GL·iNet



Manuel d’utilisation

GL-SFT1200 / Opal

Routeur de voyage Wi-Fi 5

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
- Choisir un emplacement adapté à l'appareil
- 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 d'accès à 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 de la communauté GL.iNet
- Assistance technique : contactez notre équipe d’assistance depuis 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 distribuée, 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 appartiennent à leurs propriétaires respectifs et sont des marques commerciales ou déposées.

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 8

1.1 Présentation du produit 9

1.1.1 Aspect extérieur 9

1.1.2 Ports et boutons 10

1.1.3 LED 11

1.2 Caractéristiques techniques 11

1.3 Contenu de l'emballage 12

Chapitre 2 Branchements 13

2.1 Choix de l'emplacement 14

2.2 Branchement du routeur 14

Chapitre 3 Connexion à l'interface du routeur 15

Chapitre 4 Configuration de la connexion Internet 17

4.1 Assistant de configuration rapide 18

4.2 Configuration manuelle de la connexion Internet 19

4.2.1 Connexion à Internet par câble Ethernet 20

4.2.2 Connexion à Internet via un réseau Wi-Fi existant 25

4.2.3 Connexion à Internet par partage de connexion USB 31

4.2.4 Connexion à Internet via un modem USB 36

Chapitre 5 Réseau sans fil 38

5.1 Affichage de l'état du Wi-Fi 39

5.2 Paramètres sans fil 40

5.2.1 Wi-Fi 5 GHz 40

5.2.2 Wi-Fi 2,4 GHz 42

5.2.3 BSSID aléatoire 44

Chapitre 6 Appareils clients 46

6.1 Informations sur les appareils 48

6.2 Actions 50

6.3 Suppression de clients 54

6.4 Tri 55

Chapitre 7 Services cloud 56

7.1 GoodCloud 57

7.1.1 Activation de GoodCloud 58
7.1.2 Gestion de votre routeur 61
7.1.3 Dissociation de l'appareil 66
7.1.4 Désactivation de GoodCloud 66
7.2 AstroWarp 68
Chapitre 8 Comprendre les VPN 69
8.1 Introduction 70
8.2 Cas d'utilisation 71
Chapitre 9 Tableau de bord VPN 73
9.1 Assistant de configuration VPN 74
9.2 Mode VPN 77
9.2.1 Mode global 78
9.2.2 Mode par règles 79
Chapitre 10 Configuration d'un serveur VPN 90
10.1 Configuration d'un serveur OpenVPN 91
10.1.1 Préparation 91
10.1.2 Étapes de configuration 92
10.1.3 Dépannage 95
10.2 Configuration d'un serveur WireGuard 96
10.2.1 Préparation 96
10.2.2 Étapes de configuration 97
10.2.3 Dépannage 100
Chapitre 11 Configuration d'un client VPN 101
11.1 Configuration d'un client OpenVPN 102
11.1.1 Préparation 102
11.1.2 Configuration de NordVPN 102
11.1.3 Configuration manuelle d'un client OpenVPN pour un autre fournisseur 108
11.2 Configuration d'un client WireGuard 111
11.2.1 Préparation 111
11.2.2 Configuration d'AzireVPN 112
11.2.3 Configuration de Hide.me 117
11.2.4 Configuration d'IPVanish 120
11.2.5 Configuration de Mullvad 125
11.2.6 Configuration de NordVPN 130

11.2.7 Configuration de PIA (Private Internet Access) 135
11.2.8 Configuration de Surfshark 140
11.2.9 Configuration manuelle d'un client WireGuard pour un autre fournisseur ... 145
Chapitre 12 Réseau 151
12.1 Multi-WAN 152
12.1.1 Suivi de l'état des interfaces 152
12.1.2 Mode Multi-WAN 155
12.2 LAN 158
12.2.1 Paramètres de base 158
12.2.2 Serveur DHCP 160
12.2.3 Réservation d'adresses 162
12.3 Réseau invité 163
12.3.1 Paramètres de base 163
12.3.2 Serveur DHCP 165
12.4 DNS 167
12.4.1 Paramètres généraux 167
12.4.2 Paramètres du serveur DNS 168
12.4.3 Modification du fichier hosts 170
12.5 Ports Ethernet 172
12.6 IPv6 173
12.6.1 Mode IPv6 174
12.6.2 Méthode d'obtention du DNS 174
12.7 IGMP Snooping 175
12.8 Mode réseau 176
12.9 Passerelle transparente 178
12.10 Accélération réseau 180
Chapitre 13 Sécurité 182
13.1 Redirection de port 183
13.1.1 DMZ 183
13.1.2 Redirection de port 184
13.2 Contrôle d'administration 187
13.2.1 Contrôle d'accès 187
13.2.2 Contrôle d'accès distant 190
13.2.3 Ouverture de ports sur le routeur 191

13.3 Mode NAT 192
Chapitre 14 Applications 193
14.1 Extensions 194
14.2 DNS dynamique 195
14.2.1 Activation du DDNS 195
14.2.2 Vérification du fonctionnement du DDNS 198
14.2.3 Accès HTTPS à distance 200
14.2.4 Accès SSH à distance 203
14.3 Stockage réseau 205
14.3.1 Branchement du stockage 205
14.3.2 Configuration de Samba 206
Chapitre 15 Système 209
15.1 Vue d'ensemble 210
15.2 Mot de passe administrateur 211
15.3 Mise à jour 212
15.3.1 Mise à jour en ligne 212
15.3.2 Mise à jour locale 213
15.4 Tâches planifiées 215
15.4.1 Programmation du voyant LED 215
15.4.2 Redémarrage planifié 216
15.4.3 Programmation du Wi-Fi 5 GHz 217
15.4.4 Programmation du Wi-Fi 2,4 GHz 220
15.5 Fuseau horaire 223
15.6 Paramètres du commutateur 224
15.7 Réinitialisation du micrologiciel 225
15.8 Journaux 226
15.9 Paramètres avancés 228

Chapitre 1

Présentation de votre routeur

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

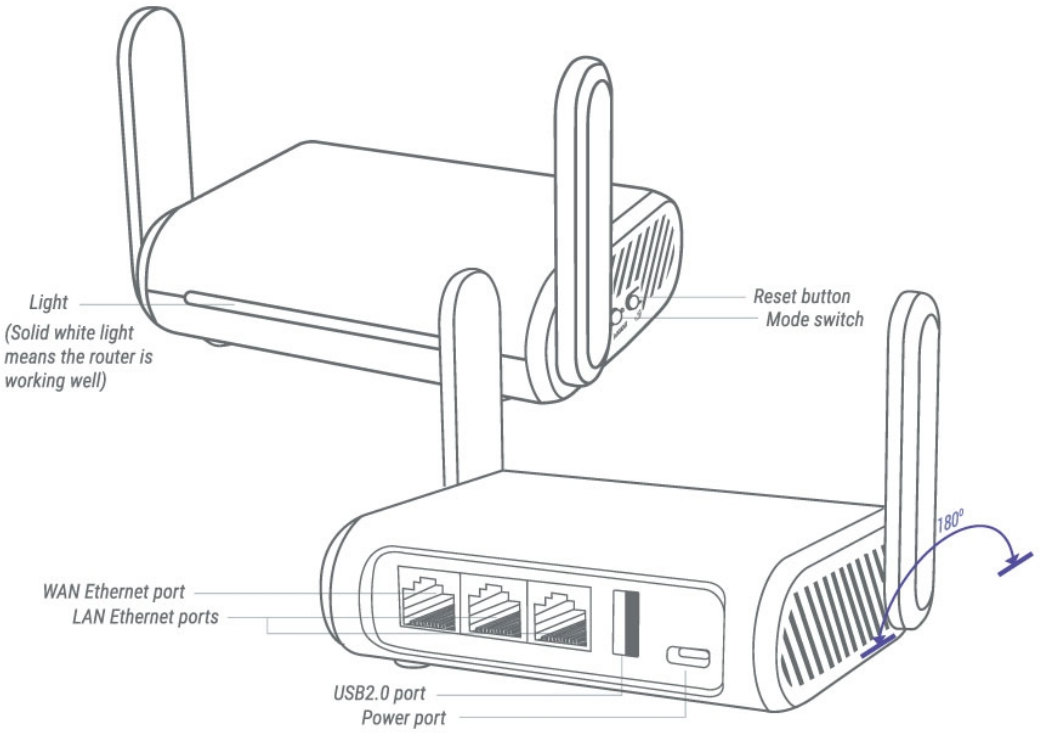
1.1 Présentation du produit

Opal (GL-SFT1200) est un routeur de voyage de poche offrant un débit sans fil de 1 200 Mbit/s. Son format compact facilite le transport et répond aux besoins d’accès Internet sans fil des petites entreprises, des petits appartements et des voyageurs d’affaires.

1.1.1 Aspect extérieur



1.1.2 Ports et boutons



Élément	Description
Prise d'alimentation	Pour brancher l'adaptateur secteur.
Port WAN	Pour raccorder le routeur à un modem ou à une prise Ethernet.
Port LAN	Pour connecter des appareils au routeur par câble.
Port USB 2.0	Pour brancher un périphérique de stockage USB au routeur.
Bouton de réinitialisation	Maintenez le bouton enfoncé pendant **4 secondes** pour réparer votre connexion réseau ; Maintenez enfoncé pendant **10 secondes**, puis relâchez : le routeur retrouve ses paramètres d'usine.
Commutateur	Un commutateur physique permet de modifier certains paramètres du routeur d'un simple geste. Configurez-le dans l'interface Web pour activer ou désactiver les fonctions souhaitées.

1.1.3 LED

État	Signification
Bleu fixe	Démarrage en cours
Bleu à pulsation lente	Appareil démarré, sans connexion Internet
Blanc fixe	Connexion Internet établie
Bleu clignotant rapidement	Réinitialisation en cours

1.2 Caractéristiques techniques

Interfaces	1 port Ethernet WAN 1 port Ethernet LAN 1 port USB 2.0 1 entrée d'alimentation USB-C 1 bouton de réinitialisation 1 commutateur
CPU	SF19A28, deux cœurs à 1 GHz
Mémoire / Stockage	DDR3 128 Mo / mémoire flash SPI NAND 128 Mo
Protocoles	IEEE 802.11a/b/g/n/ac
Débit Wi-Fi	300 Mbit/s (2,4 GHz), 867 Mbit/s (5 GHz)
Antennes	2 antennes Wi-Fi externes non amovibles
Débit Ethernet	10/100/1 000 Mbit/s
Alimentation	USB-C, 5 V / 3 A
Consommation électrique	< 6 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	118 × 85 × 30 mm / 145 g
Autres ressources	Fiche technique / Micrologiciel / Application / Déballage / Tutoriels

*Les débits Wi-Fi sont fondés sur les normes IEEE 802.11, par exemple 802.11ax pour le Wi-Fi 6. Le débit et la portée réels peuvent être réduits par les obstacles environnants (murs, métal), la congestion du réseau ou les capacités des appareils clients.

1.3 Contenu de l’emballage

L’adaptateur fourni dépend du pays de livraison.

L’emballage contient :

- 1 Opal (GL-SFT1200)
- 1 guide de démarrage rapide
- 1 câble Ethernet
- 1 carte de remerciement
- 1 adaptateur secteur
- 1 adaptateur de prise (selon le pays de livraison)

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 chaleu**r : 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** : placez le routeur à un endroit permettant de le brancher facilement à une prise de courant et de connecter plusieurs appareils, par exemple au centre du salon.
- **Disposition des câbles** : disposez les câbles et le cordon d’alimentation de manière à éviter tout risque de trébuchement.
- **Surface stable** : posez le routeur sur une surface plane et horizontale, comme une étagère ou un bureau, pour assurer sa stabilité.
- **Évitez les interférences électromagnétiques** : éloignez le routeur des sources d’interférences, comme les appareils Bluetooth ou 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, sélectionnez le réseau Wi-Fi du routeur dans la liste des réseaux disponibles et saisissez le mot de passe. Le nom du réseau et le mot de passe par défaut figurent sur l’étiquette du routeur.
   - **Ethernet** : reliez votre appareil à un 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

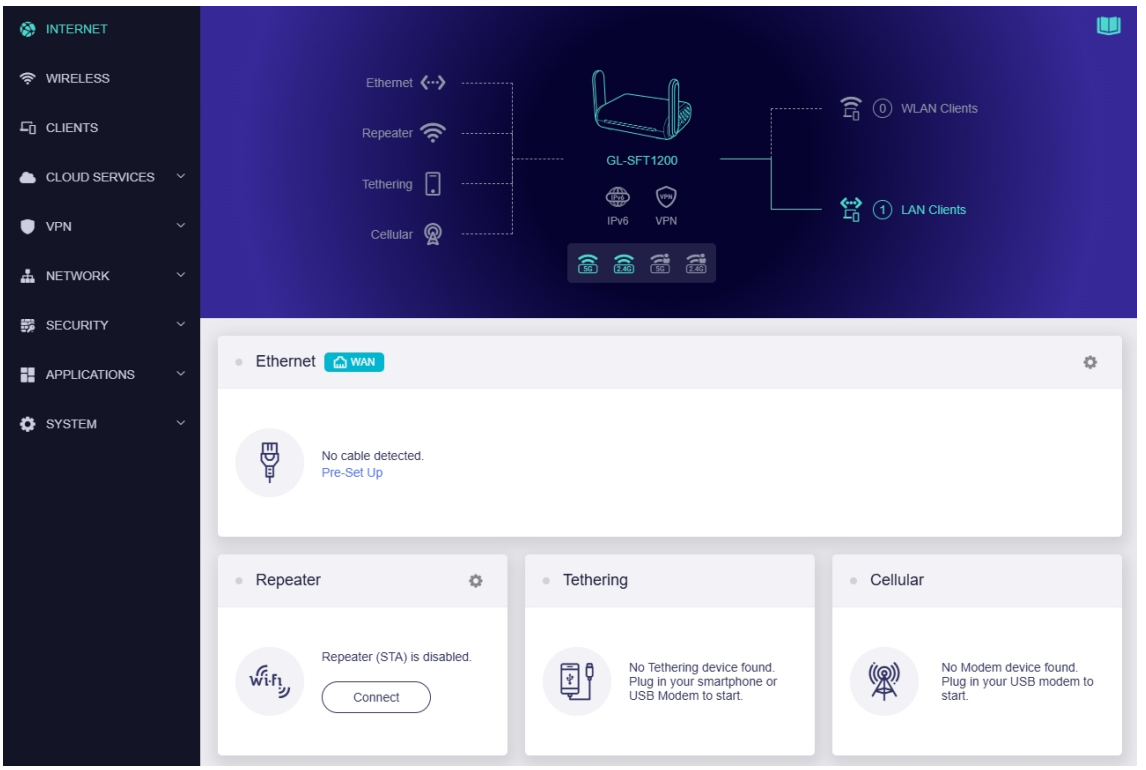
Ce chapitre explique comment vous connecter à l’interface d’administration Web du routeur.

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 à l'interface d'administration Web du routeur.

1. Connectez un appareil (par exemple, un ordinateur de bureau ou 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. Définissez le SSID et le mot de passe de votre Wi-Fi. Si vous modifiez les informations du Wi-Fi ici, reconnectez-vous au réseau mis à jour, puis cliquez sur **Appliquer (Apply)**.
5. Vous accédez alors à l'interface d'administration Web du routeur.



Chapitre 4

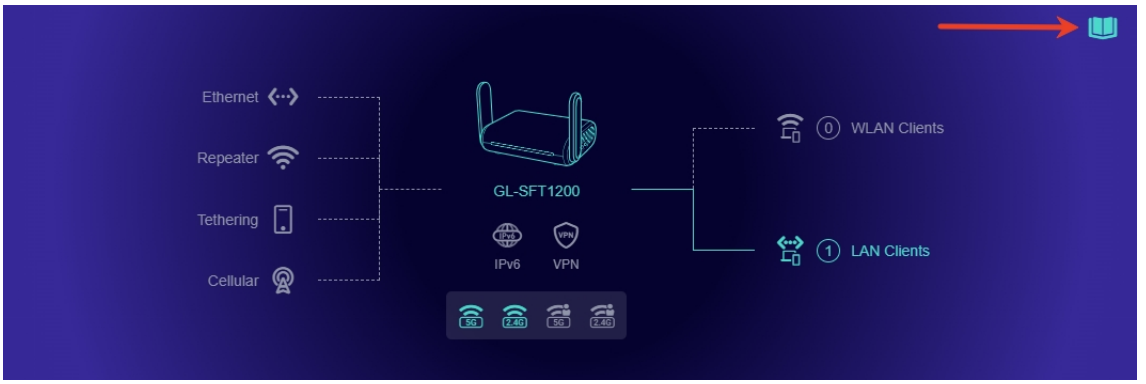
Configuration de la connexion Internet

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

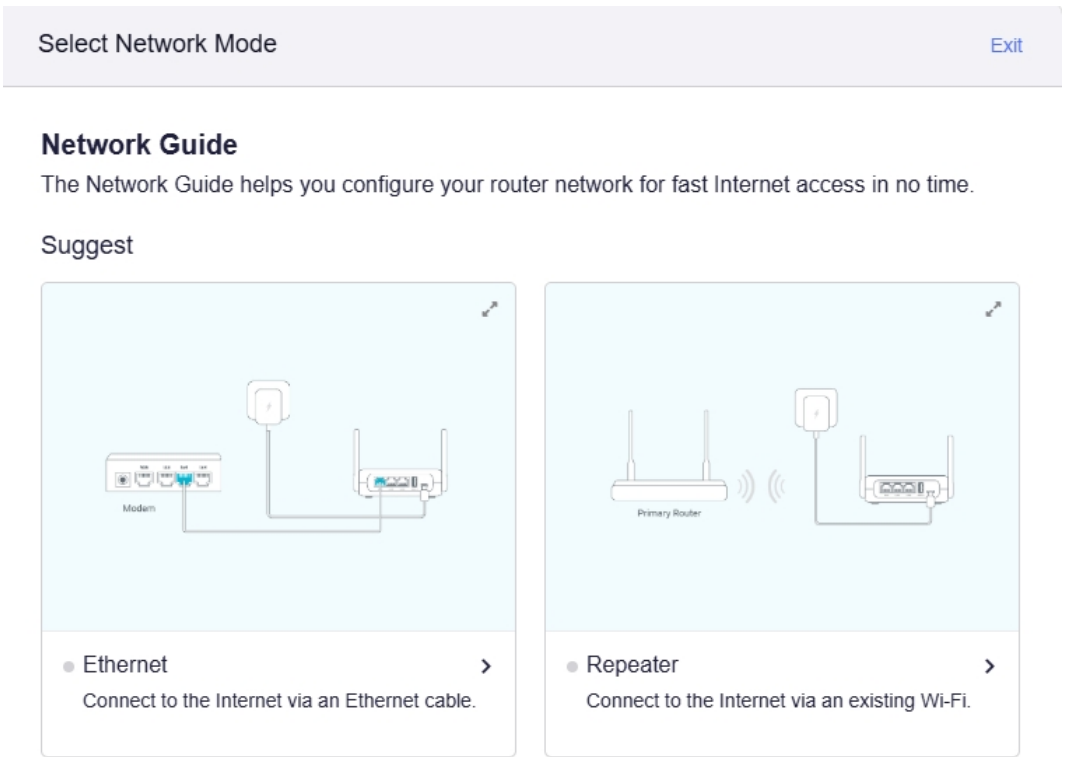
4.1 Assistant de configuration rapide

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’adapter les paramètres réseau avancés à vos besoins et de vérifier ou de modifier les connexions existantes.

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

1. **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.

2. **Répéteur (Repeater)** : ce mode permet au routeur de se connecter à un réseau Wi-Fi existant pour étendre sa couverture et créer un réseau local distinct et sécurisé. Il peut toutefois réduire le débit de transmission. Il convient aux zones mal couvertes nécessitant une extension du signal ou aux lieux publics où vous souhaitez renforcer la sécurité de votre connexion.

3. **Partage de connexion USB (USB Tethering)** : reliez un smartphone ou un autre appareil compatible au routeur à l’aide d’un câble USB pour partager sa connexion mobile, par exemple 4G ou 5G. Cette solution pratique convient à un accès Internet temporaire, notamment en déplacement ou dans les zones sans accès fixe à Internet.

4. **Modem USB** : branchez au routeur un modem USB cellulaire contenant une carte SIM. Le routeur se connecte alors à Internet via un réseau mobile 4G ou 5G, indépendamment d’un accès fixe. Cette méthode offre une grande mobilité et convient notamment à une utilisation en véhicule ou en extérieur.

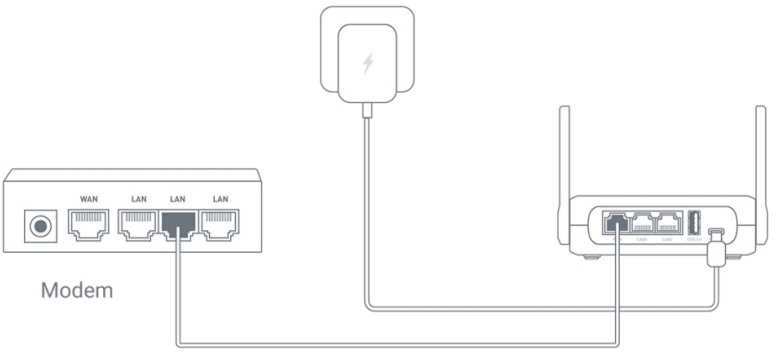
4.2.1 Connexion à Internet par câble Ethernet

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.

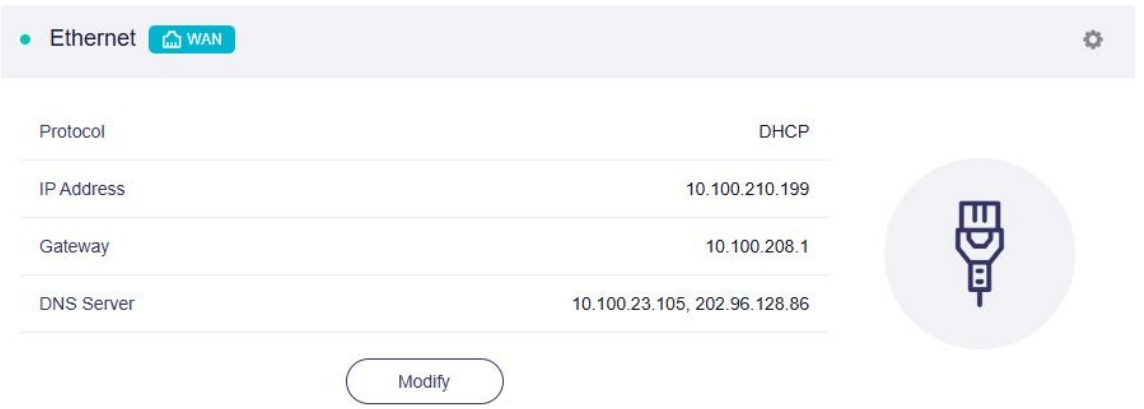
Configuration de base

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 (modem du FAI, routeur principal, commutateur réseau ou prise Ethernet) à l'aide d'un câble Ethernet.

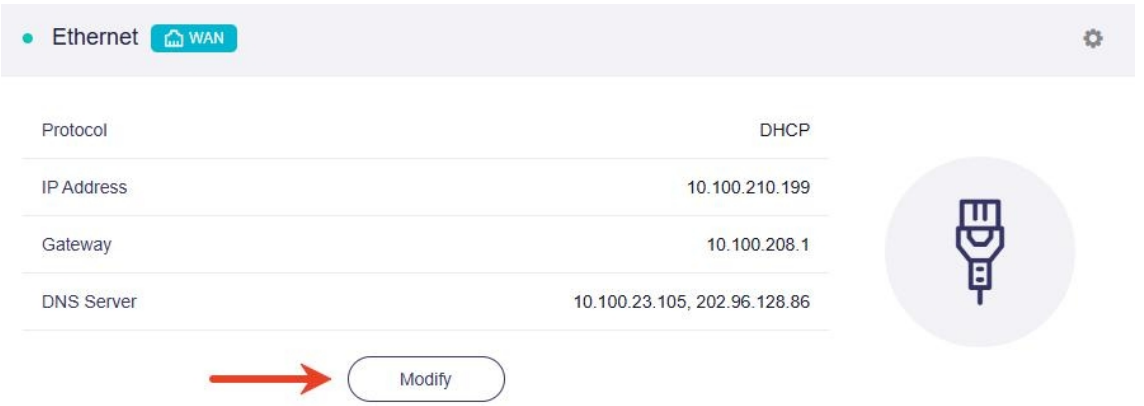


2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Ethernet**. Si la connexion est établie, la section Ethernet affiche les informations réseau, notamment le protocole, l'adresse IP, la passerelle et le serveur DNS.



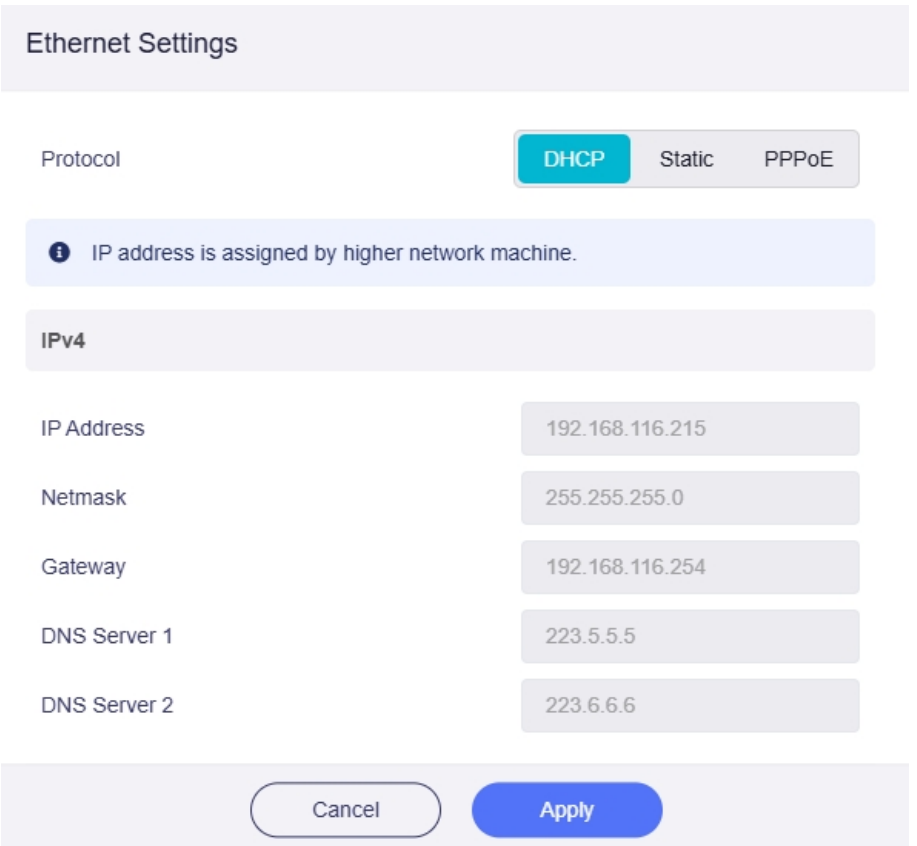
Protocoles

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



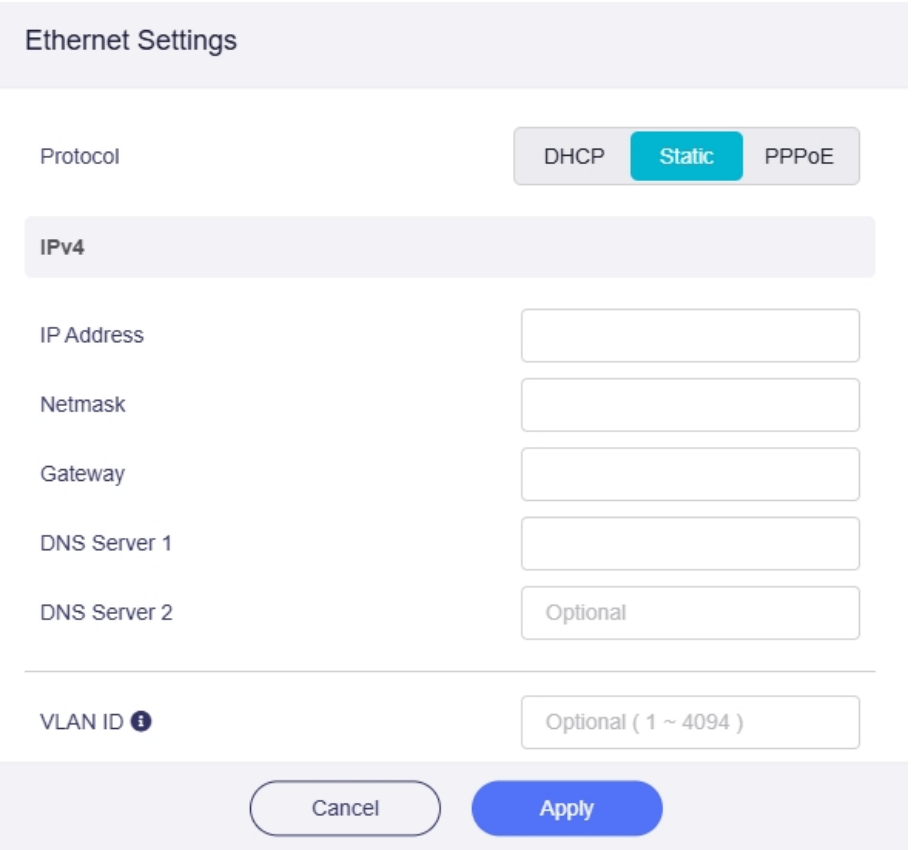
- **DHCP**

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



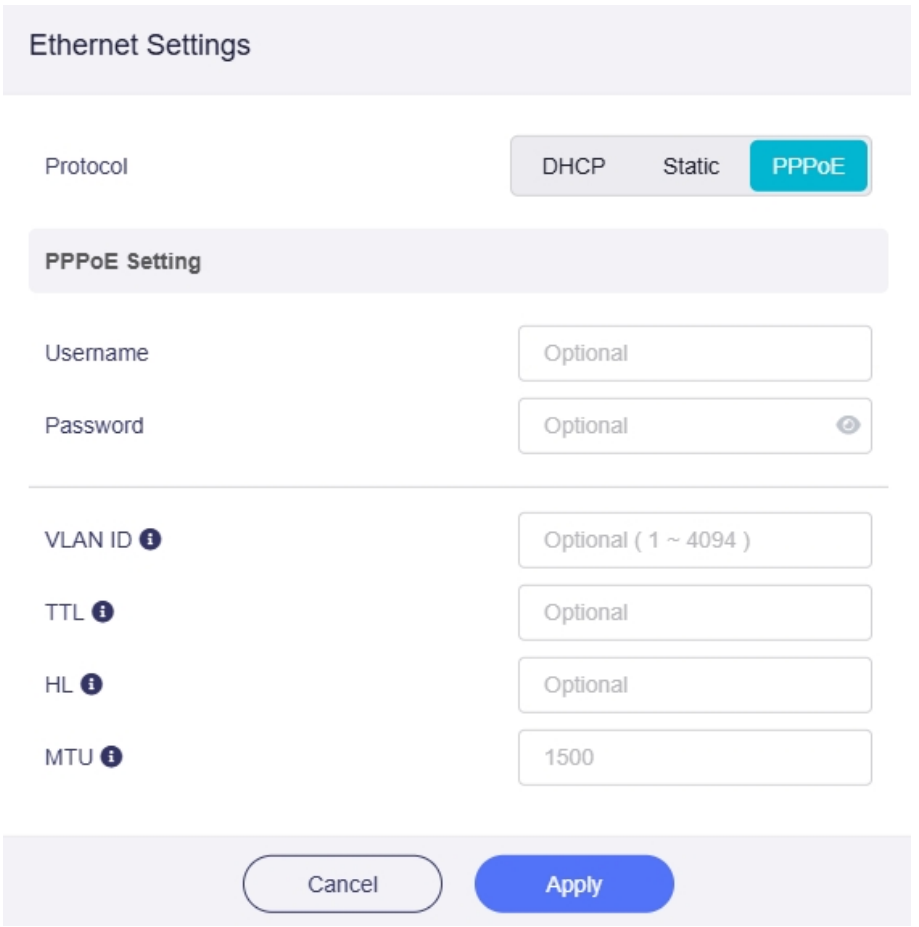
- **Statique (Static)**

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



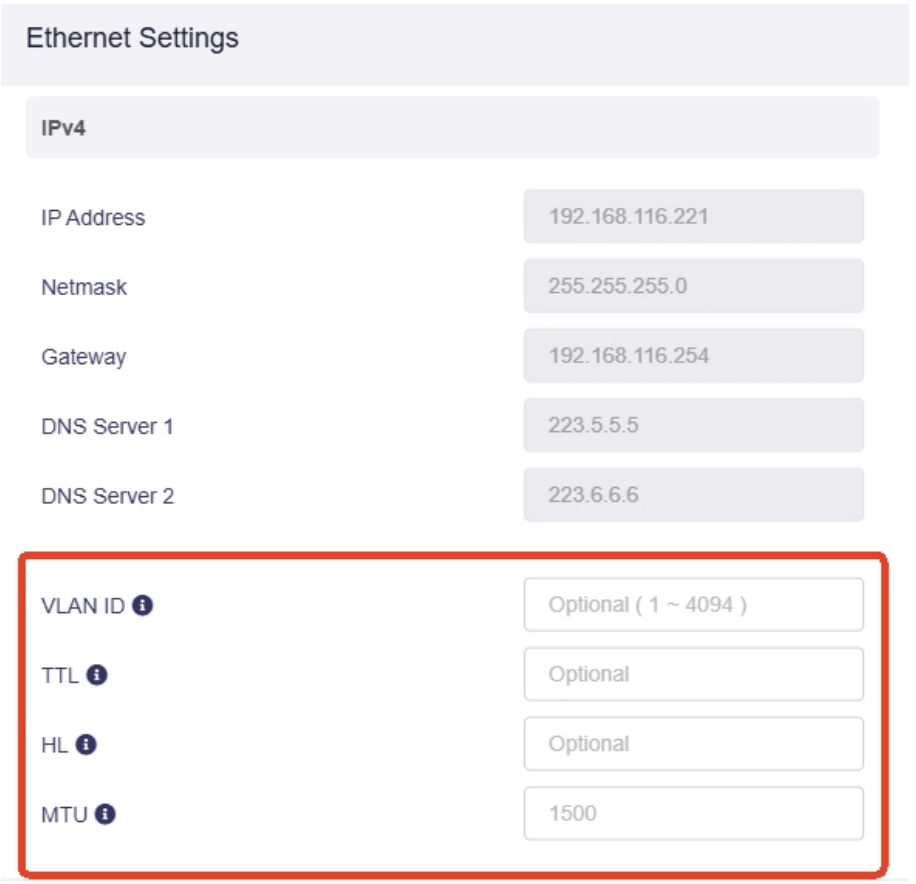
- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) est un protocole réseau très utilisé par les FAI. Ceux-ci fournissent généralement un modem ainsi qu'un identifiant et un mot de passe propres à votre connexion, 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

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**

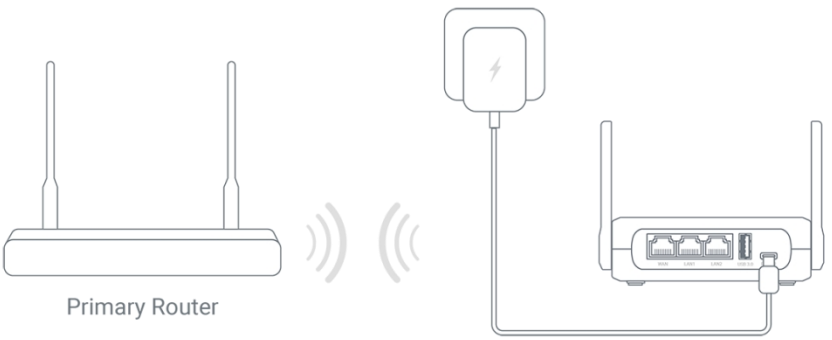
  Le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour modifier ce comportement, vous pouvez définir ici une valeur fixe. Le paramètre TTL ne s'applique qu'à IPv4.
- **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.

4.2.2 Connexion à Internet via un réseau Wi-Fi existant

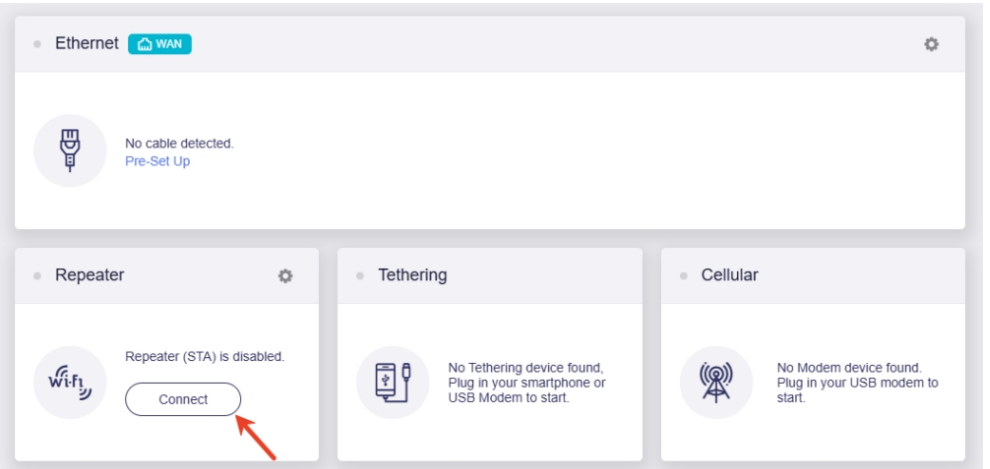
Connectez le routeur en mode répéteur à un réseau Wi-Fi existant pour renforcer la couverture et créer un réseau local isolé du réseau principal. Dans un hôtel ou un café proposant un point d'accès public gratuit, le répéteur étend le signal Wi-Fi, permet à plusieurs appareils de se connecter par câble ou sans fil et protège votre réseau.



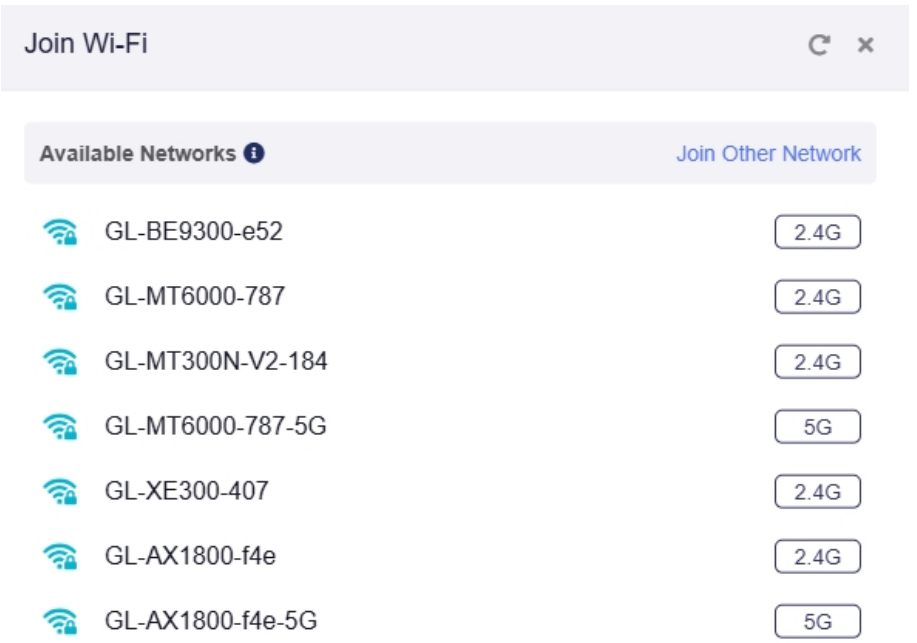
La fonction répéteur GL.iNet utilise par défaut le mode WISP (Wireless Internet Service Provider). Le routeur crée ainsi son propre sous-réseau et agit comme un pare-feu pour vous protéger du réseau public.

Configuration de base

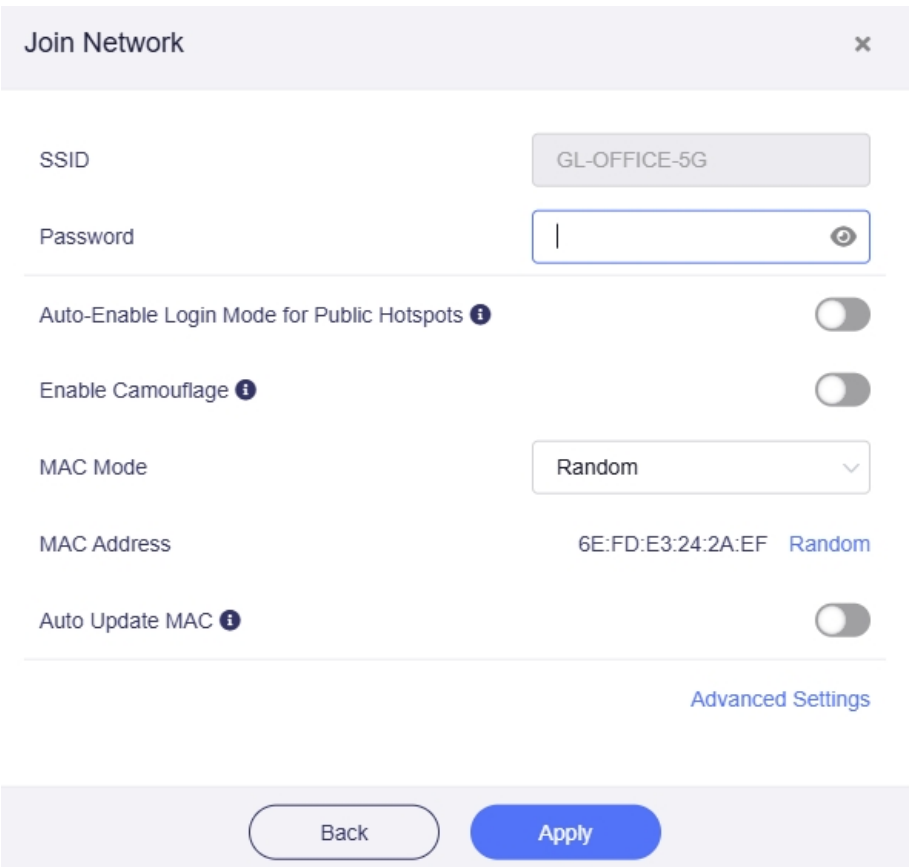
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Répéteur (Repeater)**. Cliquez sur **Connecter (Connect)**.



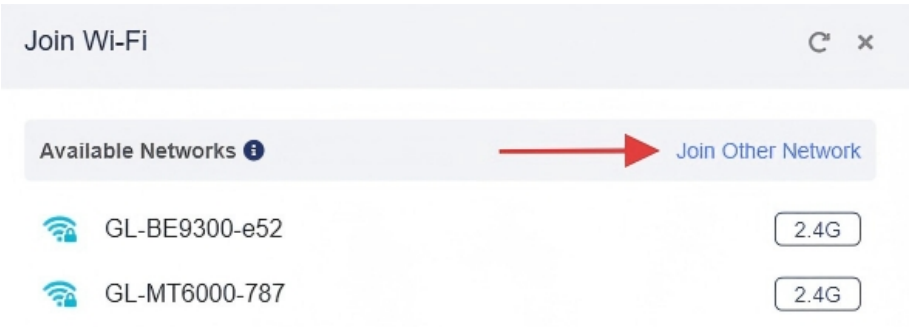
2. Dans la fenêtre qui s’affiche, choisissez le réseau Wi-Fi souhaité dans la liste des réseaux disponibles.



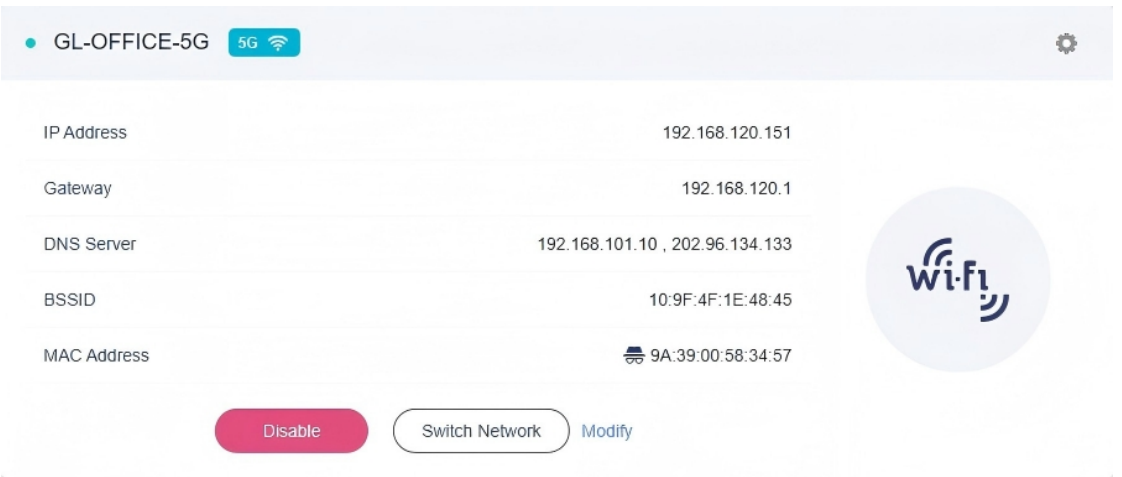
3. Saisissez le mot de passe Wi-Fi correct, puis cliquez sur **Appliquer (Apply)**.



Si le SSID du réseau souhaité n'apparaît pas dans la liste, cliquez sur **Rejoindre un autre réseau (Join Other Network)** dans l'angle supérieur droit. Saisissez le SSID et les autres informations demandées, puis cliquez sur **Appliquer (Apply)**.

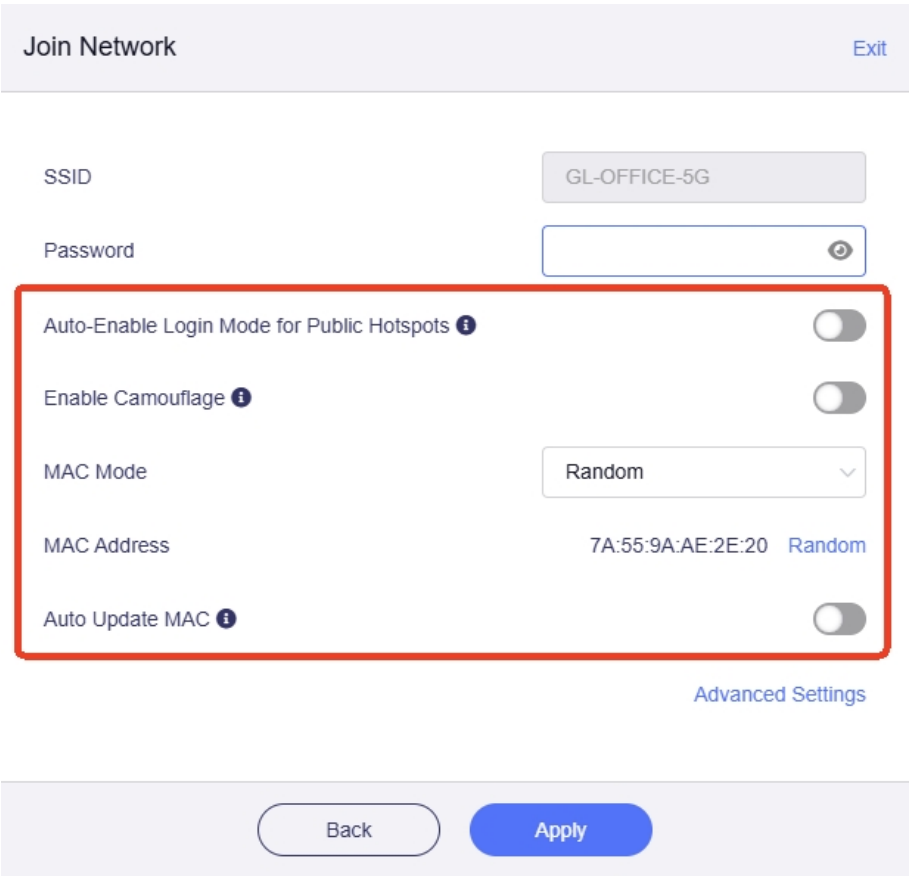


4. Patientez une minute pendant la connexion du routeur. Une fois la connexion établie, la page se présente comme ci-dessous.



Paramètres des points d’accès publics

Pour connecter le routeur à un point d’accès public doté d’un portail captif, il est recommandé d’activer les fonctions suivantes afin de 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 MAC souhaitée ne figure pas dans la liste, saisissez manuellement celle que vous voulez cloner. De nombreux appareils utilisent des adresses MAC aléatoires, souvent appelées « adresse Wi-Fi privée » ou « adresse matérielle aléatoire », pour se connecter aux réseaux Wi-Fi. L'adresse MAC affichée ici peut donc différer de l'adresse physique réelle de l'appareil.
Aléatoire (Random)	Génère automatiquement une adresse MAC aléatoire pour la connexion.

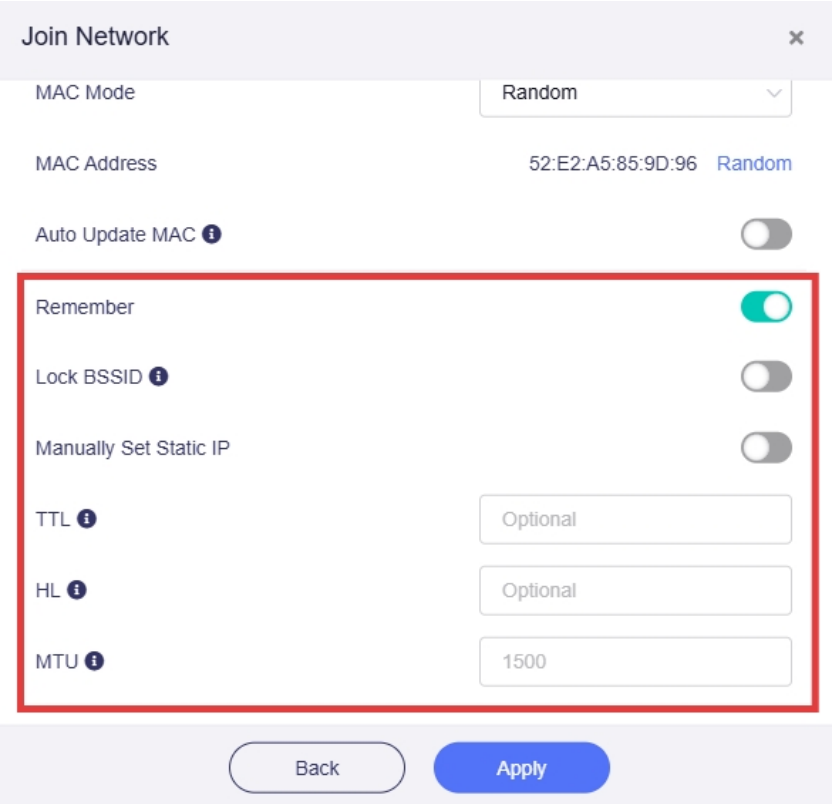
- **Mise à jour automatique de l'adresse MAC**

  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.

Paramètres avancés

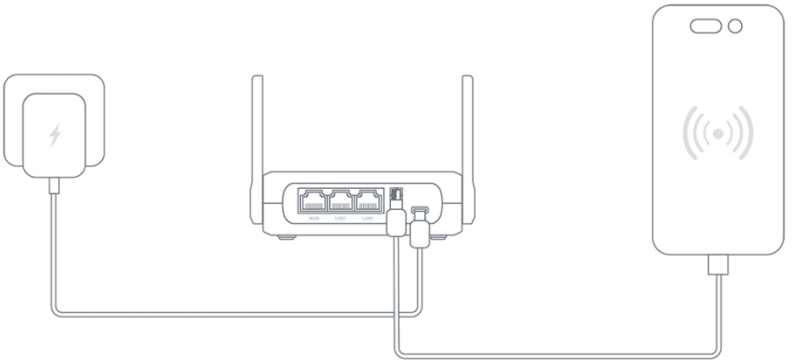
Des paramètres avancés facultatifs sont disponibles lors de la connexion au réseau.



- **Mémoriser (Remember)** : activez cette option pour mémoriser le réseau Wi-Fi auquel le routeur se connecte en mode répéteur. Elle est disponible à partir du micrologiciel v4.7.
- **Verrouiller le BSSID (Lock BSSID)** : si cette option est activée, lorsque le routeur sélectionne un réseau utilisant ce SSID, il ne se connecte qu'au point d'accès correspondant au BSSID choisi.
- **Définir manuellement une IP statique** : cette option est disponible à partir du micrologiciel v4.7.
- **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. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour camoufler ce comportement, vous pouvez définir ici une valeur fixe. Le TTL ne s'applique qu'à IPv4.
- **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.

4.2.3 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.

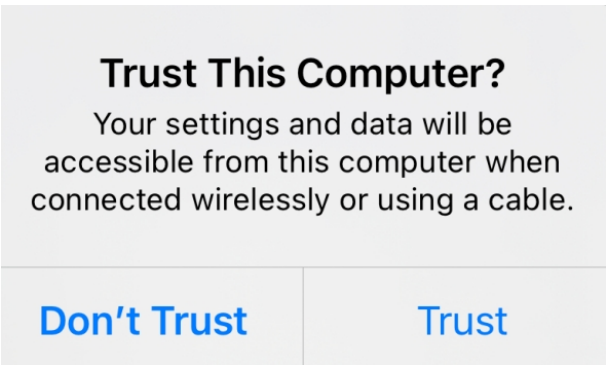


Les modems autonomes, dits « host-less », utilisent également le mode de partage de connexion USB lors de leur configuration.

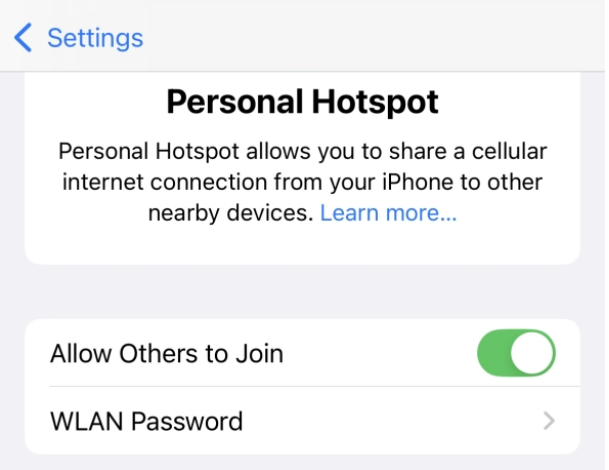
Remarque : certains opérateurs mobiles limitent le partage de connexion ou le facturent en supplément. Renseignez-vous auprès de votre opérateur.

Partage de connexion avec un iPhone

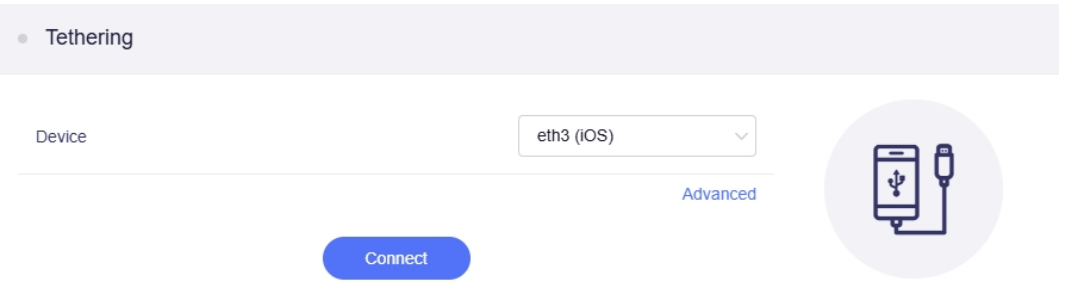
1. Reliez l'iPhone au port USB du routeur à l'aide d'un câble USB. Une boîte de dialogue vous demande si vous souhaitez faire confiance à cet appareil. Touchez **Se fier (Trust)** pour continuer.



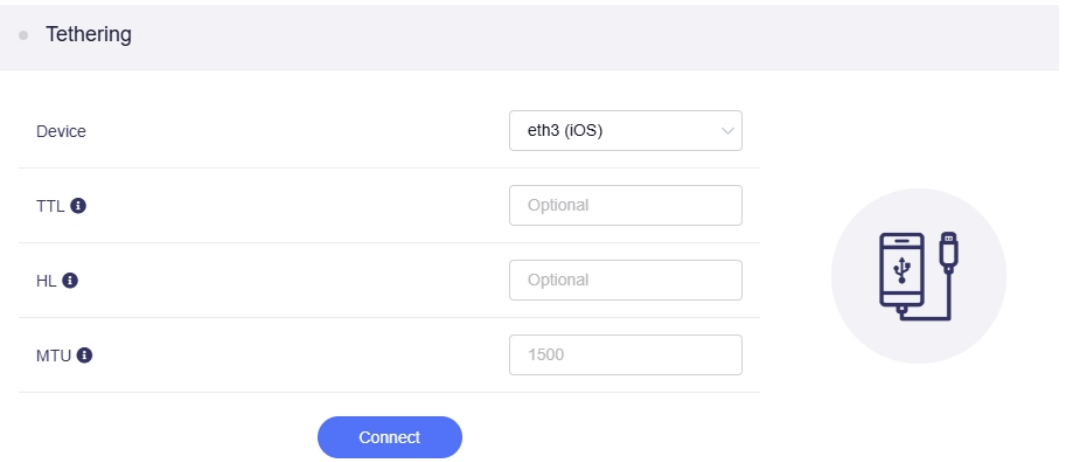
2. Sur l'iPhone, ouvrez **Réglages (Settings)** > **Partage de connexion (Personal Hotspot)**. Activez **Autoriser d'autres utilisateurs (Allow Others to Join)**.



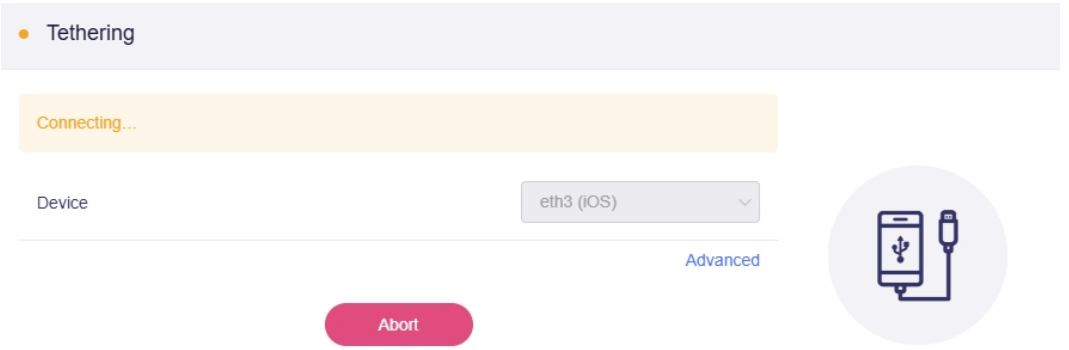
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



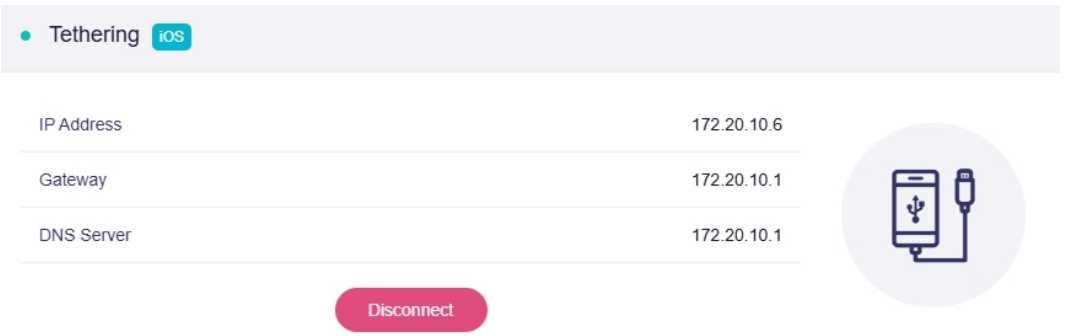
Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)**. Ajustez les paramètres, puis cliquez sur **Connecter (Connect)**.



4. La connexion démarre.

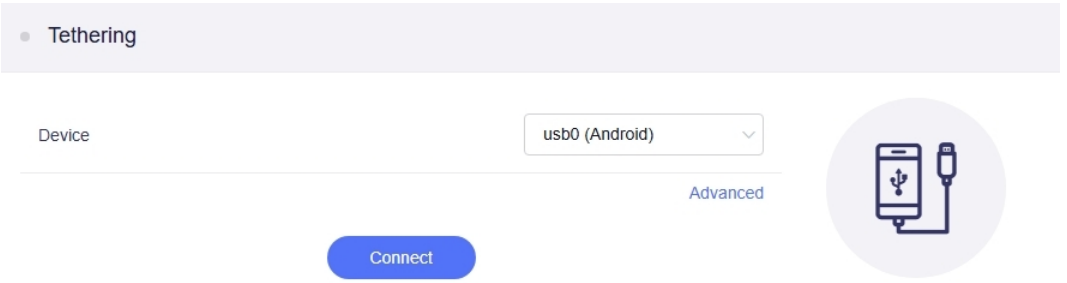


Une fois la connexion établie, cette page en affiche les détails.

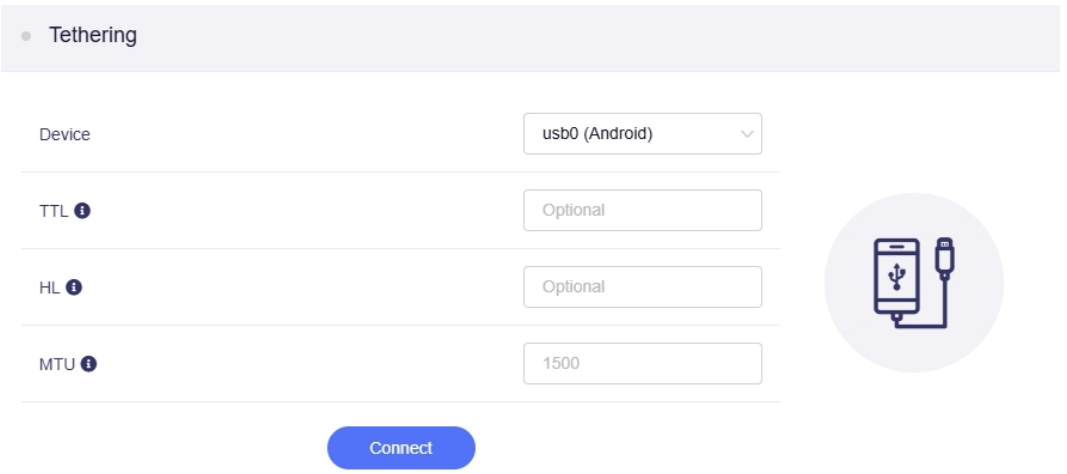


Partage de connexion avec un téléphone Android

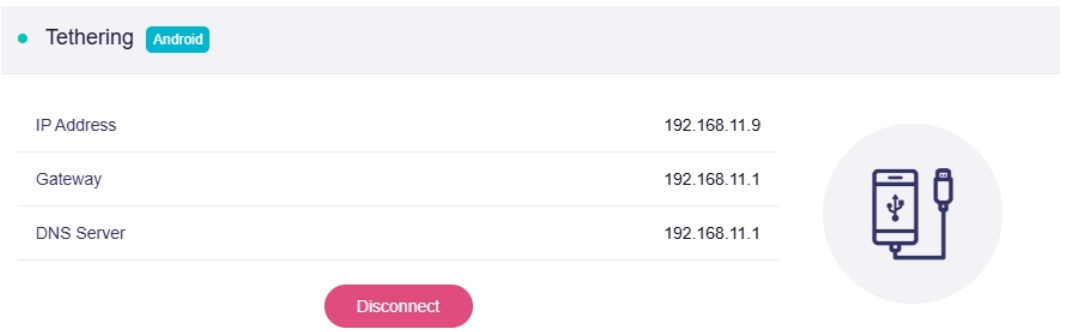
1. Reliez le téléphone Android au port USB du routeur avec un câble USB. Une boîte de dialogue peut afficher les préférences USB (USB preferences). Si vous y êtes invité, sélectionnez **Partage de connexion USB (USB Tethering)** ou **Transfert de fichiers (File Transfer)**.
2. Sur le téléphone, ouvrez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



Dépannage

Si le partage de connexion échoue, essayez les solutions suivantes :

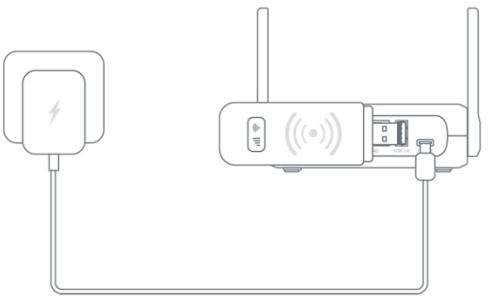
- Utilisez le bloc d'alimentation d'origine du routeur.
- Débranchez puis rebranchez le câble USB.
- Essayez un autre câble USB. Vérifiez qu'il permet le transfert de données, et pas seulement la recharge.

- 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.

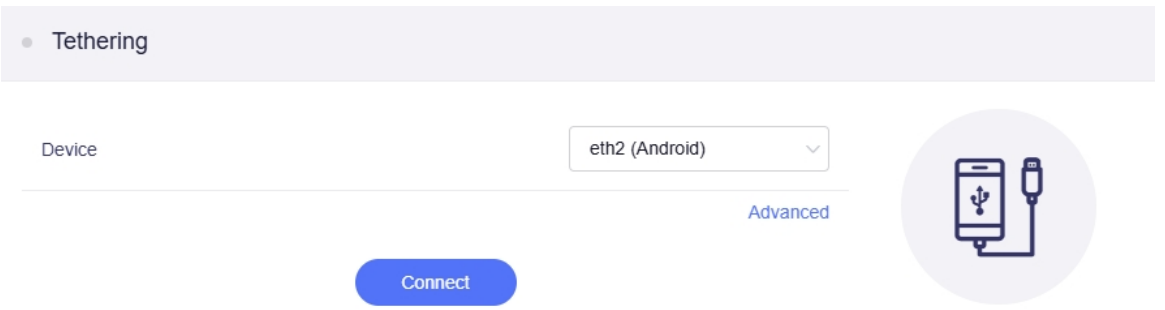
4.2.4 Connexion à Internet via un modem USB

Branchez un modem USB cellulaire au port USB du routeur pour le connecter à Internet. Le routeur utilise alors les réseaux 4G ou 5G sans dépendre d'un accès fixe à Internet. Cette méthode convient à une utilisation en véhicule ou en extérieur. La connexion est gérée par l'interface Partage de connexion (Tethering) ou Cellulaire (Cellular) du routeur.

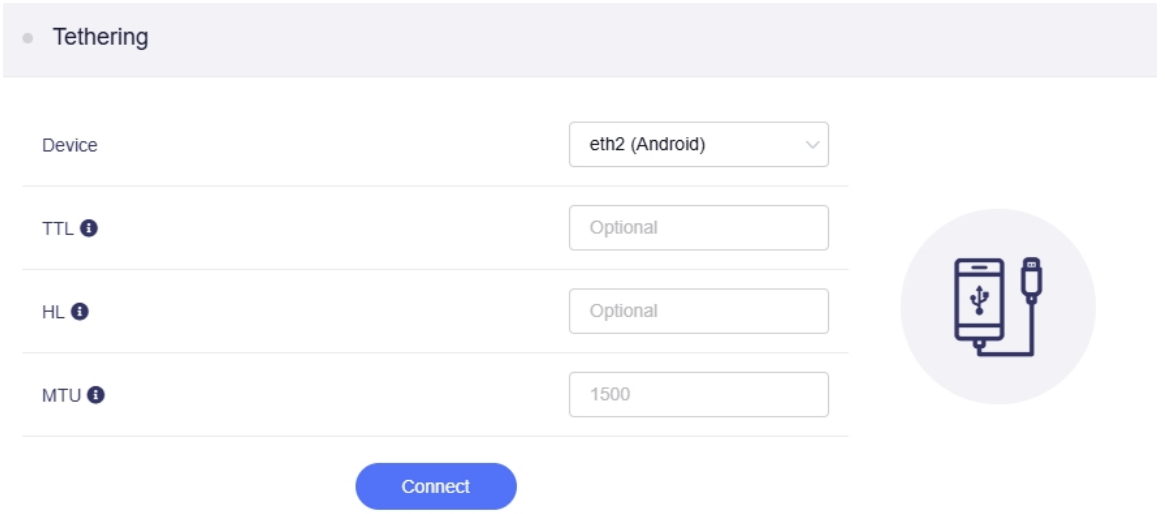


Suivez les étapes ci-dessous pour connecter le routeur à Internet via un modem USB.

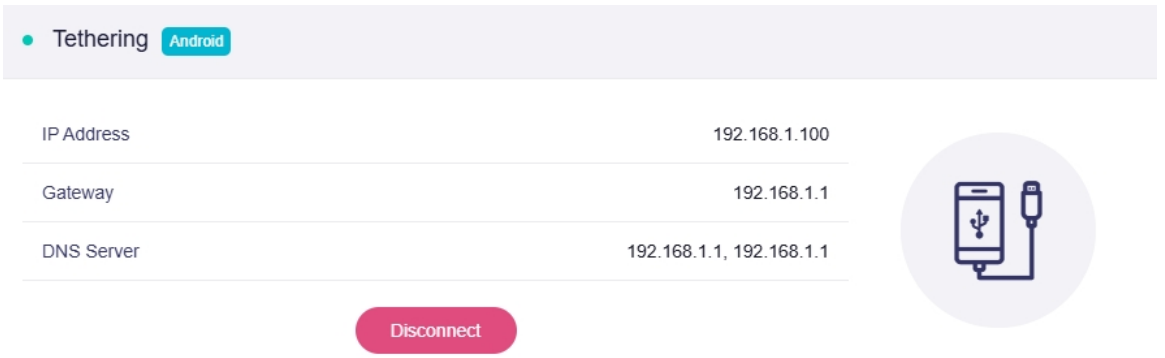
1. Avant d'allumer le routeur, branchez à son port USB un modem USB contenant une carte SIM.
2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Partage de connexion (Tethering)**. Cliquez sur **Connecter (Connect)**.



Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)** et ajustez-les avant de cliquer sur **Connecter (Connect)**.

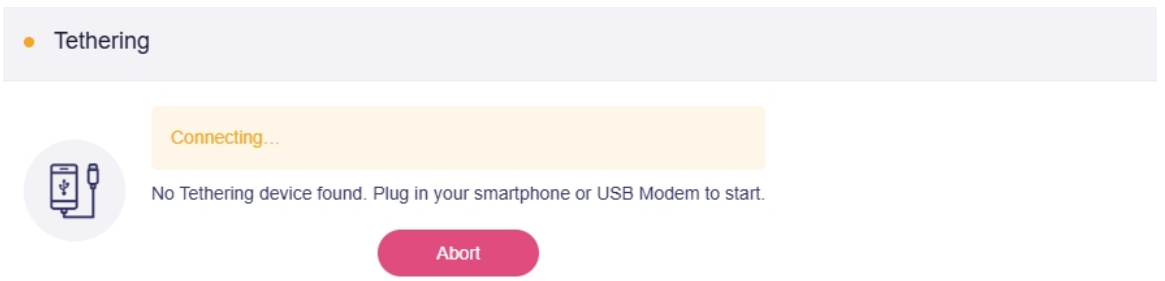


3. La connexion démarre. Une fois établie, cette page affiche les informations réseau.



Conseils :

1. Après la configuration initiale, si vous redémarrez le routeur en laissant le modem USB branché ou si vous rebranchez le modem, celui-ci est reconnu automatiquement. La connexion réseau s'établit sans avoir à cliquer de nouveau sur « Connecter ».
2. Si vous débranchez le modem USB, la page affiche « Aucun appareil de partage de connexion détecté » (No Tethering device found), comme ci-dessous. L'interface de partage de connexion reste à l'état « Connexion en cours » (Connecting).



