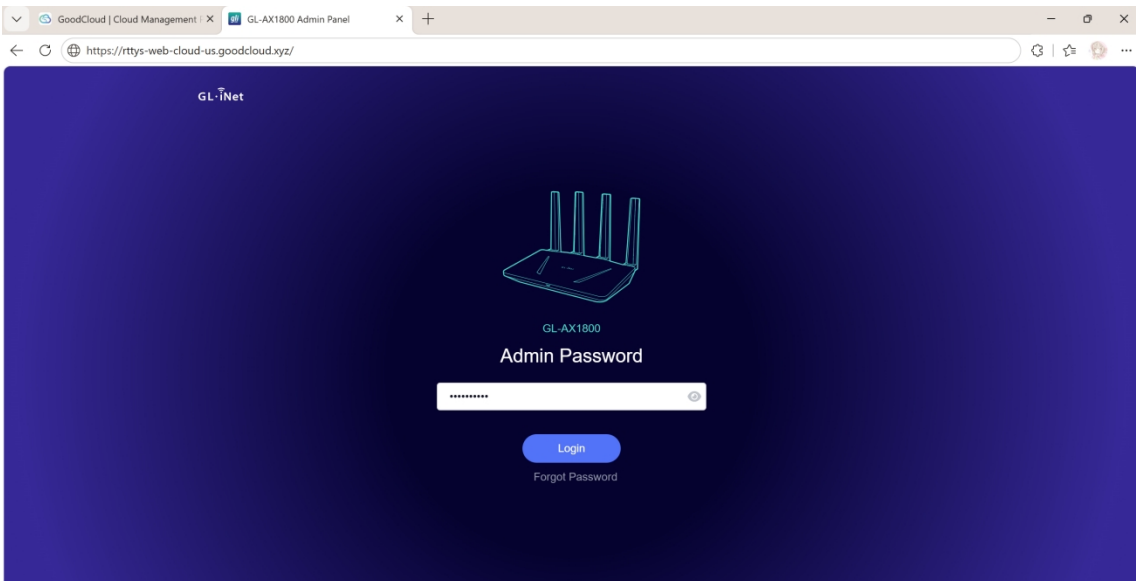
2. Accedi alla piattaforma GoodCloud e vai a **Dispositivi > Dispositivi associati**. Fai clic sul dispositivo a cui desideri accedere e accederai alla pagina dei dettagli del dispositivo.
3. Nella pagina dei dettagli del dispositivo, fai clic sul pulsante **GUI remota** nell'angolo in alto a destra.



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

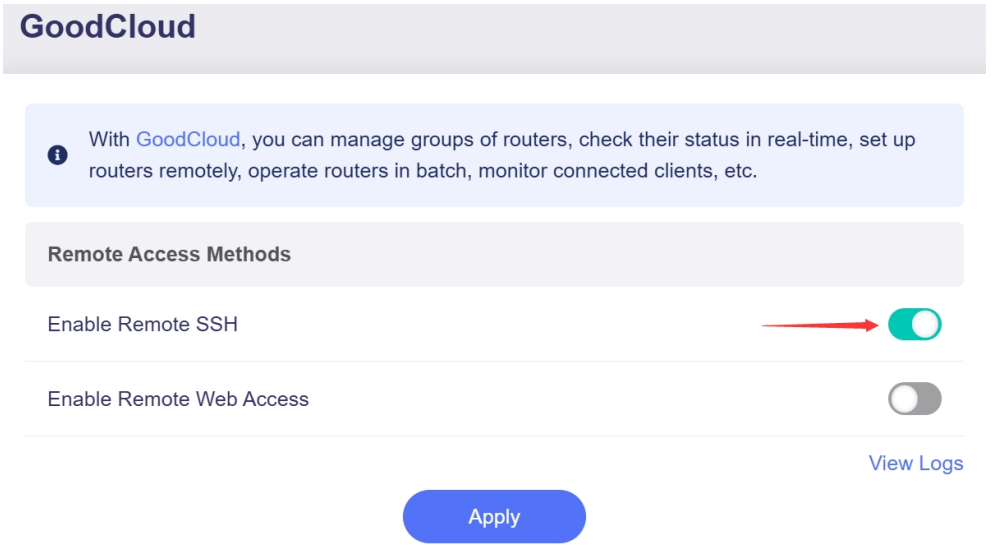


5. Verrai reindirizzato alla pagina di accesso del router. Inserisci la password dell'amministratore per accedere da remoto al pannello di amministrazione web del router.

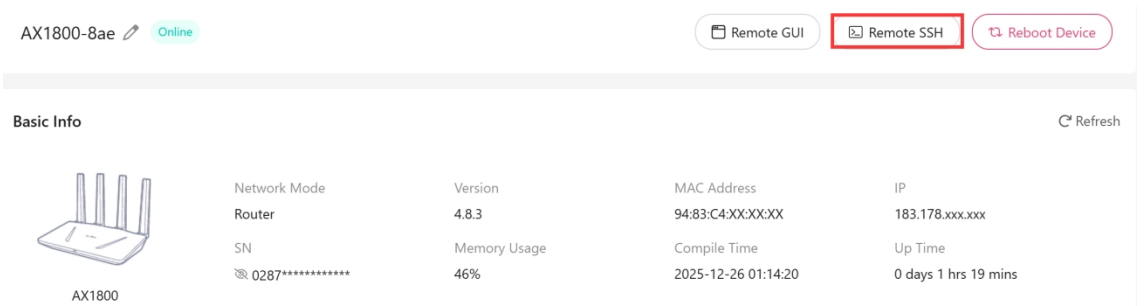


SSH remoto

1. Accedi al pannello di amministrazione web del router, vai 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.

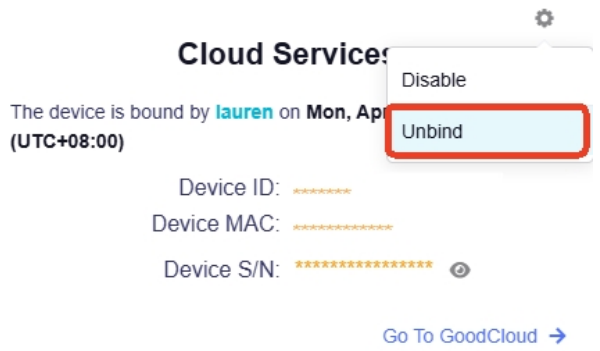


4. Registro come **root** e inserisci la password per accedere al terminale del tuo router.

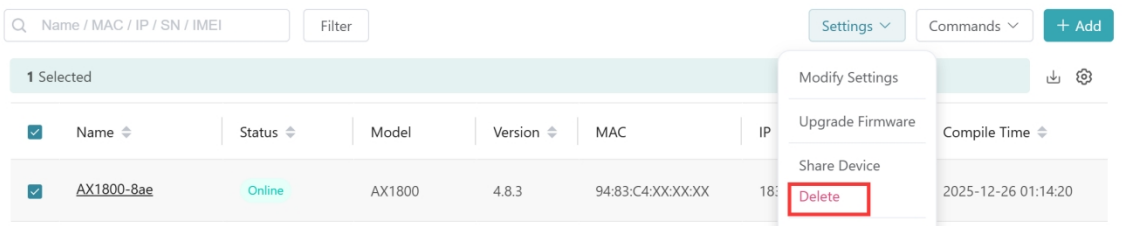


7.1.3 Dissociazione del dispositivo

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.

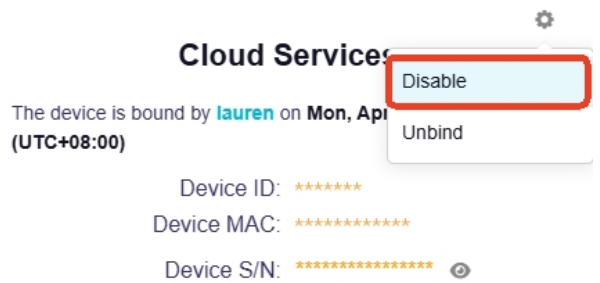


In alternativa, accedi alla piattaforma cloud e vai a **Dispositivo** > **Dispositivi associati**. Seleziona il dispositivo che desideri scollegare, fai clic su **Impostazioni** nell'angolo in alto a destra, quindi seleziona **Elimina**. Il tuo dispositivo verrà quindi scollegato dal tuo account GoodCloud.



7.1.4 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.

7.2 AstroWarp

AstroWarp è una piattaforma di rete avanzata progettata per fornire reti remote e gestione remota dei dispositivi senza soluzione di continuità.

Costruito appositamente per l'integrazione del router GL.iNet, AstroWarp supporta la gestione completa dei dispositivi su intere reti, consentendo il controllo sia del dispositivo superiore che di quello inferiore.

Concentrandosi sulla gestione a livello di rete e sul futuro supporto per il controllo a livello hardware, AstroWarp offre una soluzione più solida e affidabile per la gestione dei dispositivi e il mantenimento di reti sicure e stabili.

Fai riferimento a astrowarp.net per ulteriori informazioni.

Capitolo 8

Conoscere le VPN

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

8.1 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.

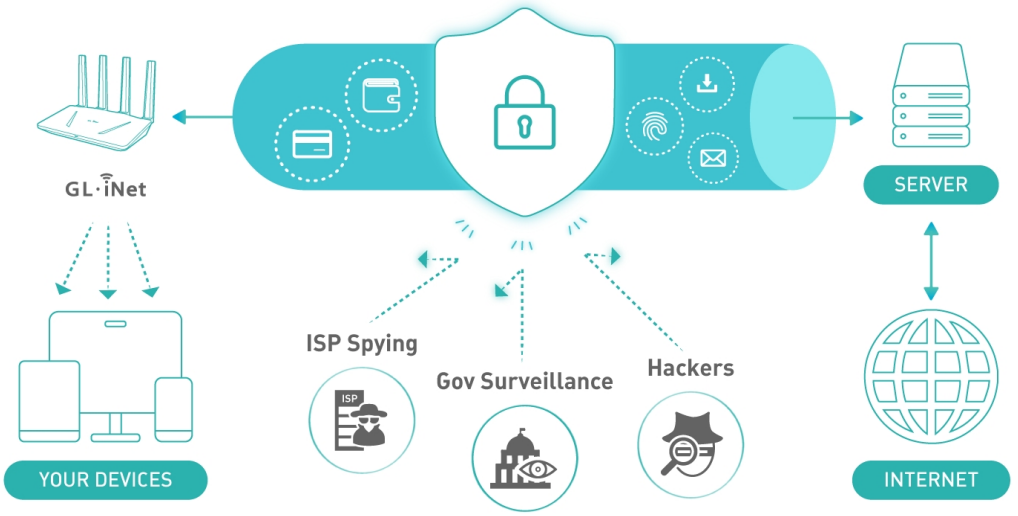
WireGuard

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.

8.2 Scenari di utilizzo

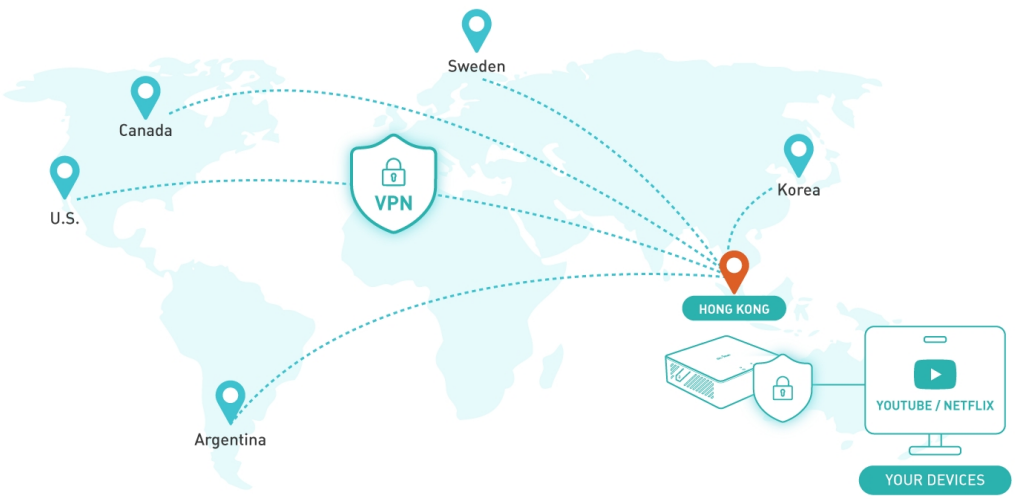
1. **Privacy dei dati personali**

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



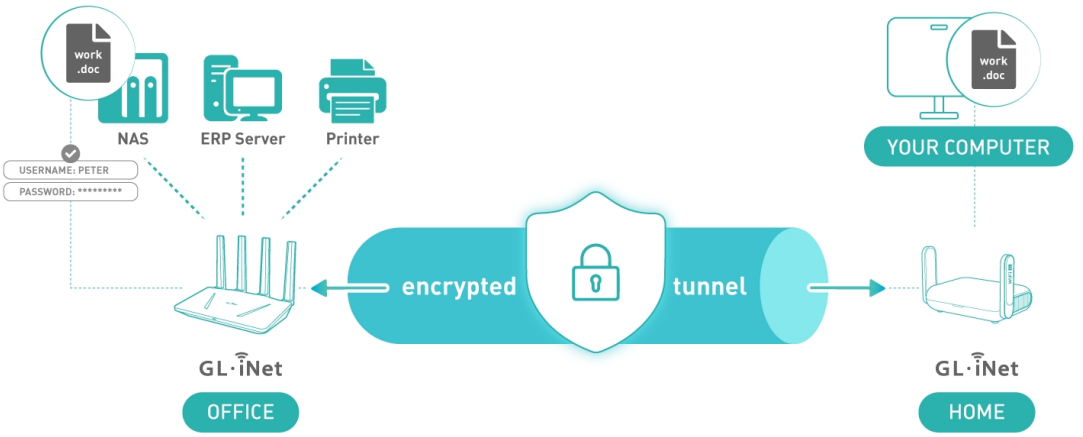
2. **Accesso illimitato in tutto il mondo**

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



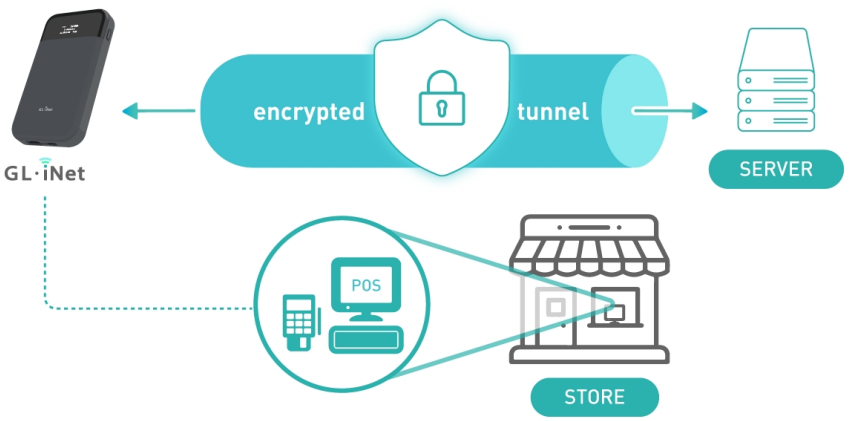
3. **Sicurezza dei dati delle piccole imprese**

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



4. **Infrastruttura di pagamento sicura**

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



Capitolo 9

Dashboard VPN

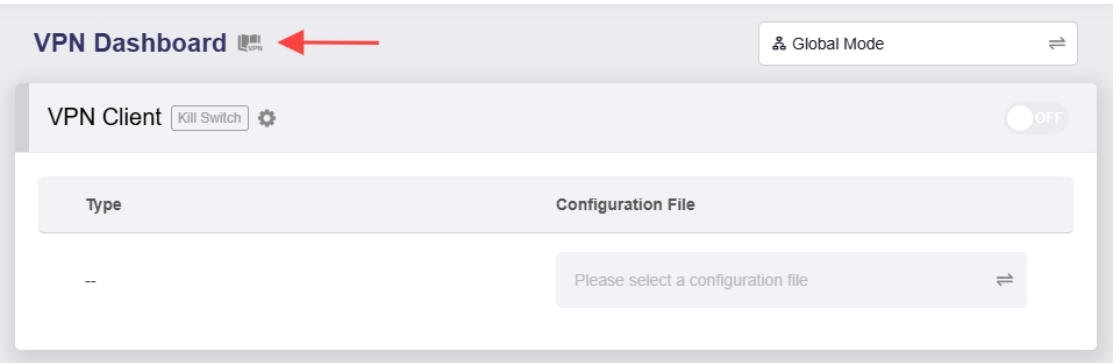
Questo capitolo introduce come gestire le connessioni VPN tramite pannello di amministrazione web.

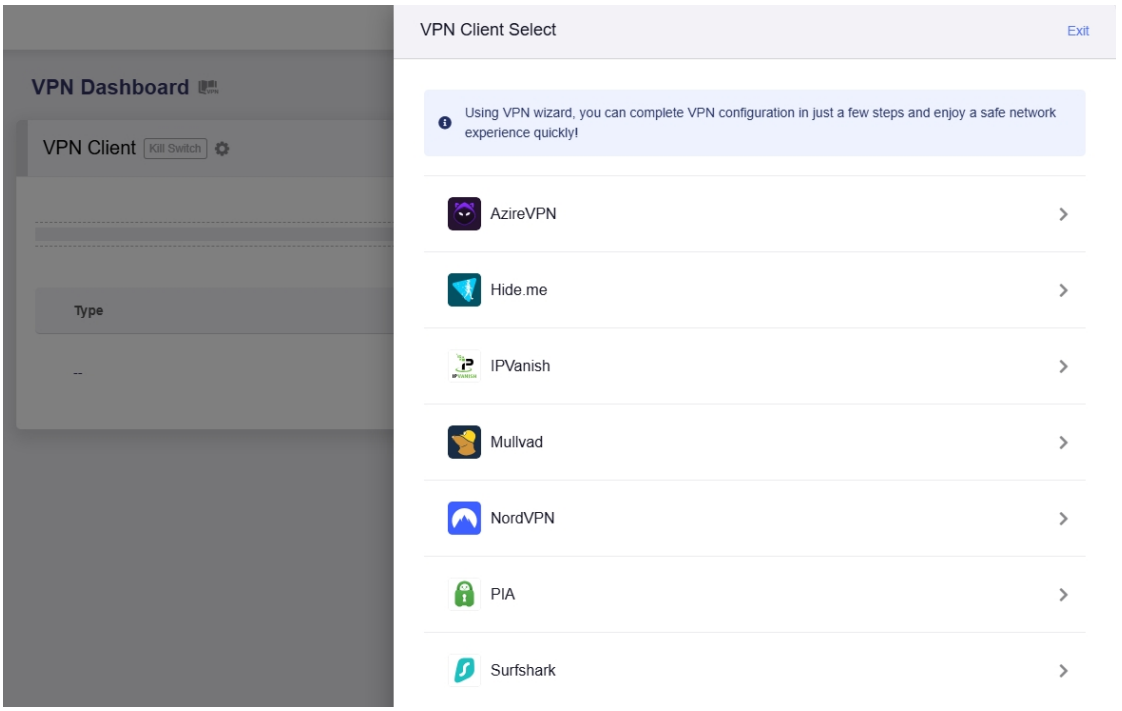
Accedi al pannello di amministrazione web del router e vai a **VPN** > **Dashboard VPN**.

Quando il router è impostato come client VPN attiva, il dashboard VPN visualizza i dettagli della connessione VPN, come regole del tunnel, indirizzo del server, statistiche sul traffico, IP virtuale client e registro della connessione. Ti consente inoltre di configurare impostazioni avanzate come VPN Kill Switch, Masquerading IP e MTU.

9.1 Configurazione guidata VPN

Per iniziare, fai clic sull'icona del libro nell'angolo in alto a sinistra e segui la procedura guidata di configurazione della VPN per completare rapidamente la configurazione della VPN.



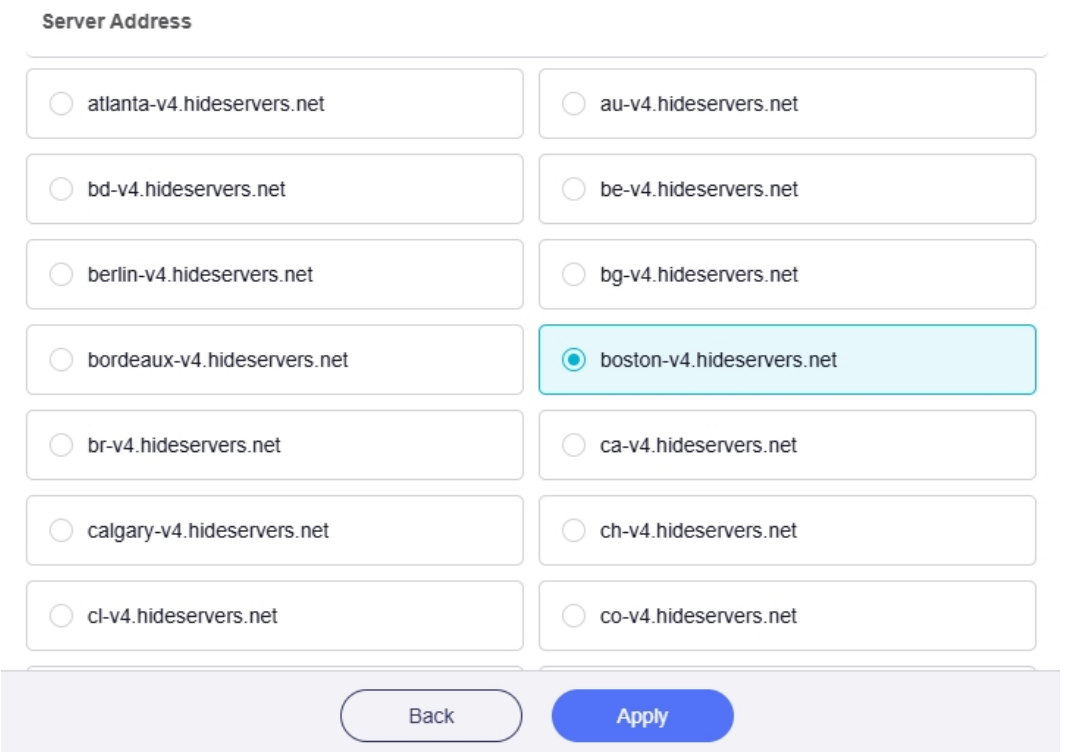


Nota: la configurazione guidata della VPN è valida solo per i servizi VPN integrati, inclusi AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA e Surfshark. Per altri provider VPN, salta la procedura guidata e vai su **VPN** > **Client OpenVPN** o **Client WireGuard** per configurare manualmente la VPN.

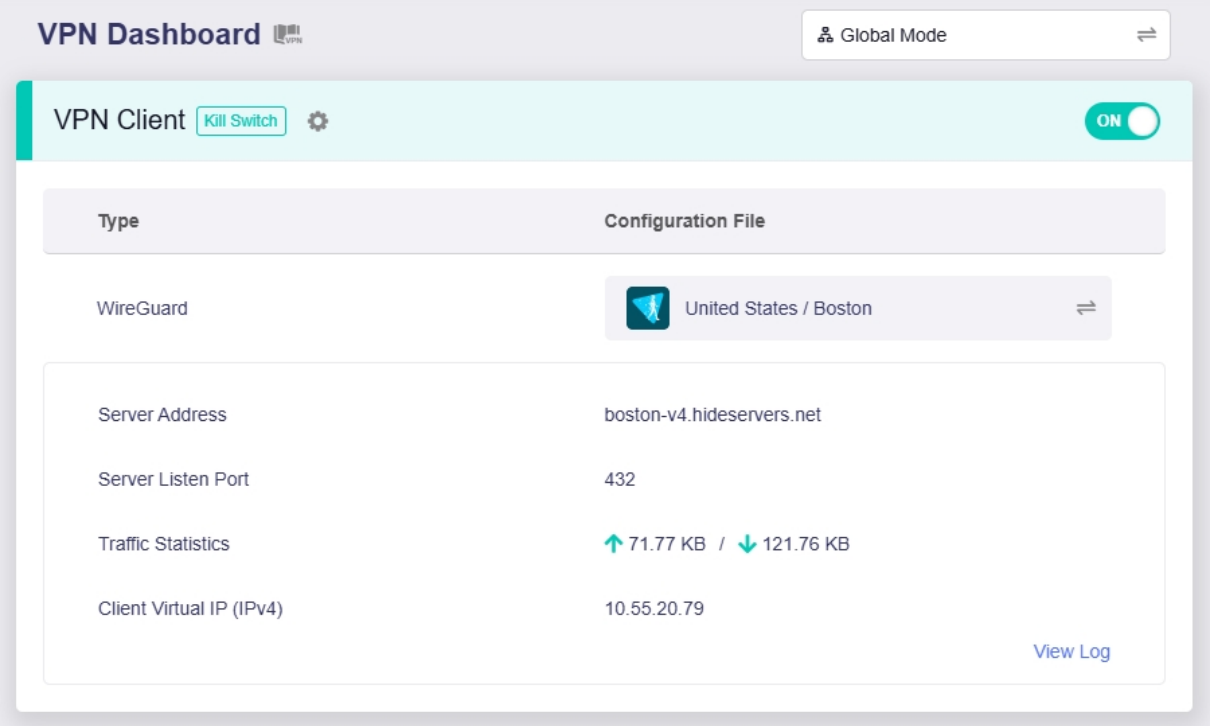
Ecco un esempio con **Hide.me**. Accedi con le credenziali Hide.me.



Seleziona un server VPN e fai clic su **Applica**. Questo è il server a cui ti connetterai e il tuo indirizzo IP pubblico sembrerà provenire dalla posizione del server selezionato.

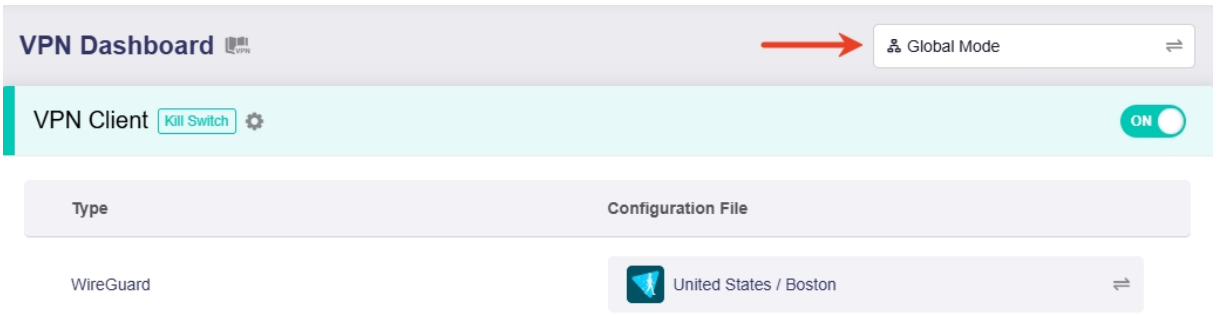


Si connetterà automaticamente. Una volta connesso, vai su **Dashboard VPN**. Vedrai che un tunnel VPN è stato abilitato, visualizzando dettagli tra cui il protocollo VPN (ad esempio, WireGuard), file di configurazione, indirizzo del server, porta di ascolto del server, statistiche sul traffico e indirizzo IP virtuale client. Puoi anche visualizzare i registri di connessione nell'angolo in basso a destra.

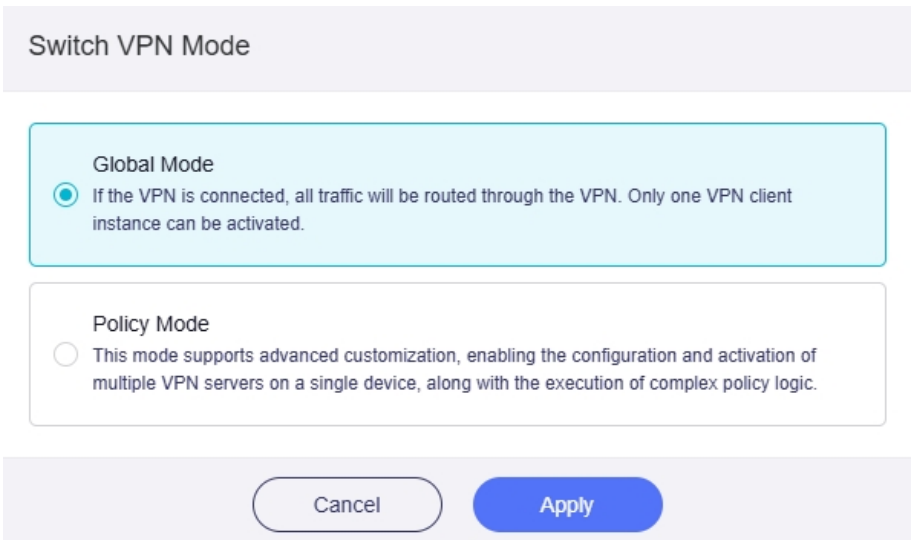


9.2 Modalità VPN

Sullo Dashboard VPN, fai clic sul pulsante nell'angolo in alto a destra per cambiare modalità VPN, se necessario.



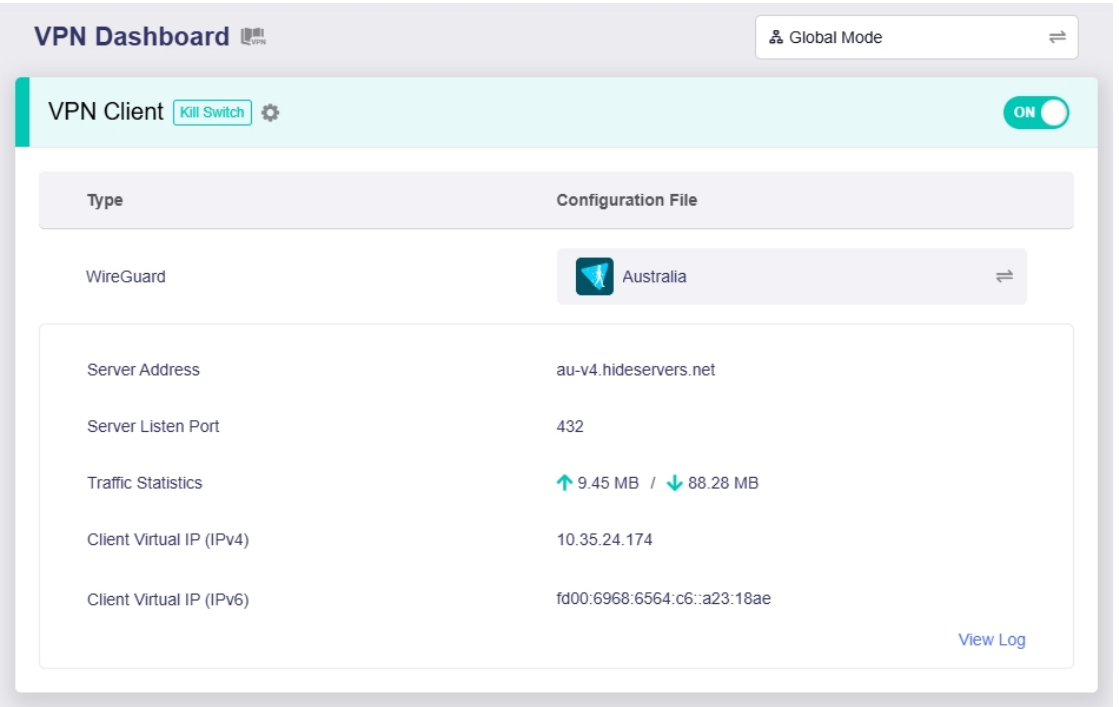
Sono disponibili due modalità: **modalità globale** e **modalità delle policy**.



9.2.1 Modalità globale

In questa modalità, tutto il traffico verrà instradato attraverso il tunnel VPN e sarà possibile attivare solo un'istanza client VPN. È ideale per scenari che richiedono che tutto il traffico del dispositivo passi attraverso un singolo server VPN, come la sicurezza di rete unificata o l'accesso a contenuti specifici della regione.

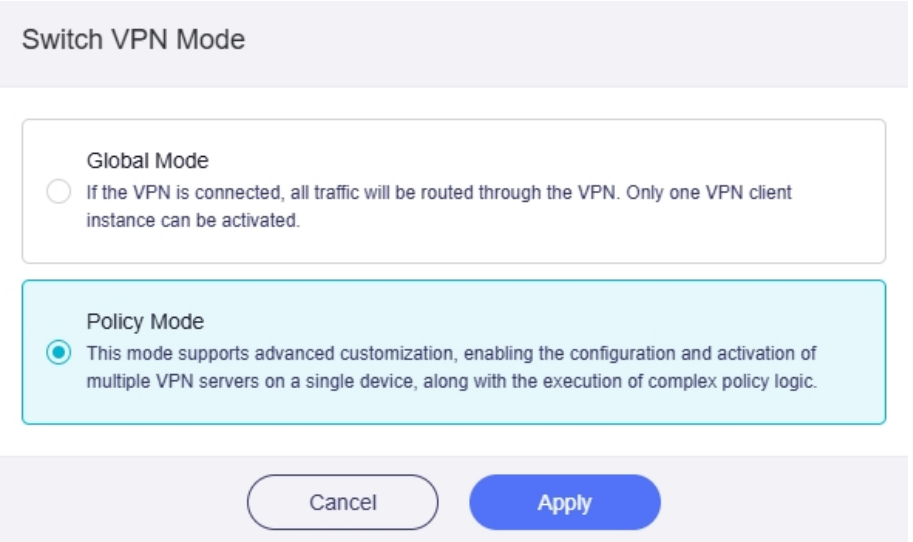
Nell'esempio seguente, il router si connette a un server australiano utilizzando il protocollo WireGuard. Tutto il traffico proveniente dai client connessi verrà instradato attraverso questo tunnel VPN.



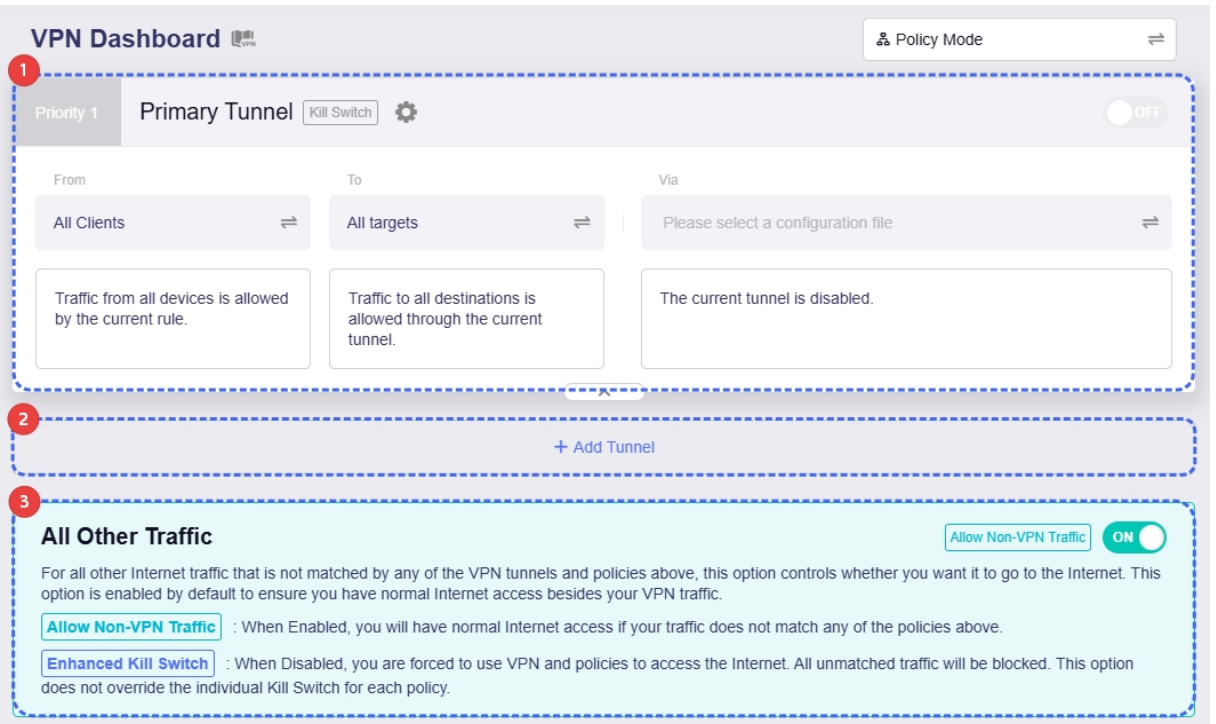
9.2.2 Modalità delle policy

In questa modalità, puoi connettere un singolo router a più server VPN e personalizzare le regole VPN. È adatto ai casi che richiedono una gestione flessibile del traffico, come l'instradamento di traffico diverso verso destinazioni diverse attraverso più server VPN.

Passa dalla modalità VPN alla **Modalità delle policy** e fai clic su **Applica**.



Dopo il passaggio, se la VPN non è abilitata, la pagina viene visualizzata come di seguito, incluse tre sezioni: **Tunnel primario**, **Aggiungi tunnel** e **Tutto il resto del traffico**.

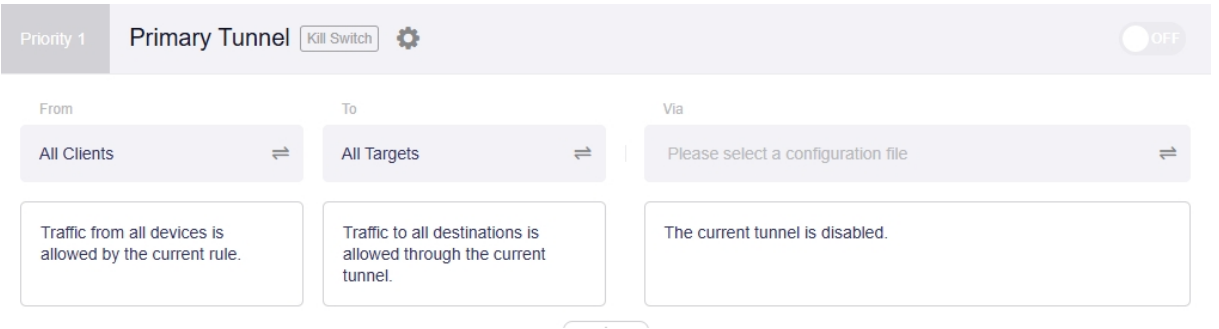


Tunnel primario

Il tunnel primario è un tunnel preimpostato in Modalità delle policy. Per impostazione predefinita ha la priorità più alta ed è possibile modificarne la priorità quando sono configurati più tunnel.

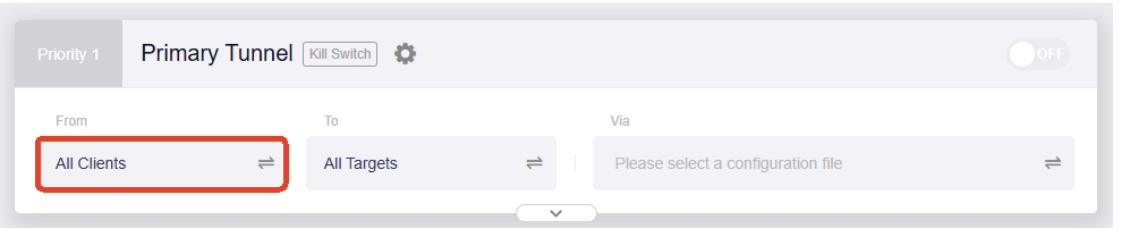
In questo tunnel, puoi personalizzare la regola del tunnel impostando tre fattori:

- **Da**: si riferisce alla sorgente del traffico, ovvero al traffico che dovrebbe essere instradato attraverso questo tunnel.
- **A**: si riferisce alla destinazione del traffico, verso la quale il traffico viene instradato attraverso questo tunnel.
- **Via**: si riferisce al metodo di instradamento del traffico, ovvero se utilizzare la VPN.

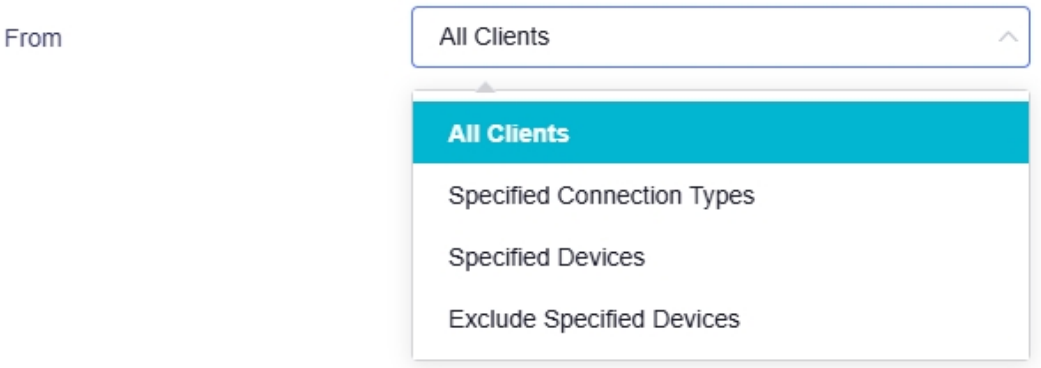


Segui i passaggi seguenti per configurare la regola del tunnel.

1. Fai clic sulla casella grigia a sinistra.

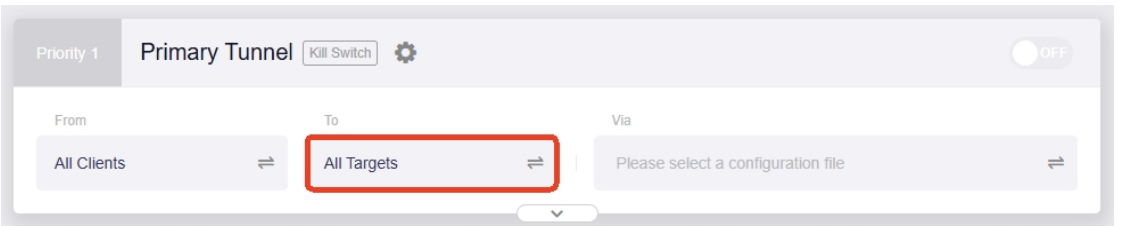


2. Seleziona il dispositivo a cui desideri che corrisponda a questa regola e fai clic su **Applica**.

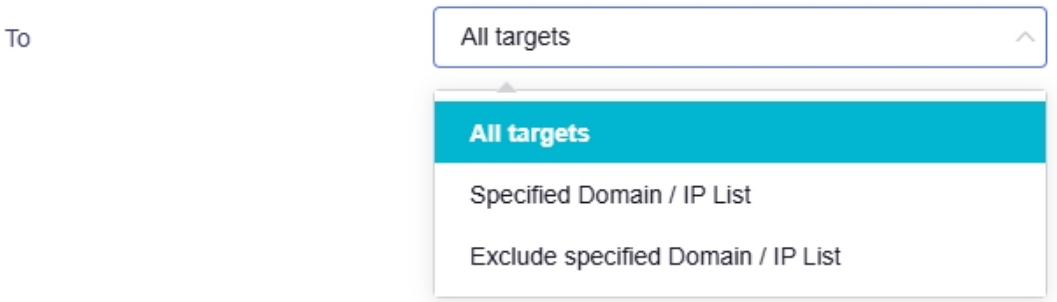


- **Tutti i client**: se selezionato, il traffico proveniente da tutti i dispositivi corrisponderà a questa regola.
- **Tipi di connessione specificati**: se selezionato, il traffico proveniente dai tipi di connessione specificati (ad esempio, sottorete LAN, gateway drop-in, rete ospiti) corrisponderà 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.

3. Fai clic sulla casella centrale in grigio.



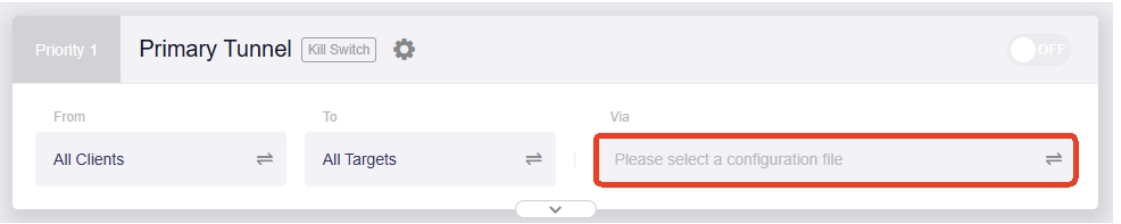
4. Seleziona la destinazione verso la quale verrà instradato il traffico tramite questo tunnel e fai clic su **Applica**.



- **Tutti i target**: se selezionato, il traffico che corrisponde a questa regola verrà instradato verso tutte le destinazioni.
- **Dominio specificato/Elenco IP**: se selezionato, il traffico corrispondente a questa regola verrà instradato al dominio/IP specificato. È necessario inserire manualmente il dominio/IP specificato oppure inserire il collegamento URL di sottoscrizione. La specifica di un dominio principale coprirà tutti i suoi sottodomini.
- **Escludi elenco domini/IP specificati**: se selezionato, il traffico corrispondente a questa regola **NON** verrà instradato al dominio/IP specificato. È necessario inserire manualmente il dominio/IP specificato oppure inserire il collegamento URL di sottoscrizione. La specifica di un dominio principale coprirà tutti i suoi sottodomini.

Nota: se selezioni Sottoscrivi URL, il nome di dominio o l'indirizzo IP nell'URL verrà aggiornato automaticamente ogni giorno. Assicurati di inserire l'URL corretto. Il rilevamento dell'URL verificherà la validità del nome di dominio o dell'indirizzo IP.

5. Fai clic sulla casella disattivata a destra.



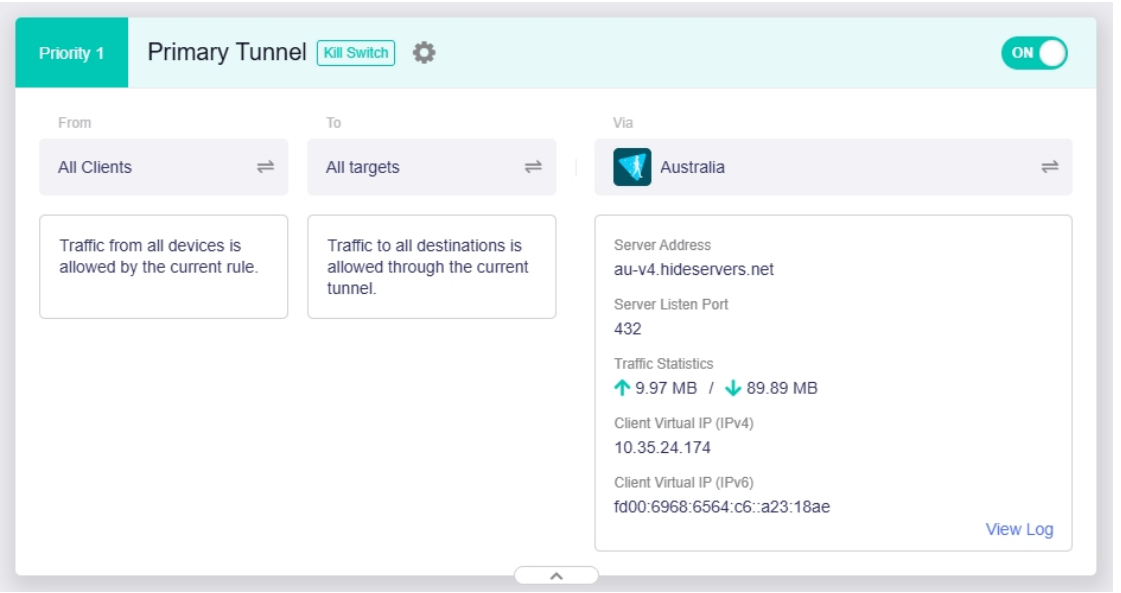
6. Seleziona il metodo di instradamento per questo tunnel: **Usa VPN** o **Non usare VPN**.



- **Usa VPN**: se selezionato, il traffico corrispondente a questa regola verrà instradato alle destinazioni selezionate tramite tunnel VPN. Devi selezionare un file di configurazione VPN per questa regola.
- **Non usare VPN**: se selezionato, il traffico corrispondente a questa regola verrà instradato alle destinazioni selezionate tramite la rete WAN locale anziché VPN.

7. Dopo aver configurato l'origine del traffico, la destinazione e il metodo di instradamento, l'impostazione della regola del tunnel primario è completa. Nell'esempio seguente, la regola del tunnel è: tutti i client connessi a questo router accederanno a Internet tramite

VPN; Il loro traffico verrà instradato attraverso questo tunnel VPN al server australiano e infine uscirà da questo server su Internet.

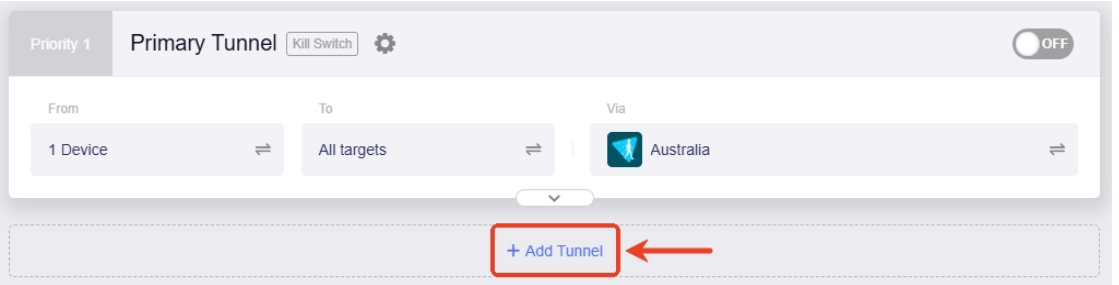


Nota: per sicurezza, vai su Tutto il resto del traffico e Opzioni tunnel per verificare altre impostazioni prima di abilitare questo tunnel.

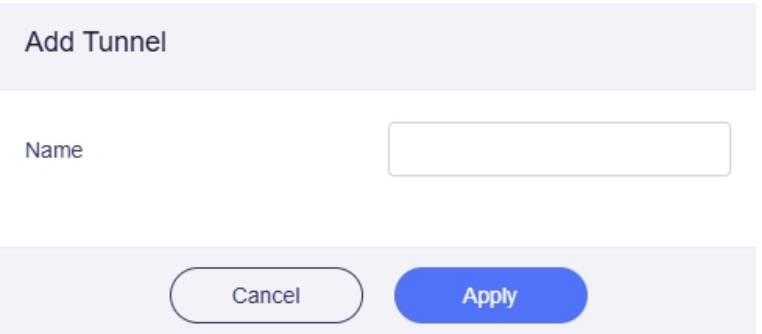
Aggiungi tunnel

Aggiungi tunnel se devi instradare il traffico da dispositivi diversi a destinazioni diverse. Segui i passaggi seguenti per aggiungere un tunnel.

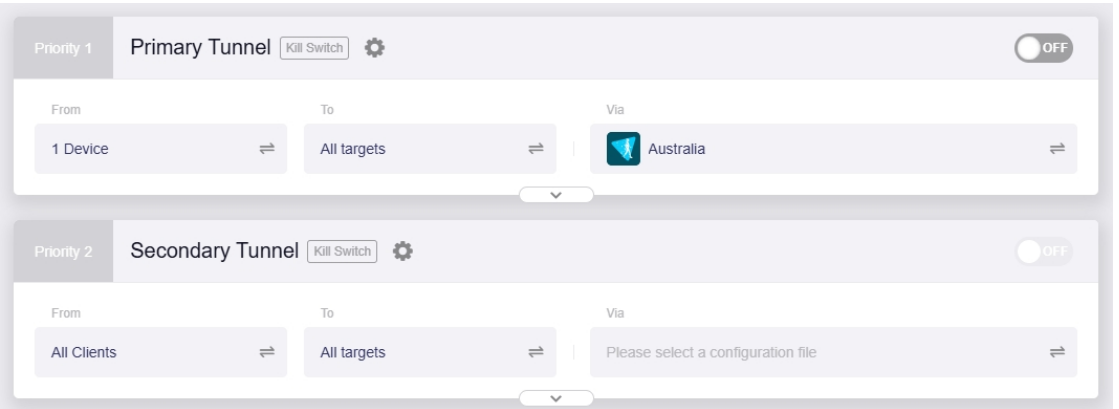
1. Fai clic su **Aggiungi tunnel** sotto il tunnel principale.



2. Dai un nome al tunnel.



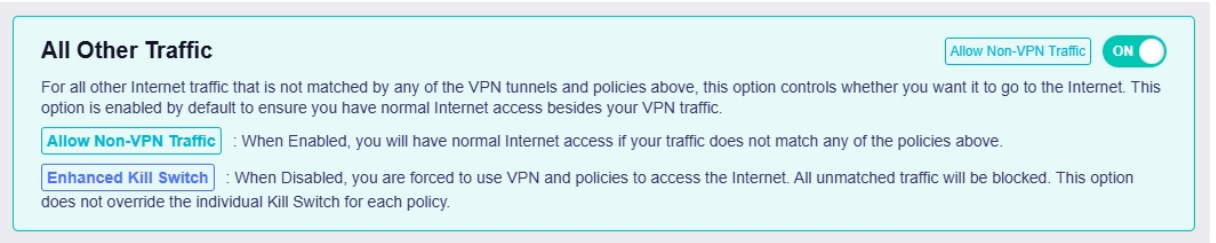
3. Otterrai un altro tunnel sullo Dashboard VPN. È possibile creare fino a tunnel 5 (incluso il tunnel primario preimpostato).



4. Configura le regole del tunnel impostando la sorgente del traffico, le destinazioni e il metodo di instradamento. Una volta terminato, verifica le altre impostazioni in Tutto il resto del traffico e Opzioni tunnel per la sicurezza prima di abilitare i tunnel.

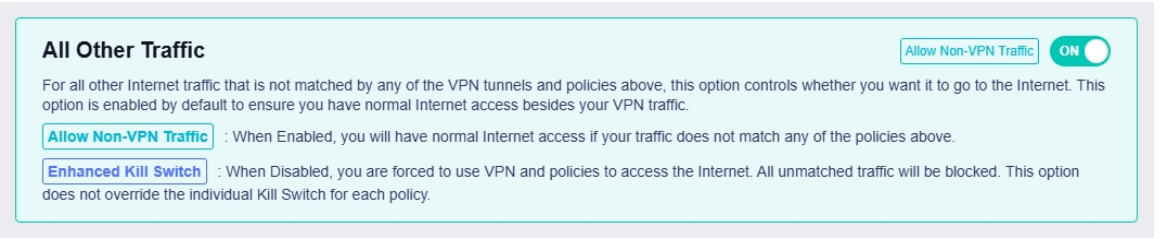
Tutto il resto del traffico

In Modalità delle policy, un tunnel predefinito preattivato viene mostrato nella parte inferiore dello Dashboard VPN.

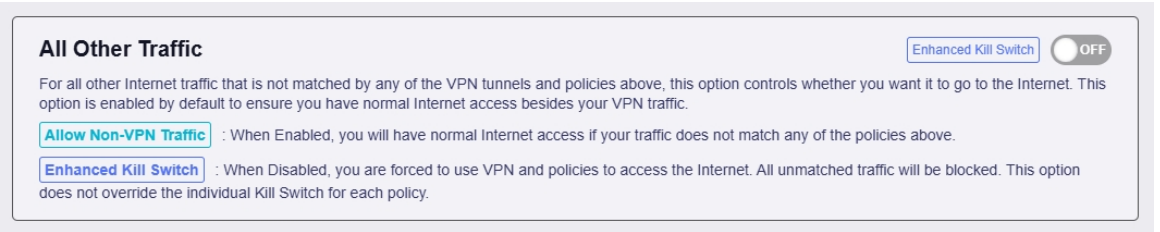


Questo tunnel controlla se il traffico che non corrisponde a nessuno dei gruppi di tunnel VPN sopra indicati può accedere a Internet. È abilitato per impostazione predefinita per garantire il normale accesso a Internet per il traffico non instradato tramite VPN.

- Se abilitato, il traffico senza corrispondenza può comunque accedere a Internet.



- Se disabilitato, solo il traffico instradato tramite VPN può accedere a Internet. Tutto il traffico non VPN e il traffico in failover dalle connessioni VPN verranno bloccati. Questa opzione non sovrascrive il singolo Kill Switch per ciascun tunnel VPN.

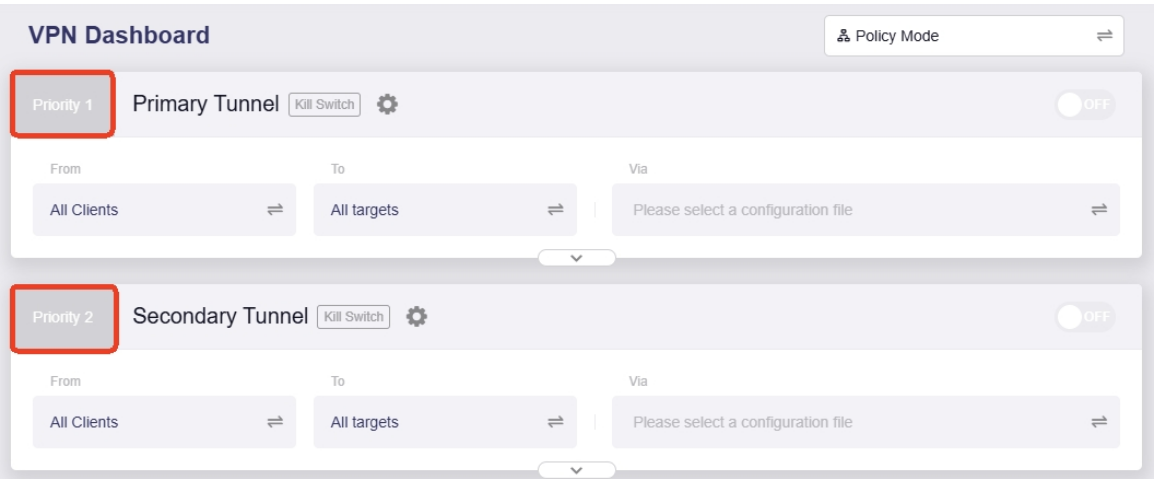


Priorità dei tunnel

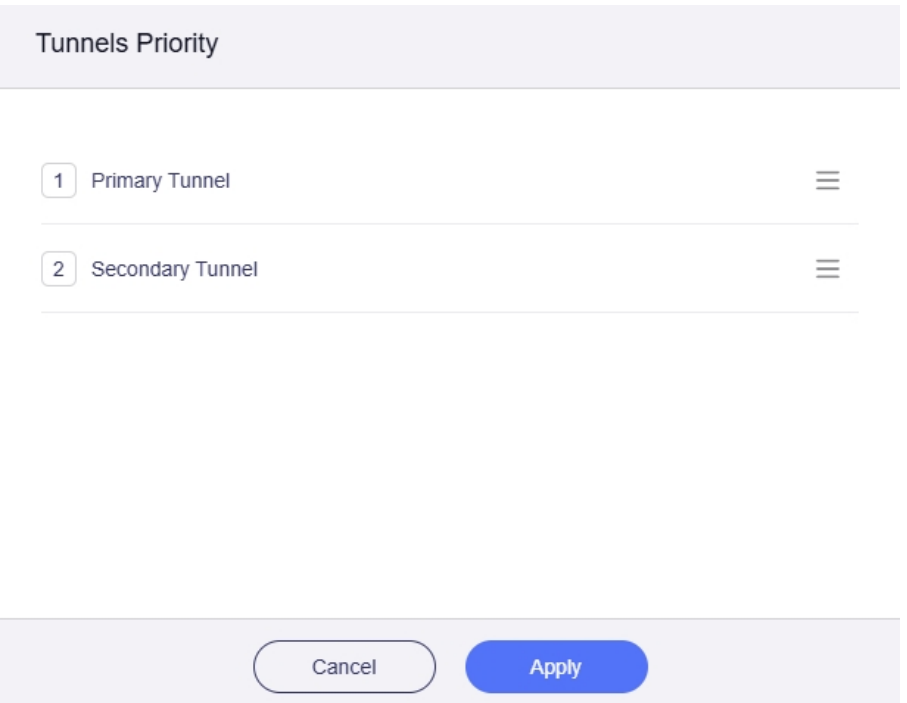
Per impostazione predefinita, il tunnel primario preimpostato ha la massima priorità, seguito da altri tunnel aggiunti manualmente (se presenti), quindi dal tunnel Tutto il resto del traffico preimpostato per garantire la connettività di rete tramite la rete ISP locale (WAN).

Se è necessario modificare la priorità del tunnel, seguire i passaggi seguenti.

1. Fai clic **sull'etichetta** di priorità nell'angolo in alto a sinistra di qualsiasi tunnel (ad esempio, Priorità 1 / Priorità 2).



2. Nella finestra pop-up, fai clic e tieni premuta l'icona a tre linee a destra per riordinare il tunnel, quindi fai clic su **Applica**.

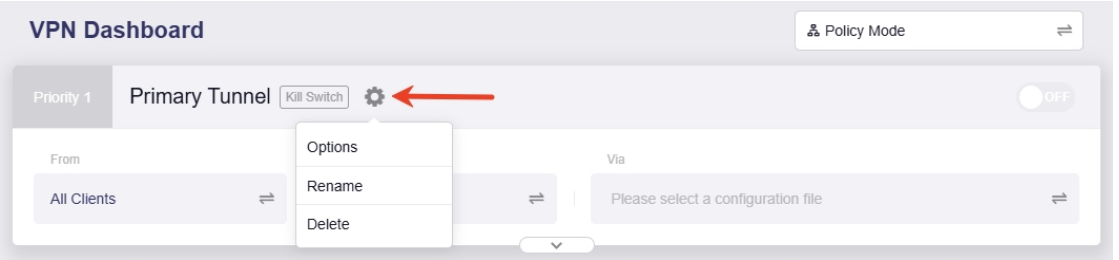


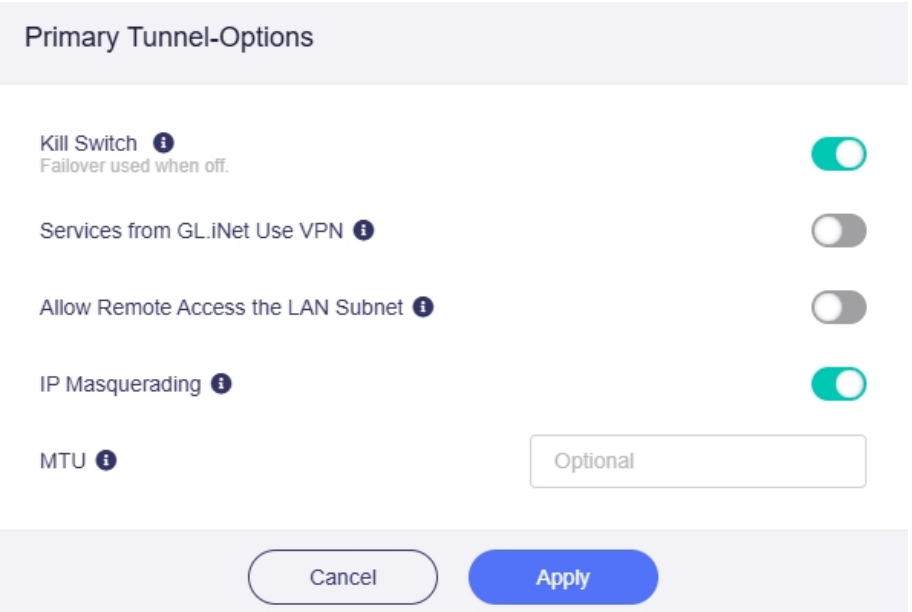
Quando sono abilitati più tunnel, il router instraderà il traffico nel seguente ordine:

1. Il traffico tenterà innanzitutto di soddisfare la regola del tunnel con la priorità più alta. Se abbinato, verrà instradato attraverso quel tunnel; in caso contrario, proverà il tunnel con priorità successivo e così via, finché non corrisponderà al tunnel "Tutto il resto del traffico".
2. Se un tunnel VPN si disconnette inaspettatamente, il sistema determinerà se eseguire il failover del traffico verso il tunnel con priorità successivo in base al fatto che **Kill Switch** di questo tunnel sia abilitato.
    - Quando Kill Switch è abilitato, il traffico verrà bloccato e non verrà eseguito il failover al tunnel prioritario successivo.
    - Quando Kill Switch è disabilitato, il traffico eseguirà il failover al tunnel con priorità successiva e tenterà di soddisfare le regole del tunnel.
3. Il tunnel **Tutto il resto del traffico** è abilitato per impostazione predefinita per garantire che il traffico che non corrisponde ai tunnel VPN possa comunque accedere a Internet.
    - Se abilitato, instrada il traffico senza corrispondenza o di failover attraverso la WAN locale.
    - Se disabilitato, rafforza lo Kill Switch e blocca il regolare accesso a Internet per prevenire perdite di IP.

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 accanto al nome di un tunnel.





- **Kill Switch**: se abilitato, il traffico corrispondente a questo tunnel VPN verrà bloccato quando la connessione fallisce inaspettatamente; in caso contrario, eseguirà il failover sui successivi tunnel prioritari o WAN.
- **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 LAN Sottorete**: se abilitato, sarà consentito accesso remoto a questo router (IP tunnel) e ai dispositivi LAN tramite VPN. Richiede che il server VPN pubblicizzi un percorso di ritorno alla sottorete LAN di questo router.

- **Masquerading IP**: se abilitato, gli IP di origine della LAN client verranno riscritti nell'IP del tunnel VPN del router. Disabilitato solo per configurazioni da sito a sito in cui il peer remoto conosce le sottoreti LAN.
- **MTU**: lo MTU impostato per il tunnel sovrascriverà l'elemento MTU nel file di configurazione.

Capitolo 10

Configurazione del server VPN

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

10.1 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.

10.1.1 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:

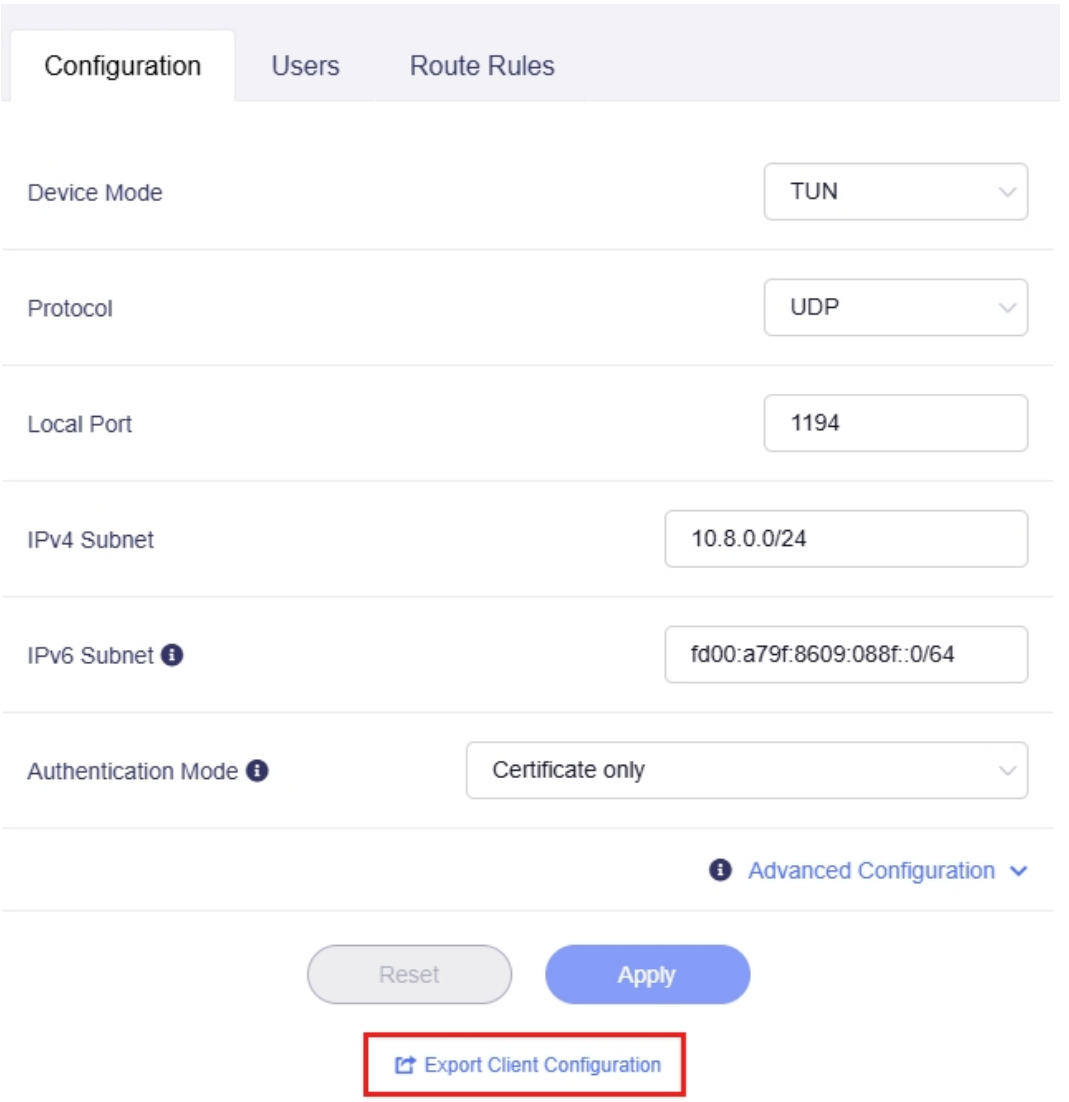
   - Se disponi di un router primario a monte del tuo router GL.iNet, accedi ad esso e verifica che abbia un indirizzo IP pubblico assegnato dal tuo ISP.
   - Chiedi al tuo ISP un indirizzo IP pubblico. Ciò potrebbe comportare un costo aggiuntivo.
   - Se i due metodi precedenti non funzionano (ad esempio,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

10.1.2 Procedura di configurazione

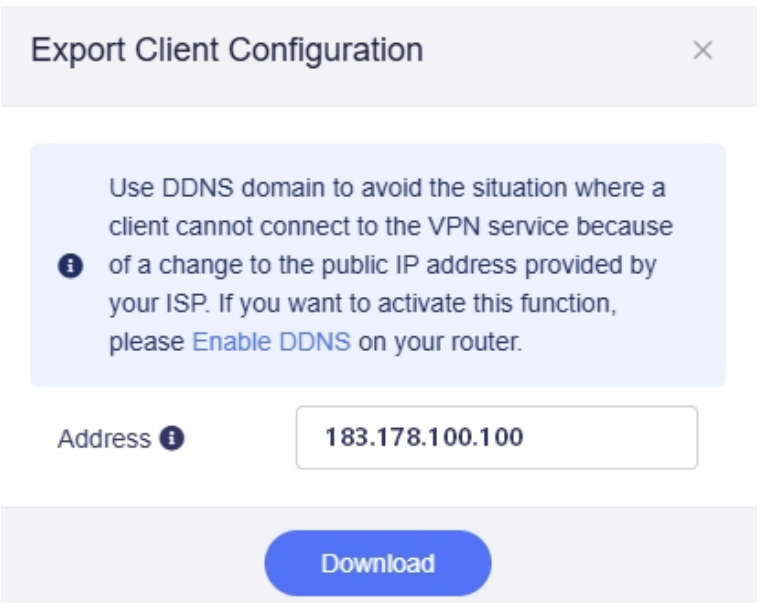
1. Accedi al pannello di amministrazione web del router, vai a **VPN** > **Server OpenVPN**, quindi fai clic su **Genera configurazione** (solo per la configurazione iniziale del server VPN).
2. Applica la configurazione.
   La configurazione predefinita funziona nella maggior parte dei casi. Fai clic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



- **Modalità dispositivo**: TAP-S2S o Tun. Vedi qui per le differenze.
- **Protocollo**: UDP o TCP. Vedi qui per le differenze.

