GL·iNet



Manuel d’utilisation

GL-X3000 / Spitz AX

Routeur cellulaire Wi-Fi 6 double SIM 4G/5G

Version du micrologiciel 4.8.3

À propos de ce manuel

Ce manuel vous accompagne dans la prise en main de votre appareil. Il présente les principales caractéristiques du produit, les branchements, la connexion à l'interface d'administration Web, la configuration initiale et les instructions détaillées pour toutes les fonctions accessibles dans cette interface.

Ce guide vous permettra de :

- Découvrir les principales caractéristiques du produit
- Effectuer les branchements en suivant les instructions étape par étape
- Vous connecter facilement à l'interface d'administration Web
- Effectuer la configuration initiale et maîtriser toutes les fonctions de l'interface d'administration Web

Conventions utilisées

Ces symboles et couleurs vous aident à suivre les étapes plus facilement.

Convention	Signification
Texte turquoise souligné	Lien cliquable permettant d'ouvrir une page Web ou une section précise
Texte en gras	Met en évidence des informations importantes, notamment les titres, les liens et les noms exacts des menus et des éléments de l'interface Web de l'appareil
>	Chemin permettant d'ouvrir la page correspondante (par exemple, Système > Micrologiciel)
Remarque	Informations essentielles pour la configuration, l'utilisation et la sécurité. Leur non-respect peut entraîner un échec de configuration, un dysfonctionnement ou des dommages matériels
Conseils	Conseils pour tirer le meilleur parti de votre appareil

Remarque :

- Les fonctions de l'appareil peuvent varier selon le modèle et la version du micrologiciel.
- La disponibilité des produits varie selon les régions ou les spécifications du fournisseur d'accès à Internet (FAI).

- Les images, procédures et descriptions de ce guide sont fournies à titre d'illustration et peuvent différer de votre situation réelle.

Besoin d'aide ou d'informations complémentaires ?

- Mise à jour du micrologiciel : Centre de téléchargement des micrologiciels GL.iNet | Routeurs
- Communauté : échangez sur nos produits et partagez vos expériences sur le forum communautaire GL.iNet
- Assistance technique : contactez notre équipe d'assistance sur la page de contact

Copyright © 2026 GL.iNet Technology (HK) Ltd. Tous droits réservés.
Aucune partie de ce manuel ne peut être reproduite, transcrite, traduite ou diffusée, sous quelque forme ou par quelque moyen que ce soit, sans l'autorisation écrite préalable de GL.iNet Technology (HK) Ltd. GL.iNet est une marque déposée de GL.iNet Technology (Hong Kong) Ltd. en Chine et/ou dans d'autres pays et régions. Tous les autres noms de marques et de produits mentionnés dans ce manuel sont des marques commerciales ou déposées de leurs propriétaires respectifs.
Le contenu de ce document peut être modifié sans préavis, notamment à la suite de mises à jour du produit. Sauf accord contraire, ce document est fourni à titre informatif uniquement. Les déclarations, informations et recommandations qu'il contient ne constituent aucune forme de garantie.

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

Table des matières

Chapitre 1 Présentation de votre routeur 9

1.1 Présentation du produit 10

1.1.1 Aspect extérieur 10

1.1.2 Ports et boutons 11

1.1.3 LED 12

1.2 Caractéristiques techniques 13

1.3 Contenu de l'emballage 14

Chapitre 2 Branchements 15

2.1 Choix de l'emplacement 16

2.2 Branchement du routeur 16

Chapitre 3 Connexion à l'interface du routeur 17

Chapitre 4 Configuration de la connexion Internet 19

4.1 Assistant de configuration rapide 20

4.2 Configuration manuelle de la connexion Internet 21

4.2.1 Connexion à Internet via un câble Ethernet 21

4.2.2 Connexion à Internet via un réseau Wi-Fi existant 27

4.2.3 Connexion à Internet par partage de connexion USB 41

4.2.4 Connexion à Internet via le réseau cellulaire 45

Chapitre 5 Réseau sans fil 71

5.1 Affichage de l'état du Wi-Fi 72

5.2 Paramètres sans fil 73

5.2.1 Wi-Fi 5 GHz 73

5.2.2 Wi-Fi 2,4 GHz 75

5.2.3 BSSID aléatoire 77

Chapitre 6 Appareils clients 79

6.1 Informations sur les appareils 80

6.2 Actions 83

6.3 Suppression de clients 86

6.4 Tri 86

Chapitre 7 Services cloud 87

7.1 GoodCloud 88

7.1.1 Activation de GoodCloud 89

7.1.2 Gestion de votre routeur 91
7.1.3 Dissociation de l'appareil 97
7.1.4 Désactivation de GoodCloud 97
7.2 AstroWarp 99
Chapitre 8 Comprendre les VPN 100
8.1 Introduction 101
8.1.1 VPN 101
8.1.2 Routeur VPN 101
8.1.3 OpenVPN 101
8.1.4 WireGuard 101
8.2 Cas d'utilisation 102
Chapitre 9 Tableau de bord VPN 104
9.1 Assistant de configuration VPN 105
9.2 Mode VPN 108
9.2.1 Mode global 109
9.2.2 Mode par règles 110
Chapitre 10 Configuration d'un serveur VPN 121
10.1 Serveur OpenVPN 122
10.1.1 Préparation 122
10.1.2 Étapes de configuration 123
10.1.3 Vérification de la connexion 126
10.1.4 Options du serveur 127
10.1.5 Communication entre clients 128
10.2 Serveur WireGuard 131
10.2.1 Préparation 131
10.2.2 Étapes de configuration 132
10.2.3 Vérification de la connexion 136
10.2.4 Options du serveur 137
Chapitre 11 Configuration d'un client VPN 139
11.1 Client OpenVPN 140
11.1.1 Préparation 140
11.1.2 Configuration de NordVPN 140
11.1.3 Configuration manuelle d'un client OpenVPN pour un autre fournisseur 146
11.2 Configuration d'un client WireGuard 149

11.2.1 Préparation 149
11.2.2 Configuration d'AzireVPN 150
11.2.3 Configuration de Hide.me 155
11.2.4 Configuration d'IPVanish 158
11.2.5 Configuration de Mullvad 163
11.2.6 Configuration de NordVPN 168
11.2.7 Configuration de PIA (Private Internet Access) 173
11.2.8 Configuration de Surfshark 178
11.2.9 Configuration manuelle d'un client WireGuard pour un autre fournisseur 183
Chapitre 12 Tor 189
Chapitre 13 Applications 192
13.1 Extensions 193
13.2 DNS dynamique 194
13.2.1 Activation du DDNS 194
13.2.2 Vérification du fonctionnement du DDNS 197
13.2.3 Accès HTTPS à distance 199
13.2.4 Accès SSH à distance 202
13.3 Stockage réseau 204
13.3.1 Branchement du stockage 204
13.3.2 Configuration de Samba 205
13.3.3 Configuration de WebDAV 208
13.3.4 Configuration de DLNA 211
13.4 AdGuard Home 212
13.5 Contrôle parental 215
13.5.1 Configuration rapide 215
13.5.2 Dépannage 224
13.6 ZeroTier 225
13.6.1 Configuration de ZeroTier 226
13.6.2 Autoriser l'accès distant au WAN 230
13.6.3 Autoriser l'accès distant au LAN 231
13.7 Tailscale 232
13.7.1 Configuration de Tailscale 233
13.7.2 Autoriser l'accès distant au WAN 236
13.7.3 Autoriser l'accès distant au LAN 237

13.7.4 Nœuds de sortie personnalisés 238
13.8 Gestion eSIM 239
13.8.1 État actuel de l'eSIM 240
13.8.2 Liste des profils eSIM 241
Chapitre 14 Réseau 248
14.1 Redirection de port 249
14.1.1 DMZ 249
14.1.2 Redirection de port 250
14.2 Multi-WAN 253
14.2.1 Suivi de l'état des interfaces 253
14.2.2 Mode Multi-WAN 256
14.3 LAN 259
14.3.1 Paramètres de base 259
14.3.2 Serveur DHCP 260
14.3.3 Réservation d'adresses 262
14.4 Réseau invité 263
14.4.1 Paramètres de base 263
14.4.2 Serveur DHCP 264
14.5 DNS 266
14.5.1 Paramètres généraux 266
14.5.2 Paramètres du serveur DNS 267
14.5.3 Modification du fichier hosts 269
14.6 Ports Ethernet 271
14.7 Mode réseau 272
14.8 IPv6 274
14.8.1 Mode IPv6 275
14.8.2 Méthode d'obtention du DNS 275
14.9 Passerelle transparente 276
14.10 IGMP Snooping 278
14.11 Accélération réseau 279
14.12 Paramètres NAT 280
Chapitre 15 Système 281
15.1 Vue d'ensemble 282
15.2 Mise à jour 283

15.2.1 Mise à jour en ligne du micrologiciel 283
15.2.2 Mise à jour locale du micrologiciel 284
15.2.3 Mise à jour en ligne du modem 285
15.2.4 Mise à jour locale du modem 285
15.3 Tâches planifiées 286
15.3.1 Programmation du voyant LED 286
15.3.2 Redémarrage planifié 288
15.3.3 Programmation du Wi-Fi 5 GHz 289
15.3.4 Programmation du Wi-Fi 2,4 GHz 291
15.4 Fuseau horaire 293
15.5 Journaux 295
15.6 Sécurité 297
15.6.1 Mot de passe administrateur 297
15.6.2 Contrôle d’accès 298
15.6.3 Contrôle d’accès distant 300
15.6.4 Ouverture de ports sur le routeur 301
15.7 Réinitialisation du micrologiciel 302
15.8 Paramètres avancés 303
Déclaration UE de conformité 305

Chapitre 1

Présentation de votre routeur

Ce chapitre présente le routeur, ses caractéristiques techniques et le contenu de l’emballage.

1.1 Présentation du produit

Spitz AX (GL-X3000) est une passerelle cellulaire Wi-Fi 6 double SIM conçue pour fournir des connexions rapides et fiables, notamment dans les zones isolées et lors de déplacements en voiture. Elle offre quatre modes d’accès à Internet : réseau cellulaire (cartes SIM), Ethernet, répéteur et partage de connexion USB. Elle prend en charge le Multi-WAN (basculement et équilibrage de charge), les VPN (OpenVPN et WireGuard), le contrôle parental, AdGuard Home, la redirection de ports, Tailscale et bien d’autres fonctions.

1.1.1 Aspect extérieur

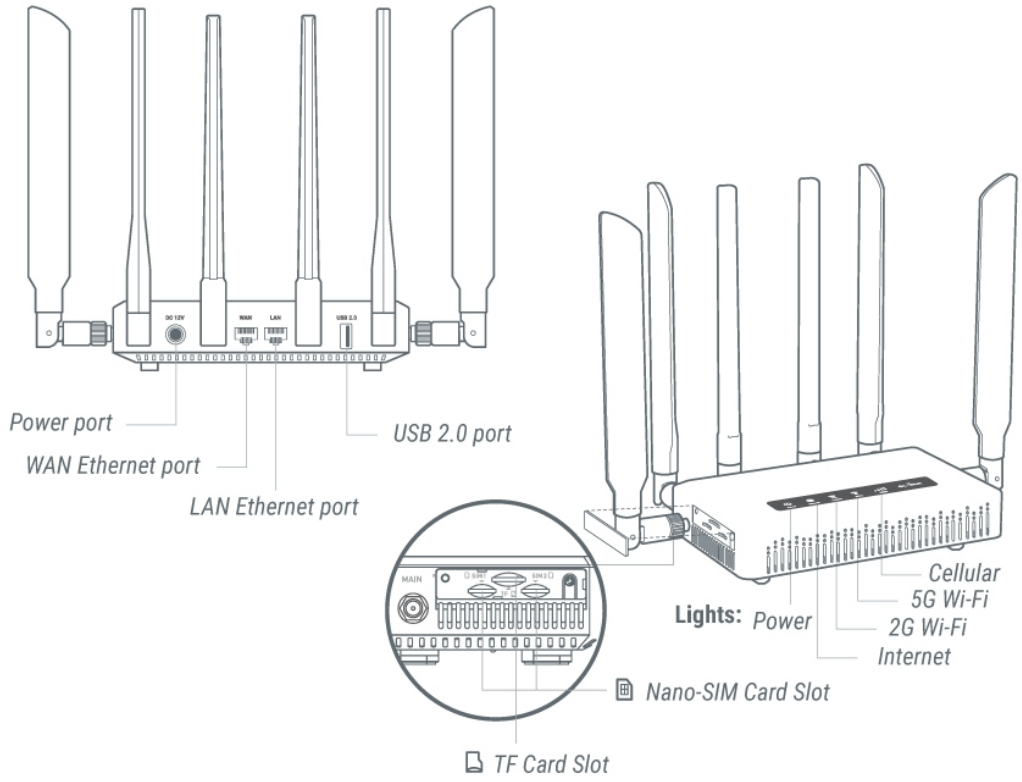








1.1.2 Ports et boutons



Élément	Fonction
Port Ethernet WAN	Relie le routeur à un réseau en amont à 10/100/1 000/2 500 Mbit/s.
Port Ethernet LAN	Relie un appareil client au routeur par câble à 10/100/1 000 Mbit/s.
Port USB 2.0	Permet de brancher un modem USB, un appareil de partage de connexion ou un périphérique de stockage USB compatible.
Emplacement pour carte microSD	Accepte une carte microSD d'une capacité maximale de 1 To.
Emplacements pour cartes nano-SIM	Acceptent deux cartes nano-SIM. Une seule carte SIM est active à la fois ; l'autre sert de secours.
Bouton de réinitialisation	Appuyez pendant moins de 3 secondes pour réinitialiser le réseau, ou pendant 10 secondes pour rétablir les paramètres d'usine.

Élément	Fonction
Entrée d’alimentation DC5521	Accepte l’adaptateur 12 V / 2,5 A fourni ou une alimentation de 9 à 36 V CC.
Connecteurs d’antennes cellulaires	Permettent de brancher quatre antennes cellulaires (SMA, 600 MHz à 6 GHz).
Connecteurs d’antennes Wi-Fi	Permettent de brancher deux antennes Wi-Fi (PR-SMA, 2,4 à 2,5 GHz et 5,15 à 5,84 GHz).

1.1.3 LED

État de l’appareil	Alim.	Internet	2,4 GHz	5 GHz	Réseau cellulaire
Internet connecté (réseau cellulaire actif)	Vert fixe	Vert fixe	Vert fixe	Vert fixe	Vert fixe
Internet connecté (réseau cellulaire inactif)	Vert fixe	Vert fixe	Vert fixe	Vert fixe	Éteint
Aucune connexion Internet	Vert fixe	Éteint	Vert fixe	Vert fixe	Éteint
Mise à jour du micrologiciel	Vert fixe	Clignote toutes les 0,5 s	Clignote toutes les 0,5 s	Clignote toutes les 0,5 s	Vert fixe
Réinitialisation du réseau (appui < 3 s)	Clignote toutes les 1 s	Vert fixe	Vert fixe	Vert fixe	Vert fixe
Réinitialisation d’usine (appui de 10 s)	Clignote toutes les 0,25 s	Vert fixe	Vert fixe	Vert fixe	Vert fixe

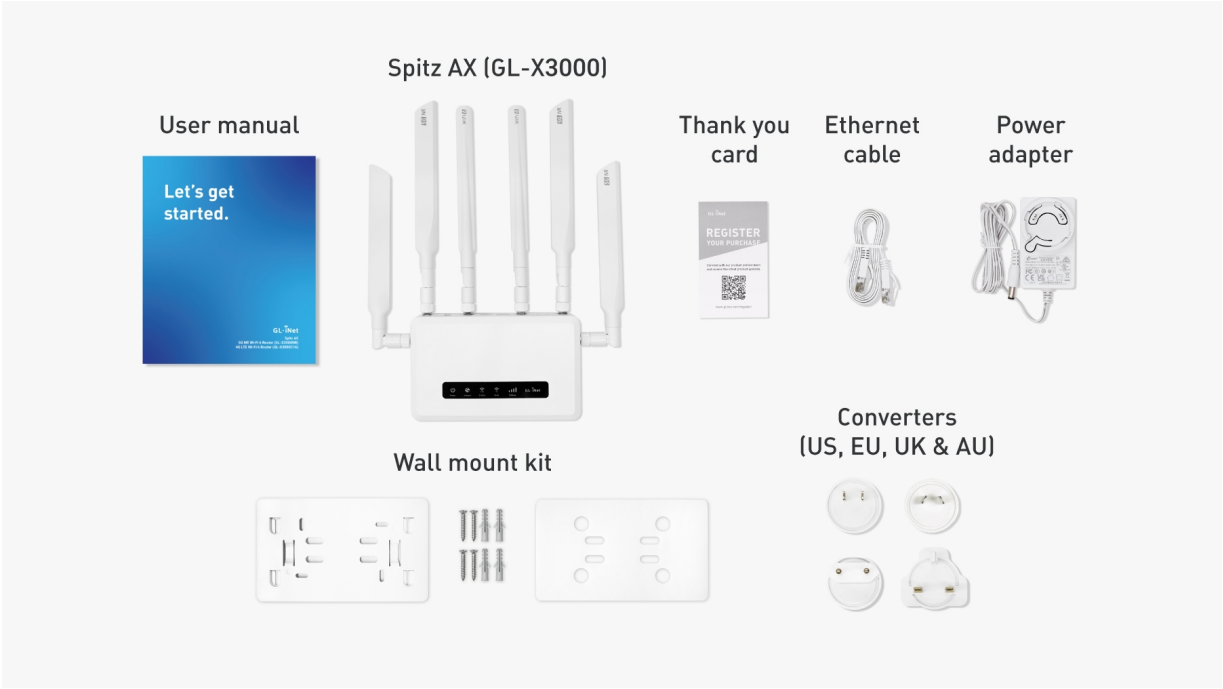
Conseil : lorsque le routeur est connecté à Internet, le clignotement du voyant LED 2,4 GHz ou 5 GHz indique que des appareils Wi-Fi sont connectés et transmettent des données.

1.2 Caractéristiques techniques

Élément	Détails
Interfaces	1 port Ethernet WAN 1 port Ethernet LAN 1 port USB 2.0 1 emplacement pour carte microSD (1 To max.) 2 emplacements pour cartes nano-SIM 1 bouton de réinitialisation
CPU	MediaTek, deux cœurs à 1,3 GHz
Mémoire / Stockage	DDR4 512 Mo / eMMC 8 Go
Protocoles	IEEE 802.11a/b/g/n/ac/ax
Débit Wi-Fi	574 Mbit/s (2,4 GHz), 2 402 Mbit/s (5 GHz)
Débit Ethernet	Port WAN : 10/100/1 000/2 500 Mbit/s Port LAN : 10/100/1 000 Mbit/s
Antennes	4 antennes cellulaires (SMA, 600 MHz à 6 GHz) 2 antennes Wi-Fi (PR-SMA, 2,4 à 2,5 GHz, 5,15 à 5,84 GHz)
Voyants LED	Système / Wi-Fi 5 GHz / Wi-Fi 2,4 GHz / Internet / Intensité du signal cellulaire
Alimentation	DC5521, 12 V / 2,5 A (5,5 × 2,1 mm) [adaptateur fourni] / 9 à 36 V
Consommation électrique	< 14 W
Température de fonctionnement	0 à 40 °C (32 à 104 °F)
Température de stockage	−20 à 70 °C (−4 à 158 °F)
Dimensions / Poids	155 × 95 × 36 mm / 520 g
Autres ressources	Fiche technique | Micrologiciel | Application | Déballage | Tutoriels | Kit média

1.3 Contenu de l’emballage

- 1 Spitz AX (GL-X3000)
- 1 manuel d’utilisation
- 1 carte de remerciement
- 1 câble Ethernet
- 1 kit de fixation murale
- 1 adaptateur secteur
- 4 adaptateurs



Chapitre 2

Branchements

Ce chapitre explique comment choisir l’emplacement du routeur et effectuer les branchements.

2.1 Choix de l’emplacement

Suivez ces conseils pour choisir un emplacement offrant les meilleures performances.

- **Évitez l’humidité et la chaleur :** ne placez pas le routeur dans un endroit exposé à l’eau, à l’humidité ou à des températures élevées, par exemple près d’un évier ou d’un radiateur.
- **Ventilation et refroidissement :** placez le routeur dans un endroit frais et bien ventilé pour permettre une bonne dissipation de la chaleur.
- **Emplacement central :** choisissez un endroit permettant de raccorder facilement le routeur à l’alimentation et à plusieurs appareils, par exemple au centre du salon.
- **Disposition des câbles :** acheminez les câbles et le cordon d’alimentation de manière à éviter tout risque de trébuchement.
- **Installation :** posez le routeur sur une surface plane et stable, comme une étagère ou un bureau, ou fixez-le au mur à l’aide du kit fourni.
- **Évitez les interférences électromagnétiques :** éloignez le routeur des sources d’interférences, notamment les appareils Bluetooth et les fours à micro-ondes, pour limiter les perturbations du signal.

2.2 Branchement du routeur

1. **Mise sous tension**

   Assemblez les deux parties de l’adaptateur secteur. Branchez-le au routeur, puis à une prise de courant. Le routeur démarre automatiquement.

2. **Connexion d’un appareil au routeur**

   Connectez un appareil, tel qu’un ordinateur portable ou un smartphone, au routeur par Wi-Fi ou à l’aide d’un câble Ethernet.

   - **Wi-Fi :** sur votre appareil, ouvrez Paramètres > WLAN, recherchez le nom du réseau Wi-Fi du routeur dans la liste des réseaux disponibles et saisissez le mot de passe. Le nom et le mot de passe par défaut figurent sur l’étiquette du routeur.
   - **Ethernet :** reliez votre appareil au port LAN du routeur à l’aide d’un câble Ethernet.

3. **Connexion à l’interface du routeur**

   Lors de la première connexion au routeur, Internet n’est pas encore disponible. Connectez-vous à l’interface du routeur comme indiqué au chapitre 3 et effectuez la configuration initiale pour accéder à Internet.

Chapitre 3

Connexion à l’interface du routeur

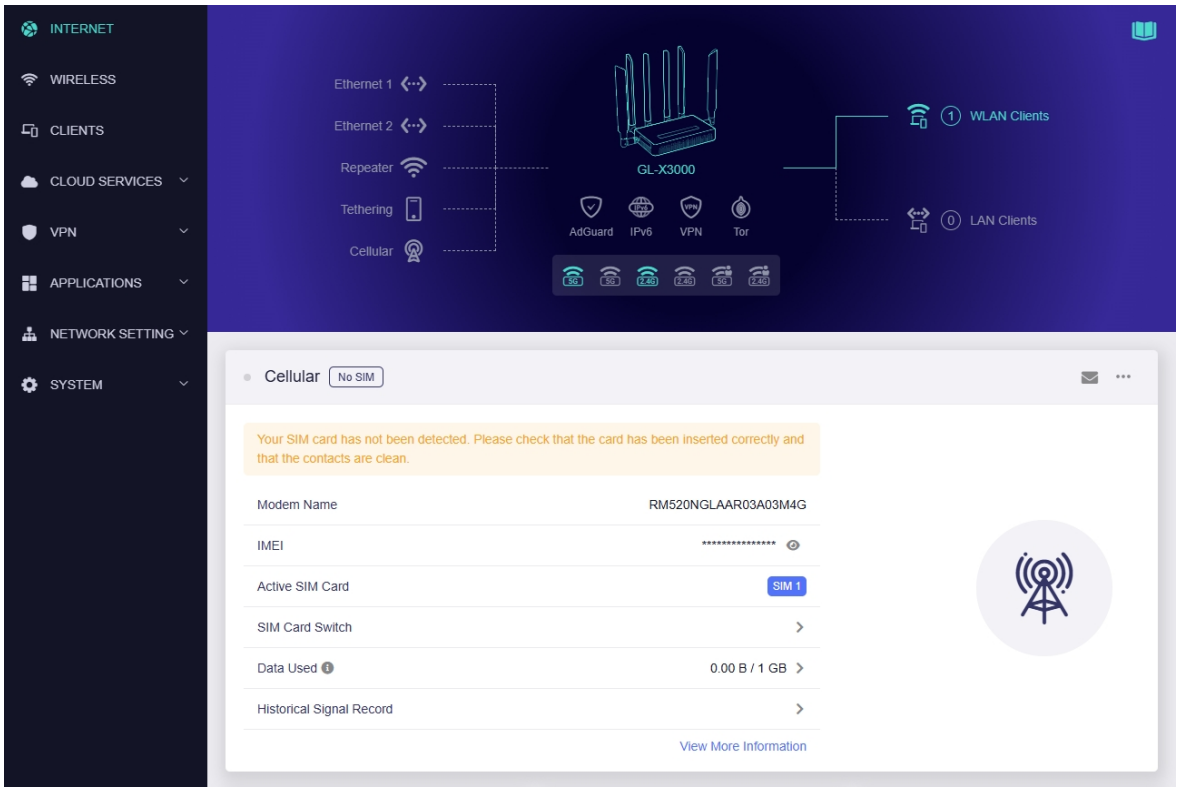
Ce chapitre explique comment vous connecter à l’interface d’administration Web du routeur.

Configurez et gérez votre routeur depuis une interface d'administration Web accessible sur Windows, macOS ou Linux avec un navigateur, comme Microsoft Edge, Google Chrome, Mozilla Firefox ou Apple Safari.

Remarque : si vous préférez utiliser l'application GL.iNet plutôt que l'interface d'administration Web, téléchargez l'application et suivez les instructions à l'écran.

Suivez les étapes ci-dessous pour vous connecter au routeur via l'interface d'administration Web.

1. Connectez un appareil, par exemple un ordinateur de bureau ou un ordinateur portable, au routeur par Wi-Fi ou avec un câble Ethernet.
2. Ouvrez un navigateur Web (Chrome ou Edge est recommandé) et accédez à http://192.168.8.1. La page de connexion à l'interface d'administration Web s'affiche. Si vous ne parvenez pas à y accéder, consultez cette page pour obtenir de l'aide.
3. Définissez votre mot de passe administrateur. Pour renforcer la sécurité, choisissez un mot de passe robuste. Cliquez ensuite sur **Suivant (Next)** pour continuer.
4. Vous accédez alors à l'interface d'administration Web du routeur.



Chapitre 4

Configuration de la connexion Internet

Ce chapitre présente les différentes méthodes de connexion Internet permettant d’adapter le routeur à votre environnement réseau.

4.1 Assistant de configuration rapide

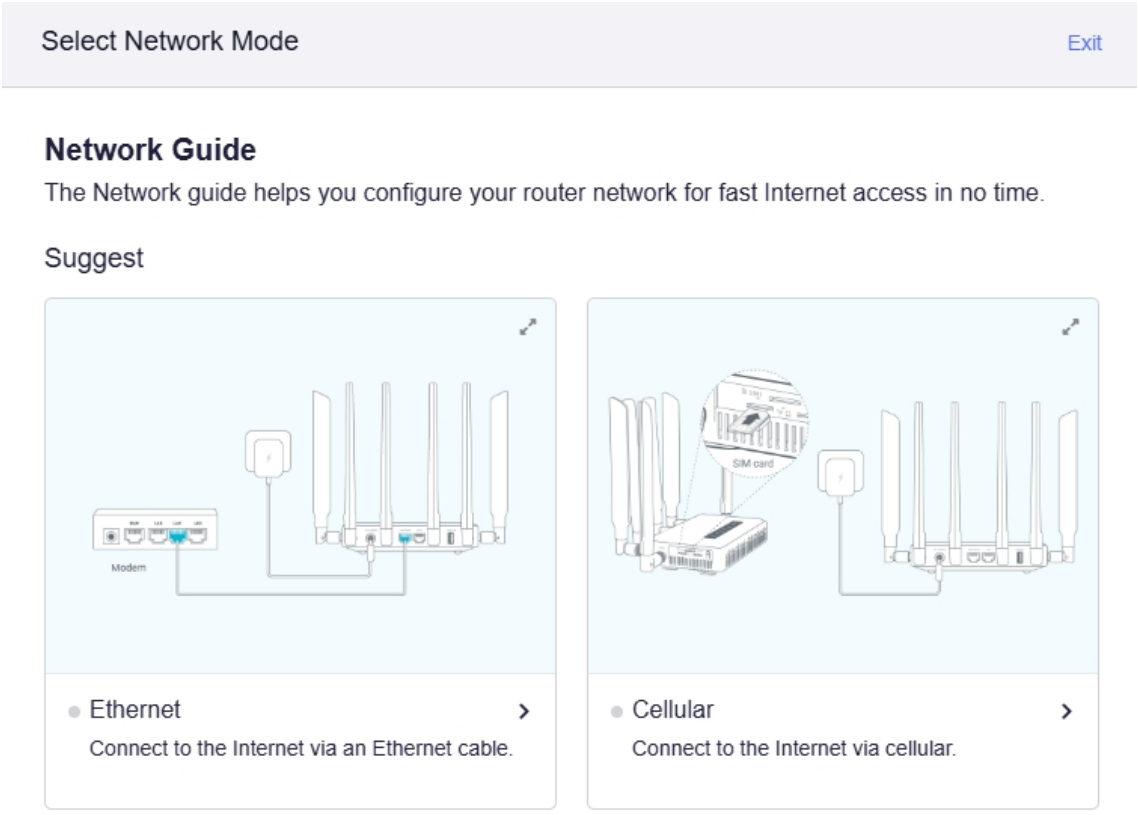
L’assistant de configuration Web vous guide dans la configuration réseau du routeur.

Suivez les étapes ci-dessous pour lancer l’assistant.

1. Connectez-vous à l’interface d’administration Web du routeur comme indiqué au chapitre 3.
2. Sur la page d’accueil, cliquez sur l’icône en forme de livre dans l’angle supérieur droit.



3. Suivez l’assistant de configuration pour configurer le routeur et établir une connexion Internet.



Si vous utilisez l’application GL.iNet, suivez les instructions à l’écran pour configurer l’accès à Internet.

4.2 Configuration manuelle de la connexion Internet

L’assistant facilite la configuration rapide du réseau. La configuration manuelle permet d’ajuster les paramètres avancés à vos besoins et de vérifier ou de modifier les connexions existantes.

Ce routeur propose quatre modes de connexion à Internet : Ethernet, Répéteur, Partage de connexion USB et Cellulaire. Choisissez celui qui convient à vos besoins.

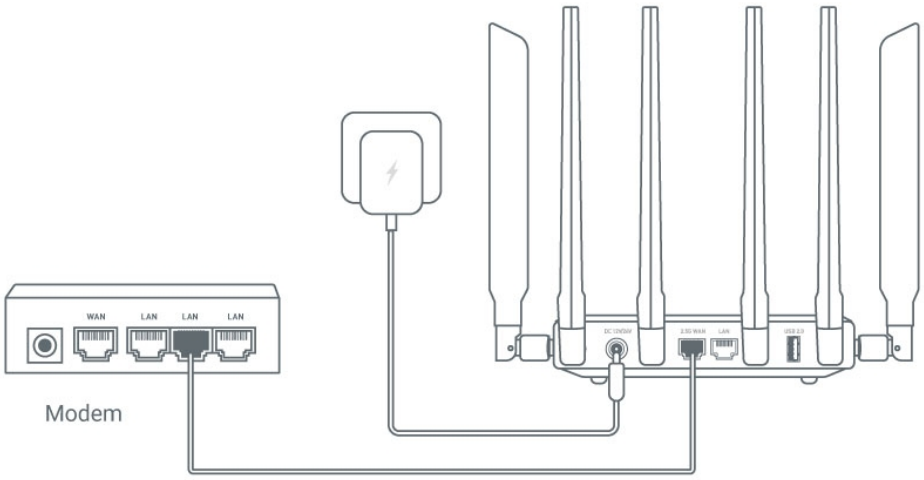
4.2.1 Connexion à Internet via un câble Ethernet

Reliez le routeur au réseau haut débit en branchant un câble Ethernet sur le port WAN. Le routeur obtient généralement une adresse IP automatiquement via DHCP. Vous pouvez également définir une adresse IP statique ou configurer PPPoE manuellement. Cette méthode offre une connexion stable et rapide, adaptée au domicile et au bureau disposant d’un accès fixe à Internet.

4.2.1.1 Étapes de base

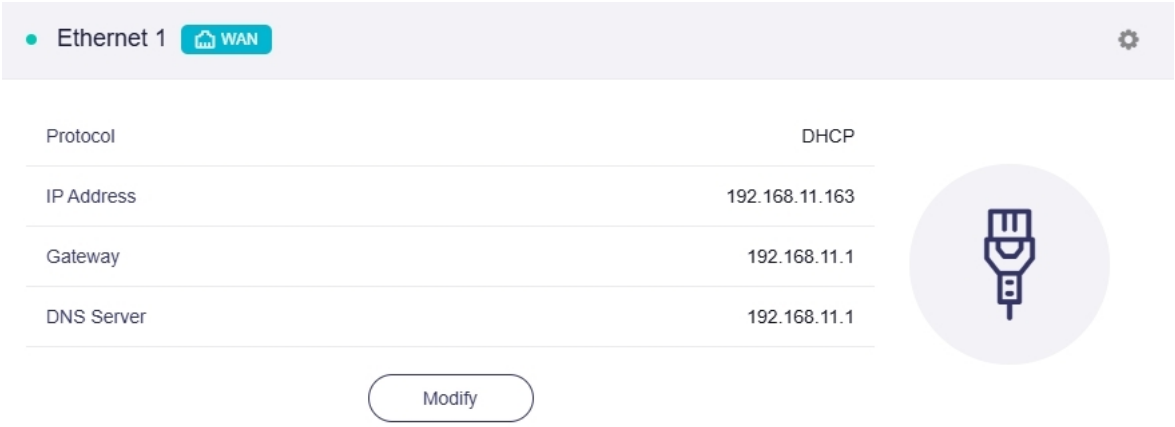
Suivez les étapes ci-dessous pour connecter le routeur à Internet à l’aide d’un câble Ethernet.

1. Reliez le port WAN du routeur à l’appareil en amont, par exemple un modem du FAI, un routeur, un commutateur réseau ou une prise Ethernet, à l’aide d’un câble Ethernet.



2. Connectez-vous à l’interface d’administration Web du routeur et ouvrez **INTERNET** > section **Ethernet**.

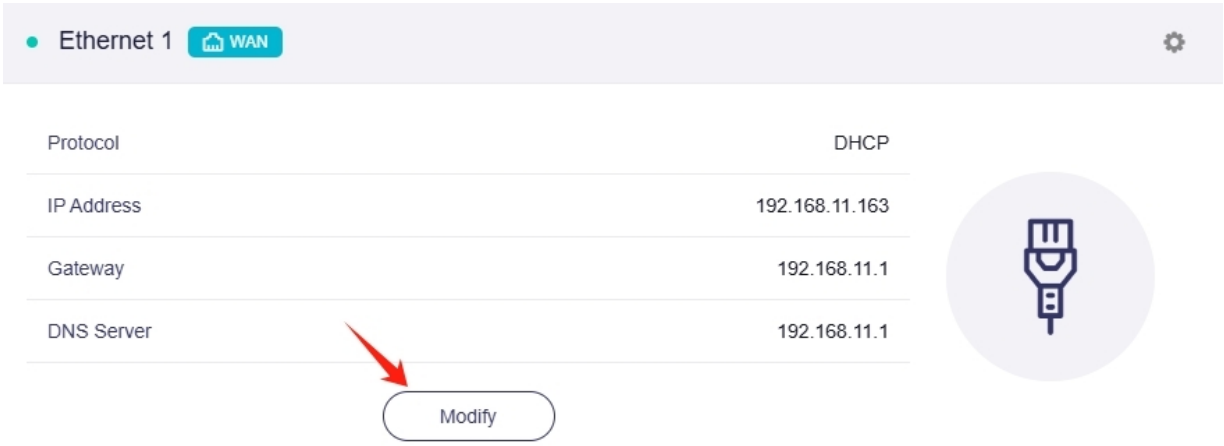
Si la connexion est établie, la section Ethernet affiche les informations réseau, notamment le protocole, l'adresse IP, la passerelle et le serveur DNS.



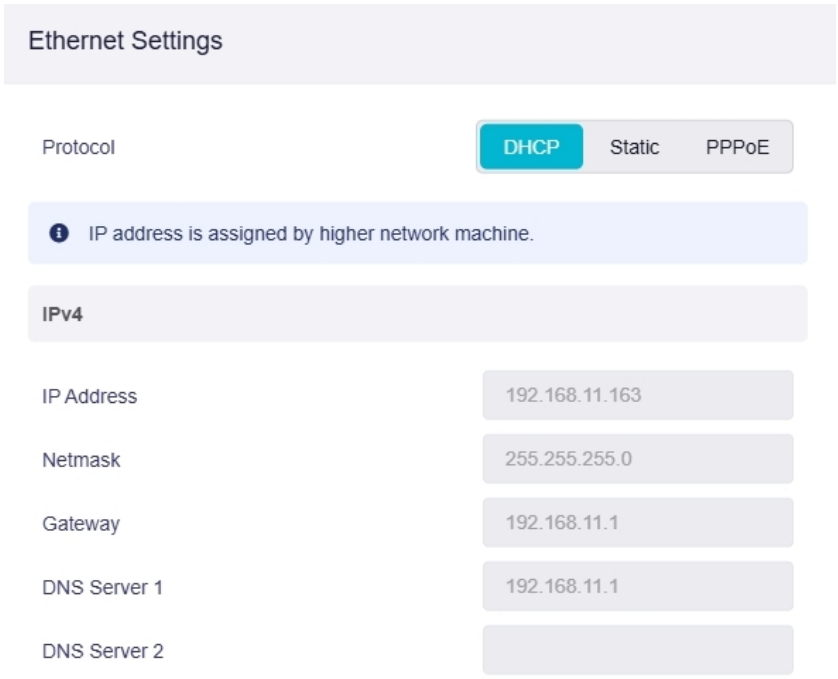
Conseil : vous pouvez transformer le port WAN en port LAN si nécessaire. Cette possibilité est utile lorsque vous utilisez le routeur comme répéteur, car le port WAN physique est alors inutilisé. Vous disposez ainsi d'un port LAN supplémentaire.

4.2.1.2 Protocoles

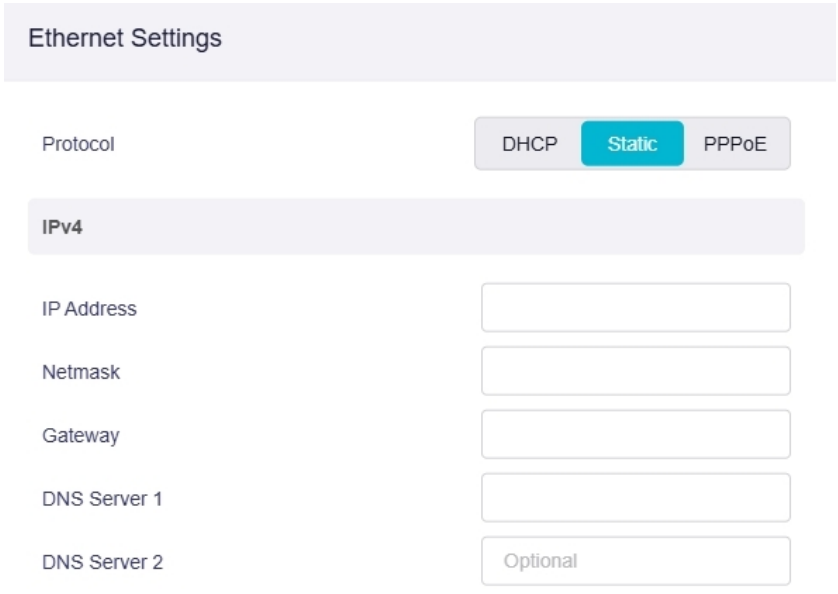
Trois protocoles sont disponibles : DHCP, Statique et PPPoE. Cliquez sur **Modifier (Modify)** pour changer de protocole.



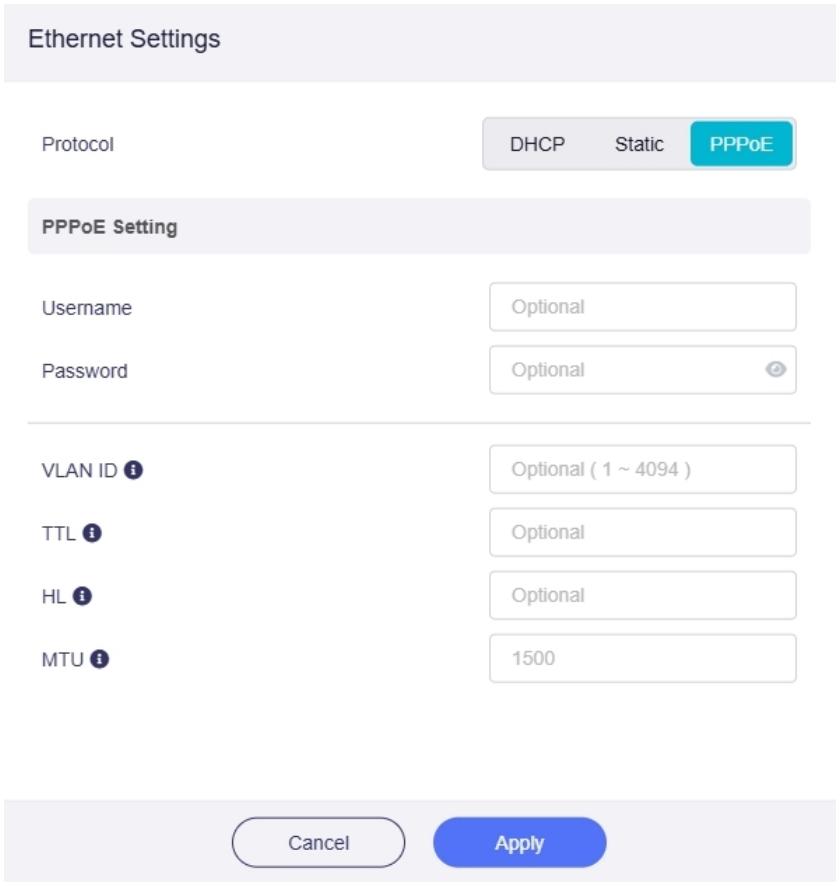
- **DHCP**
  DHCP est le protocole par défaut et le plus courant. Selon un modèle client-serveur, il attribue automatiquement des adresses IP et d'autres paramètres de communication aux appareils d'un réseau IP.



- **Statique (Static)**
  Une adresse IP statique est nécessaire si votre fournisseur d'accès à Internet (FAI) vous attribue une adresse IP fixe ou si vous souhaitez configurer manuellement les paramètres réseau, comme l'adresse IP, la passerelle et le masque de sous-réseau.

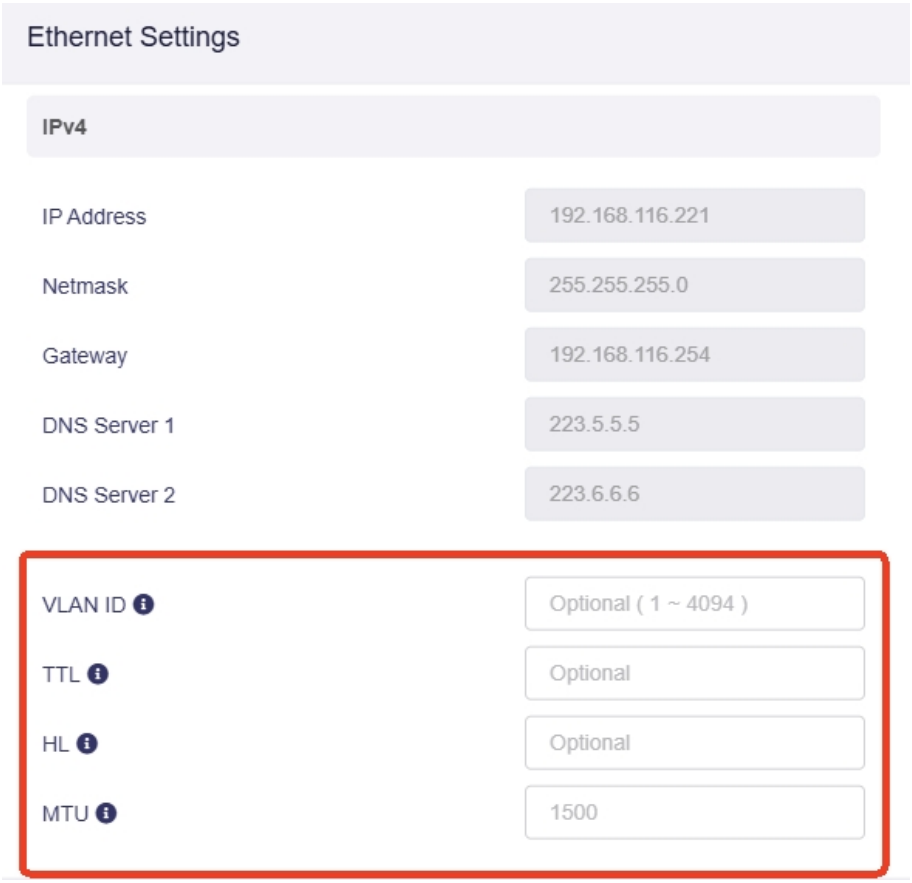


- **PPPoE**
  PPPoE est un protocole utilisé par la plupart des FAI. Ceux-ci fournissent généralement un modem ainsi qu'un identifiant et un mot de passe, nécessaires pour configurer l'accès à Internet.


Ethernet Settings
Protocol
DHCP
Static
PPPoE
PPPoE Setting
Username
Optional
Password
Optional
VLAN ID
Optional (1 ~ 4094)
TTL
Optional
HL
Optional
MTU
1500
Cancel
Apply

4.2.1.3 Paramètres avancés

Outre les paramètres essentiels, ces trois protocoles proposent des paramètres avancés facultatifs.

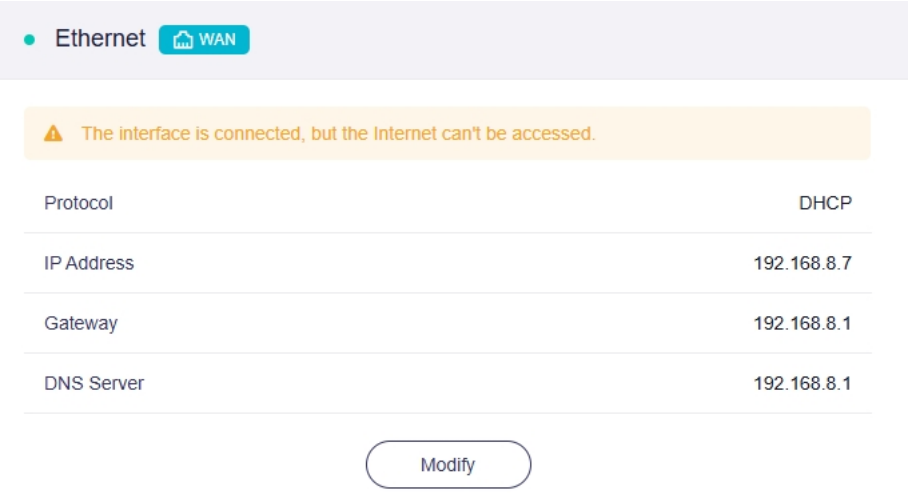


- **VLAN ID** : ce paramètre n'est nécessaire que si le serveur du fournisseur exige un identifiant VLAN balisé précis pour cette interface.
- **TTL** : le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Ce paramètre ne s'applique qu'à IPv4. Pour modifier ou simuler le TTL, définissez ici une valeur fixe. Sur la plupart des modèles, saisissez le TTL effectif souhaité augmenté de 1 pour compenser cette diminution automatique.
- **HL** : en IPv6, le champ HL (Hop Limit, limite de sauts) limite le nombre de sauts que peuvent effectuer les paquets dans le réseau. Il remplit le même rôle que le TTL en IPv4.
- **MTU** : la valeur MTU par défaut est de 1 500 octets.

4.2.1.4 Dépannage

Si un câble Ethernet est branché au port WAN mais que l’accès à Internet est indisponible, le message jaune ci-dessous s’affiche.

« L’interface est connectée, mais l’accès à Internet est impossible. » (The interface is connected, but the Internet can’t be accessed.)

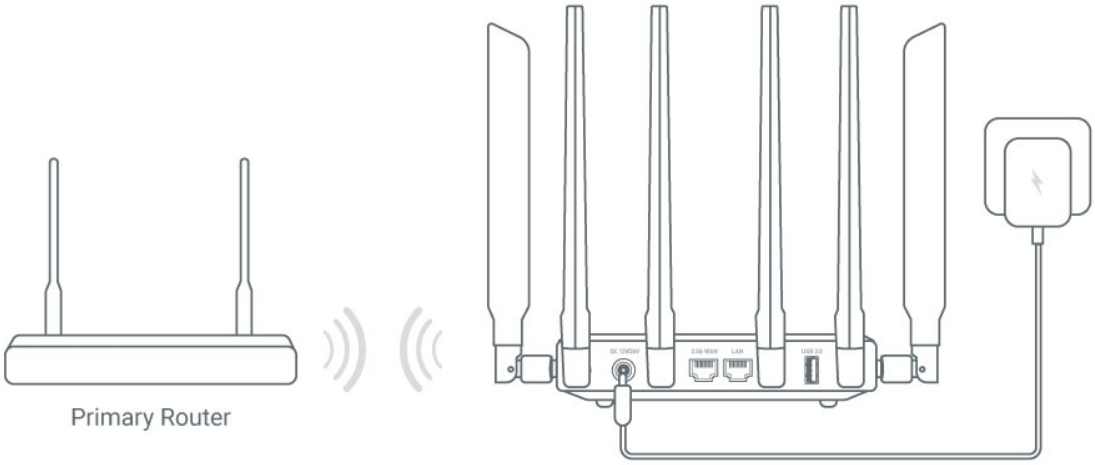


Pour résoudre ce problème :

1. Vérifiez que l’appareil en amont dispose d’un accès à Internet.
2. Ouvrez la page Multi-WAN pour vérifier l’état de l’interface Ethernet.

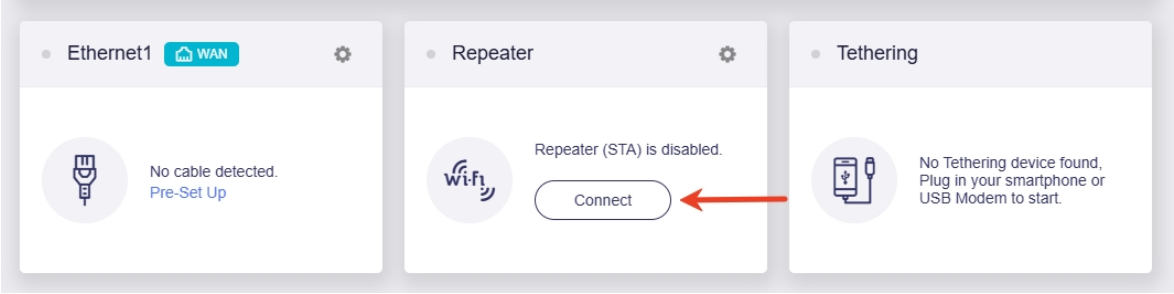
4.2.2 Connexion à Internet via un réseau Wi-Fi existant

Le mode répéteur permet de connecter le routeur à un réseau sans fil existant, par exemple au Wi-Fi gratuit d'un hôtel ou d'un café. Il utilise par défaut le mode WISP (Wireless Internet Service Provider). Le routeur crée ainsi son propre sous-réseau et agit comme un pare-feu pour vous protéger du réseau public.

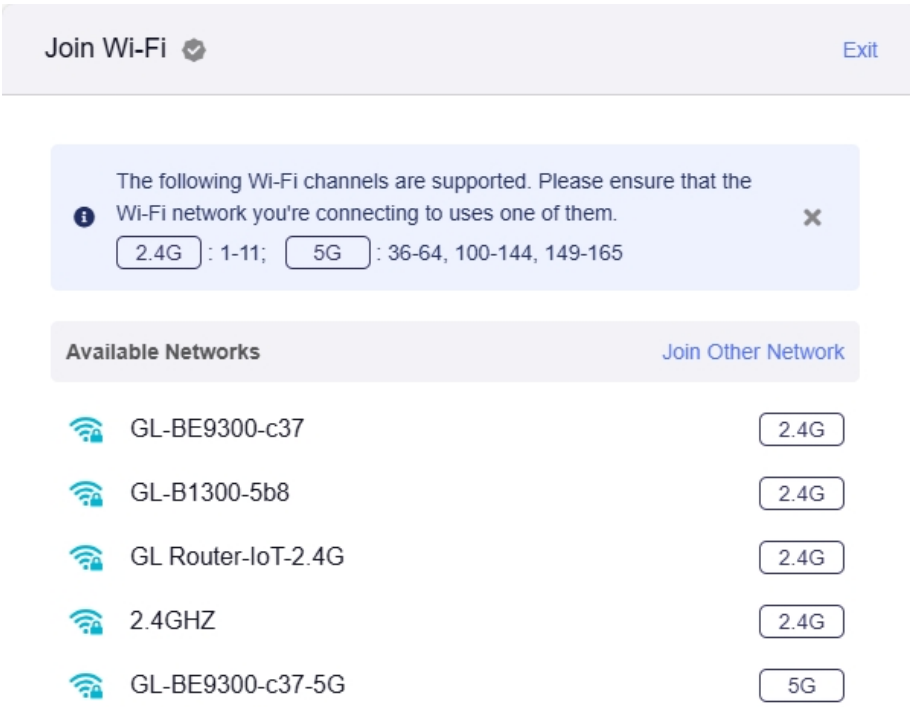


4.2.2.1 Étapes de base

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > section **Répéteur (Repeater)**, puis cliquez sur **Connecter (Connect)**.



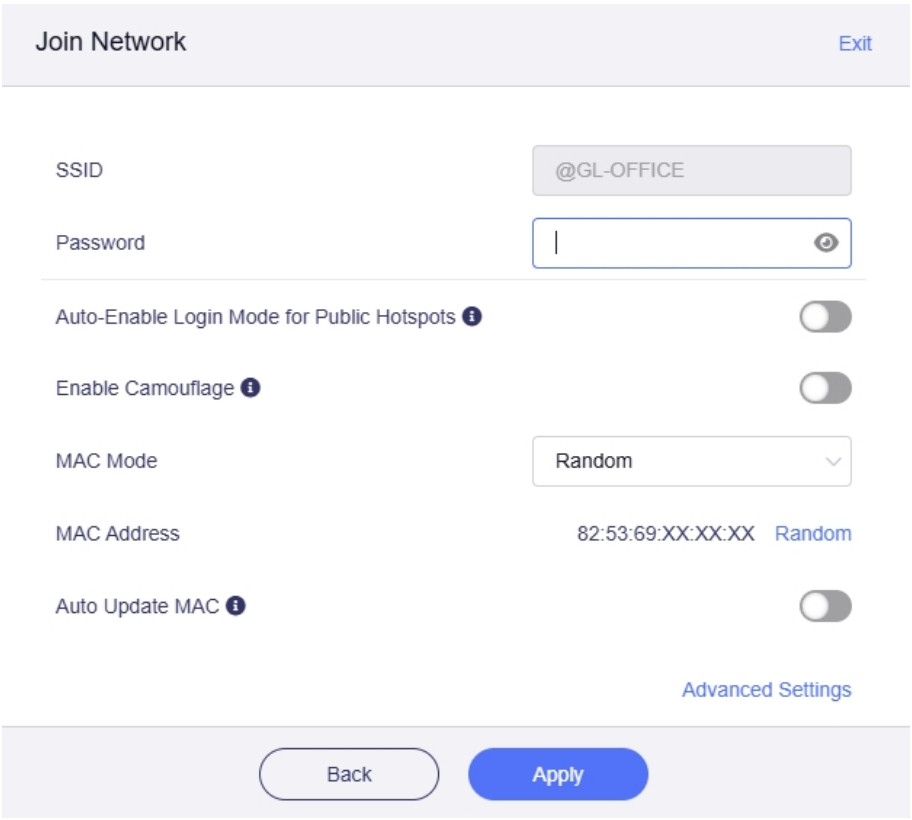
2. Choisissez le réseau Wi-Fi souhaité dans la liste des réseaux disponibles.



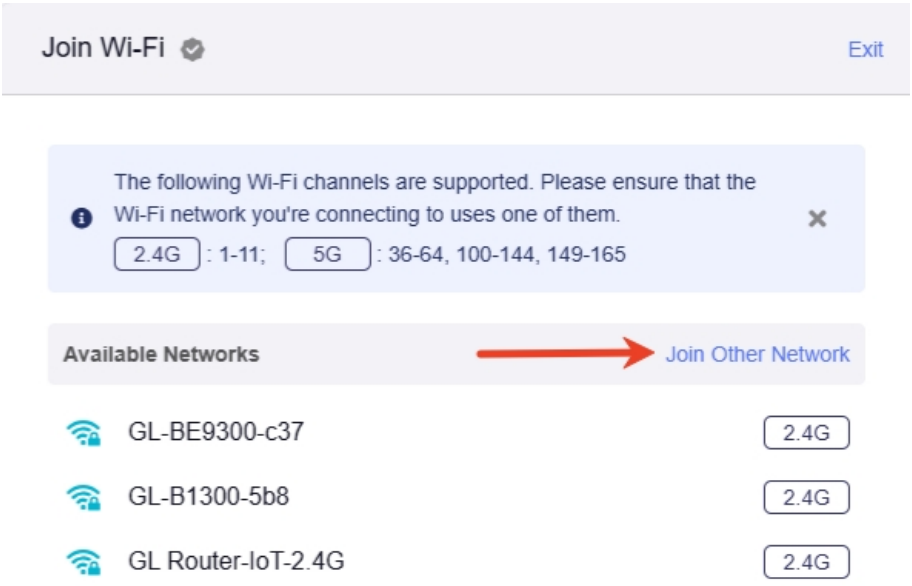
Remarque :

1. Cette page affiche les canaux Wi-Fi pris en charge par le routeur. Vérifiez que le réseau auquel vous souhaitez vous connecter utilise l'un de ces canaux ; sinon, il risque de ne pas figurer dans la liste des réseaux disponibles.
2. Lorsque vous recherchez le partage de connexion d'un iPhone, laissez l'iPhone déverrouillé pour maintenir l'émission des balises Wi-Fi. Sinon, le routeur risque de ne pas détecter ce point d'accès.

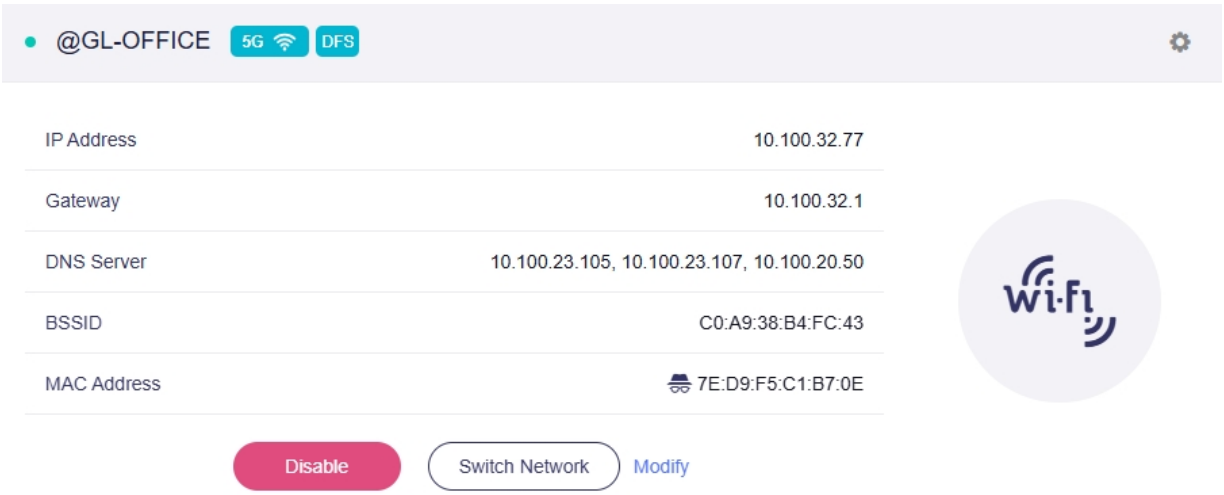
3. Saisissez le mot de passe Wi-Fi correct, puis cliquez sur **Appliquer (Apply)**.



Conseil : si le SSID Wi-Fi souhaité ne figure pas dans la liste des réseaux disponibles, cliquez sur **Rejoindre un autre réseau (Join Other Network)** dans l'angle supérieur droit. Saisissez manuellement le SSID et les autres informations requises, puis cliquez sur **Appliquer (Apply)**.

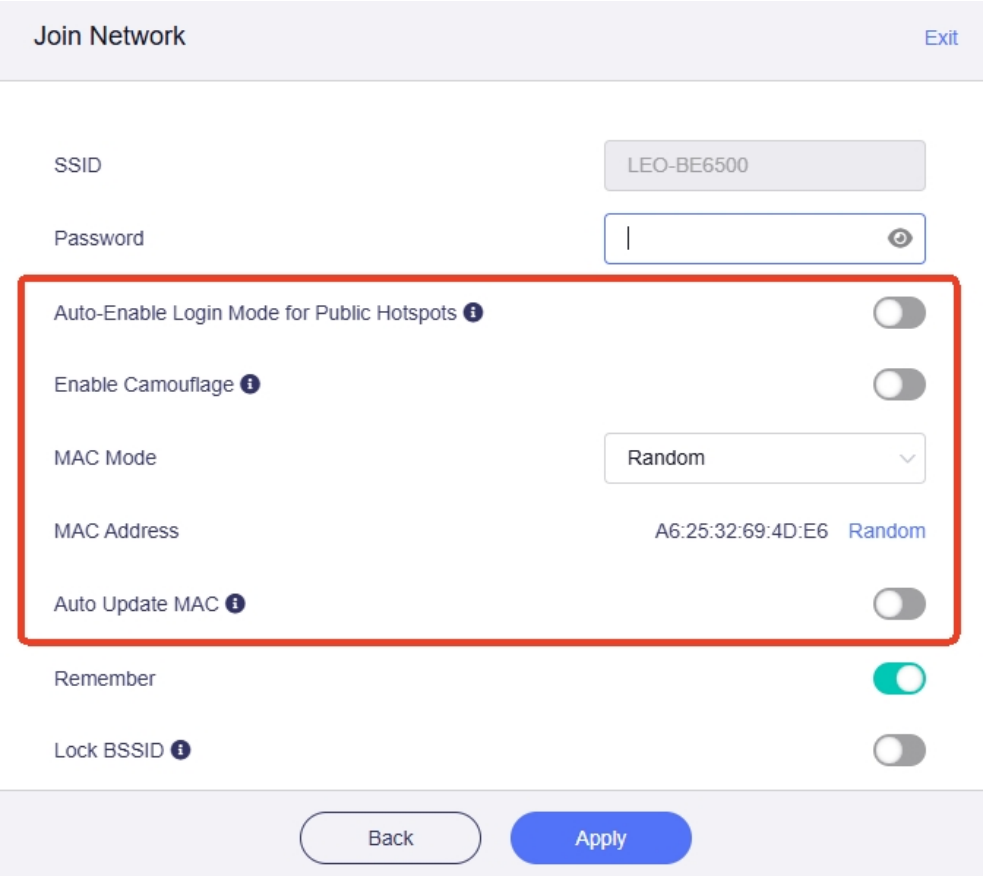


4. Après un court délai, la connexion est établie si le mot de passe est correct.


@GL-OFFICE
5G
DFS
IP Address
10.100.32.77
Gateway
10.100.32.1
DNS Server
10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID
C0:A9:38:B4:FC:43
MAC Address
7E:D9:F5:C1:B7:0E
Disable
Switch Network
Modify

4.2.2.2 Points d’accès publics

Lorsque vous connectez le routeur à un point d’accès public doté d’un portail captif, les fonctions suivantes peuvent faciliter la connexion.



- **Activation automatique du mode de connexion aux points d’accès publics**
  Si cette option est activée, le routeur passe automatiquement en mode de connexion aux points d’accès publics lorsqu’il est connecté à un point d’accès mais ne peut pas accéder à Internet. Certains services sont alors suspendus et le mode DNS passe en automatique, ce qui peut révéler votre activité réseau au fournisseur du réseau, par exemple l’hôtel ou le centre commercial. Même si cette option est désactivée, le routeur vous propose ce mode lorsqu’il détecte un portail captif ou ne parvient pas à s’y connecter.
- **Activer le camouflage**
  Si cette option est activée, le routeur prend l’identité de l’appareil client utilisé pour accéder à l’interface d’administration en reproduisant son adresse MAC.
- **Mode MAC**
  Choisissez l’adresse MAC utilisée par le routeur pour se connecter au point d’accès public.

Adresse d’usine (Factory)	Utilise l’adresse MAC attribuée à l’appareil en usine.
Clonage (Clone)	Copie l’adresse MAC d’un appareil client pour établir la connexion. Si l’adresse souhaitée n’apparaît pas dans la liste, saisissez-la manuellement. Remarque : de nombreux appareils utilisent des adresses MAC aléatoires, souvent appelées « adresse Wi-Fi privée » ou « adresse matérielle aléatoire », lorsqu’ils se connectent au Wi-Fi. L’adresse affichée ici peut donc différer de l’adresse MAC physique de l’appareil.
Aléatoire (Random)	Génère automatiquement une adresse MAC aléatoire pour la connexion.

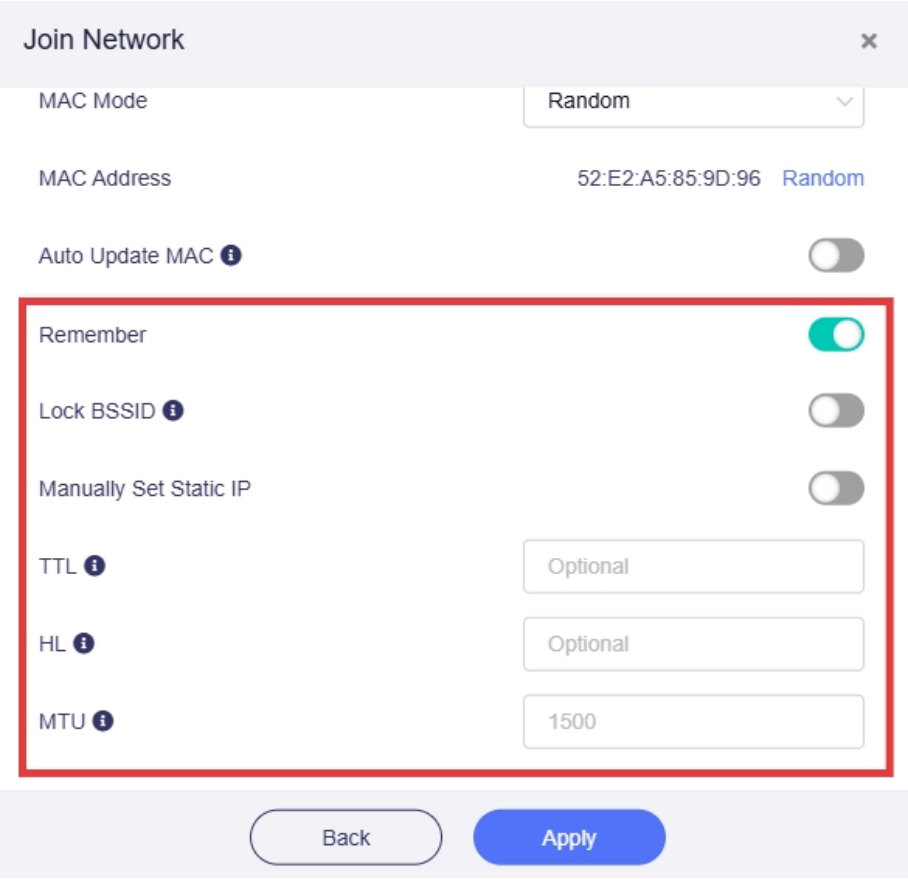
- **Mise à jour automatique de l’adresse MAC**

  Si cette option est activée, l’adresse MAC est mise à jour automatiquement.

Lors de l’enregistrement de la configuration réseau, le mode MAC et toute adresse MAC clonée ou aléatoire sont associés au SSID enregistré. Vous pouvez modifier ces paramètres manuellement pour chaque SSID à tout moment.

4.2.2.3 Paramètres avancés

Des options supplémentaires sont disponibles lors de la connexion au réseau.

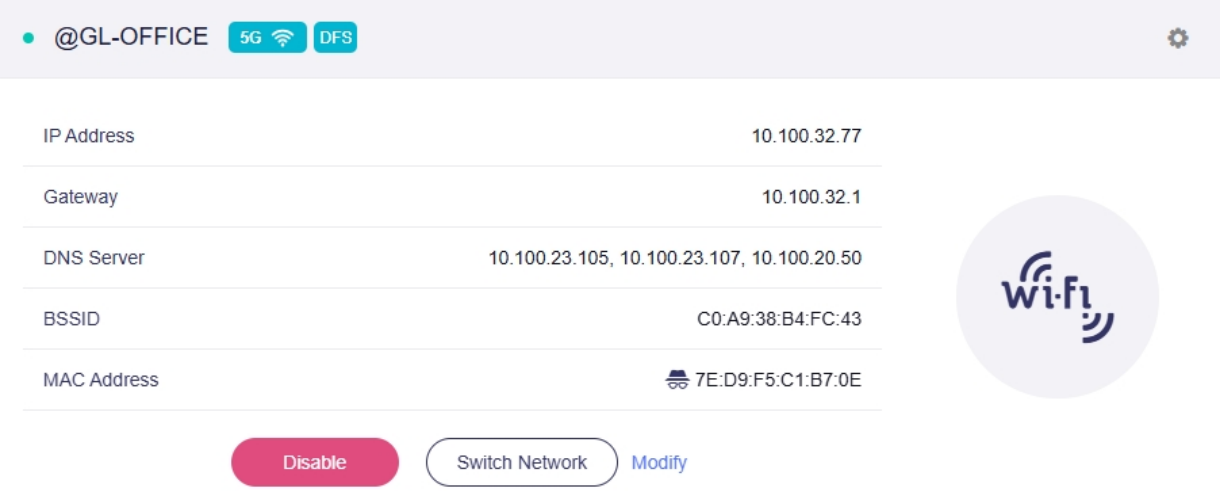


- **Mémoriser (Remember)** : activez cette option pour mémoriser le réseau Wi-Fi actuellement utilisé en mode répéteur.
- **Verrouiller le BSSID (Lock BSSID)** : lorsque cette option est activée, le routeur se connecte uniquement au point d'accès correspondant au BSSID sélectionné, même si d'autres points d'accès utilisent le même SSID.
- **Définir manuellement une IP statique (Manually Set Static IP)** : lorsque cette option est activée, vous pouvez définir une adresse IPv4 fixe, un masque de sous-réseau, une passerelle et des serveurs DNS pour la connexion du répéteur, au lieu d'obtenir ces paramètres automatiquement.
- **TTL** : le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Renseignez-le selon les exigences de l'opérateur. Ce paramètre ne s'applique qu'à IPv4. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour modifier ce comportement, saisissez le TTL effectif souhaité augmenté de 1 afin de compenser cette diminution automatique.

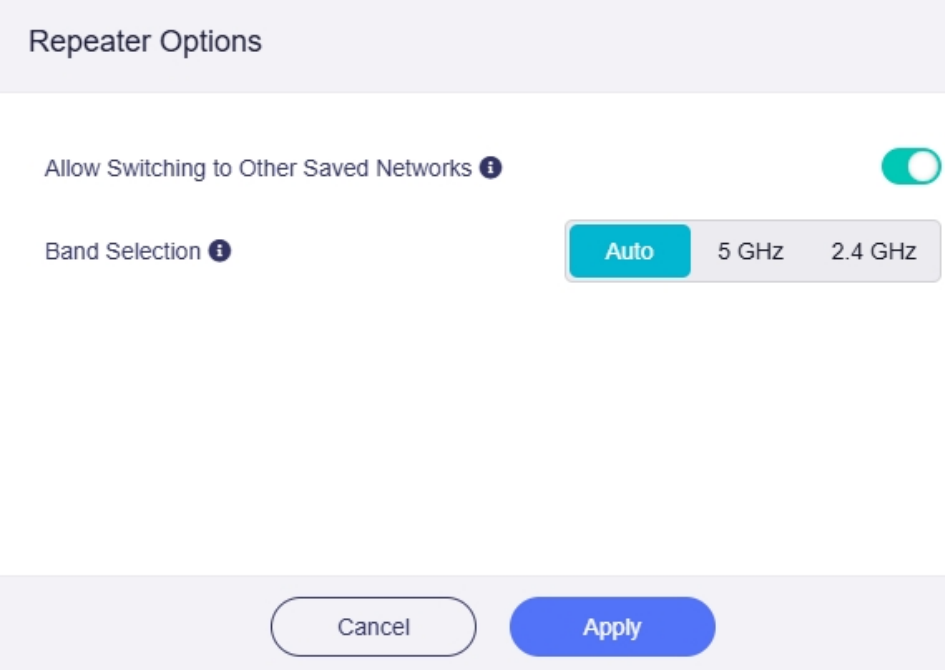
- **HL** : en IPv6, le champ HL (Hop Limit, limite de sauts) limite le nombre de sauts des paquets dans le réseau. Il remplit le même rôle que le TTL en IPv4.
- **MTU** : la valeur par défaut est de 1 500.

4.2.2.4 Options du répéteur

Cliquez sur l'engrenage dans l'angle supérieur droit de la section Répéteur connecté.



Les options du répéteur s'affichent comme suit.

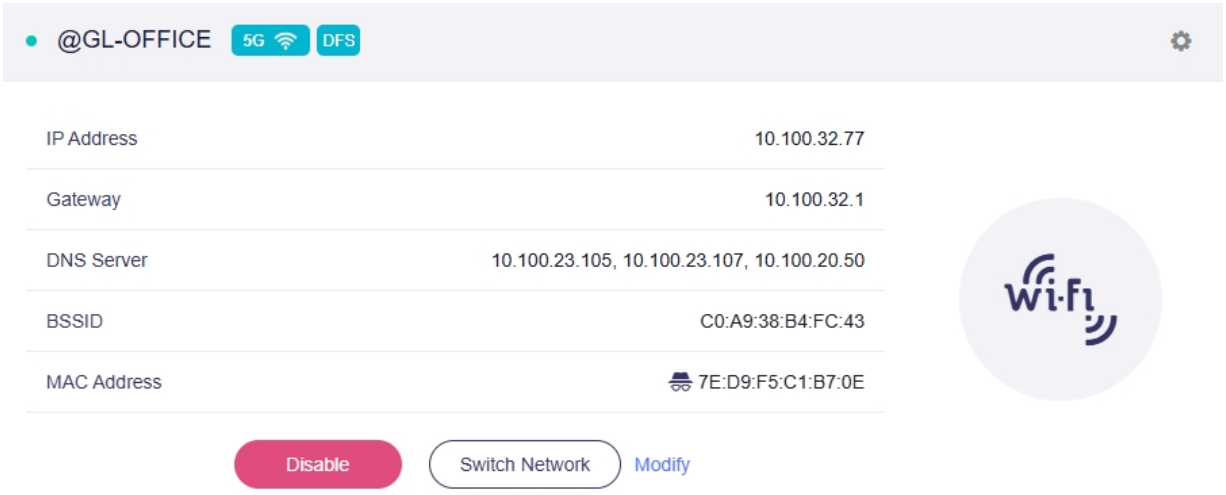


- **Autoriser le basculement vers d'autres réseaux enregistrés (Allow Switching to Other Saved Networks)** : lorsque cette option est activée, le routeur se connecte automatiquement à un autre réseau enregistré si le réseau Wi-Fi actuel devient indisponible.

- **Sélection de la bande (Band Selection)** : si vous sélectionnez une bande manuellement, le routeur recherche uniquement les réseaux Wi-Fi de cette bande et ne se connecte qu'à ceux-ci.

4.2.2.5 Gestion des réseaux connus

Pour gérer les réseaux connus, cliquez sur **Changer de réseau (Switch Network)**.

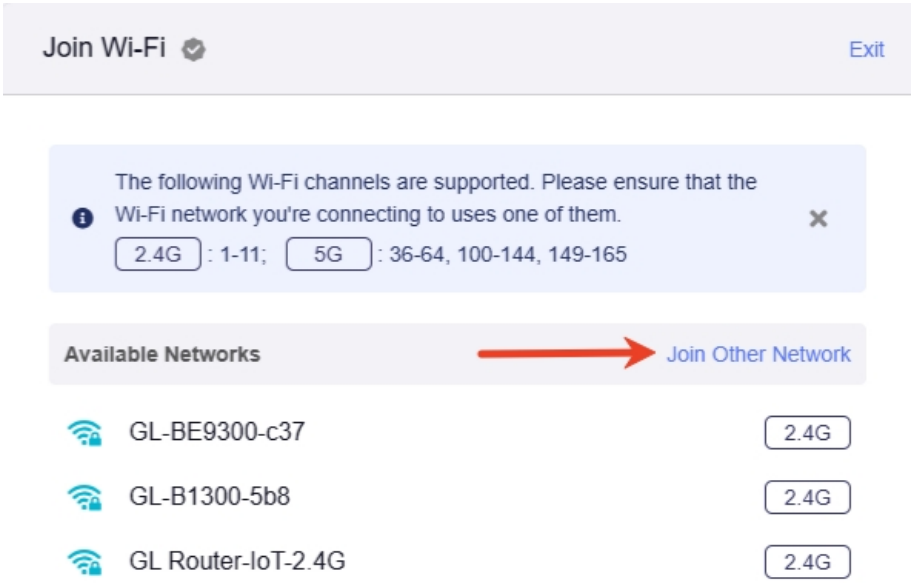


Dans la section **Réseaux connus (Known Networks)**, cliquez sur la corbeille pour supprimer un réseau, ou sur l'engrenage pour le configurer.

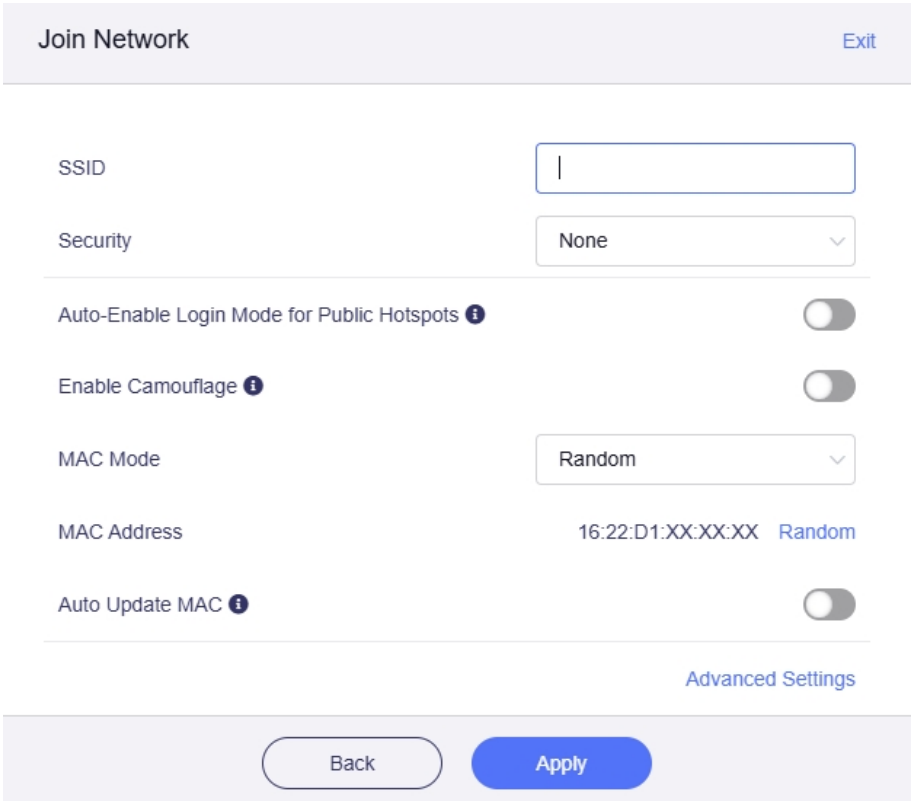


4.2.2.6 Rejoindre un autre réseau

Si le SSID ne figure pas dans la liste des réseaux disponibles ou s'il est masqué, cliquez sur **Rejoindre un autre réseau (Join Other Network)**.

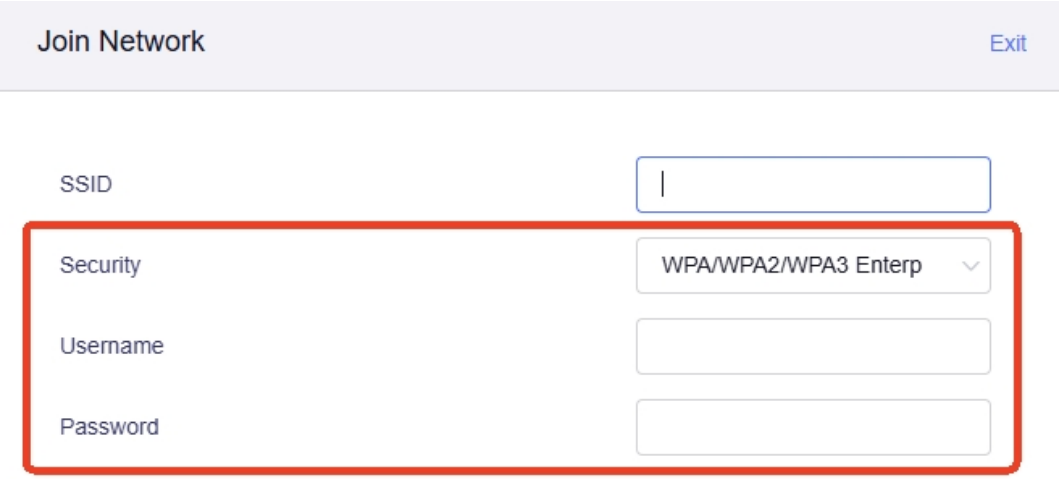


Saisissez le **SSID**, sélectionnez la **Sécurité (Security)** et saisissez le mot de passe si nécessaire, puis cliquez sur **Appliquer (Apply)**.



Les paramètres de **Sécurité (Security)** proposent deux ou trois options selon le modèle.

- Aucune : aucun mot de passe n'est nécessaire.
- WPA/WPA2/WPA3 : option courante, prise en charge par presque tous les réseaux Wi-Fi.
- WPA/WPA2/WPA3 Enterprise : utilise le protocole EAP (Extensible Authentication Protocol) pour l'authentification. Un identifiant et un mot de passe valides sont nécessaires, généralement sur les réseaux d'entreprise ou de campus.



Pour obtenir des instructions détaillées sur la connexion aux réseaux EAP en mode répéteur, consultez cette page.

4.2.2.7 Reconnexion

Dans les situations suivantes, le routeur tente périodiquement de se reconnecter au Wi-Fi. Vous pouvez désactiver manuellement cette fonction si nécessaire. En cas d'erreur de SSID ou de mot de passe, supprimez le réseau de la liste des réseaux connus pour résoudre le problème.

1. SSID ou mot de passe incorrect saisi lors de la configuration du répéteur.
2. Routeur déplacé hors de portée du routeur en amont après la connexion initiale.
3. SSID ou mot de passe modifié, ou accès restreint par le routeur en amont après la connexion.

Le processus de reconnexion comporte trois phases distinctes : attente, recherche et connexion.

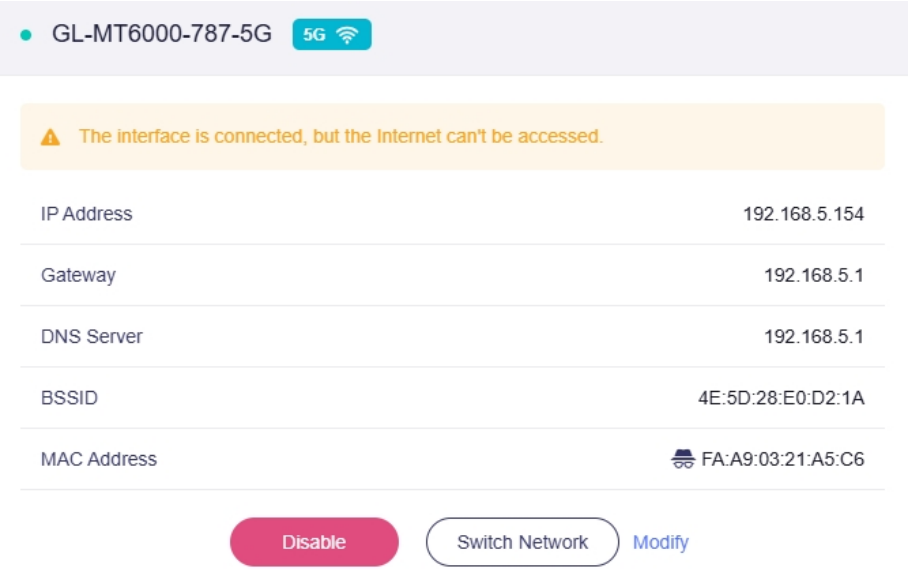
1. Phase d'attente : aucune perturbation ; le routeur attend que les conditions de reconnexion soient réunies.
2. Phase de recherche : des pertes de paquets peuvent survenir sur la bande recherchée. Les nouveaux appareils peuvent rencontrer des difficultés de connexion. Sur les modèles GL-AXT1800 et GL-AX1800, le Wi-Fi invité est temporairement désactivé.
3. Phase de connexion : le Wi-Fi principal de la bande concernée peut être interrompu pendant quelques secondes lors du rétablissement de la connexion.

Remarque : les problèmes surviennent généralement pendant les phases de recherche et de connexion.

4.2.2.8 Dépannage

Lorsque le routeur est connecté à un réseau Wi-Fi en mode répéteur mais que l'accès à Internet est indisponible, le message jaune ci-dessous s'affiche.

« L'interface est connectée, mais l'accès à Internet est impossible. » (The interface is connected, but the Internet can't be accessed.)



Pour résoudre ce problème :

1. Vérifiez que l'appareil en amont, c'est-à-dire le réseau Wi-Fi auquel votre routeur est connecté, dispose d'un accès à Internet.
2. Ouvrez la page Multi-WAN pour vérifier l'état de l'interface du répéteur.

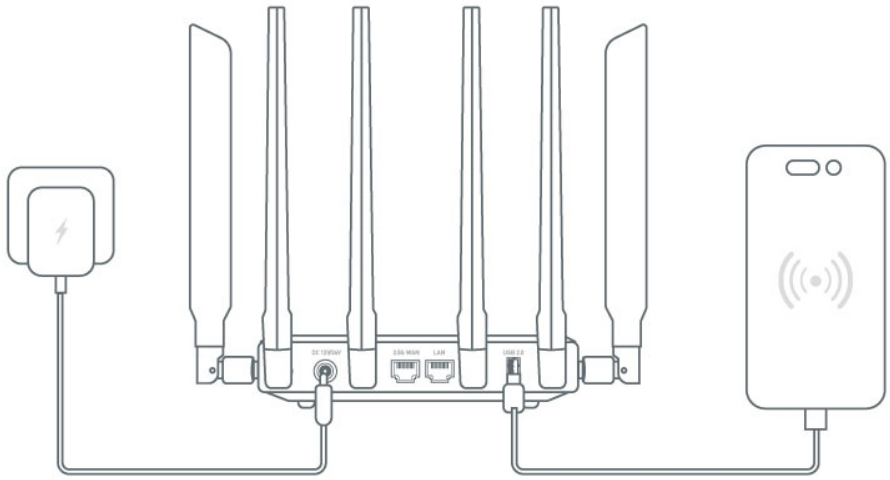
4.2.2.9 DFS

DFS (Dynamic Frequency Selection, sélection dynamique de fréquence) est un mécanisme qui change automatiquement de canal Wi-Fi pour éviter les interférences avec les radars. Lorsqu'il se connecte à un réseau Wi-Fi 5 GHz en amont, le routeur suit ce réseau pour l'utilisation ou non d'un canal DFS.

- Si le Wi-Fi en amont utilise un canal DFS détectable, le Wi-Fi 5 GHz du routeur utilise le même canal.
- Le Wi-Fi 5 GHz du routeur passe à un canal non DFS si le Wi-Fi en amont ne peut pas être détecté ou si la connexion échoue.

4.2.3 Connexion à Internet par partage de connexion USB

Le partage de connexion USB, ou Tethering, consiste à relier un smartphone au routeur avec un câble USB pour partager sa connexion mobile, par exemple 4G ou 5G. Cette méthode convient à un accès Internet temporaire, notamment en déplacement ou dans les zones sans accès fixe à Internet.

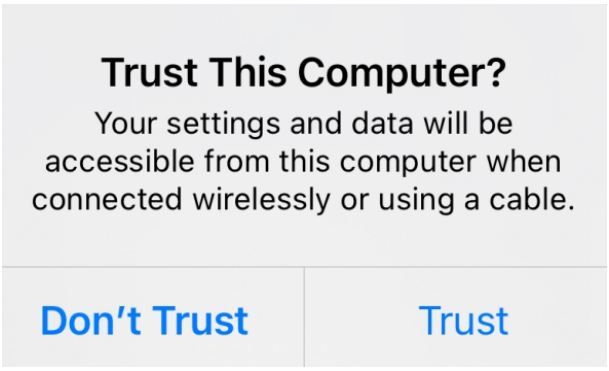


Les modems autonomes (host-less) fonctionnent également en mode Partage de connexion lors de la configuration de la connexion cellulaire.

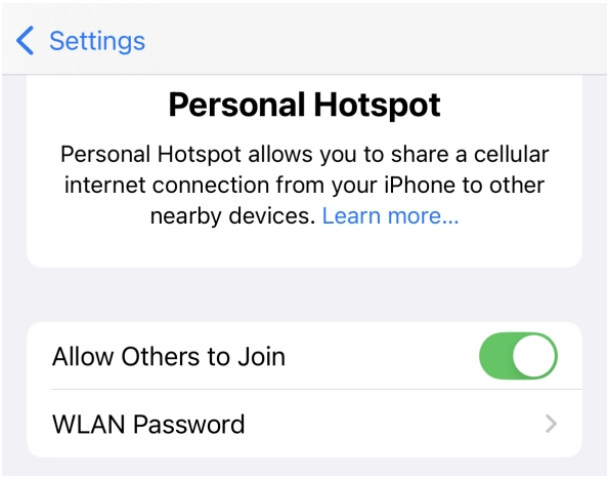
Remarque : certains opérateurs mobiles limitent le partage de connexion ou le facturent en supplément. Renseignez-vous auprès de votre opérateur.

4.2.3.1 iPhone

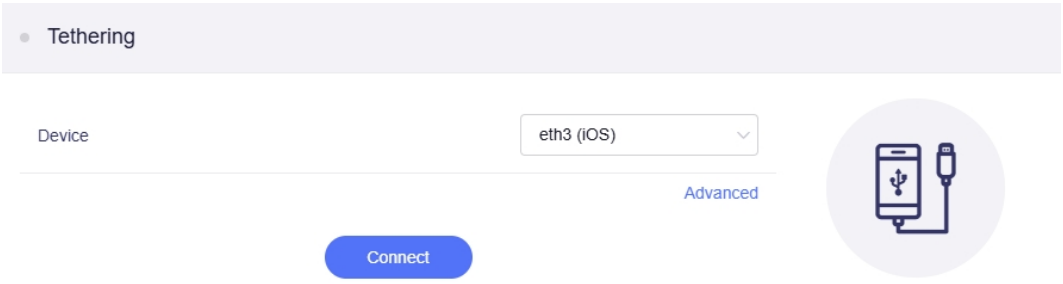
1. Reliez l'iPhone au port USB du routeur à l'aide d'un câble USB. Une boîte de dialogue vous demande si vous souhaitez faire confiance à cet appareil. Touchez **Se fier (Trust)** pour continuer.



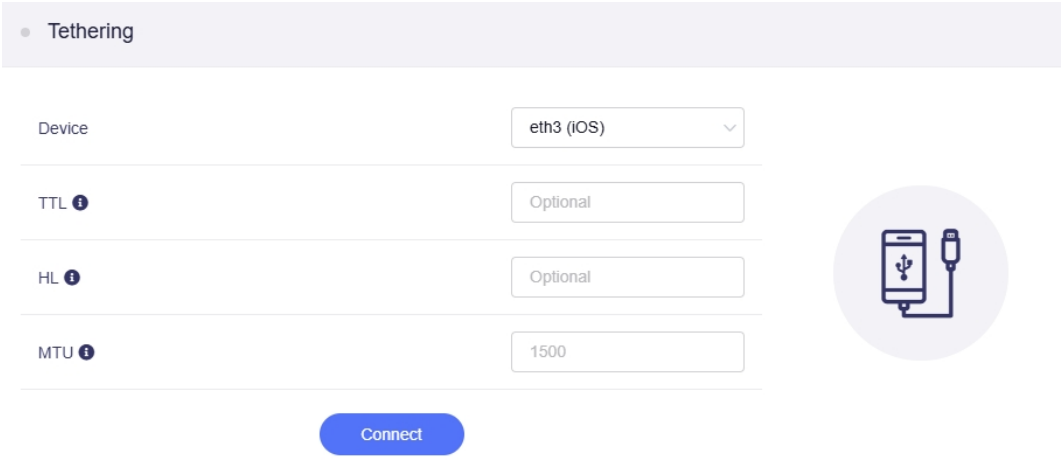
2. Sur l'iPhone, ouvrez **Réglages (Settings)** > **Partage de connexion (Personal Hotspot)**. Activez **Autoriser d'autres utilisateurs (Allow Others to Join)**.



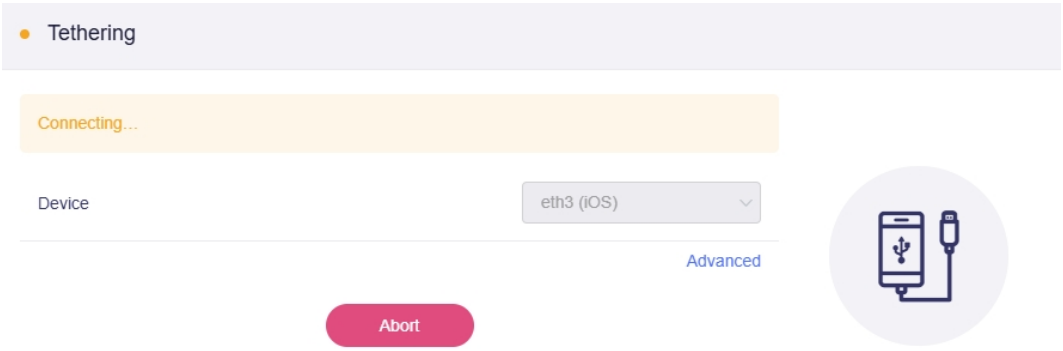
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



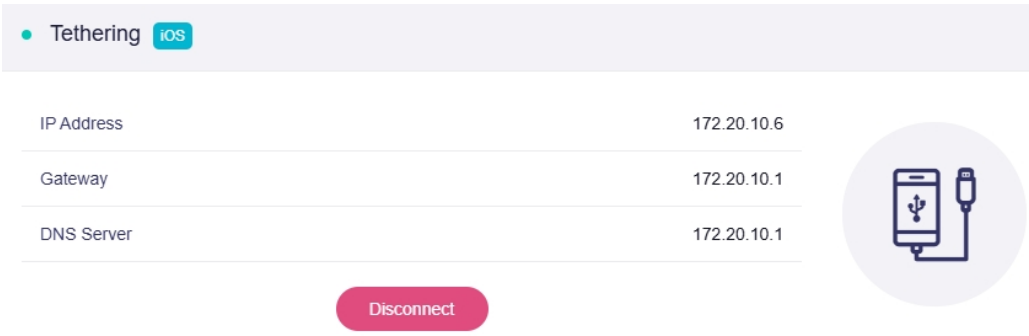
Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)**. Ajustez les paramètres, puis cliquez sur **Connecter (Connect)**.



4. La connexion démarre.



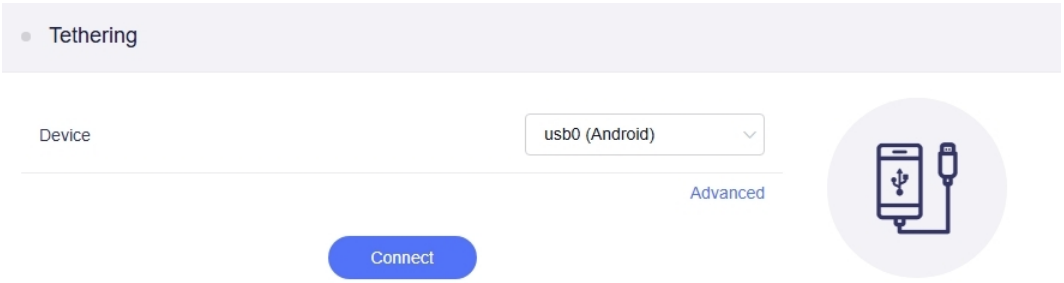
Une fois la connexion établie, cette page en affiche les détails.



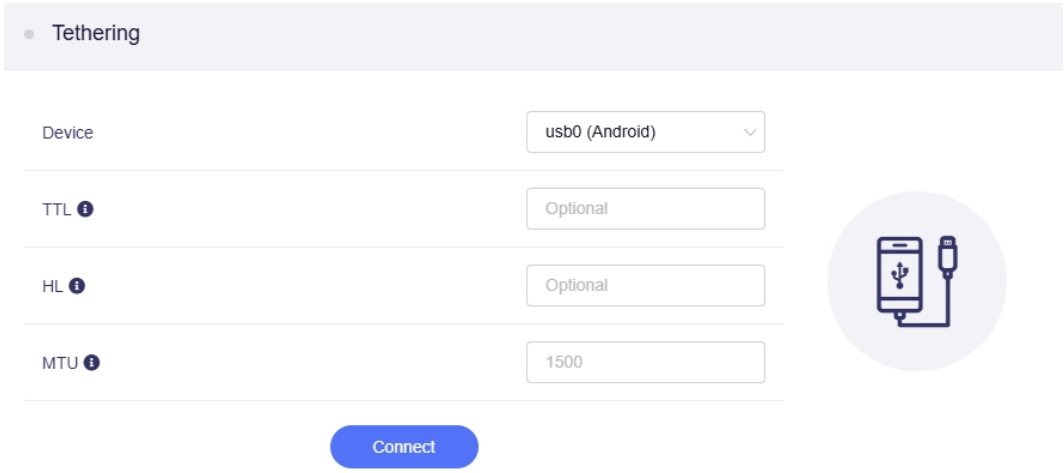
4.2.3.2 Android

1. Reliez le téléphone Android au port USB du routeur avec un câble USB. Une boîte de dialogue peut afficher les préférences USB (USB preferences). Si vous y êtes invité, sélectionnez **Partage de connexion USB (USB Tethering)** ou **Transfert de fichiers (File Transfer)**.

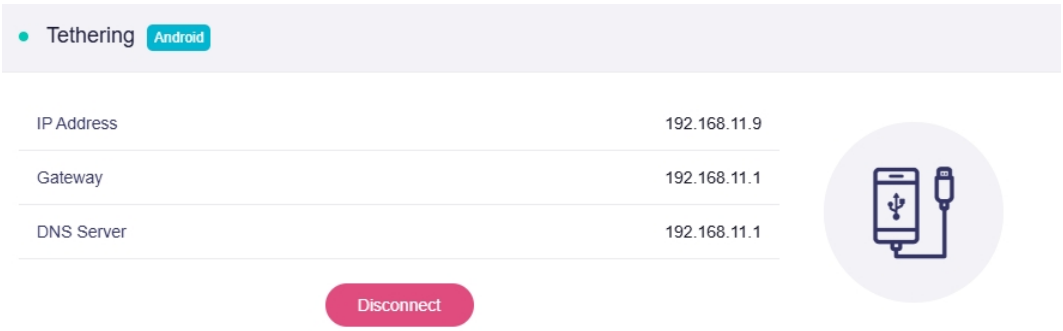
2. Sur le téléphone, ouvrez **Paramètres (Settings)** > **Réseau et Internet (Network & Internet)** > **Point d'accès personnel (Personal Hotspot)**. Activez **Point d'accès personnel (Personal Hotspot)** ou **Partage de connexion USB (USB Tethering)**. (La procédure d'activation du partage de connexion USB varie selon la marque. Consultez les paramètres de votre appareil pour trouver cette option et contactez l'assistance du fabricant si nécessaire.)
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, puis ouvrez **INTERNET** > **Partage de connexion (Tethering)**. Cliquez sur **Connecter (Connect)**.



Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)**. Ajustez les paramètres, puis cliquez sur **Connecter (Connect)**.



4. Une fois la connexion établie, cette page affiche son état.



4.2.3.3 Dépannage

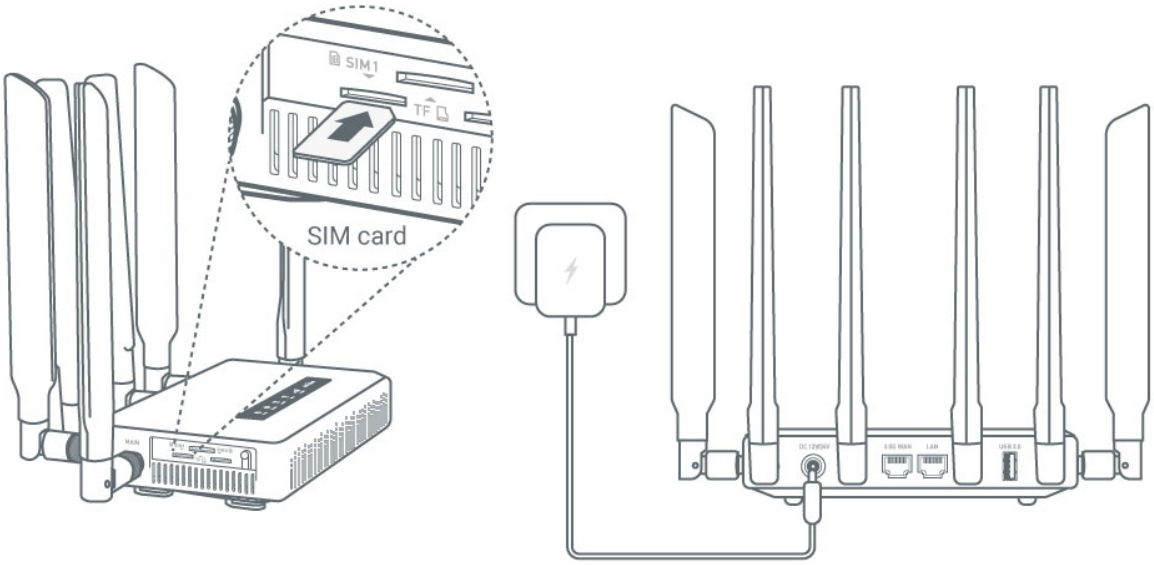
Si la connexion échoue, essayez les mesures de dépannage suivantes :

- Utilisez le bloc d'alimentation d'origine du routeur.
- Débranchez puis rebranchez le câble USB.
- Essayez un autre câble USB. Vérifiez qu'il permet le transfert de données, et pas seulement la recharge.
- Désactivez puis réactivez plusieurs fois le « partage de connexion USB » sur le téléphone Android.
- Désactivez puis réactivez plusieurs fois « Autoriser d'autres utilisateurs » sur l'iPhone.
- Redémarrez votre smartphone et réessayez.

Si le problème persiste, contactez notre assistance technique à l'adresse support@gl-inet.com.

4.2.4 Connexion à Internet via le réseau cellulaire

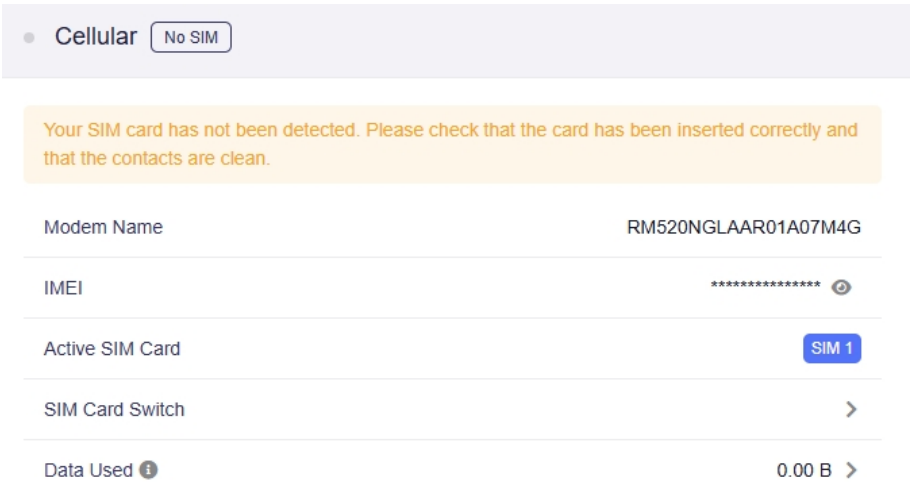
Spitz AX (GL-X3000) intègre un modem cellulaire double SIM. Une seule carte SIM est active à la fois ; l'autre sert de secours. Vous pouvez passer manuellement d'une carte SIM à l'autre.



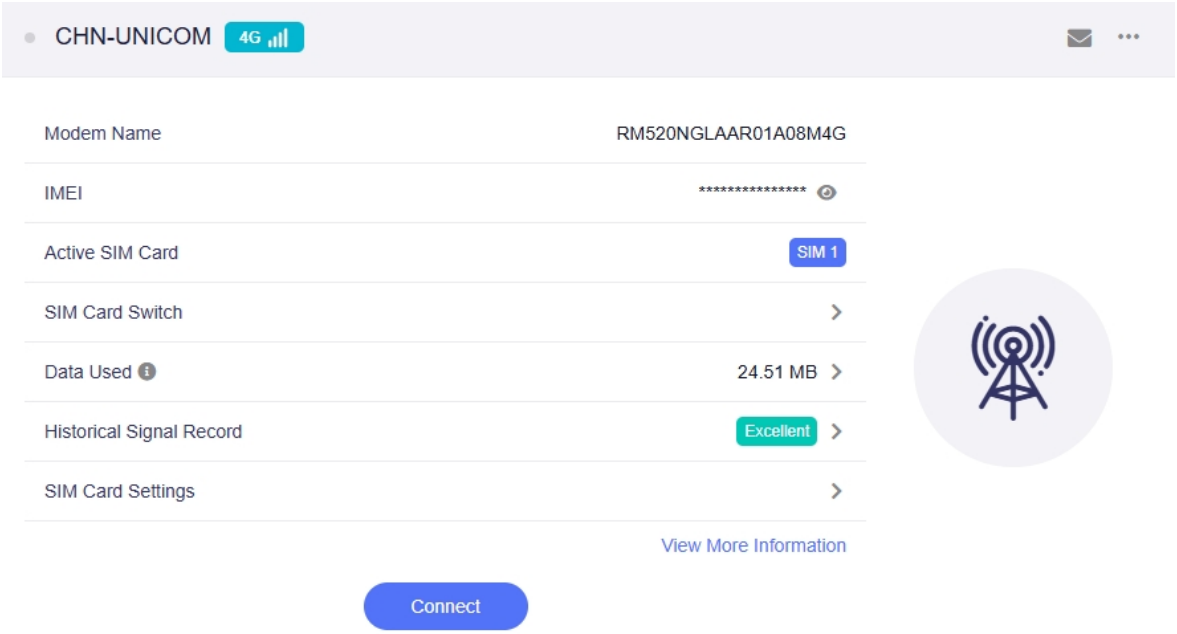
4.2.4.1 Configuration automatique

Nous vous recommandons d'éteindre d'abord le routeur, d'insérer les cartes SIM préalablement activées dans leurs emplacements, puis de le rallumer. Si vous insérez une carte SIM après le démarrage du routeur, l'interface d'administration Web risque de ne pas s'actualiser automatiquement. Dans ce cas, actualisez la page ou redémarrez le routeur.

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Cellulaire (Cellular)**.
2. Si aucune carte SIM n'est insérée, le message « Votre carte SIM n'a pas été détectée » (Your SIM card has not been detected) s'affiche.

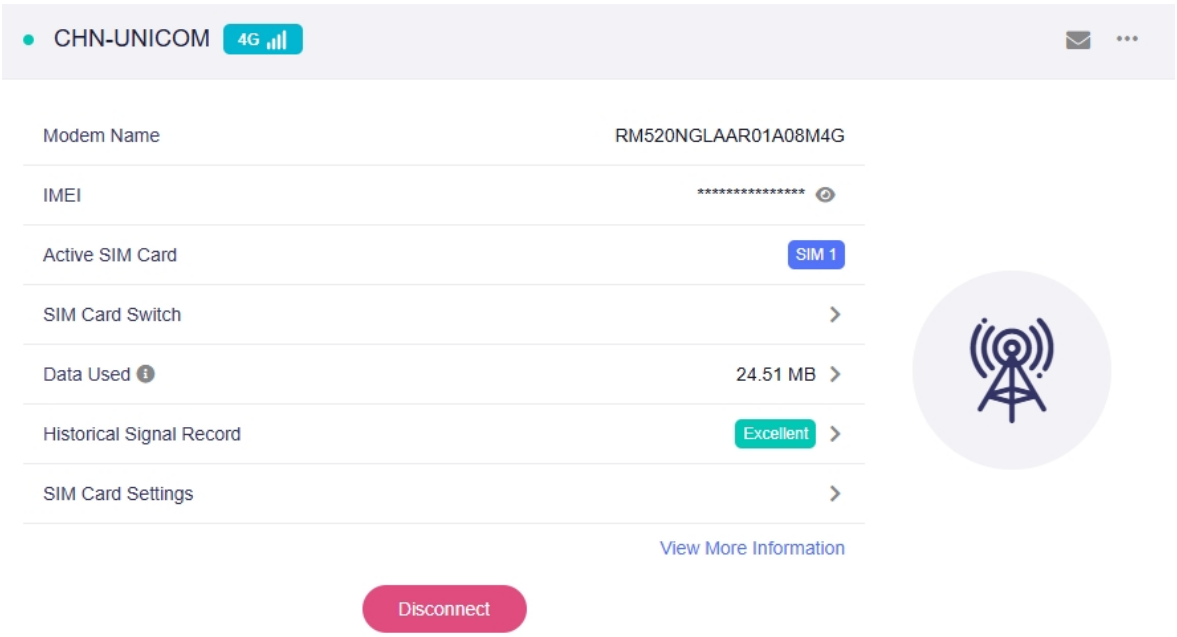


3. Lorsqu’une carte SIM est insérée, la page s’affiche comme suit. Cliquez sur **Connecter (Connect)**.

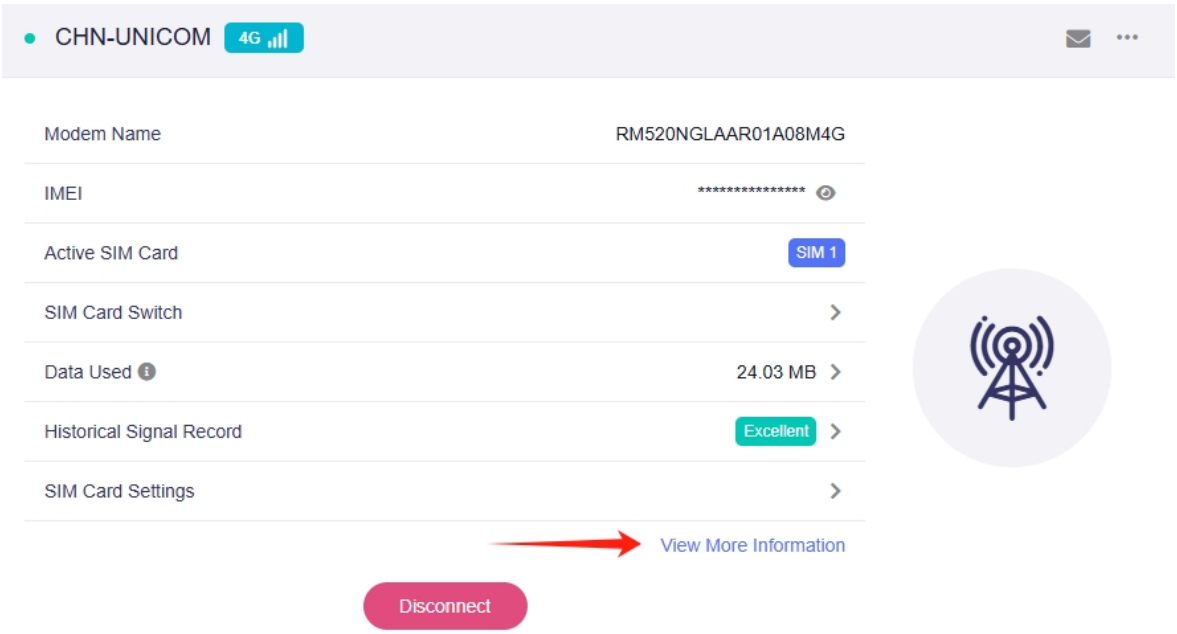


Conseil : si la carte SIM n’est pas détectée, redémarrez le routeur pour vérifier si elle peut être reconnue.

4. Une fois la connexion cellulaire établie, la page affiche les informations réseau et un point vert confirmant la connexion.



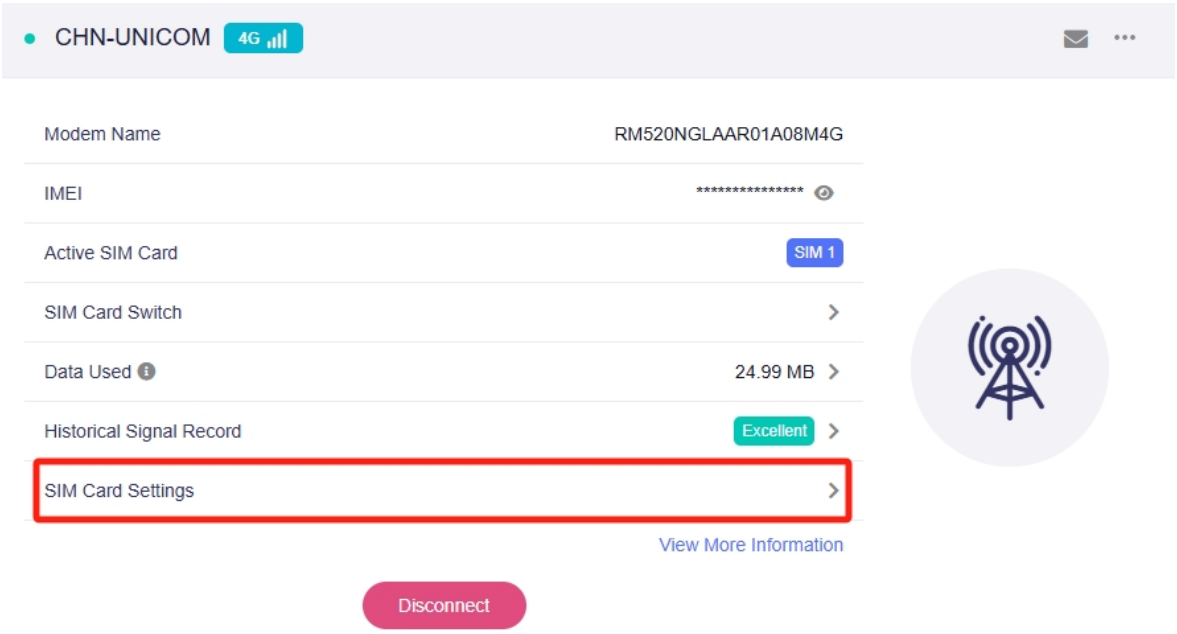
5. Cliquez sur **Afficher plus d’informations (View More Information)** pour consulter les détails du modem, de la carte SIM, de la connexion Internet et du signal cellulaire.



