GL·iNet



Manuel d’utilisation

GL-MT2500 / Brume 2

Passerelle de sécurité

Version du micrologiciel 4.7.4

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 5

1.1 Présentation du produit 6

1.1.1 Aspect extérieur 6

1.1.2 Ports et boutons 7

1.1.3 LED 9

1.2 Caractéristiques techniques 9

1.3 Contenu de l'emballage 10

Chapitre 2 Branchements 11

2.1 Choix de l'emplacement 12

2.2 Branchement du routeur 12

Chapitre 3 Connexion à l'interface du routeur 13

Chapitre 4 Configuration de la connexion Internet 15

4.1 Assistant de configuration rapide 16

4.2 Configuration manuelle de la connexion Internet 17

4.2.1 Connexion à Internet par câble Ethernet 18

4.2.2 Connexion à Internet par partage de connexion USB 24

4.2.3 Connexion à Internet via un modem USB 30

Chapitre 5 Appareils clients 32

5.1 Informations sur les appareils 33

5.2 Actions 35

5.3 Suppression de clients 38

5.4 Tri 39

Chapitre 6 Services cloud 40

6.1 GoodCloud 41

6.1.1 Activation de GoodCloud 42

6.1.2 Gestion de votre routeur 45

6.1.3 Dissociation de l'appareil 50

6.1.4 Désactivation de GoodCloud 50

6.2 AstroWarp 51

Chapitre 7 Présentation du VPN 52

7.1 Introduction 53

7.2 Cas d'utilisation 54
Chapitre 8 Tableau de bord VPN 56
8.1 Client VPN 58
8.1.1 Options du client 58
8.1.2 Mode proxy 60
8.1.3 Options globales 61
8.2 Serveur VPN 64
8.2.1 Options du serveur 64
8.2.2 Règles de routage du serveur 67
8.2.3 Options globales 67
Chapitre 9 Configuration d'un serveur VPN 69
9.1 Configuration d'un serveur OpenVPN 70
9.1.1 Préparation 70
9.1.2 Étapes de configuration 71
9.1.3 Dépannage 73
9.2 Configuration d'un serveur WireGuard 74
9.2.1 Préparation 74
9.2.2 Étapes de configuration 75
9.2.3 Dépannage 78
Chapitre 10 Configuration d'un client VPN 79
10.1 Configuration d'un client OpenVPN 80
10.1.1 Préparation 80
10.1.2 Configuration de NordVPN 80
10.1.3 Configuration manuelle d'un client OpenVPN pour un autre fournisseur 86
10.2 Configuration d'un client WireGuard 89
10.2.1 Préparation 89
10.2.2 Configuration d'AzireVPN 90
10.2.3 Configuration de Hide.me 95
10.2.4 Configuration d'IPVanish 98
10.2.5 Configuration de Mullvad 103
10.2.6 Configuration de NordVPN 108
10.2.7 Configuration de PIA (Private Internet Access) 113
10.2.8 Configuration de Surfshark 118
10.2.9 Configuration manuelle d'un client WireGuard pour un autre fournisseur 123

Chapitre 11 Tor 129
Chapitre 12 Applications 131
12.1 Extensions 132
12.2 DNS dynamique 133
12.2.1 Activation du DDNS 133
12.2.2 Vérification du fonctionnement du DDNS 136
12.2.3 Accès HTTPS à distance 138
12.2.4 Accès SSH à distance 141
12.3 Stockage réseau 143
12.3.1 Branchement du stockage 143
12.3.2 Configuration de Samba 144
12.3.3 Configuration de WebDAV 147
12.3.4 Configuration de DLNA 150
12.4 AdGuard Home 151
12.5 Contrôle parental 154
12.5.1 Configuration rapide 154
12.5.2 Dépannage 163
12.6 ZeroTier 164
12.6.1 Configuration de ZeroTier 164
12.6.2 Autoriser l'accès distant au WAN 169
12.6.3 Autoriser l'accès distant au LAN 170
12.7 Tailscale 171
12.7.1 Configuration de Tailscale 171
12.7.2 Autoriser l'accès distant au WAN 175
12.7.3 Autoriser l'accès distant au LAN 175
12.7.4 Nœuds de sortie personnalisés 176
Chapitre 13 Réseau 177
13.1 Redirection de port 178
13.1.1 DMZ 178
13.1.2 Redirection de port 179
13.2 Multi-WAN 182
13.2.1 Suivi de l'état des interfaces 182
13.2.2 Mode Multi-WAN 185
13.3 LAN 187

13.3.1 Paramètres de base 187
13.3.2 Serveur DHCP 188
13.3.3 Réservation d'adresses 190
13.4 DNS 191
13.4.1 Paramètres du serveur DNS 192
13.4.2 Modification du fichier hosts 194
13.5 Gestion des ports 196
13.6 Mode réseau 197
13.7 IPv6 199
13.7.1 Mode IPv6 200
13.7.2 Méthode d'obtention du DNS 200
13.8 Passerelle transparente 201
13.9 IGMP Snooping 203
13.10 Accélération réseau 204
13.11 Paramètres NAT 206
Chapitre 14 Système 207
14.1 Vue d'ensemble 208
14.2 Mise à jour 209
14.2.1 Mise à jour en ligne 209
14.2.2 Mise à jour locale 210
14.3 Tâches planifiées 212
14.3.1 Programmation du voyant LED 212
14.3.2 Redémarrage planifié 213
14.4 Fuseau horaire 214
14.5 Journaux 215
14.6 Sécurité 217
14.6.1 Mot de passe administrateur 217
14.6.2 Contrôle d'accès 218
14.6.3 Contrôle d'accès distant 220
14.6.4 Ouverture de ports sur le routeur 221
14.7 Réinitialisation du micrologiciel 222
14.8 Paramètres avancés 223

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

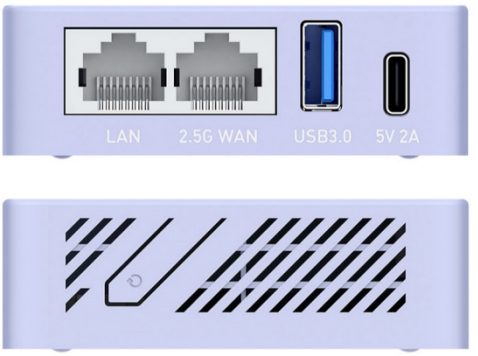
Brume 2 (GL-MT2500/GL-MT2500A) est une passerelle VPN légère et puissante fonctionnant sous OpenWrt v21.02. Son format compact permet d'héberger un serveur VPN à domicile ou de déployer un réseau SD-WAN (site à site) pour les petites et moyennes entreprises. Deux variantes sont proposées : GL-MT2500 avec un boîtier en plastique et GL-MT2500A avec un boîtier en aluminium.

1.1.1 Aspect extérieur

GL-MT2500



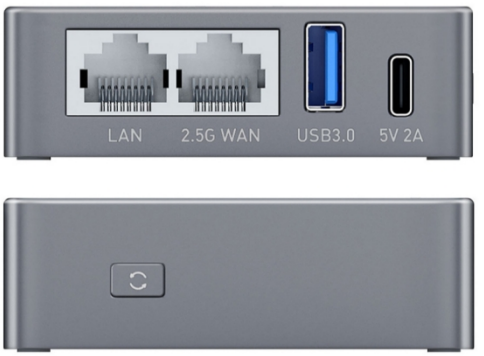
GL-MT2500



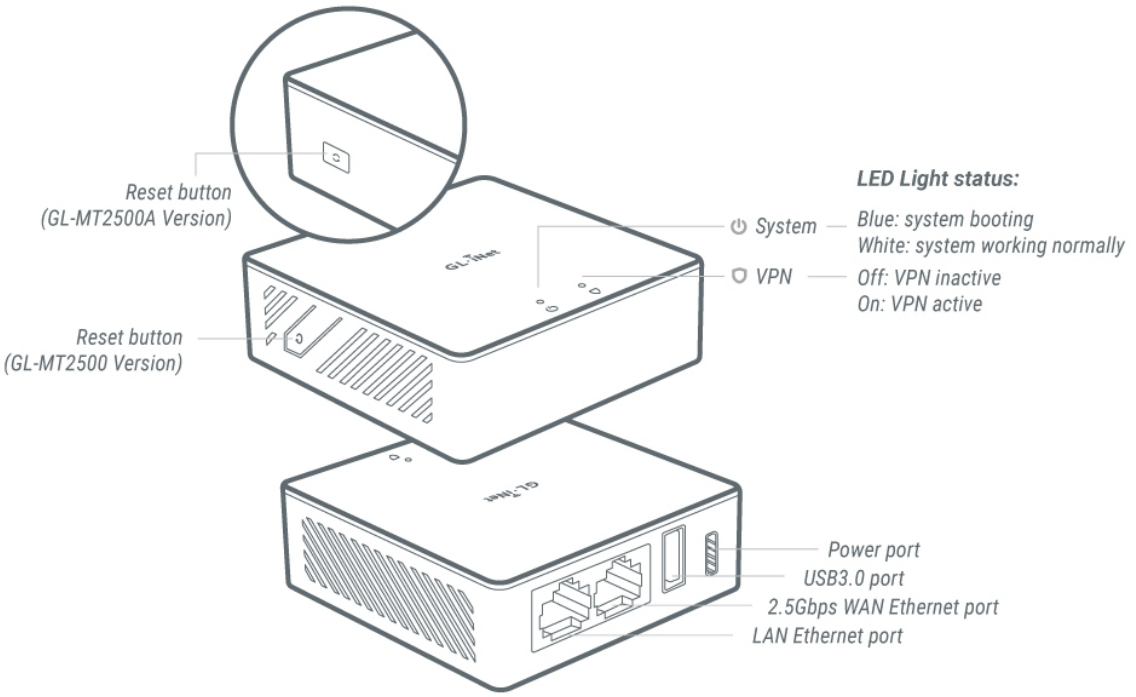
GL-MT2500A



GL-MT2500A



1.1.2 Ports et boutons



Élément	Description
Prise d'alimentation	Permet de brancher l'adaptateur secteur.
Port WAN 2,5G	Permet de relier le routeur à un modem ou à une prise Ethernet pour accéder à Internet.
Port LAN	Permet de brancher des appareils filaires si nécessaire.
Port USB 3.0	Pour les supports de stockage USB, le partage de connexion USB d'un téléphone et les clés de connexion mobile compatibles.
Bouton de réinitialisation	Maintenez le bouton enfoncé pendant **4 secondes** puis relâchez-le pour rétablir votre réseau. Le voyant système devient bleu et clignote lentement jusqu'à ce que votre réseau soit rétabli.

	Maintenez le bouton enfoncé pendant **10 secondes** puis relâchez-le pour rétablir les paramètres d'usine du routeur. Le voyant système devient bleu et clignote rapidement. Toutes les données sont effacées lorsque le voyant reste allumé en bleu.

1.1.3 LED

LED	État
Système	Bleu : démarrage du système
	Blanc : connecté à Internet
VPN	Éteint : VPN inactif
	Allumé : VPN actif

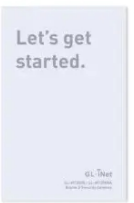
1.2 Caractéristiques techniques

Interfaces	1 port Ethernet WAN 2,5G 2 ports Ethernet LAN 2,5G 1 port USB 3.0 Type-C 1 port d'alimentation USB Type-C 1 bouton de réinitialisation
CPU	MediaTek MT7981B double cœur, à 1,3 GHz
Mémoire / Stockage	DDR4 1 Go / eMMC 8 Go
Débit Ethernet	Port WAN : 10/100/1000/2500 Mbit/s Port LAN : 10/100/1000 Mbit/s
Alimentation	Type-C, 5 V/2 A
Consommation électrique	< 2,6 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	GL-MT2500 : 70 × 70 × 22 mm / 60 g GL-MT2500A : 70 × 70 × 22 mm / 157 g
Autres ressources	Fiche technique / Micrologiciel / Application / Déballage / Tutoriels

1.3 Contenu de l’emballage

L’emballage contient :

- 1 × Brume 2 (GL-MT2500/GL-MT2500A)
- 1 manuel d’utilisation (guide de démarrage rapide)
- 1 câble Ethernet
- 1 carte de remerciement
- 1 carte de garantie
- 1 adaptateur secteur
- 1 adaptateur de prise (selon le pays de livraison)



1 x User manual



1 x Brume 2 (GL-MT2500)



1 x Ethernet cable



1 x Thank you card



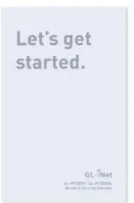
1 x Warranty card



1 x Power adapter



Converters
(Base on your shipping countries)



1 x User manual



1 x Brume 2 (GL-MT2500A)



1 x Ethernet cable



1 x Thank you card



1 x Warranty card



1 x Power adapter



Converters
(Base on your shipping countries)

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.

2.2 Branchement du routeur

1. **Mise sous tension**
   Assemblez les deux éléments de l’adaptateur secteur. Branchez-le sur votre Brume 2, puis sur une prise de courant. L’appareil démarre automatiquement.
2. **Connexion d’un appareil au routeur**
   Reliez un appareil filaire, par exemple un ordinateur de bureau ou portable, au port LAN de Brume 2 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 terminez la configuration initiale avant d’accéder à Internet.

Chapitre 3

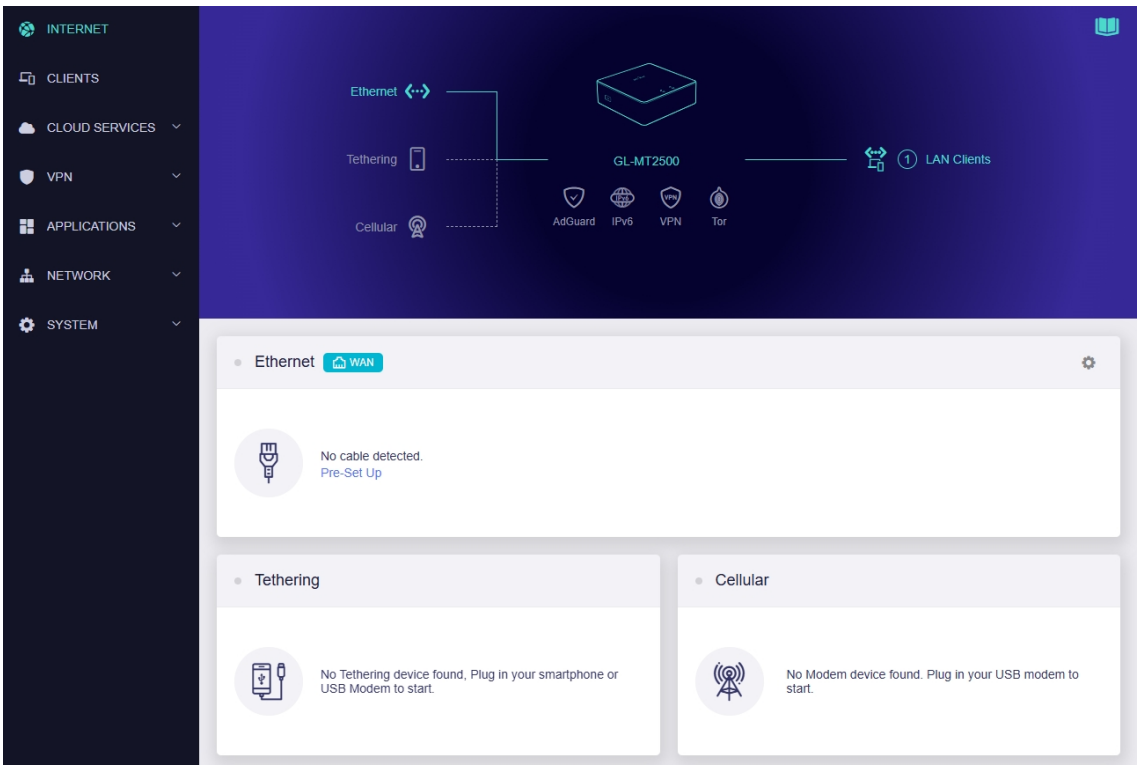
Connexion à l’interface du routeur

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.

Suivez les étapes ci-dessous pour vous connecter à l’interface d’administration Web du routeur.

1. Reliez un appareil (par exemple un ordinateur de bureau ou portable) au port LAN de Brume 2 à l’aide d’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. L’interface d’administration Web de Brume 2 s’ouvre.



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.

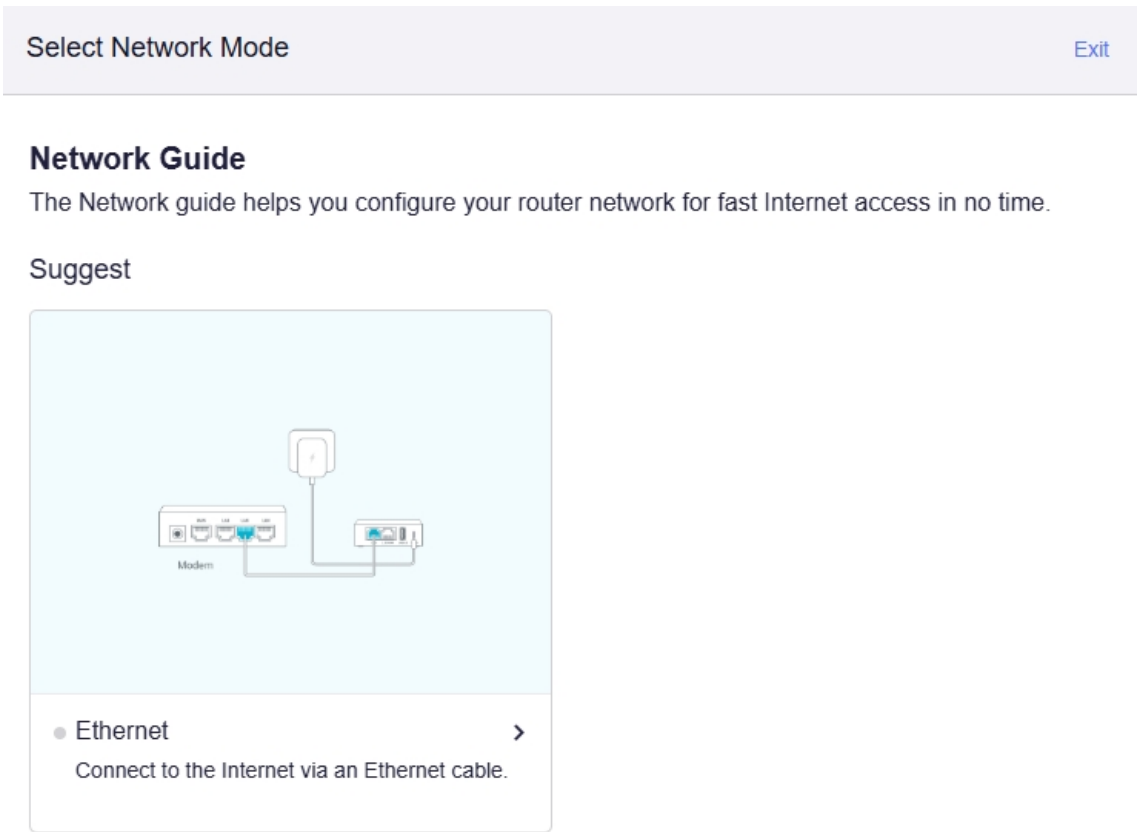
4.1 Assistant de configuration rapide

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.



4.2 Configuration manuelle de la connexion Internet

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

Brume 2 propose trois modes de connexion à Internet : Ethernet, partage de connexion USB et modem USB/réseau cellulaire. Choisissez le mode adapté 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. **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.

3. **Modem USB/réseau cellulaire (USB Modem/Cellular)** : insérez dans le routeur un modem cellulaire USB contenant une carte SIM. Le routeur se connecte alors à Internet via le réseau mobile 4G/5G, sans dépendre d’une connexion haut débit fixe. Cette solution offre une grande mobilité et convient notamment à une utilisation en véhicule ou en extérieur.

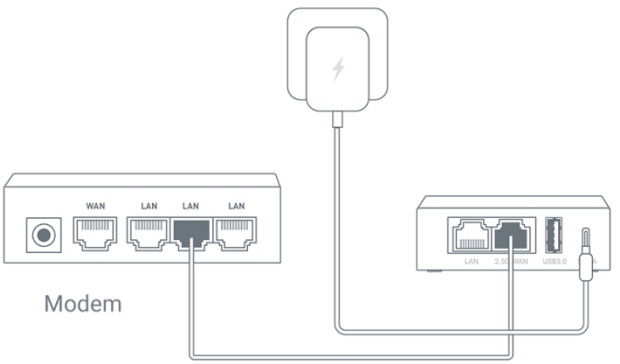
4.2.1 Connexion à Internet par câble Ethernet

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.

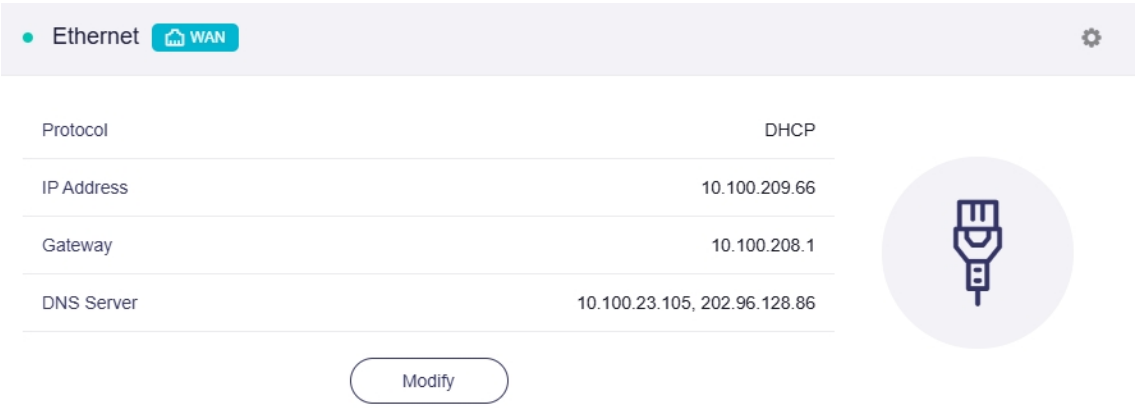
Configuration de base

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.

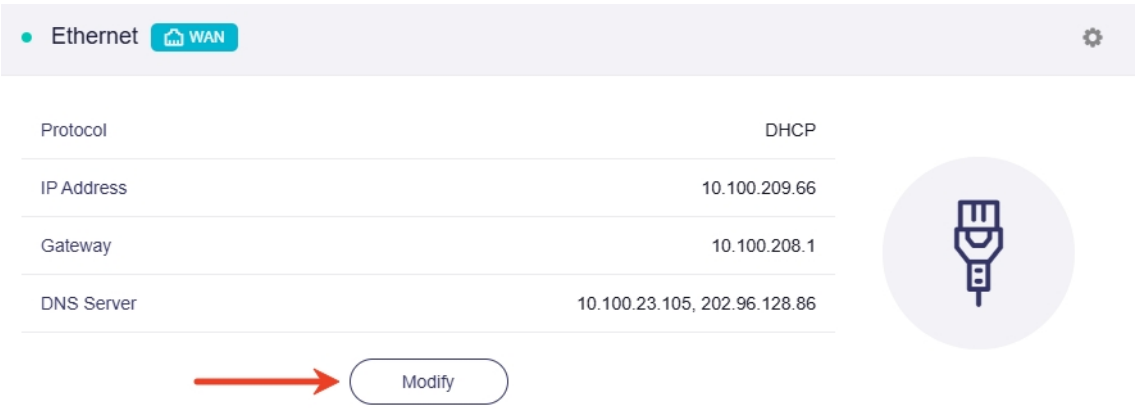


2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Ethernet**. Si la connexion est établie, la section Ethernet affiche les informations réseau, notamment le protocole, l'adresse IP, la passerelle et le serveur DNS.


Ethernet
WAN
Protocol
DHCP
IP Address
10.100.209.66
Gateway
10.100.208.1
DNS Server
10.100.23.105, 202.96.128.86
Modify

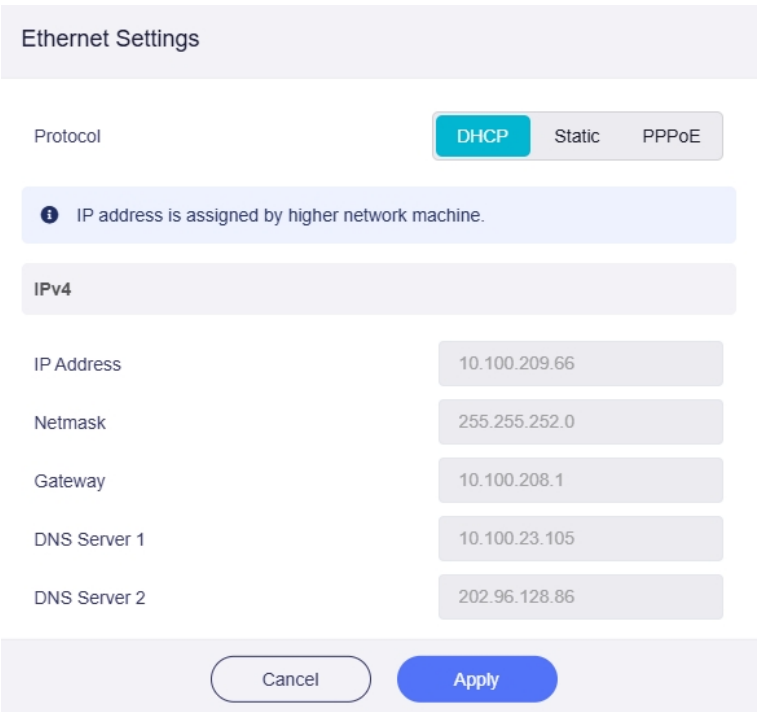
Protocoles

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



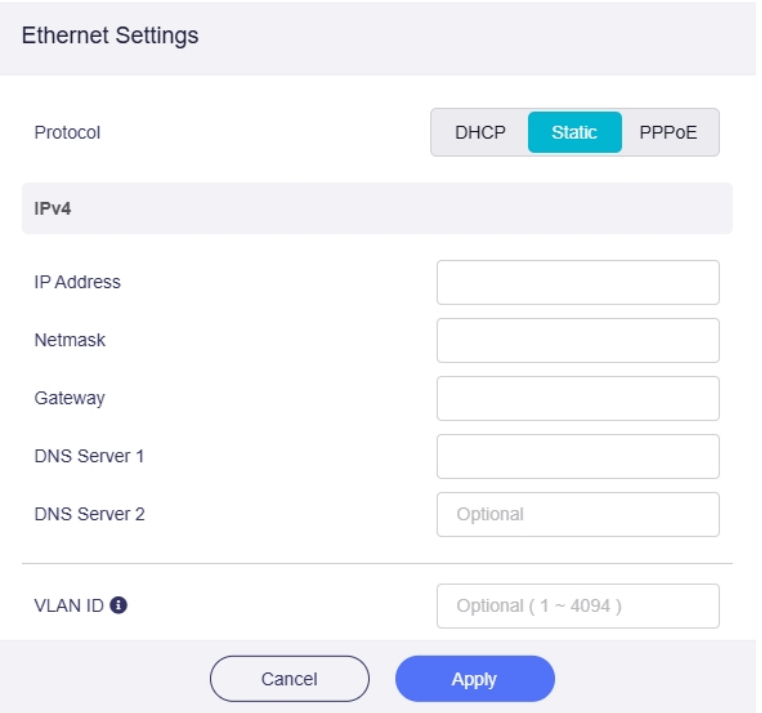
- **DHCP**

  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.



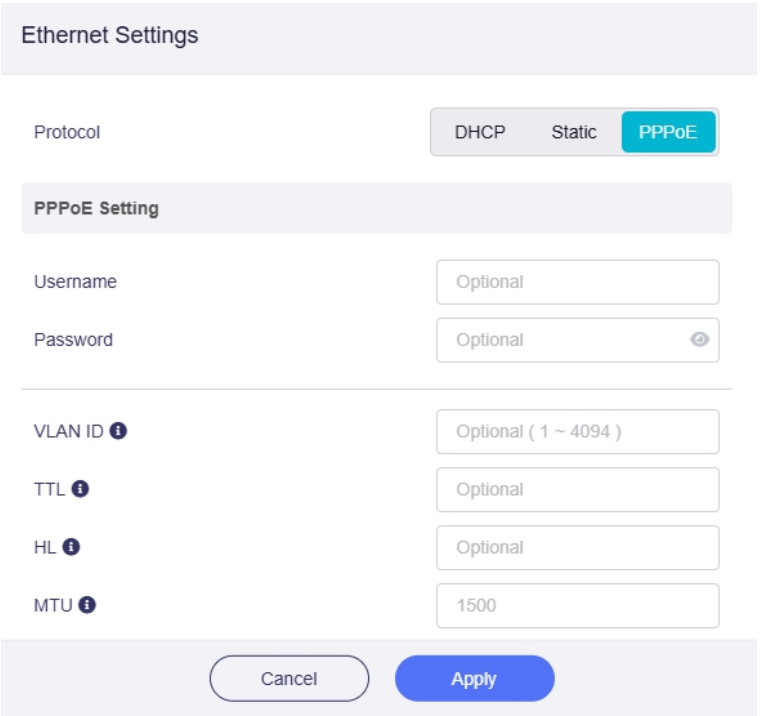
- **Statique (Static)**

  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.



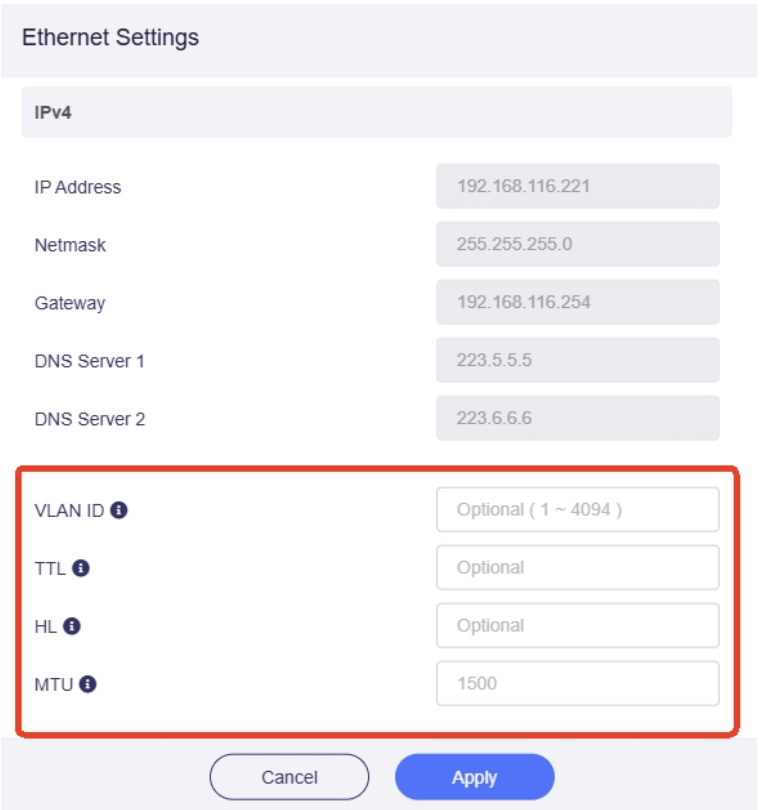
- **PPPoE**

  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

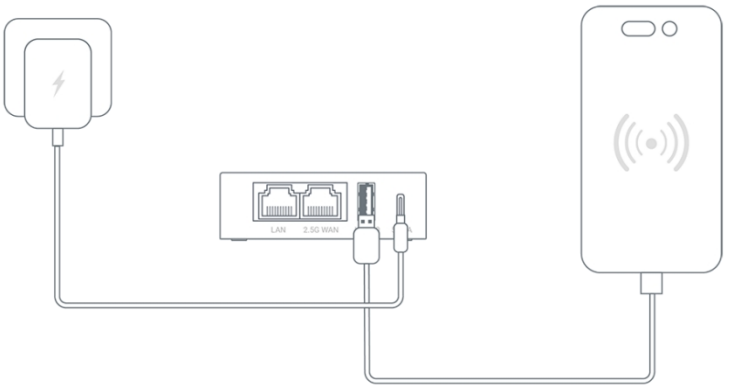
Outre les paramètres essentiels, ces trois protocoles proposent des paramètres avancés facultatifs.



- **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 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.

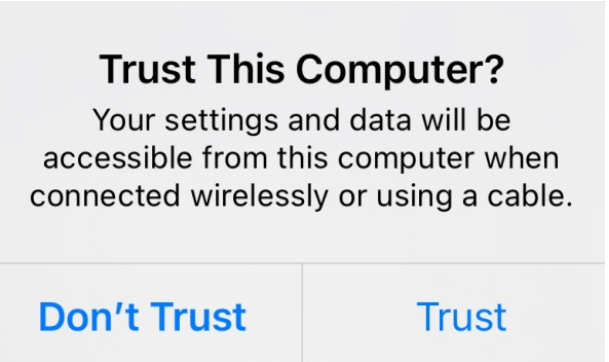


Les modems autonomes, dits « host-less », utilisent également le mode de partage de connexion USB lors de leur configuration.

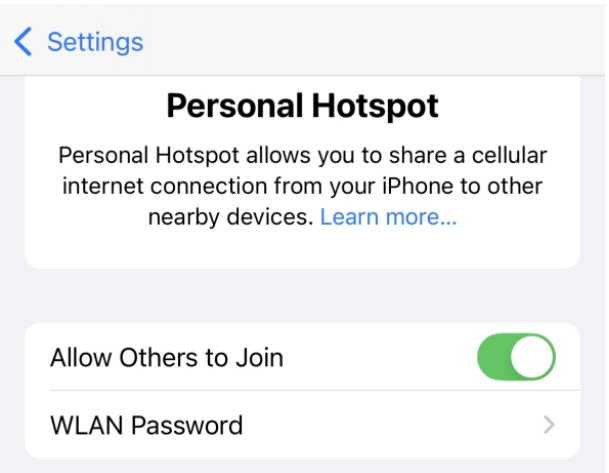
Remarque : certains opérateurs mobiles limitent le partage de connexion ou le facturent en supplément. Renseignez-vous auprès de votre opérateur.

Partage de connexion avec un iPhone

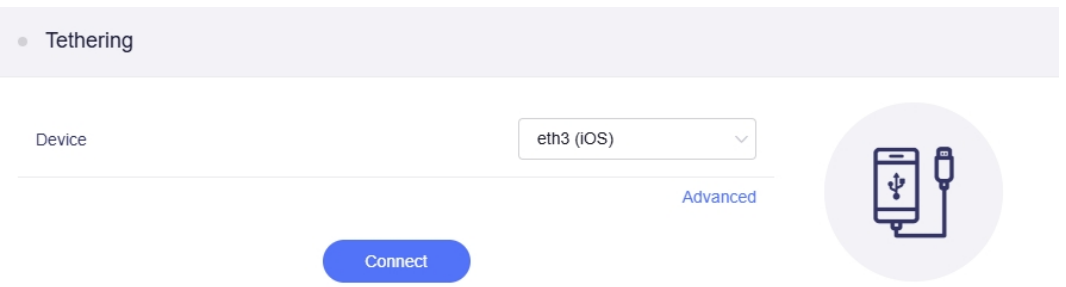
1. Reliez l'iPhone au port USB du routeur à l'aide d'un câble USB. Une boîte de dialogue vous demande si vous souhaitez faire confiance à cet appareil. Touchez **Se fier (Trust)** pour continuer.



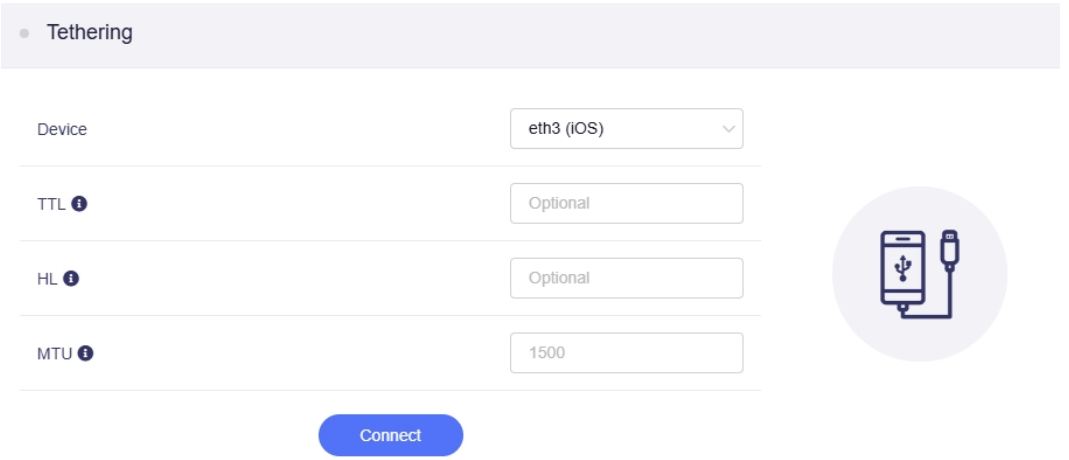
2. Sur l'iPhone, ouvrez **Réglages (Settings)** > **Partage de connexion (Personal Hotspot)**. Activez **Autoriser d'autres utilisateurs (Allow Others to Join)**.



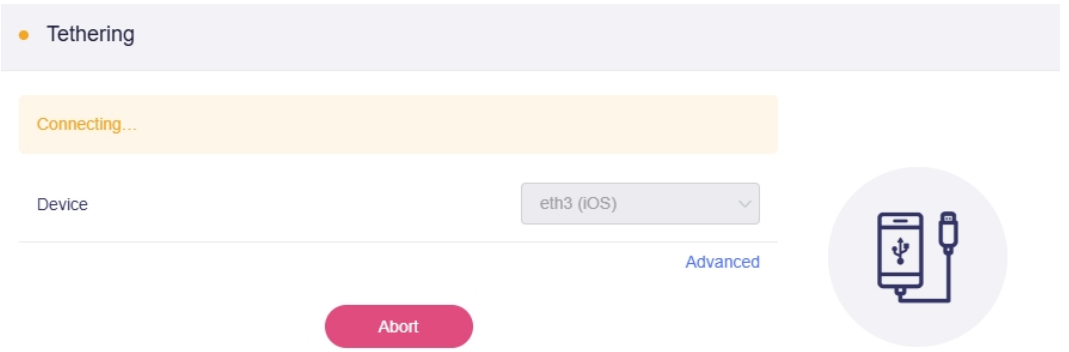
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



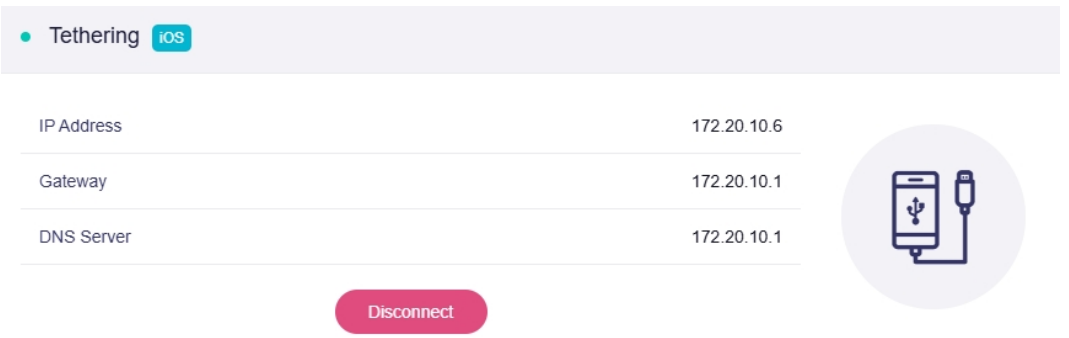
Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)** et ajustez-les avant de cliquer sur **Connecter (Connect)**.



4. La connexion démarre.

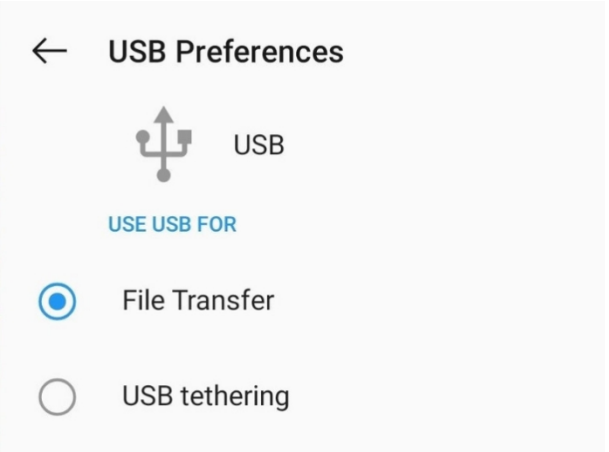


Une fois la connexion établie, cette page en affiche les détails.



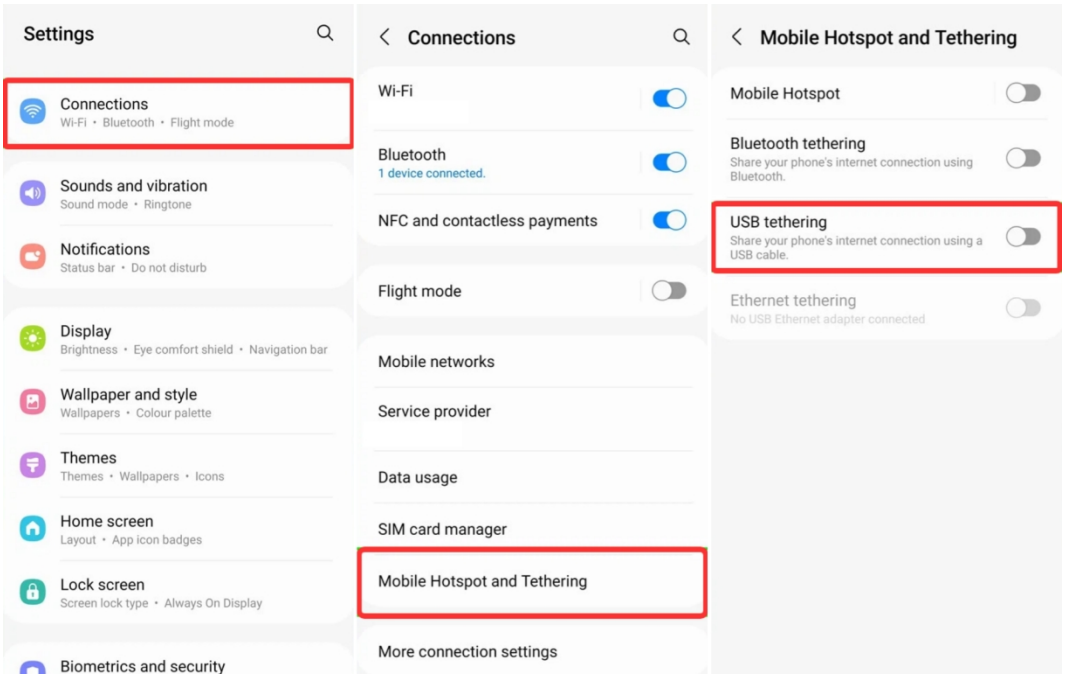
Partage de connexion avec un téléphone Android

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)**.



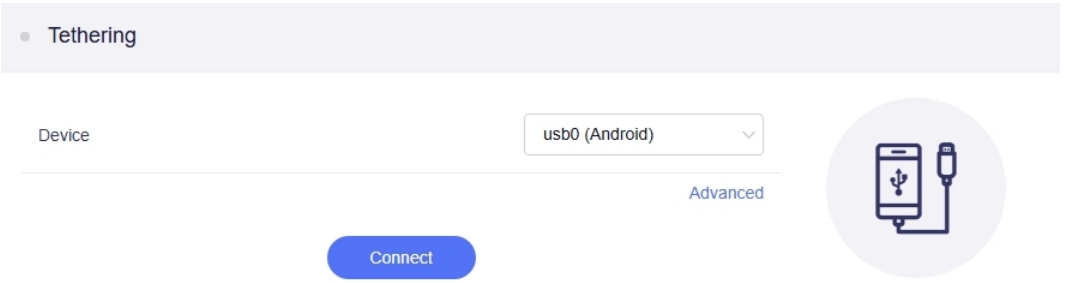
2. Sur votre téléphone, ouvrez **Paramètres (Settings)** > **Réseau et Internet (Network & Internet)** > **Point d'accès personnel (Personal Hotspot)**.

   Activez **Point d'accès personnel (Personal Hotspot)** ou **Partage de connexion USB (USB Tethering)**.

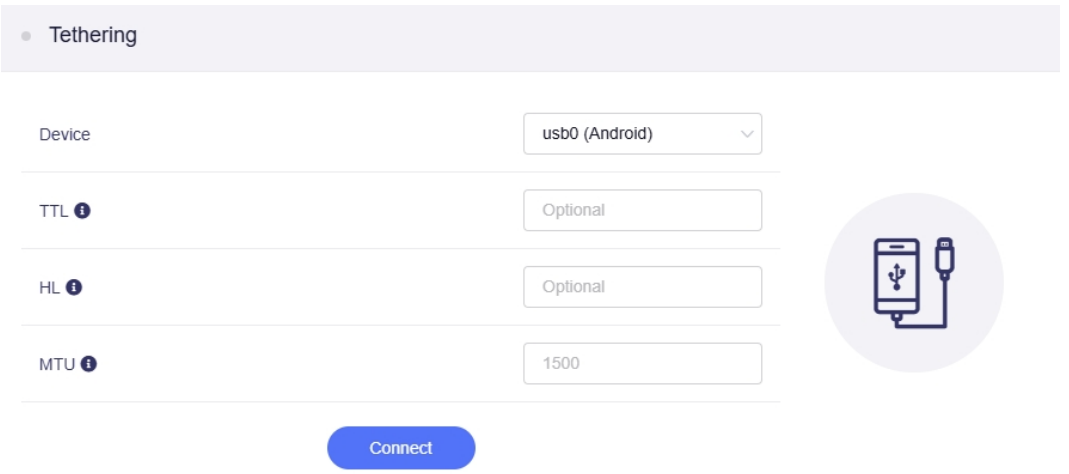


   (Les étapes d'activation du partage de connexion USB varient selon la marque. Consultez les paramètres de votre appareil pour trouver cette option et contactez l'assistance du fabricant si nécessaire.)

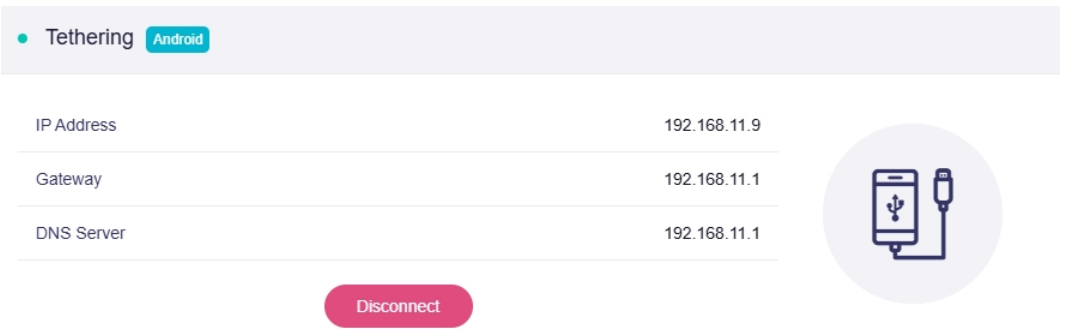
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, puis ouvrez **INTERNET** > **Partage de connexion (Tethering)**. Cliquez sur **Connecter (Connect)**.



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



4. La connexion démarre. Une fois établie, son état apparaît sur cette page.



Dépannage

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

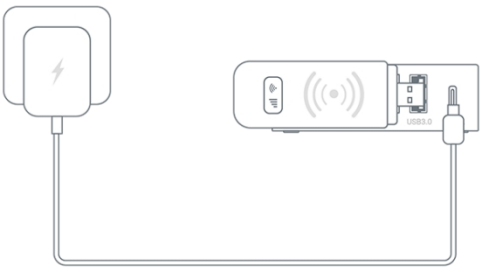
- Utilisez le bloc d'alimentation d'origine du routeur.
- Débranchez puis rebranchez le câble USB.
- Essayez un autre câble USB. Vérifiez qu'il permet le transfert de données, et pas seulement la recharge.

- 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.

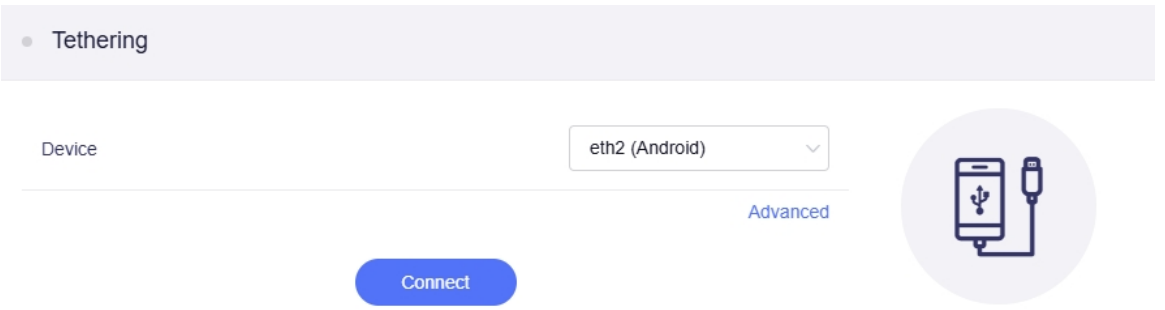
4.2.3 Connexion à Internet via un modem USB

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.

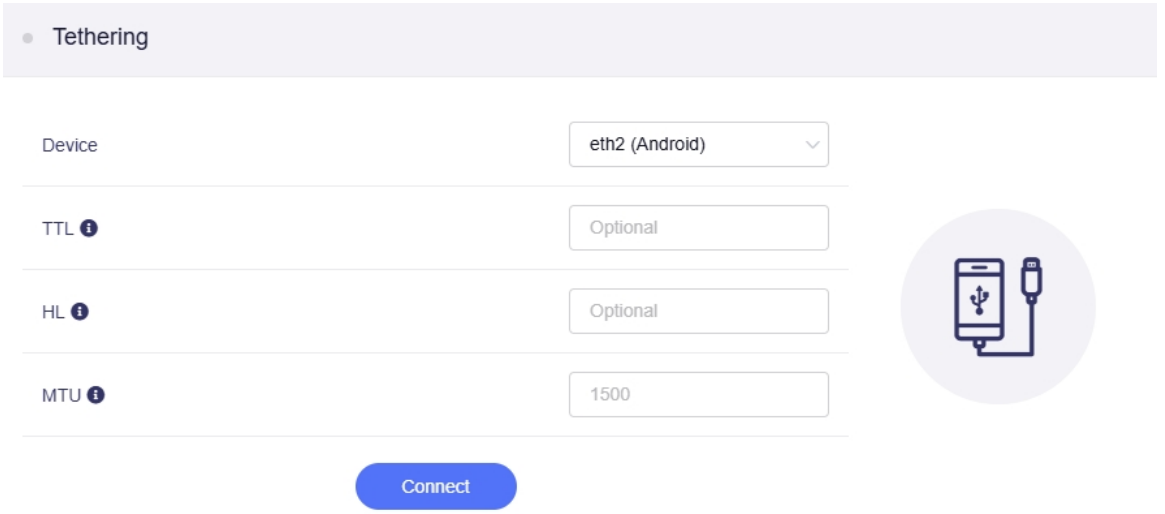


Suivez les étapes ci-dessous pour connecter le routeur à Internet via un modem USB.

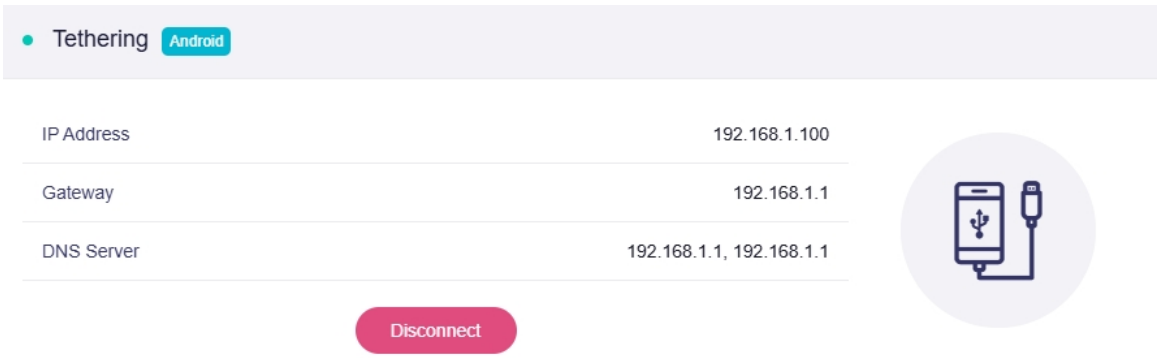
1. Avant d'allumer le routeur, branchez à son port USB un modem USB contenant une carte SIM.
2. Dans l'interface d'administration Web, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



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

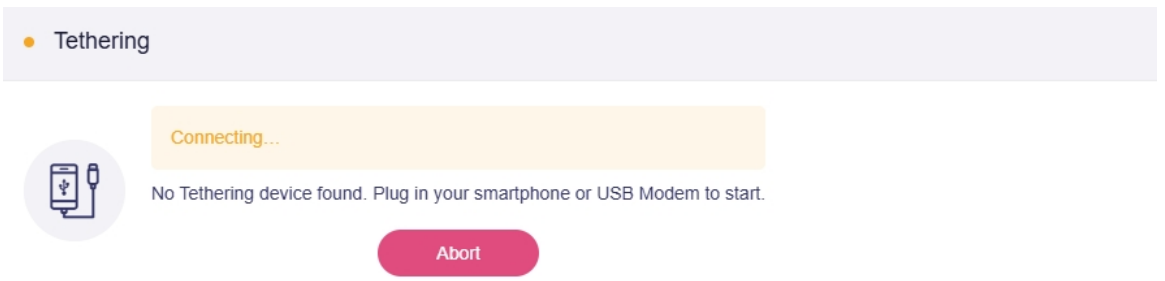


3. La connexion démarre. Une fois établie, cette page affiche les informations réseau.



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

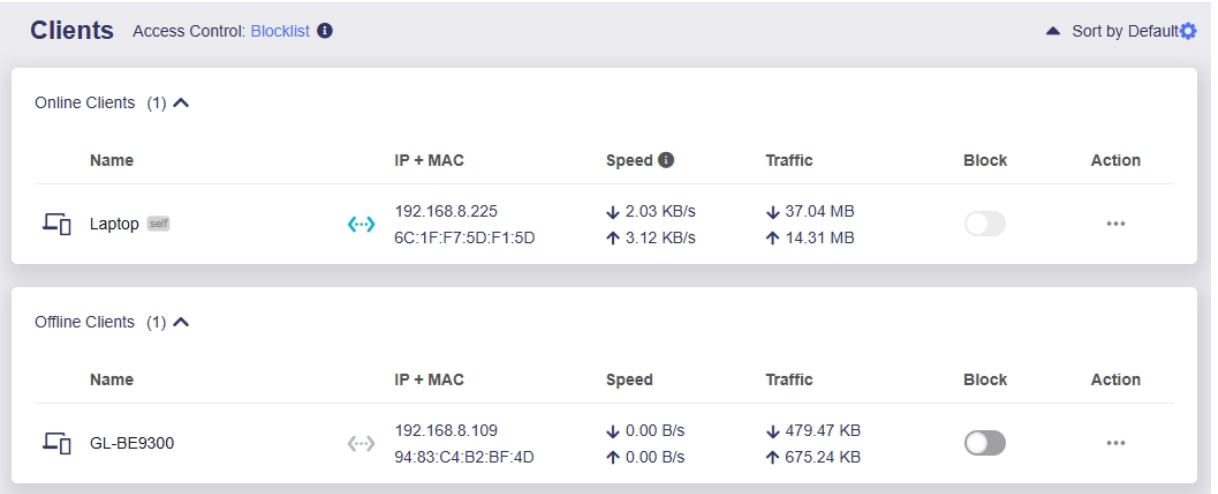
Appareils clients

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

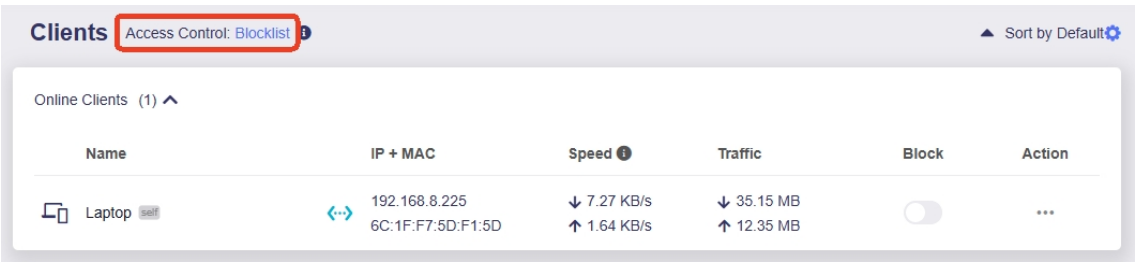
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **CLIENTS**.

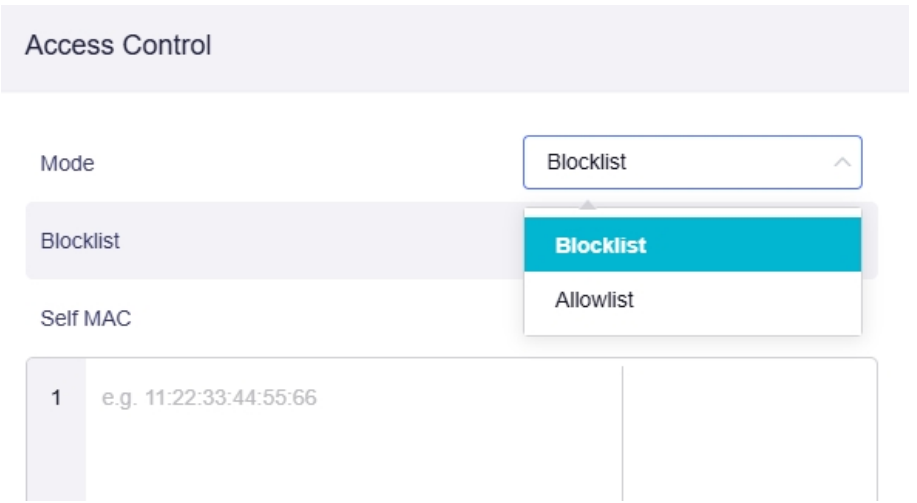
La page Clients affiche, de gauche à droite, le nom des appareils connectés, leur type de connexion, leurs adresses IP et MAC, leur débit et leur trafic. Elle permet également de réserver une adresse IP, de bloquer un client ou d'effectuer d'autres actions rapidement.

5.1 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 indique les adresses IP et MAC de l'appareil connecté.
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. **Bloquer (Block)**
   La cinquième colonne permet de bloquer un appareil connecté en un clic.
   Le contrôle d'accès utilise par défaut la liste de blocage. Vous pouvez sélectionner la liste d'autorisation en haut de la page.



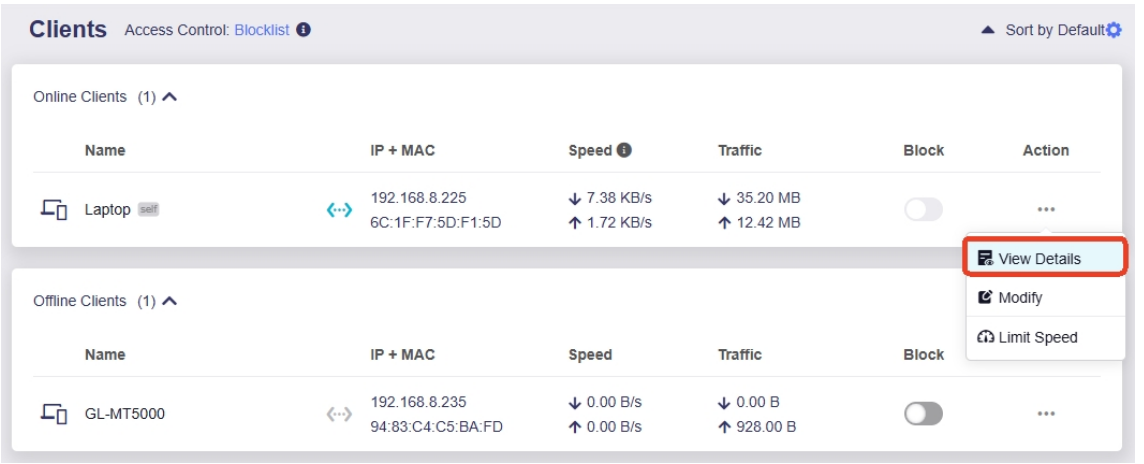


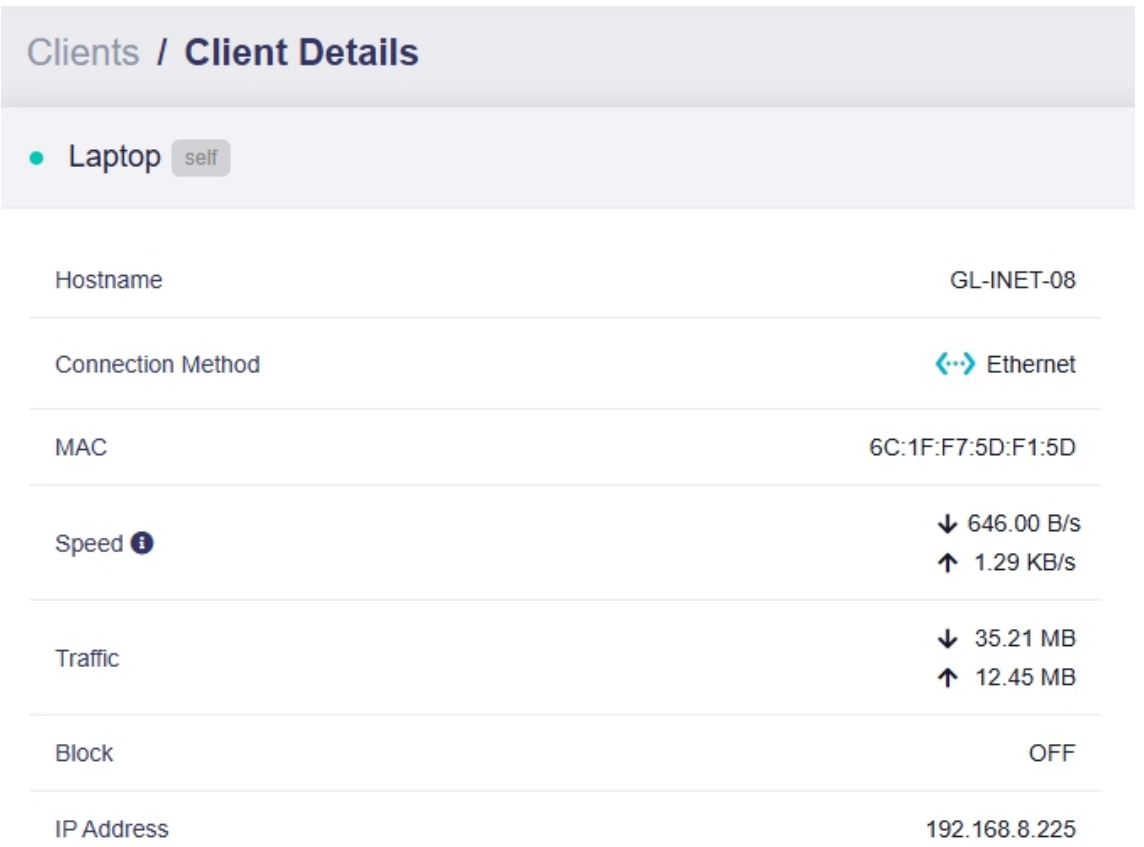
- **Liste de blocage (Blacklist)** : les appareils dont l'adresse MAC figure dans cette liste ne peuvent pas se connecter au routeur. Le blocage repose sur l'adresse MAC : un appareil bloqué peut donc se reconnecter s'il utilise une autre adresse MAC.
- **Liste d'autorisation (Allowlist)** : seuls les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

5.2 Actions

1. **Afficher les détails**

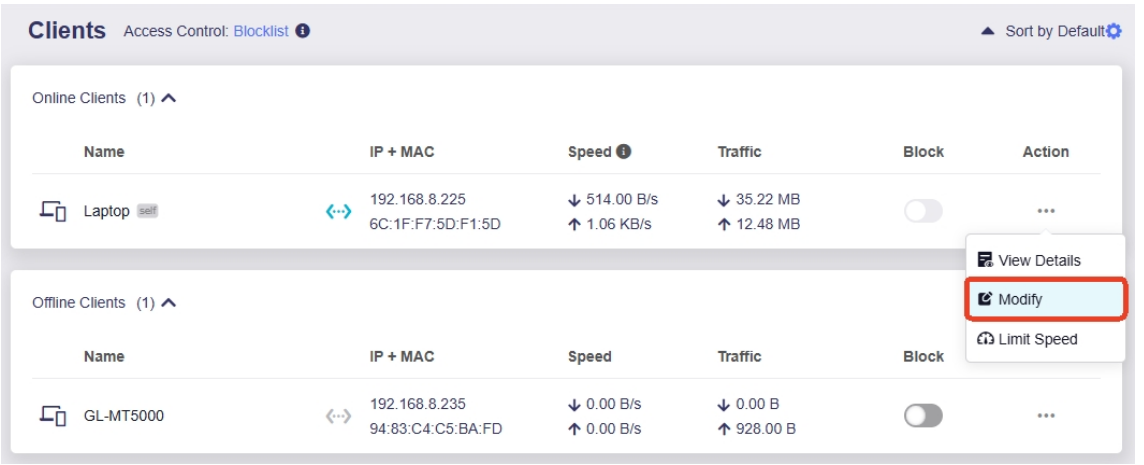
   Cliquez sur les trois points dans la colonne **Action**, puis sur **Afficher les détails (View Details)** dans le menu déroulant pour consulter les informations de l'appareil sur une seule page.

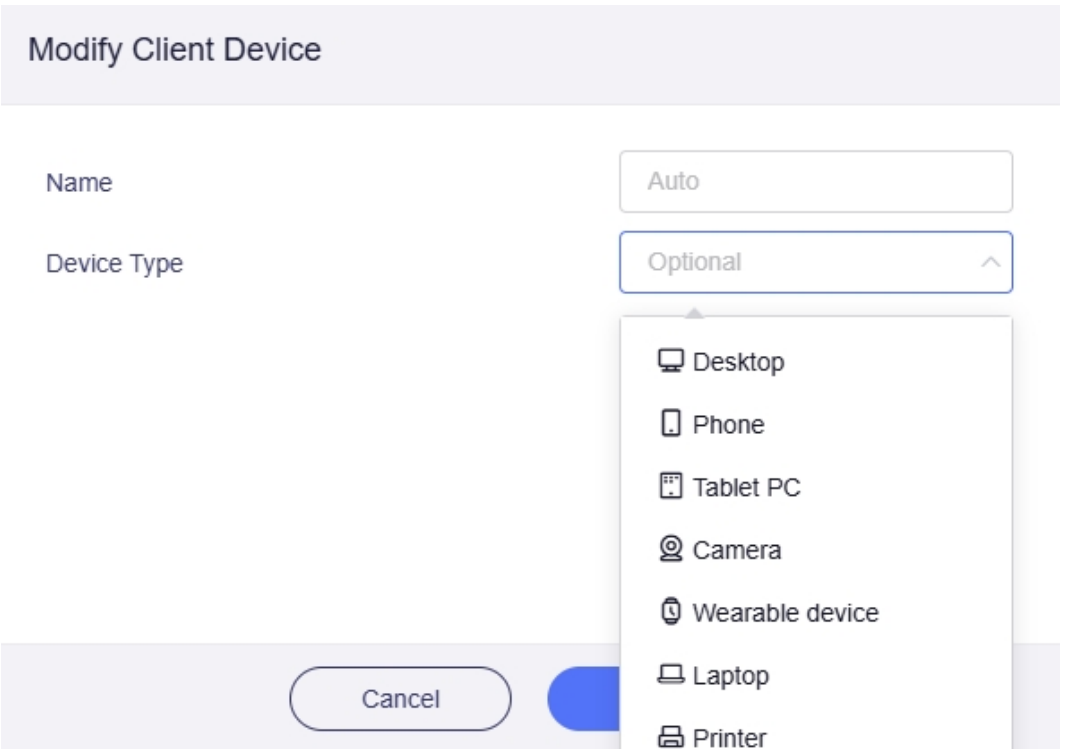




2. **Modifier**

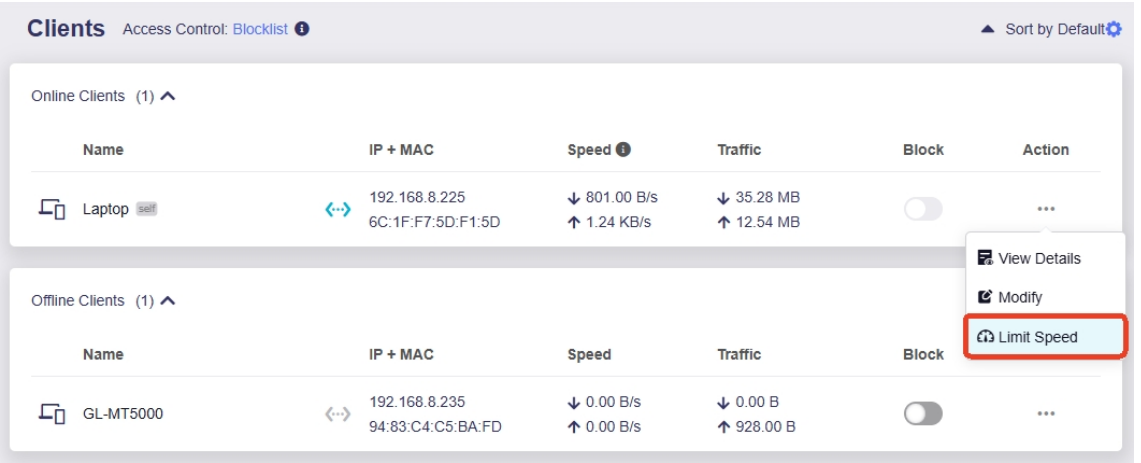
Cliquez sur les trois points dans la colonne **Action**, puis sur **Modifier (Modify)** dans le menu déroulant pour modifier le nom et le type de l'appareil.



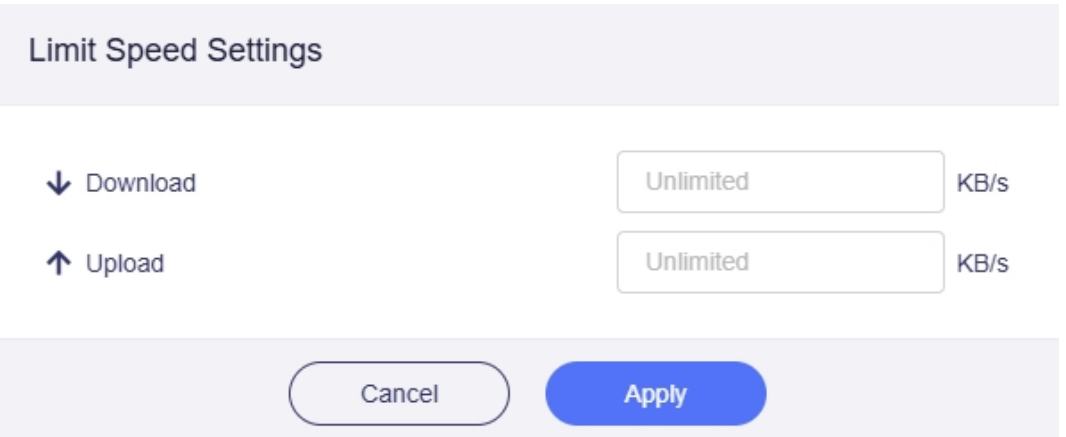


3. **Limiter le débit**

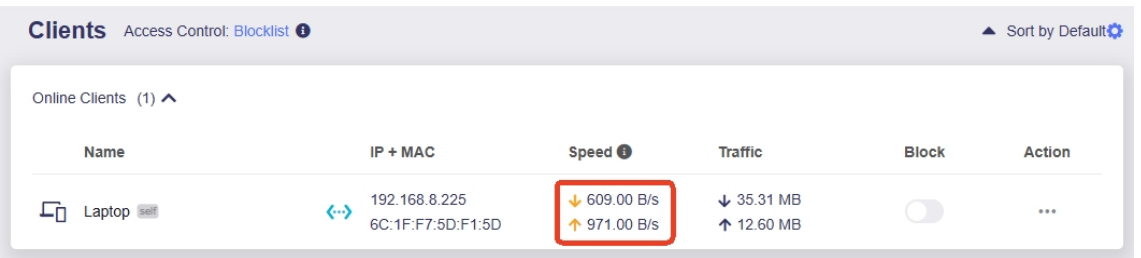
Cliquez sur les trois points dans la colonne **Action**, puis sur **Limiter le débit (Limit Speed)** dans le menu déroulant.



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



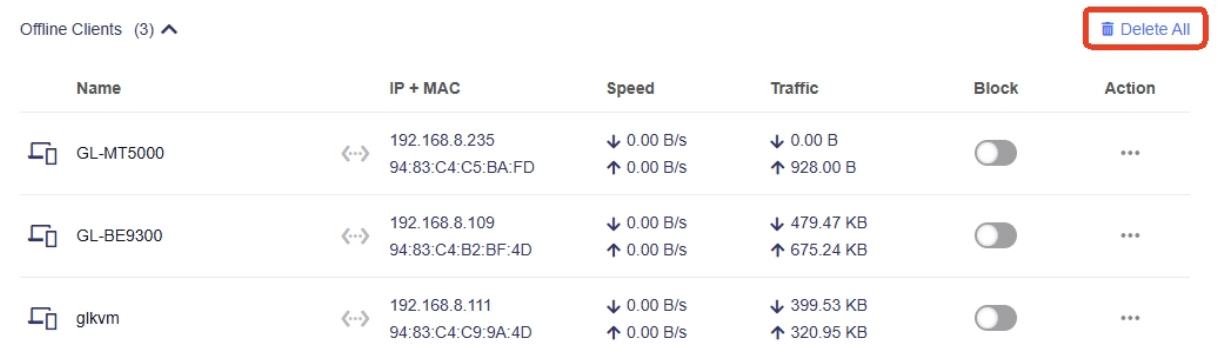
Lorsqu'une limite de débit est appliquée à un appareil, les flèches de débit montant et descendant deviennent jaunes.



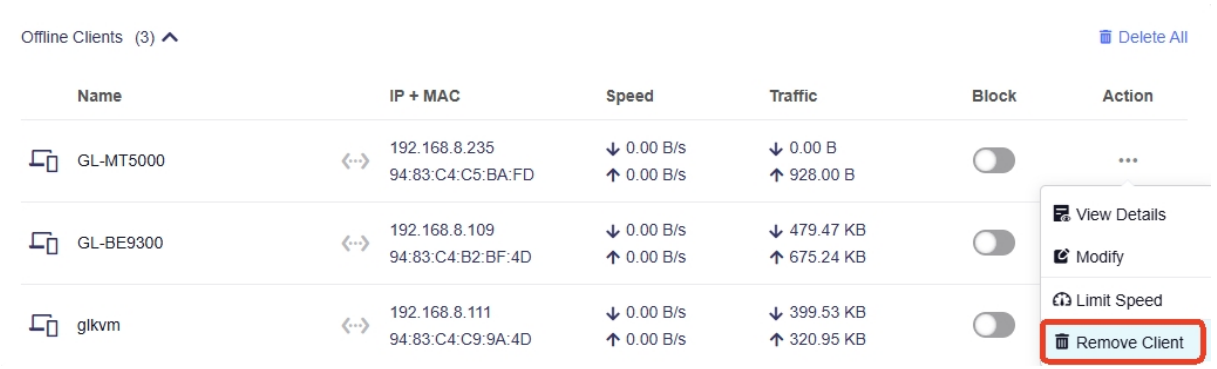
Conseil : si l'option Limiter le débit n'apparaît pas, ouvrez **RÉSEAU (NETWORK)** > **Accélération réseau (Network Acceleration)** et désactivez l'accélération. L'option Limiter le débit devient alors disponible.

5.3 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.