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

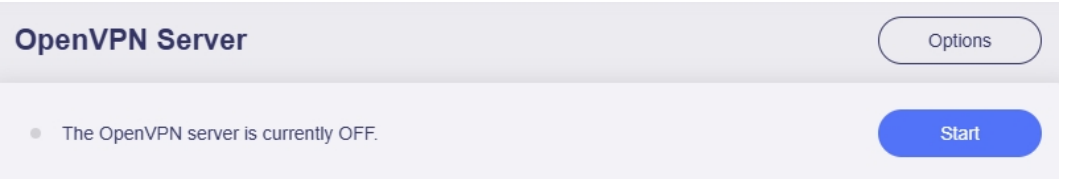
3. Esporta configurazione client.
   Dopo aver fatto clic su **Esporta configurazione client** nella parte inferiore della scheda Configurazione (o dopo aver applicato la configurazione modificata), verrà visualizzata una finestra come segue. Fai clic su **Scarica** per esportare la configurazione.



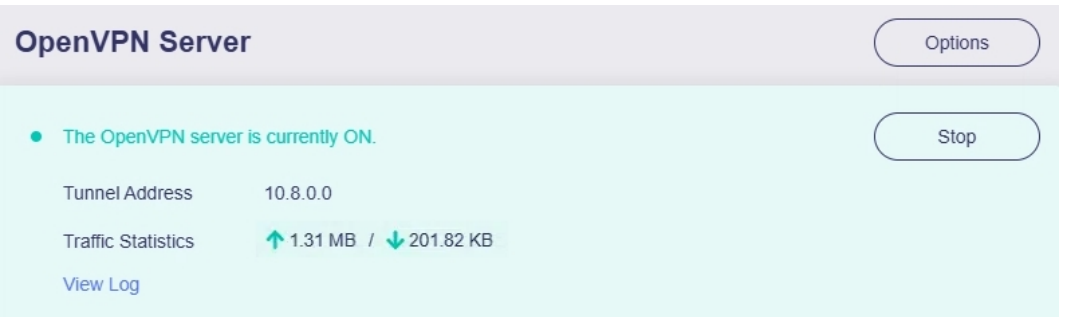
Suggerimenti:

- 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.



10.1.3 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.

10.2 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.

10.2.1 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.

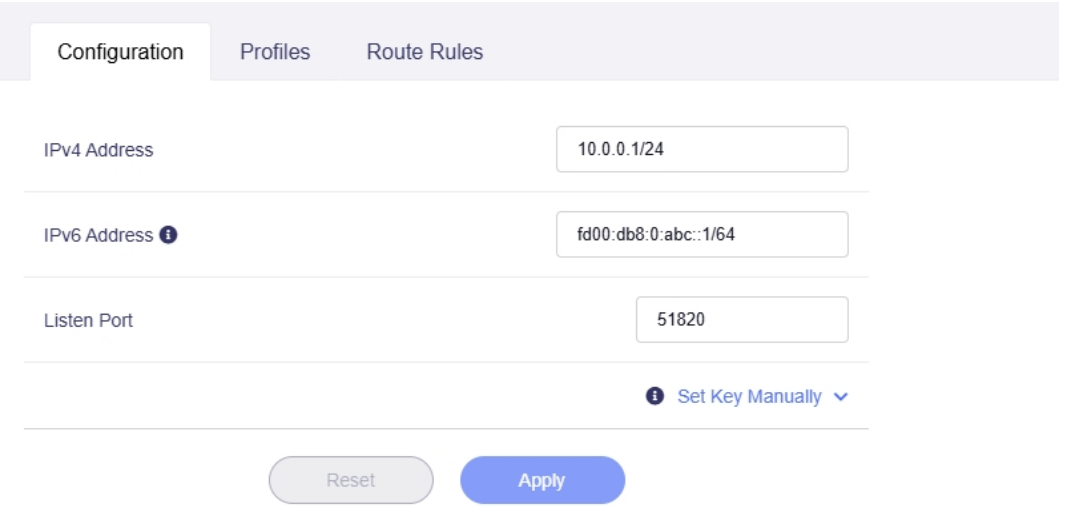
2. **Conferma se è richiesto il port forwarding**

   - 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.

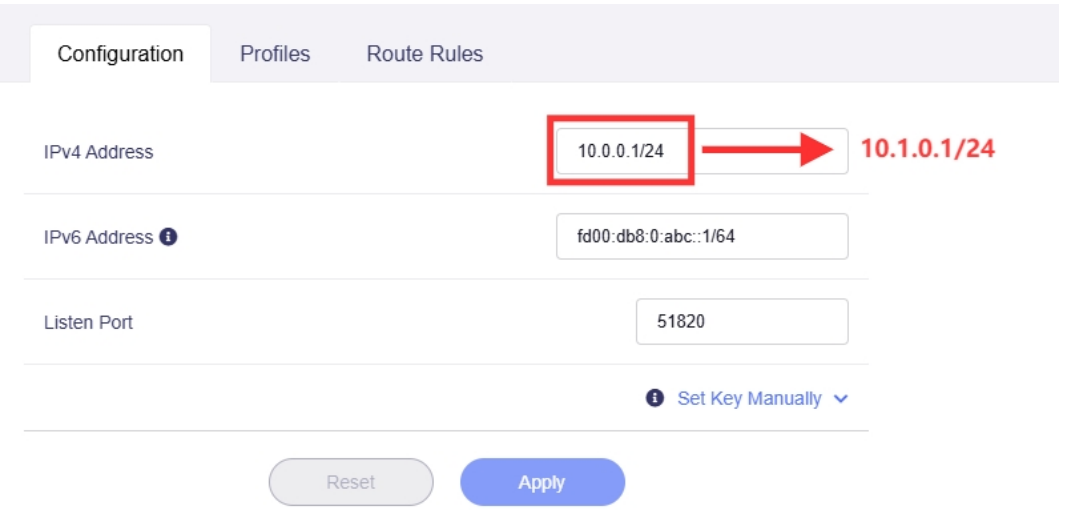
10.2.2 Procedura di configurazione

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.

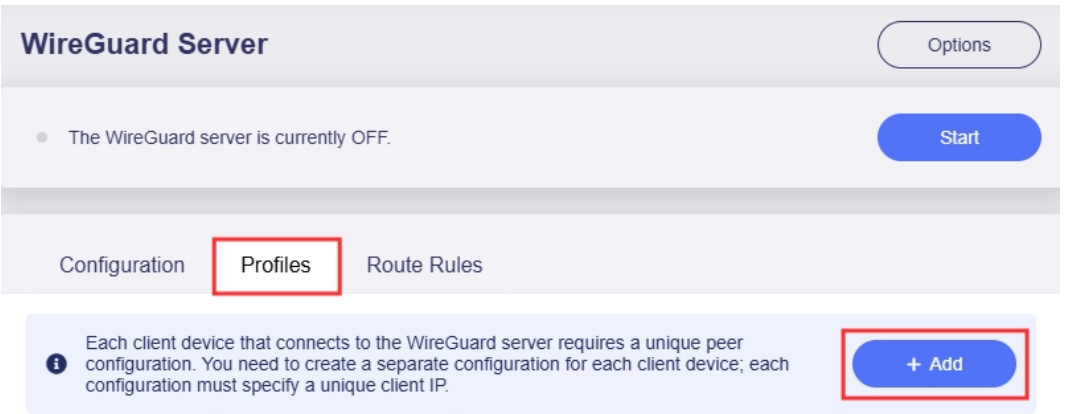


   Se l'indirizzo IPv4 è in conflitto con il gateway del router upstream, modifica l'indirizzo IPv4 con un altro (ad esempio, **10.1.0.1/24**) e fai clic su **Applica**. Assicurati che la notazione CIDR "/24" sia inclusa per evitare problemi di connettività.

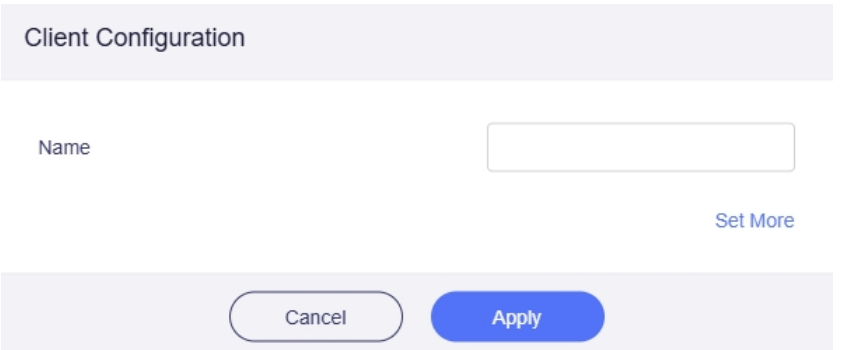


3. Aggiungi un profilo.

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.



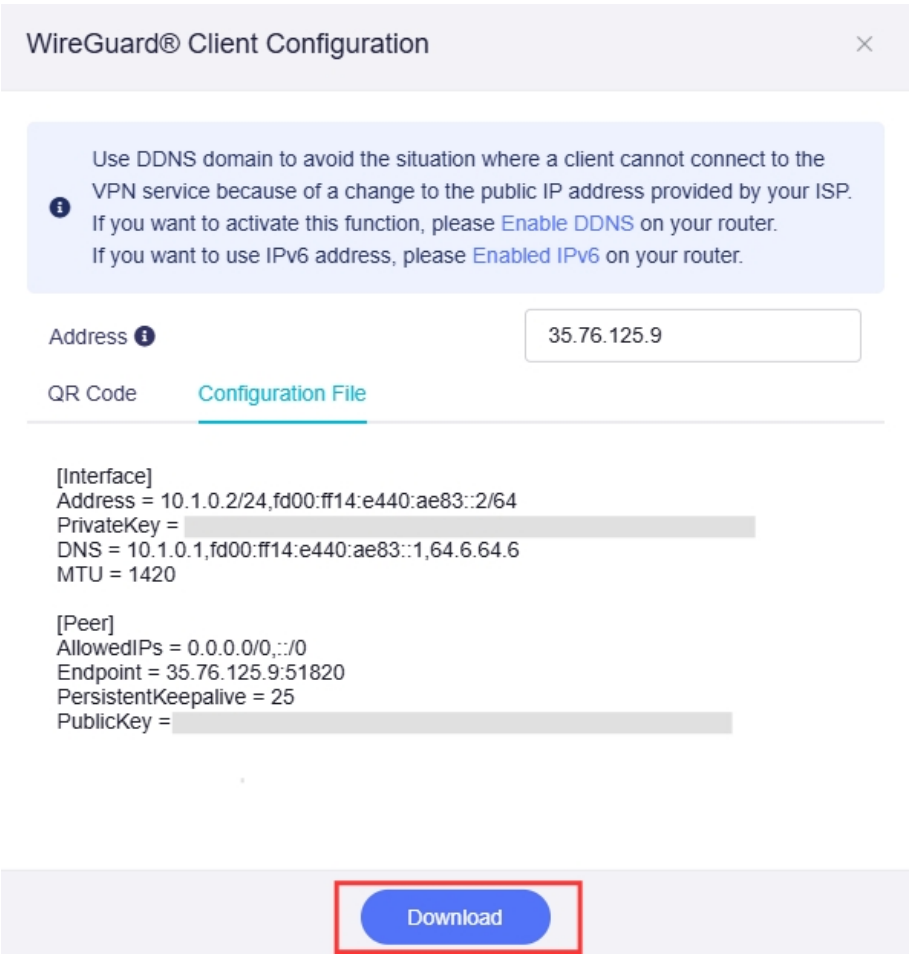
Suggerimento: se desideri accedere ai dispositivi LAN del client WireGuard dal tuo server WireGuard, passa alla scheda **Regole di routing** per configurare le regole di routing. Vedi qui per i dettagli.

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.

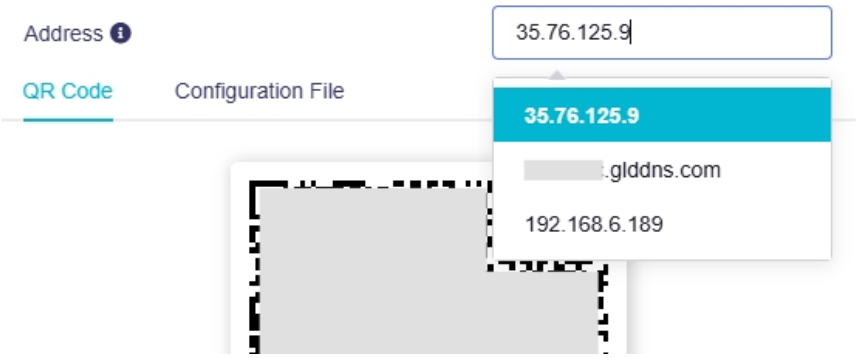
   - **Codice QR**: adatto per dispositivi (ad esempio smartphone, tablet, laptop) con l'app WireGuard installata. Se desideri impostare un dispositivo specifico come client WireGuard, apri semplicemente l'app WireGuard e scansiona il codice QR per importare un file di configurazione.
   - **Testo normale**: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



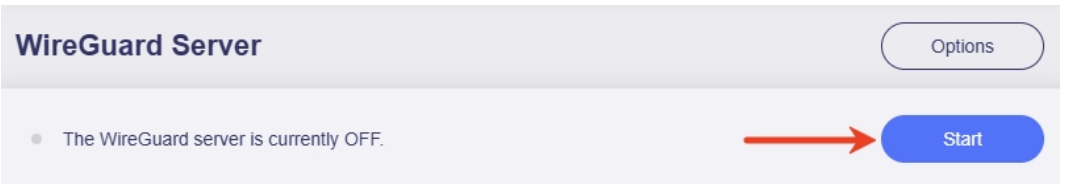
Suggerimenti:

- 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.

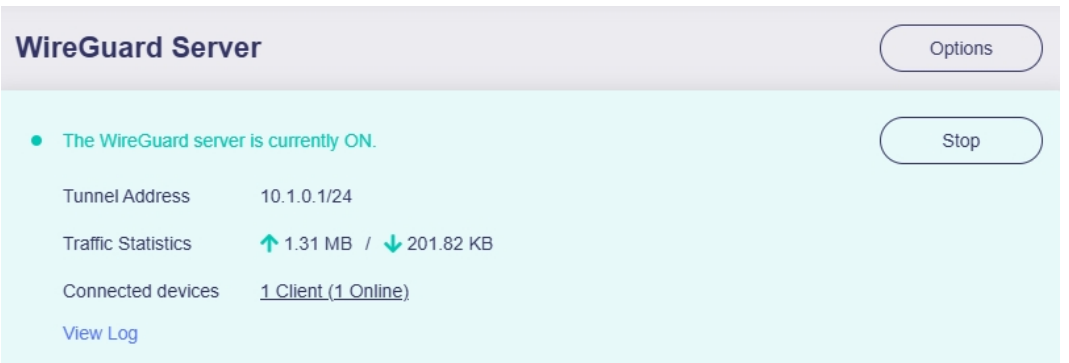


5. Avvia il server WireGuard.

   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.



10.2.3 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 11

Configurazione del client VPN

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

11.1 Configurazione del client OpenVPN

11.1.1 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.

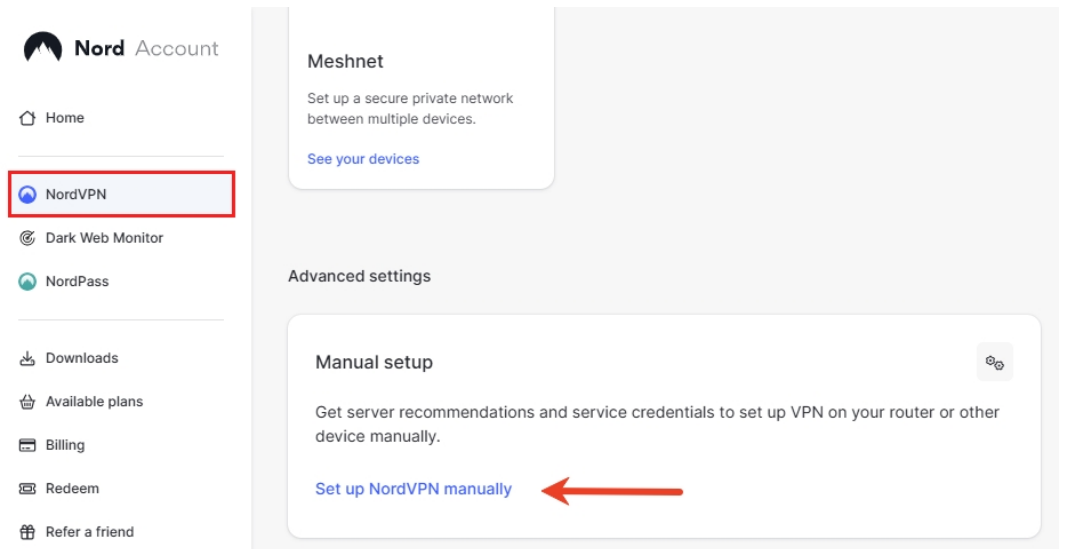
Successivamente, visita il sito Web ufficiale del fornitore di servizi VPN a cui sei iscritto e ottieni le credenziali del servizio o il file di configurazione. Se non sai come ottenere il file di configurazione, fai riferimento a questo collegamento o contatta il loro supporto.

11.1.2 Configurazione di NordVPN

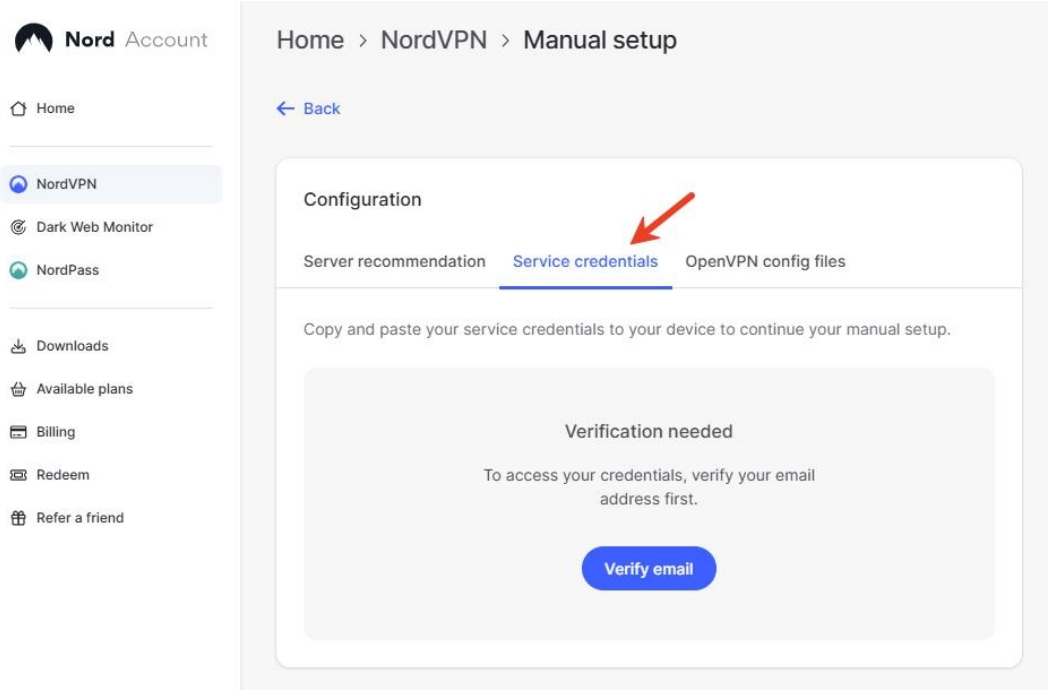
NordVPN è integrato in GL.iNet pannello di amministrazione web. Puoi acquisire file di configurazione per tutti i server NordVPN inserendo le credenziali del tuo account (ottenute dalla dashboard NordVPN) nell'app mobile pannello di amministrazione web o GL.iNet del router, eliminando la necessità di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

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

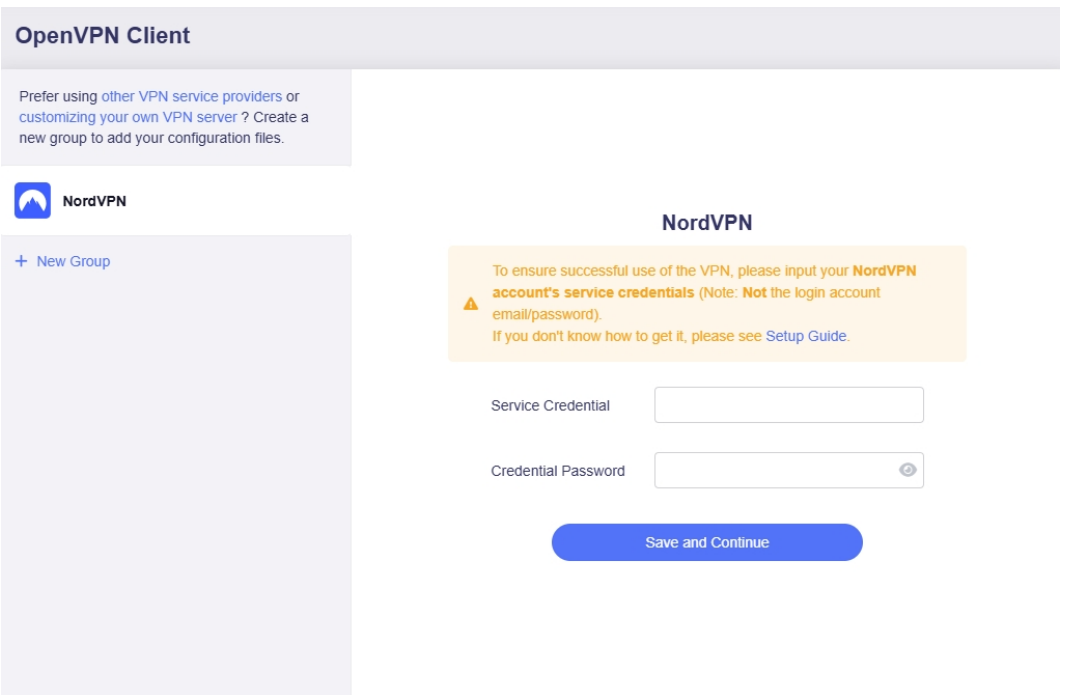
1. Accedi al tuo account web NordVPN qui.
2. Nella Nord Dashboard, fai clic su **NordVPN**, quindi su **Configura NordVPN manualmente**.



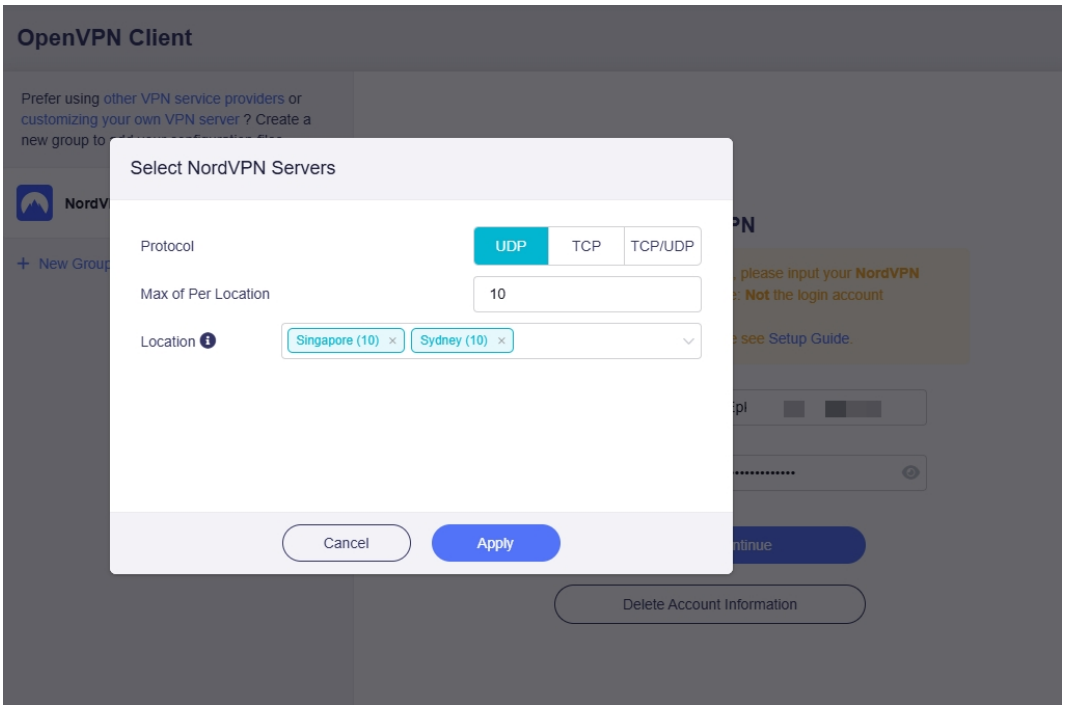
Troverai le **credenziali del servizio**. Copiali per un uso successivo.



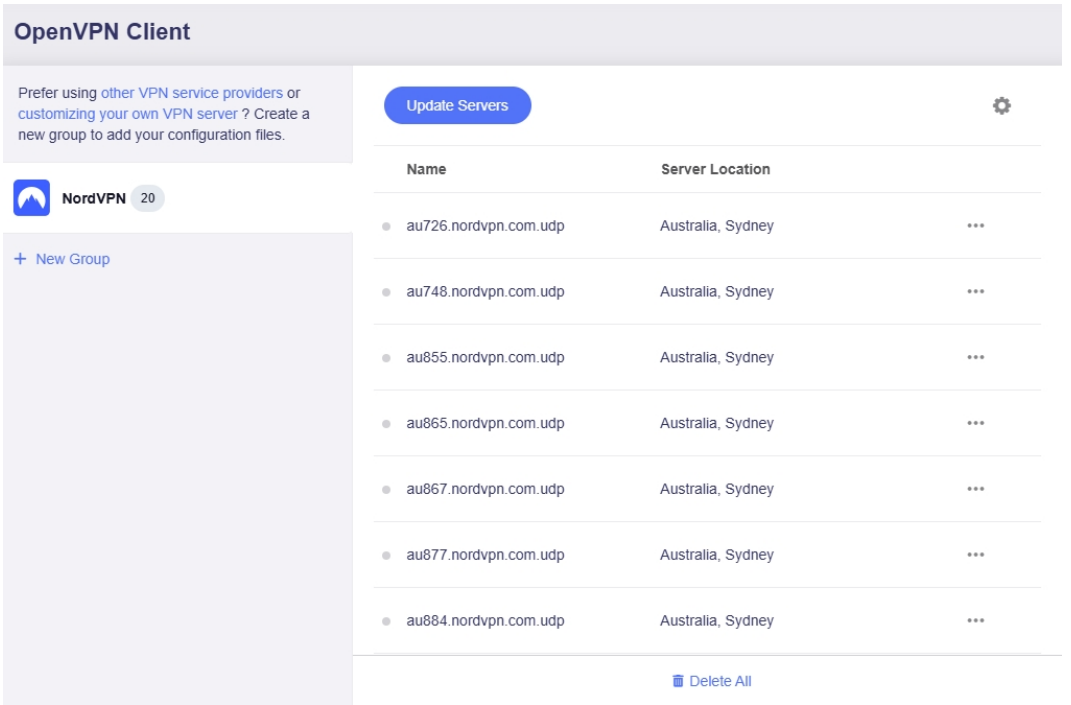
3. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client OpenVPN** > **NordVPN**. Inserisci le credenziali del servizio (Nota: NON è l'e-mail/password dell'account di accesso), quindi fai clic su **Salva e continua**.



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

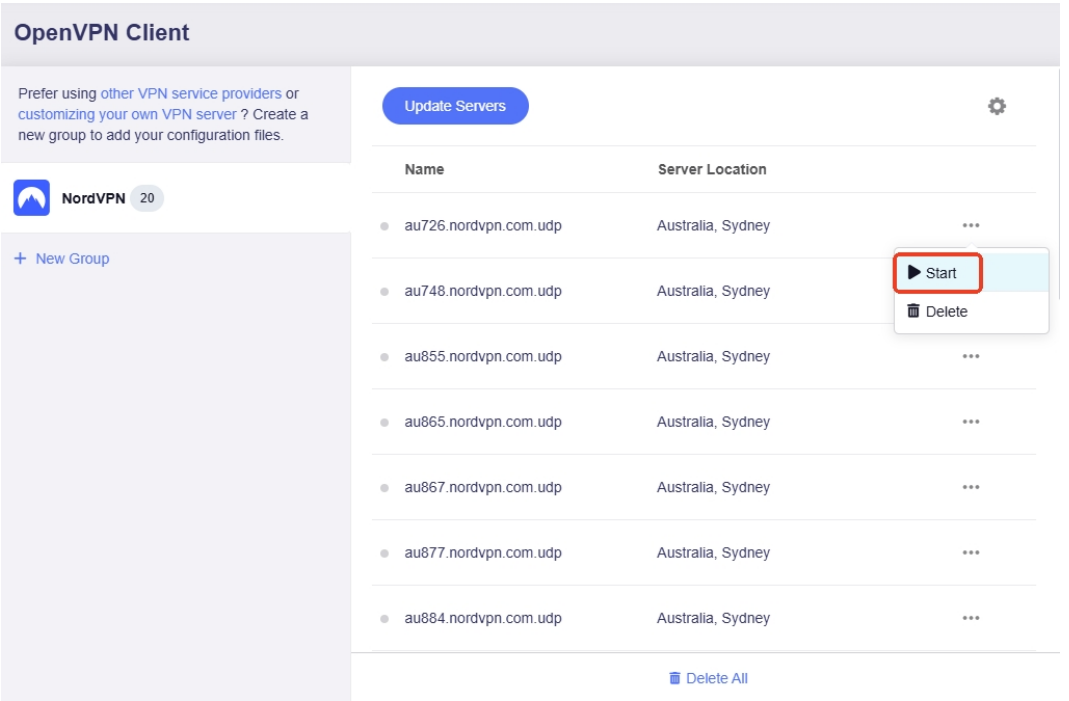


Scaricherà i file di configurazione.

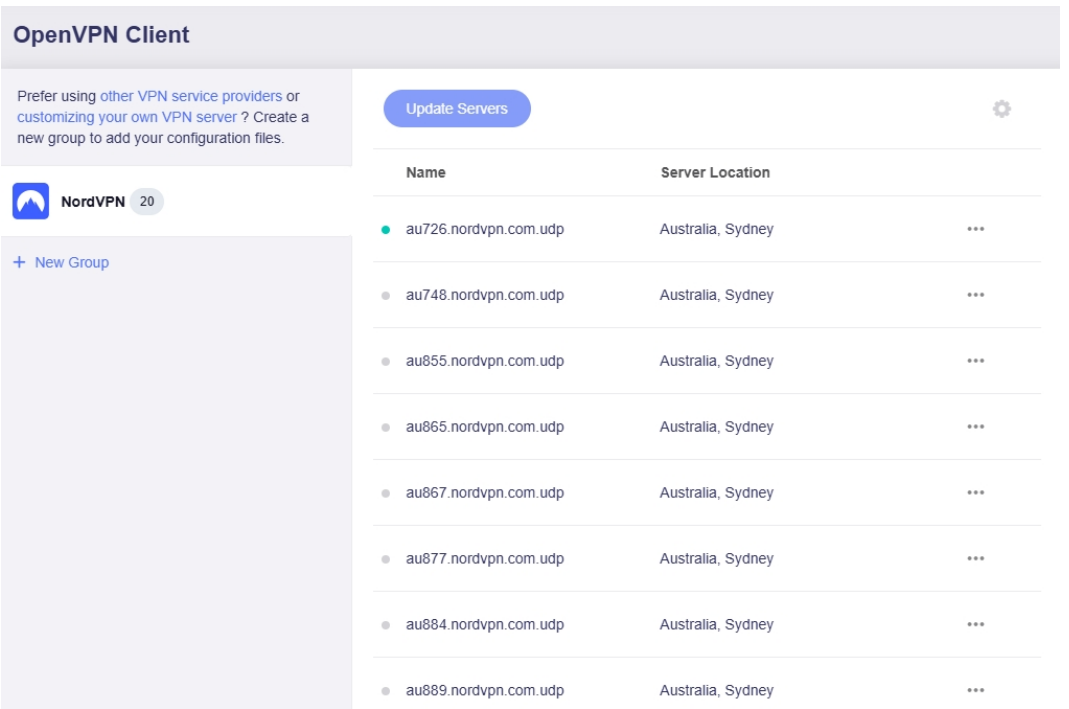


5. Avvia una connessione.

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



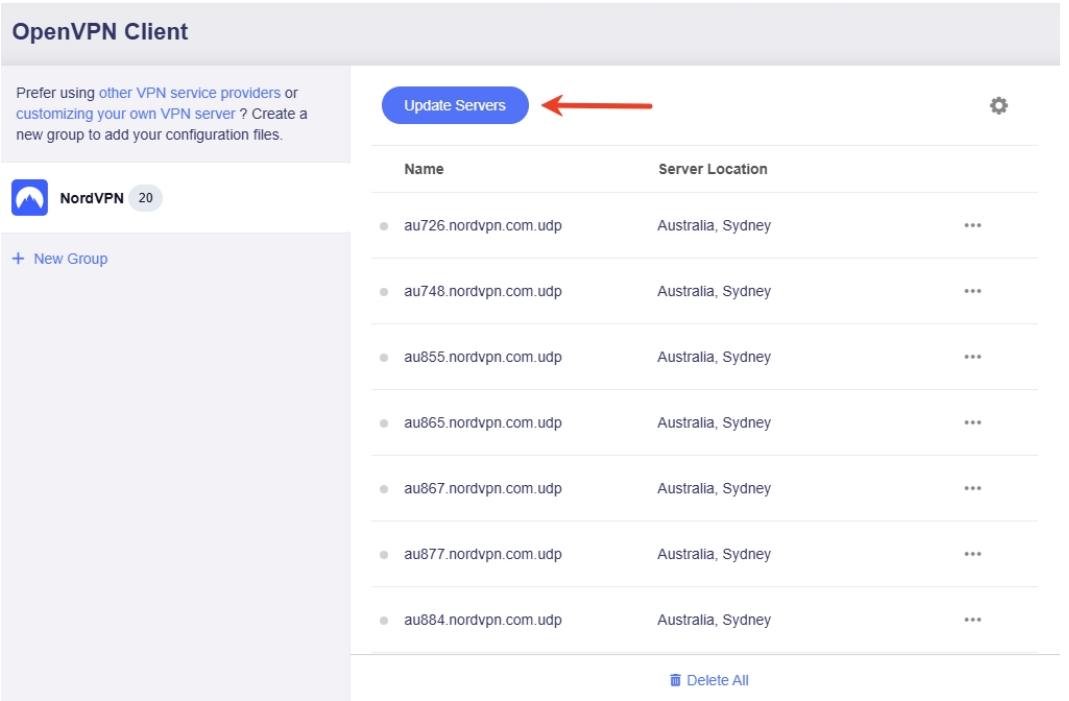
6. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

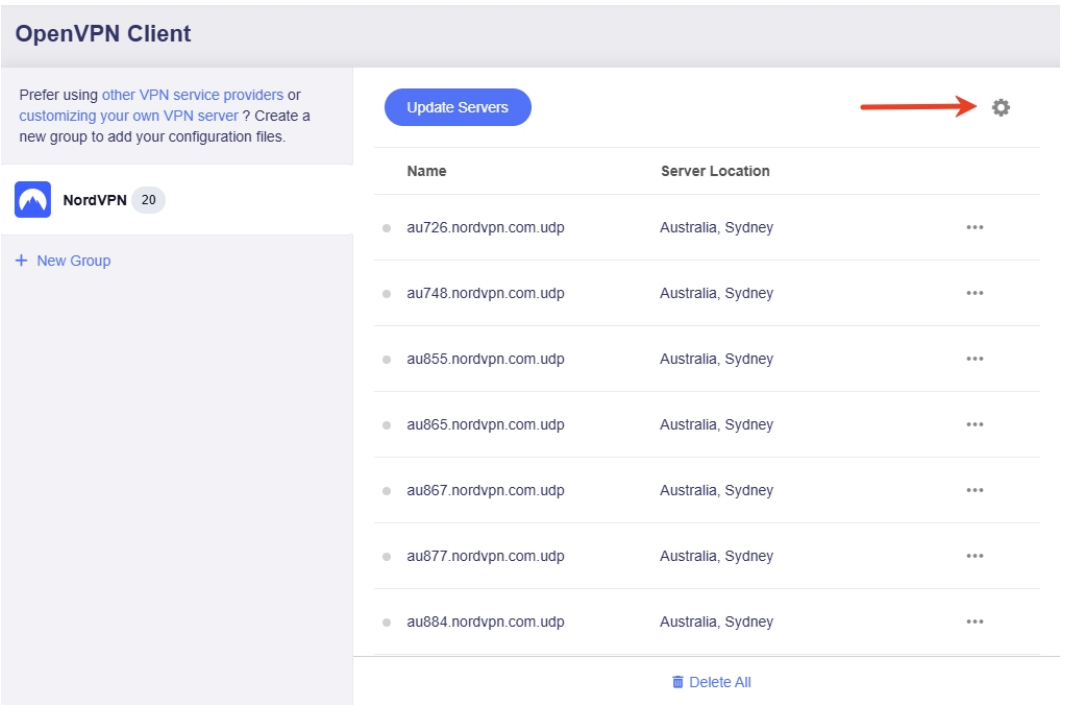
7. Aggiorna server.

   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.



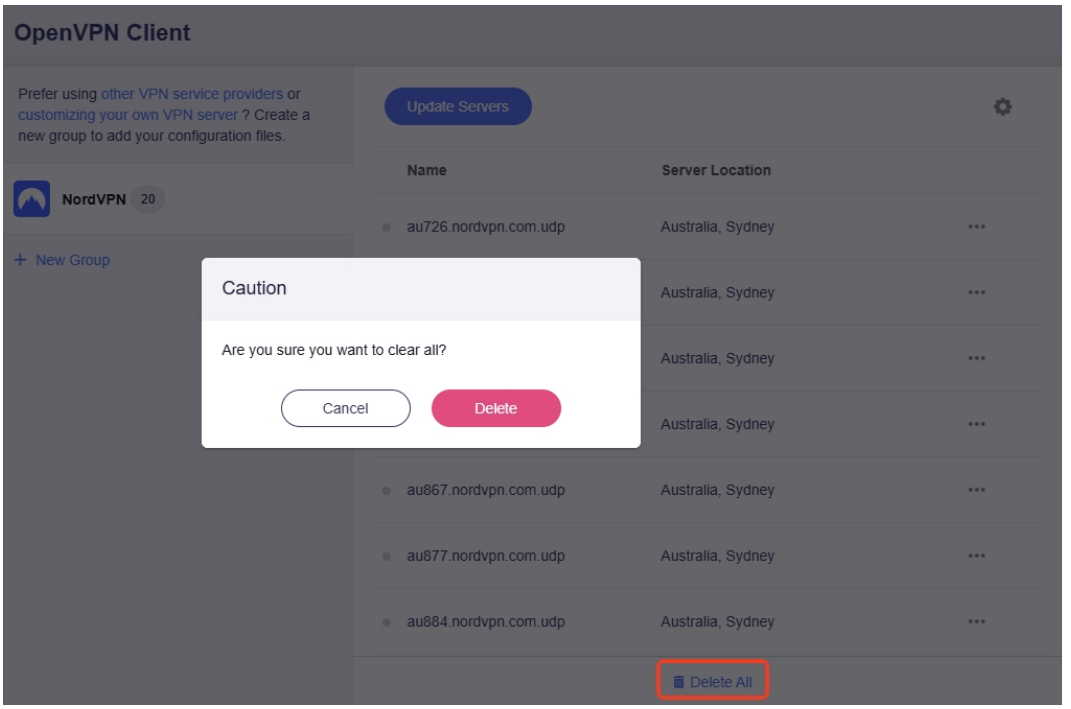
8. Modifica credenziali.

   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.

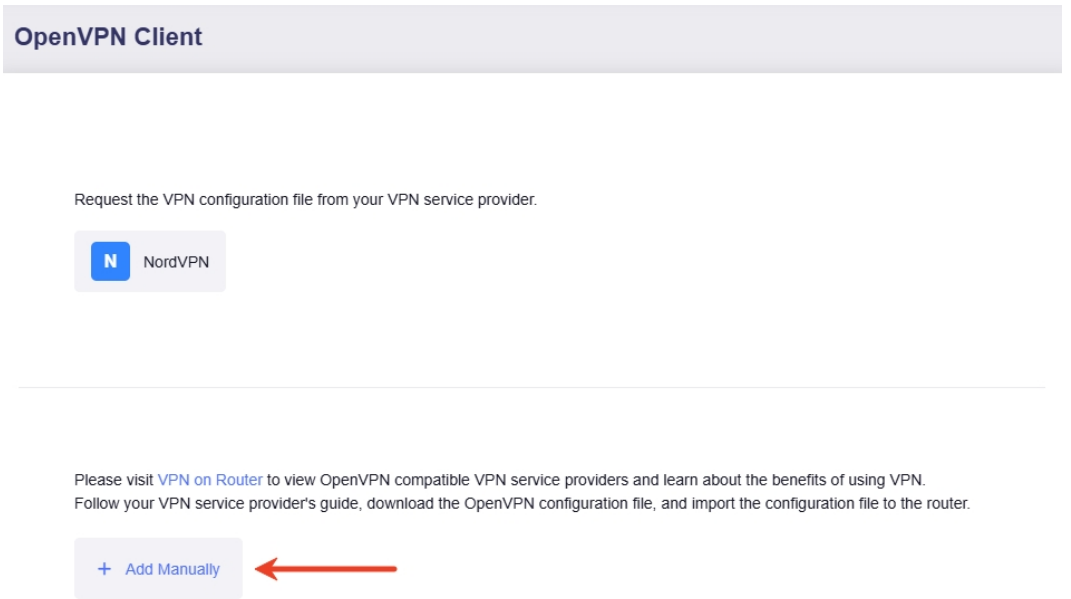

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
+ New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp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

11.1.3 Configurazione manuale del client OpenVPN (altri provider)

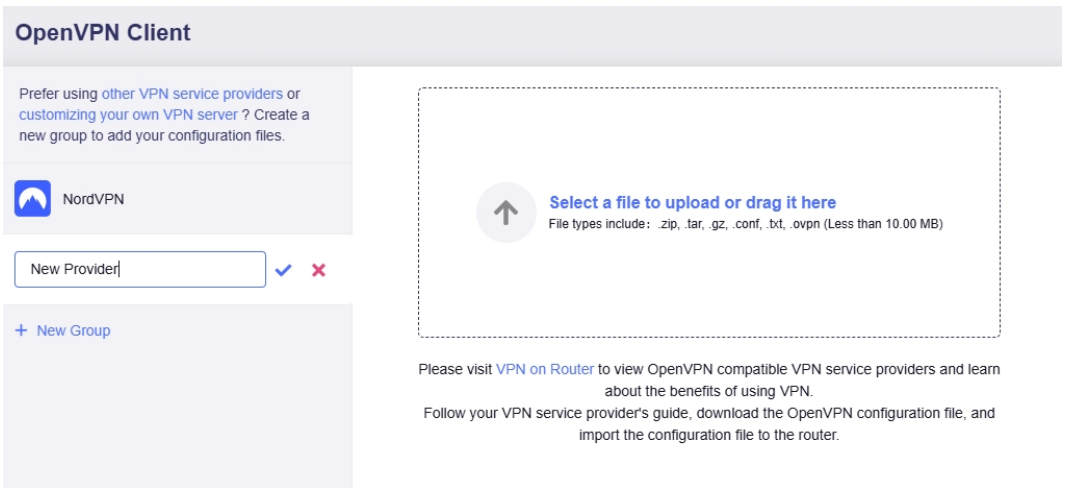
Se il tuo fornitore di servizi OpenVPN non è integrato nel nostro pannello di amministrazione, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare un client OpenVPN.

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

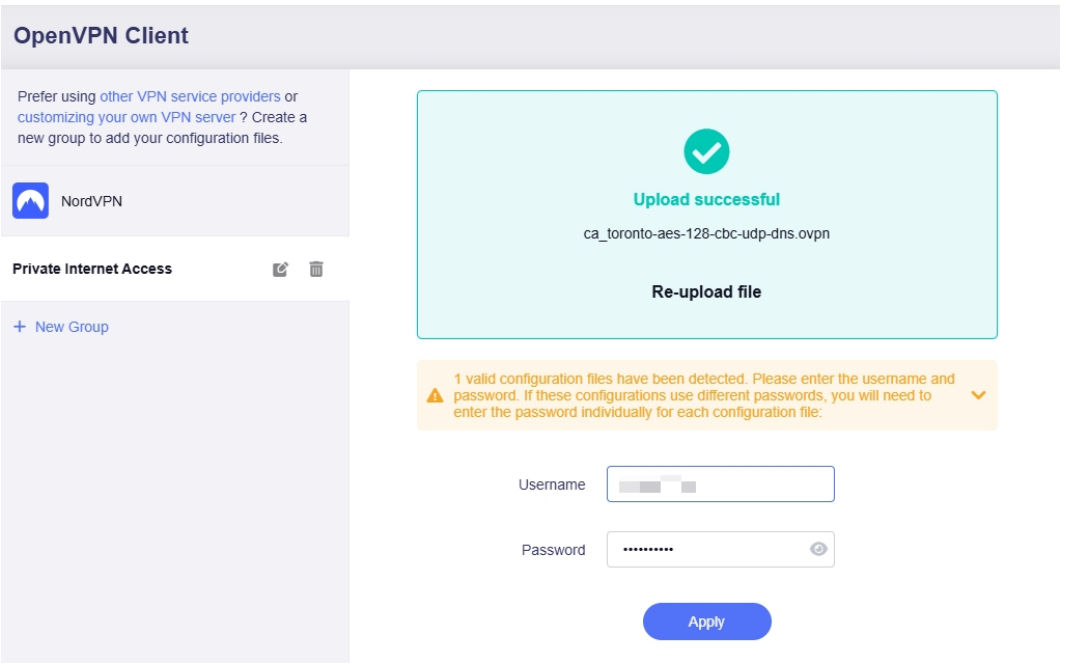
1. Scarica un file di configurazione dal sito Web ufficiale di Private Internet Access.
2. Accedi al pannello di amministrazione web del tuo router, vai a **VPN** > **Client OpenVPN** e fai clic su **Aggiungi manualmente**.



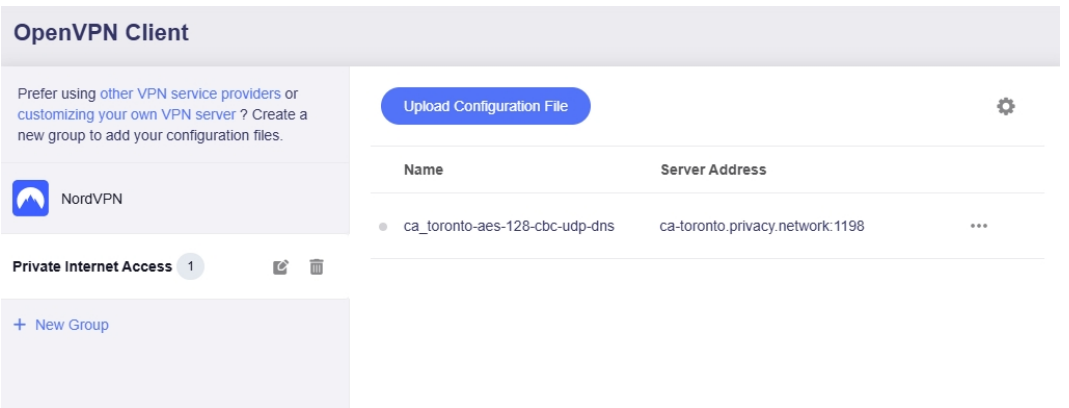
3. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.



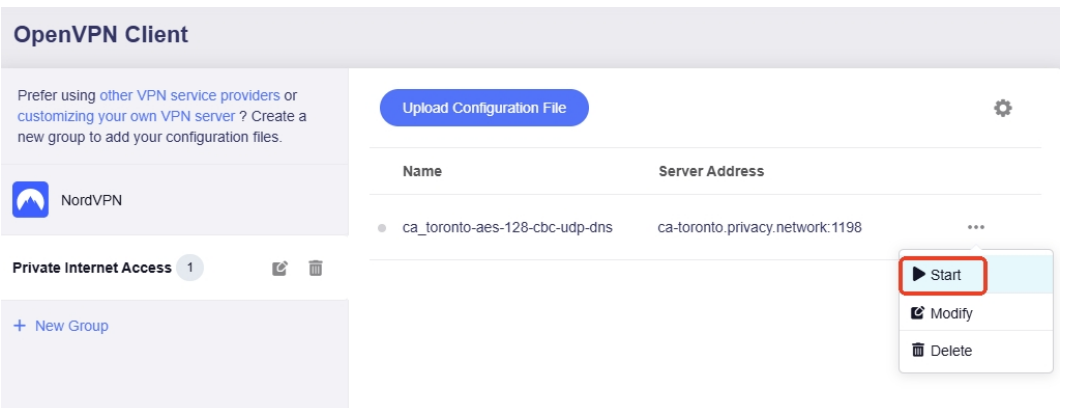
4. Carica il tuo file di configurazione OpenVPN. Inserisci le credenziali, se richieste, quindi fai clic su **Applica**.



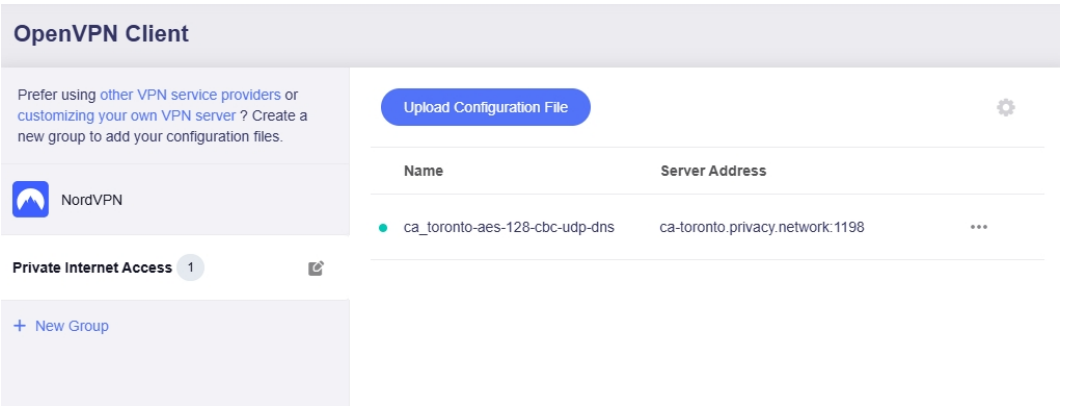
Vedrai il file di configurazione caricato.



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**.

11.2 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.

11.2.1 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.

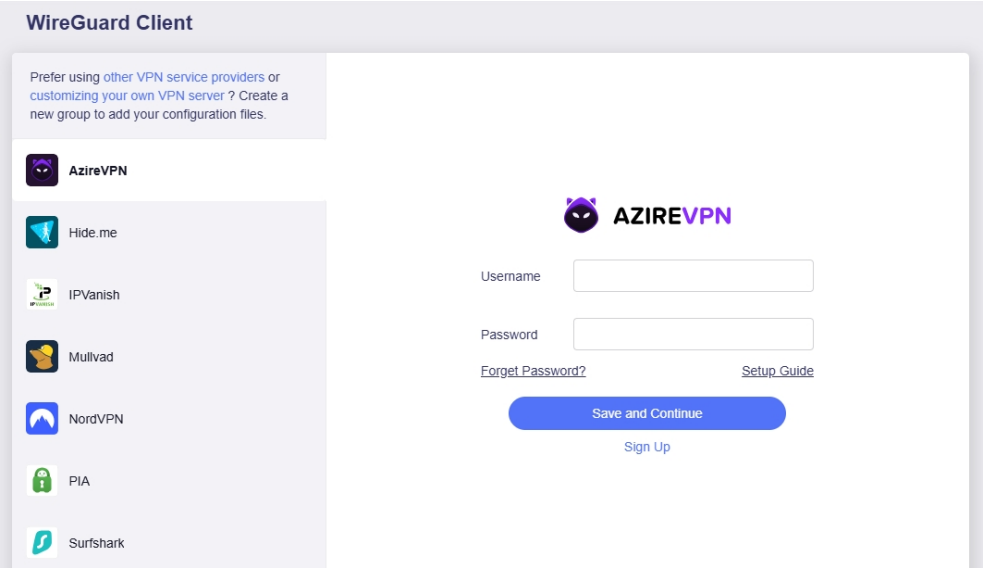
Successivamente, seleziona il fornitore di servizi WireGuard corrispondente di seguito per individuare rapidamente le istruzioni dettagliate.

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

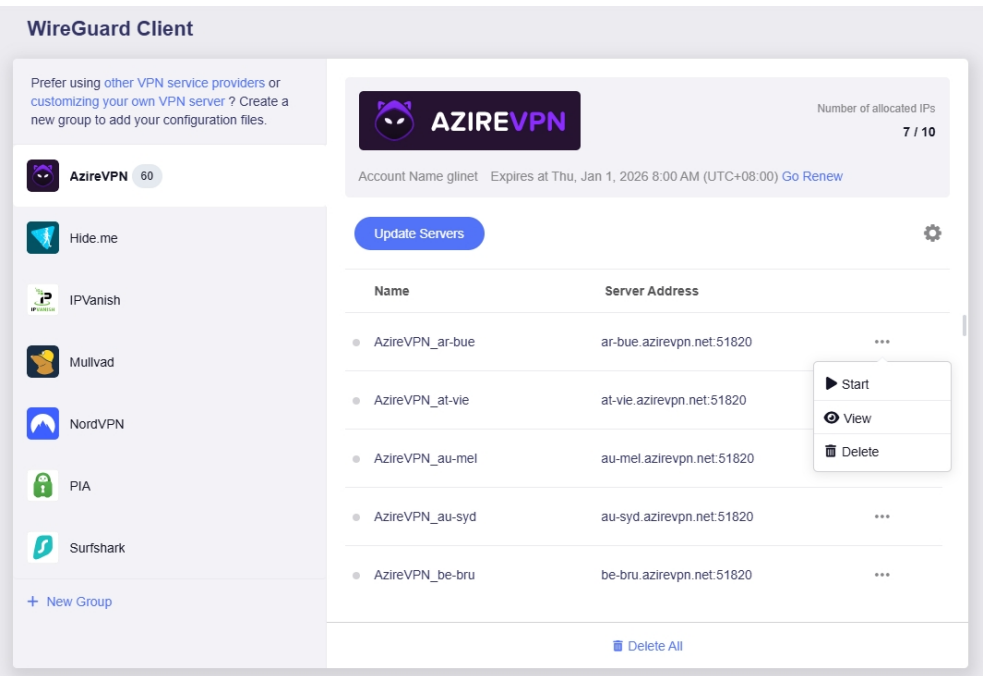
11.2.2 Configurazione di AzireVPN

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

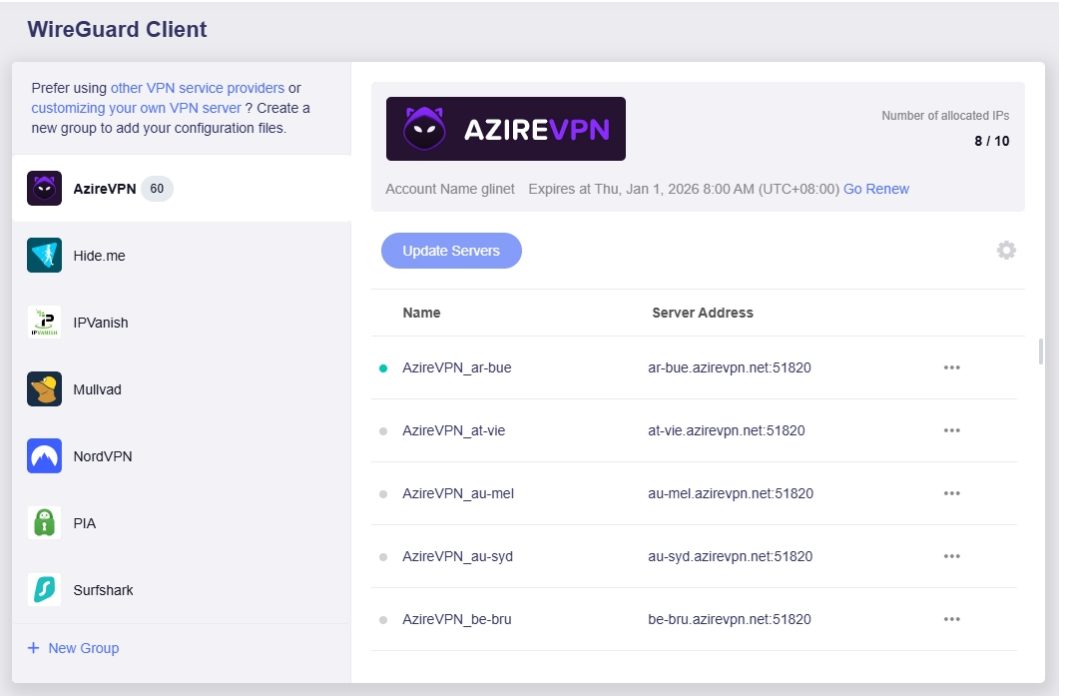
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **AzireVPN**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



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



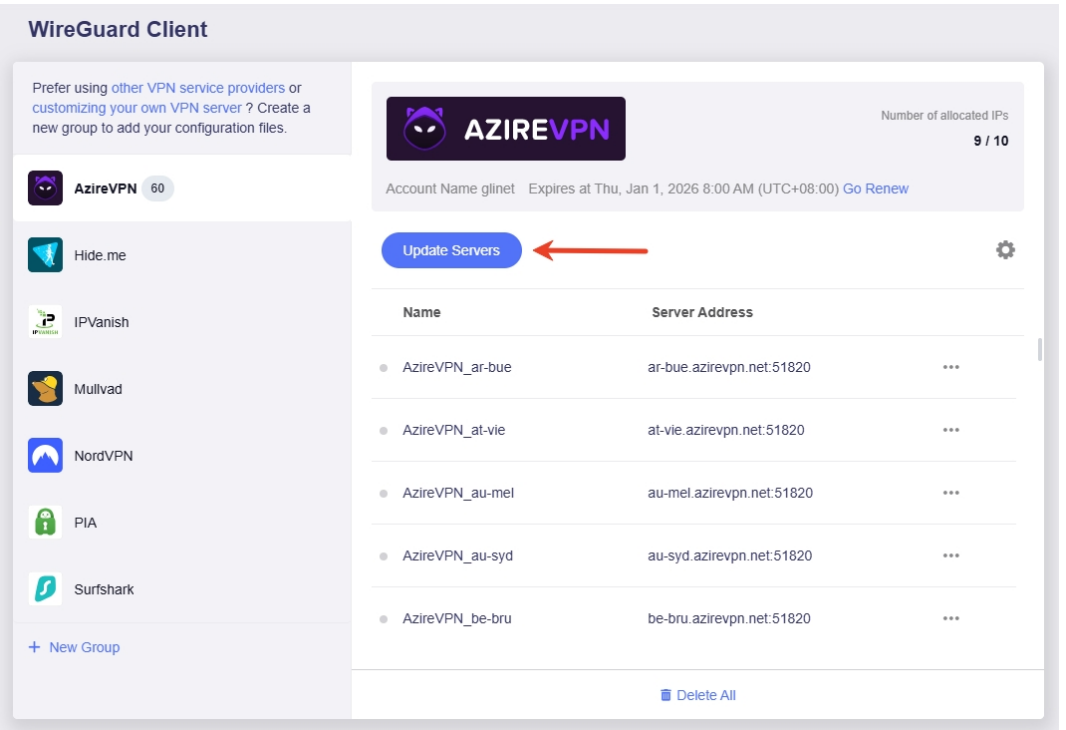
4. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

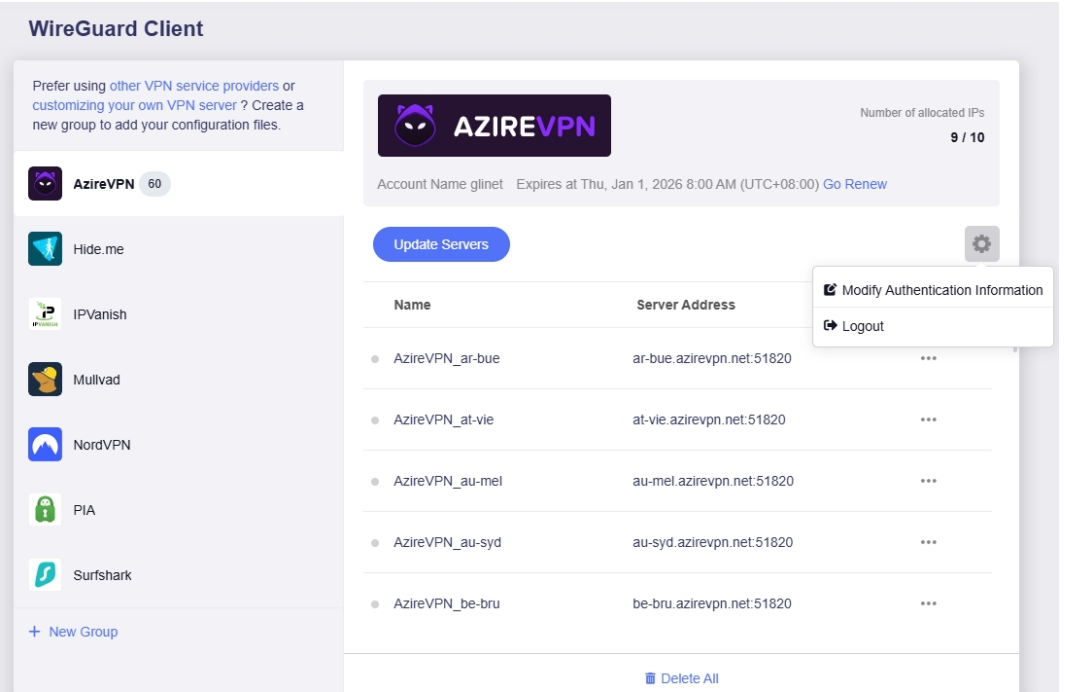
5. Aggiorna server.

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.



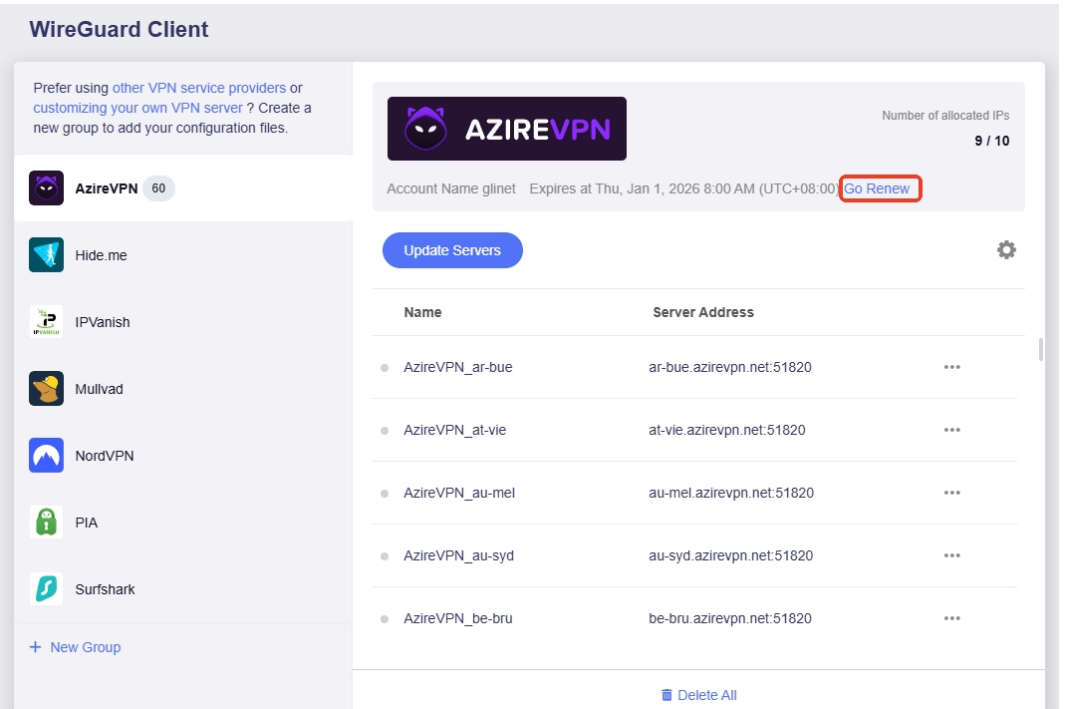
6. Modifica credenziali o esci.

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



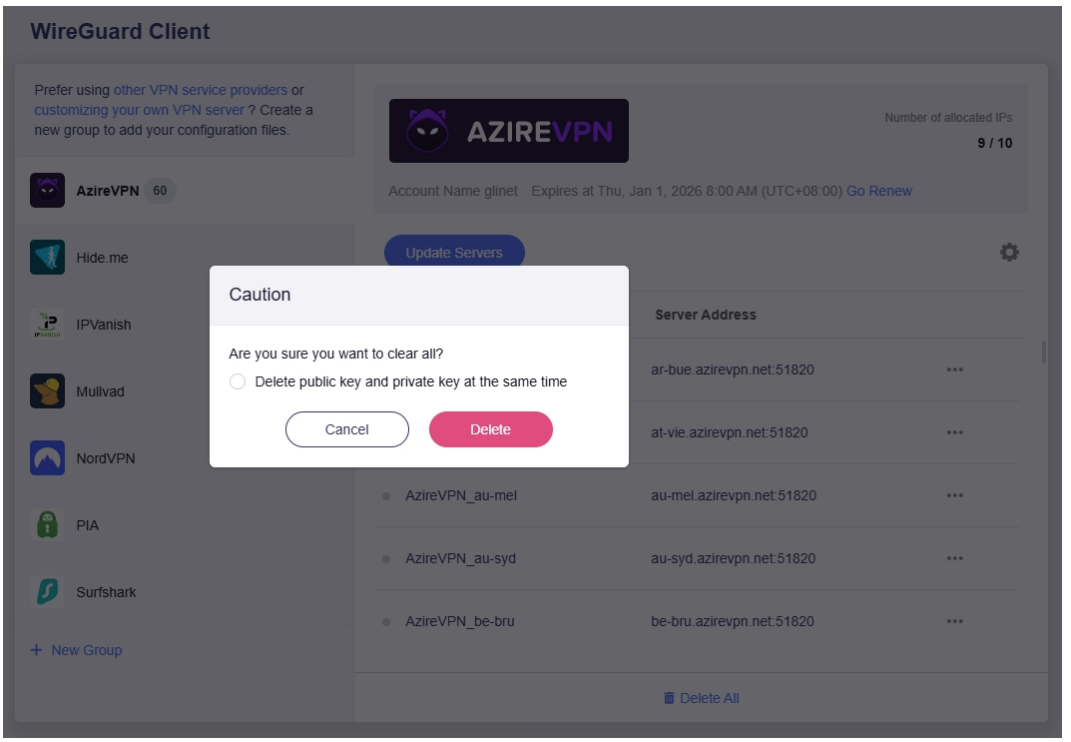
7. Rinnova.