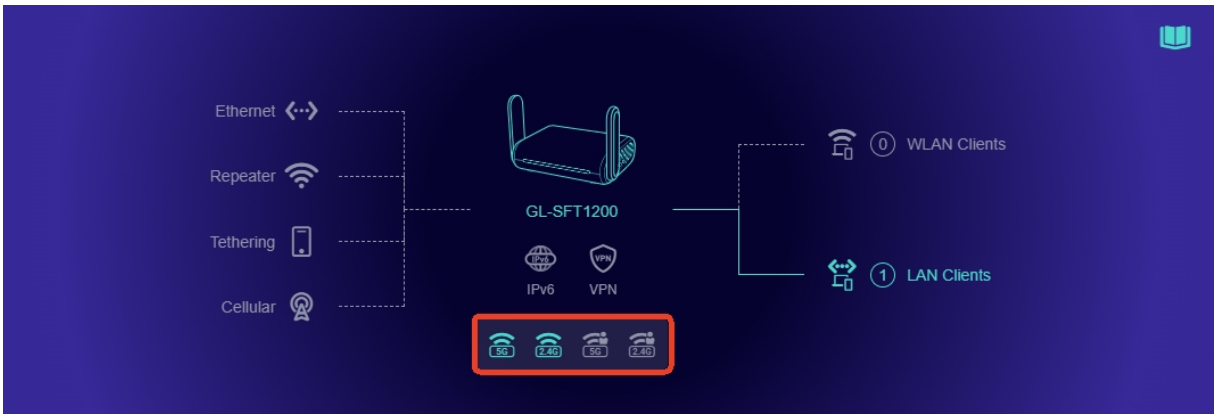
Chapitre 5

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 du modèle 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.



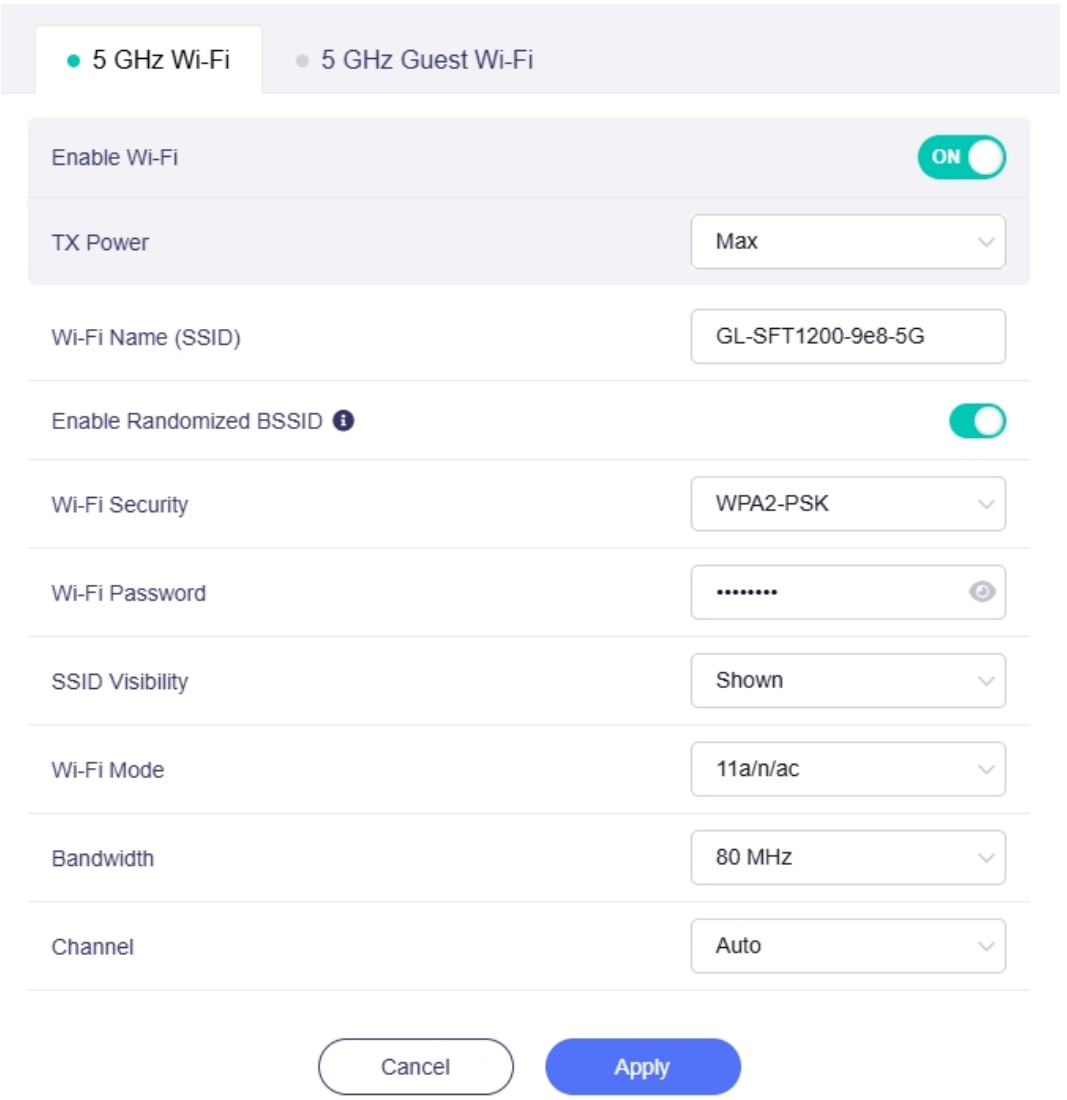
5.2 Paramètres sans fil

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

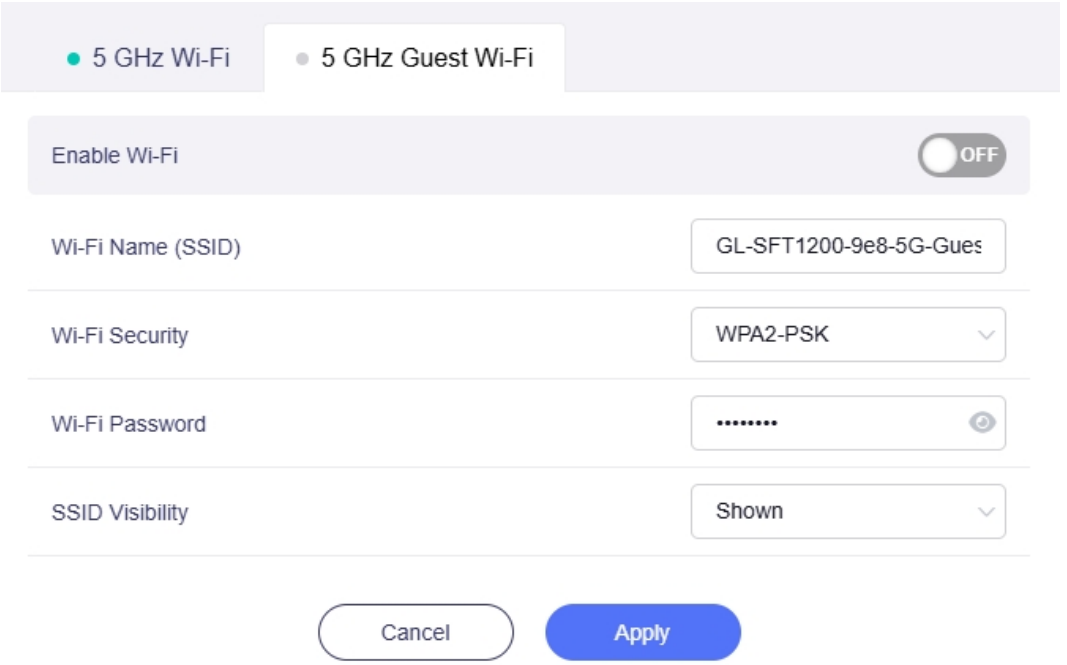
La page Sans fil affiche les paramètres Wi-Fi 2,4 GHz et 5 GHz du routeur. Chaque bande comprend un réseau principal et un réseau invité, que vous pouvez gérer séparément.

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.

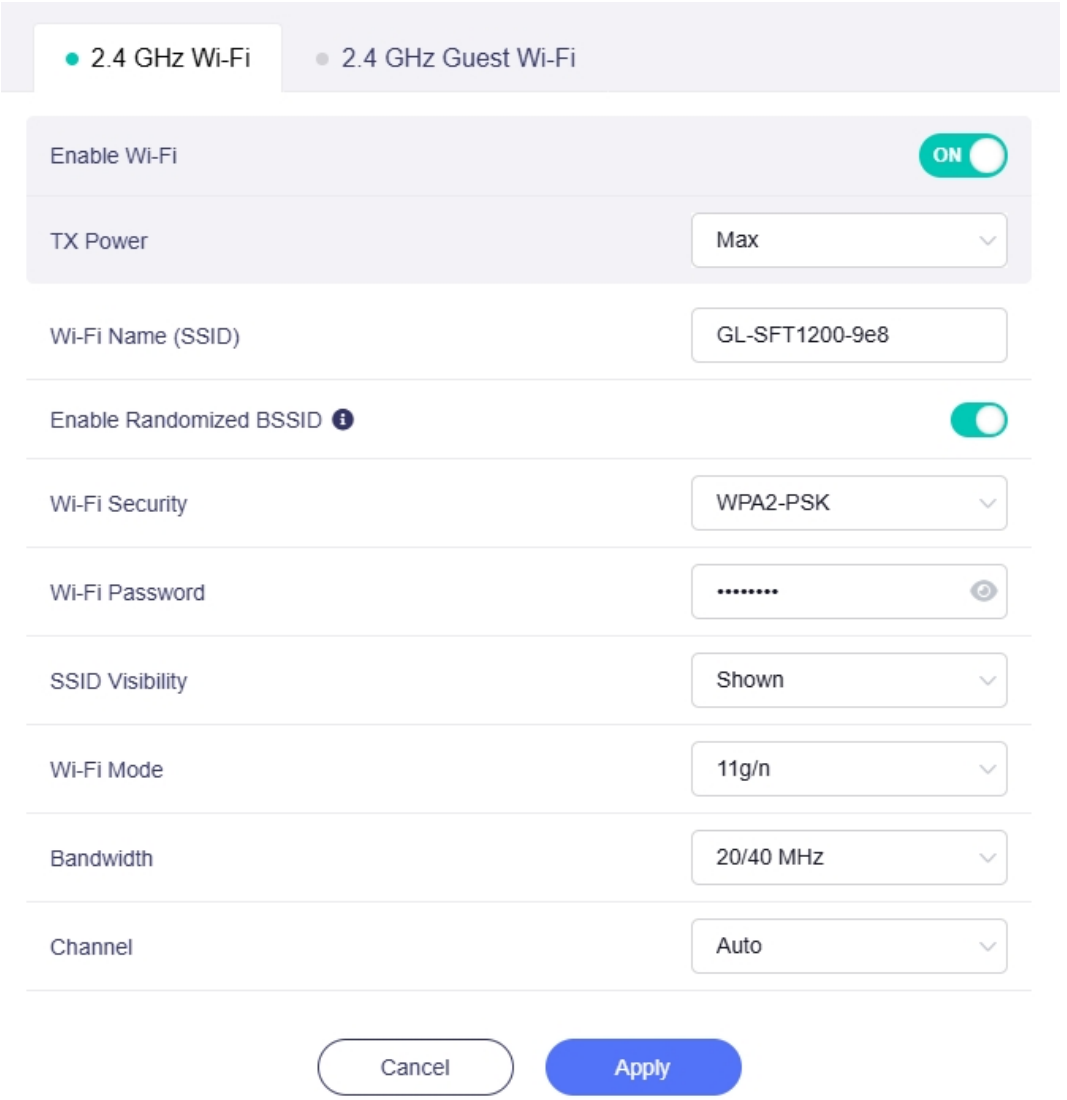


Remarque :

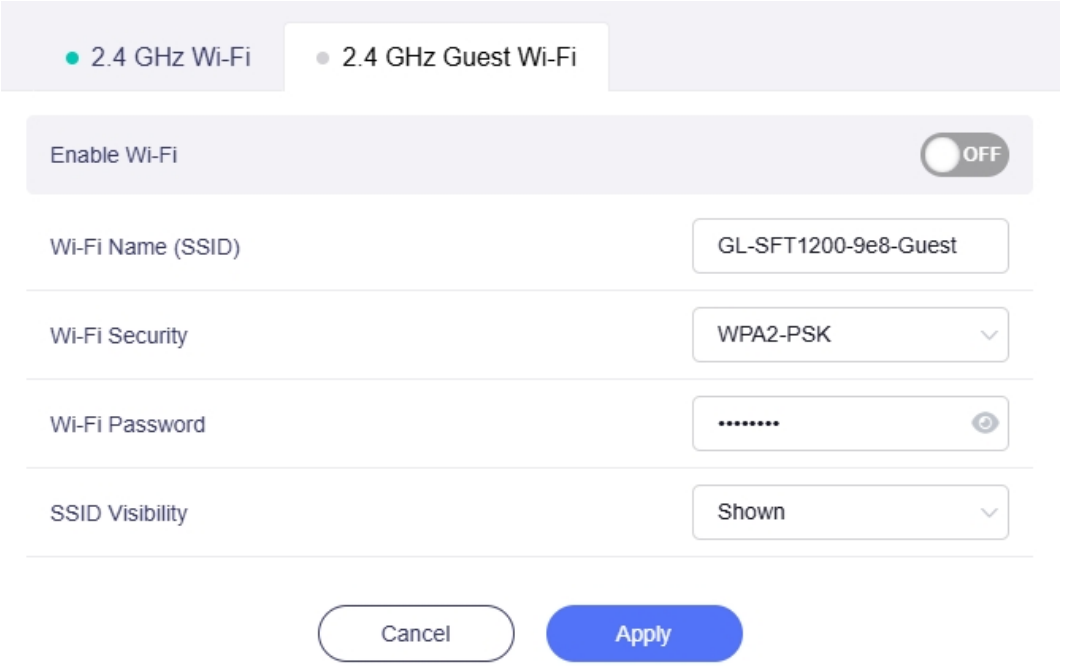
1. **Le BSSID aléatoire (Randomized BSSID)** est activé par défaut. Il vise à empêcher les fabricants d'appareils clients de collecter sur leurs serveurs les BSSID des réseaux Wi-Fi voisins et les coordonnées GPS des appareils clients.
2. Les paramètres **Largeur de canal (Bandwidth)** et **Canal (Channel)**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

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.

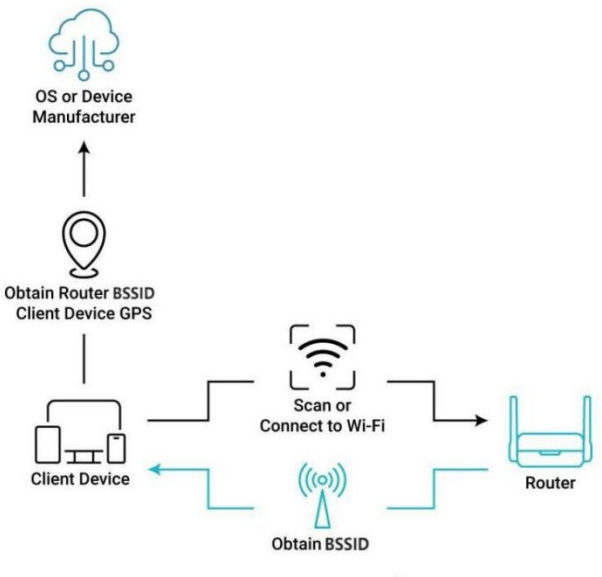
5.2.3 BSSID aléatoire

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.

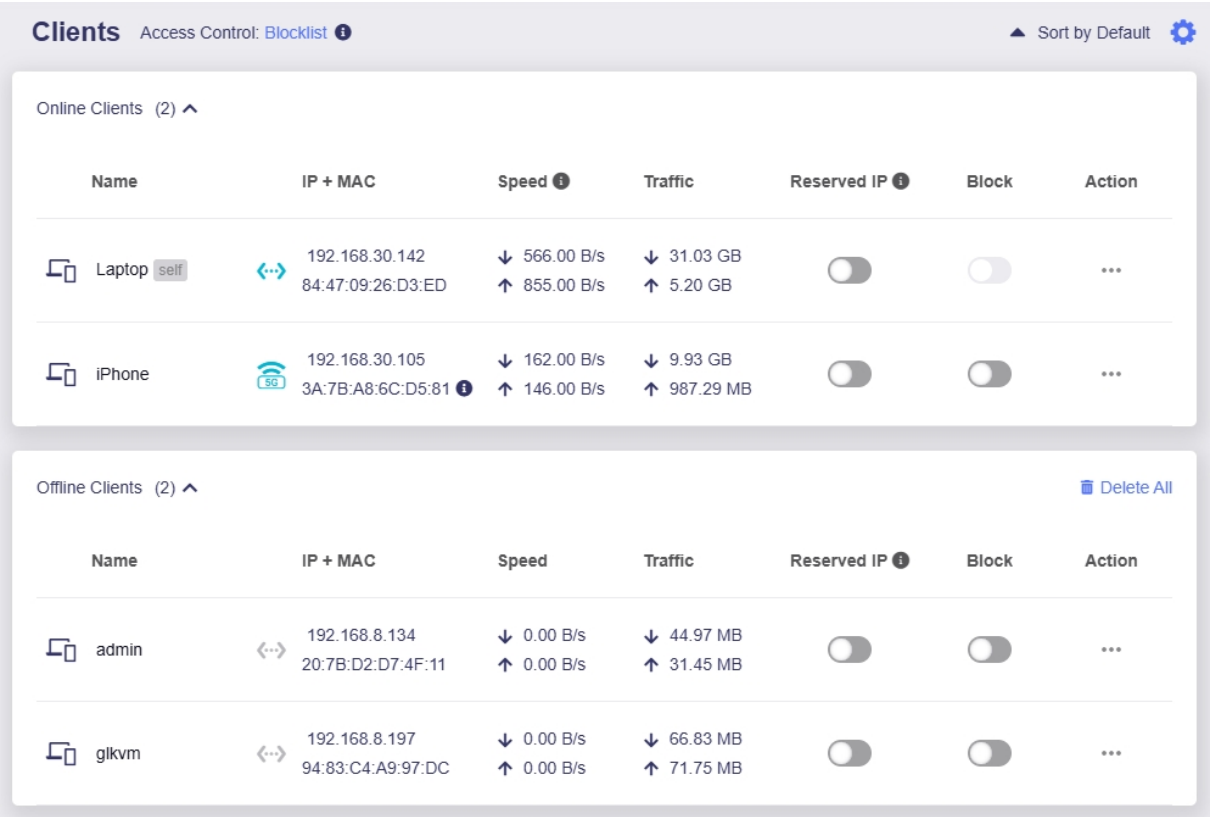
Chapitre 6

Appareils clients

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

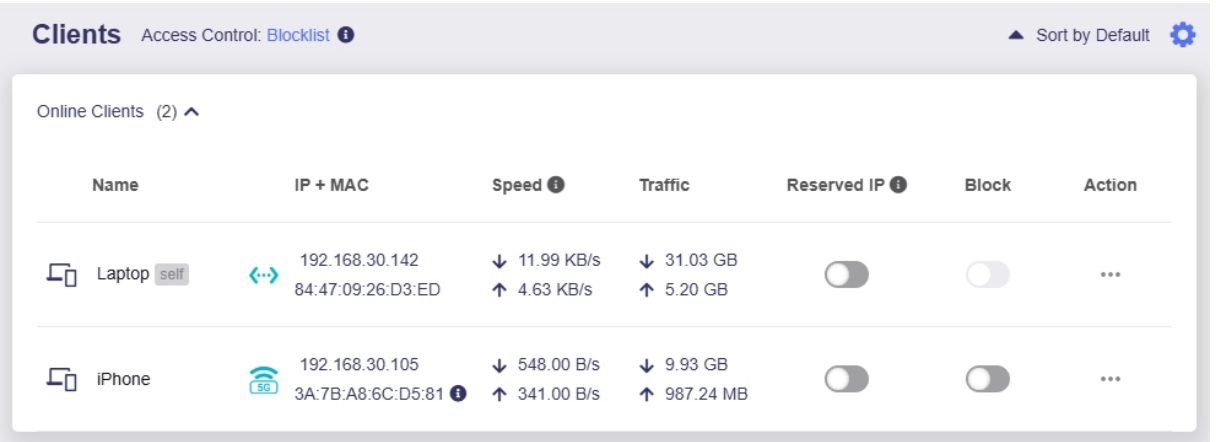
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **CLIENTS**.

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.



- **Clients en ligne (Online Clients)** : appareils actuellement connectés au réseau du routeur.
- **Clients hors ligne (Offline Clients)** : appareils déjà connectés au routeur auparavant, mais actuellement déconnectés.

6.1 Informations sur les appareils



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.

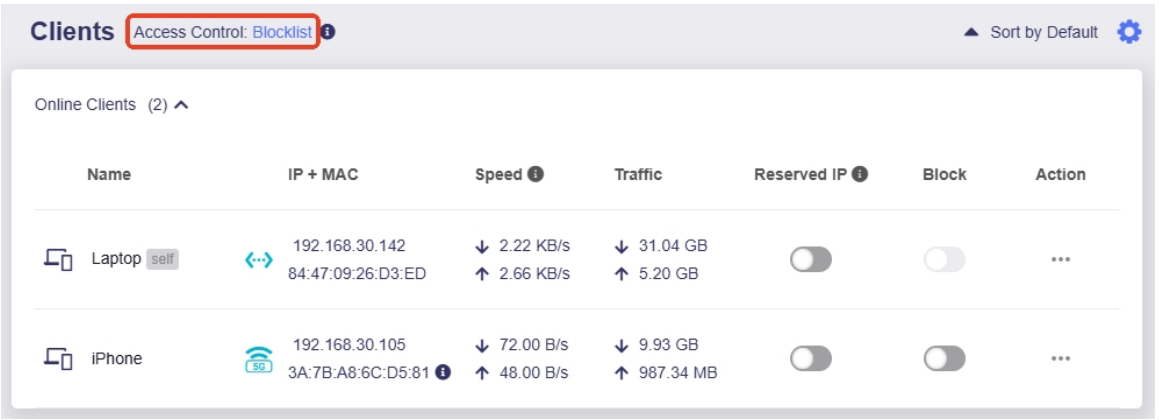
4. **Trafic** : la quatrième colonne affiche le trafic Internet de l'appareil connecté.

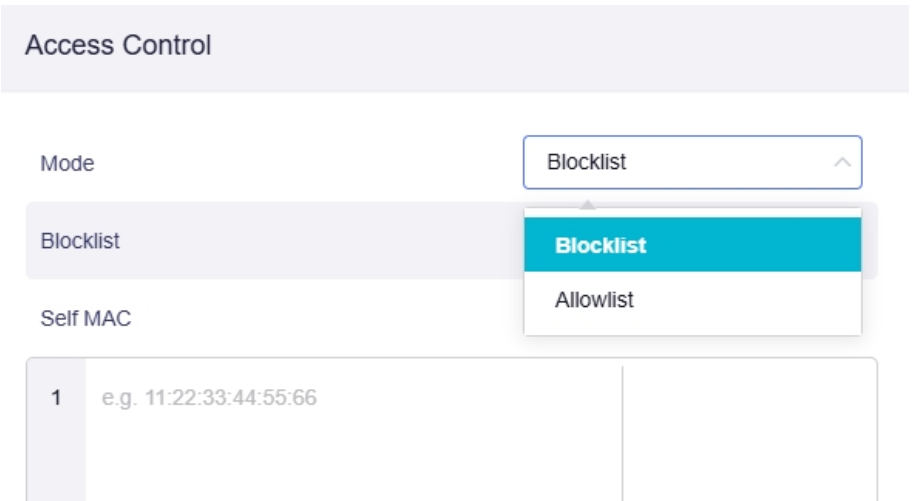
5. **Réserver une adresse IP**

   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.



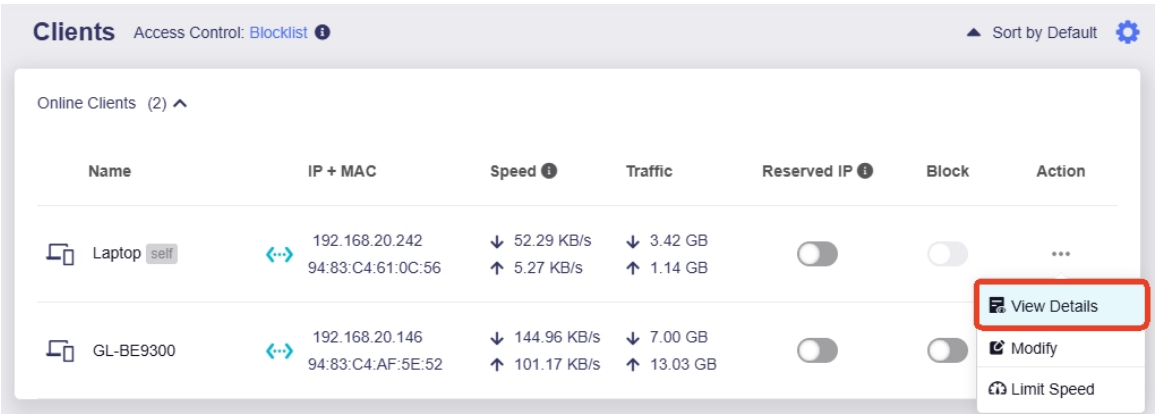


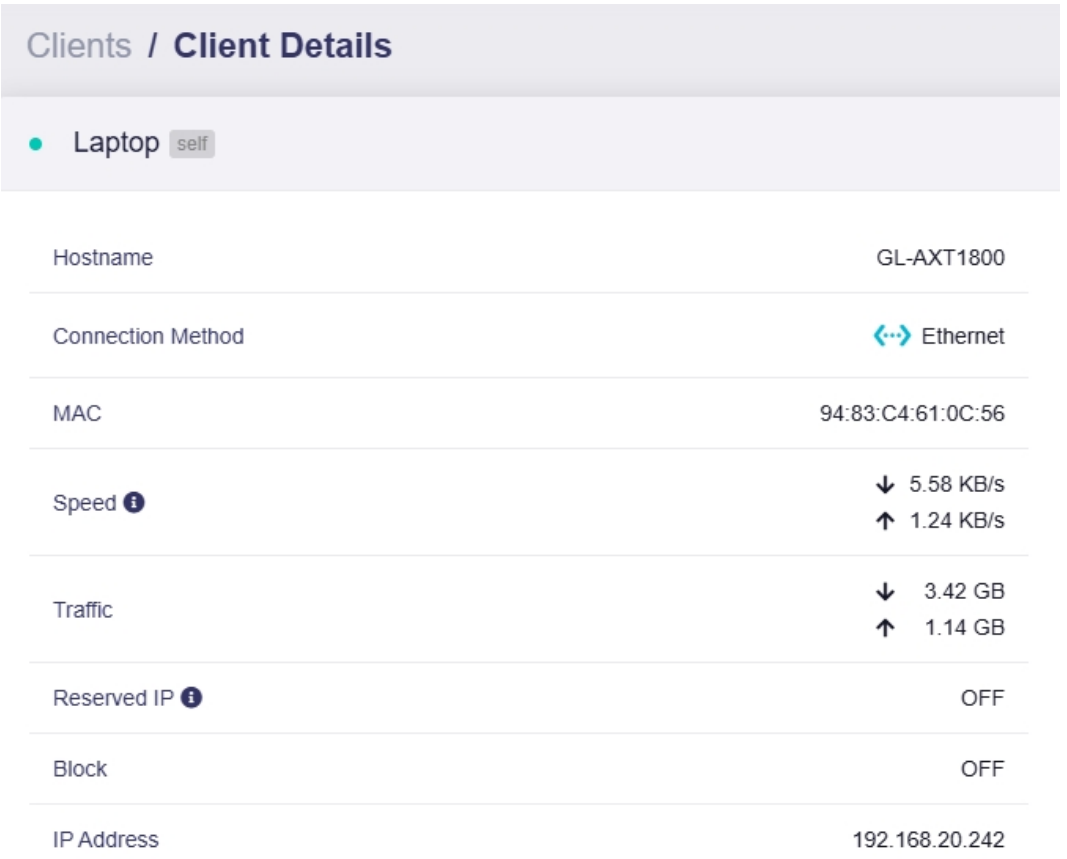
- **Liste de blocage (Blacklist)** : les appareils dont l'adresse MAC figure dans cette liste ne peuvent pas se connecter au routeur. Le blocage repose sur l'adresse MAC : un appareil bloqué peut donc se reconnecter s'il utilise une autre adresse MAC.
- **Liste d'autorisation (Allowlist)** : seuls les 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**

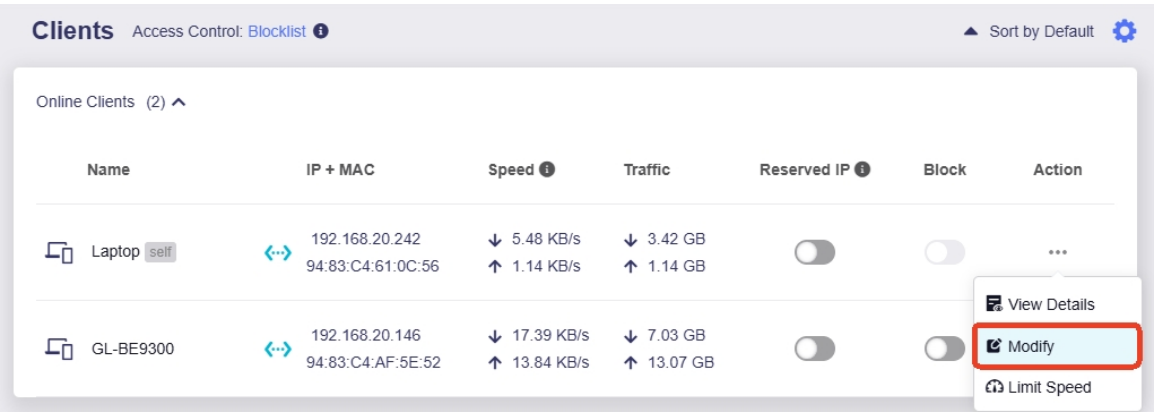
   Cliquez sur les trois points dans la colonne **Action**, puis sur **Afficher les détails (View Details)** dans le menu déroulant pour consulter les informations de l'appareil sur une seule page.

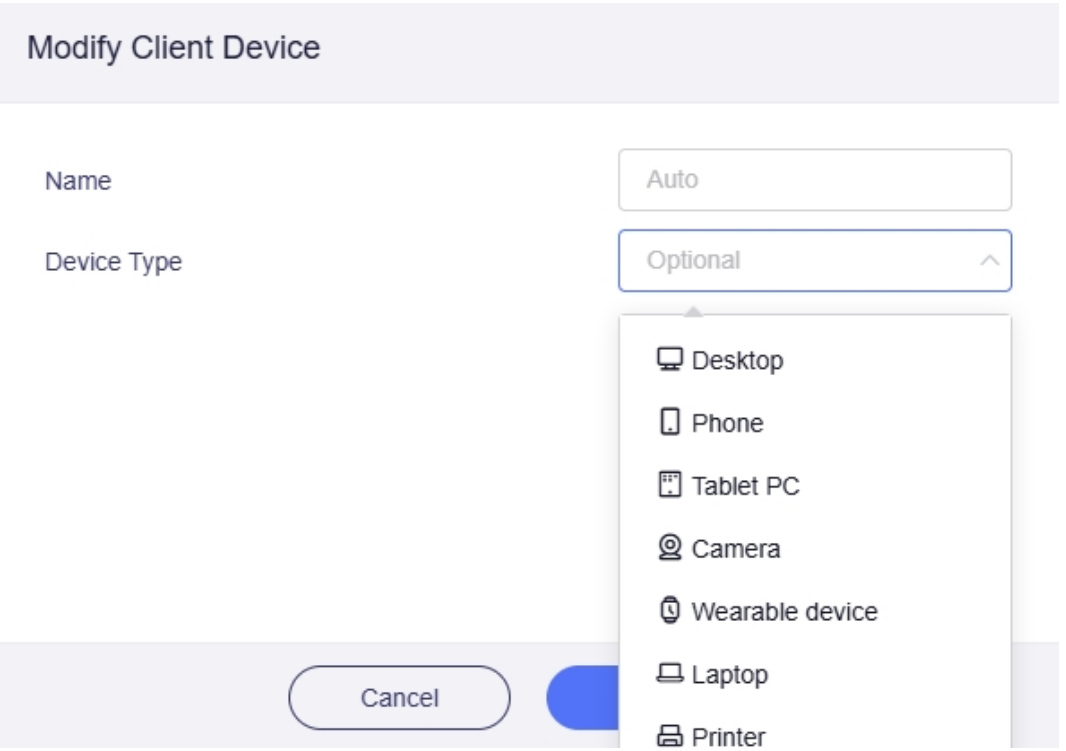




2. **Modifier**

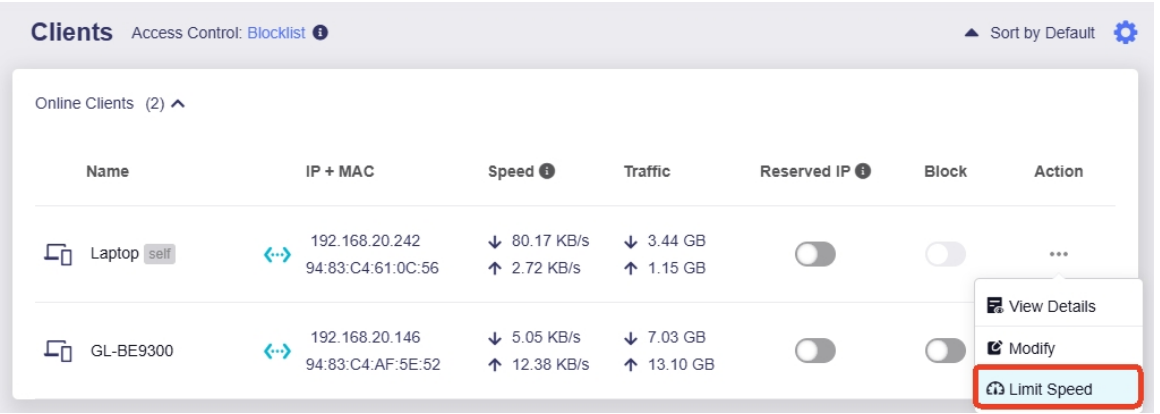
Cliquez sur les trois points dans la colonne **Action**, puis sur **Modifier (Modify)** dans le menu déroulant pour modifier le nom et le type de l'appareil.



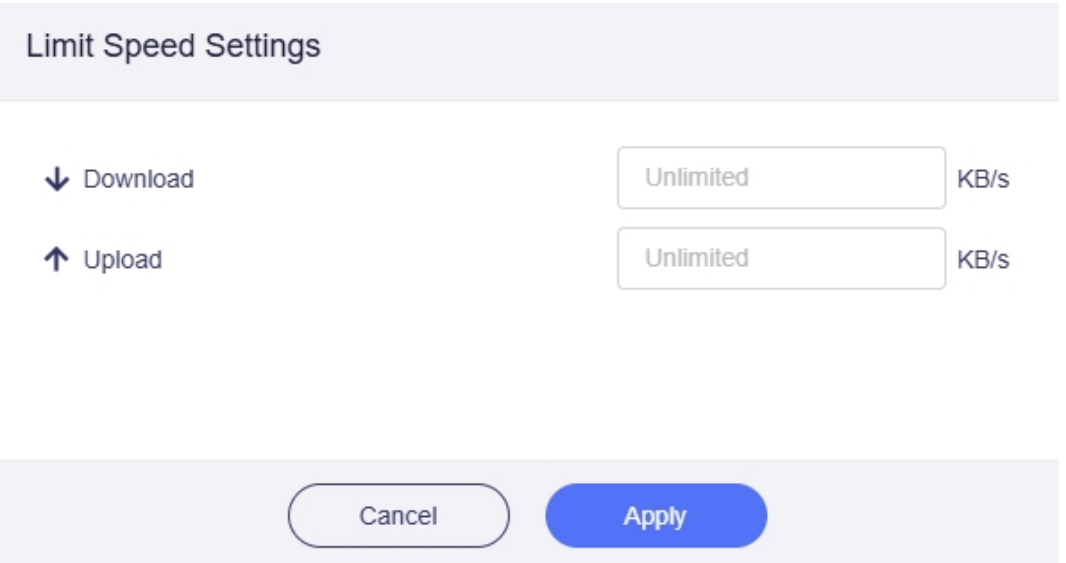


3. **Limiter le débit**

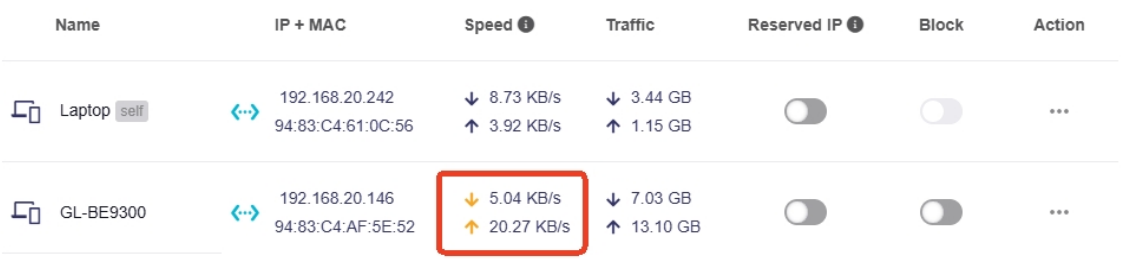
Cliquez sur les trois points dans la colonne **Action**, puis sur **Limiter le débit (Limit Speed)** dans le menu déroulant.



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



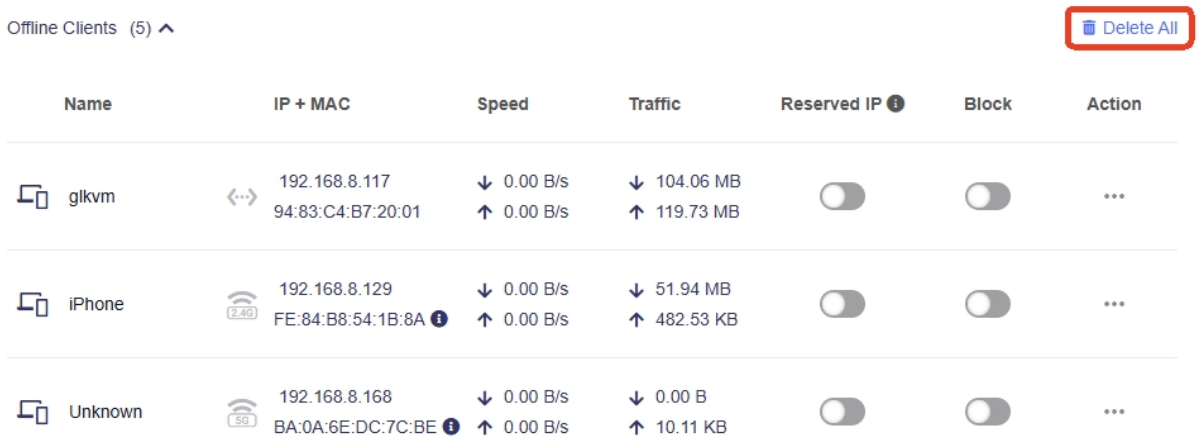
Lorsqu'une limite de débit est appliquée à un appareil, les flèches de débit montant et descendant deviennent jaunes.



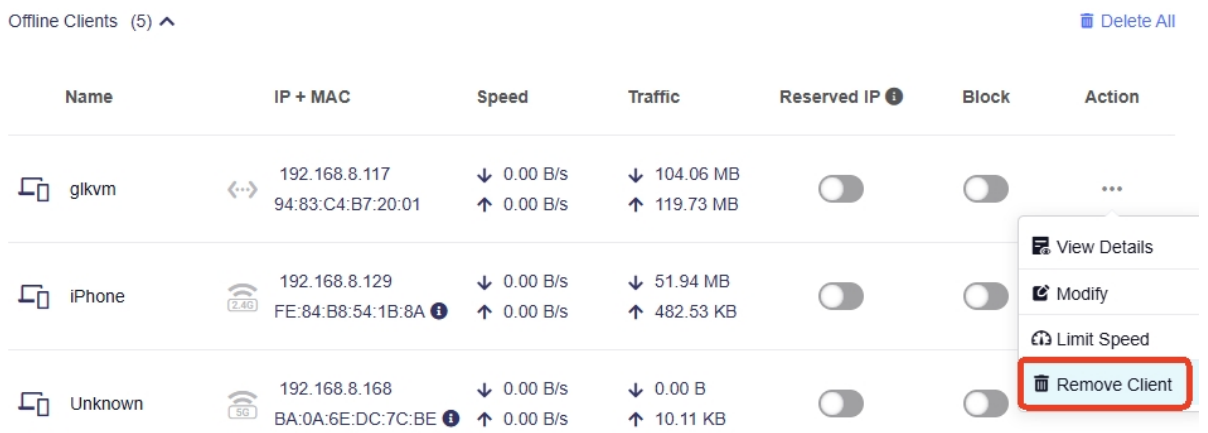
Conseil : si l’option Limiter le débit n’apparaît pas, ouvrez **RÉSEAU (NETWORK)** > **Accélération réseau (Network Acceleration)** et désactivez l’accélération. L’option Limiter le débit devient alors disponible.

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.

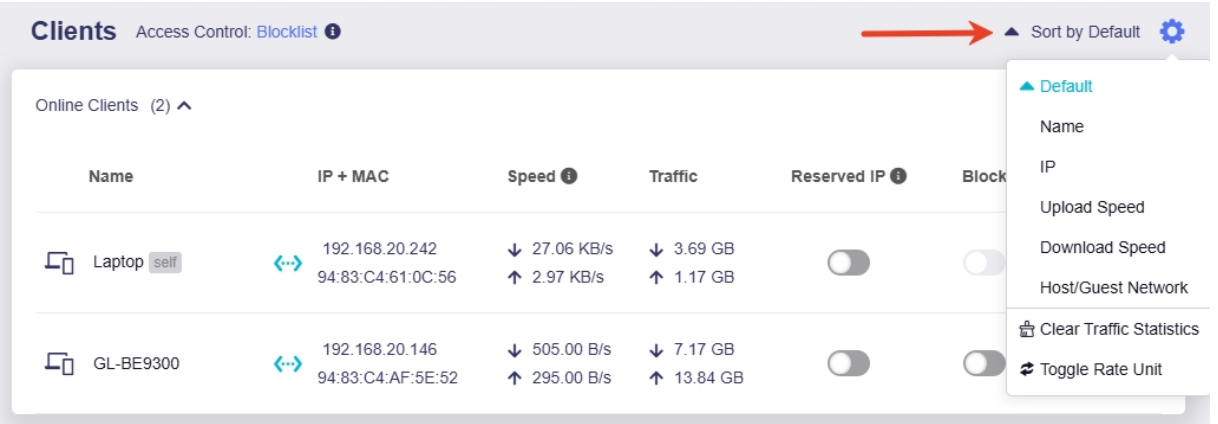


Pour supprimer un client précis, cliquez sur les trois points dans la colonne **Action**, puis sur **Supprimer le client (Remove Client)** dans le menu déroulant.



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.

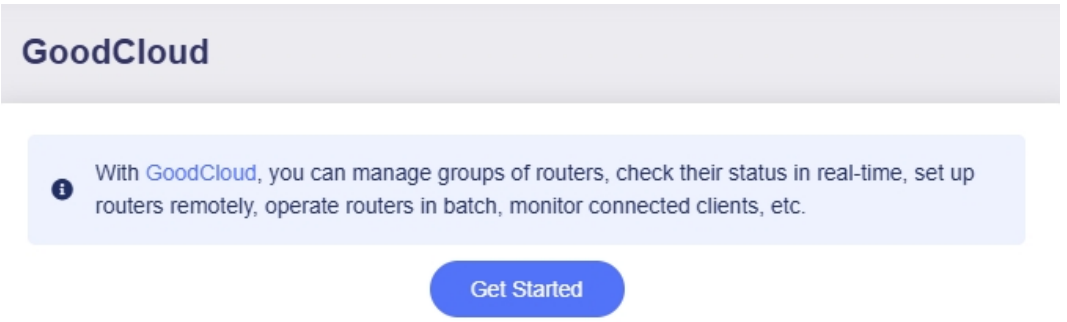
Avec GoodCloud, vous pouvez :

- 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

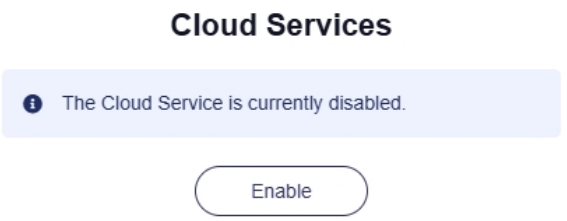
Certaines fonctions sont proposées dans les offres Enterprise et VAR (Value Added Reseller, revendeur à valeur ajoutée). Consultez cette page pour en savoir plus.

7.1.1 Activation de GoodCloud

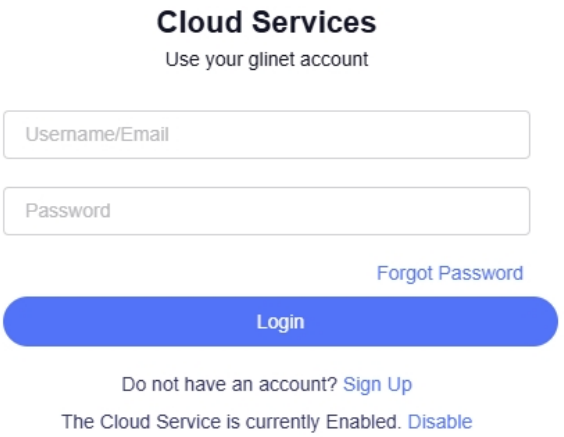
1. Connectez-vous à l'interface d'administration Web, ouvrez **SERVICE CLOUD (CLOUD SERVICE)** > **GoodCloud**, puis cliquez sur **Commencer (Get Started).**



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



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

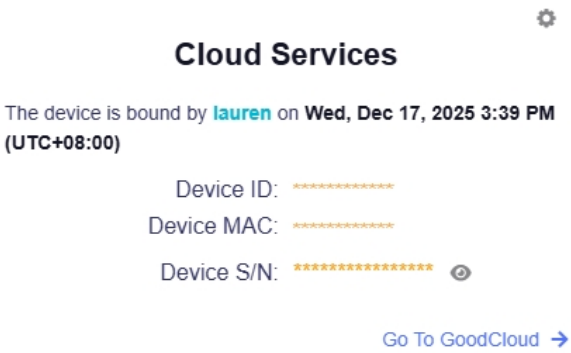


Conseils :

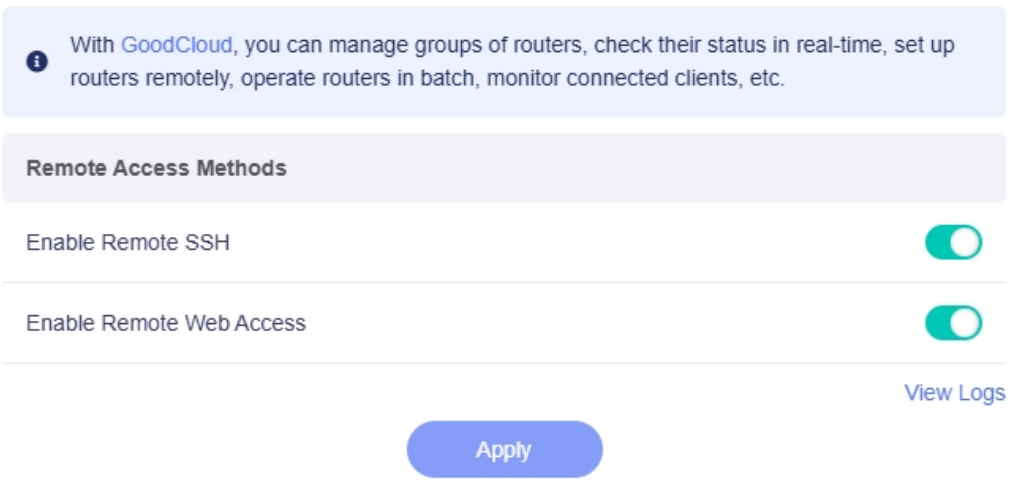
- La procédure d'association à GoodCloud varie selon la version du micrologiciel.

- 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. Cette fonction facilite la gestion à distance, la configuration réseau et le dépannage. Vous pouvez activer ou désactiver cet accès ici.



- **SSH à distance (Remote SSH)** : accédez au terminal du routeur depuis GoodCloud via SSH.
- **Accès Web à distance (Remote Web Access)** : accédez à l'interface d'administration Web du routeur depuis GoodCloud via HTTP ou HTTPS.

- **Afficher les journaux (View Logs)** : ouvre la page Journal et affiche le journal Cloud.

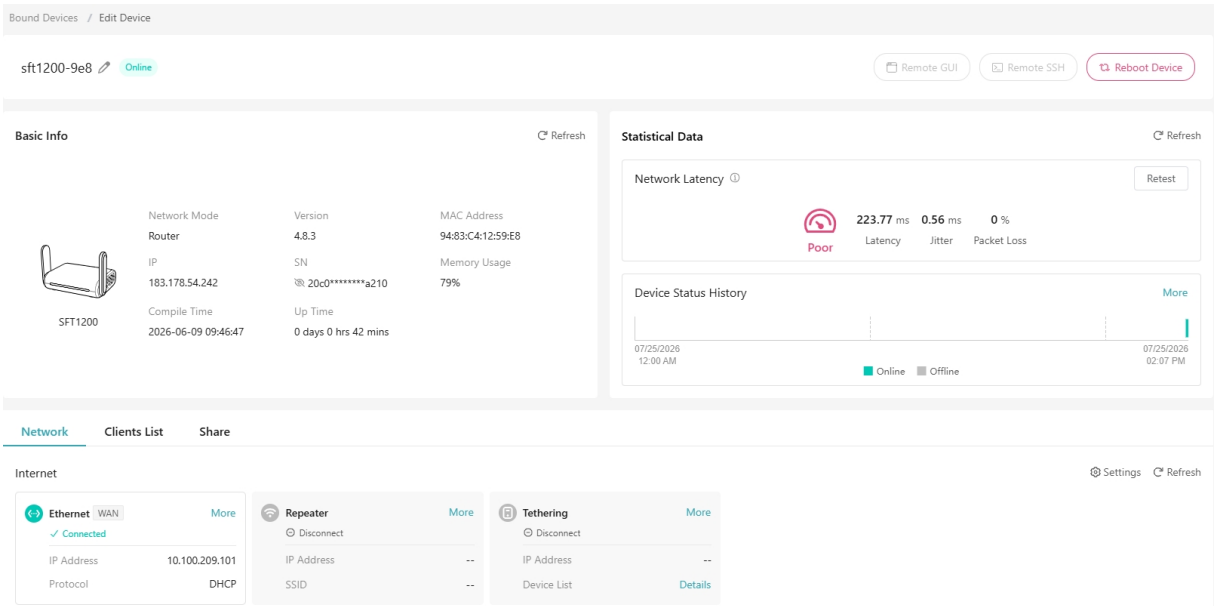
7.1.2 Gestion de votre routeur

Consultation des informations 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.

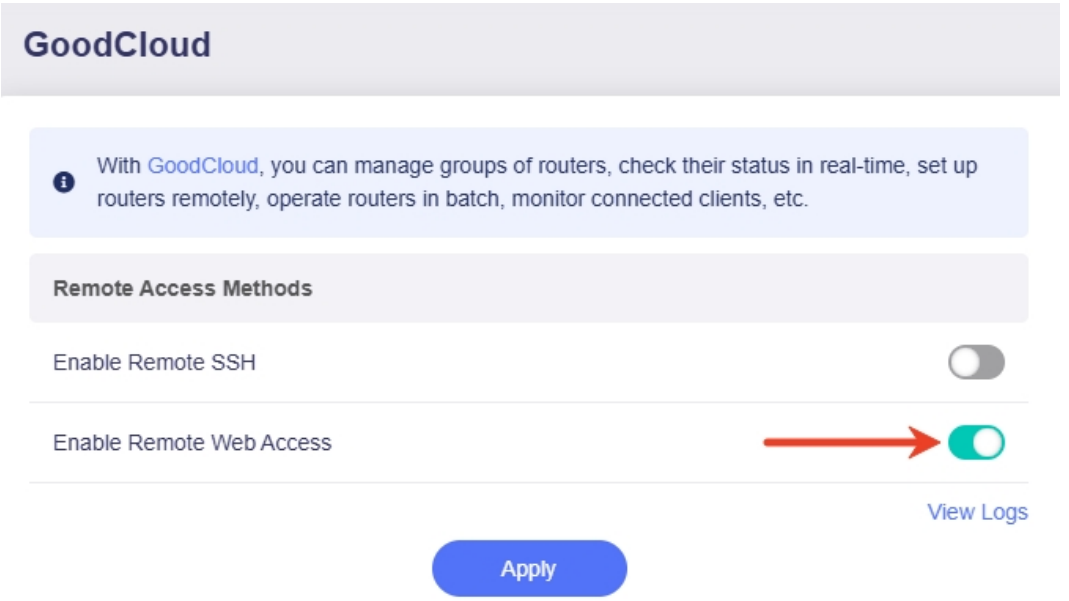


Cliquez sur le nom de l’appareil pour ouvrir sa page de détails. Elle présente les informations de base, les statistiques, la vue d’ensemble du réseau, la liste des clients et la chronologie. Vous pouvez également effectuer des opérations avancées, comme accéder au routeur à distance ou le redémarrer.

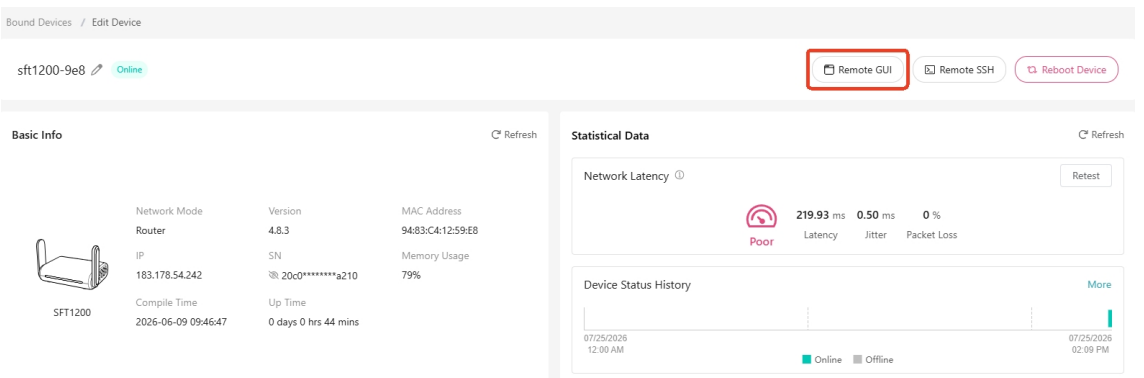


Accès Web à distance

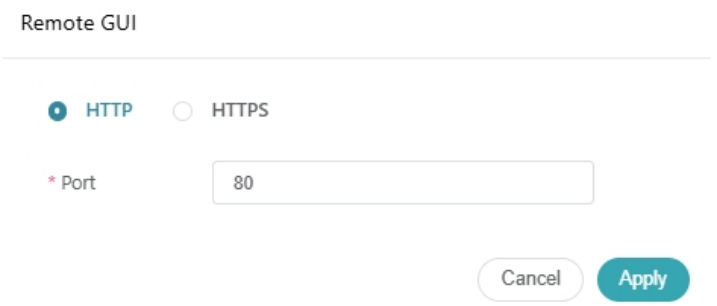
1. Dans l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud**, activez **Accès Web à distance (Remote Web Access)**, puis cliquez sur **Appliquer (Apply)**.



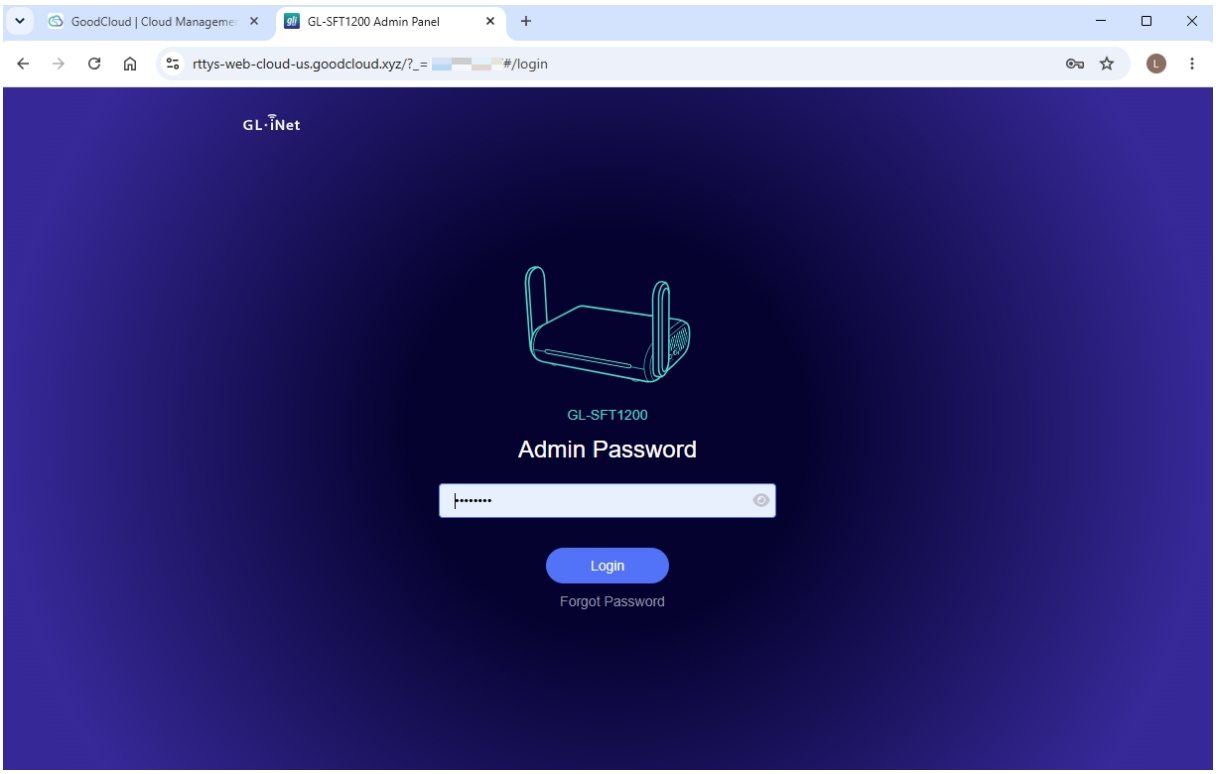
2. Connectez-vous à GoodCloud et ouvrez **Appareil (Device)** > **Appareils associés (Bound Devices)**. Cliquez sur l'appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
3. Sur cette page, cliquez sur le bouton **Interface à distance (Remote GUI)** dans l'angle supérieur droit.



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)**.

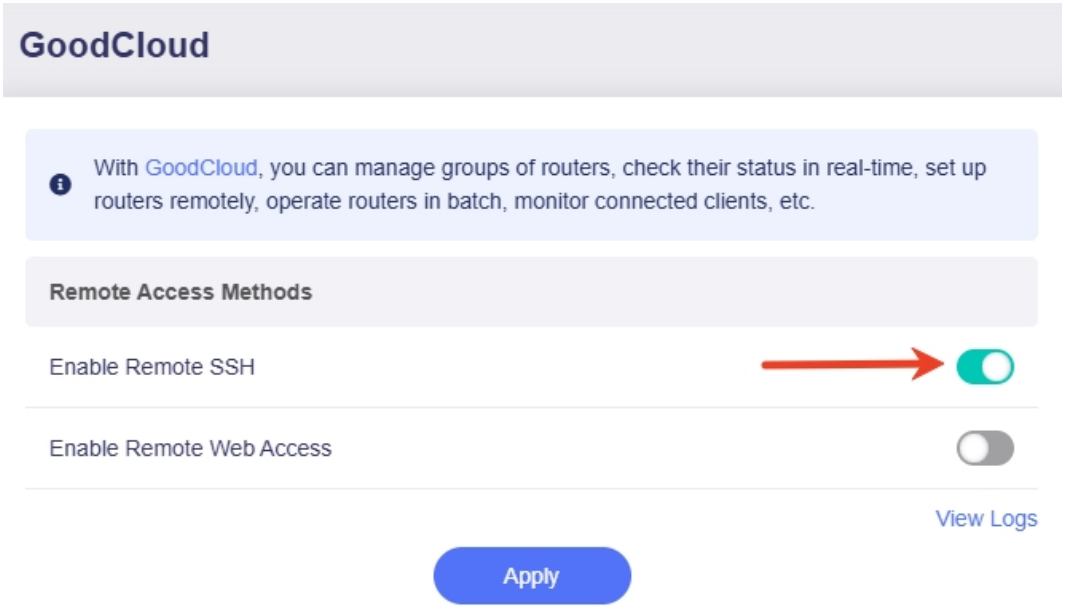


5. La page de connexion du routeur s’ouvre. Saisissez le mot de passe administrateur pour accéder à distance à l’interface d’administration Web.

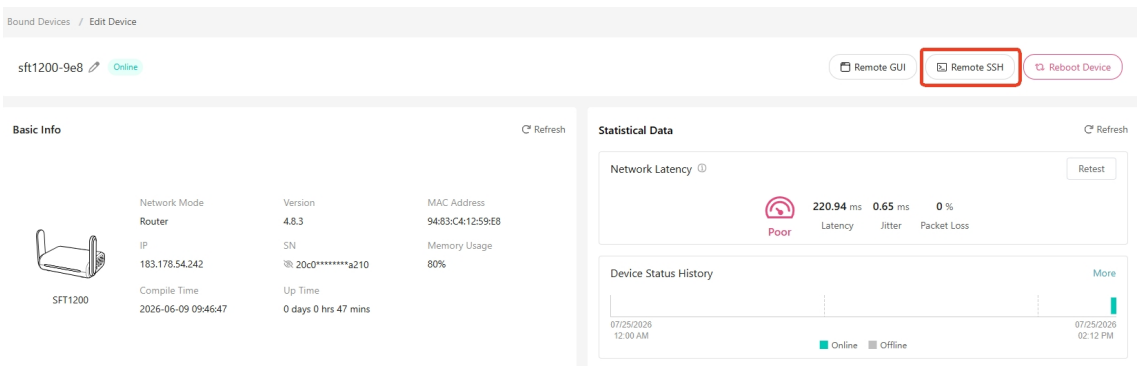


SSH à distance

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.

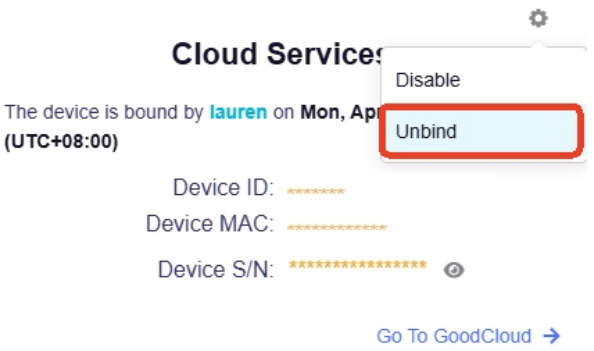


4. Connectez-vous avec l'identifiant **root** et saisissez le mot de passe pour accéder au terminal du routeur.

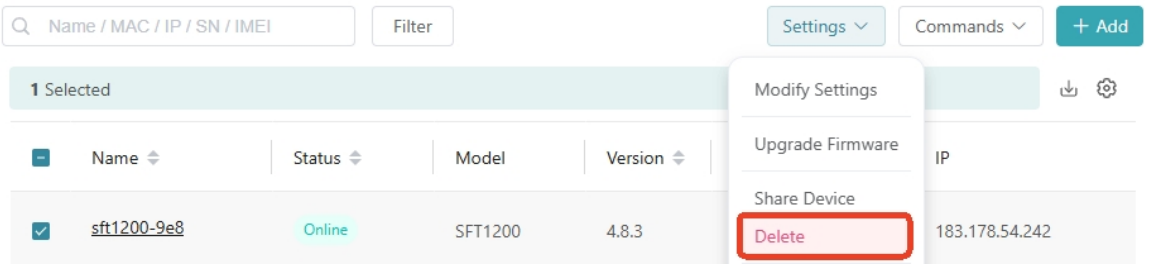

GL-SFT1200 login: root
Password:
BusyBox v1.29.3 () built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 18.06, LEDE
root@GL-SFT1200:~#

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.

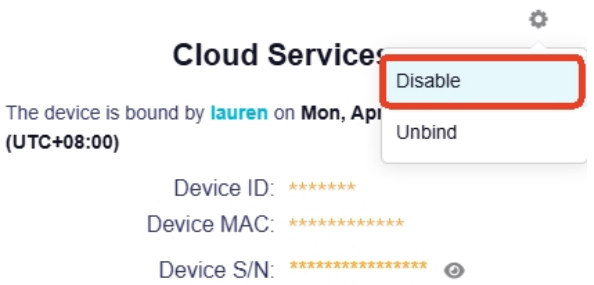


Vous pouvez également vous connecter à la plateforme Cloud et ouvrir **Appareil (Device)** > **Appareils associés (Bound Devices)**. Sélectionnez l’appareil à dissocier, cliquez sur **Paramètres (Settings)** dans l’angle supérieur droit, puis sélectionnez **Supprimer (Delete)**. L’appareil est alors 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 facilite la mise en réseau et la gestion des appareils à distance.

Conçu pour s’intégrer aux routeurs GL.iNet, AstroWarp permet de gérer les appareils sur l’ensemble du réseau, en amont comme en aval.

Grâce à une gestion globale du réseau et à la prise en charge prévue du contrôle au niveau matériel, AstroWarp offre une solution robuste et fiable pour gérer les appareils et maintenir des réseaux stables et sécurisés.

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

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.

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.

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.

WireGuard

WireGuard est un protocole VPN léger et rapide, plus simple et plus efficace qu'OpenVPN. Il utilise une cryptographie moderne et une base de code réduite, qui facilite l'audit et renforce la sécurité. Ses algorithmes ChaCha20 et Poly1305 assurent le chiffrement et l'intégrité des données.

8.2 Cas d’utilisation

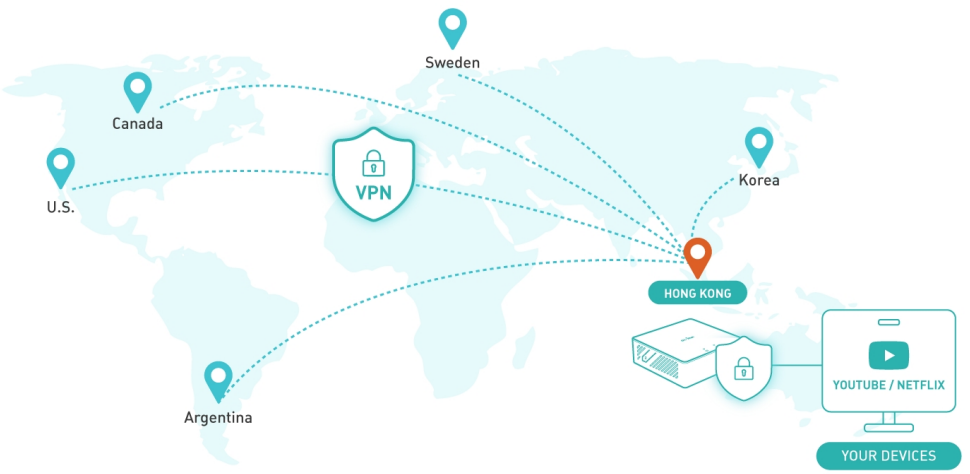
1. **Protection des données personnelles**

   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.



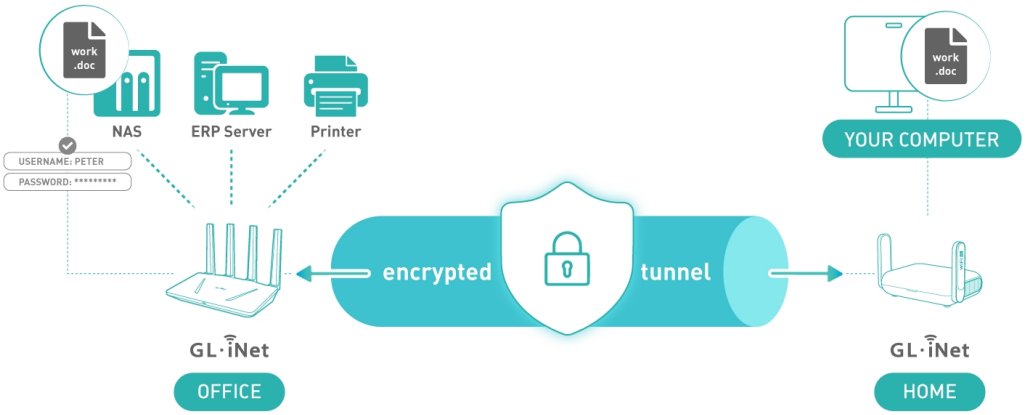
2. **Accès aux contenus depuis le monde entier**

   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.



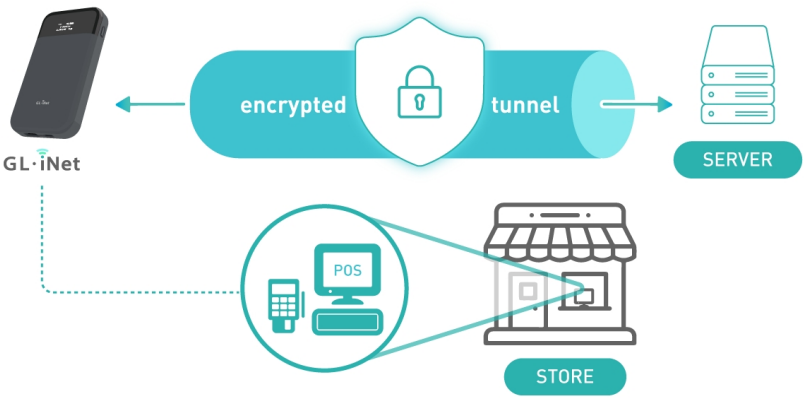
3. **Sécurité des données des petites entreprises**

   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

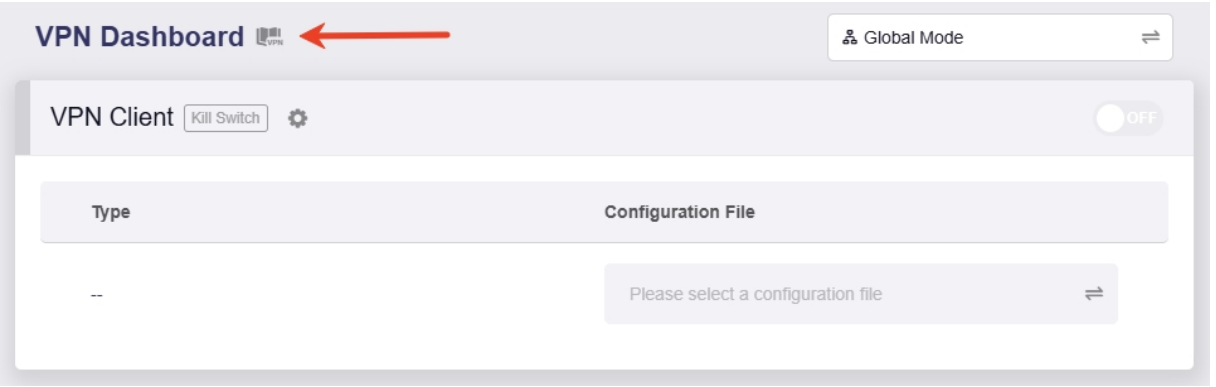
Ce chapitre explique comment gérer les connexions VPN depuis l’interface d’administration Web.

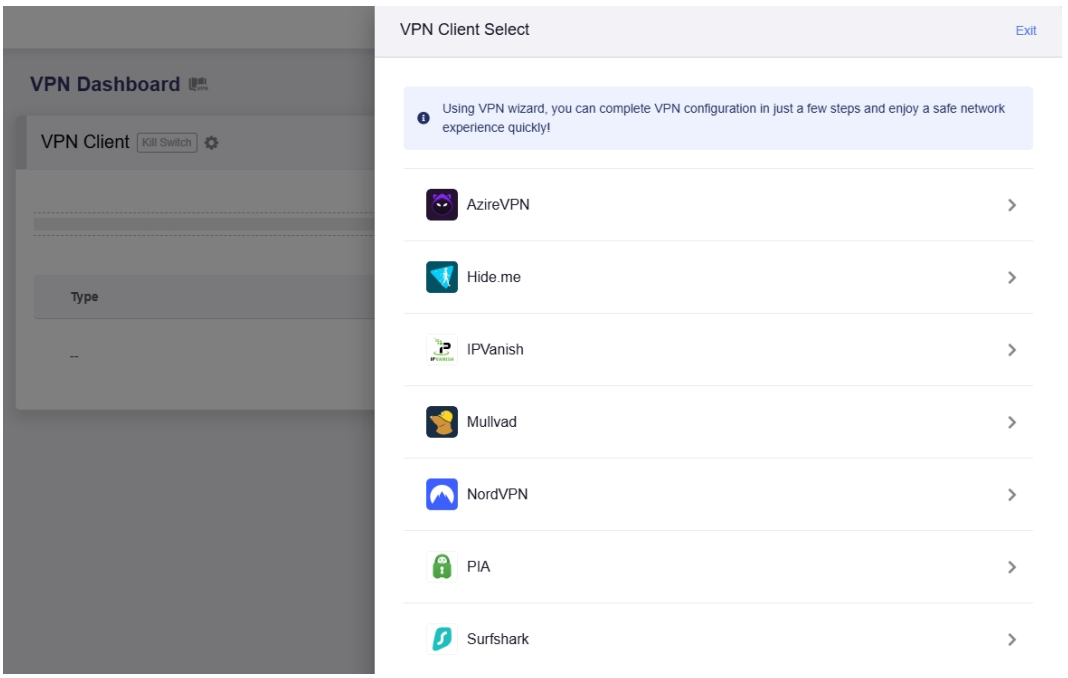
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Tableau de bord VPN (VPN Dashboard)**.