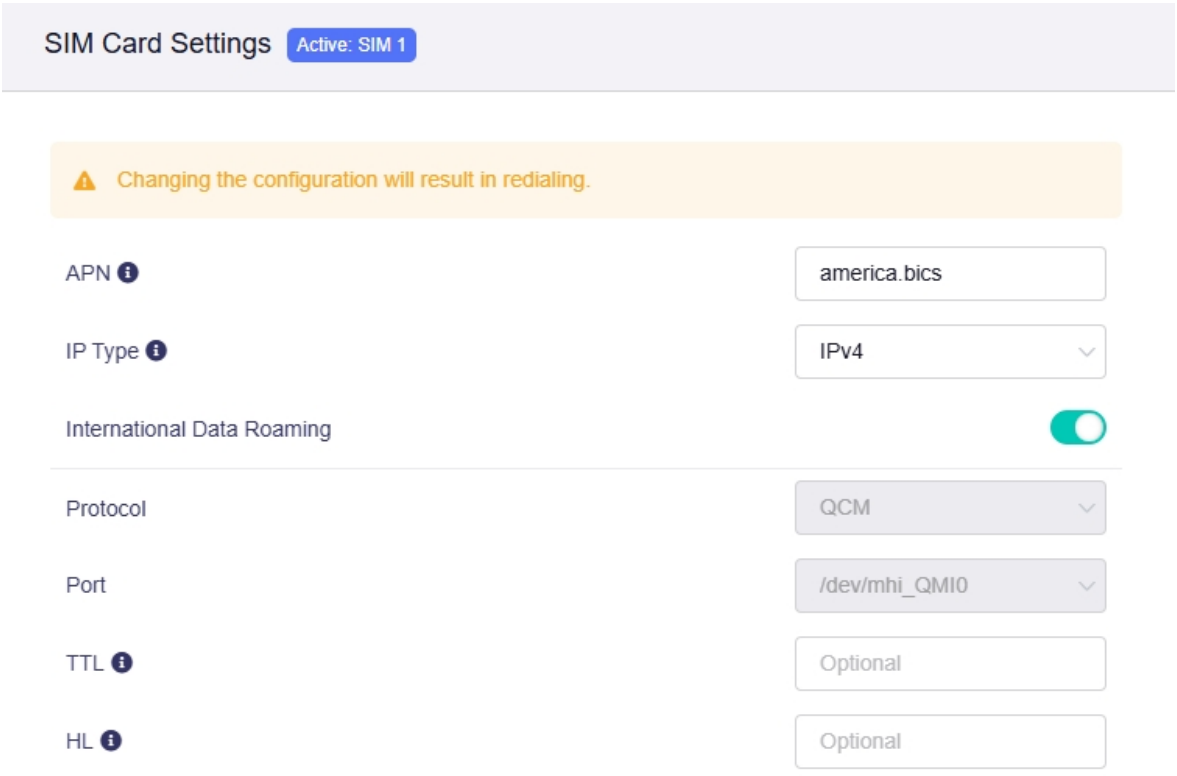
Si la configuration automatique échoue, essayez la **configuration manuelle**.

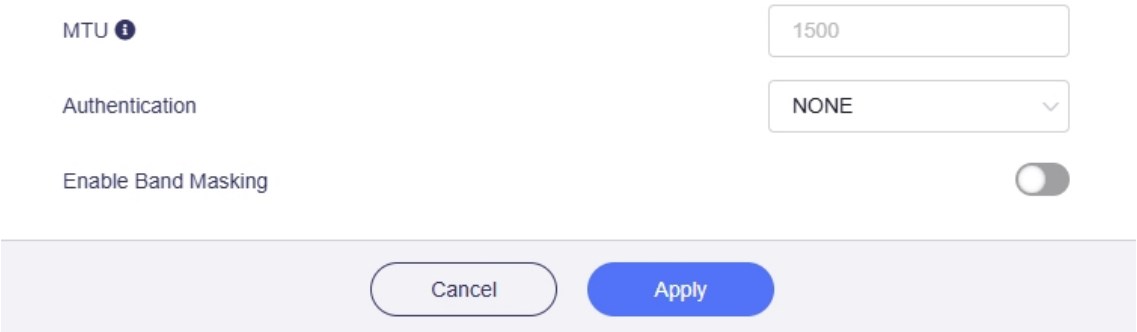
4.2.4.2 Configuration manuelle

1. Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**, puis cliquez sur **Paramètres de la carte SIM (SIM Card Settings)**.



2. Vous pouvez consulter ou modifier les paramètres cellulaires de la carte SIM active. L'application des modifications déclenche une reconnexion.

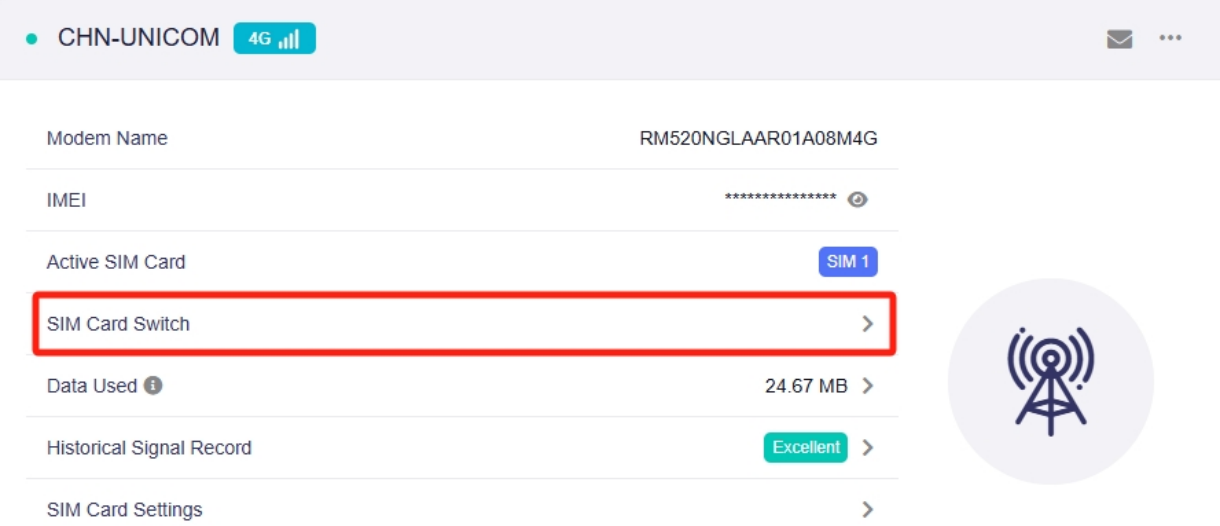




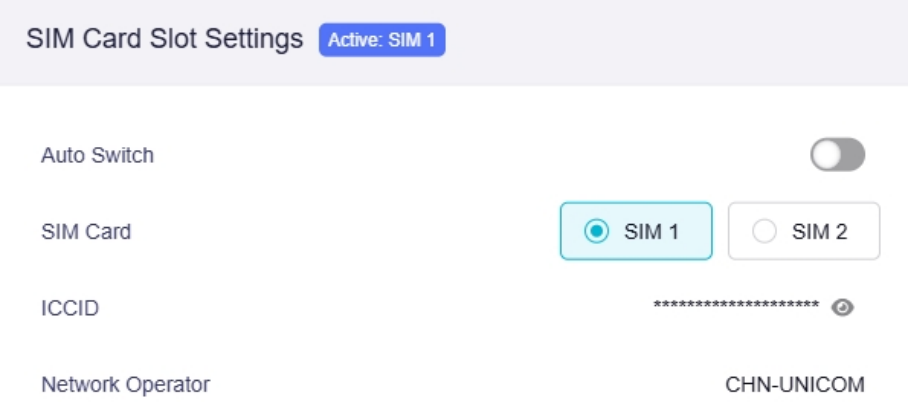
- **APN** : l'APN (Access Point Name, nom du point d'accès) est un paramètre de passerelle nécessaire à la connexion cellulaire. Il permet au routeur d'accéder à Internet via votre opérateur mobile. Vous pouvez utiliser l'APN par défaut ou définir un APN personnalisé fourni par votre opérateur.
- **Protocole (Protocol)** : protocole de communication cellulaire détecté automatiquement, par exemple QMI ou QCM, selon le modem et l'opérateur.
- **Port** : port série détecté automatiquement pour communiquer avec le modem cellulaire.
- **TTL** : le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Ce paramètre ne s'applique qu'à IPv4. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour modifier ce comportement, saisissez le TTL effectif souhaité augmenté de 1 afin de compenser cette diminution automatique.
- **HL** : en IPv6, le champ HL (Hop Limit, limite de sauts) limite le nombre de sauts que peuvent effectuer les paquets dans le réseau. Il remplit le même rôle que le TTL en IPv4.
- **MTU** : la valeur MTU par défaut est de 1 500 octets.
- **Authentification (Authentication)** : choisissez la méthode d'authentification exigée par votre opérateur, par exemple NONE, PAP ou CHAP. La valeur est généralement NONE si aucun identifiant n'est nécessaire.
- **Masquage des bandes (Band Masking)** : activez cette option pour bloquer certaines bandes ou utiliser uniquement des bandes cellulaires précises. Consultez la section 4.2.4.6 Masquage des bandes pour en savoir plus.

4.2.4.3 Paramètres des emplacements SIM

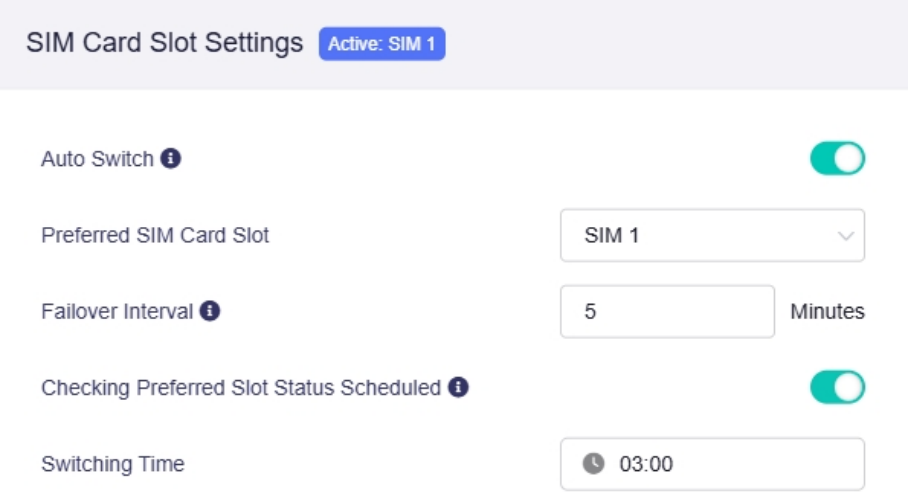
Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**, puis cliquez sur **Basculement de carte SIM (SIM Card Switch)**.



La page affiche le bouton de basculement automatique, la carte SIM active, l'ICCID et l'opérateur réseau.



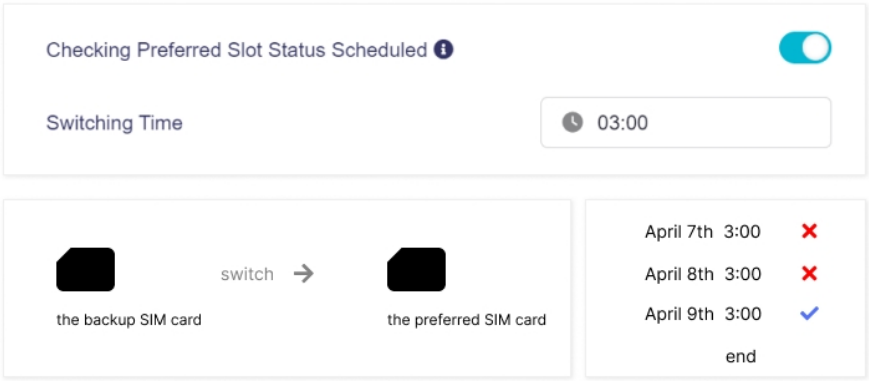
Si deux cartes SIM sont insérées, vous pouvez activer **Basculement automatique (Auto Switch)**.



- **Basculement automatique (Auto Switch)** : permet de passer automatiquement de SIM 1 à SIM 2 et inversement. La méthode de détection du réseau utilisée est celle configurée sur la page Multi-WAN.
- **Emplacement SIM préféré (Preferred SIM Card Slot)** : choisissez SIM 1 ou SIM 2 comme carte SIM préférée.
- **Intervalle de basculement (Failover Interval)** : les valeurs disponibles vont de 5 minutes à 24 heures.

  Si la connexion Internet reste indisponible après un basculement, l'appareil revient à l'emplacement SIM préféré et attend cet intervalle avant de tenter un nouveau basculement. Cette option s'applique lorsque ni la carte SIM préférée ni la carte SIM de secours ne reçoit de signal. L'appareil passe d'une carte à l'autre jusqu'à ce que l'une d'elles reçoive un signal valide.
- **Vérification programmée de l'emplacement préféré (Checking Preferred Slot Status Scheduled)**

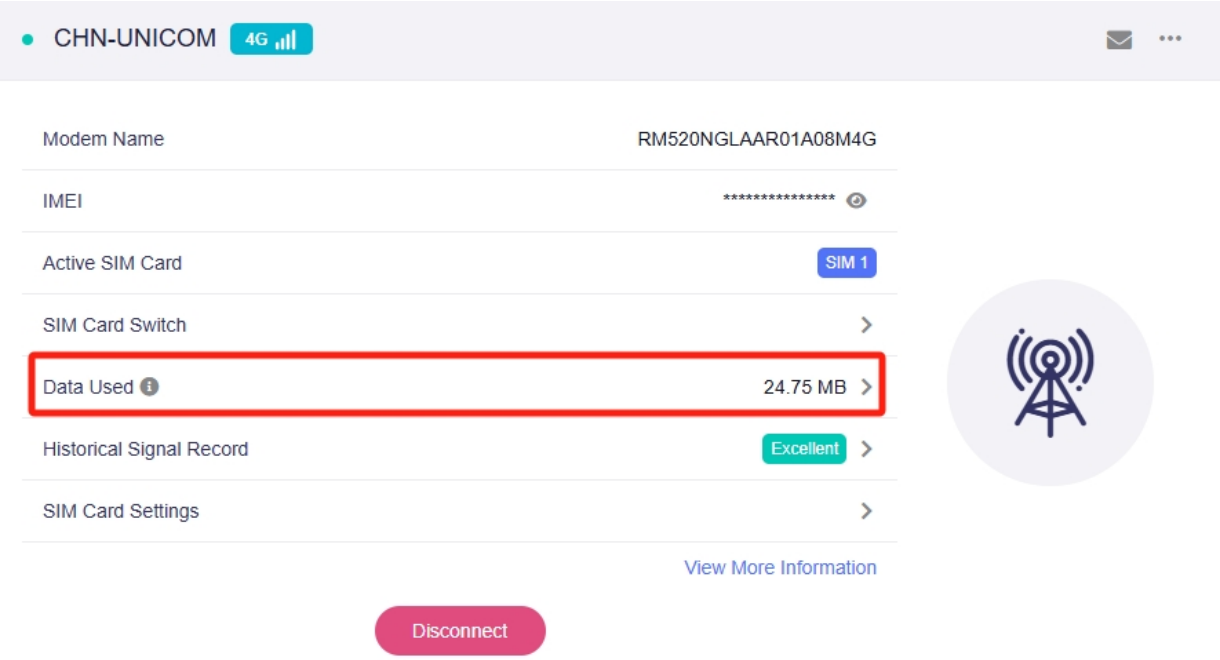
  Lorsque cette option est activée, l'appareil vérifie chaque jour l'emplacement SIM préféré à l'heure définie. Il tente d'y revenir si la carte SIM préférée retrouve un accès à Internet. Cela évite une consommation excessive de données sur la carte SIM de secours. Si la carte SIM préférée ne reçoit toujours aucun signal, l'appareil continue d'utiliser la carte SIM de secours.



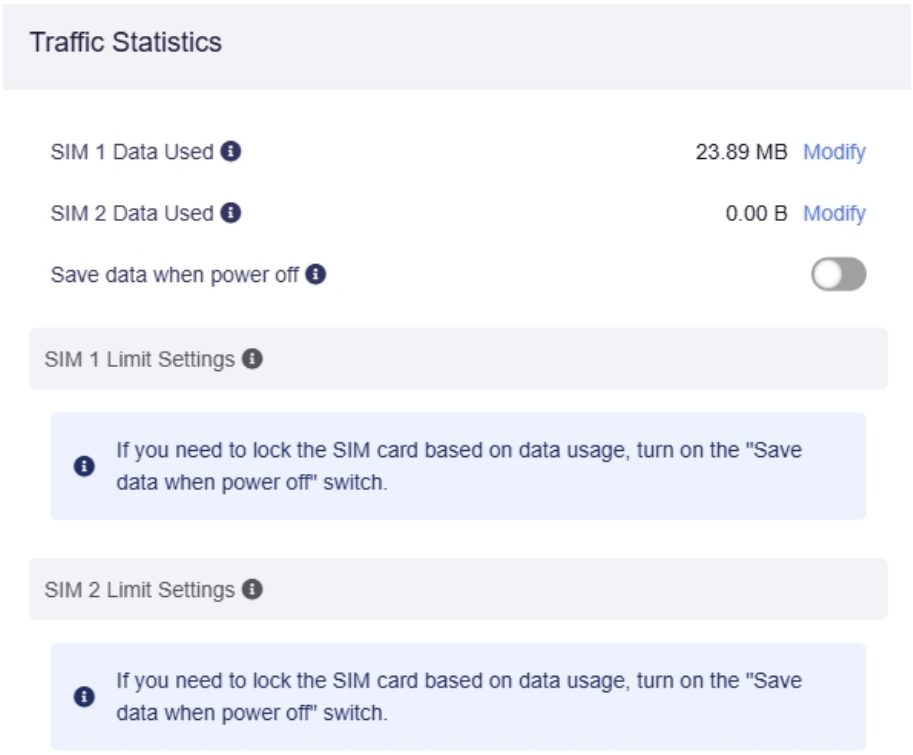
Remarque : le basculement automatique ne passe pas immédiatement à l'autre carte SIM. L'appareil doit d'abord confirmer que la carte SIM actuelle ne peut pas accéder à Internet. Ensuite, l'autre carte SIM n'étant pas en veille, son activation prend également du temps.

4.2.4.4 Statistiques de trafic

Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**, puis cliquez sur **Données utilisées (Data Used)**.



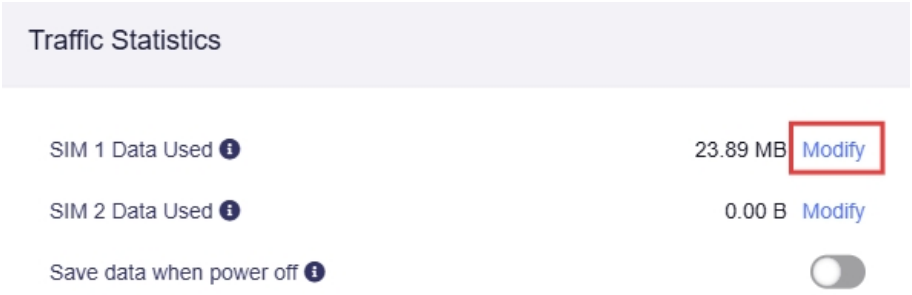
La page **Statistiques de trafic (Traffic Statistics)** s'ouvre. Elle affiche la consommation des cartes SIM et permet de définir des limites de données.



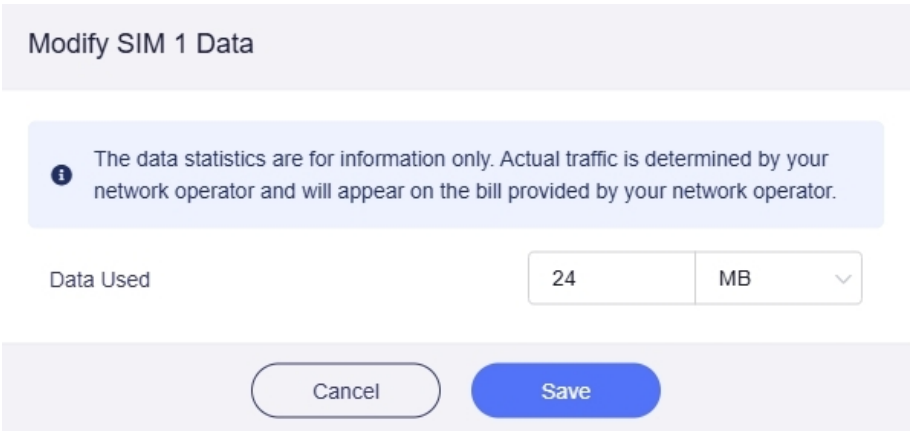
Si la consommation dépasse le plafond défini, modifiez manuellement le **Plafond de données (Data Cap Amount)** ou les **Données utilisées (Data Used)**. Sinon, la connexion peut être interrompue ou une autre carte SIM peut être sélectionnée automatiquement sur les modèles double SIM.

- **Modification de la consommation de données**

  Cliquez sur **Modifier (Modify)** à droite de la consommation de SIM 1 ou SIM 2.

  Vous pouvez alors modifier ou remettre à zéro la consommation de données.

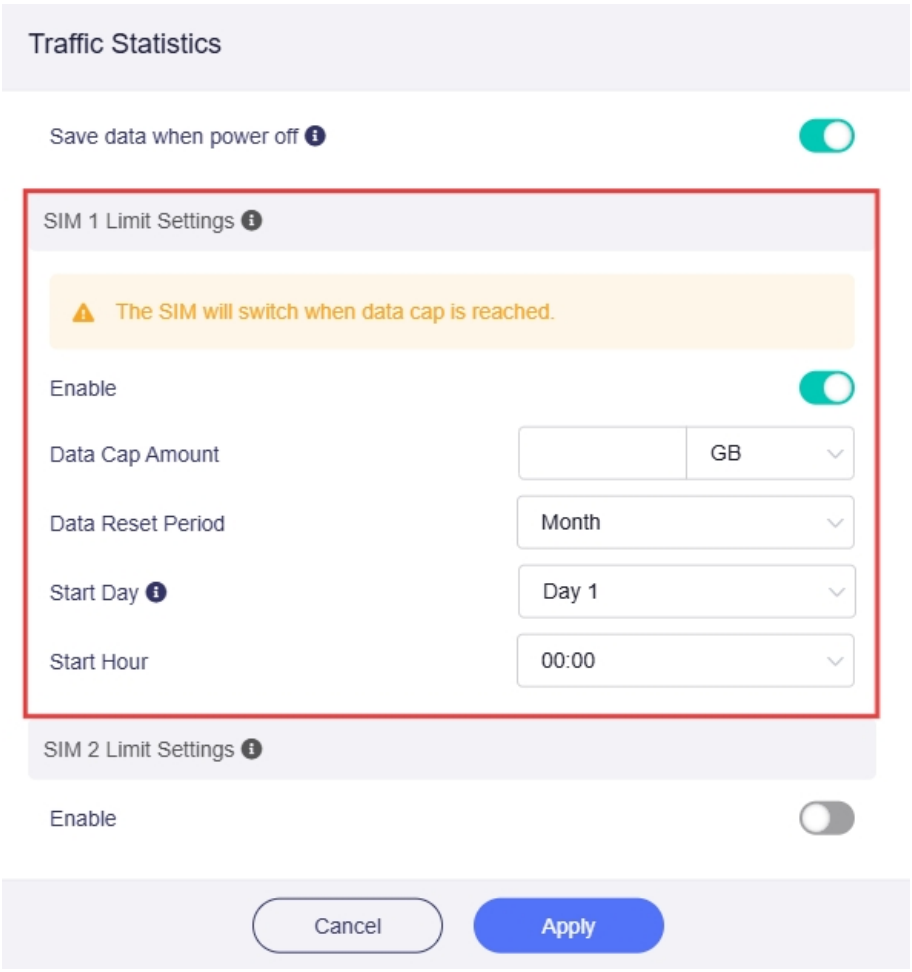


- **Définition d’une limite de données SIM**

  Pour définir une limite, activez d’abord **Conserver les données après extinction (Save data when power off)**. La consommation enregistrée sera ainsi conservée même après l’extinction de l’appareil.



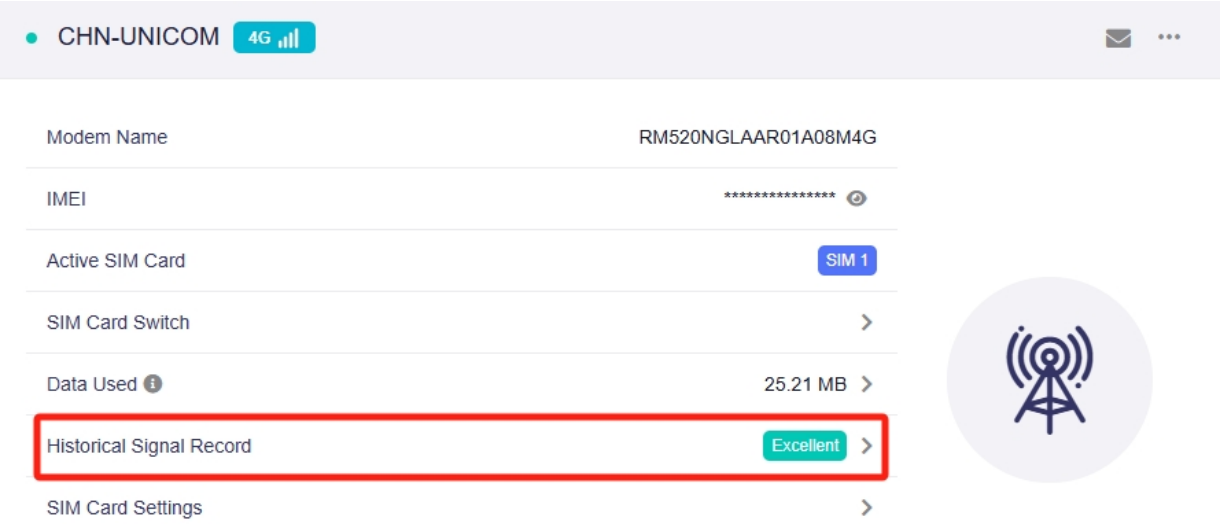
  Activez ensuite les paramètres de limite de SIM 1 ou SIM 2.



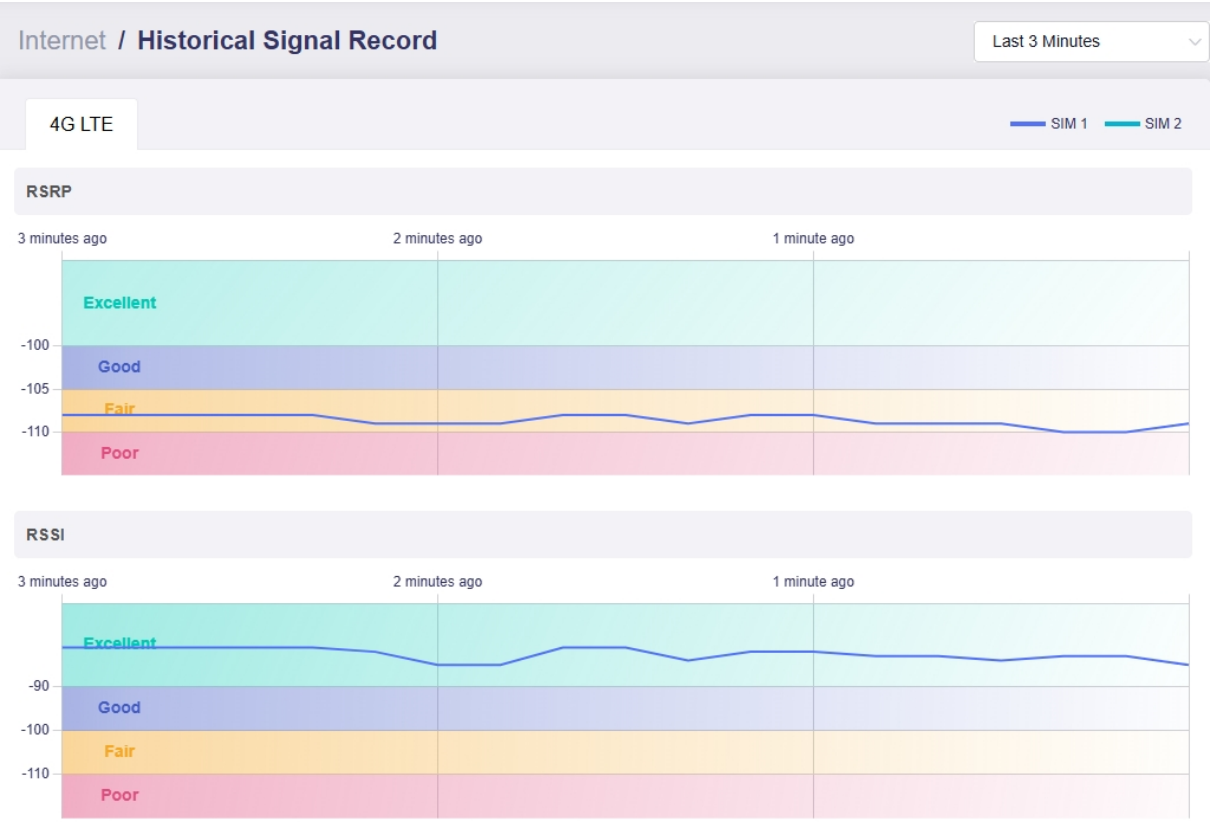
Sur les modèles double SIM, nous recommandons d’activer également le **basculement automatique des emplacements SIM (SIM Card Slot Auto Switch)**. Si un plafond est défini pour SIM 1 et que le basculement automatique est activé, l’appareil passe automatiquement de SIM 1 à SIM 2 lorsque la consommation de SIM 1 dépasse ce plafond. SIM 1 est alors désactivée.

4.2.4.5 Historique du signal

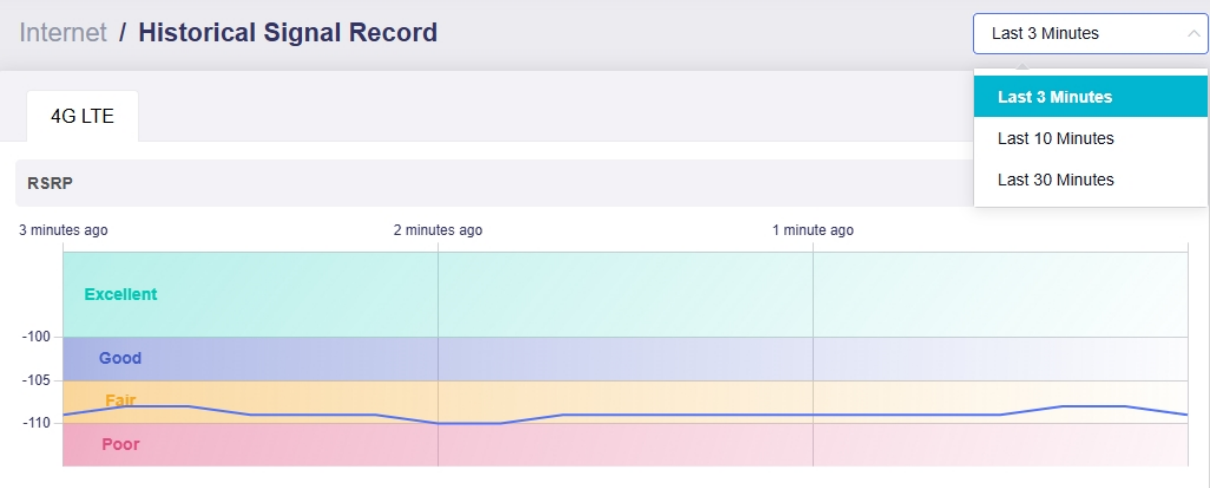
Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**, puis cliquez sur **Historique du signal (Historical Signal Record)**.



Vous pouvez y vérifier la qualité de la connexion cellulaire. Si le signal est faible, essayez de changer de station de base pour obtenir un meilleur signal.



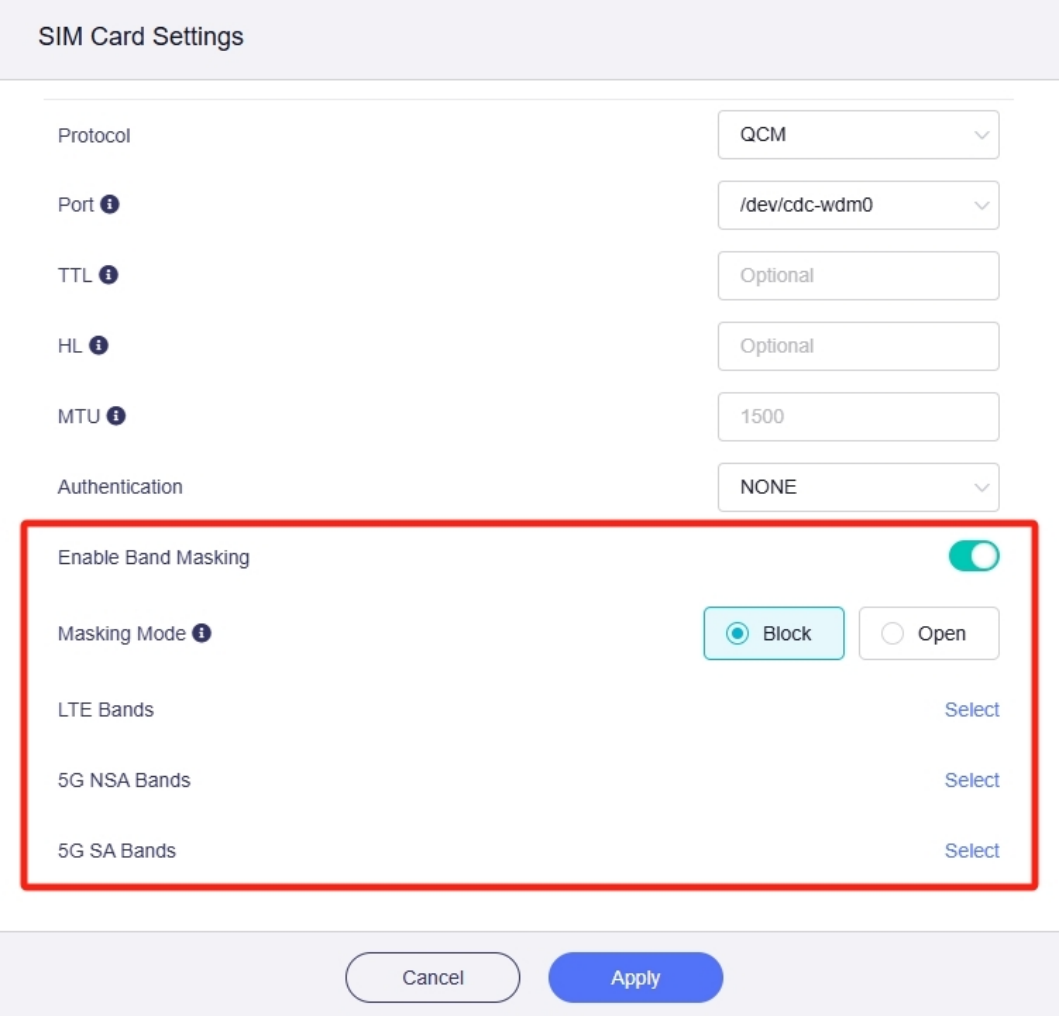
Consultez l’historique de l’intensité du signal en sélectionnant une période dans l’angle supérieur droit.



4.2.4.6 Masquage des bandes

Le masquage des bandes permet de bloquer certaines bandes ou d'utiliser uniquement les bandes cellulaires souhaitées pour améliorer un signal faible.

Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)** > **Paramètres de la carte SIM (SIM Card Settings)**, puis activez **Activer le masquage des bandes (Enable Band Masking)**.



Sélectionnez le **Mode de masquage (Masking Mode)**, Blocage (Block) ou Autorisation (Open), puis choisissez les bandes LTE, 5G NSA et 5G SA.

4.2.4.7 SMS et transfert de SMS

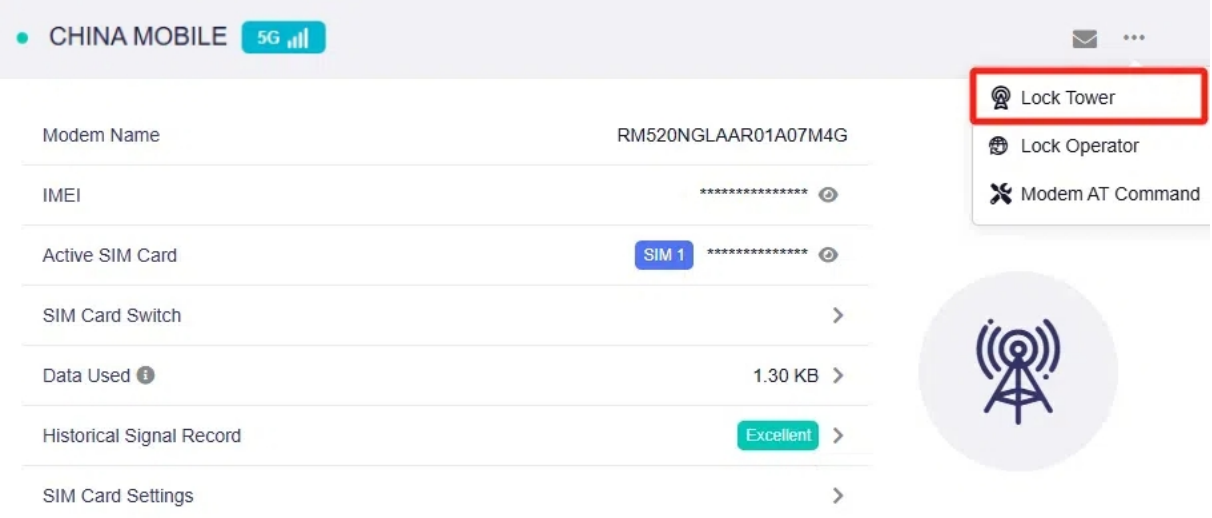
Consultez les sections SMS et Transfert de SMS.

4.2.4.8 Verrouillage d’une station de base

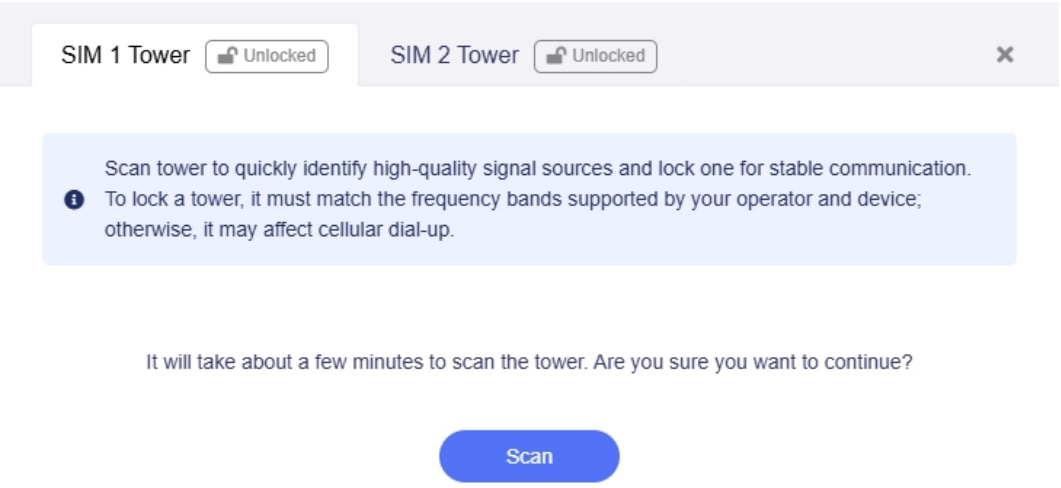
Pour obtenir un signal de qualité et une connexion cellulaire stable, vous pouvez essayer de verrouiller la connexion sur une station de base.

Remarque : la station verrouillée doit utiliser des bandes de fréquences prises en charge par votre opérateur et votre appareil ; sinon, la connexion risque d’échouer.

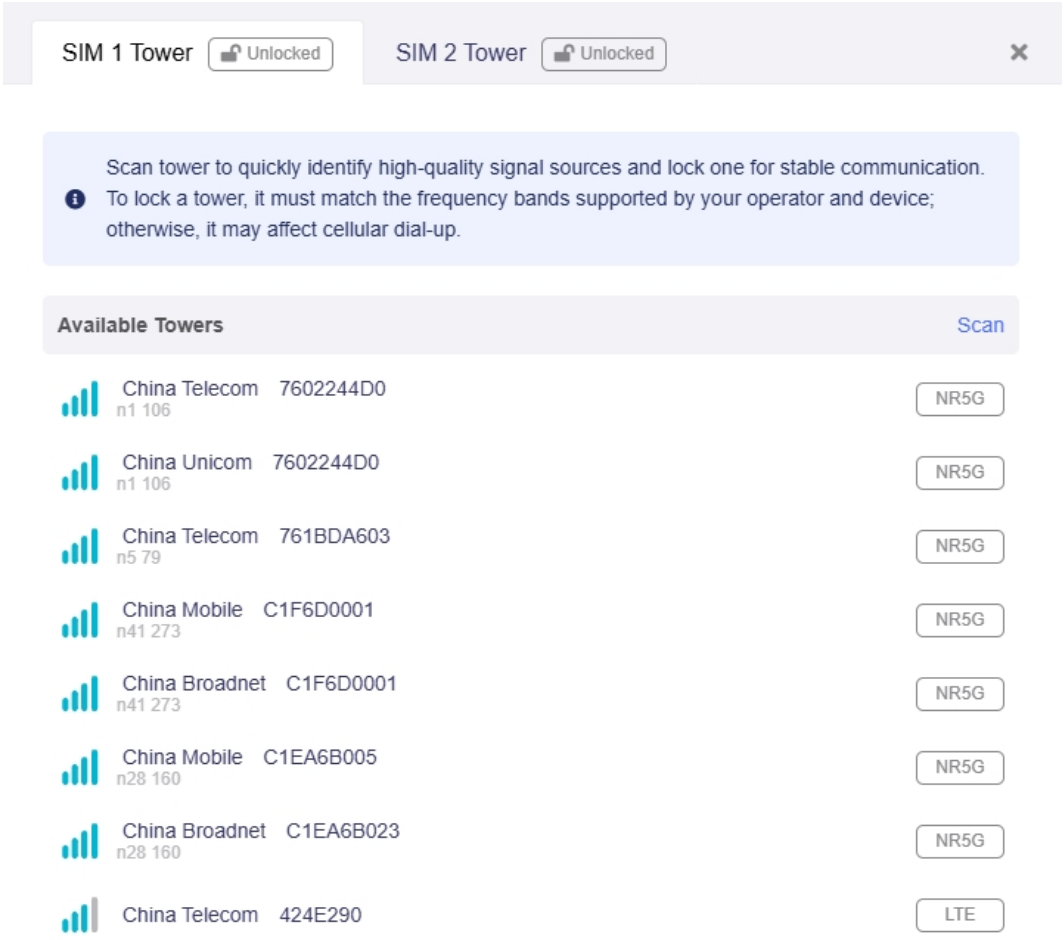
Dans l’interface d’administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**. Cliquez sur les trois points dans l’angle supérieur droit, puis sélectionnez **Verrouiller une station de base (Lock Tower)**.



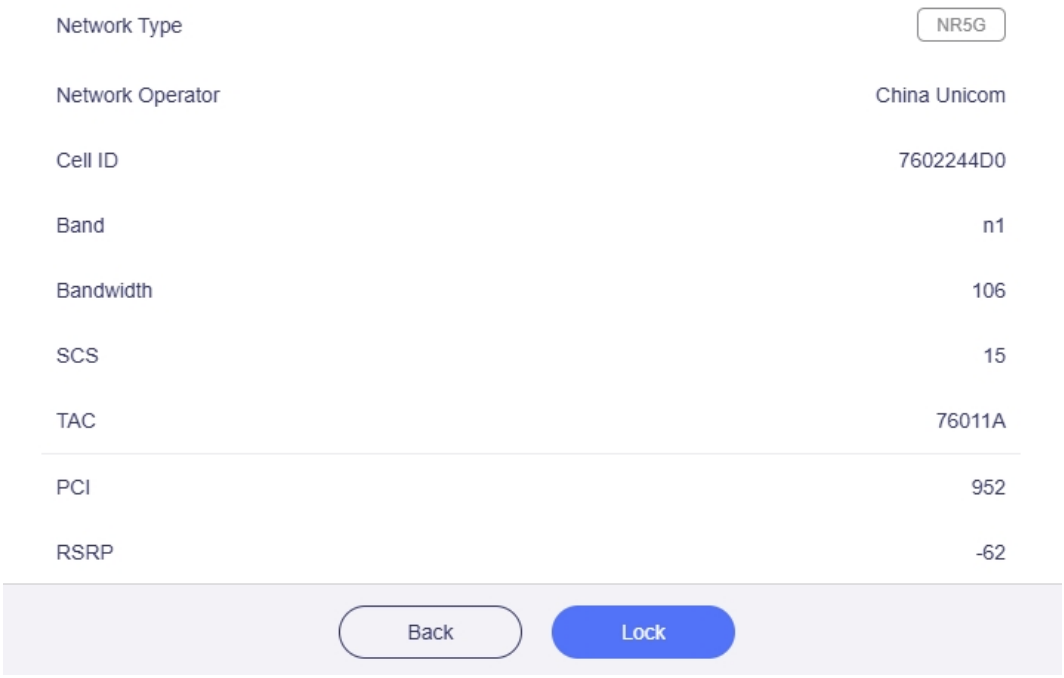
Cliquez sur **Rechercher (Scan)** pour rechercher les stations de base cellulaires. L’opération prend quelques minutes. N’actualisez pas la page pendant la recherche.



Les stations disponibles s’affichent.



Cliquez sur une station pour consulter ses détails et verrouiller la connexion sur celle-ci.



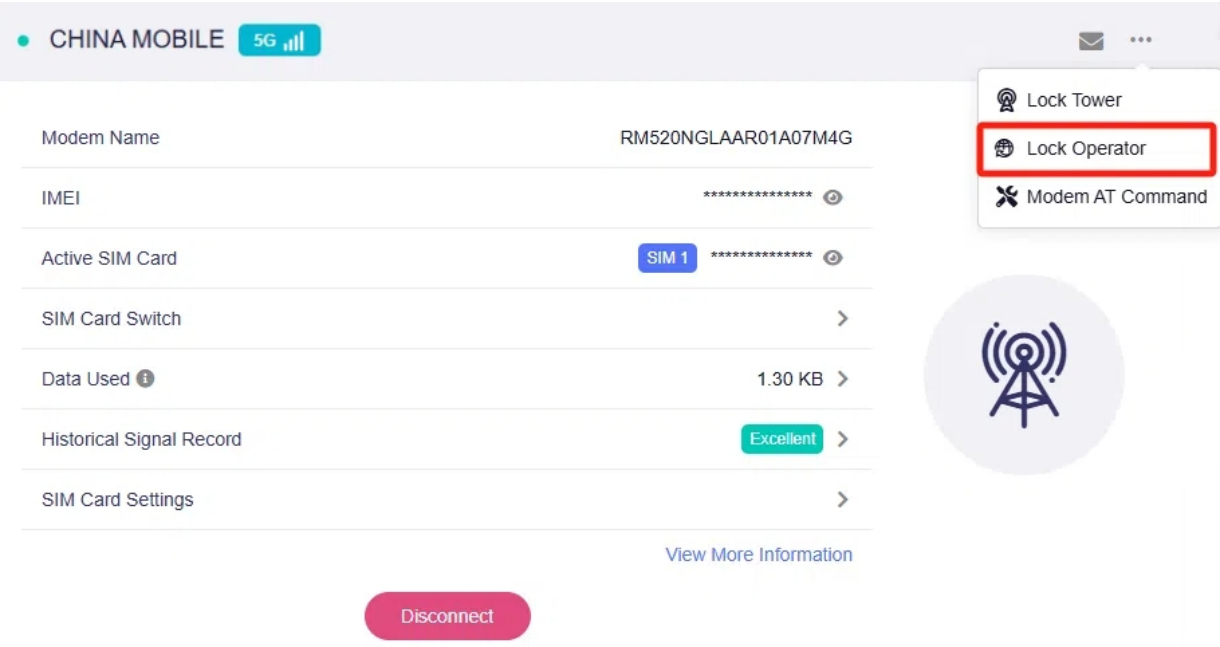
Remarque :

1. L’appareil peut ne pas détecter toutes les stations lorsque l’interface cellulaire est activée.
2. Si la station verrouillée ne correspond pas aux paramètres de masquage des bandes ou d’APN, le routeur ne peut pas se connecter au réseau cellulaire.
3. Après le verrouillage d’une station de base, le routeur tente encore de s’y reconnecter après un redémarrage, même si vous l’avez déplacé. Cela peut empêcher la connexion automatique au réseau cellulaire au nouvel emplacement. Dans ce cas, déverrouillez la station actuelle ou verrouillez manuellement la connexion sur une autre station.

4.2.4.9 Verrouillage de l’opérateur

En verrouillant un opérateur mobile, le routeur utilise uniquement son réseau. Cela assure une connexion stable et évite des frais d’itinérance imprévus, notamment dans les zones frontalières où l’appareil pourrait se connecter à un réseau étranger.

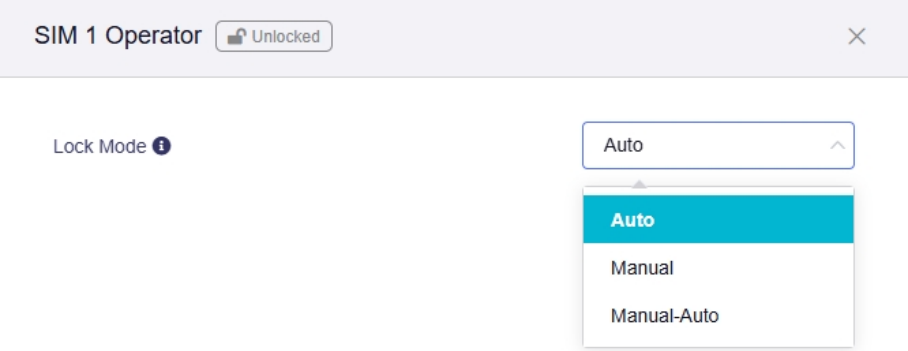
Dans l’interface d’administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**. Cliquez sur les trois points dans l’angle supérieur droit, puis sélectionnez **Verrouiller l’opérateur (Lock Operator)**.



Trois modes sont disponibles :

- **Automatique (Auto)** : se connecte automatiquement au réseau d’un opérateur disponible.
- **Manuel (Manual)** : verrouille manuellement la connexion sur un opérateur précis.

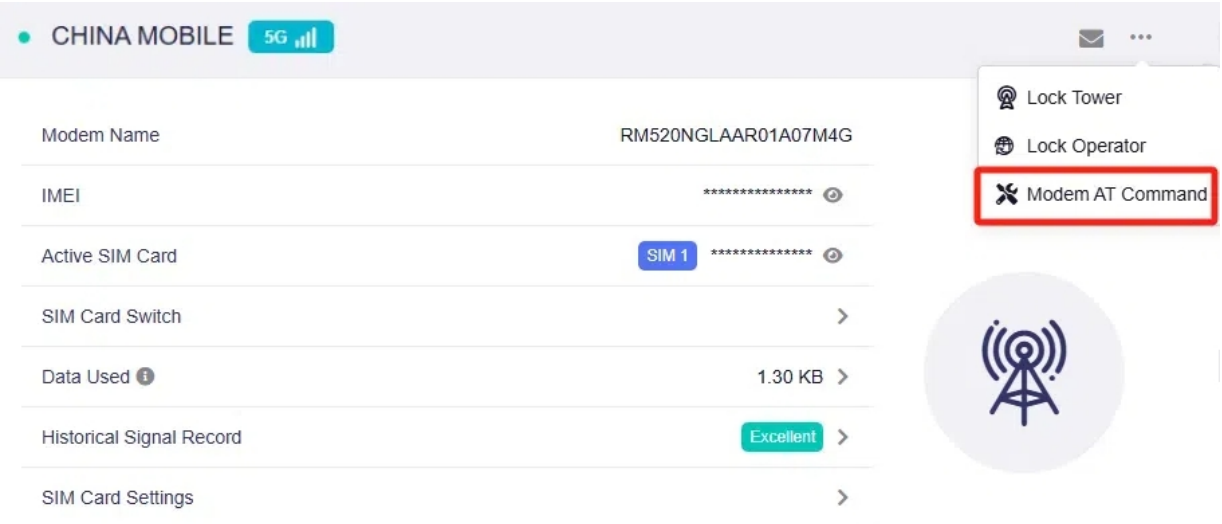
- **Manuel-Automatique (Manual-Auto)** : passe automatiquement au réseau d'un opérateur disponible si le verrouillage manuel échoue.



4.2.4.10 Commandes AT du modem

Les commandes AT sont des instructions standard permettant de communiquer avec le modem cellulaire. Cette fonction permet d'envoyer des commandes et de vérifier l'état du modem.

Dans l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Cellulaire (Cellular)**. Cliquez sur les trois points dans l'angle supérieur droit, puis sélectionnez **Commandes AT du modem (Modem AT Command)**.



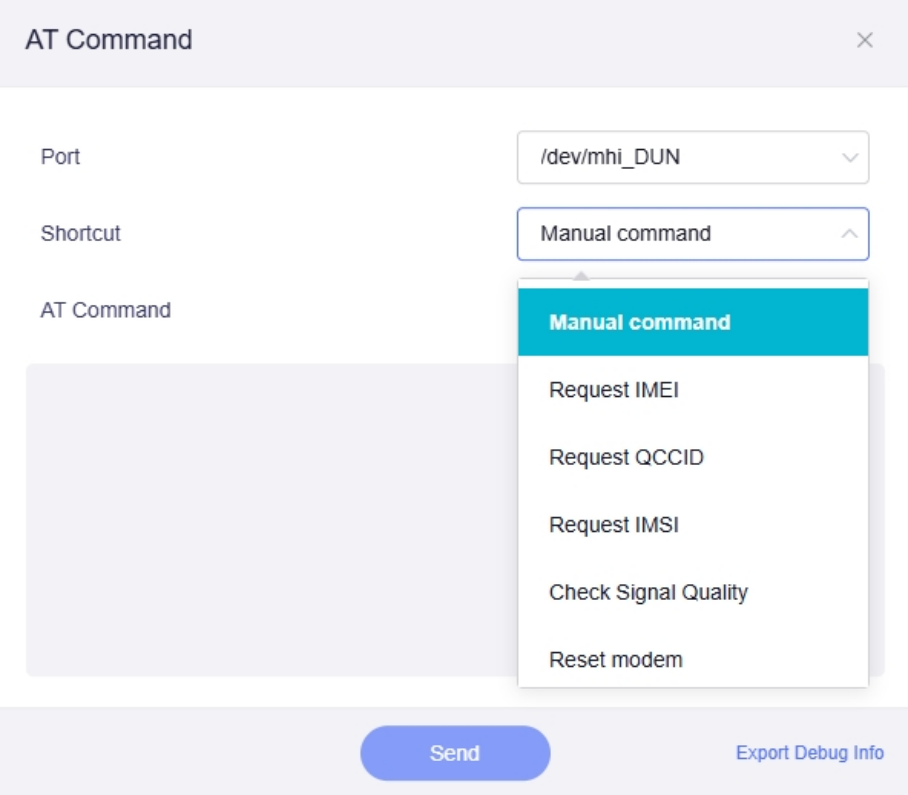
La page des commandes AT s'ouvre.

- **Commande manuelle**

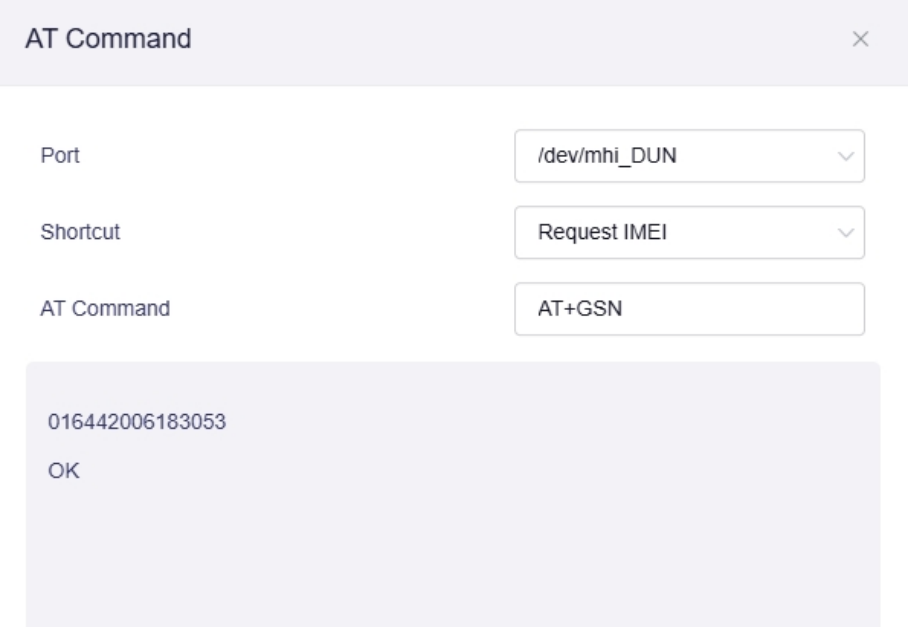
  Lorsque Raccourci (Shortcut) est défini sur Commande manuelle (Manual command), saisissez la commande souhaitée dans le champ Commande AT (AT Command). Le résultat s'affiche dans la zone grise en bas de la page.

- **Commande prédéfinie**

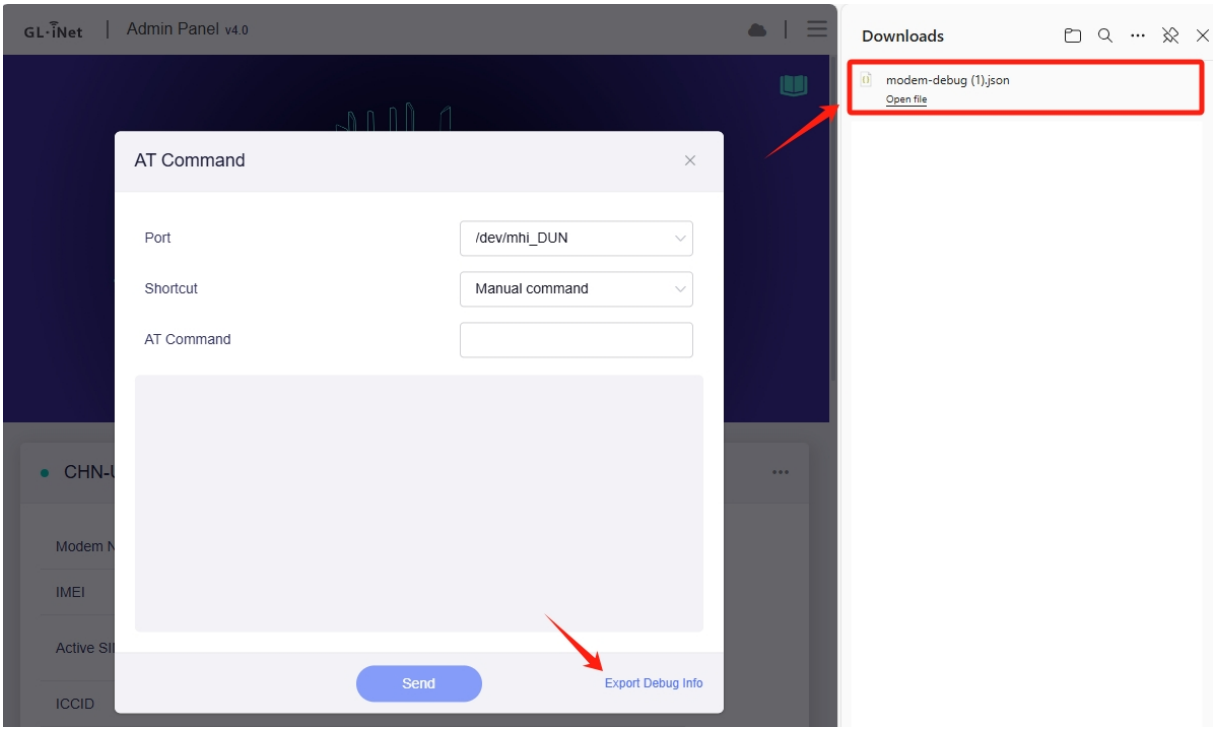
  Vous pouvez aussi ouvrir la liste Raccourci (Shortcut) et sélectionner une commande prédéfinie, comme Demander l'IMEI (Request IMEI), Vérifier la qualité du signal (Check Signal Quality) ou Réinitialiser le modem (Reset Modem).



Par exemple, sélectionnez le raccourci « Demander l'IMEI » (Request IMEI) et cliquez sur « Envoyer » (Send). Le résultat s'affiche comme ci-dessous.



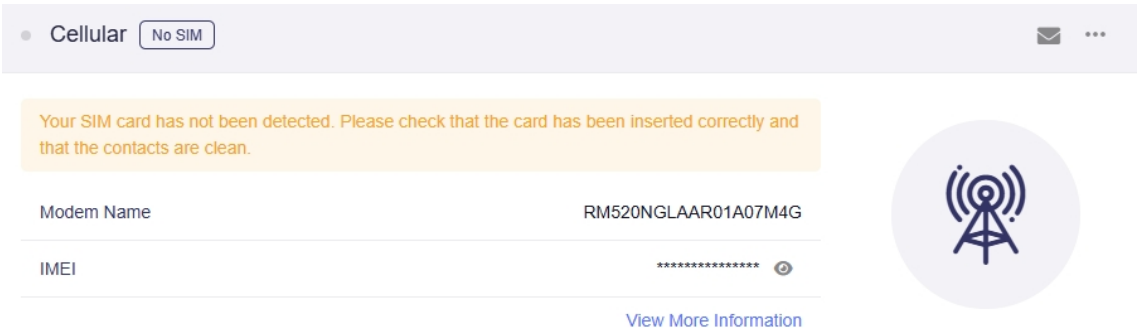
Dans l'angle inférieur droit, cliquez sur **Exporter les informations de débogage (Export Debug Info)** pour télécharger un fichier .json.



4.2.4.11 Dépannage

Si vous ne parvenez pas à établir une connexion cellulaire, choisissez la solution correspondant au message d'erreur affiché.

- **Aucune SIM / Votre carte SIM n’a pas été détectée (No SIM / Your SIM card has not been detected).**



Voici quelques mesures à essayer.

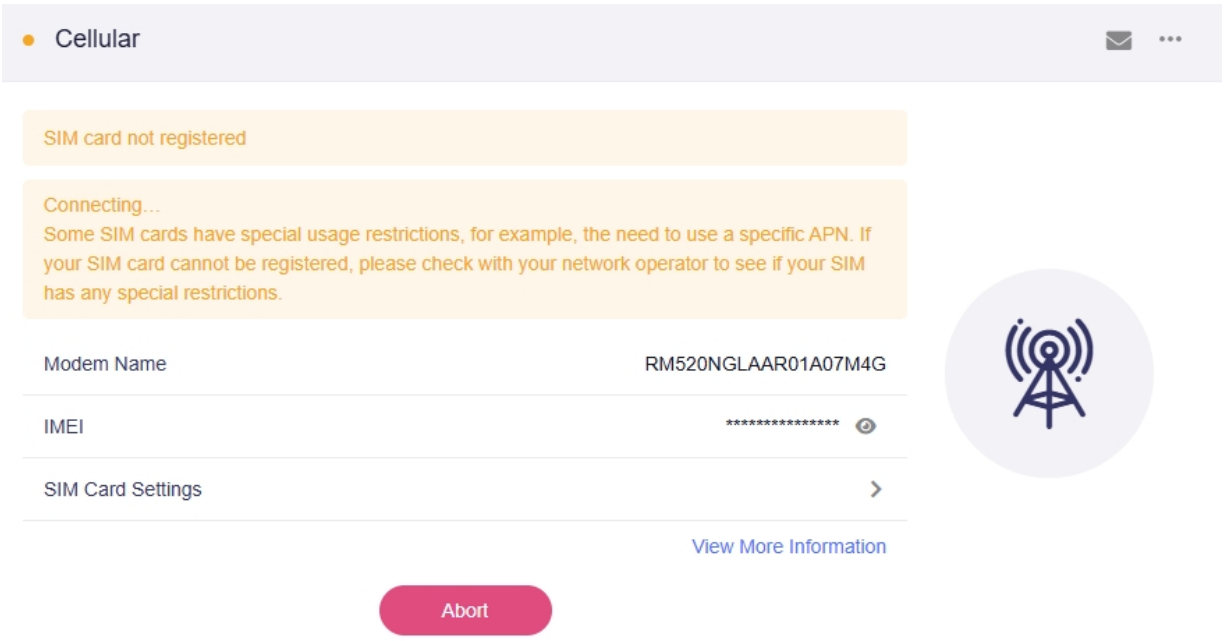
1. Actualisez la page et attendez quelques minutes pour vérifier si la carte SIM est détectée.
2. Vérifiez que la carte SIM est correctement insérée. Alignez son encoche sur le repère correspondant de l’emplacement pour respecter le sens d’insertion.
3. Éteignez le routeur, retirez puis réinsérez la carte SIM, et rallumez le routeur.
4. Essayez une autre carte SIM si vous en avez une.

Si le problème persiste, téléchargez les journaux et envoyez-les à support@gl-inet.com.

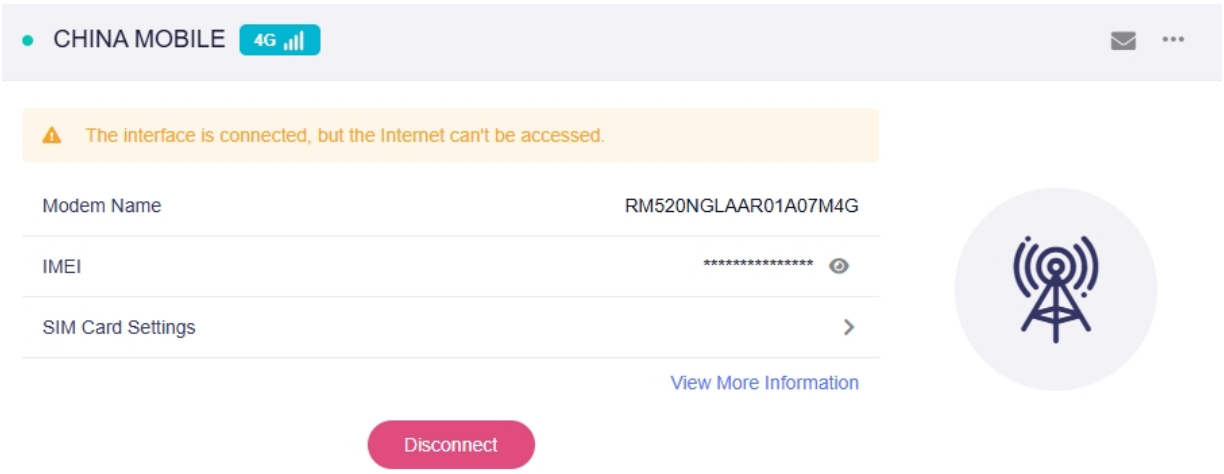
- **Carte SIM non enregistrée / L’interface est connectée, mais l’accès à Internet est impossible (SIM card not registered / The interface is connected, but the Internet can’t be accessed).**

Deux messages d’erreur peuvent signaler ce problème :

(1) Carte SIM non enregistrée (SIM card not registered).



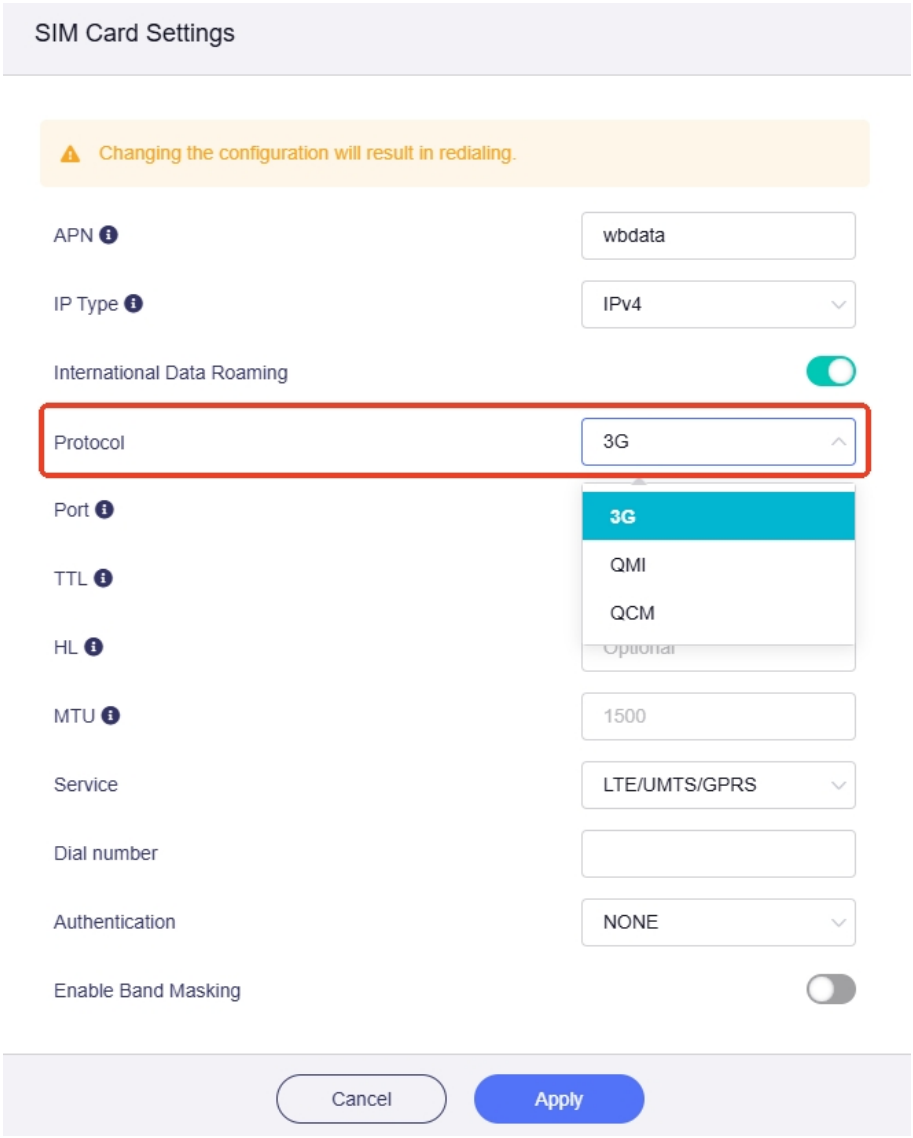
(2) L'interface est connectée, mais l'accès à Internet est impossible (The interface is connected, but the Internet can't be accessed).



Voici quelques mesures à essayer.

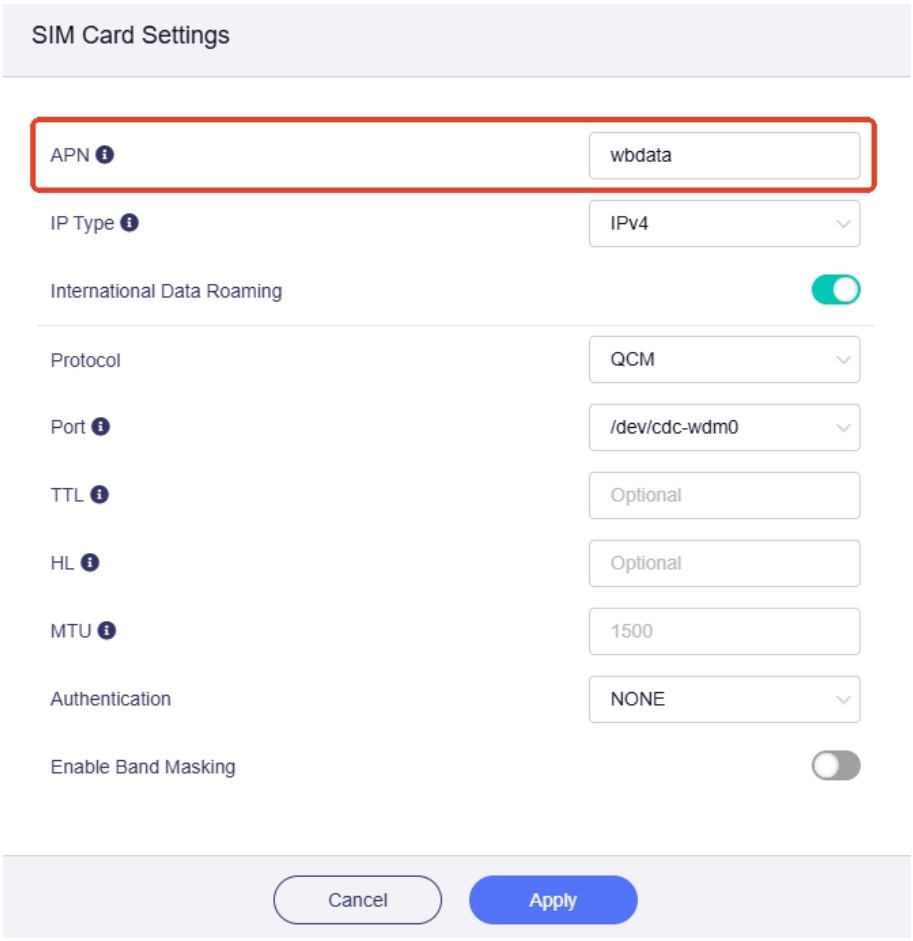
1. Actualisez la page et attendez quelques minutes pour vérifier si l'erreur disparaît.
2. Cliquez sur **Déconnecter (Disconnect)/Abandonner (Abort)**, puis sur **Connecter (Connect)** pour tenter une reconnexion.
3. Redémarrez le routeur.
4. Vérifiez que la carte SIM est active. Insérez-la dans un smartphone et assurez-vous qu'elle dispose d'un forfait de données actif et qu'elle permet un accès normal à Internet, ou contactez votre opérateur pour le vérifier.

5. Certains opérateurs peuvent exiger le protocole 3G pour la connexion réseau. Ouvrez **Paramètres de la carte SIM (SIM Card Settings)** > **Protocole (Protocol)**, sélectionnez **3G**, puis cliquez sur **Appliquer (Apply)**.



L'appareil se reconnecte automatiquement. Attendez quelques minutes pour vérifier si la connexion est établie.

6. Certaines cartes SIM sont soumises à des restrictions particulières, par exemple l'utilisation d'un APN précis. Si votre carte SIM ne parvient pas à s'enregistrer sur le réseau, contactez l'opérateur pour vérifier ces restrictions. Si nécessaire, ouvrez **Paramètres de la carte SIM (SIM Card Settings)** > **APN**, définissez l'APN correct, puis cliquez sur **Appliquer (Apply)**.



7. Cliquez sur **Afficher plus d'informations (View More Information)** pour vérifier l'intensité du signal cellulaire. Si le signal est faible, assurez-vous que l'antenne est correctement installée. Placez le routeur dans un endroit dégagé pour améliorer la réception.
8. Vérifiez si **Masquage des bandes (Band Masking)** ou **Verrouiller une station de base (Lock Tower)** est activé. Si c'est le cas, désactivez ces fonctions et tentez une reconnexion.

Si le problème persiste, téléchargez les journaux et envoyez-les à support@gl-inet.com.

Chapitre 5

Réseau sans fil

Ce chapitre explique comment vérifier l’état du Wi-Fi et configurer les paramètres sans fil.

5.1 Affichage de l’état du Wi-Fi

Les réseaux Wi-Fi du routeur sont activés par défaut. L’icône Wi-Fi correspondante s’allume sous l’image de l’appareil sur la page INTERNET.



Lorsque vous placez le pointeur sur l’icône d’un réseau Wi-Fi activé, un code QR s’affiche comme ci-dessous. Scannez-le pour vous connecter rapidement au réseau correspondant.



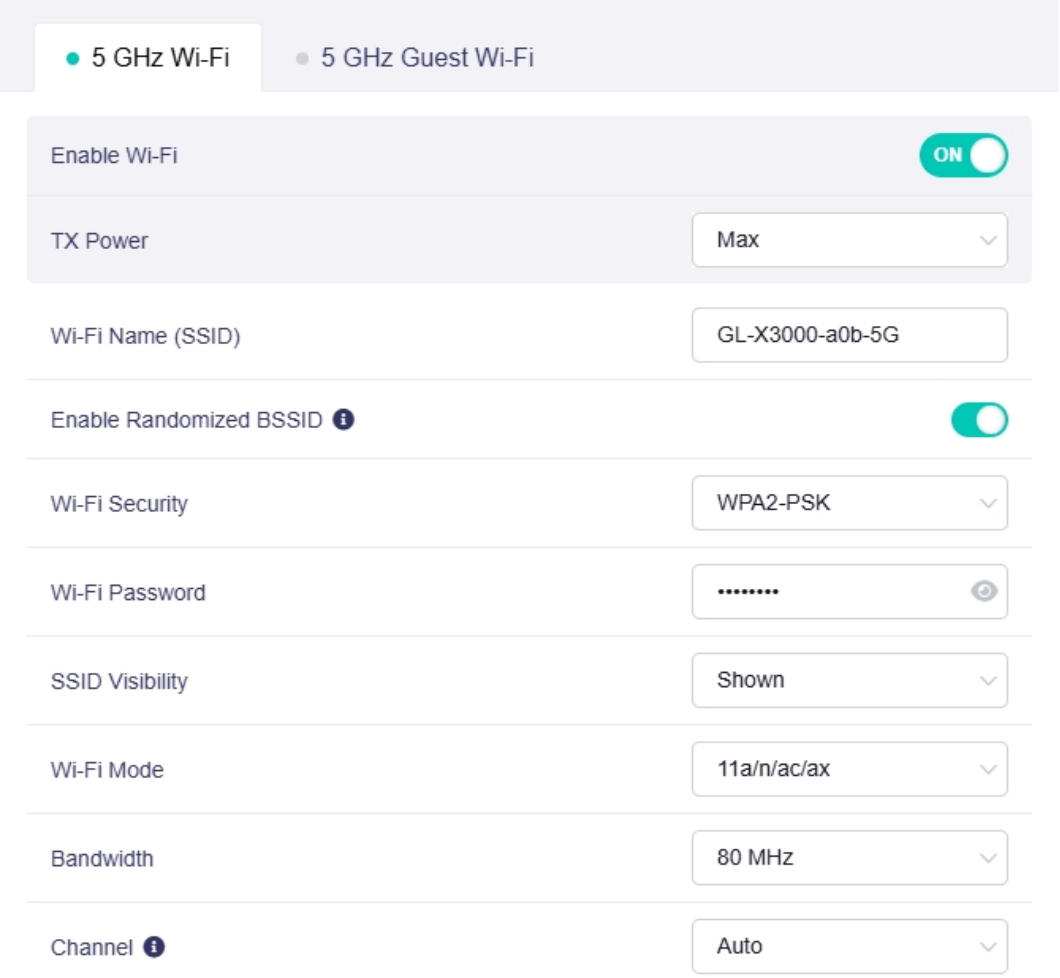
5.2 Paramètres sans fil

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU SANS FIL (WIRELESS)**.

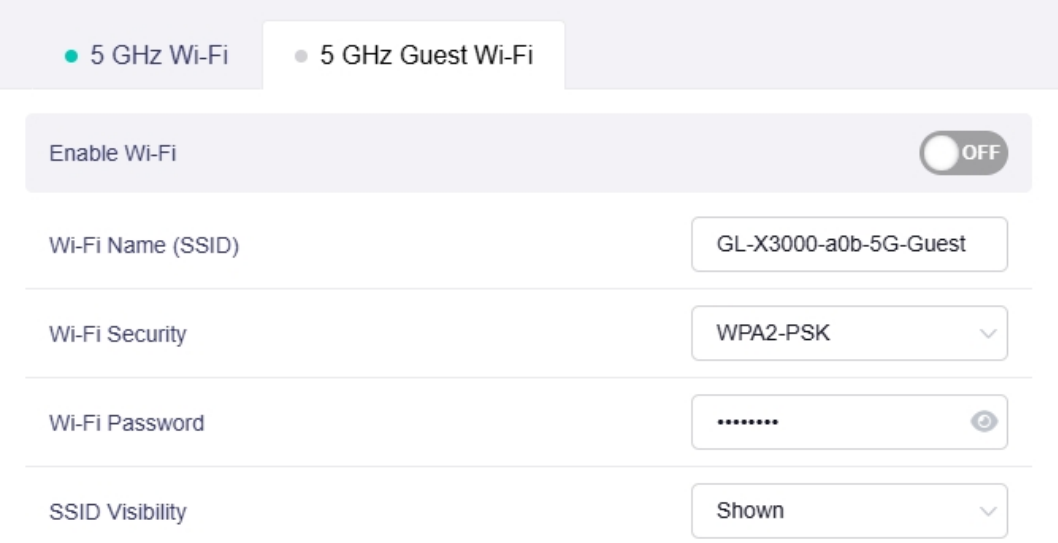
La page Sans fil affiche les paramètres Wi-Fi 2,4 GHz et 5 GHz du routeur. Chaque bande comprend un réseau principal et un réseau invité, que vous pouvez gérer séparément.

5.2.1 Wi-Fi 5 GHz

Pour le Wi-Fi principal 5 GHz, vous pouvez activer ou désactiver le réseau, définir la puissance d'émission, activer ou désactiver le BSSID aléatoire et régler le nom du réseau (SSID), la sécurité, le mot de passe, la visibilité du SSID, le mode, la largeur de bande et le canal.



Le Wi-Fi invité 5 GHz propose des paramètres simplifiés : activation ou désactivation du réseau, nom du réseau (SSID), sécurité, mot de passe et visibilité du SSID.

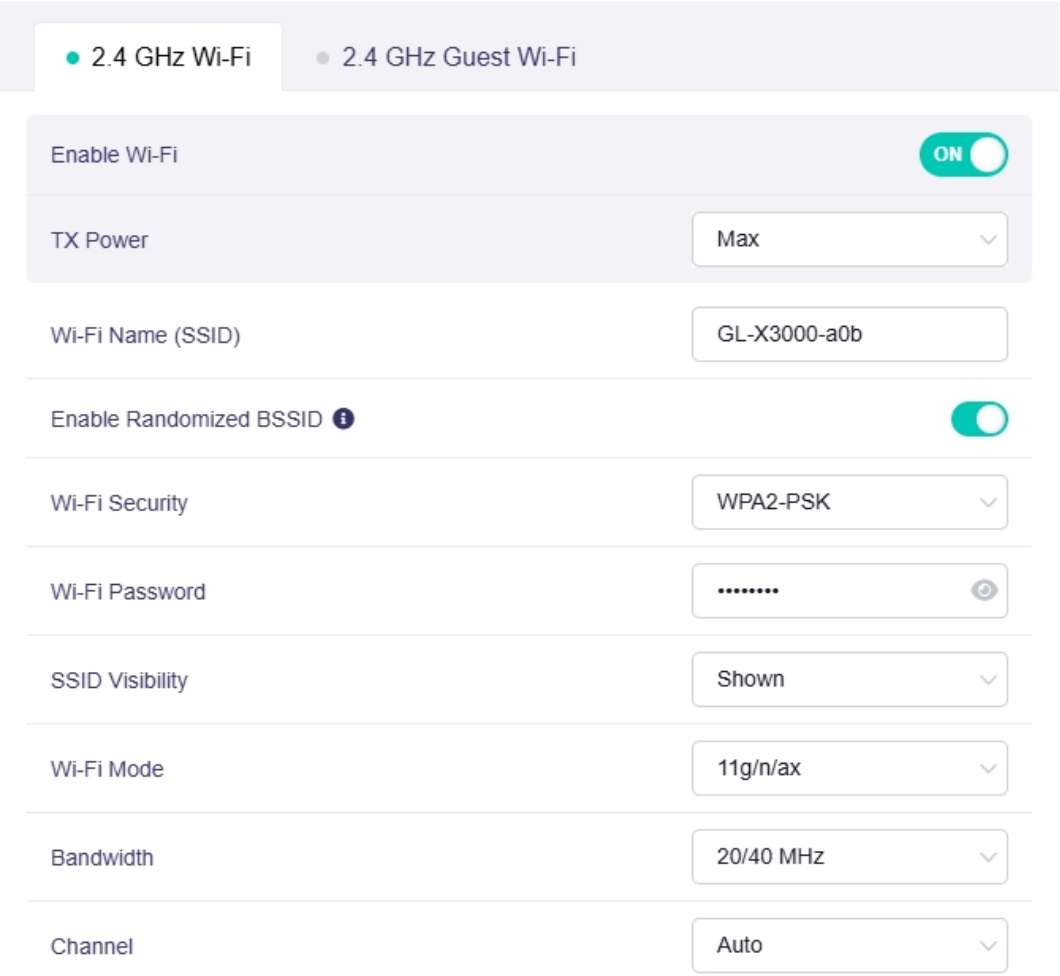


Remarque :

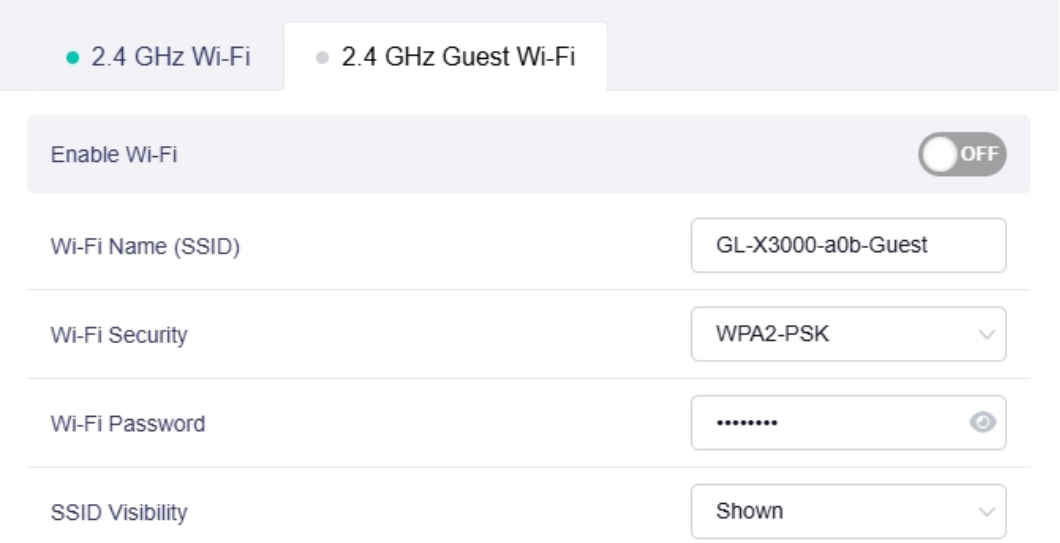
1. **Le BSSID aléatoire (Randomized BSSID)** est activé par défaut. Il vise à empêcher les fabricants d'appareils clients de collecter sur leurs serveurs les BSSID des réseaux Wi-Fi voisins et les coordonnées GPS des appareils clients.
2. Les paramètres **Largeur de canal (Bandwidth)** et **Canal (Channel)** ne peuvent pas être modifiés lorsque le routeur fonctionne en mode répéteur : ils suivent ceux du réseau auquel il se connecte.
3. Lorsque **Canal (Channel)** est réglé sur **Auto**, le Wi-Fi du routeur ne bascule pas automatiquement sur un canal DFS.
4. Lorsque la **Largeur de canal (Bandwidth)** est réglée sur **160 MHz** (uniquement sur certains modèles), le Wi-Fi utilise toujours un canal DFS, même si vous sélectionnez un canal non DFS ou le réglage Auto.

5.2.2 Wi-Fi 2,4 GHz

Pour le Wi-Fi principal 2,4 GHz, vous pouvez activer ou désactiver le réseau, définir la puissance d'émission, activer ou désactiver le BSSID aléatoire et régler le nom du réseau (SSID), la sécurité, le mot de passe, la visibilité du SSID, le mode, la largeur de bande et le canal.



Le Wi-Fi invité 2,4 GHz propose des paramètres simplifiés : activation ou désactivation du réseau, nom du réseau (SSID), sécurité, mot de passe et visibilité du SSID.



Remarque :

1. **Le BSSID aléatoire (Randomized BSSID)** est activé par défaut. Il vise à empêcher les fabricants d'appareils clients de collecter sur leurs serveurs les BSSID des réseaux Wi-Fi voisins et les coordonnées GPS des appareils clients.
2. Les paramètres **Largeur de canal (Bandwidth)** et **Canal (Channel)** ne peuvent pas être modifiés lorsque le routeur fonctionne en mode répéteur : ils suivent ceux du réseau auquel il se connecte.
3. Lorsque **Canal (Channel)** est réglé sur **Auto**, le Wi-Fi du routeur ne bascule pas automatiquement sur un canal DFS.

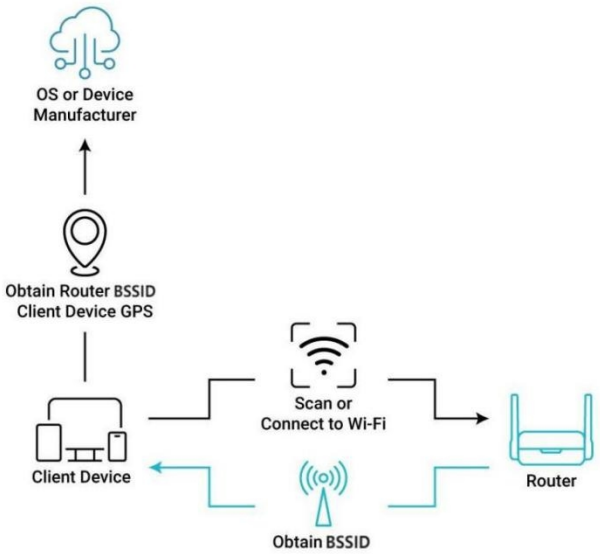
5.2.3 BSSID aléatoire

Le BSSID aléatoire vise à empêcher les fabricants d'appareils clients de collecter sur leurs serveurs les BSSID des réseaux Wi-Fi voisins et les coordonnées GPS des appareils clients.

Comment les fabricants collectent les données de localisation

Les fabricants d'appareils clients collectent généralement la position géographique des points d'accès Wi-Fi en utilisant leurs BSSID uniques pour localiser les appareils. Lorsqu'un appareil client, comme un téléphone ou un ordinateur, recherche un réseau ou se connecte à un routeur :

- Les autres appareils situés dans la zone de couverture Wi-Fi du routeur peuvent voir leur position et leurs déplacements révélés.
- Si un appareil utilise le GPS pour se localiser, il transmet régulièrement au serveur du fabricant les BSSID Wi-Fi voisins et les coordonnées GPS correspondantes.



Risques liés au suivi par localisation collaborative

Même les appareils sans GPS, ou dont le GPS est désactivé, peuvent estimer leur position à partir des BSSID visibles. Ce système collaboratif de localisation présente toutefois des vulnérabilités. Des attaquants peuvent l'utiliser pour constituer une base mondiale des positions des points d'accès Wi-Fi et suivre les déplacements des appareils en continu, au détriment de la vie privée et de la sécurité des utilisateurs.

Comment le BSSID aléatoire protège votre vie privée

Pour limiter ces vulnérabilités, les routeurs GL.iNet intègrent une fonction de BSSID aléatoire destinée à protéger votre vie privée.

Dans l'interface Web, ouvrez **SANS FIL (WIRELESS)** > **Wi-Fi 5 GHz (5GHz Wi-Fi)** ou **Wi-Fi 2,4 GHz (2.4GHz Wi-Fi)**. L'option BSSID aléatoire est activée par défaut : l'appareil génère un BSSID aléatoire et le renouvelle à chaque démarrage. Si vous la désactivez, le routeur utilise de nouveau sa véritable adresse MAC.

Remarque : sur une même bande de fréquences, le BSSID du réseau invité reste cohérent avec celui du réseau principal.

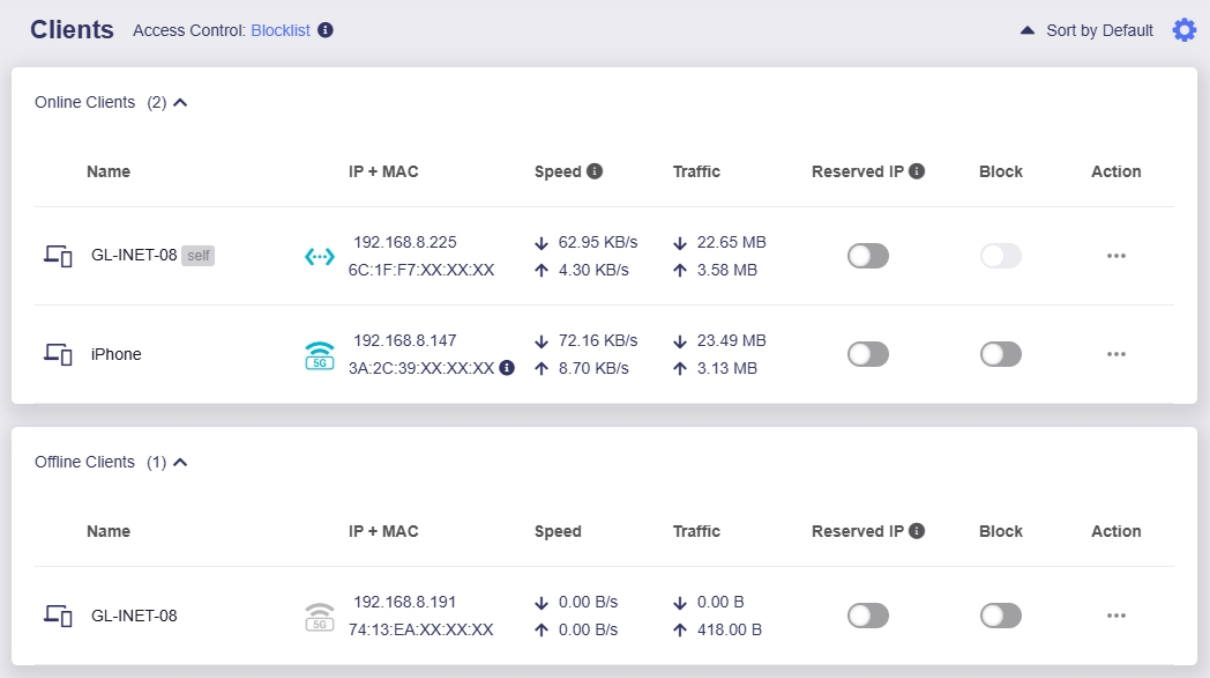
Chapitre 6

Appareils clients

Ce chapitre explique comment consulter les informations des appareils connectés et gérer leurs connexions.

6.1 Informations sur les appareils

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **CLIENTS**.
La page Clients affiche, de gauche à droite, le nom des appareils connectés, leur type de connexion, leurs adresses IP et MAC, leur débit et leur trafic. Elle permet également de réserver une adresse IP, de bloquer un client ou d'effectuer d'autres actions rapidement.



Conseil : les clients en ligne (Online Clients) sont les appareils actuellement connectés au réseau du routeur. Les clients hors ligne (Offline Clients) sont les appareils qui s'y sont déjà connectés, mais qui sont désormais déconnectés.

1. **Nom de l'appareil**
   La première colonne affiche le nom et le type de l'appareil, selon le nom d'hôte fourni par celui-ci. L'icône bleue à côté du nom indique le mode de connexion : l'appareil est relié au routeur par un câble Ethernet.
2. **Adresses IP et MAC**
   La deuxième colonne affiche les adresses IP et MAC de l'appareil connecté. Si l'appareil utilise une adresse MAC aléatoire, un message le signale.



Une adresse MAC dont le deuxième caractère est 2, 6, A ou E, sans distinction de casse, est considérée comme aléatoire. Certains appareils utilisent toutefois une autre règle de génération : cette méthode de détection peut donc manquer de précision.

3. **Débit**

   La troisième colonne affiche le débit Internet de l'appareil connecté. Il s'agit du débit moyen des trois dernières minutes. Le calcul commence à l'ouverture de cette page : si elle n'est ouverte que depuis 10 secondes, la moyenne porte uniquement sur ces 10 secondes.

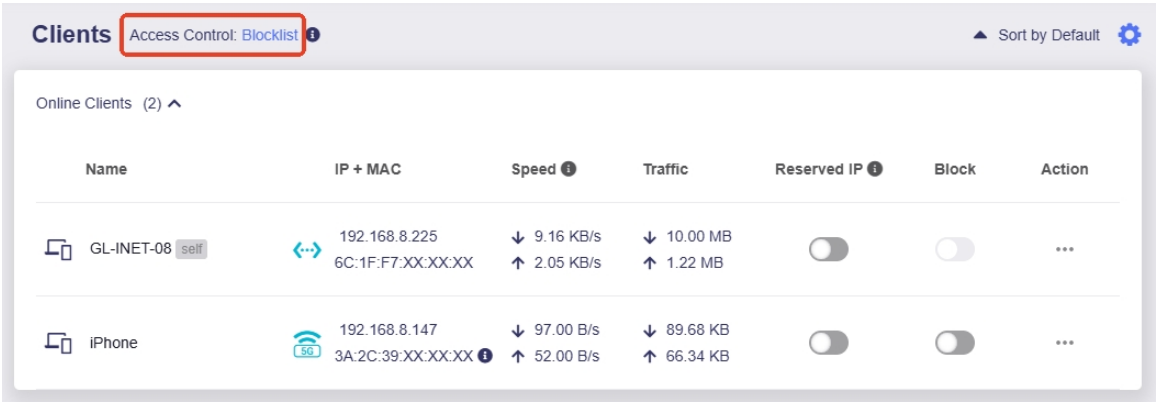
4. **Trafic** : la quatrième colonne affiche le trafic Internet de l'appareil connecté.

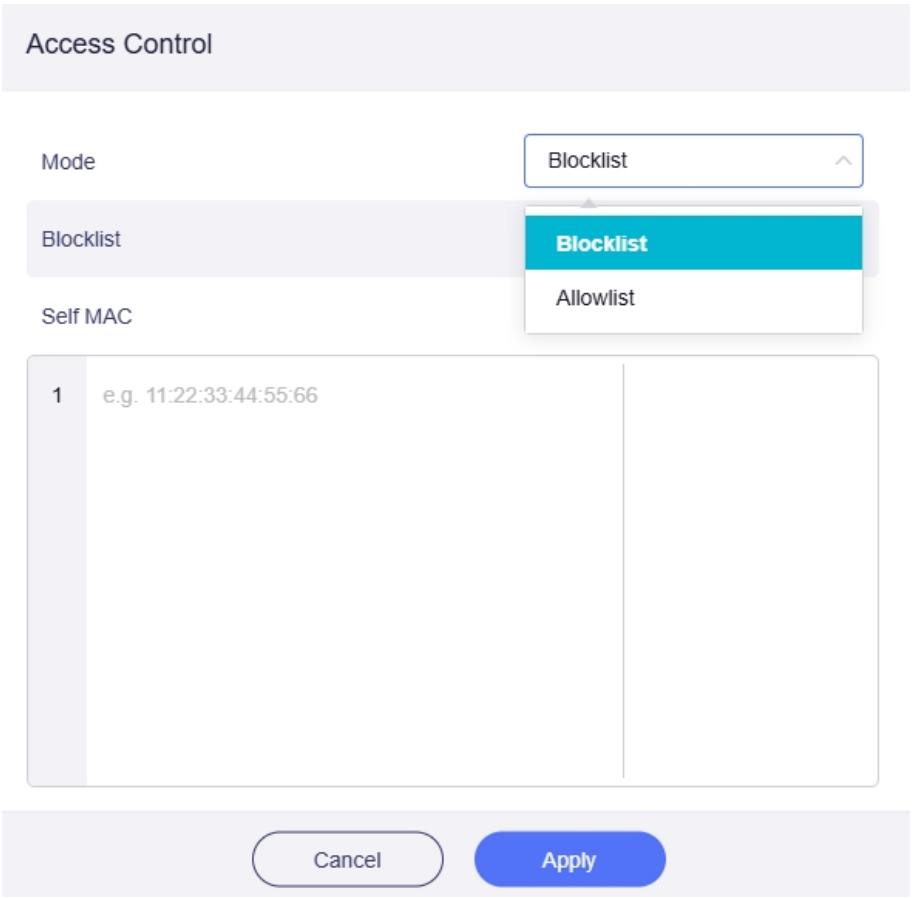
5. **Réserver une adresse IP**

   La cinquième colonne permet de réserver en un clic une adresse IP pour l'appareil connecté. Lorsqu'une adresse est réservée pour un client du réseau local, celui-ci reçoit toujours la même adresse IP à chaque connexion au routeur.

6. **Liste de blocage**

   La sixième colonne permet de bloquer certains appareils connectés en un clic.
   Par défaut, la règle de contrôle d'accès utilise une liste de blocage. Vous pouvez choisir une liste d'autorisation en haut de la page.



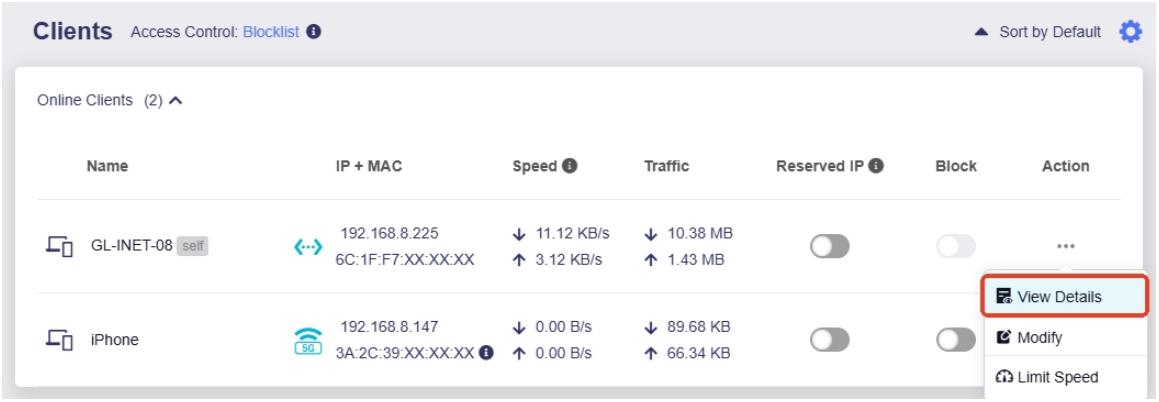


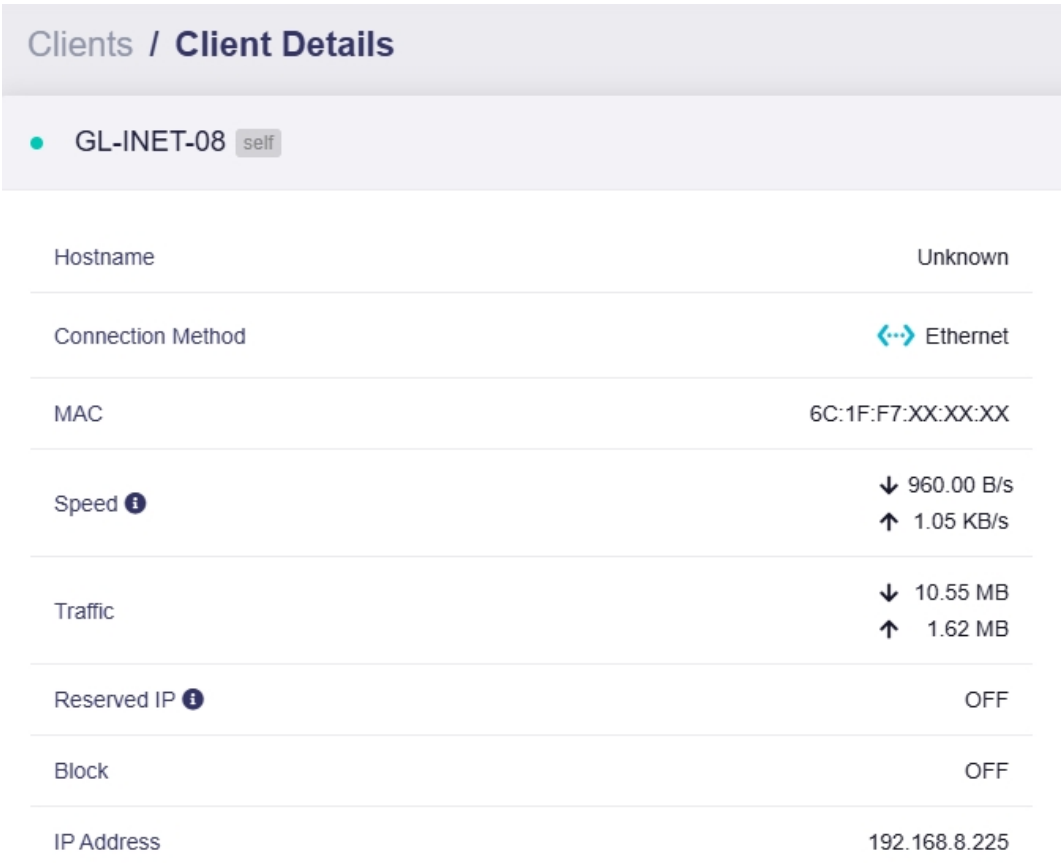
- **Liste de blocage (Blacklist)** : les appareils dont l'adresse MAC figure dans cette liste ne peuvent pas se connecter au routeur. Le blocage repose sur l'adresse MAC : un appareil bloqué peut donc se reconnecter s'il utilise une autre adresse MAC.
- **Liste d'autorisation (Allowlist)** : seuls les appareils possédant les adresses MAC indiquées peuvent se connecter au routeur. Ce mode convient aux appareils IoT et à la gestion des réseaux d'entreprise.

6.2 Actions

1. **Afficher les détails**

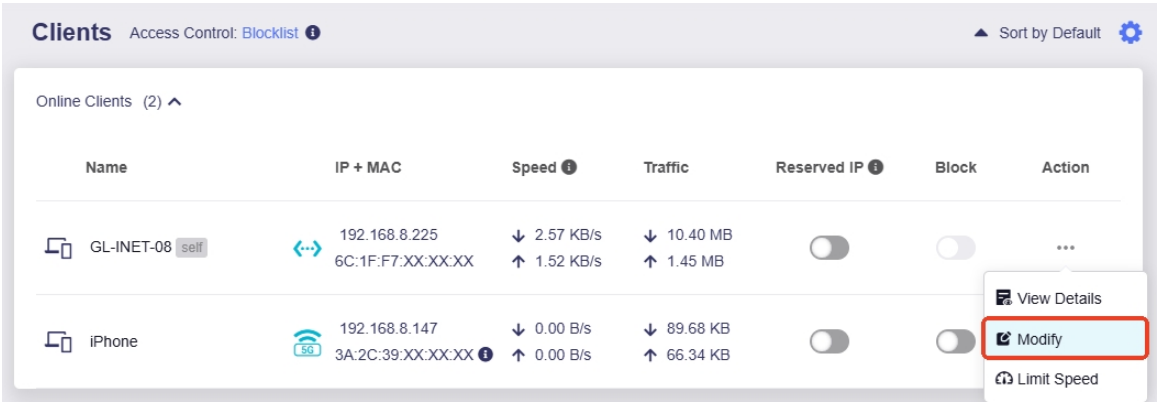
   Cliquez sur les trois points dans la colonne **Action**, puis sur **Afficher les détails (View Details)** dans le menu déroulant pour consulter les informations de l'appareil sur une seule page.

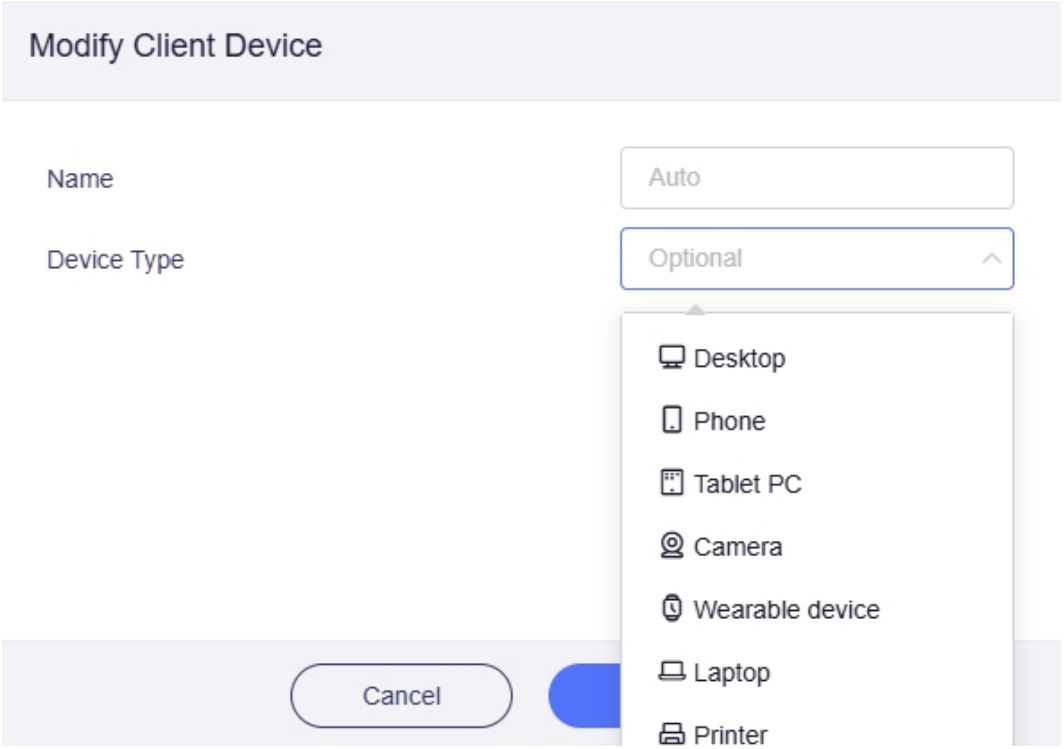




2. **Modifier**

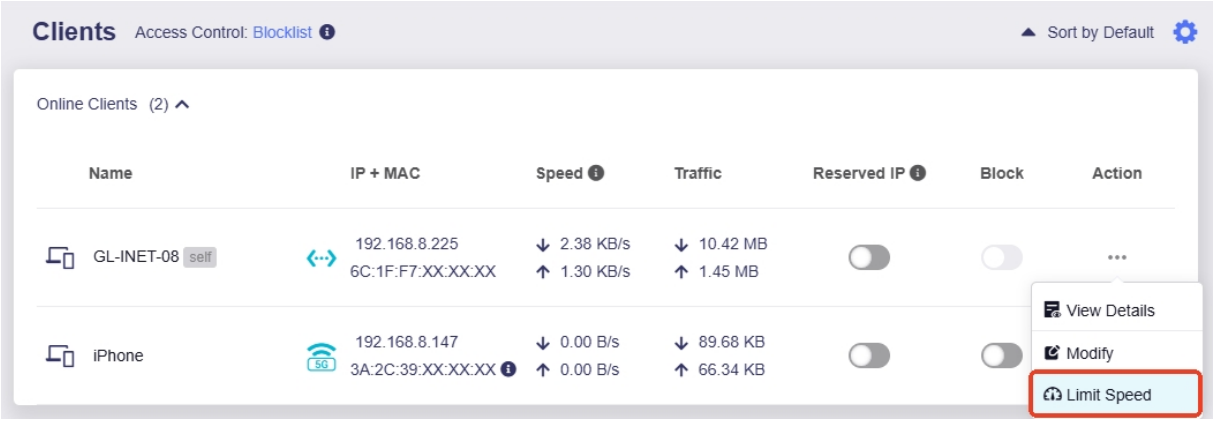
Cliquez sur les trois points dans la colonne **Action**, puis sur **Modifier (Modify)** dans le menu déroulant pour modifier le nom et le type de l'appareil.



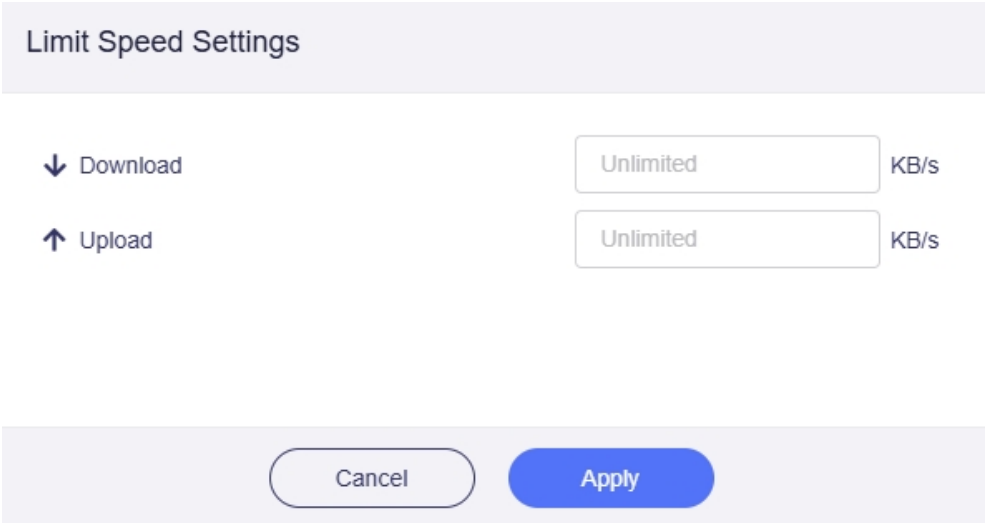


3. **Limiter le débit**

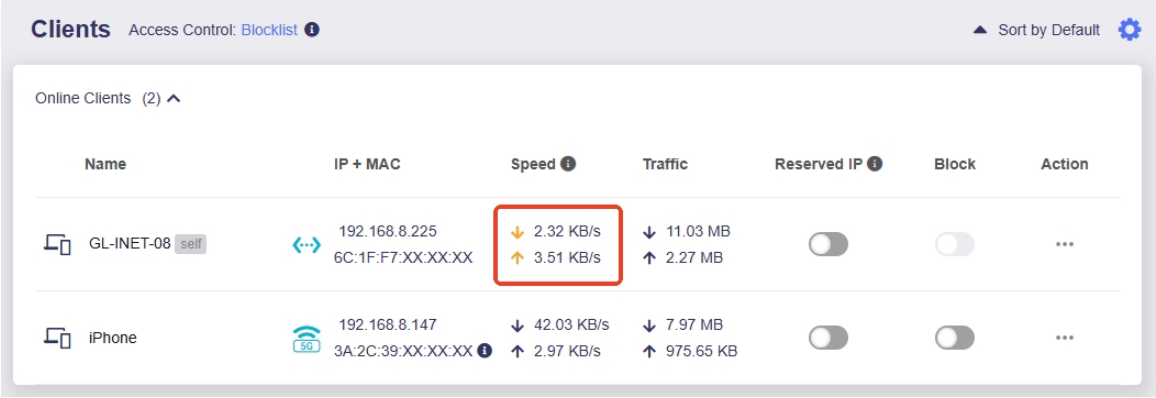
Cliquez sur les trois points dans la colonne **Action**, puis sur **Limiter le débit (Limit Speed)** dans le menu déroulant.



Vous pouvez limiter le débit d'un appareil connecté. L'unité utilisée est le Ko/s (KB/s).