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



8. Elimina tutti i file.

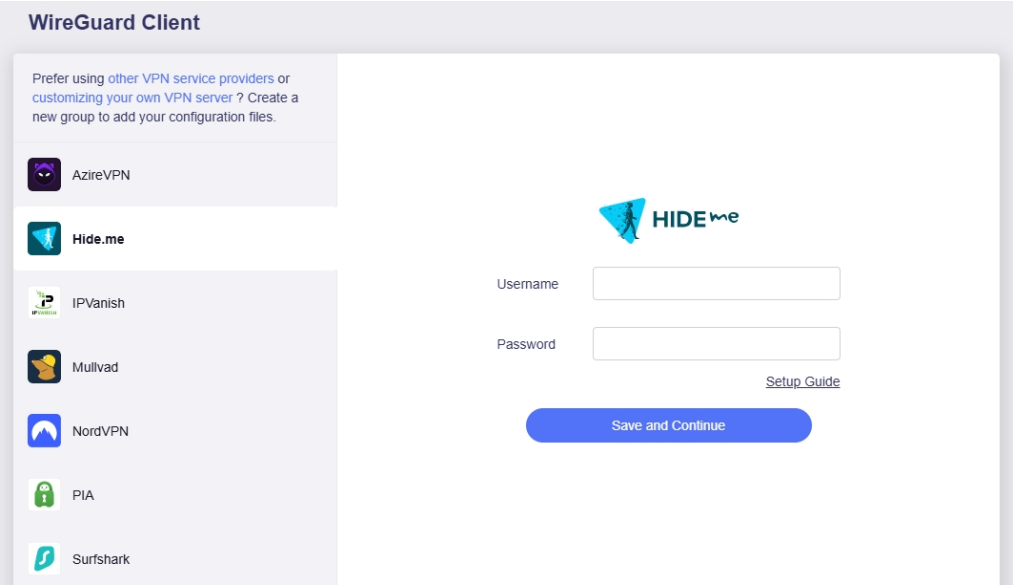
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



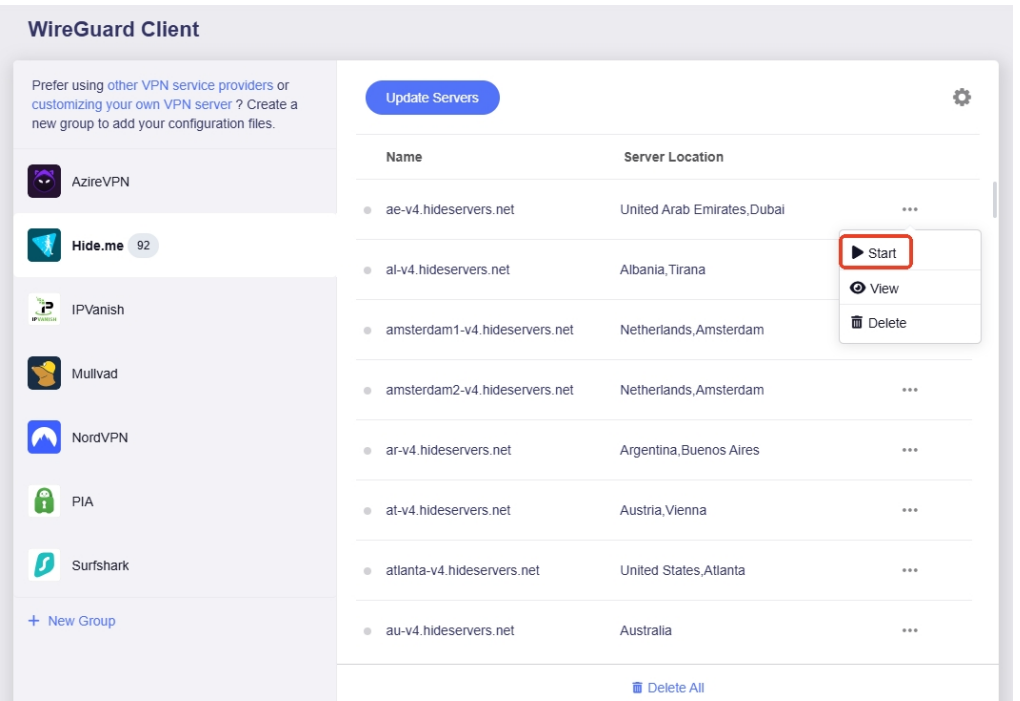
11.2.3 Configurazione di Hide.me

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

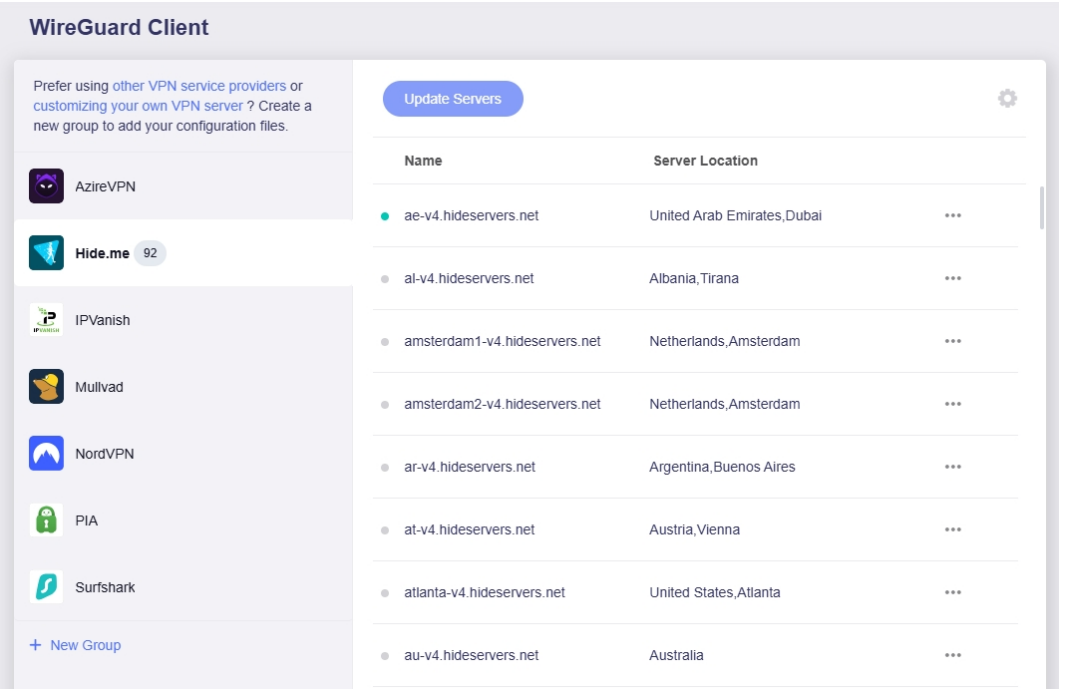
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Hide.me**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**. Genererà file di configurazione per ciascun server.



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



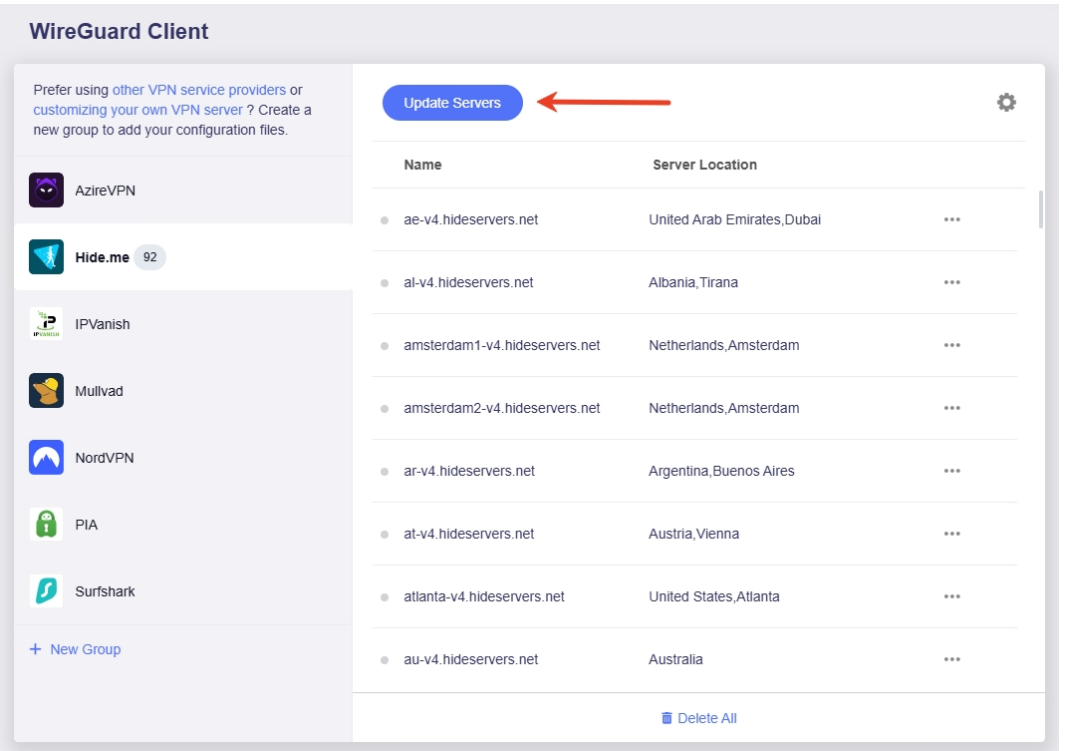
4. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

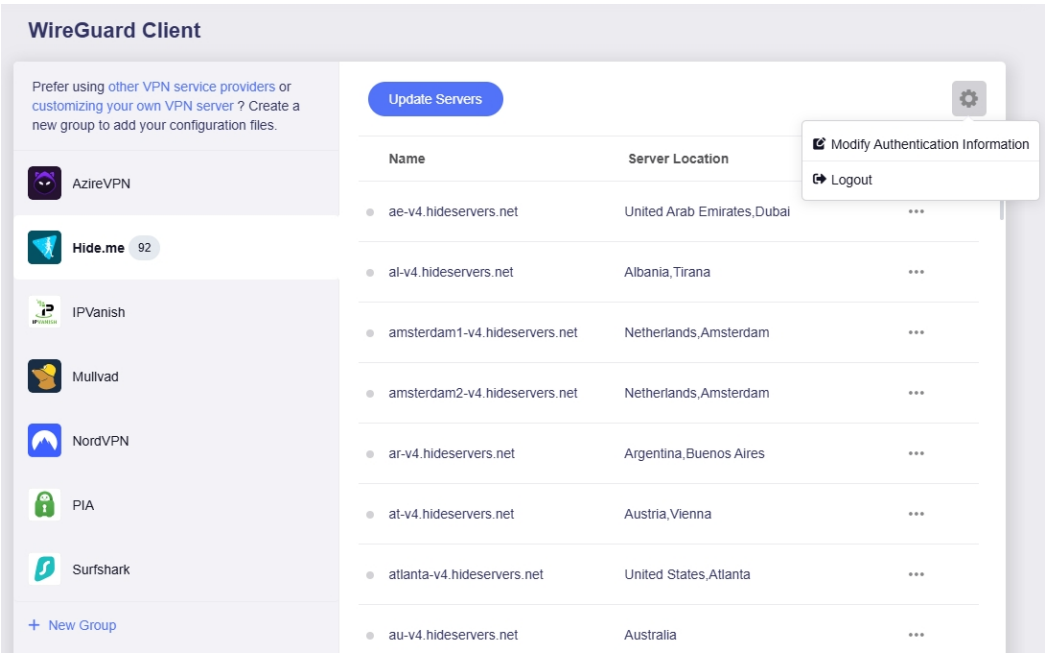
5. Aggiorna server.

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.



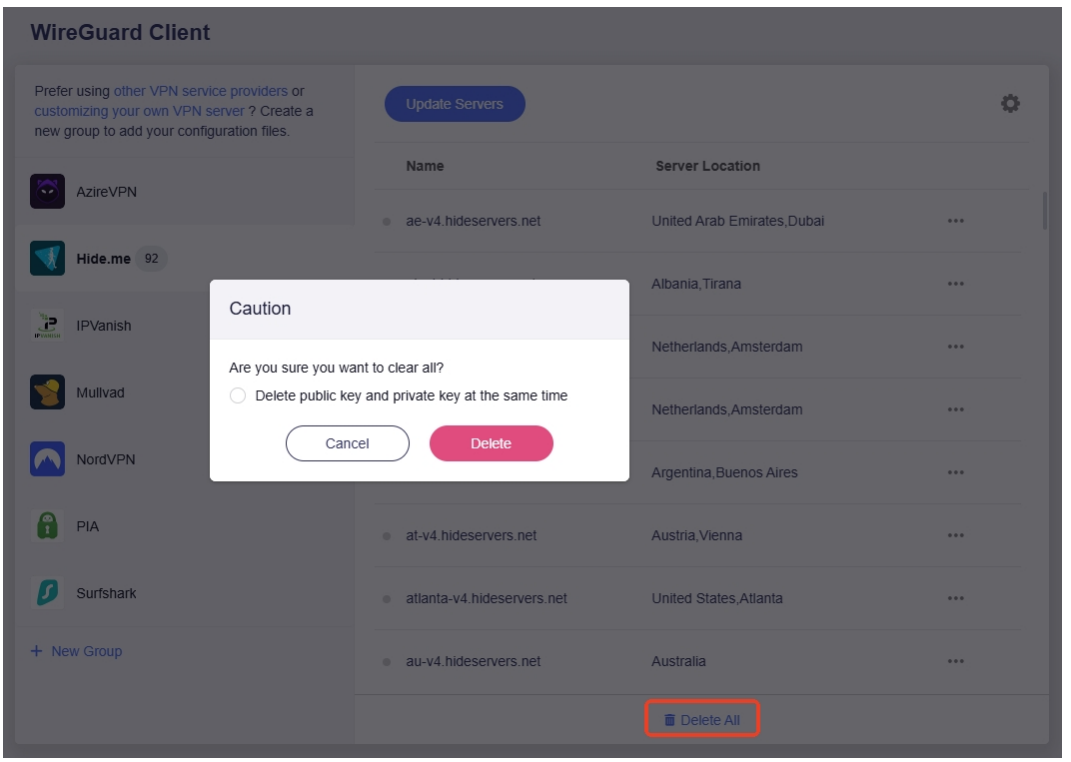
6. Modifica credenziali o esci.

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



7. Elimina tutti i file.

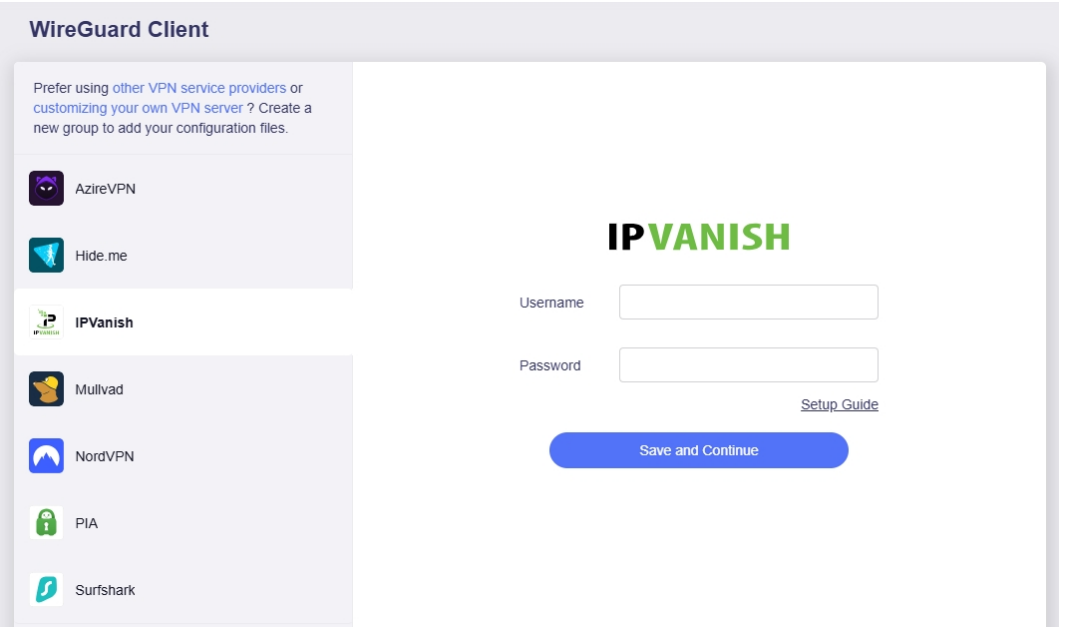
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



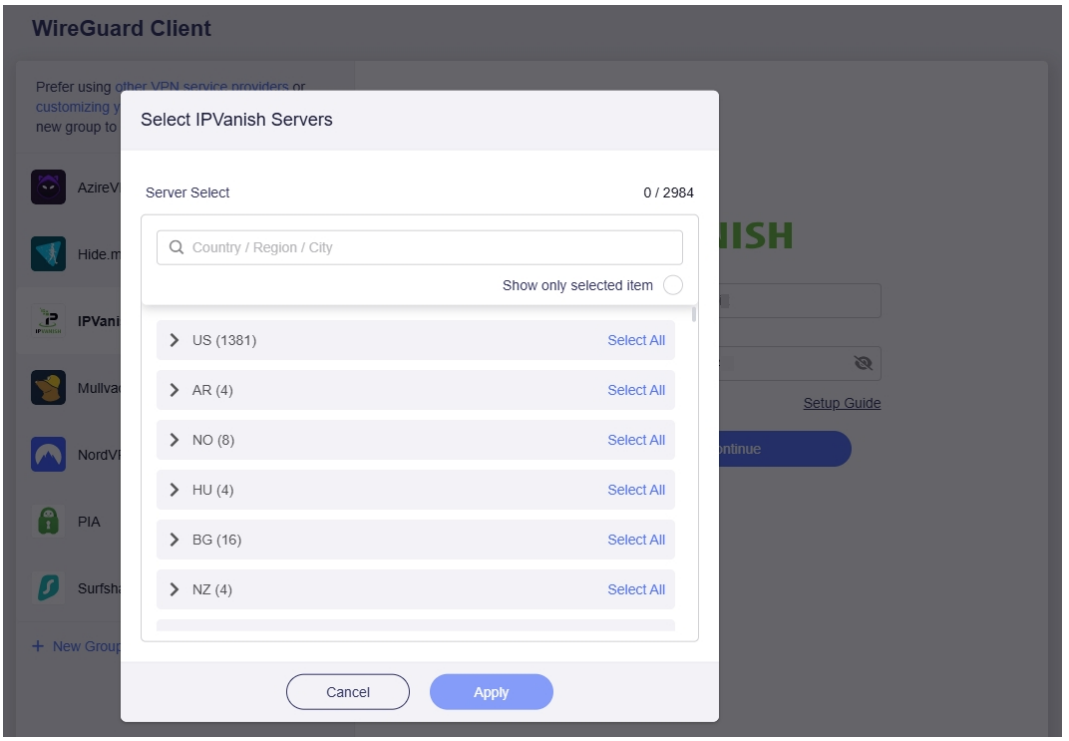
11.2.4 Configurazione di IPVanish

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

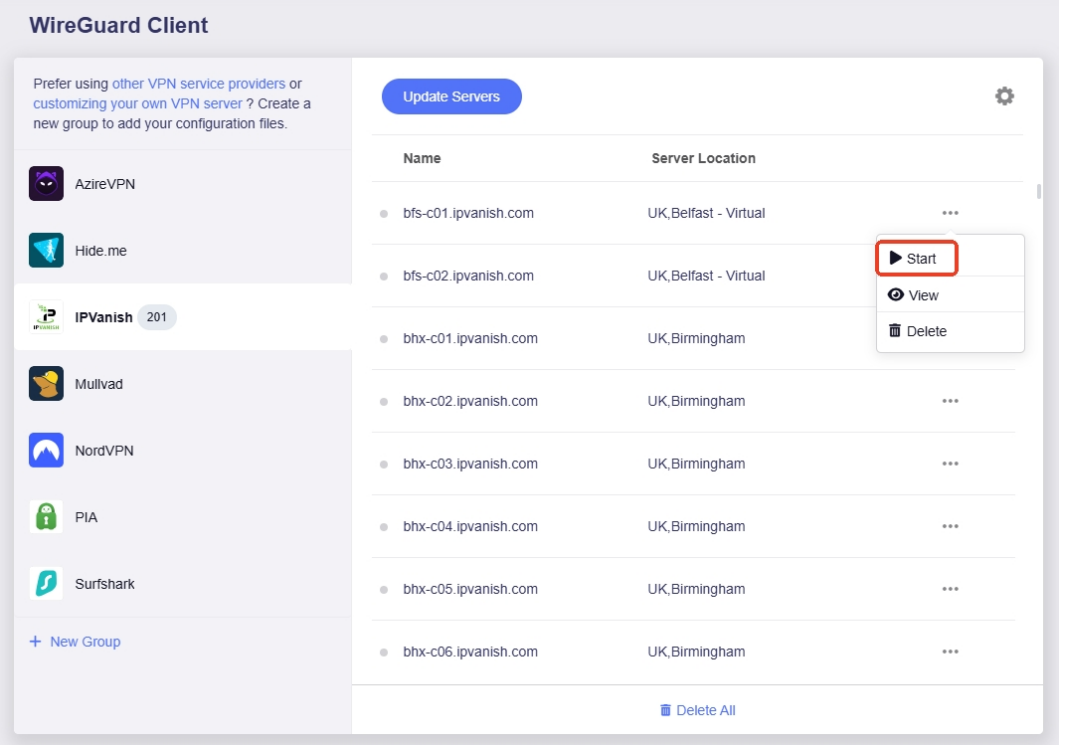
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **IPVanish**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



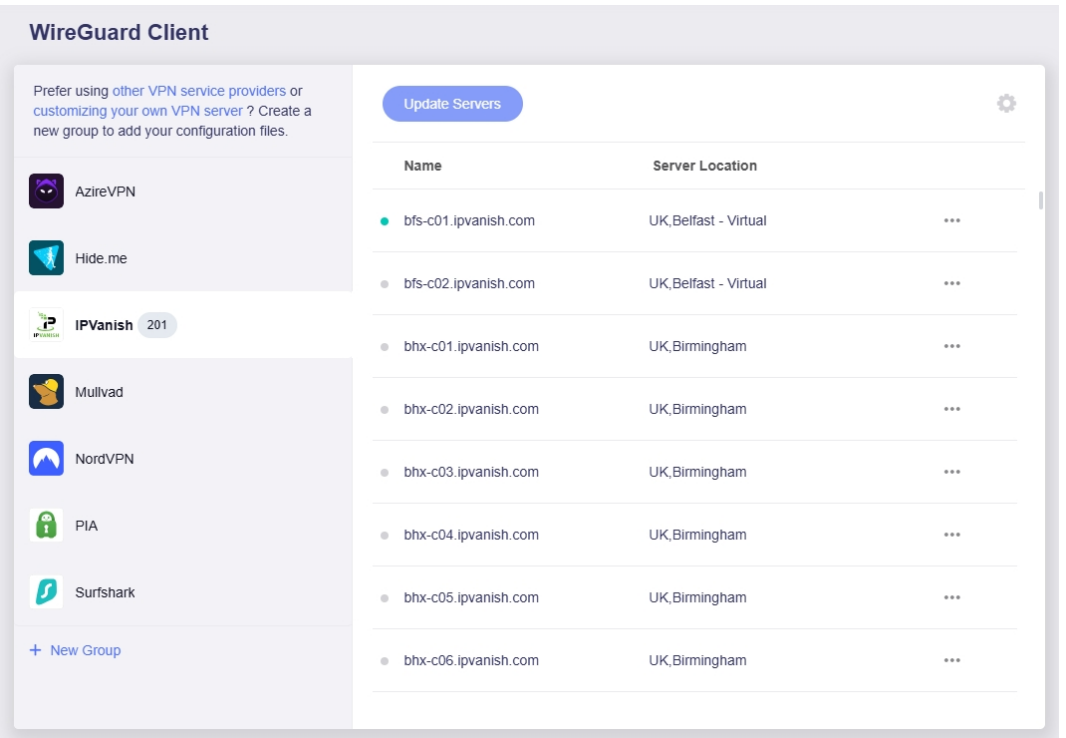
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



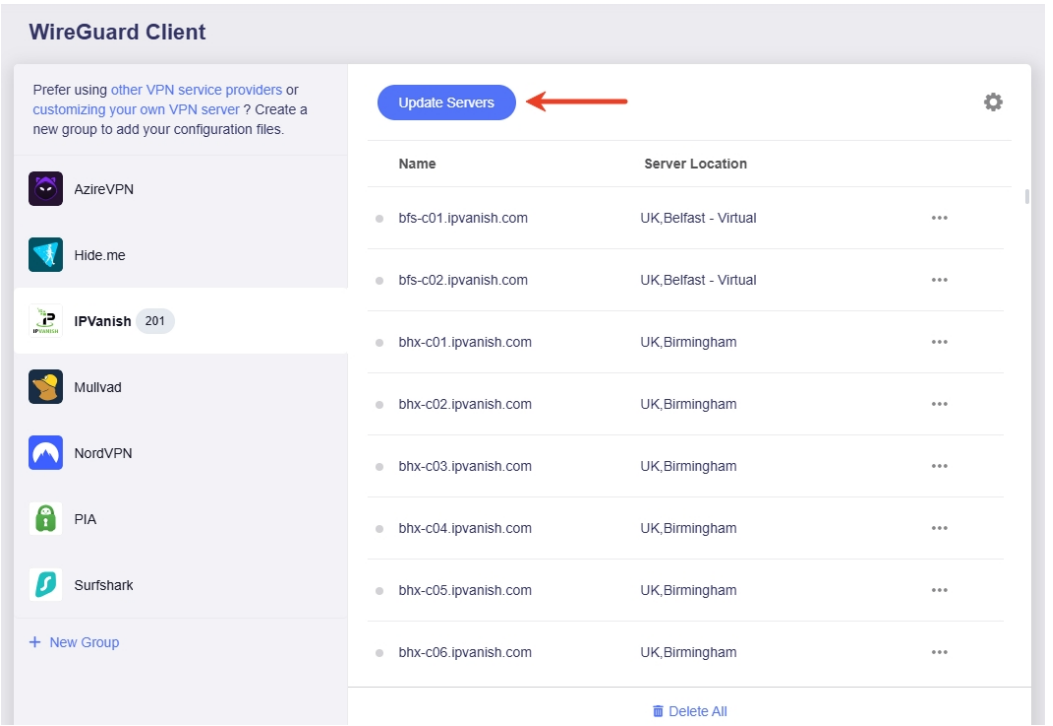
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

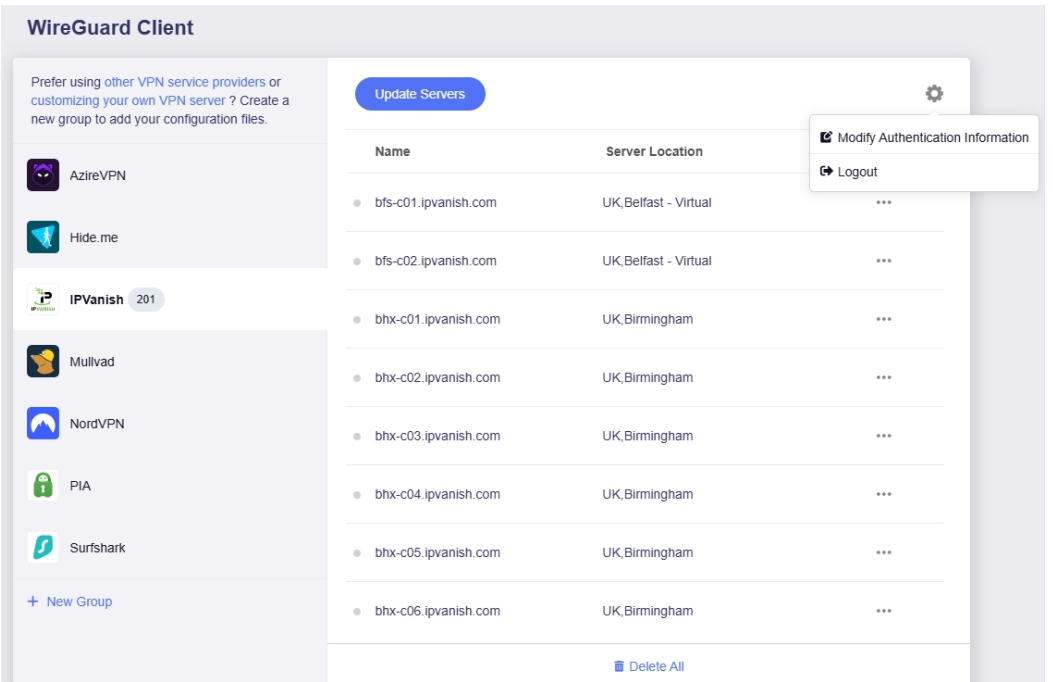
6. Aggiorna server.

   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.



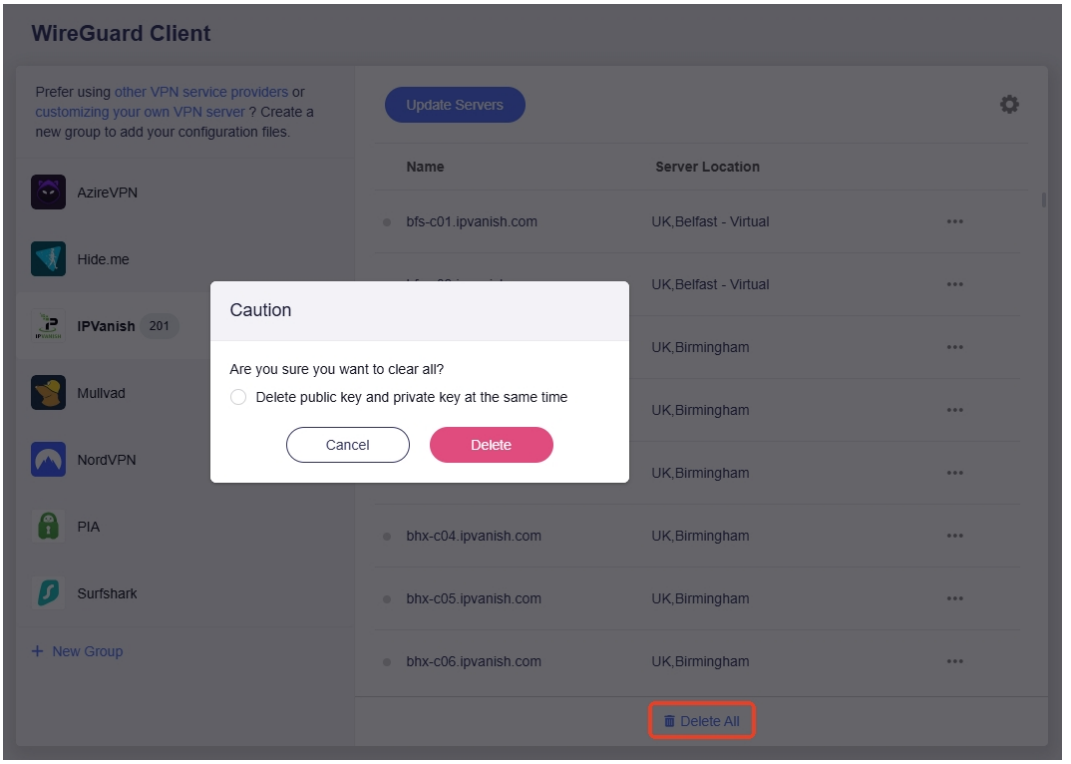
7. Modifica credenziali o esci.

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



8. Elimina tutti i file.

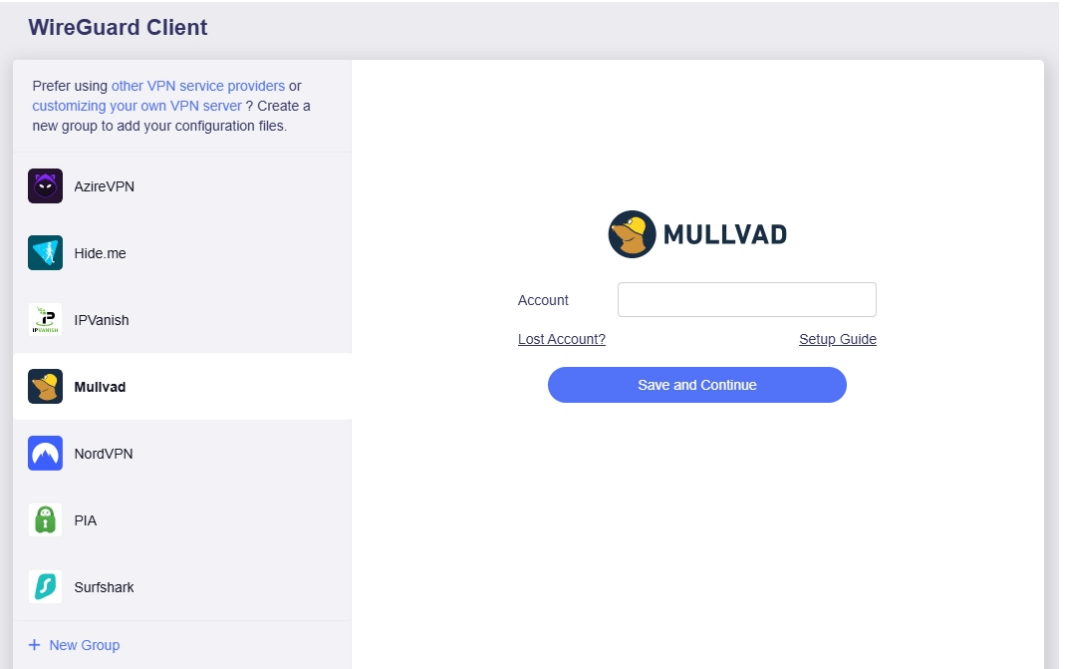
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



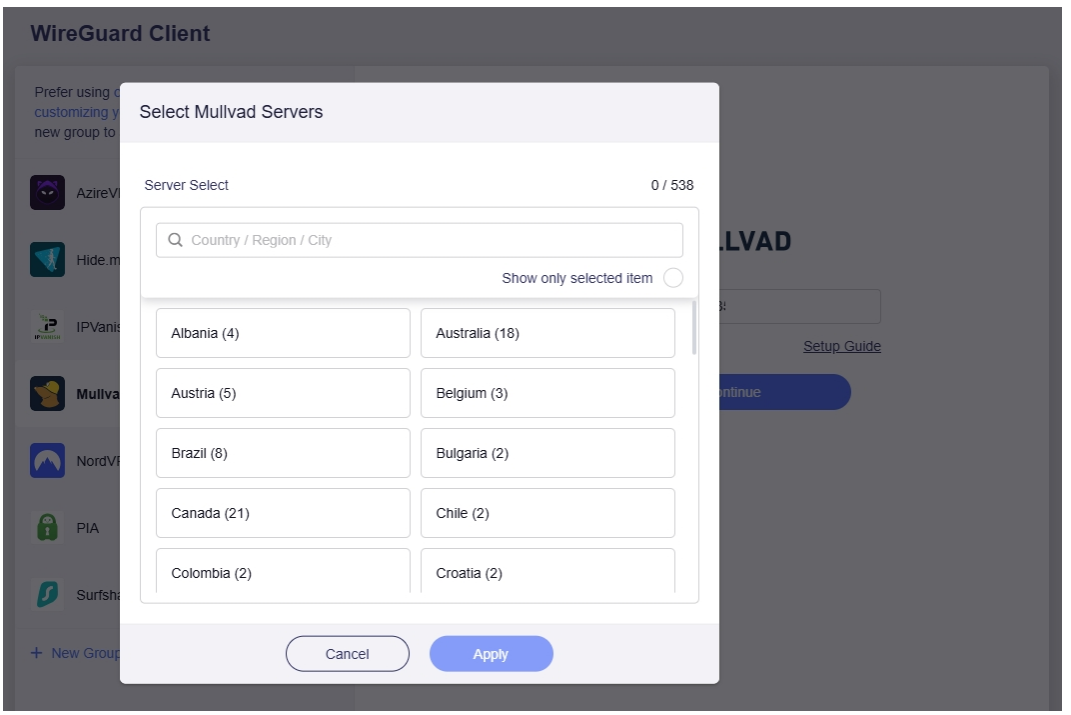
11.2.5 Configurazione di Mullvad

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

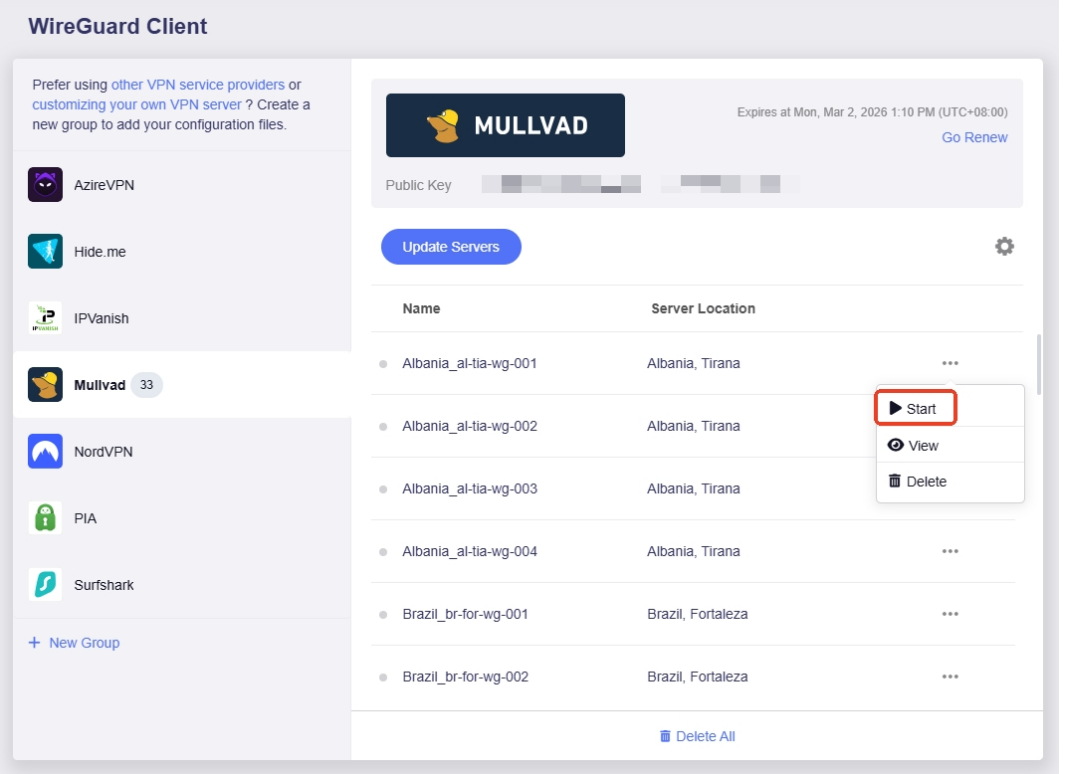
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Mullvad**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



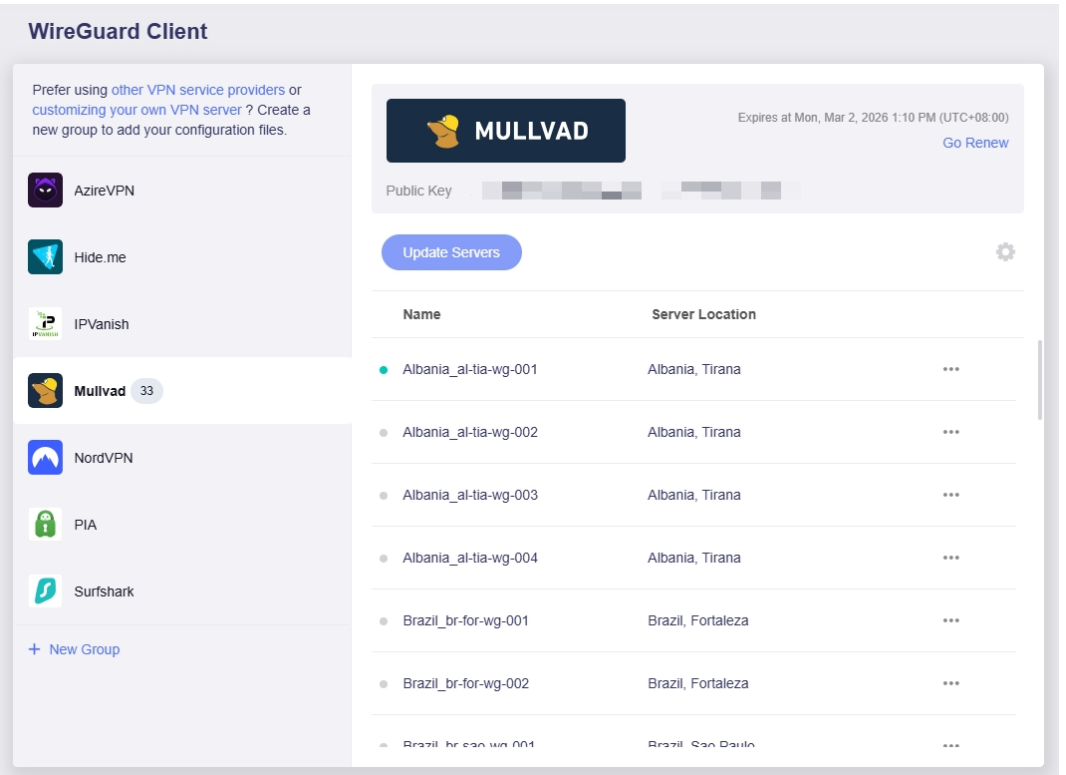
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



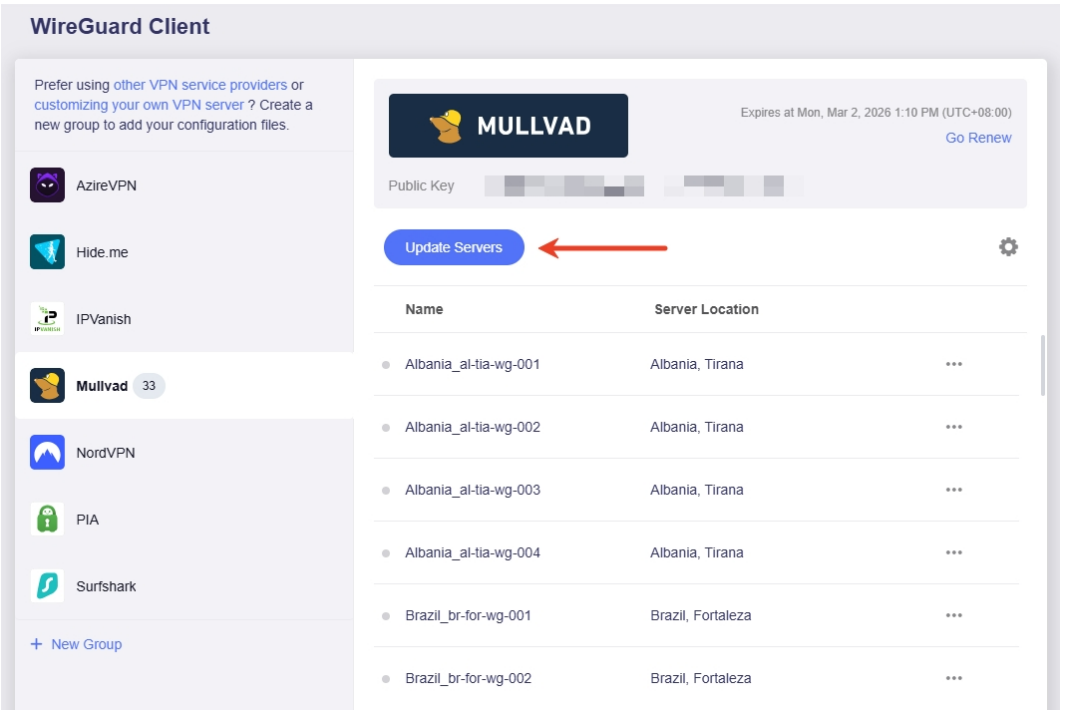
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

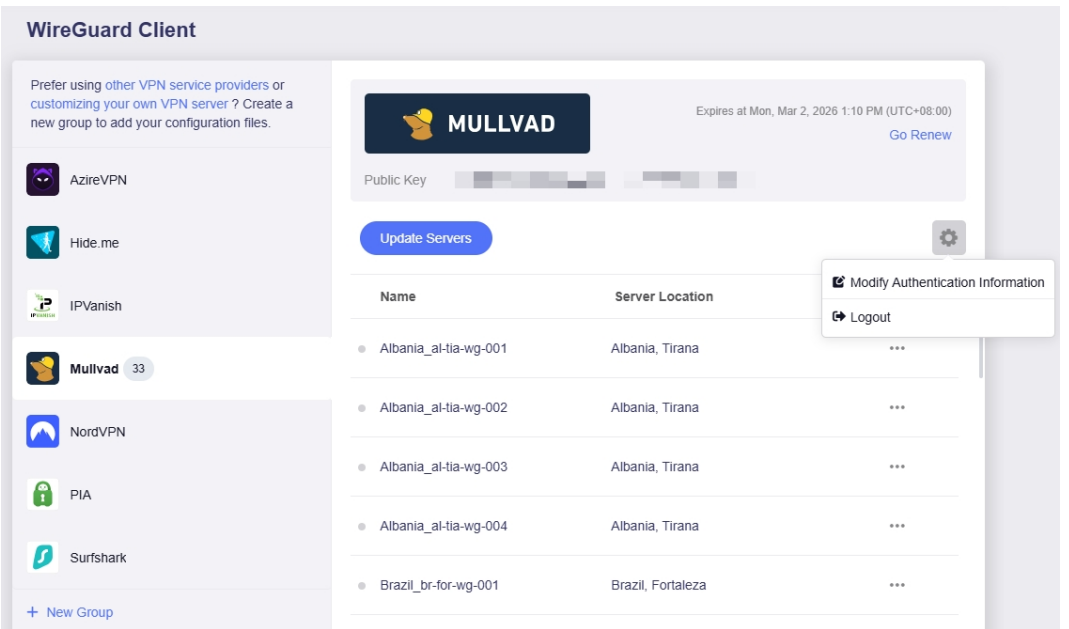
6. Aggiorna server.

   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.



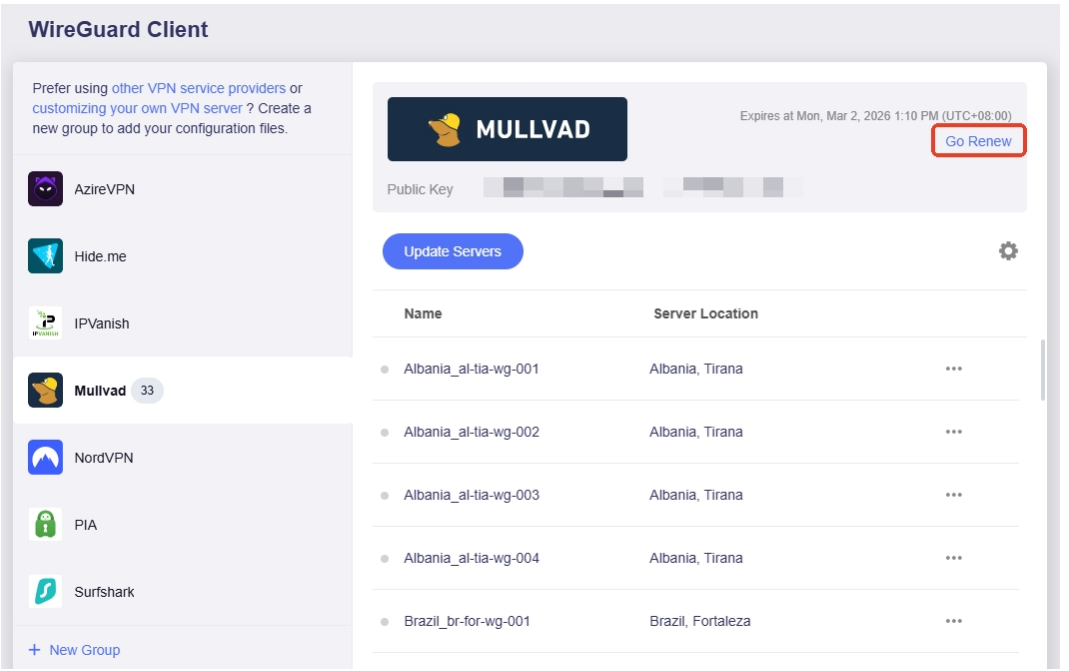
7. Modifica credenziali o esci.

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



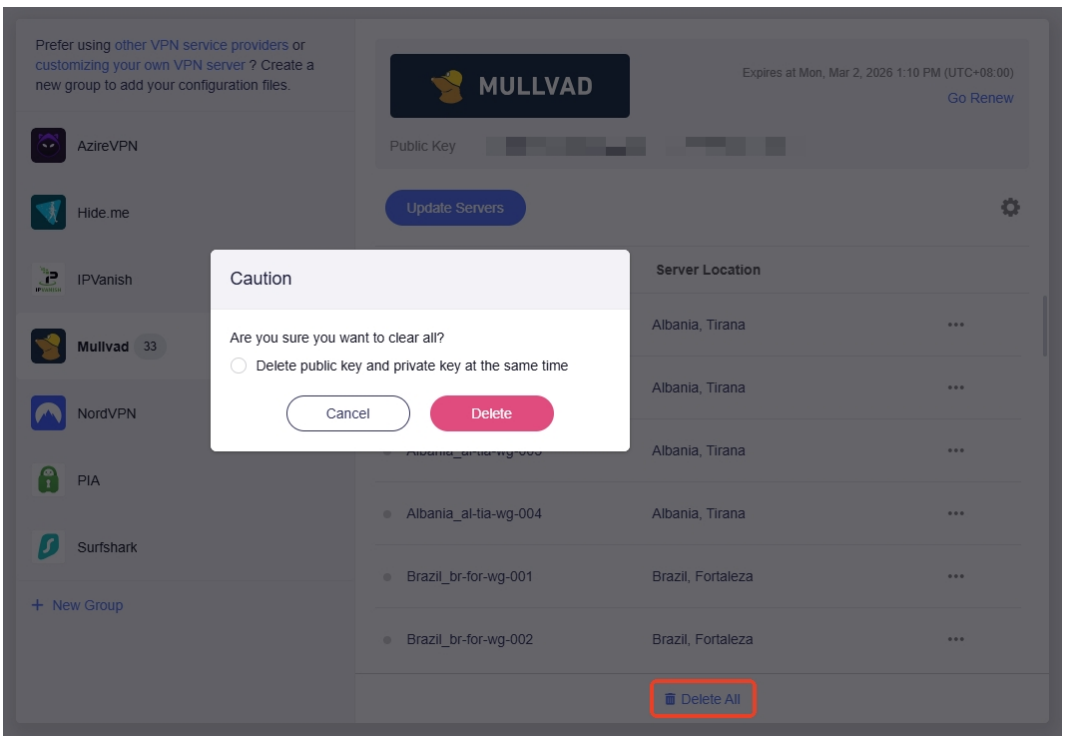
8. Rinnova.

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



9. Elimina tutti i file.

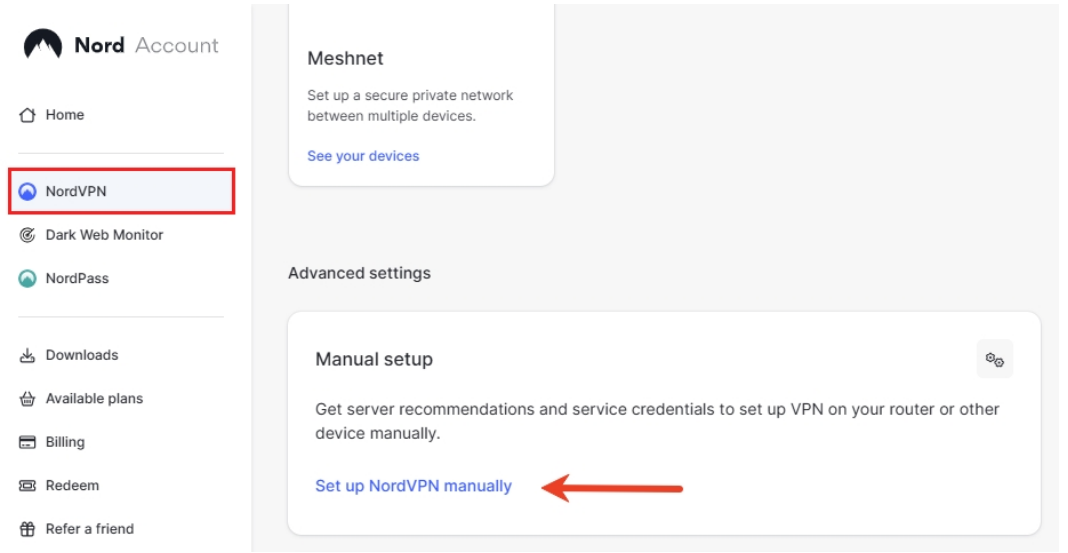
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



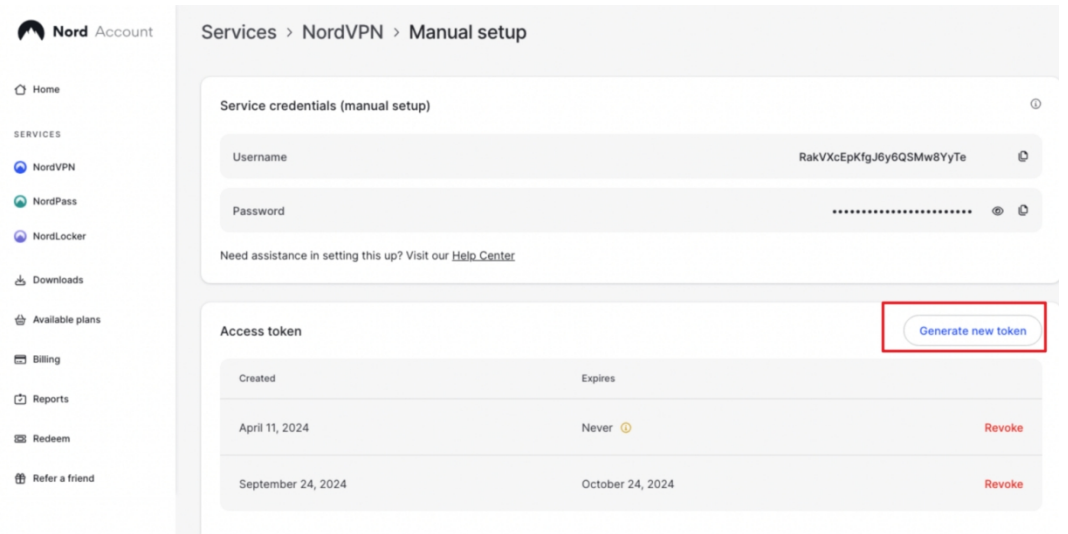
11.2.6 Configurazione di NordVPN

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

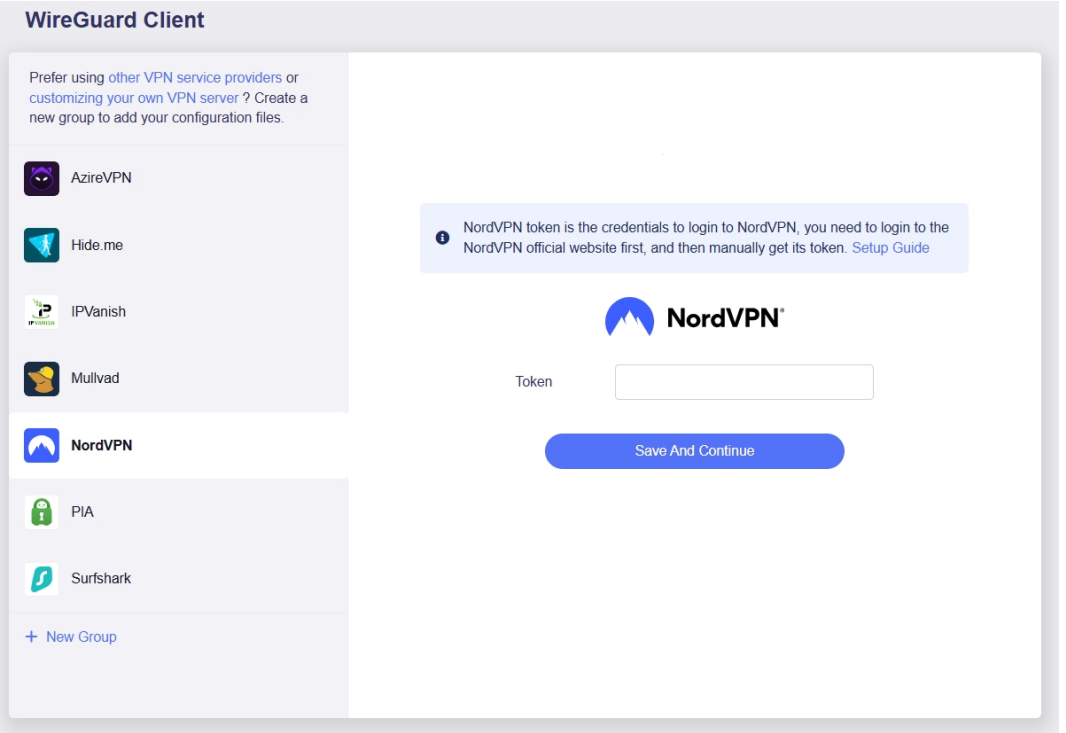
1. Accedi al tuo account web NordVPN qui.
2. Nella Nord Dashboard, fai clic su **NordVPN**, quindi su **Configura NordVPN manualmente**.



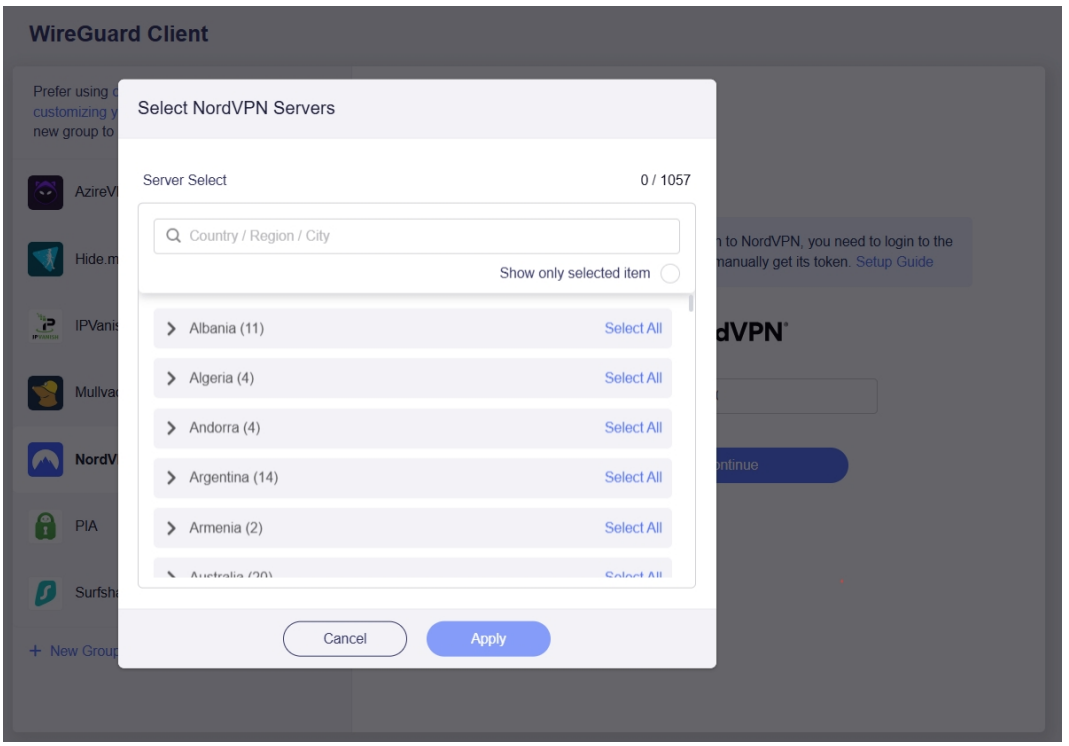
Troverai il **Token di accesso**. Crea un token di accesso e copialo per un uso successivo.



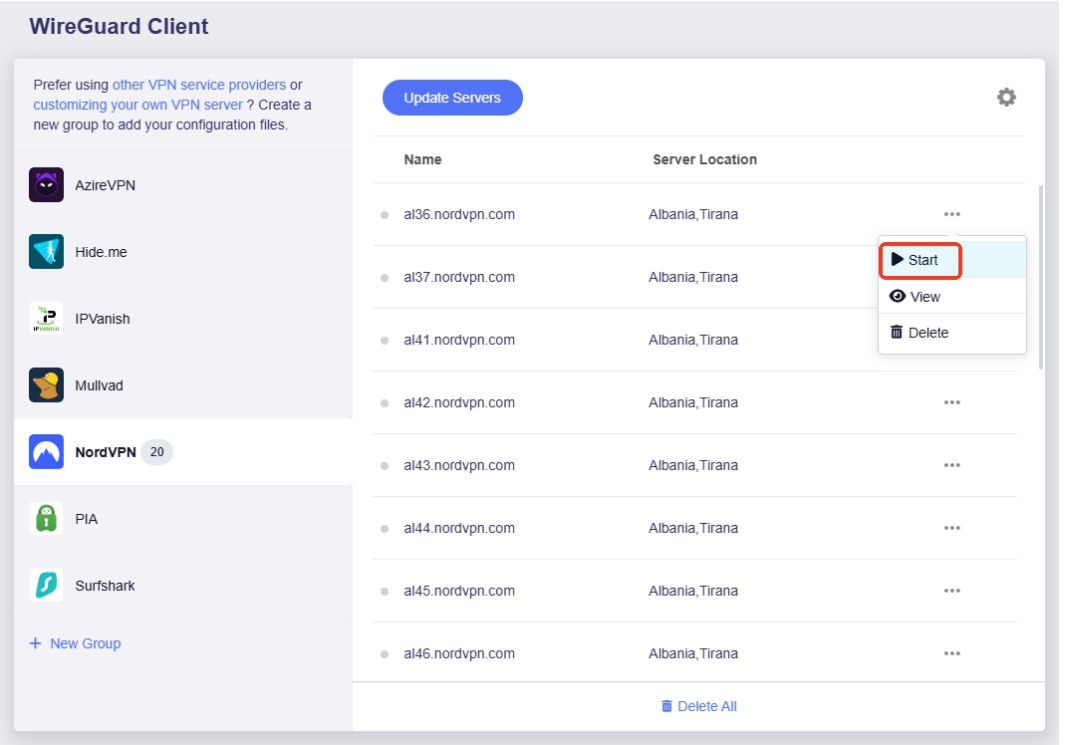
3. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **NordVPN**.
4. Inserisci il token e fai clic su **Salva e continua**.



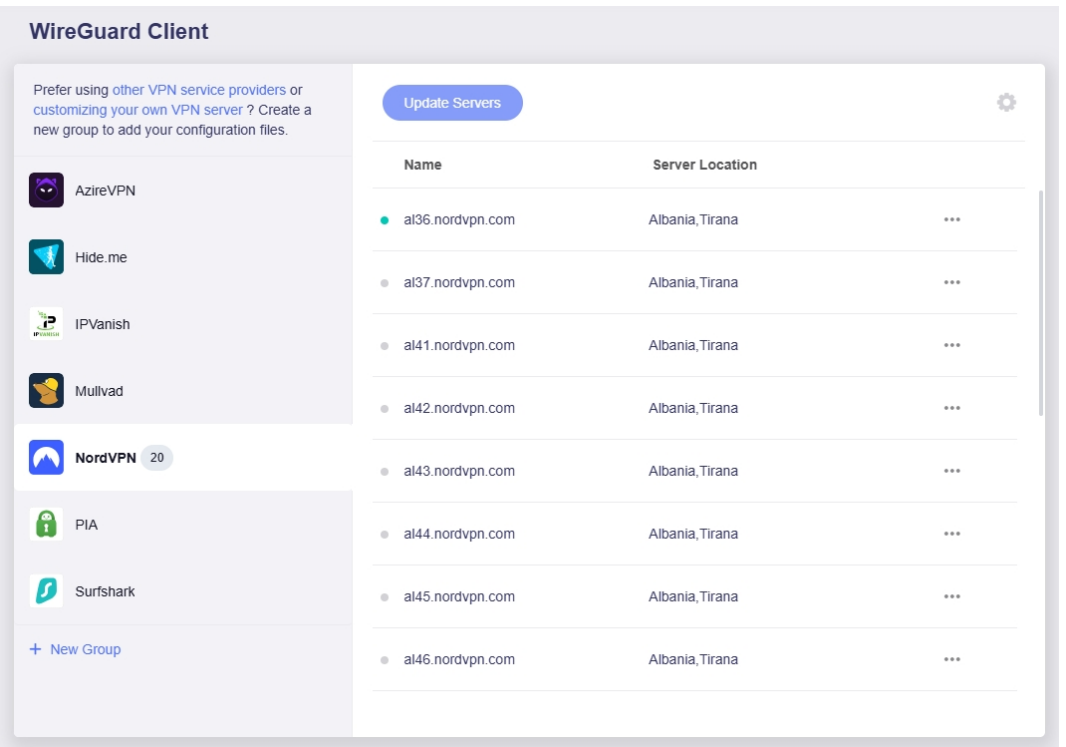
5. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



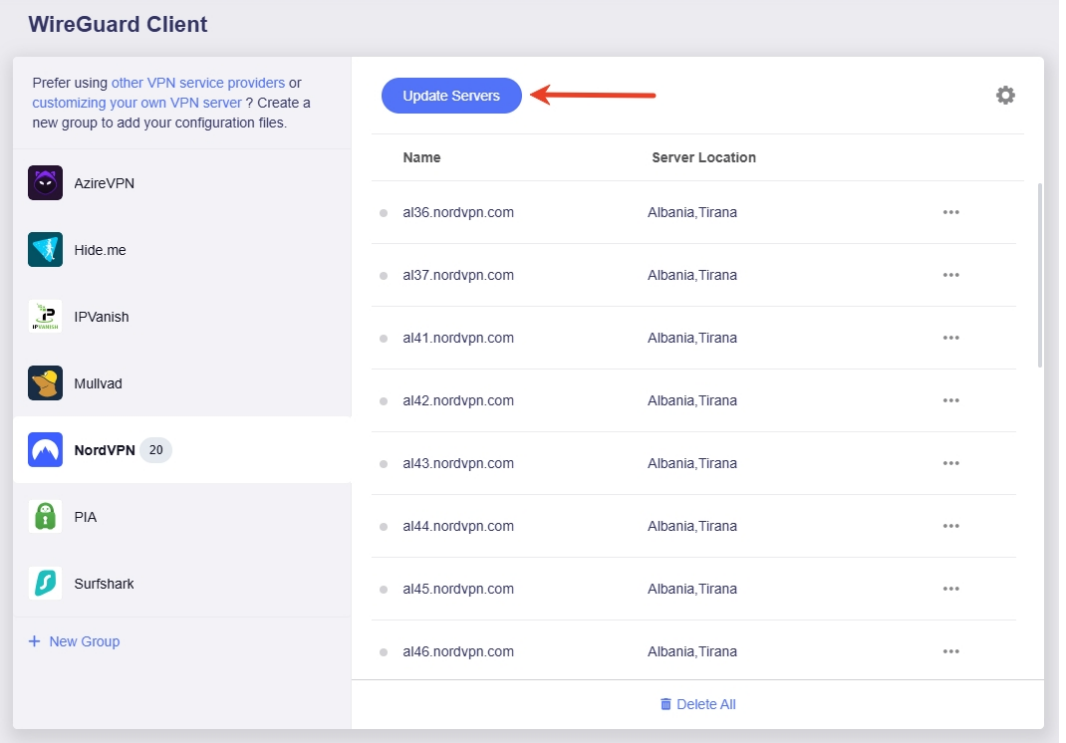
7. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

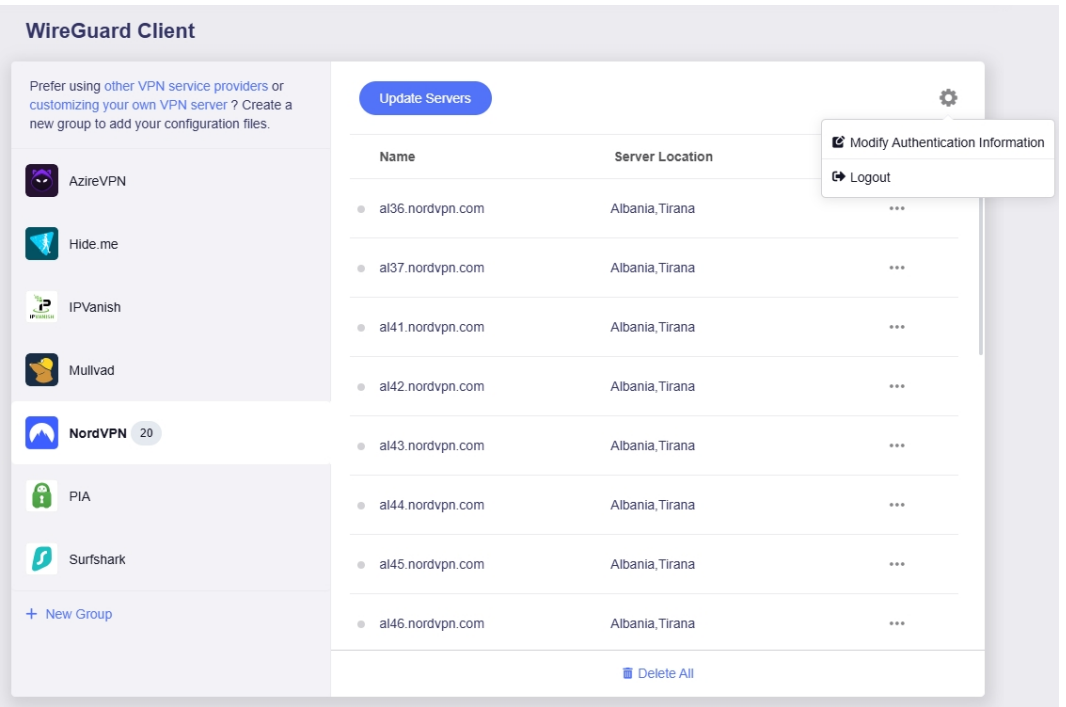
8. Aggiorna server.