Lorsque le routeur fonctionne comme client VPN, le tableau de bord affiche les règles du tunnel, l'adresse du serveur, les statistiques de trafic, l'adresse IP virtuelle du client et le journal de connexion. Vous pouvez également régler les paramètres avancés, comme le coupe-circuit VPN (Kill Switch), le masquage IP et la 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.



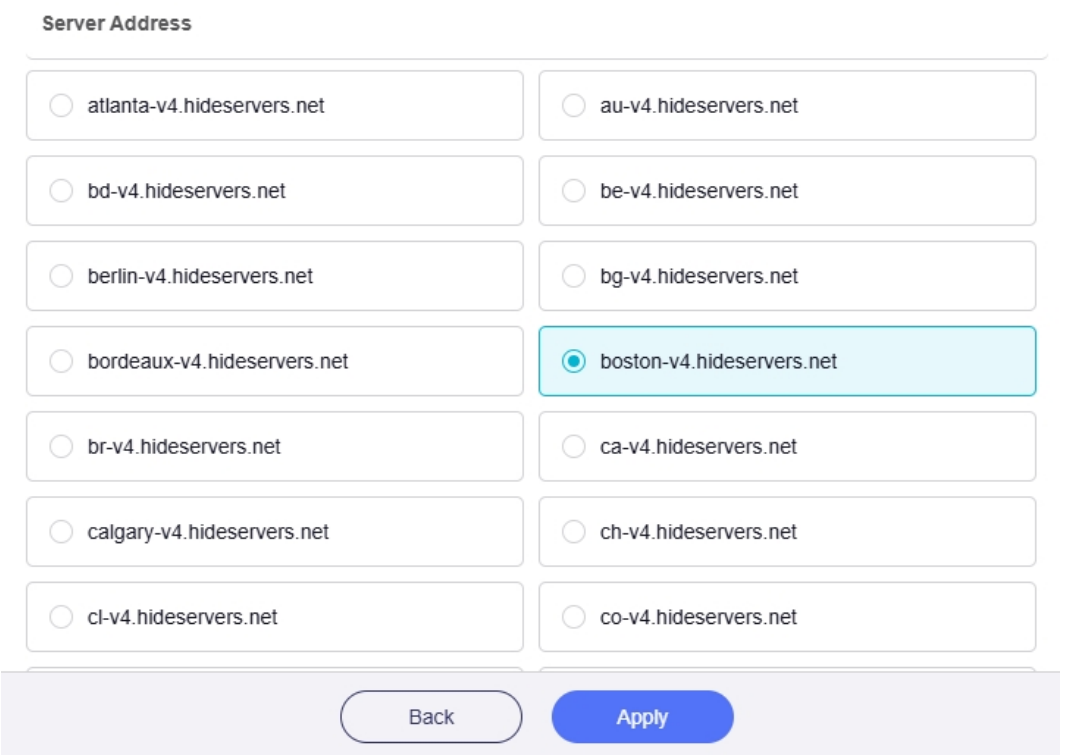


Remarque : l'assistant prend uniquement en charge les services VPN intégrés : AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA et Surfshark. Pour un autre fournisseur, ignorez l'assistant et ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** ou **Client WireGuard (WireGuard Client)** pour effectuer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

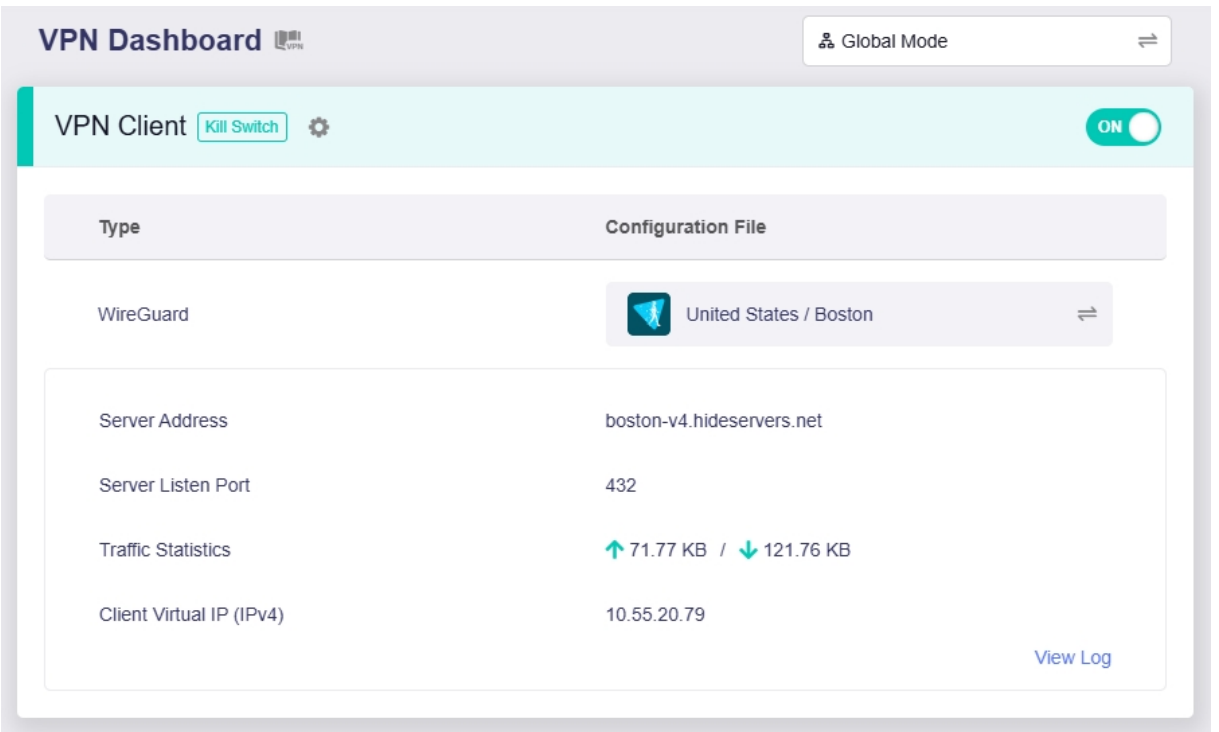
Voici un exemple avec **Hide.me**. Connectez-vous avec vos identifiants Hide.me.



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

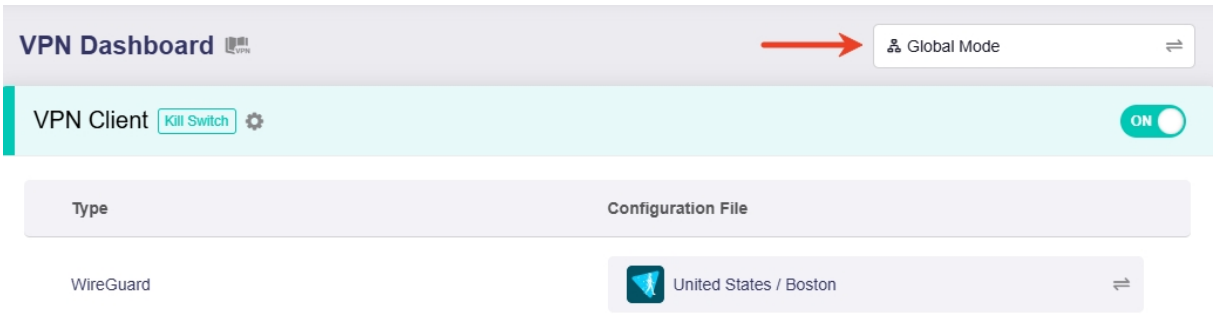


La connexion s'établit automatiquement. Ouvrez ensuite le **Tableau de bord VPN (VPN Dashboard)**. Le tunnel activé affiche le protocole VPN, par exemple WireGuard, le fichier de configuration, l'adresse et le port d'écoute du serveur, les statistiques de trafic et l'adresse IP virtuelle du client. Vous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

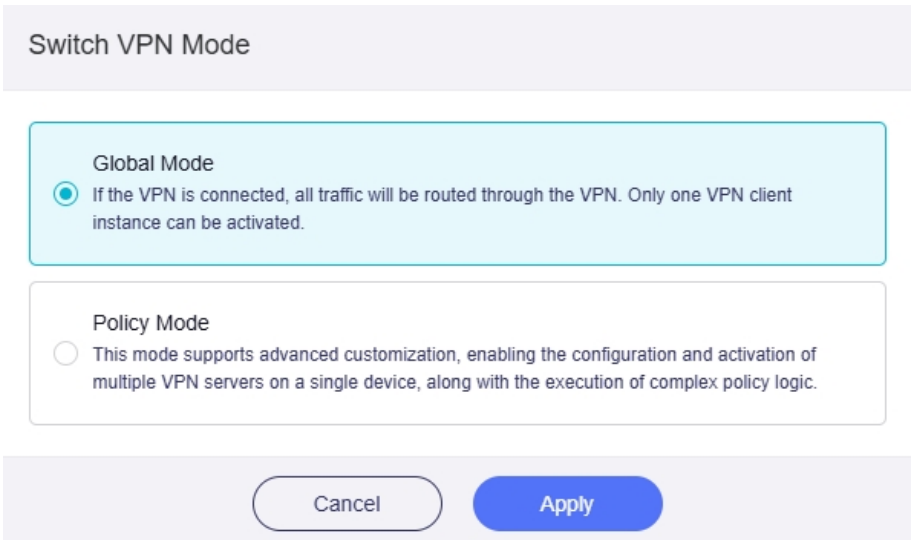


9.2 Mode VPN

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



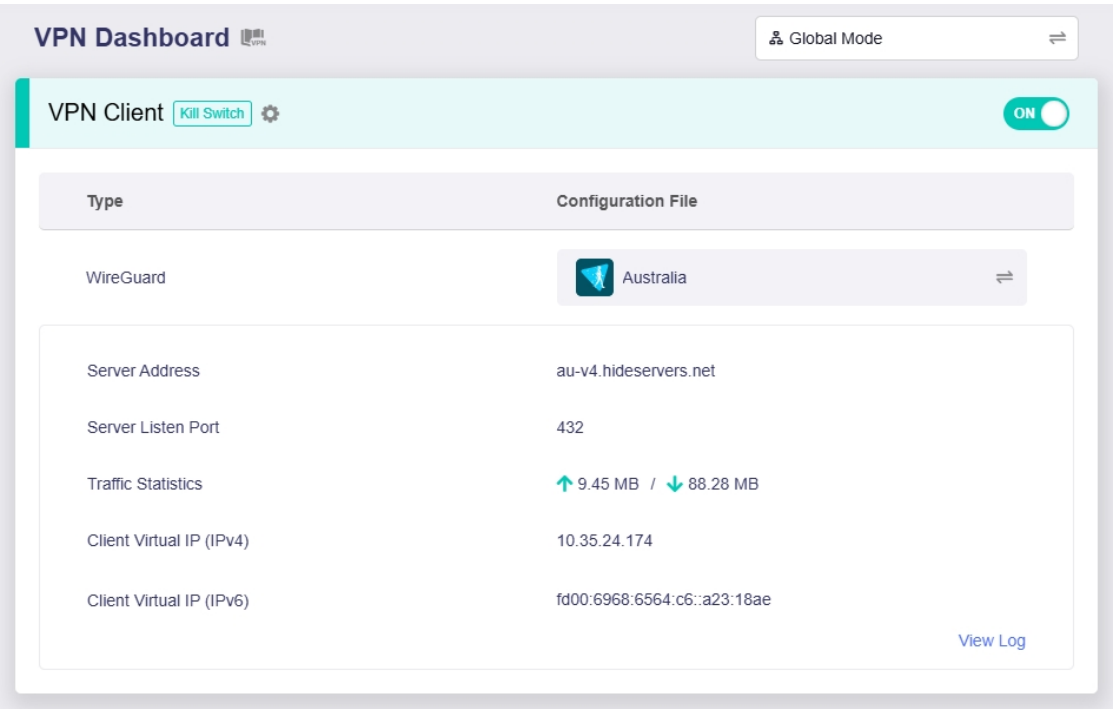
Deux modes sont disponibles : **Mode global (Global Mode)** et **Mode par règles (Policy Mode)**.



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.

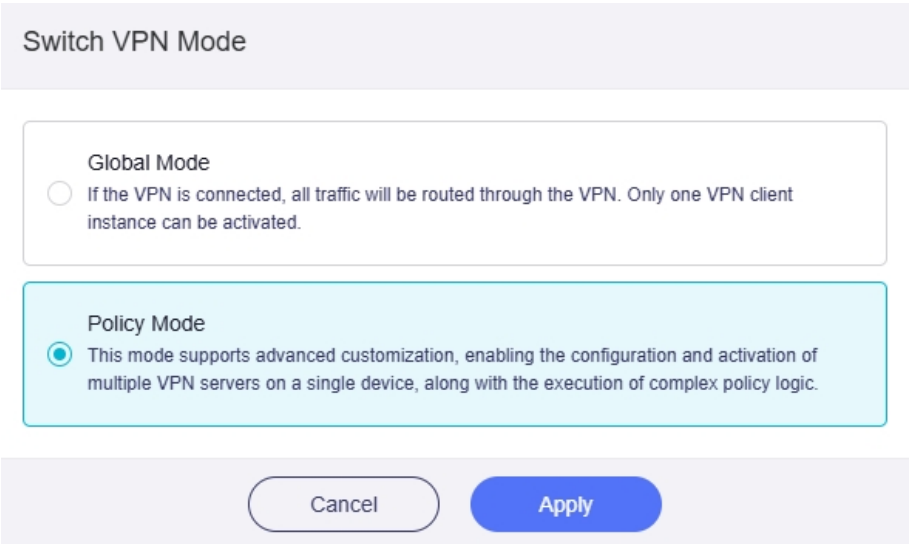
Dans l'exemple suivant, le routeur se connecte à un serveur australien avec WireGuard. Tout le trafic des clients connectés passe par ce tunnel VPN.



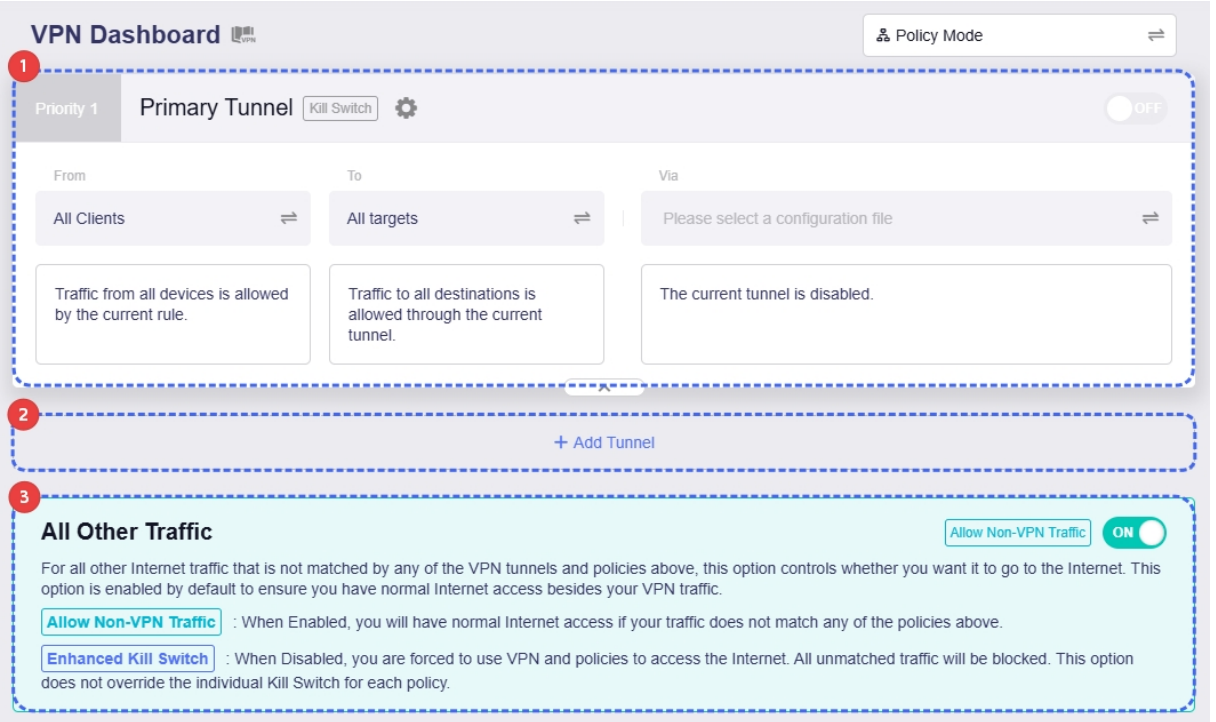
9.2.2 Mode par règles

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)**.

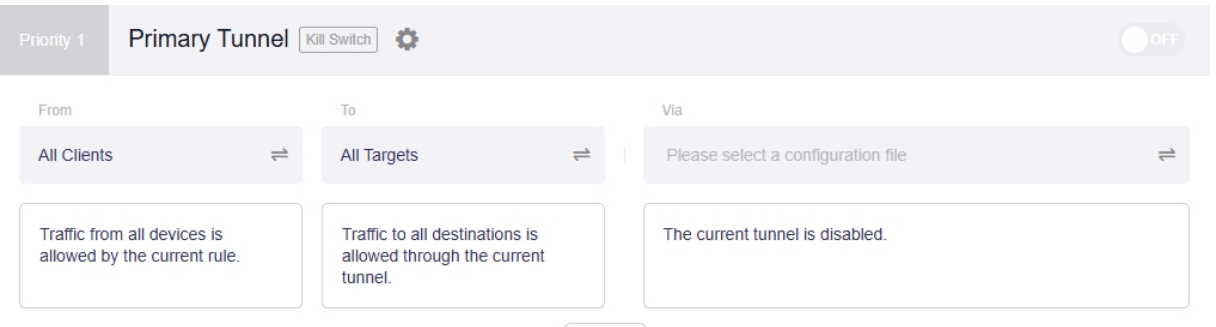


Tunnel principal

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.

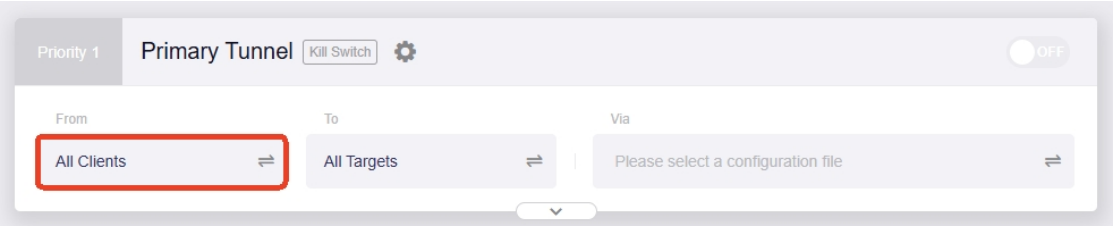
Personnalisez la règle de ce tunnel à l'aide de trois critères :

- **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.

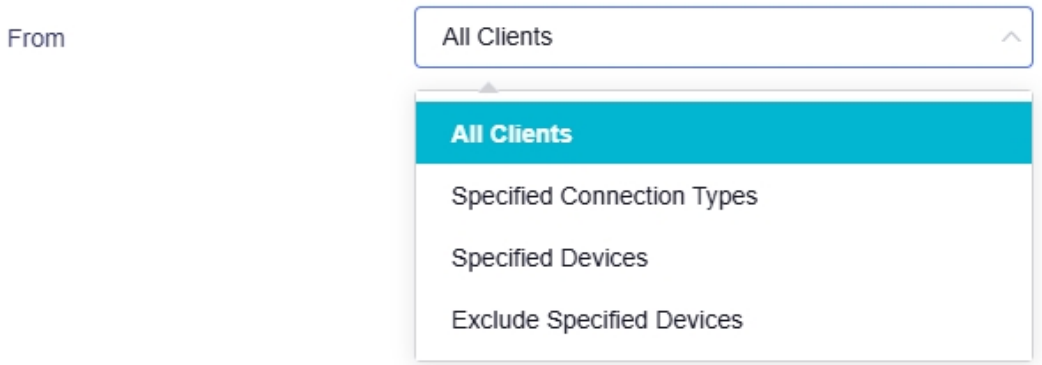


Suivez les étapes ci-dessous pour configurer la règle du tunnel.

1. Cliquez sur la zone grisée de gauche.

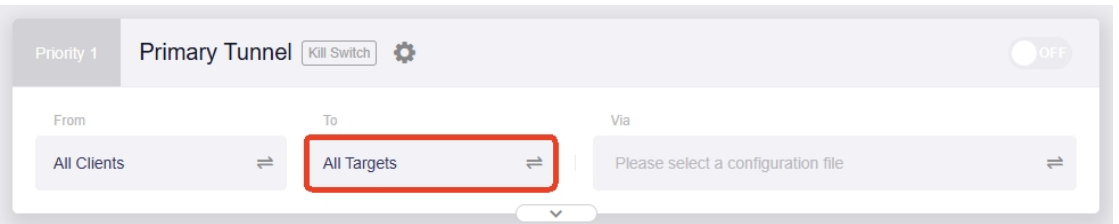


2. Sélectionnez la source du trafic à laquelle cette règle doit s'appliquer, puis cliquez sur **Appliquer (Apply)**.

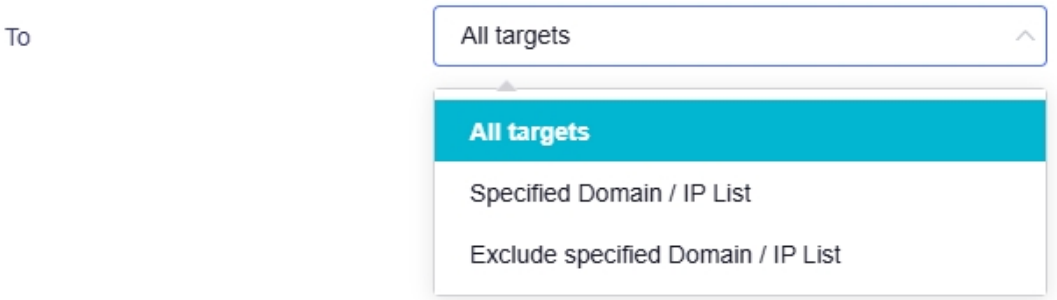


- **Tous les clients (All Clients)** : la règle s'applique au trafic de tous les appareils.
- **Types de connexion spécifiés (Specified Connection Types)** : la règle s'applique au trafic des types de connexion choisis, par exemple le sous-réseau LAN, la passerelle transparente ou le réseau invité.
-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



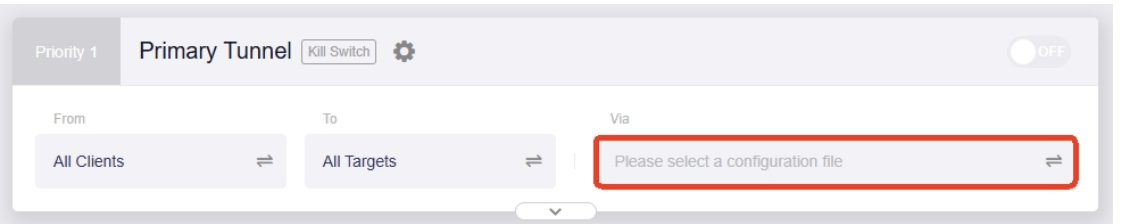
4. Sélectionnez les destinations vers lesquelles acheminer le trafic par ce tunnel, puis cliquez sur **Appliquer (Apply)**.



- **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.

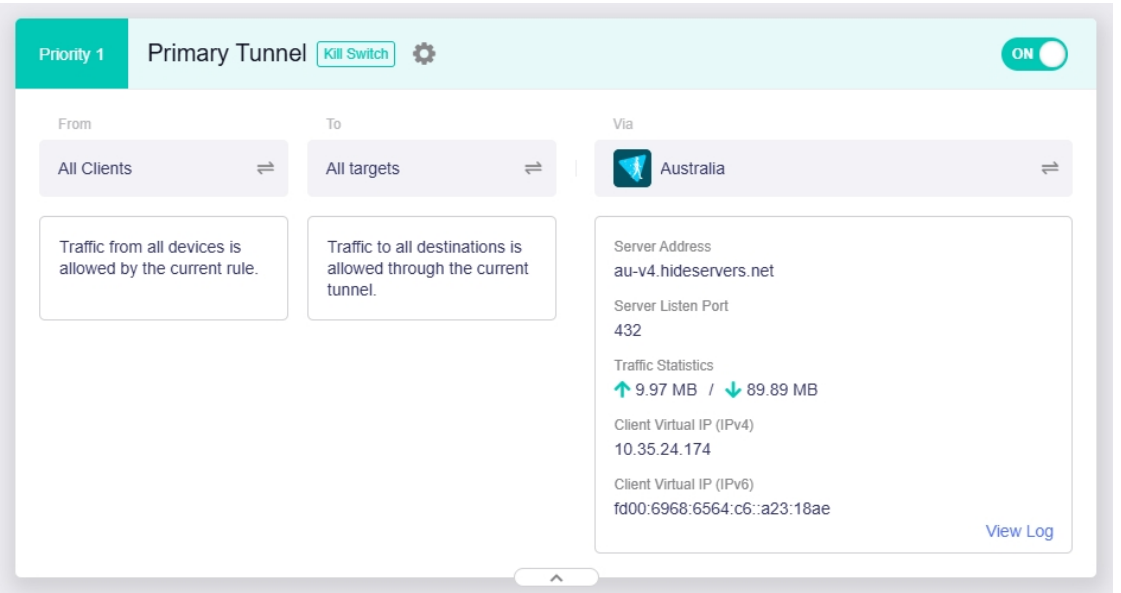


6. Choisissez la méthode de routage du tunnel : **Utiliser le VPN (Use VPN)** ou **Ne pas utiliser le VPN (Not Use VPN)**.



- **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.



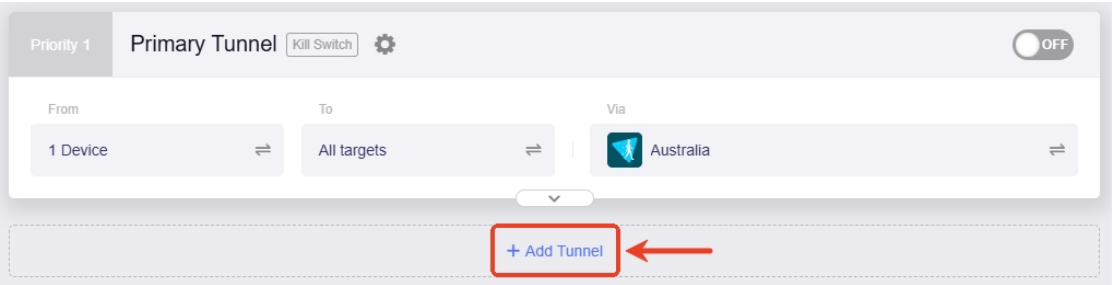
Remarque : pour votre sécurité, vérifiez les paramètres Tout autre trafic (All Other Traffic) et Options du tunnel (Tunnel Options) avant d'activer ce tunnel.

Ajouter un tunnel

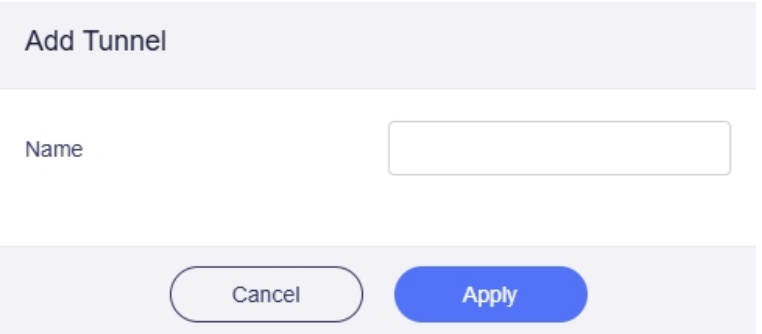
Ajoutez des tunnels pour acheminer le trafic de différents appareils vers différentes destinations.

Suivez les étapes ci-dessous pour ajouter un tunnel.

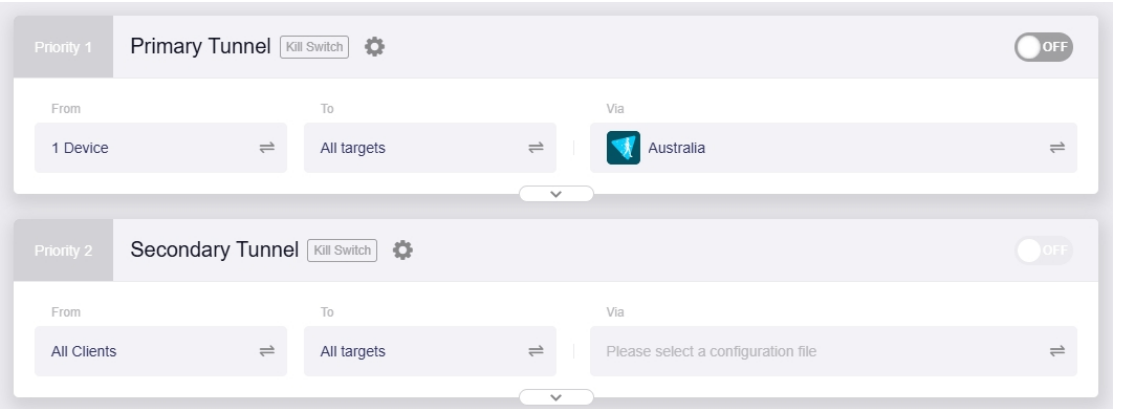
1. Cliquez sur **Ajouter un tunnel (Add Tunnel)** sous le tunnel principal.



2. Donnez un nom au tunnel.



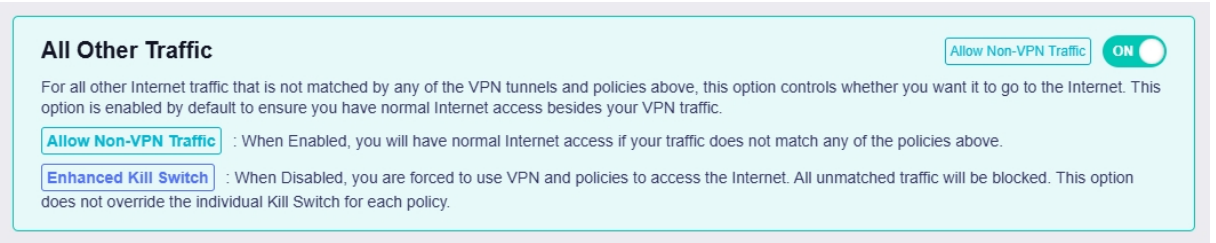
3. Un tunnel supplémentaire apparaît dans le tableau de bord VPN. Vous pouvez créer jusqu'à cinq tunnels, y compris le tunnel principal prédéfini.



4. Définissez la source, les destinations et la méthode de routage. Vérifiez ensuite les paramètres Tout autre trafic (All Other Traffic) et Options du tunnel (Tunnel Options) pour votre sécurité avant d'activer les tunnels.

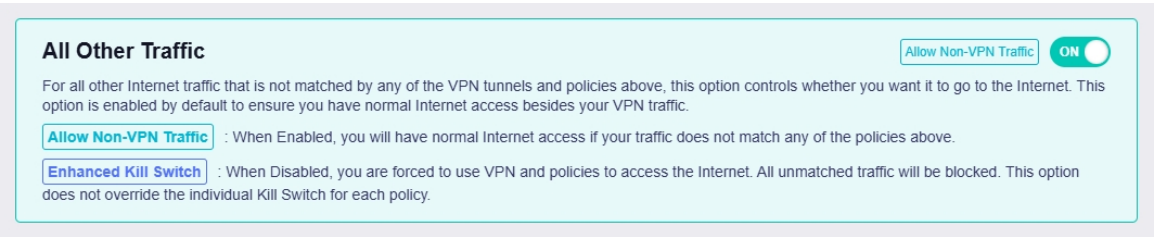
Tout autre trafic

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

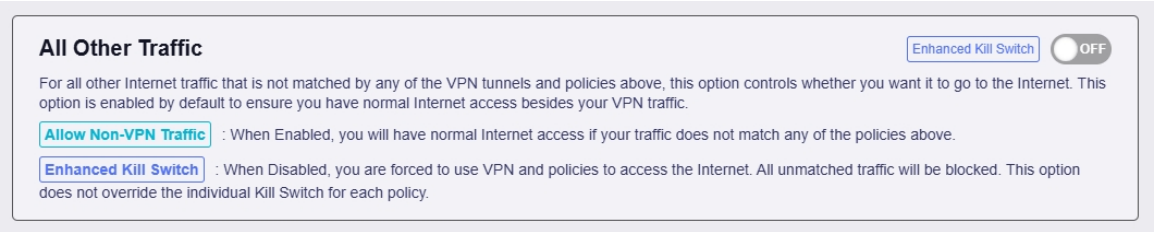


Ce tunnel détermine si le trafic ne correspondant à aucun des groupes de tunnels VPN précédents peut accéder à Internet. Il est activé par défaut afin de maintenir l'accès Internet du trafic qui n'utilise pas le VPN.

- 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.

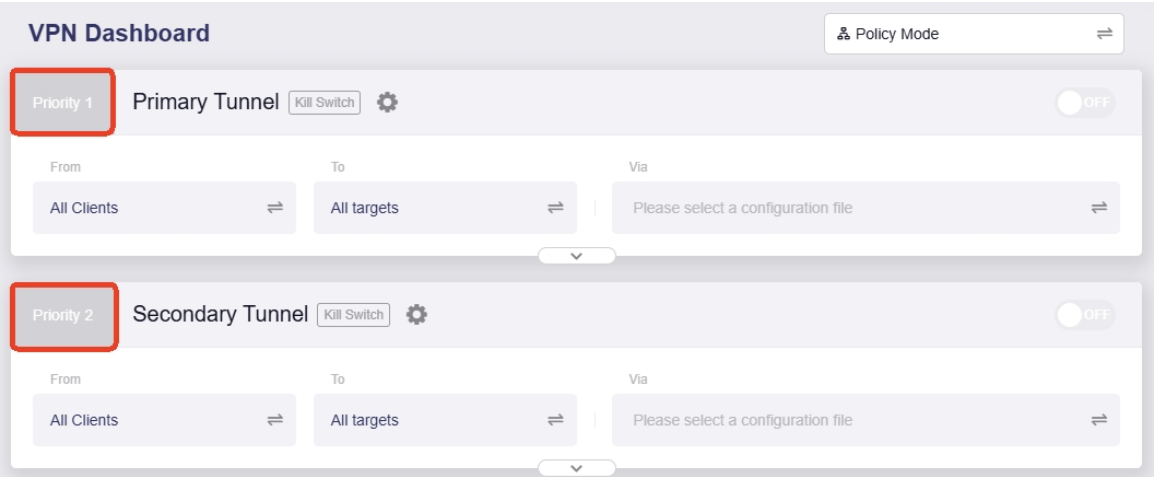


Priorité des tunnels

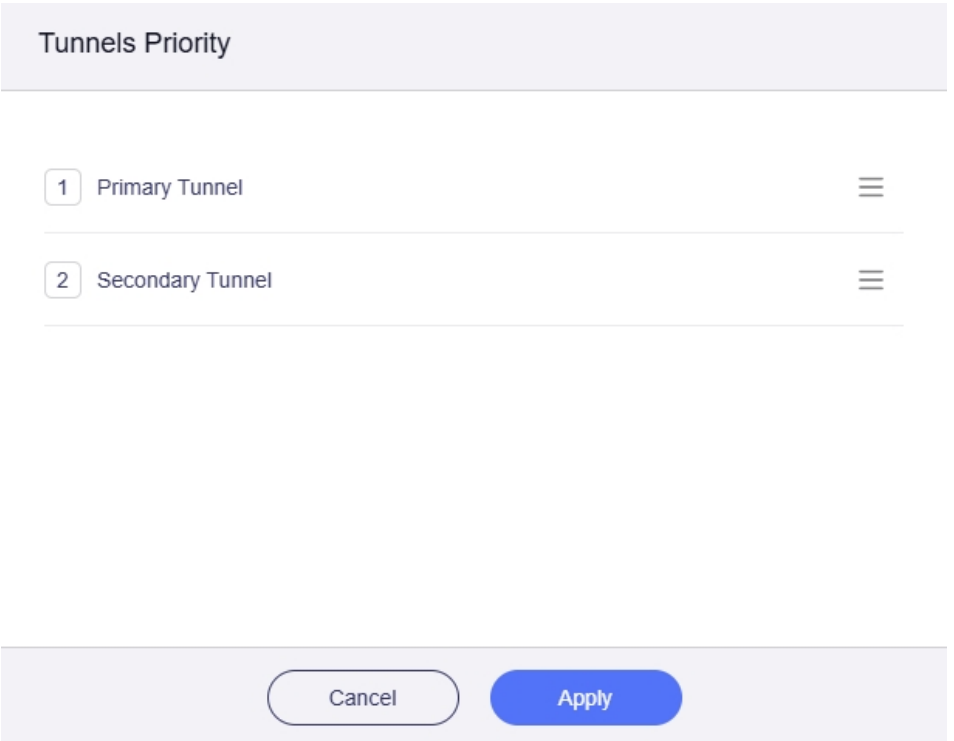
Par défaut, le tunnel principal a la priorité la plus élevée. Viennent ensuite les tunnels ajoutés manuellement, puis le tunnel prédéfini Tout autre trafic, qui assure la connexion via le réseau WAN du FAI local.

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)**.

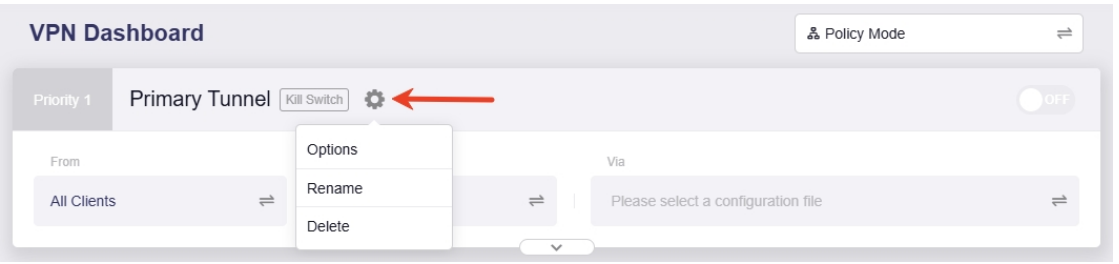


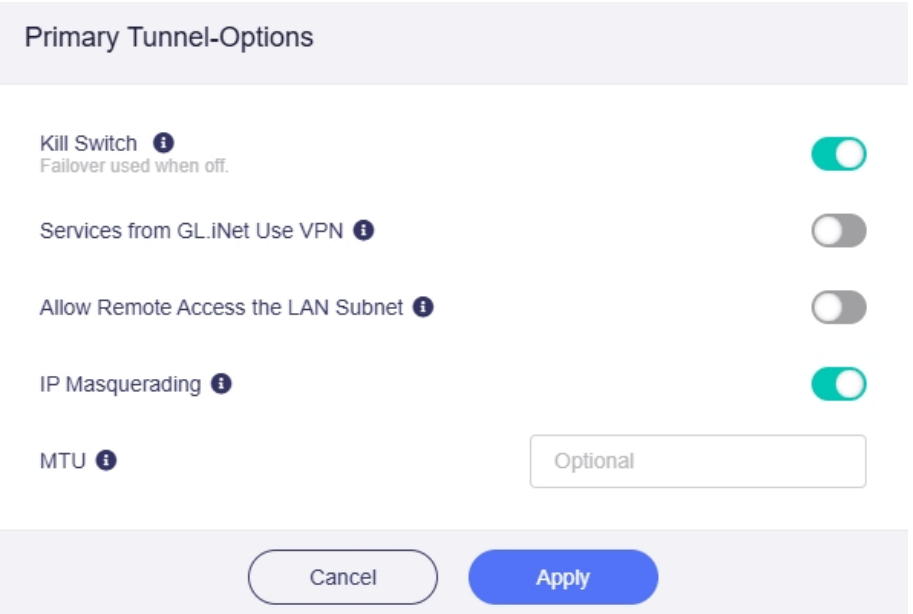
Lorsque plusieurs tunnels sont activés, le routeur achemine le trafic dans l'ordre suivant :

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.

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.

Chapitre 10

Configuration d’un serveur VPN

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

10.1 Configuration d’un 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 :

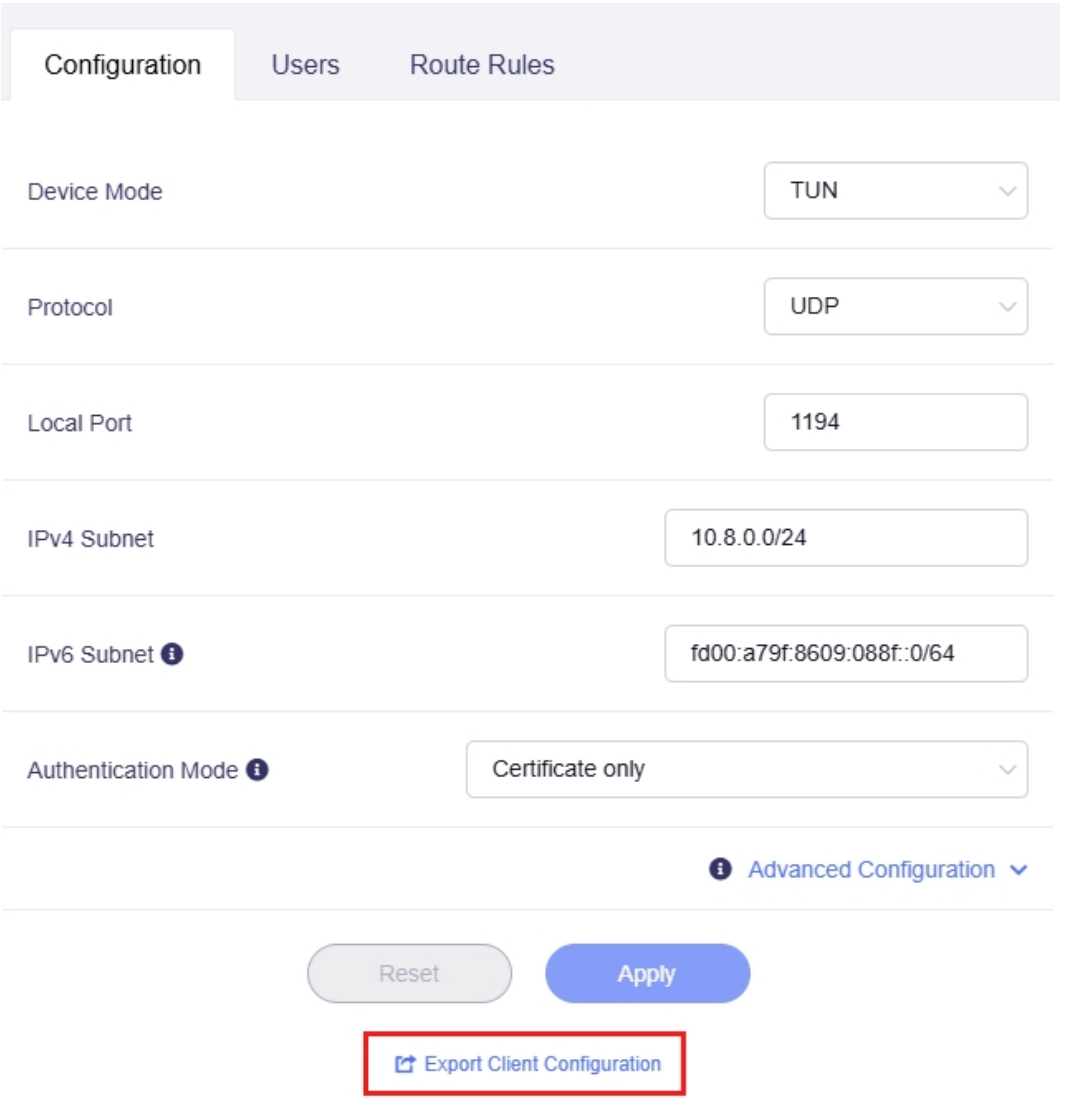
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions 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

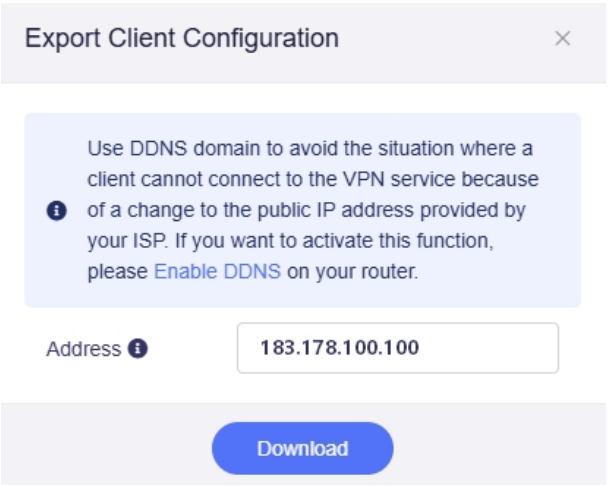
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur OpenVPN (OpenVPN Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.
   La configuration par défaut convient à la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

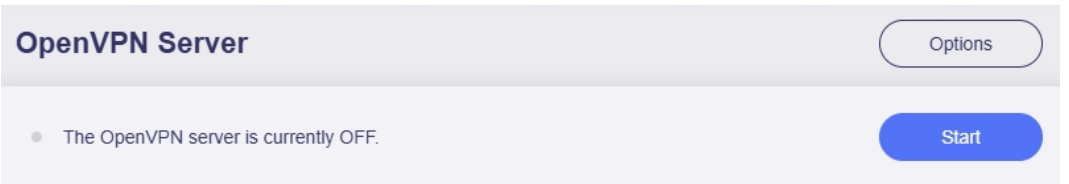


Conseils :

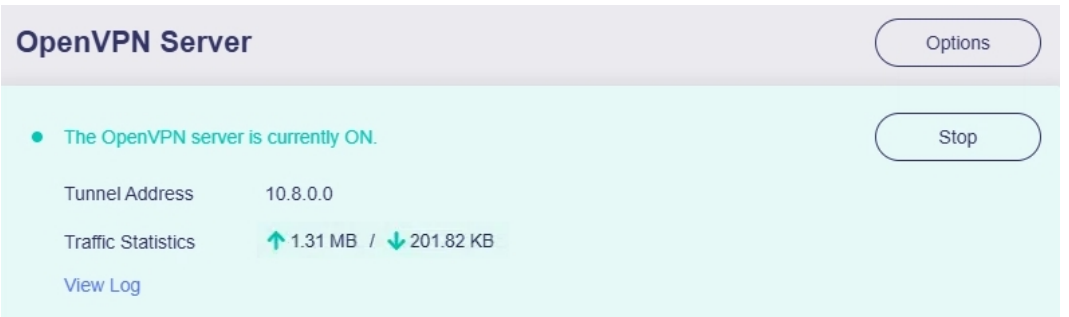
- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Depuis le micrologiciel v4.8, vous pouvez choisir l'adresse du serveur dans une liste avant d'exporter le 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 Dépannage

Voici les causes courantes d’un échec de connexion :

- Le serveur VPN ne possède pas d’adresse IP publique. Consultez cette page pour obtenir de l’aide.
- Une redirection de port peut être nécessaire. Consultez cette page pour obtenir de l’aide.
- 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.

10.2 Configuration d’un serveur WireGuard

WireGuard® est un VPN simple, rapide et moderne, fondé sur une cryptographie de pointe. Il vise à être plus rapide, plus simple et plus pratique qu’IPSec, tout en limitant la complexité de configuration, et nettement plus performant qu’OpenVPN. 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 :

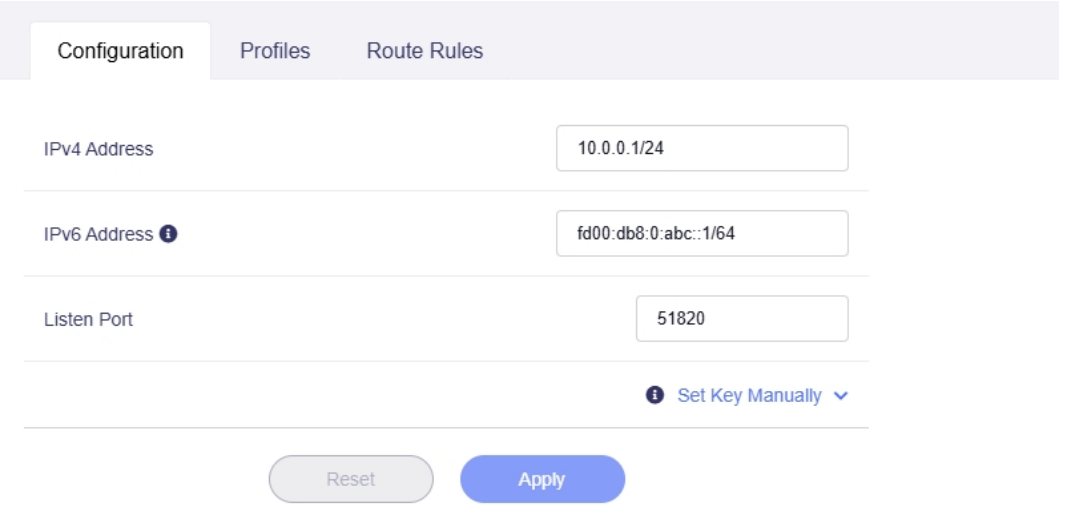
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions 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**

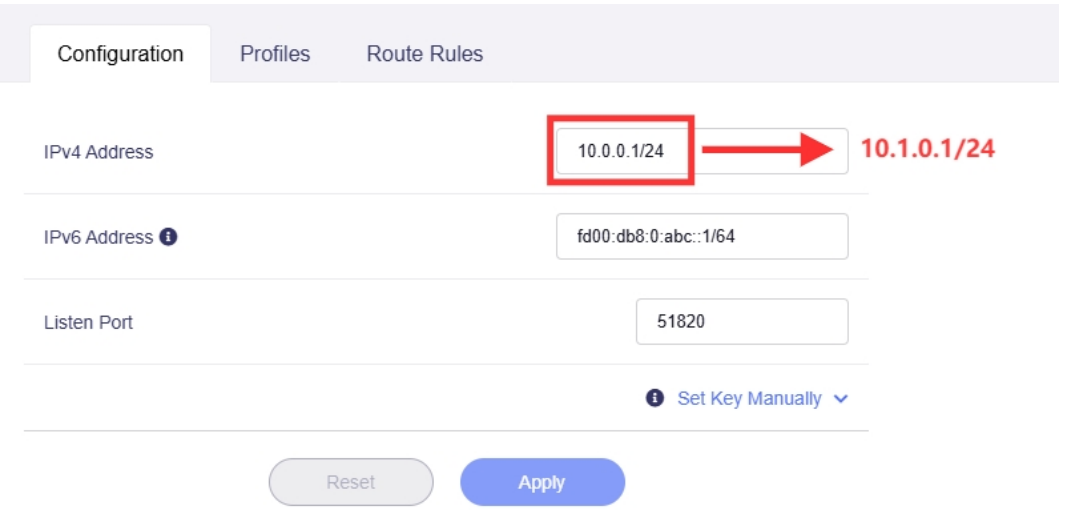
   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n’est nécessaire. Passez à l’étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs 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.

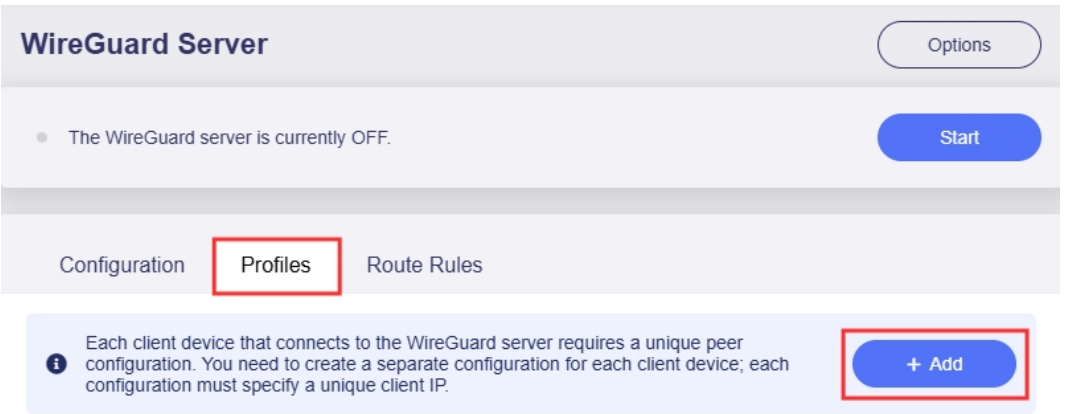


   En cas de conflit, choisissez une autre adresse IPv4, par exemple **10.1.0.1/24**, puis cliquez sur **Appliquer (Apply)**. Conservez la notation CIDR « /24 » pour éviter les problèmes de connexion.

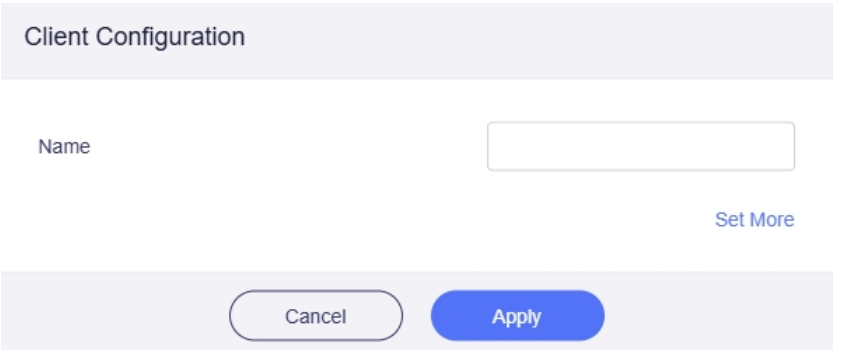


3. Ajoutez un profil.

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.



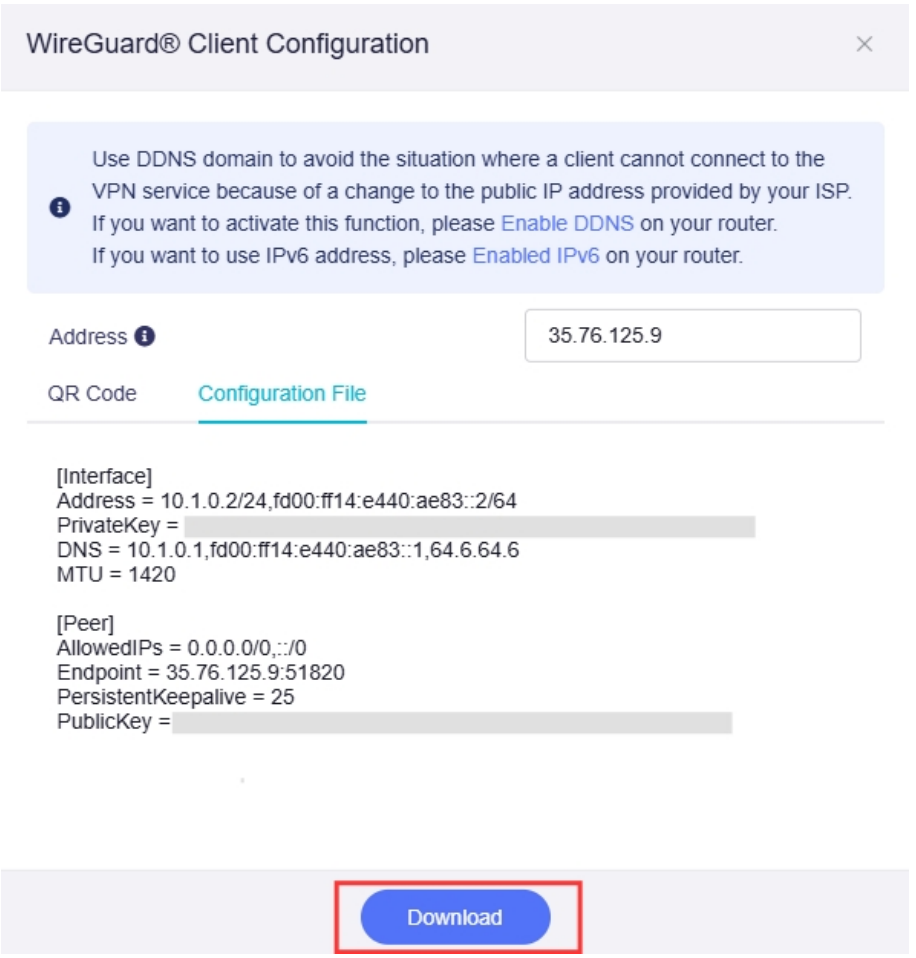
Conseil : pour accéder aux appareils du LAN du client WireGuard depuis le serveur WireGuard, configurez les routes dans l'onglet **Règles de routage (Route Rules)**. Consultez cette page pour en savoir plus.

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.

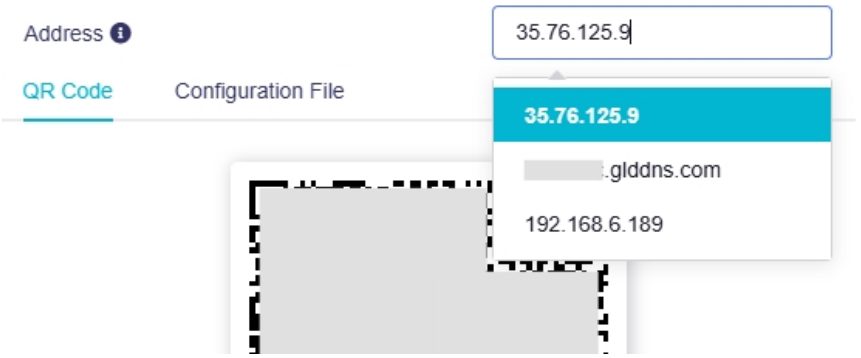
   - **Code QR** : adapté aux appareils disposant de l'application WireGuard, comme les smartphones, tablettes et ordinateurs portables. Ouvrez l'application WireGuard sur l'appareil à configurer comme client et scannez le code QR pour importer la configuration.
   - **Texte brut** : permet de consulter 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.

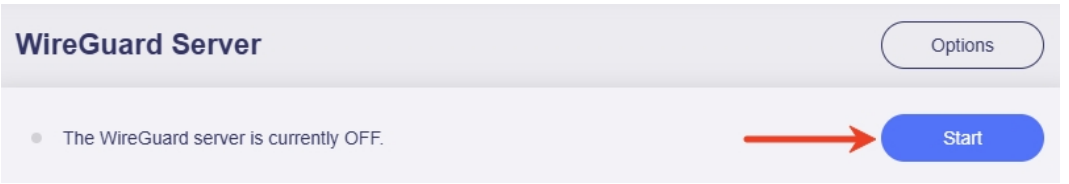


Conseils :

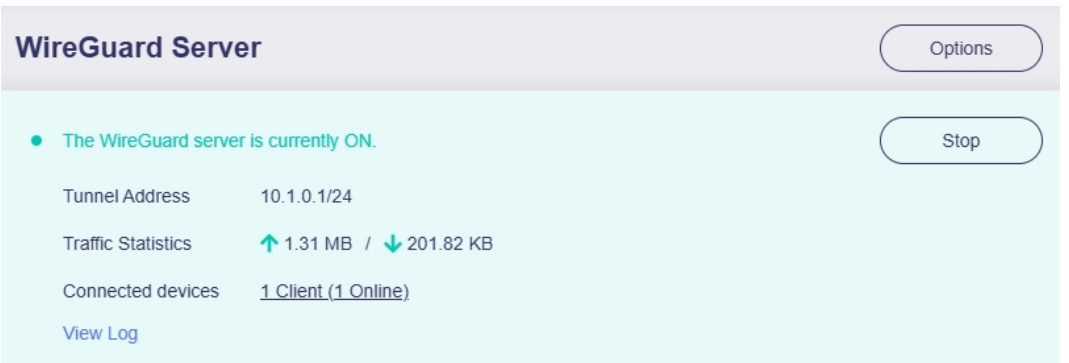
- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Depuis le micrologiciel v4.8, vous pouvez choisir l'adresse du serveur dans une liste avant d'exporter le 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 Dépannage

Voici les causes courantes d'un échec de connexion :

- Le serveur VPN ne possède pas d'adresse IP publique. Consultez cette page pour obtenir de l'aide.
- Une redirection de port peut être nécessaire. Consultez cette page pour obtenir de l'aide.
- Votre FAI bloque le port utilisé par le serveur WireGuard. Choisissez un autre port ou contactez votre FAI.
- La connexion VPN peut être bloquée dans certains pays ou certaines régions.

Chapitre 11

Configuration d’un client VPN

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

11.1 Configuration d’un 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.

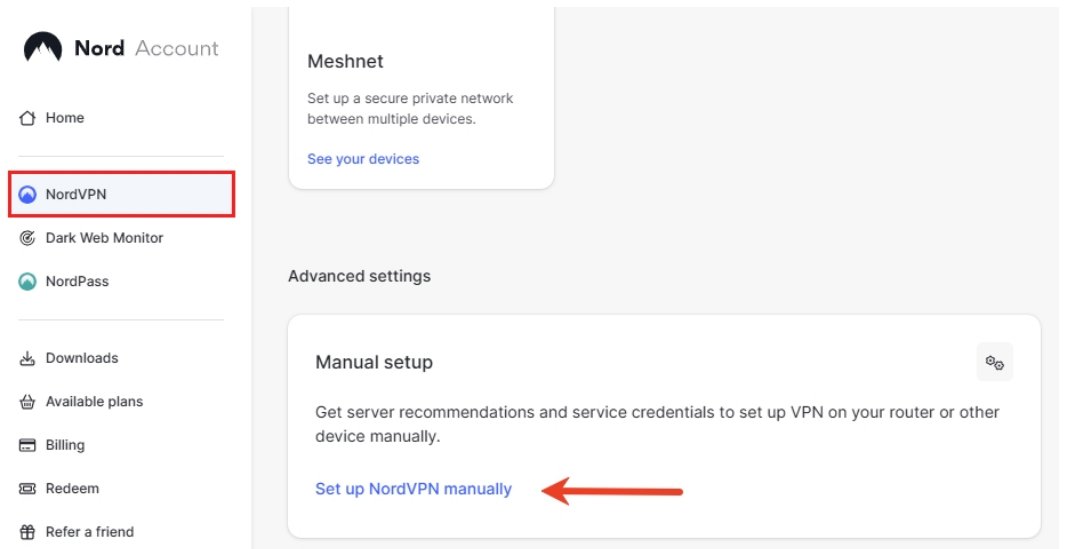
Rendez-vous ensuite sur le site officiel de votre fournisseur VPN pour obtenir les identifiants de service ou le fichier de configuration. Si vous ne savez pas comment obtenir ce fichier, consultez ce lien ou contactez l’assistance du fournisseur.

11.1.2 Configuration de NordVPN

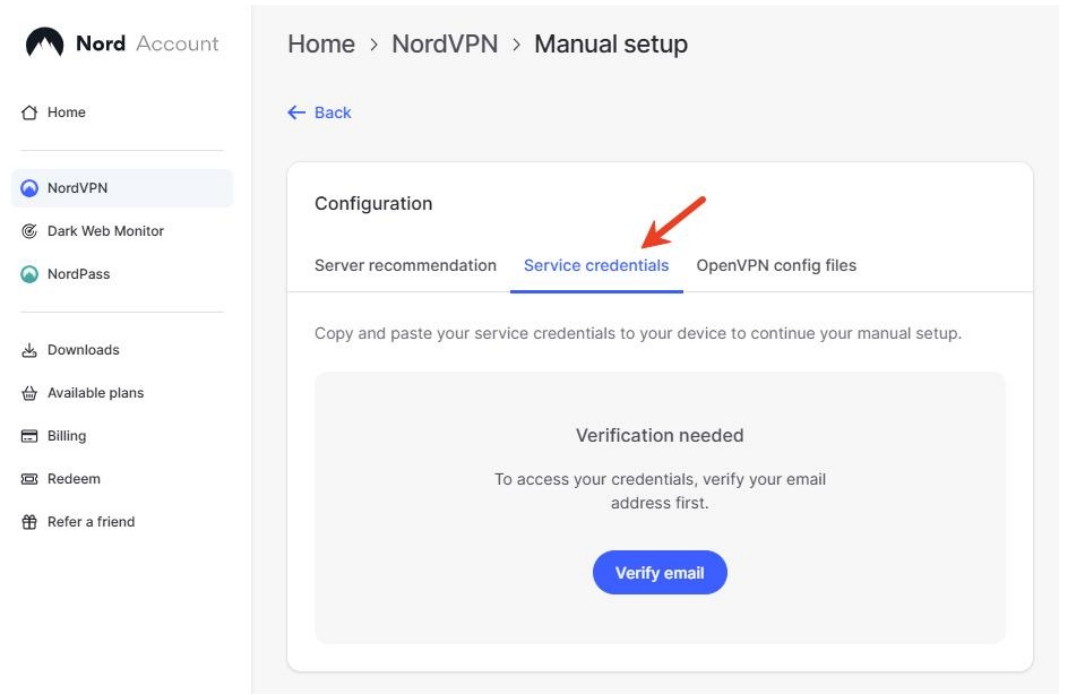
NordVPN est intégré à l’interface d’administration Web GL.iNet. Saisissez les identifiants obtenus dans le tableau de bord NordVPN dans l’interface du routeur ou dans l’application mobile GL.iNet pour récupérer les fichiers de configuration de tous les serveurs NordVPN, sans importation manuelle.

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

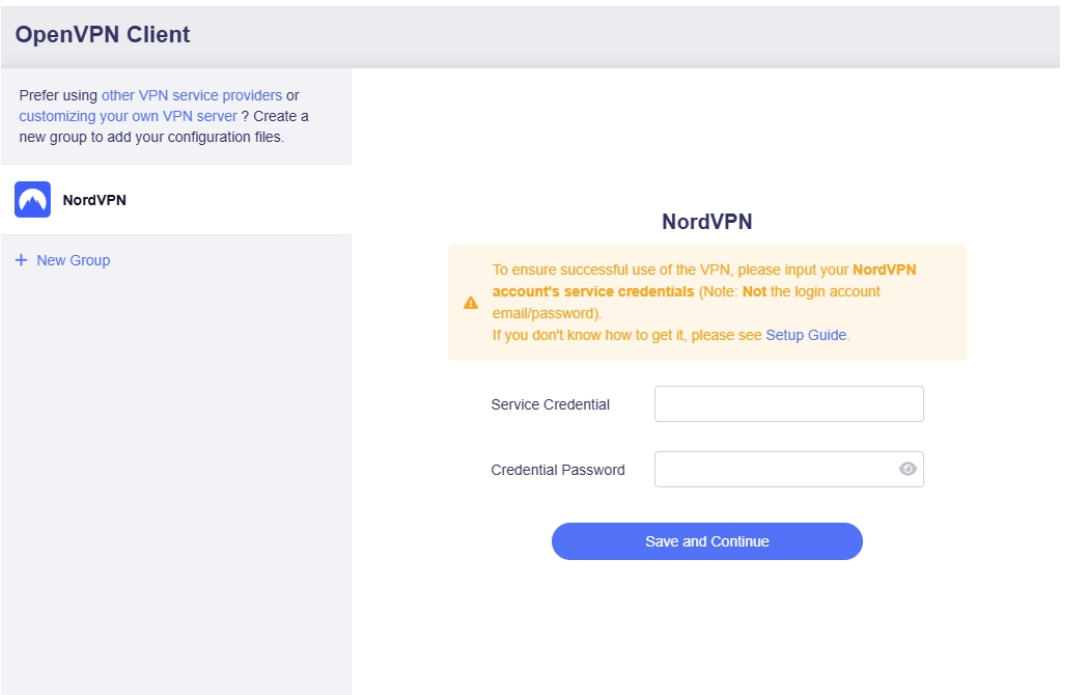
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



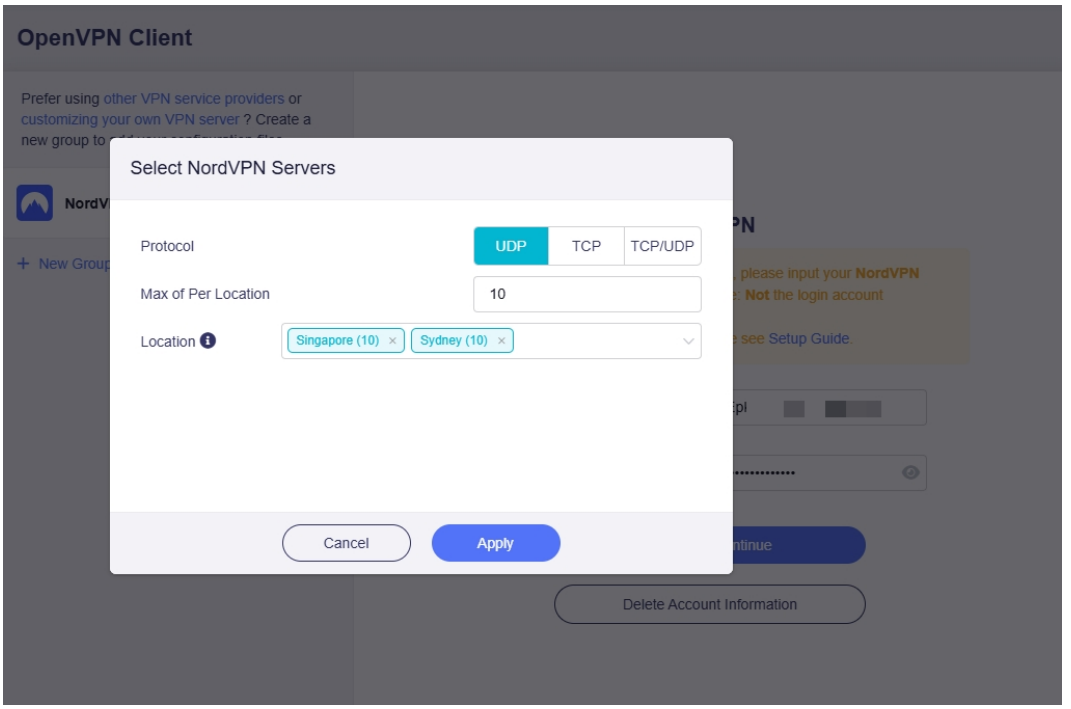
Repérez les **identifiants de service (service credentials)** et copiez-les pour les utiliser ensuite.