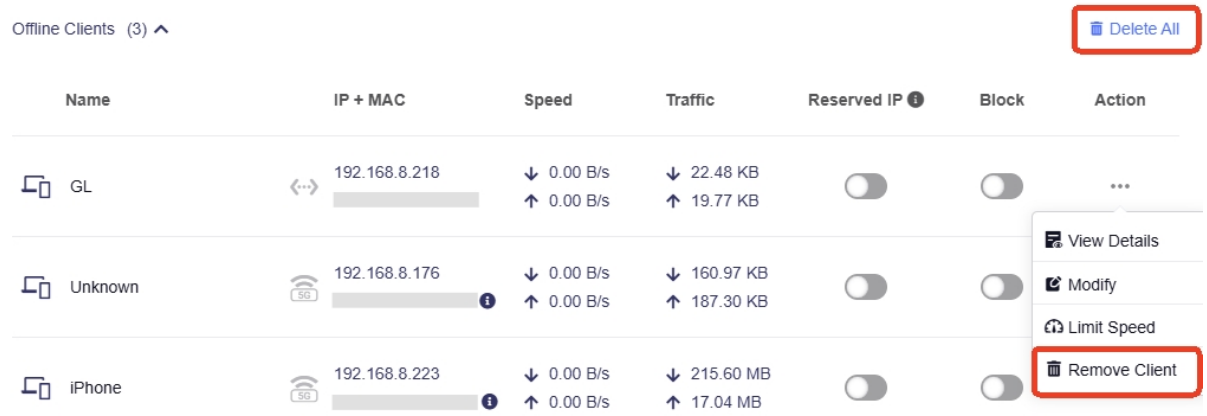


Lorsqu'une limite de débit est appliquée à un appareil, les flèches de débit montant et descendant deviennent jaunes.



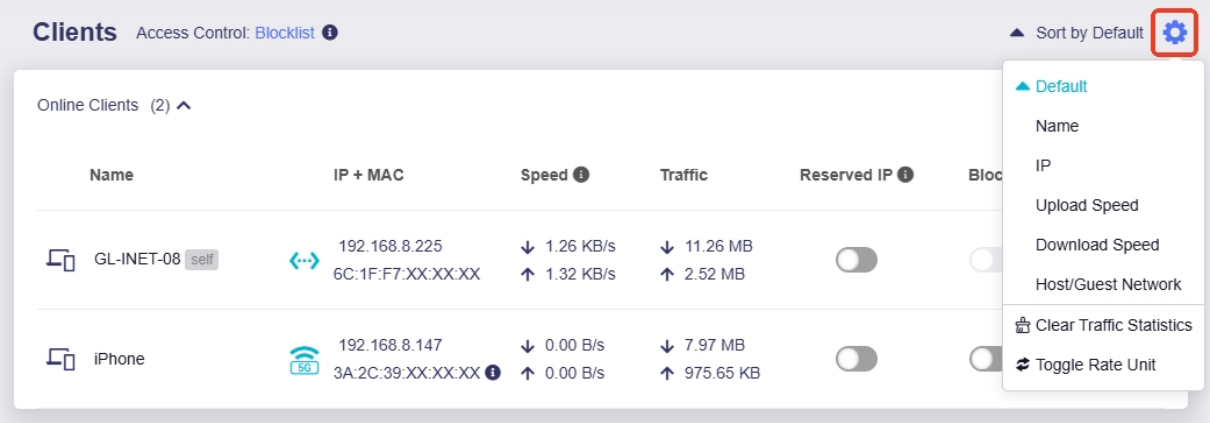
6.3 Suppression de clients

Dans la section **Clients hors ligne (Offline Clients)**, cliquez sur **Tout supprimer (Delete All)** dans l'angle supérieur droit pour supprimer tous les clients hors ligne. Pour supprimer un client précis, cliquez sur l'icône à trois points dans la colonne **Action**, puis sur **Supprimer le client (Remove Client)** dans le menu déroulant.



6.4 Tri

Vous pouvez définir la règle de tri des appareils en haut à droite de la page Clients.



Les règles de tri par défaut sont les suivantes.

- L'appareil utilisé pour accéder à l'interface d'administration Web du routeur apparaît toujours en premier.
- Dans la section **Clients en ligne (Online Clients)**, les appareils connectés depuis le plus longtemps apparaissent en premier.
- Dans la section **Clients hors ligne (Offline Clients)**, les appareils déconnectés depuis le plus longtemps apparaissent en premier.

Chapitre 7

Services cloud

Ce chapitre présente deux services cloud : GoodCloud et AstroWarp.

7.1 GoodCloud

GL.iNet GoodCloud simplifie le déploiement et la gestion à distance des appareils connectés. Cette plateforme permet d'accéder facilement aux routeurs GL.iNet et de les gérer à distance. En centralisant les appareils réseau dans le cloud, elle facilite les opérations groupées, comme le déploiement de configurations réseau et les mises à jour logicielles. Vous pouvez également accéder à l'interface d'administration Web ou au terminal du routeur via SSH pour gérer les appareils de bout en bout, quel que soit leur emplacement.

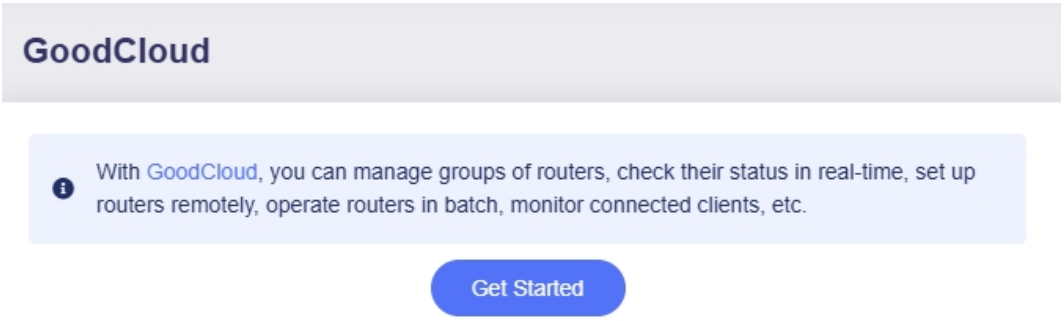
Avec GoodCloud, vous pouvez :

- Vérifier l'état du routeur en temps réel
- Gérer des groupes de routeurs
- Configurer les routeurs à distance
- Surveiller les clients connectés
- Effectuer des opérations groupées sur les routeurs
- Établir une connexion site à site

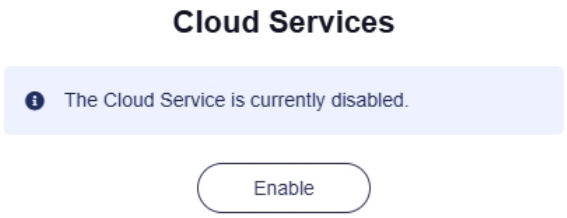
Certaines fonctions sont proposées dans les offres Enterprise et VAR (Value Added Reseller, revendeur à valeur ajoutée). Consultez cette page pour en savoir plus.

7.1.1 Activation de GoodCloud

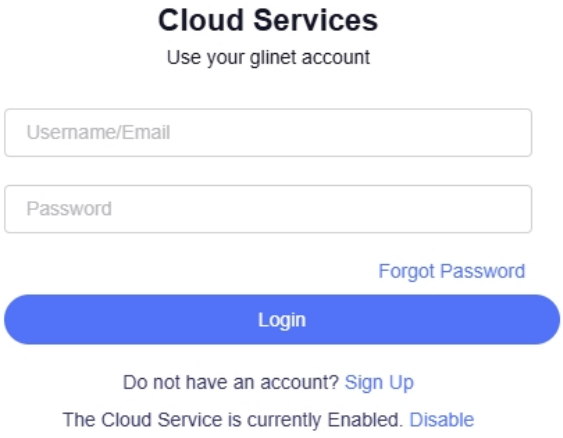
1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICE)** > **GoodCloud**, puis cliquez sur **Commencer (Get Started)**.



2. Une fenêtre s'ouvre dans l'angle supérieur droit. Cliquez sur **Activer (Enable)**.



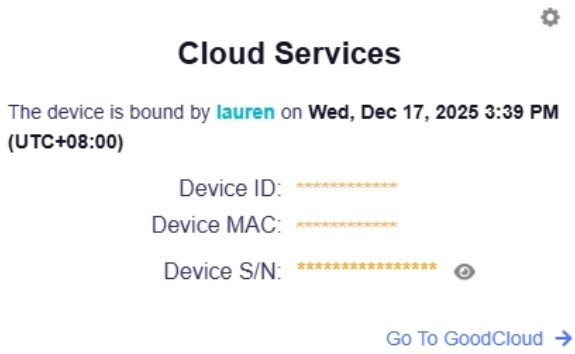
3. Connectez-vous avec votre compte GL.iNet Cloud. Si vous n'avez pas de compte, créez-en un, puis connectez-vous. Le routeur est alors automatiquement associé à votre compte.



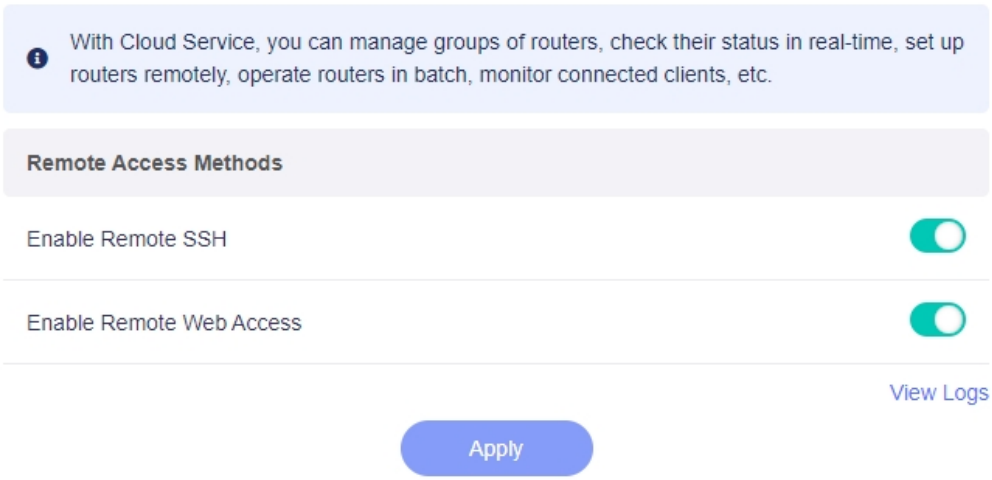
Conseils :

- La procédure d'association à GoodCloud varie selon la version du micrologiciel.
- Si vous ne recevez pas l'e-mail de vérification, consultez votre dossier de courrier indésirable ou réessayez plus tard. Pour obtenir de l'aide, écrivez-nous à support@gl-inet.com.

4. Une fois l'association réussie, cliquez sur l'**icône Cloud** dans l'angle supérieur droit de l'interface Web. Les informations d'association s'affichent : compte associé, date d'association, identifiant de l'appareil, adresse MAC et numéro de série.



5. Ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud** et activez l'accès à distance.
   GoodCloud permet d'accéder à distance à l'interface d'administration Web et au terminal du routeur associé. Vous pouvez activer ou désactiver cet accès ici.

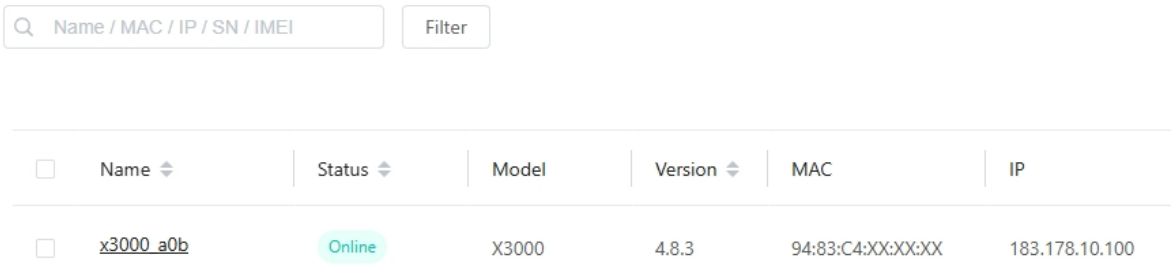


- **SSH à distance (Remote SSH) :** permet d'accéder au terminal du routeur depuis GoodCloud via SSH.
- **Accès Web à distance (Remote Web Access) :** permet d'accéder à l'interface d'administration Web du routeur depuis GoodCloud via HTTP/HTTPS.
- **Afficher les journaux (View Logs) :** ouvre la page Journal et affiche le journal Cloud.

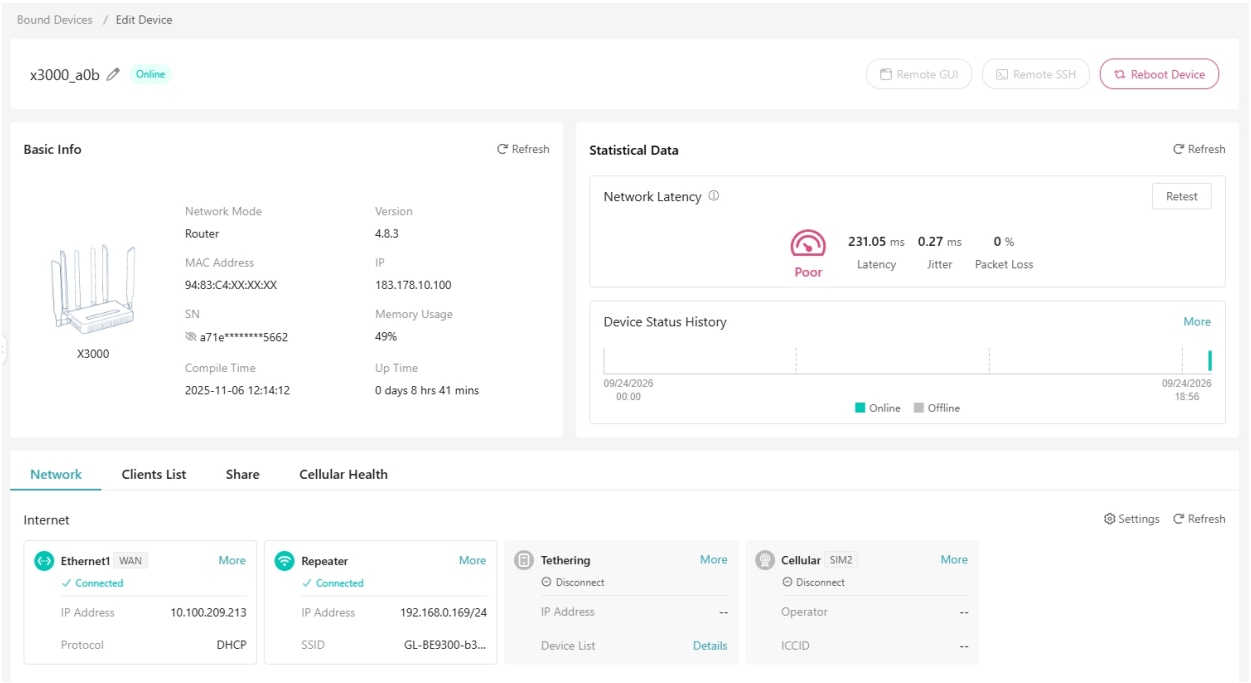
7.1.2 Gestion de votre routeur

7.1.2.1 Consultation des détails de l’appareil

Connectez-vous à GoodCloud, puis ouvrez **Appareil (Device)** > **Appareils associés (Bound Devices)**. Vous pouvez consulter les informations de base de l’appareil : nom d’hôte, état (en ligne ou hors ligne), modèle, version du micrologiciel et adresse MAC.

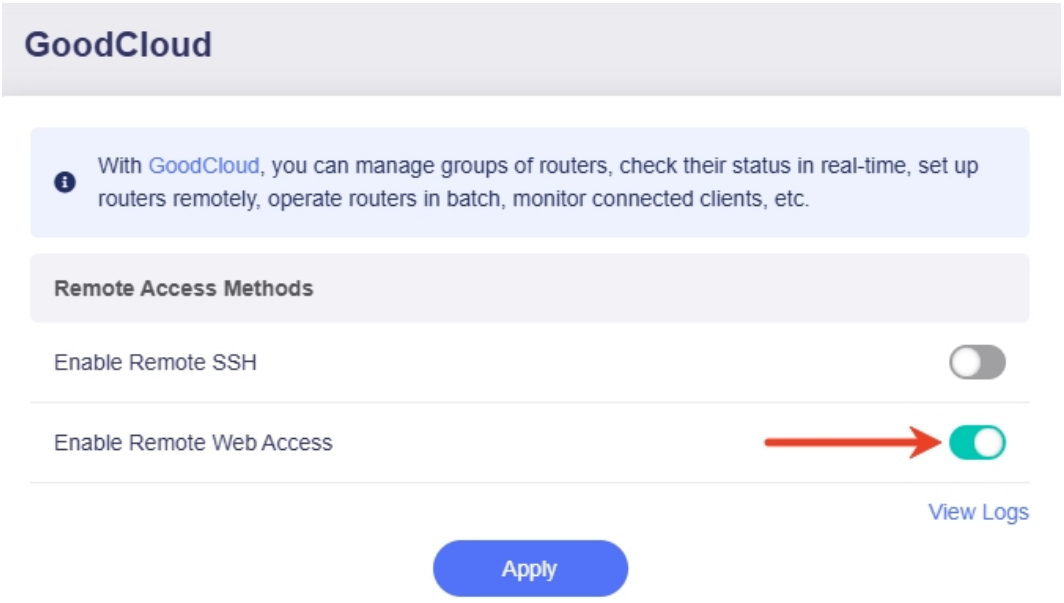


Cliquez sur le nom de l’appareil pour ouvrir sa page de détails. Elle présente les informations de base, les statistiques, la vue d’ensemble du réseau, la liste des clients et la chronologie. Vous pouvez également effectuer des opérations avancées, comme accéder au routeur à distance ou le redémarrer.

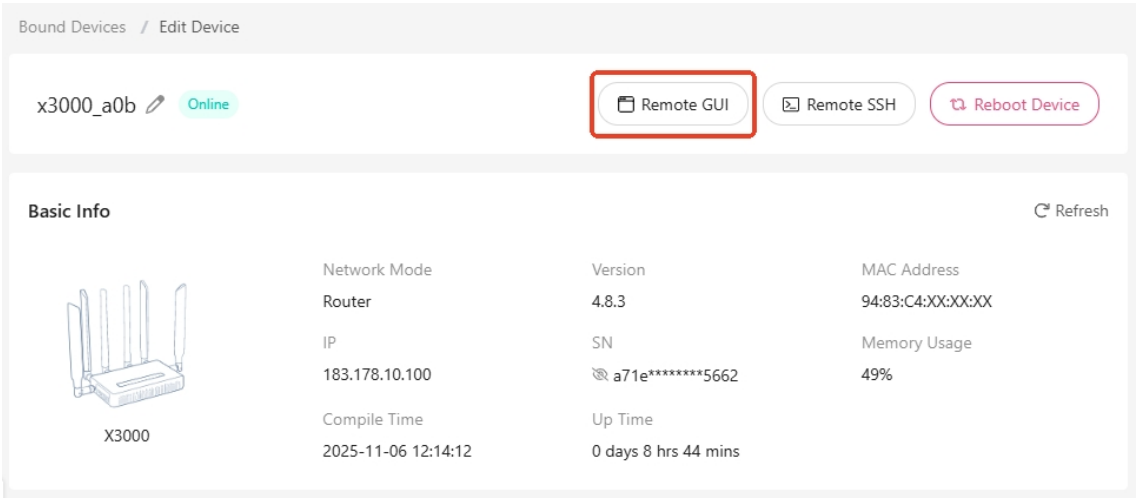


7.1.2.2 Accès Web à distance

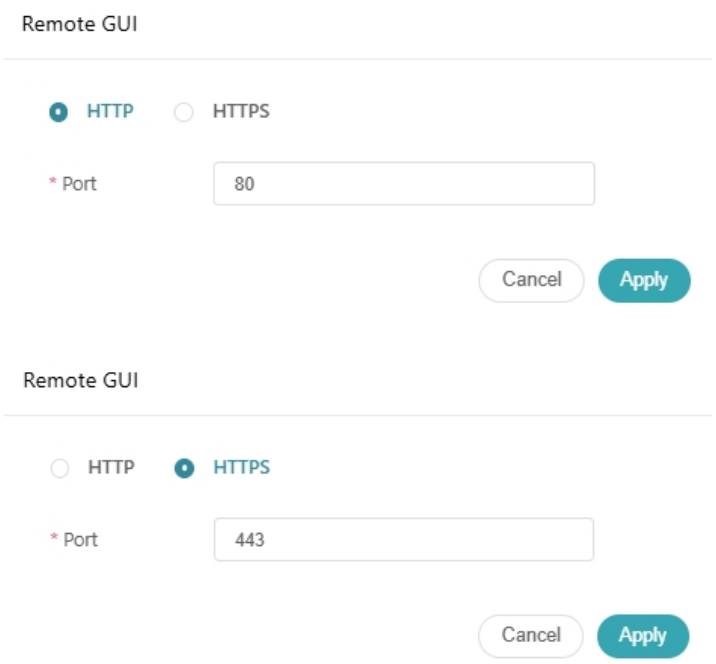
1. Dans l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud**, activez **Accès Web à distance (Remote Web Access)**, puis cliquez sur **Appliquer (Apply)**.



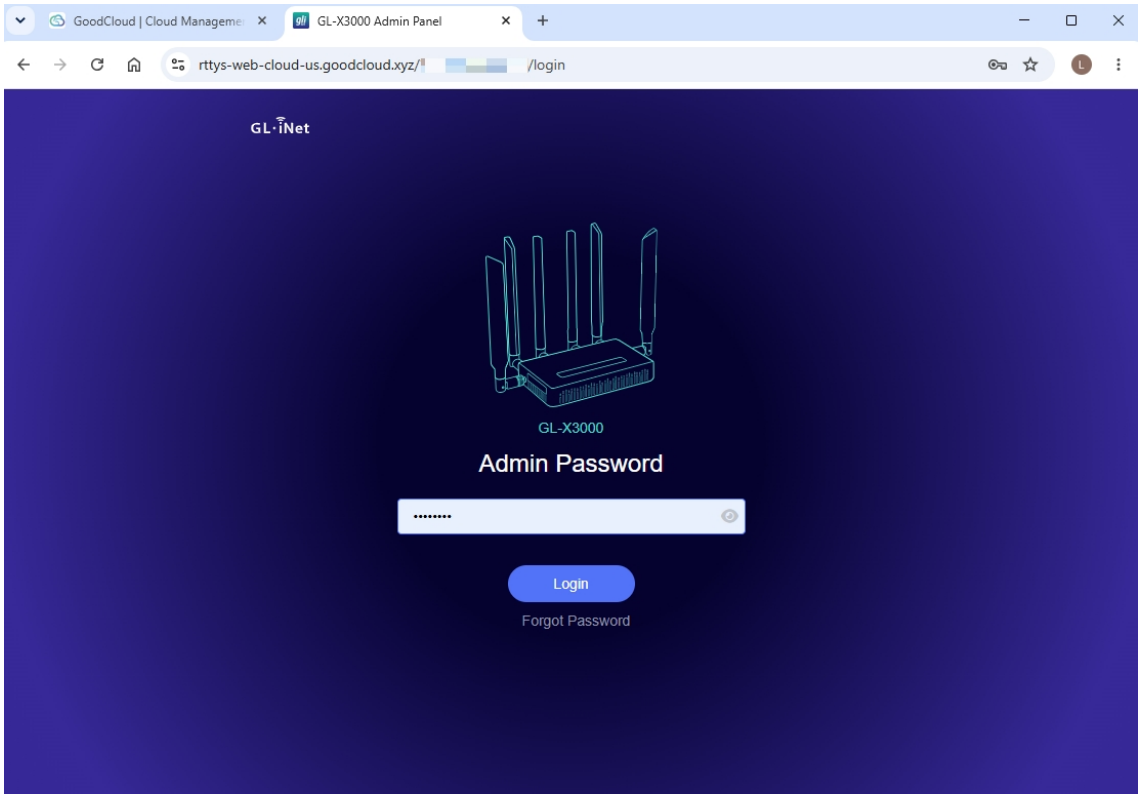
2. Connectez-vous à GoodCloud et ouvrez **Appareil (Device)** > **Appareils associés (Bound Devices)**. Cliquez sur l'appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
3. Sur cette page, cliquez sur le bouton **Interface à distance (Remote GUI)** dans l'angle supérieur droit.



4. Sélectionnez le protocole de transfert et le port. Les valeurs par défaut sont **HTTP** et le port **80**. Vous pouvez choisir HTTPS si nécessaire ; le port passe alors automatiquement à 443. Cliquez ensuite sur **Appliquer (Apply)**.

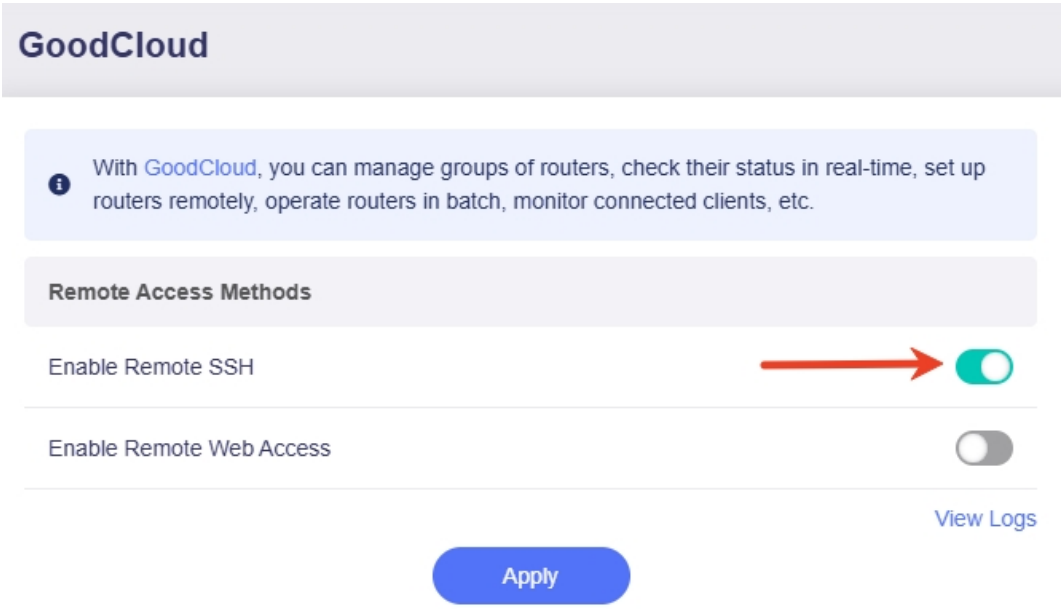


5. La page de connexion du routeur s’ouvre. Saisissez le mot de passe administrateur pour accéder à distance à l’interface d’administration Web.

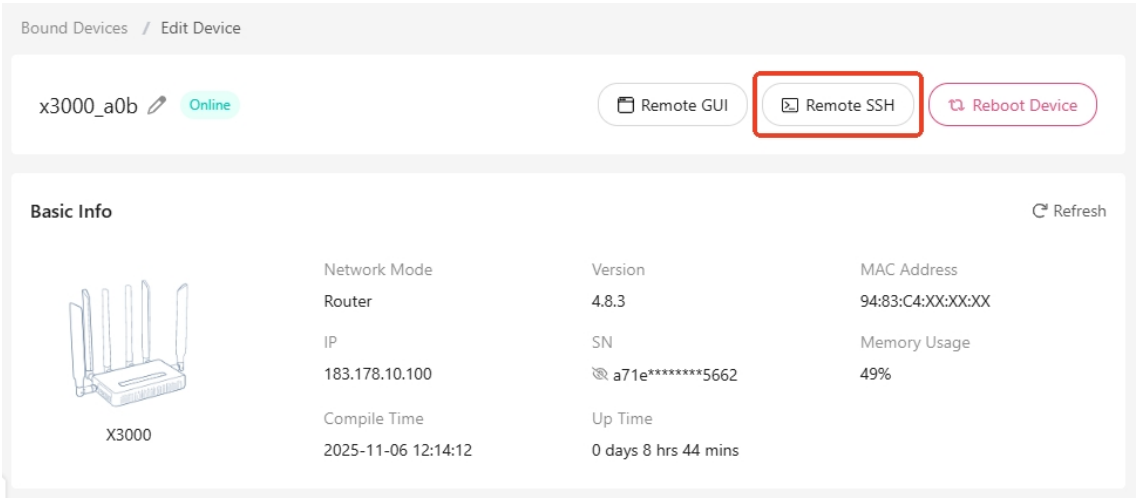

GoodCloud | Cloud Manageme
GL-X3000 Admin Panel
rttys-web-cloud-us.goodcloud.xyz/
/login
GL·iNet
GL-X3000
Admin Password
Login
Forgot Password

7.1.2.3 SSH à distance

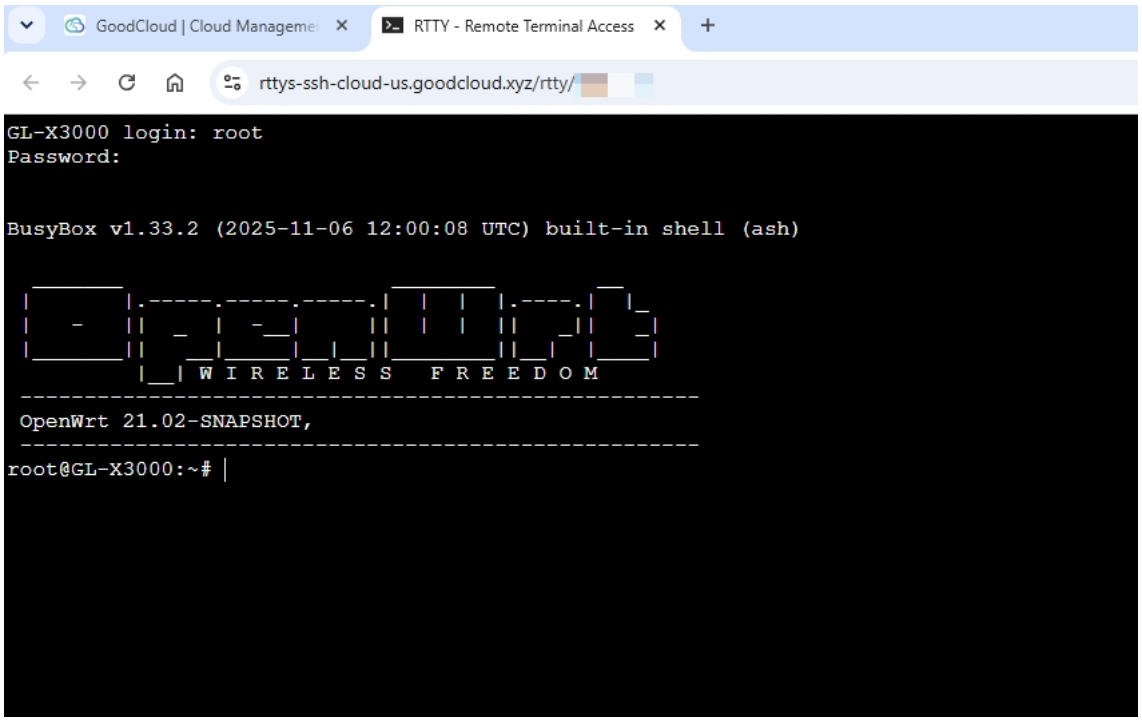
1. Dans l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud**, activez **SSH à distance (Remote SSH)**, puis cliquez sur **Appliquer (Apply)**.



2. Connectez-vous à GoodCloud et ouvrez **Appareil (Device)** > **Appareils associés (Bound Devices)**. Cliquez sur l'appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
3. Sur cette page, cliquez sur le bouton **SSH à distance (Remote SSH)** dans l'angle supérieur droit.

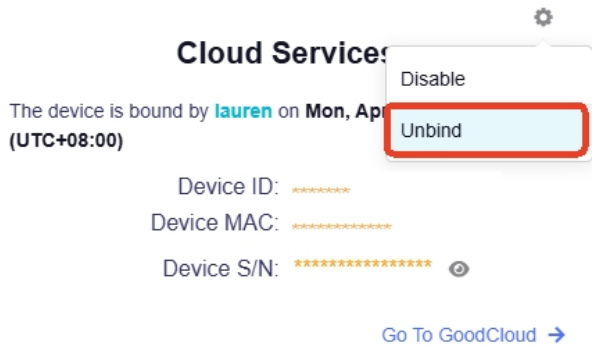


4. Connectez-vous avec l'identifiant **root** et saisissez le mot de passe pour accéder au terminal du routeur.

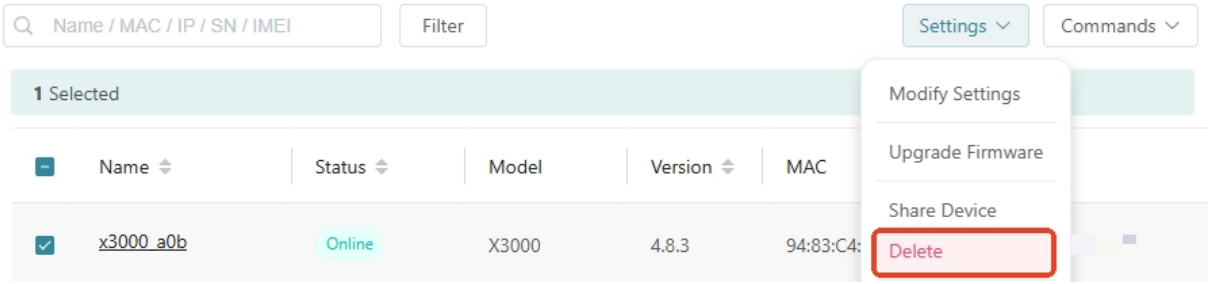

GoodCloud | Cloud Manageme
RTTY - Remote Terminal Access
rttys-ssh-cloud-us.goodcloud.xyz/rtty/
GL-X3000 login: root
Password:
BusyBox v1.33.2 (2025-11-06 12:00:08 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-X3000:~#

7.1.3 Dissociation de l’appareil

Dans l’interface Web du routeur, cliquez sur l’icône Cloud dans l’angle supérieur droit. Dans le menu, cliquez sur l’engrenage, puis sélectionnez **Dissocier (Unbind)**. L’appareil est alors dissocié de votre compte GoodCloud.

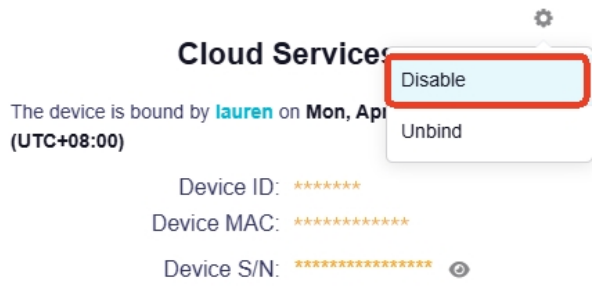


Vous pouvez également vous connecter à la plateforme Cloud et ouvrir **Appareil (Device)** > **Appareils associés (Bound Devices)**. Sélectionnez l’appareil à dissocier, cliquez sur **Paramètres (Settings)** dans l’angle supérieur droit, puis sélectionnez **Supprimer (Delete)**. L’appareil est alors dissocié de votre compte GoodCloud.



7.1.4 Désactivation de GoodCloud

Si vous ne souhaitez plus connecter l’appareil au cloud, cliquez sur l’icône Cloud dans l’angle supérieur droit. Dans le menu, cliquez sur l’engrenage et sélectionnez **Désactiver (Disable)**.

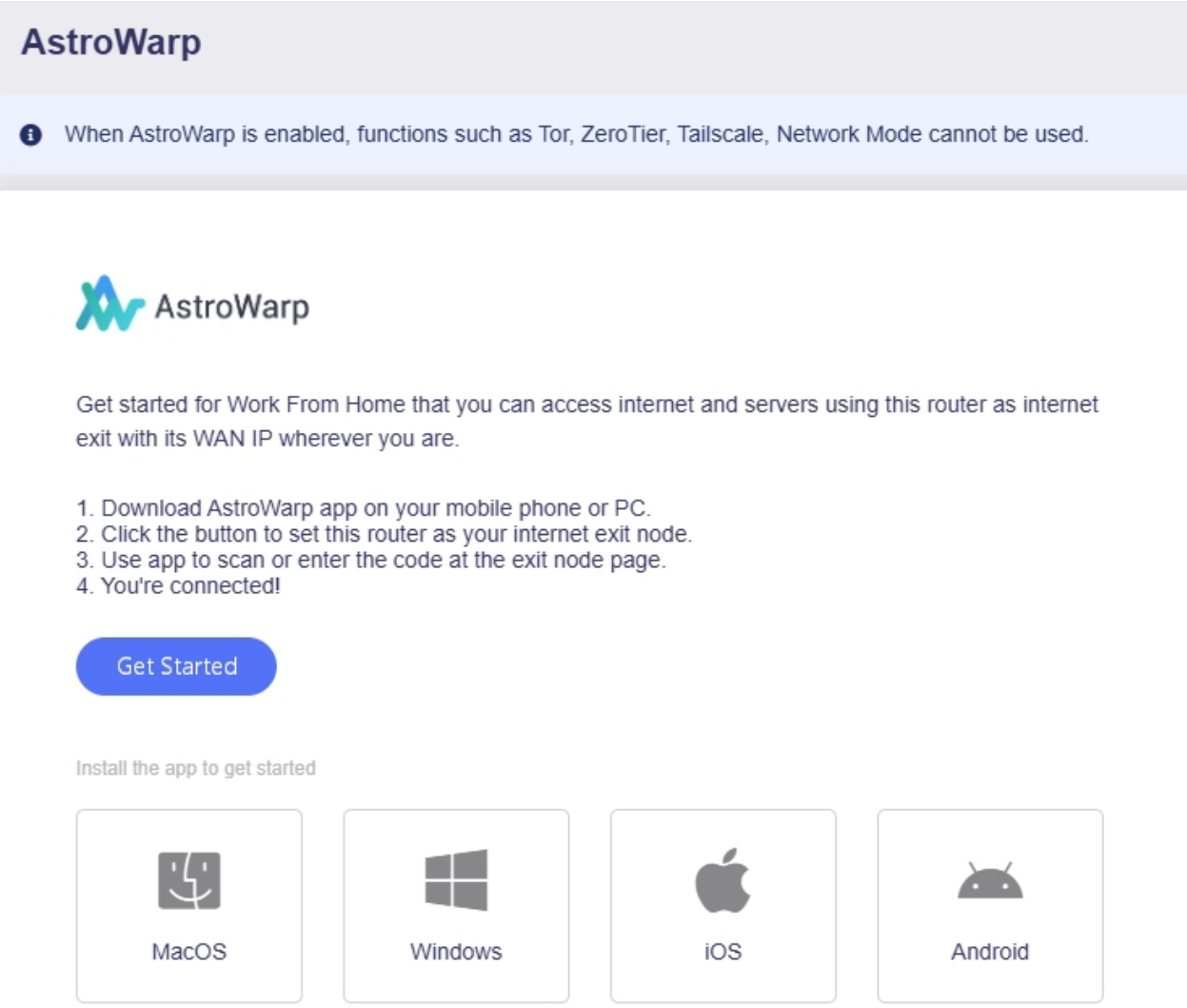


Le service Cloud est alors désactivé.

7.2 AstroWarp

AstroWarp est une plateforme réseau avancée qui relie plusieurs routeurs GL.iNet au sein d'un réseau unifié pour faciliter l'accès à distance. Ses possibilités de configuration flexibles, sa simplicité d'utilisation et sa protection de la confidentialité assurent une connectivité sûre et fiable. Pour le télétravail ou l'accès sécurisé aux ressources internes d'une entreprise répartie sur plusieurs sites, AstroWarp offre une solution réseau performante et protégée.

Connectez-vous à l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICE)** > **AstroWarp**, puis cliquez sur **Commencer (Get Started)**. Suivez ensuite les instructions pour configurer votre réseau. Consultez astrowarp.net pour en savoir plus.



Chapitre 8

Comprendre les VPN

Ce chapitre présente les principes des VPN et leurs principaux cas d’utilisation.

8.1 Introduction

8.1.1 VPN

Un VPN (Virtual Private Network, réseau privé virtuel) établit un tunnel privé et chiffré entre un appareil et un serveur distant. Il protège les données transmises et permet d'accéder de manière sécurisée à des réseaux privés ou à accès restreint.

8.1.2 Routeur VPN

Un routeur VPN intègre une fonction VPN qui protège tous les appareils connectés. Configuré comme client VPN, il achemine l'ensemble du trafic dans un tunnel chiffré, sans configuration individuelle de chaque appareil. Vous protégez ainsi plusieurs appareils à la fois, gagnez du temps et maintenez une configuration cohérente, en réduisant les risques liés à des réglages individuels incorrects.

Les routeurs GL.iNet prennent en charge plus de 30 services VPN commerciaux courants utilisant OpenVPN et WireGuard. Importez vos fichiers de configuration VPN pour activer une connexion sécurisée. Consultez cette page pour obtenir la liste complète des fournisseurs VPN tiers.

8.1.3 OpenVPN

OpenVPN est un protocole VPN open source utilisant la sécurité SSL/TLS pour établir des connexions d'un appareil à un site ou de site à site. Il prend en charge plusieurs méthodes de chiffrement, TCP et UDP, et facilite le passage à travers les pare-feu et le NAT.

8.1.4 WireGuard

WireGuard® est un protocole VPN léger et rapide, plus simple et plus efficace qu'OpenVPN. Il utilise une cryptographie moderne pour améliorer l'efficacité, une base de code réduite pour faciliter les audits de sécurité et des algorithmes de pointe (ChaCha20/Poly1305) pour le chiffrement et l'intégrité des données.

*WireGuard® est une marque déposée de Jason A. Donenfeld.

8.2 Cas d’utilisation

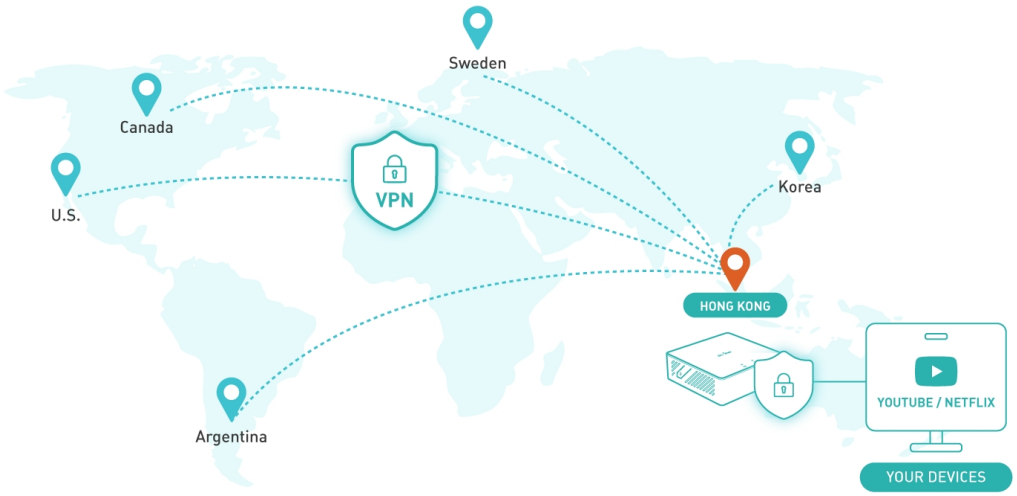
1. **Protection des données personnelles**

   Grâce au routeur, le service VPN protège de nombreux appareils : ordinateurs portables, téléphones, tablettes, mais aussi consoles de jeux, téléviseurs et appareils de streaming. Vos données sont protégées sur les connexions filaires comme sans fil. Vous pouvez également personnaliser les règles VPN pour adapter la protection de certains appareils.



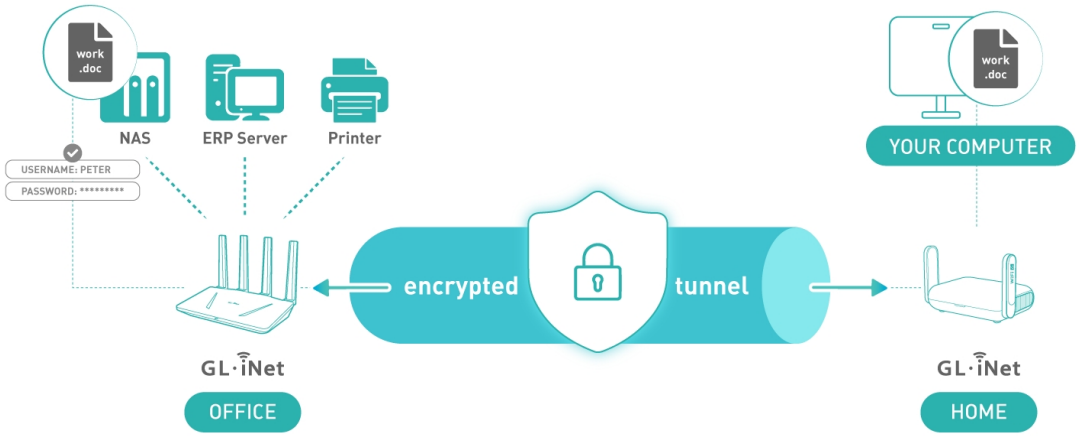
2. **Accès aux contenus depuis le monde entier**

   Certains sites limitent l’accès selon votre localisation. Un VPN peut permettre de lever ces restrictions lorsque cela est nécessaire. En vous connectant à différents serveurs tiers, vous obtenez des adresses IP différentes pour naviguer ou accéder aux sites soumis à des restrictions géographiques.



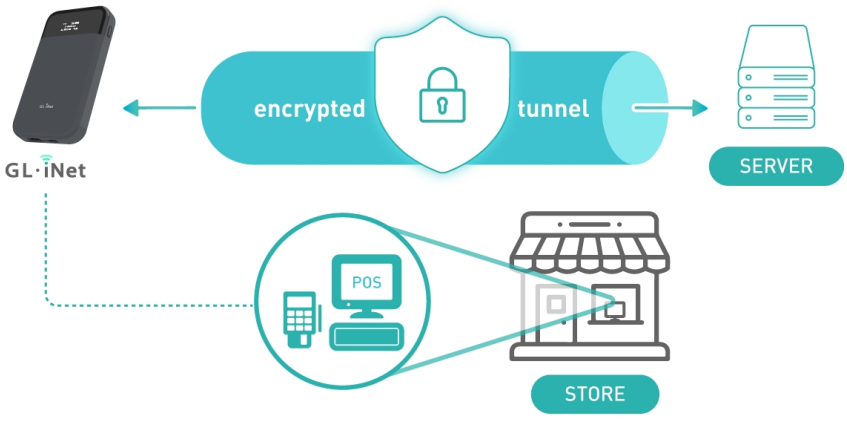
3. **Sécurité des données des petites entreprises**

   De nombreuses personnes travaillent dans des espaces de coworking ou des cafés et utilisent le Wi-Fi public gratuit. Ces réseaux sont exposés aux cyberattaques. En configurant votre routeur de voyage comme client VPN, vous disposez d'une connexion sécurisée pour travailler où que vous soyez.



4. **Sécurisation des paiements**

   Les petits commerçants traitent les données de paiement de leurs clients lors des transactions sur place. Avec un routeur VPN, leurs terminaux de paiement transmettent les informations de carte bancaire par un tunnel VPN chiffré pour sécuriser les paiements.



Chapitre 9

Tableau de bord VPN

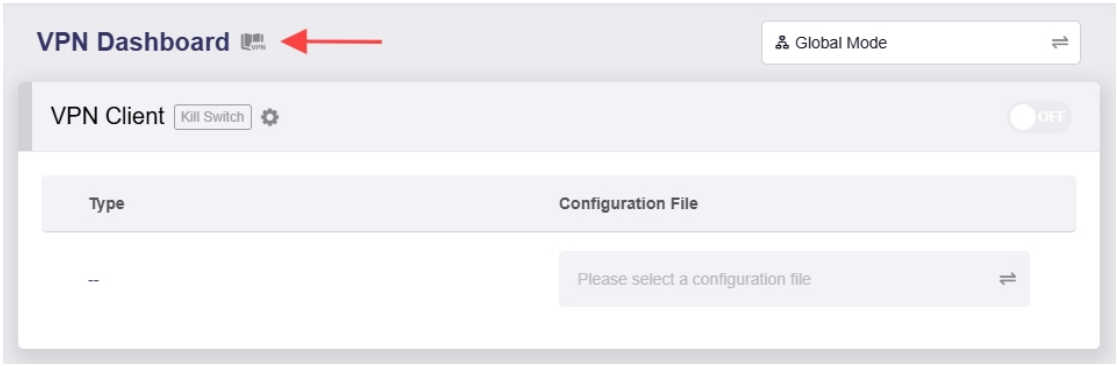
Ce chapitre explique comment gérer les connexions VPN depuis l’interface d’administration Web.

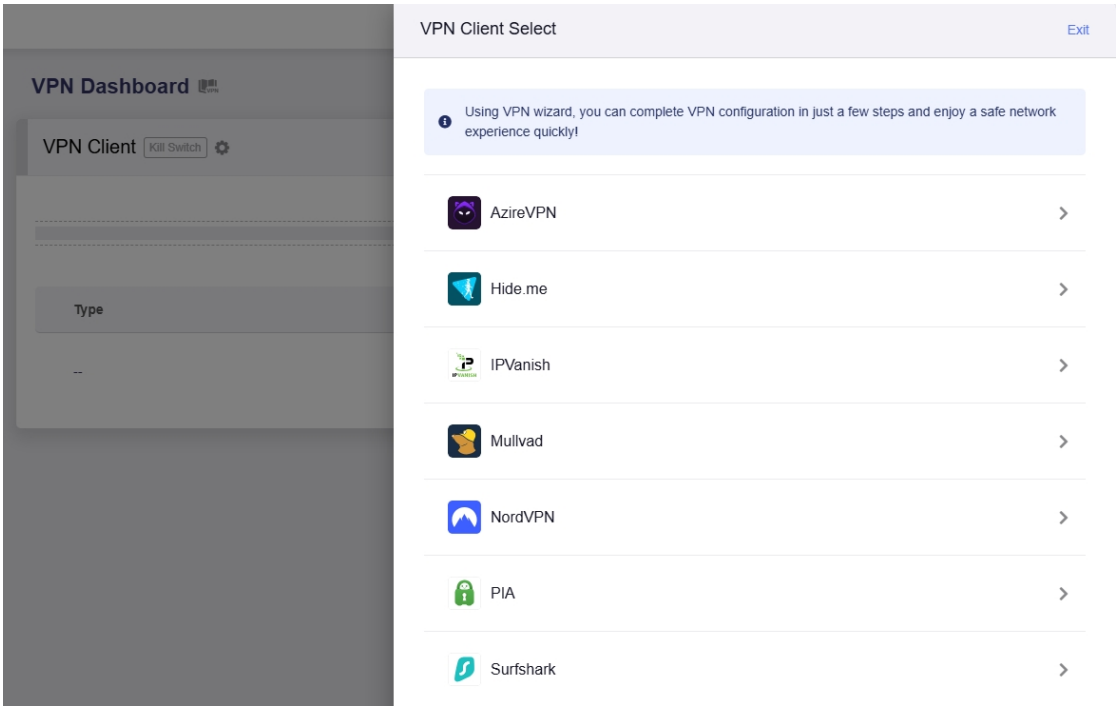
Connectez-vous à l’interface d’administration Web du routeur et ouvrez **VPN** > **Tableau de bord VPN (VPN Dashboard)**.

Le tableau de bord VPN affiche les détails de la connexion : règles du tunnel, adresse du serveur, statistiques de trafic, IP virtuelle du client et journal de connexion. Vous pouvez aussi régler des options avancées, comme le coupe-circuit VPN, le masquage IP et le MTU, et activer plusieurs connexions VPN pour utiliser plusieurs tunnels.

9.1 Assistant de configuration VPN

Pour commencer, cliquez sur l’icône en forme de livre dans l’angle supérieur gauche et suivez l’assistant pour configurer rapidement le VPN.



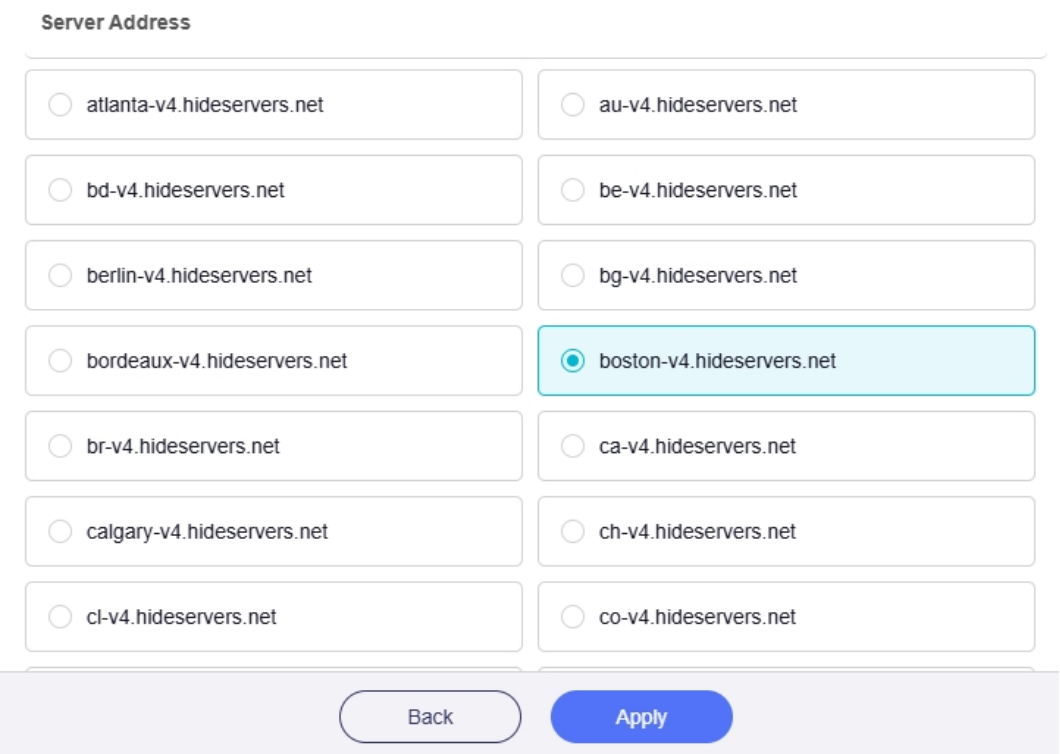


Remarque : l'assistant prend uniquement en charge les services VPN intégrés : AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA et Surfshark. Pour un autre fournisseur, ignorez l'assistant et ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** ou **Client WireGuard (WireGuard Client)** pour effectuer la configuration manuellement.

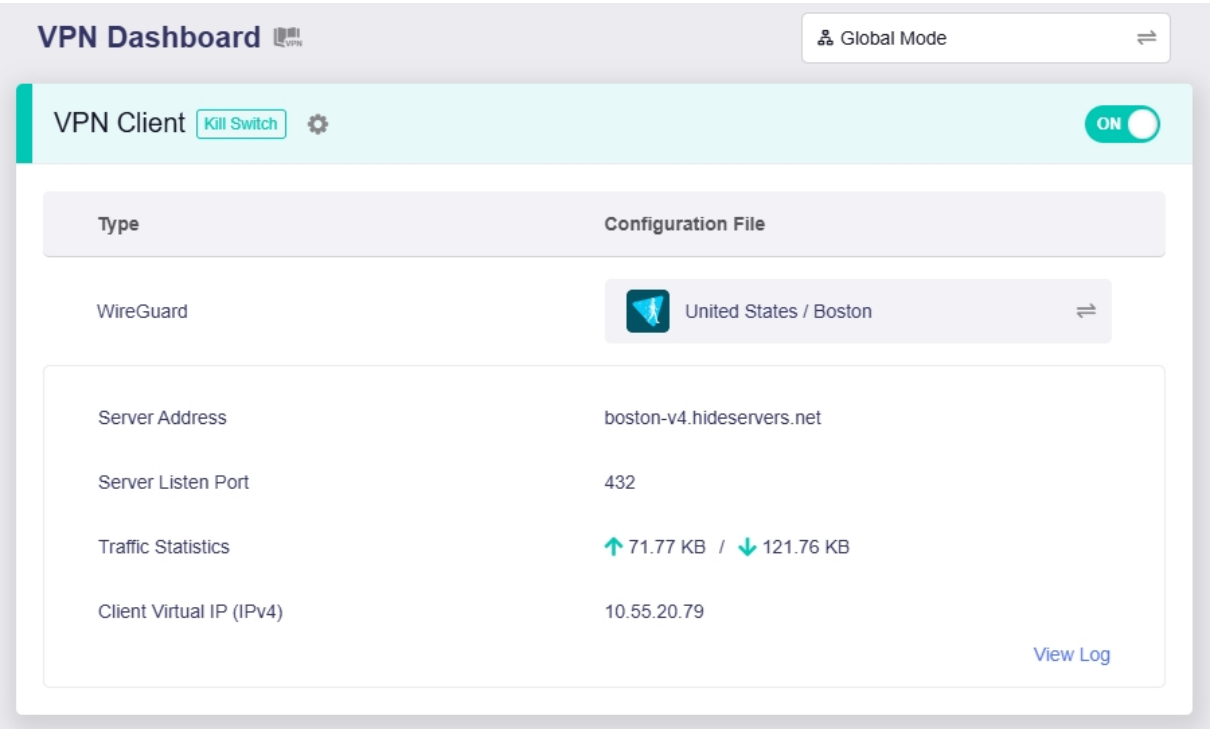
Voici un exemple avec **Hide.me**. Connectez-vous avec vos identifiants Hide.me.



Sélectionnez un serveur VPN et cliquez sur **Appliquer (Apply)**. Votre connexion utilisera ce serveur et votre adresse IP publique semblera provenir de son emplacement.

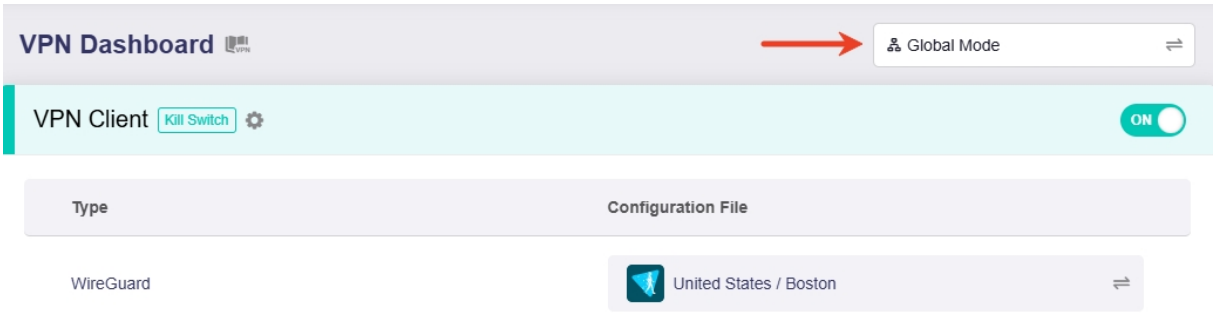


La connexion s'établit automatiquement. Ouvrez ensuite le **Tableau de bord VPN (VPN Dashboard)**. Le tunnel activé affiche le protocole VPN, par exemple WireGuard, le fichier de configuration, l'adresse et le port d'écoute du serveur, les statistiques de trafic et l'adresse IP virtuelle du client. Vous pouvez consulter le journal de connexion dans l'angle inférieur droit.

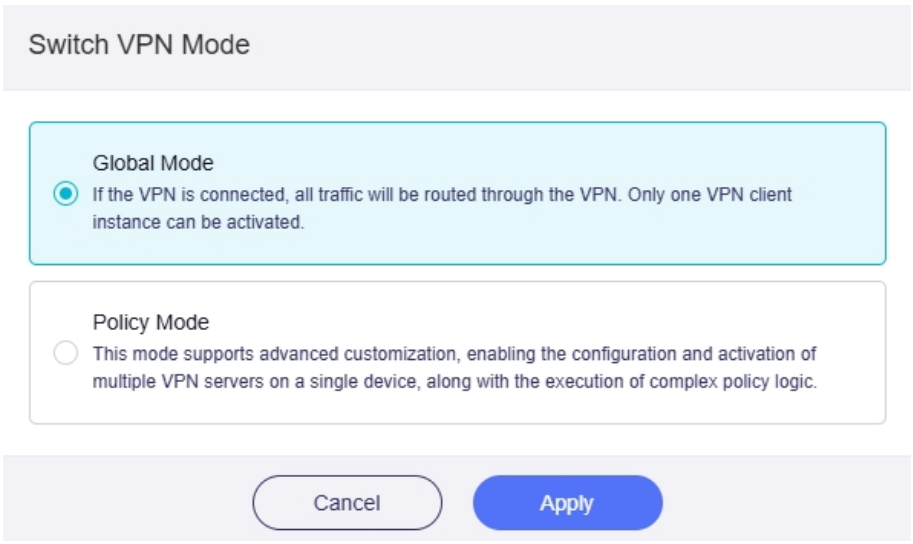


9.2 Mode VPN

Dans le tableau de bord VPN, cliquez sur le bouton dans l’angle supérieur droit pour changer de mode si nécessaire.



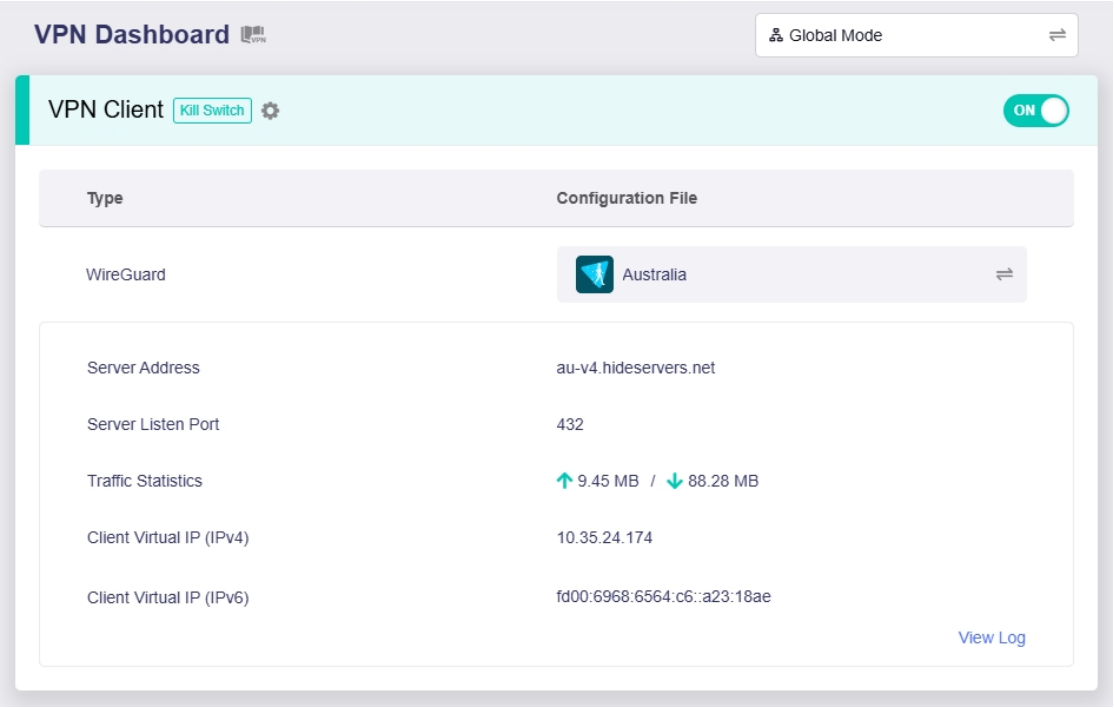
Deux modes sont disponibles : **Mode global (Global Mode)** et **Mode par règles (Policy Mode)**.



9.2.1 Mode global

Dans ce mode, tout le trafic passe par le tunnel VPN et une seule instance de client VPN peut être activée. Ce mode convient lorsque tous les appareils doivent utiliser un même serveur VPN, par exemple pour appliquer une protection uniforme ou accéder à des contenus d'une région donnée.

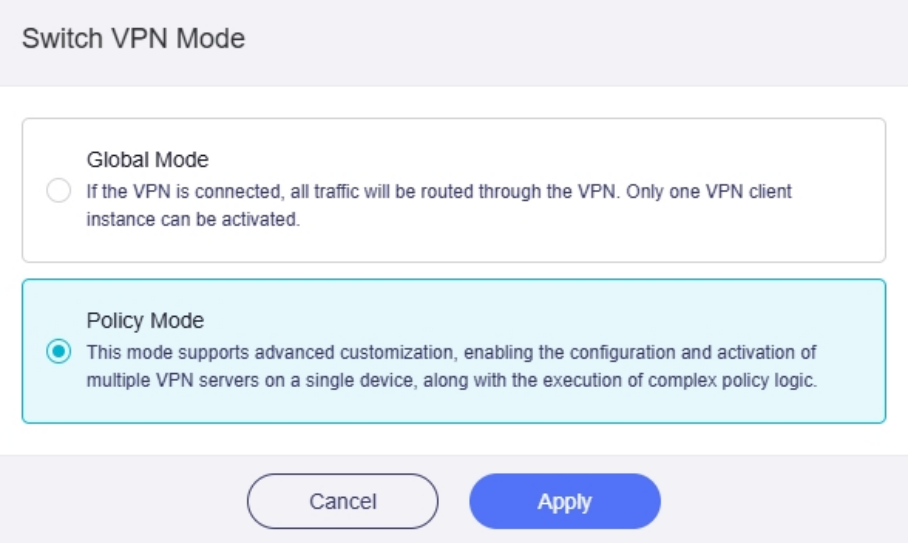
Dans l'exemple suivant, le routeur se connecte à un serveur australien avec WireGuard. Tout le trafic des clients connectés passe par ce tunnel VPN.



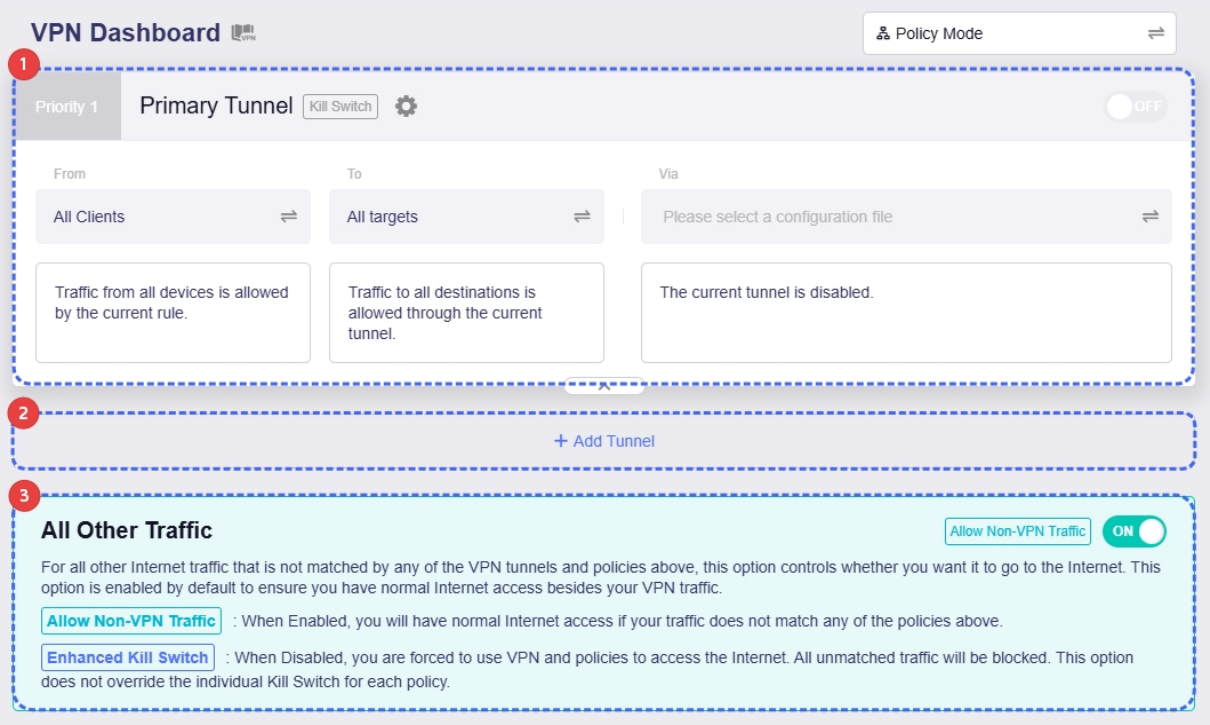
9.2.2 Mode par règles

Ce mode permet de connecter un routeur à plusieurs serveurs VPN et de personnaliser les règles de routage. Il convient à une gestion souple du trafic, par exemple pour acheminer différents flux vers différentes destinations via plusieurs serveurs VPN.

Sélectionnez **Mode par règles (Policy Mode)**, puis cliquez sur **Appliquer (Apply)**.



Après ce changement, si aucun VPN n'est activé, la page comporte trois sections : **Tunnel principal (Primary Tunnel)**, **Ajouter un tunnel (Add Tunnel)** et **Tout autre trafic (All Other Traffic)**.

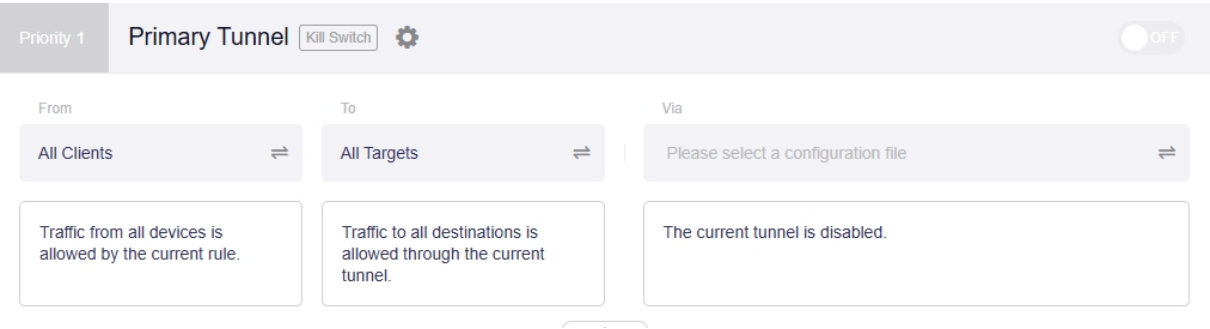


9.2.2.1 Tunnel principal

Le tunnel principal est prédéfini en mode par règles. Il a la priorité la plus élevée par défaut. Vous pouvez modifier cette priorité lorsque plusieurs tunnels sont configurés.

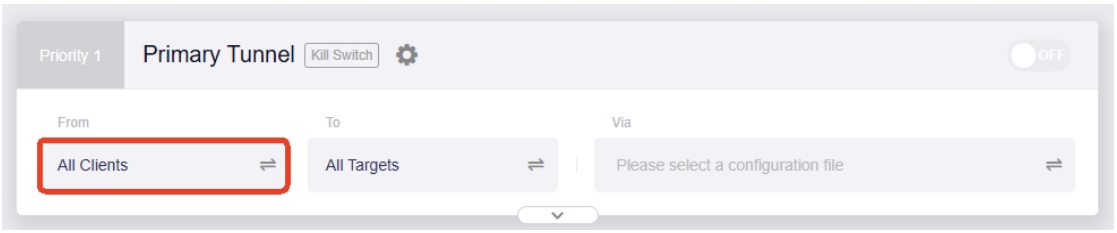
Personnalisez la règle de ce tunnel à l'aide de trois critères :

- **Depuis (From)** : source du trafic, c'est-à-dire le trafic à acheminer par ce tunnel.
- **Vers (To)** : destination vers laquelle le trafic est acheminé par ce tunnel.
- **Via** : méthode d'acheminement du trafic, avec ou sans VPN.

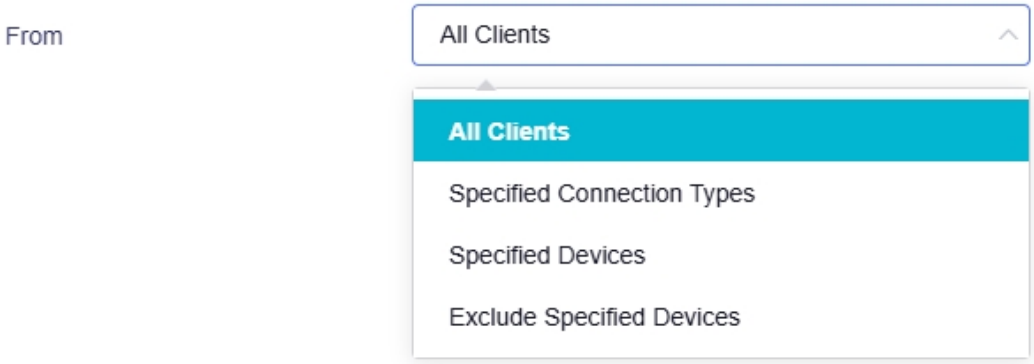


Suivez les étapes ci-dessous pour configurer la règle du tunnel.

1. Cliquez sur la zone grisée de gauche.

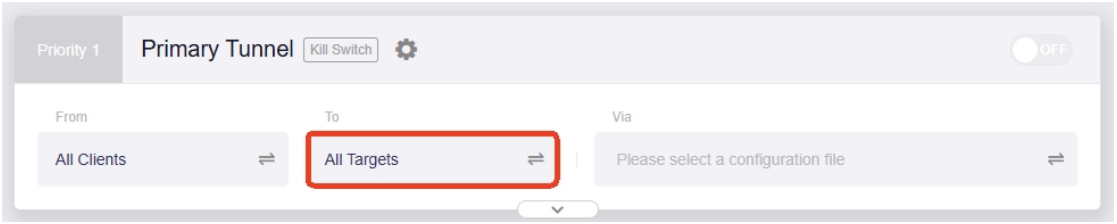


2. Sélectionnez les appareils auxquels appliquer la règle, puis cliquez sur **Appliquer (Apply)**.

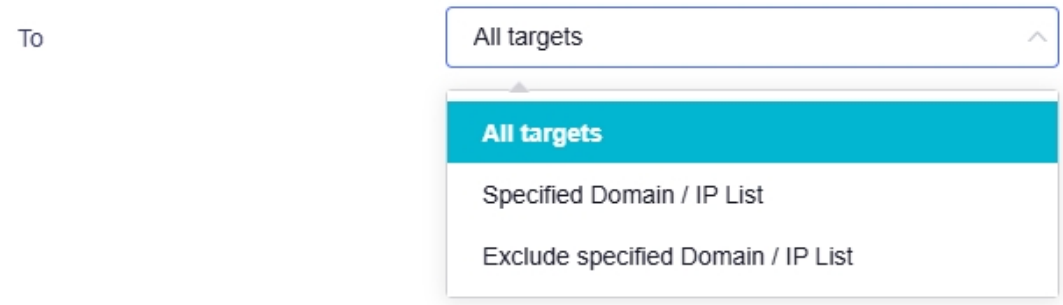


- **Tous les clients (All Clients)** : la règle s'applique au trafic de tous les appareils.
- **Types de connexion spécifiés (Specified Connection Types)** : la règle s'applique au trafic des types de connexion choisis, par exemple le sous-réseau LAN, la passerelle transparente ou le réseau invité.
- **Appareils spécifiés (Specified Devices)** : la règle s'applique au trafic des appareils choisis, identifiés par leur adresse MAC.
- **Exclure les appareils spécifiés (Exclude Specified Devices)** : la règle **ne s'applique pas** au trafic des appareils choisis, identifiés par leur adresse MAC.

3. Cliquez sur la zone grisée du milieu.



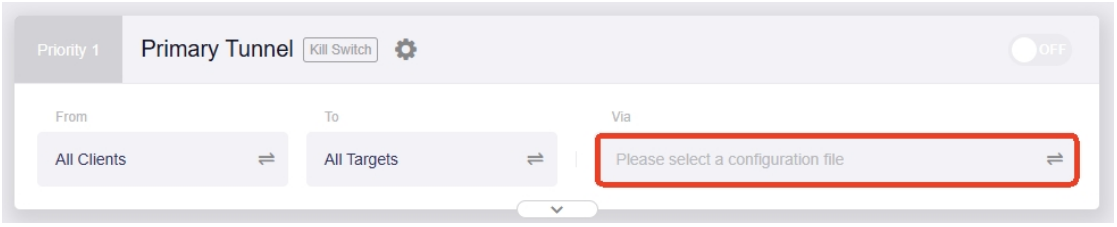
4. Sélectionnez les destinations vers lesquelles acheminer le trafic par ce tunnel, puis cliquez sur **Appliquer (Apply)**.



- **Toutes les destinations (All Targets)** : la règle s'applique au trafic vers toutes les destinations.
- **Liste de domaines/IP spécifiés (Specified Domain / IP List)** : la règle s'applique au trafic vers les domaines et adresses IP indiqués. Saisissez-les manuellement ou renseignez l'URL d'abonnement. Un domaine racine englobe tous ses sous-domaines.
- **Exclure les domaines/IP spécifiés (Exclude specified Domain / IP List)** : la règle **ne s'applique pas** au trafic vers les domaines et adresses IP indiqués. Saisissez-les manuellement ou renseignez l'URL d'abonnement. Un domaine racine englobe tous ses sous-domaines.

Remarque : si vous utilisez une URL d'abonnement, les domaines et adresses IP de la liste sont mis à jour automatiquement chaque jour. Saisissez une URL correcte. La vérification de l'URL contrôle la validité des domaines ou des adresses IP.

5. Cliquez sur la zone grisée de droite.

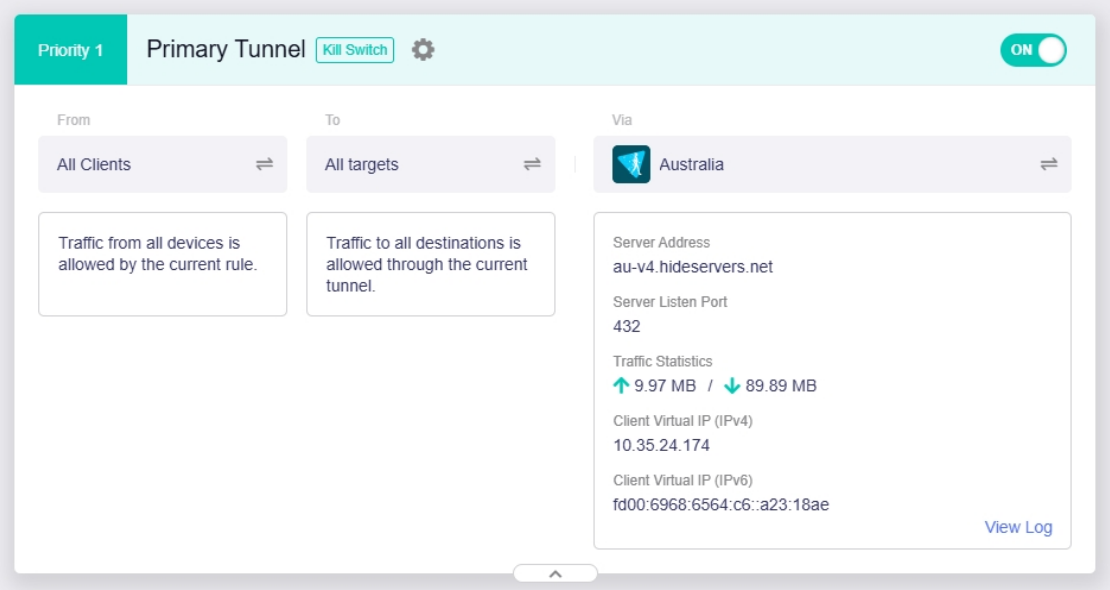


6. Choisissez la méthode de routage du tunnel : **Utiliser le VPN (Use VPN)** ou **Ne pas utiliser le VPN (Not Use VPN)**.



- **Utiliser le VPN (Use VPN)** : le trafic correspondant à la règle est acheminé vers les destinations choisies par le tunnel VPN. Sélectionnez un fichier de configuration VPN pour cette règle.
- **Ne pas utiliser le VPN (Not Use VPN)** : le trafic correspondant à la règle est acheminé vers les destinations choisies par le réseau WAN local, sans VPN.

7. Après avoir défini la source, la destination et la méthode de routage, la règle du tunnel principal est configurée. Dans l'exemple suivant, tous les clients du routeur accèdent à Internet via le VPN. Leur trafic passe par le tunnel jusqu'au serveur australien, puis sort de ce serveur vers Internet.

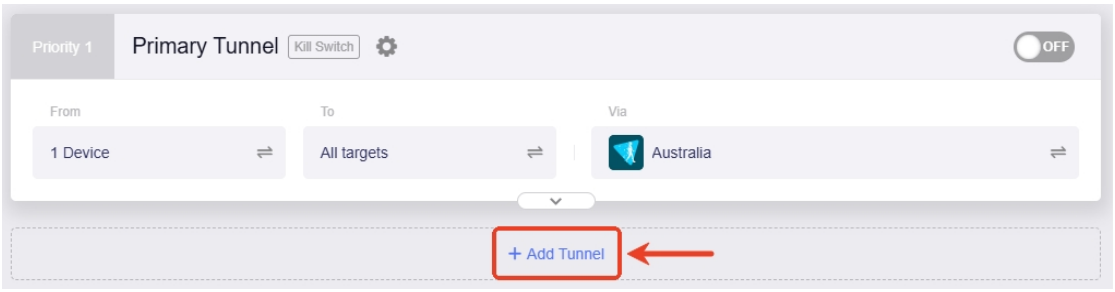


Remarque : pour votre sécurité, consultez les sections **9.2.2.3 Tout autre trafic** et **9.2.2.4 Options du tunnel** pour vérifier les autres paramètres avant d'activer ce tunnel.

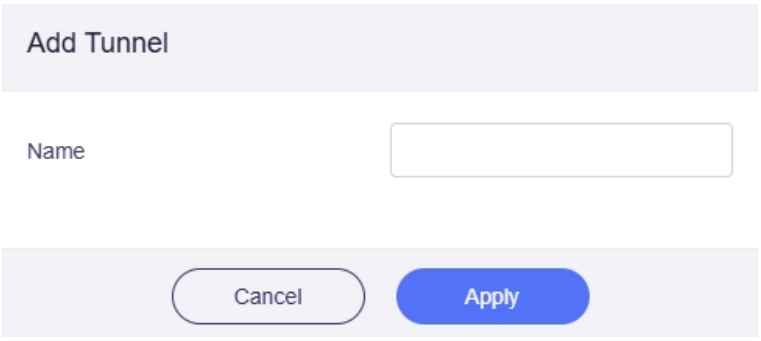
9.2.2.2 Ajout d'un tunnel

Ajoutez des tunnels pour acheminer le trafic de différents appareils vers différentes destinations. Suivez les étapes ci-dessous pour ajouter un tunnel.

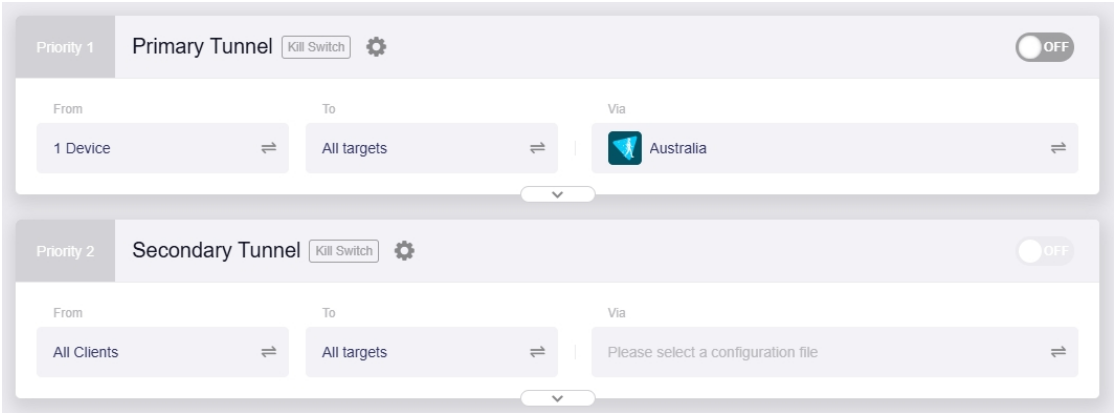
1. Cliquez sur **Ajouter un tunnel (Add Tunnel)** sous le tunnel principal.



2. Donnez un nom au tunnel.



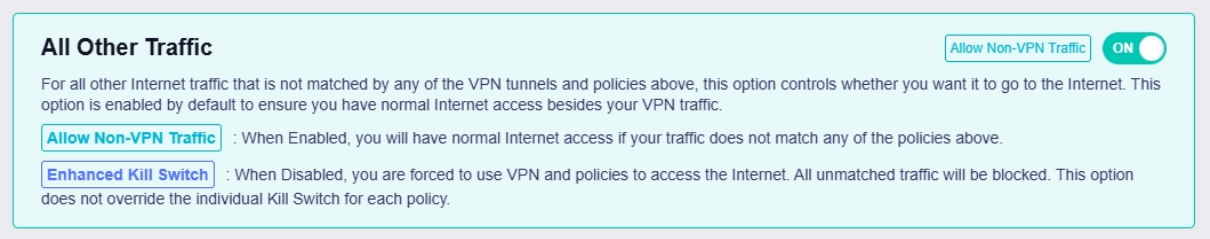
3. Un tunnel supplémentaire apparaît dans le tableau de bord VPN. Vous pouvez créer jusqu'à cinq tunnels, y compris le tunnel principal prédéfini.



4. Configurez les règles du tunnel en définissant la source du trafic, les destinations et la méthode de routage. Ensuite, consultez les sections **9.2.2.3 Tout autre trafic** et **9.2.2.4 Options du tunnel** pour vérifier les autres paramètres avant d'activer ce tunnel.

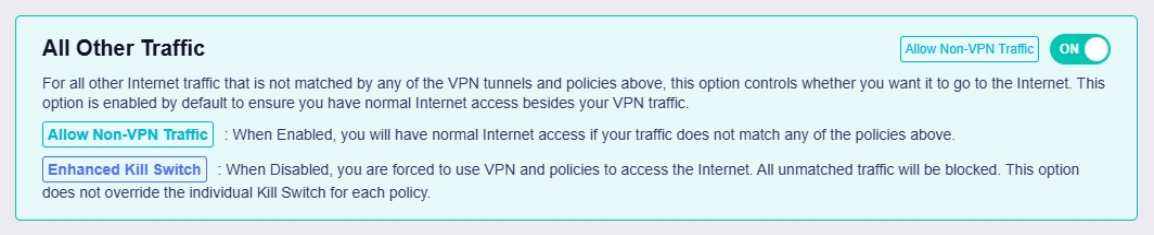
9.2.2.3 Tout autre trafic

En mode par règles, un tunnel par défaut, déjà activé, apparaît en bas du tableau de bord VPN.

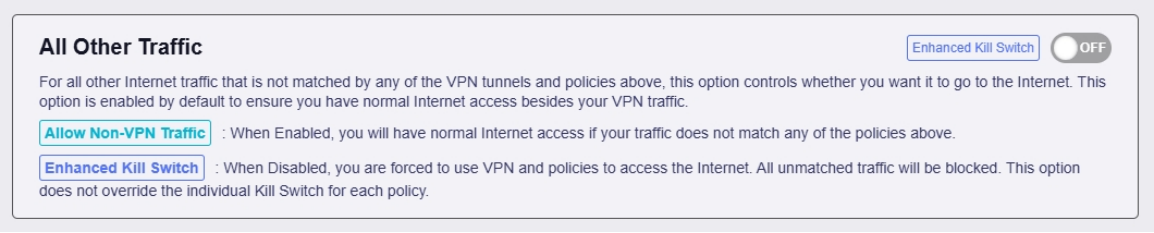


Ce tunnel détermine si le trafic ne correspondant à aucun des groupes de tunnels VPN précédents peut accéder à Internet. Il est activé par défaut afin de maintenir l'accès Internet du trafic qui n'utilise pas le VPN.

- Lorsqu'il est activé, le trafic ne correspondant à aucune règle peut accéder à Internet.

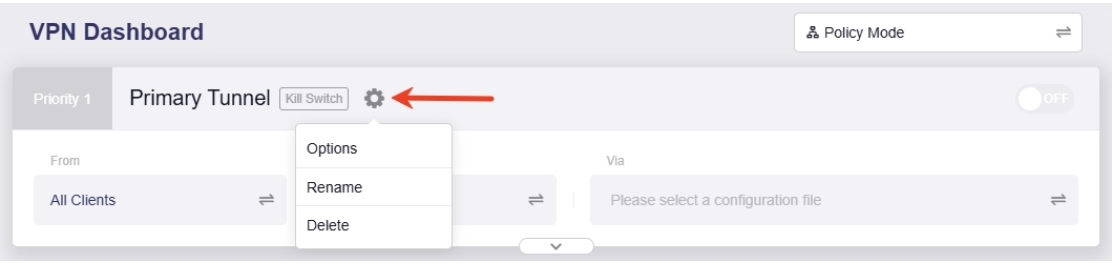


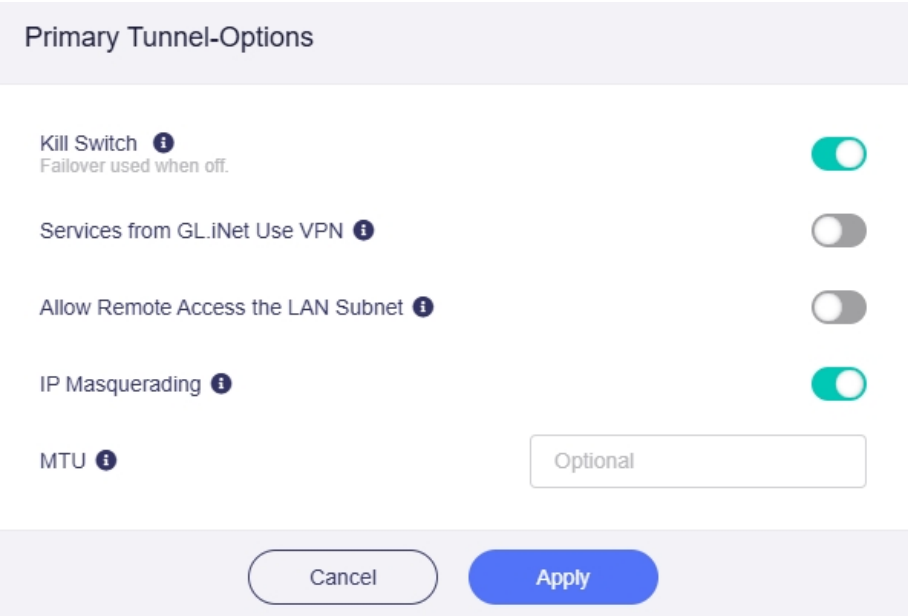
- Lorsqu'il est désactivé, seul le trafic acheminé par VPN peut accéder à Internet. Tout le trafic sans VPN et le trafic de secours provenant des connexions VPN sont bloqués. Cette option ne remplace pas le coupe-circuit propre à chaque tunnel.



9.2.2.4 Options du tunnel

Vous pouvez régler les paramètres avancés de chaque tunnel VPN, comme le coupe-circuit, le masquage IP et la MTU. Cliquez sur l'engrenage à côté du nom du tunnel.





- **Coupe-circuit (Kill Switch)** : s'il est activé, le trafic correspondant à ce tunnel est bloqué en cas de déconnexion imprévue. Sinon, il bascule vers les tunnels de priorité suivante ou vers le WAN.
- **Services GL.iNet via le VPN (Services from GL.iNet Use VPN)** : si cette option est activée, GoodCloud, DDNS et rtty transmettent leurs paquets par les tunnels VPN. Elle est désactivée par défaut, car ces services ont généralement besoin de l'adresse IP réelle de l'appareil pour fonctionner correctement.
- **Autoriser l'accès distant au sous-réseau LAN (Allow Remote Access the LAN Subnet)** : autorise l'accès au routeur, via son IP de tunnel, et aux appareils LAN à travers le VPN. Le serveur VPN doit annoncer une route de retour vers le sous-réseau LAN de ce routeur.
- **Masquage IP (IP Masquerading)** : remplace les adresses IP source des clients LAN par l'adresse IP du tunnel VPN du routeur. Désactivez-le uniquement pour une configuration site à site dans laquelle le pair distant connaît vos sous-réseaux LAN.

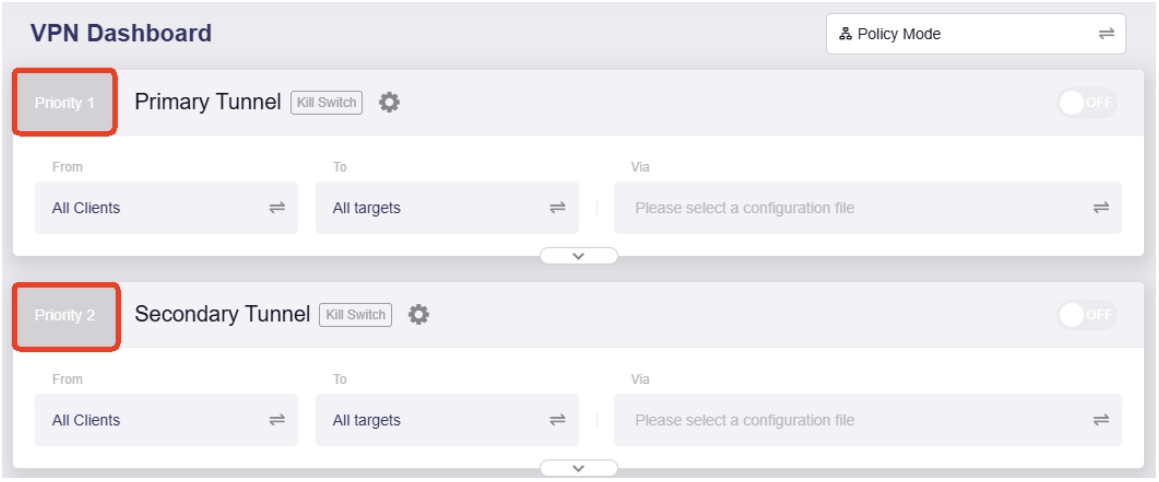
- **MTU** : la MTU définie pour le tunnel remplace celle du fichier de configuration.

9.2.2.5 Priorité des tunnels

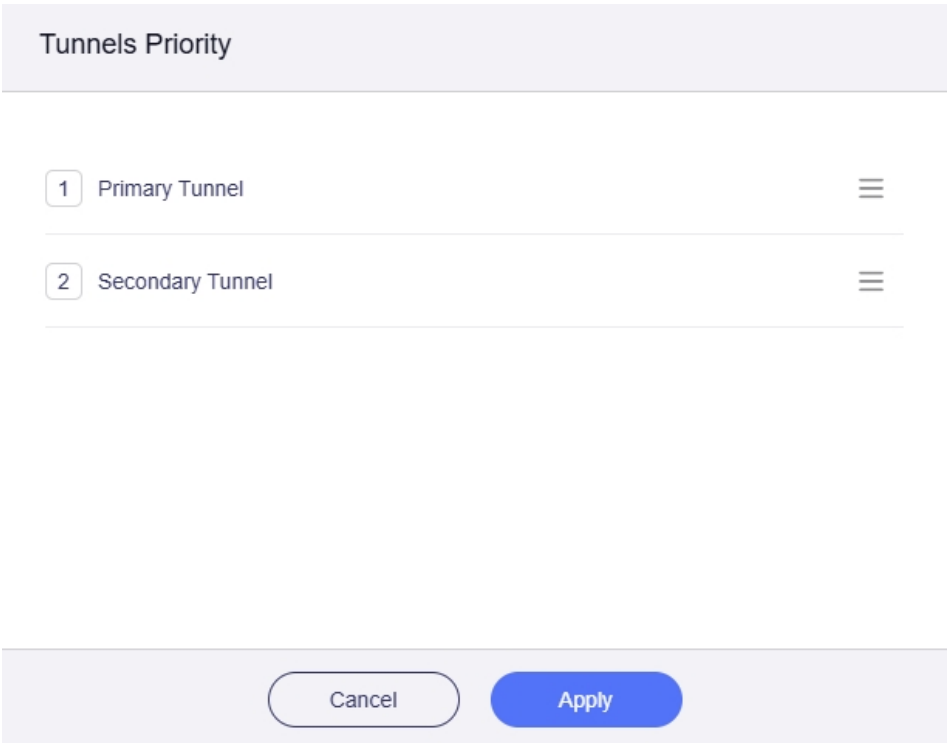
Par défaut, le tunnel principal a la priorité la plus élevée. Viennent ensuite les tunnels ajoutés manuellement, puis le tunnel prédéfini Tout autre trafic, qui assure la connexion via le réseau WAN du FAI local.

Pour modifier la priorité des tunnels, procédez comme suit.

1. Cliquez sur l'étiquette de priorité dans l'angle supérieur gauche d'un tunnel, par exemple Priorité 1 ou Priorité 2.



2. Dans la fenêtre qui s'affiche, maintenez l'icône à trois lignes située à droite et faites-la glisser pour réordonner le tunnel. Cliquez ensuite sur **Appliquer (Apply)**.



Lorsque plusieurs tunnels sont activés, le routeur achemine le trafic dans l'ordre suivant :

1. Il vérifie d'abord la règle du tunnel le plus prioritaire. Si le trafic correspond, il emprunte ce tunnel. Sinon, le routeur examine le tunnel de priorité suivante, et ainsi de suite jusqu'au tunnel « Tout autre trafic ».
2. Si un tunnel VPN se déconnecte de façon inattendue, le système décide de basculer ou non le trafic vers le tunnel suivant selon l'état du **coupe-circuit (Kill Switch)** de ce tunnel.
   - Si le coupe-circuit est activé, le trafic est bloqué et ne bascule pas vers le tunnel suivant.
   - Si le coupe-circuit est désactivé, le trafic bascule vers le tunnel suivant et ses règles sont examinées.
3. Le tunnel **Tout autre trafic (All Other Traffic)** est activé par défaut pour maintenir l'accès Internet du trafic ne correspondant à aucun tunnel VPN.
   - Lorsqu'il est activé, il achemine le trafic sans règle correspondante ou le trafic de secours via le WAN local.
   - Lorsqu'il est désactivé, il renforce le coupe-circuit et bloque l'accès Internet ordinaire pour éviter les fuites d'adresse IP.

Chapitre 10

Configuration d’un serveur VPN

Ce chapitre explique comment configurer un routeur GL.iNet comme serveur OpenVPN ou WireGuard.

10.1 Serveur OpenVPN

OpenVPN est un protocole VPN open source qui utilise le chiffrement SSL/TLS pour sécuriser les connexions point à point et site à site. Pour configurer un serveur OpenVPN sur un routeur GL.iNet, regardez cette vidéo ou suivez les étapes ci-dessous.

10.1.1 Préparation

1. **Vérifiez que vous disposez d'une adresse IP publique**

   Cliquez ici pour vérifier si votre fournisseur d'accès à Internet (FAI) vous attribue une adresse IP publique.

   Sans adresse IP publique, votre routeur ne peut pas servir de serveur OpenVPN.

   Autres solutions :

   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu'il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions ne fonctionnent pas, par exemple lorsque votre réseau est derrière un CGNAT, vous pouvez essayer notre solution SD-WAN AstroWarp.

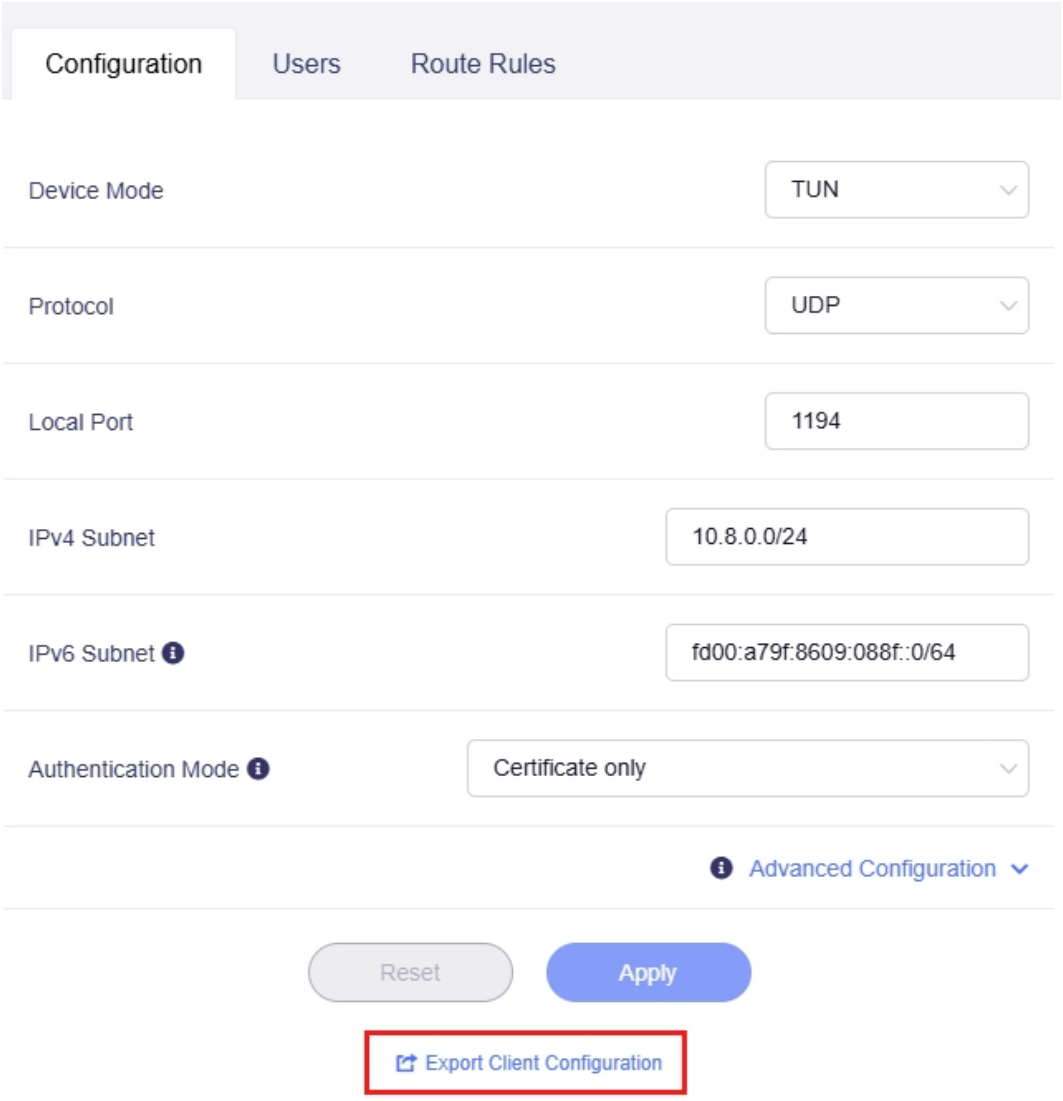
2. **Vérifiez si une redirection de port est nécessaire**

   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n'est nécessaire. Passez à l'étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs appareils intermédiaires séparent le routeur GL.iNet du routeur principal, configurez la redirection de port sur chacun d'eux.

10.1.2 Étapes de configuration

1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur OpenVPN (OpenVPN Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.

   La configuration par défaut convient à la plupart des situations. Cliquez sur **Exporter la configuration client (Export Client Configuration)** en bas de la page, puis passez à l'étape 3. Si vous avez modifié la configuration, cliquez sur **Appliquer (Apply)** avant de l'exporter.

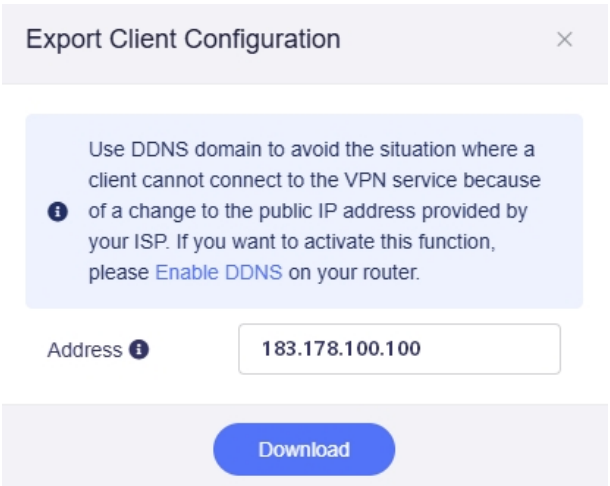


- **Mode de l'appareil (Device Mode)** : TAP-S2S ou Tun. Consultez cette page pour connaître les différences.

- **Protocole (Protocol)** : UDP ou TCP. Consultez cette page pour connaître les différences.
- **Mode d'authentification (Authentication Mode)** : détermine la méthode utilisée lors de la connexion du client au serveur. Trois options sont proposées :
  - **Certificat uniquement (Certificate Only)** : le routeur génère automatiquement les certificats et les clés du serveur et du client, puis les intègre au fichier de configuration. Aucun identifiant supplémentaire n'est requis lors de l'importation sur le client.
  - **Identifiant/mot de passe uniquement (Username/Password Only)** : le routeur génère une configuration client sans certificats ni clés. Ajoutez d'abord un identifiant et un mot de passe dans l'onglet **Utilisateurs (Users)**, puis exportez la configuration client. Renseignez ces identifiants lors de l'importation sur le client.
  - **Identifiant/mot de passe et certificat (Username/Password and Certificate)** : ajoutez d'abord un identifiant et un mot de passe dans l'onglet **Utilisateurs (Users)** avant d'exporter la configuration client. Le routeur génère également les certificats et les clés du serveur et du client et les intègre au fichier. Lors de l'importation sur le client, le certificat et la clé sont vérifiés avant l'authentification par identifiant et mot de passe, pour une sécurité à deux facteurs.
- **Configuration avancée (Advanced Configuration)** : personnalisez d'autres paramètres du serveur si nécessaire.

3. Exportez la configuration client.

   Cliquez sur **Exporter la configuration client (Export Client Configuration)** en bas de l'onglet Configuration, après avoir appliqué vos modifications éventuelles. Dans la fenêtre qui s'affiche, cliquez sur **Télécharger (Download)** pour exporter la configuration.

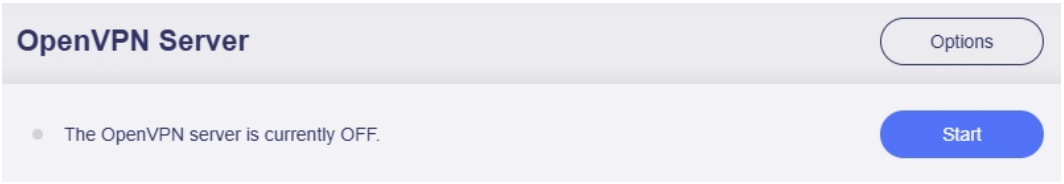


Conseils :

- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Depuis le micrologiciel v4.8, vous pouvez choisir l'adresse du serveur dans une liste avant d'exporter le fichier : IP publique, domaine DDNS ou adresse IP WAN actuelle. L'adresse est mise à jour automatiquement dans le fichier. Téléchargez de nouveau le fichier si l'adresse du serveur change.

4. Démarrez le serveur OpenVPN.

   Sur la page **Serveur OpenVPN (OpenVPN Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



   L'état de connexion apparaît en haut de la page. Si les statistiques de trafic montant et descendant s'affichent, le serveur OpenVPN fonctionne.

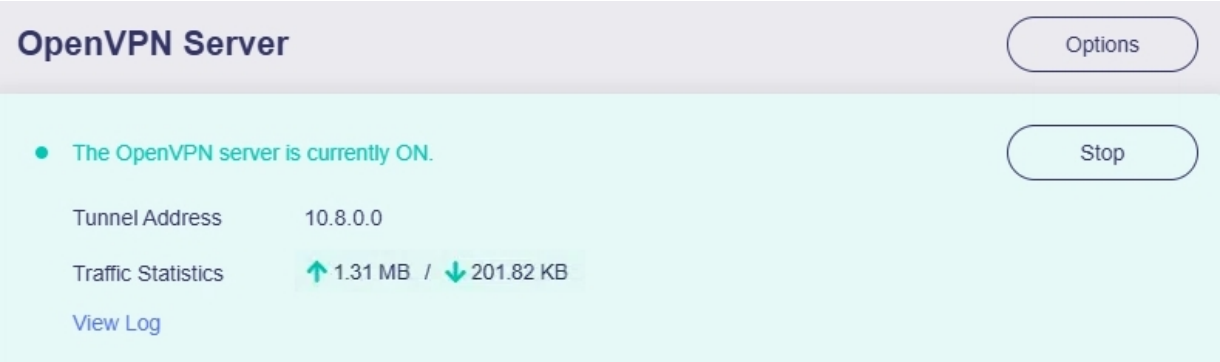


10.1.3 Vérification de la connexion

Méthode 1 : vérification de l'état du serveur

Avec le micrologiciel v4.8, vous pouvez vérifier l'état de la connexion sur la page **Serveur OpenVPN (OpenVPN Server)**.

Si des statistiques de trafic montant et descendant s'affichent, le serveur OpenVPN fonctionne.



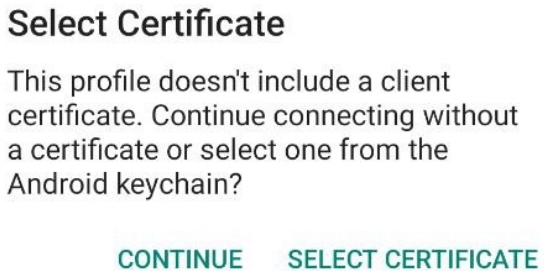
Méthode 2 : vérification de l'adresse IP du client

Importez la configuration OpenVPN exportée précédemment sur un appareil connecté à un autre réseau que le réseau local du serveur. Ouvrez ensuite un navigateur Web et recherchez votre adresse IP et votre localisation. Si elles correspondent à celles du serveur VPN, au lieu de celles de votre fournisseur d'accès à Internet, la connexion VPN est établie.

L'exemple suivant utilise un smartphone sur lequel l'application officielle OpenVPN est installée.

1. Désactivez d'abord le Wi-Fi du smartphone et utilisez uniquement les données cellulaires 4G/5G.
2. Ouvrez ensuite l'application OpenVPN, importez le fichier de configuration et lancez la connexion.
3. Vérifiez que le smartphone accède à Internet et que son adresse IP correspond à celle du serveur OpenVPN.

   Conseil : lors de l'importation du fichier dans l'application OpenVPN, le message ci-dessous peut s'afficher. Cliquez sur **CONTINUER (CONTINUE)**, car le certificat est déjà intégré au fichier de configuration.



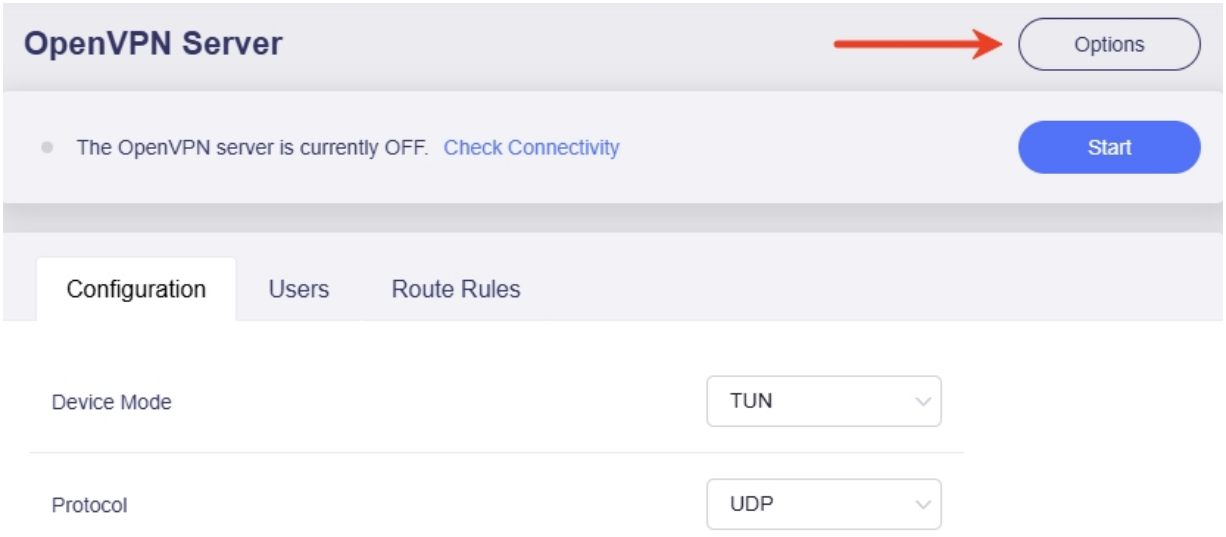
Voici les causes courantes d'un échec de connexion :

- Le serveur VPN ne dispose pas d'une adresse IP publique. Consultez la section **10.1.1 Préparation** pour en savoir plus.
- Une redirection de ports peut être nécessaire. Consultez la section **10.1.1 Préparation** pour en savoir plus.
- Votre FAI bloque le port utilisé par le serveur OpenVPN. Choisissez un autre port ou contactez votre FAI.
- La connexion VPN peut être bloquée dans certains pays ou certaines régions.

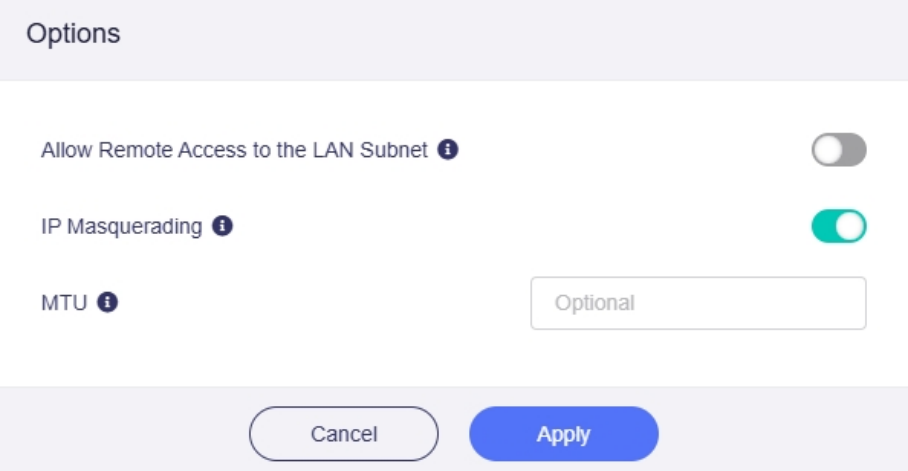
10.1.4 Options du serveur

Les options du serveur proposent des paramètres avancés, comme l'accès à distance au LAN du serveur et le masquage IP. Configurez-les selon vos besoins.

Sur la page **Serveur OpenVPN (OpenVPN Server)**, cliquez sur **Options** dans l'angle supérieur droit.



Les fonctions suivantes s'affichent dans la fenêtre.



