GL·iNet



Manuel d’utilisation

GL-A1300 / Slate Plus

Routeur de voyage Wi-Fi 5

Version du micrologiciel 4.5.22

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 9

1.1 Présentation du produit 10

1.1.1 Aspect extérieur 10

1.1.2 Ports et boutons 11

1.1.3 LED 12

1.2 Caractéristiques techniques 12

1.3 Contenu de l'emballage 13

Chapitre 2 Branchements 15

2.1 Choix de l'emplacement 16

2.2 Branchement du routeur 16

Chapitre 3 Connexion à l'interface du routeur 17

Chapitre 4 Configuration de la connexion Internet 19

4.1 Connexion à Internet via un câble Ethernet 21

4.1.1 Configuration de base 21

4.1.2 Protocole 23

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

4.2.1 Configuration de base 27

4.2.2 Options du répéteur 30

4.3 Connexion à Internet par partage de connexion USB 32

4.3.1 Partage de connexion avec un iPhone 32

4.3.2 Partage de connexion avec un appareil Android 34

4.3.3 Dépannage 35

4.4 Connexion à Internet via un modem USB 36

Chapitre 5 Réseau sans fil 38

5.1 Wi-Fi 5 GHz 39

5.2 Wi-Fi 2,4 GHz 41

Chapitre 6 Appareils clients 43

6.1 Informations sur les appareils 45

6.2 Actions 47

6.3 Suppression de clients 49

6.4 Tri 50

Chapitre 7 Présentation du VPN 51

7.1 Introduction 52
7.2 Cas d'utilisation 53
Chapitre 8 Tableau de bord VPN 55
8.1 Client VPN 56
8.1.1 Options du client 57
8.1.2 Mode par règles 59
8.1.3 Options globales 61
8.2 Serveur VPN 64
8.2.1 Options du serveur 65
8.2.2 Règles de routage du serveur 66
8.2.3 Options globales 68
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 74
9.2 Configuration d'un serveur WireGuard 75
9.2.1 Préparation 75
9.2.2 Étapes de configuration 76
9.2.3 Dépannage 79
Chapitre 10 Configuration d'un client VPN 80
10.1 Configuration d'un client OpenVPN 81
10.1.1 Préparation 81
10.1.2 Configuration de NordVPN 81
10.1.3 Configuration manuelle d'un client OpenVPN pour un autre fournisseur 87
10.2 Configuration d'un client WireGuard 90
10.2.1 Préparation 90
10.2.2 Configuration d'AzireVPN 91
10.2.3 Configuration de Mullvad 94
10.2.4 Configuration manuelle d'un client WireGuard pour un autre fournisseur 98
Chapitre 11 Tor 103
Chapitre 12 Applications 106
12.1 Extensions 107

12.2 DNS dynamique 108
12.2.1 Activation du DDNS 108
12.2.2 Vérification du fonctionnement du DDNS 111
12.2.3 Accès HTTPS à distance 113
12.2.4 Accès SSH à distance 116
12.3 GoodCloud 118
12.3.1 Activation de GoodCloud 119
12.3.2 Gestion de votre routeur 124
12.3.3 Dissociation de l'appareil 131
12.4 Stockage réseau 132
12.4.1 Branchement du stockage 132
12.4.2 Configuration de Samba 133
12.4.3 Configuration de WebDAV 136
12.4.4 Configuration de DLNA 139
12.5 AdGuard Home 140
12.6 Contrôle parental 143
12.6.1 Configuration rapide 143
12.6.2 Dépannage 152
12.7 ZeroTier 153
12.7.1 Configuration de ZeroTier 154
12.7.2 Autoriser l'accès distant au WAN 158
12.7.3 Autoriser l'accès distant au LAN 159
12.8 Tailscale 160
12.8.1 Configuration de Tailscale 161
12.8.2 Autoriser l'accès à distance au réseau WAN 164
12.8.3 Autoriser l'accès à distance au réseau LAN 165
12.8.4 Nœuds de sortie personnalisés 166
Chapitre 13 Réseau 167
13.1 Pare-feu 168
13.1.1 Redirections de ports 168
13.1.2 Ouverture de ports sur le routeur 170
13.1.3 DMZ 171
13.2 Multi-WAN 172
13.2.1 Suivi de l'état des interfaces 172

13.2.2 Mode Multi-WAN 175
13.3 LAN 178
13.3.1 Paramètres de base 178
13.3.2 Serveur DHCP 179
13.3.3 Réservation d'adresses 181
13.4 Réseau invité 182
13.4.1 Paramètres de base 182
13.4.2 Serveur DHCP 183
13.5 DNS 185
13.5.1 Paramètres généraux 185
13.5.2 Paramètres du serveur DNS 186
13.5.3 Modification du fichier hosts 188
13.6 Mode réseau 190
13.7 IPv6 192
13.7.1 Mode IPv6 192
13.7.2 Méthode d'obtention du DNS 193
13.8 Adresse MAC 194
13.9 Passerelle transparente 196
13.10 IGMP Snooping 198
13.11 Paramètres NAT 199
Chapitre 14 Système 200
14.1 Vue d'ensemble 201
14.2 Mise à jour 202
14.2.1 Mise à jour en ligne 202
14.2.2 Mise à jour locale 203
14.3 Tâches planifiées 205
14.3.1 Programmation du voyant LED 205
14.3.2 Redémarrage planifié 206
14.3.3 Programmation du Wi-Fi 5 GHz 207
14.3.4 Programmation du Wi-Fi 2,4 GHz 210
14.4 Fuseau horaire 213
14.5 Paramètres du commutateur 214
14.6 Journaux 215
14.7 Sécurité 216

14.7.1 Mot de passe administrateur 216
14.7.2 Contrôle des accès locaux 217
14.7.3 Contrôle d’accès distant 219
14.8 Réinitialisation du micrologiciel 220
14.9 Paramètres avancés 221

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

Slate Plus (GL-A1300) est un routeur de voyage de poche doté d’un processeur puissant, optimisé pour la stabilité du réseau et le traitement efficace du chiffrement VPN. Il intègre nos dernières fonctionnalités de sécurité et fonctionne sous la dernière version du système d’exploitation OpenWrt. Il est conçu pour les voyageurs fréquents qui utilisent beaucoup les réseaux VPN.

1.1.1 Aspect extérieur

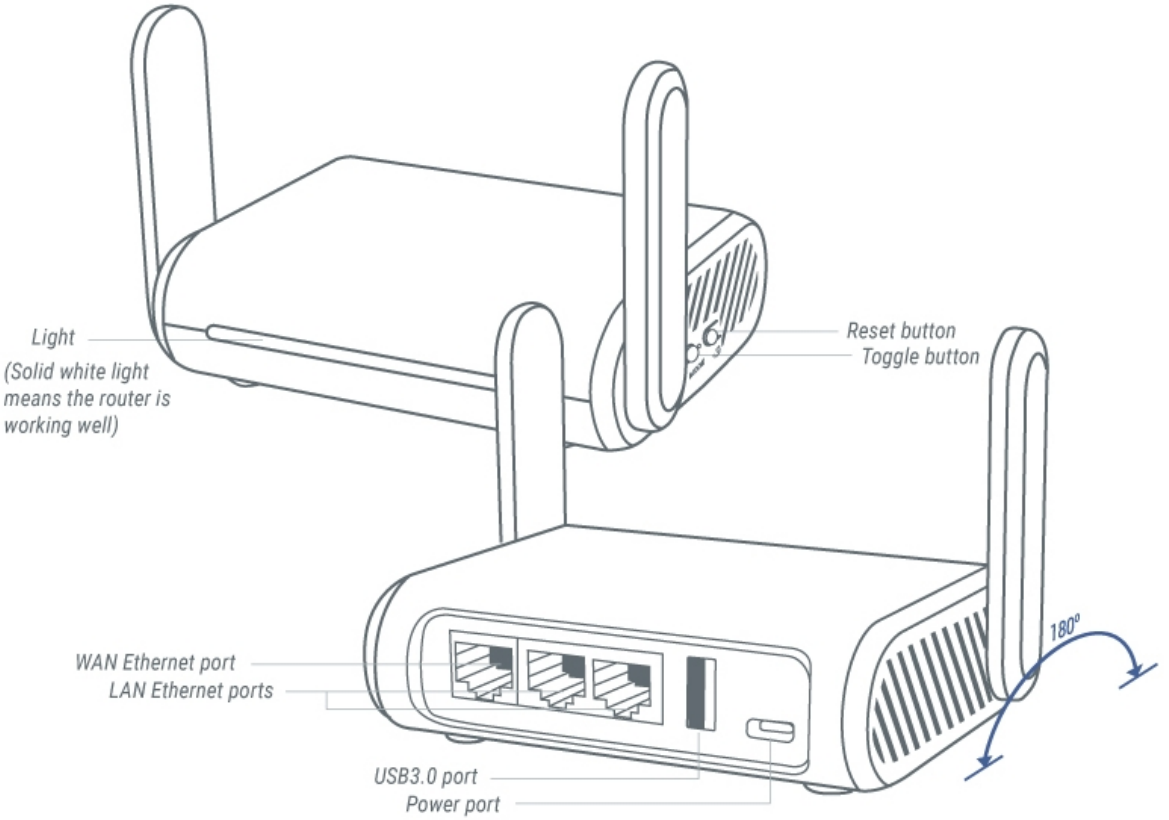








1.1.2 Ports et boutons



Élément	Description
Prise d'alimentation	Permet de brancher l'adaptateur secteur.
Port Ethernet WAN	Permet de relier le routeur à un modem ou à une prise Ethernet pour accéder à Internet.
Port Ethernet LAN	Permet de brancher des appareils filaires si nécessaire.
Port USB 3.0	Pour les périphériques 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** pour réparer votre connexion réseau ; Maintenez enfoncé pendant **10 secondes**, puis relâchez : le routeur retrouve ses paramètres d'usine.

Commutateur	Un commutateur physique permet de modifier certains paramètres du routeur d'un simple geste. Configurez-le dans l'interface Web pour activer ou désactiver les fonctions souhaitées.

1.1.3 LED

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

1.2 Caractéristiques techniques

Interfaces	1 port Ethernet WAN 2 ports Ethernet LAN 1 port USB 3.0 1 port d'alimentation Type-C 1 bouton de réinitialisation 1 commutateur
CPU	IPQ4018, quatre cœurs à 717 MHz
Mémoire / Stockage	DDR3L 256 Mo / mémoire flash NOR 4 Mo + mémoire flash NAND 128 Mo
Protocoles	IEEE 802.11a/b/g/n/ac
Débit Wi-Fi	400 Mbit/s (2,4 GHz), 867 Mbit/s (5 GHz)
Antennes	2 antennes Wi-Fi externes non amovibles

Débit Ethernet	10/100/1 000 Mbit/s
Alimentation	USB-C, 5 V / 3 A
Consommation électrique	< 6,5 W
Température de fonctionnement	0 à 40 °C (32 à 104 °F)
Température de stockage	−20 à 70 °C (−4 à 158 °F)
Dimensions / Poids	118 × 85 × 30 mm / 181 g
Autres ressources	Fiche technique / Micrologiciel / Application / Déballage

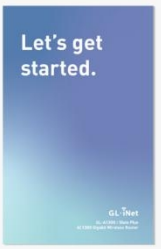
*Les débits Wi-Fi reposent sur les normes IEEE 802.11, par exemple 802.11ac pour le Wi-Fi 5. Le débit réel et la portée peuvent être inférieurs en raison d'obstacles (murs, métal), de la congestion du réseau ou des capacités des appareils clients.
*L'utilisation du Wi-Fi 5 (802.11ac) et de ses fonctionnalités (MU-MIMO, 256-QAM, HT80) nécessite des appareils clients prenant en charge les technologies correspondantes.

1.3 Contenu de l'emballage

L'adaptateur fourni dépend du pays de livraison.
L'emballage contient :

- 1 × Slate Plus (GL-A1300)
- 1 manuel d'utilisation
- 1 câble Ethernet
- 1 carte de remerciement
- 1 carte de garantie
- 1 adaptateur secteur
- 1 adaptateur de prise (selon le pays de livraison)

User manual



Slate Plus (GL-A1300)



Ethernet cable



Thank you card



Warranty card



Power adapter



Converters

(Base on your shipping countries)



US version

UK/EU version

Chapitre 2

Branchements

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

2.1 Choix de l’emplacement

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

- **Évitez l’humidité et la chaleu**r : ne placez pas le routeur dans un endroit exposé à l’eau, à l’humidité ou à des températures élevées, par exemple près d’un évier ou d’un radiateur.
- **Ventilation et refroidissement** : placez le routeur dans un endroit frais et bien ventilé pour permettre une bonne dissipation de la chaleur.
- **Emplacement central** : placez le routeur à un endroit permettant de le brancher facilement à une prise de courant et de connecter plusieurs appareils, par exemple au centre du salon.
- **Disposition des câbles** : disposez les câbles et le cordon d’alimentation de manière à éviter tout risque de trébuchement.
- **Surface stable** : posez le routeur sur une surface plane et horizontale, comme une étagère ou un bureau, pour assurer sa stabilité.
- **Évitez les interférences électromagnétiques** : éloignez le routeur des sources d’interférences, comme les appareils Bluetooth ou les fours à micro-ondes, pour limiter les perturbations du signal.

2.2 Branchement du routeur

1. **Mise sous tension**

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

   Connectez un appareil, tel qu’un ordinateur portable ou un smartphone, au routeur par Wi-Fi ou à l’aide d’un câble Ethernet.
   - **Wi-Fi** : sur votre appareil, ouvrez Paramètres > WLAN, repérez le nom du réseau Wi-Fi du routeur dans la liste des réseaux disponibles et saisissez le mot de passe. Le nom du réseau et le mot de passe par défaut figurent sur l’étiquette du routeur.
   - **Ethernet** : reliez votre appareil à un port LAN du routeur à l’aide d’un câble Ethernet.
3. **Connexion à l’interface du routeur**

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

Chapitre 3

Connexion à l’interface du routeur

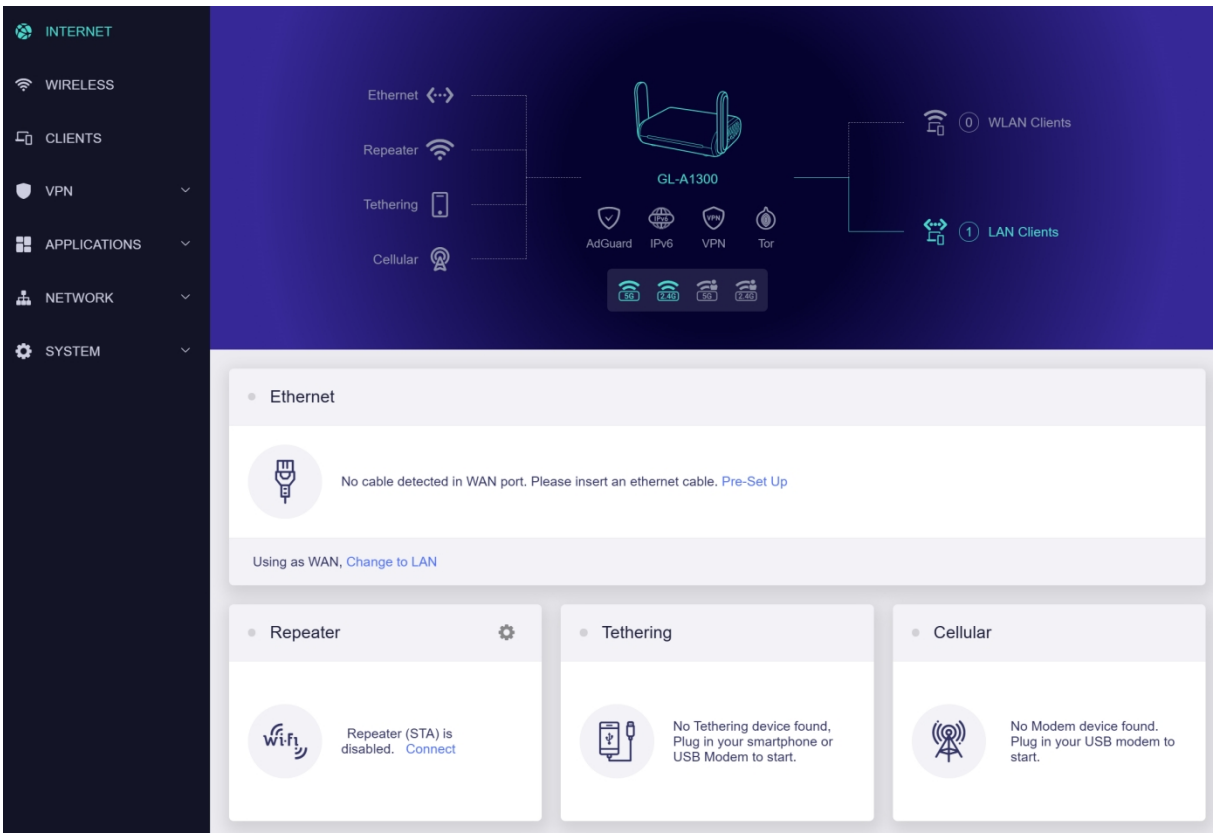
Ce chapitre explique comment vous connecter à l’interface d’administration Web du routeur.

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

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

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

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



Chapitre 4

Configuration de la connexion Internet

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

Slate Plus propose quatre modes de connexion à Internet : Ethernet, répéteur, partage de connexion USB et modem USB. Choisissez celui qui convient à vos besoins.

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

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

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

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

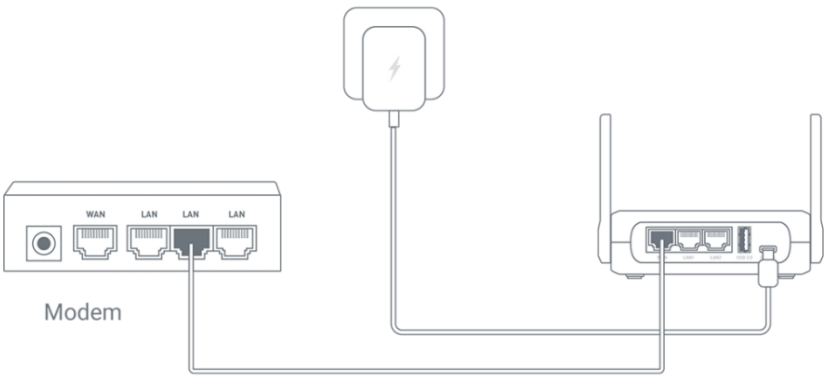
4.1 Connexion à Internet via un câble Ethernet

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

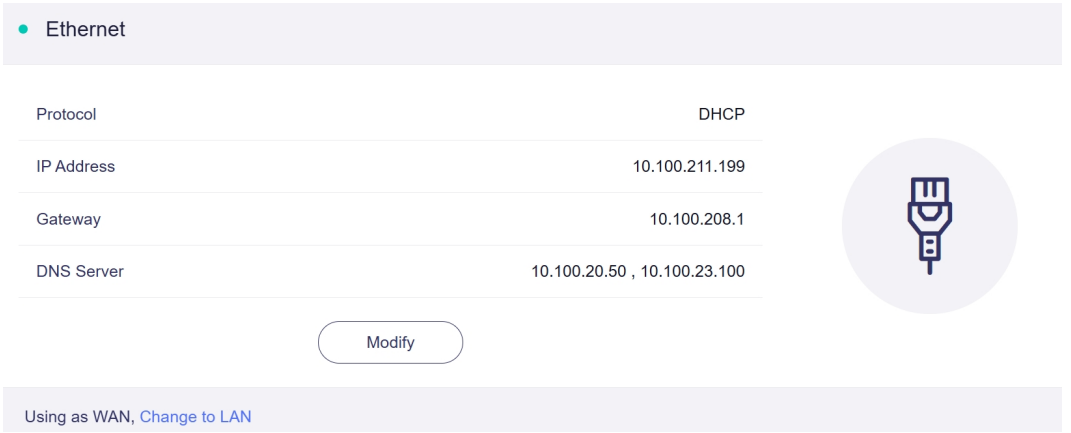
4.1.1 Configuration de base

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.

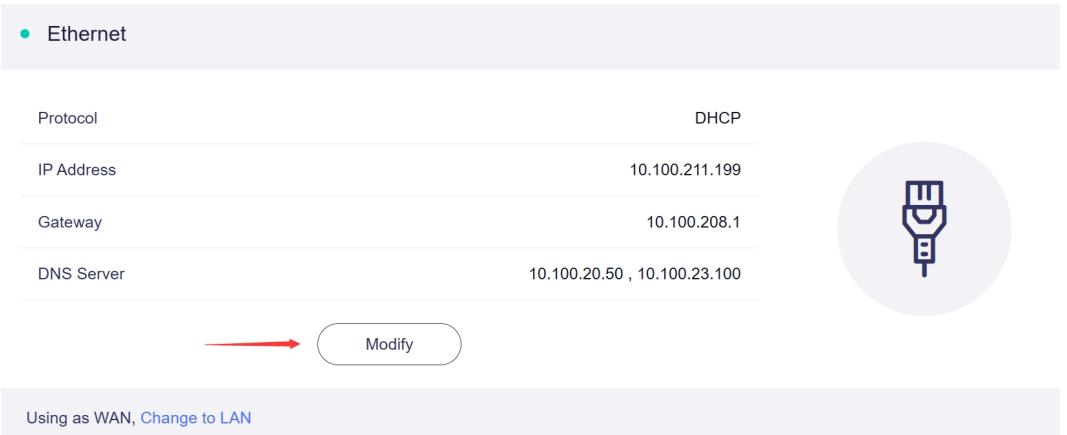


2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Ethernet**. Si la connexion est établie, la section Ethernet affiche les informations réseau, notamment le protocole, l'adresse IP, la passerelle et le serveur DNS.


Ethernet
Protocol
DHCP
IP Address
10.100.211.199
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Modify
Using as WAN, Change to LAN

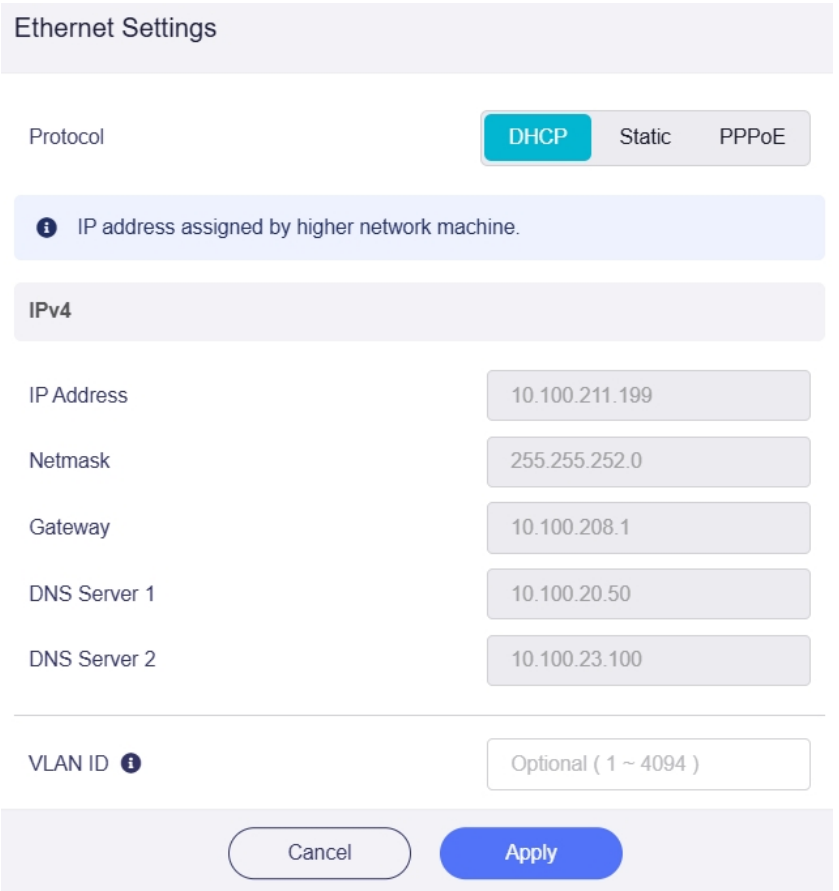
4.1.2 Protocole

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



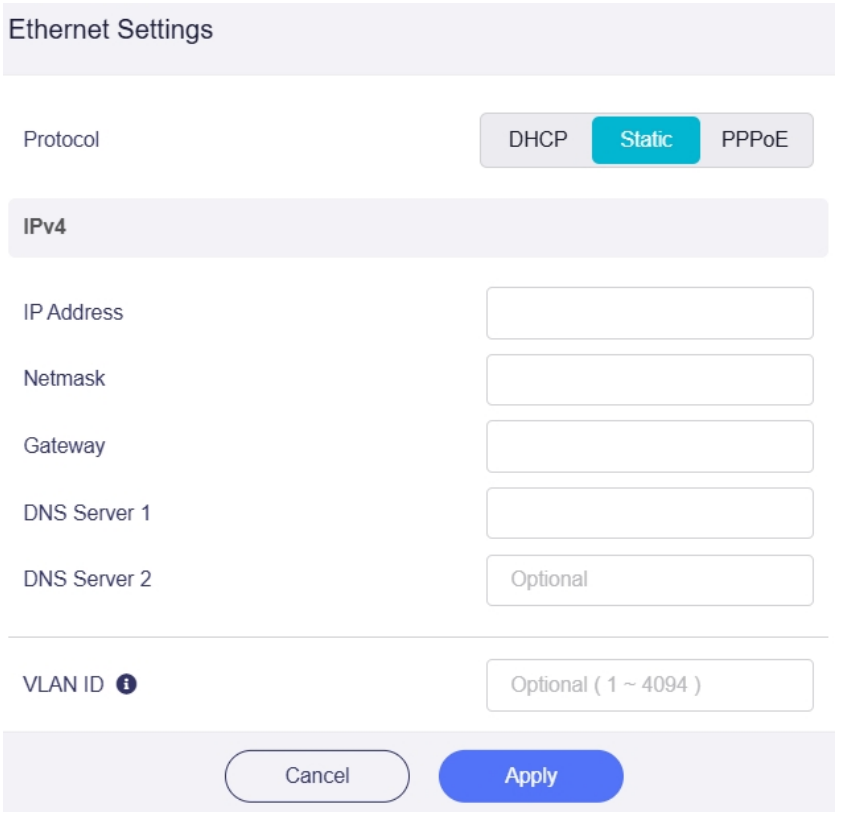
- **DHCP**

  DHCP est le protocole réseau par défaut et le plus courant. Il attribue automatiquement des adresses IP et d'autres paramètres de configuration aux appareils d'un réseau IP selon un modèle client-serveur. Vous pouvez définir un **ID de VLAN (VLAN ID)** si votre fournisseur exige que l'interface utilise un ID de VLAN étiqueté spécifique.



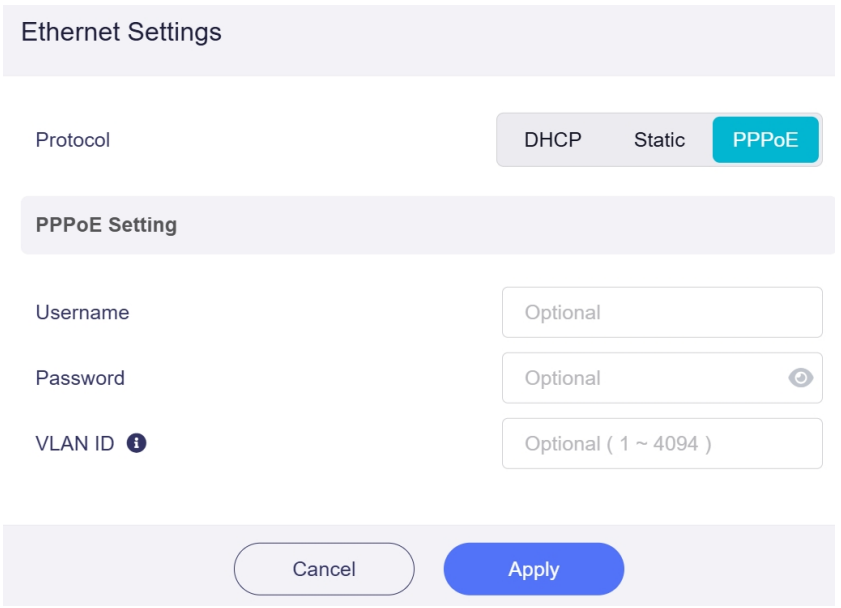
- **Statique (Static)**

  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 configurer manuellement les paramètres réseau, tels que l'adresse IP, la passerelle et le masque de sous-réseau. Vous pouvez définir un **ID de VLAN (VLAN ID)** si votre fournisseur exige que l'interface utilise un ID de VLAN étiqueté spécifique.



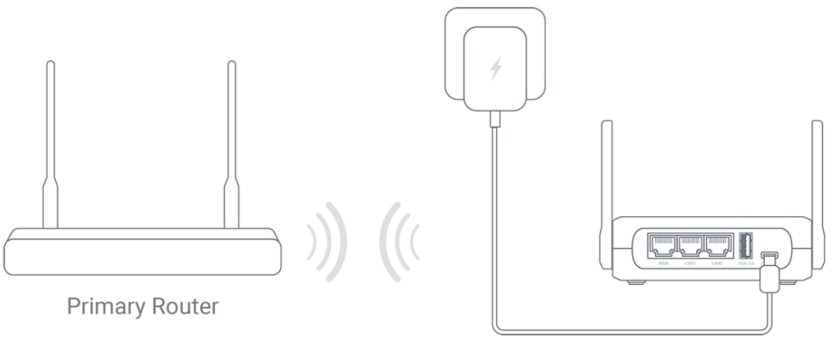
- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) est un protocole réseau largement utilisé par les fournisseurs d'accès à Internet. Ceux-ci fournissent généralement un modem ainsi qu'un nom d'utilisateur et un mot de passe uniques, nécessaires pour établir une connexion à Internet. Vous pouvez définir un **ID de VLAN (VLAN ID)** si votre fournisseur exige que l'interface utilise un ID de VLAN étiqueté spécifique.


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

4.2 Connexion à Internet via un réseau Wi-Fi existant

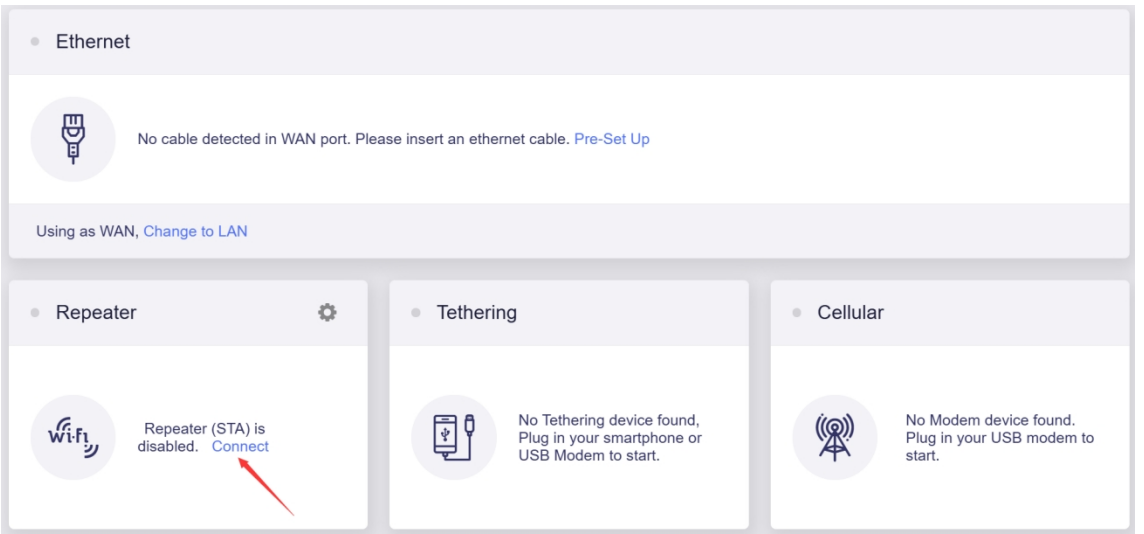
Connectez le routeur en mode répéteur à un réseau Wi-Fi existant pour renforcer la couverture et créer un réseau local isolé du réseau principal. Dans un hôtel ou un café proposant un point d'accès public gratuit, le répéteur étend le signal Wi-Fi, permet à plusieurs appareils de se connecter par câble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



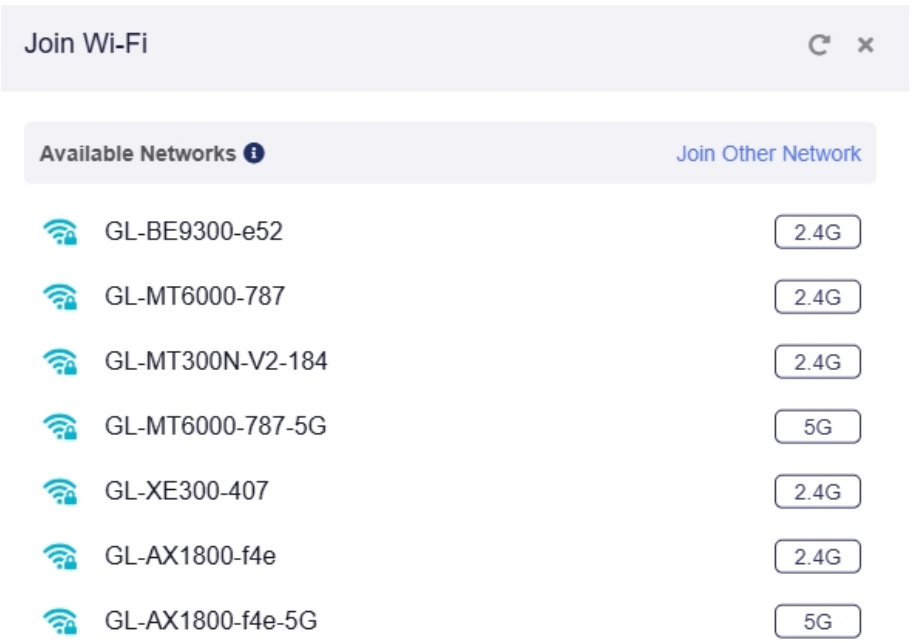
La fonction répéteur GL.iNet utilise par défaut le mode WISP (Wireless Internet Service Provider). Le routeur crée ainsi son propre sous-réseau et agit comme un pare-feu pour vous protéger du réseau public.

4.2.1 Configuration de base

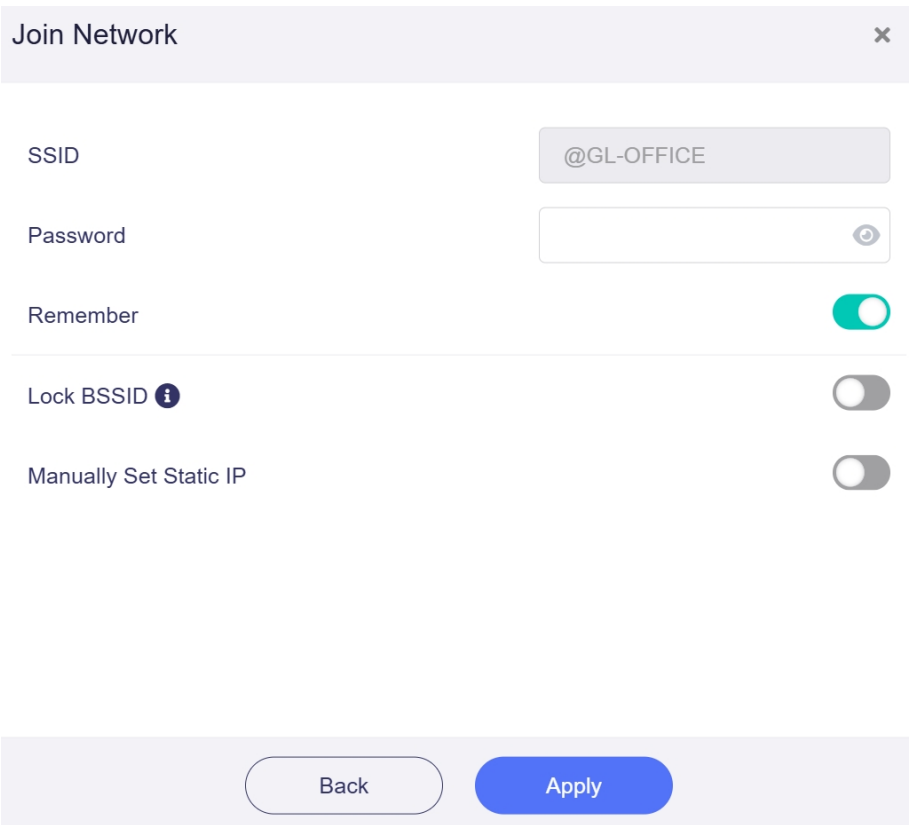
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Répéteur (Repeater)**. Cliquez sur **Connecter (Connect)**.



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



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

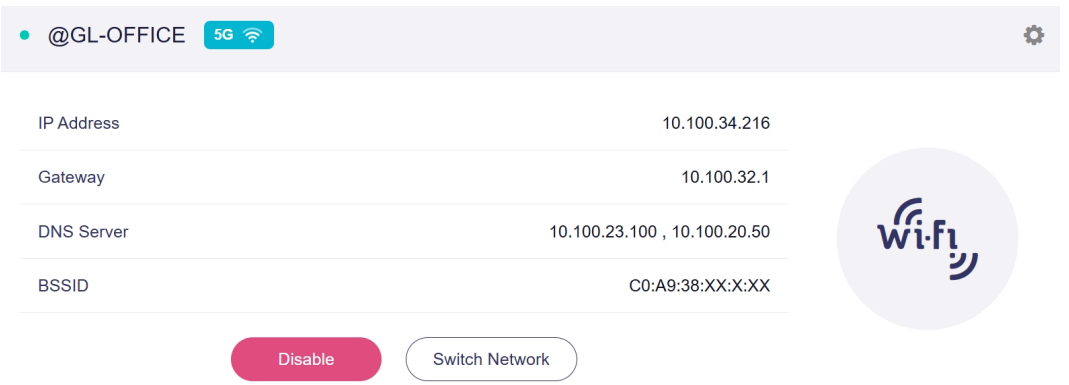


- **Mémoriser (Remember)** : activez cette option pour mémoriser le réseau Wi-Fi actuellement utilisé en mode répéteur.
- **Verrouiller le BSSID (Lock BSSID)** : lorsque cette option est activée, le routeur se connecte uniquement au point d'accès correspondant au BSSID sélectionné, même si d'autres points d'accès utilisent le même SSID.
- **Définir manuellement une adresse IP statique (Manually Set Static IP)** : si cette option est activée, vous pouvez configurer manuellement l'adresse IP, le masque de sous-réseau, la passerelle et les serveurs DNS, au lieu d'obtenir automatiquement les paramètres IP via DHCP.

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

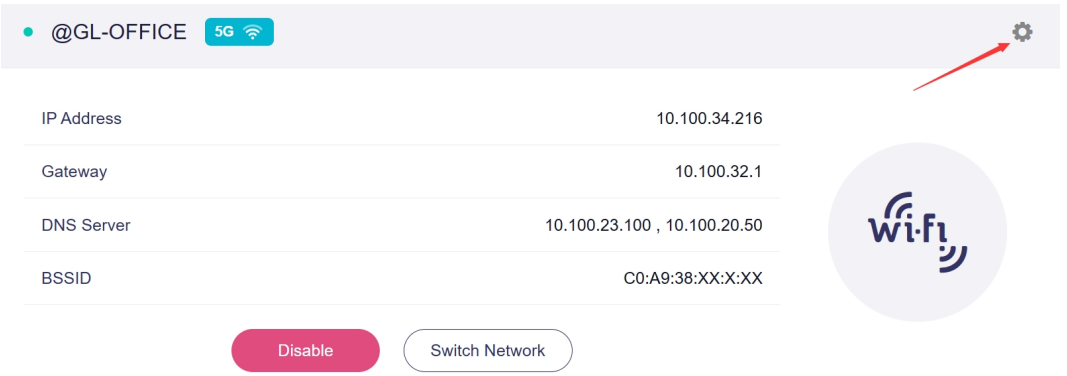


5. Patientez une minute pendant la connexion du routeur. Une fois la connexion établie, la page se présente comme ci-dessous.

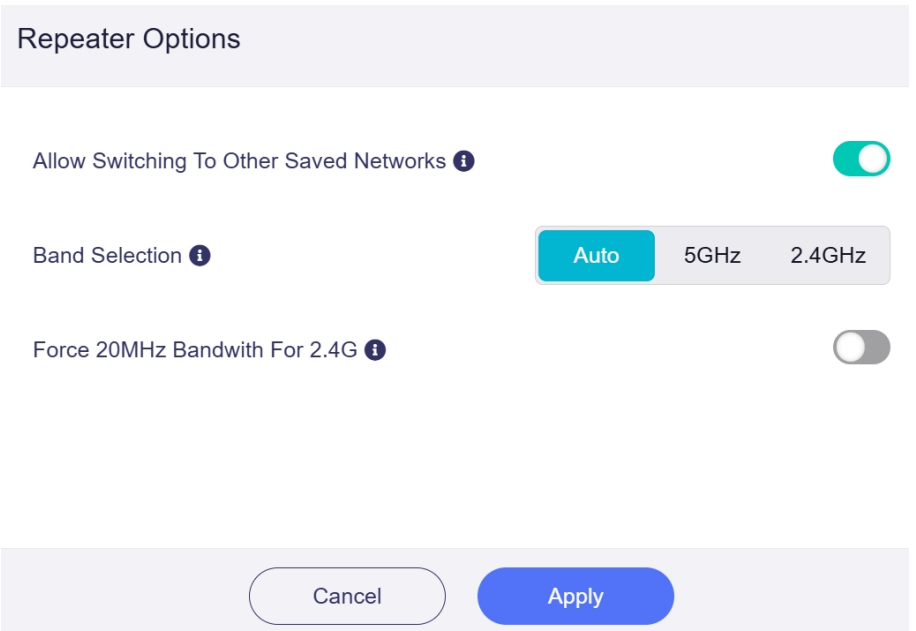


4.2.2 Options du répéteur

Cliquez sur l'icône d'engrenage en haut à droite pour configurer les options du répéteur.



La page peut varier selon la version du micrologiciel.



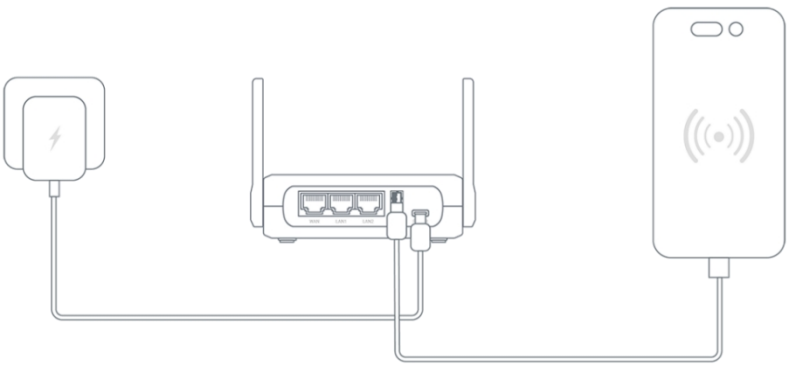
- **Autoriser le passage à d'autres réseaux enregistrés (Allow Switching to Other Saved Networks)** : si cette option est activée, le routeur se connecte automatiquement à un autre réseau enregistré lorsqu'il ne peut pas se connecter au réseau Wi-Fi actuel.
- **Sélection de bande (Band Selection)** : si vous sélectionnez manuellement une bande, le routeur ne recherche pas les réseaux Wi-Fi utilisant une autre bande et ne s'y connecte pas.

- **Forcer une largeur de bande de 20 MHz en 2,4 GHz (Force 20MHz Bandwidth for 2.4G)** : si cette option est activée, l’appareil améliore la stabilité de la connexion en réduisant son débit.

  Remarque : cette option fonctionne uniquement lors de la répétition d’un réseau Wi-Fi 2,4 GHz.

4.3 Connexion à Internet par partage de connexion USB

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

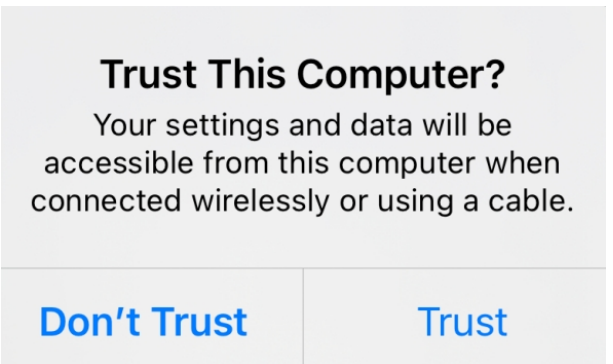


Les modems autonomes, dits « host-less », utilisent également le mode de partage de connexion USB lors de leur configuration.

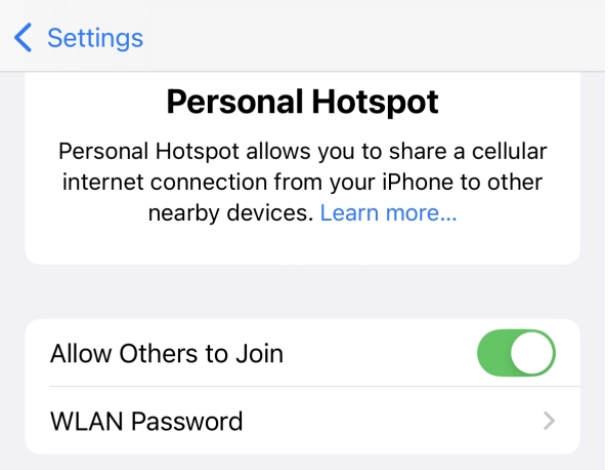
Remarque : certains opérateurs mobiles limitent le partage de connexion ou le facturent en supplément. Renseignez-vous auprès de votre opérateur.

4.3.1 Partage de connexion avec un iPhone

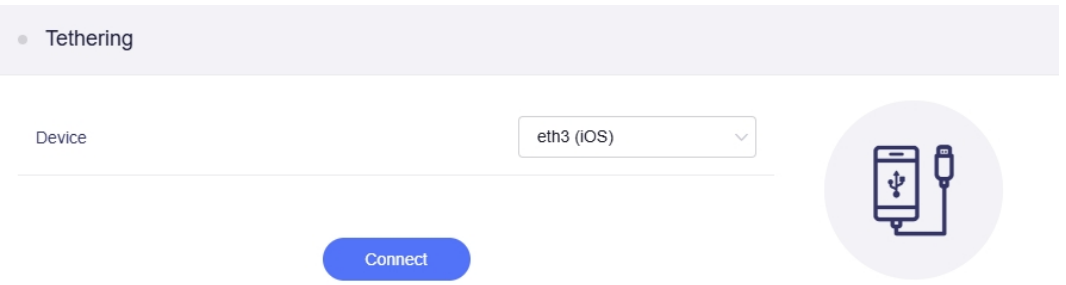
1. Reliez l'iPhone au port USB du routeur à l'aide d'un câble USB. Une boîte de dialogue vous demande si vous souhaitez faire confiance à cet appareil. Touchez **Se fier (Trust)** pour continuer.



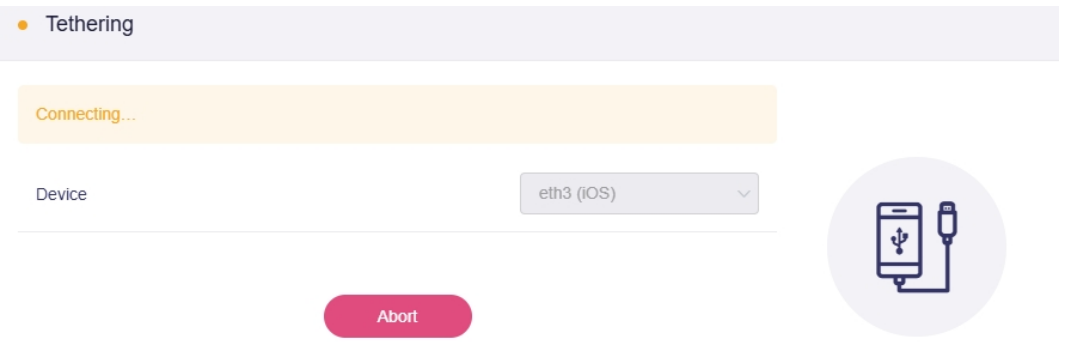
2. Sur l'iPhone, ouvrez **Réglages (Settings)** > **Partage de connexion (Personal Hotspot)**. Activez **Autoriser d'autres utilisateurs (Allow Others to Join)**.



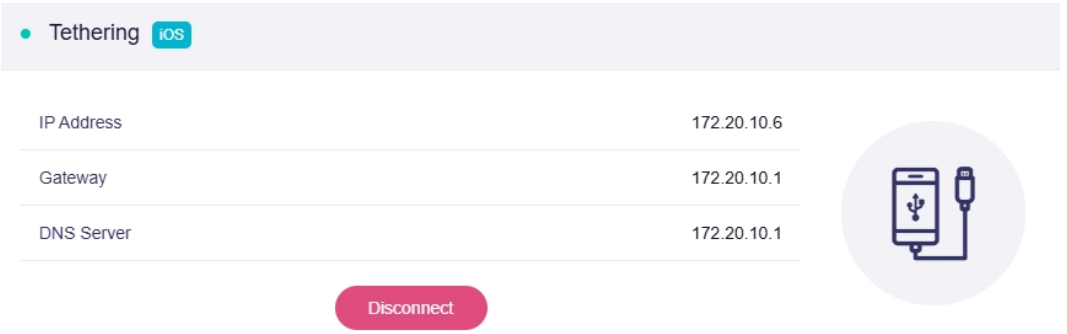
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



4. La connexion démarre.

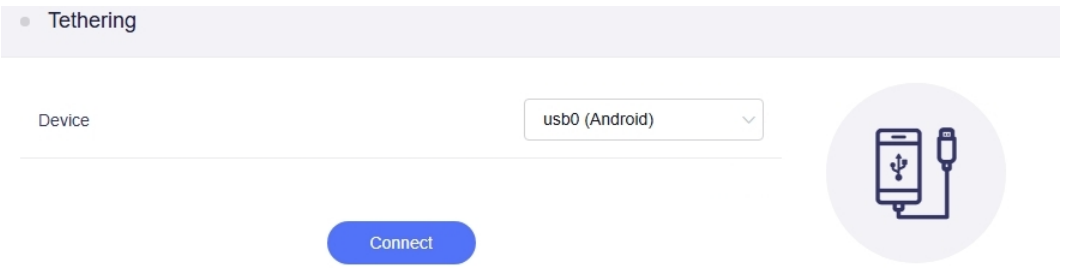


Une fois la connexion établie, cette page en affiche les détails.

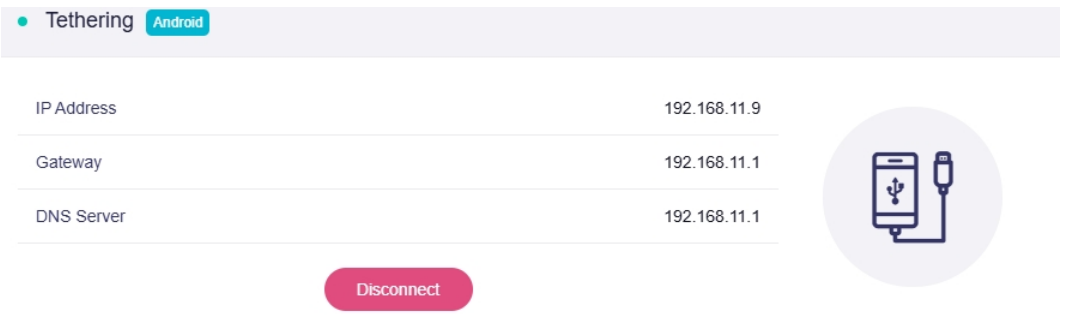


4.3.2 Partage de connexion avec un appareil Android

1. Reliez le téléphone Android au port USB du routeur avec un câble USB. Une boîte de dialogue peut afficher les préférences USB (USB preferences). Si vous y êtes invité, sélectionnez **Partage de connexion USB (USB Tethering)** ou **Transfert de fichiers (File Transfer)**.
2. Sur le téléphone, ouvrez **Paramètres (Settings)** > **Réseau et Internet (Network & Internet)** > **Point d'accès personnel (Personal Hotspot)**. Activez **Point d'accès personnel (Personal Hotspot)** ou **Partage de connexion USB (USB Tethering)**. (La procédure d'activation du partage de connexion USB varie selon la marque. Consultez les paramètres de votre appareil pour trouver cette option et contactez l'assistance du fabricant si nécessaire.)
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, puis ouvrez **INTERNET** > **Partage de connexion (Tethering)**. Cliquez sur **Connecter (Connect)**.



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



4.3.3 Dépannage

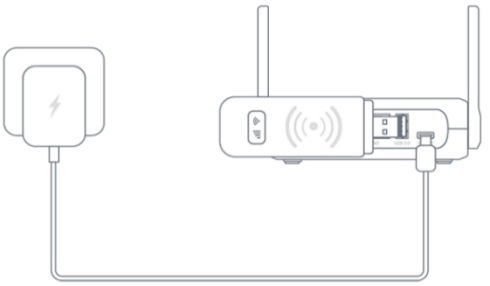
Si le partage de connexion échoue, essayez les solutions suivantes :

- 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.

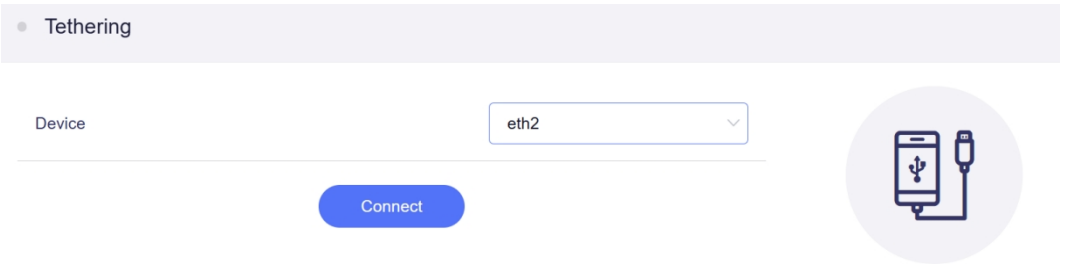
4.4 Connexion à Internet via un modem USB

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

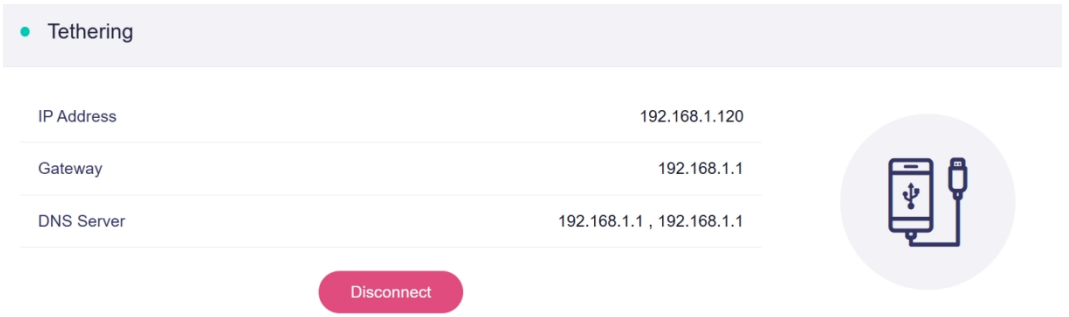


Suivez les étapes ci-dessous pour connecter le routeur à Internet via un modem USB.

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



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



Conseil : après la configuration initiale, si vous redémarrez le routeur en laissant le modem USB branché ou si vous le rebranchez au routeur, le modem sera reconnu automatiquement et une connexion réseau sera établie sans avoir à cliquer de nouveau sur « Connecter (Connect) ».

Chapitre 5

Réseau sans fil

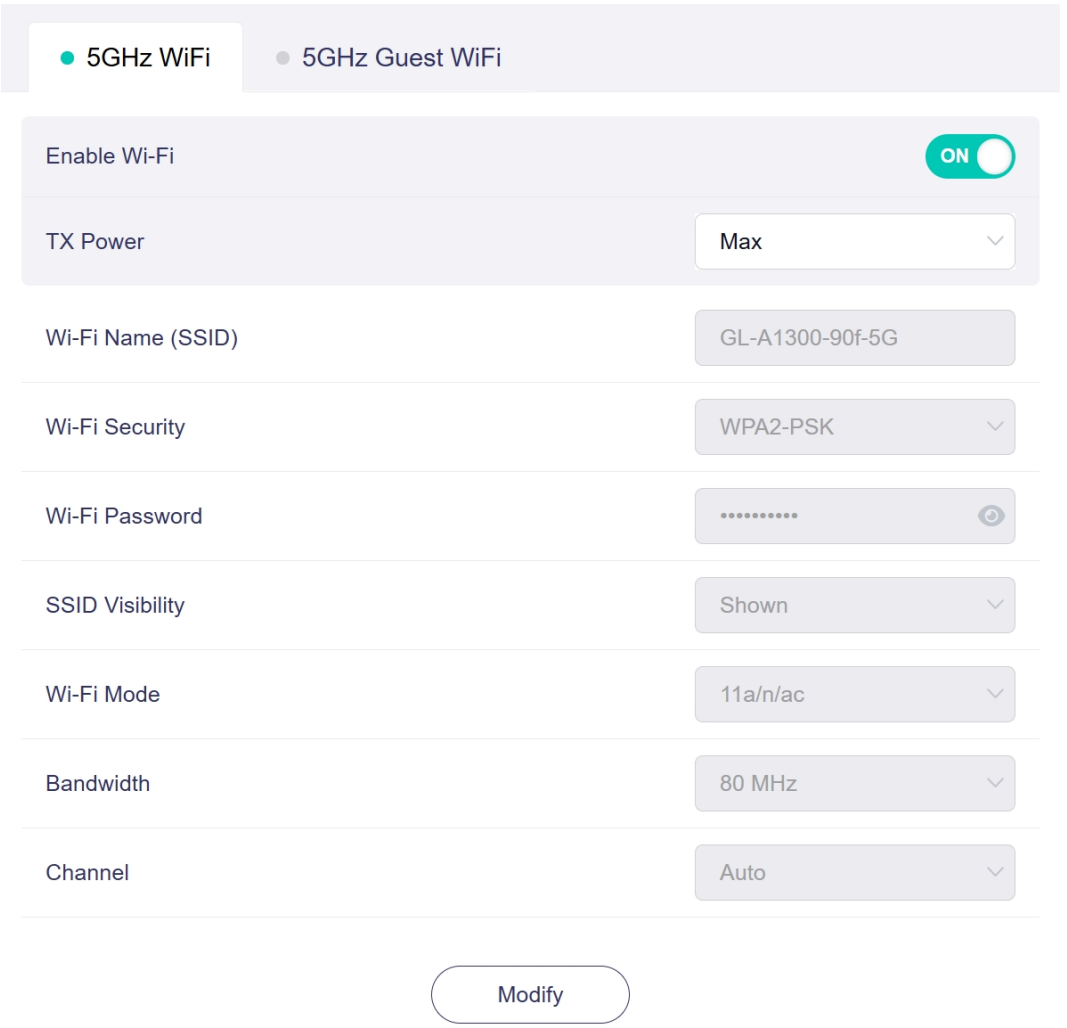
Ce chapitre explique comment consulter et configurer les paramètres du réseau sans fil.

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

Cette page affiche les paramètres Wi-Fi des bandes 2,4 GHz et 5 GHz. Chaque bande comporte un réseau principal et un réseau invité pour faciliter leur gestion.

5.1 Wi-Fi 5 GHz

Le réseau Wi-Fi principal 5 GHz permet de configurer plusieurs paramètres : activation ou désactivation du Wi-Fi, puissance d'émission, nom du réseau (SSID), sécurité, mot de passe, visibilité du SSID, mode, largeur de bande et canal.

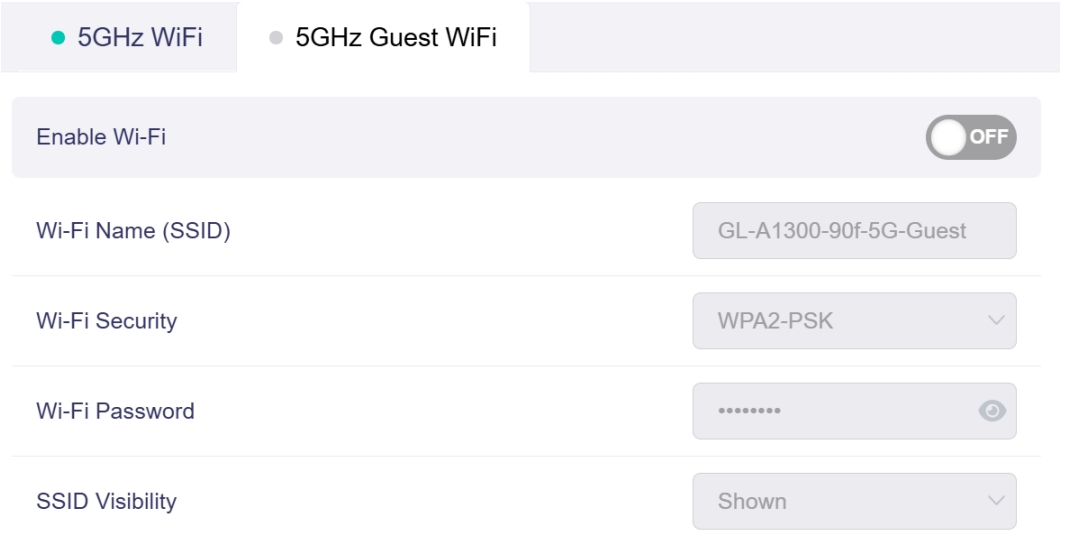


Remarque :

1. Les paramètres **Largeur de canal (Bandwidth)** et **Canal (Channel)** ne peuvent pas être modifiés lorsque le routeur fonctionne en mode répéteur : ils suivent ceux du réseau auquel il se connecte.

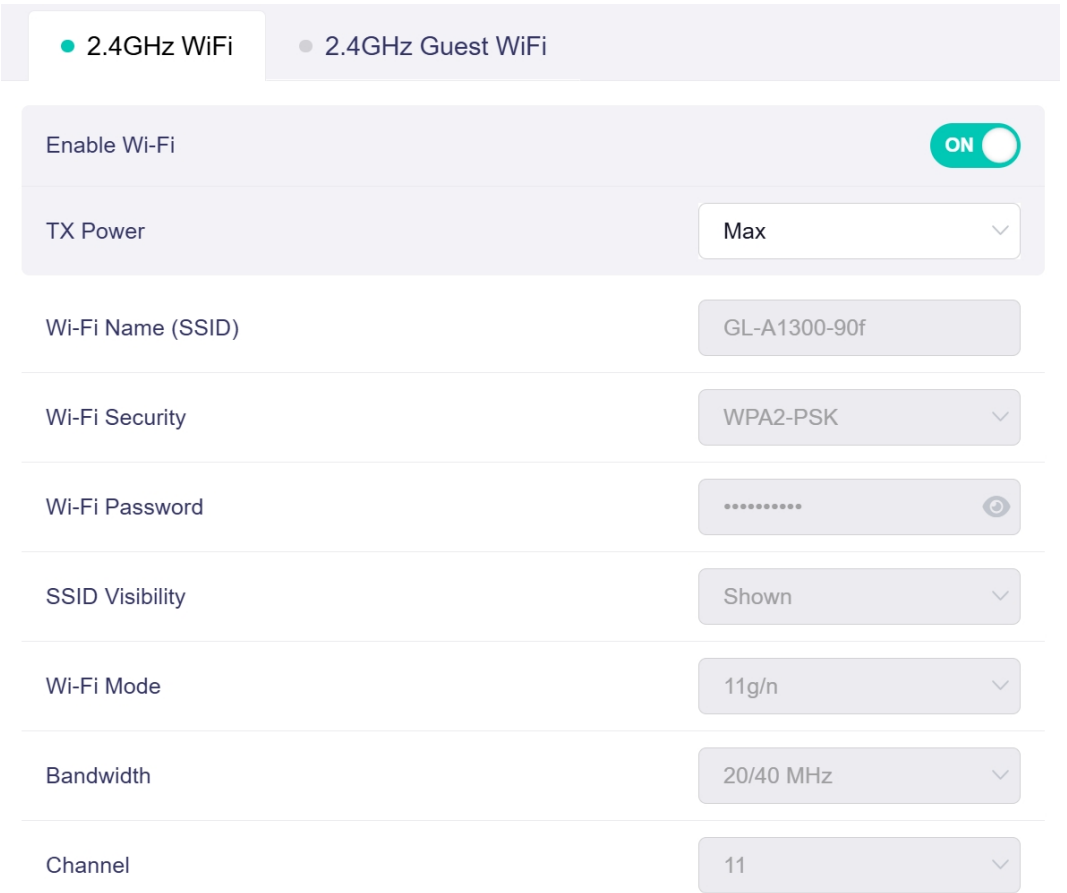
2. Lorsque **Canal (Channel)** est réglé sur **Auto**, le Wi-Fi du routeur ne bascule pas automatiquement sur un canal DFS.

Pour le réseau Wi-Fi invité 5 GHz, vous pouvez activer ou désactiver le Wi-Fi et définir le nom du réseau (SSID), la sécurité, le mot de passe et la visibilité du SSID.

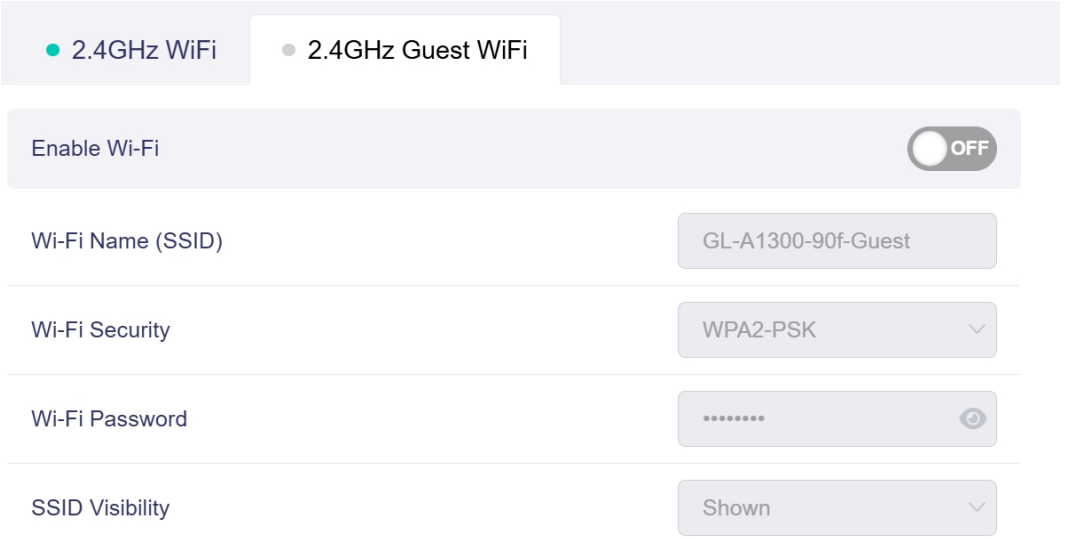


5.2 Wi-Fi 2,4 GHz

Le réseau Wi-Fi principal 2,4 GHz permet de configurer plusieurs paramètres : activation ou désactivation du Wi-Fi, puissance d'émission, nom du réseau (SSID), sécurité, mot de passe, visibilité du SSID, mode, largeur de bande et canal.



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



Remarque : la **largeur de bande (Bandwidth)** et le **canal (Channel)** ne peuvent pas être modifiés lorsque le routeur est configuré en répéteur, car ils sont déterminés par le réseau répété.