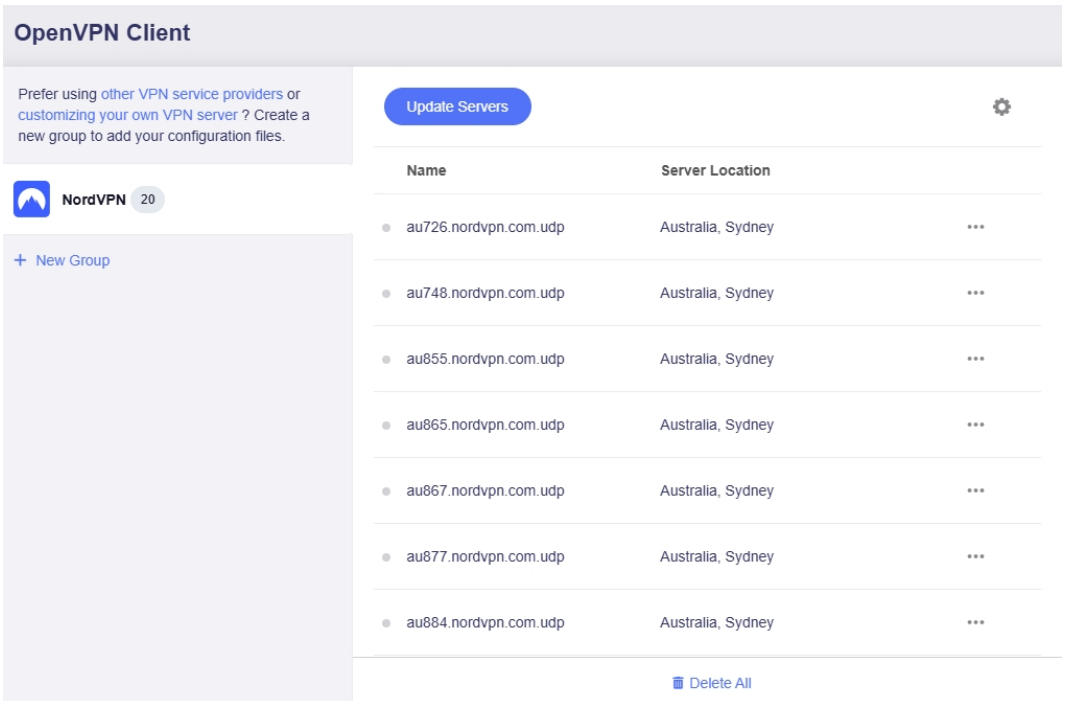
3. Dans l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** > **NordVPN**. Saisissez les identifiants de service, qui ne sont PAS l’adresse e-mail et le mot de passe de connexion au compte, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



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

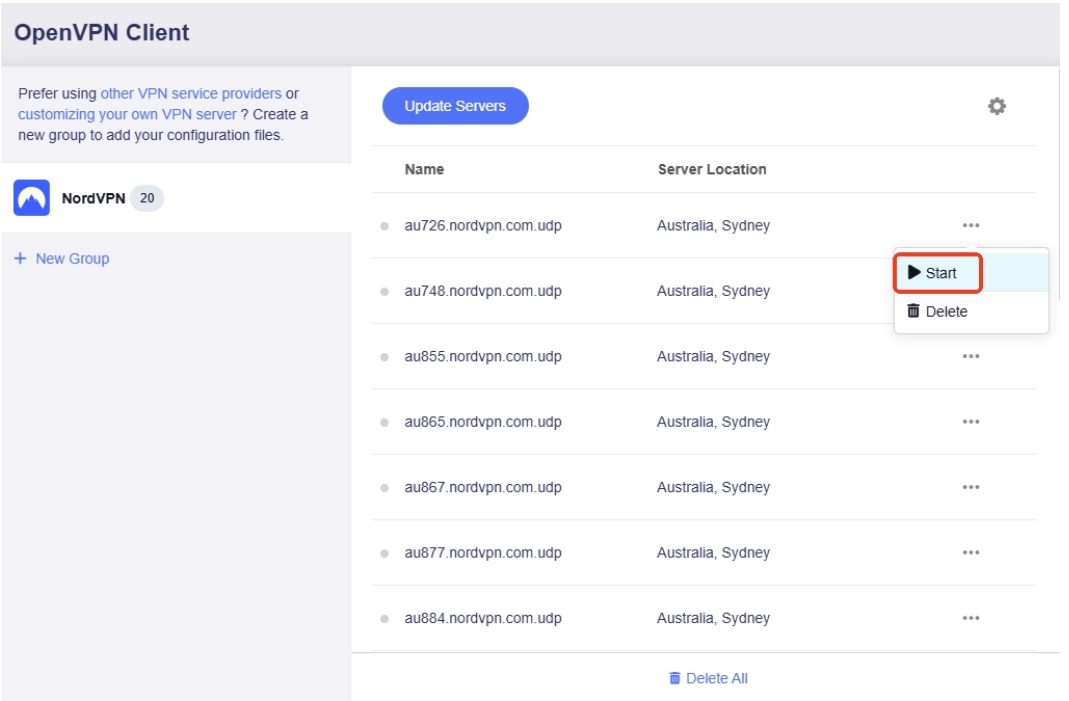


Les fichiers de configuration sont téléchargés.

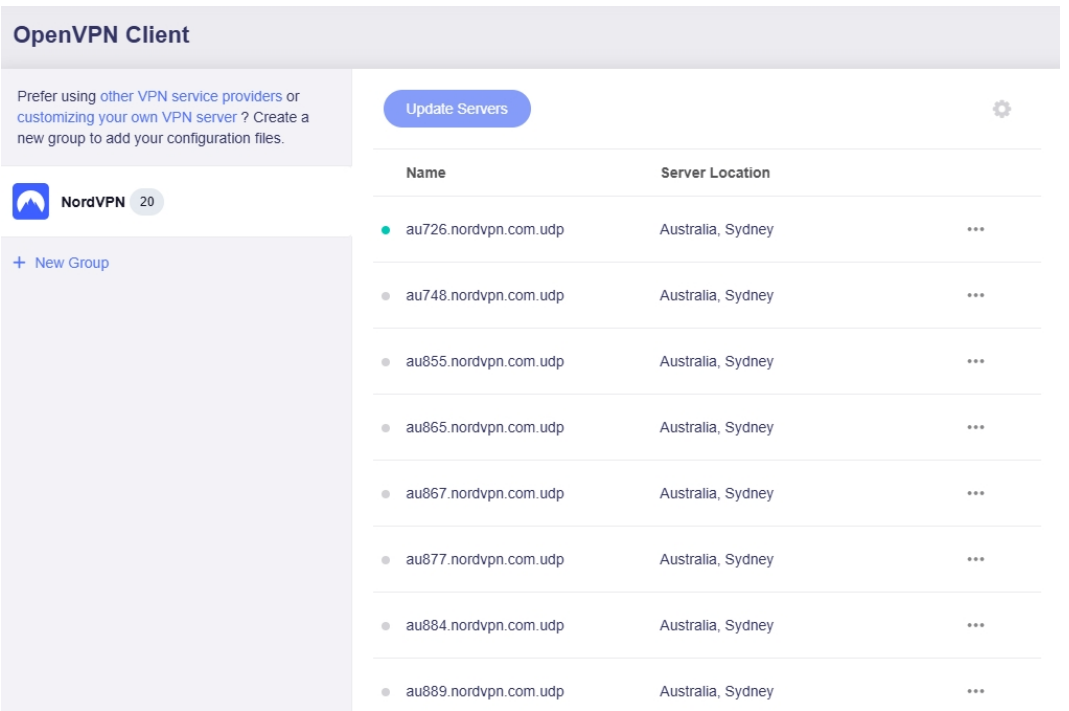


5. Établissez une connexion.

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



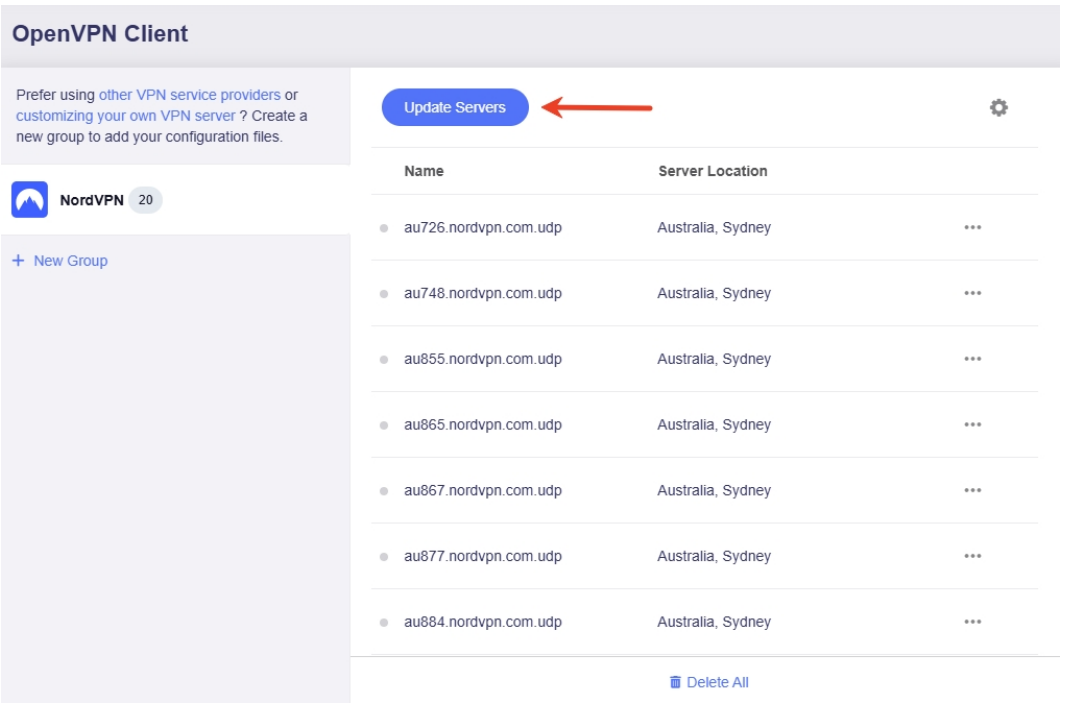
6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

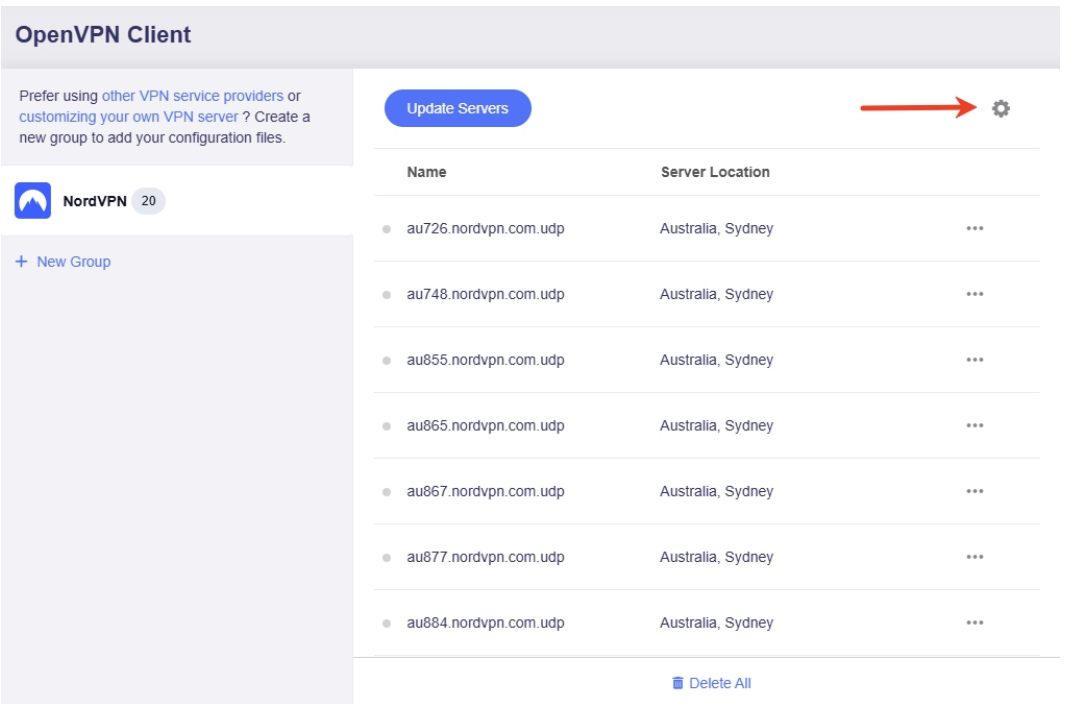
7. Mettez à jour les serveurs.

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.



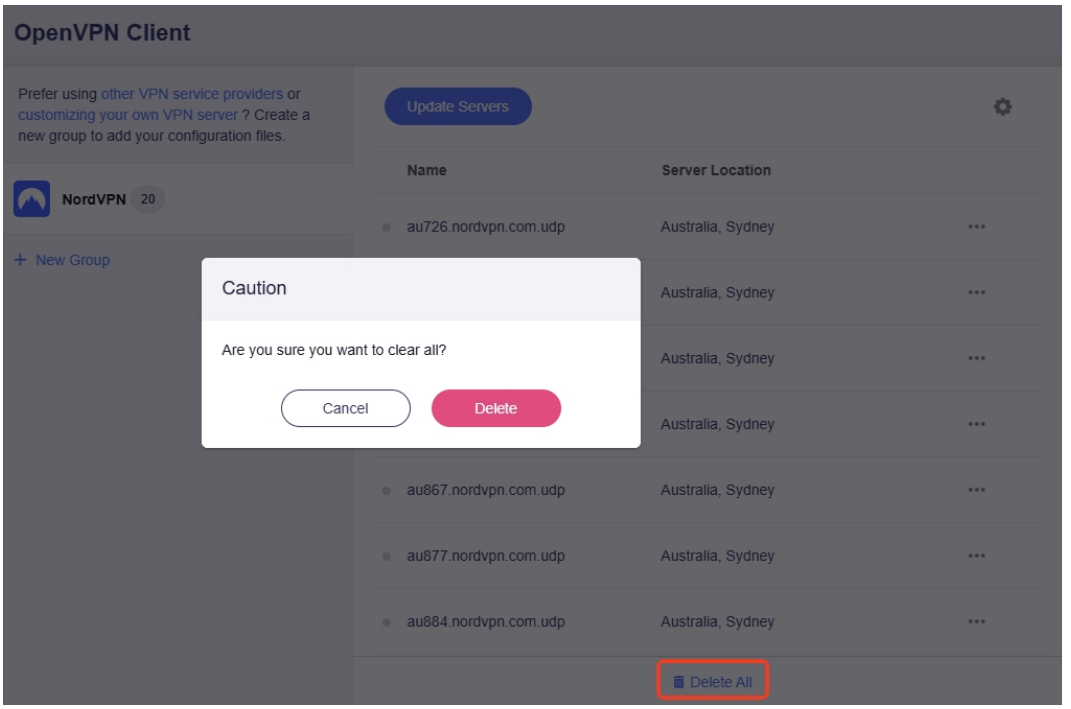
8. Modifiez les identifiants.

   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.

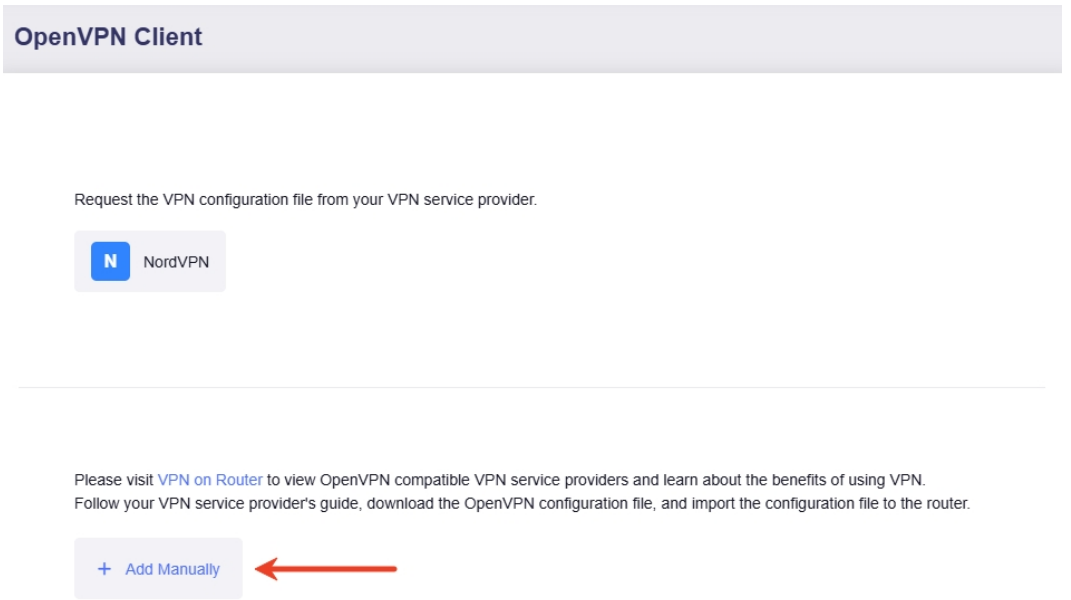


11.1.3 Configuration manuelle d’un client OpenVPN pour un autre fournisseur

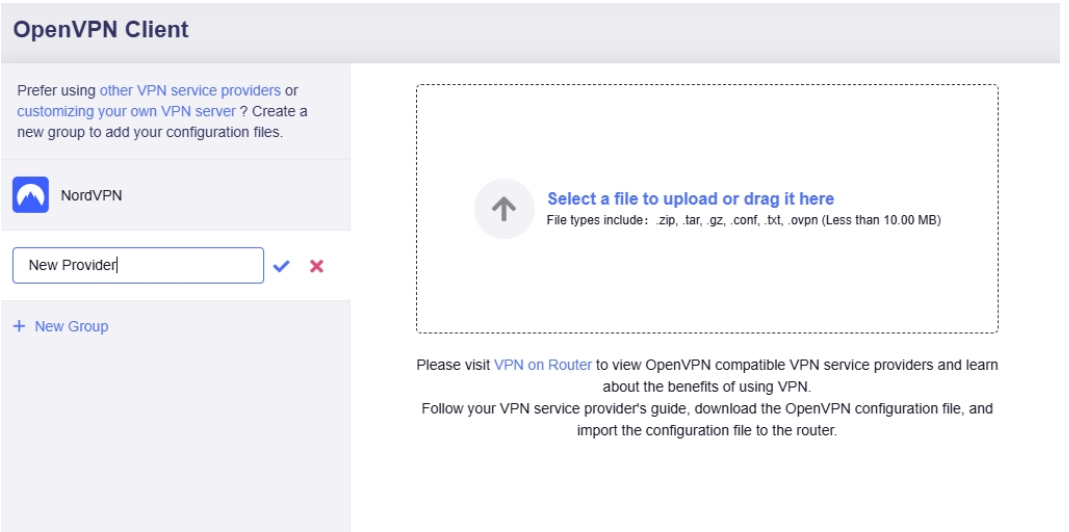
Si votre fournisseur OpenVPN n’est pas intégré à notre interface, récupérez d’abord le fichier de configuration sur son site officiel. Importez-le ensuite sur le routeur pour configurer le client OpenVPN.

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

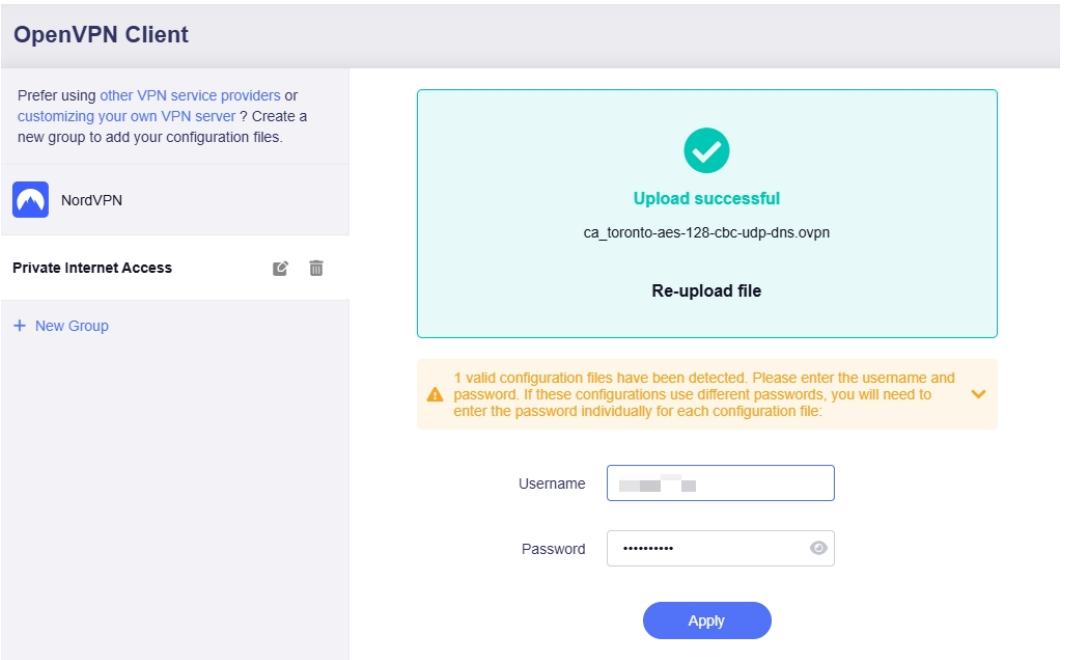
1. Téléchargez un fichier de configuration sur le site officiel de Private Internet Access.
2. Dans l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)**, puis cliquez sur **Ajouter manuellement (Add Manually)**.



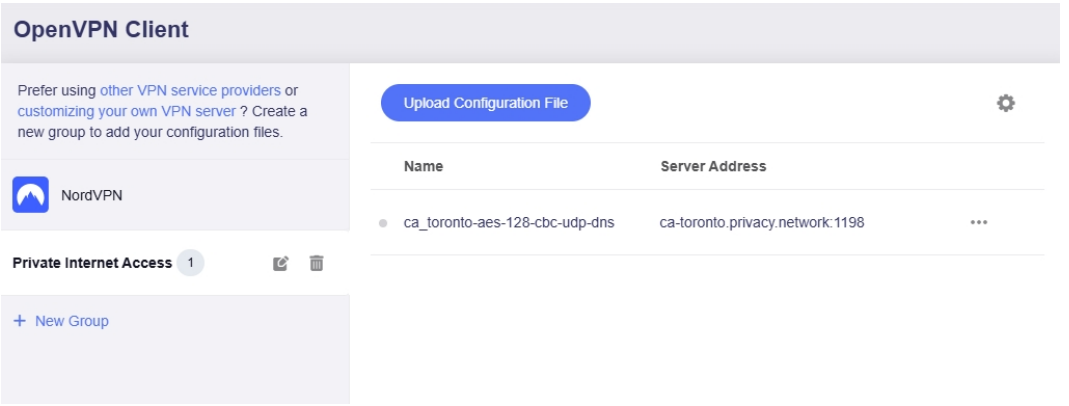
3. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



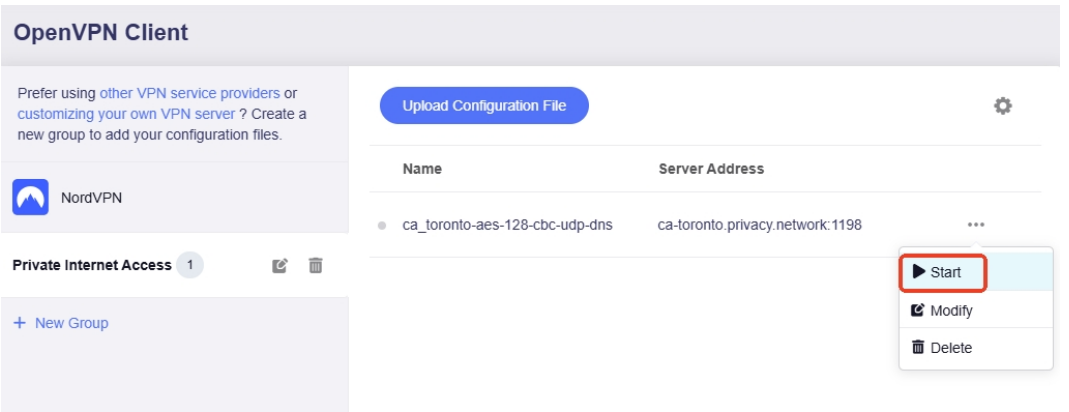
4. Importez votre fichier de configuration OpenVPN. Saisissez les identifiants si nécessaire, puis cliquez sur **Appliquer (Apply)**.



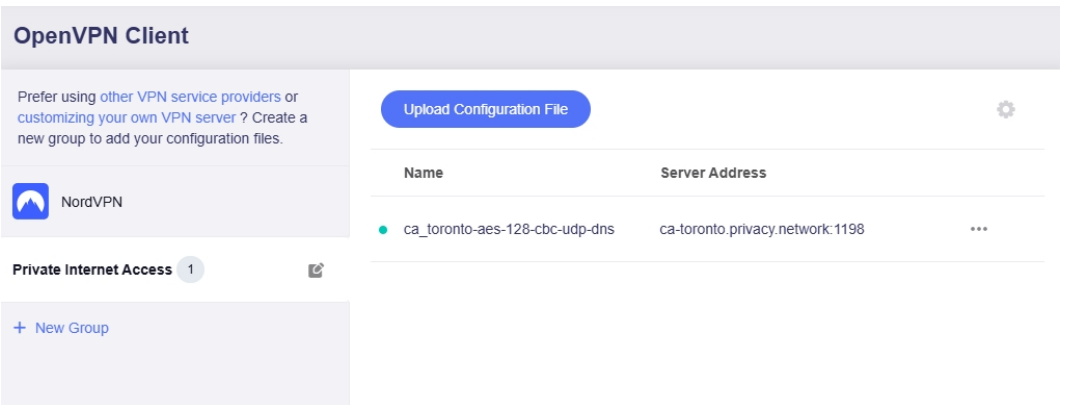
Le fichier importé apparaît dans la liste.



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 depuis 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.

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.

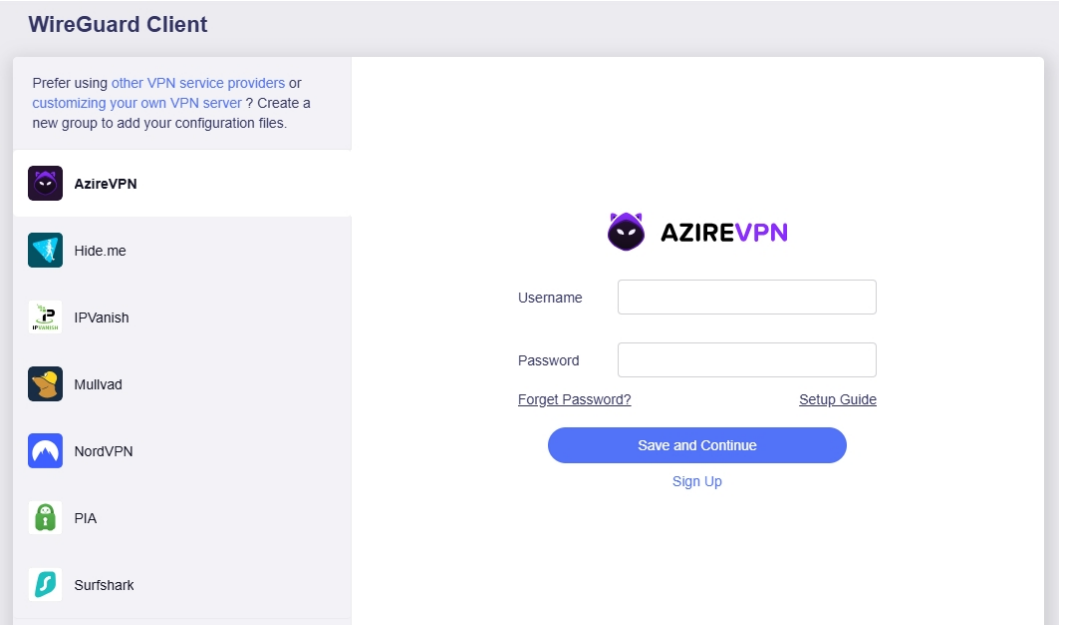
Sélectionnez ensuite votre fournisseur ci-dessous pour accéder directement aux instructions détaillées.

- 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

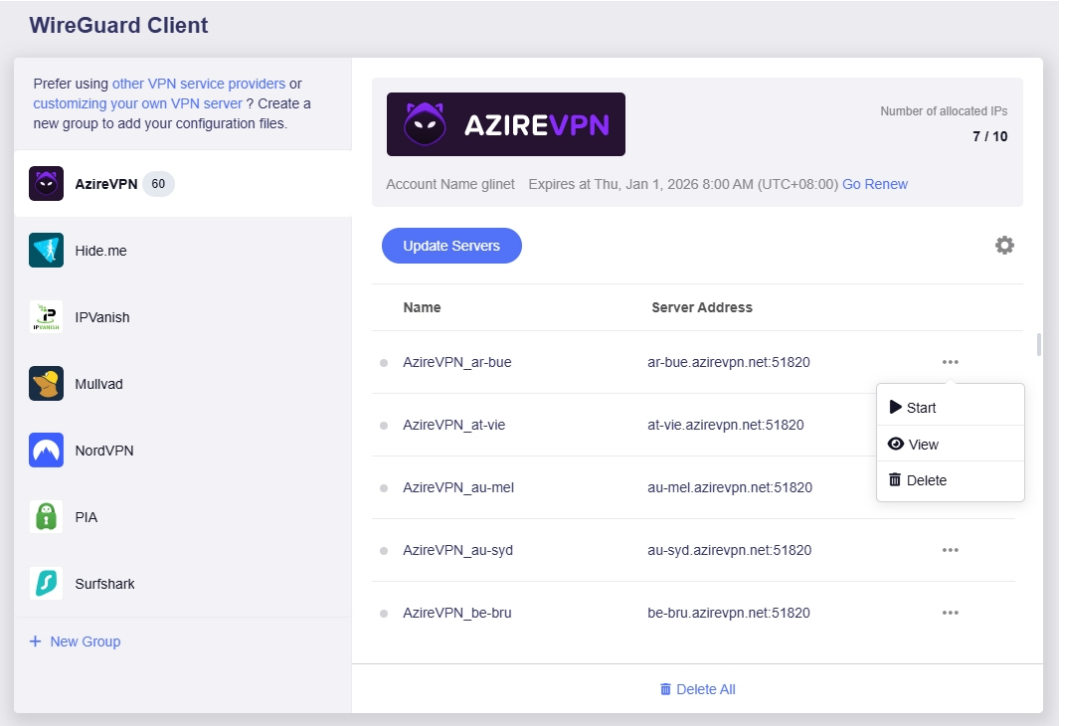
11.2.2 Configuration d’AzireVPN

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

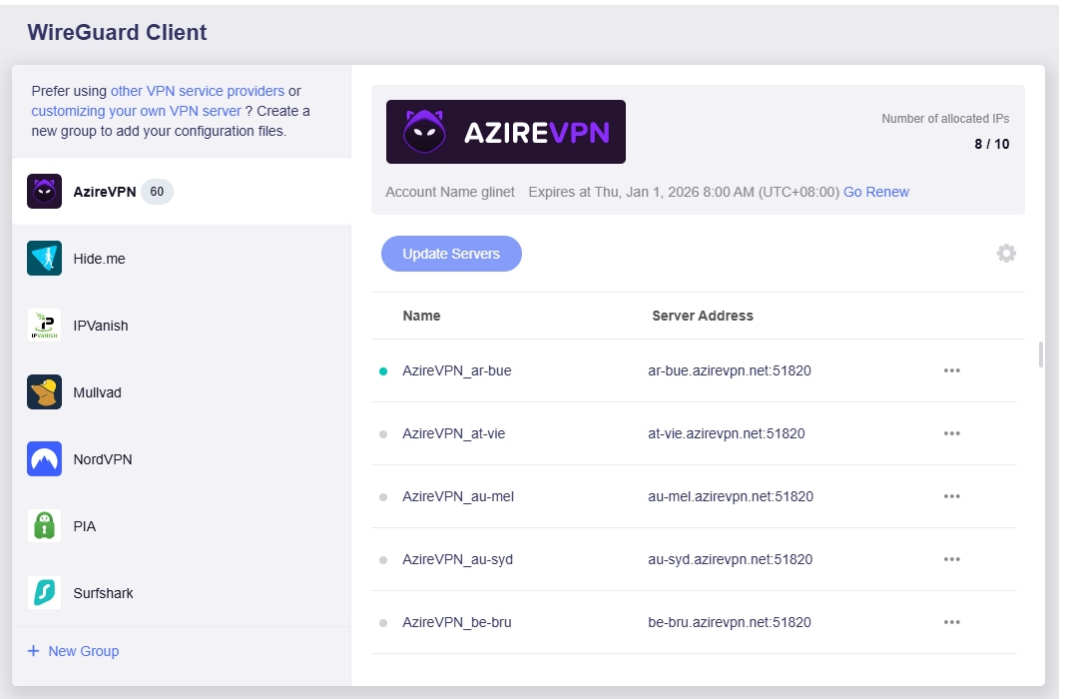
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **AzireVPN**.
2. Saisissez l’identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



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



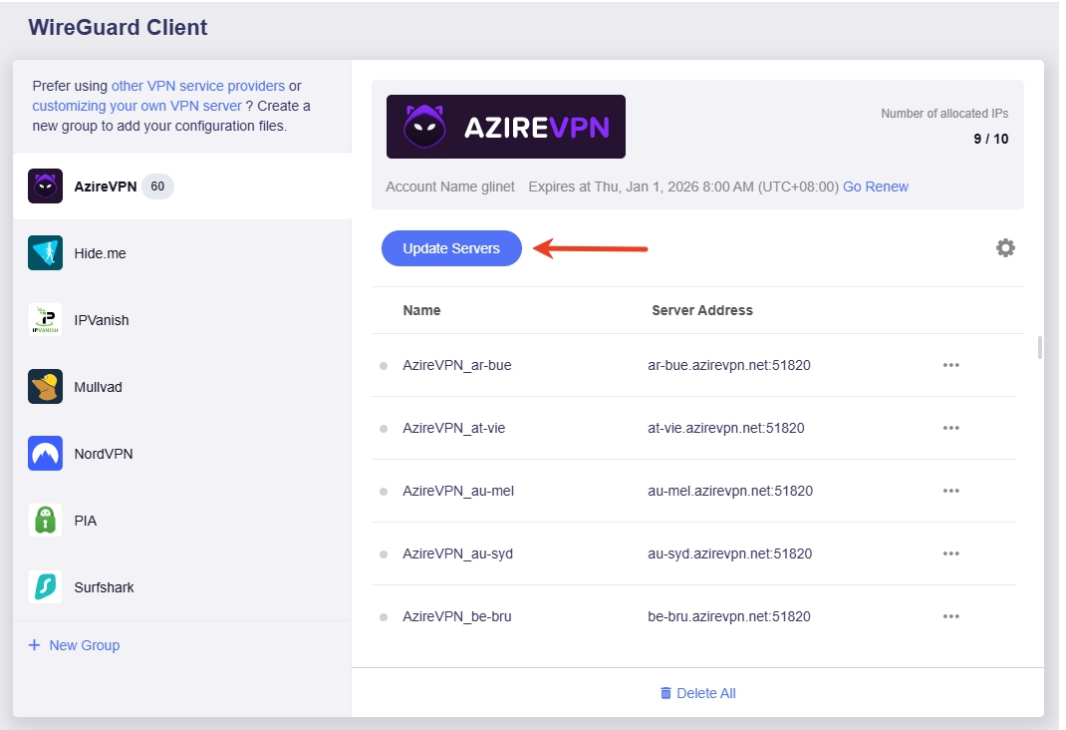
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



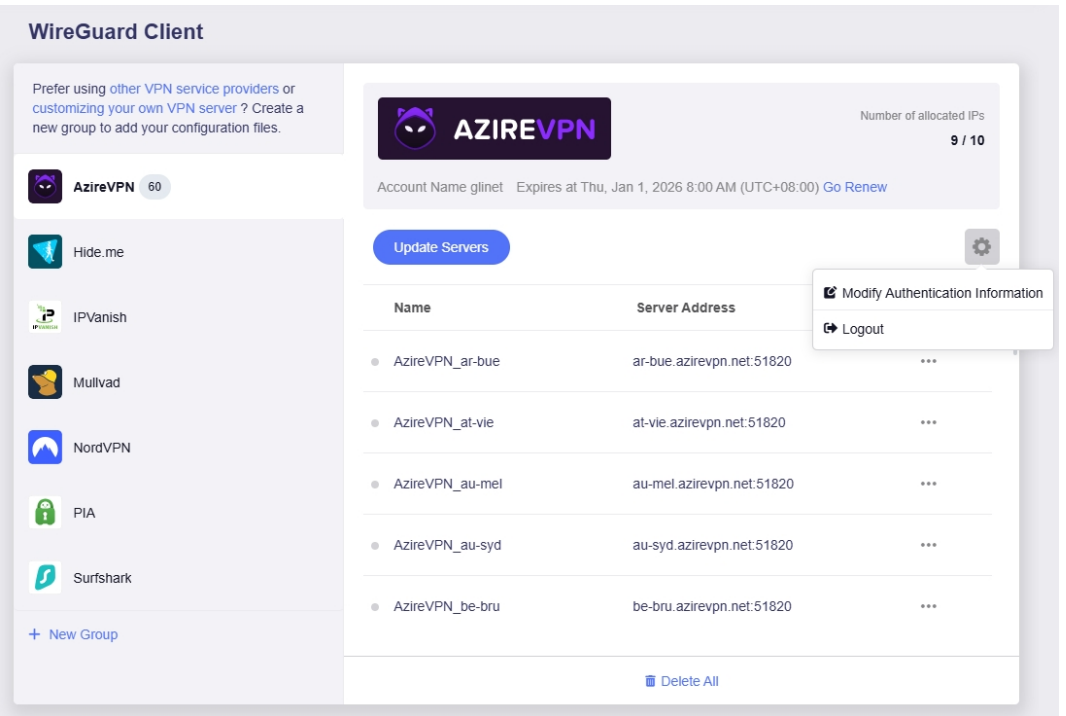
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

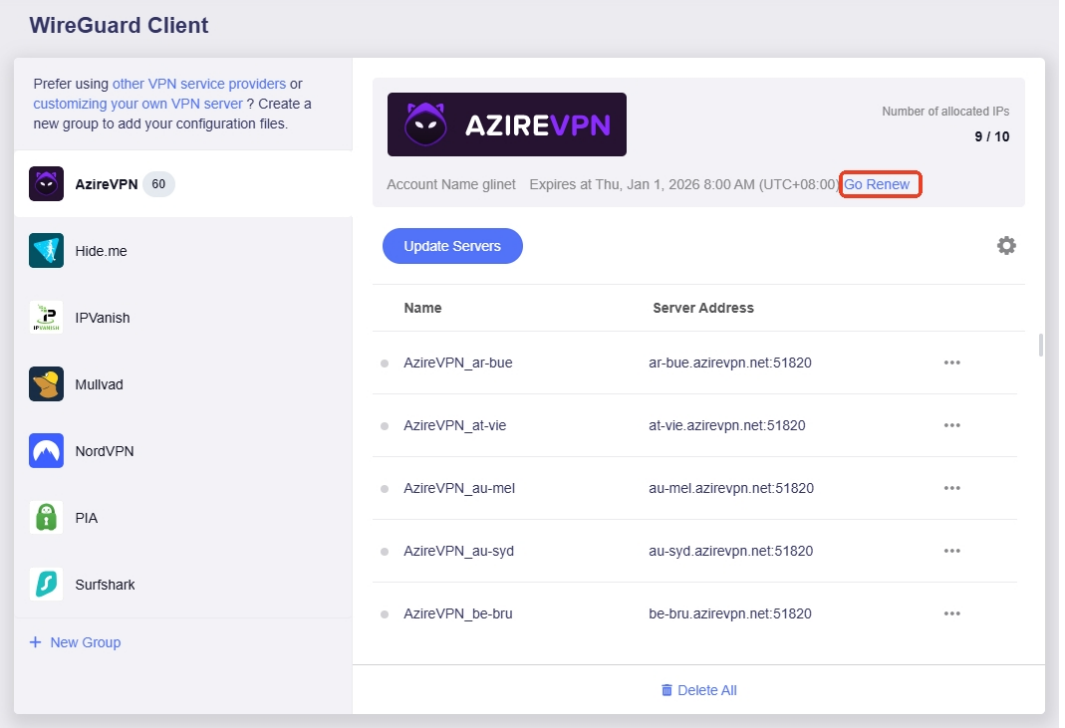


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.

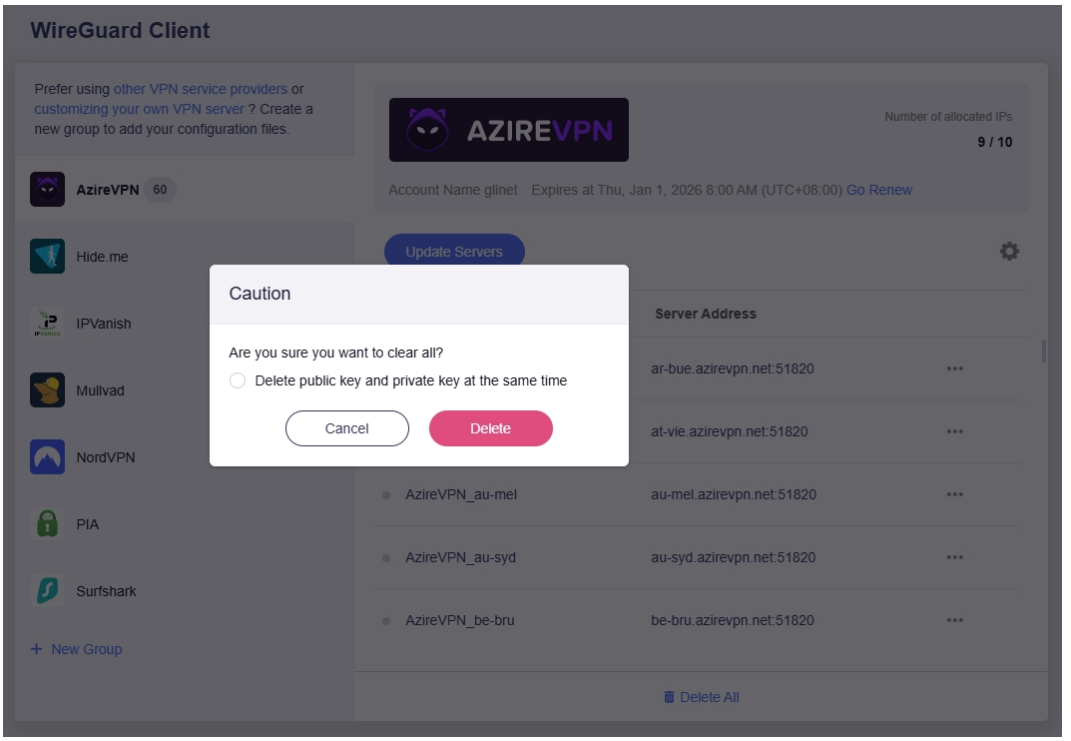


7. Renouvelez l'abonnement.

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



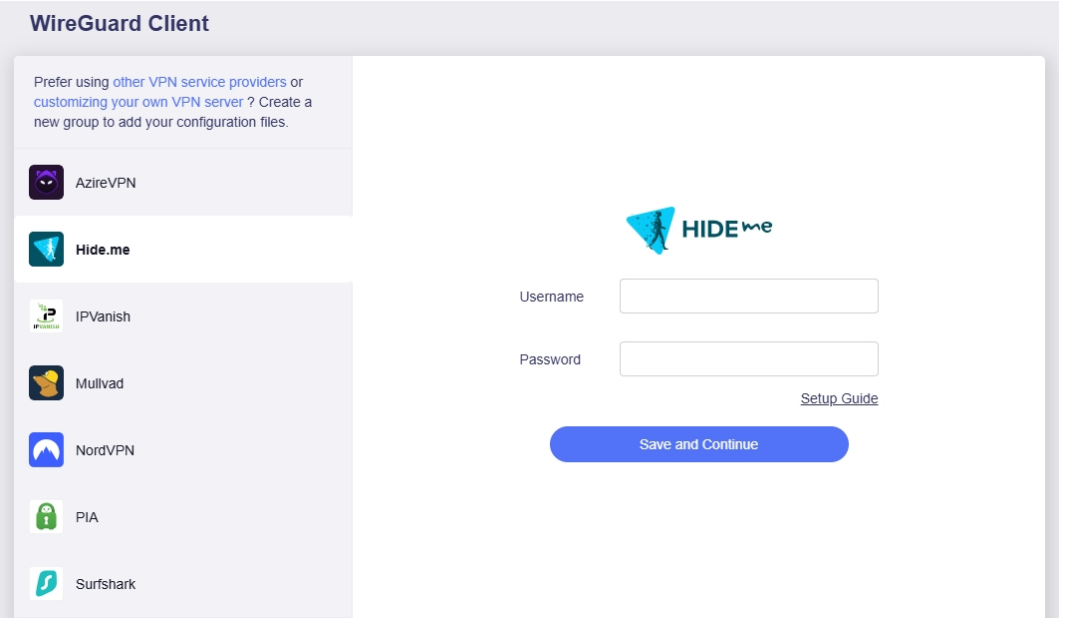
8. Supprimez tous les fichiers.
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.


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

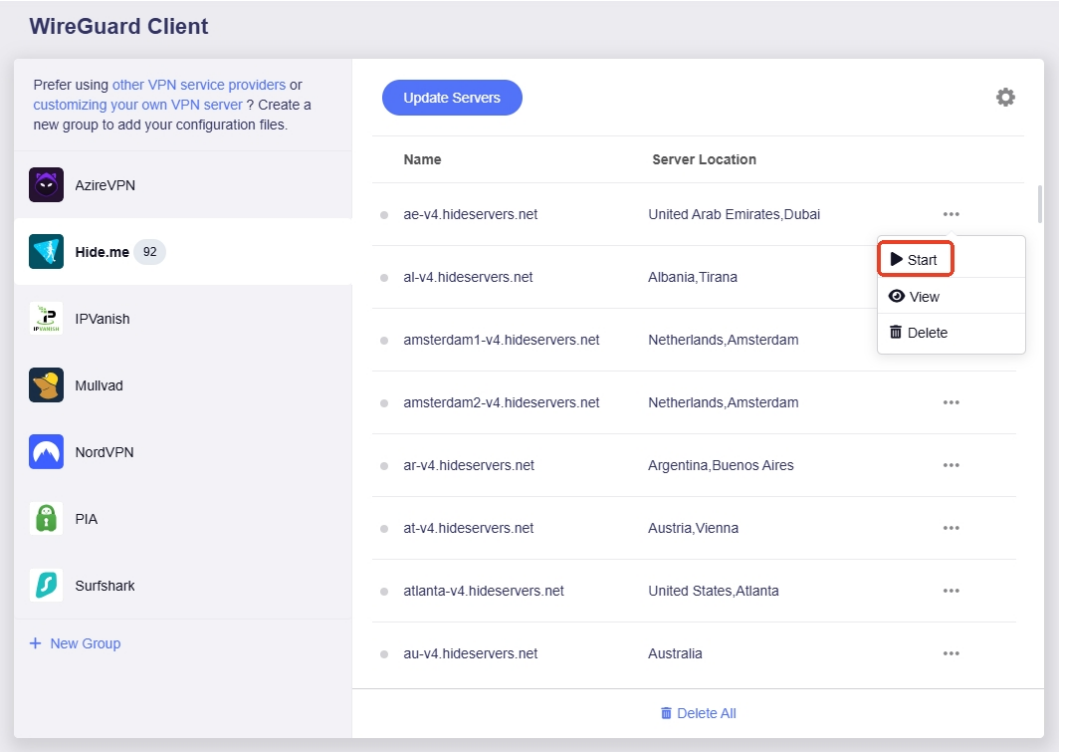
11.2.3 Configuration de Hide.me

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

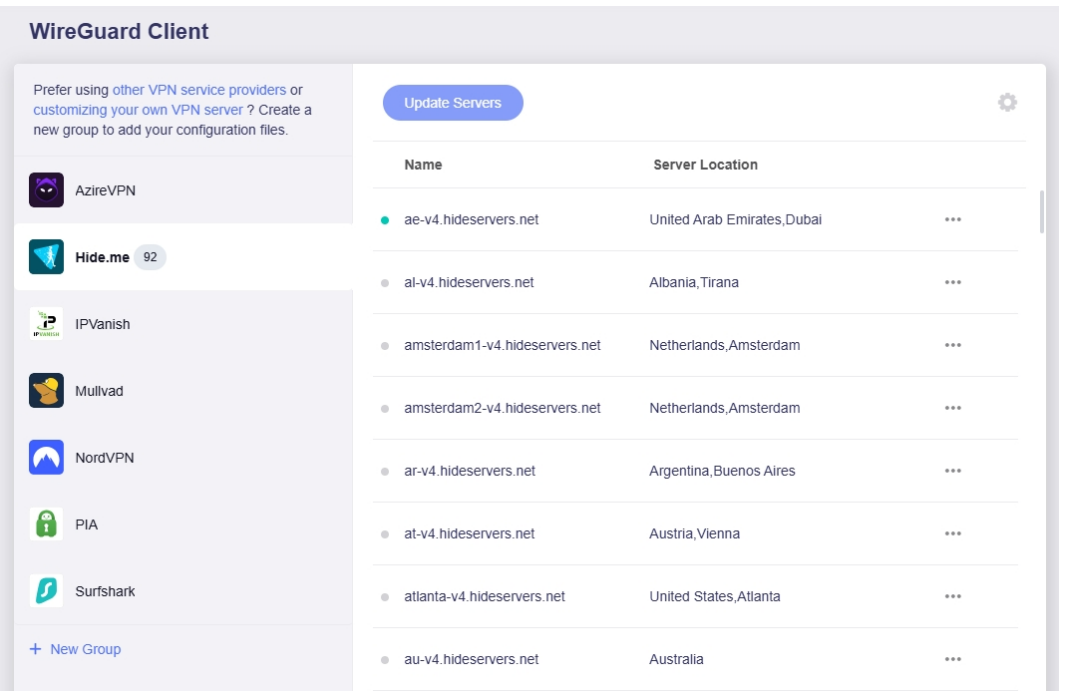
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Hide.me**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



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



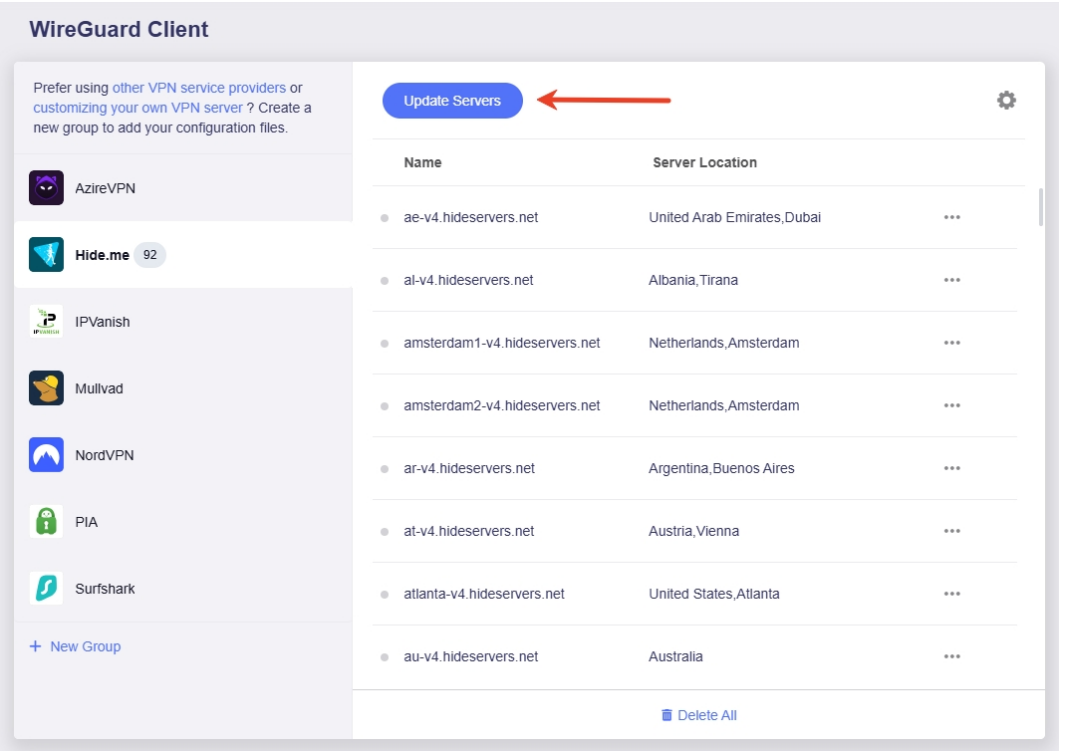
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



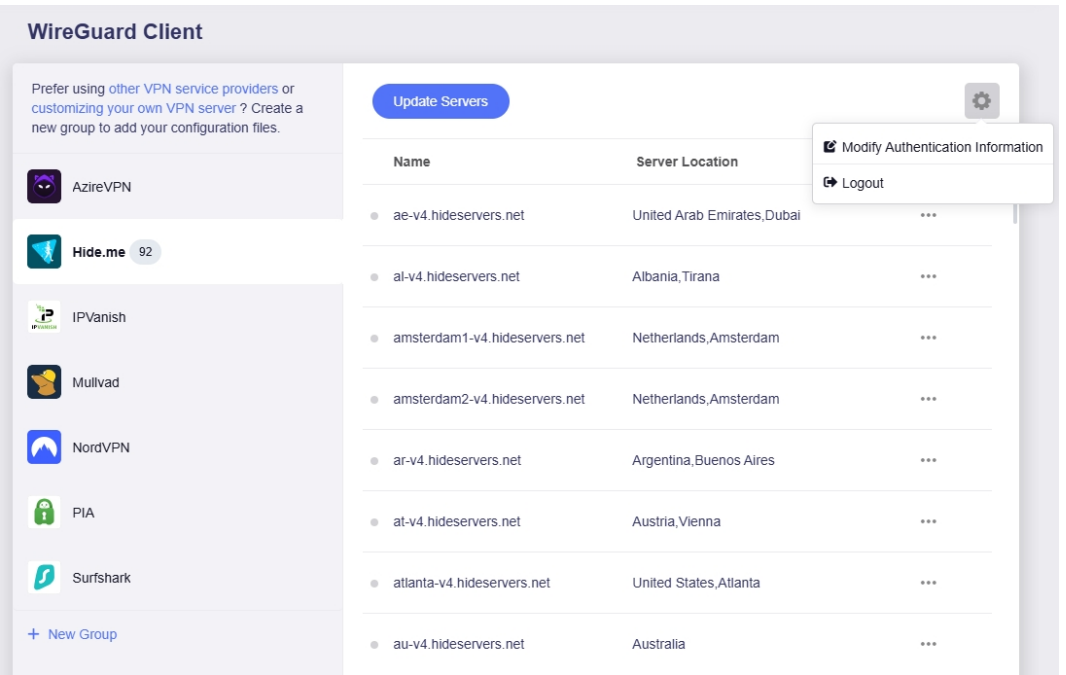
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

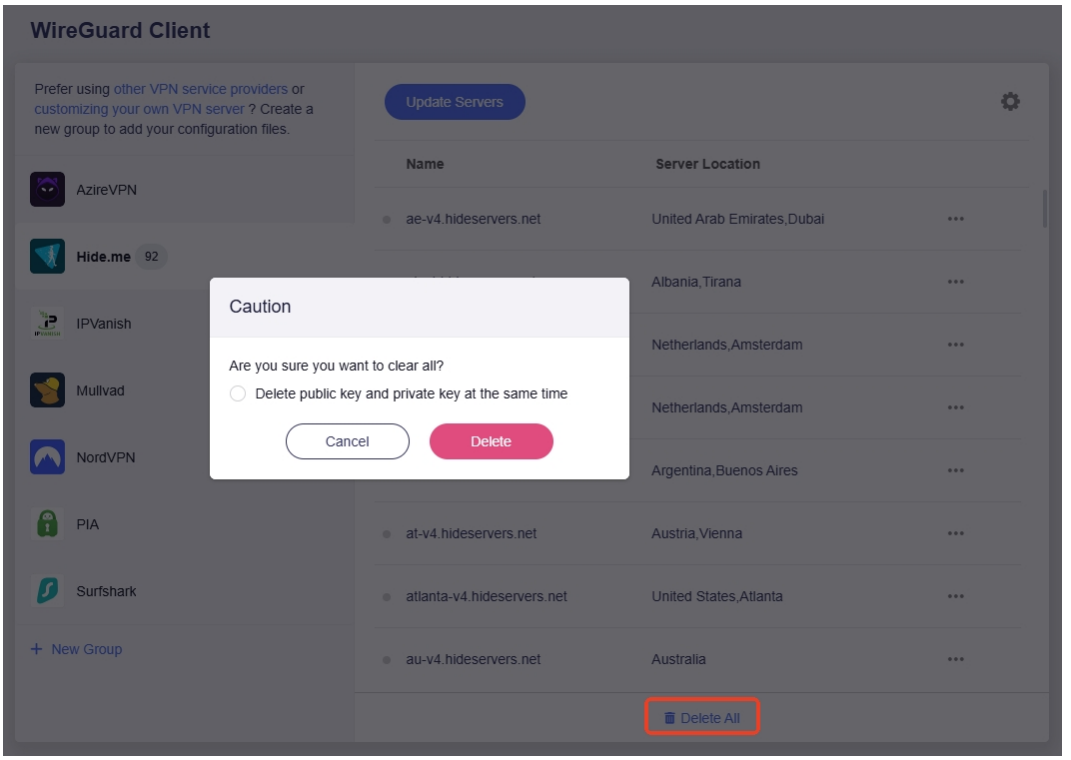


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



7. Supprimez tous les fichiers.

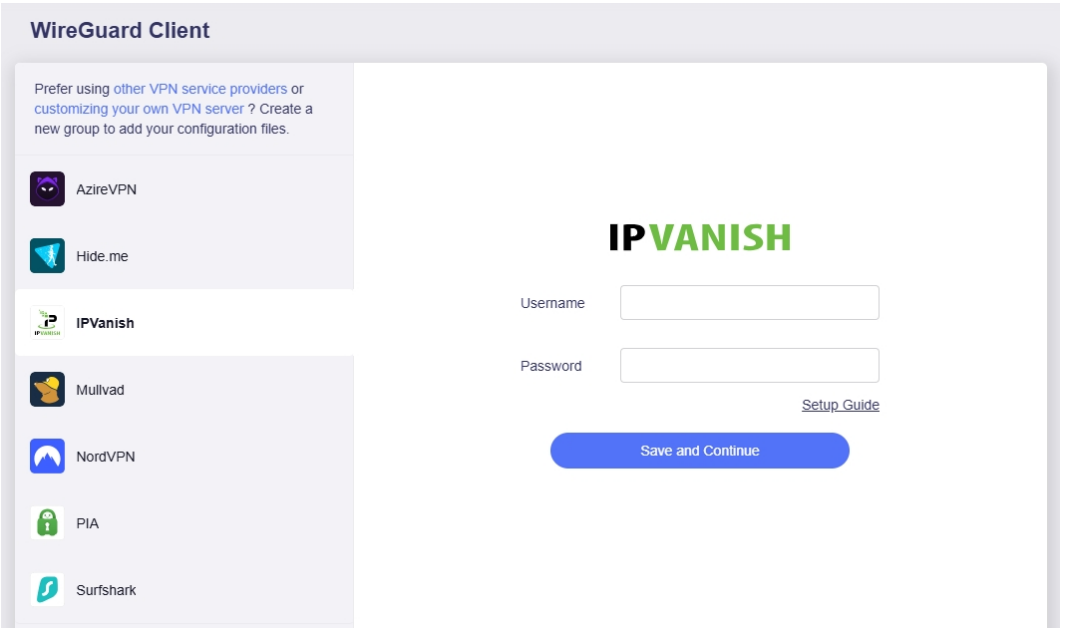
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



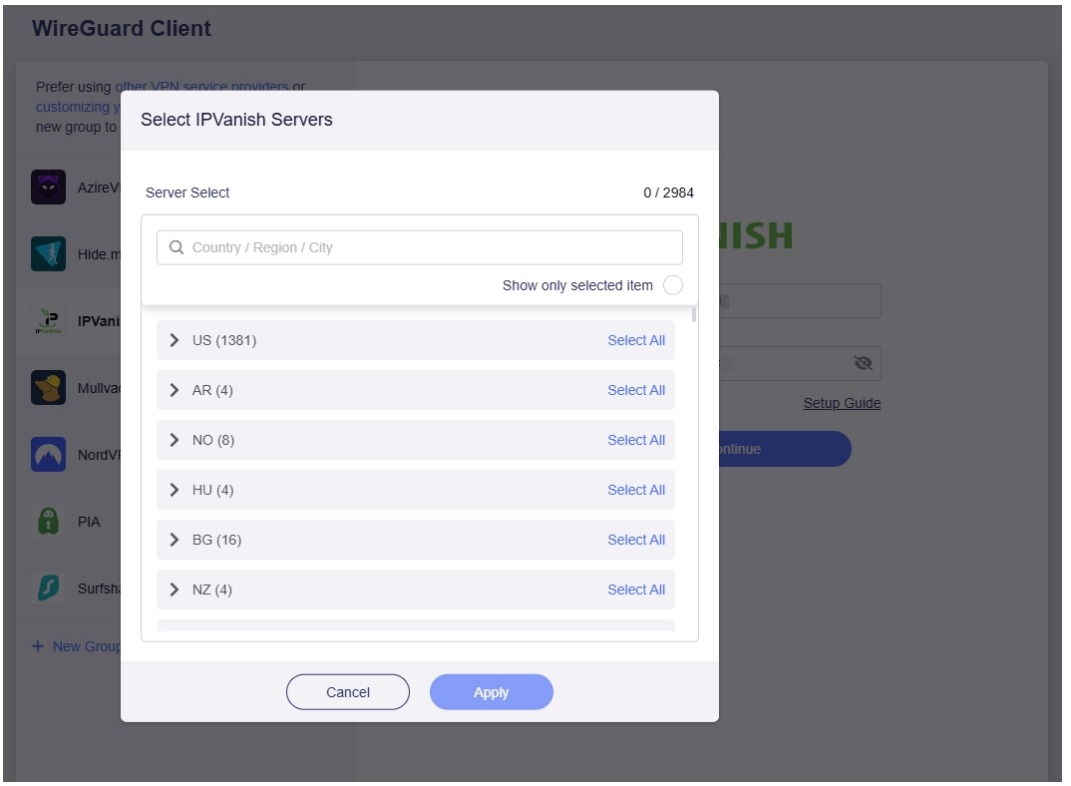
11.2.4 Configuration d'IPVanish

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

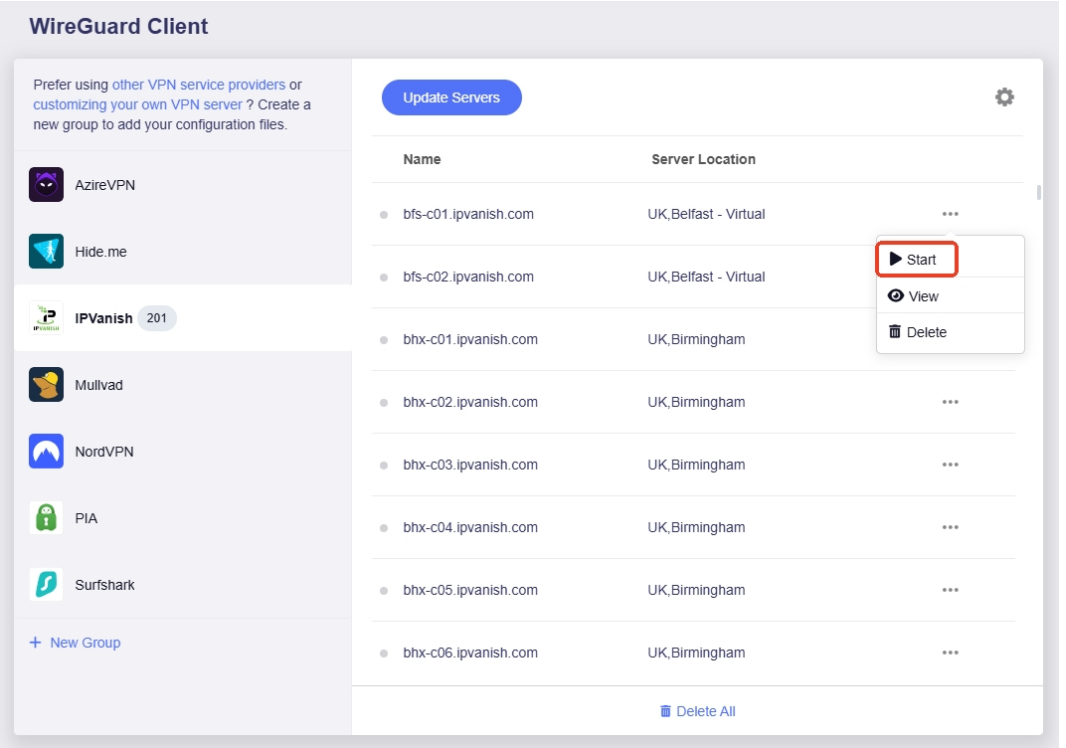
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **IPVanish**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



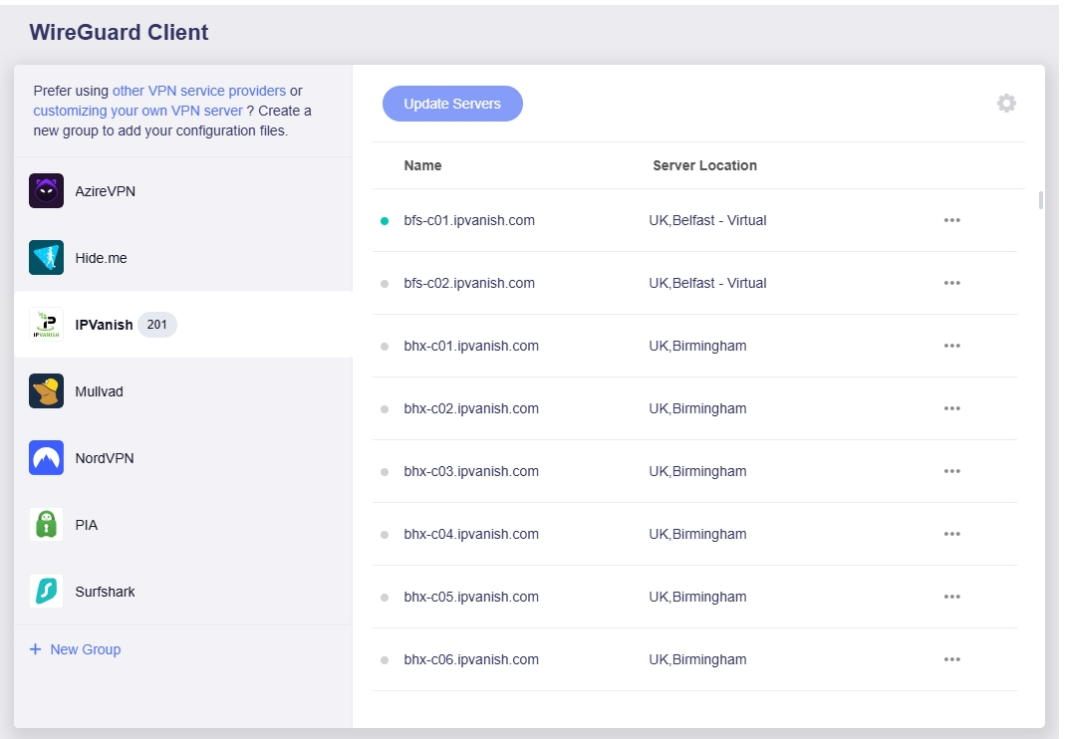
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



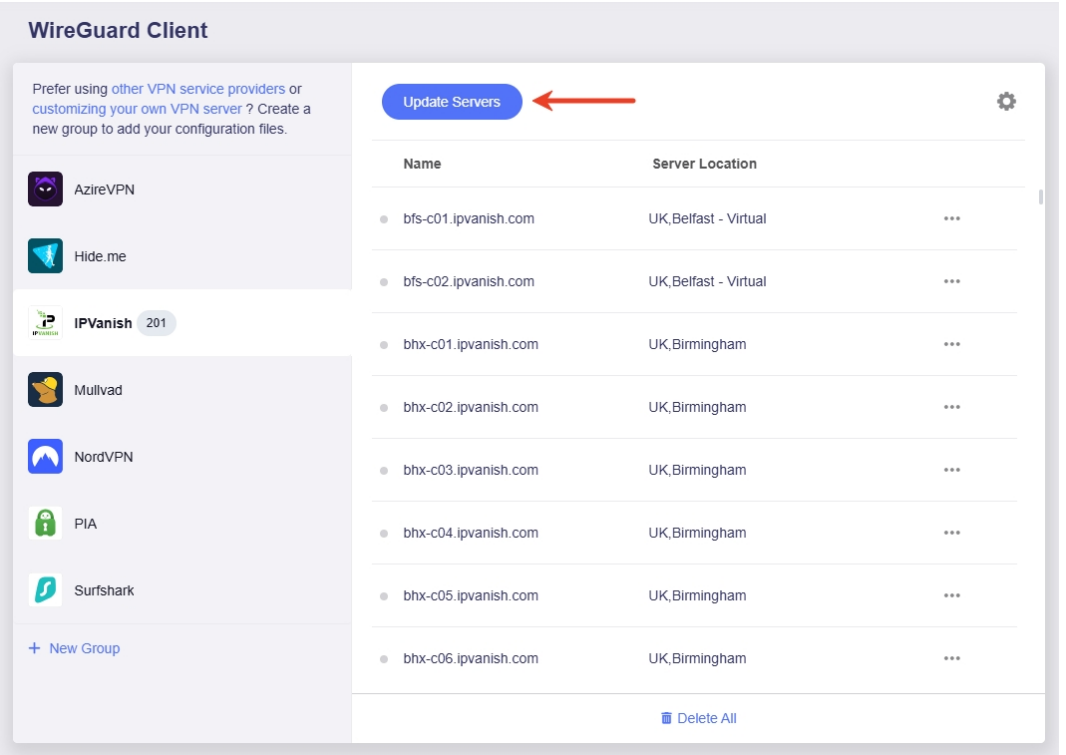
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



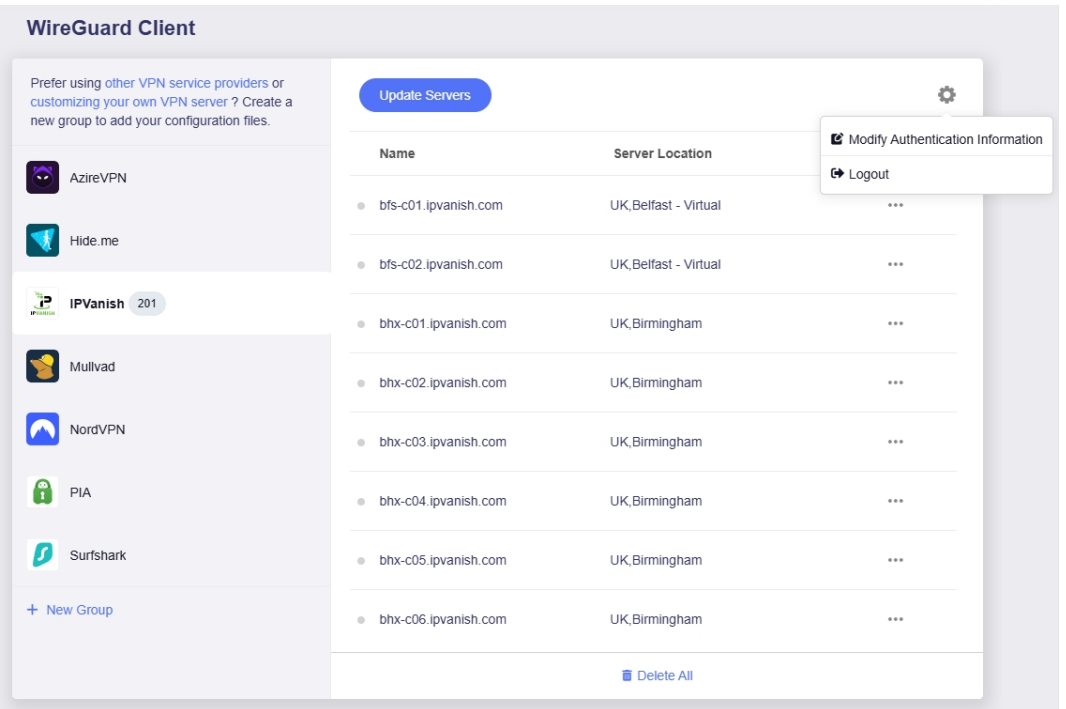
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

