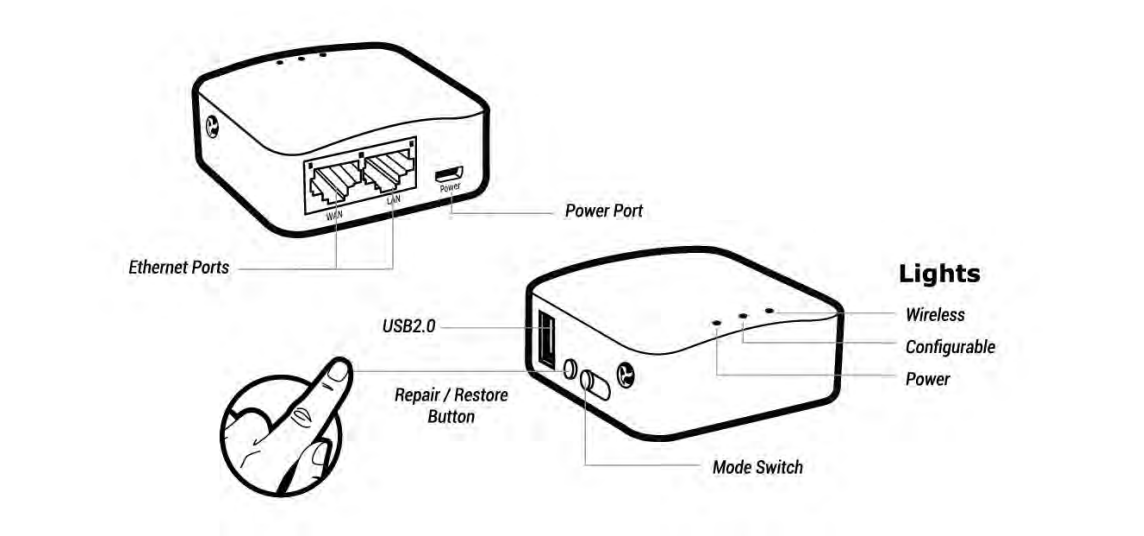
Démarrage avec GL.iNet Mini Router de Voyage

Modèles:

GL-MT300N, GL-MT300N-V2

GL-AR150, GL-AR150-PoE, GL-AR150-Ext-2, GL-AR150-Ext-PoE-2

GL-AR300M, GL-AR300M-Ext, GL-AR300M16, GL-AR300M16-Ext, GL-AR300M-Lite

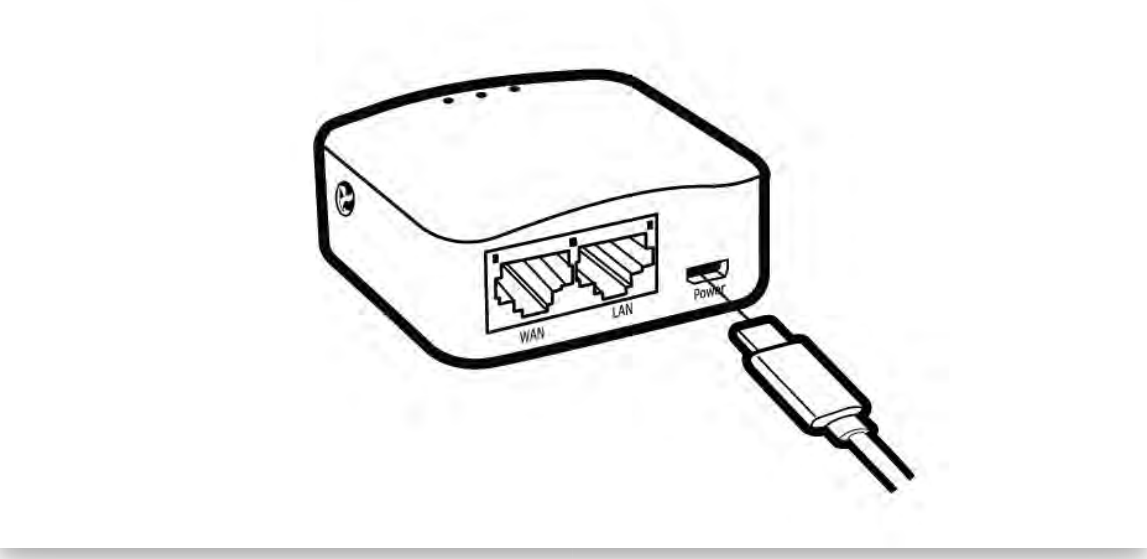


Note: GL-AR300M-Lite n'a qu'un seul port Ethernet.

---

1. Puissance sur

Branchez le câble d'alimentation Micro USB sur le port d'alimentation du routeur. Assurez-vous d'utiliser un adaptateur d'alimentation standard 5V/2A. Dans le cas contraire, il peut entraîner un dysfonctionnement.



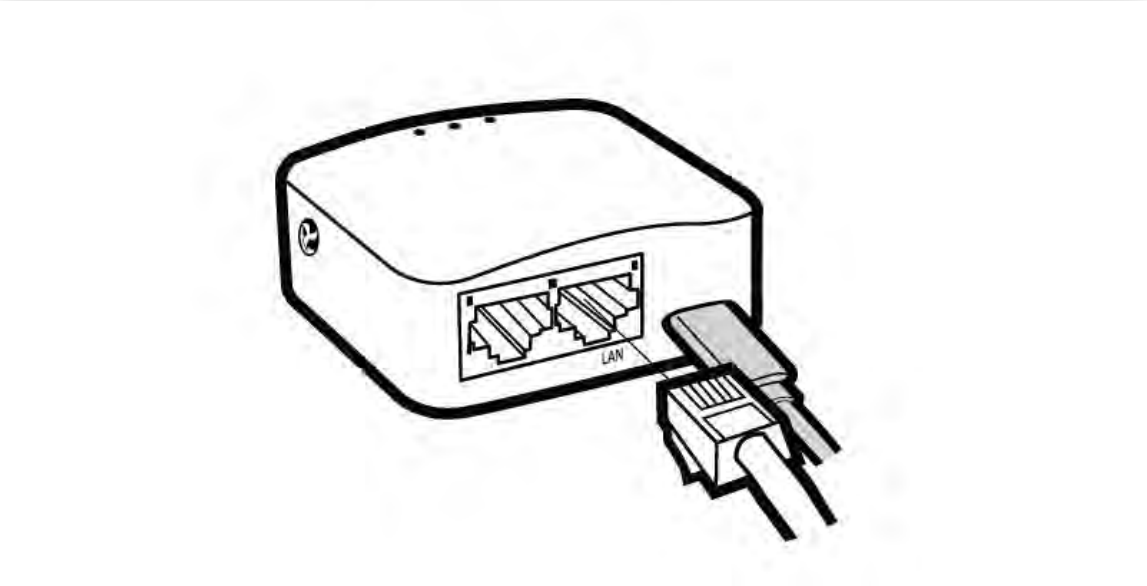
2. Connecter

Vous pouvez vous connecter au routeur via un câble Ethernet ou un Wi-Fi.

Remarque: Cette étape ne relie vos appareils qu'au réseau local (LAN) du routeur. Vous ne pouvez pas accéder à Internet à l'heure actuelle. Afin de vous connecter à Internet, veuillez terminer les procédures de configuration ci-dessous, puis suivre Internet pour mettre en place une connexion Internet.

Connectez-vous via LAN

Connectez votre appareil au port LAN du routeur via un câble Ethernet.



Remarque: GL-AR300M-Lite ne dispose que d'un port Ethernet qui fonctionne en WAN par défaut.

Vous ne pouvez vous y connecter via Wi-Fi que lorsque vous avez configuré le routeur. Une fois que vous vous êtes connecté à lui, vous pouvez changer le port WAN en port LAN dans Internet afin que vous puissiez vous y connecter via un câble Ethernet.

Se connecter via Wi-Fi

Recherchez le SSID du routeur dans votre appareil et saisissez le mot de passe par défaut: ***goodlife***.

Note: Le SSID a été imprimé sur l'étiquette du fond du routeur avec les formats suivants:

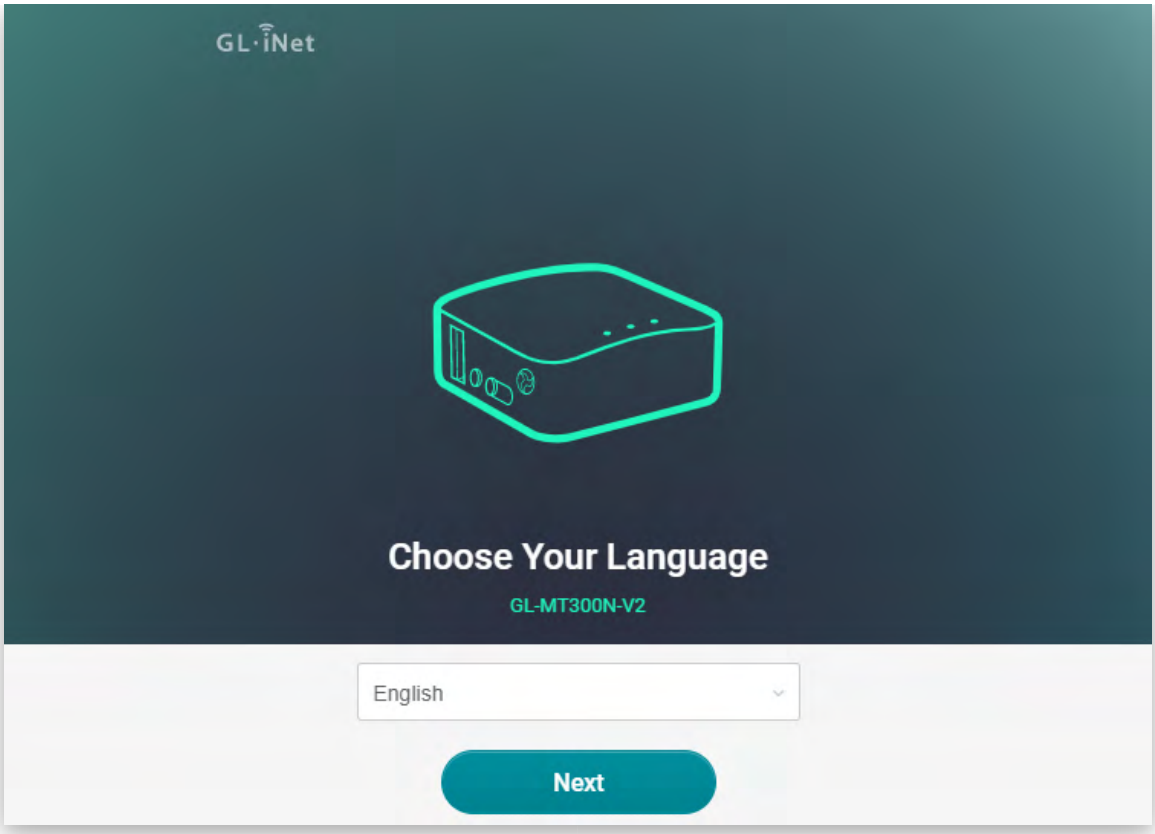
- **GL-MT300N-XXX**
- **GL-MT300N-V2-XXX**
- **GL-AR150-XXX**
- **GL-AR300M-XXX**
- **GL-AR300M-XXX-NOR**

3. Accès au panel d'administration web

Ouvrez un navigateur Web (nous recommandons Chrome, firefox) et visitez http://192.168.8.1. Vous serez dirigé vers la configuration initiale du panneau d'administration web.

1) Configuration des langues

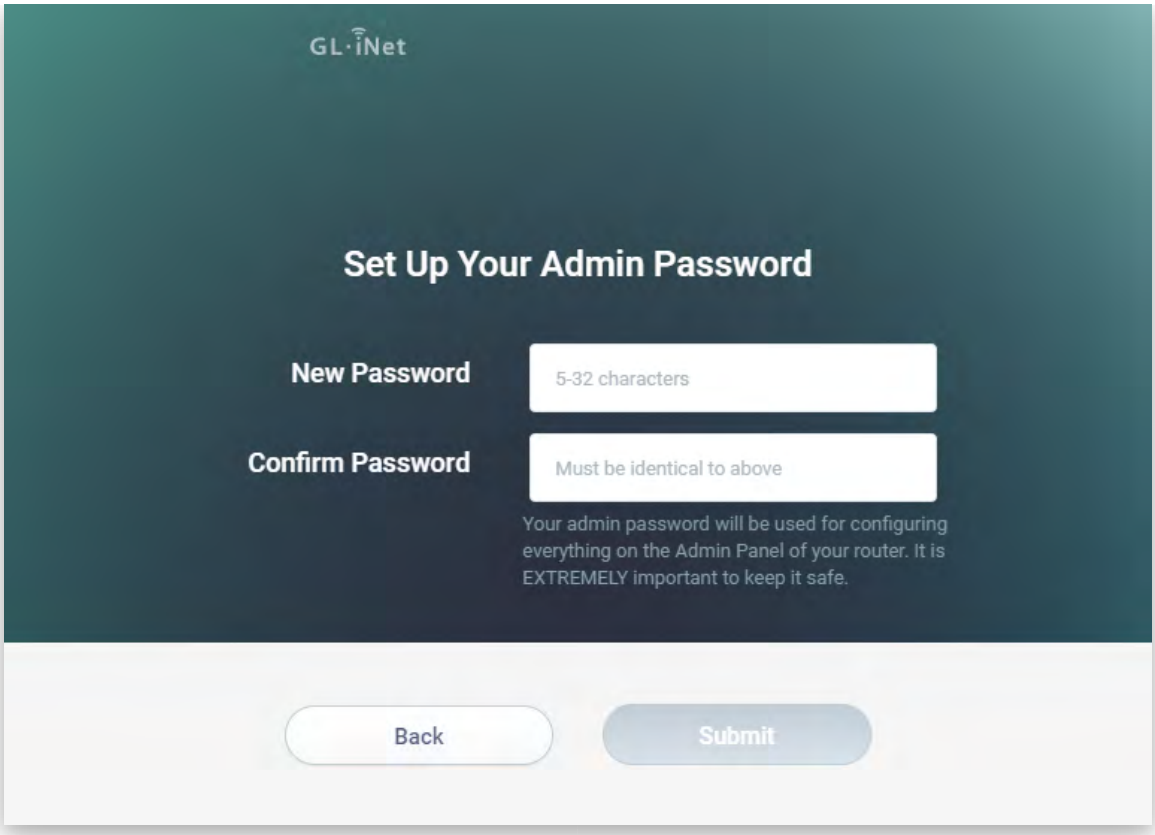
Vous devez choisir la langue d'affichage du panneau d'administration. Actuellement, nos routeurs sont favorables à **l'anglais**, **à l'anglais**, **à l'allemand**, **au français**, **à l'espagnol**, **à l'italien 日本語, au niveau de l'anglaisРусский**, au **, au , au , au , au , au , au , au ,** au



Note: Si votre navigateur se réoriente toujours vers LuCI (http://192.168.8.1/cgi-bin/luci), vous pouvez visiter: http://192.168.8.1/index au lieu de http://192.168.8.1.

2) Paramétrage du mot de passe de l'administration

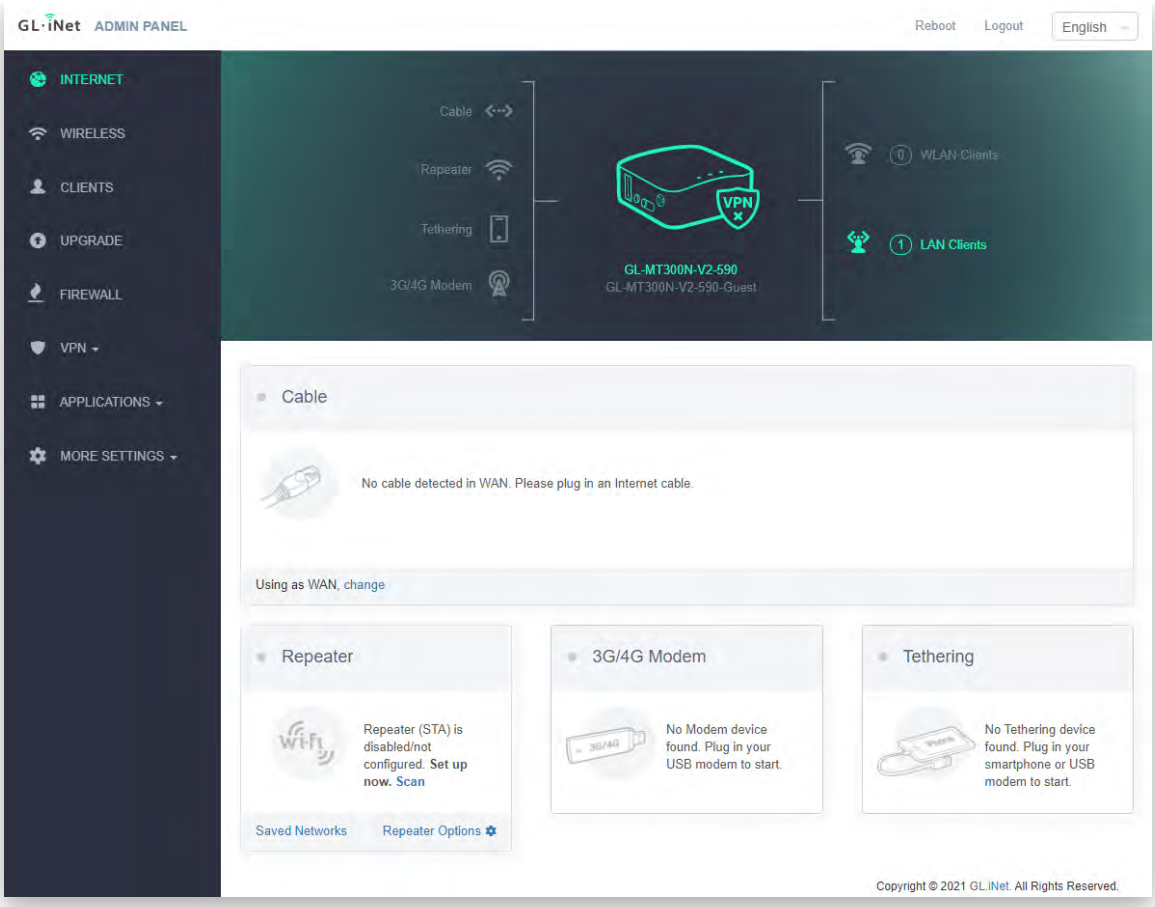
Il n'y a pas de mot de passe par défaut pour ce panneau d'administration. Vous devez définir votre propre mot de passe, qui doit être d'au moins 5 caractères. Ensuite, cliquez sur `Submit` de procéder.



Remarque: Ce mot de passe est destiné à ce panneau d'administration Web et au système Linux intégré. Il ne changera pas votre mot de passe Wi-Fi.

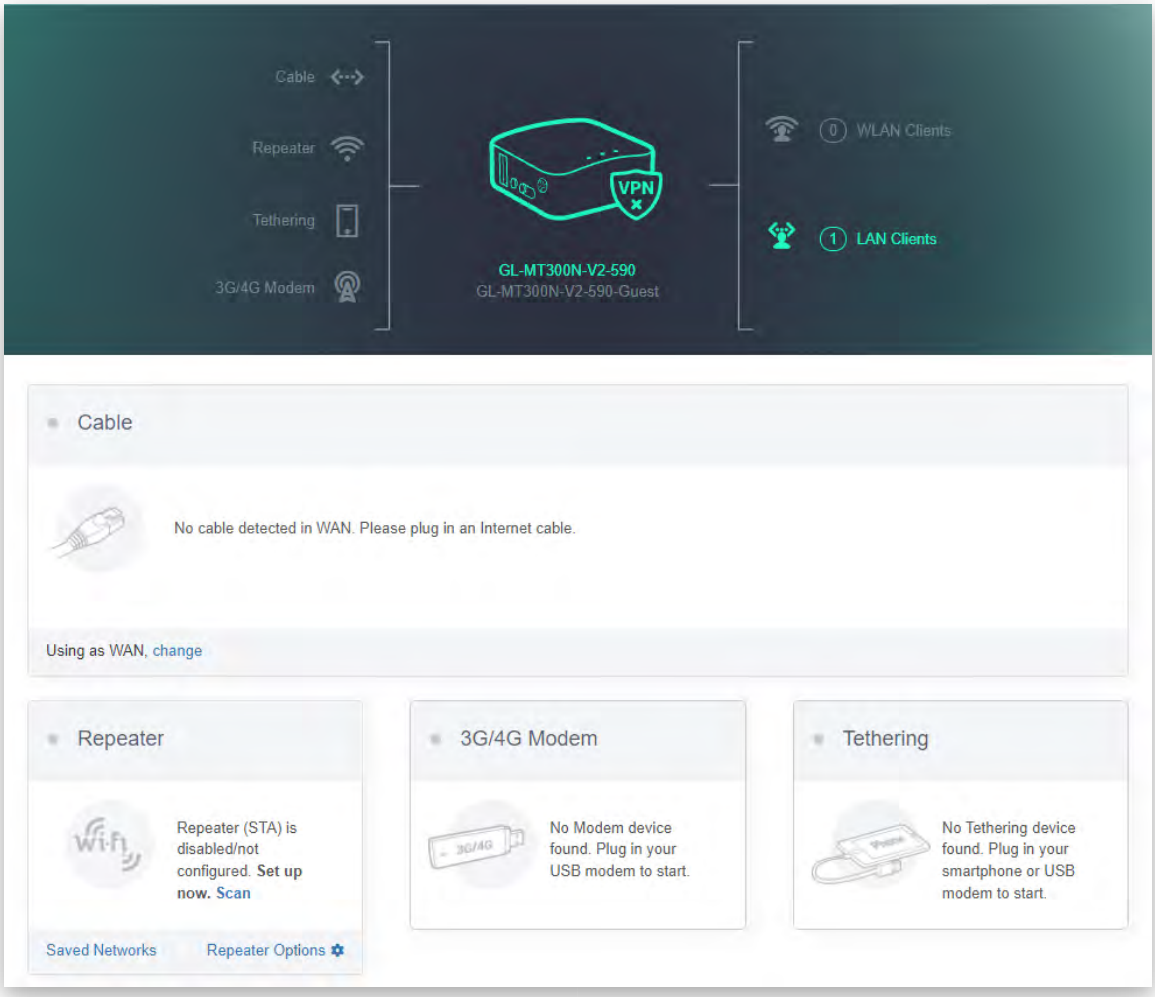
3) Panneau d'administration

Après la configuration initiale, vous entrerez dans le Web Admin Panel du routeur. Il vous permet de vérifier l'état et de gérer les paramètres du routeur.

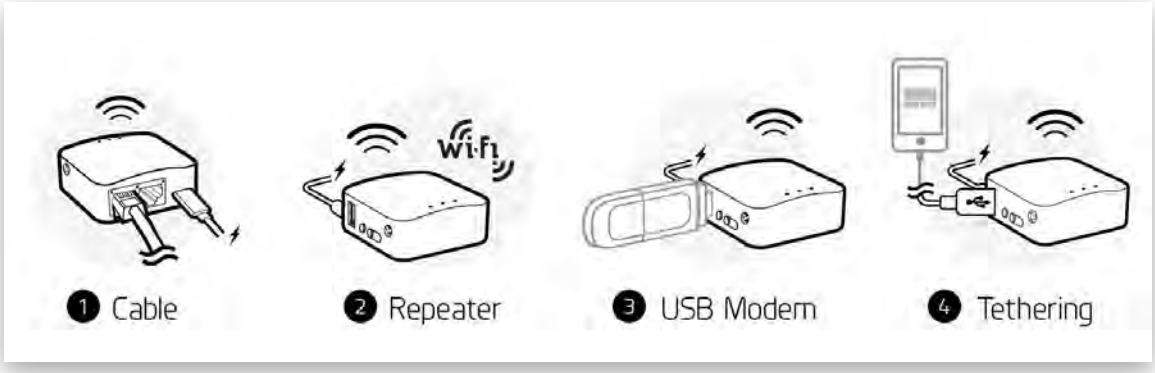

GL·iNet ADMIN PANEL
Reboot
Logout
English
INTERNET
WIRELESS
CLIENTS
UPGRADE
FIREWALL
VPN
APPLICATIONS
MORE SETTINGS
Cable
Repeater
Tethering
3G/4G Modem
VPN
GL-MT300N-V2-590
GL-MT300N-V2-590-Guest
0 WLAN Clients
1 LAN Clients
Cable
No cable detected in WAN. Please plug in an Internet cable.
Using as WAN, change
Repeater
Repeater (STA) is disabled/not configured. Set up now. Scan
Saved Networks
Repeater Options
3G/4G Modem
No Modem device found. Plug in your USB modem to start.
Tethering
No Tethering device found. Plug in your smartphone or USB modem to start.
Copyright © 2021 GL.iNet. All Rights Reserved.

INTERNET

Sur le côté gauche du panneau d'administration web



Il y a au total 4 types de méthode de connexion que vous pouvez utiliser pour accéder à Internet: **câble**, **répéteur**, **modem 3G/4G** et **Tethering**.



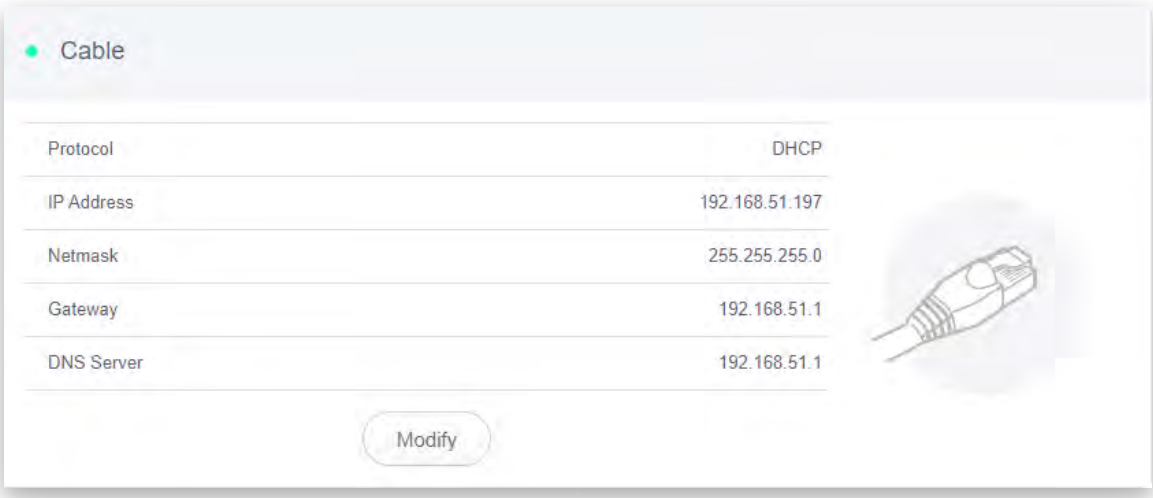
1. Câble

Connectez le routeur au modem ou au routeur principal via le câble Ethernet pour accéder à Internet.

Remarque: Avant de brancher le câble Ethernet sur le port WAN du routeur, vous pouvez cliquer sur `Use as LAN` *de placer le port WAN comme un port LAN. C'est utile lorsque vous utilisez le routeur comme répéteur. En conséquence, vous pouvez avoir un autre port LAN.*

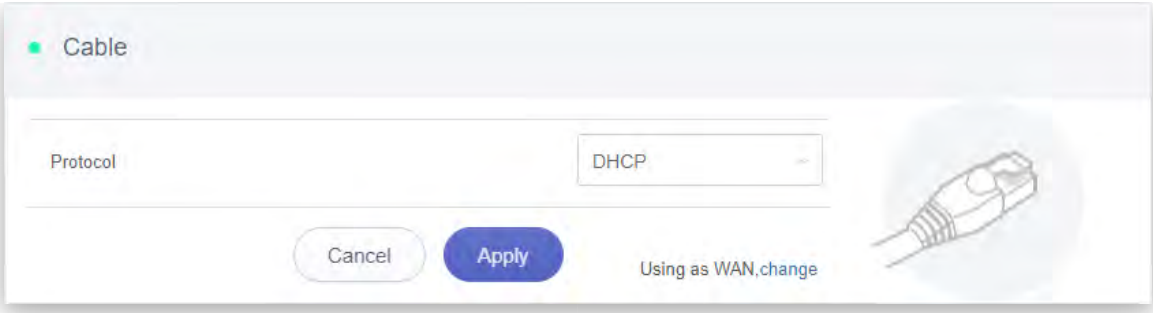


Brancher le câble Ethernet dans le port WAN du routeur. Les informations de votre connexion seront indiquées dans la section Cable. DHCP est le protocole par défaut. Vous pouvez cliquer sur `Modify` de modifier le protocole.



DHCP

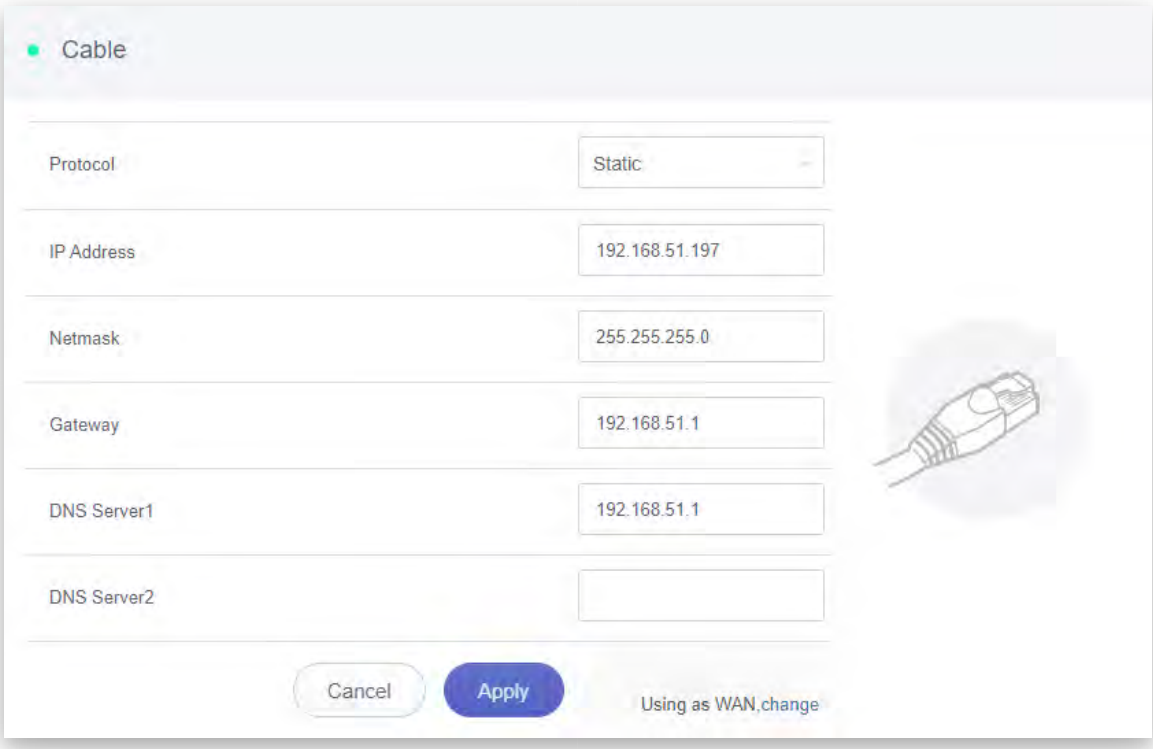
DHCP est le protocole par défaut et le plus courant. Il ne nécessite aucune configuration manuelle.



Statique

Static est nécessaire si votre fournisseur de services Internet (ISP) a fourni une adresse IP fixe pour vous ou si vous souhaitez configurer manuellement les informations réseau telles que l'adresse IP, la passerelle, le Netmask.

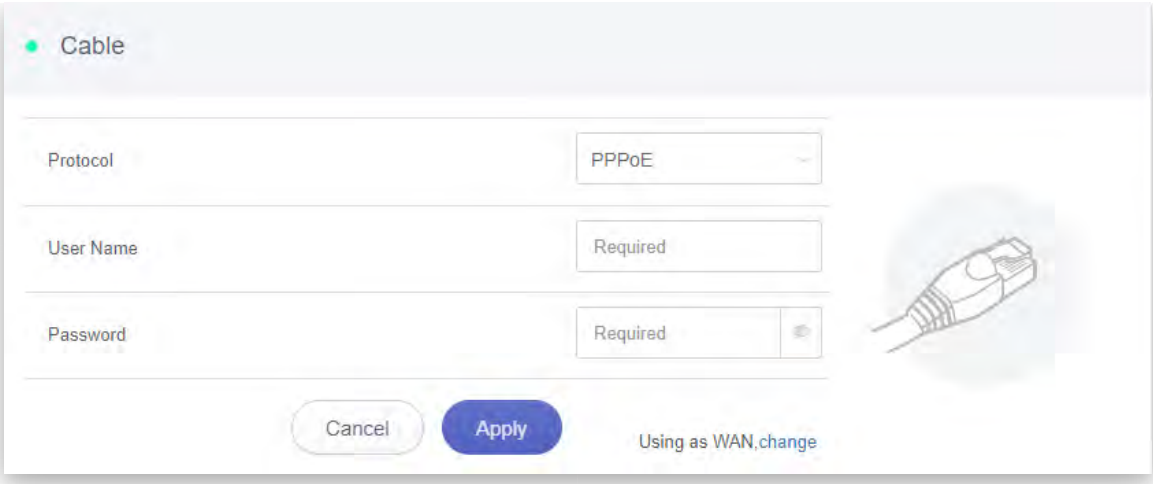
Les réglages actuels seront automatiquement remplis une fois que vous aurez choisi Static. Changez-le en fonction de vos besoins, puis cliquez sur `Apply`.



PPPoE

Le PPPoE est exigé par de nombreux fournisseurs de services Internet (FSI). En général, votre FAI vous donnera un modem et vous fournira un nom d'utilisateur et mot de passe dont vous avez besoin lorsque vous créez la connexion Internet.

Sous le protocole PPPoE, entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur `Apply`.

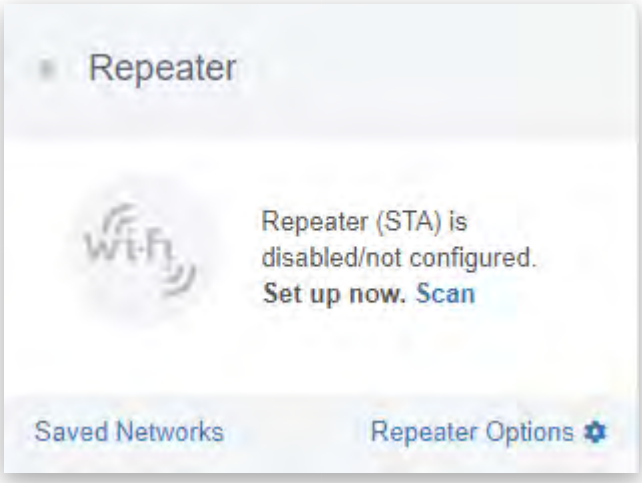


2. Répéteur

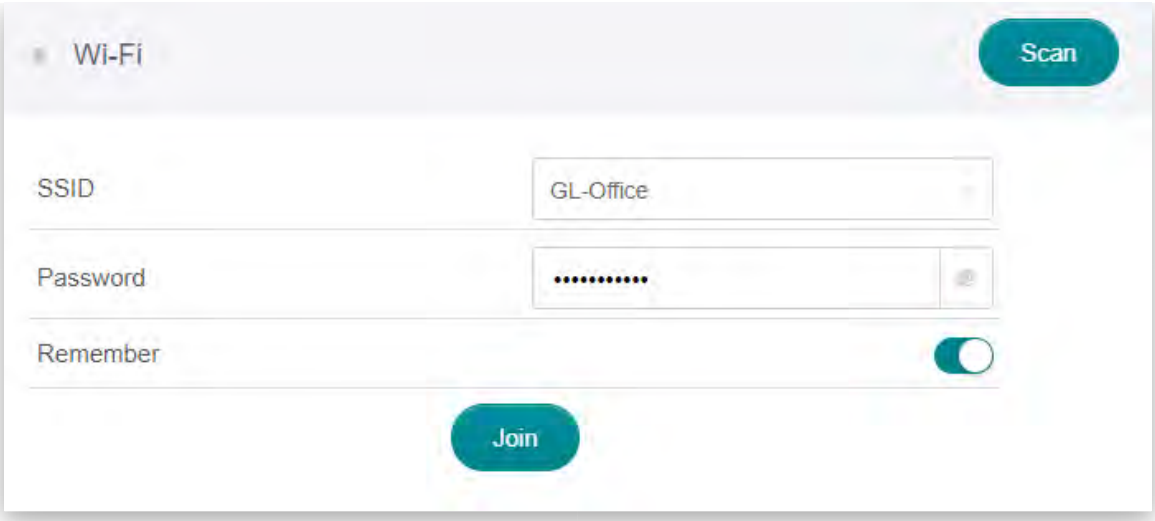
L'utilisation de Repeater signifie connecter le routeur à un autre réseau sans fil existant, par exemple lorsque vous utilisez une connexion Wi-Fi gratuite dans un hôtel ou un café.

Il fonctionne en mode WISP (Wireless Internet Service Provider) par défaut, ce qui signifie que le routeur créera son propre sous-réseau et servira de pare-feu pour vous protéger du réseau public.

Dans la section Répéteur, cliquez sur `Scan` à la recherche des réseaux sans fil disponibles à proximité.



Choisissez un SSID dans la liste déroulante et entrez son mot de passe. Vous pouvez également activer le bouton **Remember** pour sauvegarder le réseau sans fil commandé en cours. Enfin, cliquez sur `Join` .



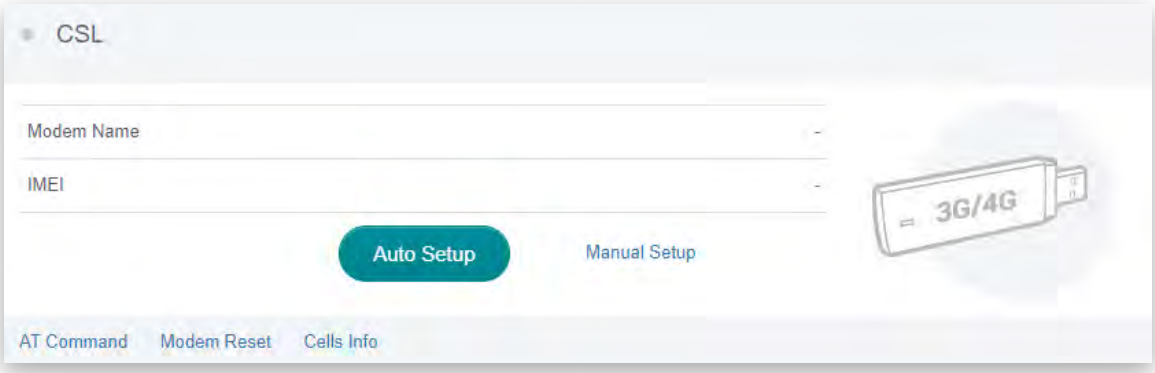
3. Modem USB 3G/4G

Vous pouvez vous connecter à Internet à l'aide d'un modem USB 3G/4G.

Certaines cartes SIM peuvent avoir besoin d'être activées la première fois que vous les utilisez, alors s'il vous plaît, activez-les dans votre téléphone avant de les utiliser dans votre routeur.

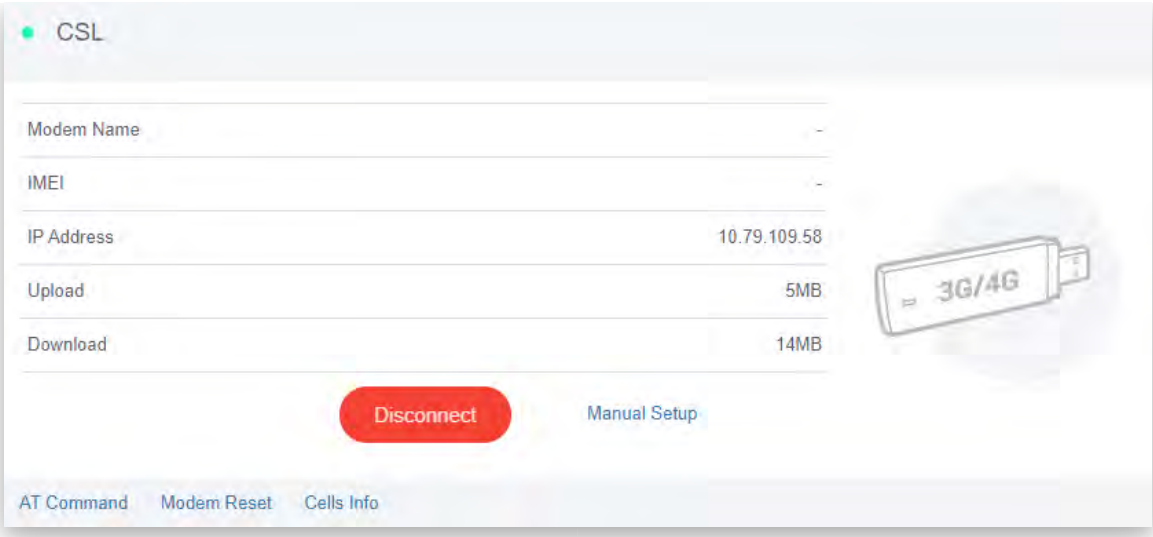
Nous vous recommandons d'éteindre d'abord le routeur, d'insérer votre carte SIM dans le modem USB, puis de brancher le modem USB dans le port USB du routeur, puis de l'allumer.

La première fois, lorsque le routeur est sous tension, il peut ne pas se connecter automatiquement, mais il a lu le nom de votre support dans le coin supérieur gauche, et vous devez cliquer `Auto Setup`.



Après un certain temps, il sera connecté.

Normalement, la deuxième fois, lorsque le routeur est sous tension, après un certain temps, il reconnaît automatiquement la carte SIM et établit une connexion. Il se peut qu'il n'obtienne pas l'information du signal, du nom du modem et de l'IMEI.

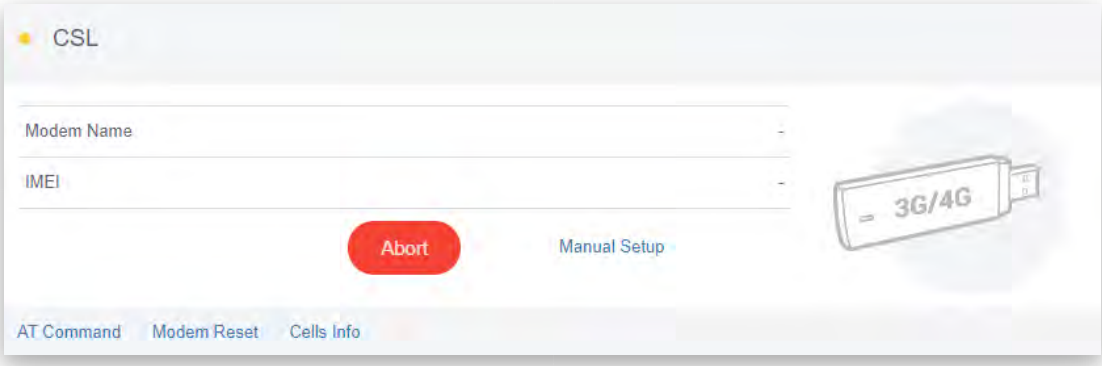


Si vous insérez un modem usb à l'allumer, il ne se connectera pas automatiquement.

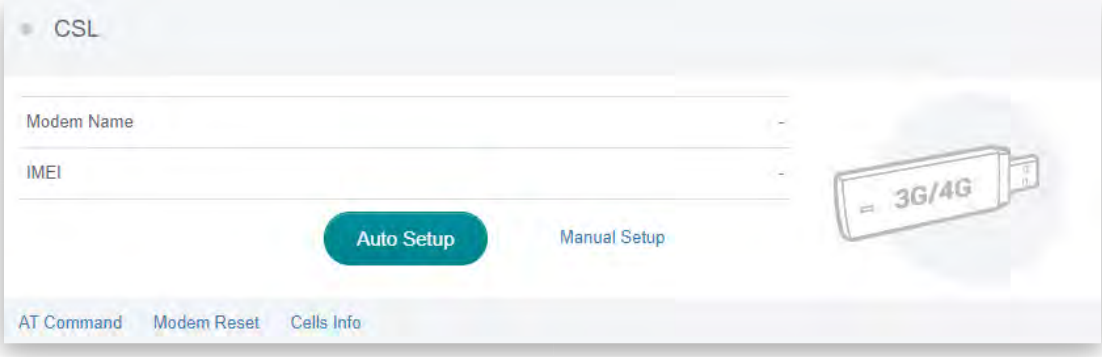
S'il indique le nom du transporteur dans le coin supérieur gauche, vous pouvez cliquer sur `Abort`. Après un certain temps, le bouton se tournera vers `Auto Setup`, puis cliquer sur `Auto Setup`.