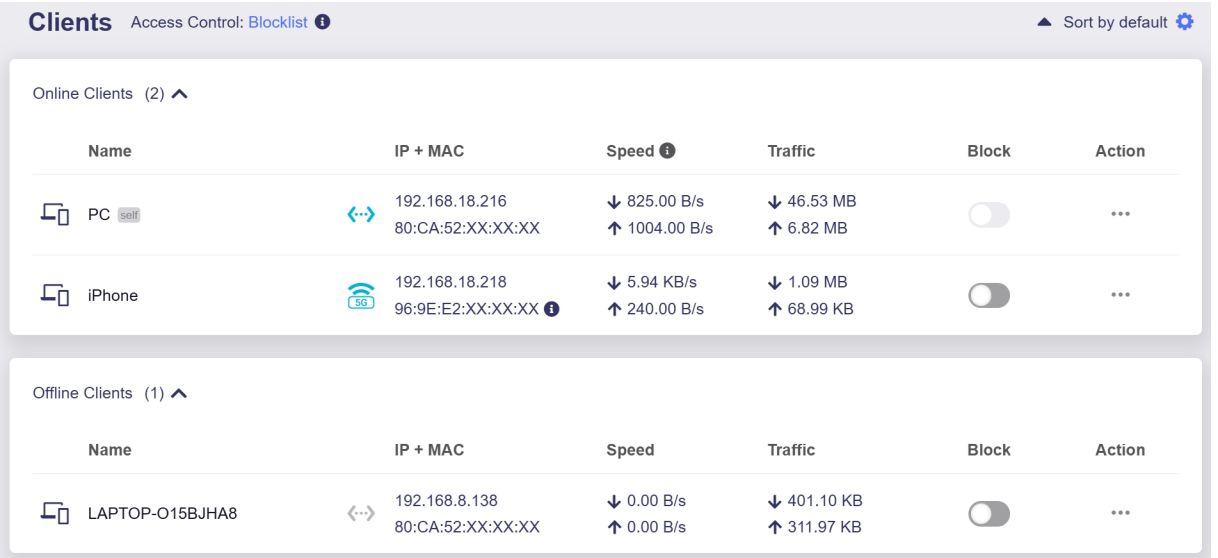
Chapitre 6

Appareils clients

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

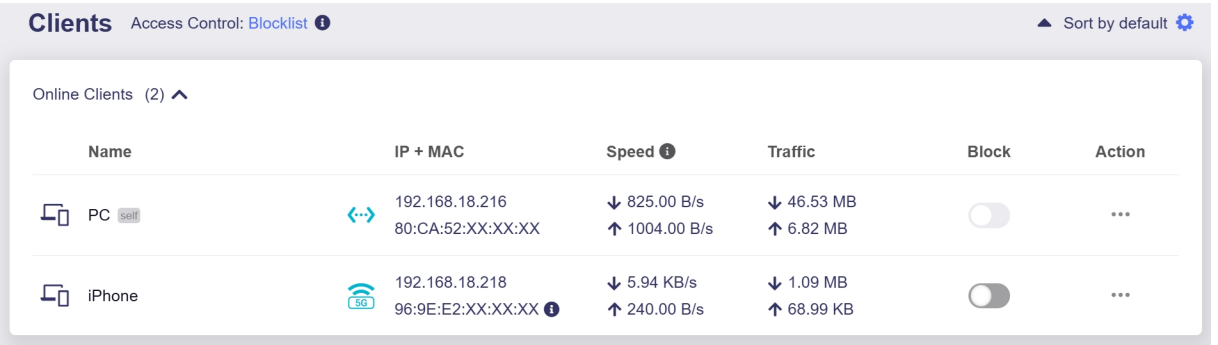
Connectez-vous à l’interface d’administration Web du routeur et ouvrez **CLIENTS**.

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



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

6.1 Informations sur les appareils



1. **Nom de l'appareil**

   La première colonne affiche le nom et le type de l'appareil, selon le nom d'hôte fourni par celui-ci. L'icône bleue à côté du nom indique le mode de connexion : l'appareil est relié au routeur par un câble Ethernet.

2. **Adresses IP et MAC**

   La deuxième colonne affiche les adresses IP et MAC de l'appareil connecté. Si l'appareil utilise une adresse MAC aléatoire, un message le signale.



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

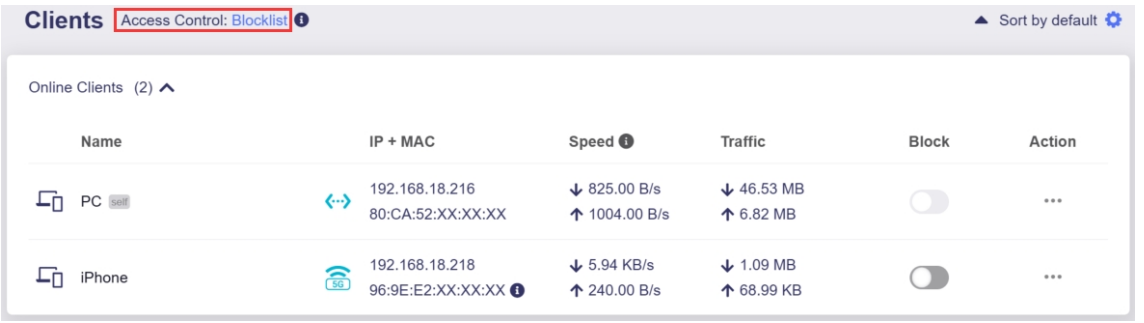
3. **Débit**

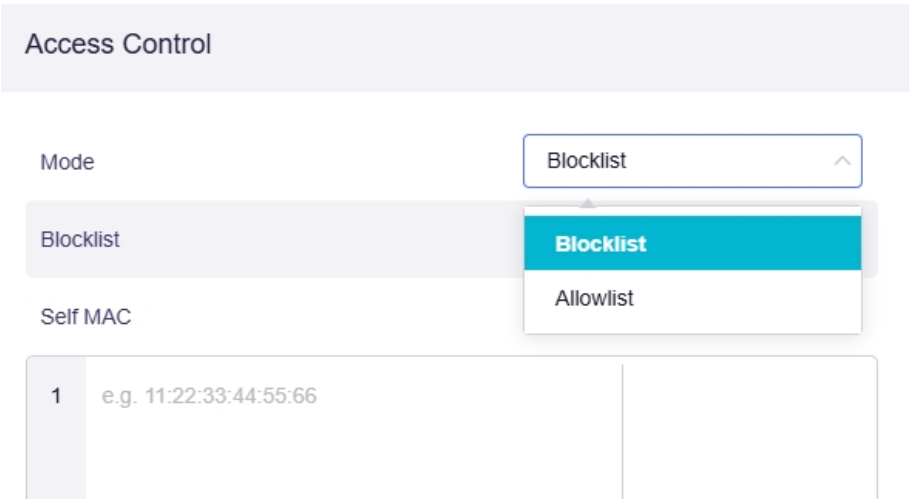
   La troisième colonne affiche le débit Internet de l'appareil connecté. Il s'agit du débit moyen des trois dernières minutes. Le calcul commence à l'ouverture de cette page : si elle n'est ouverte que depuis 10 secondes, la moyenne porte uniquement sur ces 10 secondes.

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

5. **Liste de blocage**

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



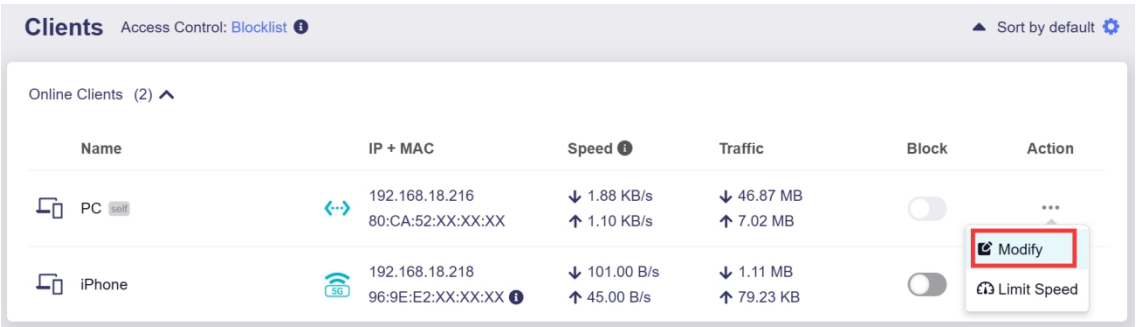


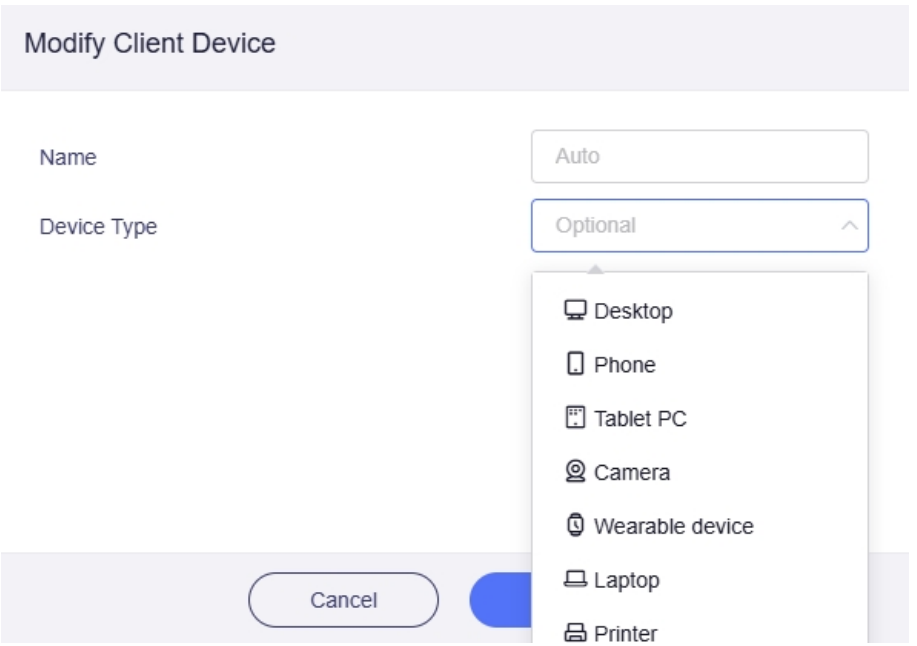
- **Liste de blocage (Blacklist)** : les appareils dont l'adresse MAC figure dans cette liste ne peuvent pas se connecter au routeur. Le blocage repose sur l'adresse MAC : un appareil bloqué peut donc se reconnecter s'il utilise une autre adresse MAC.
- **Liste d'autorisation (Allowlist)** : seuls les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

6.2 Actions

1. **Modifier**

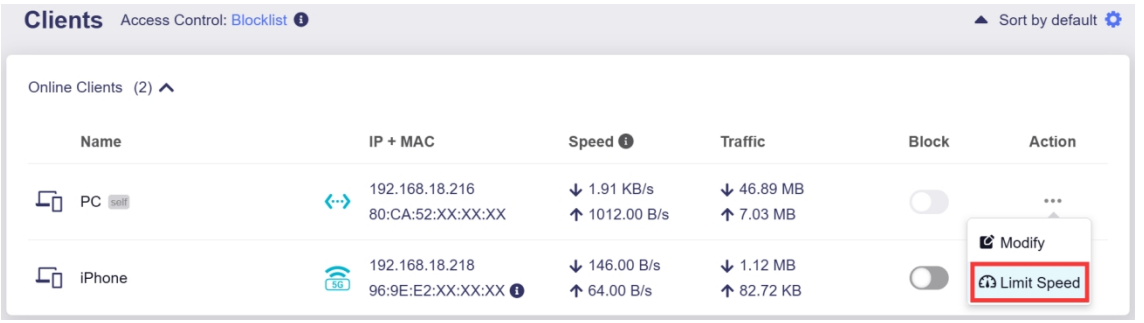
   Cliquez sur les trois points dans la colonne **Action**, puis sur **Modifier (Modify)** dans le menu déroulant pour modifier le nom et le type de l'appareil.



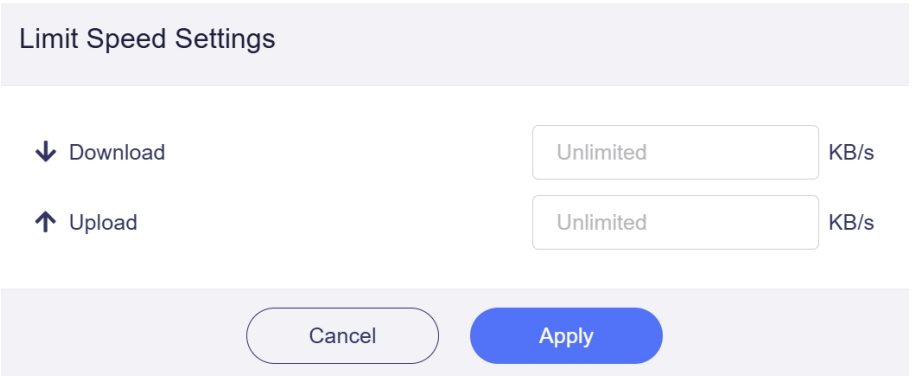


2. **Limiter le débit**

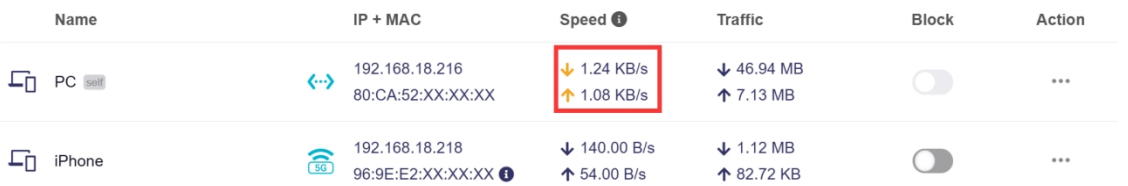
Cliquez sur les trois points dans la colonne **Action**, puis sur **Limiter le débit (Limit Speed)** dans le menu déroulant.



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

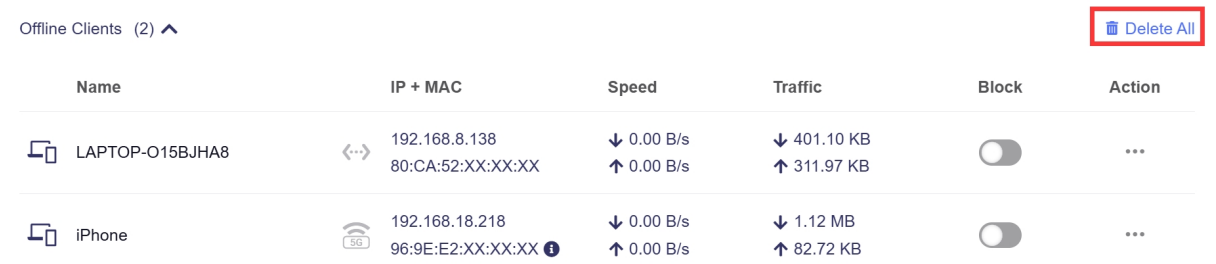


Lorsqu'une limite de débit est appliquée à un appareil, les flèches de débit montant et descendant deviennent jaunes.

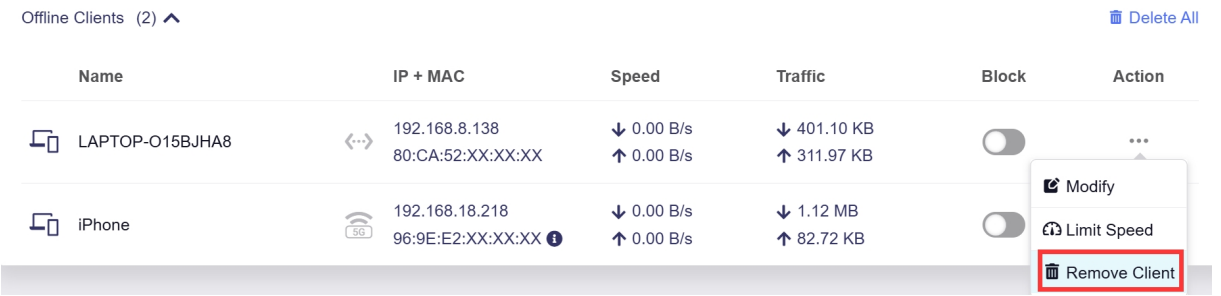


6.3 Suppression de clients

Dans la section **Clients hors ligne (Offline Clients)**, cliquez sur **Tout supprimer (Delete All)** dans l'angle supérieur droit pour supprimer tous les clients hors ligne.

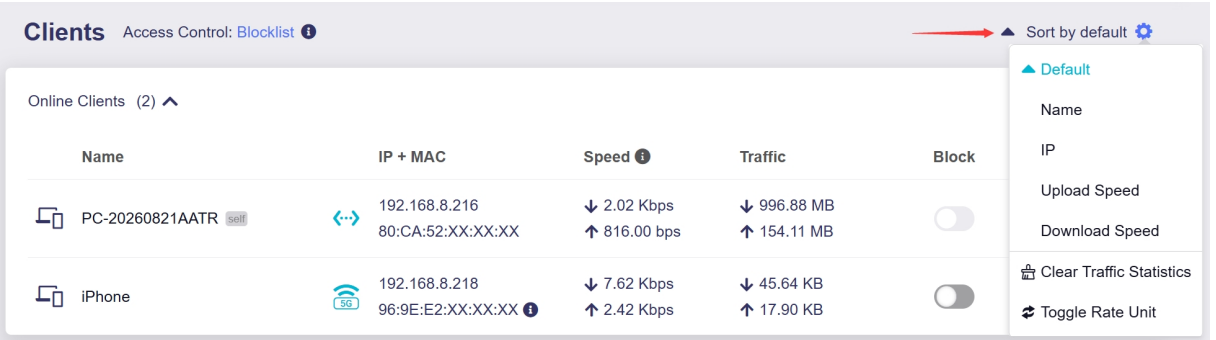


Pour supprimer un client précis, cliquez sur les trois points dans la colonne **Action**, puis sur **Supprimer le client (Remove Client)** dans le menu déroulant.



6.4 Tri

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



L'ordre de tri par défaut est le suivant :

- L'appareil que vous utilisez pour accéder à l'interface d'administration 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.

Outre les règles de tri, le menu déroulant propose les fonctions suivantes :

- **Effacer les statistiques de trafic (Clear Traffic Statistics)** : efface en un clic les statistiques de trafic de tous les clients en ligne. Les valeurs de la colonne Trafic sont remises à zéro, puis le comptage reprend.



- **Changer l'unité de débit (Toggle Rate Unit)** : alterne l'unité de la colonne Débit entre **Ko/s (KB/s)** et **kbit/s (Kbps)**.

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

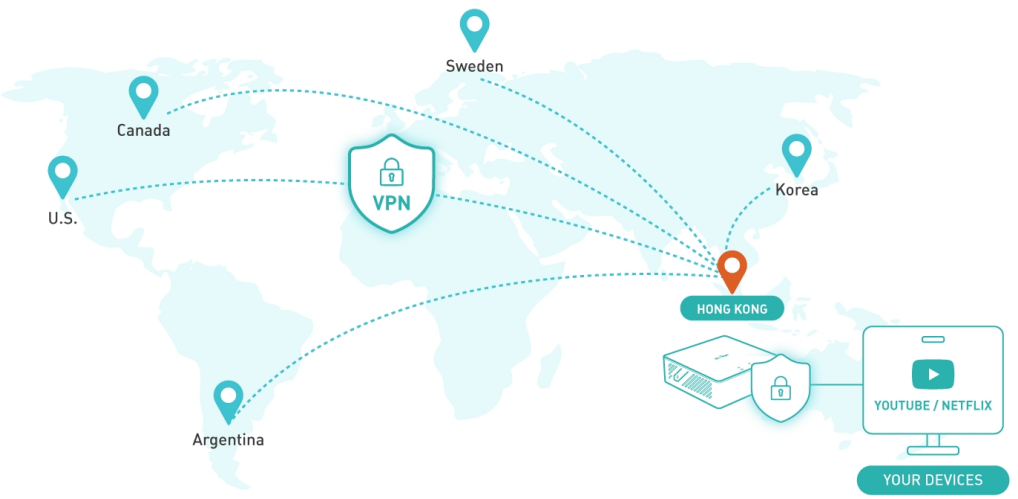
1. **Protection des données personnelles**

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



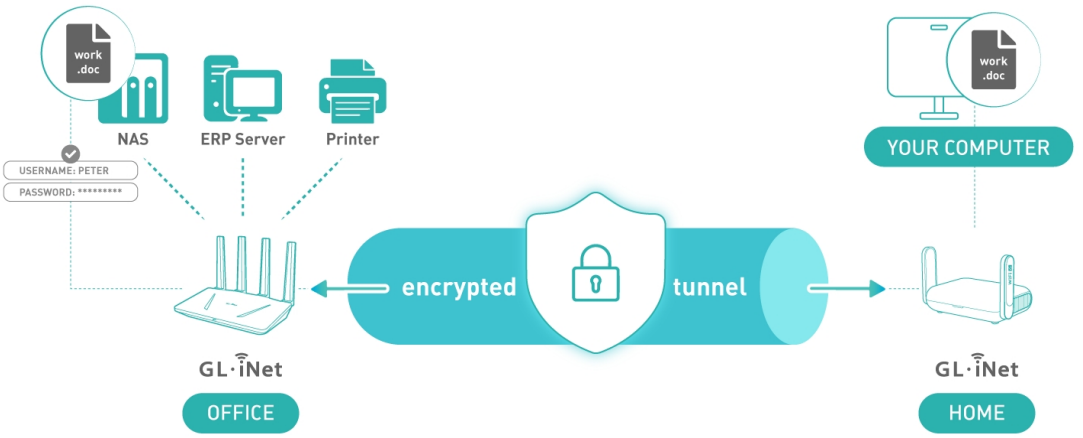
2. **Accès aux contenus depuis le monde entier**

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



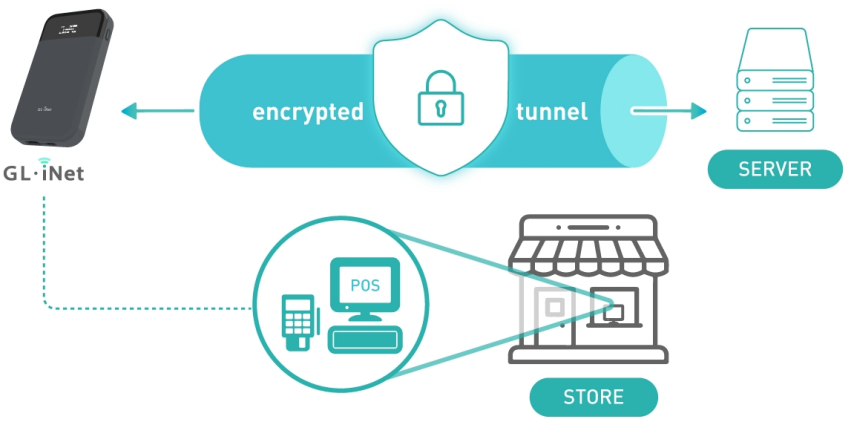
3. **Sécurité des données des petites entreprises**

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



4. **Sécurisation des paiements**

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



Chapitre 8

Tableau de bord VPN

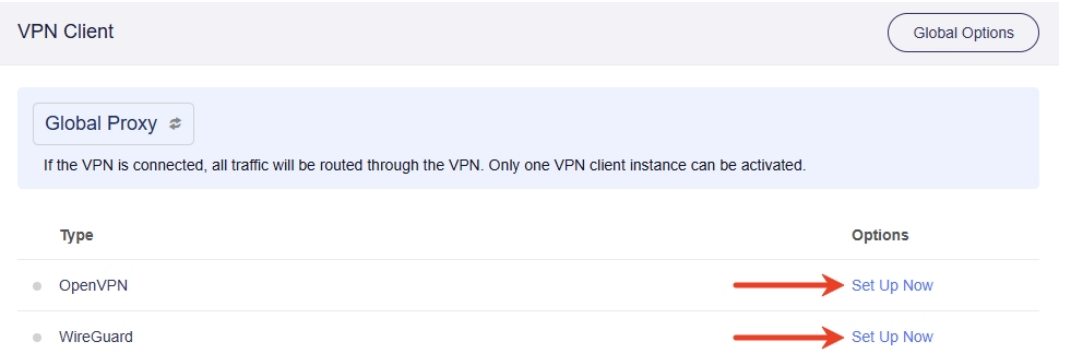
Ce chapitre explique comment gérer les connexions VPN depuis l’interface d’administration Web.

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

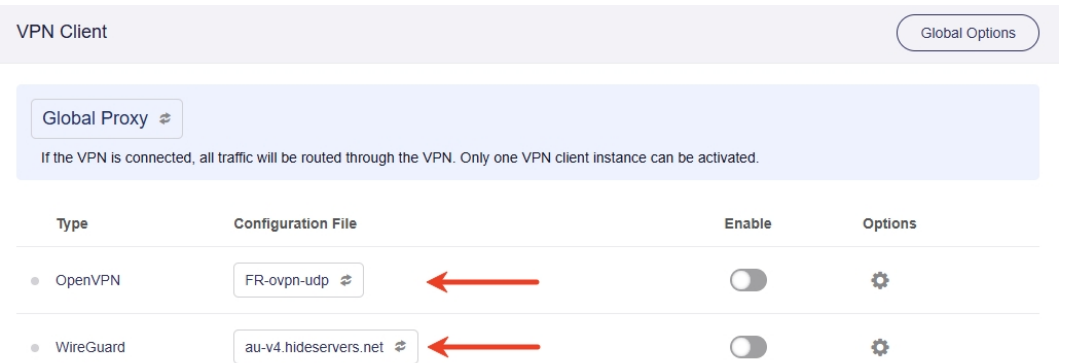
Lorsque le routeur fonctionne comme client VPN actif, le tableau de bord VPN affiche les informations de connexion : adresse du serveur, statistiques du trafic, adresse IP virtuelle du client et journal de connexion. Il permet également de configurer des paramètres avancés tels que Bloquer le trafic hors VPN (Block non-VPN traffic), Autoriser l'accès au WAN (Allow Access WAN) et Services GL.iNet via le VPN (Services from GL.iNet Use VPN).

8.1 Client VPN

Lorsque vous ouvrez le **Tableau de bord VPN (VPN Dashboard)** pour la première fois et qu'aucun fichier de configuration OpenVPN ou WireGuard n'est disponible, la page s'affiche comme ci-dessous. Cliquez sur **Configurer maintenant (Set Up Now)** pour ouvrir la page **Client OpenVPN (OpenVPN Client)** ou **Client WireGuard (WireGuard Client)** et y importer vos fichiers de configuration VPN.

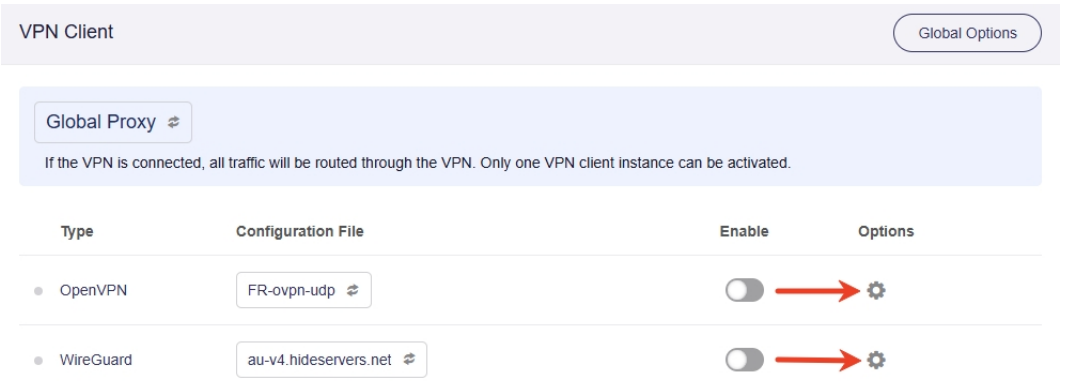


Après l'importation, votre configuration apparaît dans la colonne **Fichier de configuration (Configuration File)**. Si vous avez importé plusieurs fichiers de configuration, cliquez sur le champ pour passer de l'un à l'autre.

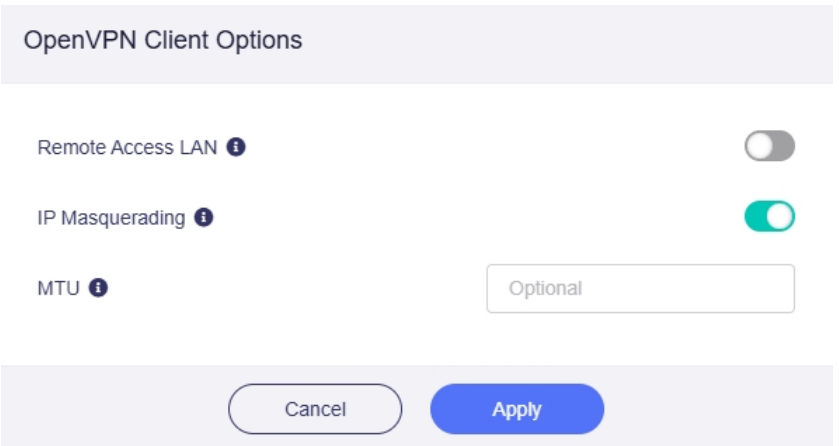


8.1.1 Options du client

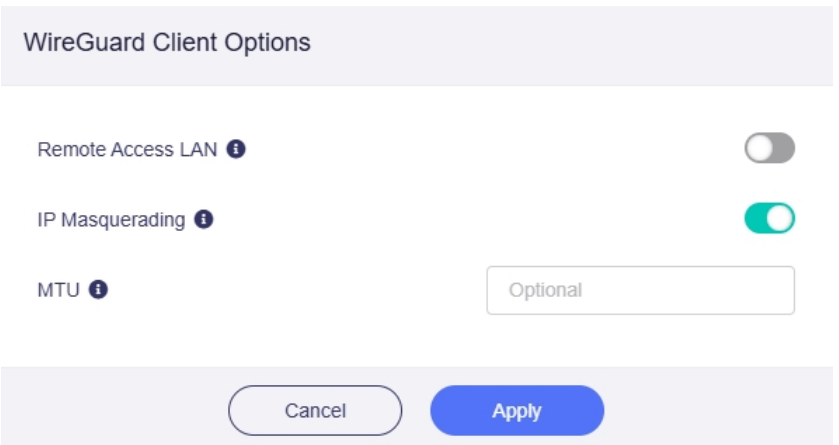
Cliquez sur l’engrenage à droite pour ouvrir les options du client OpenVPN ou WireGuard.



Les options du client OpenVPN sont présentées ci-dessous.

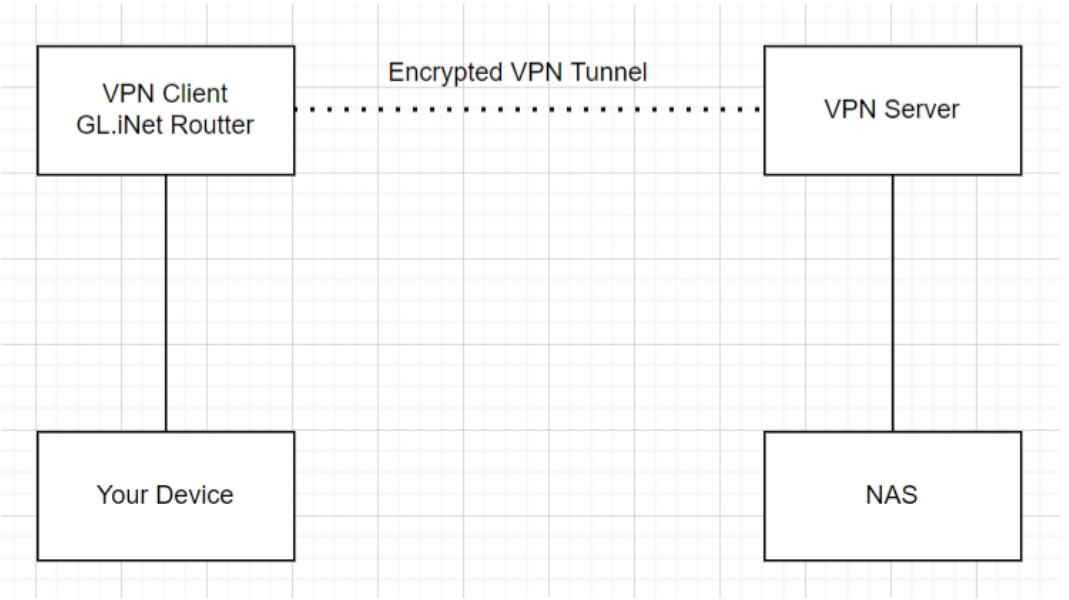


Les options du client WireGuard sont présentées ci-dessous.



- **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.

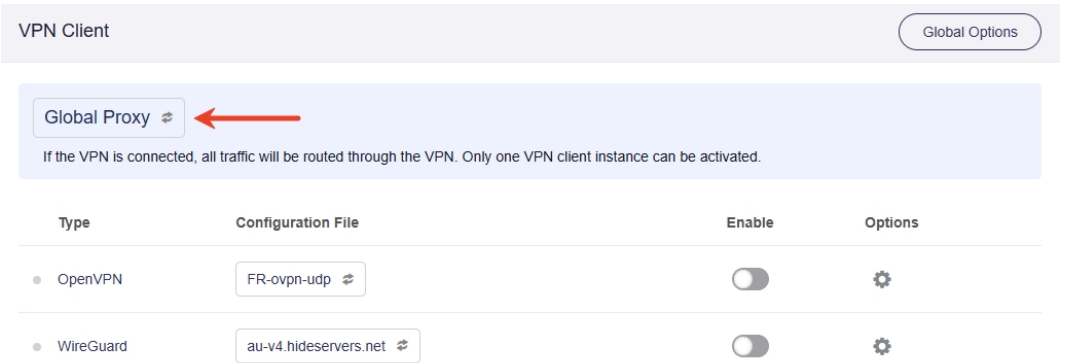
Dans l’exemple du schéma ci-dessous, le routeur GL.iNet fonctionne comme client VPN et se connecte à un serveur VPN via le tunnel VPN. Lorsque cette option est activée, les appareils situés du côté du serveur VPN (par exemple, un NAS) peuvent accéder au routeur GL.iNet et aux appareils de son réseau local. Vous devez pour cela ajouter une règle de routage sur le serveur VPN 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 par règles

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 de proxy sont disponibles : 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'adresse IP de destination**

     Dans ce mode, 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**

     Dans ce mode, seul le trafic de certains appareils du réseau local, identifiés par leur adresse MAC, passe par le VPN. Une seule instance de client VPN peut être activée.

   - **Selon le VLAN**

     Dans ce mode, 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)**

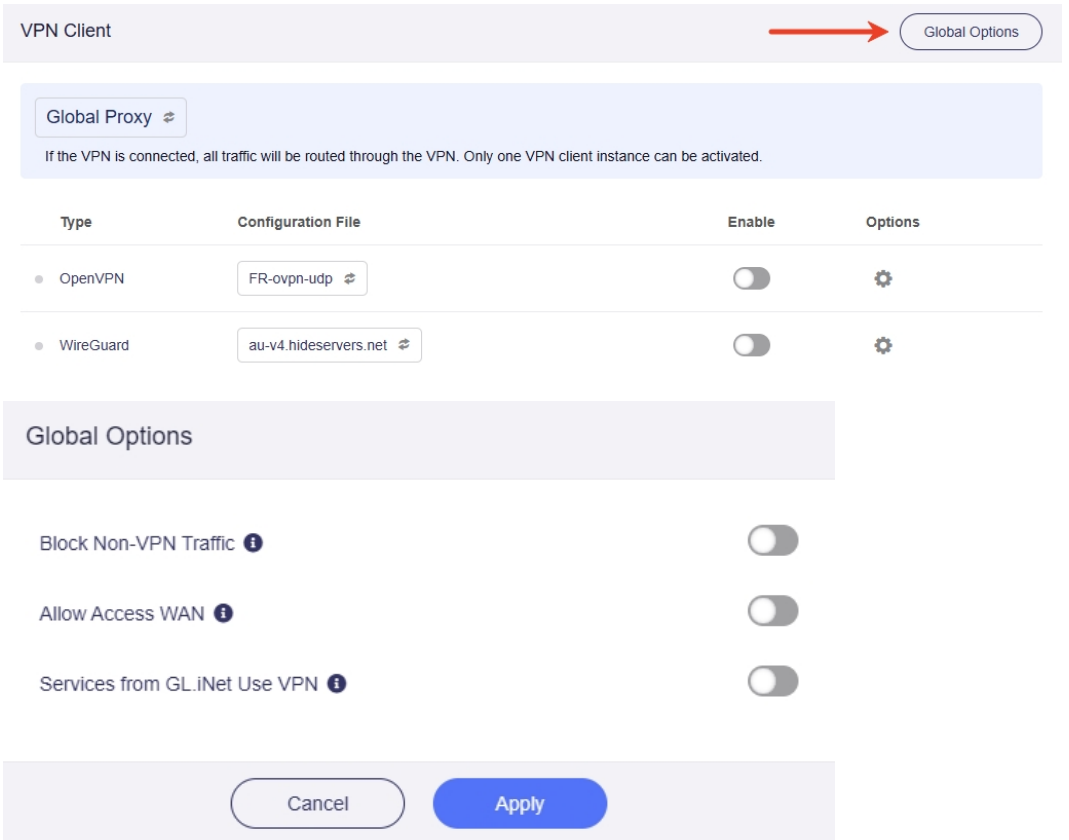
   - **Détection automatique (Auto Detect)**

     Les règles de routage définies dans le fichier de configuration de chaque client VPN ou transmises par le serveur VPN sont utilisées.

- **Personnaliser les règles de routage (Customize Routing Rules)**
  Vous pouvez configurer manuellement les règles de routage de chaque instance de client VPN.

8.1.3 Options globales

Cliquez sur **Options générales (Global Options)** dans l'angle supérieur droit pour configurer les paramètres avancés de votre client VPN.



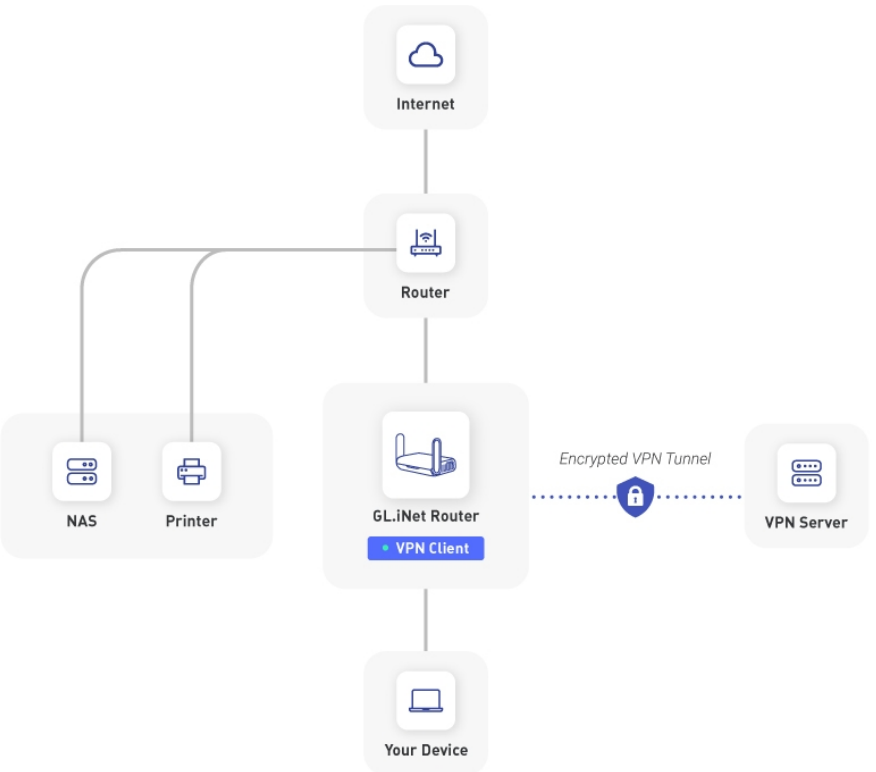
- **Bloquer le trafic hors VPN (Block Non-VPN Traffic)** : lorsque cette option est activée, tout le trafic Internet doit passer exclusivement par le tunnel VPN. Il ne peut pas emprunter d'autres interfaces, telles que la connexion WAN de votre FAI local. Si la connexion VPN est interrompue de manière inattendue, tout le trafic Internet est bloqué afin d'éviter un basculement vers la connexion WAN habituelle. Cela empêche les fuites liées à une défaillance du VPN, à une configuration DNS incorrecte du client ou à d'autres problèmes similaires.

  Cette fonction est également appelée coupe-circuit VPN (VPN Kill Switch). Elle évite l'exposition des données de l'utilisateur sur Internet. Un coupe-circuit classique interrompt automatiquement l'accès à Internet lorsque la connexion VPN échoue. La fonction Bloquer le trafic hors VPN des routeurs GL.iNet offre une protection plus étendue contre les fuites et couvre les situations suivantes :

  a. Fuite DNS

b. Fuite IPv6
c. Fuite WebRTC
d. Interruption de la connexion VPN
e. Applications lancées avant l'établissement du VPN
f. Fuites de trafic propres à certaines applications

- **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.

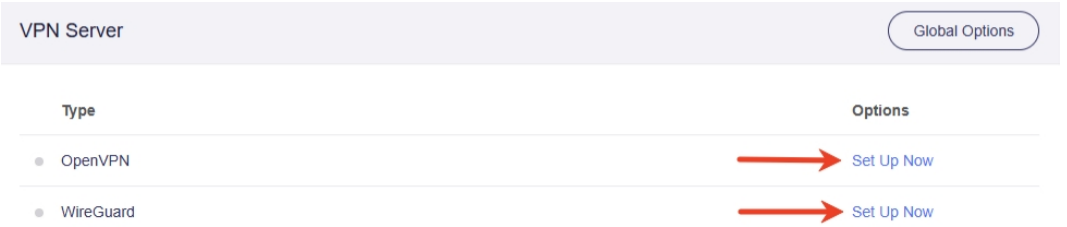
Cette option sert principalement à permettre l'accès des clients aux appareils du sous-réseau amont. Toutefois, le routeur ne peut pas distinguer le trafic de ce sous-réseau du trafic Internet ordinaire. Si les appareils clients accèdent directement à des ressources via des adresses IP publiques, un 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.

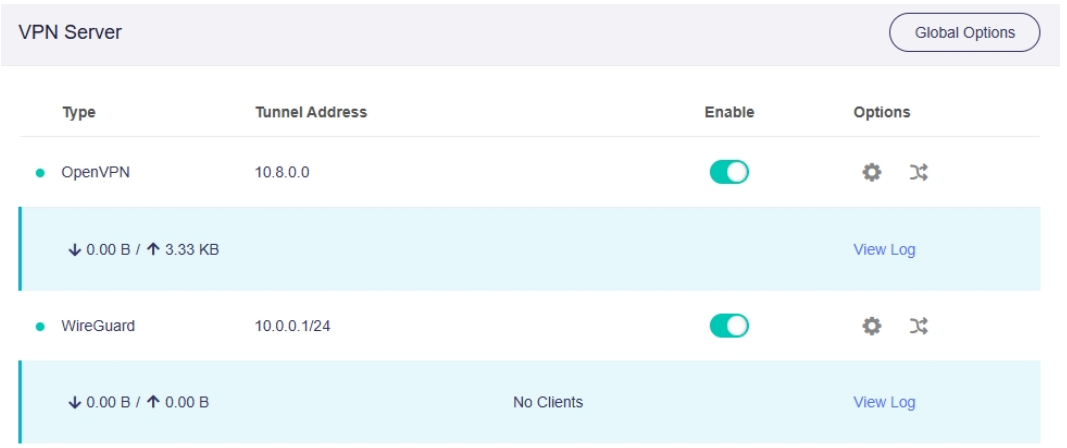
- **Utiliser le VPN pour les services GL.iNet (Services From GL.iNet Use VPN)** : permet aux services GoodCloud, DDNS et rtty de transmettre leurs paquets par les tunnels VPN. Cette option est désactivée par défaut, car ces services ont généralement besoin de l’adresse IP réelle de l’appareil pour fonctionner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

8.2 Serveur VPN

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

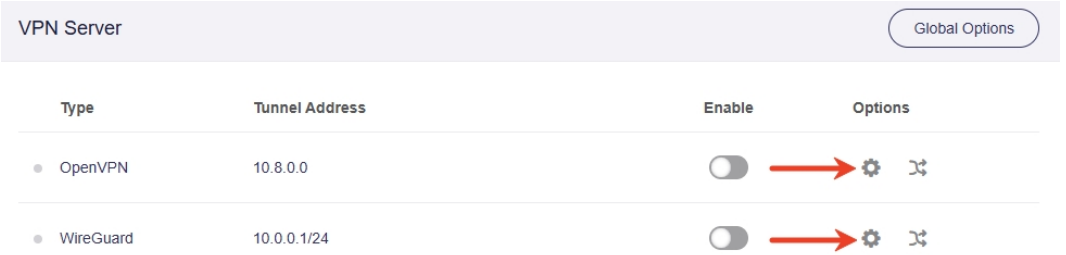


Une fois le serveur OpenVPN ou WireGuard activé, la page affiche son état comme ci-dessous.

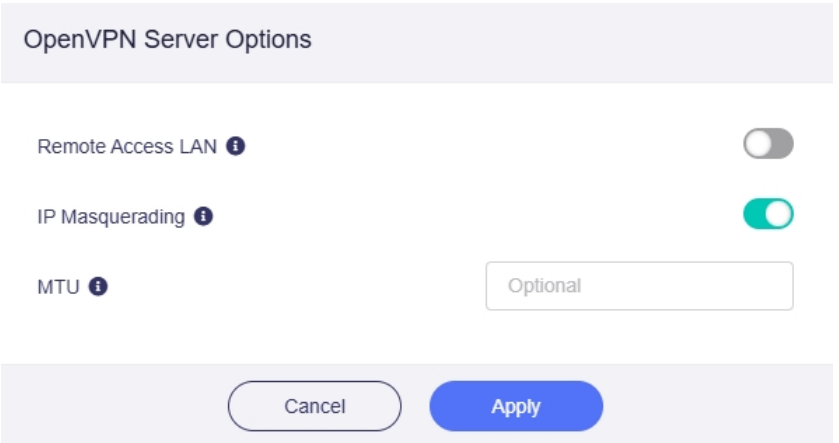


8.2.1 Options du serveur

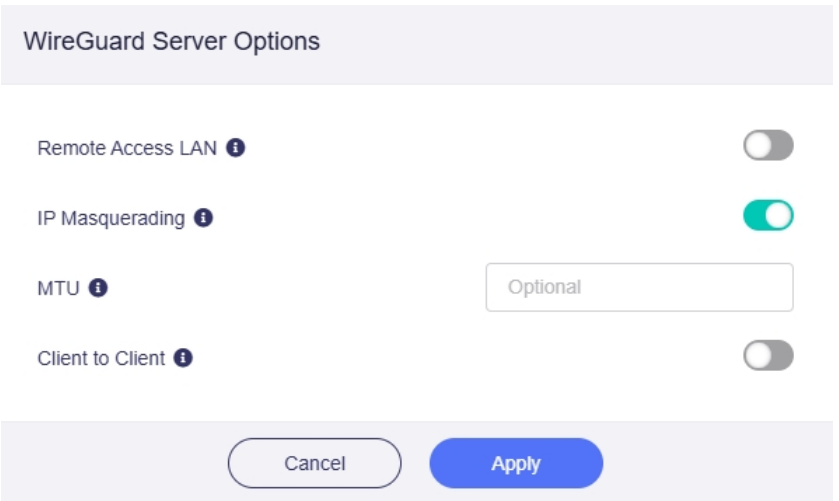
Cliquez sur l'engrenage à droite pour ouvrir les options du serveur OpenVPN ou WireGuard.



Les options du serveur OpenVPN sont présentées ci-dessous.



Les options du serveur WireGuard sont présentées ci-dessous.



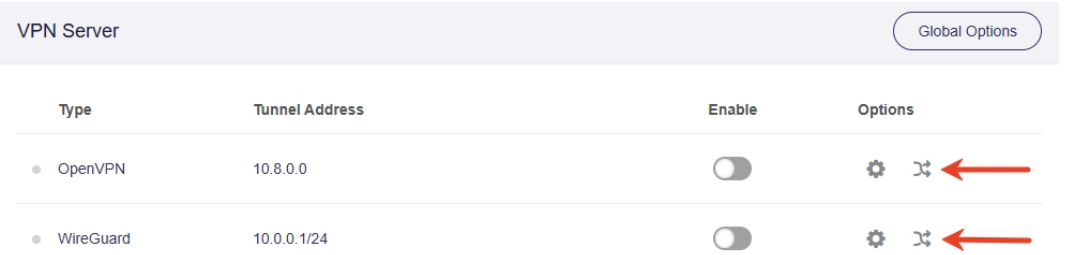
- **Accès distant au LAN (Remote Access LAN)** : permet d'accéder aux ressources du sous-réseau LAN du serveur par le tunnel VPN.
- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l'IP du tunnel VPN du routeur. Ne désactivez cette option que

pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.

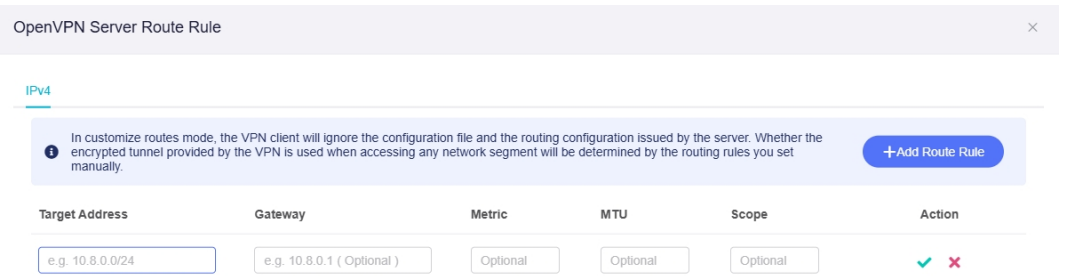
- **MTU** : unité de transmission maximale (Maximum Transmission Unit). La valeur choisie pour le tunnel remplace les paramètres MTU du fichier de configuration.
- **Communication entre clients (Client to Client)** : lorsque cette option est activée, les clients VPN connectés à ce serveur peuvent communiquer entre eux à l'aide de leurs adresses IP de tunnel VPN. Pour leur permettre d'accéder aussi aux sous-réseaux LAN des autres clients, vous devez ajouter des règles de routage sur le serveur VPN pour annoncer ces sous-réseaux distants.

8.2.2 Règles de routage du serveur

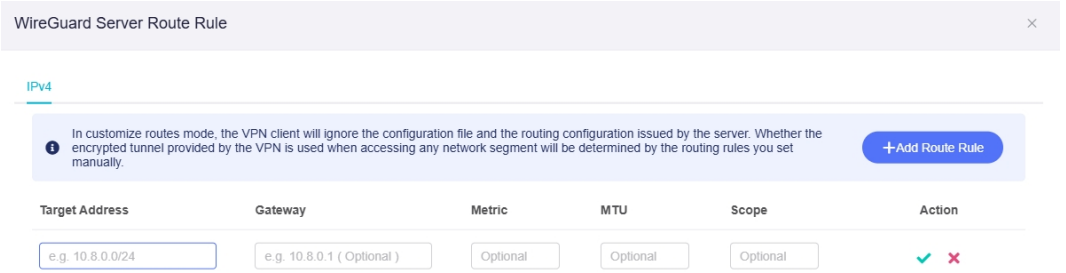
Cliquez sur l'icône de routage à droite pour personnaliser les règles de routage OpenVPN ou WireGuard selon vos besoins.



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.



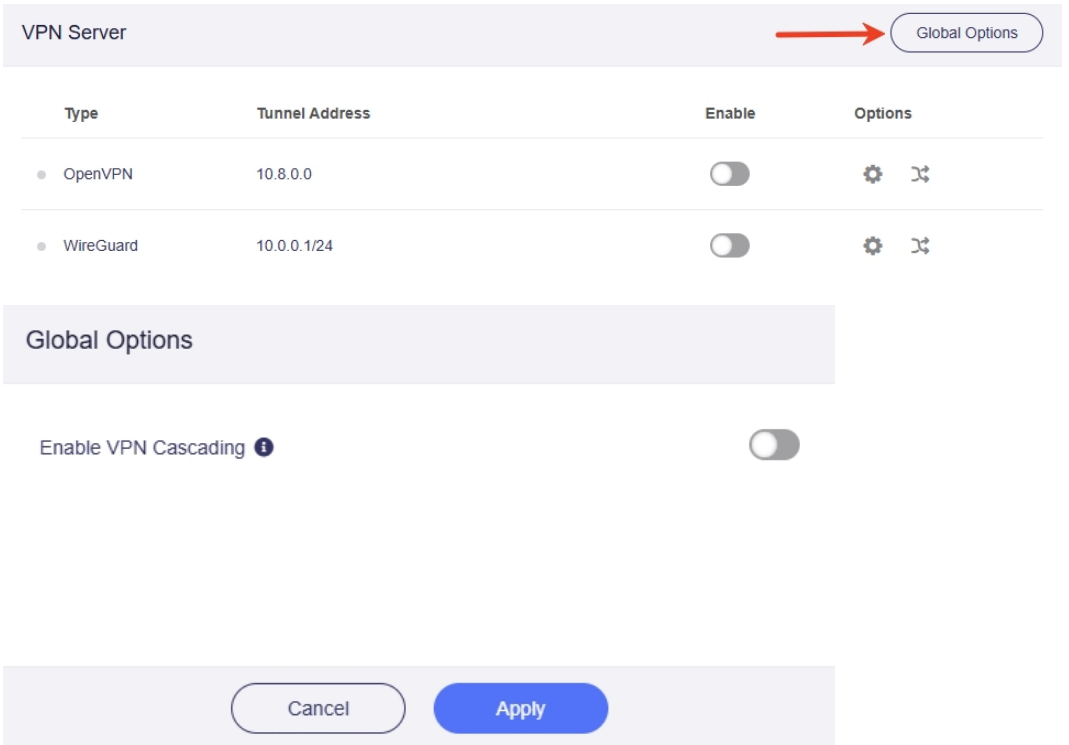
Les règles de routage du serveur WireGuard sont présentées ci-dessous. Cliquez sur **Ajouter une règle de routage (Add Route Rule)**, renseignez l'**adresse cible (Target Address)** et la **passerelle (Gateway)**, puis cliquez sur la coche verte pour appliquer la règle.



Remarque : en mode de routage personnalisé, le client VPN ignore le fichier de configuration et la configuration de routage transmise par le serveur. L'utilisation du tunnel VPN chiffré pour accéder à un segment réseau dépend alors des règles de routage que vous définissez manuellement.

8.2.3 Options globales

Cliquez sur **Options générales (Global Options)** dans l'angle supérieur droit pour configurer les paramètres avancés de votre serveur VPN.



Si la **cascade VPN (VPN Cascading)** est activée et que ce routeur joue simultanément le rôle de serveur VPN et de client VPN, le trafic des clients VPN distants connectés à son serveur VPN transite par le tunnel VPN amont qu'il utilise en tant que client VPN. En savoir plus sur la cascade VPN.

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 :

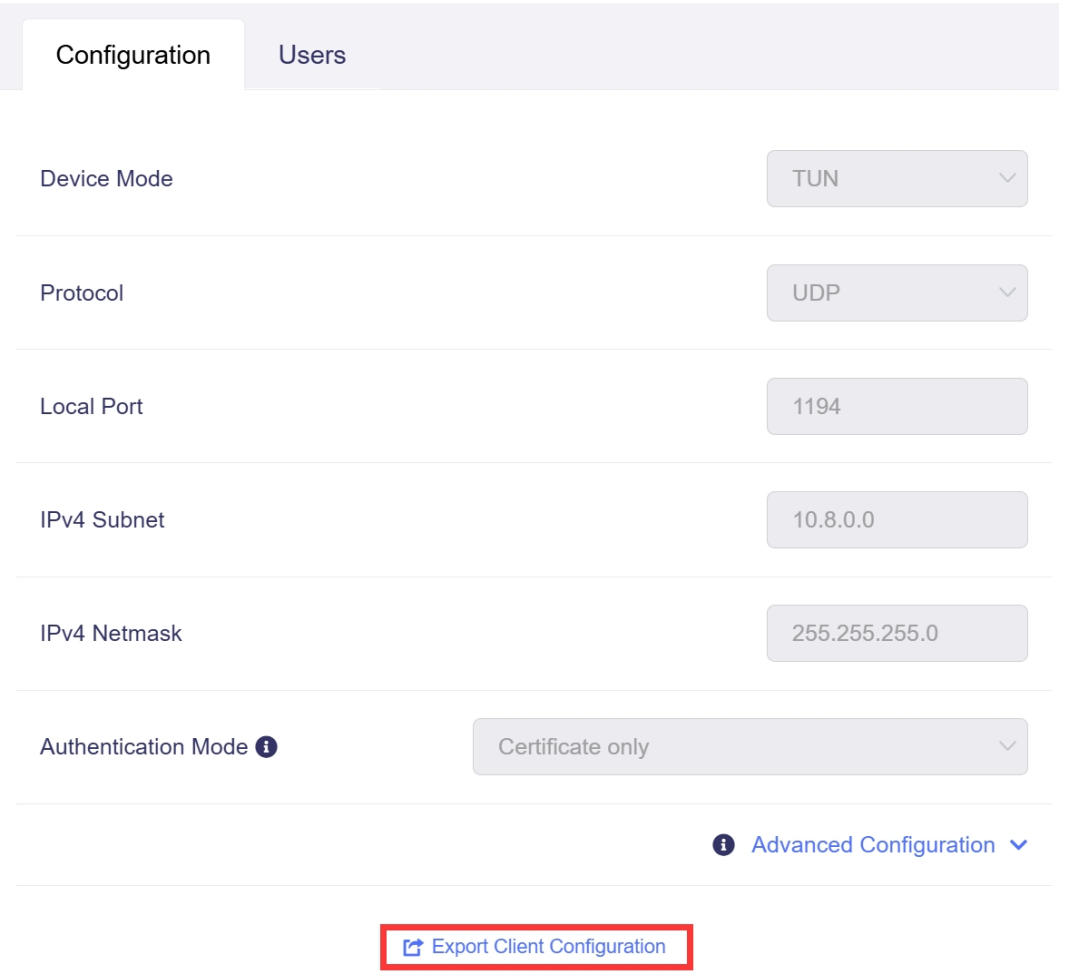
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.

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

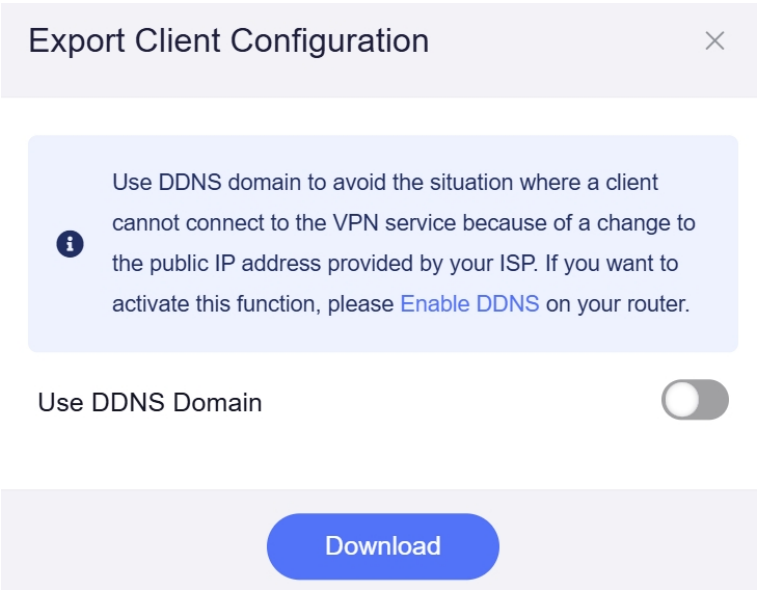
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur OpenVPN (OpenVPN Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.
   La configuration par défaut convient à la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

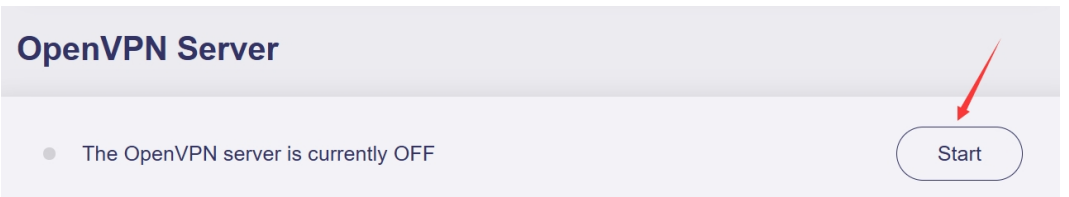
3. Exportez la configuration client.
   Cliquez sur **Exporter la configuration client (Export Client Configuration)** en bas de l’onglet Configuration, après avoir appliqué vos modifications éventuelles. Dans la fenêtre qui s’affiche, cliquez sur **Télécharger (Download)** pour exporter la configuration.



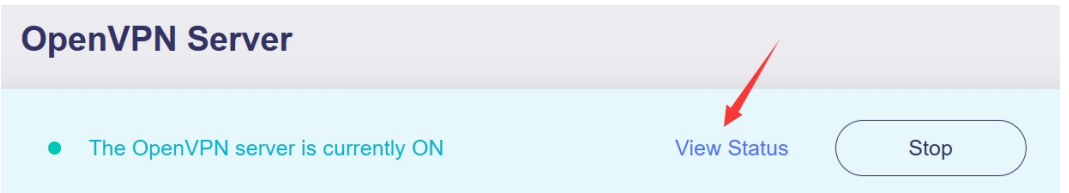
Conseil : si votre adresse IP publique change fréquemment, accédez à **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le nom de domaine DDNS comme adresse du serveur.

4. Démarrez le serveur OpenVPN.

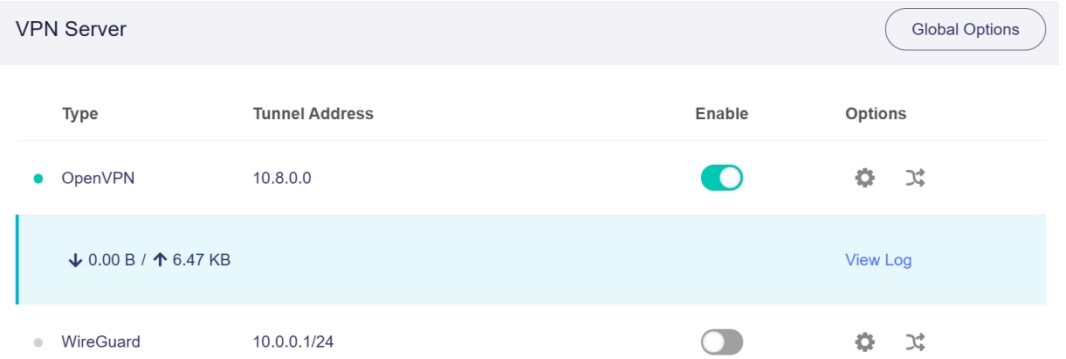
   Sur la page **Serveur OpenVPN (OpenVPN Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



Pour consulter l'état de connexion du serveur, cliquez sur **Afficher l'état (View Status)**.



Vous accédez alors au tableau de bord VPN. Si les statistiques du trafic montant et descendant apparaissent sur cette page, le serveur OpenVPN fonctionne.



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 :

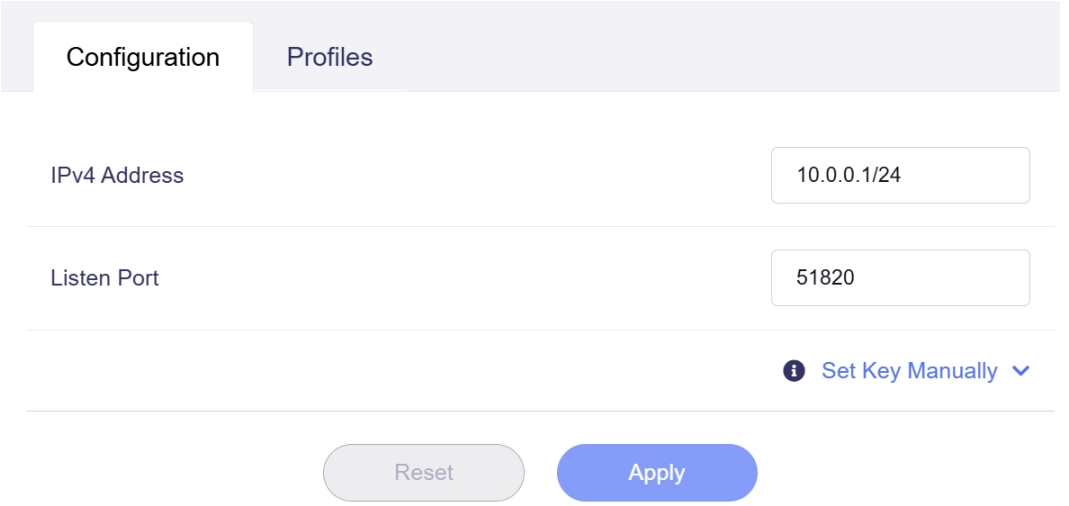
   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.

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

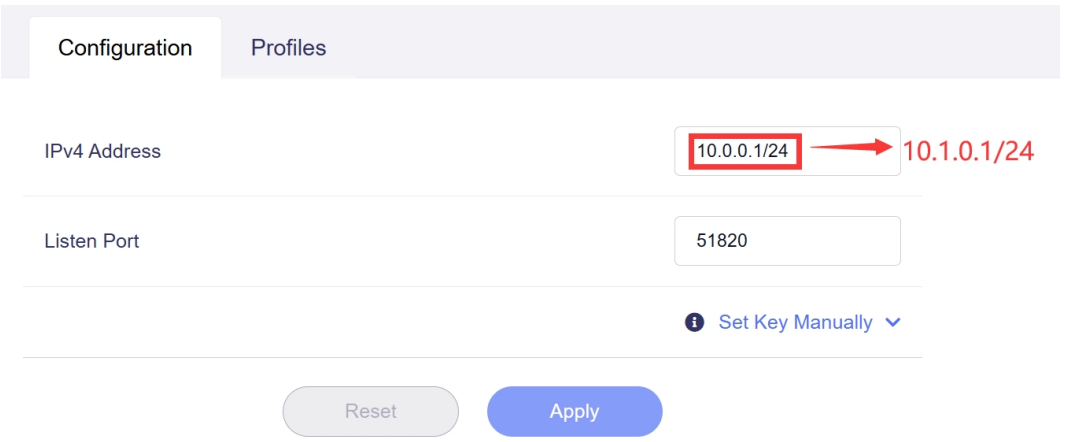
   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n’est nécessaire. Passez à l’étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs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

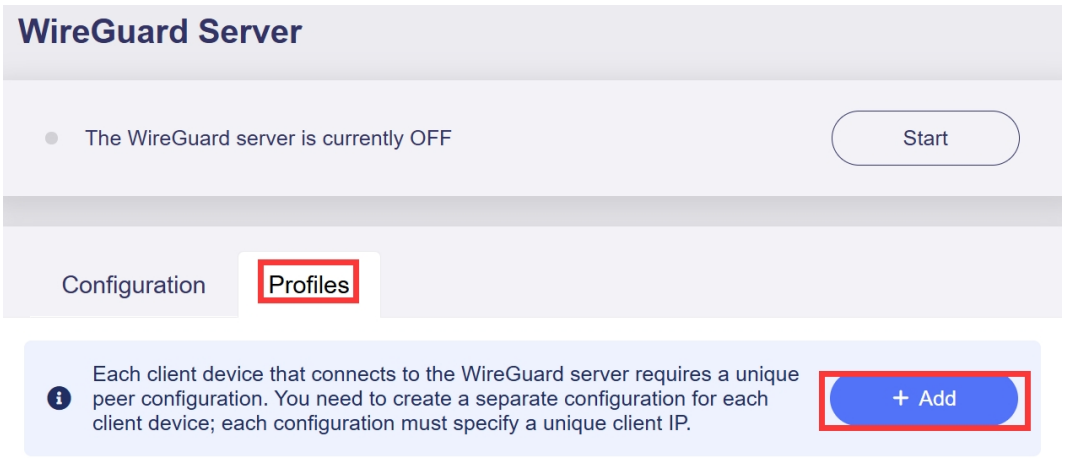
1. Dans l'interface d'administration Web, ouvrez **VPN** > **Serveur WireGuard (WireGuard Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)**, uniquement lors de la configuration initiale du serveur.
2. Appliquez la configuration.
   La configuration par défaut convient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



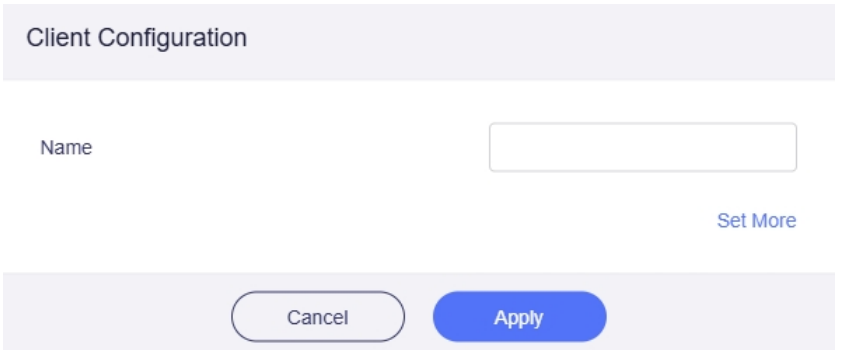
   En cas de conflit, choisissez une autre adresse IPv4, par exemple **10.1.0.1/24**, puis cliquez sur **Appliquer (Apply)**. Conservez la notation CIDR « /24 » pour éviter les problèmes de connexion.