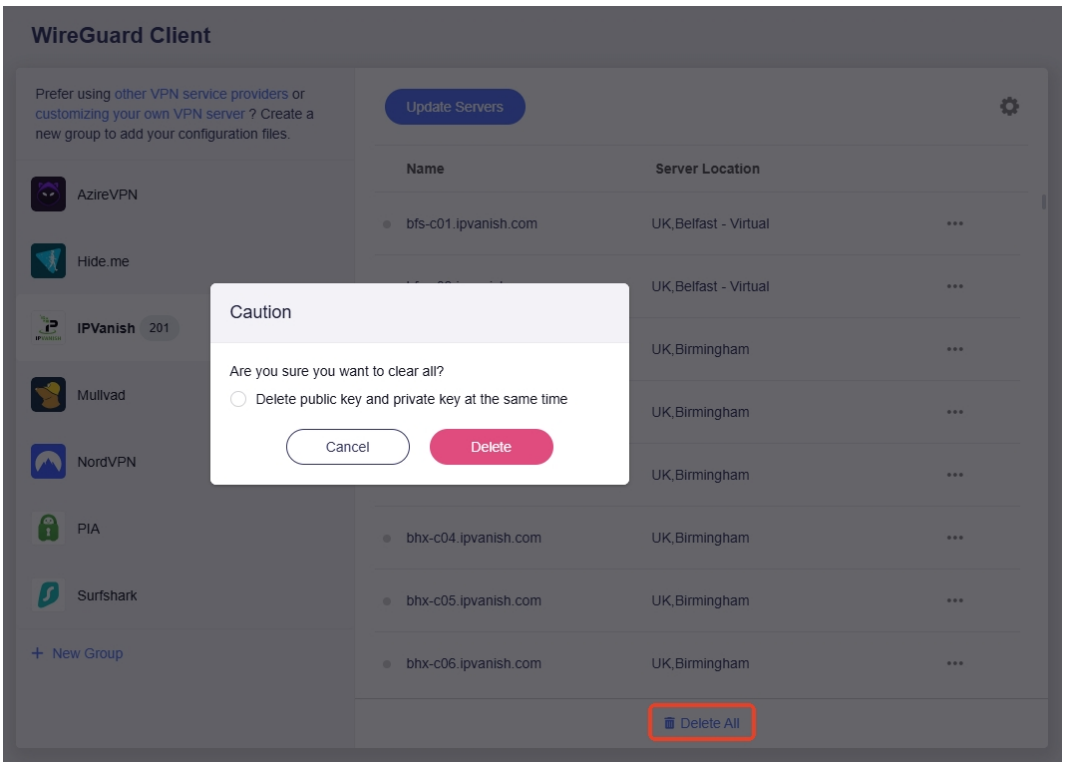


7. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

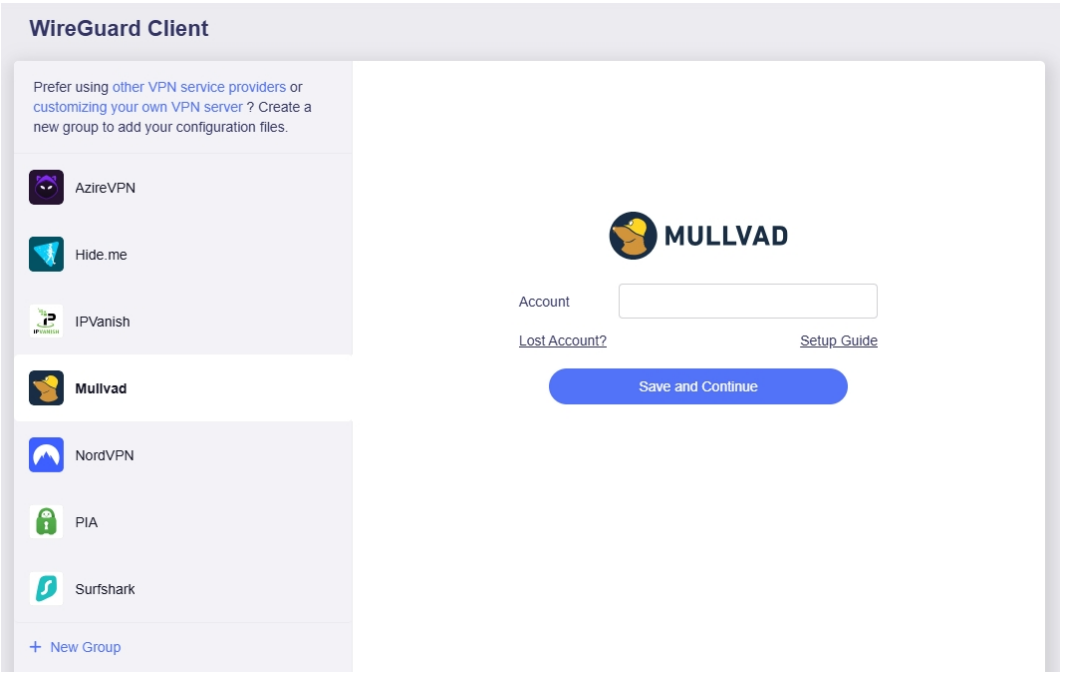
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



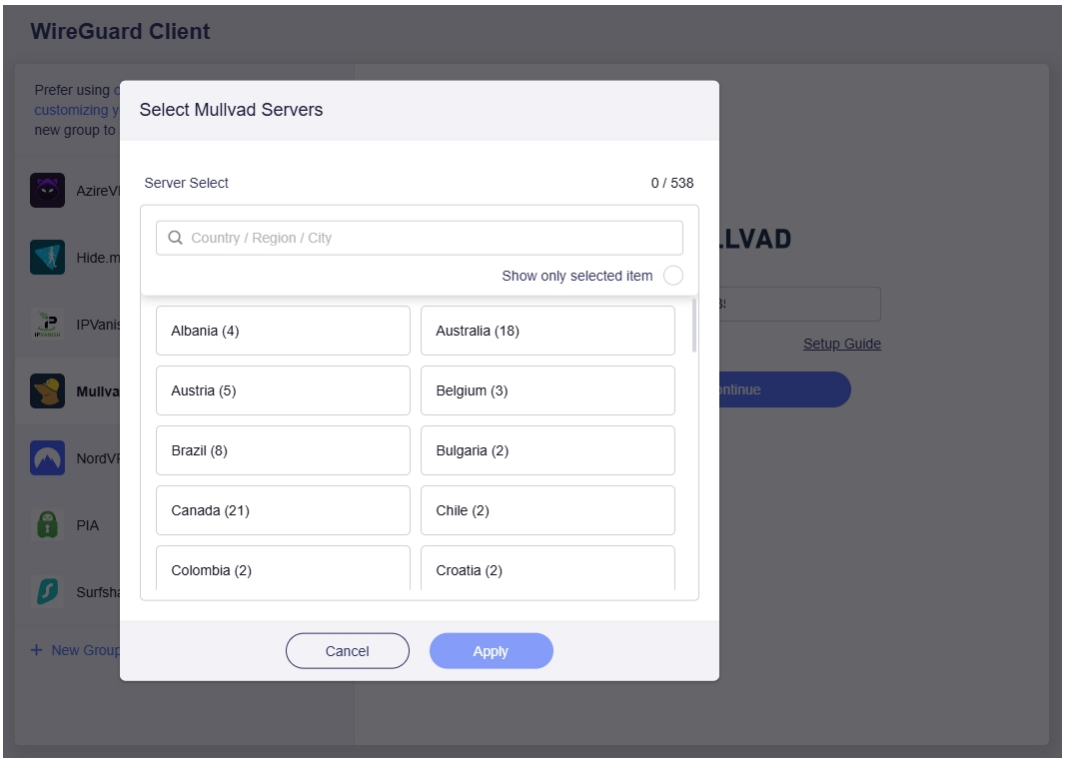
11.2.5 Configuration de Mullvad

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

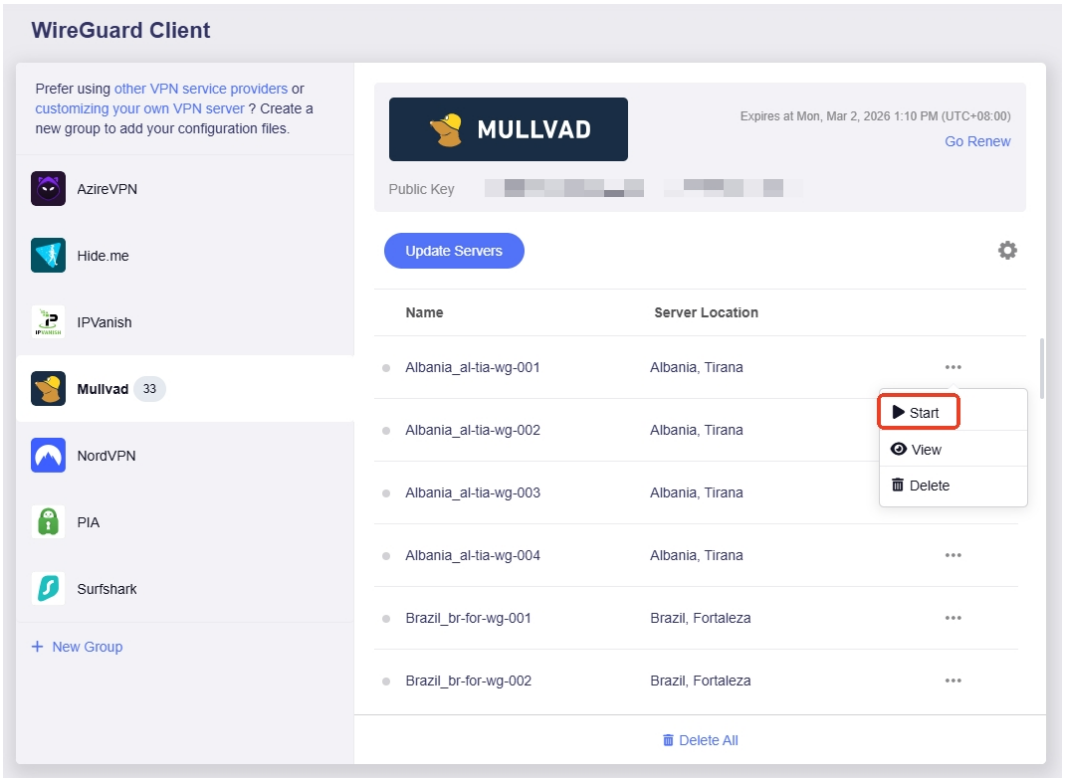
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Mullvad**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



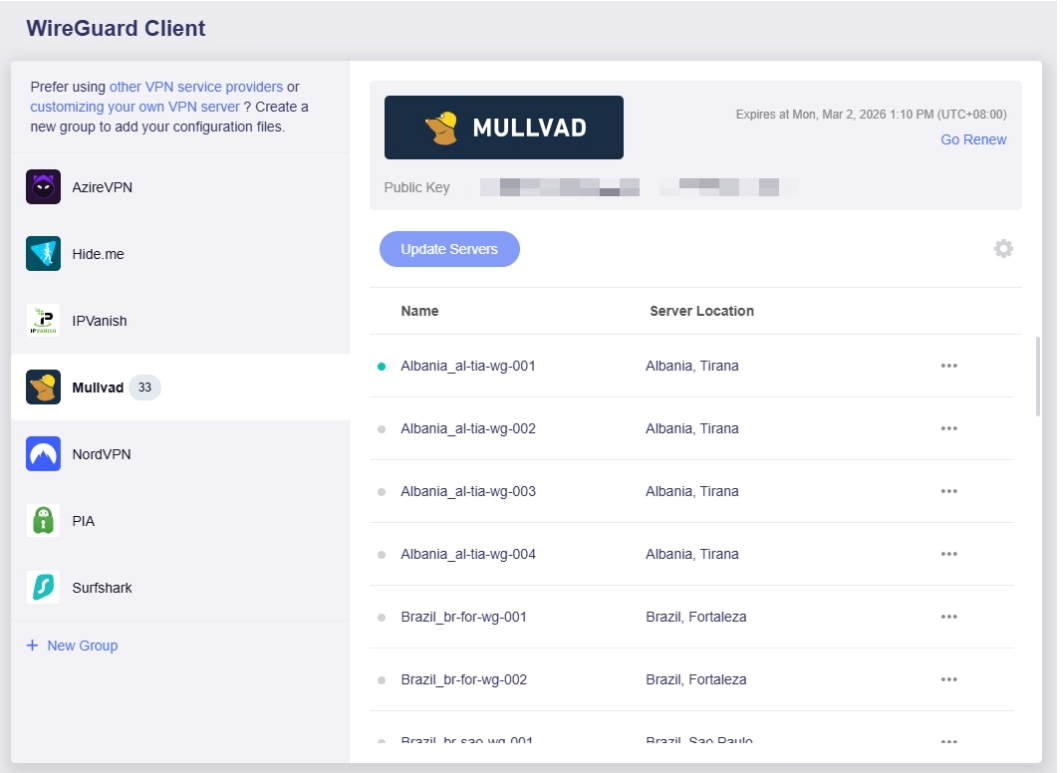
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



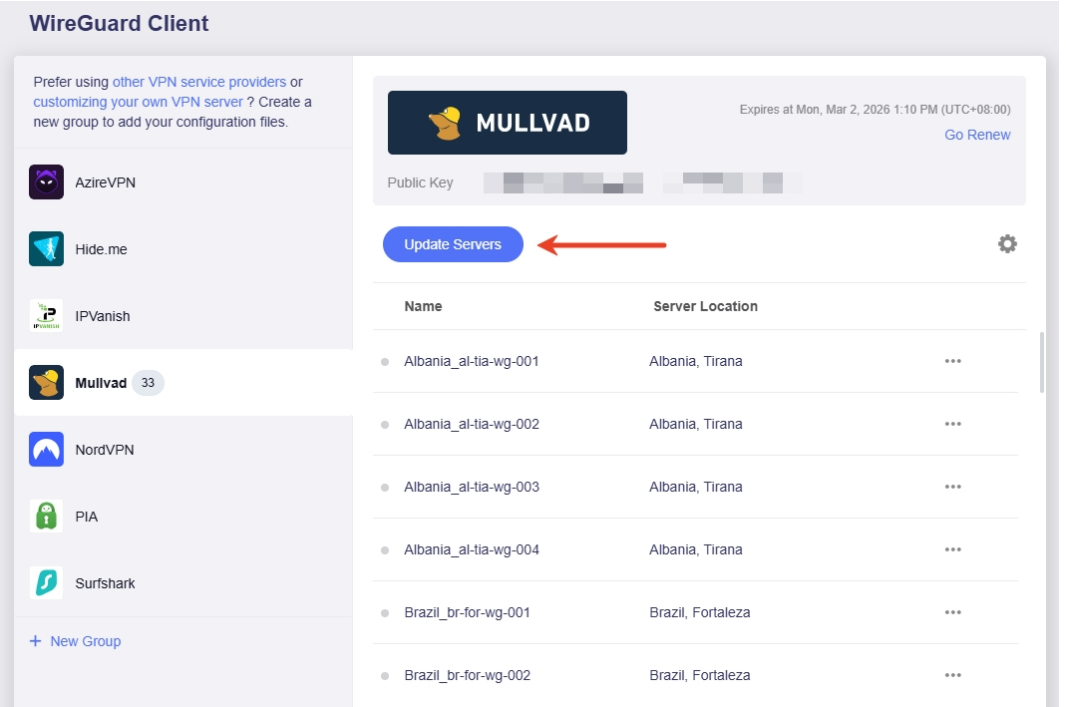
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

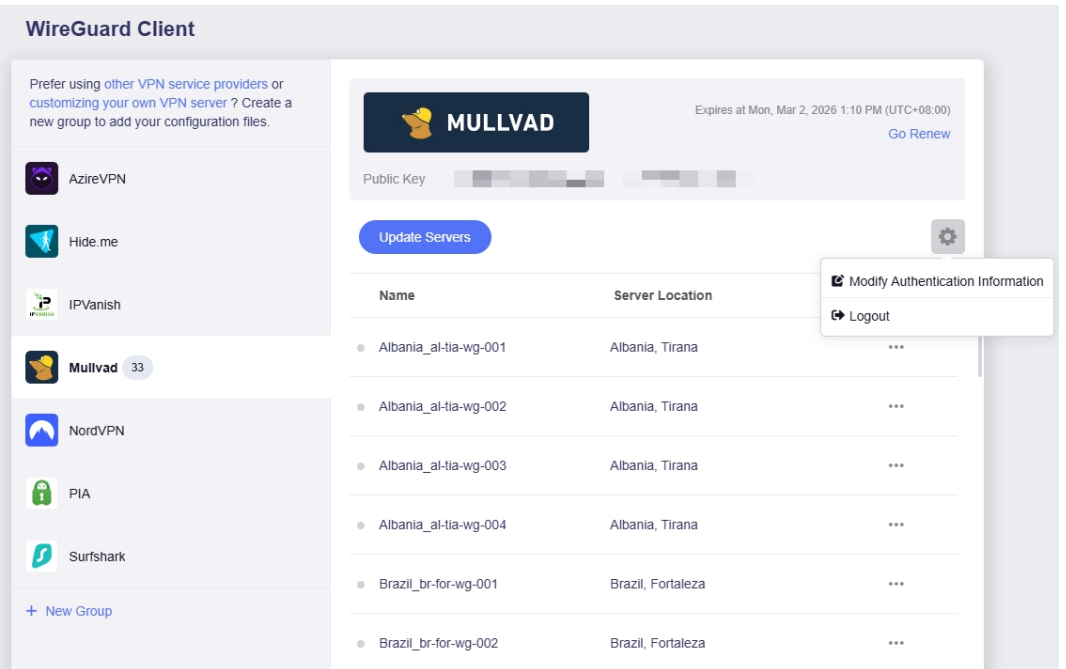
6. Mettez à jour les serveurs.

   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.



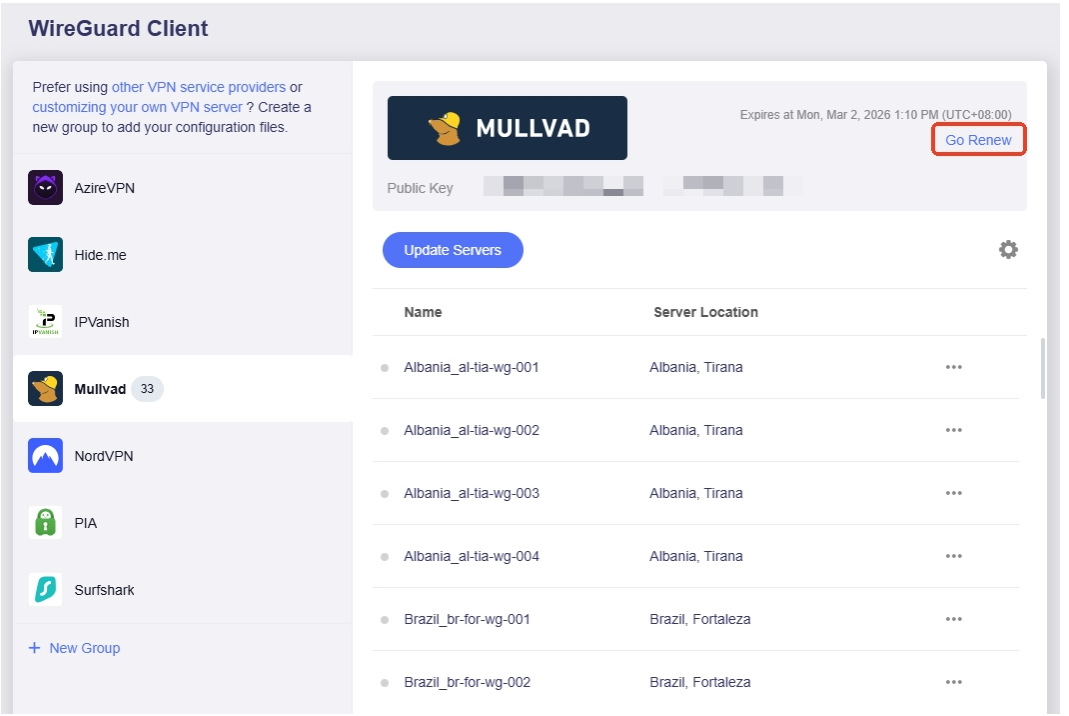
7. Modifiez les identifiants ou déconnectez-vous.

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



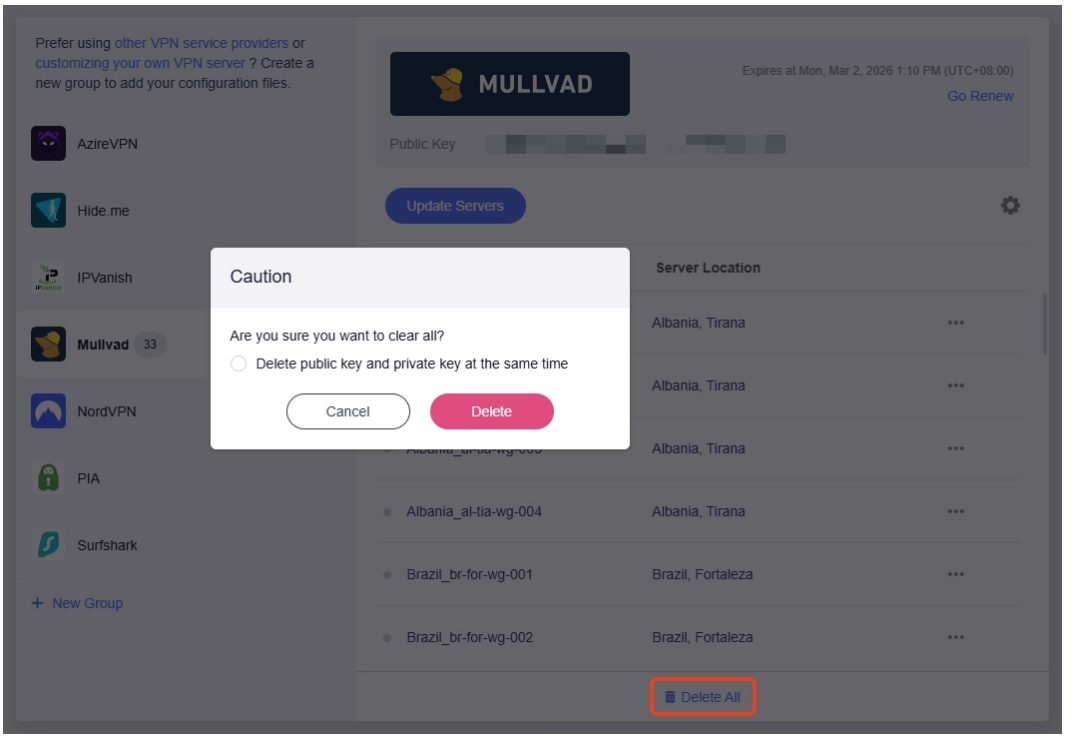
8. Renouvelez l’abonnement.

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



9. Supprimez tous les fichiers.

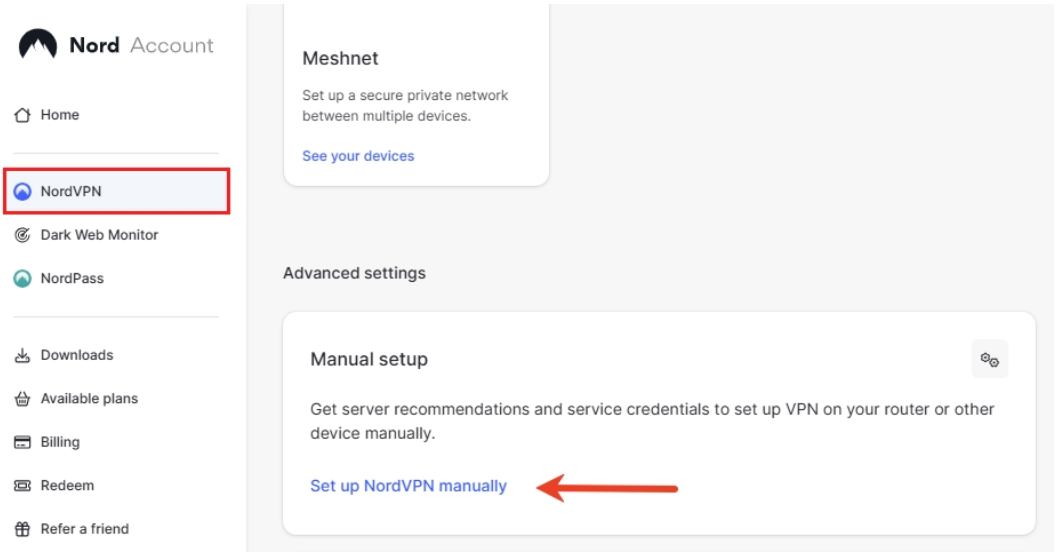
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



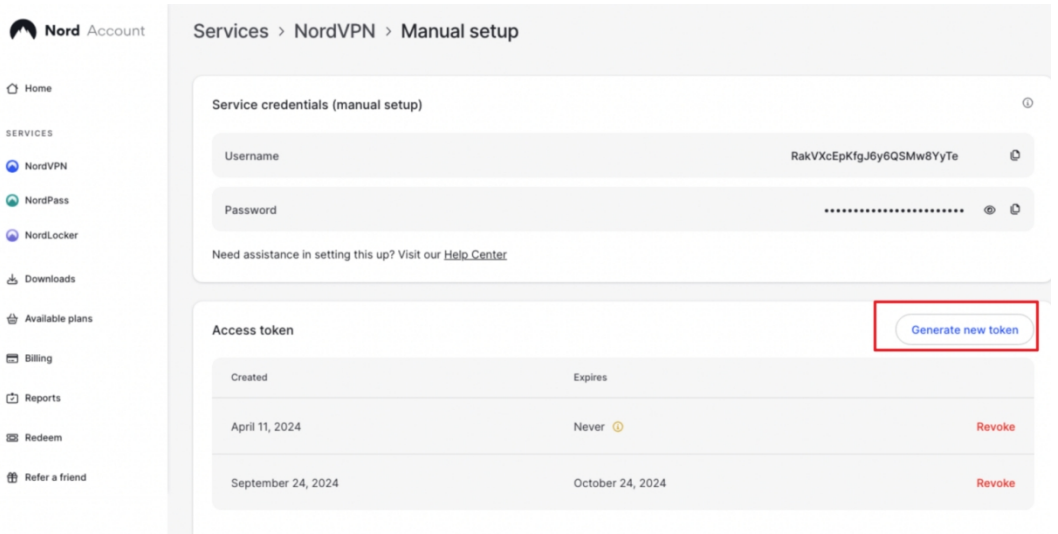
11.2.6 Configuration de NordVPN

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

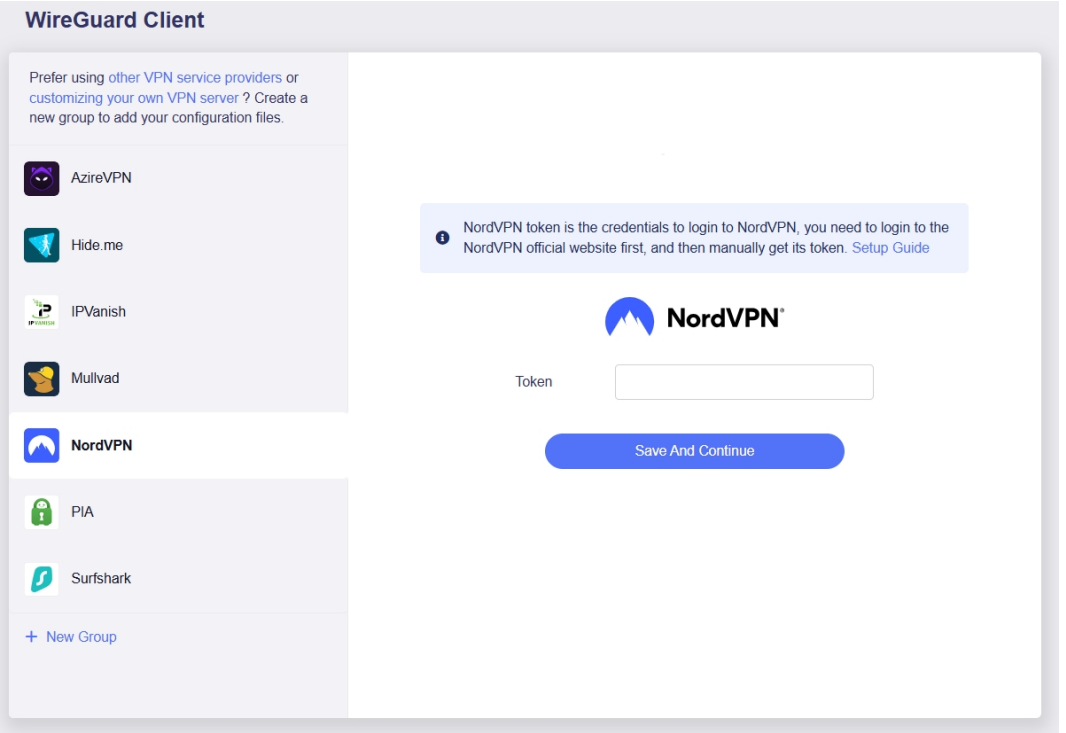
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



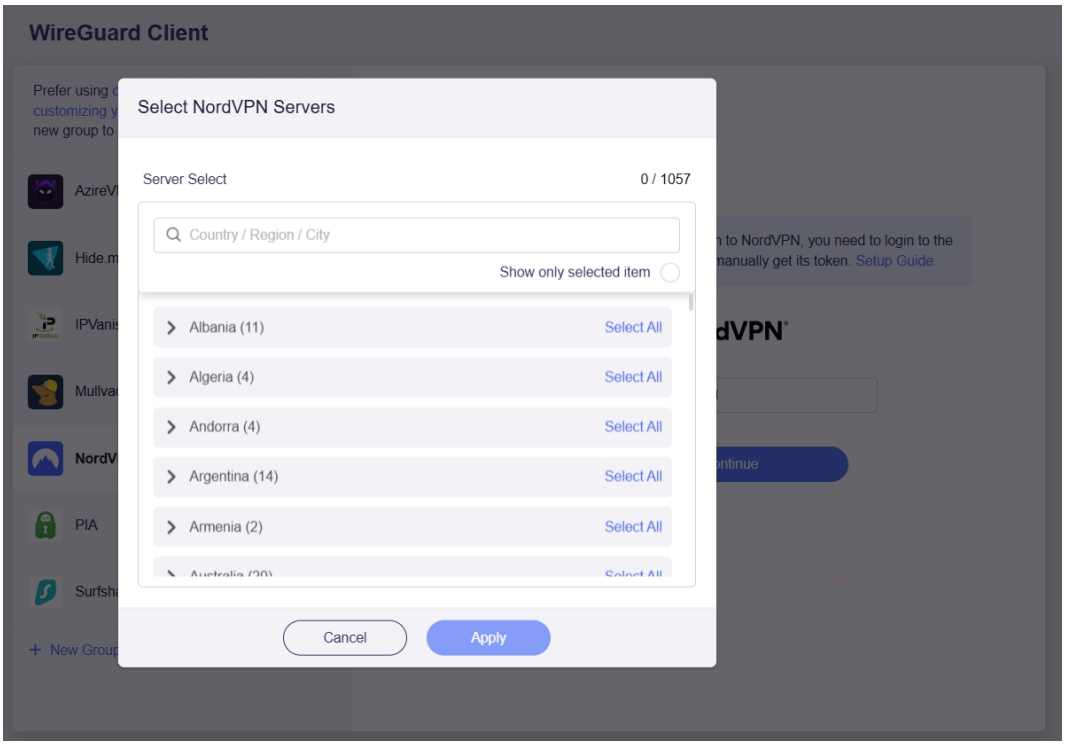
Repérez la section **Jeton d'accès (Access Token)**. Créez un jeton et copiez-le pour l'utiliser ensuite.



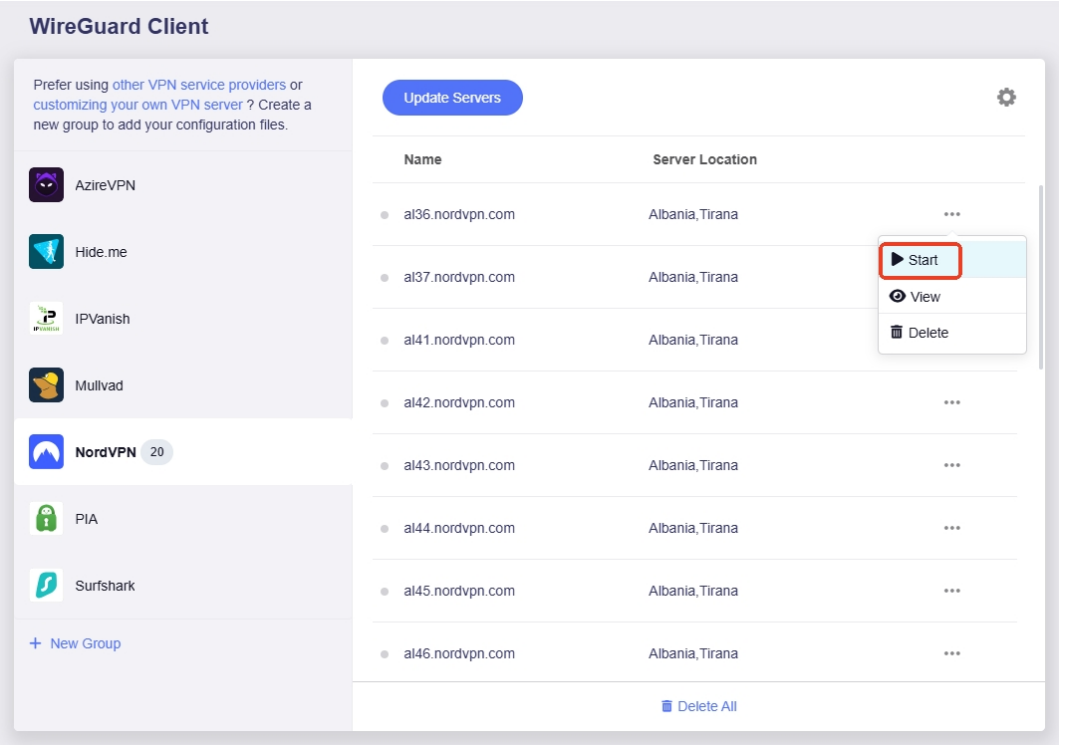
3. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **NordVPN**.
4. Saisissez le jeton et cliquez sur **Enregistrer et continuer (Save and Continue)**.



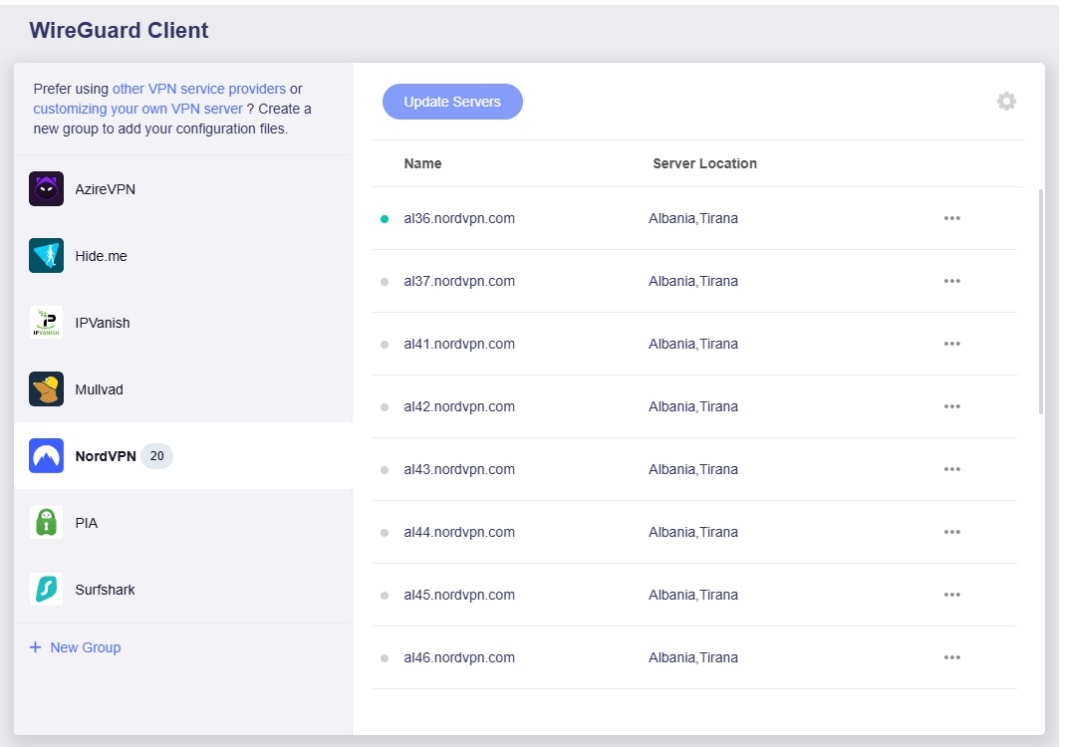
5. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



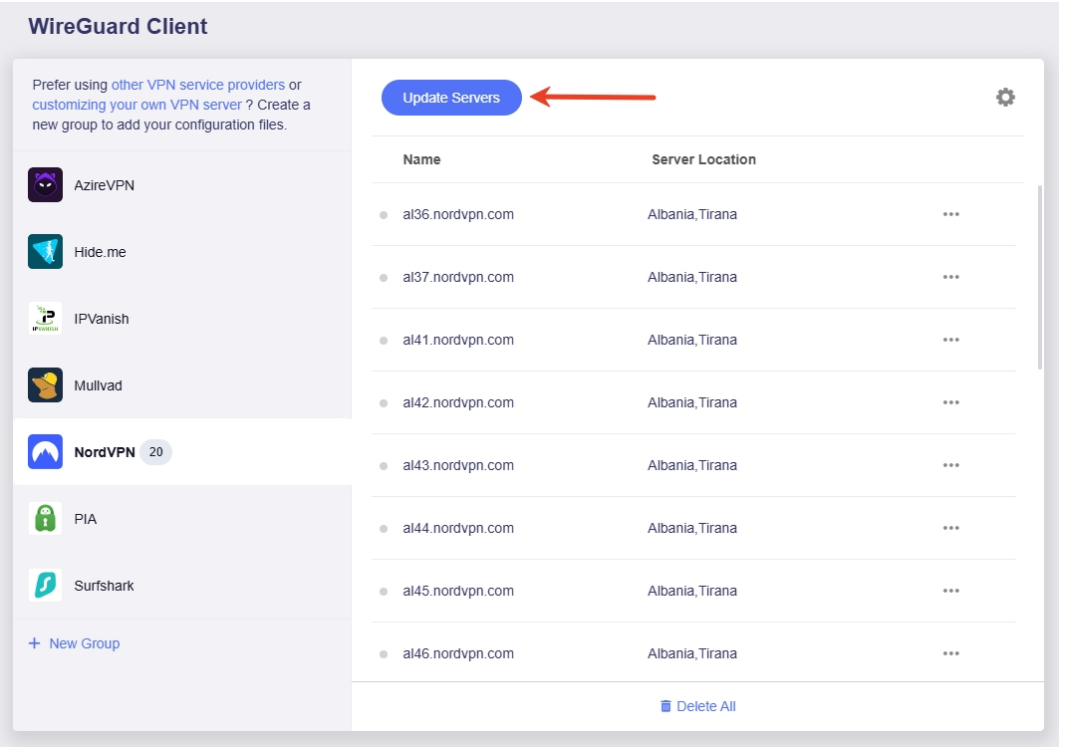
7. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



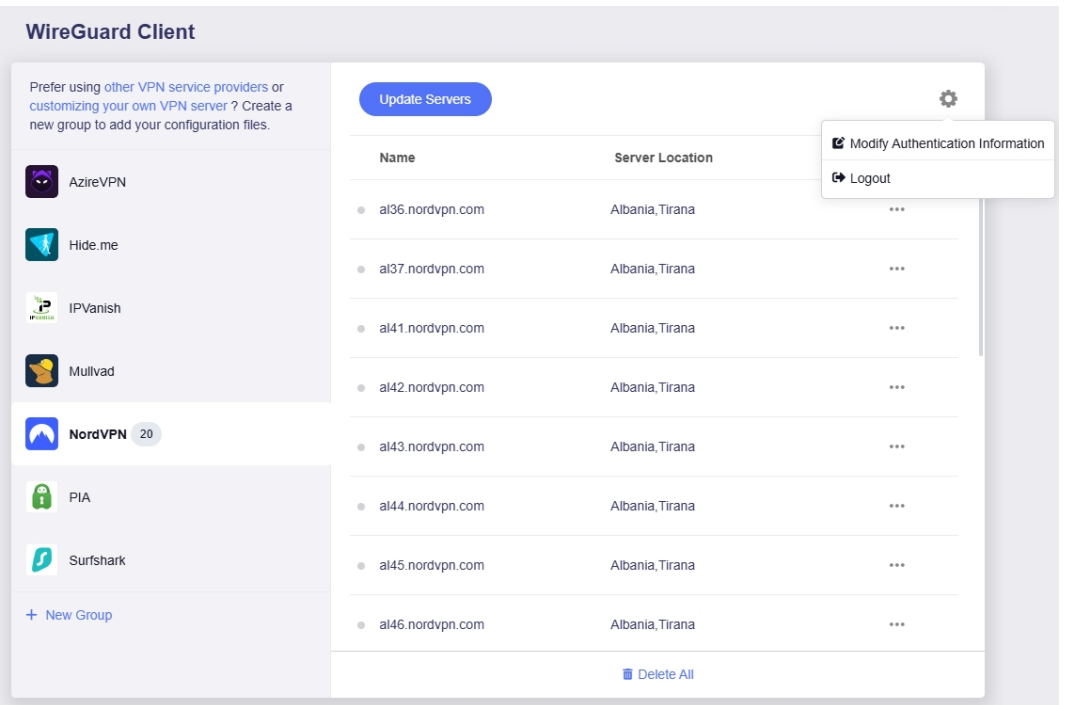
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

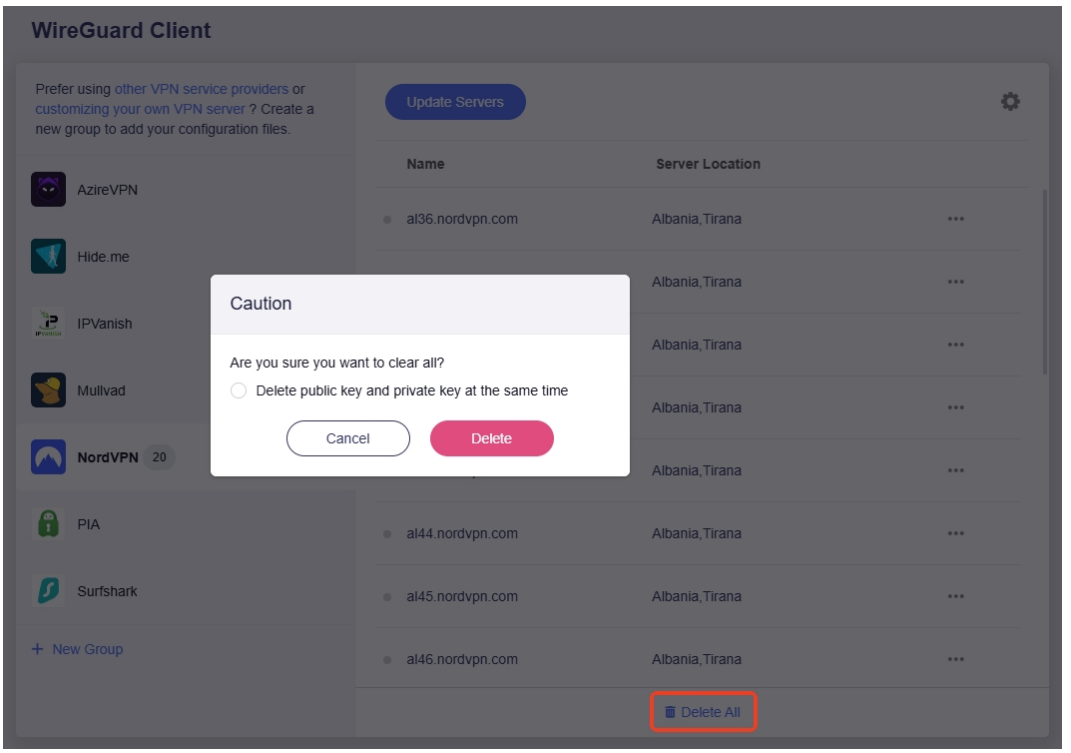


9. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



10. Supprimez tous les fichiers.

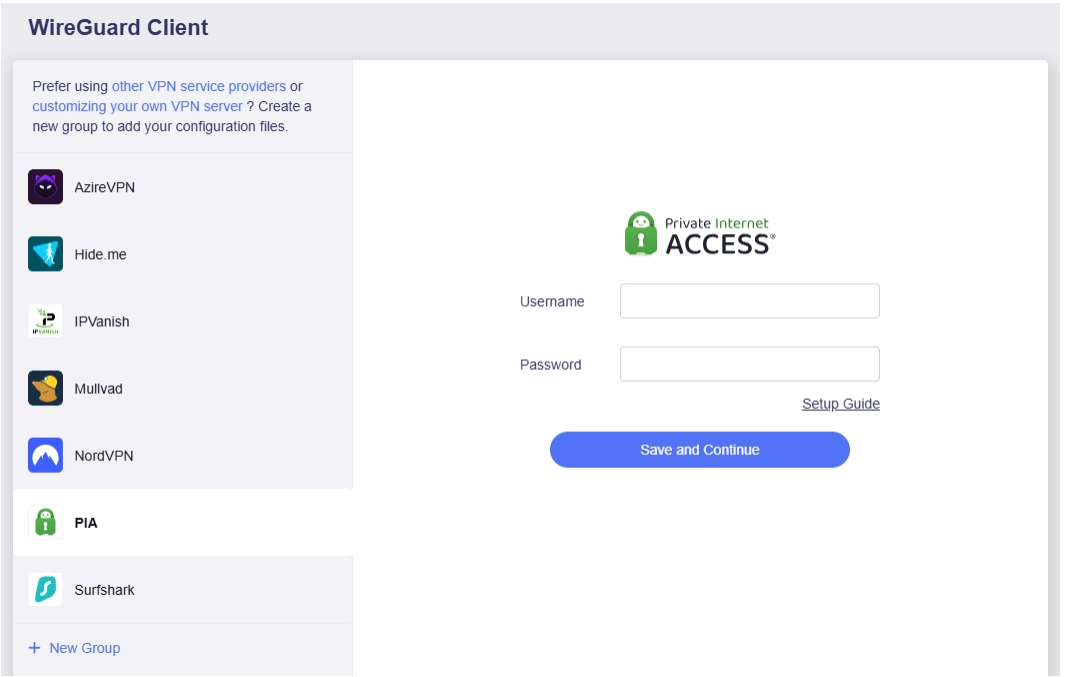
    Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



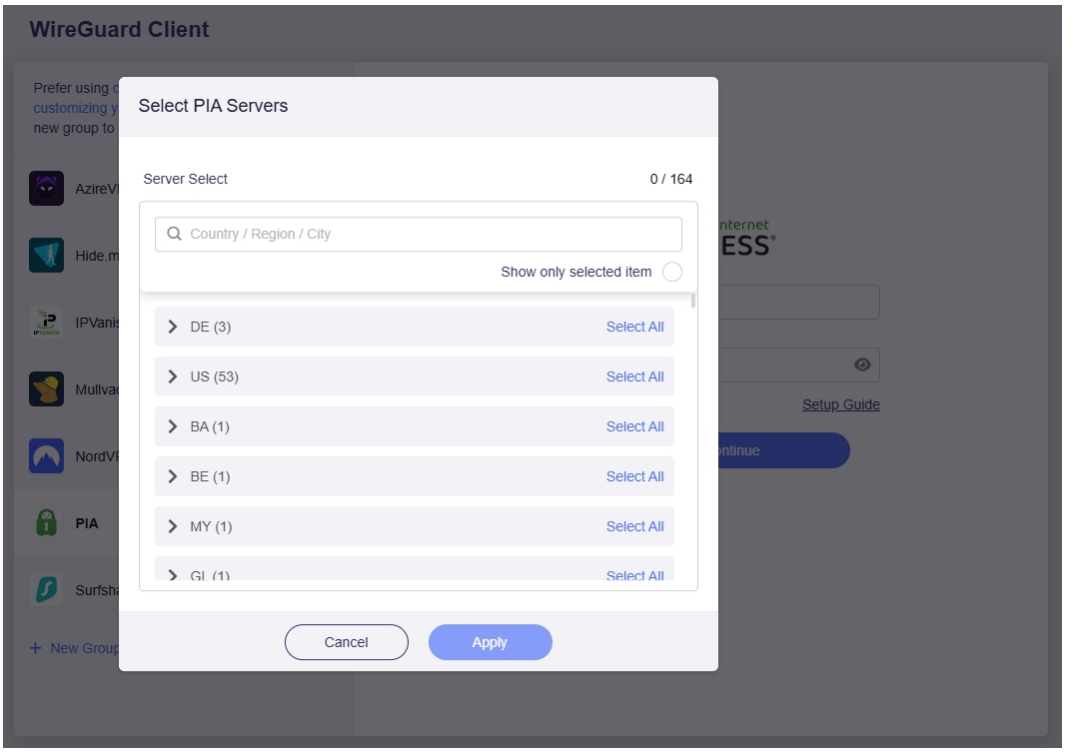
11.2.7 Configuration de PIA (Private Internet Access)

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

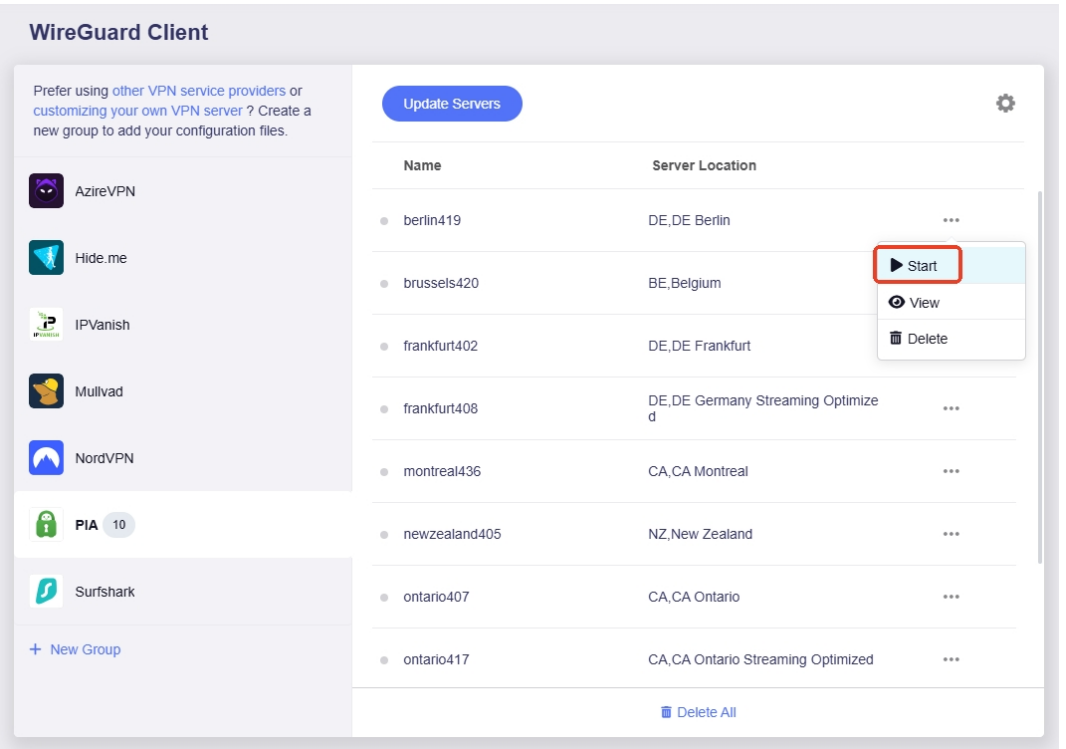
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **PIA**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



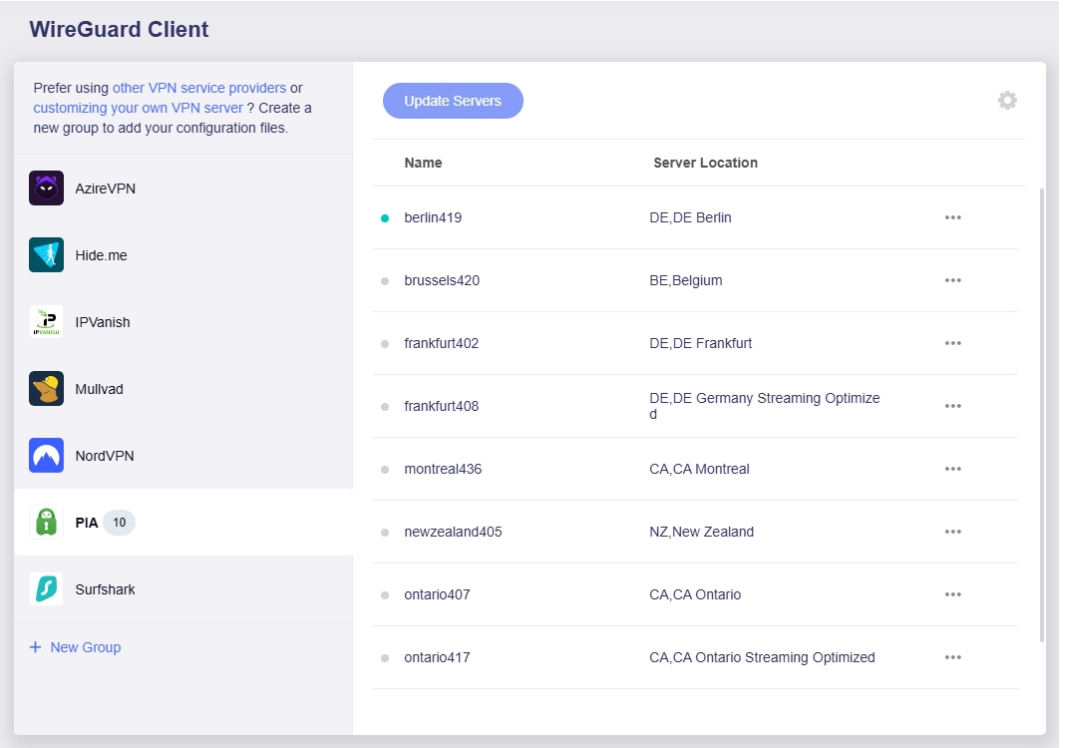
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



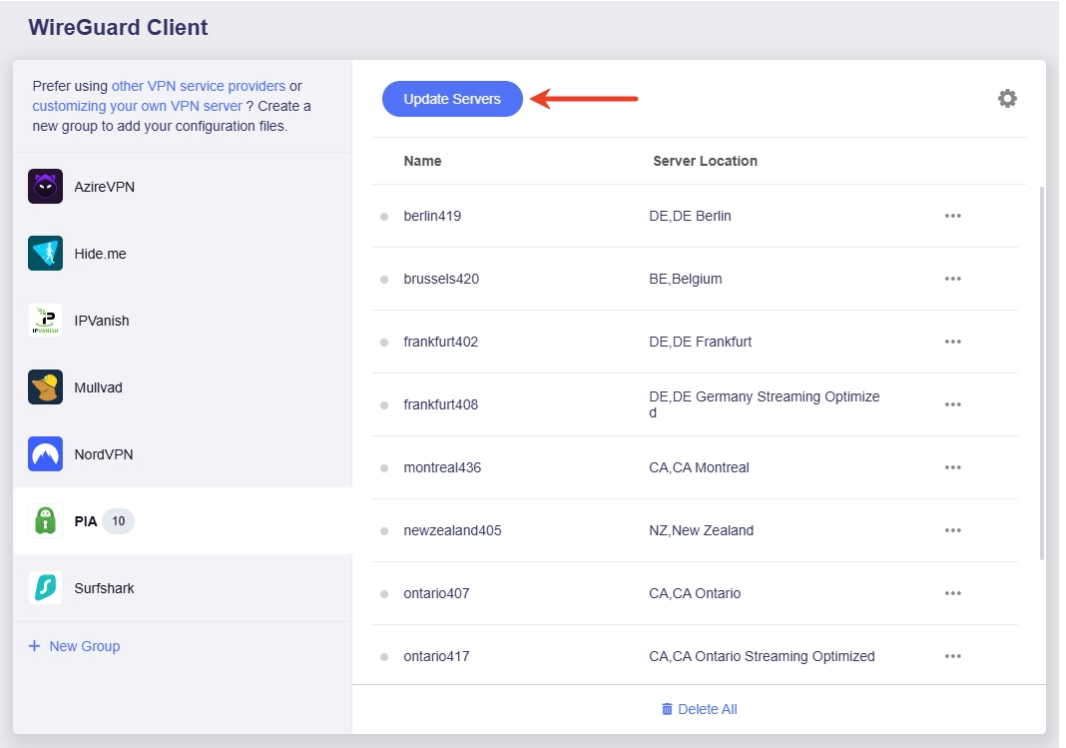
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

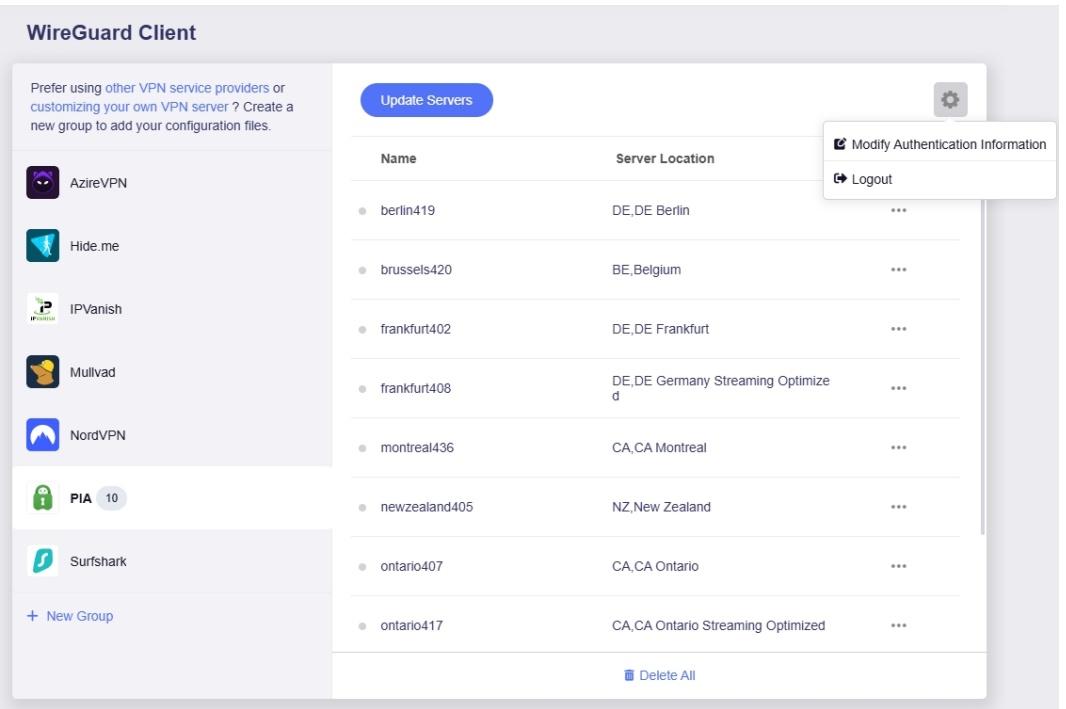
6. Mettez à jour les serveurs.

   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.



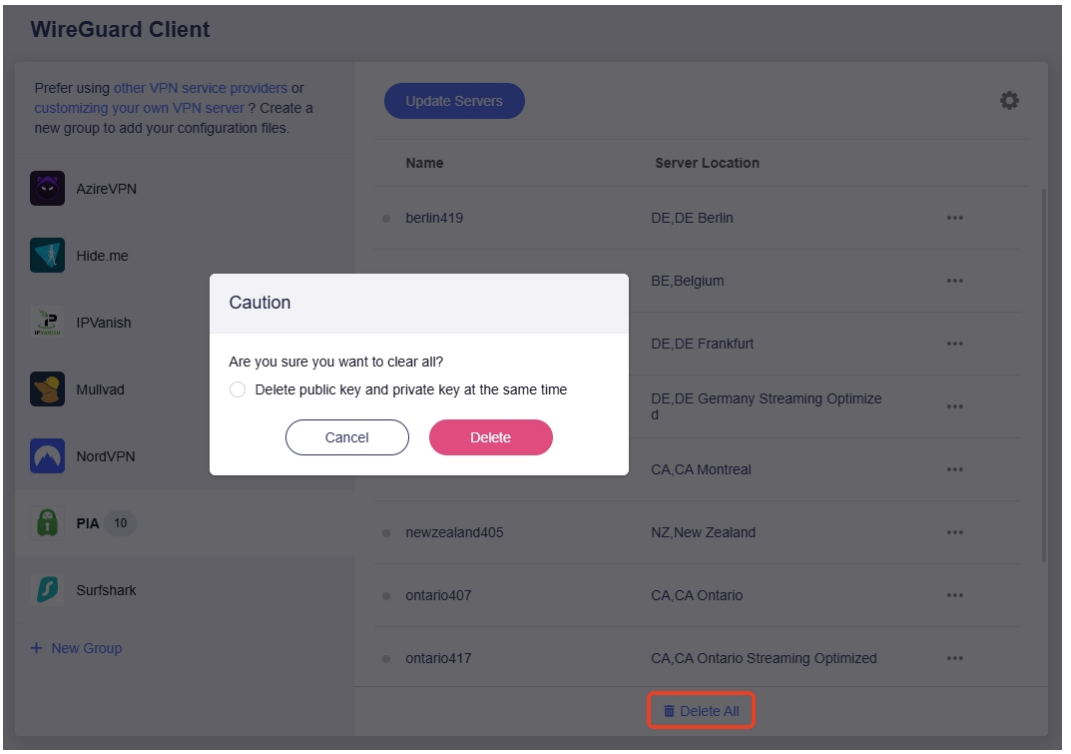
7. Modifiez les identifiants ou déconnectez-vous.

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



8. Supprimez tous les fichiers.

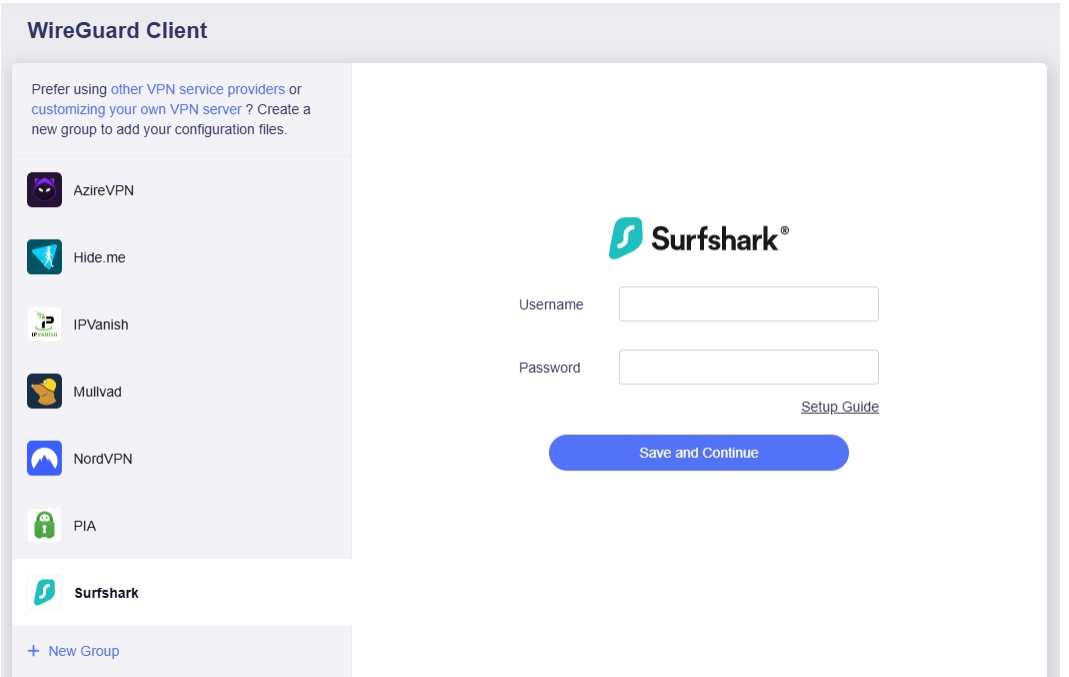
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



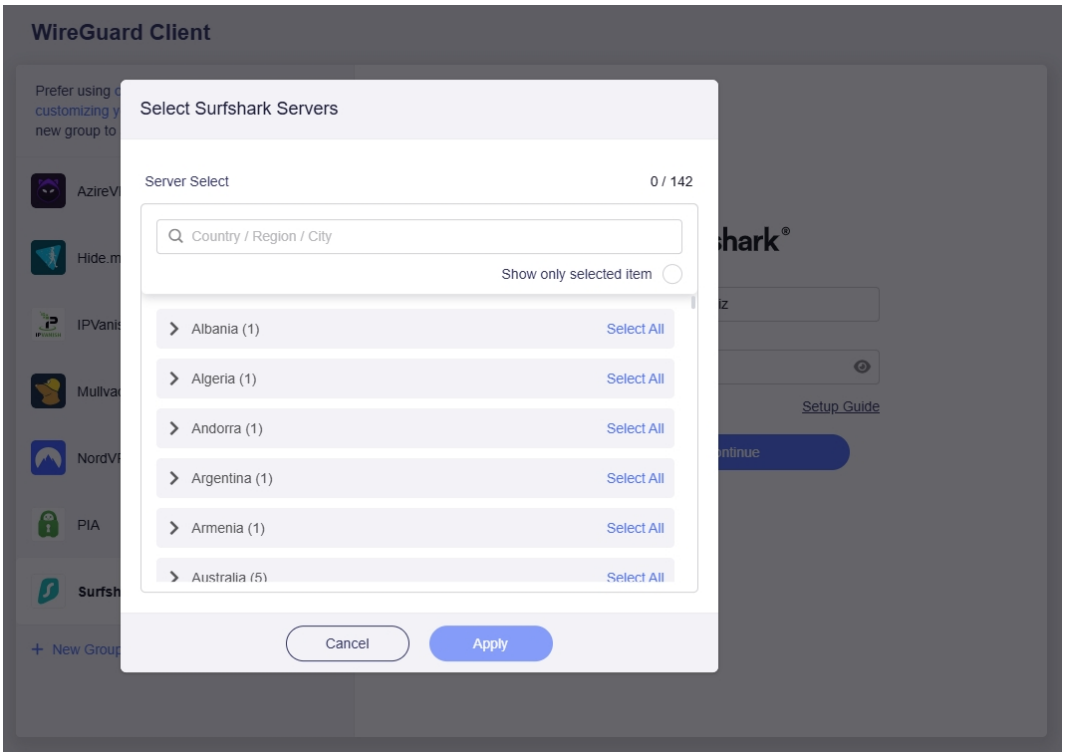
11.2.8 Configuration de Surfshark

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

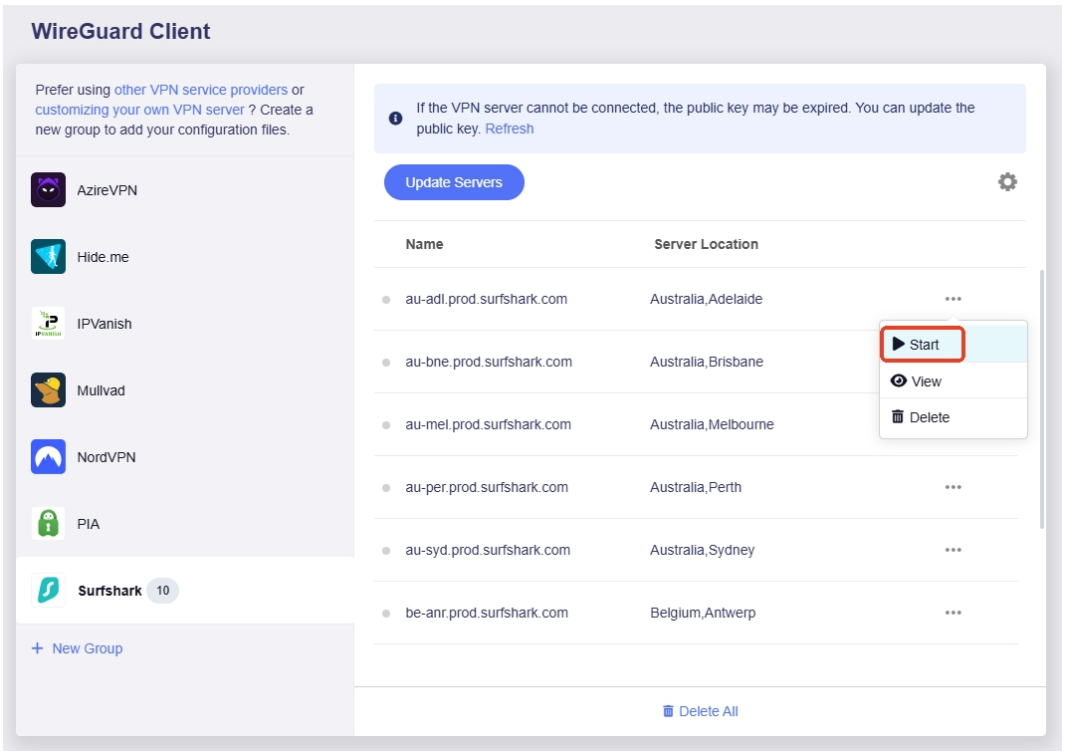
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Surfshark**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



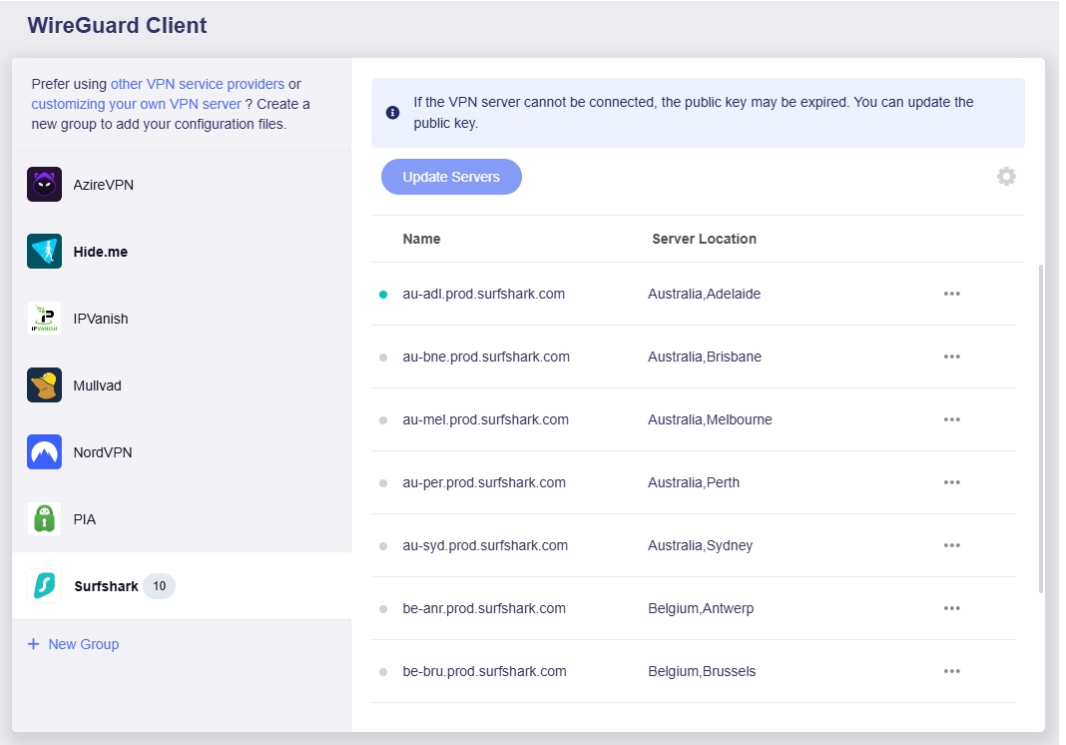
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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

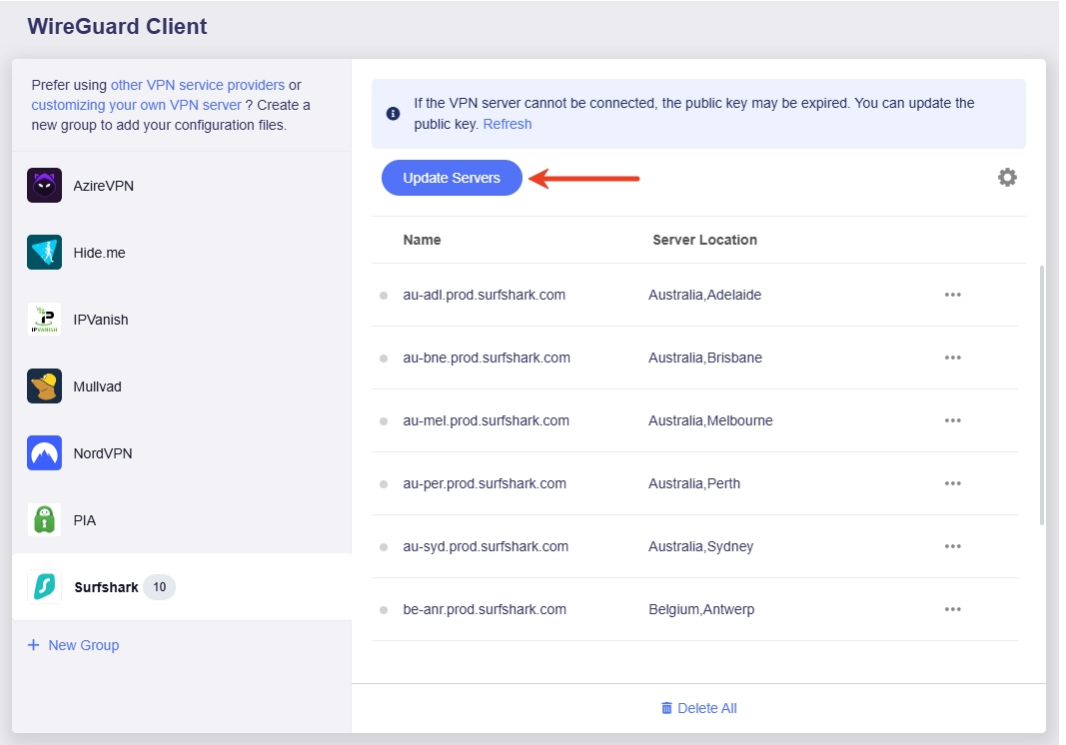


5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



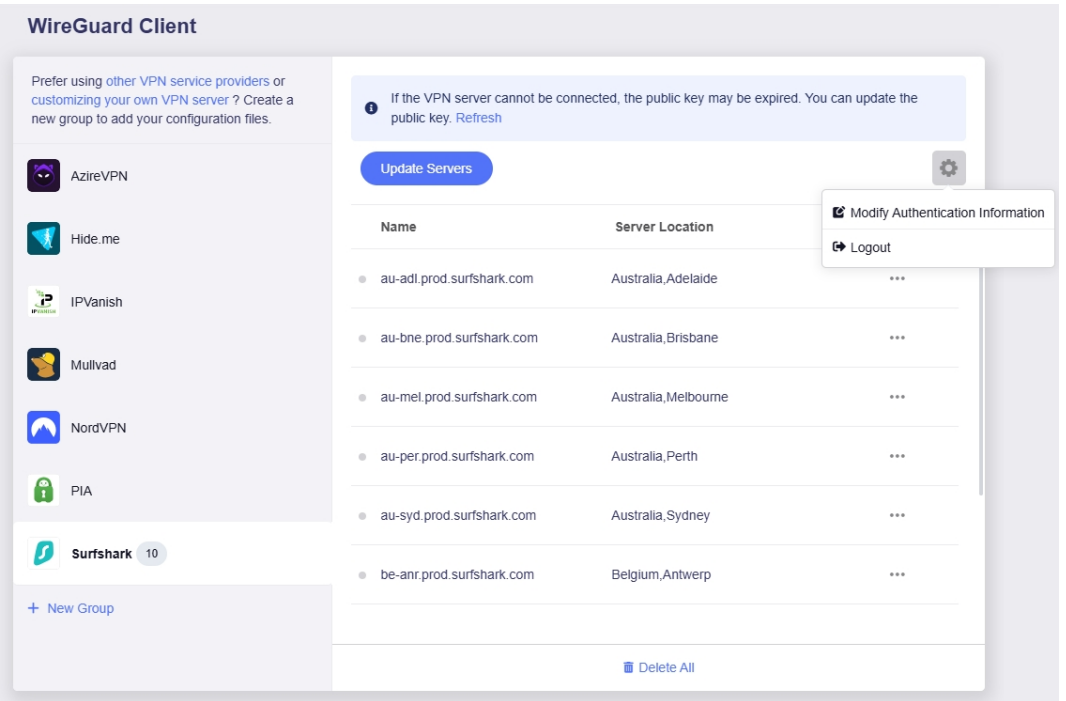
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.