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.



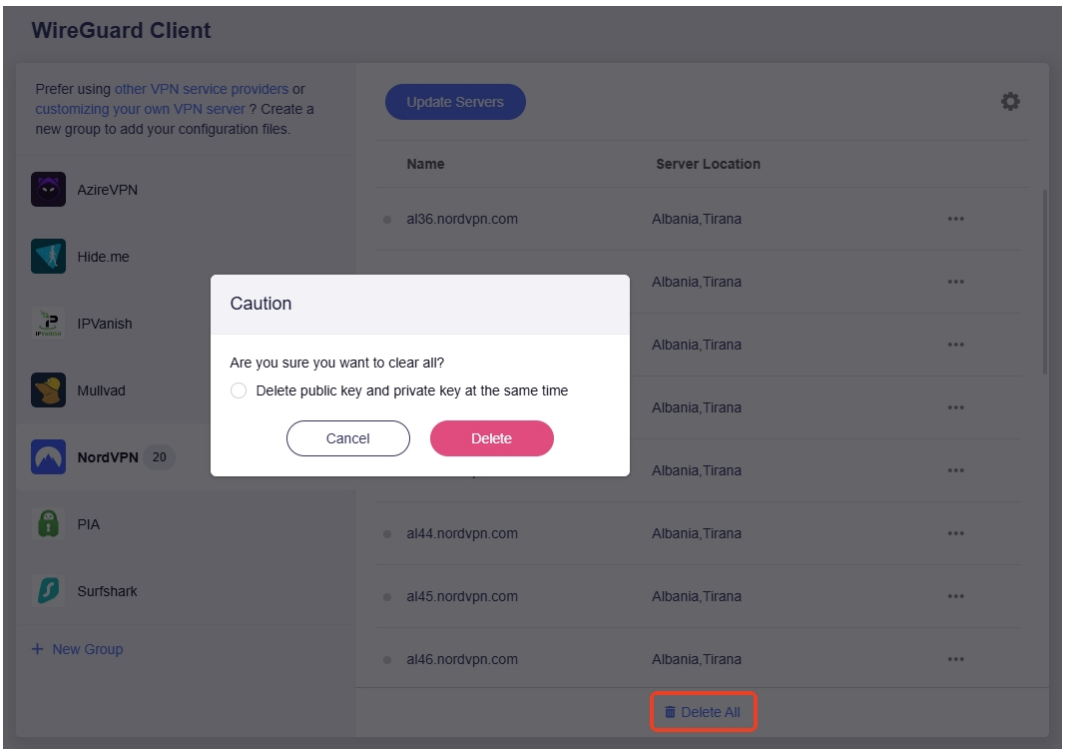
9. Modifica credenziali o esci.

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



10. Elimina tutti i file.

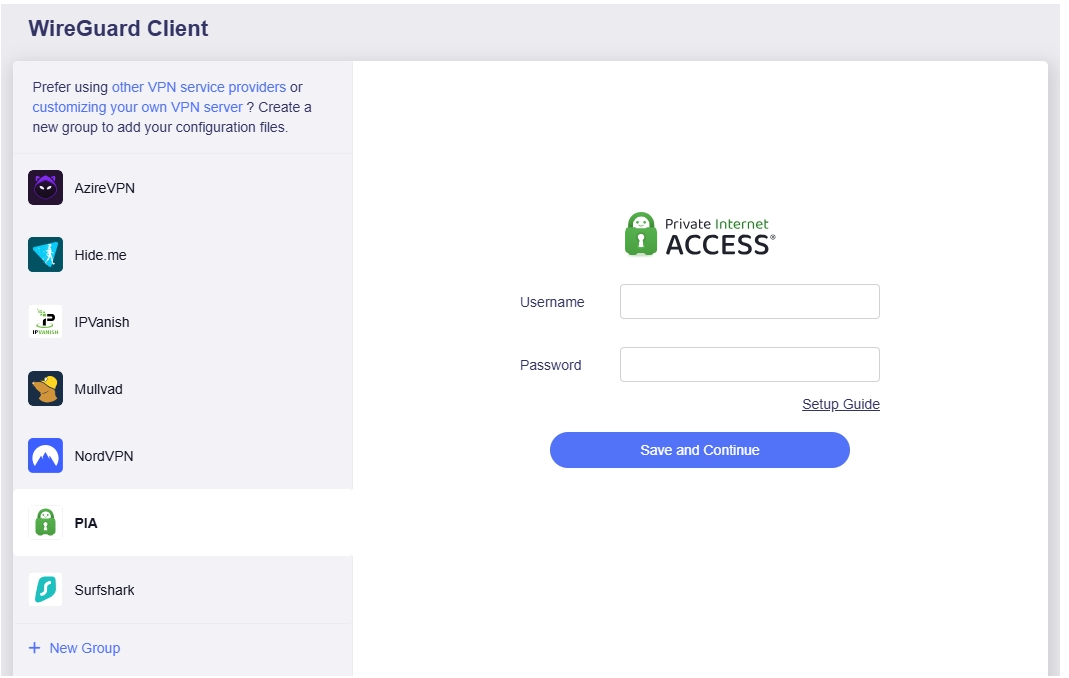
    Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



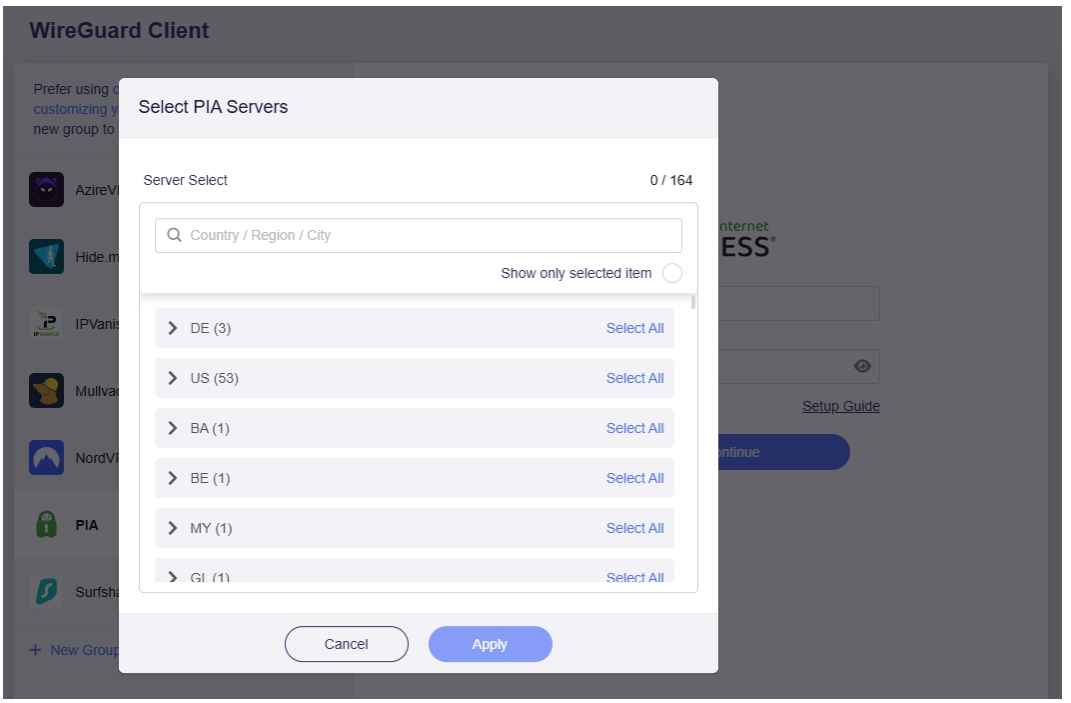
11.2.7 Configurazione di PIA (Private Internet Access)

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

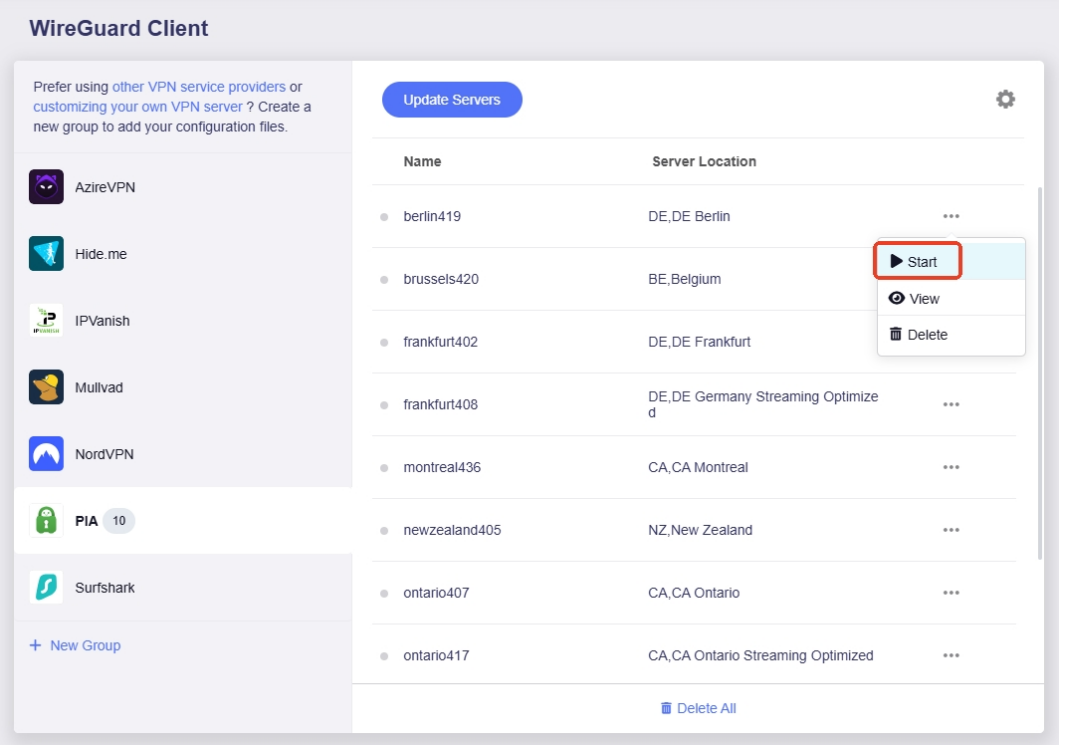
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **PIA**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



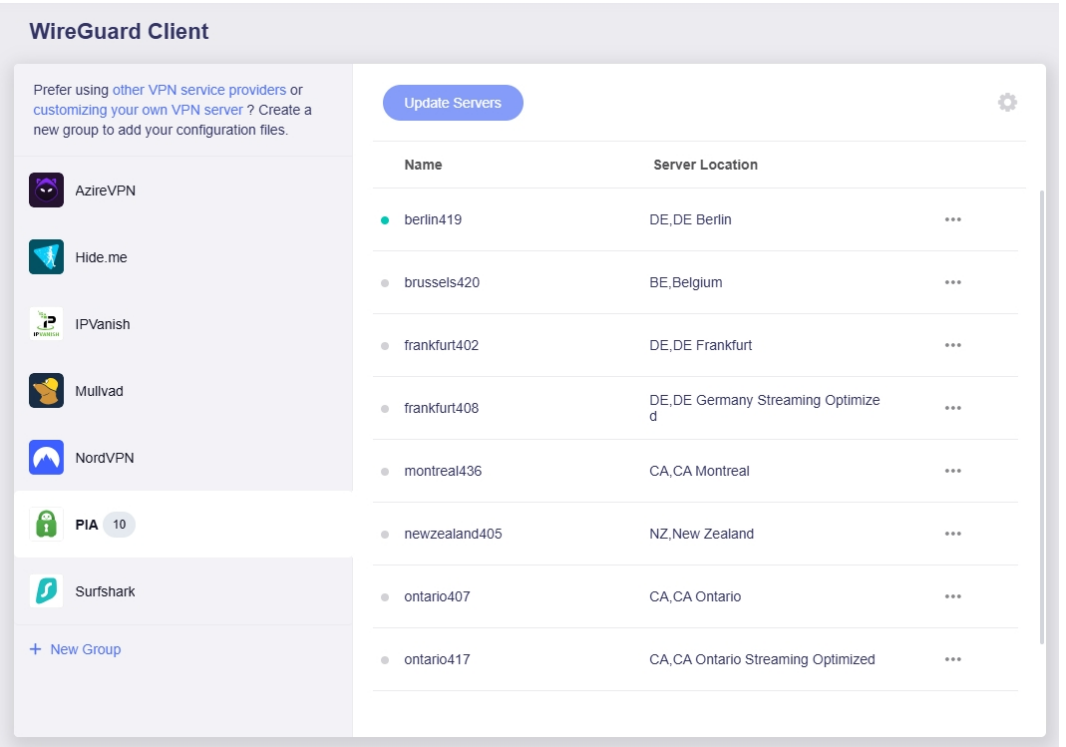
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



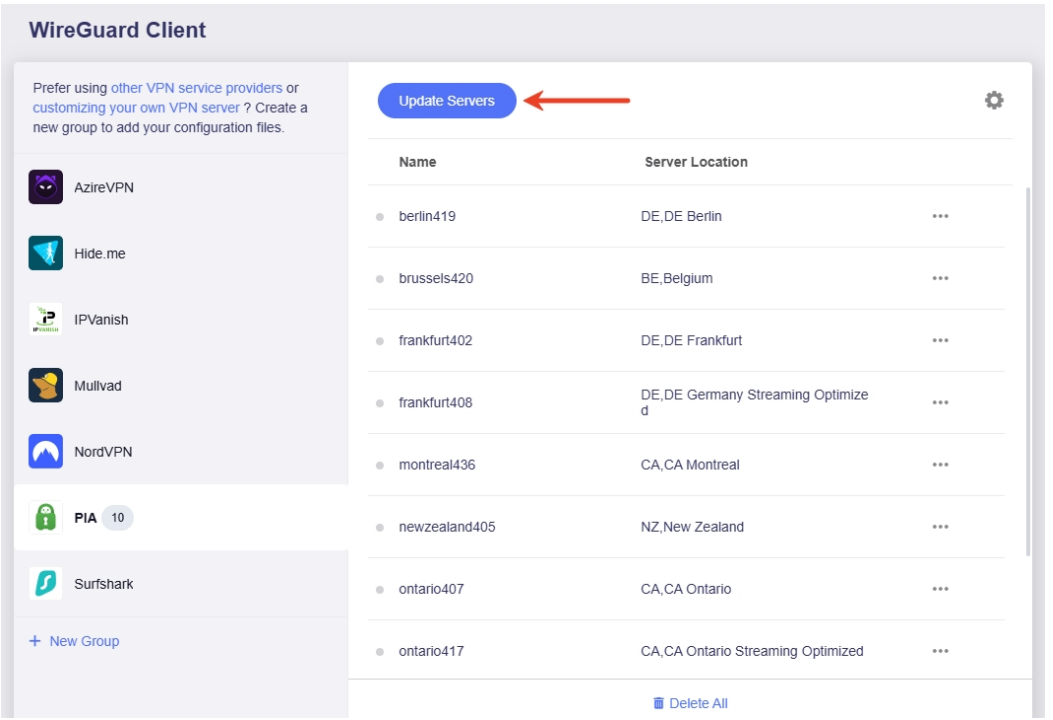
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

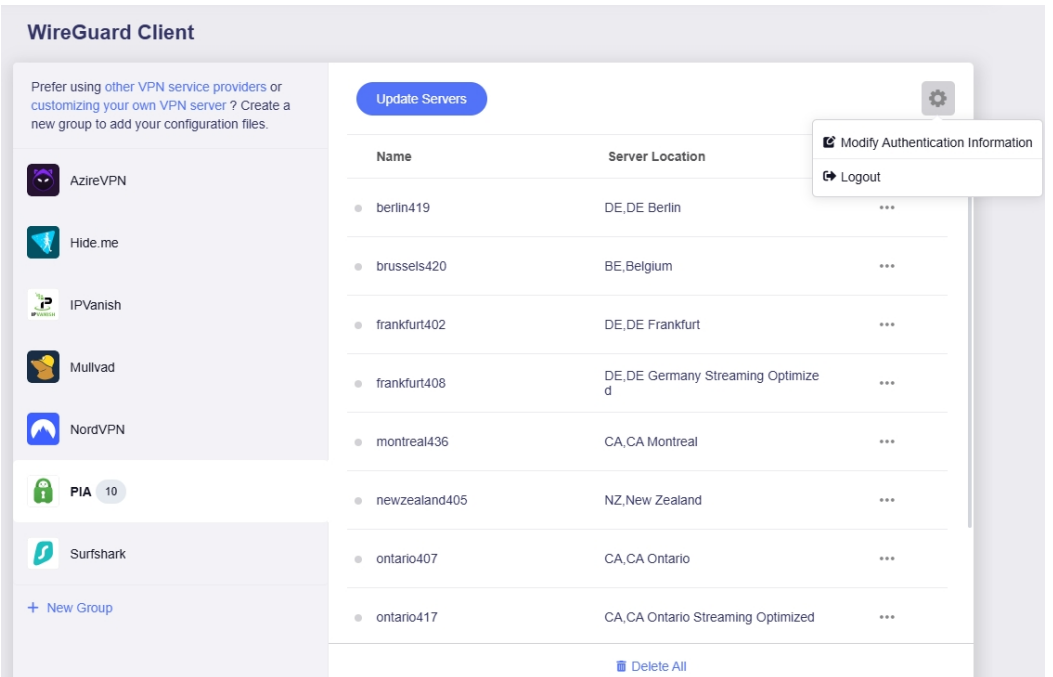
6. Aggiorna server.

   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.



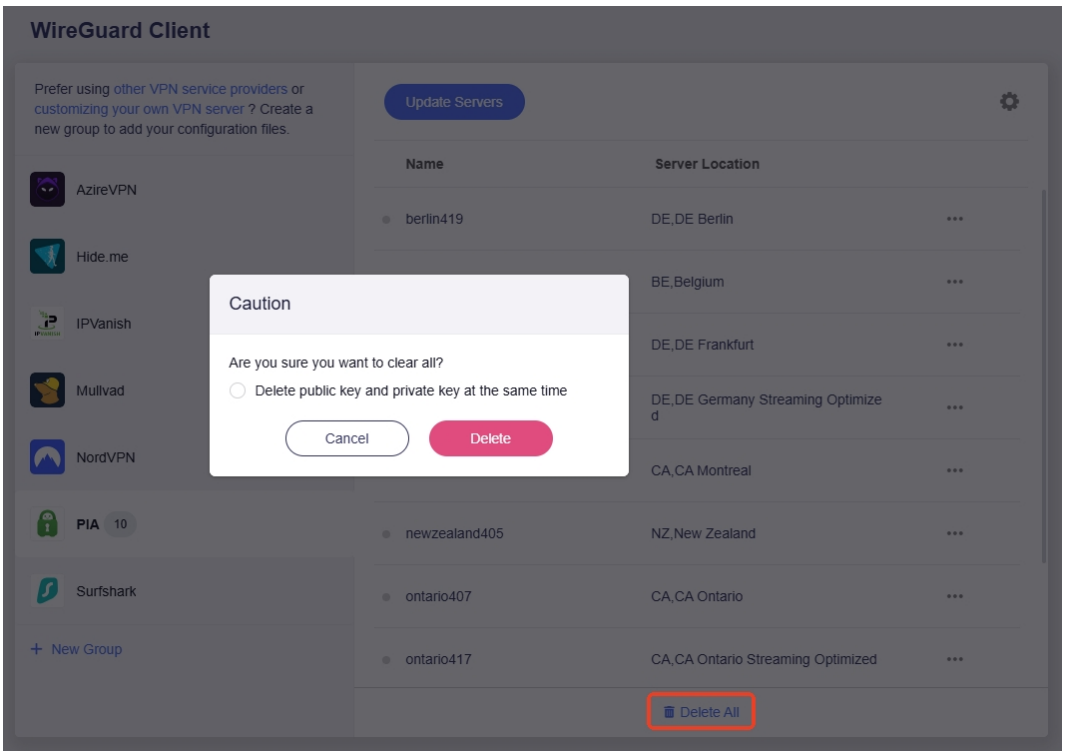
7. Modifica credenziali o esci.

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



8. Elimina tutti i file.

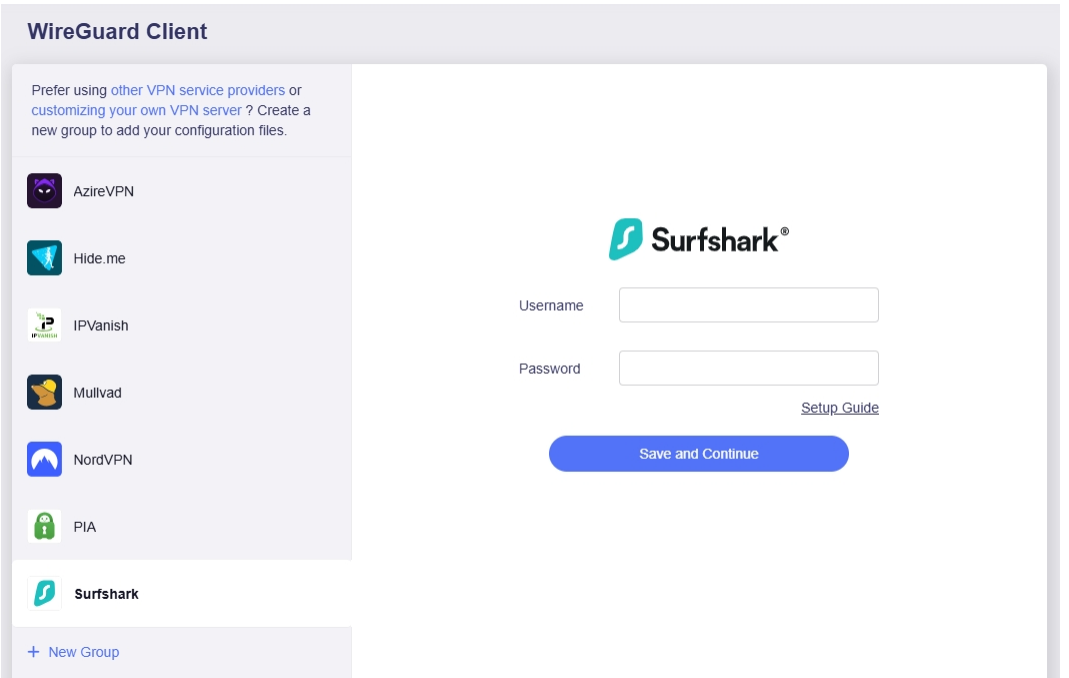
   Puoi fare clic su **Elimina tutto** per eliminare tutti i file di configurazione con un clic e scegliere se eliminare contemporaneamente le chiavi privata e pubblica.



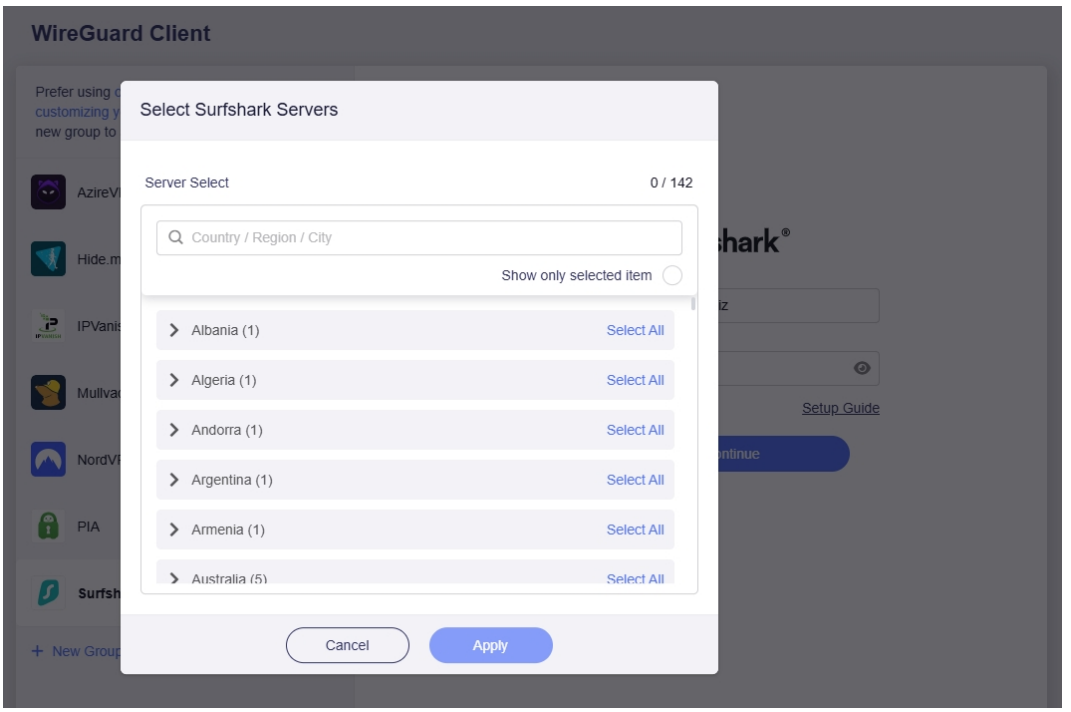
11.2.8 Configurazione di Surfshark

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

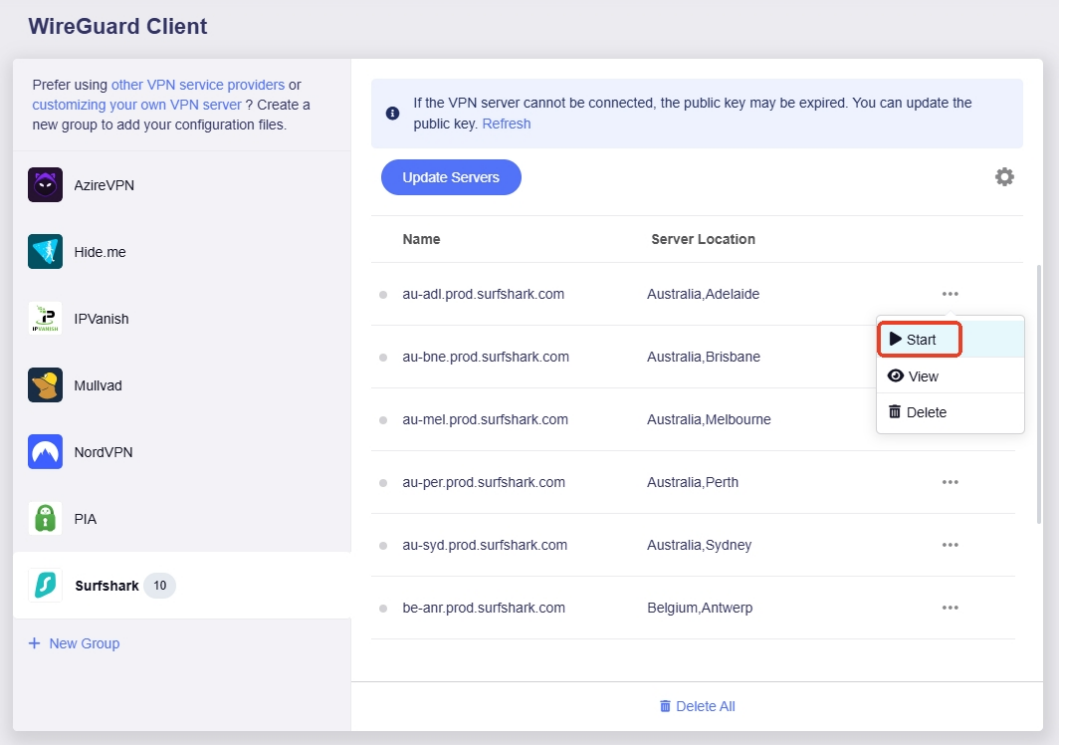
1. Accedi al pannello di amministrazione web del tuo router e vai su **VPN** > **Client WireGuard** > **Surfshark**.
2. Inserisci il nome utente e la password, quindi fai clic su **Salva e continua**.



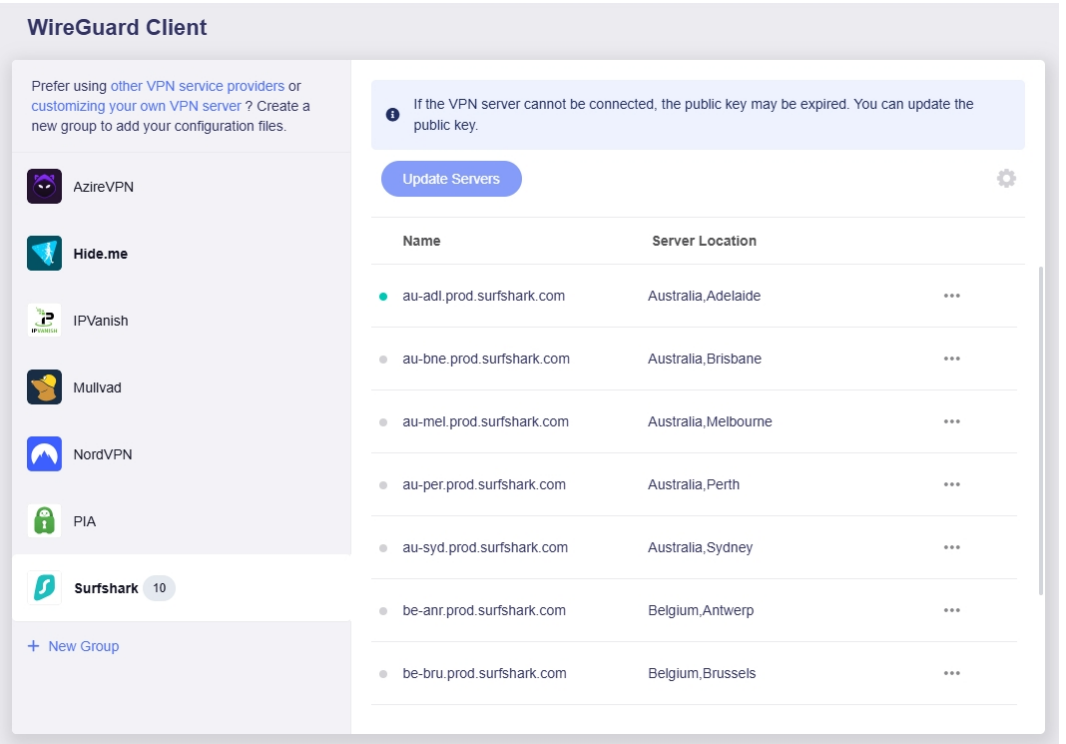
3. Seleziona i server a cui desideri connetterti e fai clic su **Applica**.



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



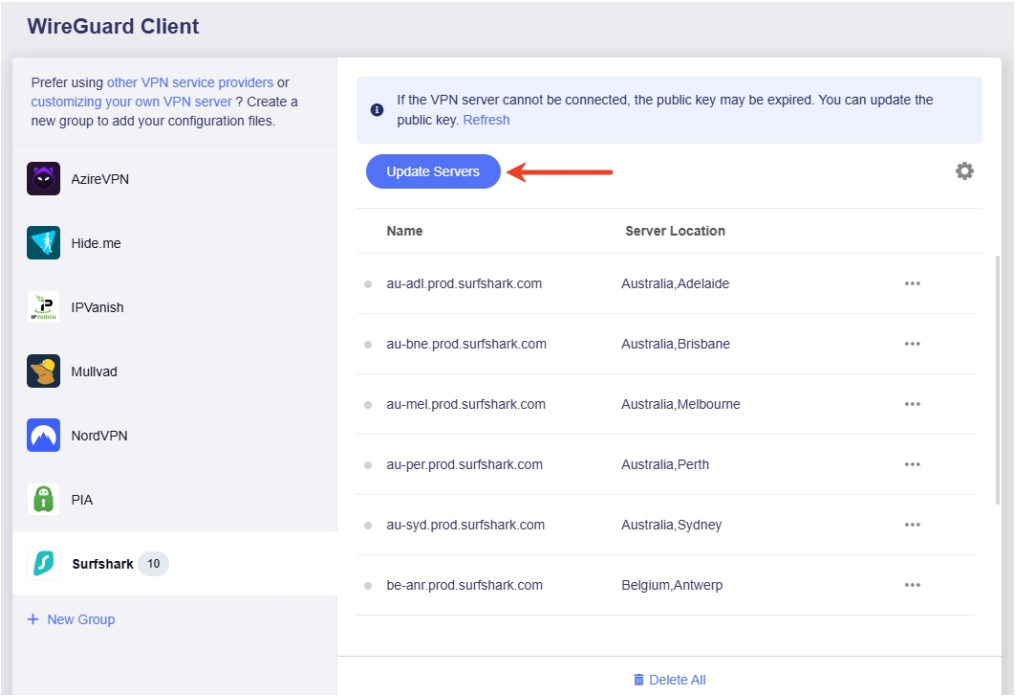
5. Una volta connesso, apparirà un punto verde accanto al file di configurazione.



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

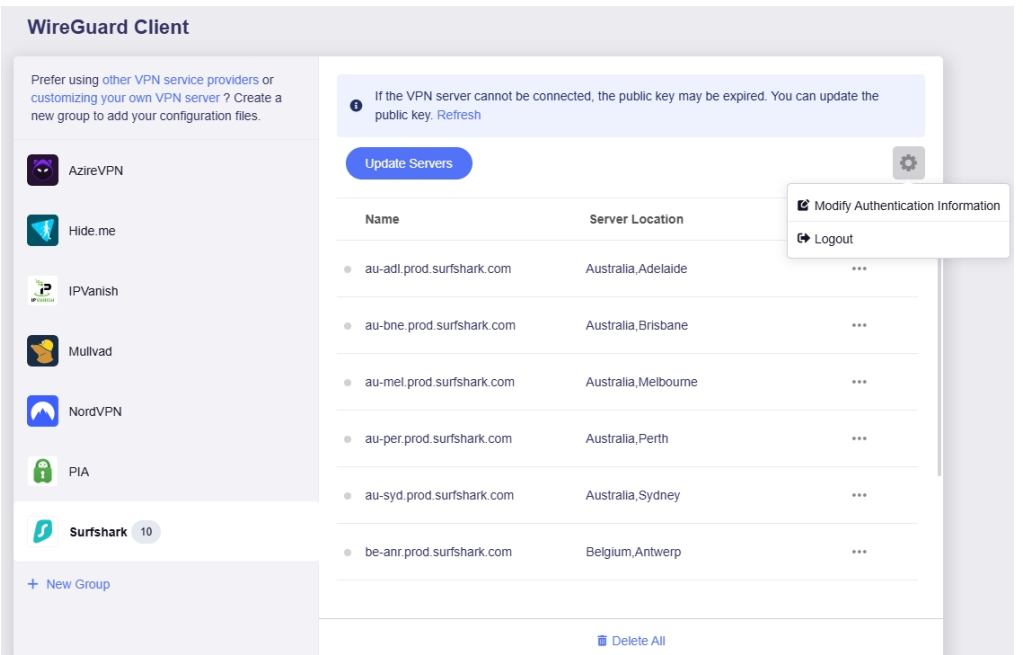
6. Aggiorna server.

   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.



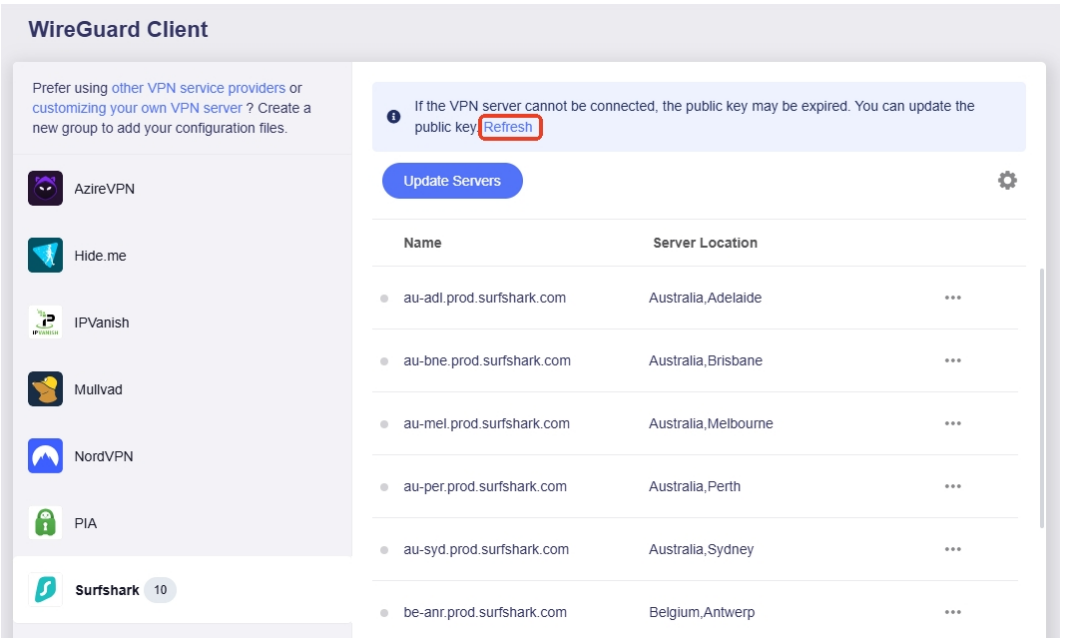
7. Modifica credenziali o esci.

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



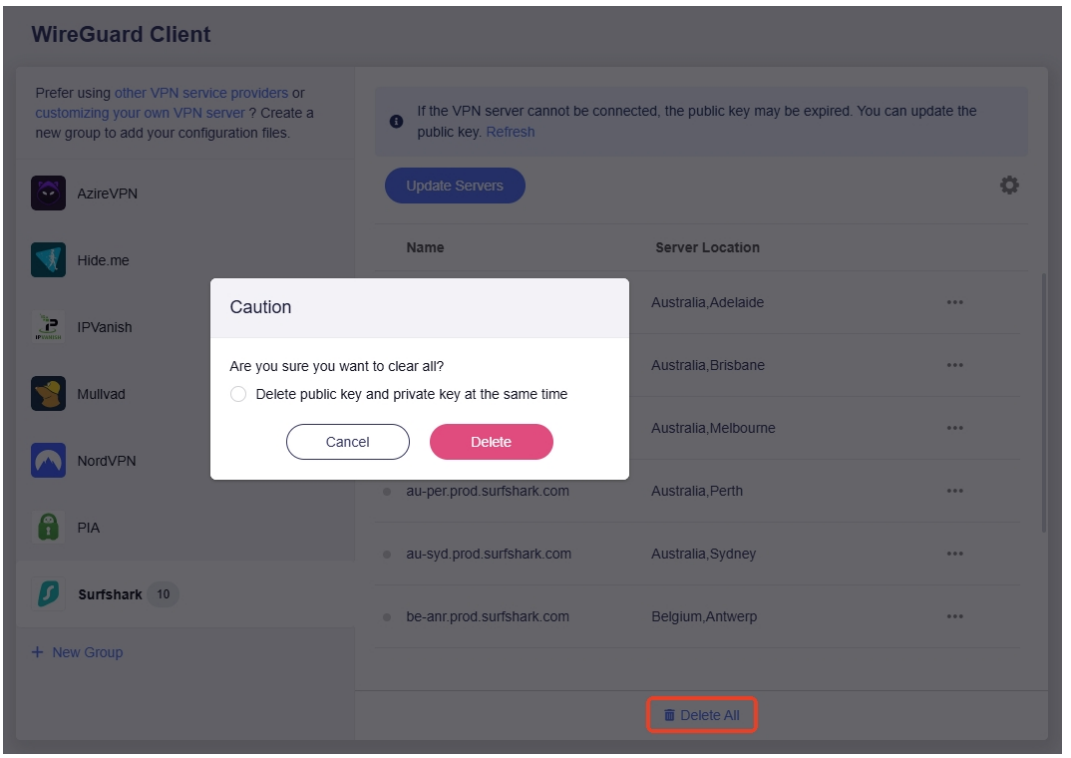
8. Aggiorna.

   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.

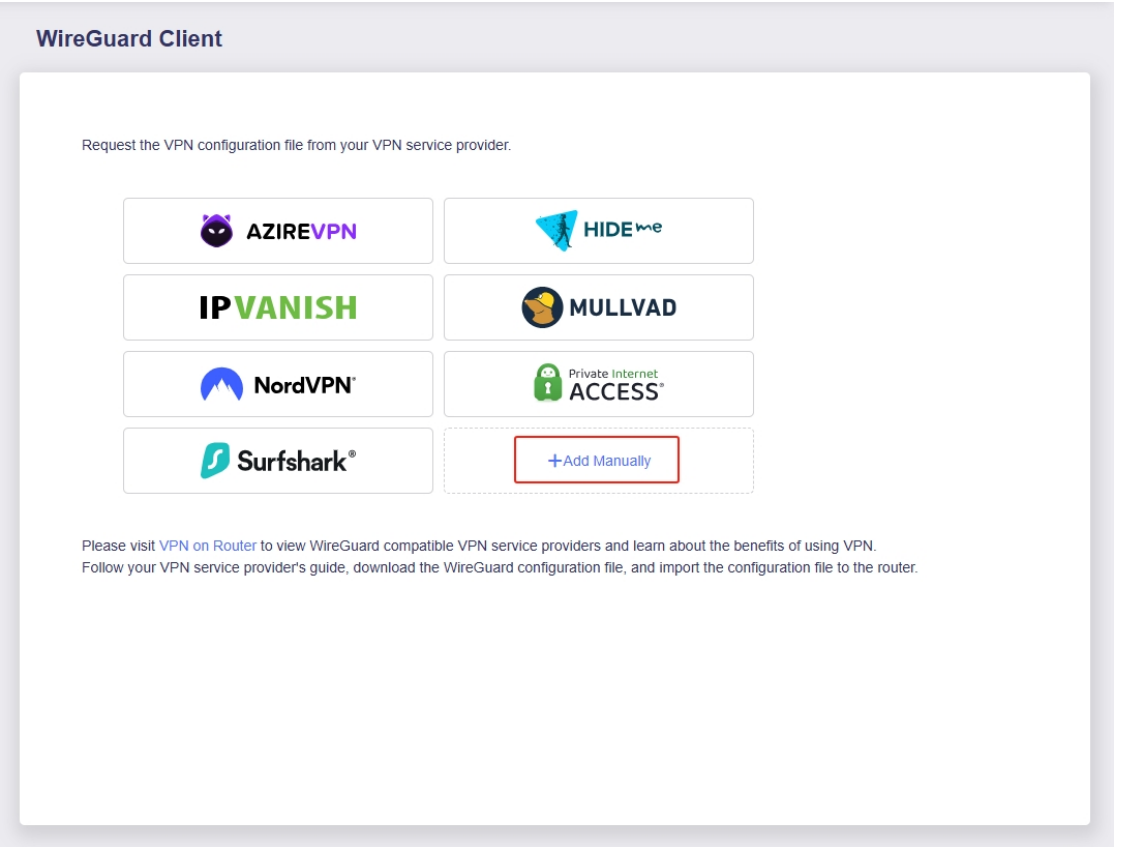


11.2.9 Configurazione manuale del client WireGuard (altri provider)

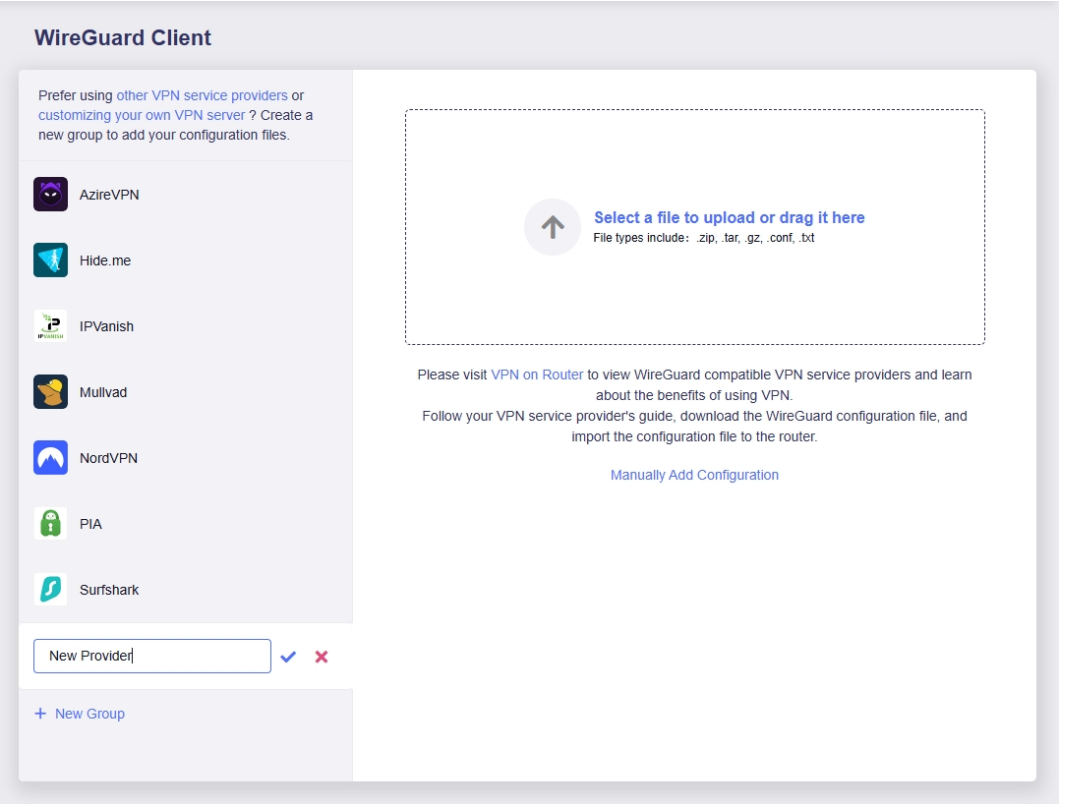
Se il tuo fornitore di servizi WireGuard non è integrato nel pannello di amministrazione web, visita prima il sito Web ufficiale del fornitore di servizi a cui sei iscritto per ottenere il file di configurazione. Quindi caricalo sul router per configurare uno WireGuard client. Se non sai come scaricare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

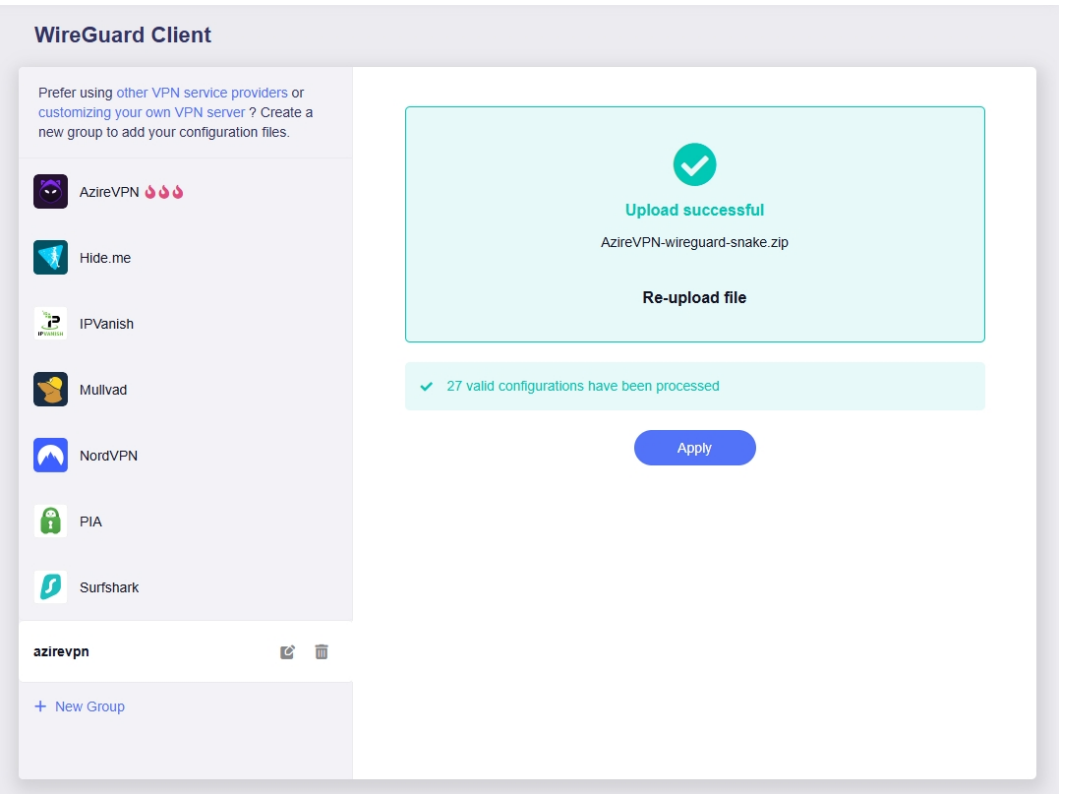
1. Accedi al pannello di amministrazione web del tuo router e vai a **VPN** > **Client WireGuard** > **Aggiungi manualmente**.



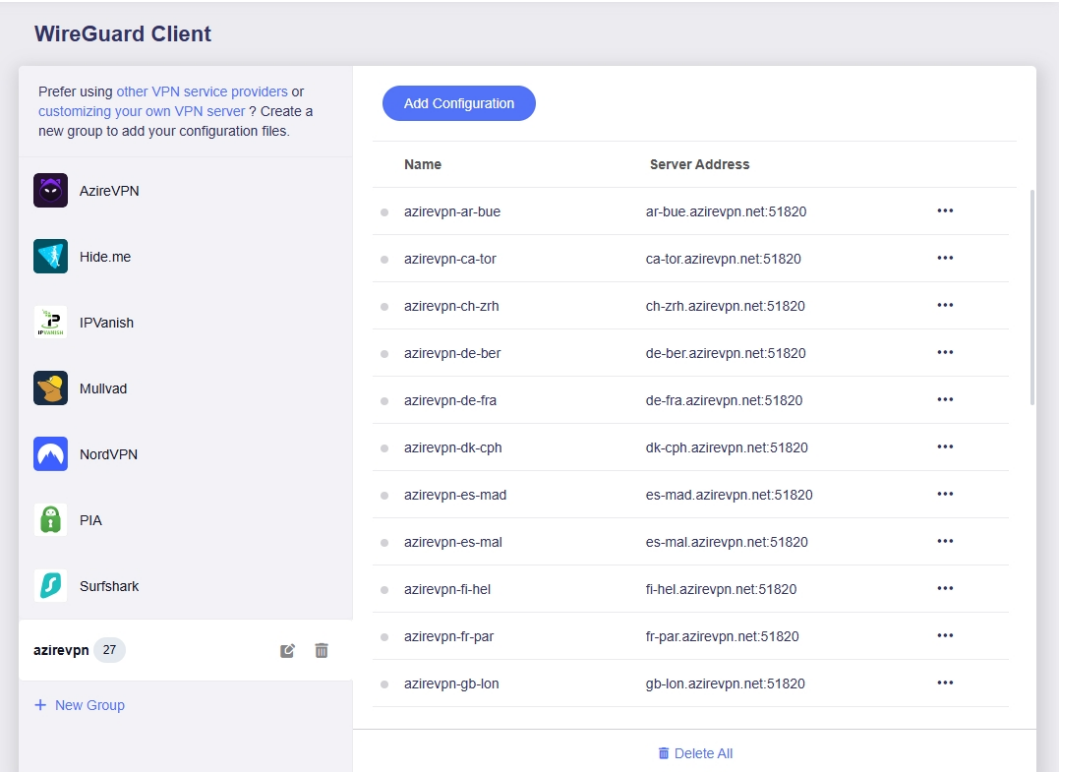
2. Verrà creato un gruppo nella barra laterale sinistra. Imposta un nome descrittivo per il gruppo.



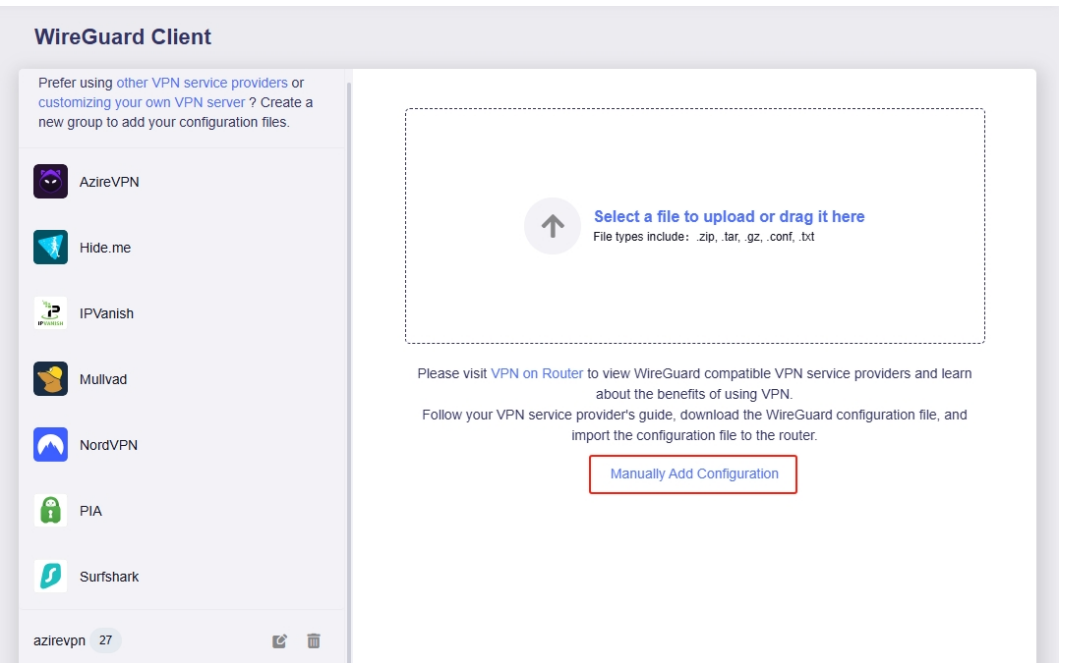
3. Fai clic sull'area di caricamento per caricare il file di configurazione WireGuard (formati supportati: zip, tar, gz, conf, txt) e fai clic su **Applica**.

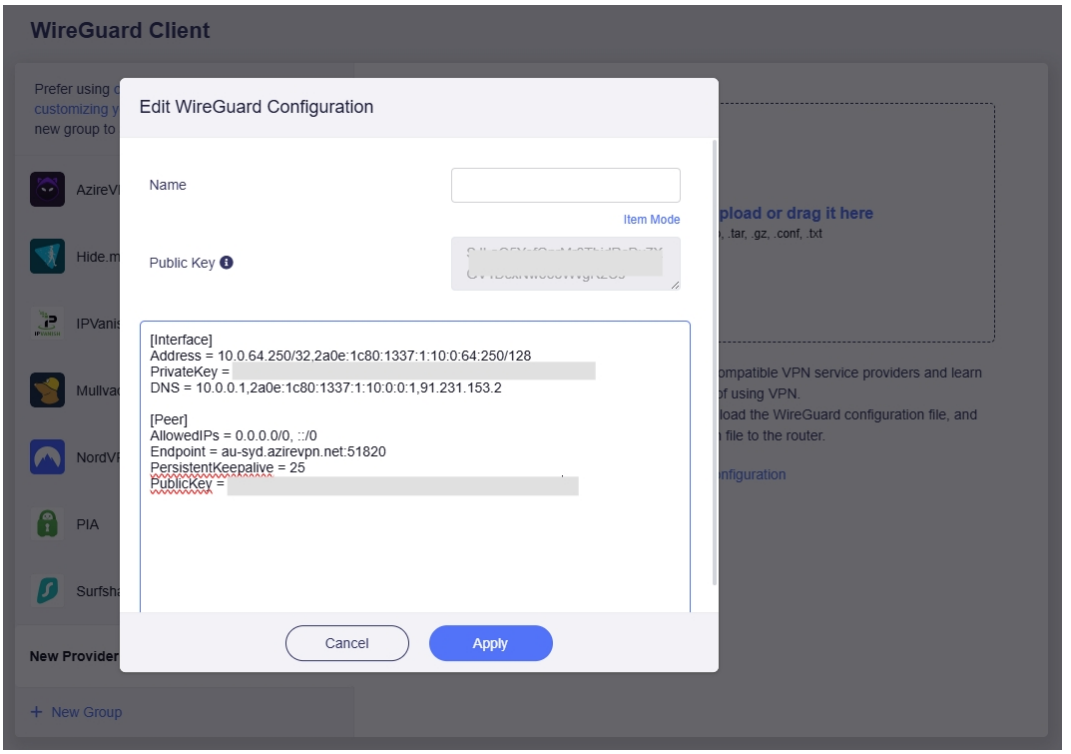


Se carichi un file compresso contenente più file di configurazione, verrà decompresso automaticamente, come mostrato di seguito.

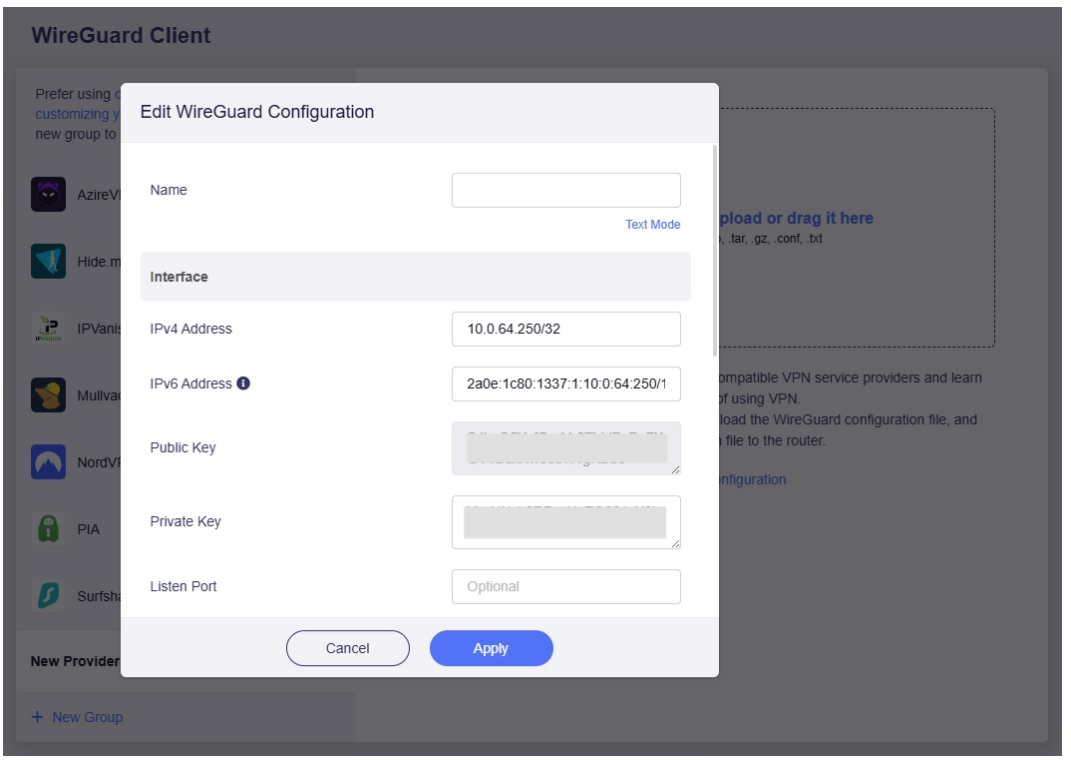


In alternativa, puoi fare clic su **Aggiungi manualmente la configurazione** nella parte inferiore dell'area di caricamento, aggiungere i dettagli della configurazione in formato testo e fare clic su **Applica**.

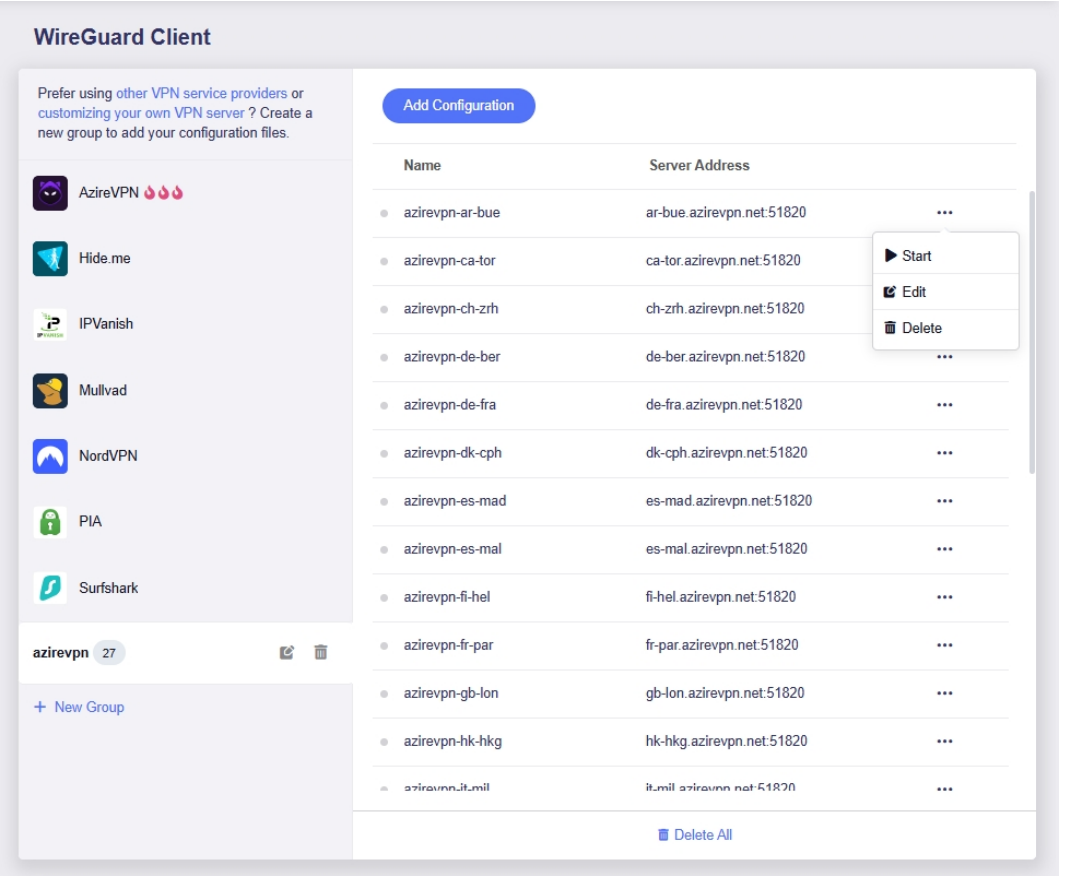




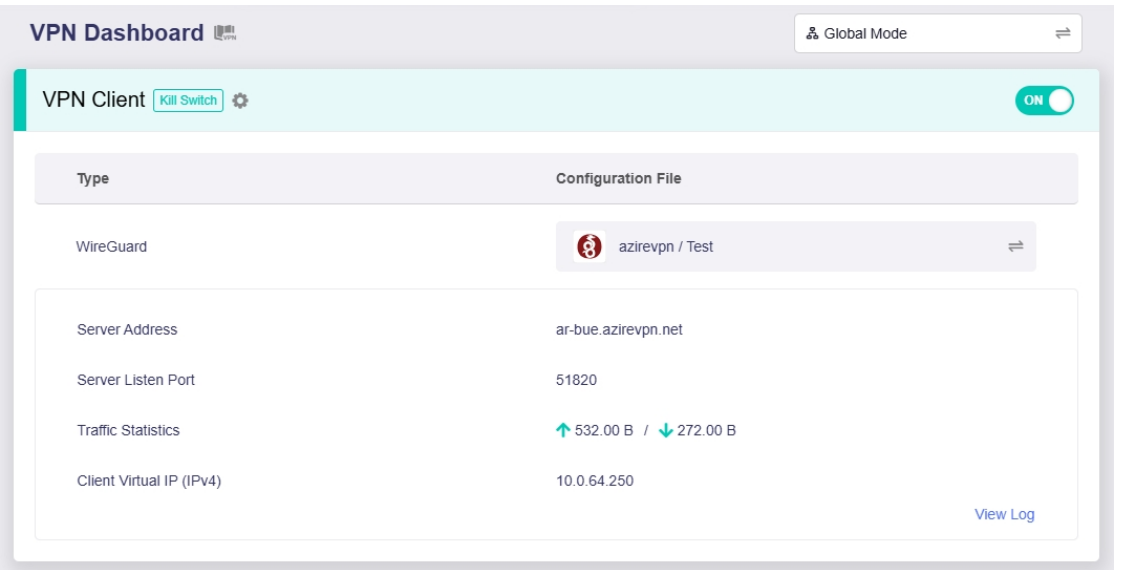
Per verificare ogni parametro, passa alla modalità Voce e controlla i dettagli della configurazione, quindi fai clic su **Applica**.



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 12

Rete

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

12.1 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.

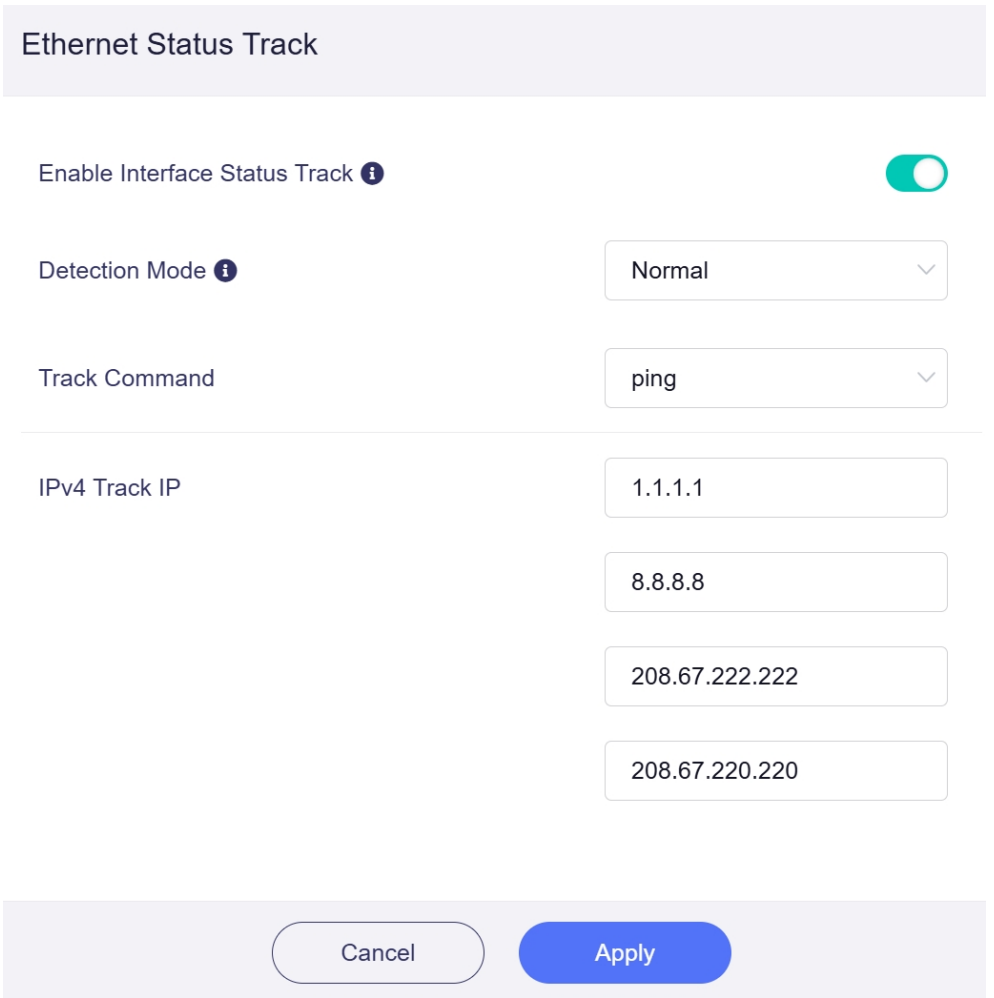
Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **Multi-WAN**. Questa pagina include due sezioni: Monitoraggio dello stato dell'interfaccia e Modalità Multi-WAN.

12.1.1 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.