S'il ne montre pas le nom du transporteur, vous pouvez cliquer `Modem Reset`.

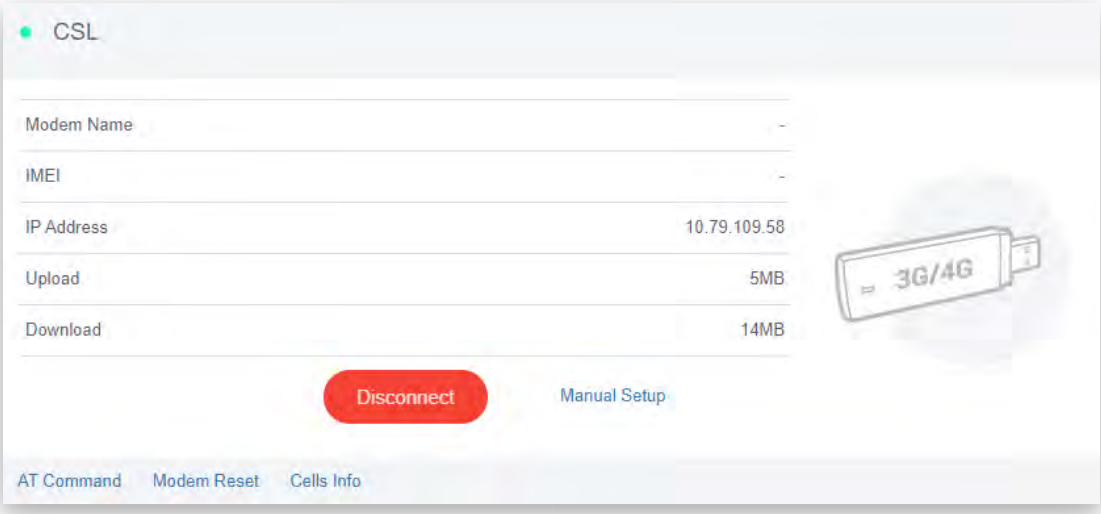
1. Veuillez noter qu'il y a votre nom de transporteur dans le coin supérieur gauche. Cliquez sur `Abort`, attendez un moment, et si ça ne marche pas, cliquez `Modem Reset`.



2. Vous pouvez entrer dans cet écran, puis vous devez cliquer `Auto Setup`, veuillez noter qu'à ce moment, il y a votre nom de transporteur dans le coin supérieur gauche de celui-ci.

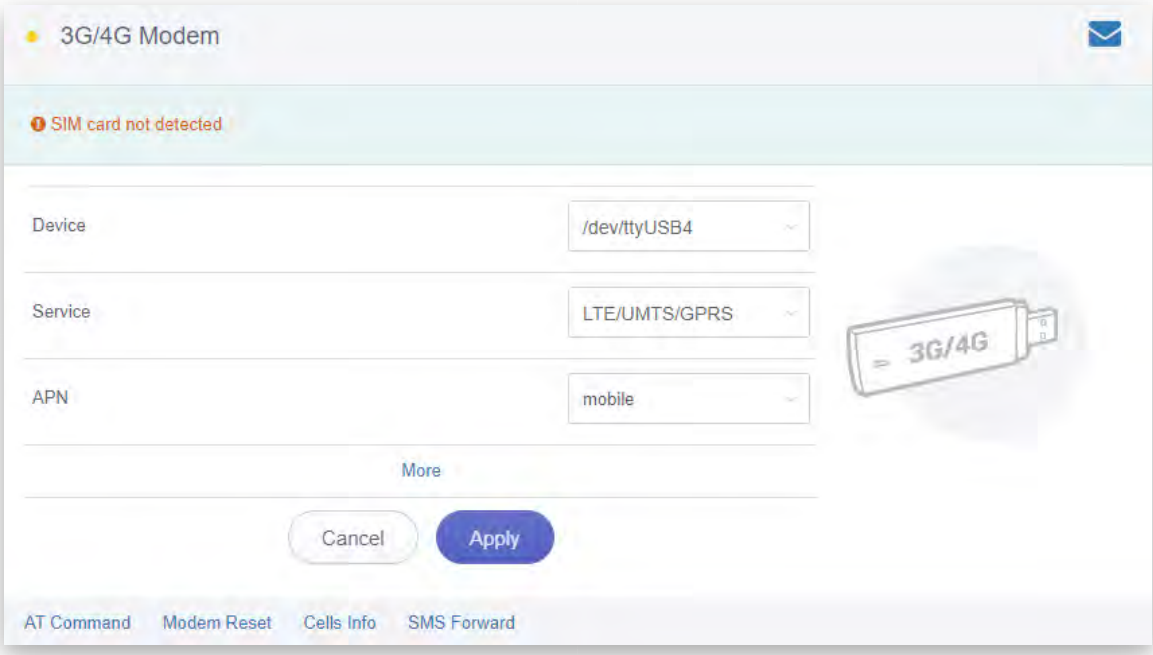


3. Attendez un moment et il sera connecté.



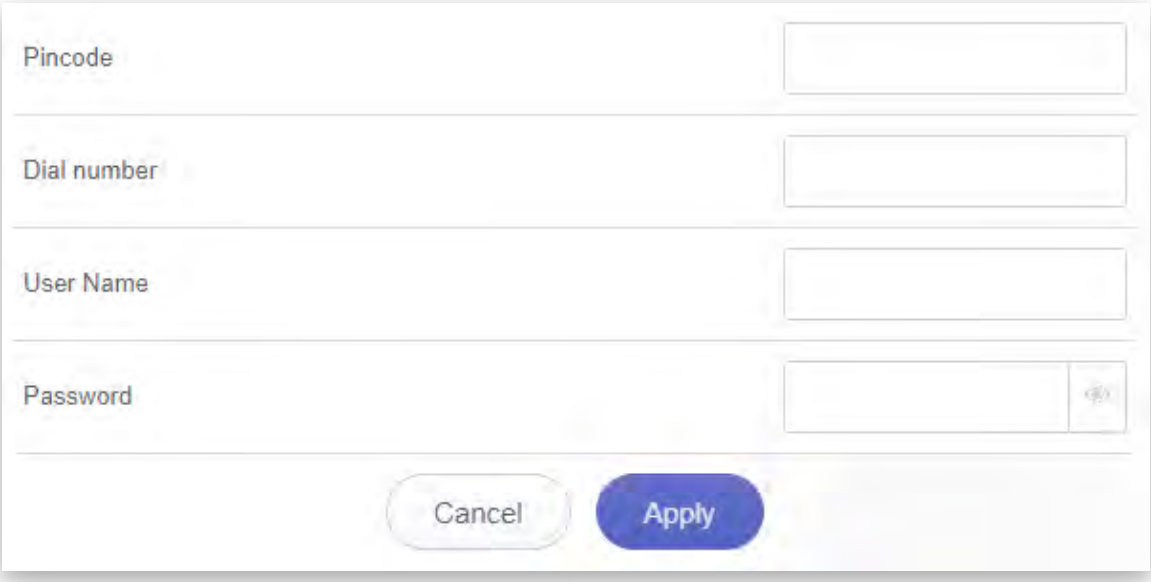
Mise en place manuelle

Parfois, `Auto Setup` ne pas travailler, vous pouvez essayer `Manual Setup` .



- **Dispositif** : Choisissez **/dev/cdc-wdm0** si votre modem supporte la QMI, sinon vous devez choisir **/dev/ttyUSB**, qui peut inclure plusieurs **ttyUSB** de 0 à 3. Vous devez choisir la bonne en fonction de la spécification du modem. Nous vous suggérons d'essayer **ttyUSB0** d'abord.
- **Type de service** : Indiquez le type de service de votre carte SIM.
- **APN** : Confirmez avec votre support de carte SIM.

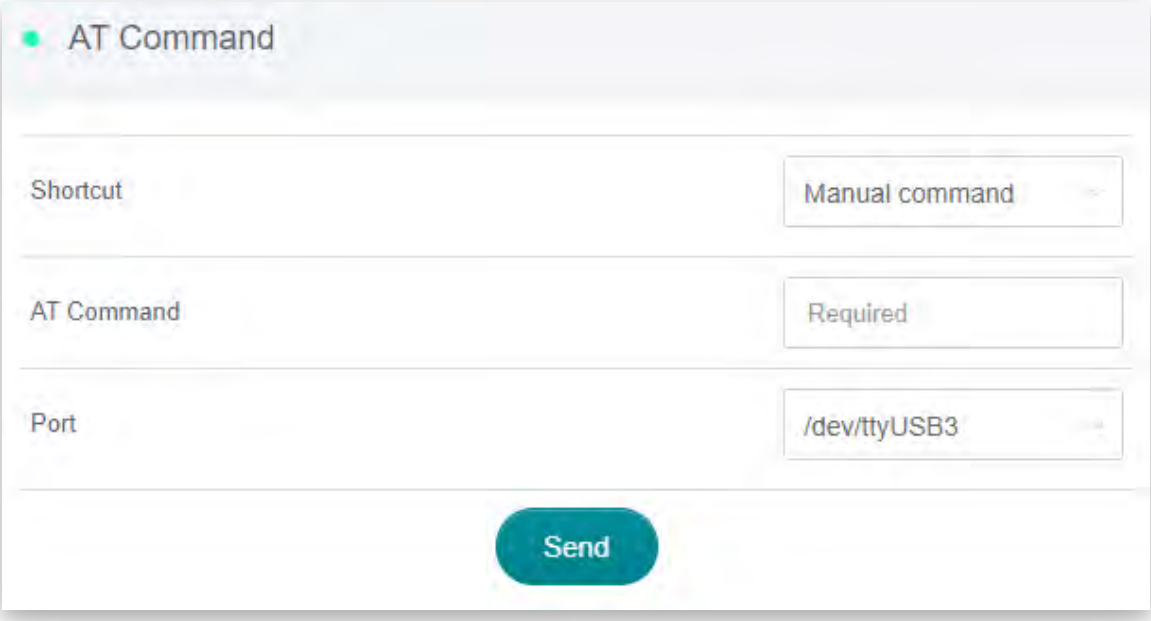
Cliquez sur `More` montrera les paramètres avancés:



- **Numéro de numéro de** numéro: En général, c'est une valeur par défaut et vous n'avez pas besoin de la définir manuellement. Cependant, si vous avez cette information, veuillez la saisir.
- **Pincode, Username et Password** : Généralement, ceux-ci ne sont pas nécessaires pour une carte SIM déverrouillée. Cependant, si vous avez une carte SIM verrouillée, veuillez consulter votre prestataire de services.

Commande AT

Le modem intégré prend en charge la commande AT pour la gestion et la configuration du modem. Dans la section modem 3G/4G, cliquez sur `AT Command` .



- **Shortcut:** There are several pre-configured AT commands that you can use directly. If you want to run your own AT command, choose **Manual command**.
- **AT Command:** The place where you can input AT command. For the list of AT command, please refer to the AT command manual of the built-in modem.
- **Port:** The default port for AT command is **/dev/ttyUSB2**.

Compatible Modems

Here is a list of supported modems that we had tested before.

Model	3G/4G	Tested	Tested by	Comments*
Quectel EC20-E, EC20-A, EC20-C	4G	Yes	GL.iNet	
Quectel EC25-E, EC25-A, EC25-V, EC25-C	4G	Yes	GL.iNet	
Quectel UC20-E	3G	Yes	GL.iNet	
ZTE ME909s-821	4G	Yes	GL.iNet	
Huawei E1550	3G	Yes	GL.iNet	
Huawei E3276	4G	Yes	GL.iNet	
TP-Link MA260	3G	Yes	GL.iNet	
ZTE M823	4G	Yes	Arnas Risqianto	
ZTE MF190	3G	Yes	Arnas Risqianto	
Huawei E3372	4G	Yes	anonymous	
Pantech UML290VW (Verizon)	4G	Yes	GL.iNet/ steven	QMI

Model	3G/4G	Tested	Tested by	Comments*
Pantech UML295 (Verizon)	4G	Yes	GL.iNet/ steven	Host-less
Novatel USB551L (Verizon)	4G	Yes	GL.iNet/ steven	QMI
Verizon U620L (Verizon)	4G	Yes		Host-less

*QMI: This modem supports QMI mode. Please choose /dev/cdc-wdm0 in the Device** list.

*Host-less: This modem supports tethering mode, please set up by using Tethering but not 3G/4G modem.

You can also search on the forum or create a post for asking.

---

4. Tethering

Using a USB cable to share network from your smartphone to the router is called Tethering. Host-less modem works in Tethering during the setup of the modem as well.

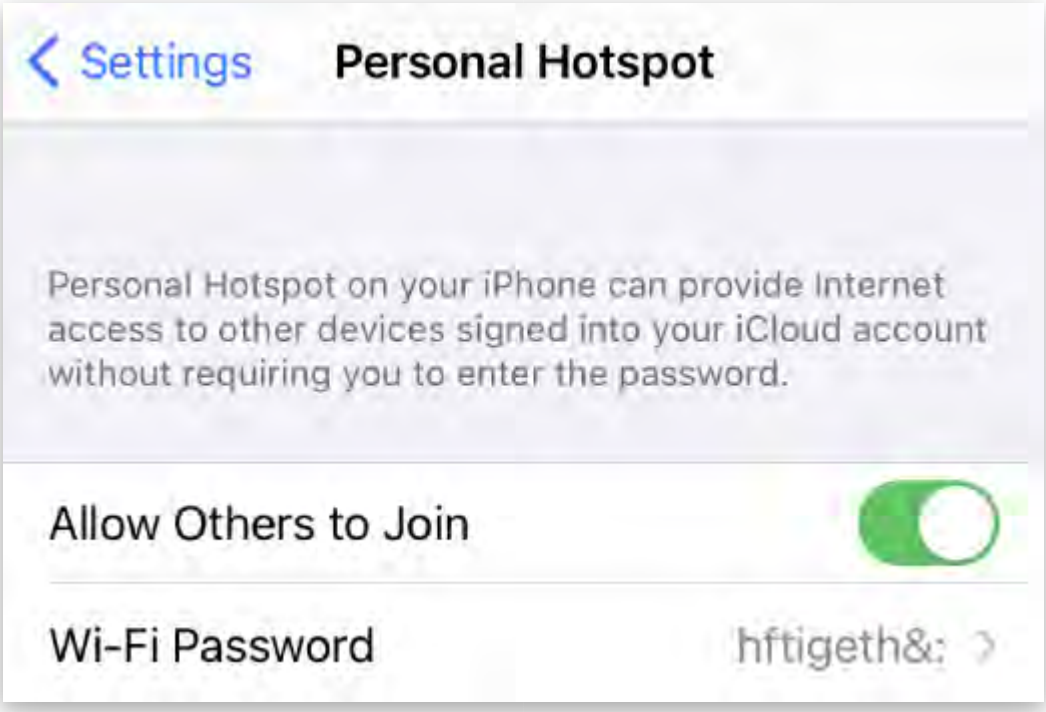
For host-less modem tethering, plug it into the USB port of the router.

For iPhone tethering:

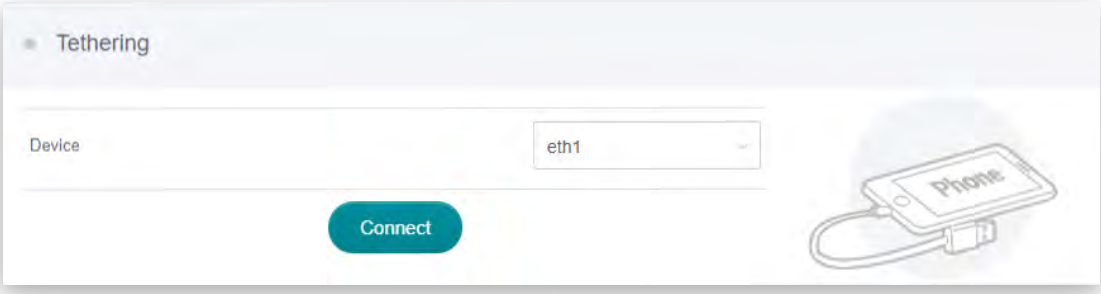
1. Connect iPhone to the USB port of the router. It will pop up a message asking to trust this computer? Click "Trust" to contine. Because we are connecting the iPhone to the router, so here is to TRUST the router.



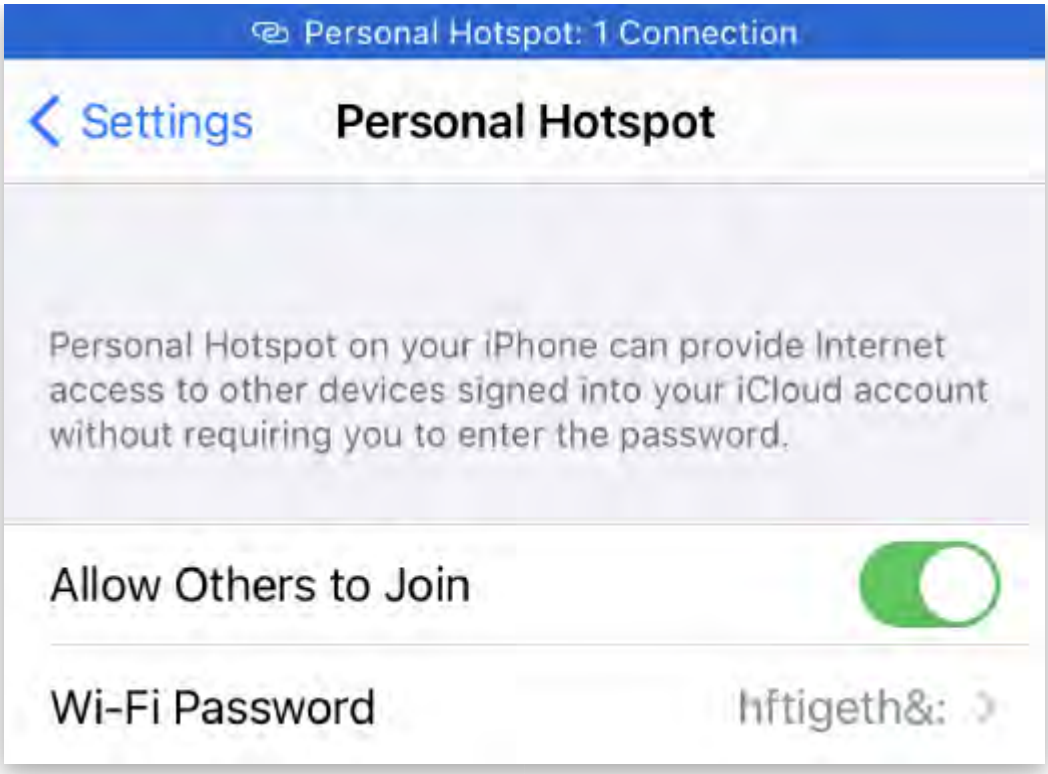
2. Go to iPhone -> Settings -> Personal Hotspot -> Turn on Allow Others to Join.



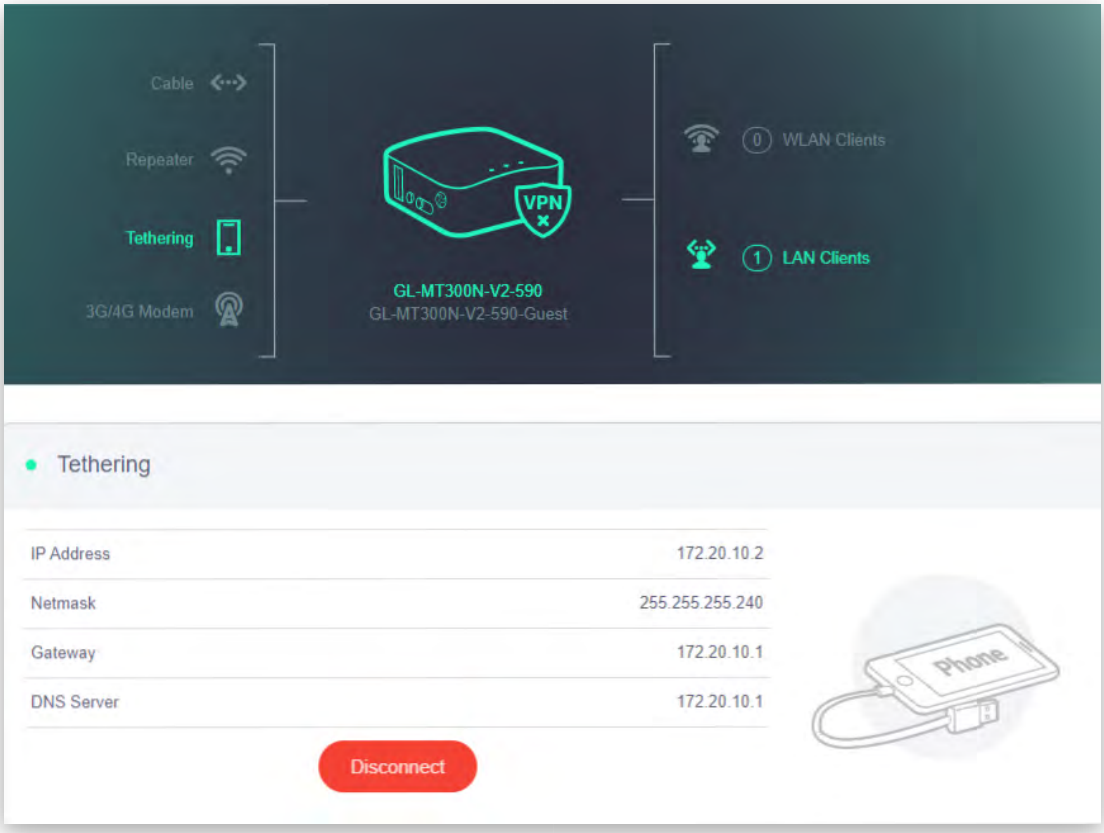
3. Use a computer or another phone, connect to the router, then go to web Admin Panel, on the left side bar, choose "INTERNET" and click "Connect" in the middle of the page.



4. It will show connected information on the top of your phone screen and the web Admin Panel once you connect successfully.



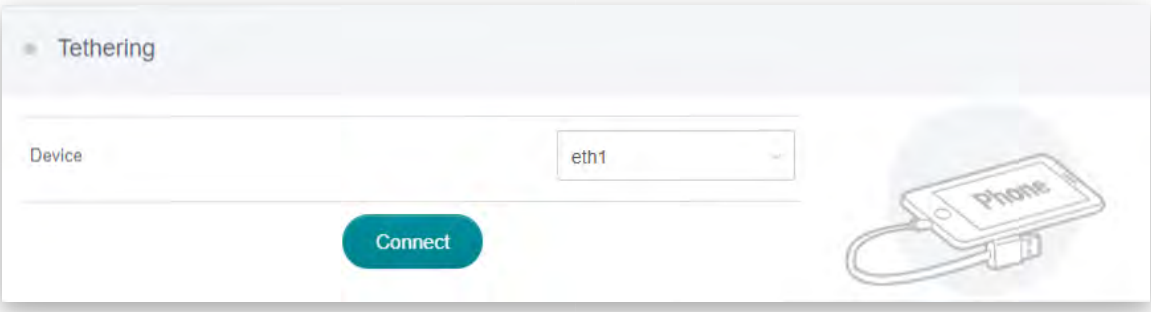
Tethering connected.



If the connection fails, please turn off and turn on `Allow Others to Join` for a few times.

For Android phone tethering, the procedure is similar to iPhone. Connect it to the USB port of the router then check Settings -> Personal hotspot -> Usb network sharing.

After plugging in your device, the Tethering section will update and your device will be shown on the device list. The device name will begin with **eth** or **usb** such as **eth2**, **usb0**. Choose your device and click `Connect`.

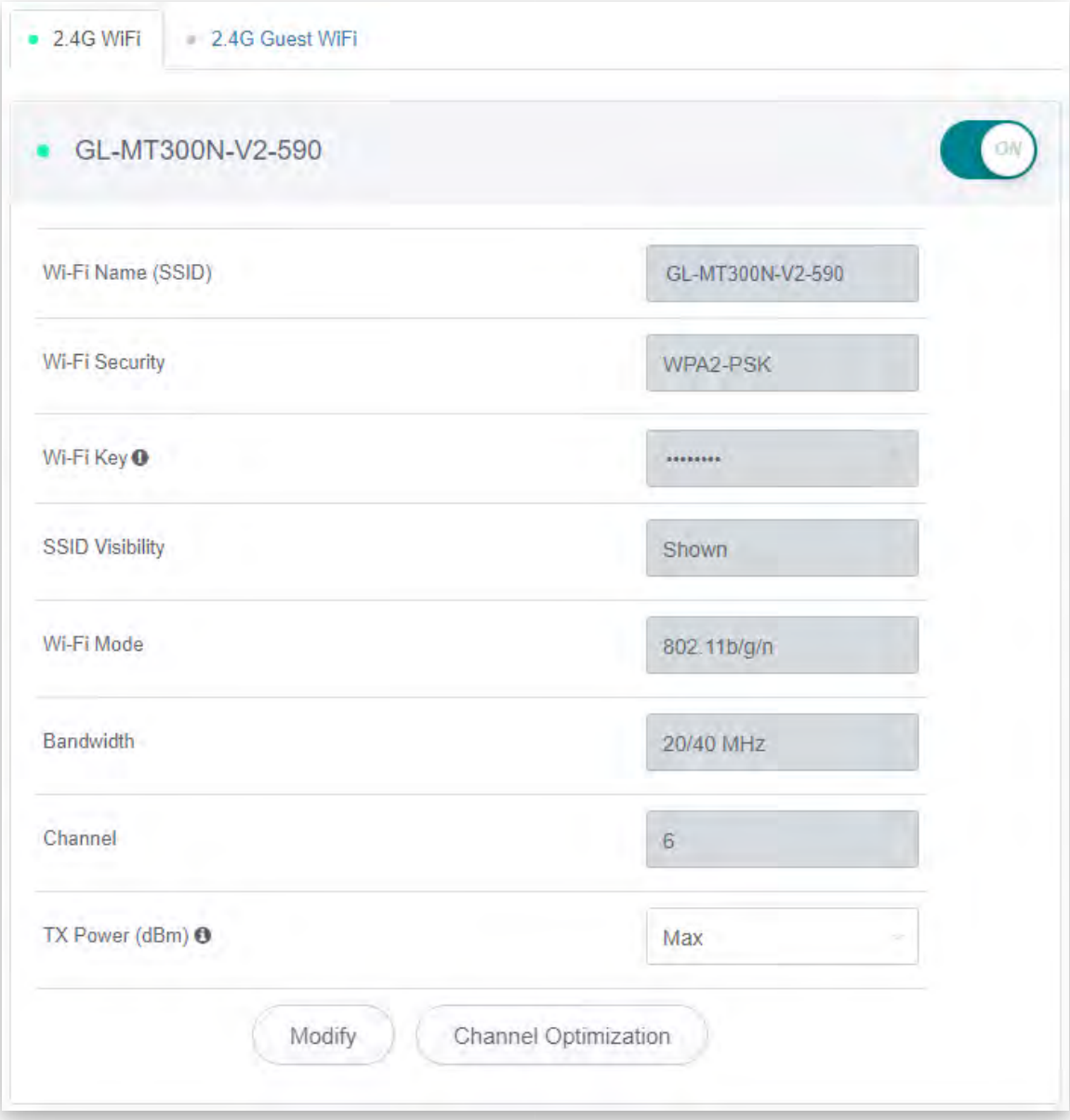


FIL ESTIEME

Sur le côté gauche du panneau d'administration web

Les mini-routeurs n'ont qu'un Wi-Fi de 2,4G.

Sans fil



En `WIRELESS`, vous pouvez vérifier l'état actuel et modifier les paramètres du réseau sans fil créé par le routeur. Le réseau sans fil peut être mis en marche ou bloqué en abattant le réseau

sans fil. `ON/OFF` bouton.

Nom Wi-Fi (SSID): Le nom du Wi-Fi.

Wi-Fi Security : la méthode de cryptage du Wi-Fi.

Clé Wi-Fi : le mot de passe du Wi-Fi, qui doit comporter au moins 6 caractères. Nous vous suggérons de le changer lorsque vous recevrez le routeur.

Visibilité du SSID: Montrer ou cacher le SSID.

Mode Wi-Fi: Choisissez la norme IEEE pour les WLAN.

Largeur de bande : La largeur du canal.

Canal : Le routeur ne choisira pas le meilleur canal lui-même. Vous devez choisir un canal manuellement. Si votre routeur est utilisé comme répéteur Wi-Fi, le canal sera fixé selon le réseau sans fil connecté.

SpeedVitesse: La vitesse sans fil du routeur.

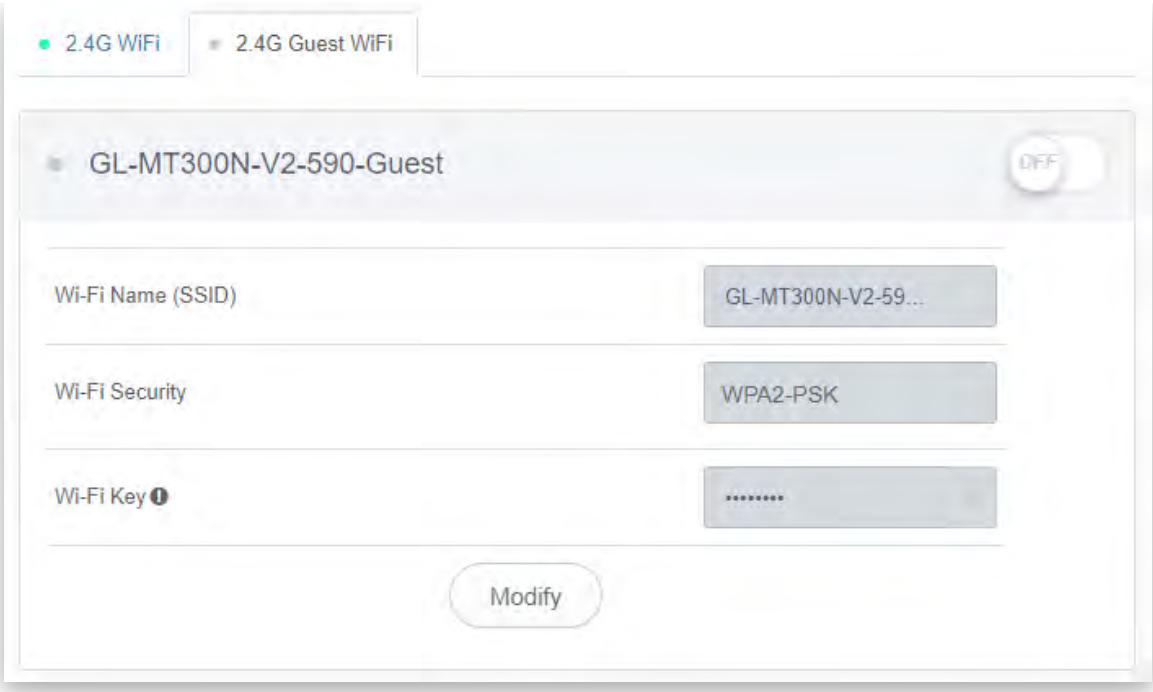
Puissance TX (dBm): Il spécifie l'intensité du signal.

Cliquez sur `Modify` changer les paramètres du réseau sans fil.

Cliquez sur `Channel Optimization` sélectionnera automatiquement le canal le plus approprié en fonction de l'environnement actuel.

Wi-Fi invité

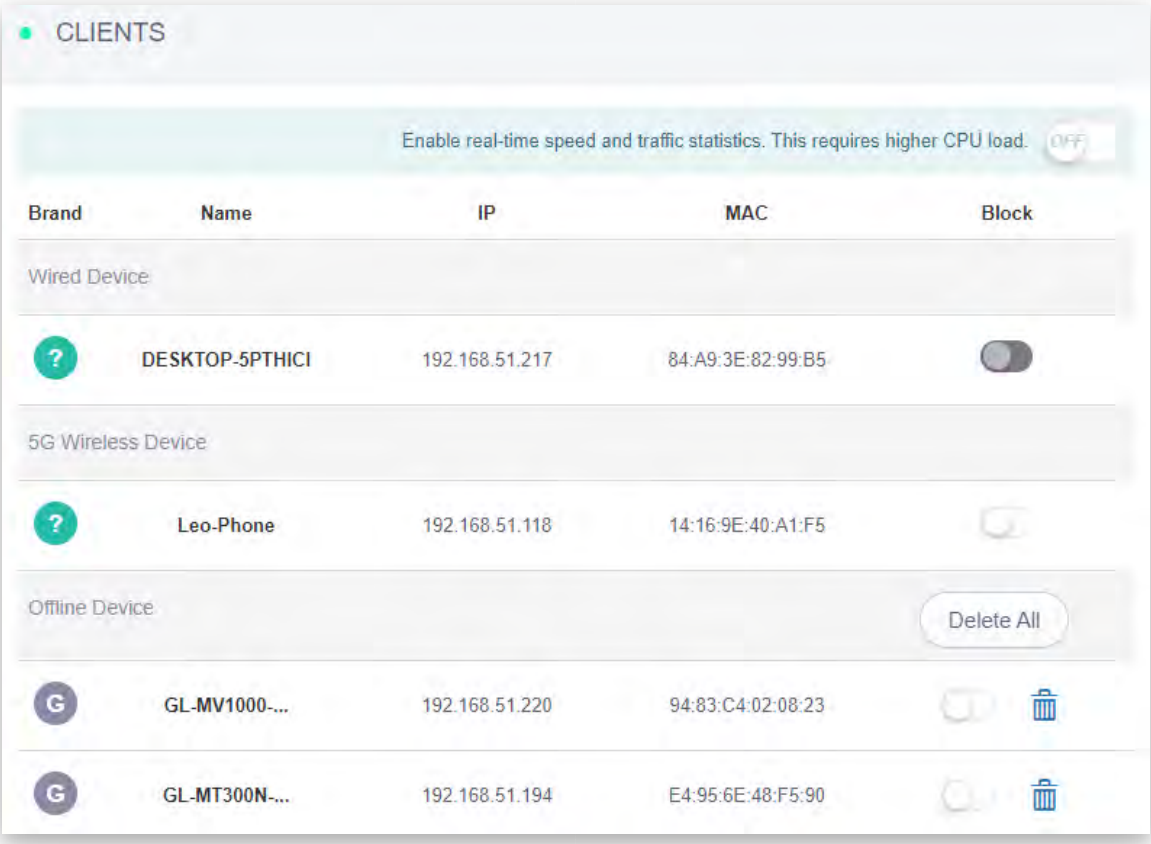
Guest Wi-Fi est éteint par défaut, vous pouvez l'activer pour les visiteurs. Le Wi-Fi invité est séparé du Wi-Fi par défaut. C'est-à-dire que vous ne pouvez accéder à Internet que dans Guest Wi-Fi, pas le web Admin Panel.


2.4G WiFi
2.4G Guest WiFi
GL-MT300N-V2-590-Guest
OFF
Wi-Fi Name (SSID)
GL-MT300N-V2-59...
Wi-Fi Security
WPA2-PSK
Wi-Fi Key
Modify

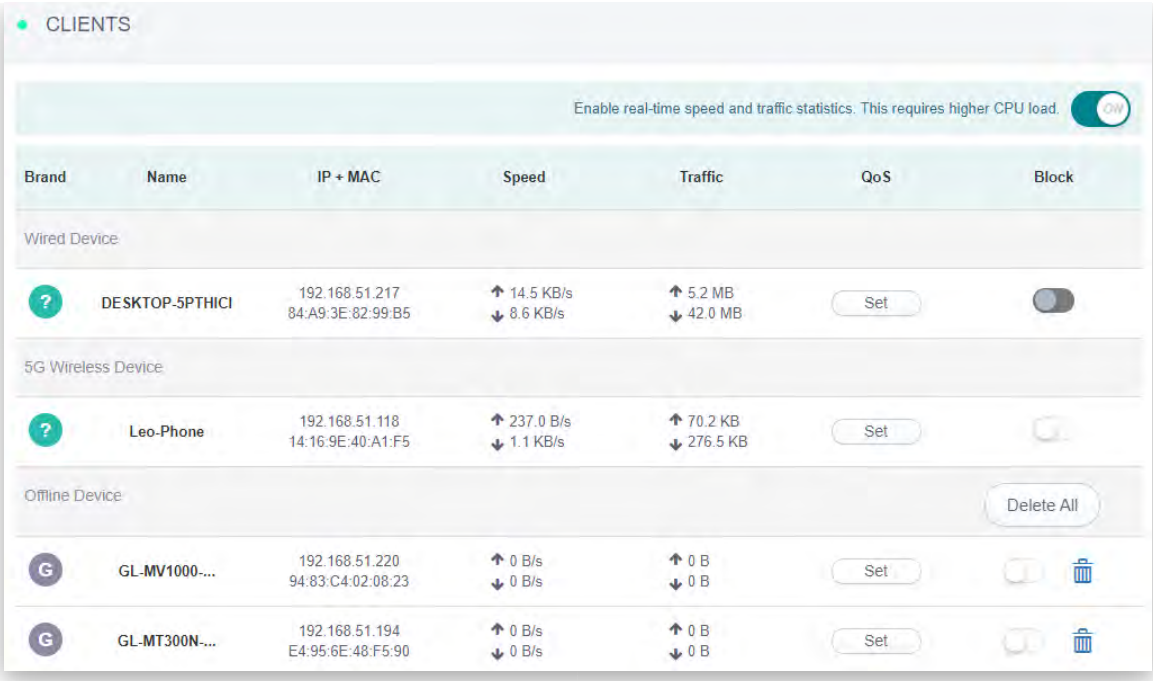
CLIENTS

Sur le côté gauche du panneau d'administration web

Vous pouvez gérer tous les clients connectés dans `CLIENTS` Page. Vous pouvez voir leur nom, leur adresse IP, leur adresse MAC et leur type de connexion. Cliquez sur le bouton de droite pour bloquer n'importe quel client indésirable, vous ne pouvez pas vous bloquer vous-même. Cliquez sur l'icône de la corbeille pour supprimer l'appareil hors ligne.



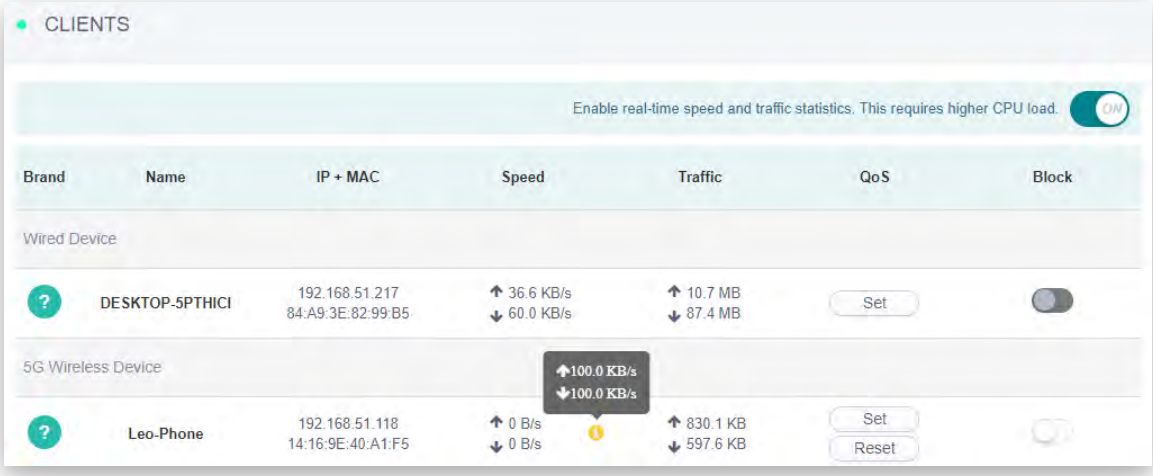
Après que vous vous allumiez `Enable real-time speed and traffic statistics`. Vous pouvez voir toutes les informations sur le trafic et la vitesse de tous les appareils. **Notez que cela nécessite une charge CPU plus élevée**.



Vous pouvez définir la QoS pour certains clients en cliquant sur `Set`, un dialogue va apparaître, entrer la vitesse et cliquer sur **Appliquer**.



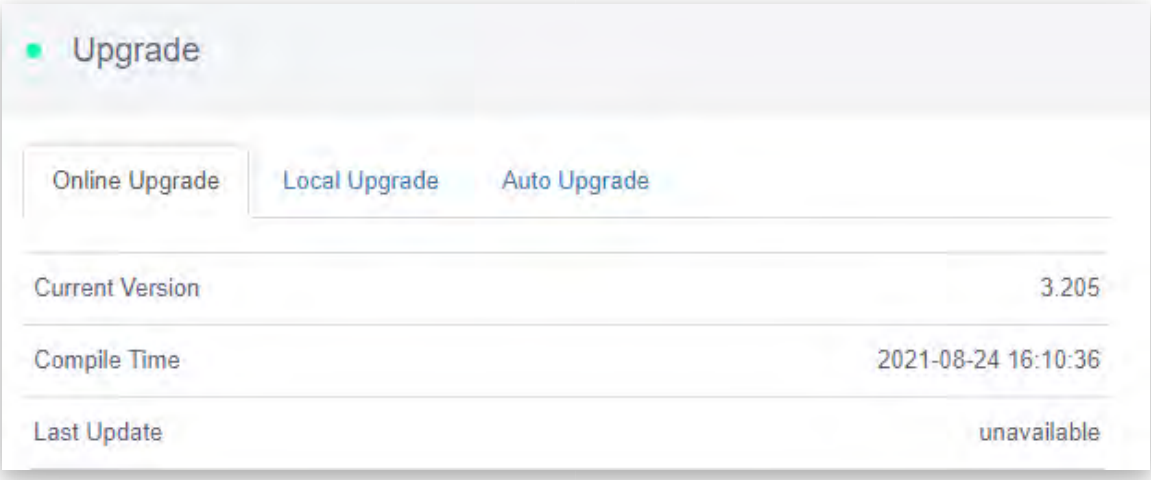
Il y a un "point d'exclamation" jaune en dehors du client limité de vitesse, stationnaire pour vérifier la vitesse limitée. Cliquez sur `Reset` supprimer la restriction.



UPGRADE

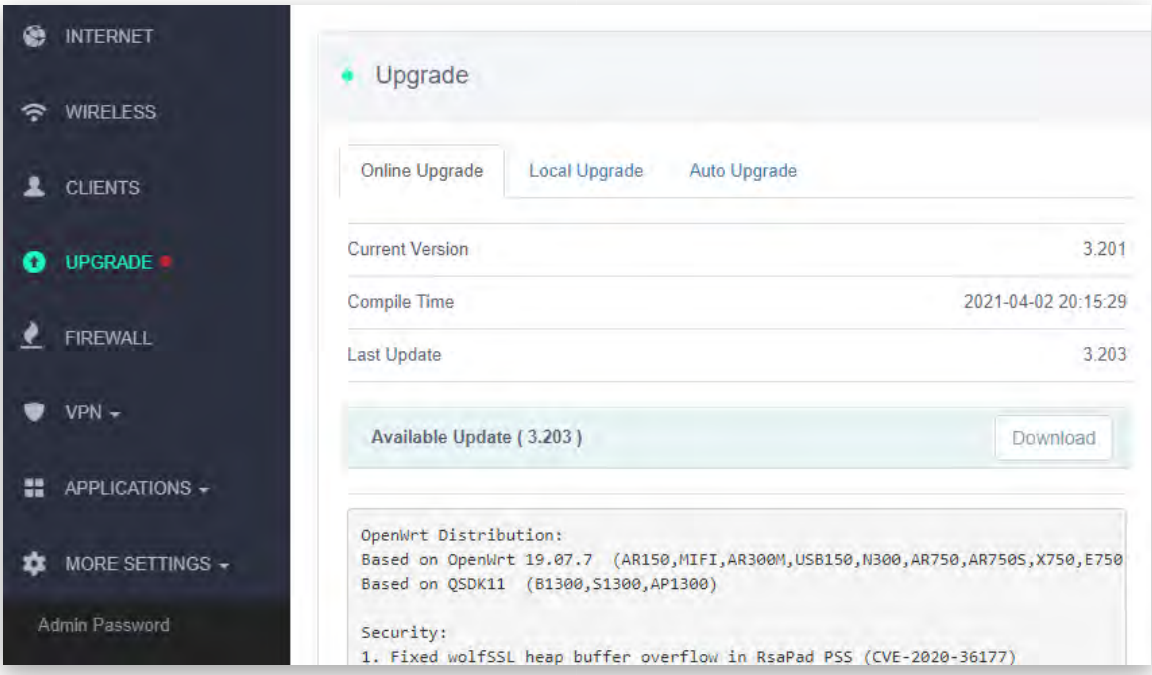
Sur le côté gauche du panneau d'administration web - UPGRADE

Cliquez sur `UPGRADE` pour vérifier toute mise à jour disponible et mise à niveau du micrologiciel.