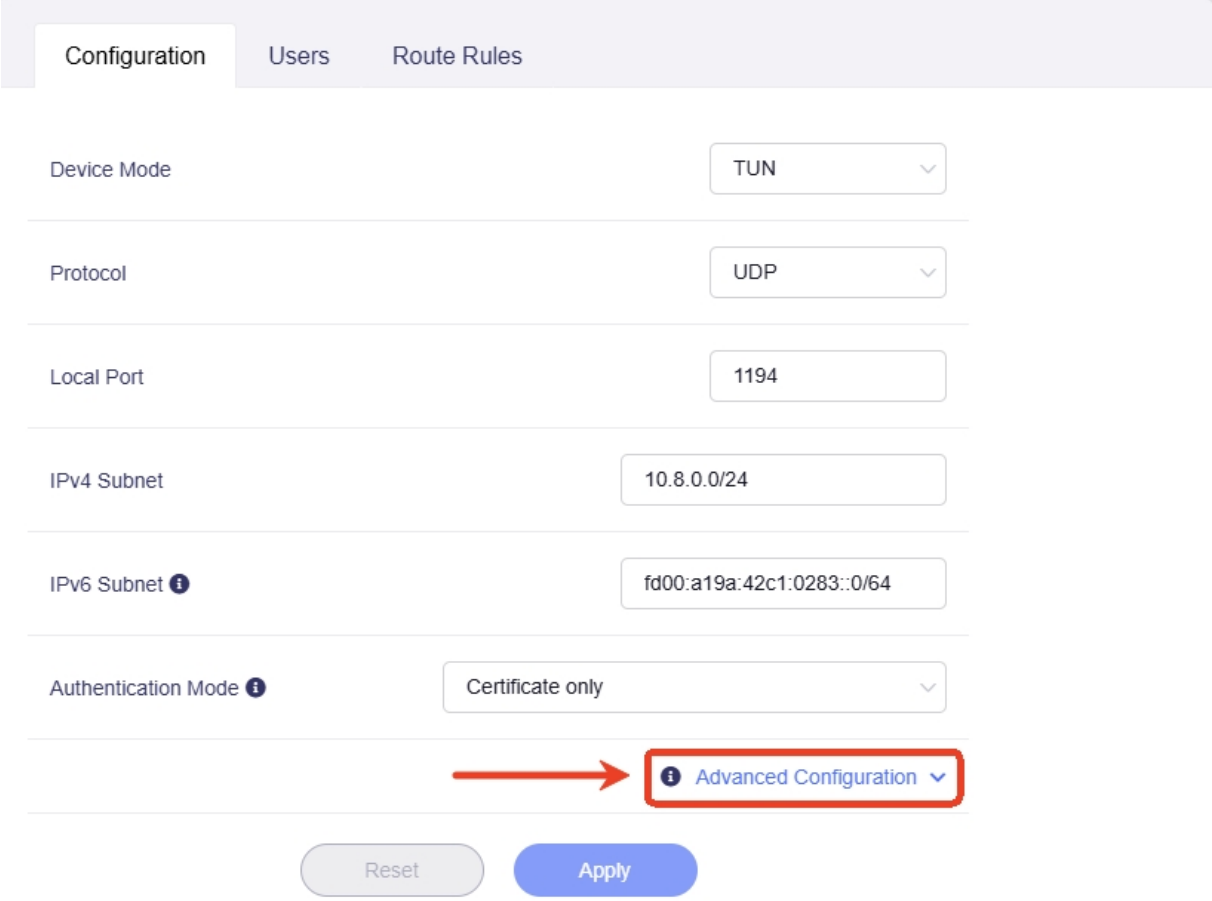
- **Autoriser l'accès distant au sous-réseau LAN (Allow Remote Access to the LAN Subnet)** : lorsque cette option est activée, les ressources du sous-réseau LAN du serveur sont accessibles par le tunnel VPN.
- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l'IP du tunnel VPN du routeur. Ne désactivez cette option que pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.
- **MTU** : unité de transmission maximale (Maximum Transmission Unit). La valeur choisie pour le tunnel remplace les paramètres MTU du fichier de configuration.

10.1.5 Communication entre clients

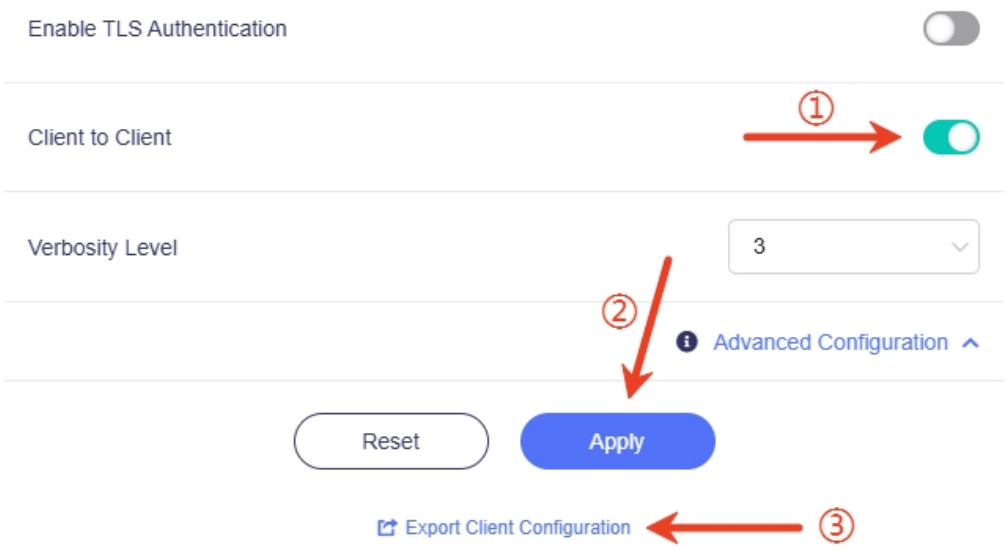
La communication entre clients est une fonction du serveur VPN. Lorsqu'elle est activée, les clients VPN connectés peuvent communiquer entre eux à l'aide de leurs adresses IP respectives dans le tunnel VPN.

Si nécessaire, procédez comme suit pour activer cette fonction sur le serveur OpenVPN.

1. Sur la page **Serveur OpenVPN (OpenVPN Server)**, cliquez sur **Configuration avancée (Advanced Configuration)** dans l'angle inférieur droit.



2. Activez **Communication entre clients (Client to Client)** et cliquez sur **Appliquer (Apply)**. Exportez ensuite une nouvelle configuration et importez-la sur les clients OpenVPN.



Conseil : cette fonction annonce uniquement l’adresse IP de chaque client dans le tunnel. Elle ne rend pas automatiquement accessibles les sous-réseaux LAN situés derrière les clients VPN. Pour permettre aux clients d’accéder aux sous-réseaux LAN des autres clients, ajoutez des règles de routage sur le serveur VPN annonçant ces sous-réseaux distants.

10.2 Serveur WireGuard

WireGuard® est un VPN particulièrement simple, rapide et moderne, qui utilise une cryptographie de pointe. Il vise à être plus rapide, plus simple, plus léger et plus pratique qu'IPSec, sans sa complexité, tout en offrant des performances nettement supérieures à celles d'OpenVPN.
*WireGuard® est une marque déposée de Jason A. Donenfeld.

Pour configurer un serveur WireGuard sur un routeur GL.iNet, regardez cette vidéo ou suivez les étapes ci-dessous.

10.2.1 Préparation

1. **Vérifiez que vous disposez d'une adresse IP publique**

   Cliquez ici pour vérifier si votre fournisseur d'accès à Internet vous attribue une adresse IP publique.

   Sans adresse IP publique, votre routeur ne peut pas servir de serveur WireGuard.

   Autres solutions :

   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu'il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions ne fonctionnent pas, par exemple lorsque votre réseau est derrière un CGNAT, vous pouvez essayer notre solution SD-WAN AstroWarp.

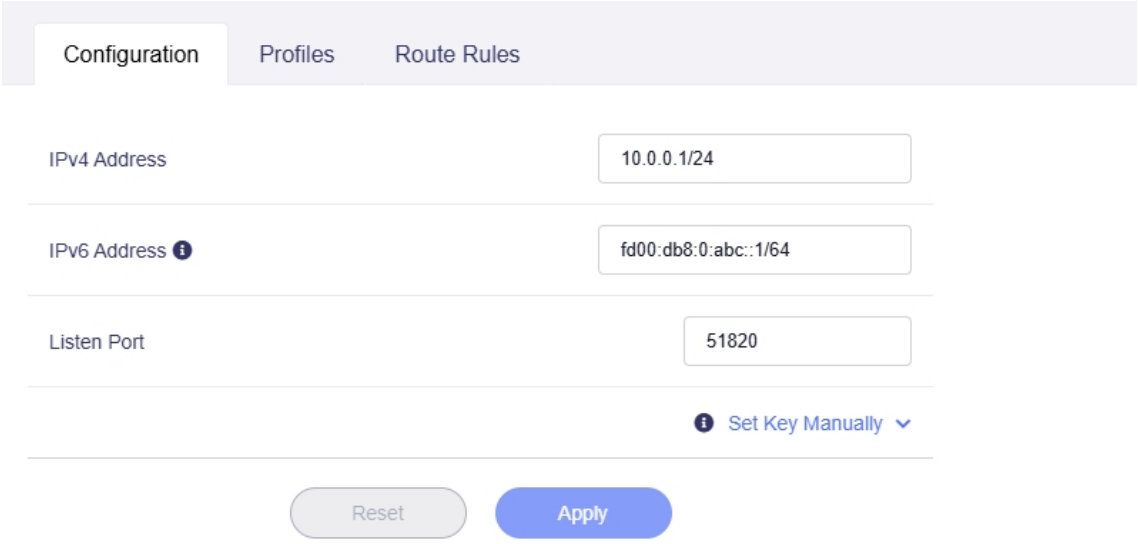
2. **Vérifiez si une redirection de port est nécessaire**

   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n'est nécessaire. Passez à l'étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs appareils intermédiaires séparent le routeur GL.iNet du routeur principal, configurez la redirection de port sur chacun d'eux.

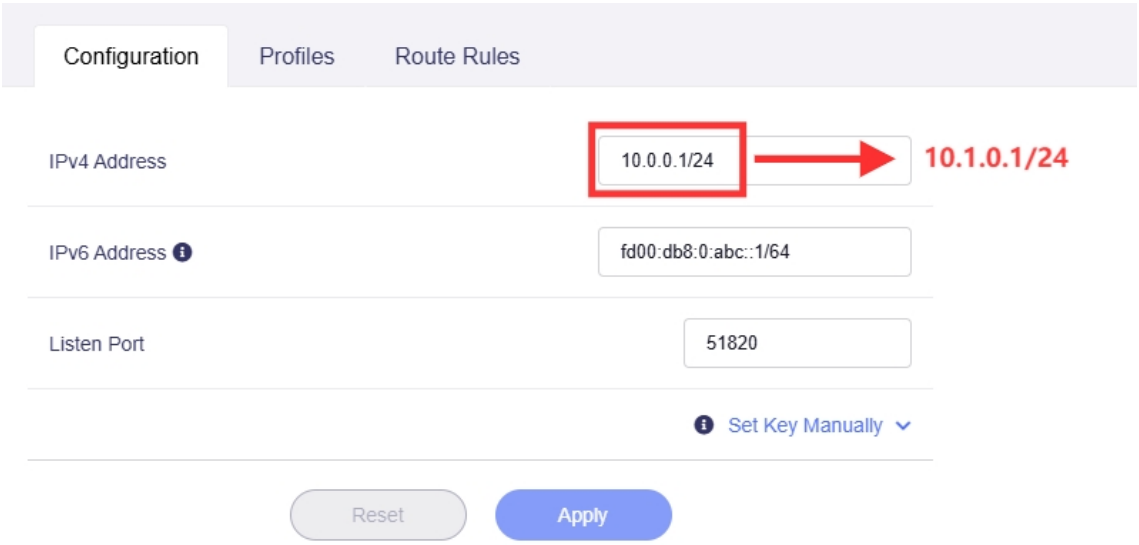
10.2.2 Étapes de configuration

1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur WireGuard (WireGuard Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.

   La configuration par défaut convient à la plupart des situations. Ne modifiez l'adresse IPv4 que si elle entre en conflit avec la passerelle du routeur en amont.

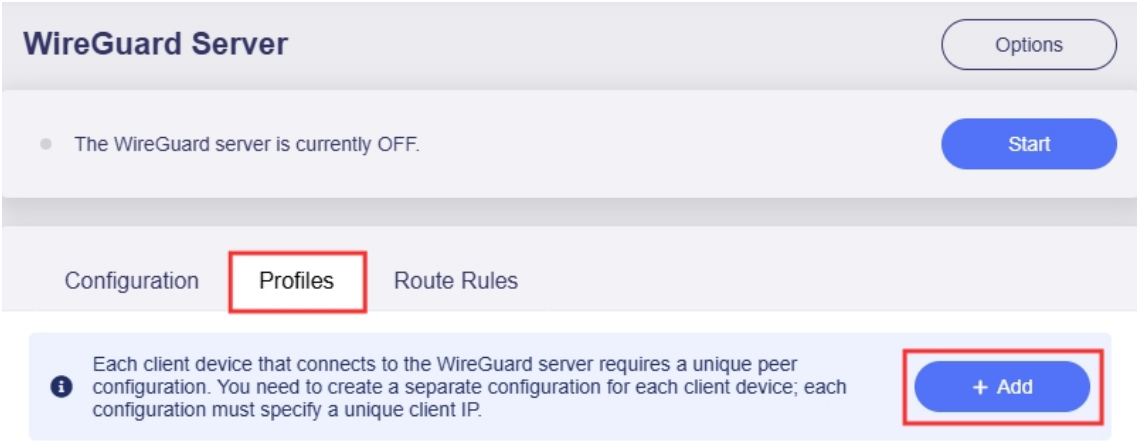


   En cas de conflit, choisissez une autre adresse IPv4, par exemple **10.1.0.1/24**, puis cliquez sur **Appliquer (Apply)**. Conservez la notation CIDR « /24 » pour éviter les problèmes de connexion.

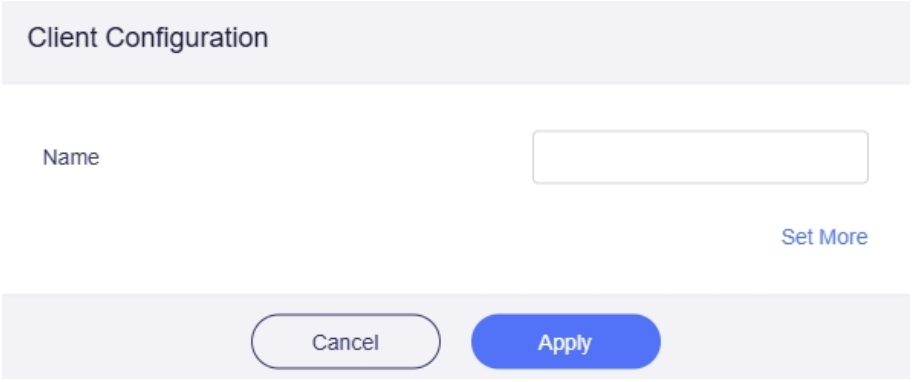


3. Ajoutez un profil.

Ouvrez l'onglet **Profils (Profiles)**, puis cliquez sur **Ajouter (Add)** pour générer un profil pour votre appareil.



Saisissez un nom explicite et cliquez sur **Appliquer (Apply)** pour continuer.



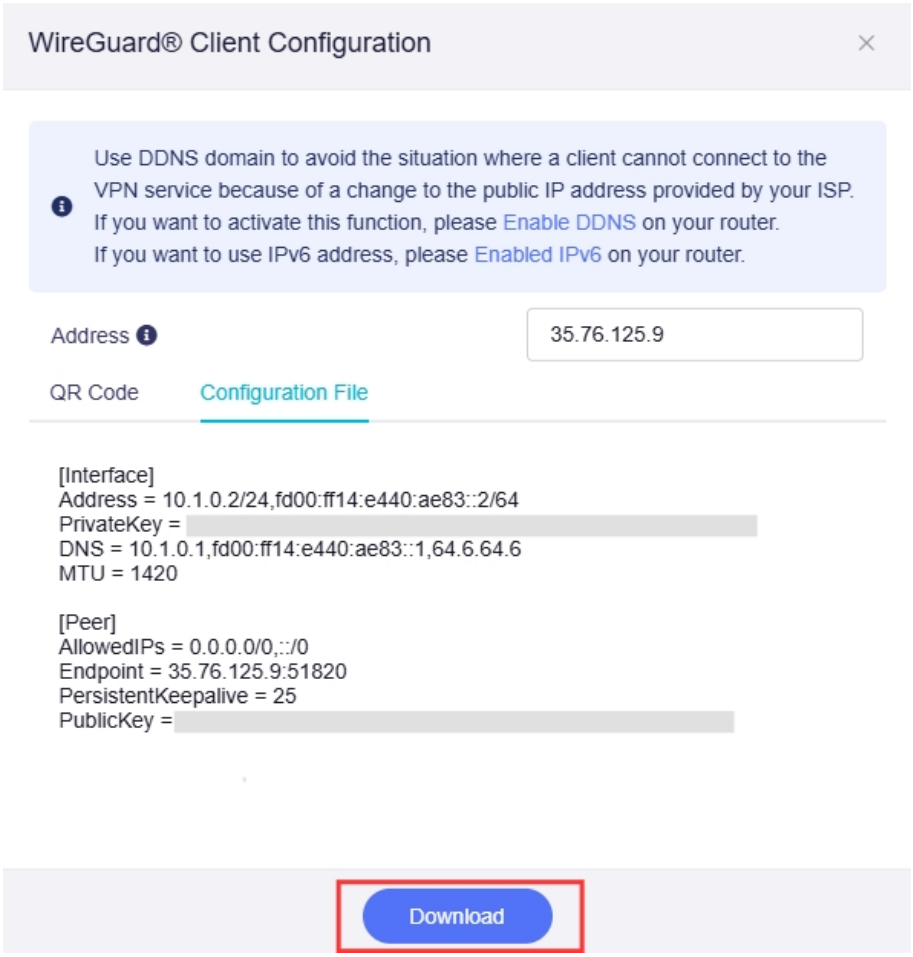
Conseil : pour accéder aux appareils du LAN du client WireGuard depuis le serveur WireGuard, configurez les routes dans l'onglet **Règles de routage (Route Rules)**. Consultez cette page pour en savoir plus.

4. Téléchargez la configuration.

   Après l'ajout du profil, le routeur génère la configuration sous trois formes : code QR, texte brut et fichier .conf. Choisissez la méthode qui vous convient.

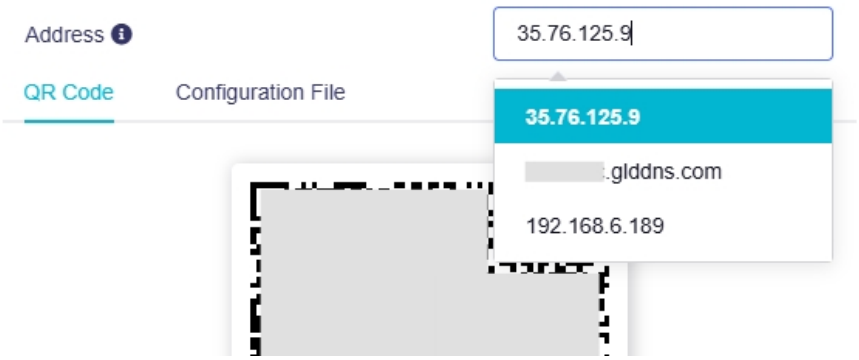
   - **Code QR** : adapté aux appareils disposant de l'application WireGuard, comme les smartphones, tablettes et ordinateurs portables. Ouvrez l'application WireGuard sur l'appareil à configurer comme client et scannez le code QR pour importer la configuration.
   - **Texte brut** : permet de consulter la configuration et de la copier-coller ailleurs pour une configuration manuelle, par exemple dans l'application WireGuard ou sur un routeur GL.iNet.

- **Fichier .conf** : cliquez sur **Télécharger (Download)** pour enregistrer le fichier .conf sur votre appareil. Vous pouvez ensuite l'importer directement dans l'application WireGuard ou sur un routeur GL.iNet.



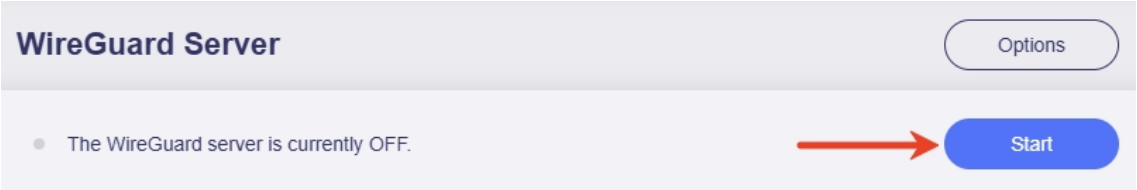
Conseils :

- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Depuis le micrologiciel v4.8, vous pouvez choisir l'adresse du serveur dans une liste avant d'exporter le fichier : IP publique, domaine DDNS ou adresse IP WAN actuelle. L'adresse est mise à jour automatiquement dans le fichier. Téléchargez de nouveau le fichier si l'adresse du serveur change.

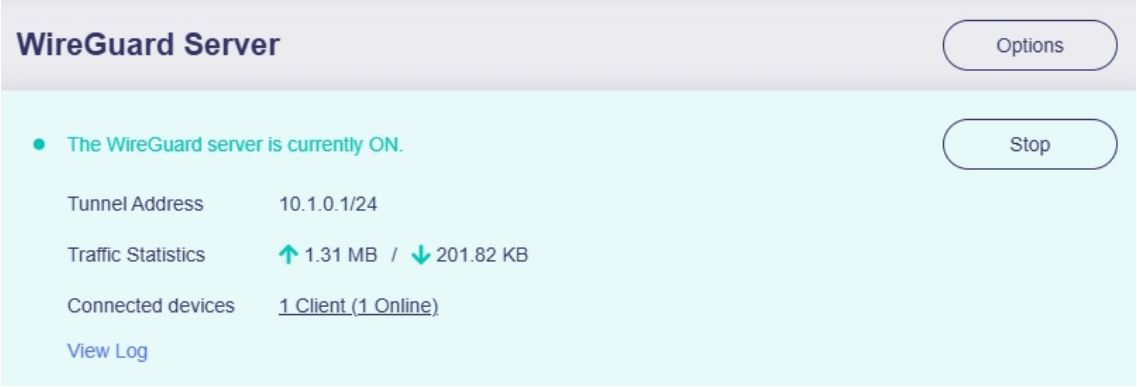


5. Démarrez le serveur WireGuard.

   Sur la page **Serveur WireGuard (WireGuard Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



   L'état de connexion apparaît en haut de la page. Si les statistiques de trafic montant et descendant et les appareils connectés s'affichent, le serveur WireGuard fonctionne.

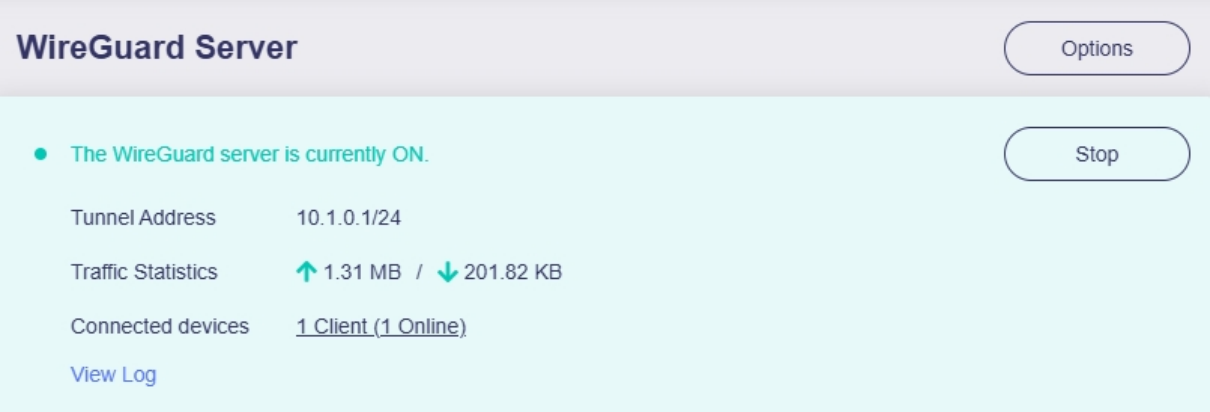


10.2.3 Vérification de la connexion

Méthode 1 : vérification de l’état du serveur

Avec le micrologiciel v4.8, vous pouvez vérifier l’état de la connexion sur la page **Serveur WireGuard (WireGuard Server)**.

Si des statistiques de trafic montant et descendant ainsi que des appareils connectés en ligne s’affichent, le serveur WireGuard fonctionne et des clients WireGuard y sont connectés.



Si le trafic et le nombre de clients sont tous deux à zéro, aucun client WireGuard n’est connecté.



Méthode 2 : vérification de l’adresse IP du client

Importez la configuration WireGuard exportée précédemment sur un appareil connecté à un autre réseau que le réseau local du serveur. Ouvrez ensuite un navigateur Web et recherchez votre adresse IP et votre localisation. Si elles correspondent à celles du serveur VPN, au lieu de celles de votre fournisseur d’accès à Internet, la connexion VPN est établie.

L’exemple suivant utilise un smartphone sur lequel l’application officielle WireGuard est installée.

1. Désactivez d’abord le Wi-Fi du smartphone et utilisez uniquement les données cellulaires 4G/5G.

2. Ouvrez ensuite l’application WireGuard, importez le fichier de configuration et lancez la connexion.
3. Vérifiez que le smartphone accède à Internet et que son adresse IP correspond à celle du serveur WireGuard.

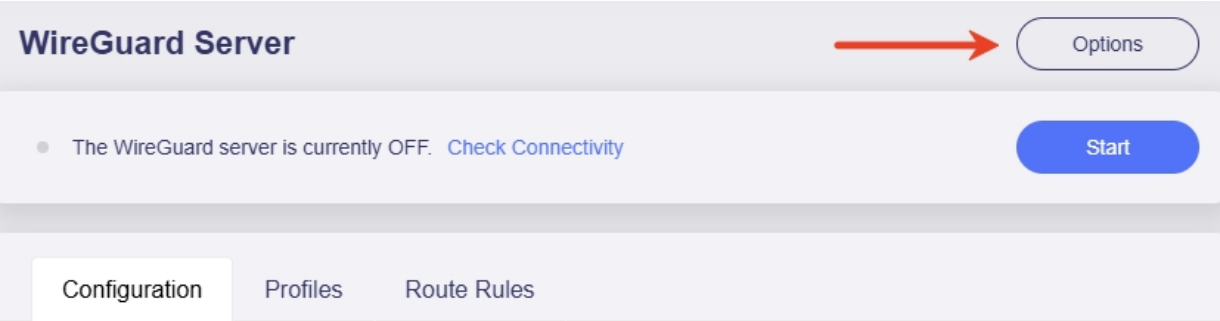
Voici les causes courantes d’un échec de connexion :

- Le serveur VPN ne dispose pas d’une adresse IP publique. Consultez la section **10.2.1 Préparation** pour en savoir plus.
- Une redirection de ports peut être nécessaire. Consultez la section **10.2.1 Préparation** pour en savoir plus.
- Le port utilisé par le Serveur WireGuard (WireGuard Server) est bloqué par votre fournisseur d’accès à Internet. Choisissez un autre port ou contactez votre FAI.
- La connexion VPN peut être bloquée dans certains pays ou certaines régions.

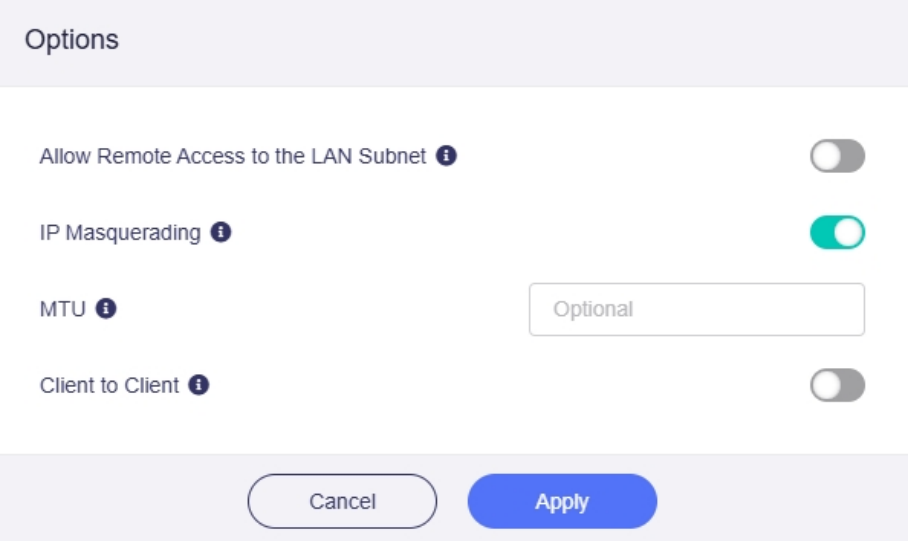
10.2.4 Options du serveur

Les options du serveur proposent des paramètres avancés, comme l’accès à distance au LAN du serveur et le masquage IP. Configurez-les selon vos besoins.

Sur la page **Serveur WireGuard (WireGuard Server)**, cliquez sur **Options** dans l’angle supérieur droit.



Les fonctions suivantes s’affichent dans la fenêtre.



- **Autoriser l’accès distant au sous-réseau LAN (Allow Remote Access to the LAN Subnet)** : lorsque cette option est activée, les ressources du sous-réseau LAN du serveur sont accessibles par le tunnel VPN.
- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l’IP du tunnel VPN du routeur. Ne désactivez cette option que pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.
- **MTU** : unité de transmission maximale (Maximum Transmission Unit). La valeur choisie pour le tunnel remplace les paramètres MTU du fichier de configuration.
- **Communication entre clients (Client to Client)** : lorsque cette option est activée, les clients VPN connectés à ce serveur peuvent communiquer entre eux à l’aide de leurs adresses IP respectives dans le tunnel VPN.
  Cette fonction annonce uniquement l’adresse IP de chaque client dans le tunnel. Elle ne rend pas automatiquement accessibles les sous-réseaux LAN situés derrière les clients VPN. Pour permettre aux clients d’accéder aux sous-réseaux LAN des autres clients, ajoutez des règles de routage sur le serveur VPN annonçant ces sous-réseaux distants.

Chapitre 11

Configuration d’un client VPN

Ce chapitre explique comment configurer un routeur GL.iNet comme client OpenVPN ou WireGuard.

11.1 Client OpenVPN

11.1.1 Préparation

Vérifiez d'abord que vous disposez d'un abonnement actif auprès d'un fournisseur VPN prenant en charge la configuration manuelle d'OpenVPN. Consultez cette page pour connaître les fournisseurs OpenVPN compatibles avec GL.iNet.

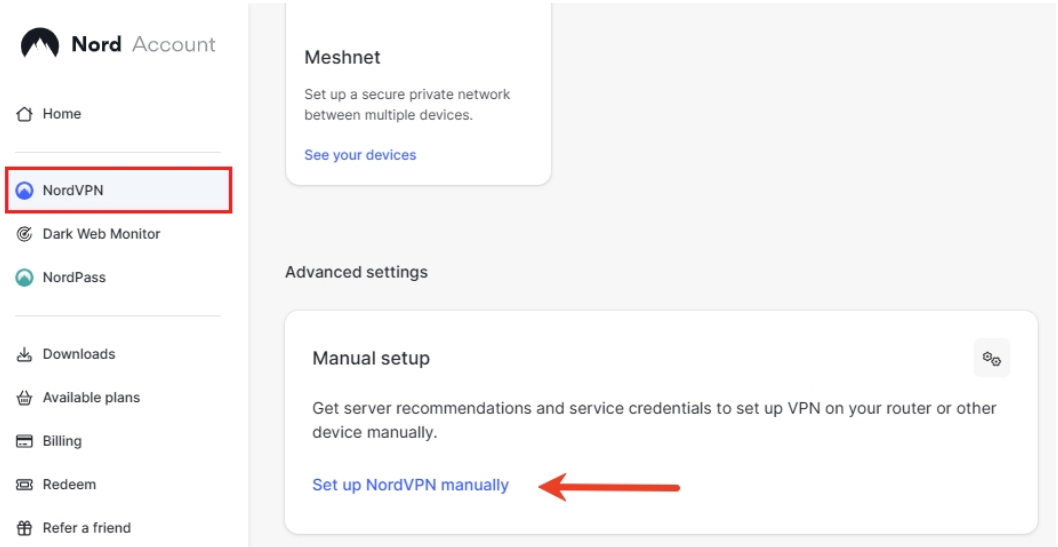
Rendez-vous ensuite sur le site officiel de votre fournisseur VPN pour obtenir les identifiants de service ou le fichier de configuration. Si vous ne savez pas comment obtenir ce fichier, consultez ce lien ou contactez l'assistance du fournisseur.

11.1.2 Configuration de NordVPN

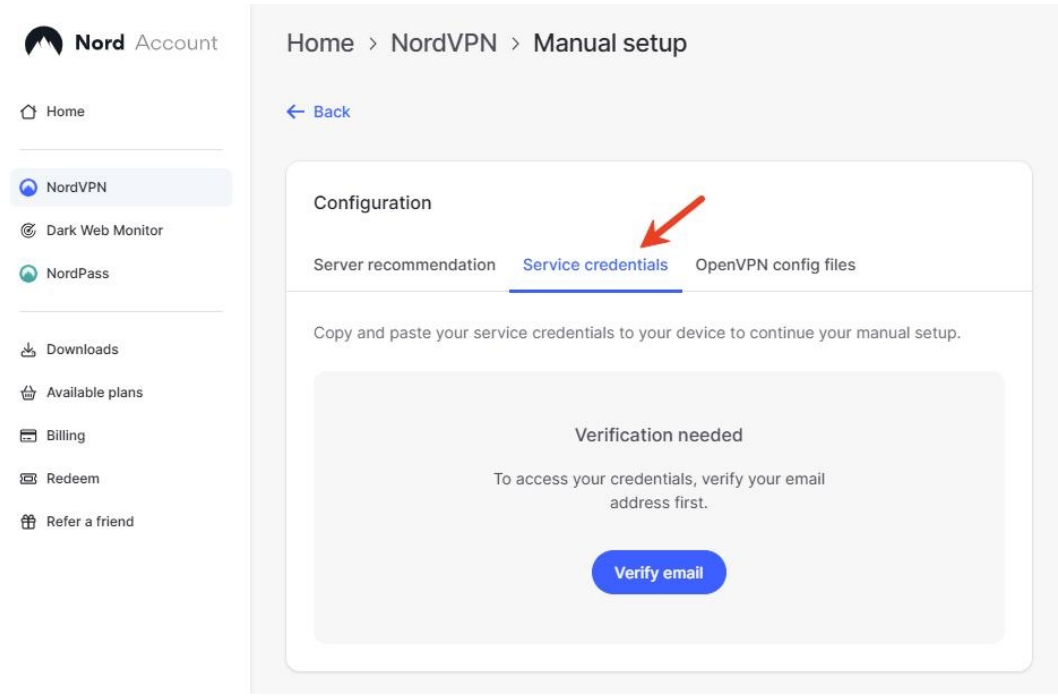
NordVPN est intégré à l'interface d'administration Web GL.iNet. Saisissez les identifiants obtenus dans le tableau de bord NordVPN dans l'interface du routeur ou dans l'application mobile GL.iNet pour récupérer les fichiers de configuration de tous les serveurs NordVPN, sans importation manuelle.

Suivez les étapes ci-dessous pour configurer le routeur comme client NordVPN.

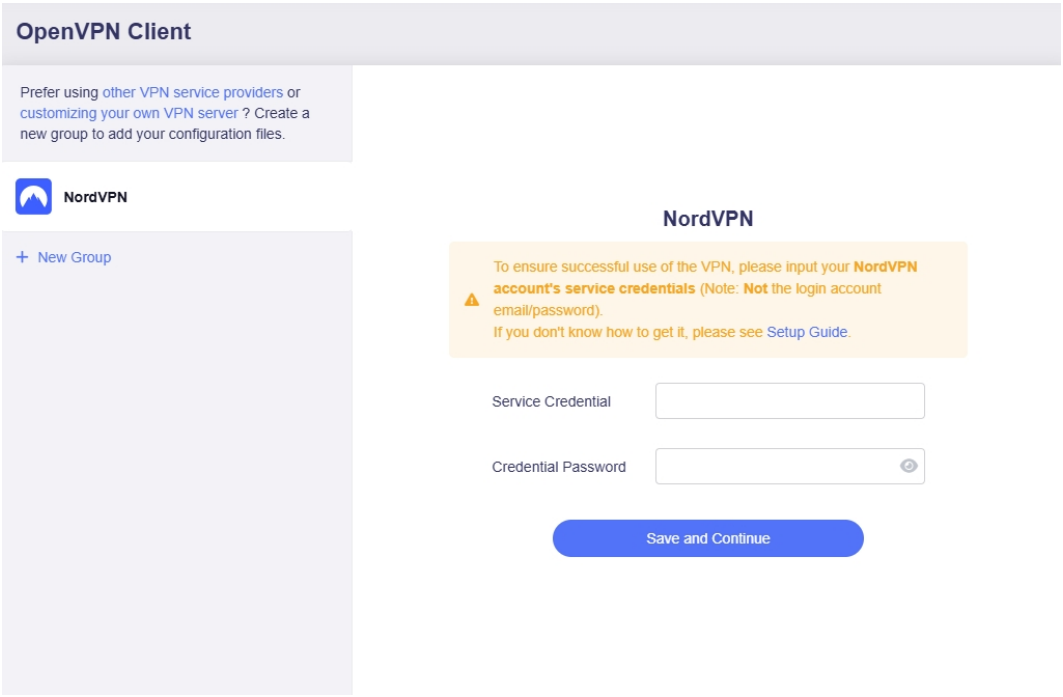
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



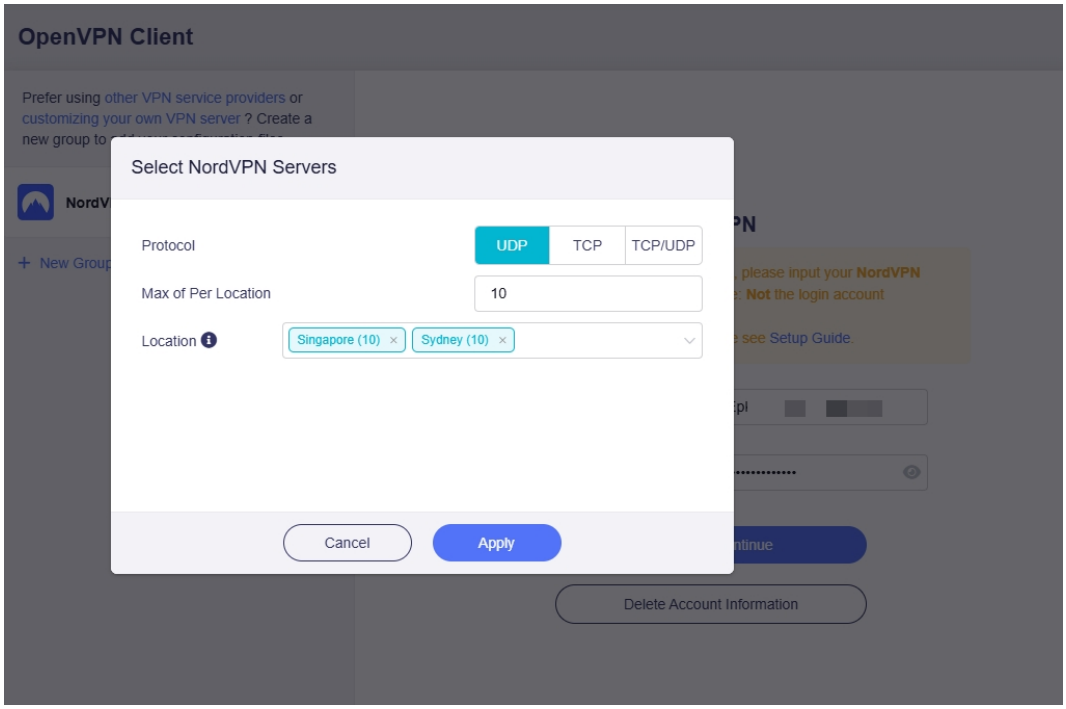
Repérez les **identifiants de service (service credentials)** et copiez-les pour les utiliser ensuite.



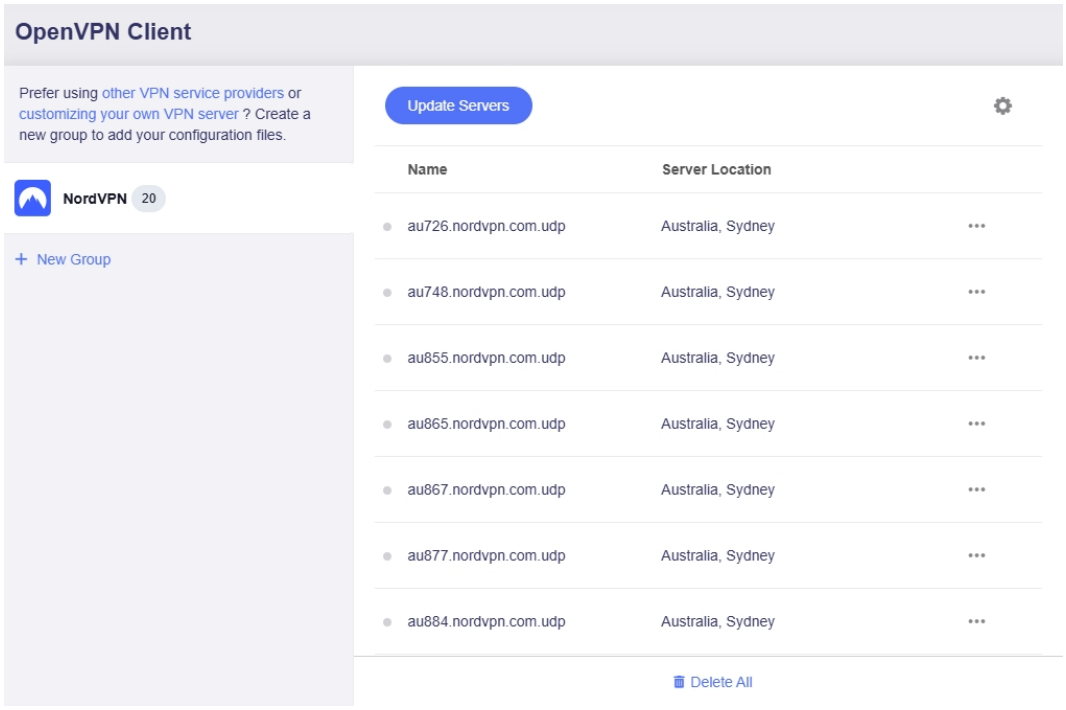
3. Dans l'interface d'administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** > **NordVPN**. Saisissez les identifiants de service, qui ne sont PAS l'adresse e-mail et le mot de passe de connexion au compte, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



4. Choisissez le protocole, le nombre maximal de serveurs par emplacement et les emplacements, puis cliquez sur **Appliquer (Apply)**.

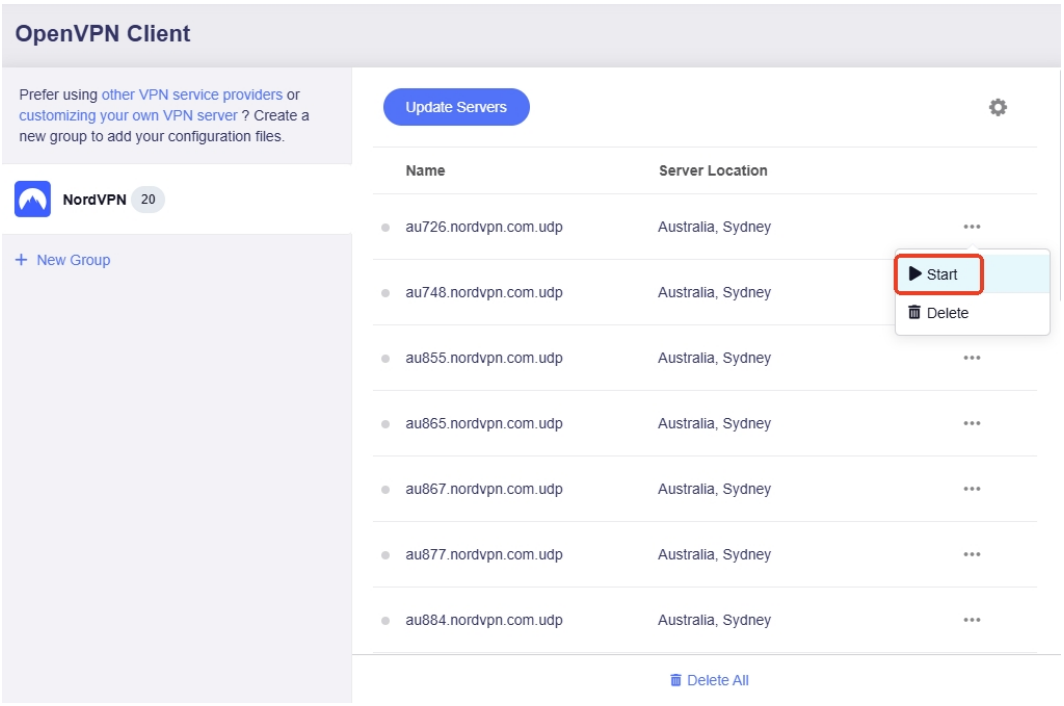


Les fichiers de configuration sont téléchargés.

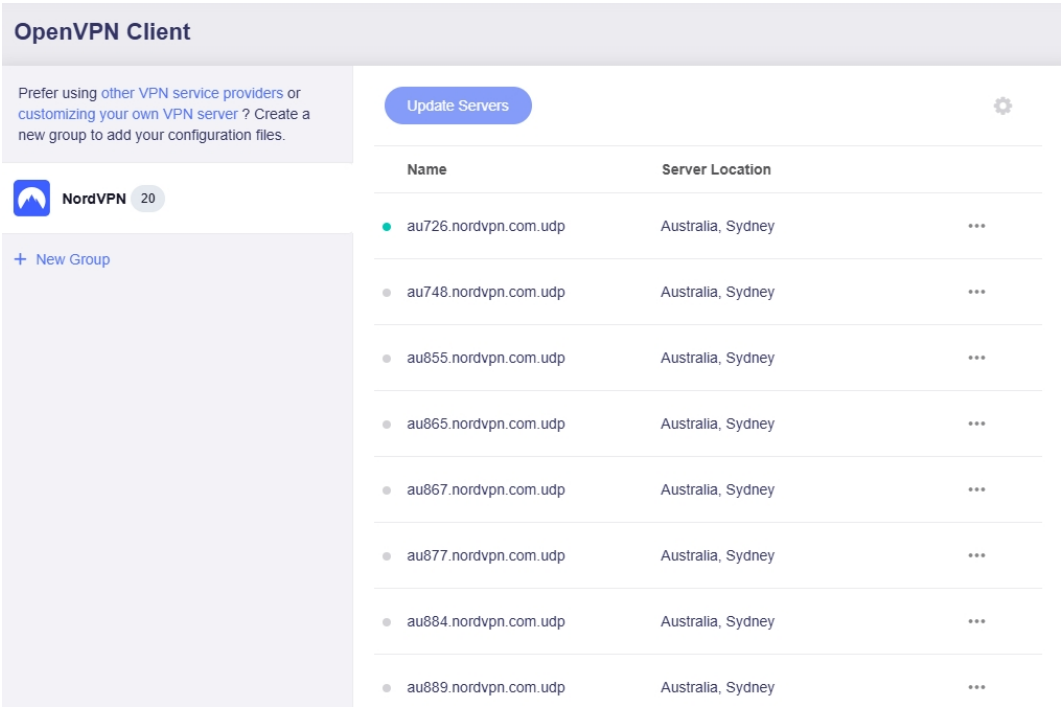


5. Établissez une connexion.

   Sélectionnez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



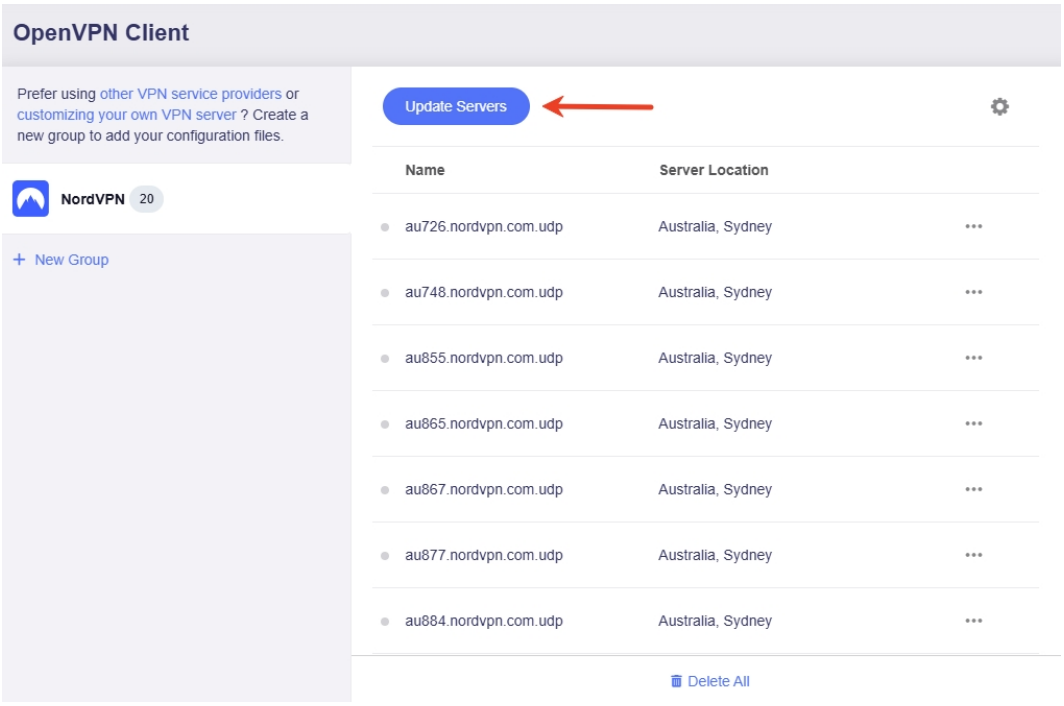
6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

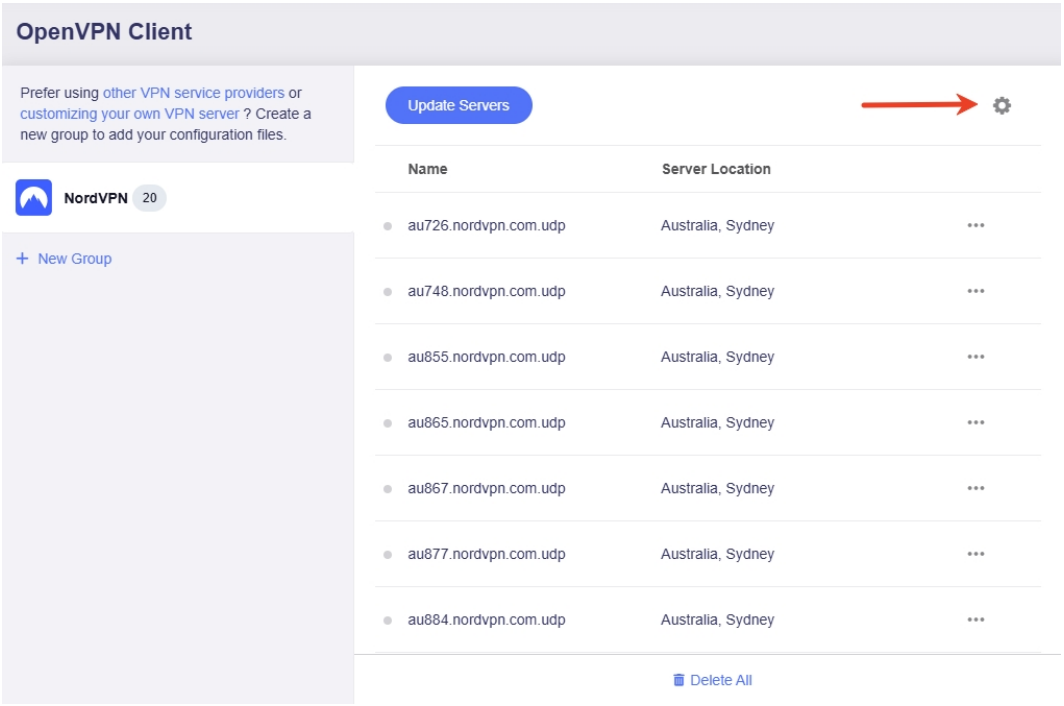
7. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



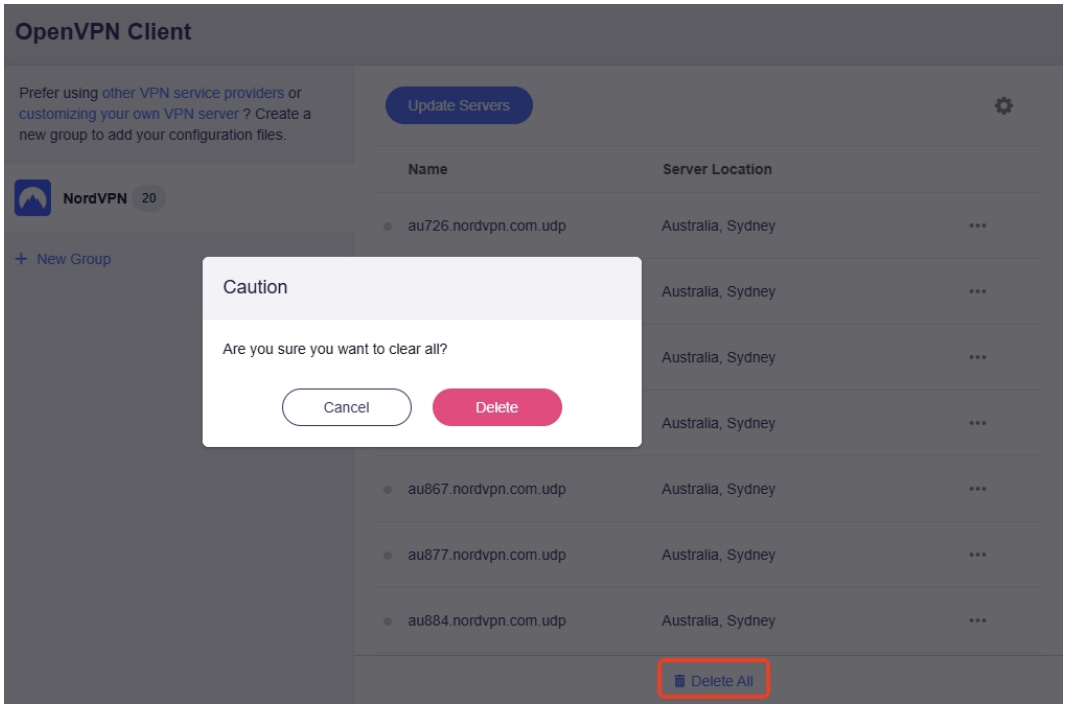
8. Modifiez les identifiants.

   Cliquez sur l'engrenage pour modifier vos identifiants de connexion.



9. Supprimez tous les fichiers.

Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic.

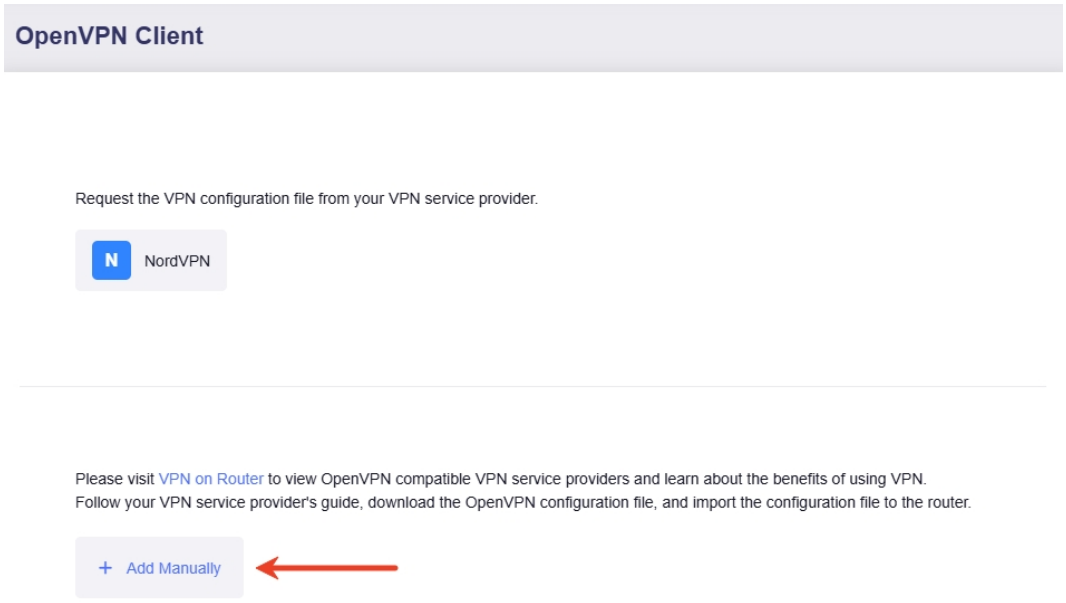


11.1.3 Configuration manuelle d’un client OpenVPN pour un autre fournisseur

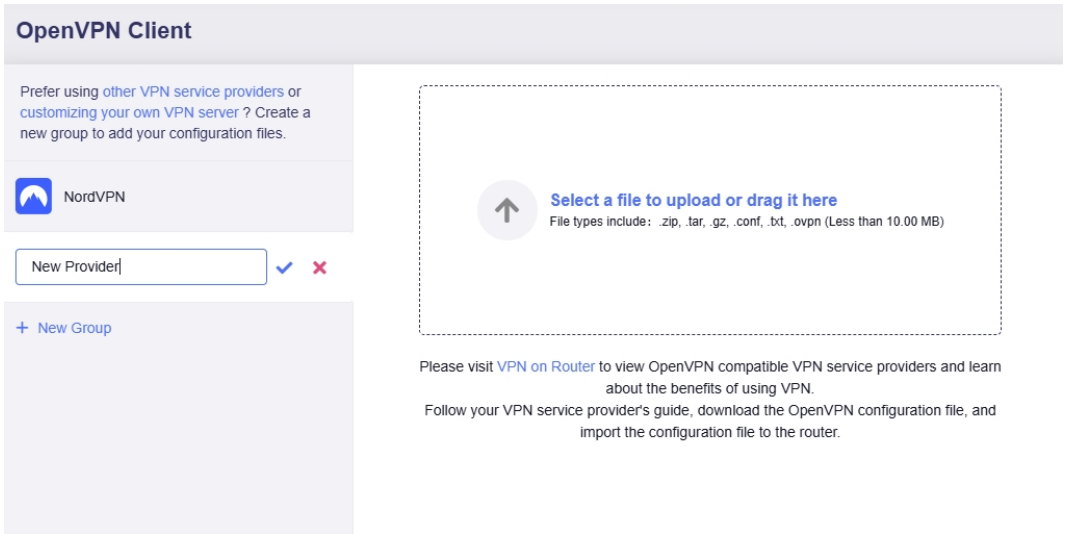
Si votre fournisseur OpenVPN n’est pas intégré à notre interface, récupérez d’abord le fichier de configuration sur son site officiel. Importez-le ensuite sur le routeur pour configurer le client OpenVPN.

Dans les étapes suivantes, nous prenons PIA (Private Internet Access) comme exemple.

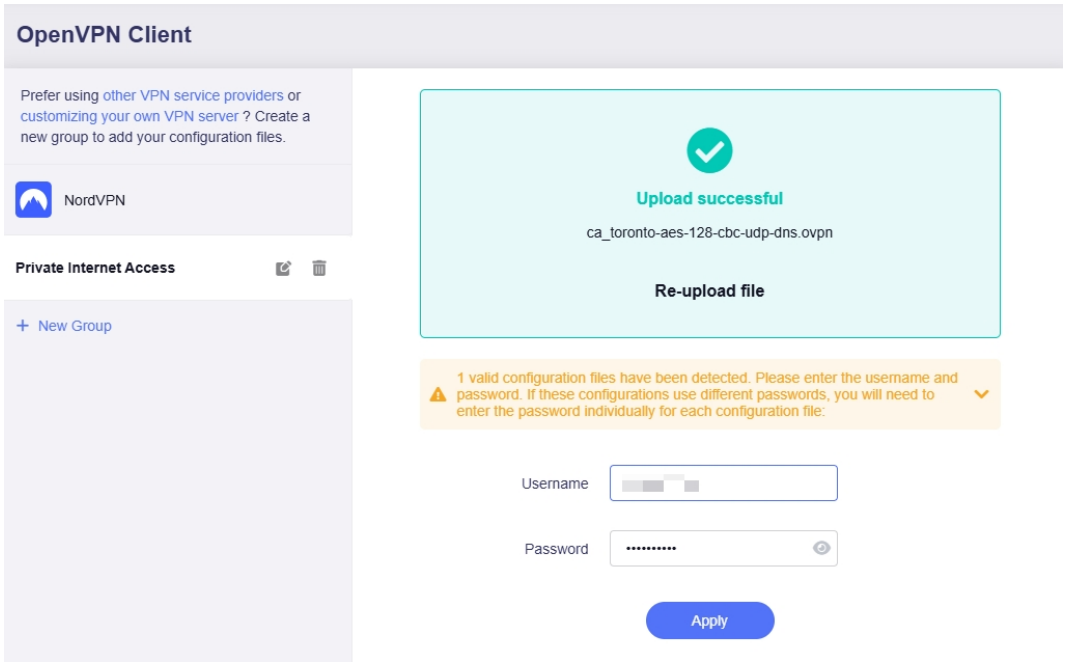
1. Téléchargez un fichier de configuration sur le site officiel de Private Internet Access.
2. Dans l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)**, puis cliquez sur **Ajouter manuellement (Add Manually)**.



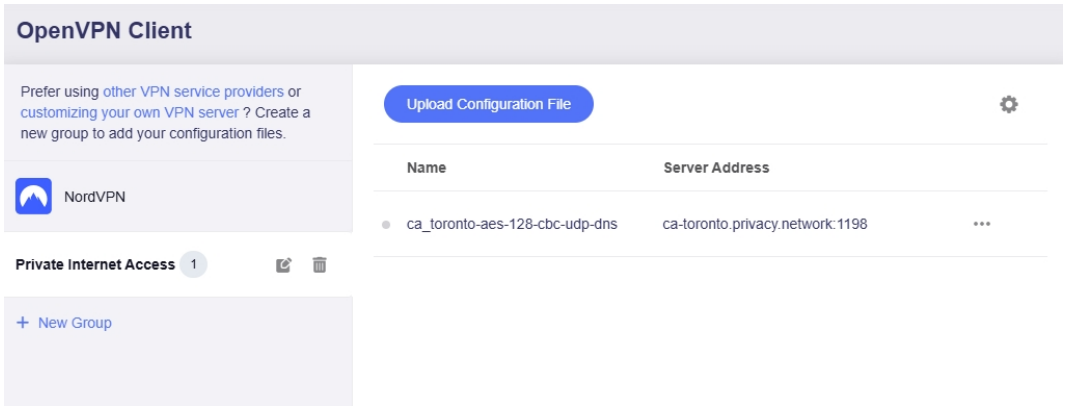
3. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



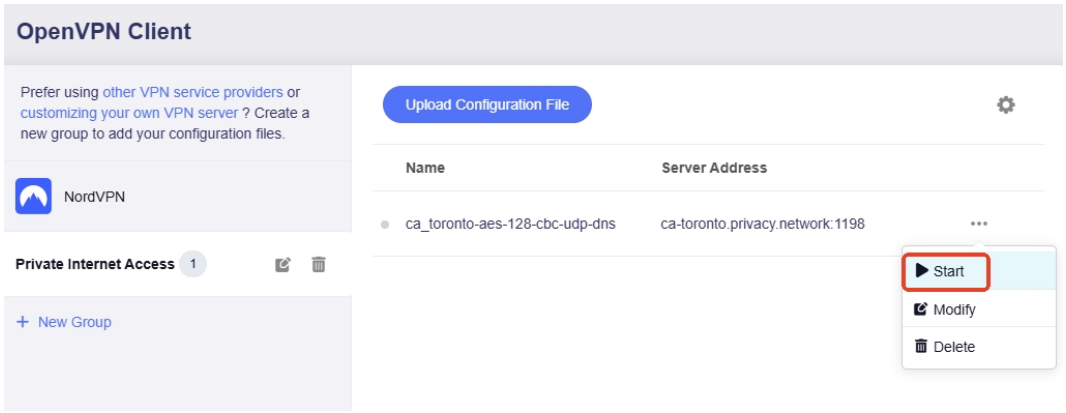
4. Importez votre fichier de configuration OpenVPN. Saisissez les identifiants si nécessaire, puis cliquez sur **Appliquer (Apply)**.



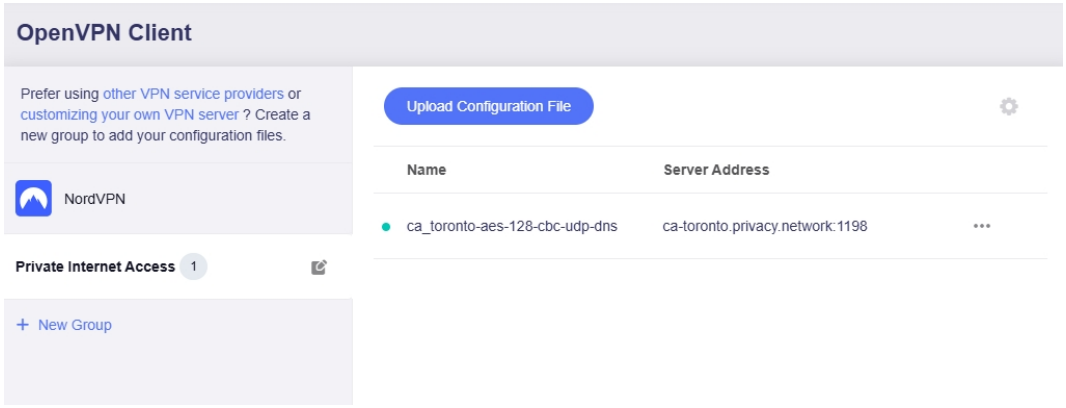
Le fichier importé apparaît dans la liste.



5. Cliquez sur les trois points à droite pour lancer la connexion.



6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

11.2 Configuration d’un client WireGuard

Vous pouvez configurer le client WireGuard® via l’application mobile GL.iNet ou l’interface d’administration Web.

- L’application mobile intègre plusieurs fournisseurs WireGuard, comme AzireVPN, Mullvad VPN, OVPN, StrongVPN et PIA VPN. Pour configurer le service, saisissez les identifiants de votre abonnement. Ouvrez l’application et suivez les instructions à l’écran.
- L’interface Web intègre également plusieurs fournisseurs WireGuard et propose une configuration manuelle. Saisissez les identifiants de votre abonnement pour une configuration rapide ou importez manuellement un fichier de configuration.

*WireGuard® est une marque déposée de Jason A. Donenfeld.

11.2.1 Préparation

Vérifiez d’abord que vous disposez d’un abonnement actif auprès d’un fournisseur VPN prenant en charge la configuration manuelle de WireGuard. Consultez cette page pour connaître les fournisseurs WireGuard compatibles avec GL.iNet.

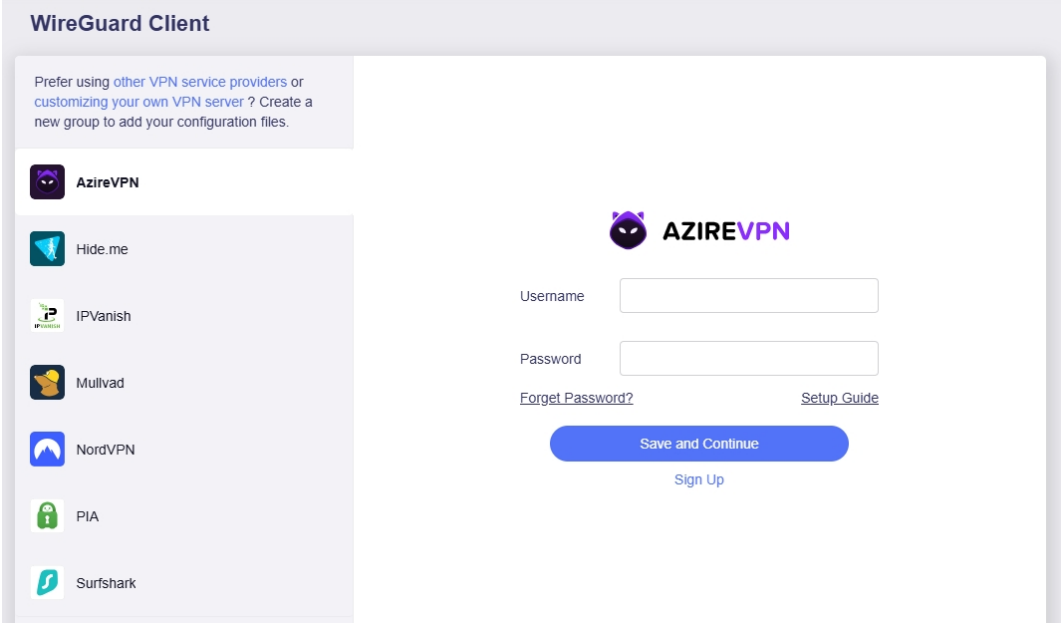
Sélectionnez ensuite votre fournisseur ci-dessous pour accéder directement aux instructions détaillées.

- Configuration d’AzireVPN
- Configuration de Hide.me
- Configuration d’IPVanish
- Configuration de Mullvad
- Configuration de NordVPN
- Configuration de PIA (Private Internet Access)
- Configuration de Surfshark
- Configuration manuelle d’un client WireGuard pour un autre fournisseur

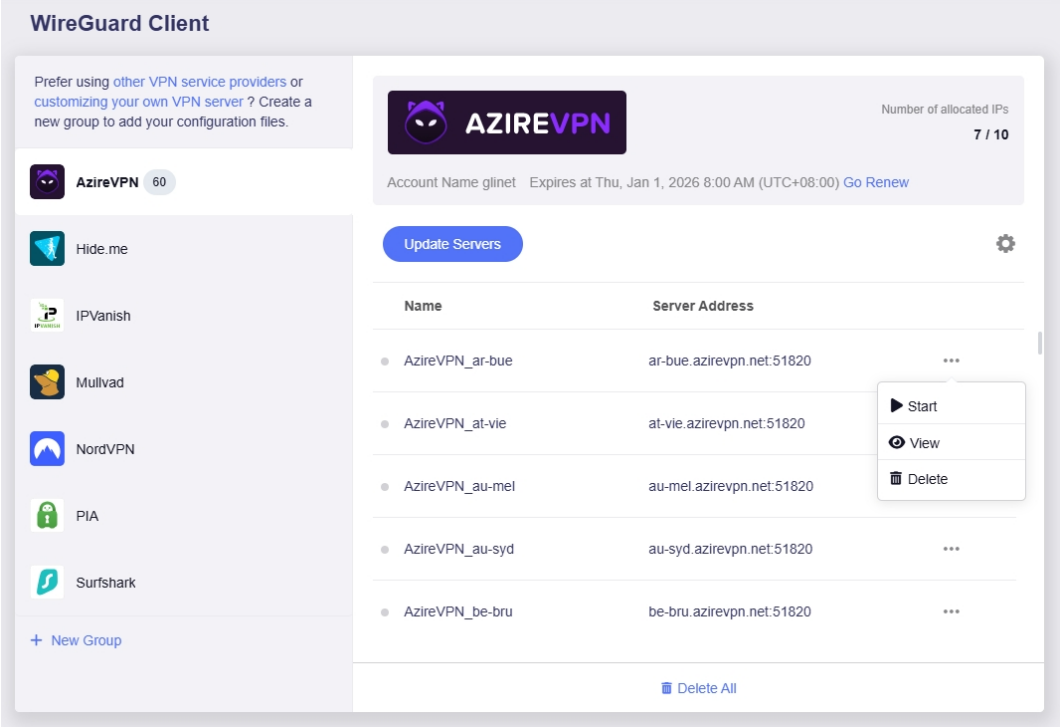
11.2.2 Configuration d’AzireVPN

Suivez les étapes ci-dessous pour configurer le routeur comme client AzireVPN.

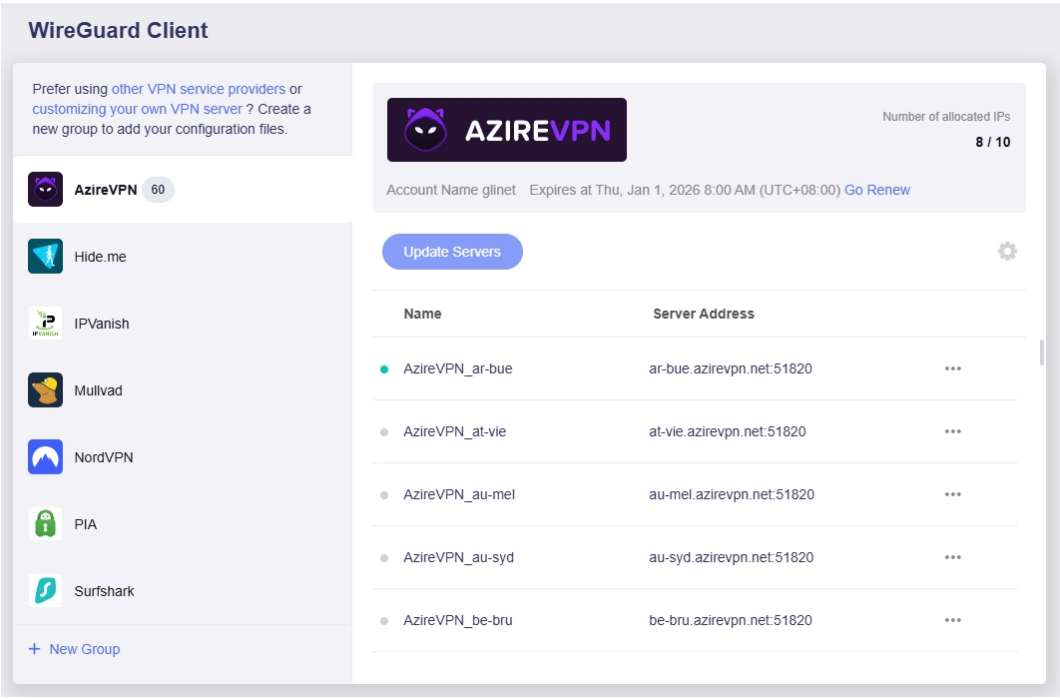
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **AzireVPN**.
2. Saisissez l’identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



3. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



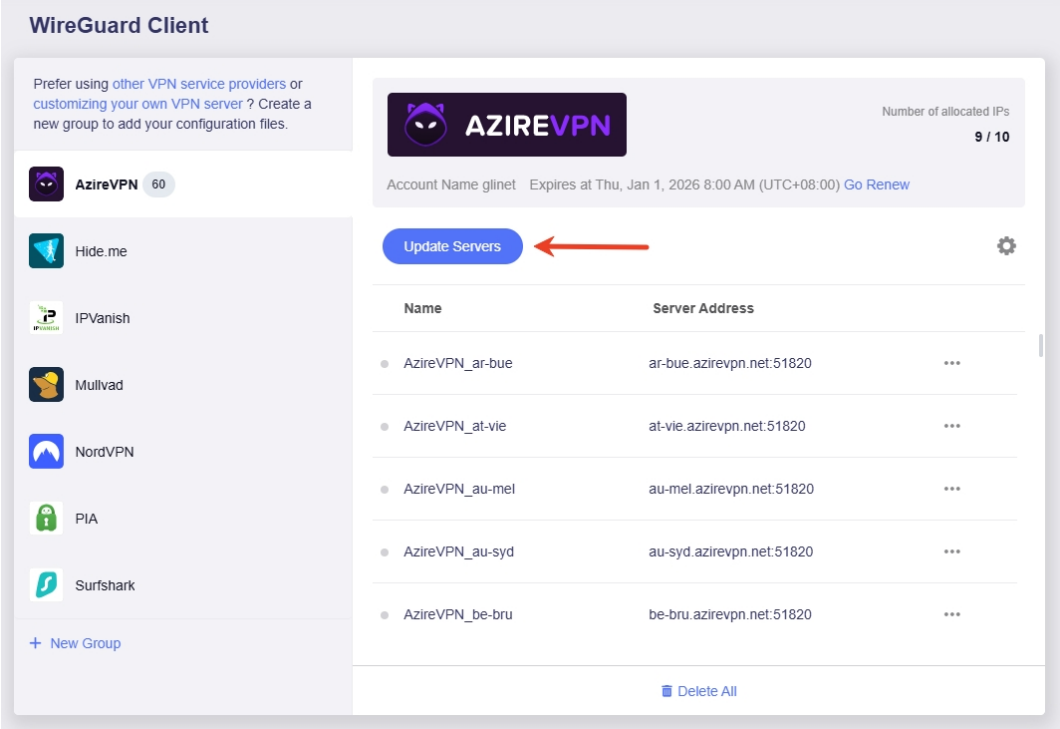
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



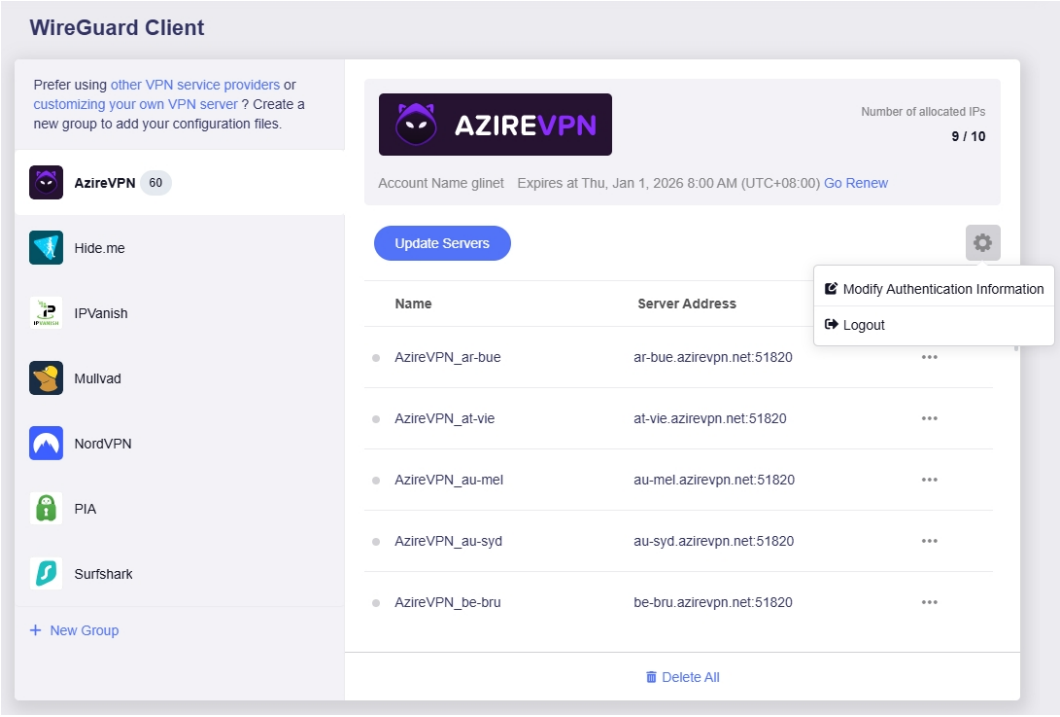
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

5. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

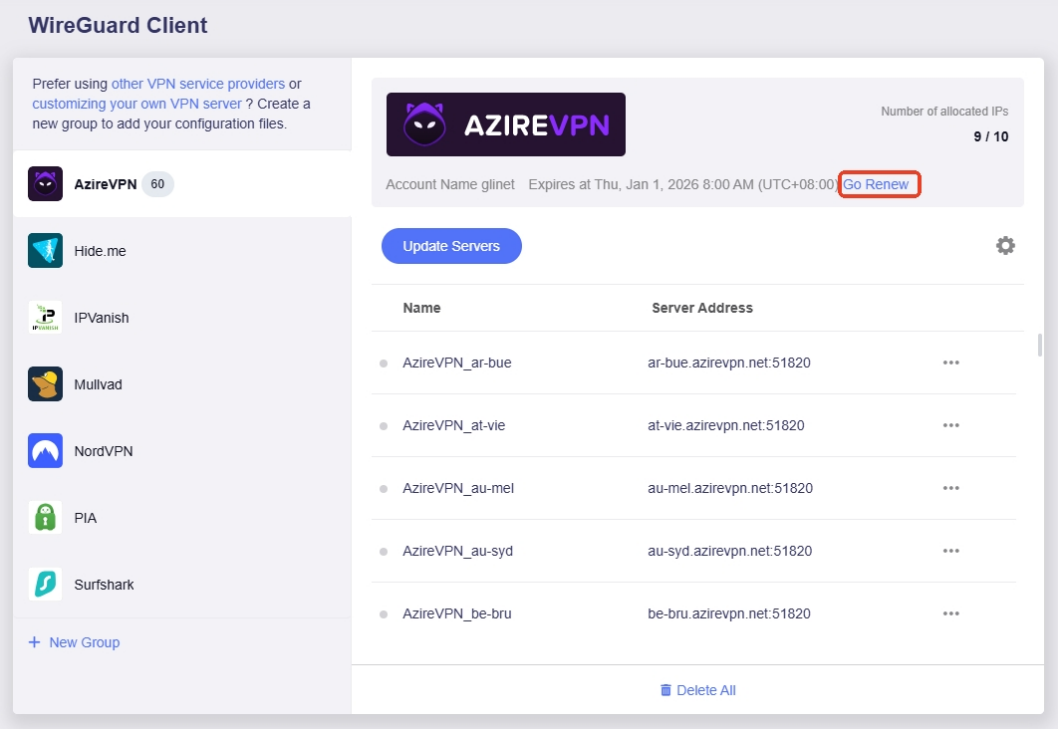


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



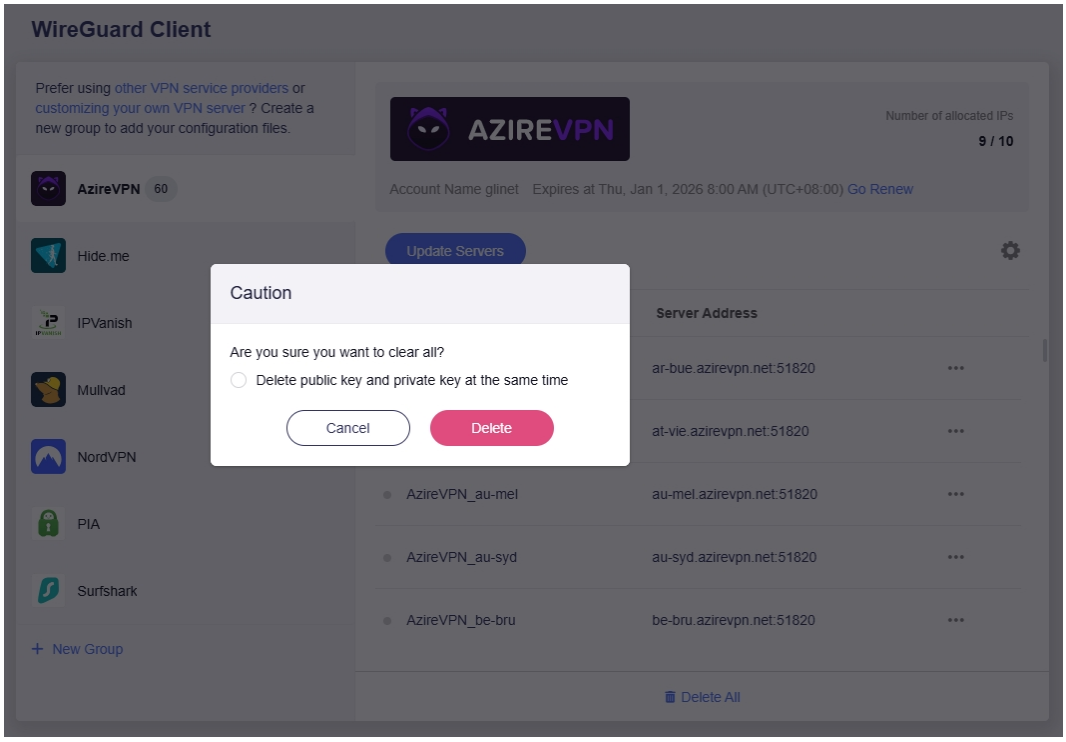
7. Renouvelez l'abonnement.

Cliquez sur **Renouveler (Go Renew)** pour ouvrir le site officiel et renouveler votre abonnement.



8. Supprimez tous les fichiers.

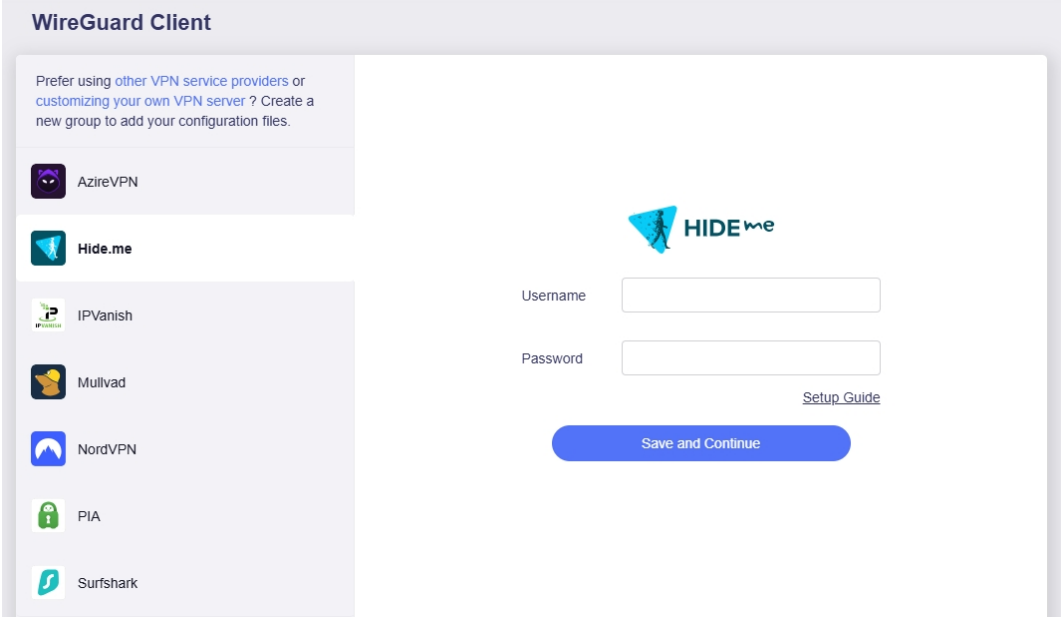
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
AzireVPN 60
Hide.me
IPVanish
Mullvad
NordVPN
PIA
Surfshark
New Group
AZIREVPN
Number of allocated IPs
9 / 10
Account Name glinet Expires at Thu, Jan 1, 2026 8:00 AM (UTC+08:00) Go Renew
Update Servers
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete
Server Address
ar-bue.azirevpn.net:51820
at-vie.azirevpn.net:51820
AzireVPN_au-mel
au-mel.azirevpn.net:51820
AzireVPN_au-syd
au-syd.azirevpn.net:51820
AzireVPN_be-bru
be-bru.azirevpn.net:51820
Delete All

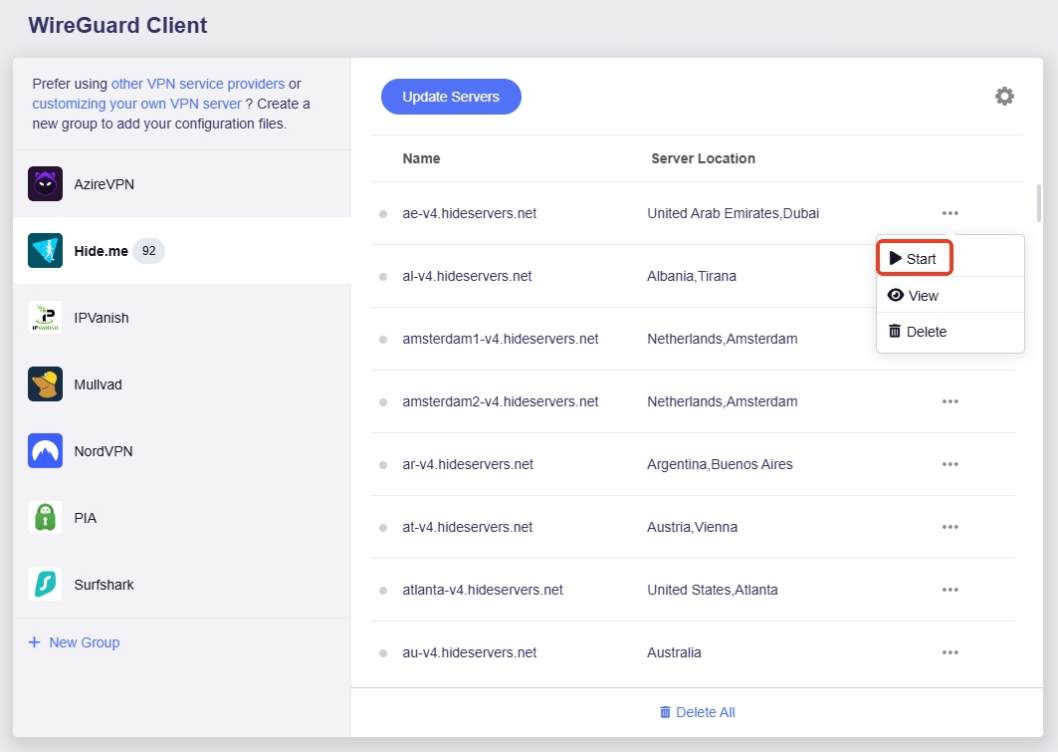
11.2.3 Configuration de Hide.me

Suivez les étapes ci-dessous pour configurer le routeur comme client Hide.me.

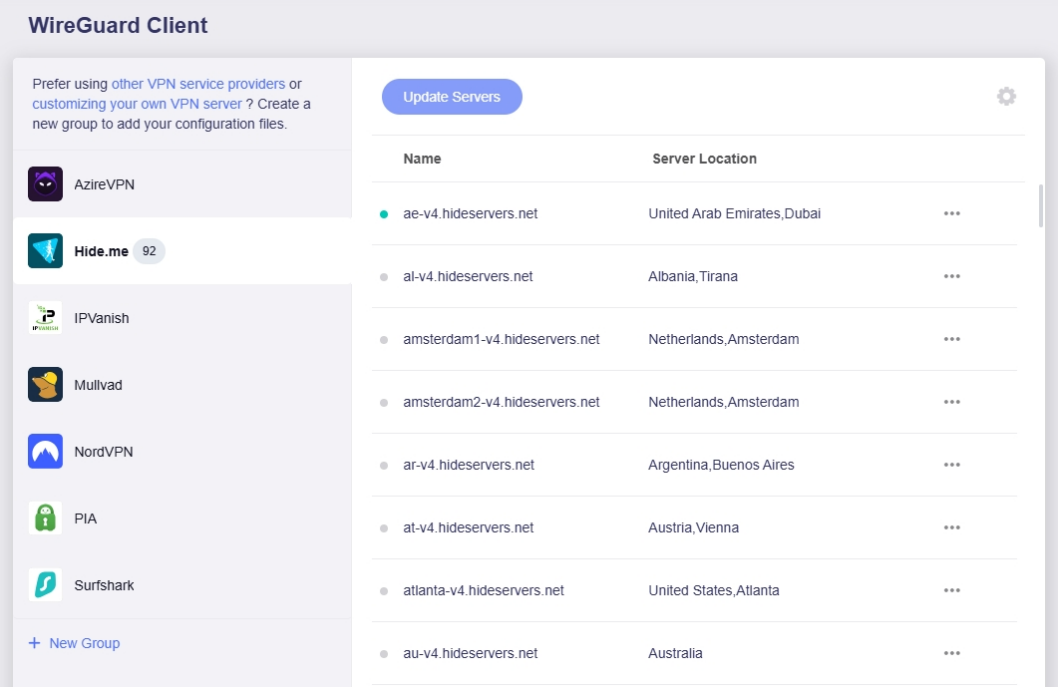
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Hide.me**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



3. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



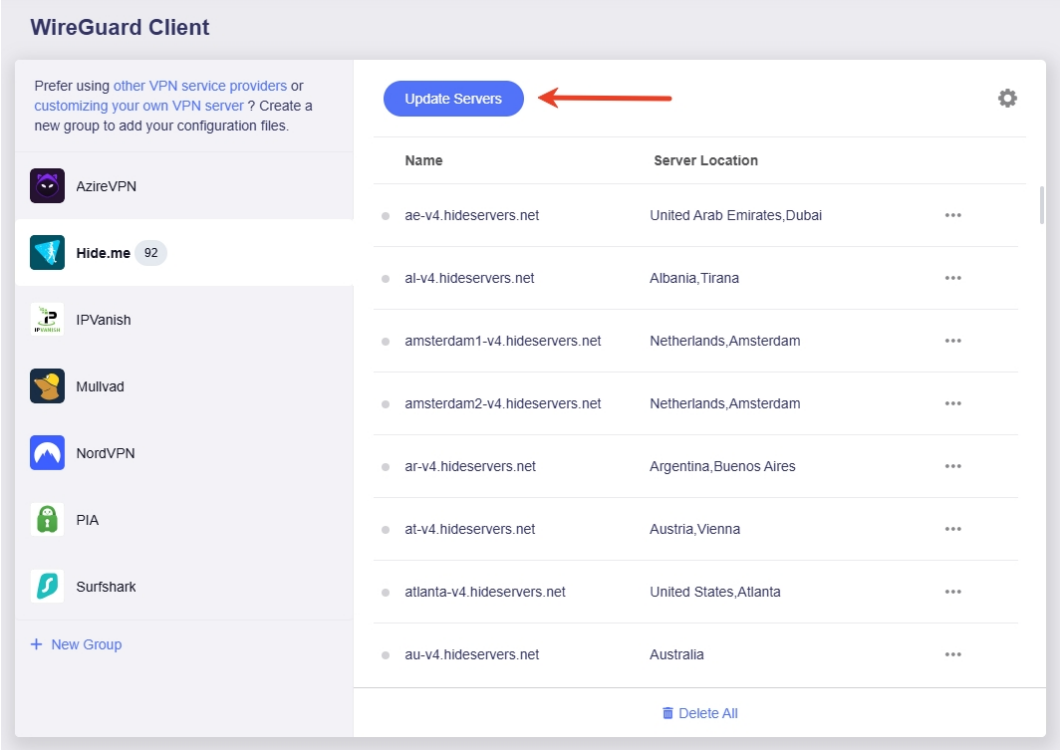
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



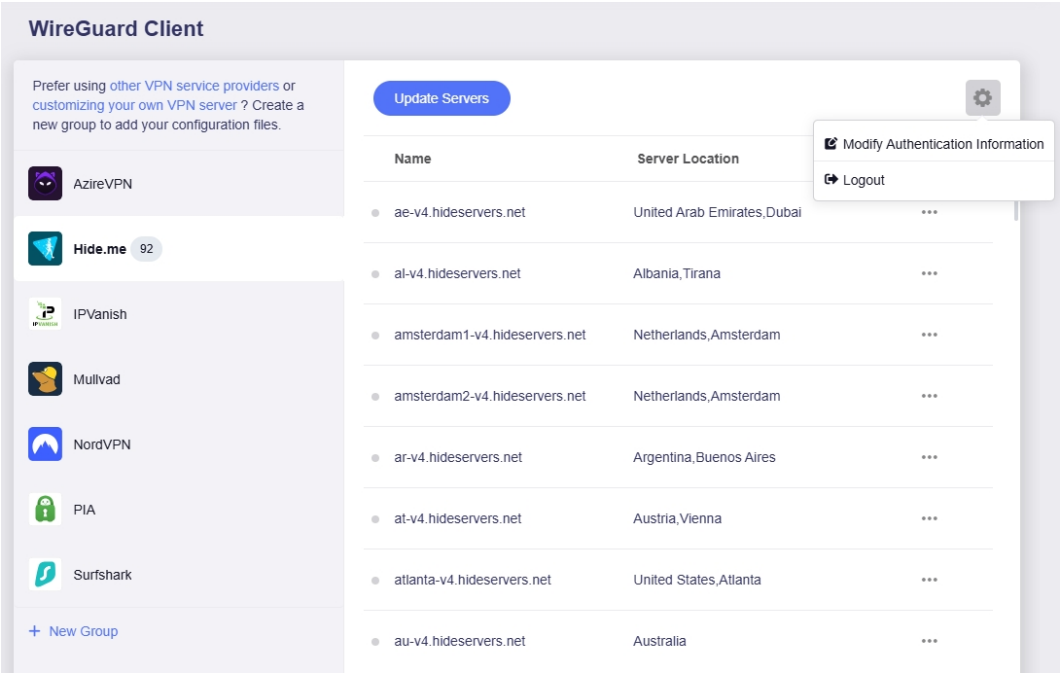
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

5. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

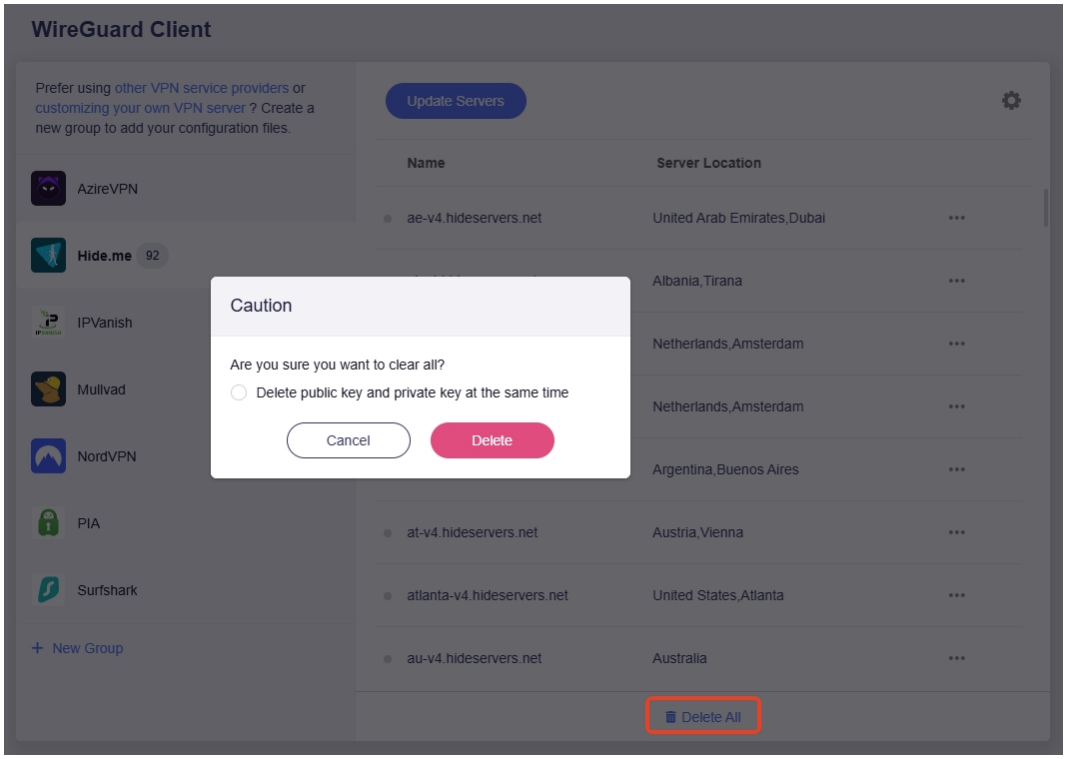


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



7. Supprimez tous les fichiers.

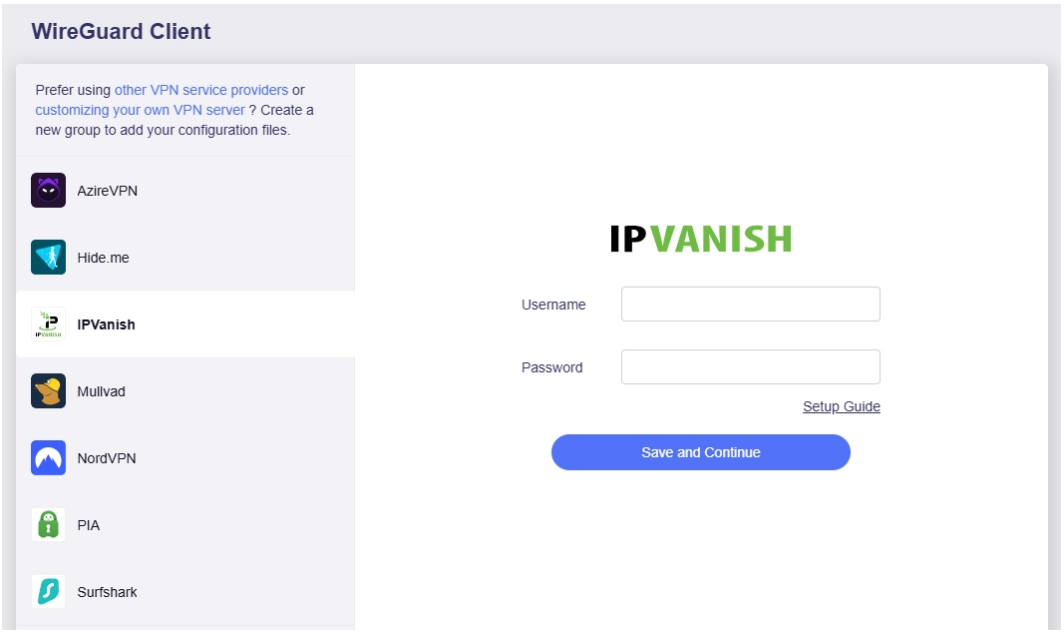
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



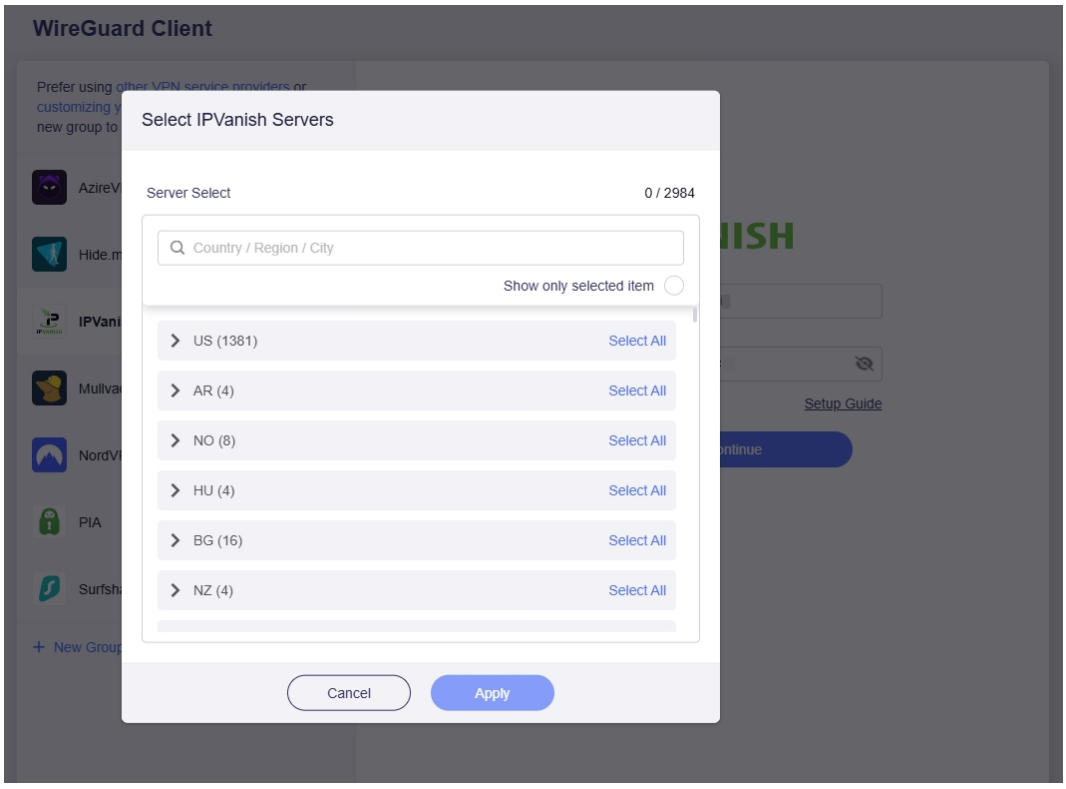
11.2.4 Configuration d'IPVanish

Suivez les étapes ci-dessous pour configurer le routeur comme client IPVanish.

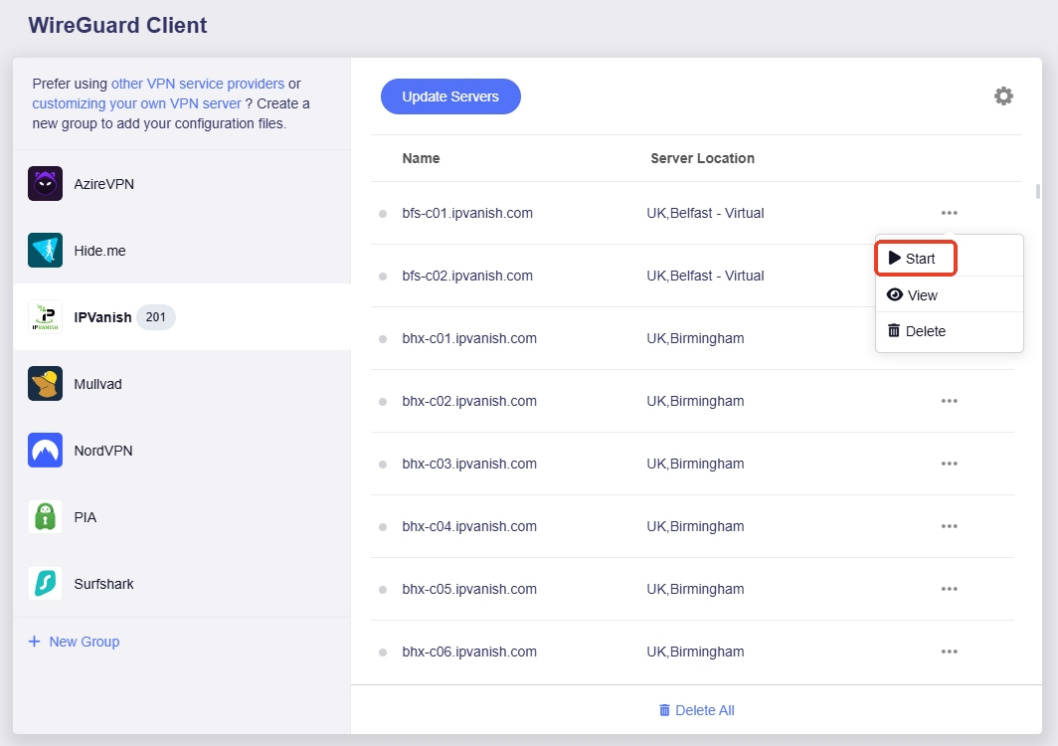
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **IPVanish**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



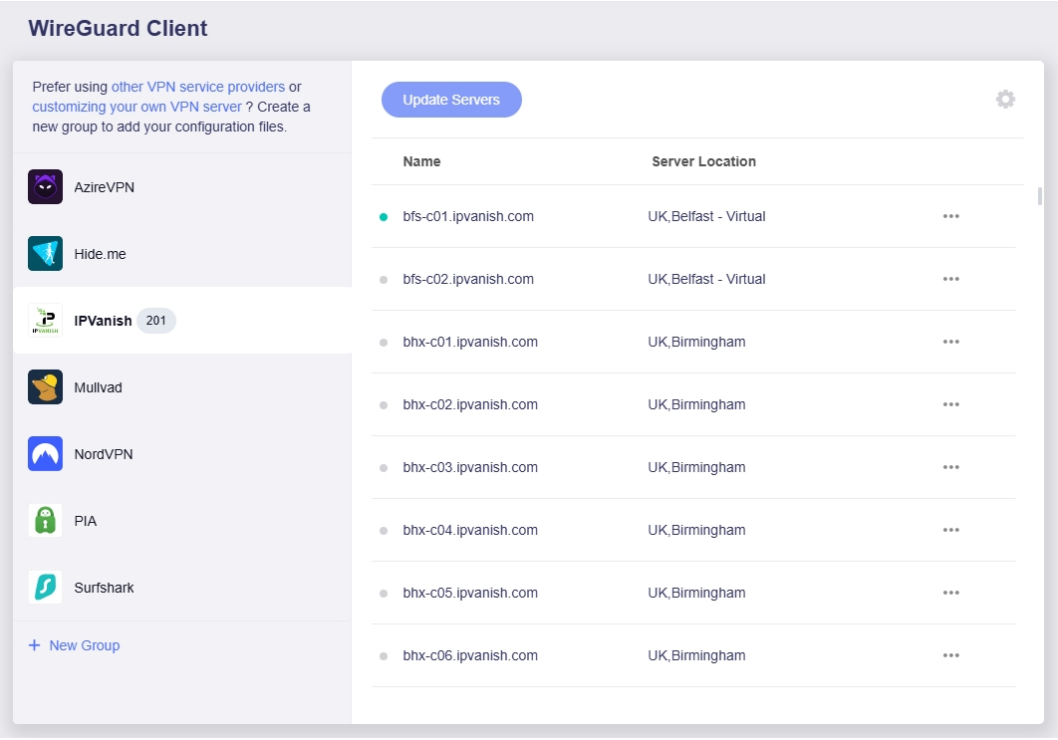
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



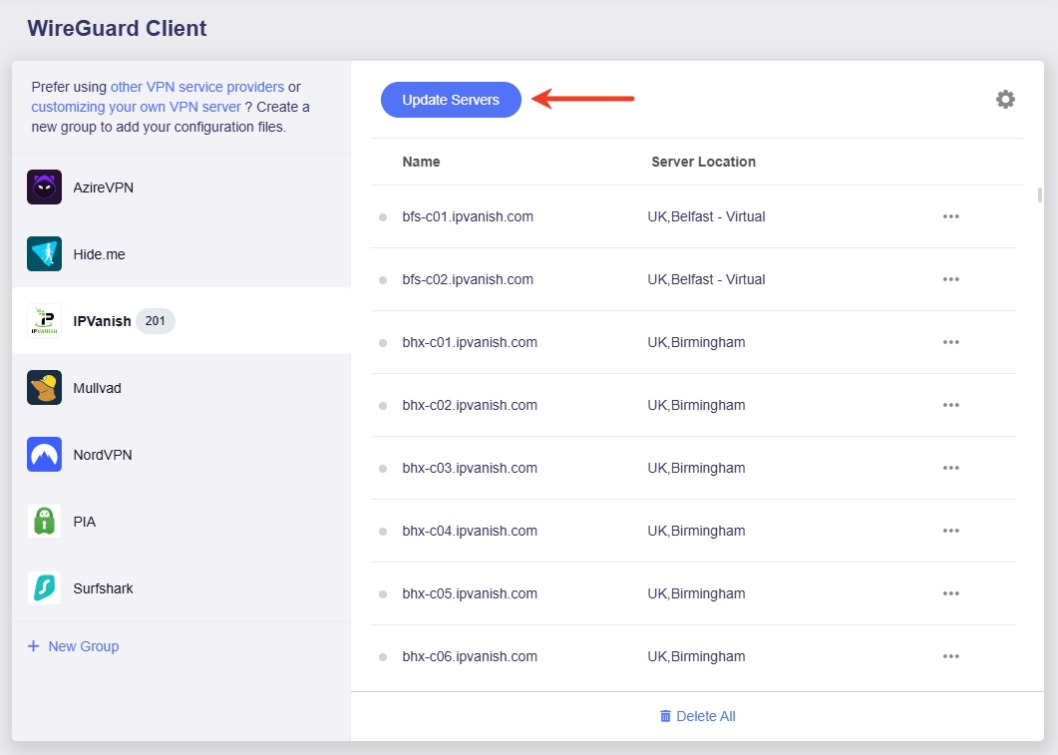
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

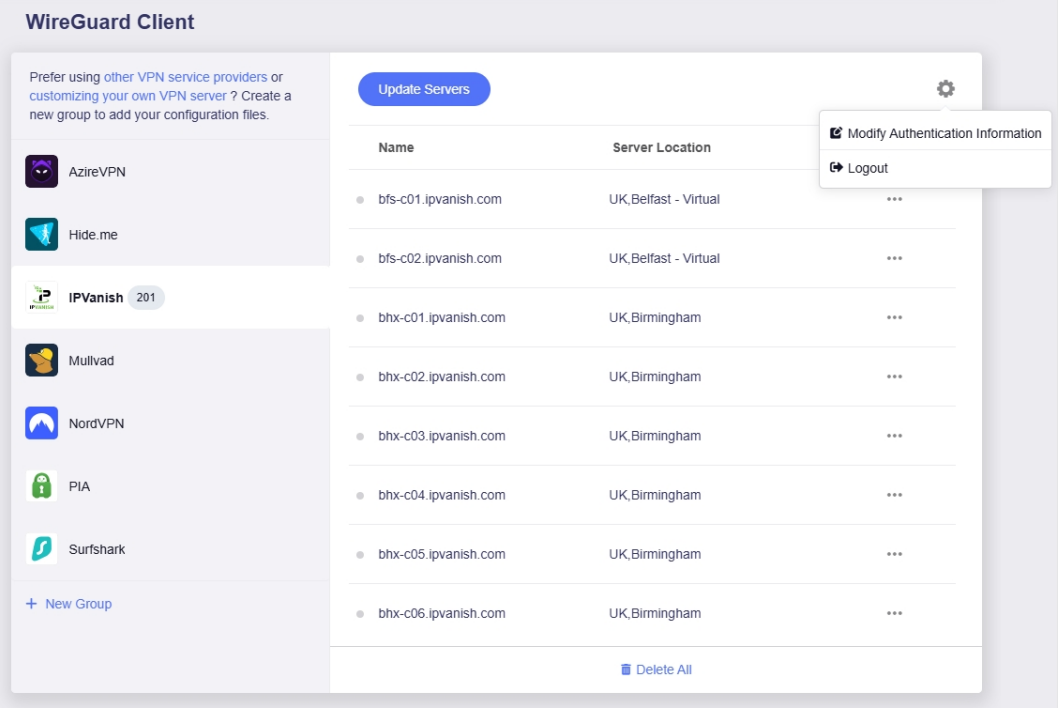
6. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



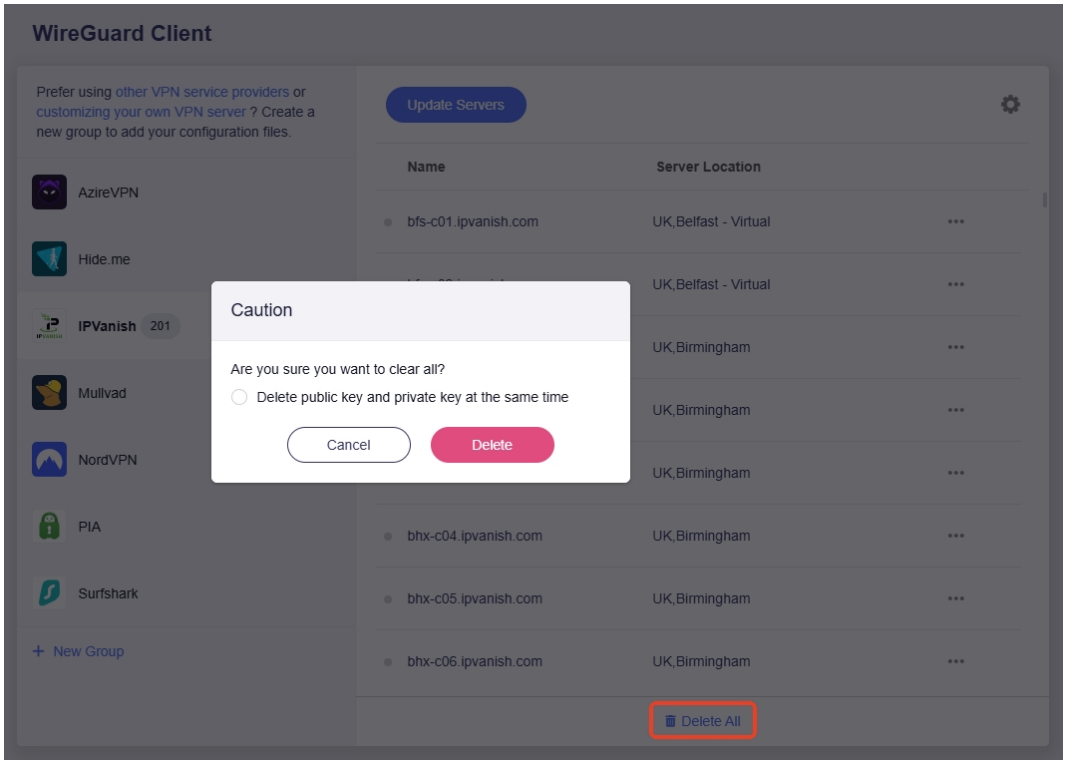
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

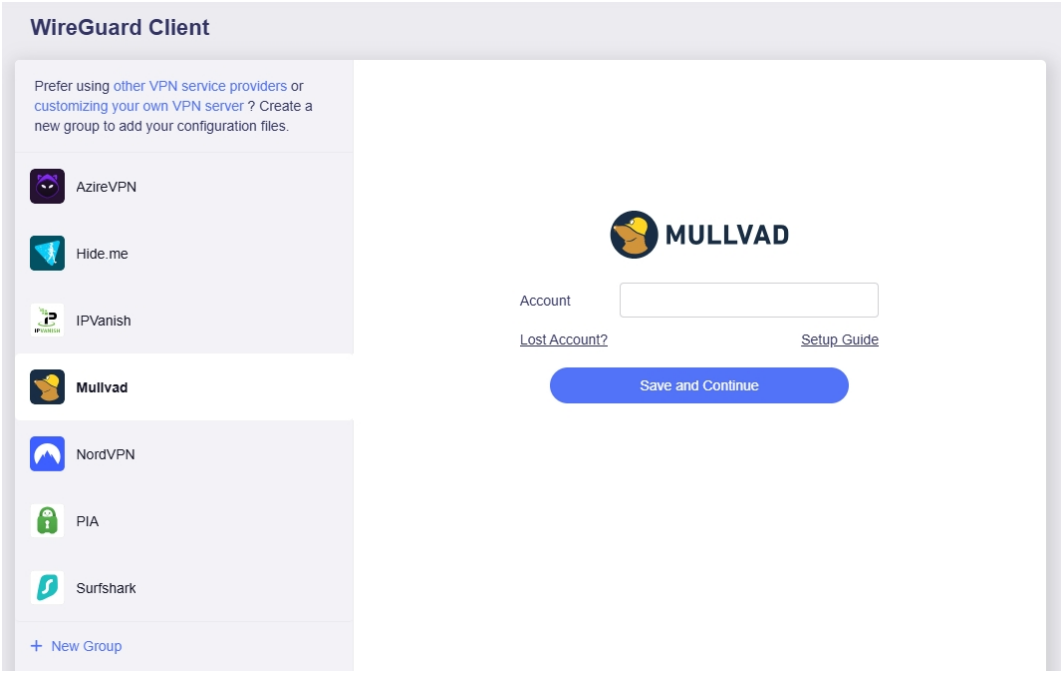
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



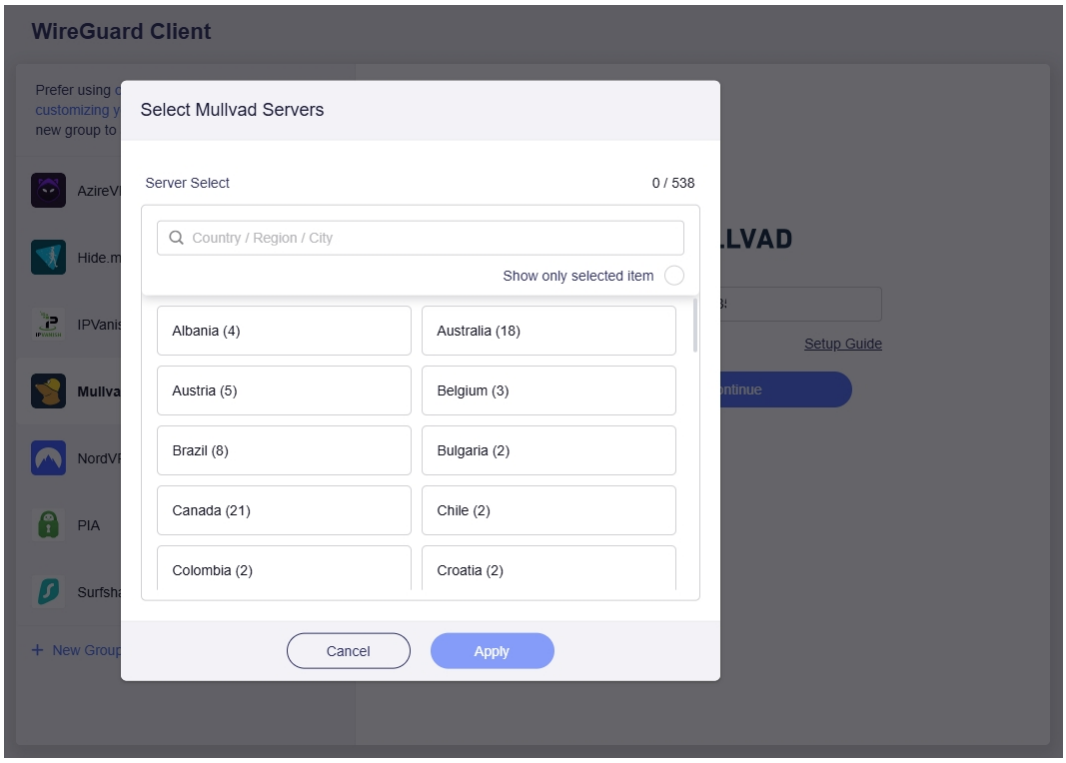
11.2.5 Configuration de Mullvad

Suivez les étapes ci-dessous pour configurer le routeur comme client Mullvad.