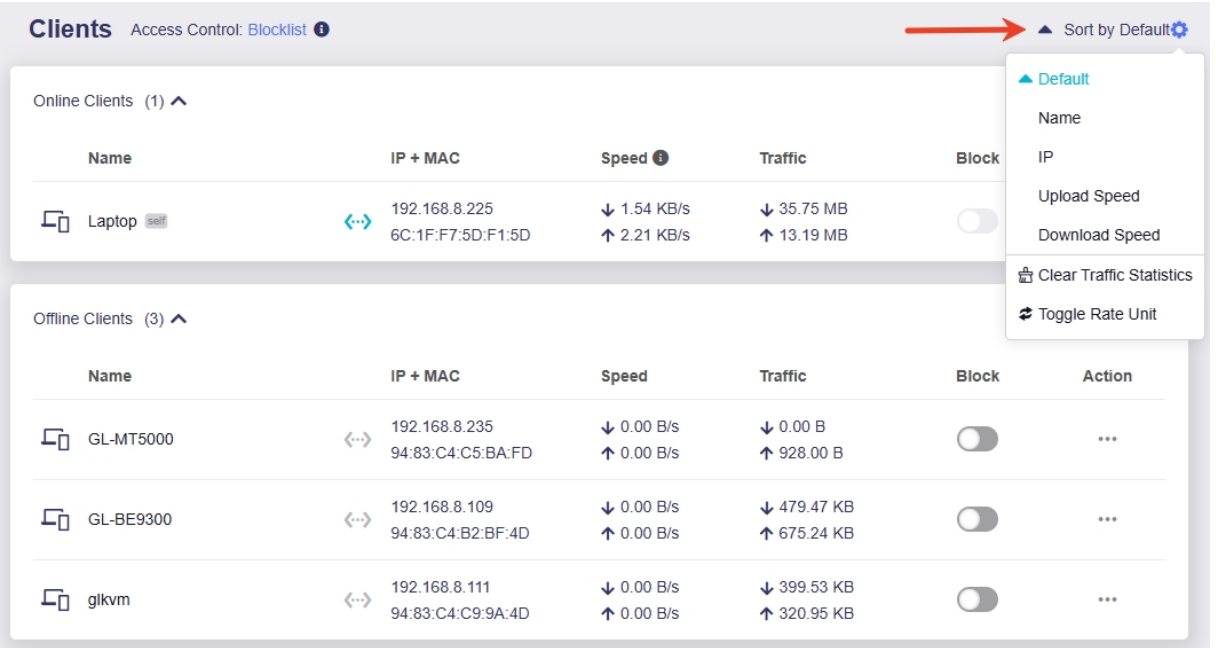


Pour supprimer un client précis, cliquez sur les trois points dans la colonne **Action**, puis sur **Supprimer le client (Remove Client)** dans le menu déroulant.



5.4 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 6

Services cloud

Ce chapitre présente deux services cloud : GoodCloud et AstroWarp.

6.1 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.

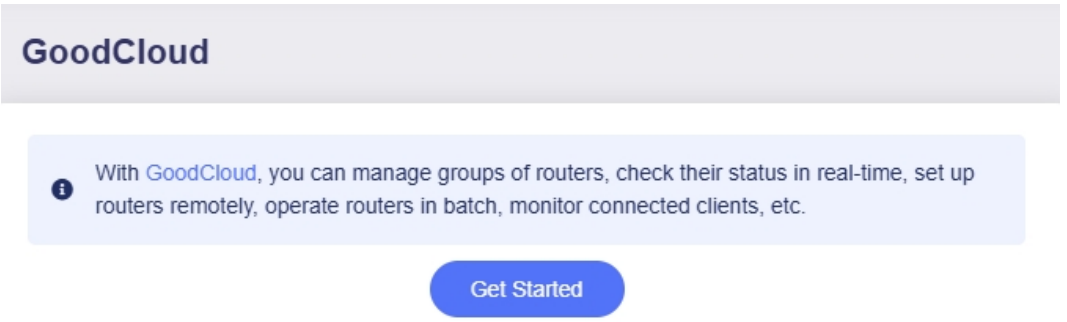
Avec GoodCloud, vous pouvez :

- 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

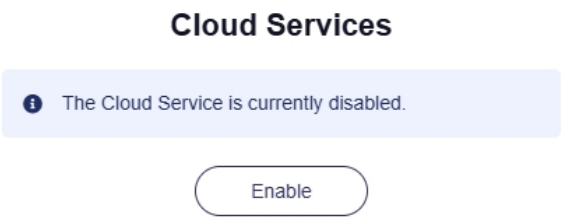
Certaines fonctions sont proposées dans les offres Enterprise et VAR (Value Added Reseller, revendeur à valeur ajoutée). Consultez cette page pour en savoir plus.

6.1.1 Activation de GoodCloud

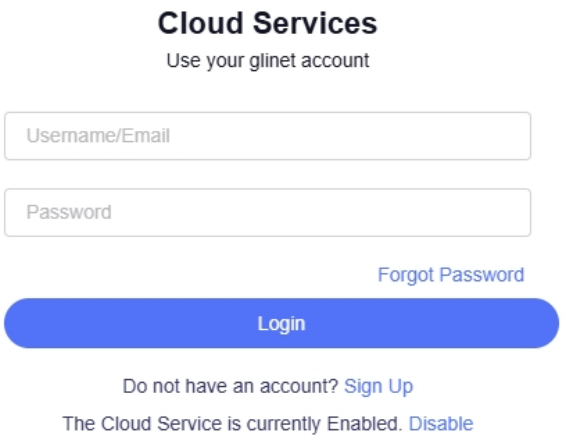
1. Connectez-vous à l'interface d'administration Web, ouvrez **SERVICE CLOUD (CLOUD SERVICE)** > **GoodCloud**, puis cliquez sur **Commencer (Get Started).**



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.

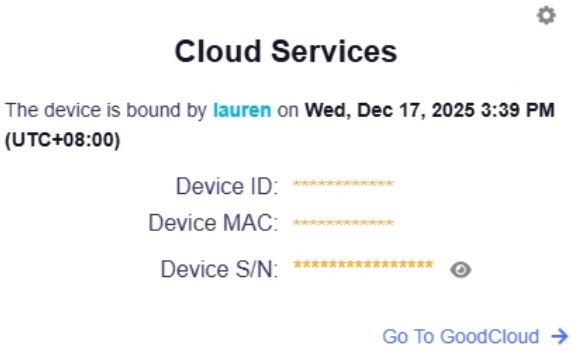


Conseils :

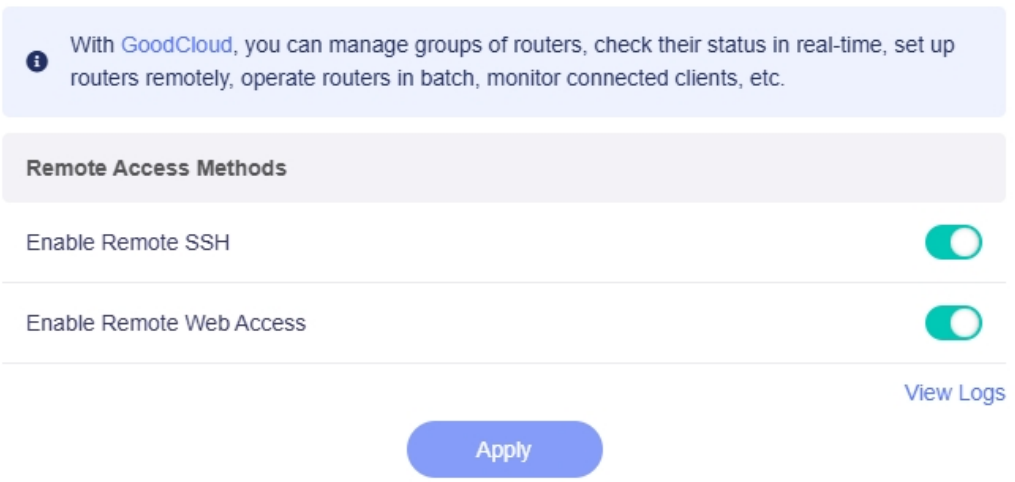
- La procédure d'association à GoodCloud varie selon la version du micrologiciel.

- 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 Web et au terminal du routeur associé. Cette fonction facilite l'administration, la configuration du réseau et le dépannage à distance. Vous pouvez activer ou désactiver ici l'accès distant au routeur.



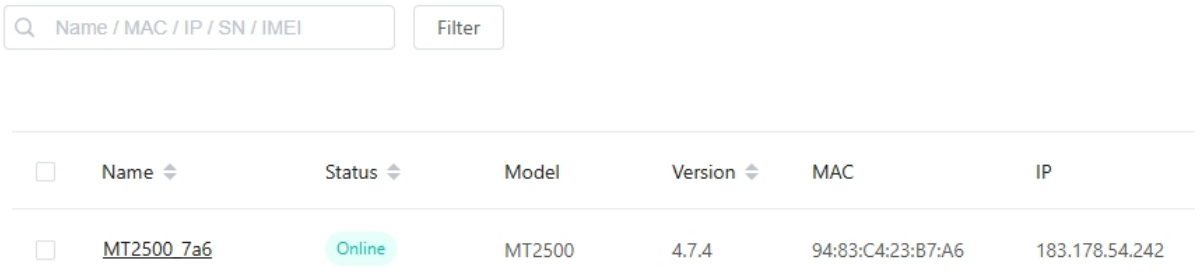
- **SSH à distance (Remote SSH)** : accédez au terminal du routeur depuis GoodCloud via SSH.
- **Accès Web à distance (Remote Web Access)** : accédez à l'interface d'administration Web du routeur depuis GoodCloud via HTTP ou HTTPS.

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

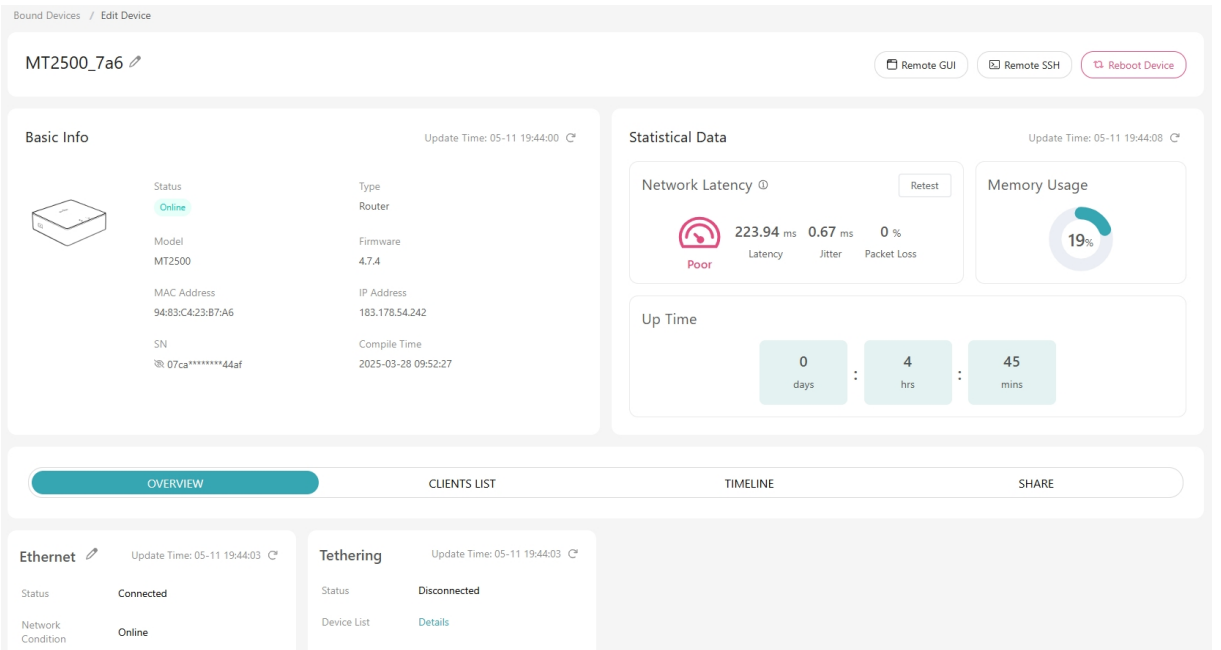
6.1.2 Gestion de votre routeur

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.

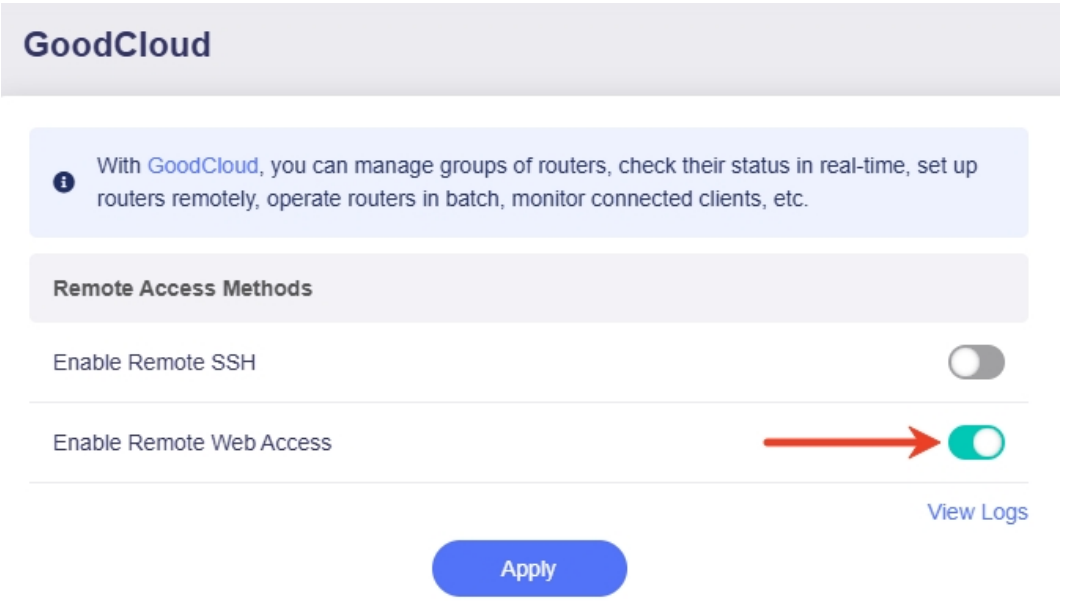


Cliquez sur le nom de l’appareil pour ouvrir sa page de détails. Elle présente les informations de base, les statistiques, la vue d’ensemble du réseau, la liste des clients et la chronologie. Vous pouvez également effectuer des opérations avancées, comme accéder au routeur à distance ou le redémarrer.

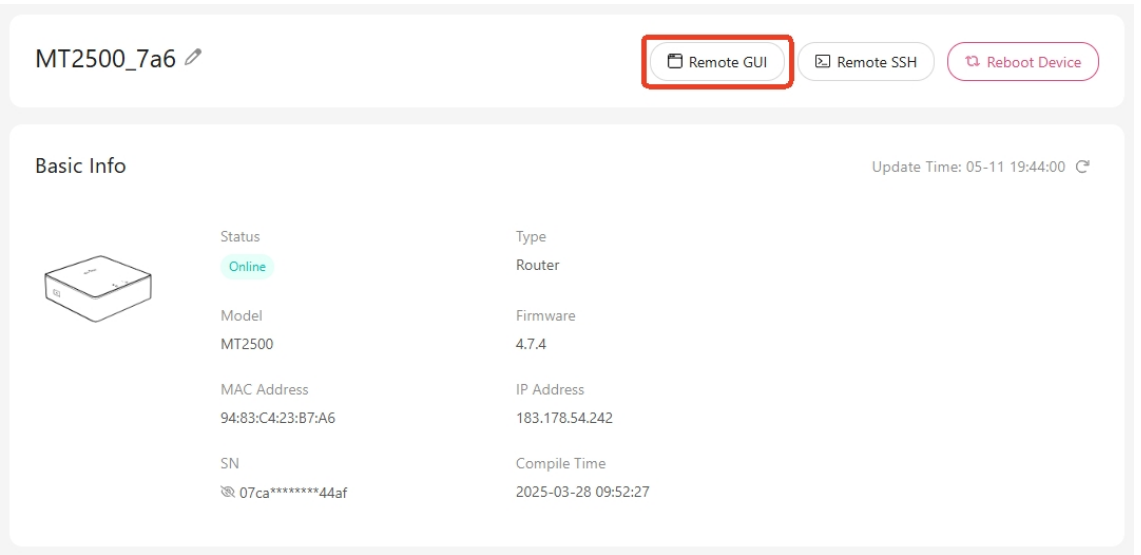


Accès distant à l’interface Web

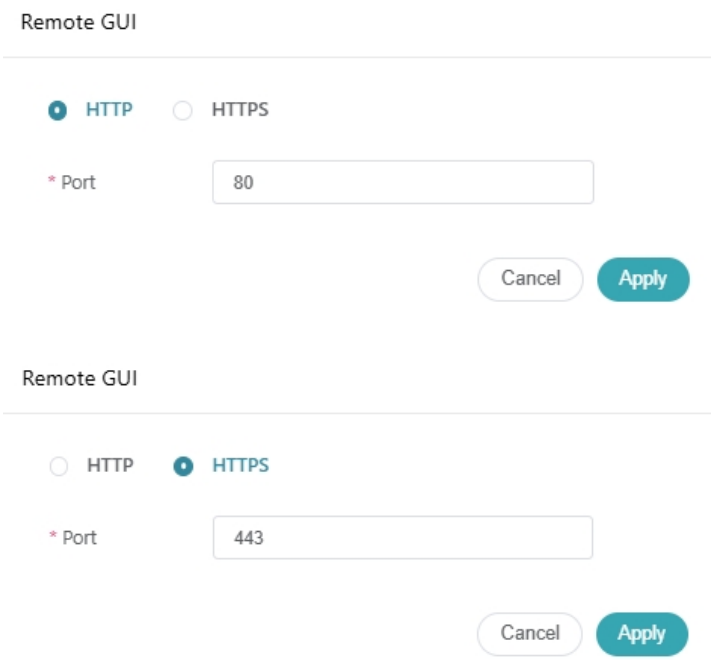
1. Dans l’interface d’administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud**, activez **Accès Web à distance (Remote Web Access)**, puis cliquez sur **Appliquer (Apply)**.



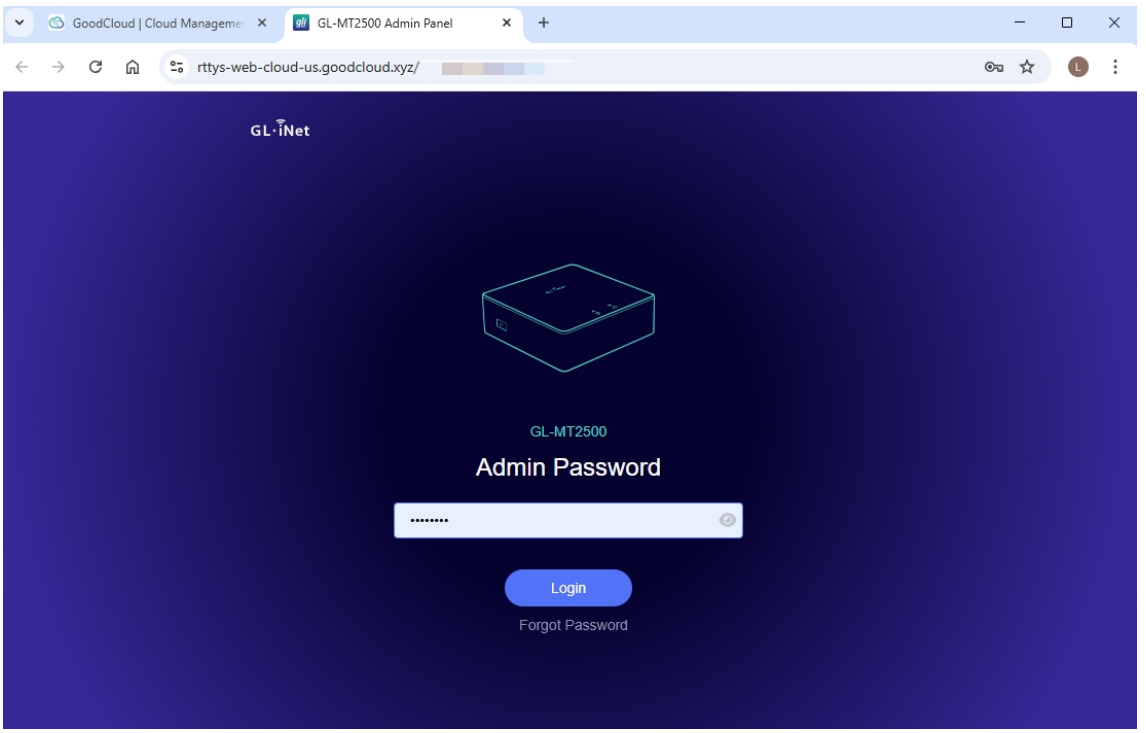
2. Connectez-vous à GoodCloud et ouvrez **Appareil (Device)** > **Appareils associés (Bound Devices)**. Cliquez sur l’appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
3. Sur cette page, cliquez sur le bouton **Interface à distance (Remote GUI)** dans l’angle supérieur droit.



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)**.

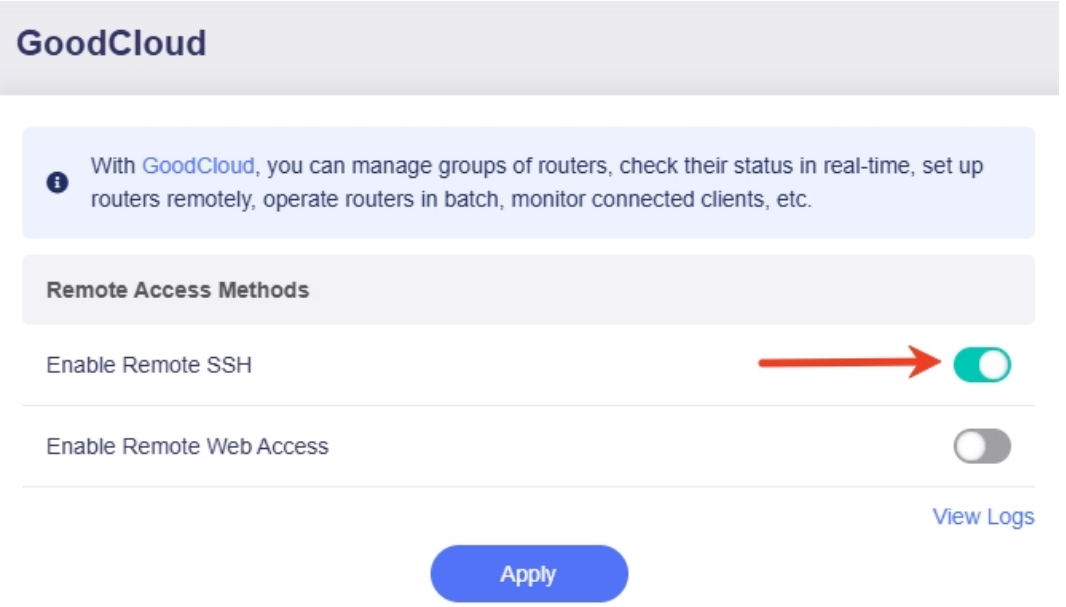


5. La page de connexion du routeur s’ouvre. Saisissez le mot de passe administrateur pour accéder à distance à l’interface d’administration Web.

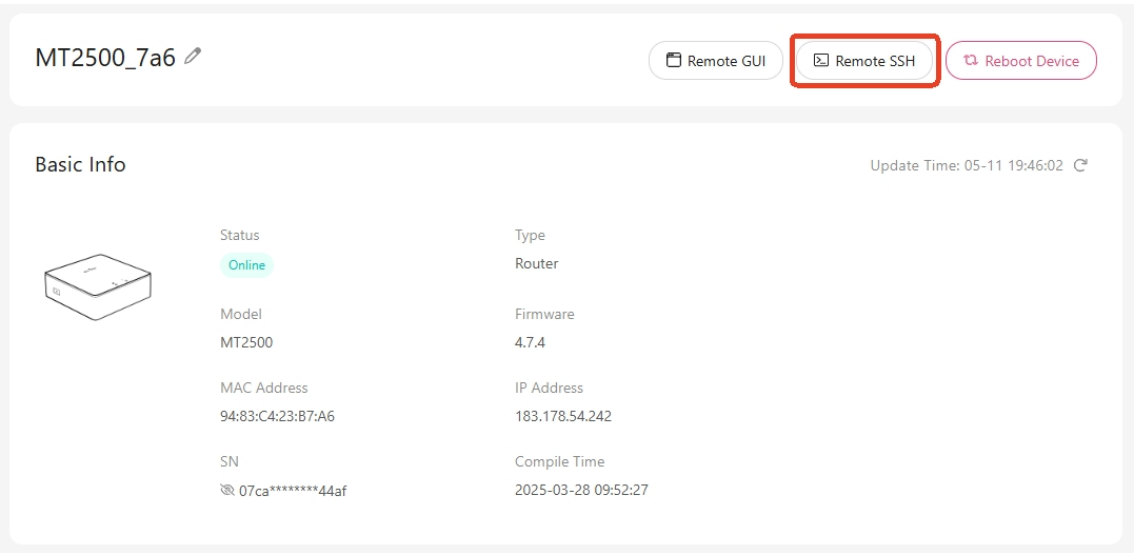


Accès distant au terminal

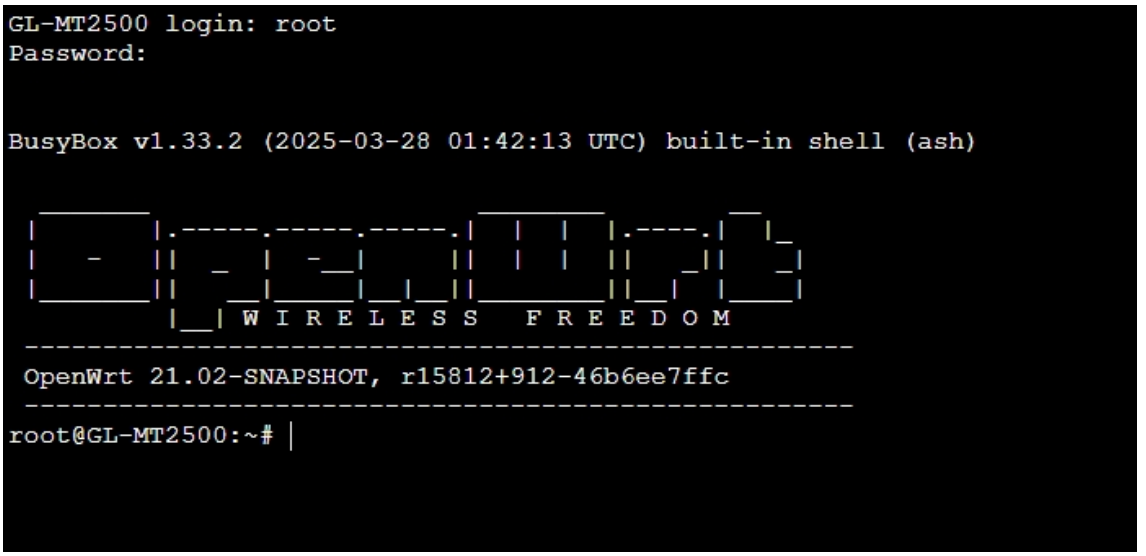
1. Dans l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodCloud**, activez **SSH à distance (Remote SSH)**, puis cliquez sur **Appliquer (Apply)**.



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.

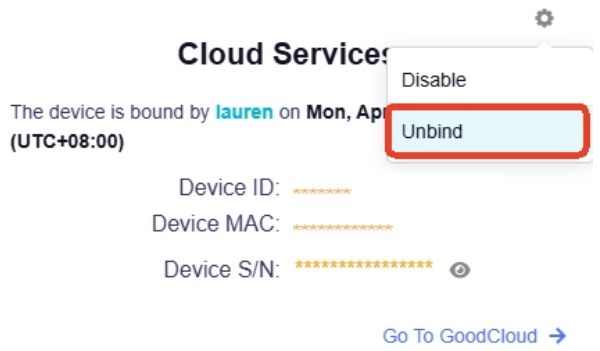


4. Connectez-vous avec l’identifiant **root** et saisissez le mot de passe pour accéder au terminal du routeur.

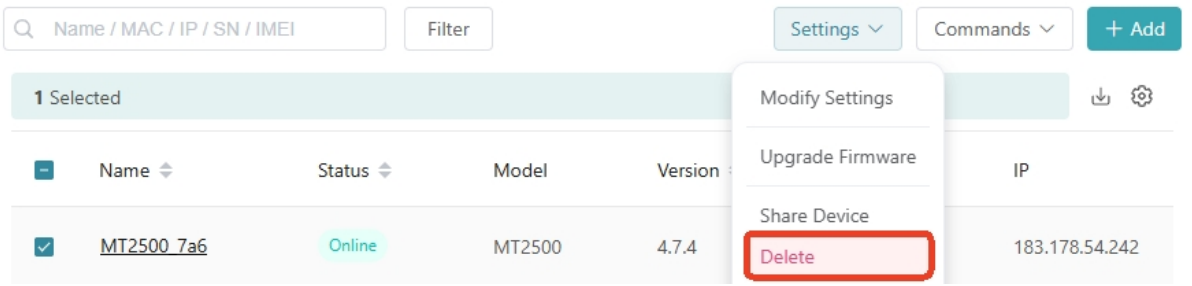


6.1.3 Dissociation de l’appareil

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.

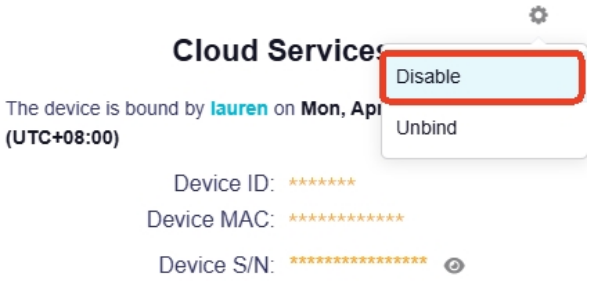


Vous pouvez également vous connecter à la plateforme Cloud et ouvrir **Appareil (Device)** > **Appareils associés (Bound Devices)**. Sélectionnez l’appareil à dissocier, cliquez sur **Paramètres (Settings)** dans l’angle supérieur droit, puis sélectionnez **Supprimer (Delete)**. L’appareil est alors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



6.1.4 Désactivation de GoodCloud

Pour déconnecter l’appareil du cloud, cliquez sur l’icône du cloud en haut à droite. Dans le menu déroulant, cliquez sur l’engrenage et sélectionnez **Désactiver (Disable)**. Le service cloud est alors désactivé.



6.2 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 7

Présentation du VPN

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

7.1 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.

7.2 Cas d’utilisation

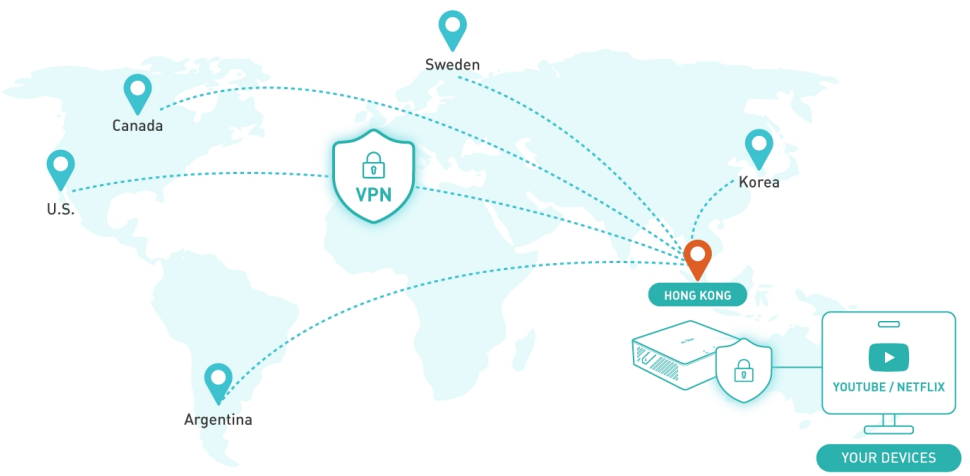
1. **Protection des données personnelles**

   Le service VPN de ce routeur fonctionne avec de nombreux appareils filaires : ordinateurs de bureau et portables, consoles de jeux, téléviseurs connectés et appareils de streaming. Toutes les données transmises par connexion filaire sont protégées par le VPN. Vous pouvez également personnaliser les règles VPN pour adapter la protection à certains appareils.



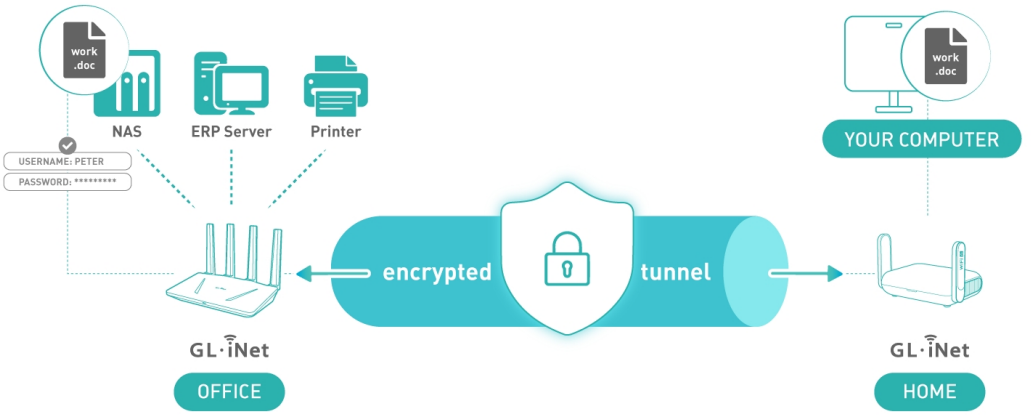
2. **Accès aux contenus depuis le monde entier**

   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.



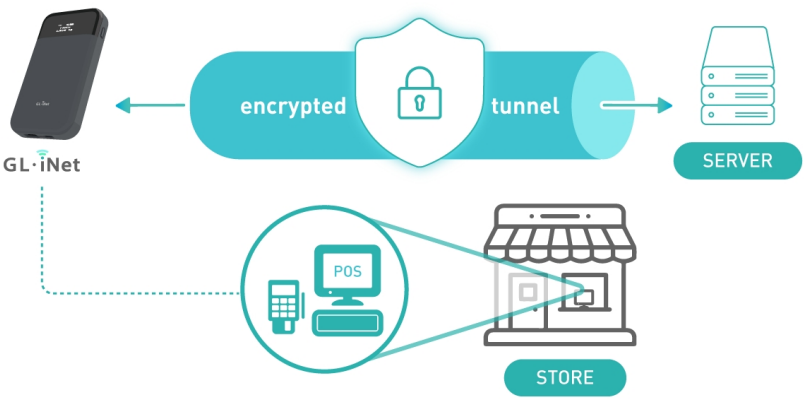
3. **Sécurité des données des petites entreprises**

   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 8

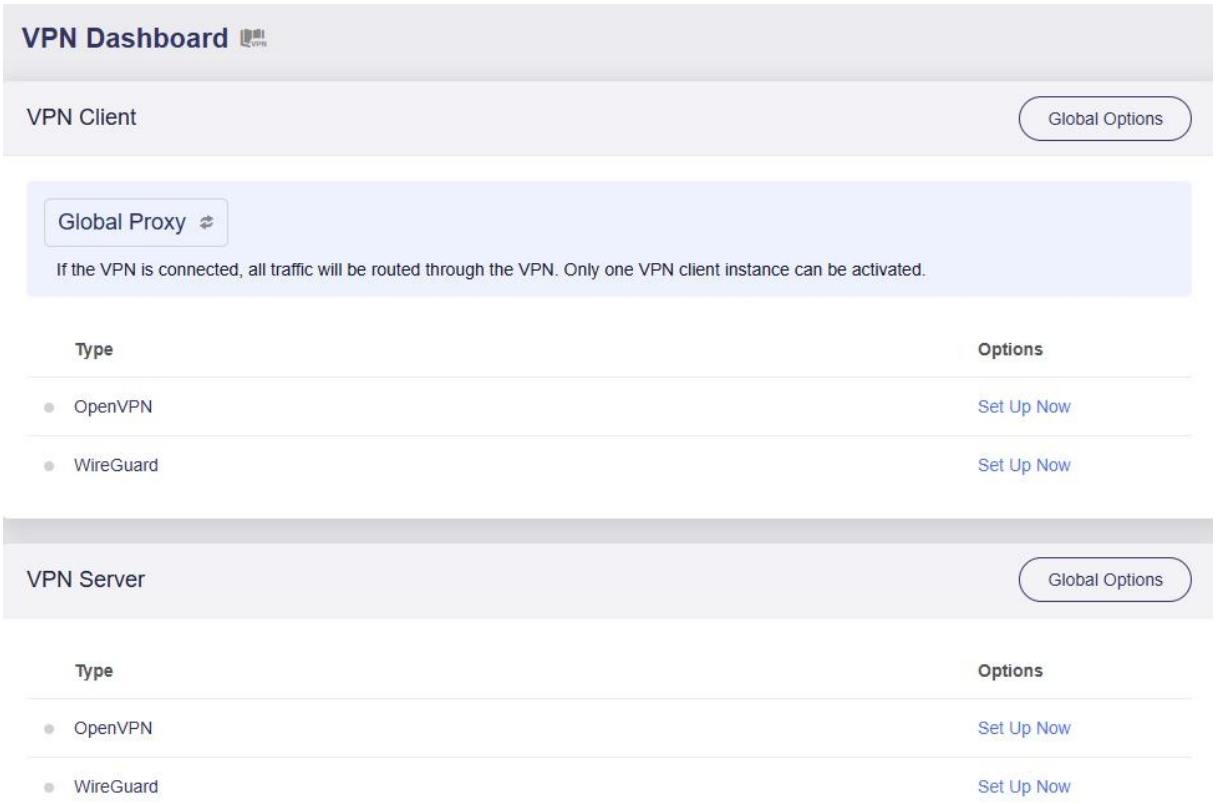
Tableau de bord VPN

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

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

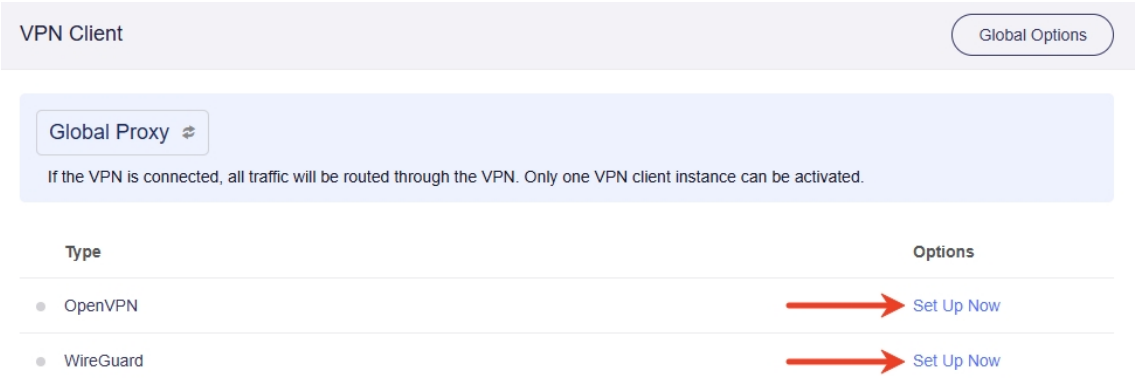
Le tableau de bord VPN affiche les détails de la connexion VPN : adresse du serveur, statistiques du trafic, adresse IP virtuelle du client et journal de connexion. Il permet aussi de configurer des paramètres avancés tels que le coupe-circuit VPN, les règles VPN, le masquage IP, la MTU et le VPN en cascade.

Cette page comprend deux sections : **Client VPN (VPN Client)** et **Serveur VPN (VPN Server)**.

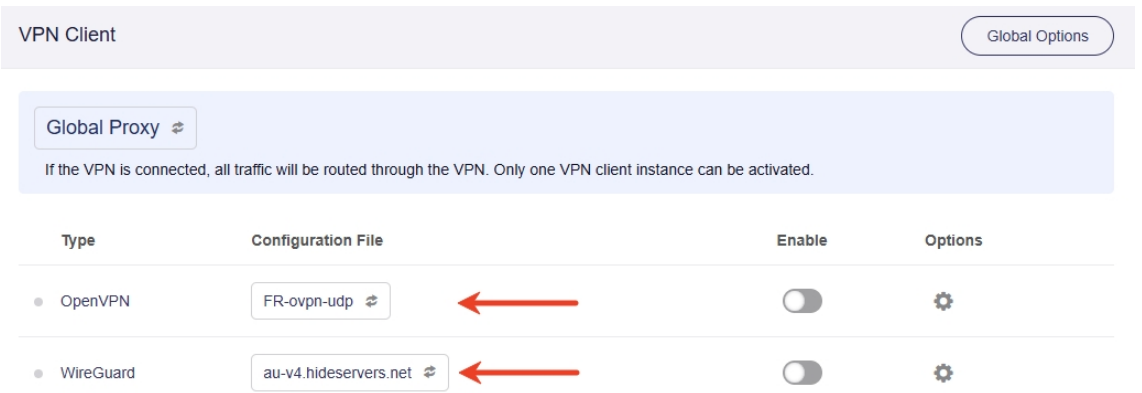


8.1 Client VPN

Lors de la première ouverture de cette page, si aucun fichier de configuration OpenVPN ou WireGuard n'est disponible, l'écran ci-dessous s'affiche. Cliquez sur **Configurer maintenant (Set Up Now)** pour accéder à la page Client OpenVPN ou Client WireGuard et téléverser votre fichier de configuration VPN.



Après le téléversement, votre configuration apparaît dans la colonne Fichier de configuration (Configuration File). Si vous avez téléversé plusieurs fichiers, cliquez sur le champ pour en sélectionner un autre.

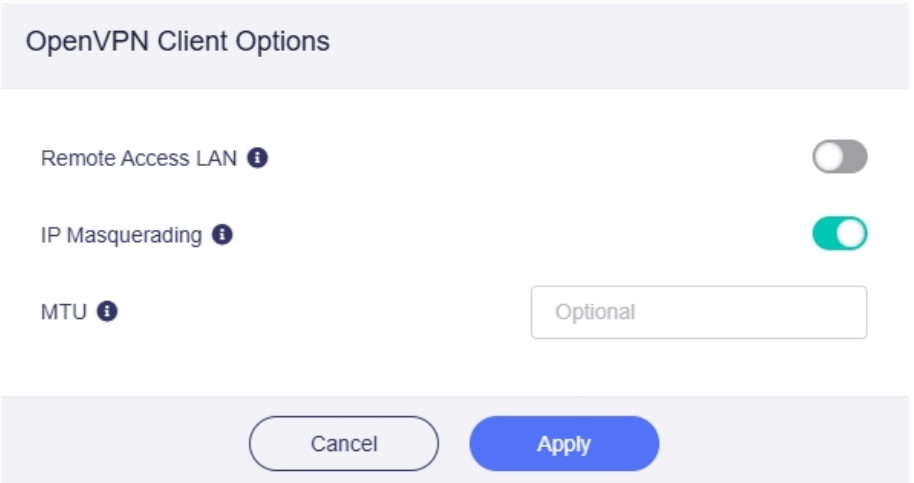


8.1.1 Options du client

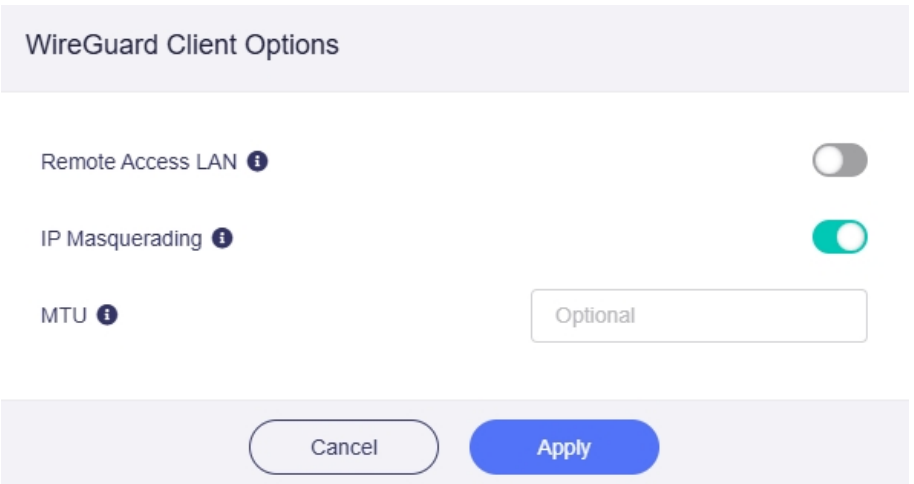
Cliquez sur l'engrenage à droite pour ouvrir les options du client OpenVPN ou WireGuard.



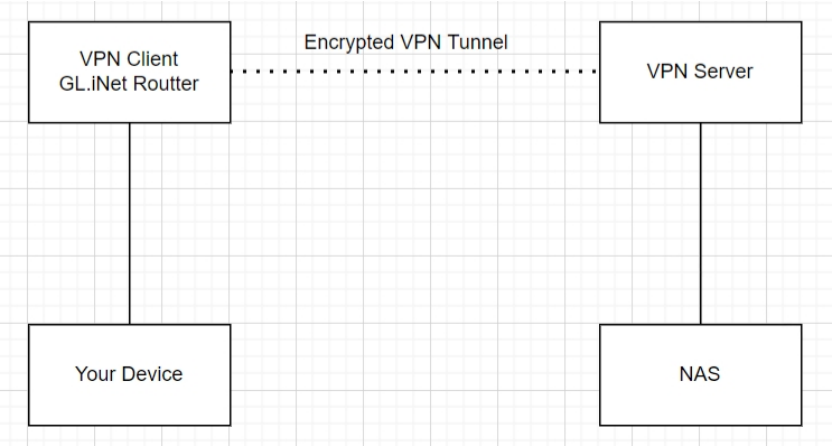
Les options du client OpenVPN sont présentées ci-dessous.



Les options du client WireGuard sont présentées ci-dessous.



- **Accès distant au LAN (Remote Access LAN)** : autorise l'accès à distance à ce routeur et aux appareils de son réseau LAN via le VPN. Le serveur VPN doit annoncer une route vers le sous-réseau LAN de ce routeur.

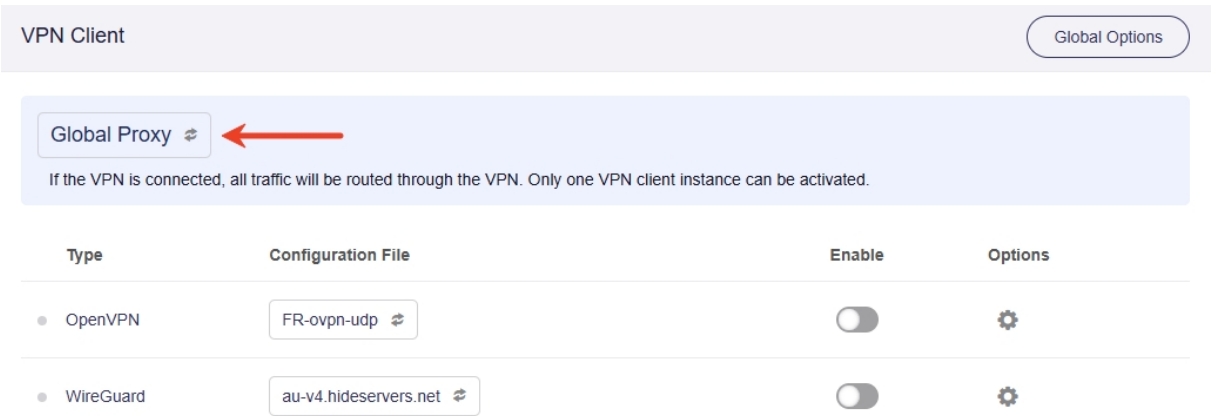


Dans le schéma ci-dessus, le routeur GL.iNet fonctionne comme client VPN et se connecte à un serveur VPN par un tunnel VPN. Lorsque cette option est activée, les appareils du côté serveur VPN, par exemple un NAS, peuvent accéder au routeur GL.iNet et aux appareils de son réseau LAN. Pour cela, ajoutez sur le serveur VPN une règle de routage vers le sous-réseau LAN du routeur GL.iNet.

- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l'IP du tunnel VPN du routeur. Ne désactivez cette option que pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.
- **MTU** : unité de transmission maximale (Maximum Transmission Unit). Ce paramètre facultatif permet de personnaliser la MTU du tunnel VPN. La valeur choisie remplace celle du fichier de configuration.

8.1.2 Mode proxy

Le mode proxy par défaut de la connexion VPN est **Proxy global (Global Proxy)**. Cliquez sur le champ en haut à droite pour choisir un autre mode.



Trois modes proxy sont proposés : **Proxy global (Global Proxy)**, **Mode par règles (Policy Mode)** et **Mode de routage (Route Mode)**.

1. **Proxy global (Global Proxy)**

   Dans ce mode, tout le trafic passe par le VPN. Une seule instance de client VPN peut être activée.

2. **Mode par règles (Policy Mode)**

   Ce mode propose trois types de règles.

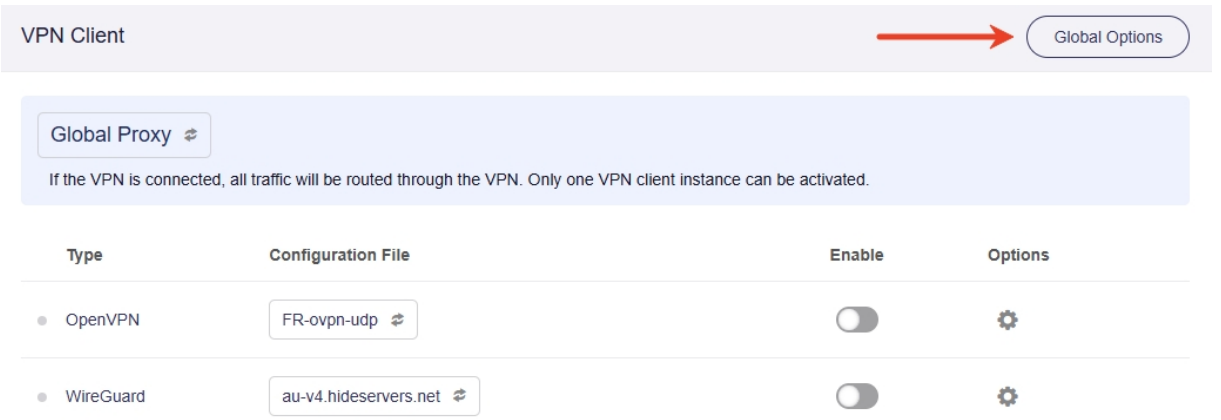
   - **Selon le domaine ou l'IP cible (Based on the Target Domain or IP)** : seul le trafic de certains sites Web identifiés par leur adresse IP ou leur nom de domaine passe par le VPN. Une seule instance de client VPN peut être activée.
   - **Selon l'appareil client (Based on the Client Device)** : seul le trafic de certains appareils LAN identifiés par leur adresse MAC passe par le VPN. Une seule instance de client VPN peut être activée.
   - **Selon le VLAN (Based on the VLAN)** : seul le trafic de certains VLAN passe par le VPN. Une seule instance de client VPN peut être activée.

3. **Mode de routage (Route Mode)**

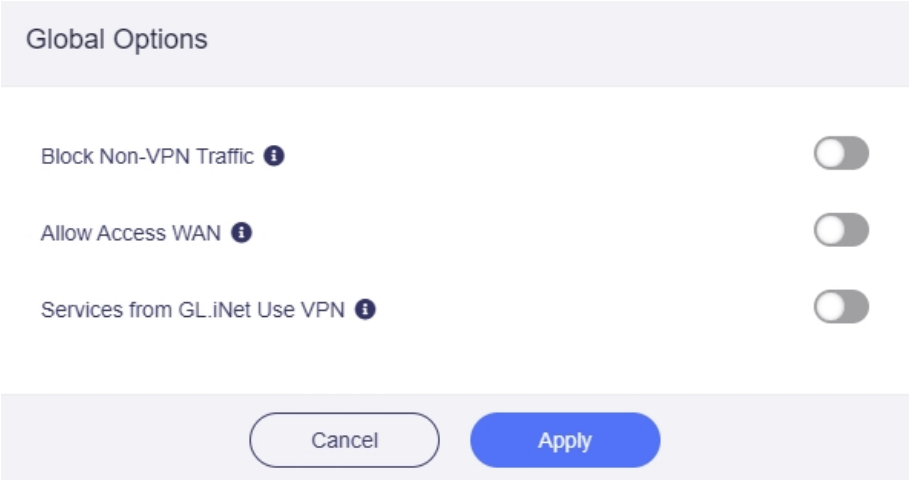
   - **Détection automatique (Auto Detect)** : utilise les règles de routage définies dans chaque fichier de configuration du client VPN ou fournies par le serveur VPN.
   - **Personnaliser les règles de routage (Customize Routing Rules)** : permet de configurer manuellement les règles de routage de chaque instance de client VPN.

8.1.3 Options globales

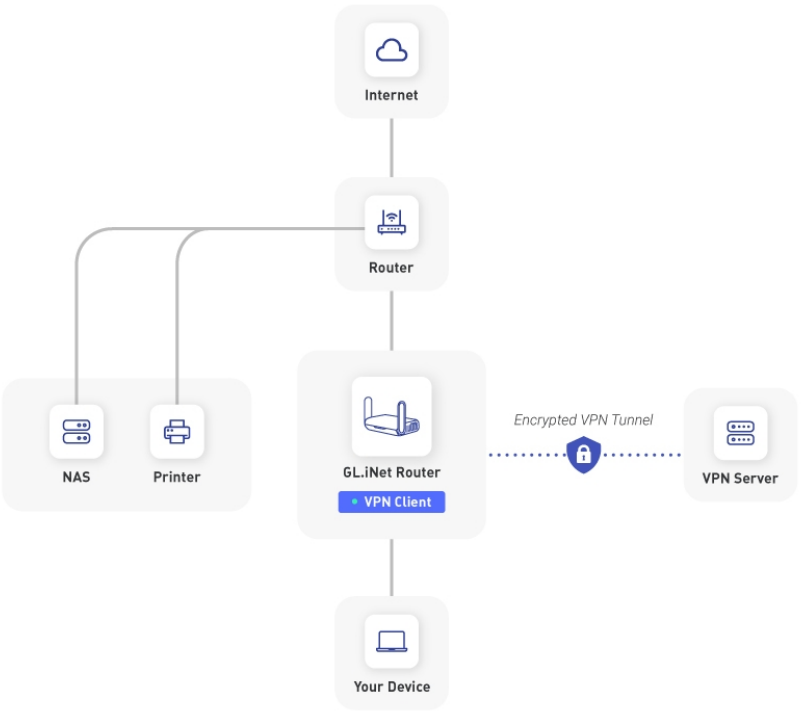
Cliquez sur **Options globales (Global Options)** en haut à droite pour configurer les paramètres du client VPN.



La fenêtre ci-dessous s'ouvre.



- **Bloquer le trafic hors VPN (Block Non-VPN Traffic)** : cette fonction est aussi appelée **coupe-circuit VPN (VPN Kill Switch)**. Lorsqu'elle est activée, tout le trafic Internet doit passer exclusivement par le tunnel VPN et ne peut emprunter aucune autre interface, telle que le WAN du fournisseur d'accès local. Si la connexion VPN est interrompue de manière inattendue, tout le trafic Internet est bloqué pour empêcher le basculement vers la connexion WAN habituelle. Cela évite les fuites de trafic liées à une défaillance du VPN, à des paramètres DNS clients incorrects ou à des problèmes similaires.
- **Autoriser l'accès au WAN (Allow Access WAN)** : permet aux appareils clients locaux d'accéder aux services du côté WAN, par exemple aux imprimantes, NAS et autres appareils du sous-réseau amont, pendant que le VPN est actif.

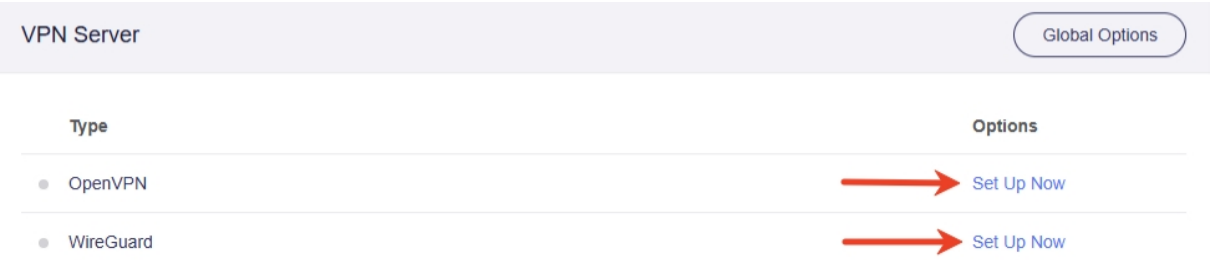


Comme le montre le schéma ci-dessus, cette fonction permet aux appareils locaux d'accéder aux hôtes du sous-réseau amont, notamment aux imprimantes et NAS. Cette option sert principalement à permettre l'accès des clients aux appareils du sous-réseau amont. Toutefois, le routeur ne peut pas distinguer le trafic de ce sous-réseau du trafic Internet ordinaire. Si les appareils clients accèdent directement à des ressources via des adresses IP publiques, un risque de fuite de trafic existe. Les options **Autoriser l'accès au WAN (Allow Access WAN)** et **Bloquer le trafic hors VPN (Block Non-VPN Traffic)** s'excluent donc mutuellement et ne peuvent pas être activées simultanément.

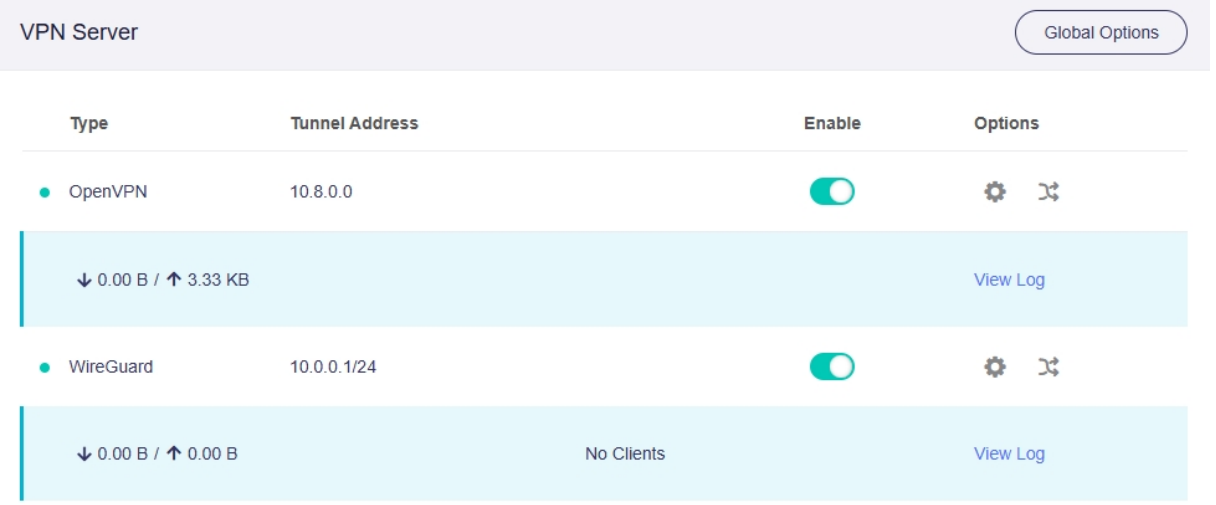
- **Utiliser le VPN pour les services GL.iNet (Services From GL.iNet Use VPN)** : permet aux services GoodCloud, DDNS et rtty de transmettre leurs paquets par les tunnels VPN. Cette option est désactivée par défaut, car ces services ont généralement besoin de l'adresse IP réelle de l'appareil pour fonctionner correctement.

8.2 Serveur VPN

Si le routeur n’a jamais été configuré comme serveur OpenVPN ou WireGuard, l’écran ci-dessous s’affiche. Cliquez sur **Configurer maintenant (Set Up Now)** pour ouvrir la page Serveur OpenVPN ou Serveur WireGuard et initialiser votre serveur VPN.

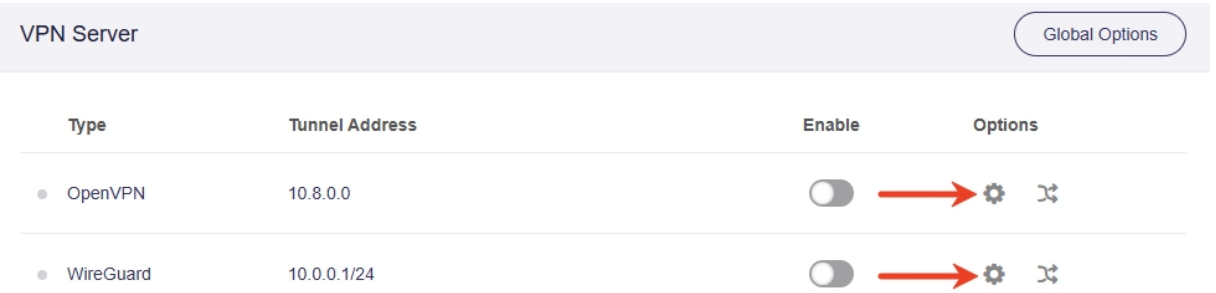


Une fois le serveur OpenVPN ou WireGuard activé, la page affiche son état comme ci-dessous.

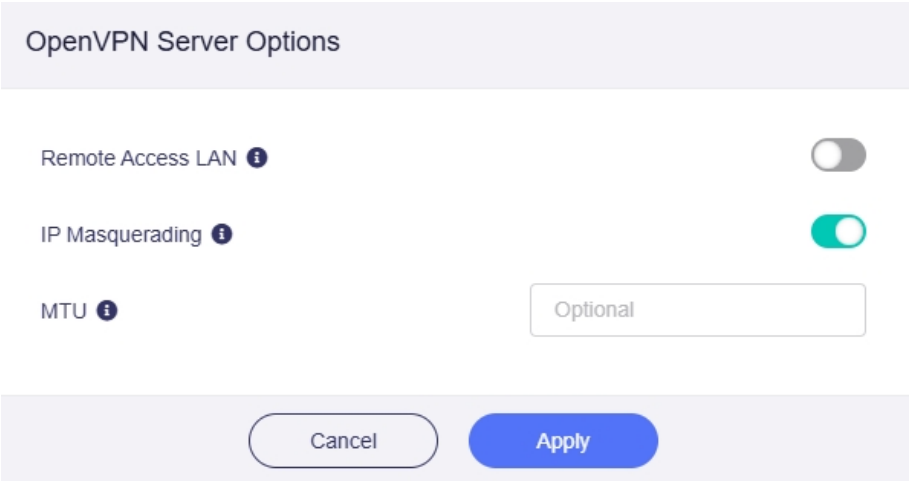


8.2.1 Options du serveur

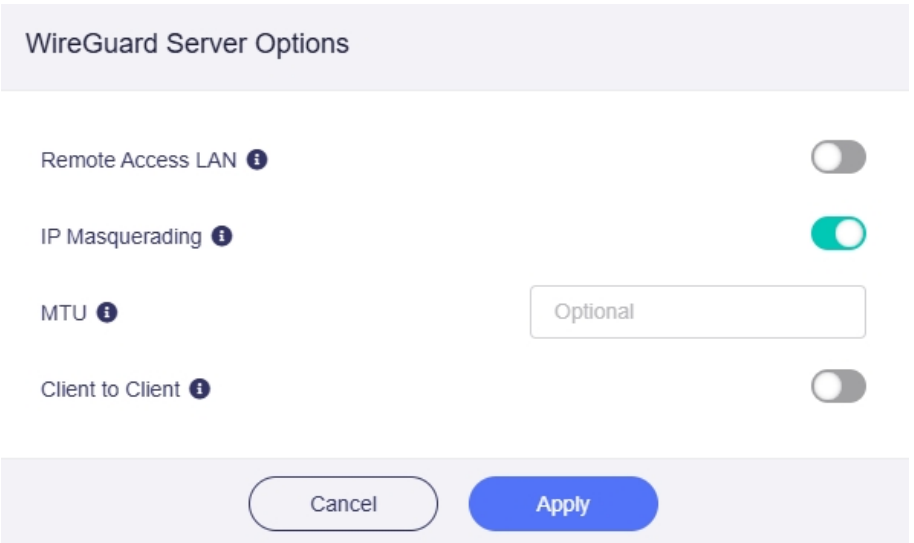
Cliquez sur l’engrenage à droite pour ouvrir les options du serveur OpenVPN ou WireGuard.



Les options du serveur OpenVPN sont présentées ci-dessous.



Les options du serveur WireGuard sont présentées ci-dessous.

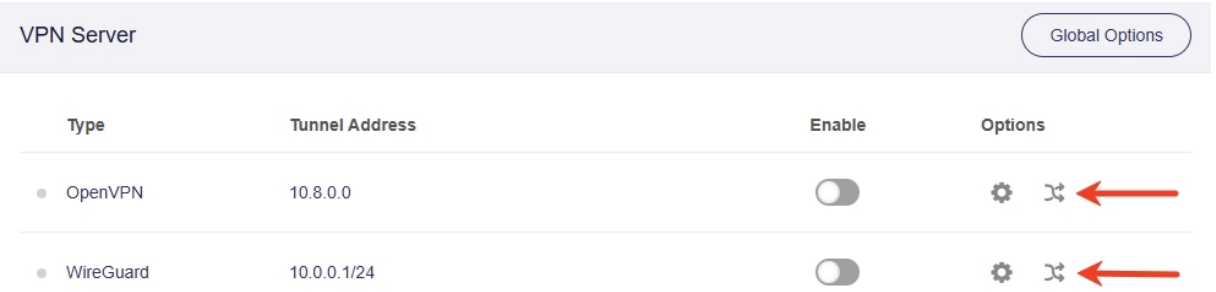


- **Accès distant au LAN (Remote Access LAN)** : permet d'accéder aux ressources du sous-réseau LAN du serveur par le tunnel VPN.
- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l'IP du tunnel VPN du routeur. Ne désactivez cette option que pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.
- **MTU** : unité de transmission maximale (Maximum Transmission Unit). La valeur choisie pour le tunnel remplace les paramètres MTU du fichier de configuration.
- **Communication entre clients (Client to Client)** : permet aux clients VPN connectés à ce serveur de communiquer entre eux via leurs adresses IP de tunnel VPN. Pour qu'ils

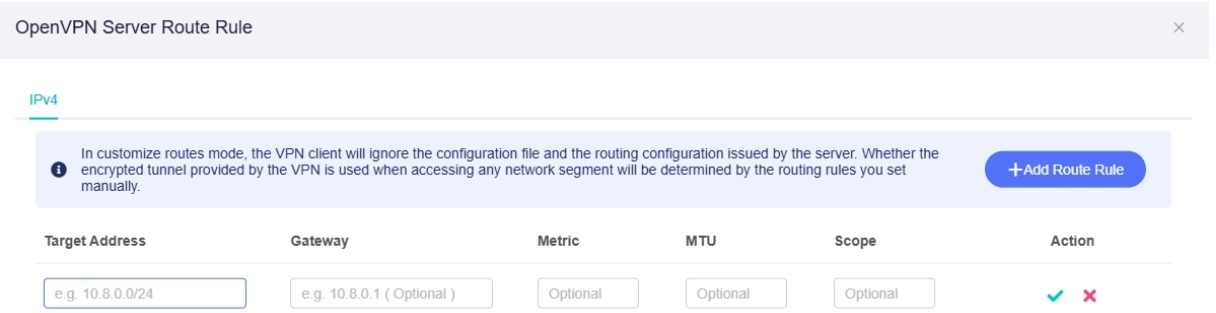
puissent également accéder aux sous-réseaux LAN des autres clients, le serveur VPN doit annoncer les routes correspondantes vers ces sous-réseaux LAN distants.

8.2.2 Règles de routage du serveur

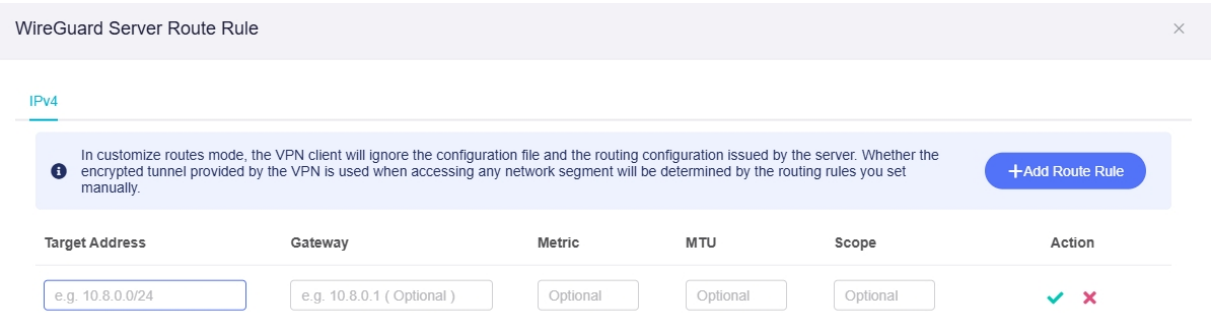
Cliquez sur l'icône de routage à droite pour personnaliser les règles de routage OpenVPN ou WireGuard selon vos besoins.



Les règles de routage du serveur OpenVPN sont présentées ci-dessous. Cliquez sur **Ajouter une règle de routage (Add Route Rule)**, renseignez l'**adresse cible (Target Address)** et la **passerelle (Gateway)**, puis cliquez sur la coche verte pour appliquer la règle.

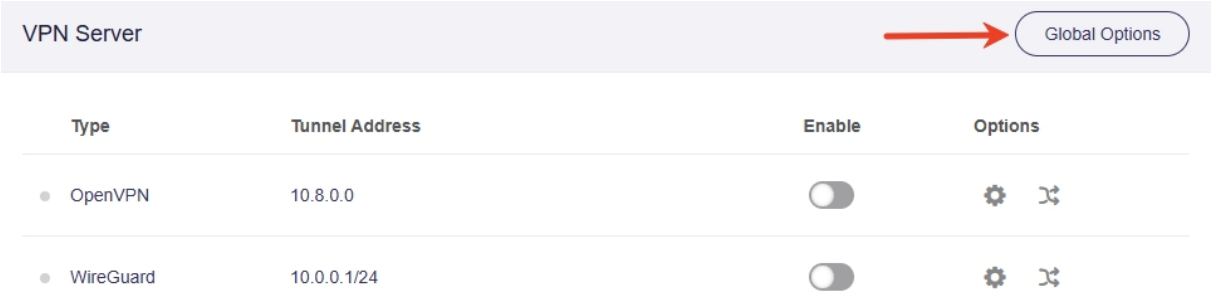


Les règles de routage du serveur WireGuard sont présentées ci-dessous. Cliquez sur **Ajouter une règle de routage (Add Route Rule)**, renseignez l'**adresse cible (Target Address)** et la **passerelle (Gateway)**, puis cliquez sur la coche verte pour appliquer la règle.

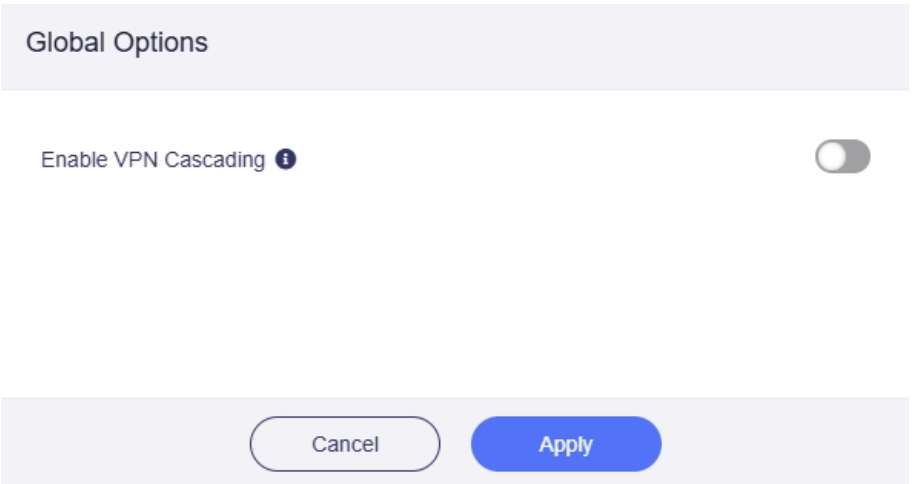


8.2.3 Options globales

Cliquez sur **Options globales (Global Options)** en haut à droite pour configurer les paramètres du serveur VPN.



La fenêtre ci-dessous s’ouvre.



- **VPN en cascade (VPN Cascading)** : lorsque ce routeur fonctionne simultanément comme serveur VPN et client VPN, cette option fait passer le trafic des clients VPN distants connectés à son serveur VPN par le tunnel VPN amont utilisé par le routeur en tant que client. Consultez cette page pour en savoir plus.

Chapitre 9

Configuration d’un serveur VPN

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

9.1 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.

9.1.1 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 :

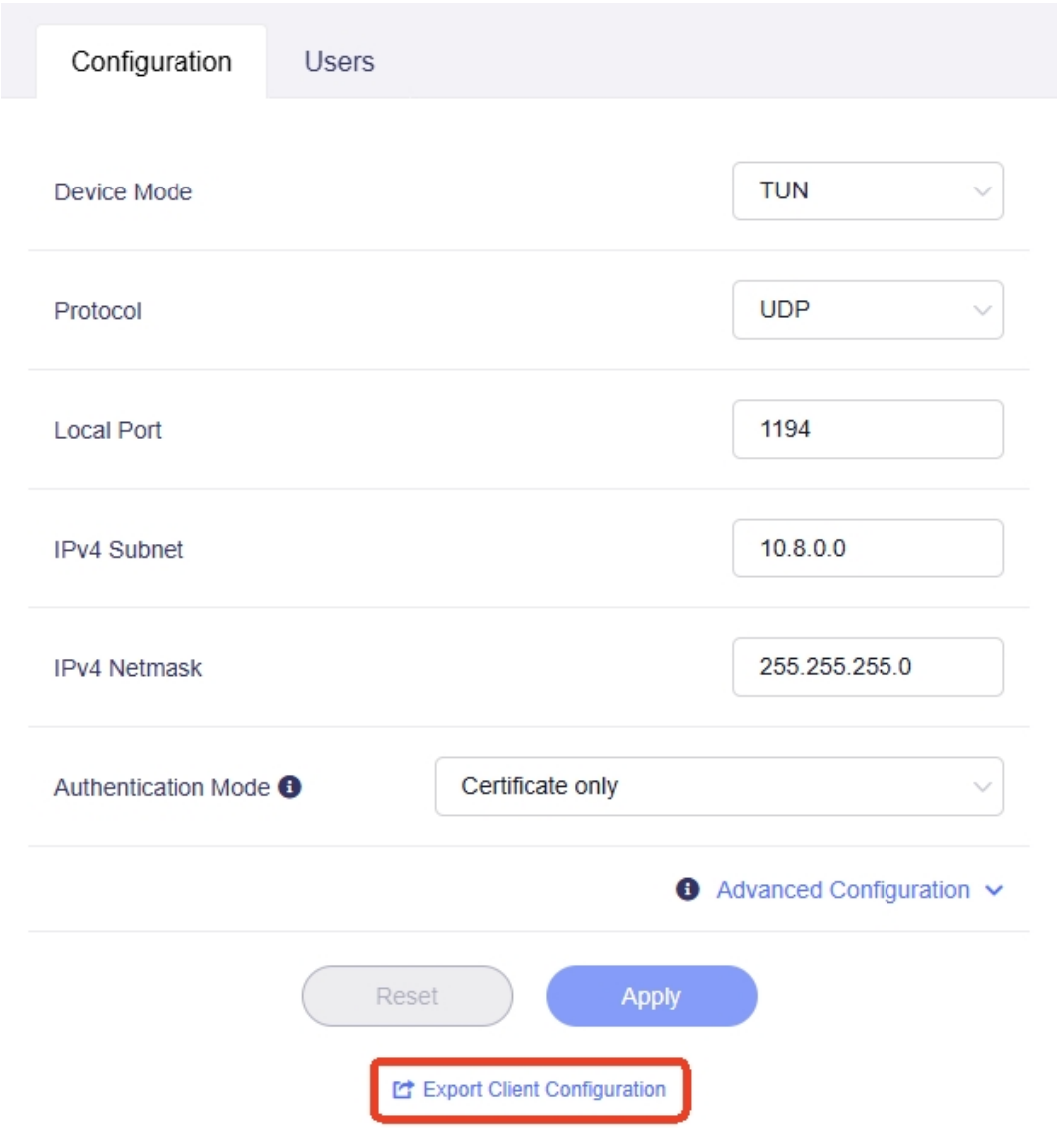
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions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

9.1.2 Étapes de configuration

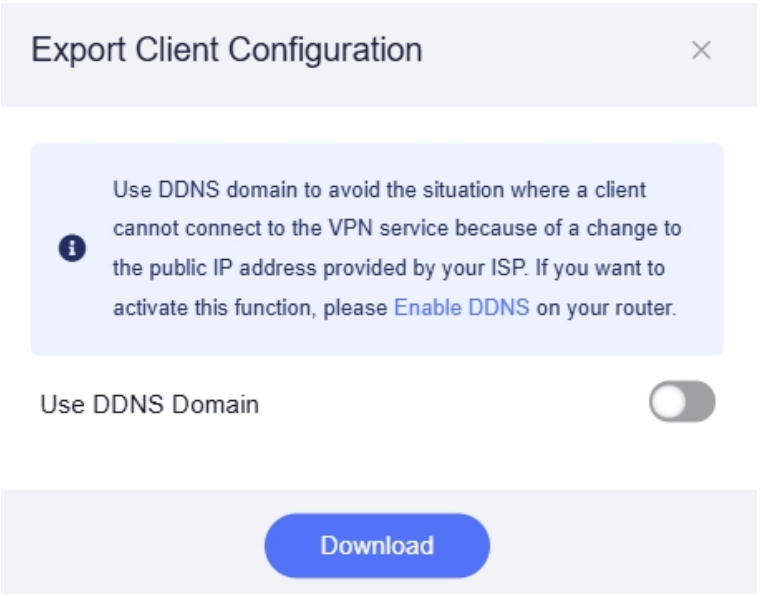
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur OpenVPN (OpenVPN Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.
   La configuration par défaut convient à la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

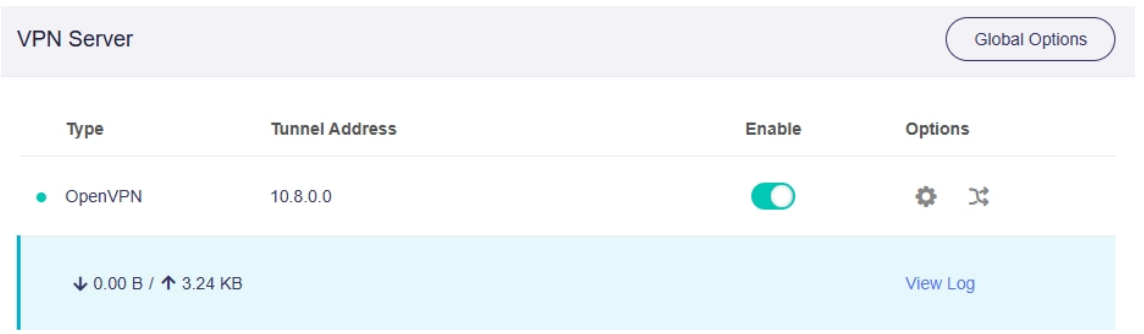
- **Protocole (Protocol)** : UDP ou TCP. Consultez cette page pour connaître les différences.
- **Mode d'authentification (Authentication Mode)** : détermine la méthode utilisée lors de la connexion du client au serveur. Trois options sont proposées :
  - **Certificat uniquement (Certificate Only)** : 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 selon vos besoins.