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



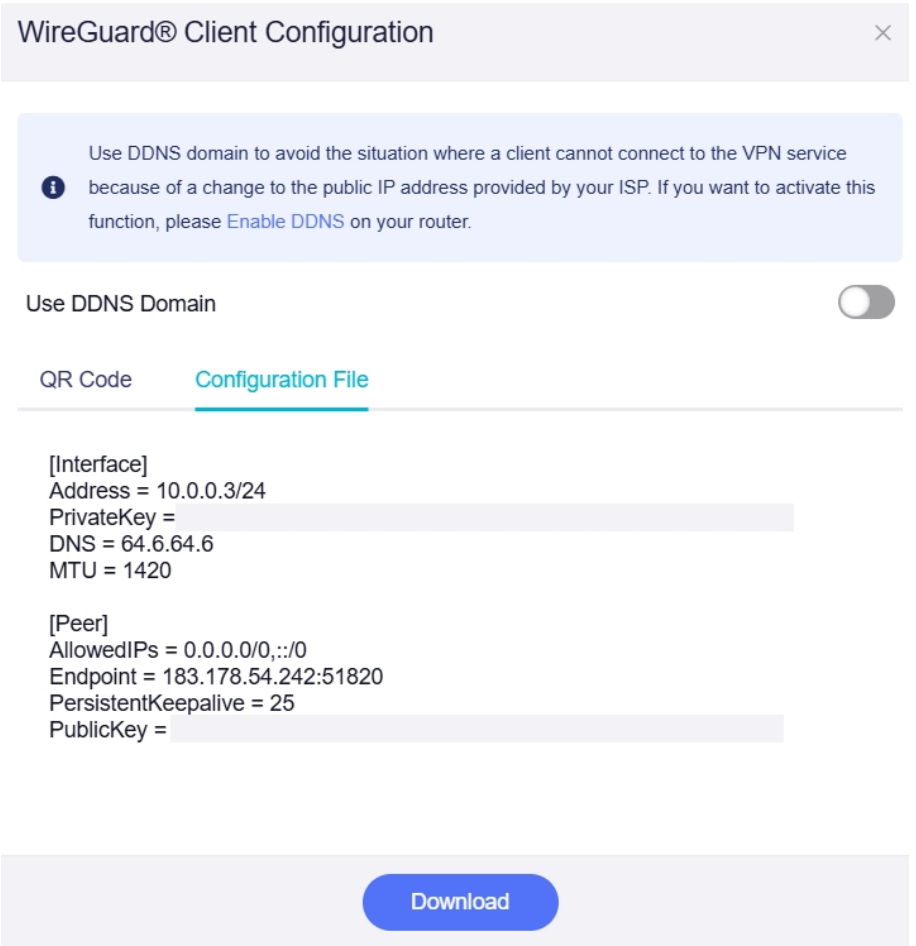
Saisissez un nom explicite et cliquez sur **Appliquer (Apply)** pour continuer.



4. Téléchargez la configuration.

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

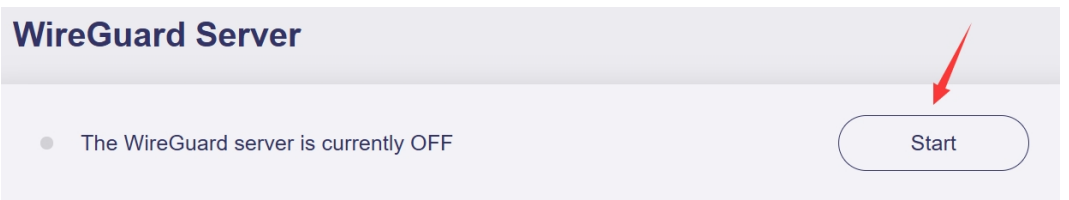
   - **Code QR** : adapté aux appareils disposant de l'application WireGuard, comme les smartphones, tablettes et ordinateurs portables. Ouvrez l'application WireGuard sur l'appareil à configurer comme client et scannez le code QR pour importer la configuration.
   - **Texte brut** : permet de consulter la configuration et de la copier-coller ailleurs pour une configuration manuelle, par exemple dans l'application WireGuard ou sur un routeur GL.iNet.
   - **Fichier .conf** : cliquez sur **Télécharger (Download)** pour enregistrer le fichier .conf sur votre appareil. Vous pouvez ensuite l'importer directement dans l'application WireGuard ou sur un routeur GL.iNet.



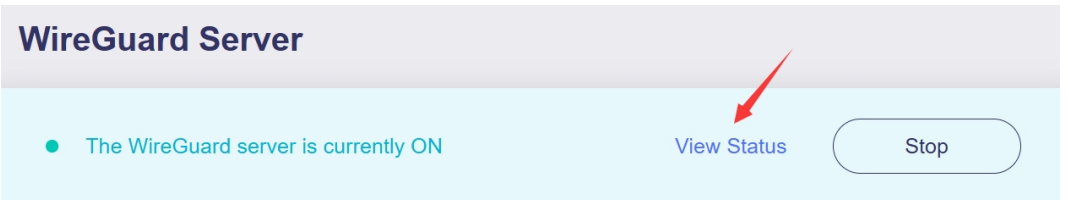
Conseil : si votre adresse IP publique change fréquemment, accédez à **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le nom de domaine DDNS comme adresse du serveur.

5. Démarrez le serveur WireGuard.

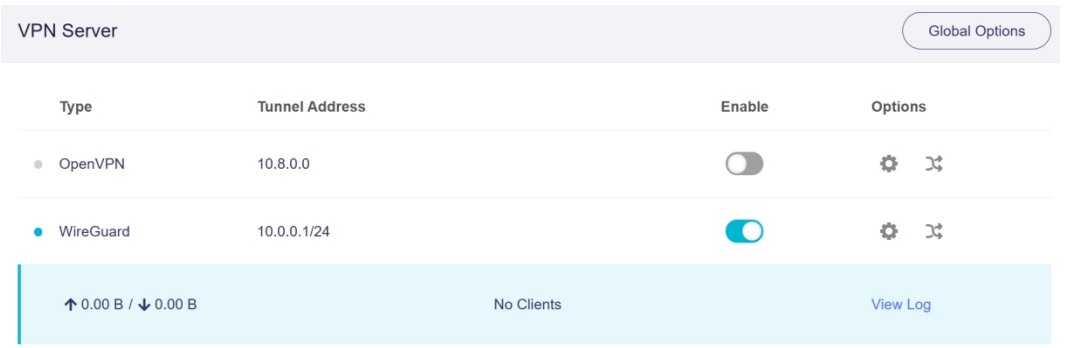
   Sur la page **Serveur WireGuard (WireGuard Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



Pour consulter l'état de connexion du serveur, cliquez sur **Afficher l'état (View Status)**.



Vous accédez alors au tableau de bord VPN. Si les statistiques du trafic montant et descendant apparaissent sur cette page, le serveur OpenVPN fonctionne.



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.

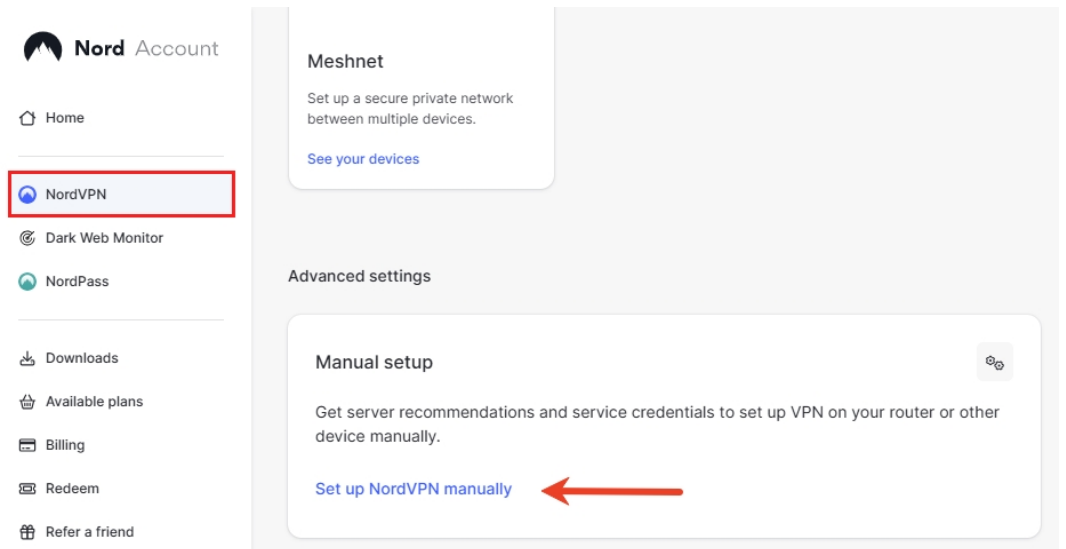
Rendez-vous ensuite sur le site officiel de votre fournisseur VPN pour obtenir les identifiants de service ou le fichier de configuration. Si vous ne savez pas comment obtenir ce fichier, consultez ce lien ou contactez l’assistance du fournisseur.

10.1.2 Configuration de NordVPN

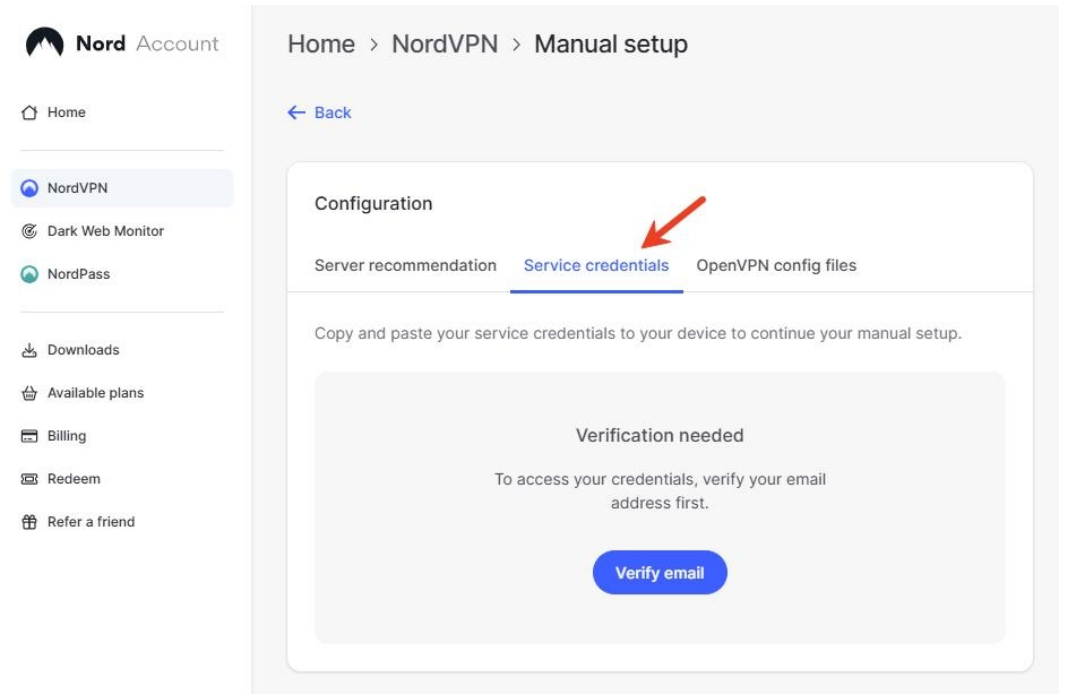
NordVPN est intégré à l’interface d’administration Web GL.iNet. Saisissez les identifiants obtenus dans le tableau de bord NordVPN dans l’interface du routeur ou dans l’application mobile GL.iNet pour récupérer les fichiers de configuration de tous les serveurs NordVPN, sans importation manuelle.

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

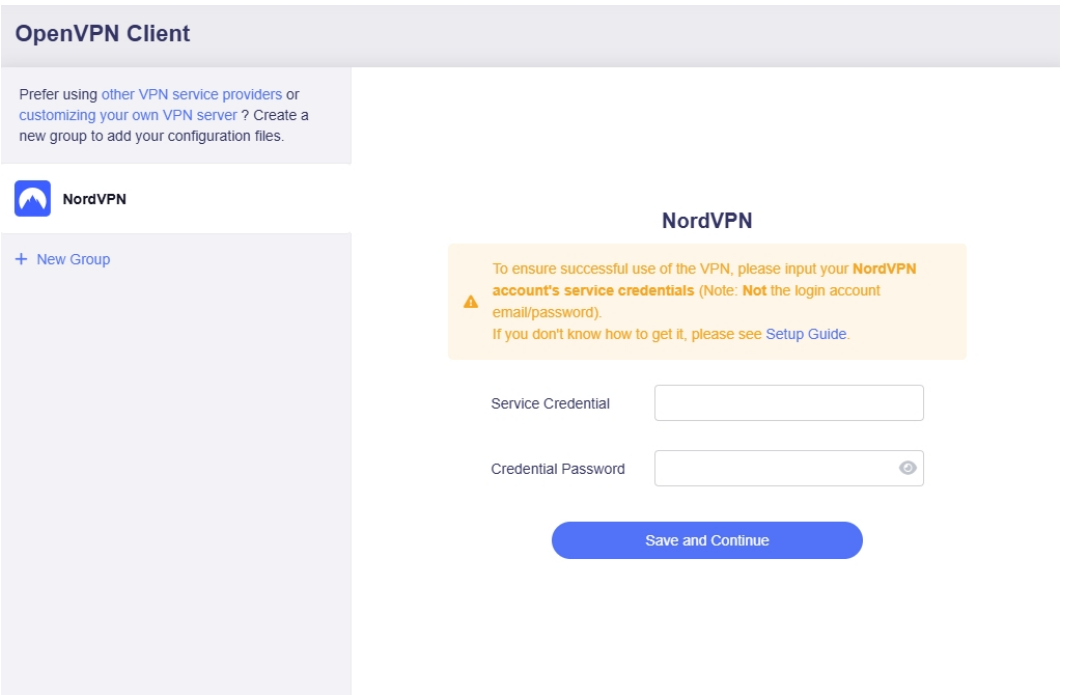
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



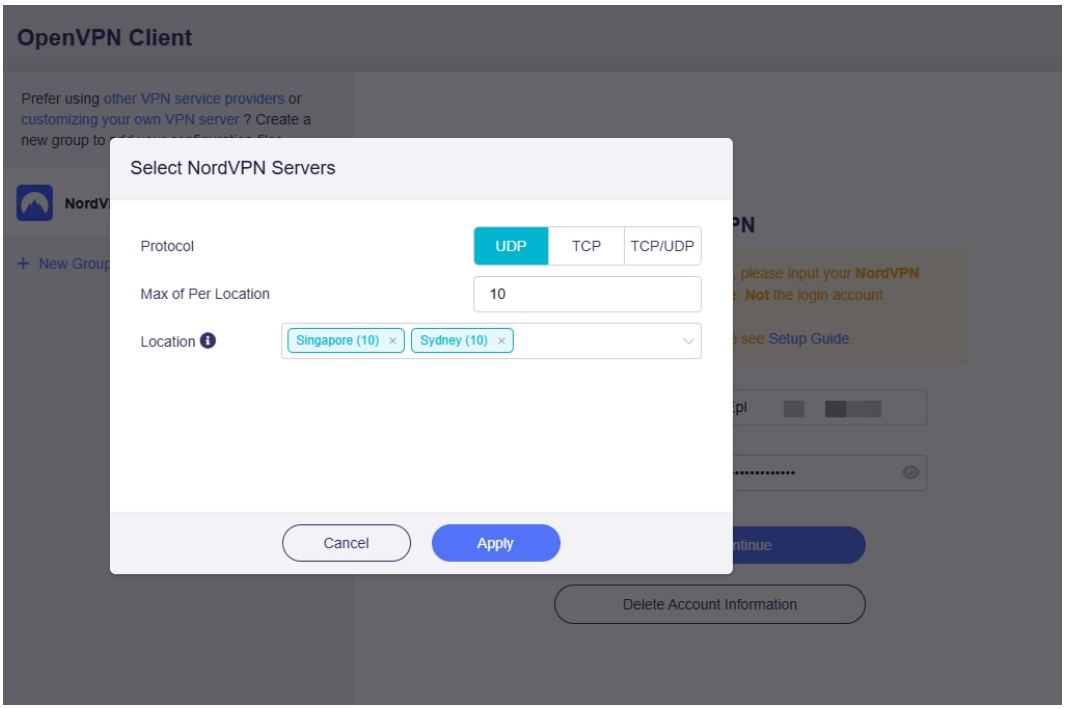
Repérez les **identifiants de service (service credentials)** et copiez-les pour les utiliser ensuite.



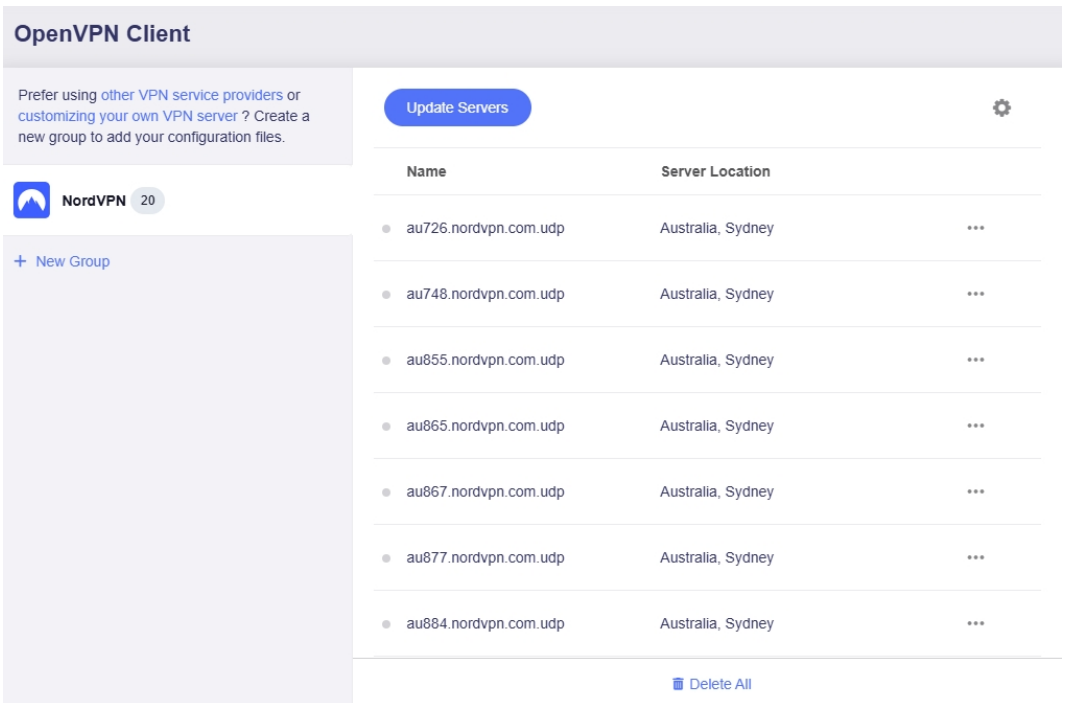
3. Dans l'interface d'administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** > **NordVPN**. Saisissez les identifiants de service, qui ne sont PAS l'adresse e-mail et le mot de passe de connexion au compte, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



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

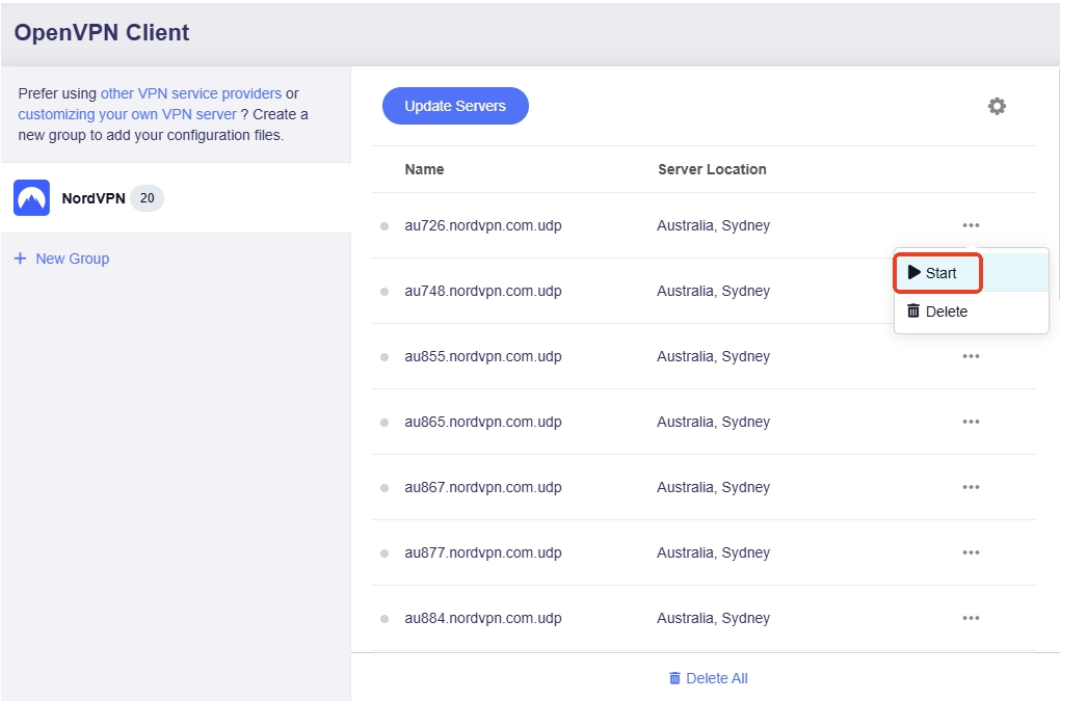


Les fichiers de configuration sont téléchargés.

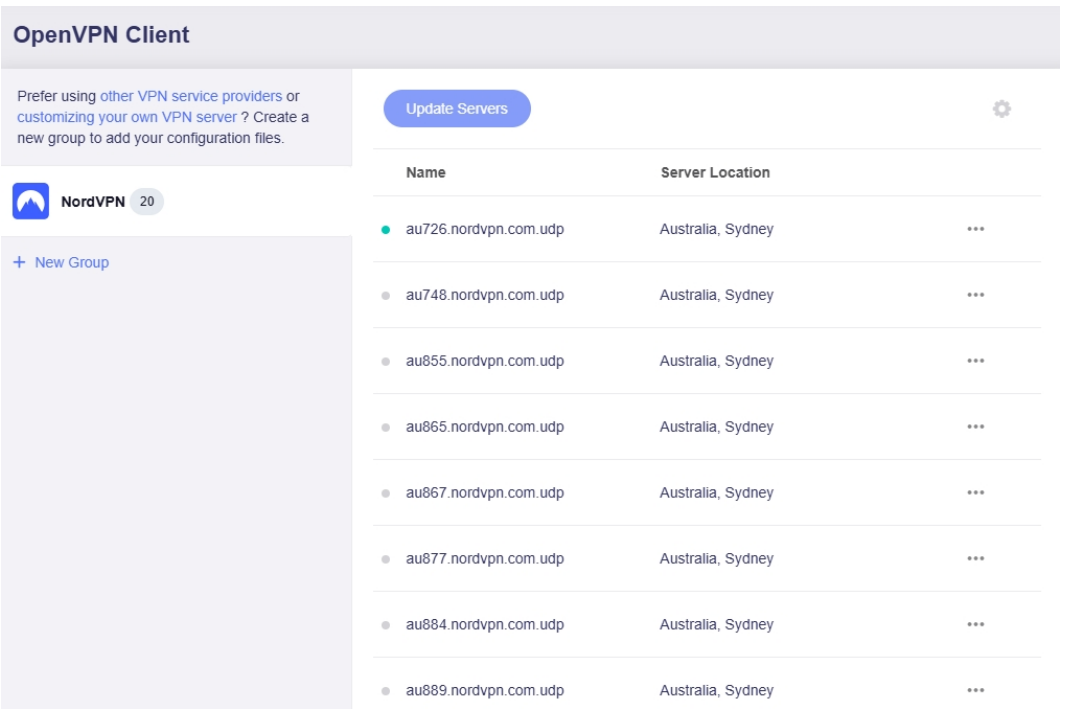


5. Établissez une connexion.

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



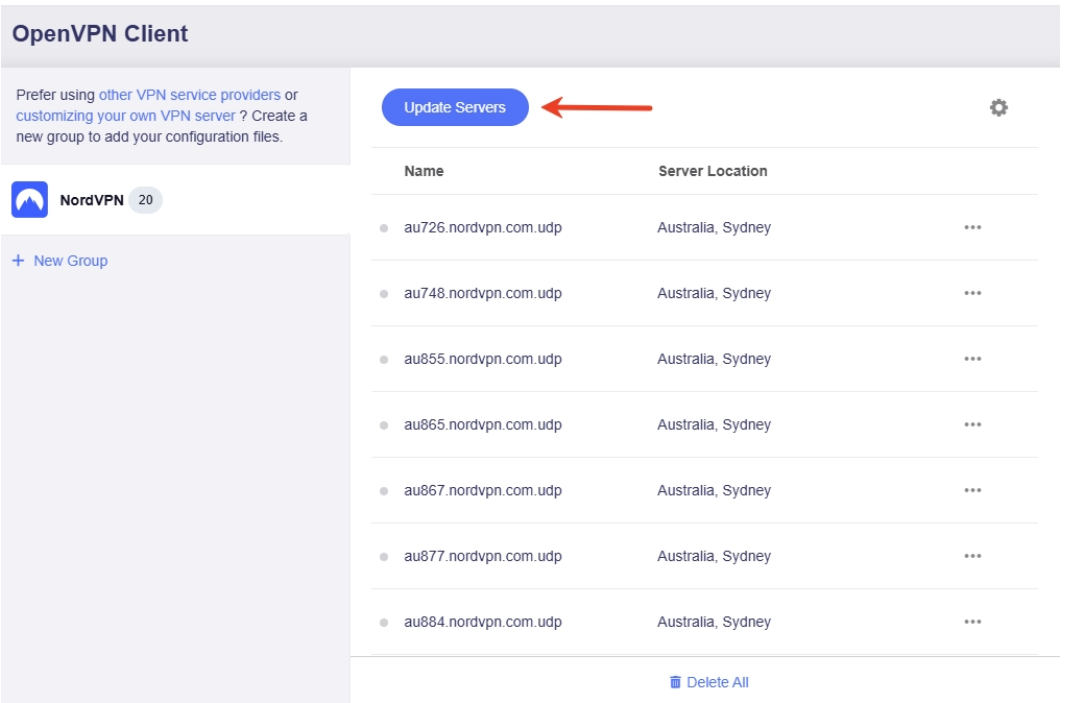
6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



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

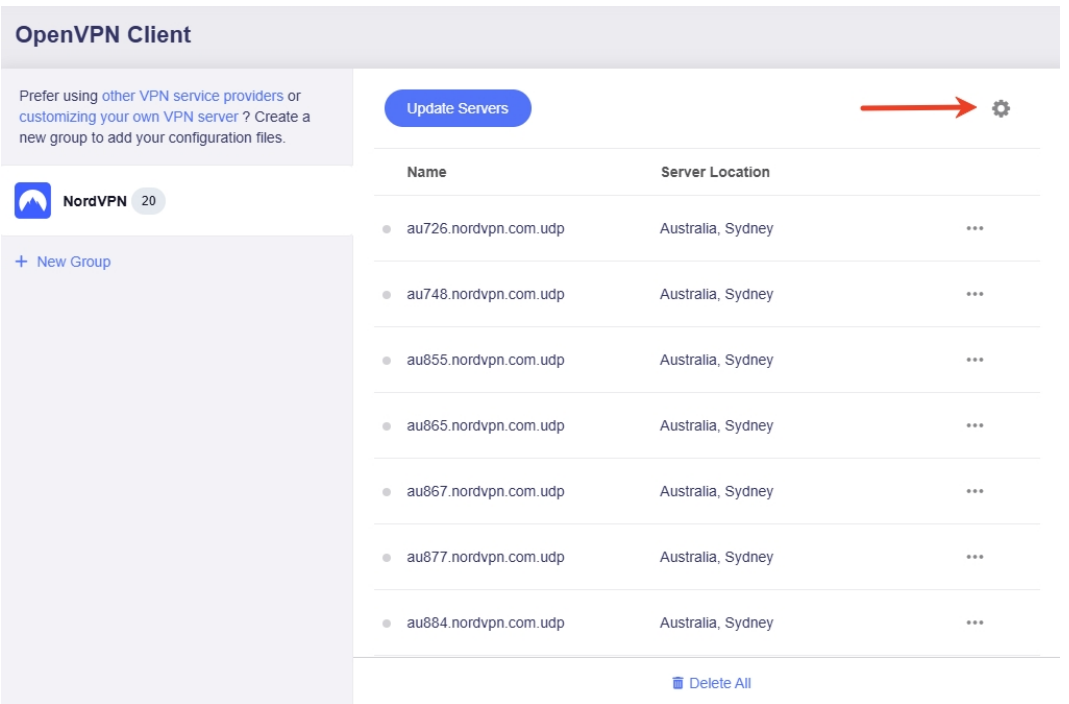
7. Mettez à jour les serveurs.

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.



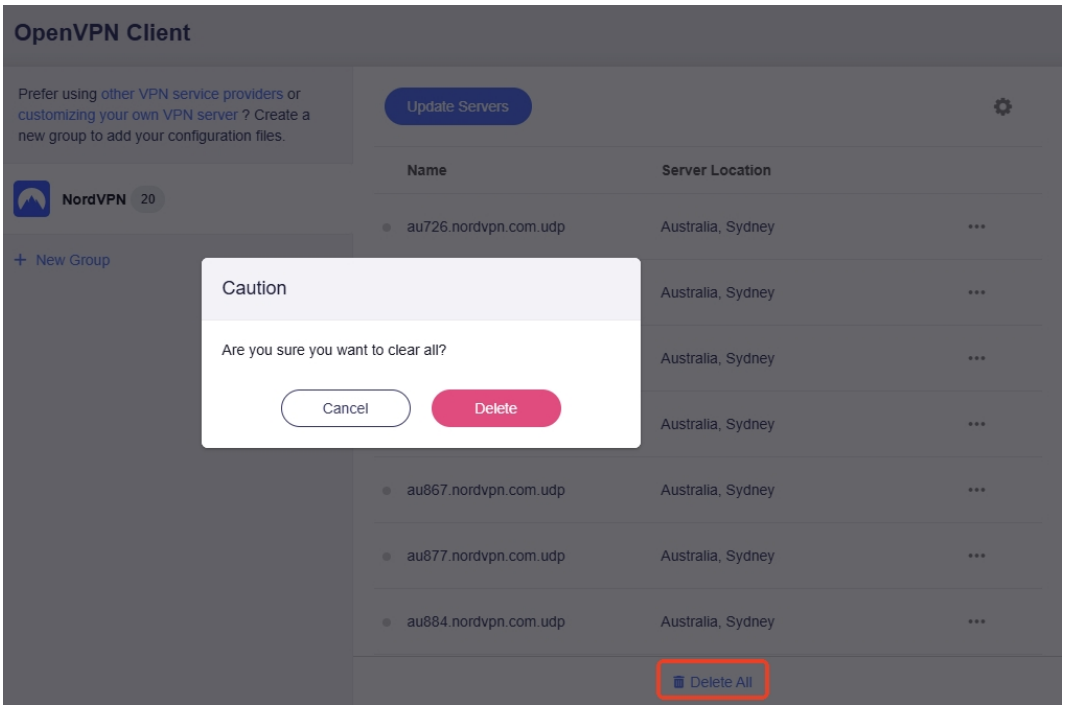
8. Modifiez les identifiants.

   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.

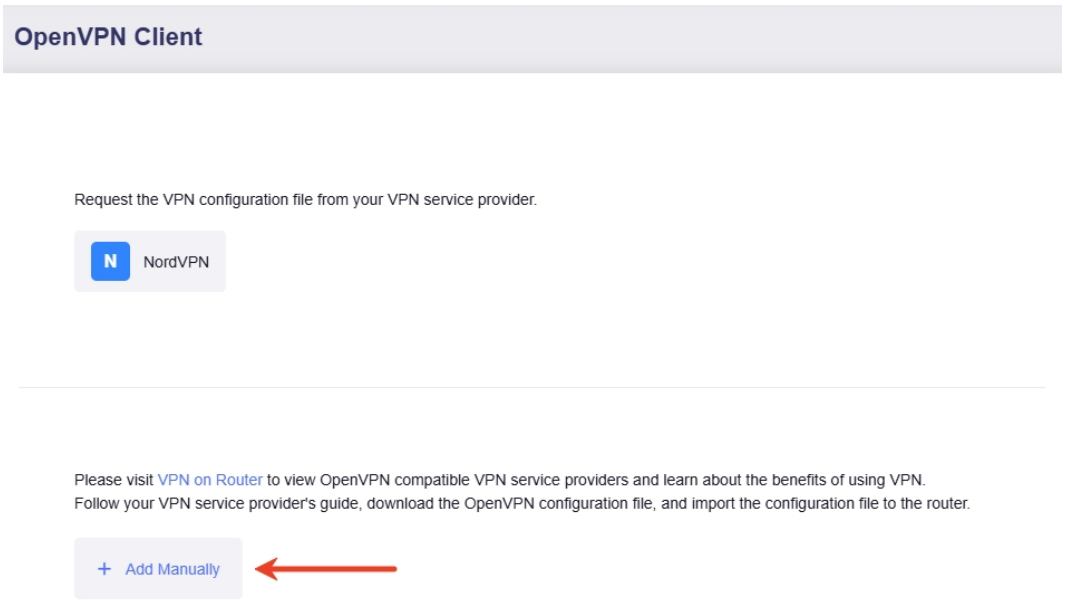


10.1.3 Configuration manuelle d’un client OpenVPN pour un autre fournisseur

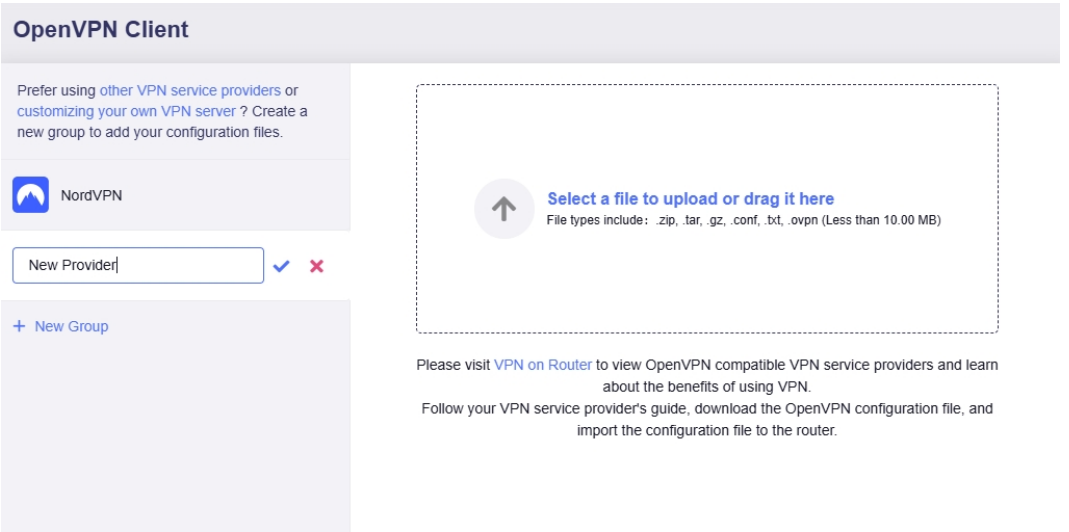
Si votre fournisseur OpenVPN n’est pas intégré à notre interface, récupérez d’abord le fichier de configuration sur son site officiel. Importez-le ensuite sur le routeur pour configurer le client OpenVPN.

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

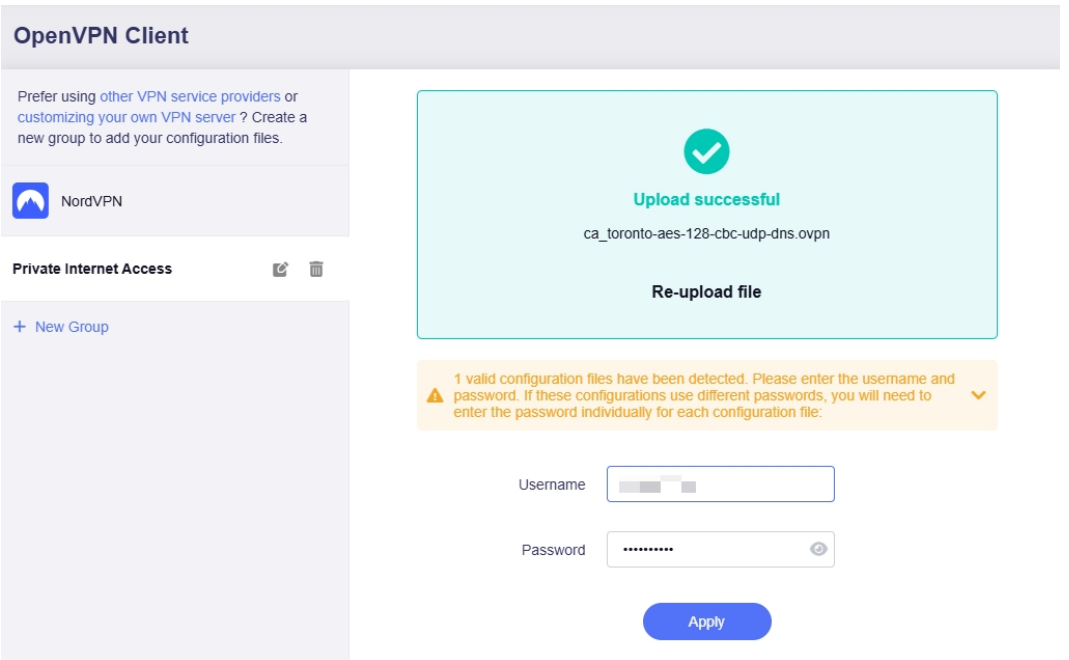
1. Téléchargez un fichier de configuration sur le site officiel de Private Internet Access.
2. Dans l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)**, puis cliquez sur **Ajouter manuellement (Add Manually)**.



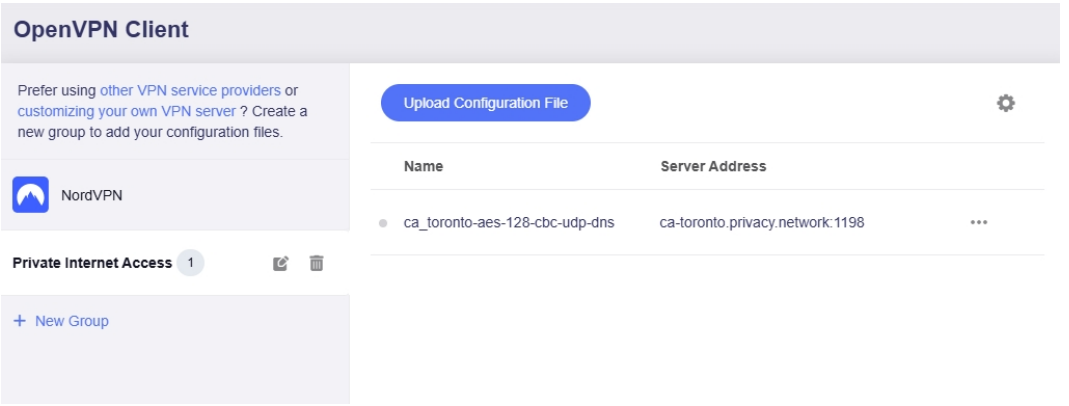
3. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



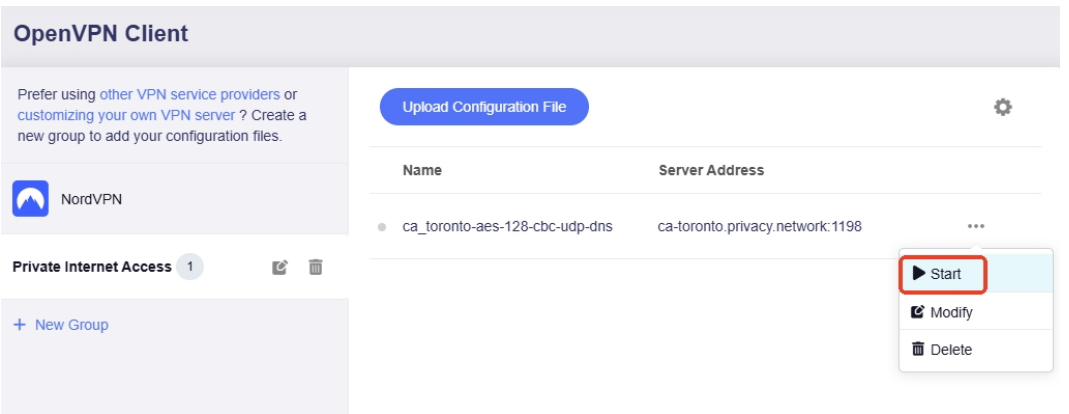
4. Importez votre fichier de configuration OpenVPN. Saisissez les identifiants si nécessaire, puis cliquez sur **Appliquer (Apply)**.



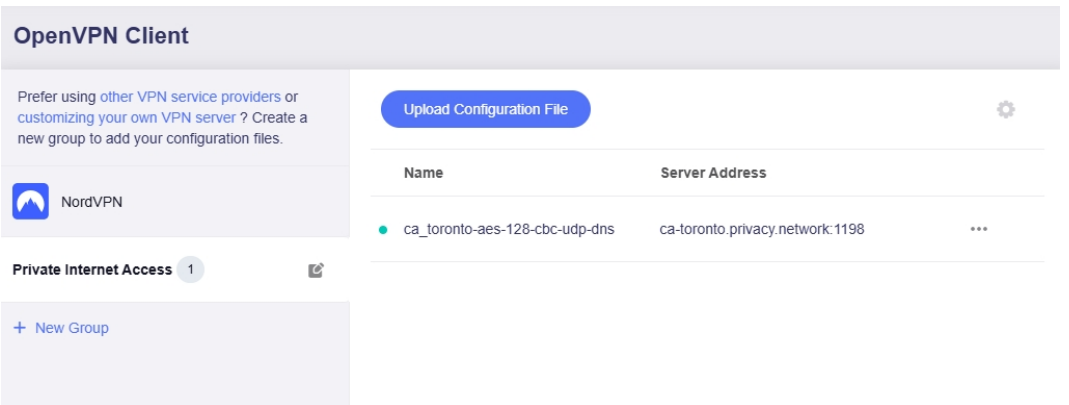
Le fichier importé apparaît dans la liste.



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.

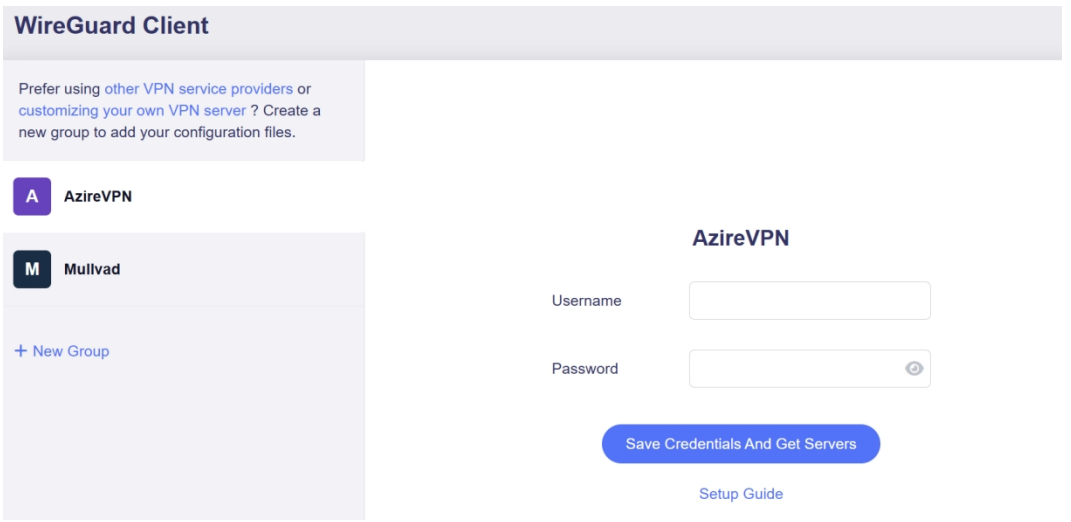
Sélectionnez ensuite votre fournisseur ci-dessous pour accéder directement aux instructions détaillées.

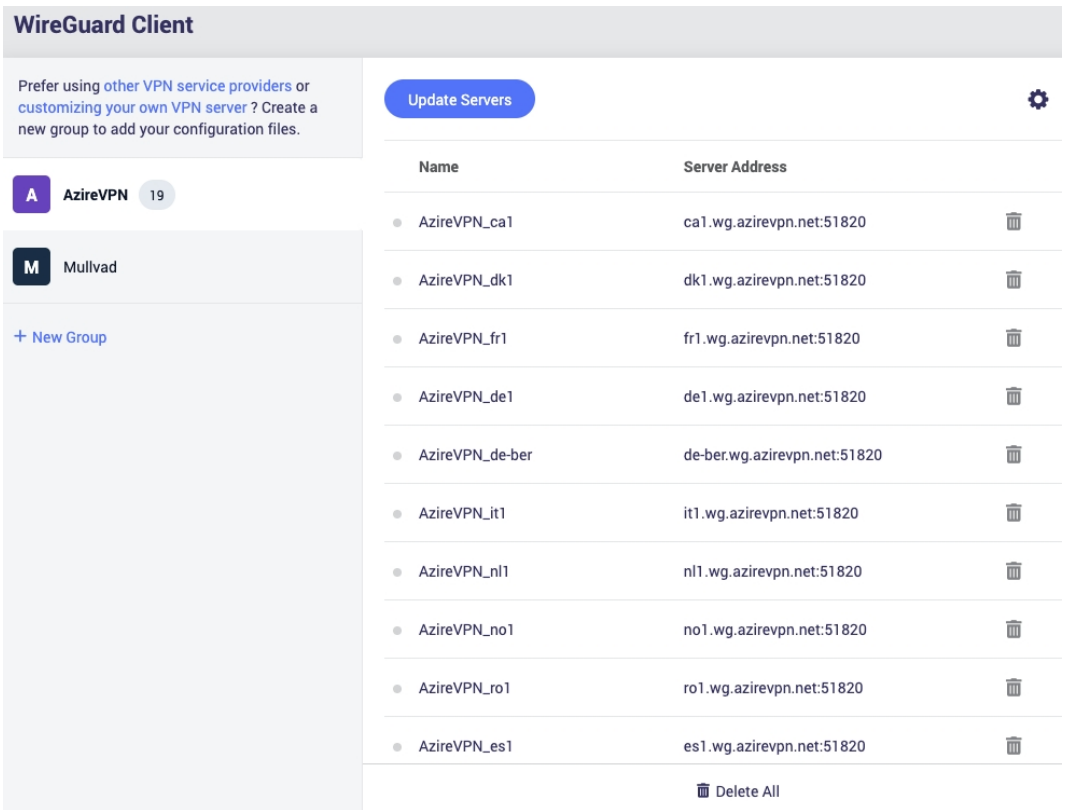
- Configuration d’AzireVPN
- Configuration de Mullvad
- Configuration manuelle d’un client WireGuard pour un autre fournisseur

10.2.2 Configuration d’AzireVPN

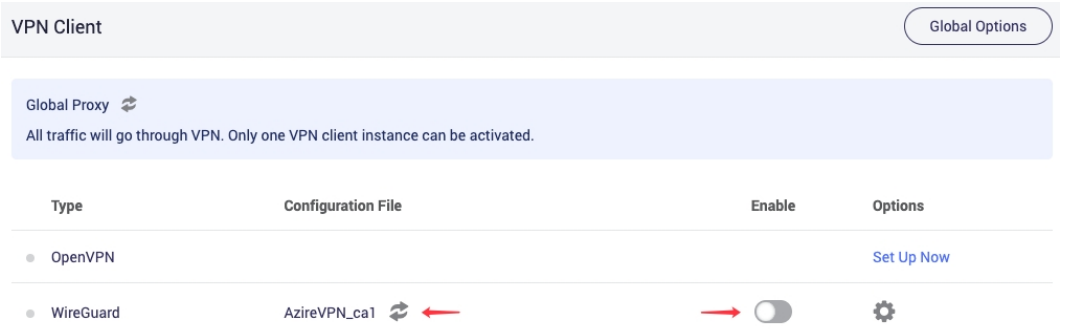
Suivez les étapes ci-dessous pour configurer le routeur comme client AzireVPN.

1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **AzireVPN**.
2. Saisissez le nom d’utilisateur et le mot de passe, puis cliquez sur **Enregistrer les identifiants et récupérer les serveurs (Save Credentials And Get Servers)**. Des fichiers de configuration sont générés pour chaque serveur.

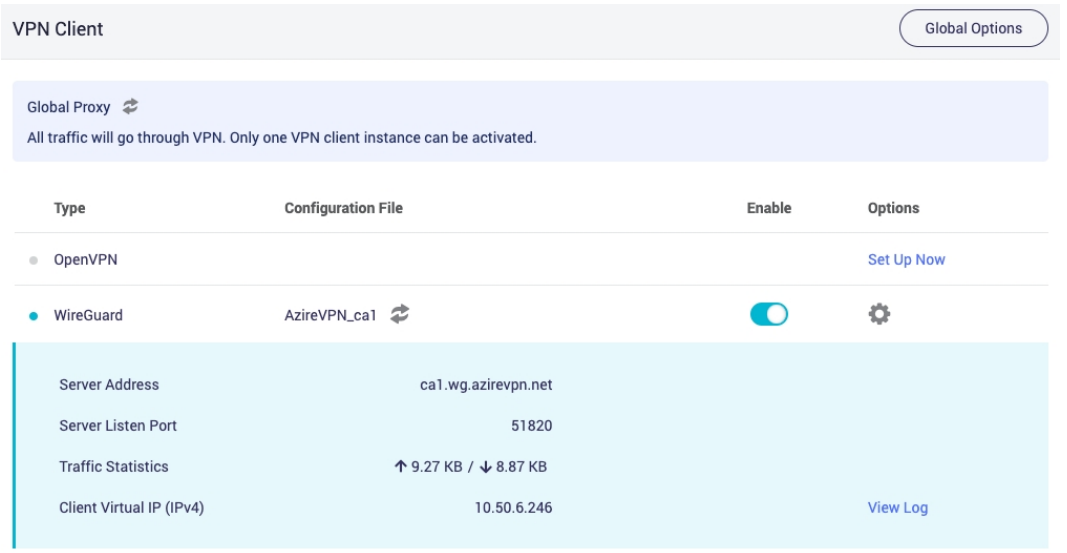




3. Accédez au tableau de bord VPN pour activer la connexion.

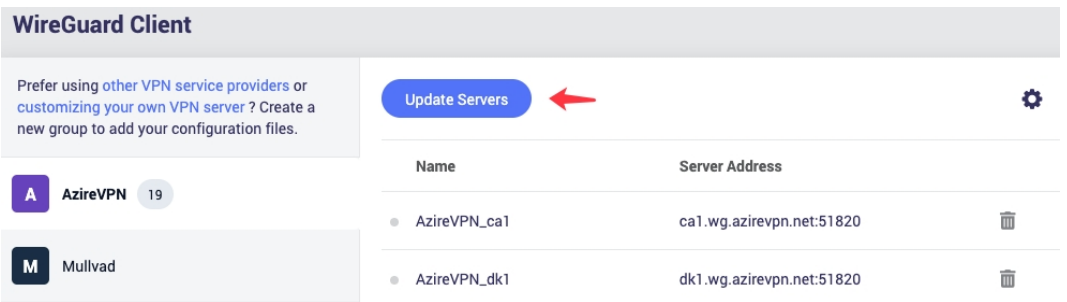


Une fois connecté, vous devriez voir votre adresse IP ainsi que le nombre d'octets envoyés et reçus.



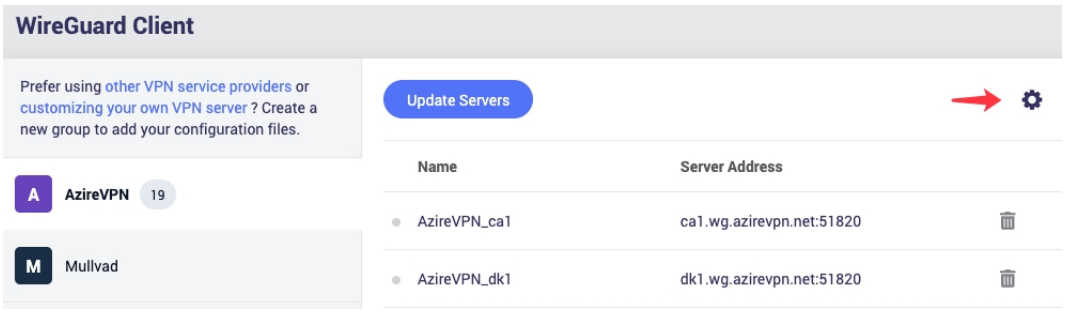
4. Mettez à jour les serveurs.

AzireVPN peut effectuer des opérations de maintenance ou arrêter certains serveurs, ce qui peut entraîner un échec de connexion. Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste des serveurs disponibles.



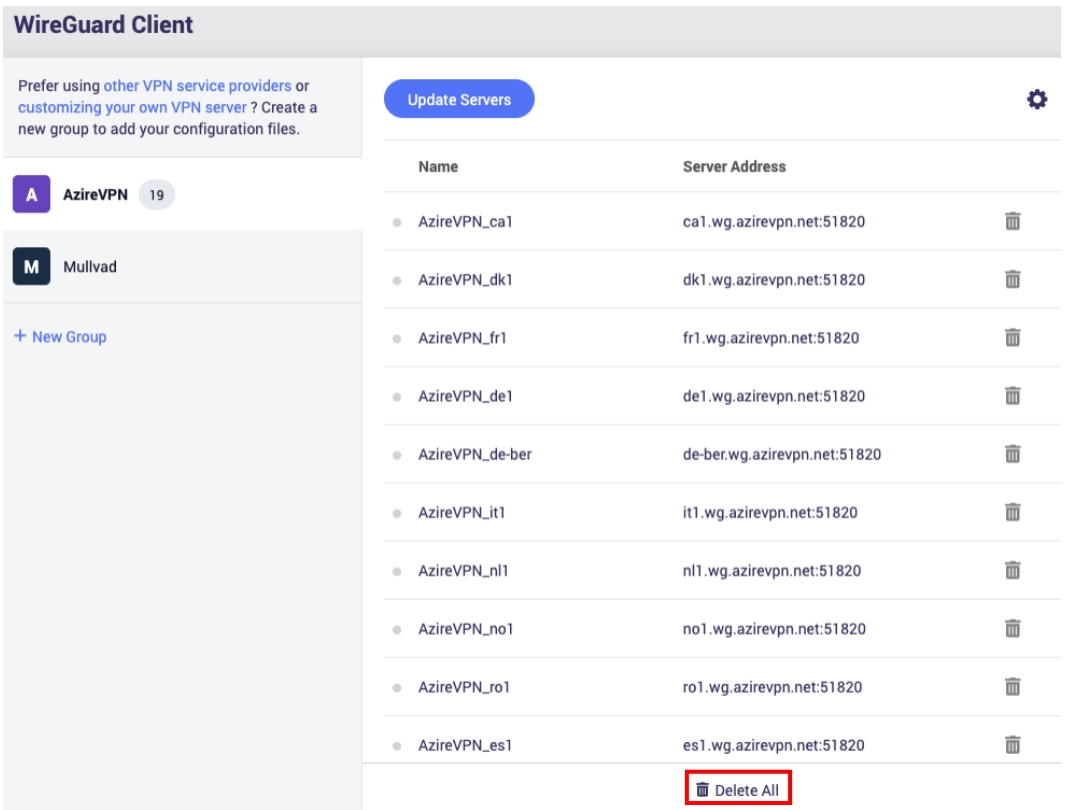
5. Modifiez les identifiants.

Cliquez sur l'icône d'engrenage pour modifier les identifiants.



6. Supprimez tous les fichiers.

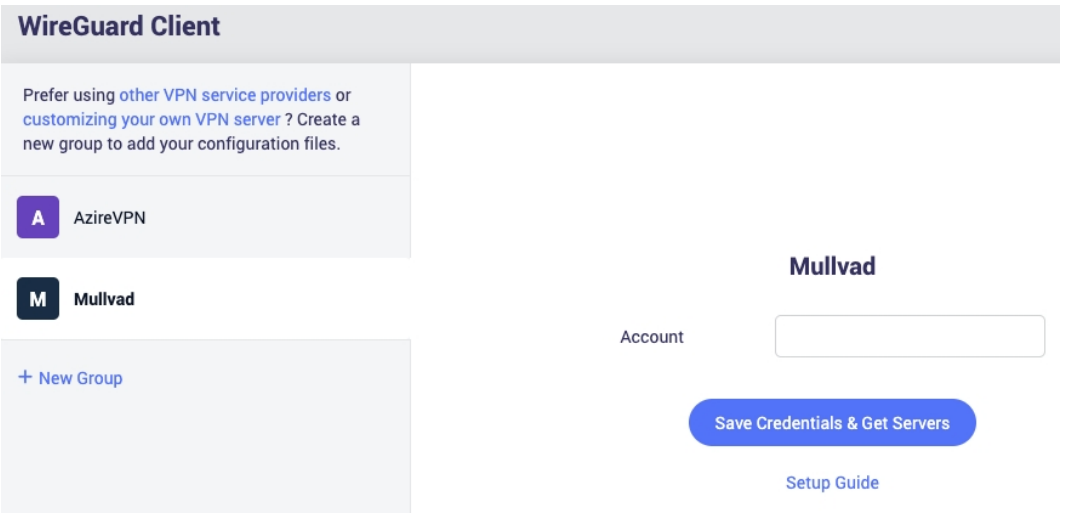
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic.



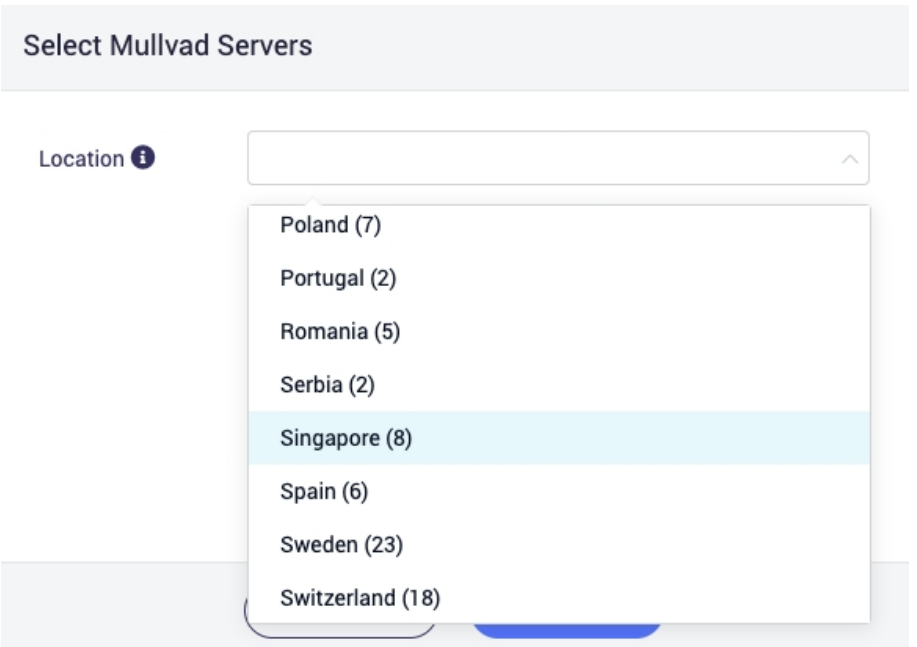
10.2.3 Configuration de Mullvad

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 votre numéro de compte Mullvad à 16 chiffres, puis cliquez sur **Enregistrer les identifiants et récupérer les serveurs (Save Credentials & Get Servers)**.

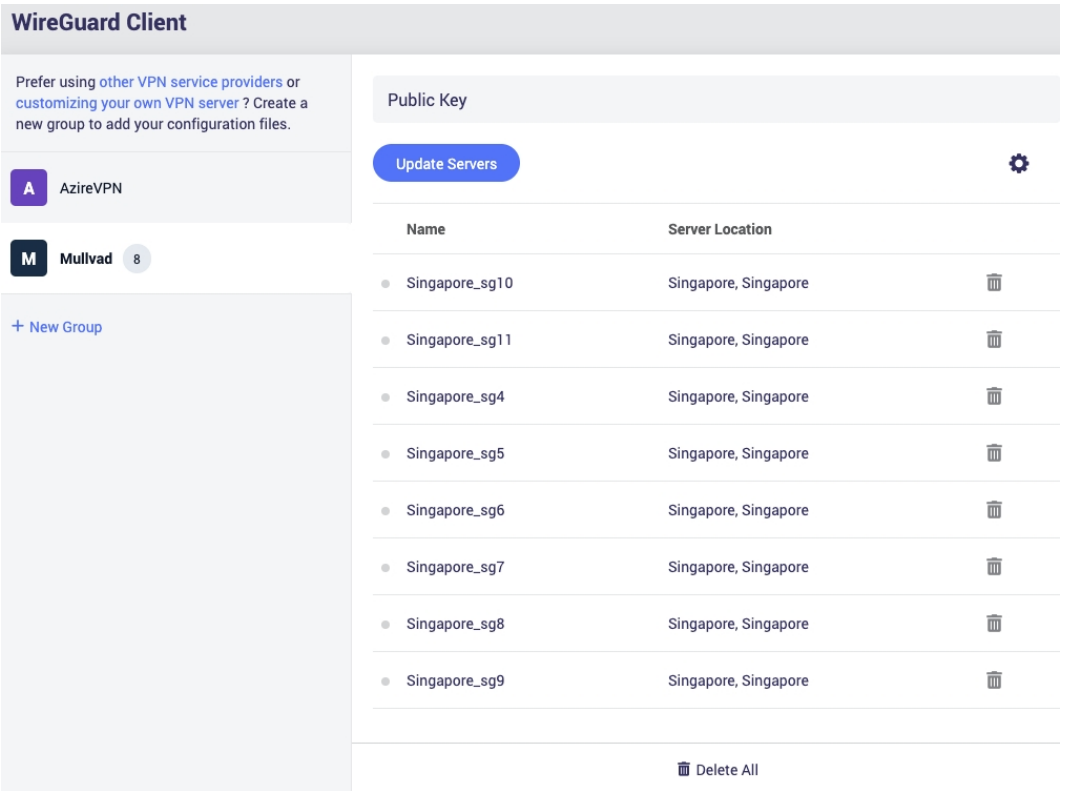


Une boîte de dialogue s'affiche pour vous permettre de choisir un emplacement.

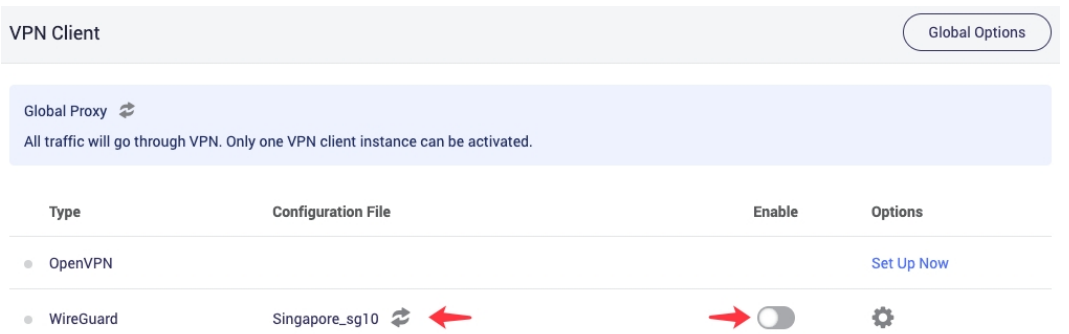


Les fichiers de configuration du serveur à l'emplacement sélectionné sont ensuite générés.

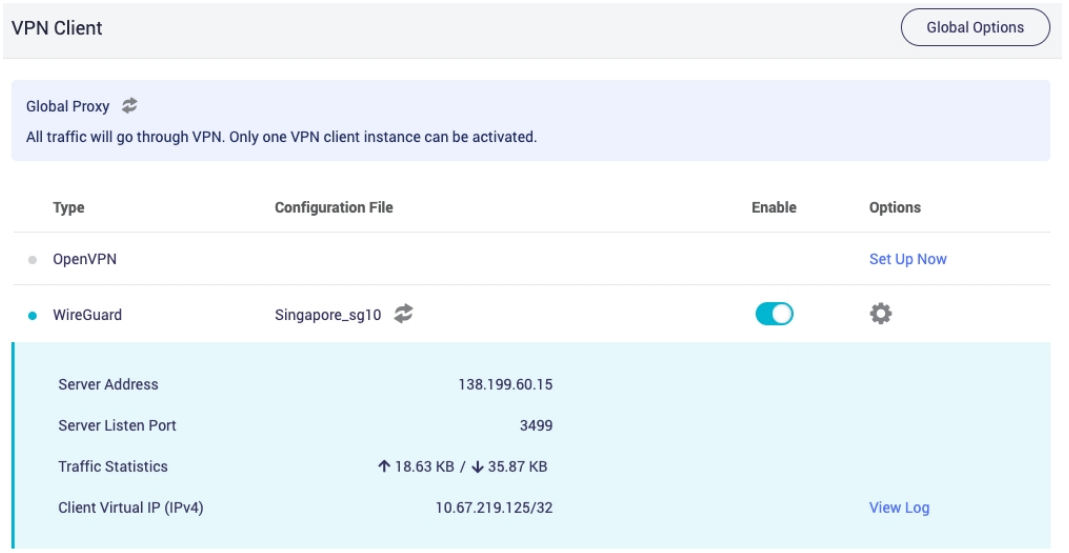
La **clé publique (Public Key)** est la clé publique WireGuard à transmettre au serveur Mullvad. Vous pouvez disposer de cinq clés à la fois et gérer vos clés WireGuard sur la page de votre compte Mullvad.



3. Accédez au tableau de bord VPN pour activer la connexion.

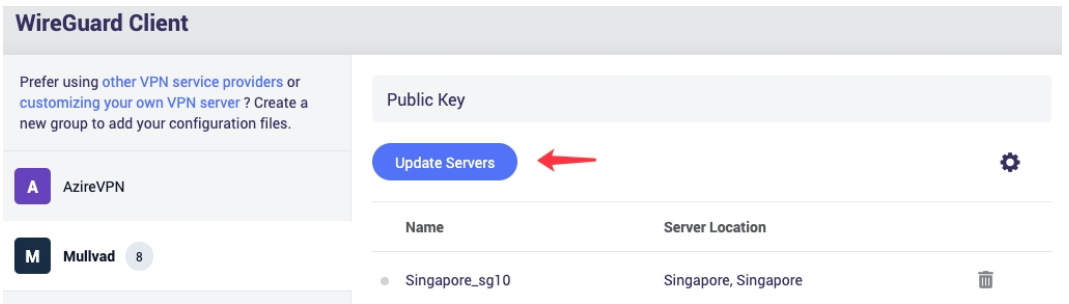


Une fois connecté, vous devriez voir votre adresse IP ainsi que le nombre d’octets envoyés et reçus.



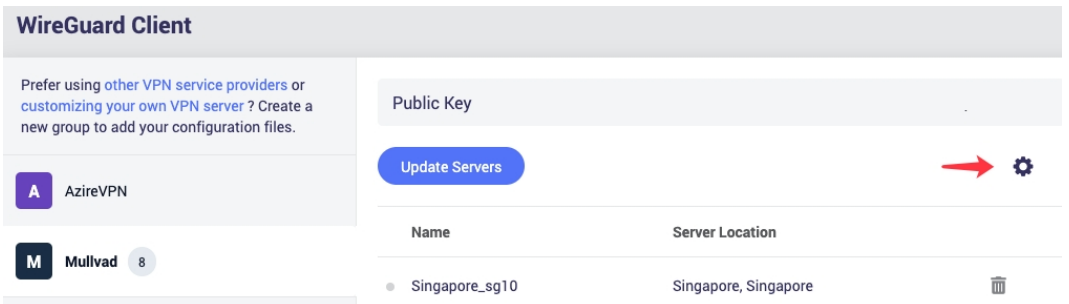
4. Serveurs de mise à jour (Update servers)

   Mullvad peut effectuer des opérations de maintenance ou arrêter certains serveurs, ce qui peut entraîner un échec de connexion. Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste des serveurs disponibles.