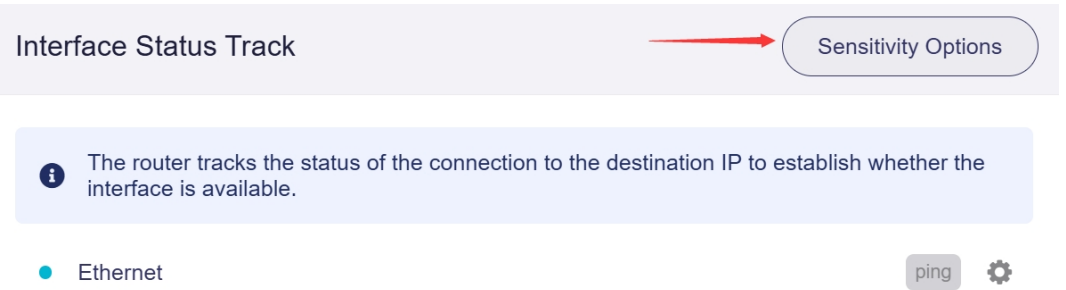
Nella sezione **Monitoraggio dello stato dell'interfaccia**, fai clic sull'icona a forma di ingranaggio a destra per accedere alle impostazioni di monitoraggio dello stato per ciascuna interfaccia di rete. Di seguito sono riportate le impostazioni di monitoraggio dello stato per l'interfaccia Ethernet.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



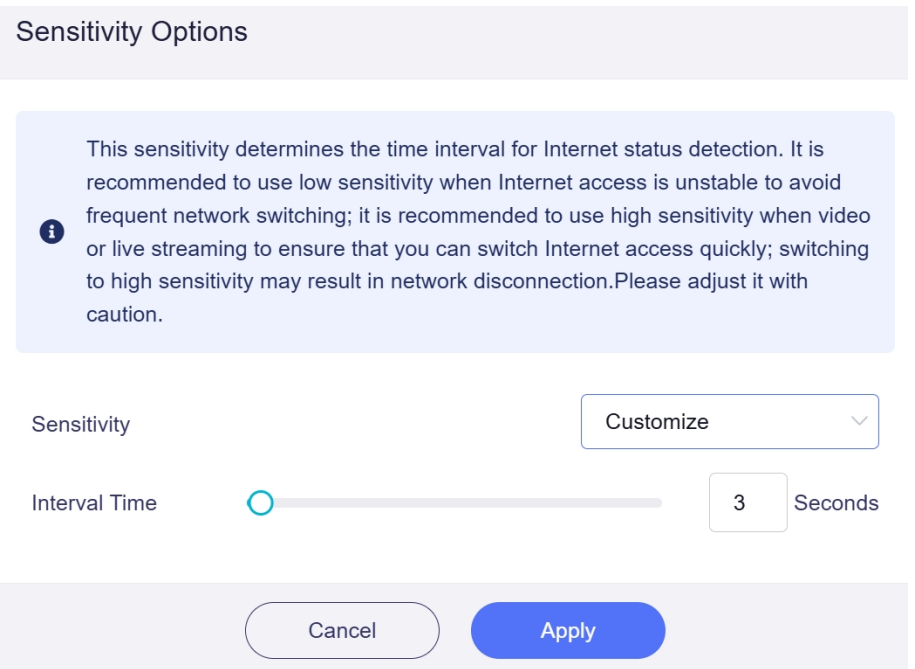
- **Abilita monitoraggio dello stato dell'interfaccia**: è abilitato per impostazione predefinita. Se disabilitato, il router determinerà lo stato dell'interfaccia in base alle condizioni fisiche (ad esempio, se il cavo Ethernet è collegato).
- **Modalità di rilevamento**: questa funzionalità è stata 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 IPv4 da monitorare, se necessario.

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



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



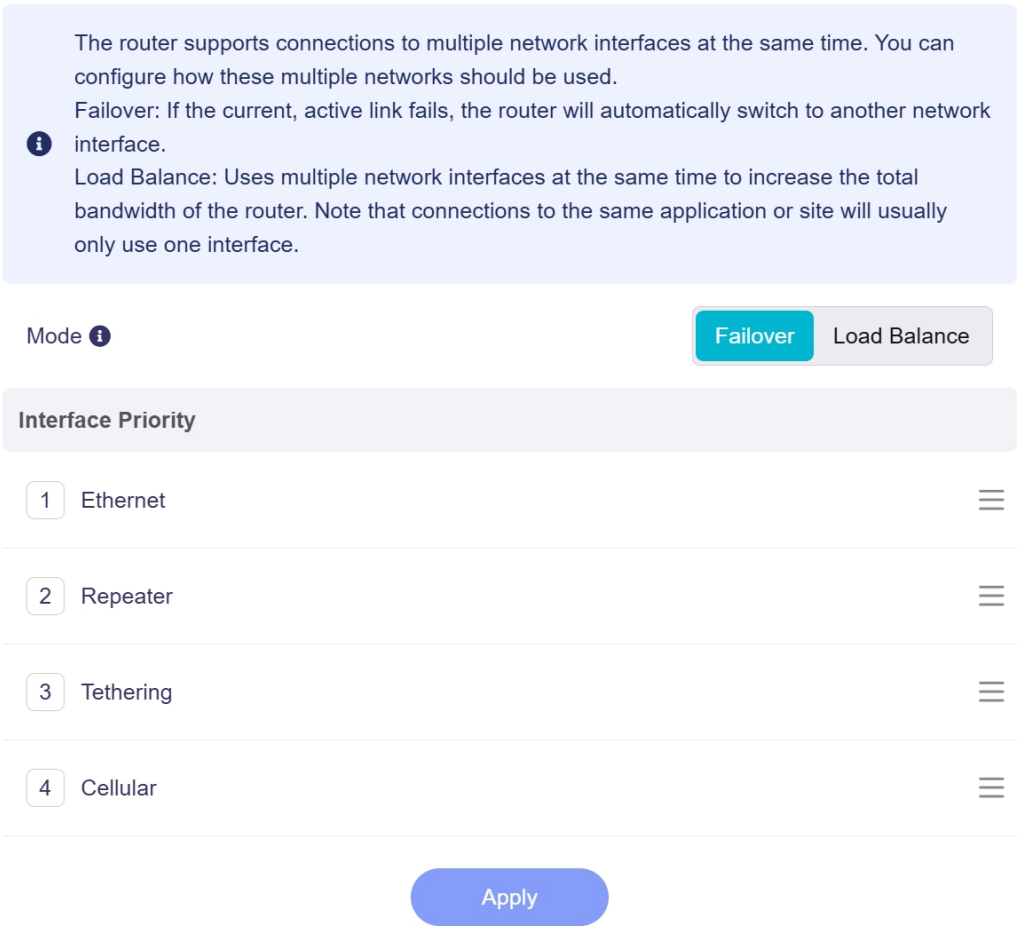
12.1.2 Modalità Multi-WAN

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.

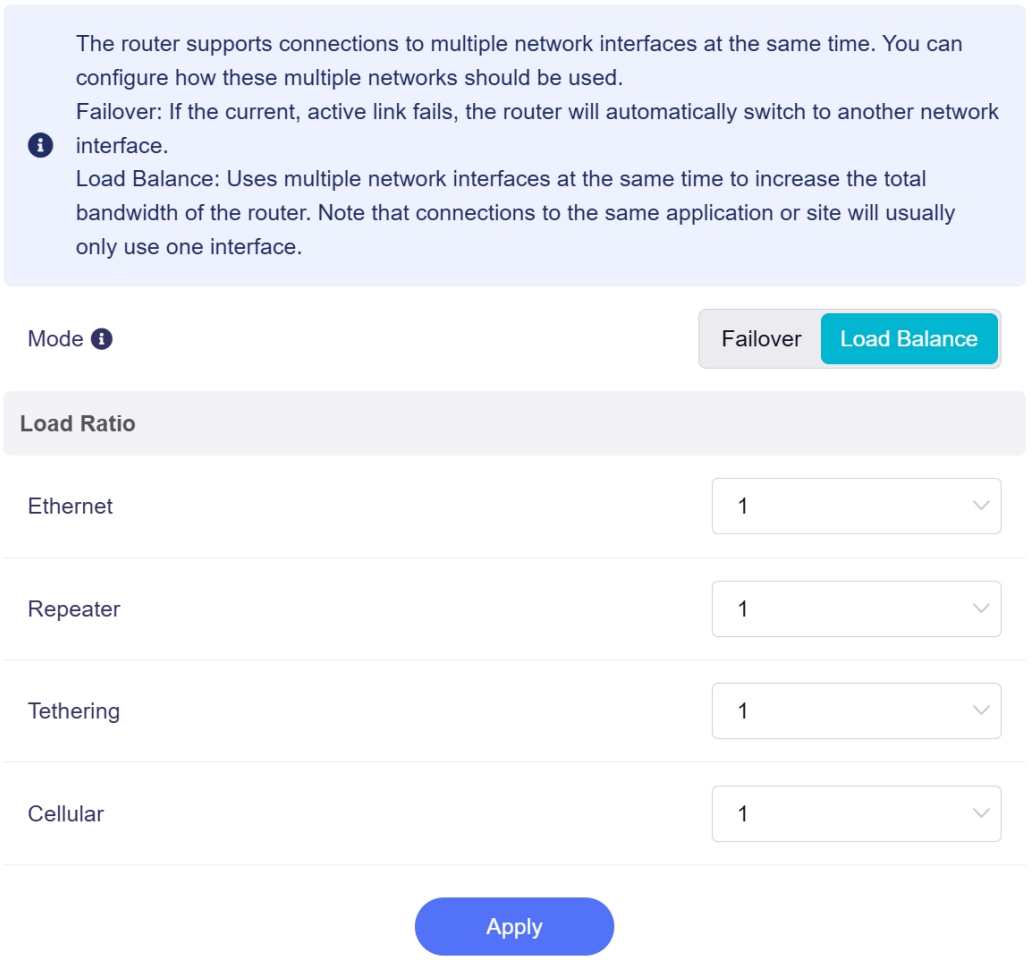
Puoi impostare livelli di priorità per ciascuna interfaccia: quando l'interfaccia attualmente utilizzata fallisce, il router passa alla successiva interfaccia disponibile con la priorità più alta. Una volta ripristinata una connessione con priorità più alta, il router tornerà automaticamente ad essa.



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



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

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

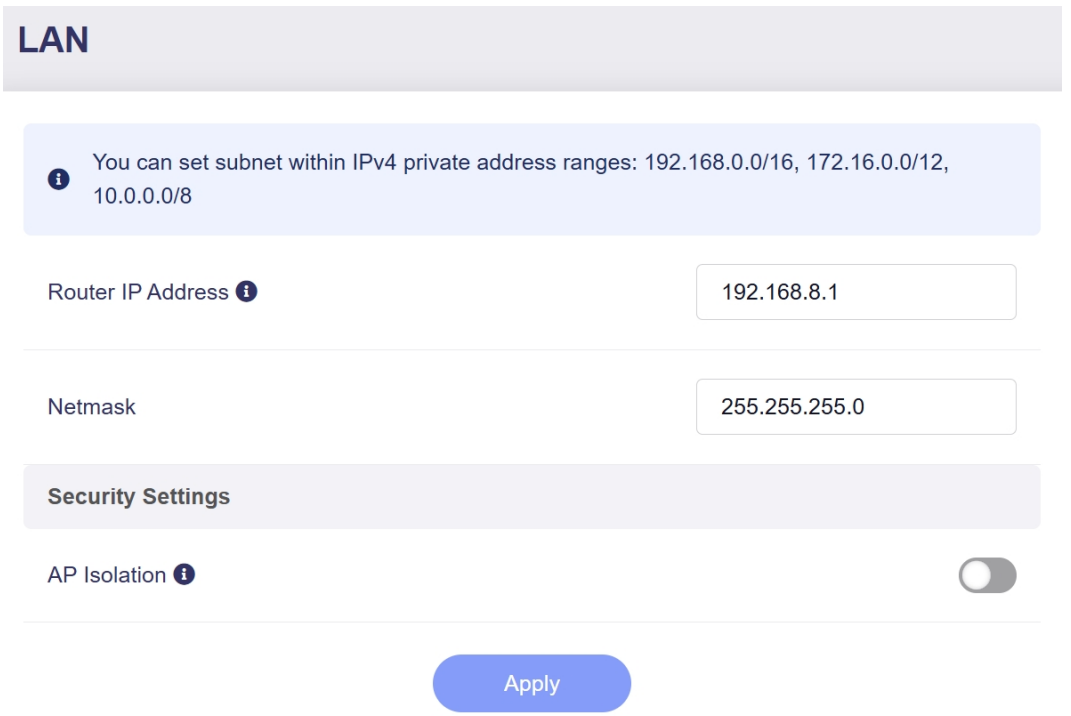
12.2 LAN

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.

12.2.1 Impostazioni di base

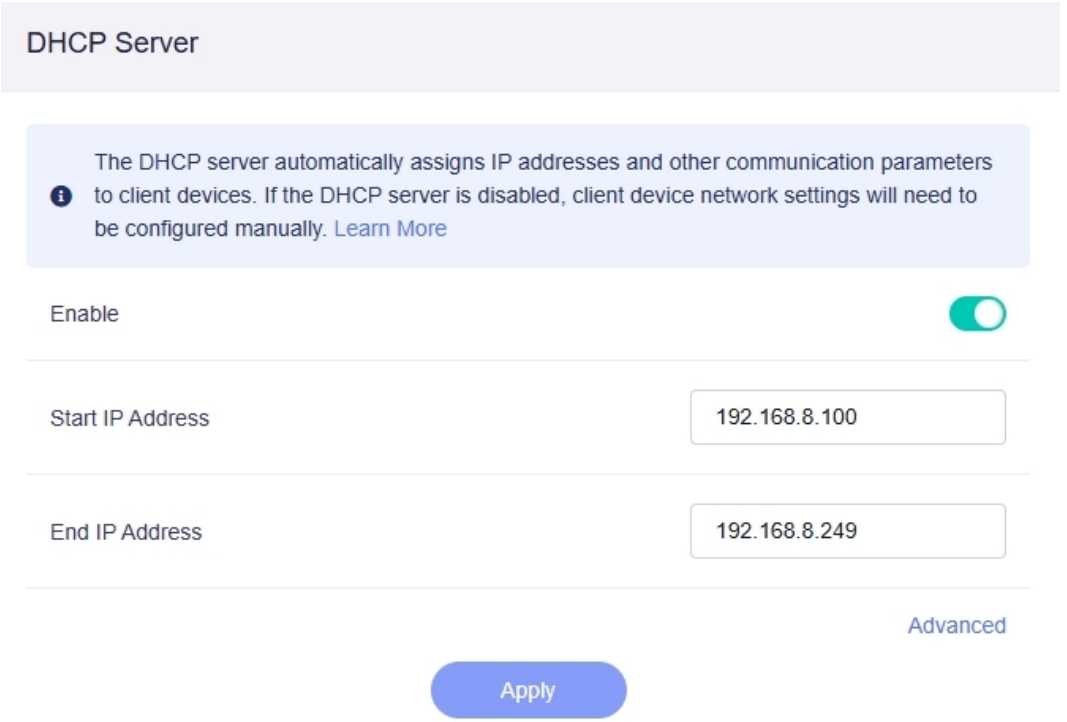
Le impostazioni di base includono l'indirizzo IP del router e Maschera di rete. È possibile impostare la sottorete all'interno degli intervalli di indirizzi privati IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



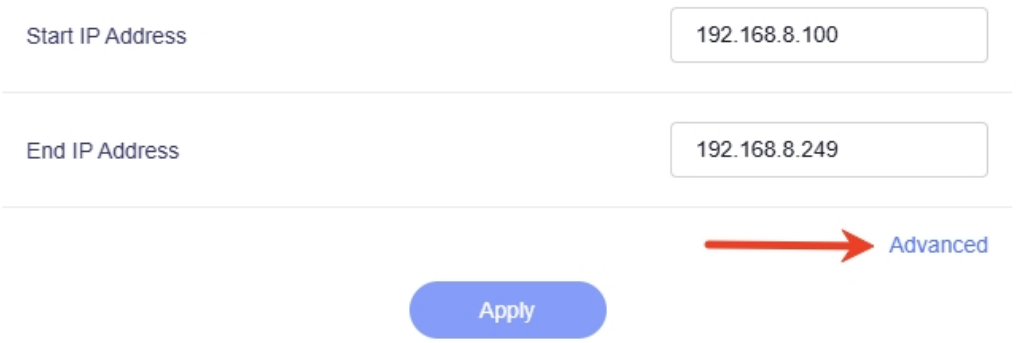
- **Indirizzo IP del router**: questo è l'indirizzo inserito nella barra degli indirizzi del browser per accedere al pannello di amministrazione del router. Per impostazione predefinita è 192.168.8.1 e può essere modificato se è in conflitto con la rete upstream.
- **Maschera di rete**: sono disponibili due opzioni: 255.255.255.0 e 255.255.0.0.
- **Isolamento AP**: puoi isolare i dispositivi client in un segmento di rete separato. Questi dispositivi non saranno in grado di comunicare con altri dispositivi sulla stessa rete.

12.2.2 Server DHCP

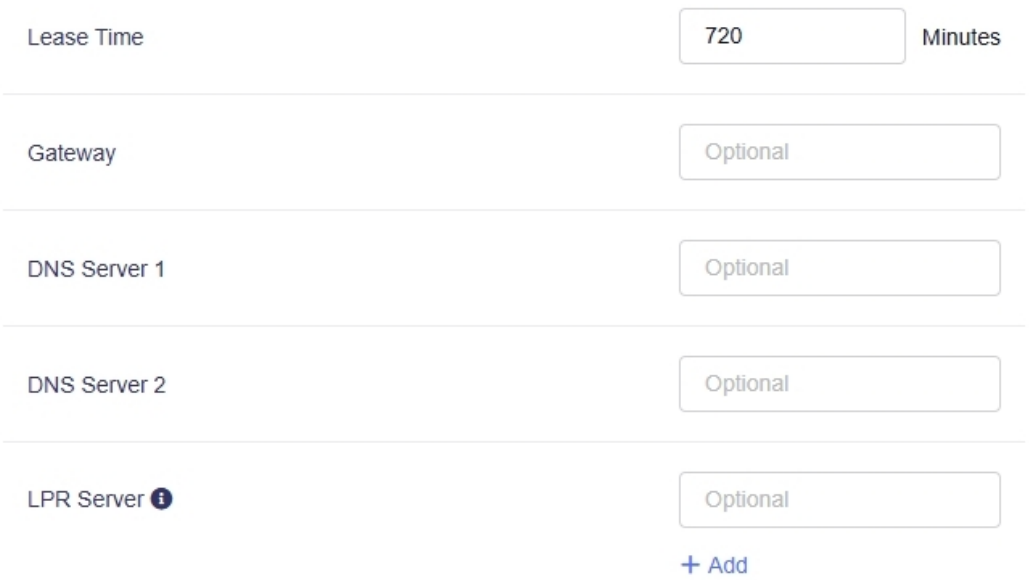
Il server DHCP assegna automaticamente indirizzi IP e altri parametri di comunicazione a ciascun client connesso. Il server DHCP del router GL.iNet è abilitato per impostazione predefinita e il pool di indirizzi IP del server DHCP varia da 192.168.8.100 a 192.168.8.249. Se necessario, è possibile personalizzare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



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



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



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

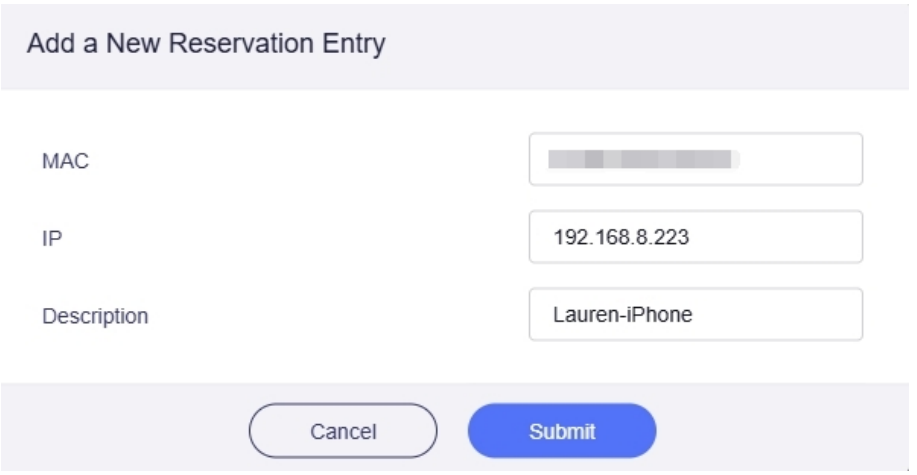
Nota: se il server DHCP è disabilitato, è necessario configurare manualmente l'IP statico e altri parametri di comunicazione per ciascun client. Vedi qui per i dettagli.

12.2.3 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, se necessario.

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



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



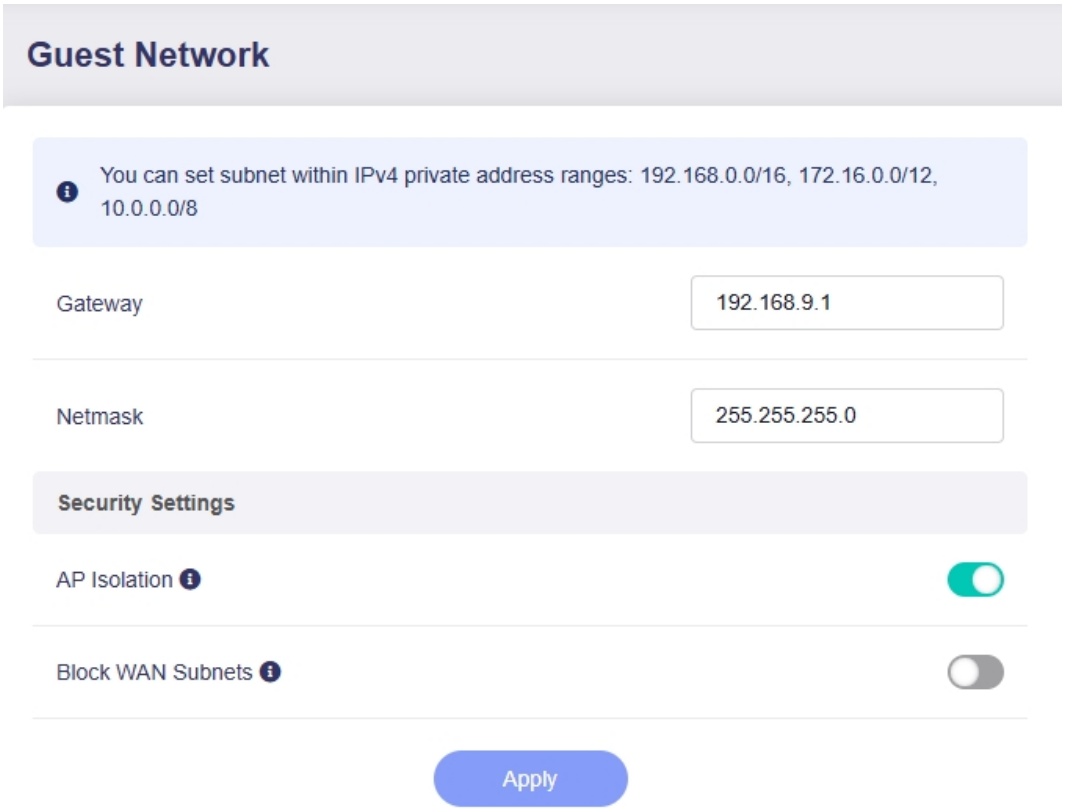
12.3 Rete ospiti

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

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

12.3.1 Impostazioni di base

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

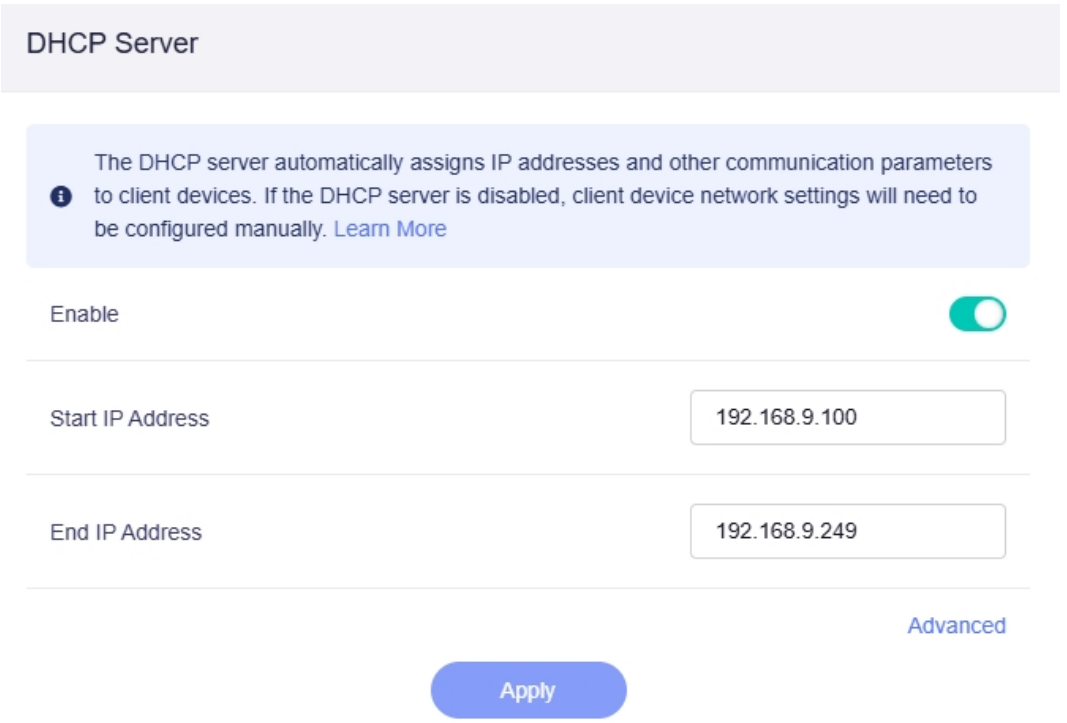


- **Gateway**: di default è 192.168.9.1 e può essere modificato se necessario, ma non deve entrare in conflitto con il gateway della rete principale.
- **Maschera di rete**: sono disponibili due opzioni: 255.255.255.0 e 255.255.0.0.
- **Isolamento AP**: viene utilizzato per isolare i client della rete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

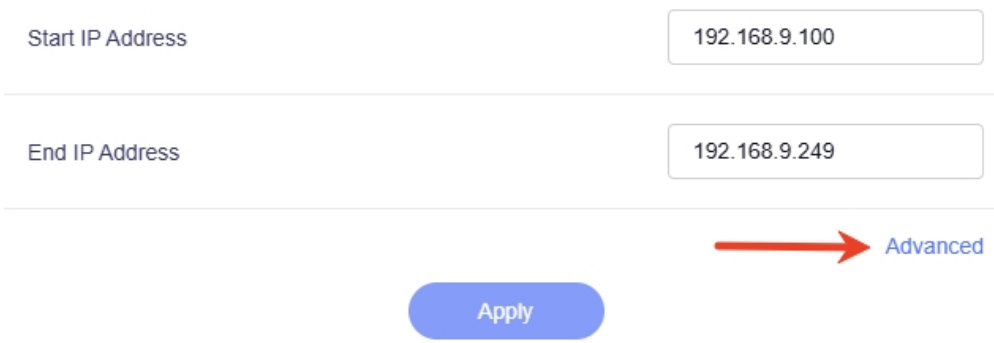
- **Blocca sottoreti WAN**: se abilitato, la rete ospiti non sarà in grado di accedere alla rete upstream o al segmento di rete corrispondente.

12.3.2 Server DHCP

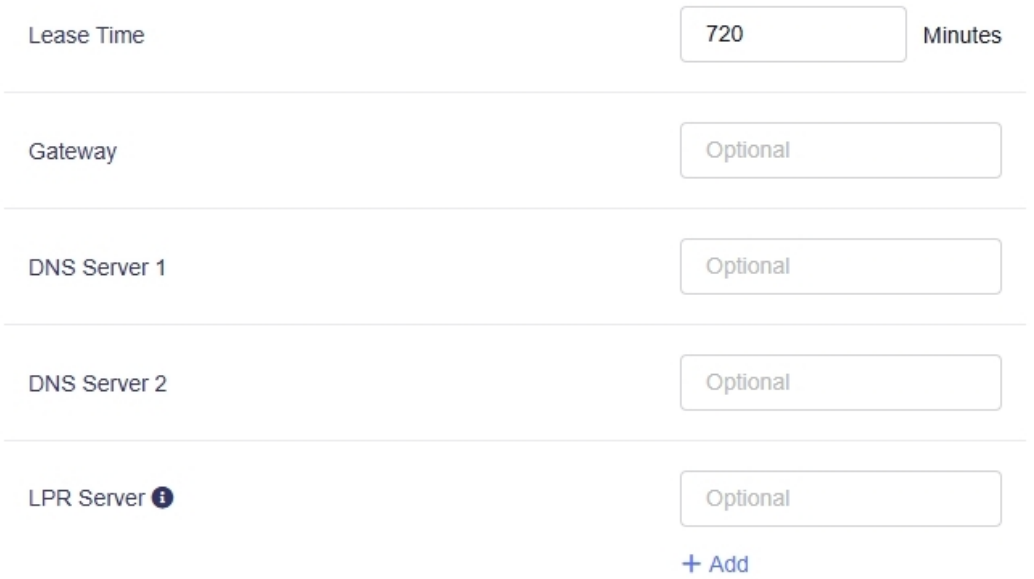
Poiché la rete ospiti è disabilitata per impostazione predefinita, il suo server DHCP è disabilitato e nascosto finché non viene abilitato manualmente.
Se abilitato, il server DHCP assegna automaticamente indirizzi IP e altri parametri di comunicazione a ciascun client connesso. Il pool di indirizzi IP del server DHCP per la rete ospiti varia da 192.168.9.100 a 192.168.9.249. Se necessario, puoi personalizzare l'intervallo di indirizzi.



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



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



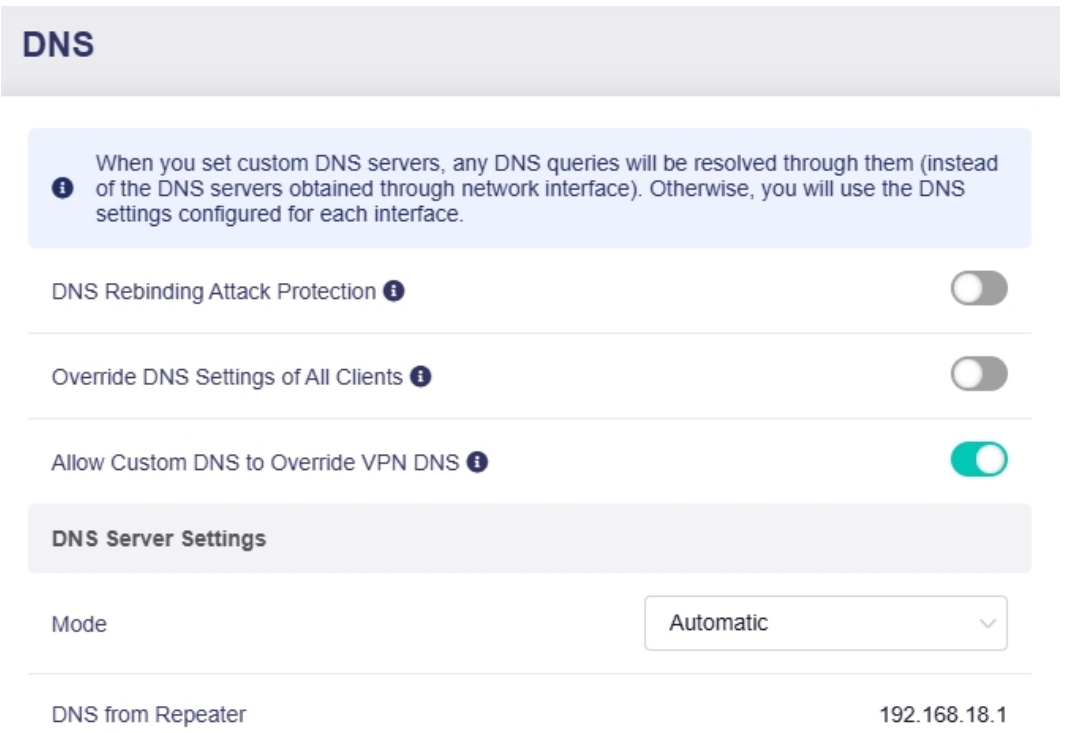
- **Durata del lease**: la durata durante la quale un dispositivo può utilizzare un indirizzo IP assegnato tramite DHCP della rete ospiti.
- **Gateway**: il componente router che instrada il traffico tra la rete ospiti e le reti esterne (ad esempio Internet).
- **Server DNS 1**: il server primario responsabile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

12.4 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) nel 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.

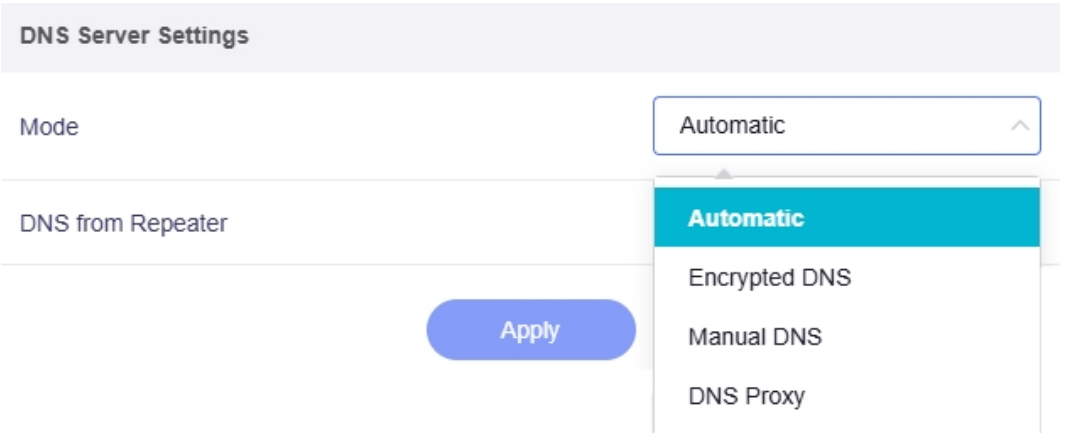
Accedi al pannello di amministrazione web del tuo router e vai su **RETE** > **DNS**. Questa pagina ti consente di configurare le impostazioni relative al DNS, incluse le opzioni di sicurezza, le modalità server e le regole di priorità DNS per diversi scenari di rete.



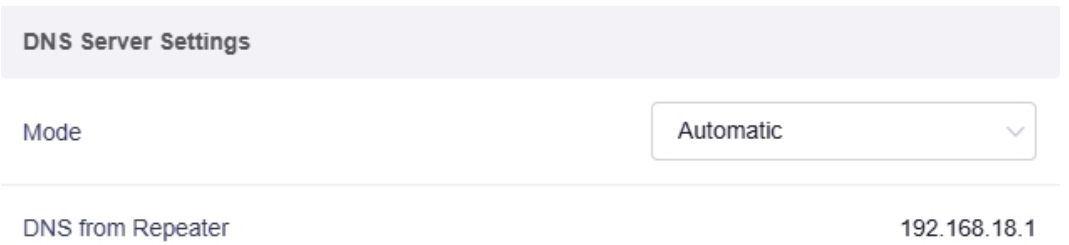
- **Protezione dagli attacchi di riassociazione DNS**: protegge dagli attacchi di riassociazione DNS bloccando i tentativi dannosi di risoluzione DNS. Tieni presente che abilitarlo potrebbe causare un errore di ricerca DNS privato; disabilitalo se la tua rete utilizza un captive portal (ad esempio, pagine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

12.4.1 Impostazioni del server DNS

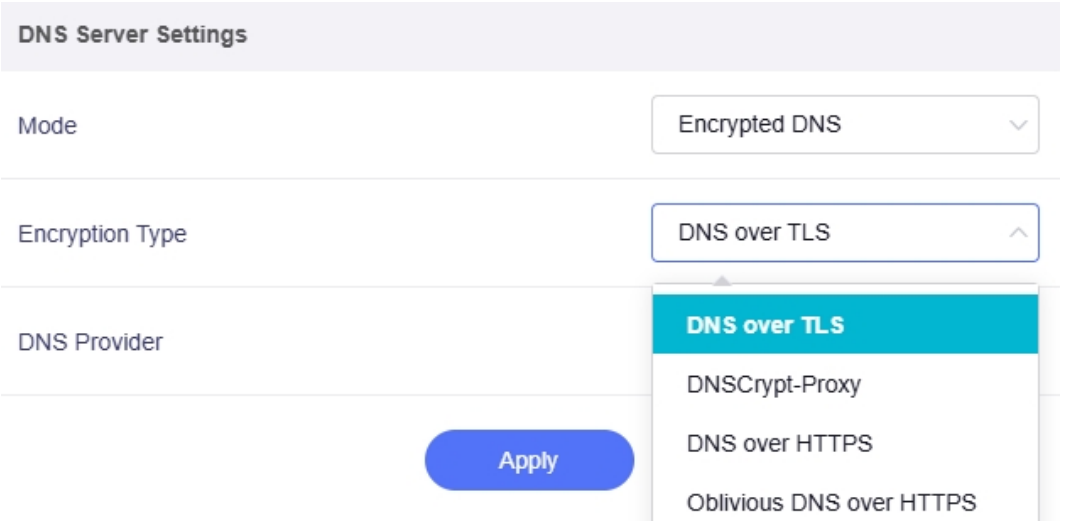
Esistono quattro modalità per il server DNS: automatico, DNS crittografato, DNS manuale e proxy DNS.



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

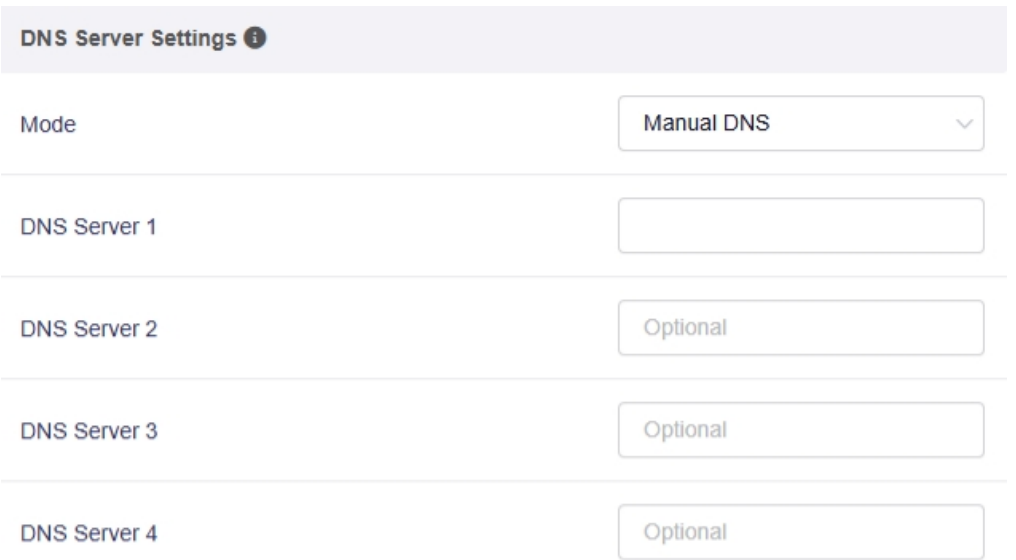


2. **DNS crittografato**: se selezionato, il router utilizzerà protocolli crittografati per elaborare le query DNS, proteggendo i dati di risoluzione da intercettazioni o manomissioni.
   Ha quattro tipi di crittografia: DNS su TLS, DNSCrypt-Proxy, DNS su HTTPS e Oblivious DNS su HTTPS.



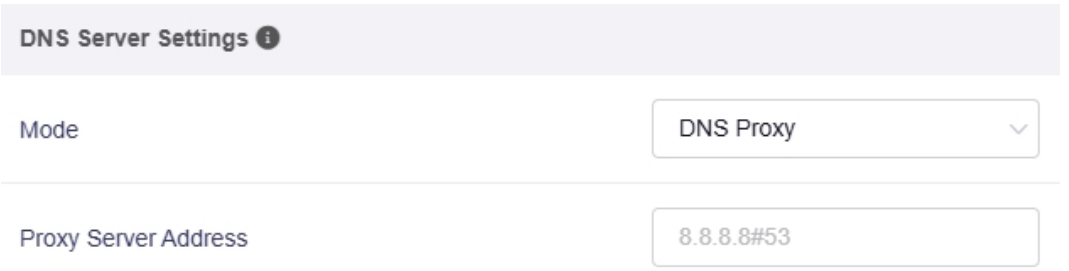
   - Per DNS su TLS, seleziona un provider DNS tra Control D, NextDNS e Cloudflare.
   - Per gli altri tre (ovvero DNSCrypt-Proxy, DNS over HTTPS e Oblivious DNS over HTTPS), seleziona almeno un server DNS dal repository. È possibile selezionare fino a server 8. Quando vengono selezionati più server, il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

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



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

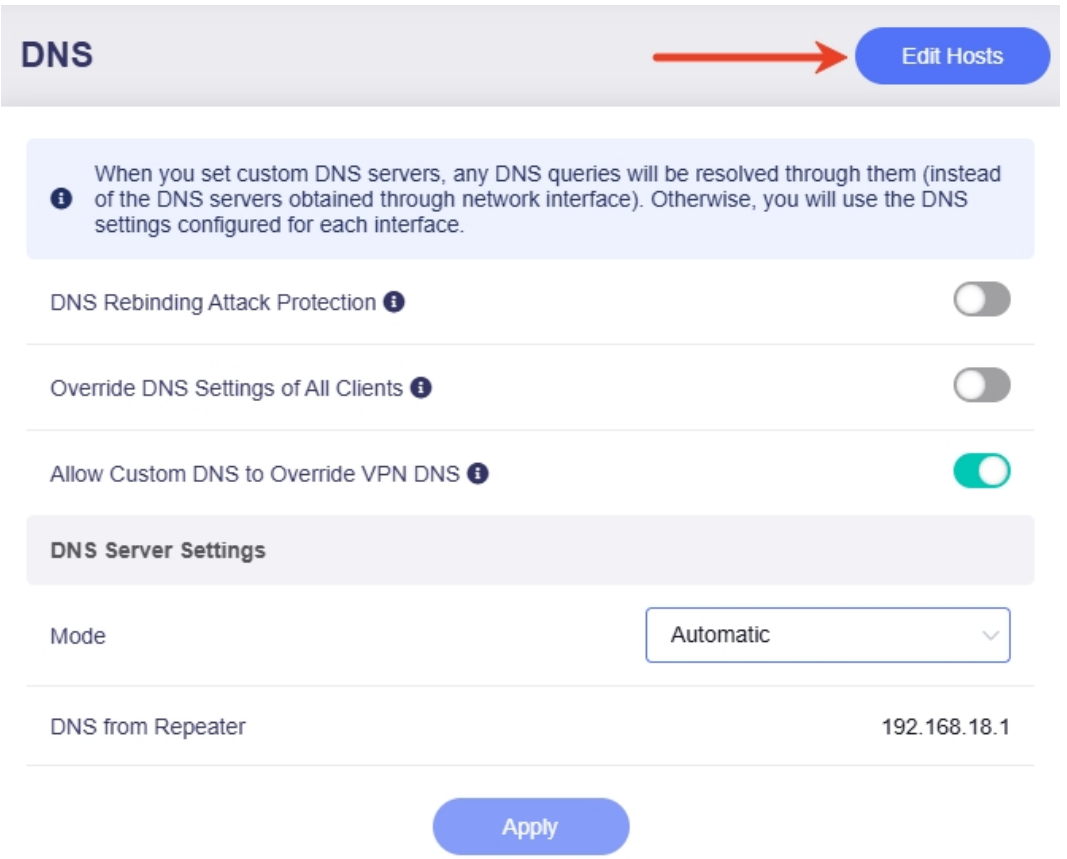
4. **Proxy DNS**: se selezionato, il router inoltra tutte le query DNS tramite un server proxy, consentendo la risoluzione tramite l'ambiente di rete del proxy per esigenze di accesso specifiche.



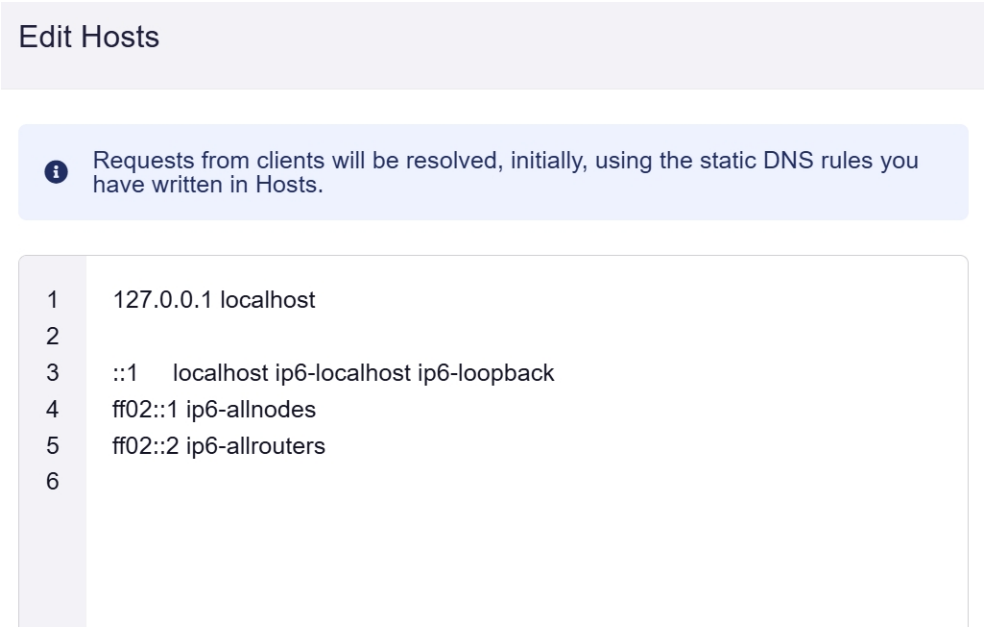
12.4.2 Modifica del file hosts

Puoi definire regole di risoluzione DNS statiche, se necessario.

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



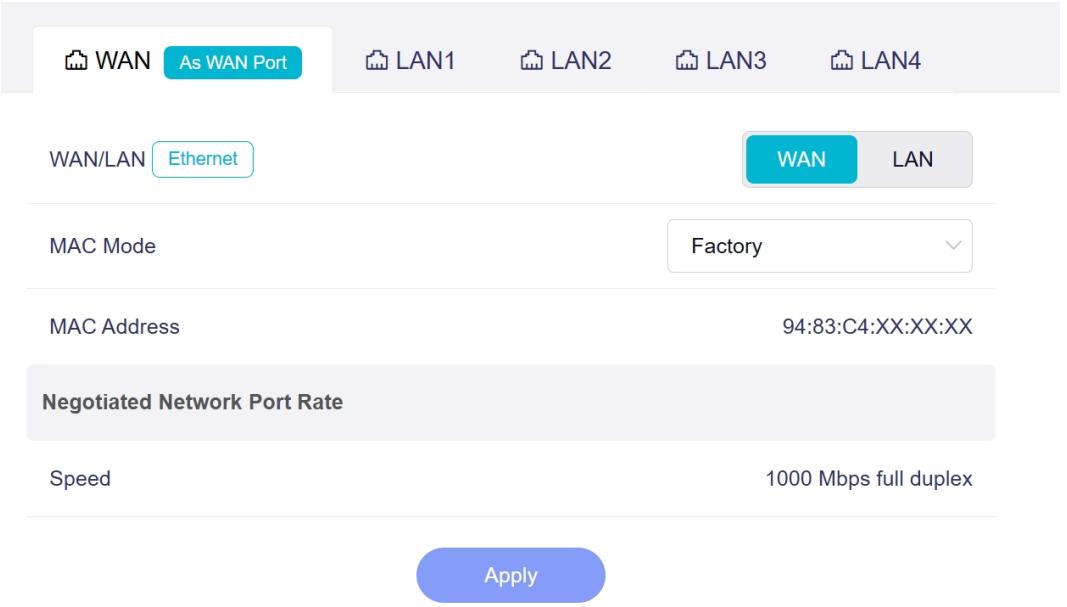
Le richieste dei client verranno risolte preferenzialmente utilizzando le regole DNS statiche scritte qui, consentendoti di mappare manualmente gli indirizzi IP sui nomi host (ad esempio, le voci predefinite come 127.0.0.1 localhost per il loopback locale) per il controllo personalizzato della risoluzione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



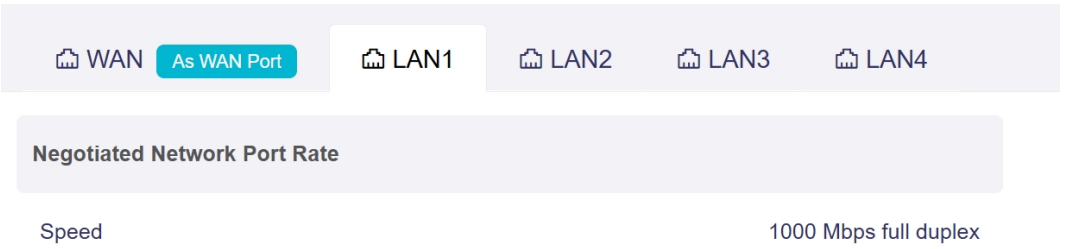
12.5 Porta Ethernet

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.



Le sezioni LAN mostrano la velocità negoziata per ciascuna porta LAN corrispondente.



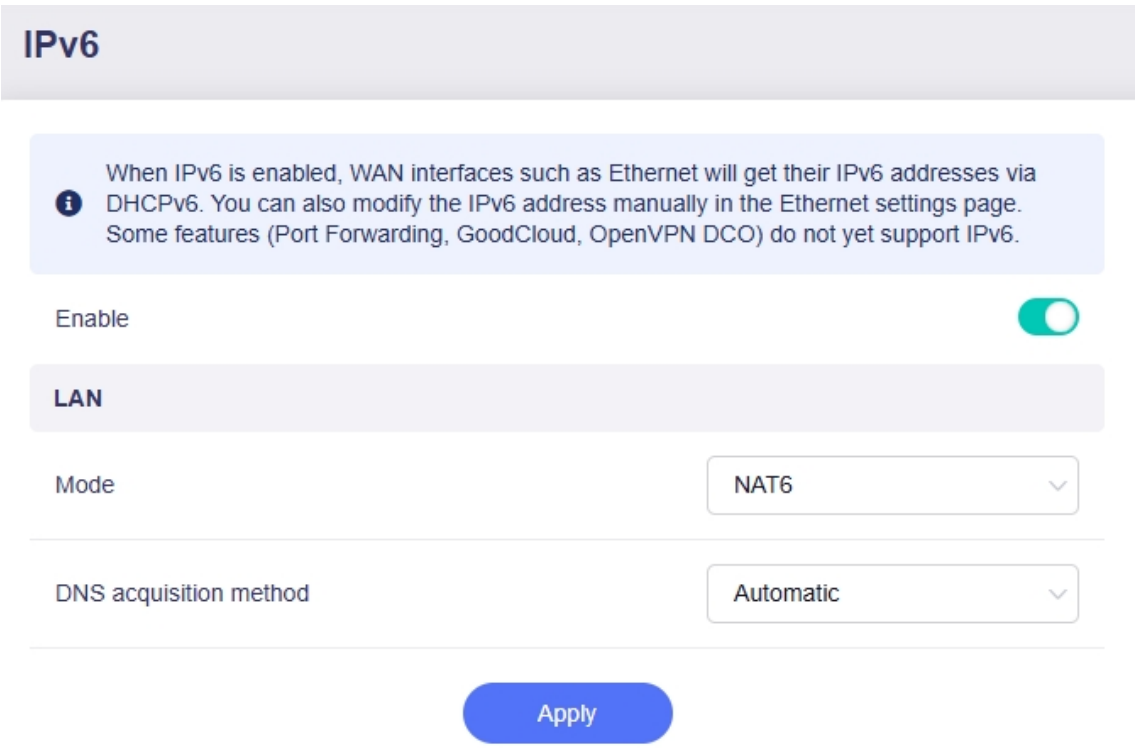
Nota: la velocità negoziata delle porte WAN e LAN viene visualizzata solo quando un cavo Ethernet è collegato. Dipende sia dalla porta Ethernet sia dal cavo Ethernet.

12.6 IPv6

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

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

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



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

12.6.1 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.

12.6.2 Metodo di acquisizione DNS

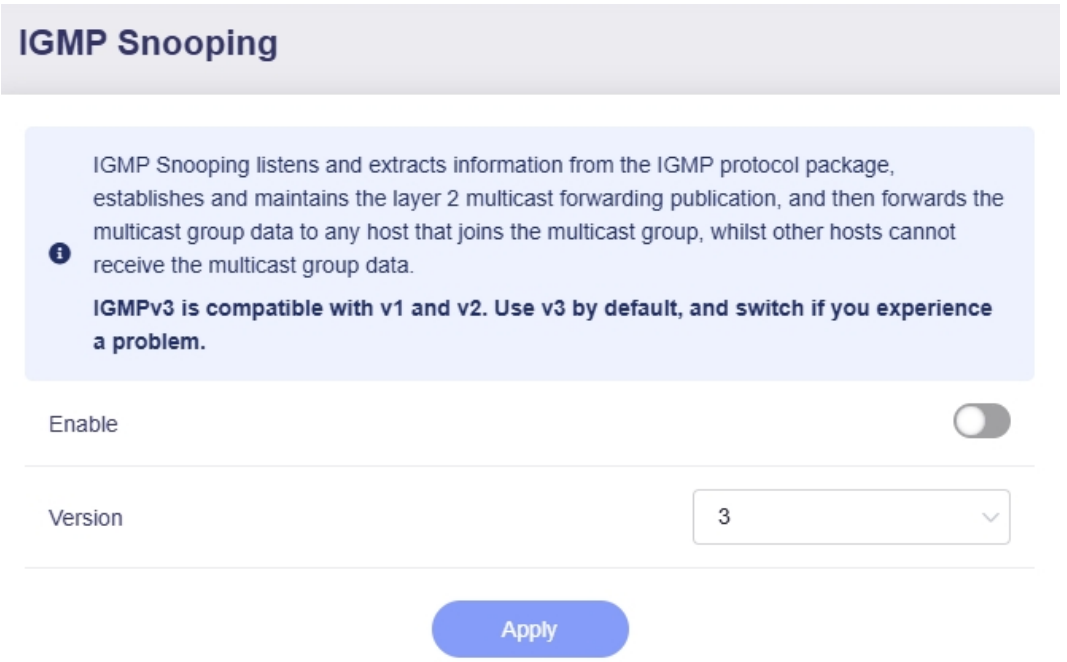
Determina il modo in cui il router ottiene gli indirizzi del server DNS IPv6. Sono disponibili due opzioni: Automatico e Manuale.

- **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.

12.7 IGMP Snooping

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

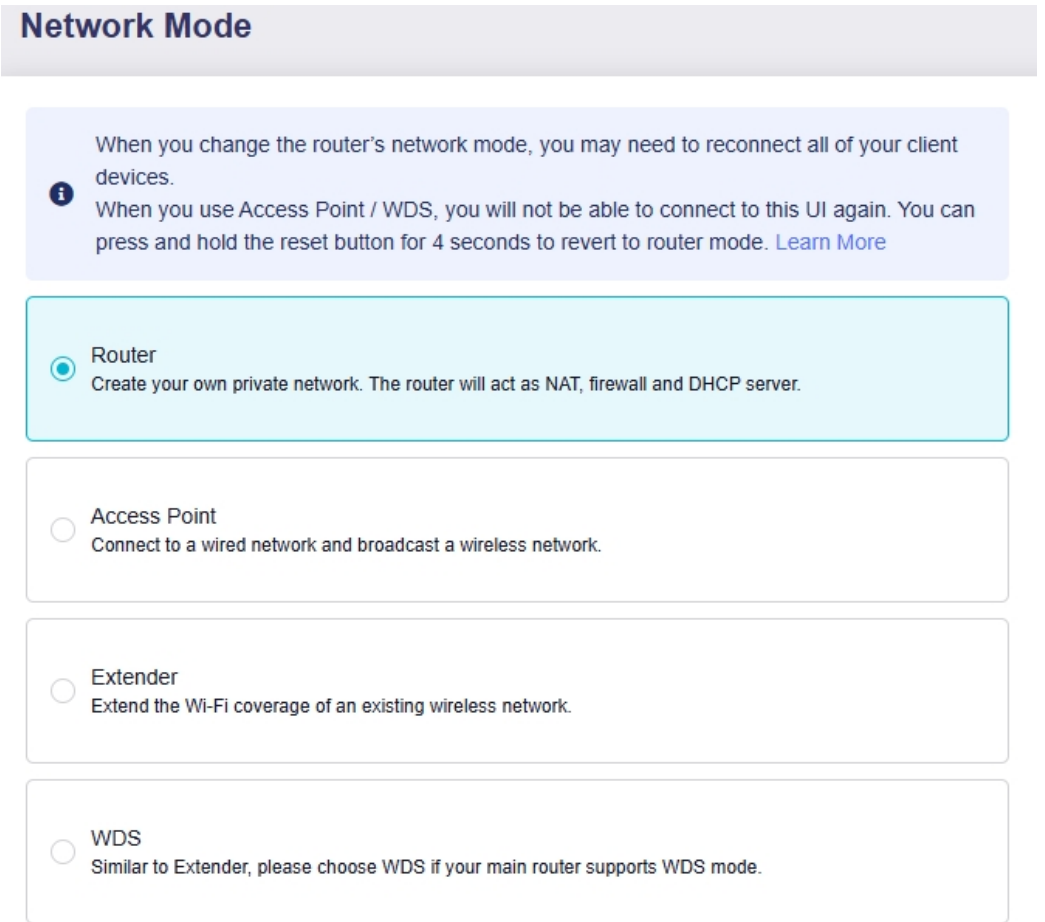
Accedi al pannello di amministrazione web del tuo router e vai a **RETE** > **IGMP Snooping**. Puoi abilitarlo per utilizzare la funzione multicast sul tuo router, se necessario.



12.8 Modalità di rete

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

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



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

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

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

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

Nota:

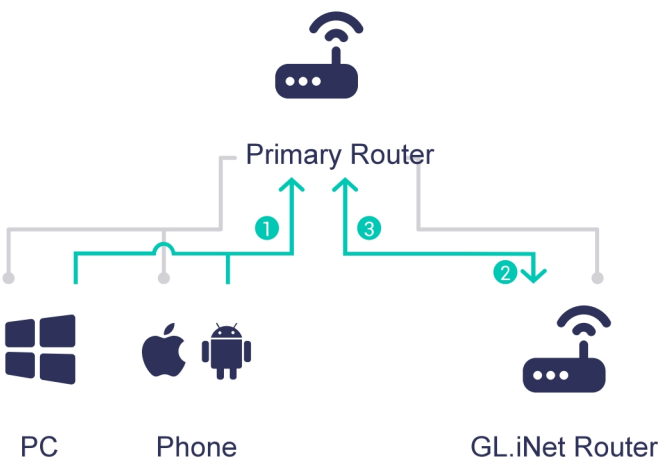
1. Quando la modalità di rete viene modificata, tutti i dispositivi client devono riconnettersi al router per una connettività di rete stabile.
2. **In modalità Punto di accesso / WDS, non sarai in grado di accedere al pannello di amministrazione web utilizzando l'indirizzo IP originale**. È invece necessario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

12.9 Gateway drop-in

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

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

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



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

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

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

Puoi abilitare Gateway drop-in per tutti o dispositivi specifici collegati al router principale. Vedi questo collegamento per maggiori dettagli.

Capitolo 13

Controllo del traffico

Questo capitolo introduce il controllo parentale, fornendo uno strumento dedicato per filtrare i siti Web e impostare limiti di utilizzo.

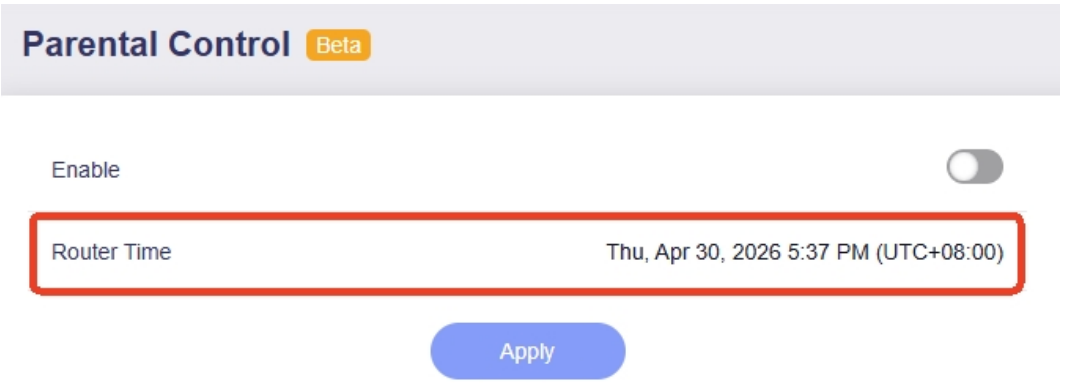
13.1 Controllo parentale

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.

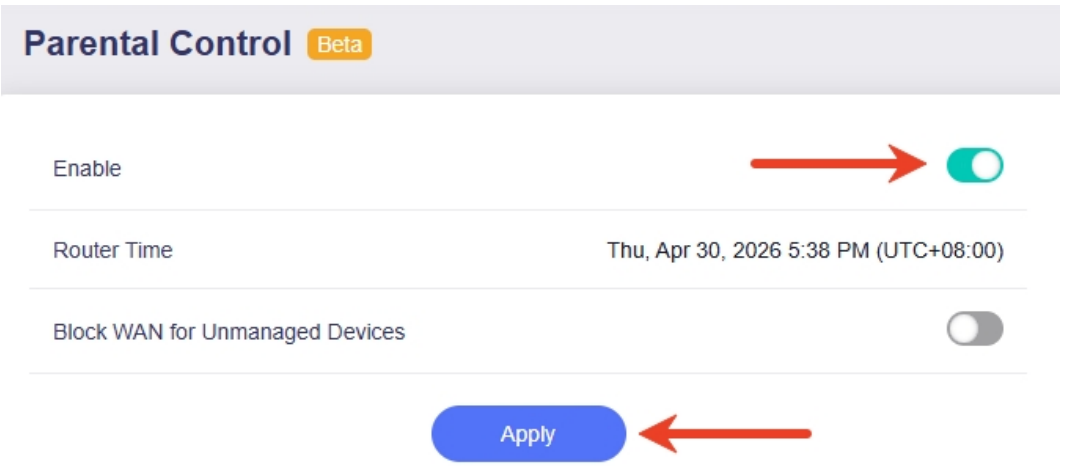
13.1.1 Configurazione rapida

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

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



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



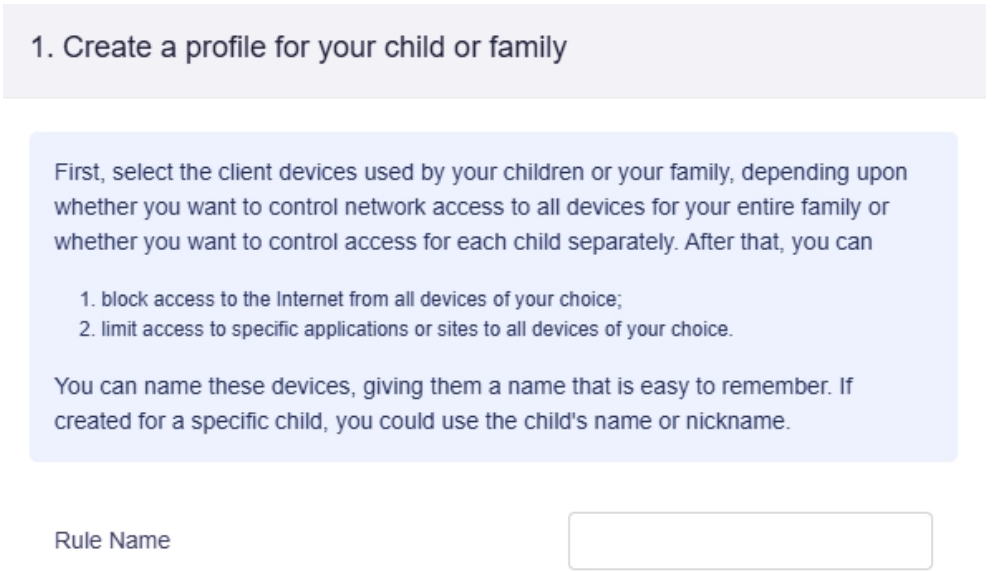
- **Blocca WAN per dispositivi non gestiti**: blocca l'accesso a Internet per tutti i dispositivi che non sono presenti nell'elenco Controllo parentale.

Ecco un caso d'uso come riferimento.

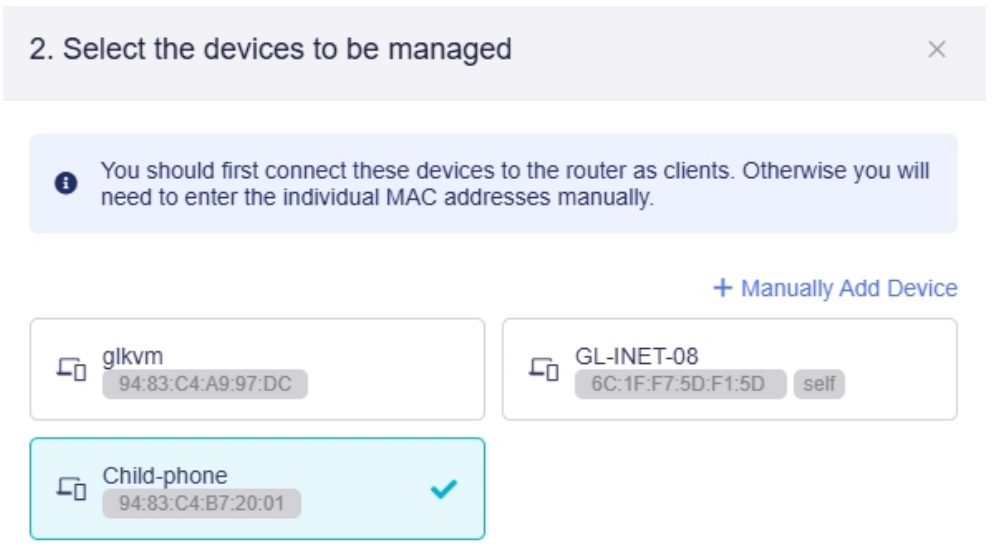
Scenario: i dispositivi in questo profilo possono accedere a Internet solo per studiare da 8 AM a 11 AM nei giorni feriali e per giocare da 6 PM a 8 PM nei fine settimana. L'accesso a Internet è bloccato per impostazione predefinita in tutti gli altri momenti.

Procedura di configurazione:

1. Crea un profilo e personalizza un nome.

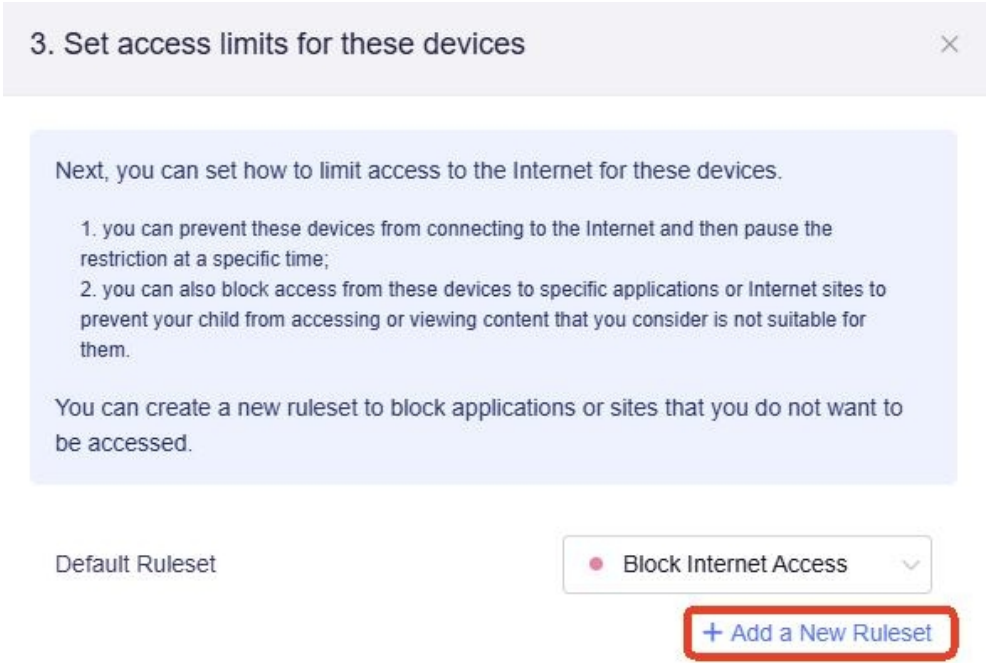


2. Seleziona i dispositivi che desideri gestire. Collegali prima al router. Se non sono stati collegati al router, aggiungili manualmente inserendo i loro indirizzi MAC.