3. Après avoir cliqué sur **Exporter la configuration client (Export Client Configuration)** au bas de l'onglet Configuration, ou après avoir appliqué les modifications de configuration, la fenêtre ci-dessous s'ouvre. Cliquez sur **Télécharger (Download)** pour exporter la configuration. **Remarque** : si votre adresse IP publique change fréquemment, activez le DDNS avant de cliquer sur Télécharger. Vous pourrez alors utiliser le nom de domaine DDNS comme adresse du serveur.



4. Activez le serveur OpenVPN.

   Ouvrez le **Tableau de bord VPN (VPN Dashboard)** et activez le serveur OpenVPN avec le commutateur. Il démarre comme indiqué ci-dessous.



9.1.3 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.

9.2 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.

9.2.1 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 :

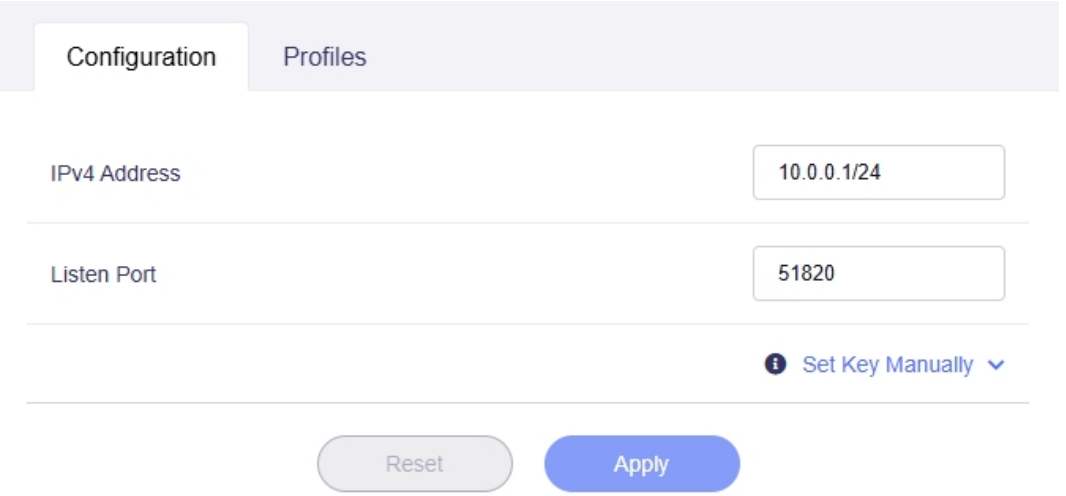
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux solutions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

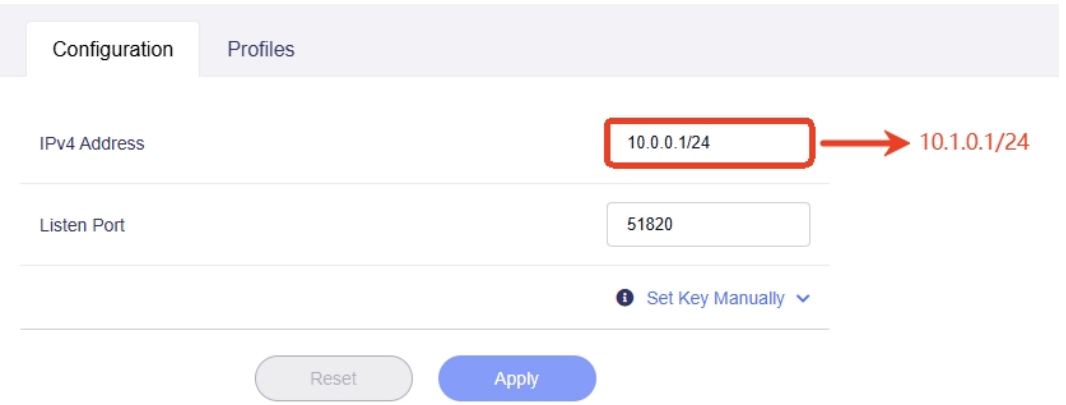
   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n’est nécessaire. Passez à l’étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs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

9.2.2 Étapes de configuration

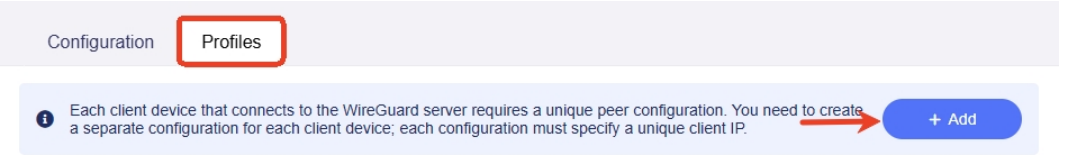
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur WireGuard (WireGuard Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.
   La configuration par défaut convient à la plupart des situations. Ne modifiez l'adresse IPv4 que si elle entre en conflit avec la passerelle du routeur en amont.



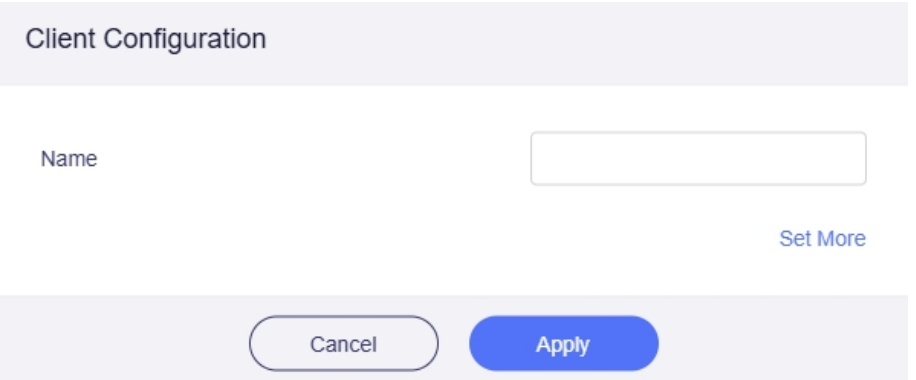
   En cas de conflit, choisissez une autre adresse IPv4, par exemple **10.1.0.1/24**, puis cliquez sur **Appliquer (Apply)**. Conservez la notation CIDR « /24 » pour éviter les problèmes de connexion.



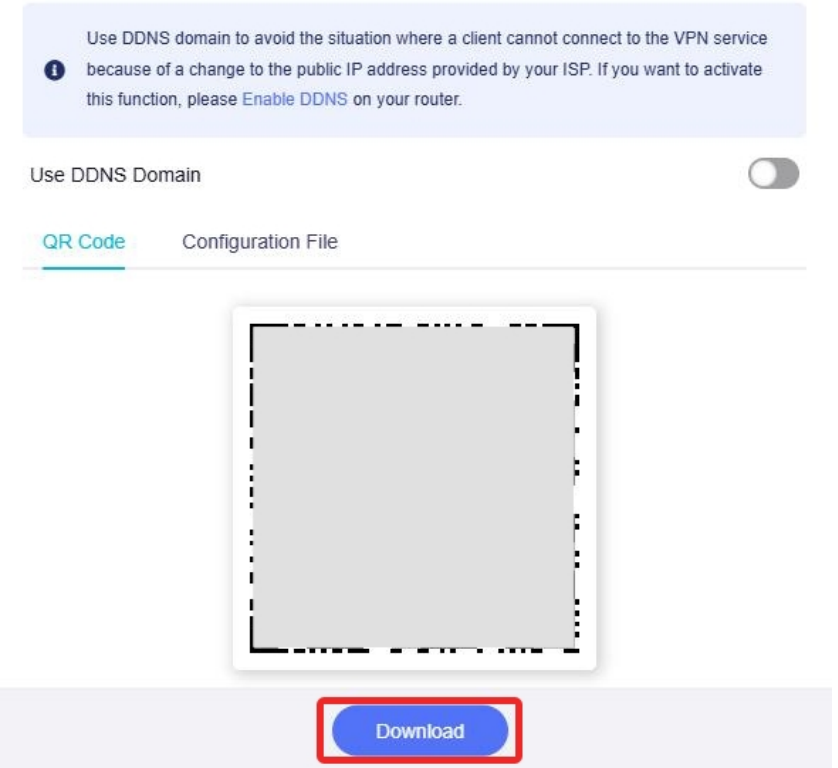
3. Ajoutez un profil.
   Ouvrez l'onglet **Profils (Profiles)**, puis cliquez sur **Ajouter (Add)** pour générer un profil pour votre appareil.



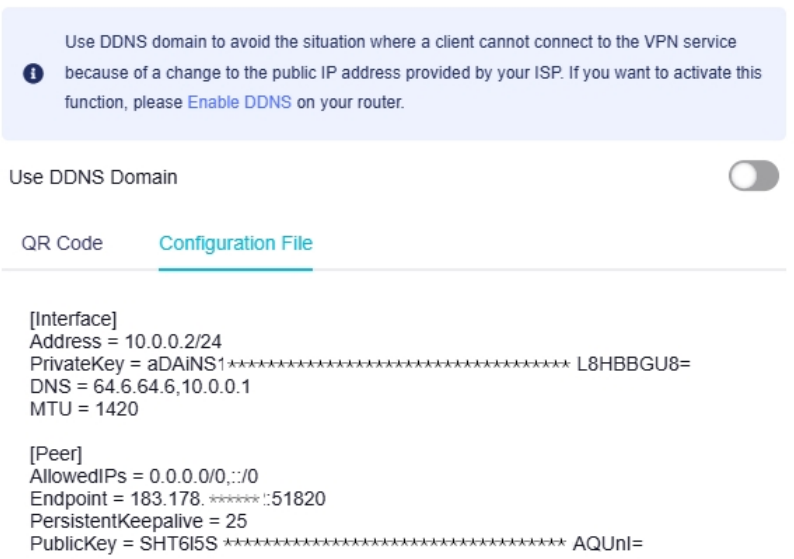
Saisissez un nom explicite et cliquez sur **Appliquer (Apply)** pour continuer.



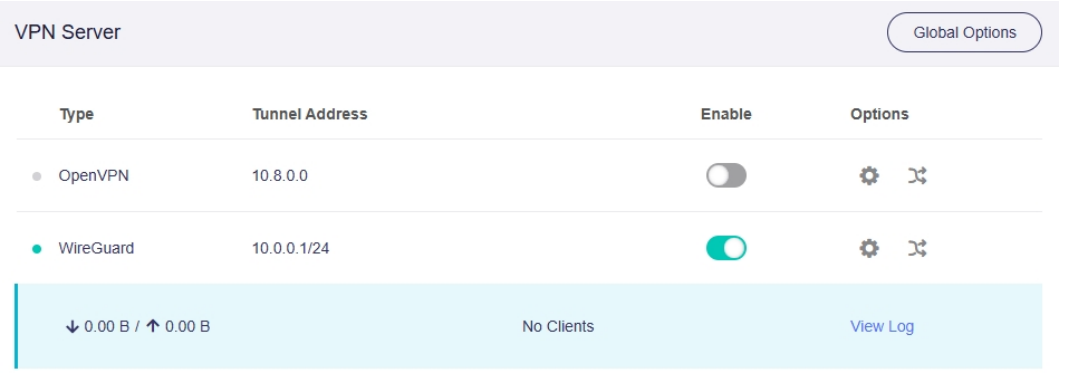
4. Après l'ajout d'un profil, le routeur génère un fichier de configuration sous trois formes : code QR, fichier .conf et texte brut. Choisissez le format qui vous convient. **Remarque** : si votre adresse IP publique change fréquemment, activez le DDNS avant de télécharger le fichier.
   - **Code QR** : 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.
   - **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.



- **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.



5. Activez le serveur WireGuard.
   Ouvrez le **Tableau de bord VPN (VPN Dashboard)** et activez votre serveur WireGuard avec le commutateur. Il démarre comme indiqué ci-dessous.



9.2.3 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 10

Configuration d’un client VPN

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

10.1 Configuration d’un client OpenVPN

10.1.1 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.

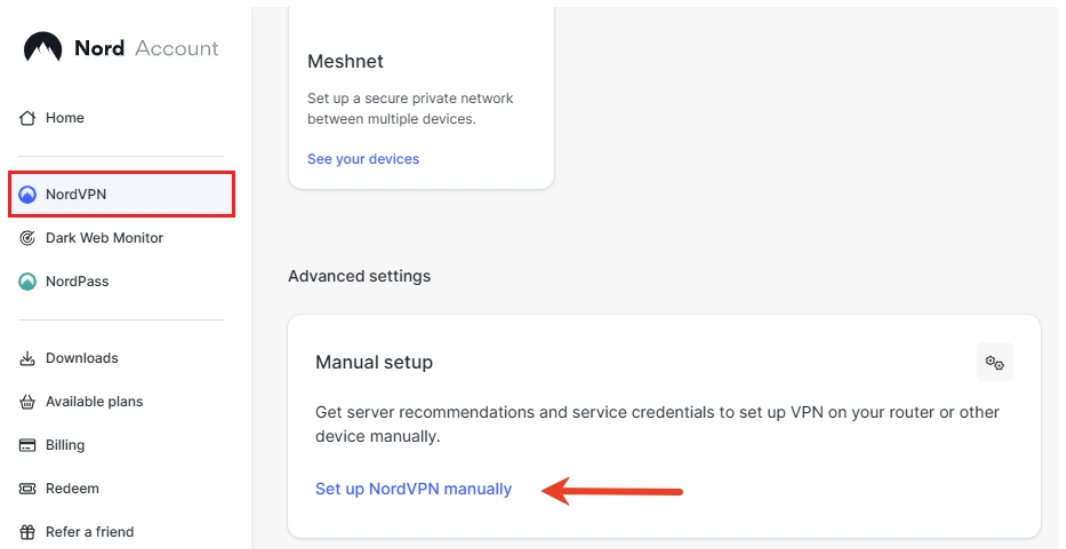
Rendez-vous ensuite sur le site officiel de votre fournisseur VPN pour obtenir les identifiants de service ou le fichier de configuration. Si vous ne savez pas comment obtenir ce fichier, consultez ce lien ou contactez l’assistance du fournisseur.

10.1.2 Configuration de NordVPN

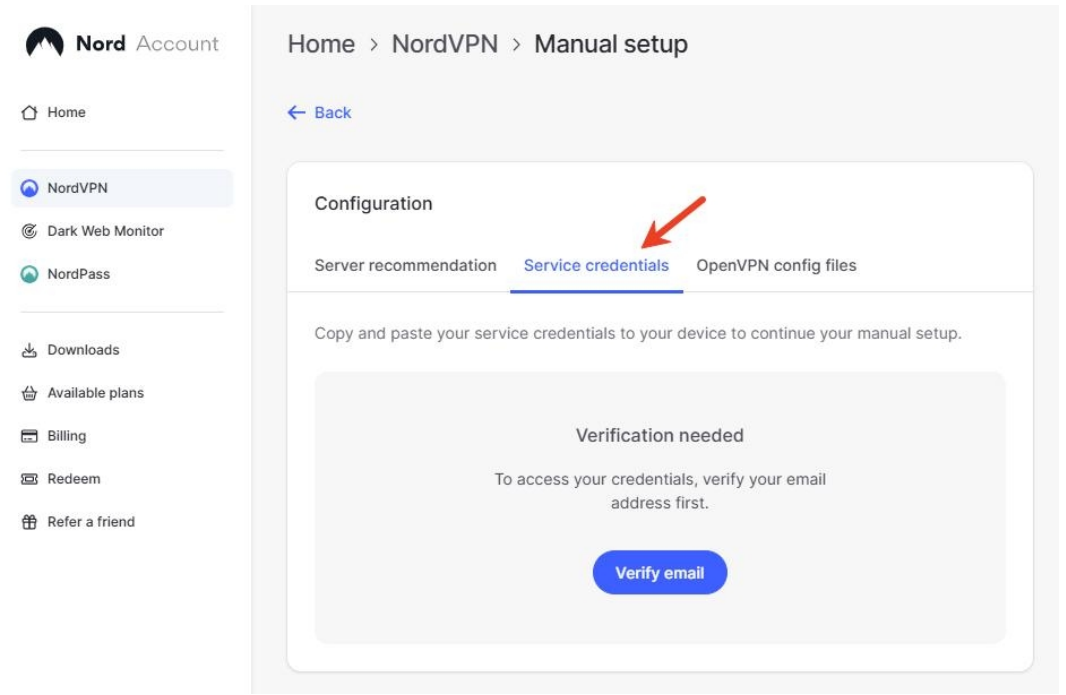
NordVPN est intégré à l’interface d’administration Web GL.iNet. Saisissez les identifiants obtenus dans le tableau de bord NordVPN dans l’interface du routeur ou dans l’application mobile GL.iNet pour récupérer les fichiers de configuration de tous les serveurs NordVPN, sans importation manuelle.

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

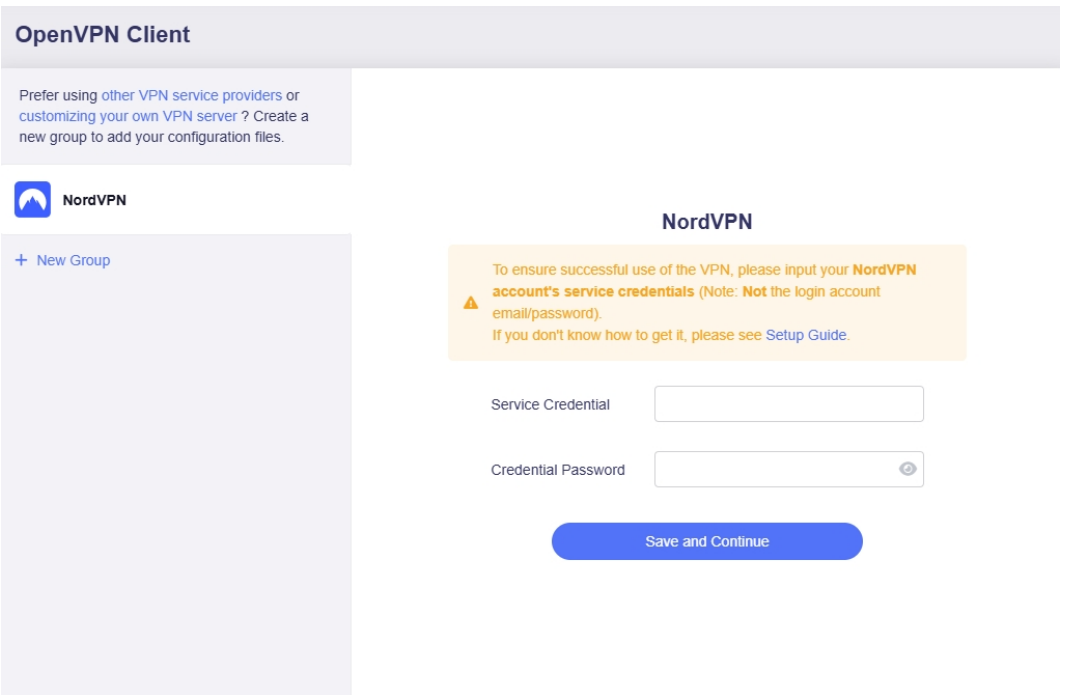
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



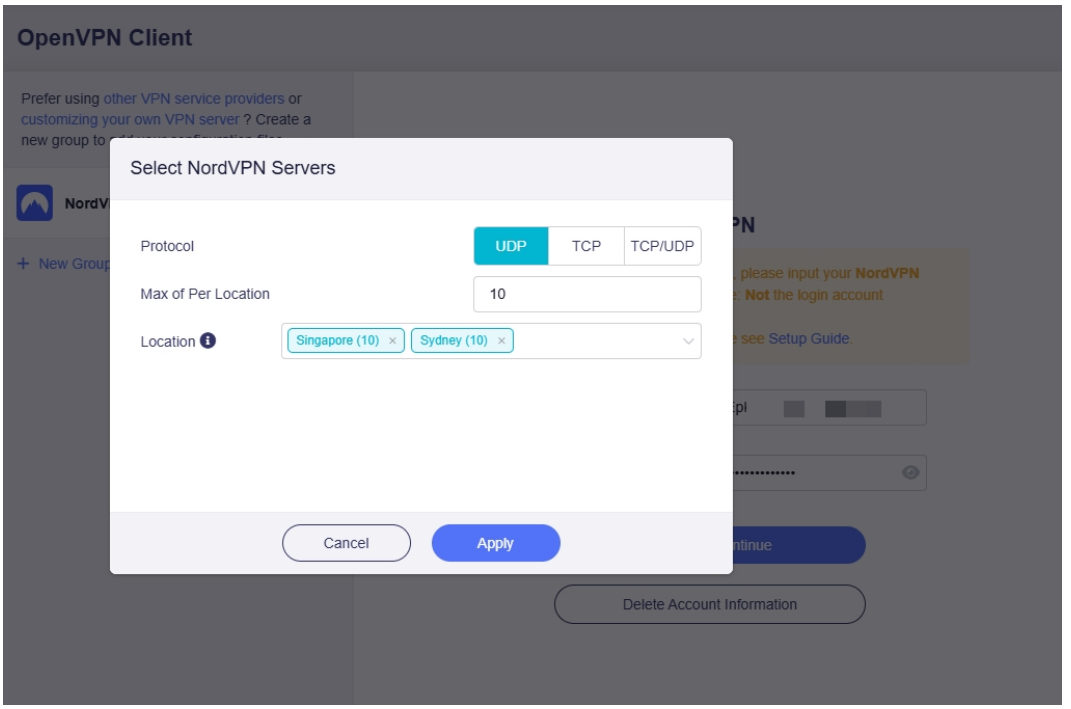
Repérez les **identifiants de service (service credentials)** et copiez-les pour les utiliser ensuite.



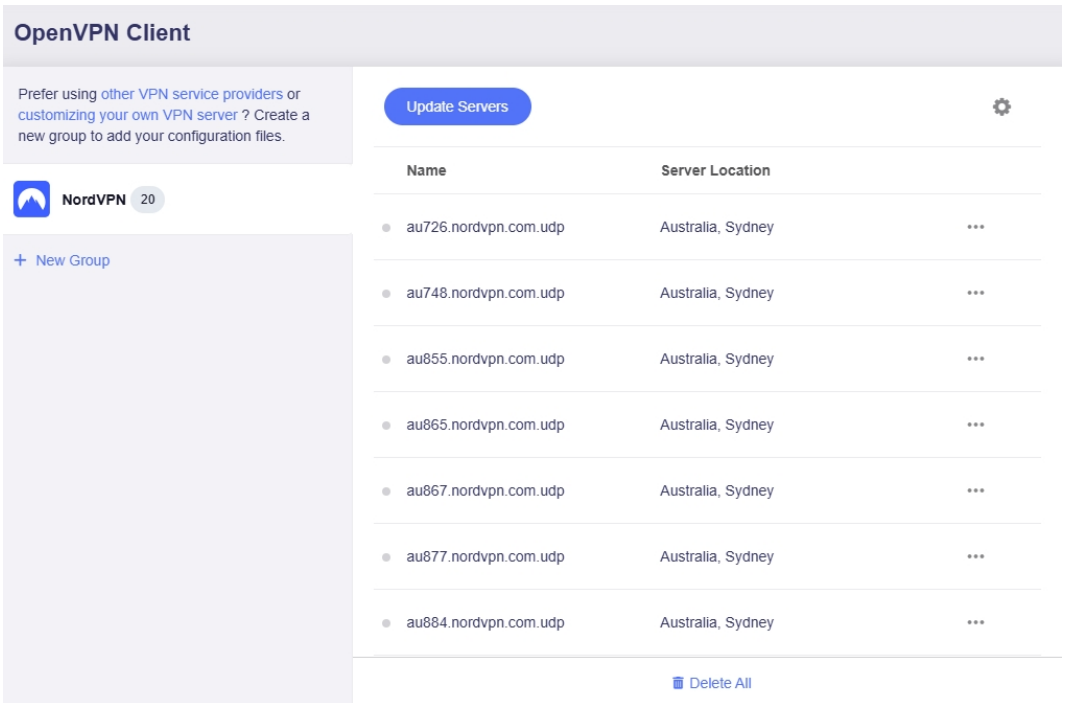
3. Dans l'interface d'administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** > **NordVPN**. Saisissez les identifiants de service, qui ne sont PAS l'adresse e-mail et le mot de passe de connexion au compte, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



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

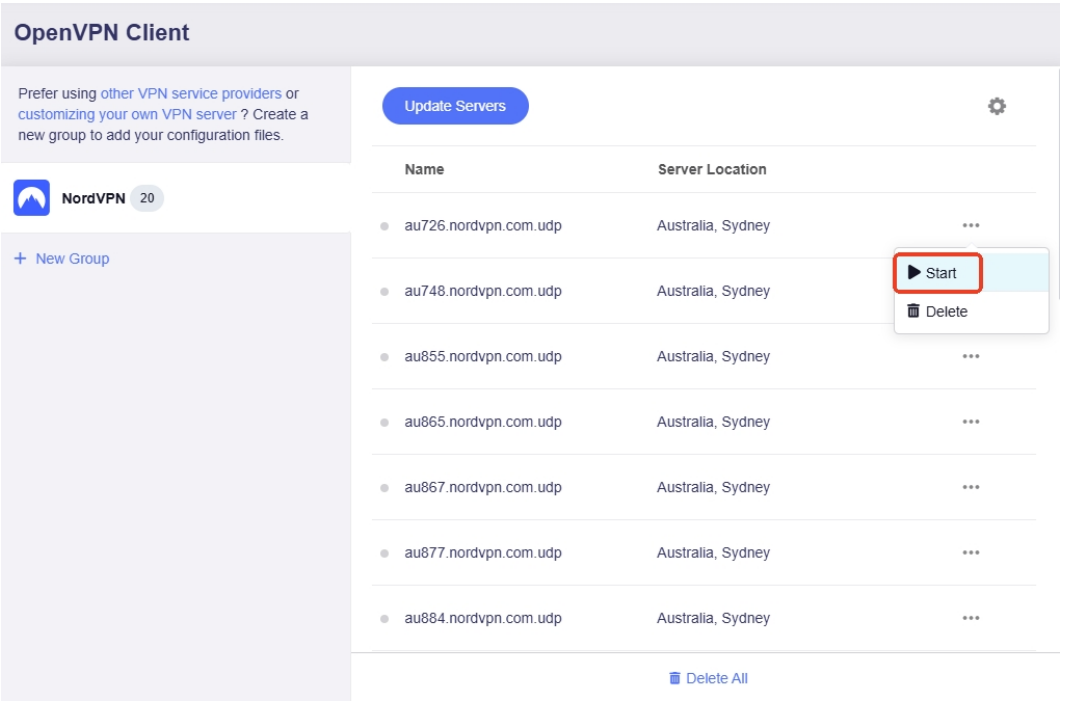


Les fichiers de configuration sont téléchargés.

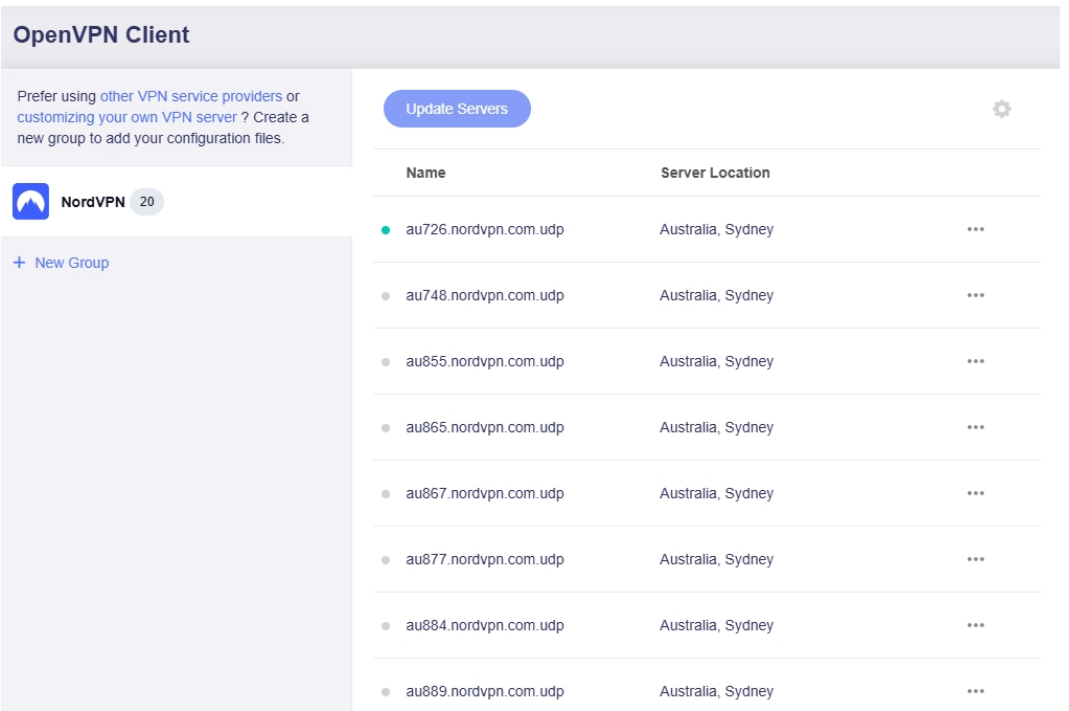


5. Établissez une connexion.

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



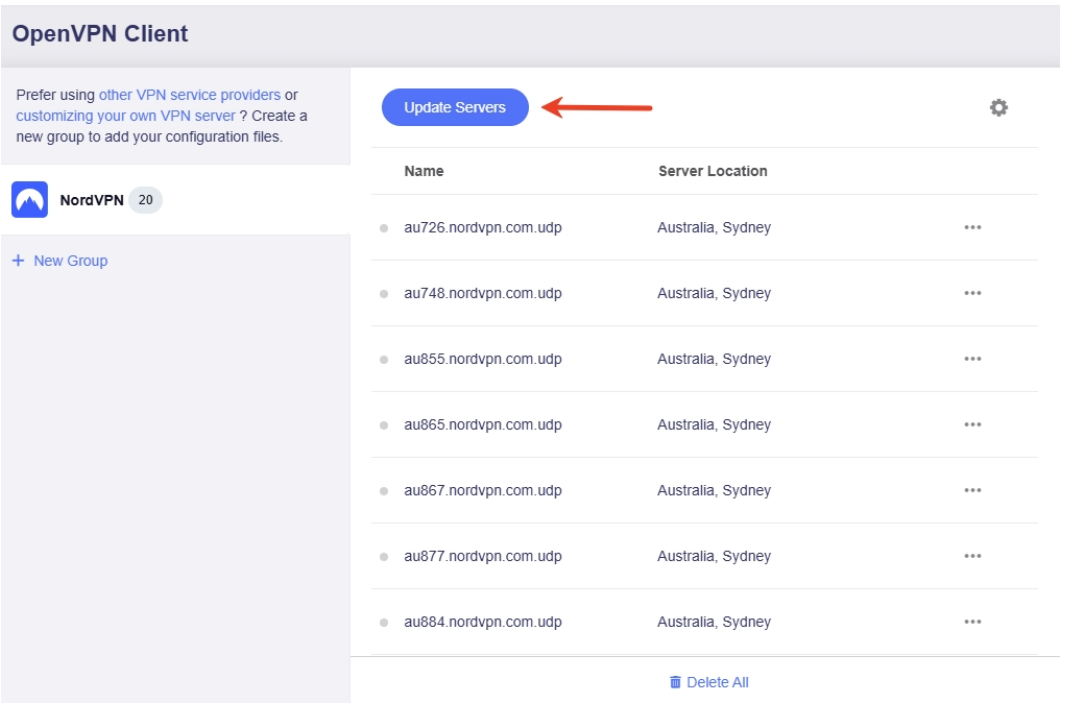
6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

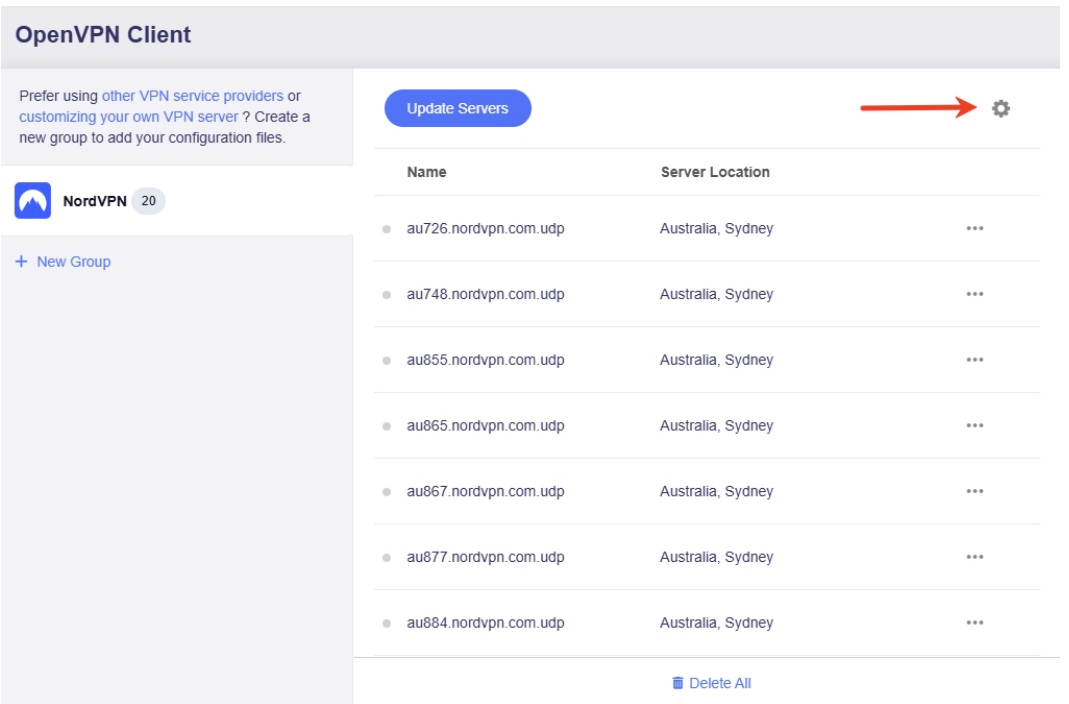
7. Mettez à jour les serveurs.

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.



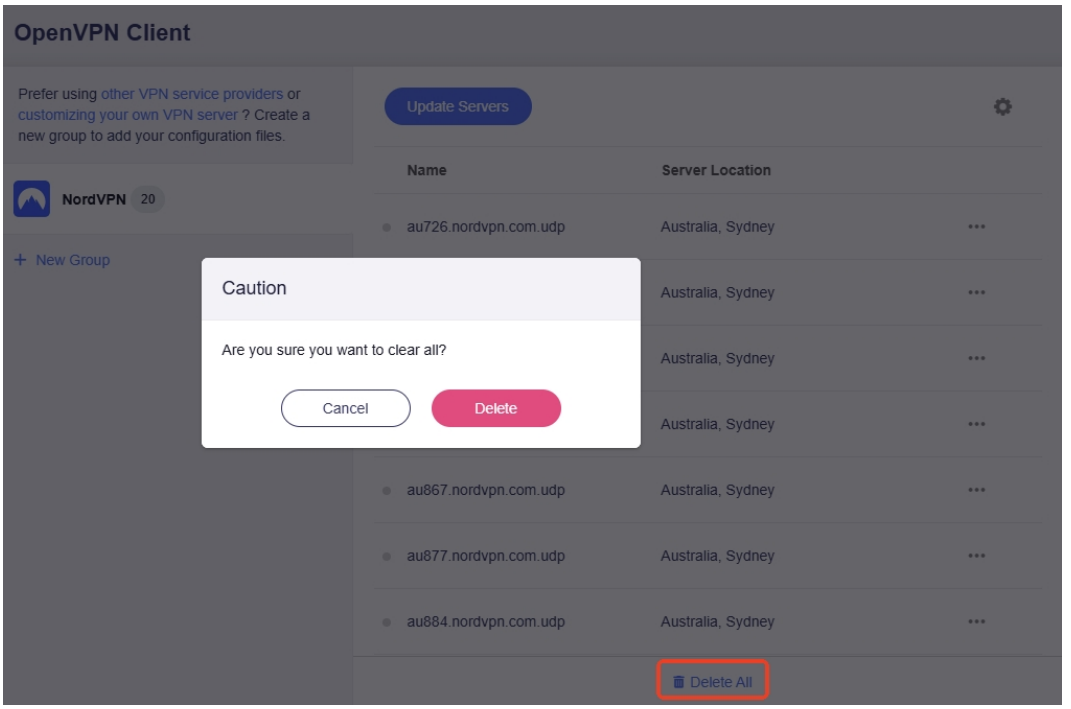
8. Modifiez les identifiants.

   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.

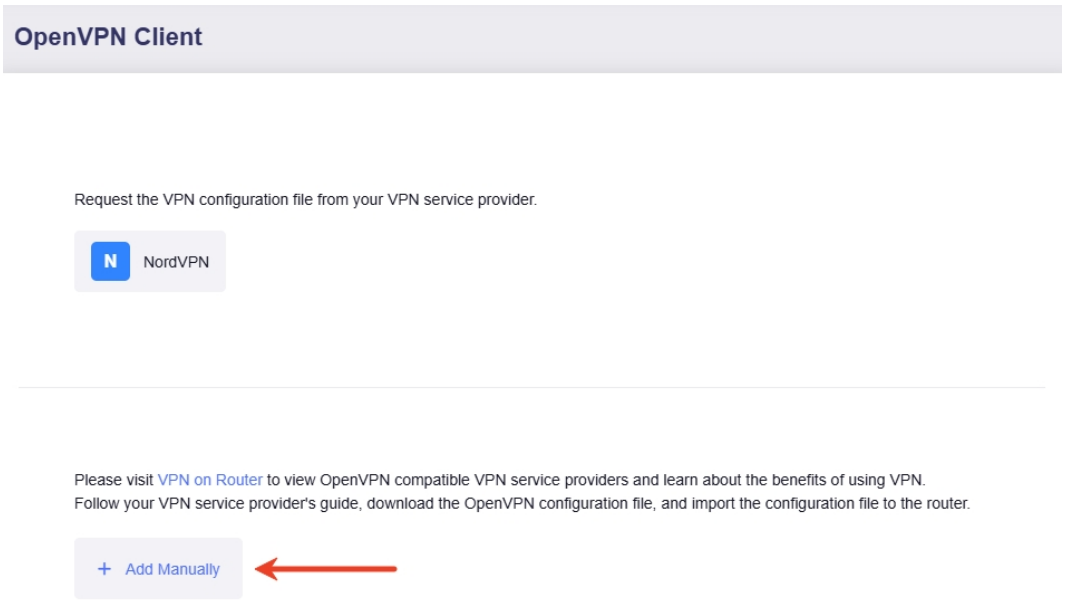


10.1.3 Configuration manuelle d’un client OpenVPN pour un autre fournisseur

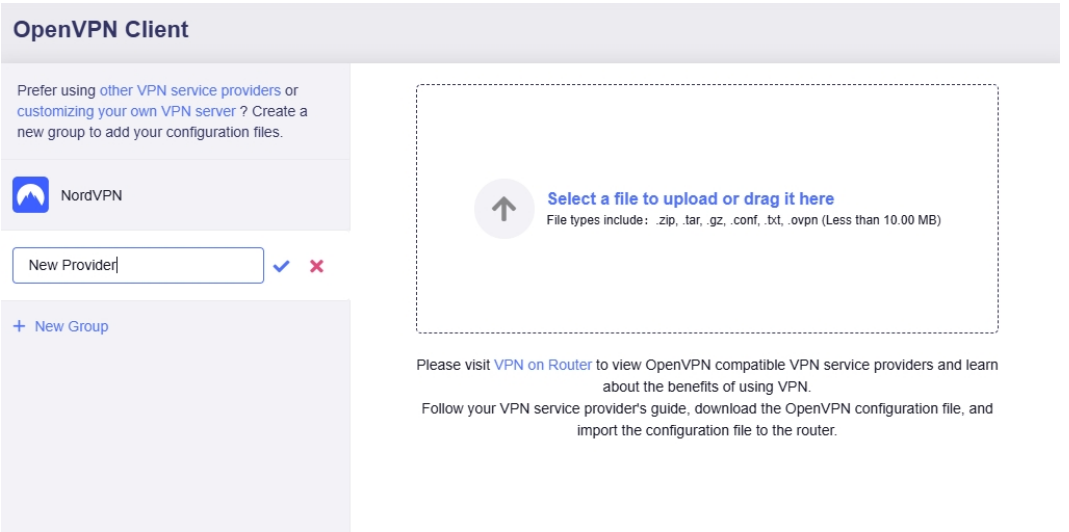
Si votre fournisseur OpenVPN n’est pas intégré à notre interface, récupérez d’abord le fichier de configuration sur son site officiel. Importez-le ensuite sur le routeur pour configurer le client OpenVPN.

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

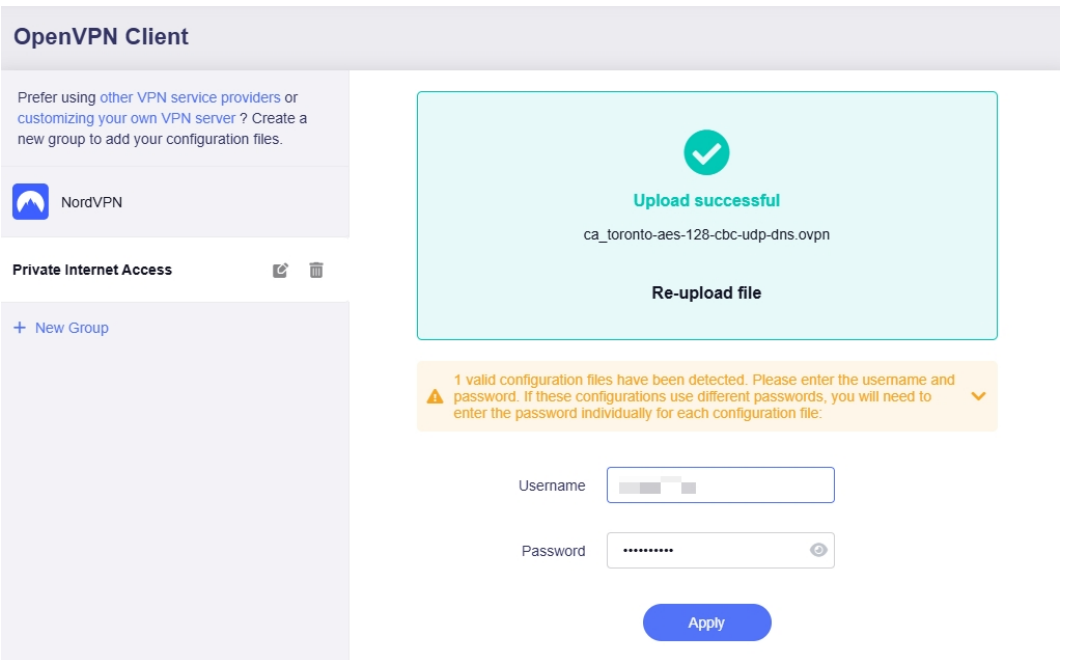
1. Téléchargez un fichier de configuration sur le site officiel de Private Internet Access.
2. Dans l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)**, puis cliquez sur **Ajouter manuellement (Add Manually)**.



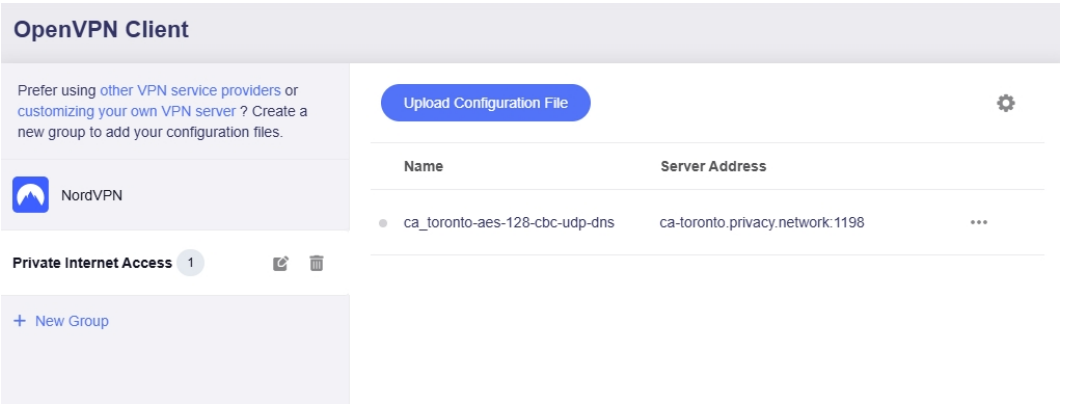
3. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



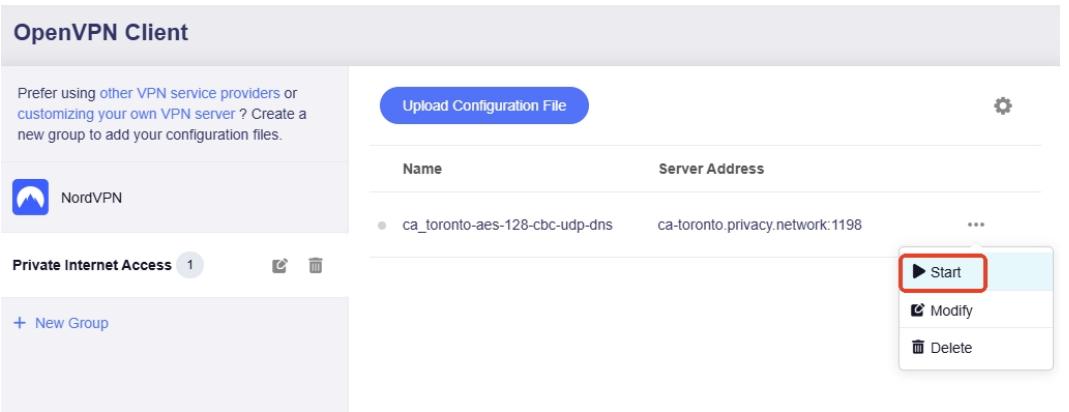
4. Importez votre fichier de configuration OpenVPN. Saisissez les identifiants si nécessaire, puis cliquez sur **Appliquer (Apply)**.



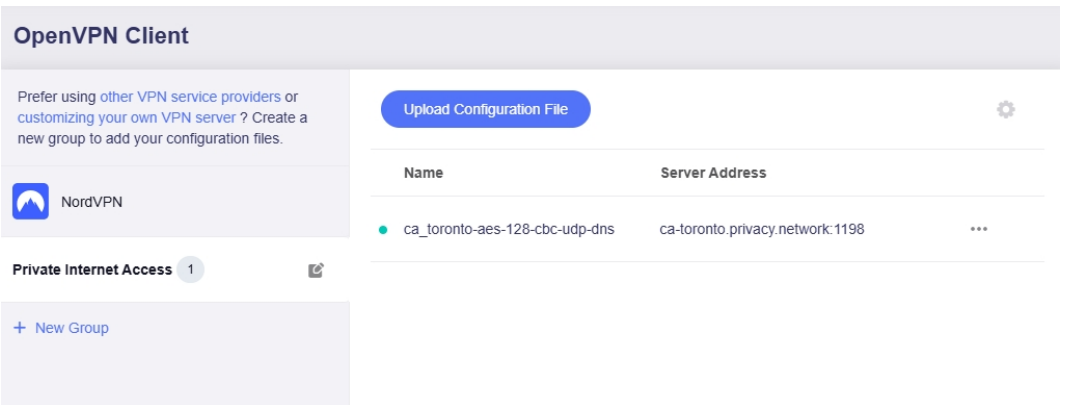
Le fichier importé apparaît dans la liste.



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)**.

10.2 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.

10.2.1 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.

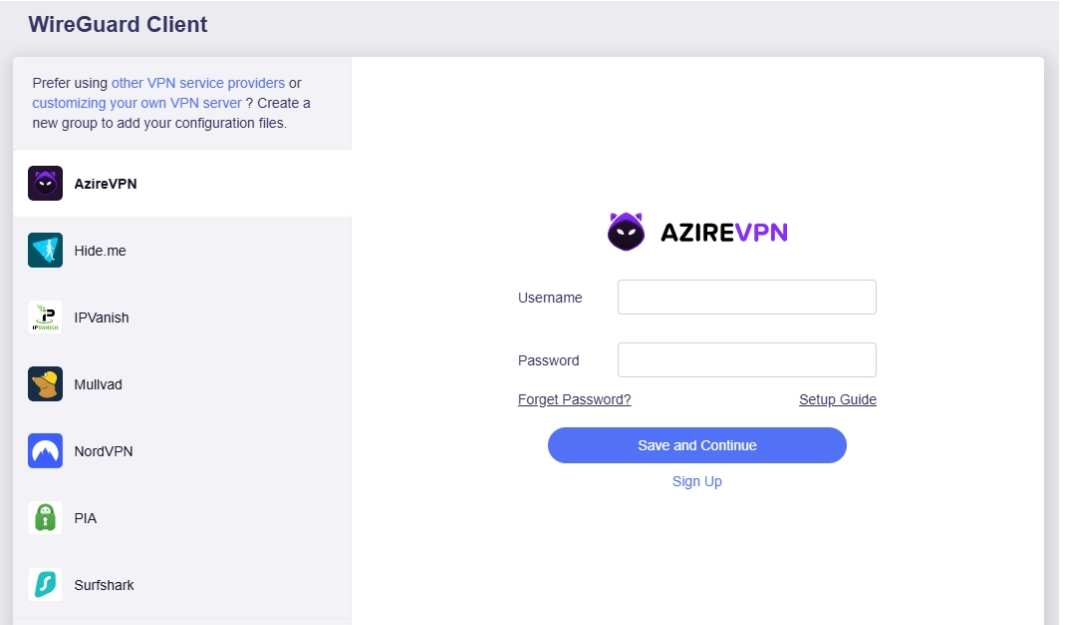
Sélectionnez ensuite votre fournisseur ci-dessous pour accéder directement aux instructions détaillées.

- 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

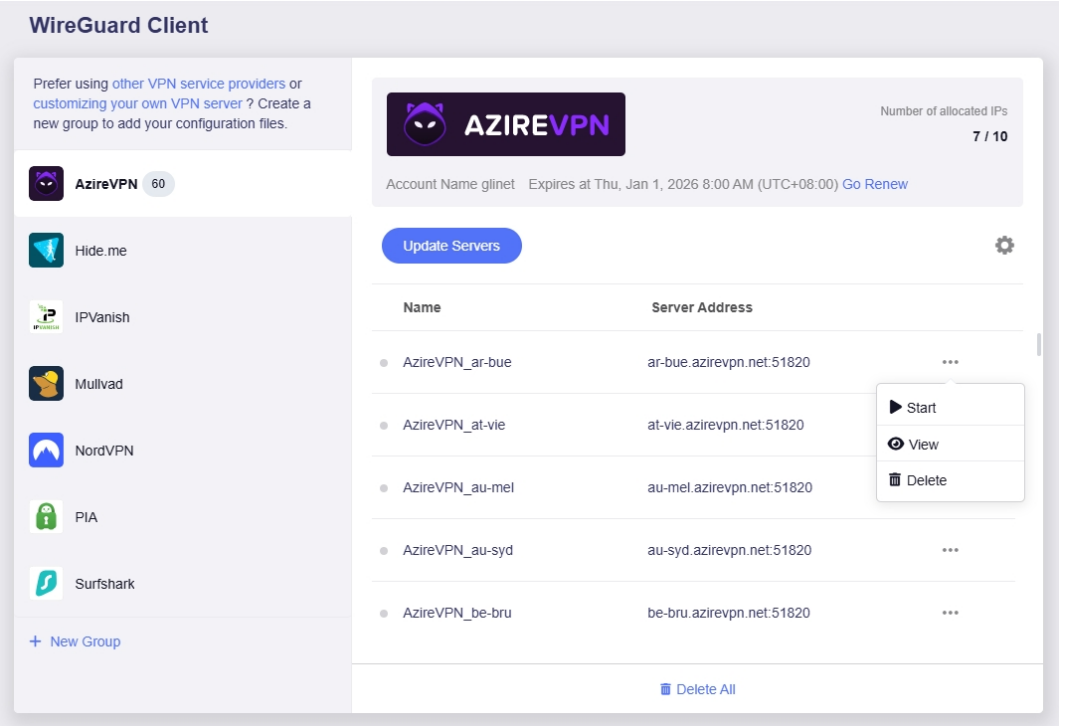
10.2.2 Configuration d’AzireVPN

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

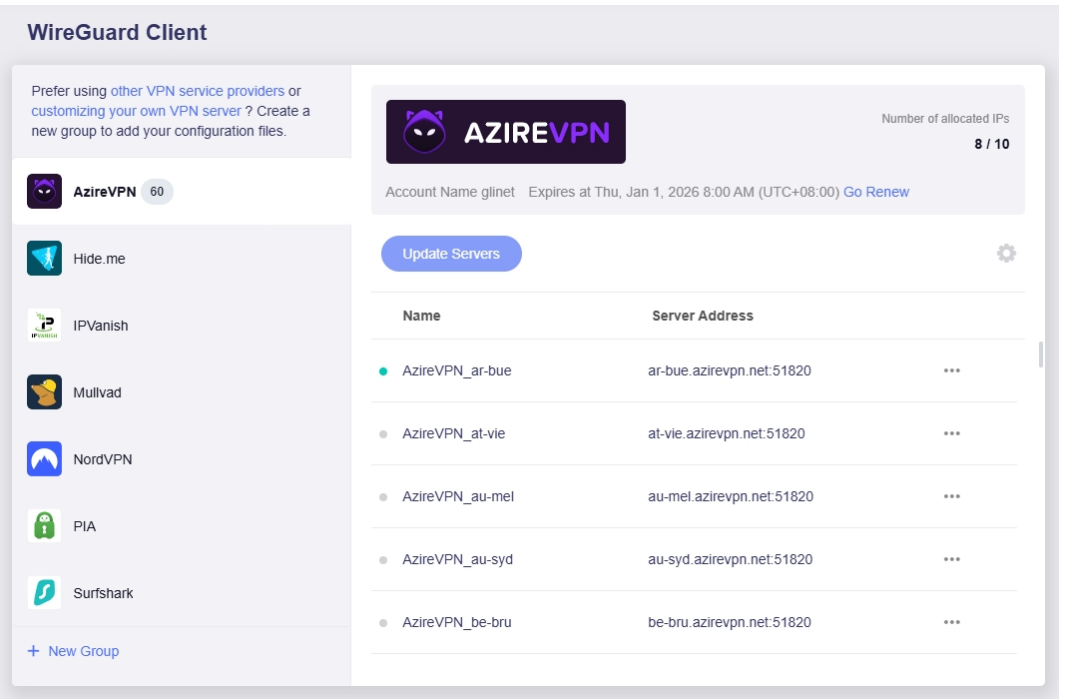
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **AzireVPN**.
2. Saisissez l’identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



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



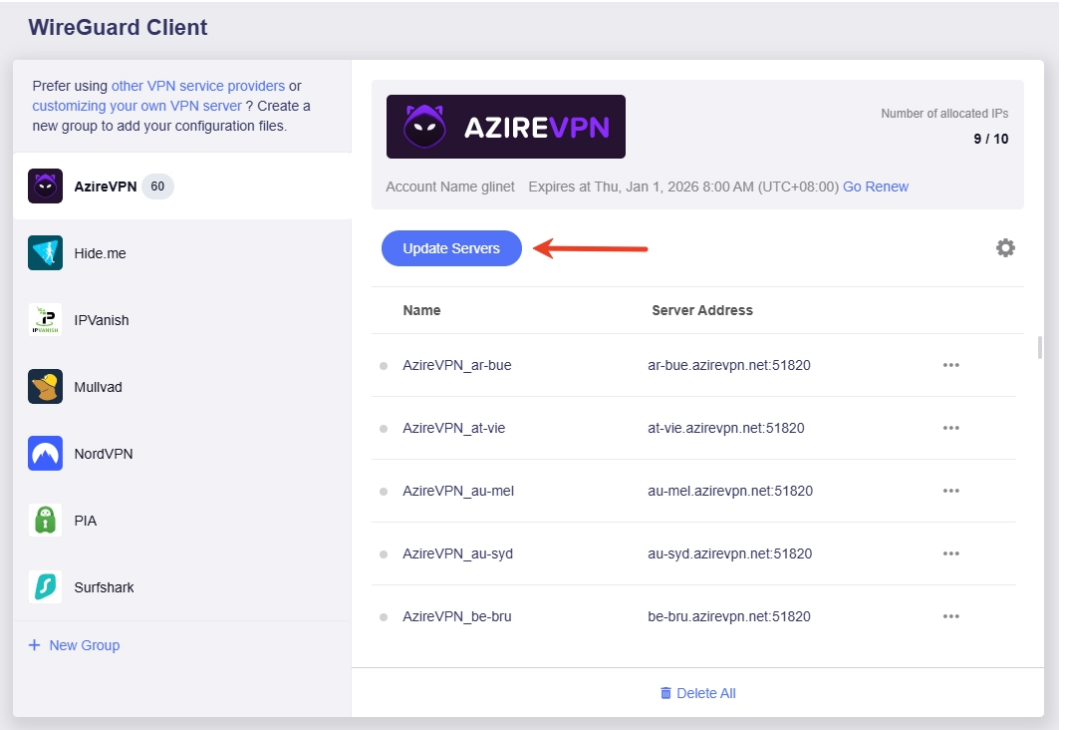
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



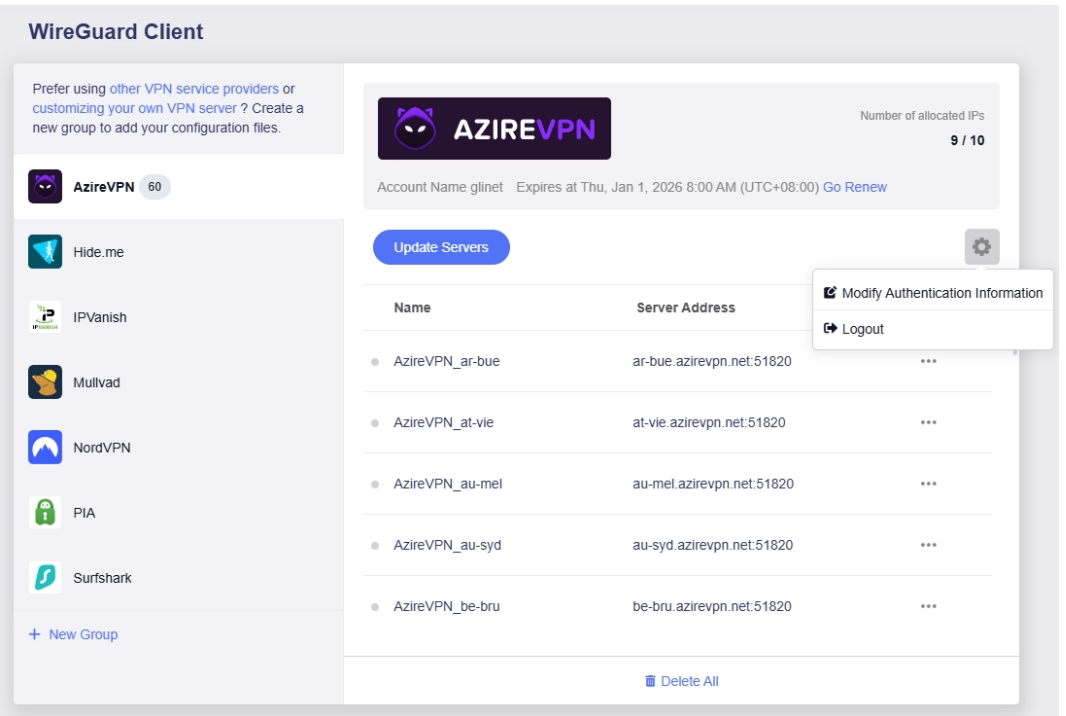
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

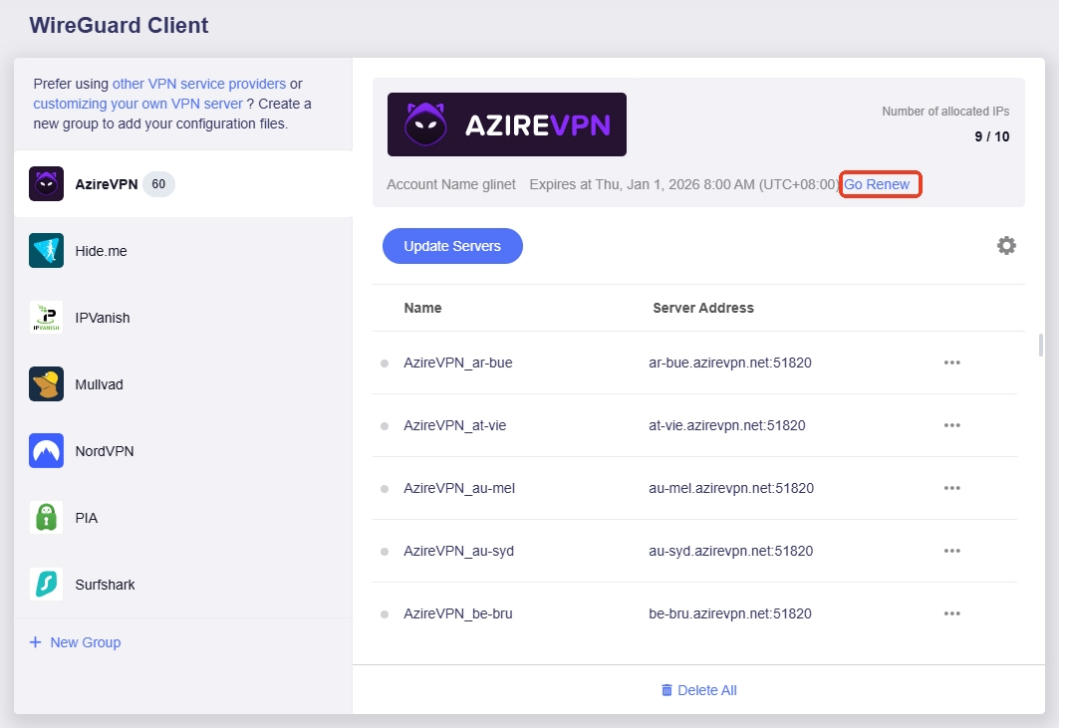


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.

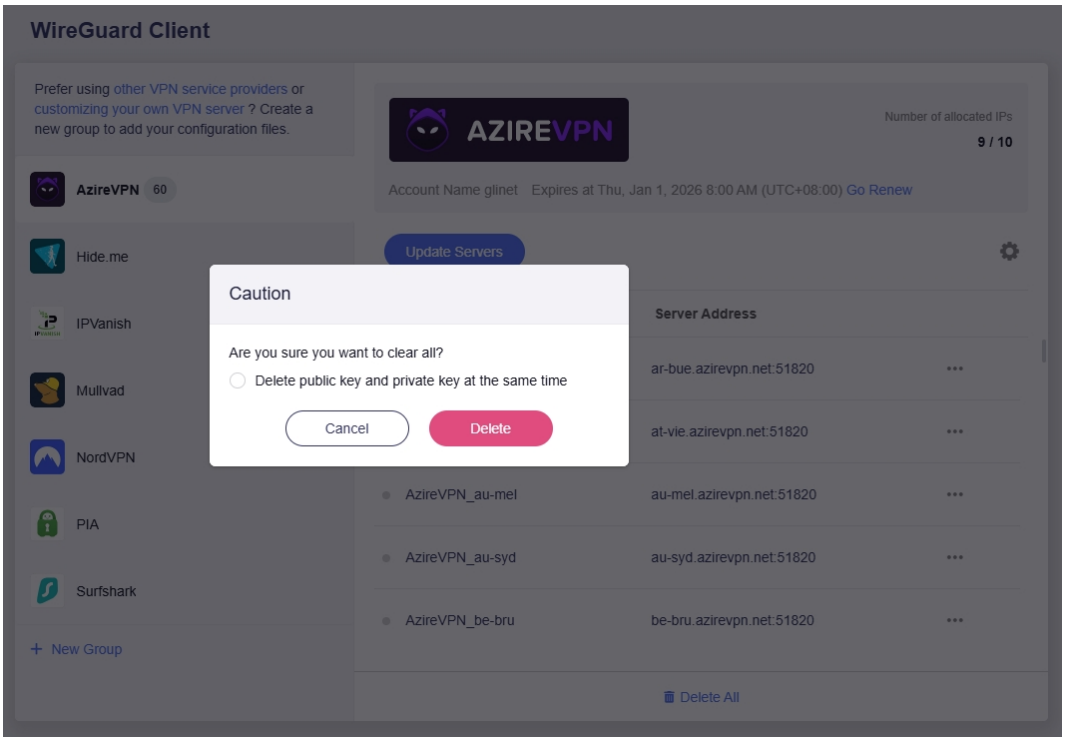


7. Renouvelez l'abonnement.

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



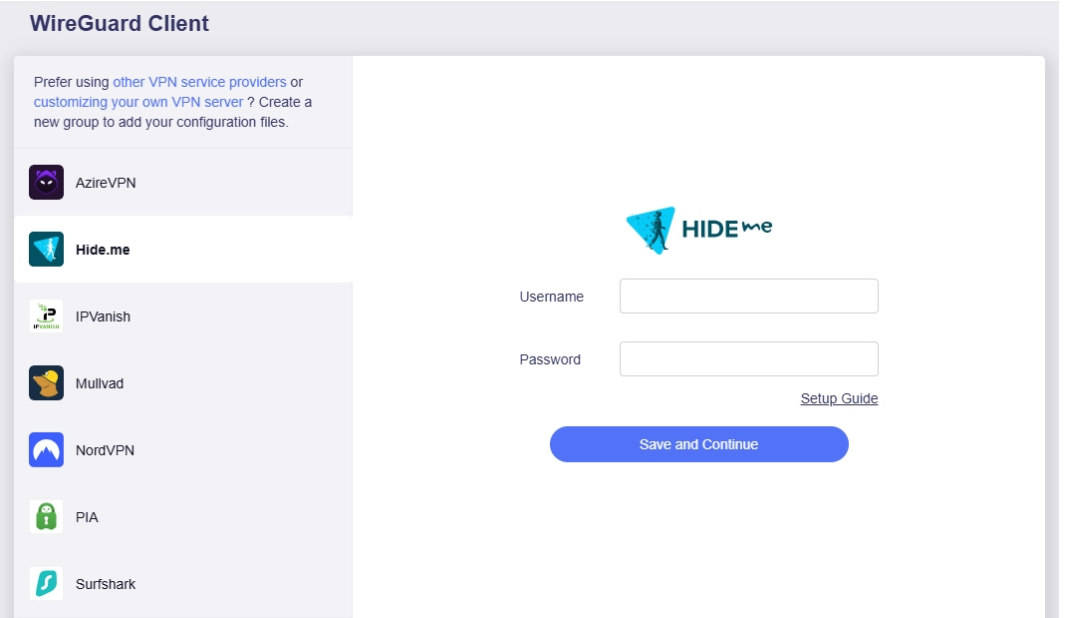
8. Supprimez tous les fichiers.
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.