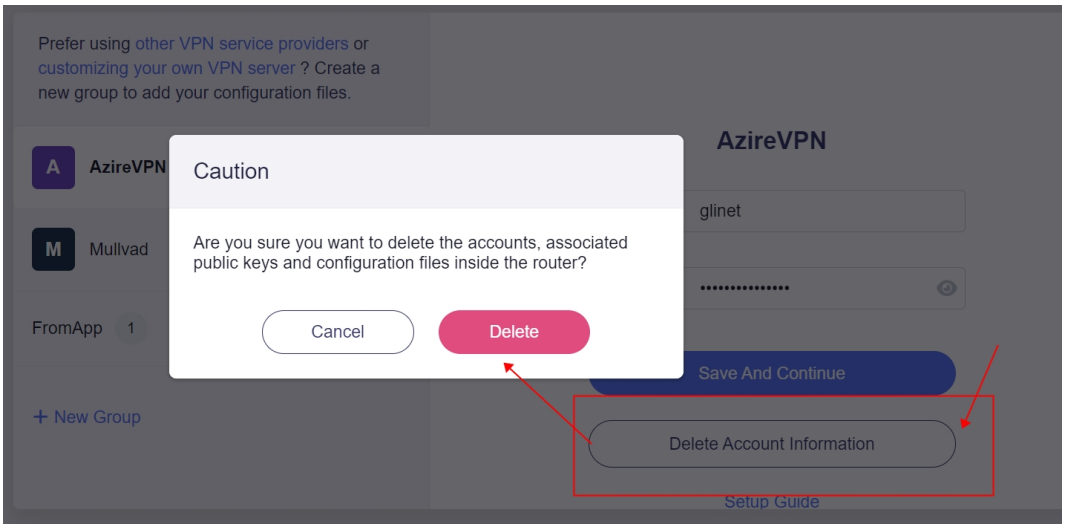
5. Modifier les identifiants

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



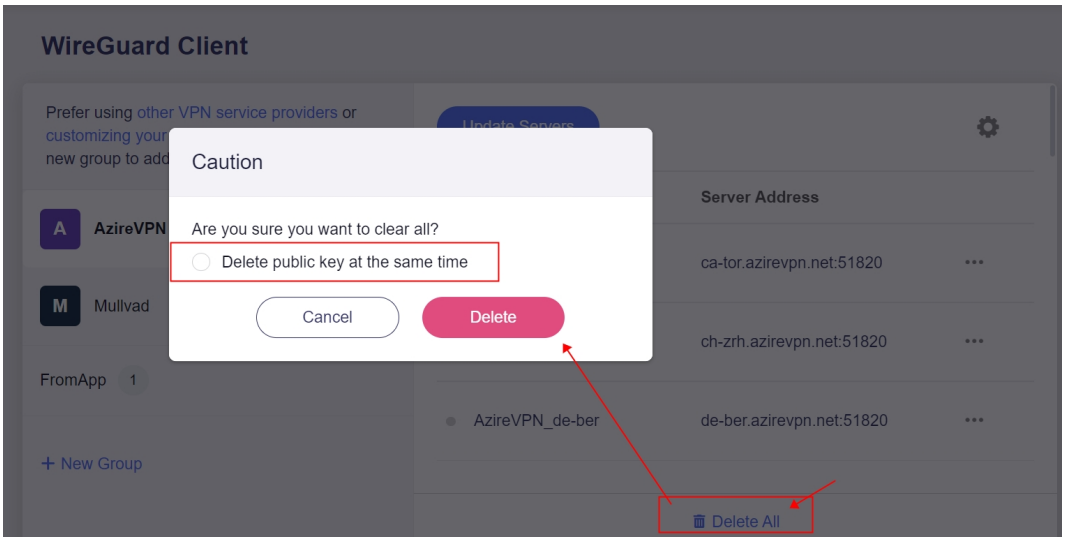
6. Supprimer les informations du compte

   Si vous cliquez sur **Supprimer (Delete)**, les identifiants du compte, la clé privée, la clé publique et les fichiers de configuration sont supprimés **du routeur**.



7. Supprimer

   Permet de supprimer tous les fichiers de configuration en un clic et propose également de supprimer la clé privée et la clé publique.

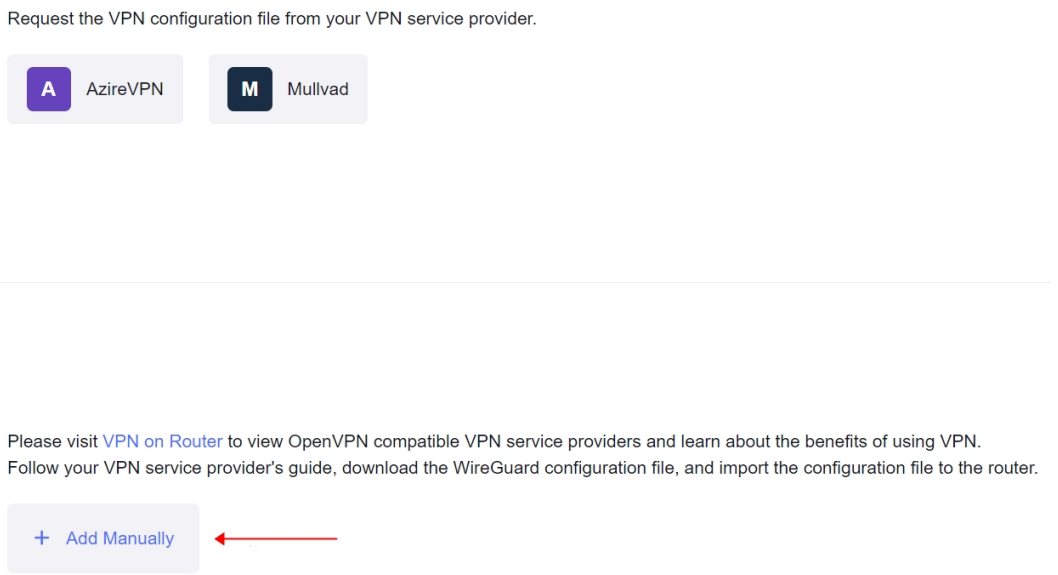


10.2.4 Configuration manuelle d’un client WireGuard pour un autre fournisseur

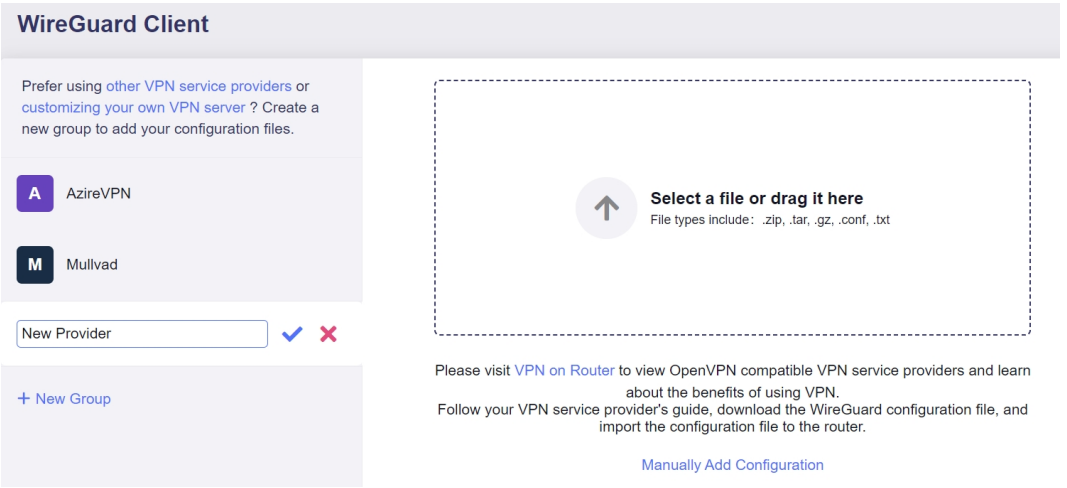
Si votre fournisseur WireGuard n’est pas intégré à l’interface Web, récupérez d’abord le fichier de configuration sur son site officiel, puis importez-le sur le routeur. Si vous ne savez pas comment télécharger les fichiers, consultez ce guide ou contactez l’assistance du fournisseur.

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

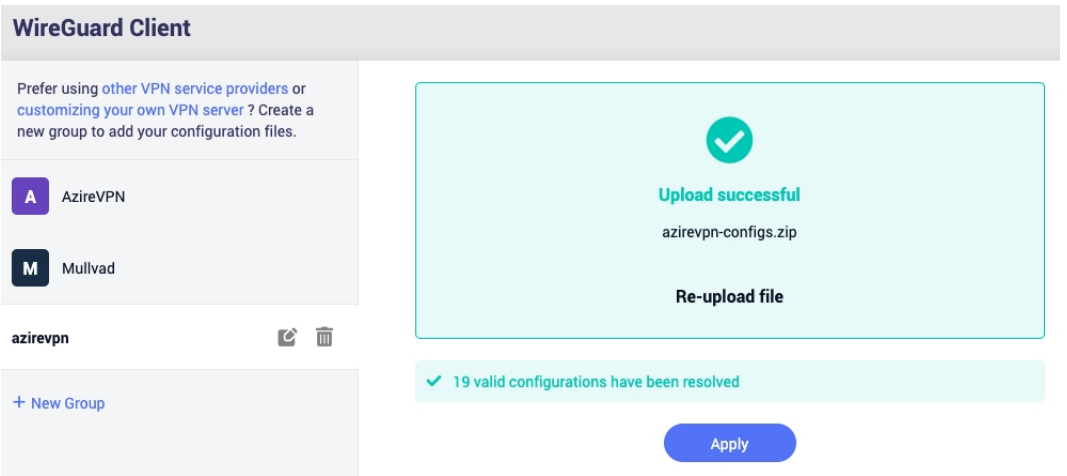
1. Dans l’interface d’administration Web, ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Ajouter manuellement (Add Manually)**.



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

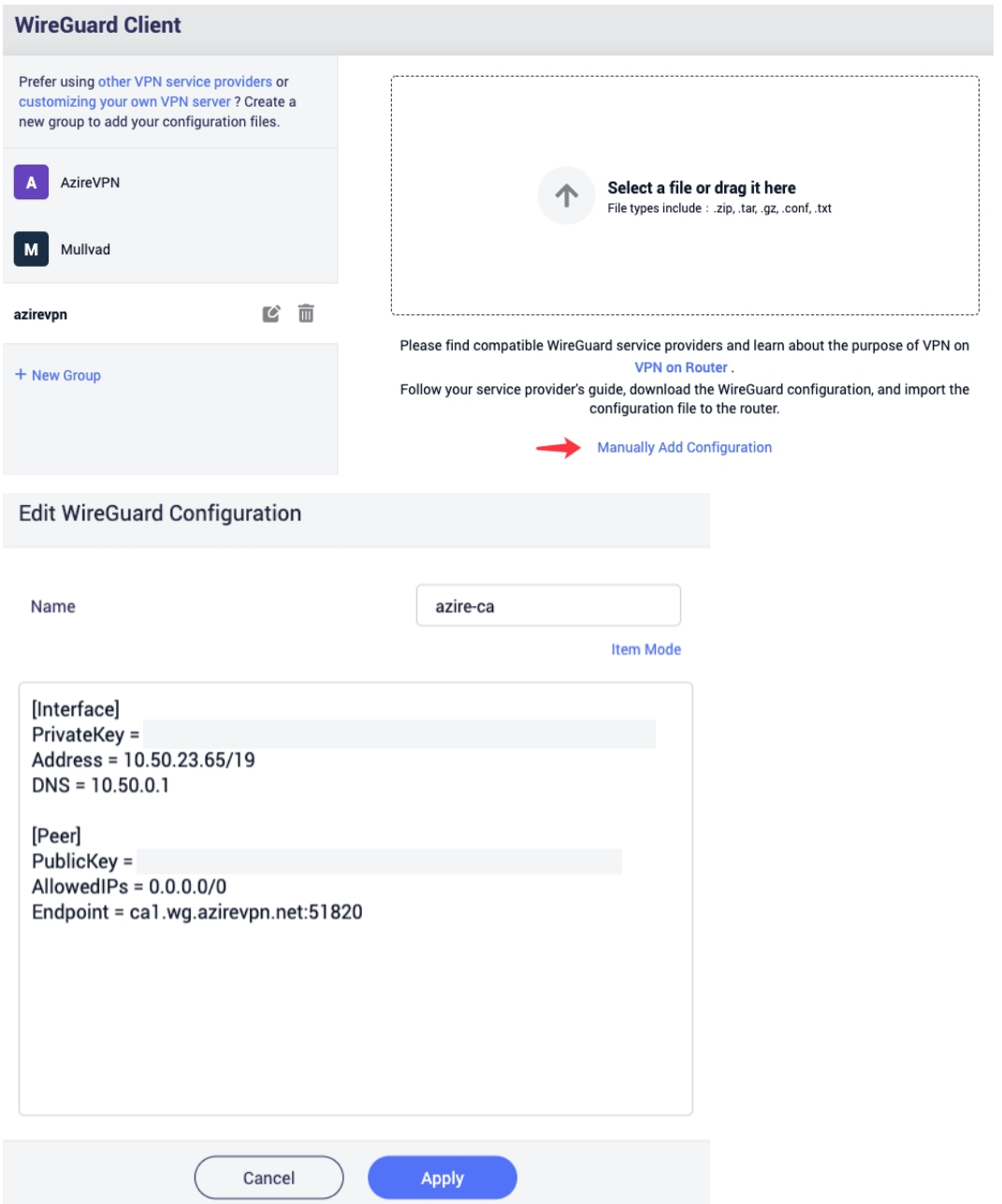


3. Cliquez sur la zone d'importation et sélectionnez votre fichier WireGuard. Les formats zip, tar, gz, conf et txt sont pris en charge. Cliquez sur **Appliquer (Apply)**.

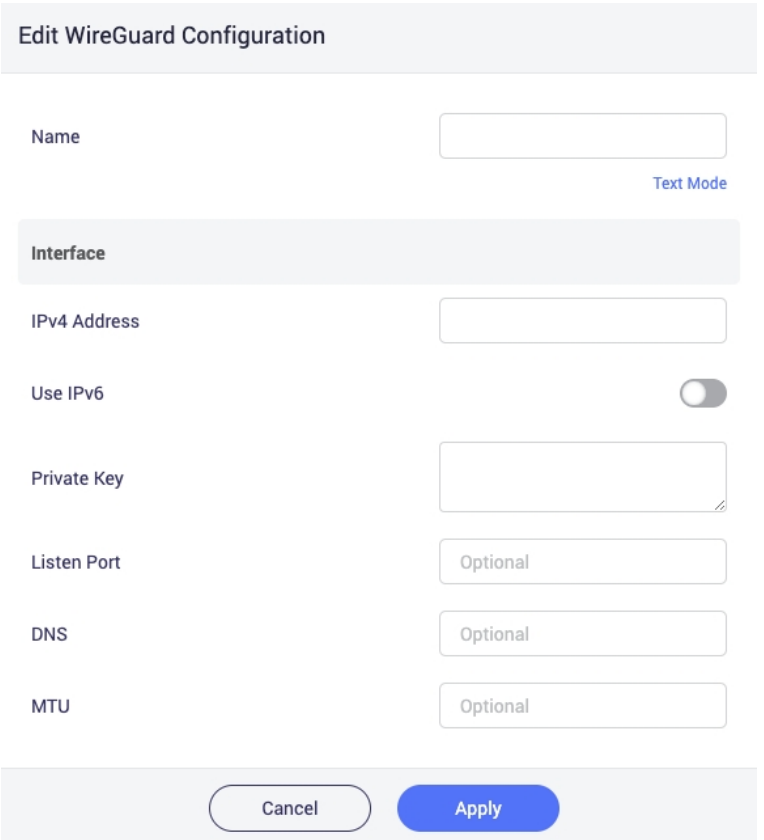


Si vous importez une archive contenant plusieurs fichiers de configuration, elle sera décompressée automatiquement.

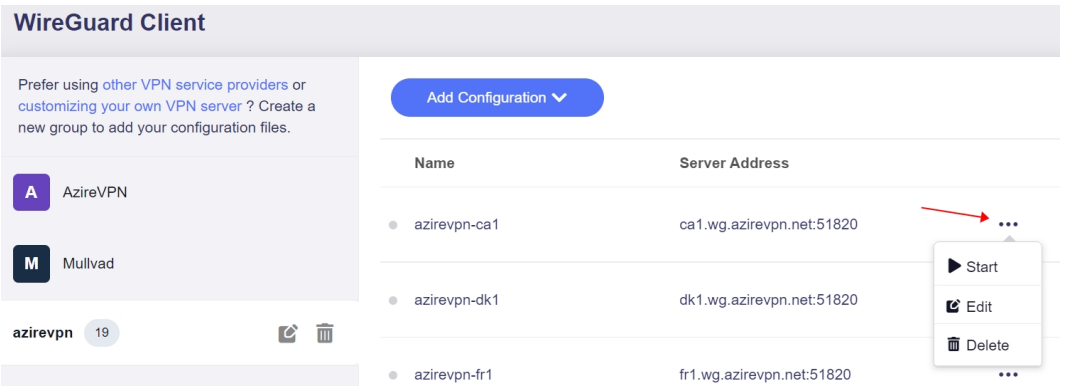
Vous pouvez aussi cliquer sur **Ajouter une configuration manuellement (Manually Add Configuration)** en bas de la zone d'importation, renseigner la configuration sous forme de texte, puis cliquer sur **Appliquer (Apply)**.



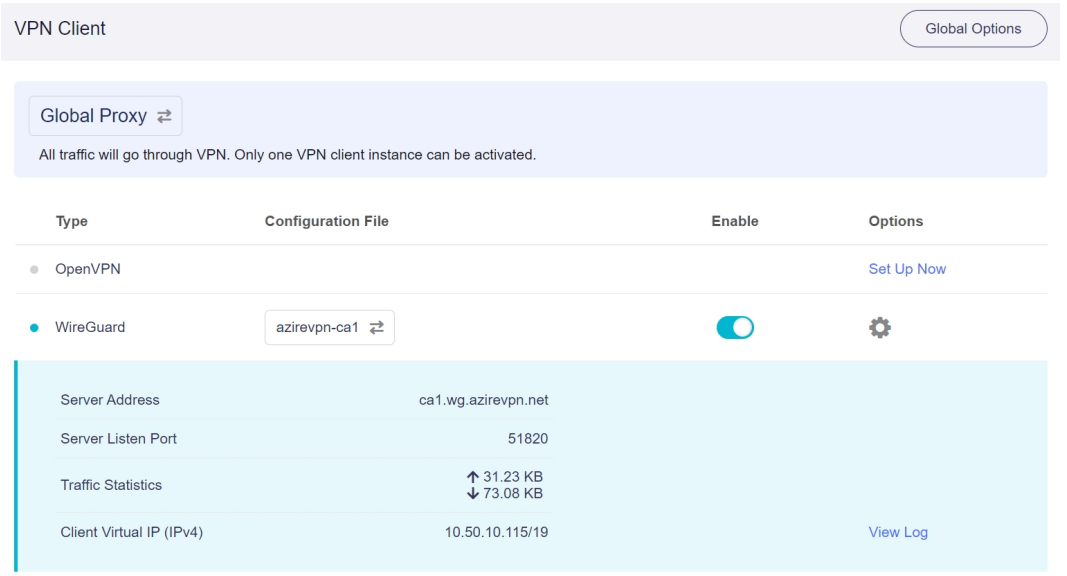
Pour vérifier chaque paramètre, passez en mode Élément (Item), contrôlez la configuration, puis cliquez sur **Appliquer (Apply)**.



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)**.


VPN Client
Global Options
Global Proxy
All traffic will go through VPN. Only one VPN client instance can be activated.
Type
Configuration File
Enable
Options
OpenVPN
Set Up Now
WireGuard
azirevpn-ca1
Server Address
ca1.wg.azirevpn.net
Server Listen Port
51820
Traffic Statistics
31.23 KB
73.08 KB
Client Virtual IP (IPv4)
10.50.10.115/19
View Log

Chapitre 11

Tor

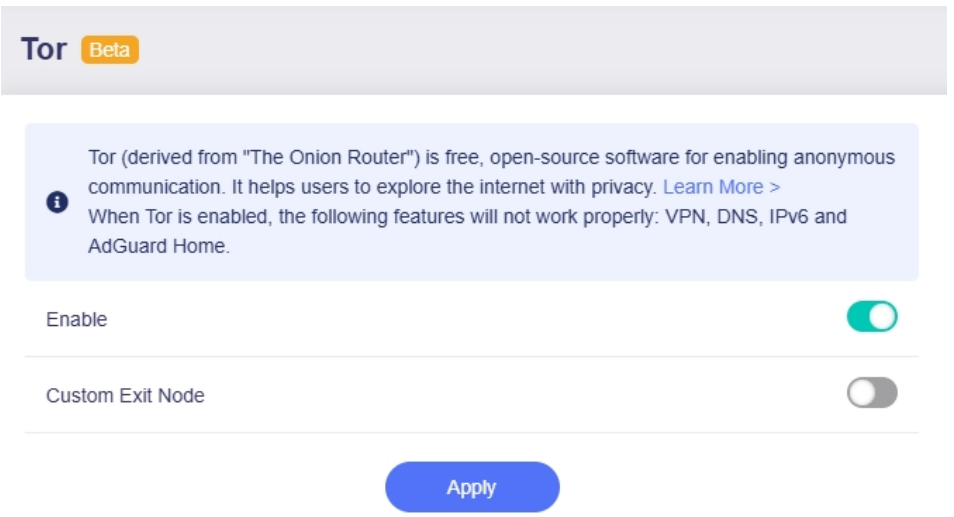
Ce chapitre présente brièvement Tor (The Onion Router), un logiciel libre et gratuit permettant des communications anonymes.

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.

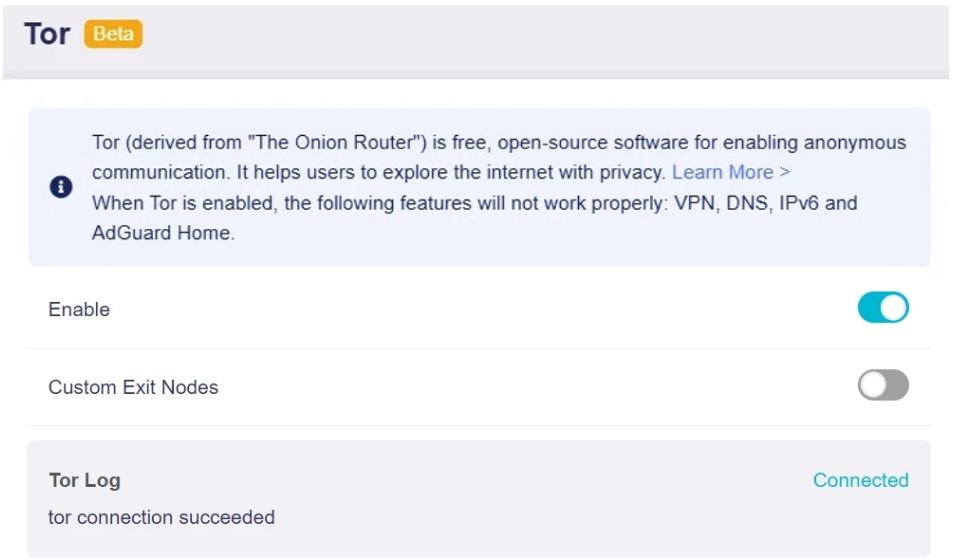
Lorsque Tor est activé, VPN, DNS, IPv6 et AdGuard Home ne fonctionnent pas correctement.

Pour configurer Tor, procédez comme suit.

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



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


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

Chapitre 12

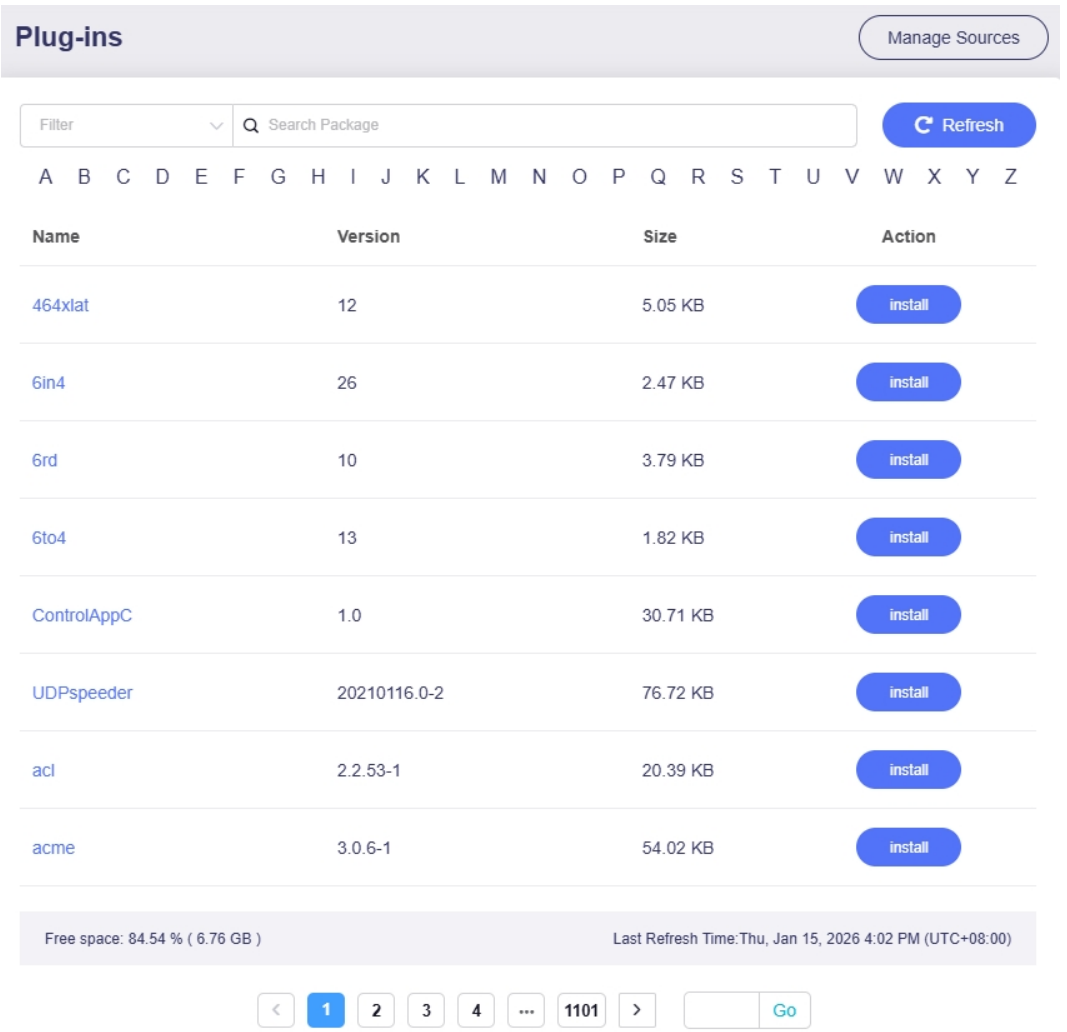
Applications

Ce chapitre présente certaines applications des routeurs GL.iNet, notamment les modules complémentaires, le DNS dynamique, GoodCloud, le stockage réseau, AdGuard Home, le 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 :

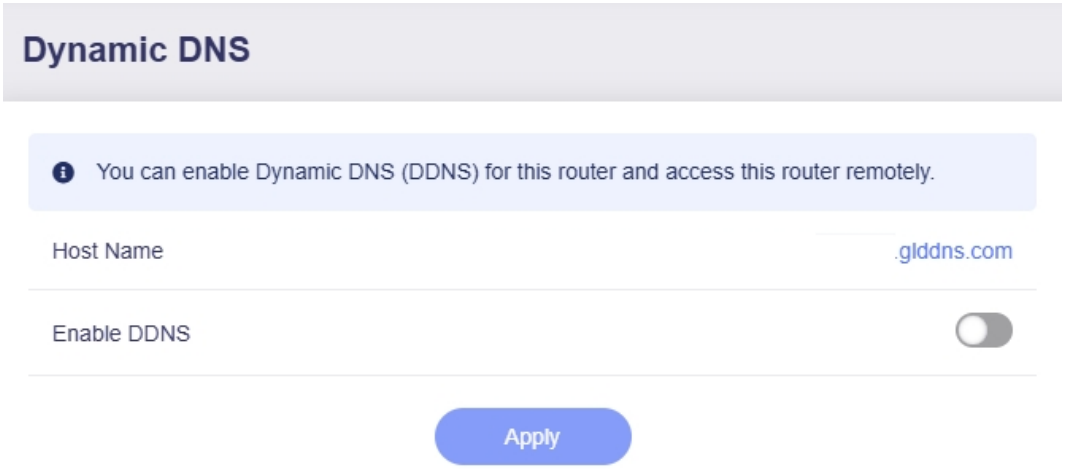
1. Il est déconseillé de mettre à jour les extensions préinstallées dans le micrologiciel officiel GL.iNet, comme nginx, AdGuard Home ou Tailscale.
2. Les extensions tierces installées manuellement peuvent être mises à jour. GL.iNet n'est toutefois pas responsable des problèmes de sécurité qu'elles peuvent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

12.2 DNS dynamique

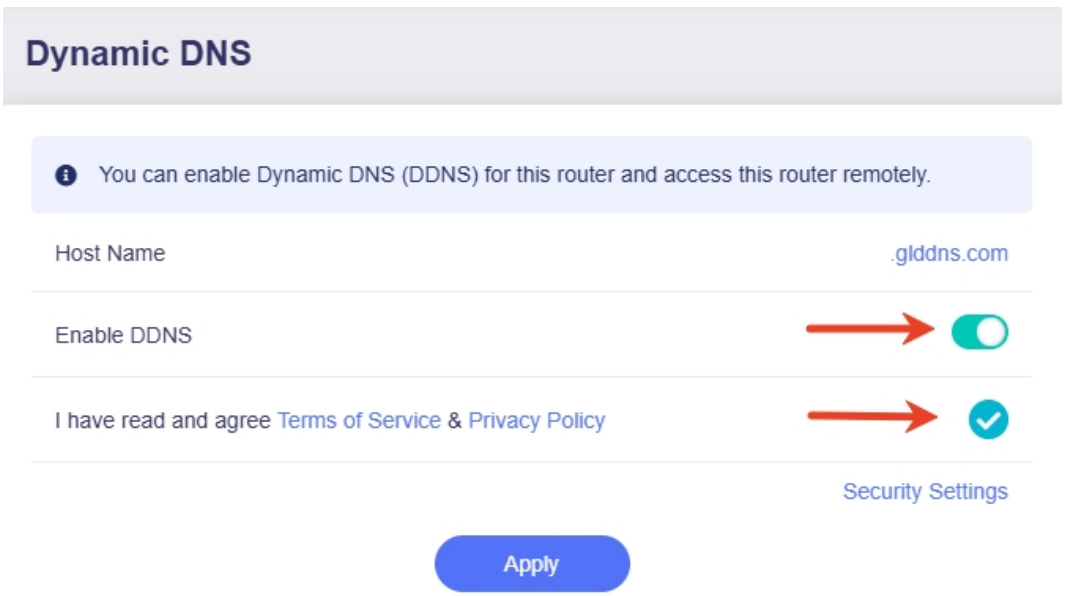
Le DNS dynamique (DDNS) associe un nom de domaine à l'adresse IP dynamique d'un appareil réseau. Il permet d'accéder au routeur à distance. Cette fonction nécessite une adresse IP publique.

12.2.1 Activation du DDNS

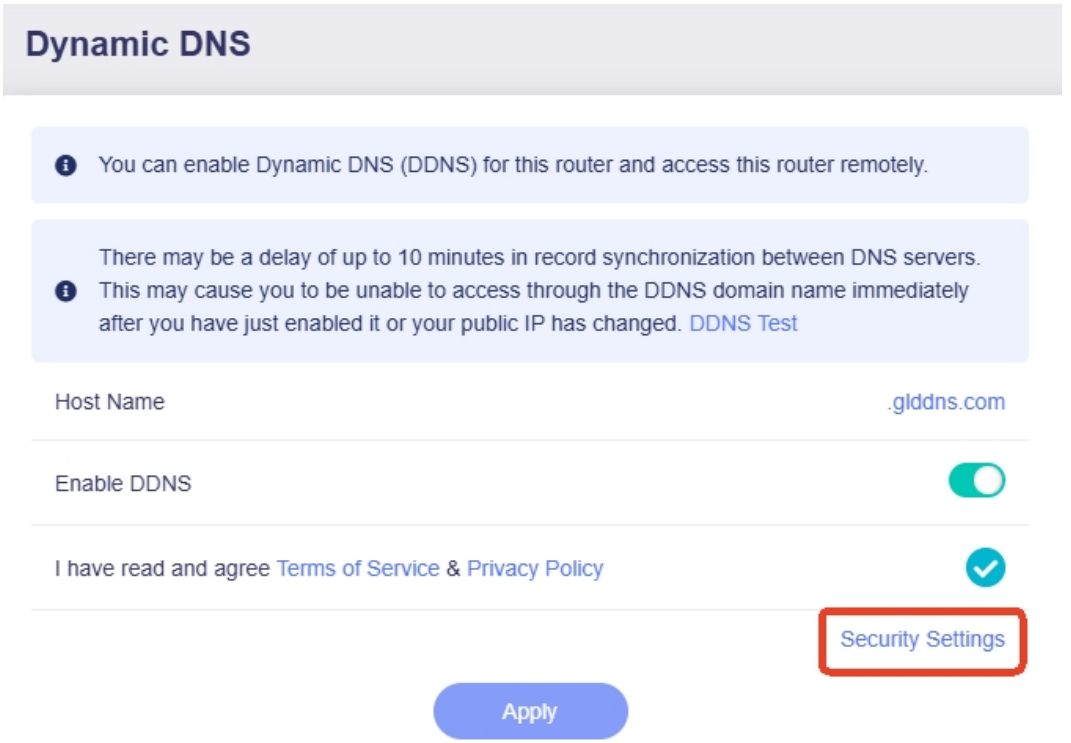
1. Dans l'interface d'administration Web, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)**. La page ci-dessous s'affiche.



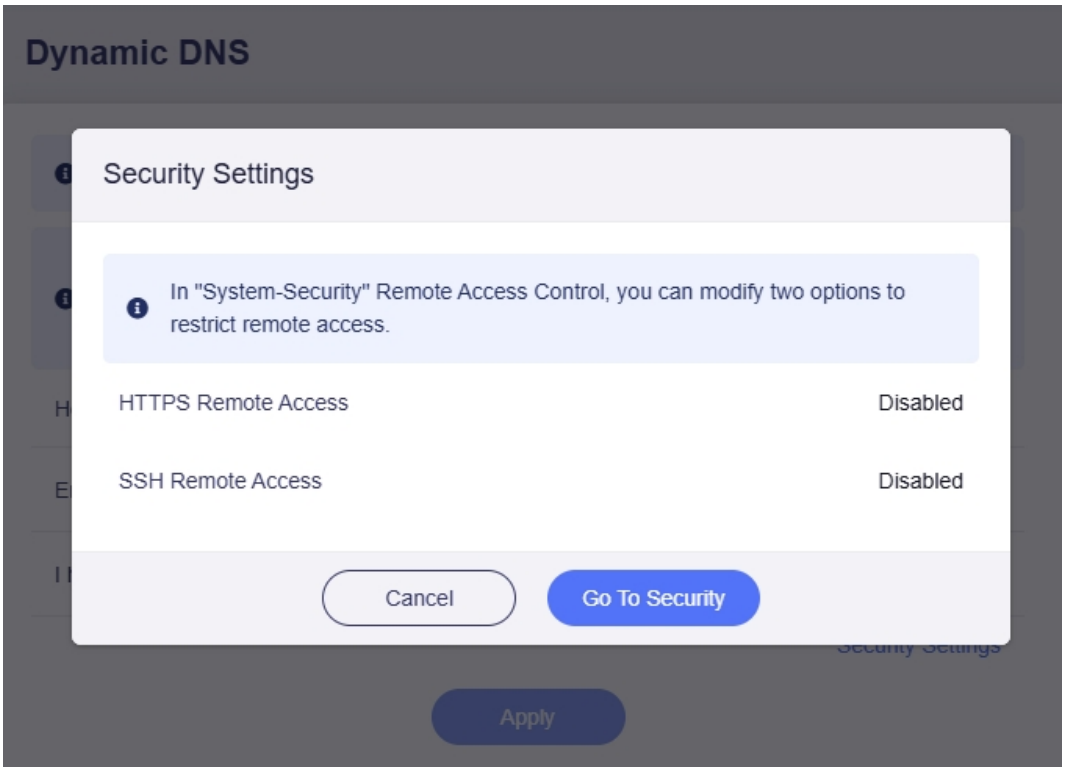
2. Activez **Activer le DDNS (Enable DDNS)**, lisez et acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



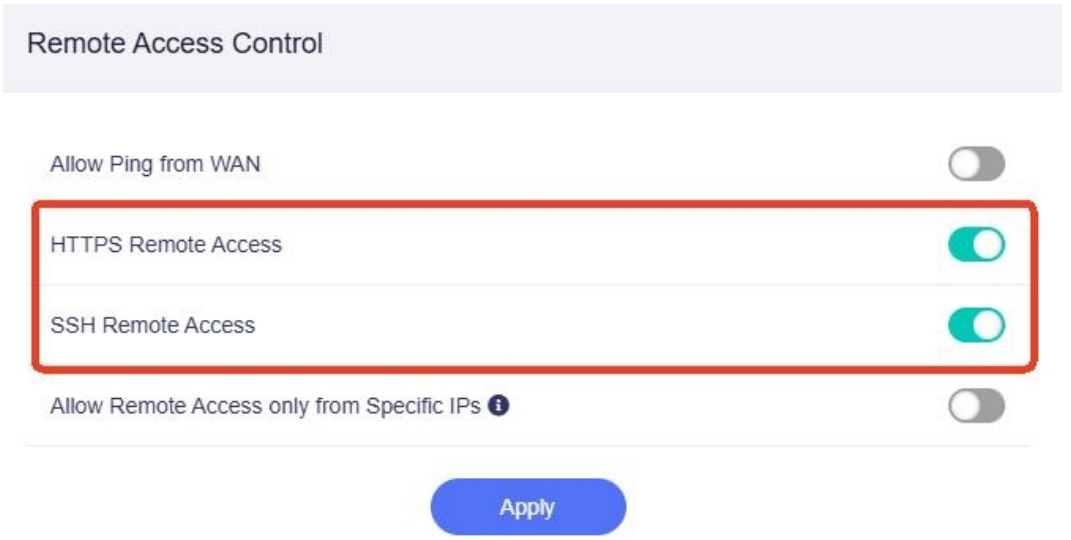
3. Cliquez sur **Paramètres de sécurité (Security Settings)** dans l'angle inférieur droit.



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



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



Remarque :

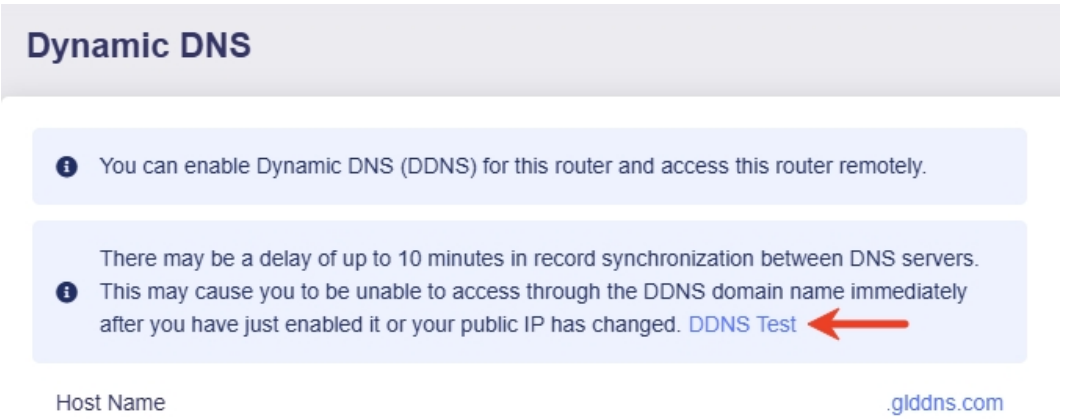
1. La synchronisation des enregistrements entre serveurs DNS peut prendre jusqu’à 10 minutes. L’accès par le domaine DDNS peut donc être indisponible immédiatement après son activation ou après un changement d’IP publique.
2. Si vous activez simultanément le DDNS et un client VPN, vérifiez que Services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

12.2.2 Vérification du fonctionnement du DDNS

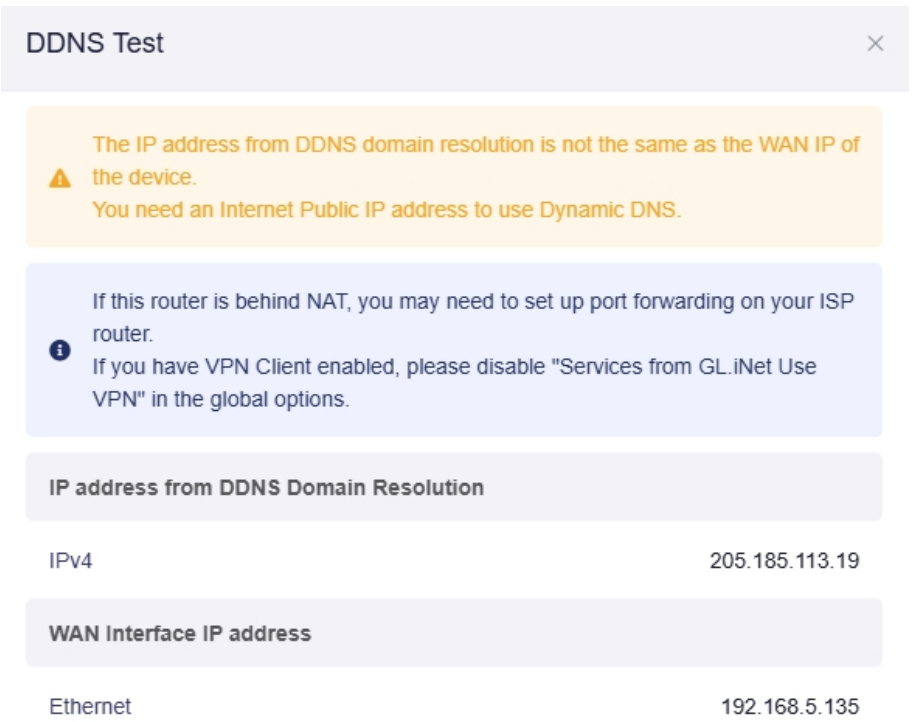
Vérifiez le DDNS avec l'outil de test intégré ou manuellement à l'aide de commandes.

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, comme ci-dessous.



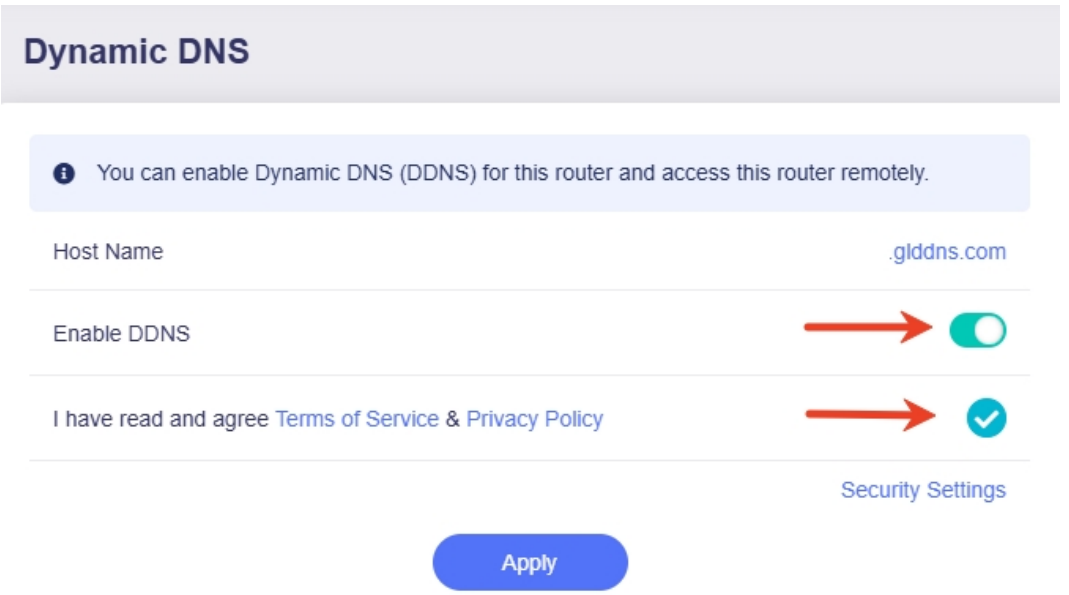
   - Remplacez « xxxxxxx.glddns.com » par votre nom d'hôte.
   - « 8.8.8.8 » est le DNS de Google. Utilisez-le ou indiquez un autre serveur, puis appuyez sur Entrée.
2. Une IP publique, comme « 183.178.10.100 » dans l'image, indique que le domaine DDNS est bien associé à une adresse publique. Un message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

12.2.3 Accès HTTPS à distance

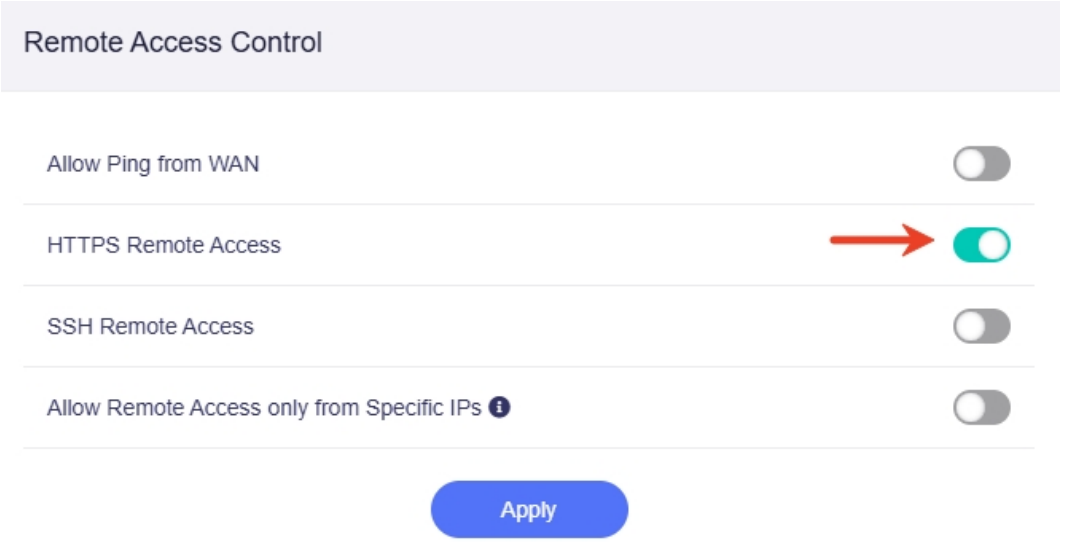
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 443** sur le routeur en amont.

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)**.

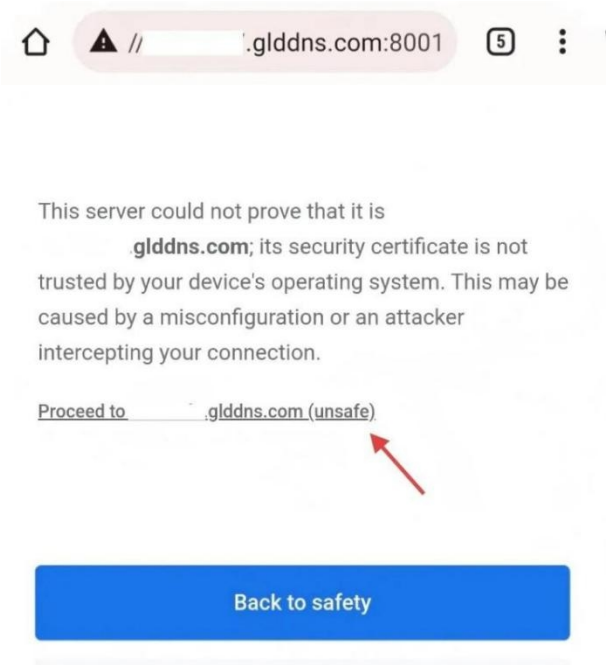


2. Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Sécurité (Security)** > **Contrôle d'accès distant (Remote Access Control)**. Activez **Accès HTTPS à distance (HTTPS Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



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

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



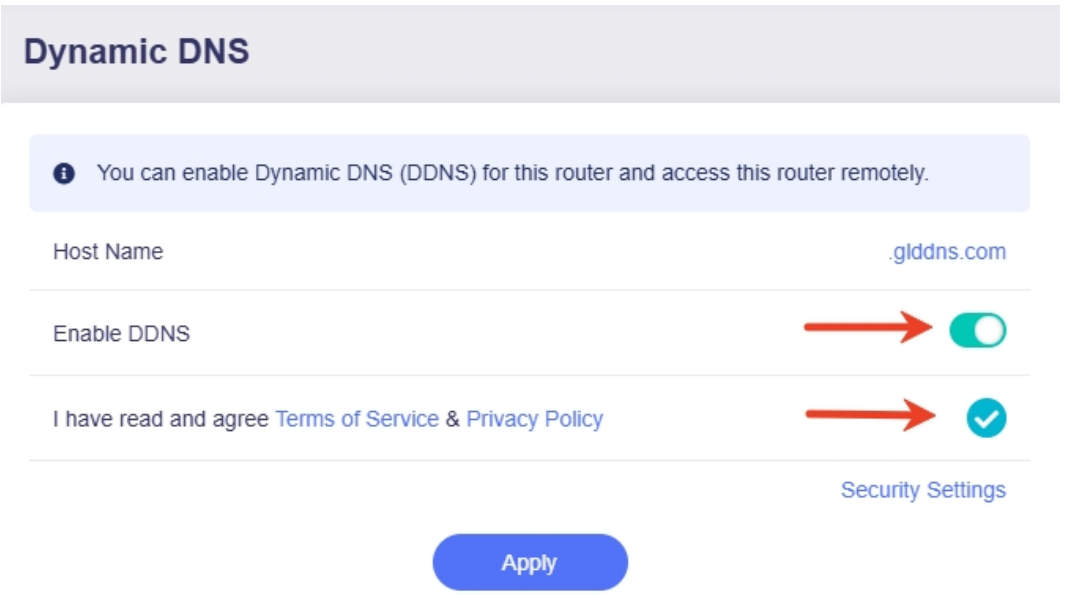
Vous pouvez alors accéder à l'interface Web par le nom d'hôte DDNS en **HTTPS**.

12.2.4 Accès SSH à distance

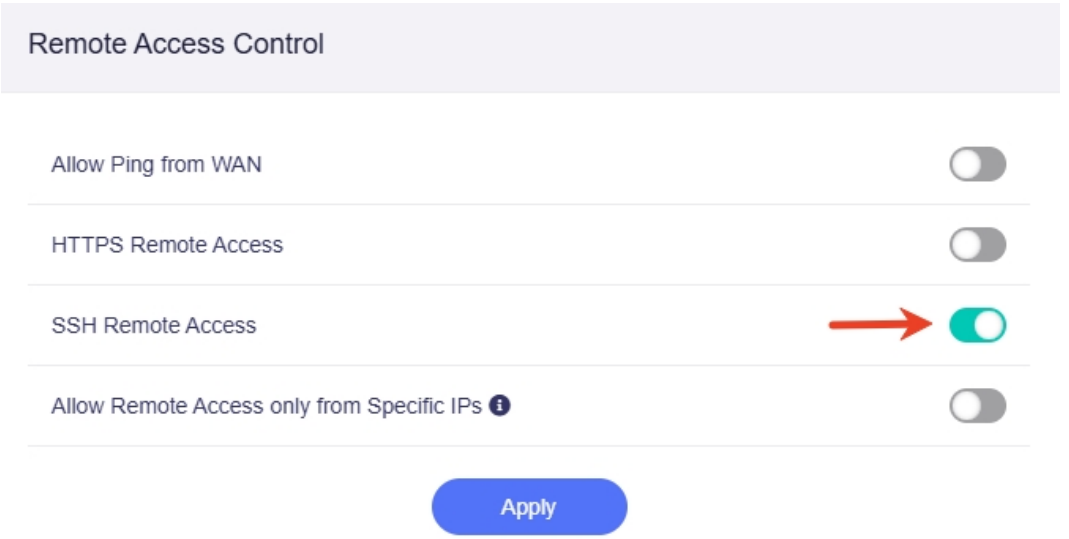
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 22** sur le routeur en amont.

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 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.

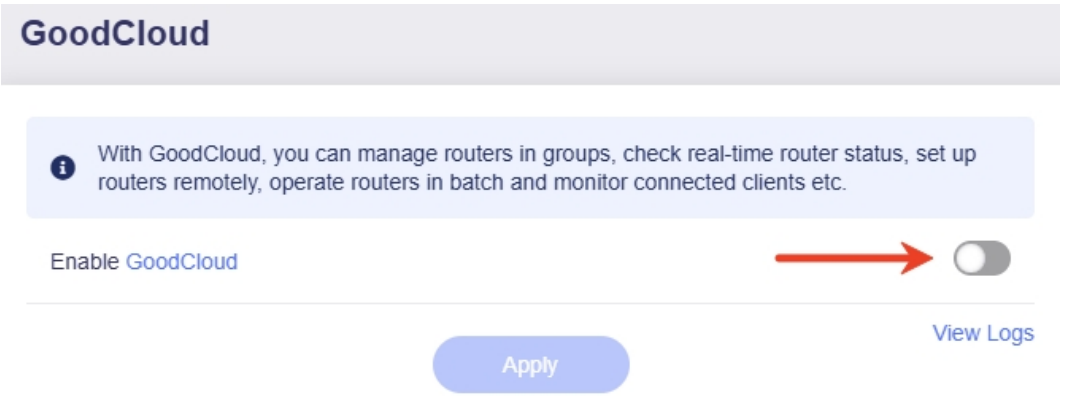
Avec GoodCloud, vous pouvez :

- 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

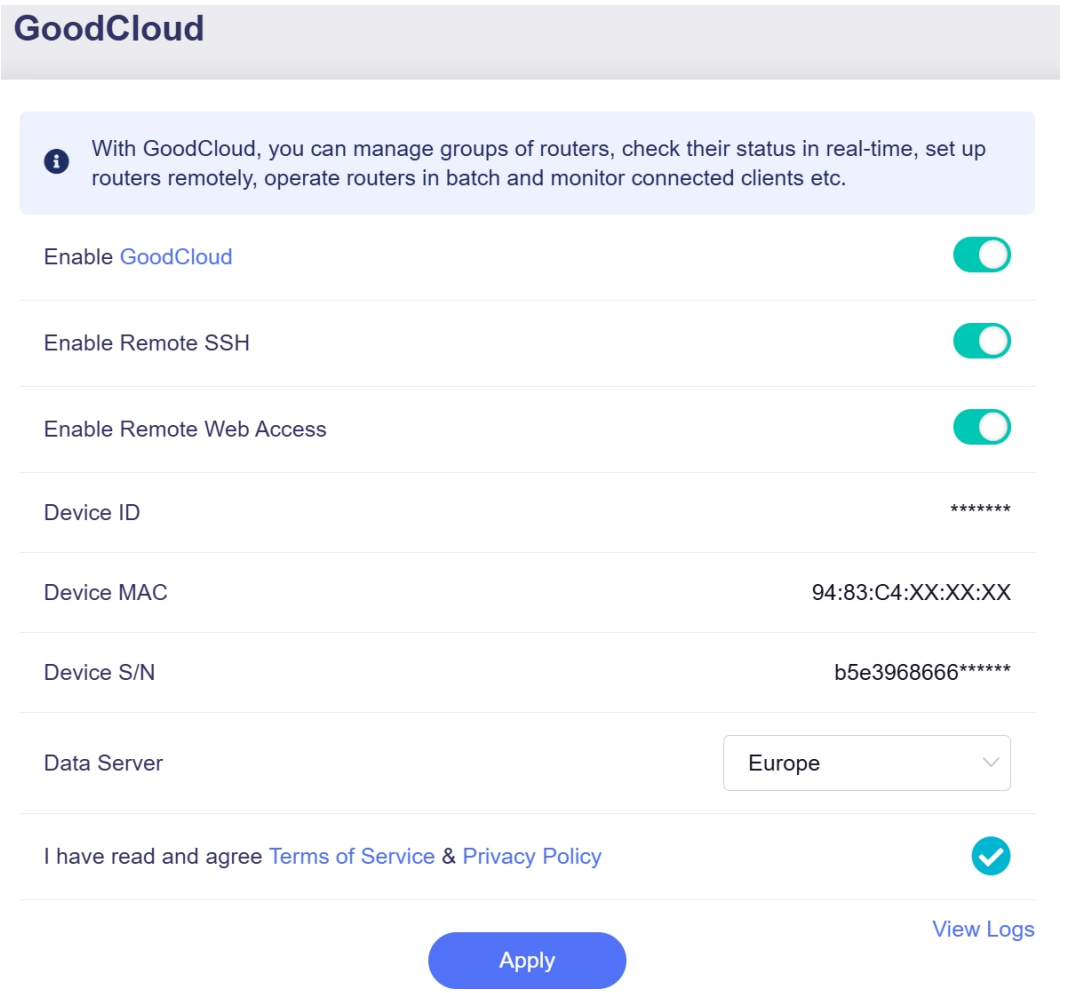
Certaines fonctions sont proposées dans les offres Enterprise et VAR (Value Added Reseller, revendeur à valeur ajoutée). Consultez cette page pour en savoir plus.

12.3.1 Activation de GoodCloud

1. Connectez-vous à l'interface d'administration Web du routeur, puis accédez à **APPLICATIONS** > **GoodCloud**. Activez GoodCloud à l'aide du commutateur.

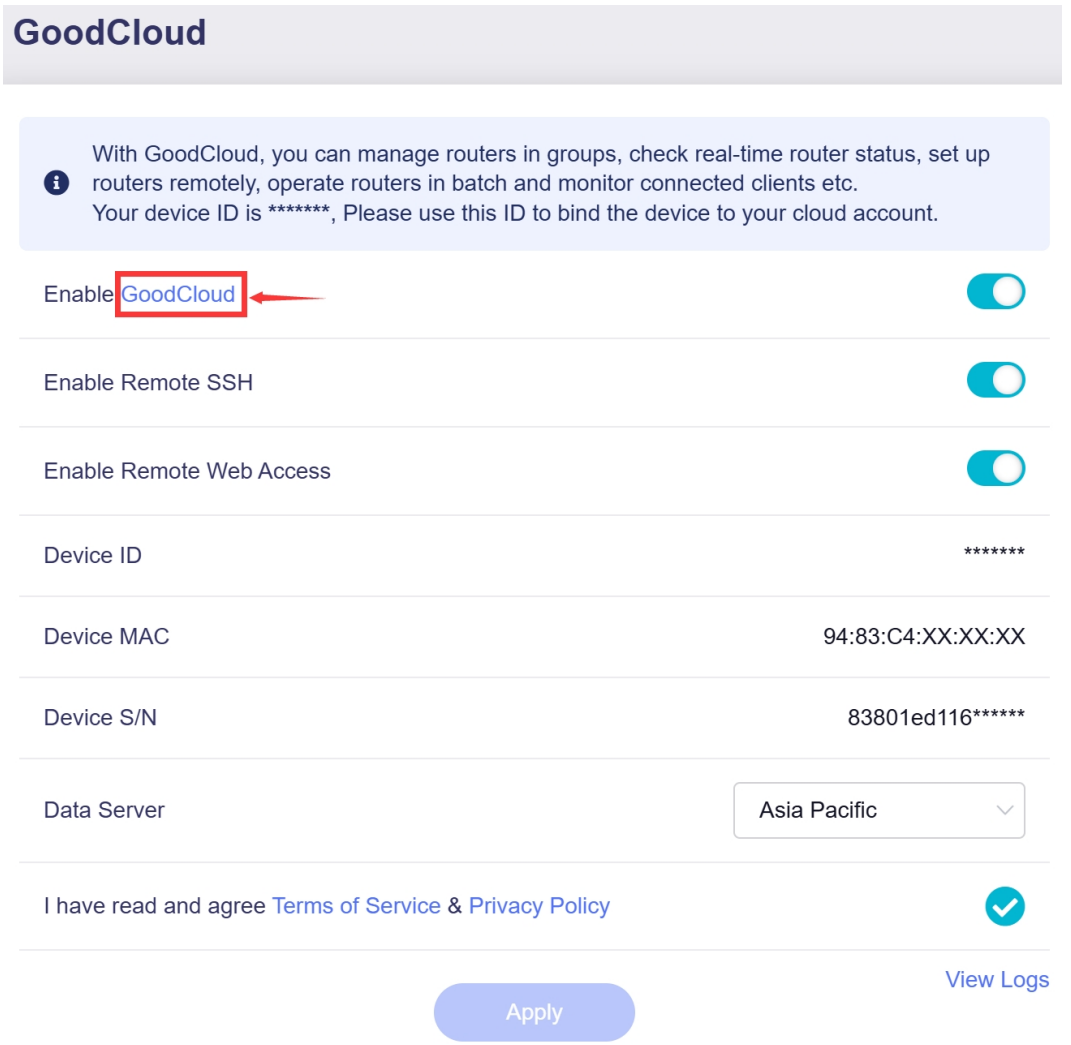


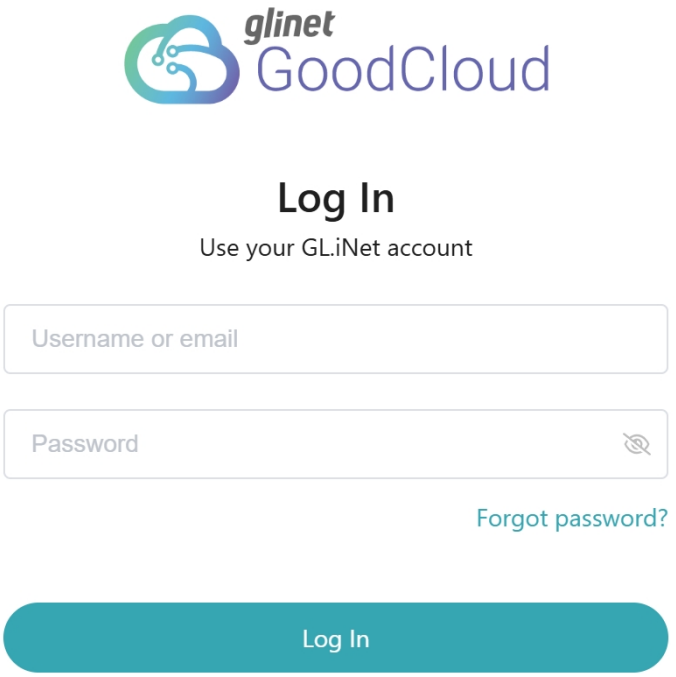
Activez **SSH à distance (Remote SSH)** et **Accès Web à distance (Remote Web Access)** si nécessaire, sélectionnez le serveur le plus proche, lisez et acceptez les **conditions d'utilisation et la politique de confidentialité (Terms of Service & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



- **SSH à distance (Remote SSH)** : permet d'accéder à distance au terminal du routeur via SSH depuis la plateforme GoodCloud.
- **Accès Web à distance (Remote Web Access)** : permet d'accéder à distance à l'interface d'administration Web du routeur via HTTP/HTTPS depuis la plateforme GoodCloud.
- **Serveur de données (Data Server)** : choisissez le serveur le plus proche de votre appareil. Trois options sont disponibles : Asie-Pacifique (Japon), Amérique (Oregon) et Europe (Irlande).
- **Afficher les journaux (View Logs)** : ouvre la page Journal et affiche le journal Cloud.

2. Cliquez sur GoodCloud pour ouvrir la page de connexion et connectez-vous avec votre compte GL.iNet Cloud. Si vous n'avez pas de compte, créez-en un, puis connectez-vous. Une fois la connexion établie, le routeur sera automatiquement associé à votre compte.

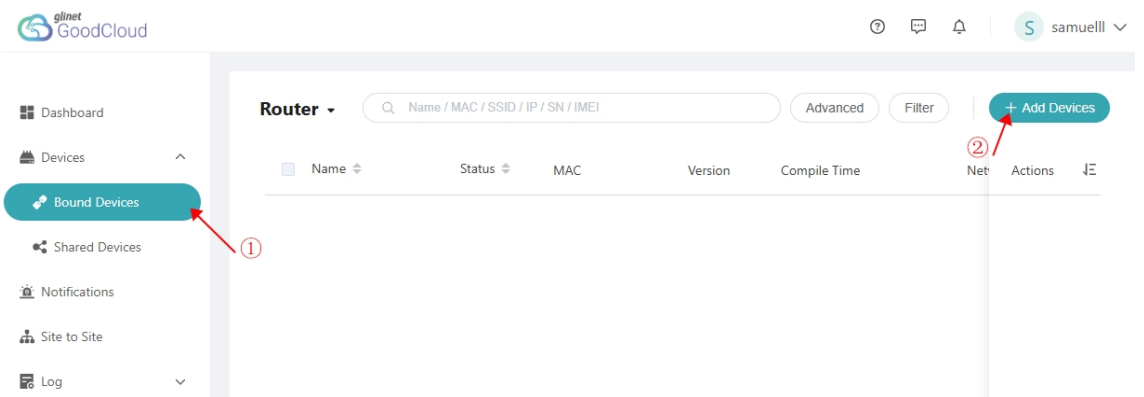

GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is *******, Please use this ID to bind the device to your cloud account.
Enable GoodCloud
Enable Remote SSH
Enable Remote Web Access
Device ID
****
Device MAC
94:83:C4:XX:XX:XX
Device S/N
83801ed116******
Data Server
Asia Pacific
I have read and agree Terms of Service & Privacy Policy
View Logs
Apply



Conseils :

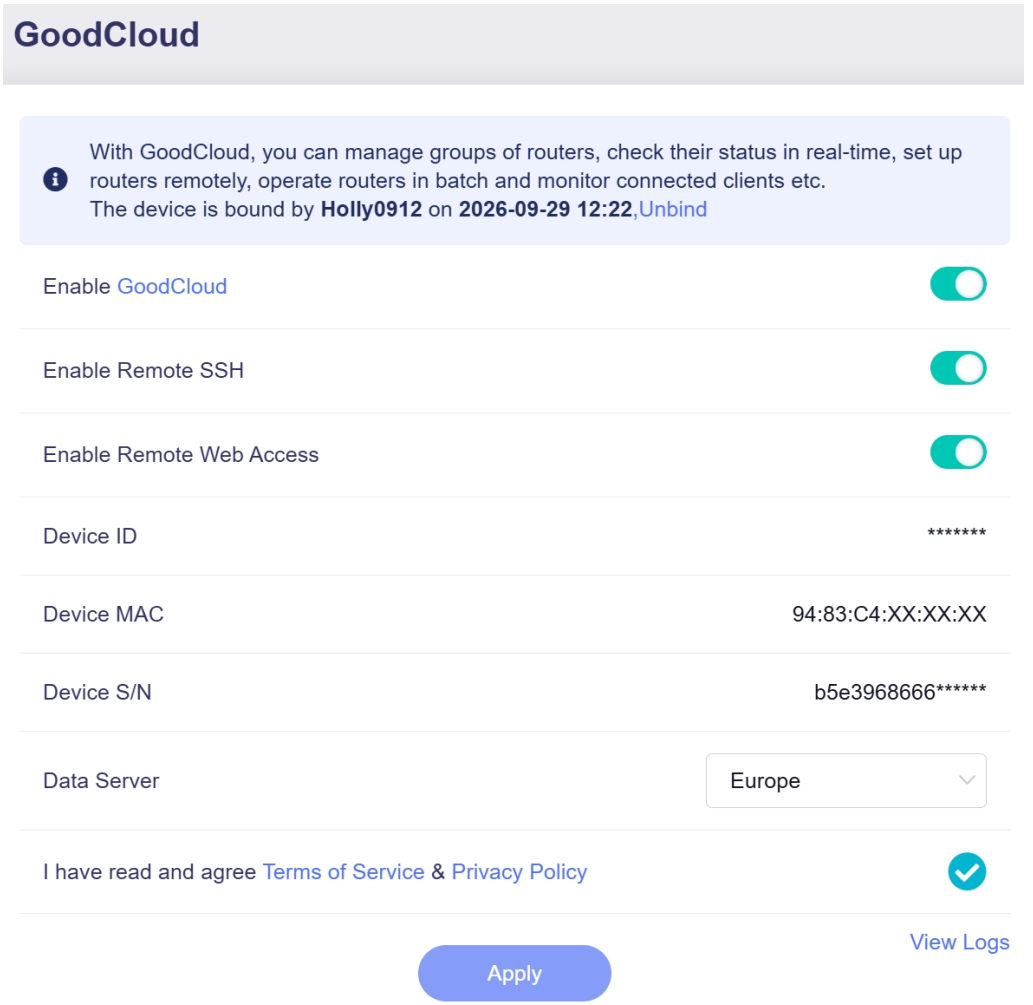
- La procédure d'association à GoodCloud varie selon la version du micrologiciel.
- Si vous ne recevez pas l'e-mail de vérification, consultez votre dossier de courrier indésirable ou réessayez plus tard. Pour obtenir de l'aide, écrivez-nous à support@gl-inet.com.