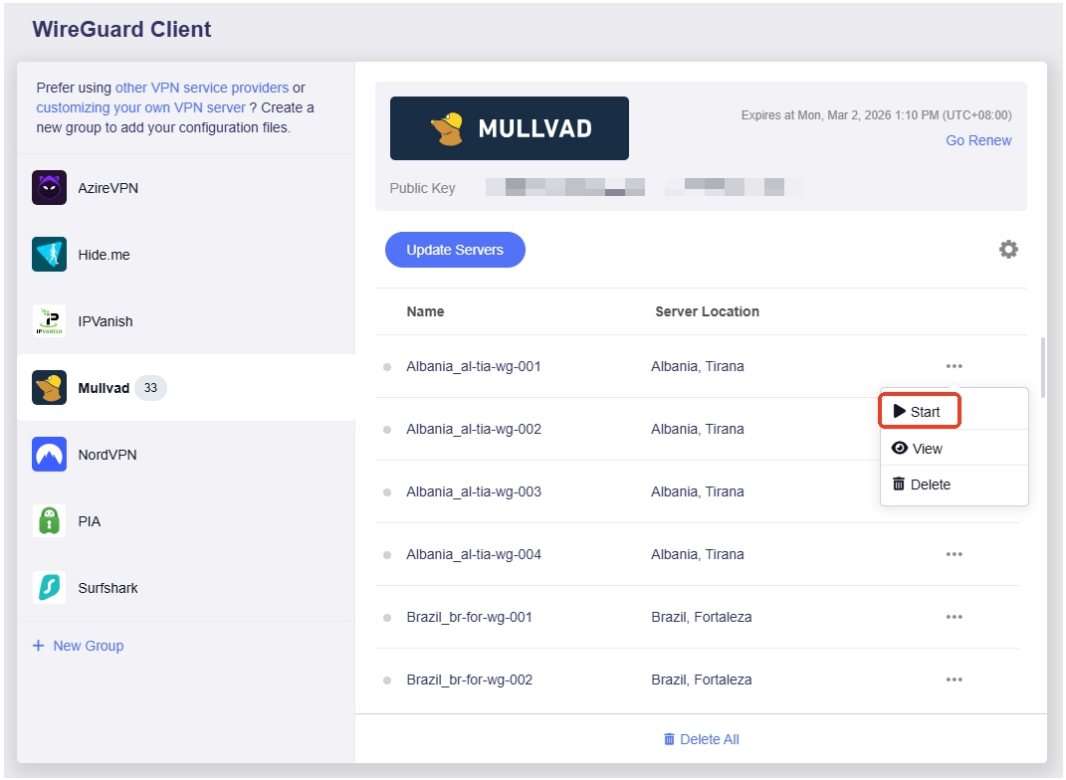
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Mullvad**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



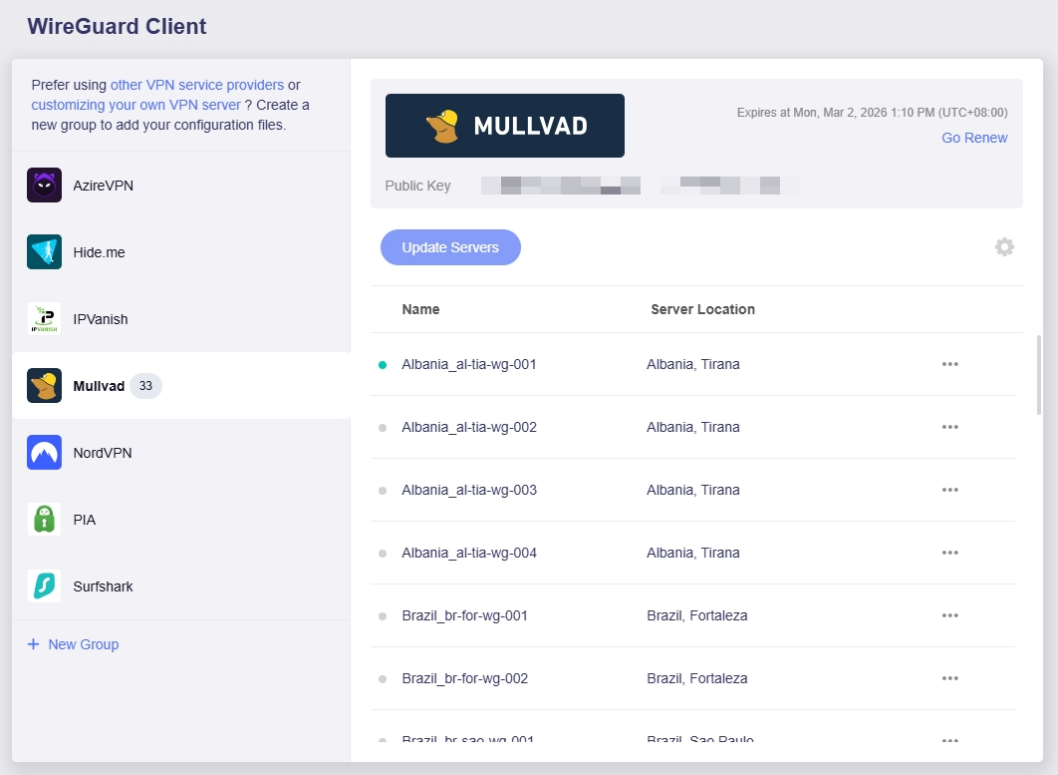
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



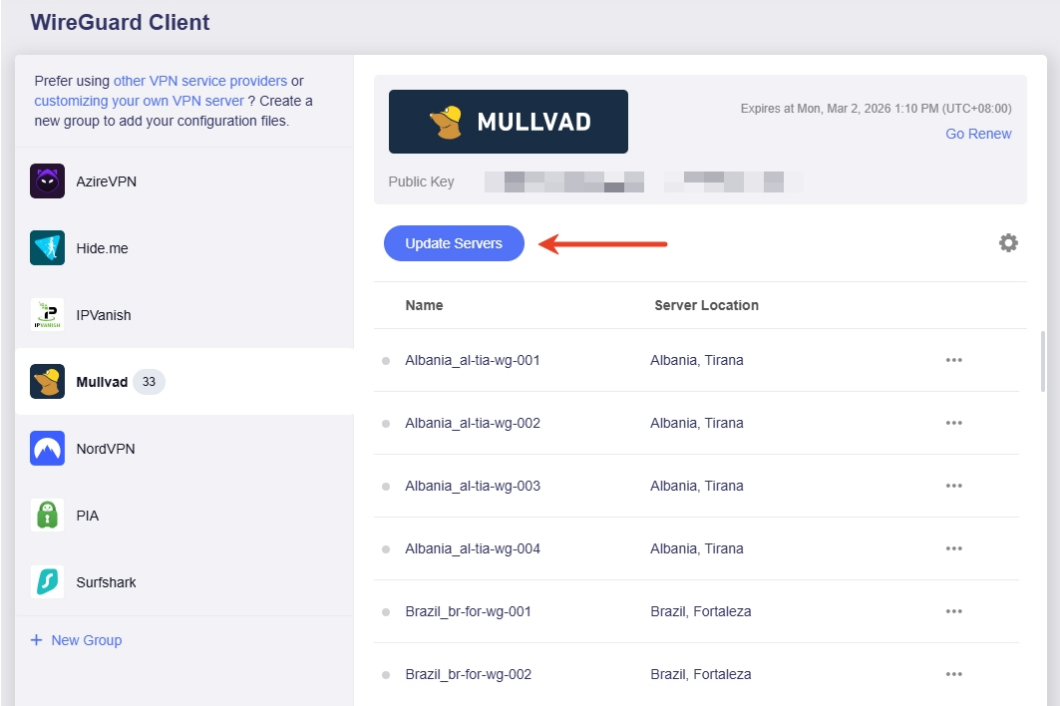
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

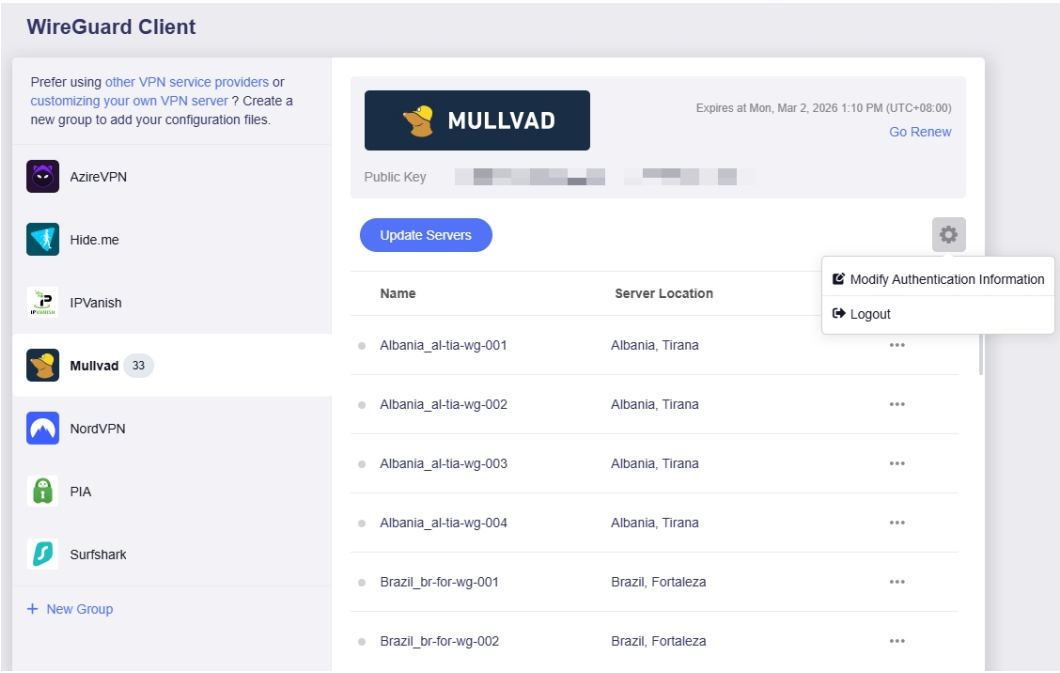
6. Mettez à jour les serveurs.

   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



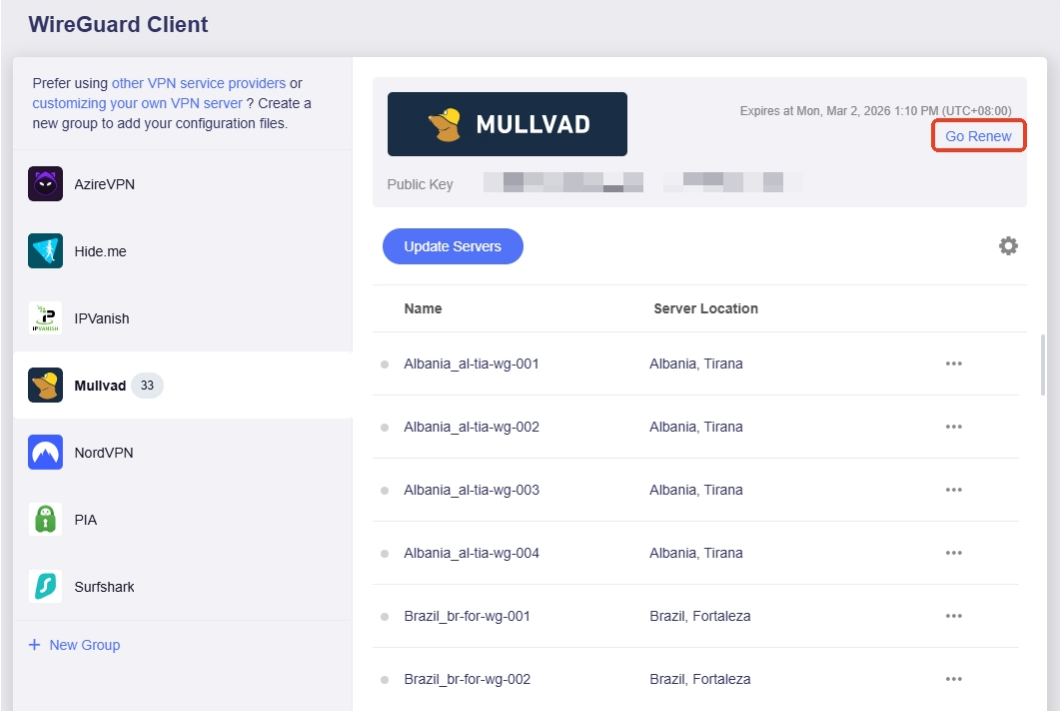
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



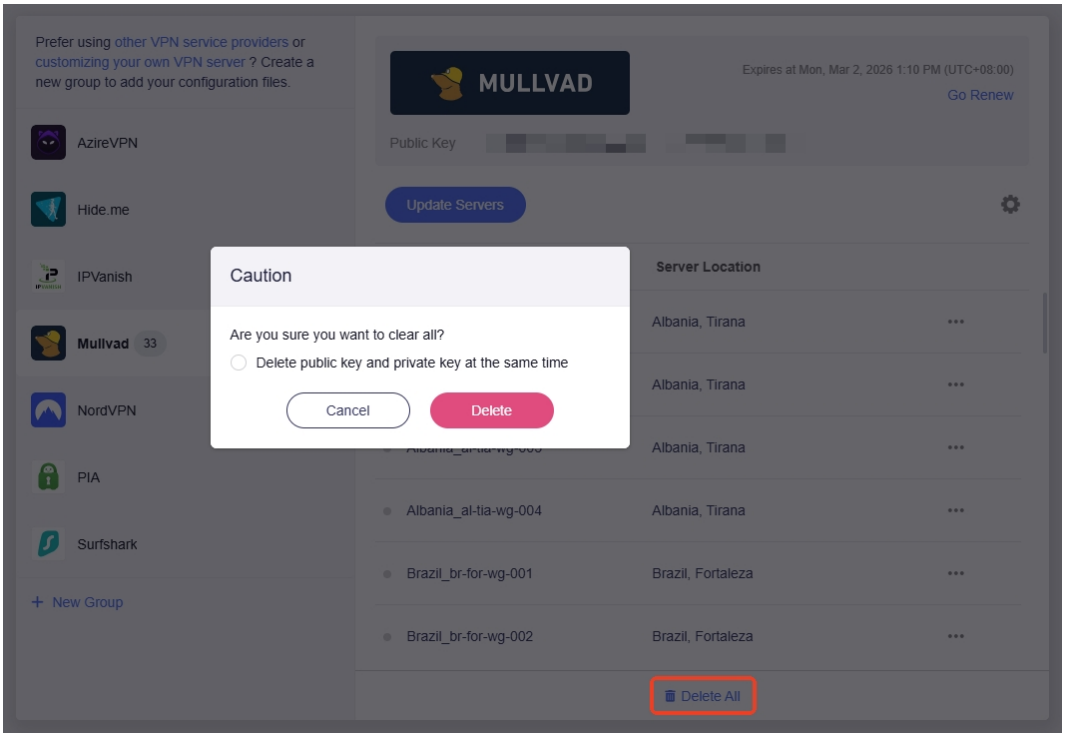
8. Renouvelez l'abonnement.

   Cliquez sur **Renouveler (Go Renew)** pour ouvrir le site officiel et renouveler votre abonnement.



9. Supprimez tous les fichiers.

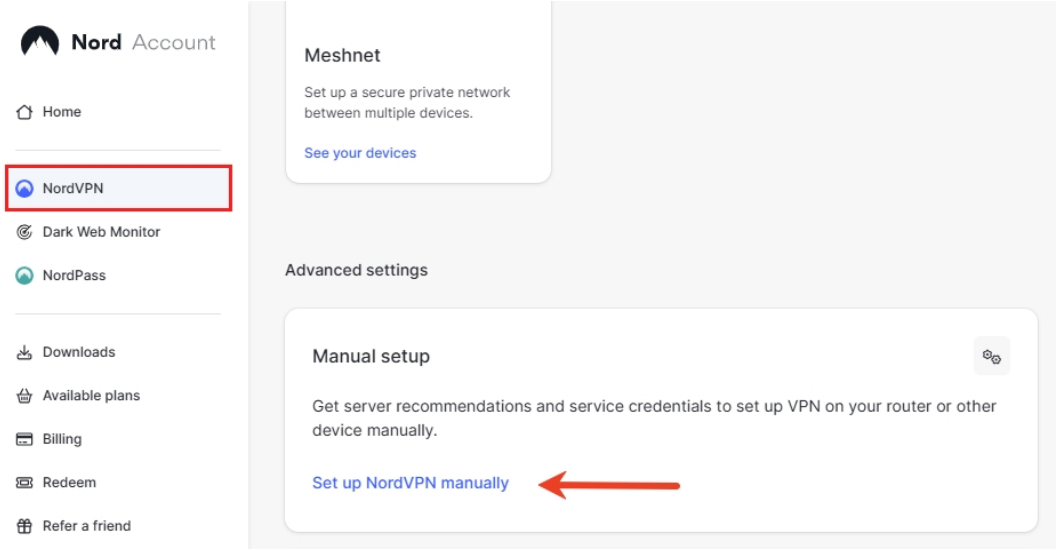
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



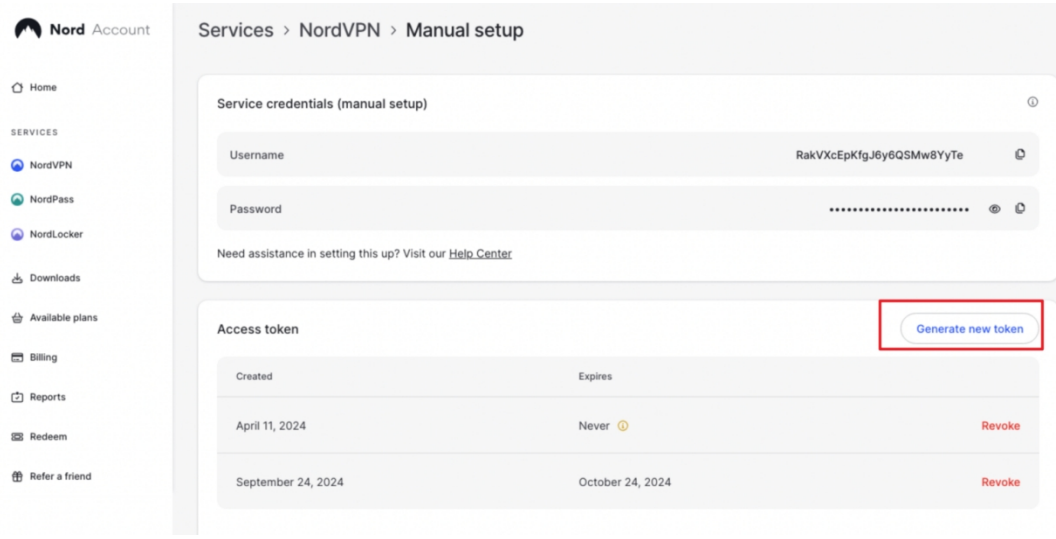
11.2.6 Configuration de NordVPN

Suivez les étapes ci-dessous pour configurer le routeur comme client NordVPN.

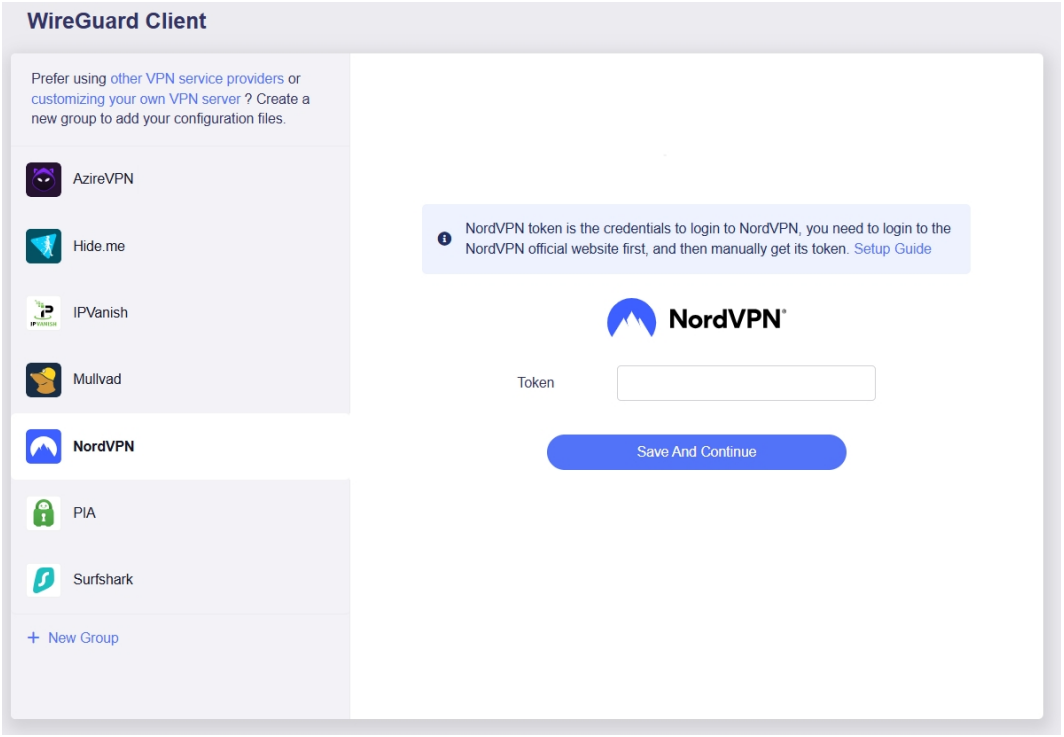
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



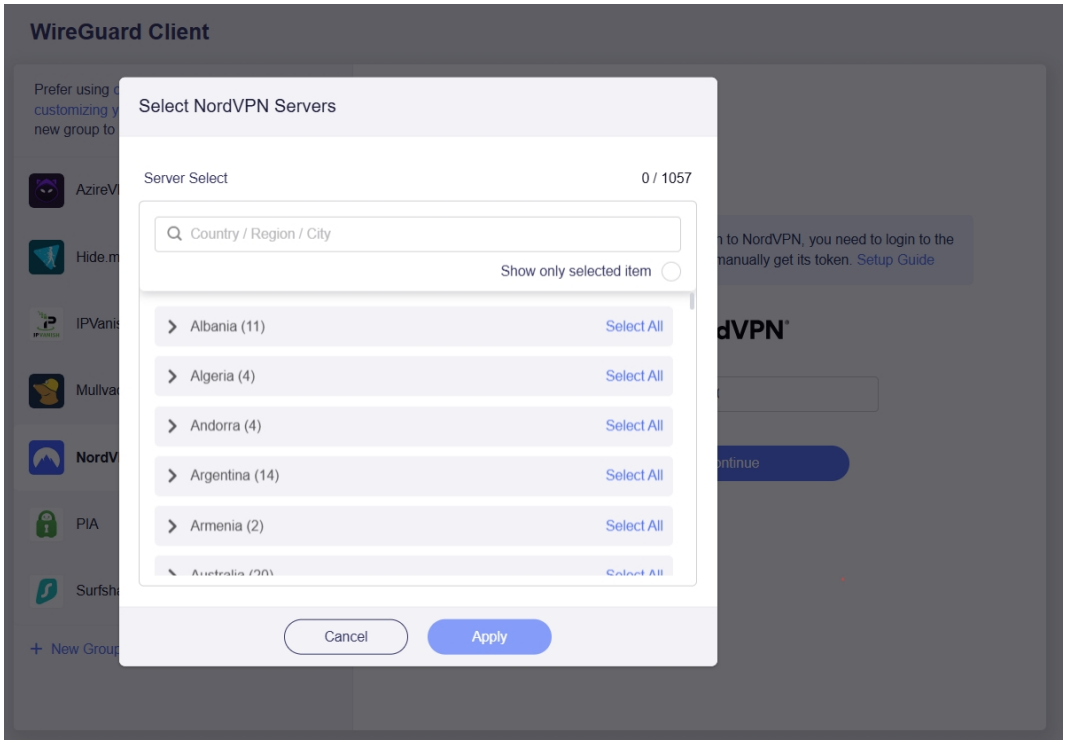
Repérez la section **Jeton d'accès (Access Token)**. Créez un jeton et copiez-le pour l'utiliser ensuite.



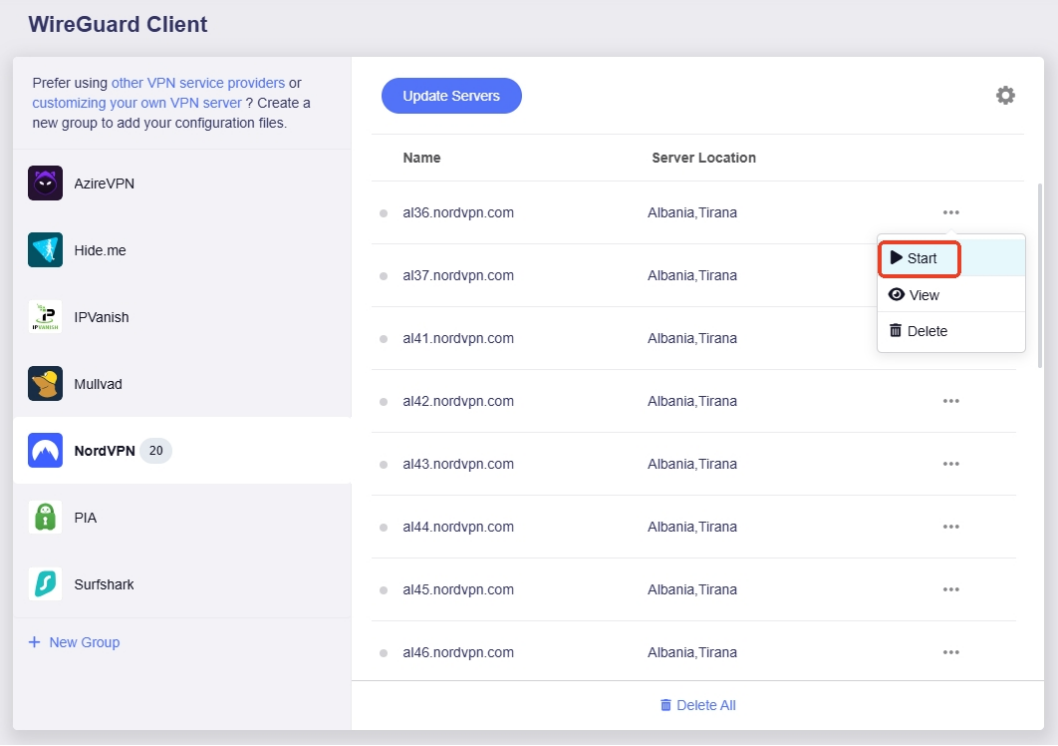
3. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **NordVPN**.
4. Saisissez le jeton et cliquez sur **Enregistrer et continuer (Save and Continue)**.



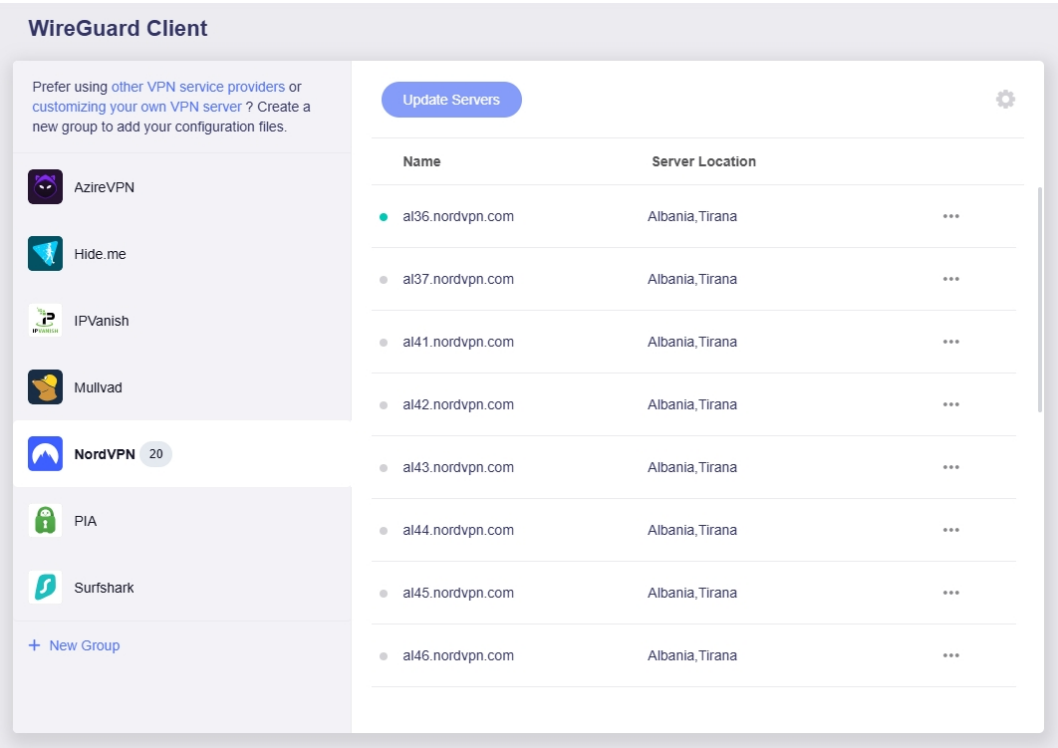
5. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



6. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



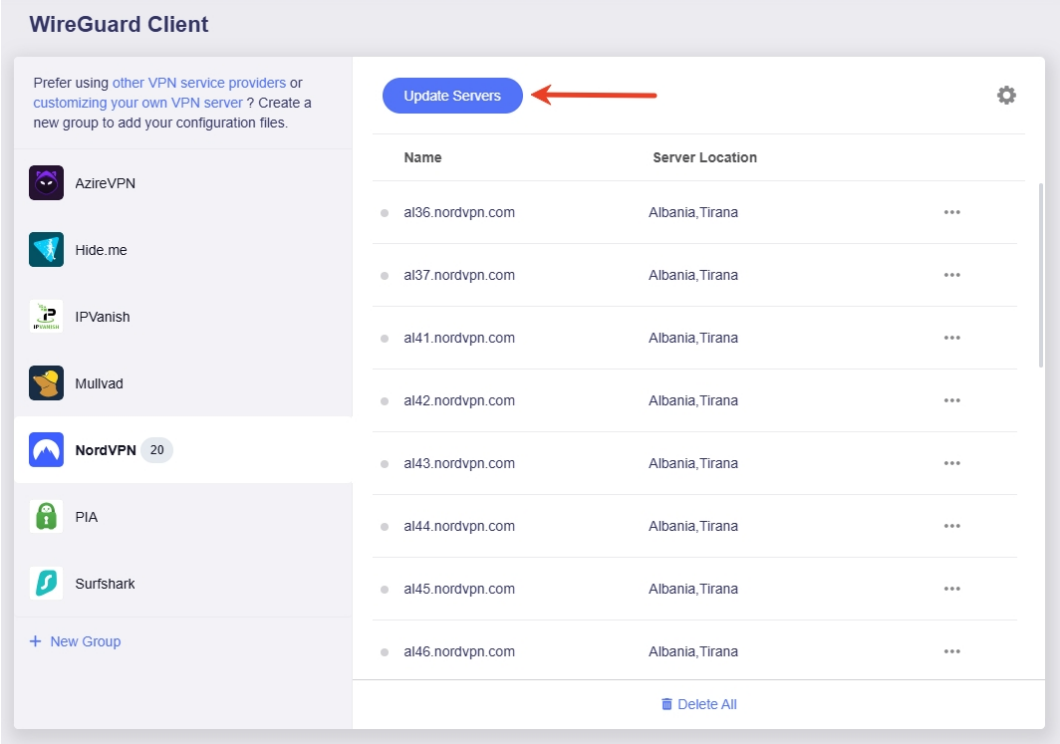
7. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

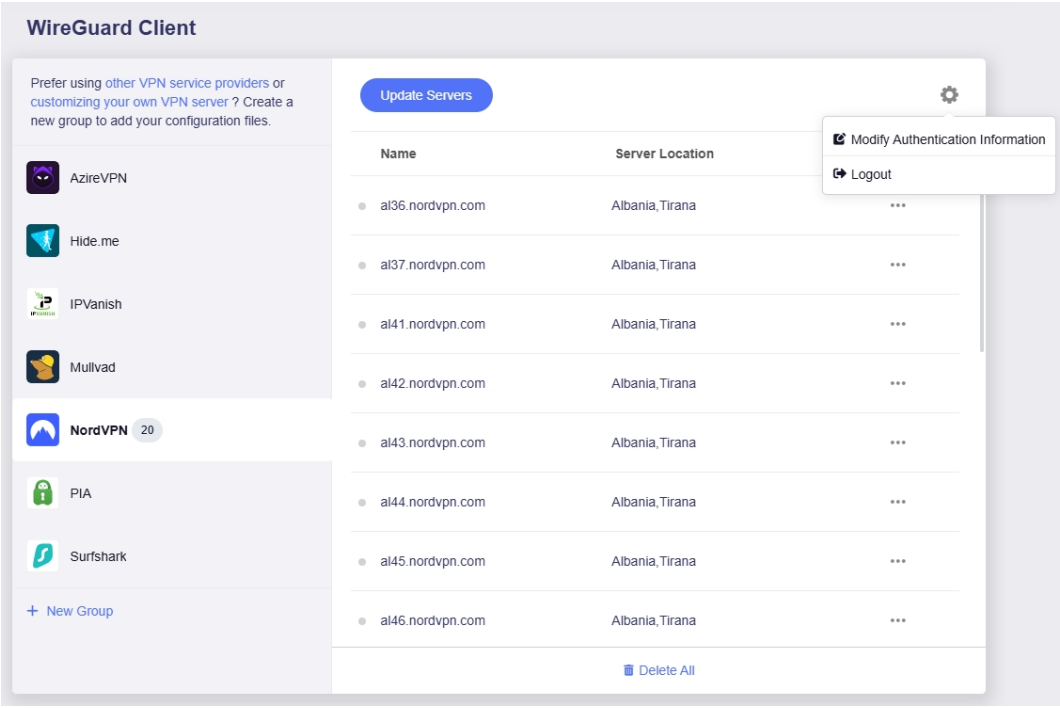
8. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



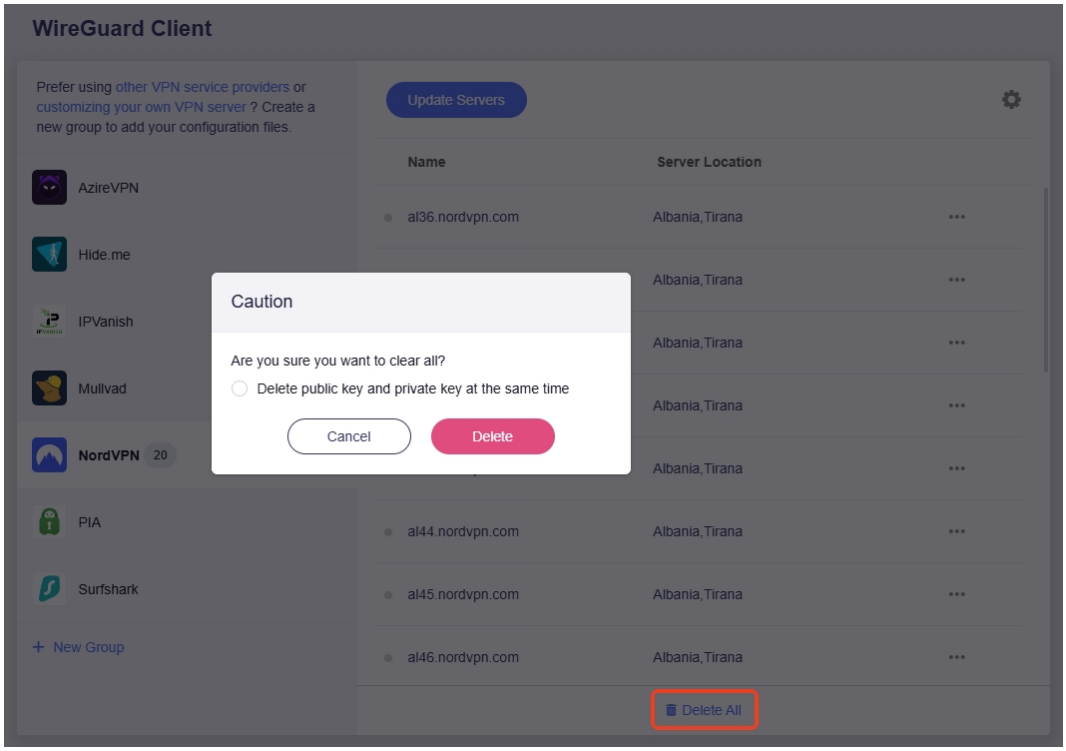
9. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



10. Supprimez tous les fichiers.

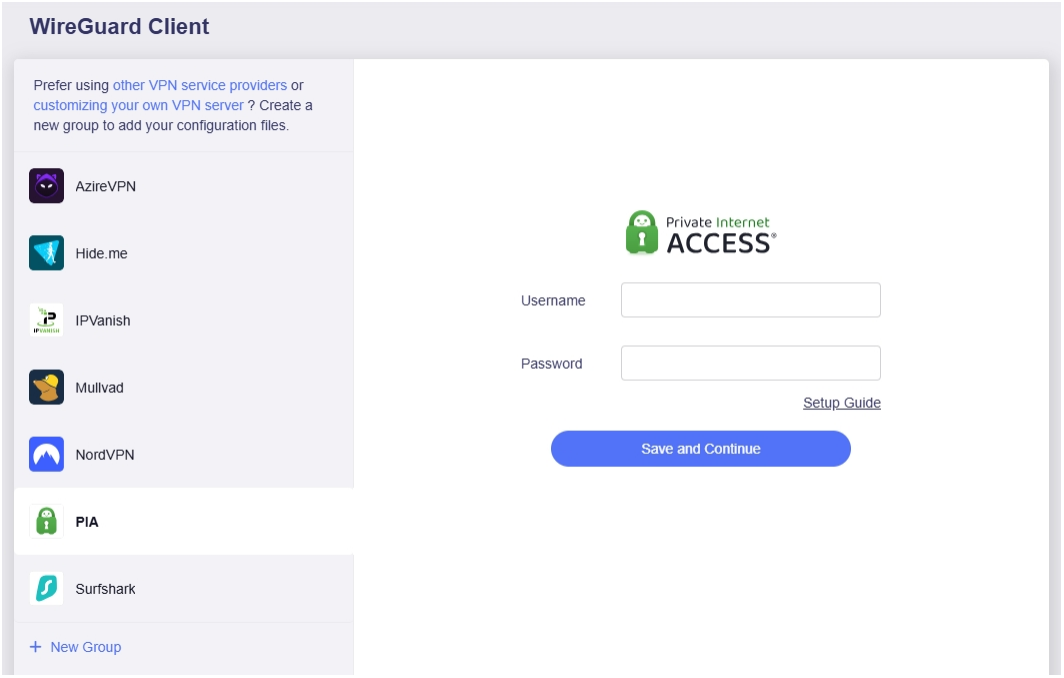
    Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



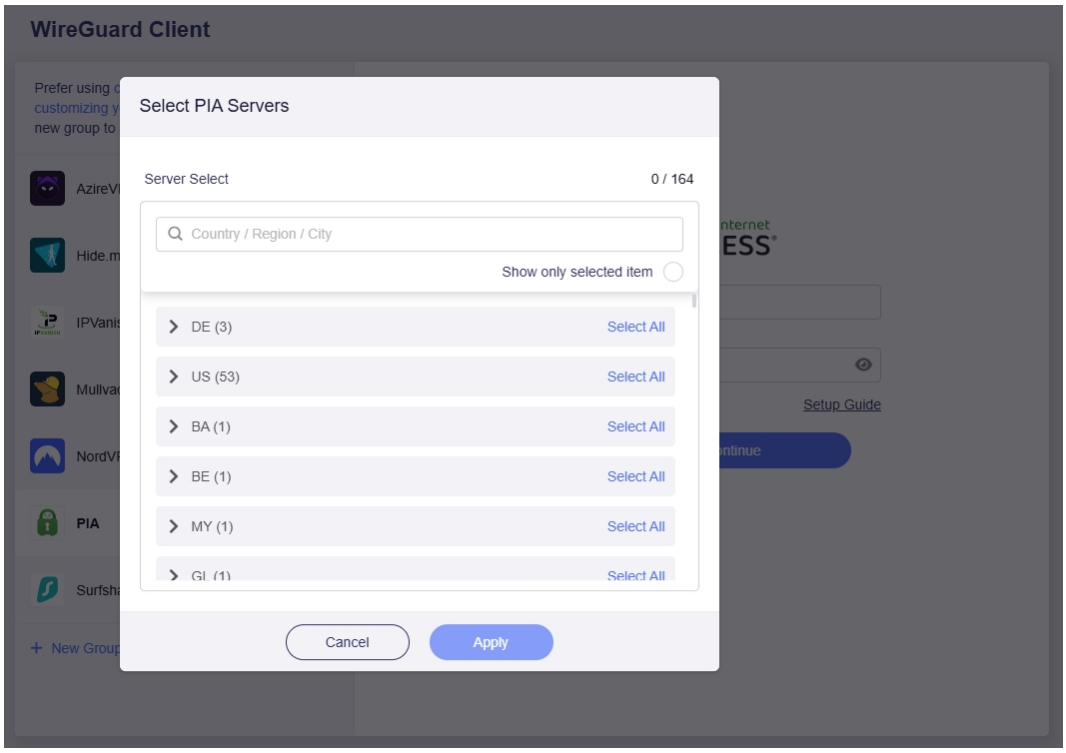
11.2.7 Configuration de PIA (Private Internet Access)

Suivez les étapes ci-dessous pour configurer le routeur comme client PIA.

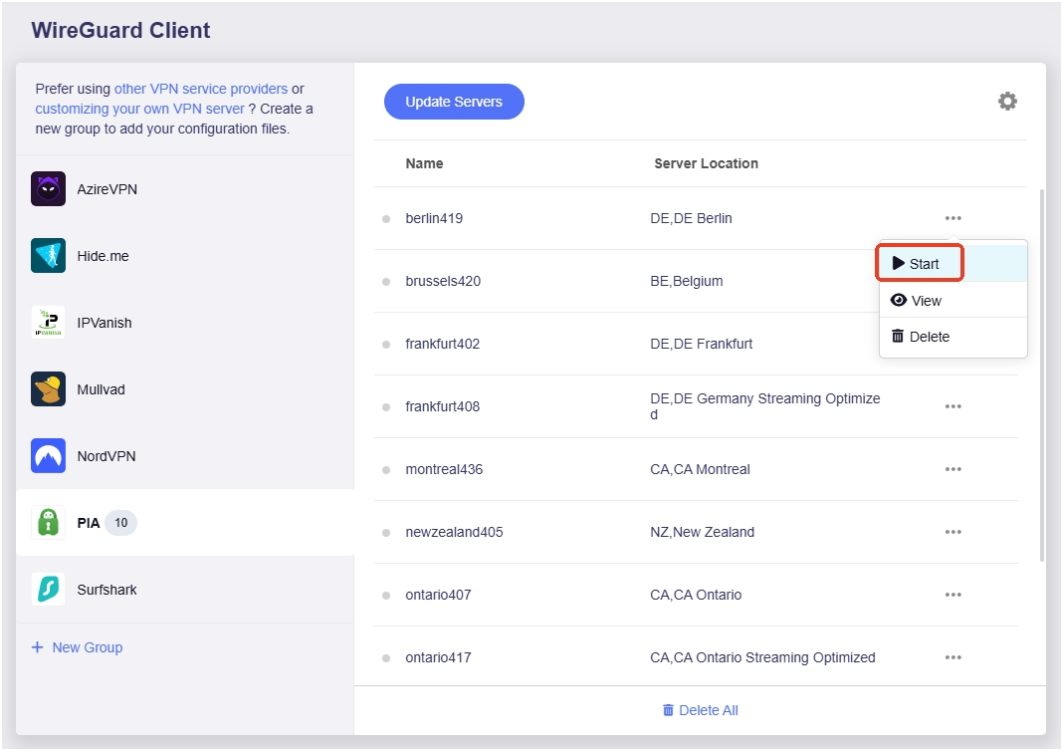
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **PIA**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



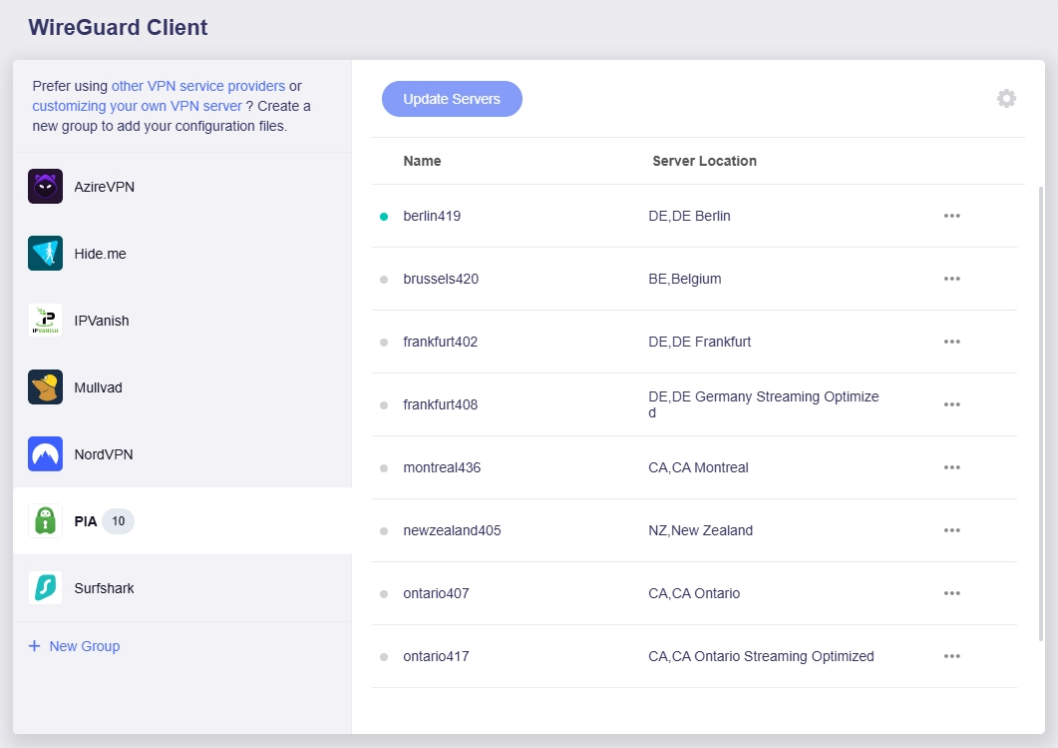
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



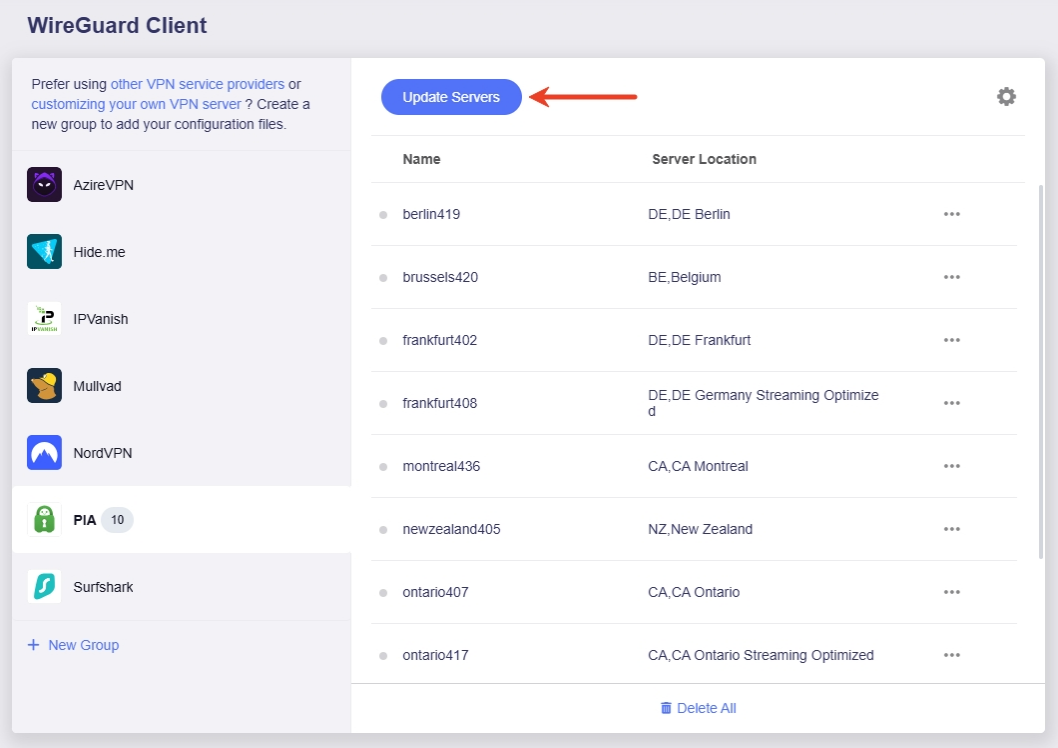
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

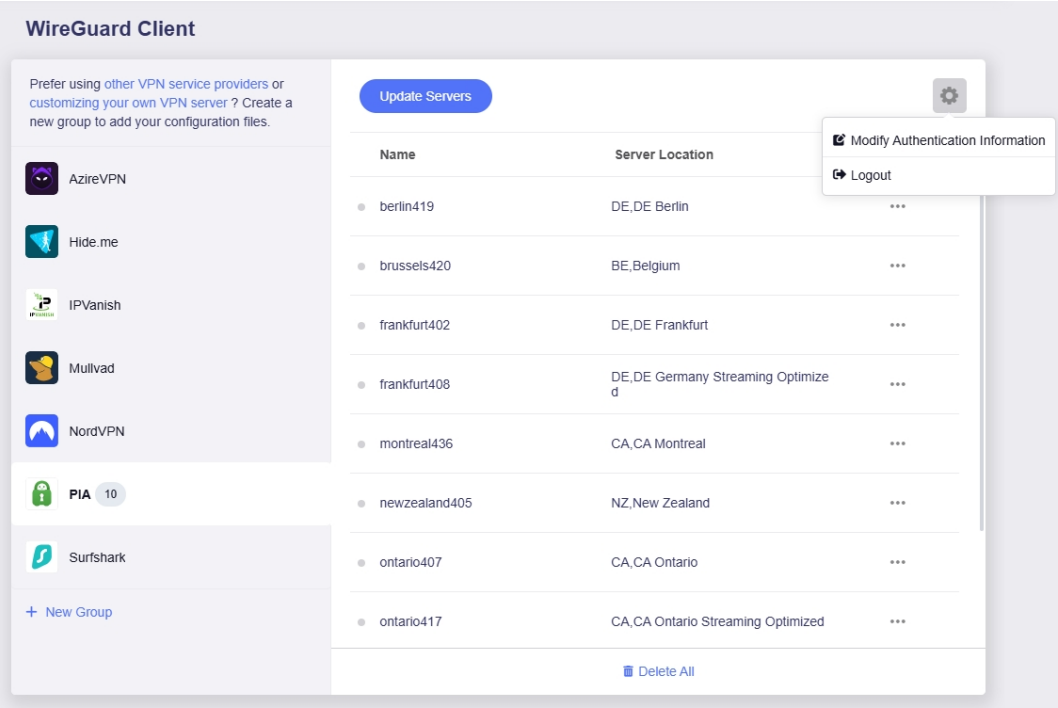
6. Mettez à jour les serveurs.

   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



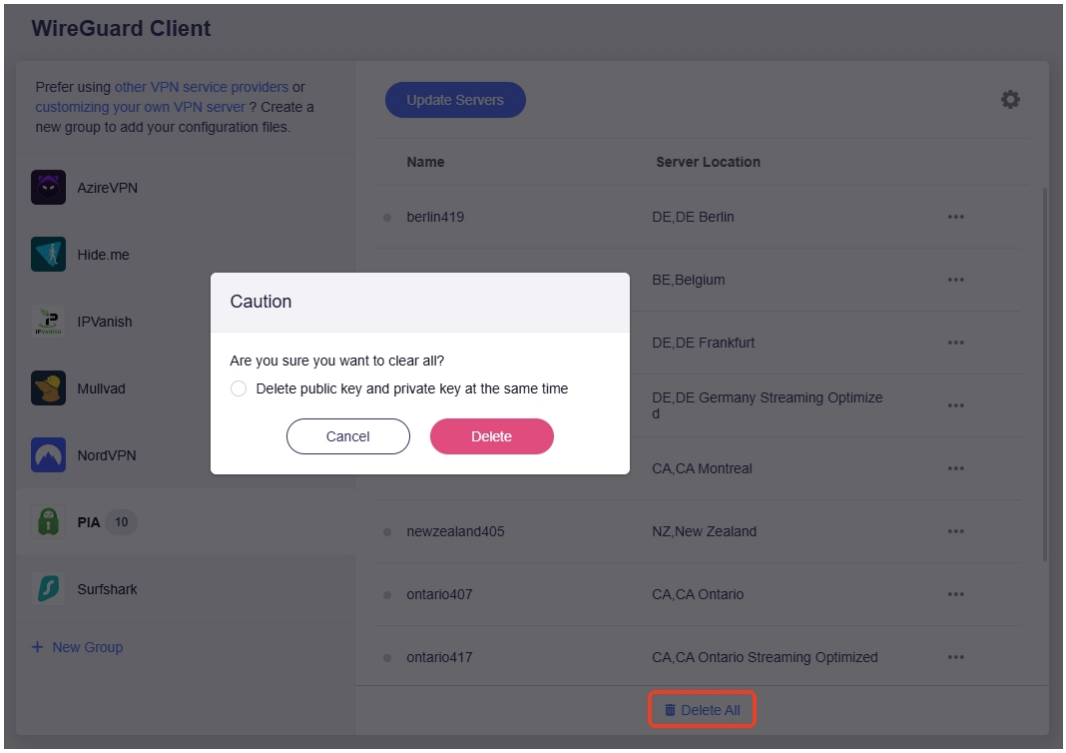
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l’engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

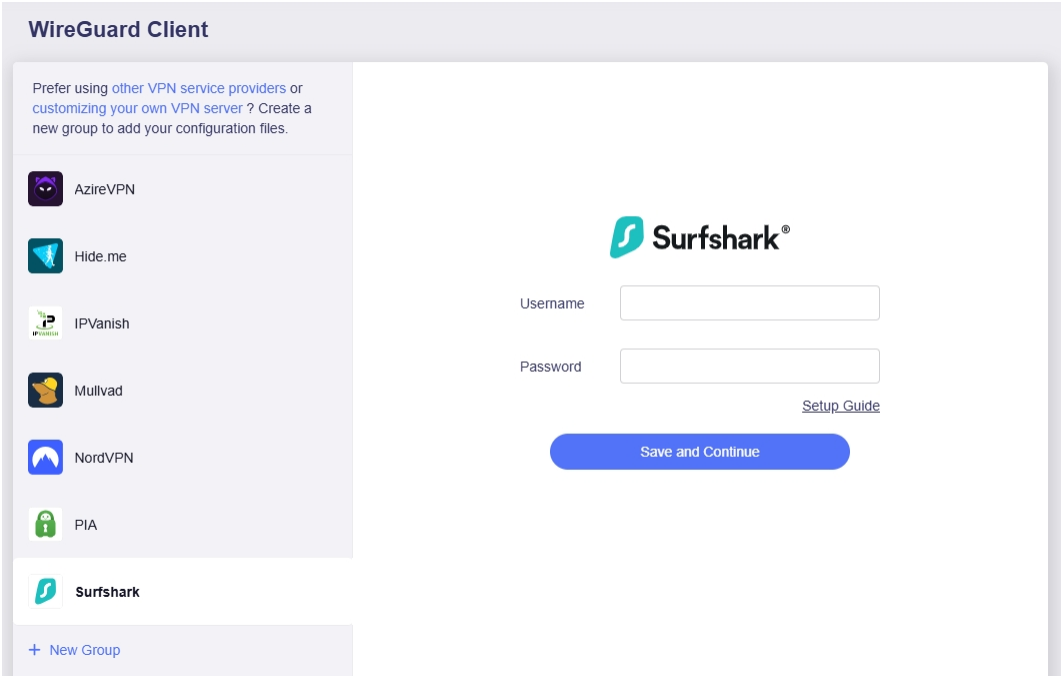
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



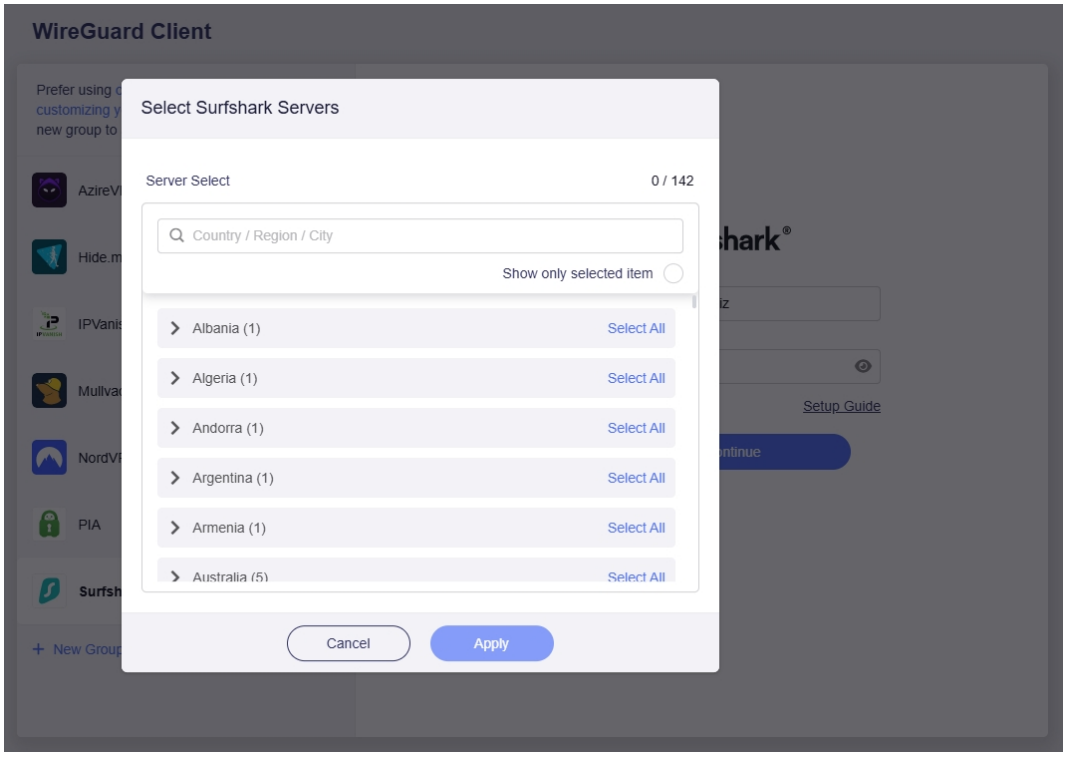
11.2.8 Configuration de Surfshark

Suivez les étapes ci-dessous pour configurer le routeur comme client Surfshark.

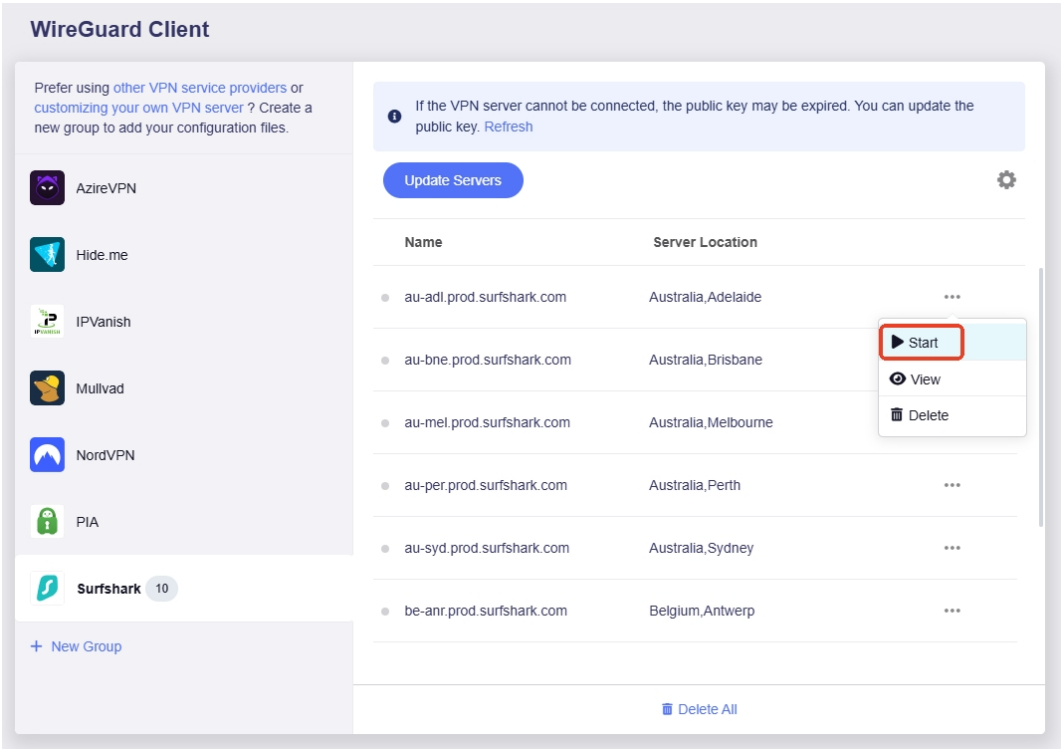
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Surfshark**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



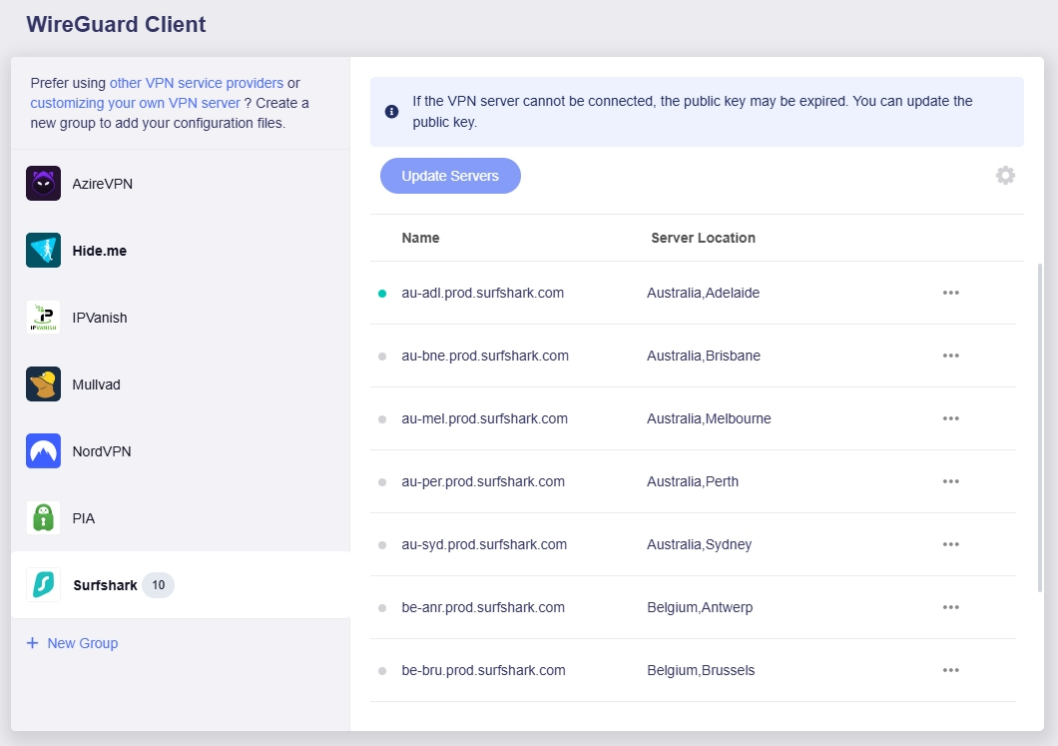
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



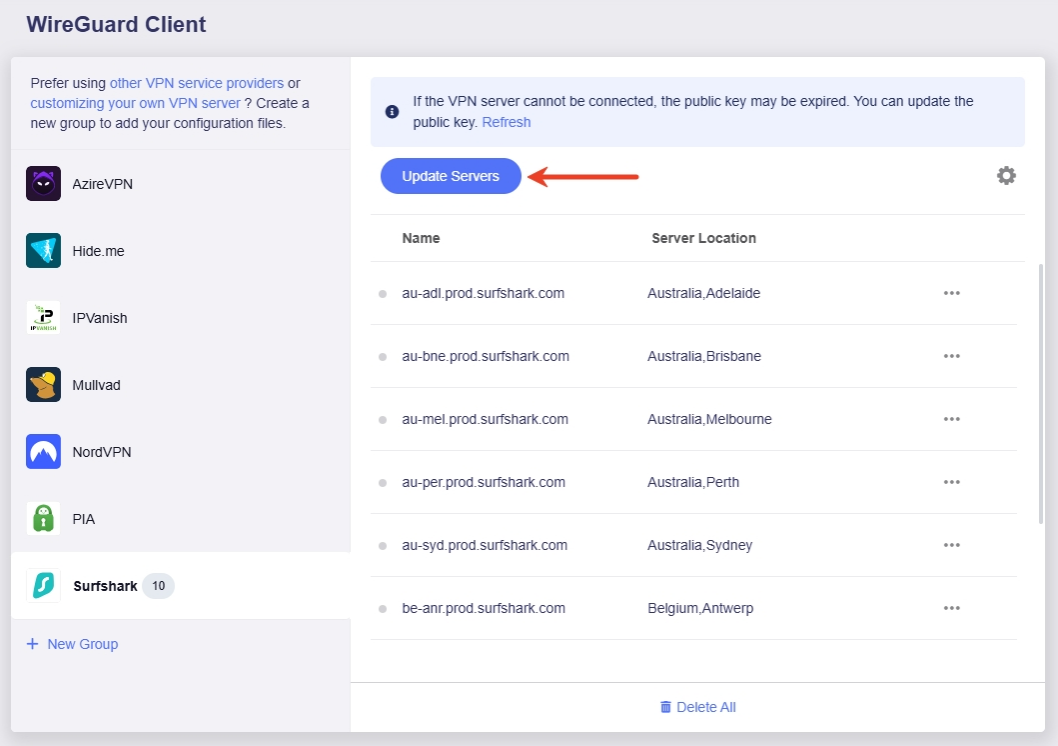
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

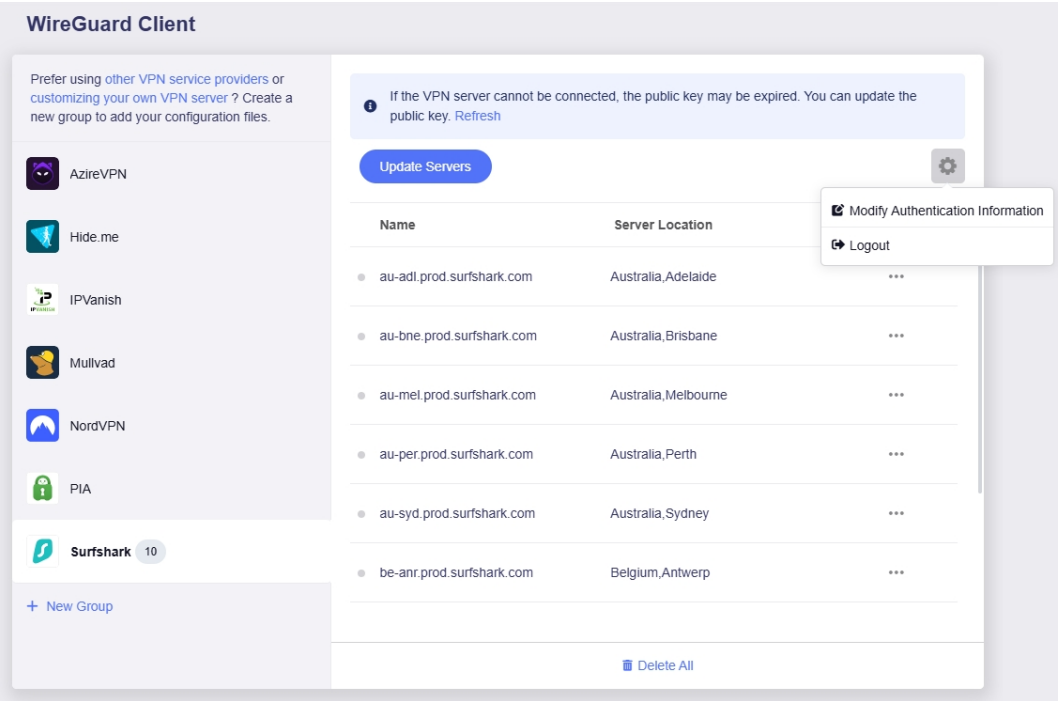
6. Mettez à jour les serveurs.

   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



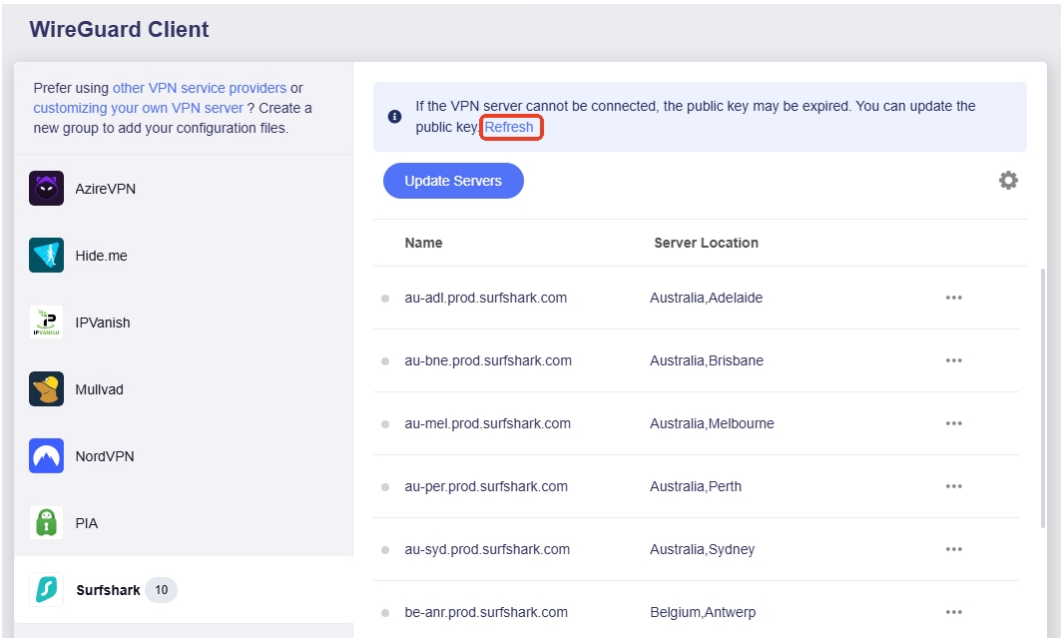
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



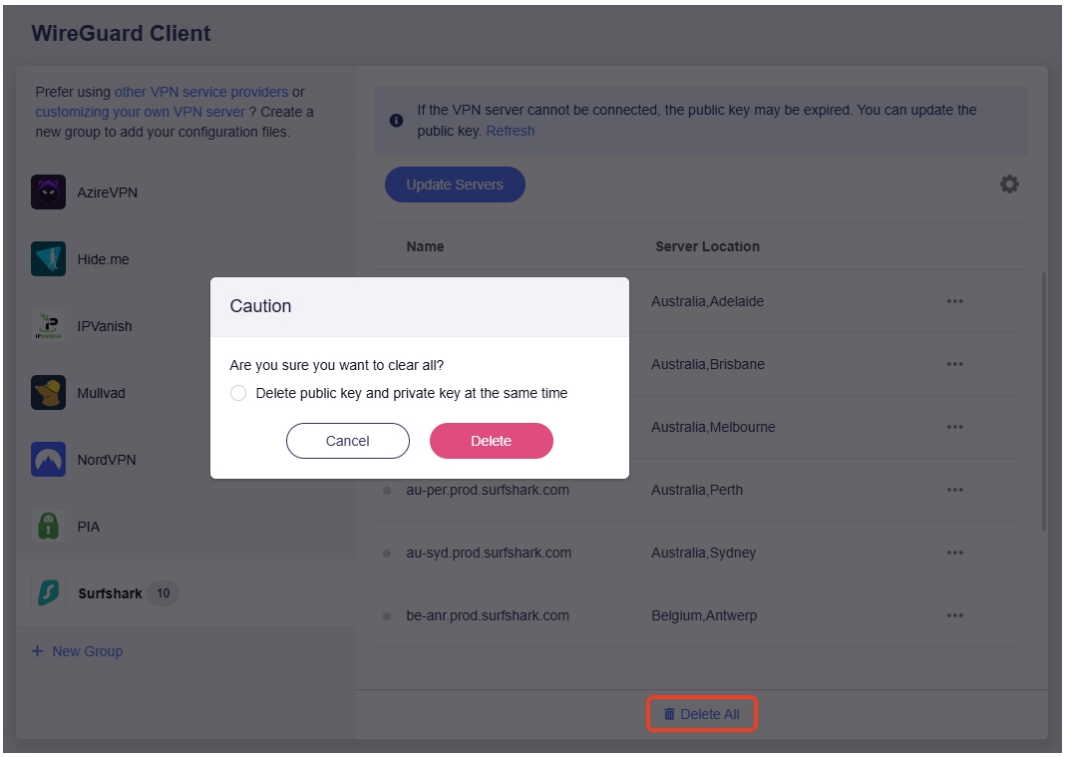
8. Actualisez les données.

   Si la connexion au serveur VPN échoue, cliquez sur **Actualiser (Refresh)** pour mettre à jour la clé publique.



9. Supprimez tous les fichiers.

   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.

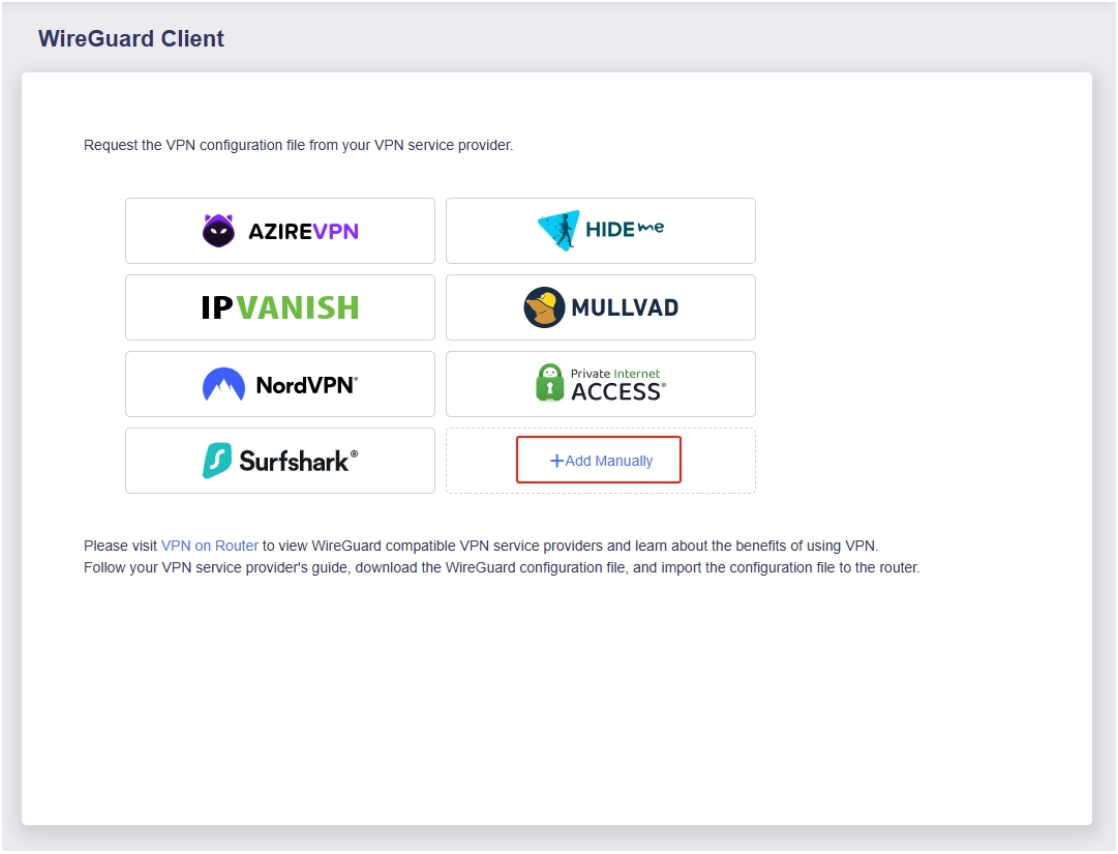


11.2.9 Configuration manuelle d’un client WireGuard pour un autre fournisseur

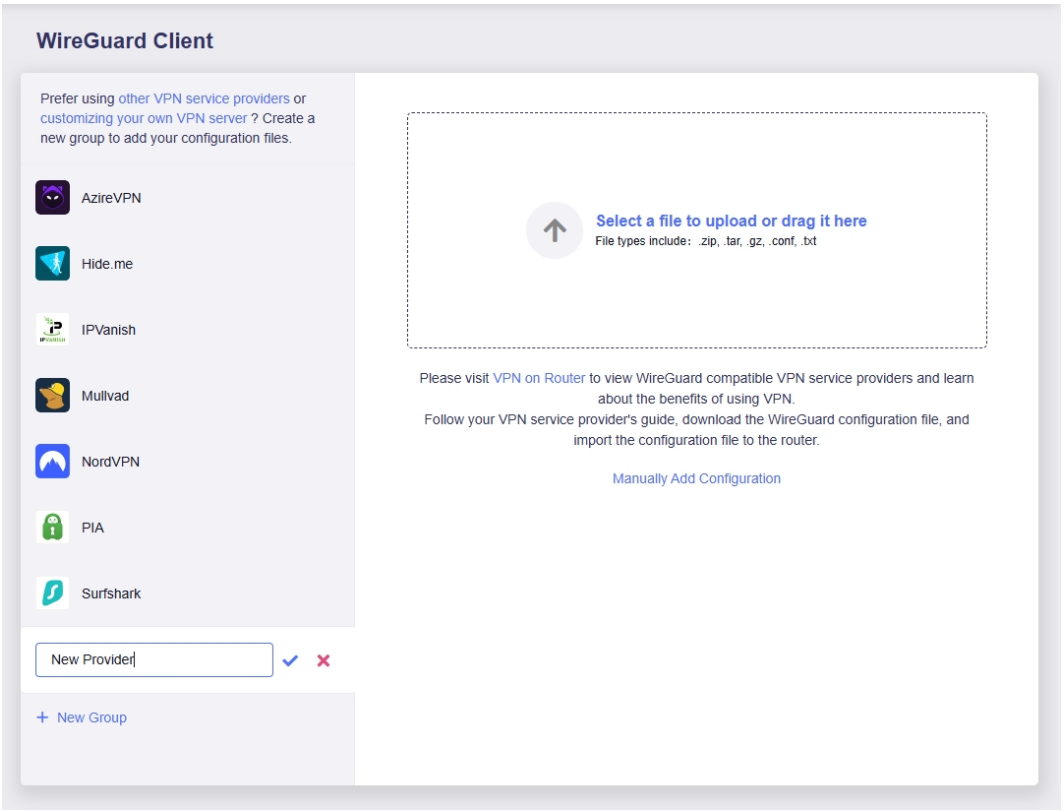
Si votre fournisseur WireGuard n’est pas intégré à l’interface Web, récupérez d’abord le fichier de configuration sur son site officiel, puis importez-le sur le routeur. Si vous ne savez pas comment télécharger les fichiers, consultez ce guide ou contactez l’assistance du fournisseur.

Suivez les étapes ci-dessous pour importer le fichier sur le routeur et configurer le client WireGuard.

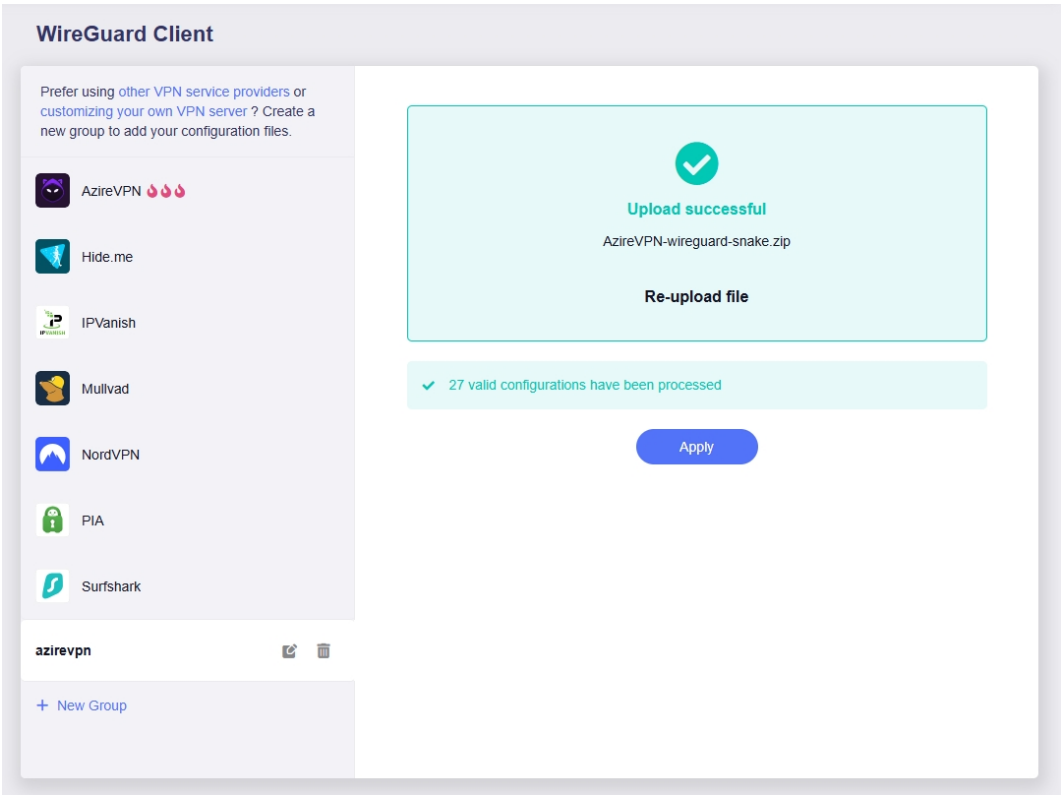
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Ajouter manuellement (Add Manually)**.



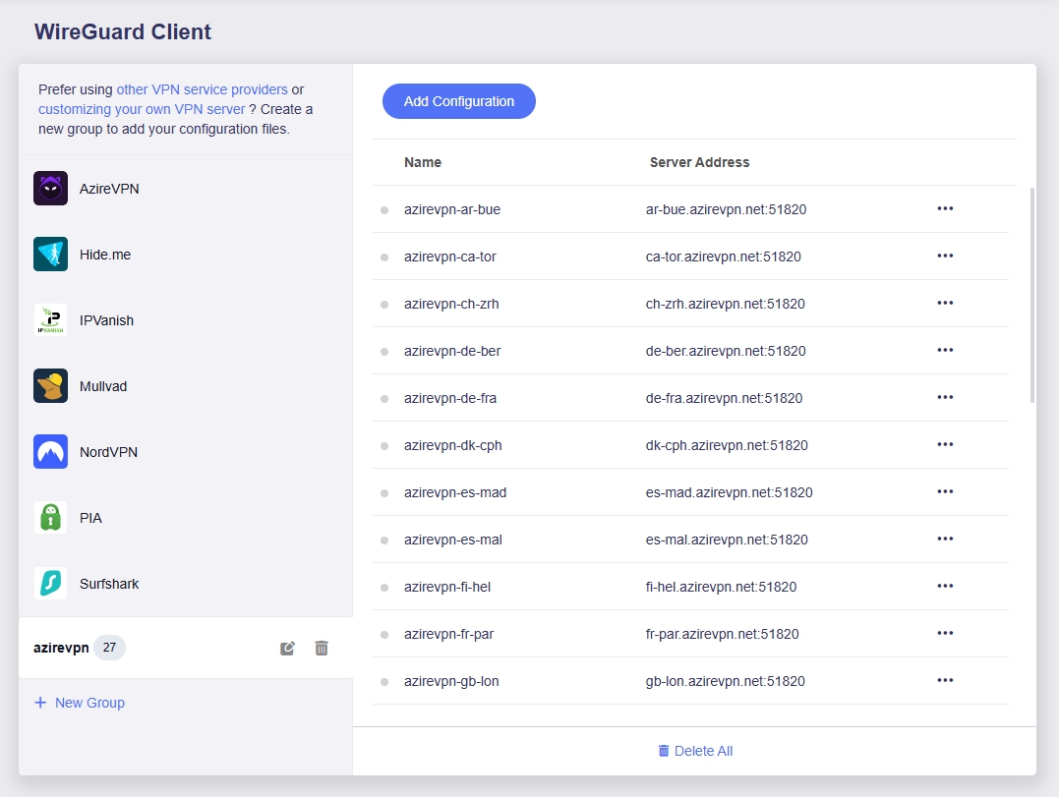
2. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



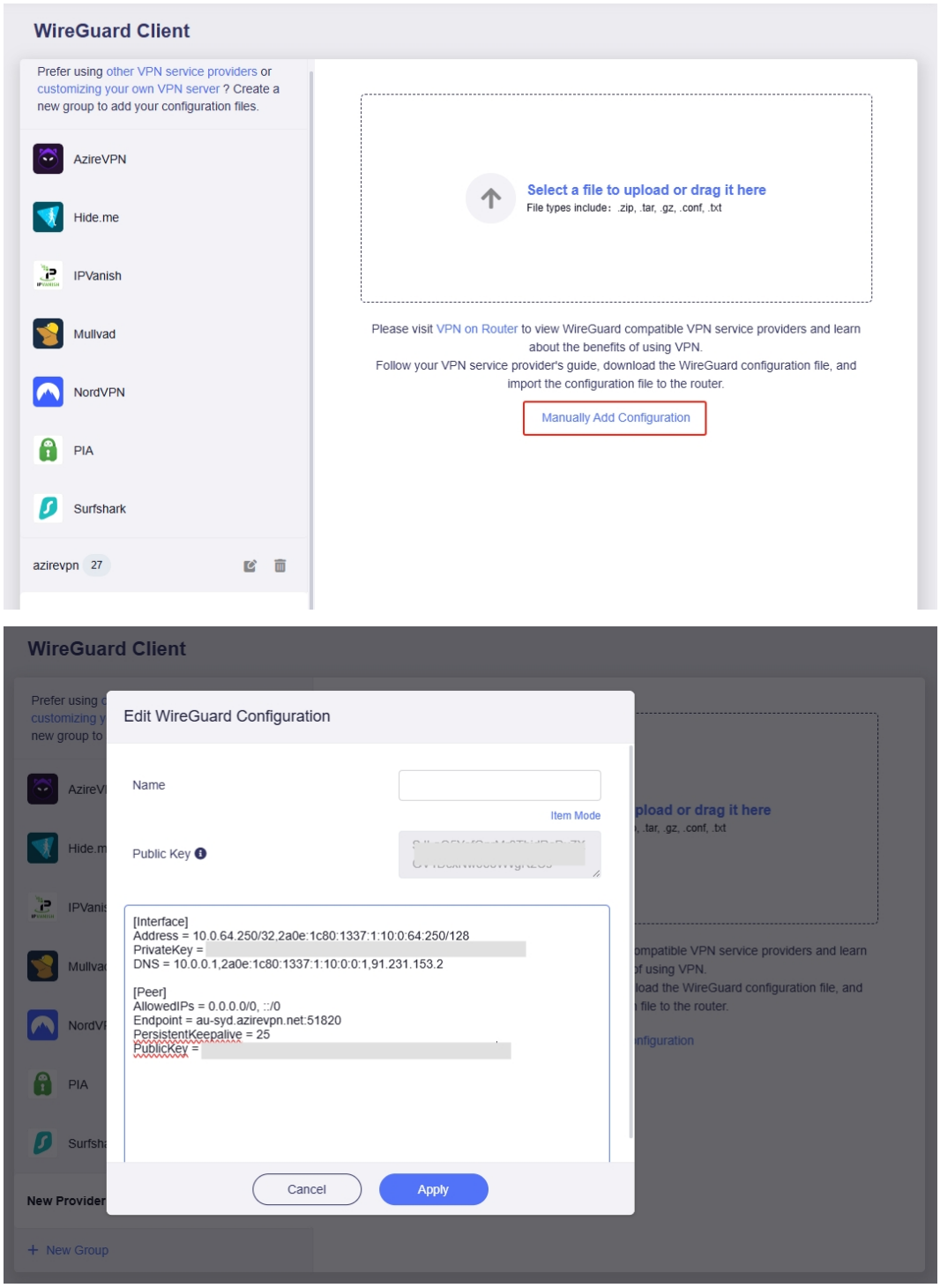
3. Cliquez sur la zone d’importation et sélectionnez votre fichier WireGuard. Les formats zip, tar, gz, conf et txt sont pris en charge. Cliquez sur **Appliquer (Apply)**.



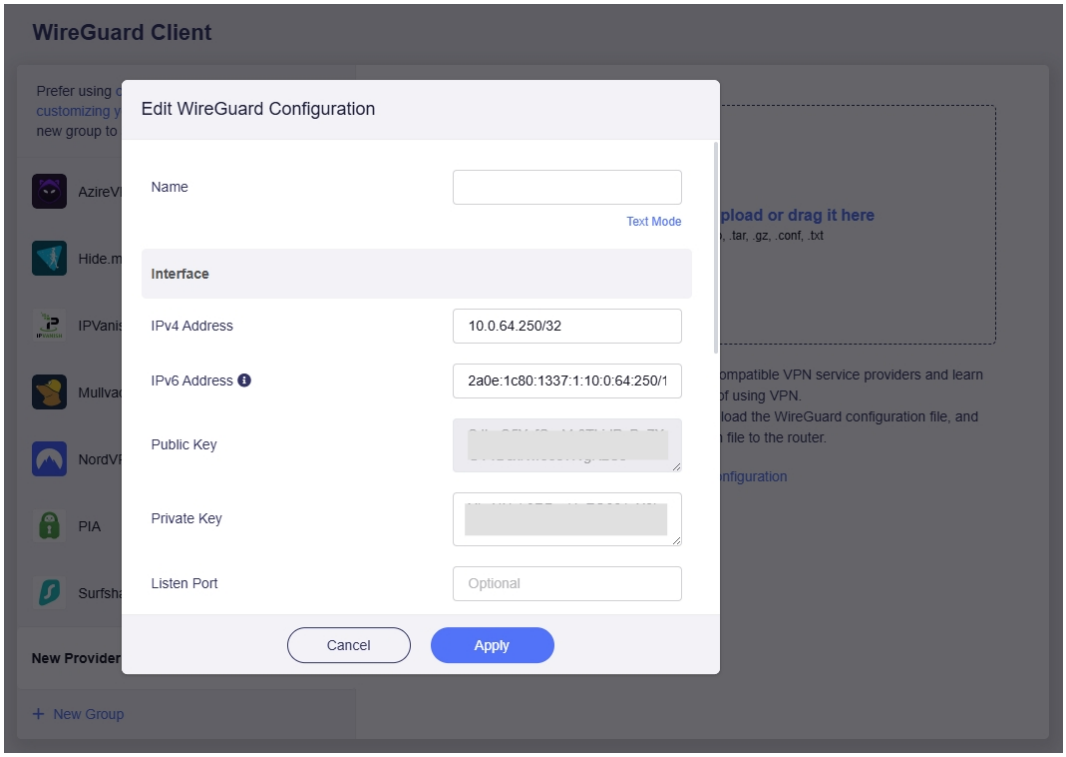
Si vous importez une archive contenant plusieurs fichiers de configuration, elle est décompressée automatiquement, comme ci-dessous.



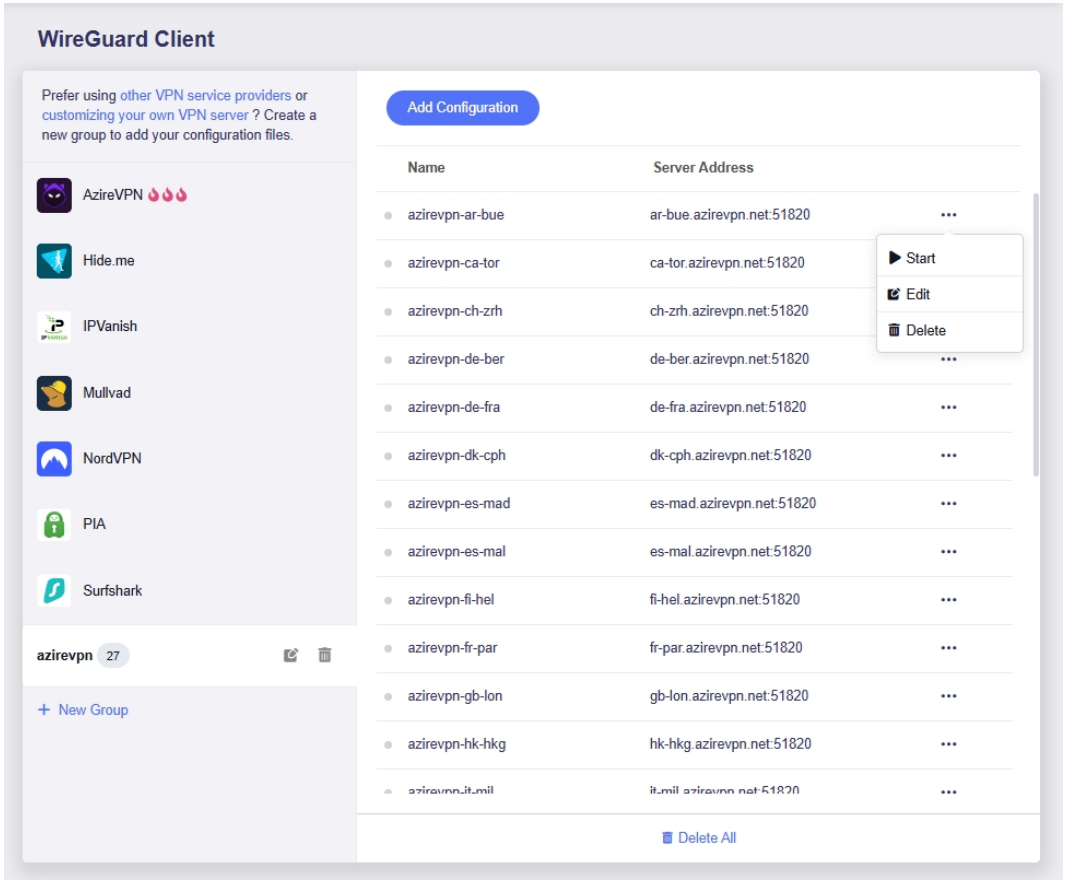
Vous pouvez aussi cliquer sur **Ajouter une configuration manuellement (Manually Add Configuration)** en bas de la zone d'importation, renseigner la configuration sous forme de texte, puis cliquer sur **Appliquer (Apply)**.



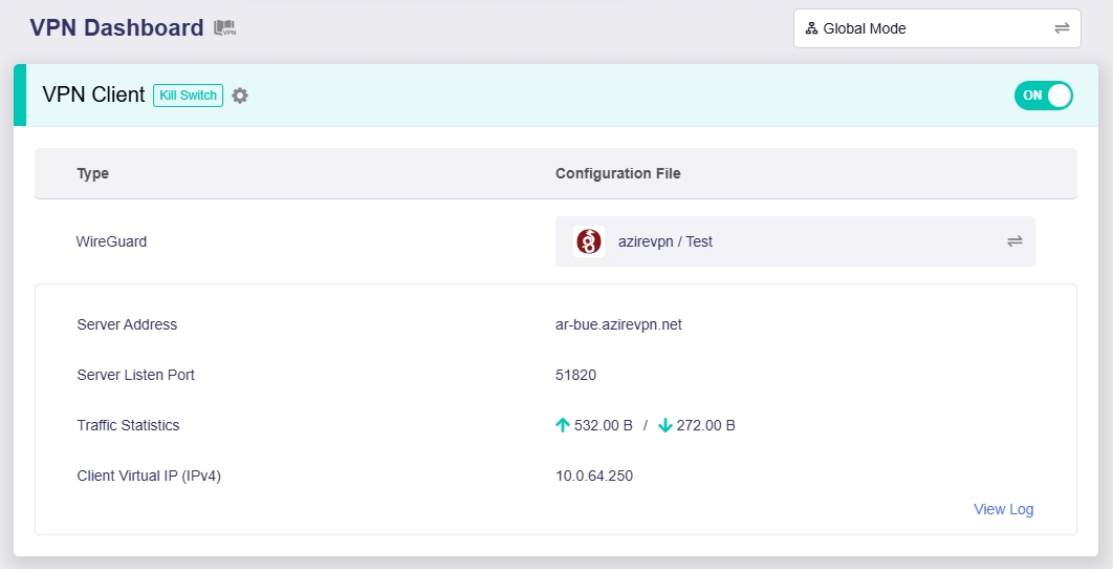
Pour vérifier chaque paramètre, passez en mode Élément (Item), contrôlez la configuration, puis cliquez sur **Appliquer (Apply)**.



4. Cliquez sur les trois points à droite pour lancer la connexion.



5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration. Consultez les détails dans le **Tableau de bord VPN (VPN Dashboard)**.



Chapitre 12

Tor

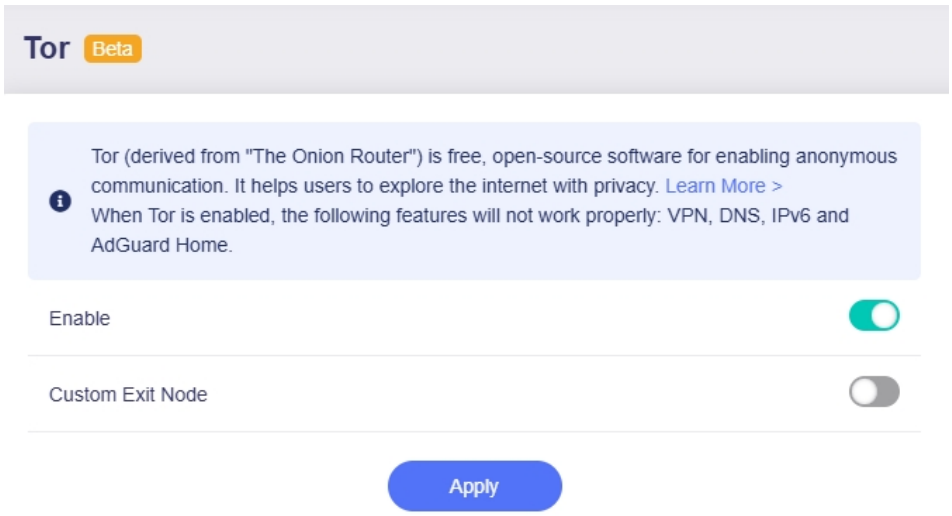
Ce chapitre présente brièvement Tor (The Onion Router), un logiciel libre et gratuit permettant des communications anonymes.

Tor, abréviation de **The Onion Router**, est un logiciel libre et gratuit permettant des communications anonymes. Il aide à naviguer sur Internet en préservant la confidentialité. Cette fonction est actuellement en version bêta et peut présenter des anomalies.

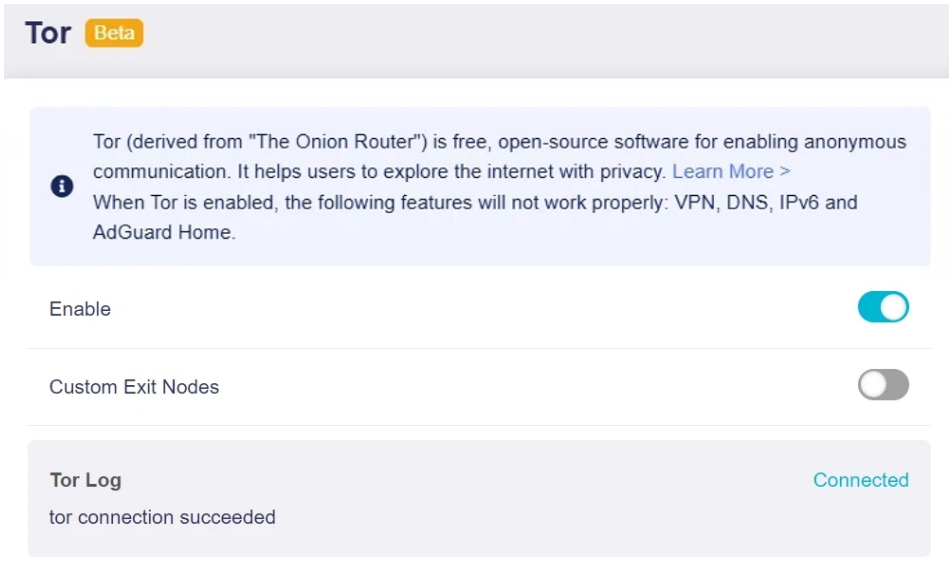
Lorsque Tor est activé, VPN, DNS, IPv6 et AdGuard Home ne fonctionnent pas correctement.

Pour configurer Tor, procédez comme suit.

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Tor**. Activez l'interrupteur, activez les nœuds de sortie personnalisés si nécessaire, puis cliquez sur **Appliquer (Apply)**.



2. La connexion démarre. Si votre réseau remplit les conditions nécessaires, l'état Connecté s'affiche.


Tor
Beta
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Learn More >
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.
Enable
Custom Exit Nodes
Tor Log
Connected
tor connection succeeded

Chapitre 13

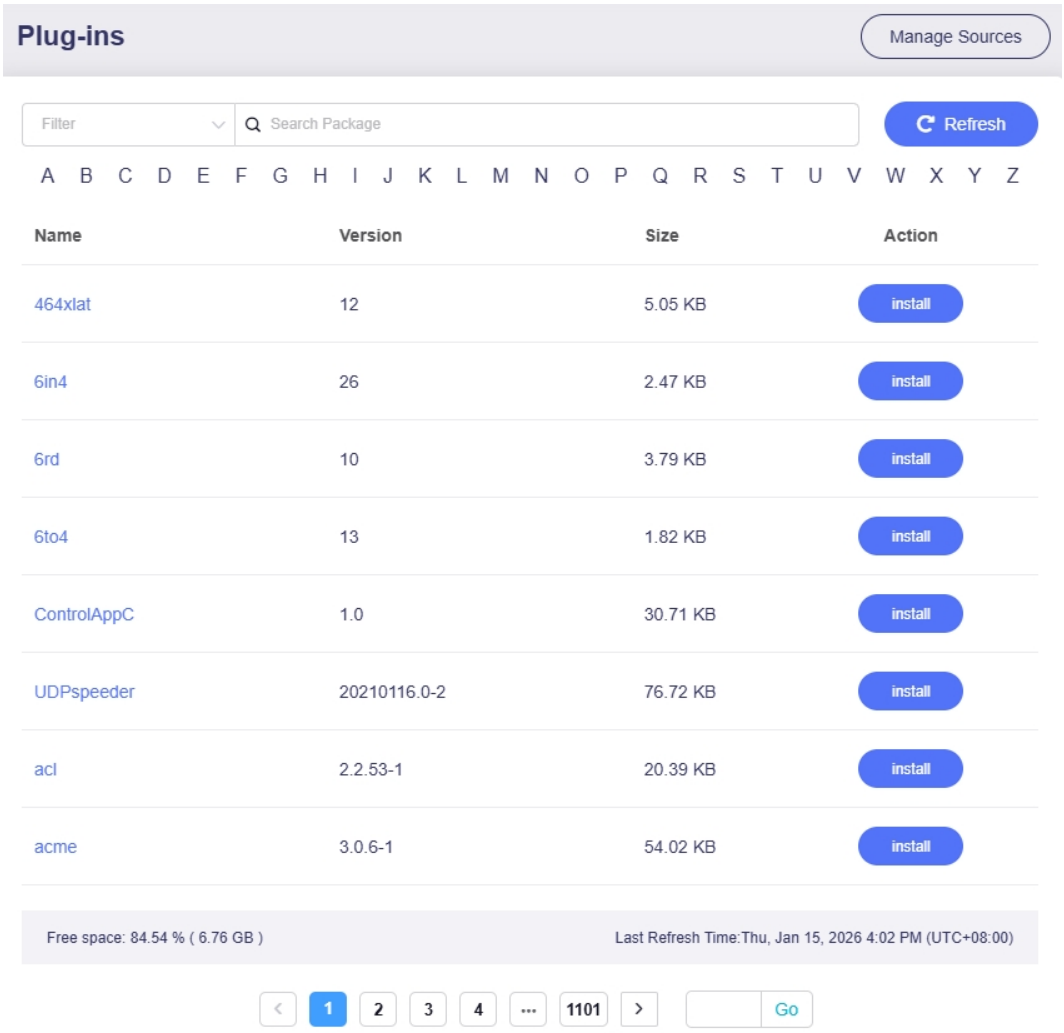
Applications

Ce chapitre présente certaines applications des routeurs GL.iNet : extensions, DNS dynamique, stockage réseau, AdGuard Home, contrôle parental, ZeroTier, Tailscale et gestion eSIM.

13.1 Extensions

La page Extensions permet de gérer les paquets OpenWrt.

Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **Extensions (Plug-ins).** Vous pouvez installer ou supprimer les paquets du dépôt. Cliquez sur **Actualiser (Refresh)** pour mettre à jour la liste avant d'installer une extension.



Remarque :

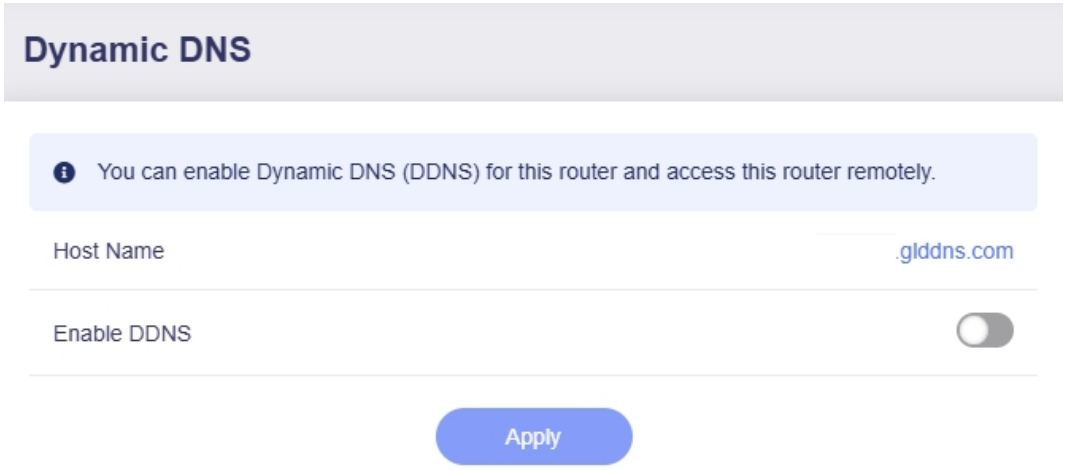
1. Il est déconseillé de mettre à jour les extensions préinstallées dans le micrologiciel officiel GL.iNet, comme nginx, AdGuard Home ou Tailscale.
2. Les extensions tierces installées manuellement peuvent être mises à jour. GL.iNet n'est toutefois pas responsable des problèmes de sécurité qu'elles peuvent entraîner. Pour toute question, contactez leurs auteurs.

13.2 DNS dynamique

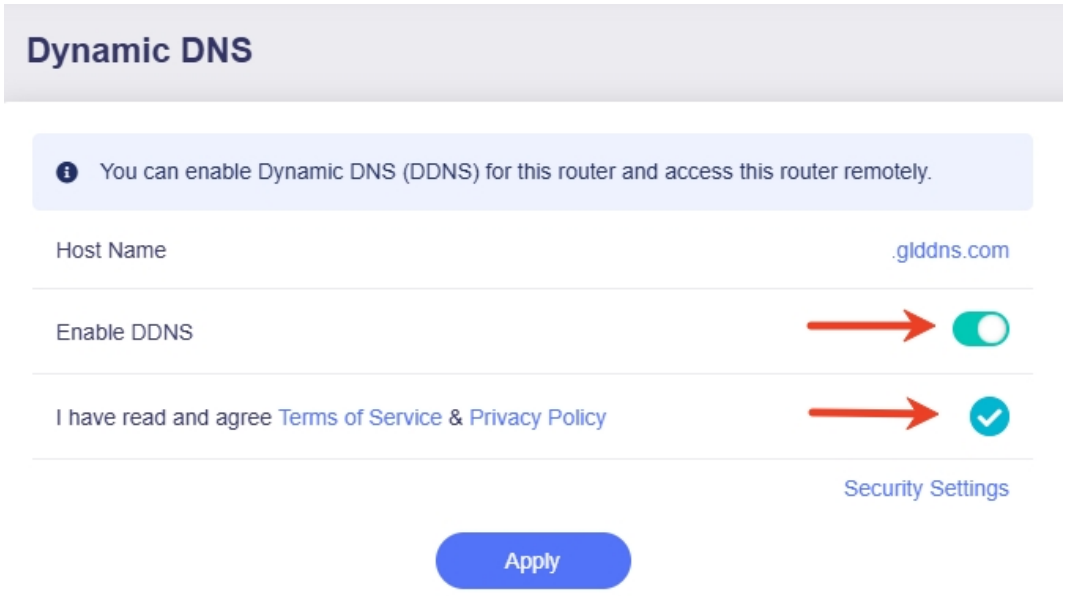
Le DNS dynamique (DDNS) associe un nom de domaine à l'adresse IP dynamique d'un appareil réseau. Il permet d'accéder au routeur à distance. Cette fonction nécessite une adresse IP publique.