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

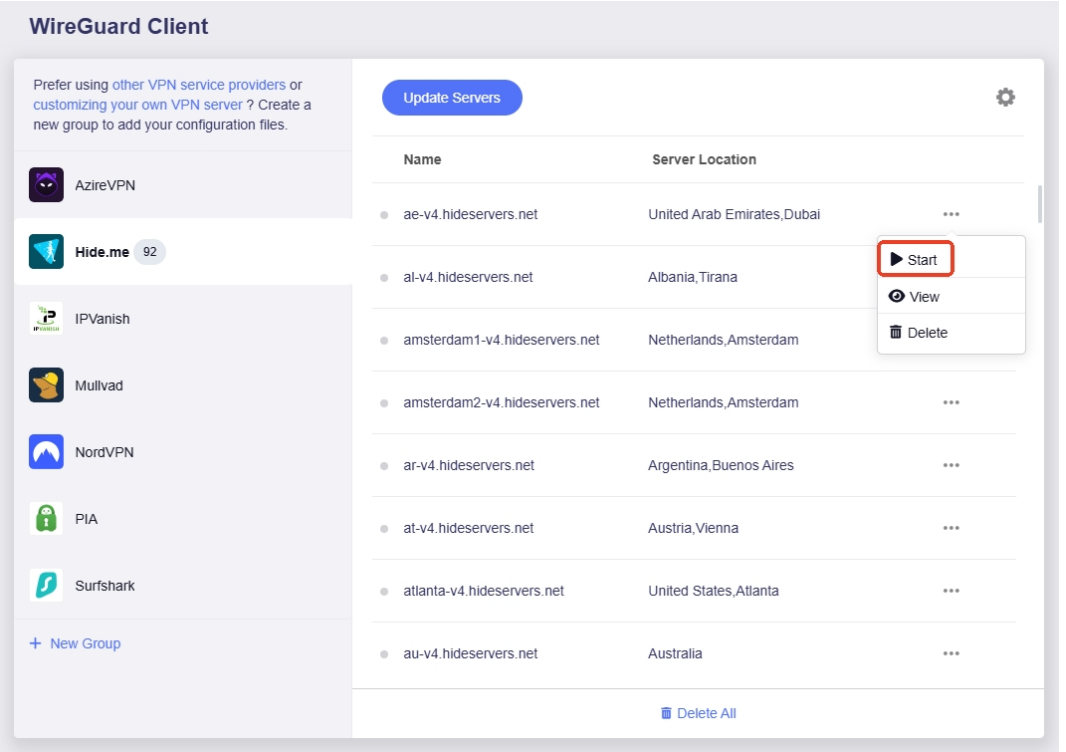
10.2.3 Configuration de Hide.me

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

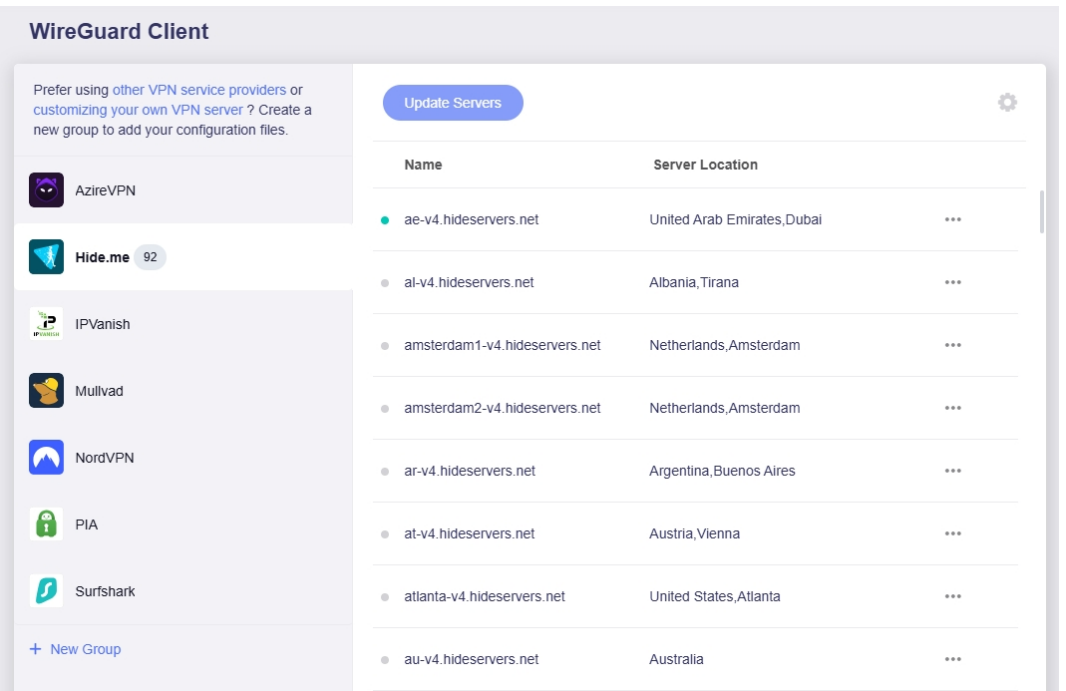
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Hide.me**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



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



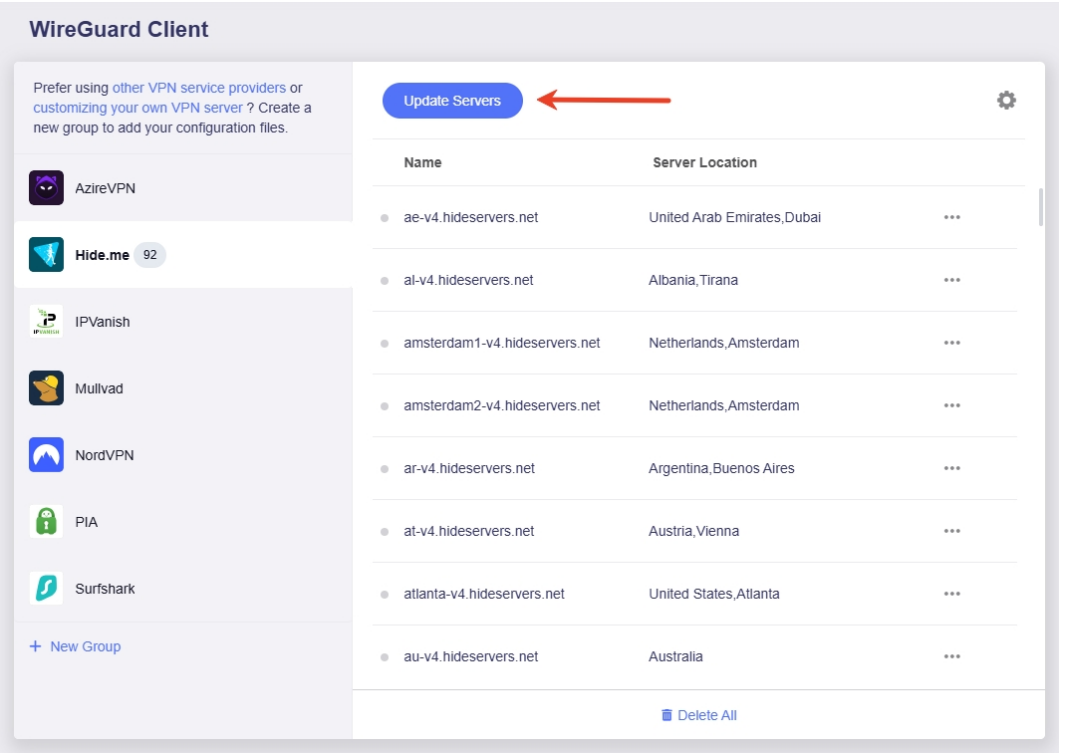
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



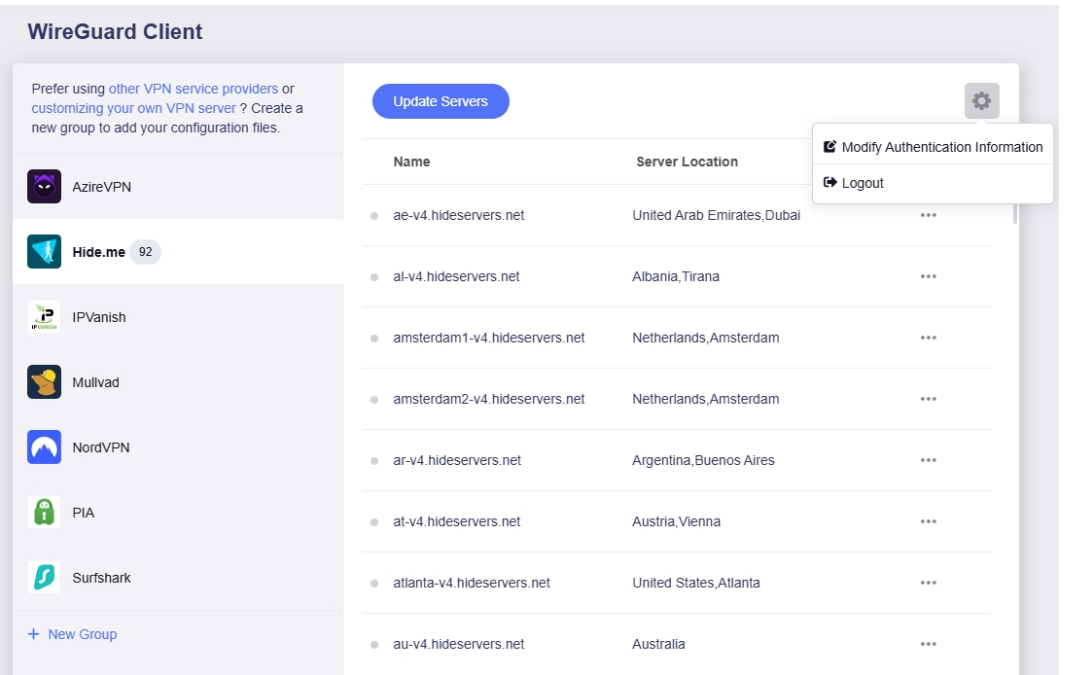
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

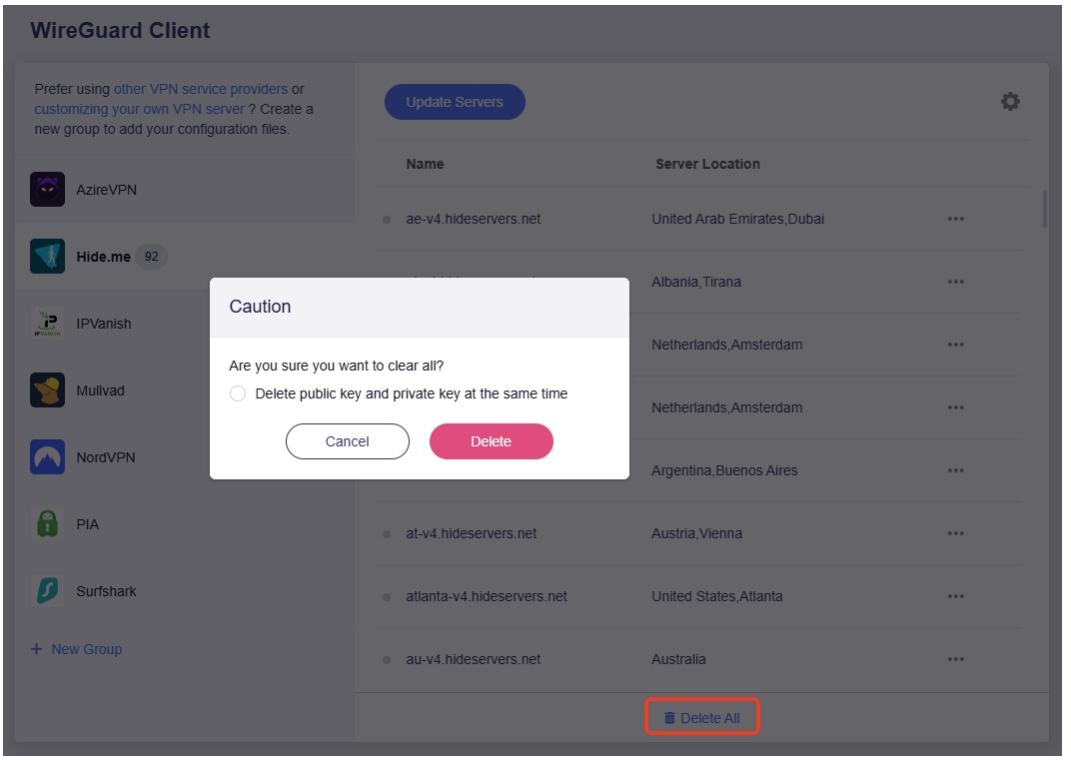


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



7. Supprimez tous les fichiers.

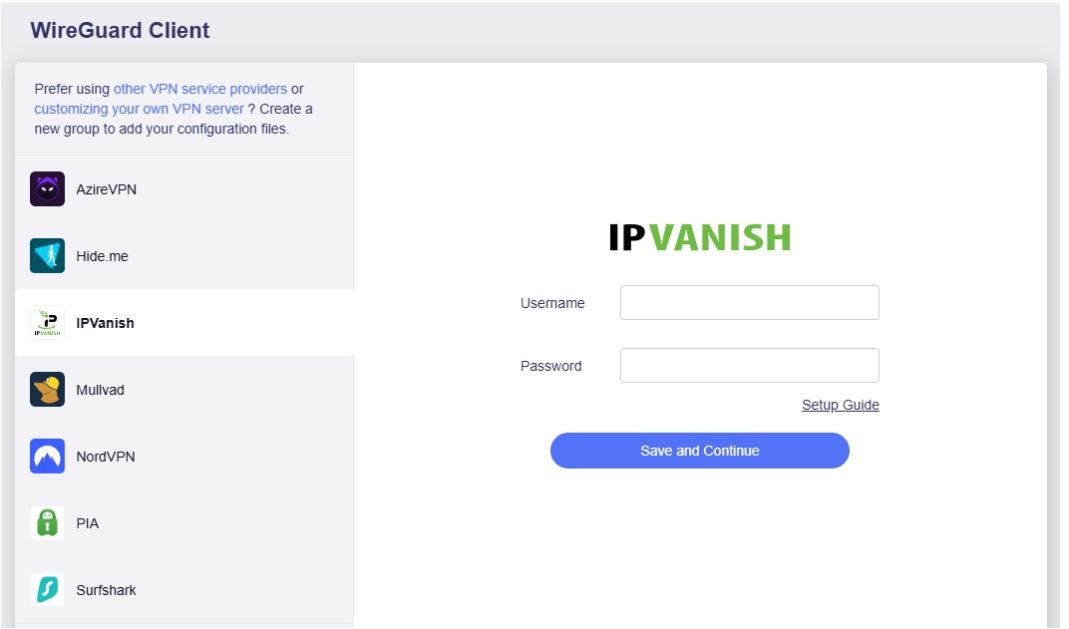
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



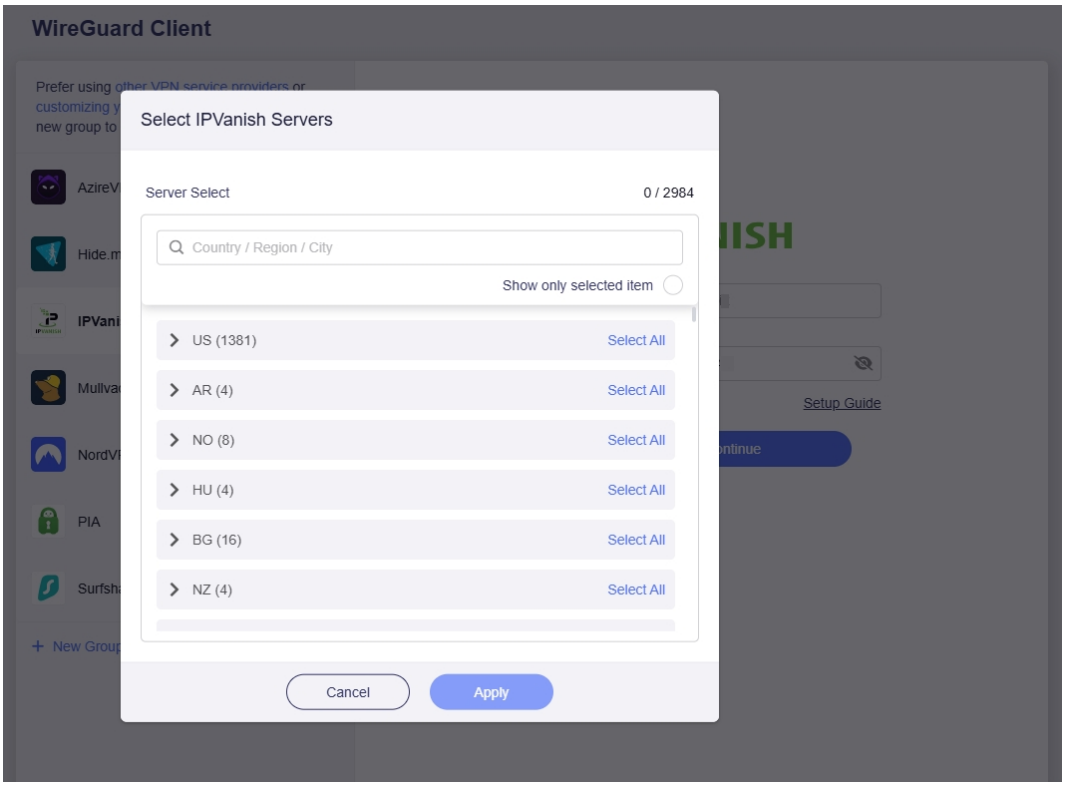
10.2.4 Configuration d'IPVanish

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

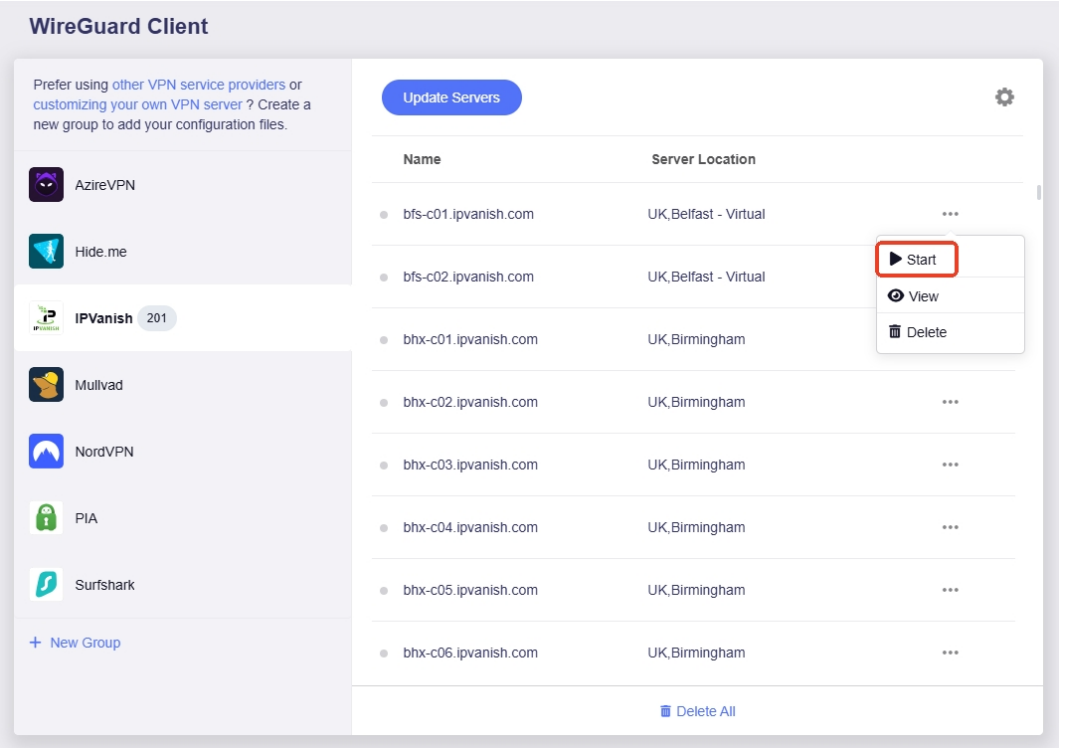
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **IPVanish**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



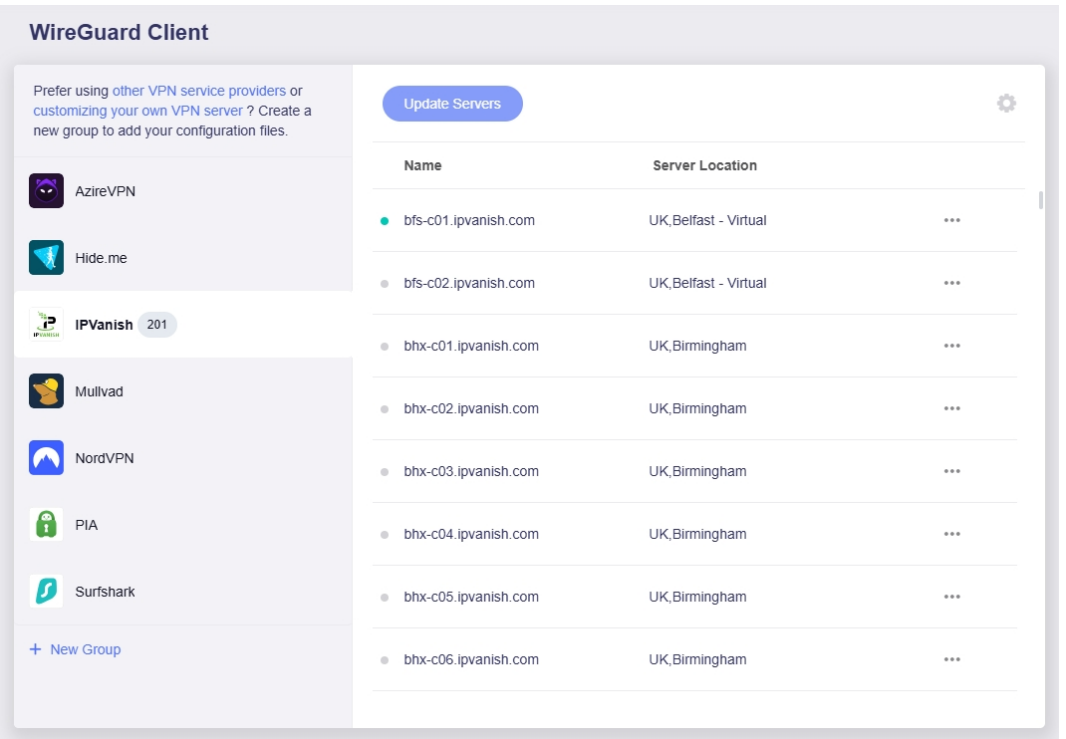
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



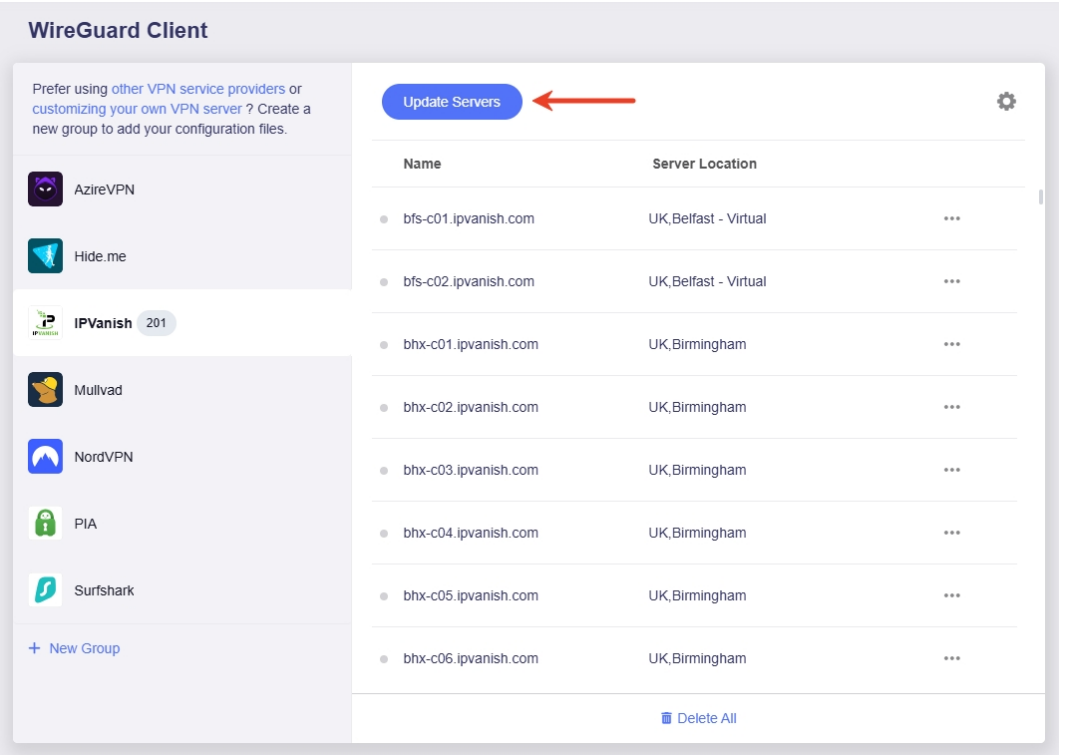
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



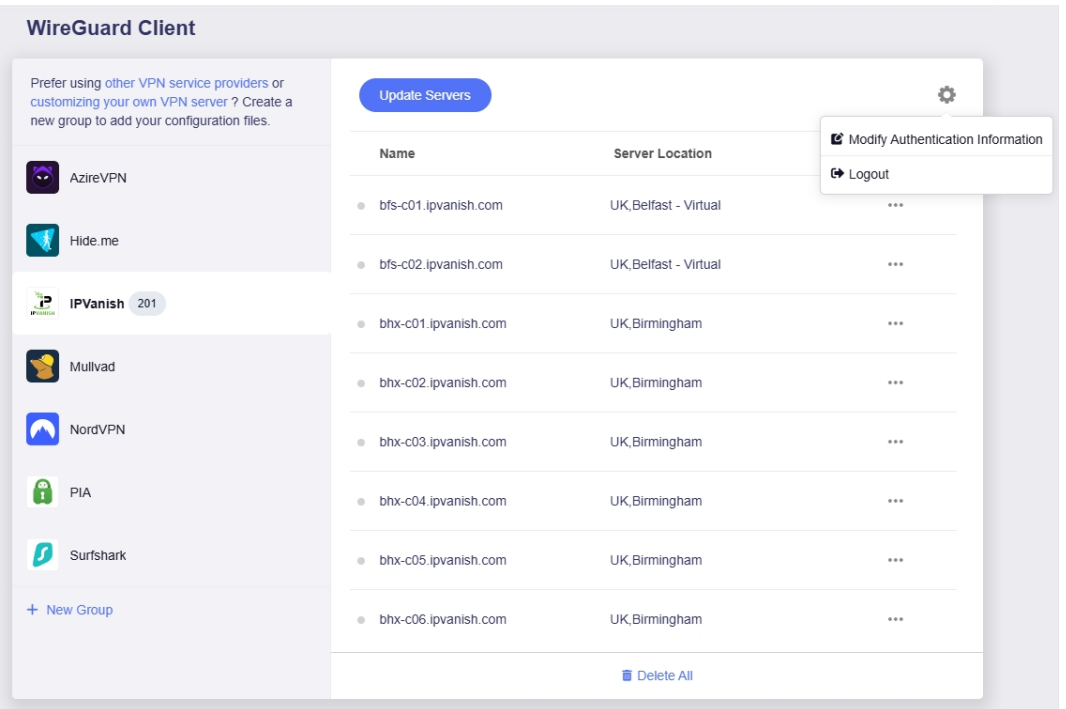
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

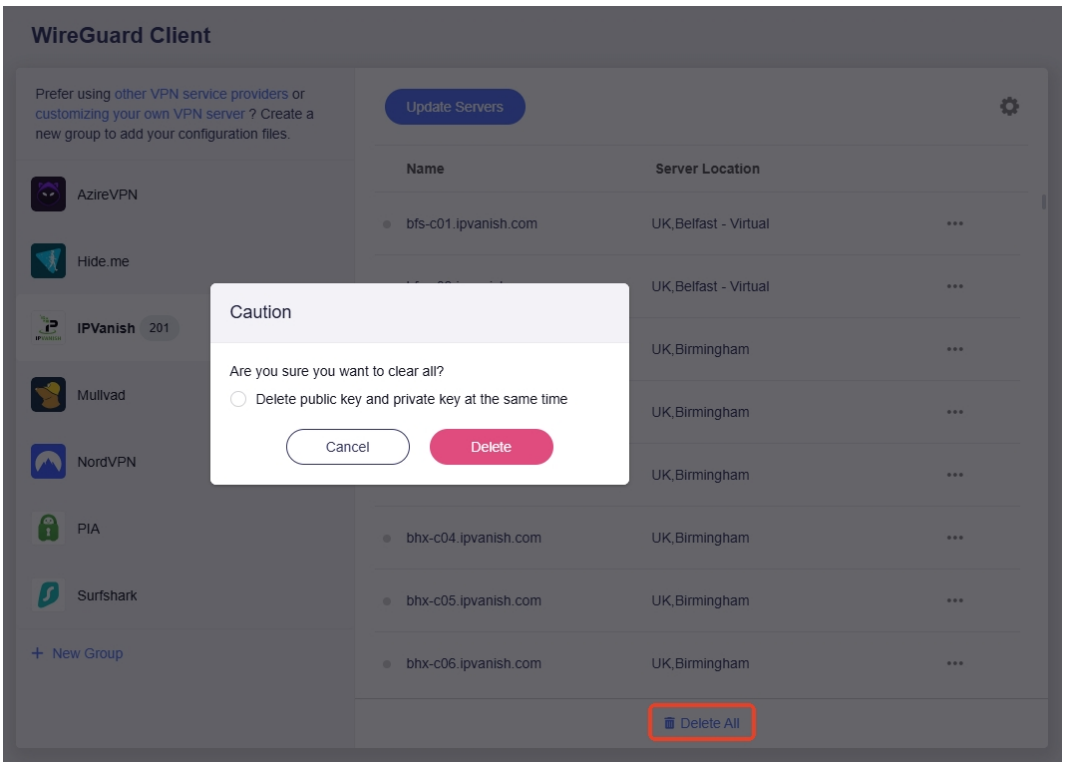


7. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

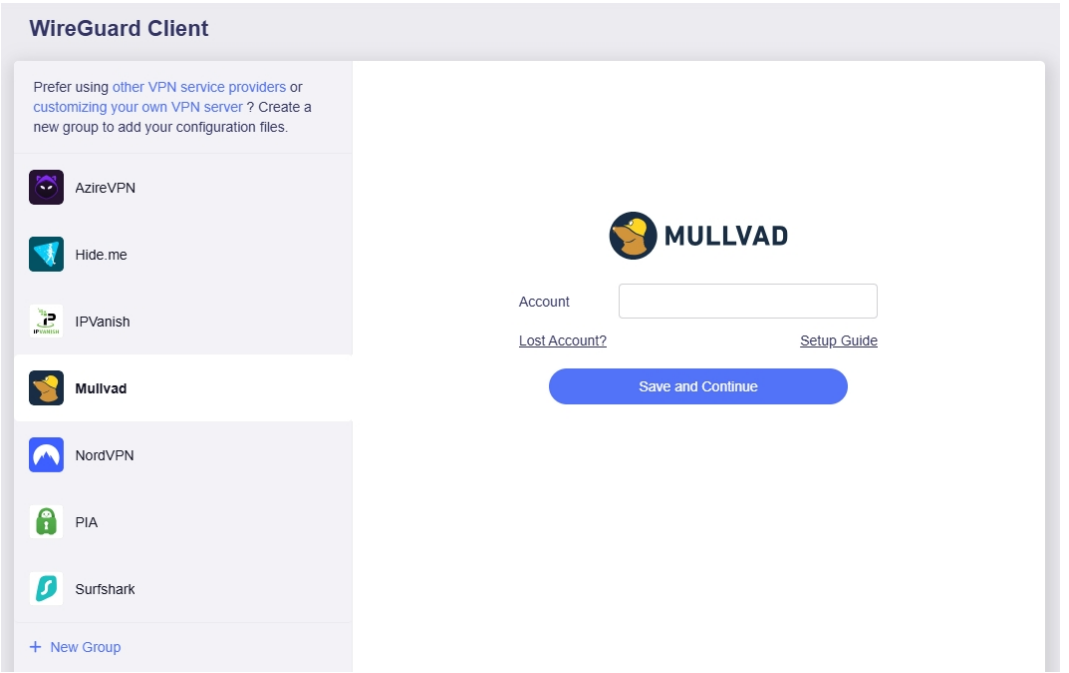
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



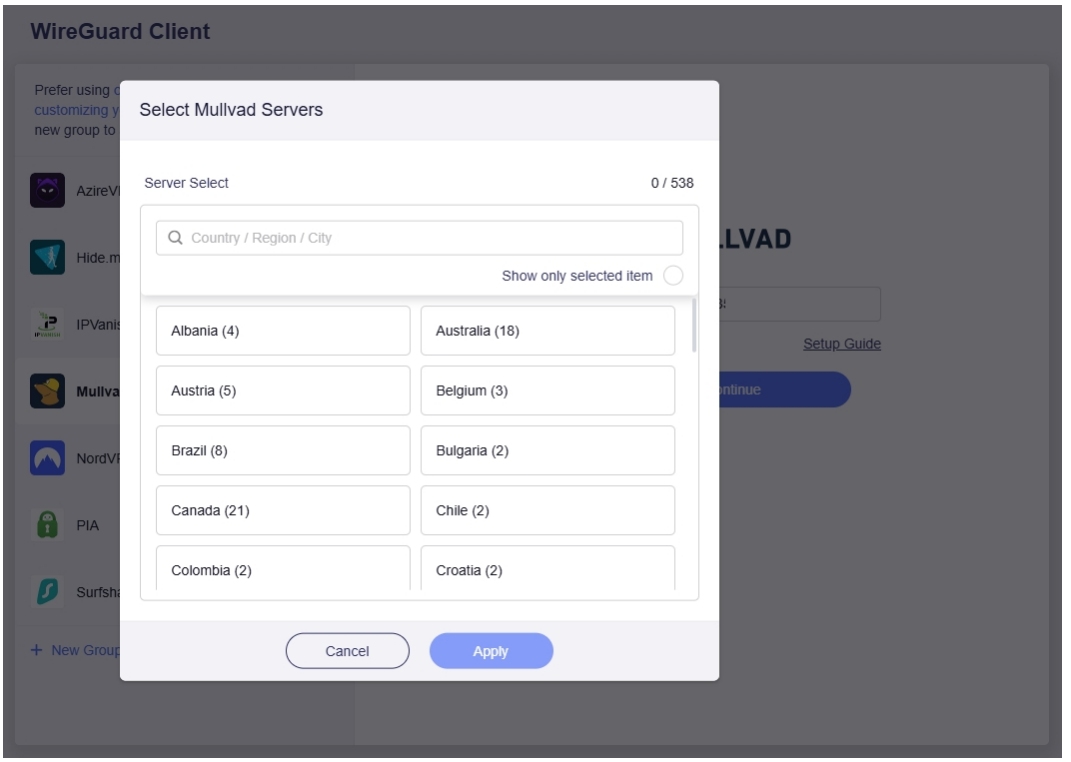
10.2.5 Configuration de Mullvad

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

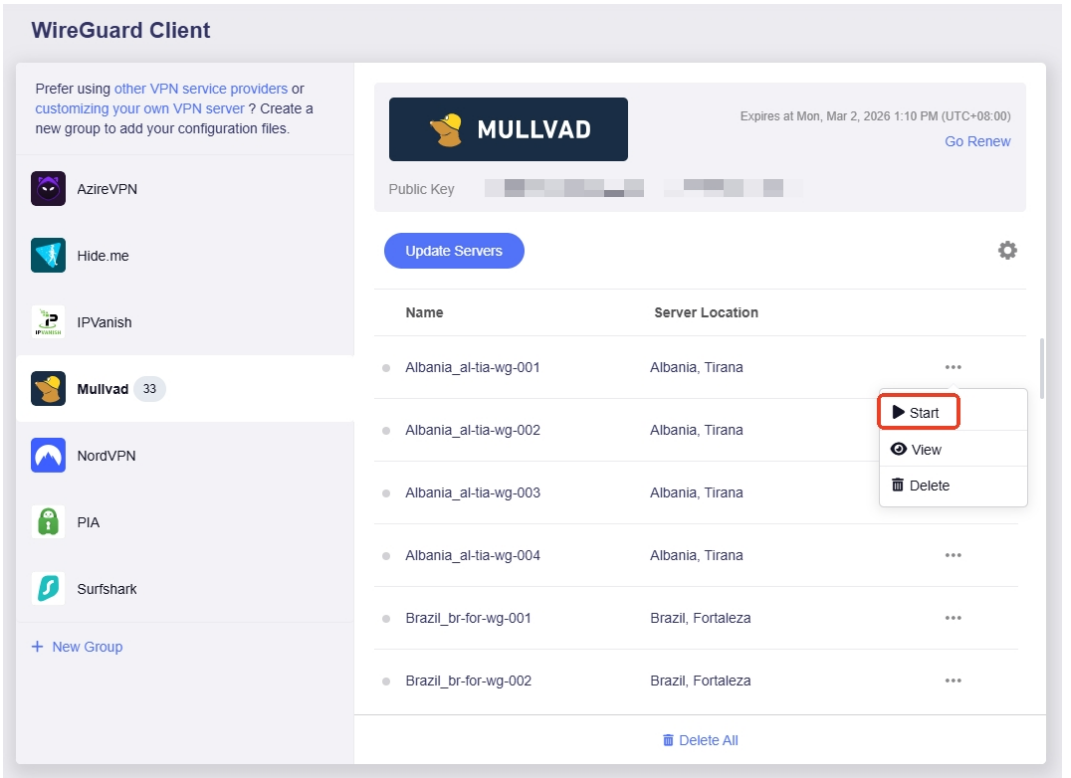
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Mullvad**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



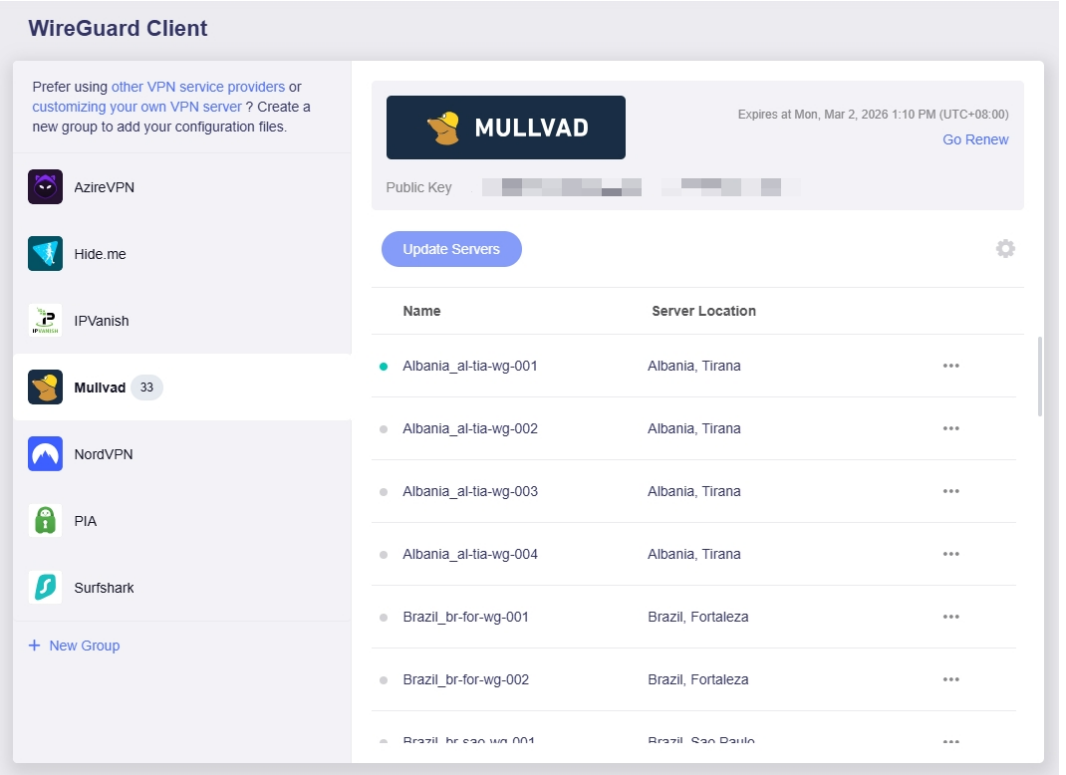
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



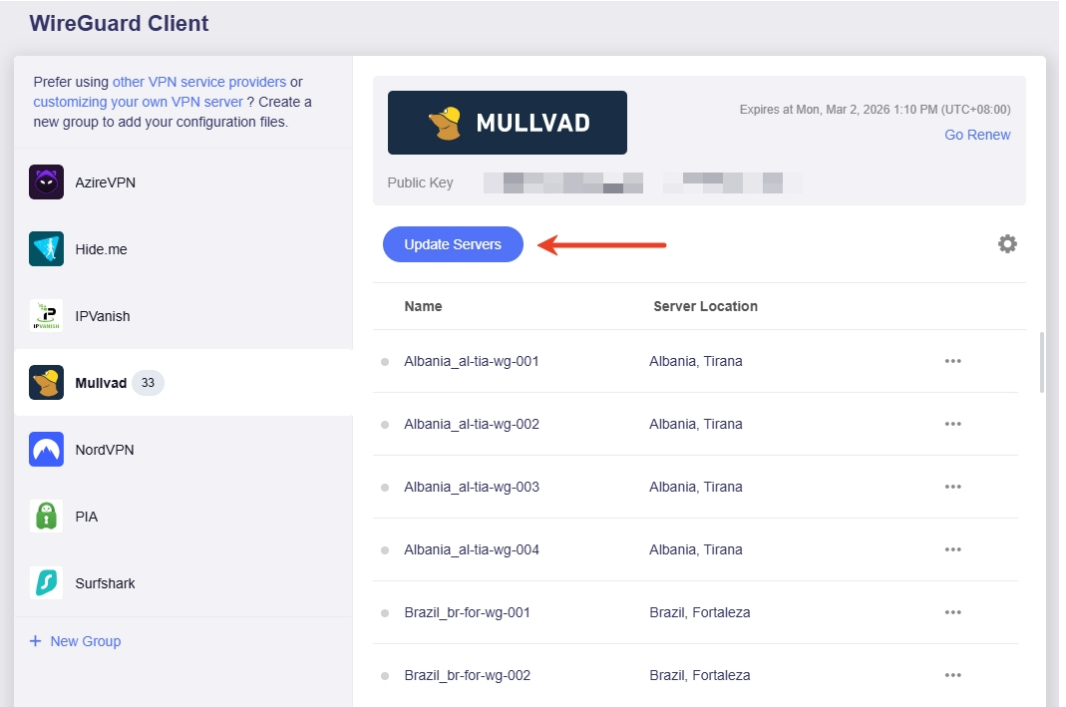
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

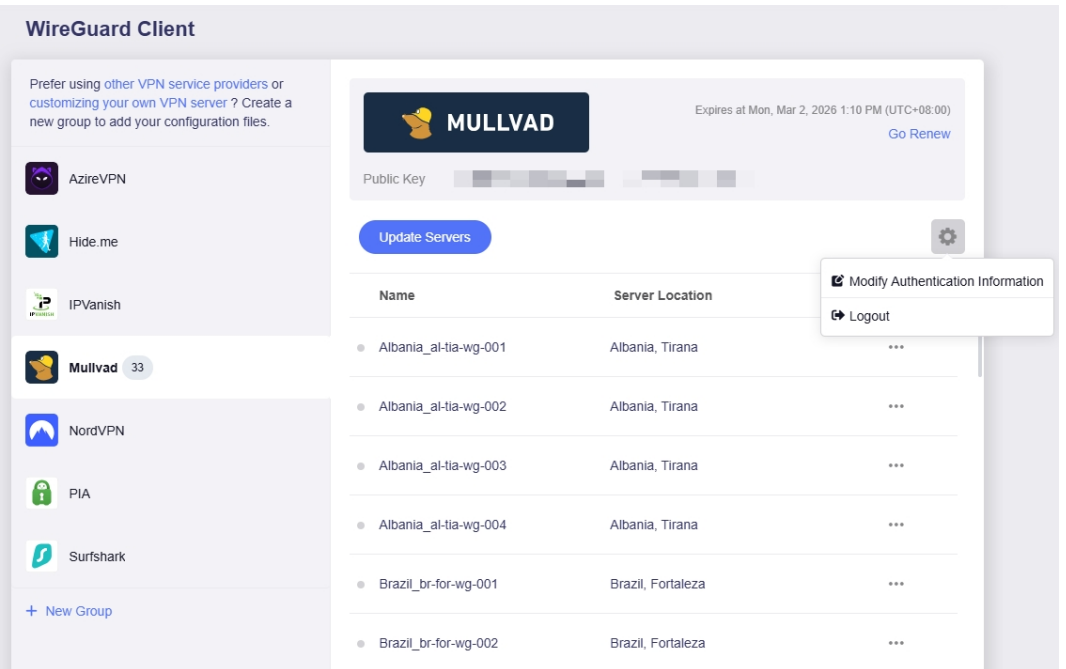
6. Mettez à jour les serveurs.

   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.



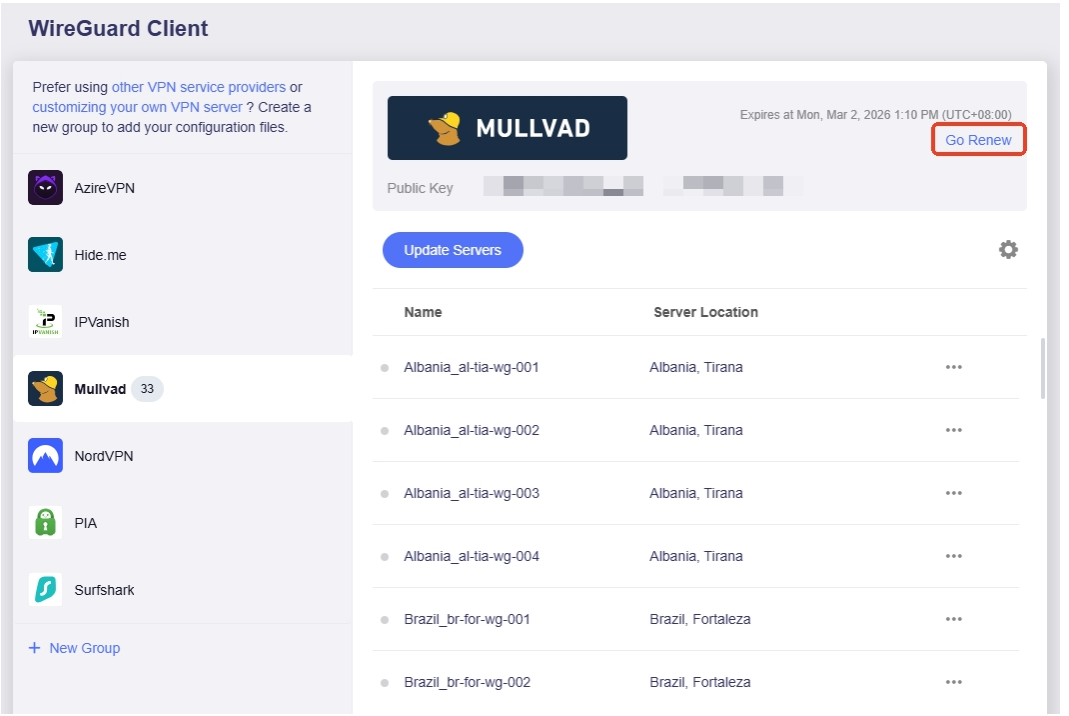
7. Modifiez les identifiants ou déconnectez-vous.

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



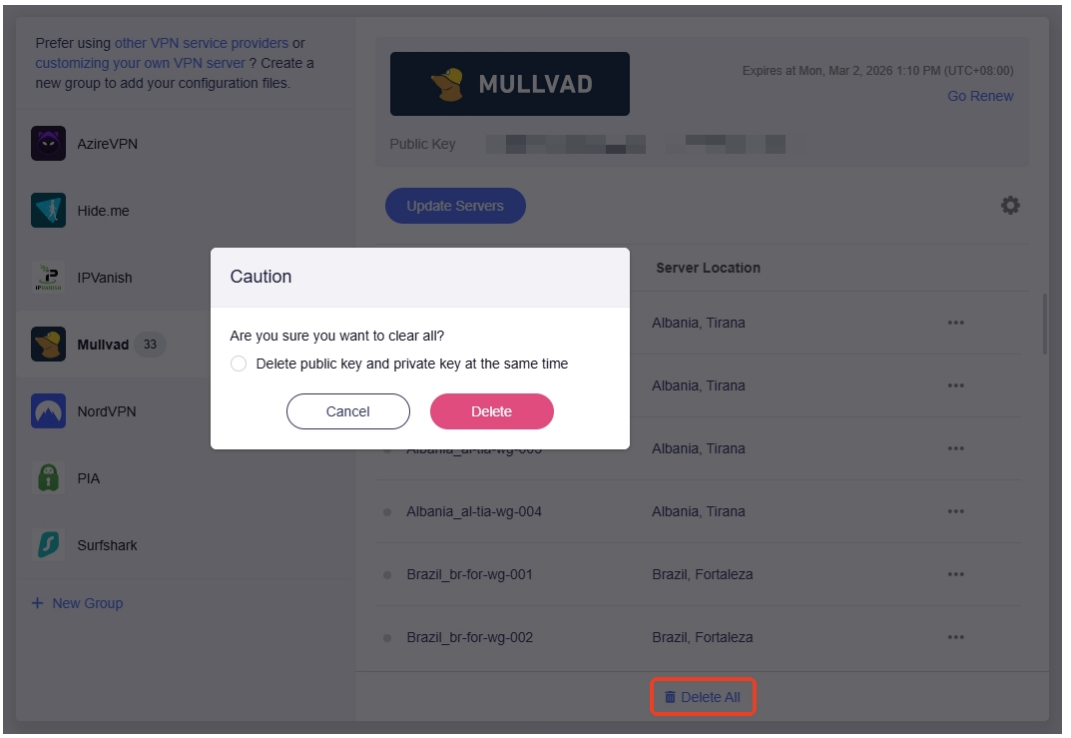
8. Renouvelez l’abonnement.

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



9. Supprimez tous les fichiers.

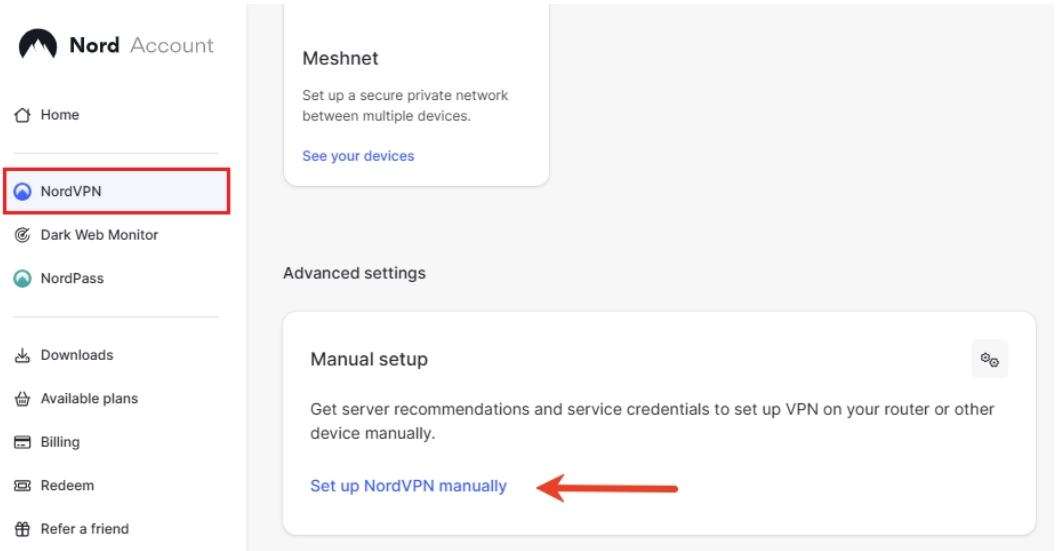
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



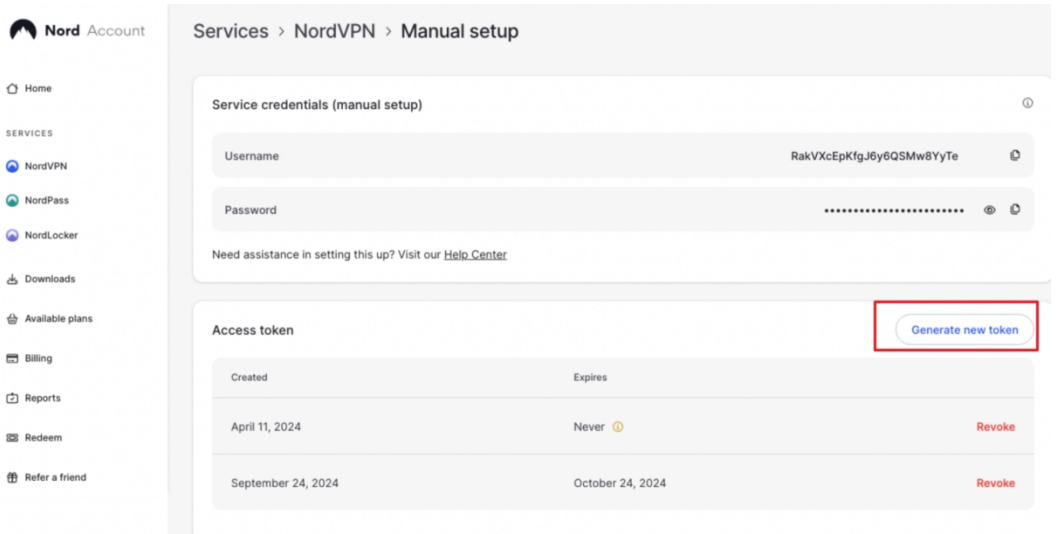
10.2.6 Configuration de NordVPN

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

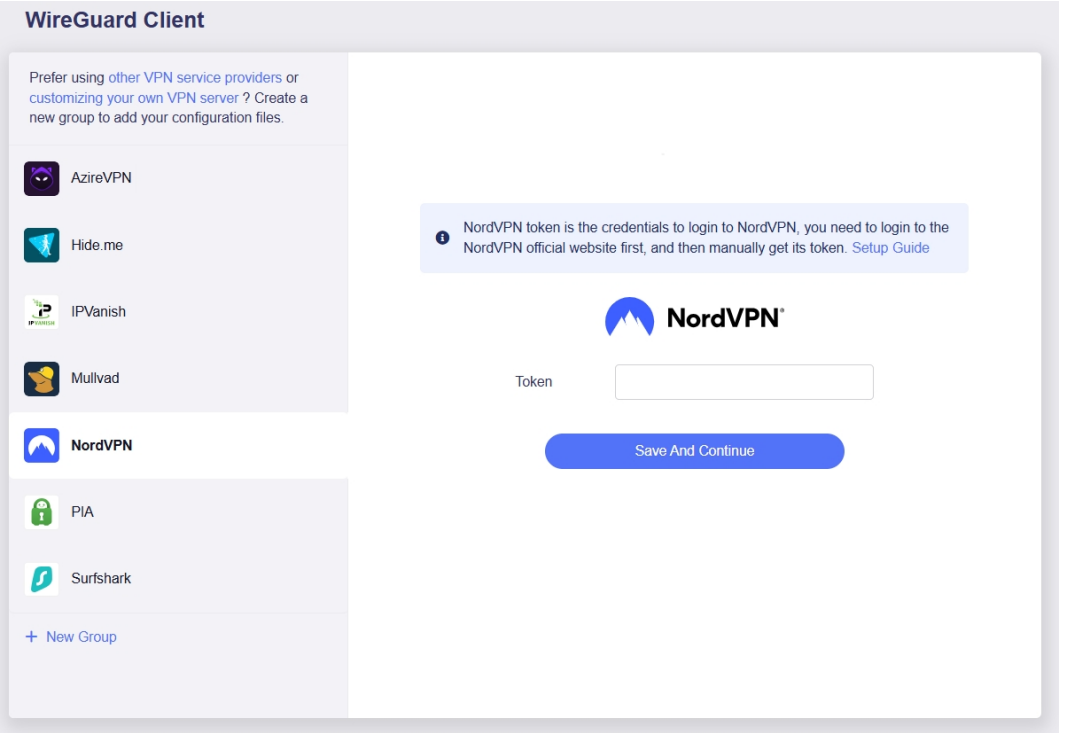
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



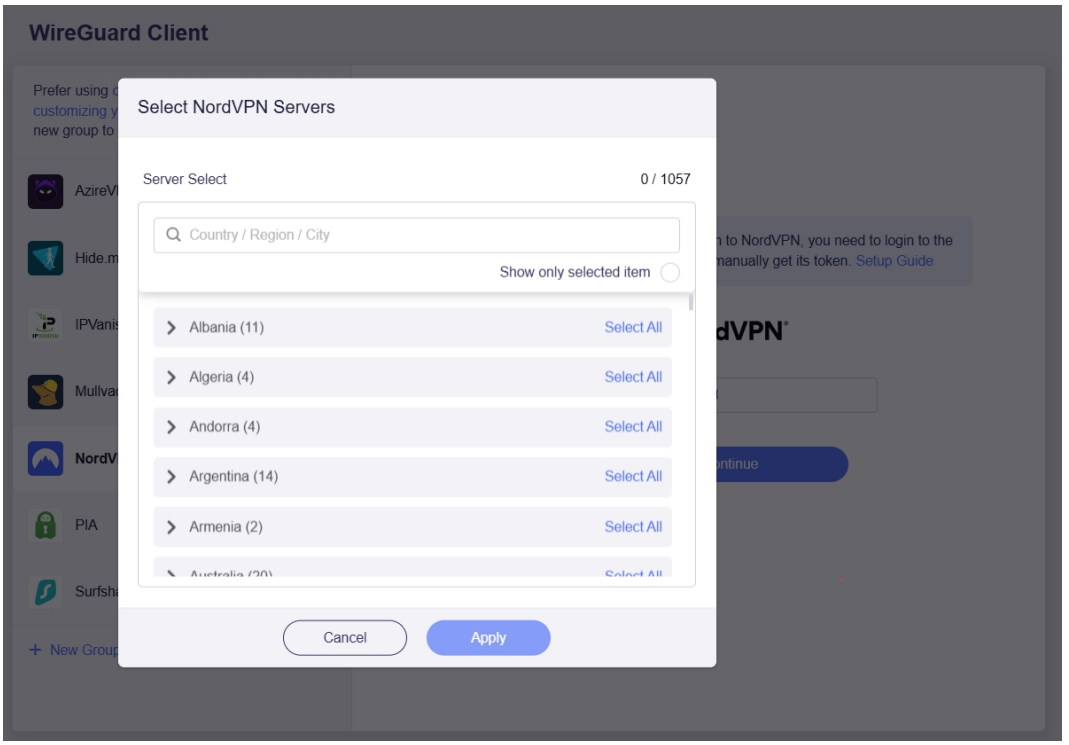
Repérez la section **Jeton d'accès (Access Token)**. Créez un jeton et copiez-le pour l'utiliser ensuite.



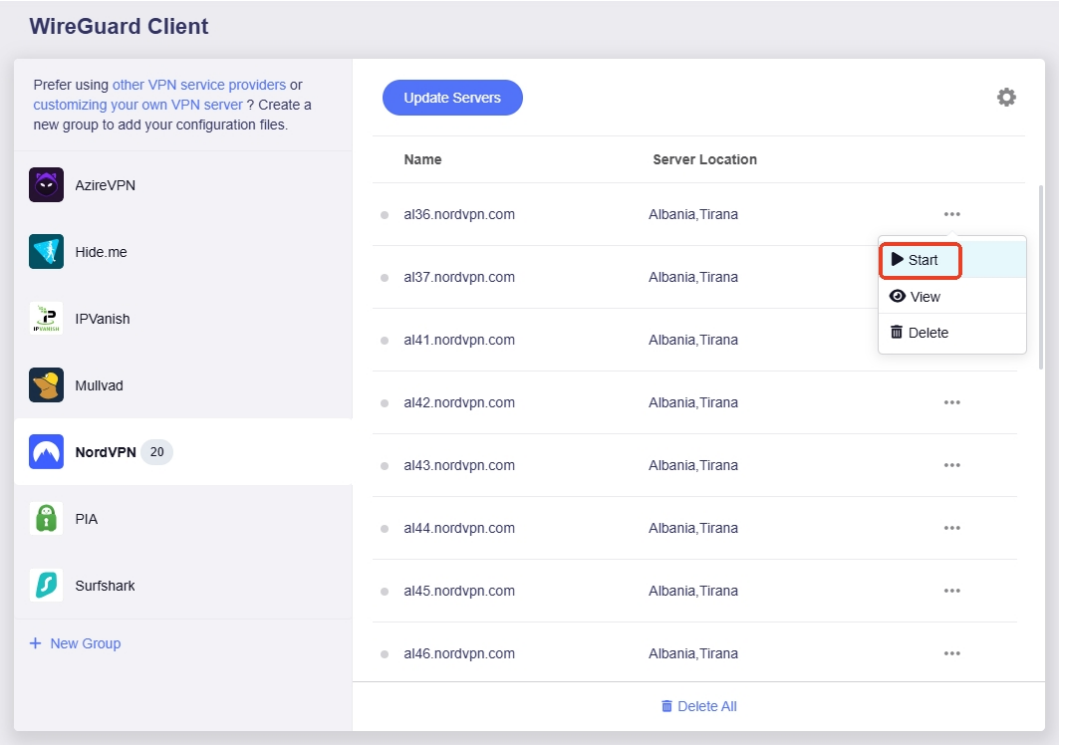
3. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **NordVPN**.
4. Saisissez le jeton et cliquez sur **Enregistrer et continuer (Save and Continue)**.



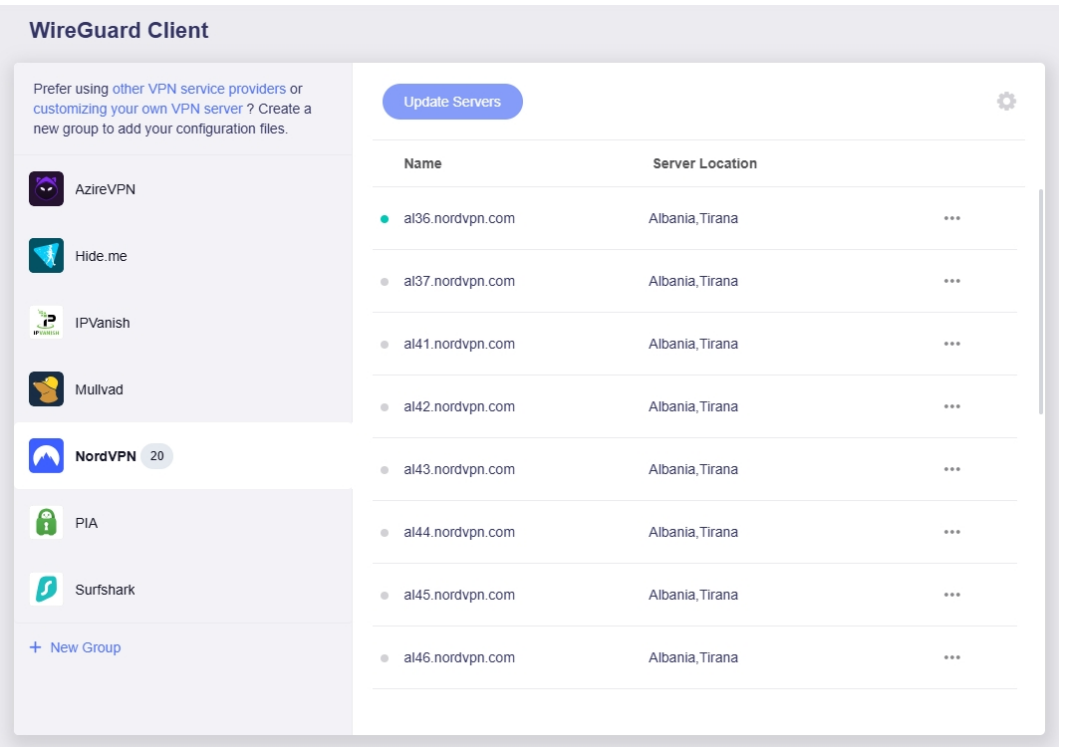
5. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



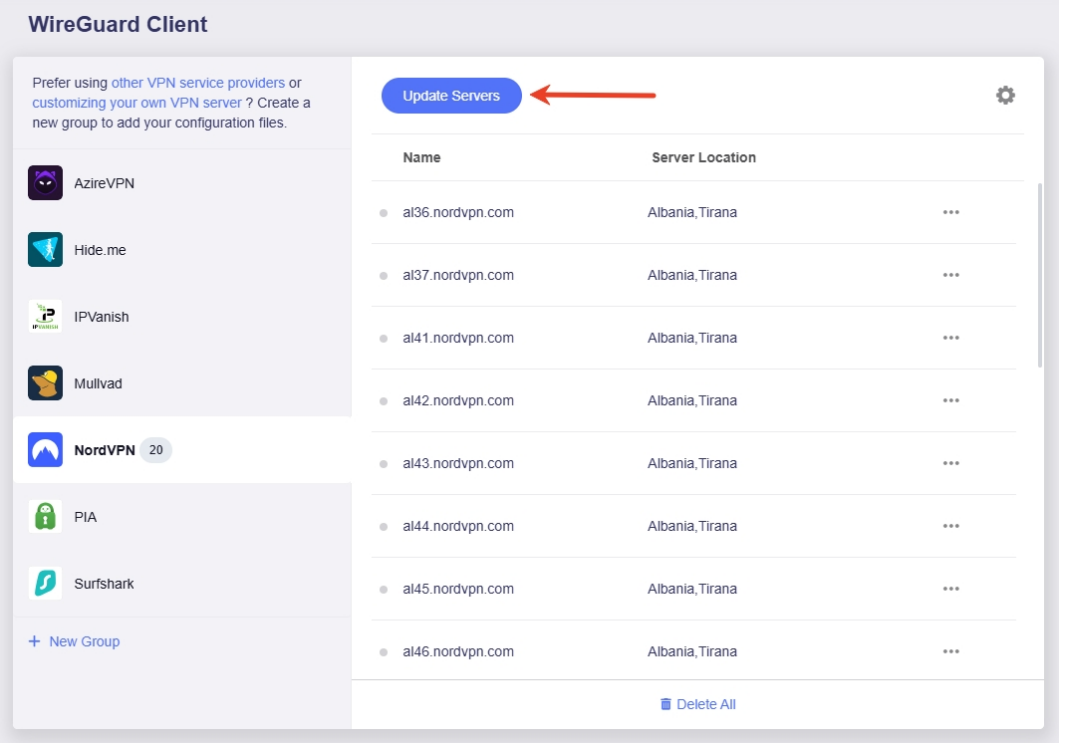
7. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



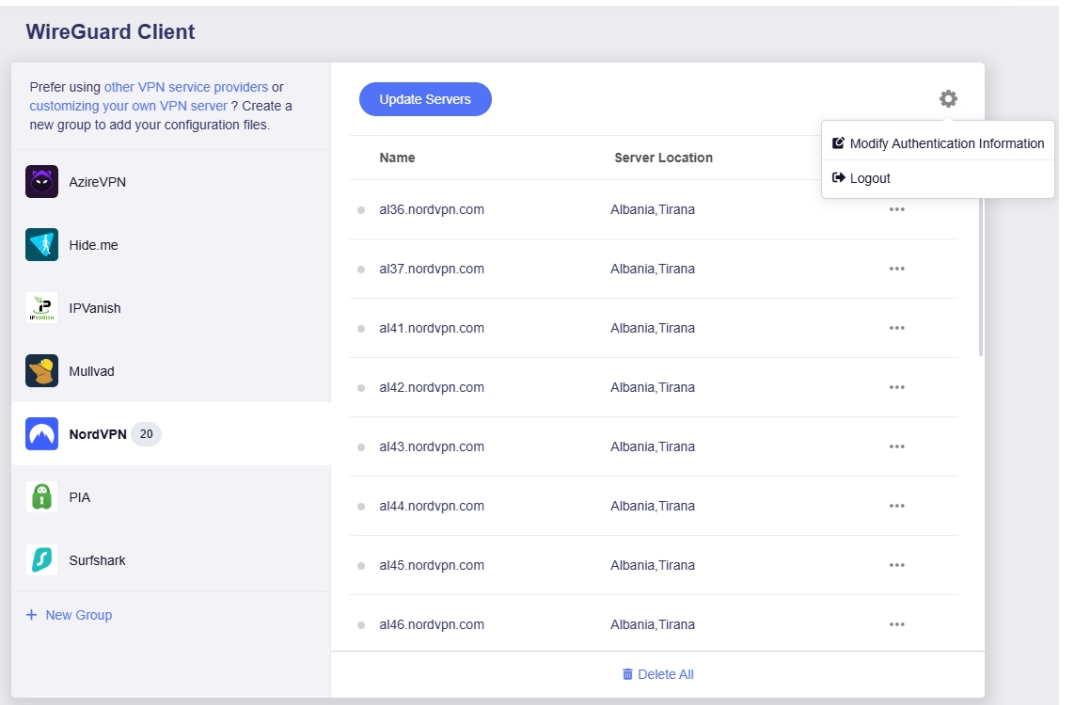
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.

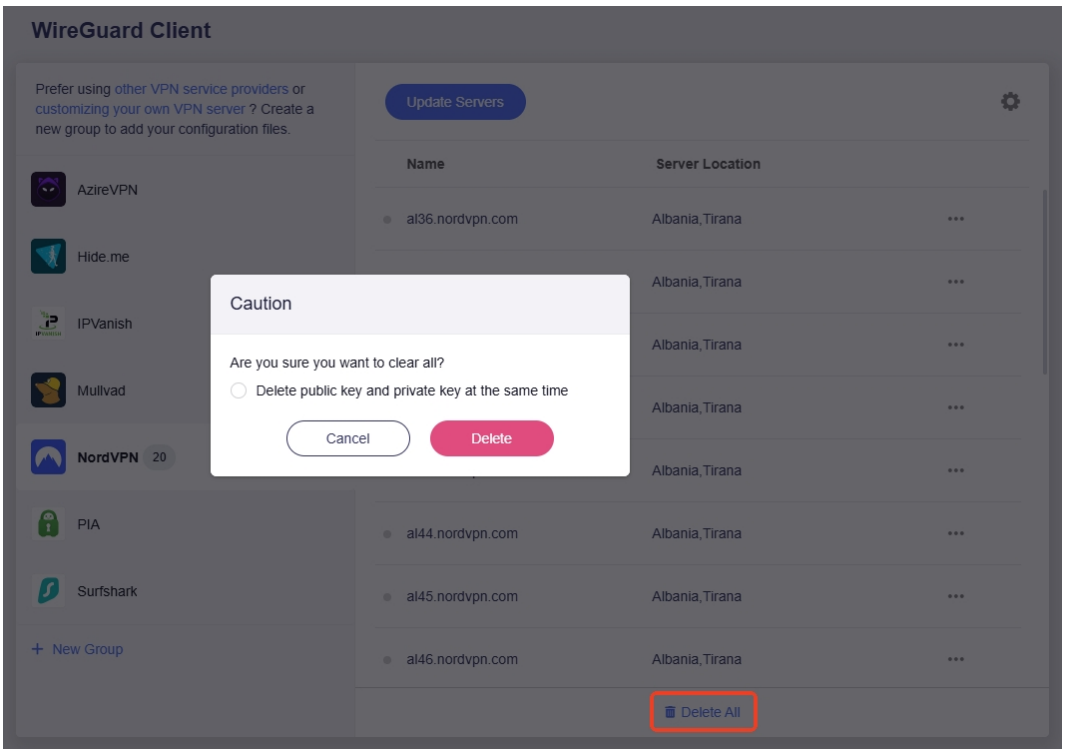


9. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



10. Supprimez tous les fichiers.

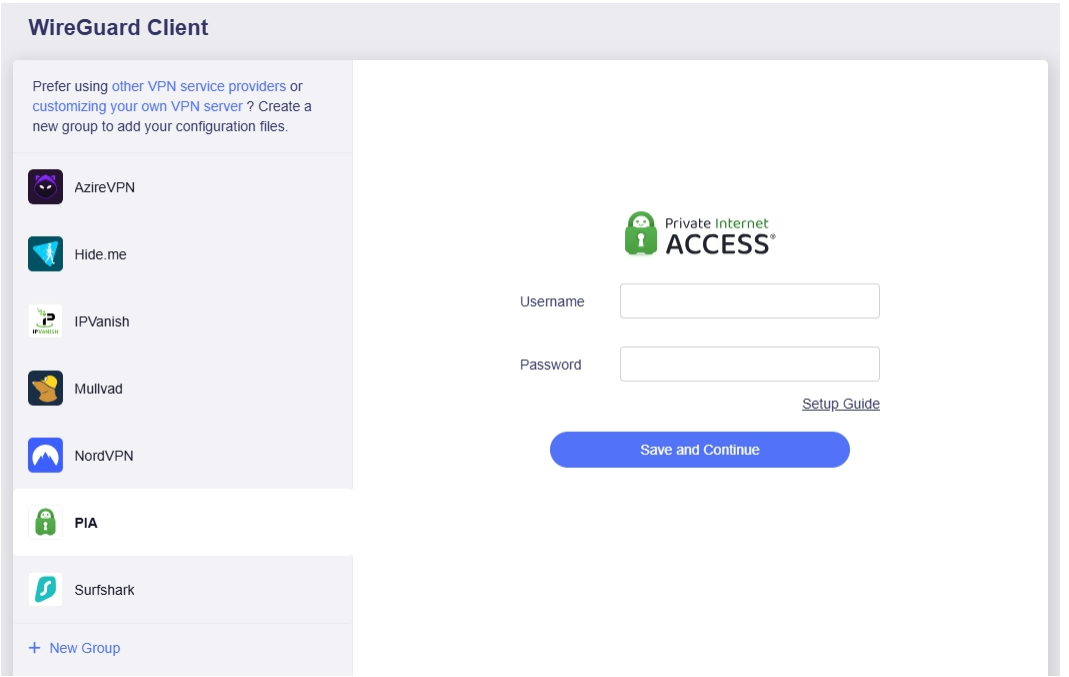
    Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



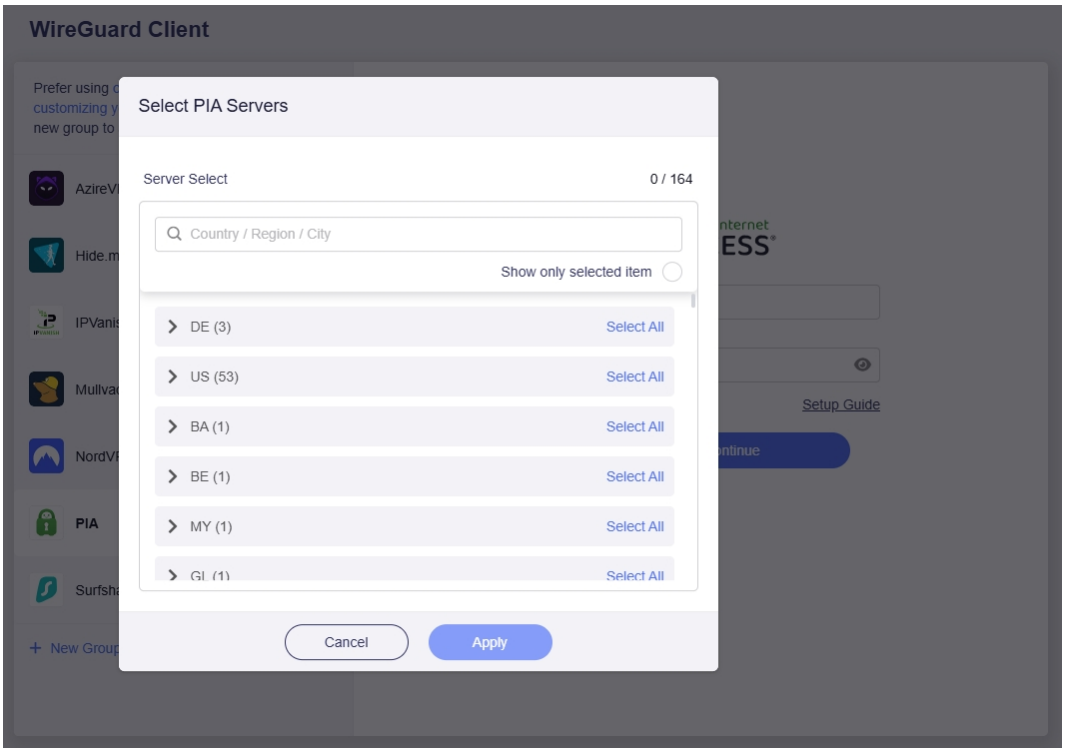
10.2.7 Configuration de PIA (Private Internet Access)

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

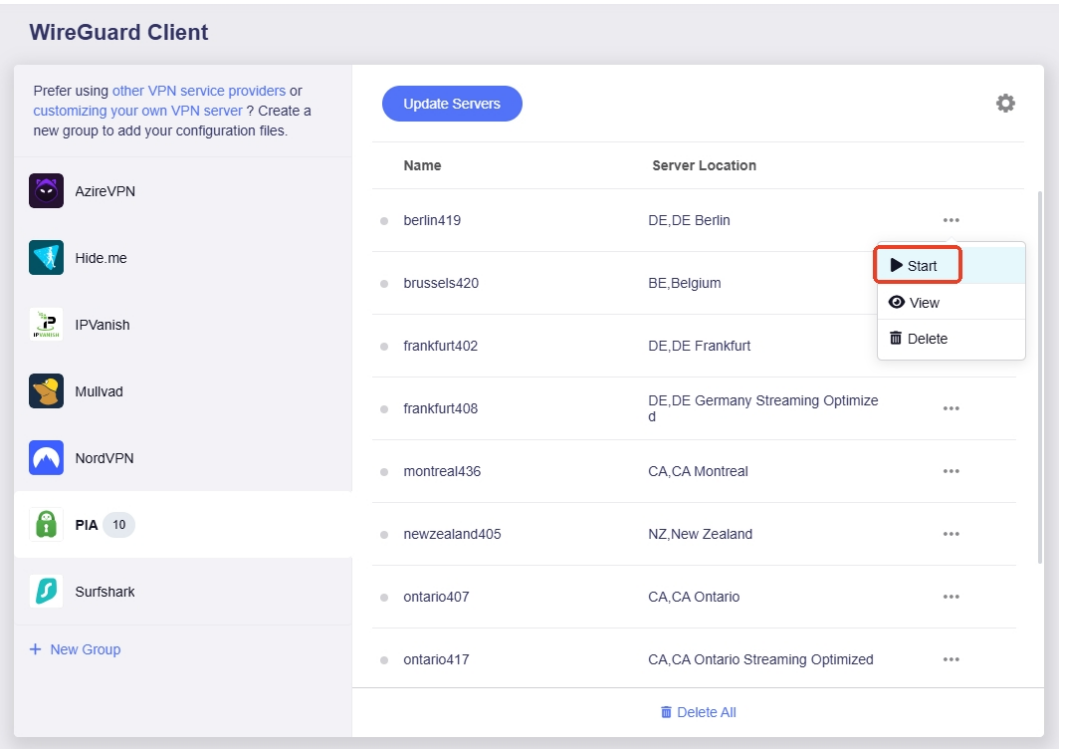
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **PIA**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



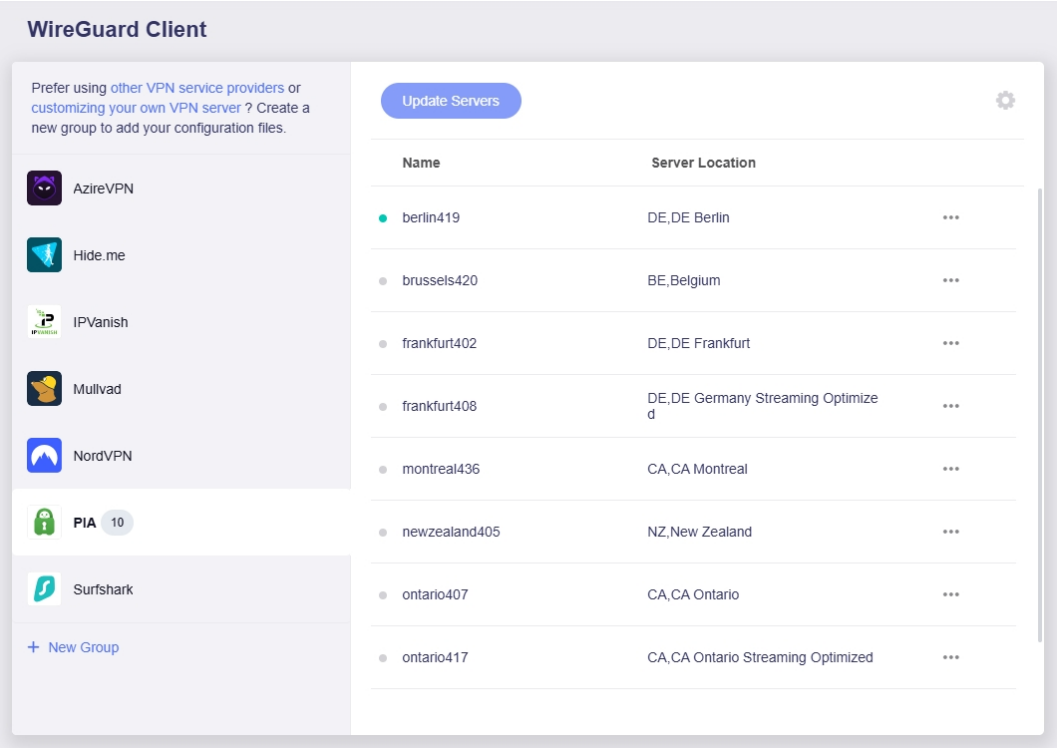
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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



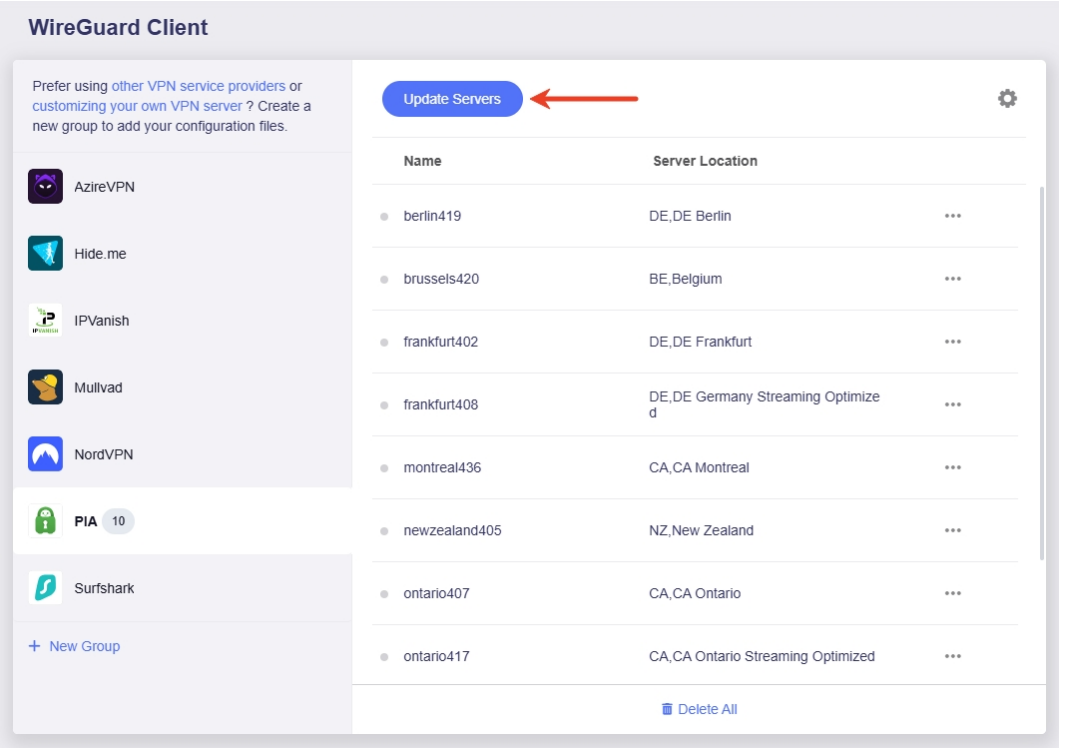
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

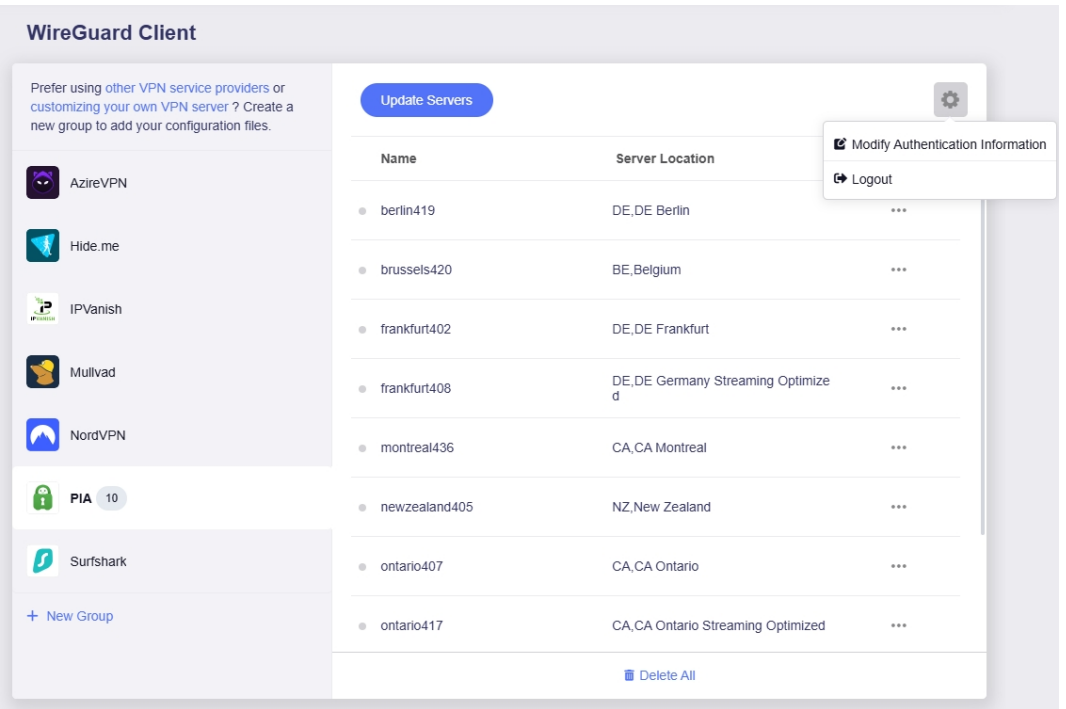
6. Mettez à jour les serveurs.