3. Sur la plateforme Cloud, accédez à **Appareils (Devices)** > **Appareils associés (Bound Devices)** > **Ajouter des appareils (Add Devices)**.



Trois méthodes permettent d'associer un appareil à votre compte GoodCloud : découverte automatique, ajout manuel et importation en masse. Cliquez ici pour en savoir plus.

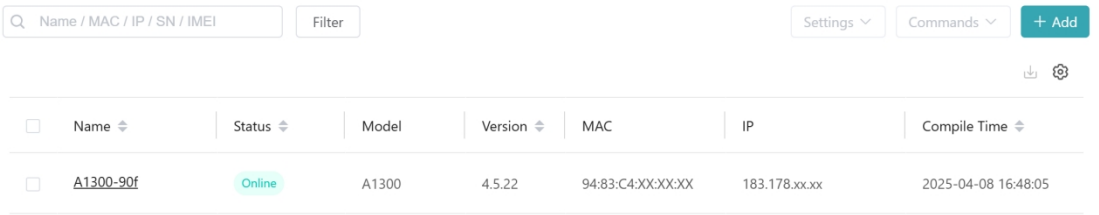
4. Une fois l’association effectuée, revenez à l’interface d’administration Web du routeur, puis accédez à **APPLICATIONS** > **GoodCloud**. Cette page affiche les informations d’association, notamment le nom d’utilisateur et la date et l’heure de l’association.



12.3.2 Gestion de votre routeur

Consultation des informations de l’appareil

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



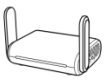
Cliquez sur le nom de l’appareil pour ouvrir sa page de détails. Elle présente les informations de base, les statistiques, la vue d’ensemble du réseau, la liste des clients et la chronologie. Vous pouvez également effectuer des opérations avancées, comme accéder au routeur à distance ou le redémarrer.

A1300-90f Online

Remote GUI | Remote SSH | Reboot Device

Basic Info

Refresh



A1300

Network Mode	Version	MAC Address	IP
Router	4.5.22	94:83:C4:XX:XX:XX	183.178.xx.xx
SN	**Memory Usage**	**Compile Time**	**Up Time**
b5e3**********	43%	2025-04-08 16:48:05	0 days 4 hrs 54 mins

Statistical Data

Refresh

Network Latency

Retest

Poor

360.44 ms	2.16 ms	0 %
Latency	Jitter	Packet Loss

Device Status History

More



Network | Clients List | Share | Cellular Health

Internet

Refresh

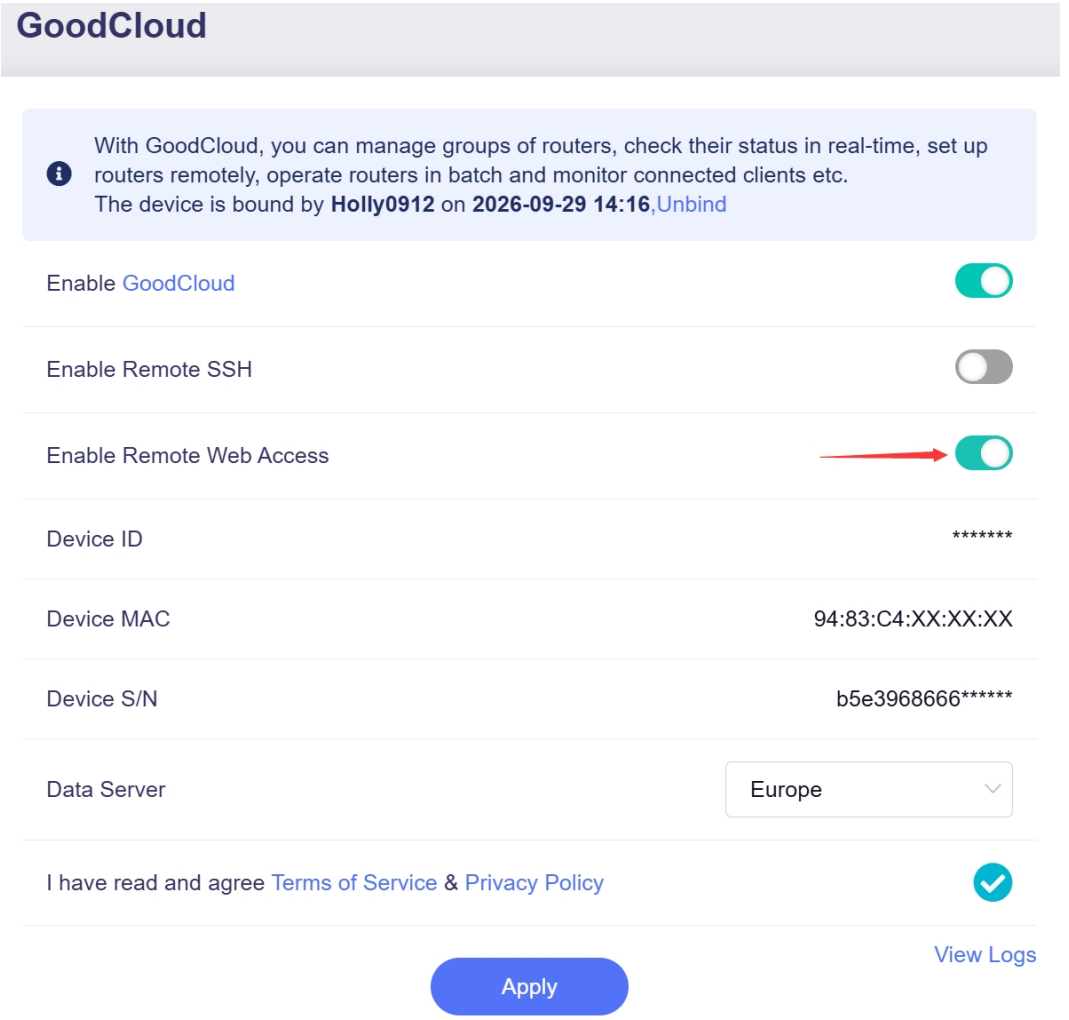
Ethernet1 More
✓ Connected
IP Address 10.100.211.199/22
Protocol DHCP

Repeater More
Disabled
IP Address --
SSID --

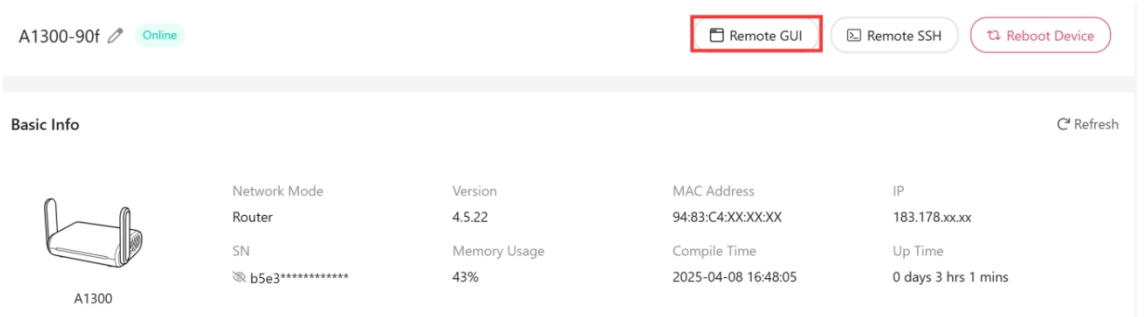
Tethering More
Disabled
IP Address --
Device List Details

Accès Web à distance

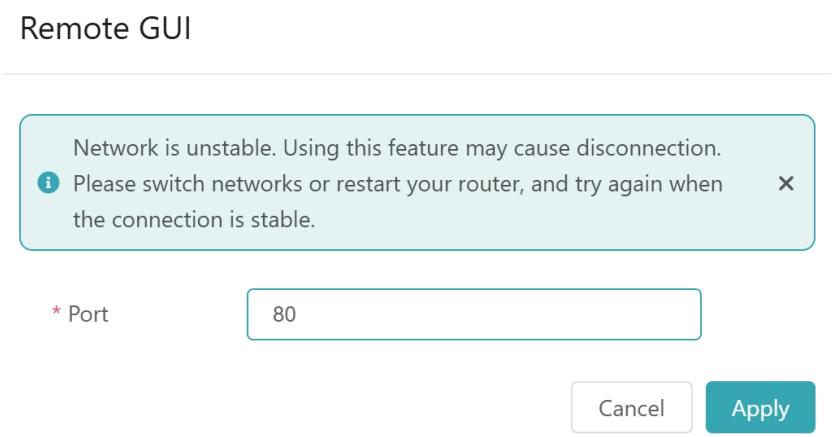
1. Connectez-vous à l'interface d'administration Web du routeur, puis accédez à **APPLICATIONS** > **GoodCloud**, activez **Accès Web à distance (Remote Web Access)**, puis cliquez sur **Appliquer (Apply)**.



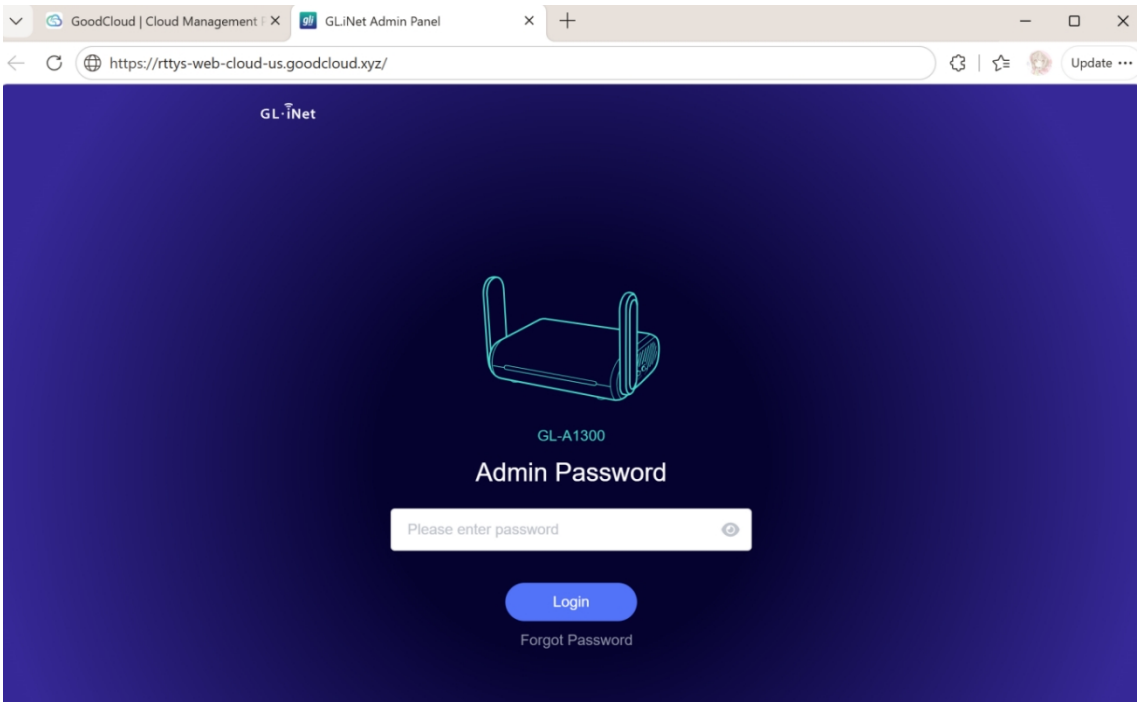
2. Connectez-vous à GoodCloud et ouvrez **Appareils (Devices)** > **Appareils associés (Bound Devices)**. Cliquez sur l'appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
3. Sur cette page, cliquez sur le bouton **Interface à distance (Remote GUI)** dans l'angle supérieur droit.



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

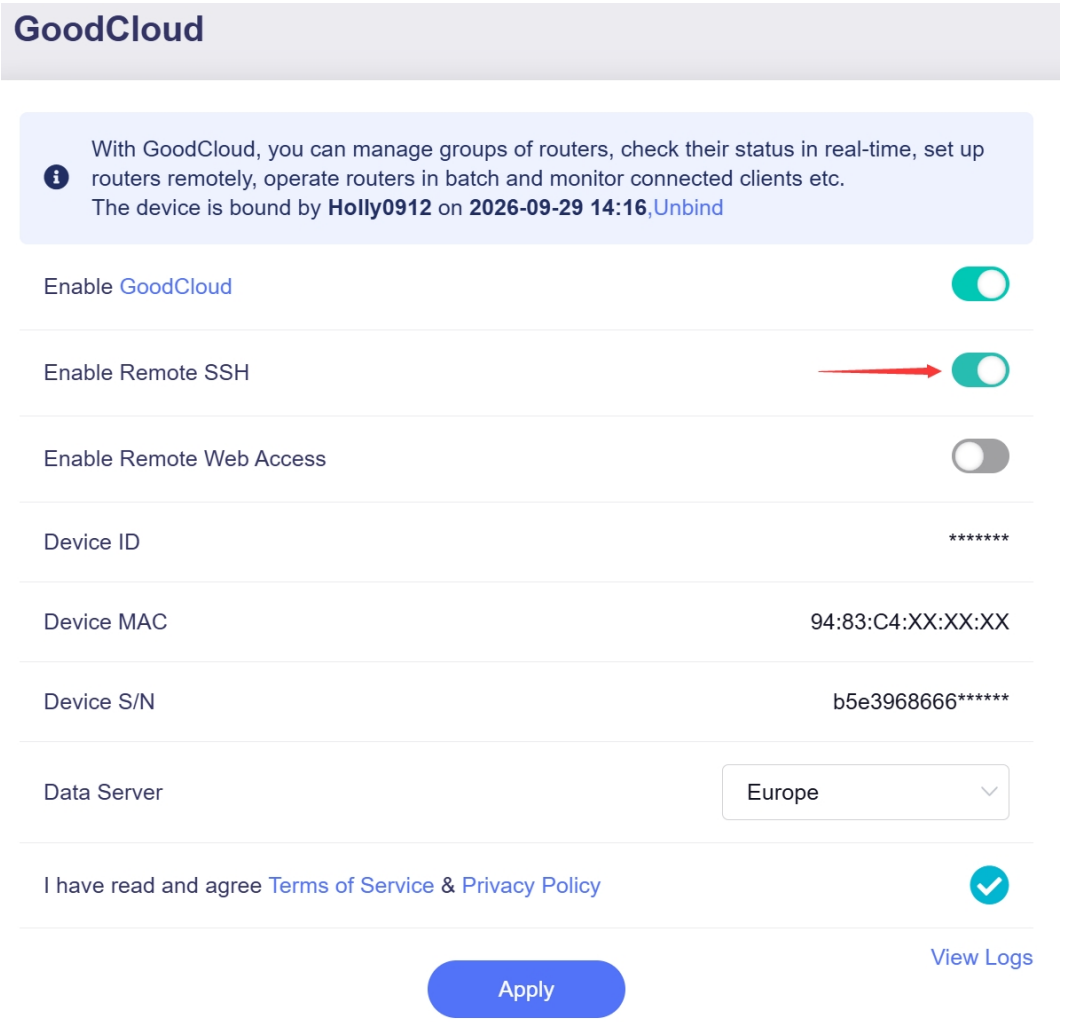


5. La page de connexion du routeur s’ouvre. Saisissez le mot de passe administrateur pour accéder à distance à l’interface d’administration Web.

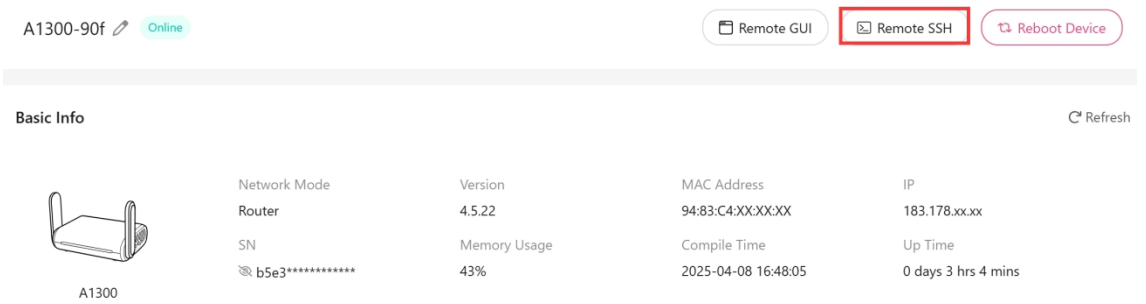

GoodCloud | Cloud Management
GL.iNet Admin Panel
https://rttys-web-cloud-us.goodcloud.xyz/
Update
GL·iNet
GL-A1300
Admin Password
Please enter password
Login
Forgot Password

SSH à distance

1. Connectez-vous à l'interface d'administration Web du routeur, puis accédez à **APPLICATIONS** > **GoodCloud**, activez **SSH à distance (Remote SSH)**, puis cliquez sur **Appliquer (Apply)**.



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



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

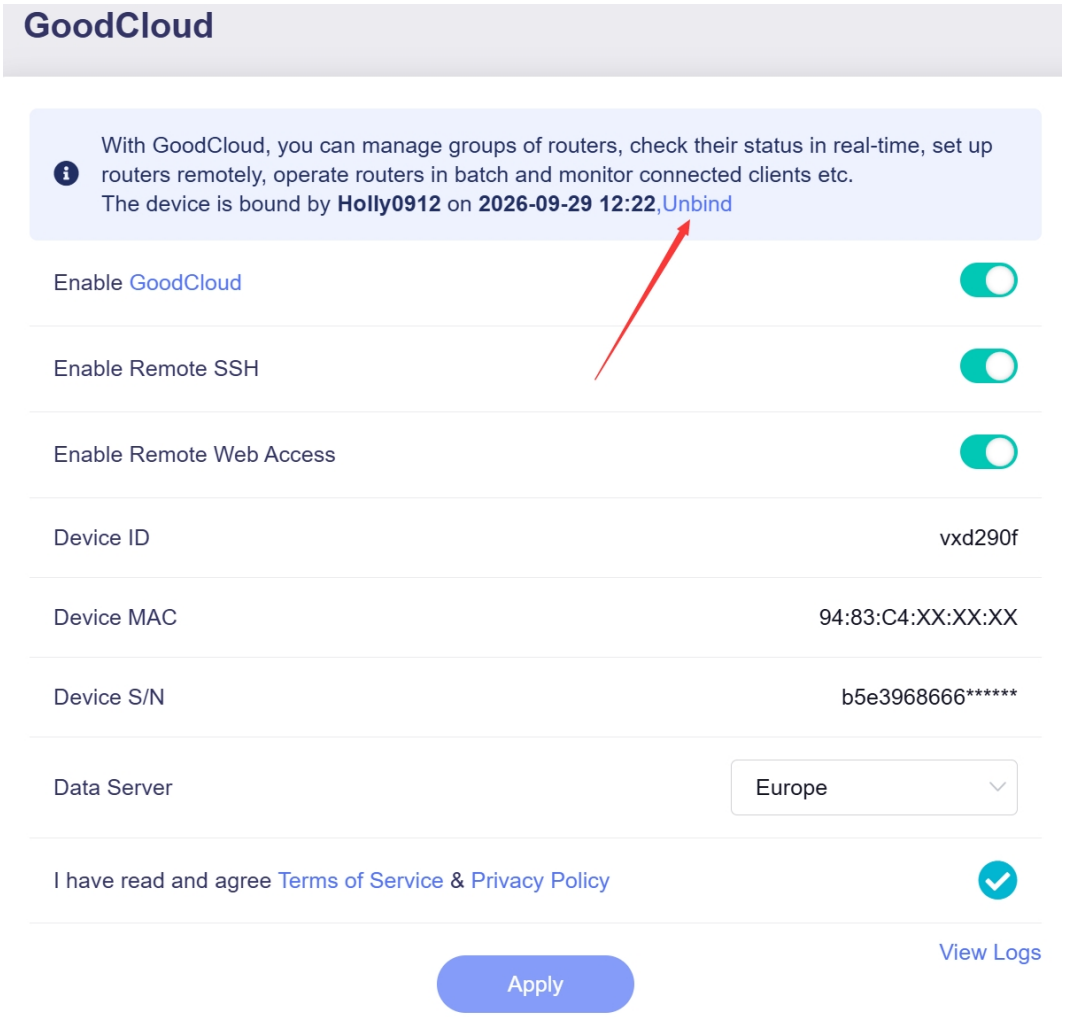
```
GL-A1300 login: root
Password:


BusyBox v1.33.2 (2022-02-16 20:29:10 UTC) built-in shell (ash)

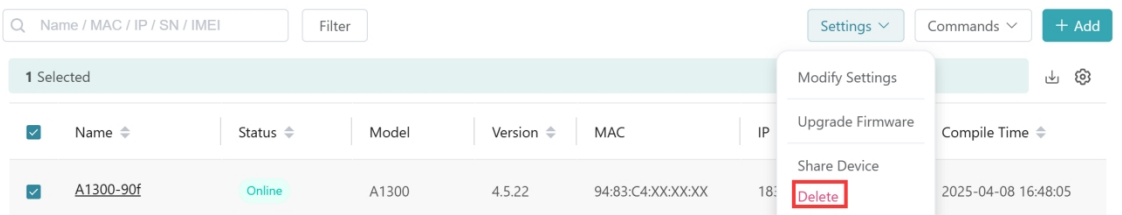
  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 21.02.2, r16495-bf0c965af0
 -----------------------------------------------------
root@GL-A1300:~#
```

12.3.3 Dissociation de l’appareil

Dans l’interface d’administration Web du routeur, cliquez sur **Dissocier (Unbind)**. L’appareil est alors dissocié de votre compte GoodCloud.



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



12.4 Stockage réseau

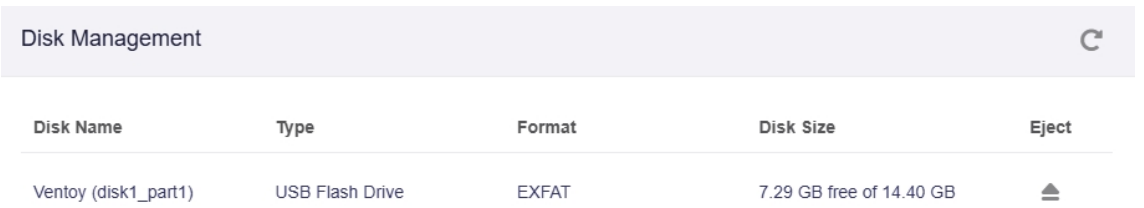
Le stockage réseau permet de partager des fichiers sans fil entre appareils en branchant un support USB ou une carte SD au routeur. Le support devient un lecteur réseau partagé, accessible aux appareils connectés par Wi-Fi.

Slate Plus possède un port USB compatible avec les clés USB et les disques durs externes portables. Vous pouvez configurer Samba, WebDAV ou DLNA pour ces périphériques de stockage, qui prennent en charge les formats courants tels que NTFS, FAT32 et EXT4.

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

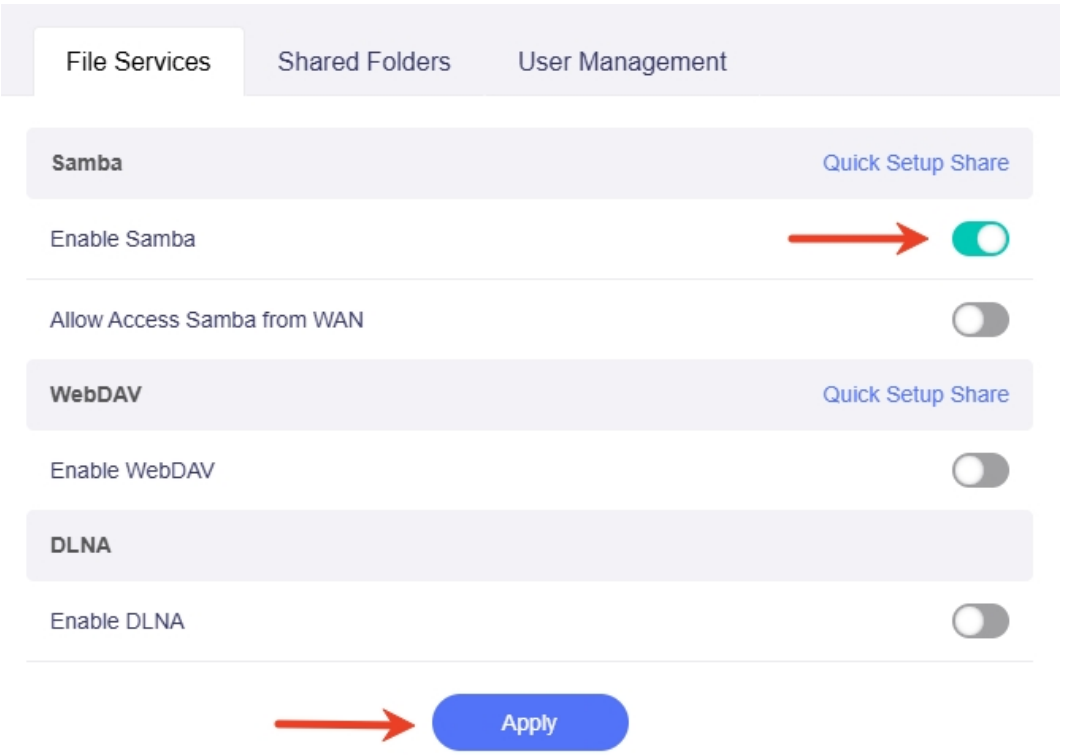
12.4.1 Branchement du stockage

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.



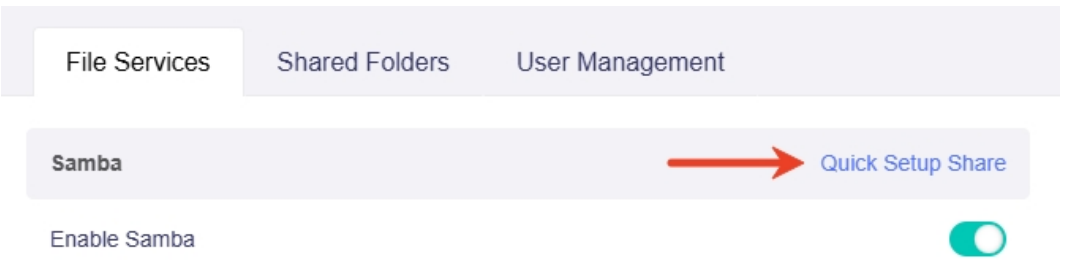
12.4.2 Configuration de Samba

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

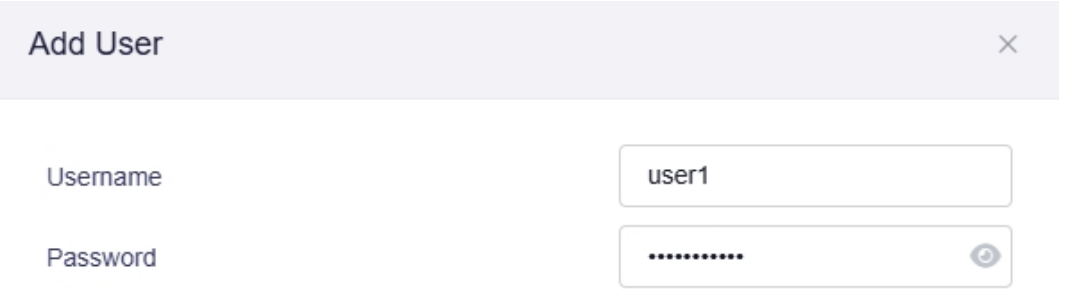


   - **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** : activez cette option pour que les appareils en amont accèdent à Samba.

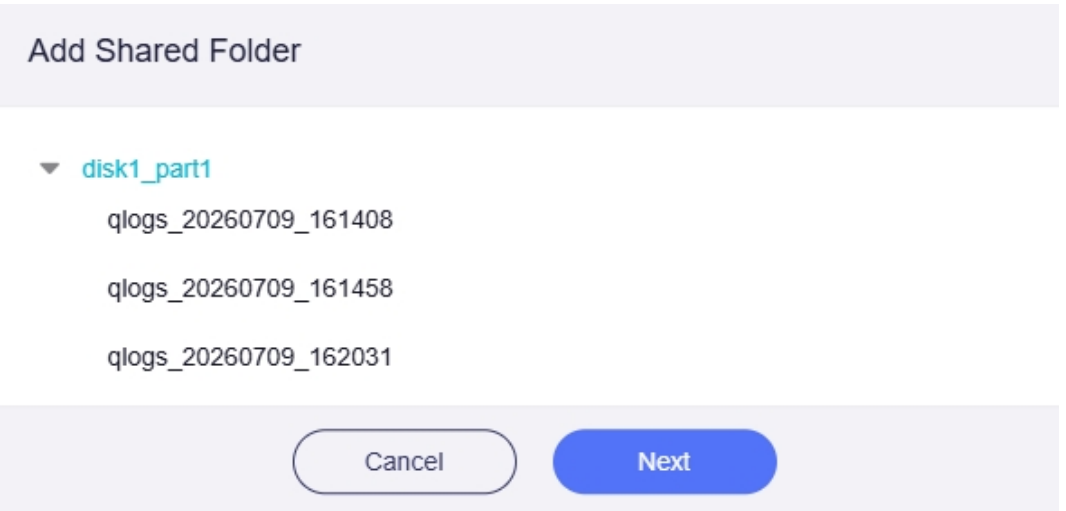
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



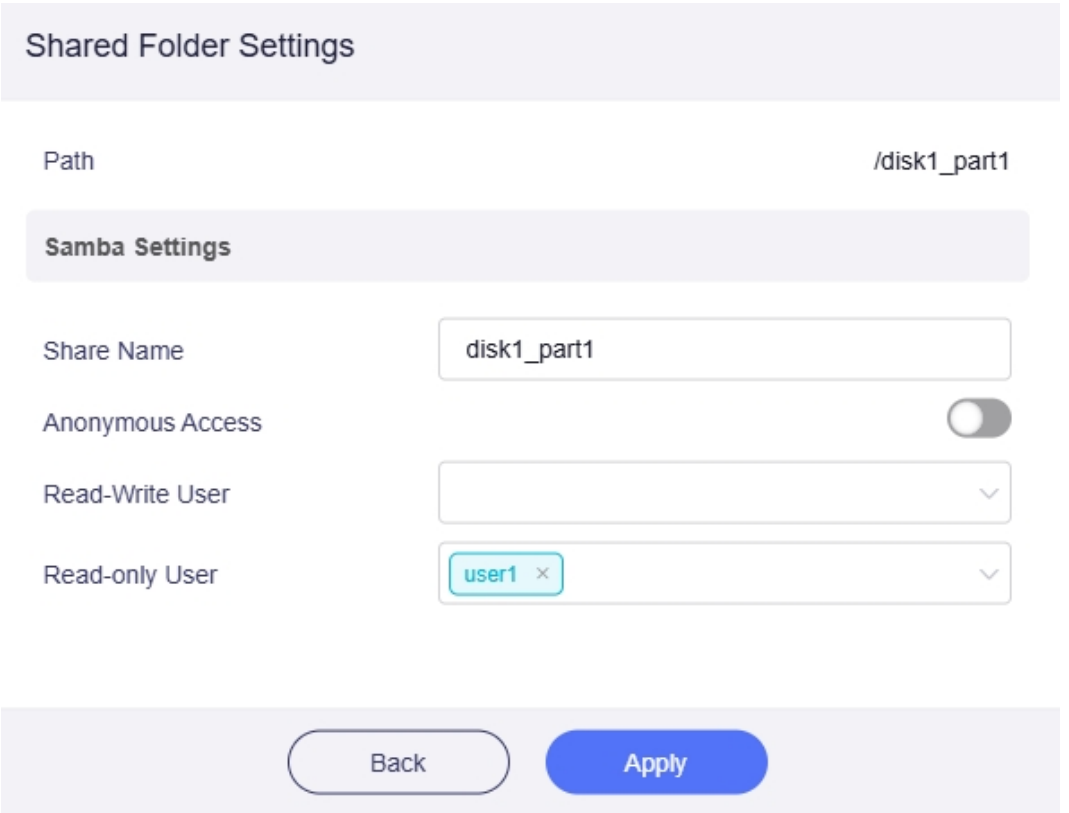
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



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.



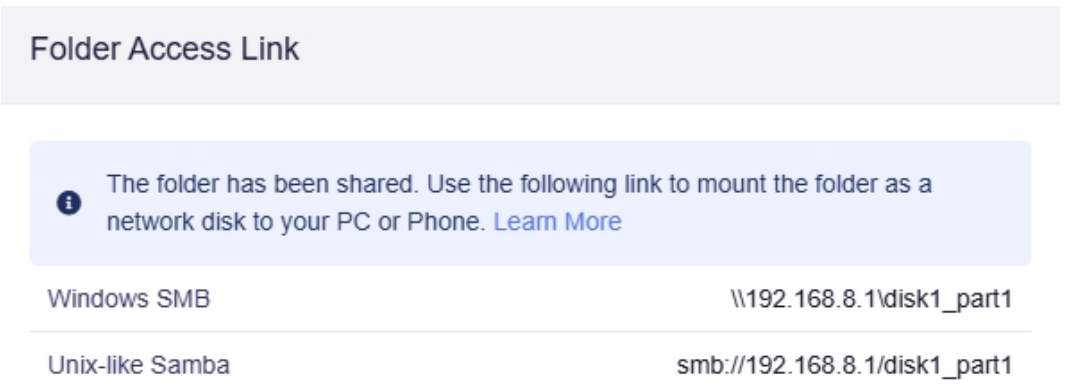
5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**. Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez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



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

6. Récupérez le lien d'accès au dossier.

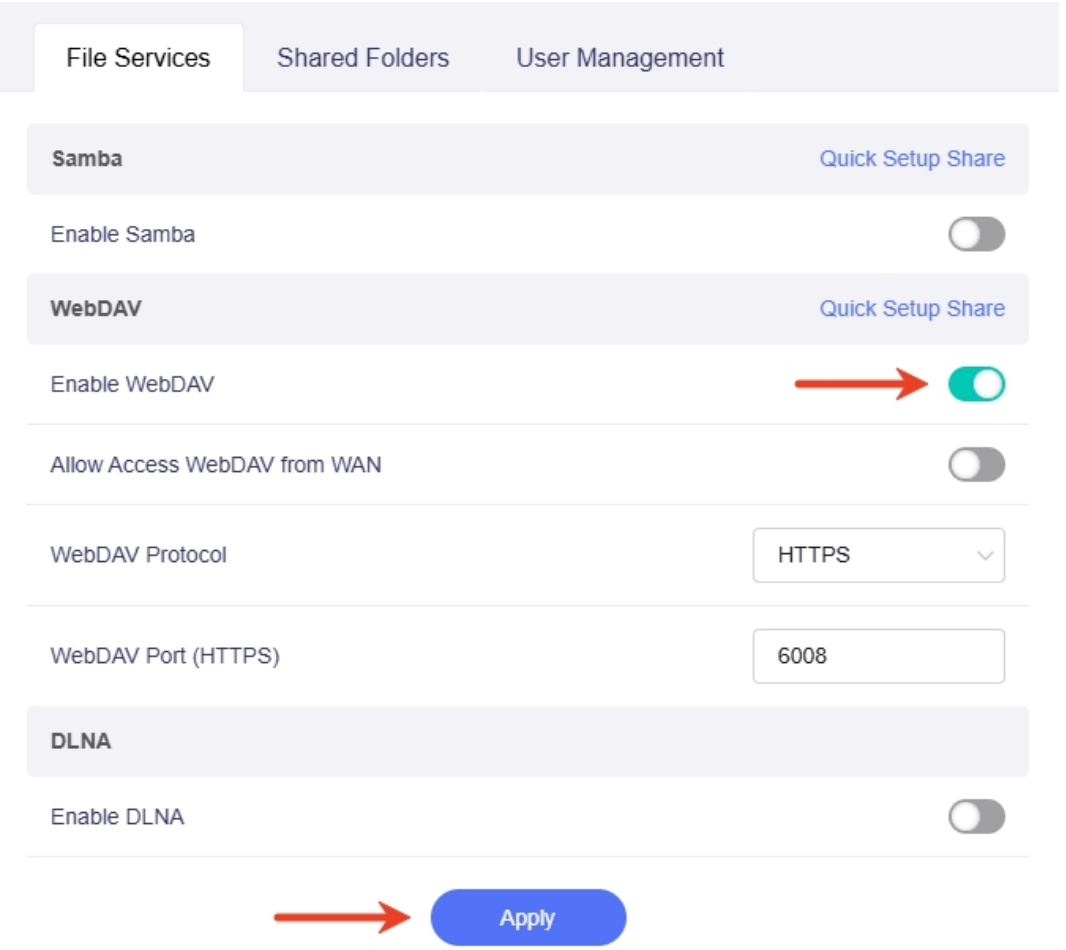
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via Samba.



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.

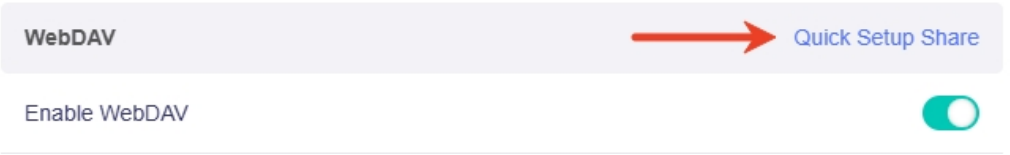
12.4.3 Configuration de WebDAV

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

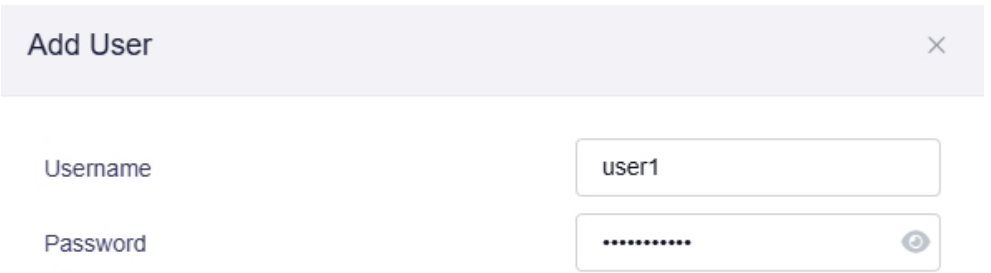


- **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** : activez cette option pour que les appareils en amont accèdent au service WebDAV.
- **Protocole WebDAV (WebDAV Protocol)** : HTTP n'est pas chiffré ; utilisez-le à vos risques. HTTPS est chiffré et utilise un certificat autosigné.
-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

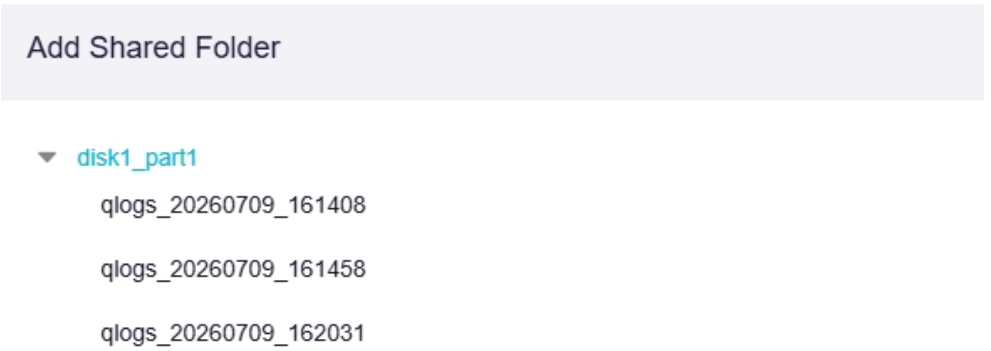
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



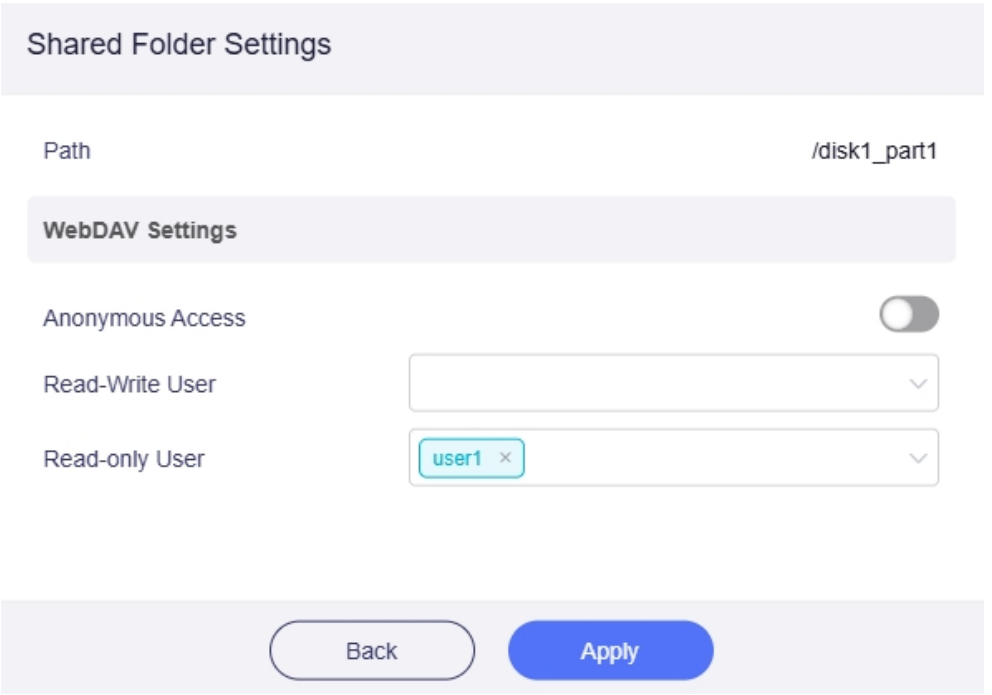
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



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



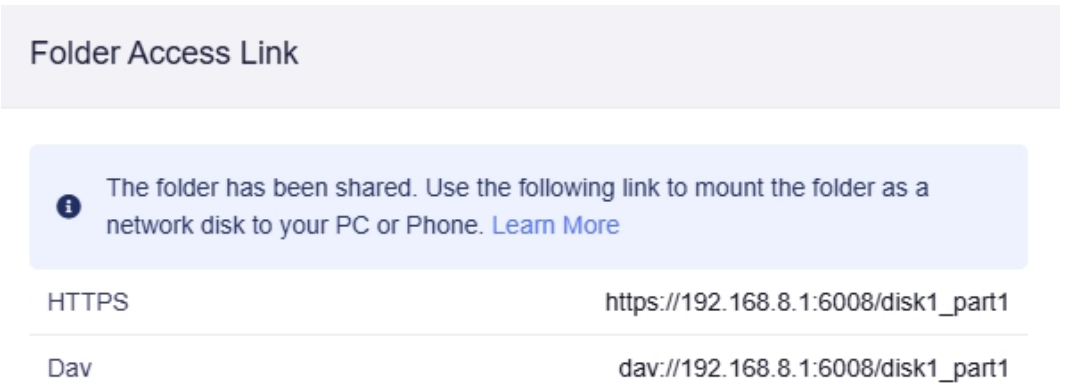
5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**.
   Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis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



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

6. Récupérez le lien d'accès au dossier.

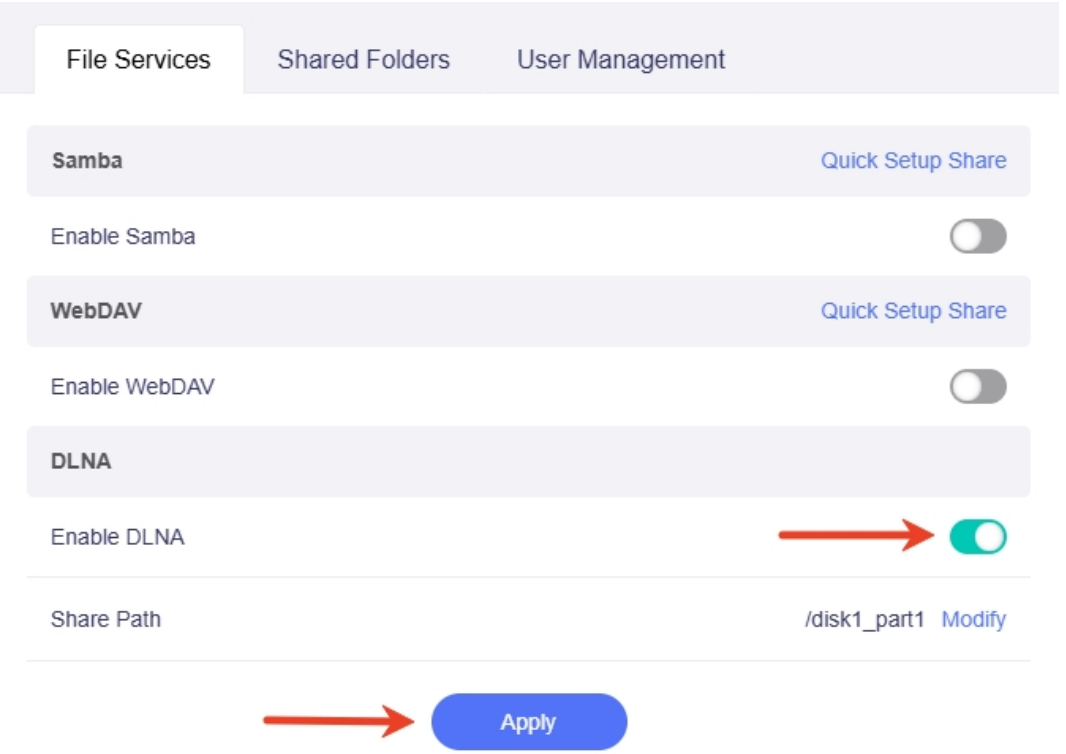
   La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via WebDAV.



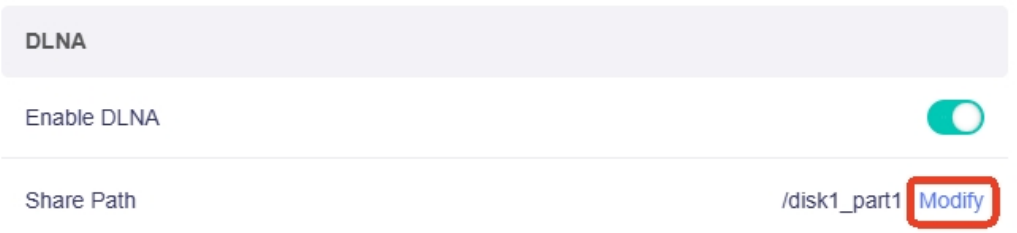
Remarque : si vous activez **Autoriser WebDAV depuis le WAN (Allow Access WebDAV from WAN)** et accédez au dossier depuis le réseau en amont, remplacez l'IP du routeur dans le lien, 192.168.8.1 par défaut, par son IP WAN affichée sur la page INTERNET.

12.4.4 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.



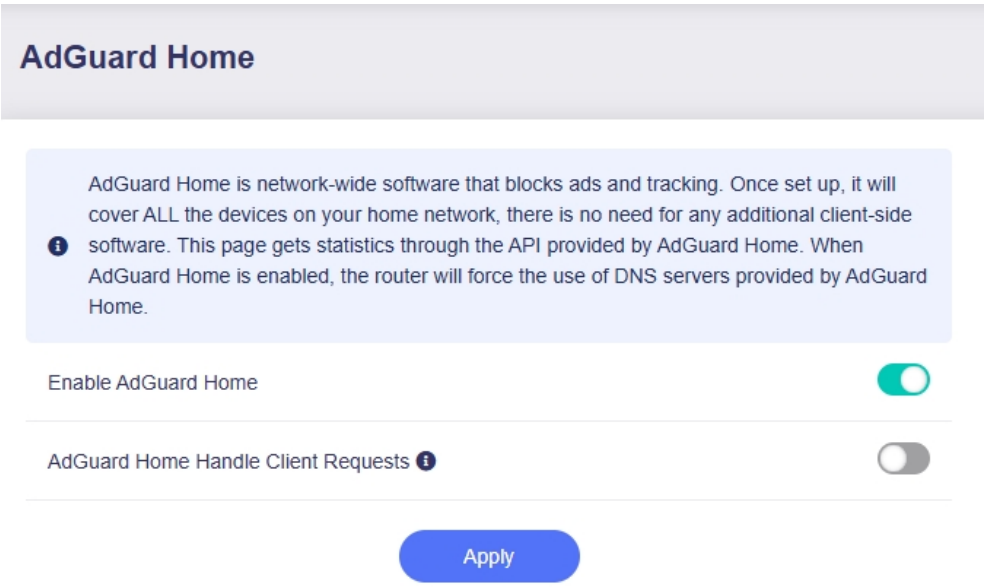
3. Connectez votre téléviseur intelligent au routeur. Il détecte automatiquement le serveur DLNA.

12.5 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.

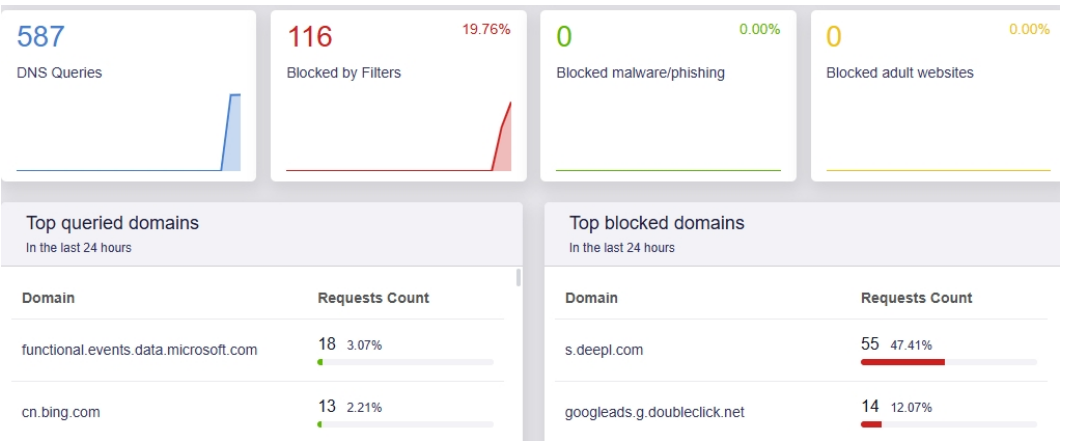
Suivez les étapes ci-dessous pour configurer AdGuard Home.

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

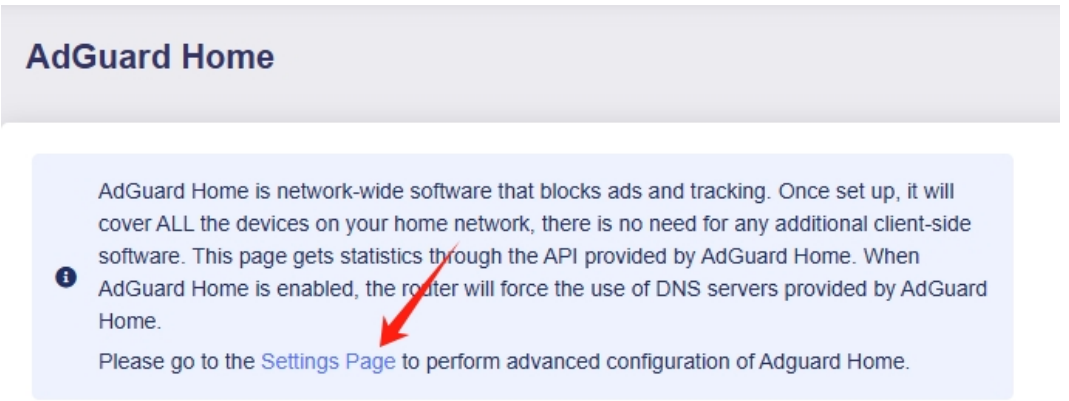


   - **AdGuard Home traite les requêtes clients (AdGuard Home Handles Client Requests)** : les requêtes DNS des clients sont alors traitées directement par AdGuard Home. Cela empêche toutefois les règles VPN fondées sur les domaines de fonctionner.

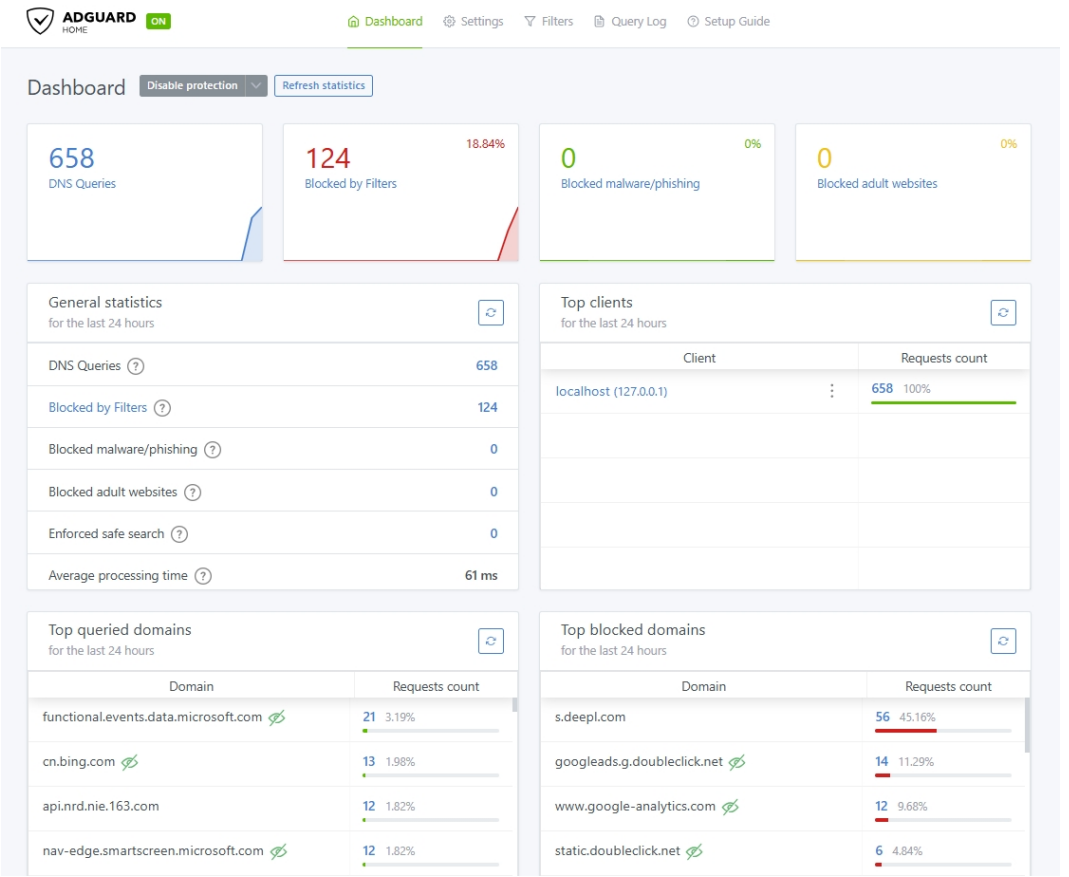
2. La page charge automatiquement les statistiques DNS, comme les requêtes et les domaines bloqués, via l'API d'AdGuard Home.



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%

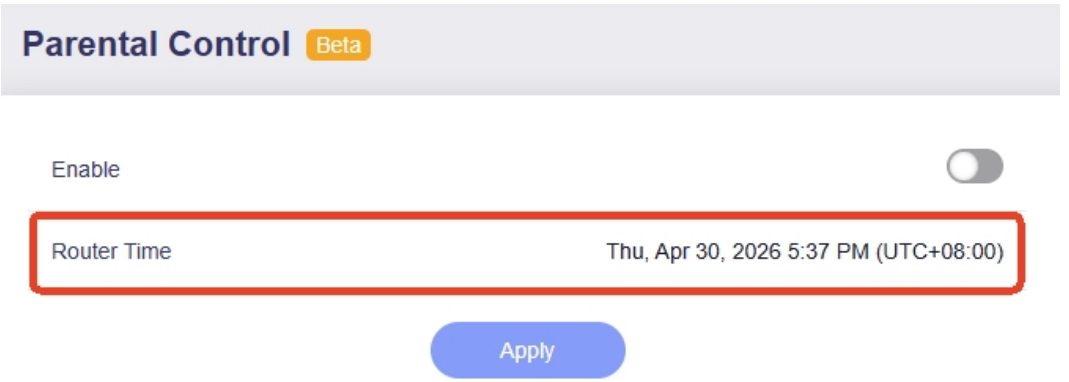
12.6 Contrôle parental

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.

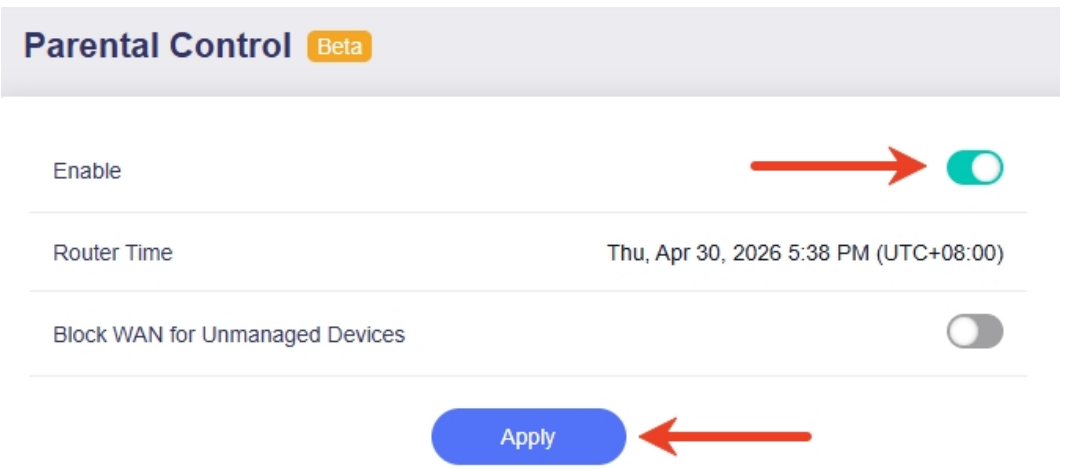
12.6.1 Configuration rapide

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.



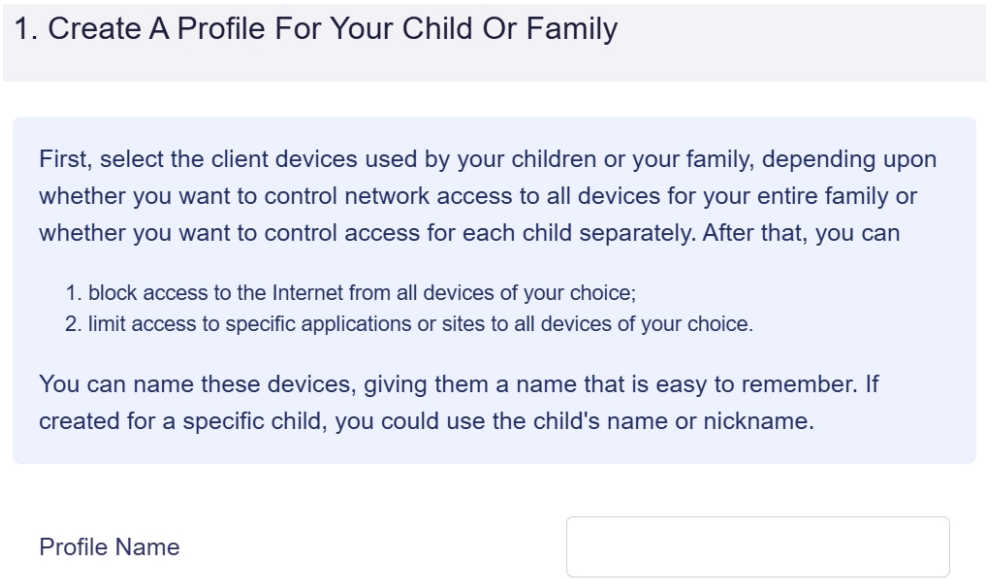
- **Bloquer le WAN pour les appareils non gérés (Block WAN for Unmanaged Devices)** : bloque l'accès Internet des appareils absents de la liste du contrôle parental.

Voici un exemple d’utilisation.

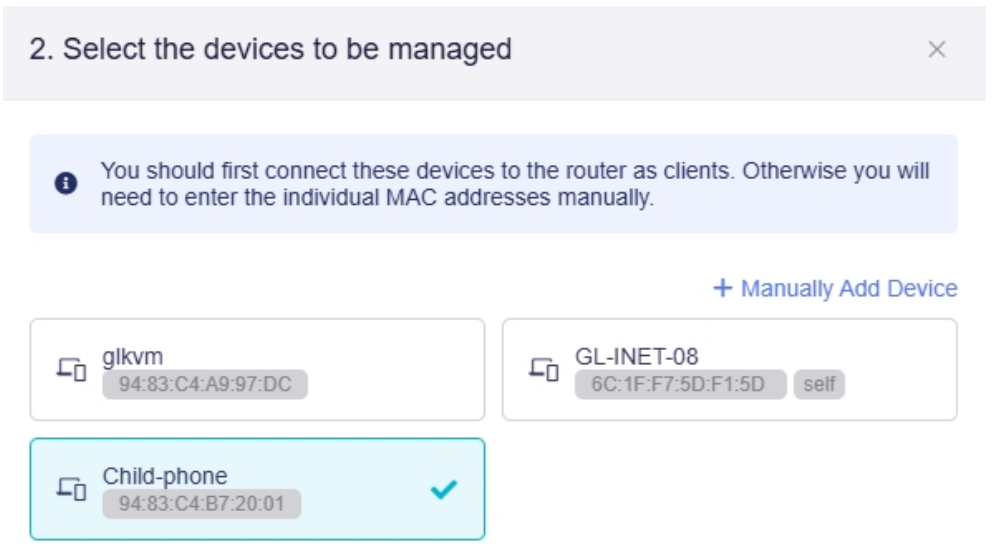
Scénario : les appareils de ce profil peuvent accéder à Internet uniquement pour étudier de 8 h à 11 h en semaine, et pour jouer de 18 h à 20 h le week-end. L’accès Internet est bloqué par défaut en dehors de ces plages.

Étapes de configuration :

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

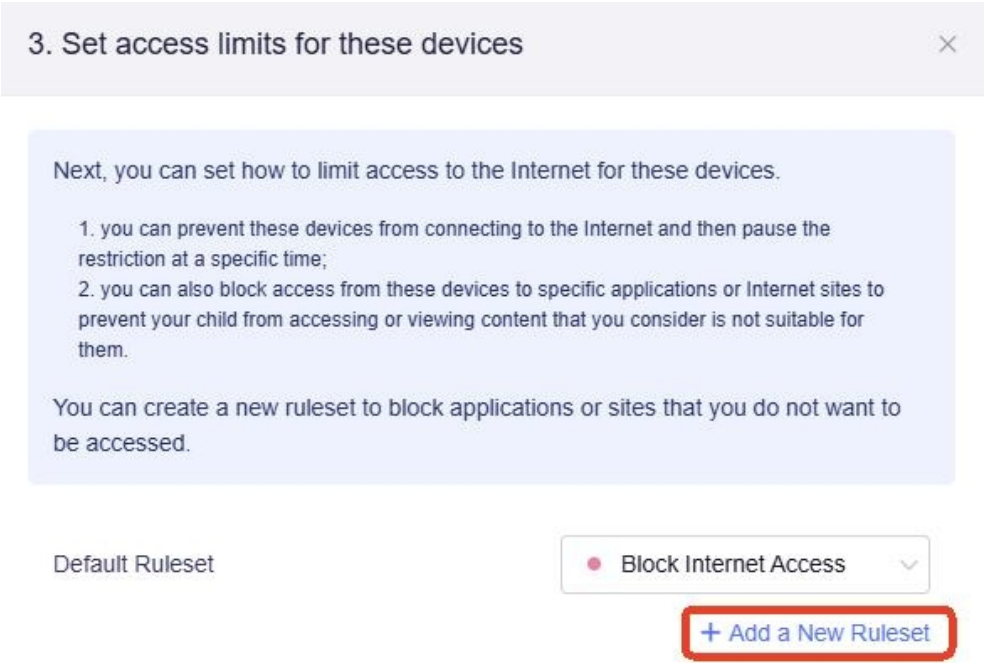


2. Sélectionnez les appareils à gérer. Connectez-les d’abord au routeur. S’ils n’y ont jamais été connectés, ajoutez-les manuellement avec leur adresse MAC.

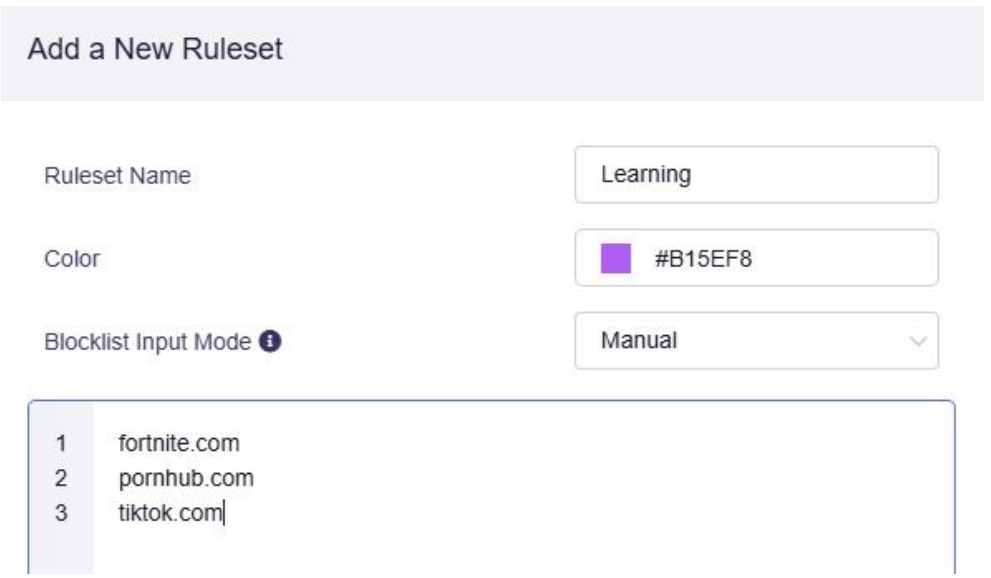


3. Définissez les limites d’accès.

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)**.

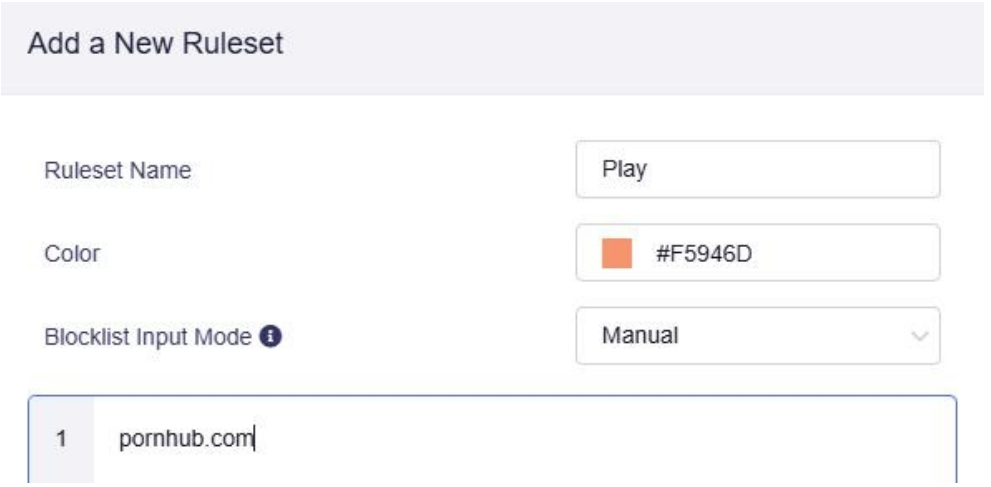


Définissez le nom, par exemple Étude, et la couleur du jeu de règles. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.