13.2.1 Activation du DDNS

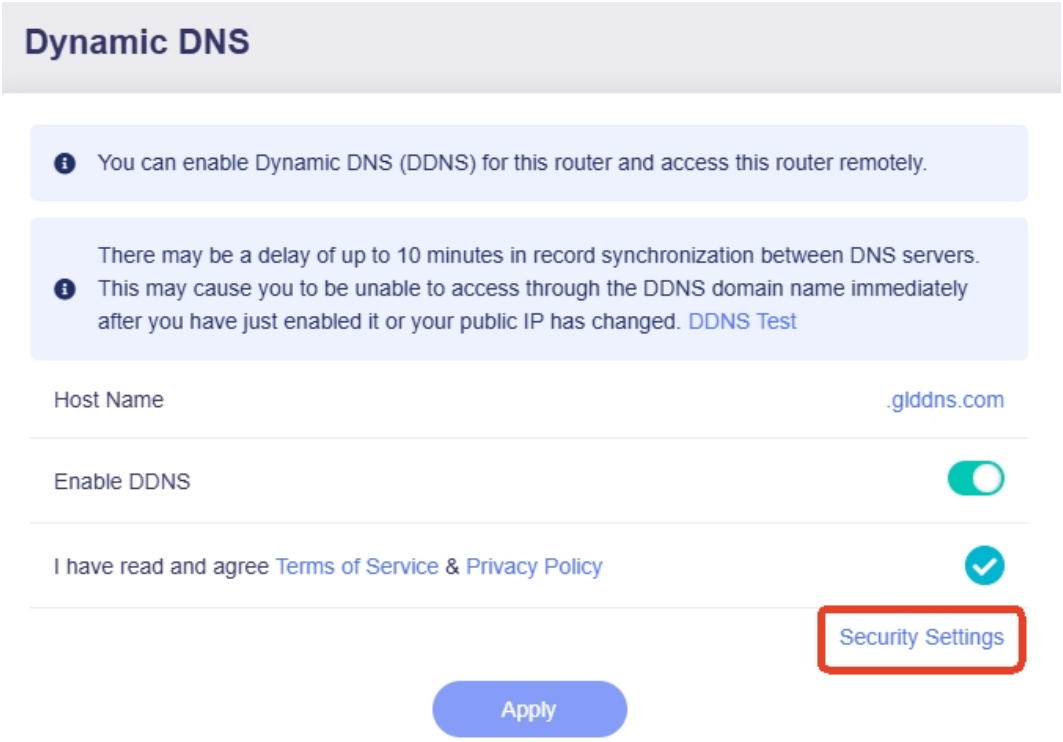
1. Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)**. La page ci-dessous s'affiche.



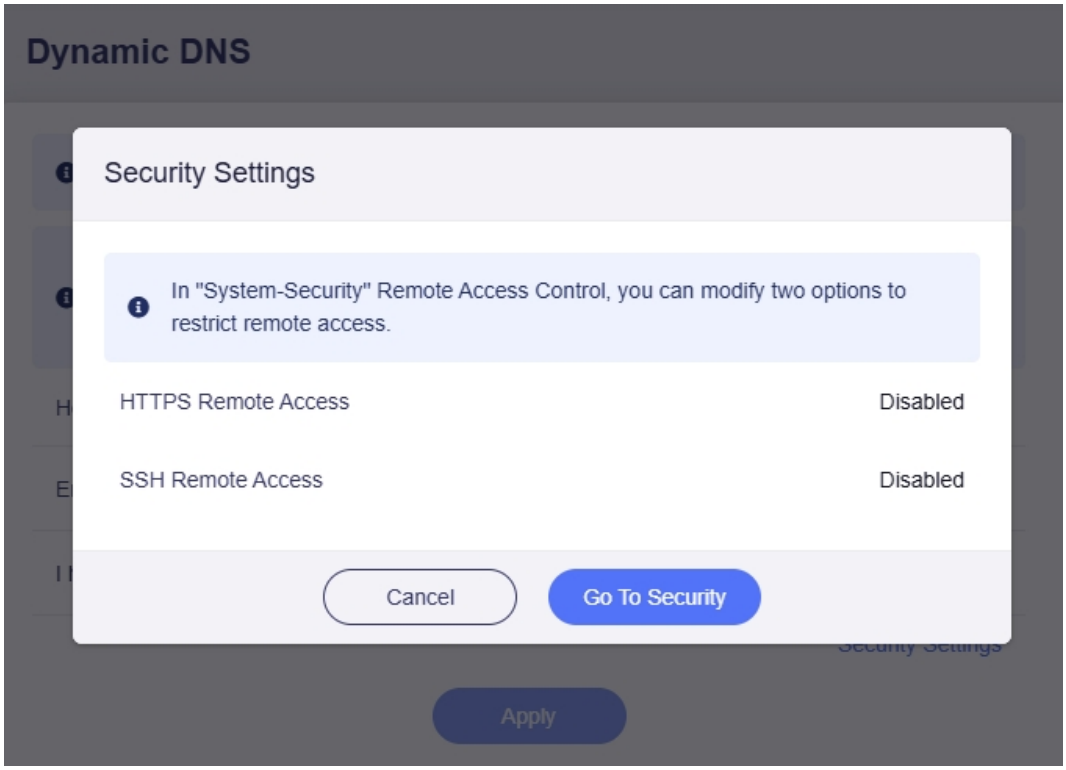
2. Activez **Activer le DDNS (Enable DDNS)**, lisez et acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



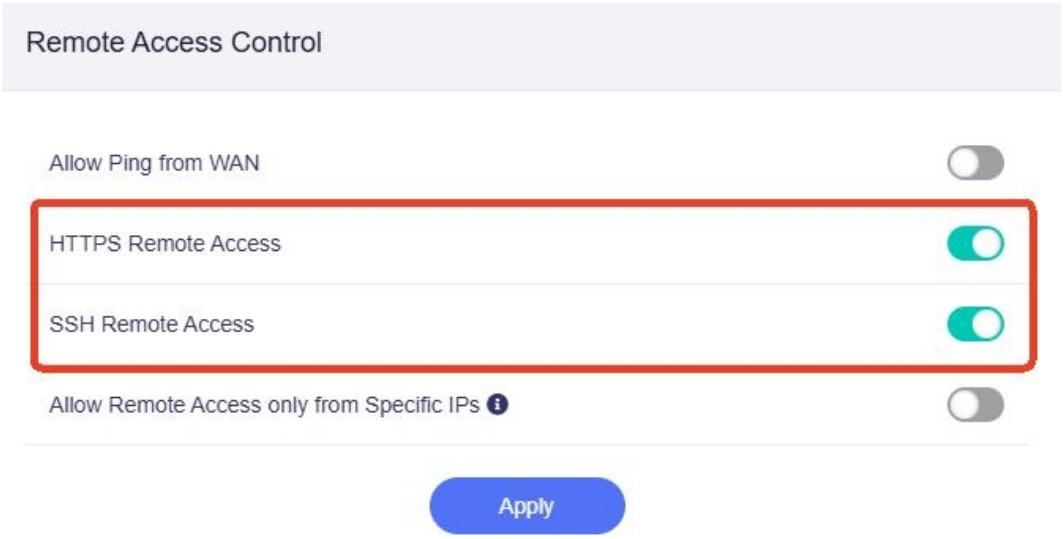
3. Cliquez sur **Paramètres de sécurité (Security Settings)** dans l'angle inférieur droit.



4. Dans la fenêtre qui s'affiche, vérifiez que l'accès distant souhaité est activé.



Si ce n’est pas le cas, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d’accès distant (Remote Access Control)** pour l’activer, puis cliquez sur **Appliquer (Apply)**.



Remarque :

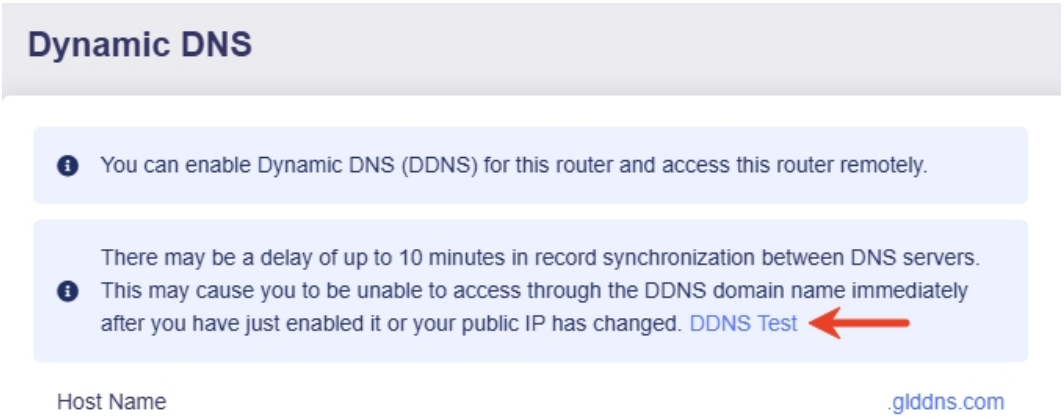
1. La synchronisation des enregistrements entre serveurs DNS peut prendre jusqu’à 10 minutes. L’accès par le domaine DDNS peut donc être indisponible immédiatement après son activation ou après un changement d’IP publique.
2. Si vous activez simultanément le DDNS et un client VPN, vérifiez que Services GL.iNet via le VPN (Services From GL.iNet Use VPN) est désactivé.

13.2.2 Vérification du fonctionnement du DDNS

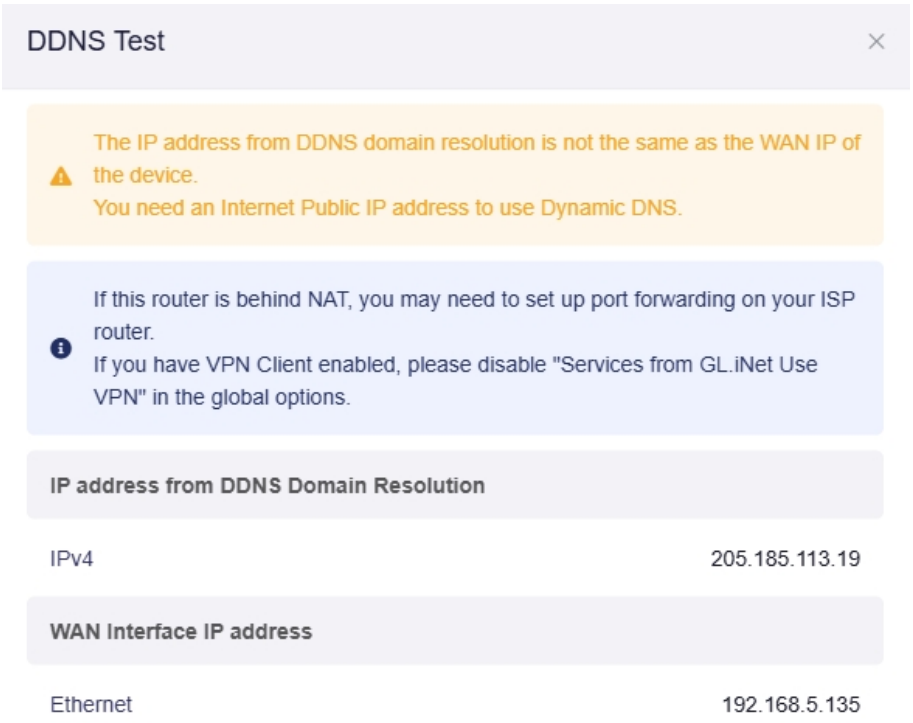
Vérifiez le DDNS avec l'outil de test intégré ou manuellement à l'aide de commandes.

Méthode 1 : outil de test DDNS

1. Sur la page DNS dynamique, cliquez sur **Test DDNS (DDNS Test)**.



2. Vérifiez que l'IP obtenue par résolution du domaine DDNS correspond à l'IP WAN du routeur. Sinon, un message jaune indique que le routeur peut se trouver derrière un NAT et qu'une redirection de port est nécessaire sur le routeur en amont.



Méthode 2 : commandes

1. Utilisez la commande nslookup avec *nslookup xxxxxxx.glddns.com 8.8.8.8* pour afficher l'adresse IP associée au domaine. L'exemple ci-dessous utilise Beryl AX (GL-MT3000).



   - Remplacez « xxxxxxx.glddns.com » par votre nom d'hôte.
   - « 8.8.8.8 » est le DNS de Google. Utilisez-le ou indiquez un autre serveur, puis appuyez sur Entrée.

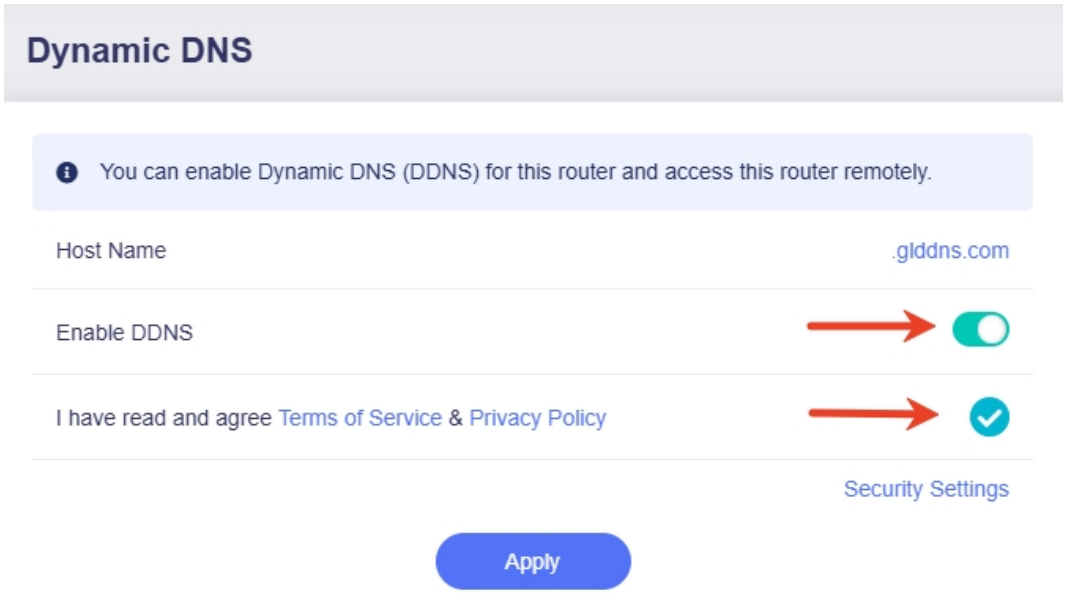
2. Une IP publique, comme « 183.178.10.100 » dans l'image, indique que le domaine DDNS est bien associé à une adresse publique. Un message comme « server can't find xxxxxxx.glddns.com » peut indiquer un échec de résolution. Passez à l'étape suivante pour vérifier.
3. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET**. Relevez l'adresse IP WAN du routeur sur l'interface actuellement active. Comparez-la à l'adresse IP publique obtenue précédemment. Si elles sont identiques, le DDNS fonctionne ; sinon, il ne fonctionne pas.

13.2.3 Accès HTTPS à distance

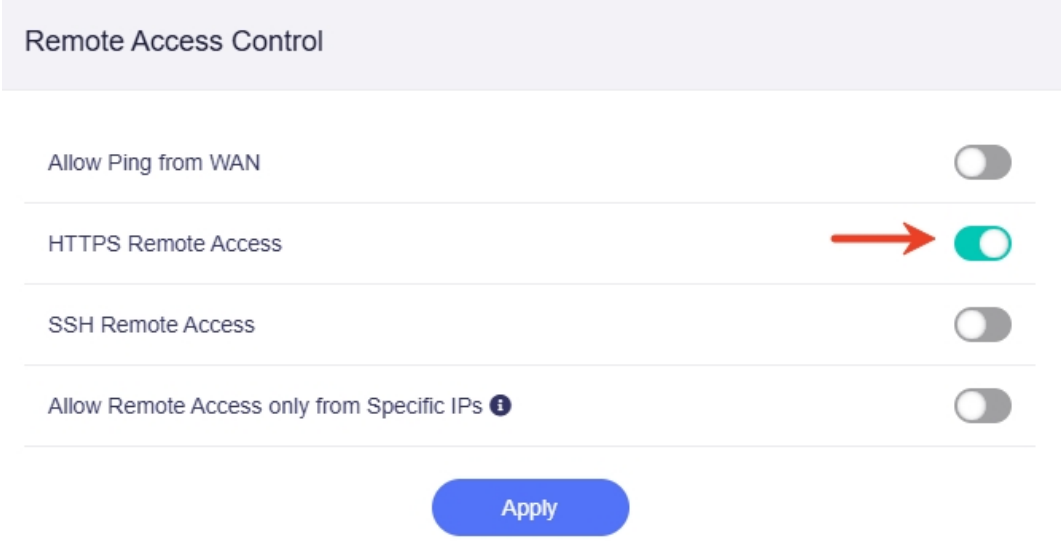
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 443** sur le routeur en amont.

Pour activer l'accès HTTPS à distance, procédez comme suit.

1. Sur la page DNS dynamique, activez **Activer le DDNS (Enable DDNS)**, acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.

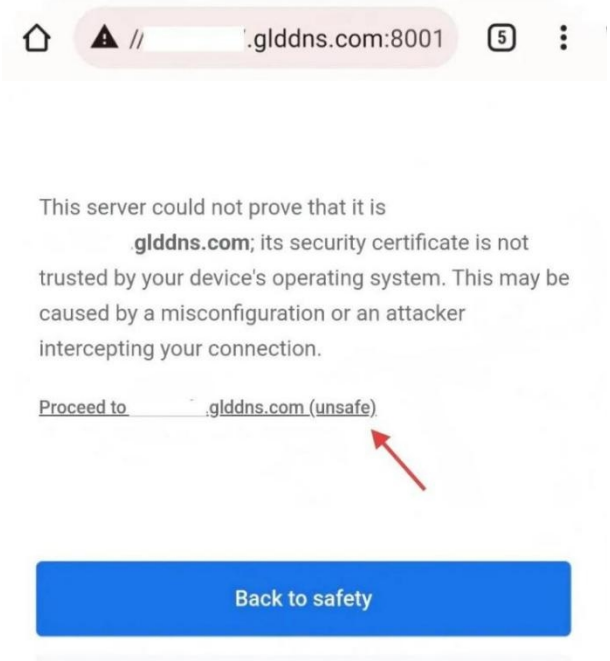


2. Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)**. Activez **Accès HTTPS à distance (HTTPS Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



3. Vous pouvez ensuite ouvrir l'interface depuis n'importe où avec le nom d'hôte DDNS en HTTPS, par exemple **https://xxxxxxx.glddns.com**. Si une redirection de port est configurée, utilisez **https://xxxxxxx.glddns.com:external_port** en remplaçant external_port par le numéro de port réel.

Remarque : cette fonction utilise des certificats autosignés. Le navigateur affiche donc « Votre connexion n'est pas privée » lors de l'accès HTTPS par le nom d'hôte DDNS. Cliquez sur **Avancé (Advanced)** en bas de la page, puis sur **Continuer vers xxxxxxx.glddns.com (Proceed to xxxxxxx.glddns.com)** pour poursuivre.



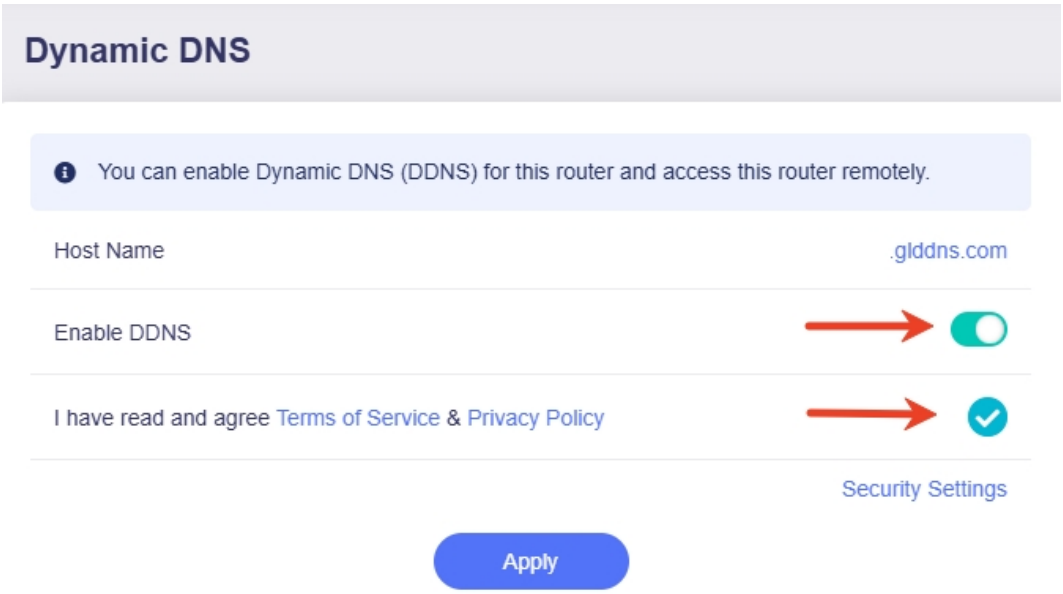
Vous pouvez alors accéder à l’interface Web par le nom d’hôte DDNS en **HTTPS**.

13.2.4 Accès SSH à distance

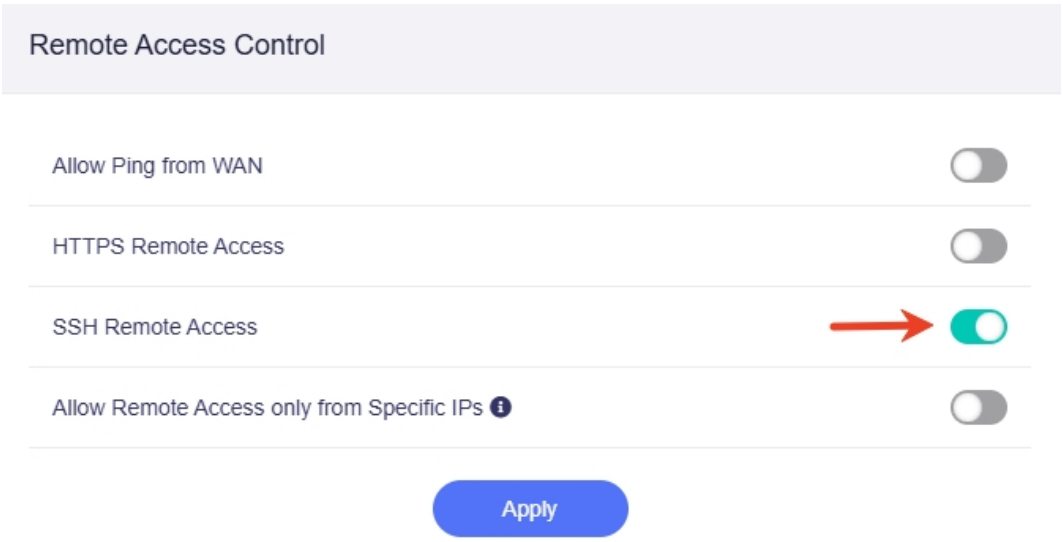
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 22** sur le routeur en amont.

Pour activer l'accès SSH à distance, procédez comme suit.

1. Sur la page DNS dynamique, activez **Activer le DDNS (Enable DDNS)**, acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



2. Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)**. Activez **Accès SSH à distance (SSH Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



Vous pouvez ensuite accéder au routeur depuis n'importe où par SSH avec le nom d'hôte DDNS, par exemple **ssh root@xxxxxxx.glddns.com**. Si une redirection de port est configurée, utilisez **ssh root@xxxxxxx.glddns.com:external_port** en remplaçant external_port par le numéro de port réel.

13.3 Stockage réseau

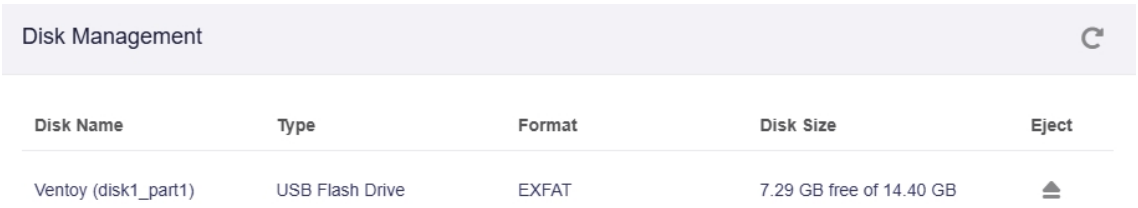
Le stockage réseau permet de partager des fichiers sans fil entre appareils en branchant un support USB ou une carte SD au routeur. Le support devient un lecteur réseau partagé, accessible aux appareils connectés par Wi-Fi.

Beryl AX possède un port USB compatible avec les clés USB et les disques durs externes portables. Vous pouvez configurer Samba, WebDAV ou DLNA pour ces supports de stockage, qui prennent en charge les formats courants, comme NTFS, FAT32 et EXT4.

Remarque : les disques durs USB consomment beaucoup d'énergie. Utilisez une alimentation externe pour éviter les dysfonctionnements.

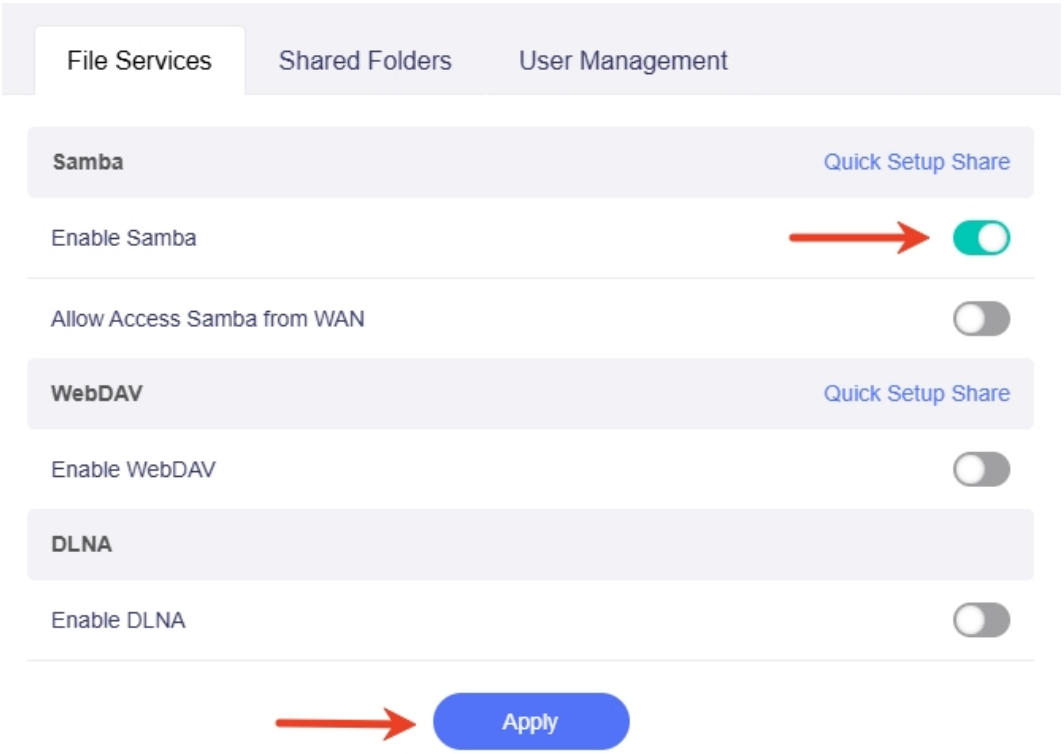
13.3.1 Branchement du stockage

1. Branchez le périphérique de stockage au routeur.
   - Pour une clé USB, branchez-la directement au port USB.
   - Pour un disque dur externe, branchez son alimentation séparée si nécessaire, puis reliez-le au routeur.
2. Dans l'interface Web, ouvrez **APPLICATIONS** > **Stockage réseau (Network Storage)**. Activez les services de transfert de fichiers et gérez les dossiers partagés ici.
3. Si le support est détecté, la section **Gestion des disques (Disk Management)** s'affiche comme ci-dessous.



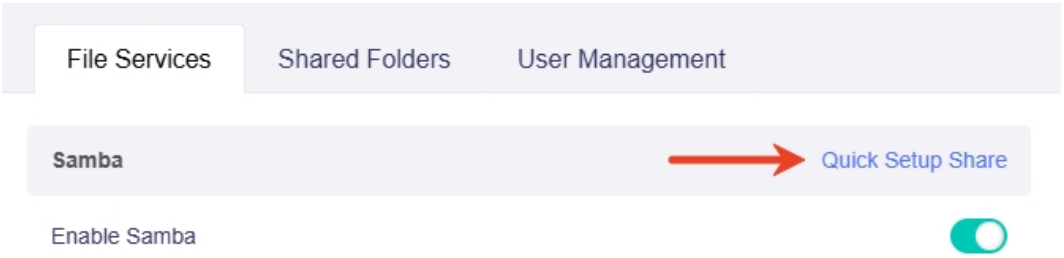
13.3.2 Configuration de Samba

1. Dans la section **Services de fichiers (File Services)**, activez **Activer Samba (Enable Samba)**, puis cliquez sur **Appliquer (Apply)**.

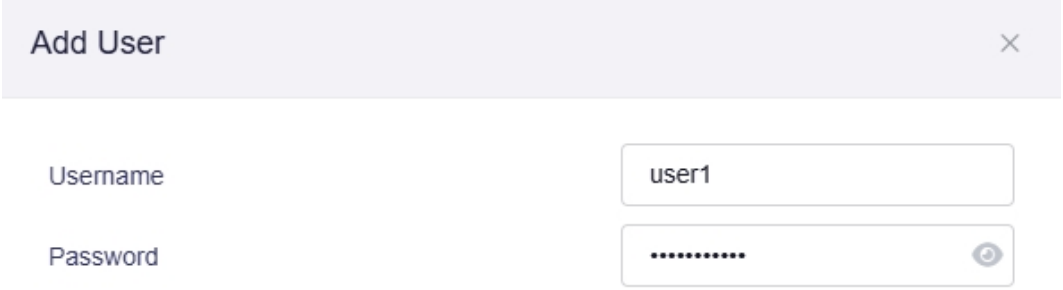


   - **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** : activez cette option pour que les appareils en amont accèdent à Samba.

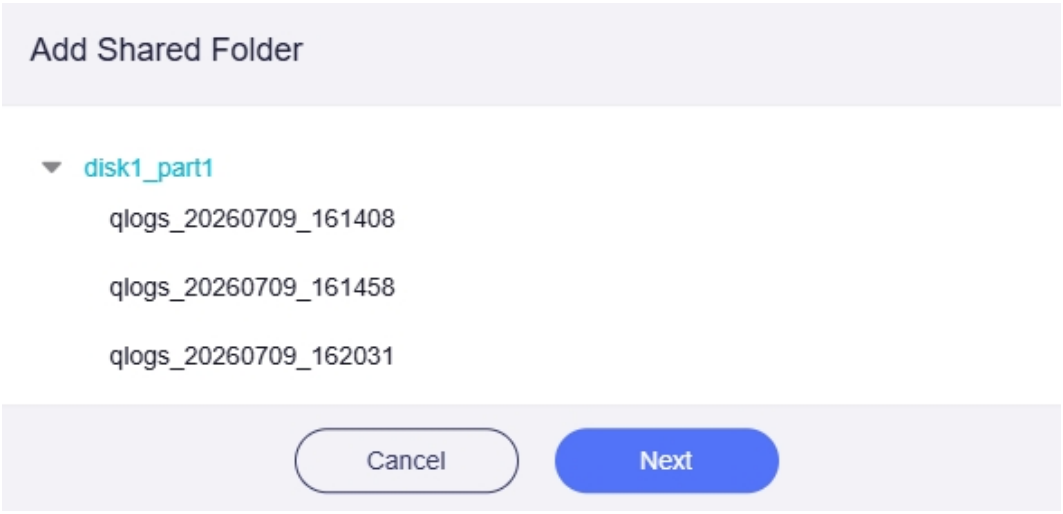
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



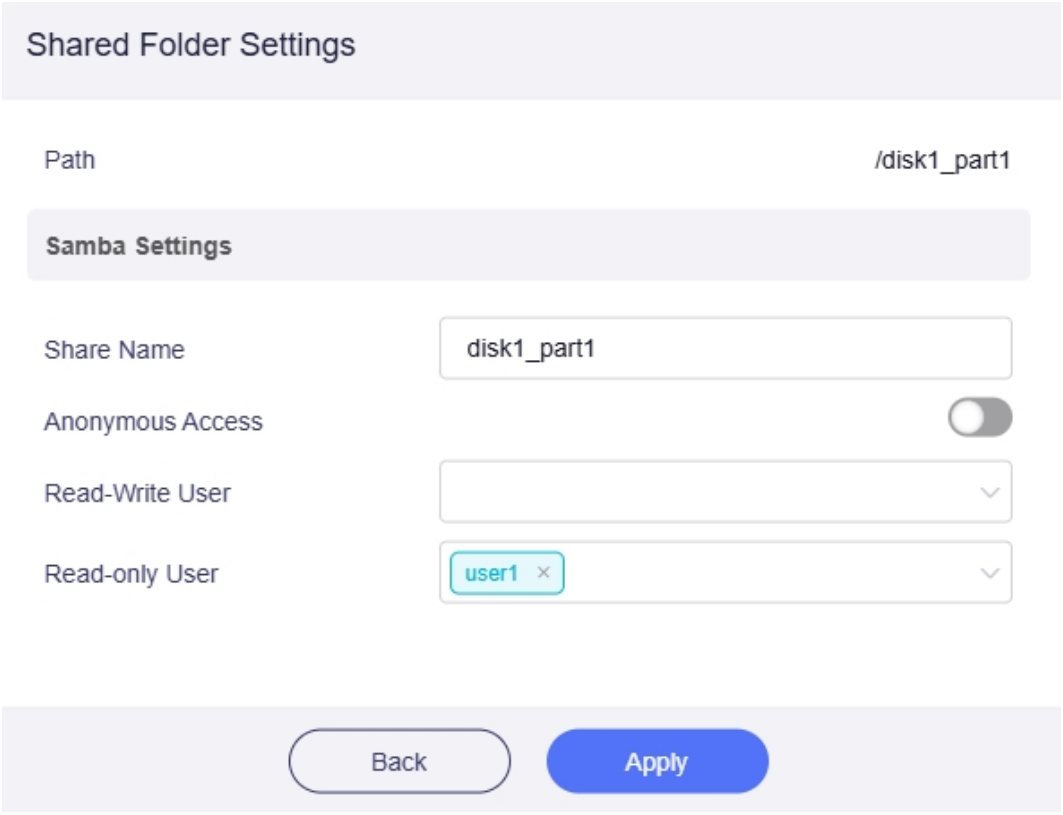
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



4. Cliquez sur le triangle pour afficher tous les dossiers. Sélectionnez le dossier à partager, puis cliquez sur **Suivant (Next)**. Pour partager le disque entier, cliquez sur son nom, par exemple disk1_part1.

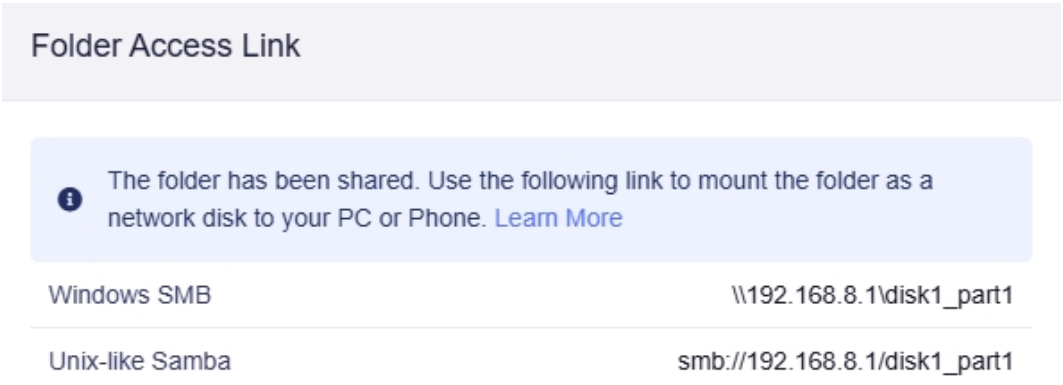


5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**. Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez sur **Appliquer (Apply)**.



Conseil : par sécurité, il est déconseillé d'activer l'accès anonyme.

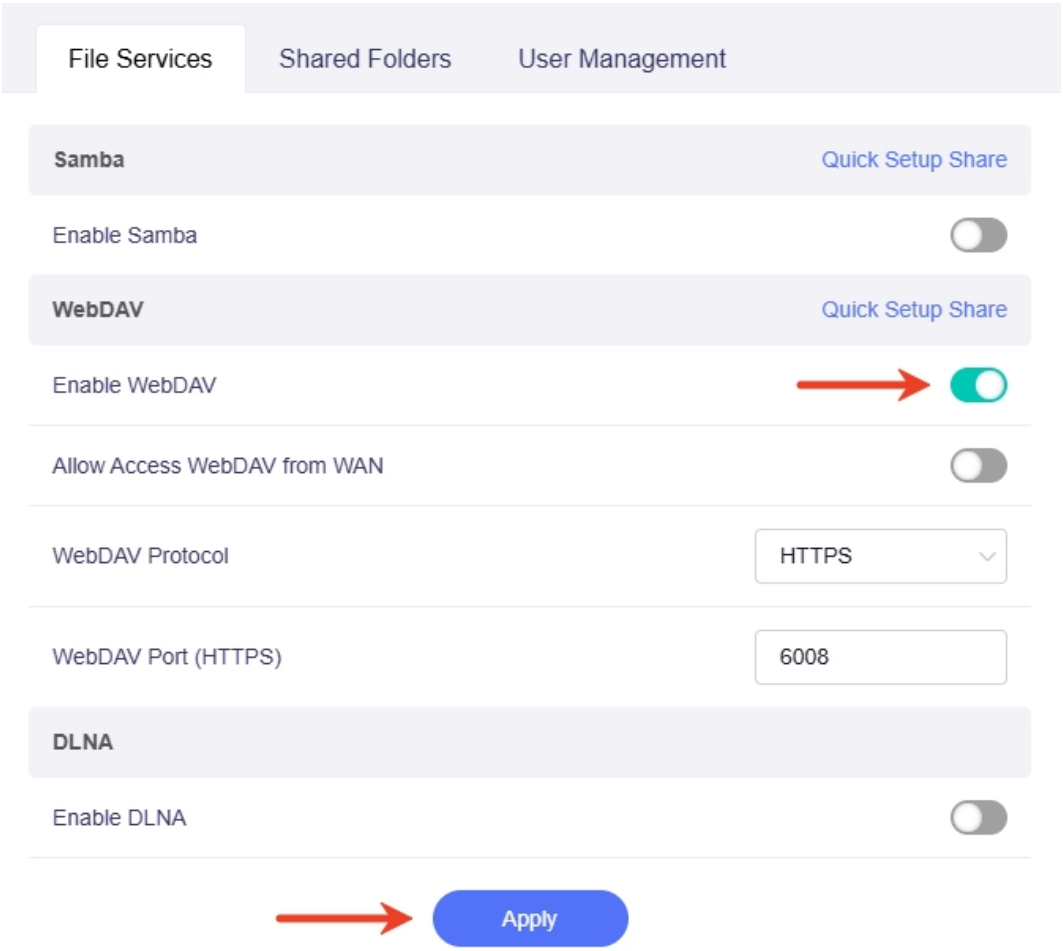
6. Récupérez le lien d'accès au dossier.
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via Samba.



Remarque : si vous activez **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** et accédez au dossier depuis le réseau en amont, remplacez l'IP du routeur dans le lien, 192.168.8.1 par défaut, par son IP WAN affichée sur la page INTERNET.

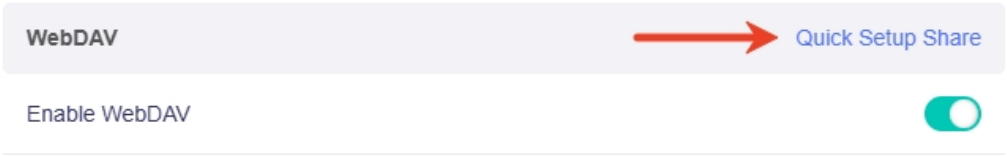
13.3.3 Configuration de WebDAV

1. Dans la section **Services de fichiers (File Services)**, activez **Activer WebDAV (Enable WebDAV)**, puis cliquez sur **Appliquer (Apply)**.

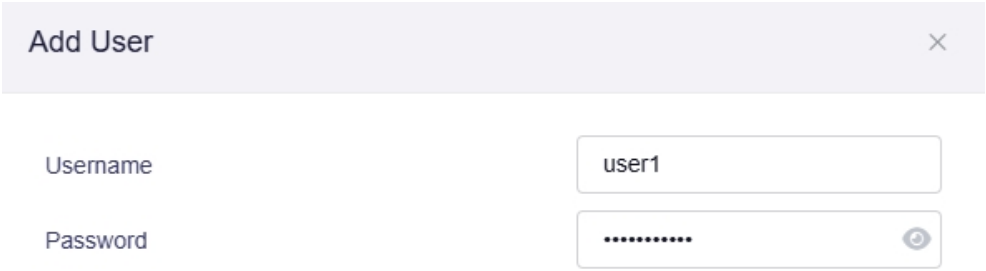


- **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** : activez cette option pour que les appareils en amont accèdent au service WebDAV.
- **Protocole WebDAV (WebDAV Protocol)** : HTTP n'est pas chiffré ; utilisez-le à vos risques. HTTPS est chiffré et utilise un certificat autosigné.
- **Port WebDAV (WebDAV Port)** : ne modifiez-le qu'en cas de conflit. La plage recommandée est de 1024 à 65535.

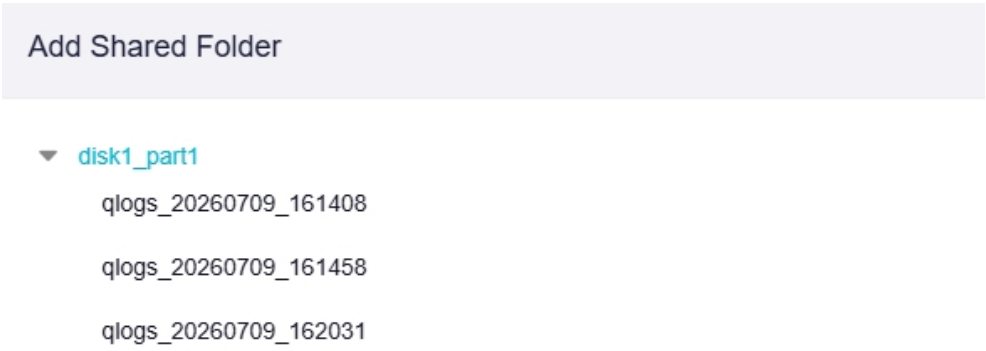
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



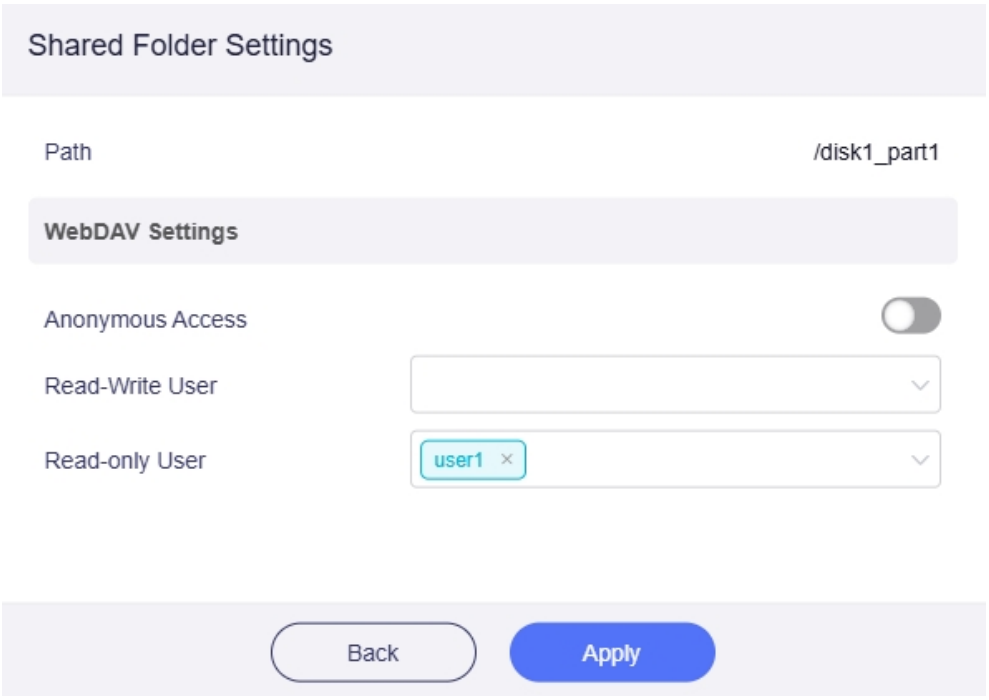
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



4. Cliquez sur le triangle pour afficher tous les dossiers. Sélectionnez le dossier à partager. Pour partager le disque entier, cliquez sur son nom, par exemple disk1_part1.



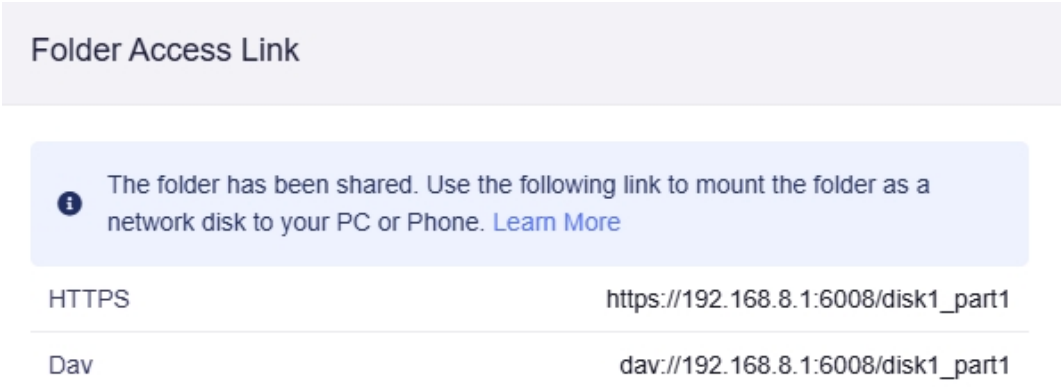
5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**.
   Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez sur **Appliquer (Apply)**.



Conseil : par sécurité, il est déconseillé d'activer l'accès anonyme (Anonymous Access).

6. Récupérez le lien d'accès au dossier.

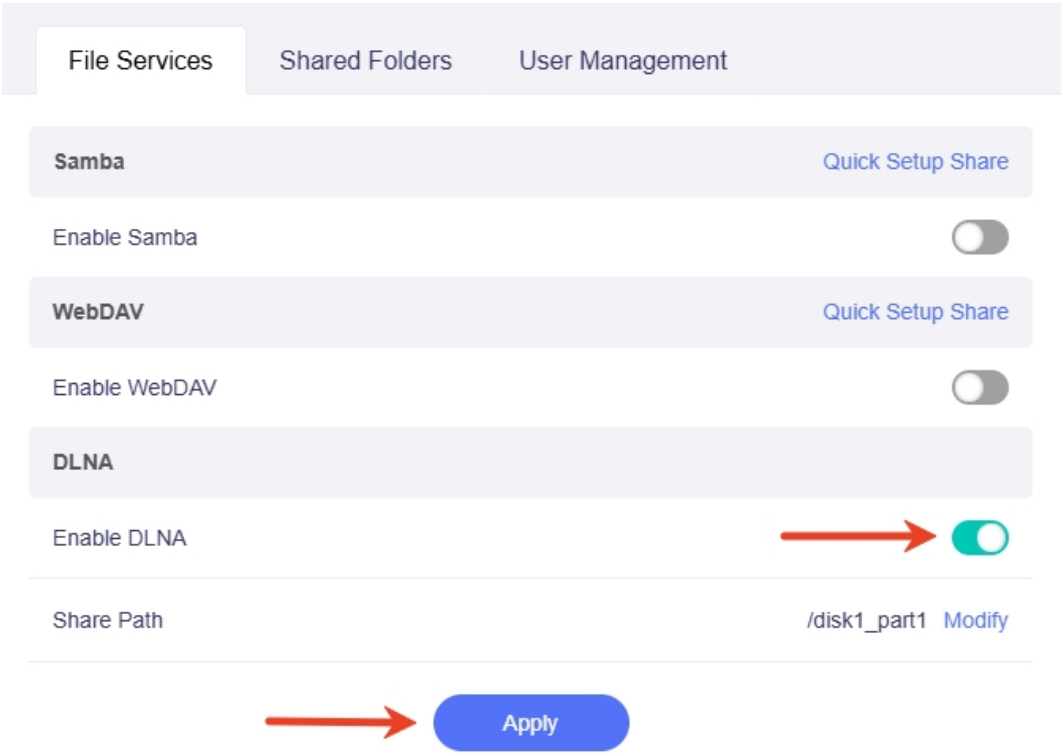
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via WebDAV.



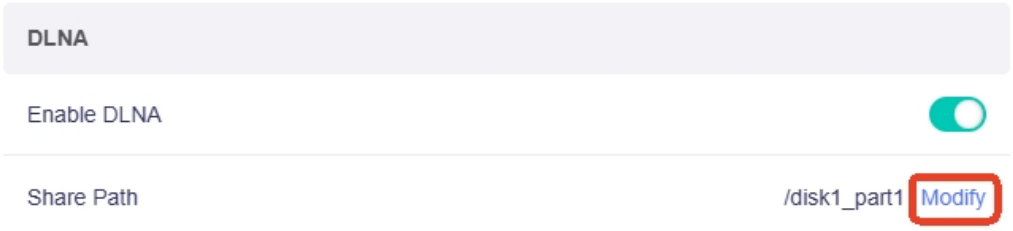
Remarque : si vous activez **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** et accédez au dossier depuis le réseau en amont, remplacez l'IP du routeur dans le lien, 192.168.8.1 par défaut, par son IP WAN affichée sur la page INTERNET.

13.3.4 Configuration de DLNA

1. Dans la section **Services de fichiers (File Services)**, activez **Activer DLNA (Enable DLNA)**, puis cliquez sur **Appliquer (Apply)**.



2. Modifiez le chemin de partage à droite si nécessaire.



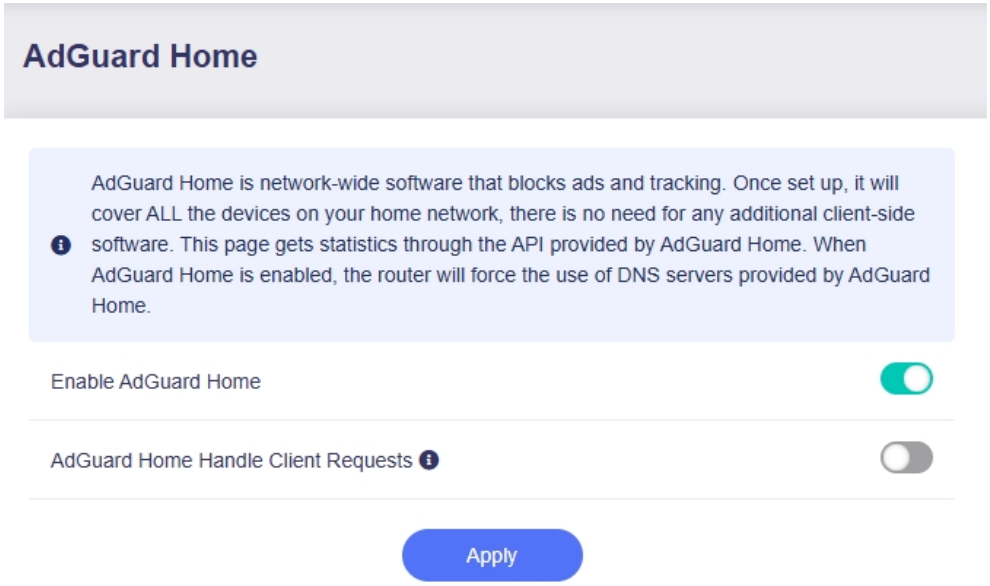
3. Connectez votre téléviseur intelligent au routeur. Il détecte automatiquement le serveur DLNA.

13.4 AdGuard Home

AdGuard Home bloque les publicités et le suivi sur l'ensemble du réseau. Une fois configuré, il couvre tous les clients sans installation de logiciel supplémentaire sur leurs appareils.

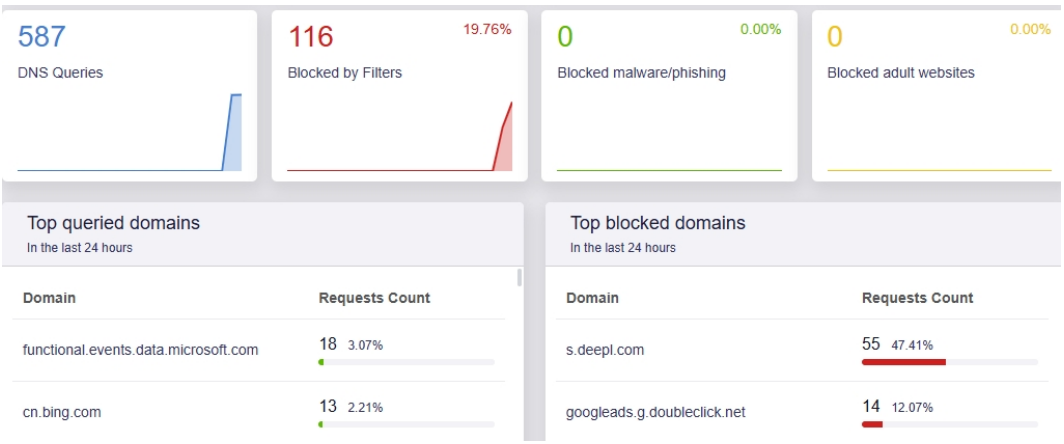
Suivez les étapes ci-dessous pour configurer AdGuard Home.

1. Dans l'interface Web, ouvrez **APPLICATIONS** > **AdGuard Home**. Activez **Activer AdGuard Home (Enable AdGuard Home)** et cliquez sur **Appliquer (Apply)**.

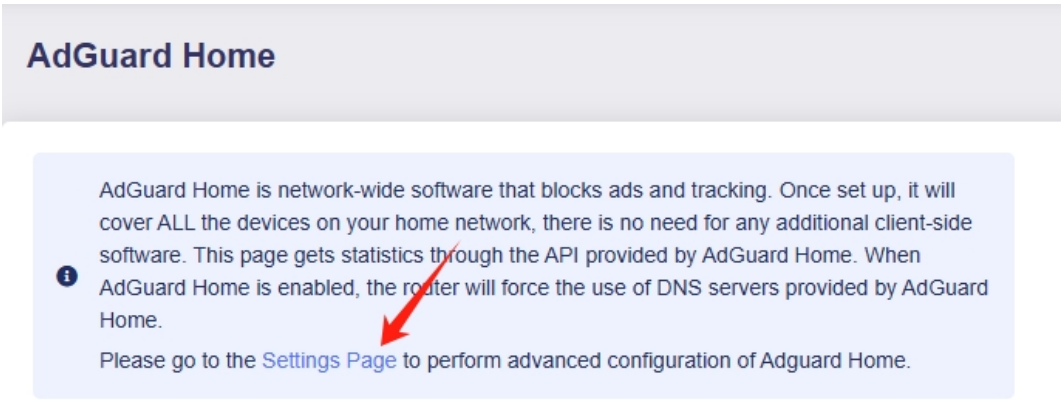


   - **AdGuard Home traite les requêtes clients (AdGuard Home Handles Client Requests)** : les requêtes DNS des clients sont alors traitées directement par AdGuard Home. Cela empêche toutefois les règles VPN fondées sur les domaines de fonctionner.

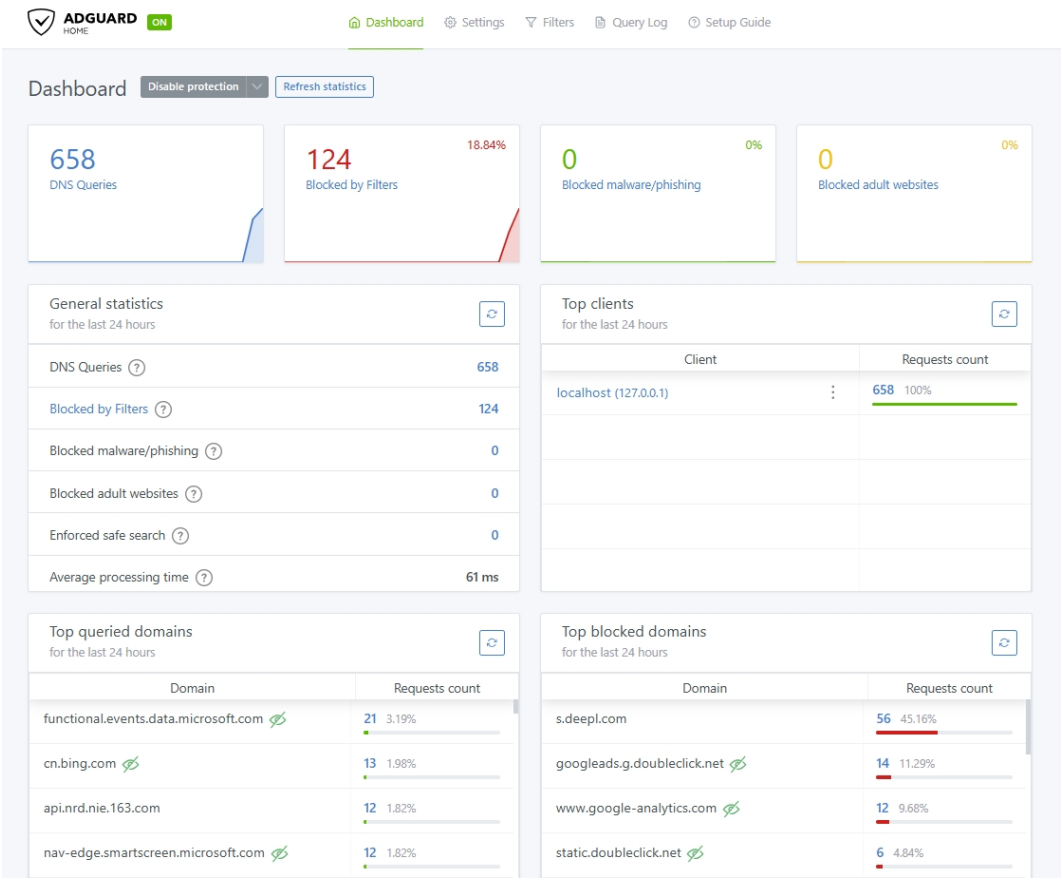
2. La page charge automatiquement les statistiques DNS, comme les requêtes et les domaines bloqués, via l'API d'AdGuard Home.



3. Cliquez sur **Page des paramètres (Settings Page)** pour configurer les paramètres avancés d'AdGuard Home.



4. La page des paramètres d'AdGuard Home s'ouvre. Consultez le centre d'assistance AdGuard Home pour obtenir de l'aide.


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

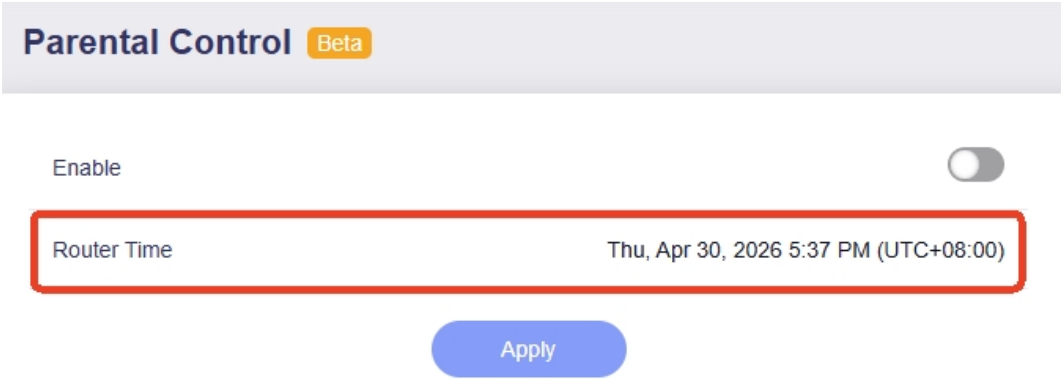
13.5 Contrôle parental

Le contrôle parental protège les enfants en bloquant les sites inadaptés et en limitant le temps d'utilisation des appareils. Il réduit l'accès aux contenus nuisibles, aide à gérer le temps d'écran et encourage un usage responsable d'Internet.

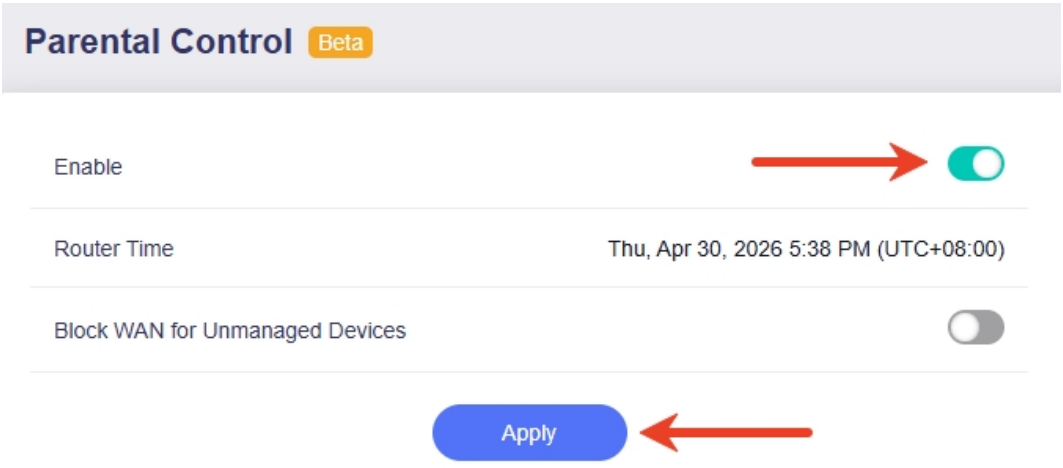
13.5.1 Configuration rapide

Suivez les étapes ci-dessous pour configurer le contrôle parental sur un routeur GL.iNet.

1. Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **Contrôle parental (Parental Control).** Vérifiez que l'heure du routeur est correcte. Sinon, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)** pour la synchroniser.



2. Activez le contrôle parental et cliquez sur **Appliquer (Apply)**. Suivez ensuite l'assistant. Vous pouvez également regarder la vidéo de configuration ici.



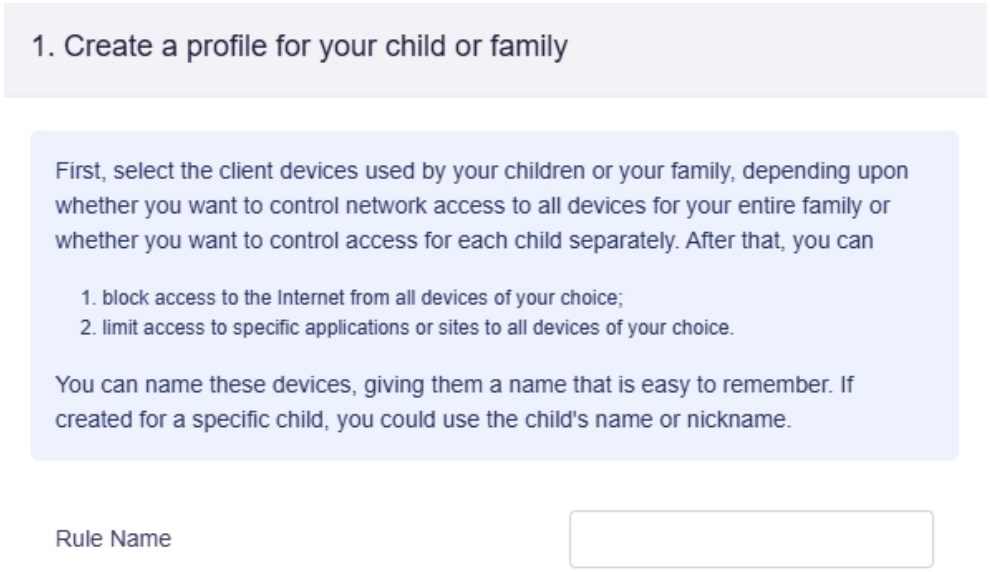
- **Bloquer le WAN pour les appareils non gérés (Block WAN for Unmanaged Devices)** : bloque l'accès Internet des appareils absents de la liste du contrôle parental.

Voici un exemple d’utilisation.

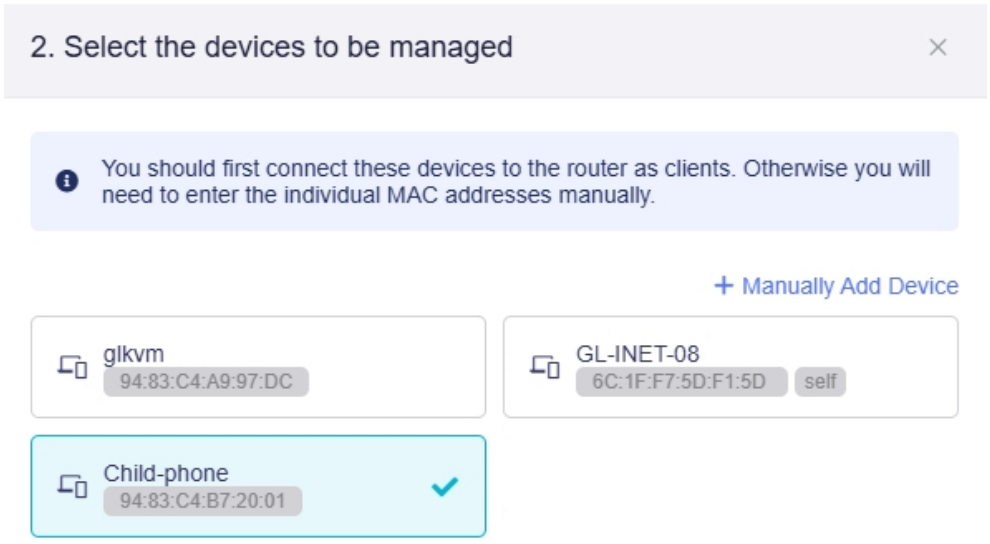
Scénario : les appareils de ce profil peuvent accéder à Internet uniquement pour étudier de 8 h à 11 h en semaine, et pour jouer de 18 h à 20 h le week-end. L’accès Internet est bloqué par défaut en dehors de ces plages.

Étapes de configuration :

1. Créez un profil et donnez-lui un nom.

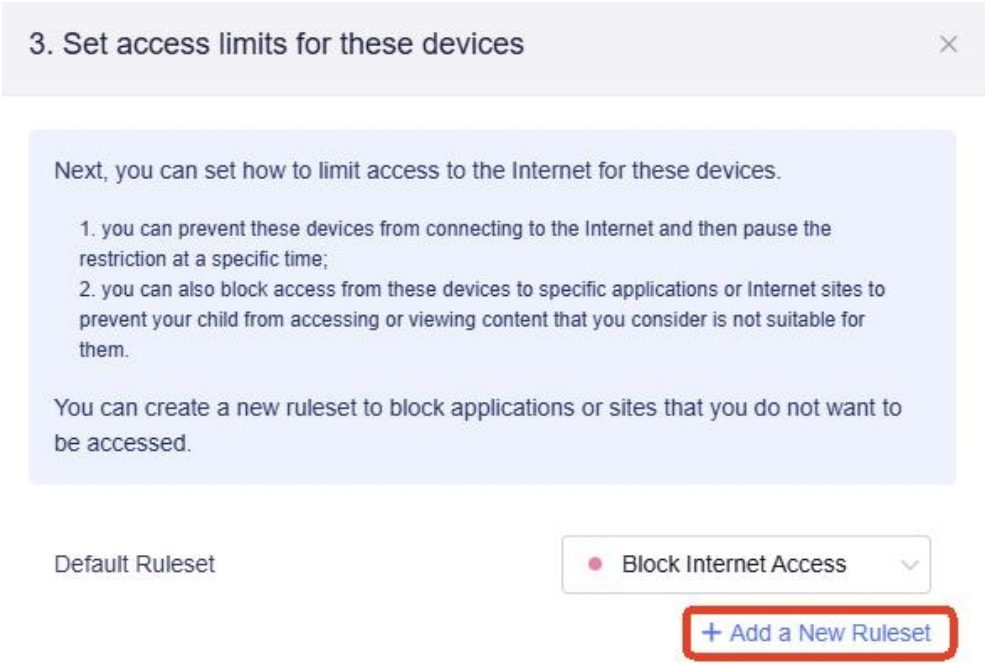


2. Sélectionnez les appareils à gérer. Connectez-les d’abord au routeur. S’ils n’y ont jamais été connectés, ajoutez-les manuellement avec leur adresse MAC.

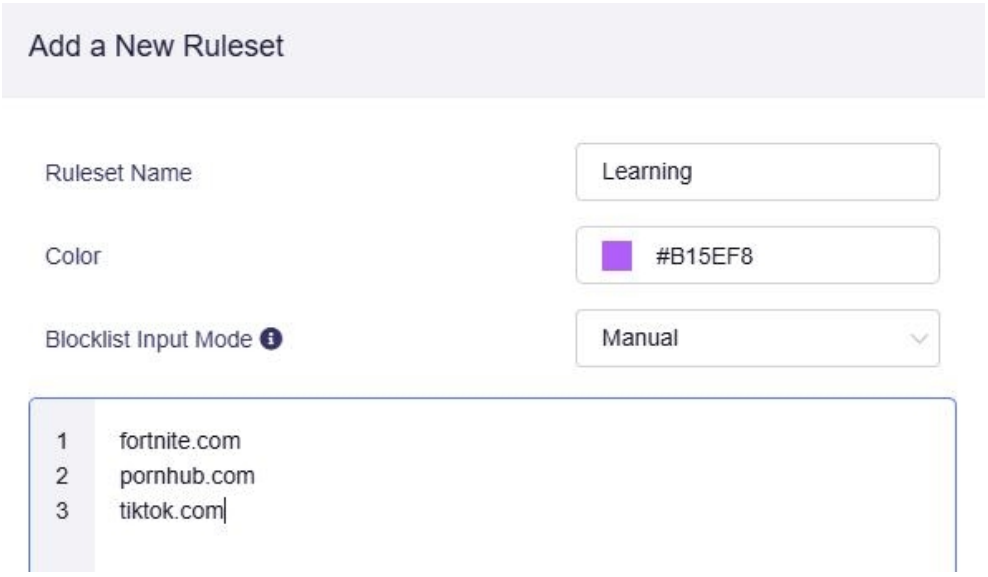


3. Définissez les limites d’accès.

Deux jeux de règles sont prédéfinis : **Bloquer l’accès Internet (Block Internet Access)** et **Sans limite (No Limit)**.
Cliquez sur **Ajouter un jeu de règles (Add a New Ruleset)** pour créer deux jeux supplémentaires : **Étude (Learning)** et **Jeu (Play)**.

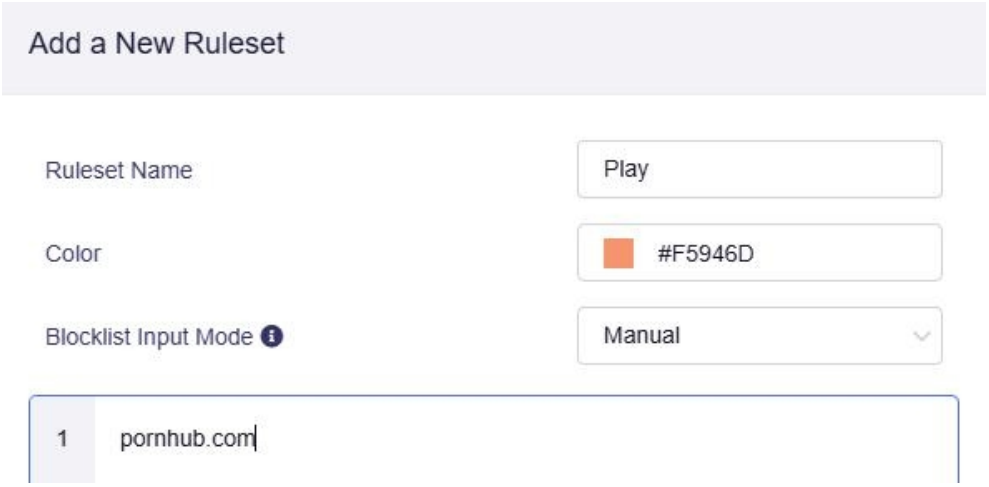


Définissez le nom, par exemple Étude, et la couleur du jeu de règles. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.

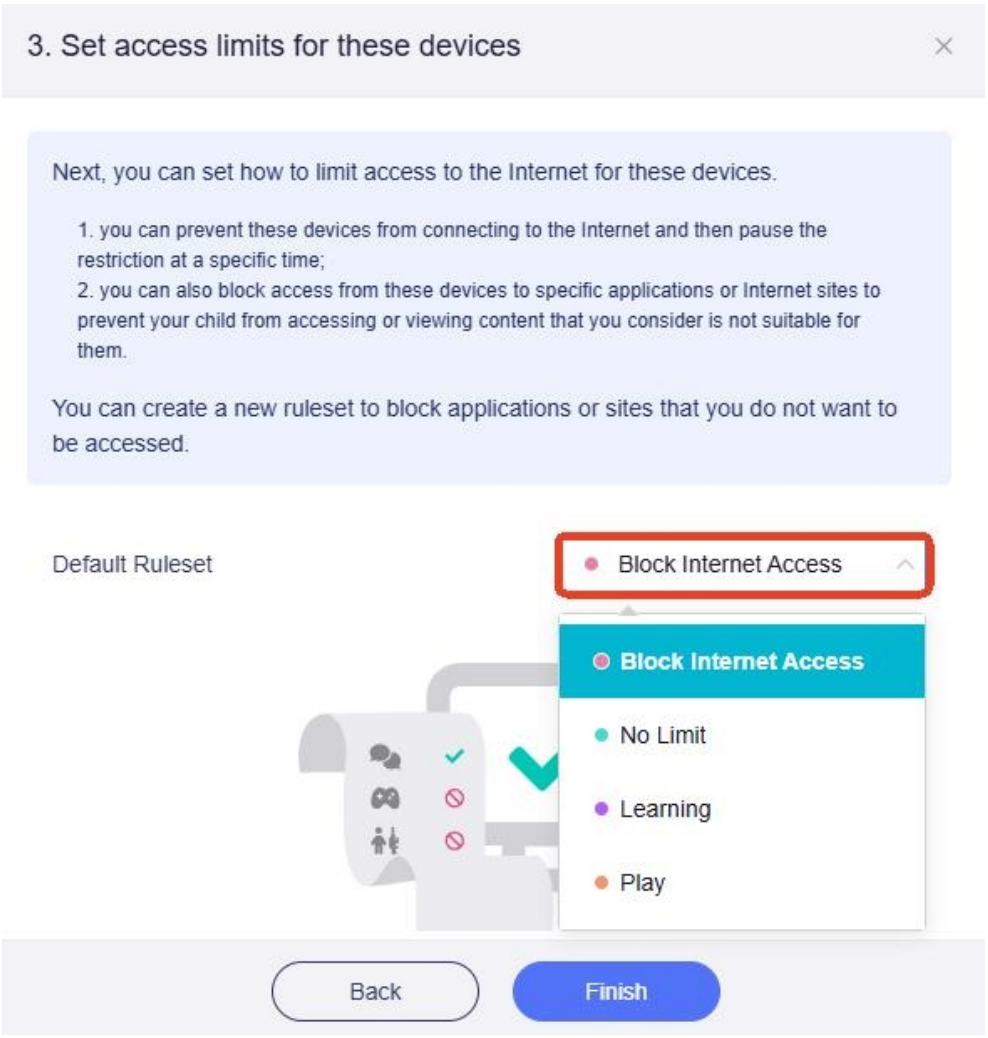


Remarque : les domaines de la liste de blocage englobent leurs sous-domaines. Par exemple, « example.com » inclut aussi « subdomain.example.com ».

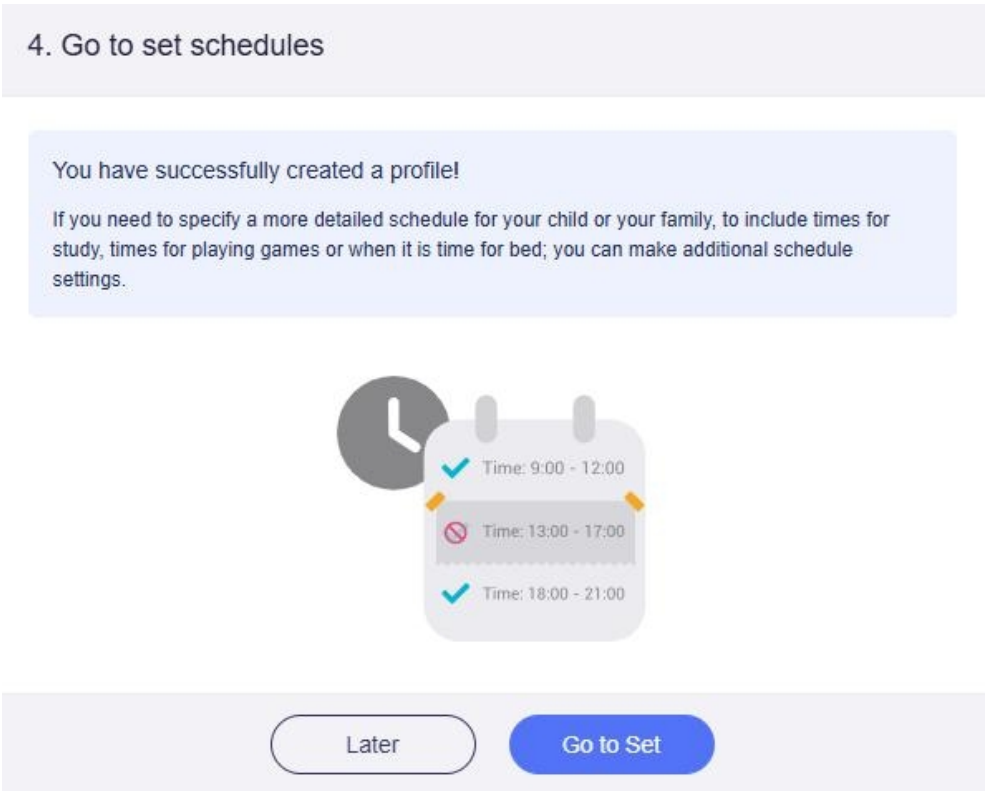
Créez de la même façon un autre jeu de règles. Définissez son nom, par exemple Jeu, et sa couleur. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.



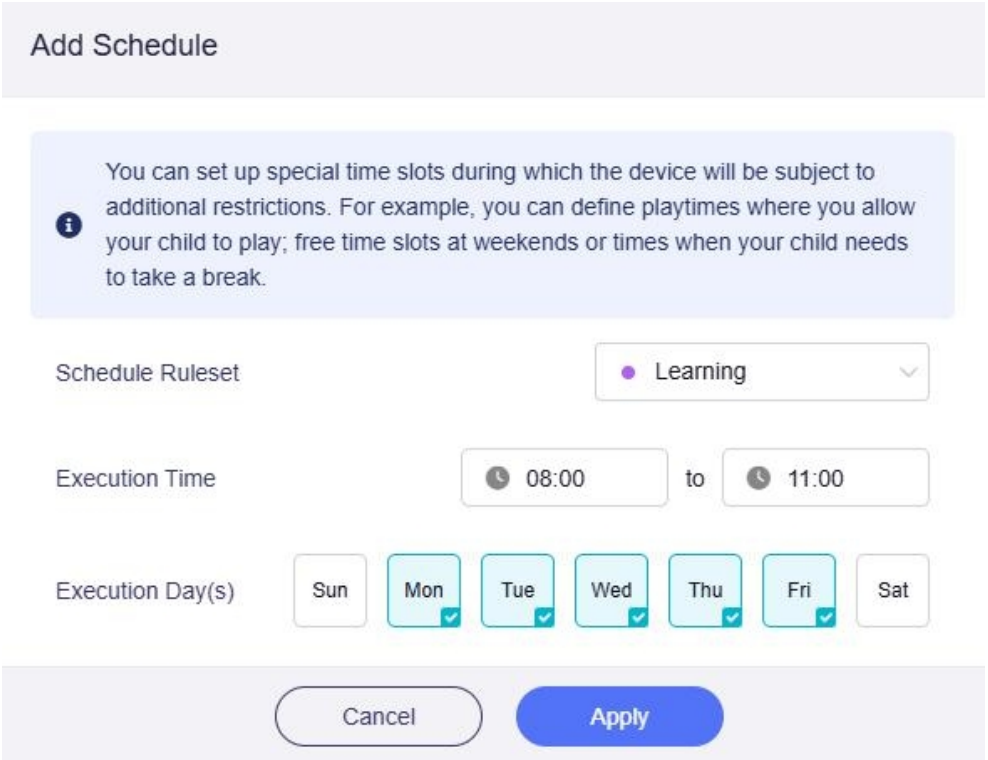
Vous disposez alors de quatre jeux de règles. Sélectionnez **Bloquer l’accès Internet (Block Internet Access)** comme **Jeu de règles par défaut (Default Ruleset)**, puis cliquez sur **Terminer (Finish)**.



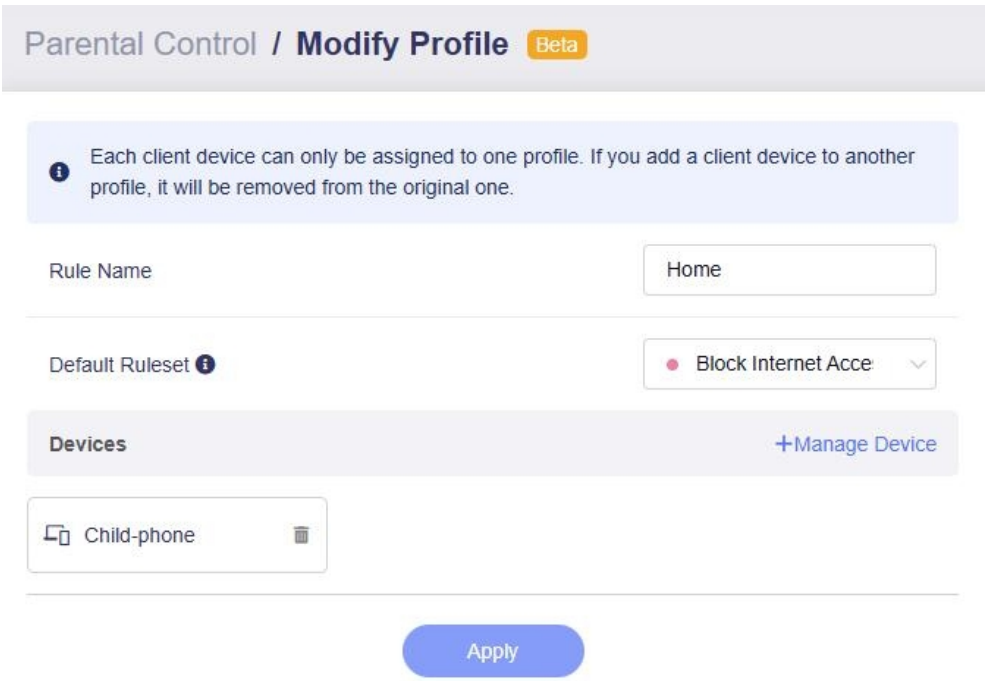
4. Définissez ensuite le planning du profil. Cliquez sur **Configurer (Go to Set)**.



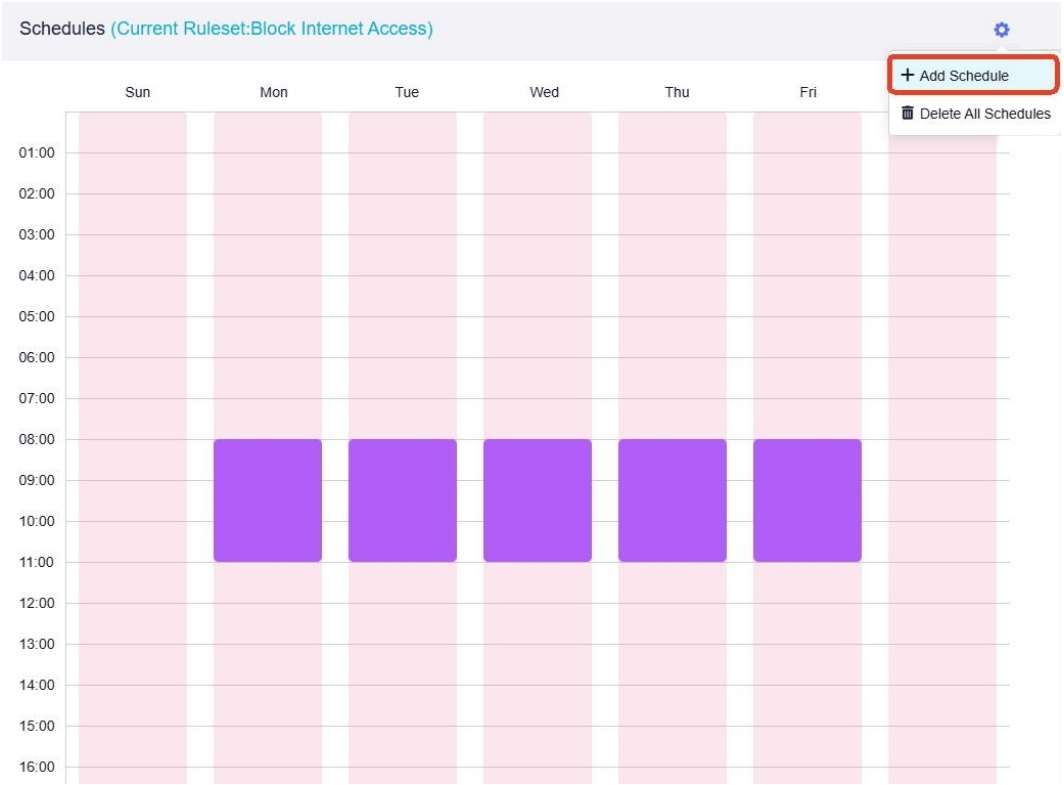
Ajoutez le jeu de règles **Étude (Learning)** au planning. Définissez l'**horaire d'exécution (Execution Time)** de 8 h à 11 h en semaine, puis cliquez sur **Appliquer (Apply)**.



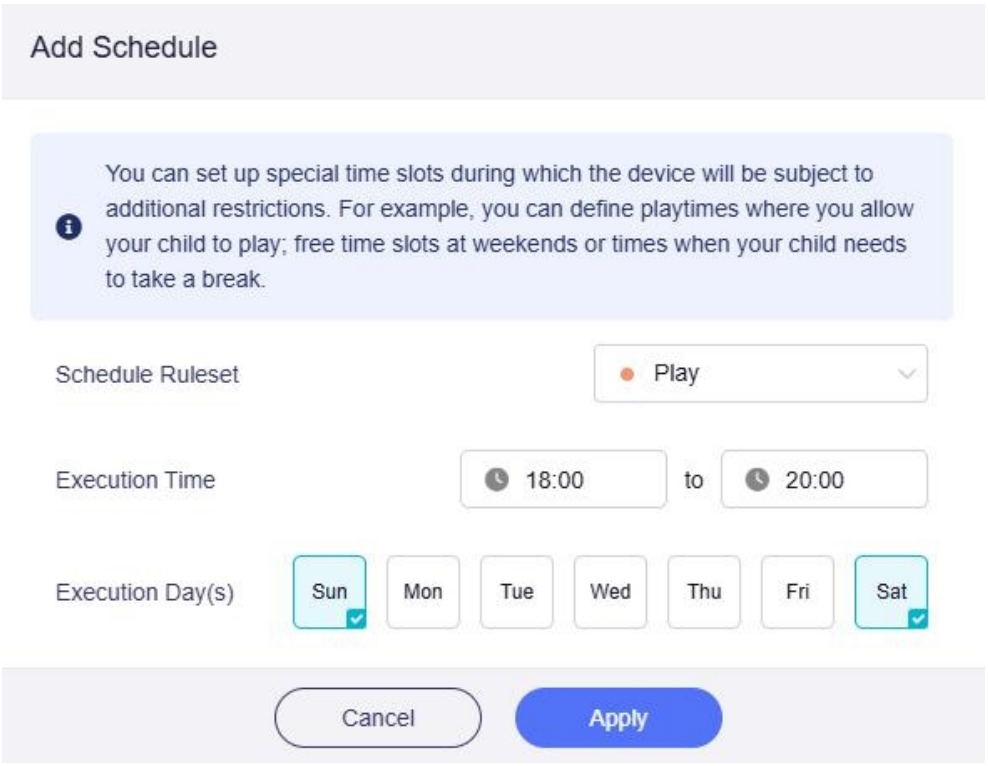
5. La page de modification du profil créé s'ouvre.



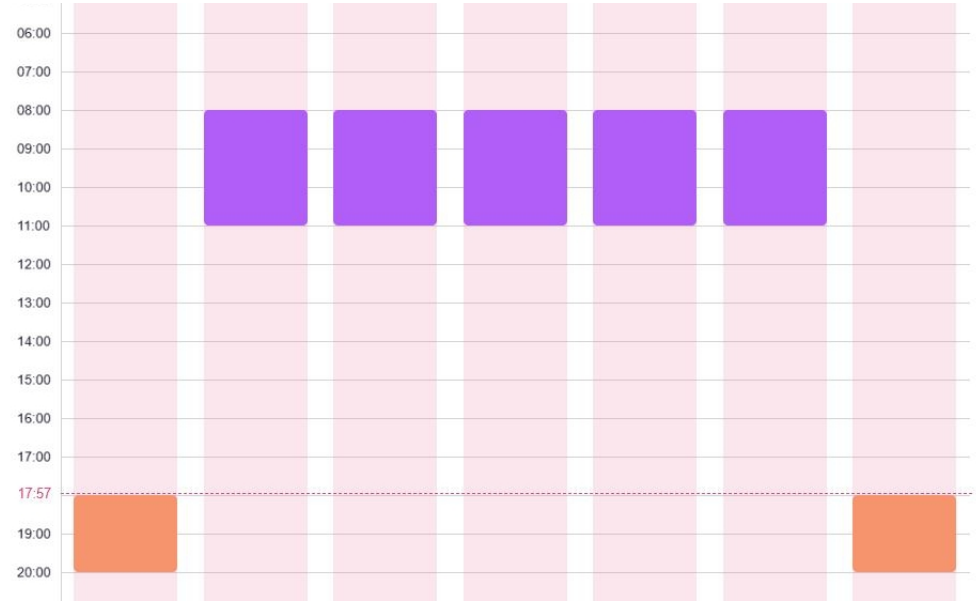
En bas de la page, le planning créé apparaît. Cliquez sur l'engrenage en haut à droite, puis sur **Ajouter une plage horaire (Add Schedule)**.



6. Ajoutez le jeu de règles **Jeu (Play)** au planning. Définissez l'**horaire d'exécution (Execution Time)** de 18 h à 20 h le week-end, puis cliquez sur **Appliquer (Apply)**.



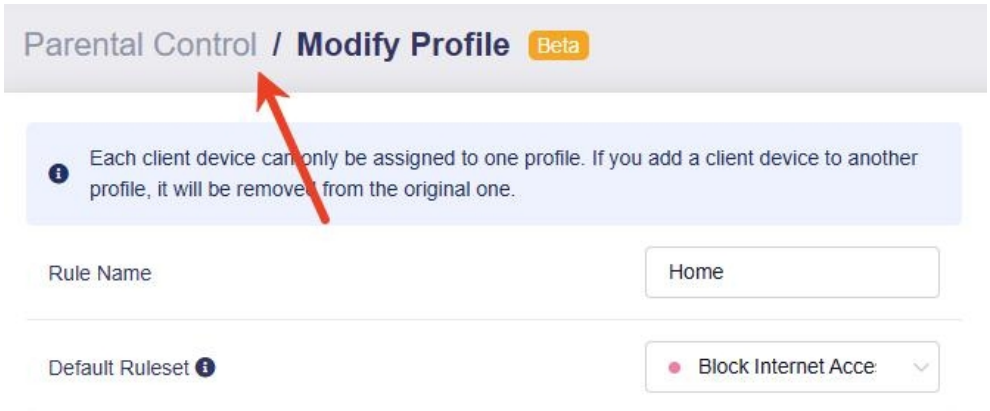
Le jeu de règles Jeu est ajouté au planning.



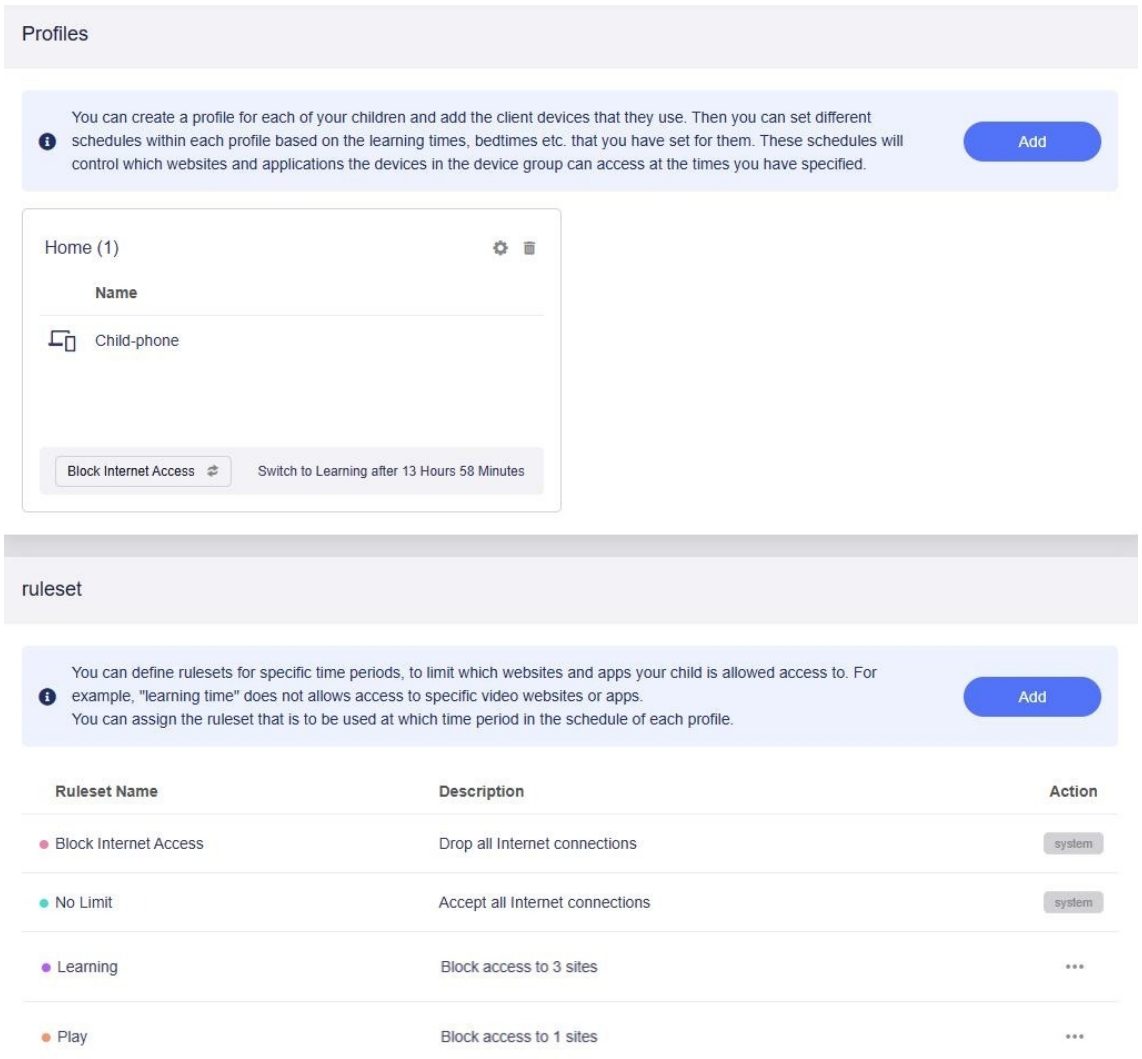
Conseils :

- La ligne rouge en pointillés indique l'heure actuelle.
- Cliquez sur un jeu de règles du planning pour modifier son horaire.

7. Cliquez sur **Contrôle parental (Parental Control)** en haut de la page pour revenir à la page principale.



La configuration finale s’affiche. Le contrôle parental s’applique désormais selon le planning. Vous pouvez modifier les profils et les jeux de règles existants ou en ajouter.



13.5.2 Dépannage

Si les réglages ne prennent pas effet, vérifiez les causes possibles suivantes.

1. Problème de cache DNS.

   Les navigateurs et les systèmes d'exploitation conservent un cache DNS qui peut retarder l'application des changements. Videz-le pour appliquer les modifications immédiatement.
2. La plage horaire du profil n'a pas encore commencé.
3. Le domaine saisi peut être incorrect.

   Le domaine public d'un site est facile à trouver, mais les domaines d'API utilisés par les applications sont rarement publiés. Pour les identifier, utilisez un outil de capture de paquets comme Wireshark ou recherchez les informations correspondantes.

   Par exemple, pour bloquer « www.google.com », saisir « google.com » donne de meilleurs résultats que « www.google.com ».
4. L'appareil cible utilise une nouvelle adresse MAC aléatoire à chaque connexion, ce qui empêche les règles de s'appliquer. Désactivez cette fonction sur l'appareil, puis ajoutez-le de nouveau au profil.

13.6 ZeroTier

ZeroTier est un VPN logiciel qui permet des communications chiffrées et sécurisées entre appareils via Internet. Il crée un réseau privé virtuel dans lequel les appareils communiquent comme sur un même réseau local, indépendamment de leur emplacement ou de la topologie réseau. Simple à configurer et à utiliser, il propose le chiffrement de bout en bout, la segmentation réseau et des fonctions de pont réseau.

La fonction ZeroTier des routeurs GL.iNet permet de rejoindre un réseau virtuel ZeroTier pour accéder à distance au routeur et aux ressources situées côté WAN et LAN.

Remarque :

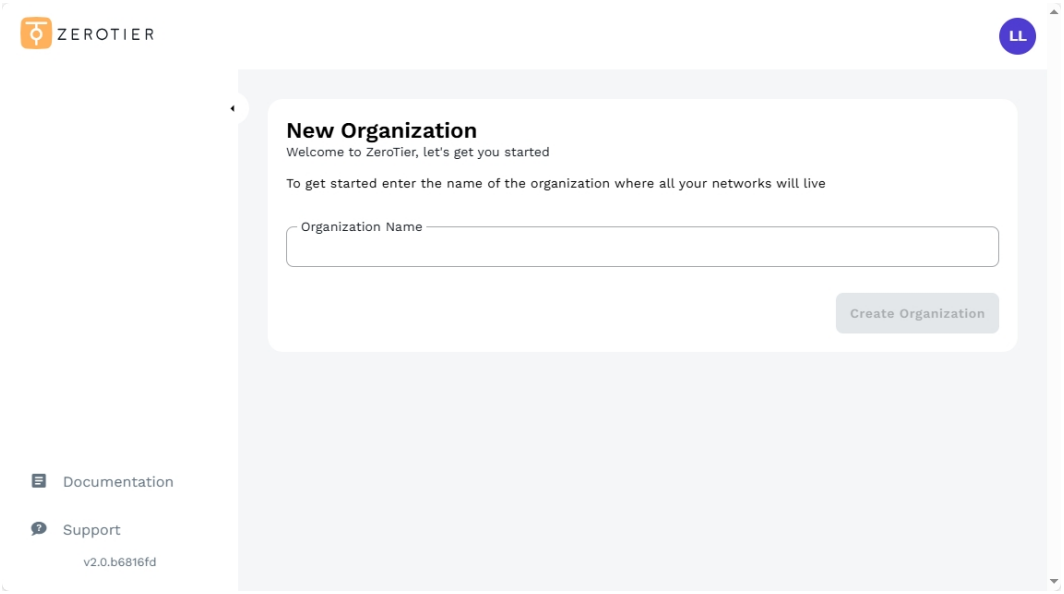
1. Il est déconseillé d'utiliser ZeroTier simultanément avec le client OpenVPN, le client WireGuard, GoodCloud Site to Site, Tailscale ou AstroWarp, car cela peut provoquer des conflits de routage.
2. Cette fonction est actuellement en version bêta et peut présenter des anomalies.

13.6.1 Configuration de ZeroTier

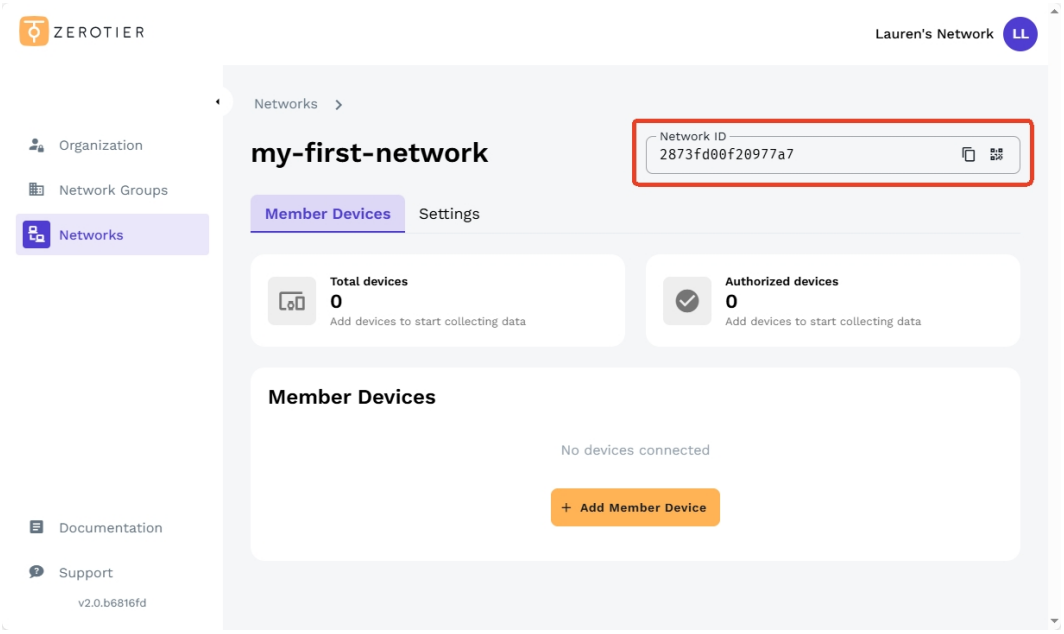
ZeroTier Central existe en deux versions : New Central et Legacy Central.

Les étapes suivantes utilisent New Central.

1. Ouvrez le site officiel ZeroTier et connectez-vous à votre compte.
2. Créez une organisation.

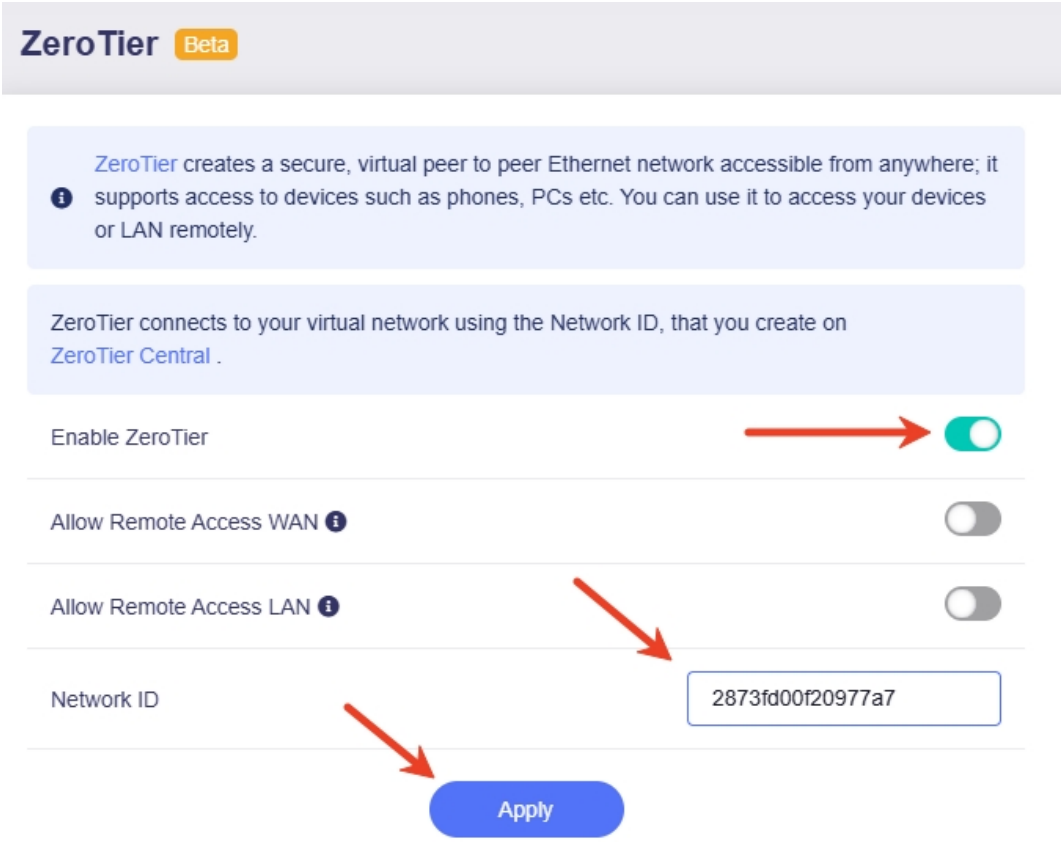


3. Choisissez une offre. L'exemple utilise l'**offre Personal**, qui comprend 10 appareils, un administrateur et un réseau. Pour ajouter des réseaux, des appareils, des routes personnalisées ou un DNS, choisissez une autre offre payante.
4. Votre réseau ZeroTier est créé.

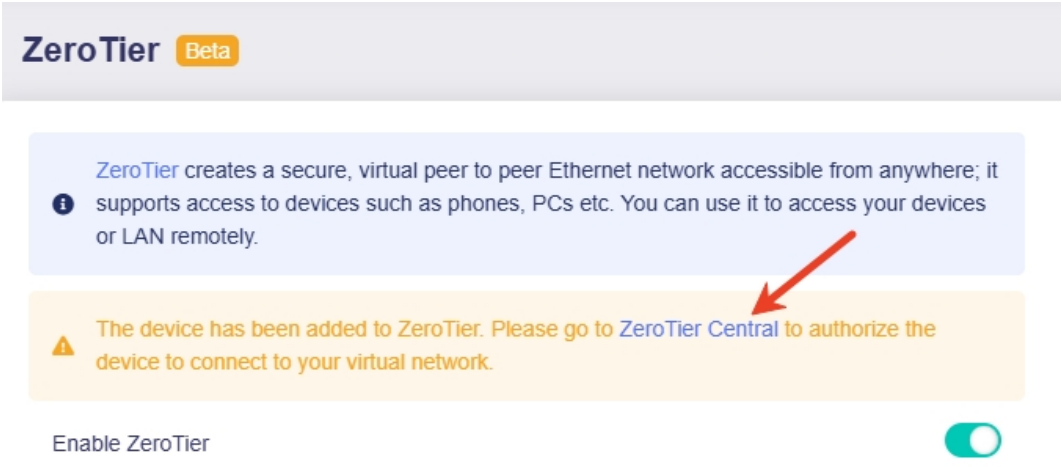


Notez l'**identifiant du réseau (Network ID)**, une suite alphanumérique de 16 caractères affichée en haut à droite. Il sera nécessaire pour connecter les autres appareils.

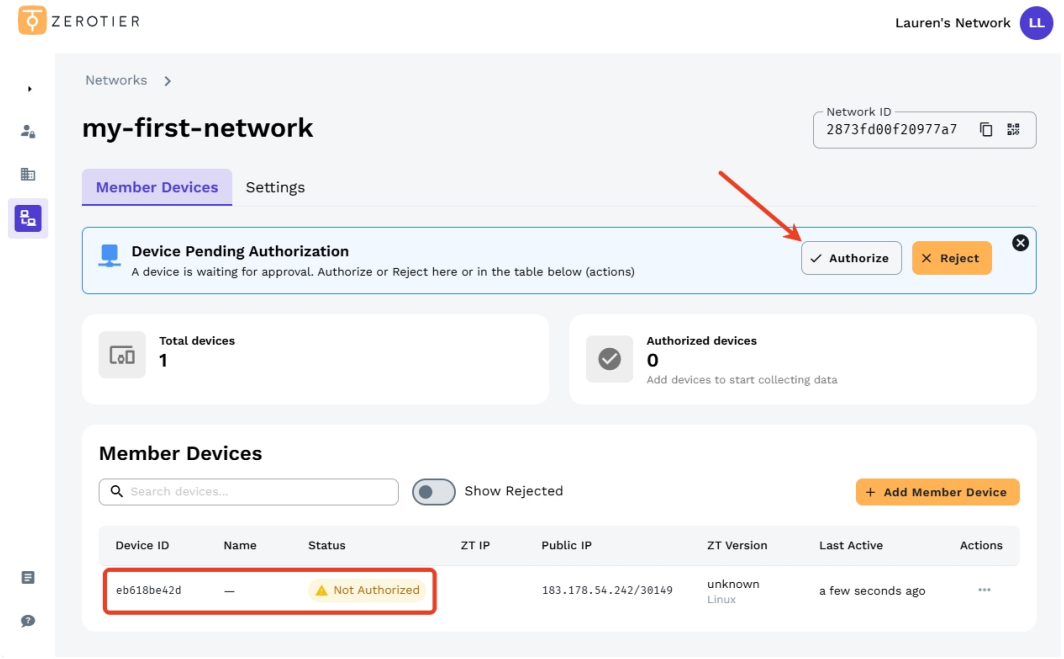
5. Dans l'interface Web du routeur, ouvrez **APPLICATIONS** > **ZeroTier**. Activez ZeroTier, saisissez l'**identifiant du réseau (Network ID)**, puis cliquez sur **Appliquer (Apply)**.



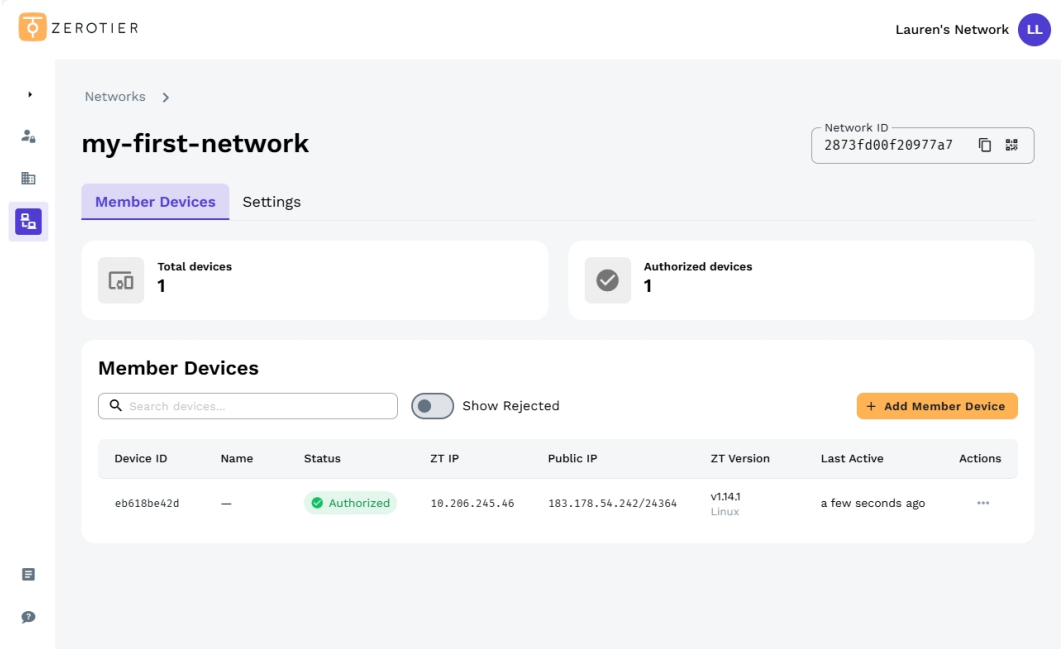
Après un court instant, la page indique qu'une autorisation est nécessaire. Cliquez sur le lien **ZeroTier Central** pour ouvrir la plateforme.



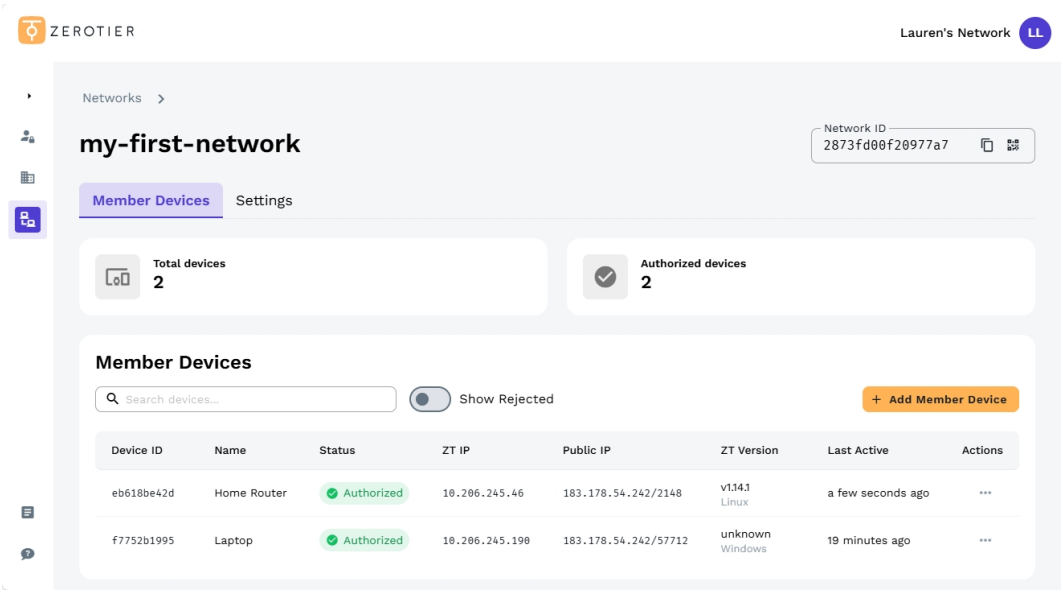
6. Dans ZeroTier Central, repérez l'appareil en attente et autorisez-le.