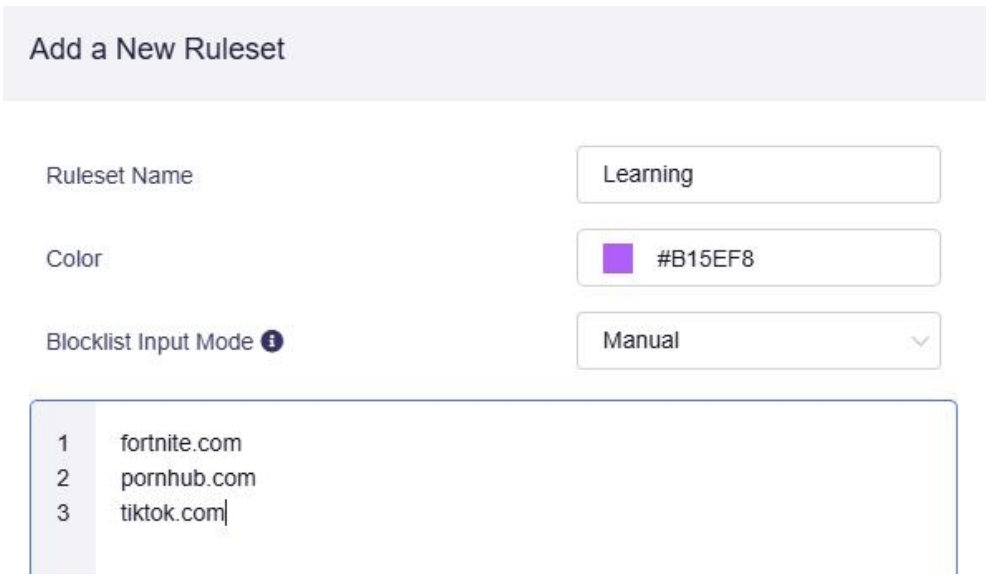


3. Imposta limite di accesso.

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

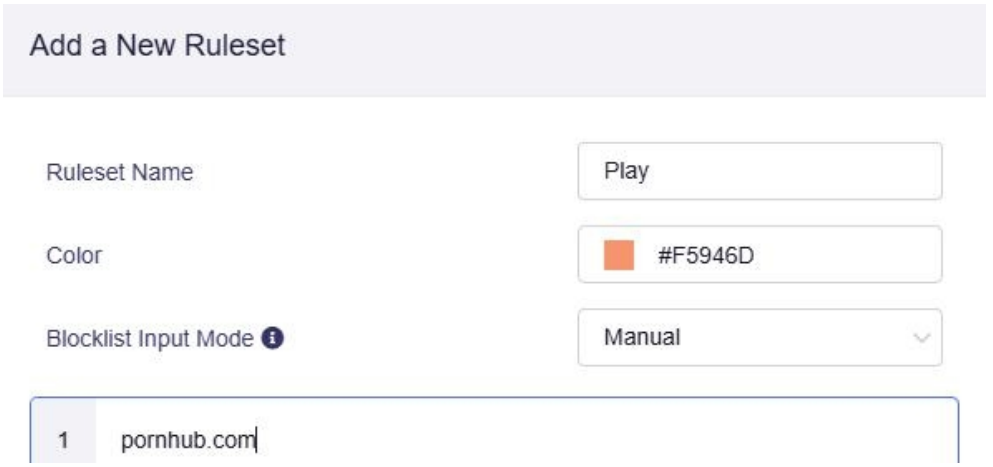


   Specifica il nome del set di regole (ad esempio, Apprendimento) e il colore, inserisci i siti Web da bloccare, quindi fai clic su **Applica**.

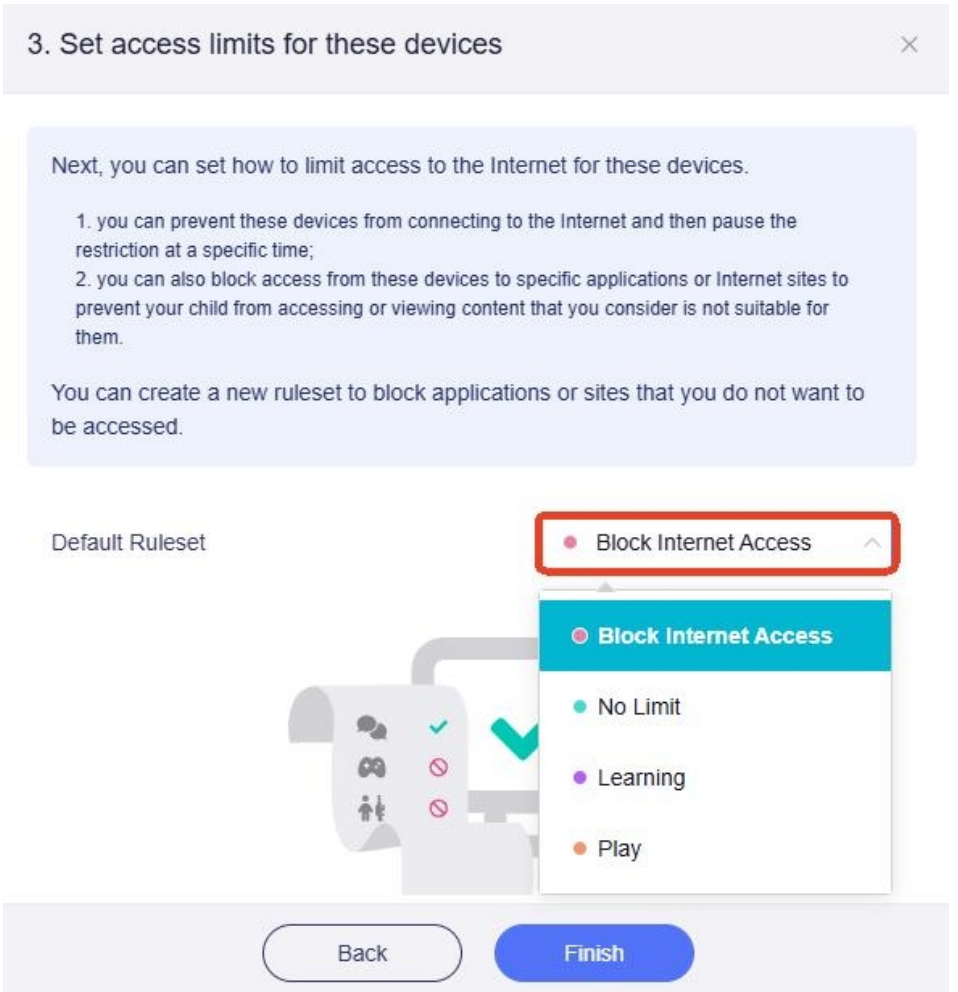


   Nota: i nomi di dominio inseriti nella blocklist devono includere i relativi sottodomini. Ad esempio, se viene inserito "esempio.com", include anche qualsiasi sottodominio, come "sottodominio.esempio.com".

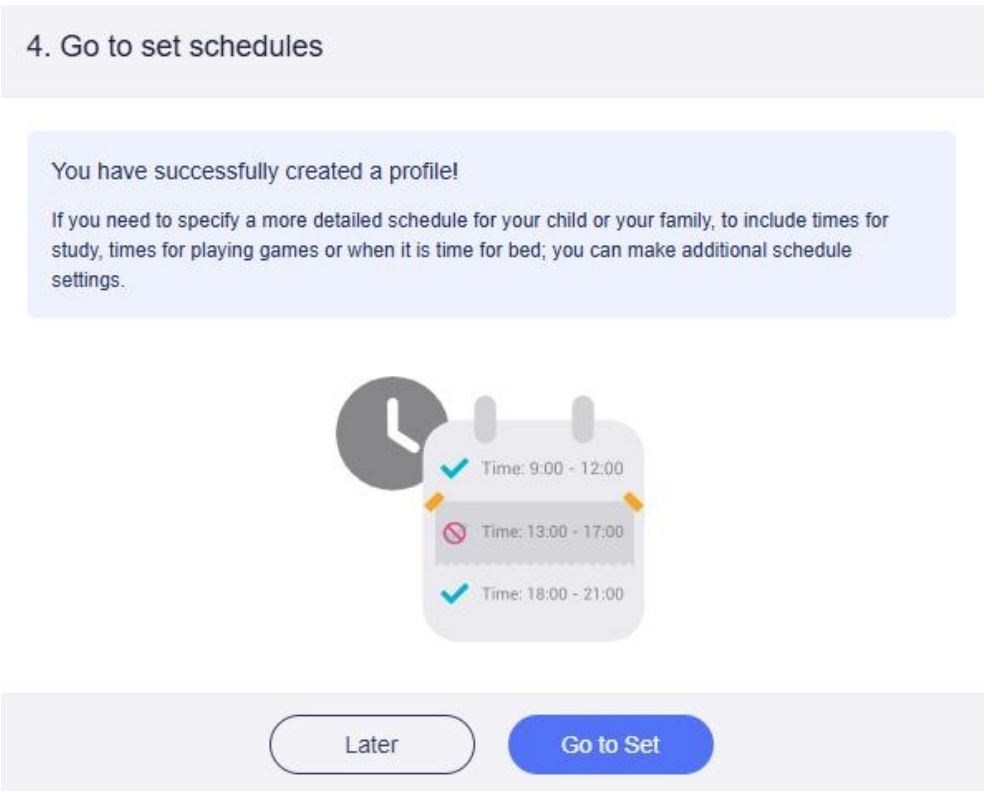
Allo stesso modo, crea un altro set di regole. Specifica il nome del set di regole (ad esempio, Gioco) e il colore, inserisci i siti Web da bloccare, quindi fai clic su **Applica**.



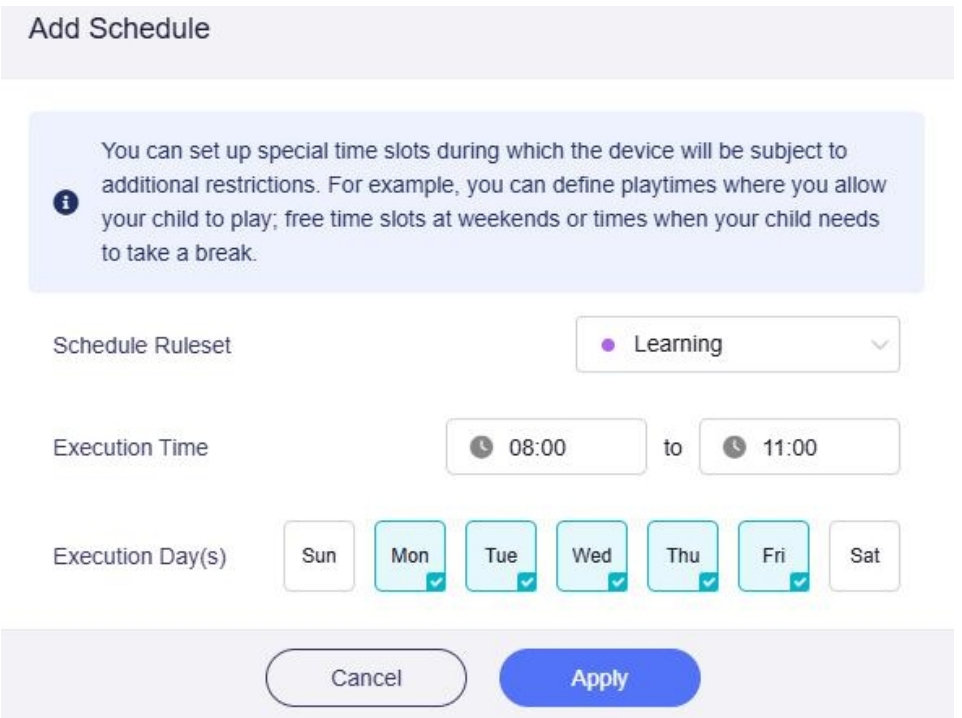
Una volta applicate, ci saranno un totale di quattro set di regole. Seleziona **Blocca l'accesso a Internet** come **set di regole predefinito** e fai clic su **Fine**.



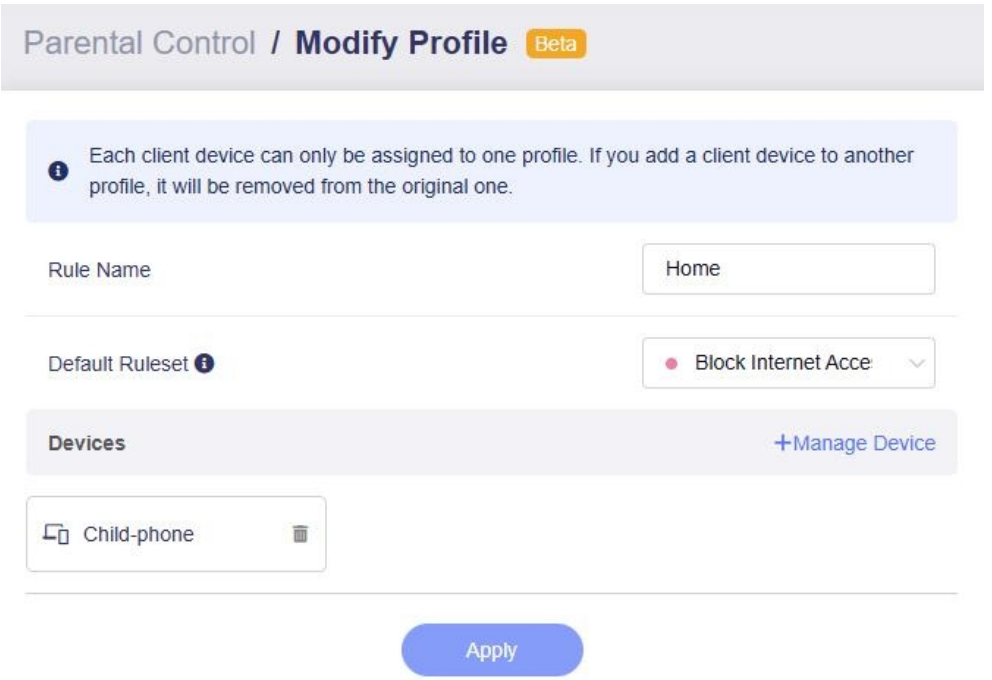
4. Successivamente, imposta la pianificazione per il tuo profilo. Fai clic su **Vai alla configurazione**.



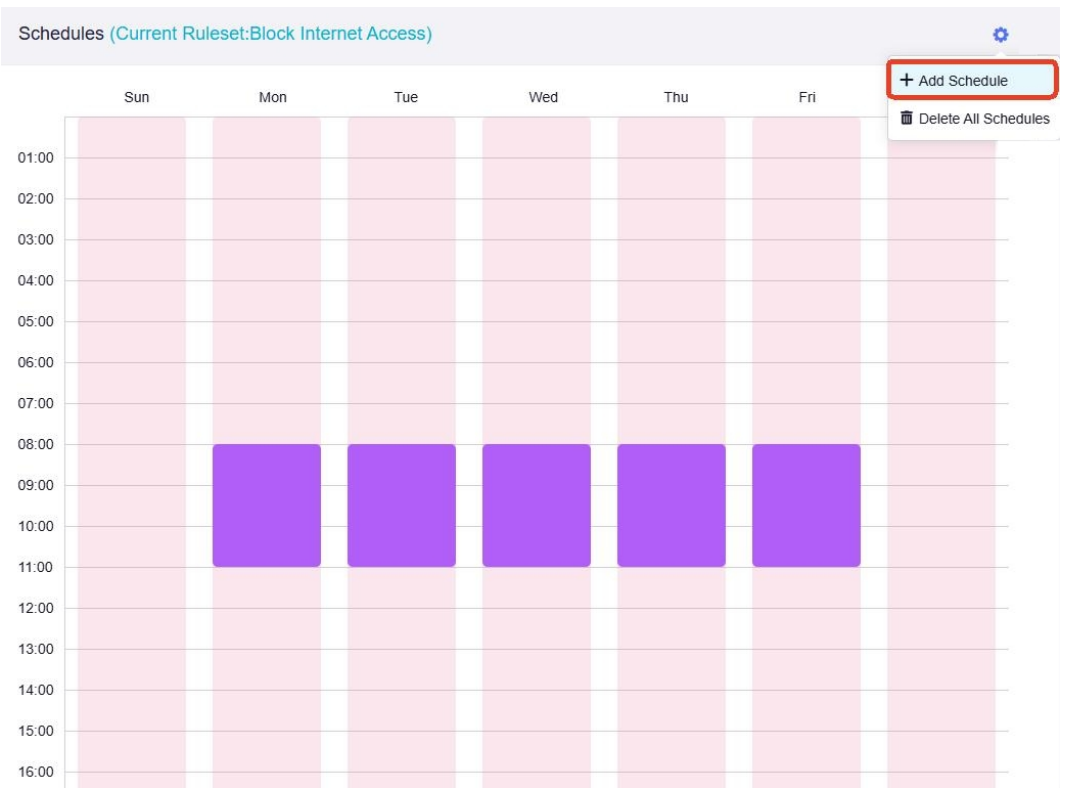
Aggiungi il set di regole di **apprendimento** al programma. Imposta l'**orario di esecuzione** da 8 AM a 11 AM nei giorni feriali, quindi fai clic su **Applica**.



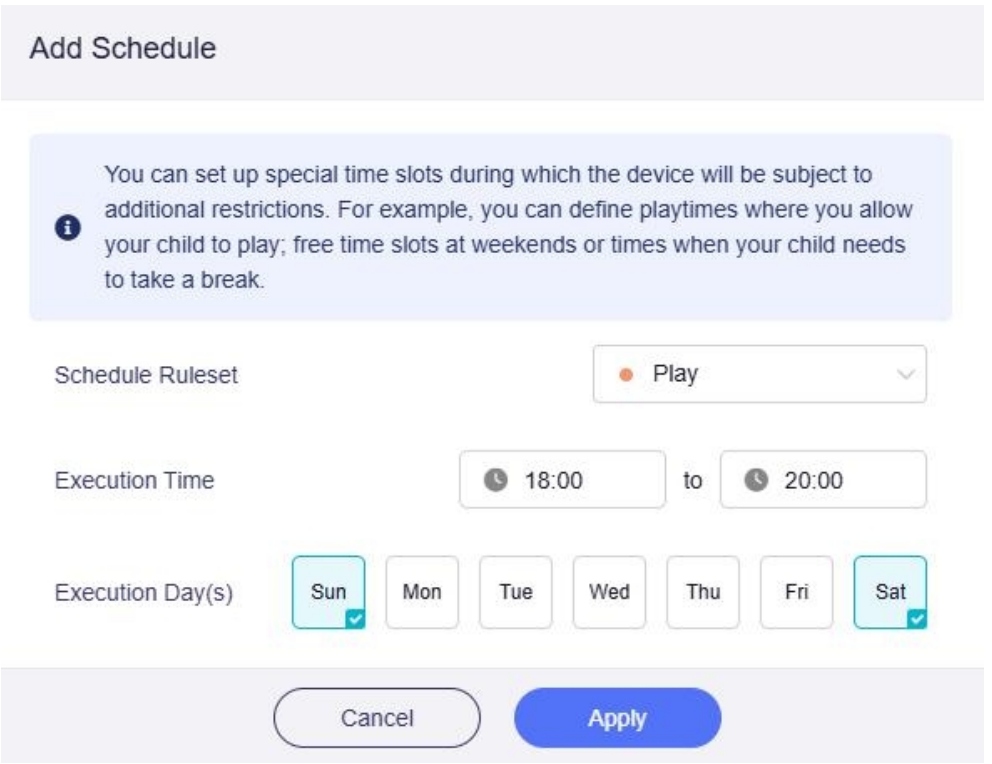
5. Verrai reindirizzato alla pagina di modifica del profilo creato.



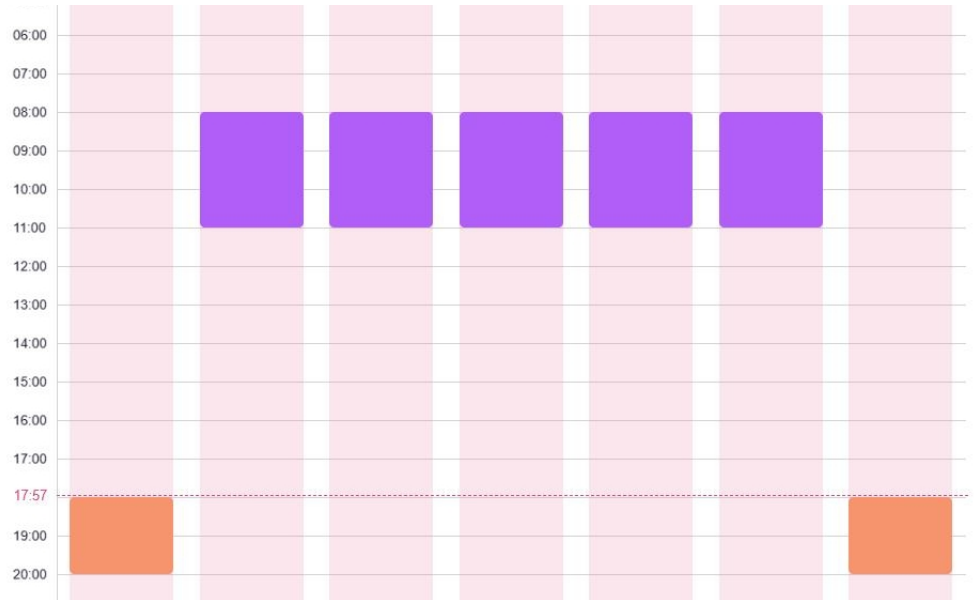
Sposta in fondo e vedrai che è stata creata una pianificazione. Fai clic sull'icona a forma di ingranaggio in alto a destra e seleziona **Aggiungi pianificazione**.



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



Le regole di gioco verranno quindi aggiunte al programma.

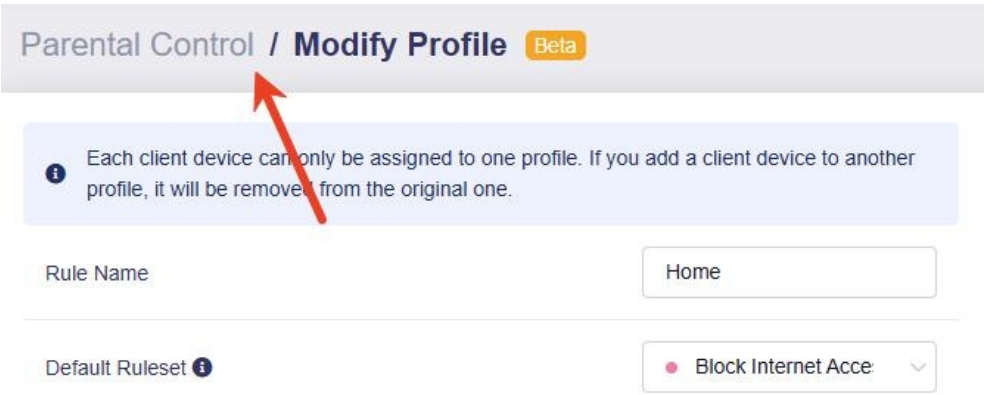


Suggerimenti:

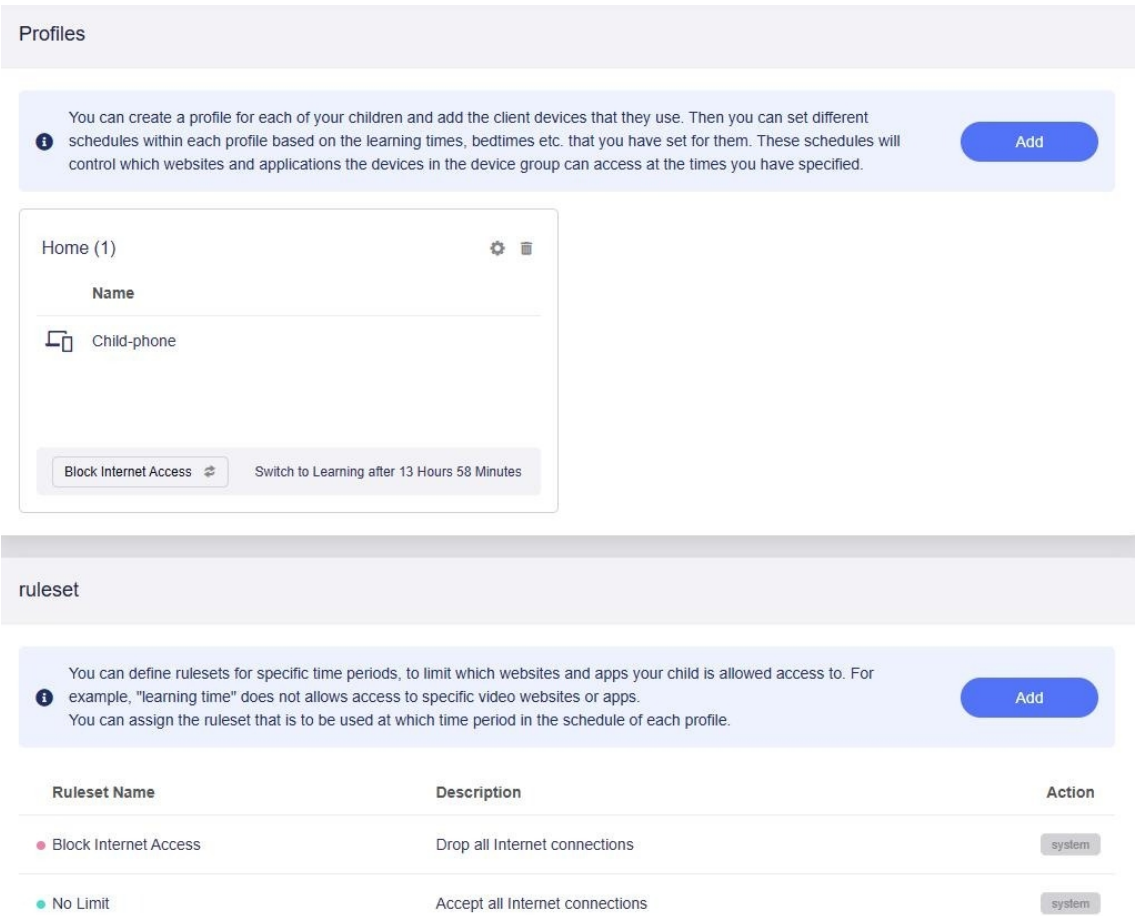
- La linea rossa tratteggiata indica l'ora corrente.

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

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



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



13.1.2 Risoluzione dei problemi

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

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

Capitolo 14

Sicurezza

Questo capitolo gestisce la sicurezza della rete, come port forwarding, il controllo di gestione e la modalità NAT.

14.1 Port forwarding

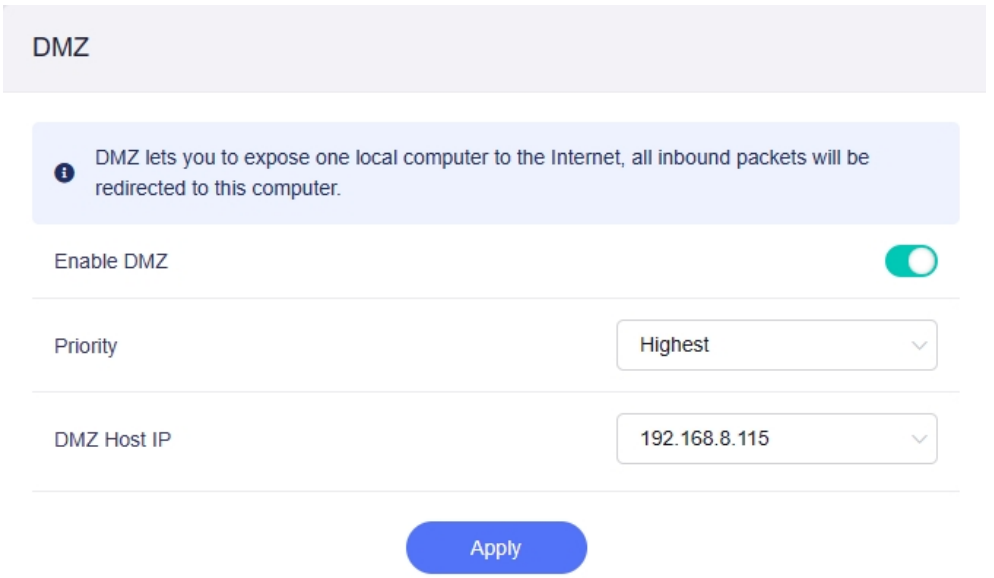
Il port forwarding è una funzionalità di rete che instrada le richieste esterne a dispositivi specifici sulla rete locale. La pagina Port forwarding include due funzioni chiave: **DMZ** (per l'accesso completo diretto a un singolo dispositivo) e **Port forwarding** (per l'accesso mirato a porte specifiche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

14.1.1 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, se necessario.

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**.



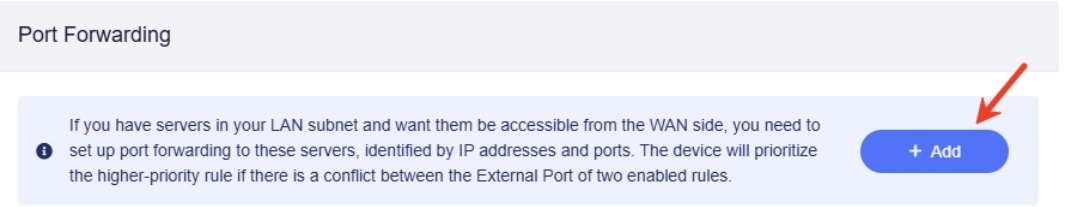
- **Priorità**: impostala su Massima o Minima. Se la priorità della DMZ è superiore alle regole di port forwarding, tutte le regole di port forwarding verranno invalidate. In caso contrario, le richieste verranno inoltrate al dispositivo client DMZ solo se la porta a cui si accede non ha una regola di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

14.1.2 Port forwarding

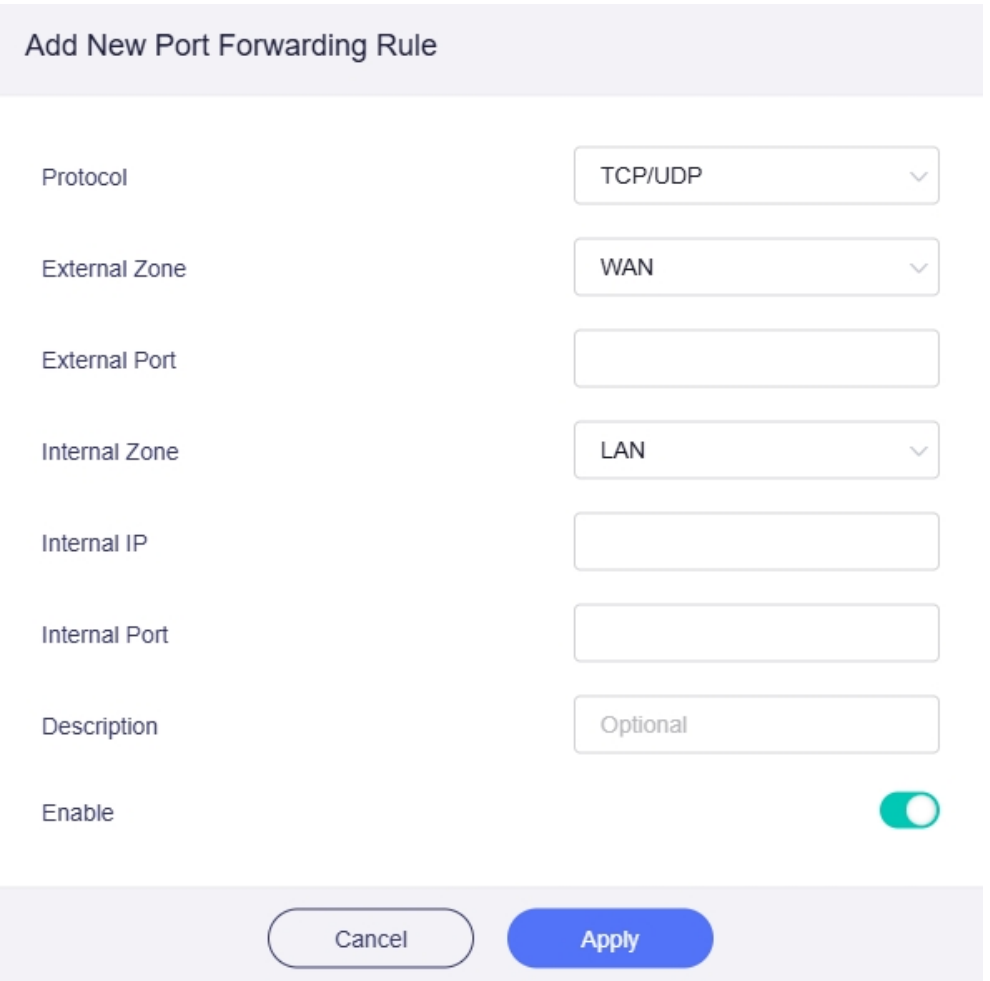
Il port forwarding consente ai computer remoti di connettersi a un computer locale o a un server dietro il firewall LAN (ad esempio server Web, server FTP).

Segui i passaggi seguenti per impostare il port forwarding, se necessario.

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



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



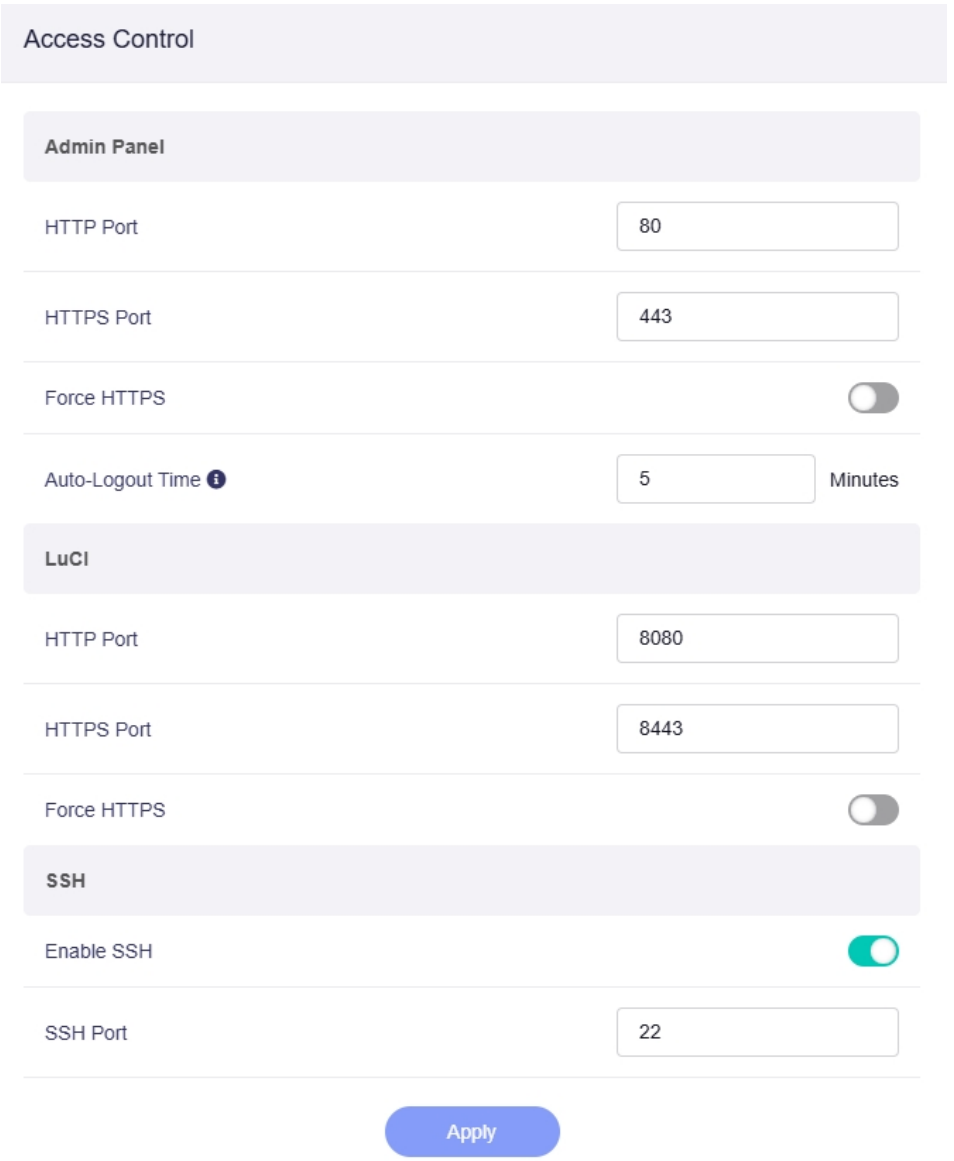
- **Protocollo**: il protocollo utilizzato. Puoi scegliere TCP, UDP o sia TCP che UDP.
- **Zona esterna**: le opzioni disponibili sono WAN, Client WireGuard, Server WireGuard, Client OpenVPN, Server OpenVPN e LAN.
- **Porta esterna**: il numero o i numeri di porte esterne. Inserisci qui un numero di 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.

14.2 Controllo di gestione

Accedi al pannello di amministrazione web del tuo router e vai a **SICUREZZA** > **Controllo di gestione**. 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.

14.2.1 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 HTTPS sicuro al pannello di amministrazione web.
- **Forza HTTPS**: se abilitato, l'accesso al 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

Installa LuCI nelle Impostazioni avanzate prima di impostarne il controllo di accesso.

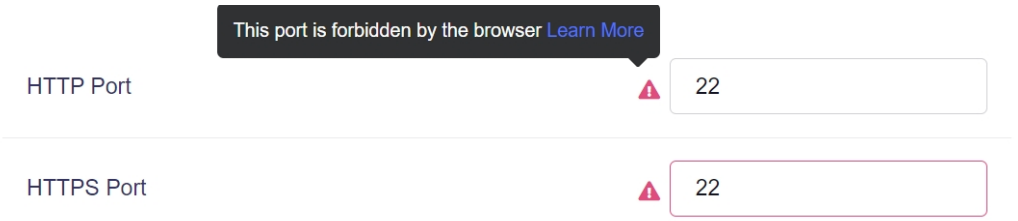
- **Porta HTTP**: predefinita su 8080, per l'accesso HTTP non crittografato all'interfaccia LuCI.
- **Porta HTTPS**: il valore predefinito è 8443, per l'accesso HTTPS sicuro all'interfaccia LuCI.
- **Forza HTTPS**: se abilitato, l'accesso all'interfaccia LuCI viene imposto per utilizzare una connessione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

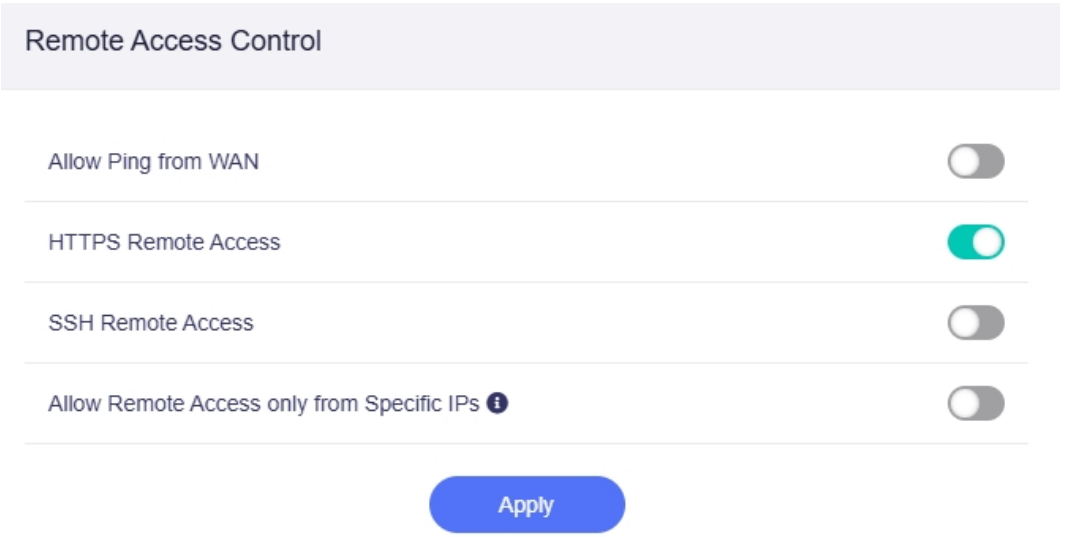
1. Se assegni un numero di porta che è in conflitto con una porta riservata (o una riservata per servizi specifici da browser/convenzioni di rete), verrà visualizzato un messaggio che indica "Questa porta è vietata dal browser".



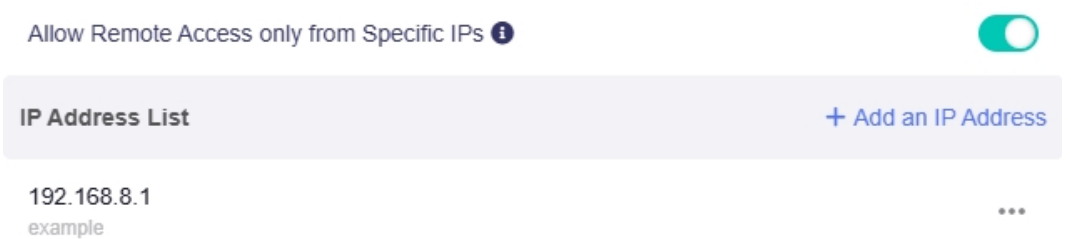
2. Se il numero di porta viene modificato nel firmware, è necessario inserire il numero di porta corretto per accedere al pannello di amministrazione. Se hai dimenticato il numero di porta, reimposta il router per ripristinare il numero di porta predefinito.

14.2.2 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.

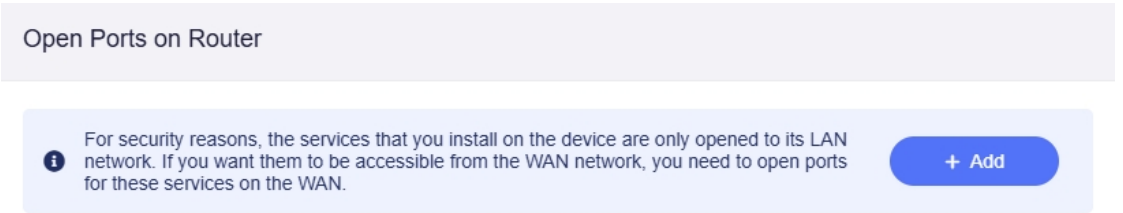


- **Consenti ping dalla WAN**: consentire il ping dal lato WAN del router può aiutare gli utenti a verificare se il router è raggiungibile tramite WAN in caso di problemi di rete, nonché a determinare la latenza di rete e la perdita di pacchetti.
- **Accesso remoto HTTPS**: l'accesso remoto HTTPS consente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

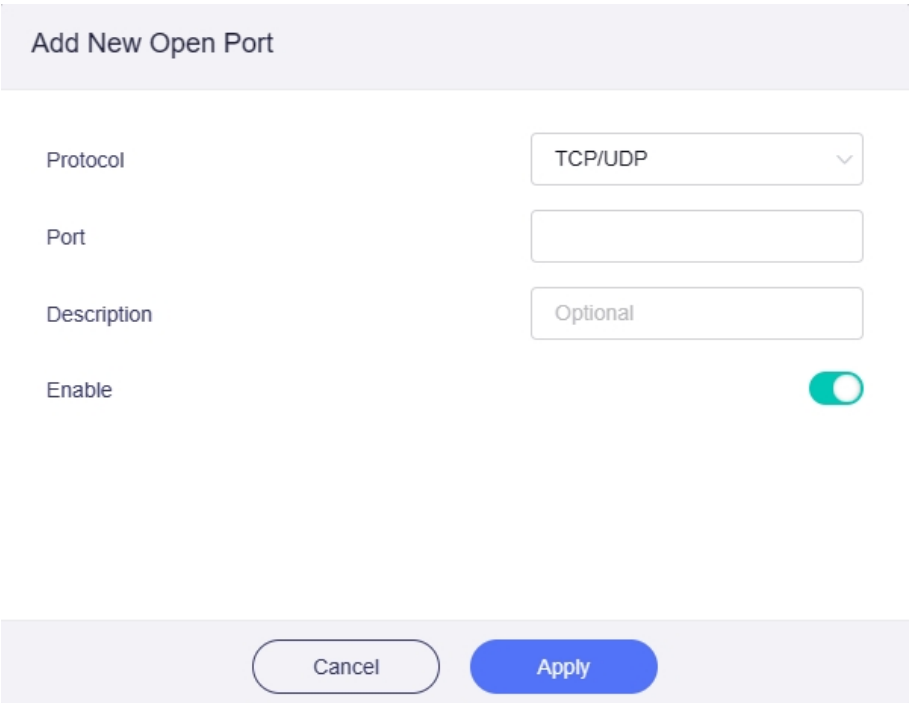


14.2.3 Apertura delle porte sul router

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.



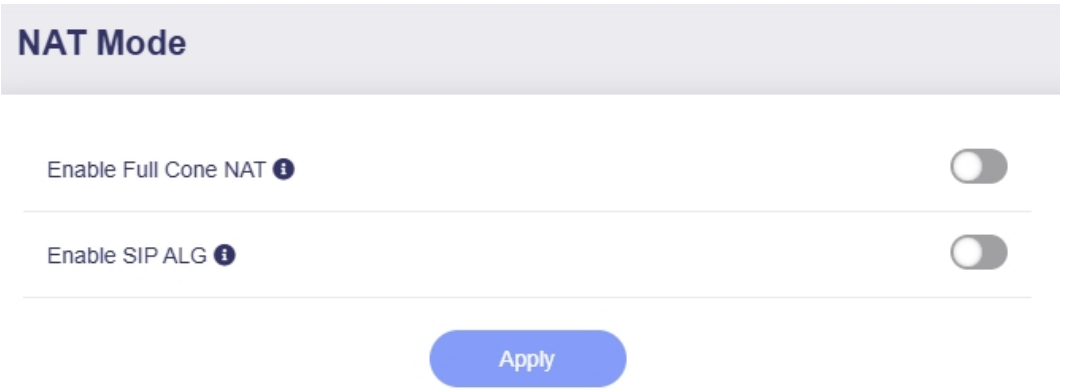
Per aprire una porta, fai clic su **Aggiungi** e inserisci le informazioni richieste nella finestra pop-up.



- **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.

14.3 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 15

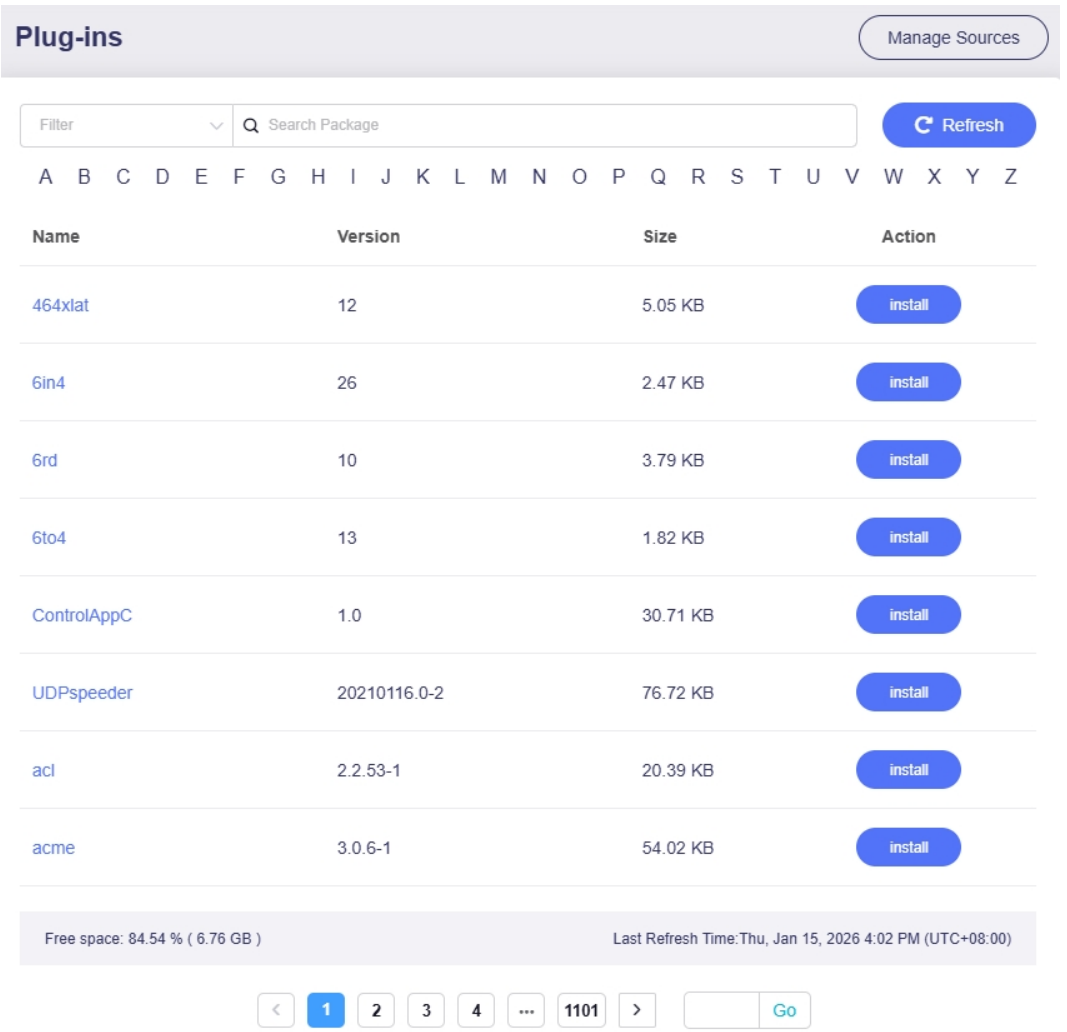
Applicazioni

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

15.1 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:

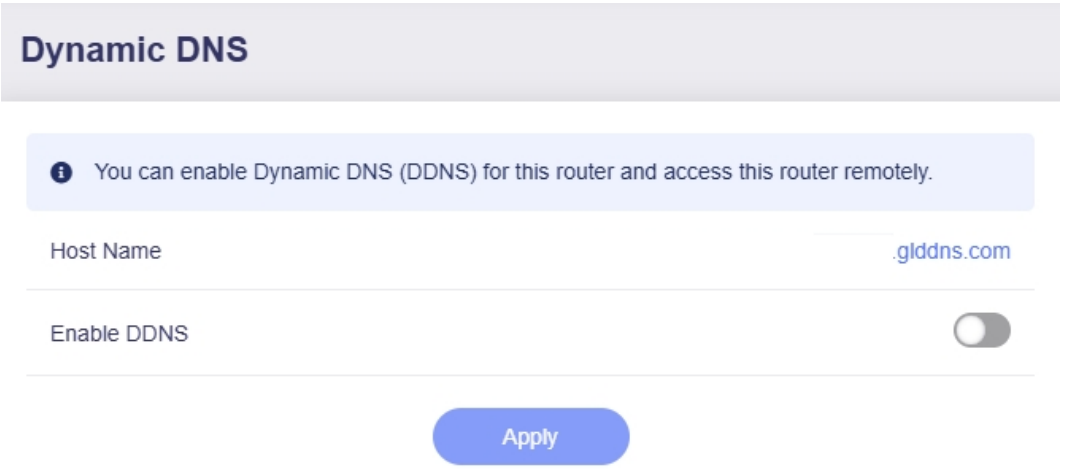
1. Non è consigliabile aggiornare i plug-in preinstallati nel firmware ufficiale GL.iNet, come nginx, adguard home, tailscale, ecc.
2. I plugin di terze parti installati manualmente dagli utenti possono essere aggiornati; tuttavia, GL.iNet non è responsabile per eventuali problemi di sicurezza derivanti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

15.2 DNS dinamico

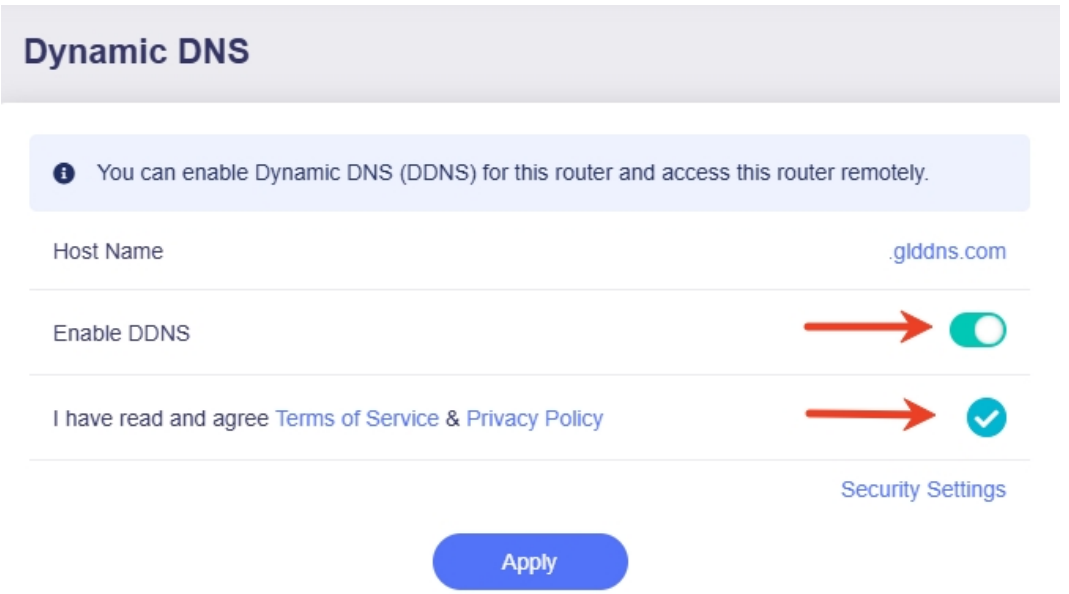
Dynamic Domain Name Service (DDNS o DNS dinamico) è un servizio utilizzato per mappare un nome di dominio all'indirizzo IP dinamico di un dispositivo di rete. Con DNS dinamico puoi accedere al tuo router da remoto. Per questa funzionalità è richiesto un indirizzo IP pubblico.

15.2.1 Abilita DDNS

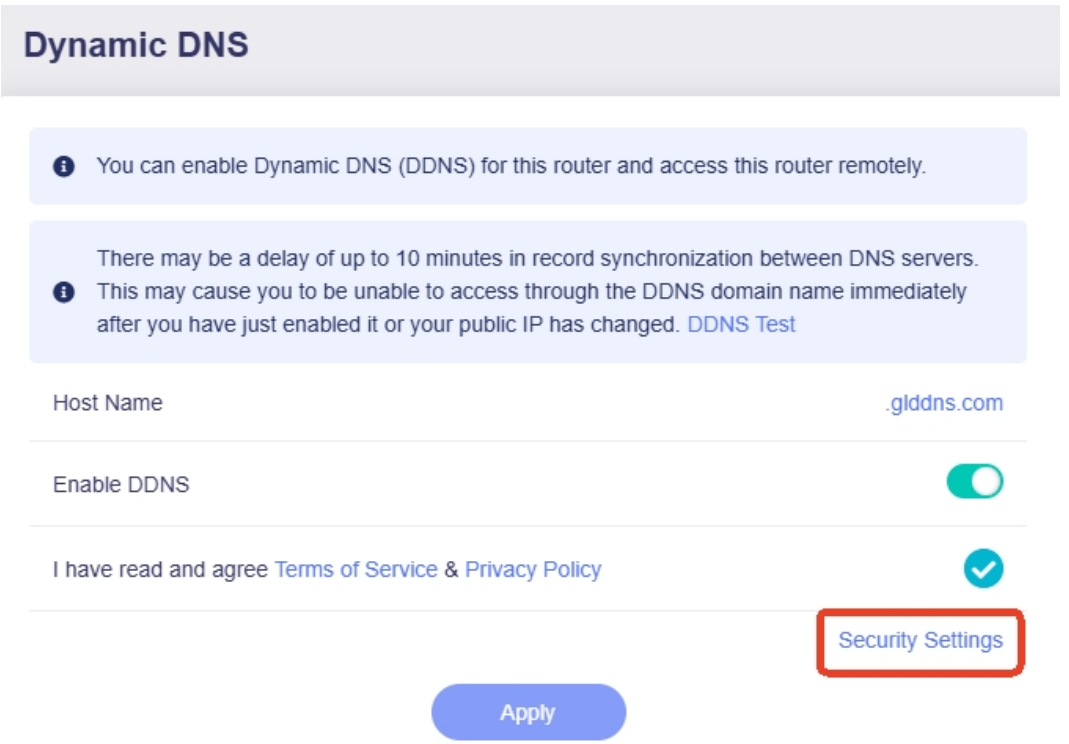
1. Accedi al pannello di amministrazione web del tuo router, vai su **APPLICAZIONI** > **DNS dinamico**, la pagina viene visualizzata come di seguito.



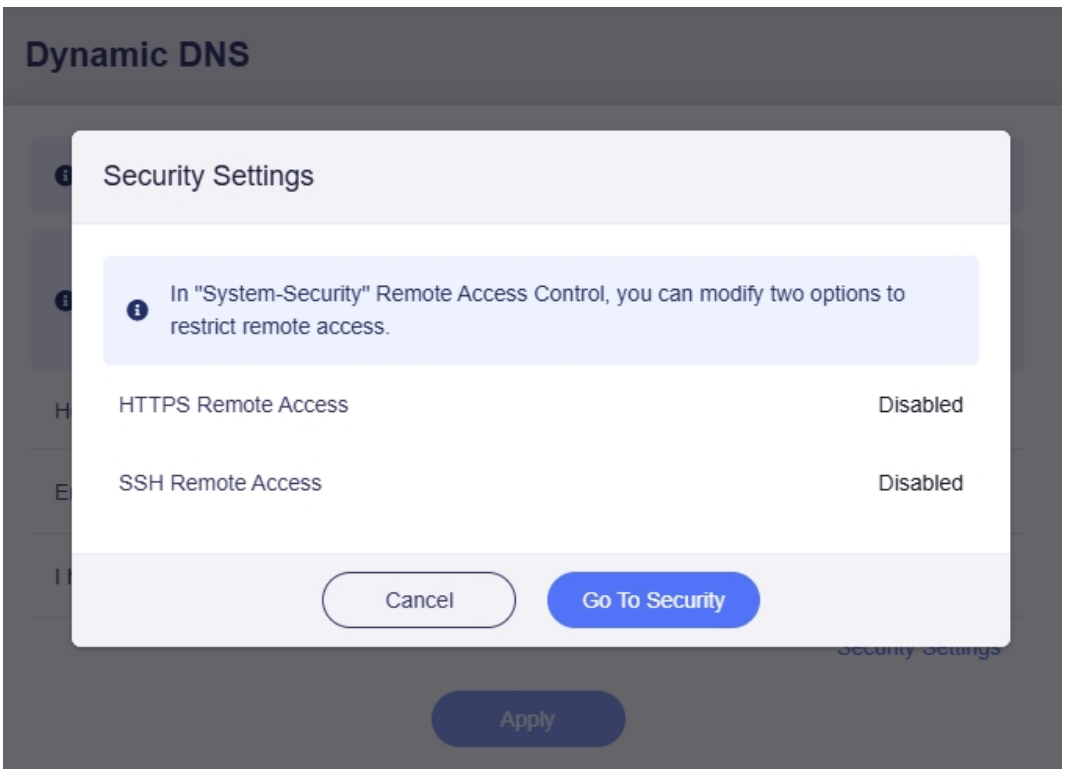
2. Attiva **Abilita DDNS**, leggi e accetta i **Termini di servizio e l'Informativa sulla privacy**, quindi fai clic su **Applica**.



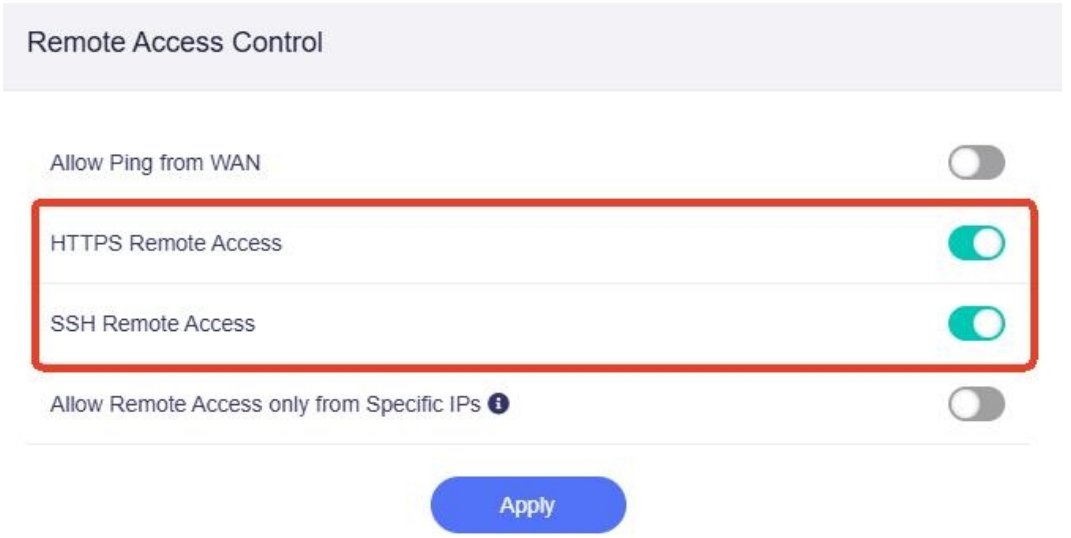
3. Fai clic su **Impostazioni di sicurezza** nell'angolo in basso a destra.



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



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



Nota:

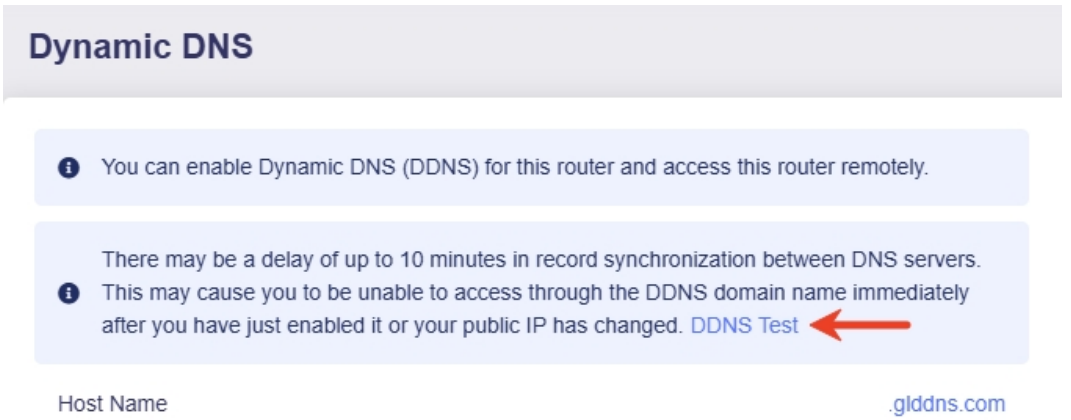
1. Potrebbe verificarsi un ritardo fino a 10 minuti nella sincronizzazione dei record tra i server DNS. Ciò potrebbe impedirti di accedere tramite il nome di dominio DDNS immediatamente dopo averlo abilitato o quando il tuo IP pubblico cambia.
2. Se abiliti DDNS e client VPN contemporaneamente, assicurati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

15.2.2 Verifica del funzionamento del DDNS

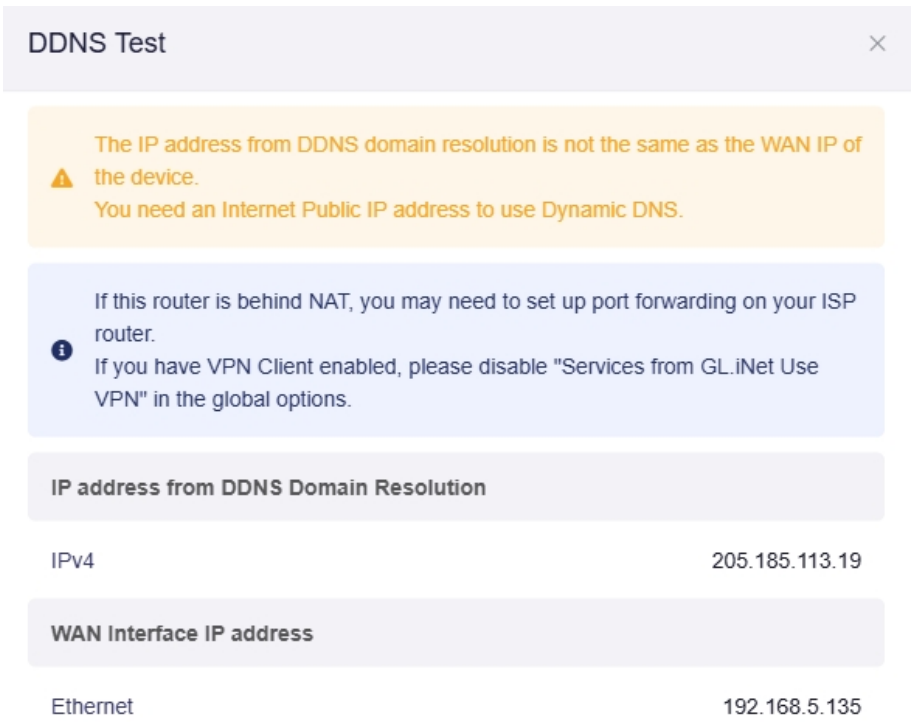
Puoi verificare se DDNS funziona utilizzando lo strumento di test DDNS o manualmente tramite comandi.

Metodo 1. Utilizzo dello strumento di verifica DDNS

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



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



Metodo 2. Utilizza i comandi

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



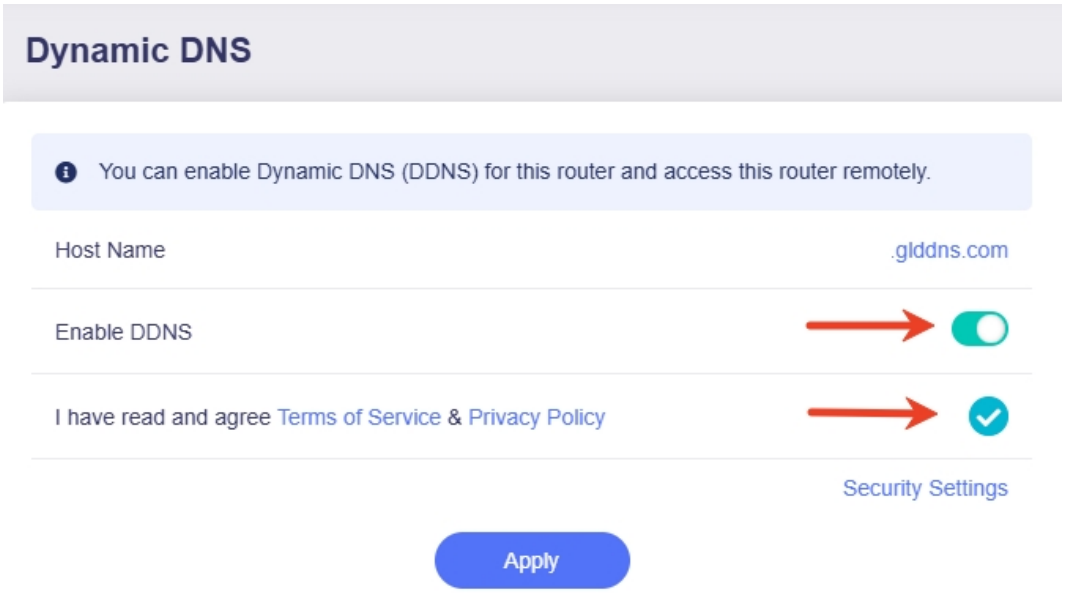
   - Sostituisci "xxxxxxx.glddns.com" nell'immagine sopra con il tuo nome host.
   - "8.8.8.8" è il DNS di Google. Usalo o sostituiscilo con altri, quindi premi Invio.
2. Se ottieni un indirizzo IP pubblico come "183.178.10.100" nell'immagine sopra, indica che il tuo dominio DDNS è stato mappato correttamente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

15.2.3 Accesso remoto HTTPS

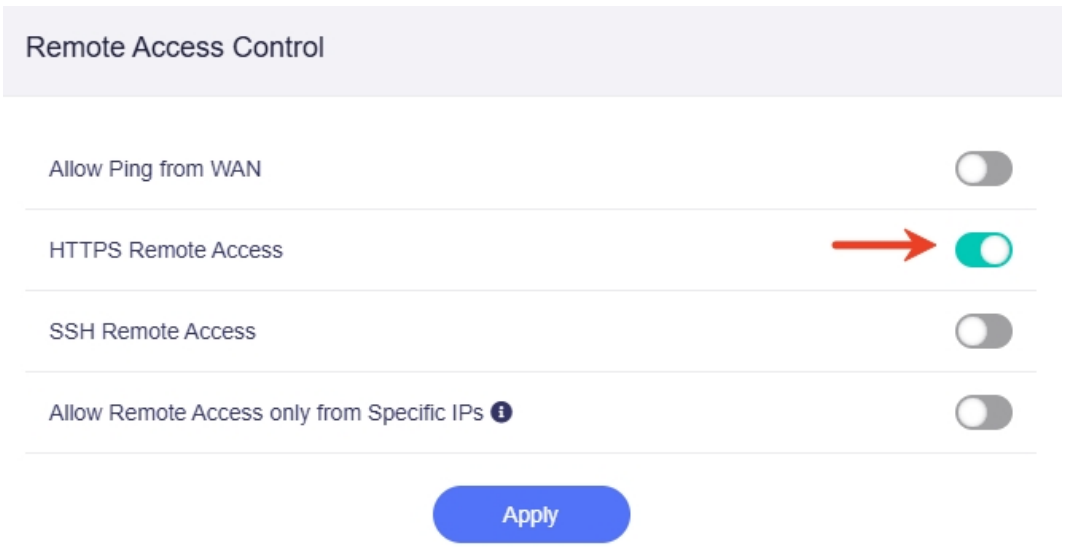
Per l'accesso remoto HTTPS è richiesto un indirizzo IP pubblico. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 443**) sul router upstream per l'accesso HTTPS.

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**.