   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.



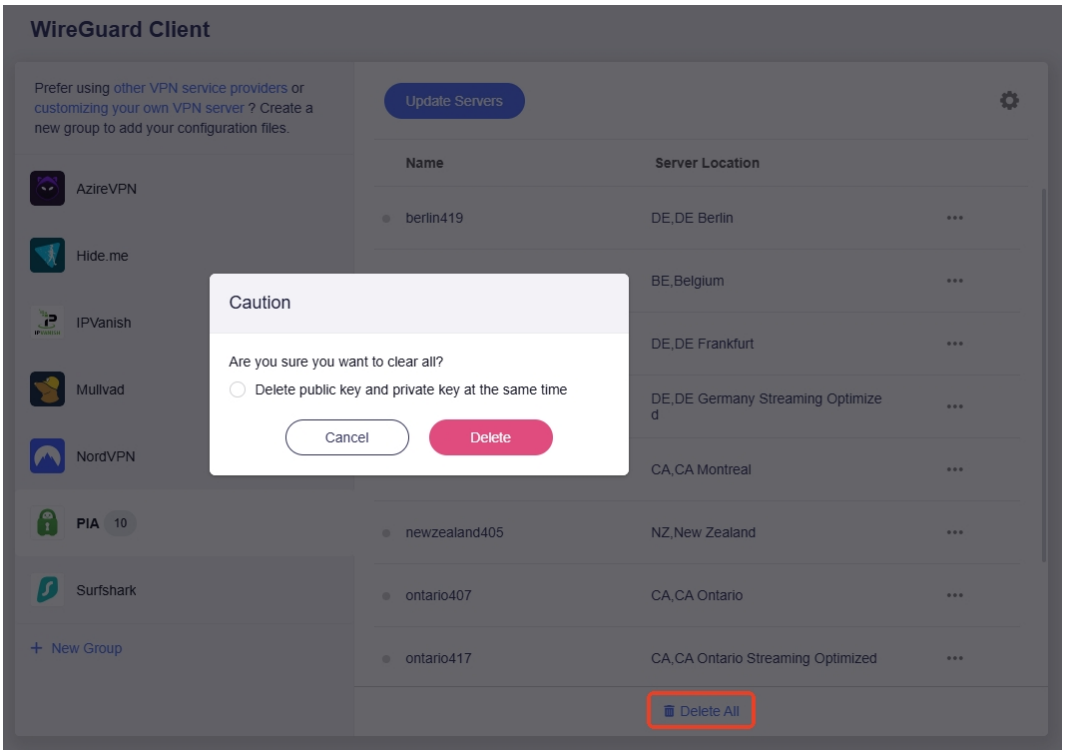
7. Modifiez les identifiants ou déconnectez-vous.

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



8. Supprimez tous les fichiers.

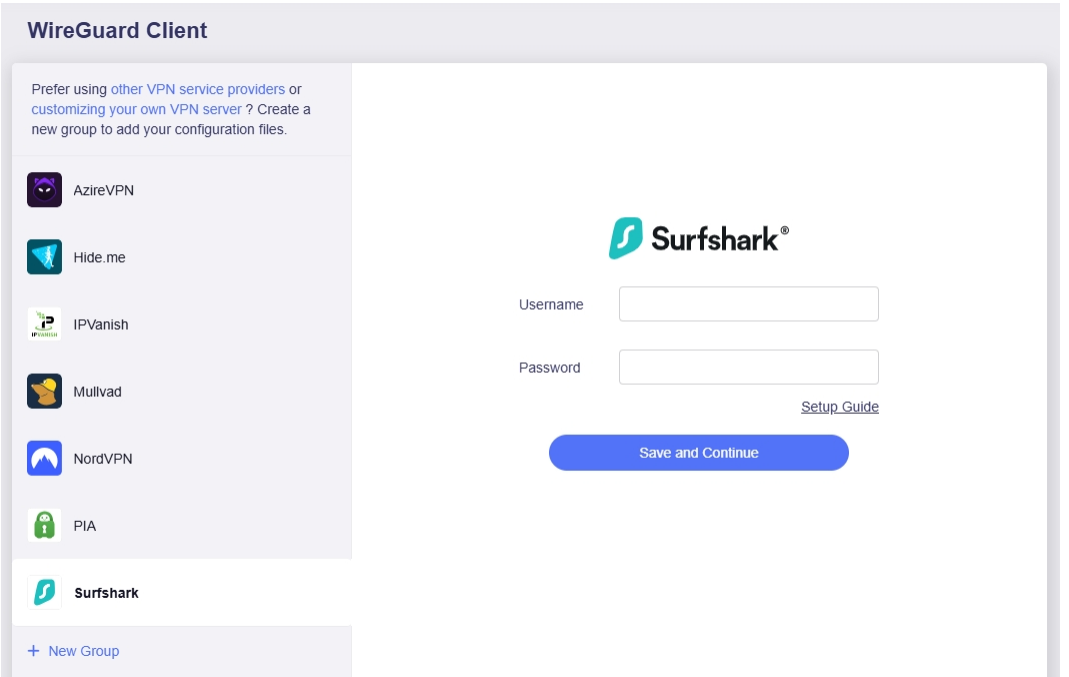
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



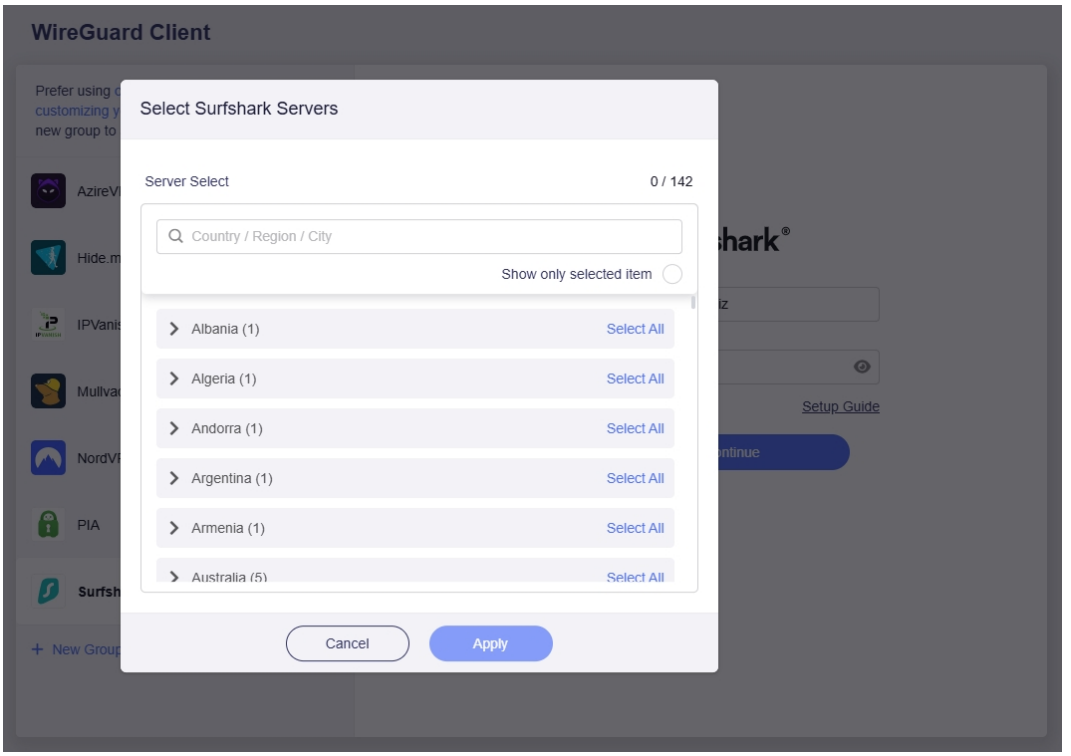
10.2.8 Configuration de Surfshark

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

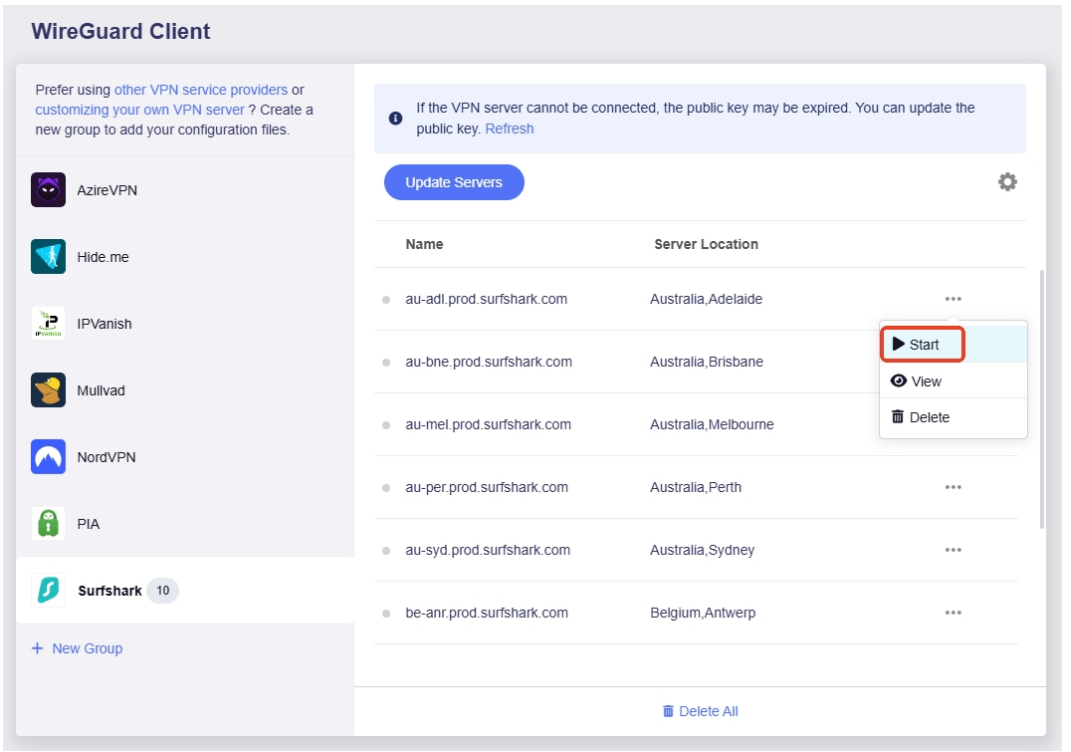
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Surfshark**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



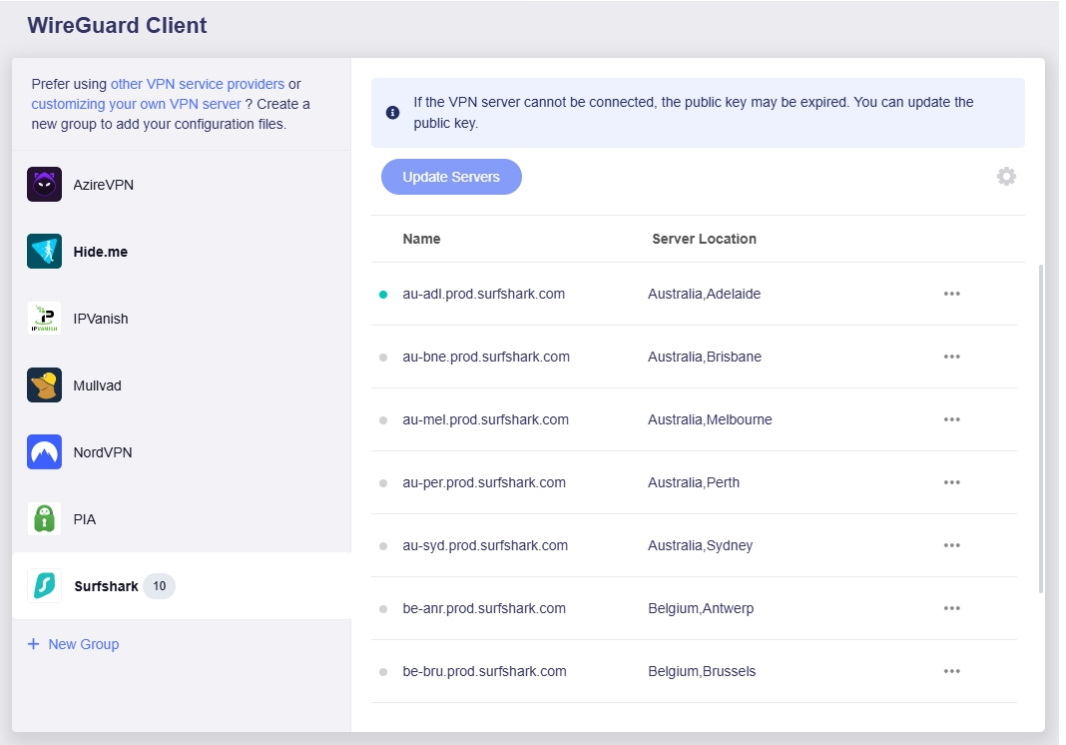
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



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

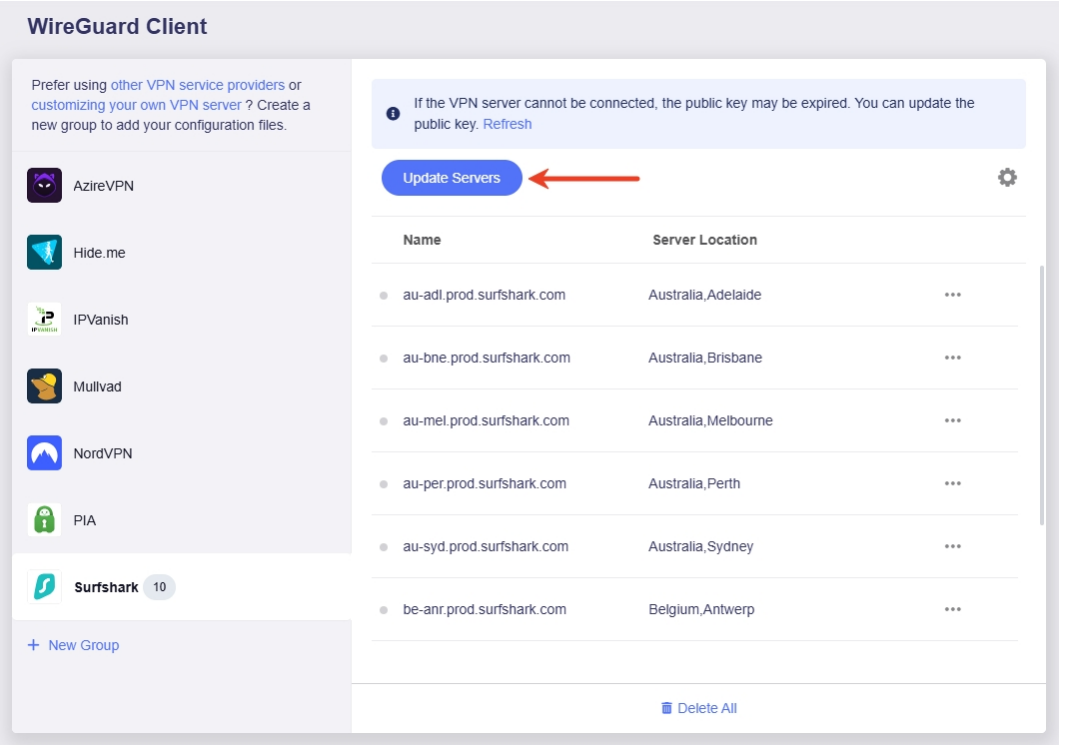


5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



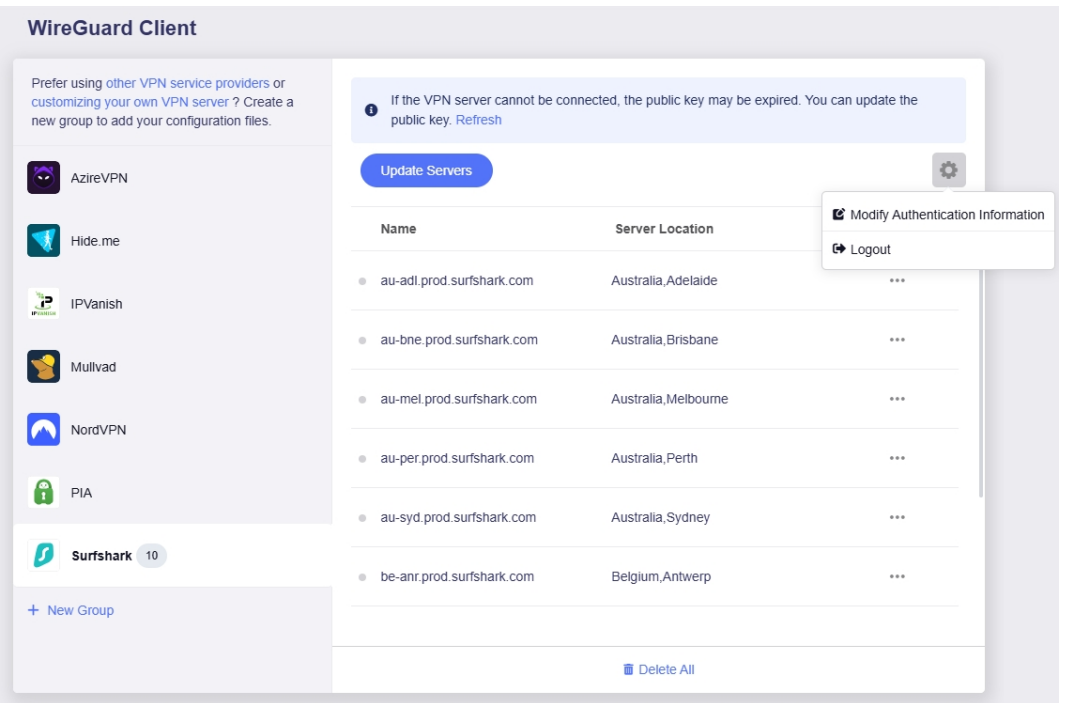
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

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.



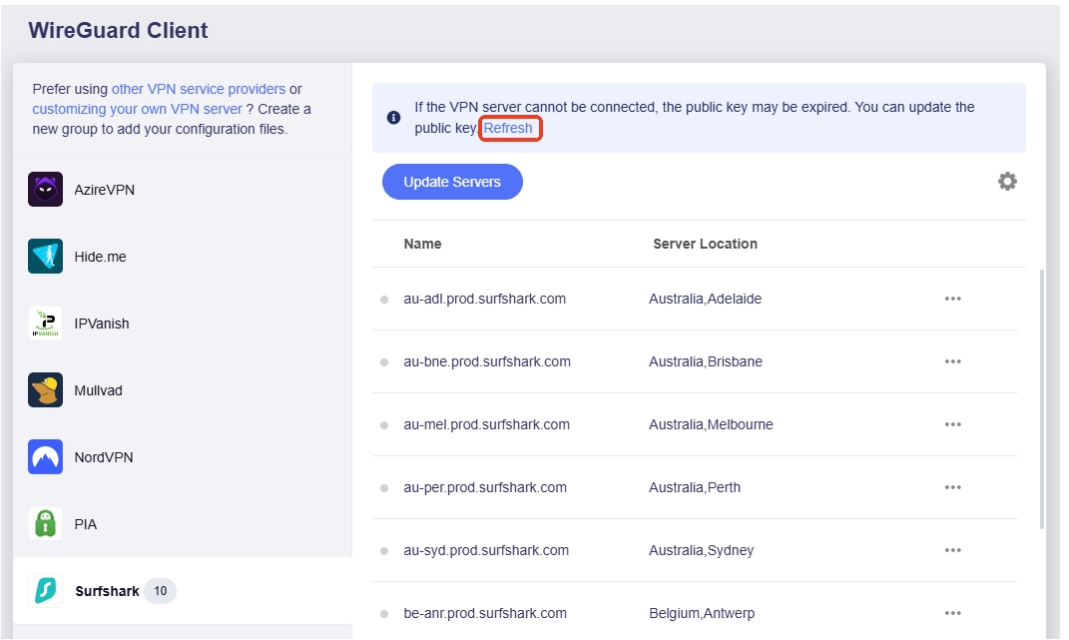
7. Modifiez les identifiants ou déconnectez-vous.

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



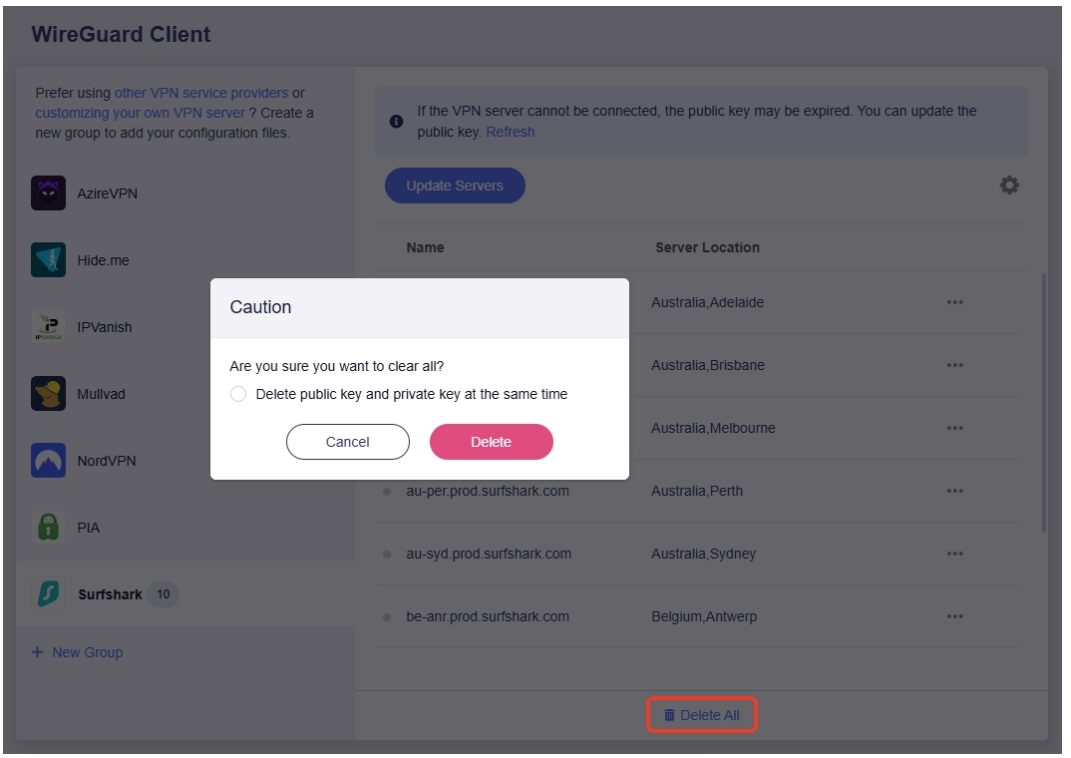
8. Actualisez les données.

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.

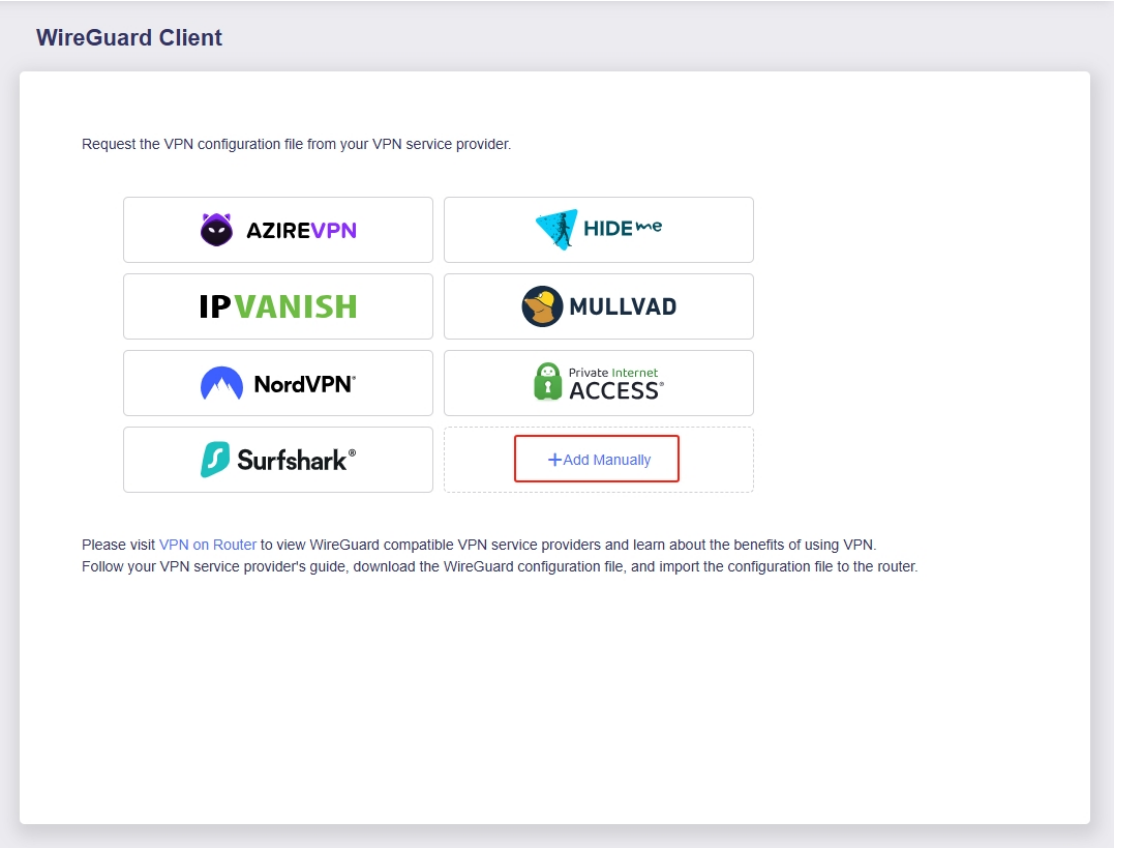


10.2.9 Configuration manuelle d’un client WireGuard pour un autre fournisseur

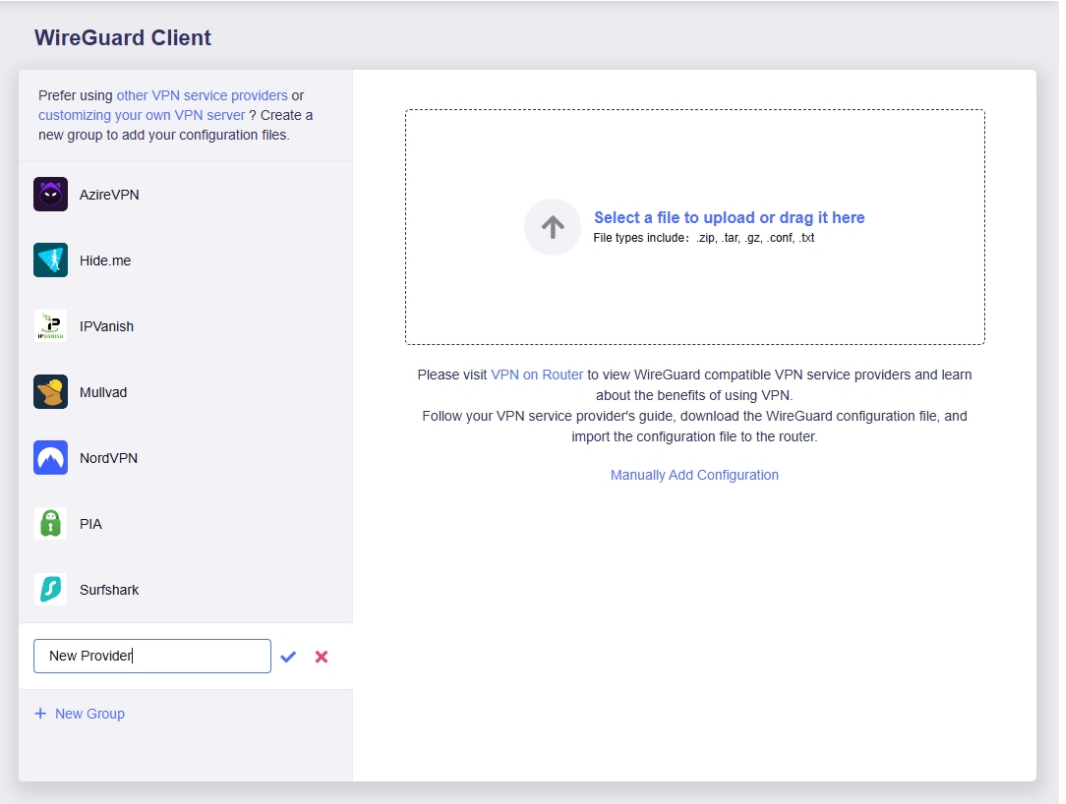
Si votre fournisseur WireGuard n’est pas intégré à l’interface Web, récupérez d’abord le fichier de configuration sur son site officiel, puis importez-le sur le routeur. Si vous ne savez pas comment télécharger les fichiers, consultez ce guide ou contactez l’assistance du fournisseur.

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

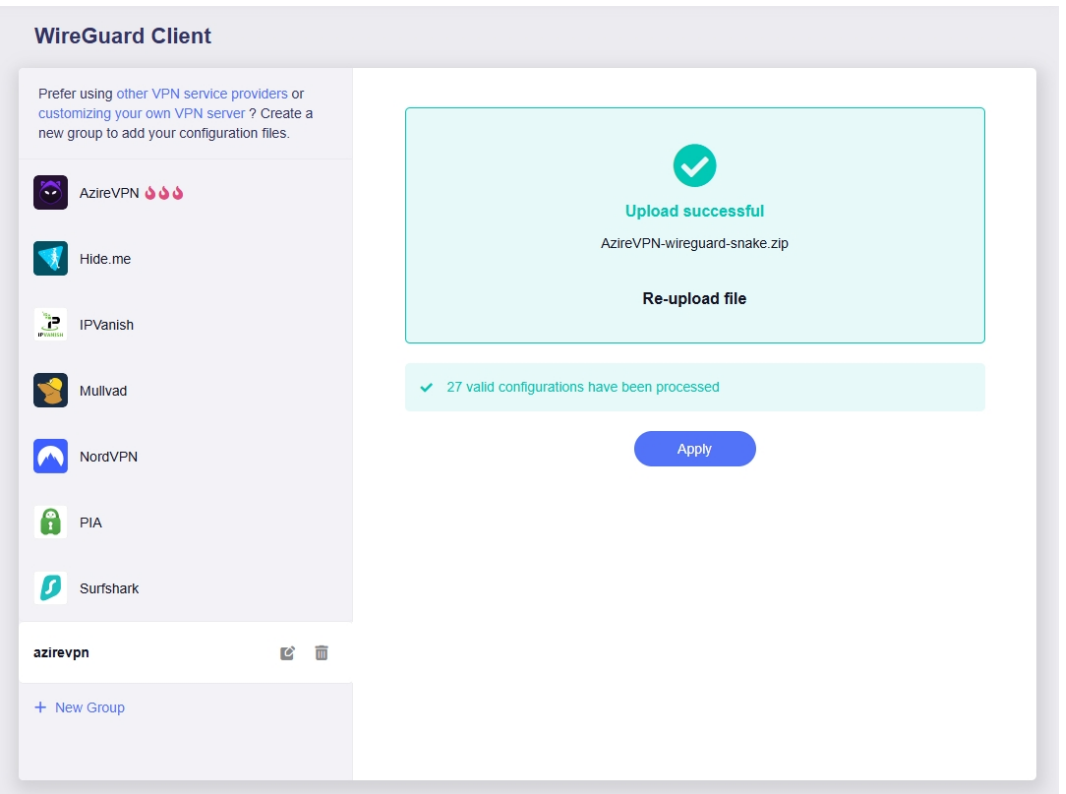
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Ajouter manuellement (Add Manually)**.



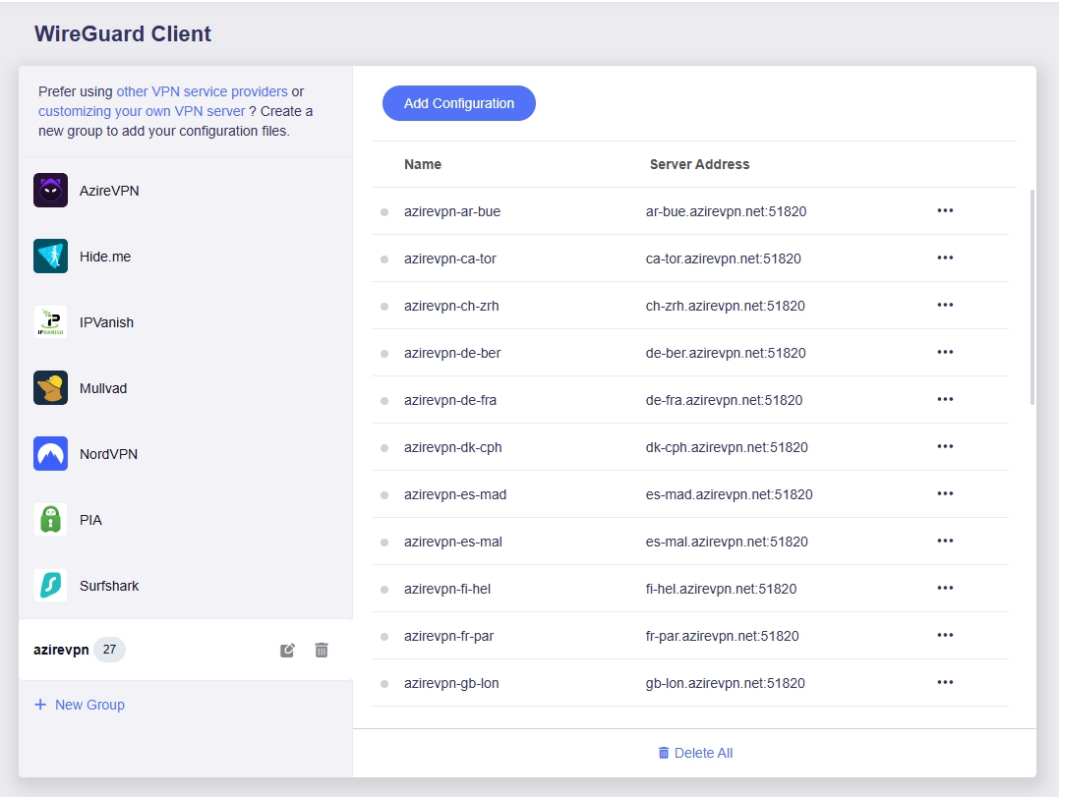
2. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



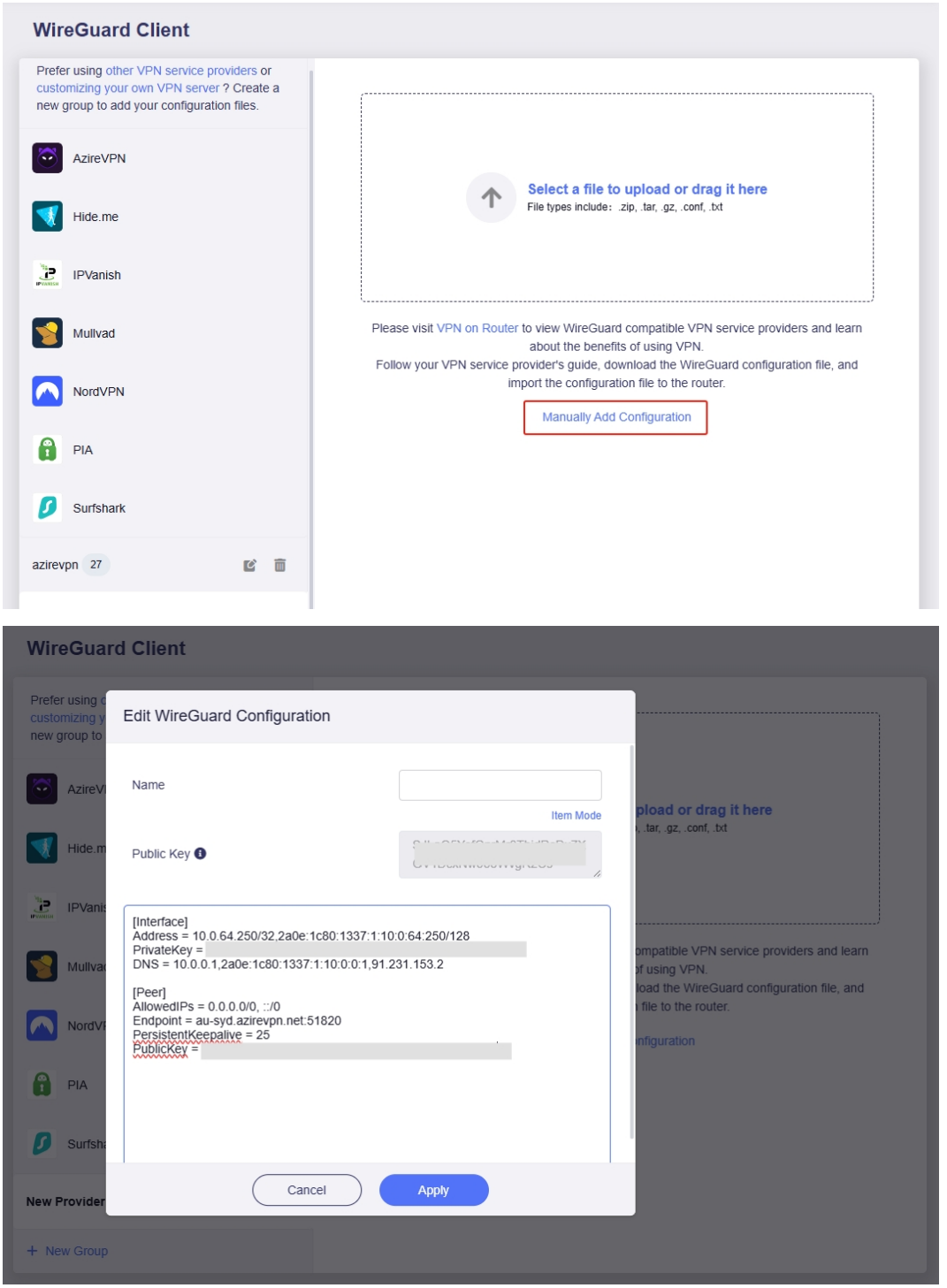
3. Cliquez sur la zone d’importation et sélectionnez votre fichier WireGuard. Les formats zip, tar, gz, conf et txt sont pris en charge. Cliquez sur **Appliquer (Apply)**.



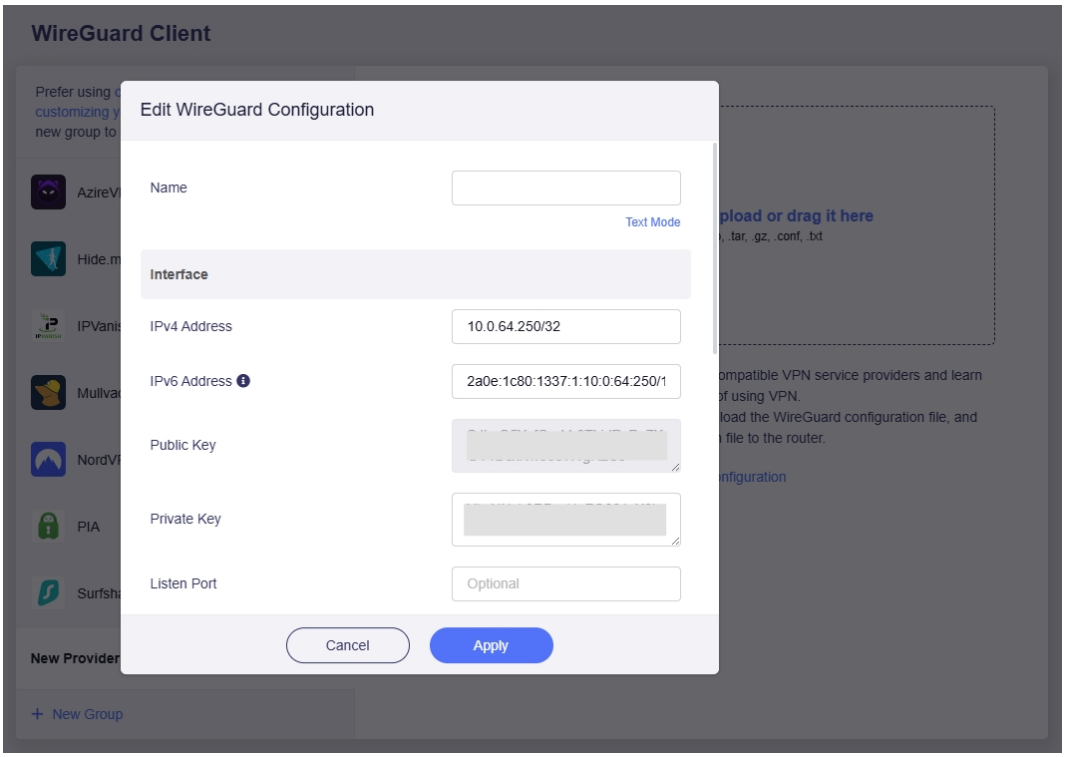
Si vous importez une archive contenant plusieurs fichiers de configuration, elle est décompressée automatiquement, comme ci-dessous.



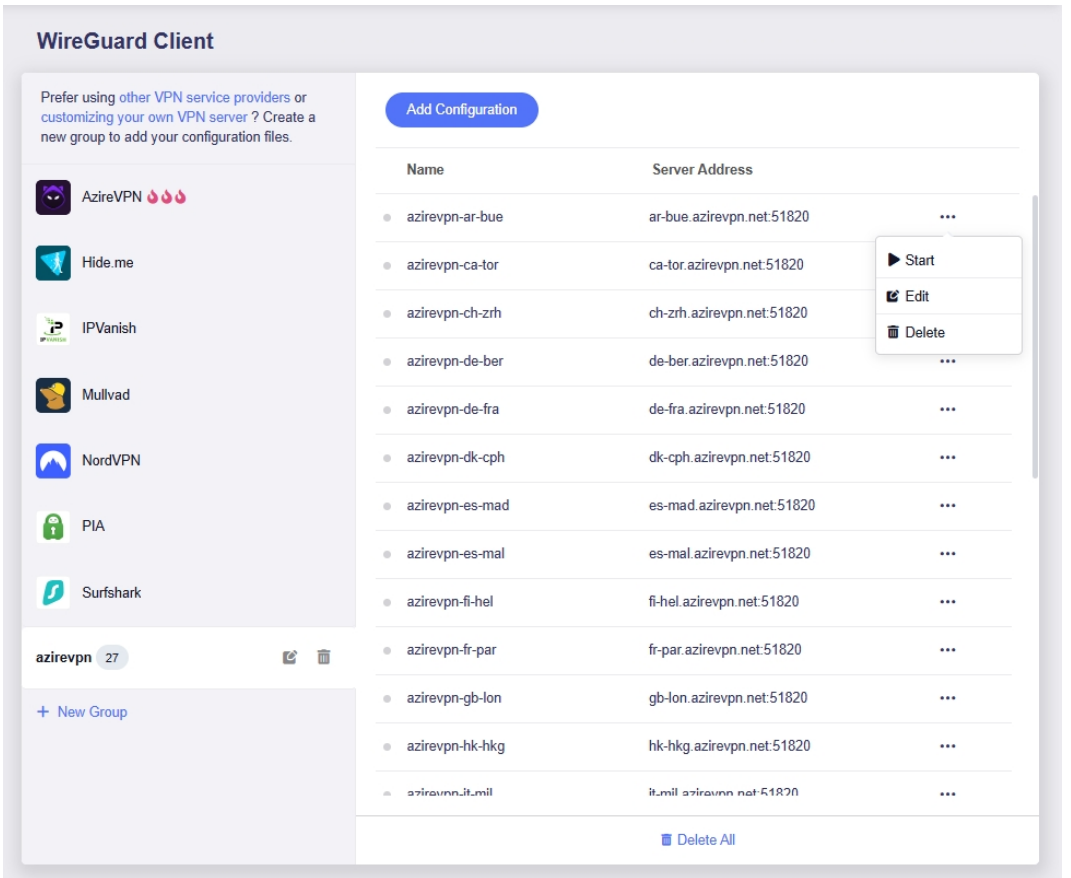
Vous pouvez aussi cliquer sur **Ajouter une configuration manuellement (Manually Add Configuration)** en bas de la zone d'importation, renseigner la configuration sous forme de texte, puis cliquer sur **Appliquer (Apply)**.



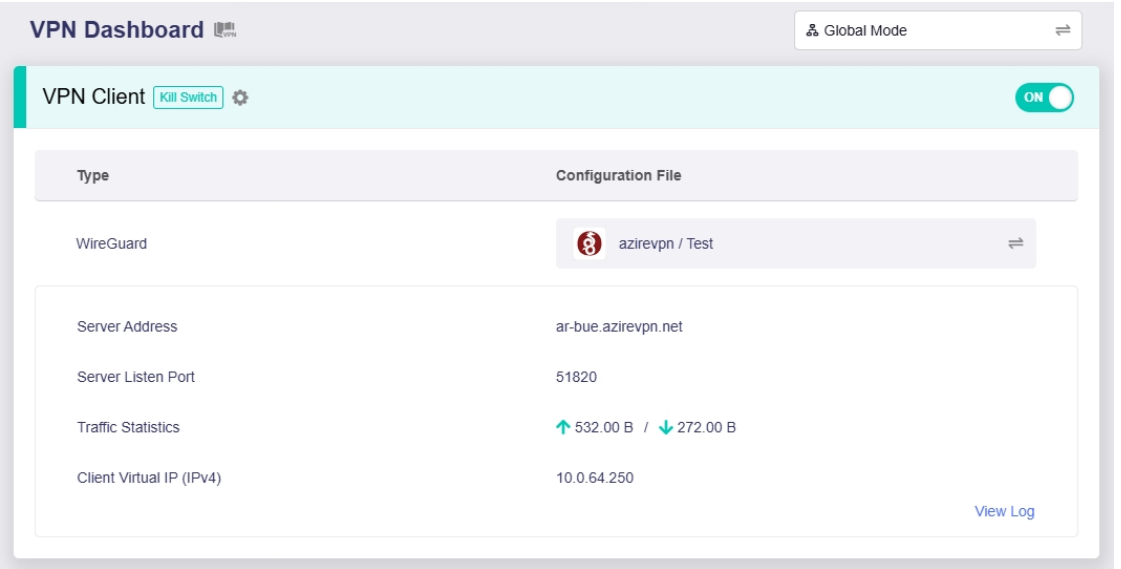
Pour vérifier chaque paramètre, passez en mode Élément (Item), contrôlez la configuration, puis cliquez sur **Appliquer (Apply)**.



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 11

Tor

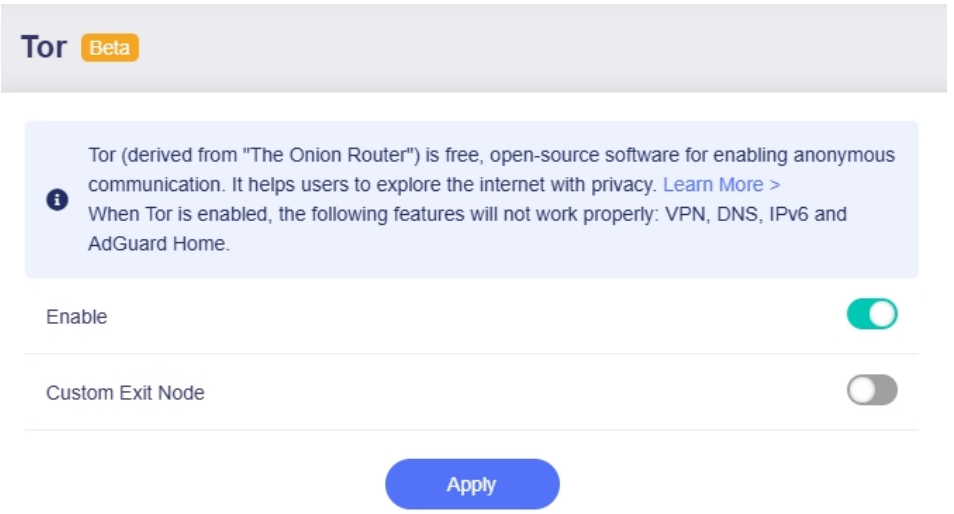
Ce chapitre présente brièvement Tor (The Onion Router), un logiciel libre et gratuit permettant des communications anonymes.

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

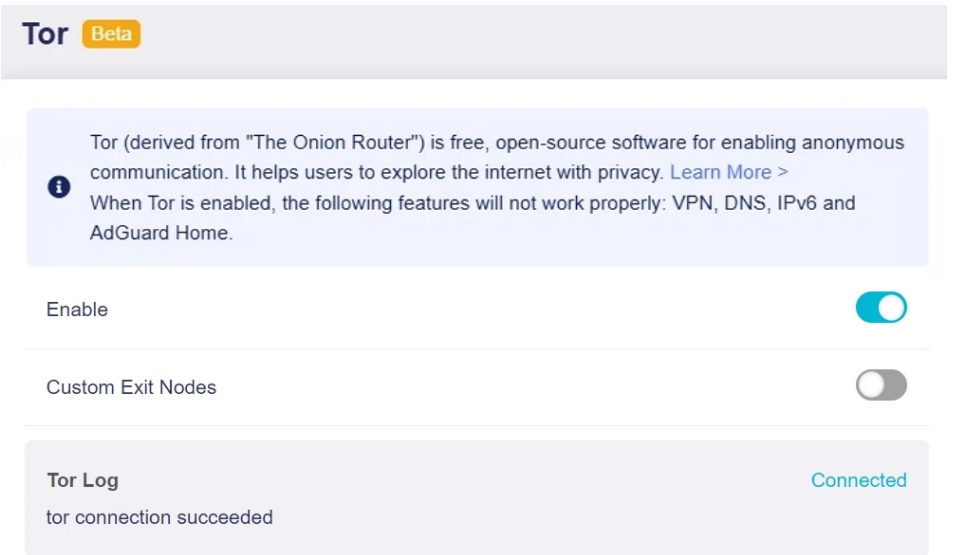
Lorsque Tor est activé, VPN, DNS, IPv6 et AdGuard Home ne fonctionnent pas correctement.

Pour configurer Tor, procédez comme suit.

1. Dans l'interface Web du routeur, ouvrez **VPN** > **Tor**. Activez Tor et, si nécessaire, les nœuds de sortie personnalisés, puis cliquez sur **Appliquer (Apply)**.



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



Chapitre 12

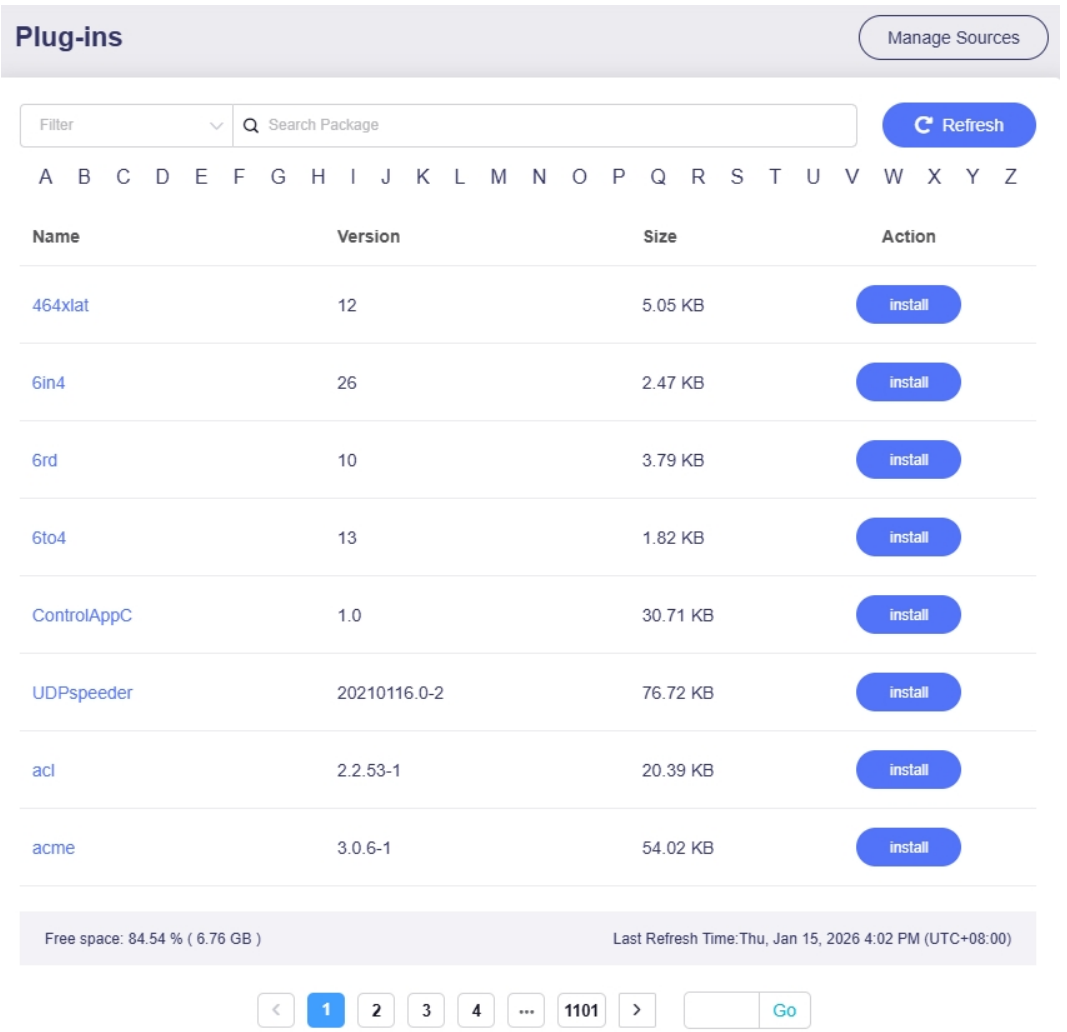
Applications

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

12.1 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 :

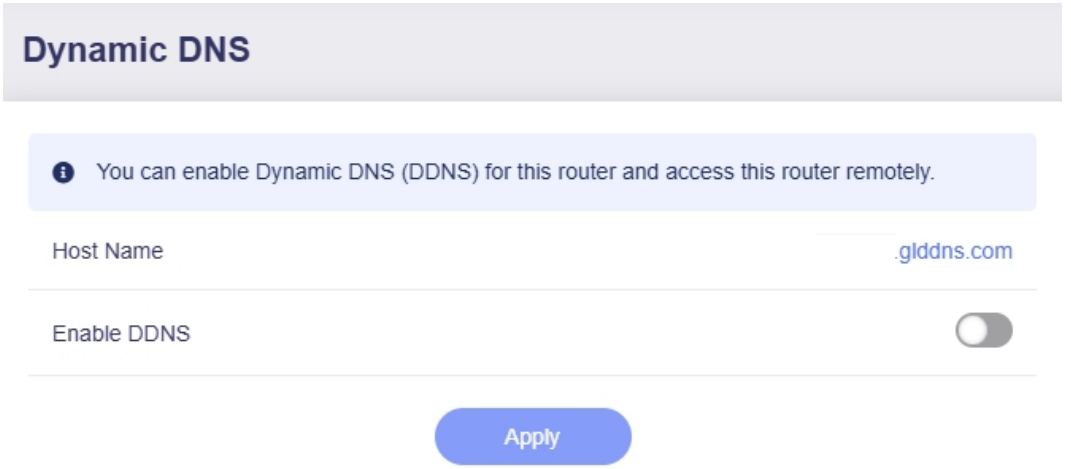
1. Il est déconseillé de mettre à jour les extensions préinstallées dans le micrologiciel officiel GL.iNet, comme nginx, AdGuard Home ou Tailscale.
2. Les extensions tierces installées manuellement peuvent être mises à jour. GL.iNet n'est toutefois pas responsable des problèmes de sécurité qu'elles peuvent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

12.2 DNS dynamique

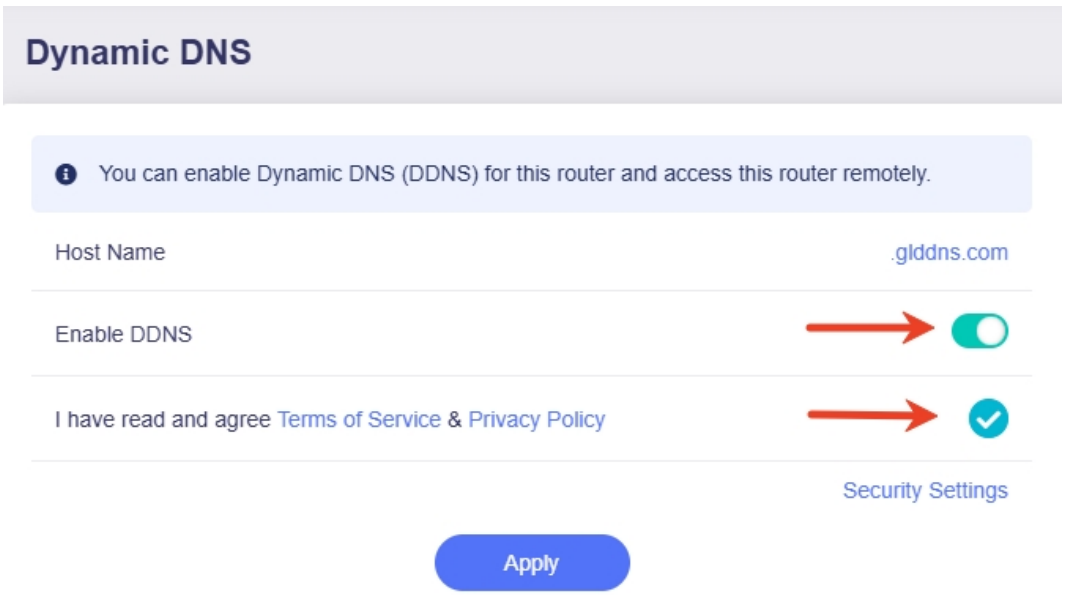
Le DNS dynamique (DDNS) associe un nom de domaine à l'adresse IP dynamique d'un appareil réseau. Il permet d'accéder au routeur à distance. Cette fonction nécessite une adresse IP publique.

12.2.1 Activation du DDNS

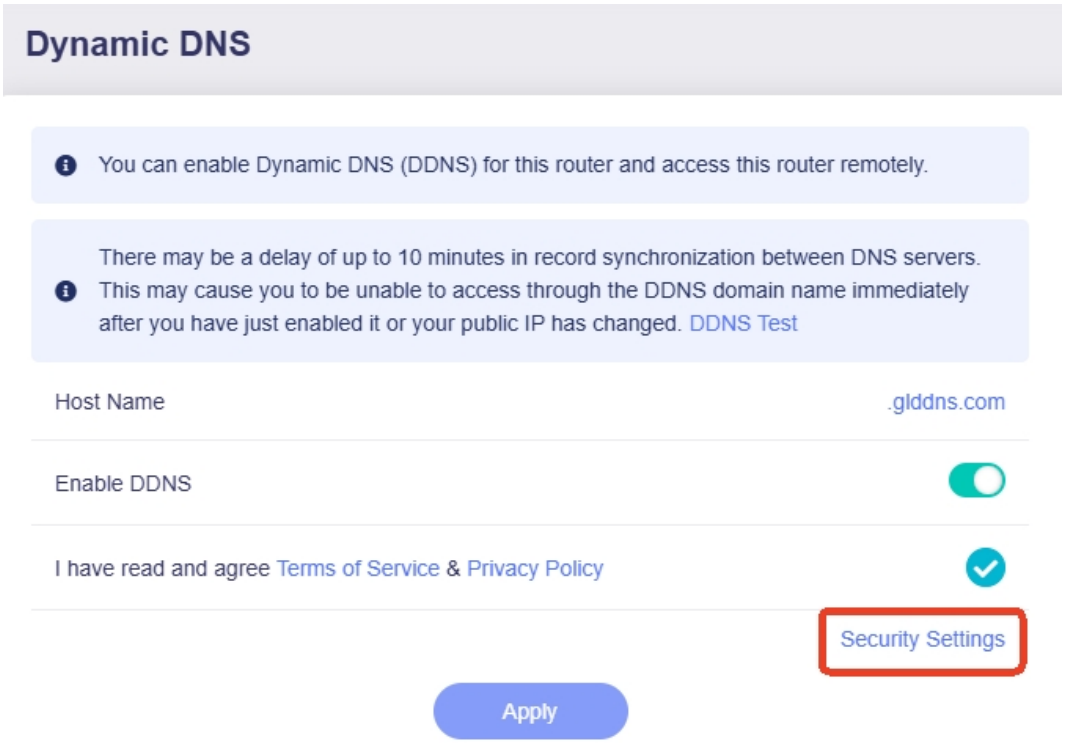
1. Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)**. La page ci-dessous s'affiche.



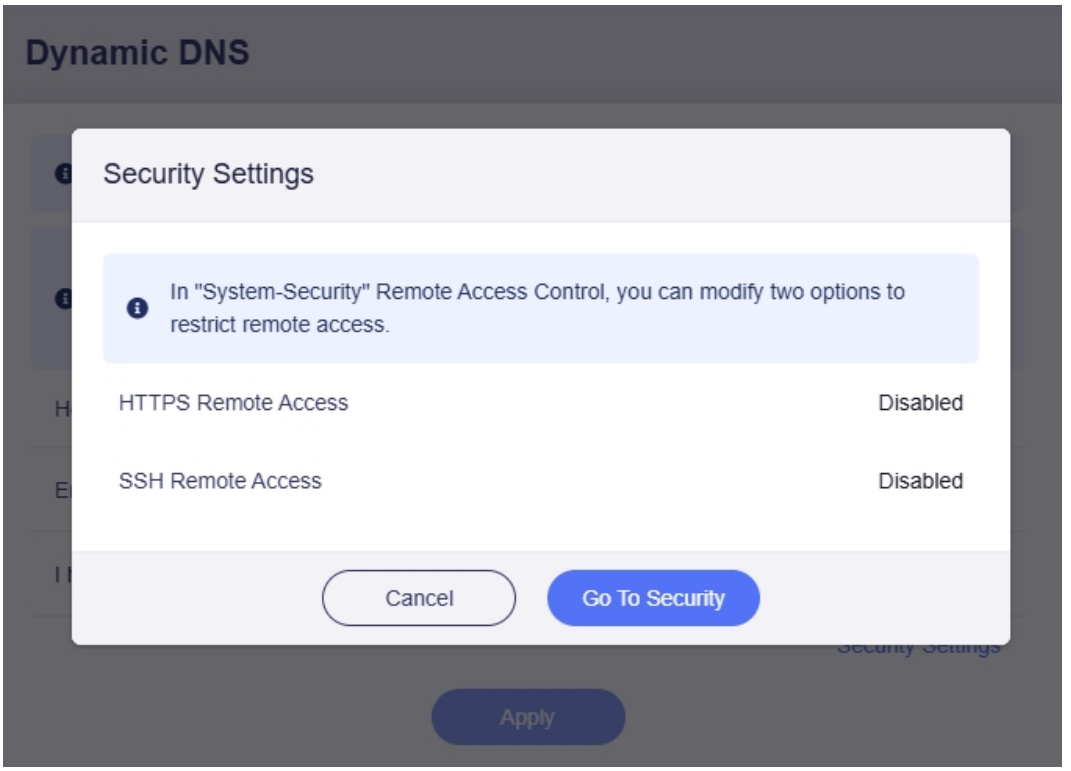
2. Activez **Activer le DDNS (Enable DDNS)**, lisez et acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



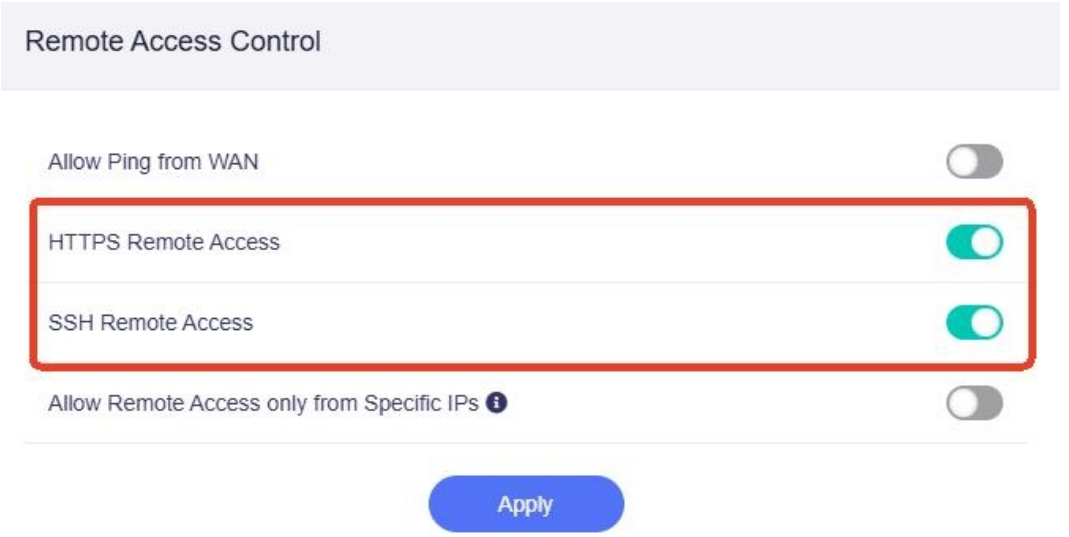
3. Cliquez sur **Paramètres de sécurité (Security Settings)** dans l'angle inférieur droit.



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



Sinon, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)** pour l'activer, puis cliquez sur **Appliquer (Apply)**.



Remarque :

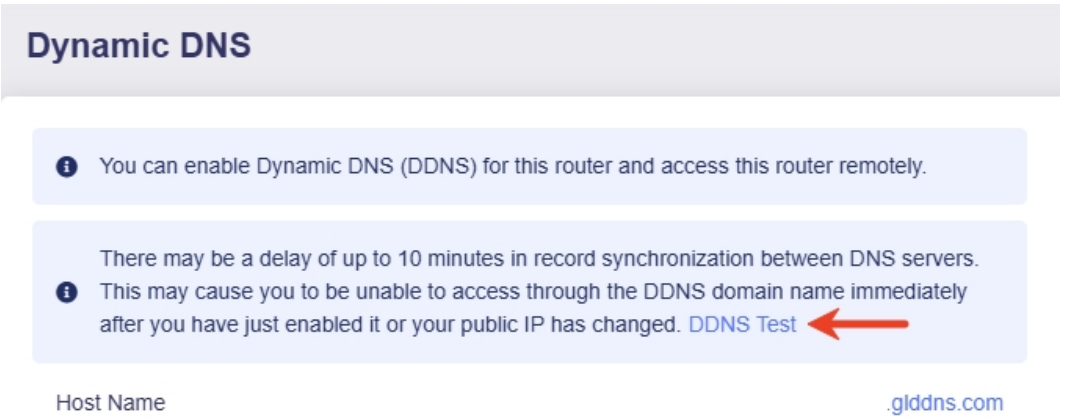
1. La synchronisation des enregistrements entre serveurs DNS peut prendre jusqu'à 10 minutes. L'accès par le domaine DDNS peut donc être indisponible immédiatement après son activation ou après un changement d'IP publique.
2. Si vous activez simultanément le DDNS et un client VPN, vérifiez que Services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

12.2.2 Vérification du fonctionnement du DDNS

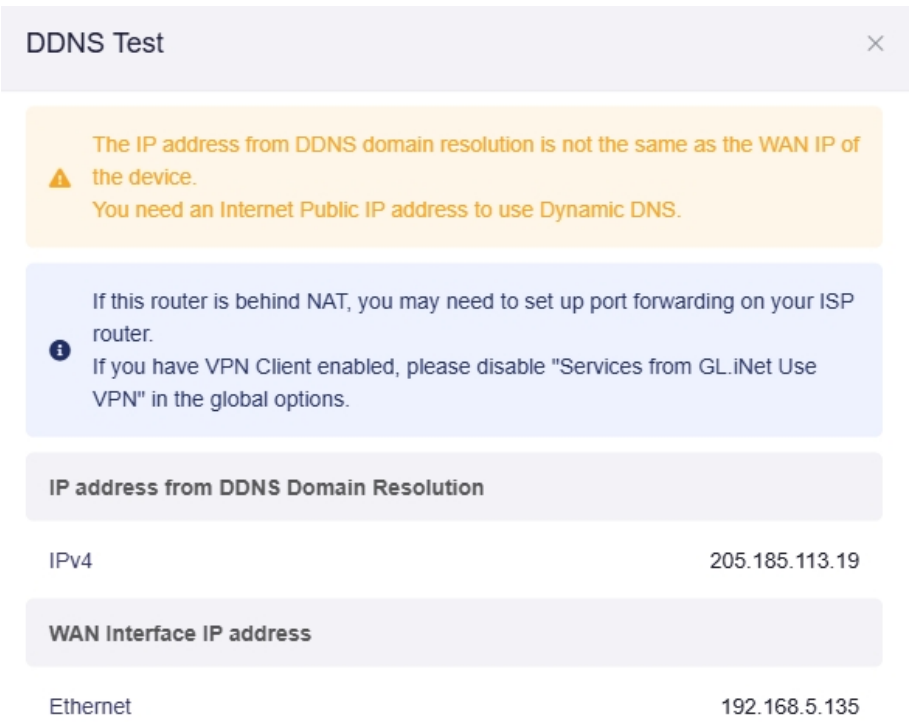
Vérifiez le DDNS avec l'outil de test intégré ou manuellement à l'aide de commandes.

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. L'exemple ci-dessous utilise Beryl AX (GL-MT3000).



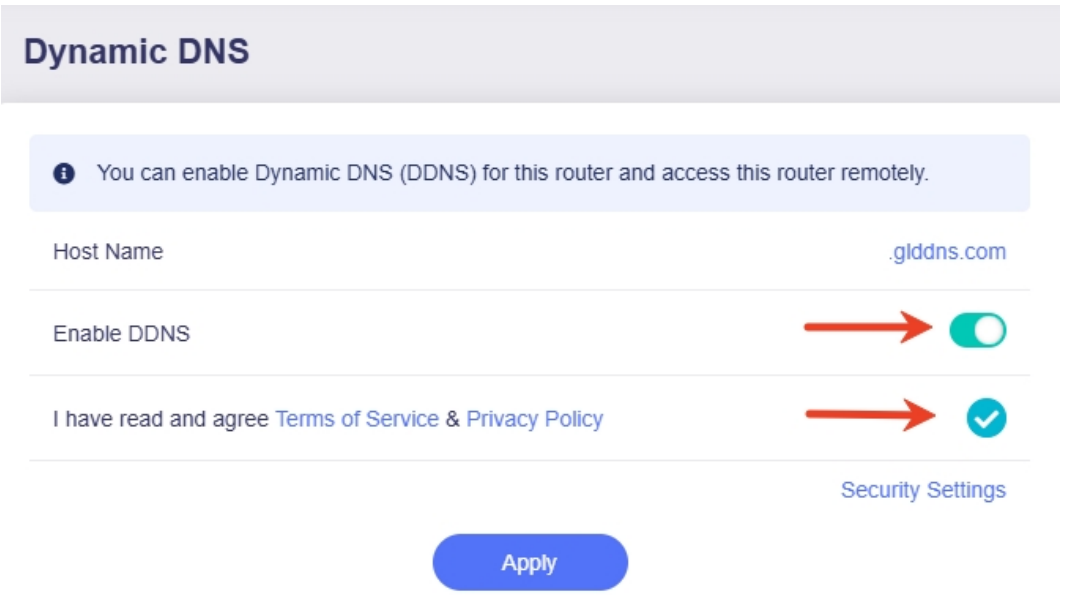
   - Remplacez « xxxxxxx.glddns.com » par votre nom d'hôte.
   - « 8.8.8.8 » est le DNS de Google. Utilisez-le ou indiquez un autre serveur, puis appuyez sur Entrée.
2. Une IP publique, comme « 183.178.10.100 » dans l'image, indique que le domaine DDNS est bien associé à une adresse publique. Un message comme « server can't find xxxxxxx.glddns.com » peut indiquer un échec de résolution. Passez à l'étape suivante pour vérifier.
3. 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.

12.2.3 Accès HTTPS à distance

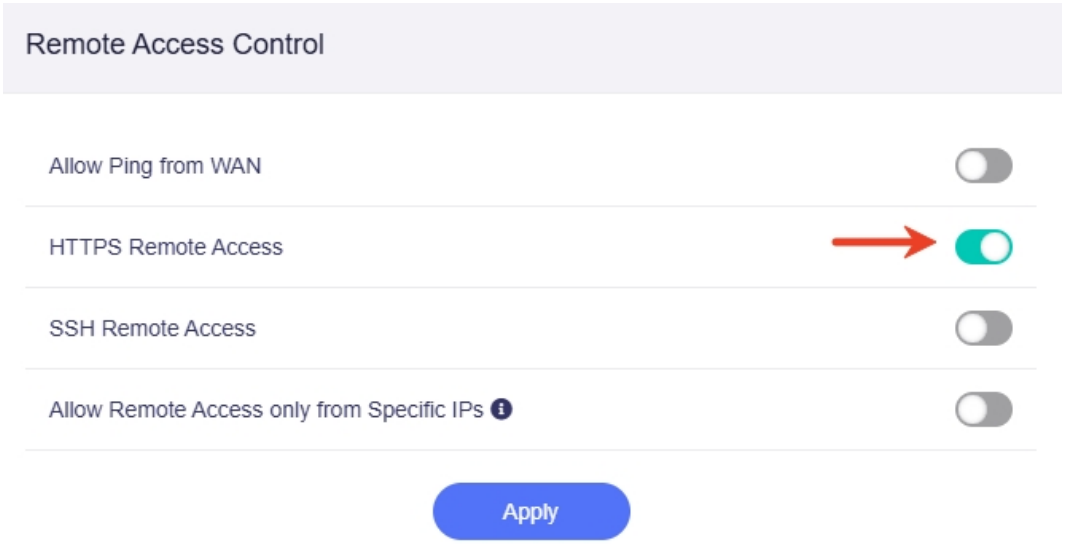
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 443** sur le routeur en amont.

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)**.

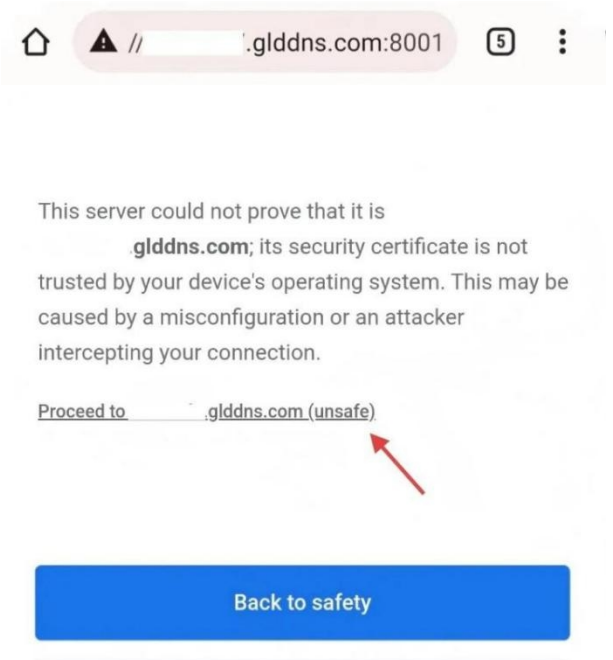


2. Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)**. Activez **Accès HTTPS à distance (HTTPS Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



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.