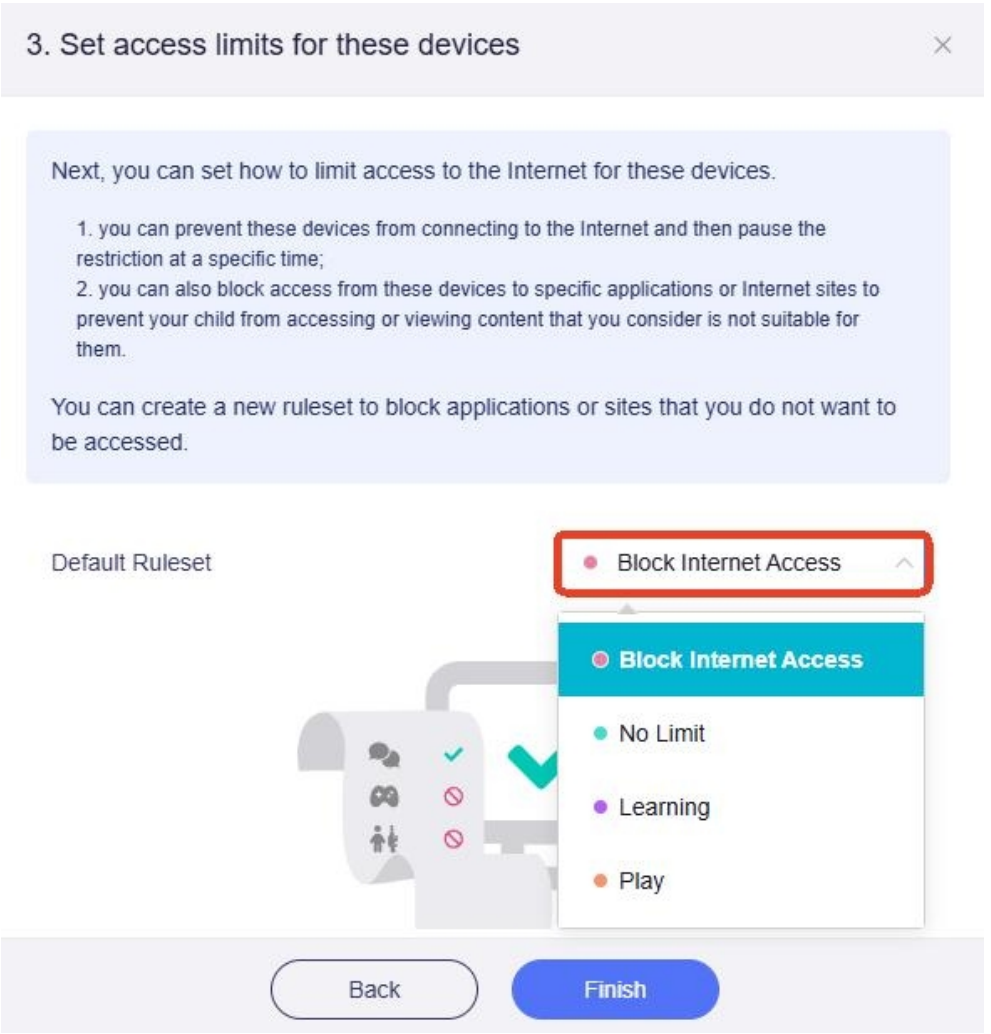


Remarque : les domaines de la liste de blocage englobent leurs sous-domaines. Par exemple, « example.com » inclut aussi « subdomain.example.com ».

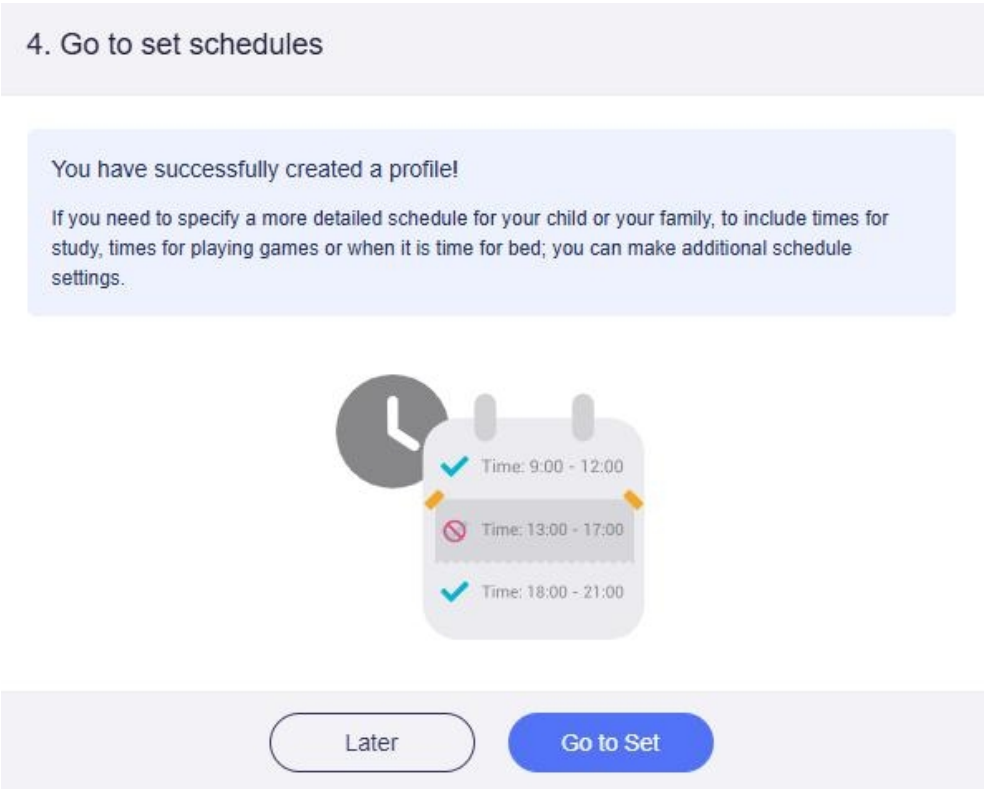
Créez de la même façon un autre jeu de règles. Définissez son nom, par exemple Jeu, et sa couleur. Saisissez les sites à bloquer, puis cliquez sur **Appliquer (Apply)**.



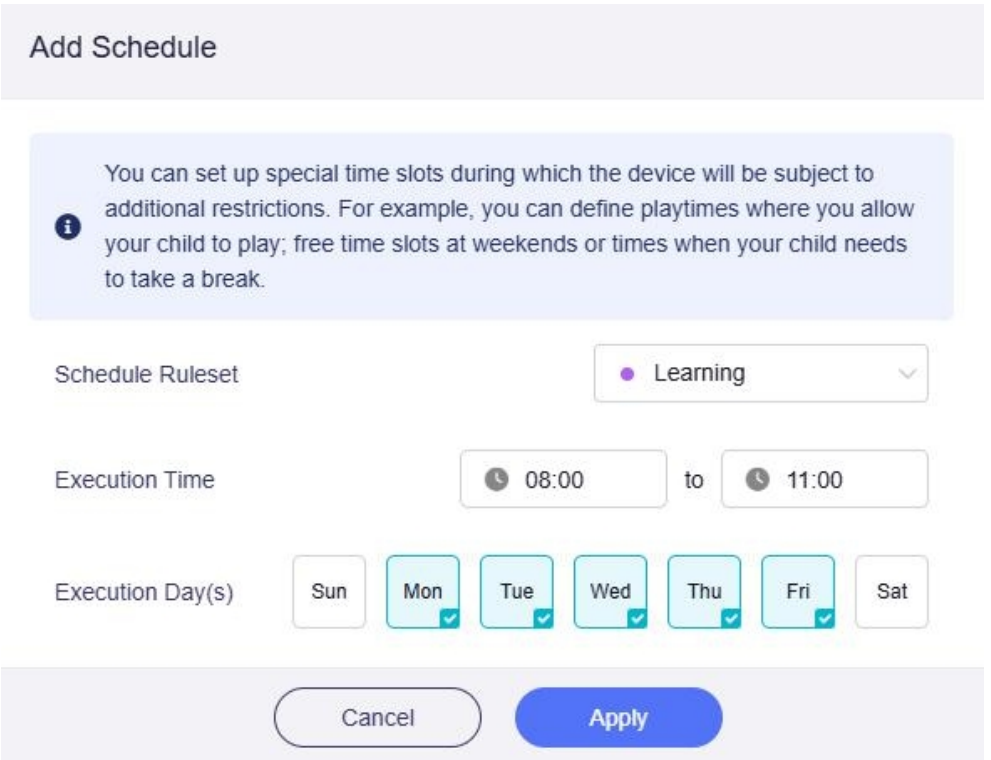
Vous disposez alors de quatre jeux de règles. Sélectionnez **Bloquer l’accès Internet (Block Internet Access)** comme **Jeu de règles par défaut (Default Ruleset)**, puis cliquez sur **Terminer (Finish)**.



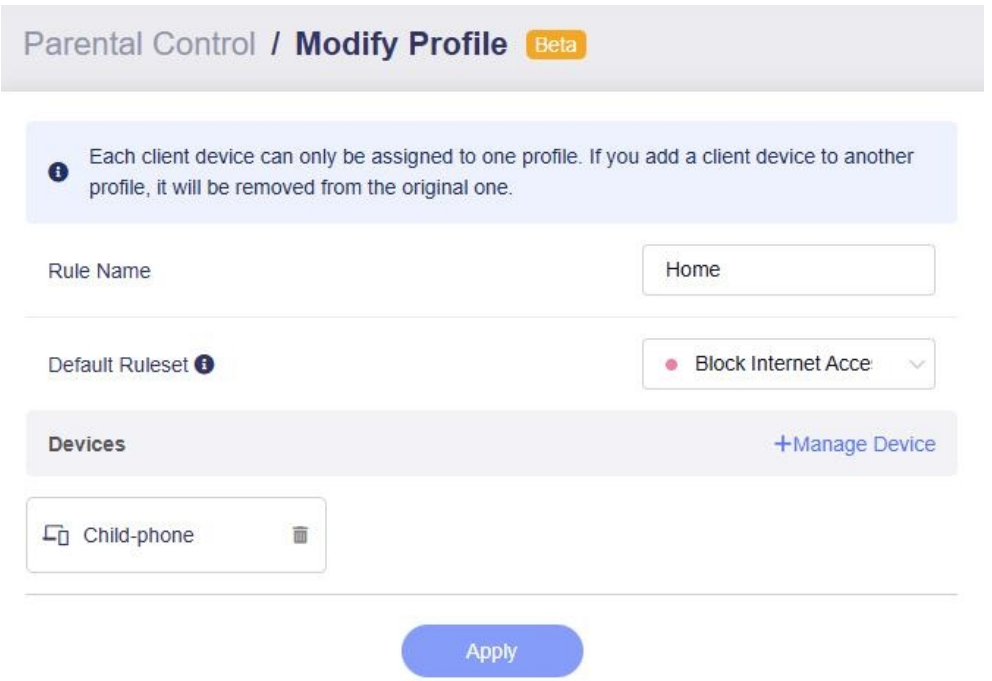
4. Définissez ensuite le planning du profil. Cliquez sur **Configurer (Go to Set)**.



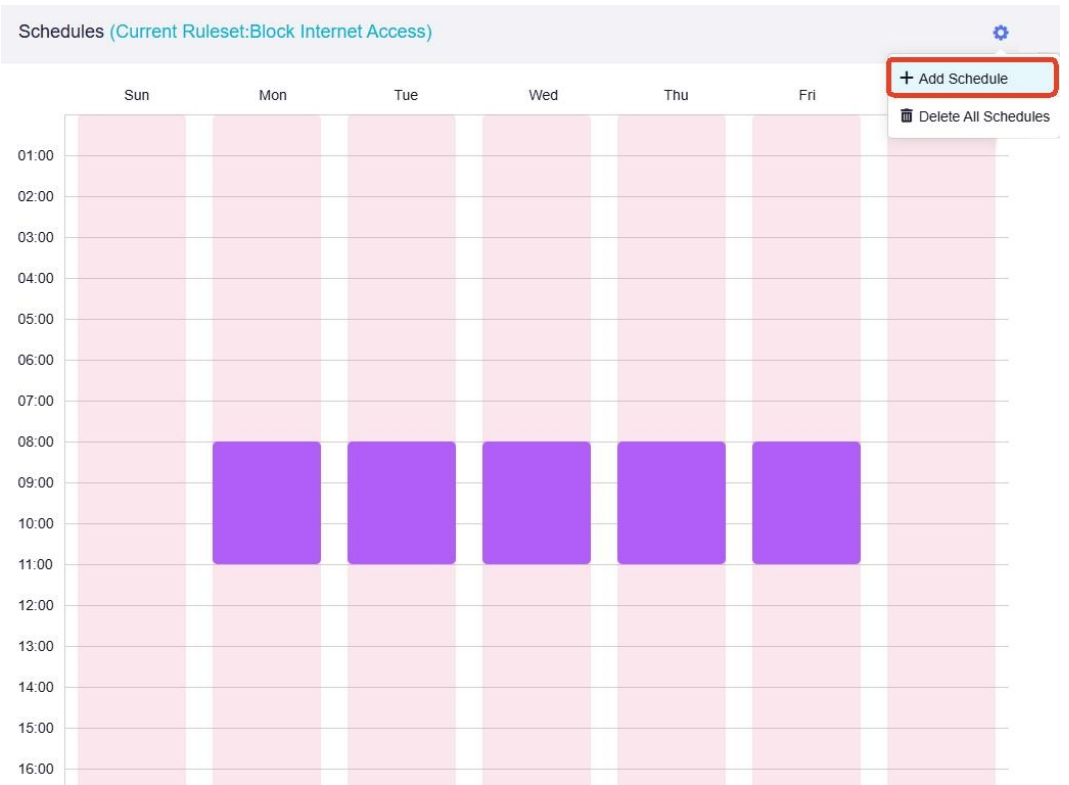
Ajoutez le jeu de règles **Étude (Learning)** au planning. Définissez l'**horaire d'exécution (Execution Time)** de 8 h à 11 h en semaine, puis cliquez sur **Appliquer (Apply)**.



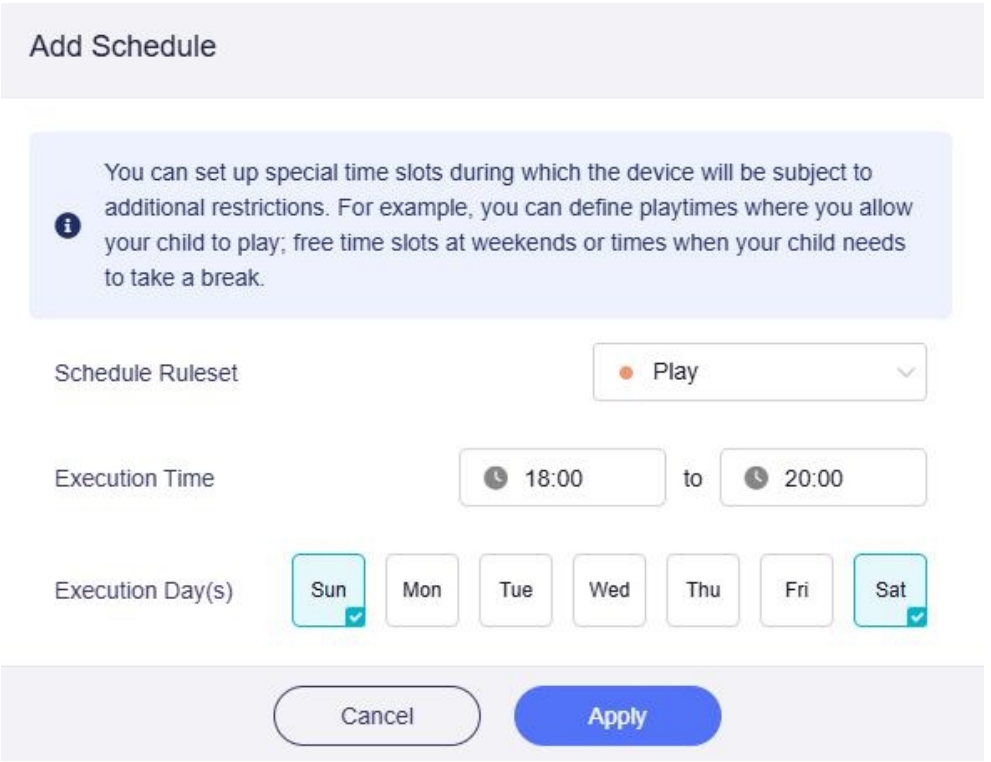
5. La page de modification du profil créé s'ouvre.



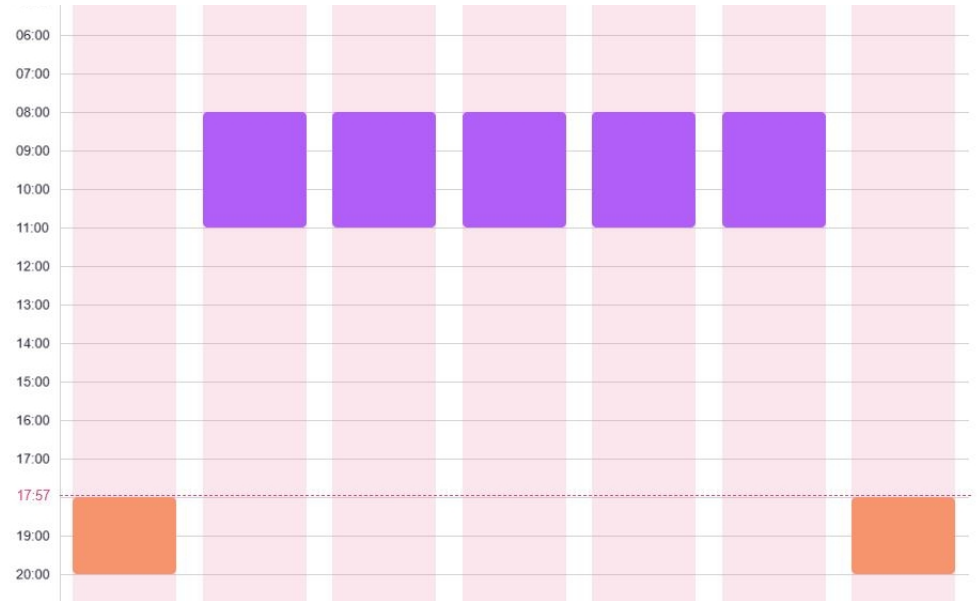
En bas de la page, le planning créé apparaît. Cliquez sur l'engrenage en haut à droite, puis sur **Ajouter une plage horaire (Add Schedule)**.



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)**.



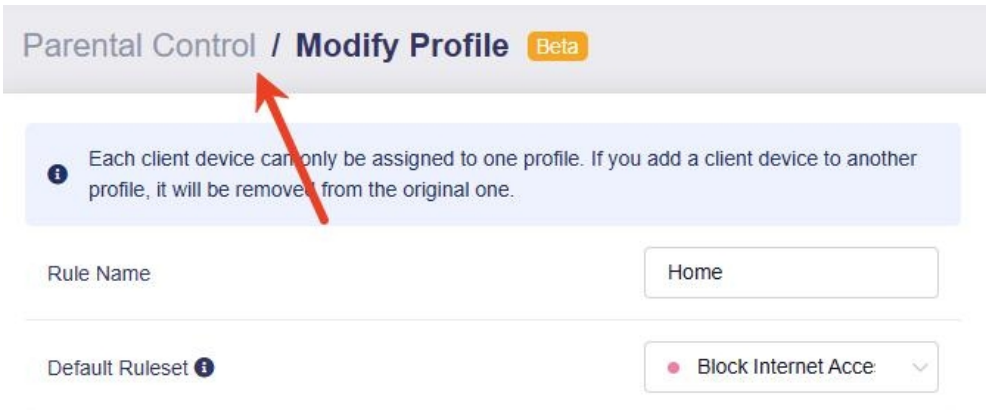
Le jeu de règles Jeu est ajouté au planning.



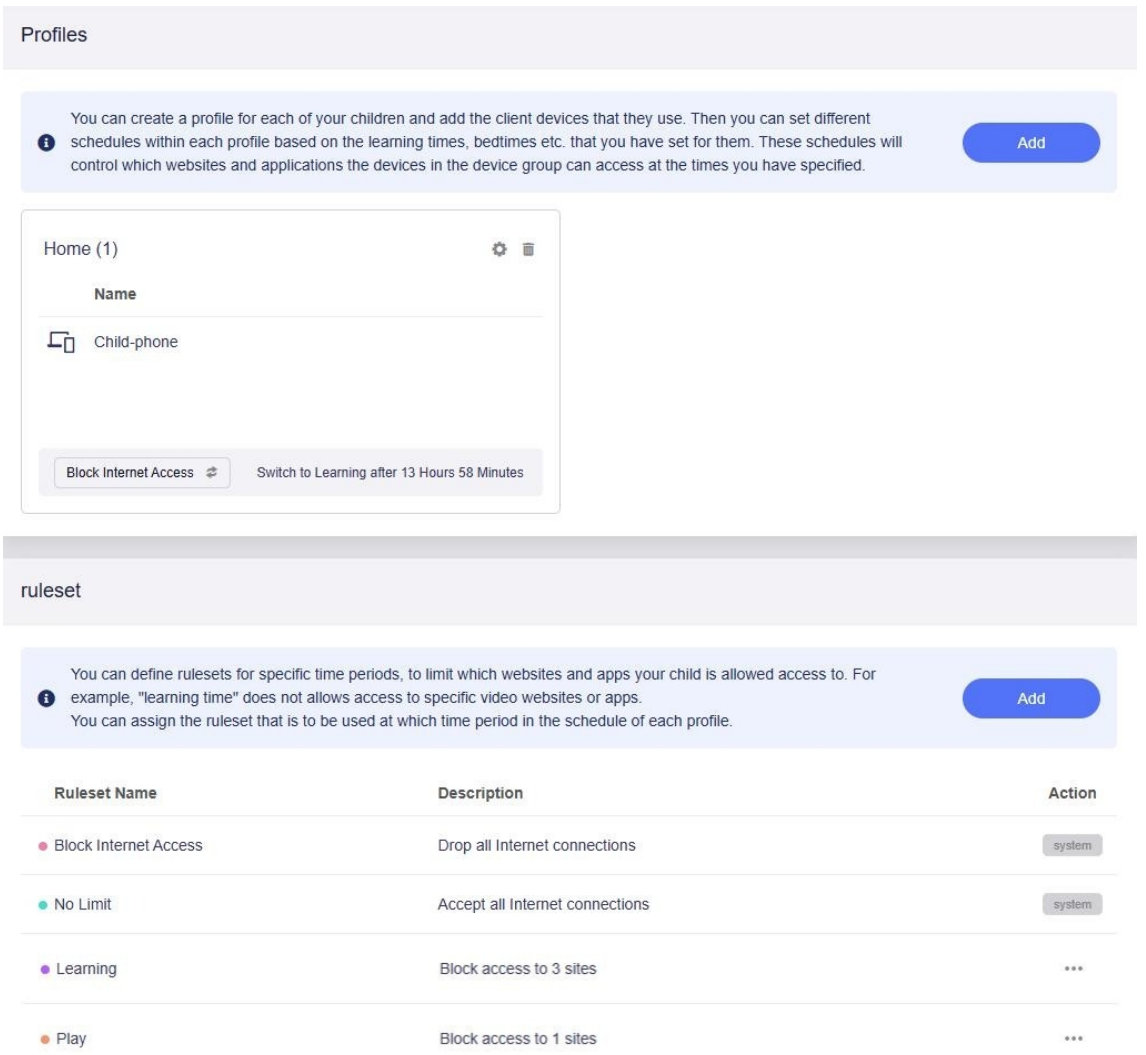
Conseils :

- 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.



12.6.2 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.

12.7 ZeroTier

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

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

Remarque :

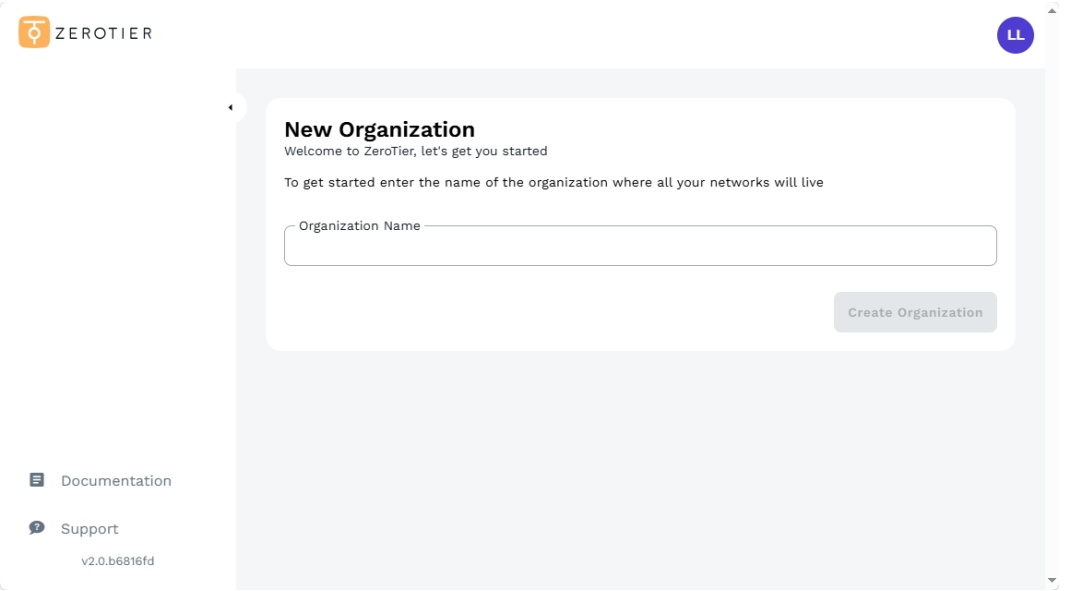
1. Il est déconseillé d'utiliser ZeroTier simultanément avec les fonctionnalités ou services suivants, car cela peut entraîner des conflits de routage : client OpenVPN, client WireGuard, GoodCloud Site to Site et Tailscale.
2. Cette fonction est actuellement en version bêta et peut présenter des anomalies.

12.7.1 Configuration de ZeroTier

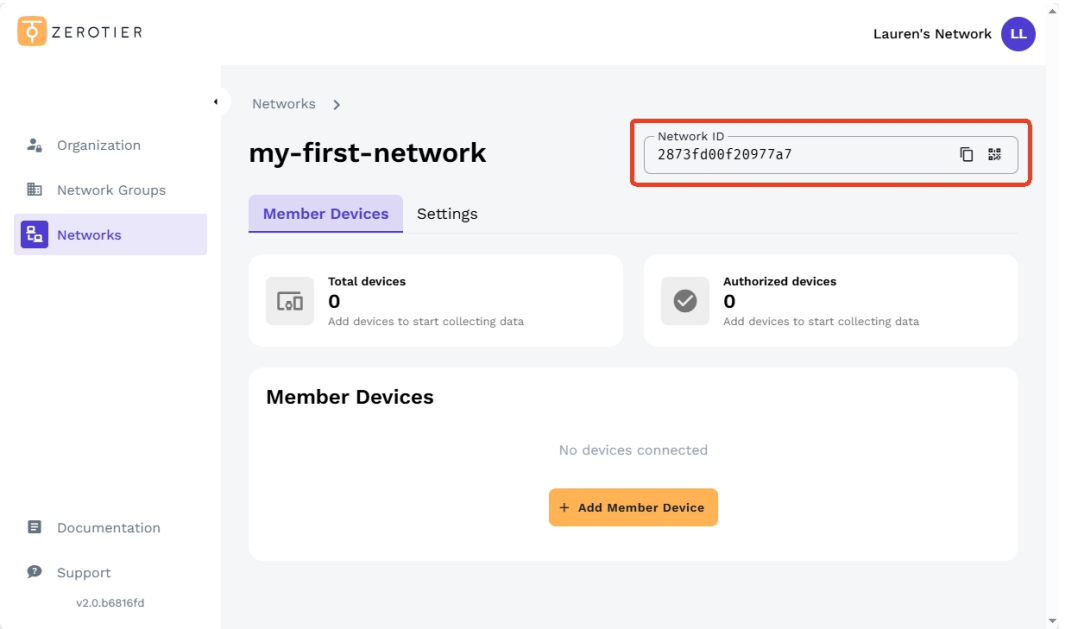
ZeroTier Central existe en deux versions : New Central et Legacy Central.

Les étapes suivantes utilisent New Central.

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

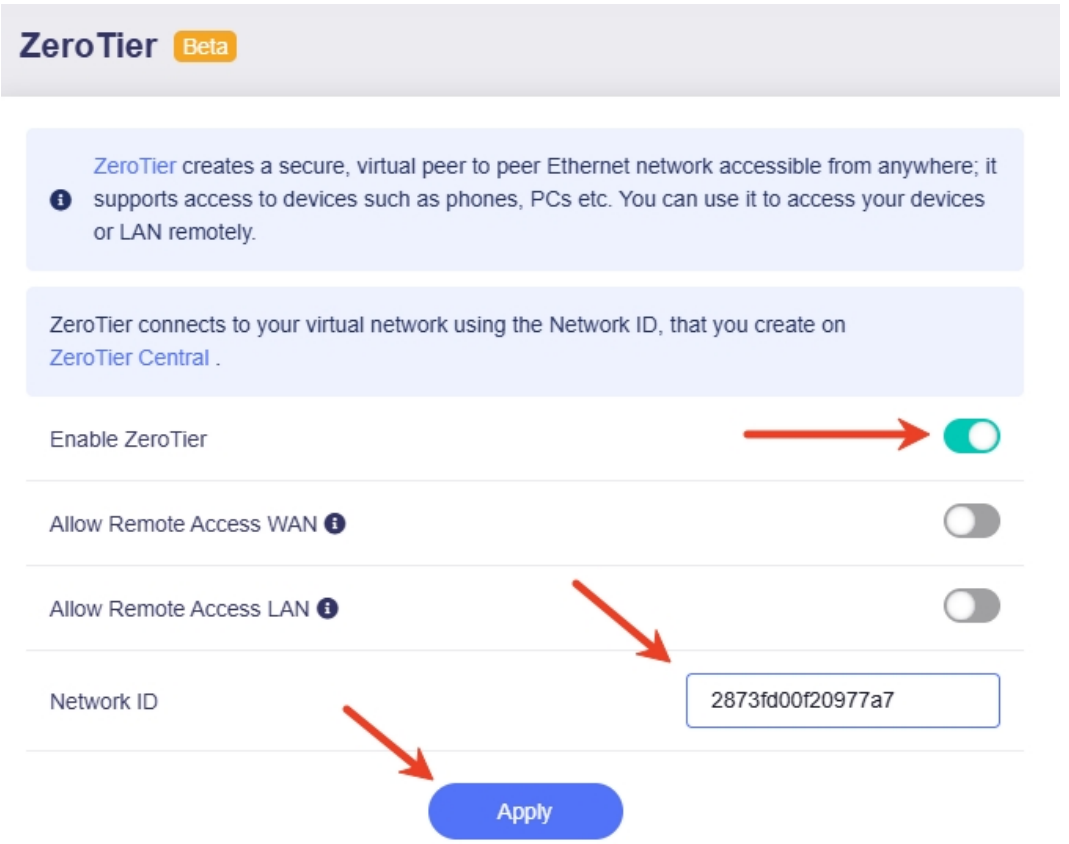


3. Choisissez une offre. L'exemple utilise l'**offre Personal**, qui comprend 10 appareils, un administrateur et un réseau. Pour ajouter des réseaux, des appareils, des routes personnalisées ou un DNS, choisissez une autre offre payante.
4. Votre réseau ZeroTier est créé.

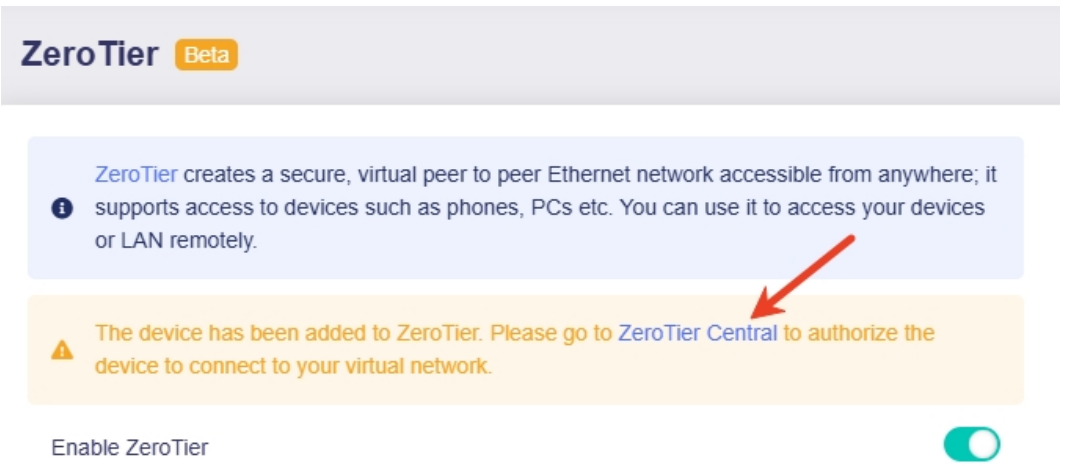


Notez l'**identifiant du réseau (Network ID)**, une suite alphanumérique de 16 caractères affichée en haut à droite. Il sera nécessaire pour connecter les autres appareils.

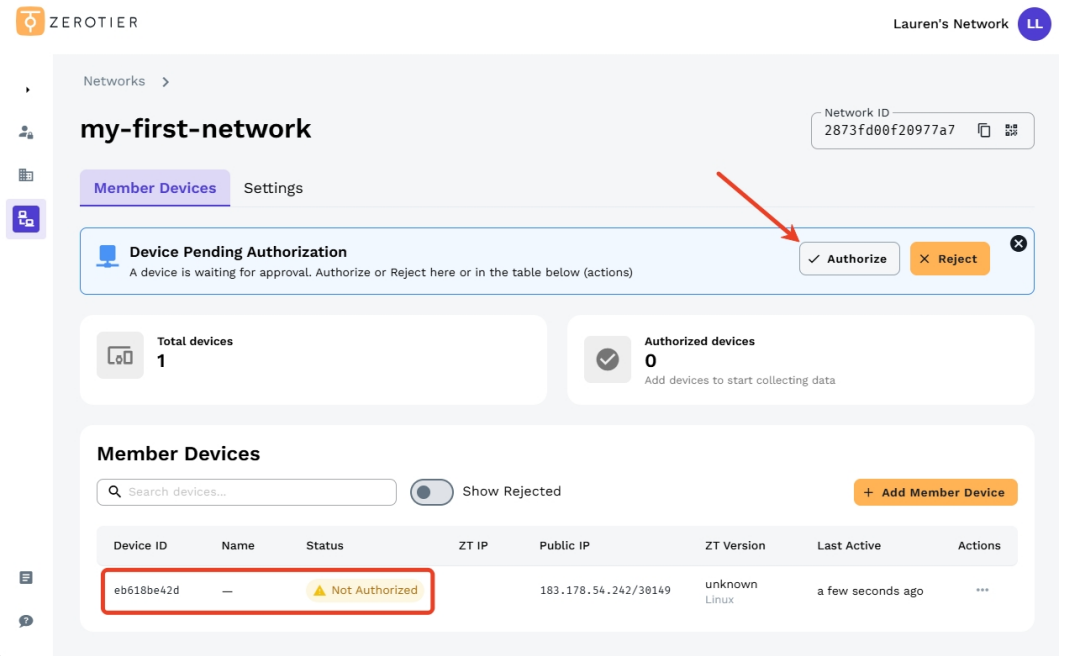
5. Dans l'interface Web du routeur, ouvrez **APPLICATIONS** > **ZeroTier**. Activez ZeroTier, saisissez l'**identifiant du réseau (Network ID)** et cliquez sur **Appliquer (Apply)**.



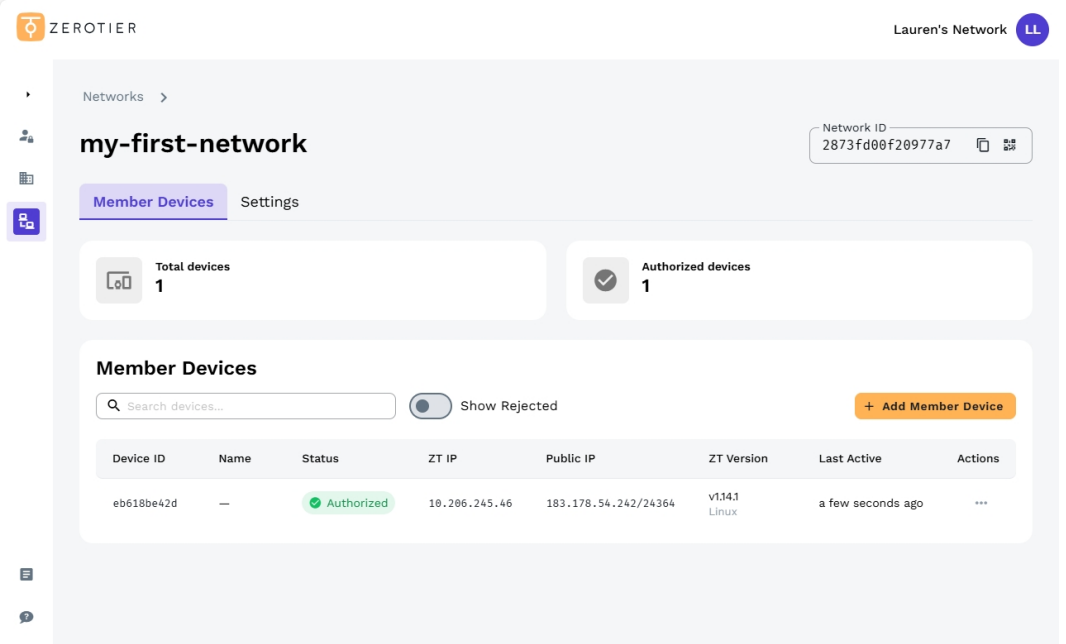
Après un court instant, la page indique qu'une autorisation est nécessaire. Cliquez sur le lien **ZeroTier Central** pour ouvrir la plateforme.



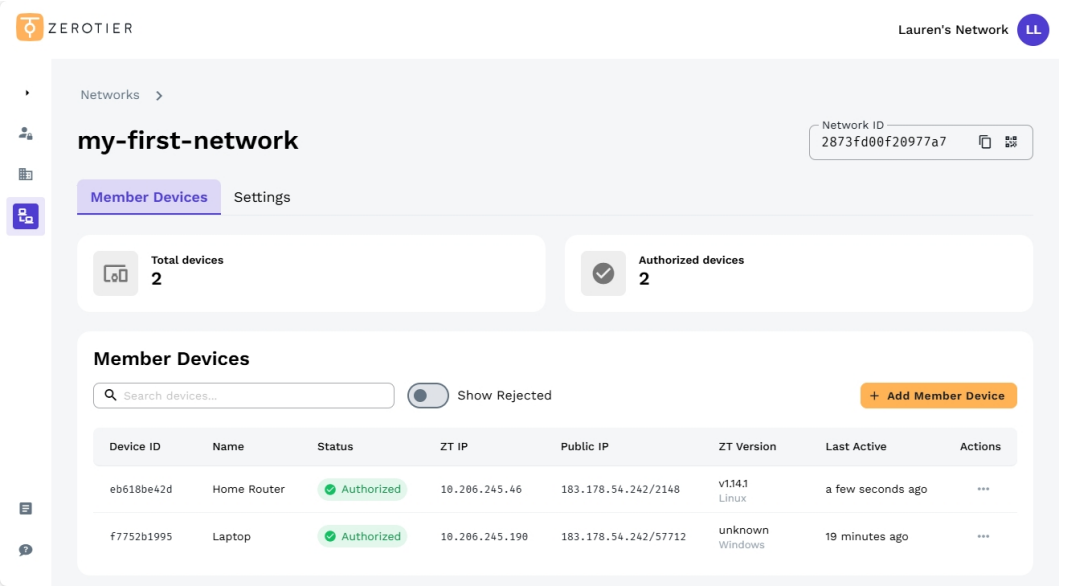
6. Dans ZeroTier Central, repérez l'appareil en attente et autorisez-le.



Une fois autorisé, il apparaît comme ci-dessous.

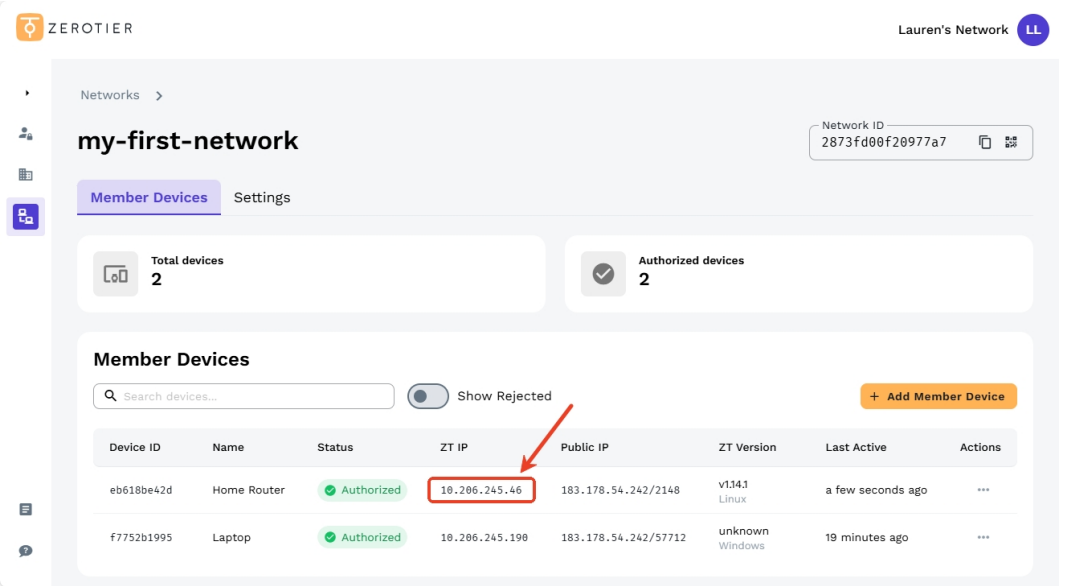


7. Ajoutez un autre appareil, comme un ordinateur ou un smartphone, au même réseau en suivant ce guide. Une fois l'ajout réussi, la page affiche les informations des membres : **identifiant de l'appareil (Device ID)**, **nom (Name)**, **état (Status)**, **IP gérée (Managed IP)** et **IP publique (Public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



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

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



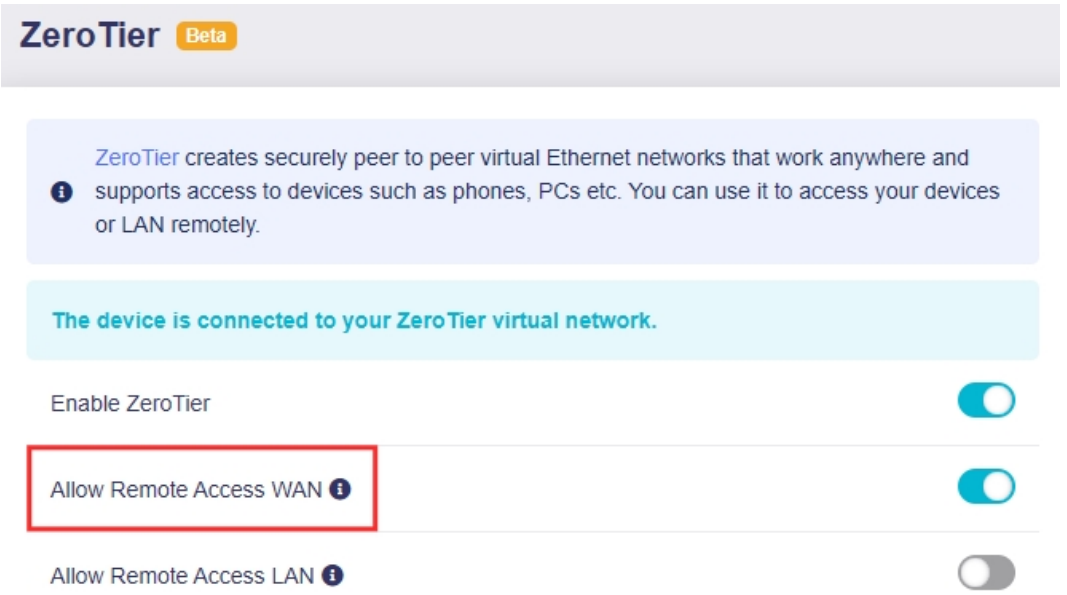
Utilisez ensuite cette IP pour accéder au routeur depuis votre ordinateur portable connecté au même réseau ZeroTier.

9. Testez la connexion.

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

12.7.2 Autoriser l’accès distant au WAN

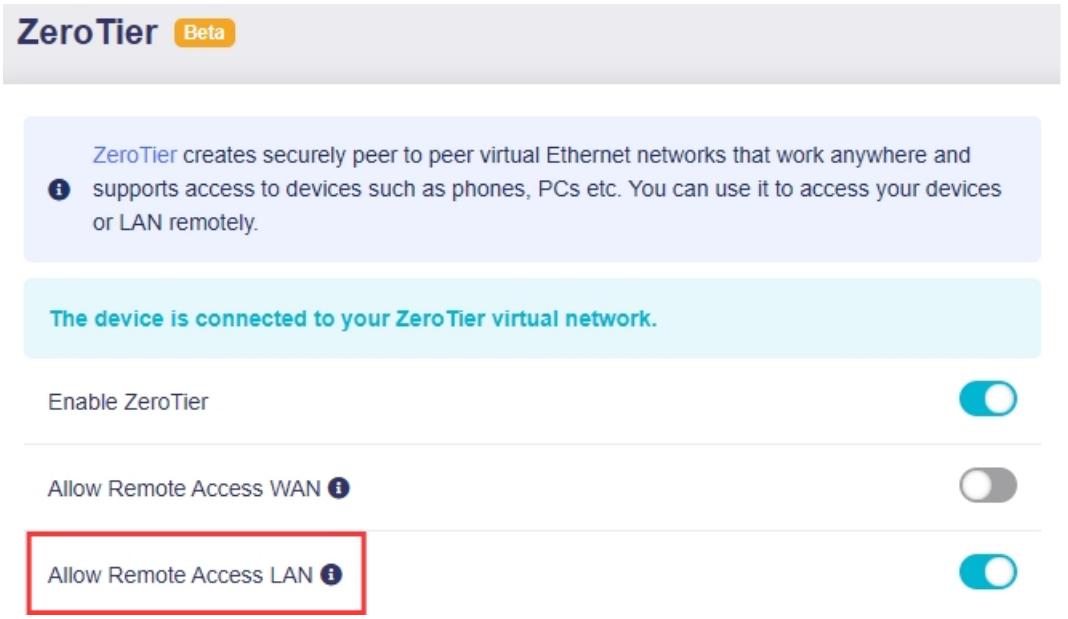
Si cette option est activée, les ressources côté WAN de l’appareil sont accessibles par le réseau virtuel ZeroTier. Consultez cette page pour en savoir plus.



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.

12.7.3 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.

12.8 Tailscale

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

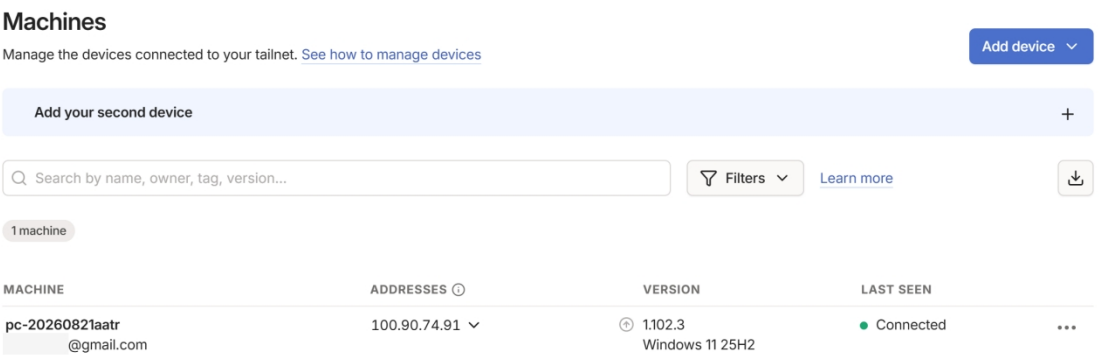
La fonction Tailscale des routeurs GL.iNet permet de rejoindre un réseau virtuel Tailscale pour accéder à distance au routeur et aux ressources situées côté WAN et LAN.

Remarque :

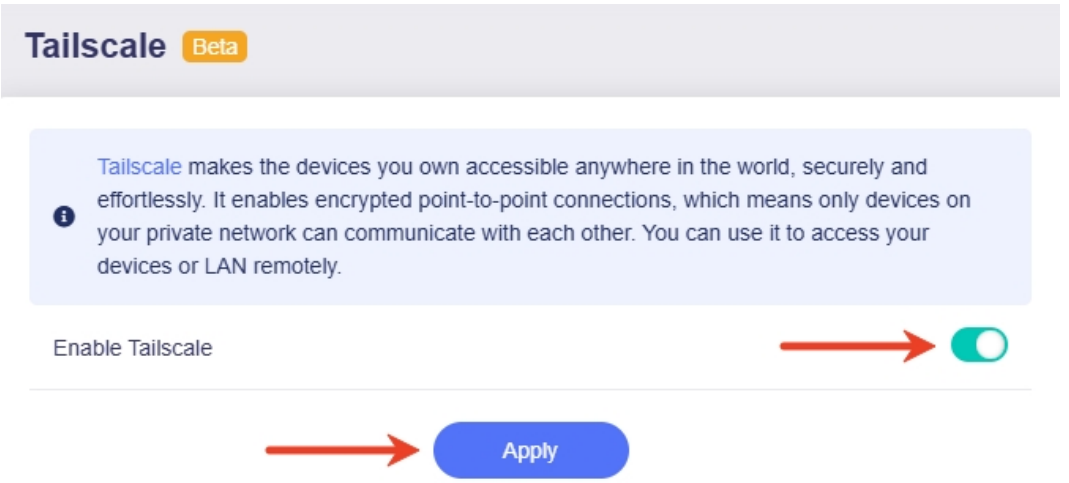
1. Tailscale étant basé sur WireGuard, il est déconseillé de l'utiliser simultanément avec les fonctionnalités ou services suivants, car cela peut entraîner des conflits de routage : client OpenVPN, client WireGuard, GoodCloud Site to Site et ZeroTier.
2. Cette fonction est actuellement en version bêta et peut présenter des anomalies.

12.8.1 Configuration de Tailscale

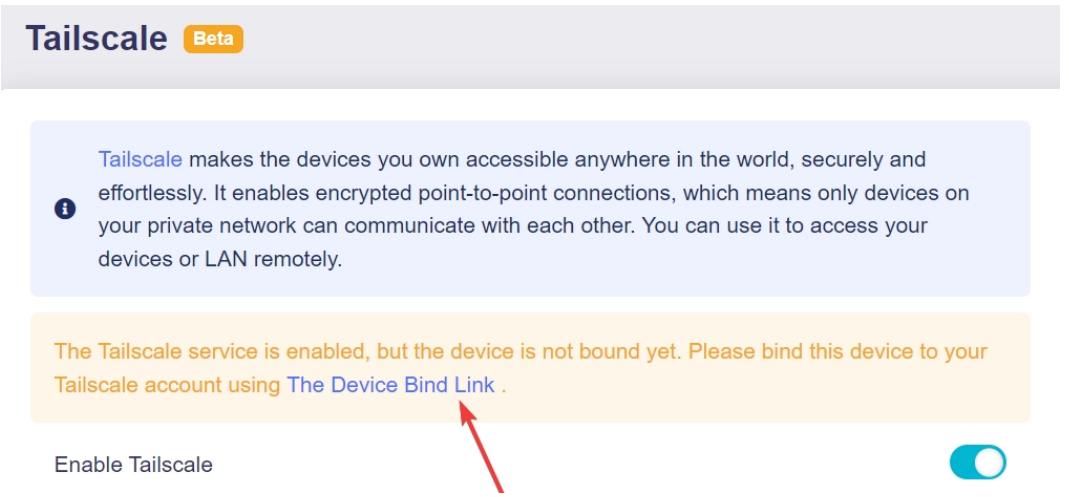
1. Créez d’abord un compte Tailscale et associez-y un ou deux appareils pour effectuer des tests. Ils apparaissent ensuite dans la console Tailscale.



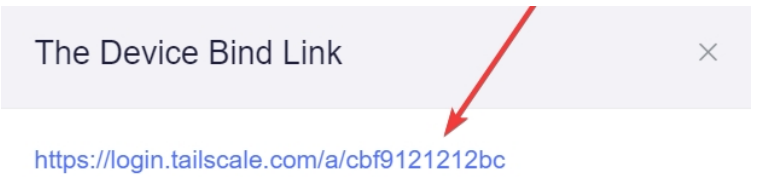
2. Dans l’interface Web du routeur, ouvrez **APPLICATIONS** > **Tailscale**. Activez **Activer Tailscale (Enable Tailscale)**, puis cliquez sur **Appliquer (Apply)**.



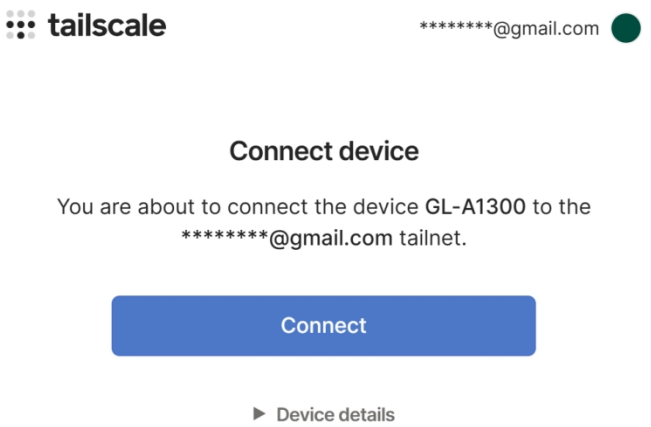
3. La page vous invite à associer l’appareil. Cliquez sur **Lien d’association de l’appareil (Device Bind Link)**.



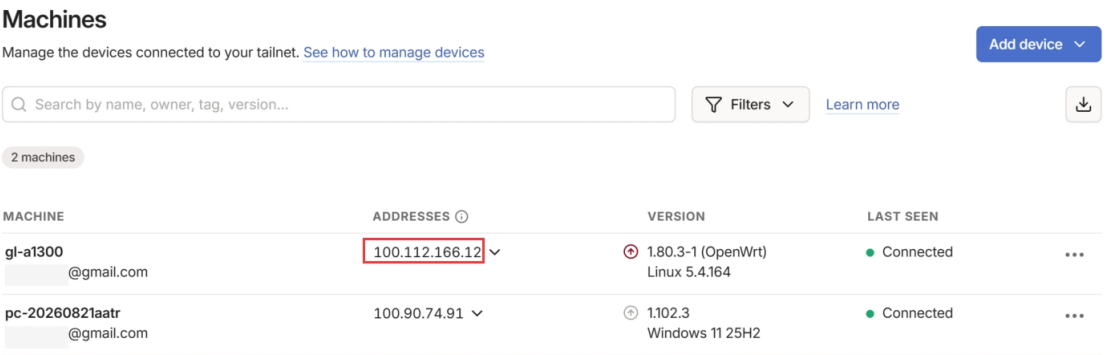
4. Dans la fenêtre qui s'affiche, cliquez sur le lien et connectez-vous à votre compte Tailscale.



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

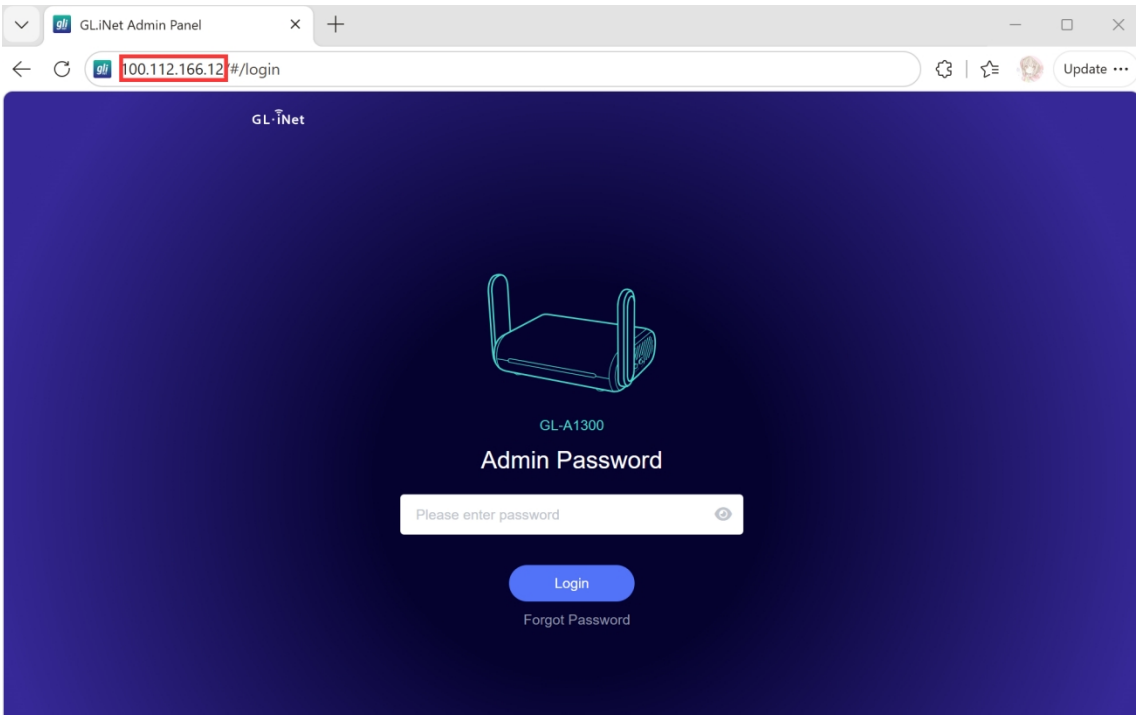


6. Vous serez alors redirigé vers la console d'administration Tailscale. Le routeur a désormais été ajouté au réseau virtuel Tailscale et vous pouvez y accéder à distance via son adresse IP virtuelle Tailscale **100.112.166.12**.



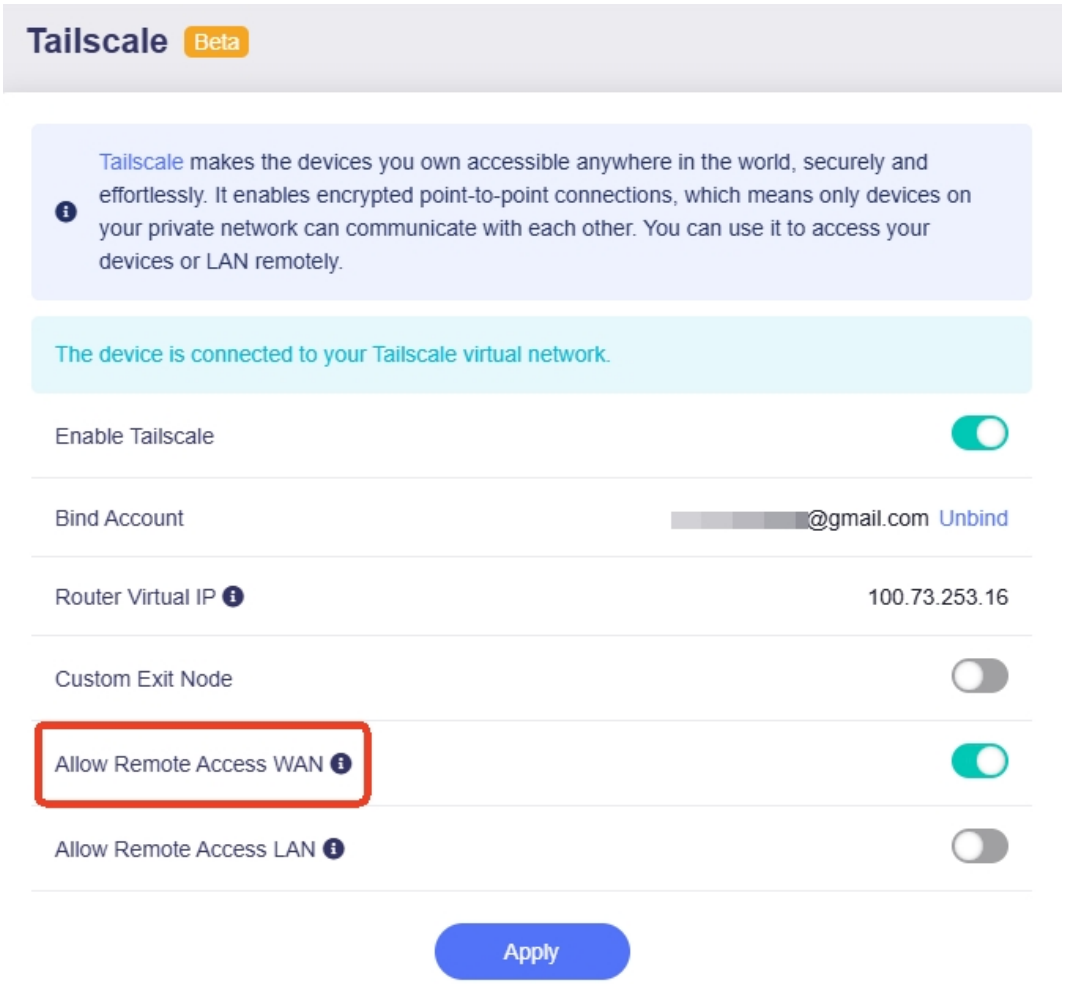
7. Testez la connexion.

   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.



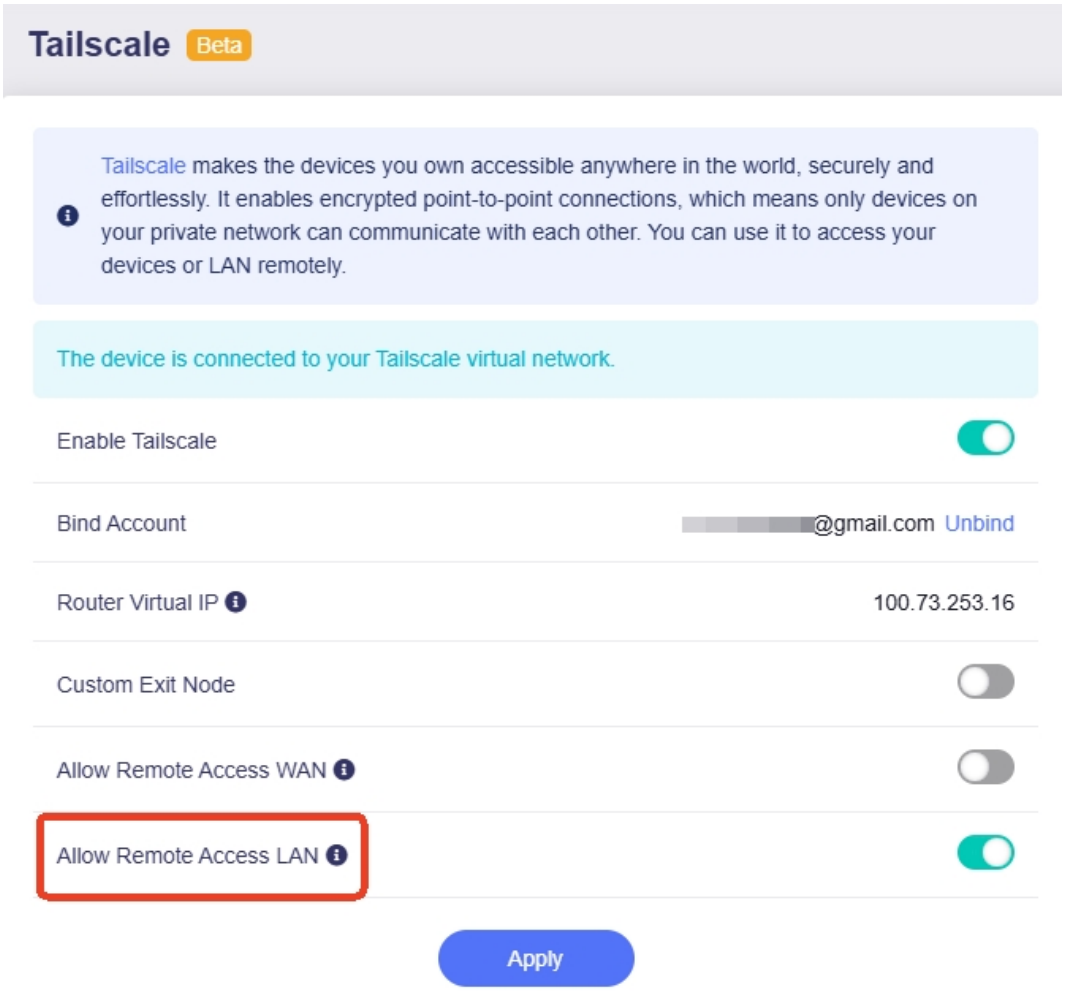
12.8.2 Autoriser l’accès à distance au réseau WAN

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.



12.8.3 Autoriser l’accès à distance au réseau LAN

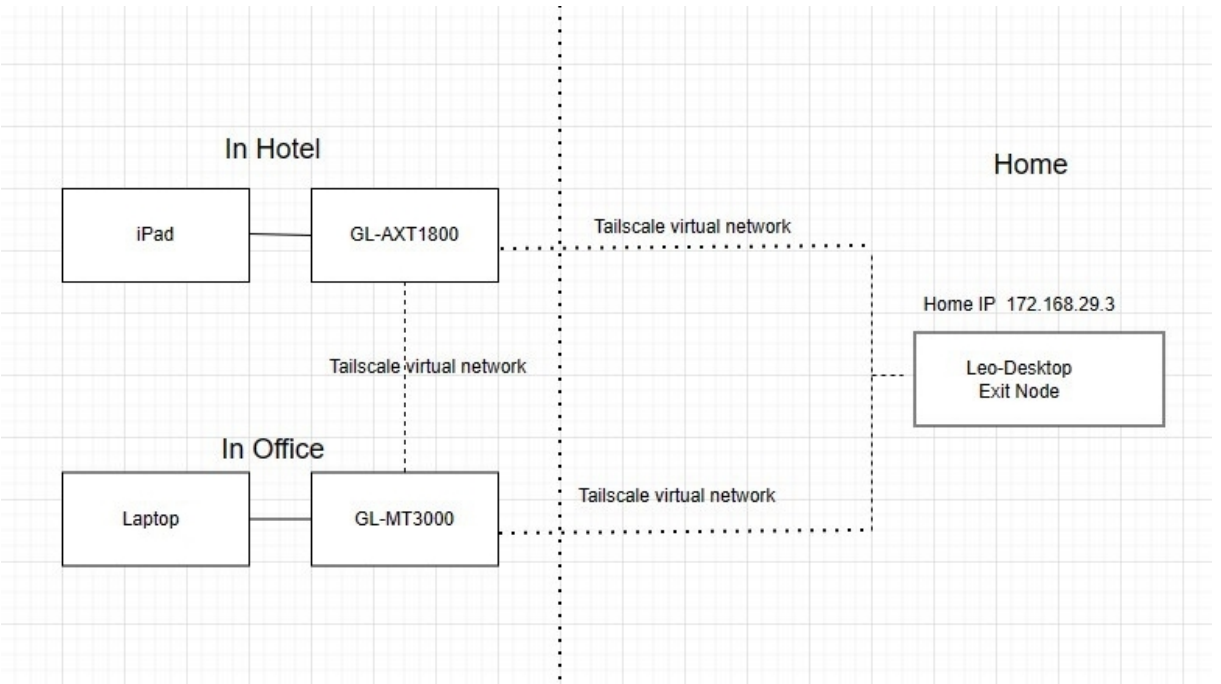
Si cette option est activée, les ressources côté LAN de l’appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



12.8.4 Nœuds de sortie personnalisés

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

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



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

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

Chapitre 13

Réseau

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

13.1 Pare-feu

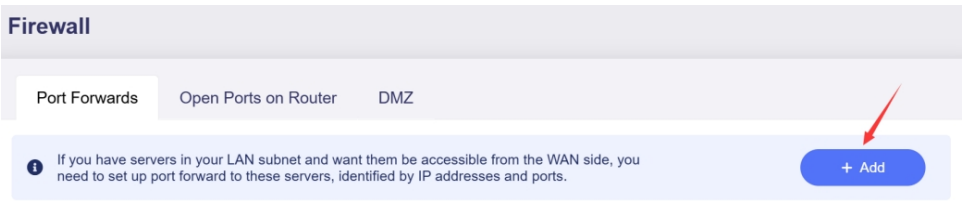
Le pare-feu est une fonction réseau qui achemine les requêtes externes vers des appareils précis de votre réseau local. La page Pare-feu comprend trois fonctions principales : **Redirections de ports (Port Forwards)** pour accéder à des ports précis des appareils, **Ouvrir des ports sur le routeur (Open Ports on Router)** pour accéder aux services exécutés sur le routeur lui-même, et **DMZ** pour donner un accès direct et complet à un appareil.