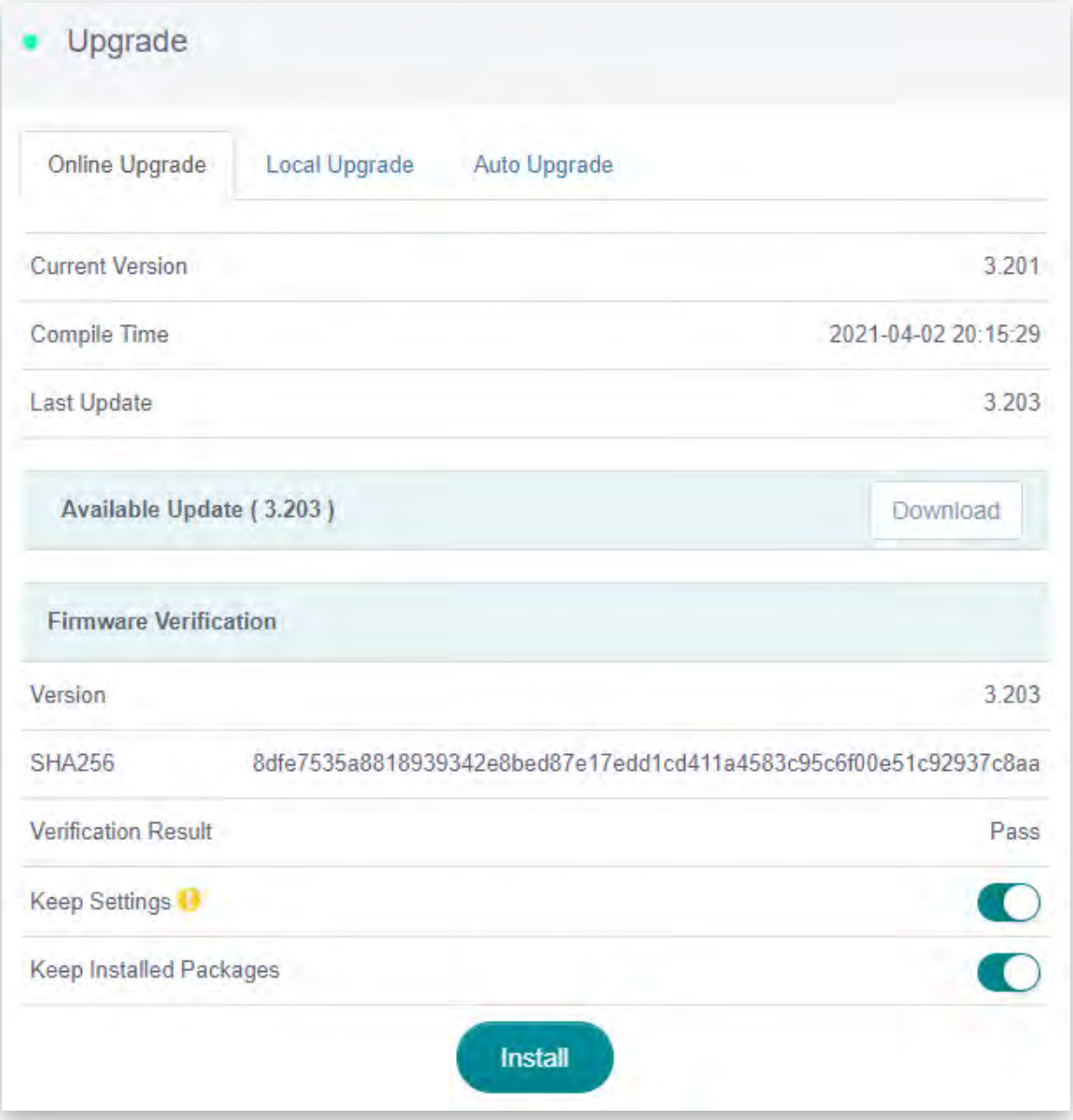


Mise à niveau en ligne

Vous pouvez trouver la version actuelle du micrologiciel ici. Si votre routeur est connecté à Internet, il vérifiera la version plus récente du micrologiciel disponible en téléchargement.



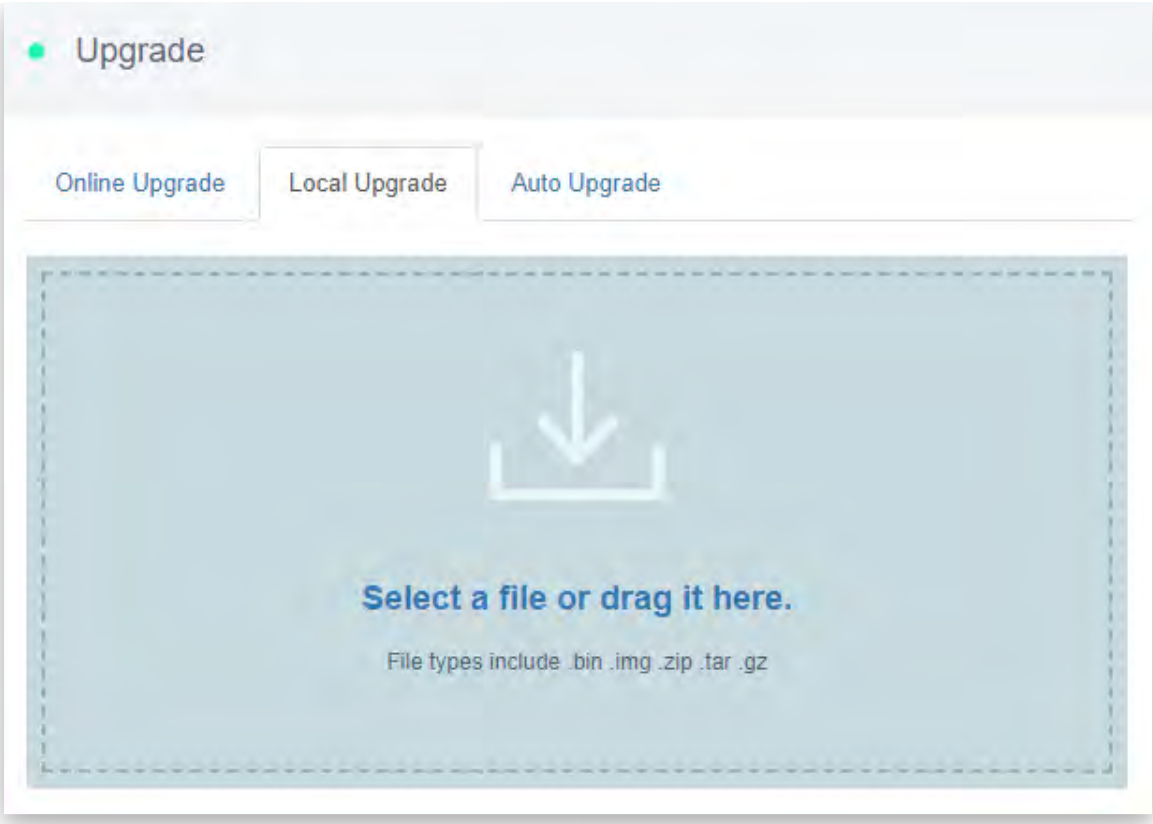
Cliquez sur `Download` un bouton pour télécharger le micrologiciel.



Remarque: si vous gardez les paramètres et rencontrez des problèmes après la mise à niveau, veuillez réinitialiser le routeur.

Amélioration de la situation locale

Cliquez sur `Local Upgrade` pour télécharger un fichier micrologiciel vers le routeur. Faites simplement glisser et déposez votre fichier micrologiciel dans la zone indiquée.

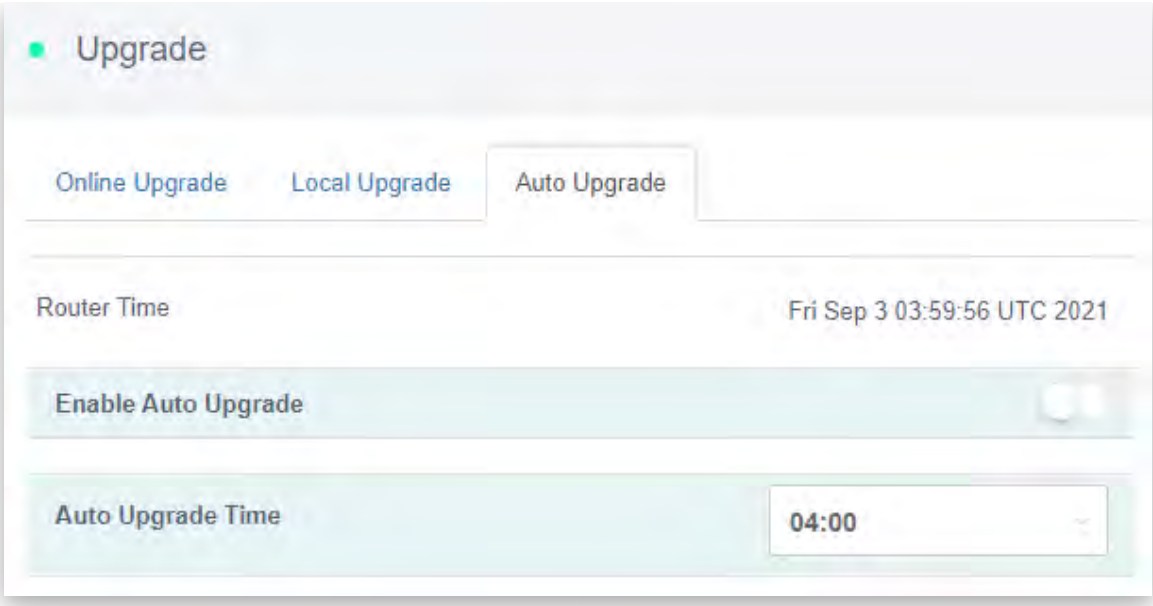


Firmware officiel

Vous pouvez télécharger le micrologiciel à partir de notre site de téléchargement.

Mise à niveau automatique

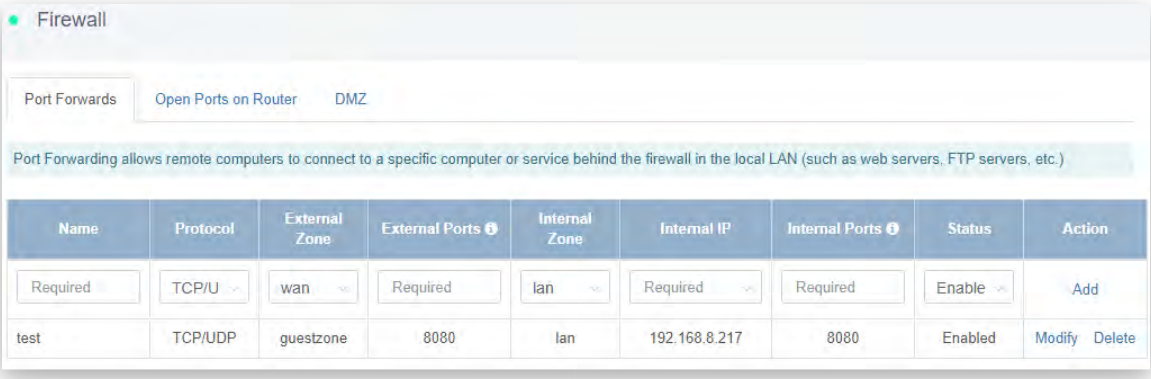
Vous pouvez activer la mise à niveau automatique. Le routeur recherchera la mise à jour et la mise à niveau disponibles automatiquement en fonction de l'heure que vous avez fixée.


Upgrade
Online Upgrade
Local Upgrade
Auto Upgrade
Router Time
Fri Sep 3 03:59:56 UTC 2021
Enable Auto Upgrade
Auto Upgrade Time
04:00

PARE FEU

Sur le côté gauche du panneau d'administration web

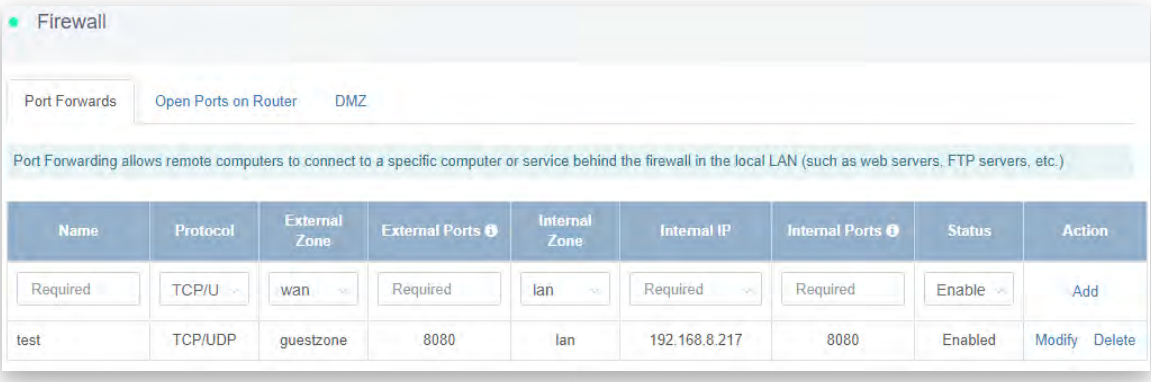
En `FIREWALL`, vous pouvez mettre en place des règles de pare-feu telles que **le transfert de port**, **le port ouvert** et **la zone démilitarisée**.



Versions portuaires

Le transfert de port permet aux ordinateurs distants de se connecter à un ordinateur ou à un service spécifique derrière le pare-feu dans le réseau local (tels que serveurs web, serveurs FTP, etc.).

Pour configurer le transfert de port, cliquez sur `Port Forwards` et entrer les paramètres requis ou cliquer `Add a New One`.



Nom : Nom de la règle.

Protocole: Le protocole utilisé, vous pouvez choisir TCP, UDP, ou à la fois TCP et UDP.

IP interne: L'adresse IP attribuée par le routeur au dispositif à laquelle il faut accéder à distance.

zone externe: les options pour les zones extérieures sont les suivantes: `wan` , `guestZone` , `wireguard` .

- `wan` est sélectionné lorsque vous souhaitez autoriser un service dans la zone WAN. Par exemple, un serveur web fonctionne sur un appareil LAN dans votre maison, il ne peut accéder que lorsque vous êtes à la maison, mais vous voulez qu'il soit accessible en dehors de votre maison, puis vous pouvez définir la zone externe comme `wan` . Vous pouvez y accéder via `wan_ip` : `external_port` . Remarque: L'accès à l'extérieur de votre domicile a besoin d'une propriété intellectuelle publique.
- `guestZone` est d'autoriser l'accès à votre service par des appareils connectés au Wi-Fi invité. Par exemple, lorsqu'un serveur web fonctionne sur un appareil LAN à votre domicile, il ne peut être consulté que par vos appareils dans le réseau local, mais pas par défaut le réseau local invité (qui est isolé du réseau local par défaut). Si vous voulez que le serveur web soit accessible dans le réseau local invité, vous devez définir la zone externe à `guestZone` . Vous pouvez accéder au service activé via `wan_ip` : `external_port` .
- `wireguard` , lorsque le routeur utilise le serveur WireGuard, il y aura le `wireguard` option. Par exemple, un serveur web fonctionne sur un appareil LAN à votre domicile. Lorsque vous vous connectez au serveur WireGuard de votre routeur, votre accès au serveur web sur l'intranet n'est pas autorisé. Pour le rendre accessible, définir la zone externe comme `wireguard` . Ensuite, il est possible d'accéder via `wan_ip` : `external_port` .

Ports extérieurs: Nombre de ports extérieurs. Vous pouvez entrer un numéro de port spécifique ici.

Ports intérieurs: le numéro de port intérieur du dispositif. Vous pouvez entrer un numéro de port spécifique. Laisser le vide s'il est identique au port extérieur.

État d'avancement : Activation de la règle.

Ports ouverts sur routeur

Les services du routeur, tels que le Web, FTP, etc., exigent que leurs ports respectifs soient ouverts sur le routeur pour être accessibles au public.

Pour ouvrir un port, cliquez sur `Open Ports on Router` et entrer les paramètres requis ou cliquer `Add a New One` .



Nom: Nom de la règle qui peut être spécifiée par l'utilisateur.

Port : le numéro de port que vous voulez ouvrir.

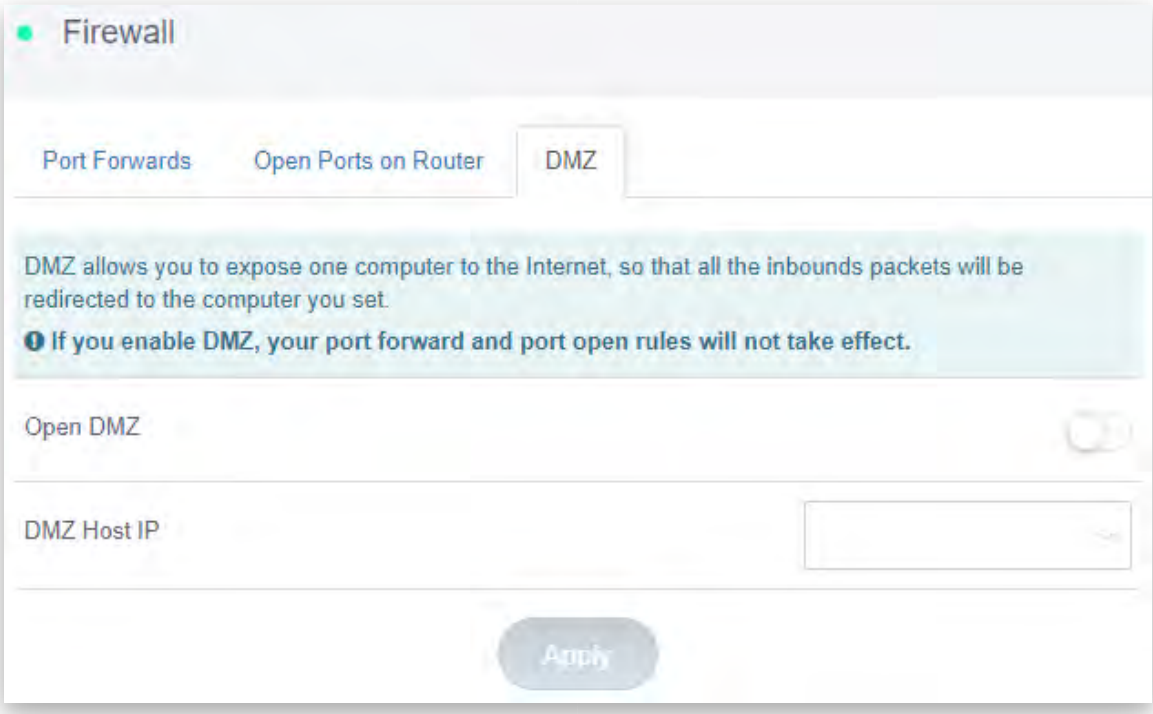
Protocole: Le protocole utilisé, vous pouvez choisir TCP, UDP, ou à la fois TCP et UDP.

État d'avancement : Activation de la règle.

DMz

La zone DM vous permet d'exposer un ordinateur sur Internet, de sorte que tous les paquets entrants seront redirigés vers l'ordinateur que vous réglez.

Cliquez sur `DMZ` et permettre `Open DMZ`. Inscrire l'adresse IP interne (ex. 192.168.8.100) de votre appareil qui va recevoir tous les paquets entrants.



VPN

Les routeurs GL.iNet ont pré-installé serveur et client VPN dans OpenVPN et WireGuard.

OpenVPN

Veuillez vous reporter aux liens ci-dessous pour l'instruction détaillée d'installation:

- **Configuration Client OpenVPN**
- **Configuration Serveur OpenVPN**

WireGuard

Veuillez vous reporter aux liens ci-dessous pour l'instruction détaillée d'installation:

- **Client WireGuard de configuration**
- **Serveur WireGuard de configuration**

Kill Switch sur Internet

Veuillez vous reporter au lien ci-dessous pour l'instruction détaillée de configuration:

- **Kill Switch sur Internet**

Politiques VPN

Veuillez vous reporter au lien ci-dessous pour l'instruction détaillée de configuration:

- **Politiques VPN**

Comment configurer OpenVPN Client sur GL.iNet routeur

OpenVPN est un protocole VPN open source qui utilise des techniques de réseau privé virtuel (VPN) pour établir des connexions sécurisées de site à site ou de point à point.

Les routeurs GL.iNet ont pré-installé OpenVPN Client and Server.

Nous recommandons WireGuard sur OpenVPN parce qu'il est beaucoup plus rapide. Pour la configuration d'un client WireGuard, veuillez consulter ici.

Si vous avez déjà acheté le service OpenVPN auprès d'un fournisseur, mais que vous ne savez pas comment obtenir le fichier de configuration, veuillez vous référer pour obtenir des fichiers de configuration auprès de fournisseurs de services OpenVPN ou demander son support.

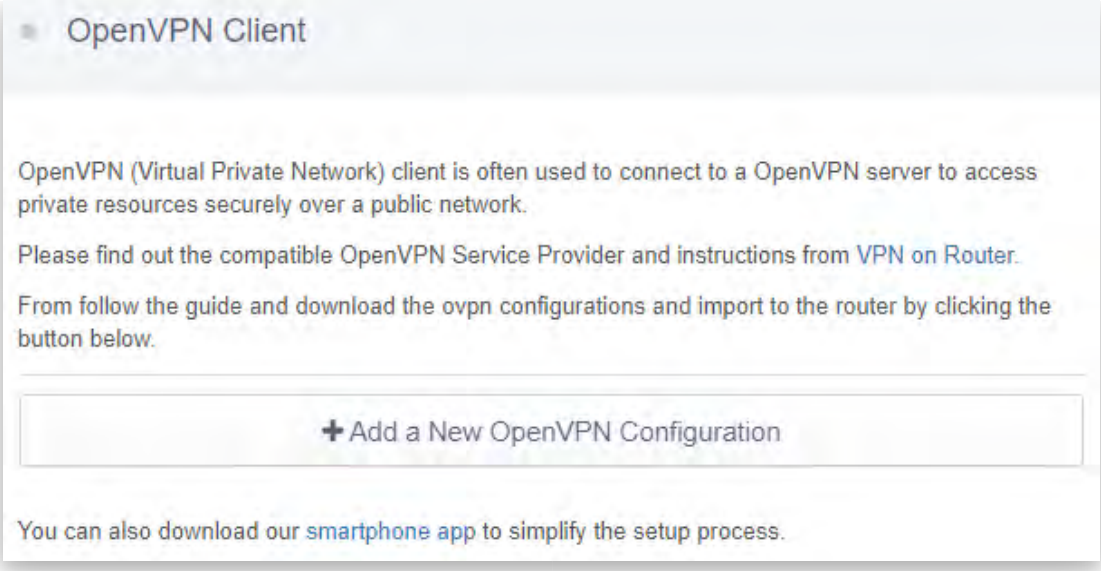
Nous pouvons configurer OpenVPN Client via le panneau d'administration web et l'application mobile. Pour l'application mobile, elle a déjà intégré NordVPN.

Configuration Client OpenVPN

Il y a un tutoriel vidéo comme ExpressVPN comme exemple, regardez ici.

Le client OpenVPN nécessite le fichier de configuration OpenVPN (.ovpn) pour créer la connexion OpenVPN.

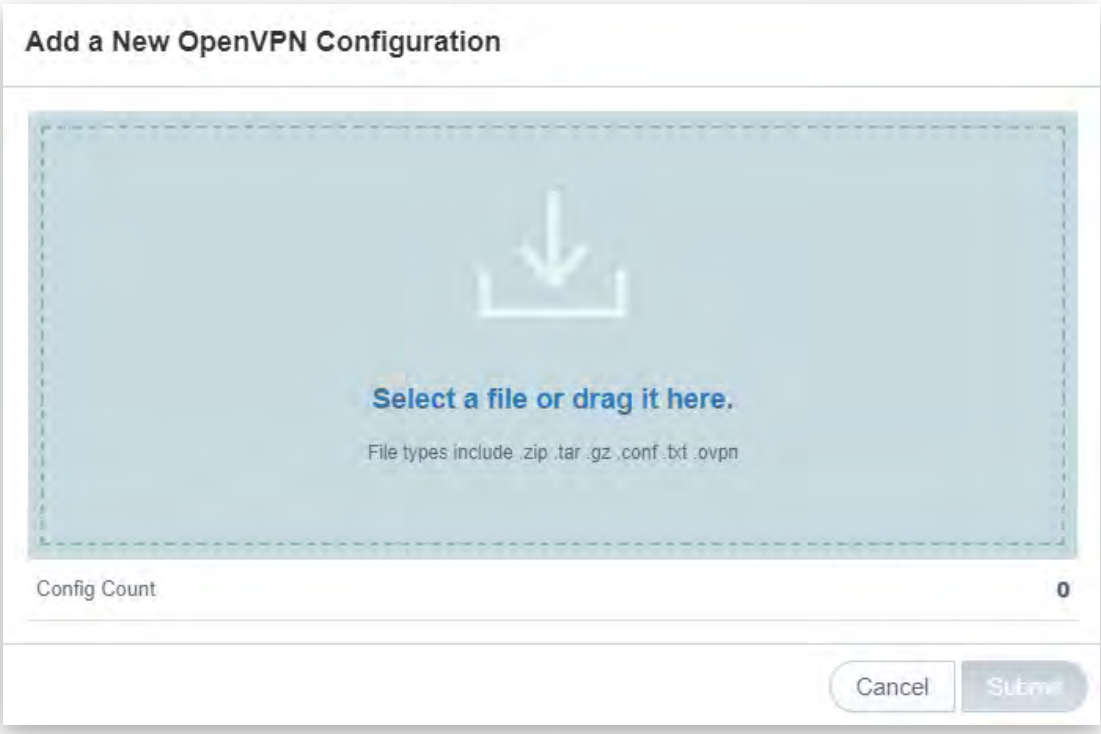
1. Accès au panneau d'administration web, sur le côté gauche, VPN -
2. Cliquez sur **Ajouter une nouvelle configuration OpenVPN**.



3. Téléchargez votre fichier de configuration OpenVPN

   Faites glisser et déposez votre fichier jusqu'aux fenêtres pop-up. Il peut s'agir d'un seul fichier .ovpn ou d'un fichier zip/tar.gz qui contient plusieurs fichiers .ovpn.

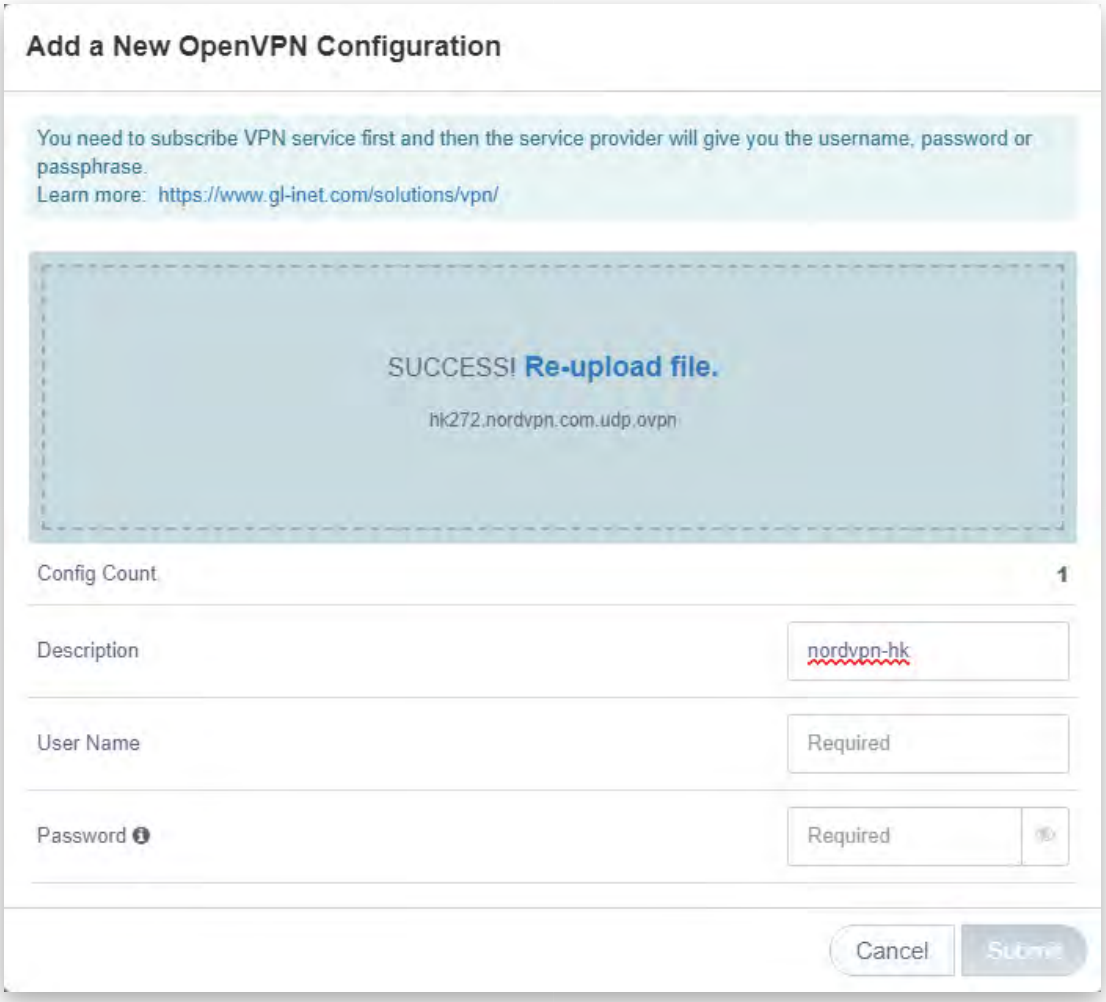
   Faites attention à ce que certains fichiers .ovpn utilisent des fichiers séparés ca, cert, crl. Ces fichiers doivent être zippés avec le fichier .ovpn avant le téléchargement.



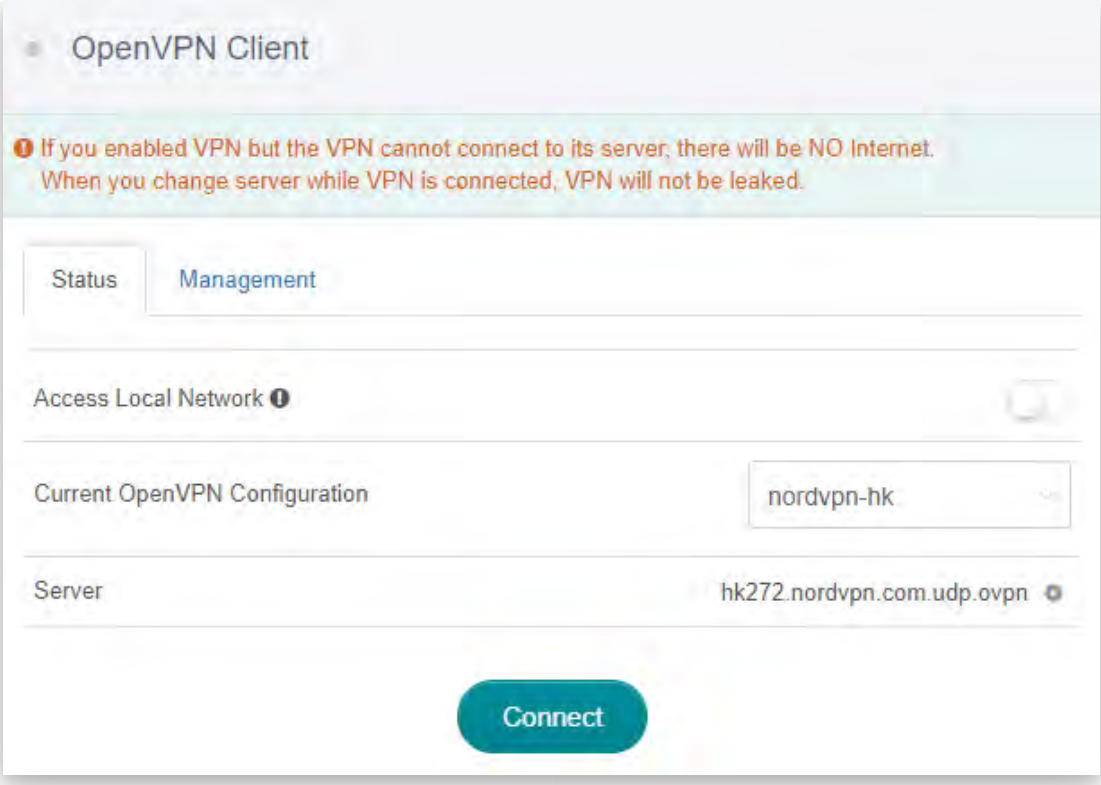
   Vous pouvez encouverr certains problèmes, comme pas assez d'espace, fichier invalide, autorisation en échec, tous les autres services VPN doivent d'abord être arrêtés, veuillez vérifier ici.

4. Saisissez une description de votre fichier de configuration OpenVPN, puis cliquez sur **Soumettre** pour terminer le processus de téléchargement. Dans certains cas, il vous demandera d'entrer le nom d'utilisateur et le mot de passe. Si vous ne connaissez pas le

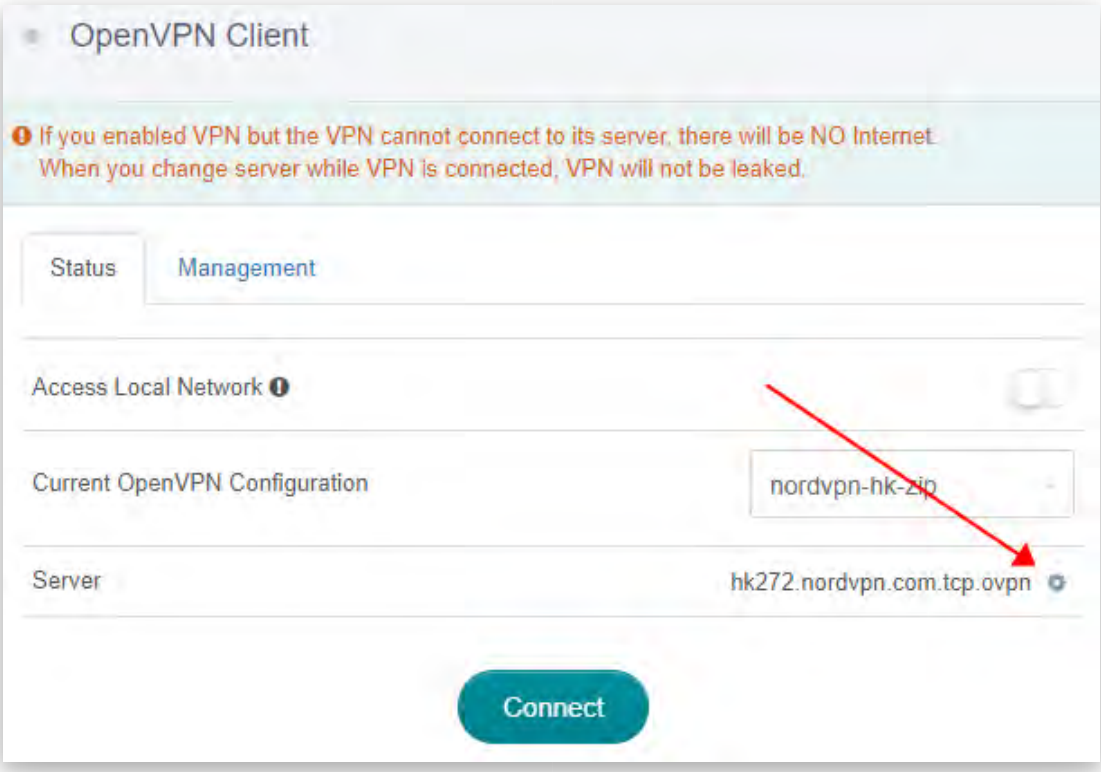
nom d'utilisateur et le mot de passe, veuillez contacter le fournisseur de services OpenVPN.



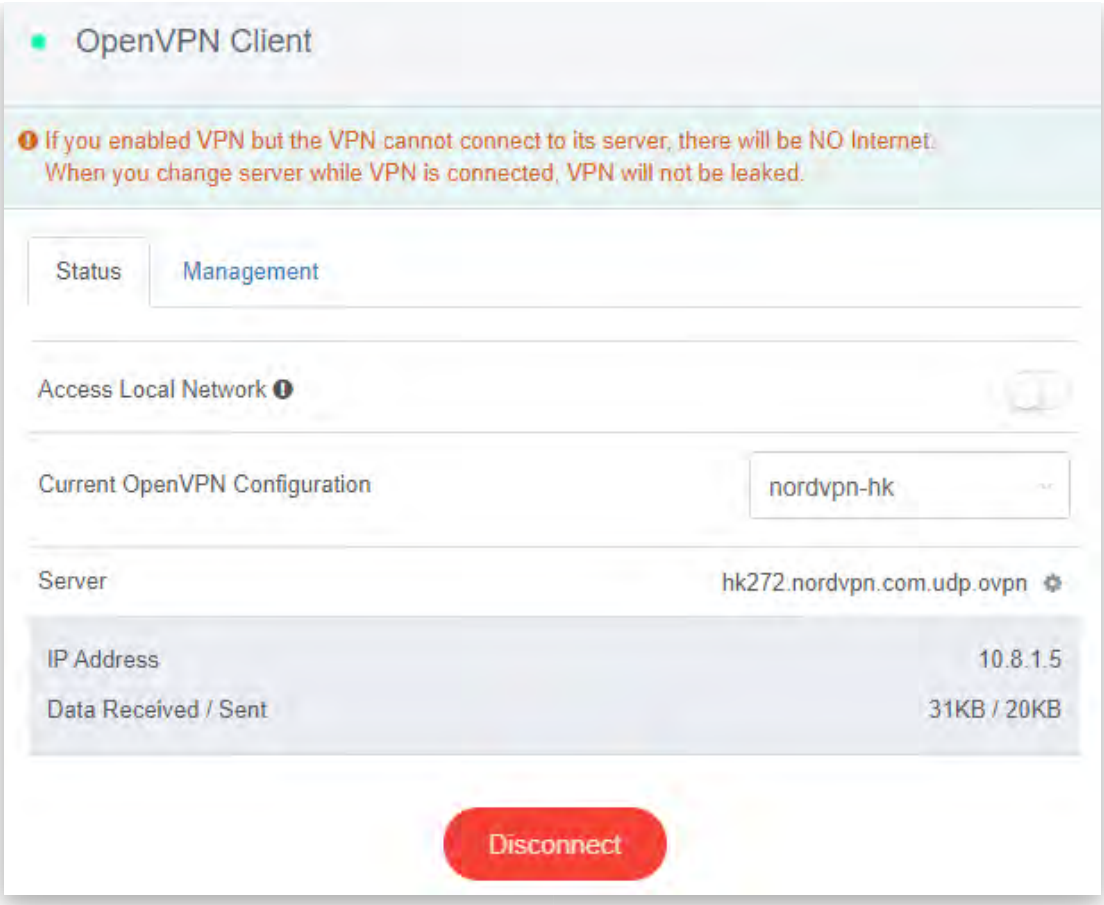
5. Vous pouvez maintenant cliquer sur **Connect** pour démarrer la connexion OpenVPN.



Si votre fichier de configuration est un fichier d'archive, comme .zip, vous pouvez changer de serveur à l'icône du crème.



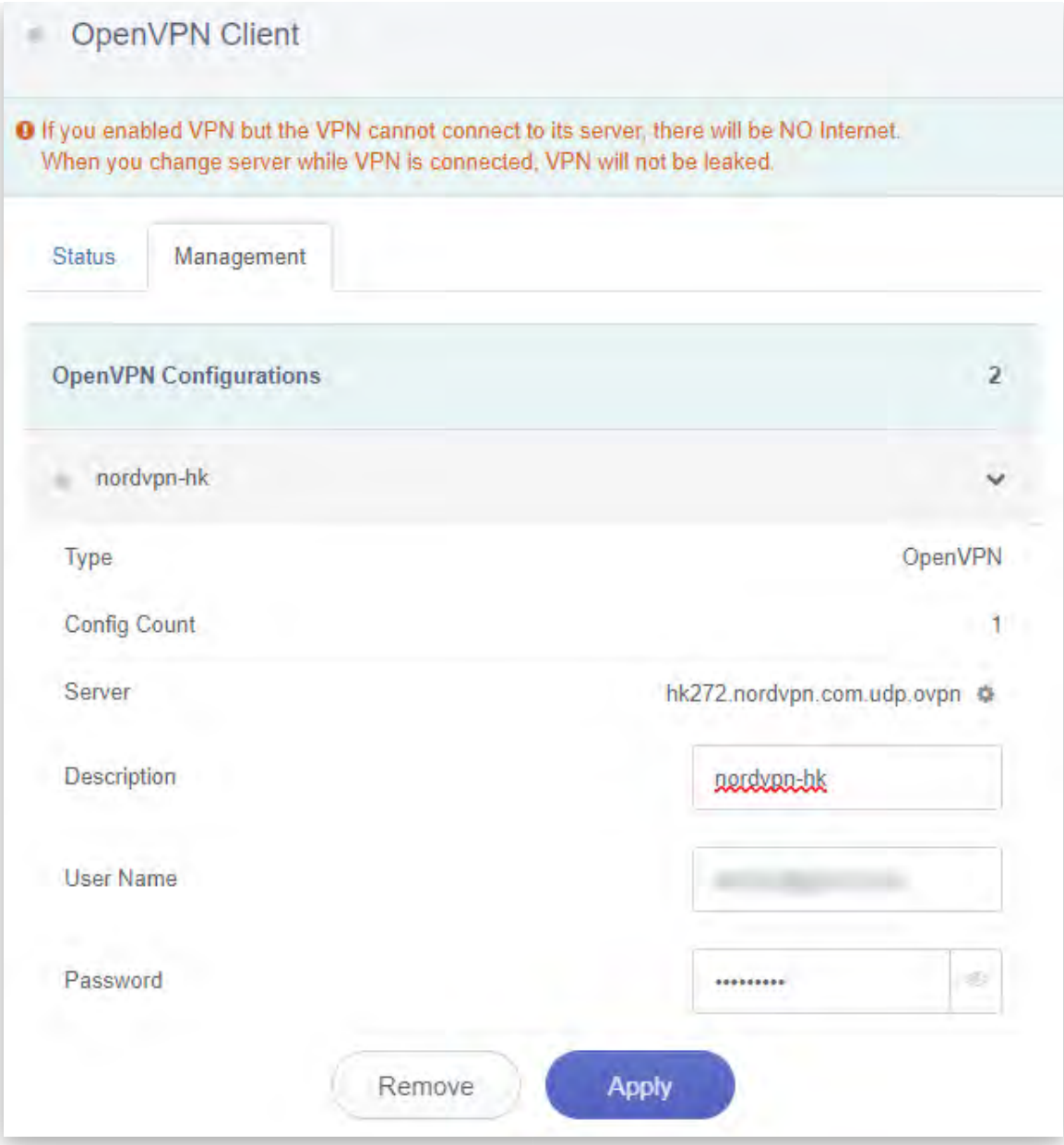
6. Une fois connecté, vous devriez trouver votre adresse IP, les données reçues/envoyées.



Remarque: il ne peut pas exécuter VPN Client and Server en même temps, et il ne peut pas non plus exécuter OpenVPN Client et WireGuard Client en même temps.

Gérer les fichiers de configuration

Cliquez sur **Gestion** pour vérifier la liste des fichiers de configuration. Vous pouvez modifier la **Description**, le **Nom de l'Utilisateur** et **le Mot** de **Pass** de chaque fichier de configuration. Vous pouvez également ajouter, supprimer un fichier de configuration ou même purger tous vos fichiers de configuration téléchargés.



Configuration du serveur OpenVPN sur le routeur GL.iNet

Vous pouvez obtenir un routeur GL.iNet pour paramétrer en serveur OpenVPN, et obtenir un autre routeur GL.iNet pour être défini en tant que client OpenVPN. Pour la configuration du serveur OpenVPN, veuillez consulter ici.

Obtenir des fichiers de configuration à partir des fournisseurs de services OpenVPN

Nous avons testé différents fournisseurs de services VPN. Par conséquent, si vous ne savez pas comment obtenir le fichier de configuration, vous pouvez suivre les instructions ci-

dessous. Cependant, vous devez contacter votre fournisseur de services pour le fichier de configuration s'il ne figure pas sous la liste ci-dessous.