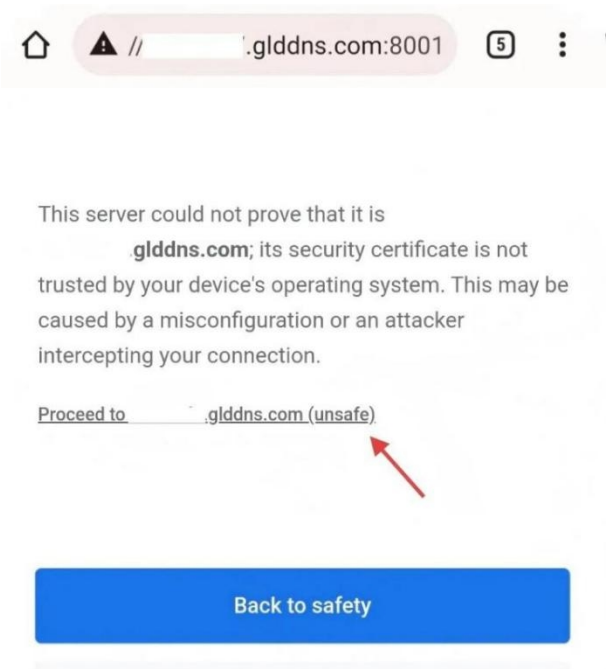


2. Nel pannello di amministrazione web, vai su **SICUREZZA** > **Controllo di gestione** > **Controllo dell'accesso remoto**. Abilita **Accesso remoto HTTPS** e fai clic su **Applica**.



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

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



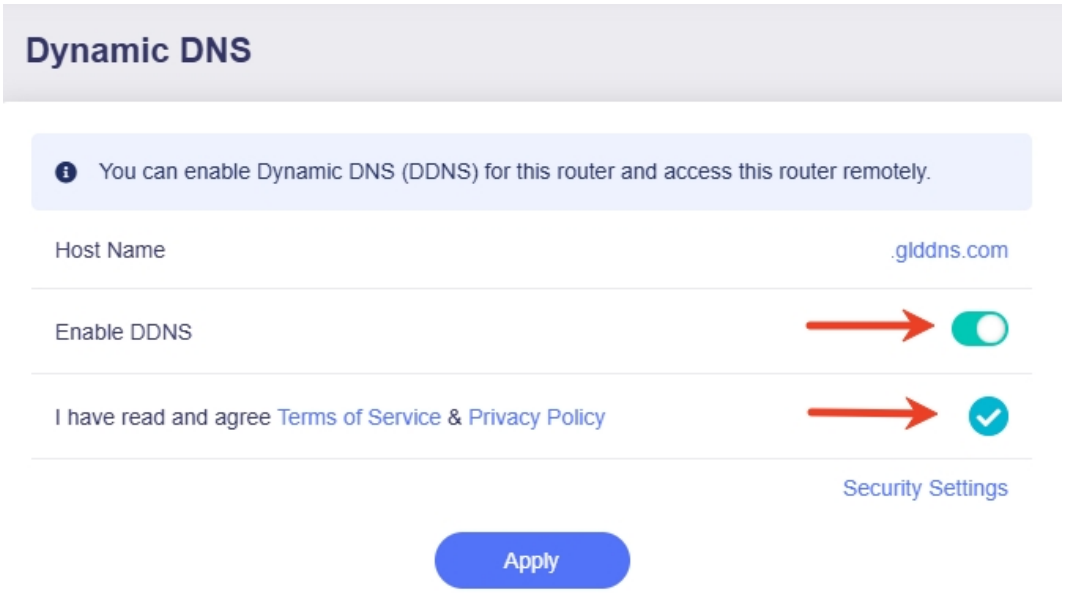
Sarai quindi in grado di accedere al pannello di amministrazione web del router utilizzando il nome host DDNS su **HTTPS**.

15.2.4 Accesso remoto SSH

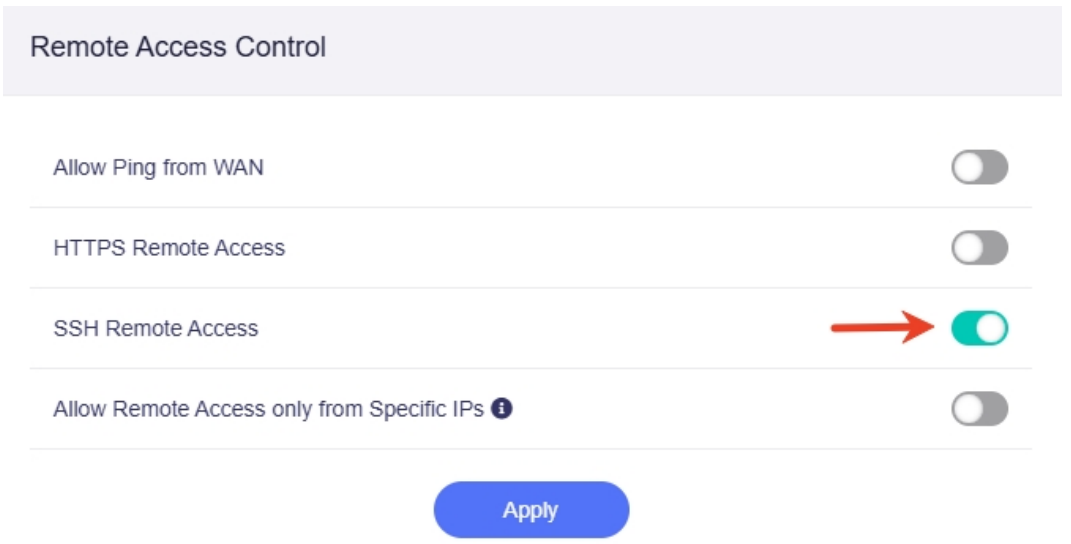
Per l'accesso remoto SSH è richiesto un **indirizzo IP pubblico**. Vedi qui per verificare se il tuo ISP ti ha assegnato un indirizzo IP pubblico. Se il tuo router è dietro NAT, configura il port forwarding (**porta 22**) sul router upstream per l'accesso remoto SSH.

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** > **Controllo di gestione** > **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).

15.3 Archiviazione di rete

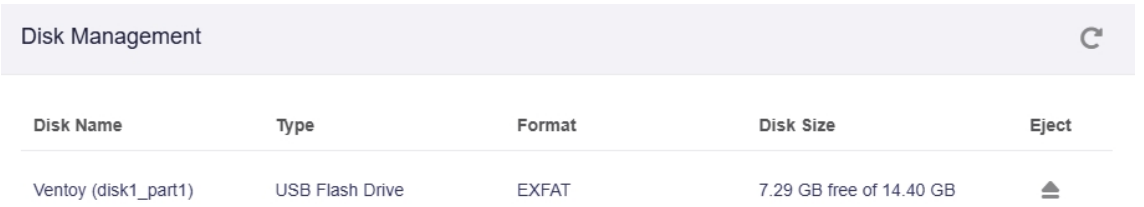
L'archiviazione di rete consente la condivisione di file wireless tra dispositivi collegando un'unità USB o una scheda SD al router. Il router converte il dispositivo di archiviazione in un'unità di rete condivisa, accessibile a tutti i dispositivi connessi tramite Wi-Fi.

Flint è dotato di una porta USB, compatibile con chiavette USB e dischi rigidi 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.

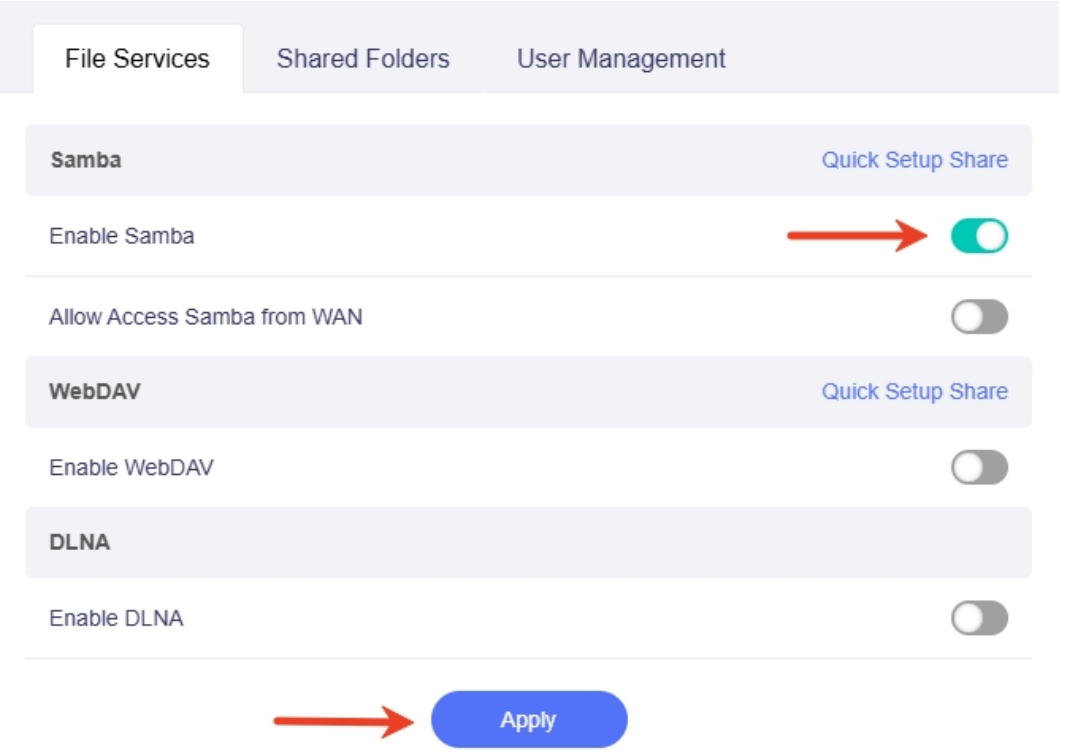
15.3.1 Collegamento del dispositivo di archiviazione

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.



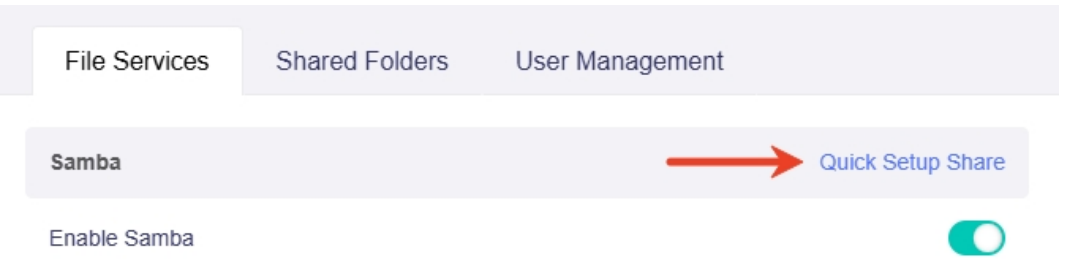
15.3.2 Configurazione di Samba

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

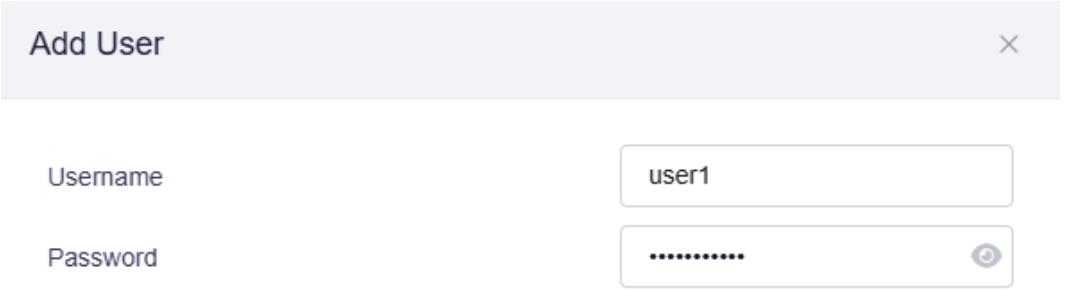


   - **Consenti accesso a Samba dalla WAN**: abilitalo se desideri che i dispositivi upstream accedano al servizio Samba.

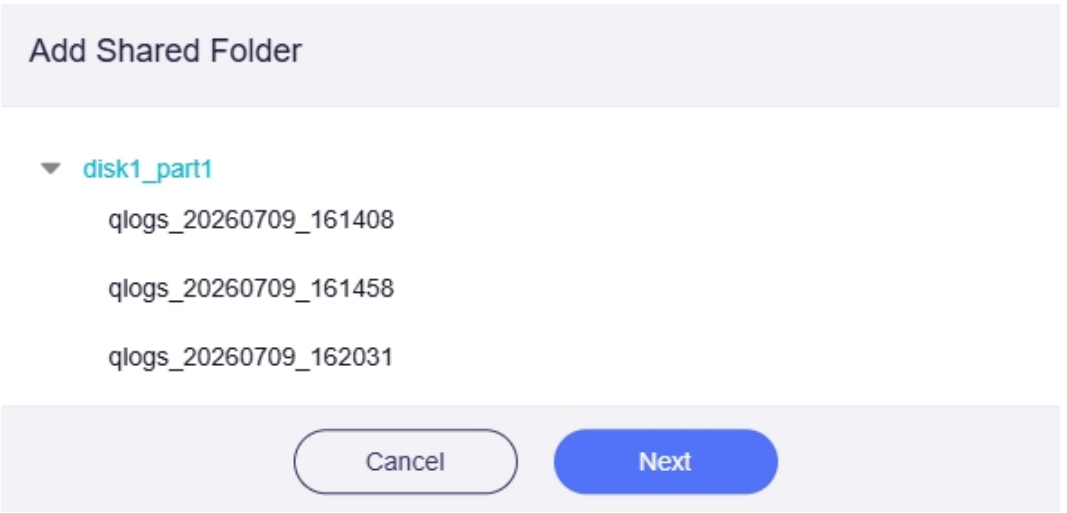
2. Fai clic su **Condivisione rapida** per impostare il collegamento condiviso.



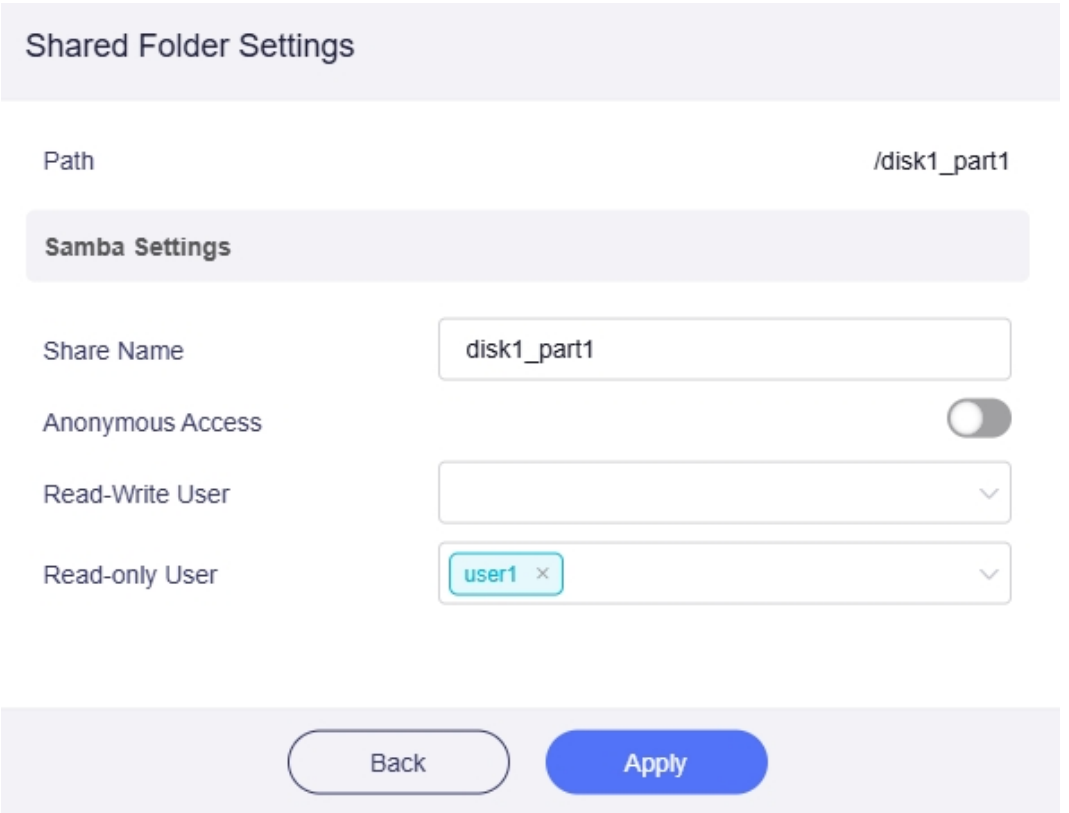
3. Aggiungi un utente e fai clic su **Avanti**. Questo passaggio verrà saltato se disponi già di un account.



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).

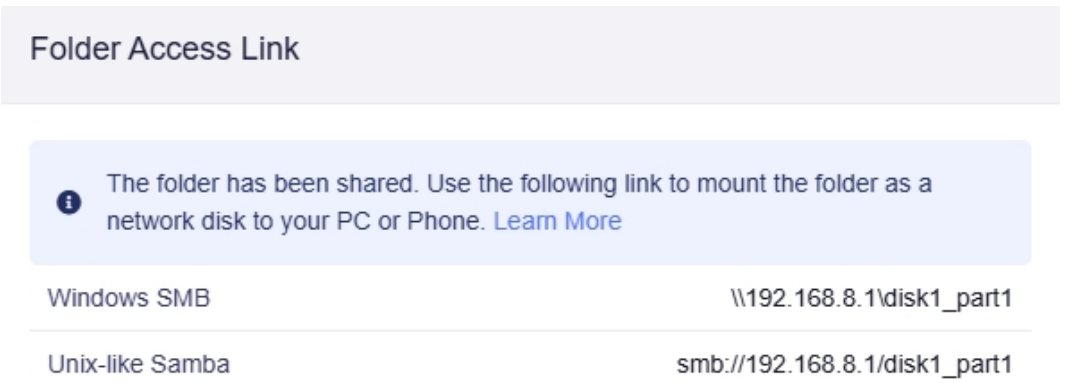


5. Imposta la cartella condivisa.
   L'utente creato nel passaggio precedente verrà aggiunto **all'utente di sola lettura** per impostazione predefinita. Se desideri che questo utente sia in grado di scrivere o eliminare file, rimuovilo da Utente di sola lettura e aggiungilo a **Utente di lettura-scrittura**,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

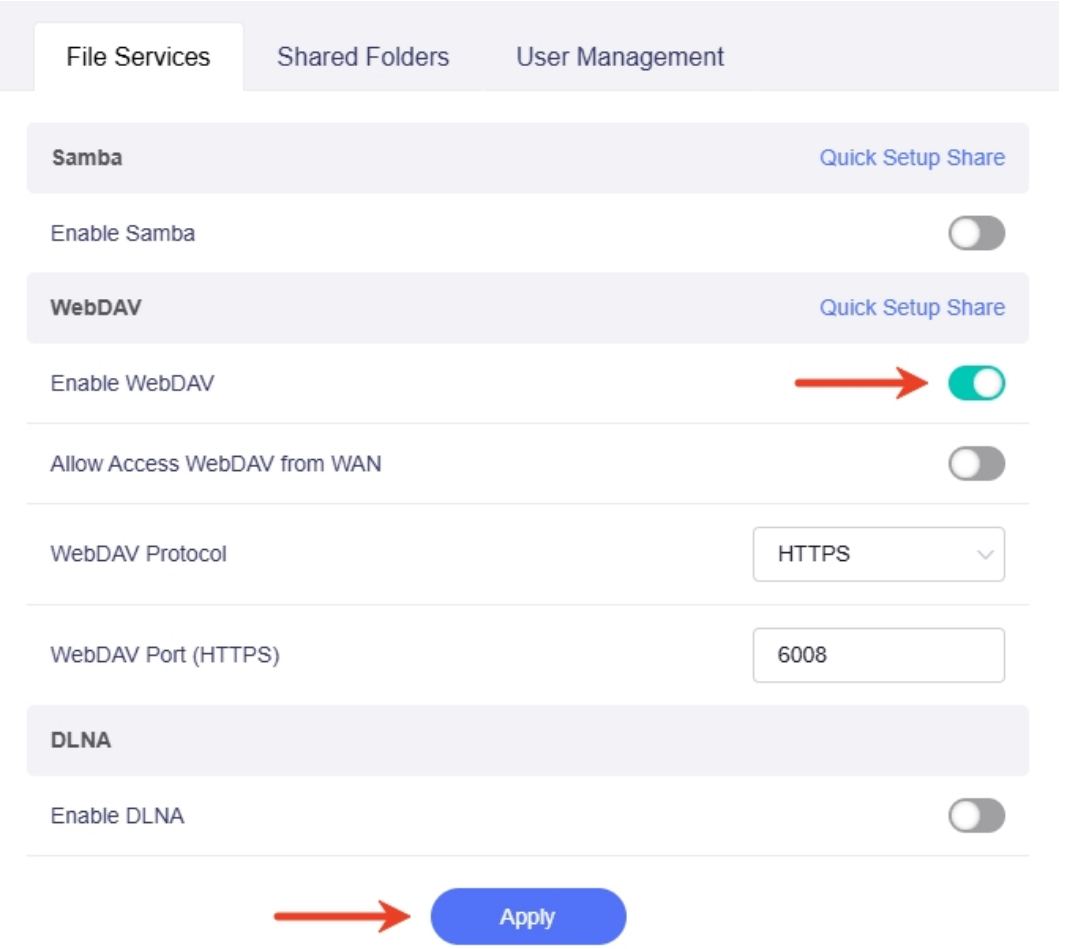


Nota: se abiliti **l'accesso Samba dalla WAN** e accedi alla cartella condivisa dalla rete upstream, sostituisci l'IP del router (predefinito: 192.168.8.1) nel collegamento di accesso con

l'IP WAN del router, che puoi trovare nella pagina INTERNET del pannello di amministrazione web.

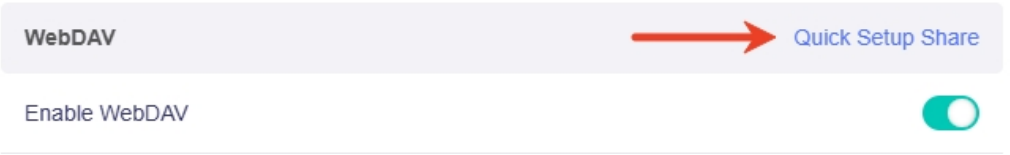
15.3.3 Configurazione di WebDAV

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

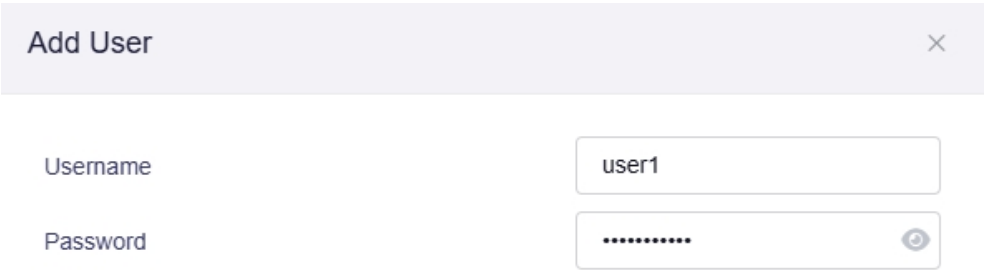


- **Consenti accesso WebDAV dalla WAN**: abilitalo se desideri che i dispositivi upstream accedano al servizio WebDAV.
- **Protocollo WebDAV**: HTTP non crittografato; utilizzarlo a proprio rischio. HTTPS è crittografato e utilizza un certificato autofirmato.
- **Porta WebDAV**: non è necessario modificare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

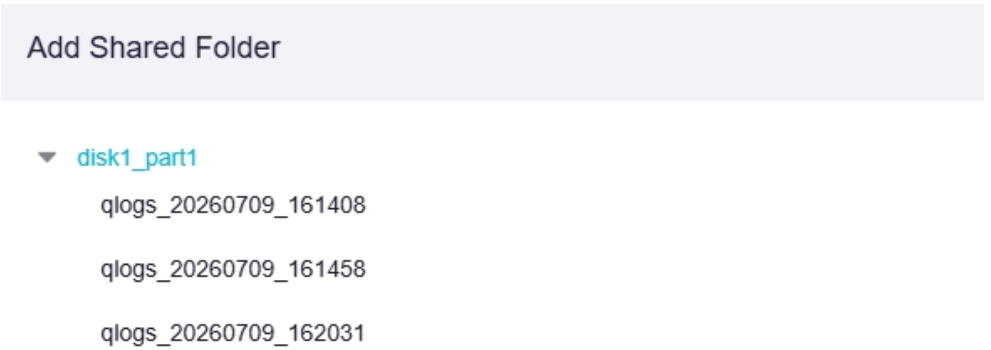
2. Fai clic su **Condivisione rapida** per impostare il collegamento condiviso.



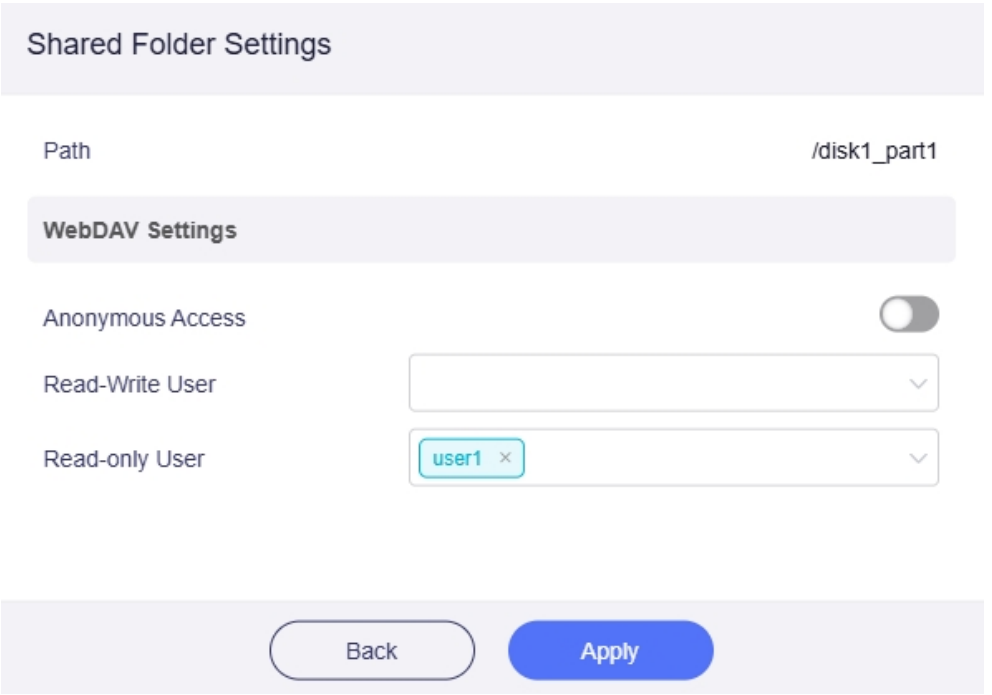
3. Aggiungi un utente e fai clic su **Avanti**. Questo passaggio verrà saltato se disponi già di un account.



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).

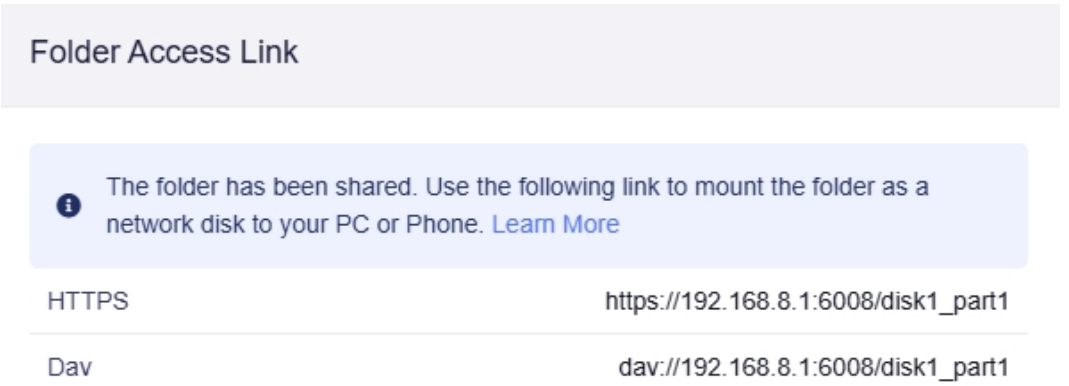


5. Imposta la cartella condivisa.
   L'utente creato nel passaggio precedente verrà aggiunto **all'utente di sola lettura** per impostazione predefinita.
   Se desideri che questo utente sia in grado di scrivere o eliminare file, rimuovilo dall'utente di sola lettura e aggiungilo **all'utente di lettura-scrittura**,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



Suggerimento: per motivi di sicurezza, non è consigliabile abilitare l'accesso anonimo.

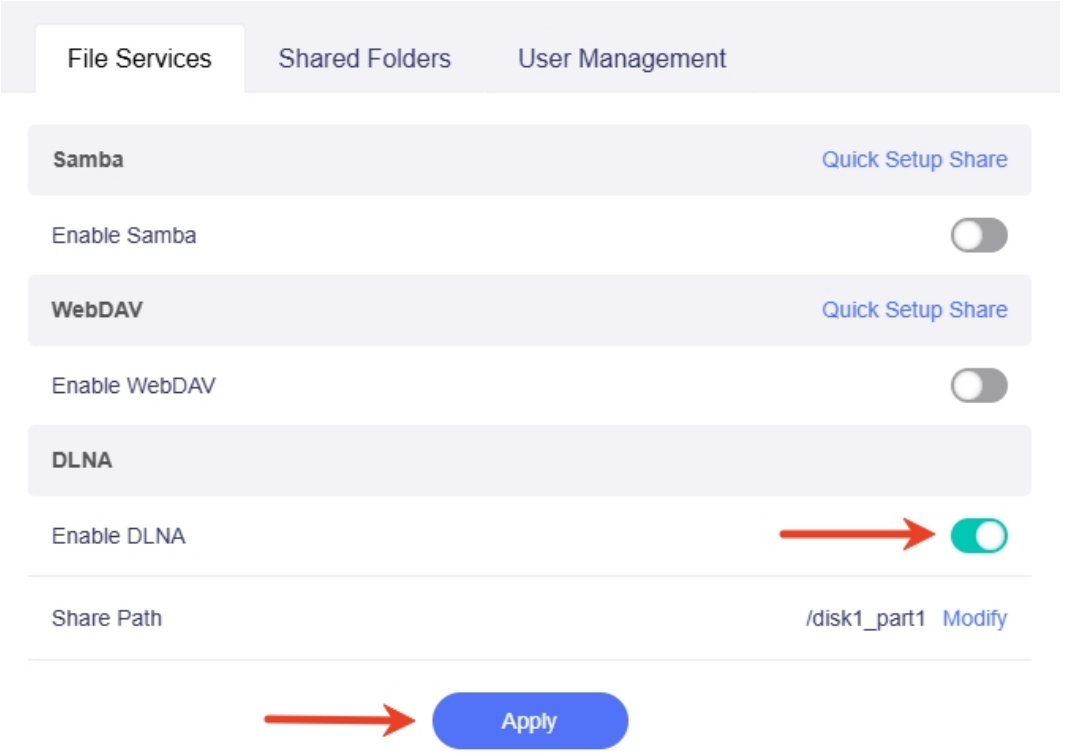
6. Ottenere il collegamento di accesso alla cartella.
   La pagina mostrerà i collegamenti per i sistemi operativi Windows e Unix-like. I sistemi simili a Unix includono Android, iOS, macOS, Ubuntu, ecc. Ora puoi accedere alla tua cartella condivisa tramite il servizio WebDAV tramite questi collegamenti.



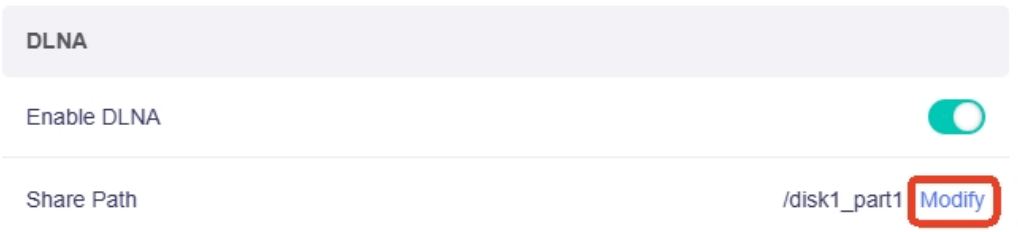
Nota: se attivi **Consenti accesso WebDAV dalla WAN** e accedi alla cartella condivisa dalla rete upstream, sostituisci l'IP del router (predefinito: 192.168.8.1) nel collegamento di accesso con l'IP WAN del router, che puoi trovare nella pagina INTERNET del pannello di amministrazione web.

15.3.4 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.



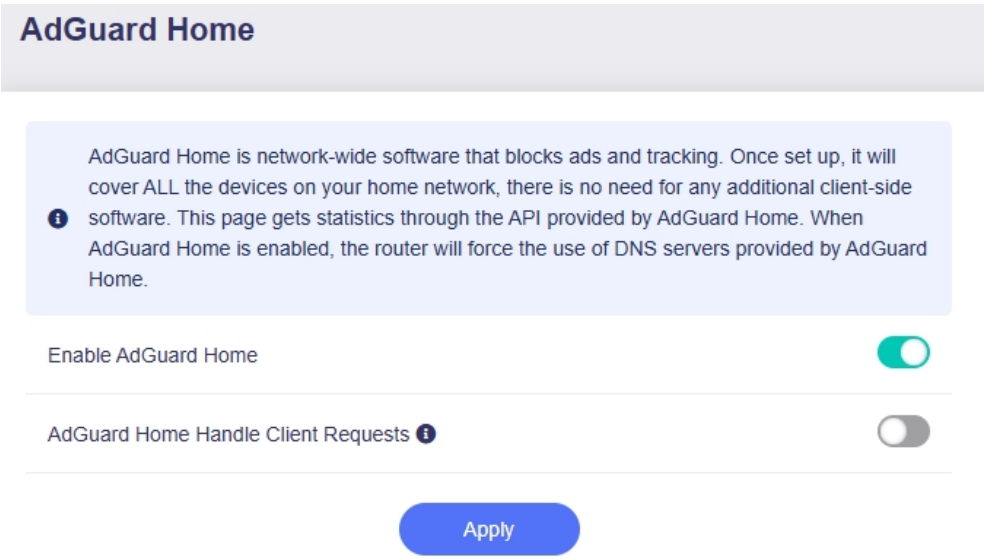
3. Collega la tua smart TV al router. Troverà automaticamente il server DLNA.

15.4 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.

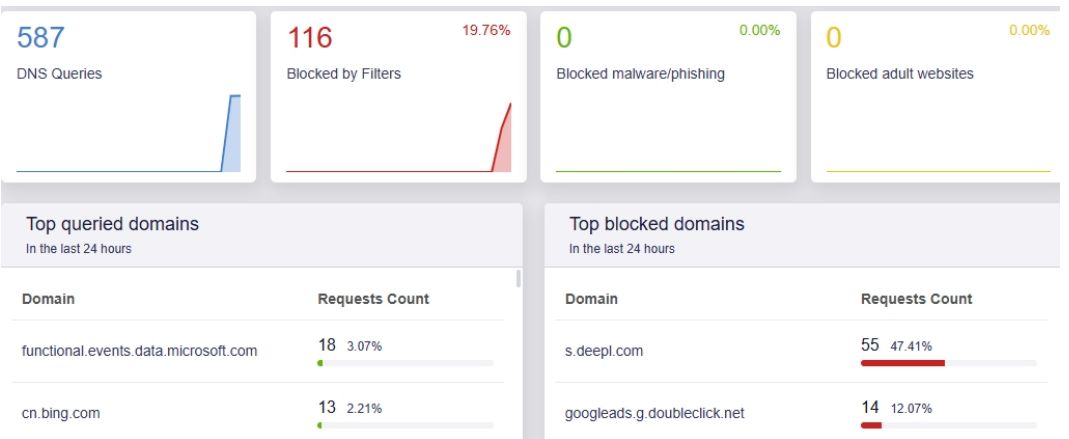
Segui questi passaggi per configurare AdGuard Home.

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

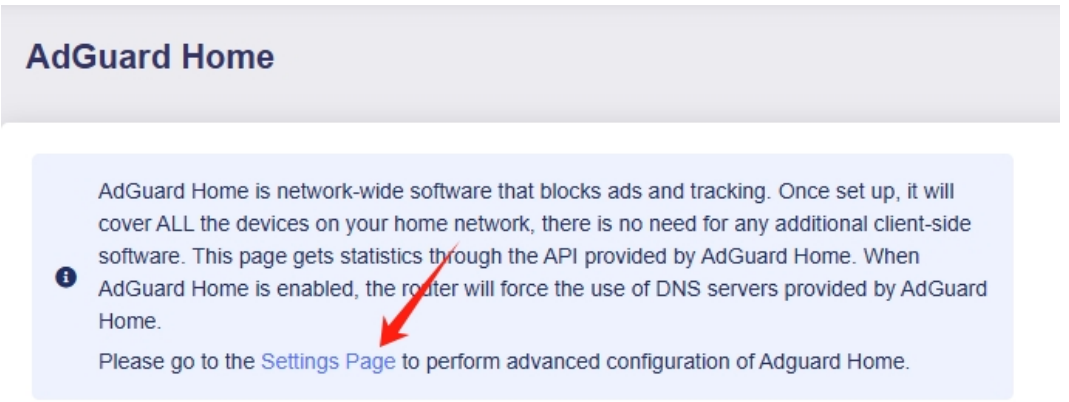


   - **AdGuard Home gestisce le richieste dei client**: se abilitato, le query DNS dai dispositivi client verranno gestite direttamente da AdGuard Home, ma ciò causerà il fallimento delle policy VPN basate sui domini.

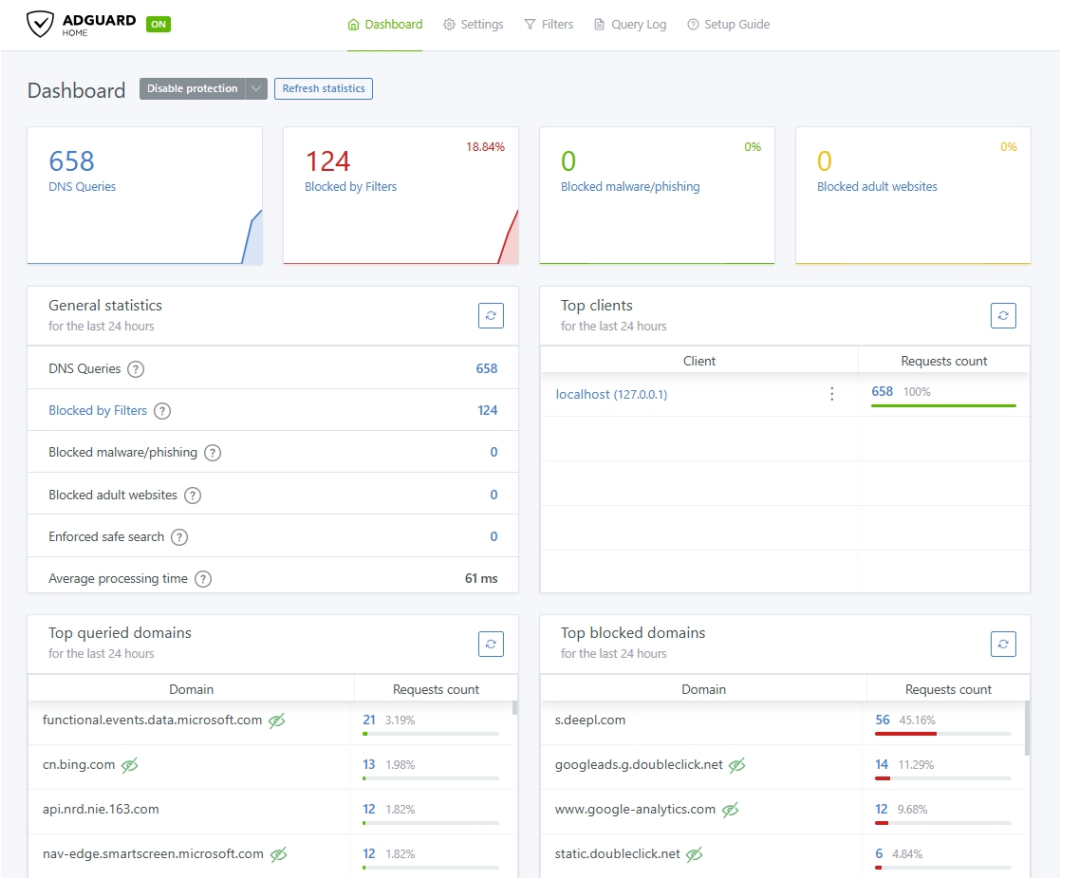
2. La pagina caricherà automaticamente le statistiche DNS (query, domini bloccati, ecc.) tramite l'API fornita da AdGuard Home.



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.



15.5 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.

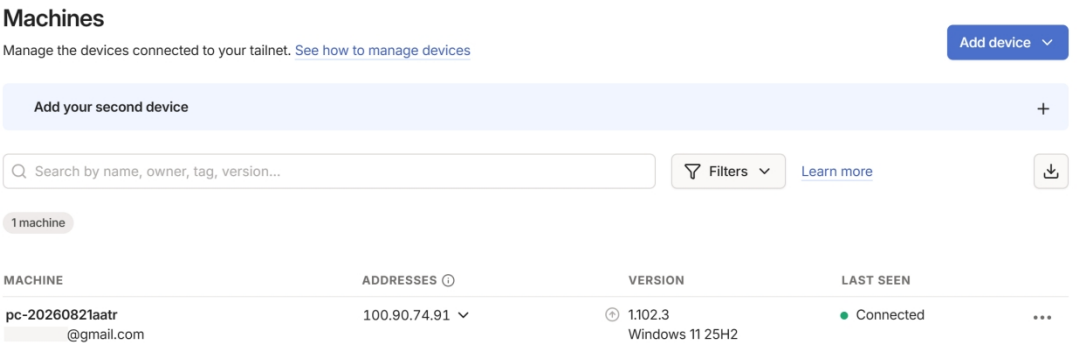
La funzionalità Tailscale sui router GL.iNet consente al router di unirsi a una rete virtuale Tailscale, consentendo l'accesso remoto al router stesso, nonché alle sue risorse lato WAN e LAN.

Nota:

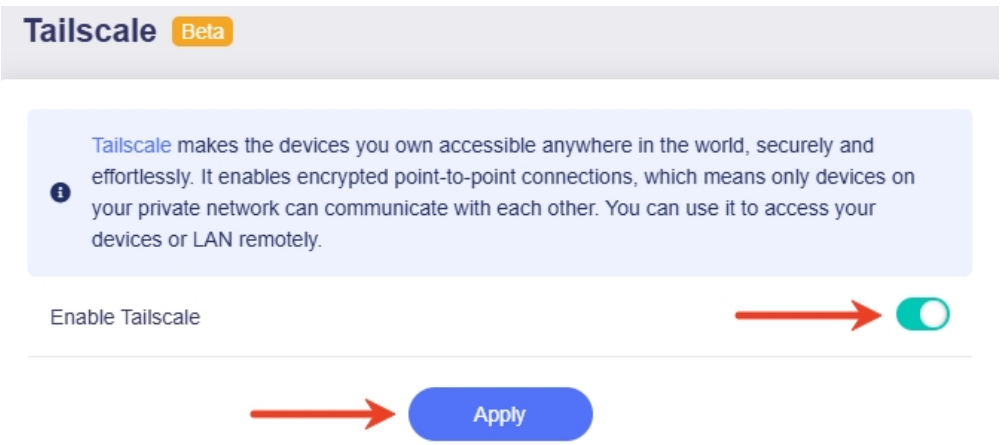
1. Poiché Tailscale è basato su WireGuard, non è consigliabile utilizzare Tailscale con una qualsiasi delle seguenti funzionalità o servizi contemporaneamente, poiché ciò potrebbe causare conflitti di routing: Client OpenVPN, Client WireGuard, GoodCloud da sito a sito, ZeroTier, AstroWarp.
2. Questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug.
3. I router GL.iNet non sono ancora disponibili come nodi di uscita. Questa funzione sarà disponibile nel firmware v4.9 e versioni successive.

15.5.1 Configurazione di Tailscale

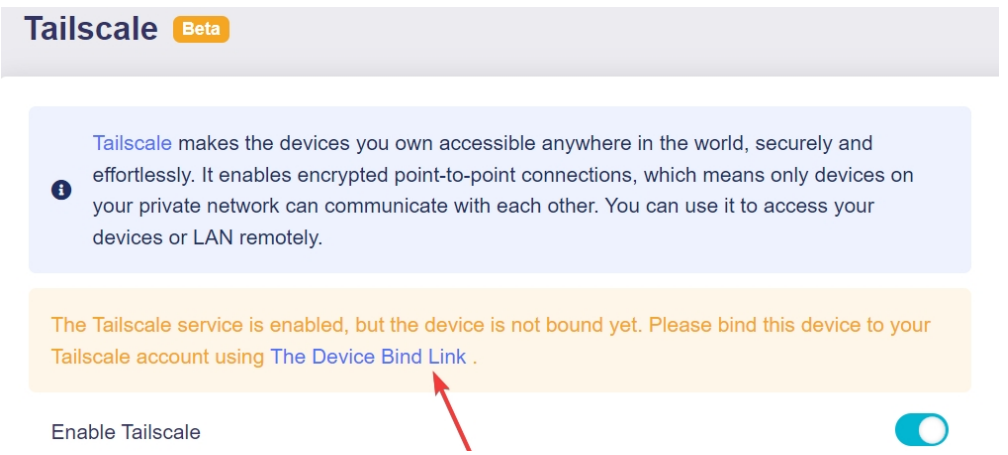
1. Registra prima un account Tailscale e associa uno o due dispositivi al tuo account Tailscale a scopo di test. Dopo l'associazione, vedrai i tuoi dispositivi nella console Tailscale.



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



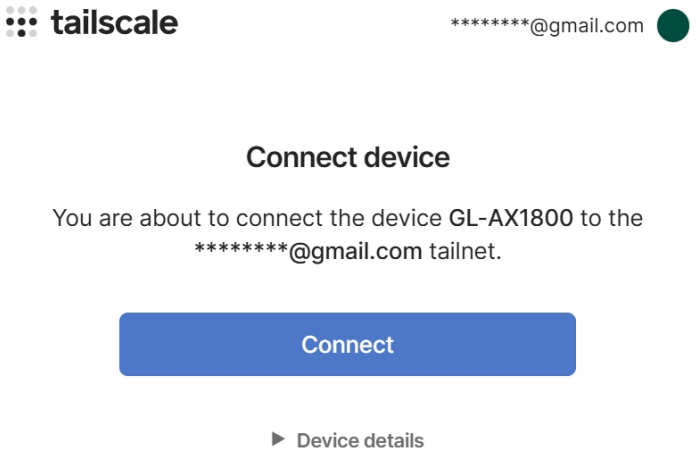
3. La pagina ti chiederà di associare il dispositivo. Fai clic su **Link di associazione del dispositivo**.



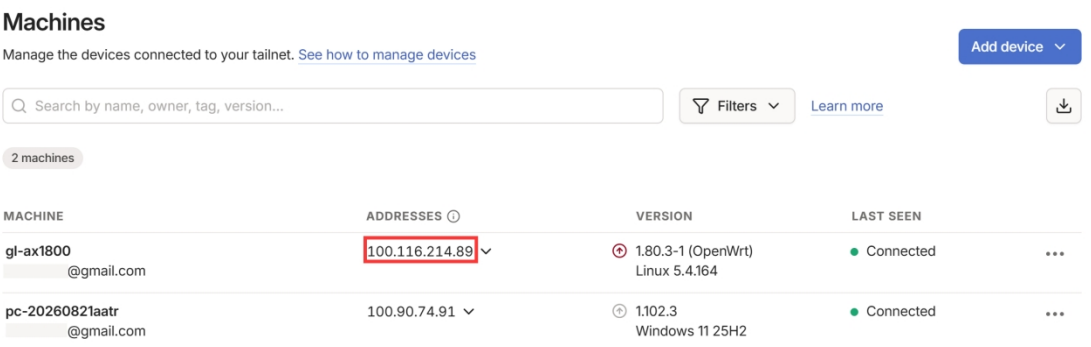
4. Nella finestra pop-up, fai clic sul collegamento e accedi con il tuo account Tailscale.



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



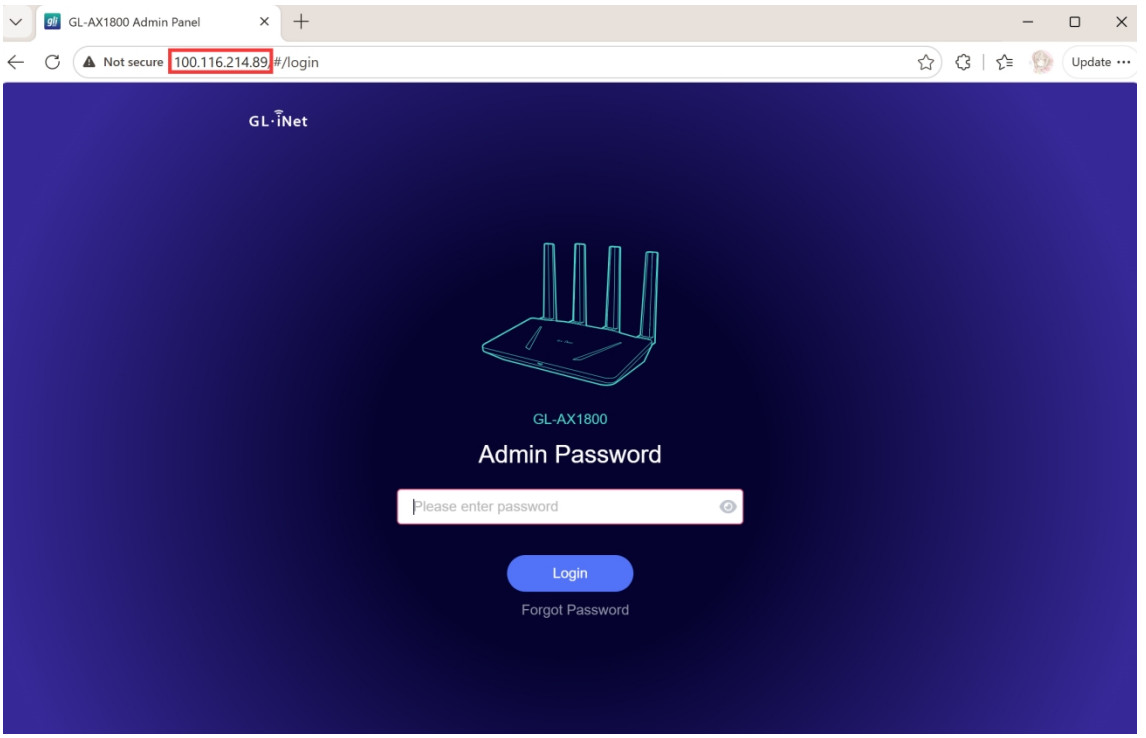
6. Verrai quindi reindirizzato alla console di amministrazione Tailscale. Ora il router è stato aggiunto alla rete virtuale Tailscale ed è possibile accedervi in remoto tramite l'IP virtuale Tailscale **100.116.214.89**.



7. Verifica connettività.

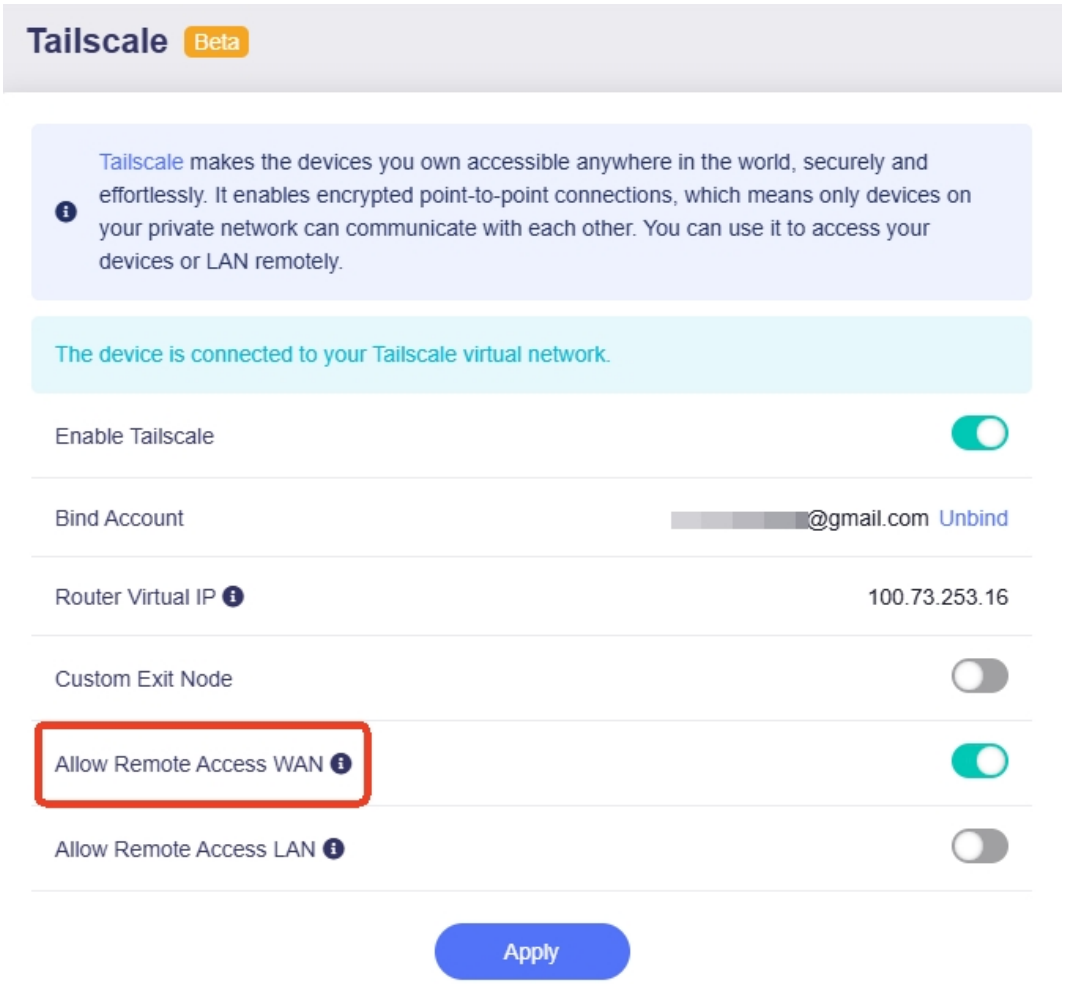
   Su un altro dispositivo connesso alla stessa rete Tailscale, apri un browser web e inserisci l'IP virtuale del router nella barra degli indirizzi. Se riesci ad accedere al pannello di amministrazione web del router, significa che Tailscale funziona. Puoi anche utilizzare

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



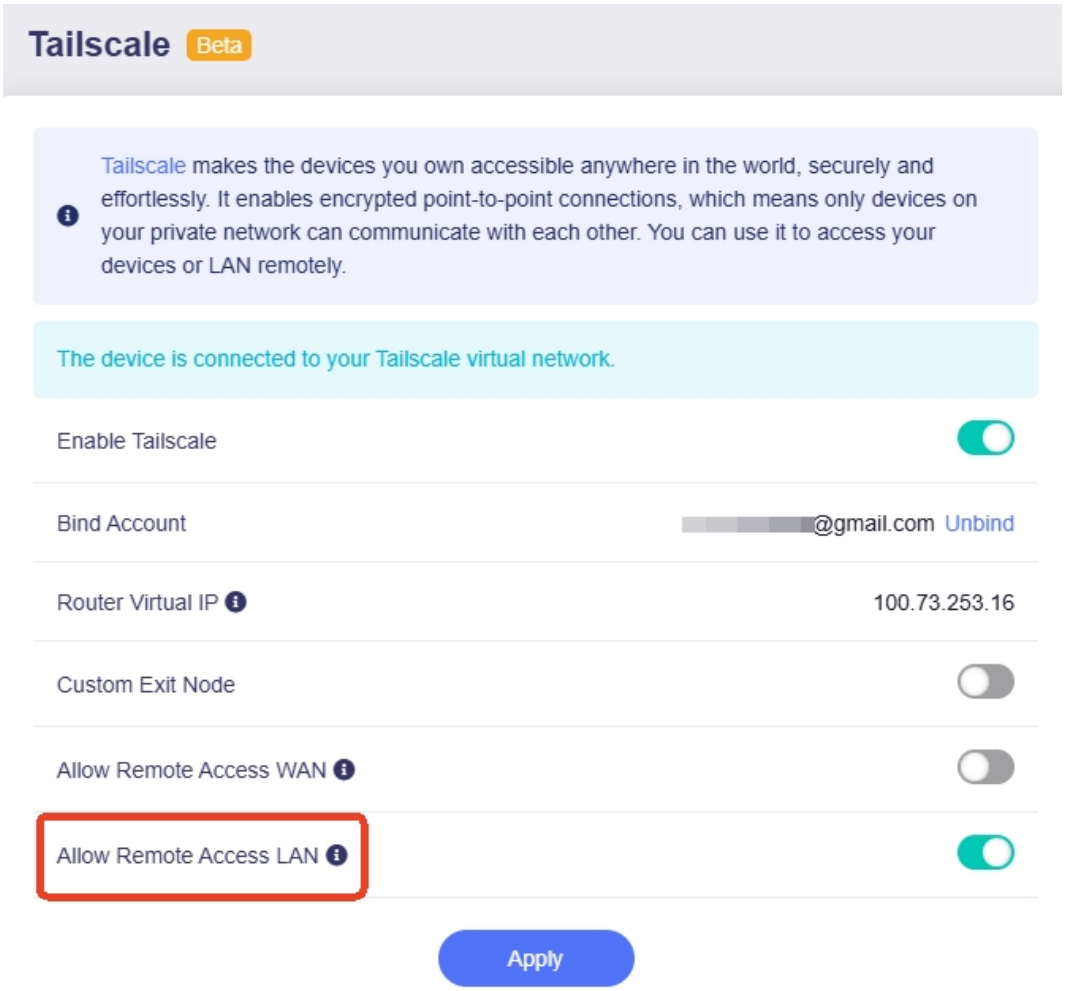
15.5.2 Consenti accesso remoto WAN

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



15.5.3 Consenti accesso remoto LAN

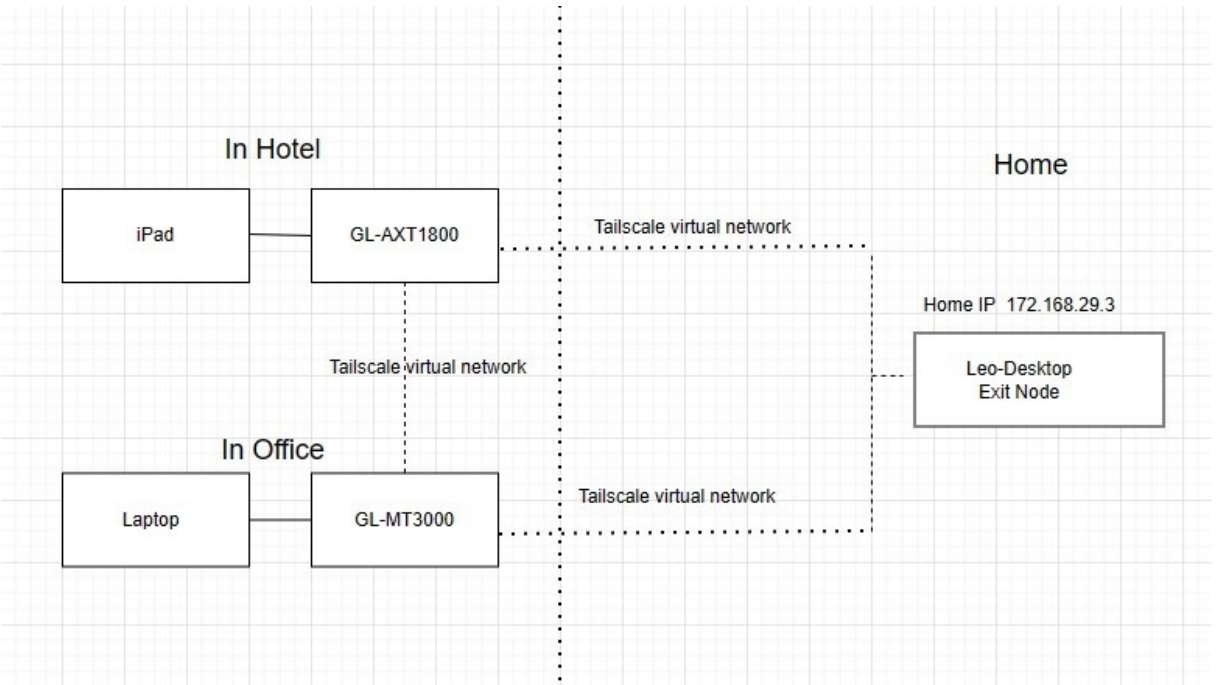
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato LAN del dispositivo tramite la rete virtuale Tailscale. Vedi qui per ulteriori dettagli.



13.5.4 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". Per configurare il nodo di uscita personalizzato sui router GL.iNet, fare riferimento a questo tutorial.

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

15.6 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:

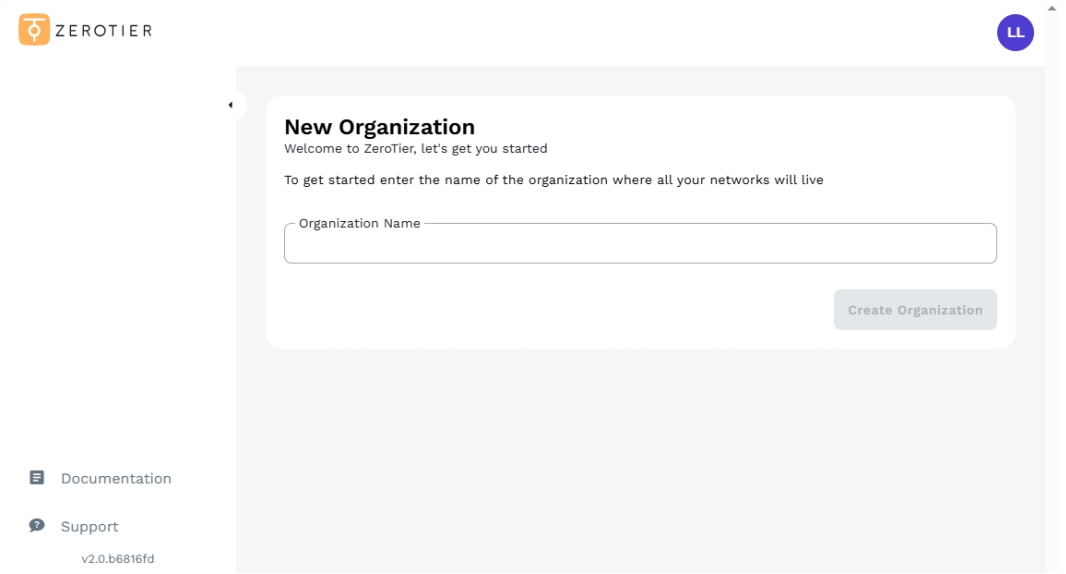
1. Non è consigliabile utilizzare ZeroTier contemporaneamente a una qualsiasi delle seguenti funzionalità o servizi, poiché ciò potrebbe causare conflitti di routing: Client OpenVPN, Client WireGuard, GoodCloud da sito a sito, Tailscale e AstroWarp.
2. Questa funzionalità è attualmente in versione beta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

15.6.1 Configurazione di ZeroTier

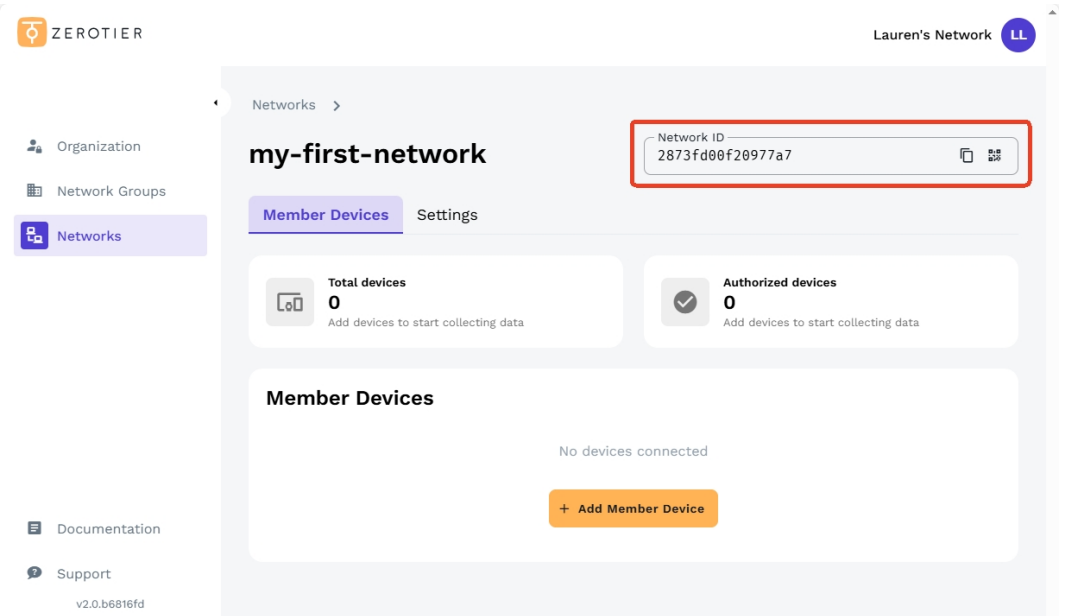
Sono disponibili due versioni di ZeroTier Central: New Central e Legacy Central.

I passaggi seguenti utilizzano New Central come esempio.

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

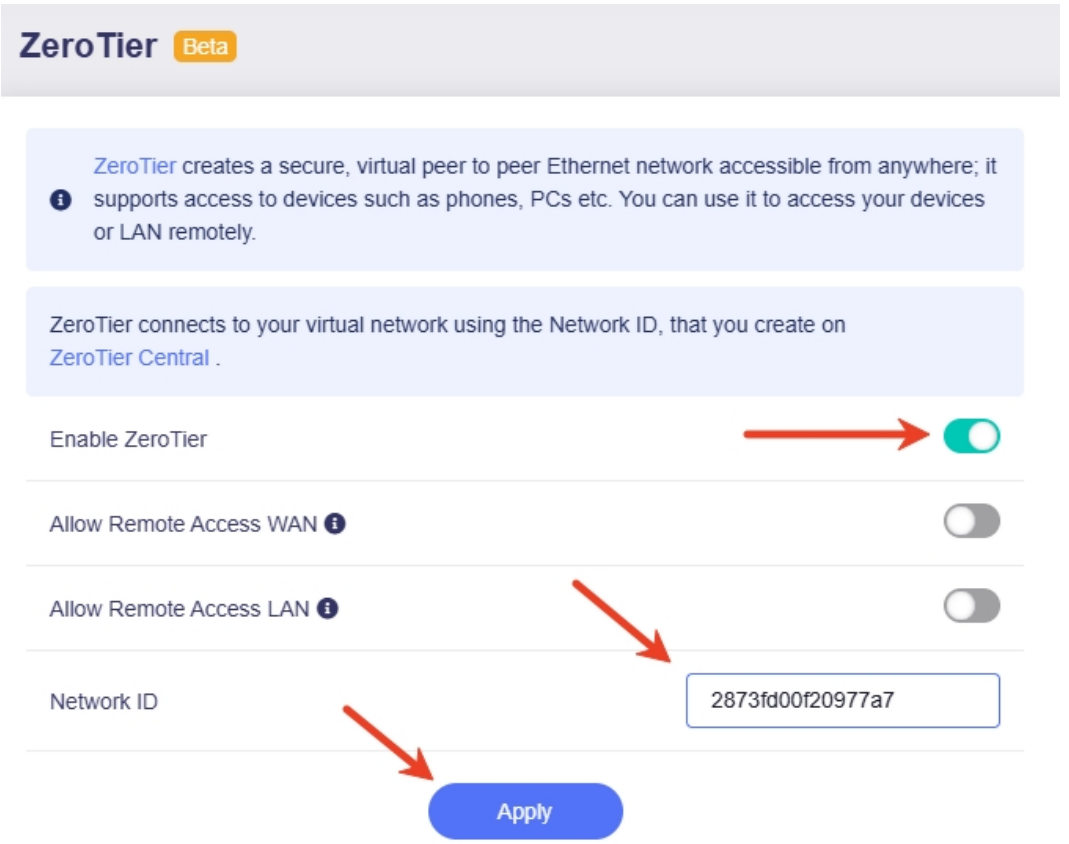


3. Seleziona un piano. Qui scegliamo **come esempio il piano Personal**, che include i dispositivi 10, l'amministratore di rete 1 e la rete 1. Se devi creare più reti, aggiungere più dispositivi o aggiungere percorsi e DNS personalizzati, scegli un altro piano a pagamento.
4. Ora la tua rete ZeroTier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

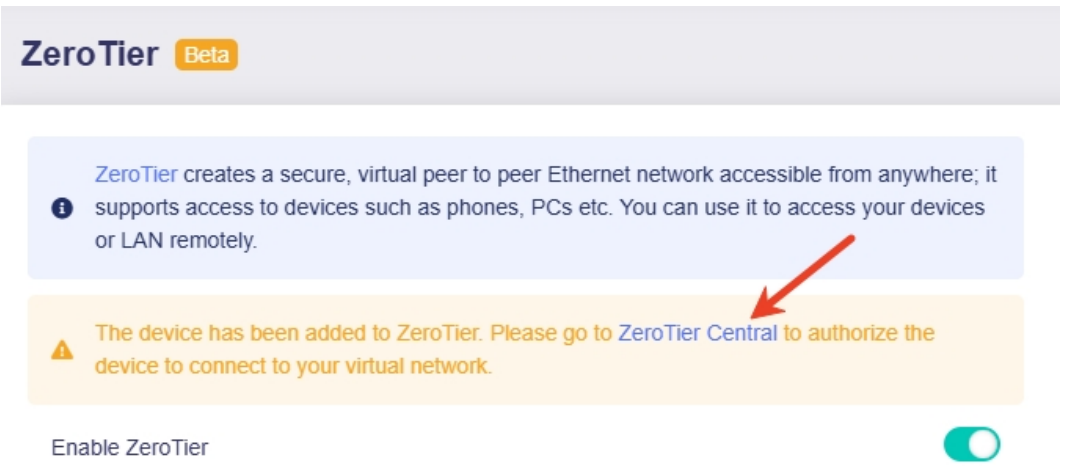


Usa nota **dell'ID di rete**, che è una combinazione alfanumerica di caratteri 16 nell'angolo in alto a destra, poiché sarà richiesto quando connetterai altri dispositivi in seguito.