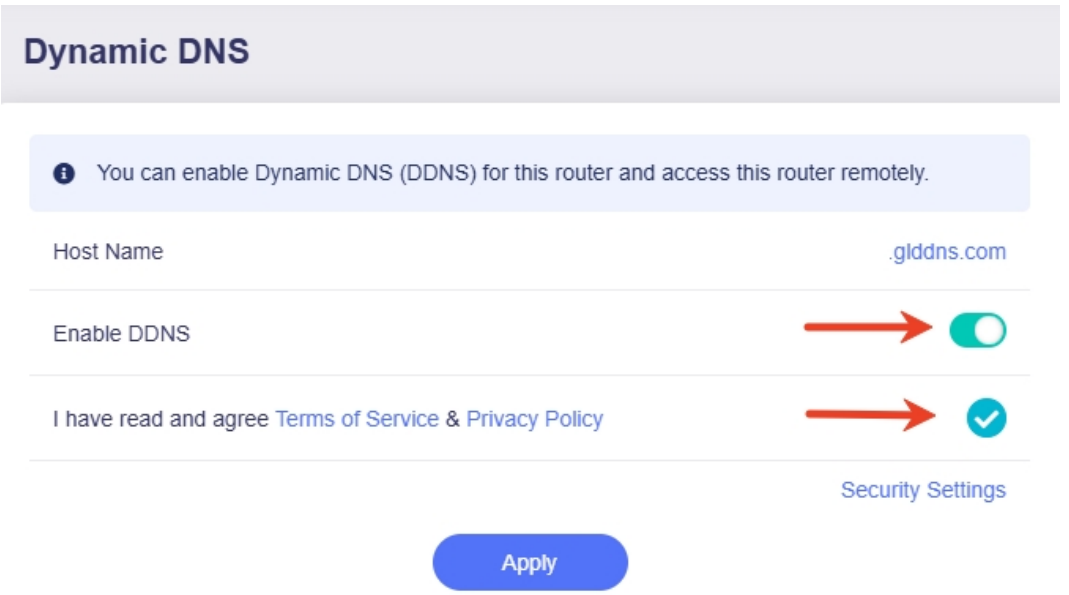
Vous pouvez alors accéder à l’interface Web par le nom d’hôte DDNS en **HTTPS**.

12.2.4 Accès SSH à distance

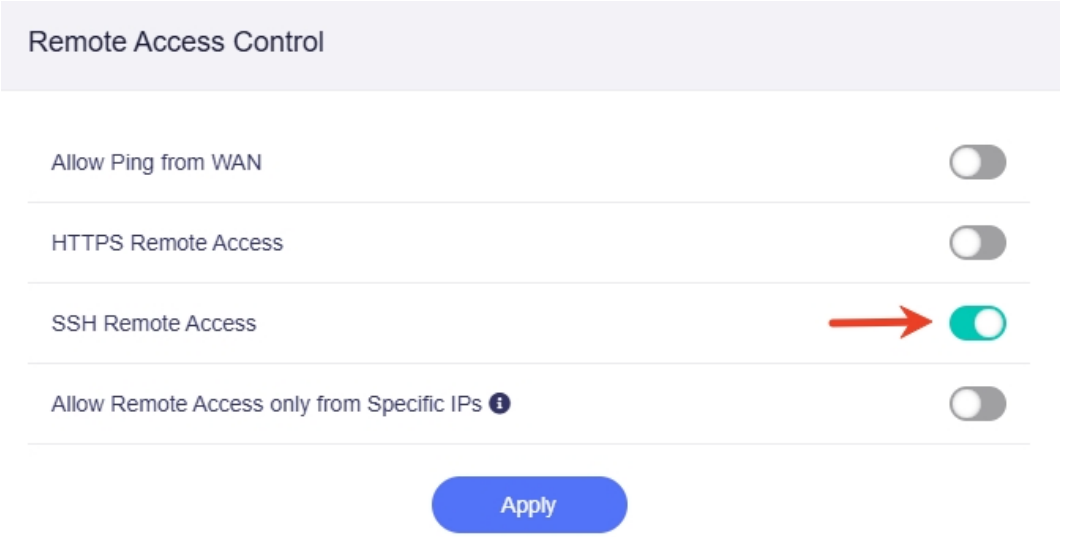
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 22** sur le routeur en amont.

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.

12.3 Stockage réseau

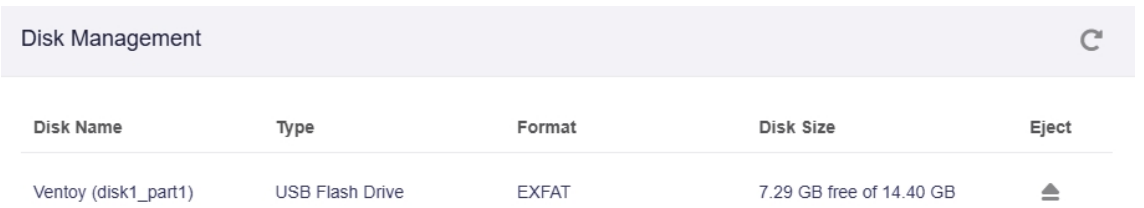
Le stockage réseau permet de partager des fichiers entre appareils en connectant une clé USB, un disque USB ou une carte SD au routeur. Celui-ci transforme le support de stockage en lecteur réseau partagé, accessible à tous les appareils connectés.

Brume 2 possède un port USB compatible avec les clés USB et les disques durs externes portables. Vous pouvez configurer Samba, WebDAV ou DLNA pour ces supports de stockage utilisant des formats courants comme NTFS, FAT32 et EXT4.

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

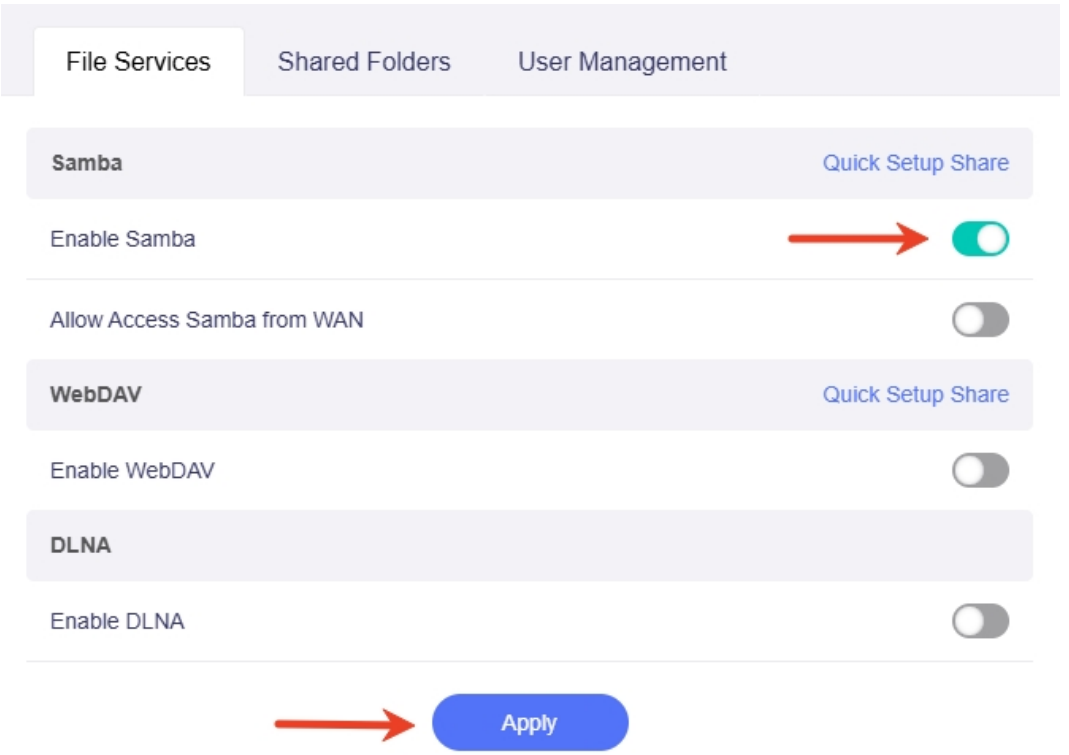
12.3.1 Branchement du stockage

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.



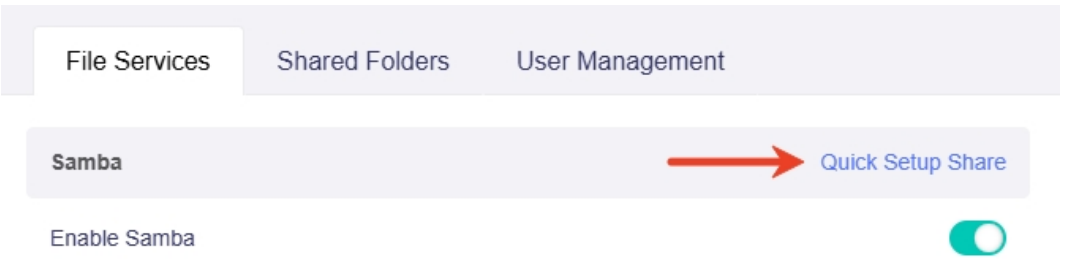
12.3.2 Configuration de Samba

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

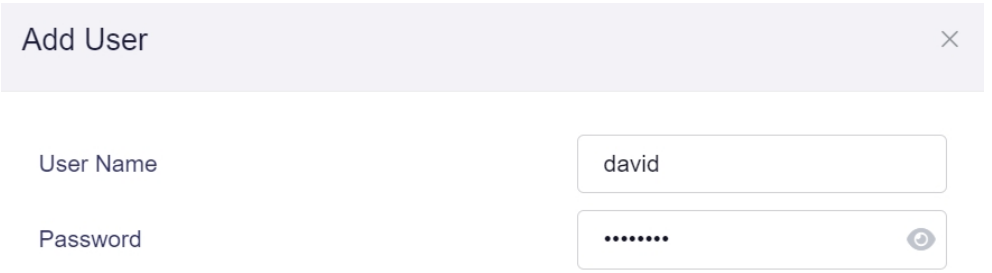


   - **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** : activez cette option pour que les appareils en amont accèdent à Samba.

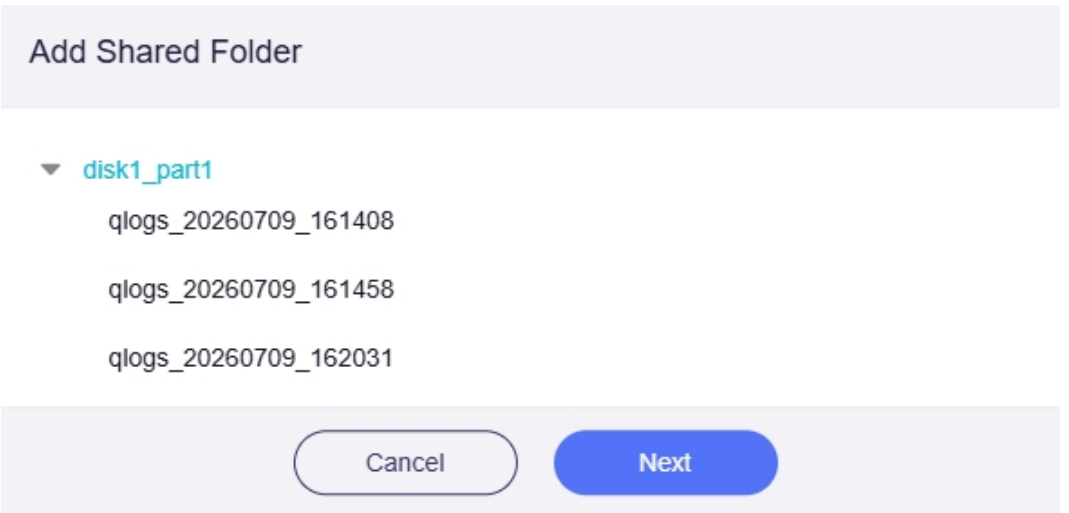
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



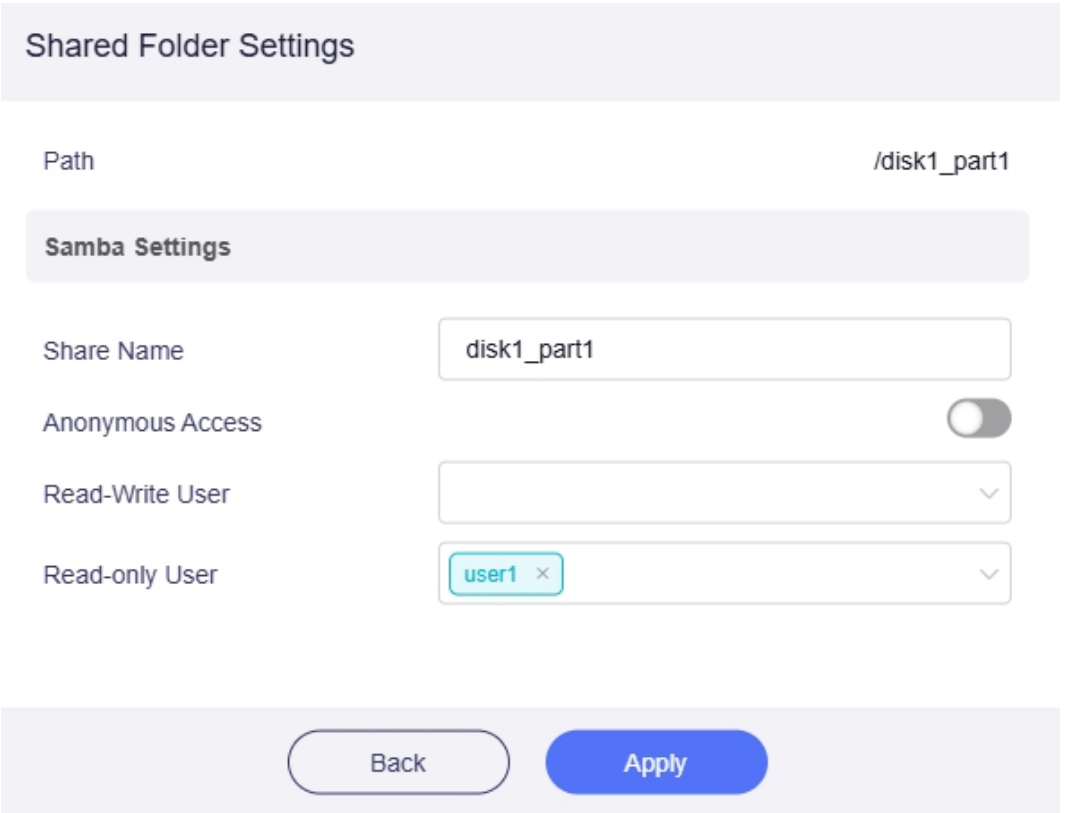
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



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.

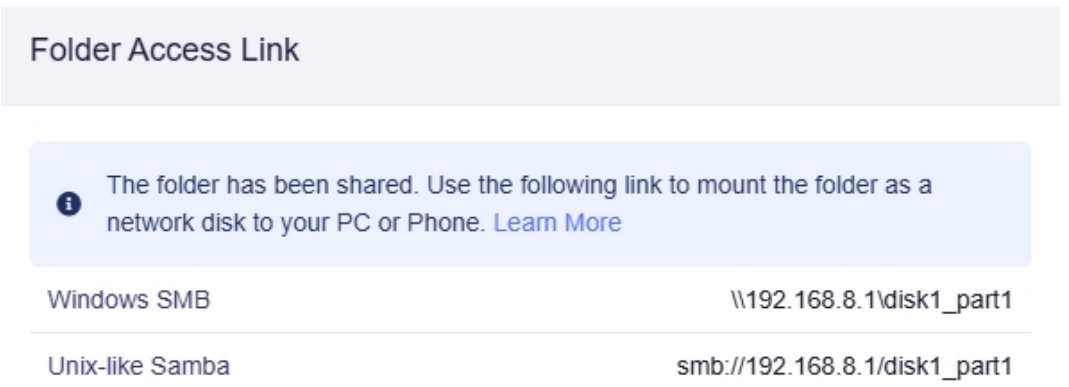


5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**. Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez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



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

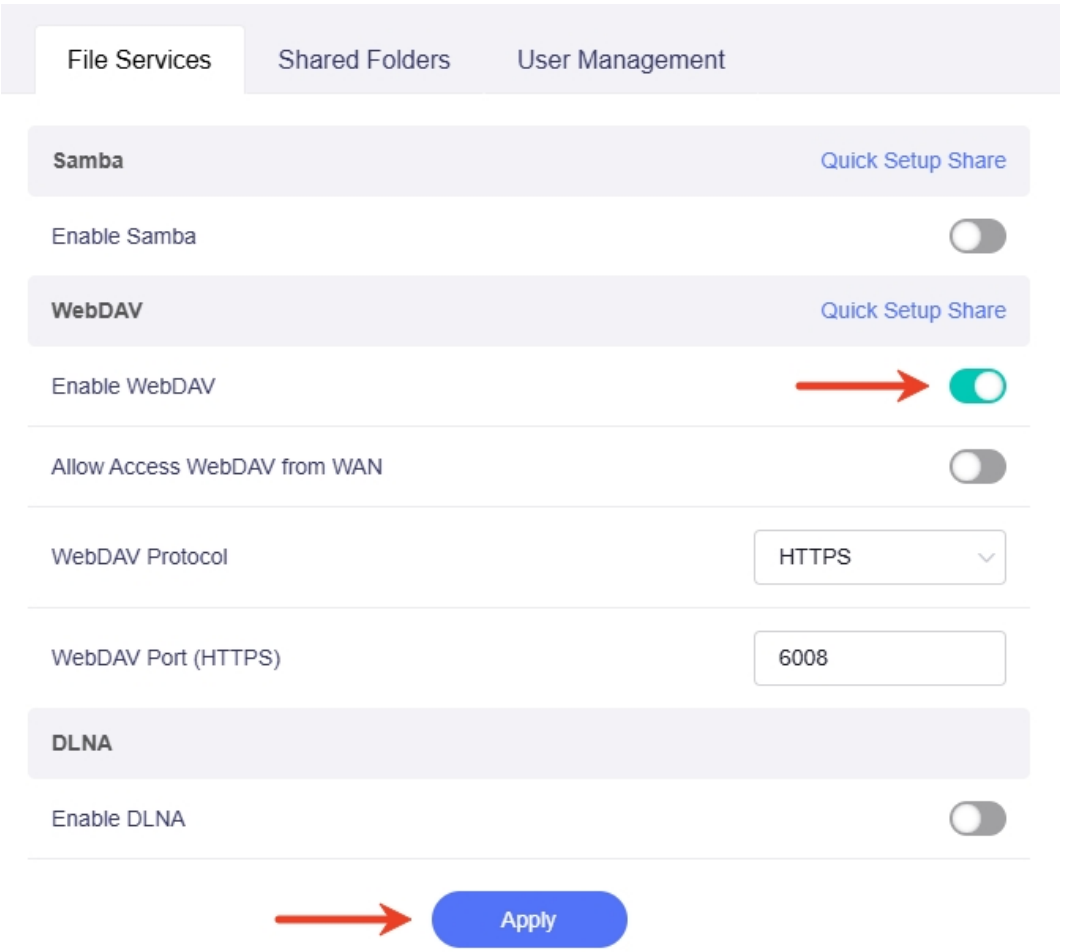
6. Récupérez le lien d'accès au dossier.
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via Samba.



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.

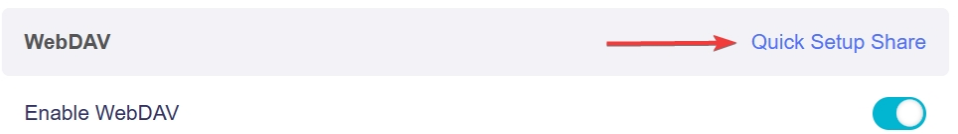
12.3.3 Configuration de WebDAV

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

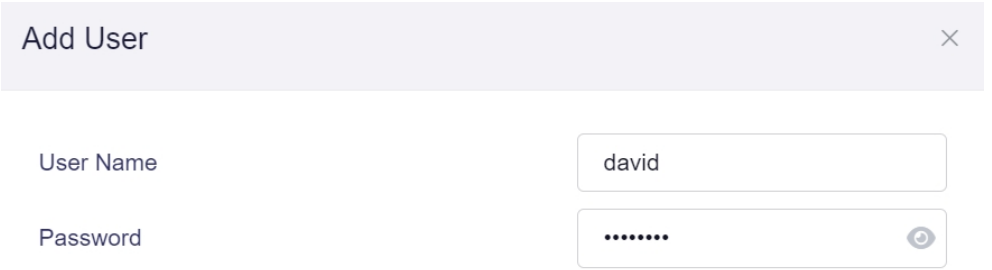


- **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** : activez cette option pour que les appareils en amont accèdent au service WebDAV.
- **Protocole WebDAV (WebDAV Protocol)** : HTTP n'est pas chiffré ; utilisez-le à vos risques. HTTPS est chiffré et utilise un certificat autosigné.
-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

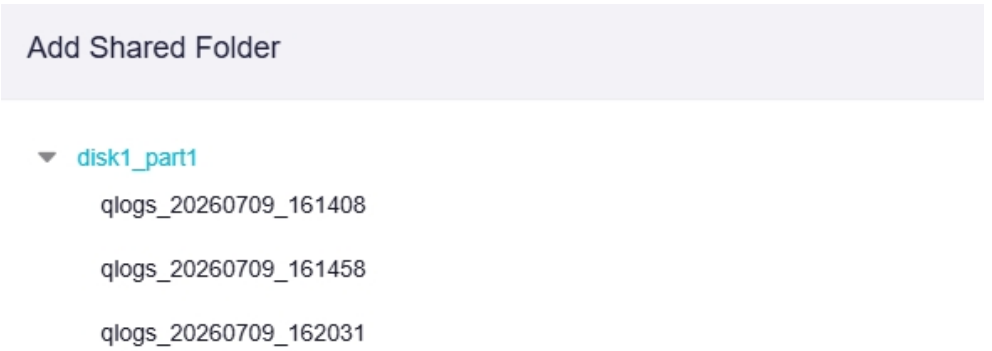
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



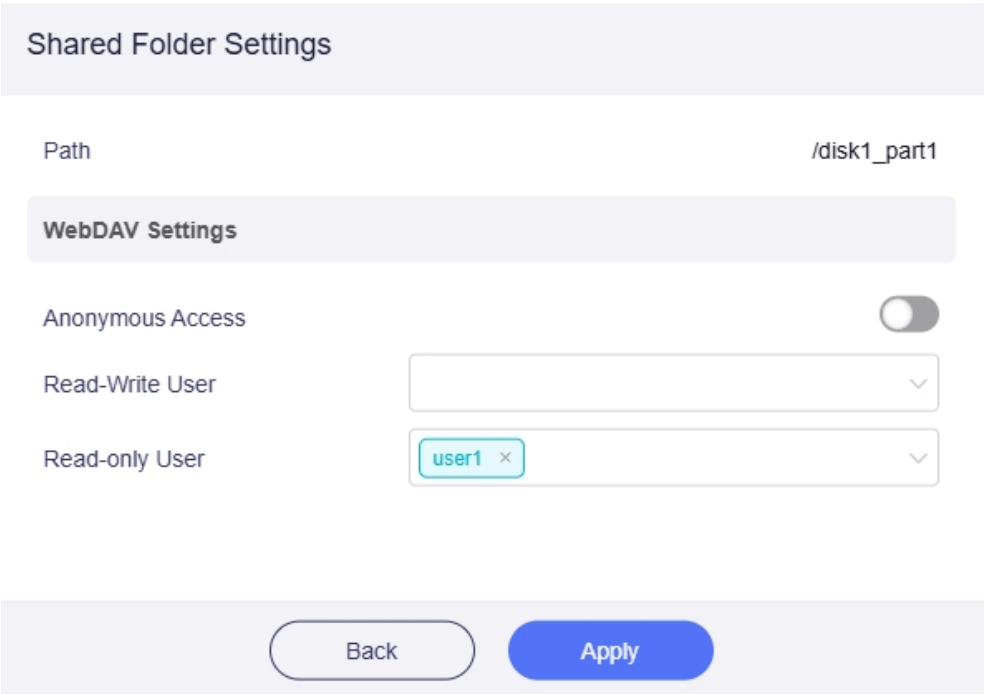
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



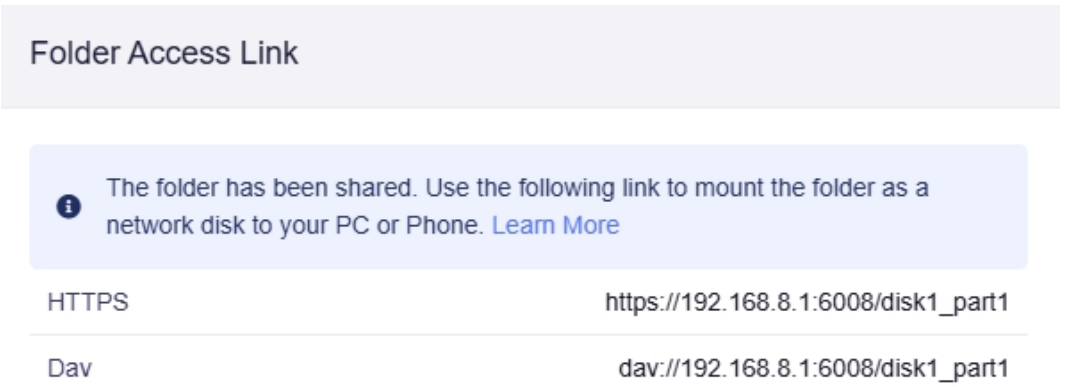
4. Cliquez sur le triangle pour afficher tous les dossiers. Sélectionnez le dossier à partager. Pour partager le disque entier, cliquez sur son nom, par exemple disk1_part1.



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



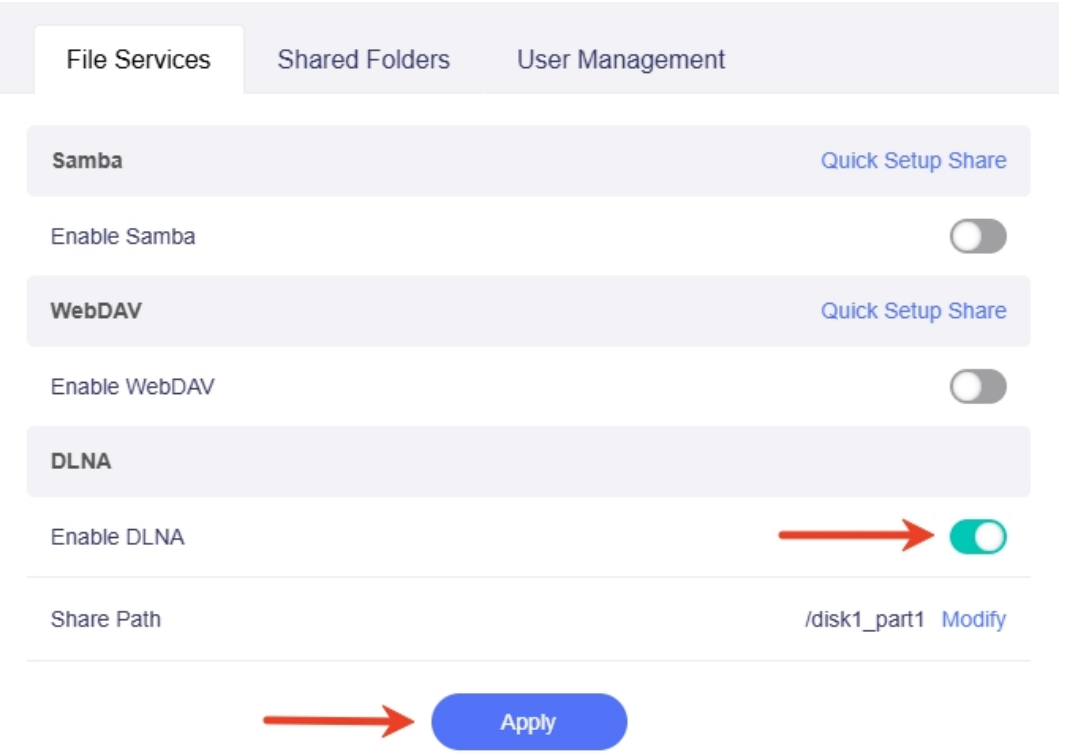
6. Récupérez le lien d’accès au dossier.
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via WebDAV.



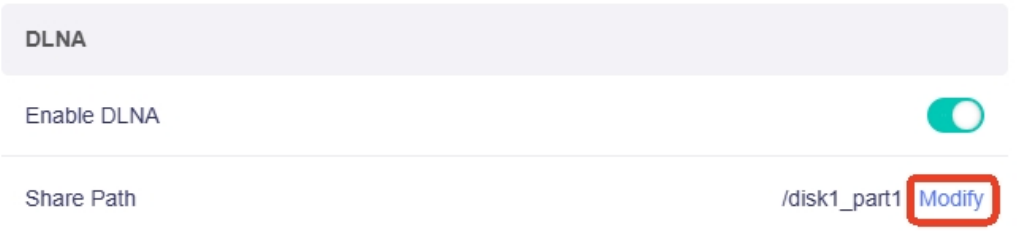
Remarque : si vous activez **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** et accédez au dossier depuis le réseau en amont, remplacez l’IP du routeur dans le lien, 192.168.8.1 par défaut, par son IP WAN affichée sur la page INTERNET.

12.3.4 Configuration de DLNA

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



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



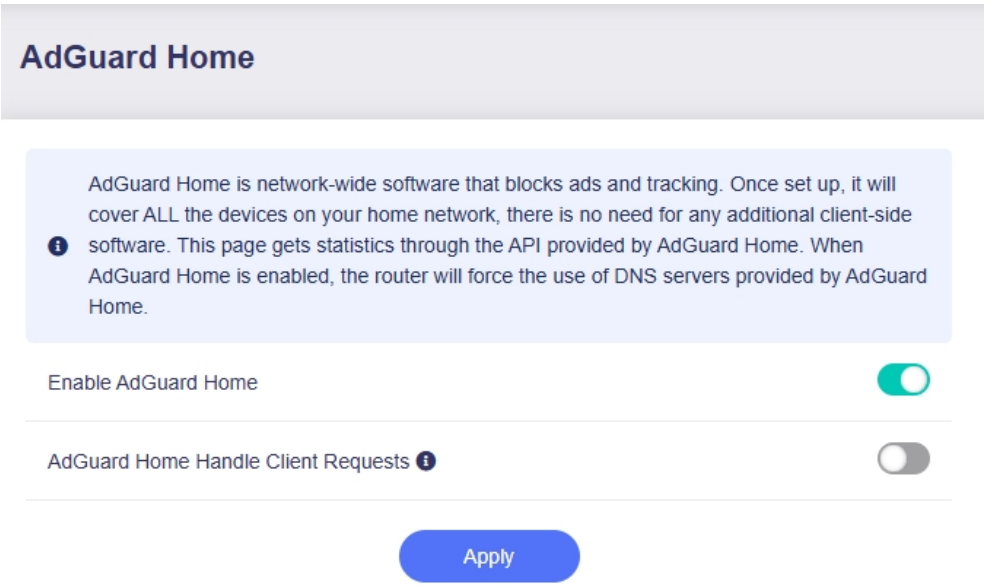
3. Connectez votre téléviseur intelligent au routeur. Il détecte automatiquement le serveur DLNA.

12.4 AdGuard Home

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

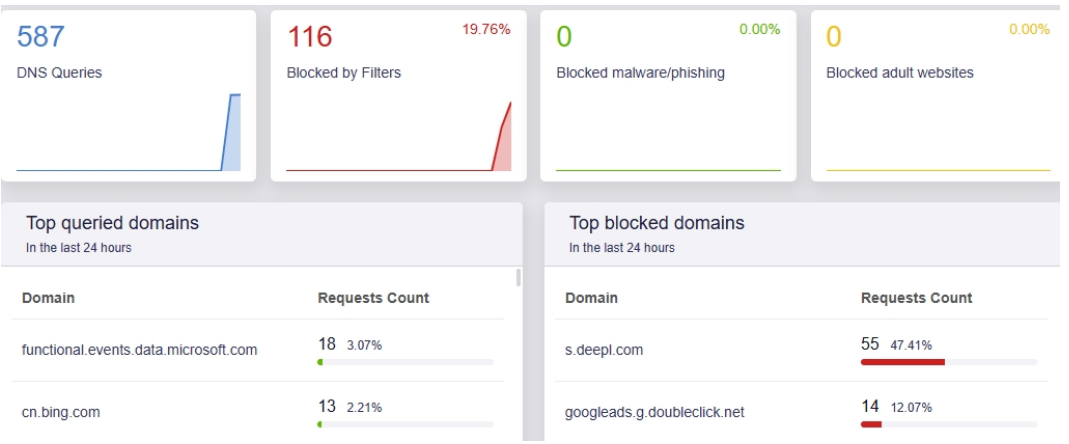
Suivez les étapes ci-dessous pour configurer AdGuard Home.

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

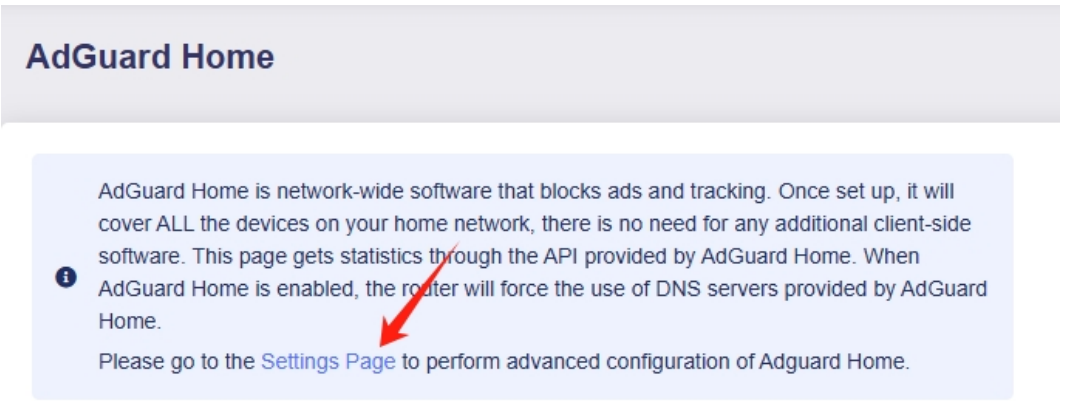


   - **AdGuard Home traite les requêtes clients (AdGuard Home Handles Client Requests)** : les requêtes DNS des clients sont alors traitées directement par AdGuard Home. Cela empêche toutefois les règles VPN fondées sur les domaines de fonctionner.

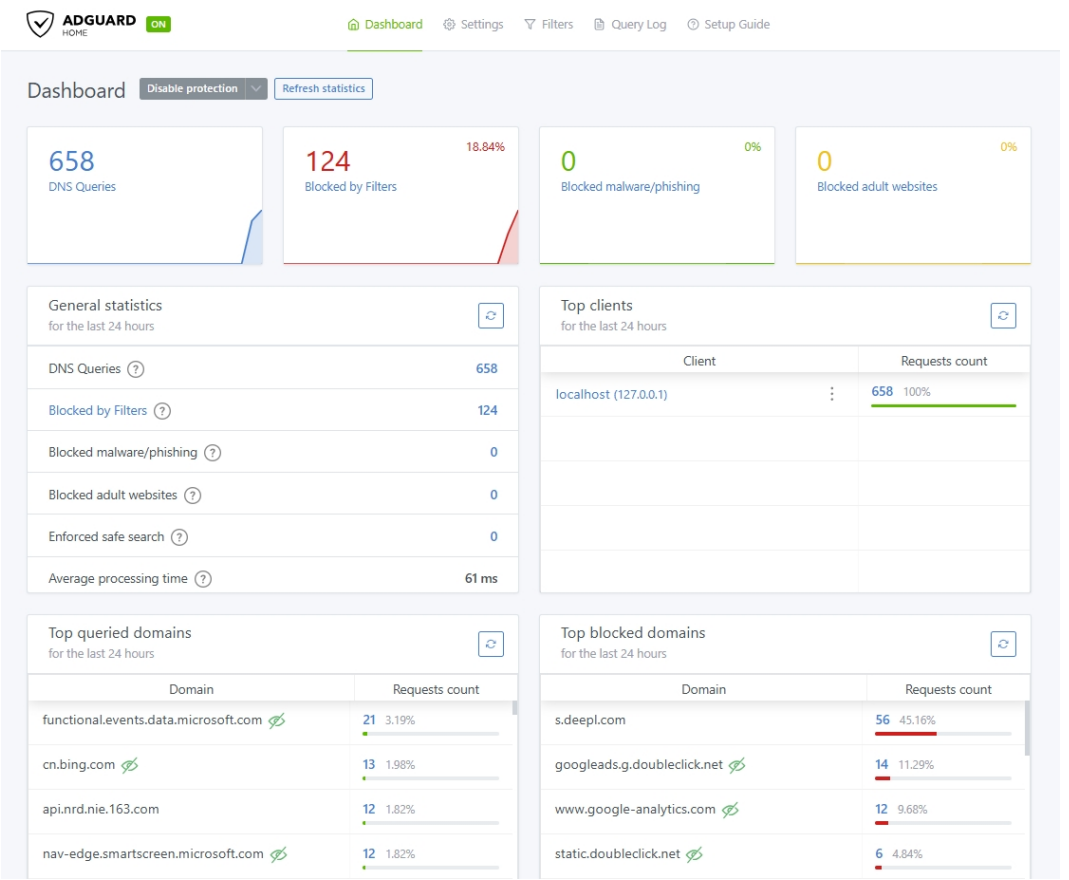
2. La page charge automatiquement les statistiques DNS, comme les requêtes et les domaines bloqués, via l'API d'AdGuard Home.



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



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


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

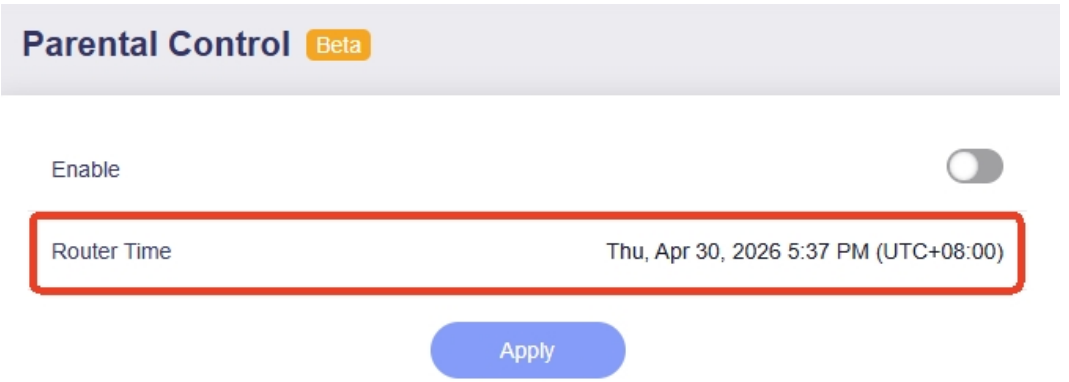
12.5 Contrôle parental

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

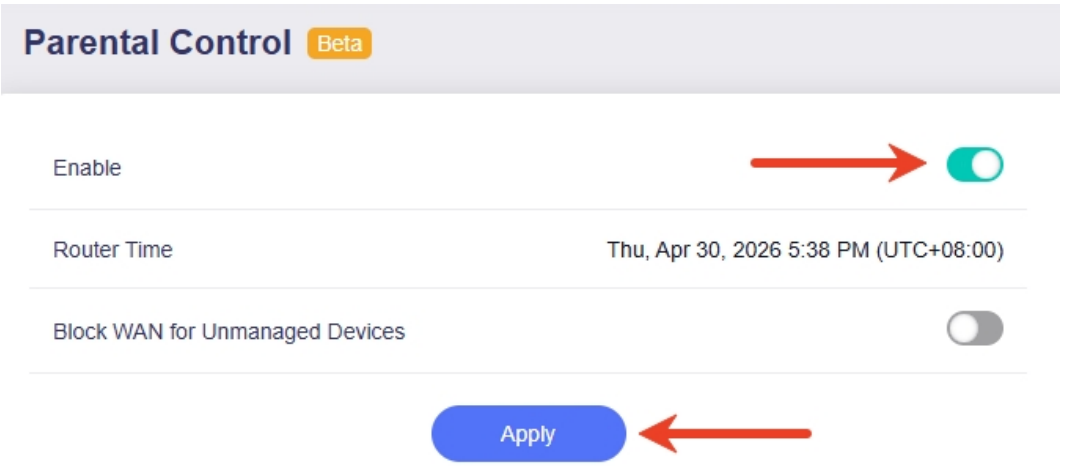
12.5.1 Configuration rapide

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

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



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



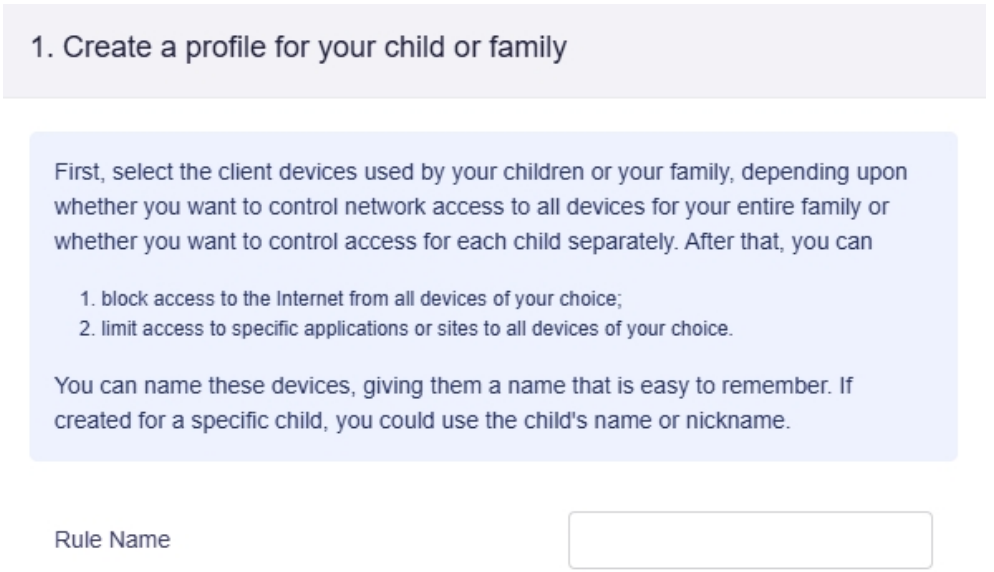
- **Bloquer le WAN pour les appareils non gérés (Block WAN for Unmanaged Devices)** : bloque l'accès Internet des appareils absents de la liste du contrôle parental.

Voici un exemple d’utilisation.

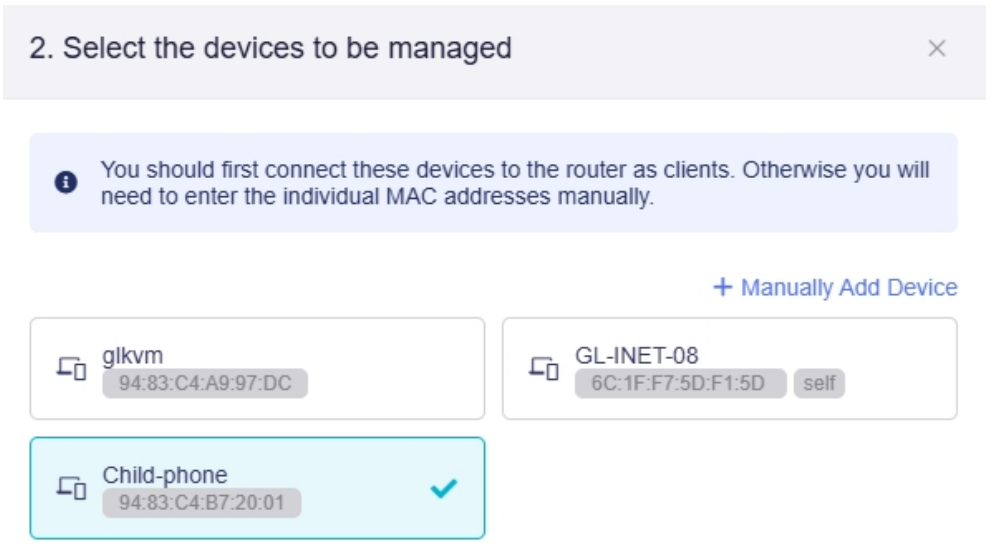
Scénario : les appareils de ce profil peuvent accéder à Internet uniquement pour étudier de 8 h à 11 h en semaine, et pour jouer de 18 h à 20 h le week-end. L’accès Internet est bloqué par défaut en dehors de ces plages.

Étapes de configuration :

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

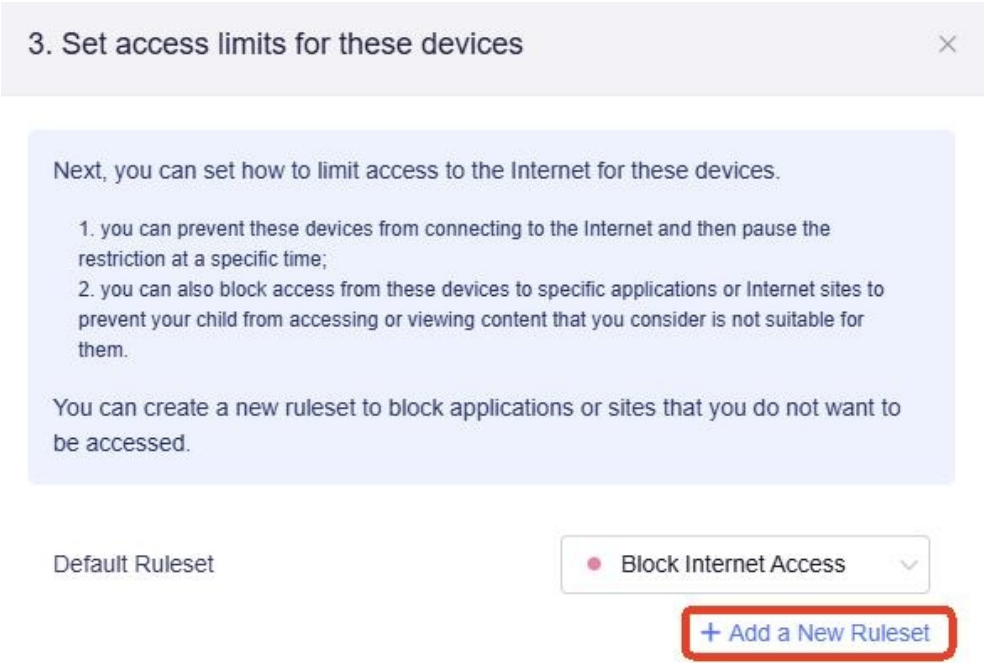


2. Sélectionnez les appareils à gérer. Connectez-les d’abord au routeur. S’ils n’y ont jamais été connectés, ajoutez-les manuellement avec leur adresse MAC.

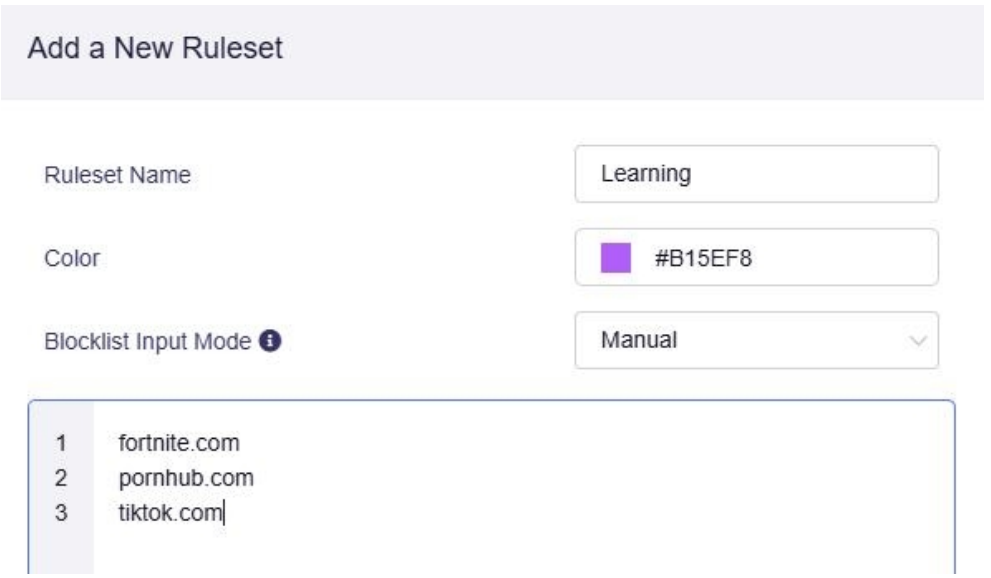


3. Définissez les limites d’accès.

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

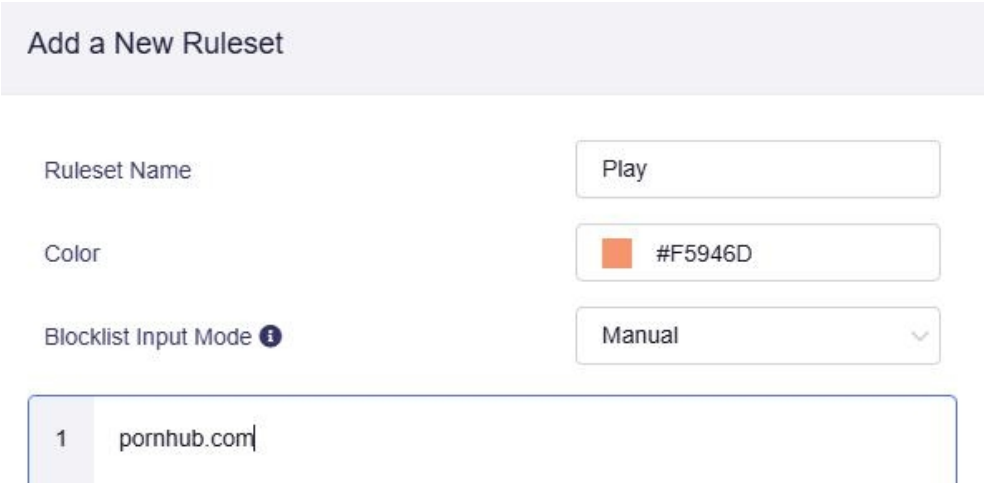


Définissez le nom, par exemple Étude, et la couleur du jeu de règles. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.

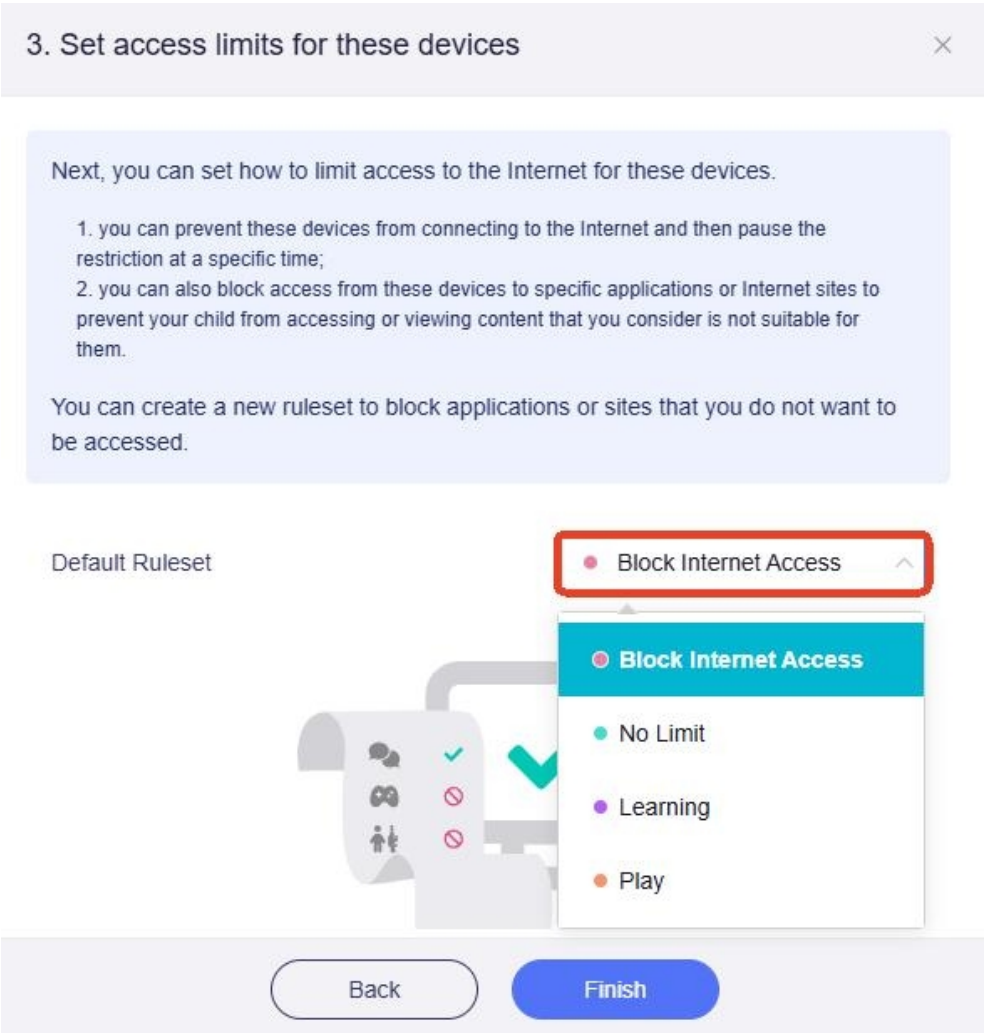


Remarque : les domaines de la liste de blocage englobent leurs sous-domaines. Par exemple, « example.com » inclut aussi « subdomain.example.com ».

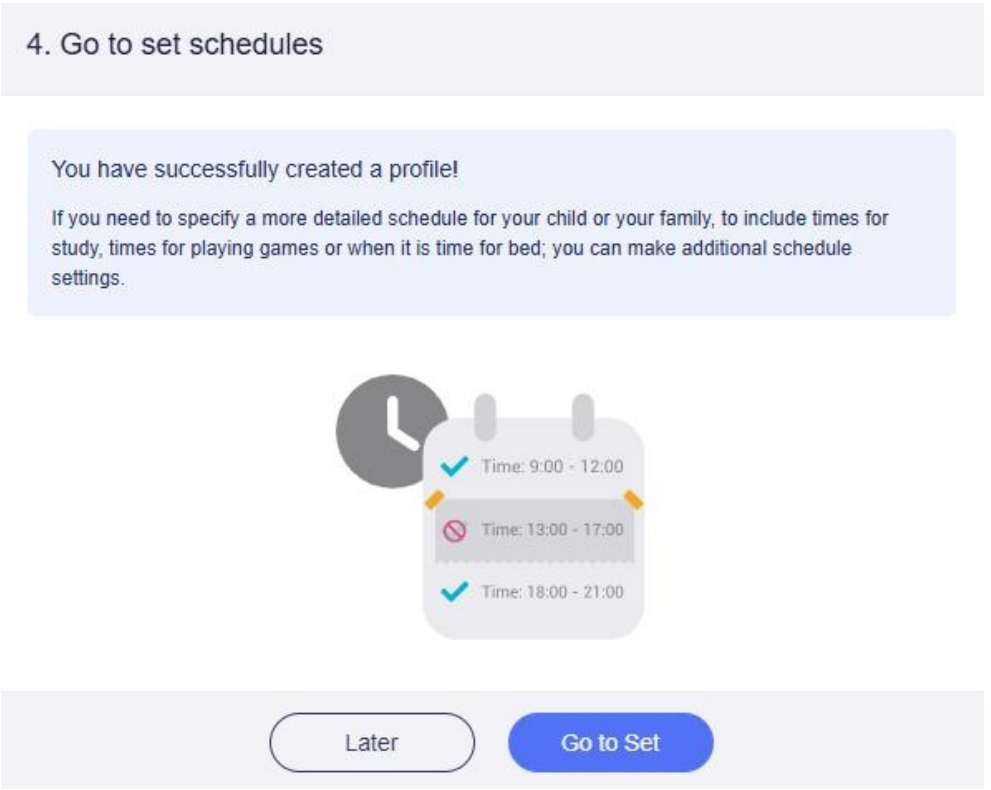
Créez de la même façon un autre jeu de règles. Définissez son nom, par exemple Jeu, et sa couleur. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.



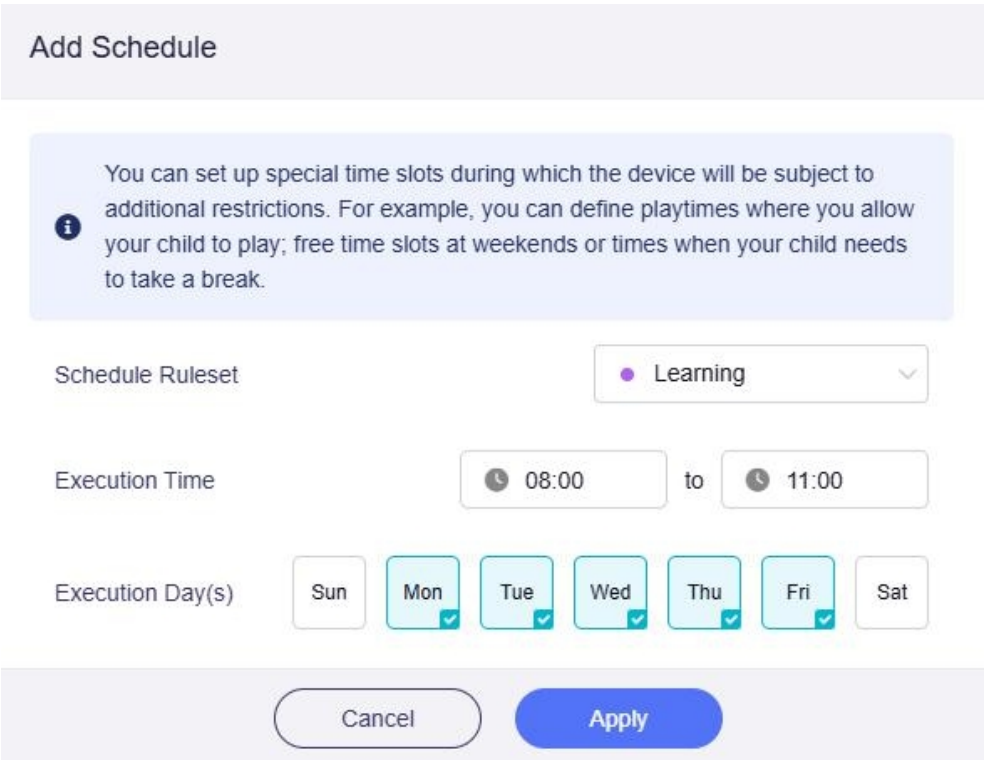
Vous disposez alors de quatre jeux de règles. Sélectionnez **Bloquer l’accès Internet (Block Internet Access)** comme **Jeu de règles par défaut (Default Ruleset)**, puis cliquez sur **Terminer (Finish)**.



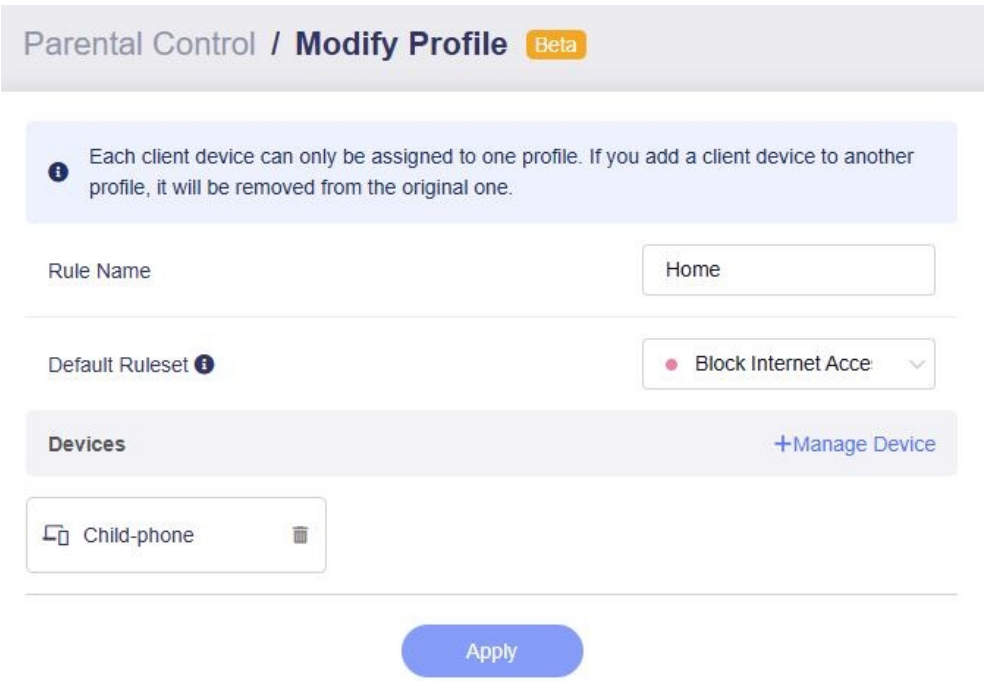
4. Définissez ensuite le planning du profil. Cliquez sur **Configurer (Go to Set)**.



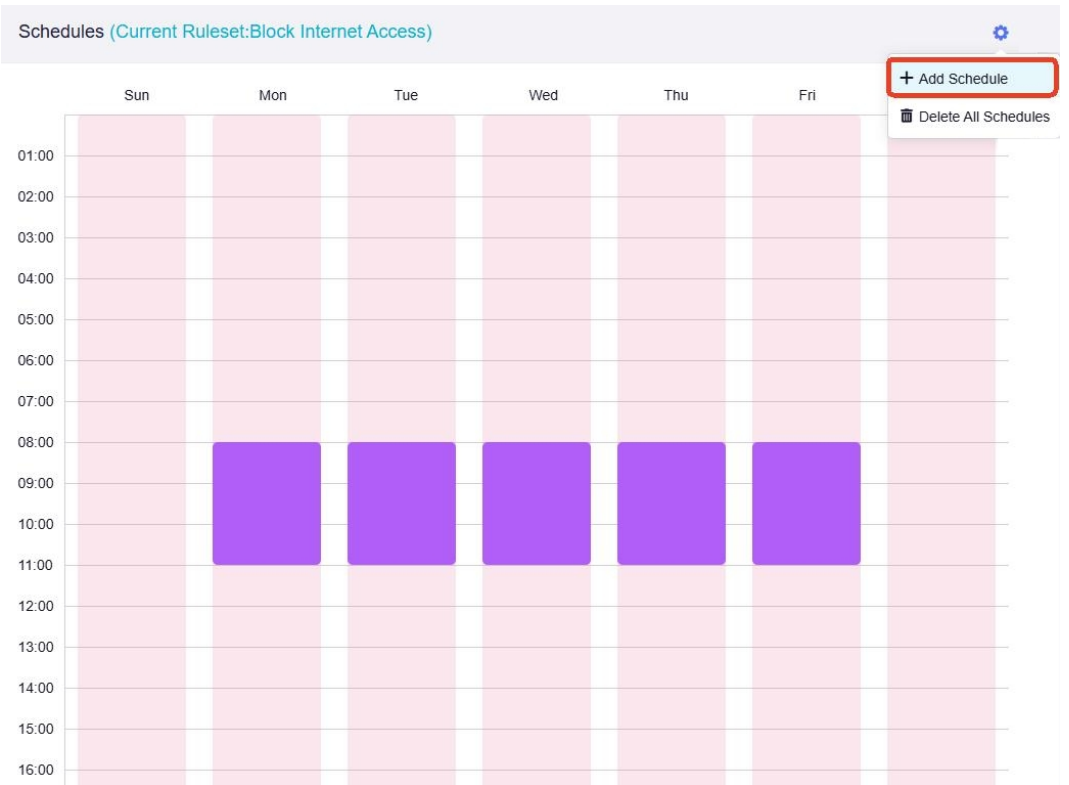
Ajoutez le jeu de règles **Étude (Learning)** au planning. Définissez l'**horaire d'exécution (Execution Time)** de 8 h à 11 h en semaine, puis cliquez sur **Appliquer (Apply)**.



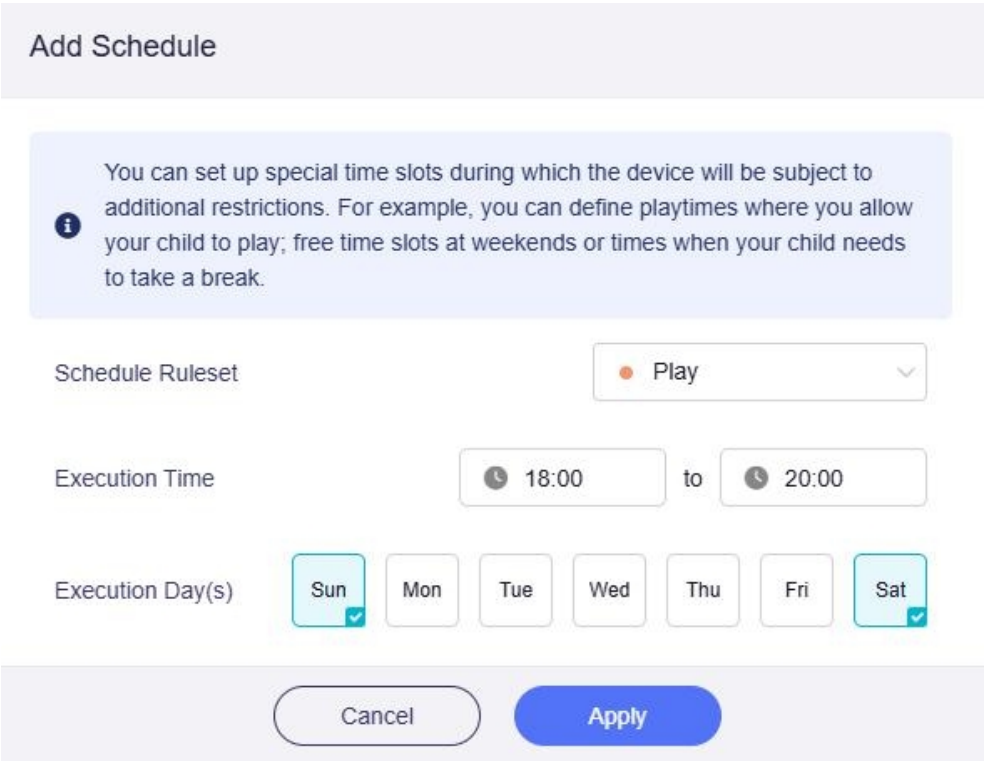
5. La page de modification du profil créé s'ouvre.



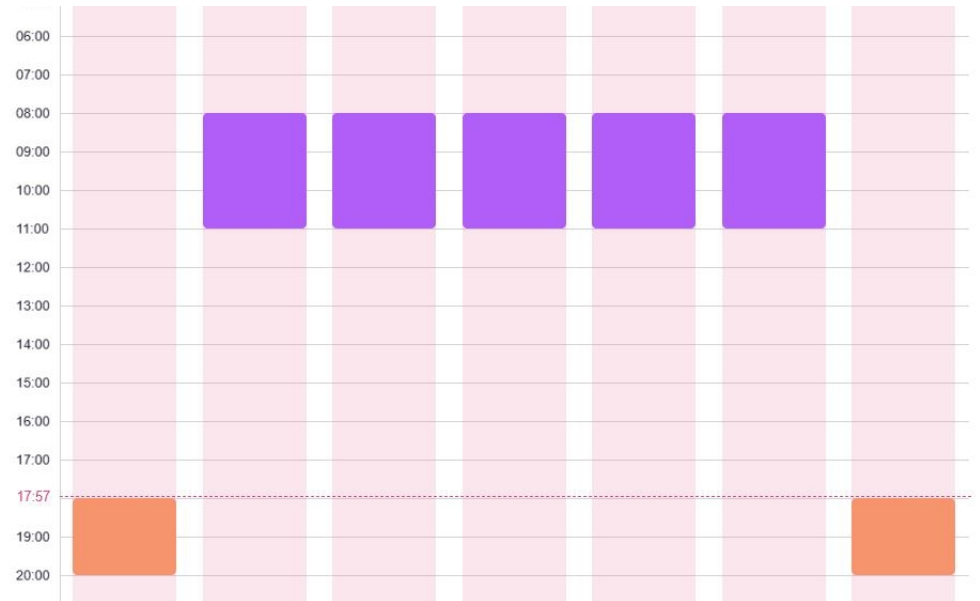
En bas de la page, le planning créé apparaît. Cliquez sur l'engrenage en haut à droite, puis sur **Ajouter une plage horaire (Add Schedule)**.



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



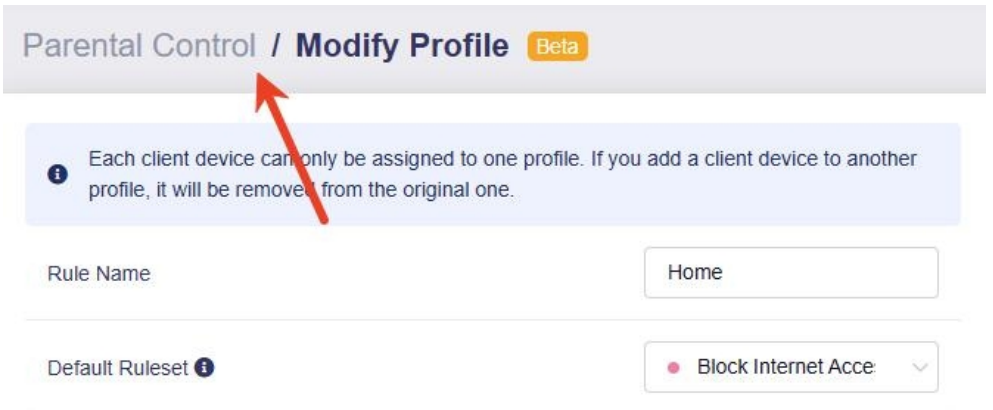
Le jeu de règles Jeu est ajouté au planning.



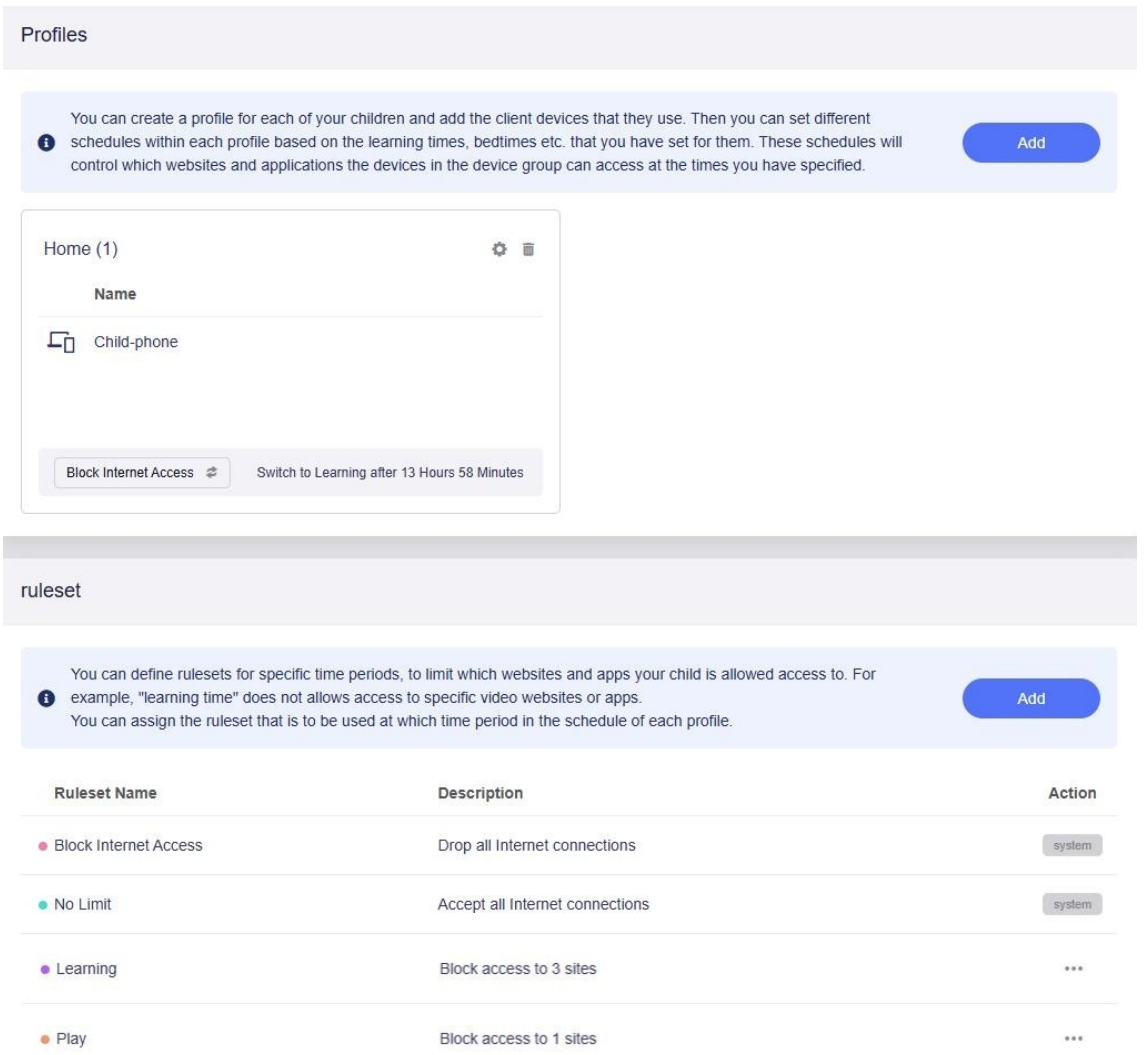
Conseils :

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

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



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



12.5.2 Dépannage

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

1. Problème de cache DNS.
   Les navigateurs et les systèmes d'exploitation conservent un cache DNS qui peut retarder l'application des changements. Videz-le pour appliquer les modifications immédiatement.
2. La plage horaire du profil n'a pas encore commencé.
3. Le domaine saisi peut être incorrect.
   Le domaine public d'un site est facile à trouver, mais les domaines d'API utilisés par les applications sont rarement publiés. Pour les identifier, utilisez un outil de capture de paquets comme Wireshark ou recherchez les informations correspondantes.
   Par exemple, pour bloquer « www.google.com », saisir « google.com » donne de meilleurs résultats que « www.google.com ».
4. L'appareil cible utilise une nouvelle adresse MAC aléatoire à chaque connexion, ce qui empêche les règles de s'appliquer. Désactivez cette fonction sur l'appareil, puis ajoutez-le de nouveau au profil.

12.6 ZeroTier

ZeroTier est un VPN défini par logiciel qui permet aux appareils de communiquer sur Internet de manière sécurisée et chiffrée. Il crée un réseau virtuel privé sur lequel les appareils communiquent comme s'ils appartenaient au même réseau local, indépendamment de leur emplacement physique et de la topologie du réseau. ZeroTier est simple à configurer et à utiliser ; il propose le chiffrement de bout en bout, la segmentation du réseau et la création de ponts réseau.

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

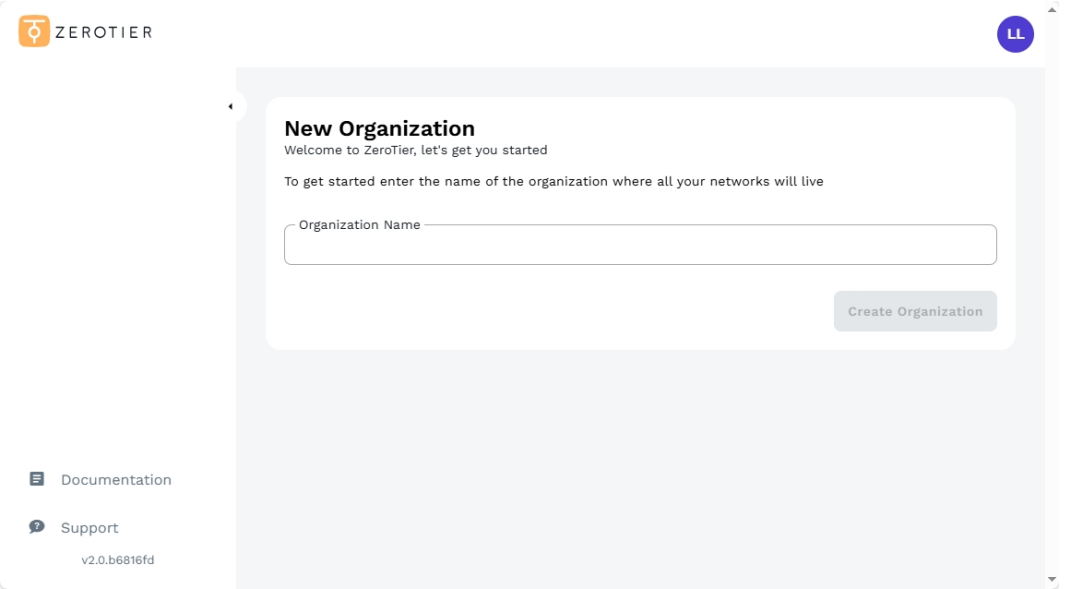
Remarque :

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

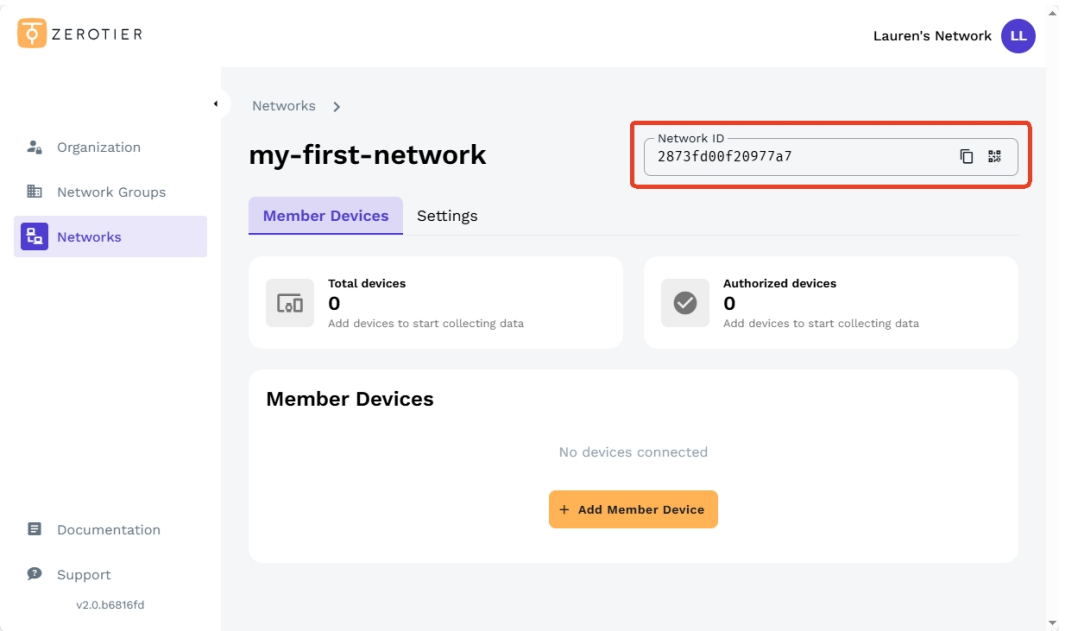
12.6.1 Configuration de ZeroTier

ZeroTier Central existe en deux versions : New Central et Legacy Central.
Les étapes suivantes utilisent New Central.