Si vous avez des problèmes dans la configuration d'OpenVPN, veuillez contacter l'adresse suivante: support.glinet.biz ou rapport dans ce billet du forum.

NordVPN

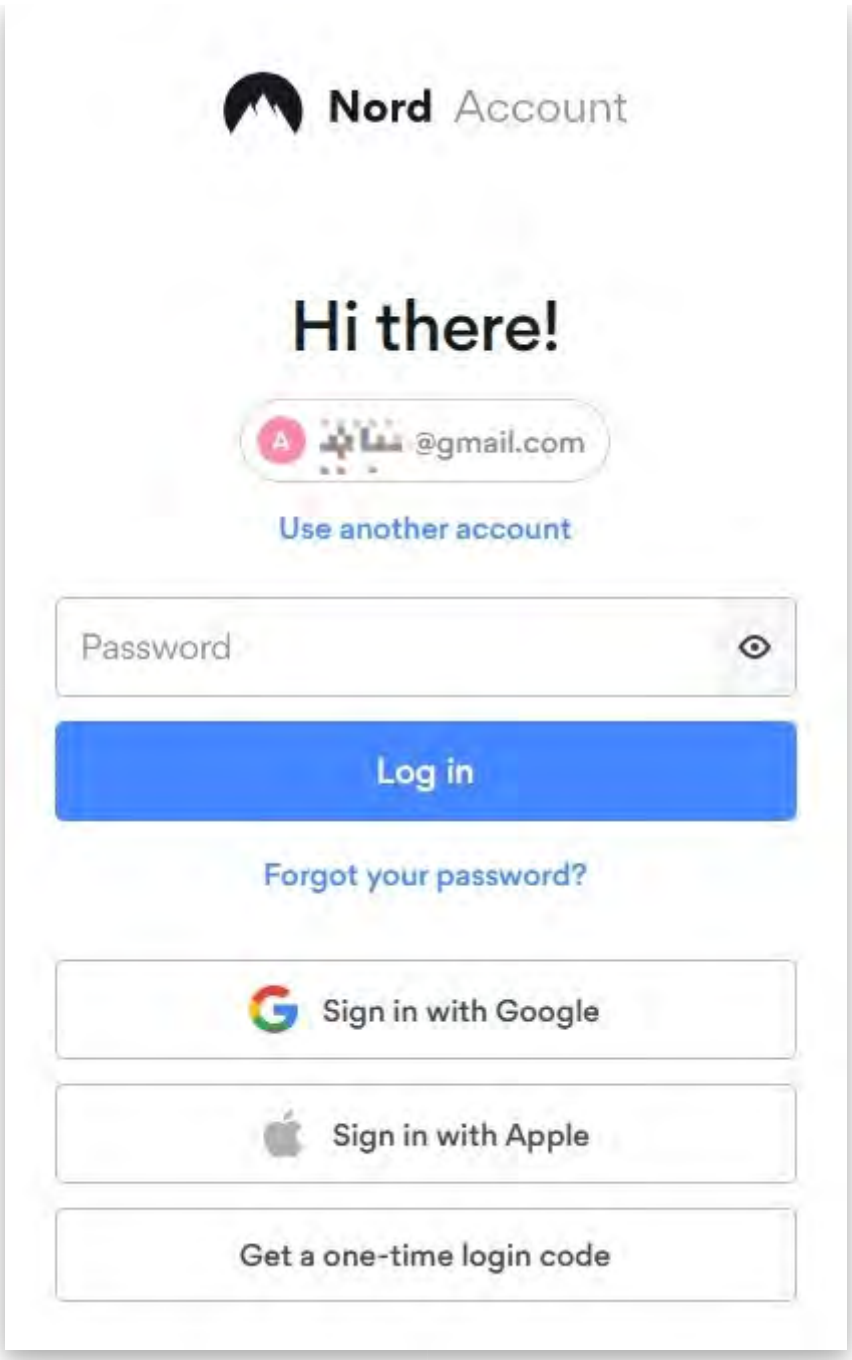
NordVPN

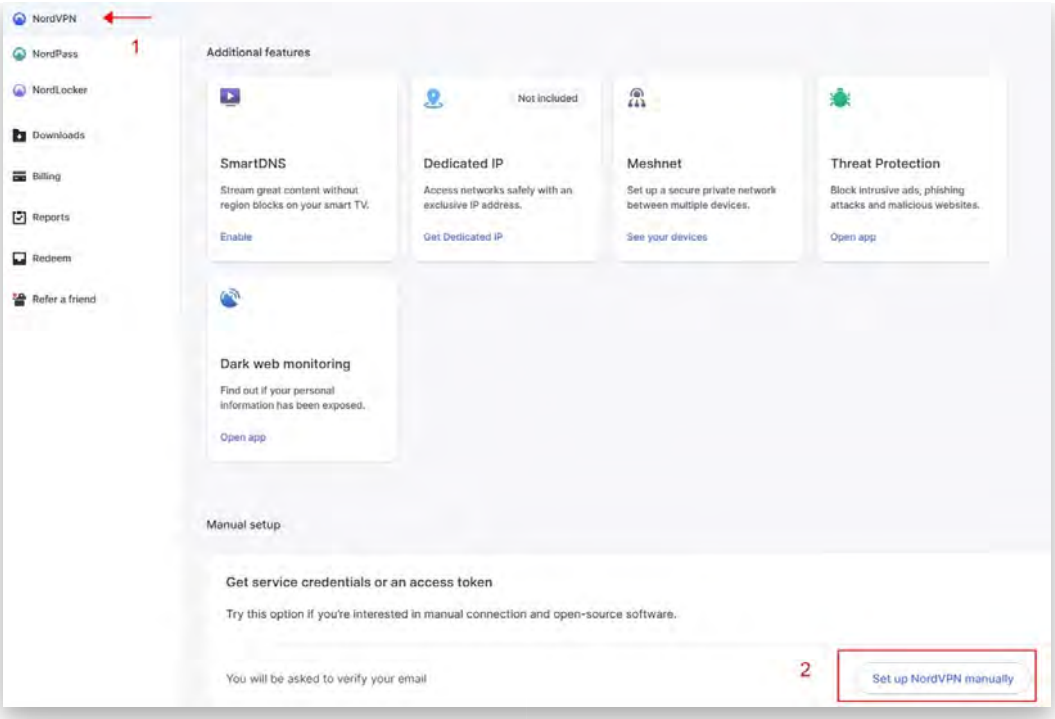
Site officiel

1. **Trouvez vos informations d'utilisateur**

   Les identifiants de service NordVPN sont différents de vos identifiants de compte NordVPN, à savoir votre adresse e-mail et votre mot de passe. Vous aurez besoin d'informations d'identification de service NordVPN pour vous connecter au VPN en utilisant la méthode de configuration manuelle OpenVPN dans le routeur.

   Connectez-vous sur le site officiel, accédez au tableau de bord du Compte Nord, où vous trouverez les justificatifs du service.

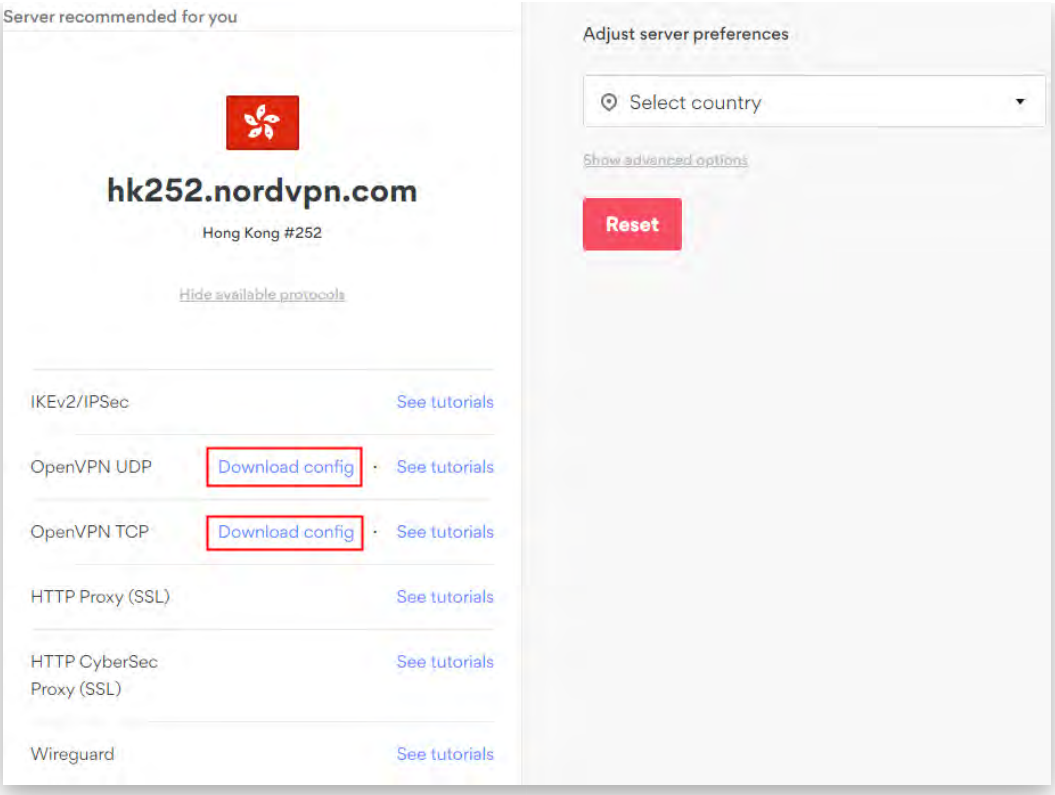

Nord Account
Hi there!
@gmail.com
Use another account
Password
Log in
Forgot your password?
Sign in with Google
Sign in with Apple
Get a one-time login code





2. **Choisir un serveur NordVPN**

   Allez à l'utilitaire de serveur recommandé NordVPN ici. Il recommandera une base de serveur sur votre réseau, cliquez sur **Afficher les protocoles disponibles** pour télécharger la configuration UDP ou TCP. Cliquez ici pour voir la différence.



Vous pouvez télécharger tous les serveurs configs ici.

Conseils: si le fichier zip est trop grand pour être téléchargé, vous pouvez supprimer un .ovpn dans le fichier .zip ou télécharger un seul fichier .ovpn.

Liaison de référence

Vous pouvez également utiliser l'application mobile pour configurer NordVPN.

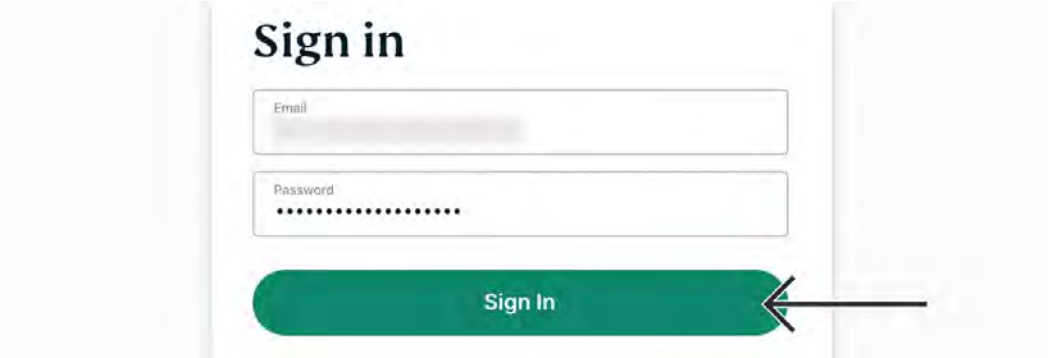
ExpressVPN

ExpressVPN

Site officiel

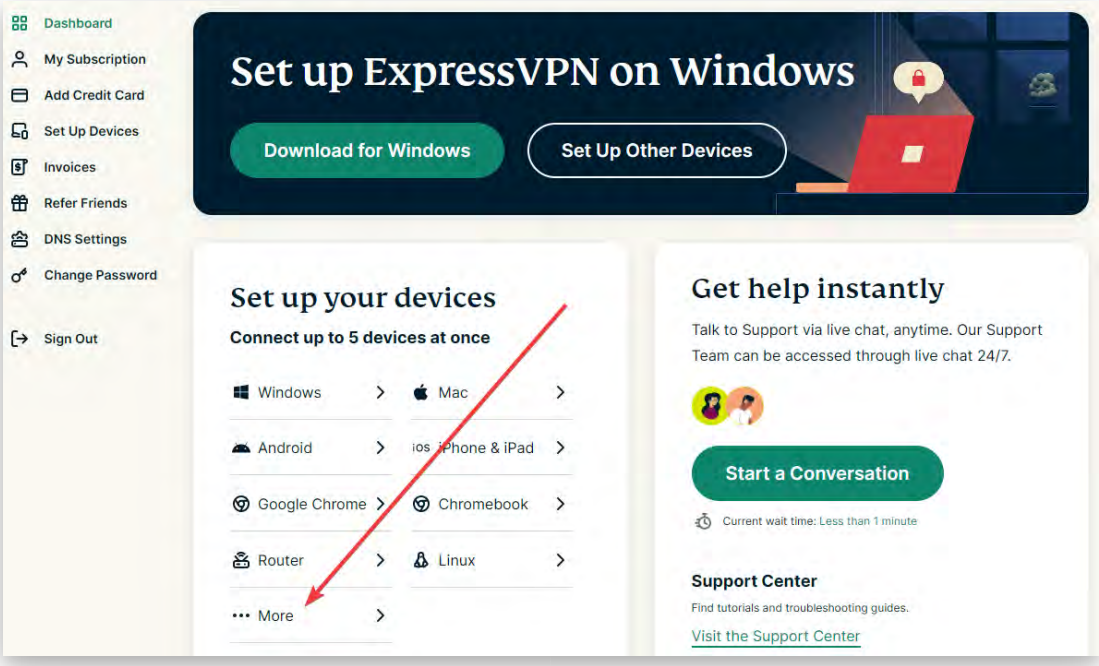
Informations citées à l'intention officielle d'Expressvpn

1. Allez sur le site web d'ExpressVPN, et connectez-vous avec vos identifiants ExpressVPN.

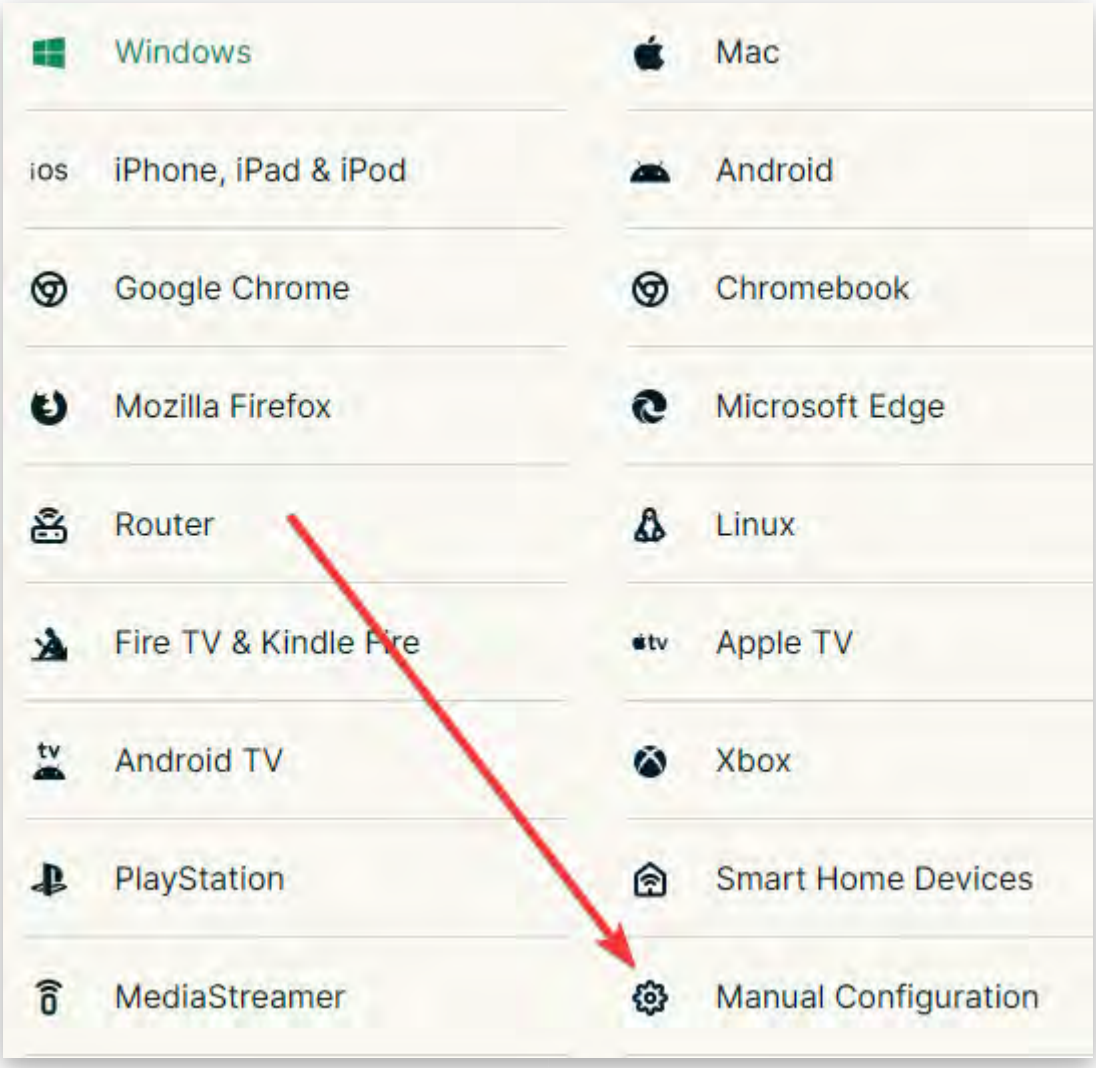


Entrez le code de vérification qui est envoyé à votre courriel.

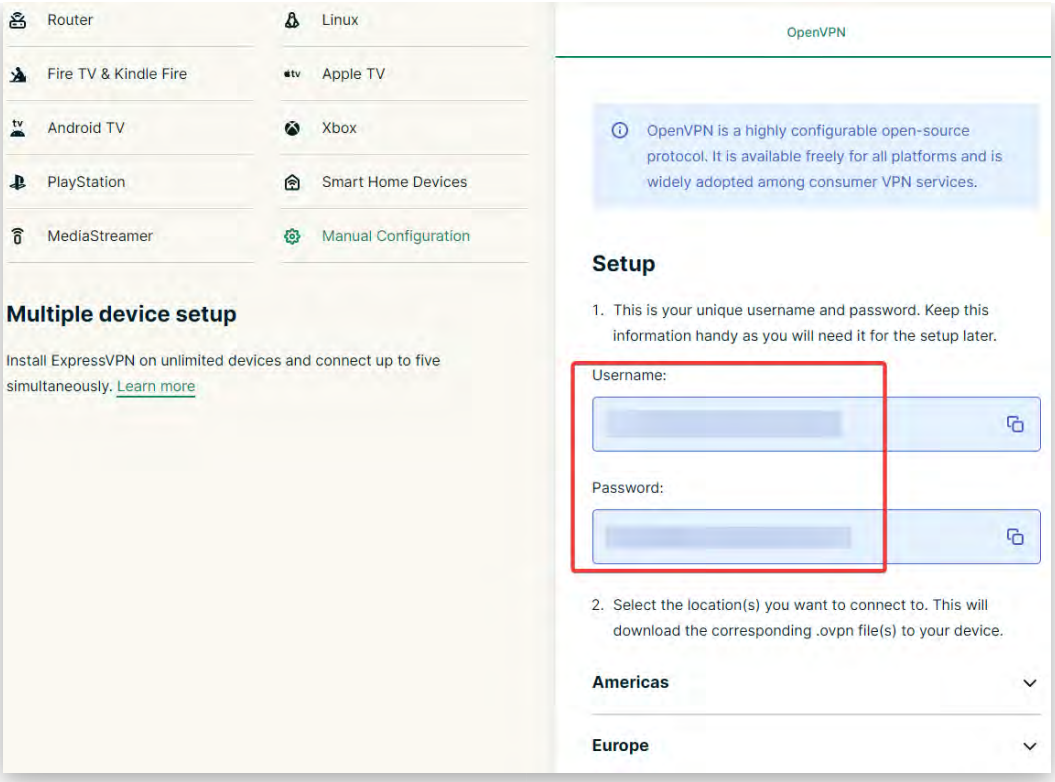
2. Dans la section "Réglez vos appareils", cliquez sur **Plus**.



1. Cliquez sur **Configuration manuelle**.



1. Vous verrez votre **nom d'utilisateur**, **votre mot de passe** et une liste de **fichiers** de **configuration OpenVPN**.



Cliquez sur le(s) emplacement(s) que vous souhaitez pour télécharger le(s) fichier(s) .ovpn.

Gardez cette fenêtre du navigateur ouverte. Vous aurez besoin de ces informations pour la configuration plus tard.

Liaison de référence

PIA (Accès privé à Internet)

PIA (Accès privé à Internet)

Site officiel

Télécharger directement.

Conseils: si le fichier zip est trop grand pour être téléchargé, vous pouvez supprimer un .ovpn dans le fichier .zip ou télécharger un seul fichier .ovpn.

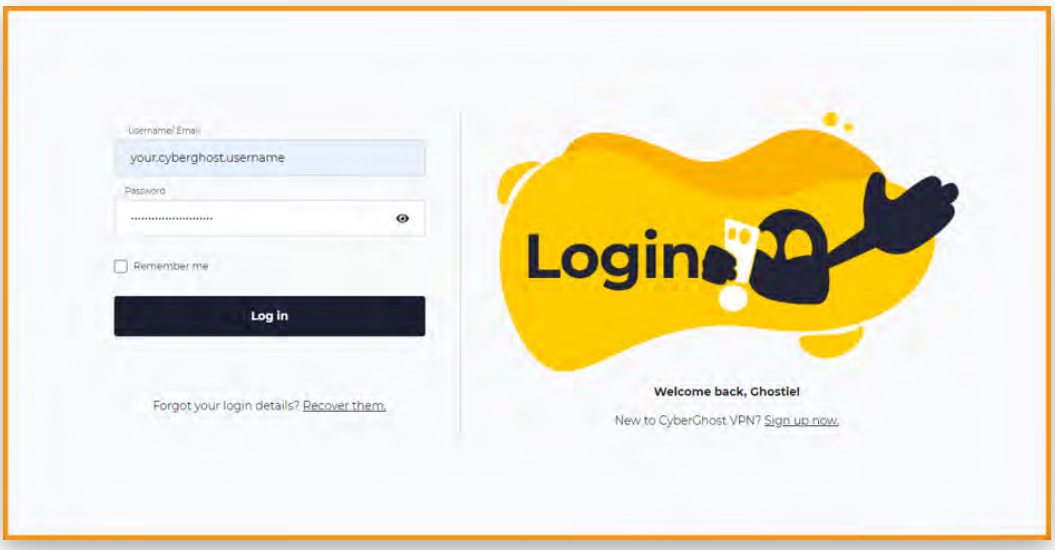
CyberGhost

CyberGhost

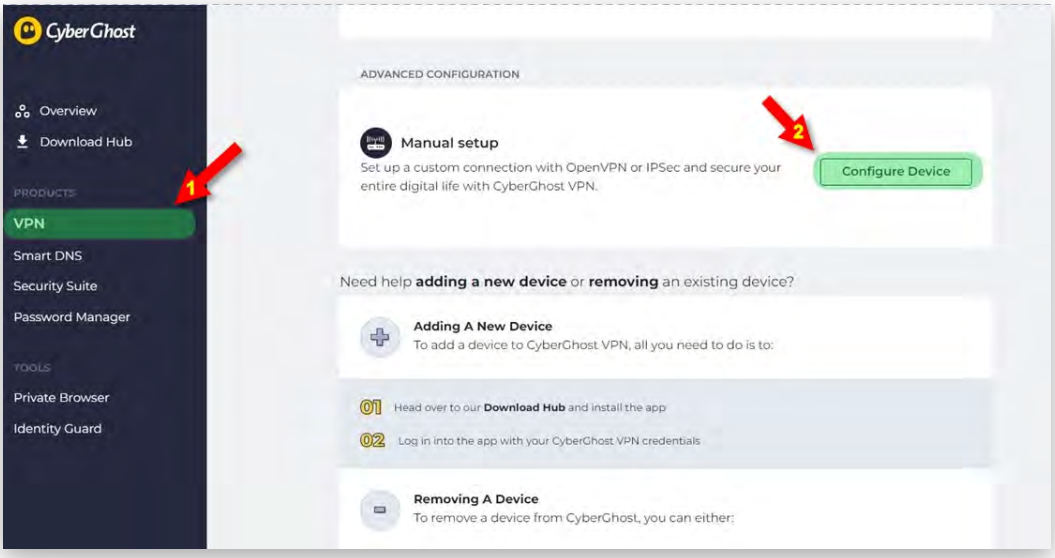
Site officiel

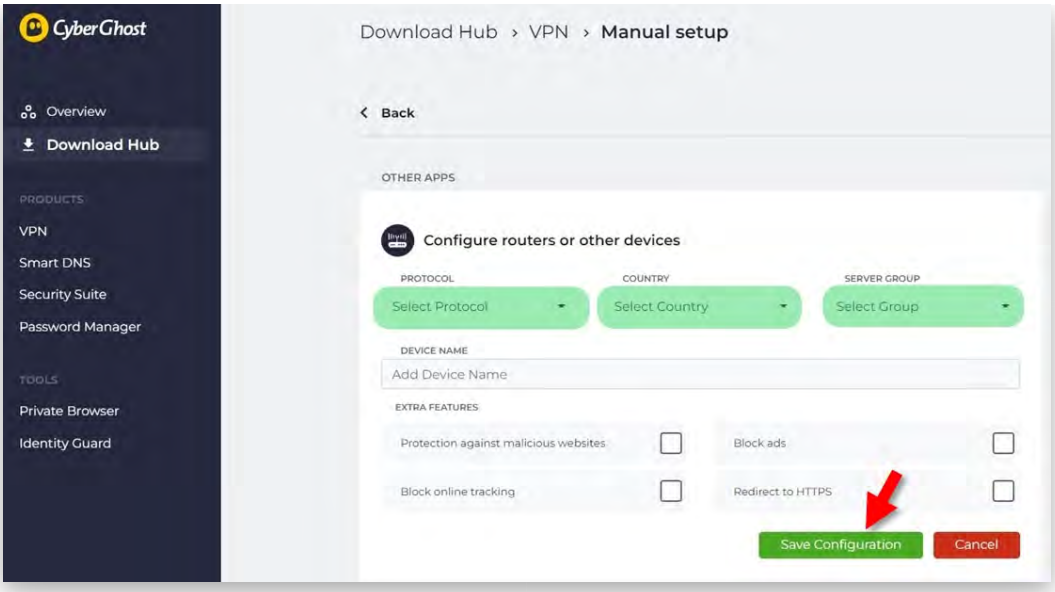
Informations citées dans l'instruction officielle de CyberGhost

1. Connectez votre compte en ligne CyberGhost VPN.



2. Sélectionnez « **VPN** » dans le menu de gauche, puis cliquez sur « **Configurer le dispositif** » et créez votre configuration de serveur, comme décrit ci-dessous :





3. Maintenant, créez votre configuration serveur, comme décrit ci-dessous:

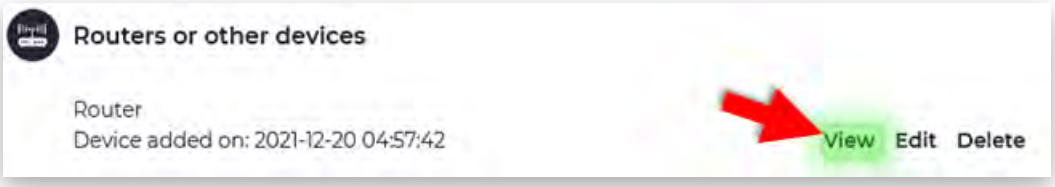
   - **Protocole** : **OpenVPN 2.3**
   - **Pays** : Étant donné que les connexions de protocole natif ne peuvent être utilisées qu'avec exactement un serveur, vous devez maintenant choisir le pays dans lequel vous voulez naviguer ; le serveur à utiliser dans ce pays sera choisi automatiquement par CyberGhost.
   - **Groupe de serveurs** : Choisissez le groupe de serveurs et le protocole OpenVPN (UDP ou TCP) que vous souhaitez utiliser

   OpenVPN UDP permet une vitesse plus élevée que la version TCP, mais peut entraîner des téléchargements interrompus dans certains cas. Il s'agit du réglage par défaut.

   OpenVPN TCP permet des connexions plus stables que la version UDP mais est un peu plus lent. Choisissez cette version, si vous avez des problèmes de connexion récurrents tels que des déconnexions soudaines.

   Une fois les paramètres souhaités choisis, sauvegardez-les avec **Save Configuration**

4. Pour visualiser les identifiants **OpenVPN** qui sont générés pour vous sur le tableau de bord de configuration, appuyez sur **View Configuration**.



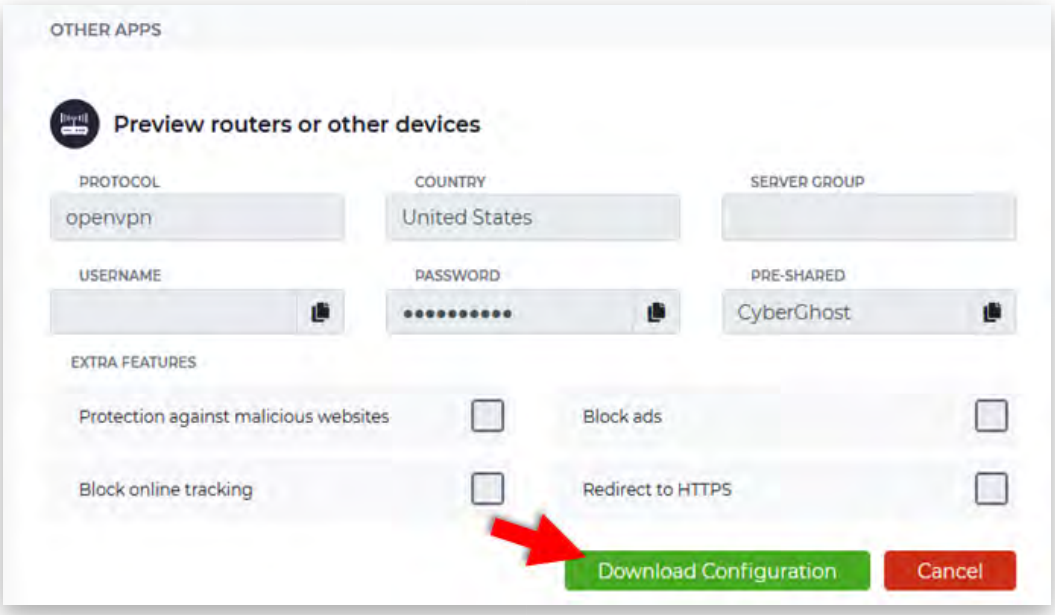
5. Après avoir défini vos préférences de connexion, veuillez prendre note des points suivants:

   - **Groupe de serveur** : Il s'agit de l'adresse du pays (serveur) avec lequel vous souhaitez être connecté, par exemple '12345-1-ca.cg-dialup.net'. Cela aborde les changements avec tous les pays que vous avez choisis dans la mesure précédente. Le serveur unique réel à utiliser sera choisi automatiquement par CyberGhost.
   - **Nom d'utilisateur** : Un nom d'utilisateur généré uniquement pour ce protocole. Ce n'est

PAS votre nom d'utilisateur de compte CyberGhost habituel, il n'est utilisé que pour s'authentifier avec les serveurs CyberGhost via des configurations manuelles. Vous en aurez besoin lorsque vous créerez OpenVPN sur les routeurs GL.iNet.

- **Mot de passe** : Un mot de passe uniquement pour l'utilisation du protocole généré. Ce n'est PAS votre mot de passe de compte CyberGhost habituel, il est utilisé uniquement pour s'authentifier avec les serveurs CyberGhost via des configurations manuelles. Vous en aurez besoin lorsque vous créerez OpenVPN sur les routeurs GL.iNet.

Une fois cela fait, veuillez télécharger le fichier de configuration. Pour cela, cliquez sur *Download Configuration* et téléchargez le fichier de configuration sur votre ordinateur



PrivateVPN

PrivateVPN

Site officiel

Télécharger directement.

Voici le lien de téléchargement officiel. En raison d'un bogue rencontré lors de l'importation du routeur, le nom du fichier à l'intérieur contient des caractères spéciaux 'Bogot'. Nous l'avons rebaptisé et fourni le lien de téléchargement ci-dessus. Nous corrigerons ce bug dans les versions futures.

Conseils: si le fichier zip est trop grand pour être téléchargé, vous pouvez supprimer un .ovpn dans le fichier .zip ou télécharger un seul fichier .ovpn.

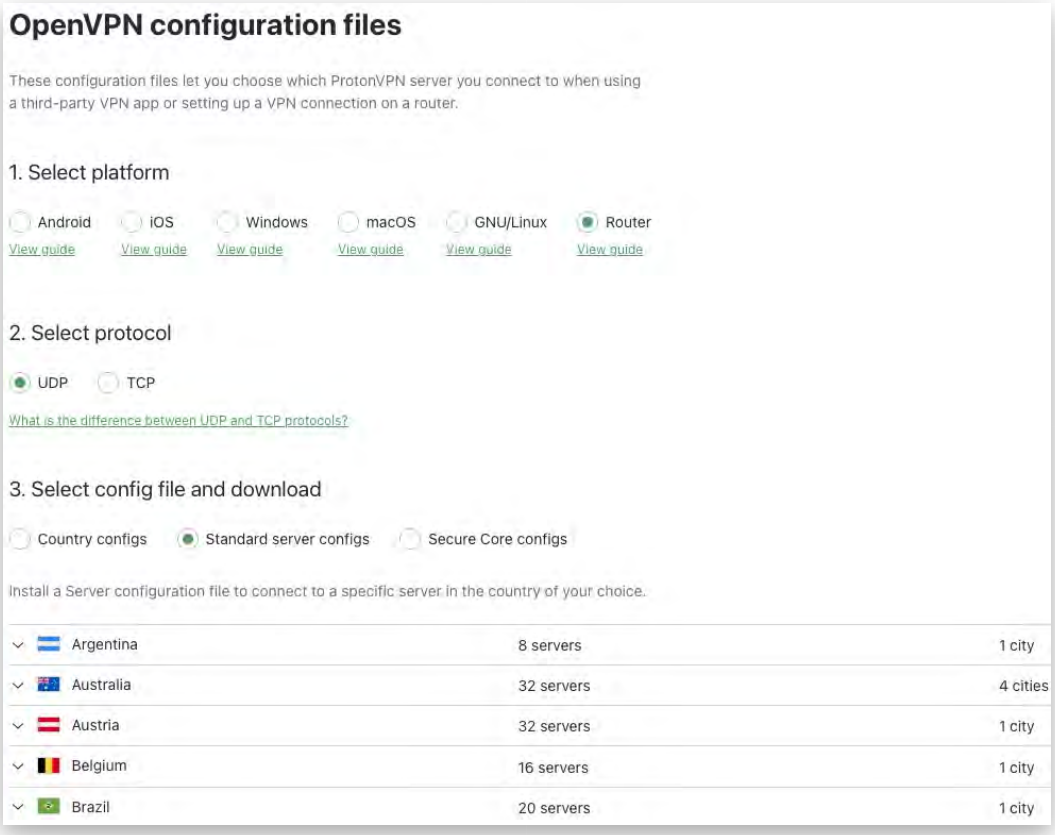
Proton VPN

Proton VPN

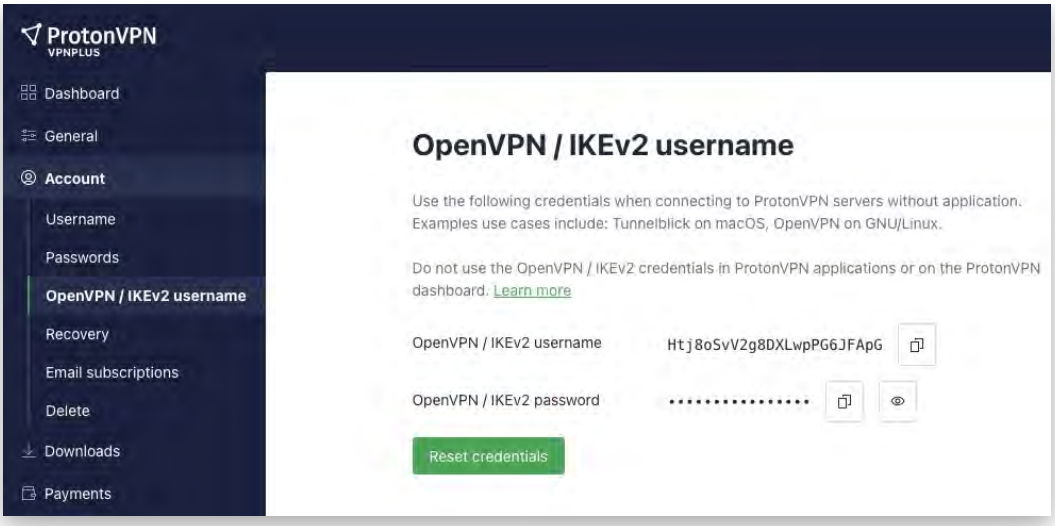
Site officiel

Proton VPN a WireGuard service, nous recommandons d'utiliser WireGuard, caisse ici.

1. Connectez votre compte Proton VPN.
2. Cliquez sur **Télécharger** sur le côté gauche.
3. Choisissez la plate-forme de routeur, le protocole, etc., trouvez votre pays cible pour télécharger le fichier de configuration.



4. Le certificat de connexion OpenVPN n'est pas celui qui connecte le tableau de bord du site Proton. Vous pouvez trouver le **nom d'utilisateur** crdential sur **Account -**



PureVPN

PureVPN

Site officiel

Télécharger directement.

Conseils: si le fichier zip est trop grand pour être téléchargé, vous pouvez supprimer un .ovpn dans le fichier .zip ou télécharger un seul fichier .ovpn.

Liaison de référence

Les routeurs GL.iNet ne prennent pas en charge la fonctionnalité IP dédiée de PureVPN, car il a besoin de PPTP.

Surfre

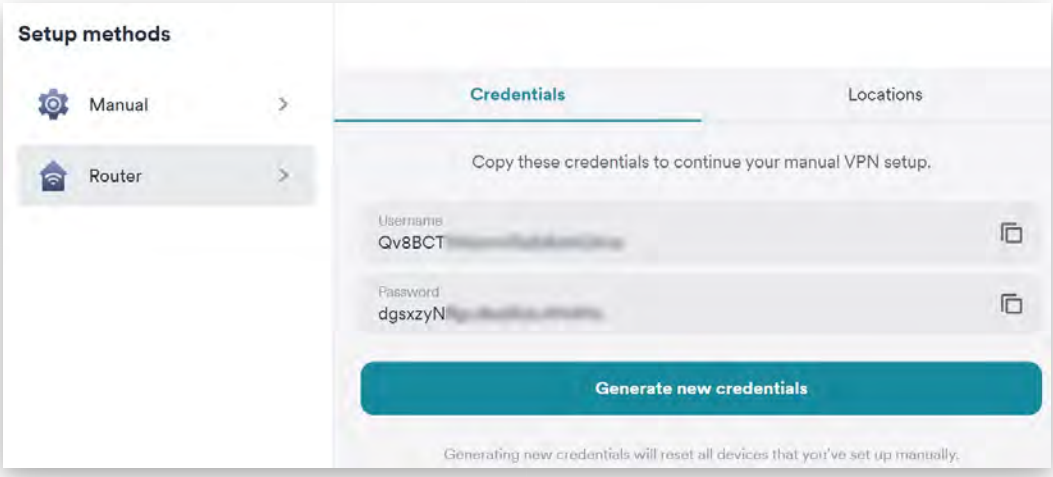
Surfre

Site officiel

1. **Trouvez vos informations d'utilisateur**

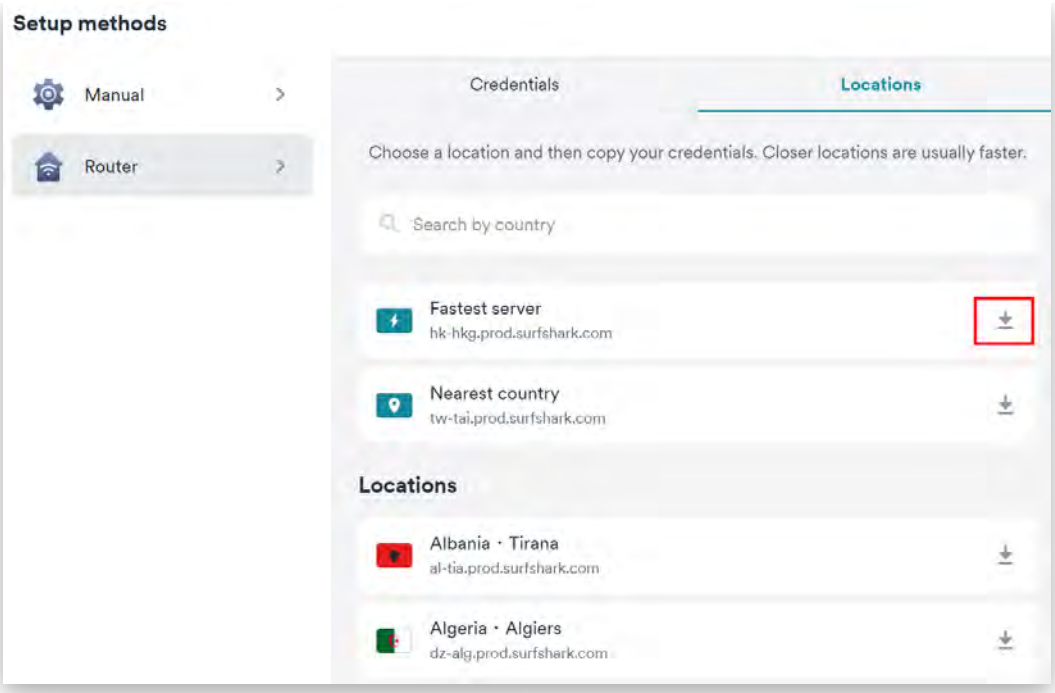
   Les identifiants du service Surfshark sont différents de vos identifiants de compte Surfshark, à savoir votre adresse e-mail et votre mot de passe. Vous aurez besoin des identifiants de service Surfshark pour vous connecter au VPN en utilisant la méthode de configuration manuelle OpenVPN dans le routeur.

   Connectez-vous au site officiel, allez sur cette page, où vous trouverez tous les détails nécessaires à une connexion manuelle.

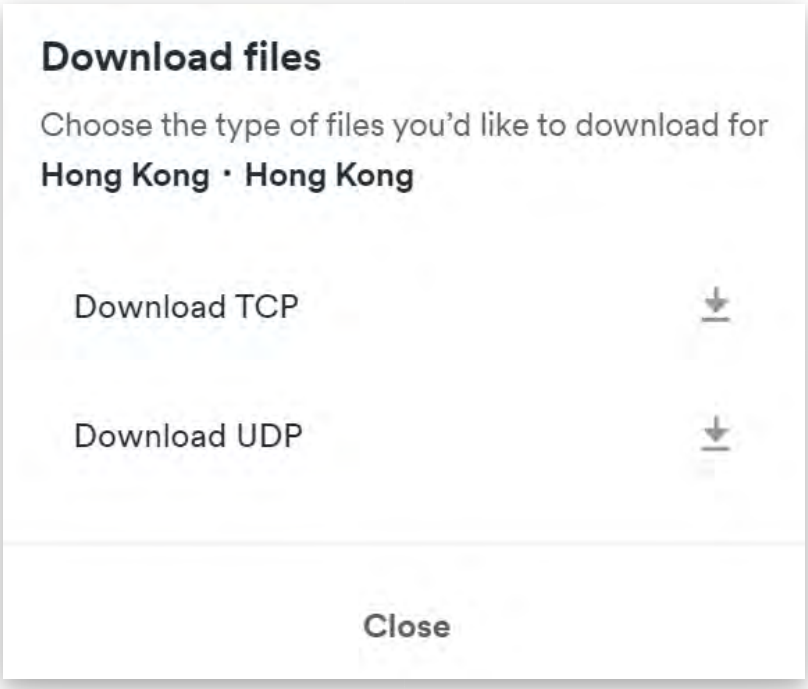


2. **Choisir un serveur Surfshark**

   Sélectionnez l'onglet **Lieux**, où vous verrez tous les serveurs Surfshark.



Il demandera de choisir TCP ou UDP. Cliquez ici pour voir la différence.