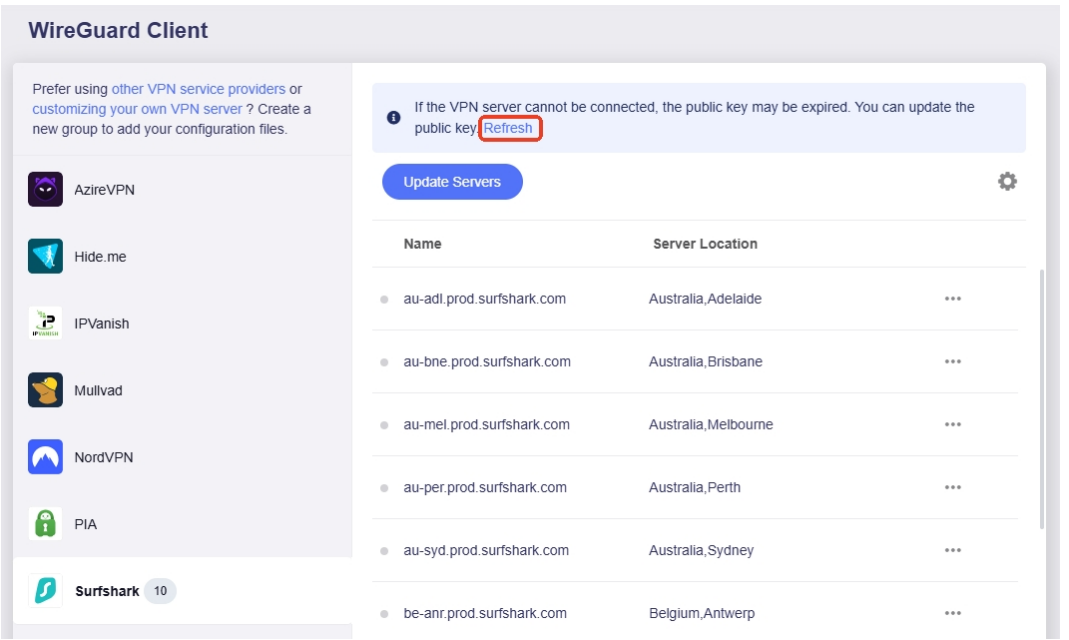
7. Modifiez les identifiants ou déconnectez-vous.

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



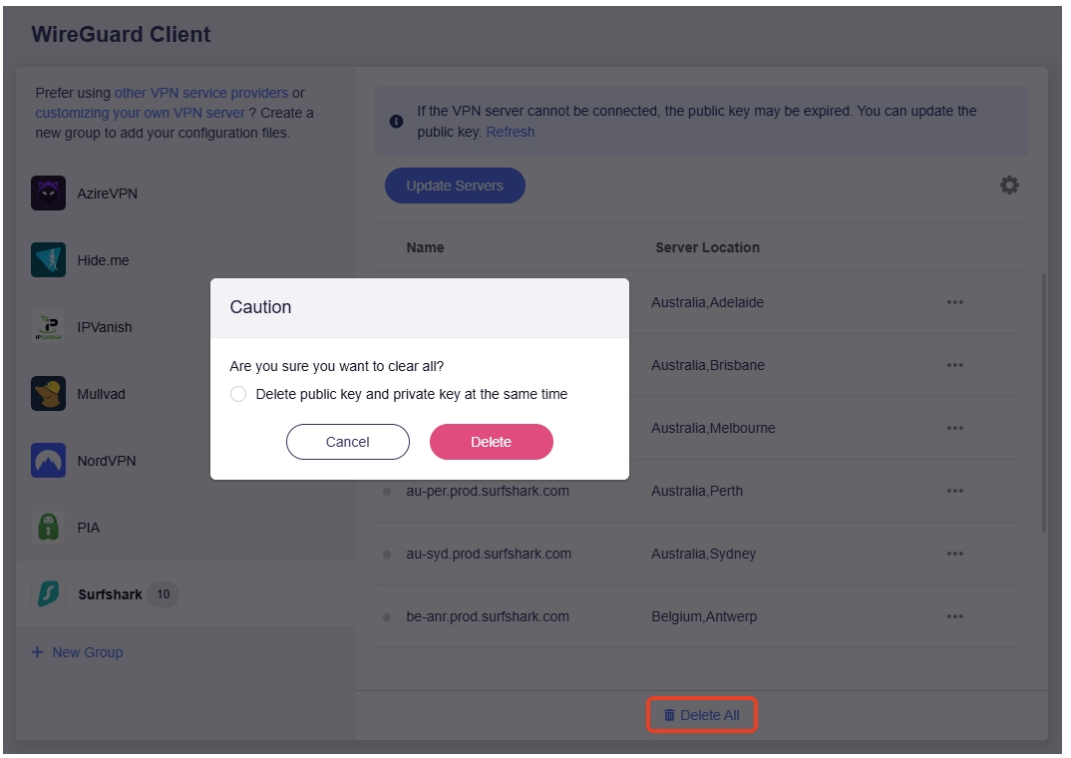
8. Actualisez les données.

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.

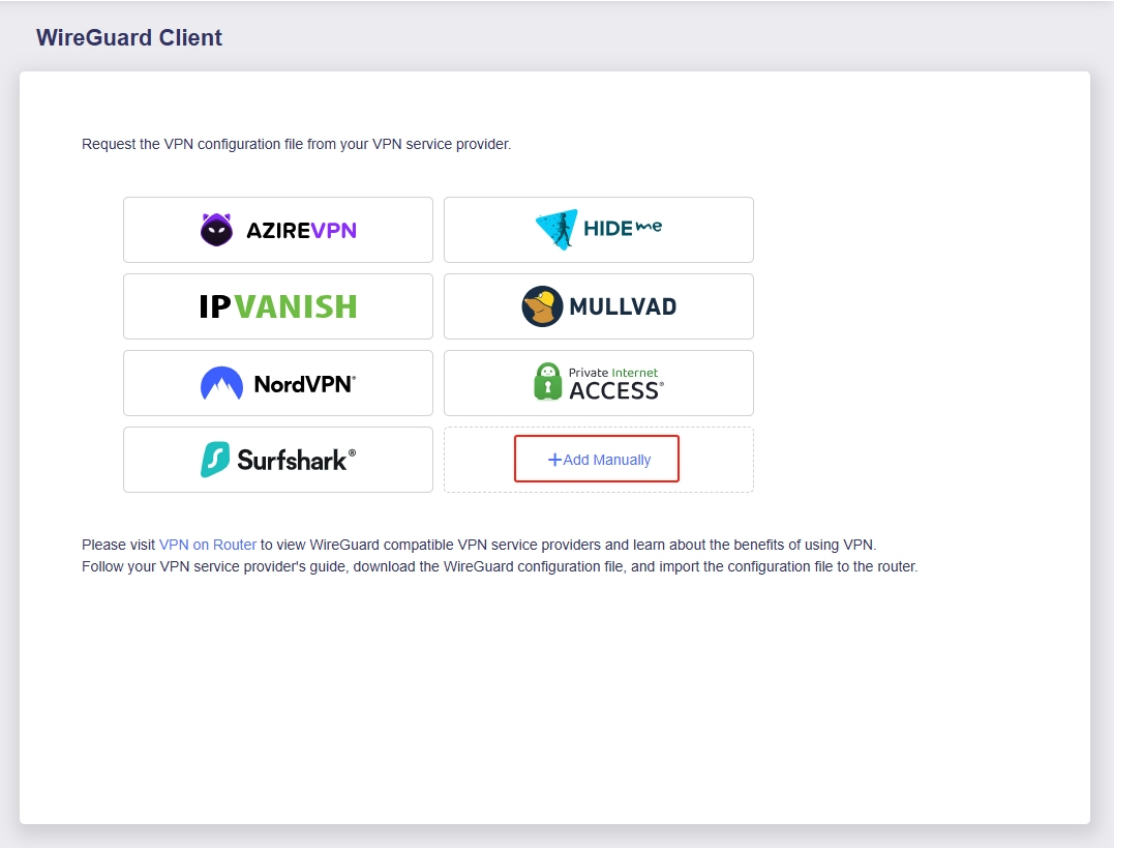


11.2.9 Configuration manuelle d’un client WireGuard pour un autre fournisseur

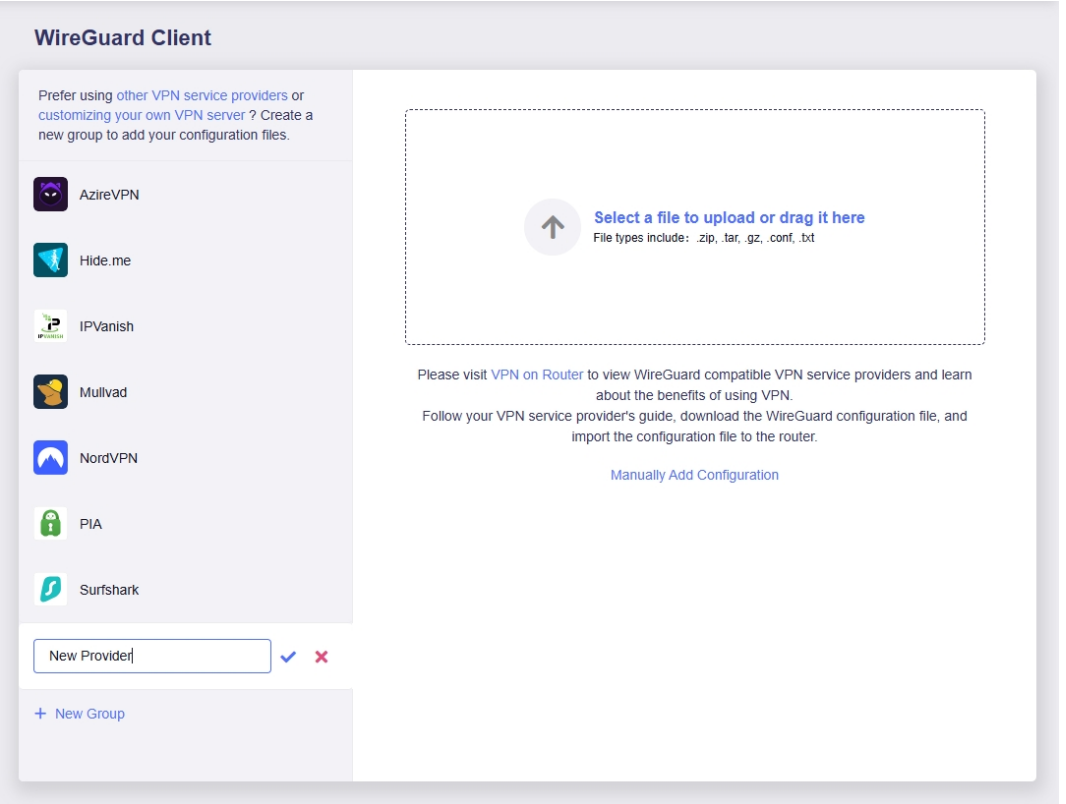
Si votre fournisseur WireGuard n’est pas intégré à l’interface Web, récupérez d’abord le fichier de configuration sur son site officiel, puis importez-le sur le routeur. Si vous ne savez pas comment télécharger les fichiers, consultez ce guide ou contactez l’assistance du fournisseur.

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

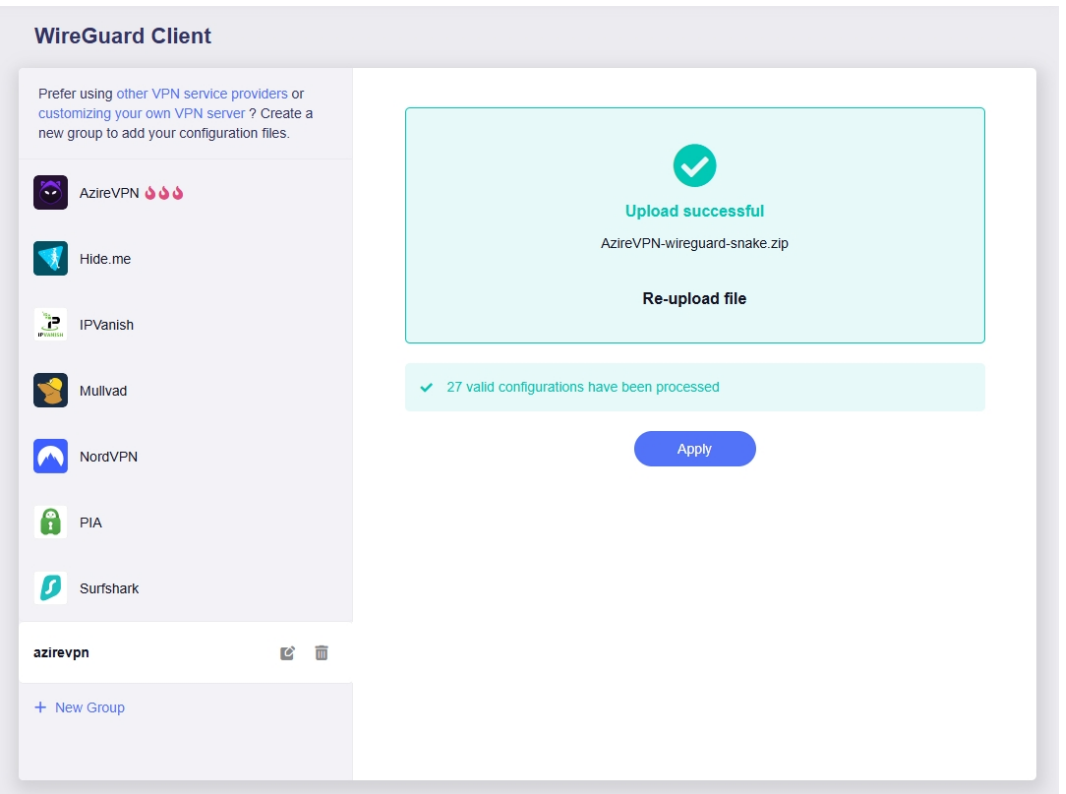
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Ajouter manuellement (Add Manually)**.



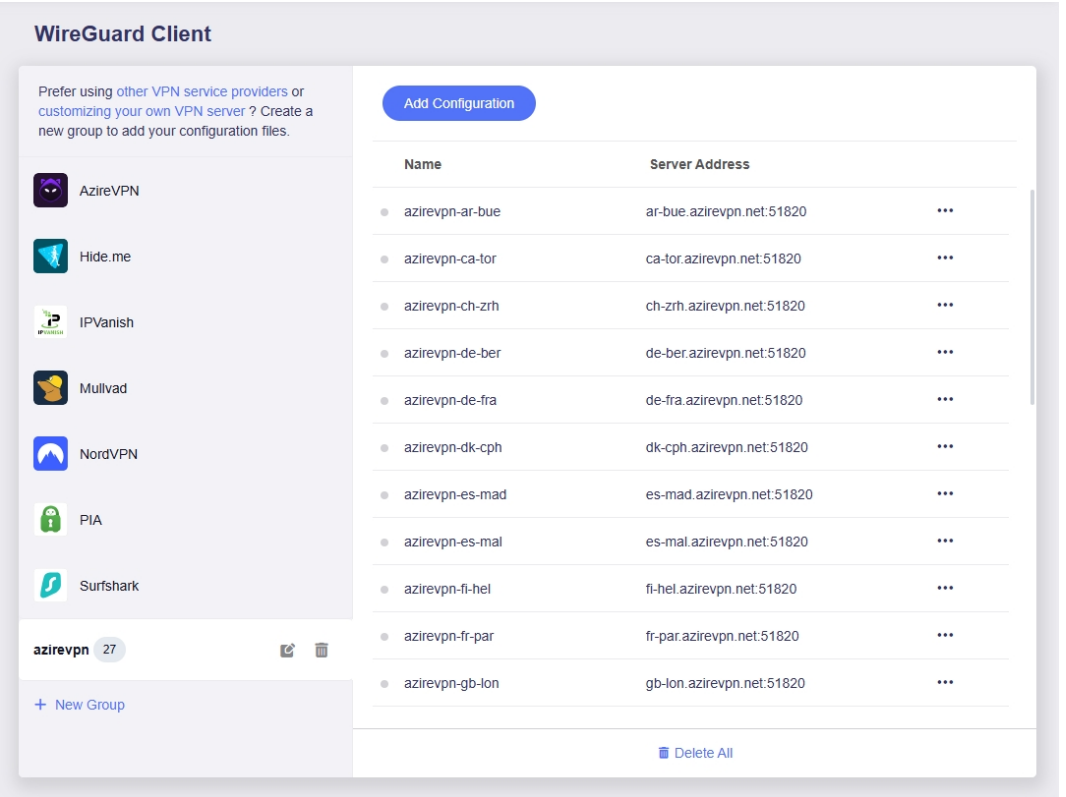
2. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



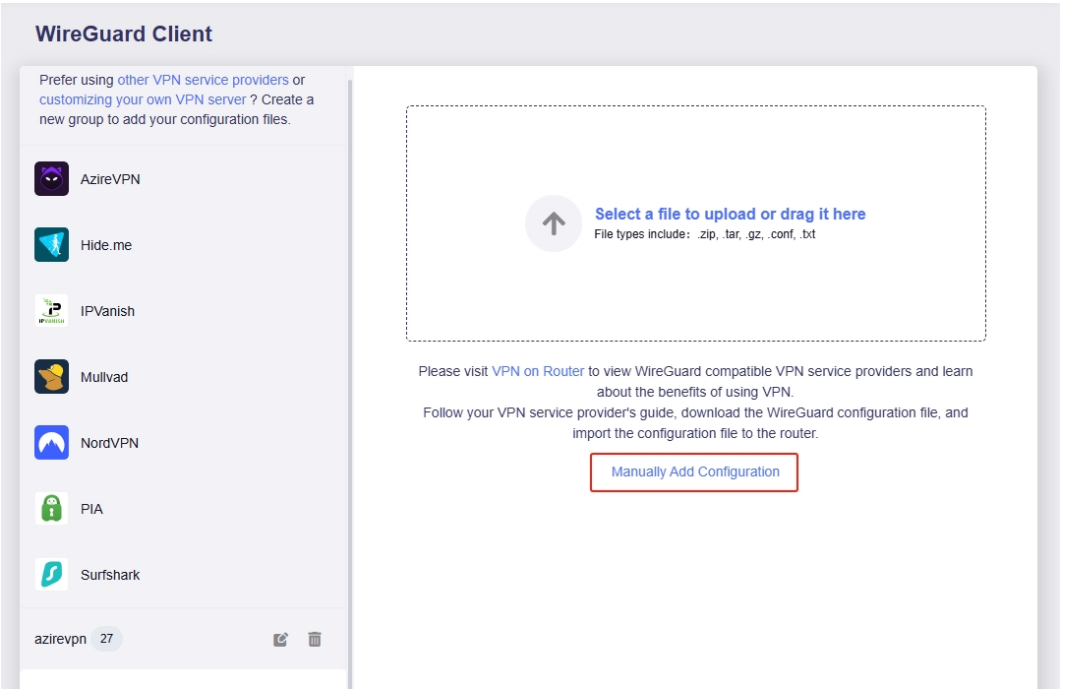
3. Cliquez sur la zone d'importation et sélectionnez votre fichier WireGuard. Les formats zip, tar, gz, conf et txt sont pris en charge. Cliquez sur **Appliquer (Apply)**.

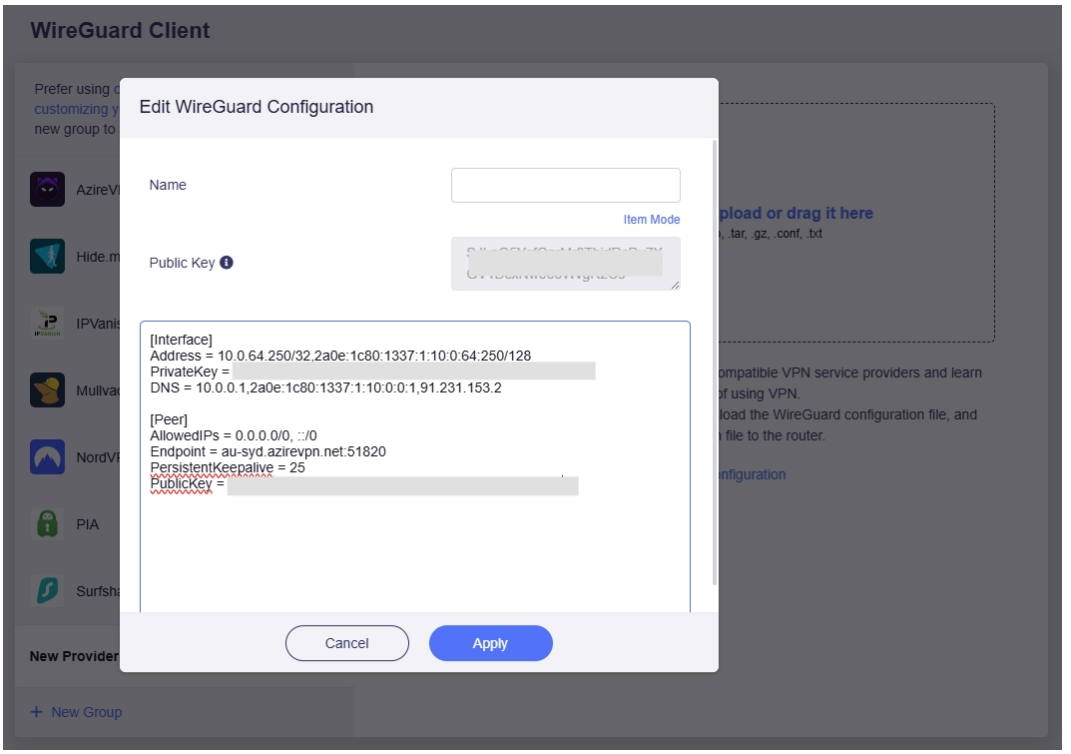


Si vous importez une archive contenant plusieurs fichiers de configuration, elle est décompressée automatiquement, comme ci-dessous.

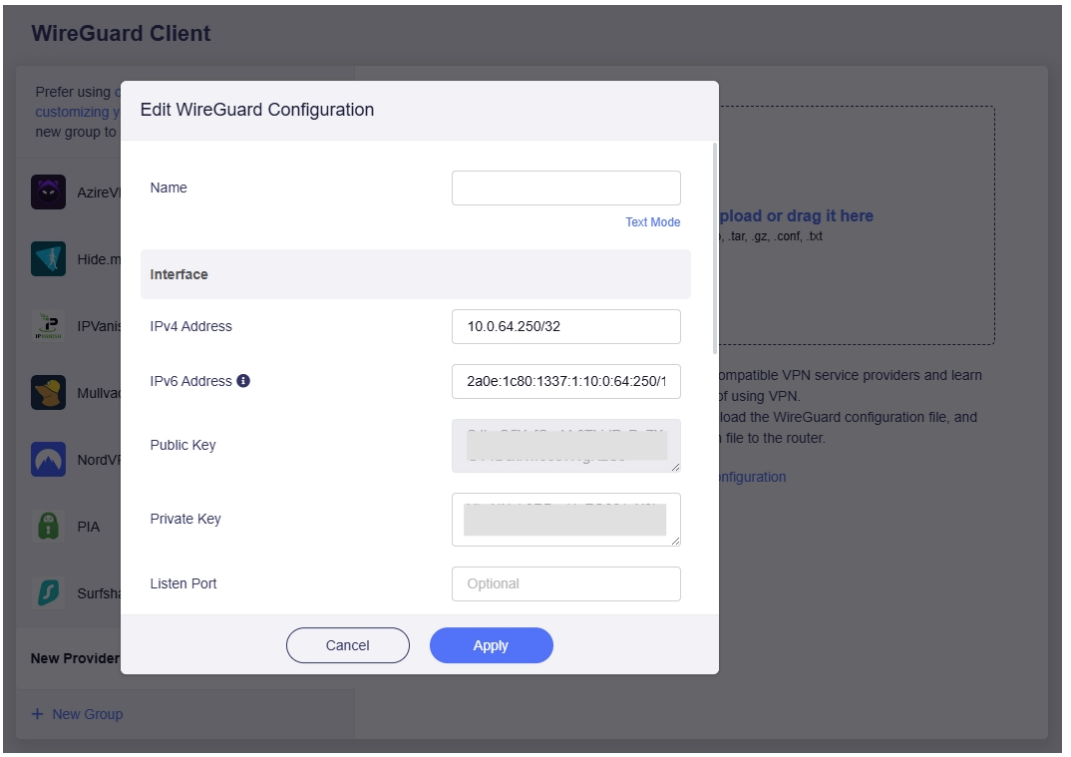


Vous pouvez aussi cliquer sur **Ajouter une configuration manuellement (Manually Add Configuration)** en bas de la zone d’importation, renseigner la configuration sous forme de texte, puis cliquer sur **Appliquer (Apply)**.

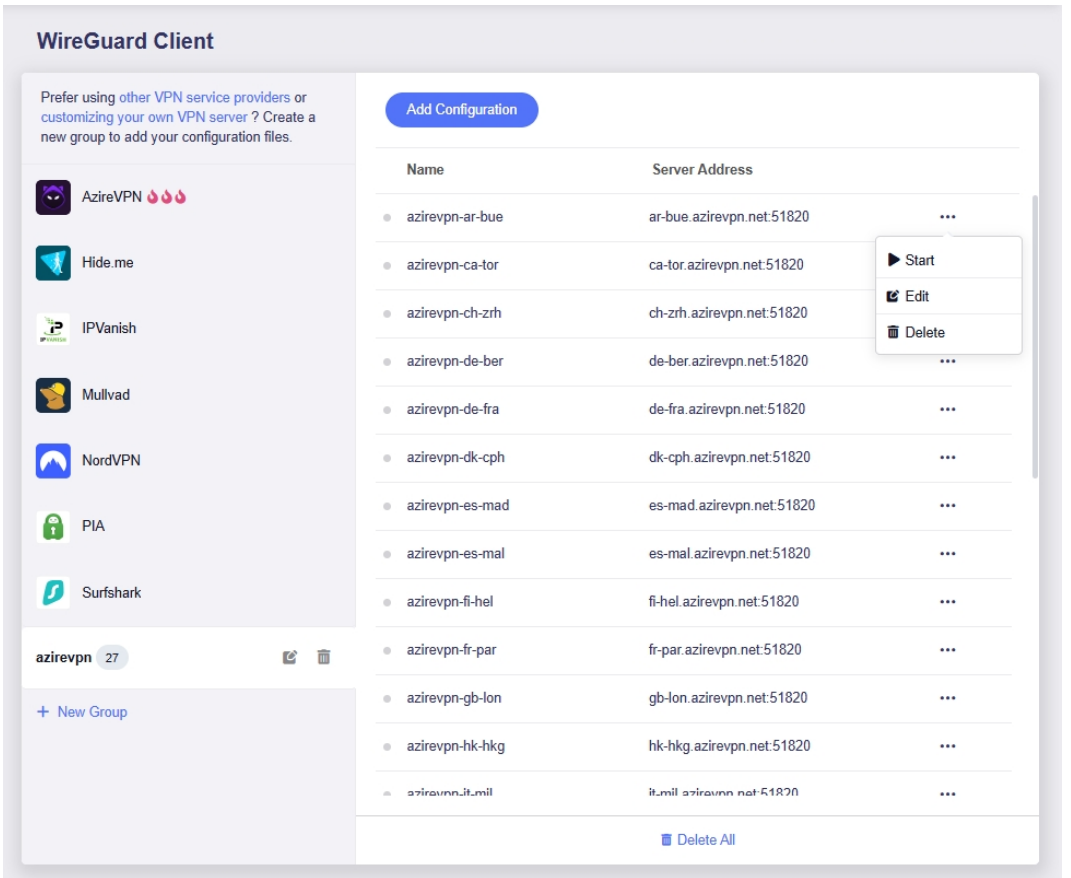




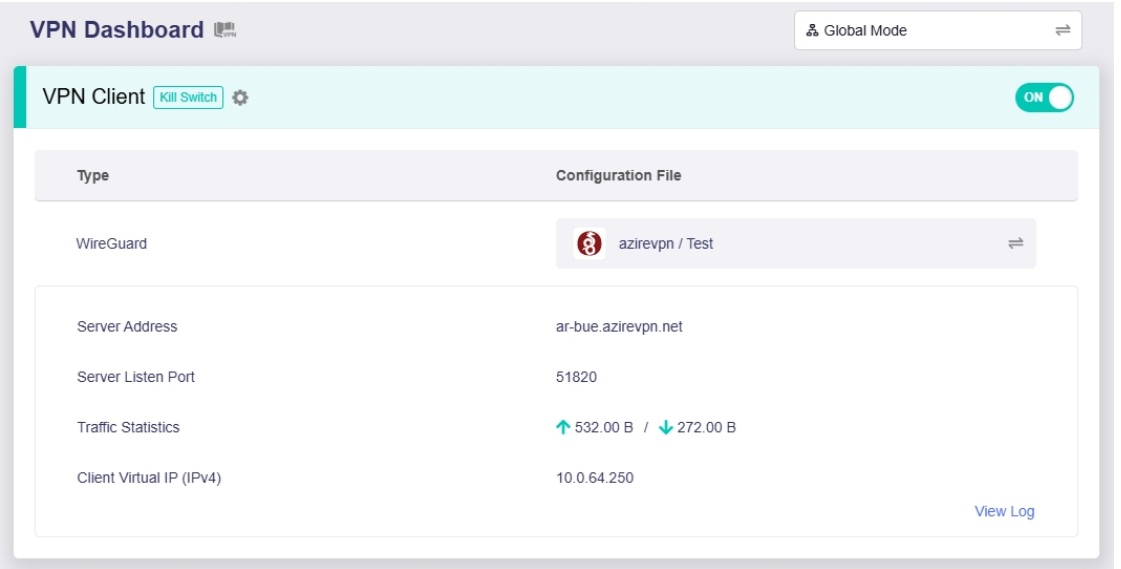
Pour vérifier chaque paramètre, passez en mode Élément (Item), contrôlez la configuration, puis cliquez sur **Appliquer (Apply)**.



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

Réseau

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

12.1 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.

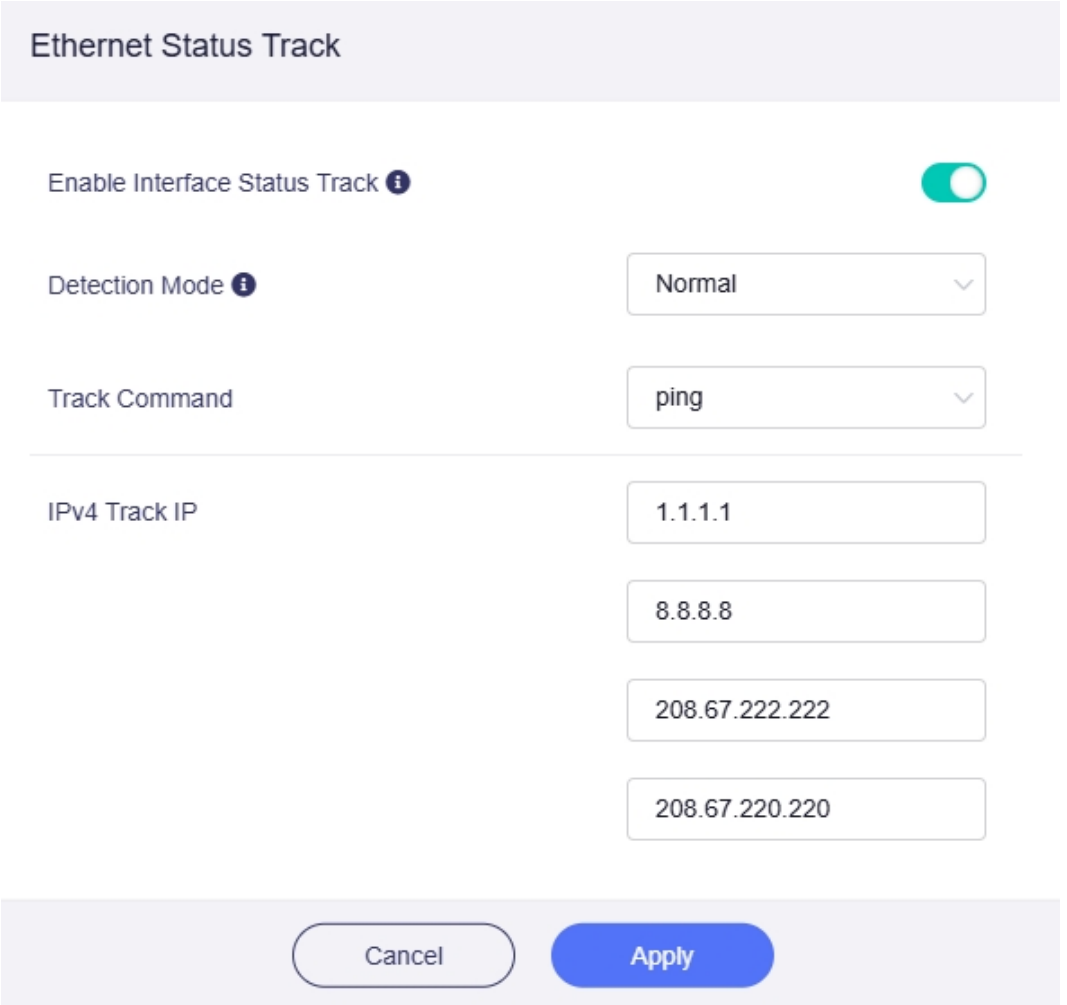
Connectez-vous au panneau d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Multi-WAN**. Cette page comporte deux sections : **Suivi de l'état des interfaces (Interface Status Track)** et **Mode Multi-WAN (Multi-WAN Mode)**.

12.1.1 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.



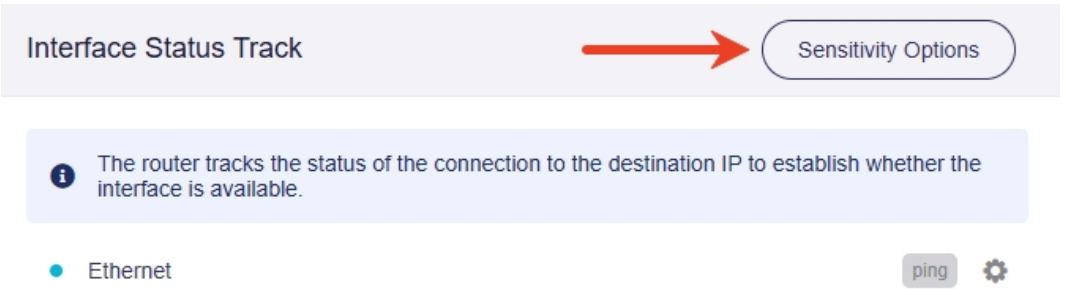
Dans la section **Suivi de l'état des interfaces (Interface Status Track)**, cliquez sur l'engrenage à droite pour régler le suivi de chaque interface. Les paramètres Ethernet sont présentés ci-dessous. La même logique s'applique aux autres interfaces.



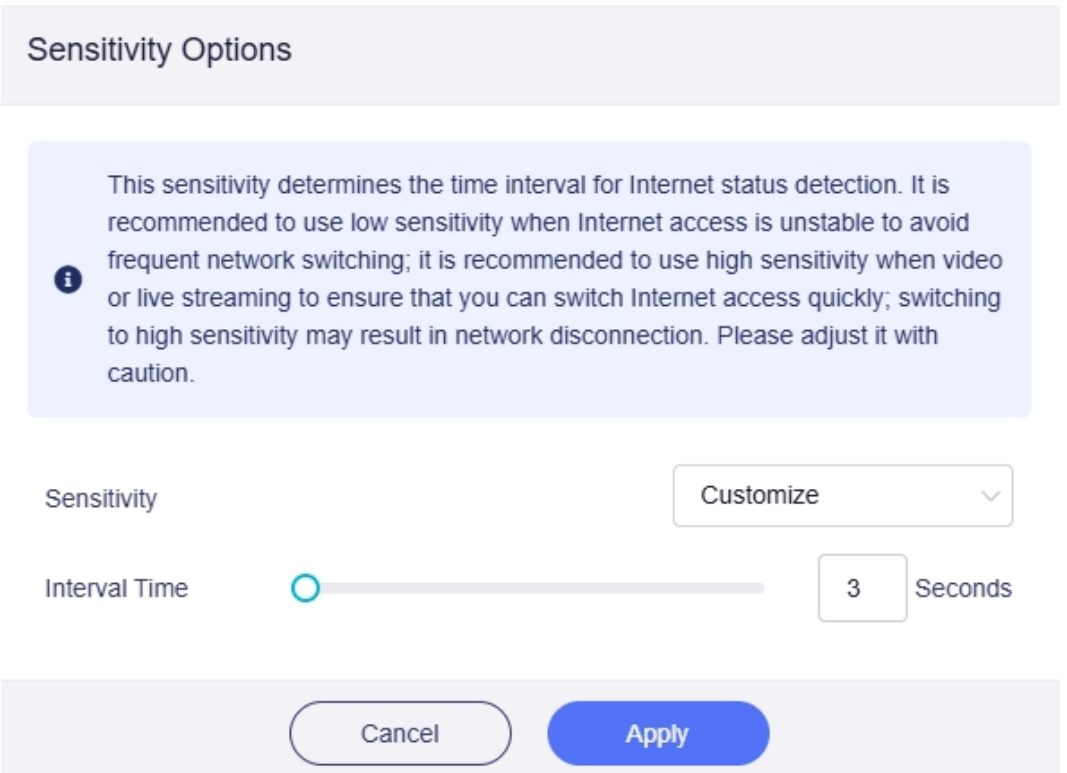
- **Activer le suivi de l'état de l'interface (Enable Interface Status Track)** : activé par défaut. Si vous le désactivez, le routeur détermine l'état de l'interface selon les conditions physiques, par exemple le branchement du câble Ethernet.
- **Mode de détection (Detection Mode)** : introduite sous 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.



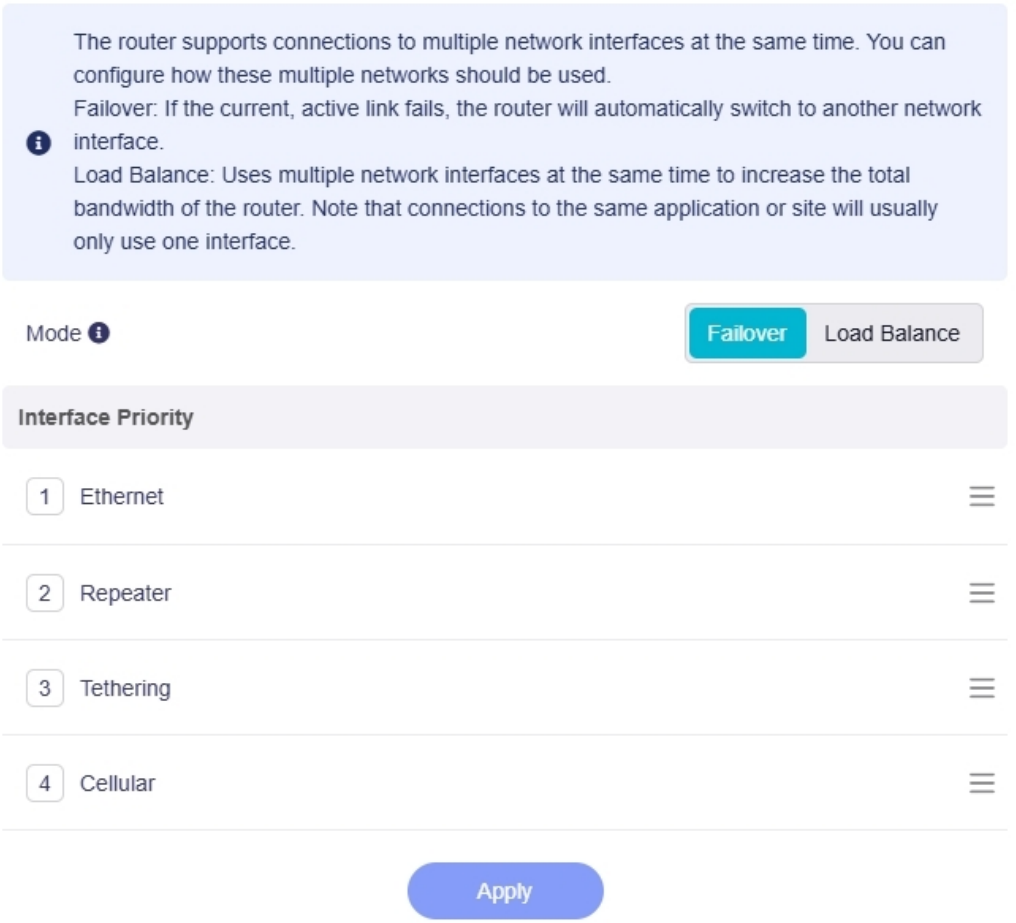
12.1.2 Mode Multi-WAN

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.

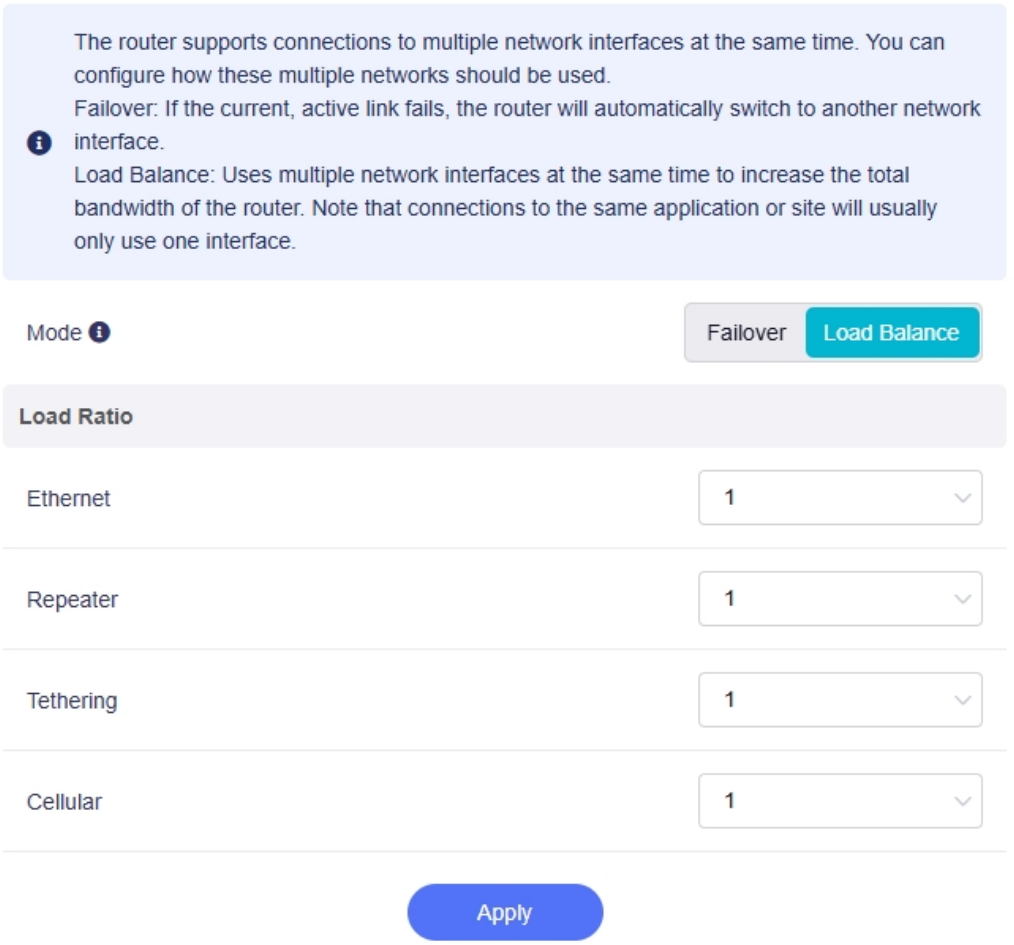


Équilibrage de charge

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.

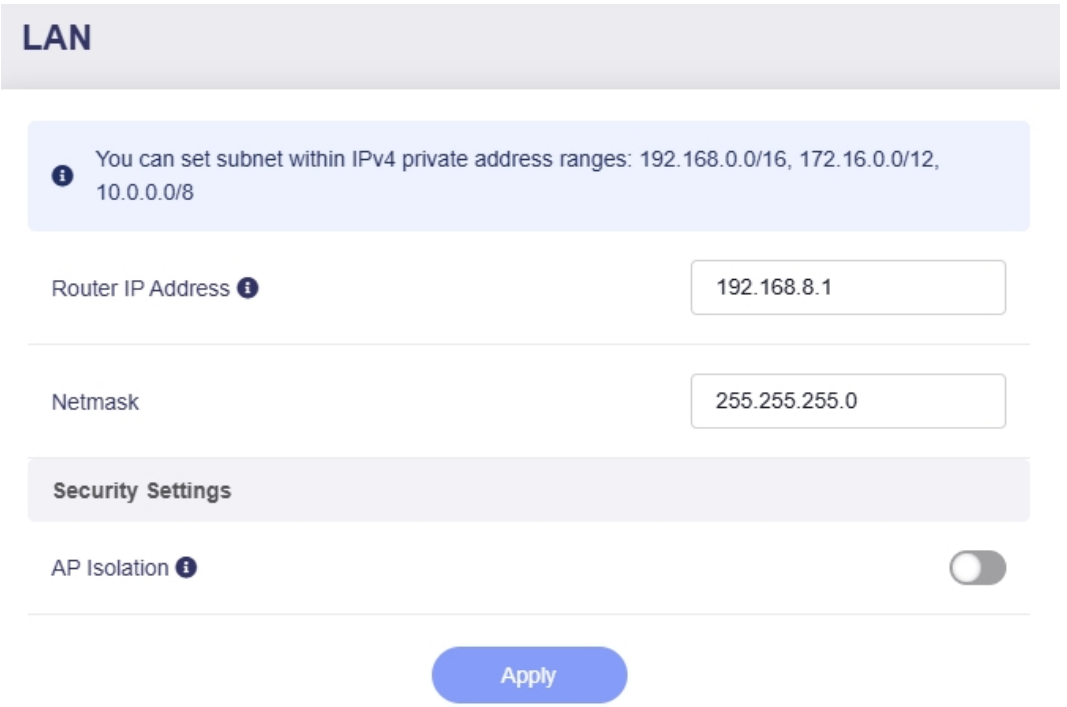
12.2 LAN

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.

12.2.1 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.

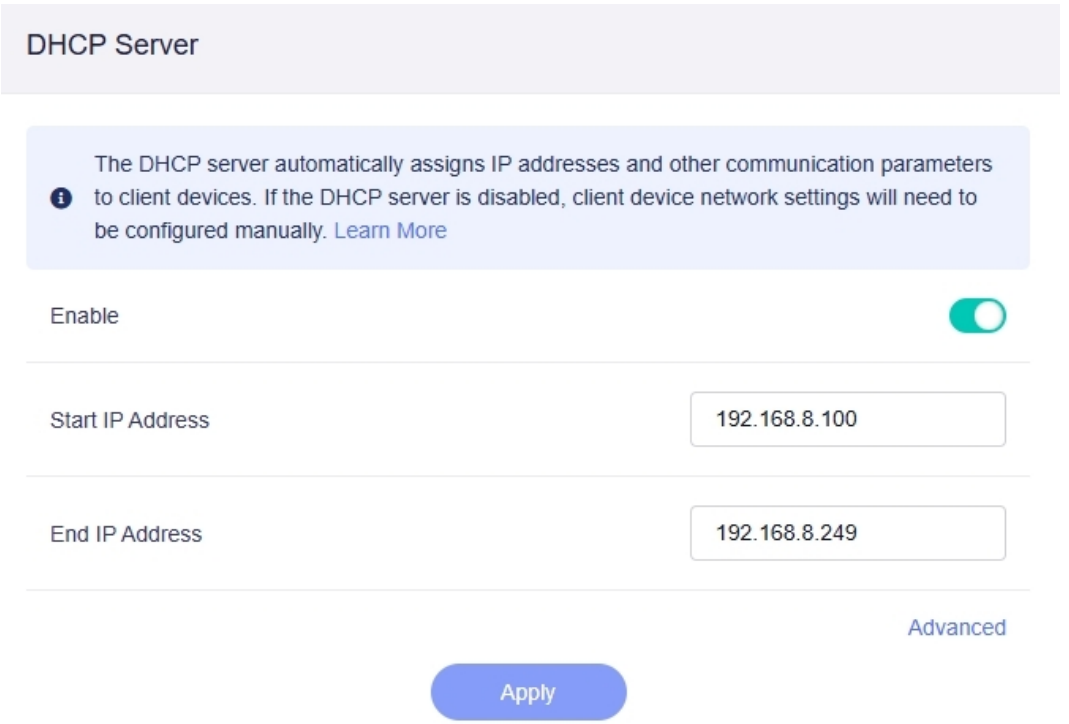


- **Adresse IP du routeur (Router IP Address)** : adresse à saisir dans le navigateur pour ouvrir l'interface d'administration. Par défaut, elle est 192.168.8.1. Modifiez-la si elle entre en conflit avec le réseau en amont.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.

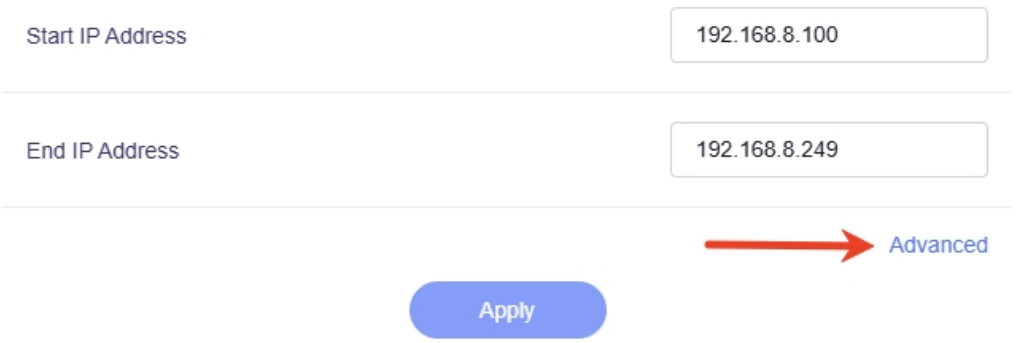
- **Isolation des clients Wi-Fi (AP Isolation)** : isole les appareils clients dans une zone réseau distincte. Ces appareils ne peuvent pas communiquer avec les autres appareils du réseau.

12.2.2 Serveur DHCP

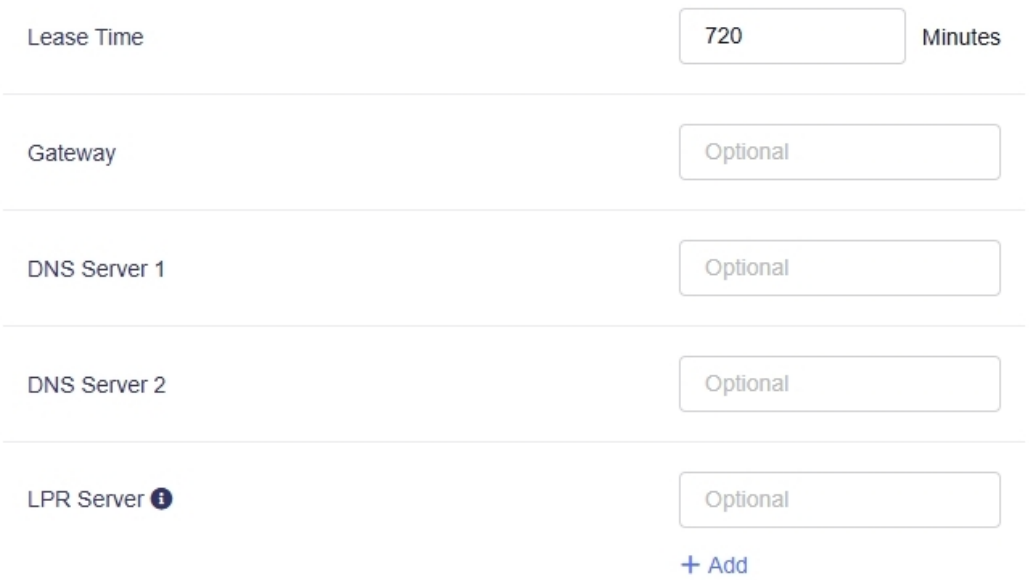
Le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Il est activé par défaut sur le routeur GL.iNet, avec une plage d'adresses de 192.168.8.100 à 192.168.8.249. Vous pouvez personnaliser cette plage.



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.

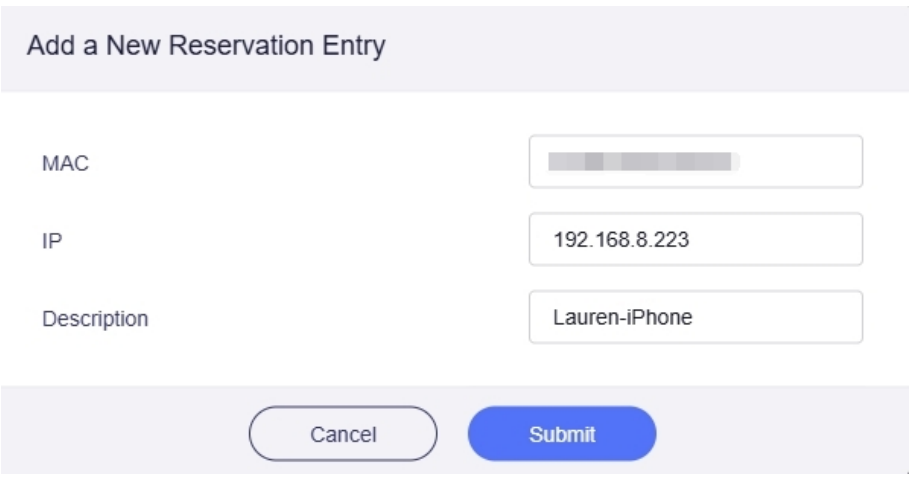
Remarque : si vous désactivez le serveur DHCP, définissez manuellement une IP statique et les autres paramètres de communication sur chaque client. Consultez cette page pour en savoir plus.

12.2.3 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.



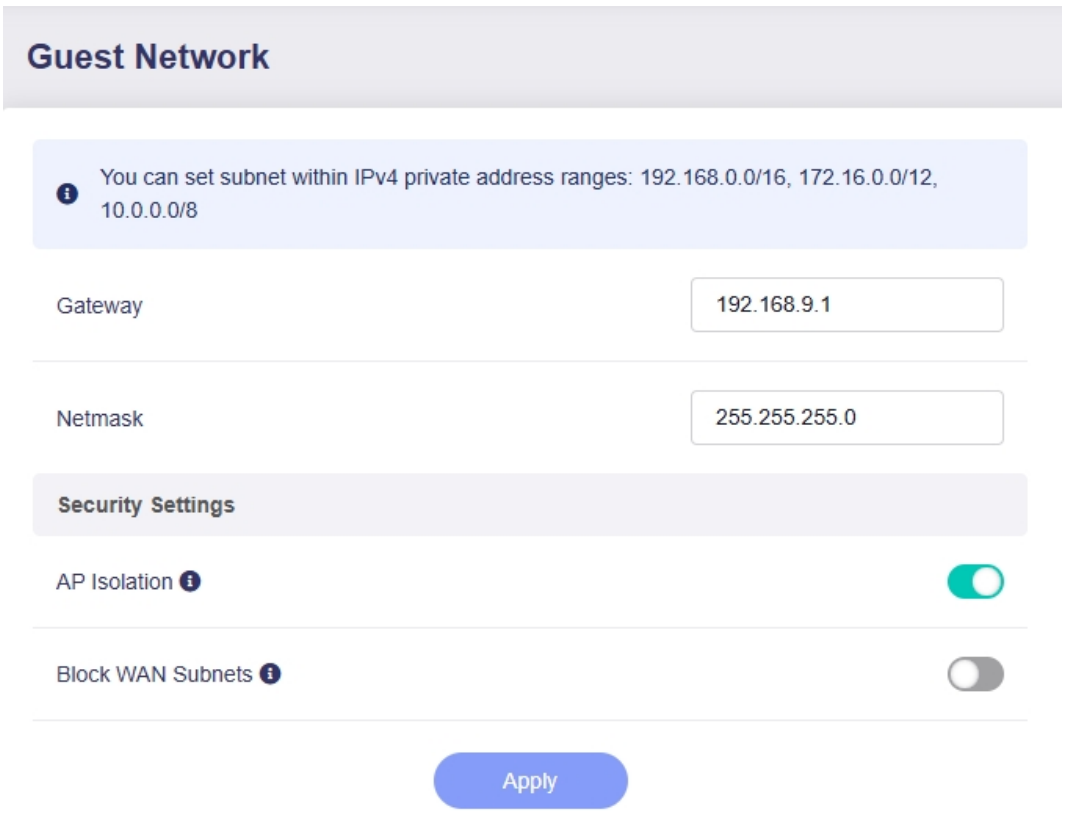
12.3 Réseau invité

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.

12.3.1 Paramètres de base

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



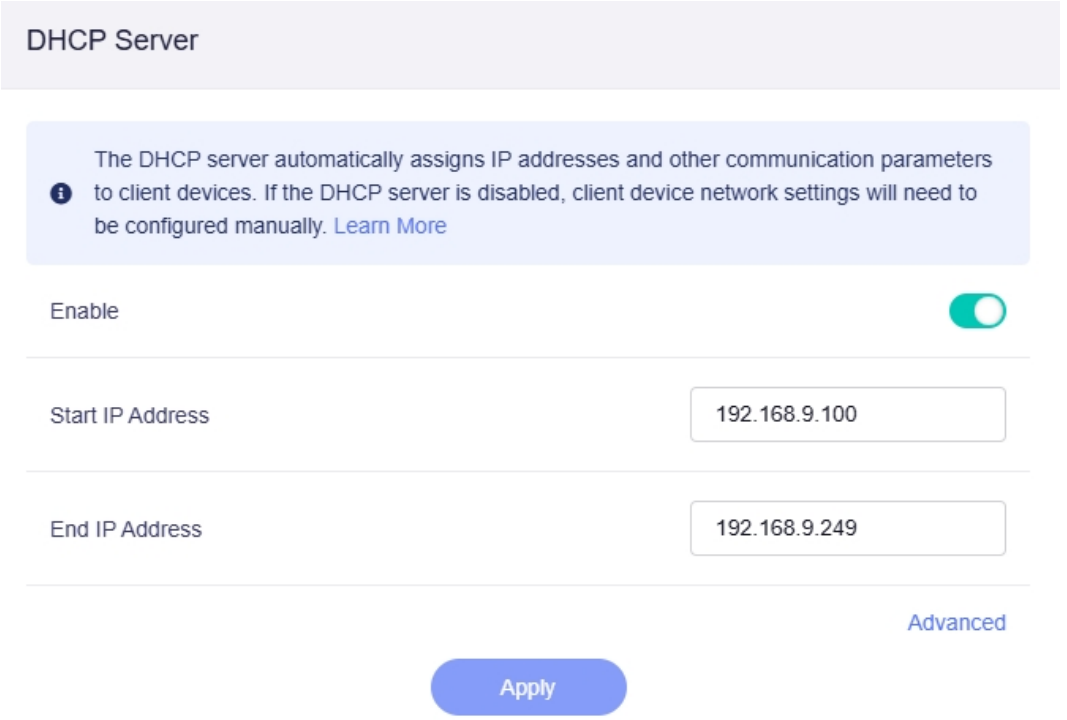
- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.9.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.

- **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.

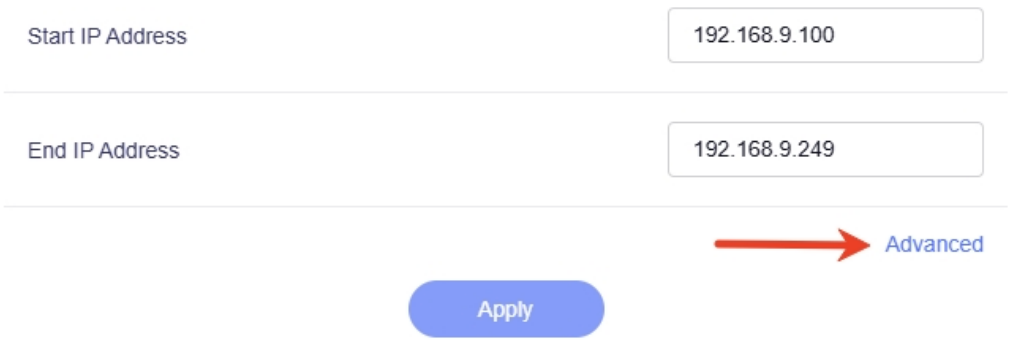
12.3.2 Serveur DHCP

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

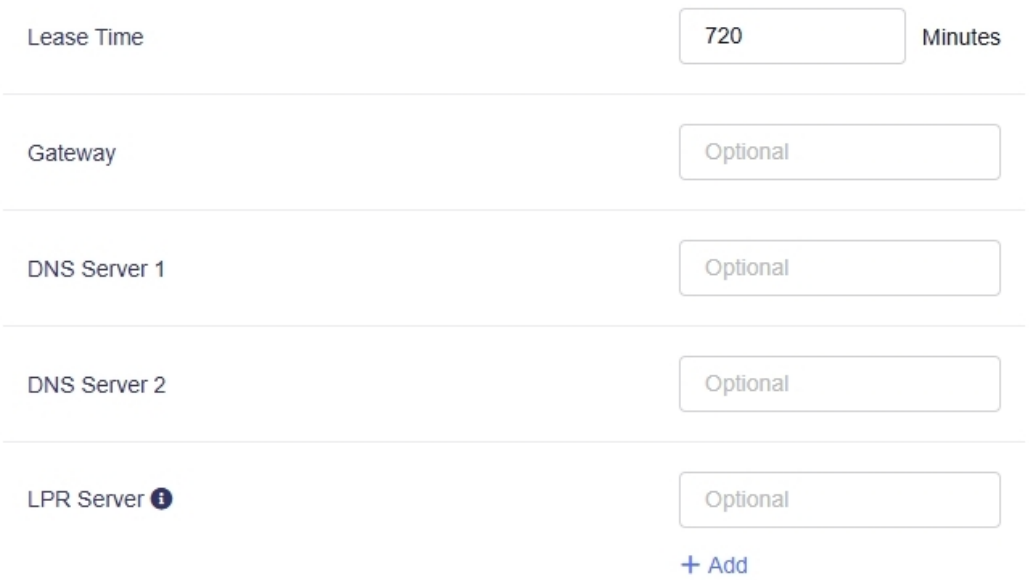
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client. Sa plage d'adresses s'étend de 192.168.9.100 à 192.168.9.249. Vous pouvez la personnaliser.



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.

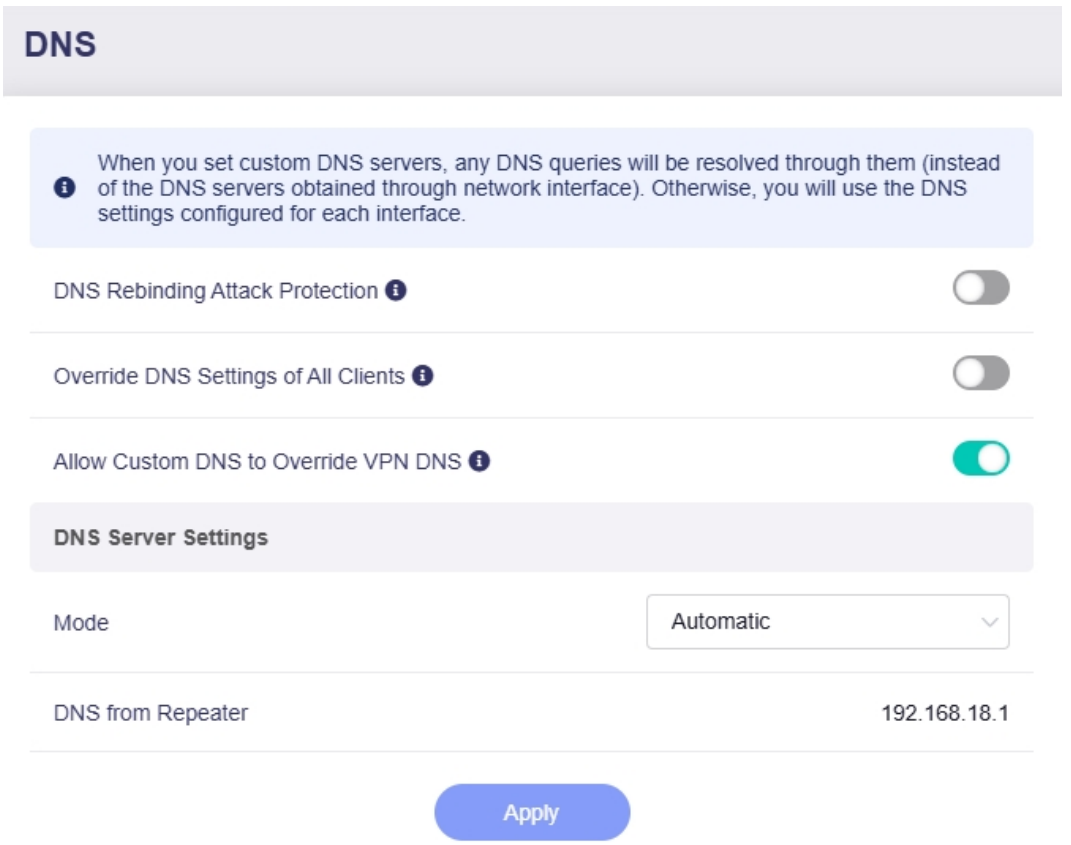
12.4 DNS

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.

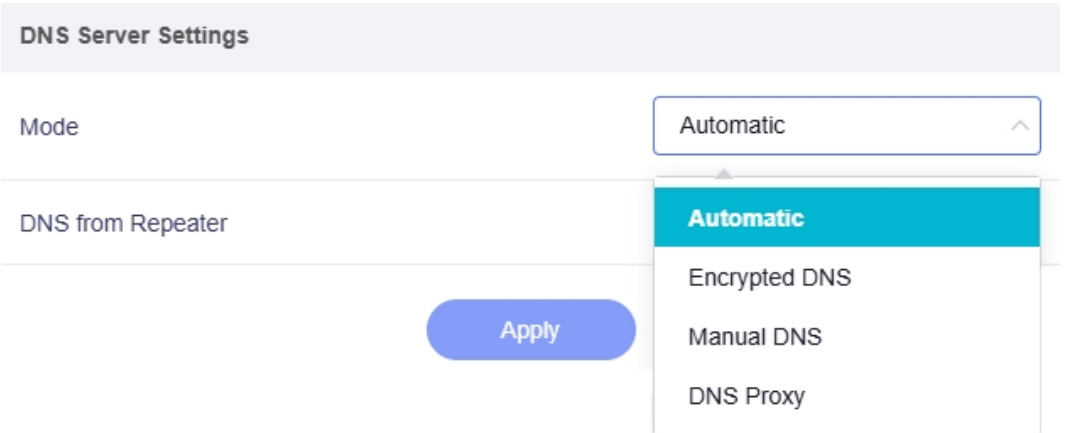
12.4.1 Paramètres généraux



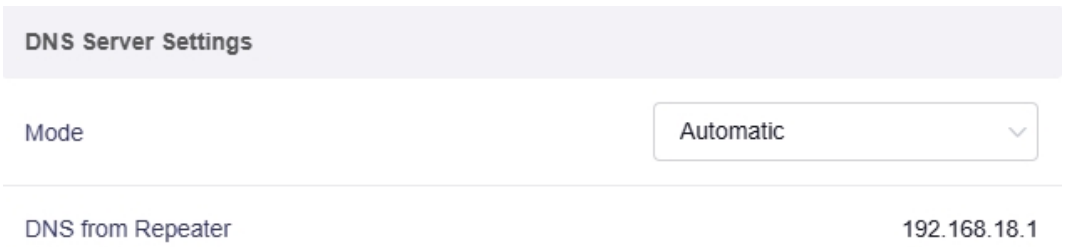
- **Protection contre le rebinding DNS (DNS Rebinding Attack Protection)** : bloque les tentatives malveillantes de résolution DNS. Elle peut toutefois empêcher certaines résolutions DNS privées. Désactivez-la si votre réseau utilise un portail captif, comme une page de connexion Wi-Fi publique.
- **Remplacer 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.

12.4.2 Paramètres du serveur DNS

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

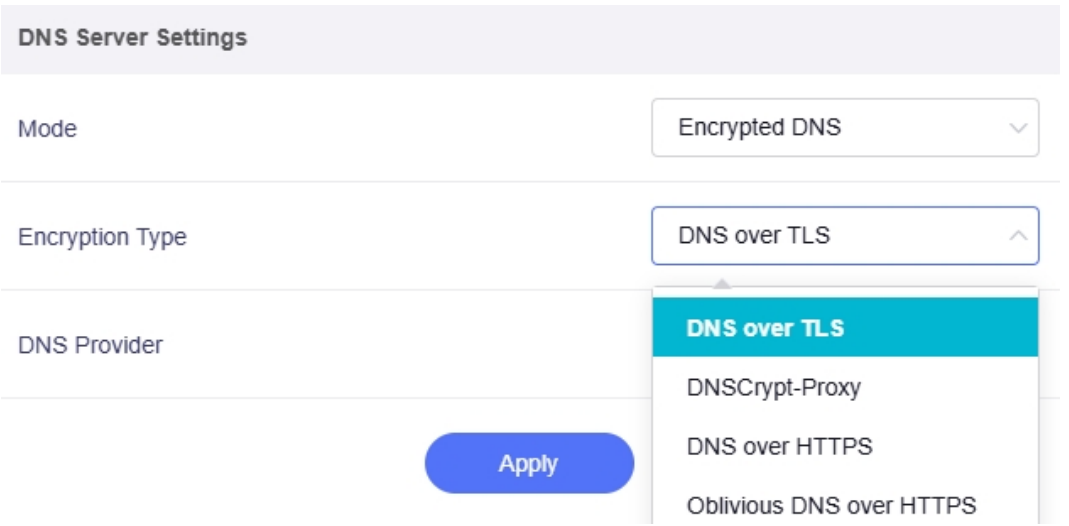


1. **Automatique (Automatic)** : le routeur obtient les adresses des serveurs DNS du réseau en amont et les applique à tous les appareils connectés.