13.1.1 Redirections de ports

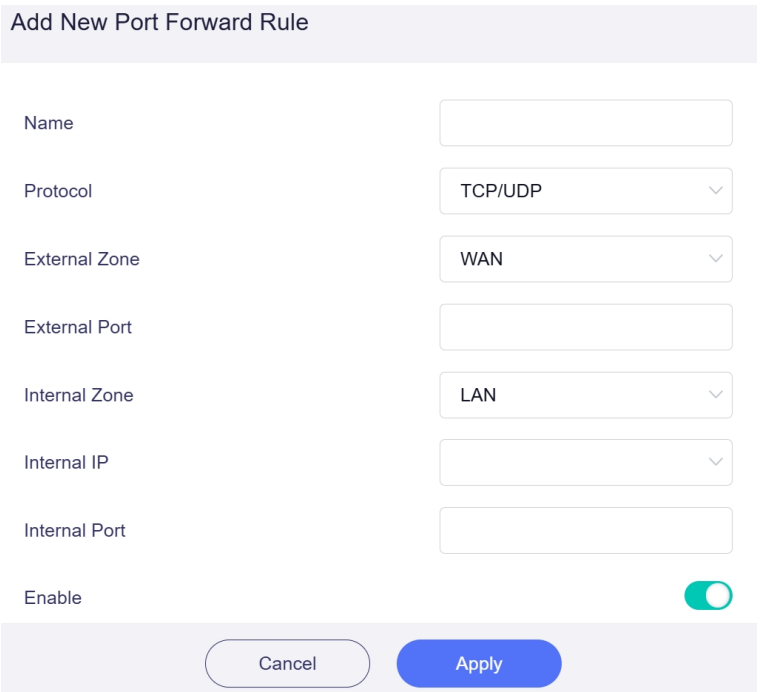
Les redirections de ports permettent à des ordinateurs distants de se connecter à un ordinateur ou à un serveur local situé derrière le pare-feu du réseau local, par exemple un serveur Web ou FTP.

Pour configurer des redirections de ports, suivez les étapes ci-dessous.

1. Connectez-vous à l'interface d'administration Web du routeur, accédez à **RÉSEAU (NETWORK)** > **Pare-feu (Firewall)** > **Redirections de ports (Port Forwards)**, puis cliquez sur **Ajouter (Add)**.



2. Dans la fenêtre qui s'affiche, saisissez ou sélectionnez les paramètres requis dans la liste déroulante pour ajouter une règle de redirection de port, puis cliquez sur **Appliquer (Apply)**.

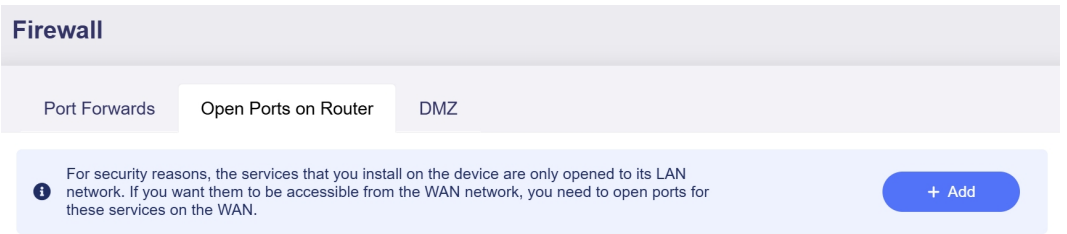


- **Nom (Name)** : nom de la règle, que vous pouvez définir.
- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP et UDP.
- **Zone externe (External Zone)** : options disponibles : WAN, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN, LAN et Invité.
- **Port externe (External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

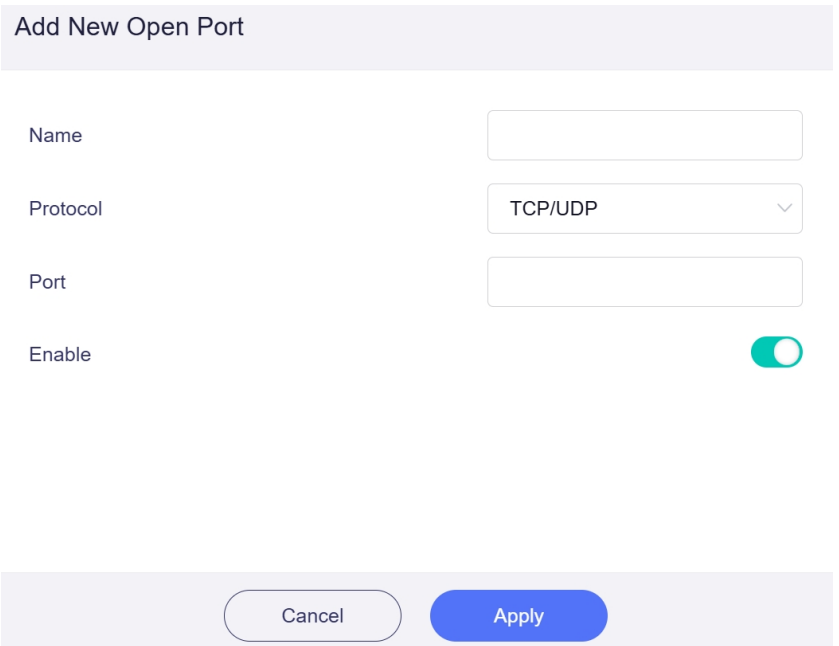
13.1.2 Ouverture de ports sur le routeur

Pour que les services du routeur, tels que les services Web et FTP, soient accessibles publiquement, leurs ports respectifs doivent être ouverts sur le routeur.

Pour ouvrir un port, sélectionnez l'onglet Ouvrir des ports sur le routeur (Open Ports on Router), puis cliquez sur Ajouter (Add).



Dans la fenêtre qui s'affiche, ouvrez un nouveau port, puis cliquez sur Appliquer (Apply).



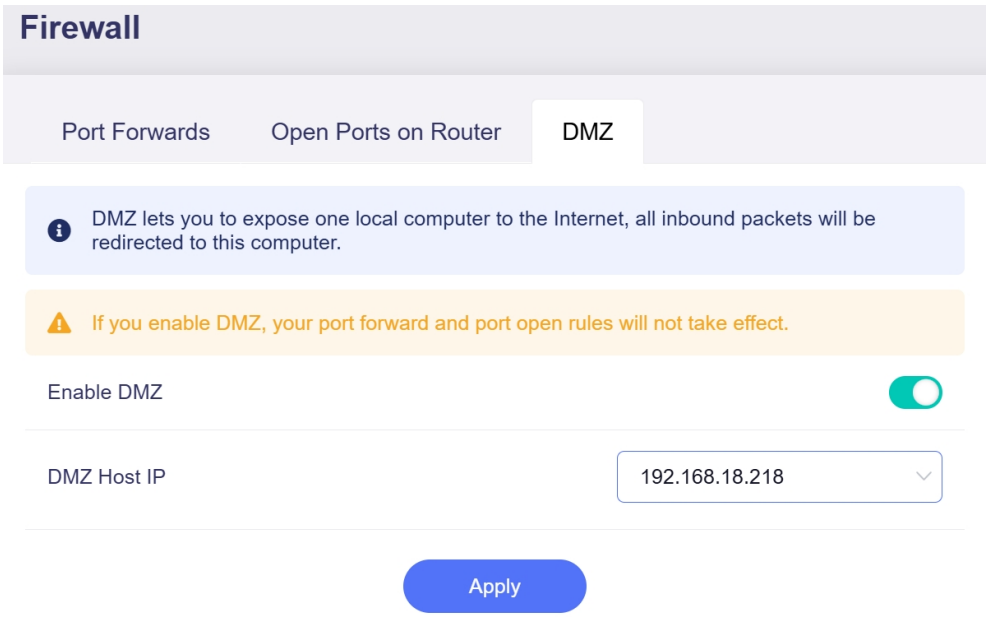
- **Nom (Name)** : nom de la règle, que vous pouvez définir.
- **Protocole (Protocol)** : protocole utilisé ; vous pouvez choisir TCP, UDP ou TCP et UDP.
- **Port** : numéro du port à ouvrir.
- **Activer (Enable)** : activez ou désactivez la règle.

13.1.3 DMZ

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

Pour activer la DMZ, procédez comme suit.

1. Connectez-vous à l'interface d'administration Web du routeur, puis accédez à **RÉSEAU (NETWORK)** > **Pare-feu (Firewall)** > **DMZ**, dans la section correspondante.
2. Activez **Activer la DMZ (Enable DMZ)**, puis sélectionnez l'**adresse IP de l'hôte DMZ (DMZ Host IP)** dans la liste déroulante. L'appareil sélectionné reçoit tous les paquets entrants. Cliquez sur **Appliquer (Apply)** pour enregistrer les paramètres.



13.2 Multi-WAN

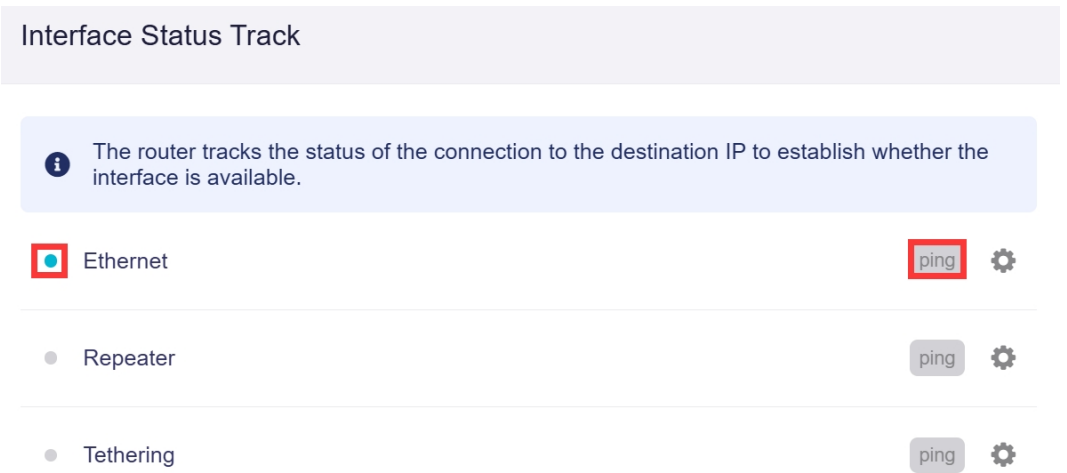
Multi-WAN permet d'utiliser simultanément plusieurs méthodes d'accès à Internet et de configurer différentes options de connexion sur le routeur. Deux modes sont proposés :

- **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.

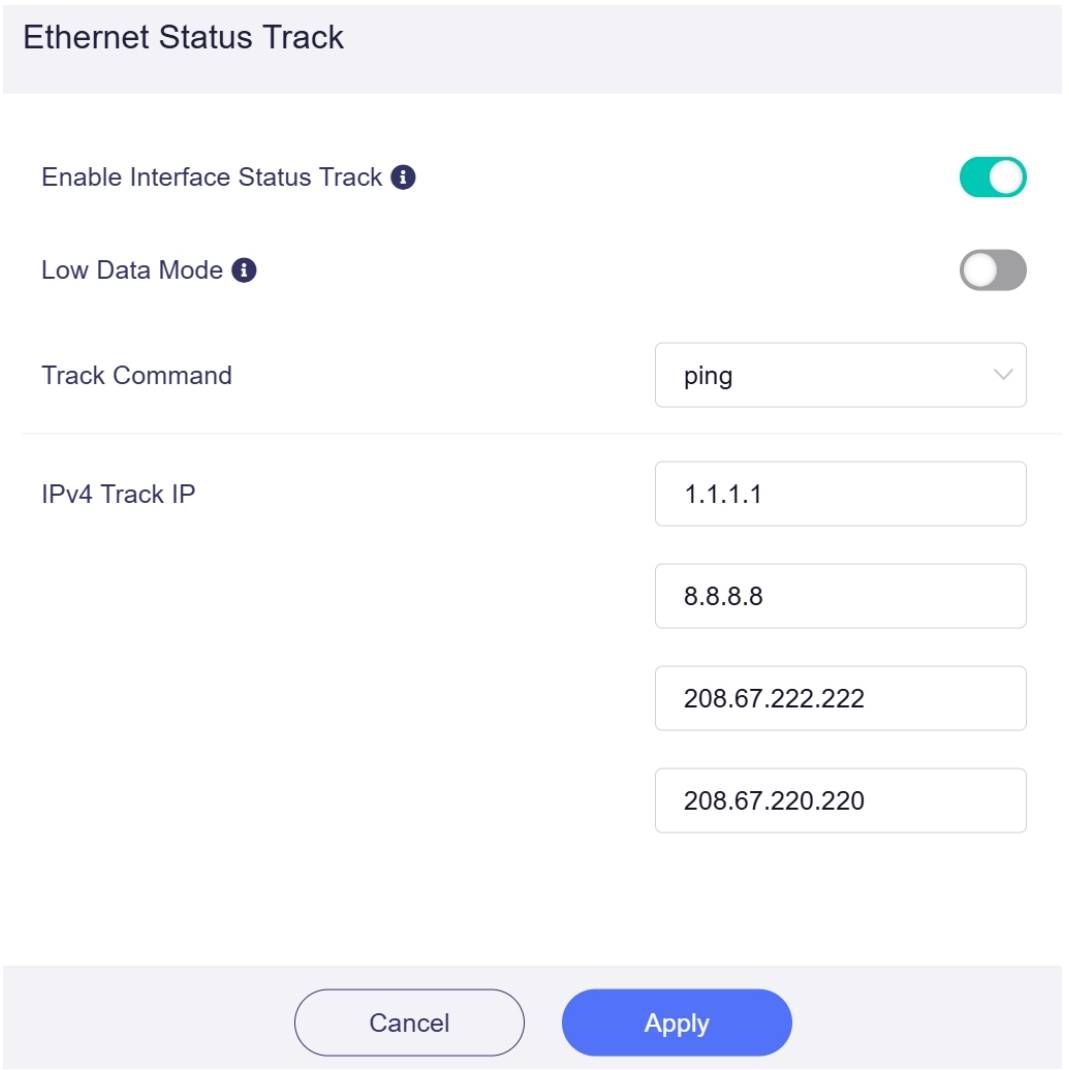
Dans l'interface d'administration Web, ouvrez **RÉSEAU (NETWORK)** > **Multi-WAN**. Cette page comporte deux sections : Suivi de l'état des interfaces et Mode Multi-WAN.

13.2.1 Suivi de l'état des interfaces

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

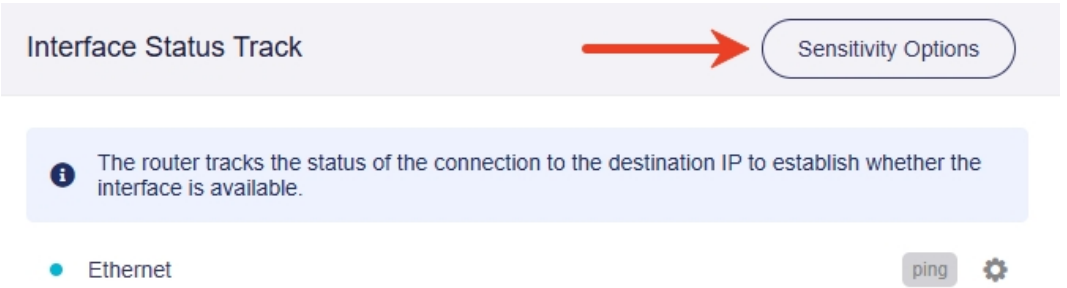


Dans la section **Suivi de l'état des interfaces (Interface Status Track)**, cliquez sur l'engrenage à droite pour régler le suivi de chaque interface. Les paramètres Ethernet sont présentés ci-dessous. La même logique s'applique aux autres interfaces.

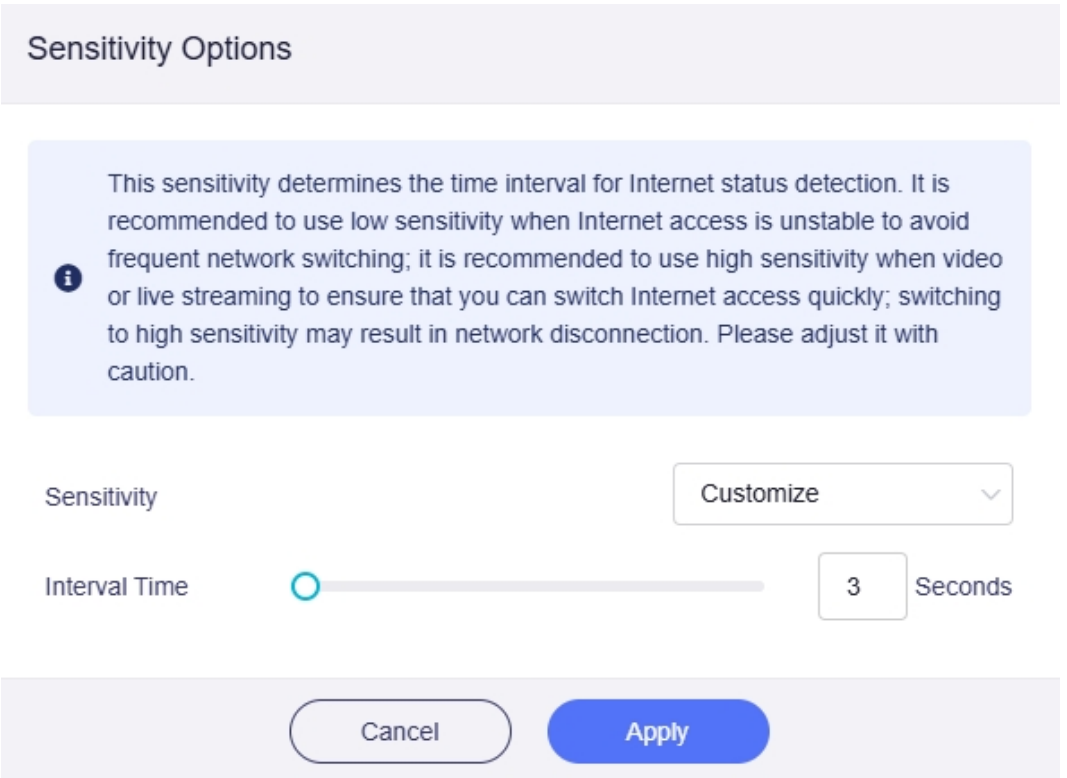


- **Activer le suivi de l'état de l'interface (Enable Interface Status Track)** : activé par défaut. Si vous le désactivez, le routeur détermine l'état de l'interface selon les conditions physiques, par exemple le branchement du câble Ethernet.
- **Mode d'économie de données (Low Data Mode)** : activez cette option pour effectuer le suivi uniquement lorsqu'une erreur réseau survient sur une interface. Ce mode est recommandé si votre forfait de données est limité.
- **Commande de suivi (Track Command)** : la commande ping vérifie la connexion à l'IP cible et la disponibilité de l'interface.
- **IP de suivi IPv4 (IPv4 Track IP)** : personnalisez les adresses IPv4 utilisées pour le suivi si nécessaire.

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



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



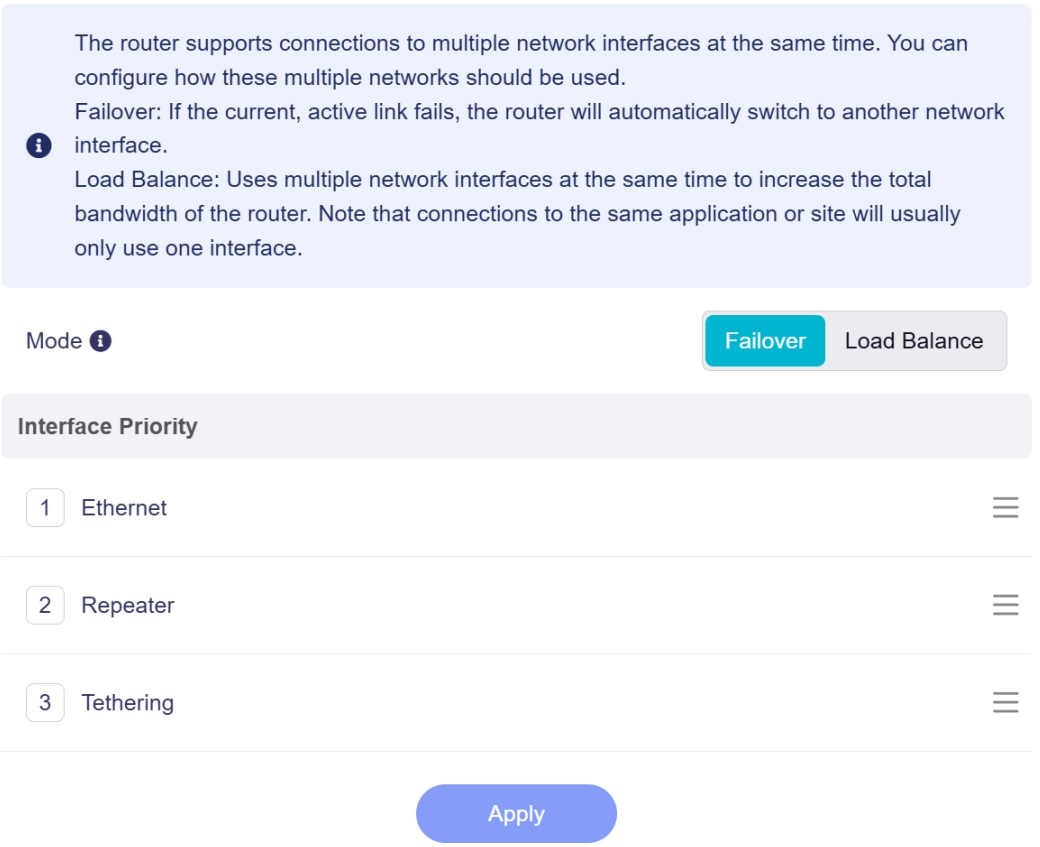
13.2.2 Mode Multi-WAN

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.

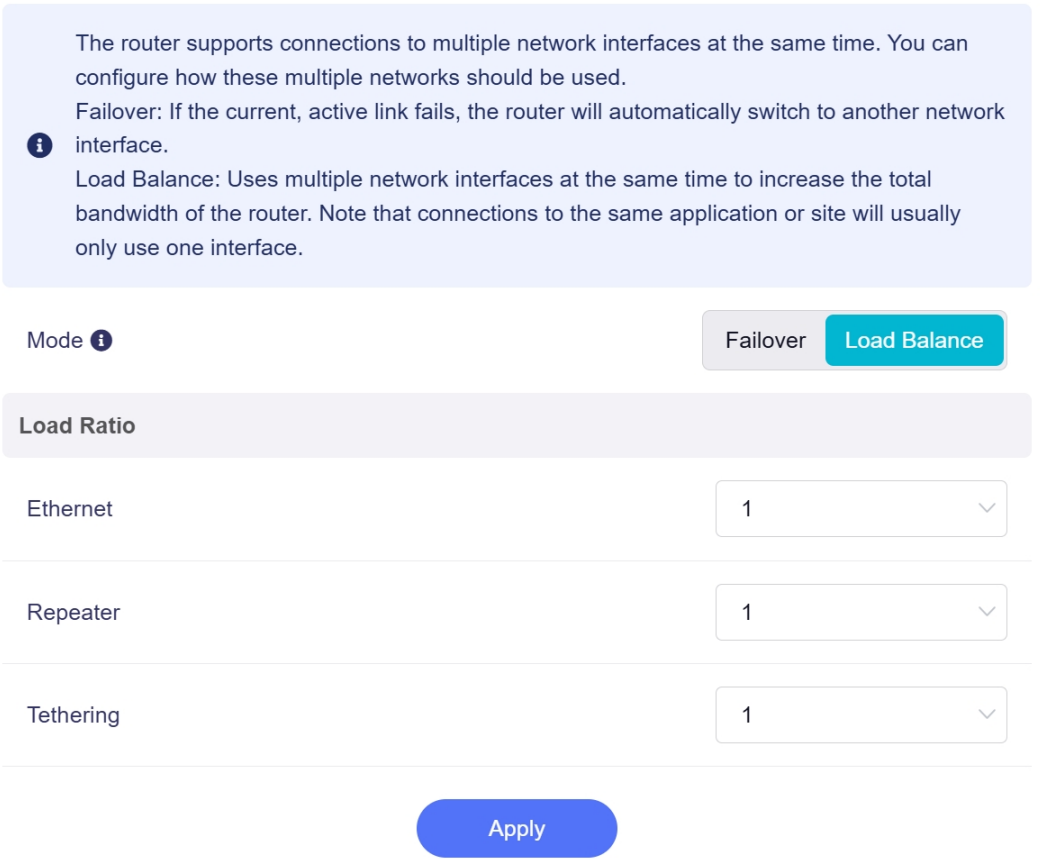


Équilibrage de charge

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

Par exemple, si le routeur est connecté simultanément à trois réseaux (Ethernet, répéteur et partage de connexion USB) et que toutes les interfaces disposent d'un accès à Internet, l'activation de l'équilibrage de charge avec un rapport de 1:1:1 permet aux trois interfaces de se partager équitablement la bande passante réseau. Le système répartit les nouvelles connexions entre ces trois interfaces selon le rapport de charge configuré de 1:1:1.



Vous pouvez également personnaliser le rapport de charge si nécessaire. Par exemple, si la connexion Ethernet offre une bande passante de 100 Mbit/s, le répéteur de 200 Mbit/s et qu'aucune connexion USB n'est active, attribuez les valeurs 1 à Ethernet, 2 au répéteur et 0 au partage de connexion USB. Le système répartira alors les nouvelles connexions entre ces interfaces selon le rapport configuré de 1:2 : Ethernet prendra donc en charge deux fois moins de connexions que le répéteur. Contrairement au mode de basculement, ce mode optimise le débit global en équilibrant le 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.

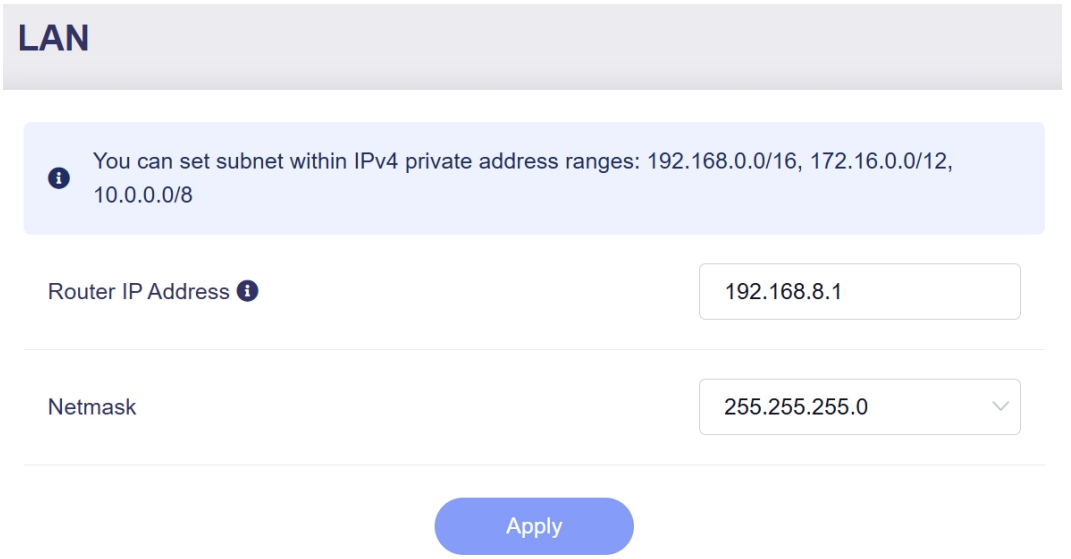
13.3 LAN

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

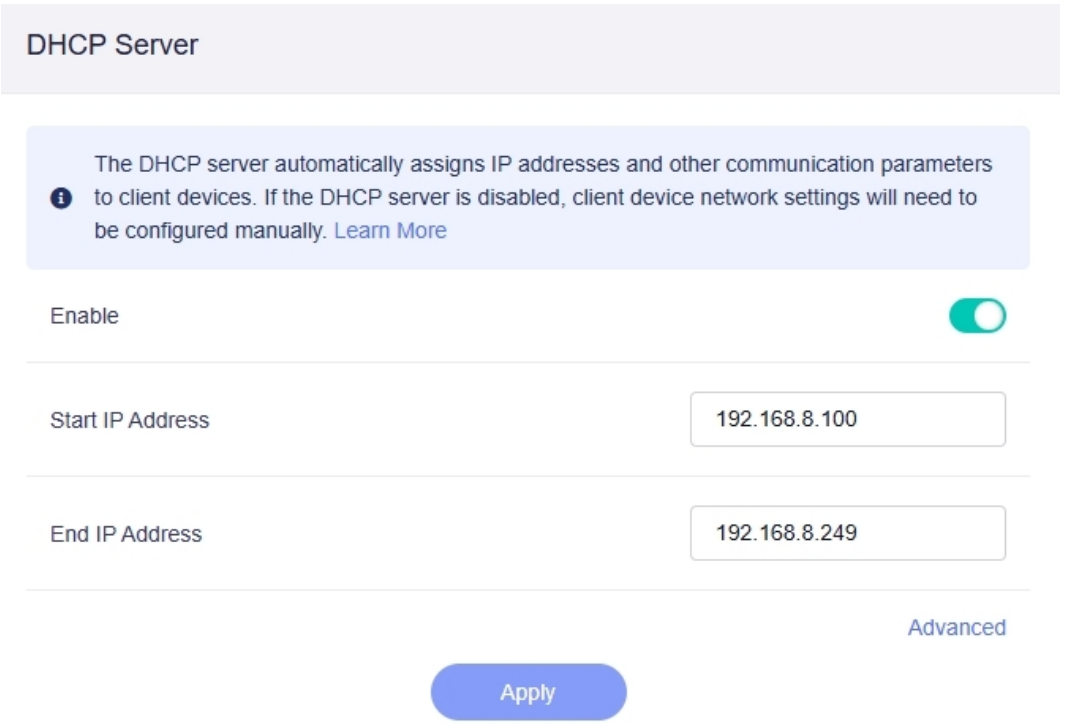
Les paramètres de base comprennent l'adresse IP du routeur et le masque de sous-réseau. Vous pouvez définir un sous-réseau dans les plages IPv4 privées : 192.168.0.0/16, 172.16.0.0/12 ou 10.0.0.0/8.



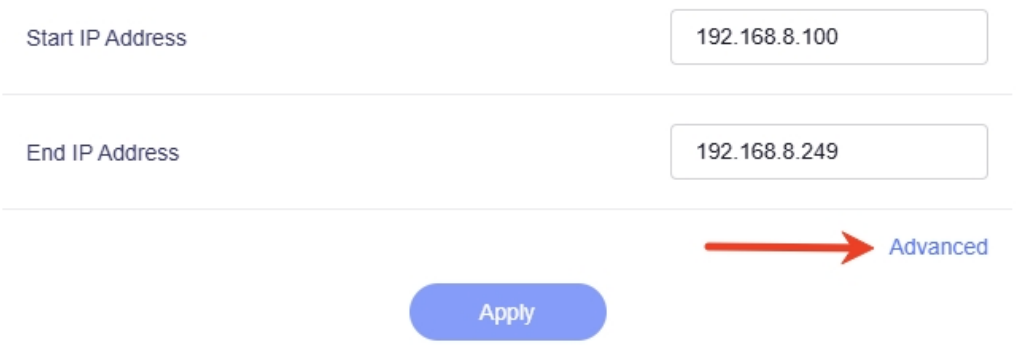
- **Adresse IP du routeur (Router IP Address)** : adresse à saisir dans le navigateur pour ouvrir l'interface d'administration. Par défaut, elle est 192.168.8.1. Modifiez-la si elle entre en conflit avec le réseau en amont.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0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

13.3.2 Serveur DHCP

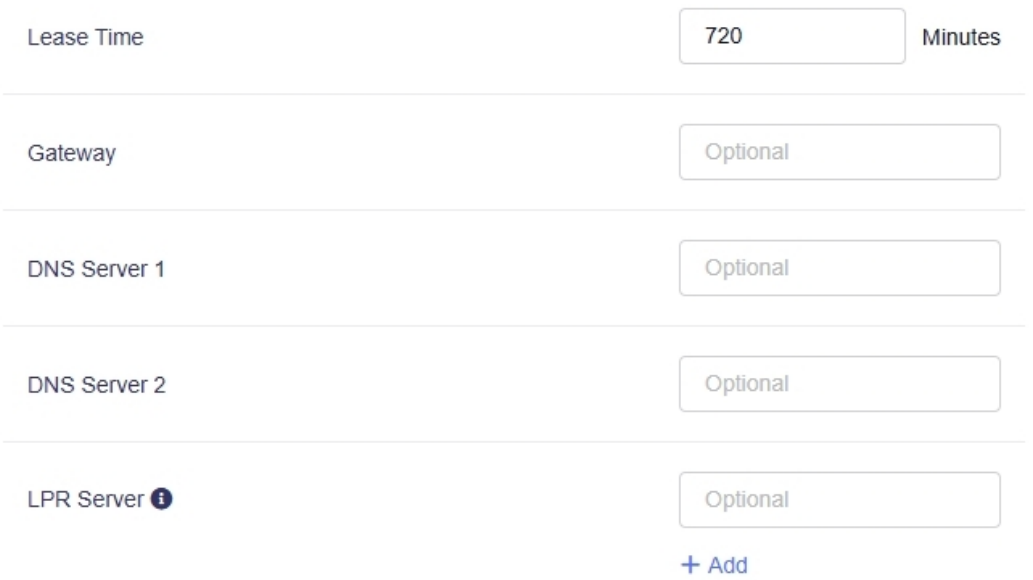
Le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Il est activé par défaut sur le routeur GL.iNet, avec une plage d'adresses de 192.168.8.100 à 192.168.8.249. Vous pouvez personnaliser cette plage.



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.

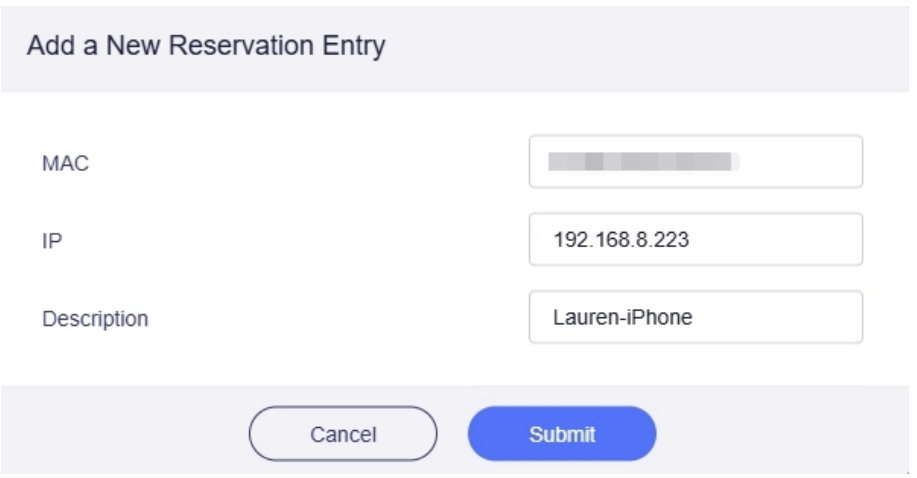
Remarque : si vous désactivez le serveur DHCP, définissez manuellement une IP statique et les autres paramètres de communication sur chaque client. Consultez cette page pour en savoir plus.

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’adresse, procédez comme suit.

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



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



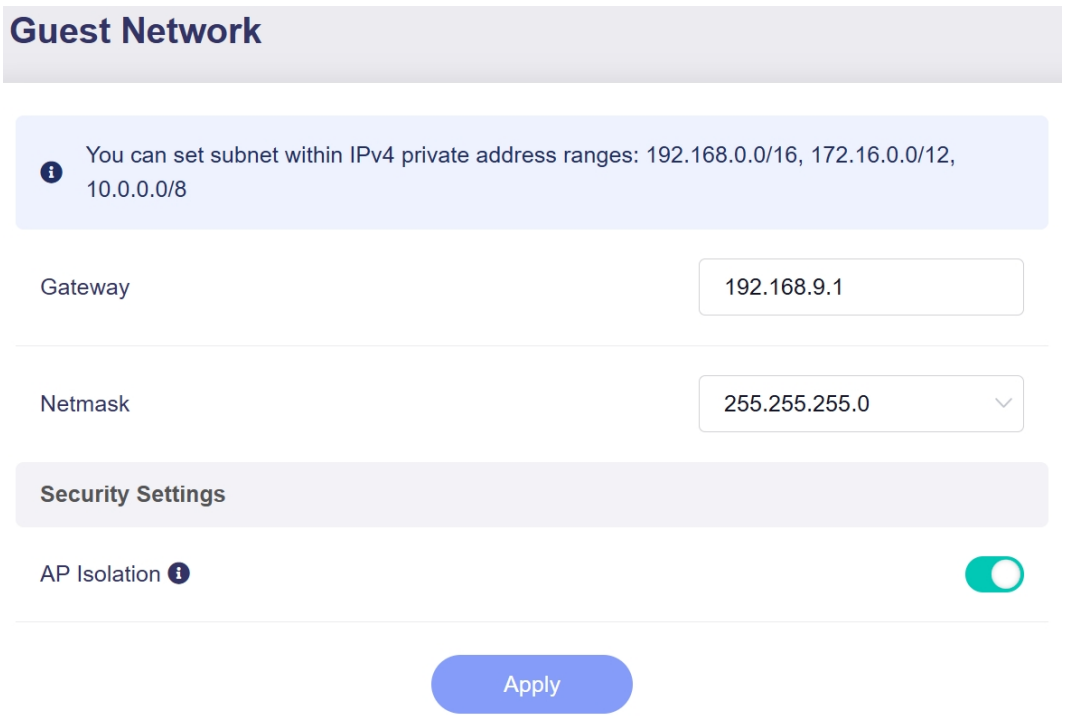
13.4 Réseau invité

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

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

13.4.1 Paramètres de base

Les paramètres de base comprennent la passerelle, le masque de sous-réseau et l'isolation des points d'accès.

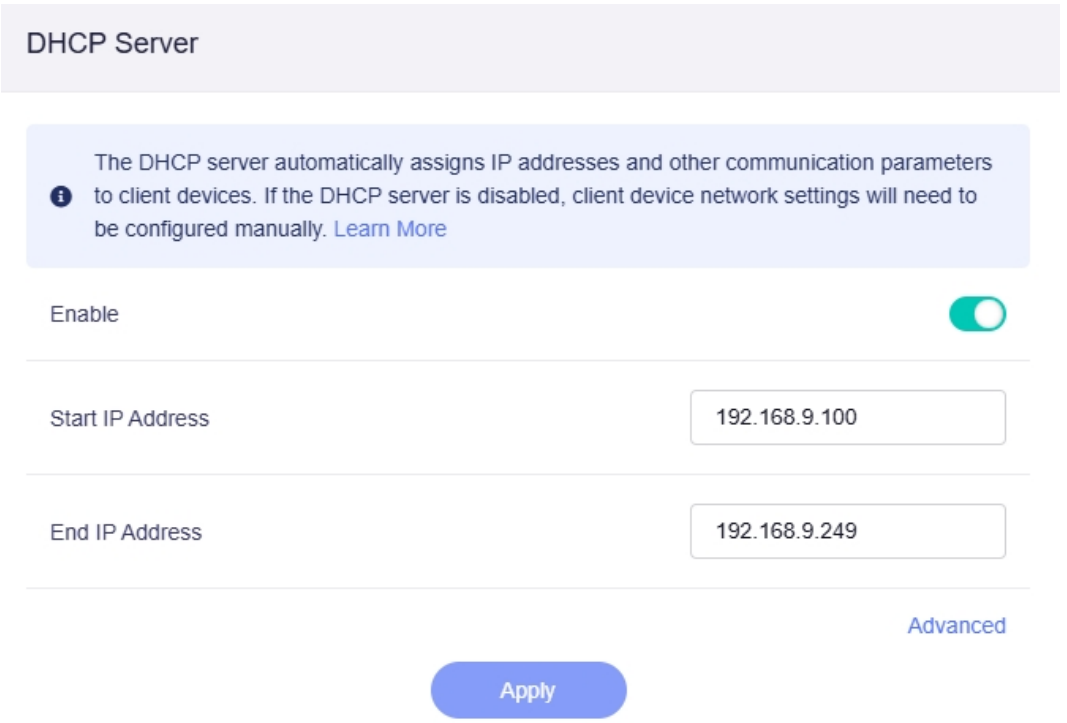


- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.9.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Isolation des clients (AP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

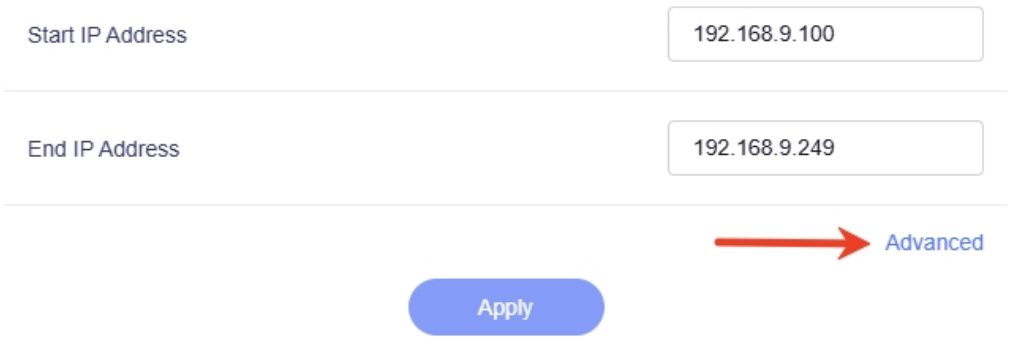
13.4.2 Serveur DHCP

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

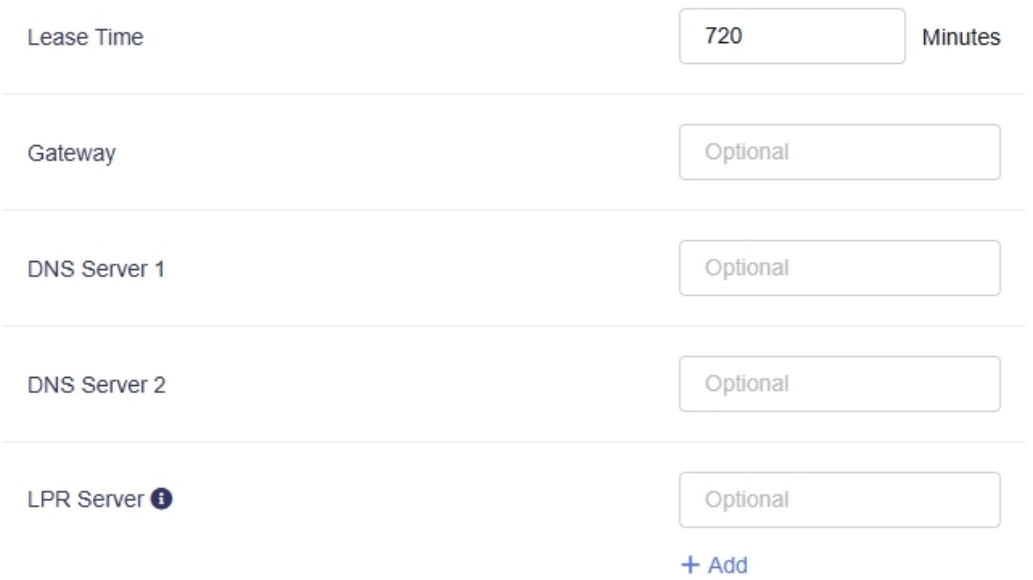
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client. Sa plage d'adresses s'étend de 192.168.9.100 à 192.168.9.249. Vous pouvez la personnaliser.



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



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



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

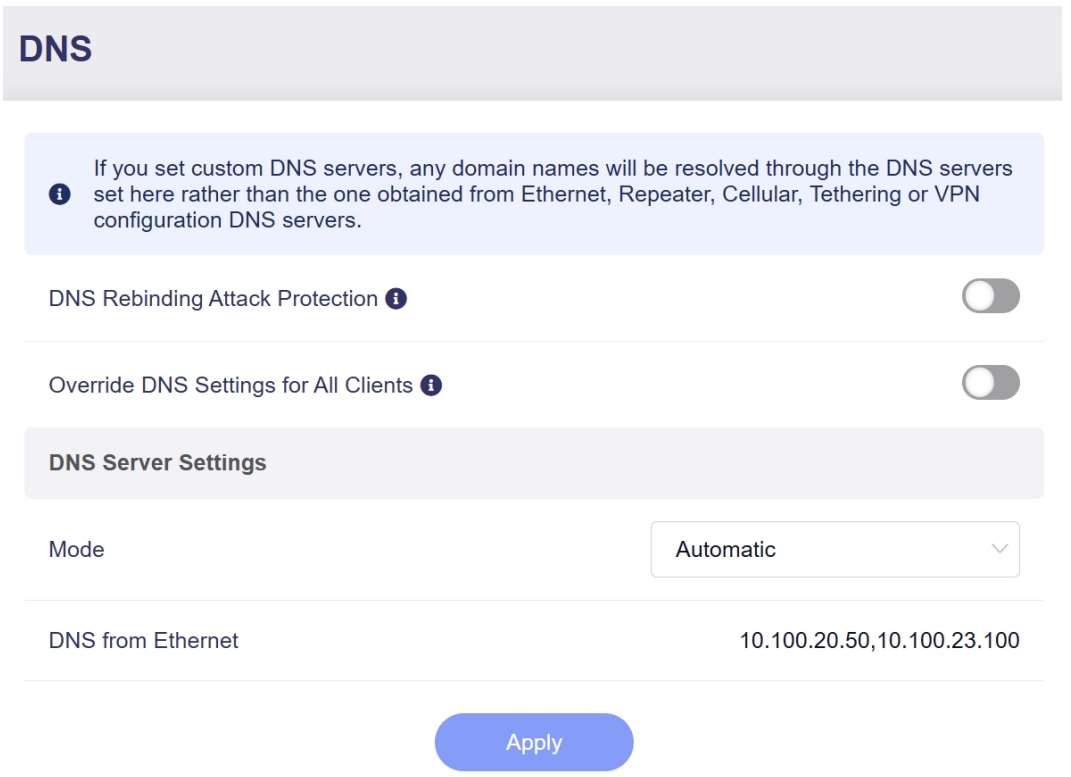
13.5 DNS

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

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

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

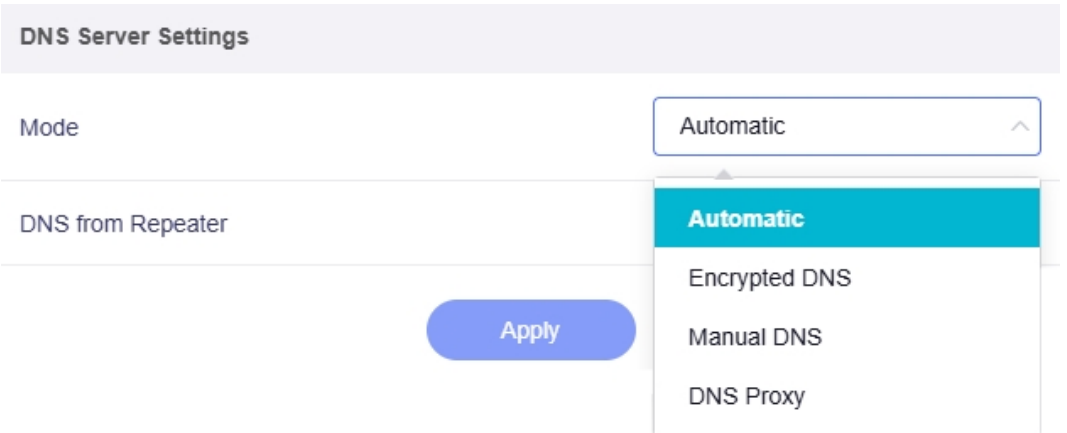
13.5.1 Paramètres généraux



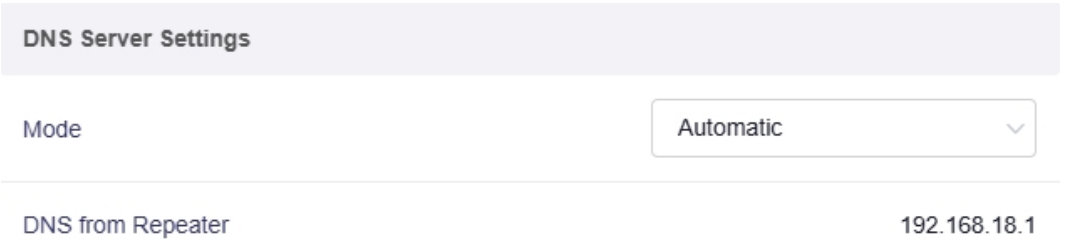
- **Protection contre le rebinding DNS (DNS Rebinding Attack Protection)** : bloque les tentatives malveillantes de résolution DNS. Elle peut toutefois empêcher certaines résolutions DNS privées. Désactivez-la si votre réseau utilise un portail captif, comme une page de connexion Wi-Fi publique.
- **Remplacer les paramètres DNS de tous les clients (Override DNS Settings of All Clients)** : impose les serveurs DNS du routeur à tous les appareils connectés, indépendamment de leurs propres réglages, pour une configuration DNS uniforme.

13.5.2 Paramètres du serveur DNS

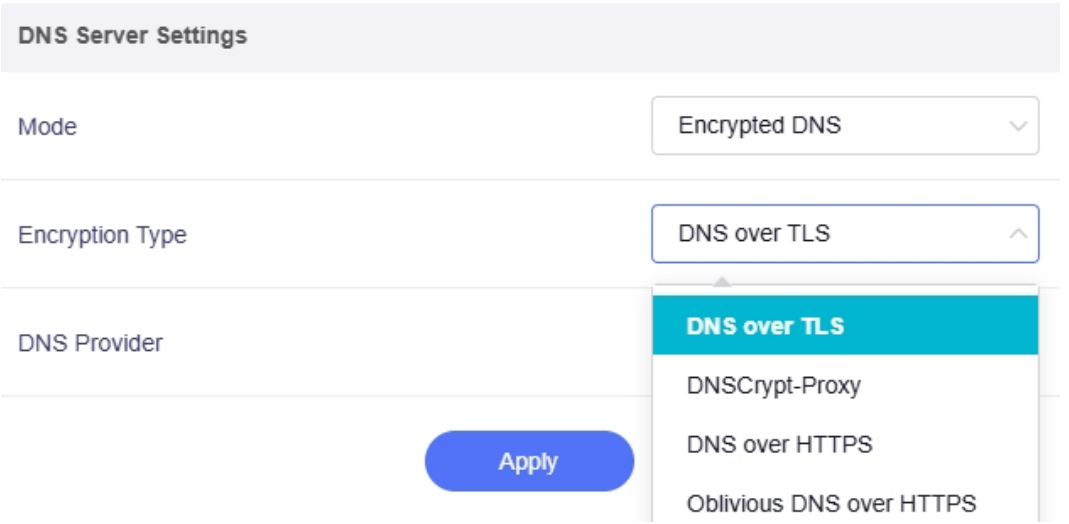
Quatre modes sont proposés : Automatique, DNS chiffré, DNS manuel et Proxy DNS.



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

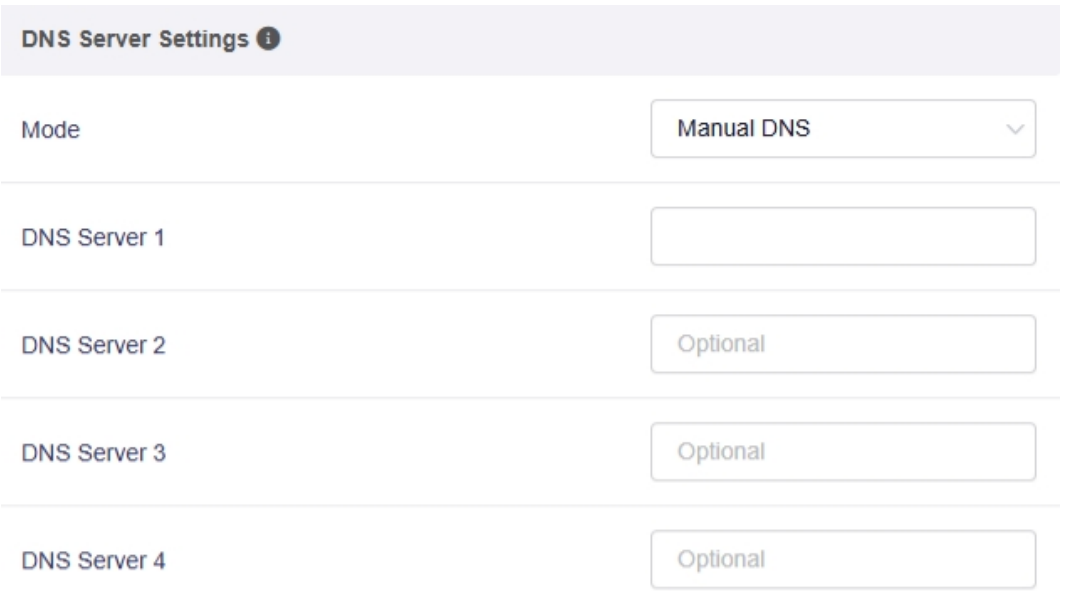


2. **DNS chiffré (Encrypted DNS)** : utilise des protocoles chiffrés pour traiter les requêtes DNS et protéger les données de résolution contre l'écoute et l'altération.
   Quatre types de chiffrement sont proposés : DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS et Oblivious DNS over HTTPS.



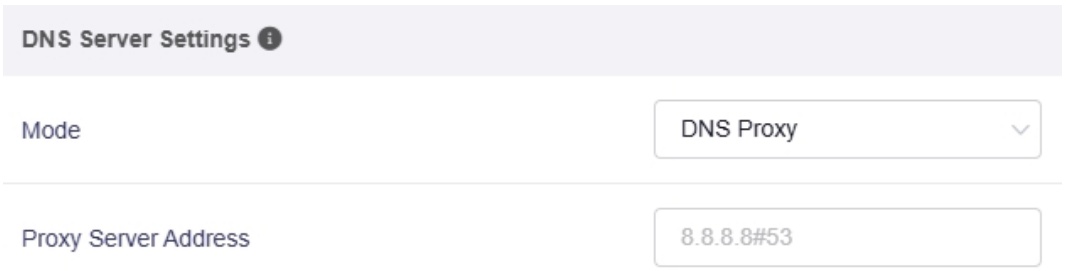
- Pour DNS over TLS, choisissez Control D, NextDNS ou Cloudflare comme fournisseur DNS.
- Pour les trois autres types, sélectionnez au moins un serveur DNS dans la liste, et jusqu'à huit serveurs. Si vous en sélectionnez plusieurs, le routeur utilise automatiquement le plus rapide.

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



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

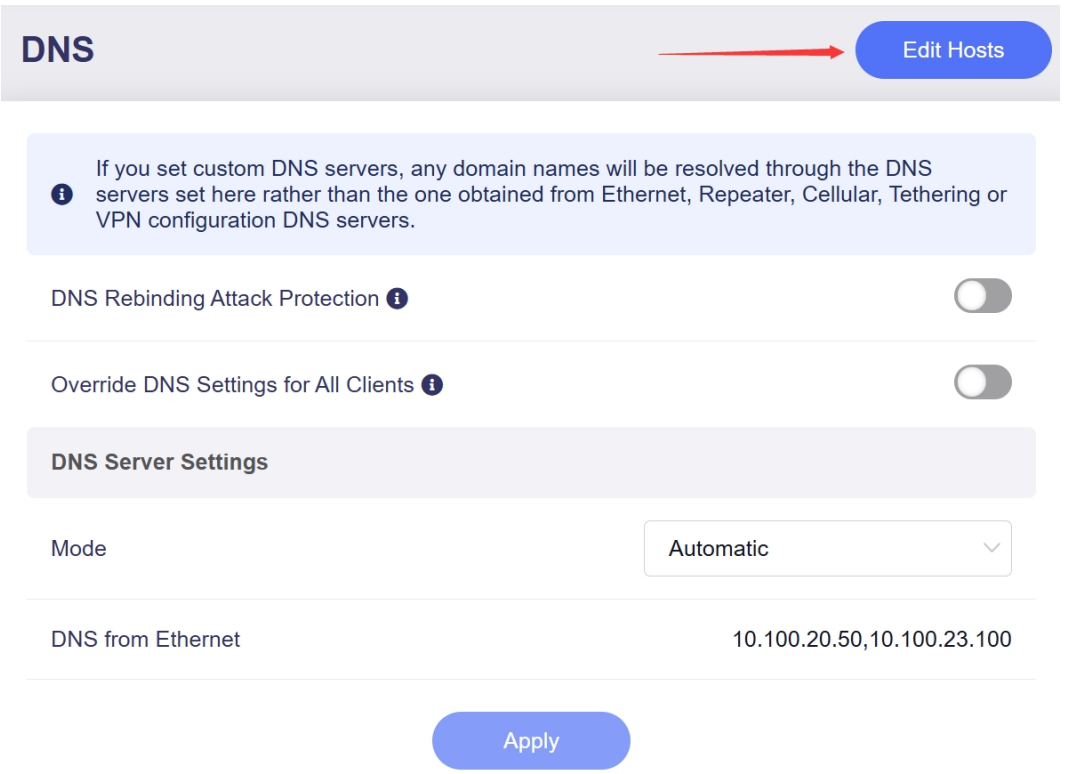
4. **Proxy DNS (DNS Proxy)** : transmet toutes les requêtes DNS par un serveur proxy et utilise son environnement réseau pour la résolution, selon vos besoins d'accès.



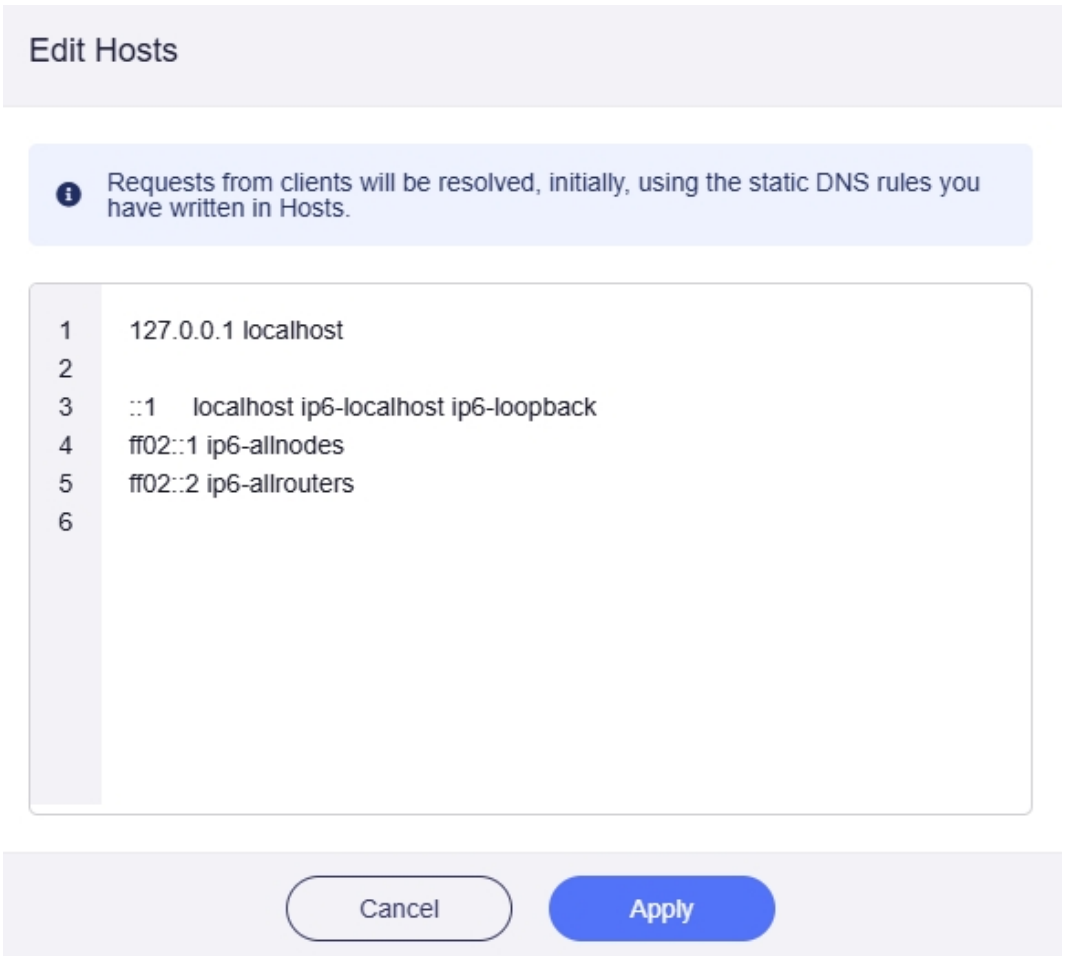
13.5.3 Modification du fichier hosts

Vous pouvez définir des règles statiques de résolution DNS.

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



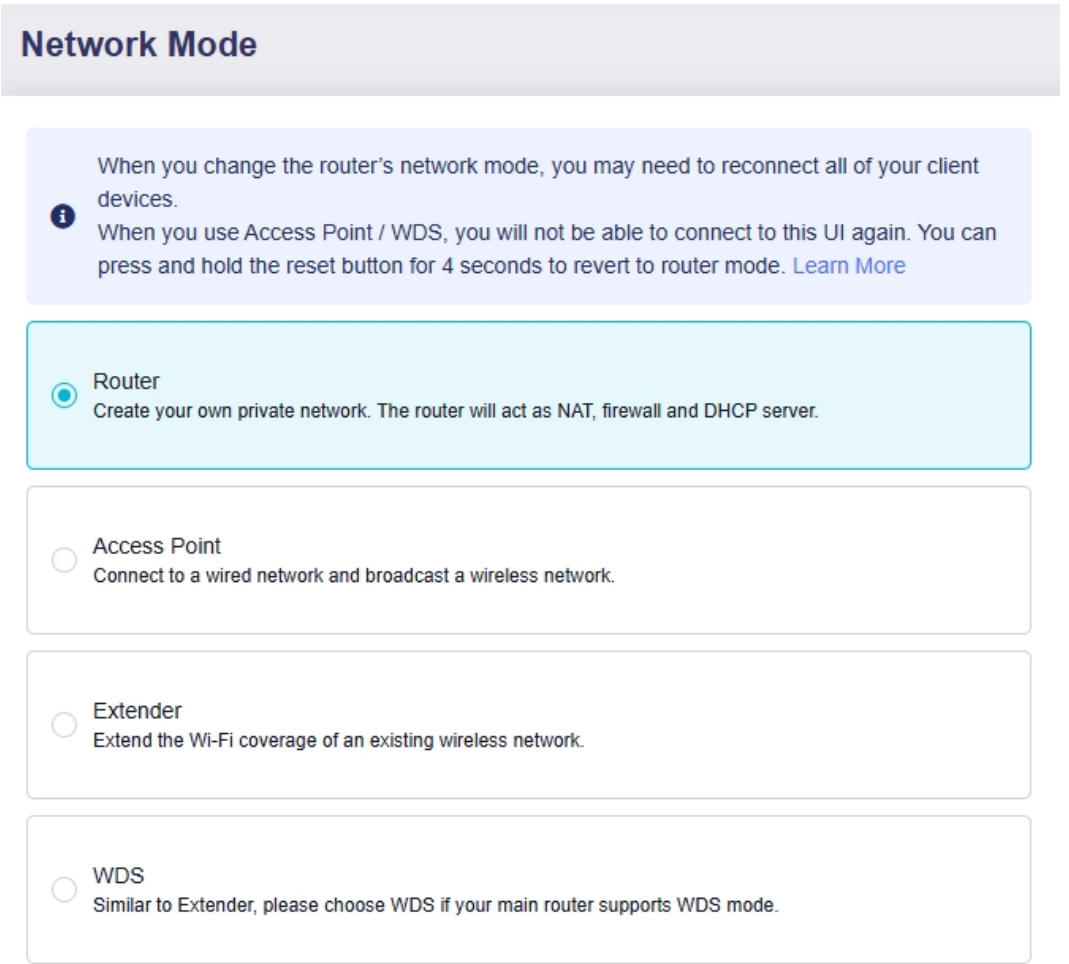
Les requêtes des clients sont résolues en priorité avec les règles statiques saisies ici. Vous pouvez associer manuellement des adresses IP à des noms d'hôtes, comme l'entrée de bouclage locale 127.0.0.1 localhost, pour personnaliser la résolution des noms.


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

13.6 Mode réseau

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

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



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

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

Remarque :

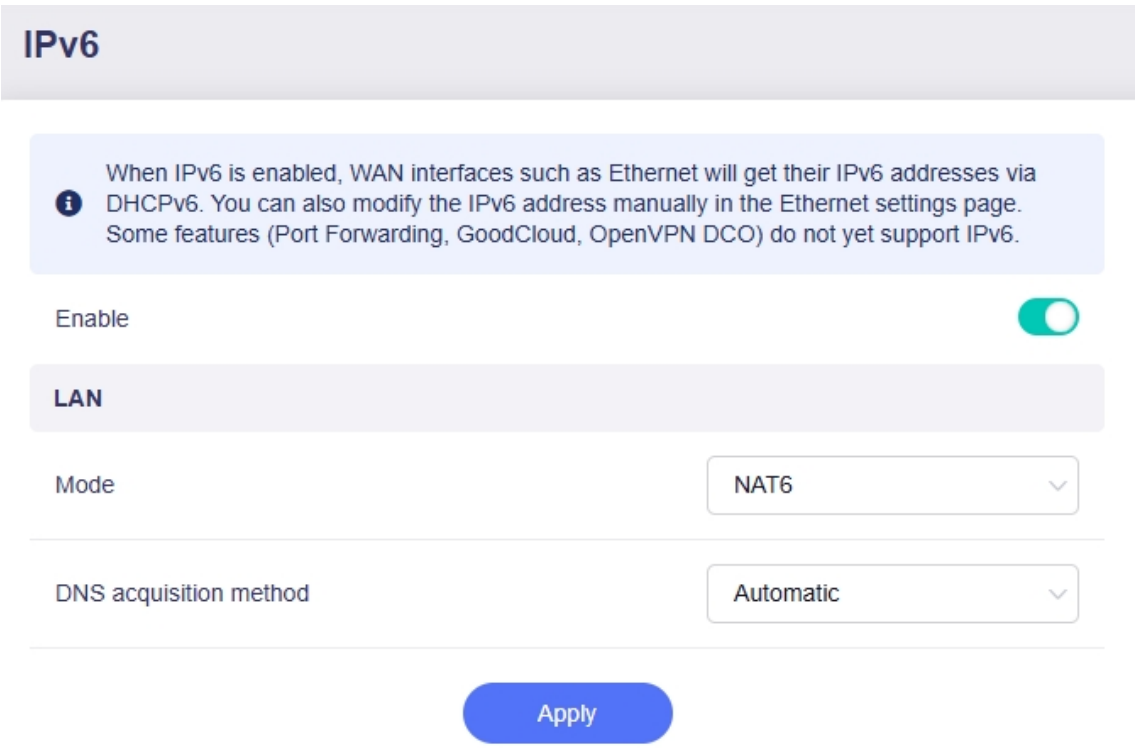
1. Après un changement de mode réseau, tous les appareils clients doivent se reconnecter au routeur pour assurer une connexion stable.
2. **En mode Point d'accès ou WDS, l'adresse IP initiale ne permet plus d'ouvrir l'interface Web**. Connectez-vous au routeur en amont pour trouver l'adresse IP qu'il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

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



Remarque : certaines fonctionnalités, telles que le pare-feu et GoodCloud, ne prennent pas encore en charge IPv6. Leur activation simultanée avec IPv6 peut entraîner des problèmes de connectivité.

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.