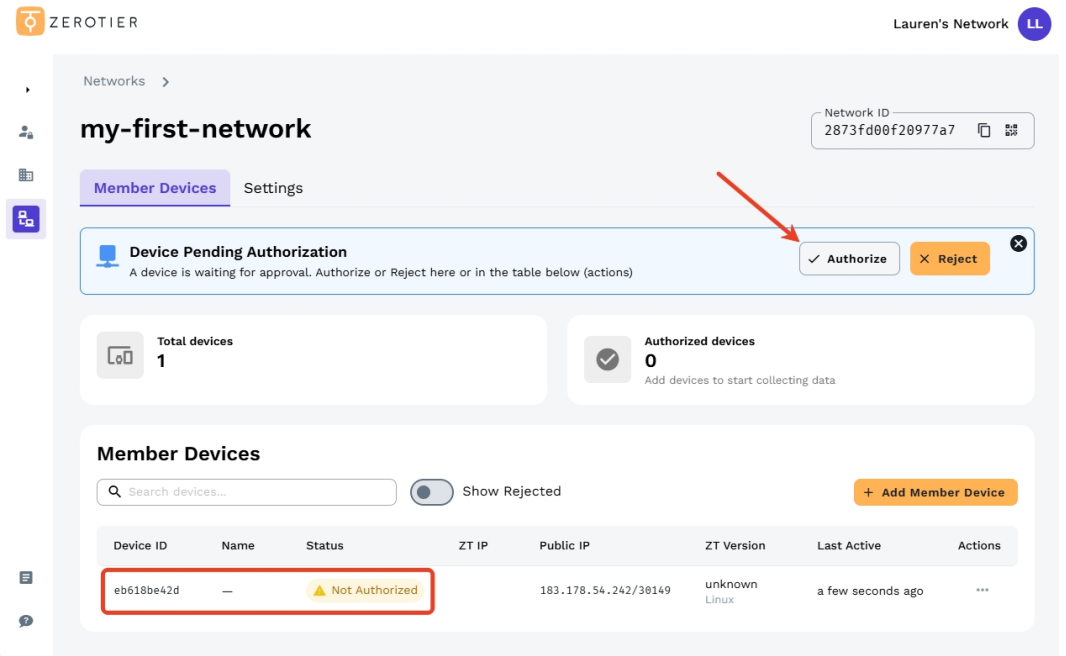
5. Accedi al pannello di amministrazione web del tuo router e vai su **APPLICAZIONI** > **ZeroTier**. Abilita ZeroTier, inserisci **l'ID di rete**, quindi fai clic su **Applica**.



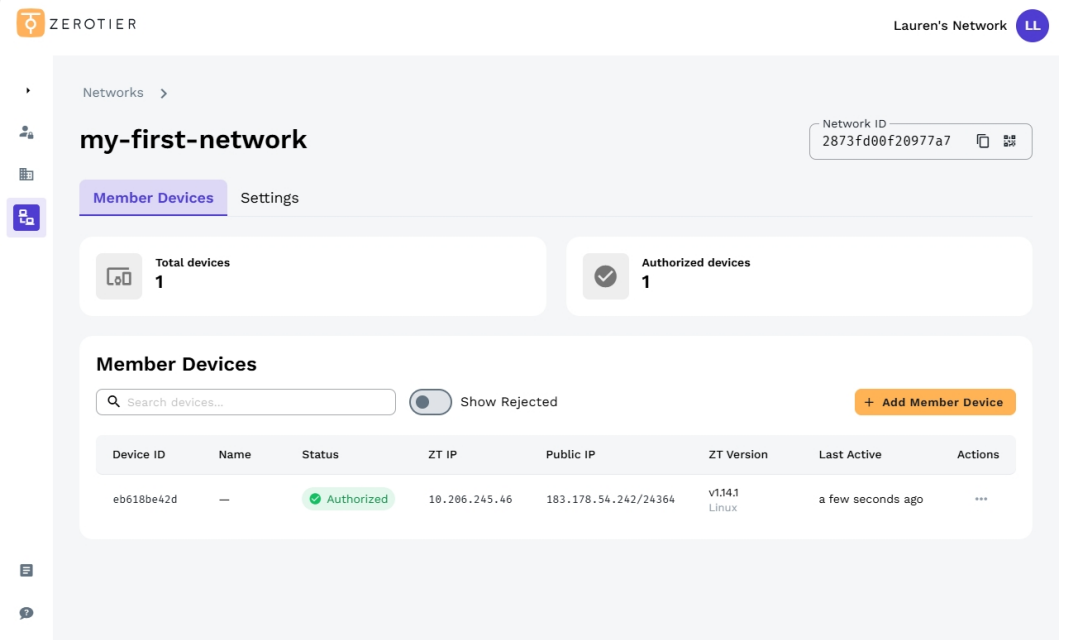
Dopo poco, la pagina indicherà che è necessaria l'autorizzazione. Fare clic **sul collegamento ipertestuale ZeroTier Central** per reindirizzare allo ZeroTier Central.



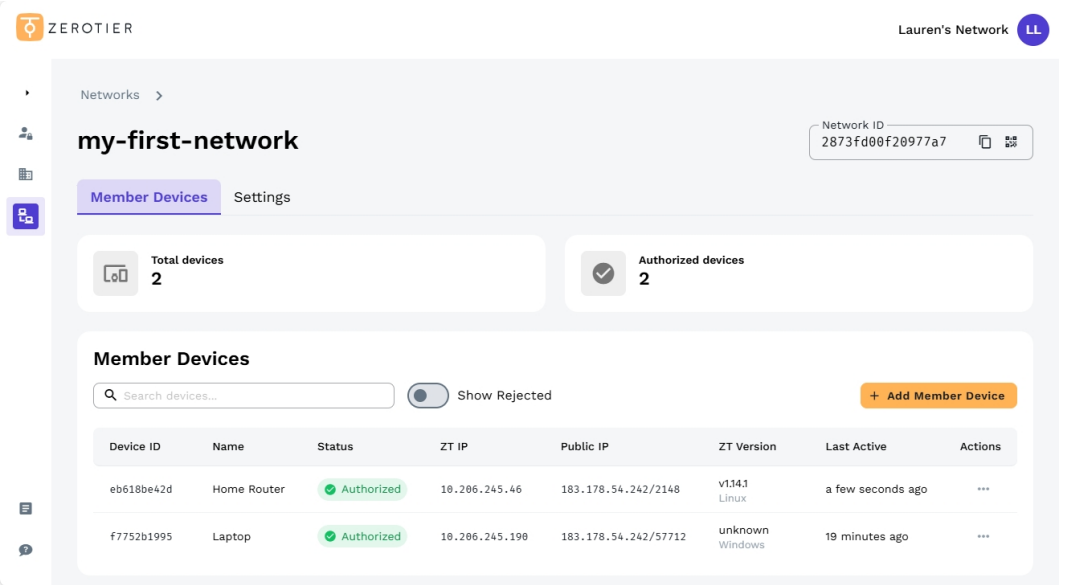
6. Sul ZeroTier Central, individua il dispositivo in sospeso e autorizzalo.



Una volta autorizzata, la pagina viene visualizzata come segue.

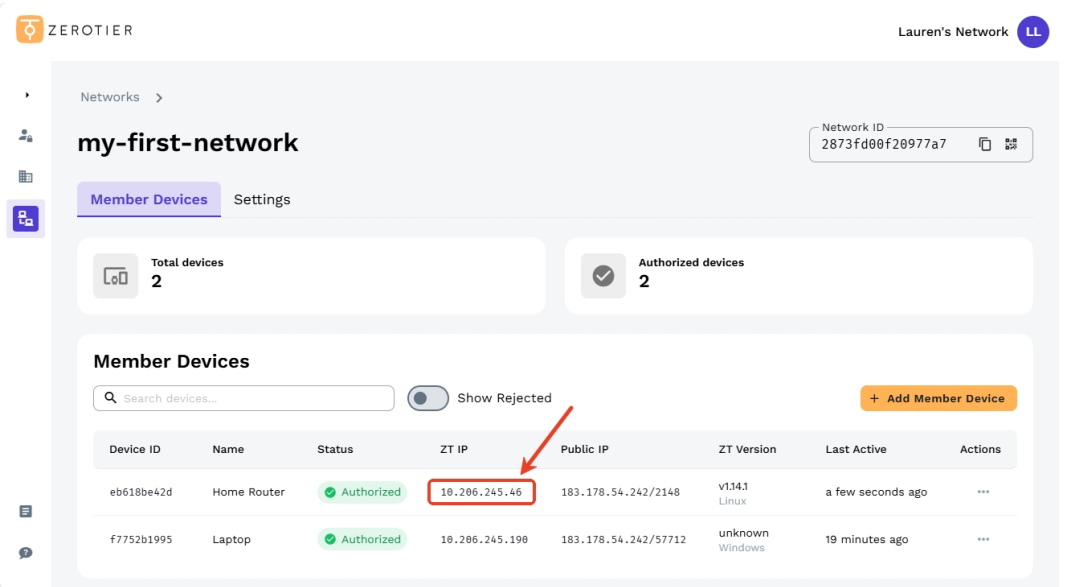


7. Aggiungi un altro dispositivo (come un computer o uno smartphone) alla stessa rete ZeroTier seguendo questa guida. Una volta aggiunta correttamente, la pagina viene visualizzata come segue. Vedrai i dettagli dei dispositivi membri, come ID dispositivo, nome, stato, IP gestito e IP pubblico.



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

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

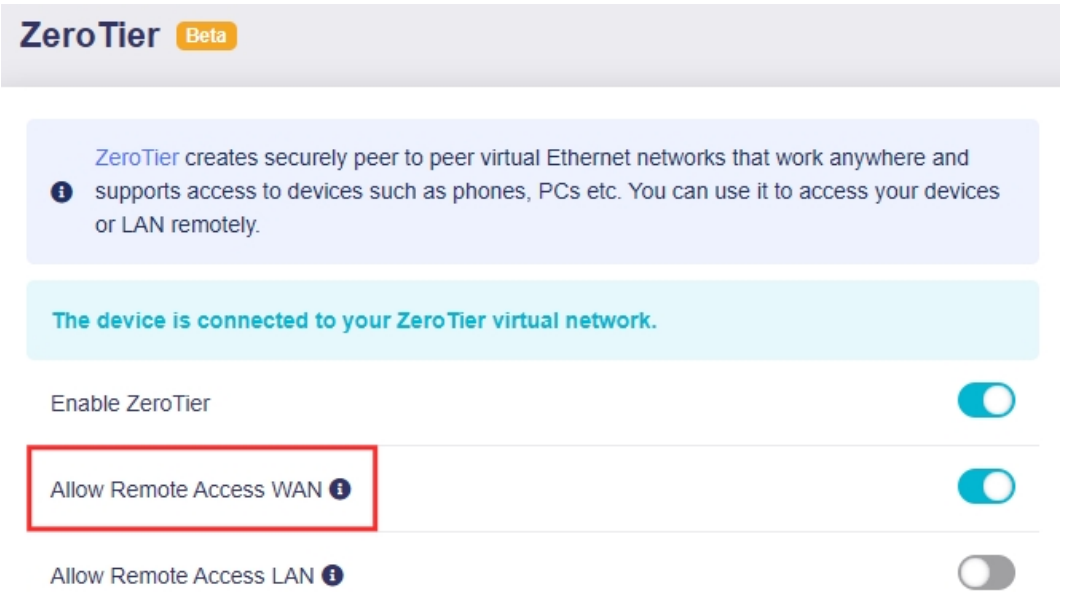


Puoi quindi utilizzare questo IP gestito per accedere al router dal tuo laptop che si trova sulla stessa rete ZeroTier.

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

15.6.2 Consenti accesso remoto WAN

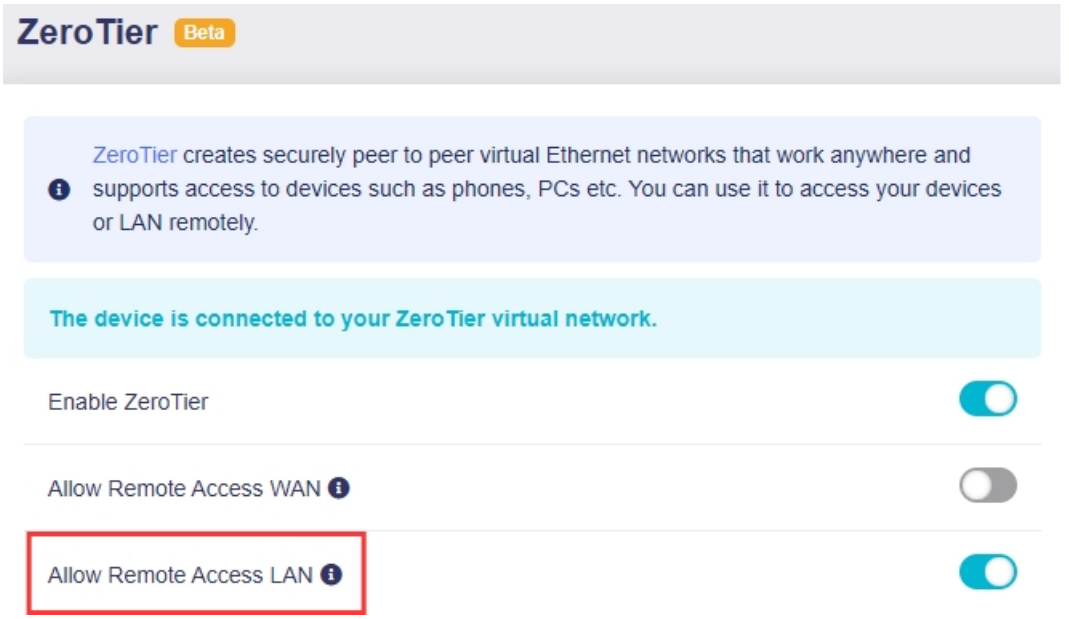
Se questa opzione è abilitata, è possibile accedere alle risorse sul lato WAN del dispositivo tramite la rete virtuale ZeroTier. Vedi qui per maggiori dettagli.



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.

15.6.3 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.



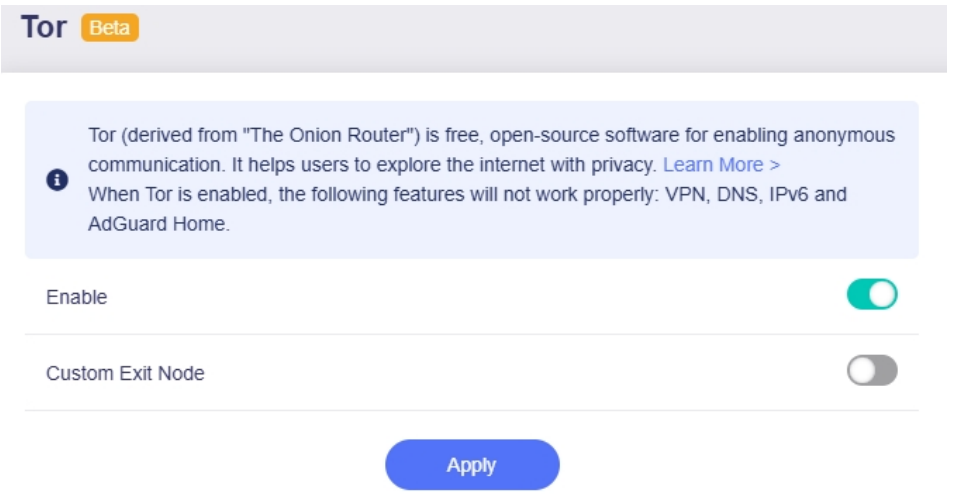
Nota: questa funzionalità richiede l'aggiunta di regole di routing alla rete ZeroTier per avere effetto. È possibile aggiungere gratuitamente un percorso personalizzato in Legacy Central, mentre in New Central puoi configurare percorsi personalizzati solo con un piano Essential o superiore. Vedi qui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

15.7 Tor

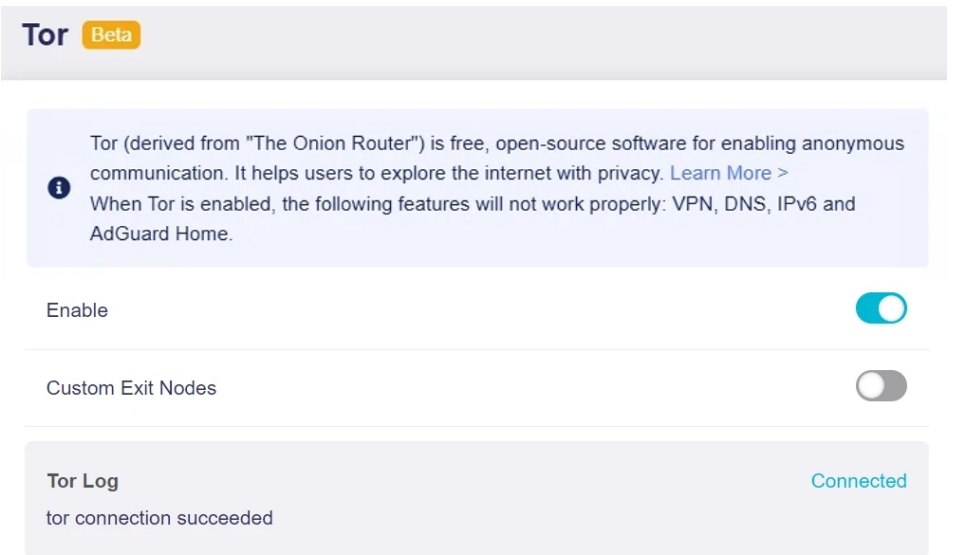
Tor (derivato da **The Onion Router**) è un software gratuito e open source per consentire la comunicazione anonima. Aiuta gli utenti a esplorare Internet con privacy. Tieni presente che questa funzionalità è attualmente in versione beta e potrebbe presentare alcuni bug. Quando Tor è abilitato, le seguenti funzionalità non funzioneranno correttamente: VPN, DNS, IPv6 e AdGuard Home.

Segui i passaggi seguenti per configurare Tor se necessario.

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 se necessario e fai clic su **Applica**.



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



Capitolo 16

Sistema

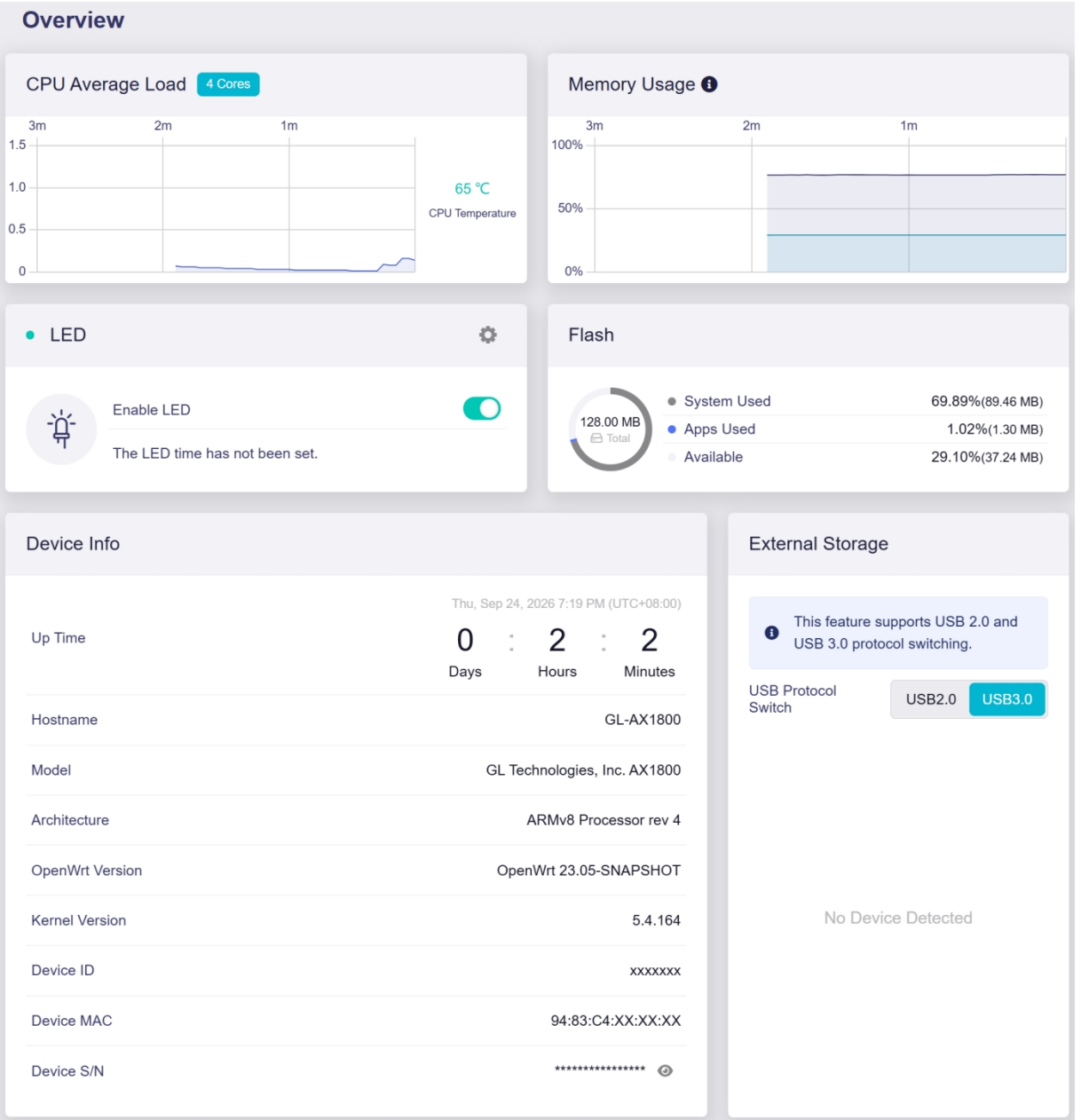
Questo capitolo tratta gli strumenti di gestione del sistema per il dispositivo, come panoramica del sistema, aggiornamento, attività pianificate, fuso orario, registro, ripristino del firmware e impostazioni avanzate.

16.1 Panoramica

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

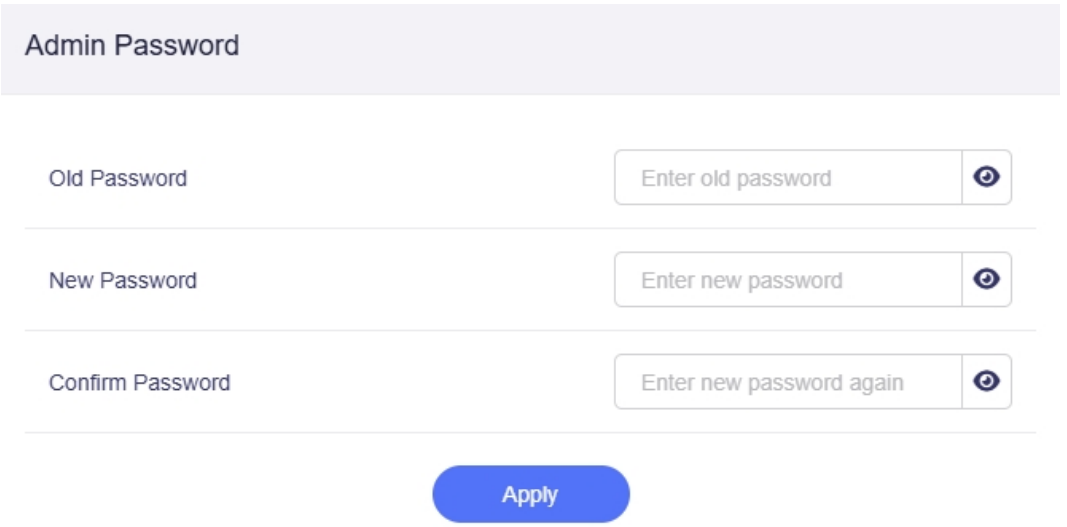
Questa pagina mostra lo stato dell'hardware e supporta alcuni semplici controlli, tra cui:

- Stato CPU, memoria e flash
- Controllo LED
- Informazioni sul dispositivo
- Cambio del protocollo di archiviazione esterna



16.2 Password amministratore

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



I requisiti per la password amministratore sono i seguenti:

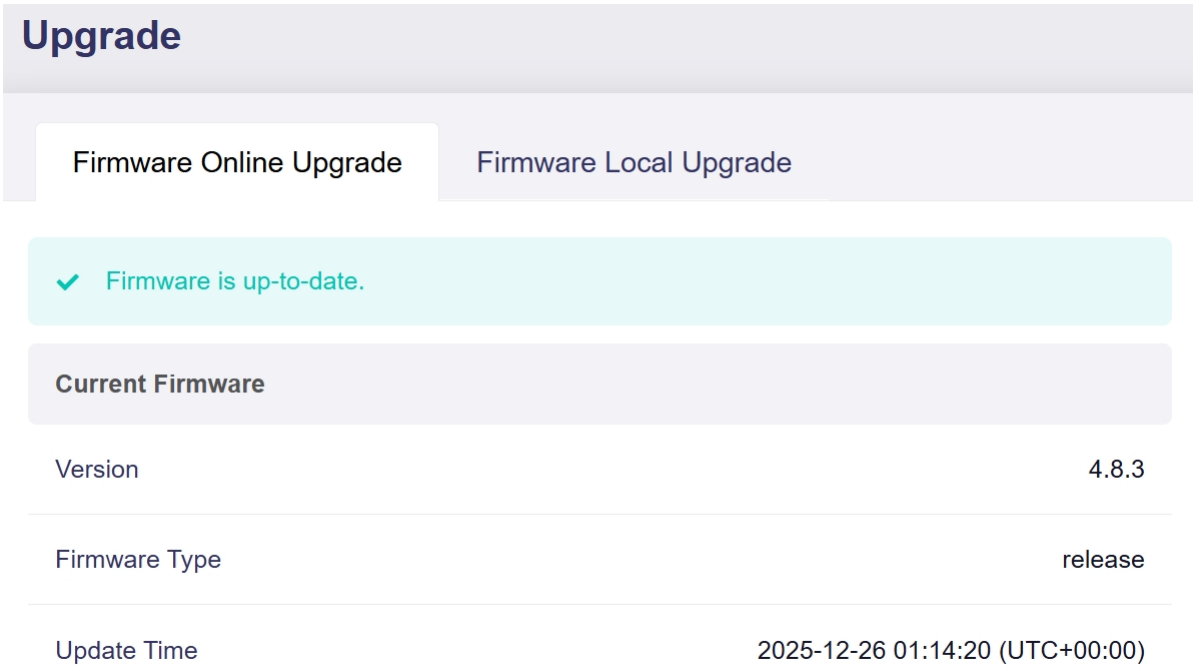
1. Minimo 10 caratteri e massimo 63 caratteri di lunghezza.
2. Sono consentiti lettere (con distinzione tra maiuscole e minuscole), numeri e simboli (ad esempio,! @ # $ % ^ & * ( ) _ + - =,. > < |? / \ [ ] { }:; " ' ` ~).
3. Sono richieste almeno due delle seguenti categorie: lettere maiuscole, lettere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

16.3 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.

16.3.1 Aggiornamento online

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

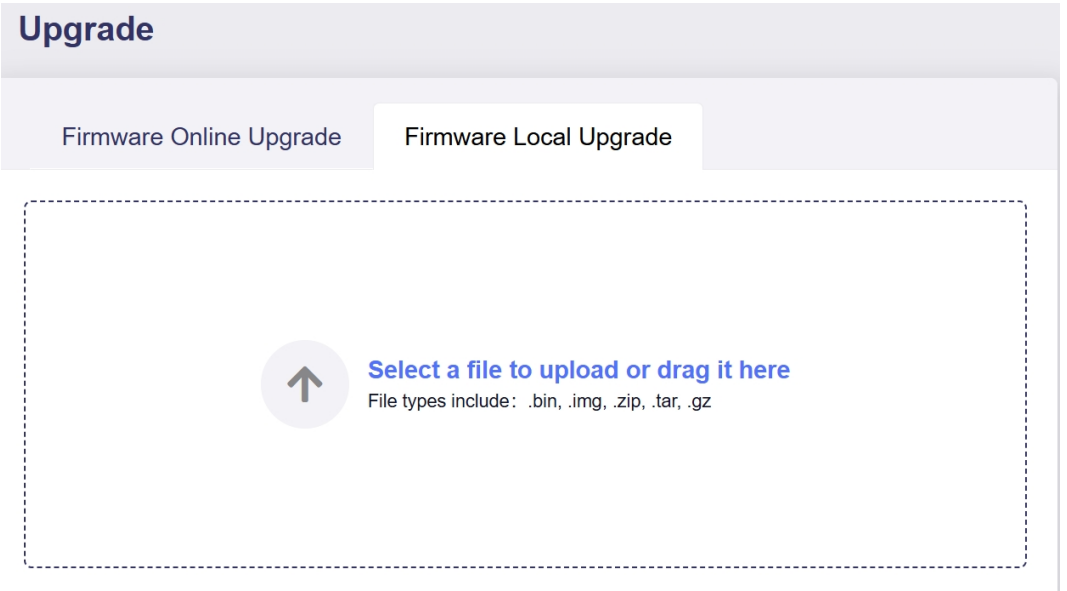


Suggerimento: quando provi a eseguire un aggiornamento online, se viene visualizzato **Download non riuscito**, vai a **SISTEMA** > **Fuso orario** e correggi l'errore del fuso orario (sincronizzazione con il browser).

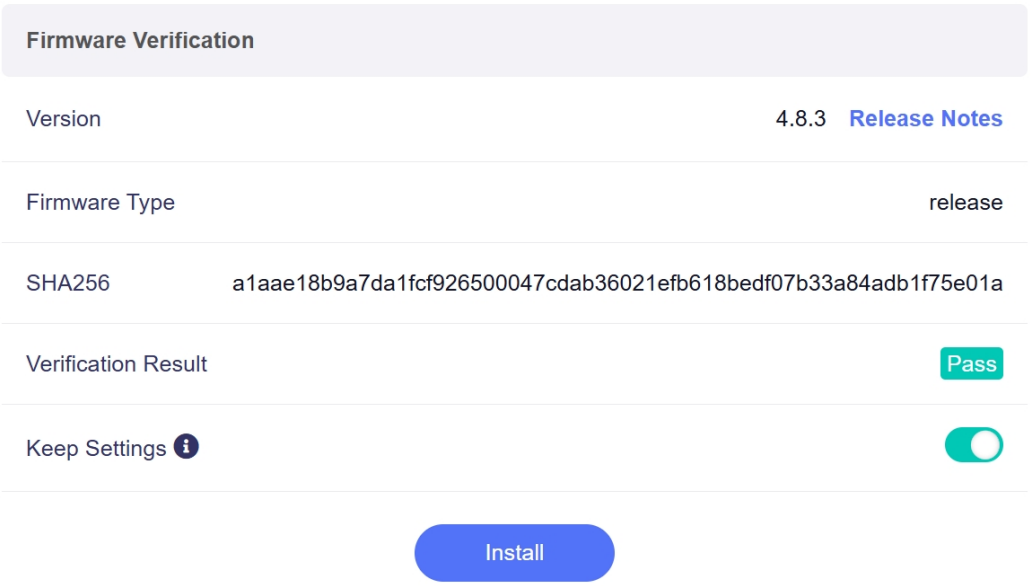
16.3.2 Aggiornamento locale

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

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



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



- **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.

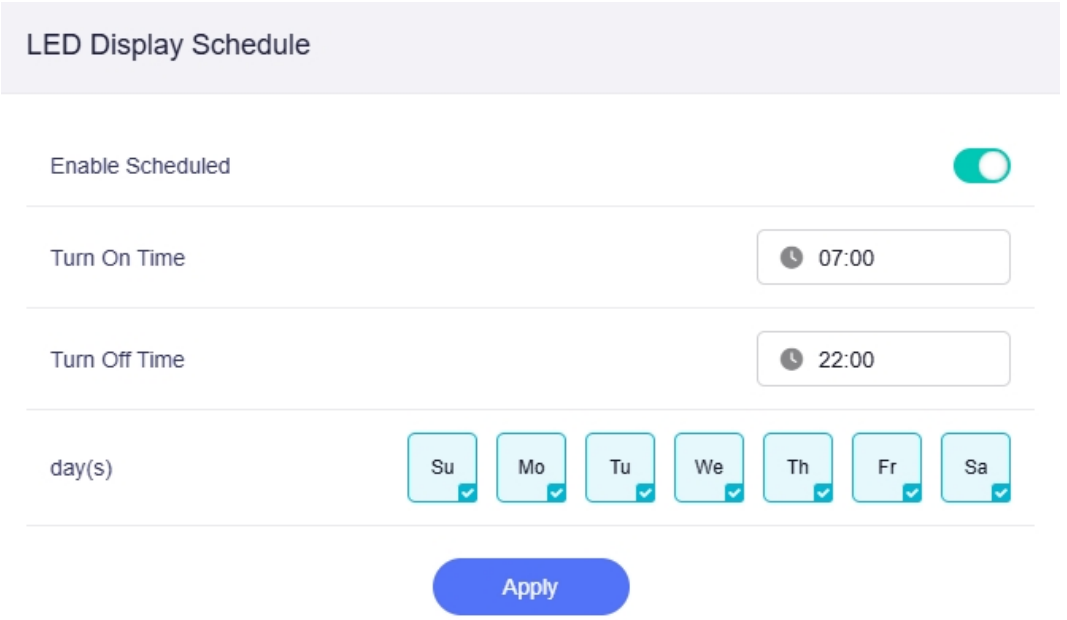
16.4 Attività pianificate

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

16.4.1 Programmazione del LED

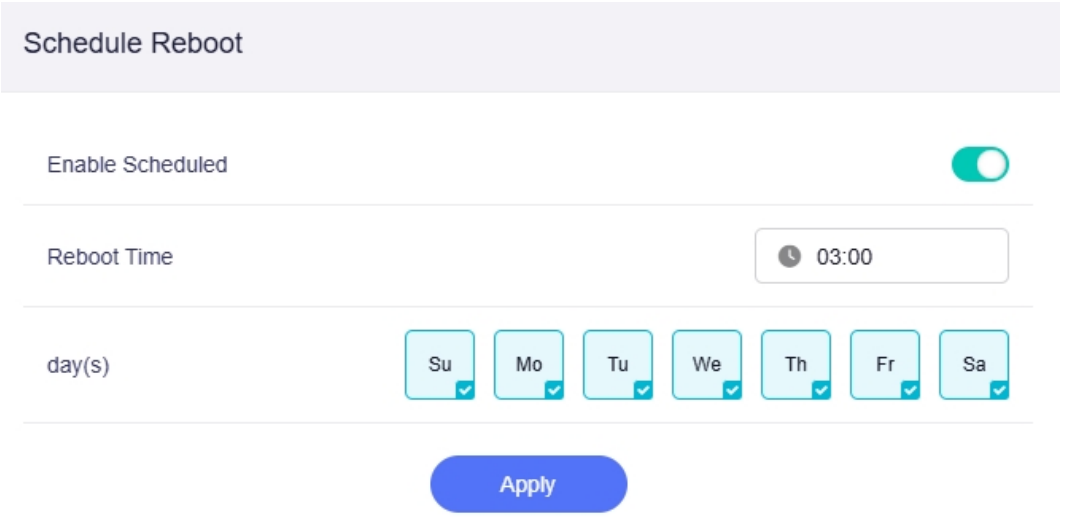
Imposta una pianificazione per la luce LED del router, se necessario, quindi fai clic su **Applica**.



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

16.4.2 Riavvio pianificato

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



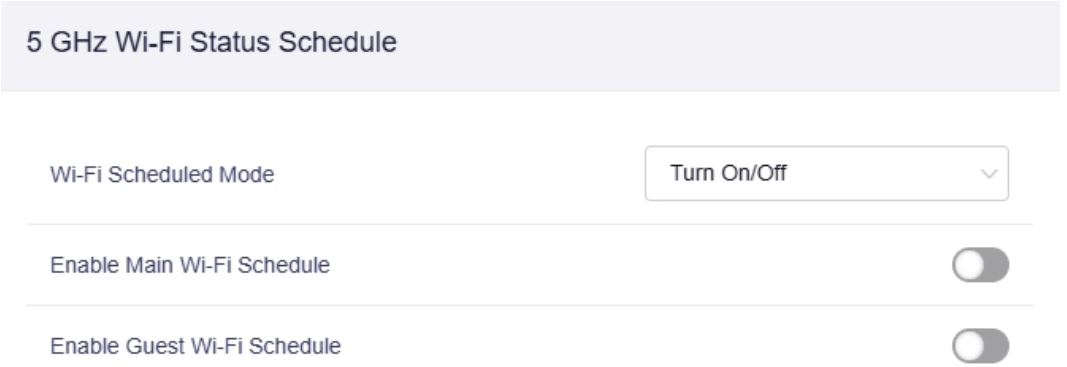
- **Abilita programmazione**: attiva questo interruttore per abilitare il riavvio pianificato.
- **Durata di riavvio**: imposta l'ora specifica (ad esempio 03:00) in cui il router si riavvierà.
- **giorno(i): seleziona i giorni** effettivi della settimana per queste impostazioni.

16.4.3 Programmazione del Wi-Fi a 5 GHz

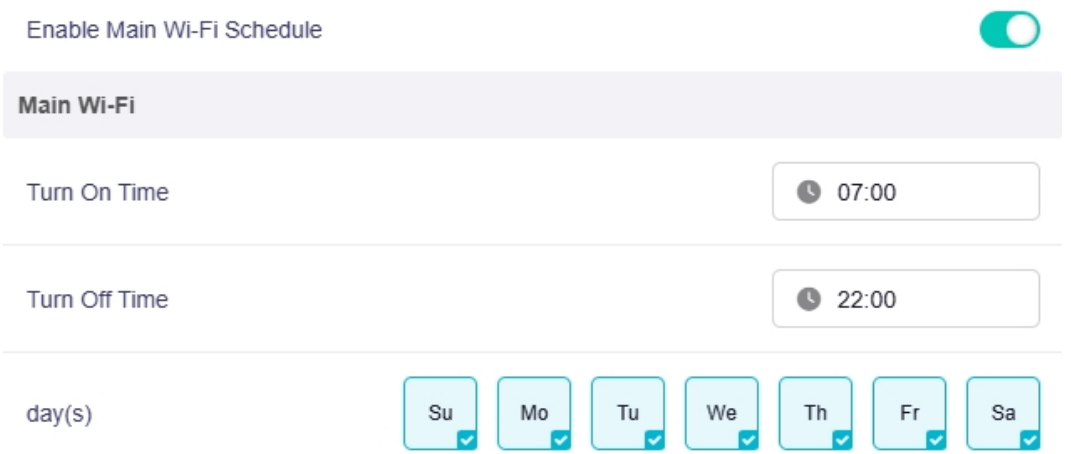
Questa funzione ti consente di impostare un programma per il tuo 5 GHz Wi-Fi. Sono disponibili due modalità: Accendi/Spegni e Cambia potenza TX.

Modalità 1: accensione/spegnimento

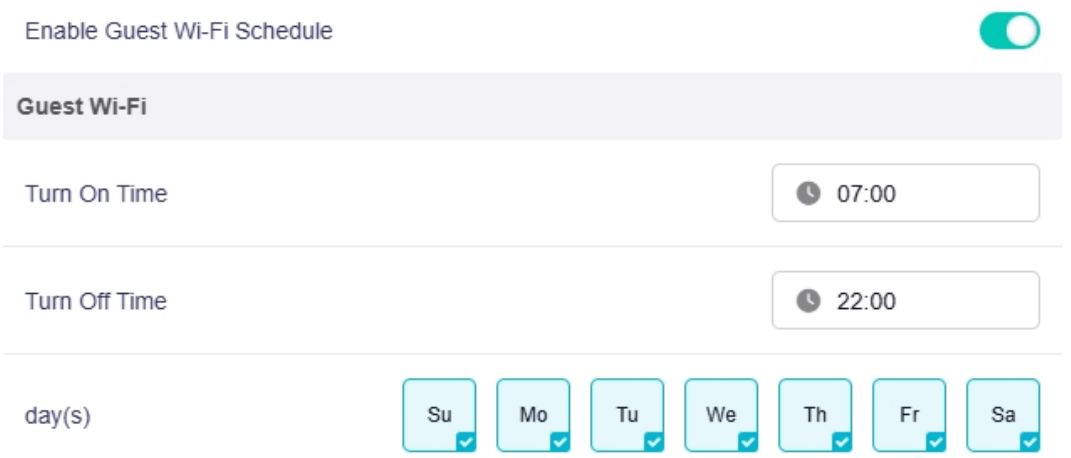
È possibile abilitare la pianificazione di accensione/spegnimento sia per 5 GHz Principale Wi-Fi che per Ospite Wi-Fi.



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

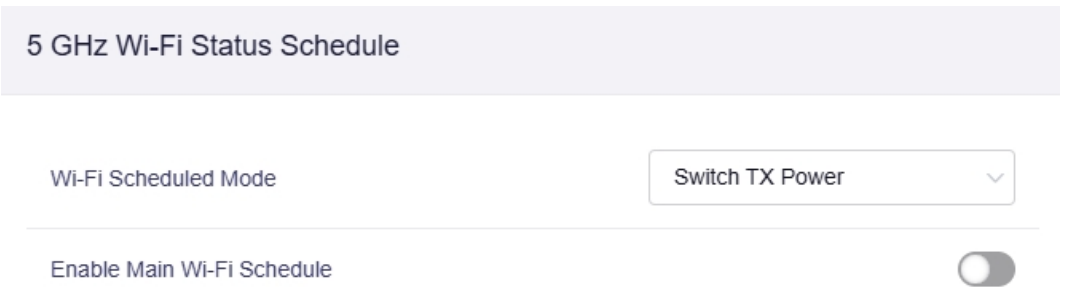


- **Programmazione del Wi-Fi ospiti**: se abilitato, imposta gli orari di accensione e spegnimento per il tuo 5 GHz Ospite Wi-Fi e seleziona una data effettiva per la settimana.

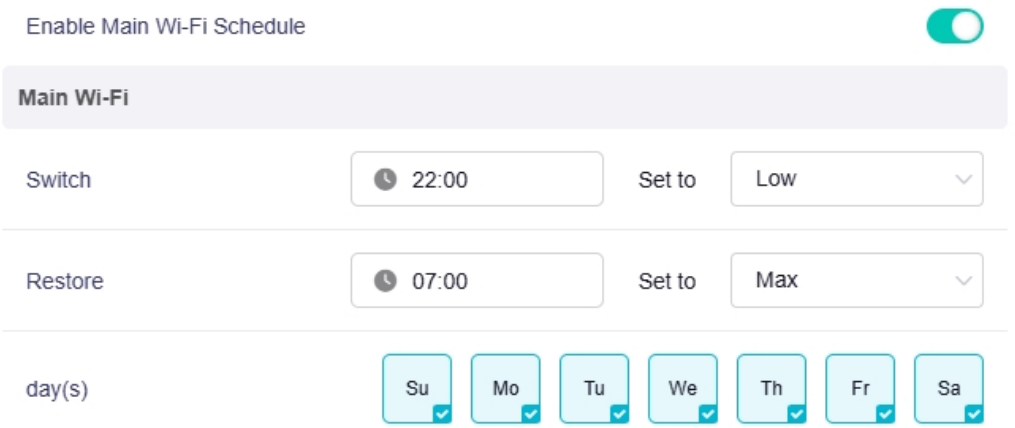


Modalità 2: cambia potenza TX

È possibile abilitare la pianificazione della commutazione dell'potenza TX per 5 GHz Wi-Fi principale.



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



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

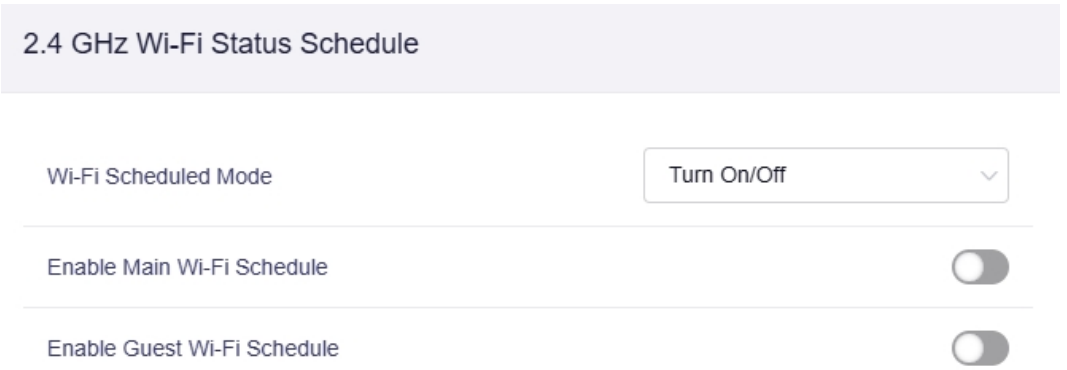
- **Ripristina**: ripristina la potenza TX a un altro livello (ad esempio Max) in un altro momento (ad esempio 07:00).
- **Giorni**: seleziona i giorni effettivi della settimana per queste impostazioni.

16.4.4 Programmazione del Wi-Fi a 2,4 GHz

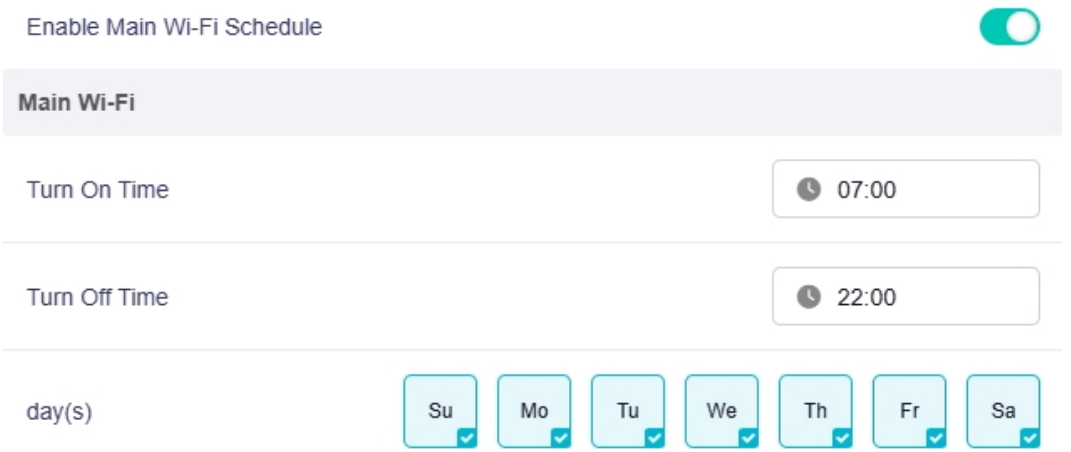
Questa funzione ti consente di impostare un programma per il tuo 2.4 GHz Wi-Fi. Sono disponibili due modalità: Accendi/Spegni e Cambia potenza TX.

Modalità 1: accensione/spegnimento

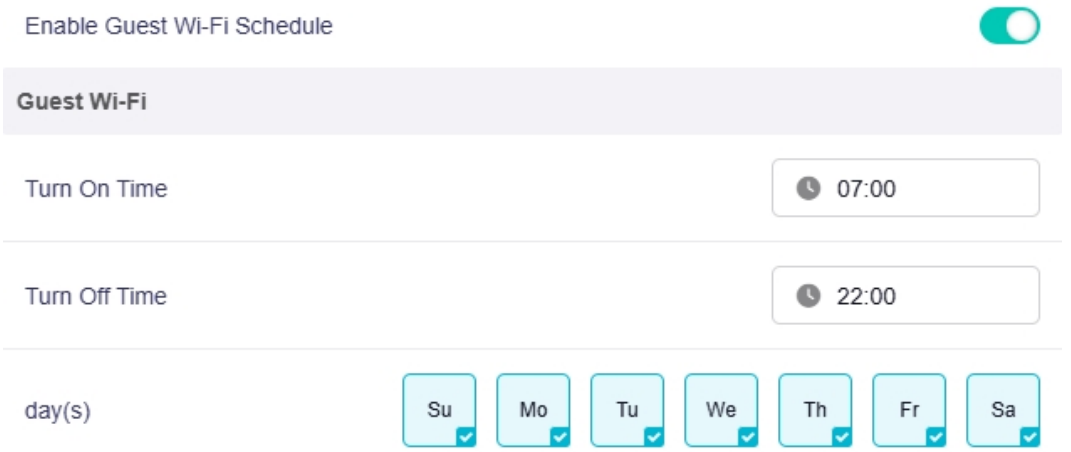
È possibile abilitare la pianificazione di accensione/spegnimento sia per 2.4 GHz Principale Wi-Fi che per Ospite Wi-Fi.



- **Programmazione del Wi-Fi principale**: se abilitato, imposta gli orari di accensione e spegnimento per il tuo 2.4 GHz Wi-Fi principale e seleziona una data effettiva per la settimana.

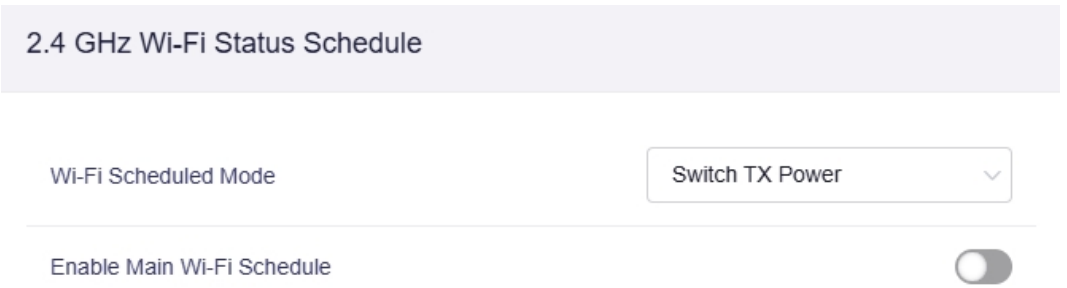


- **Programmazione del Wi-Fi ospiti**: se abilitato, imposta gli orari di accensione e spegnimento per il tuo 2.4 GHz Ospite Wi-Fi e seleziona una data effettiva per la settimana.

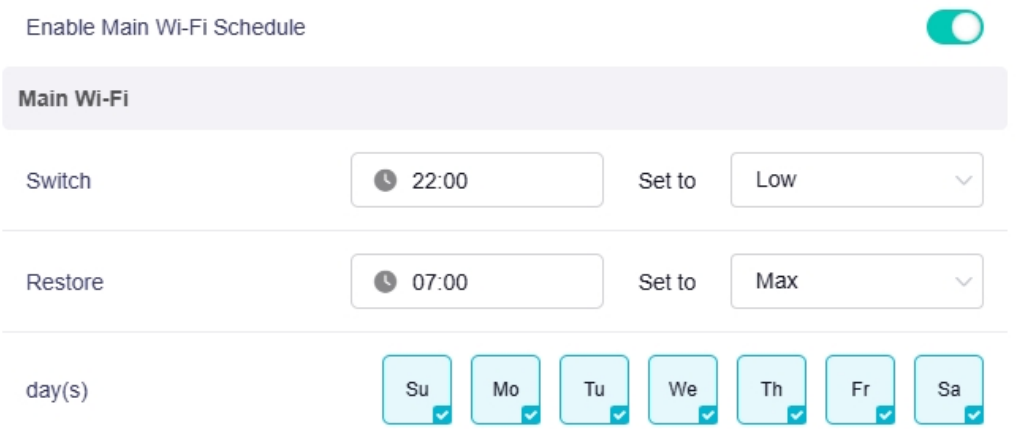


Modalità 2: cambia potenza TX

È possibile abilitare la pianificazione della commutazione della potenza TX per 2.4 GHz Wi-Fi principale.



Se abilitato, imposta due azioni temporizzate per il tuo 2.4 GHz Wi-Fi principale per cambiare la potenza TX e seleziona una data effettiva per la settimana.

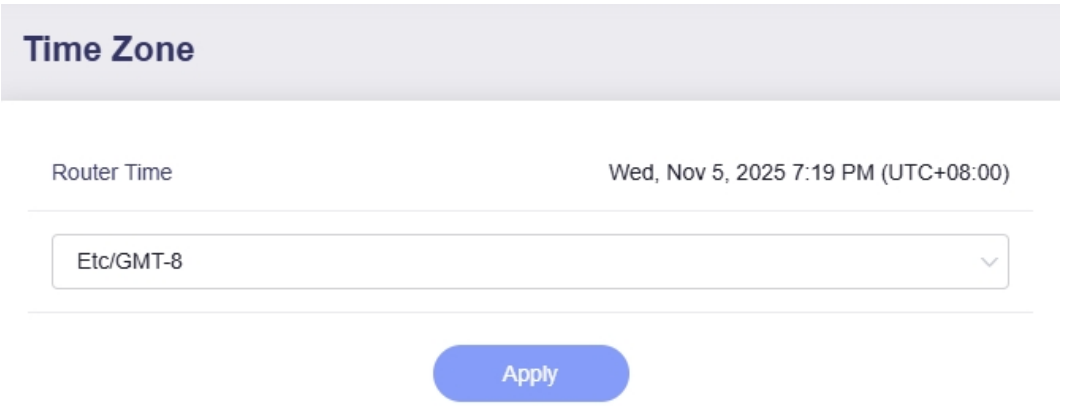


- **Interruttore**: imposta la potenza TX su un determinato livello (ad esempio Basso) a un orario specifico (ad esempio 22:00).

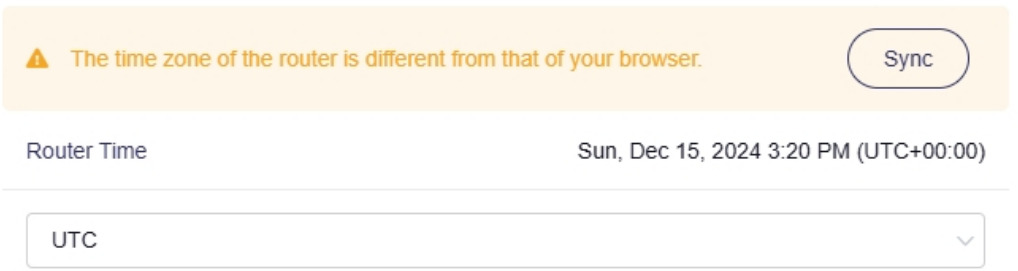
- **Ripristina**: ripristina la potenza TX a un altro livello (ad esempio Max) in un altro momento (ad esempio 07:00).
- **Giorni**: seleziona i giorni effettivi della settimana per queste impostazioni.

16.5 Fuso orario

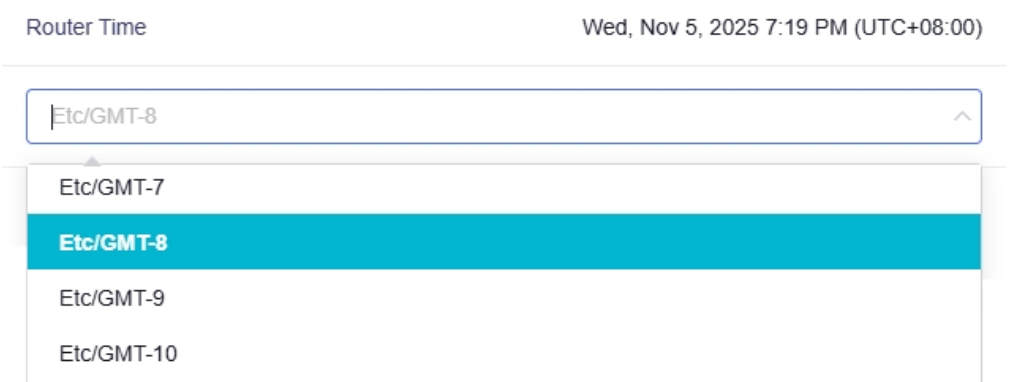
Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Fuso orario**. Questa pagina mostra l'ora di sistema del router, indicando la data, l'ora e la differenza di fuso orario corrispondente.



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



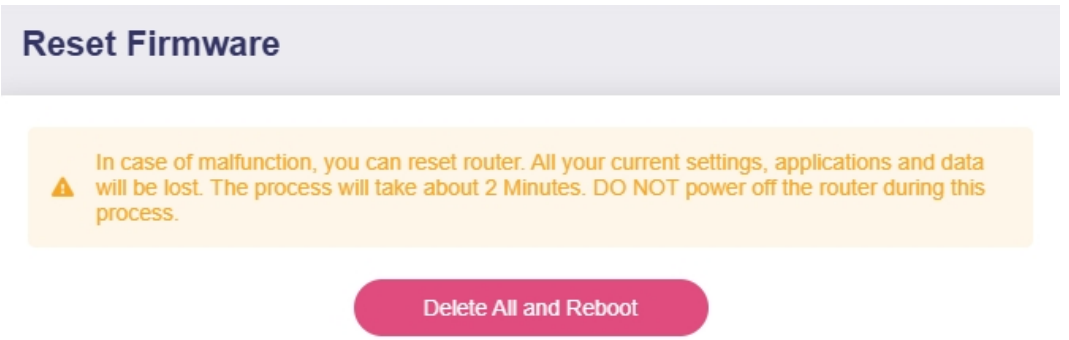
Per cambiare fuso orario, seleziona il fuso orario appropriato dall'elenco per assicurarti che l'ora di sistema del router corrisponda all'ora locale.



16.6 Ripristino del firmware

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

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

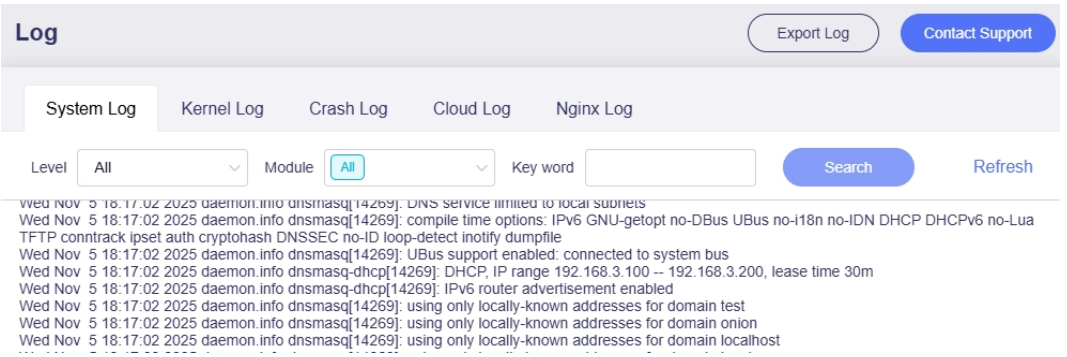


Nota: tutte le impostazioni, le applicazioni e i dati correnti verranno cancellati. Il processo richiederà circa 2 minuti. Non spegnere il router durante questo processo.

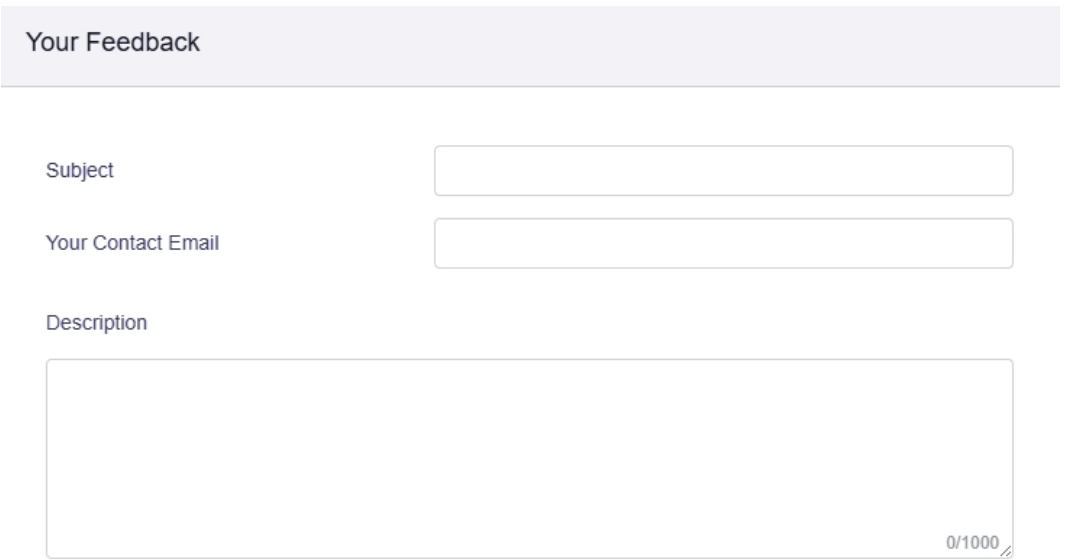
Se non riesci ad accedere al pannello di amministrazione web del router, prova a ripristinare il router utilizzando il pulsante di ripristino fisico sul lato.

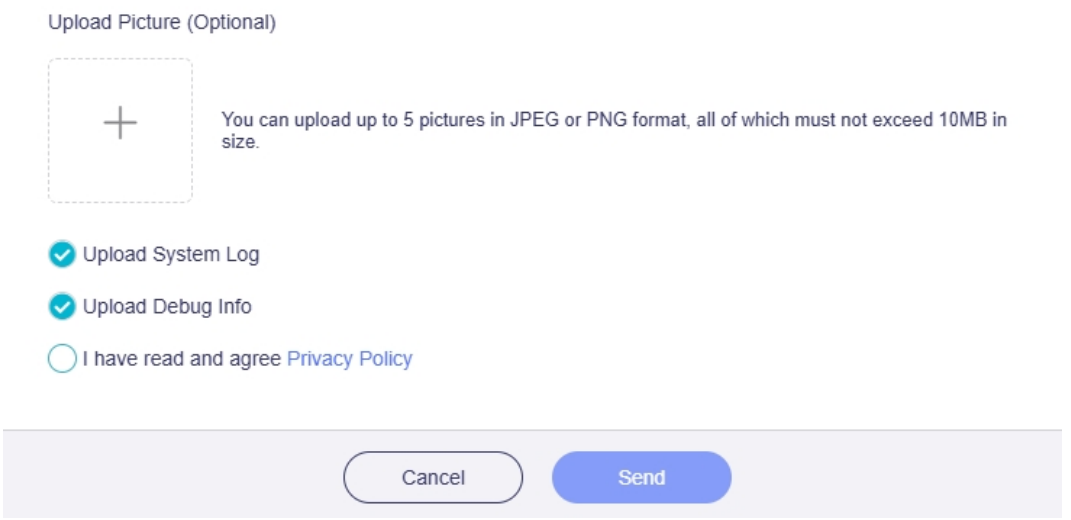
16.7 Registro

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



- **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.



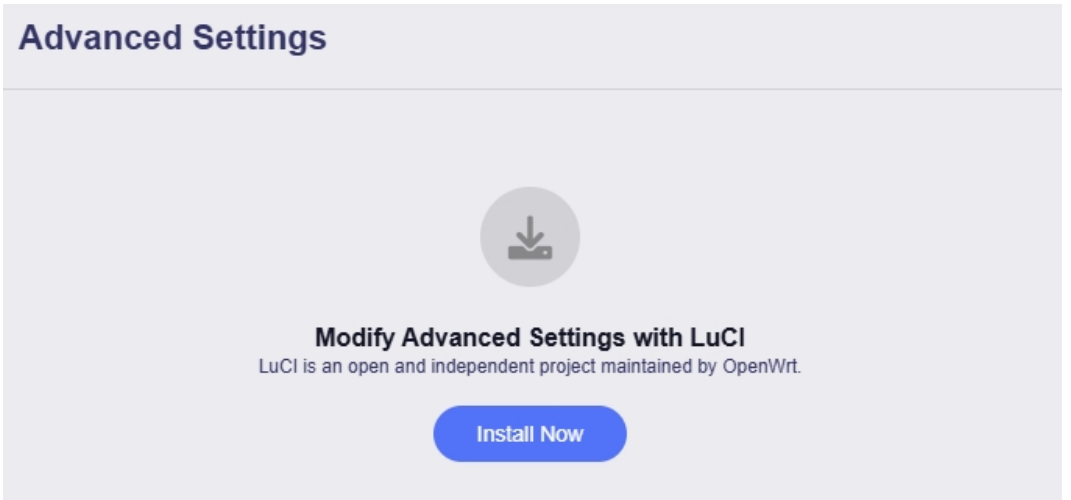

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.8 Impostazioni avanzate

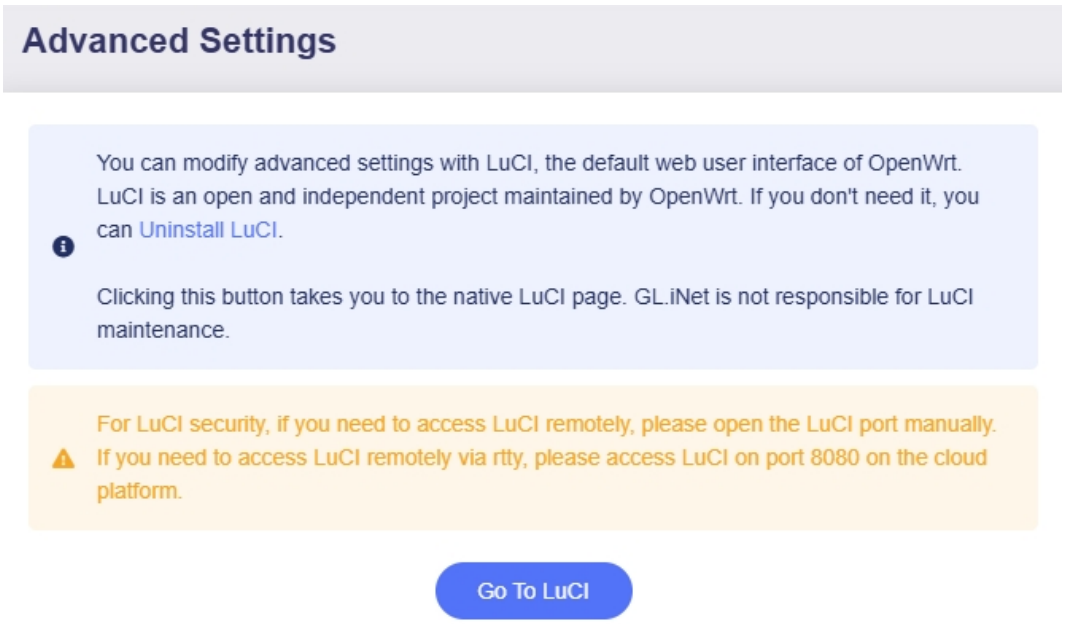
Accedi al pannello di amministrazione web del tuo router e vai a **SISTEMA** > **Impostazioni avanzate**. Questa pagina consente di modificare le impostazioni avanzate in LuCI, che è l'interfaccia utente web predefinita di OpenWrt. Essendo un progetto aperto e indipendente gestito da OpenWrt, LuCI viene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

Segui i passaggi seguenti per accedere all'interfaccia LuCI.

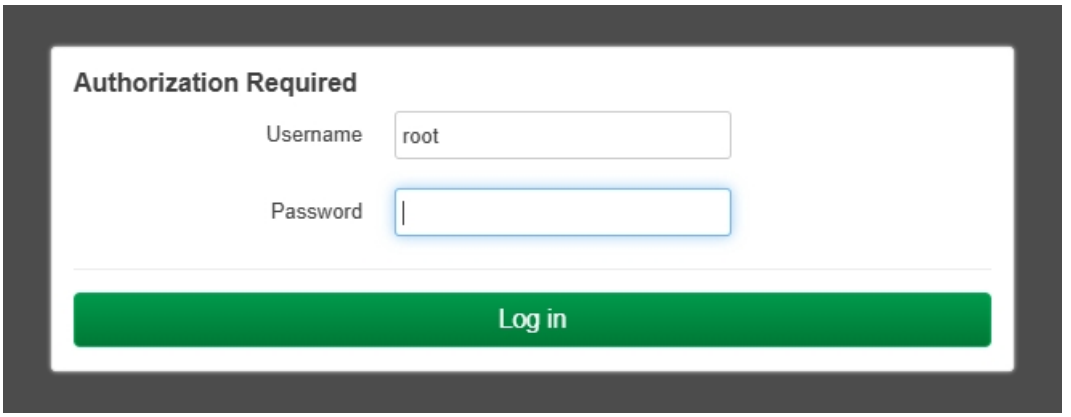
1. Fai clic su **Installa ora** e verrà installata l'interfaccia LuCI.



2. Fai clic su **Vai a LuCI** e verrai reindirizzato alla pagina di accesso di LuCI.



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



Quindi accederai all'interfaccia LuCI.