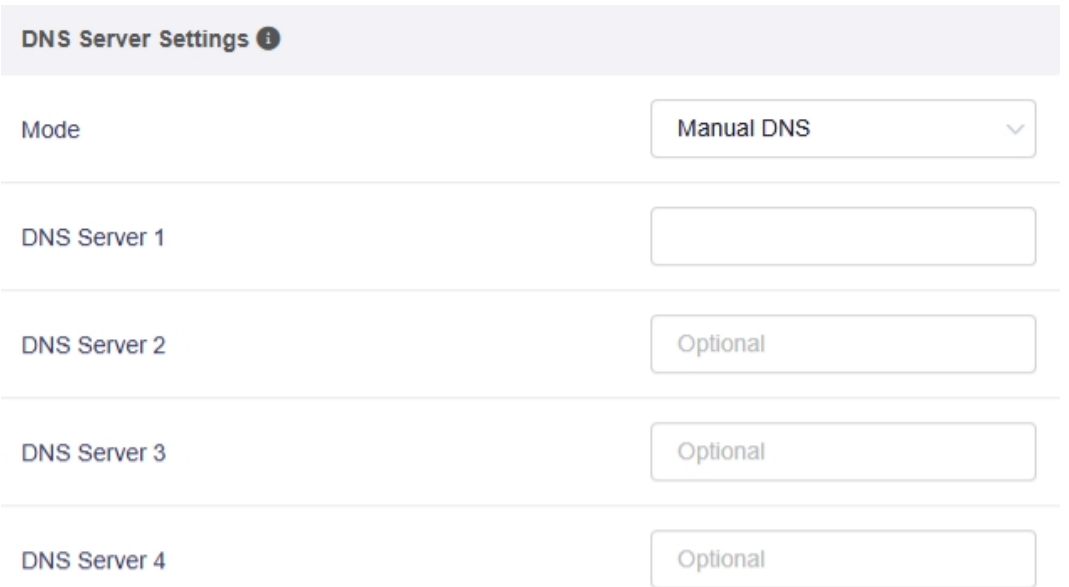
2. **DNS chiffré (Encrypted DNS)** : utilise des protocoles chiffrés pour traiter les requêtes DNS et protéger les données de résolution contre l'écoute et l'altération.

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



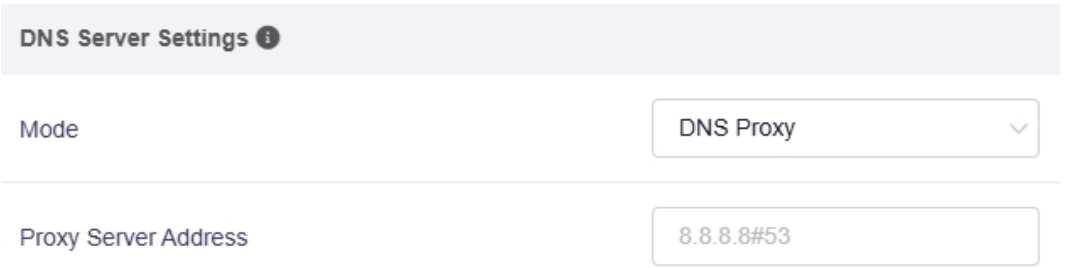
- Pour DNS over TLS, choisissez Control D, NextDNS ou Cloudflare comme fournisseur DNS.
- Pour les trois autres types, sélectionnez au moins un serveur DNS dans la liste, et jusqu'à huit serveurs. Si vous en sélectionnez plusieurs, le routeur utilise automatiquement le plus rapide.

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.

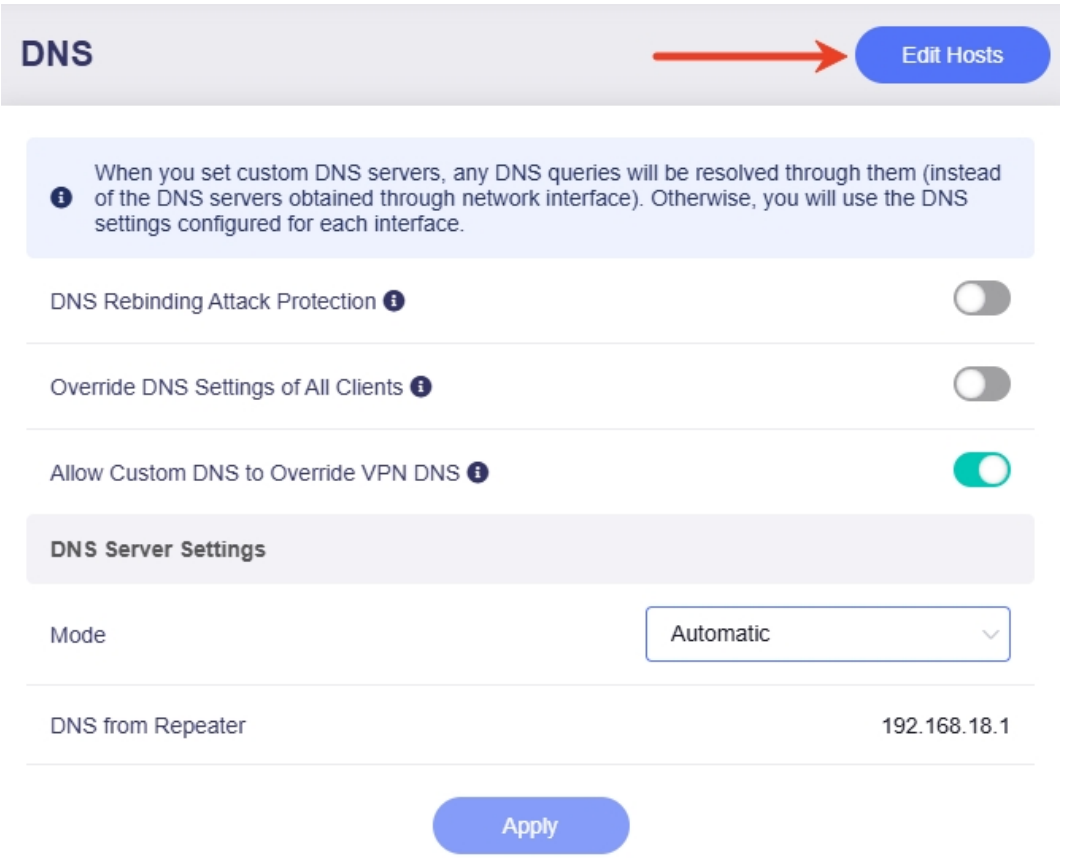
4. **Proxy DNS (DNS Proxy)** : transmet toutes les requêtes DNS par un serveur proxy et utilise son environnement réseau pour la résolution, selon vos besoins d'accès.



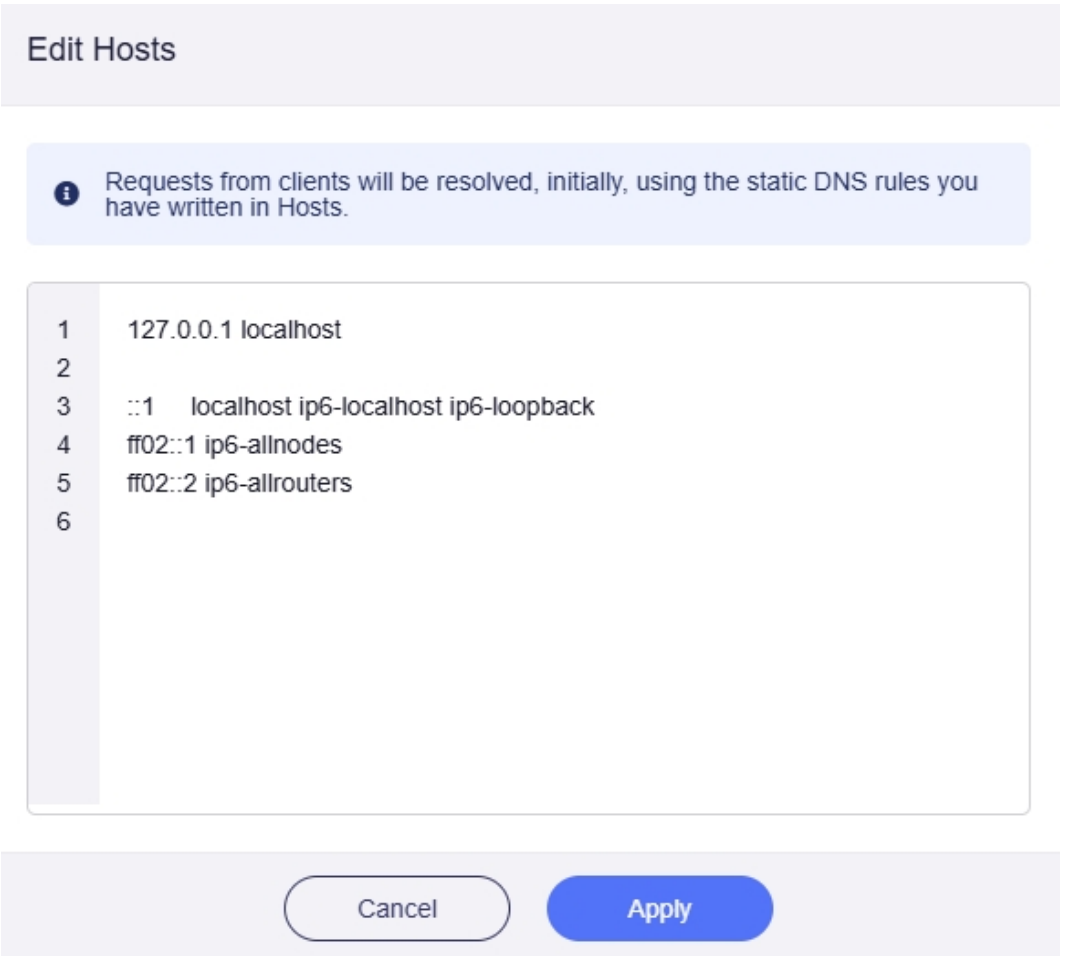
12.4.3 Modification du fichier hosts

Vous pouvez définir des règles statiques de résolution DNS.

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



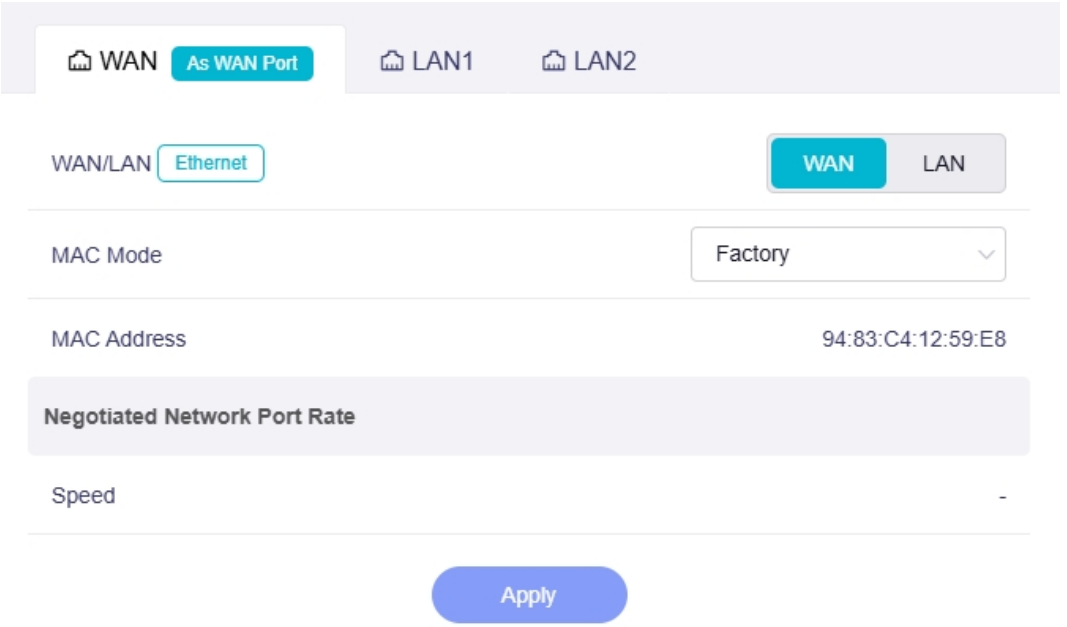
Les requêtes des clients sont résolues en priorité avec les règles statiques saisies ici. Vous pouvez associer manuellement des adresses IP à des noms d’hôtes, comme l’entrée de bouclage locale 127.0.0.1 localhost, pour personnaliser la résolution des noms.



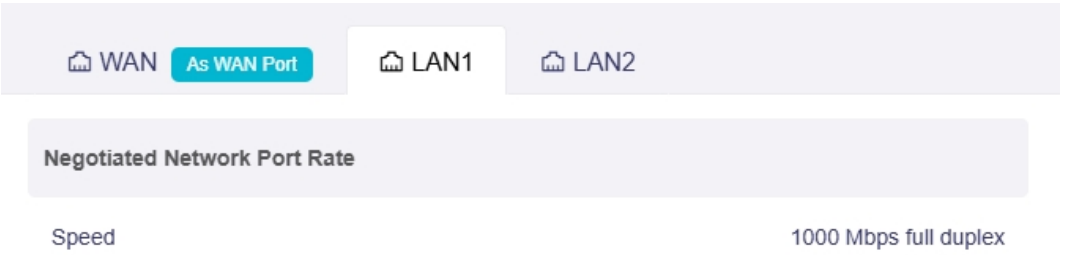
12.5 Ports Ethernet

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.



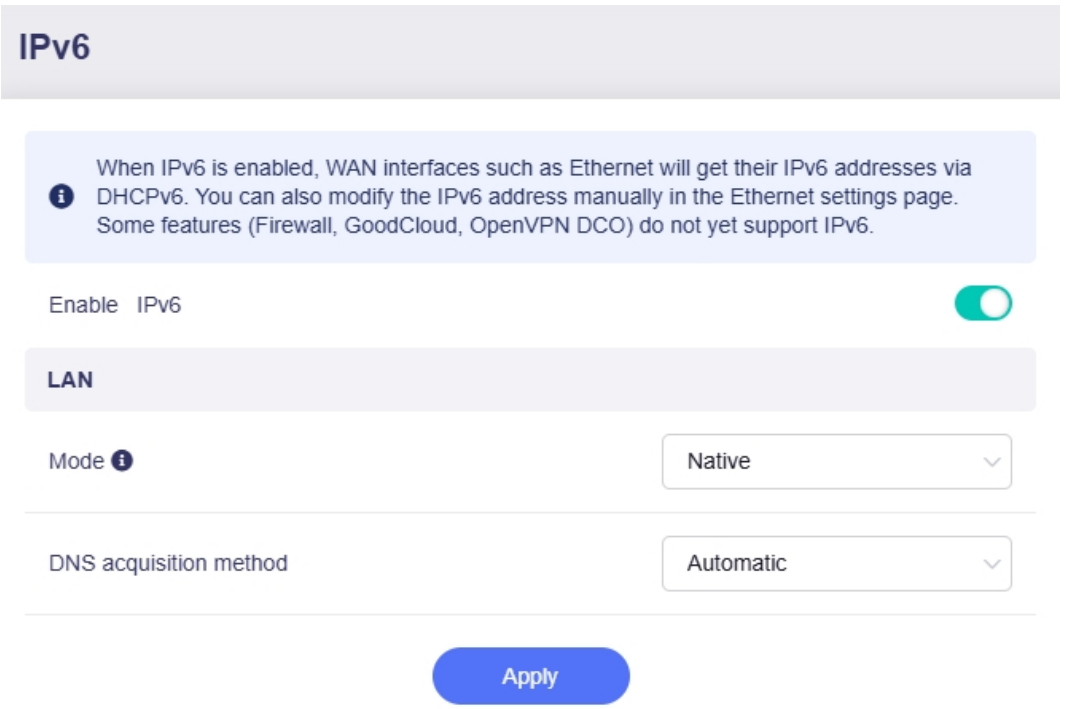
Remarque : le débit négocié des ports WAN et LAN ne s'affiche que lorsqu'un câble Ethernet est branché. Il dépend des capacités du port et du câble Ethernet.

12.6 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.

12.6.1 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.

12.6.2 Méthode d'obtention du DNS

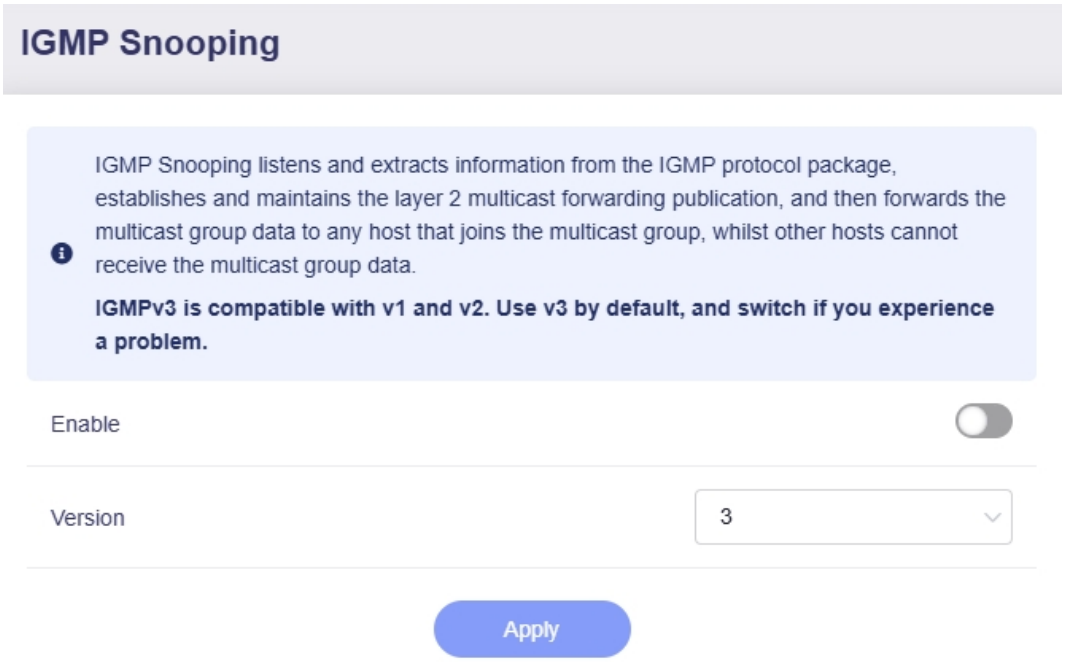
Ce paramètre détermine comment le routeur obtient les adresses des serveurs DNS IPv6. Deux options sont disponibles : Automatique et Manuelle.

- **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.

12.7 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.

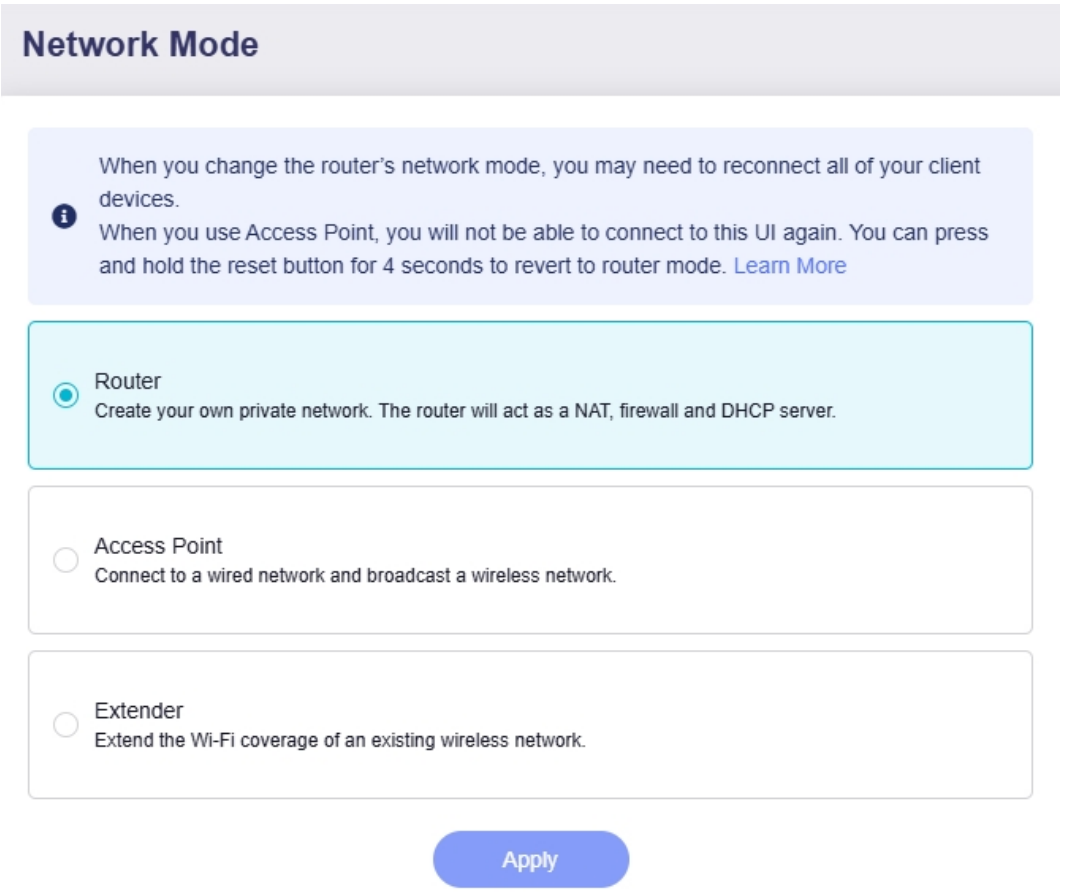
Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **IGMP Snooping**. Activez cette fonction si vous souhaitez utiliser le multicast sur le routeur.



12.8 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.

Remarque :

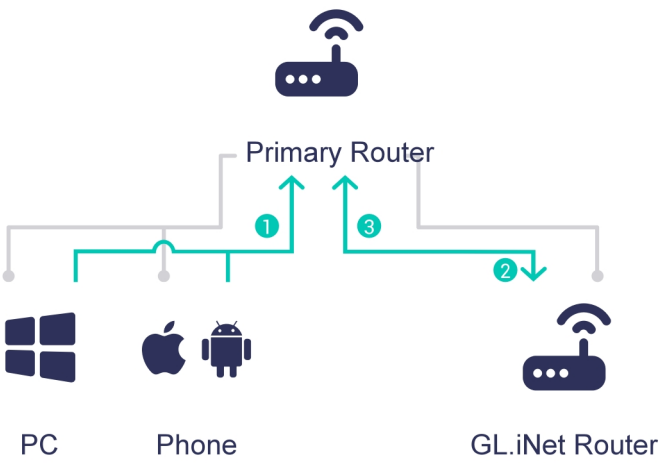
1. Après un changement de mode réseau, tous les appareils clients doivent se reconnecter au routeur pour assurer une connexion stable.
2. **En mode Point d'accès, l'adresse IP d'origine ne permet plus d'accéder à l'interface d'administration Web**. Connectez-vous au routeur en amont pour trouver l'adresse IP qu'il a attribuée à ce routeur, puis utilisez-la pour ouvrir l'interface. Si vous n'avez pas accès au routeur en amont, maintenez le bouton de réinitialisation enfoncé pendant 4 secondes pour revenir au mode Routeur par défaut.
3. **En mode Point d'accès ou Extension, les fonctions suivantes sont indisponibles** : contrôle d'accès (liste d'autorisation et liste 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.

12.9 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.



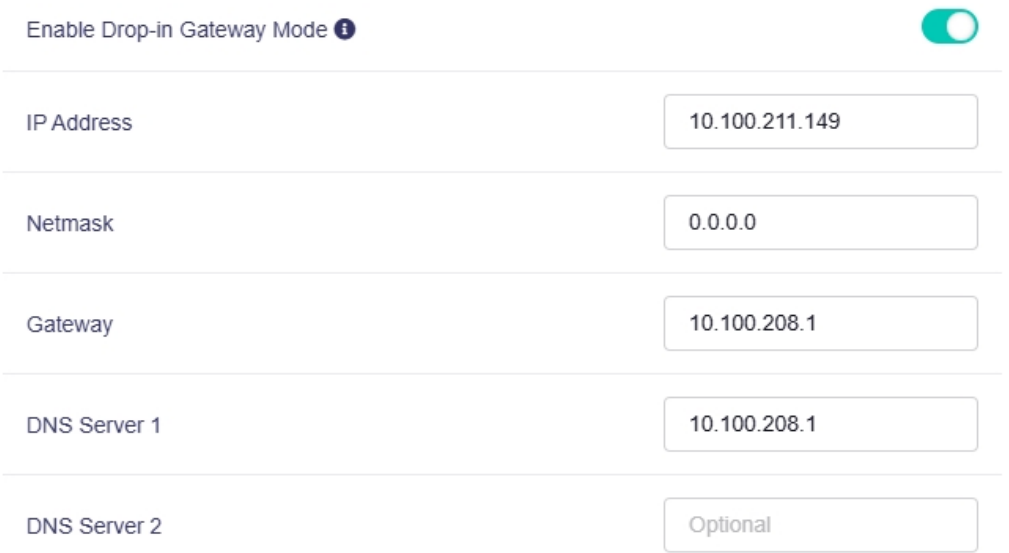
Le schéma ci-dessus comporte des lignes grises et des lignes vertes munies de trois flèches numérotées.

- **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 :

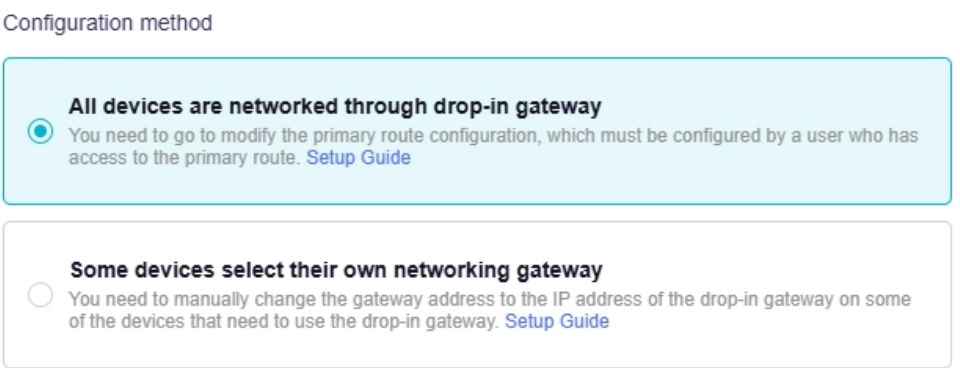
1. Le trafic des appareils clients est d'abord transmis au routeur principal.
2. Le routeur principal l'envoie au routeur GL.iNet pour traitement, par exemple le filtrage publicitaire ou le chiffrement VPN.
3. Après traitement, le trafic retourne au routeur principal, qui remet les données aux clients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



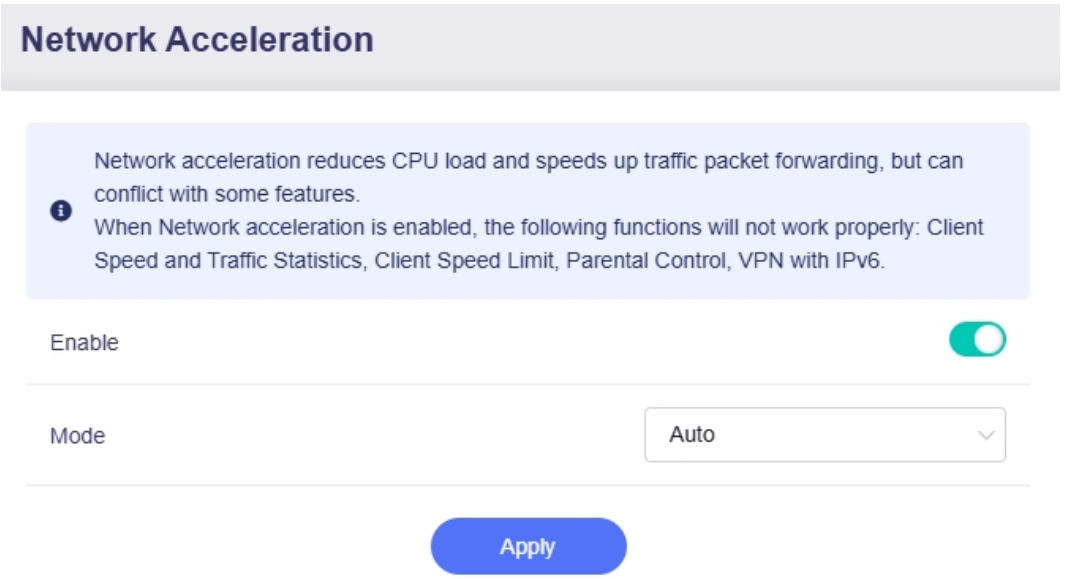
2. Choisissez la méthode de configuration, puis cliquez sur **Appliquer (Apply)**. Consultez ce tutoriel pour en savoir plus.



12.10 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.

Chapitre 13

Sécurité

Ce chapitre présente la gestion de la sécurité réseau, notamment la redirection de ports, les paramètres d’accès administrateur et le mode NAT.

13.1 Redirection de port

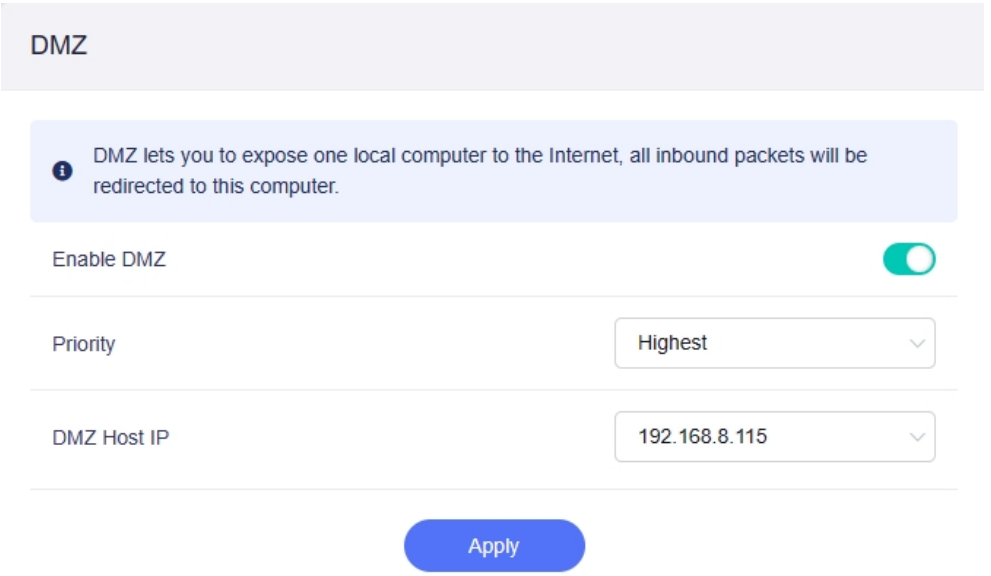
La redirection de port achemine les requêtes externes vers des appareils précis du réseau local. Cette page propose deux fonctions : **DMZ**, pour un accès direct complet à un appareil, et **Redirection de port (Port Forwarding)**, pour un accès ciblé à certains ports.

13.1.1 DMZ

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

Pour activer la DMZ, procédez comme suit.

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SÉCURITÉ (SECURITY)** > **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)**.



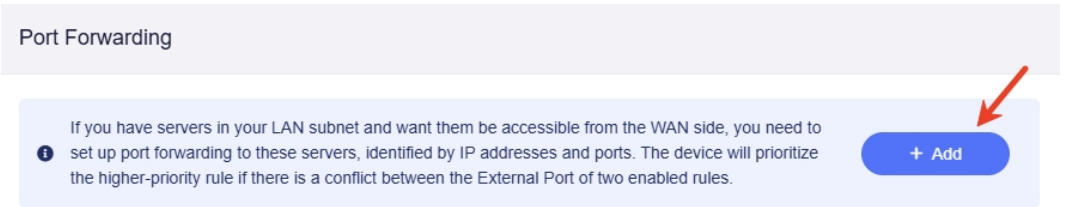
- **Priorité (Priority)** : choisissez La plus élevée ou La plus faible. Si la DMZ est prioritaire sur les règles de redirection de port, celles-ci deviennent inopérantes. Sinon, les requêtes ne sont transmises au client DMZ que si aucune règle ne correspond au port demandé.
- **IP de l'hôte DMZ (DMZ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

13.1.2 Redirection de port

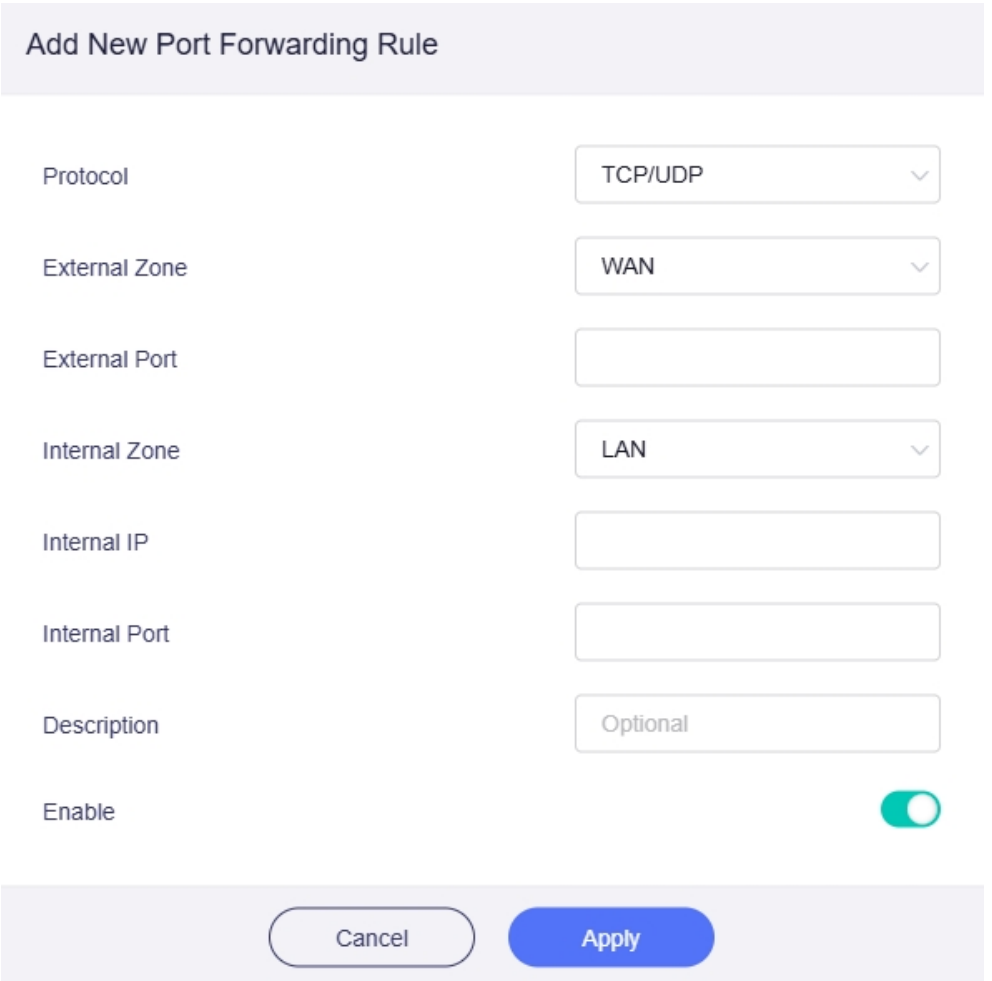
La redirection de port permet à des ordinateurs distants de se connecter à un ordinateur ou serveur local situé derrière le pare-feu LAN, comme un serveur Web ou FTP.

Pour configurer une redirection de port, procédez comme suit.

1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **SÉCURITÉ (SECURITY)** > **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.

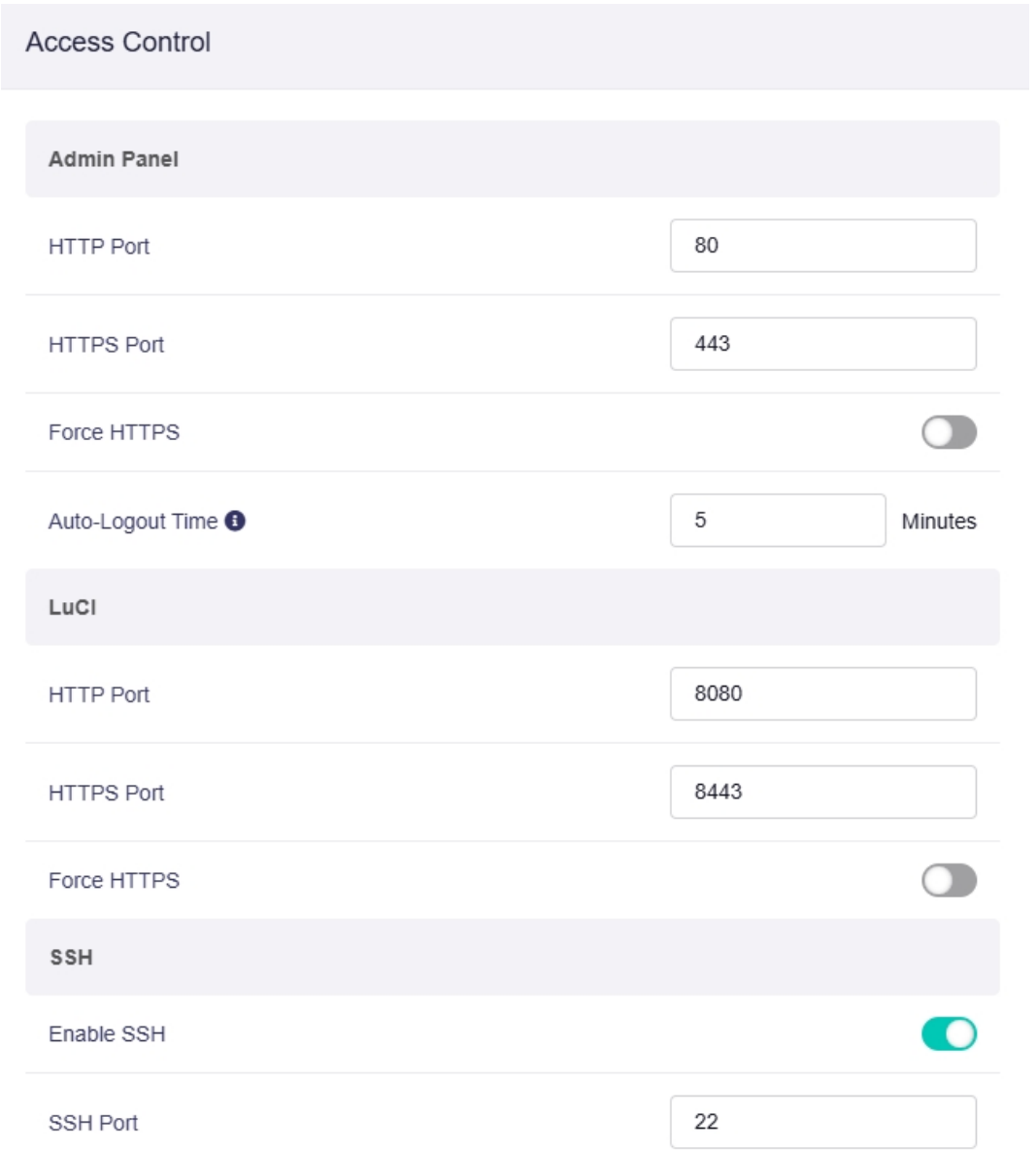
- **Description** : nom ou description de la règle, facultatif.
- **Activer (Enable)** : active ou désactive la règle.

13.2 Contrôle d’administration

Connectez-vous au panneau d’administration Web du routeur et ouvrez **SÉCURITÉ (SECURITY)** > **Contrôle de gestion (Management Control)**. Cette page comporte trois sections : Contrôle d’accès local, Contrôle d’accès à distance et Ports ouverts sur le routeur.

13.2.1 Contrôle d’accès

Cette section gère l’accès aux différentes interfaces du routeur : panneau d’administration Web, LuCI et SSH. Elle permet de prévenir les tentatives de balayage et d’intrusion sur les ports par défaut et d’éviter les problèmes réseau dus 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

Installez d’abord LuCI dans les Paramètres avancés (Advanced Settings) avant de configurer son contrôle d’accès.

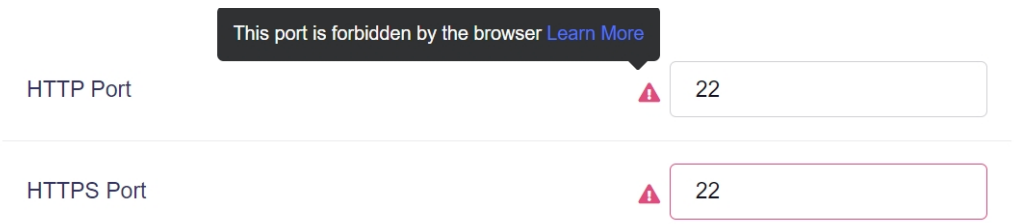
- **Port HTTP (HTTP Port)** : 8080 par défaut, pour l’accès HTTP non chiffré à LuCI.
- **Port HTTPS (HTTPS Port)** : 8443 par défaut, pour l’accès HTTPS sécurisé à LuCI.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à LuCI.

SSH

- **Activer SSH (Enable SSH)** : activée par défaut, cette option autorise ou interdit l’accès au routeur par SSH.
- **Port SSH (SSH Port)** : 22 par défaut, utilisé pour l’accès SSH au routeur.

Remarque :

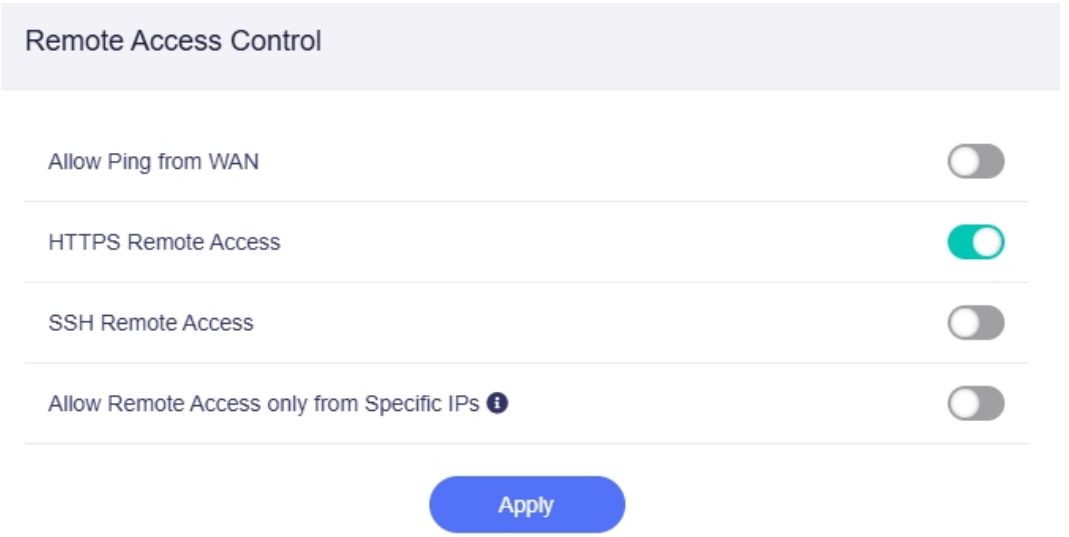
1. Si le port choisi entre en conflit avec un port réservé, notamment par les navigateurs ou les conventions réseau, le message « Ce port est interdit par le navigateur » (This port is forbidden by the browser) s’affiche.



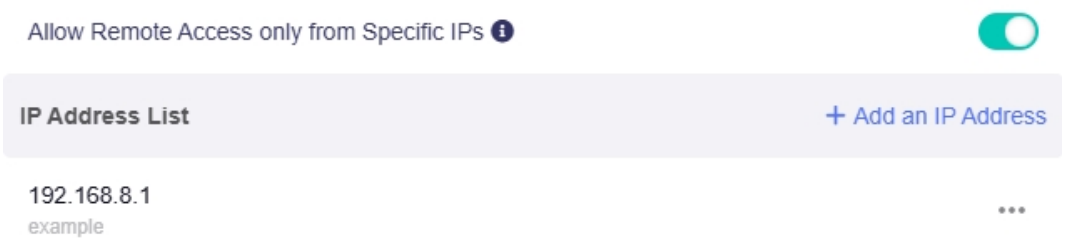
2. Si le numéro de port a été modifié dans le micrologiciel, vous devez saisir le bon numéro pour accéder au panneau d'administration. Si vous l'avez oublié, réinitialisez le routeur pour rétablir le numéro de port par défaut.
3. Les paramètres d'accès LuCI ne sont disponibles qu'après son installation. S'ils n'apparaissent pas, ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)** pour installer LuCI.

13.2.2 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.

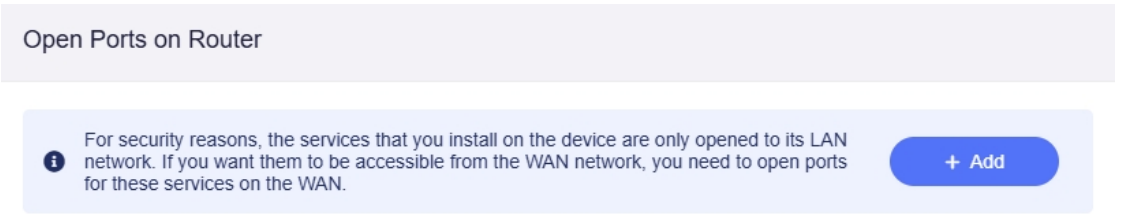


- **Autoriser le ping depuis le WAN (Allow Ping from WAN)** : permet de vérifier que le routeur est joignable depuis le WAN en cas de problème et de mesurer la latence et les pertes de paquets.
- **Accès HTTPS à distance (HTTPS Remote Access)** : permet d’accéder de manière sécurisée à l’interface Web 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.

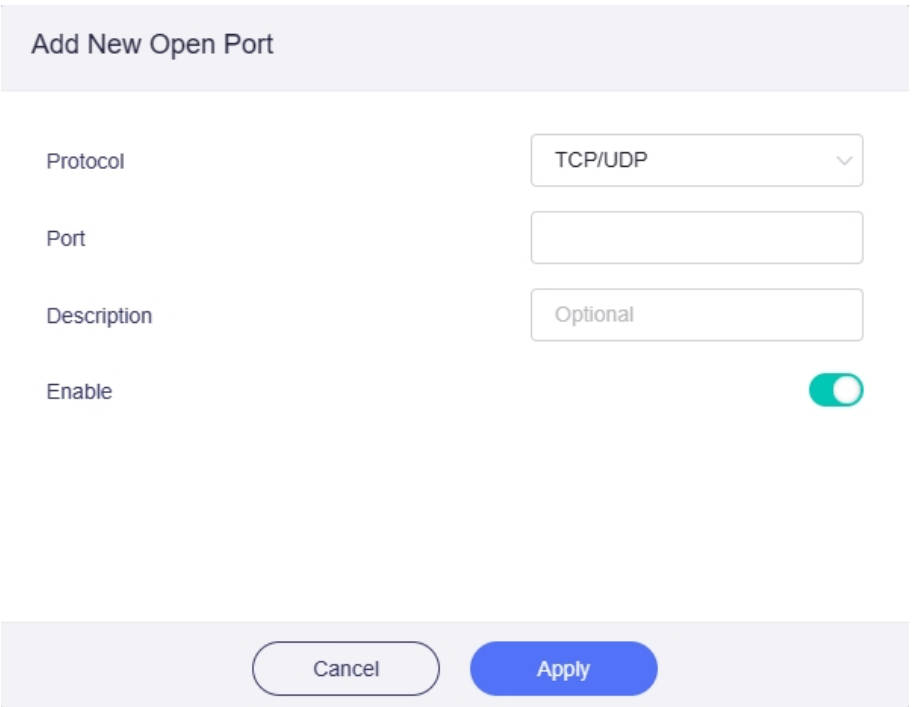


13.2.3 Ouverture de ports sur le routeur

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.



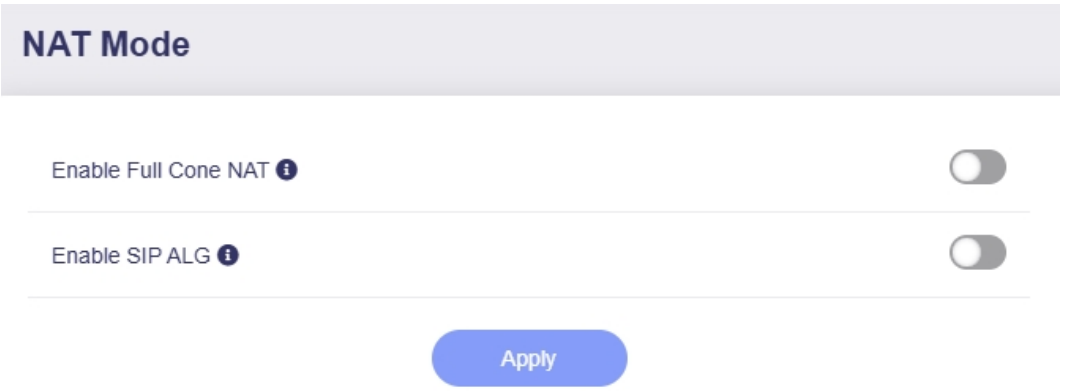
Pour ouvrir un port, cliquez sur **Ajouter (Add)**, puis renseignez les informations demandées dans la fenêtre.



- **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.

13.3 Mode NAT

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SÉCURITÉ (SECURITY)** > **Mode NAT (NAT Mode)**. Cette page permet de configurer deux fonctions liées au NAT : 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 14

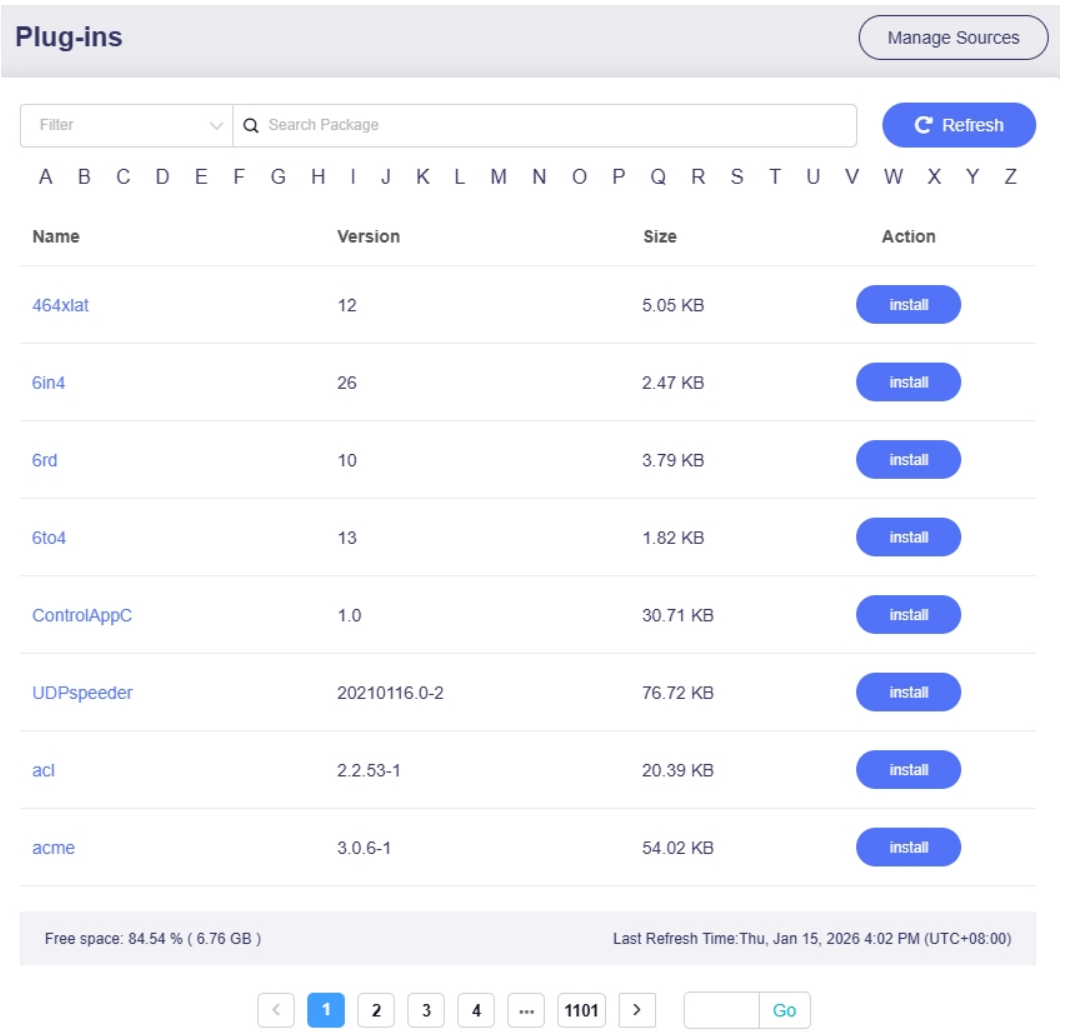
Applications

Ce chapitre présente certaines applications des routeurs GL.iNet, notamment les plug-ins, le DNS dynamique et le stockage réseau.

14.1 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 :

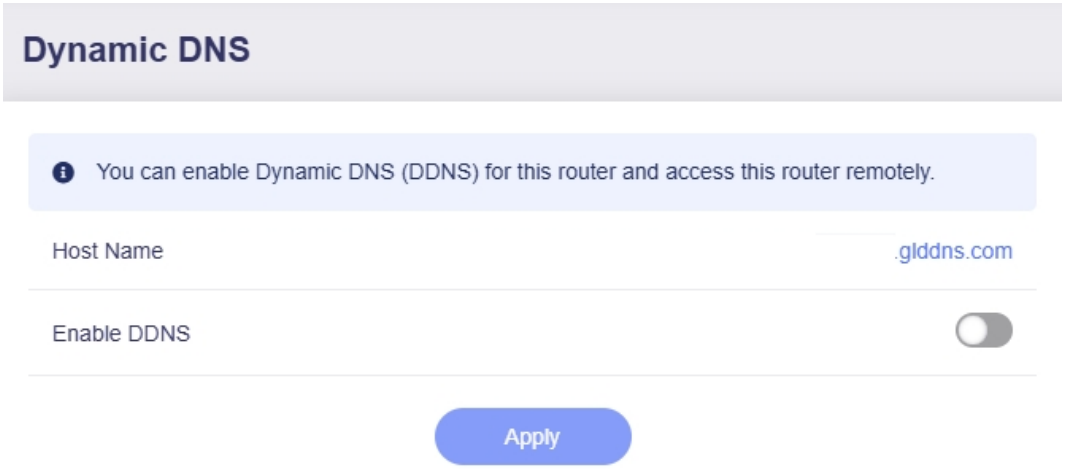
1. Il est déconseillé de mettre à jour les extensions préinstallées dans le micrologiciel officiel GL.iNet, comme nginx, AdGuard Home ou Tailscale.
2. Les extensions tierces installées manuellement peuvent être mises à jour. GL.iNet n'est toutefois pas responsable des problèmes de sécurité qu'elles peuvent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

14.2 DNS dynamique

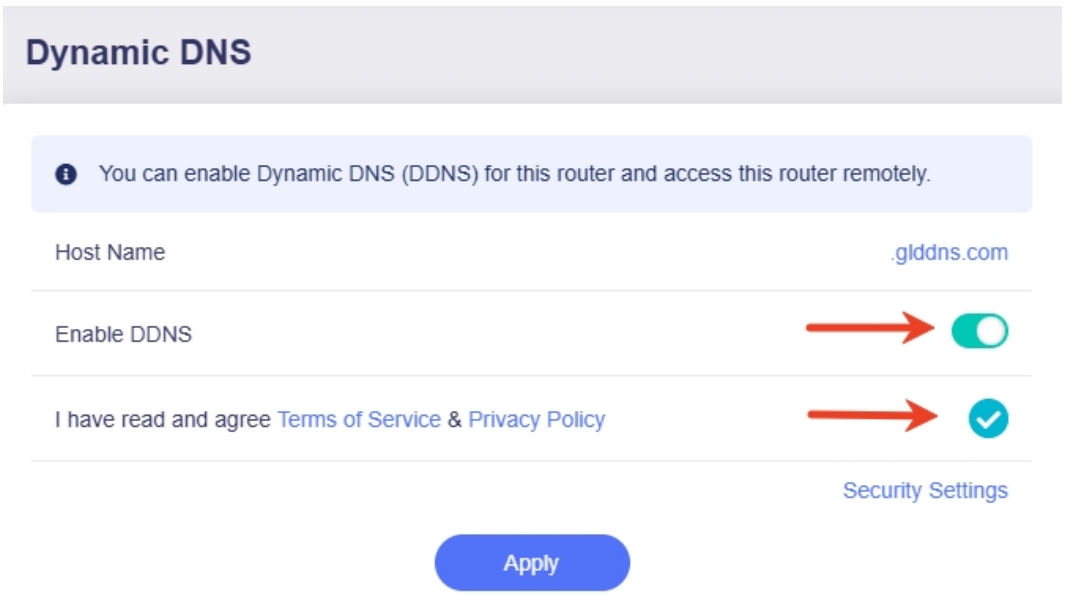
Le DNS dynamique (DDNS) associe un nom de domaine à l'adresse IP dynamique d'un appareil réseau. Il permet d'accéder au routeur à distance. Cette fonction nécessite une adresse IP publique.

14.2.1 Activation du DDNS

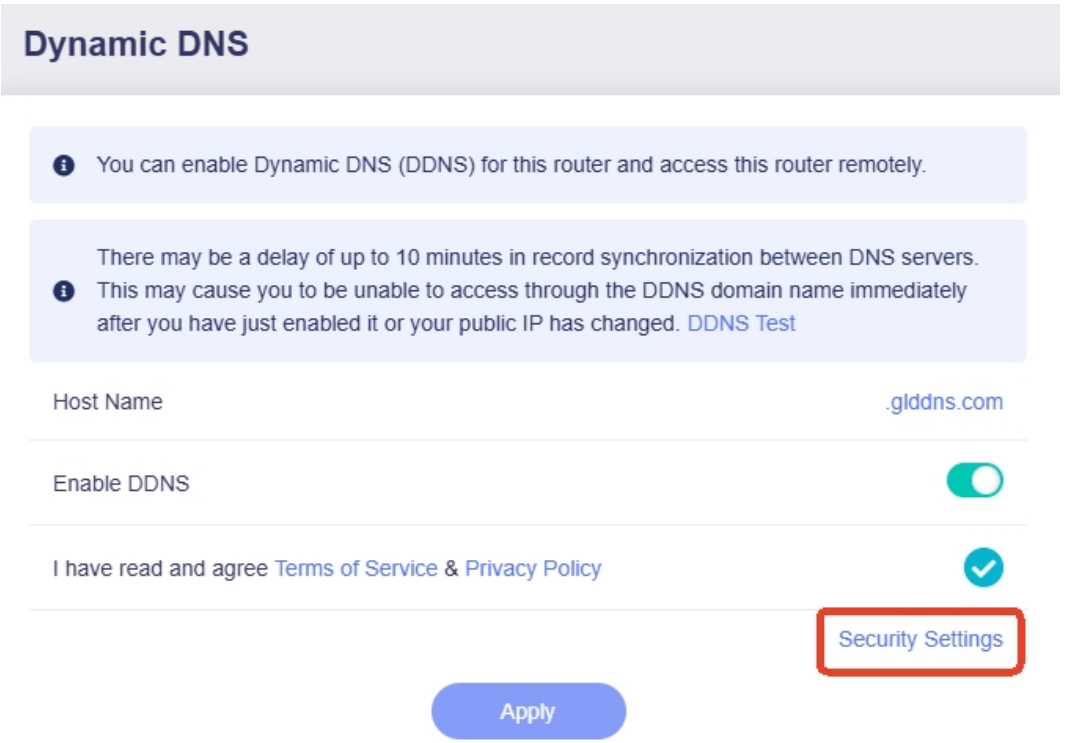
1. Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)**. La page ci-dessous s'affiche.



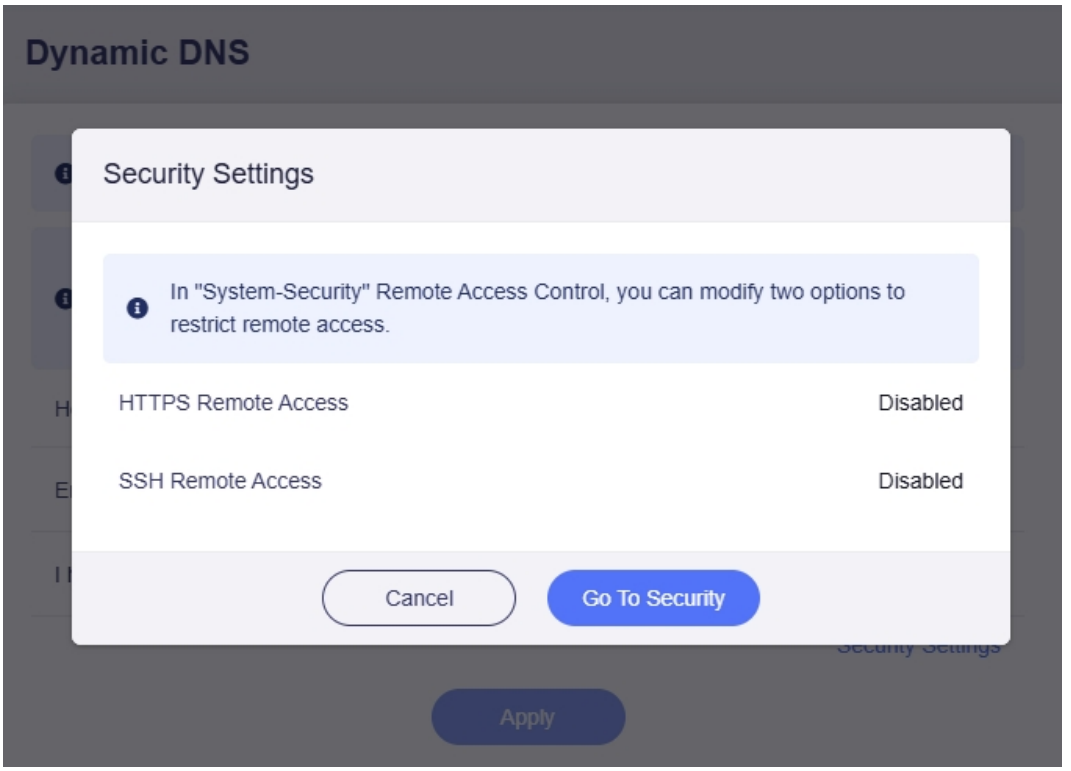
2. Activez **Activer le DDNS (Enable DDNS)**, lisez et acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



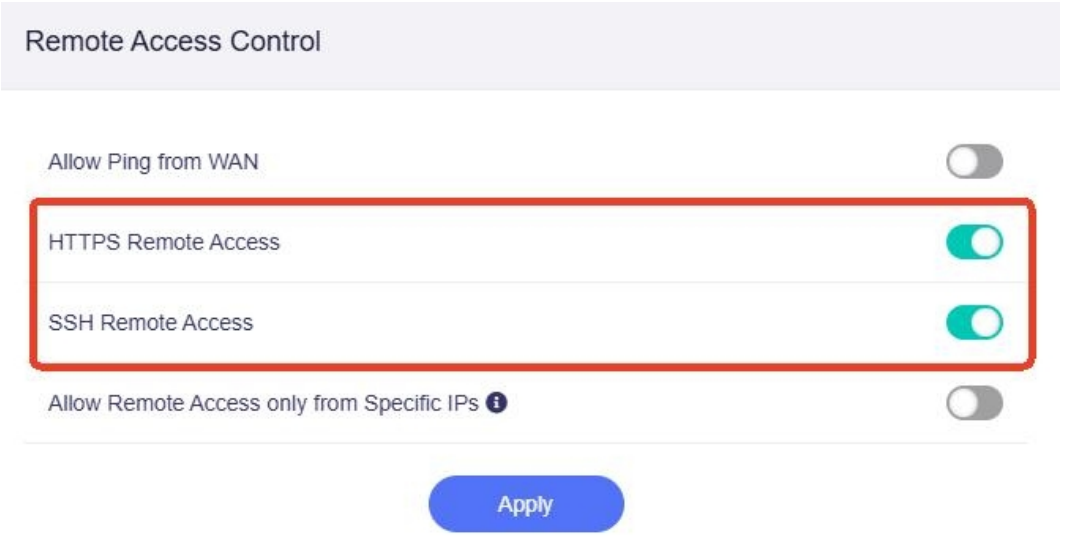
3. Cliquez sur **Paramètres de sécurité (Security Settings)** dans l'angle inférieur droit.



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



Sinon, ouvrez **Système (System)** > **Sécurité (Security)** > **Contrôle d'accès à distance (Remote Access Control)** pour l'activer, puis cliquez sur **Appliquer (Apply)**.



Remarque :

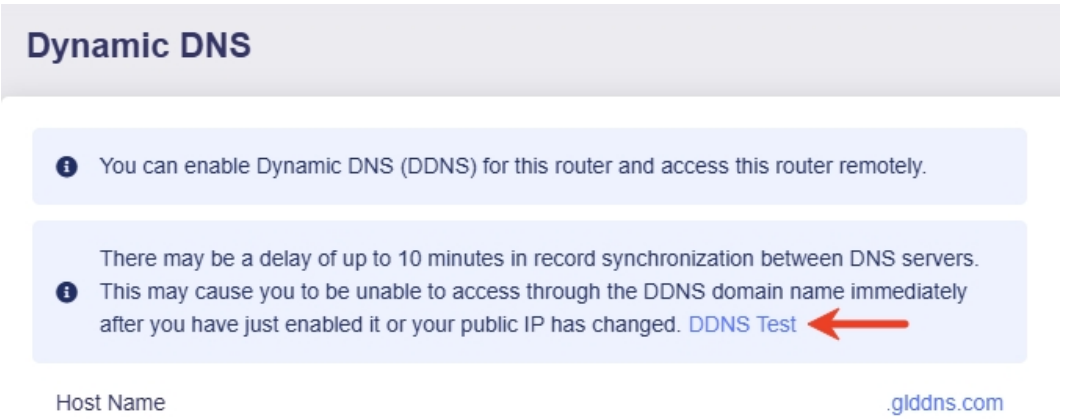
1. La synchronisation des enregistrements entre serveurs DNS peut prendre jusqu'à 10 minutes. L'accès par le domaine DDNS peut donc être indisponible immédiatement après son activation ou après un changement d'IP publique.
2. Si vous activez simultanément le DDNS et un client VPN, vérifiez que Services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

14.2.2 Vérification du fonctionnement du DDNS

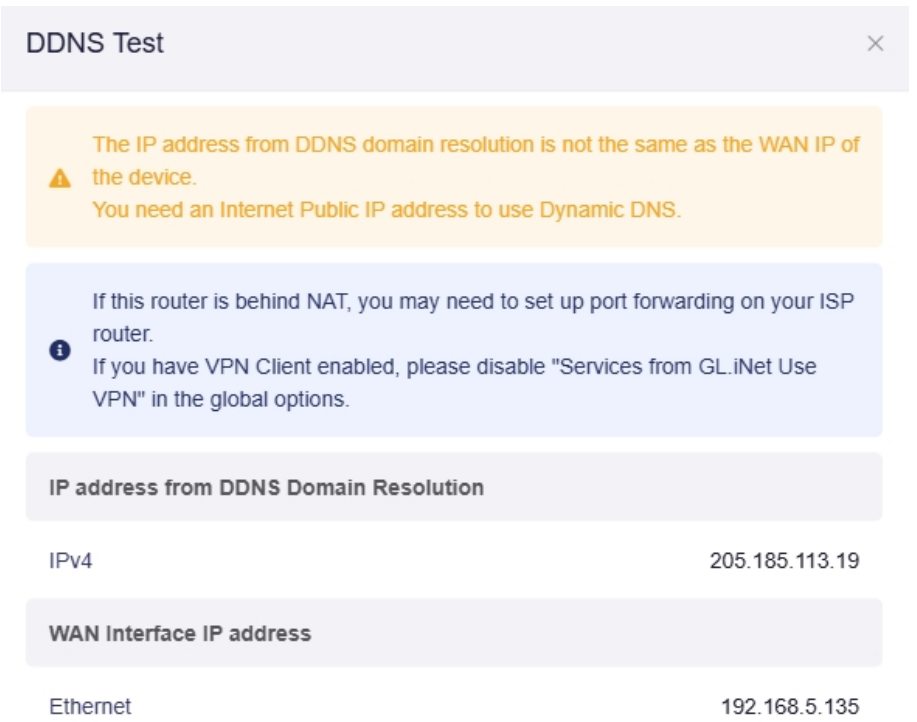
Vérifiez le DDNS avec l'outil de test intégré ou manuellement à l'aide de commandes.

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 nslookup avec la commande *nslookup xxxxxxx.glddns.com 8.8.8.8* pour afficher l'adresse IP associée au domaine, comme ci-dessous.



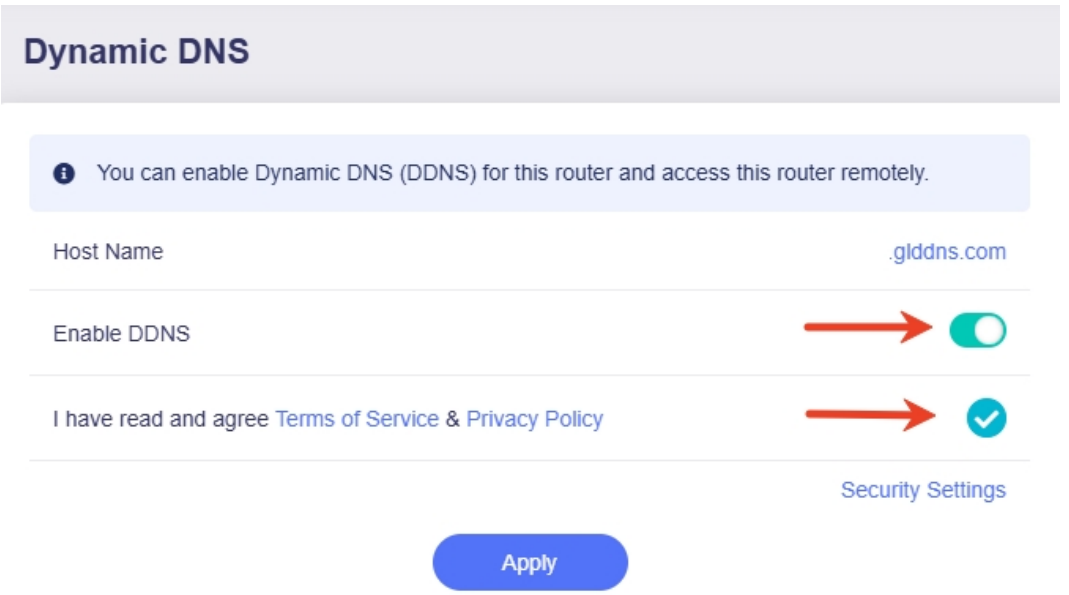
   - Remplacez « xxxxxxx.glddns.com » par votre nom d'hôte.
   - « 8.8.8.8 » est le DNS de Google. Utilisez-le ou indiquez un autre serveur, puis appuyez sur Entrée.
2. Une IP publique, comme « 183.178.10.100 » dans l'image, indique que le domaine DDNS est bien associé à une adresse publique. Un message comme « server can't find xxxxxxx.glddns.com » peut indiquer un échec de résolution. Passez à l'étape suivante pour vérifier.
3. Dans l'interface Web du routeur, ouvrez **INTERNET** et repérez l'IP WAN de l'interface active. Comparez-la à l'IP publique obtenue précédemment. Si elles sont identiques, le DDNS fonctionne ; sinon, il ne fonctionne pas.