Vous pouvez télécharger toutes les configurations ici directement.

Conseils: si le fichier zip est trop grand pour être téléchargé, vous pouvez supprimer un .ovpn dans le fichier .zip ou télécharger un seul fichier .ovpn.

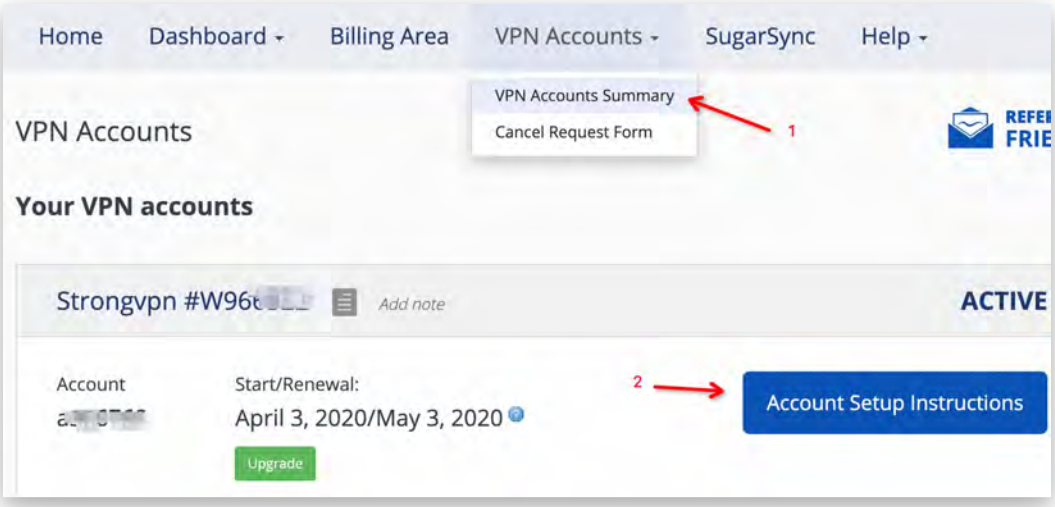
Liaison de référence

StrongVPN

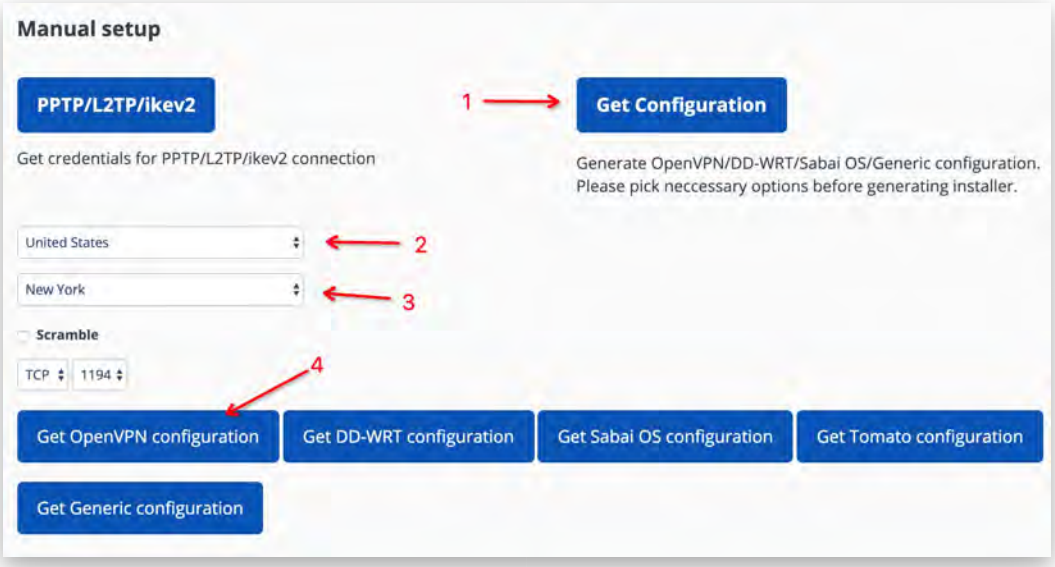
StrongVPN

Site officiel

1. Connectez-vous avec votre compte StrongVPN et vous pourrez ensuite voir le résumé des comptes VPN. Cliquez sur Instructions de configuration du compte ».



2. Trouvez la section Configuration manuelle, suivez les étapes pour obtenir la configuration.

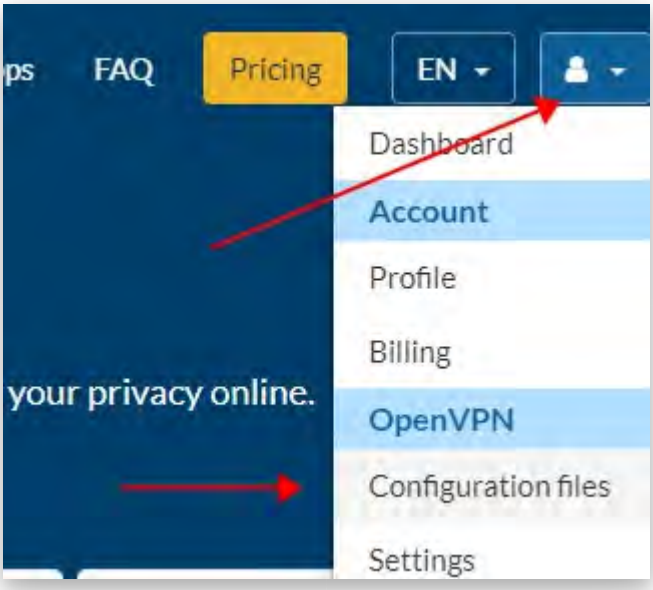


OVPN

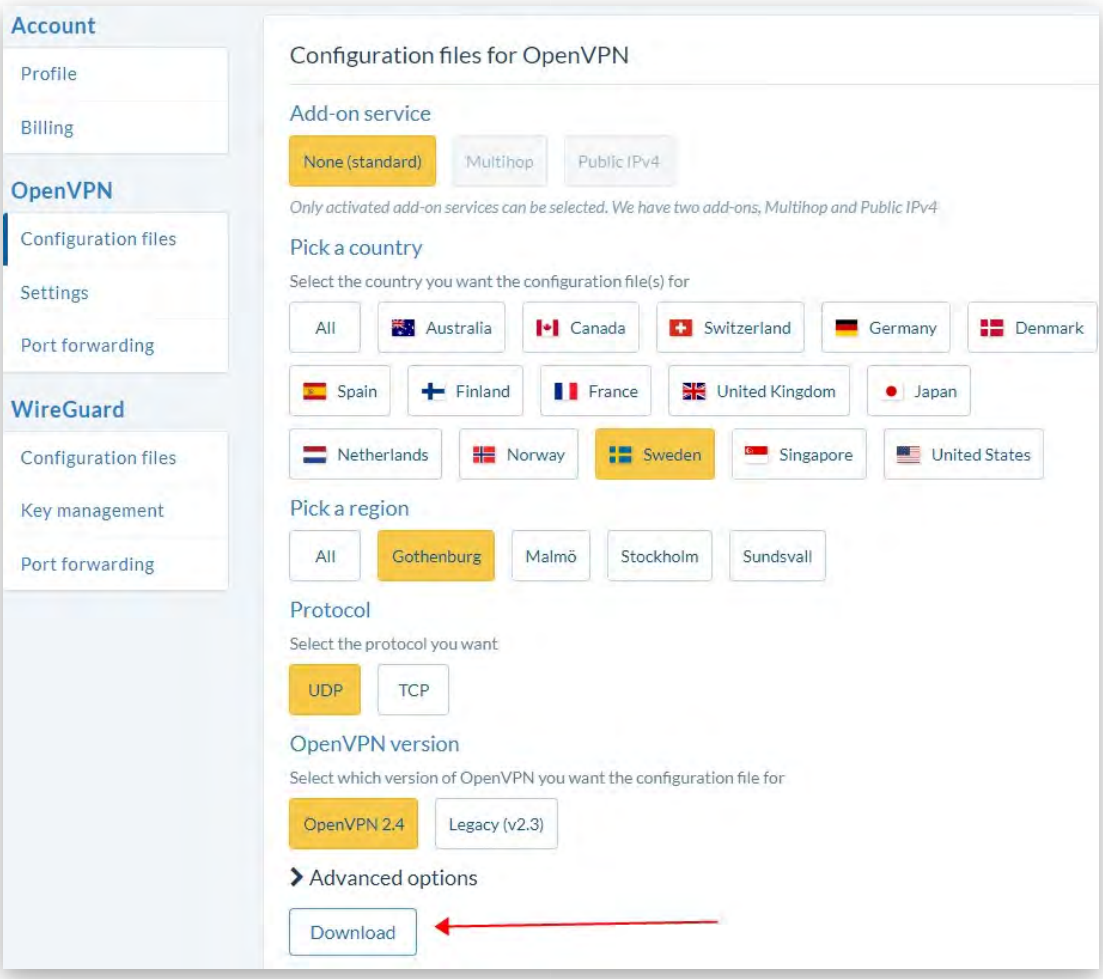
OVPN

Site officiel

Tout simplement, connectez-vous, puis vous pouvez facilement obtenir le fichier de configurations OpenVPN en cliquant sur le menu ci-dessous.



Choisissez le serveur et téléchargez.



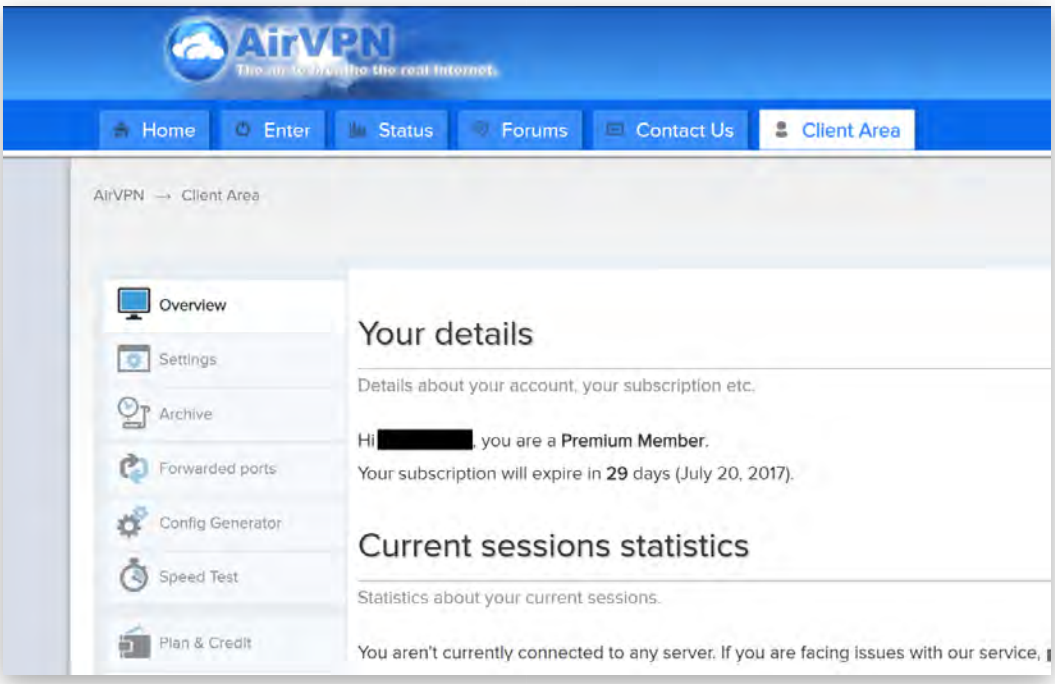
Le nom d'utilisateur et le mot de passe sont les mêmes que vous connectez OVPN.

AirVPN

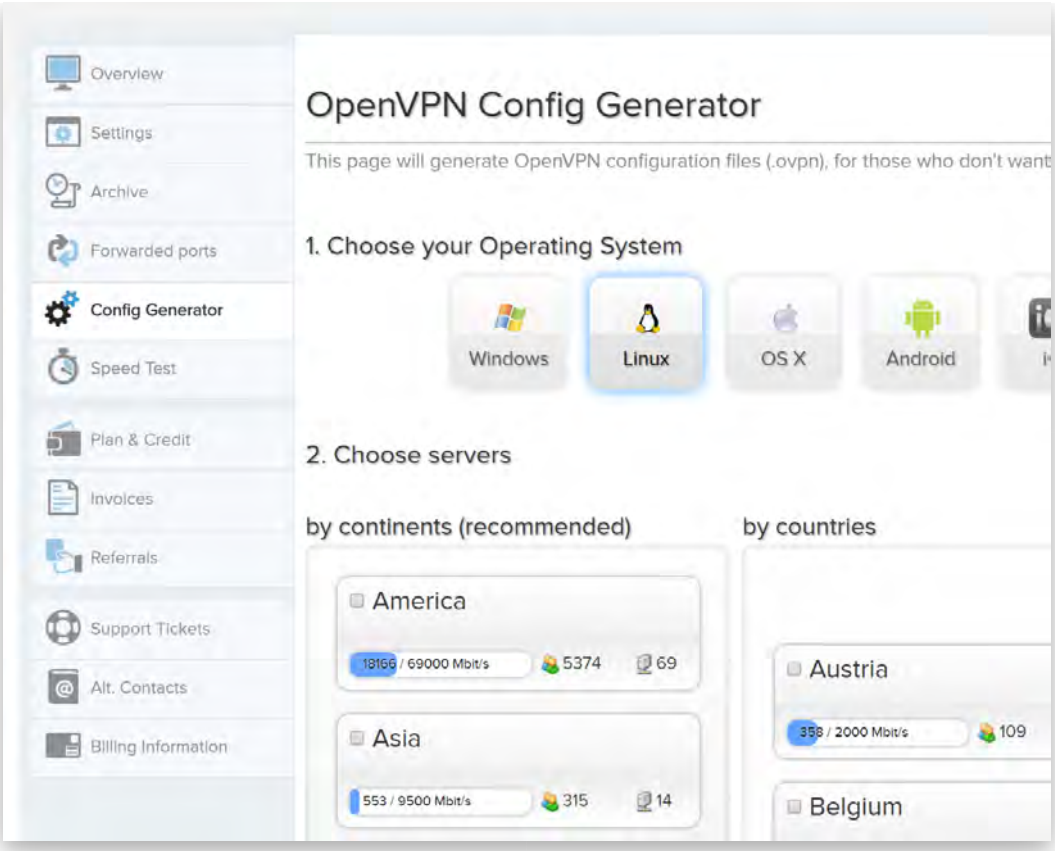
AirVPN

Site officiel

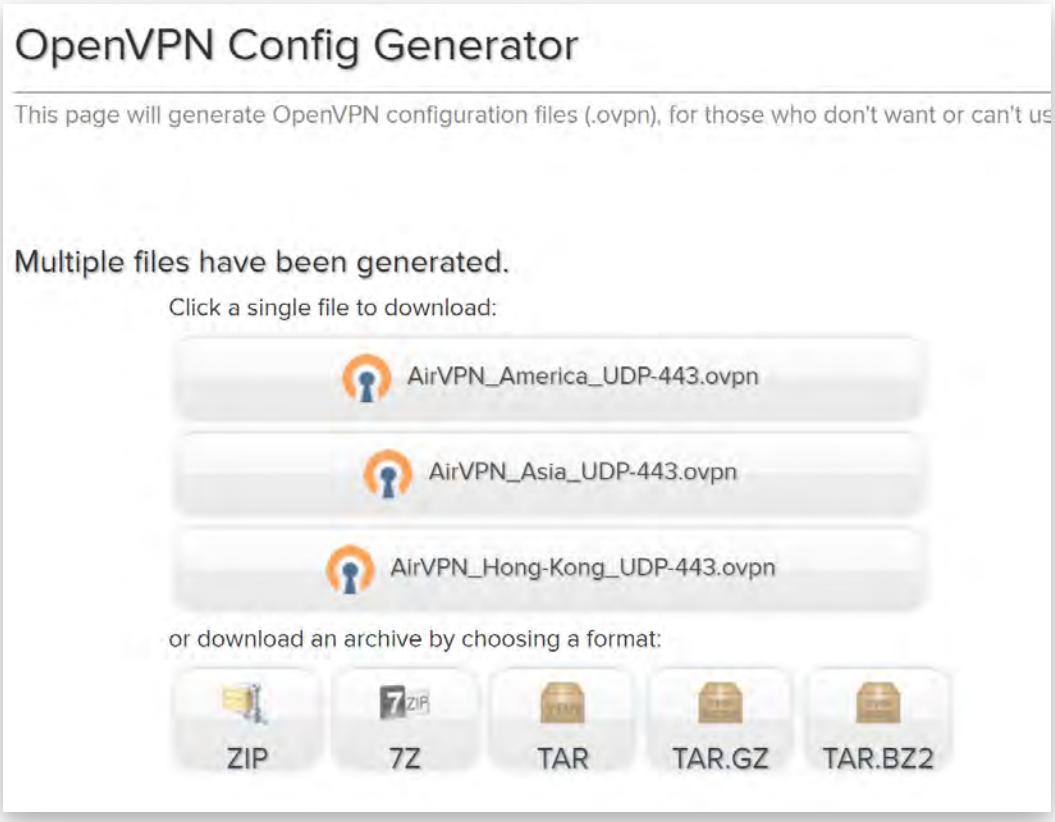
1. Login your AirVPN acoount



2. Choose Config Generator on the left and then choose Linux as your operating system. Next, choose your preferred server.



3. You will be able to see the download page of the configuration file.



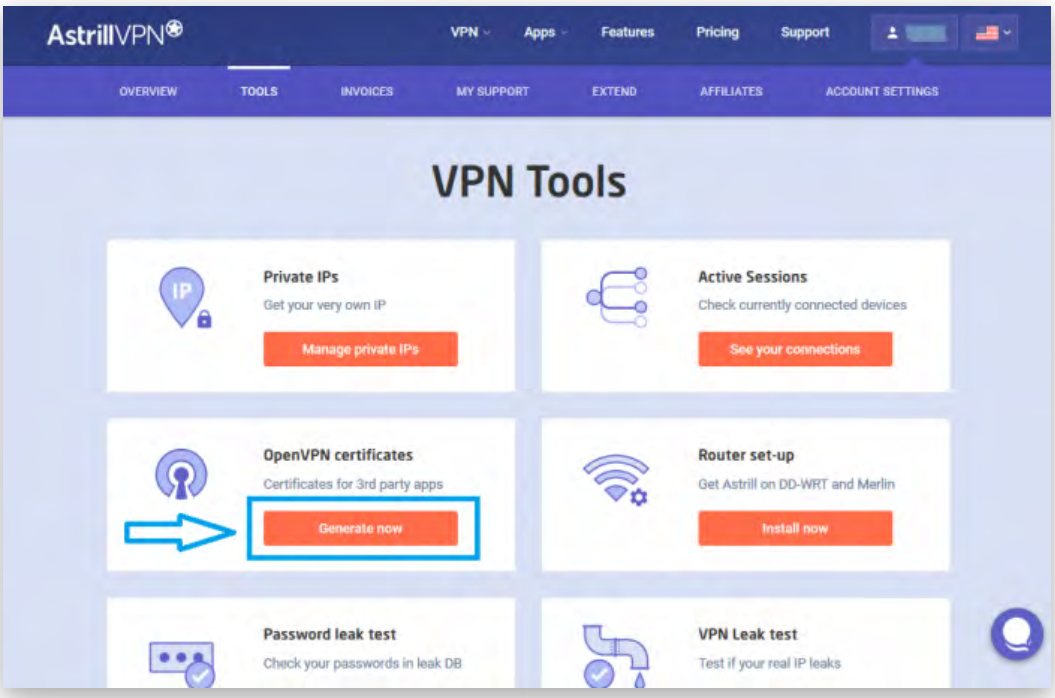
Astrill

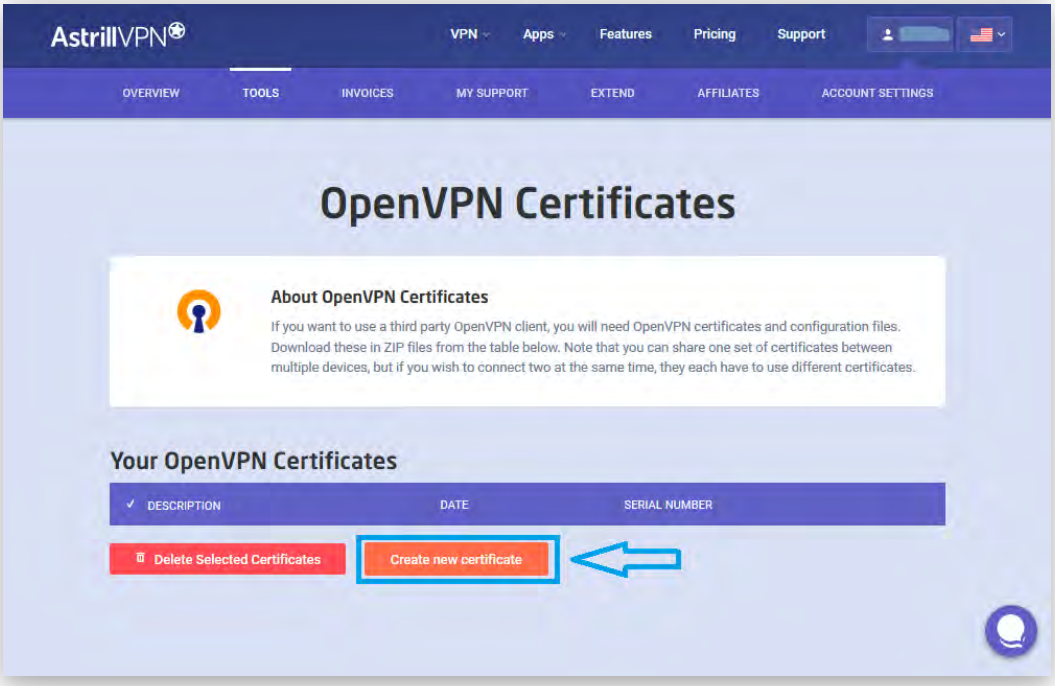
Astrill

Official Website

Information quoted from Astrill official instruction

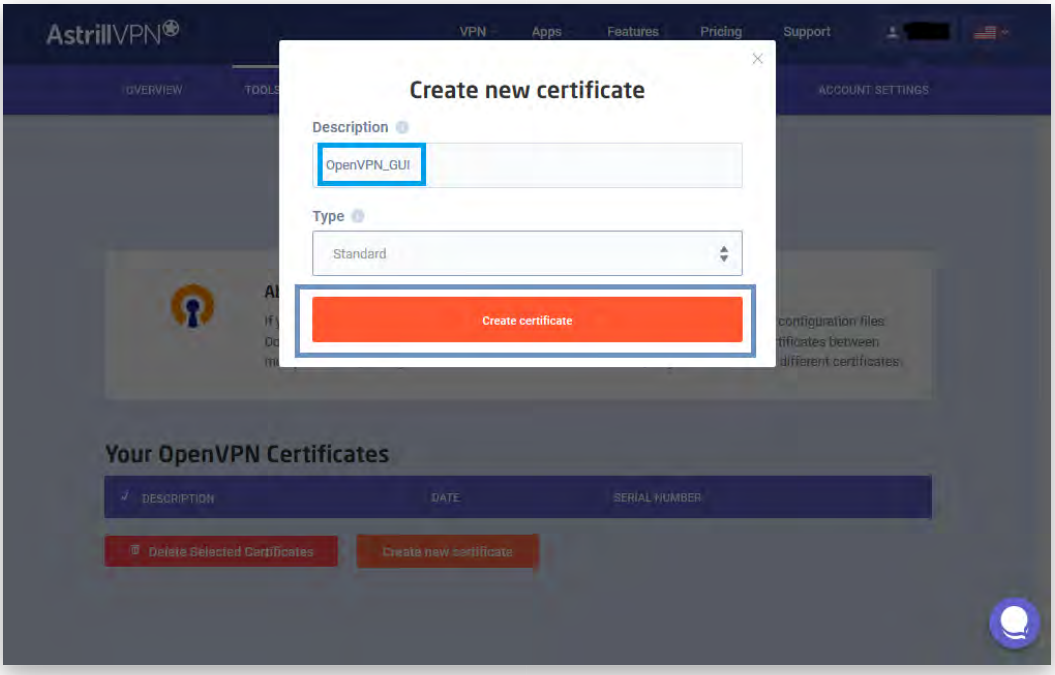
1. Generate and Download Astrill Openvpn configuration ZIP



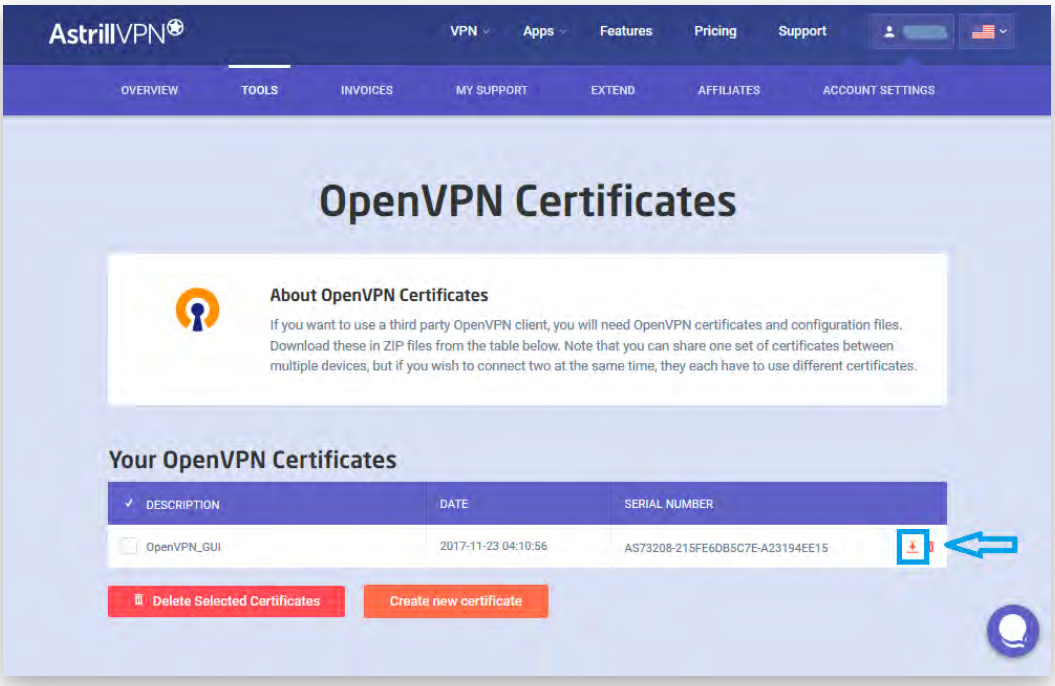


2. Type a Description like OPENVPN_GUI.

3. Click on ADD to my certificates button.



4. Once OpenVPN certificate is added, click on Download button.



bolehvpn

bolehvpn

Official Website

Login in Dashboard, download your configuration files and select the Linux_iOS inline format. Extract the zip files after completing the download.

Tips: if the zip file is too big to upload, you can delete some .ovpn in .zip file or upload single .ovpn file.

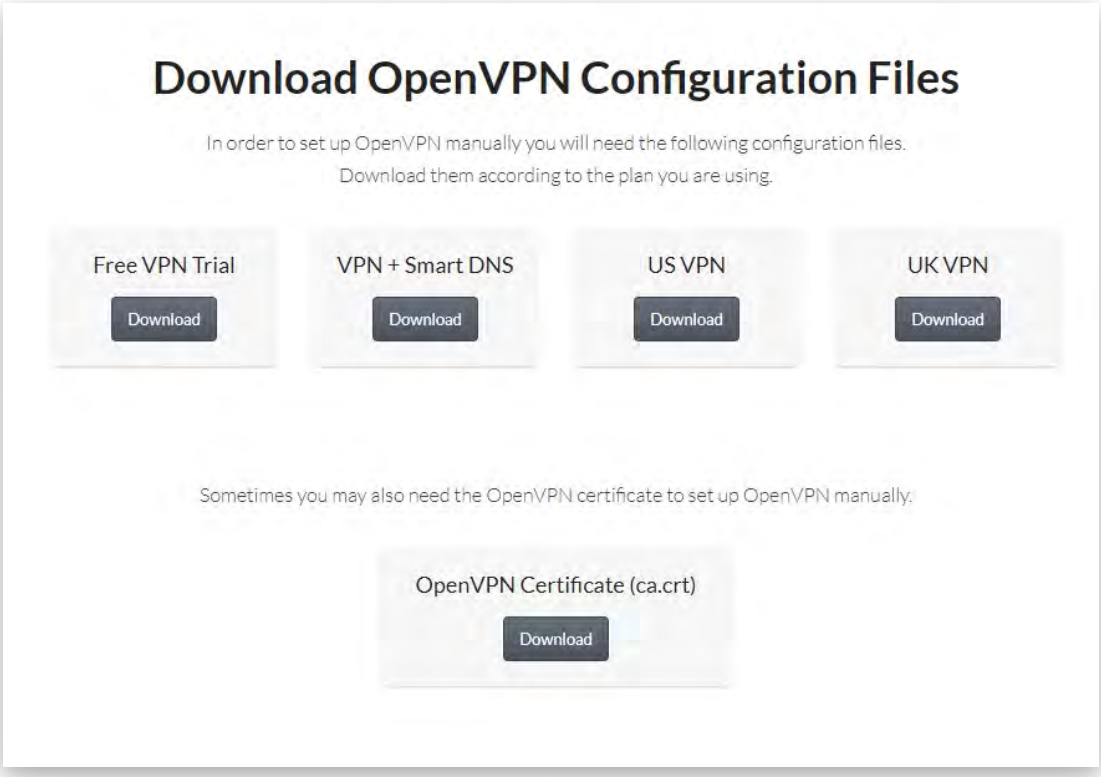
Refer link

CactusVPN

CactusVPN

Official Website

Download directly.



Cryptostorm

Cryptostorm

Official Website

Download directly.

FastestVPN

FastestVPN

Official Website

Download FastestVPN Config Files zip folder for OpenVPN TCP and UDP from here

Tips: if the zip file is too big to upload, you can delete some .ovpn in .zip file or upload single .ovpn file.

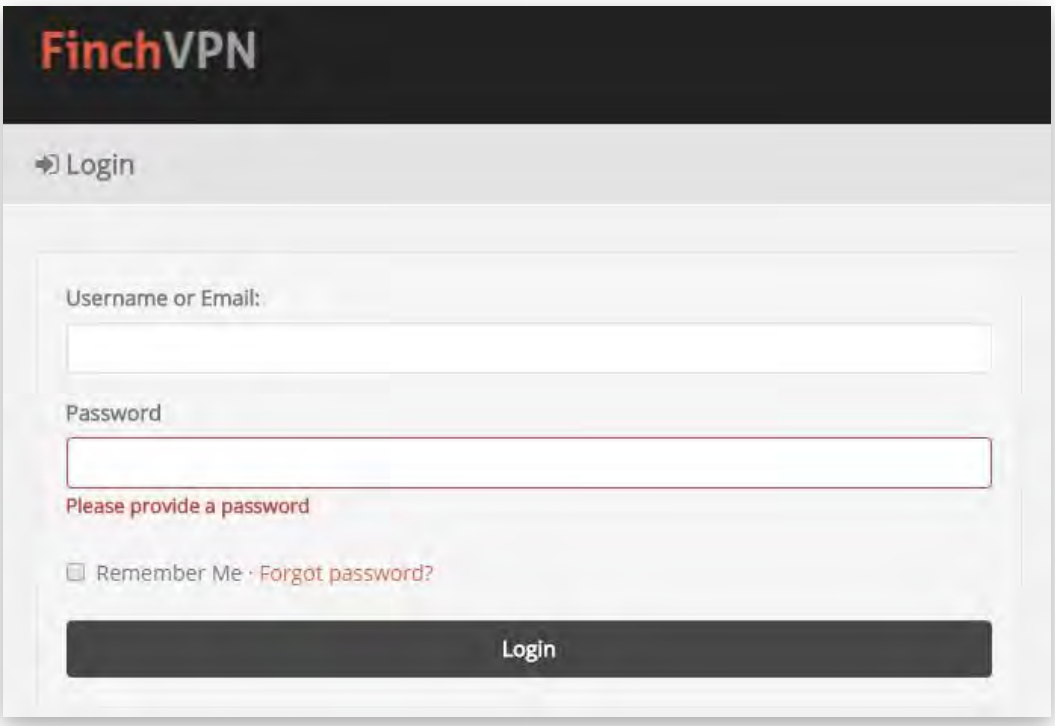
Refer link

FinchVPN

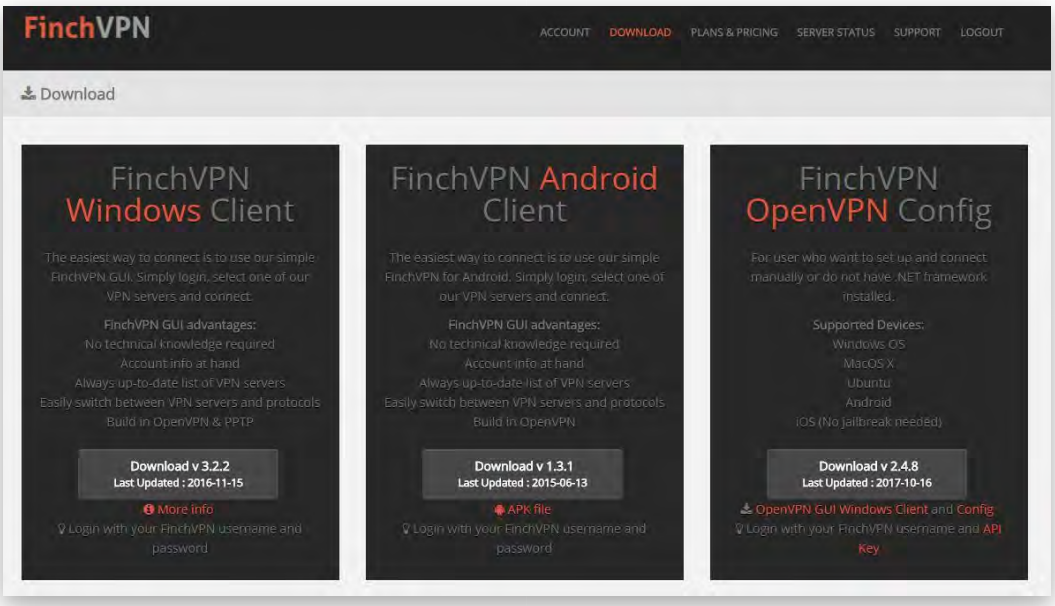
FinchVPN

Official Website

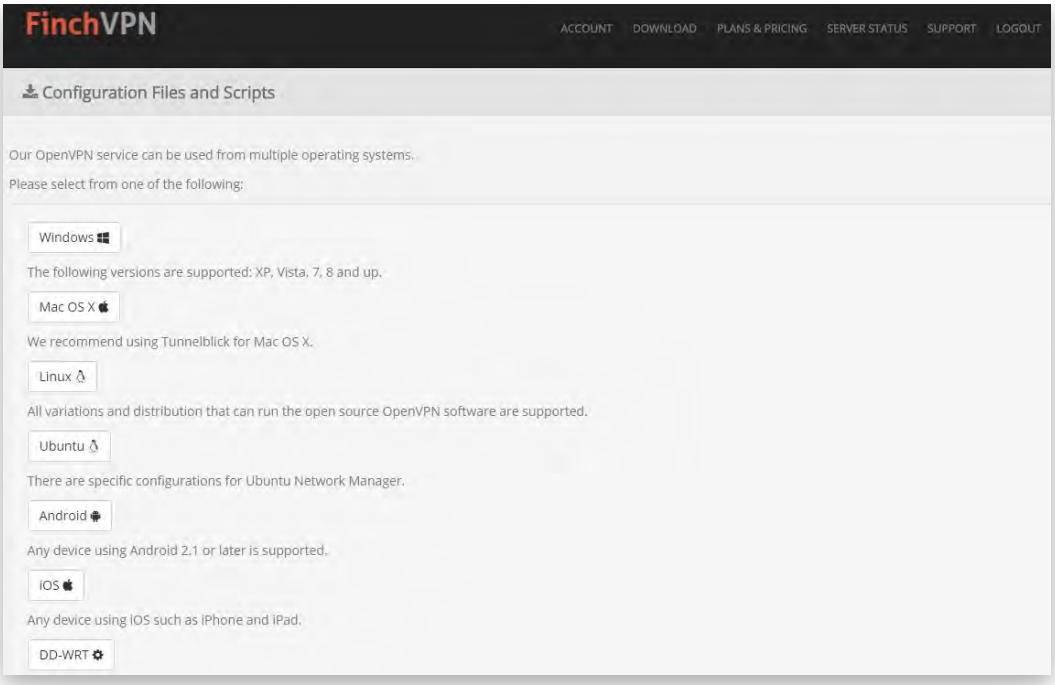
1. Login your FinchVPN account.



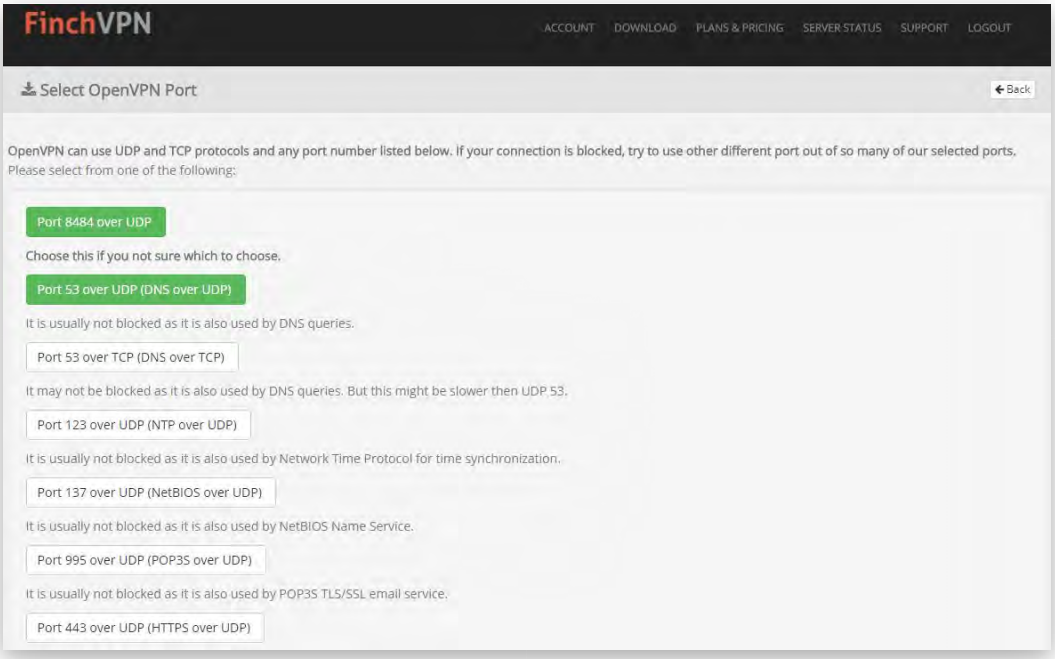
2. Go to the Download page and click Download under FinchVPN OpenVPN Config.



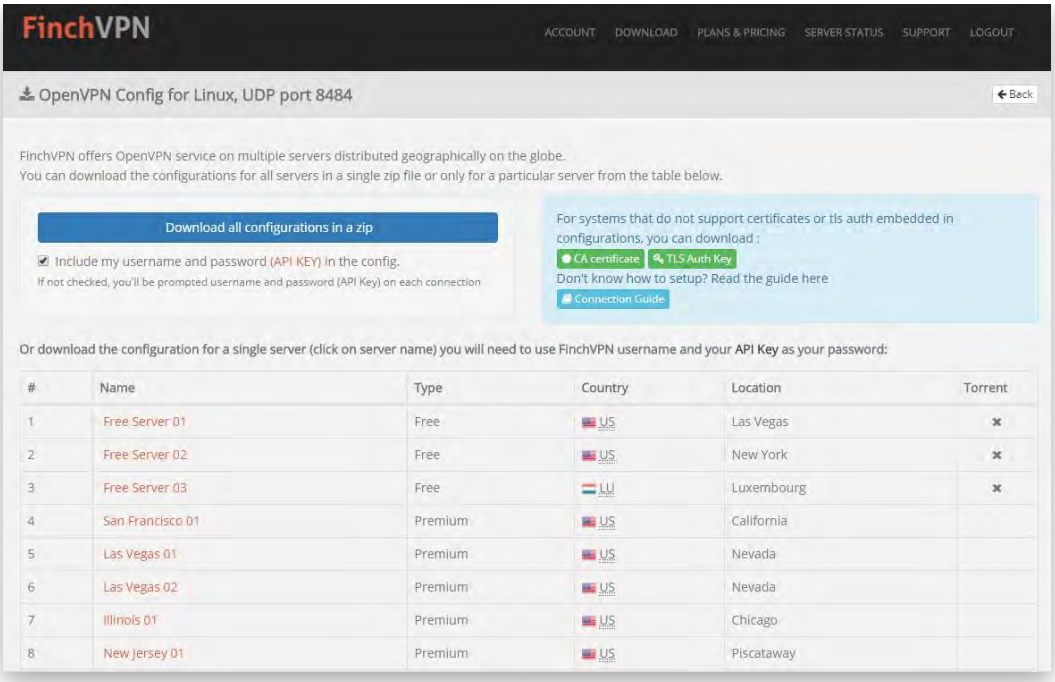
3. Choose Linux



4. Choose the protocol based on your preference. Generally, you can choose the first one **Port 8484 over UDP**



5. Remember to tick the box to include your username and password before download the file.

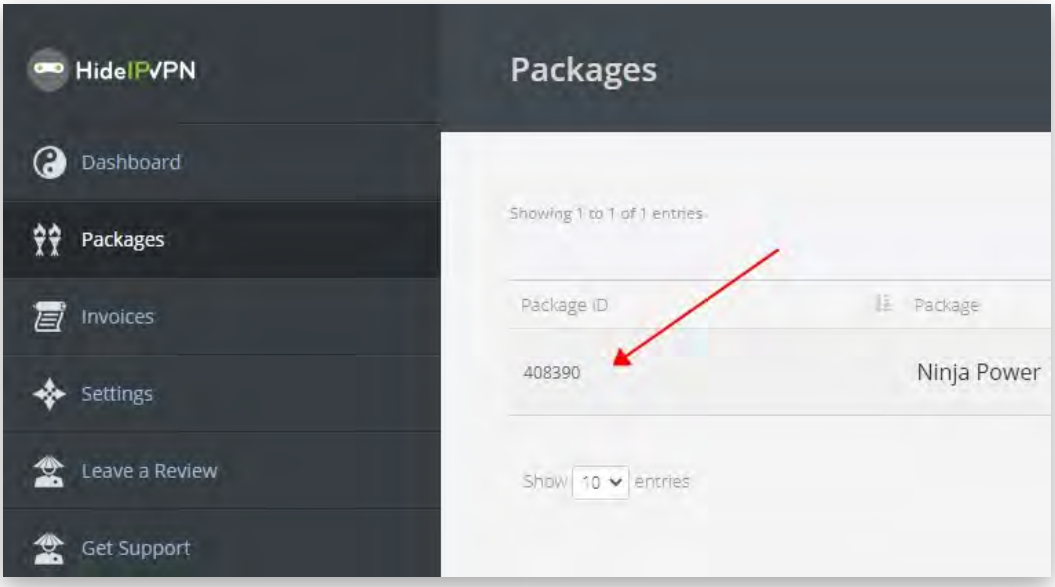

FinchVPN
ACCOUNT
DOWNLOAD
PLANS & PRICING
SERVER STATUS
SUPPORT
LOGOUT
OpenVPN Config for Linux, UDP port 8484
Back
FinchVPN offers OpenVPN service on multiple servers distributed geographically on the globe.
You can download the configurations for all servers in a single zip file or only for a particular server from the table below.
Download all configurations in a zip
Include my username and password (API KEY) in the config.
If not checked, you'll be prompted username and password (API Key) on each connection
For systems that do not support certificates or tls auth embedded in configurations, you can download :
CA certificate
TLS Auth Key
Don't know how to setup? Read the guide here
Connection Guide
Or download the configuration for a single server (click on server name) you will need to use FinchVPN username and your API Key as your password:
Name Type Country Location Torrent
1 Free Server 01 Free US Las Vegas
2 Free Server 02 Free US New York
3 Free Server 03 Free LU Luxembourg
4 San Francisco 01 Premium US California
5 Las Vegas 01 Premium US Nevada
6 Las Vegas 02 Premium US Nevada
7 Illinois 01 Premium US Chicago
8 New Jersey 01 Premium US Piscataway

HideIPVPN

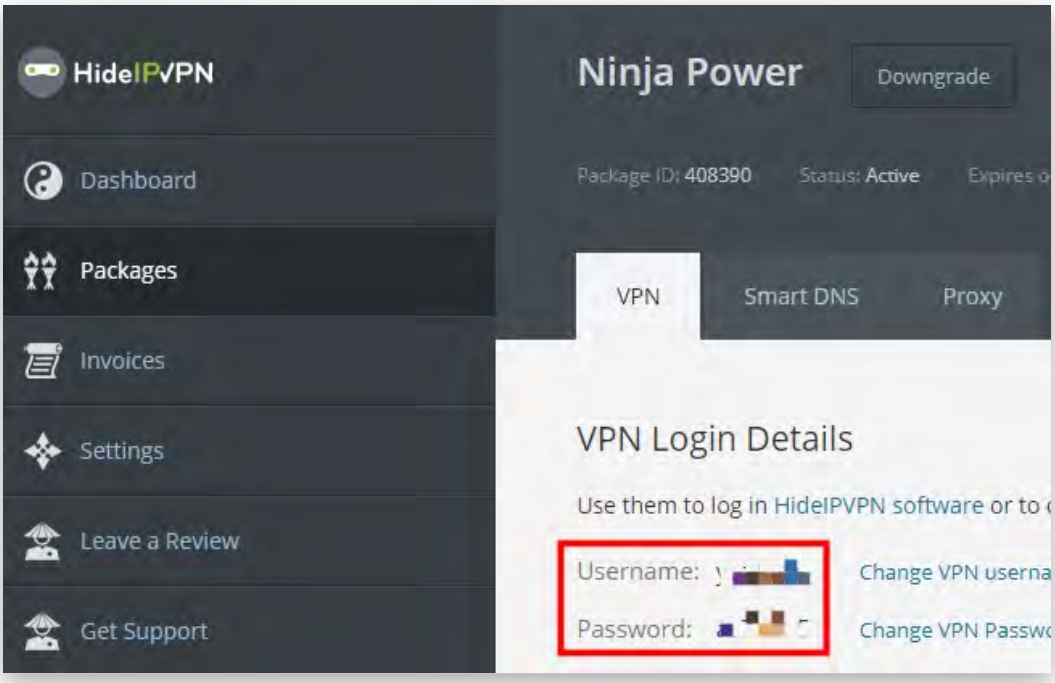
HideIPVPN

Official Website

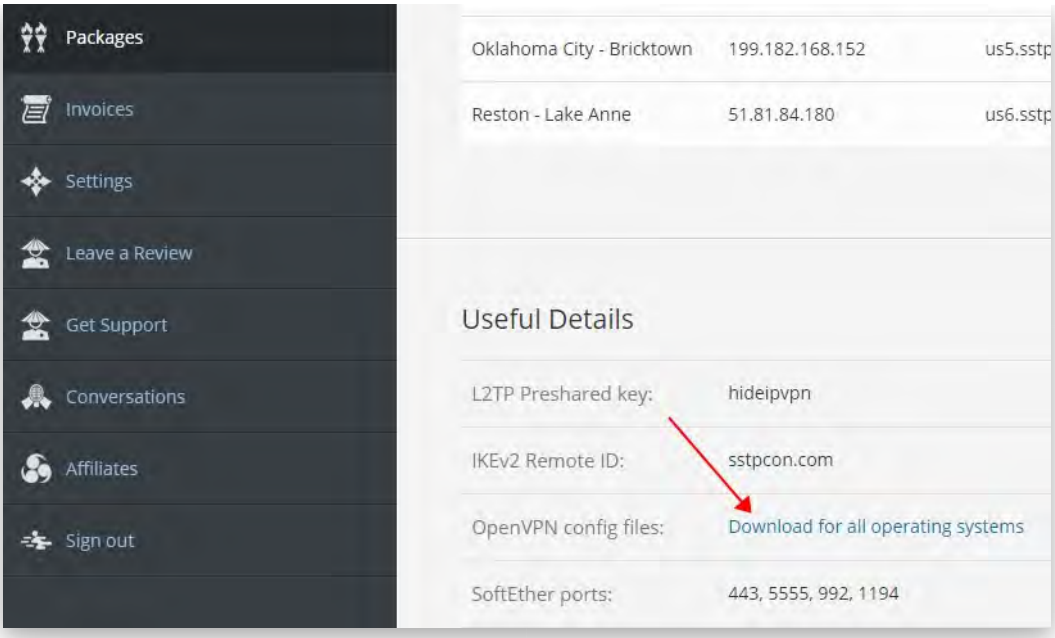
1. Login your HideIPVPN account.
2. Go to Package on the left side, click the your package, make sure it is active.