Une fois autorisé, il apparaît comme ci-dessous.

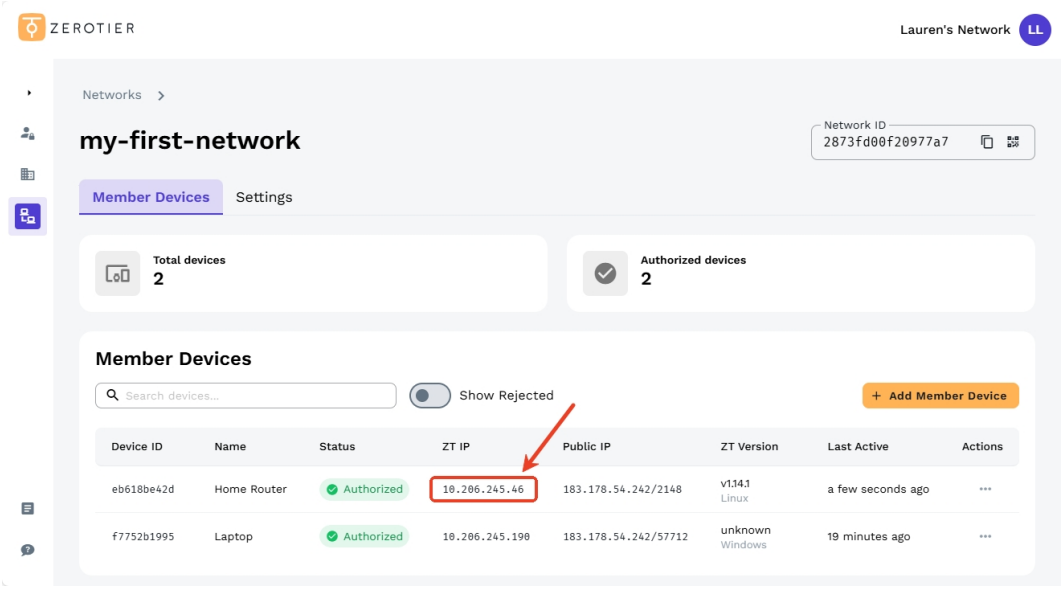


7. Ajoutez un autre appareil, comme un ordinateur ou un smartphone, au même réseau en suivant ce guide. Une fois l'ajout réussi, la page affiche les informations des membres : **identifiant de l'appareil (Device ID)**, **nom (Name)**, **état (Status)**, **IP gérée (Managed IP)** et **IP publique (Public IP)**.



Conseil : cliquez sur les trois points à droite pour modifier le nom, les adresses IP gérées et les paramètres avancés d'un appareil membre.

8. Cliquez sur l'**IP gérée (Managed IP)** du routeur pour la copier.



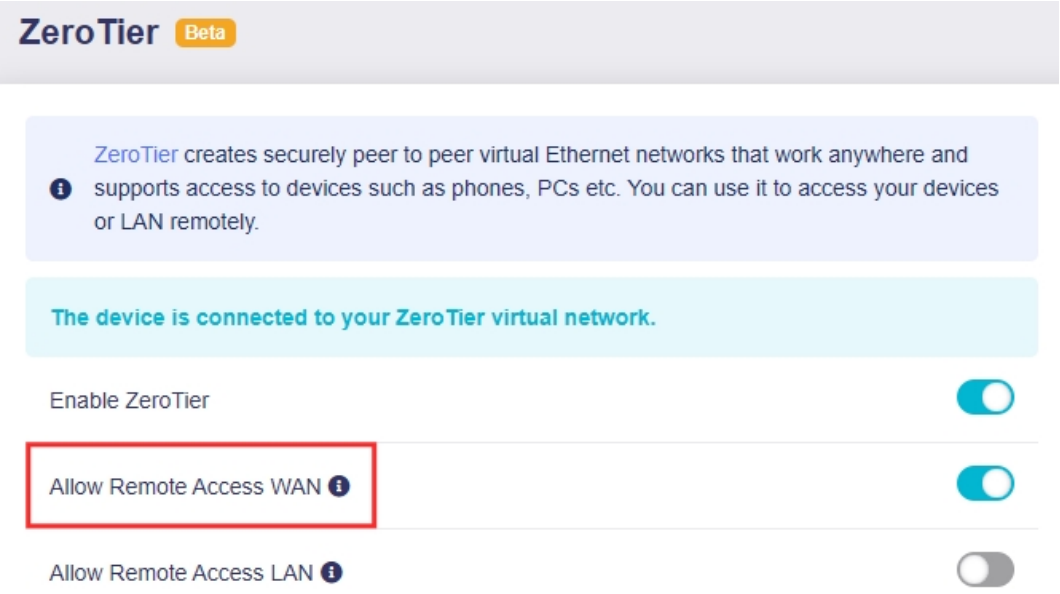
Utilisez ensuite cette IP pour accéder au routeur depuis votre ordinateur portable connecté au même réseau ZeroTier.

9. Testez la connexion.

   Sur cet ordinateur, ouvrez un navigateur et saisissez l'IP gérée copiée à l'étape précédente. Si l'interface Web du routeur s'ouvre, la connexion ZeroTier fonctionne.

13.6.2 Autoriser l’accès distant au WAN

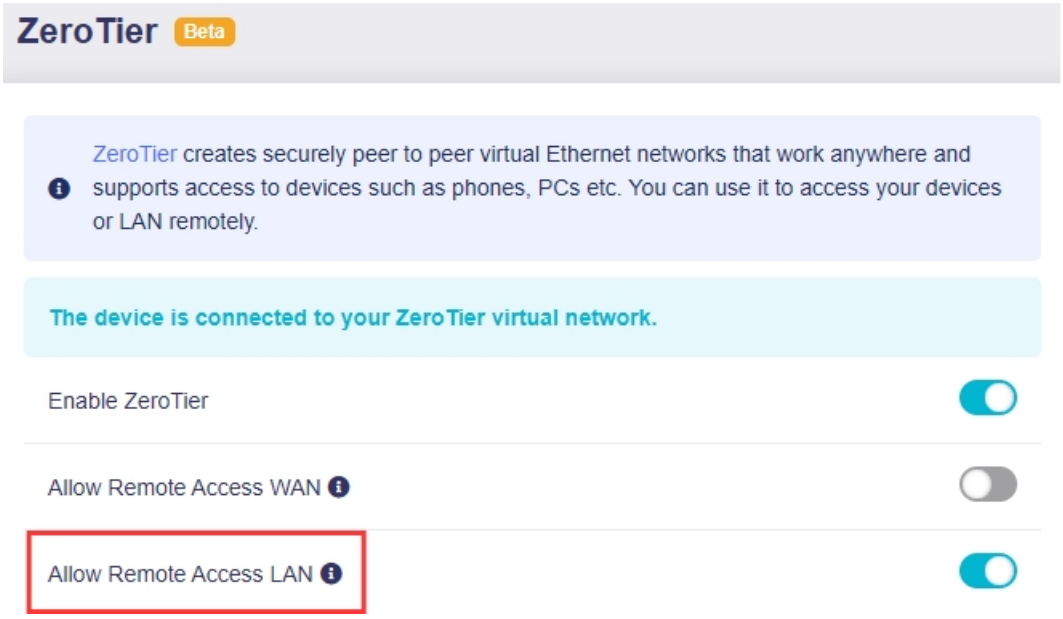
Si cette option est activée, les ressources côté WAN de l’appareil sont accessibles par le réseau virtuel ZeroTier. Consultez cette page pour en savoir plus.



Remarque : cette fonction nécessite l’ajout de règles de routage au réseau ZeroTier pour fonctionner. Legacy Central permet d’ajouter gratuitement une route personnalisée ; dans New Central, un abonnement Essential ou supérieur est nécessaire pour configurer des routes personnalisées. Tarifs ZeroTier

13.6.3 Autoriser l’accès distant au LAN

Si cette option est activée, les ressources côté LAN de l’appareil sont accessibles par le réseau virtuel ZeroTier. Consultez cette page pour en savoir plus.



Remarque : cette fonction nécessite l’ajout de règles de routage au réseau ZeroTier pour fonctionner. Legacy Central permet d’ajouter gratuitement une route personnalisée ; dans New Central, un abonnement Essential ou supérieur est nécessaire pour configurer des routes personnalisées. Tarifs ZeroTier

13.7 Tailscale

Tailscale est un service VPN qui permet d'accéder à vos appareils et applications personnels depuis le monde entier, simplement et en toute sécurité.

La fonction Tailscale des routeurs GL.iNet permet de rejoindre un réseau virtuel Tailscale pour accéder à distance au routeur et aux ressources situées côté WAN et LAN.

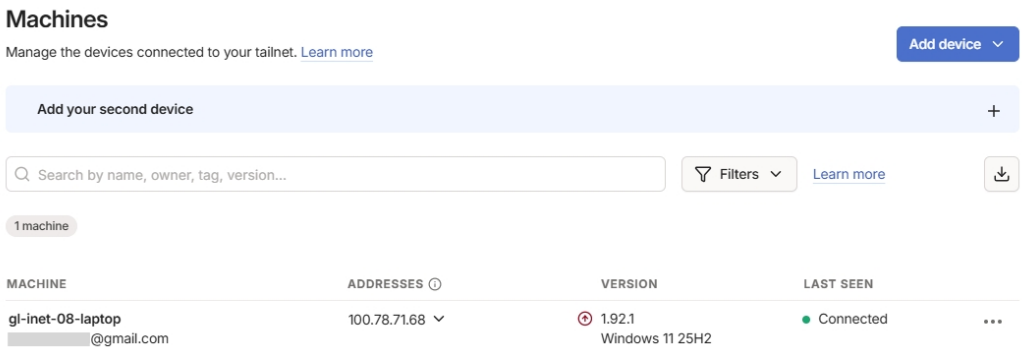
Remarque :

1. Tailscale étant fondé sur WireGuard, il est déconseillé de l'utiliser simultanément avec le client OpenVPN, le client WireGuard, GoodCloud Site to Site, ZeroTier ou AstroWarp, car cela peut provoquer des conflits de routage.
2. Cette fonction est actuellement en version bêta et peut présenter des anomalies.
3. Les routeurs GL.iNet ne peuvent pas encore servir de nœuds de sortie. Cette fonction sera disponible à partir du micrologiciel v4.9.

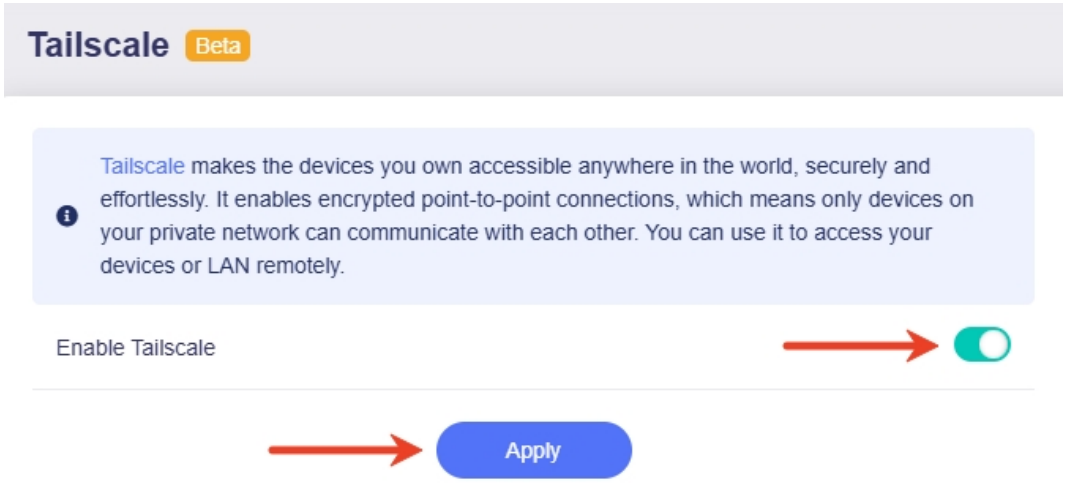
13.7.1 Configuration de Tailscale

L’exemple suivant utilise Beryl AX (GL-MT3000) et un ordinateur portable.

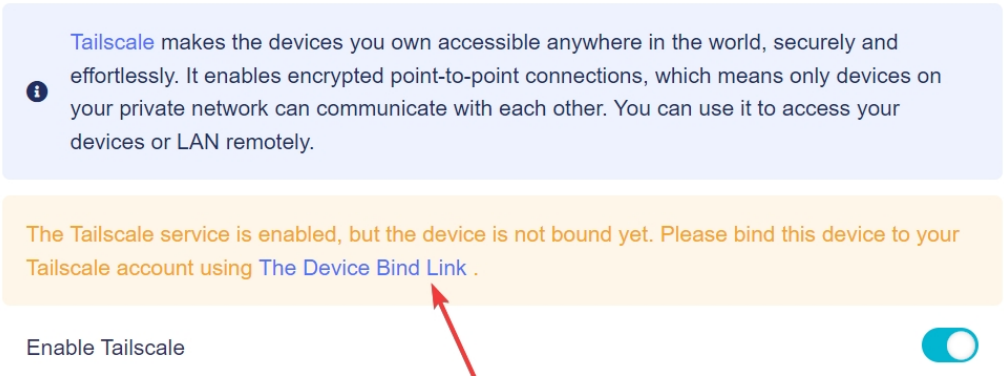
1. Créez d’abord un compte Tailscale et associez-y un ou deux appareils pour effectuer des tests. Ils apparaissent ensuite dans la console Tailscale.



2. Dans l’interface Web du routeur, ouvrez **APPLICATIONS** > **Tailscale**. Activez **Activer Tailscale (Enable Tailscale)**, puis cliquez sur **Appliquer (Apply)**.



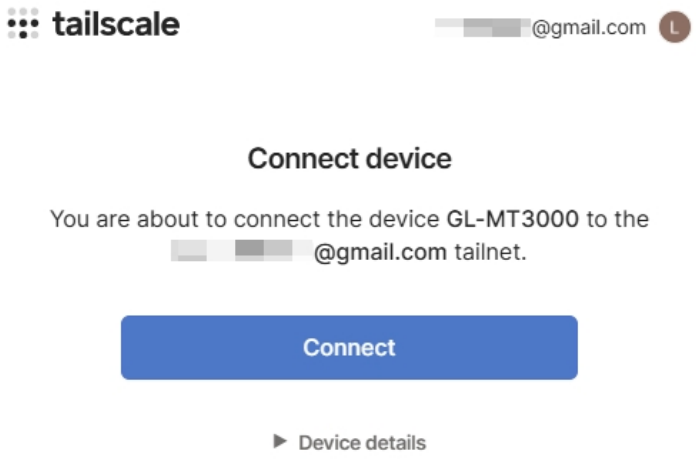
3. La page vous invite à associer l’appareil. Cliquez sur **Lien d’association de l’appareil (Device Bind Link)**.



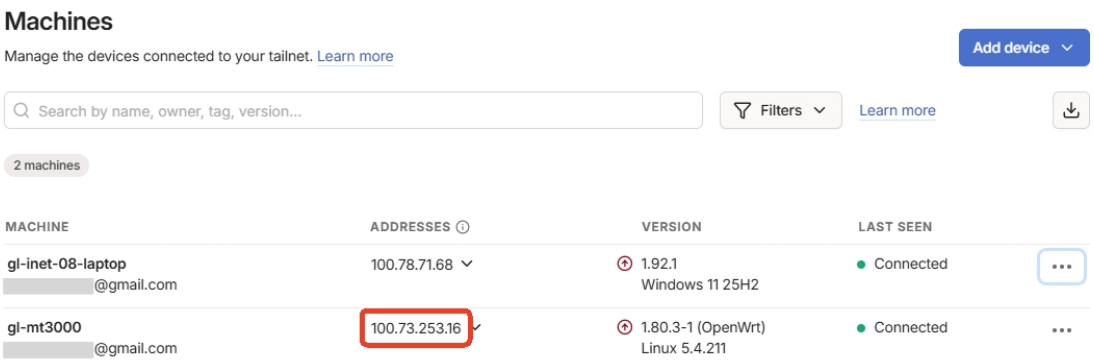
4. Dans la fenêtre qui s'affiche, cliquez sur le lien et connectez-vous à votre compte Tailscale.



5. Confirmez ensuite l'appareil en cliquant sur **Connecter (Connect)**.

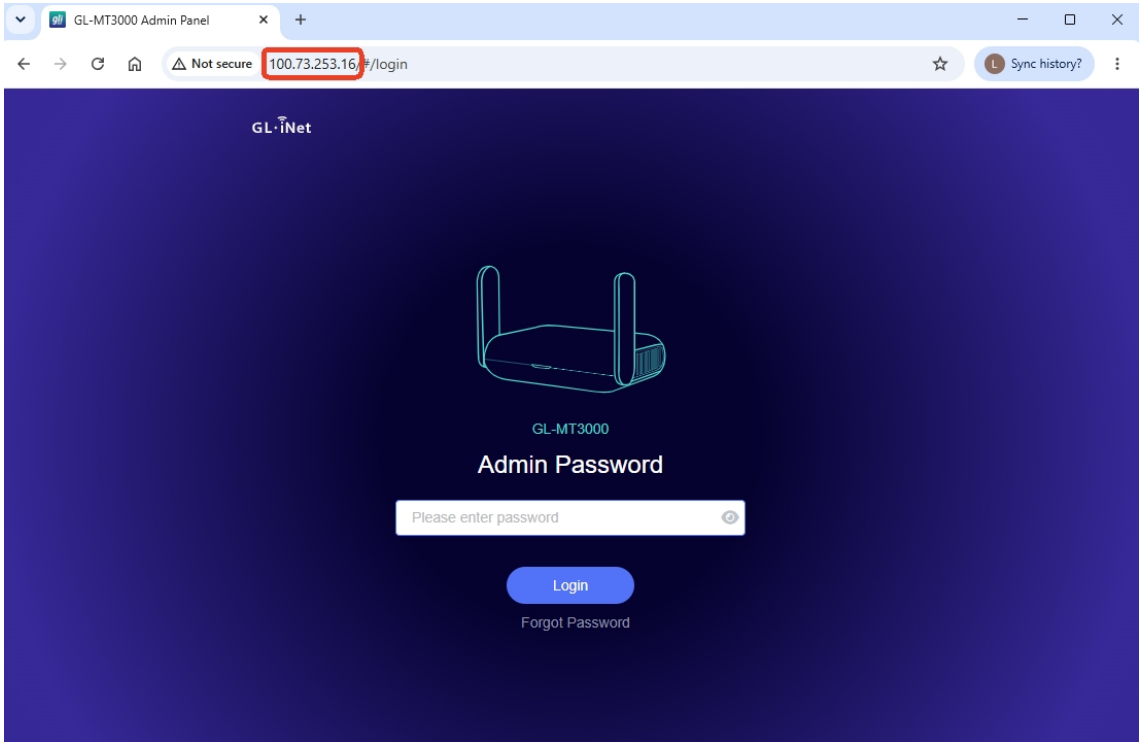


6. Vous êtes ensuite redirigé vers la console d'administration Tailscale. Le routeur fait désormais partie du réseau virtuel Tailscale et peut être accessible à distance via son adresse IP virtuelle Tailscale **100.73.253.16**.



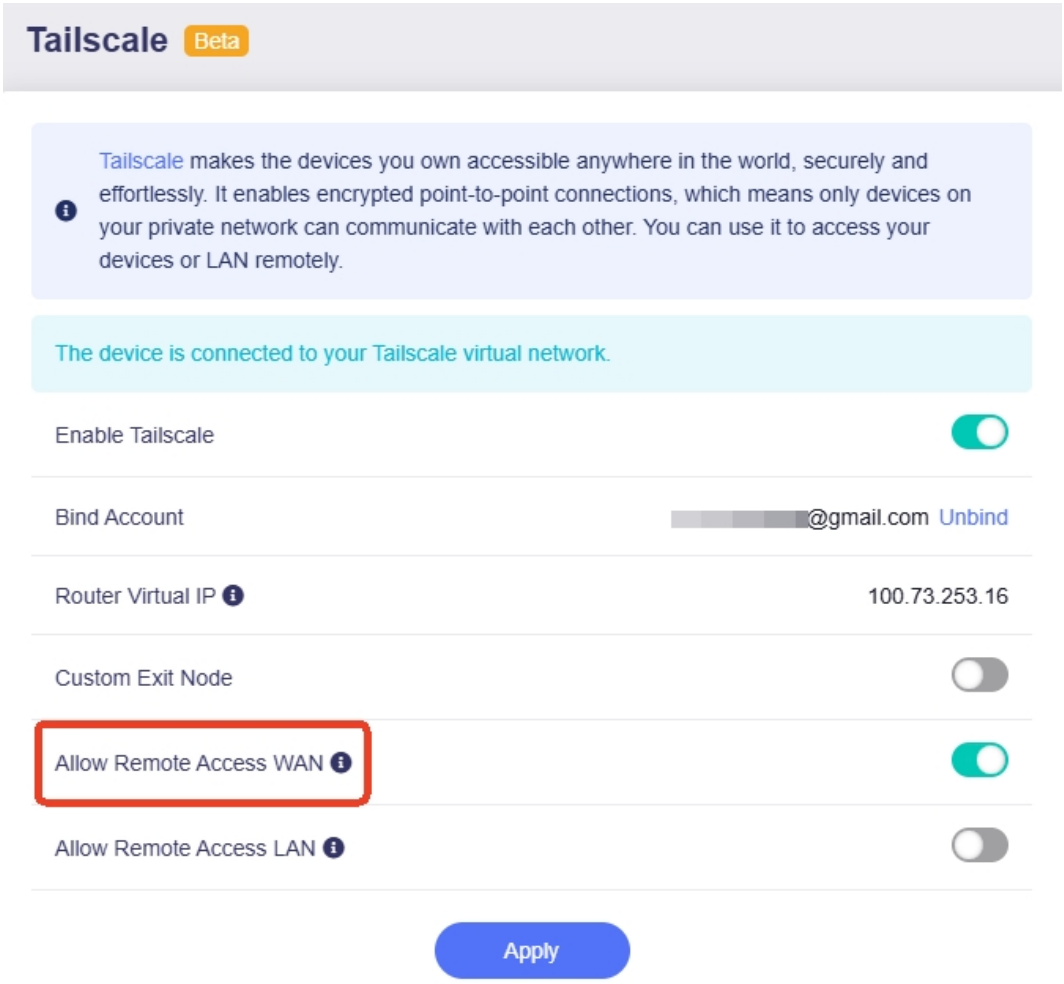
7. Testez la connexion.

   Sur un autre appareil du même réseau Tailscale, ouvrez un navigateur et saisissez l'IP virtuelle du routeur. Si l'interface Web s'ouvre, Tailscale fonctionne. Vous pouvez aussi tester la connexion avec ping ou accéder au terminal par SSH via cette IP.



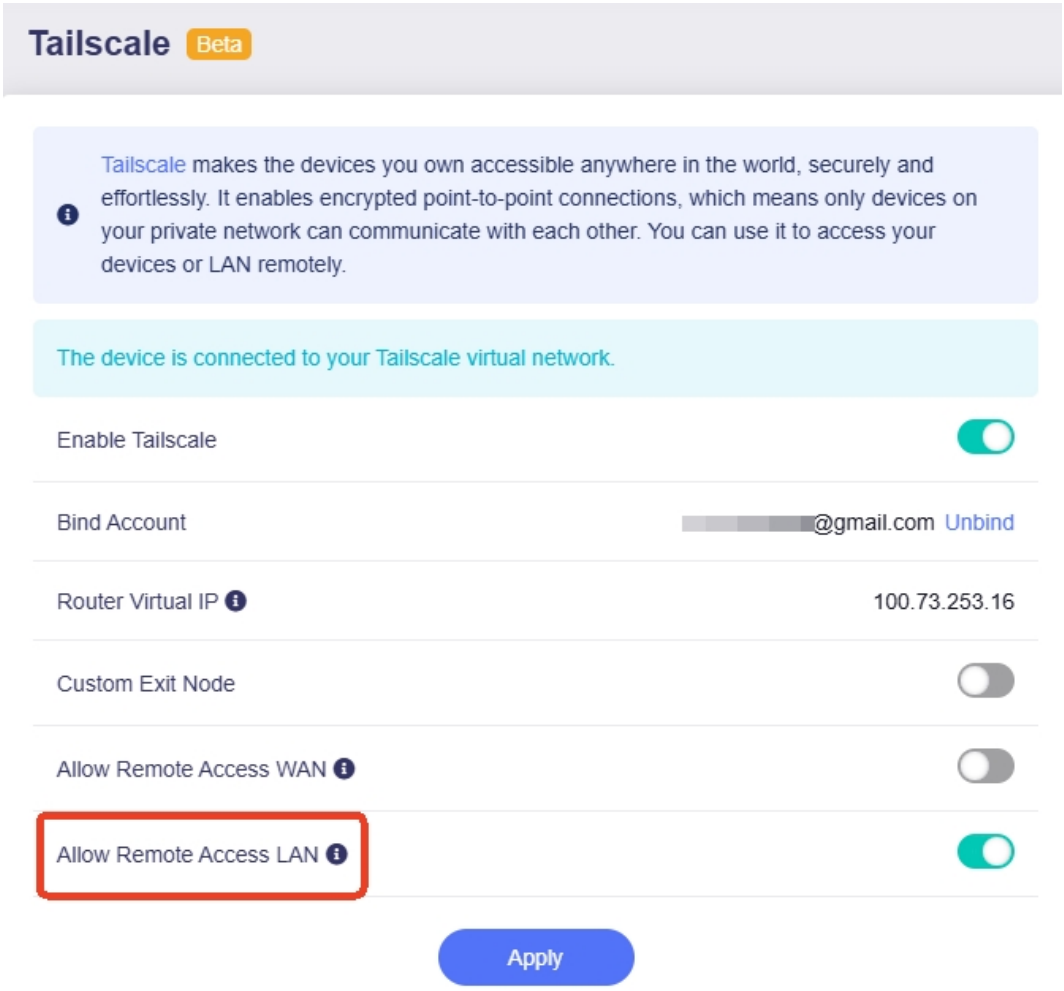
13.7.2 Autoriser l’accès distant au WAN

Si cette option est activée, les ressources côté WAN de l’appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



13.7.3 Autoriser l’accès distant au LAN

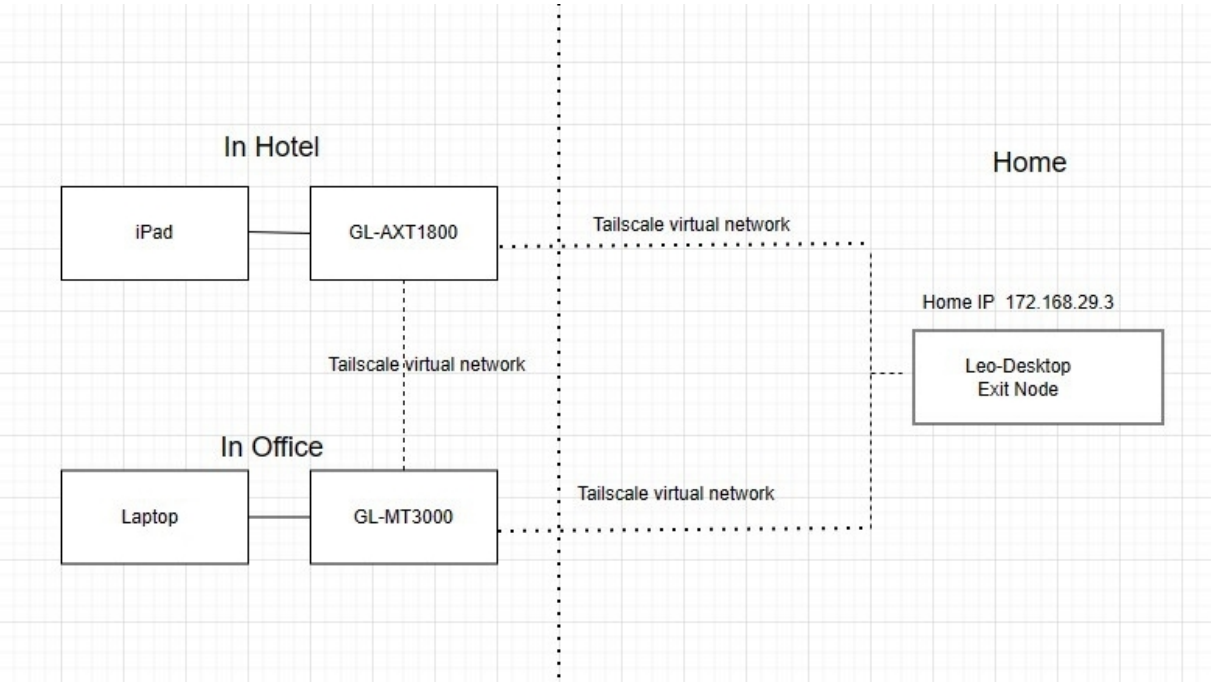
Si cette option est activée, les ressources côté LAN de l’appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



13.7.4 Nœuds de sortie personnalisés

Par défaut, Tailscale fonctionne comme un réseau superposé : il achemine uniquement le trafic entre les appareils utilisant Tailscale et ne traite pas votre trafic Internet public, comme la navigation sur Google.

Vous pouvez toutefois vouloir faire passer ce trafic par Tailscale. Par exemple, en déplacement à l'étranger, pour accéder à des services bancaires réservés à votre pays, configurez votre ordinateur domestique disposant d'une IP publique comme nœud de sortie. Réglez les autres appareils du même Tailnet, comme les GL-AXT1800 et GL-MT3000 ci-dessous, pour qu'ils l'utilisent. Tout leur trafic Internet public passe alors par ce nœud.



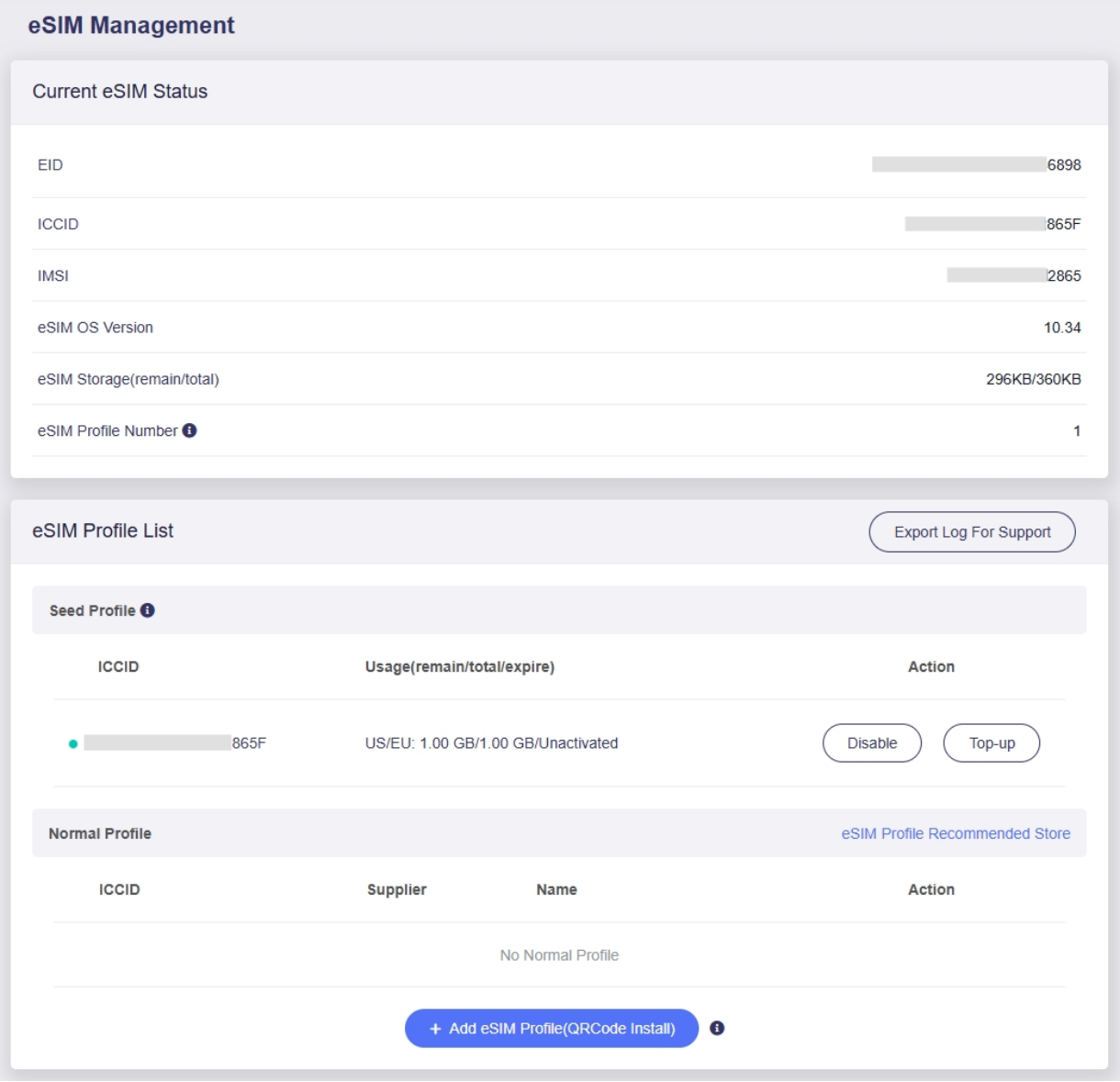
Un nœud de sortie achemine le trafic Internet sortant des appareils de votre Tailnet et joue ainsi le rôle d'un serveur VPN. Tout le trafic Internet extérieur à Tailscale semble provenir de son emplacement, ce qui facilite l'accès aux contenus géorestreints et renforce la confidentialité. L'appareil chargé de cet acheminement est appelé « nœud de sortie (Exit Node) ». Consultez ce tutoriel pour configurer un nœud de sortie personnalisé sur les routeurs GL.iNet.

Remarque : si le serveur DNS du routeur utilise une IP privée accessible uniquement sur le réseau local, l'emploi d'un nœud de sortie peut interrompre l'accès Internet. Définissez manuellement un DNS public, comme 8.8.8.8, pour l'éviter.

13.8 Gestion eSIM

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **APPLICATIONS** > **Gestion eSIM (eSIM Management)**.

Cette page permet de vérifier l'état de la carte physique eSIM et de gérer les profils eSIM. Elle comporte deux sections : **État actuel de l'eSIM (Current eSIM Status)** et **Liste des profils eSIM (eSIM Profile List)**.



13.8.1 État actuel de l’eSIM

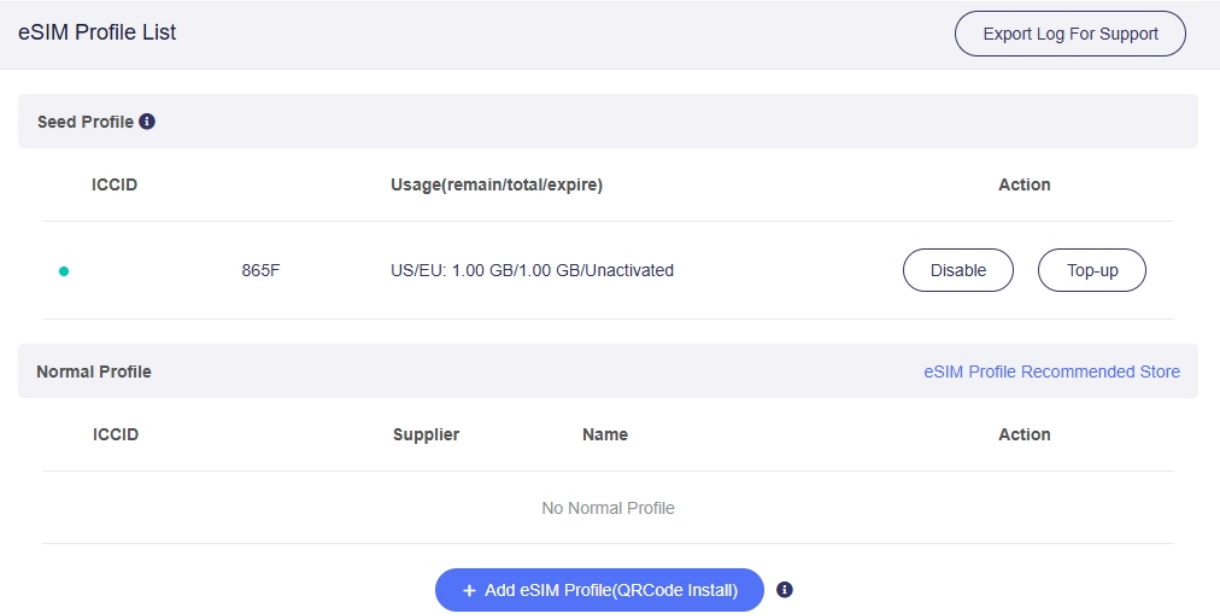
Cette section affiche les informations de base et les détails du profil eSIM actuellement actif.



- **EID :** identifiant unique mondial de l’eUICC (puce eSIM), utilisé pour l’identification et la gestion des profils.
- **ICCID :** identifiant de la carte à circuit intégré du profil eSIM actuellement actif.
- **IMSI :** identité internationale de l’abonné mobile du profil eSIM actuellement actif.
- **Version du système eSIM (eSIM OS Version) :** version du système d’exploitation de l’eUICC, qui détermine sa compatibilité et les fonctionnalités prises en charge.
- **Stockage eSIM (restant/total) (eSIM Storage (remain/total)) :** capacité de stockage disponible et totale de l’eUICC pour les profils eSIM.
- **Nombre de profils eSIM (eSIM Profile Number) :** nombre de profils actuellement stockés sur l’eUICC. Leur taille varie selon les opérateurs ; le nombre de profils pouvant être enregistrés varie donc également.

13.8.2 Liste des profils eSIM

Cette section présente les informations du profil eSIM initial et des profils standard.



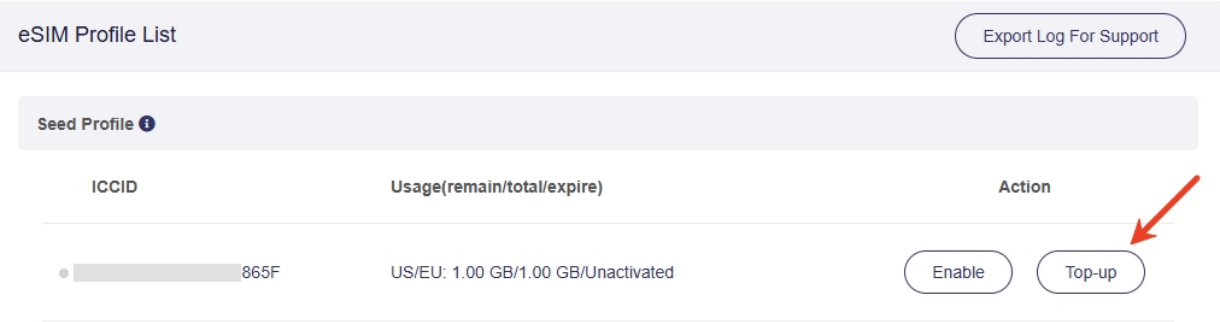
- **Profil initial (Seed Profile)** : ce profil préchargé inclut 1 Go de données gratuites pour les États-Unis et l'Europe, ainsi que 100 Mo de données utilisables dans le monde entier. Ces données sont valables pendant un an à compter de l'activation et permettent de télécharger d'autres profils partout dans le monde. Vous pouvez suivre la consommation du profil initial, notamment les données restantes, le volume total et la date d'expiration.
- **Profil standard (Normal Profile)** : lorsque vous achetez un profil eSIM et l'importez à l'aide d'un code QR ou d'un code d'activation, il apparaît ici.

13.8.2.1 Recharge du profil initial

GL.iNet fournit un profil initial préchargé comprenant 100 Mo de données utilisables dans le monde entier et 1 Go de données valables en Europe et aux États-Unis, pour la configuration initiale et l'activation des profils eSIM. Ce forfait permet de télécharger de nouveaux profils eSIM à votre arrivée à une destination sans accès à Internet.

Si les données gratuites préchargées sont épuisées ou ont expiré et que vous souhaitez continuer d'utiliser le service, vous pouvez recharger le profil initial.

Dans la section Profil initial (Seed Profile), cliquez sur le bouton **Recharger (Top-up)** à droite.



Dans la fenêtre qui s'affiche, scannez le code QR et suivez les instructions pour effectuer la recharge.



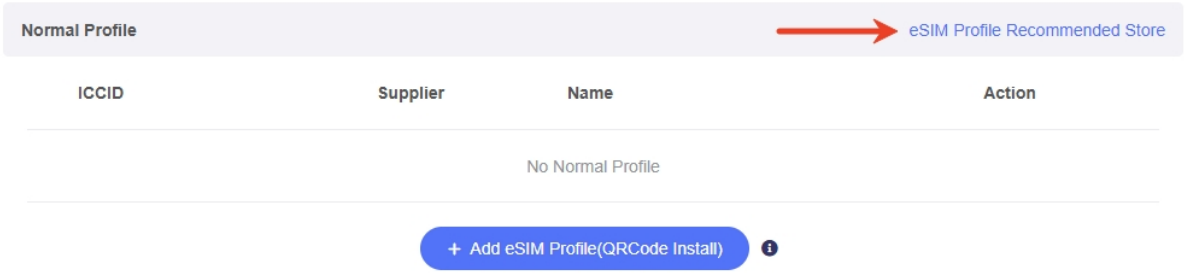
13.8.2.2 Achat d'un profil eSIM

Vous pouvez acheter des profils eSIM dans nos boutiques recommandées, dans des boutiques testées ou auprès d'autres fournisseurs eSIM tiers.

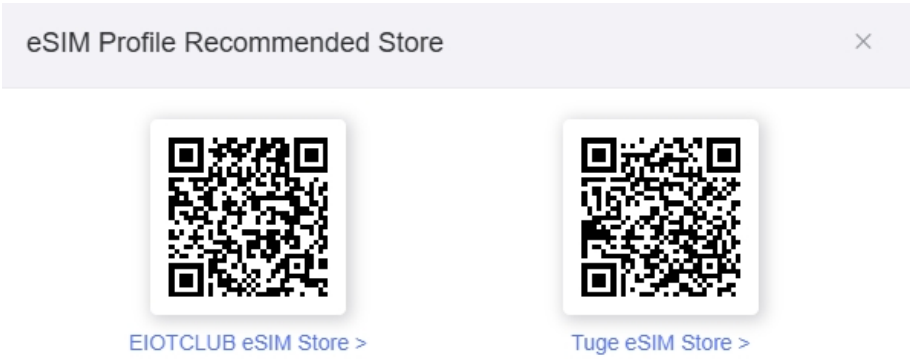
Option 1 : achat dans nos boutiques recommandées.

Deux boutiques sont recommandées : EIOTCLUB eSIM Store et Tuge eSIM Store.

Dans la section Profil standard (Normal Profile), cliquez sur **Boutiques recommandées pour les profils eSIM (eSIM Profile Recommended Store)** à droite.



Scannez le code QR ou cliquez sur les liens pour acheter des profils eSIM.



Remarque : tous les profils et forfaits eSIM achetés dans ces deux boutiques sont entièrement compatibles avec les routeurs GL.iNet. Pour toute question, contactez notre assistance à support@gl-inet.com.

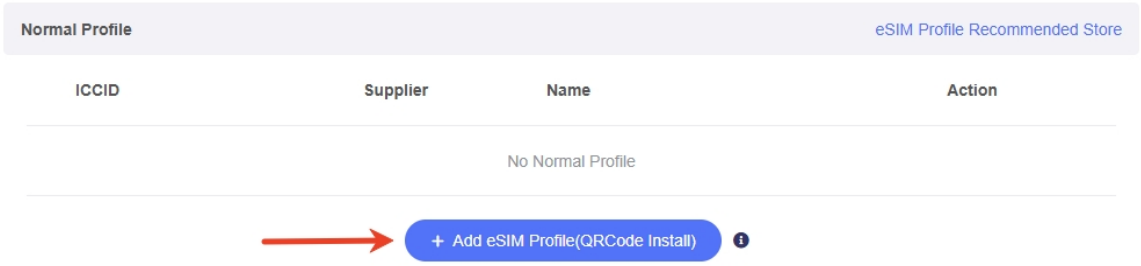
Option 2 : achat dans des boutiques testées.
Consultez ce lien pour afficher la liste des boutiques testées par GL.iNet.
Remarque : nous ne pouvons pas garantir la compatibilité de tous les profils ou forfaits de ces boutiques avec les routeurs GL.iNet. GL.iNet n'ayant aucun partenariat avec elles, nous ne pouvons pas assurer le service après-vente ni intervenir pour les remboursements.

Option 3 : achat auprès d'autres fournisseurs eSIM tiers.
Vous pouvez également acheter des profils eSIM auprès d'autres fournisseurs tiers de votre choix.
Toutefois, nous ne pouvons pas garantir leur entière compatibilité avec les routeurs GL.iNet. Effectuez votre achat en connaissance de cause. GL.iNet n'est pas responsable des problèmes d'incompatibilité.
Pour le service après-vente ou les remboursements, contactez le fournisseur eSIM concerné.

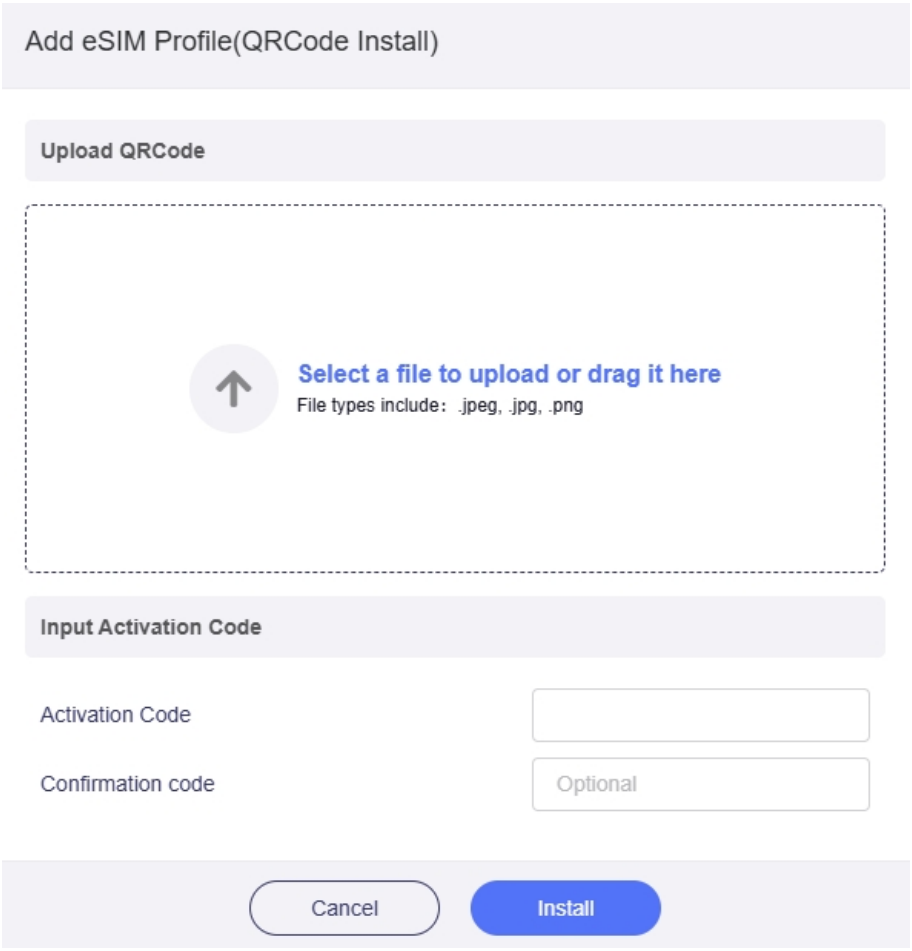
13.8.2.3 Importation d’un profil eSIM

Après l’achat d’un profil eSIM, vous recevez généralement un code QR ou un code d’activation. Enregistrez le code QR sur votre appareil, puis procédez comme suit pour importer le profil eSIM.

1. Dans la section Profil standard (Normal Profile), cliquez sur **Ajouter un profil eSIM (Add eSIM Profile)** en bas de la page.

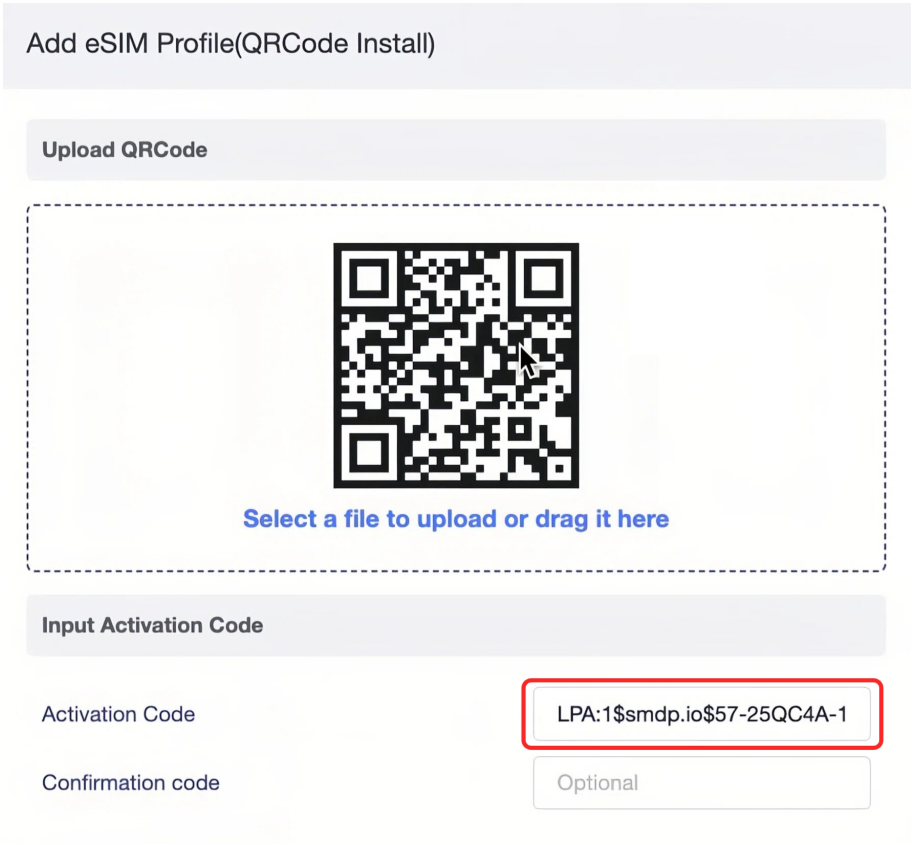


2. Importez le code QR de votre eSIM ou saisissez le code d’activation, puis cliquez sur **Installer (Install)**. Le profil eSIM est alors téléchargé et installé sur le routeur.



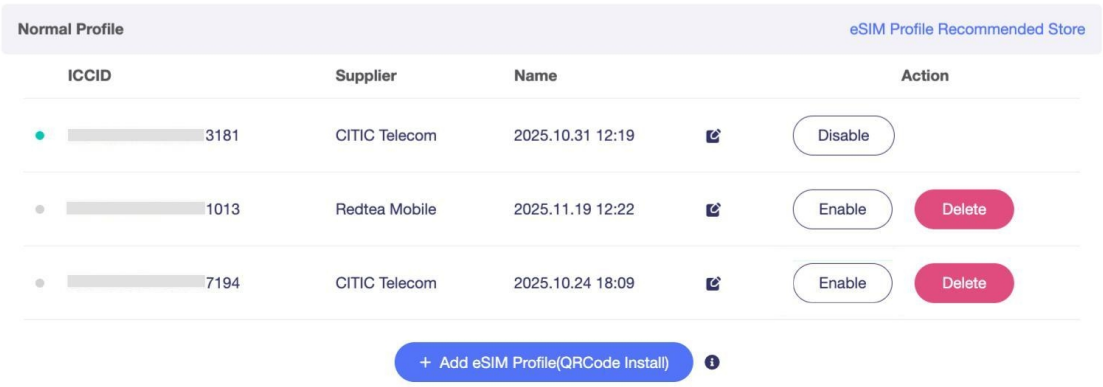
Remarque :

1. La plupart des profils eSIM ne peuvent être téléchargés et installés qu'une seule fois.
2. Un code QR correctement formaté fournit un code d'activation commençant par **LPA:**. Toutefois, certains codes QR non standard fournissent uniquement le code d'activation brut, sans ce préfixe. Dans ce cas, ajoutez manuellement LPA: au début du code avant de cliquer sur Installer (Install).

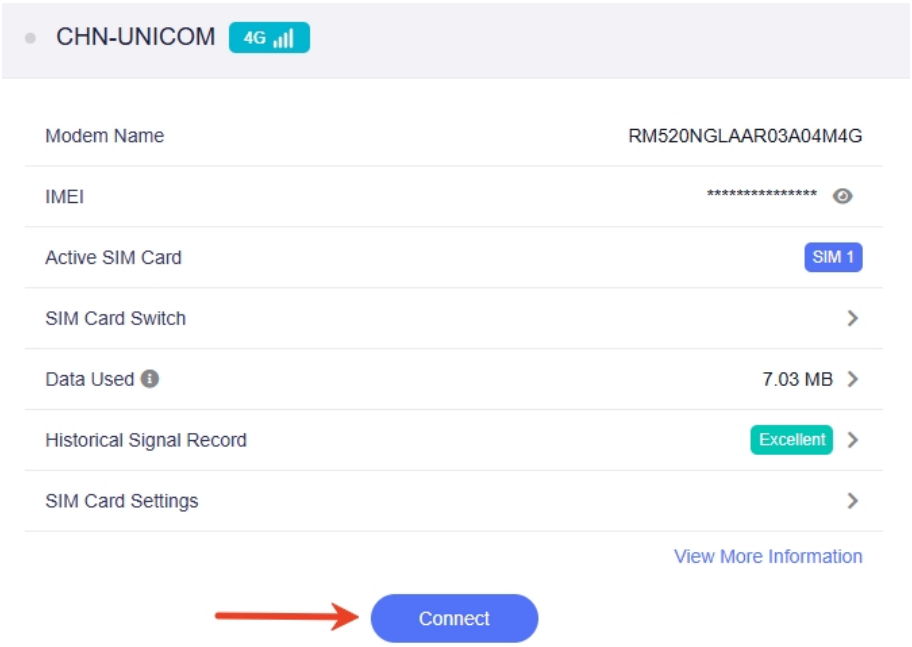


3. Si vous n'avez pas encore acheté de profil eSIM, vous pouvez en acheter un dans les boutiques recommandées. Consultez la section 13.8.2.2 Achat d'un profil eSIM pour en savoir plus.

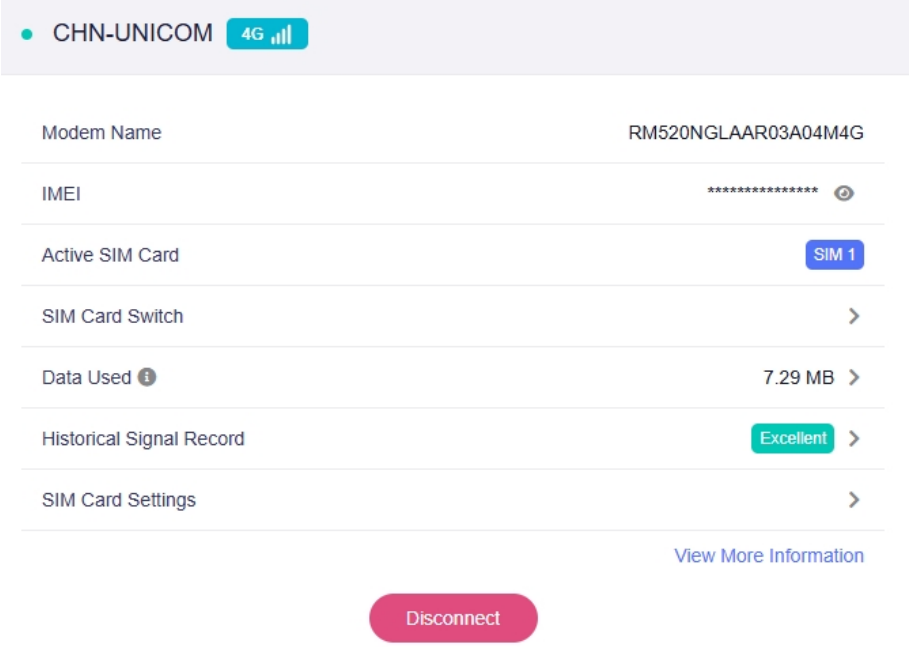
3. Après l'importation, le nouveau profil eSIM apparaît dans la liste **Profil standard (Normal Profile)**. Cliquez sur **Activer (Enable)** pour l'activer.



4. Connexion à Internet.
   Après l'activation du profil eSIM, ouvrez **INTERNET** > **Cellulaire (Cellular)**. Cliquez sur **Connecter (Connect)** pour établir une connexion Internet via ce profil.



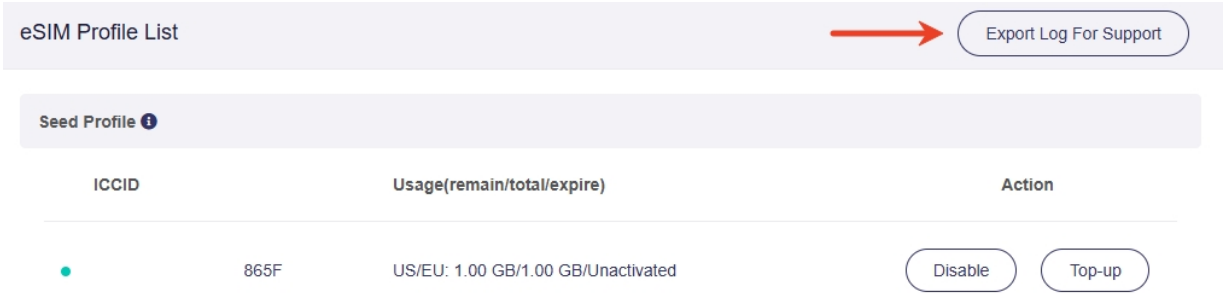
   Remarque : certains profils eSIM peuvent nécessiter des paramètres supplémentaires, comme l'APN, le code PIN ou le TTL. Si nécessaire, cliquez sur **Configuration manuelle (Manual Setup)** ou **Paramètres de la carte SIM (SIM Card Settings)** pour les régler. Dans certains cas, vous devez redémarrer l'appareil pour établir la connexion Internet.
5. Une fois la connexion via le profil eSIM établie, la page s'affiche comme suit :



13.8.2.4 Exportation des journaux pour l'assistance

Cliquez sur **Exporter les journaux pour l'assistance (Export Log for Support)** pour consulter tous les journaux liés à l'eSIM.

Si vous rencontrez un problème nécessitant une assistance technique, exportez les journaux eSIM et envoyez-les à notre équipe à l'adresse support@gl-inet.com.



Chapitre 14

Réseau

Ce chapitre présente les paramètres de configuration et de gestion du réseau, notamment LAN, DNS et IPv6.

14.1 Redirection de port

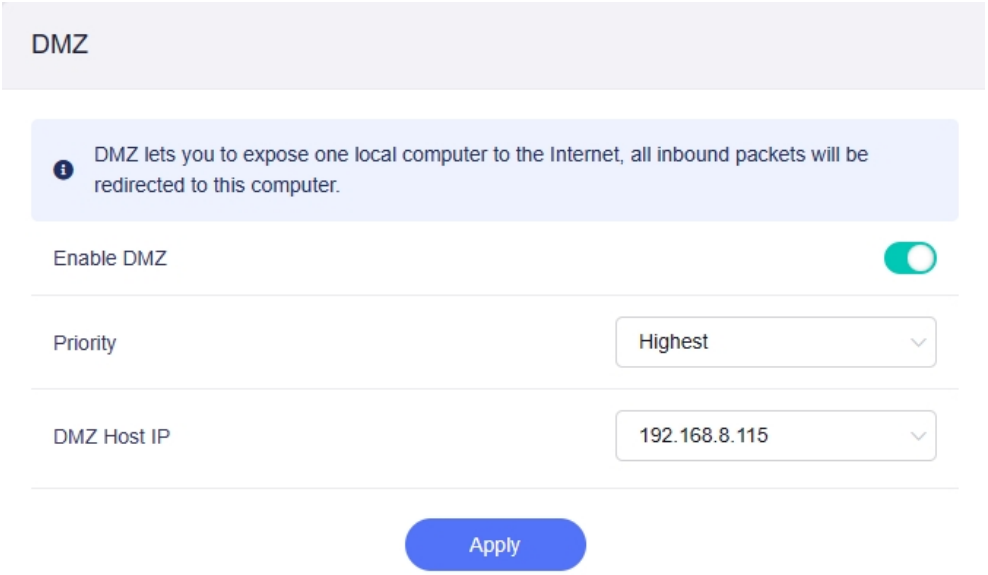
La redirection de port achemine les requêtes externes vers des appareils précis du réseau local. Cette page propose deux fonctions : **DMZ**, pour un accès direct complet à un appareil, et **Redirection de port (Port Forwarding)**, pour un accès ciblé à certains ports.

14.1.1 DMZ

La DMZ expose un ordinateur à Internet en lui redirigeant tous les paquets entrants.

Pour activer la DMZ, procédez comme suit.

1. Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Redirection de port (Port Forwarding)** > section **DMZ**.
2. Activez **Activer la DMZ (Enable DMZ)**. Sélectionnez la priorité et l'IP de l'hôte DMZ dans les listes, puis cliquez sur **Appliquer (Apply)**.



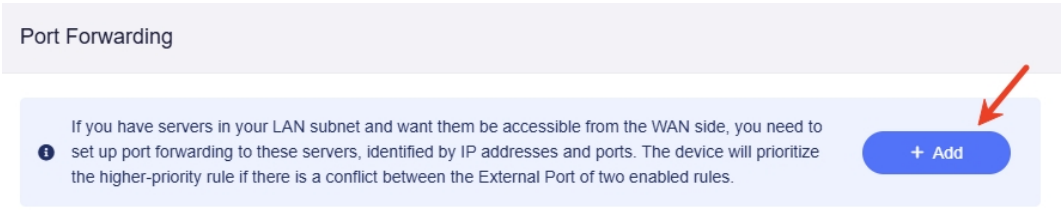
- **Priorité (Priority)** : choisissez La plus élevée ou La plus faible. Si la DMZ est prioritaire sur les règles de redirection de port, celles-ci deviennent inopérantes. Sinon, les requêtes ne sont transmises au client DMZ que si aucune règle ne correspond au port demandé.
- **IP de l'hôte DMZ (DMZ Host IP)** : sélectionnez l'adresse IP interne de l'appareil qui recevra tous les paquets entrants.

14.1.2 Redirection de port

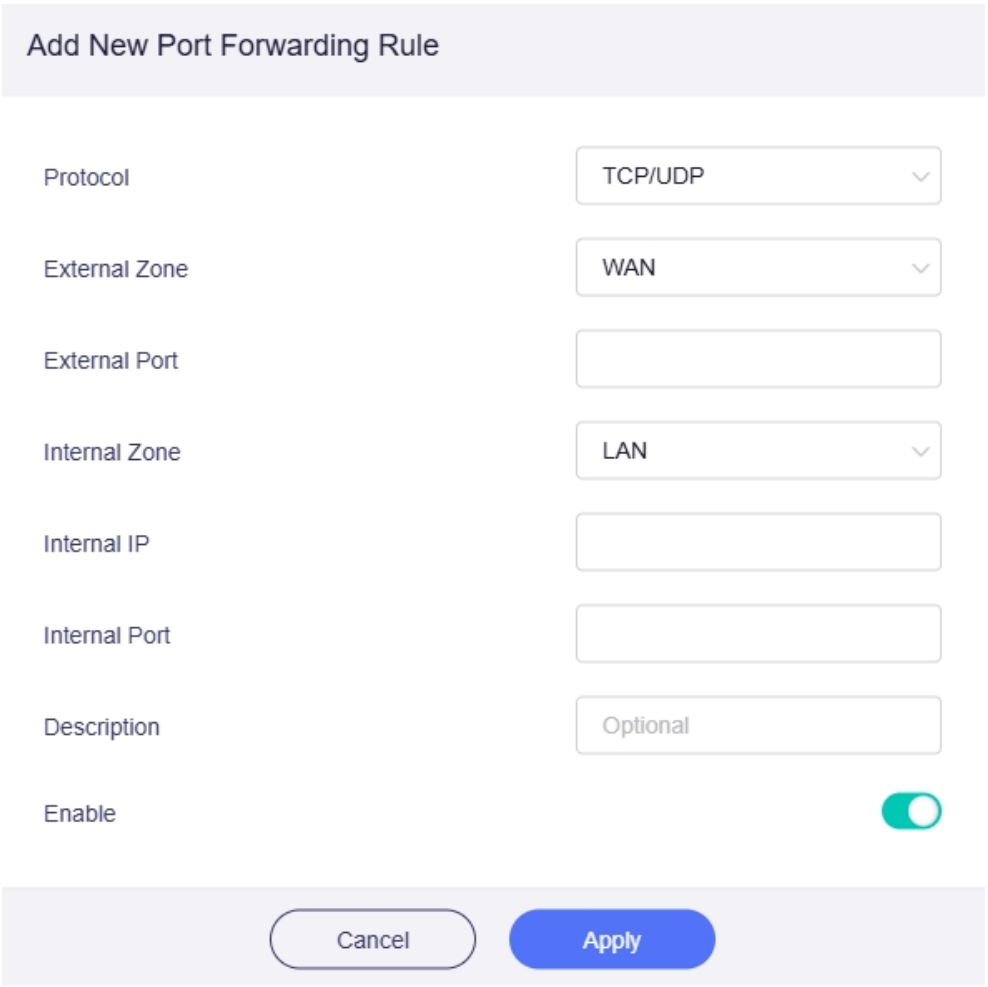
La redirection de port permet à des ordinateurs distants de se connecter à un ordinateur ou serveur local situé derrière le pare-feu LAN, comme un serveur Web ou FTP.

Pour configurer une redirection de port, procédez comme suit.

1. Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Redirection de port (Port Forwarding)** > **Redirection de port (Port Forwarding)**, puis cliquez sur **Ajouter (Add)**.



2. Dans la fenêtre qui s'affiche, saisissez ou sélectionnez les paramètres nécessaires, puis cliquez sur **Appliquer (Apply)** pour ajouter la règle.



- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP et UDP.
- **Zone externe (External Zone)** : options disponibles : WAN, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN, LAN et Invité.
- **Port externe (External Port)** : numéro de port externe compris entre 1 et 65535. Définissez un port ou une plage en séparant le premier et le dernier numéro par un tiret, par exemple 501-510.
- **Zone interne (Internal Zone)** : options disponibles : LAN, Invité, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN et WAN.
- **IP interne (Internal IP)** : adresse IP attribuée par le routeur à l'appareil nécessitant un accès distant. Si vous avez défini un port unique dans Port externe, définissez-en un ici. Si vous avez défini une plage dans Port externe, renseignez la plage correspondante ici.
- **Port interne (Internal Port)** : numéro de port interne de l'appareil. Saisissez un port précis. Laissez ce champ vide s'il est identique au port externe.

- **Description** : nom ou description de la règle, facultatif.
- **Activer (Enable)** : active ou désactive la règle.

14.2 Multi-WAN

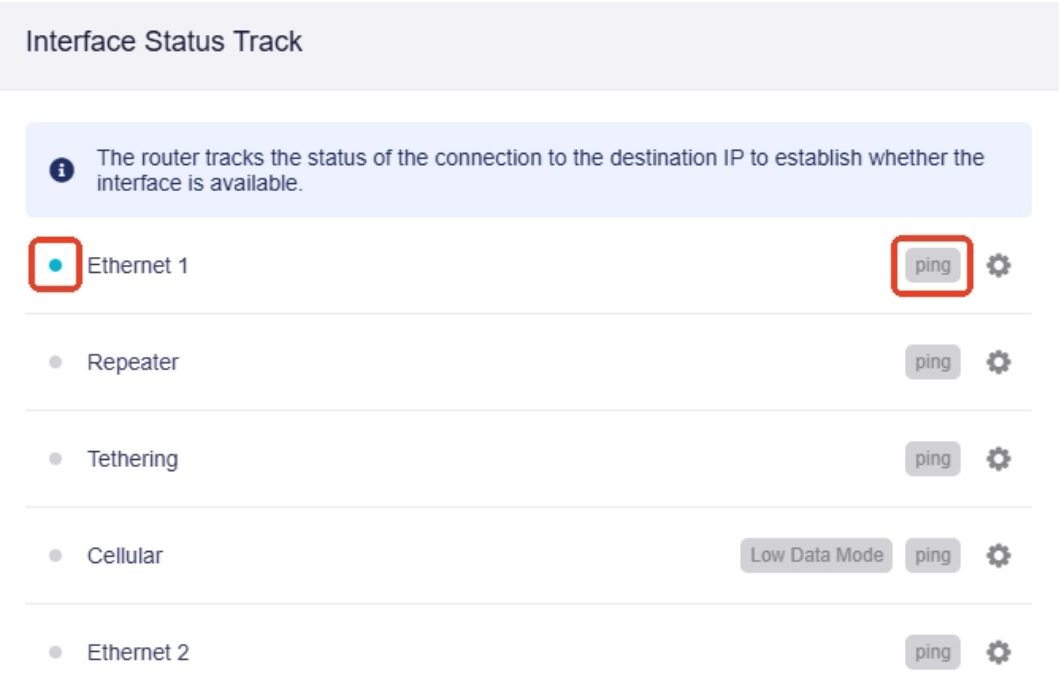
Multi-WAN permet d'utiliser simultanément plusieurs méthodes d'accès à Internet et de configurer différentes options de connexion sur le routeur. Deux modes sont proposés :

- **Basculement (Failover)** : passe automatiquement à une connexion de secours peu après la défaillance de la connexion principale pour maintenir l'accès réseau.
- **Équilibrage de charge (Load Balance)** : répartit le trafic entre les connexions disponibles selon un ratio défini, afin de les utiliser simultanément et d'optimiser la bande passante.

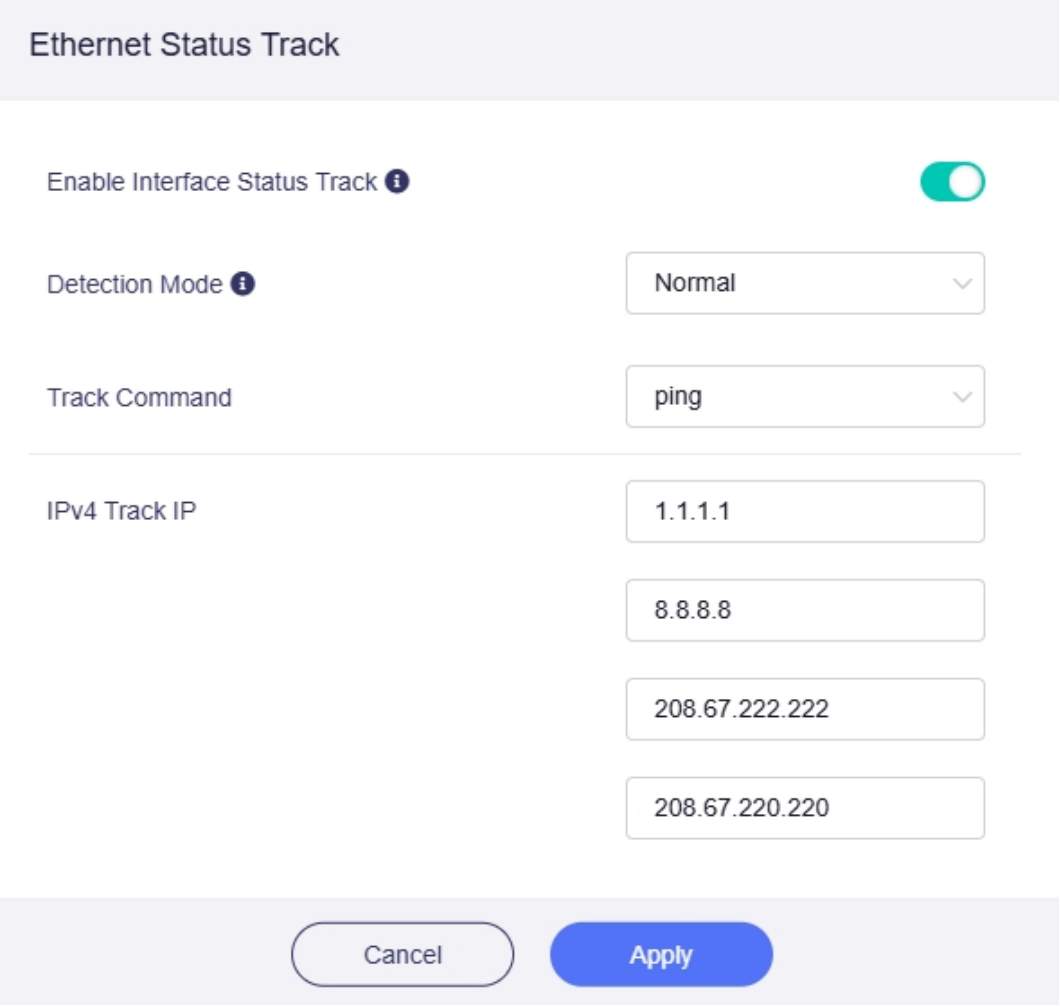
Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Multi-WAN**. Cette page comporte deux sections : Suivi de l'état des interfaces et Mode Multi-WAN.

14.2.1 Suivi de l'état des interfaces

Les routeurs GL.iNet utilisent la commande **ping** pour vérifier la connexion à une adresse IP cible et déterminer si l'interface est disponible. Un point vert apparaît à gauche si elle est disponible ; sinon, il est gris.



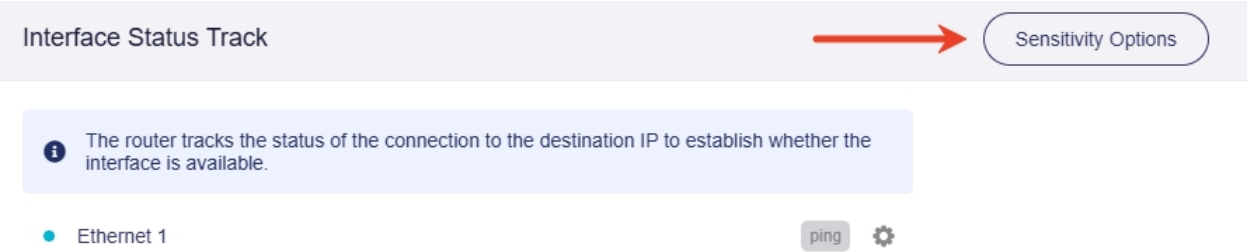
Dans la section **Suivi de l'état des interfaces (Interface Status Track)**, cliquez sur l'engrenage à droite pour régler le suivi de chaque interface. Les paramètres Ethernet sont présentés ci-dessous. La même logique s'applique aux autres interfaces.



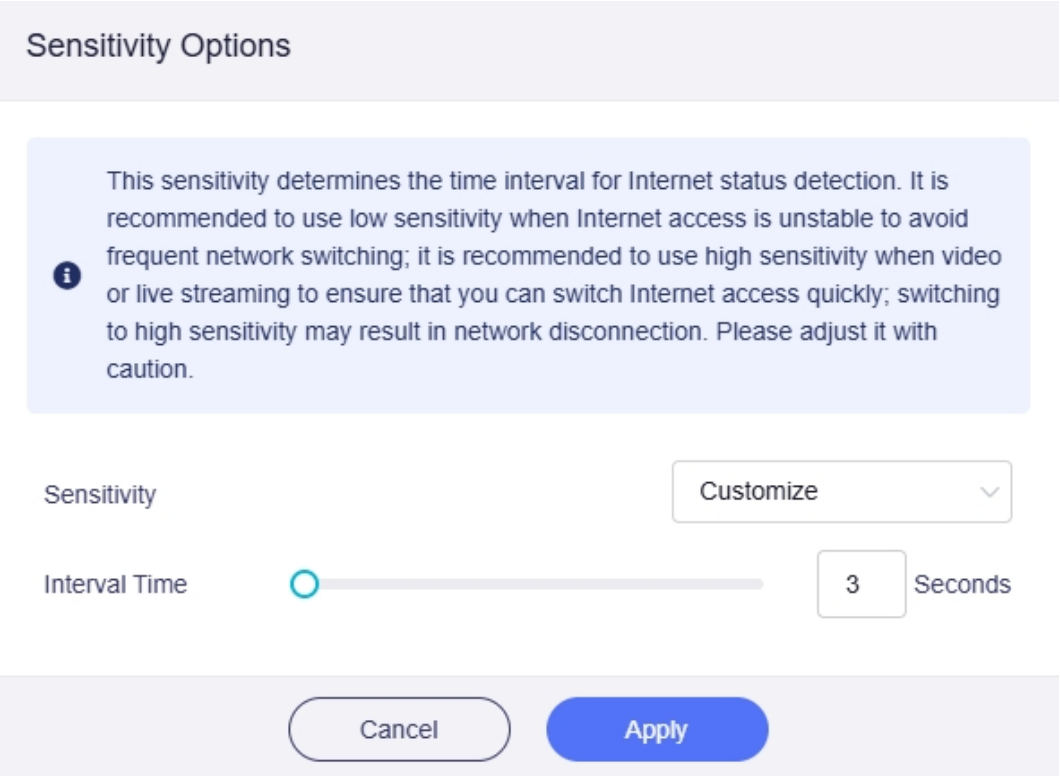
- **Activer le suivi de l'état de l'interface (Enable Interface Status Track)** : activé par défaut. Si vous le désactivez, le routeur détermine l'état de l'interface selon les conditions physiques, par exemple le branchement du câble Ethernet.
- **Mode de détection (Detection Mode)** : introduite sous le nom Mode données réduites dans le micrologiciel v4.5, cette fonction a été renommée Mode de détection en v4.7. Trois modes sont proposés : Normal, Données réduites et Strict.
  - **Normal** : mode utilisé par défaut.
  - **Faible consommation de données (Low Data)** : la surveillance ne se déclenche qu'en cas d'erreur réseau sur l'interface. Utilisez ce mode si votre forfait de données est limité. La reconnexion après une coupure peut être légèrement plus lente qu'en mode Normal. Ce mode n'est activé par défaut que pour l'interface cellulaire.
  - **Strict** : détermine l'état de l'interface uniquement à partir des résultats d'une commande de détection envoyée à une adresse IP publique.

- **Commande de suivi (Track Command)** : la commande ping vérifie la connexion à l'IP cible et la disponibilité de l'interface.
- **IP de suivi IPv4 (IPv4 Track IP)** : personnalisez les adresses IPv4 utilisées pour le suivi si nécessaire.

Cliquez sur **Options de sensibilité (Sensitivity Options)** dans l'angle supérieur droit.



Choisissez un intervalle de détection Faible, Moyen ou Élevé, ou personnalisez-le. L'intervalle peut être compris entre 0,5 et 90 secondes.

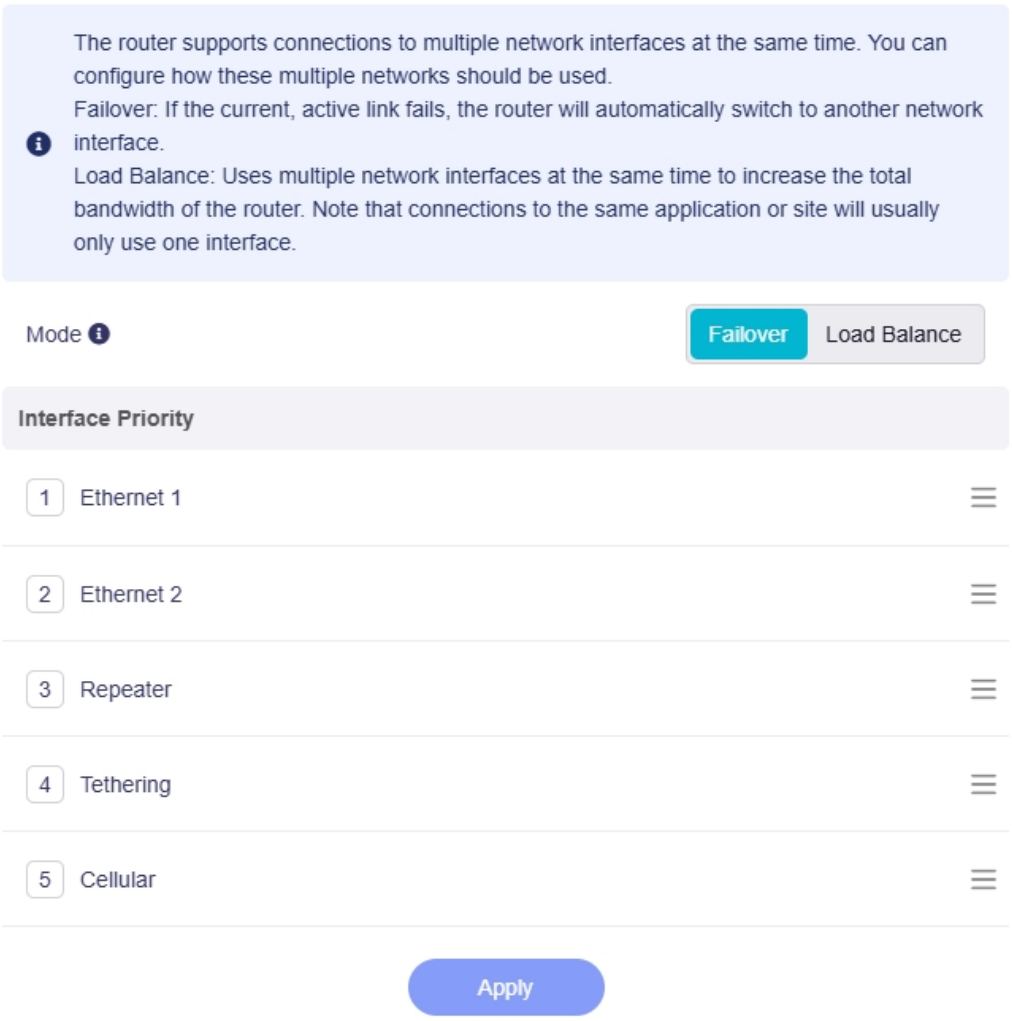


14.2.2 Mode Multi-WAN

Deux modes sont proposés : **Basculement (Failover)** et **Équilibrage de charge (Load Balance)**. Ils ne peuvent pas être utilisés simultanément.

Basculement

Le basculement est le mode par défaut lorsque plusieurs connexions sont configurées. Si la liaison active échoue, le routeur utilise automatiquement une autre interface pour accéder à Internet.

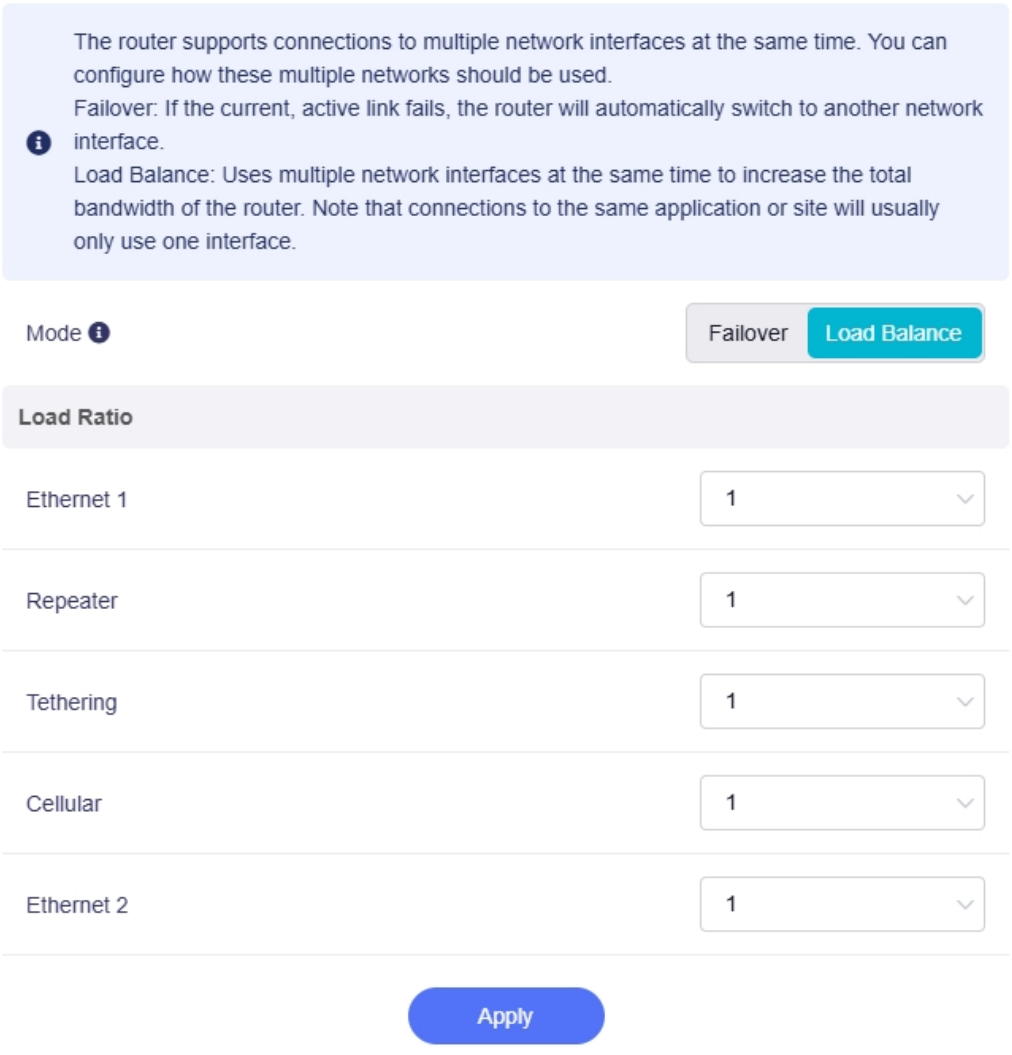


Vous pouvez définir une priorité pour chaque interface. En cas de défaillance, le routeur sélectionne l'interface disponible la plus prioritaire. Dès qu'une connexion plus prioritaire est rétablie, il l'utilise de nouveau automatiquement.

Équilibrage de charge

Ce mode utilise plusieurs interfaces simultanément pour augmenter la bande passante totale du routeur. Le système répartit les nouvelles connexions selon le ratio de charge configuré. Les connexions à une même application ou à un même site utilisent toutefois généralement une seule interface.

Le ratio de charge définit la proportion des nouvelles connexions attribuées à chaque interface réseau. Le système choisit l'interface chargée de chaque nouvelle connexion selon ce ratio.



Par exemple, si le routeur est connecté simultanément à quatre réseaux, comme Ethernet, Répéteur, Partage de connexion et Cellulaire, et que les quatre interfaces donnent accès à Internet, activez l'équilibrage de charge avec un ratio 1:1:1:1. Les nouvelles connexions sont

réparties également entre les quatre interfaces selon ce ratio, ce qui permet de partager la bande passante réseau.

Vous pouvez également personnaliser les coefficients de répartition. Par exemple, si Ethernet dispose d'une bande passante de 100 Mbit/s, Répéteur de 200 Mbit/s et qu'aucune connexion Partage de connexion ou Cellulaire n'est active, définissez les coefficients sur 1 pour Ethernet, 2 pour Répéteur et 0 pour Partage de connexion et Cellulaire. Le système répartit alors les nouvelles connexions entre ces interfaces selon le rapport 1:2 : Ethernet traite deux fois moins de connexions que Répéteur. Contrairement au mode Basculement, ce mode optimise le débit global en répartissant la charge entre toutes les interfaces disponibles.

Remarque : les connexions et le trafic existants ne suivent pas nécessairement le ratio de charge. La répartition réelle se rapproche progressivement du ratio configuré au fil de l'utilisation.

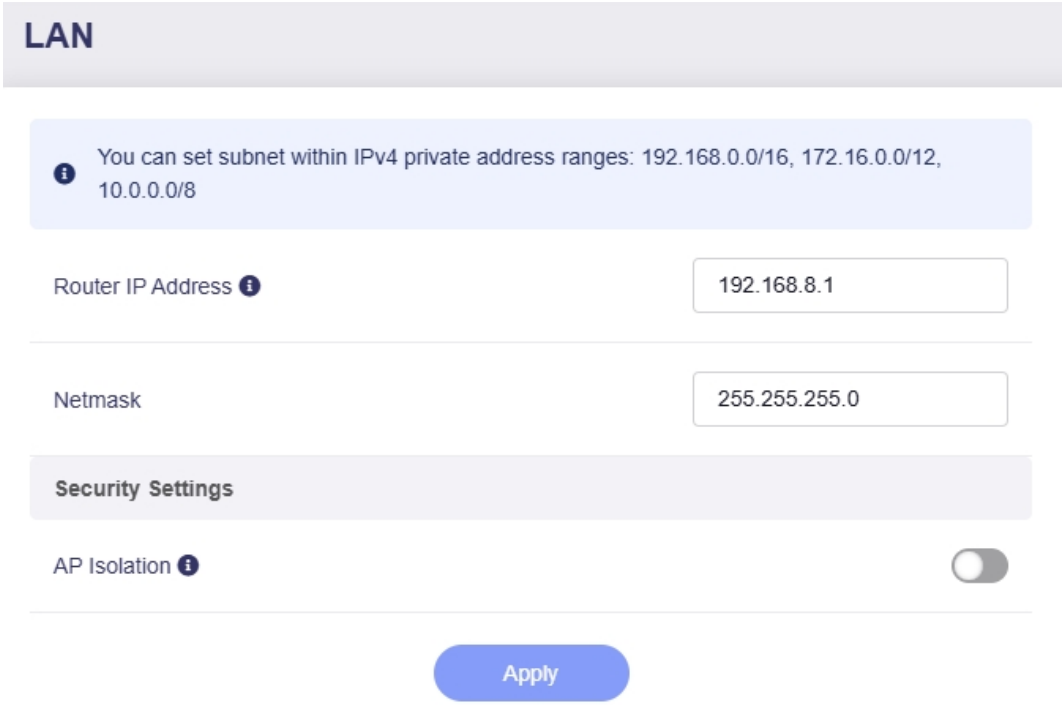
14.3 LAN

Le LAN (Local Area Network, réseau local) désigne le réseau privé auquel vos appareils se connectent par câble Ethernet.

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **LAN**. Vous pouvez y configurer les paramètres de base, le serveur DHCP et la réservation d'adresses.

14.3.1 Paramètres de base

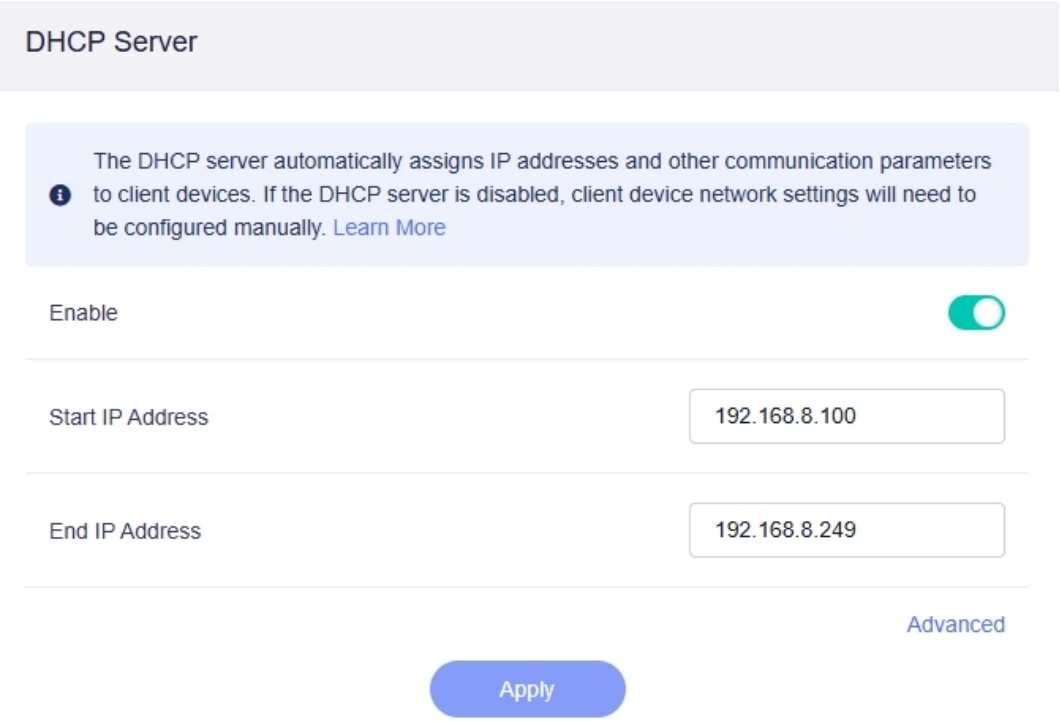
Les paramètres de base comprennent l'adresse IP du routeur et le masque de sous-réseau. Vous pouvez définir un sous-réseau dans les plages IPv4 privées : 192.168.0.0/16, 172.16.0.0/12 ou 10.0.0.0/8.



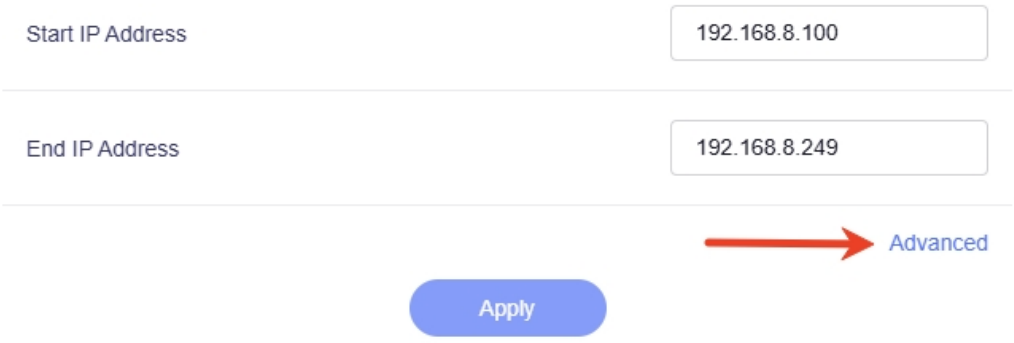
- **Adresse IP du routeur (Router IP Address)** : adresse à saisir dans le navigateur pour ouvrir l'interface d'administration. Par défaut, elle est 192.168.8.1. Modifiez-la si elle entre en conflit avec le réseau en amont.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Isolation des clients Wi-Fi (AP Isolation)** : isole les appareils clients dans une zone réseau distincte. Ces appareils ne peuvent pas communiquer avec les autres appareils du réseau.

14.3.2 Serveur DHCP

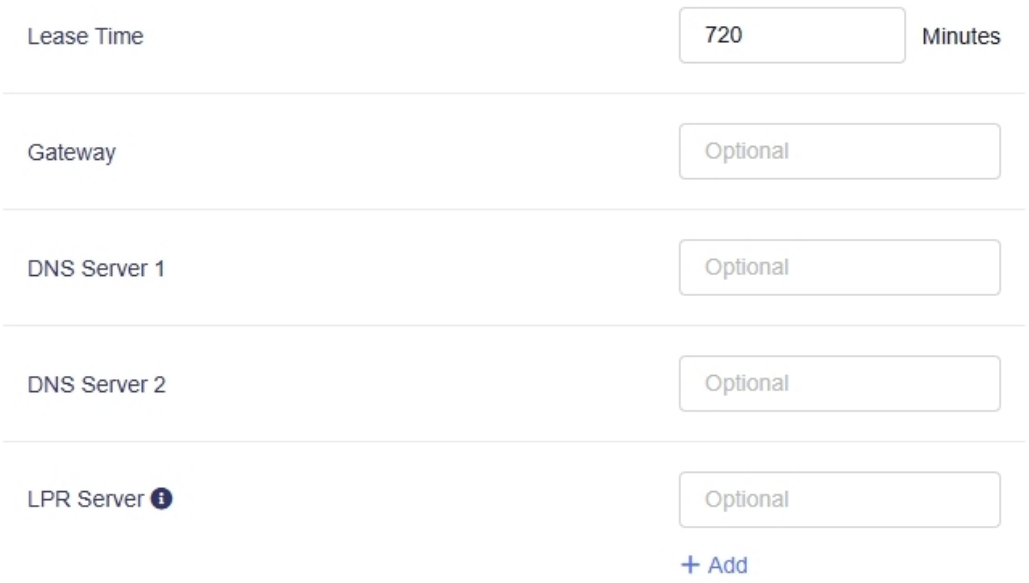
Le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Il est activé par défaut sur le routeur GL.iNet, avec une plage d'adresses de 192.168.8.100 à 192.168.8.249. Vous pouvez personnaliser cette plage.



Cliquez sur **Avancé (Advanced)** dans l'angle inférieur droit.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.



- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par DHCP.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau local et les réseaux externes, comme Internet.
- **Serveur DNS 1 (DNS Server 1)** : serveur principal chargé de convertir les noms de domaine en adresses IP.
- **Serveur DNS 2 (DNS Server 2)** : serveur de secours utilisé pour résoudre les noms de domaine si le serveur principal échoue.
- **Serveur LPR (LPR Server)** : service Line Printer Remote qui gère les tâches d'impression et permet aux appareils réseau d'envoyer des demandes à des imprimantes distantes. Plusieurs ports LPR peuvent être configurés pour les imprimantes.

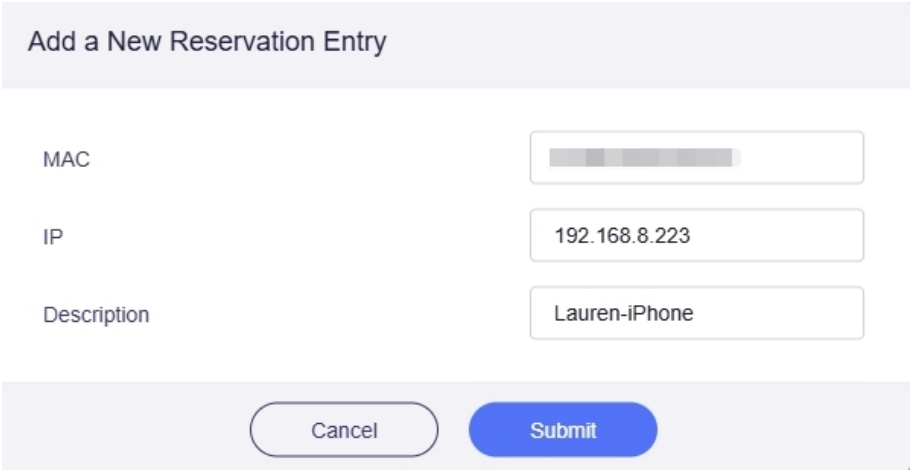
Remarque : si vous désactivez le serveur DHCP, définissez manuellement une IP statique et les autres paramètres de communication sur chaque client. Consultez cette page pour en savoir plus.

14.3.3 Réservation d’adresses

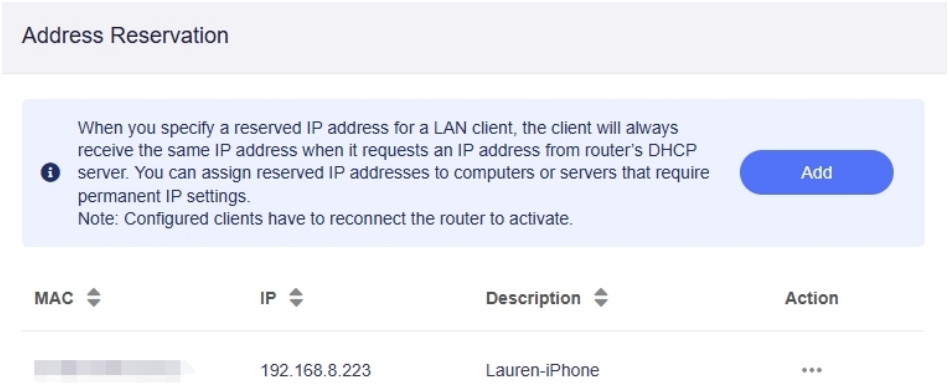
La réservation d’adresses permet d’attribuer une IP fixe à un client LAN. Celui-ci reçoit alors toujours la même adresse du serveur DHCP du routeur. Cette fonction convient aux ordinateurs et aux serveurs nécessitant une adresse permanente. Les clients concernés doivent se reconnecter au routeur pour que le réglage prenne effet.

Pour configurer une réservation d’adresse, procédez comme suit.

1. Dans l’interface d’administration Web, ouvrez **RÉSEAU (NETWORK)** > **LAN** > **Réservation d’adresses (Address Reservation)**, puis cliquez sur **Ajouter (Add)**.
2. Dans la fenêtre qui s’affiche, sélectionnez l’adresse MAC dans la liste. L’adresse IP correspondante est renseignée automatiquement. Saisissez un nom explicite, puis cliquez sur **Valider (Submit)**.



3. La nouvelle réservation apparaît dans la liste, comme ci-dessous.



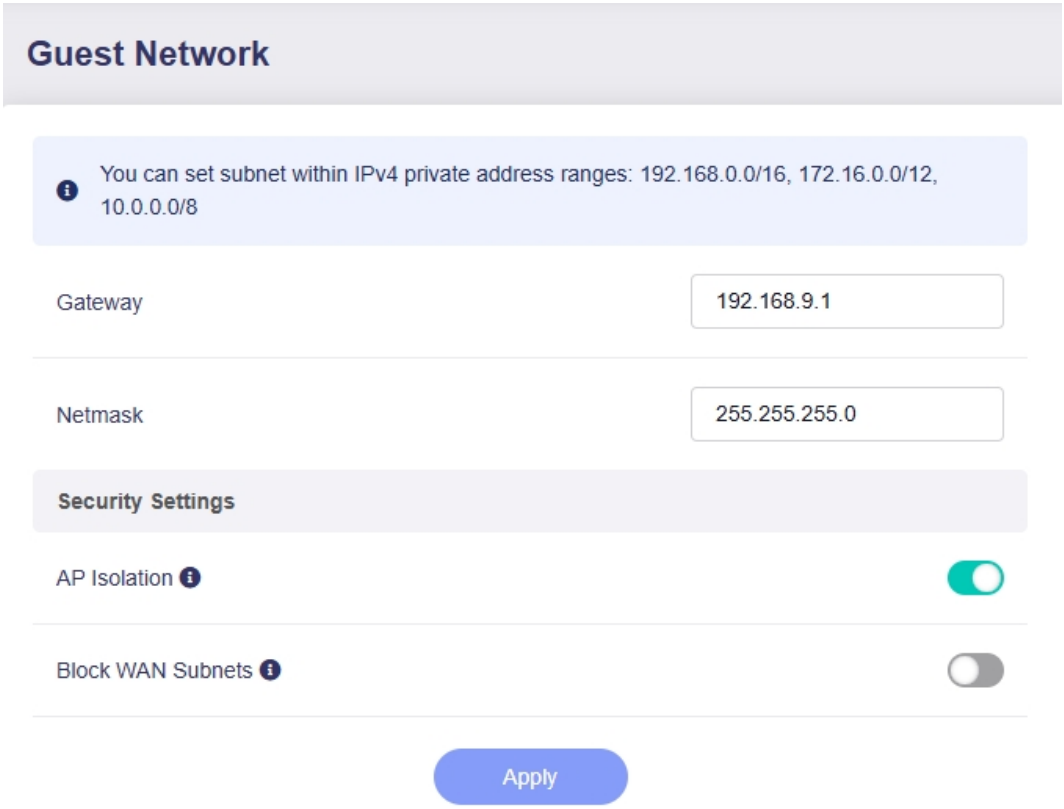
14.4 Réseau invité

Le réseau invité est un réseau dédié aux visiteurs, séparé de votre LAN principal pour protéger votre réseau privé.

Dans l'interface Web, ouvrez **RÉSEAU (NETWORK)** > **Réseau invité (Guest Network)**. Vous pouvez y configurer le réseau invité, notamment les paramètres de base et le serveur DHCP.

14.4.1 Paramètres de base

Ces paramètres comprennent la passerelle, le masque de sous-réseau, l'isolation des clients et le blocage des sous-réseaux WAN.



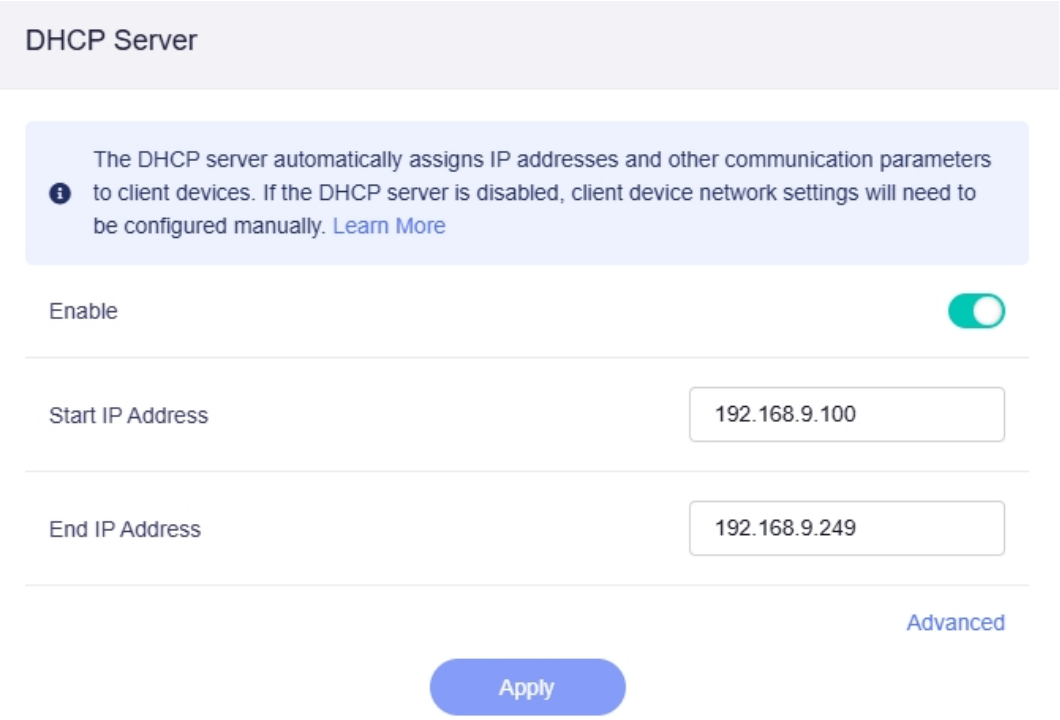
- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.9.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Isolation des clients (AP Isolation)** : isole les clients invités dans des segments distincts pour empêcher leur communication avec les autres appareils du même réseau.

- **Bloquer les sous-réseaux WAN (Block WAN Subnets)** : si cette option est activée, le réseau invité ne peut pas accéder au réseau en amont ni au segment réseau correspondant.

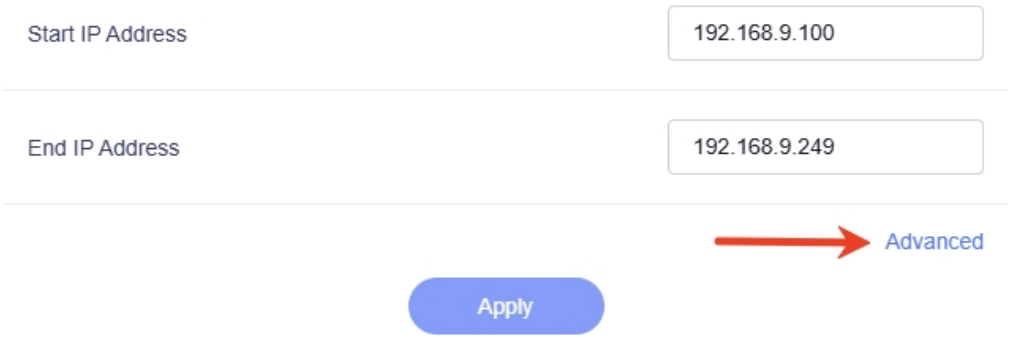
14.4.2 Serveur DHCP

Le réseau invité étant désactivé par défaut, son serveur DHCP reste désactivé et masqué jusqu'à son activation manuelle.

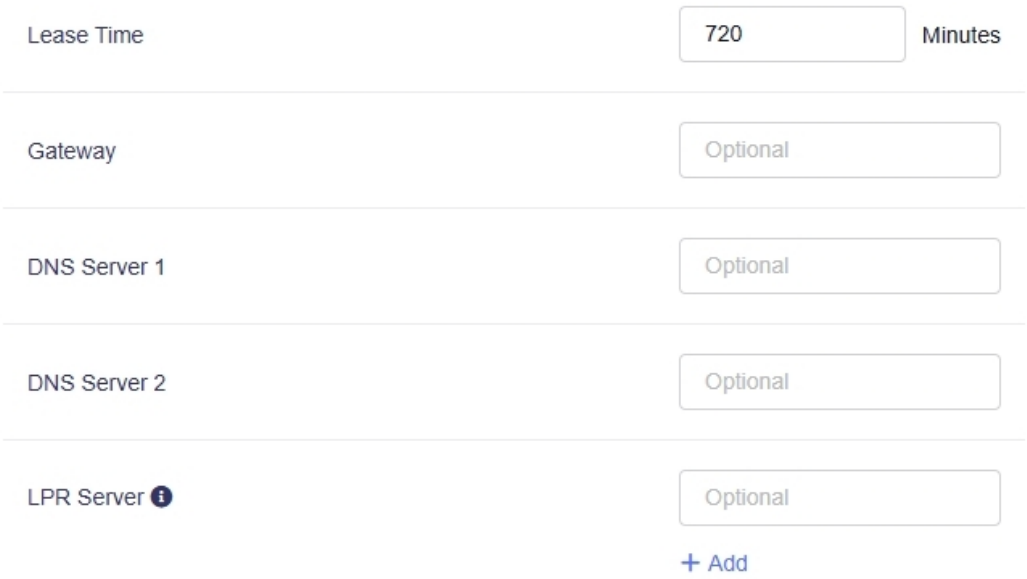
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client. Sa plage d'adresses s'étend de 192.168.9.100 à 192.168.9.249. Vous pouvez la personnaliser.



Cliquez sur **Avancé (Advanced)** dans l'angle inférieur droit.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.



- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par le DHCP du réseau invité.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau invité et les réseaux externes, comme Internet.
- **Serveur DNS 1 (DNS Server 1)** : serveur principal chargé de convertir les noms de domaine en adresses IP.
- **Serveur DNS 2 (DNS Server 2)** : serveur de secours utilisé pour résoudre les noms de domaine si le serveur principal échoue.
- **Serveur LPR (LPR Server)** : service Line Printer Remote qui gère les tâches d'impression et permet aux appareils réseau d'envoyer des demandes à des imprimantes distantes. Plusieurs ports LPR peuvent être configurés pour les imprimantes.

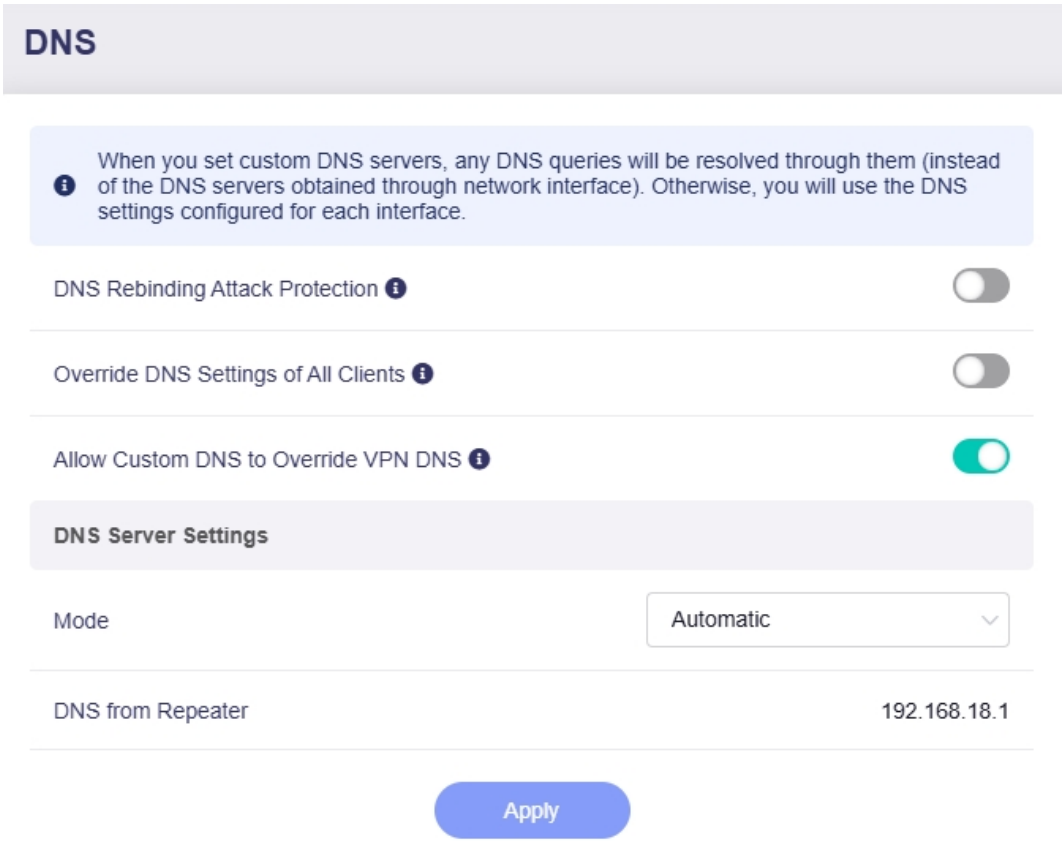
14.5 DNS

Le DNS (Domain Name System, système de noms de domaine) traduit les noms de domaine lisibles, comme www.google.com, en adresses IP afin que les appareils puissent trouver les sites Web et les services en ligne et s'y connecter.

Sur un routeur, les paramètres DNS déterminent généralement les serveurs DNS utilisés par les appareils connectés. Le routeur obtient le plus souvent leurs adresses automatiquement auprès du fournisseur d'accès à Internet ou du réseau amont. Vous pouvez aussi définir manuellement des serveurs DNS publics, comme 8.8.8.8, dans l'interface d'administration Web. Une fois configurés, ces paramètres sont généralement transmis automatiquement aux appareils connectés ; il n'est donc pas nécessaire de configurer le DNS sur chaque appareil.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **DNS**. Cette page permet de configurer les paramètres DNS.