14.2.3 Accès HTTPS à distance

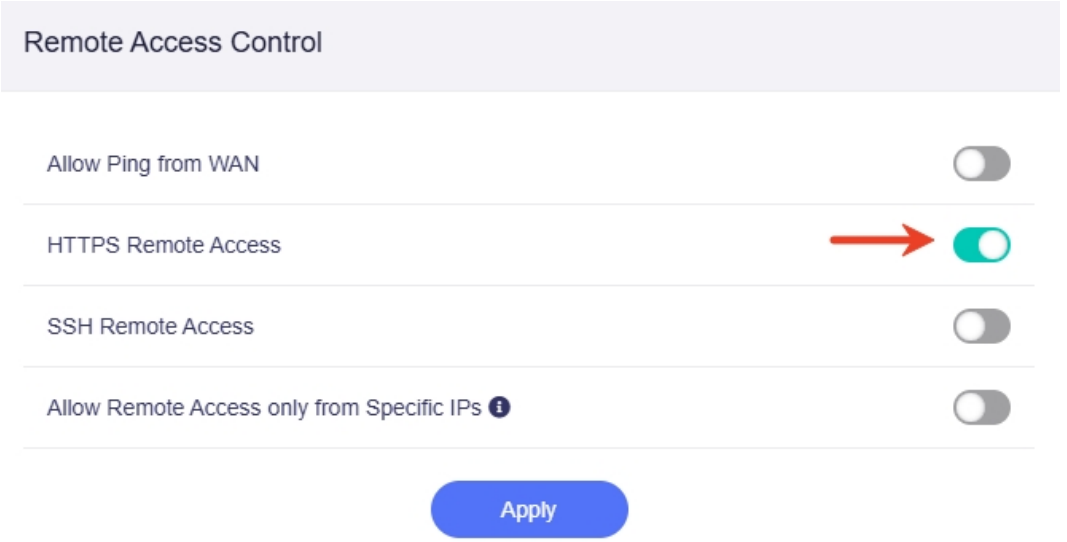
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 443** sur le routeur en amont.

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)**.

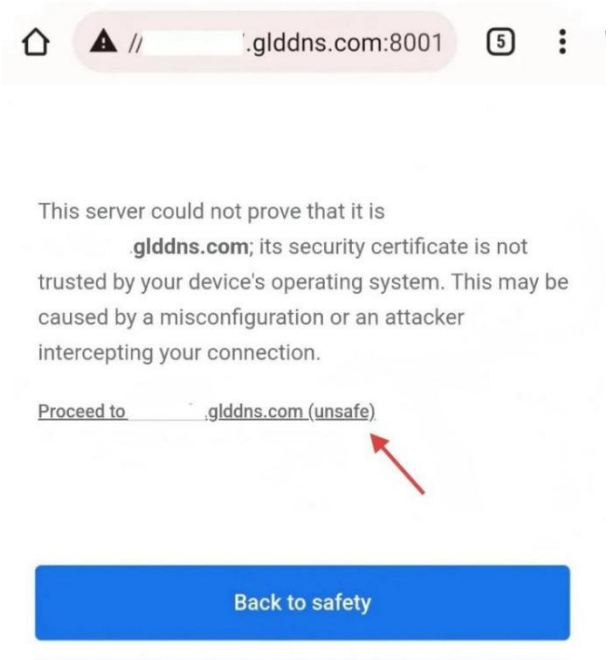


2. Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)**. Activez **Accès HTTPS à distance (HTTPS Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



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.



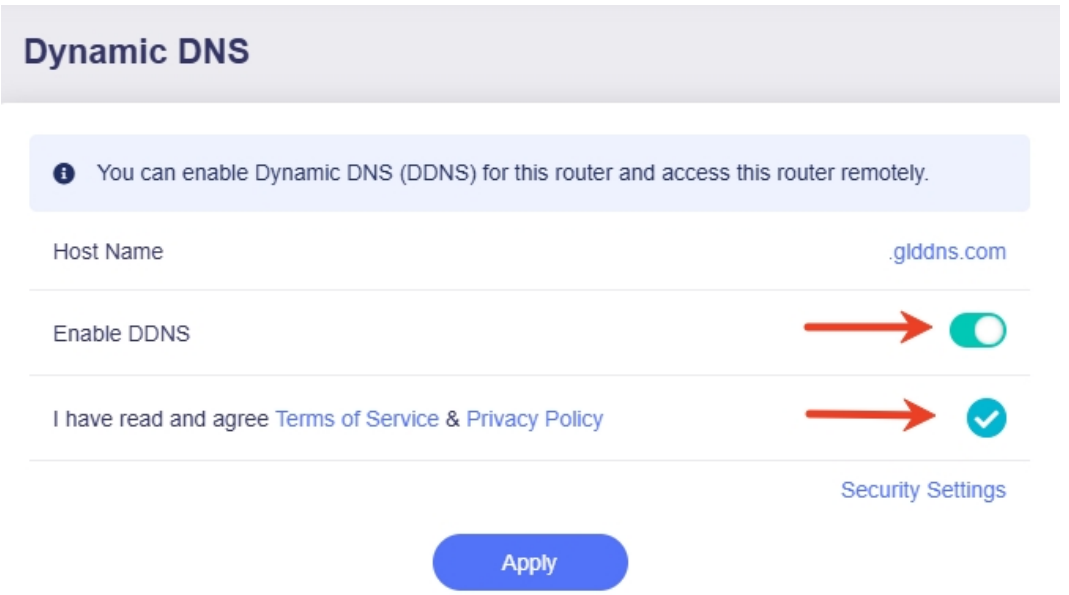
Vous pouvez alors accéder à l’interface Web par le nom d’hôte DDNS en **HTTPS**.

14.2.4 Accès SSH à distance

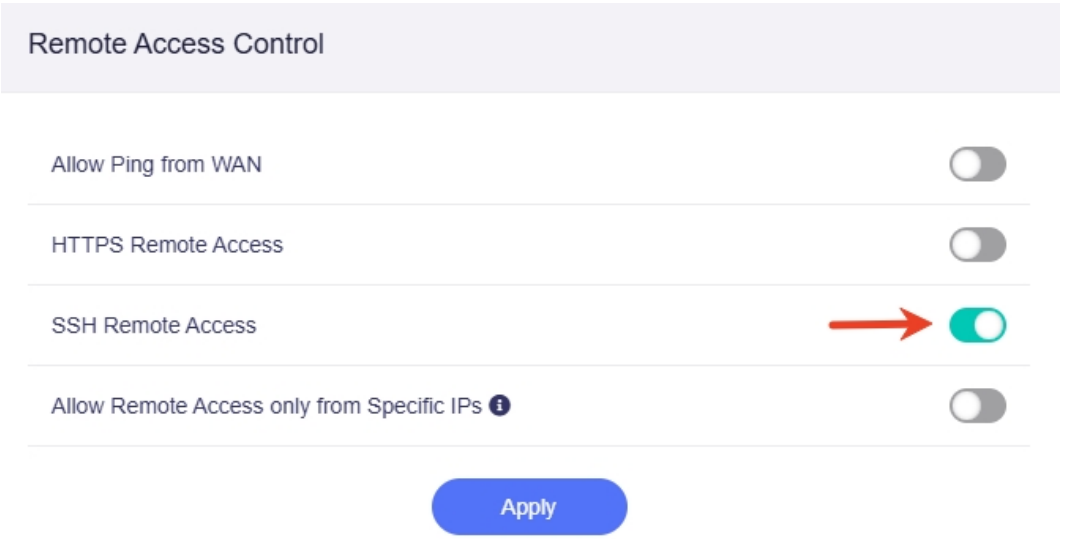
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 22** sur le routeur en amont.

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.

14.3 Stockage réseau

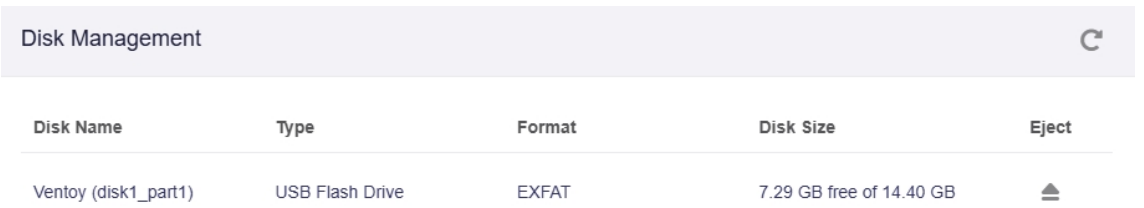
Le stockage réseau permet de partager des fichiers sans fil entre appareils en connectant une clé USB ou une carte SD au routeur. Celui-ci transforme le support de stockage en un partage réseau accessible à tous les appareils connectés au Wi-Fi.

Opal dispose d'un port USB compatible avec les clés USB et les disques durs externes portables. Vous pouvez configurer Samba pour ces supports de stockage, qui prennent en charge les formats courants tels que NTFS, FAT32 et EXT4.

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

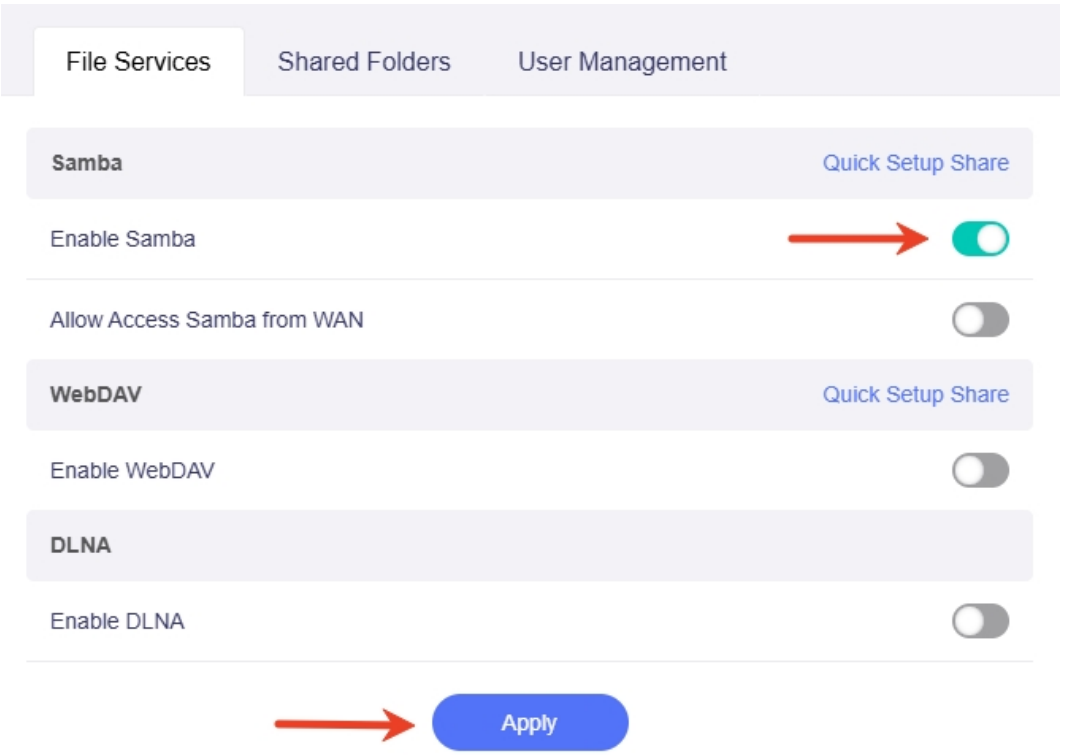
14.3.1 Branchement du stockage

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.



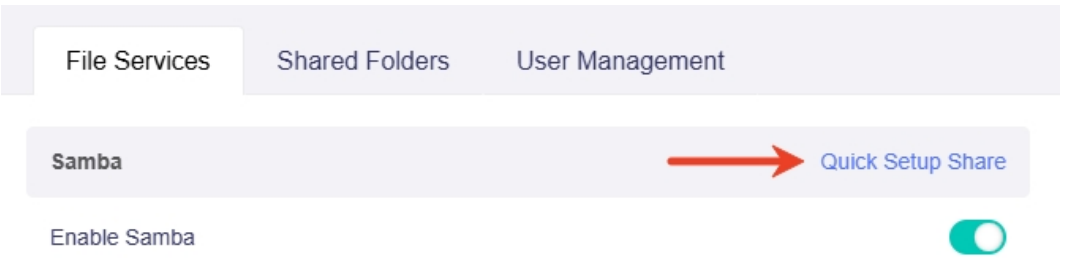
14.3.2 Configuration de Samba

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

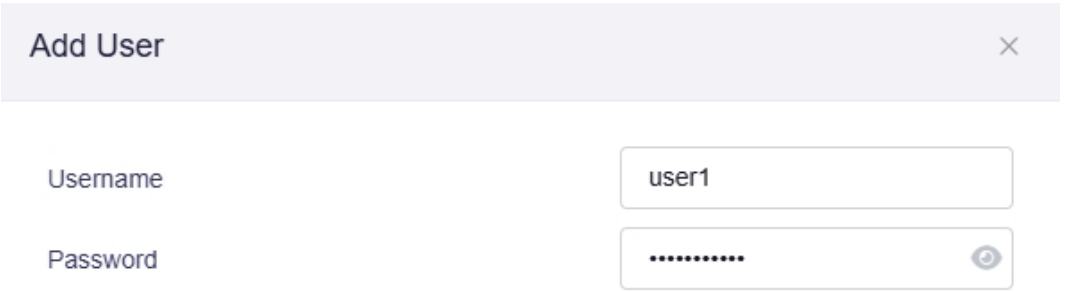


   - **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** : activez cette option pour que les appareils en amont accèdent à Samba.

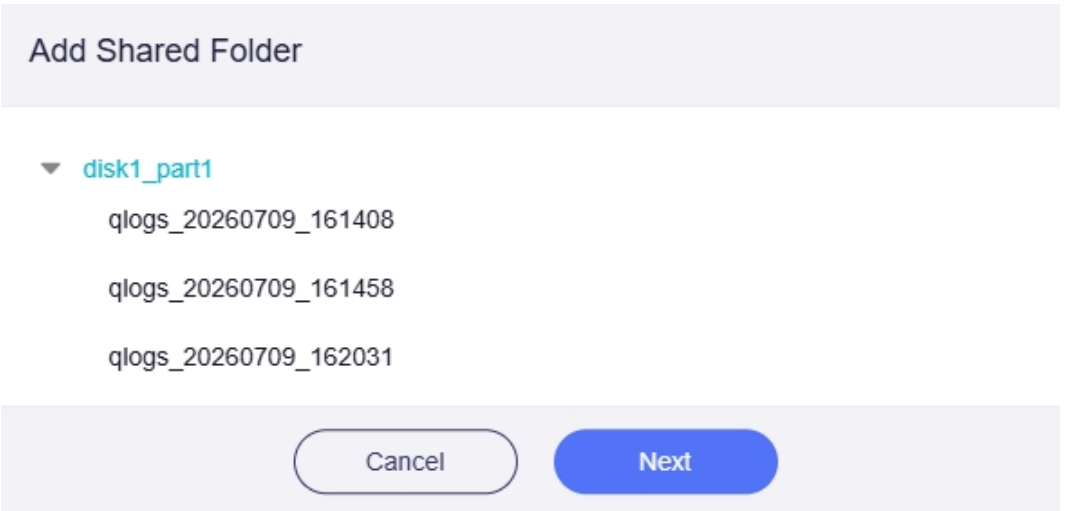
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



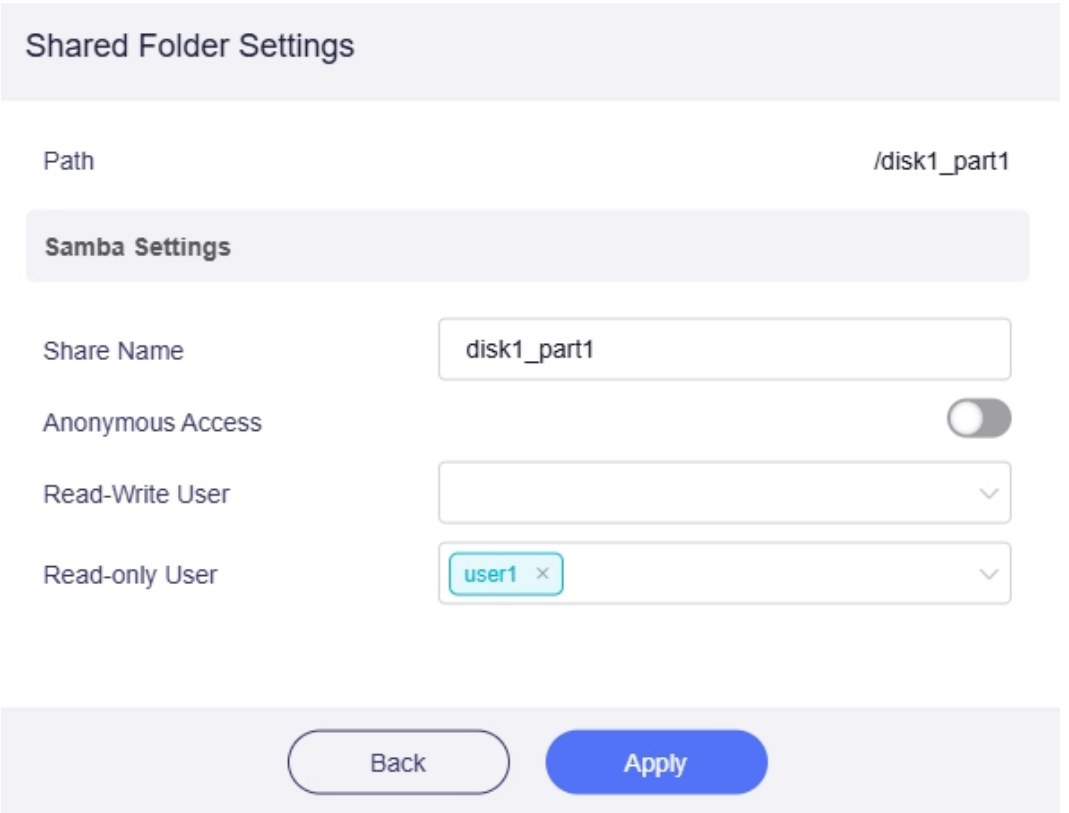
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



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.

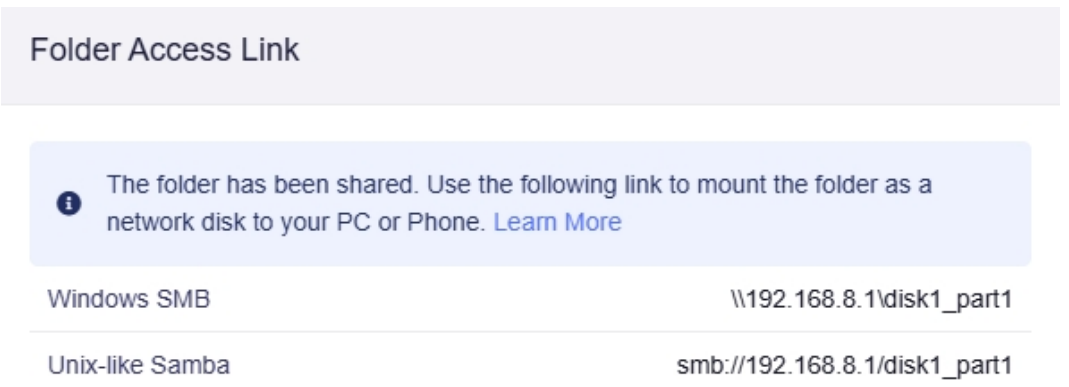


5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**. Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez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

Chapitre 15

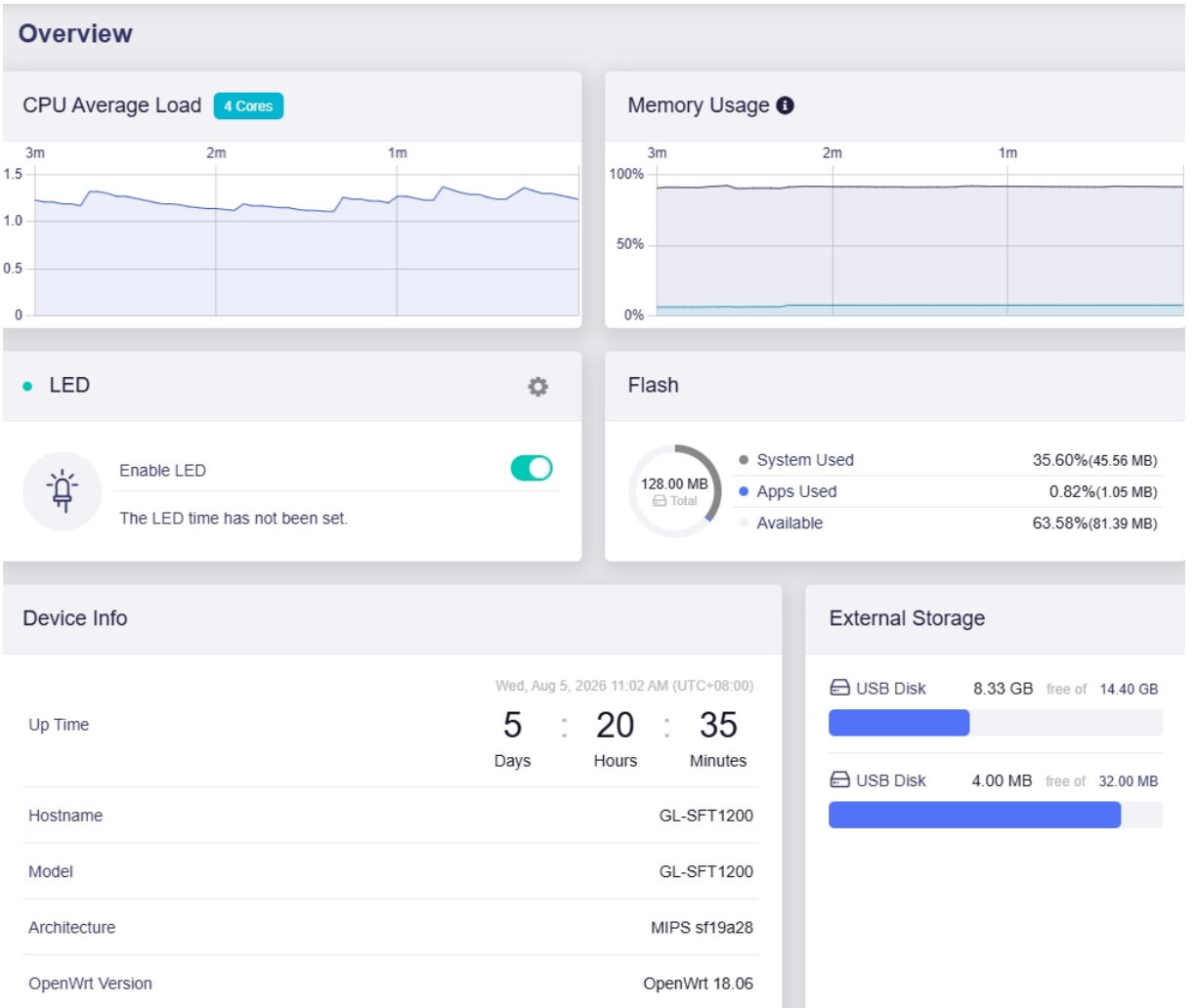
Système

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

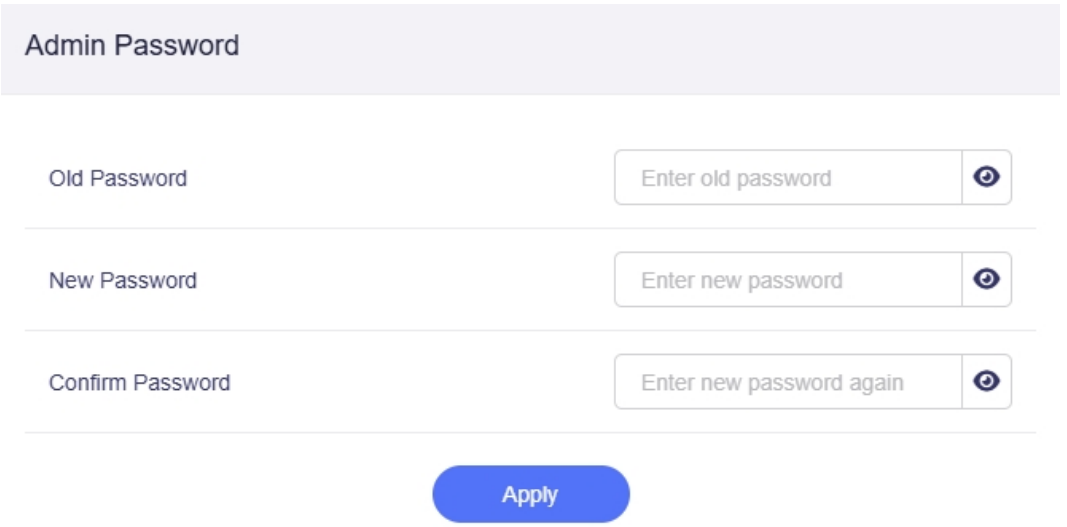
Dans l’interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Vue d’ensemble (Overview)**. Cette page affiche l’état du matériel et propose des commandes simples :

- 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 Mot de passe administrateur

Connectez-vous au panneau d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Mot de passe administrateur (Admin Password)**. Vous pouvez modifier le mot de passe de connexion au panneau d'administration Web.



Le mot de passe administrateur doit respecter les règles suivantes :

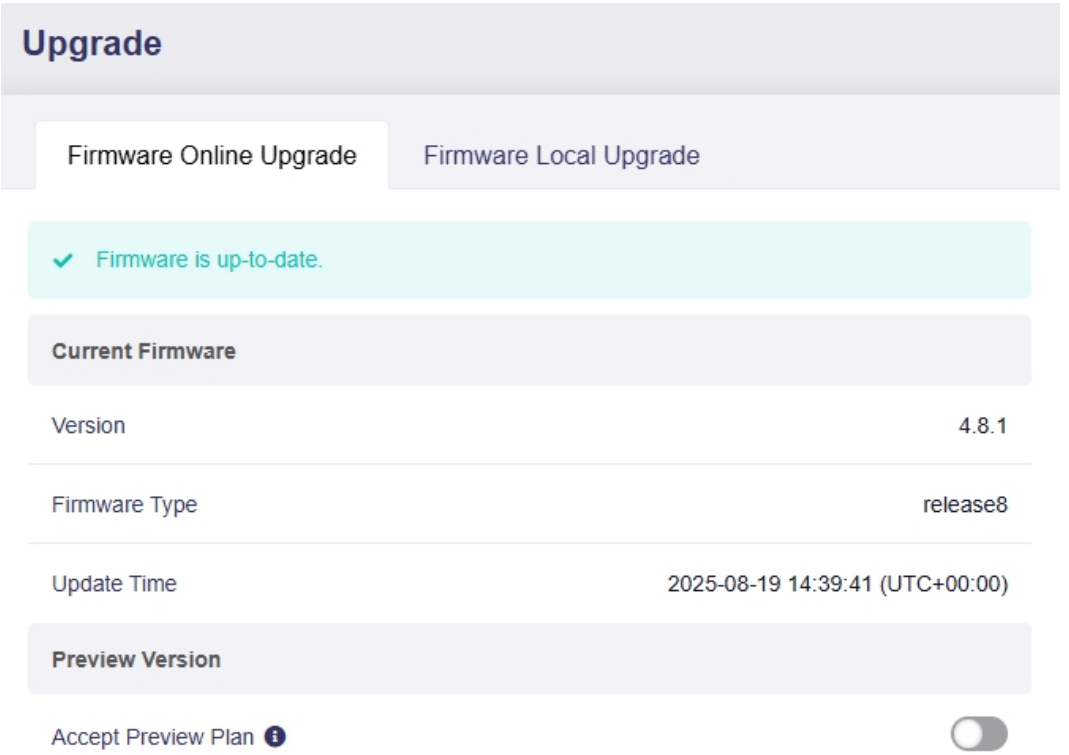
1. Entre 10 et 63 caractères.
2. Les lettres, avec distinction de casse, les chiffres et les symboles sont autorisés, par exemple : ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~
3. Au moins deux catégories sont nécessaires parmi les majuscules, les minuscules, les chiffres et les symboles.

15.3 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.

15.3.1 Mise à jour en ligne

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.



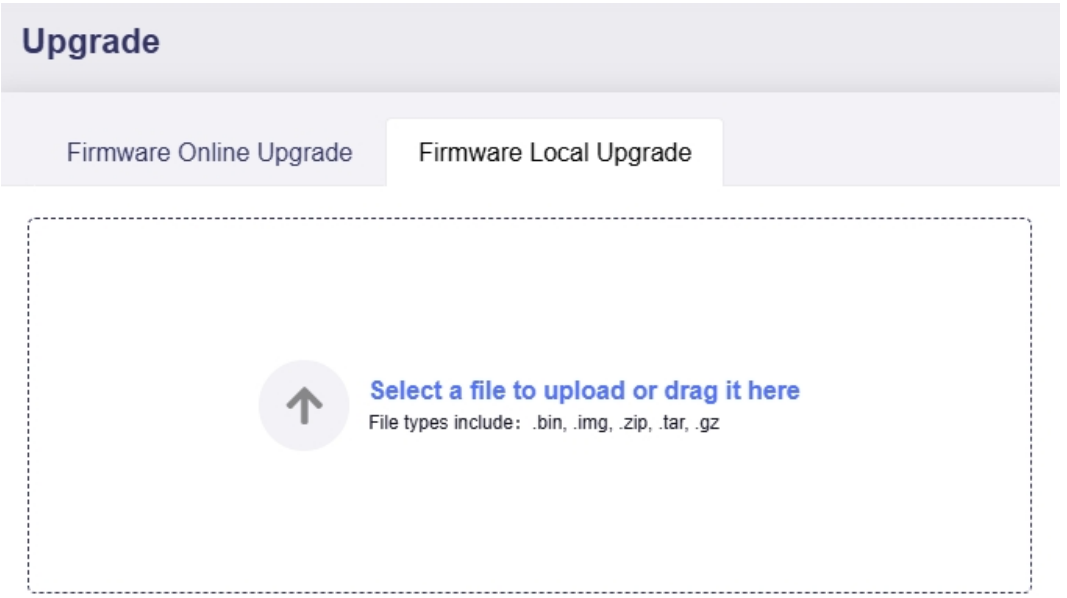
- **Accepter le programme de préversion (Accept Preview Plan)** : cette option apparaît de façon aléatoire selon le modèle et le micrologiciel. Lorsqu'elle est activée, vous pouvez essayer de nouvelles fonctions avant la sortie de la version définitive et nous faire part de vos commentaires. Une fois activée, elle le reste. Ces mises à jour peuvent être instables.

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.

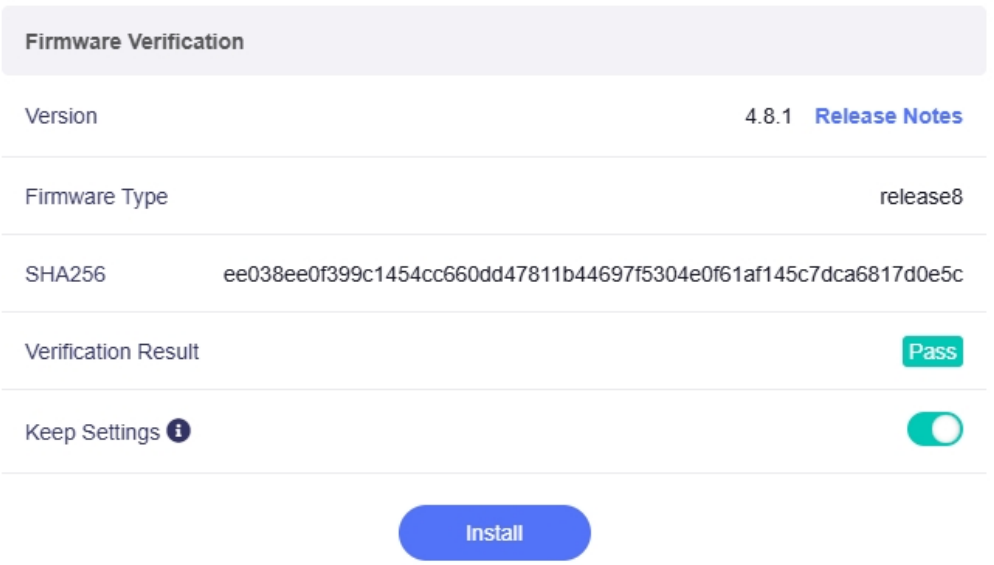
15.3.2 Mise à jour locale

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.

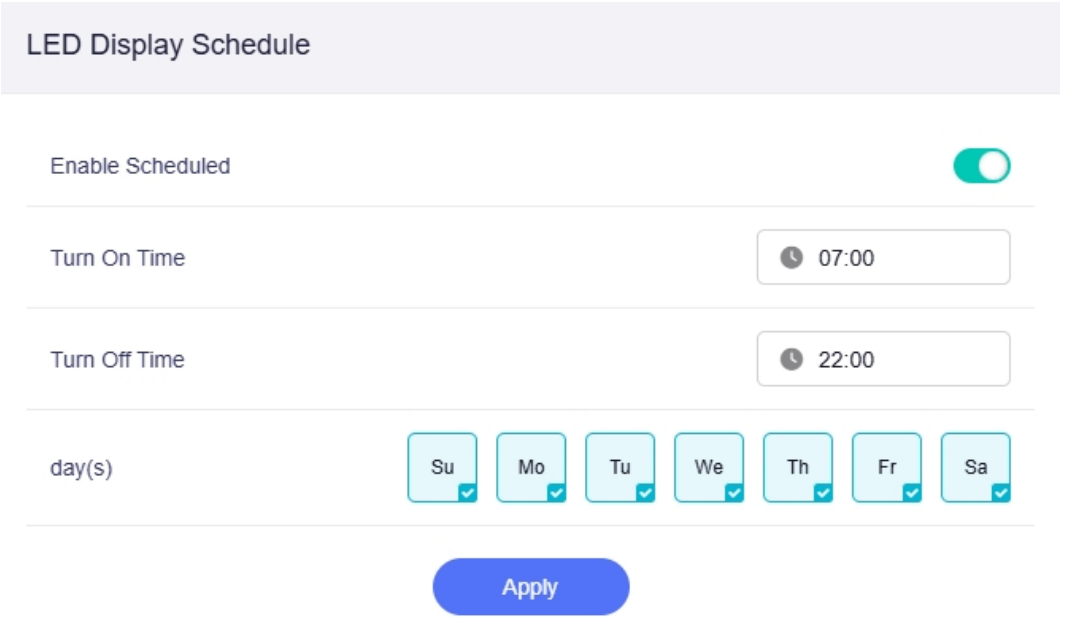
15.4 Tâches planifiées

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.

15.4.1 Programmation du voyant LED

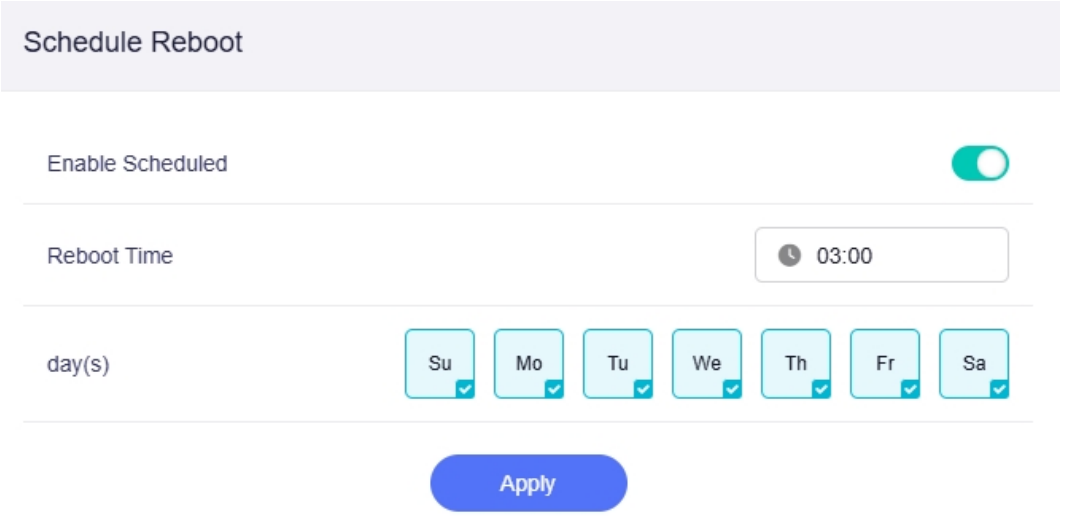
Définissez le planning du voyant si nécessaire, puis cliquez sur **Appliquer (Apply)**.



- **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.

15.4.2 Redémarrage planifié

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



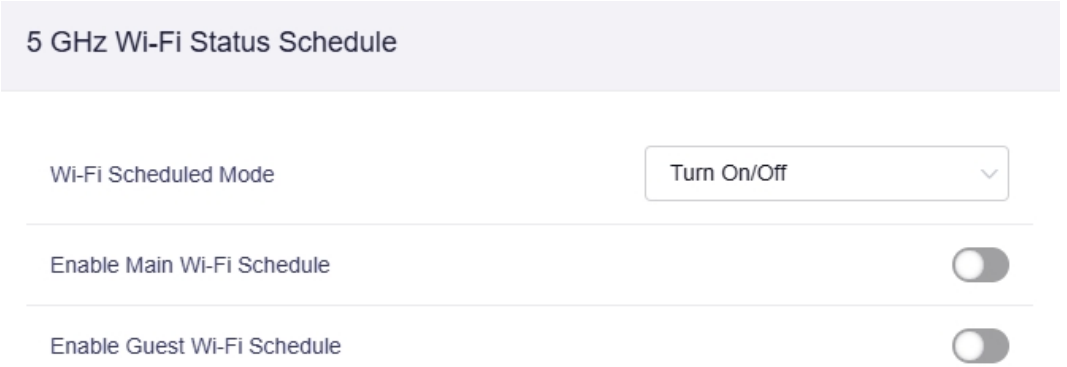
- **Activer la programmation (Enable Scheduled)** : active le redémarrage planifié.
- **Heure de redémarrage (Reboot Time)** : heure à laquelle le routeur redémarre, par exemple 03:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

15.4.3 Programmation du Wi-Fi 5 GHz

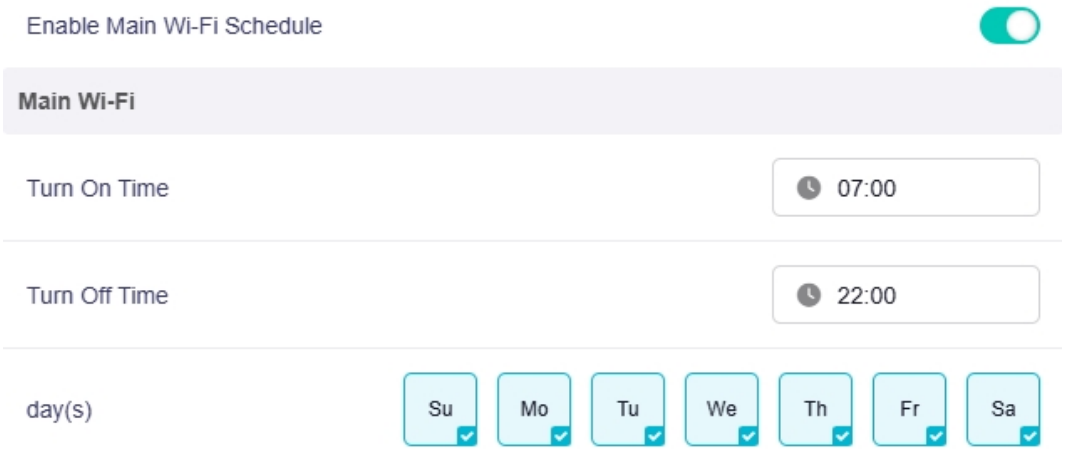
Cette fonction permet de programmer le Wi-Fi 5 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

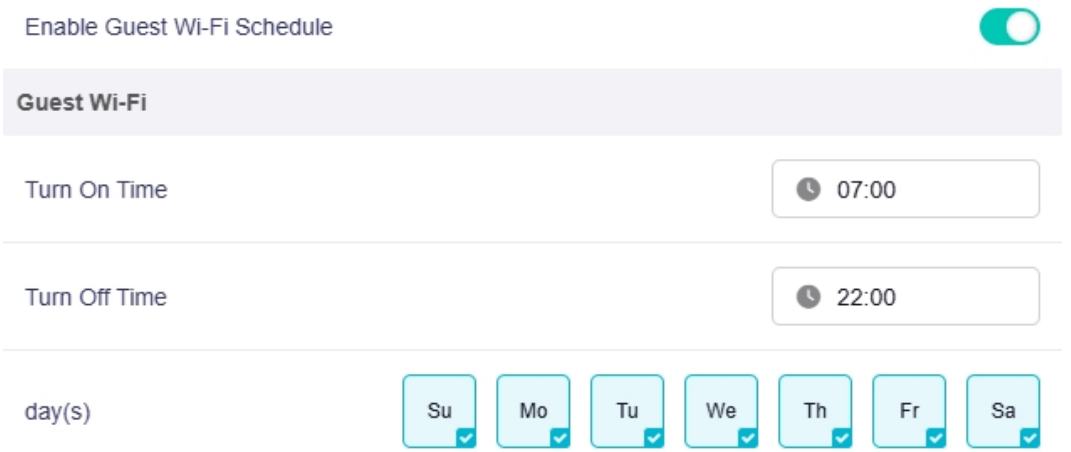
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 5 GHz.



- **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.

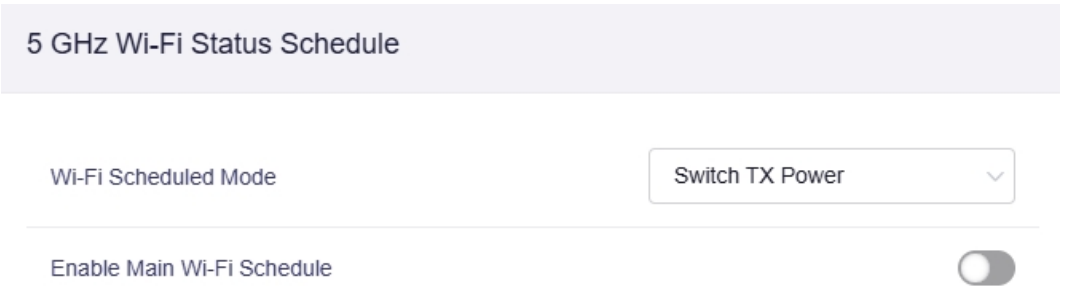


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 5 GHz et les jours concernés.

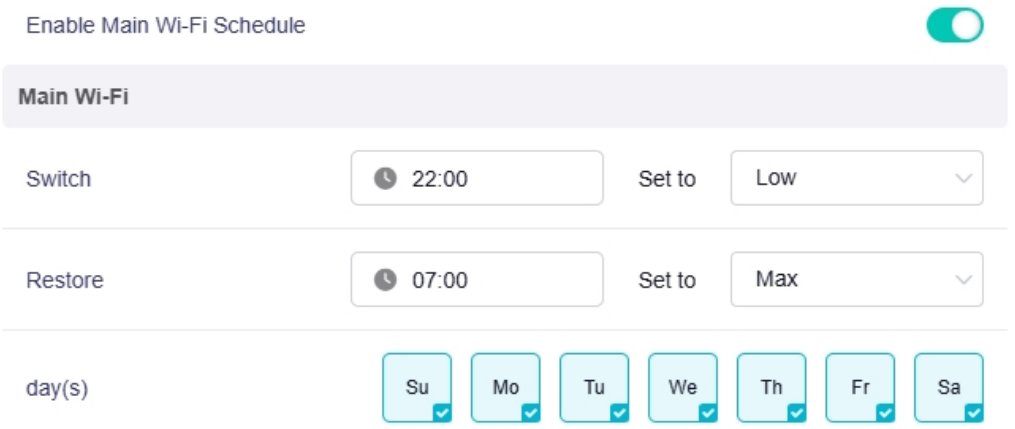


Mode 2 : Modifier la puissance d’émission

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.

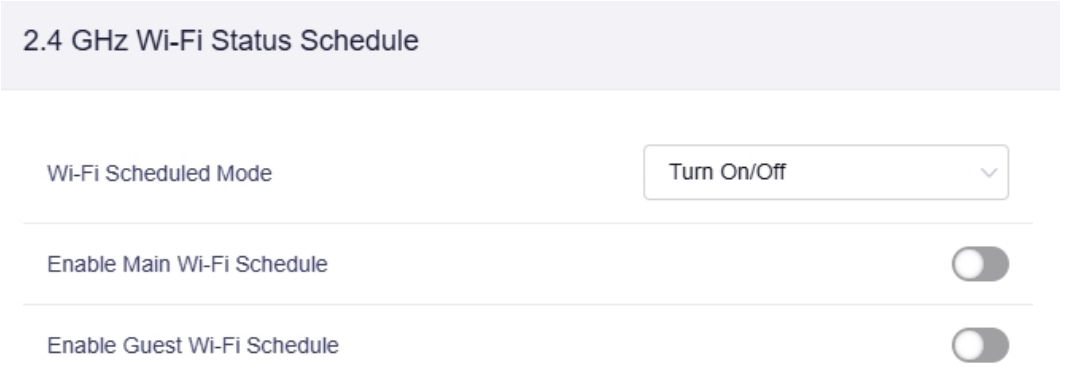
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

15.4.4 Programmation du Wi-Fi 2,4 GHz

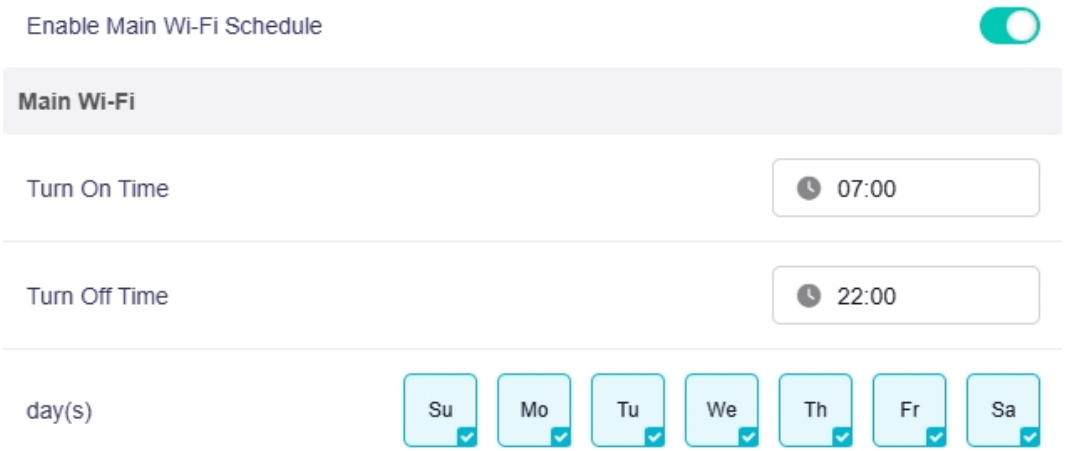
Cette fonction permet de programmer le Wi-Fi 2,4 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

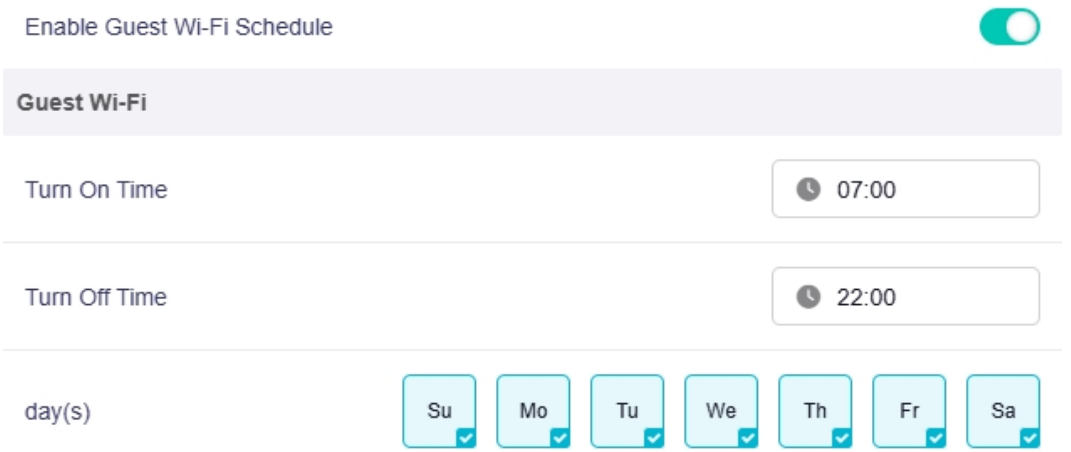
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 2,4 GHz.



- **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.

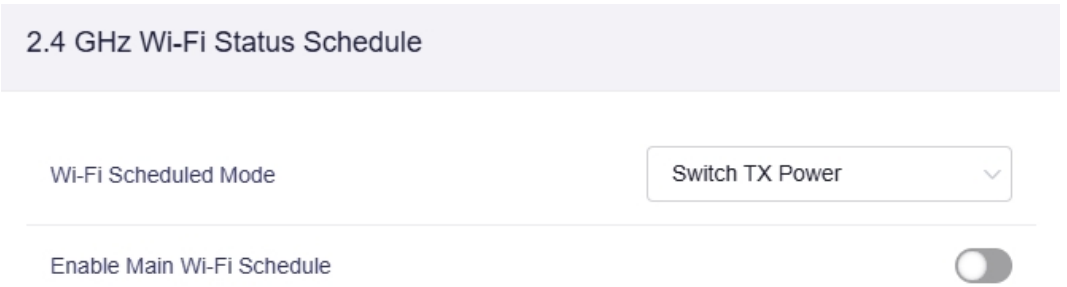


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 2,4 GHz et les jours concernés.

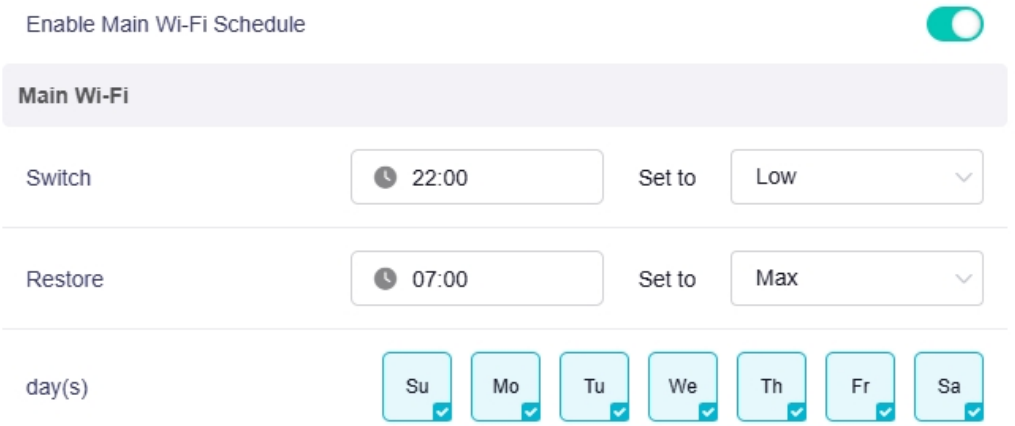


Mode 2 : Modifier la puissance d’émission

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.

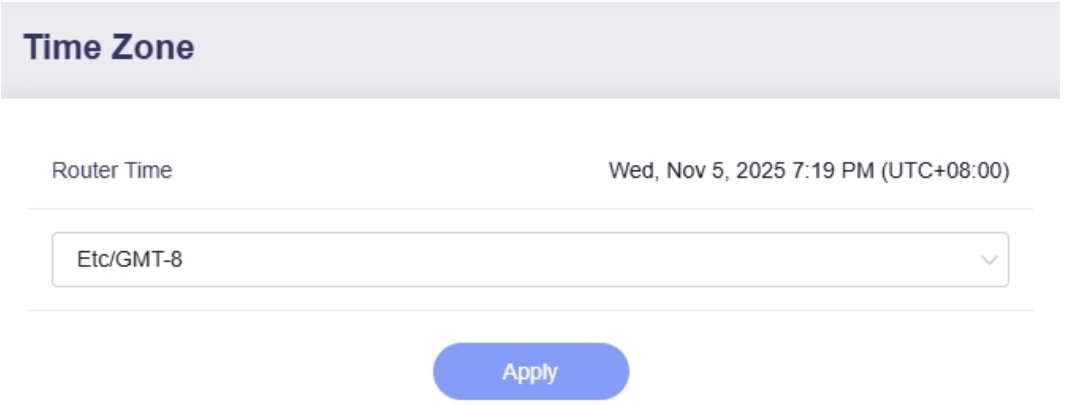


- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.

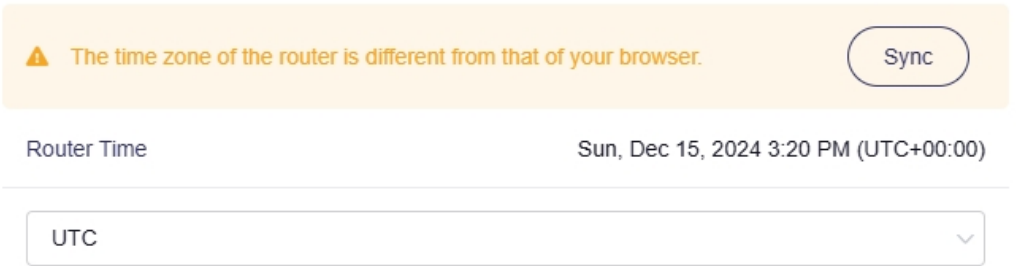
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

15.5 Fuseau horaire

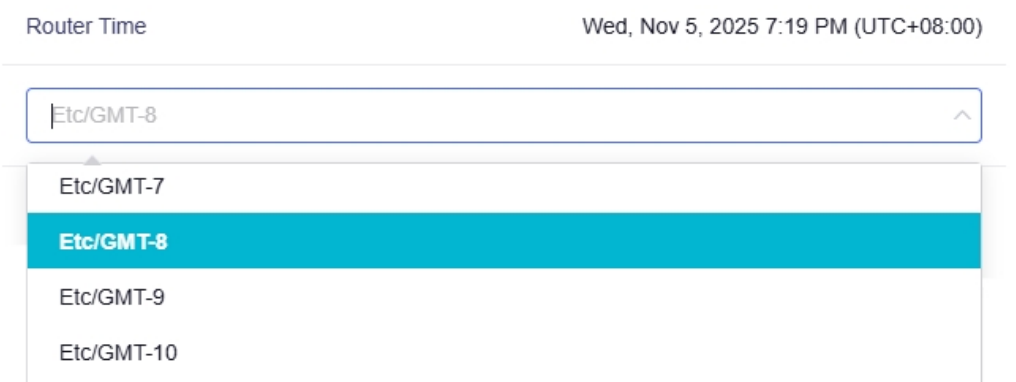
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)**. La page affiche la date et l'heure système du routeur ainsi que le décalage du fuseau horaire.



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.

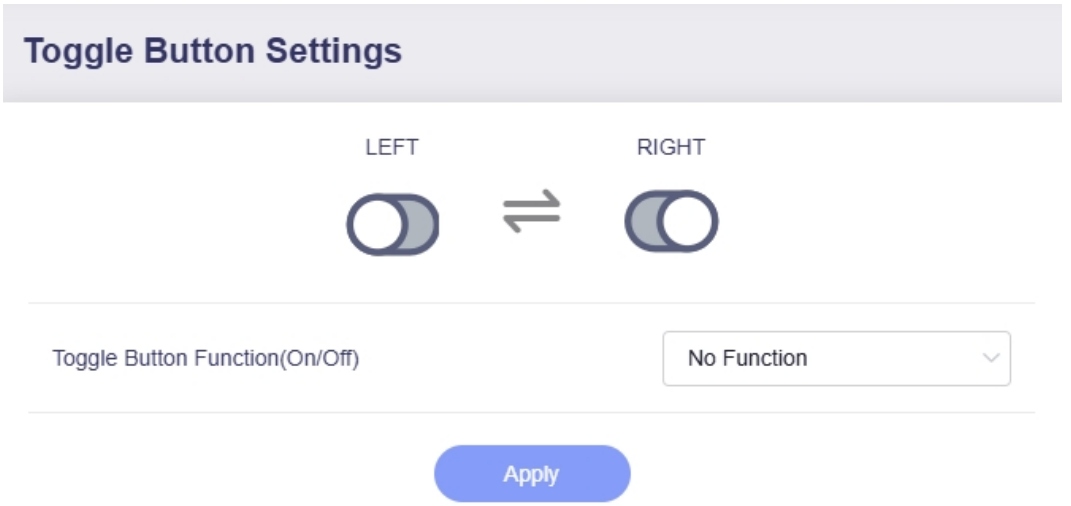


Pour changer de fuseau, sélectionnez celui qui convient dans la liste afin que l'heure du routeur corresponde à l'heure locale.

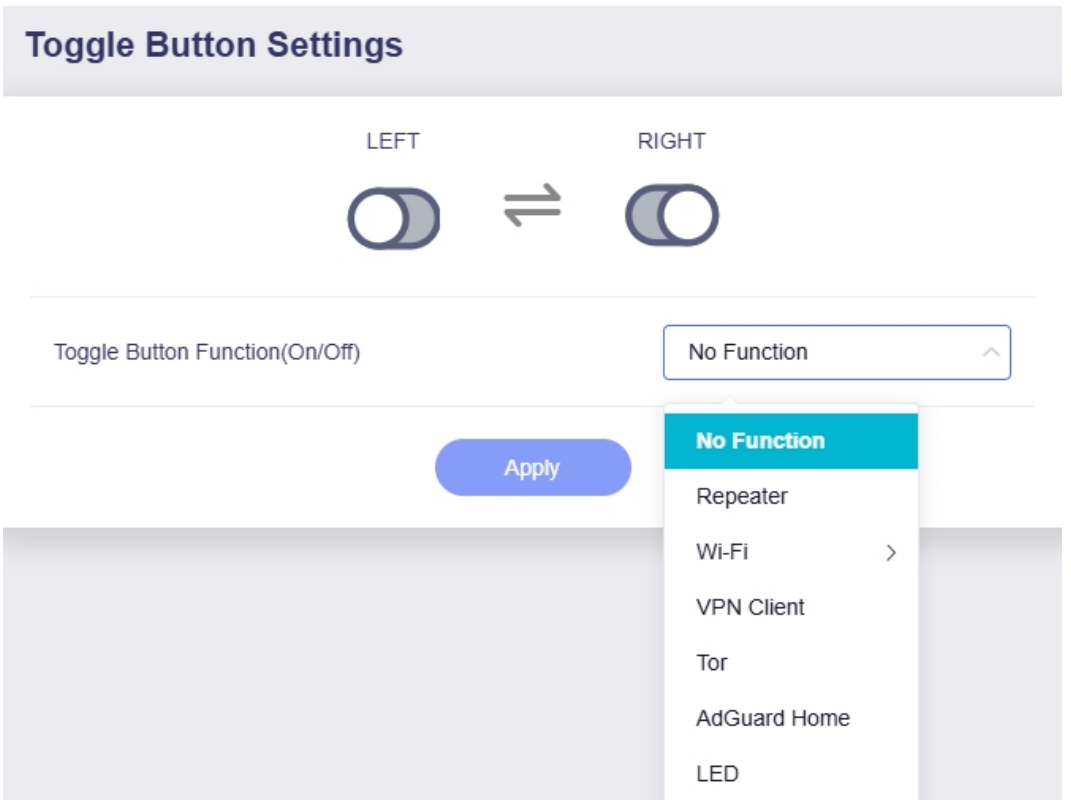


15.6 Paramètres du commutateur

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Paramètres de l'interrupteur (Toggle Button Settings)**. Cette page permet de personnaliser la fonction de l'interrupteur physique situé sur le côté du routeur pour en faciliter l'utilisation.



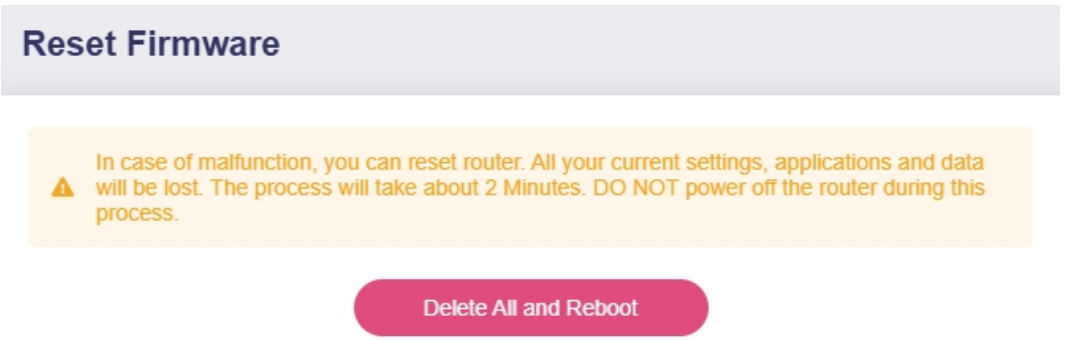
Par défaut, aucune fonction n'est attribuée au commutateur. Vous pouvez le configurer pour activer ou désactiver certaines fonctions d'un simple geste.



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.

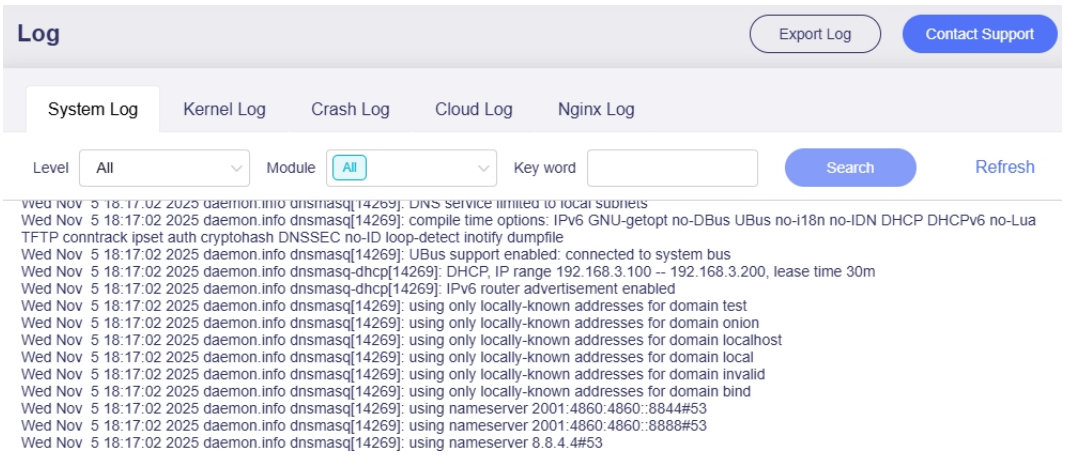


Remarque : tous vos paramètres, applications et données seront effacés. L'opération prend environ 2 minutes. N'éteignez pas le routeur pendant cette opération.

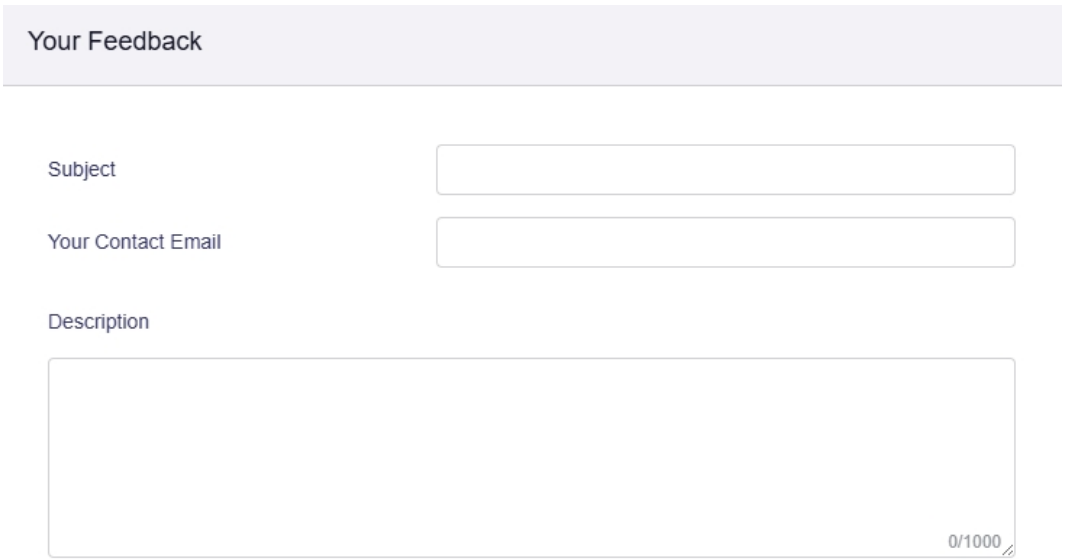
Si vous ne pouvez pas accéder à l'interface Web, utilisez le bouton physique de réinitialisation situé sur le côté du routeur.

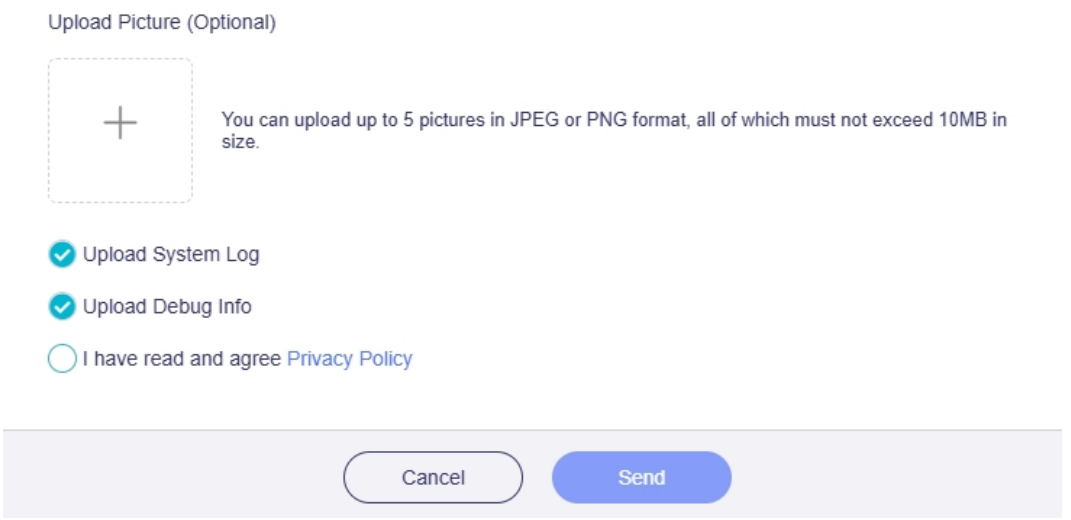
15.8 Journaux

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.



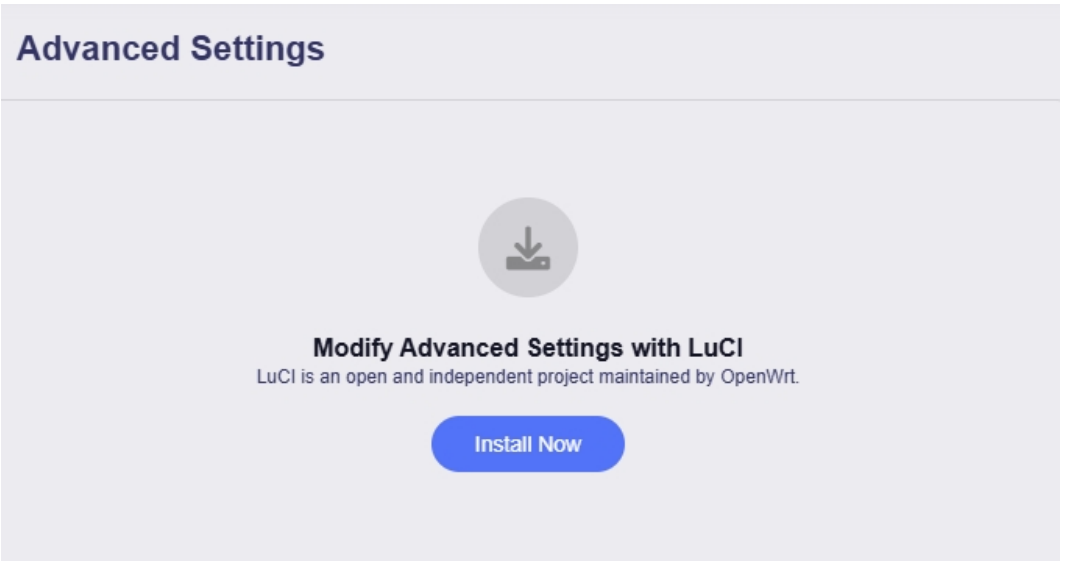

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

15.9 Paramètres avancés

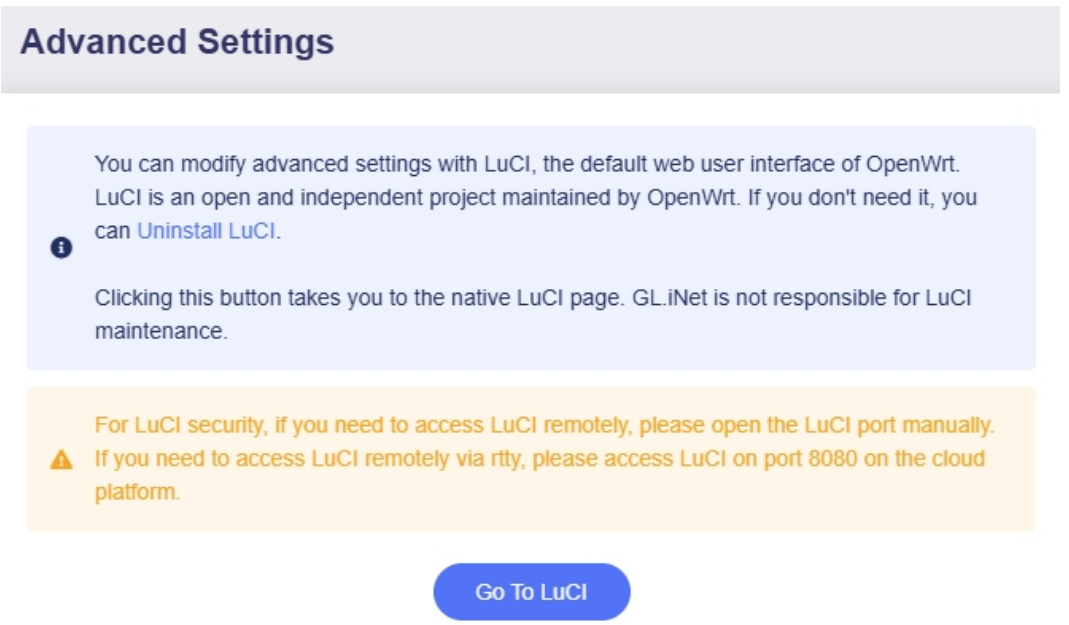
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)**. Vous pouvez y modifier les paramètres avancés dans LuCI, l'interface Web par défaut d'OpenWrt. LuCI est un projet ouvert et indépendant maintenu par OpenWrt et fourni en l'état. GL.iNet n'assure pas sa maintenance.

Pour vous connecter à LuCI, procédez comme suit.

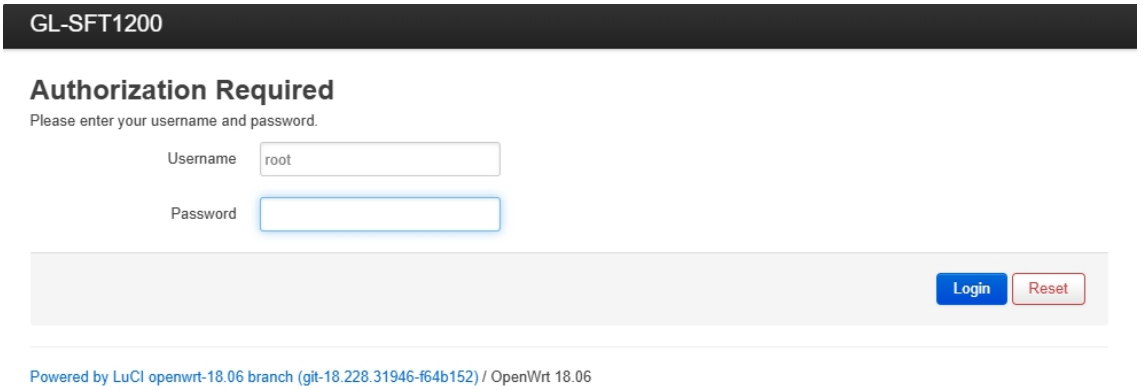
1. Cliquez sur **Installer maintenant (Install Now)** pour installer l'interface LuCI.



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.