3. On the VPN tab, there is VPN Login Details of username and password, this is for login when OpenVPN connection



4. Scroll down to download OpenVPN config files.



Hide.me VPN

Hide.me VPN

Official Website

1. Login your Hide.me account, find the Server Locations on the left side.
2. Download the OpenVPN Configuration for Windows.



Hotspot Shield

Hotspot Shield

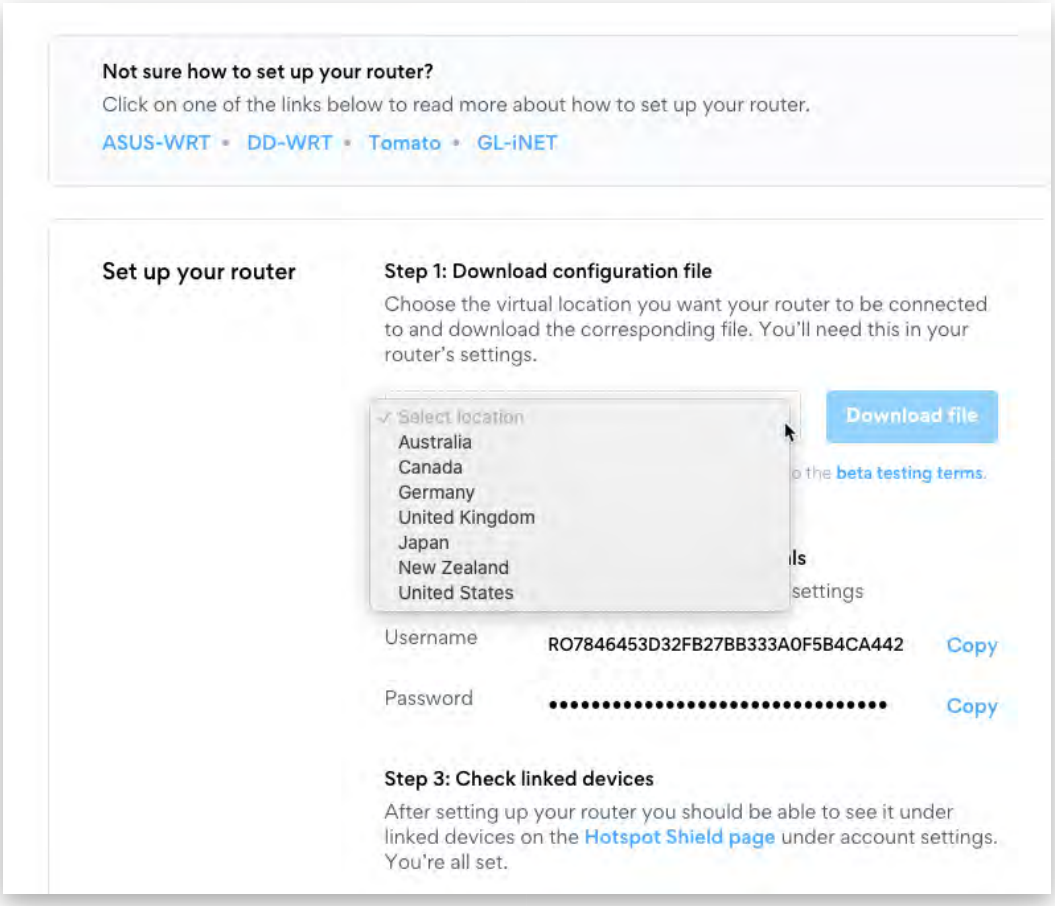
Official Website

1. Go to https://www.hotspotshield.com/ and click on Account. Sign in if you're asked.



2. Go to https://app.hotspotshield.com/app/hotspotshield/router

   Go to the Select location dropdown and pick the virtual location that the router will use. Now click on "Download file". The configuration file (config.ovpn) will be downloaded to your computer. The username and password will need to be entered when you set up the OpenVPN client on the router.



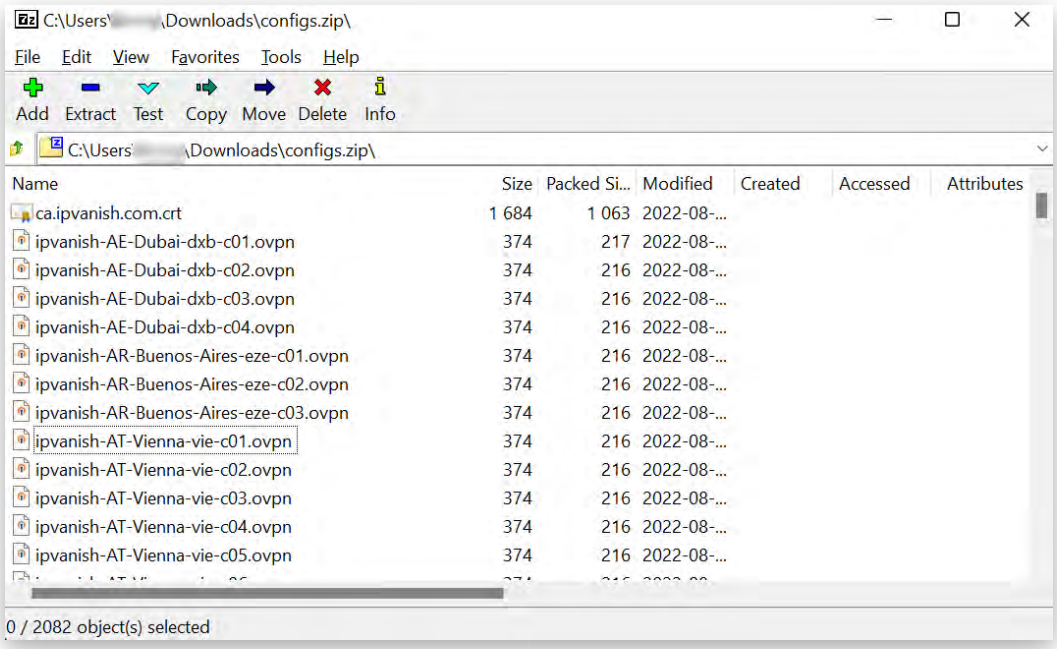
Refer link

IPVANISH

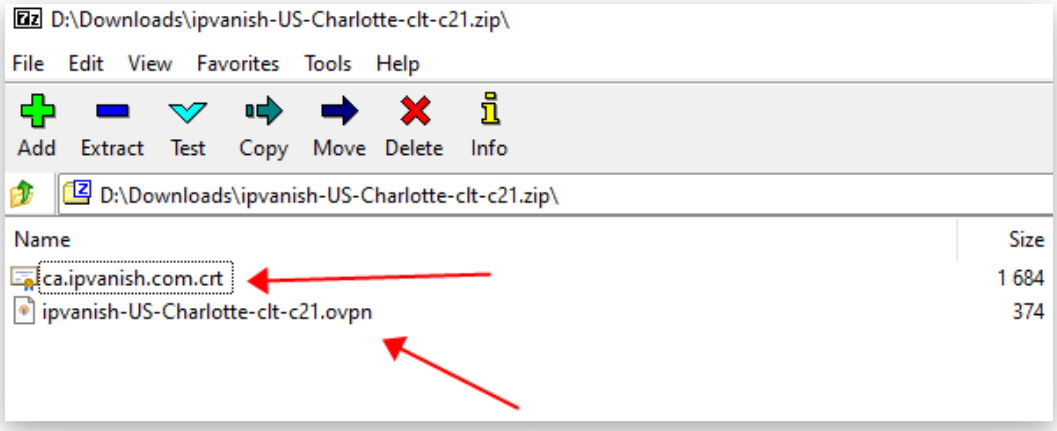
IPVANISH

Official Website

- You can download all of the config files for all of the servers from here, it contain all the server config file(.ovpn) and a certificate file(.crt). The .zip file maybe a little big for some models, please delete the configuration(.ovpn) of the server that you will not use.



- You can also download individual server configuration files here, but you will need to download **ca.ipvanish.com.crt** as well. Before uploading to the router, you need to compress the **ca.ipvanish.com.crt** and .ovpn configuration files into a .zip archive.



Refer link

IVACY

IVACY

Official Website

Download OpenVPN UDP Configs

Download OpenVPN TCP Configs

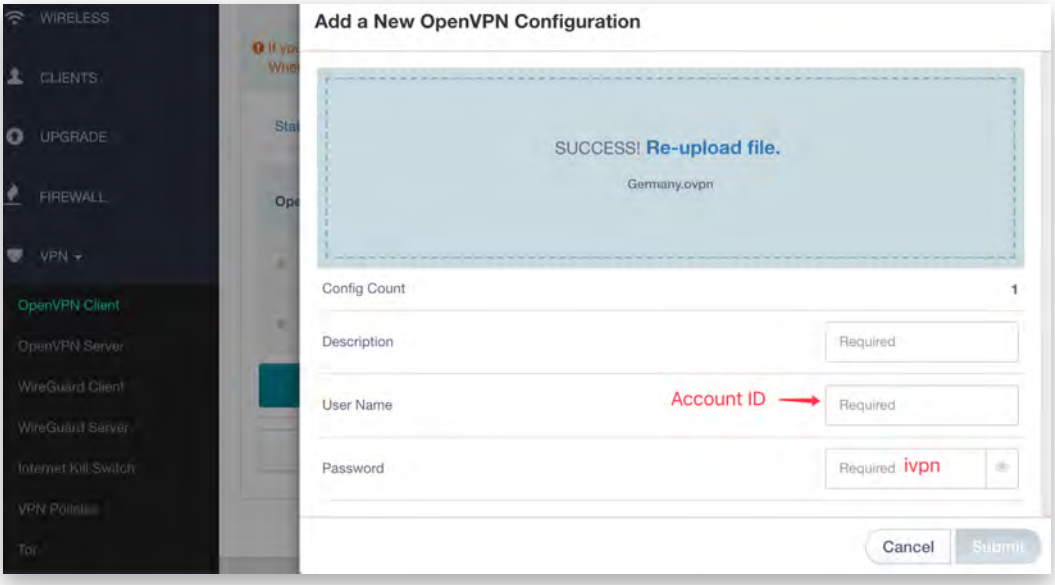
Refer link

IVPN

IVPN

Official Website

1. Download the OpenVPN config files.
2. Find the Account ID on IVPN Client Area.
3. When drag the config file to Add a New OpenVPN Configuration, you will be asked to enter User Name and Password. The User Name is your Account ID that begins with letters **ivpn**. The password can be anything, like **ivpn**



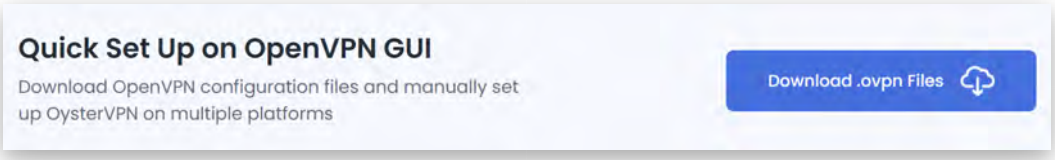
Refer link

OysterVPN

OysterVPN

Official Website

1. Access the OysterVPN server list page, click **Download .ovpn file** to download the configuration file.



2. The username and password for OpenVPN connection are the same as the one you use to login OysterVPN.

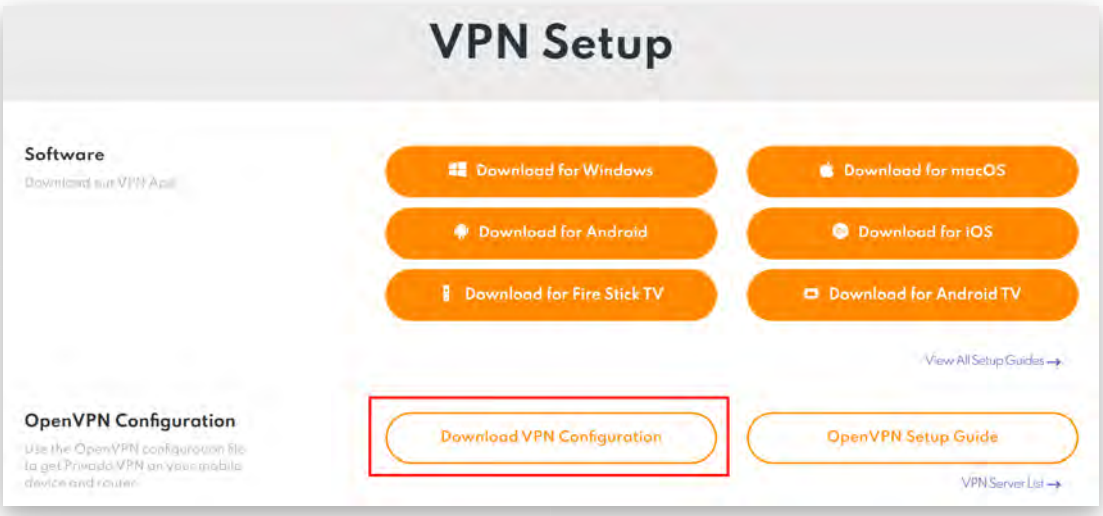
Tips: if the zip file is too big to upload, you can delete some .ovpn in .zip file or upload single .ovpn file.

PrivadoVPN

PrivadoVPN

Official Website

Just login, then you can easily find the **Download VPN Configuration**.



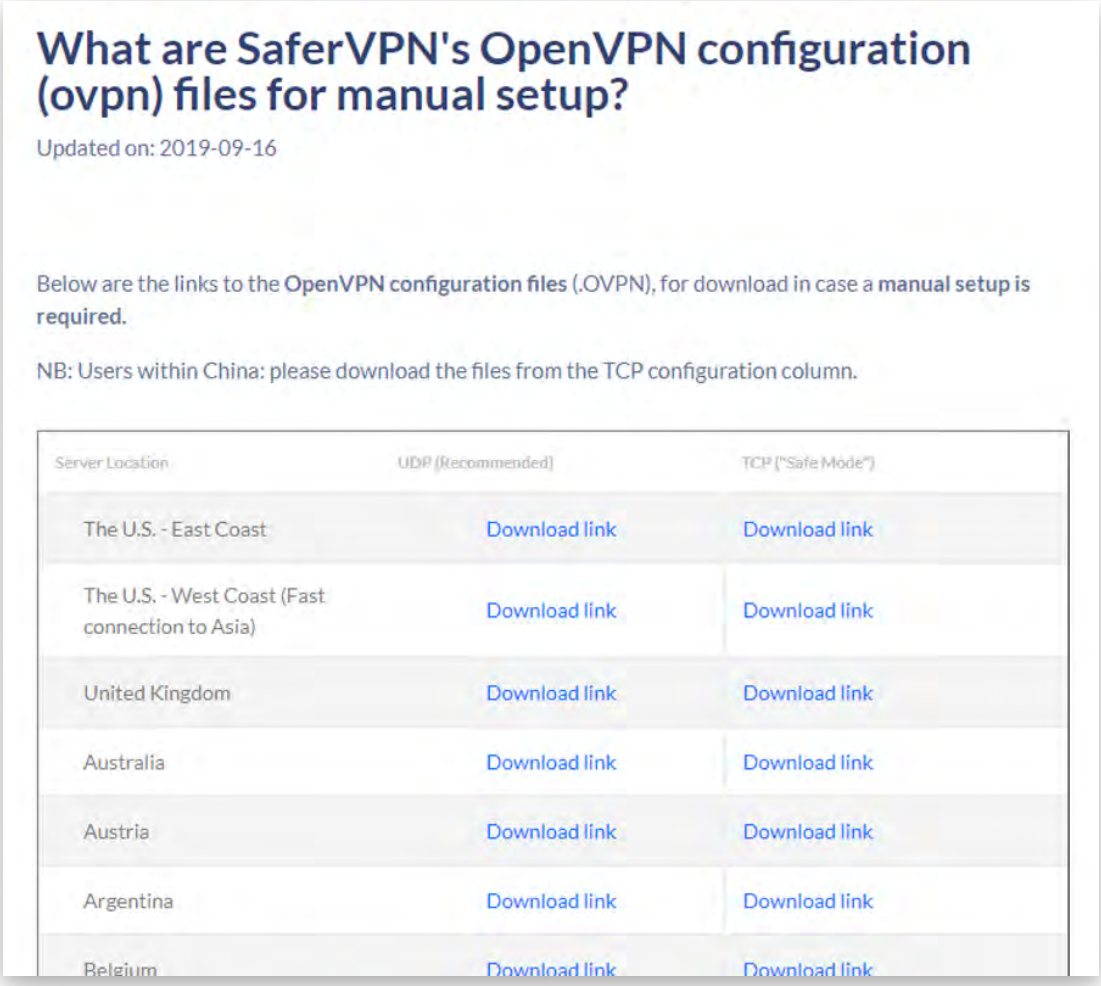
Tips: if the zip file is too big to upload, you can delete some .ovpn in .zip file or upload single .ovpn file.

SaferVPN

SaferVPN

Official Website

Download directly.



What are SaferVPN's OpenVPN configuration (ovpn) files for manual setup?

Updated on: 2019-09-16

Below are the links to the **OpenVPN configuration files** (.OVPN), for download in case a **manual setup is required.**

NB: Users within China: please download the files from the TCP configuration column.

Server Location	UDP (Recommended)	TCP ("Safe Mode")
The U.S. - East Coast	Download link	Download link
The U.S. - West Coast (Fast connection to Asia)	Download link	Download link
United Kingdom	Download link	Download link
Australia	Download link	Download link
Austria	Download link	Download link
Argentina	Download link	Download link
Belgium	Download link	Download link

StreamVPN

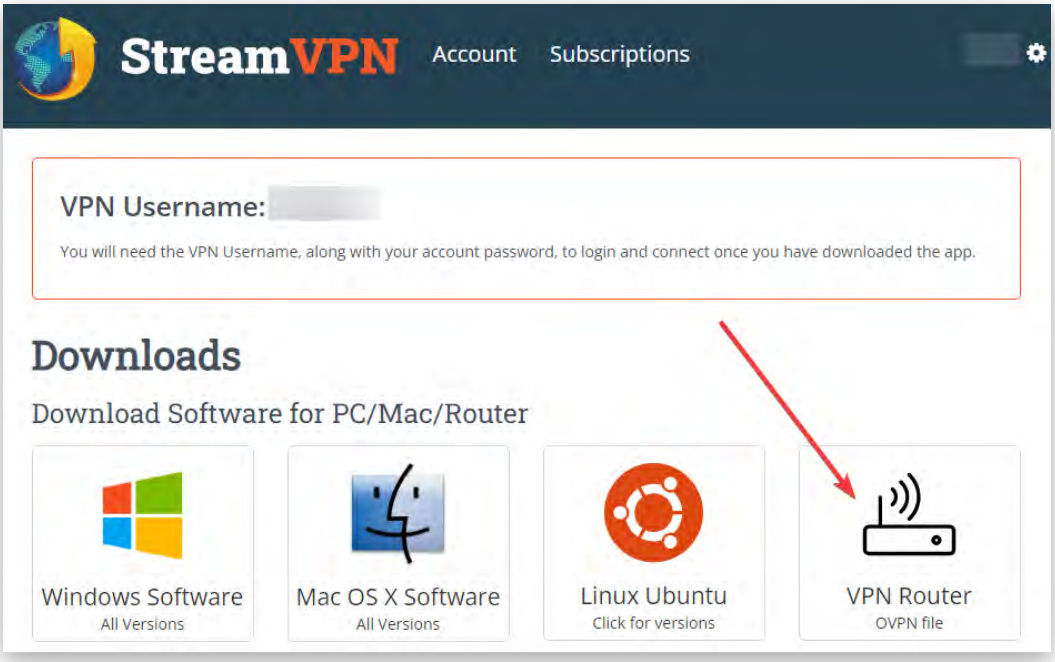
StreamVPN

Official Website

1. Login with your StreamVPN account and then you will be able to see your subscription information. Click **Install & Guides**.



2. Click **VPN Router**, it will download a .zip archive file called `StreamVPN.zip` .



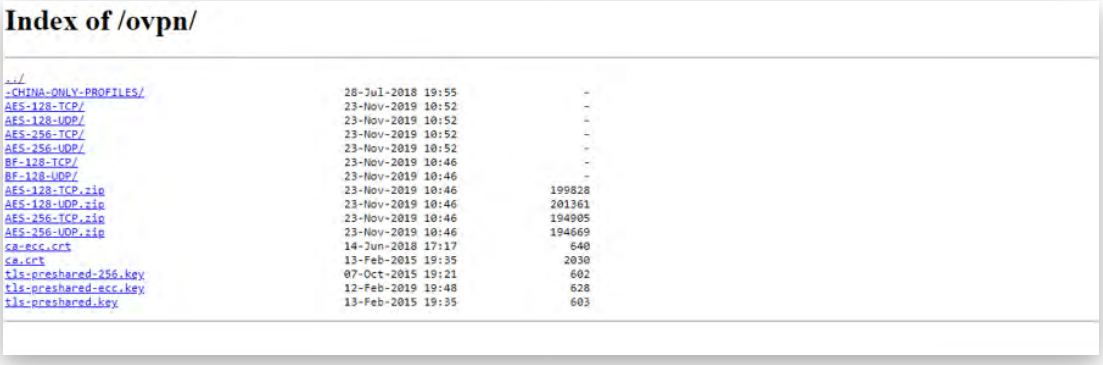
Note: Only the configuration file name contains "Primary" work.

VPN.AC

VPN.AC

Official Website

Download.



Index of /ovpn/

../		
-CHINA-ONLY-PROFILES/	28-Jul-2018 19:55	-
AES-128-TCP/	23-Nov-2019 10:52	-
AES-128-UDP/	23-Nov-2019 10:52	-
AES-256-TCP/	23-Nov-2019 10:52	-
AES-256-UDP/	23-Nov-2019 10:52	-
BF-128-TCP/	23-Nov-2019 10:46	-
BF-128-UDP/	23-Nov-2019 10:46	-
AES-128-TCP.zip	23-Nov-2019 10:46	199828
AES-128-UDP.zip	23-Nov-2019 10:46	201361
AES-256-TCP.zip	23-Nov-2019 10:46	194905
AES-256-UDP.zip	23-Nov-2019 10:46	194669
ca-ecc.crt	14-Jun-2018 17:17	640
ca.crt	13-Feb-2015 19:35	2030
tls-preshared-256.key	07-Oct-2015 19:21	602
tls-preshared-ecc.key	12-Feb-2019 19:48	628
tls-preshared.key	13-Feb-2015 19:35	603

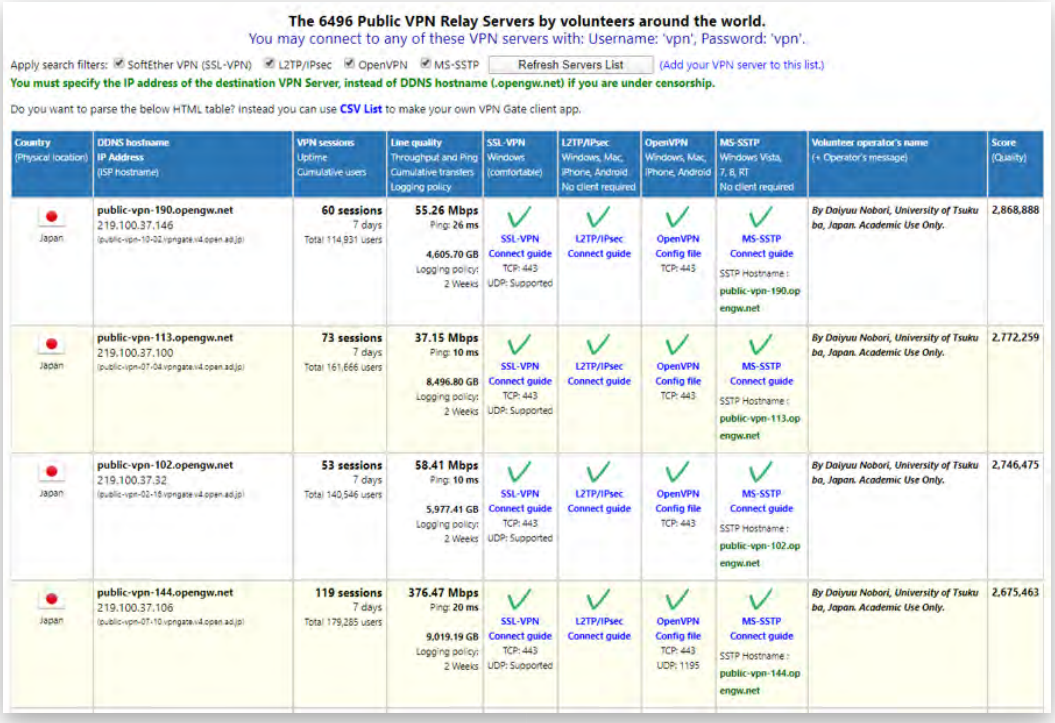
VPNGate

VPNGate

Official Website

The OpenVPN configuration files are listed on the VPN Gate website according to the server location.

1. Click OpenVPN Config file under the column **OpenVPN**.



The 6496 Public VPN Relay Servers by volunteers around the world.
You may connect to any of these VPN servers with: Username: 'vpn', Password: 'vpn'.

Apply search filters: SoftEther VPN (SSL-VPN) L2TP/IPsec OpenVPN MS-SSTP Refresh Servers List (Add your VPN server to this list.)

You must specify the IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are under censorship.

Do you want to parse the below HTML table? Instead you can use **CSV List** to make your own VPN Gate client app.

Country (Physical location)	DDNS hostname / IP Address (ISP hostname)	VPN sessions / Uptime / Cumulative users	Line quality / Throughput and Ping / Cumulative transfers / Logging policy	SSL-VPN Windows (comfortable)	L2TP/IPsec Windows, Mac, iPhone, Android No client required	OpenVPN Windows, Mac, iPhone, Android	MS-SSTP Windows Vista, 7, 8, RT No client required	Volunteer operator's name (+ Operator's message)	Score (Quality)
Japan	**public-vpn-190.opengw.net** 219.100.37.146	**60 sessions** 7 days Total 114,931 users	**55.26 Mbps** Ping: **26 ms** **4,605.70 GB** Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443	MS-SSTP Connect guide SSTP Hostname : public-vpn-190.opengw.net	*By Daiyuu Nobori, University of Tsukuba, Japan. Academic Use Only.*	2,868,888
Japan	**public-vpn-113.opengw.net** 219.100.37.100	**73 sessions** 7 days Total 161,666 users	**37.15 Mbps** Ping: **10 ms** **8,496.80 GB** Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443	MS-SSTP Connect guide SSTP Hostname : public-vpn-113.opengw.net	*By Daiyuu Nobori, University of Tsukuba, Japan. Academic Use Only.*	2,772,259
Japan	**public-vpn-102.opengw.net** 219.100.37.32	**53 sessions** 7 days Total 140,546 users	**58.41 Mbps** Ping: **10 ms** **5,977.41 GB** Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443	MS-SSTP Connect guide SSTP Hostname : public-vpn-102.opengw.net	*By Daiyuu Nobori, University of Tsukuba, Japan. Academic Use Only.*	2,746,475
Japan	**public-vpn-144.opengw.net** 219.100.37.106	**119 sessions** 7 days Total 179,285 users	**376.47 Mbps** Ping: **20 ms** **9,019.19 GB** Logging policy: 2 Weeks	SSL-VPN Connect guide TCP: 443 UDP: Supported	L2TP/IPsec Connect guide	OpenVPN Config file TCP: 443 UDP: 1195	MS-SSTP Connect guide SSTP Hostname : public-vpn-144.opengw.net	*By Daiyuu Nobori, University of Tsukuba, Japan. Academic Use Only.*	2,675,463

2. You will see the download page.


Download the OpenVPN Configuration File (.ovpn file)
You can download the .ovpn file to connect this OpenVPN server.
Use one of the following .ovpn files. Refer the Hint to choose one.
You must specify IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are in a big-brother country.
How to Install and Set up the OpenVPN Client
The .ovpn file which is including DDNS hostname
Destination DDNS Hostname: public-vpn-190.opengw.net
OpenVPN Configuration File: public-vpn-190.opengw.net (TCP 443)
OpenVPN
You must specify IP address of the destination VPN Server, instead of DDNS hostname (.opengw.net) if you are in a big-brother country.
The .ovpn file which is including IP address
Destination IP Address: 219.100.37.146
OpenVPN Configuration File: 219.100.37.146 (TCP 443)
OpenVPN

VPN Unlimited(KeepSolid)

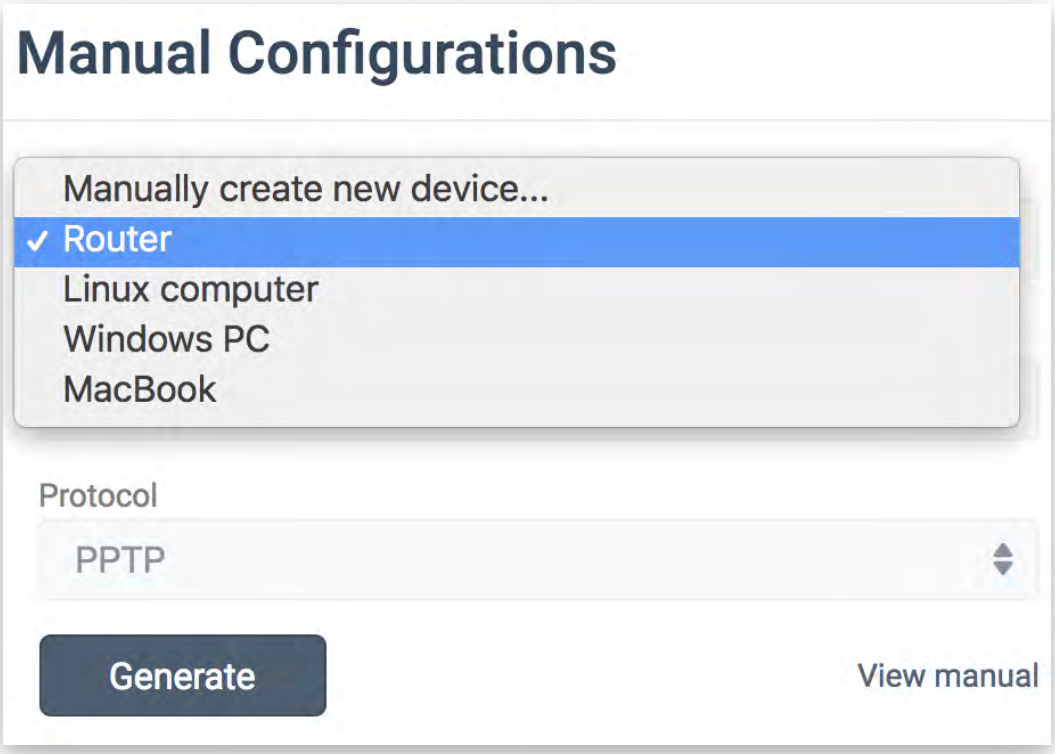
VPN Unlimited(KeepSolid)

Information quoted from VPN unlimited official instruction

Start out by logging in to your User Office, press Manage for the VPN Unlimited service, and follow a few simple steps:

1. Select a device

   Pick a device from the list or create a new one. If you are out of free slots, delete an old device or buy extra slots.

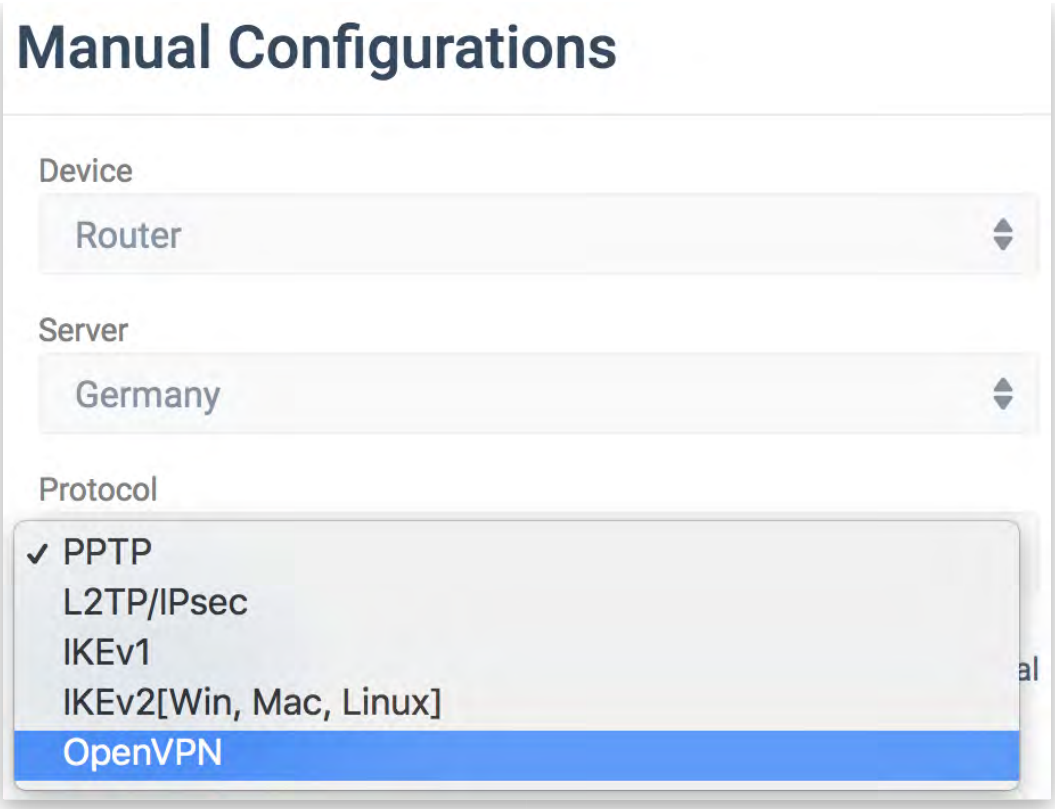


2. Choose the desired server location

   VPN Unlimited offers a large variety of servers, namely 400+ in 70+ locations. In this case, let it be Germany.

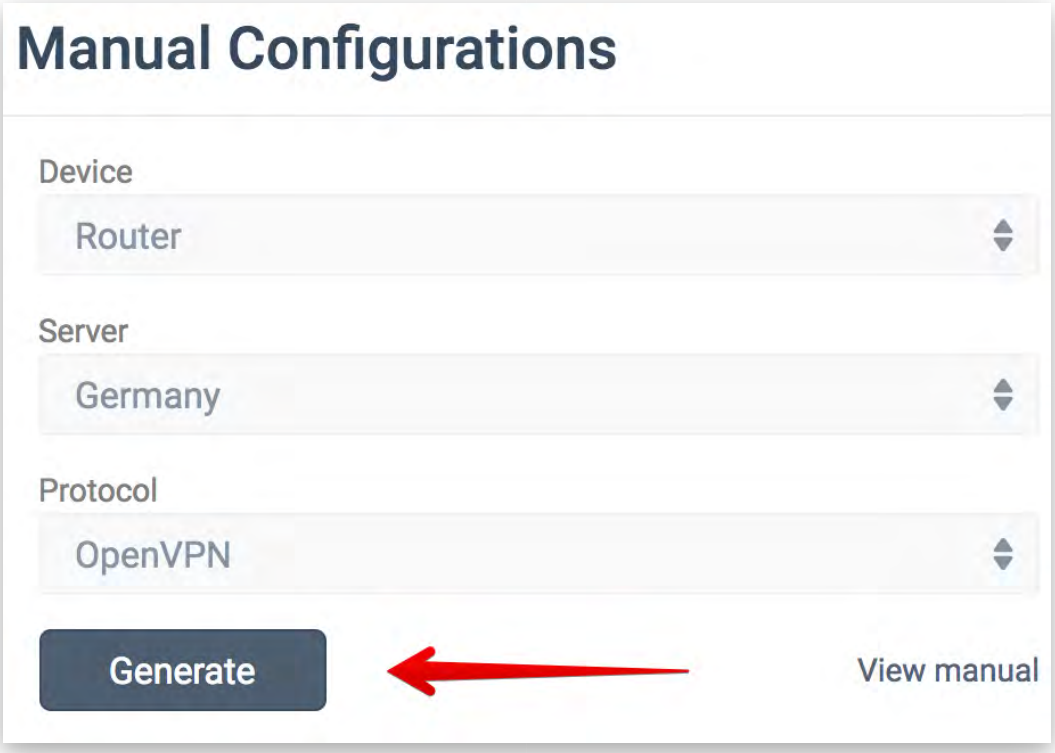
3. Select the VPN protocol

   selece OpenVPN protocol.



4. Create a configuration

   Press Generate and you will get all the data required to set up a VPN connection.



VyprVPN

VyprVPN

VyprVPN offers the OpenVPN files here: Where can I find the OpenVPN files? – VyprVPN Support

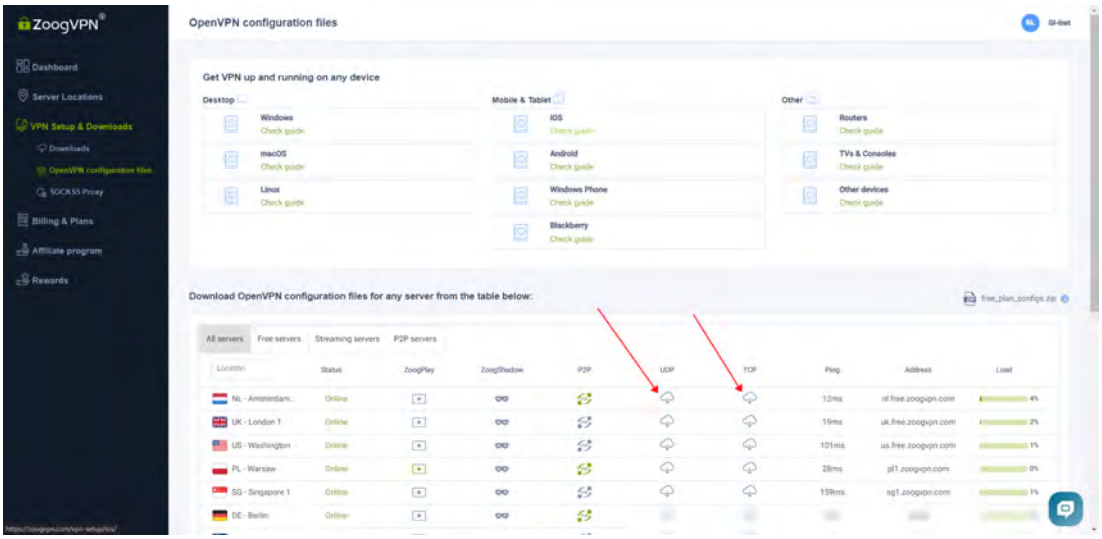
The provided zip file contains two folders with the .ovpn files. One called OpenVPN160 one OpenVPN256. Just delete the OpenVPN160 folder from the zip file then upload it to GL.iNet router as usual.

ZoogVPN

ZoogVPN

Official Website

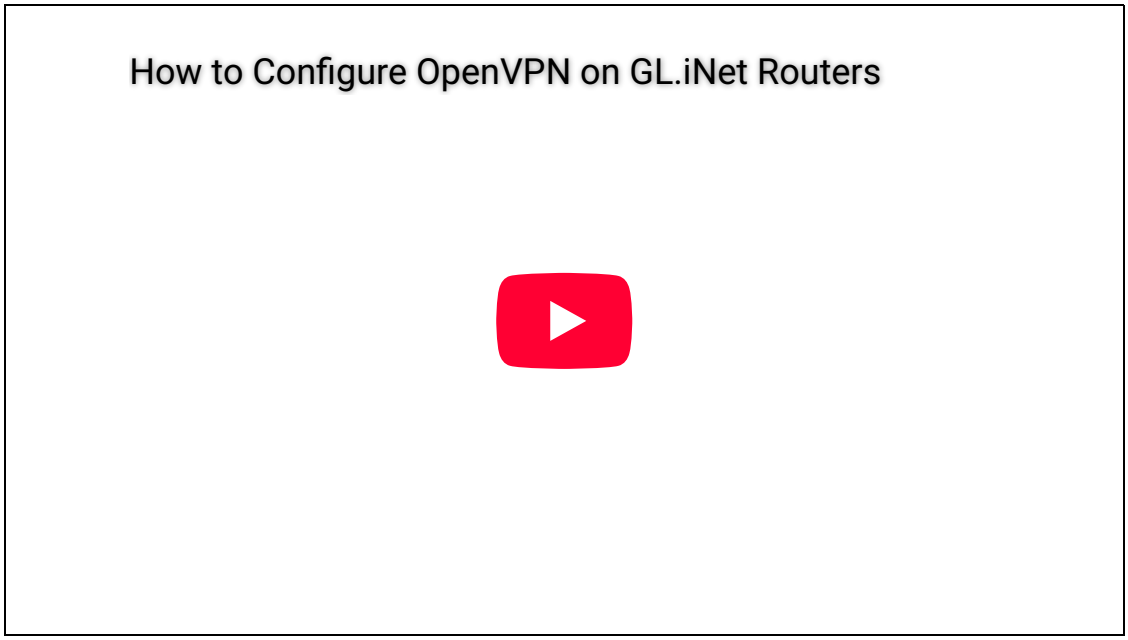
Sign in its official website, then access the OpenVPN configuration files page, you will find all the servers here. Download the configuration file in the TCP column or UDP column.