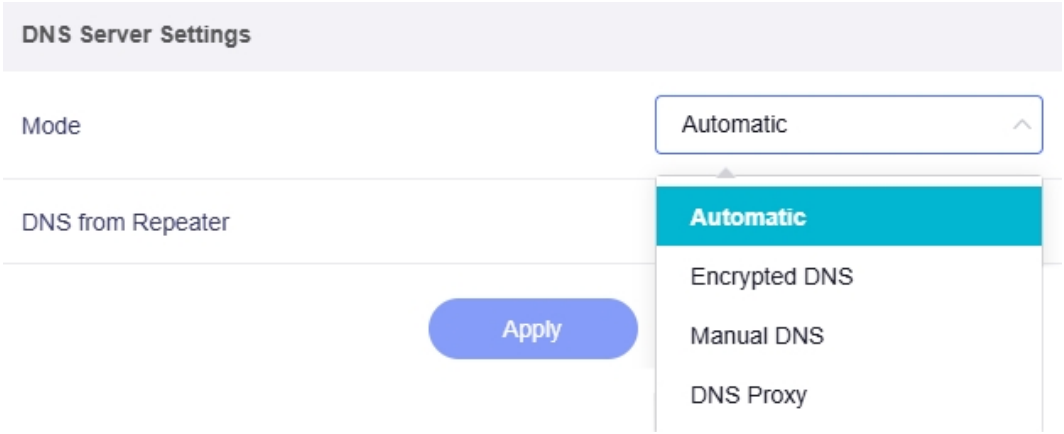
14.5.1 Paramètres généraux



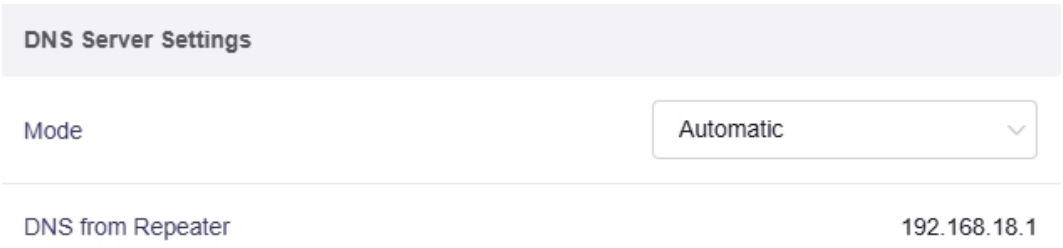
- **Protection contre le rebinding DNS (DNS Rebinding Attack Protection)** : bloque les tentatives malveillantes de résolution DNS. Elle peut toutefois empêcher certaines résolutions DNS privées. Désactivez-la si votre réseau utilise un portail captif, comme une page de connexion Wi-Fi publique.
- **Remplacer les paramètres DNS de tous les clients (Override DNS Settings of All Clients)** : impose les serveurs DNS du routeur à tous les appareils connectés, indépendamment de leurs propres réglages, pour une configuration DNS uniforme.
- **Autoriser le DNS personnalisé à remplacer le DNS VPN (Allow Custom DNS to Override VPN DNS)** : si un DNS personnalisé est défini, le trafic passant par le tunnel VPN l'utilise à la place du DNS de la connexion VPN. Vos règles DNS personnalisées restent ainsi applicables lorsque vous utilisez le VPN.

14.5.2 Paramètres du serveur DNS

Quatre modes sont proposés : Automatique, DNS chiffré, DNS manuel et Proxy DNS.

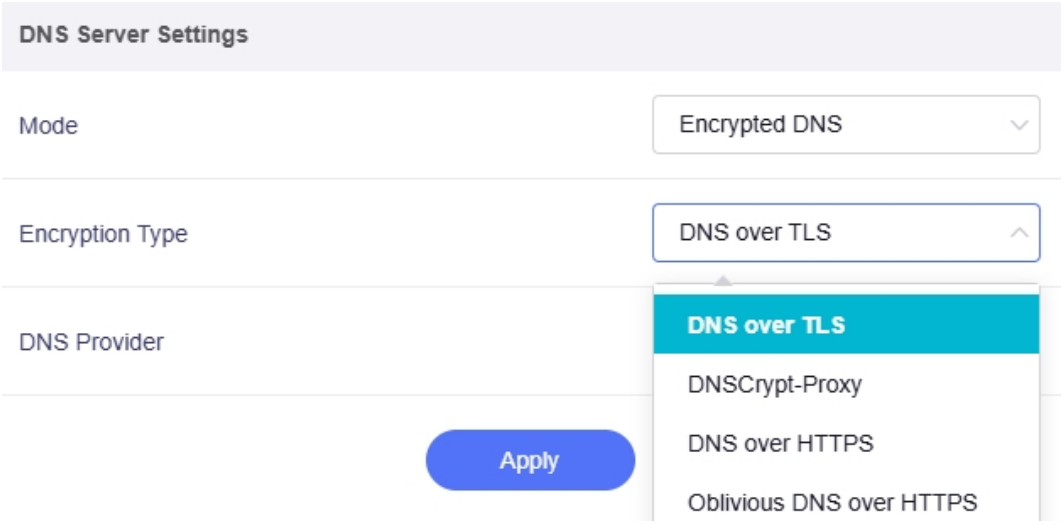


1. **Automatique (Automatic)** : le routeur obtient les adresses des serveurs DNS du réseau en amont et les applique à tous les appareils connectés.



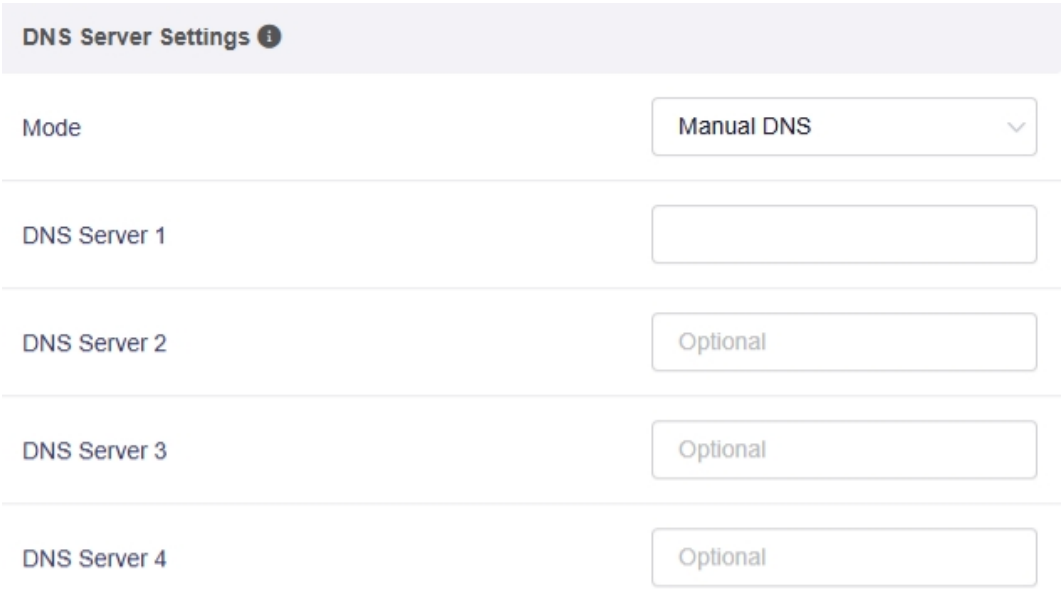
2. **DNS chiffré (Encrypted DNS)** : utilise des protocoles chiffrés pour traiter les requêtes DNS et protéger les données de résolution contre l'écoute et l'altération.

Quatre types de chiffrement sont proposés : DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS et Oblivious DNS over HTTPS.



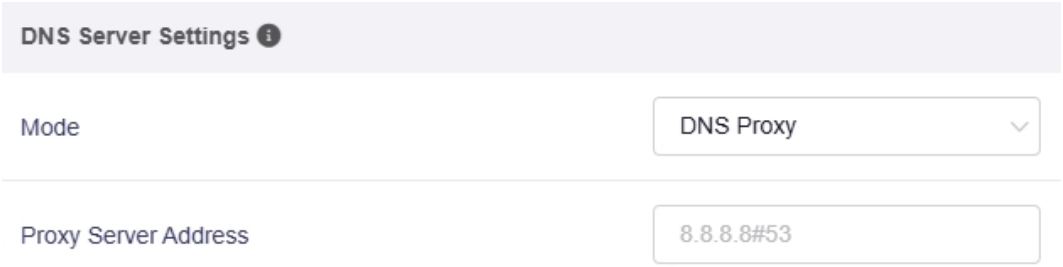
- Pour DNS over TLS, choisissez Control D, NextDNS ou Cloudflare comme fournisseur DNS.
- Pour les trois autres types, sélectionnez au moins un serveur DNS dans la liste, et jusqu'à huit serveurs. Si vous en sélectionnez plusieurs, le routeur utilise automatiquement le plus rapide.

3. **DNS manuel (Manual DNS)** : permet de personnaliser les serveurs DNS du routeur. Cliquez sur Serveur DNS 1 et choisissez un serveur dans la liste. Les autres champs DNS sont renseignés automatiquement.



Remarque : pour renseigner des adresses IPv6 dans le DNS manuel, activez d'abord IPv6 sur le routeur.

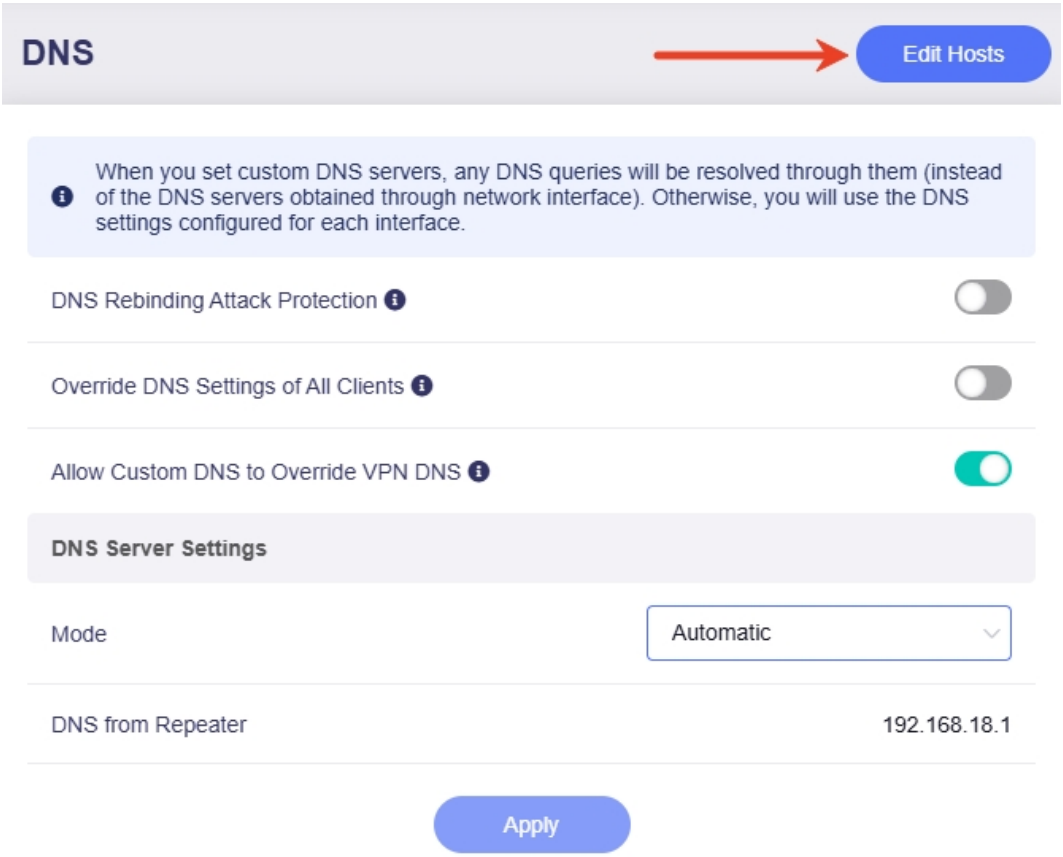
4. **Proxy DNS (DNS Proxy)** : transmet toutes les requêtes DNS par un serveur proxy et utilise son environnement réseau pour la résolution, selon vos besoins d'accès.



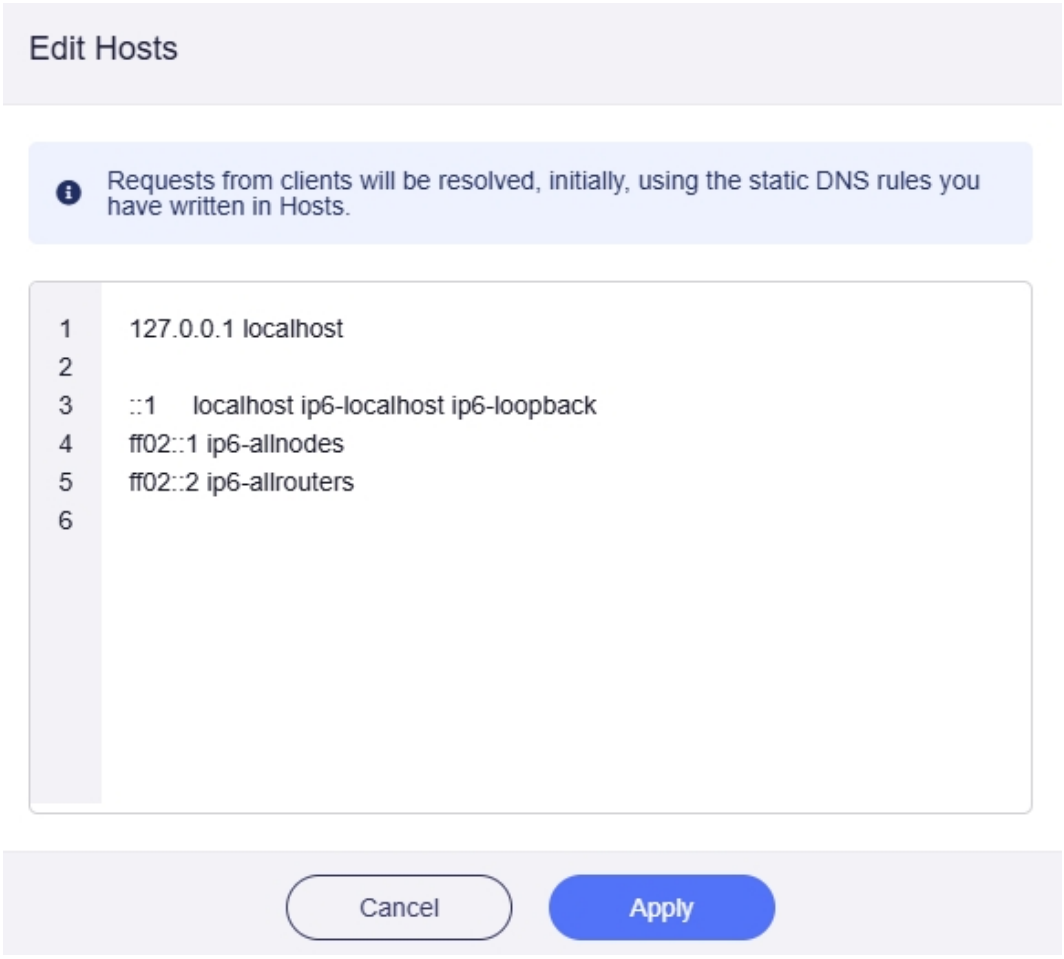
14.5.3 Modification du fichier hosts

Vous pouvez définir des règles statiques de résolution DNS.

Sur la page DNS, cliquez sur **Modifier hosts (Edit Hosts)** dans l'angle supérieur droit.



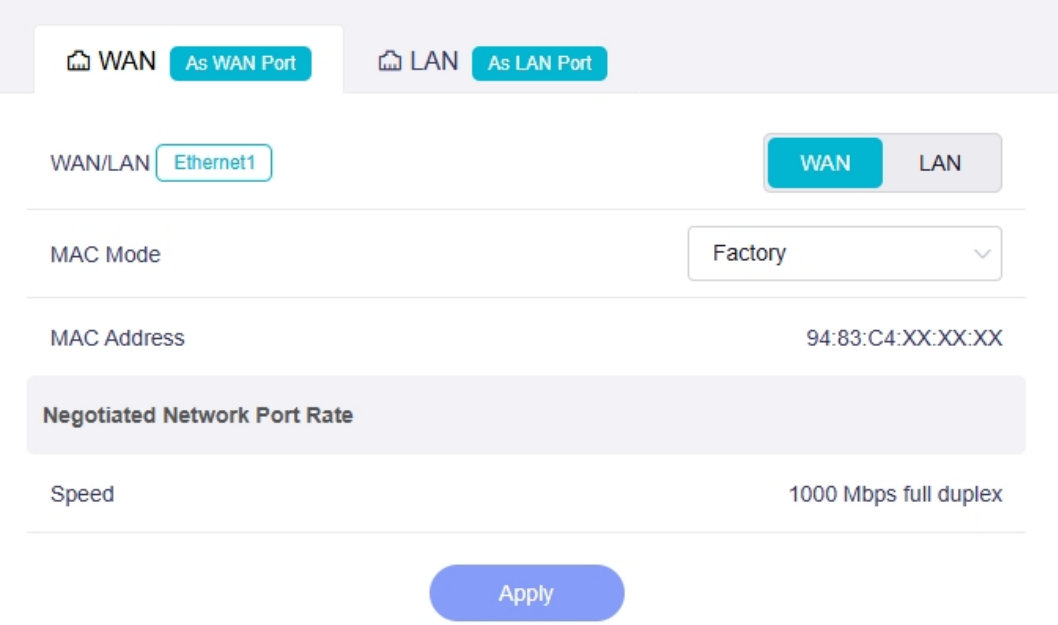
Les requêtes des clients sont résolues en priorité avec les règles statiques saisies ici. Vous pouvez associer manuellement des adresses IP à des noms d'hôtes, comme l'entrée de bouclage locale 127.0.0.1 localhost, pour personnaliser la résolution des noms.



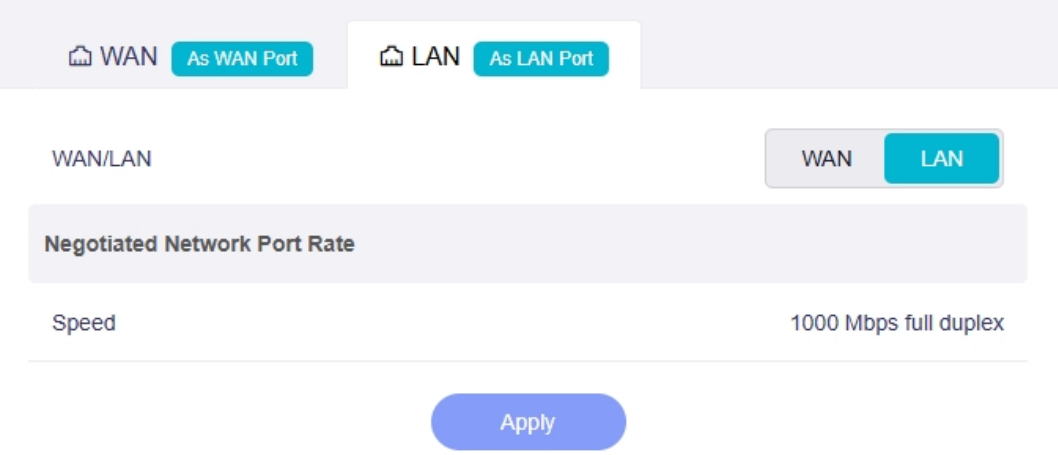
14.6 Ports Ethernet

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Ports Ethernet (Ethernet Port)** pour gérer les ports Ethernet du routeur.

La section **WAN** affiche le rôle du port, WAN ou LAN, son adresse MAC et le débit négocié.



La section **LAN** affiche le débit négocié du port LAN.

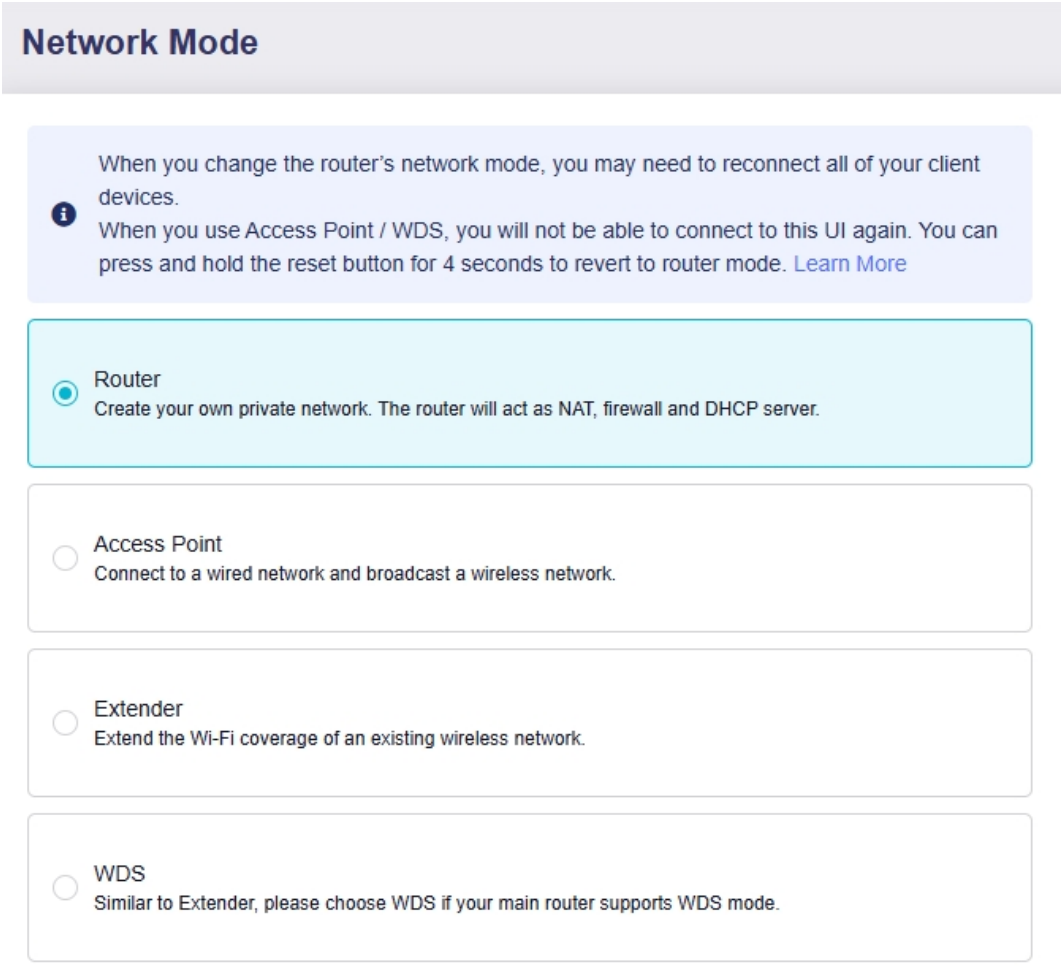


Remarque : le débit négocié des ports WAN et LAN ne s'affiche que lorsqu'un câble Ethernet est branché. Il dépend des capacités du port et du câble Ethernet.

14.7 Mode réseau

Le mode réseau définit le rôle et les fonctions du routeur selon vos besoins de déploiement.

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Mode réseau (Network Mode)** pour changer le mode du routeur.



- **Routeur (Router)** : mode par défaut de la plupart des routeurs domestiques et de petite entreprise. Il crée un réseau local privé et sert de passerelle entre Internet et les appareils connectés. Il active le NAT, le DHCP et le pare-feu intégré. Relié à une connexion en amont, comme la fibre, il attribue automatiquement des IP privées aux appareils et protège l'ensemble du réseau privé.
- **Point d'accès (Access Point)** : relie le routeur à un réseau filaire par câble LAN et diffuse un signal Wi-Fi pour étendre la couverture et connecter davantage d'appareils. Le NAT et le DHCP sont désactivés : le routeur fonctionne comme un point d'accès sans fil et un commutateur, sans servir de passerelle autonome.

- **Extenseur (Extender)** : étend la couverture d'un réseau Wi-Fi existant et réduit les zones sans signal. Le routeur reçoit les signaux du routeur principal sans fil, puis les retransmet. Aucune liaison filaire n'est nécessaire, contrairement au mode Point d'accès. La bande passante peut toutefois être divisée par deux, car l'appareil doit recevoir et transmettre simultanément.
- **WDS** : le mode Wireless Distribution System étend la couverture Wi-Fi sans fil, comme le mode Extenseur, mais permet aussi de créer des ponts sans fil entre plusieurs routeurs compatibles. Il est recommandé lorsque le routeur en amont prend en charge WDS.
  Ce mode convient aux bâtiments à plusieurs étages ou aux petits sites de bureaux où plusieurs routeurs doivent former un réseau Wi-Fi commun. Contrairement au mode Extenseur, qui relie un routeur principal à un seul extenseur, WDS permet à plusieurs routeurs interconnectés d'émettre et de recevoir les signaux pour assurer une couverture continue sur une zone plus vaste.

Remarque :

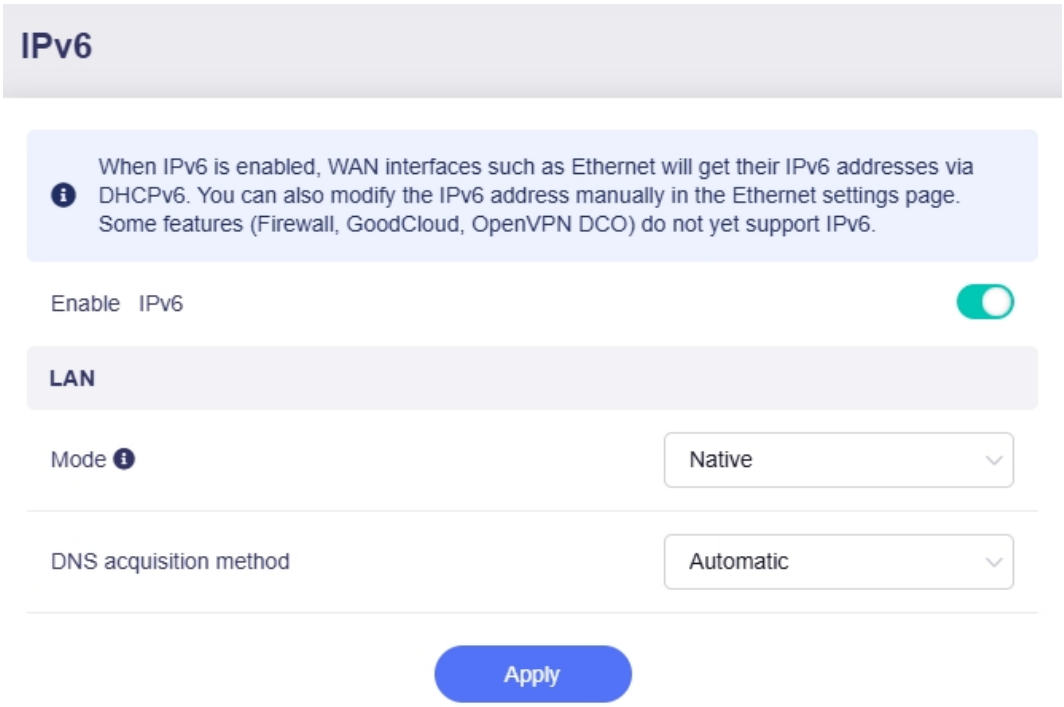
1. Après un changement de mode réseau, tous les appareils clients doivent se reconnecter au routeur pour assurer une connexion stable.
2. **En mode Point d'accès ou WDS, l'adresse IP initiale ne permet plus d'ouvrir l'interface Web**. Connectez-vous au routeur en amont pour trouver l'adresse IP qu'il a attribuée au routeur GL.iNet, puis utilisez cette adresse. Si vous ne pouvez pas accéder au routeur en amont, maintenez le bouton de réinitialisation enfoncé pendant 4 secondes pour rétablir le mode Routeur par défaut.
3. **En mode Point d'accès, Extenseur ou WDS, les fonctions suivantes sont indisponibles** : contrôle d'accès (listes d'autorisation et de blocage), AstroWarp, VPN, AdGuard Home, contrôle parental, ZeroTier, Tailscale, redirection de port, Multi-WAN, serveur DHCP, réservation d'adresses, réseau invité, DNS, port Ethernet, IPv6, passerelle transparente, IGMP Snooping, accélération réseau et paramètres NAT.

14.8 IPv6

IPv6 (Internet Protocol version 6) est la version la plus récente du protocole Internet, conçue pour remplacer IPv4. Son espace d'adressage beaucoup plus vaste répond à l'épuisement des adresses IPv4 et à la croissance mondiale du nombre d'appareils connectés.

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **IPv6** pour activer et configurer IPv6. Lorsqu'il est activé, les interfaces WAN, comme Ethernet, obtiennent leur adresse IPv6 via DHCPv6.

Activez **Activer IPv6 (Enable IPv6)**, choisissez le mode du réseau principal et la méthode d'obtention du DNS, puis cliquez sur **Appliquer (Apply).**



Remarque : certaines fonctions, comme le pare-feu, GoodCloud et OpenVPN DCO, ne prennent pas encore en charge IPv6. Leur activation simultanée avec IPv6 peut provoquer des problèmes de connexion.

14.8.1 Mode IPv6

Quatre modes sont disponibles : Natif, Passthrough, NAT6 et IPv6 statique.

- **Natif (Native)** : convient lorsque le routeur obtient directement une adresse IPv6 publique et attribue automatiquement des adresses IPv6 aux appareils connectés. Il répond aux besoins IPv6 de la plupart des utilisateurs.
- **Transmission directe (Passthrough)** : transmet les paquets IPv6 sans traitement ni conversion. Certaines applications ou certains services nécessitent de préserver intégralement les paquets pour les traiter ou les analyser. Ce mode est utilisé pour le dépannage réseau ou l'analyse de sécurité.
- **NAT6** : convient lorsque le routeur sert de passerelle et attribue des adresses IPv6 internes dynamiques aux appareils du réseau. Les terminaux se connectent par un terminal de réseau optique (ONT) et obtiennent une adresse IPv6 du réseau local.
- **IPv6 statique (Static IPv6)** : convient aux appareils ou services nécessitant une adresse IPv6 fixe, comme les serveurs ou les imprimantes réseau. L'adresse reste identique, ce qui facilite la gestion et l'accès.

14.8.2 Méthode d'obtention du DNS

Ce paramètre détermine comment le routeur obtient les adresses des serveurs DNS IPv6. Deux options sont disponibles : Automatique et Manuelle.

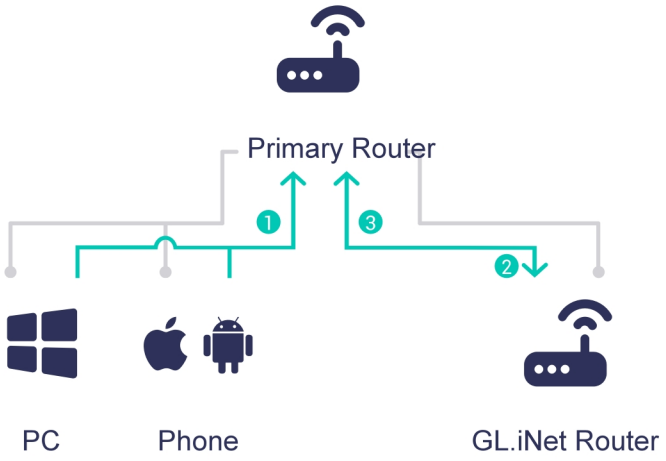
- **Automatique (Automatic)** : le routeur obtient les adresses DNS IPv6 dynamiquement, par exemple via DHCPv6.
- **Manuelle (Manual)** : saisissez les adresses des serveurs DNS IPv6 souhaités. Une configuration manuelle incorrecte peut empêcher la résolution des noms de domaine en adresses IP. Utilisez-la avec prudence.

14.9 Passerelle transparente

La passerelle transparente (Drop-in Gateway) enrichit les fonctions d'un routeur principal existant sans le remplacer ni le reconfigurer. Reliez le routeur GL.iNet au routeur principal avec un câble Ethernet pour ajouter des fonctions avancées au réseau existant, par exemple :

- Filtrer les publicités avec AdGuard Home
- Activer un client VPN
- Utiliser un DNS chiffré

La passerelle transparente agit comme un intermédiaire : le trafic des clients passe par le routeur GL.iNet pour être traité avant d'être transmis via le routeur principal. Les paramètres réseau existants sont conservés pour maintenir la connexion de tous les appareils. Vous pouvez gérer le trafic de tous les clients ou de certains clients seulement.



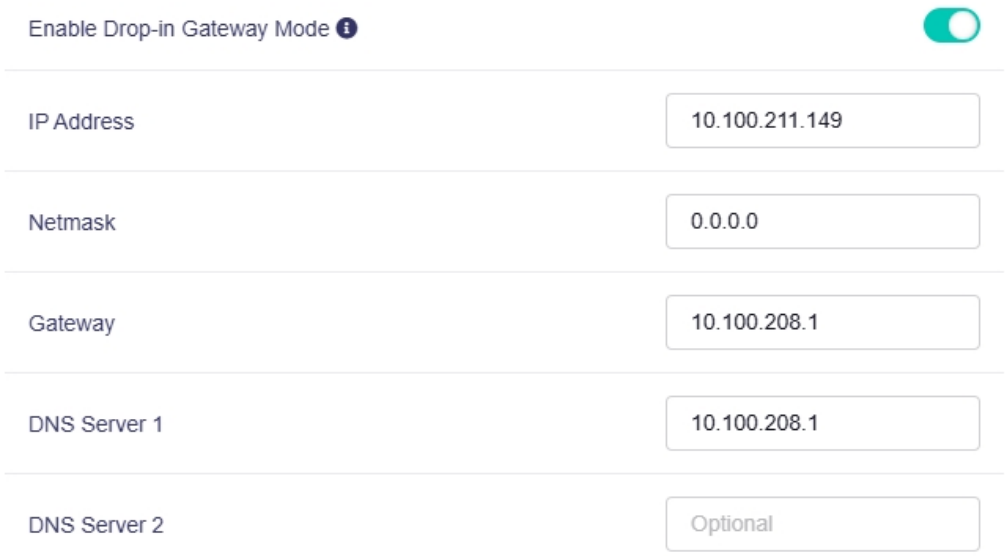
Le schéma ci-dessus comporte des lignes grises et des lignes vertes munies de trois flèches numérotées.

- **Les lignes grises** représentent les branchements physiques : les clients, comme les ordinateurs, sont connectés au routeur principal. Un câble Ethernet relie le port LAN du routeur principal au port WAN du routeur GL.iNet, sur lequel la passerelle transparente est activée.
- **Les lignes vertes** représentent le parcours des données lorsque la passerelle transparente est active. Les flèches numérotées indiquent l'ordre de circulation :

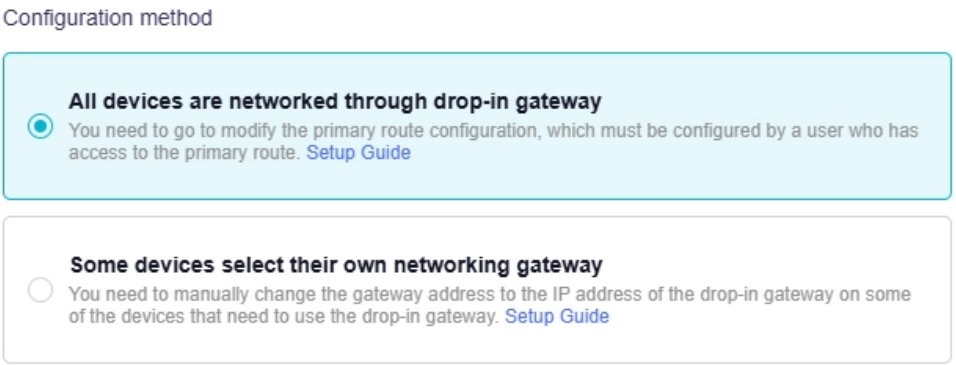
1. Le trafic des appareils clients est d'abord transmis au routeur principal.
2. Le routeur principal l'envoie au routeur GL.iNet pour traitement, par exemple le filtrage publicitaire ou le chiffrement VPN.
3. Après traitement, le trafic retourne au routeur principal, qui remet les données aux clients d'origine ou les achemine vers Internet.

Suivez les étapes ci-dessous pour activer la passerelle transparente si nécessaire.

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Passerelle transparente (Drop-in Gateway)**. Activez **Activer le mode passerelle transparente (Enable Drop-in Gateway Mode)**, puis confirmez les paramètres réseau.



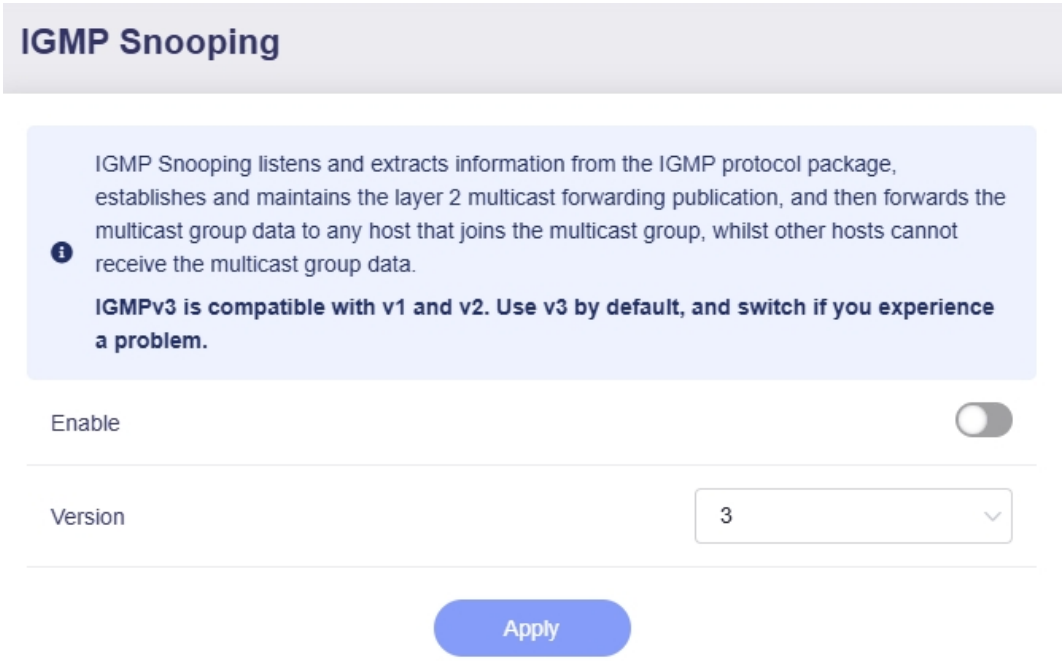
2. Choisissez la méthode de configuration, puis cliquez sur **Appliquer (Apply)**. Consultez ce tutoriel pour en savoir plus.



14.10 IGMP Snooping

IGMP Snooping analyse les paquets IGMP, en extrait les informations et crée puis maintient une table de transfert multicast de couche 2. Les données multicast sont ensuite transmises uniquement aux hôtes ayant rejoint le groupe correspondant.

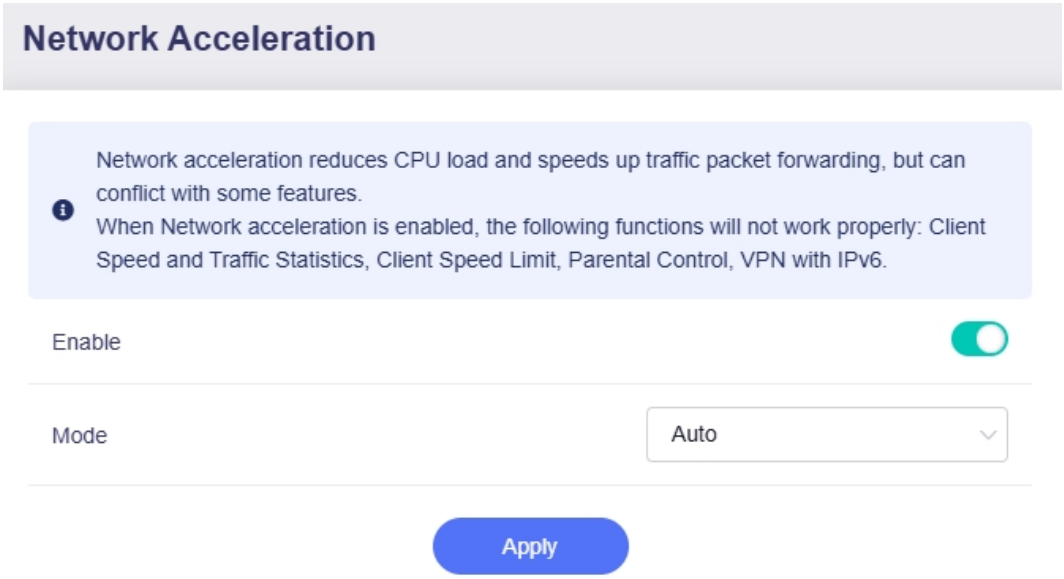
Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **IGMP Snooping**. Activez cette fonction si vous souhaitez utiliser le multicast sur le routeur.



14.11 Accélération réseau

L’accélération réseau réduit la charge du processeur et accélère le transfert des paquets, mais peut entrer en conflit avec certaines fonctions.

Connectez-vous à l’interface d’administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Accélération réseau (Network Acceleration)**. Cette page permet d’activer l’accélération réseau et de choisir le mode Automatique, Accélération matérielle ou Accélération logicielle.

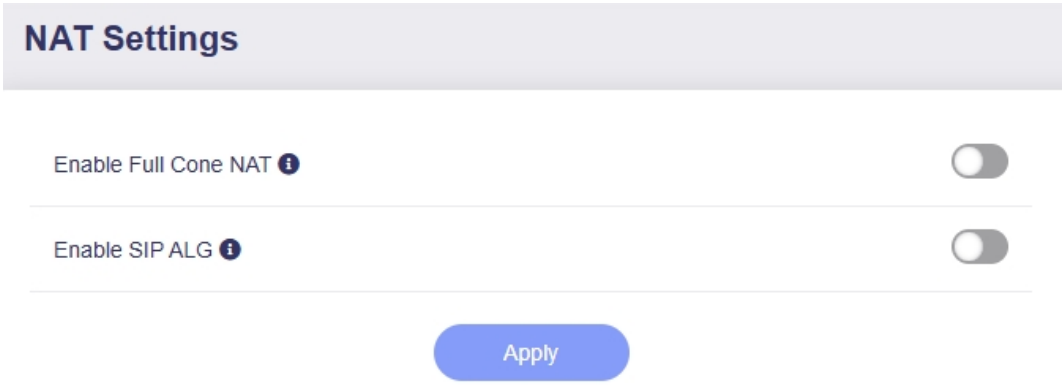


- **Automatique (Auto)** : bascule automatiquement entre les deux modes d’accélération selon l’utilisation réelle.
- **Accélération matérielle (Hardware Acceleration)** : confie les tâches réseau fréquentes, comme le NAT, le transfert de paquets et la vérification des sommes de contrôle, à du matériel dédié, tel qu’un NPU ou une puce HWNAT. Elle fonctionne sur les connexions Ethernet et Répéteur. Avec leurs chemins fixes et leurs règles simples, elle assure un débit élevé, une faible latence et une charge minimale du processeur, pour transmettre les données au débit maximal de la liaison.
- **Accélération logicielle (Software Acceleration)** : utilise le processeur principal du routeur avec un noyau ou des pilotes optimisés, comme SWNAT. Elle fonctionne sur les connexions cellulaires 4G/5G, où l’accélération matérielle est généralement indisponible, et offre une bonne compatibilité avec les protocoles complexes. Malgré sa souplesse, elle peut atteindre les limites du processeur lorsque le débit est élevé, notamment avec des fonctions avancées.

Remarque : lorsque l'accélération réseau est activée, les fonctions suivantes ne fonctionnent pas correctement : statistiques de débit des clients, statistiques de trafic, limitation du débit, contrôle parental et VPN avec IPv6.

14.12 Paramètres NAT

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Paramètres NAT (NAT Settings)**. Deux fonctions sont proposées : Full Cone NAT et SIP ALG.



- **Full Cone NAT** : peut réduire la latence et améliorer la réactivité des jeux en ligne. Son activation peut toutefois diminuer la sécurité, car elle autorise les connexions entrantes sans restriction.
- **SIP ALG** : vise à limiter les effets de plusieurs NAT sur le trafic SIP (Session Initiation Protocol). Dans la plupart des cas, cette fonction n'apporte pas d'amélioration et peut perturber les appels VoIP : son dans un seul sens, absence de sonnerie, coupures inattendues ou renvoi direct vers la messagerie vocale.

Chapitre 15

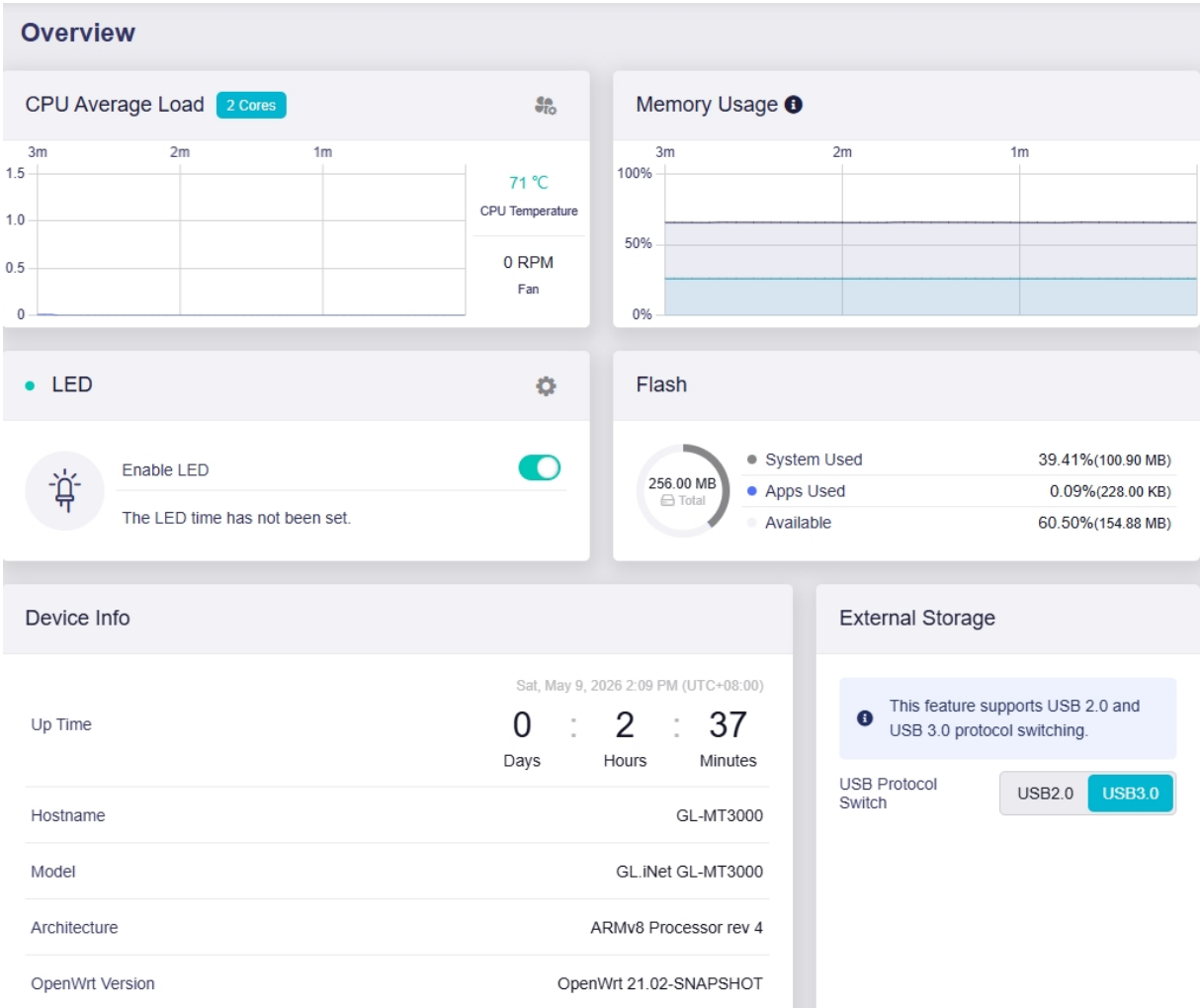
Système

Ce chapitre présente les outils de gestion de l’appareil : vue d’ensemble, mises à jour, tâches planifiées, fuseau horaire, journaux, réinitialisation du micrologiciel et paramètres avancés.

15.1 Vue d’ensemble

Dans l’interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Vue d’ensemble (Overview)**. Cette page affiche l’état du matériel et propose des commandes simples :

- État du processeur, de la mémoire et de la mémoire flash
- Commande du voyant LED
- Informations sur l’appareil
- Sélection du protocole de stockage externe

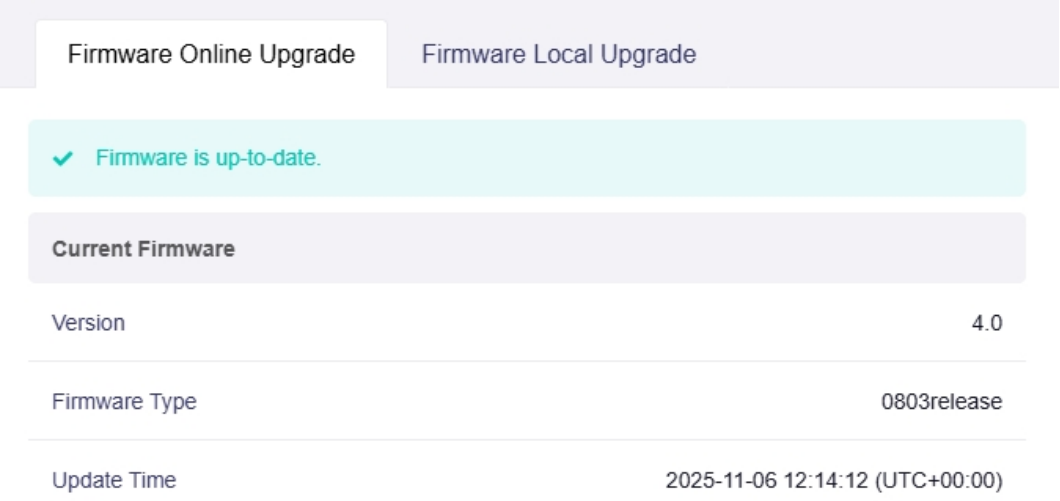


15.2 Mise à jour

Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Mise à jour (Upgrade)**. Vous pouvez mettre à jour le micrologiciel en ligne ou depuis un fichier local.

15.2.1 Mise à jour en ligne du micrologiciel

Cette page présente la version du micrologiciel, son type, par exemple stable ou bêta, et la date de mise à jour. Si le routeur est connecté à Internet, il recherche une version plus récente à télécharger.

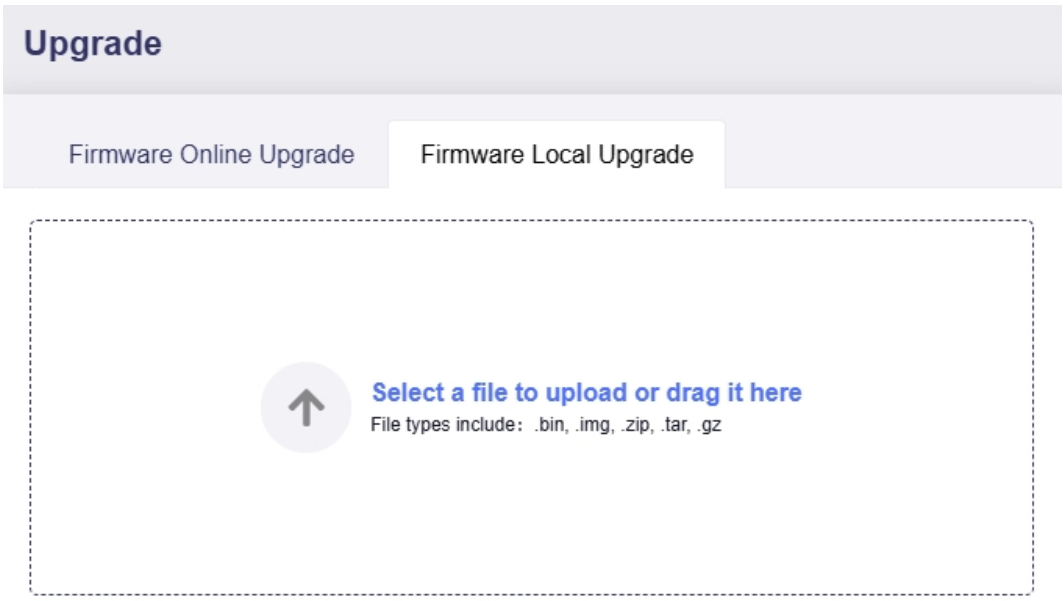


Conseil : si la mise à jour en ligne affiche **Échec du téléchargement (Download Failed)**, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)** et corrigez l'heure en la synchronisant avec le navigateur.

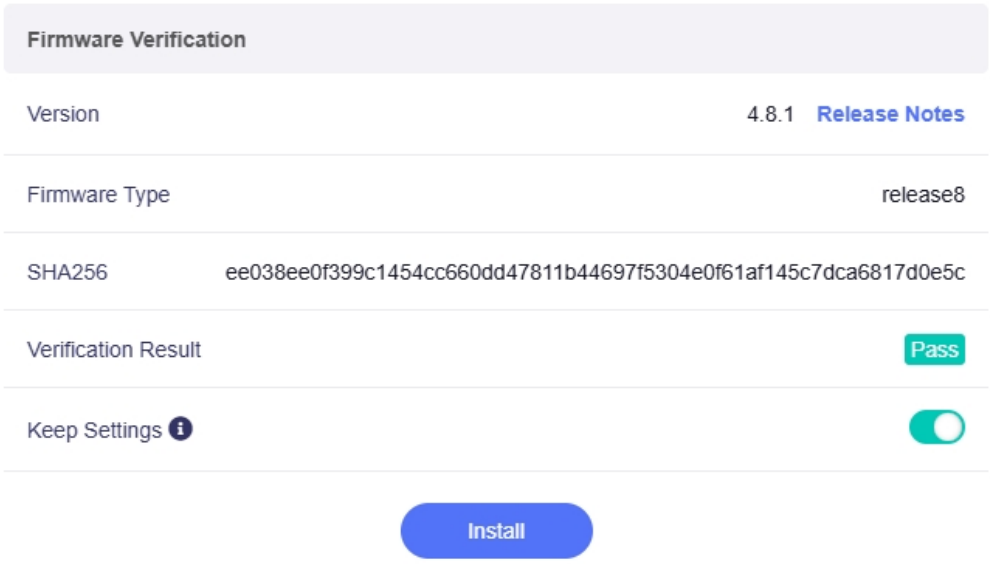
15.2.2 Mise à jour locale du micrologiciel

La mise à jour locale ne nécessite pas de connexion Internet sur le routeur.

Téléchargez le micrologiciel correspondant au modèle du routeur depuis le Centre de téléchargement (Download Center) officiel sur votre appareil. Dans l'interface Web du routeur, ouvrez **SYSTÈME (SYSTEM)** > **Mise à jour (Upgrade)** > **section Mise à jour locale (Local Upgrade)**, puis importez le fichier.



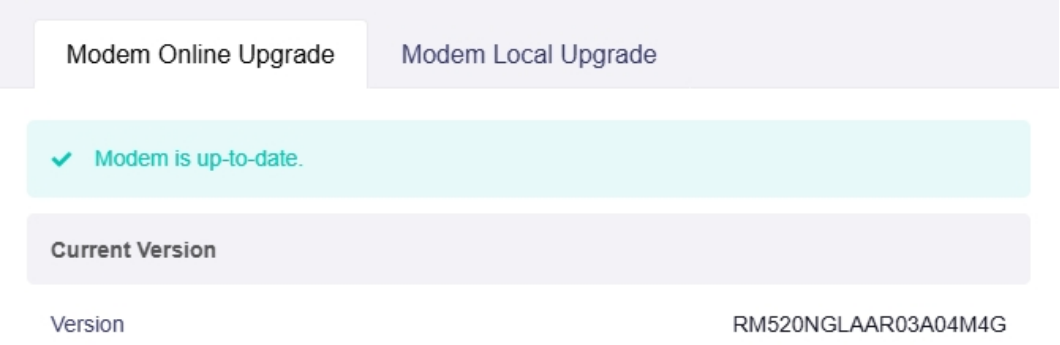
Vérifiez les informations du micrologiciel affichées avant de cliquer sur **Installer (Install)**.



- **Conserver les paramètres (Keep Settings)** : conserve vos réglages actuels. Les paquets installés manuellement doivent toutefois être réinstallés après la mise à jour. Désactivez cette option lorsque vous installez une version antérieure.

15.2.3 Mise à jour en ligne du modem

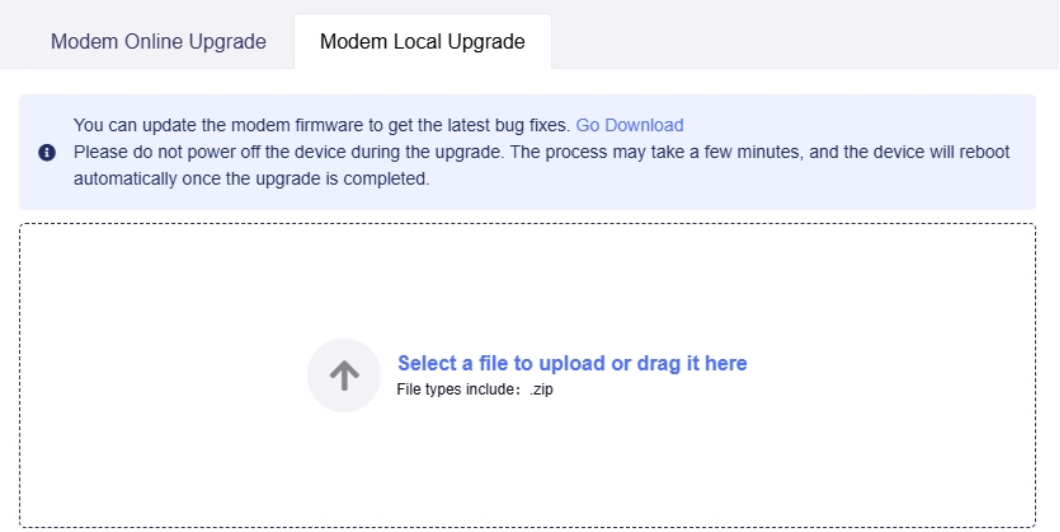
Les routeurs cellulaires GL.iNet permettent de consulter et de mettre à jour le micrologiciel du modem cellulaire depuis l'interface d'administration Web.
La version actuelle du modem cellulaire s'affiche ici. Si le routeur est connecté à Internet, il recherche automatiquement la dernière version sur le serveur du fabricant pour faciliter la mise à jour.



15.2.4 Mise à jour locale du modem

Vous pouvez essayer de mettre à jour le module cellulaire en cas d'échec ou d'instabilité de la connexion cellulaire. Nous recommandons de contacter l'assistance technique pour diagnostiquer le problème avant d'effectuer cette mise à jour.

Si nécessaire, importez manuellement un fichier de micrologiciel pour mettre à jour le modem cellulaire.



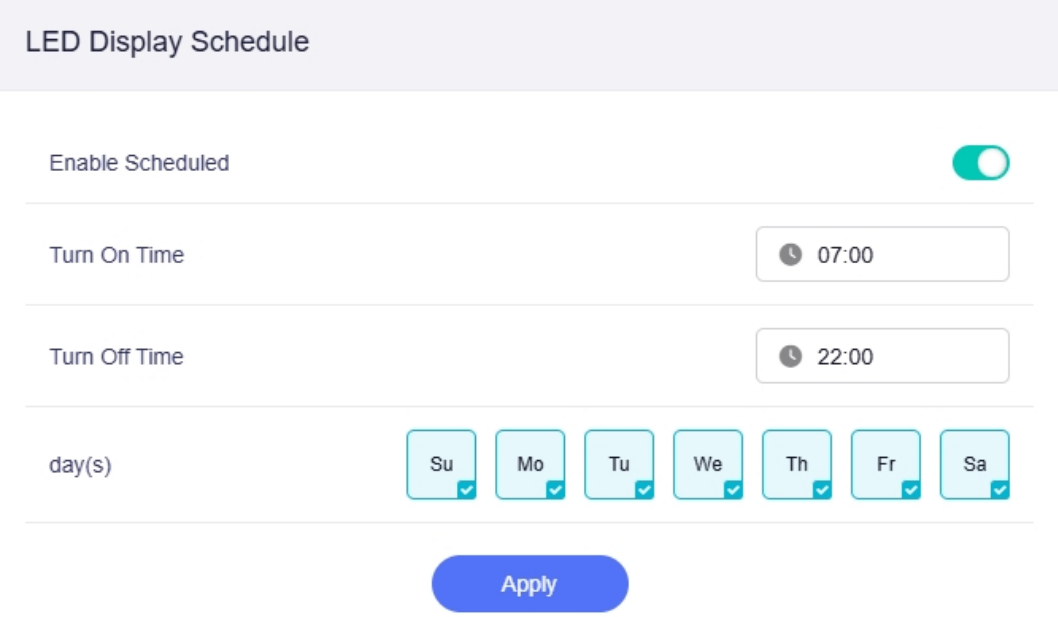
15.3 Tâches planifiées

Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Tâches planifiées (Scheduled Tasks)**. Cette page permet de planifier des actions quotidiennes, comme l'allumage et l'extinction du voyant ou le redémarrage du routeur.

Remarque : synchronisez l'heure dans la section Fuseau horaire (Time Zone) avant d'utiliser cette fonction. Si l'appareil est éteint à l'heure prévue, la tâche n'est pas exécutée.

15.3.1 Programmation du voyant LED

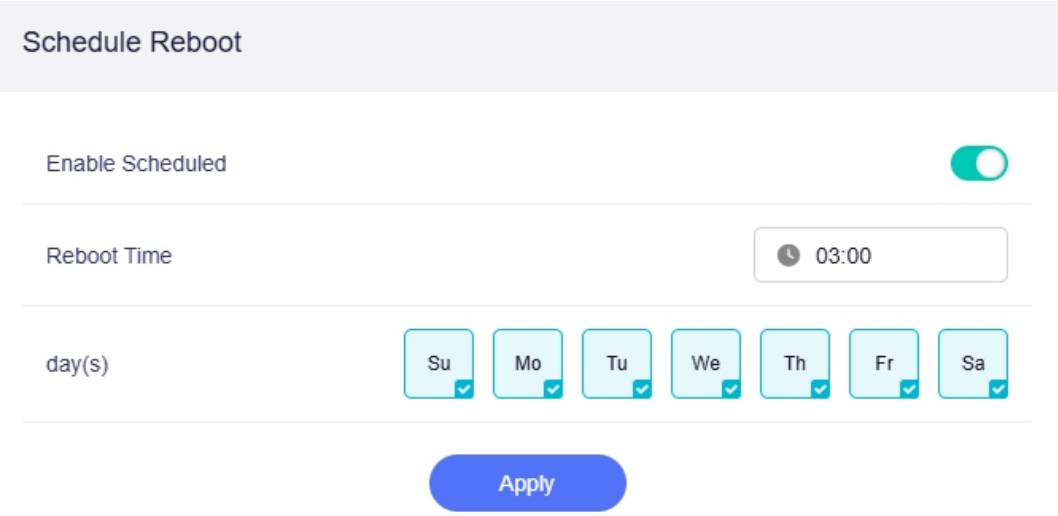
Définissez le planning du voyant si nécessaire, puis cliquez sur **Appliquer (Apply)**.



- **Activer la programmation (Enable Scheduled)** : active le planning du voyant.
- **Heure d’allumage (Turn On Time)** : heure d’allumage du voyant, par exemple 07:00.
- **Heure d’extinction (Turn Off Time)** : heure d’extinction du voyant, par exemple 22:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

15.3.2 Redémarrage planifié

Définissez le planning de redémarrage automatique, puis cliquez sur **Appliquer (Apply)**.



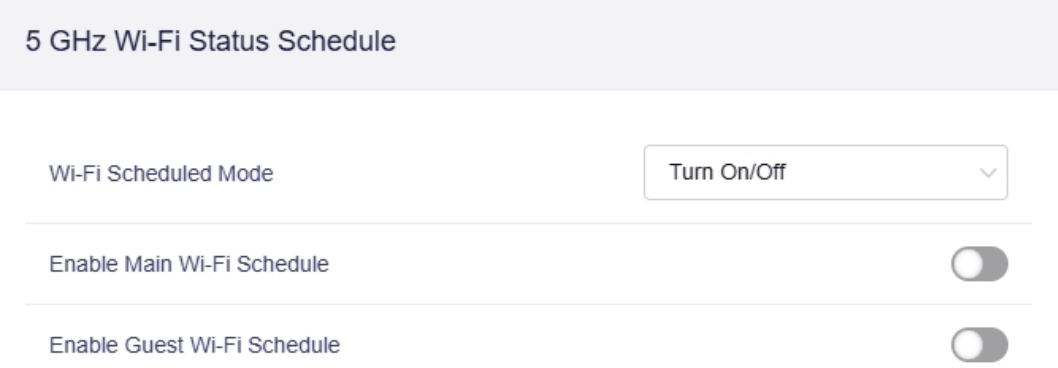
- **Activer la programmation (Enable Scheduled)** : active le redémarrage planifié.
- **Heure de redémarrage (Reboot Time)** : heure à laquelle le routeur redémarre, par exemple 03:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

15.3.3 Programmation du Wi-Fi 5 GHz

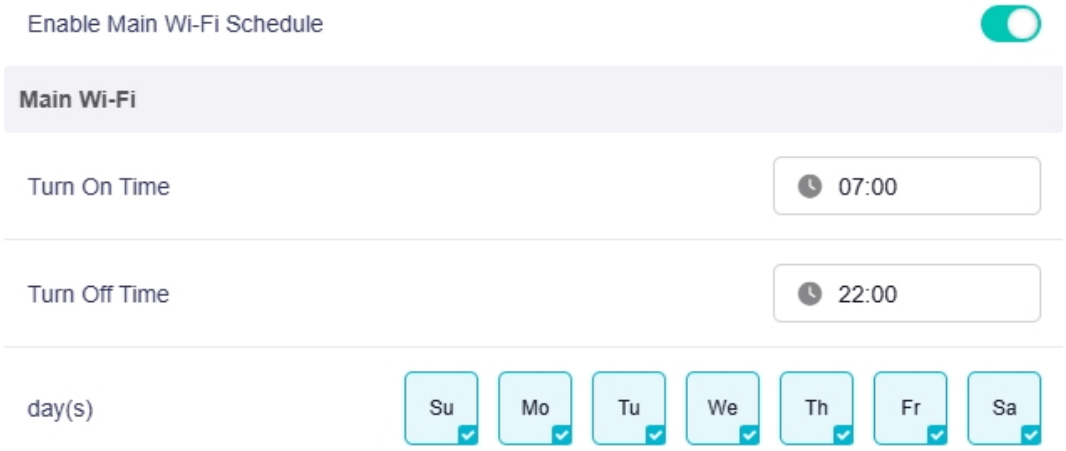
Cette fonction permet de programmer le Wi-Fi 5 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

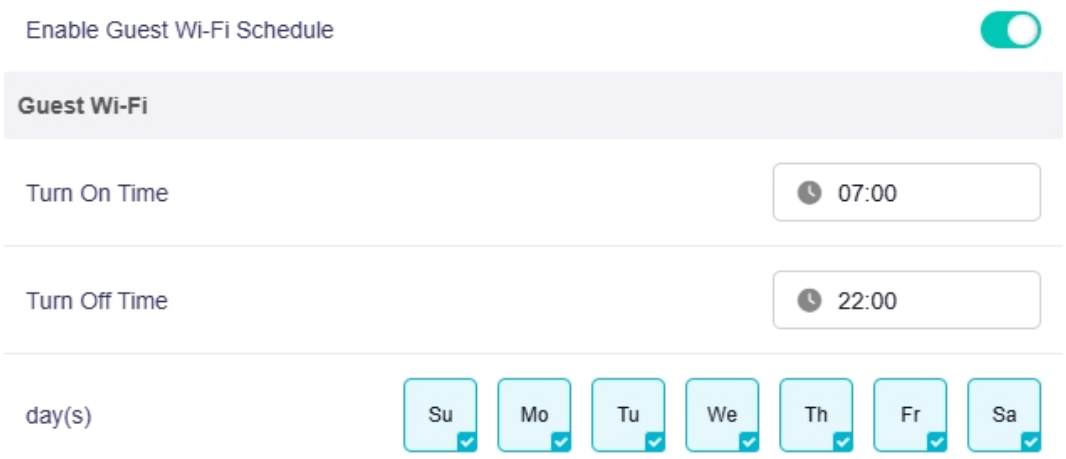
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 5 GHz.



- **Programmation du Wi-Fi principal (Main Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau principal 5 GHz et les jours concernés.

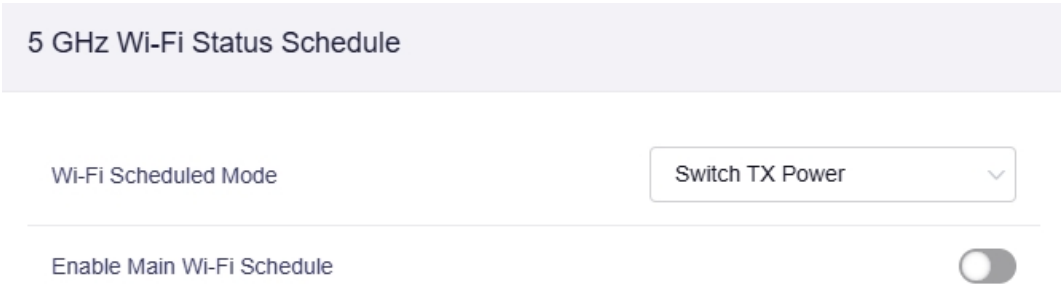


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 5 GHz et les jours concernés.

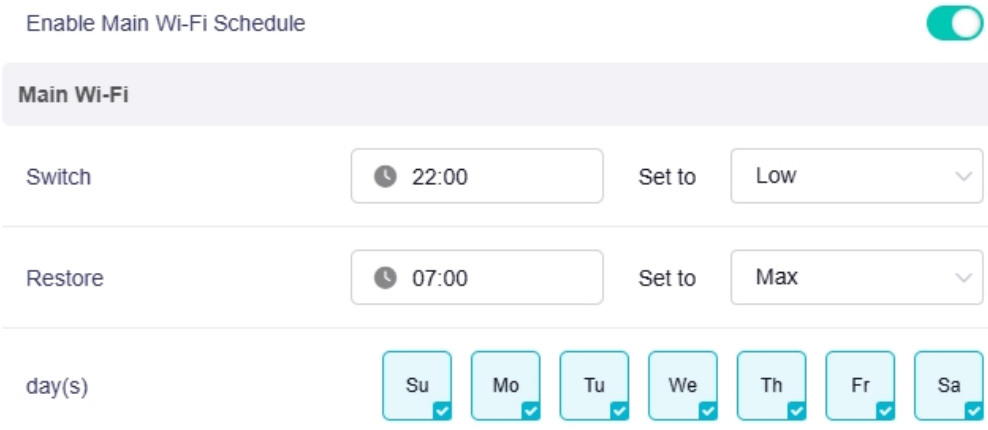


Mode 2 : Modifier la puissance d’émission

Vous pouvez programmer les changements de puissance d’émission du réseau principal 5 GHz.



Une fois cette fonction activée, définissez deux actions horaires pour modifier la puissance du Wi-Fi principal 5 GHz, puis choisissez les jours concernés.



- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.

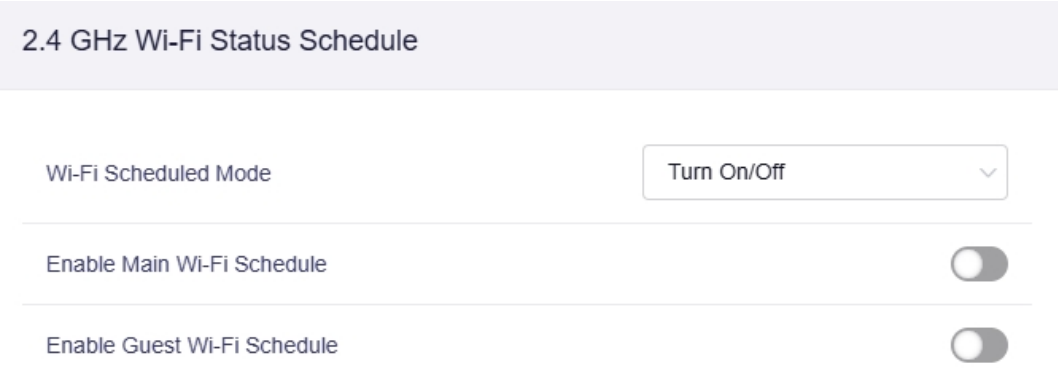
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

15.3.4 Programmation du Wi-Fi 2,4 GHz

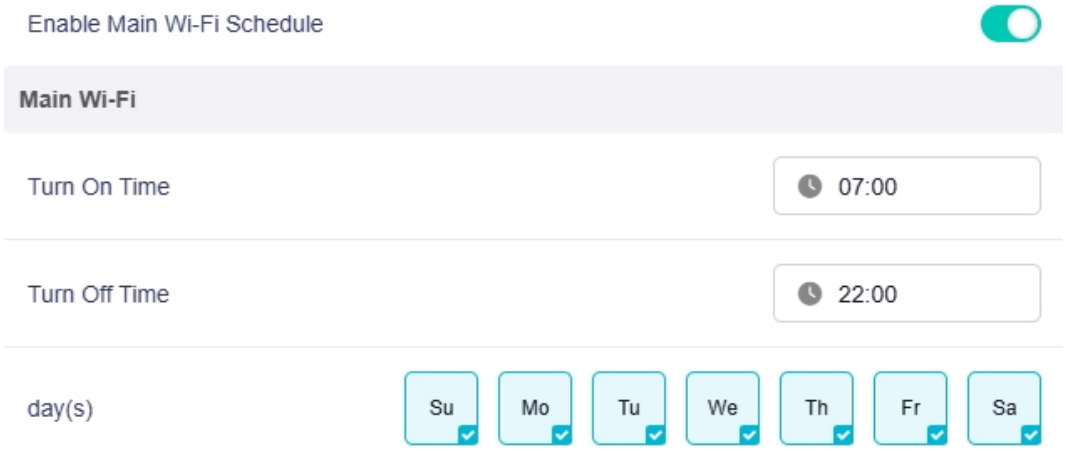
Cette fonction permet de programmer le Wi-Fi 2,4 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

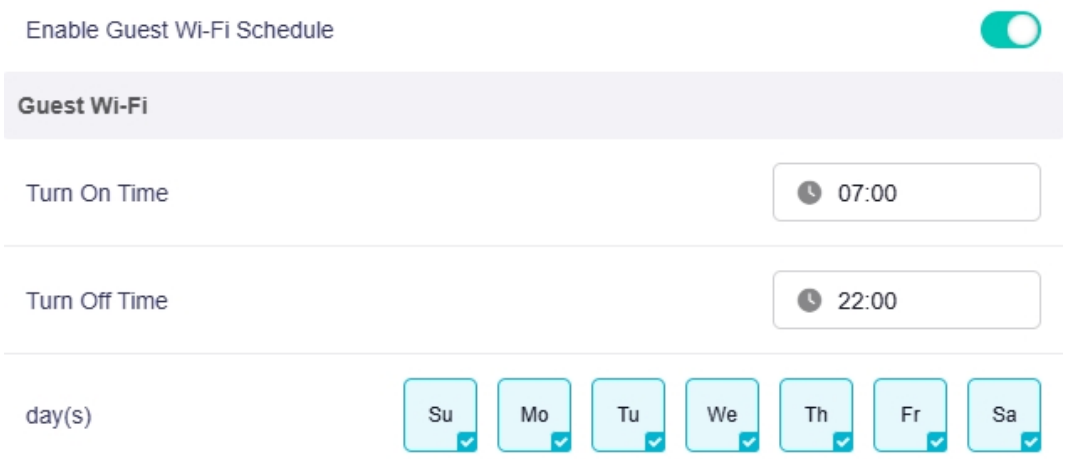
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 2,4 GHz.



- **Programmation du Wi-Fi principal (Main Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau principal 2,4 GHz et les jours concernés.

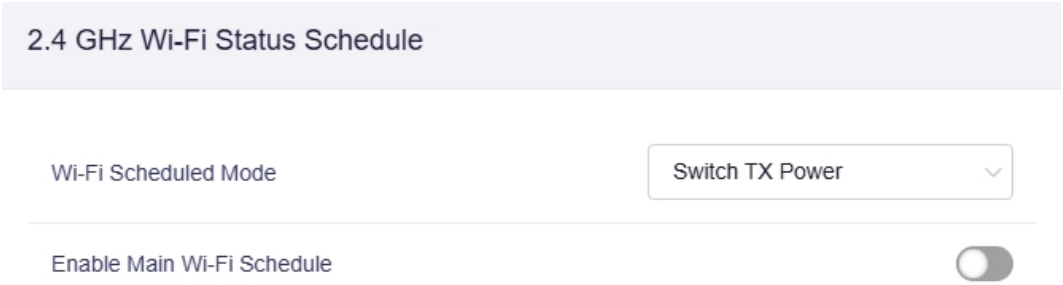


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 2,4 GHz et les jours concernés.

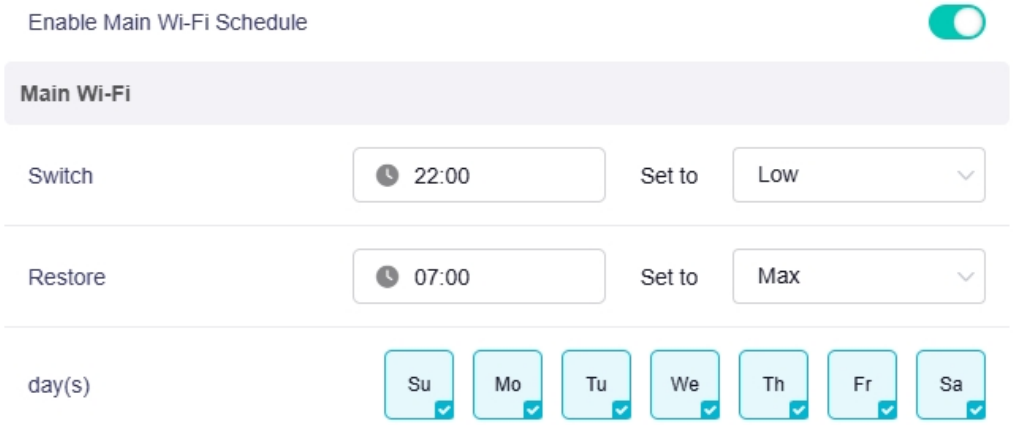


Mode 2 : Modifier la puissance d'émission

Vous pouvez programmer les changements de puissance d'émission du réseau principal 2,4 GHz.



Une fois cette fonction activée, définissez deux actions horaires pour modifier la puissance du Wi-Fi principal 2,4 GHz, puis choisissez les jours concernés.

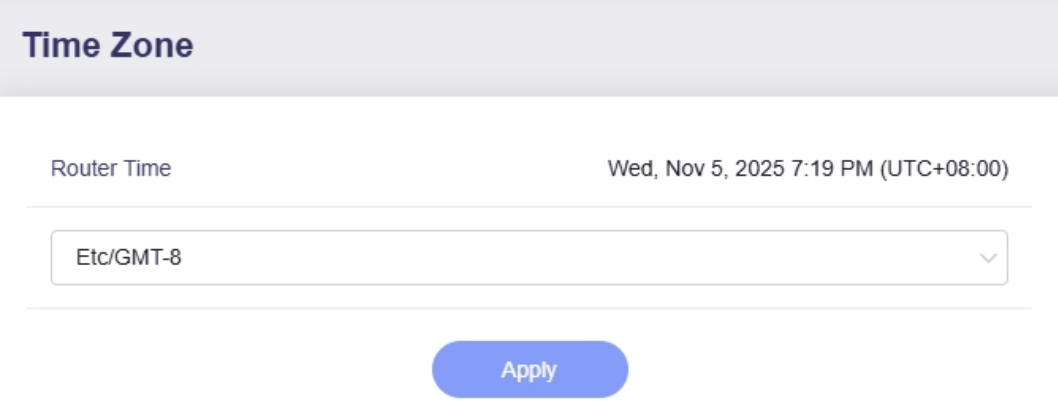


- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.

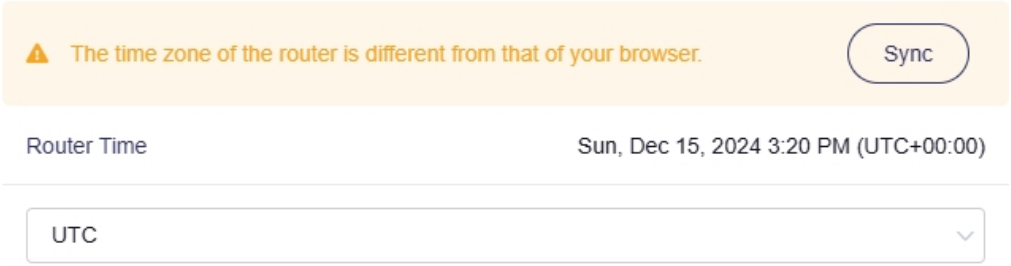
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

15.4 Fuseau horaire

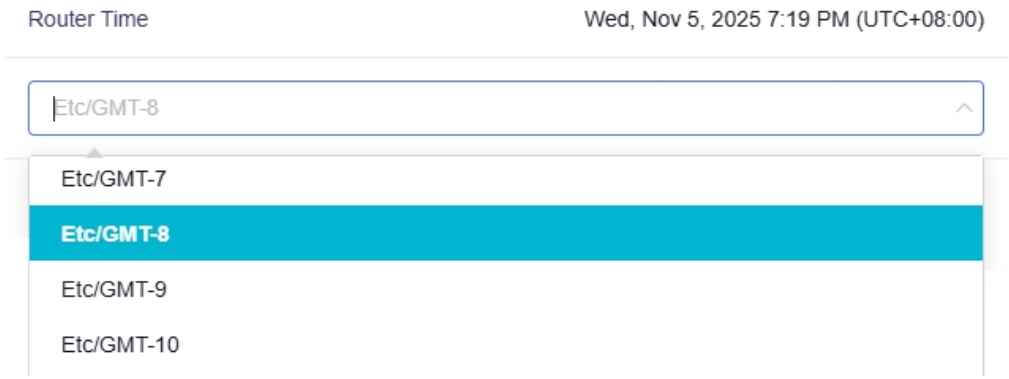
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)**. La page affiche la date et l'heure système du routeur ainsi que le décalage du fuseau horaire.



Certaines fonctions dépendent de l'heure système. Vérifiez que le fuseau horaire est correctement synchronisé. S'il diffère de celui du navigateur, un message s'affiche. Cliquez sur **Synchroniser (Sync)** pour les aligner.

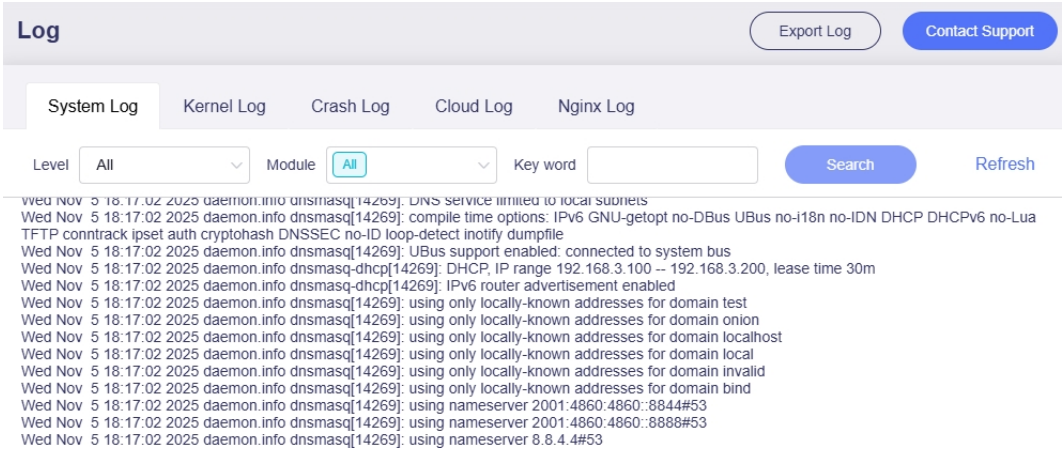


Pour changer de fuseau, sélectionnez celui qui convient dans la liste afin que l'heure du routeur corresponde à l'heure locale.

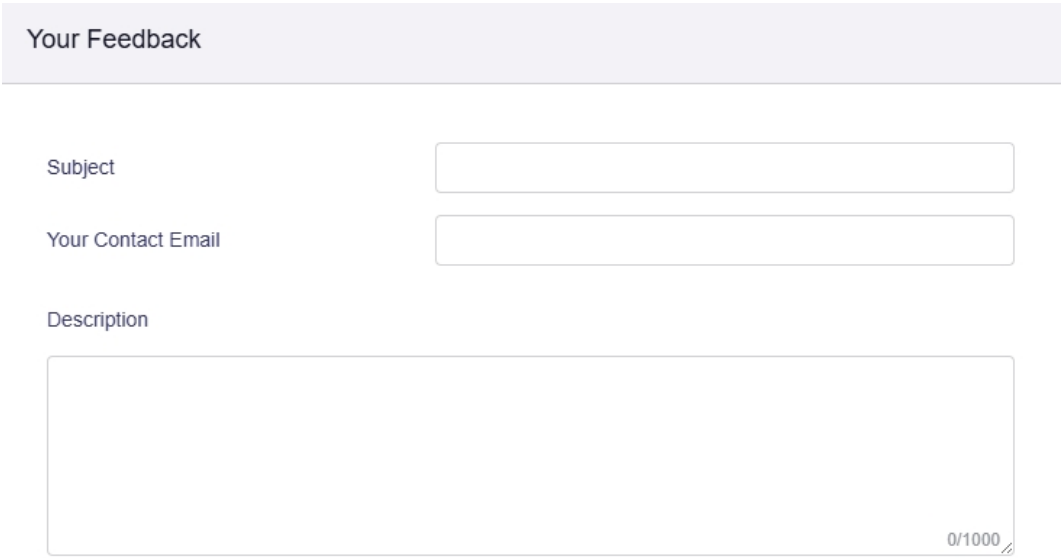

Router Time
Wed, Nov 5, 2025 7:19 PM (UTC+08:00)
Etc/GMT-8
Etc/GMT-7
Etc/GMT-8
Etc/GMT-9
Etc/GMT-10

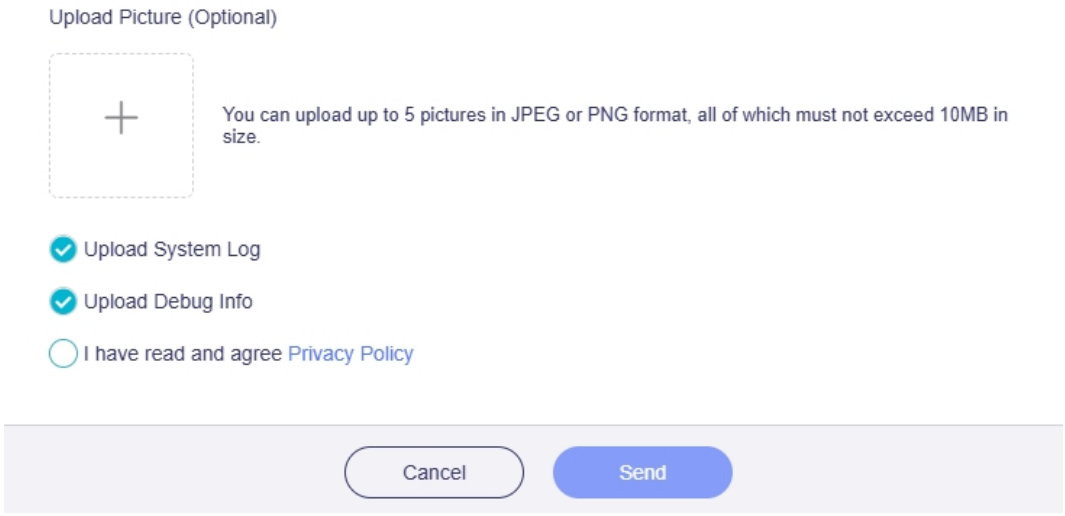
15.5 Journaux

Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Journal (Log)**. Vous pouvez consulter les journaux Système, Noyau, Plantage, Cloud et Nginx pour l'analyse et le dépannage.



- **Recherche (Search)** : filtrez rapidement le journal système par niveau, par exemple Tous, Informations ou Erreur, ou par module, comme IPv6, Partage de connexion ou Cellulaire. Vous pouvez aussi saisir des mots-clés.
- **Actualiser (Refresh)** : met à jour les journaux.
- **Exporter le journal (Export Log)** : exporte les journaux et les informations de débogage.
- **Contacter l'assistance (Contact Support)** : cliquez sur ce bouton, renseignez les détails dans la fenêtre à droite, puis cliquez sur **Envoyer (Send)**. Votre message est transmis directement à l'assistance technique GL.iNet.




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

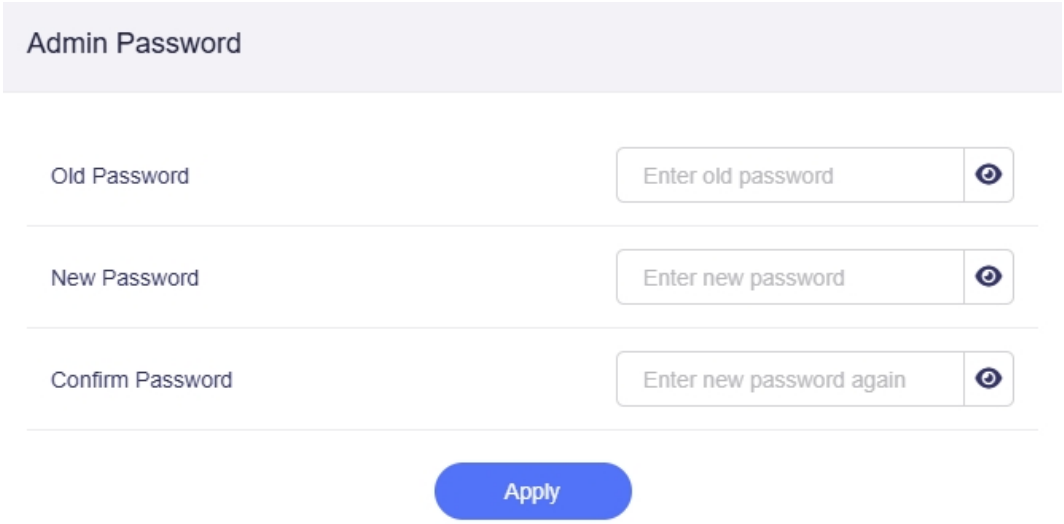
15.6 Sécurité

Dans l'interface d'administration Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)**. Cette page propose les paramètres d'administration locale et distante suivants :

- Mot de passe administrateur
- Accès local à l'interface Web, à LuCI et à SSH
- Accès HTTPS/SSH à distance
- Ouverture de ports sur le routeur

15.6.1 Mot de passe administrateur

Cette section permet de modifier le mot de passe de connexion à l'interface d'administration Web.

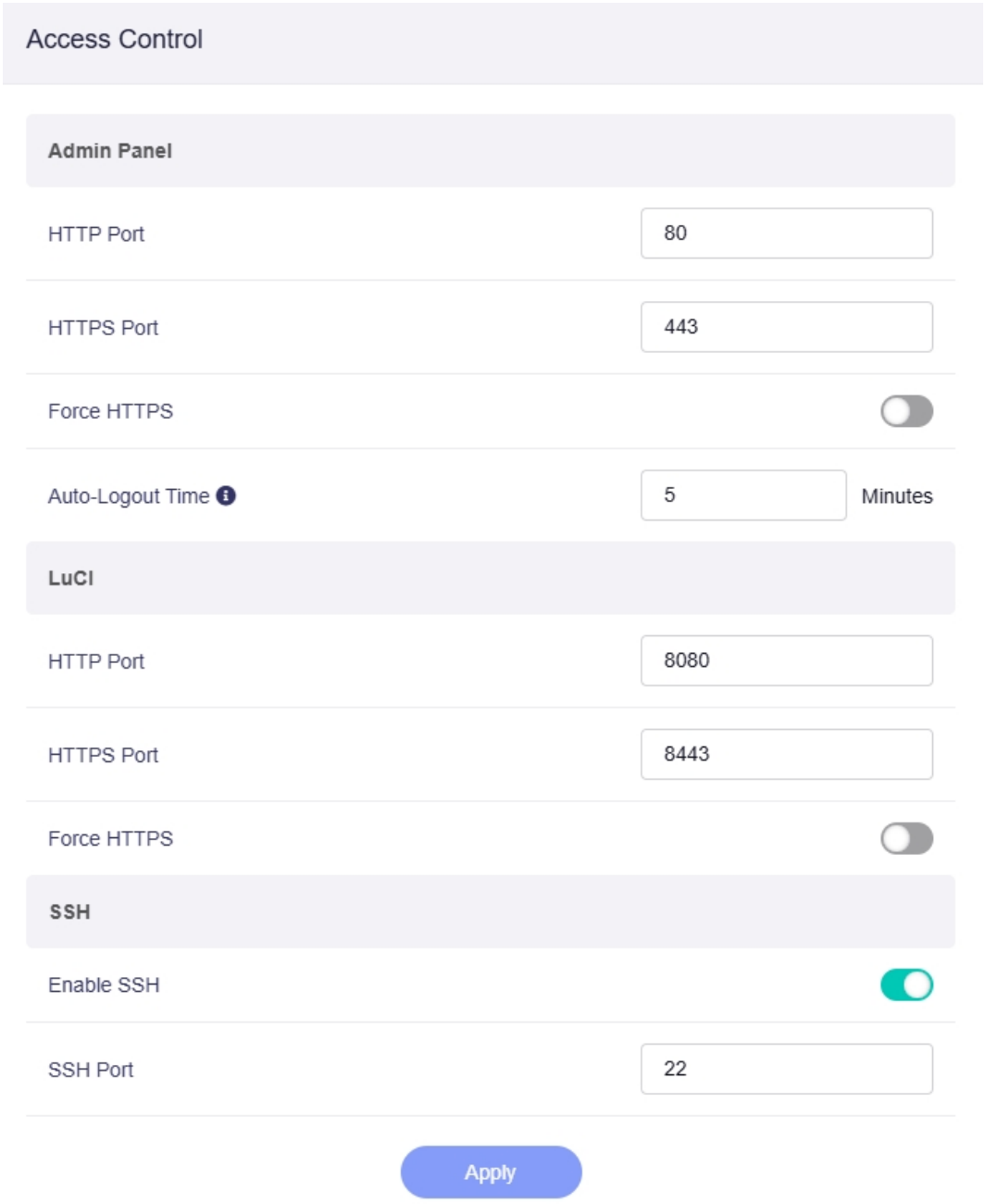


Le mot de passe administrateur doit respecter les règles suivantes :

1. Entre 10 et 63 caractères.
2. Les lettres, avec distinction de casse, les chiffres et les symboles sont autorisés, par exemple : ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~
3. Au moins deux catégories sont nécessaires parmi les majuscules, les minuscules, les chiffres et les symboles.

15.6.2 Contrôle d’accès

Cette section gère l’accès à l’interface d’administration, à LuCI et à SSH. Elle permet de limiter les tentatives d’analyse et d’intrusion sur les ports par défaut et d’éviter les problèmes liés aux conflits de ports.



Interface d’administration

- **Port HTTP (HTTP Port)** : 80 par défaut, pour l’accès HTTP non chiffré à l’interface Web.
- **Port HTTPS (HTTPS Port)** : 443 par défaut, pour l’accès HTTPS sécurisé à l’interface Web.

- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à l'interface Web.
- **Délai de déconnexion automatique (Auto-Logout Time)** : 5 minutes par défaut. Une session d'administration inactive est déconnectée après ce délai pour renforcer la sécurité. Vous pouvez le régler entre 1 minute et 3 heures.

LuCI

Remarque : installez d'abord LuCI dans les Paramètres avancés (Advanced Settings) avant de configurer son contrôle d'accès.

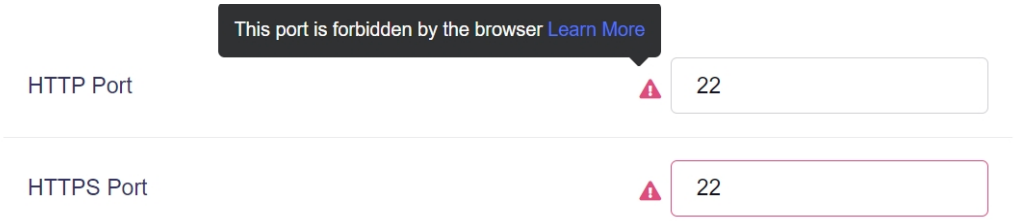
- **Port HTTP (HTTP Port)** : 8080 par défaut, pour l'accès HTTP non chiffré à LuCI.
- **Port HTTPS (HTTPS Port)** : 8443 par défaut, pour l'accès HTTPS sécurisé à LuCI.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à LuCI.

SSH

- **Activer SSH (Enable SSH)** : activé par défaut, autorise ou interdit l'accès SSH au routeur.
- **Port SSH (SSH Port)** : 22 par défaut, utilisé pour l'accès SSH au routeur.

Remarque :

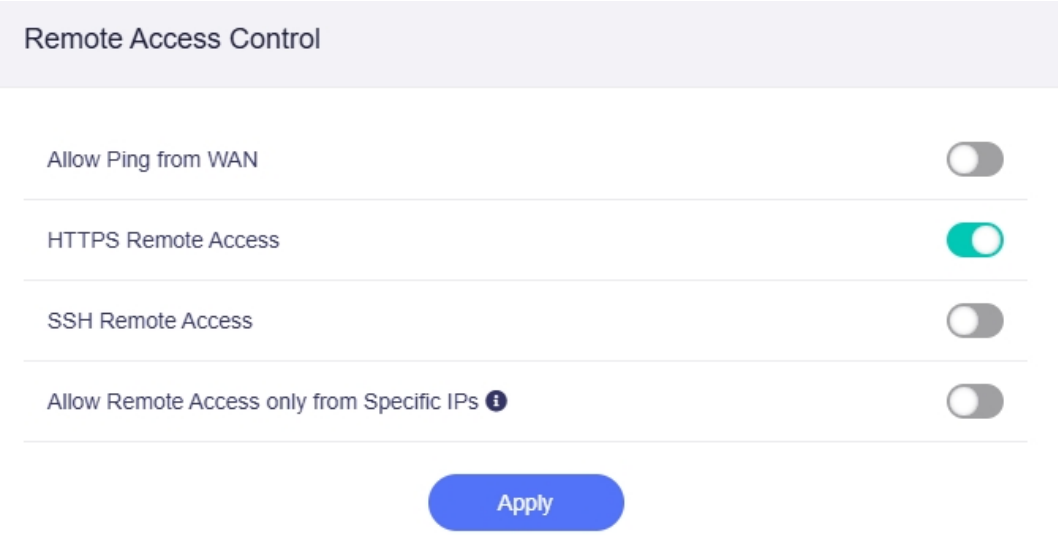
1. Si le port choisi entre en conflit avec un port réservé, notamment par les navigateurs ou les conventions réseau, le message « Ce port est interdit par le navigateur » (This port is forbidden by the browser) s'affiche.



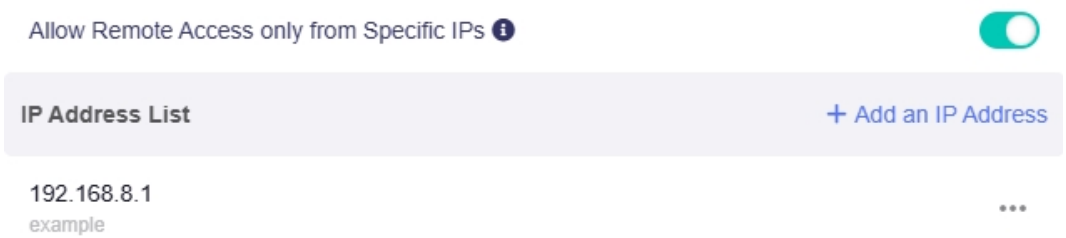
2. Si vous modifiez un port dans le micrologiciel, renseignez le nouveau numéro pour accéder à l'interface d'administration. Si vous l'avez oublié, réinitialisez le routeur pour rétablir le port par défaut.
3. Les paramètres d'accès LuCI ne sont disponibles qu'après son installation. S'ils n'apparaissent pas, ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)** pour installer LuCI.

15.6.3 Contrôle d’accès distant

Cette section gère les accès distants HTTPS et SSH et les requêtes ping depuis le WAN. Elle permet aussi de restreindre l’accès à certaines adresses IP pour concilier administration à distance et sécurité.

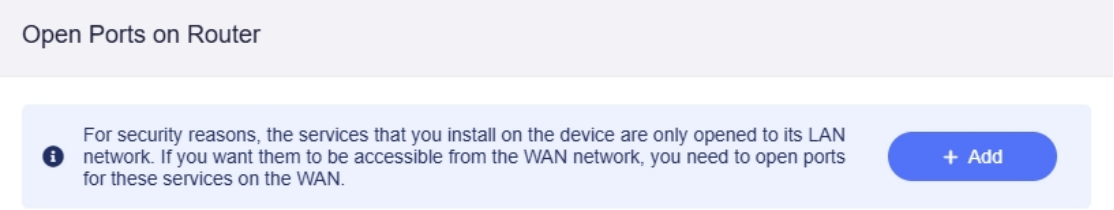


- **Autoriser le ping depuis le WAN (Allow Ping from WAN)** : permet de vérifier que le routeur est joignable depuis le WAN en cas de problème et de mesurer la latence et les pertes de paquets.
- **Accès HTTPS à distance (HTTPS Remote Access)** : permet d’accéder de manière sécurisée à l’interface Web du routeur via HTTPS. Les données échangées lors de l’administration à distance depuis un navigateur sont chiffrées.
- **Accès SSH à distance (SSH Remote Access)** : permet d’accéder au terminal et de gérer le routeur à distance par SSH, dans un tunnel chiffré.
- **Autoriser l’accès distant depuis certaines IP (Allow Remote Access from Specific IPs)** : disponible uniquement si l’une des trois fonctions précédentes est activée. Ajoutez les adresses IP autorisées pour limiter l’administration distante aux appareils qui les utilisent.

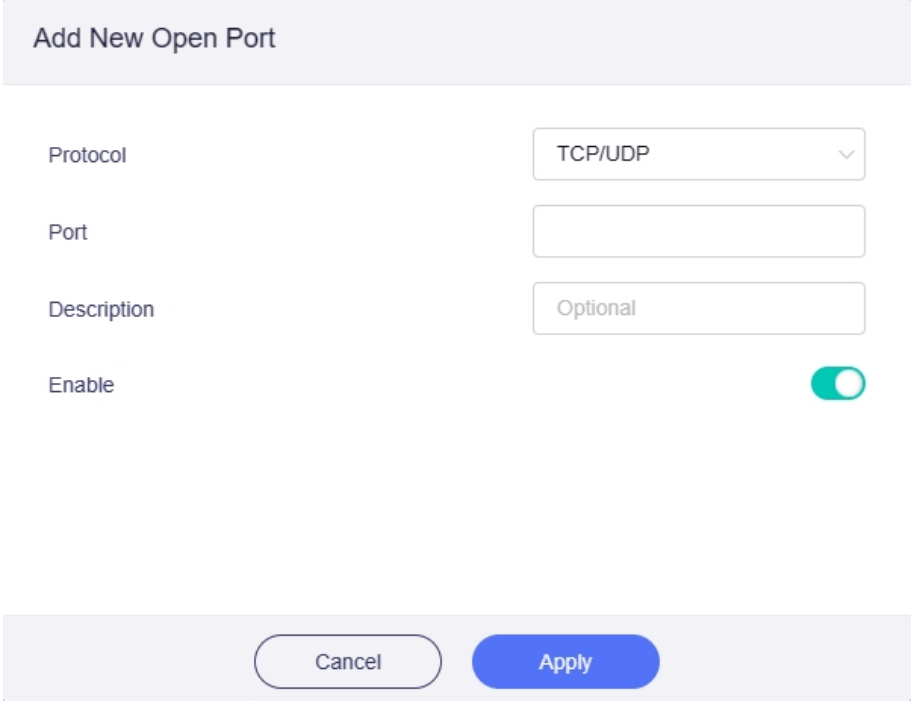


15.6.4 Ouverture de ports sur le routeur

Cette section gère l'accès aux services hébergés sur le routeur. Les services Web et FTP, par exemple, nécessitent l'ouverture de leurs ports pour être accessibles depuis le WAN. Par sécurité, les services installés ne sont accessibles que depuis le LAN par défaut. Ouvrez ici les ports nécessaires pour autoriser l'accès WAN.



Pour ouvrir un port, cliquez sur **Ajouter (Add)**, puis renseignez les informations demandées dans la fenêtre.

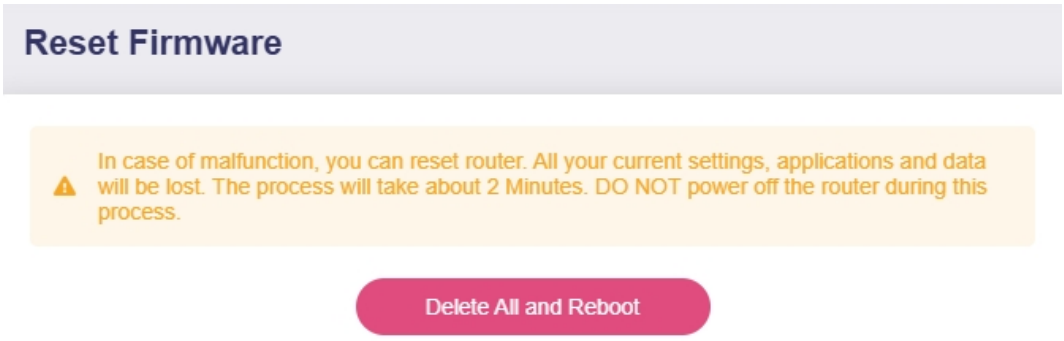


- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP/UDP. Ce choix détermine la transmission des données du service associé au port.
- **Port** : saisissez le numéro du port à ouvrir.
- **Description** (facultative) : ajoutez une brève description, comme « Serveur Web » ou « Service FTP », pour faciliter la gestion.
- **Activer (Enable)** : active ou désactive la règle de redirection.

15.7 Réinitialisation du micrologiciel

En cas de dysfonctionnement, vous pouvez essayer de réinitialiser le micrologiciel.

Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Réinitialiser le micrologiciel (Reset Firmware)**. Cliquez sur **Tout supprimer et redémarrer (Delete All and Reboot)** pour lancer la réinitialisation.



Remarque : tous vos paramètres, applications et données seront effacés. L'opération prend environ 2 minutes. N'éteignez pas le routeur pendant cette opération.

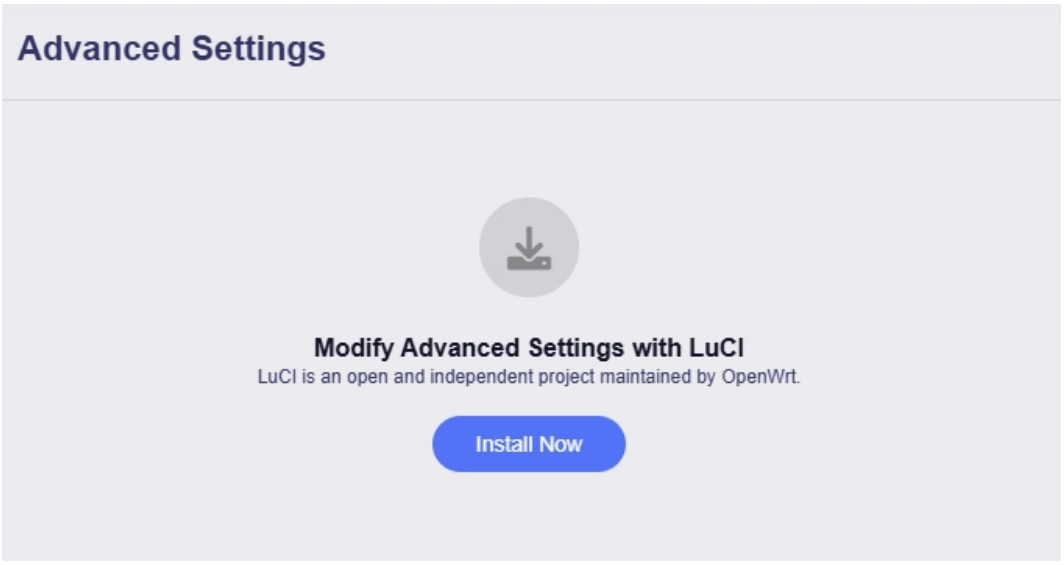
Si vous ne pouvez pas accéder à l'interface Web, utilisez le bouton physique de réinitialisation situé sur le côté du routeur.

15.8 Paramètres avancés

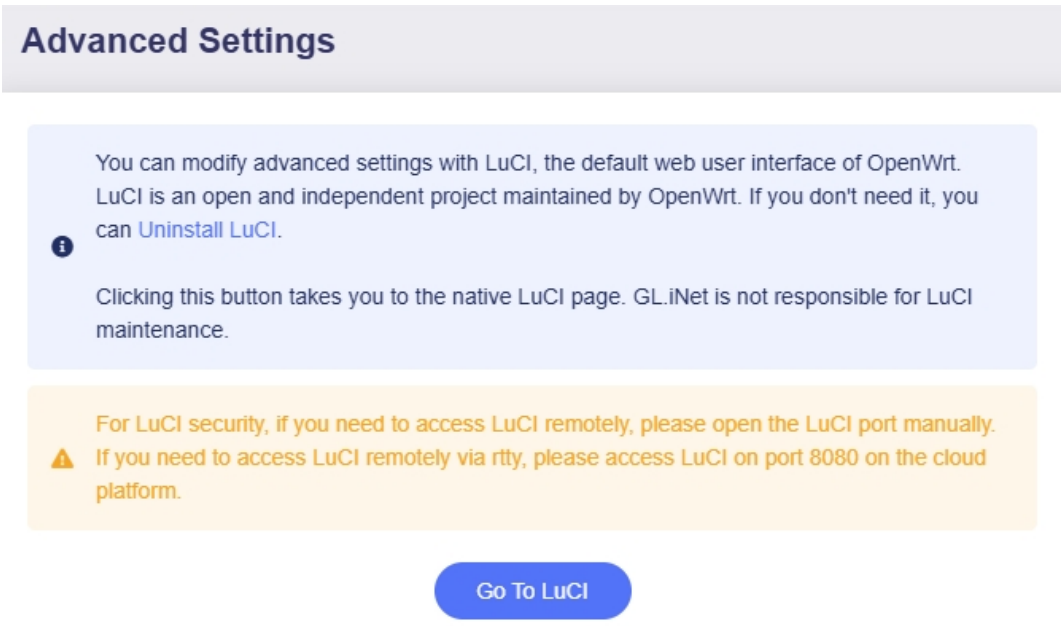
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)**. Vous pouvez y modifier les paramètres avancés dans LuCI, l'interface Web par défaut d'OpenWrt. LuCI est un projet ouvert et indépendant maintenu par OpenWrt et fourni en l'état. GL.iNet n'assure pas sa maintenance.

Pour vous connecter à LuCI, procédez comme suit.

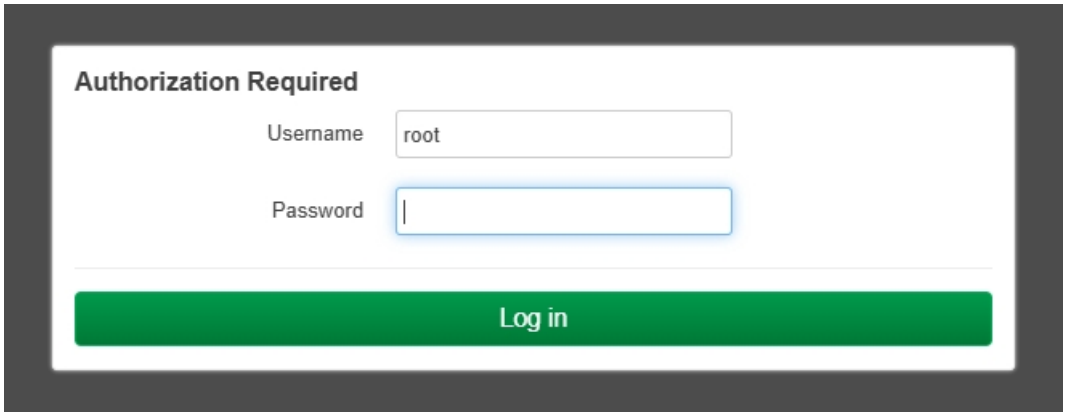
1. Cliquez sur **Installer maintenant (Install Now)** pour installer l'interface LuCI.



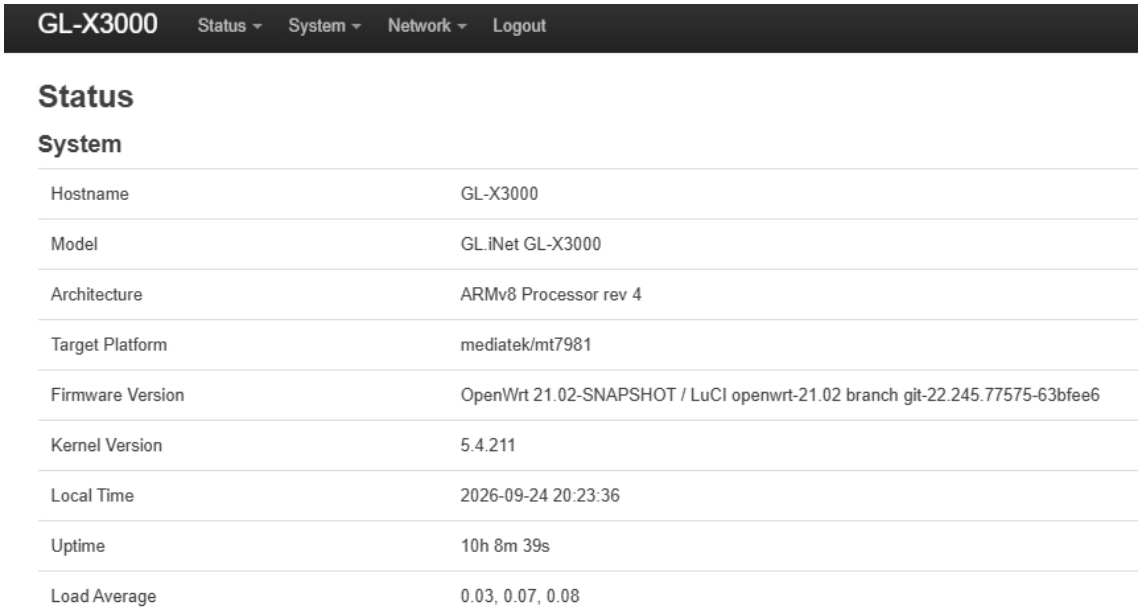
2. Cliquez sur **Accéder à LuCI (Go To LuCI)** pour ouvrir sa page de connexion.



3. Saisissez le même mot de passe que pour l’interface d’administration Web du routeur.



L’interface LuCI s’ouvre.



Déclaration UE de conformité

Par la présente, GL TECHNOLOGIES (HONG KONG) LIMITED déclare que l'équipement radio de type [Routeur Wi-Fi 6 5G NR, GL-X3000NR / Routeur Wi-Fi 6 4G LTE, GL-X3000C16] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE. Le texte intégral de la déclaration UE de conformité est disponible à l'adresse internet suivante: https://www.gl-inet.com/products/certificate.