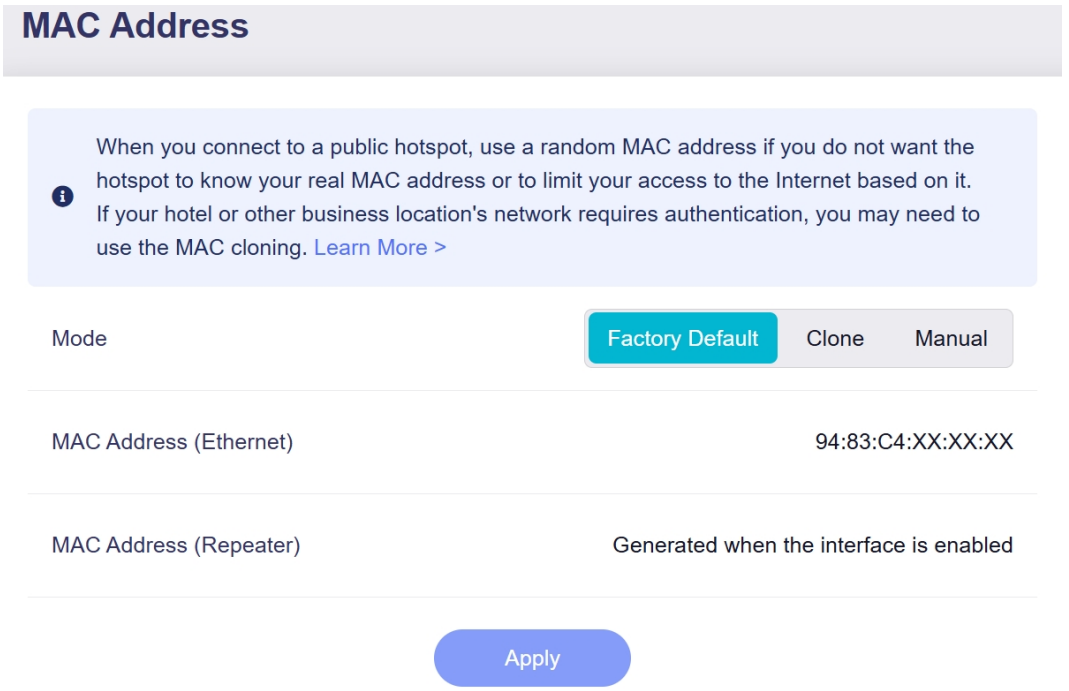
13.7.2 Méthode d'obtention du DNS

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

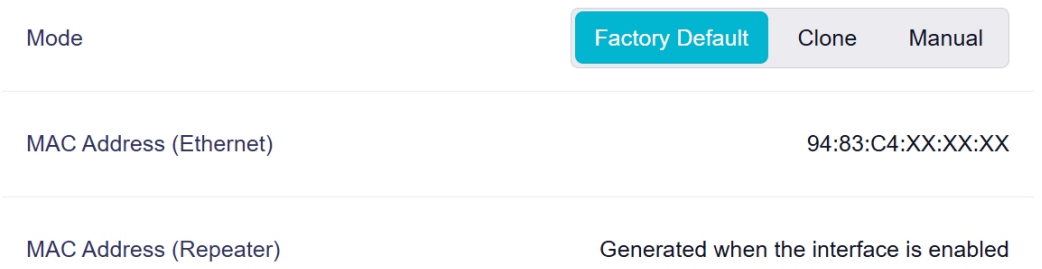
- **Automatique (Automatic)** : le routeur obtient les adresses DNS IPv6 dynamiquement, par exemple via DHCPv6.
- **Manuelle (Manual)** : saisissez les adresses des serveurs DNS IPv6 souhaités. Une configuration manuelle incorrecte peut empêcher la résolution des noms de domaine en adresses IP. Utilisez-la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

13.8 Adresse MAC

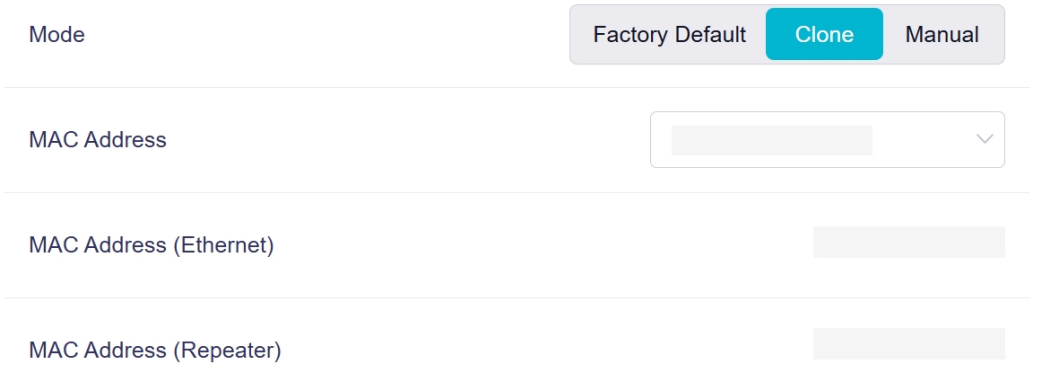
La page Adresse MAC affiche l'adresse MAC par défaut du routeur et permet de cloner celle d'un client, de saisir une adresse manuellement ou de générer une adresse aléatoire. Si l'appareil permet de configurer plusieurs ports Ethernet comme ports WAN, vous pouvez définir une adresse MAC pour chaque port. Le réglage de l'adresse MAC s'applique uniquement lorsque le port Ethernet est utilisé comme port WAN.



- **Adresse MAC définie en usine.**

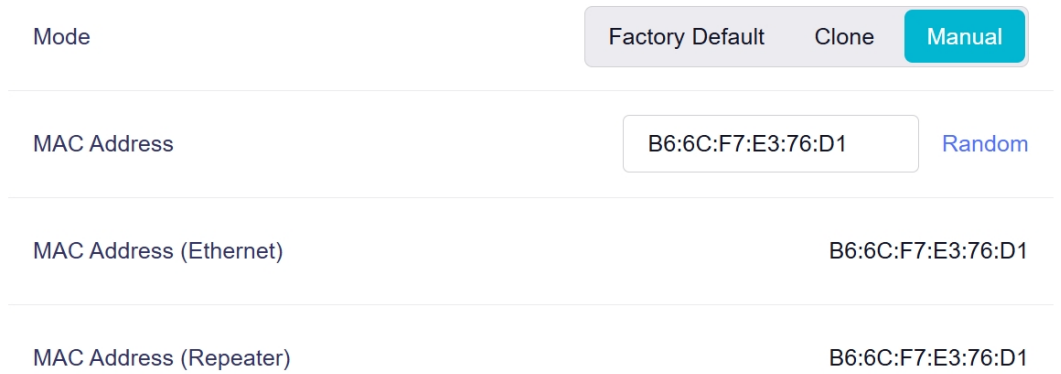


- **Cloner l’adresse MAC d’un client.**



Remarque : de nombreux appareils récents utilisent une adresse MAC aléatoire différente pour chaque réseau Wi-Fi. L’adresse MAC affichée ici peut donc différer de l’adresse réelle de l’appareil. Selon l’appareil, cette adresse aléatoire peut être appelée « adresse Wi-Fi privée » ou « adresse matérielle aléatoire ».

- **Saisir une adresse MAC manuellement ou en générer une aléatoire.**

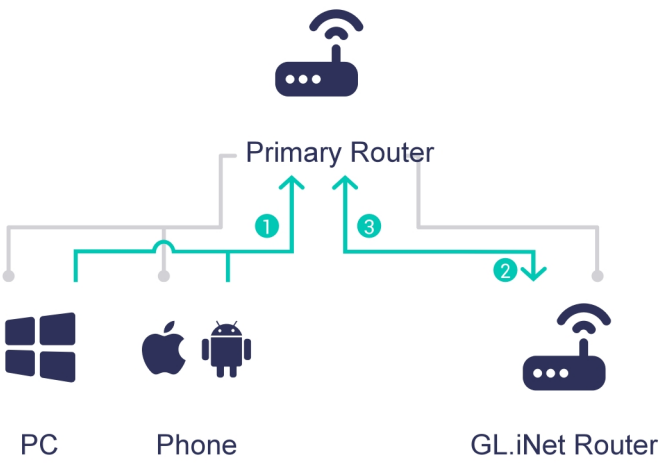


13.9 Passerelle transparente

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

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

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



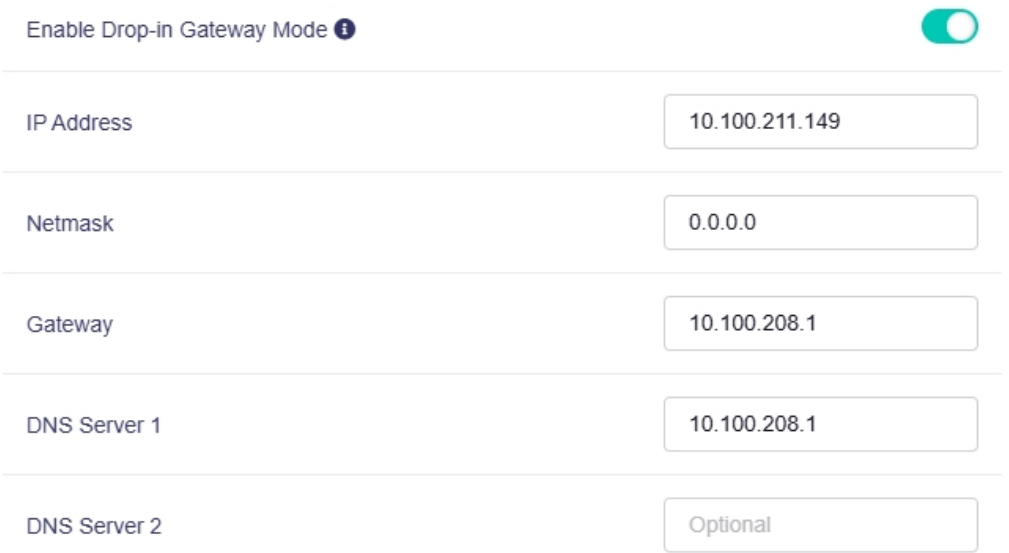
Le schéma ci-dessus comporte des lignes grises et des lignes vertes munies de trois flèches numérotées.

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

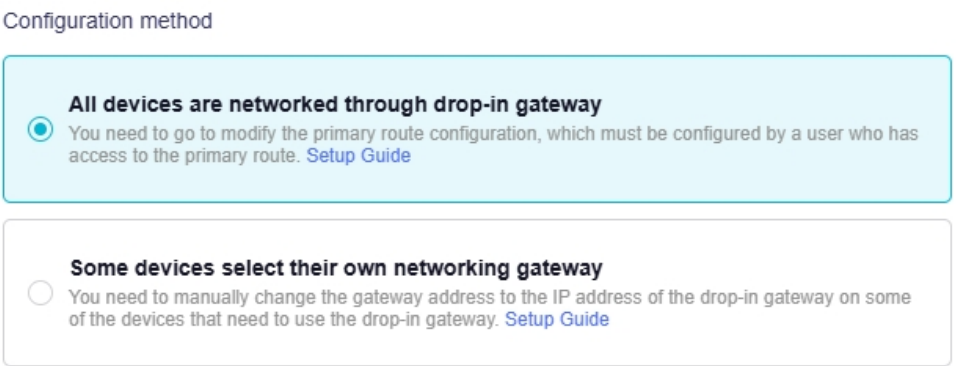
1. Le trafic des appareils clients est d'abord transmis au routeur principal.
2. Le routeur principal l'envoie au routeur GL.iNet pour traitement, par exemple le filtrage publicitaire ou le chiffrement VPN.
3. Après traitement, le trafic retourne au routeur principal, qui remet les données aux clients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

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

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



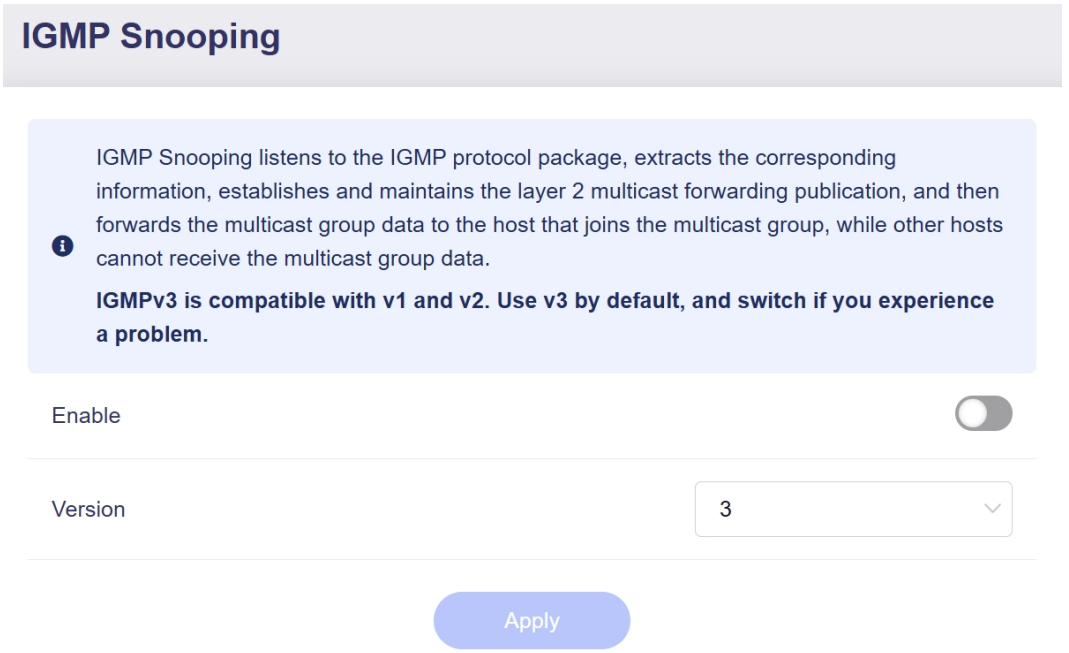
2. Choisissez la méthode de configuration, puis cliquez sur **Appliquer (Apply)**. Consultez ce tutoriel pour en savoir plus.



13.10 IGMP Snooping

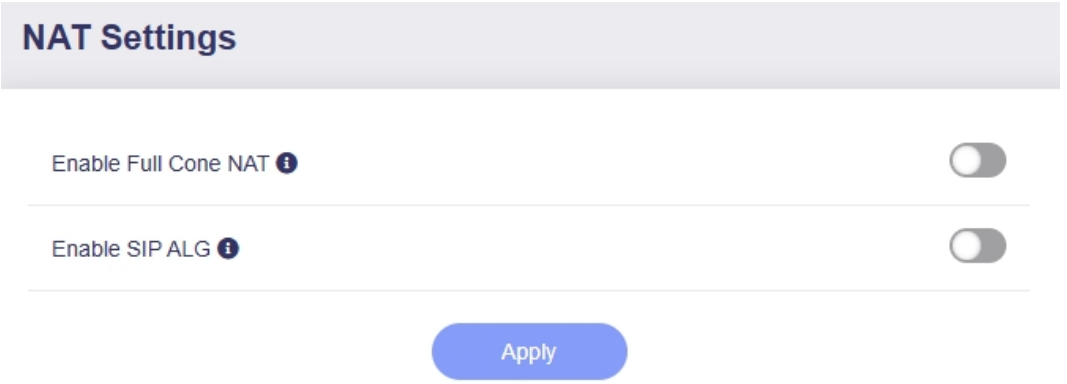
IGMP Snooping analyse les paquets IGMP, en extrait les informations et crée puis maintient une table de transfert multicast de couche 2. Les données multicast sont ensuite transmises uniquement aux hôtes ayant rejoint le groupe correspondant.

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



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

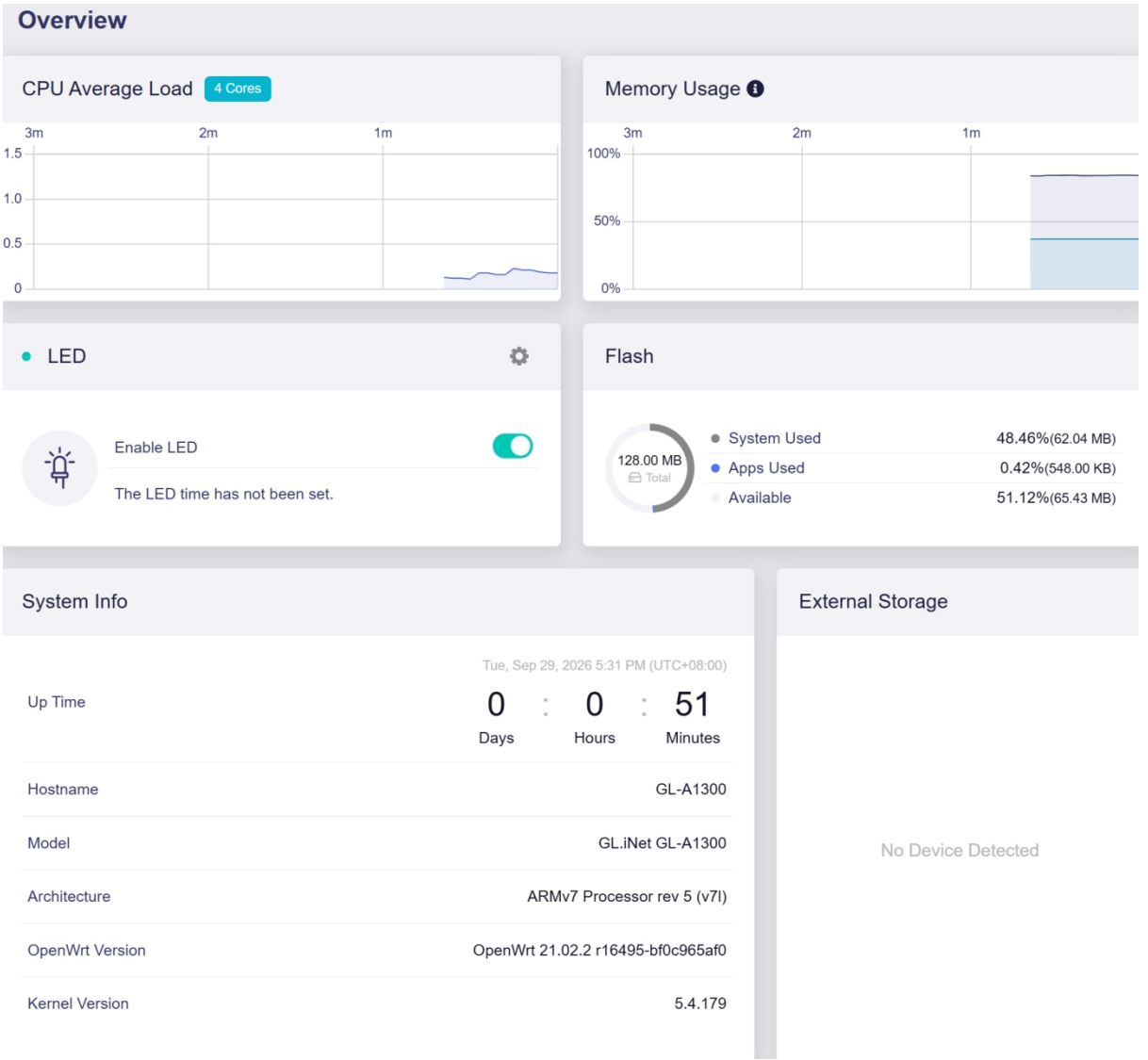
Système

Ce chapitre présente les outils de gestion de l’appareil : vue d’ensemble, mises 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

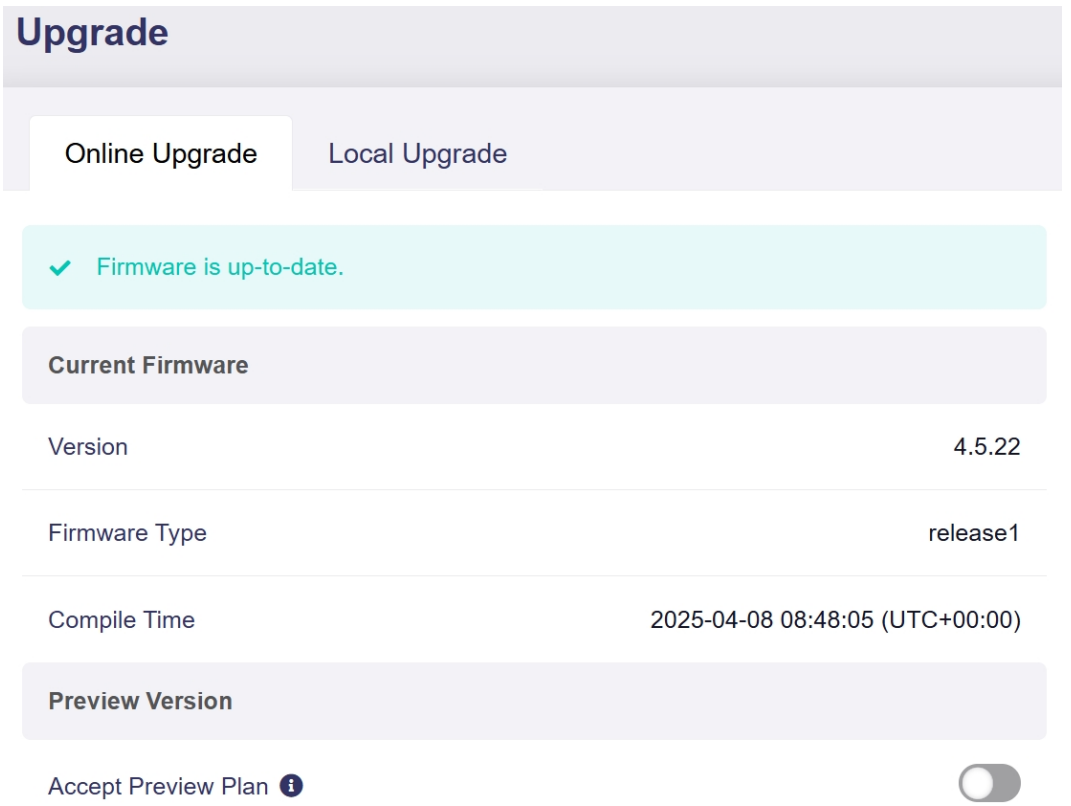


14.2 Mise à jour

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



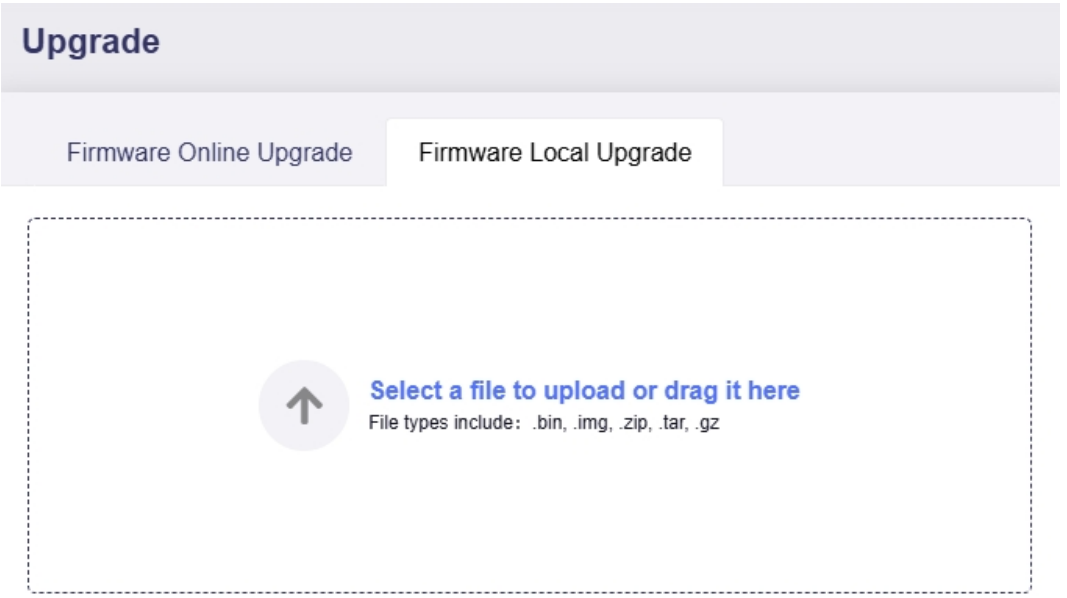
Si l'option **Accepter le programme de préversion (Accept Preview Plan)** est activée, vous pouvez essayer de nouvelles fonctionnalités avant la publication de la version définitive et nous faire part de vos commentaires. Il suffit de l'activer une fois pour qu'elle reste activée. Ces mises à jour peuvent toutefois être instables.

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

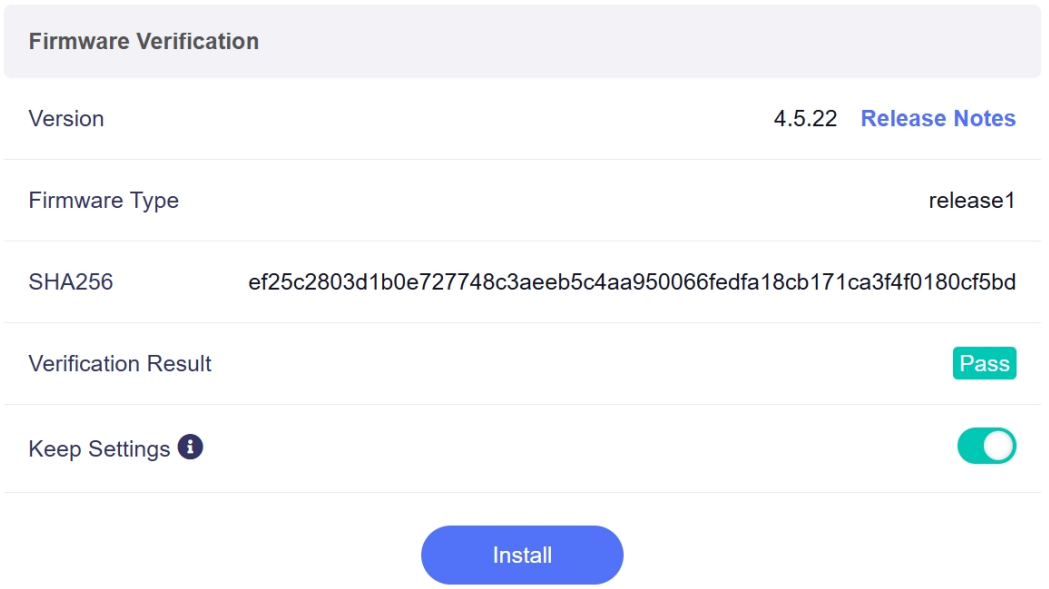
14.2.2 Mise à jour locale

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

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



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



Si l'option **Conserver les paramètres (Keep Settings)** est activée, les paramètres actuels sont conservés. Toutefois, les paquets installés manuellement doivent être réinstallés après

la mise à niveau. N’activez pas cette option lorsque vous revenez à une version antérieure du micrologiciel.

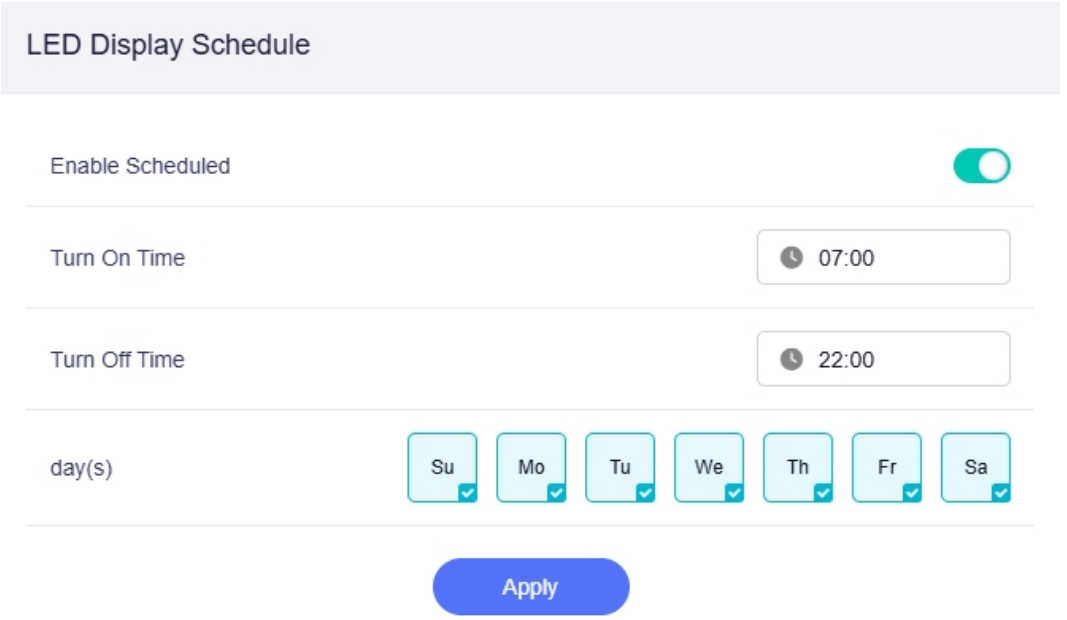
14.3 Tâches planifiées

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 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

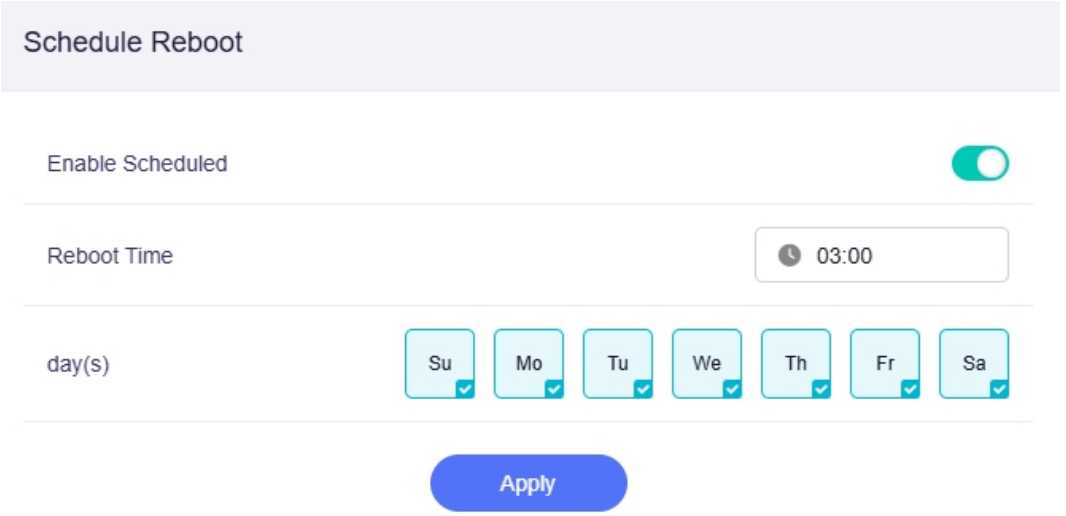
Définissez le planning du voyant si nécessaire, puis cliquez sur **Appliquer (Apply)**.



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

14.3.2 Redémarrage planifié

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



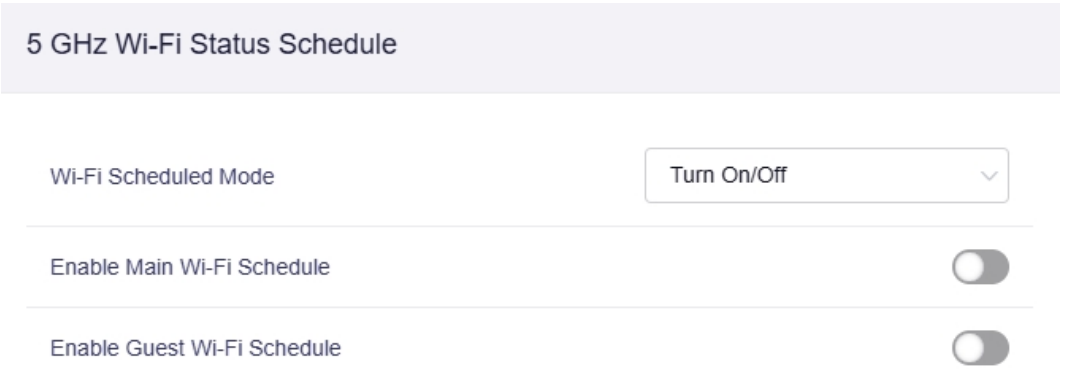
- **Activer la programmation (Enable Scheduled)** : active le redémarrage planifié.
- **Heure de redémarrage (Reboot Time)** : heure à laquelle le routeur redémarre, par exemple 03:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

14.3.3 Programmation du Wi-Fi 5 GHz

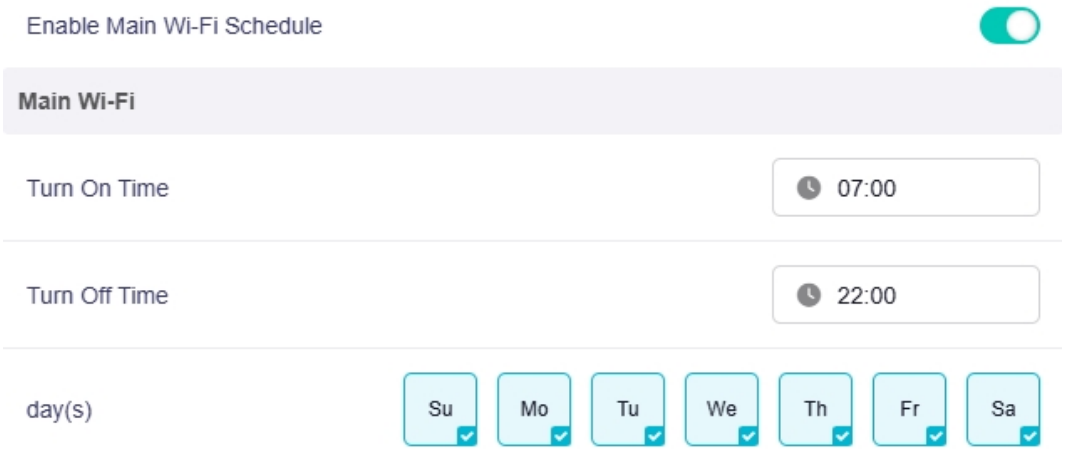
Cette fonction permet de programmer le Wi-Fi 5 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

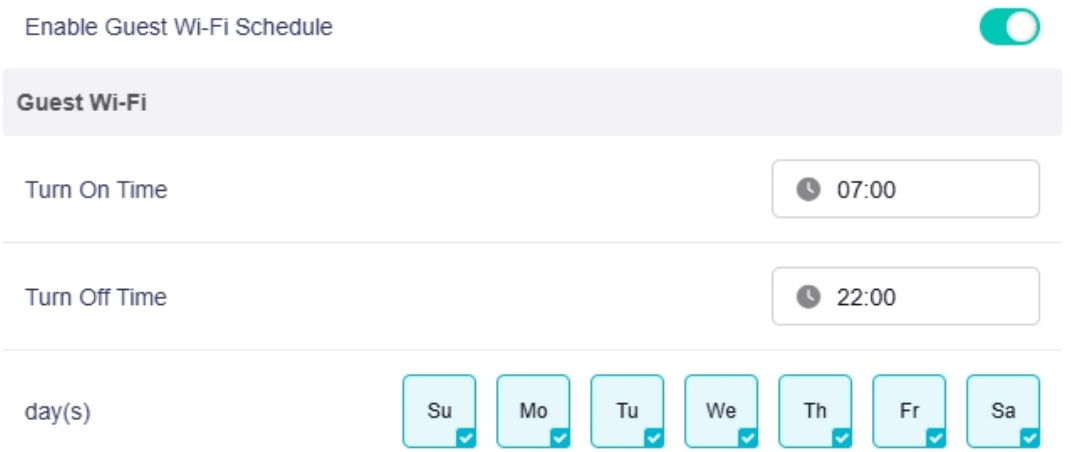
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 5 GHz.



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

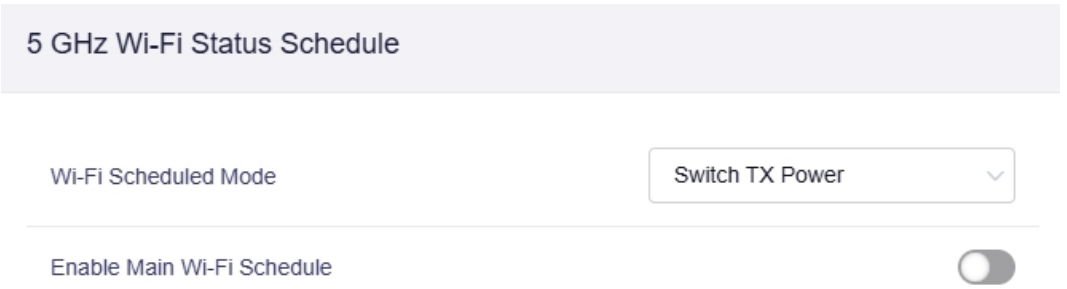


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 5 GHz et les jours concernés.

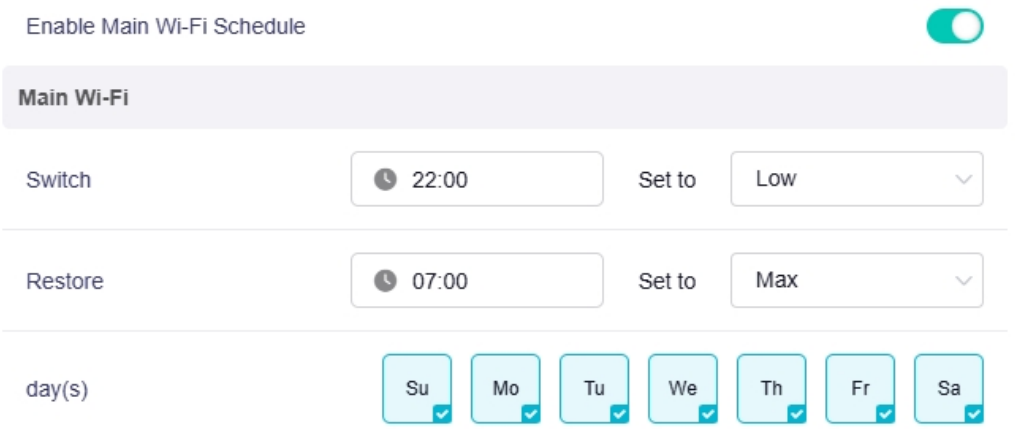


Mode 2 : Modifier la puissance d'émission

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



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



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

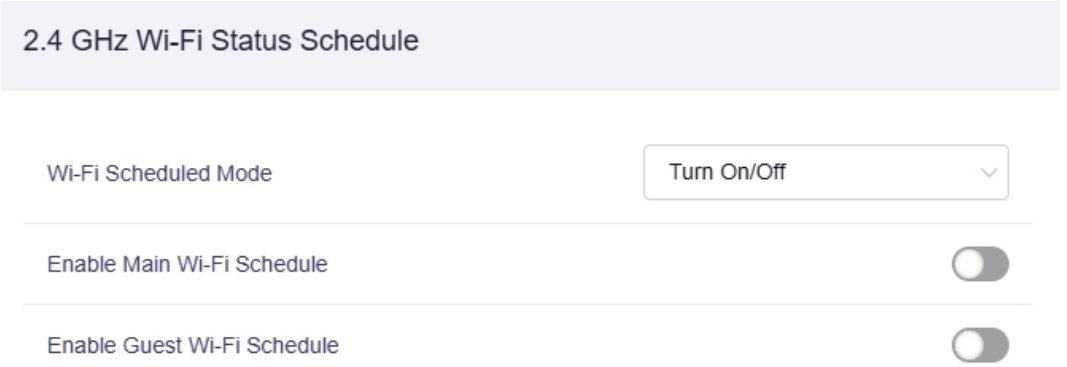
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

14.3.4 Programmation du Wi-Fi 2,4 GHz

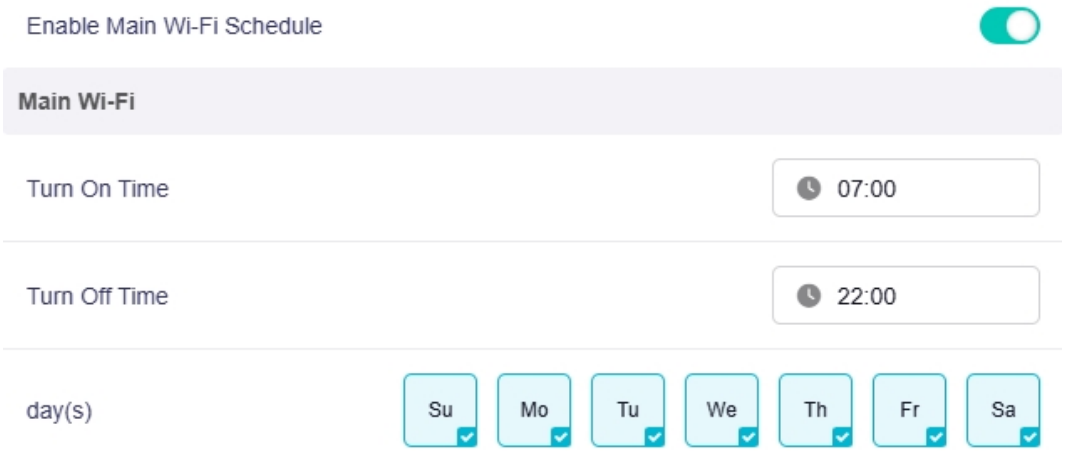
Cette fonction permet de programmer le Wi-Fi 2,4 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

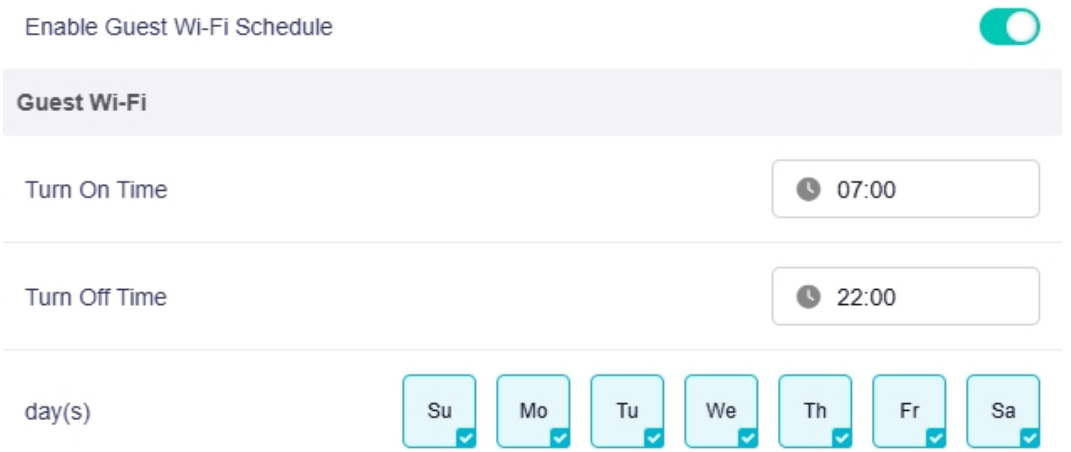
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 2,4 GHz.



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

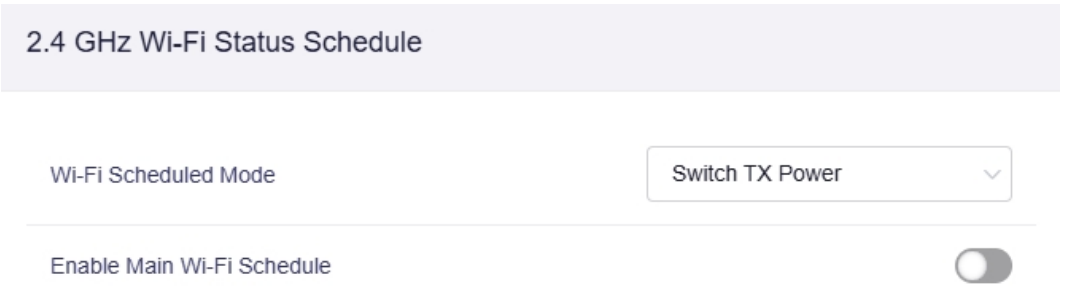


- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 2,4 GHz et les jours concernés.

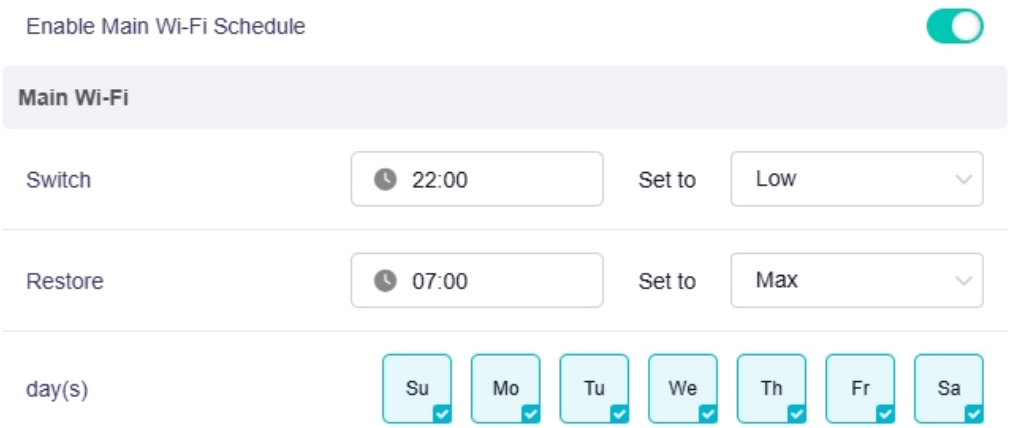


Mode 2 : Modifier la puissance d'émission

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



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

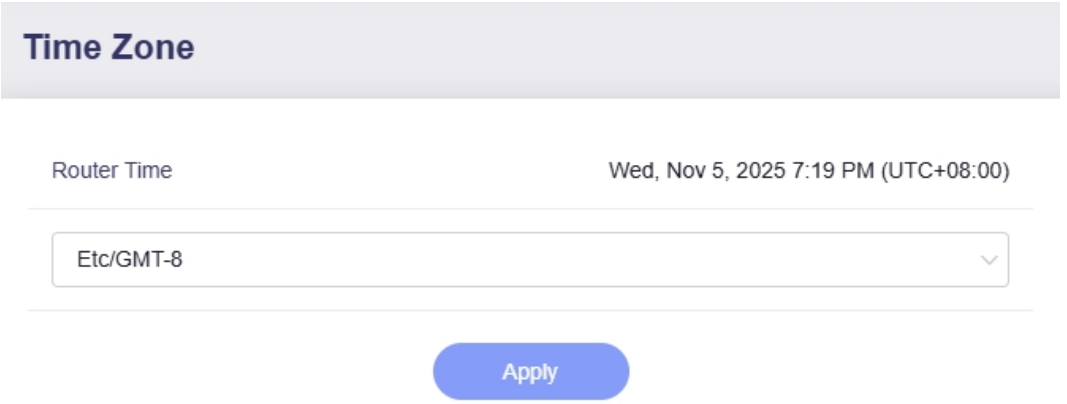


- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.

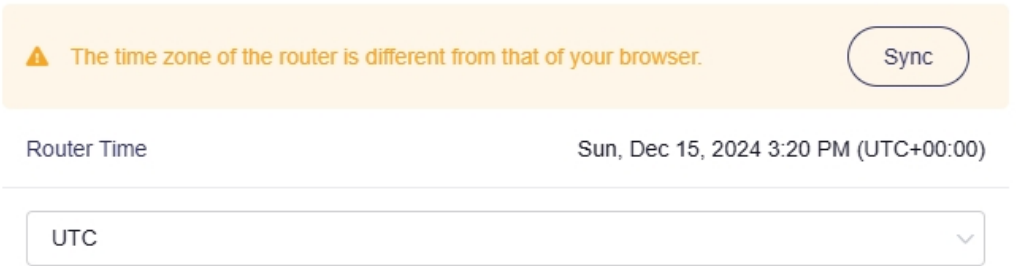
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

14.4 Fuseau horaire

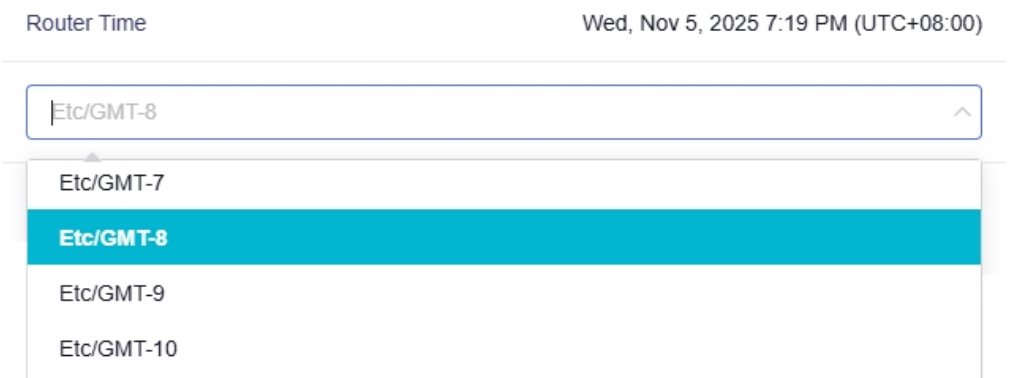
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)**. La page affiche la date et l'heure système du routeur ainsi que le décalage du fuseau horaire.



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.

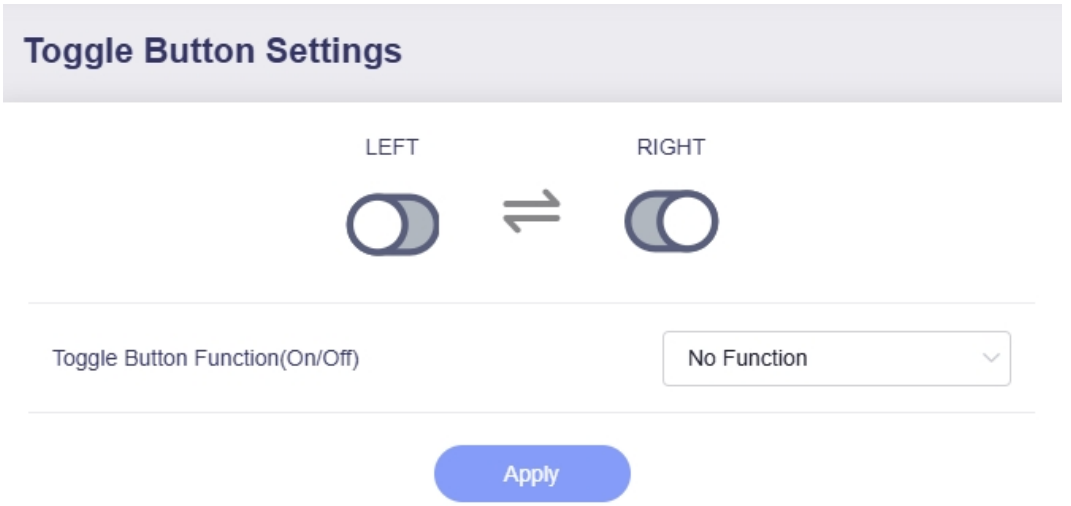


Pour changer de fuseau, sélectionnez celui qui convient dans la liste afin que l'heure du routeur corresponde à l'heure locale.

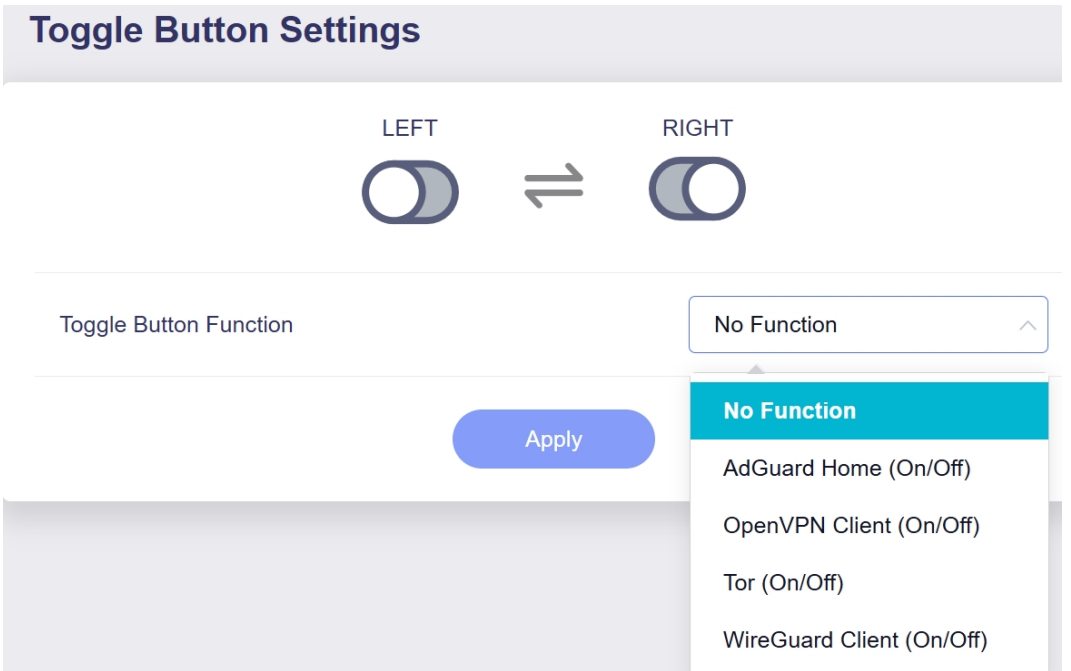


14.5 Paramètres du commutateur

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

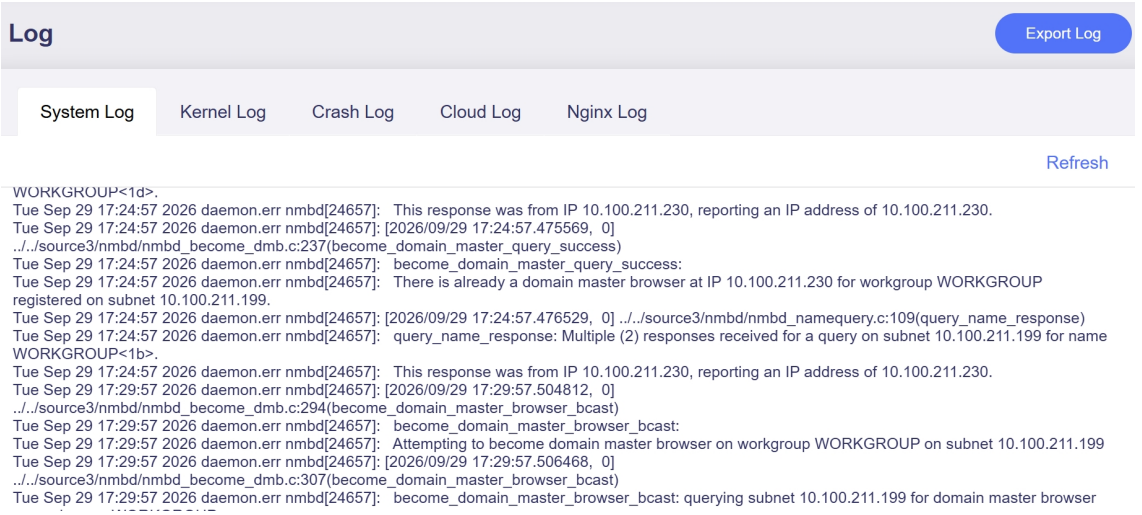


Par défaut, aucune fonction n'est attribuée au commutateur. Vous pouvez le configurer pour activer ou désactiver certaines fonctions d'un simple geste.



14.6 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.



- **Actualiser (Refresh)** : met à jour les journaux.
- **Exporter le journal (Export Log)** : exporte les journaux et les informations de débogage.

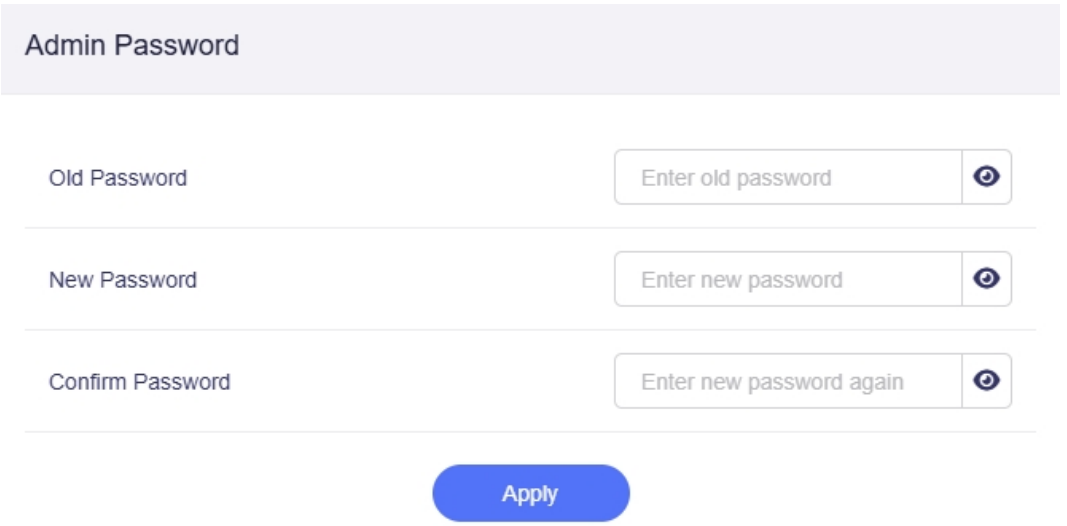
14.7 Sécurité

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

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

14.7.1 Mot de passe administrateur

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

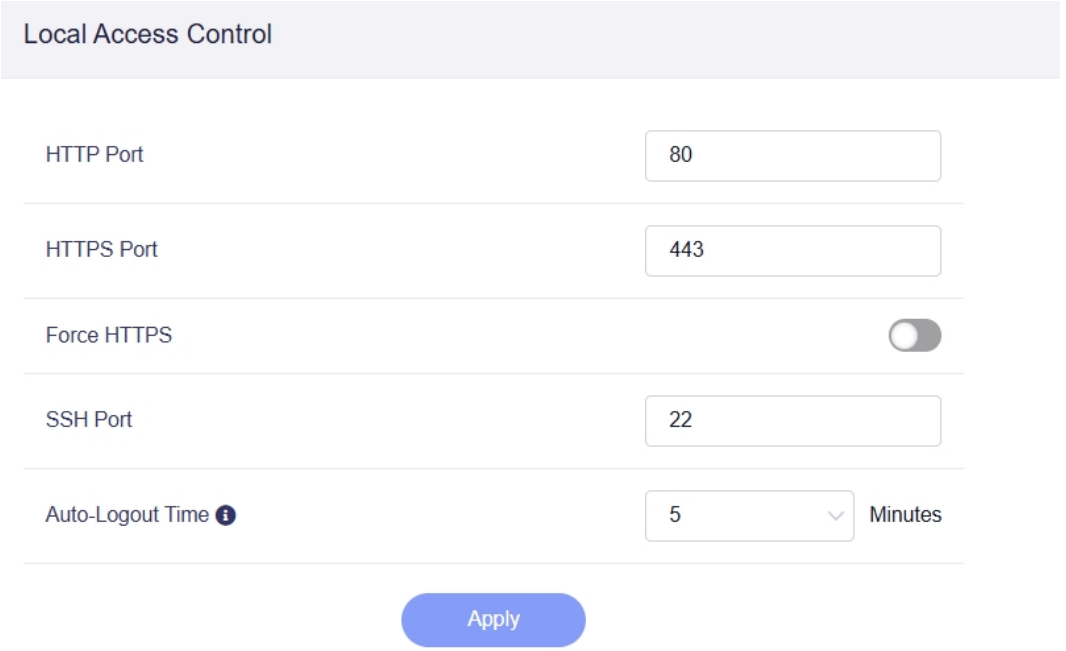


Le mot de passe administrateur doit respecter les règles suivantes :

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.

14.7.2 Contrôle des accès locaux

Cette section permet de gérer l'accès aux différentes interfaces du routeur, notamment au panneau d'administration et à SSH. Elle peut empêcher les tentatives de détection et d'intrusion sur le port par défaut et éviter les problèmes réseau dus aux conflits de ports.

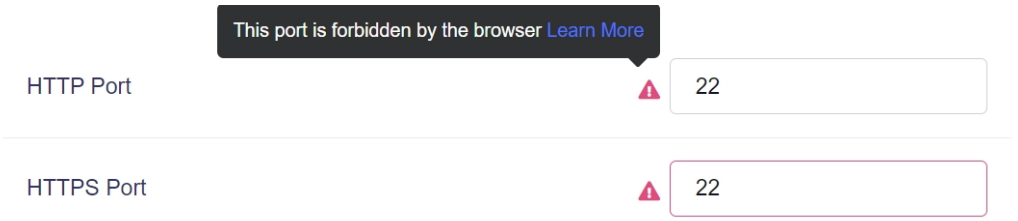


Interface d'administration

- **Port HTTP (HTTP Port)** : 80 par défaut, pour l'accès HTTP non chiffré à l'interface Web.
- **Port HTTPS (HTTPS Port)** : 443 par défaut, pour l'accès HTTPS sécurisé à l'interface Web.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à l'interface Web.
- **Port SSH (SSH Port)** : 22 par défaut, utilisé pour l'accès SSH au routeur.
- **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.

Remarque :

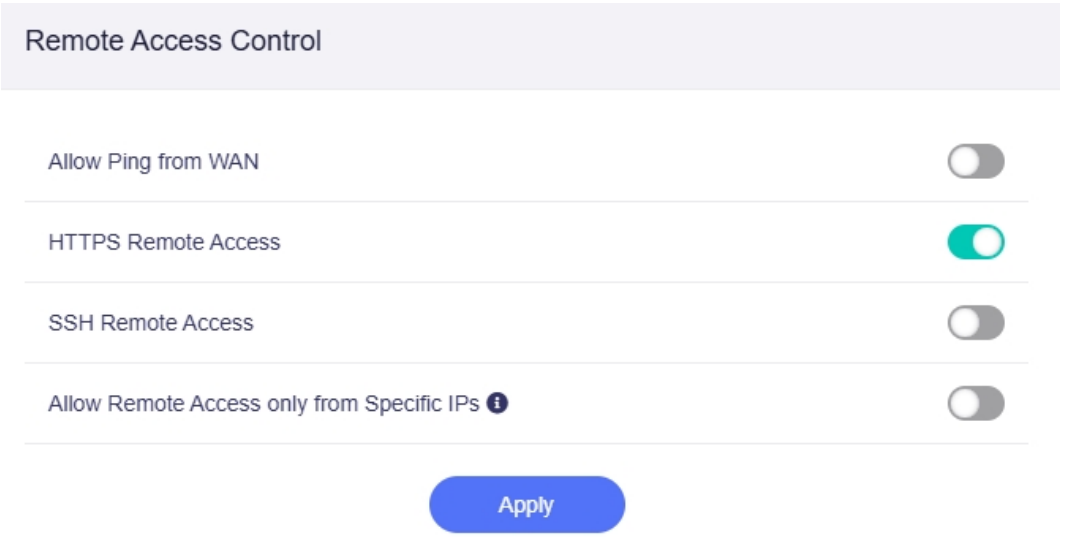
1. Si le port choisi entre en conflit avec un port réservé, notamment par les navigateurs ou les conventions réseau, le message « Ce port est interdit par le navigateur » (This port is forbidden by the browser) s'affiche.



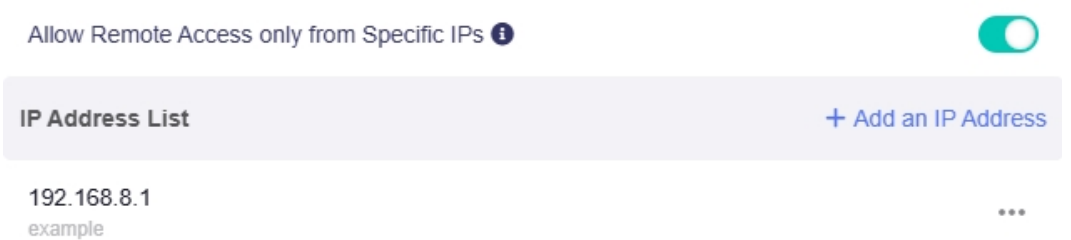
2. Si vous modifiez un port dans le micrologiciel, renseignez le nouveau numéro pour accéder à l'interface d'administration. Si vous l'avez oublié, réinitialisez le routeur pour rétablir le port par défaut.

14.7.3 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.



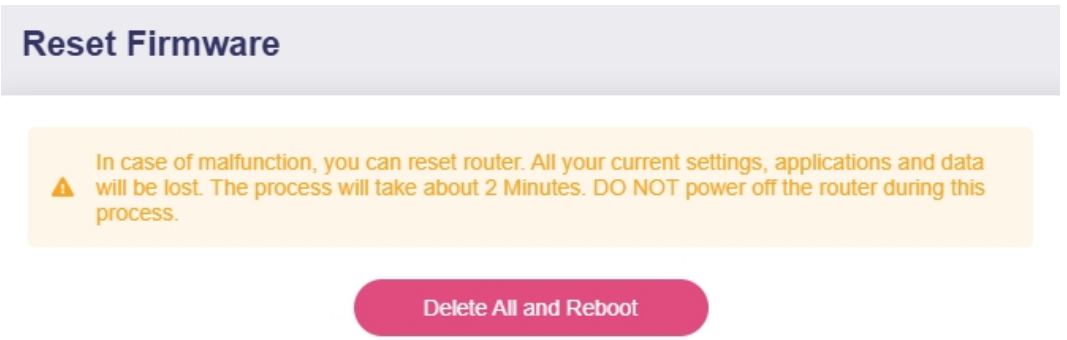
- **Autoriser le ping depuis le WAN (Allow Ping from WAN)** : permet de vérifier que le routeur est joignable depuis le WAN en cas de problème et de mesurer la latence et les pertes de paquets.
- **Accès HTTPS à distance (HTTPS Remote Access)** : permet d’accéder de manière sécurisée à l’interface Web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



14.8 Réinitialisation du micrologiciel

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

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



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

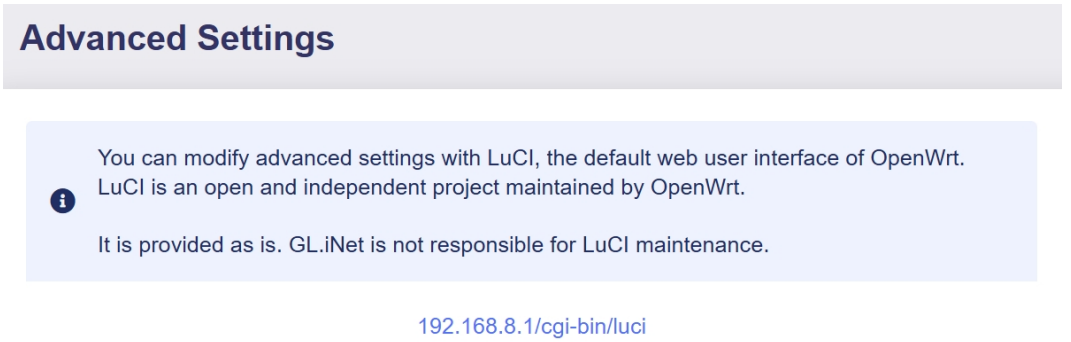
Si vous ne pouvez pas accéder à l'interface Web, utilisez le bouton physique de réinitialisation situé sur le côté du routeur.

14.9 Paramètres avancés

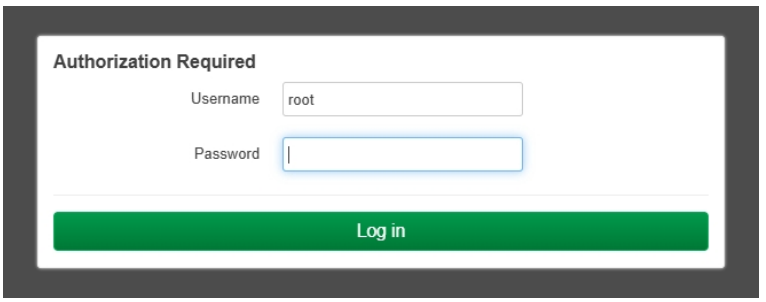
Dans l'interface Web, ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)**. Vous pouvez y modifier les paramètres avancés dans LuCI, l'interface Web par défaut d'OpenWrt. LuCI est un projet ouvert et indépendant maintenu par OpenWrt et fourni en l'état. GL.iNet n'assure pas sa maintenance.

Pour vous connecter à LuCI, procédez comme suit.

1. Cliquez sur le lien d'accès pour ouvrir la page de connexion LuCI.



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



L'interface LuCI s'ouvre.