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

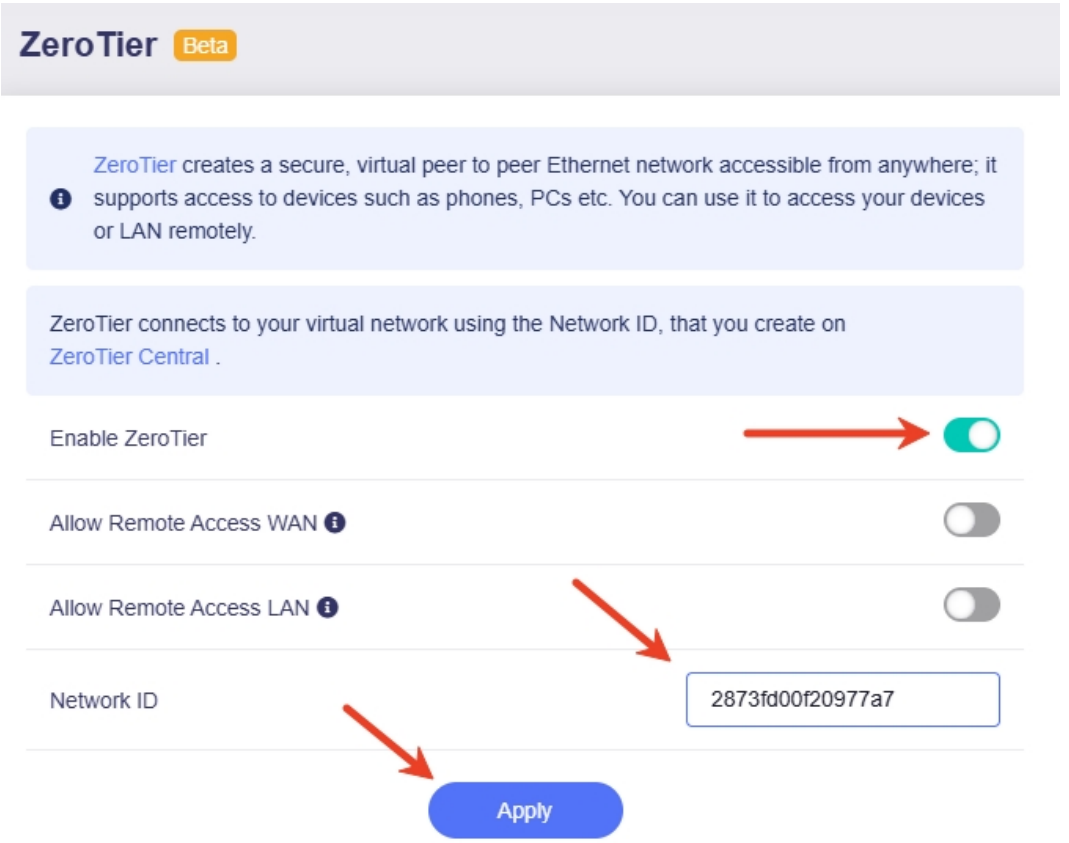


3. Choisissez une offre. L'exemple utilise l'**offre Personal**, qui comprend 10 appareils, un administrateur et un réseau. Pour ajouter des réseaux, des appareils, des routes personnalisées ou un DNS, choisissez une autre offre payante.
4. Votre réseau ZeroTier est créé.

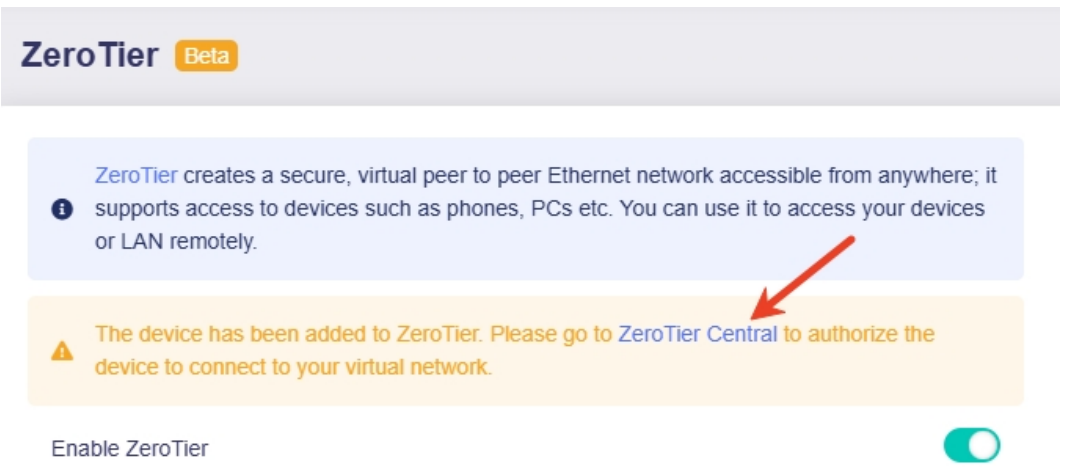


Notez l'**identifiant du réseau (Network ID)**, une suite alphanumérique de 16 caractères affichée en haut à droite. Il sera nécessaire pour connecter les autres appareils.

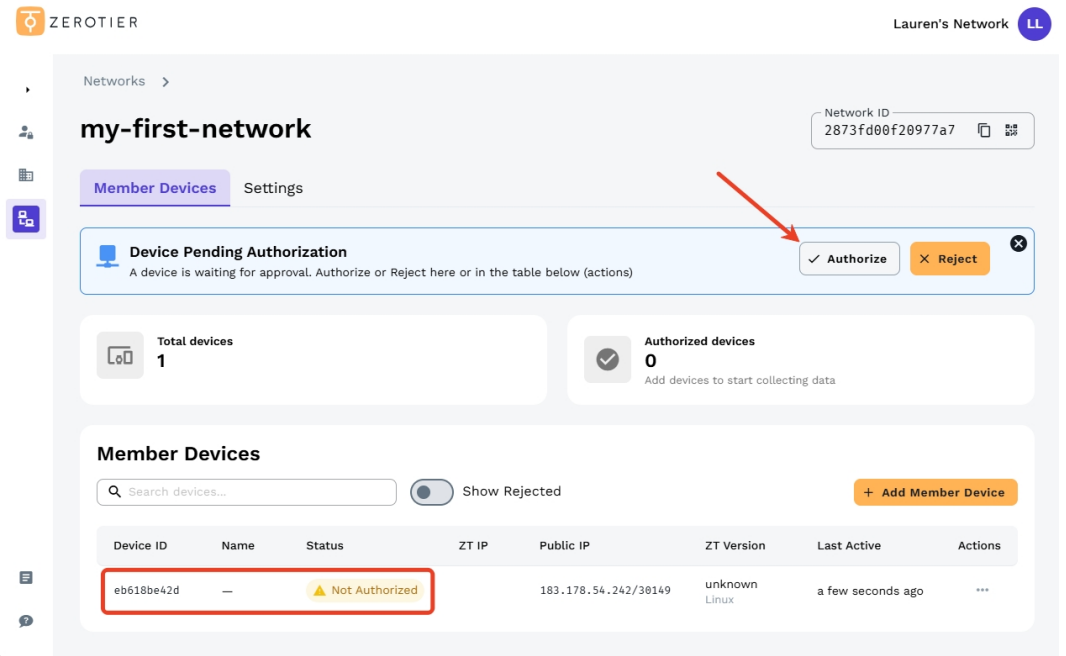
5. Dans l'interface Web du routeur, ouvrez **APPLICATIONS** > **ZeroTier**. Activez ZeroTier, saisissez l'**identifiant du réseau (Network ID)**, puis cliquez sur **Appliquer (Apply)**.



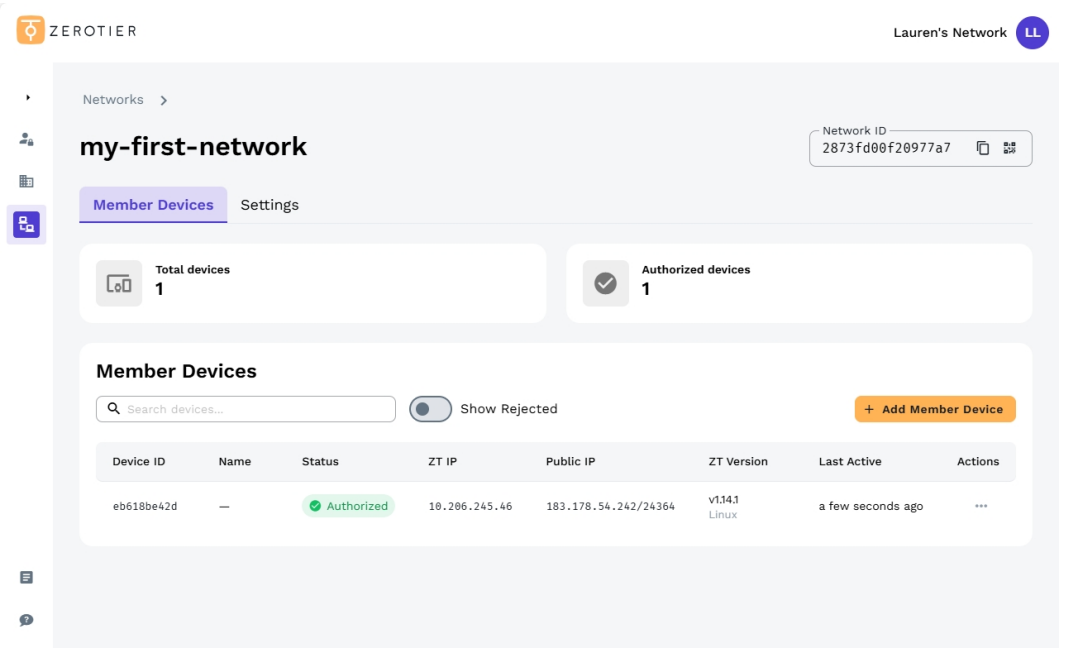
Après un court instant, la page indique qu'une autorisation est nécessaire. Cliquez sur le lien **ZeroTier Central** pour ouvrir la plateforme.



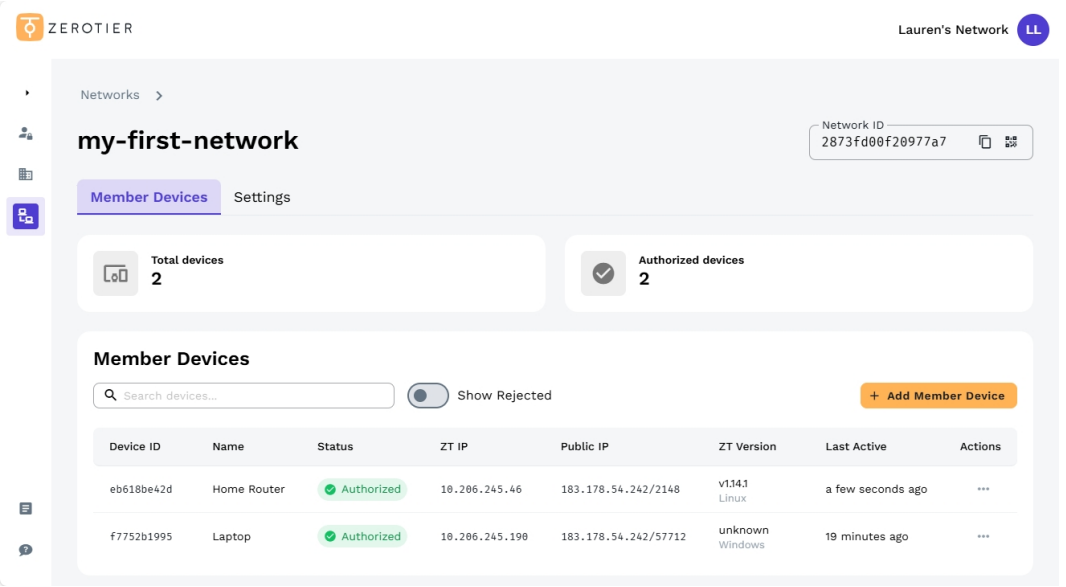
6. Dans ZeroTier Central, repérez l'appareil en attente et autorisez-le.



Une fois autorisé, il apparaît comme ci-dessous.

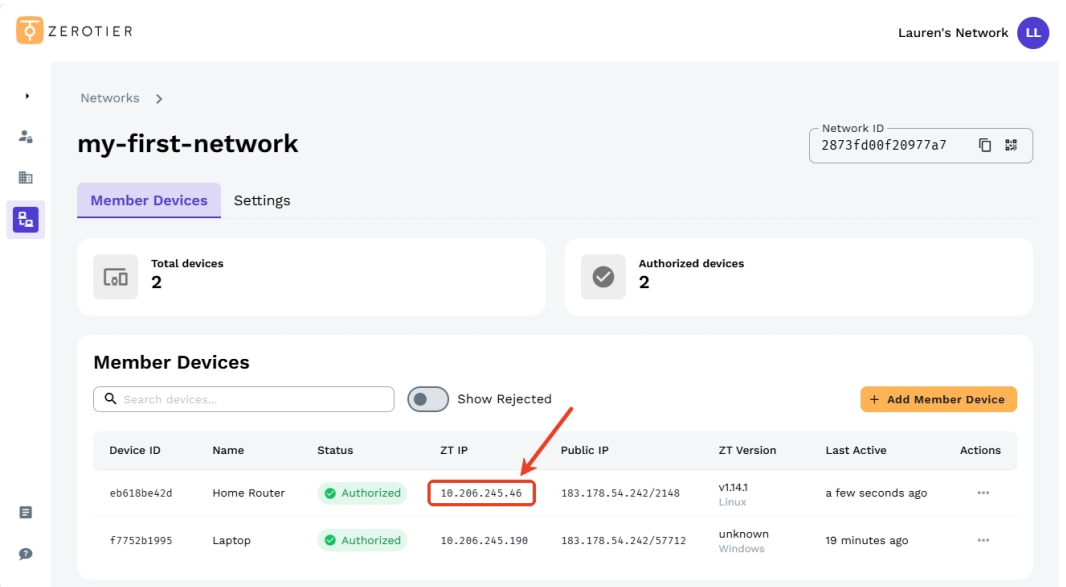


7. Ajoutez un autre appareil, comme un ordinateur ou un smartphone, au même réseau en suivant ce guide. Une fois l'ajout réussi, la page affiche les informations des membres : **identifiant de l'appareil (Device ID)**, **nom (Name)**, **état (Status)**, **IP gérée (Managed IP)** et **IP publique (Public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



Conseil : cliquez sur l'icône à trois points à droite pour modifier les paramètres d'un appareil membre : nom de l'appareil, adresse(s) IP gérée(s) (Managed IP(s)) et paramètres avancés.

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

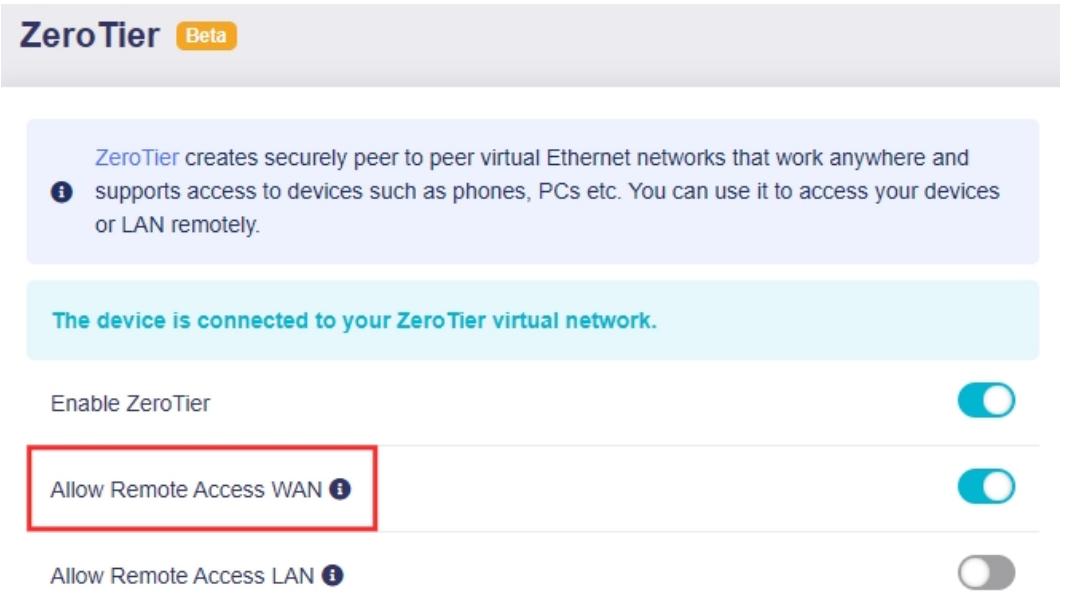


Utilisez ensuite cette IP pour accéder au routeur depuis votre ordinateur portable connecté au même réseau ZeroTier.

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

12.6.2 Autoriser l’accès distant au WAN

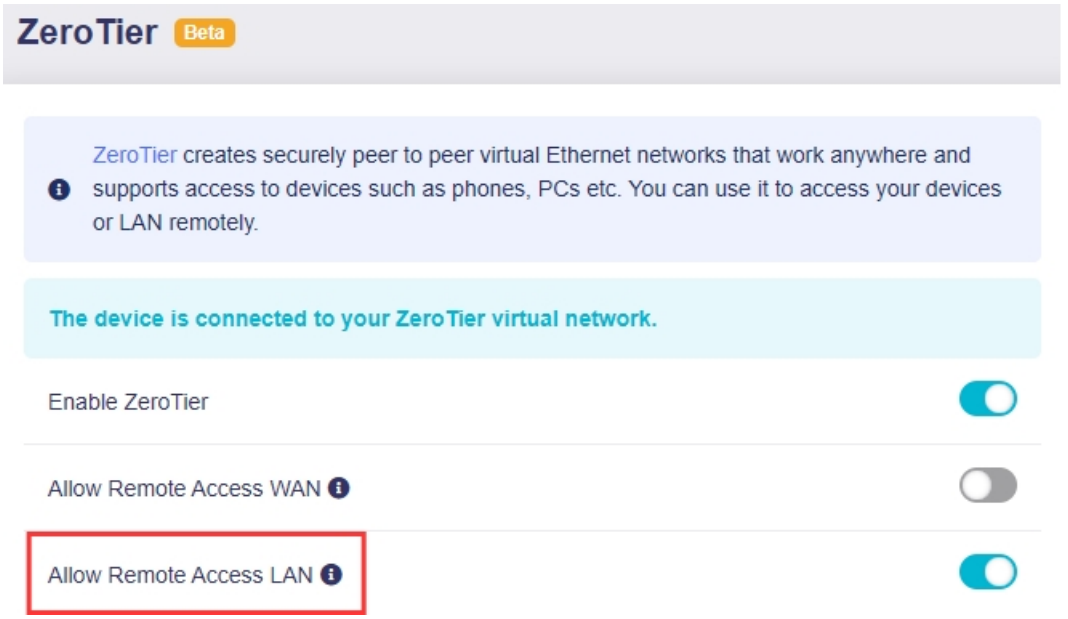
Si cette option est activée, les ressources côté WAN de l’appareil sont accessibles par le réseau virtuel ZeroTier. Consultez cette page pour en savoir plus.



Remarque : ajoutez des règles de routage au réseau ZeroTier pour utiliser cette fonction. Legacy Central permet d’ajouter gratuitement une route personnalisée. New Central nécessite une offre Essential ou supérieure. Consultez cette page pour les tarifs.

12.6.3 Autoriser l’accès distant au LAN

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



Remarque : ajoutez des règles de routage au réseau ZeroTier pour utiliser cette fonction. Legacy Central permet d’ajouter gratuitement une route personnalisée. New Central nécessite une offre Essential ou supérieure. Consultez cette page pour les tarifs.

12.7 Tailscale

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

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

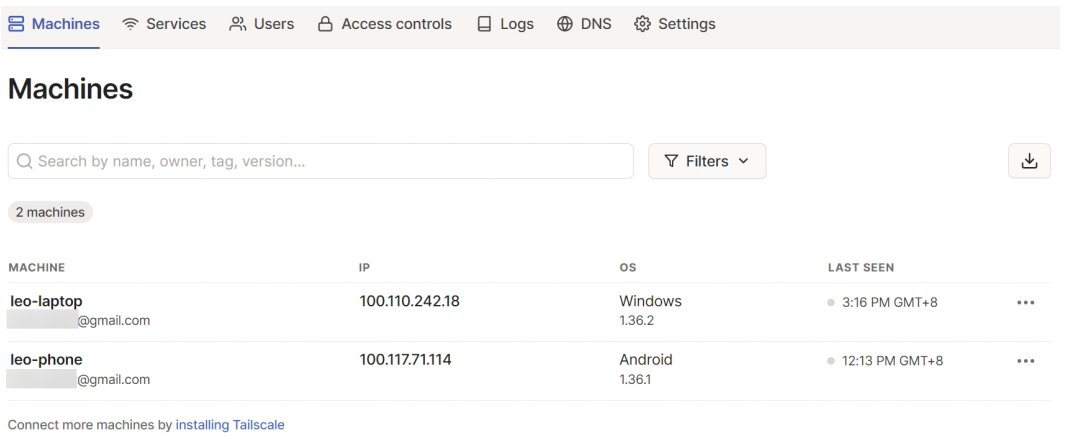
Remarque :

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

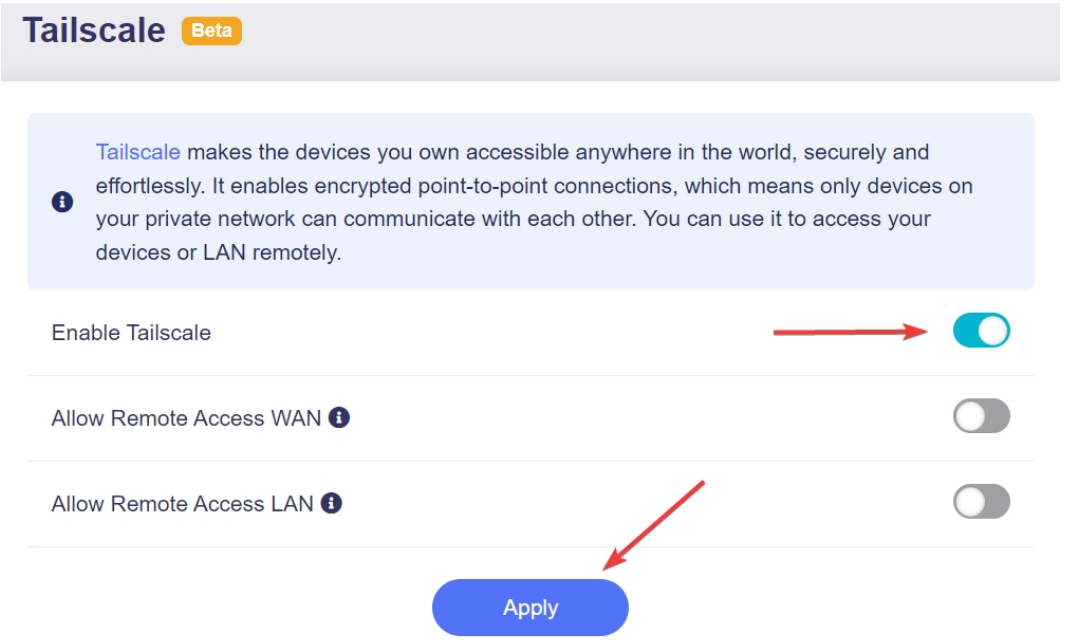
12.7.1 Configuration de Tailscale

L'exemple suivant utilise GL-MT2500 pour configurer un réseau Tailscale.

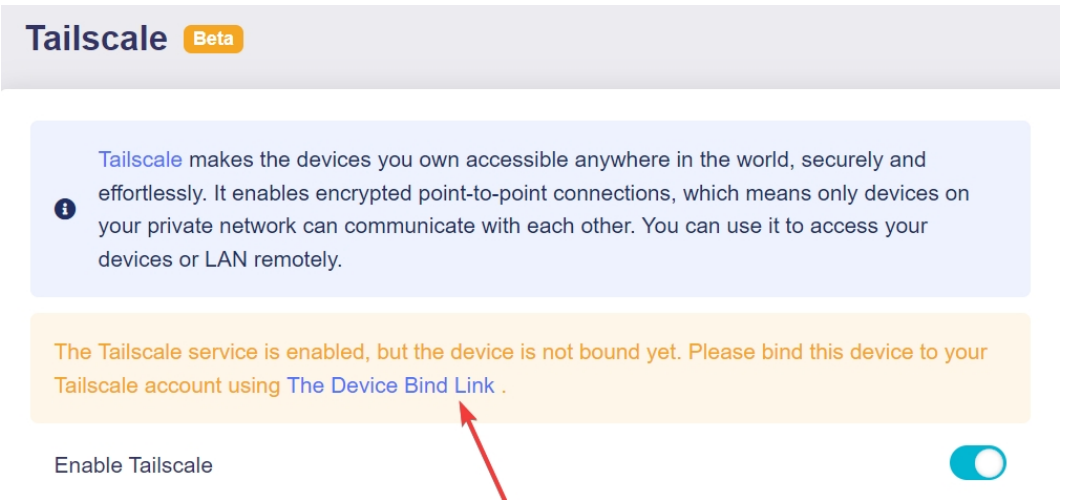
1. Créez d'abord un compte Tailscale et associez-y un ou deux appareils pour effectuer des tests. Ils apparaissent ensuite dans la console Tailscale.



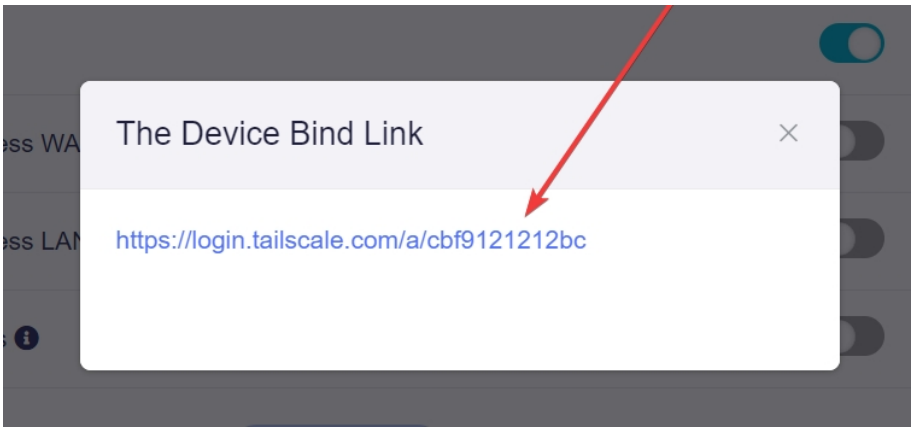
2. Dans l'interface Web du routeur, ouvrez **APPLICATIONS** > **Tailscale**. Activez **Activer Tailscale (Enable Tailscale)**, puis cliquez sur **Appliquer (Apply)**.



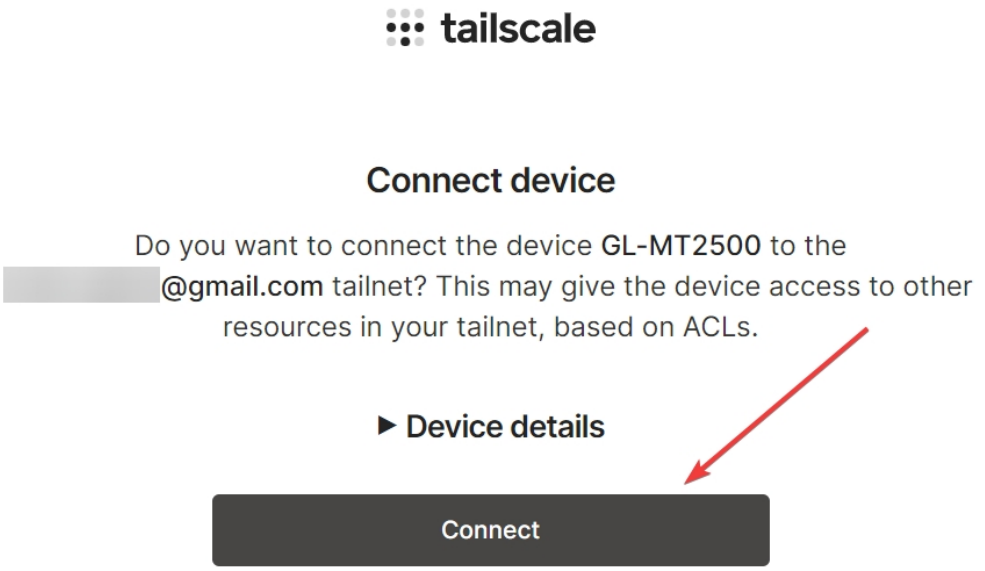
3. La page vous invite à associer l'appareil. Cliquez sur **Lien d'association de l'appareil (Device Bind Link)**.



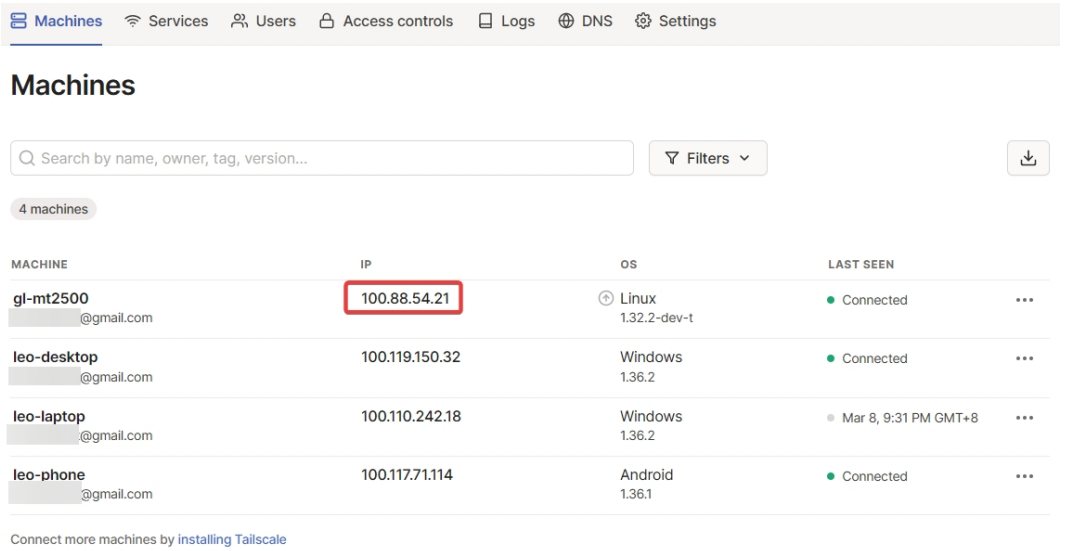
4. Dans la fenêtre qui s'affiche, cliquez sur le lien et connectez-vous à votre compte Tailscale.



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



6. La console d’administration Tailscale s’ouvre. Le routeur appartient désormais au réseau virtuel Tailscale et peut être joint à distance par son adresse virtuelle 100.88.54.21.

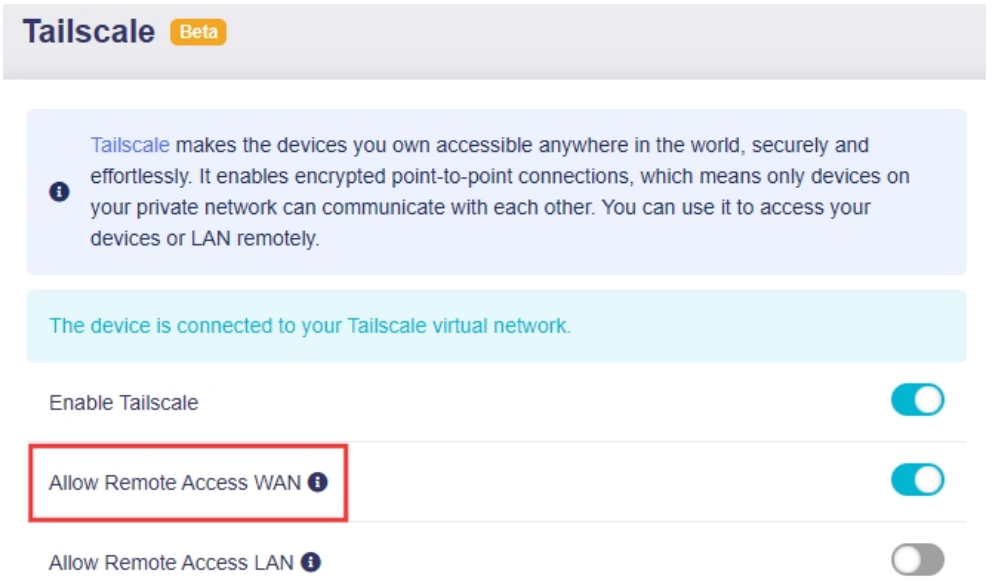


7. Testez la connexion.

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

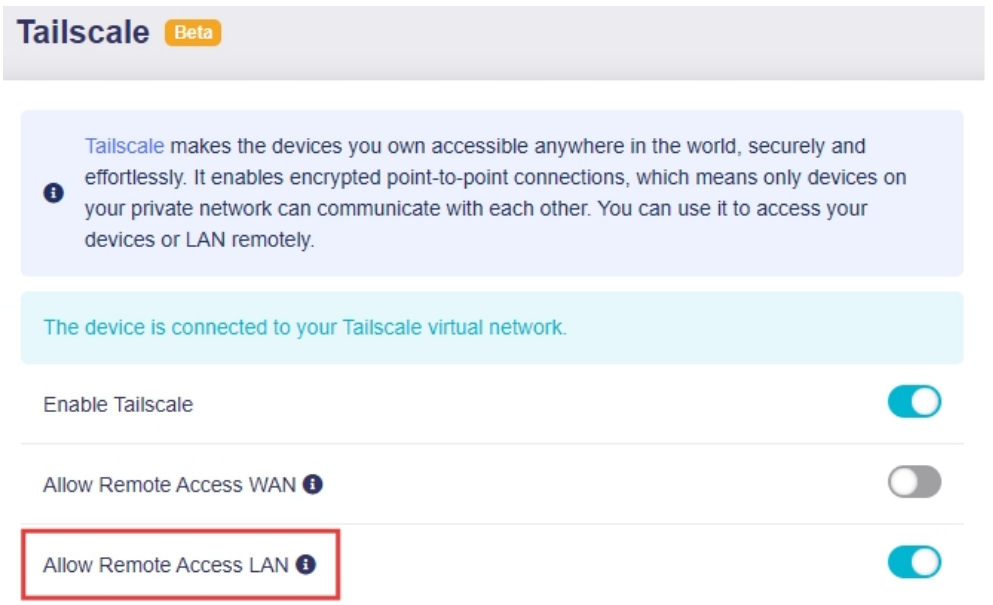
12.7.2 Autoriser l’accès distant au WAN

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



12.7.3 Autoriser l’accès distant au LAN

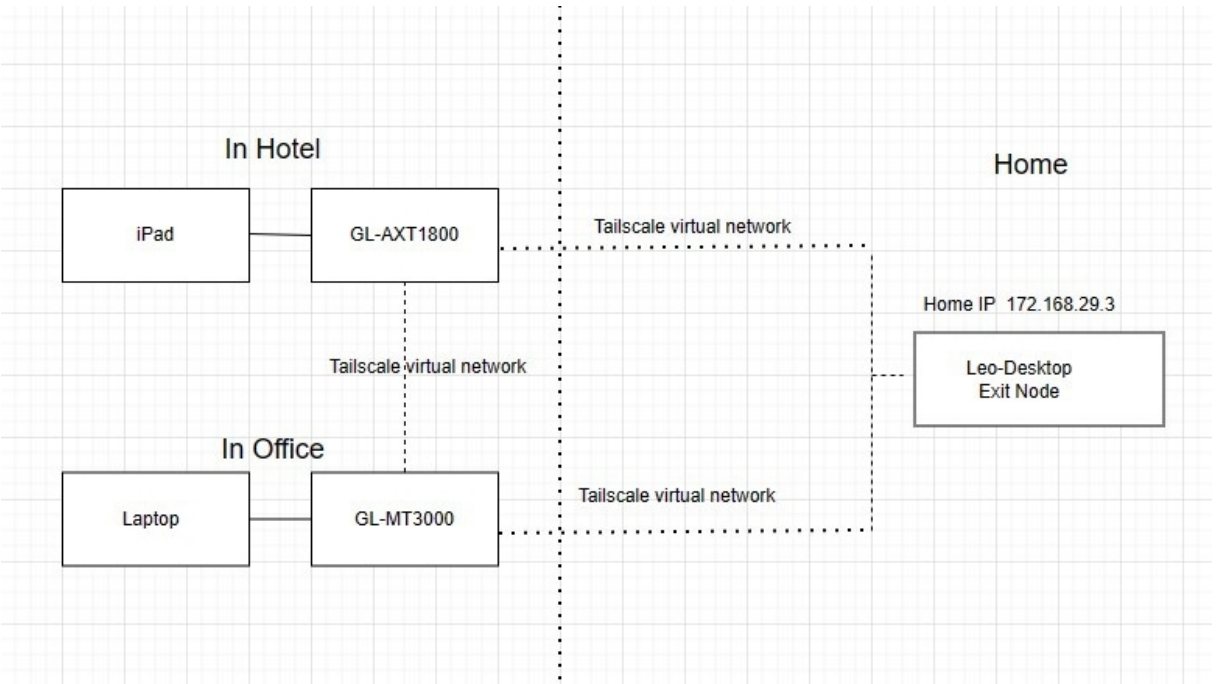
Si cette option est activée, les ressources côté LAN de l’appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



12.7.4 Nœuds de sortie personnalisés

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

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



Un nœud de sortie achemine le trafic Internet sortant des appareils du Tailnet et joue ainsi le rôle d'un serveur VPN. Tout le trafic Internet extérieur à Tailscale semble provenir de son emplacement, ce qui facilite l'accès aux contenus géorestreints et renforce la confidentialité. L'appareil chargé de cet acheminement est appelé « nœud de sortie ». Consultez cette page pour en savoir plus.

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

Chapitre 13

Réseau

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

13.1 Redirection de port

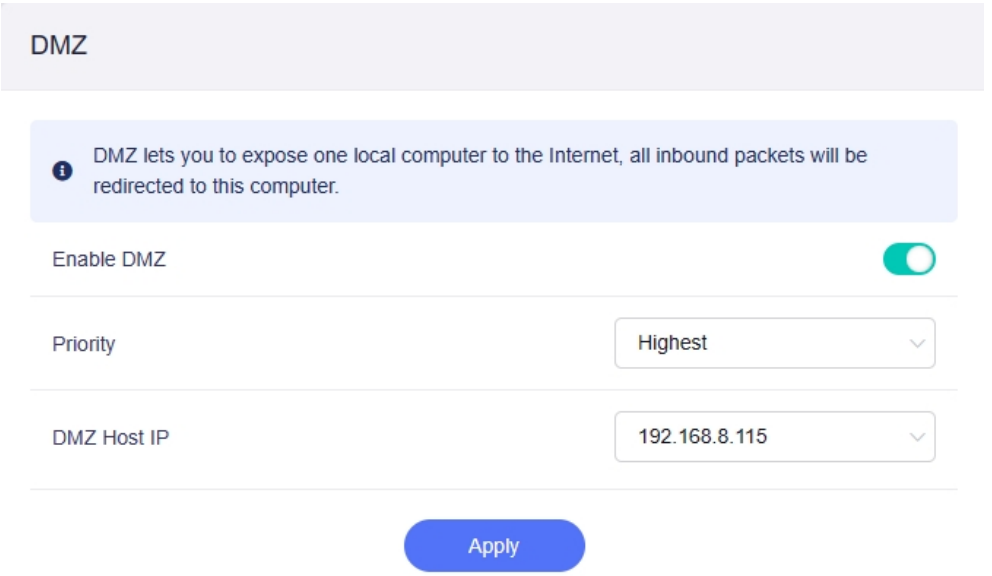
La redirection de port achemine les requêtes externes vers des appareils précis du réseau local. Cette page propose deux fonctions : **DMZ**, pour un accès direct complet à un appareil, et **Redirection de port (Port Forwarding)**, pour un accès ciblé à certains ports.

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



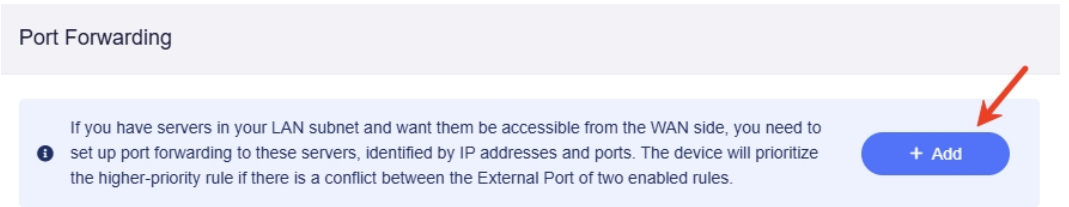
- **Priorité (Priority)** : choisissez La plus élevée ou La plus faible. Si la DMZ est prioritaire sur les règles de redirection de port, celles-ci deviennent inopérantes. Sinon, les requêtes ne sont transmises au client DMZ que si aucune règle ne correspond au port demandé.
- **IP de l'hôte DMZ (DMZ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

13.1.2 Redirection de port

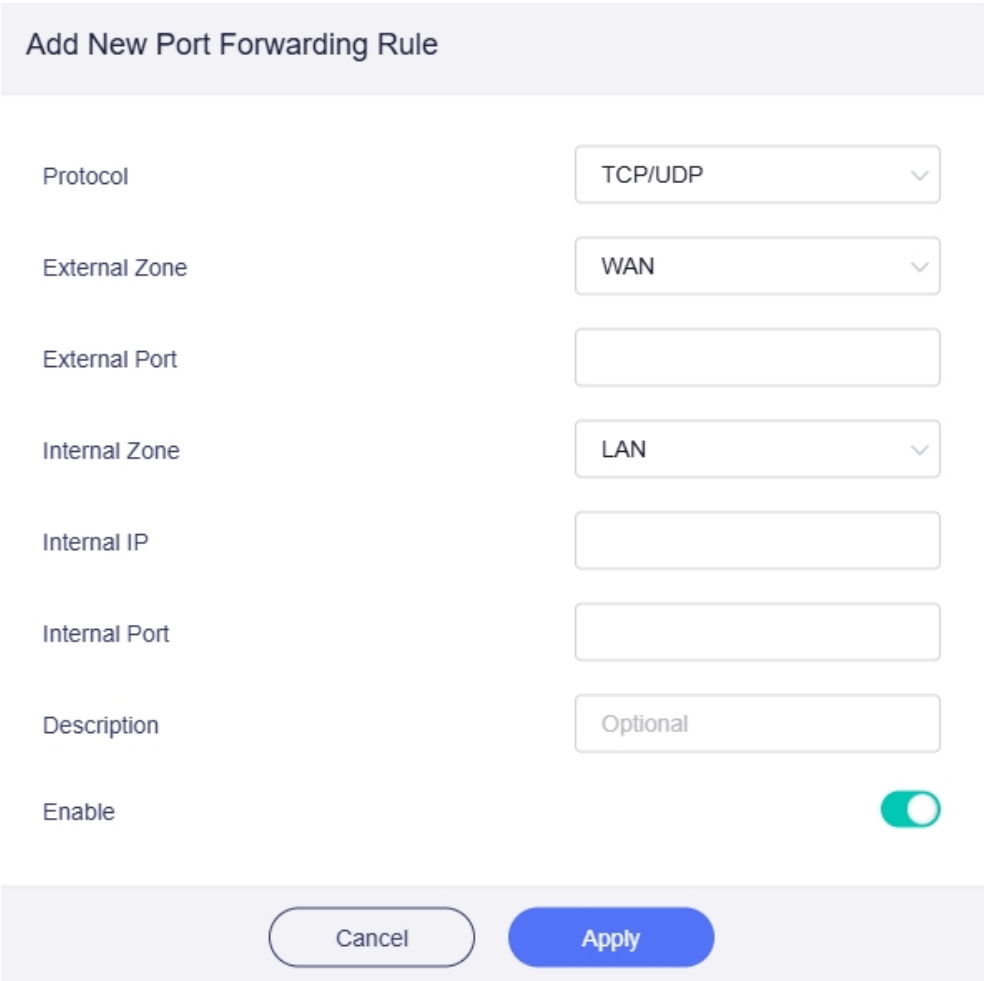
La redirection de port permet à des ordinateurs distants de se connecter à un ordinateur ou serveur local situé derrière le pare-feu LAN, comme un serveur Web ou FTP.

Pour configurer une redirection de port, procédez comme suit.

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



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



- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP et UDP.
- **Zone externe (External Zone)** : options disponibles : WAN, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN et LAN.
- **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, 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 Multi-WAN

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

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

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

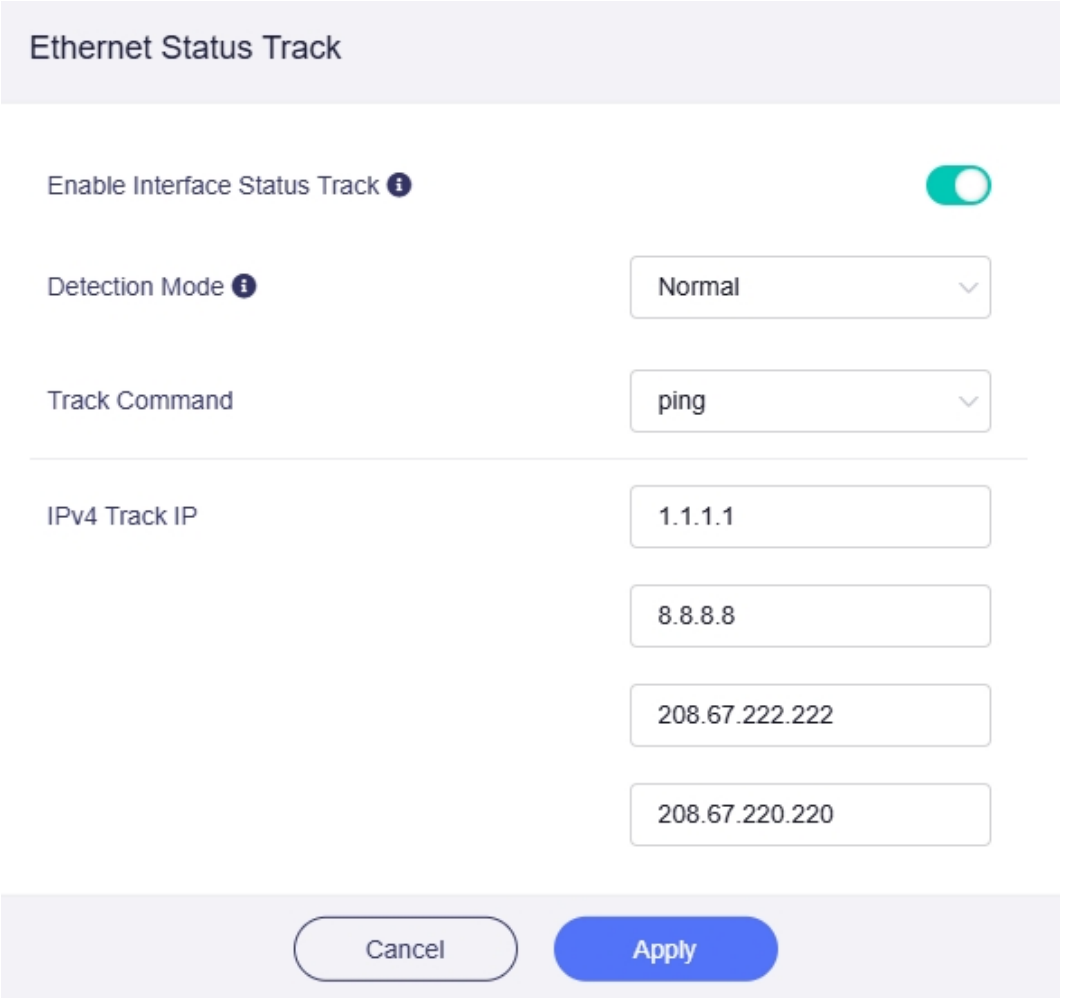
13.2.1 Suivi de l'état des interfaces

Brume 2 dispose de deux interfaces de connexion à Internet : Ethernet et partage de connexion USB. Il utilise la commande ping pour surveiller la connexion à l'adresse IP de destination et déterminer si l'interface est disponible. Un point vert apparaît à gauche si elle est disponible ; sinon, le point est gris.



Dans la section **Suivi de l'état des interfaces (Interface Status Track)**, cliquez sur l'engrenage à droite pour ouvrir les paramètres de suivi de chaque interface réseau.

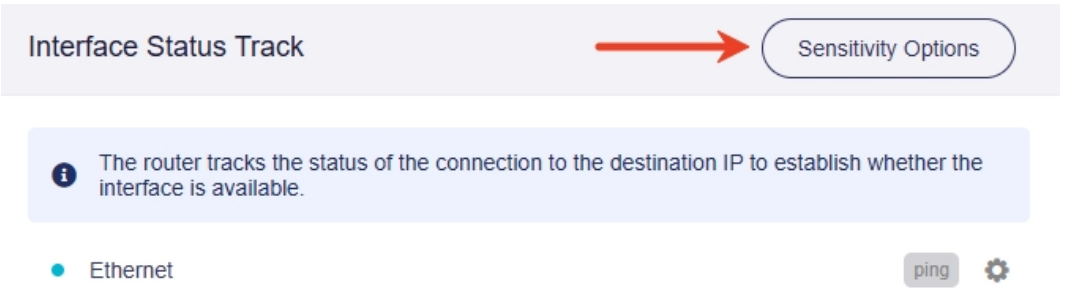
Les paramètres de suivi de l'interface Ethernet sont présentés ci-dessous. Les mêmes principes de configuration s'appliquent à l'autre interface.



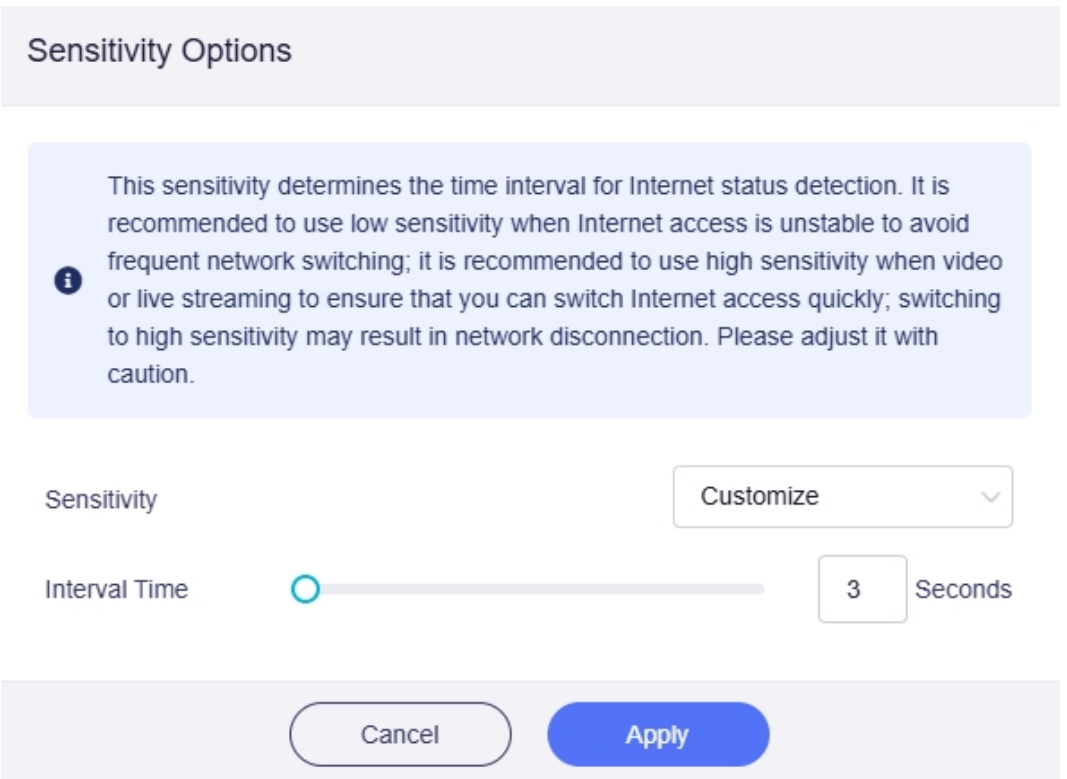
- **Activer le suivi de l'état de l'interface (Enable Interface Status Track)** : activé par défaut. Si vous le désactivez, le routeur détermine l'état de l'interface selon les conditions physiques, par exemple le branchement du câble Ethernet.
- **Mode de détection (Detection Mode)** : introduite sous 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.
  - **Mode normal (Normal Mode)** : utilisé par défaut.
  - **Mode données réduites (Low Data Mode)** : lance le suivi uniquement lorsqu'une erreur réseau survient sur l'interface. Utilisez-le avec un forfait de données limité. La reconnexion peut être légèrement plus lente qu'en mode normal. Il est activé par défaut uniquement pour l'interface cellulaire.
  - **Mode strict (Strict Mode)** : détermine l'état de l'interface uniquement à partir du résultat de la 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.

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.



Conseil : si le réseau est stable, une sensibilité élevée permet de basculer rapidement en cas de perte de connexion. Elle convient notamment au visionnage de vidéos, au streaming en direct et aux jeux. Si le réseau est instable, une sensibilité faible évite les basculements

fréquents et les échecs de connexion. Elle convient notamment au téléchargement de fichiers destinés à être mis en cache.

Remarque : le passage à une sensibilité élevée peut provoquer des interruptions ponctuelles de connexion. Modifiez ce réglage avec précaution.

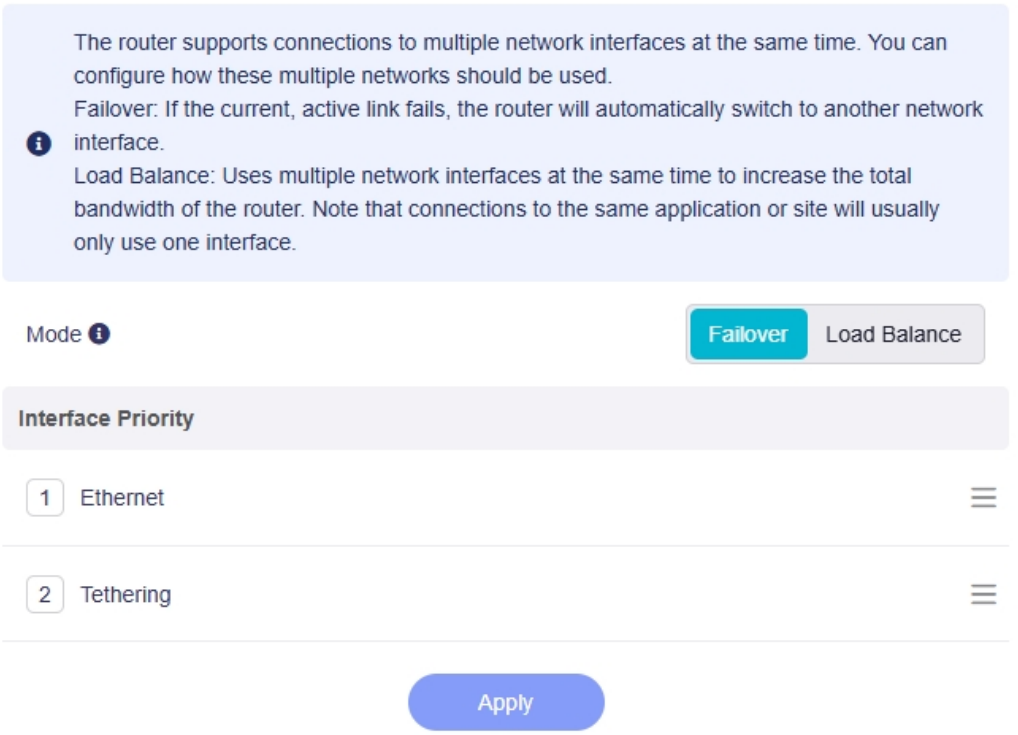
13.2.2 Mode Multi-WAN

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

Basculement

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

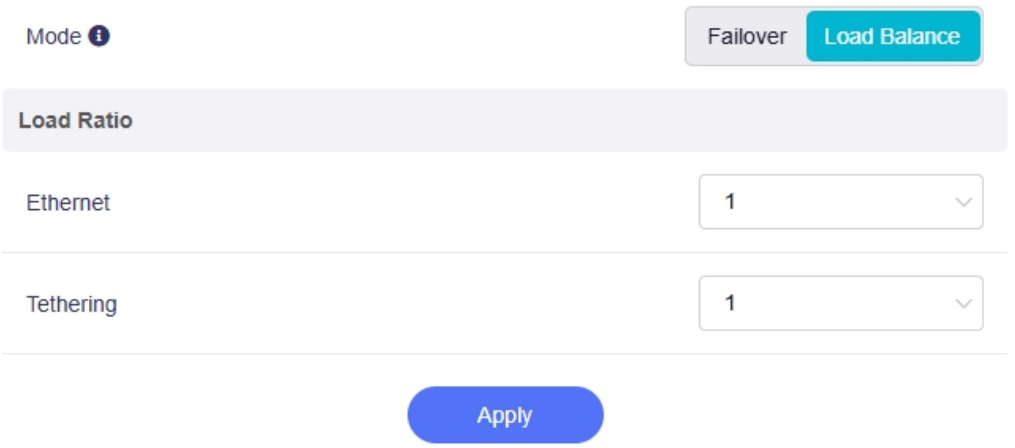
Vous pouvez définir une priorité pour chaque interface. En cas de défaillance, le routeur sélectionne l'interface disponible la plus prioritaire. Dès qu'une connexion plus prioritaire est rétablie, il l'utilise de nouveau automatiquement.



Équilibrage de charge

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

Le **rapport de charge (load ratio)** définit la proportion attribuée à chaque interface réseau. Le système répartit les nouvelles connexions entre les interfaces selon ce rapport. Par exemple, si le routeur est connecté simultanément à deux réseaux, comme Ethernet et le partage de connexion USB, et que ces deux interfaces permettent d'accéder à Internet, l'activation de la répartition de charge avec un rapport de 1:1 fait partager équitablement la bande passante entre les quatre interfaces. Le système répartit les nouvelles connexions entre ces quatre interfaces selon le rapport configuré.



Vous pouvez personnaliser le rapport de charge. Par exemple, si Ethernet offre 100 Mbit/s et le partage de connexion USB 200 Mbit/s, attribuez un poids de 1 à Ethernet et de 2 au partage de connexion USB. Le système répartit alors les nouvelles connexions entre les deux interfaces selon le rapport 1:2 : Ethernet prend en charge deux fois moins de connexions que le partage de connexion USB. À la différence du mode de basculement, ce mode optimise le débit global en équilibrant la charge du trafic 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.

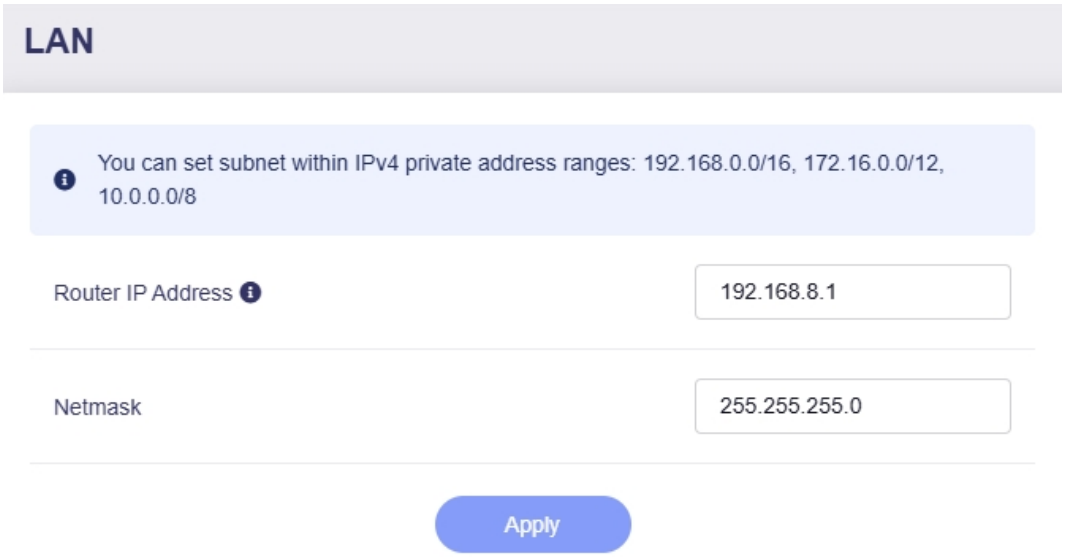
13.3 LAN

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

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

13.3.1 Paramètres de base

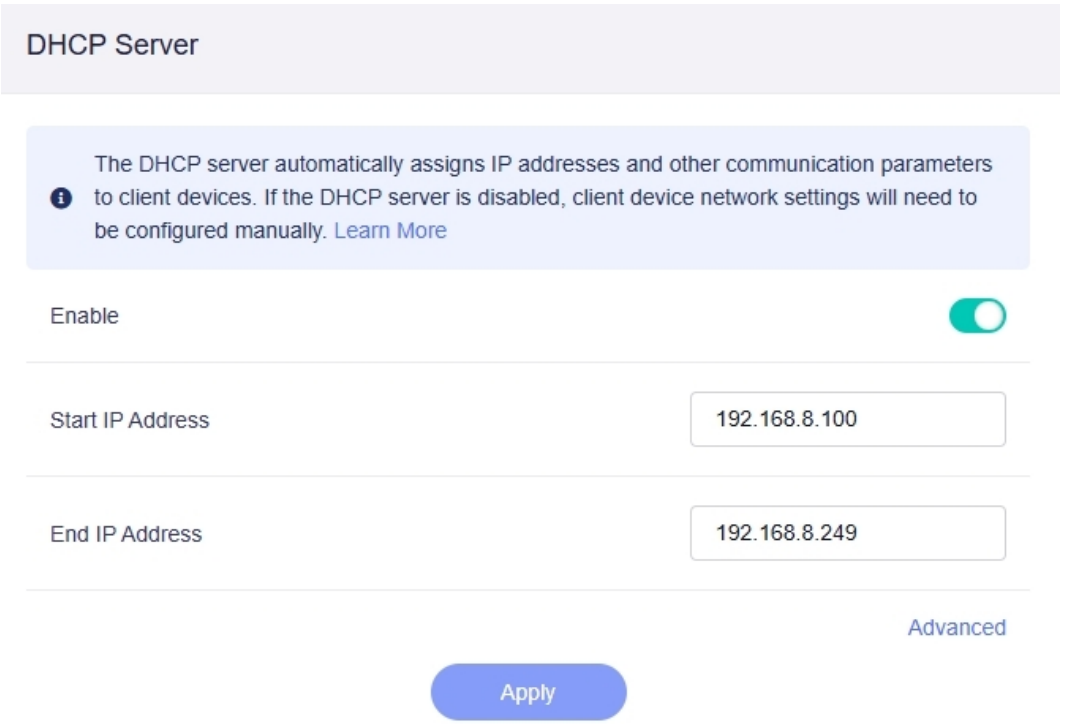
Les paramètres de base comprennent l'adresse IP du routeur et le masque de sous-réseau. Vous pouvez définir un sous-réseau dans les plages IPv4 privées : 192.168.0.0/16, 172.16.0.0/12 ou 10.0.0.0/8.



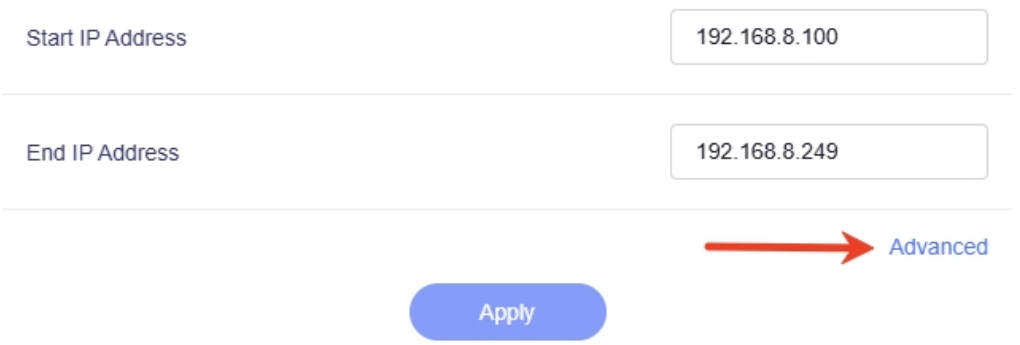
- **Adresse IP du routeur (Router IP Address)** : adresse à saisir dans le navigateur pour ouvrir l'interface d'administration. Par défaut, elle est 192.168.8.1. Modifiez-la si elle entre en conflit avec le réseau en amont.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0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

13.3.2 Serveur DHCP

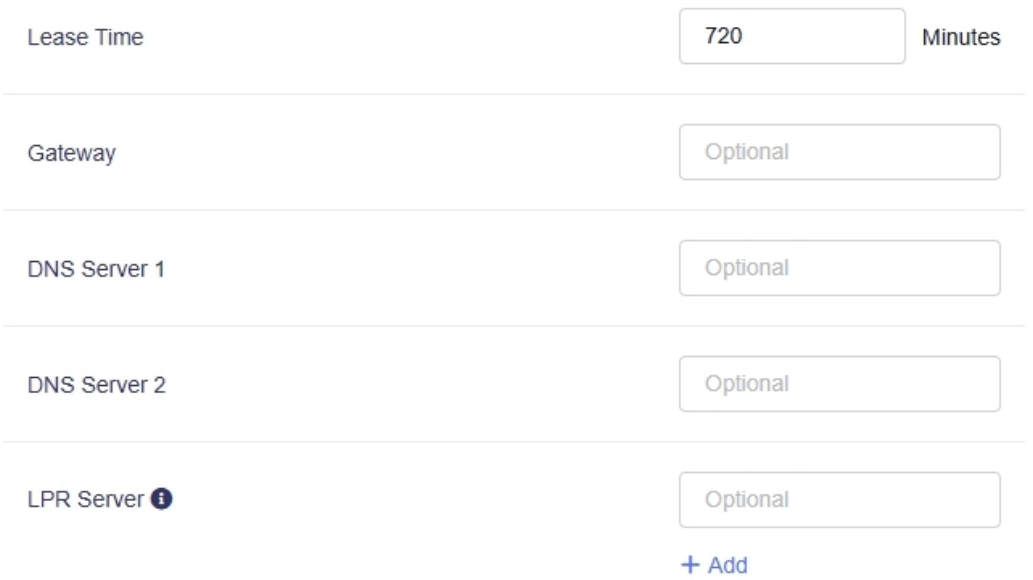
Le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Il est activé par défaut sur le routeur GL.iNet, avec une plage d'adresses de 192.168.8.100 à 192.168.8.249. Vous pouvez personnaliser cette plage.



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



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



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

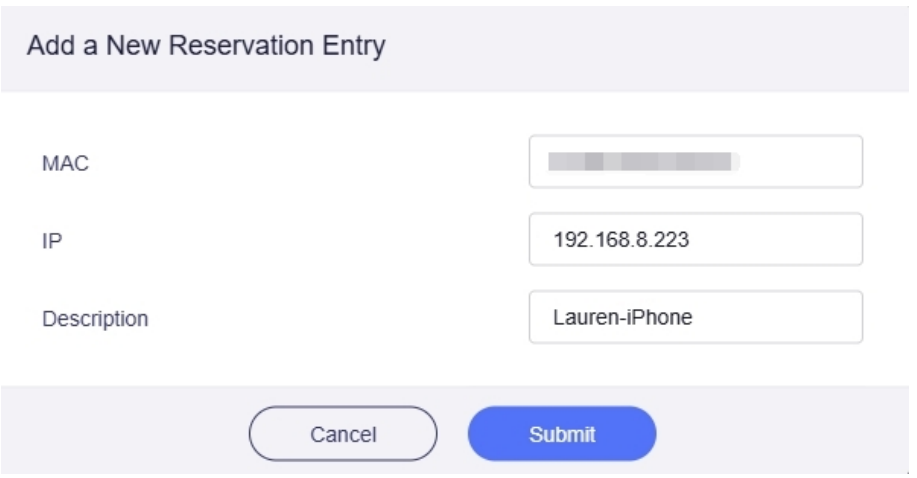
Remarque : si vous désactivez le serveur DHCP, définissez manuellement une IP statique et les autres paramètres de communication sur chaque client. Consultez cette page pour en savoir plus.

13.3.3 Réservation d’adresses

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

Pour configurer une réservation d’adresses, 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.

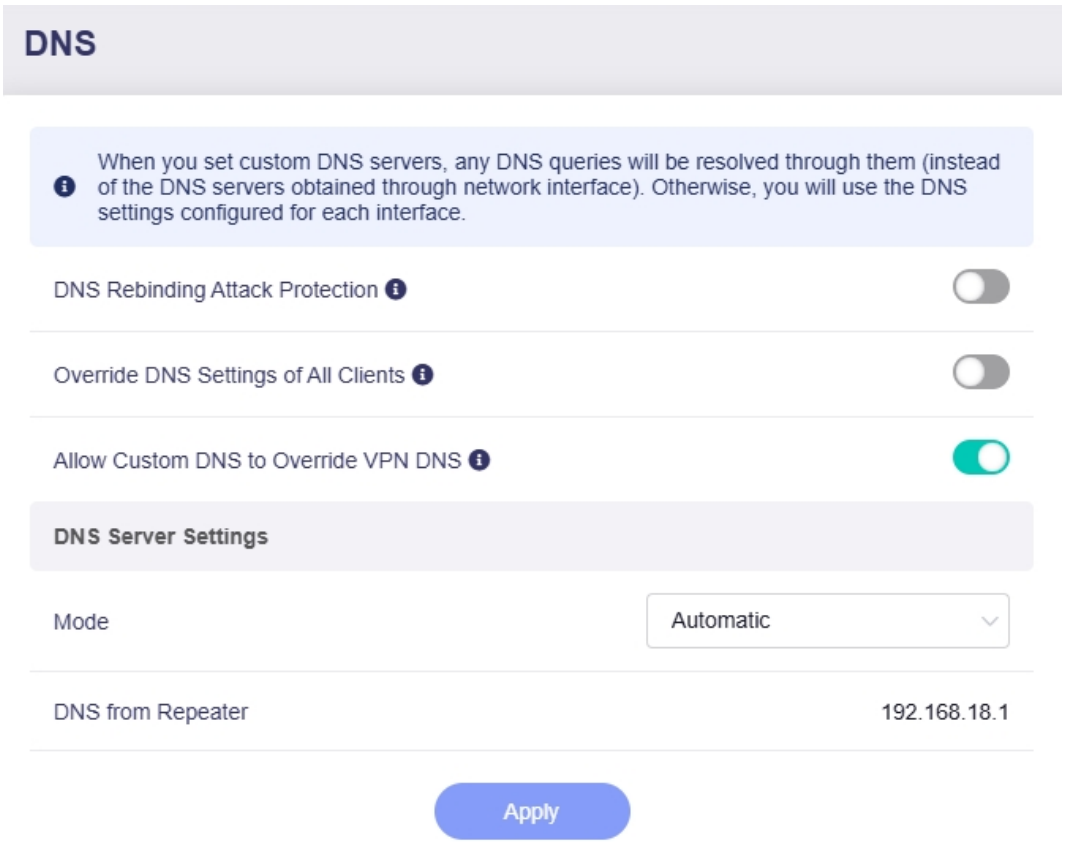


13.4 DNS

Le DNS (Domain Name System, système de noms de domaine) convertit les noms de domaine lisibles, comme www.google.com, en adresses IP utilisables par les appareils, comme 142.250.185.142, pour accéder aux sites et aux services.

Le serveur DNS intégré au routeur résout les noms de domaine pour tous les appareils connectés. Il peut obtenir automatiquement les adresses DNS du réseau en amont ou utiliser des serveurs publics personnalisés, comme 8.8.8.8, définis dans l'interface Web pour optimiser l'accès réseau ou renforcer la sécurité. Tous les appareils connectés utilisent alors ce DNS commun par défaut, sans configuration individuelle.

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **DNS**. Vous pouvez régler les options de sécurité, les modes de serveur et les règles de priorité DNS selon votre environnement réseau.



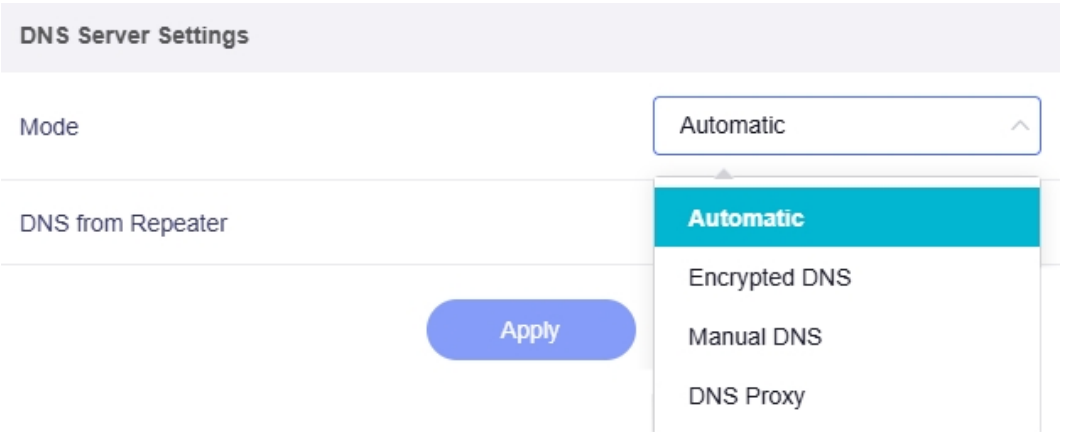
- **Protection contre les attaques par rebinding DNS (DNS Rebinding Attack Protection)** : bloque les tentatives malveillantes de résolution DNS pour protéger contre

les attaques par rebinding DNS. Son activation peut toutefois faire échouer les recherches DNS privées.

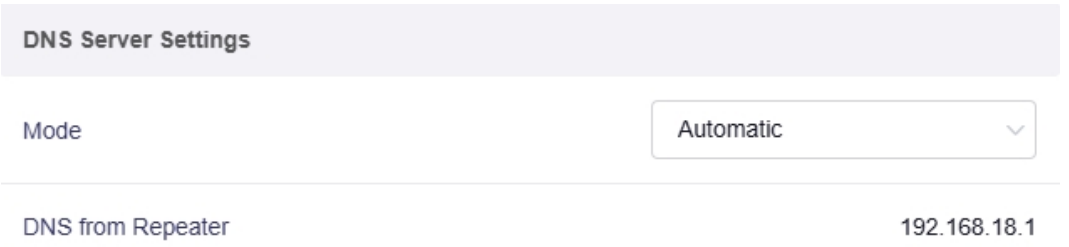
- **Remplacer les paramètres DNS de tous les clients (Override DNS Settings of All Clients)** : impose les serveurs DNS du routeur à tous les appareils connectés, indépendamment de leurs propres réglages, pour une configuration DNS uniforme.
- **Autoriser le DNS personnalisé à remplacer le DNS VPN (Allow 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.