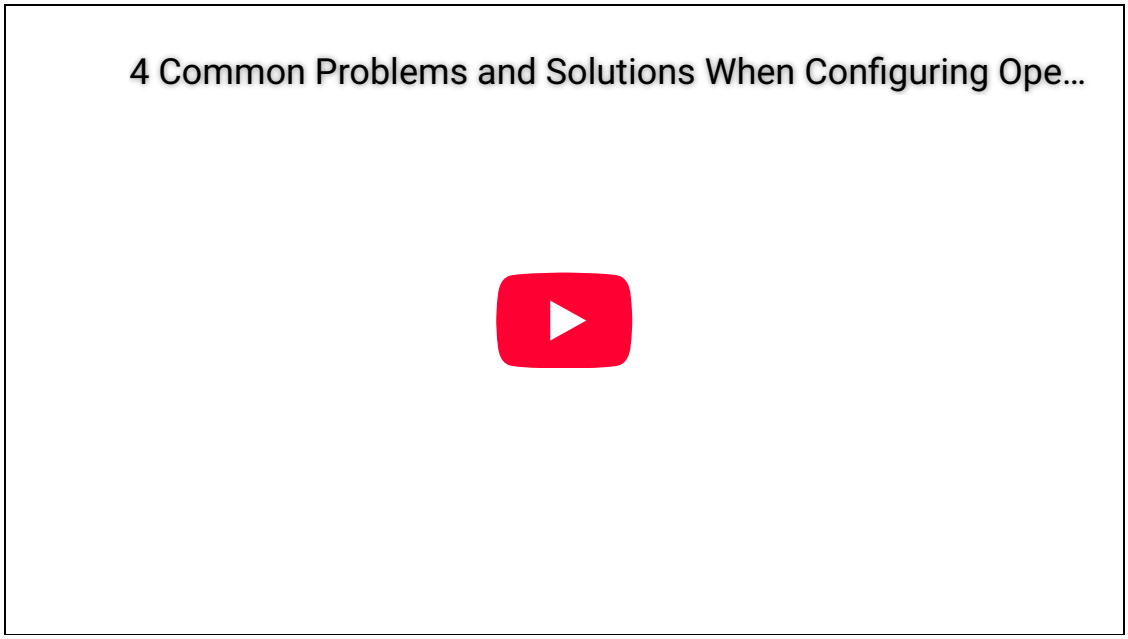
Then follow the guide to setup OpenVPN Client on GL.iNet router, the username and password are the same as the ones used to log into ZoogVPN website.

Video tutorial

These video tutorial as ExpressVPN as example to setup OpenVPN Client.



4 Common Problems and Solution When Configuring OpenVPN



Configuration du serveur OpenVPN sur routeur GL.iNet

OpenVPN est un protocole VPN open source qui utilise des techniques de réseau privé virtuel (VPN) pour établir des connexions sécurisées de site à site ou de point à point.

Les routeurs GL.iNet ont pré-installé OpenVPN Client and Server.

Nous recommandons WireGuard sur OpenVPN parce qu'il est beaucoup plus rapide. Pour la configuration d'un serveur WireGuard, veuillez consulter ici.

S'assurer que le fournisseur de services Internet vous attribue une adresse IP publique

Veuillez vérifier si vous informez vous un fournisseur de services Internet vous attribue une adresse IP publique ici.

Sinon, vous ne pouvez pas vous connecter au serveur OpenVPN.

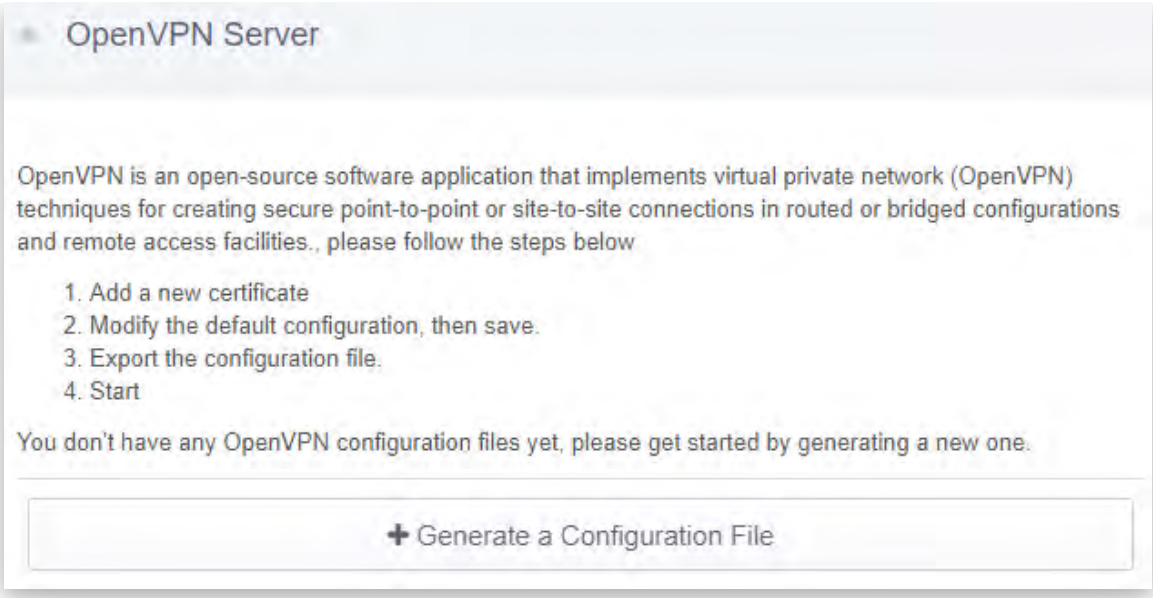
Une autre méthode est d'utiliser une solution proxy inverse, nous suggérons AstroRelay, vérifiez le tutoriel ici.

Topologie du réseau

- Si le routeur GL.iNet est le routeur principal de votre réseau, c'est simple, s'il vous plaît passer à l'étape suivante.
- Si vous avez déjà un routeur principal, alors le routeur GL.iNet est sous le routeur principal, vous pouvez avoir besoin de configurer un port en avant sur le routeur principal.
- Si vous avez déjà un routeur principal, le routeur GL.iNet est à plusieurs niveaux en dessous et vous devez mettre en place un port en avant à chaque niveau.

Initialiser OpenVPN Server

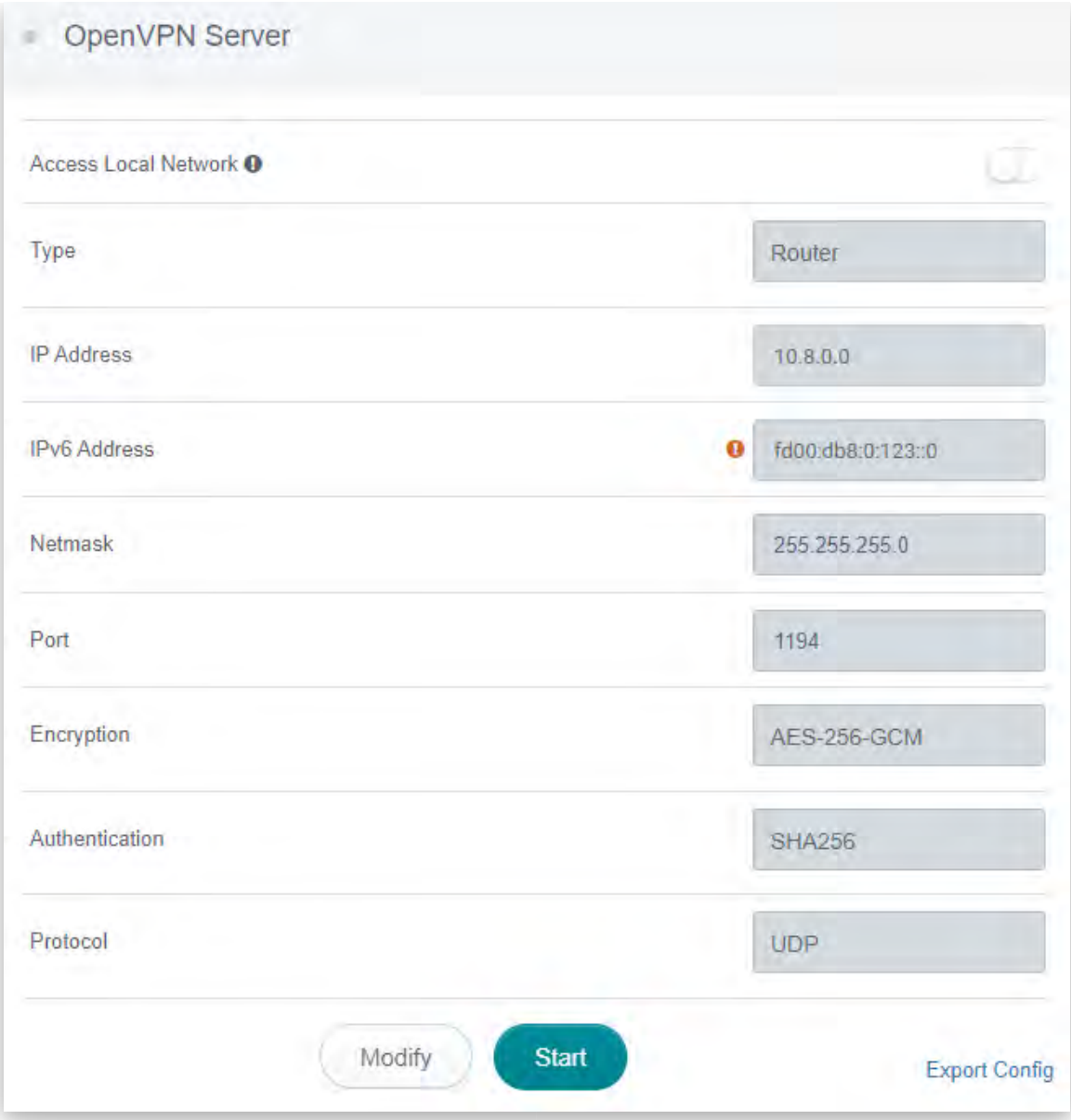
Accès au panneau d'administration web, sur le côté gauche, VPN -, OpenVPN Server. Cliquez sur `Generate a Configuration File`.



Configuration Serveur OpenVPN

Configuration du serveur

Il existe des configurations de serveurs OpenVPN prédéfinies. Vous pouvez aussi cliquer `Modify` les modifier manuellement. Cliquez sur `Apply` quand tu auras fini.

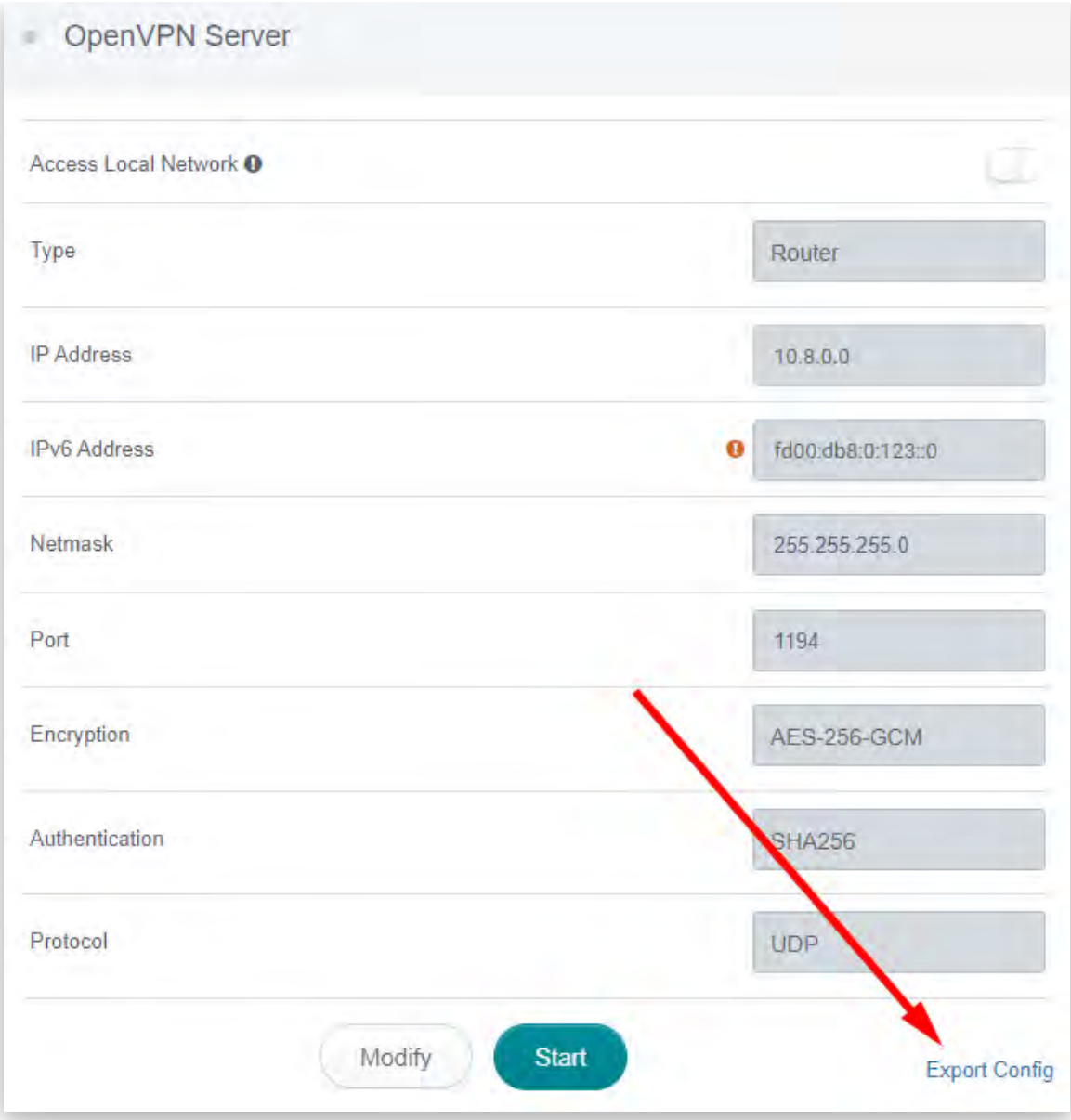


Autoriser le réseau local Access: activerez que tous les clients qui se connectent à ce serveur OpenVPN puissent accéder à votre réseau local. Veuillez utiliser avec prudence.

Notez que vous ne pouvez pas exécuter VPN Client and Server en même temps, et que vous ne pouvez pas non plus exécuter OpenVPN Client et WireGuard Client en même temps.

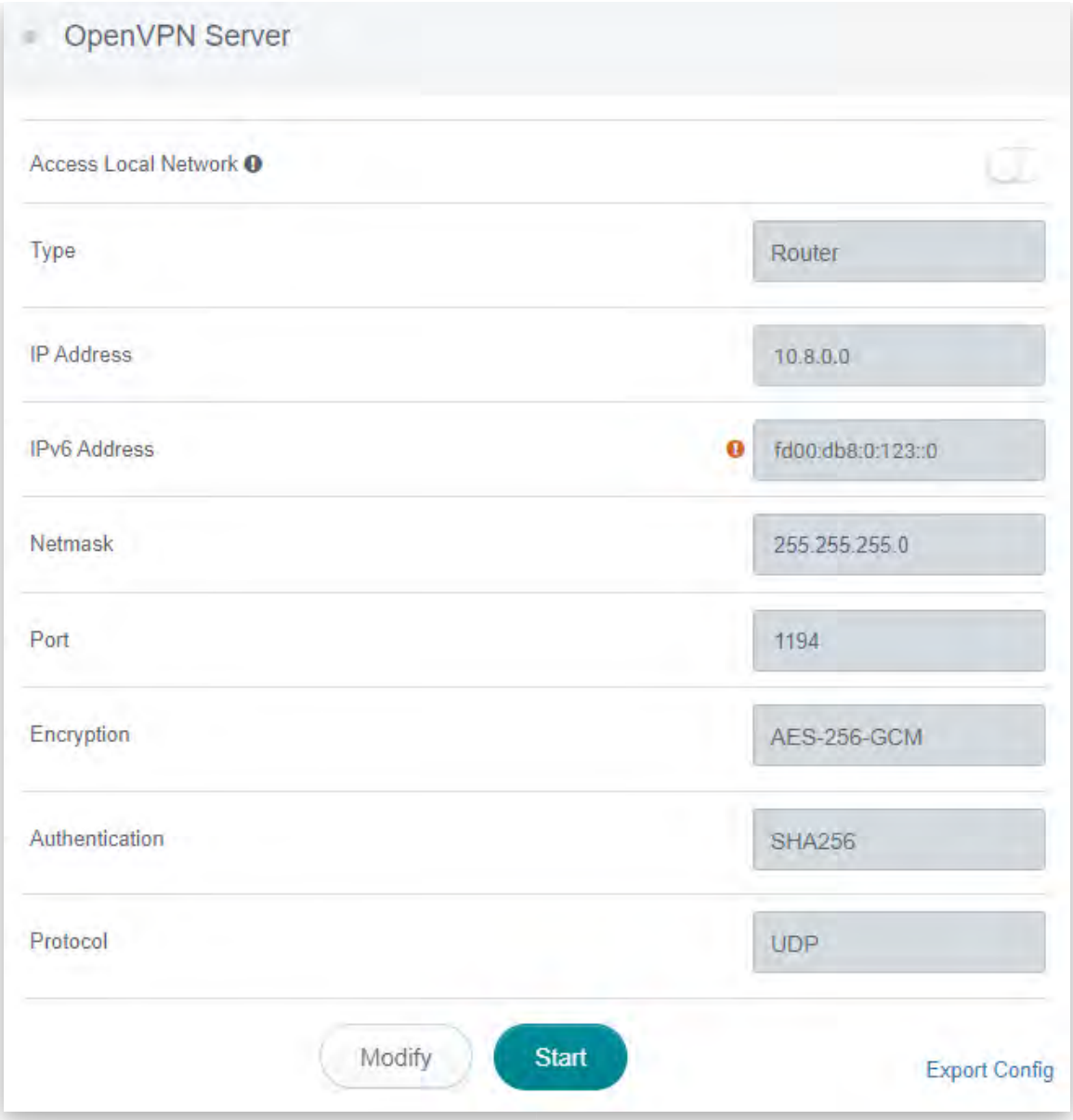
Exportation du fichier de configuration OpenVPN

Cliquez sur `Export Config` en bas à droite pour télécharger le fichier de configuration OpenVPN.

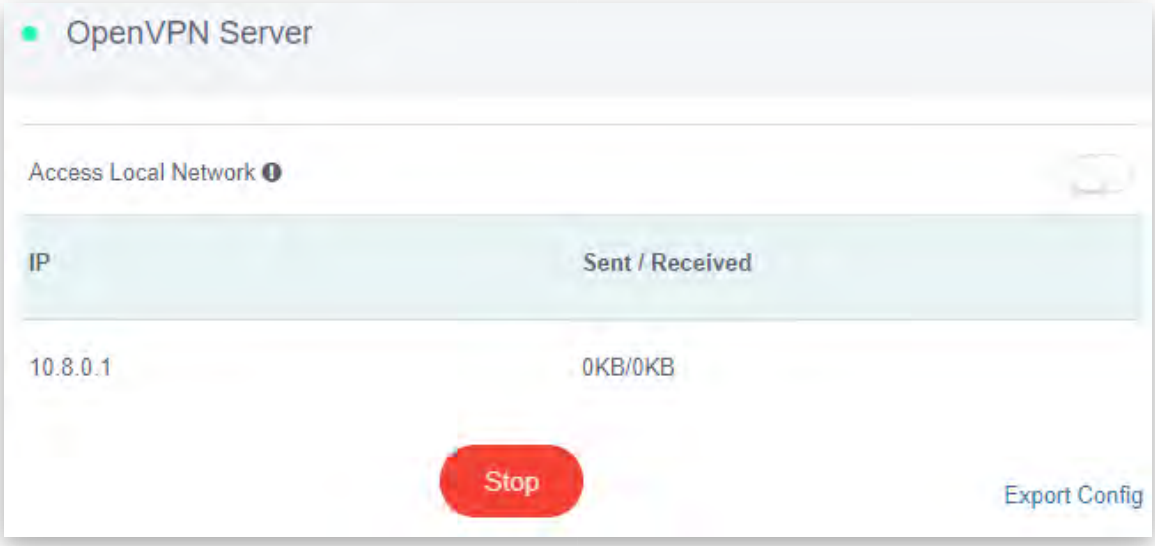


Démarrer le serveur OpenVPN

Cliquez sur `Start` pour démarrer votre serveur OpenVPN. Sinon, vous ne pourrez pas vous connecter au serveur OpenVPN en utilisant son fichier de configuration.



Cela a commencé.



Pour vérifier si OpenVPN Server fonctionne correctement

Pour vérifier si OpenVPN Server fonctionne correctement, nous pouvons utiliser un autre appareil connecté à un autre réseau et utiliser la configuration OpenVPN que nous avons exportée plus tôt pour nous connecter et voir s'il se connecte correctement et si l'adresse IP est l'IP du serveur OpenVPN.

Le moyen le plus simple est d'utiliser un téléphone portable avec l'application cliente officielle OpenVPN installée, d'éteindre sa connexion Wi-Fi et de se connecter uniquement à Internet via 3G/4G/5G. Ouvrez ensuite l'application OpenVPN, importez la configuration OpenVPN que nous avons précédemment exporté. Activez la connexion, vérifiez si le téléphone a accès à Internet et si son adresse IP est l'IP de votre serveur OpenVPN.

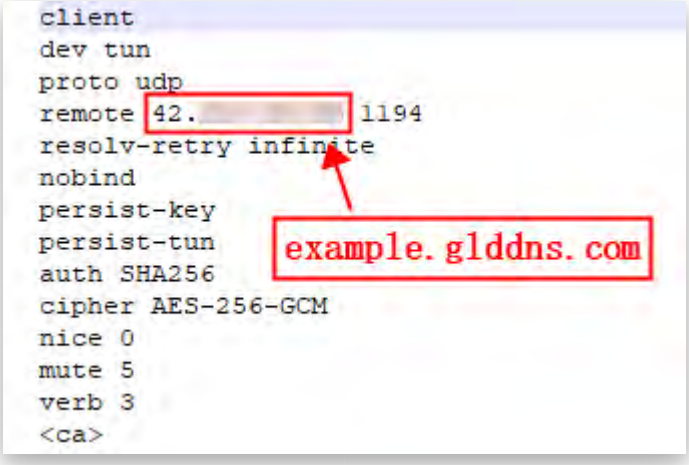
Il existe plusieurs raisons courantes pour lesquelles il n'a pas étéinfraction :

- Le fournisseur de services Internet ne vous attribue pas d'adresse IP publique, veuillez vérifier ici.
- Vous pourriez avoir besoin d'un transfert de port de configuration, veuillez vérifier ici.
- Le port que vous utilisez pour OpenVPN Server est bloqué par le fournisseur de services Internet, le passage à un autre port ou le contact avec le fournisseur de services Internet.
- Certains pays/régions peuvent bloquer la connexion VPN.

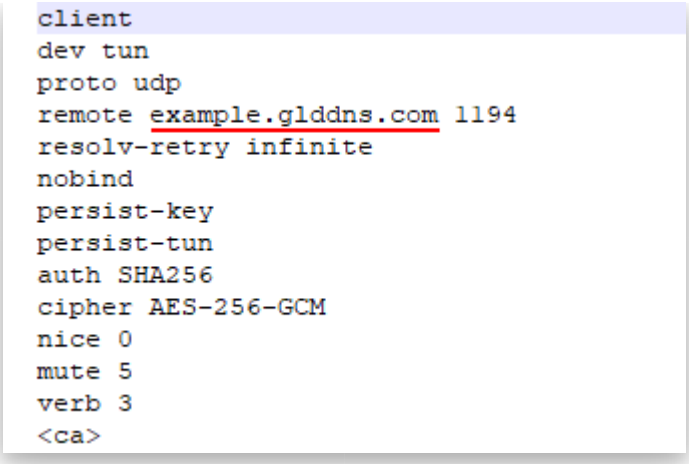
Si votre adresse IP publique est dynamique

Certains fournisseurs de services Internet peuvent parfois changer d'adresse IP. Pour surmonter cela, activez le DDNS, puis éditez la configuration pour remplacer DDNS url par votre adresse IP publique.

1. Ouvrez le fichier de configuration (.ovpn) avec un éditeur de texte (par ex. Atome, sublime).
2. Éditez la configuration pour remplacer DDNS url par votre adresse IP publique.



Après remplacement.



3. Sauver le `.ovpn` Fichier.

La connexion OpenVPN peut diminuer un certain temps lorsque l'adresse IP publique change, après la mise à jour de l'URl DDNS à la nouvelle adresse IP publique, le conneciton reprendra. Le DDNS est mis à jour toutes les 10 minutes. Si la connexion ne reprend pas, assurez-vous que l'url DDNS est pointé pour tinter new public, puis désactivez la connexion OpenVPN et allumez-vous.

OpenVPN Client App

We can use another GL.iNet router as OpenVPN Client, or use their official app on other devices with various OS.

- Please refer to OpenVPN Official Website: https://openvpn.net/vpn-client/

Configuration WireGuard sur le routeur GL.iNet

WireGuard est un VPN extrêmement simple mais rapide et moderne qui utilise **une cryptographie de pointe**. Il vise à être plus rapide, plus simple, plus mince et plus utile que l'IPSec, tout en évitant les maux de tête massifs. Il a l'intention d'être beaucoup plus performant qu'OpenVPN.

Les routeurs GL.iNet ont pré-installé WireGuard Client and Server.

Si vous avez déjà acheté le service WireGuard auprès d'un fournisseur, mais que vous ne savez pas comment obtenir les fichiers de configuration, veuillez vous référer pour obtenir des fichiers de configuration auprès des fournisseurs de services WireGuard ou demander son support.

Vous pouvez configurer WireGuard Client via le panneau d'administration web et l'application mobile. Pour l'application mobile, il a déjà intégré certains fournisseurs de services WireGuard, ils sont AzireVPN, Mullvad VPN, OVPN, StrongVPN, PIA VPN, SpiderVPN.

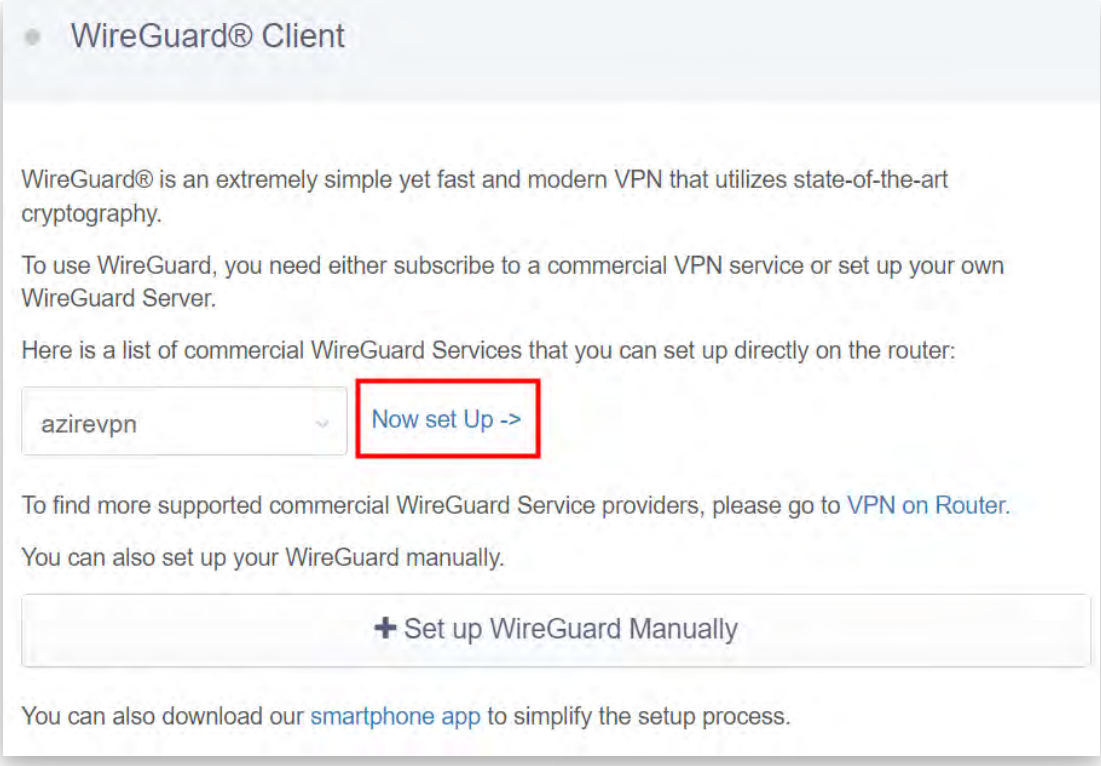
Pour être configuré via Web Admin Panel, veuillez suivre le guide ci-dessous.

Configuration AzireVPN

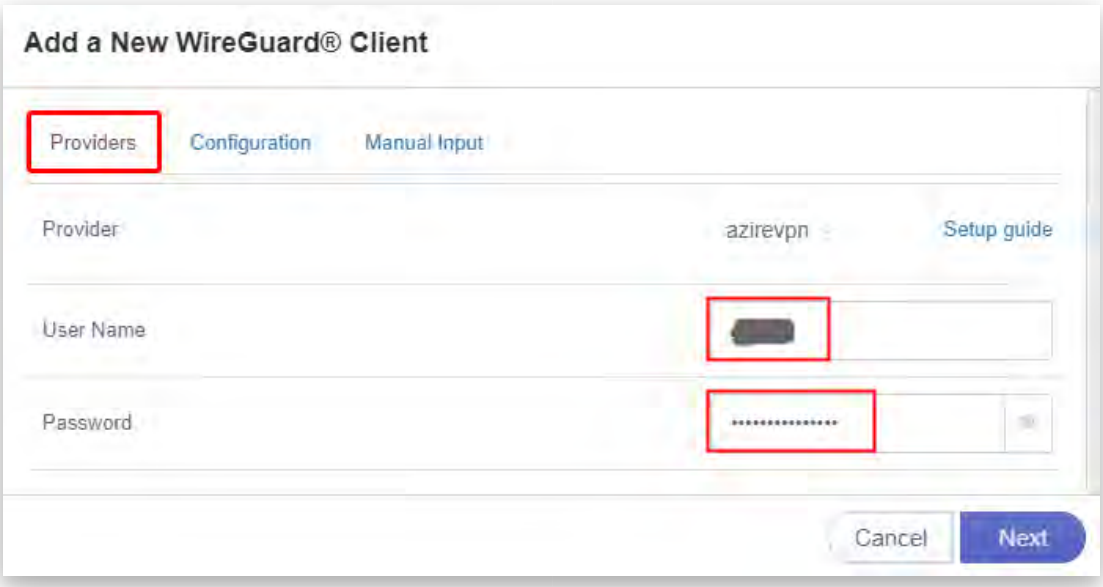
AzireVPN est un service VPN à l'esprit de la vie privée qui fournit des tunnels sûrs, modernes et robustes tels que WireGuard.

Le micrologiciel 3.x a intégré le service AzireVPN WireGuard.

1. Cliquez sur **maintenant configurer**.



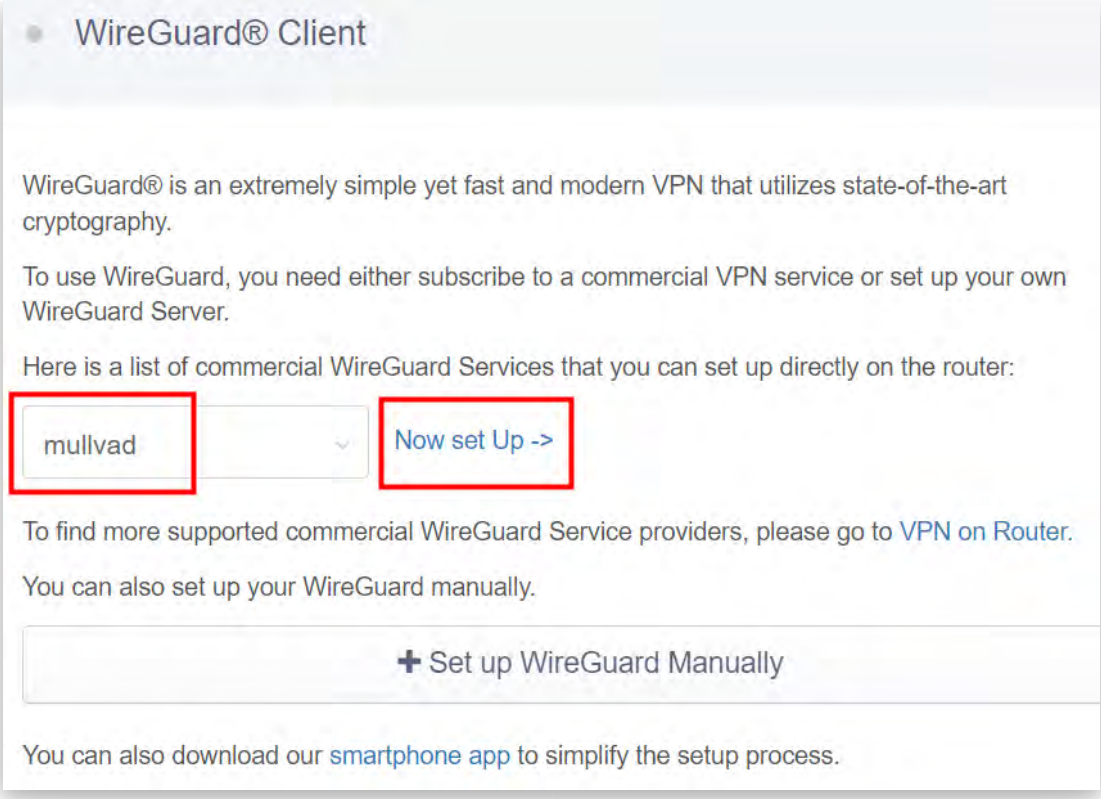
2. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Suivant**.



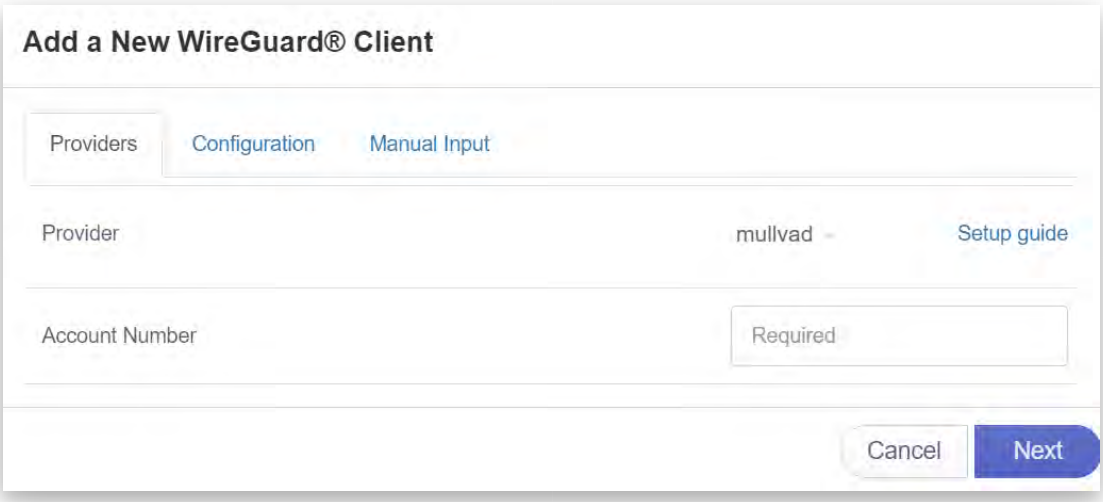
Il faudra plusieurs minutes pour obtenir des configurations, s'il vous plaît soyez patient.

Configuration Mullvad

1. Sélectionnez en tant que **mullvad** puis cliquez sur **"Simplifier" Set**.



2. Saisissez le **numéro** de **compte**, puis cliquez sur **Suivant**.

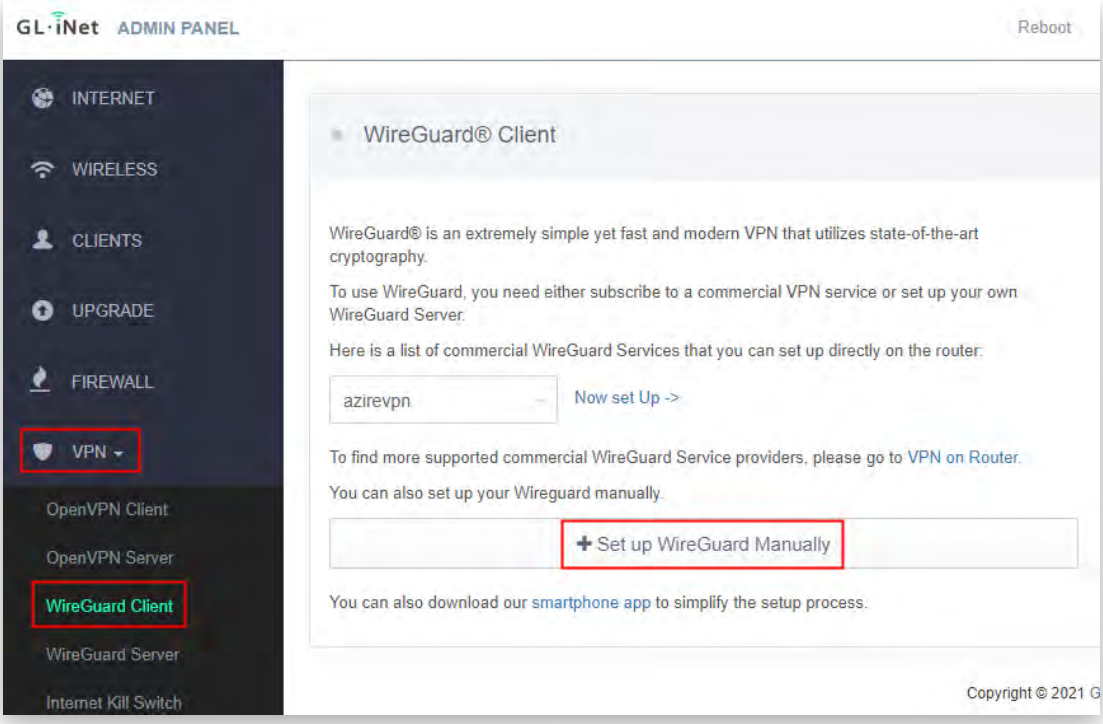


Cela prendra un peu plus de temps, s'il vous plaît soyez patient.

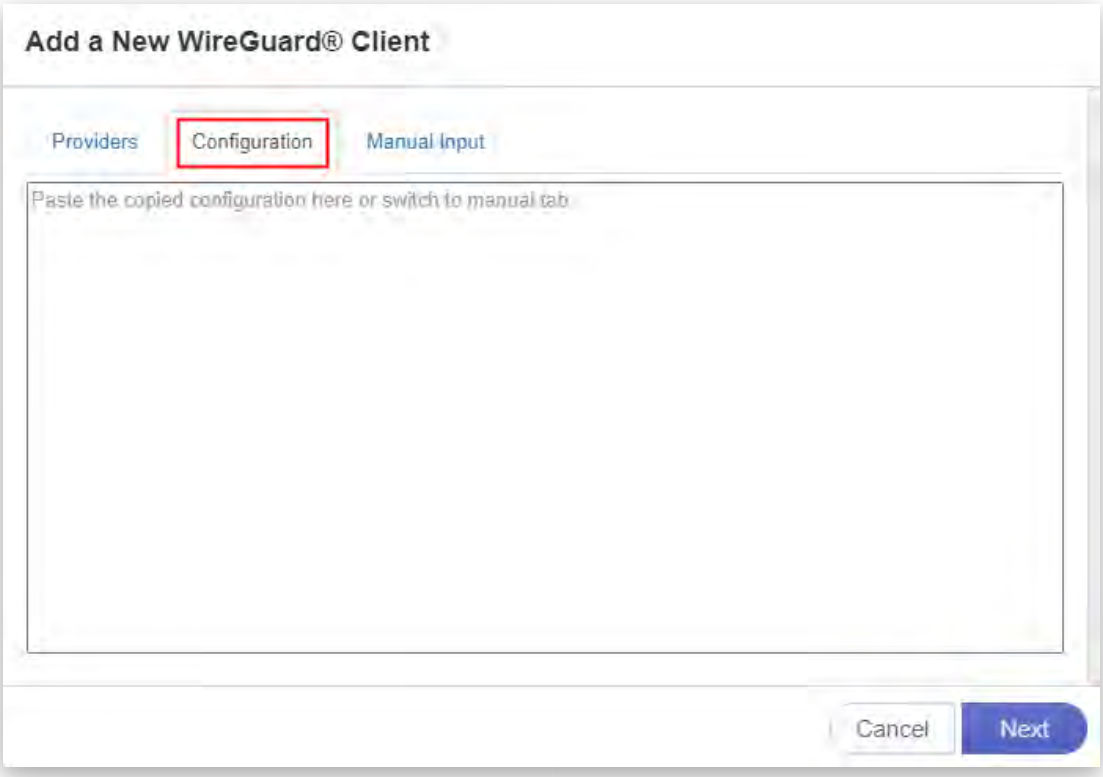
Client WireGuard de configuration

Il y a un tutoriel vidéo, s'il vous plaît regardez ici.

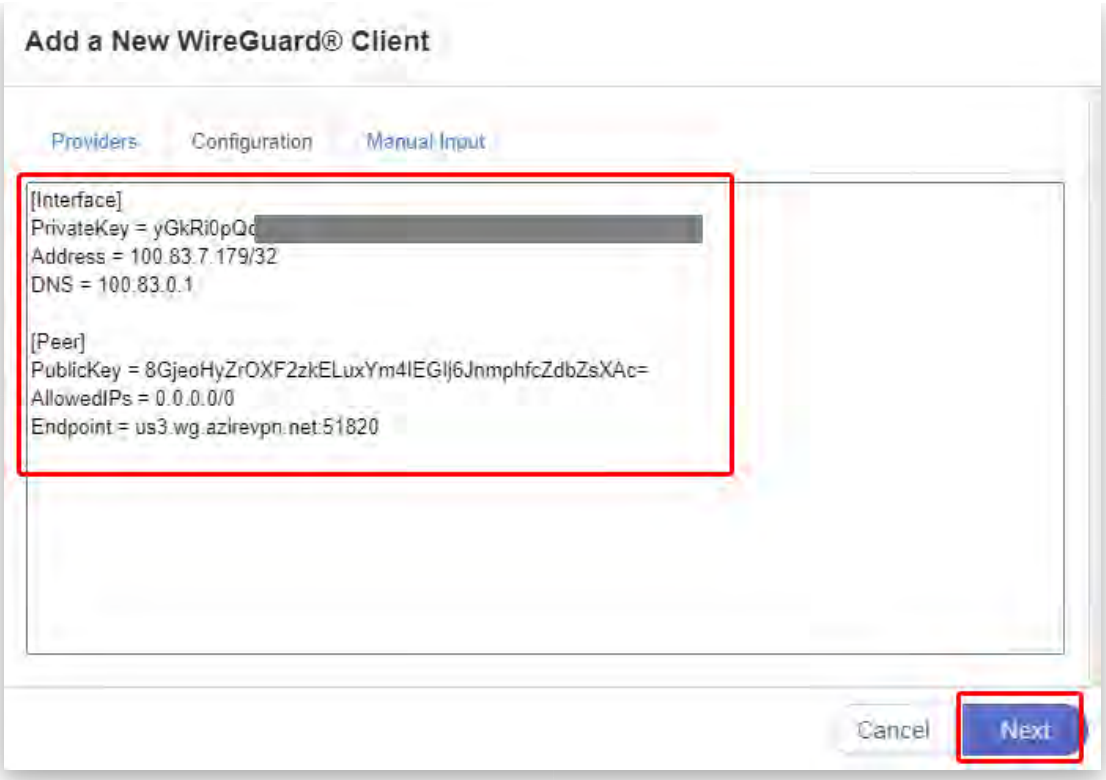
1. Veuillez cliquer sur **et mettre en place WireGuard manuellement**.