13.4.1 Paramètres du serveur DNS

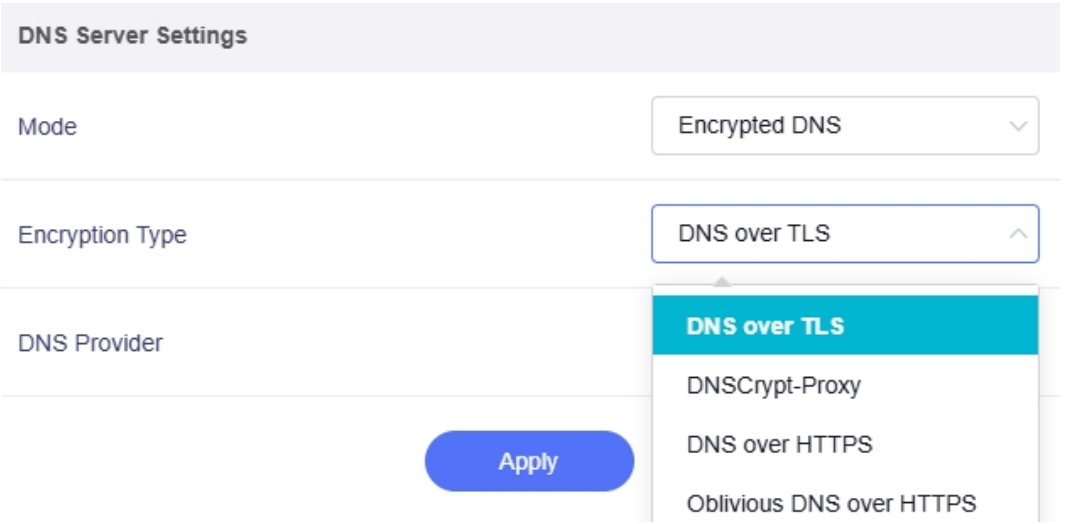
Quatre modes sont proposés : Automatique, DNS chiffré, DNS manuel et Proxy DNS.



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

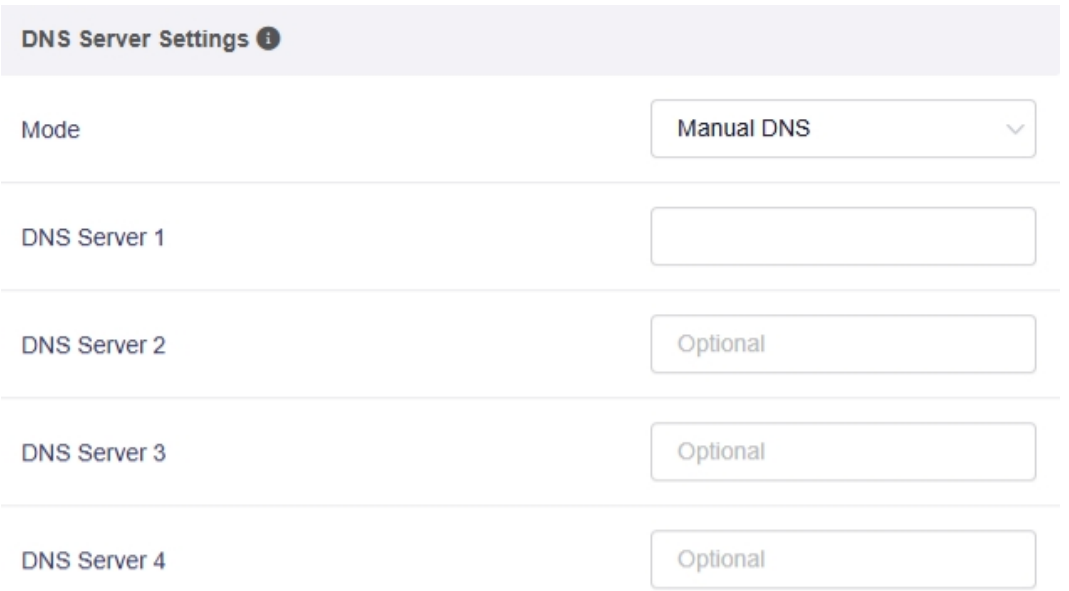


2. **DNS chiffré (Encrypted DNS)** : utilise des protocoles chiffrés pour traiter les requêtes DNS et protéger les données de résolution contre l'écoute et l'altération.
   Quatre types de chiffrement sont proposés : DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS et Oblivious DNS over HTTPS.



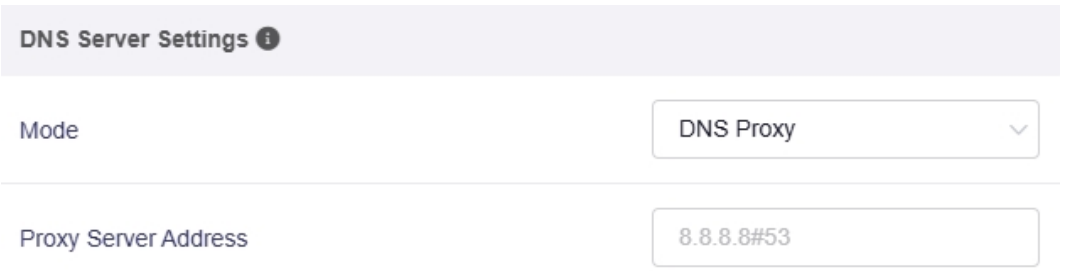
- Pour DNS over TLS, choisissez Control D, NextDNS ou Cloudflare comme fournisseur DNS.
- Pour les trois autres types, sélectionnez au moins un serveur DNS dans la liste, et jusqu'à huit serveurs. Si vous en sélectionnez plusieurs, le routeur utilise automatiquement le plus rapide.

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.

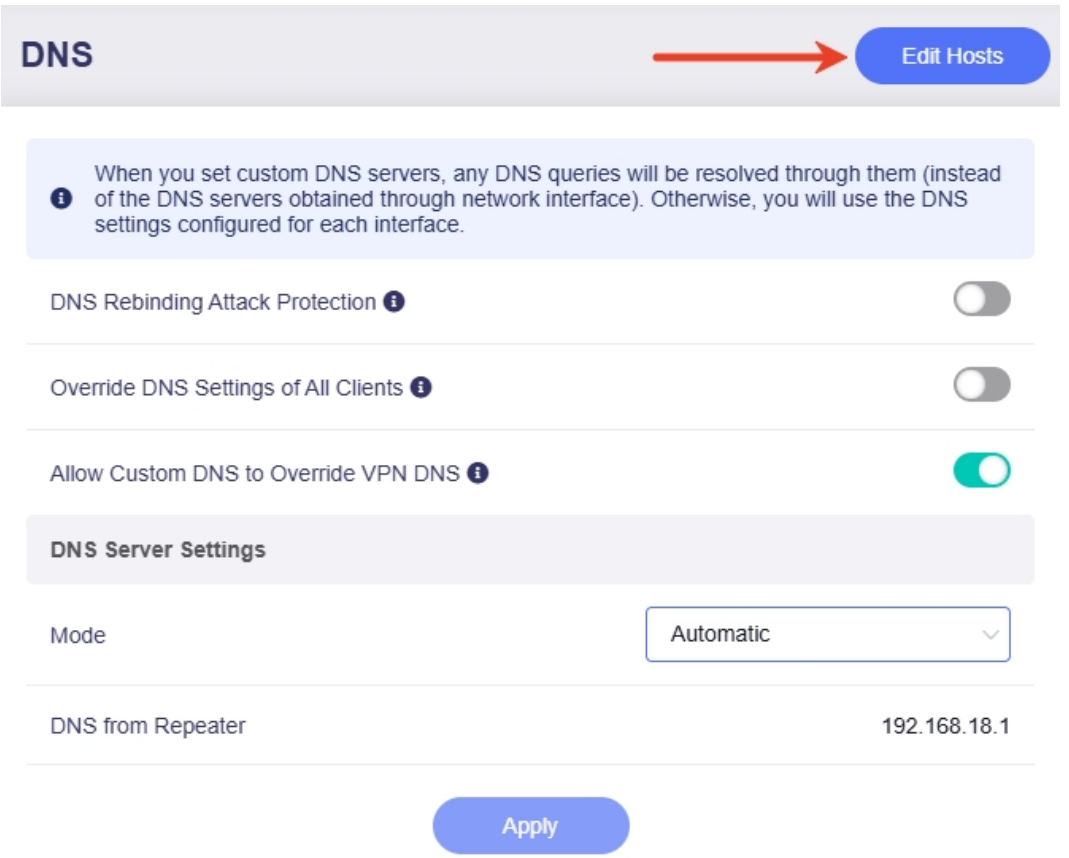
4. **Proxy DNS (DNS Proxy)** : transmet toutes les requêtes DNS par un serveur proxy et utilise son environnement réseau pour la résolution, selon vos besoins d'accès.



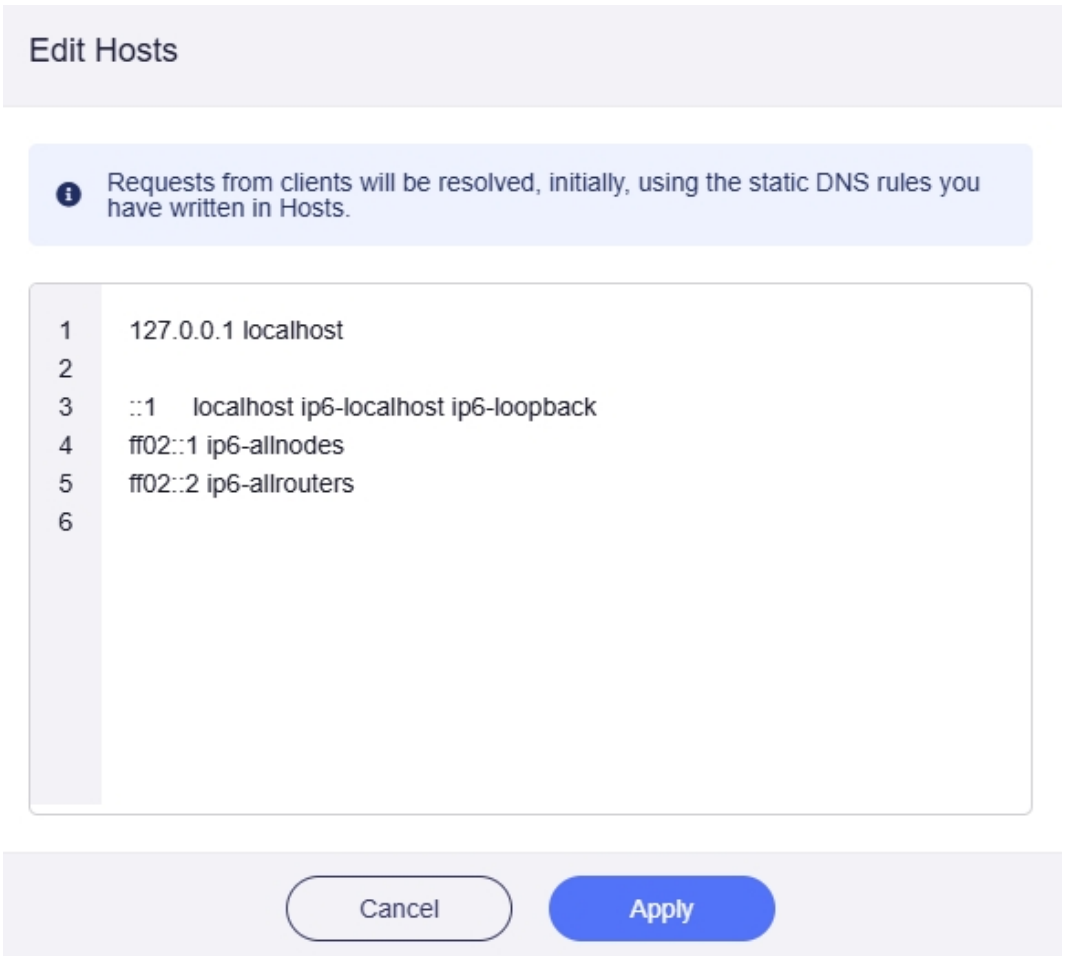
13.4.2 Modification du fichier hosts

Vous pouvez définir des règles statiques de résolution DNS.

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



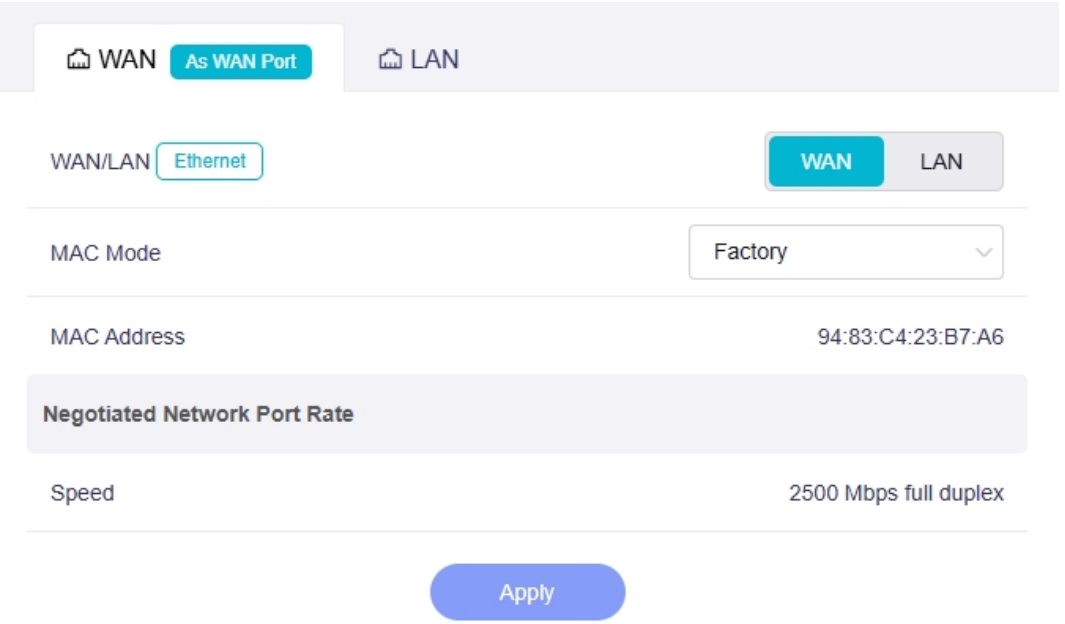
Les requêtes des clients sont résolues en priorité avec les règles statiques saisies ici. Vous pouvez associer manuellement des adresses IP à des noms d'hôtes, comme l'entrée de bouclage locale 127.0.0.1 localhost, pour personnaliser la résolution des noms.


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

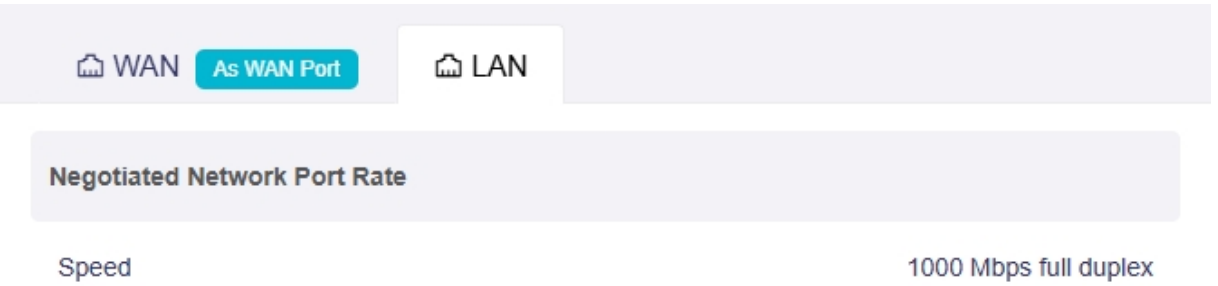
13.5 Gestion des ports

Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Gestion des ports (Port Management)** 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.

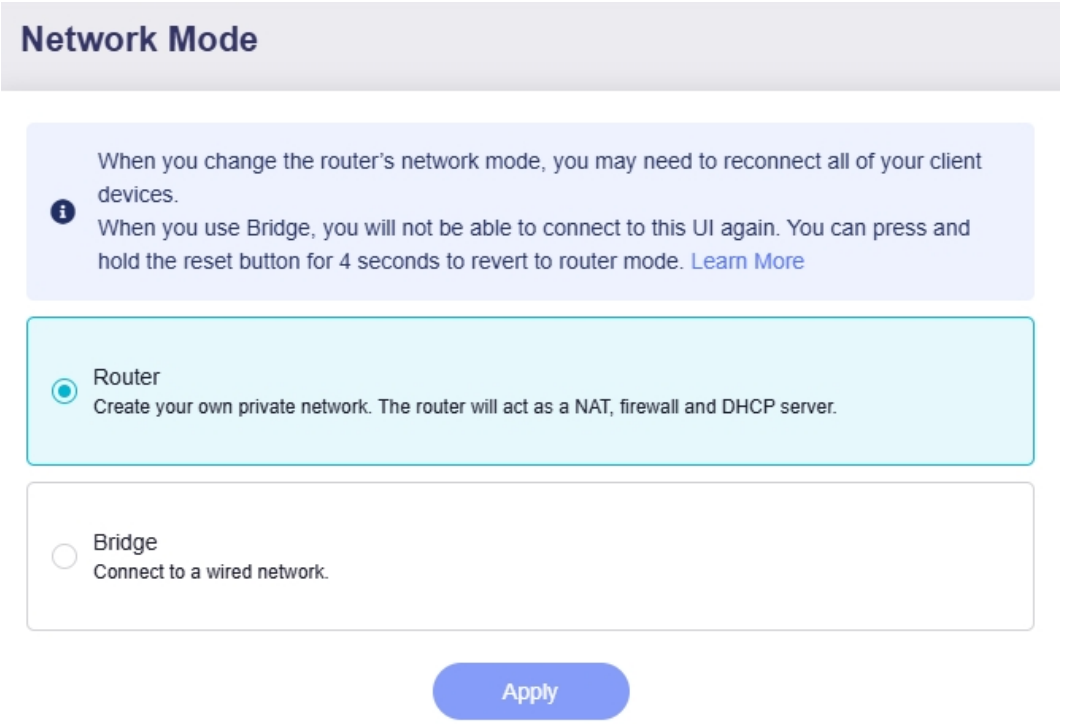


Remarque : le débit négocié des ports WAN et LAN ne s'affiche que lorsqu'un câble Ethernet est branché. Il dépend des capacités du port et du câble Ethernet.

13.6 Mode réseau

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

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Mode réseau (Network Mode)** pour changer de mode. Brume 2 propose deux modes : Routeur et Pont.



- **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.
- **Pont (Bridge)** : permet au routeur de se connecter à un réseau filaire et de servir de pont entre les appareils réseau. Dans ce mode, il fonctionne comme un commutateur : il transfère les données entre les appareils connectés sans assurer les fonctions NAT, pare-feu ou DHCP. Les appareils du même réseau peuvent ainsi communiquer directement ; le routeur sert de point de connexion.

Remarque :

1. Après un changement de mode réseau, reconnectez les appareils au routeur pour assurer une connexion stable.
2. **En mode Pont, l’interface d’administration Web n’est plus accessible via l’adresse IP d’origine**. Connectez-vous au routeur amont pour trouver l’adresse IP qu’il a attribuée à ce routeur, puis utilisez cette adresse pour ouvrir l’interface d’administration Web. Si vous ne pouvez pas accéder au routeur amont, maintenez le bouton de réinitialisation enfoncé pendant 4 secondes pour rétablir le mode Routeur par défaut.
3. **En mode Pont, les fonctions suivantes ne sont pas disponibles** : contrôle d’accès (liste d’autorisation et liste de blocage), AstroWarp, VPN, Tor, AdGuard Home, contrôle parental, ZeroTier, Tailscale, redirection de ports, Multi-WAN, serveur DHCP, réservation d’adresses, DNS, gestion des ports, IPv6, passerelle Drop-in, IGMP Snooping, accélération réseau et paramètres NAT.

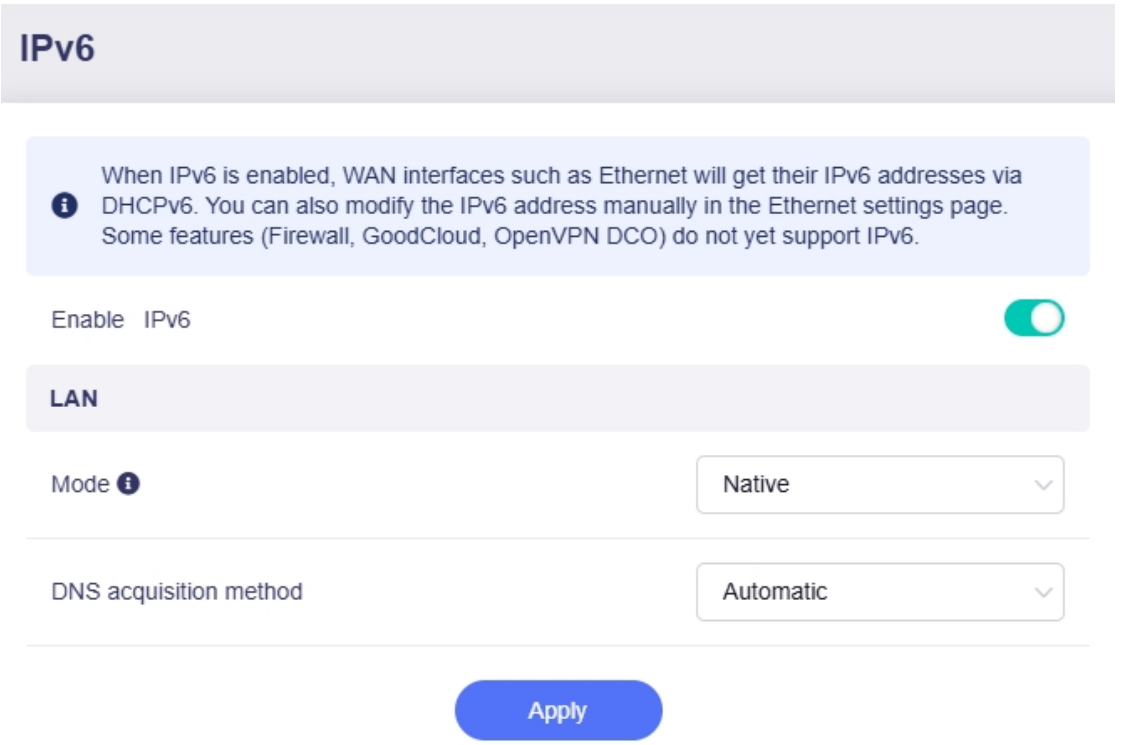
13.7 IPv6

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.

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.

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



13.7.1 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.

13.7.2 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.

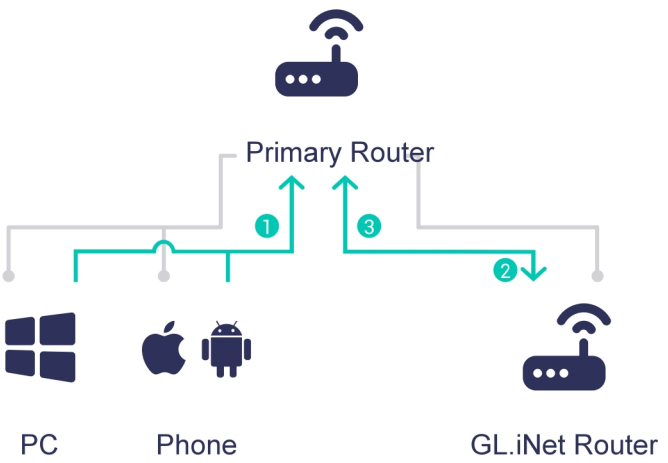
- **Automatique (Automatic)** : le routeur obtient les adresses DNS IPv6 dynamiquement, par exemple via DHCPv6.
- **Manuelle (Manual)** : saisissez les adresses des serveurs DNS IPv6 souhaités. Une configuration manuelle incorrecte peut empêcher la résolution des noms de domaine en adresses IP. Utilisez-la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

13.8 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 :

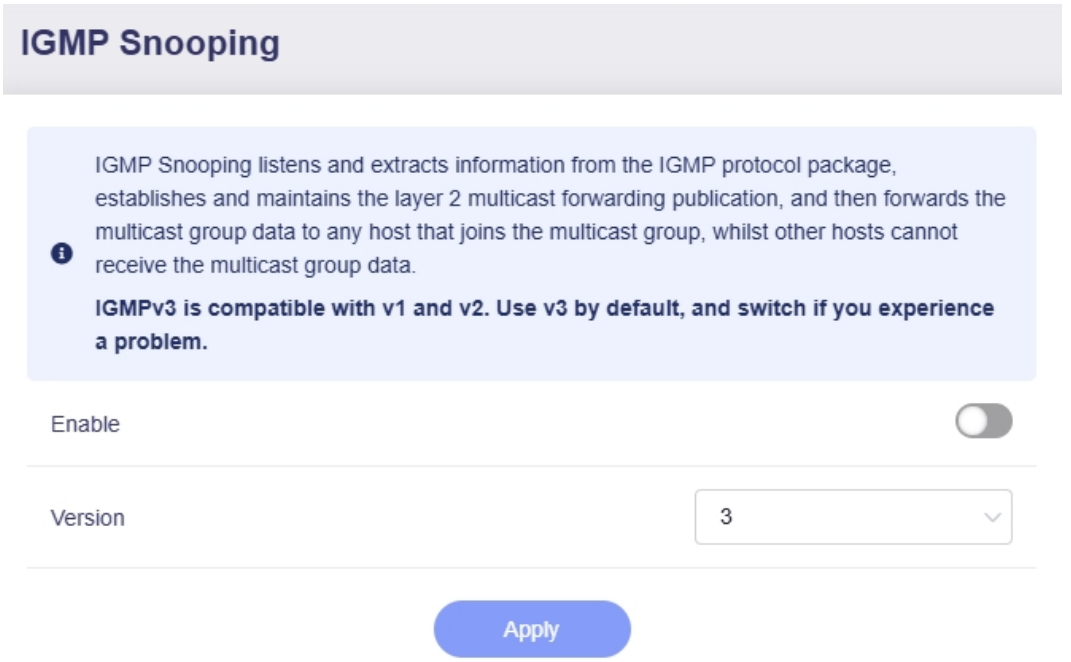
1. Le trafic des appareils clients est d’abord transmis au routeur principal.
2. Le routeur principal l’envoie au routeur GL.iNet pour traitement, par exemple le filtrage publicitaire ou le chiffrement VPN.
3. Après traitement, le trafic retourne au routeur principal, qui remet les données aux clients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

Vous pouvez activer la passerelle Drop-in pour tous les appareils connectés à votre routeur principal ou pour certains d’entre eux. Consultez ce lien pour obtenir les instructions détaillées.

13.9 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.

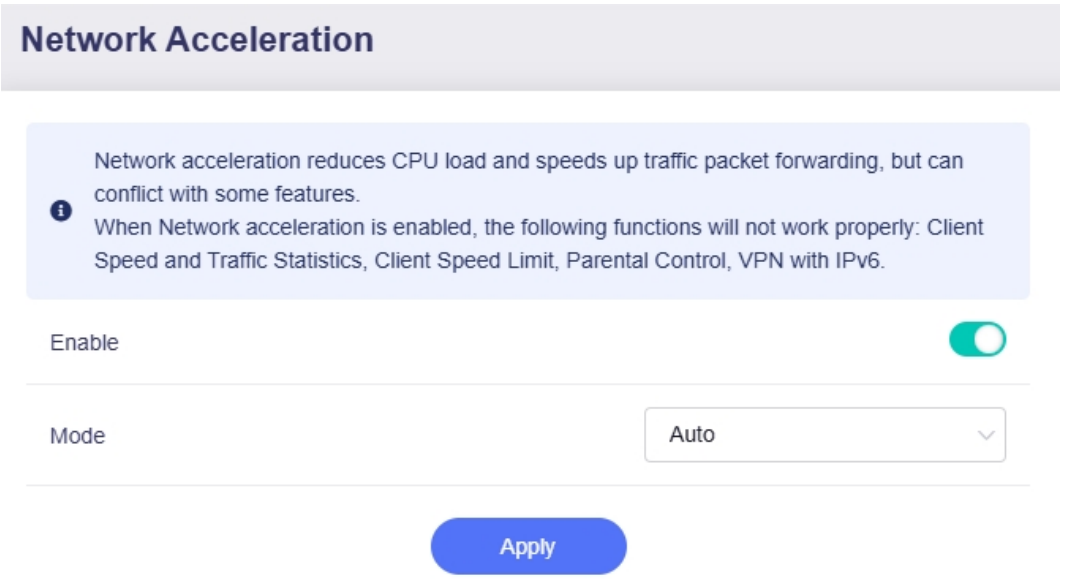
Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **IGMP Snooping**. Activez cette fonction si vous souhaitez utiliser le multicast sur le routeur.



13.10 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.



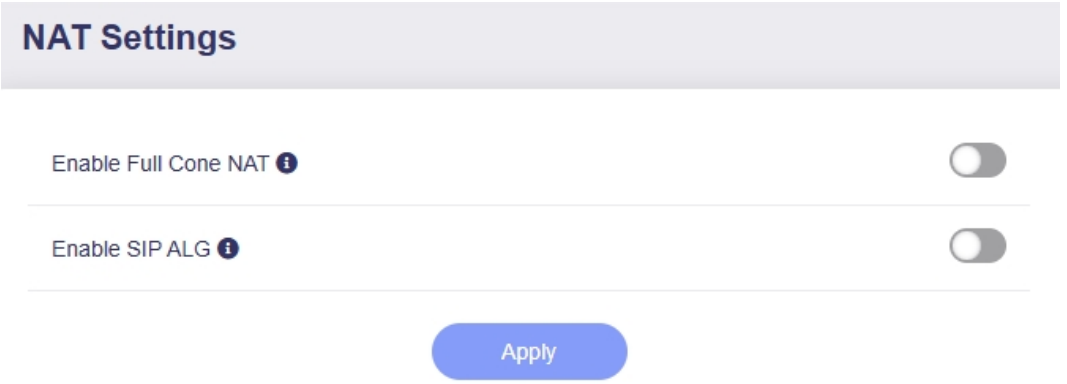
- **Automatique (Auto)** : bascule automatiquement entre les deux modes d’accélération selon l’utilisation réelle.
- **Accélération matérielle (Hardware Acceleration)** : confie les tâches réseau fréquentes, comme le NAT, le transfert de paquets et la vérification des sommes de contrôle, à du matériel dédié tel qu’une NPU ou une puce HWNAT. Elle fonctionne avec les connexions Ethernet (WAN/LAN filaires) et Répéteur (indisponible sur Brume 2). Elle est particulièrement efficace lorsque les chemins sont fixes et les règles simples : elle assure un débit élevé, une faible latence et une charge minimale du processeur pour transmettre les données au débit nominal du réseau.
- **Accélération logicielle (Software Acceleration)** : utilise le processeur général du routeur avec des noyaux ou pilotes optimisés, par exemple SWNAT. Elle fonctionne avec les connexions cellulaires 4G/5G, qui constituent généralement le principal cas où l’accélération matérielle est indisponible. Elle offre une bonne compatibilité et prend en

charge les protocoles complexes. Malgré sa souplesse, elle peut être limitée par le processeur lorsque la bande passante sollicitée est élevée, surtout avec des fonctions avancées comme la QoS ou la redirection de ports.

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

13.11 Paramètres NAT

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



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

Chapitre 14

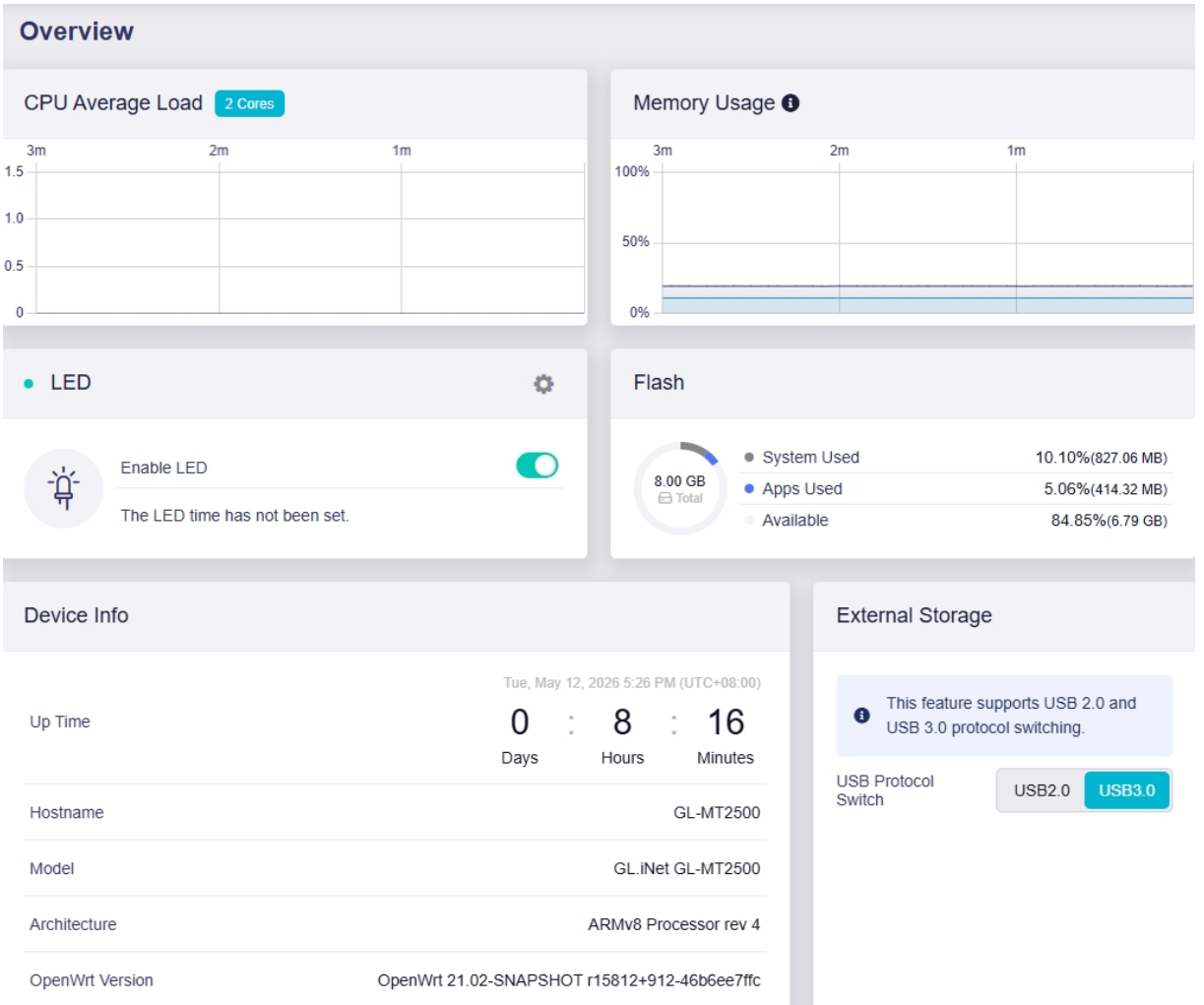
Système

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

14.1 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

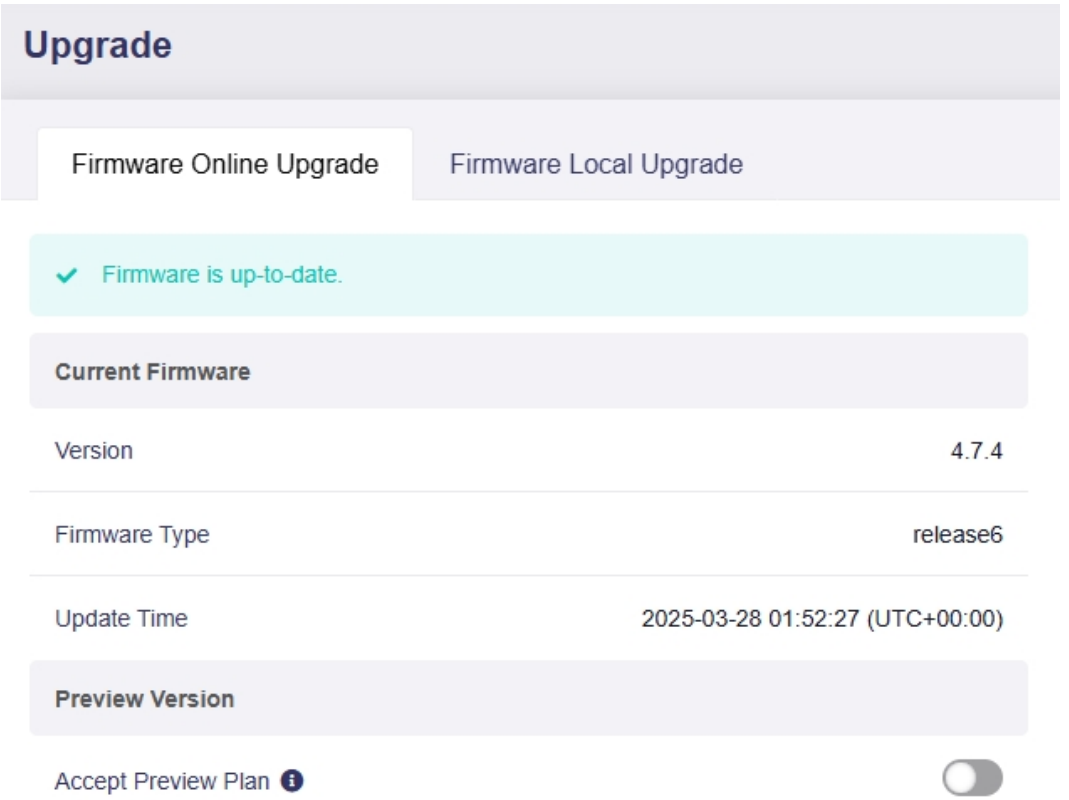


14.2 Mise à jour

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

14.2.1 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.



- **Participer au programme de préversion (Accept Preview Plan)** : activez cette option pour essayer de nouvelles fonctions avant leur version finale et nous transmettre vos commentaires. Une fois activée, elle le reste. Ces mises à jour peuvent être instables.

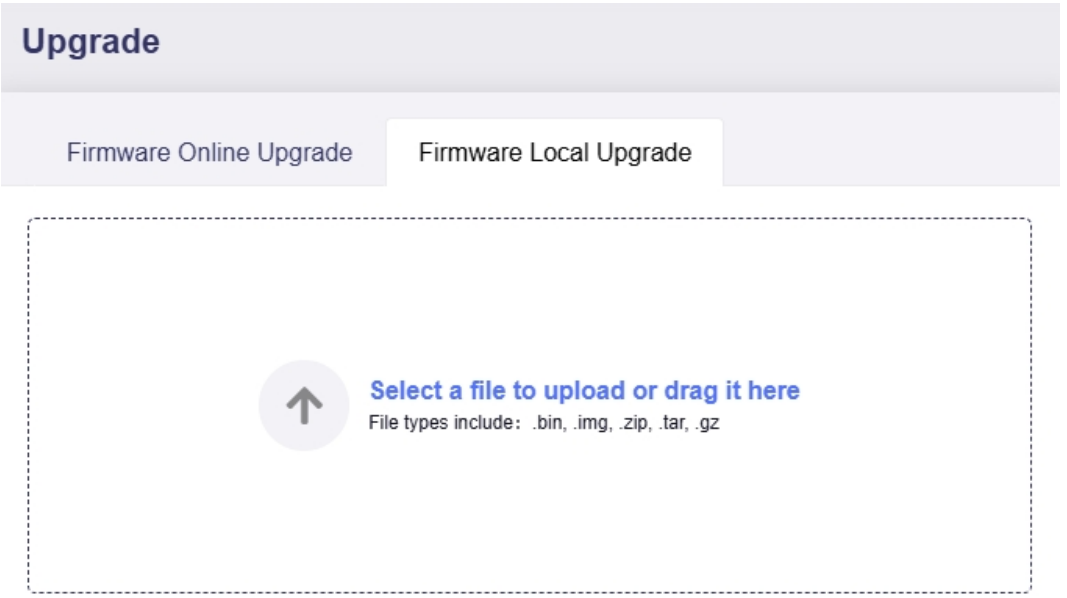
Si le routeur est connecté à Internet, il recherche une version plus récente du micrologiciel à télécharger.

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

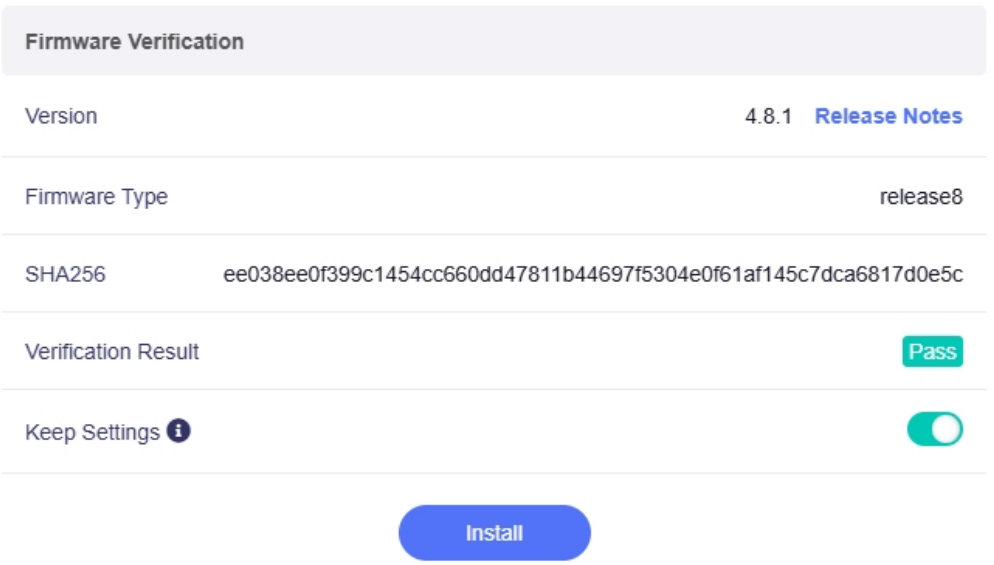
14.2.2 Mise à jour locale

Cette méthode 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.

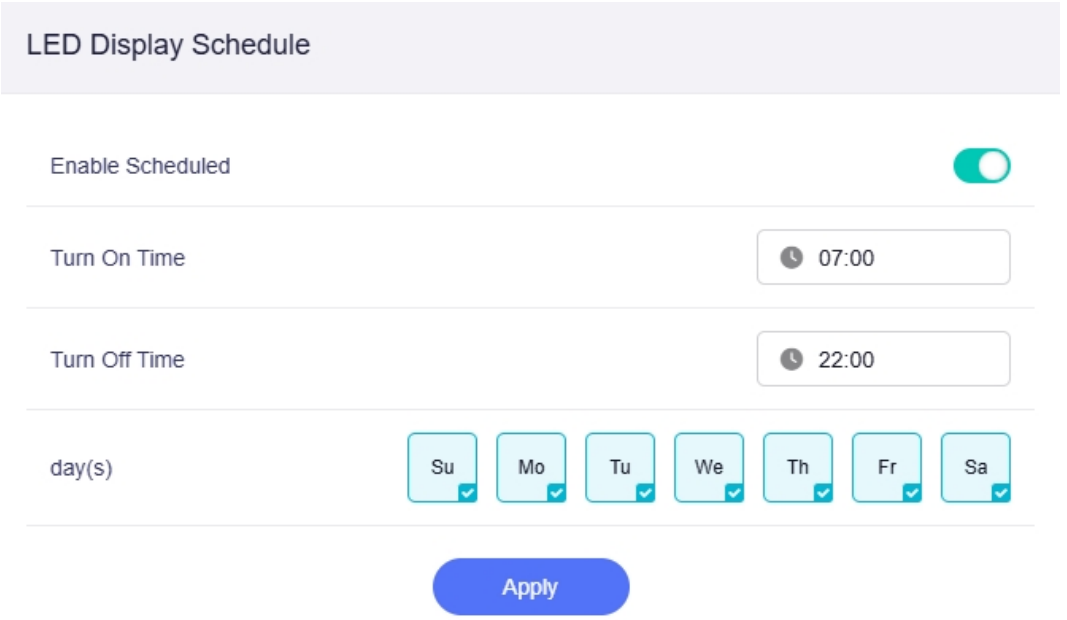
14.3 Tâches planifiées

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

Remarque : synchronisez d'abord 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.

14.3.1 Programmation du voyant LED

Cette fonction permet de programmer l'allumage et l'extinction du voyant du routeur.

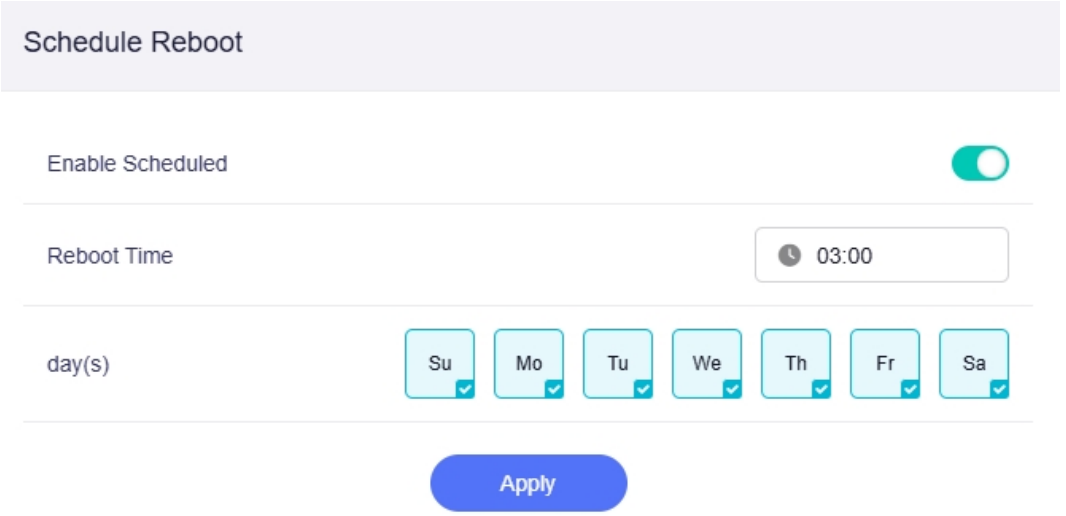


- **Activer la programmation (Enable Scheduled)** : active le planning du voyant.
- **Heure d'allumage (Turn On Time)** : heure d'allumage du voyant, par exemple 07:00.
- **Heure d'extinction (Turn Off Time)** : heure d'extinction du voyant, par exemple 22:00.
- **Jour(s) (day(s))** : jours de la semaine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

Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

14.3.2 Redémarrage planifié

Cette fonction permet de programmer le redémarrage automatique du routeur.

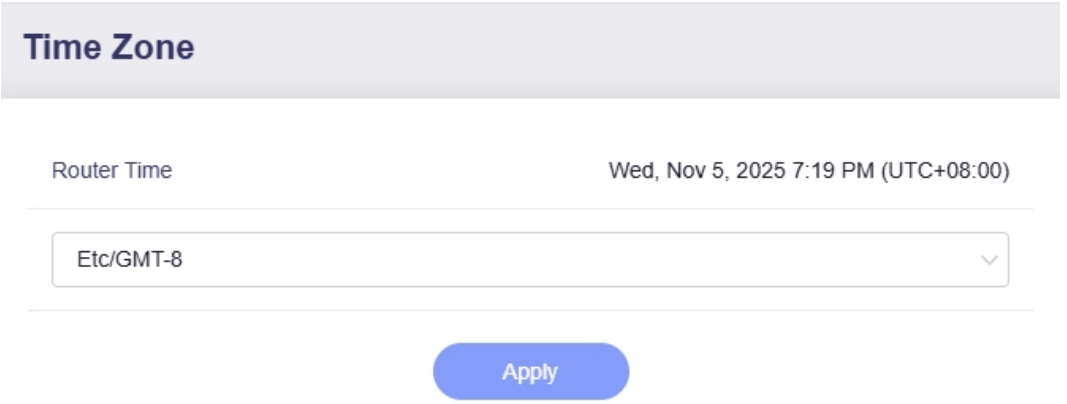


- **Activer la programmation (Enable Scheduled)** : active le redémarrage planifié.
- **Heure de redémarrage (Reboot Time)** : heure à laquelle le routeur redémarre, par exemple 03:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

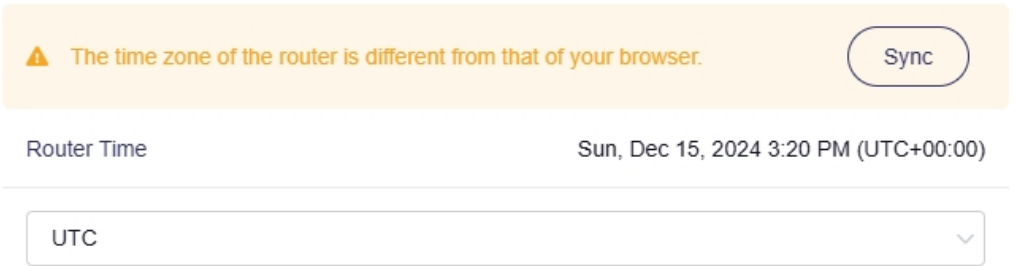
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

14.4 Fuseau horaire

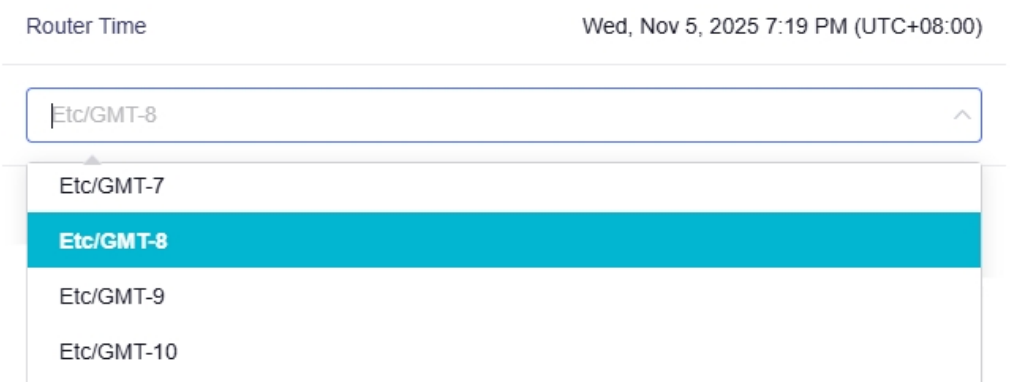
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)**. La page affiche la date et l'heure système du routeur ainsi que le décalage du fuseau horaire.



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

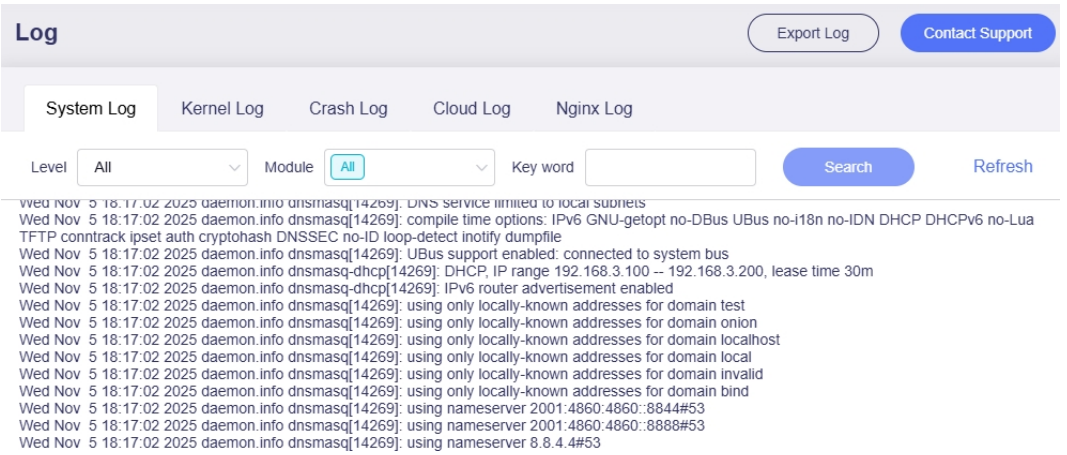


Pour changer de fuseau, sélectionnez celui qui convient dans la liste afin que l'heure du routeur corresponde à l'heure locale.

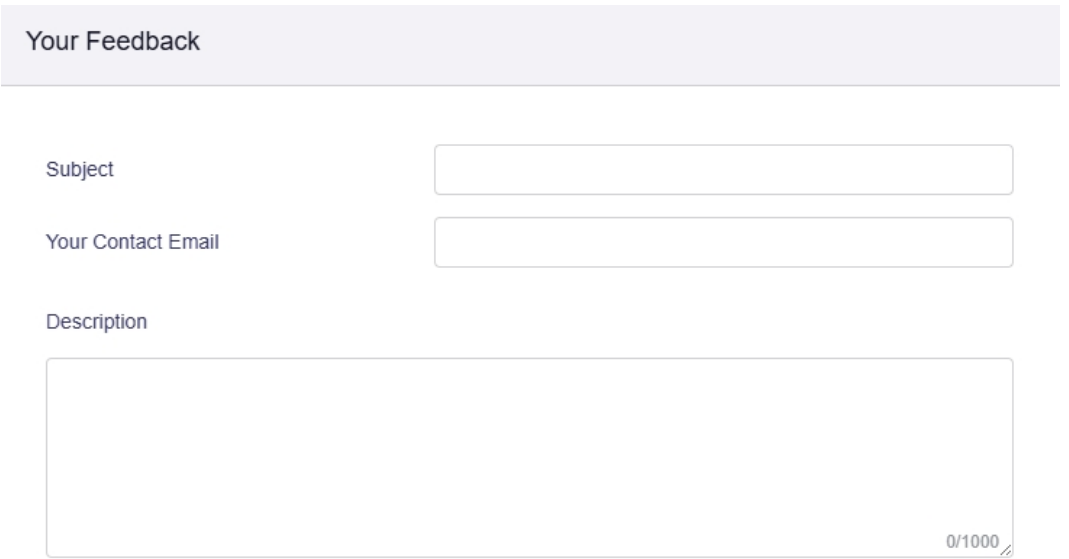


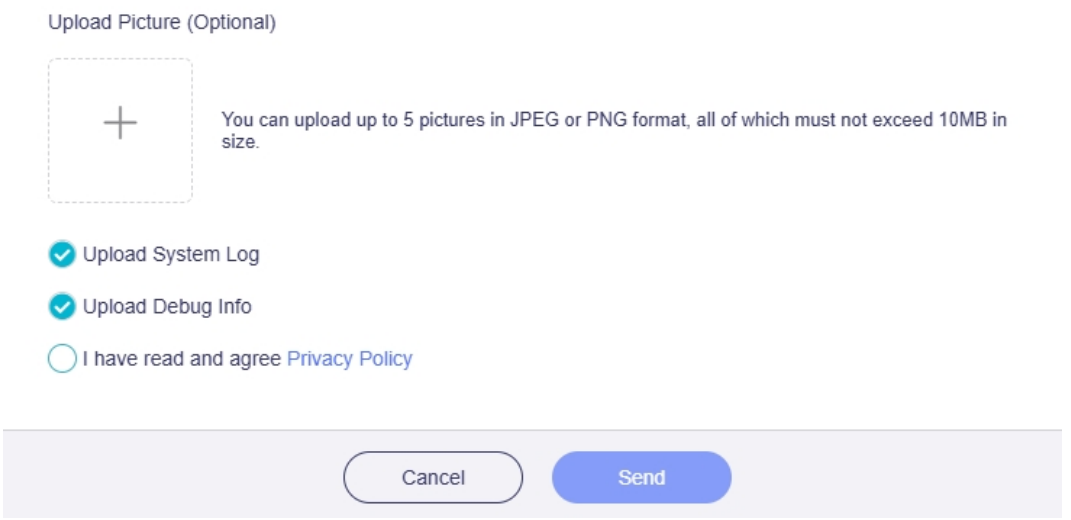
14.5 Journaux

Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Journal (Log)**. Vous pouvez consulter les journaux Système, Noyau, Plantage, Cloud et Nginx pour l'analyse et le dépannage. Certains modèles cellulaires compatibles avec l'eSIM proposent également un journal eSIM.



- **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

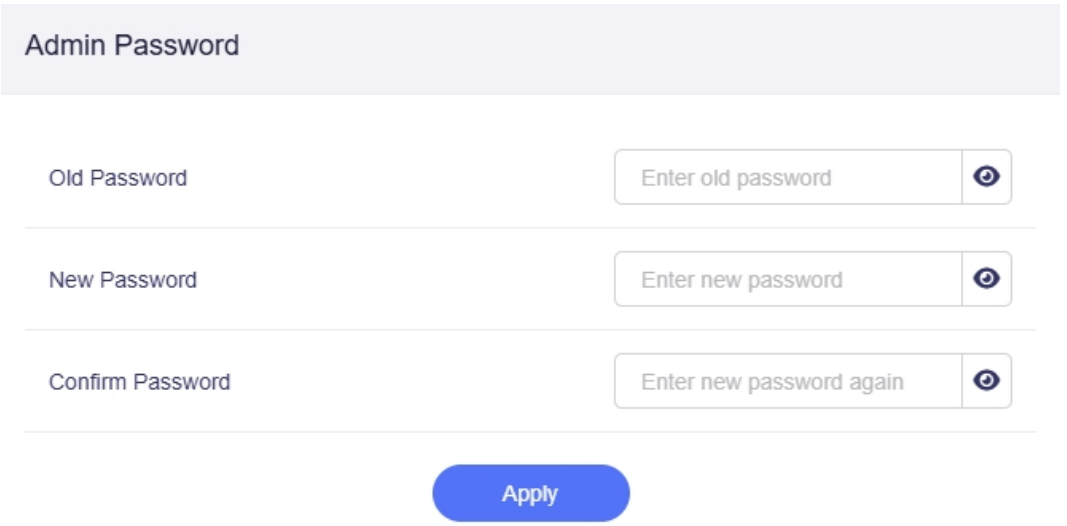
14.6 Sécurité

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

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

14.6.1 Mot de passe administrateur

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

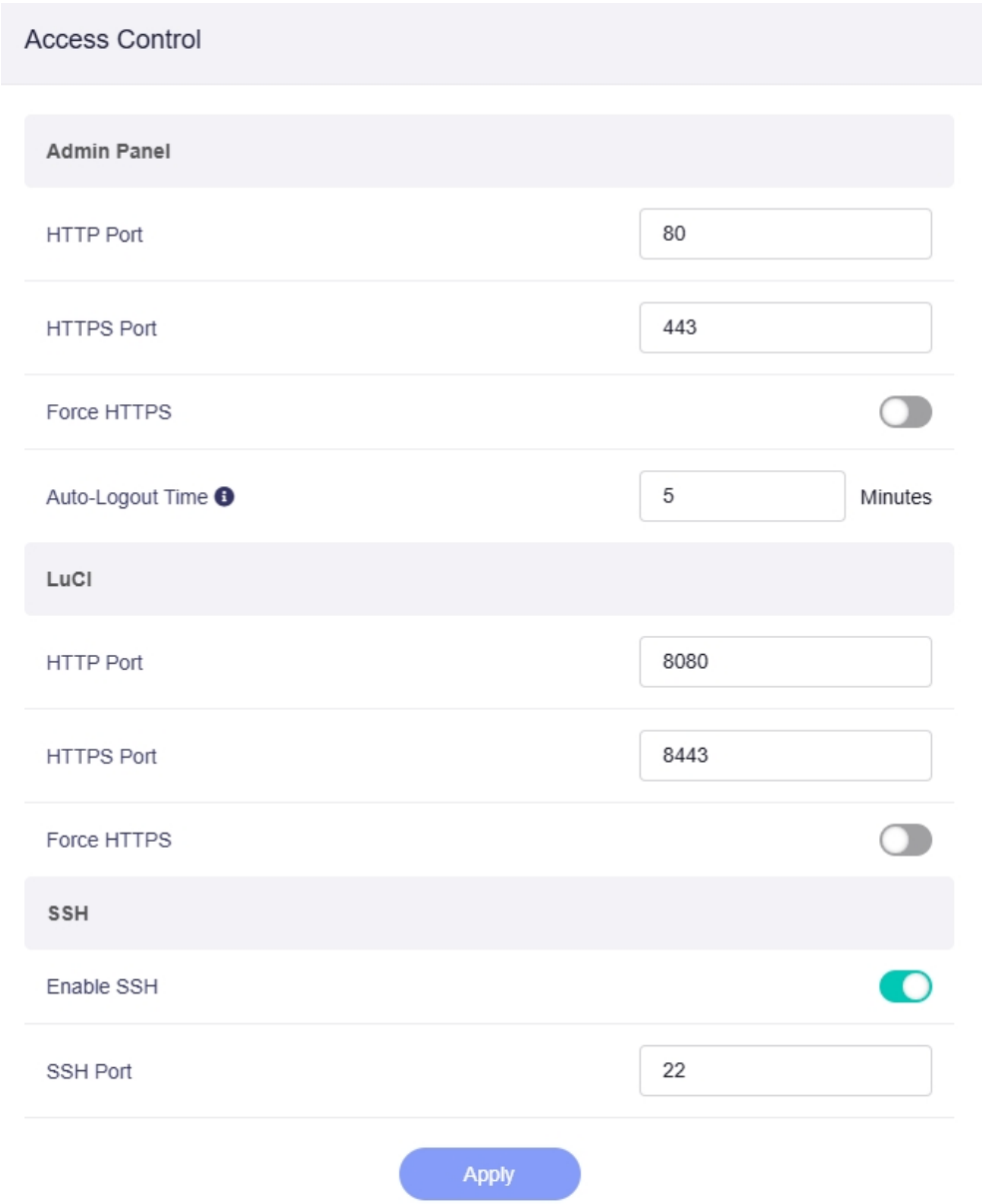


Le mot de passe administrateur doit respecter les règles suivantes :

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

14.6.2 Contrôle d’accès

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



Interface d’administration

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

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

LuCI

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

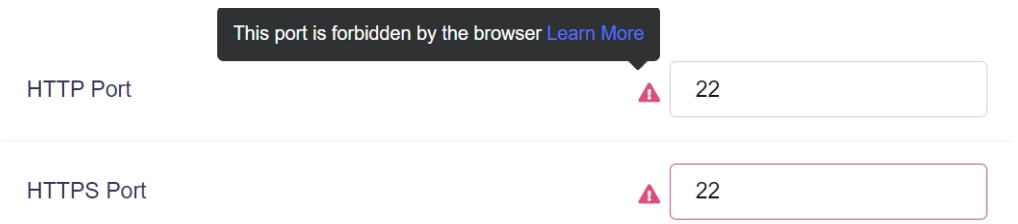
- **Port HTTP (HTTP Port)** : 8080 par défaut, pour l'accès HTTP non chiffré à LuCI.
- **Port HTTPS (HTTPS Port)** : 8443 par défaut, pour l'accès HTTPS sécurisé à LuCI.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à LuCI.

SSH

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

Remarque :

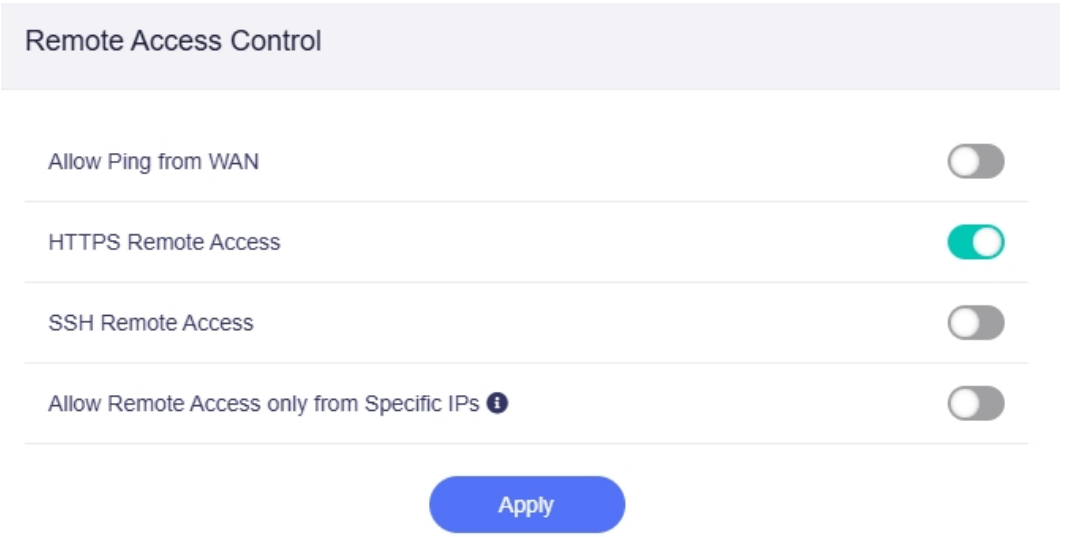
1. Si le port choisi entre en conflit avec un port réservé, notamment par les navigateurs ou les conventions réseau, le message « Ce port est interdit par le navigateur » (This port is forbidden by the browser) s'affiche.



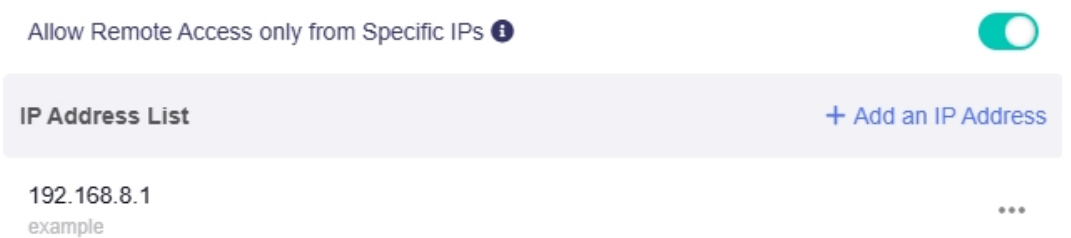
2. Si vous modifiez un port dans le micrologiciel, renseignez le nouveau numéro pour accéder à l'interface d'administration. Si vous l'avez oublié, réinitialisez le routeur pour rétablir le port par défaut.
3. Les paramètres d'accès LuCI ne sont disponibles qu'après son installation. S'ils n'apparaissent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

14.6.3 Contrôle d’accès distant

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

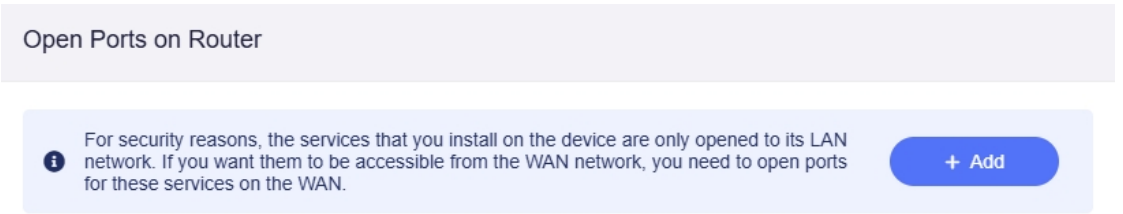


- **Autoriser le ping depuis le WAN (Allow Ping from WAN)** : permet de vérifier que le routeur est joignable depuis le WAN en cas de problème et de mesurer la latence et les pertes de paquets.
- **Accès HTTPS à distance (HTTPS Remote Access)** : permet d’accéder de manière sécurisée à l’interface Web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

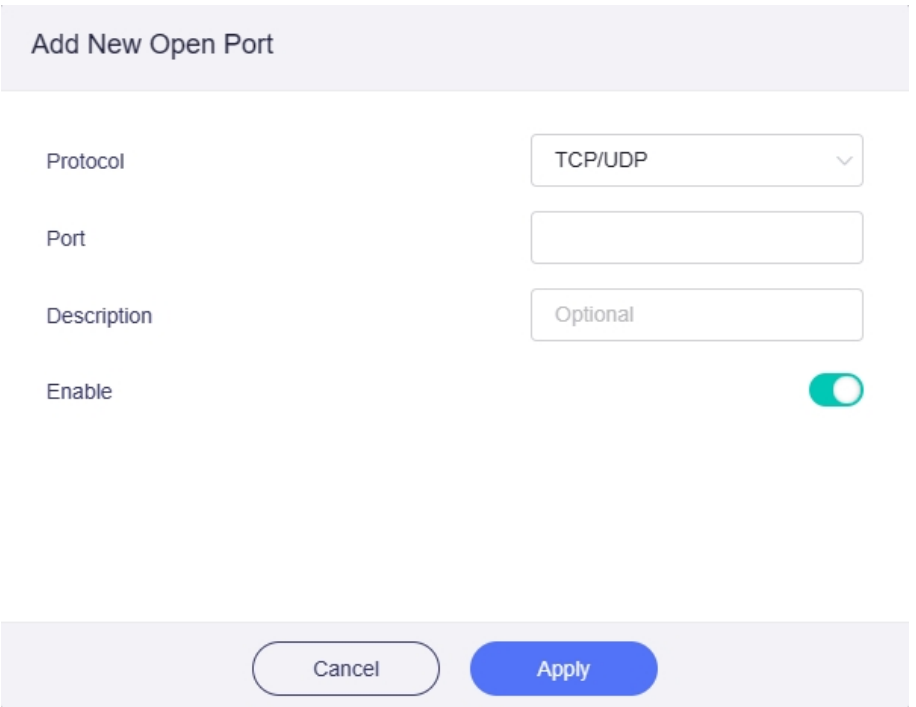


14.6.4 Ouverture de ports sur le routeur

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



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

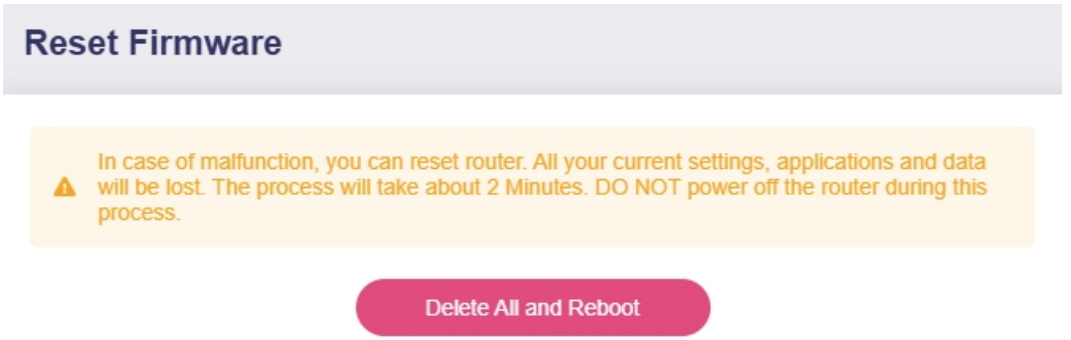


- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP/UDP. Ce choix détermine la transmission des données du service associé au port.
- **Port** : saisissez le numéro du port à ouvrir.
- **Description** (facultative) : ajoutez une brève description, comme « Serveur Web » ou « Service FTP », pour faciliter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

14.7 Réinitialisation du micrologiciel

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Réinitialiser le micrologiciel (Reset Firmware)**. En cas de dysfonctionnement du routeur, vous pouvez essayer de résoudre le problème en réinitialisant le micrologiciel.

Cliquez sur **Tout supprimer et redémarrer (Delete All and Reboot)** pour réinitialiser le micrologiciel si nécessaire.



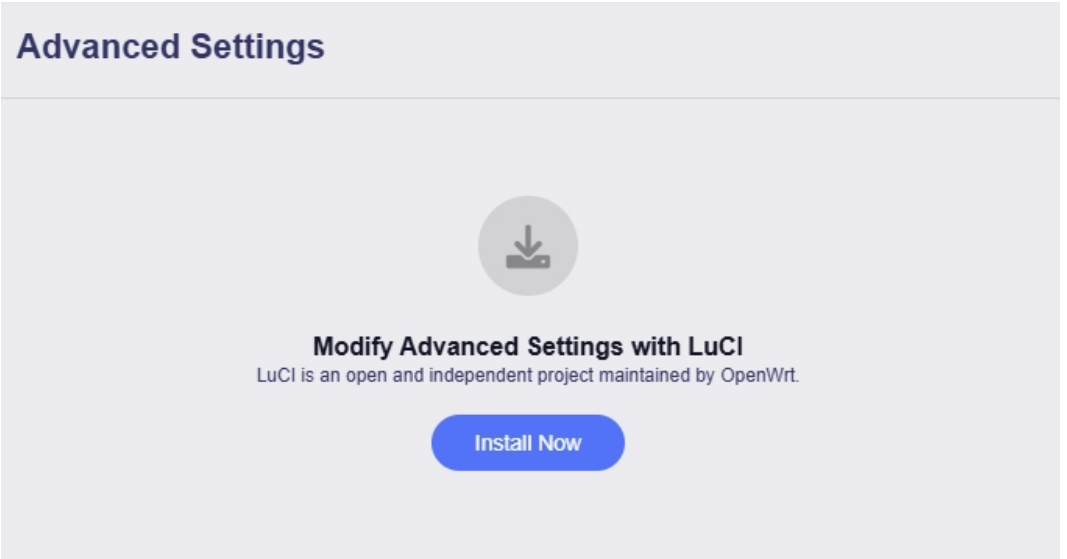
Remarque : tous vos paramètres, applications et données seront effacés. L'opération prend environ 2 minutes. N'éteignez pas le routeur pendant cette opération.

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

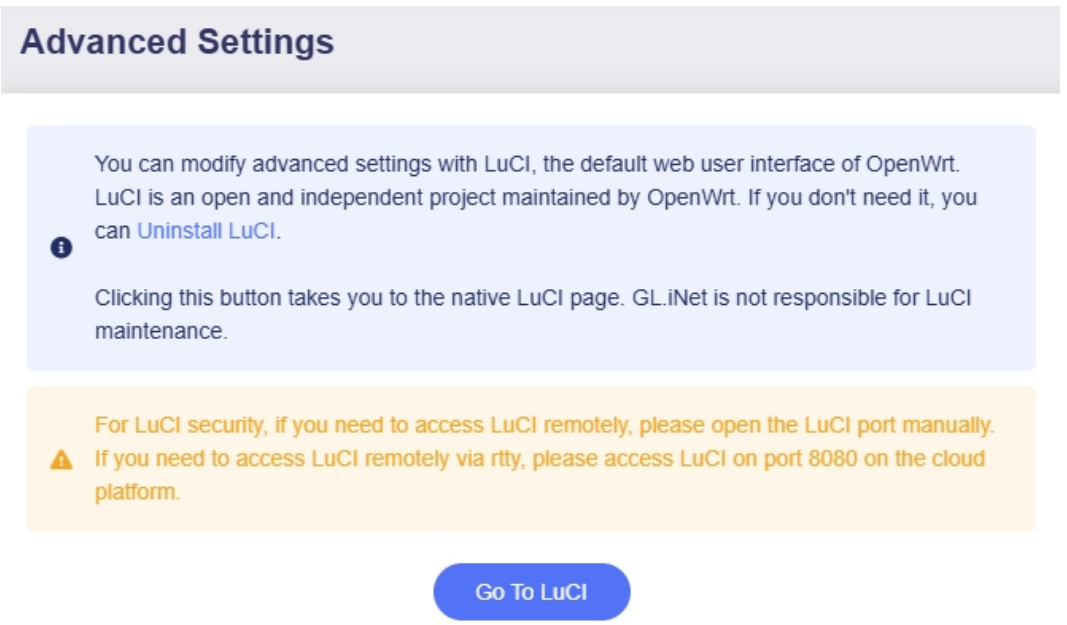
14.8 Paramètres avancés

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

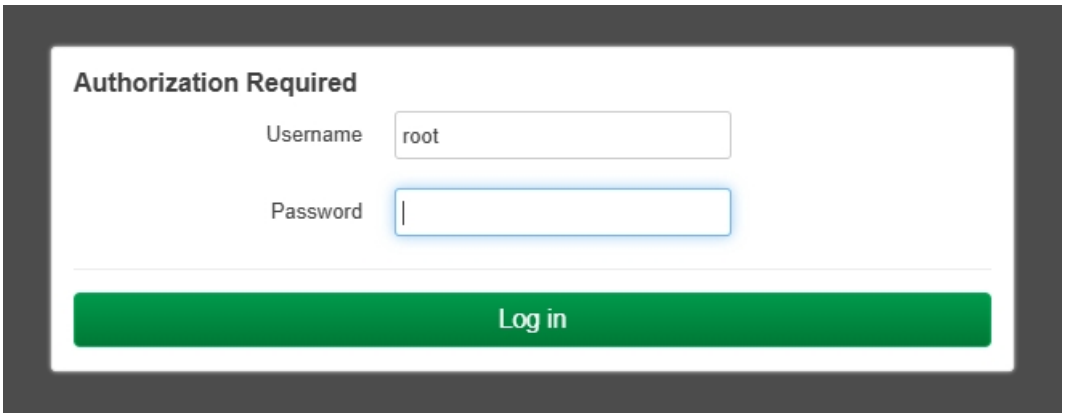
Cliquez sur **Installer maintenant (Install Now)** pour installer l'interface LuCI.



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



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



L’interface LuCI s’ouvre.