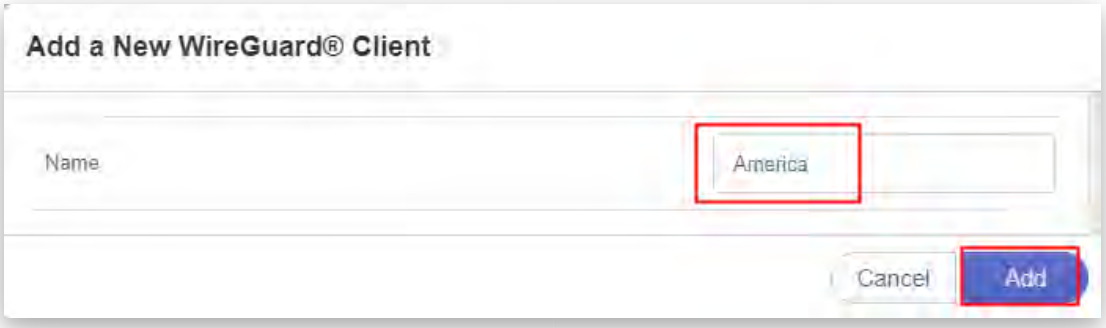
2. Il y a deux façons d'entrer la configuration.



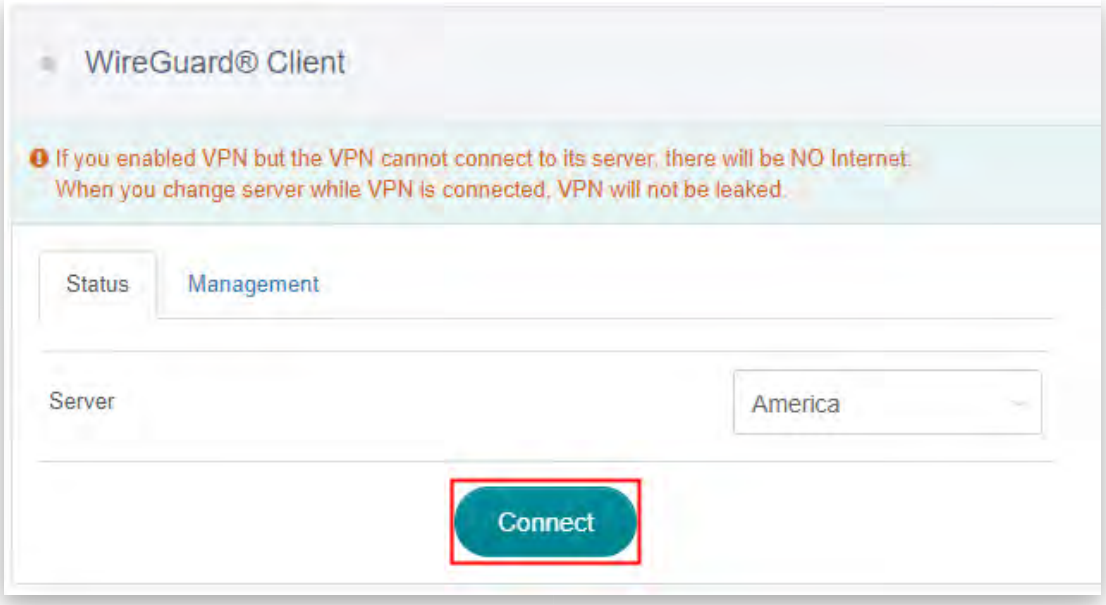
3. Vous pouvez coller la configuration sur l'onglet **Configuration**, ou créer à partir de zéro sur l'onglet **Entrée manuelle**.



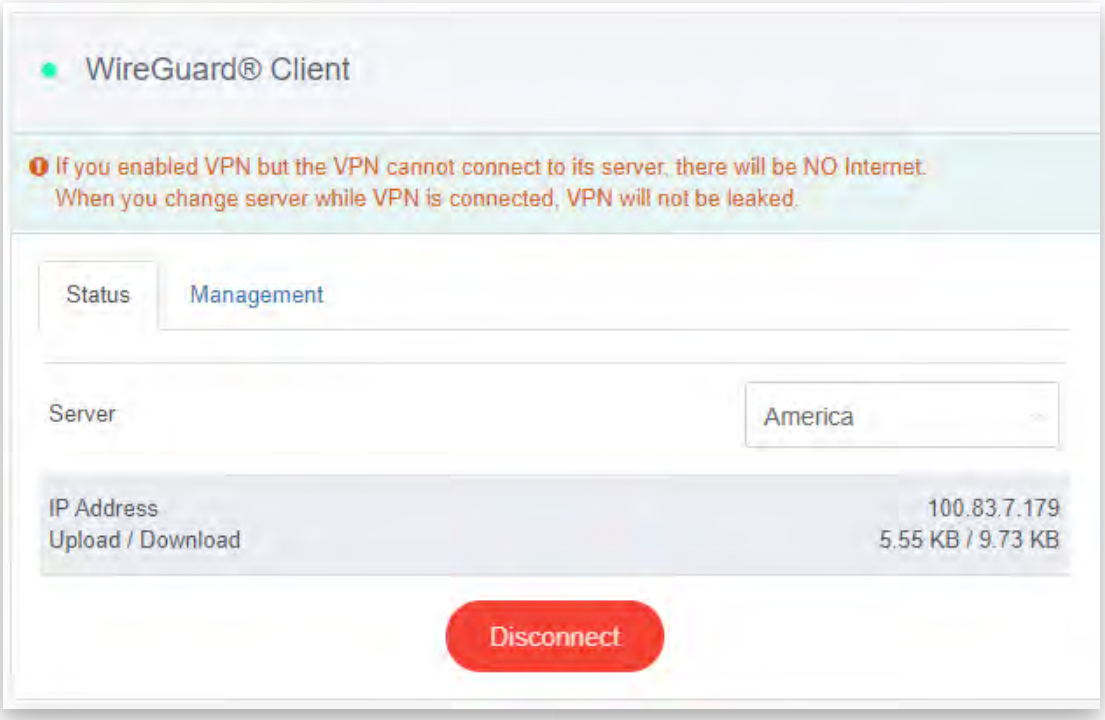
4. Spécifiez un nom descriptif, puis cliquez sur **Ajouter**.



5. Le fichier de configuration a été importé avec succès.



Choisissez le serveur et cliquez sur **Connect.**



Si elle est connectée, il affichera les informations de trafic de téléchargement et de téléchargement.

Remarque: il ne peut pas exécuter VPN Client and Server en même temps, et il ne peut pas non plus exécuter OpenVPN Client et WireGuard Client en même temps.

Configuration du serveur WireGuard sur routeur GL.iNet

Vous pouvez obtenir un routeur GL.iNet pour définir le serveur WireGuard, et obtenir un autre routeur GL.iNet pour être défini en tant que client WireGuard. Pour la configuration du serveur WireGuard, veuillez consulter ici.

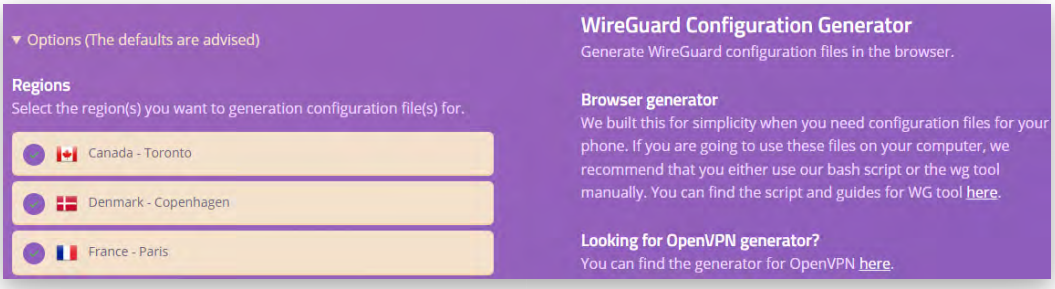
Obtenir des fichiers de configuration auprès des fournisseurs de services WireGuard

AzireVPN

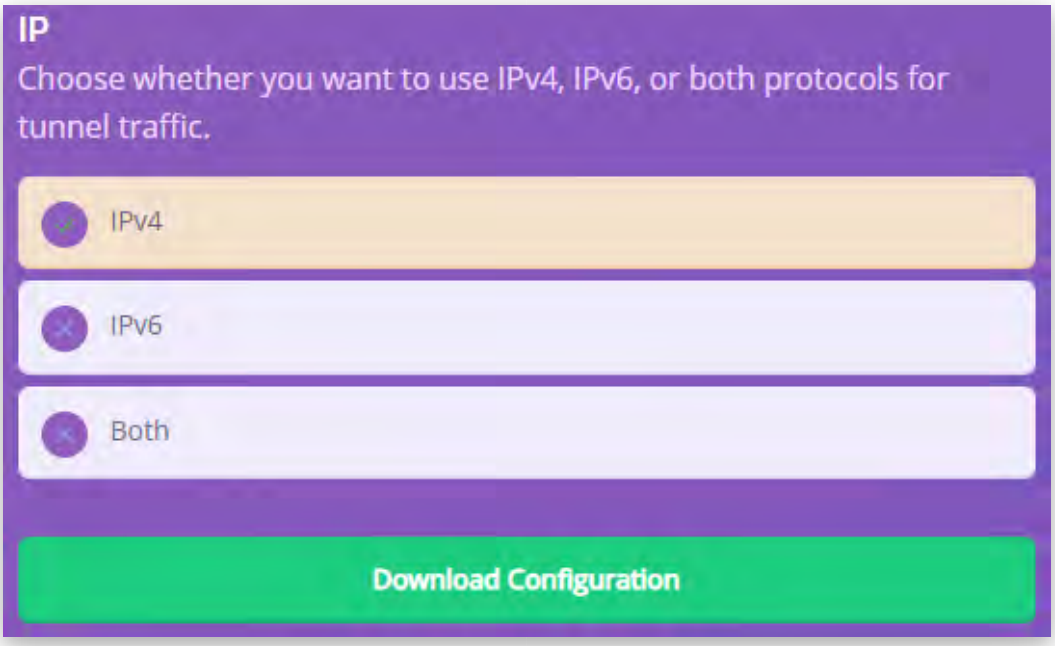
AzireVPN

Site officiel

1. Accéder au site officiel AzireVPN et à se connecter, puis accéder au générateur de configuration WireGuard



2. À l'option IP, veuillez sélectionner **IPv4**IPv4. Puis cliquez sur **Configuration de télécharger**.



3. Suivez ensuite le guide pour continuer.
4. Vous pouvez également utiliser l'application mobile pour configurer AzireVPN.

Mullvad

Mullvad

Site officiel

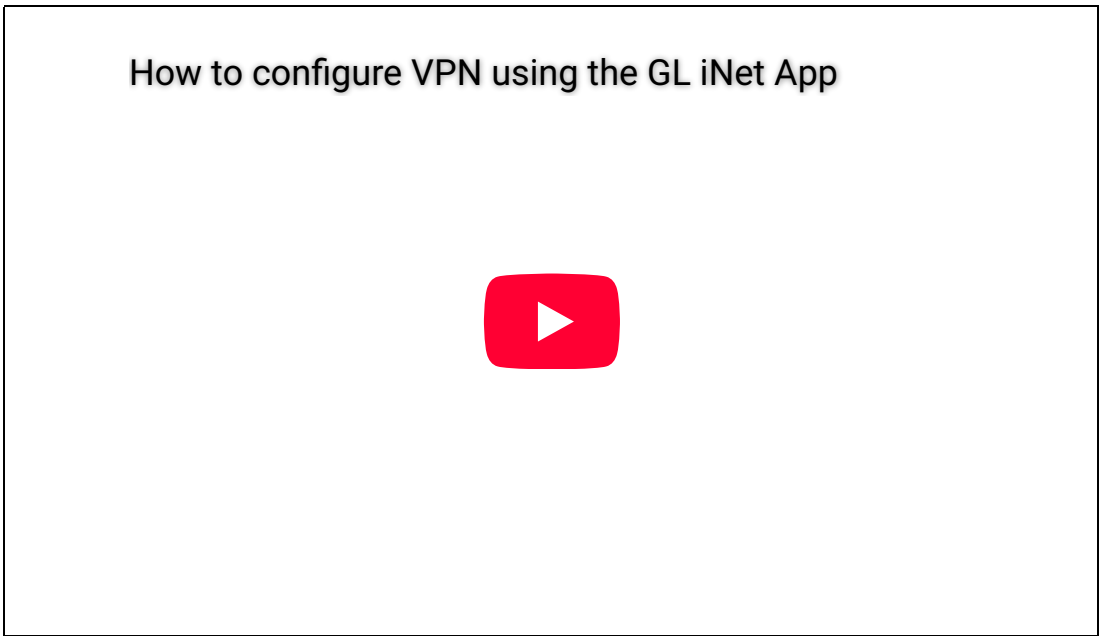
1. Accéder au site Web officiel de Mullvad et à se connecter, puis accéder au générateur de fichiers de configuration WireGuard
2. Suivez ensuite le guide pour continuer.
3. Vous pouvez également utiliser l'application mobile pour configurer Mullvad.

PIA (Accès privé à Internet)

PIA (Accès privé à Internet)

Site officiel

Il ne peut pas détecter la configuration WireGuard à partir de son site web, s'il vous plaît utiliser l'application mobile pour configurer PIA VPN.



VPN Hide.me

VPN Hide.me

Site officiel

Les fournisseurs de VPN Hide.me sont un moyen simple d'utiliser leur service WireGuard sur le routeur GL.iNet.

1. SSH vers routeur.
2. Copiez l'url d'installation sous-jacente, puis collez-la au terminal, appuyez sur la touche Entrée. (Cliquer sur la souris va la coller.)

   ```
   curl -fsSL https://raw.githubusercontent.com/eventure/hide.client.routers/master/glinet_v3/hidemevpn | sh -s install
   ```

3. Il va commencer à installer, puis demander le nom d'utilisateur et le mot de passe. Lors de la frappe ou du collage du mot de passe, aucun changement n'est visible sur le terminal, il suffit d'appuyer sur la clé Entrée après avoir tapé.
4. Une fois que vous avez terminé, allez sur le écran d'administration web et vous verrez que les fichiers de configuration sont déjà dedans. Il suffit de se connecter comme vous le feriez pour n'importe quel autre fichier de configuration.

Remarque: La clé du fichier de configuration VPN Hide.me est régénérée avant chaque connexion et devient invalide après la déconnexion, de sorte que copier ce fichier de configuration à d'autres appareils ne se connectera pas avec succès.

Liaison de référence

Proton VPN

Proton VPN

Site officiel

Si vous utilisez Proton VPN, veuillez suivre le guide ici pour générer le fichier de configuration WireGuard.

Suivez ensuite le guide pour continuer.

Windscribe

Windscribe

Site officiel

Se connecter puis accéder au générateur de Config de WireGuard. Sélectionnez l'emplacement et le port que vous souhaitez utiliser, puis cliquez sur Download Config.



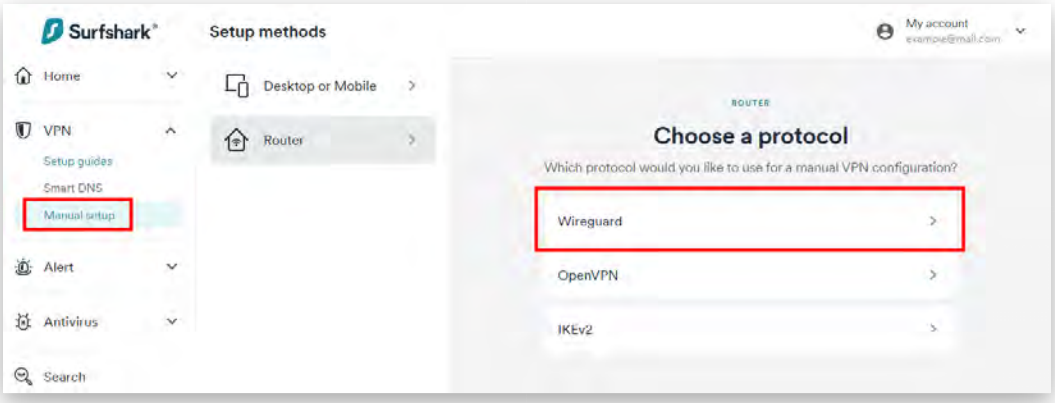
Suivez ensuite le guide pour continuer.

Surfre

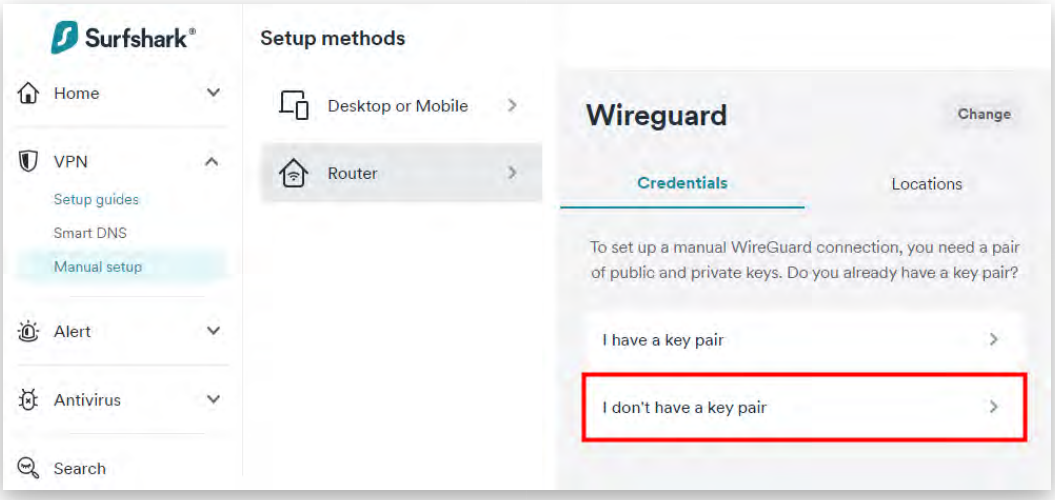
Surfre

Site officiel

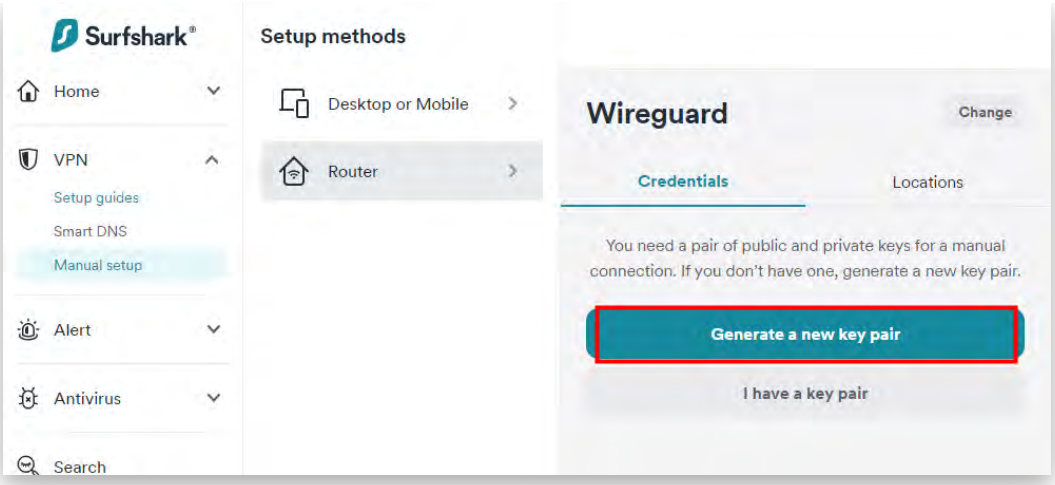
1. Si vous utilisez Surfshark, connectez-vous ensuite sur cette page, cliquez sur **Router** et sélectionnez **WireGuard**.



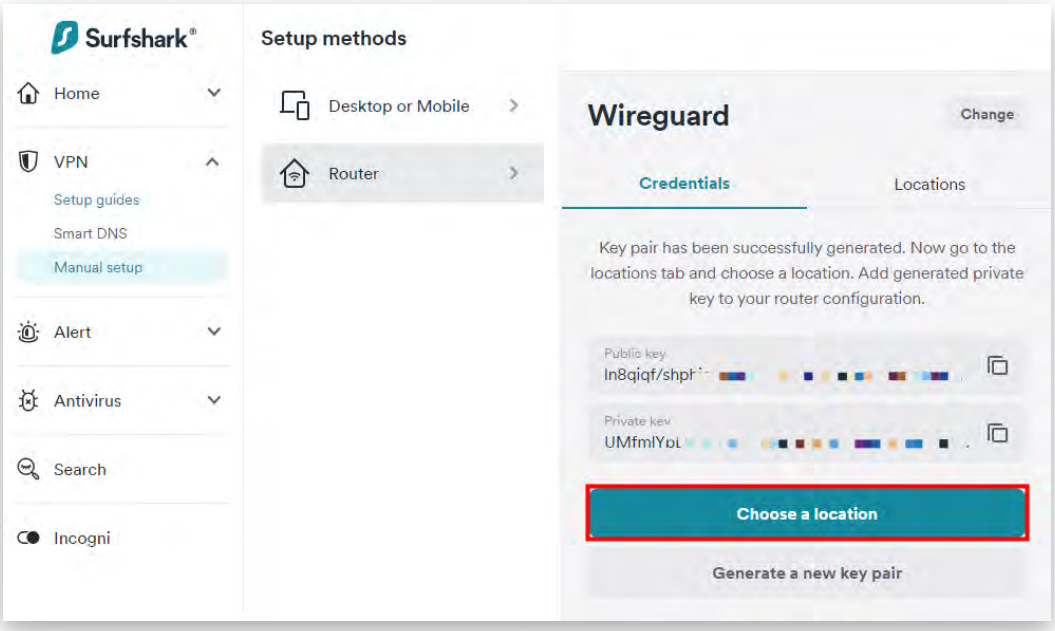
2. Dans la fenêtre suivante, sélectionnez **Je n'ai pas de paire de clés**.



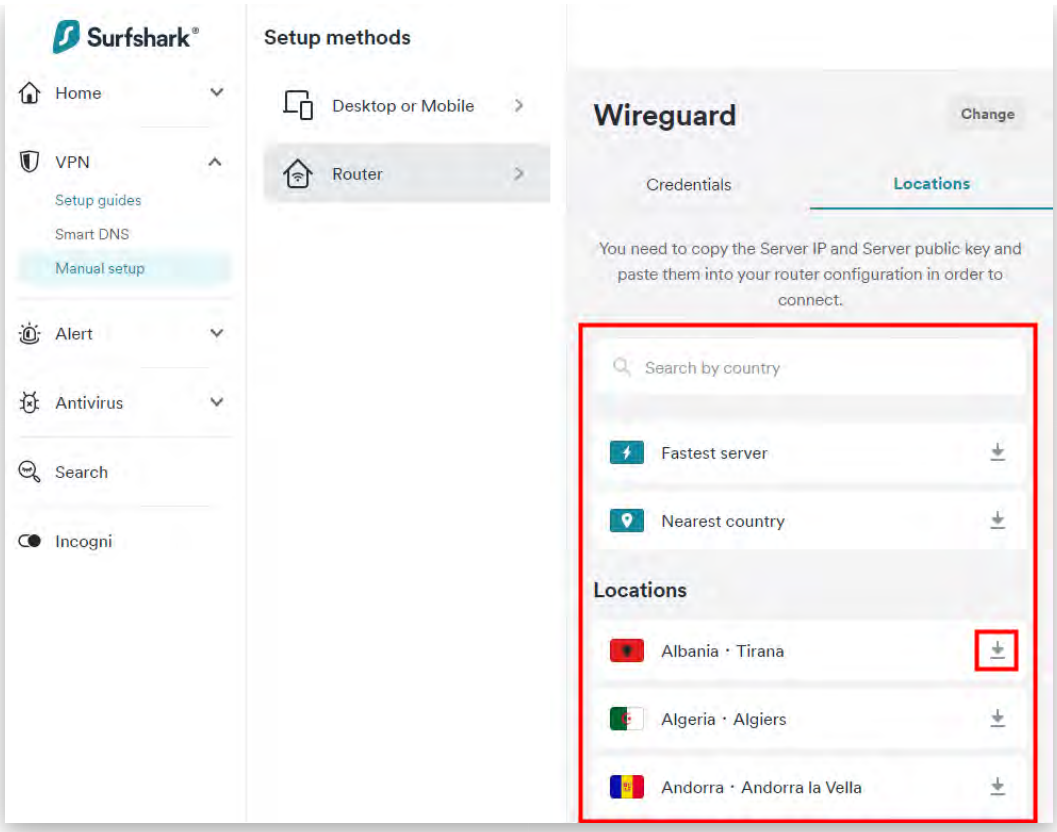
3. Select **Générez une nouvelle paire de clés**.



4. Une fois que la clé a été générée, sélectionnez **Choisissez un emplacement**.



5. Enfin, choisissez un emplacement que vous souhaitez configurer, et cliquez sur le bouton **de téléchargement** à côté de l'emplacement.



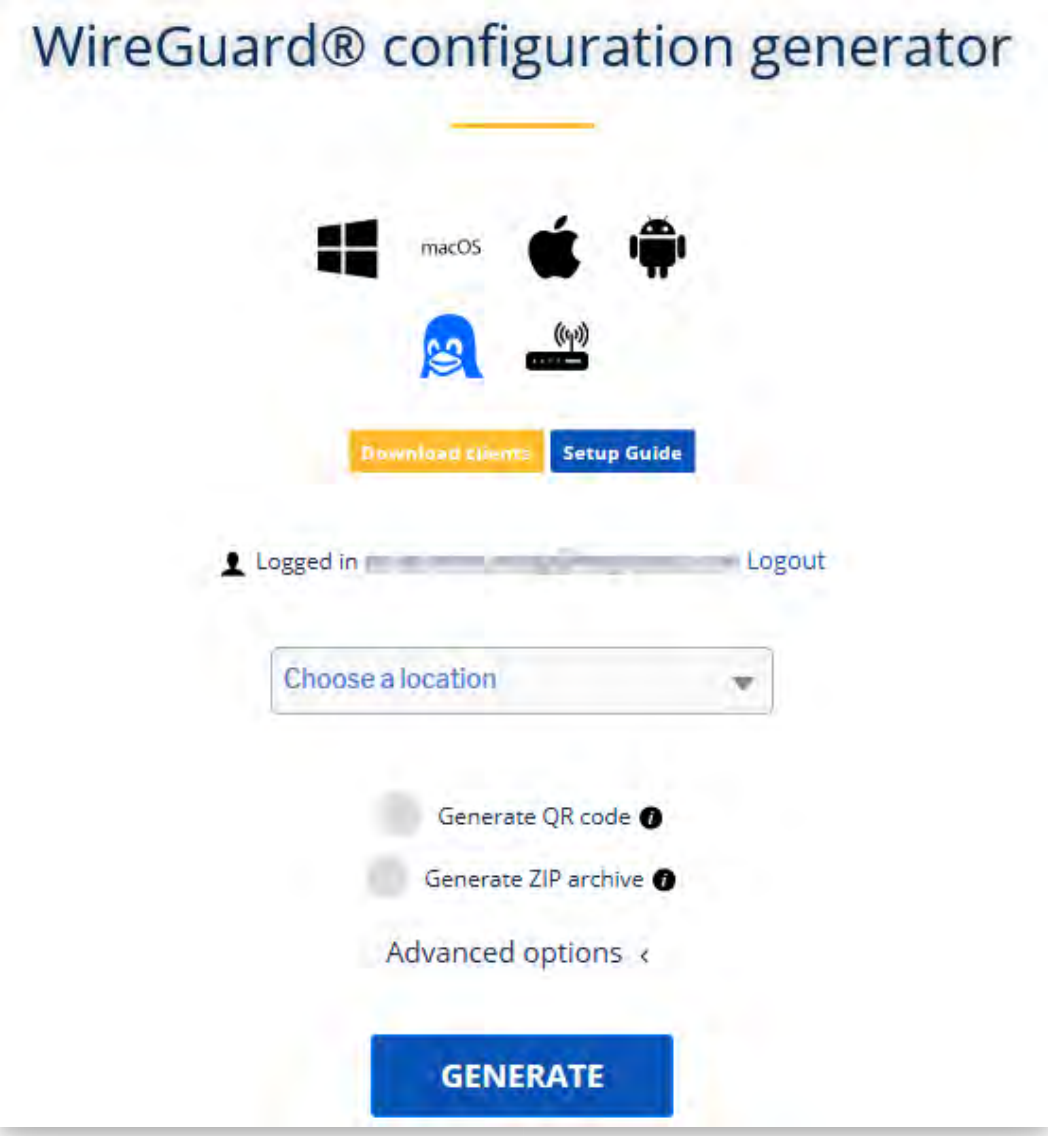
Liaison de référence

StrongVPN

StrongVPN

Site officiel

1. Si vous utilisez StrongVPN, connectez-vous à l'adresse https://wg.strongvpn.com
2. Sélectionnez un emplacement dans le menu déroulant, cliquez sur **GENERATE**, ouvrez le fichier texte téléchargé.



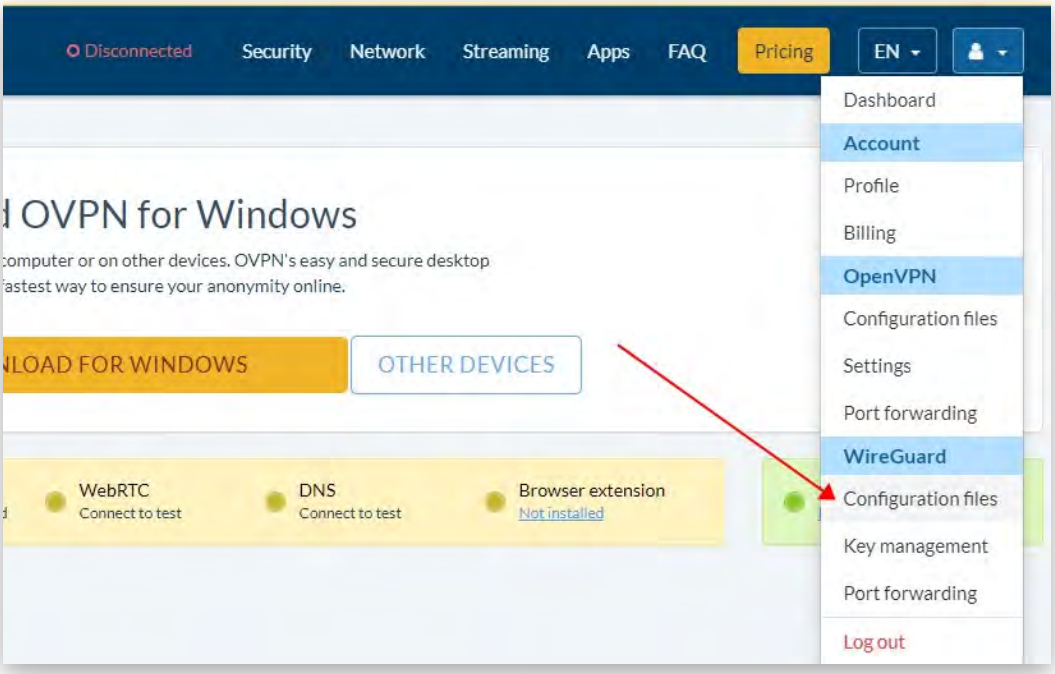
3. Suivez ensuite le guide pour continuer.
4. Vous pouvez également utiliser une application mobile pour configurer StrongVPN.

OVPN

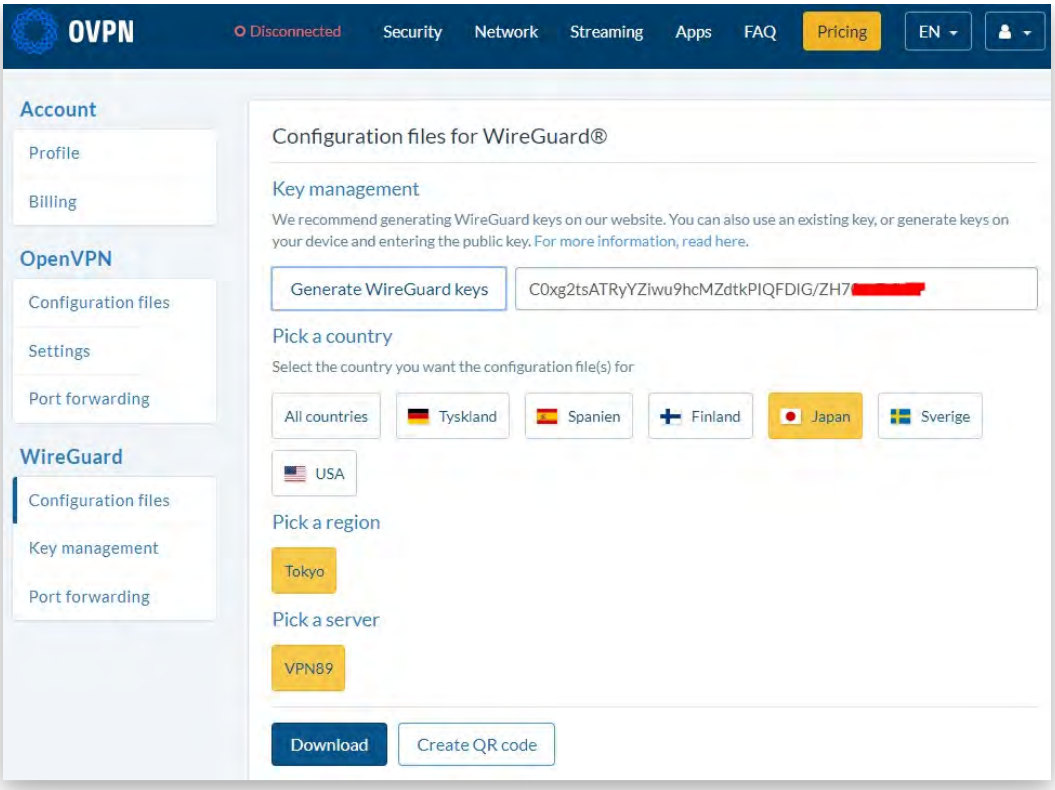
OVPN

Site officiel

1. Connectez-vous à www.ovpn.com, trouvez le menu ci-dessous pour obtenir des fichiers de configuration WireGuard.

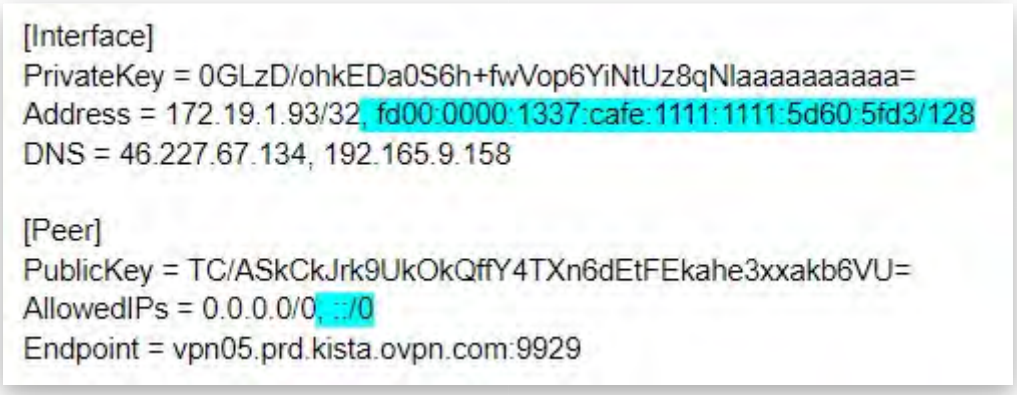


2. Cliquez sur **Generate WireGuard keys**, choisissez le serveur que vous souhaitiez, puis téléchargez la configuration.



3. Ouvrez la configuration par logiciel d'édition de texte, copiez le contenu.

   La configuration peut contenir un contenu IPv6, car les routeurs GL.iNet ne prennent pas en charge IPv6 suffisamment bon, donc s'il vous plaît supprimer le contenu IPv6. J'ai un exemple montrer ci-dessous, le contenu de point fort est le contenu IPv6.



4. Suivez ensuite le guide pour continuer.
5. Vous pouvez également utiliser l'application mobile pour configurer OVPN.

PureVPN

PureVPN

Site officiel

Veuillez suivre le guide ici pour obtenir le fichier de configuration WireGuard.

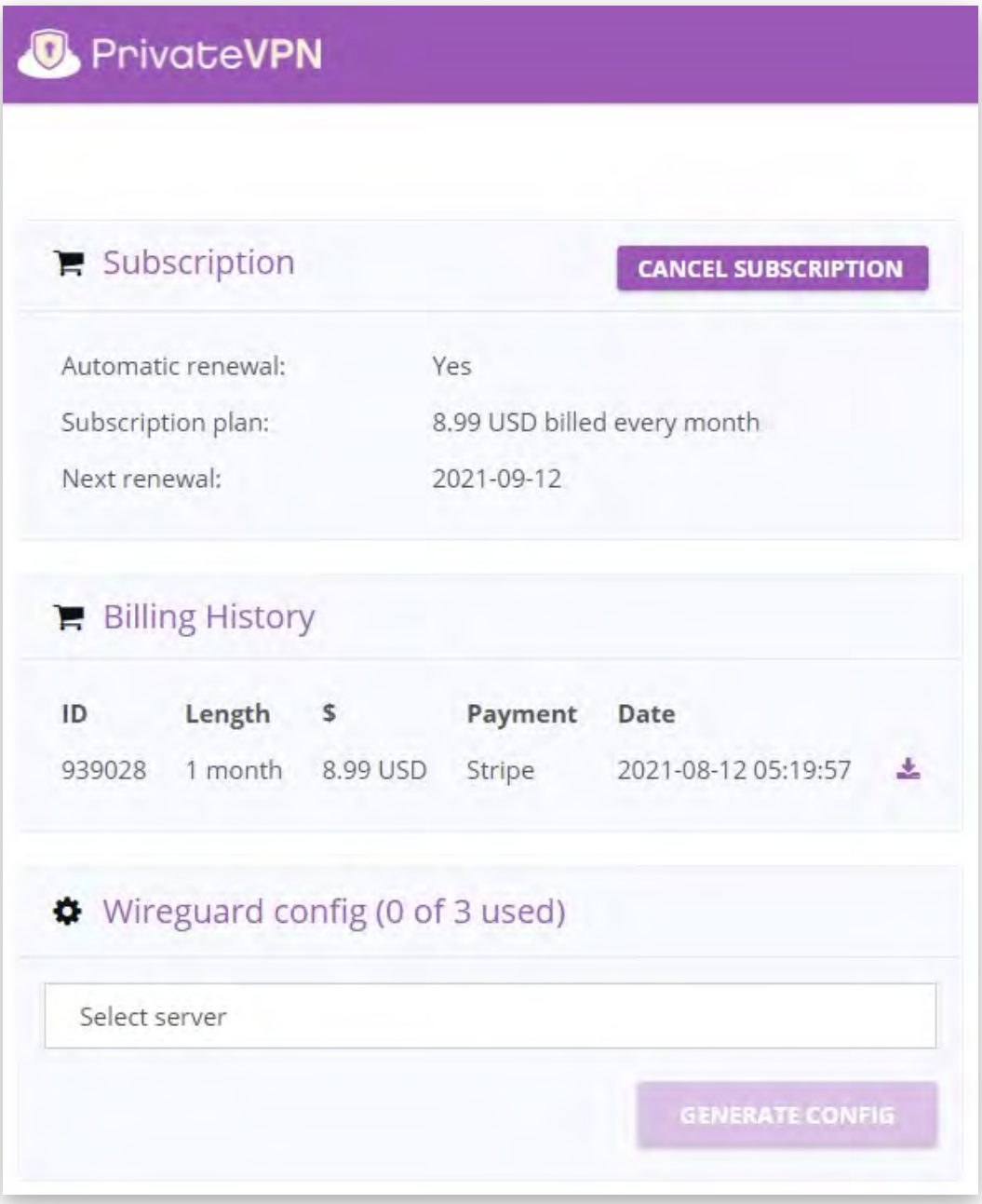
Remarque : Assurez-vous de copier le fichier et d'activer la connexion dans les 30 minutes suivant le téléchargement du profil, sinon la configuration expirera et vous devrez retigner un nouveau fichier de configuration.

PrivateVPN

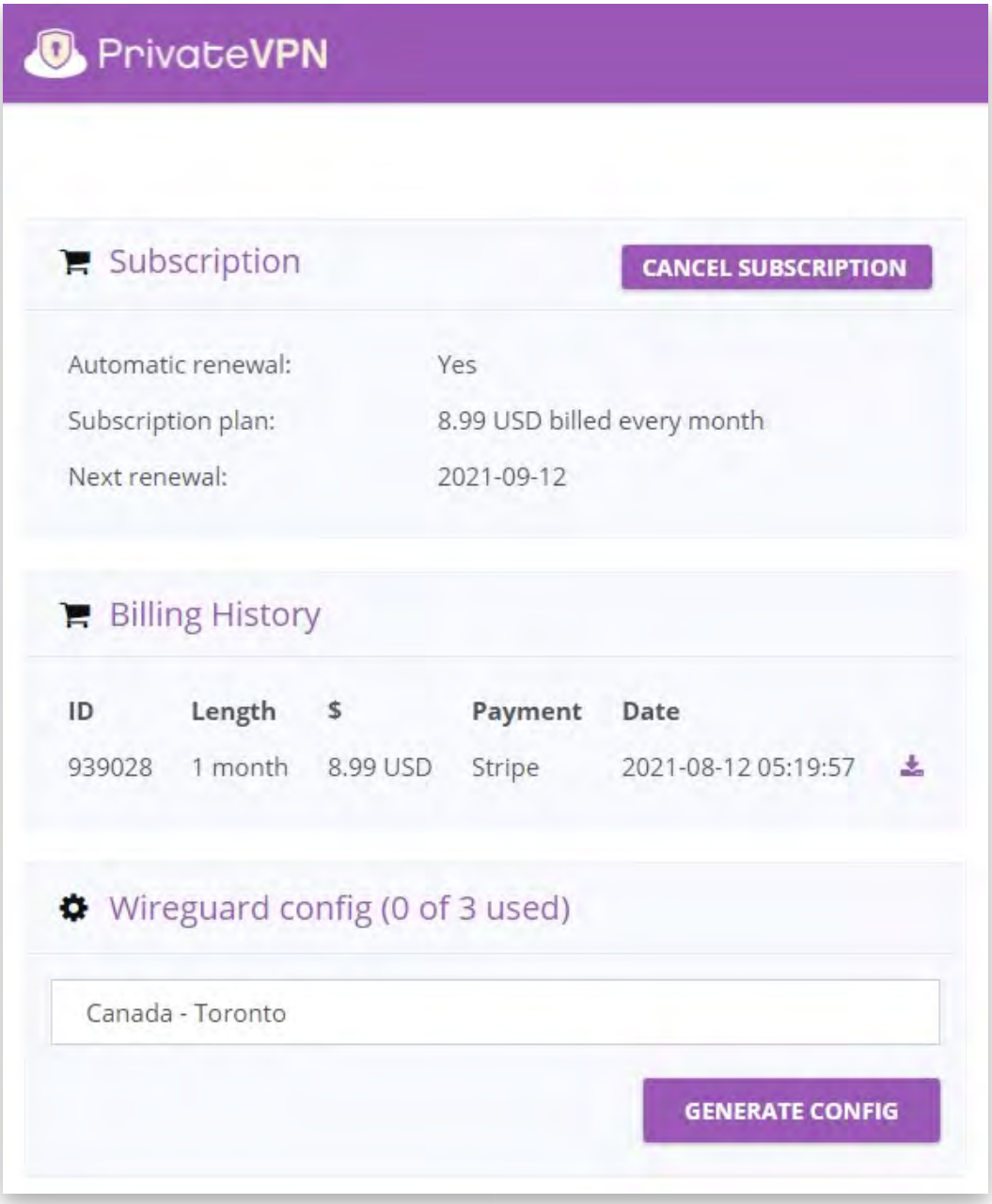
PrivateVPN

Site officiel

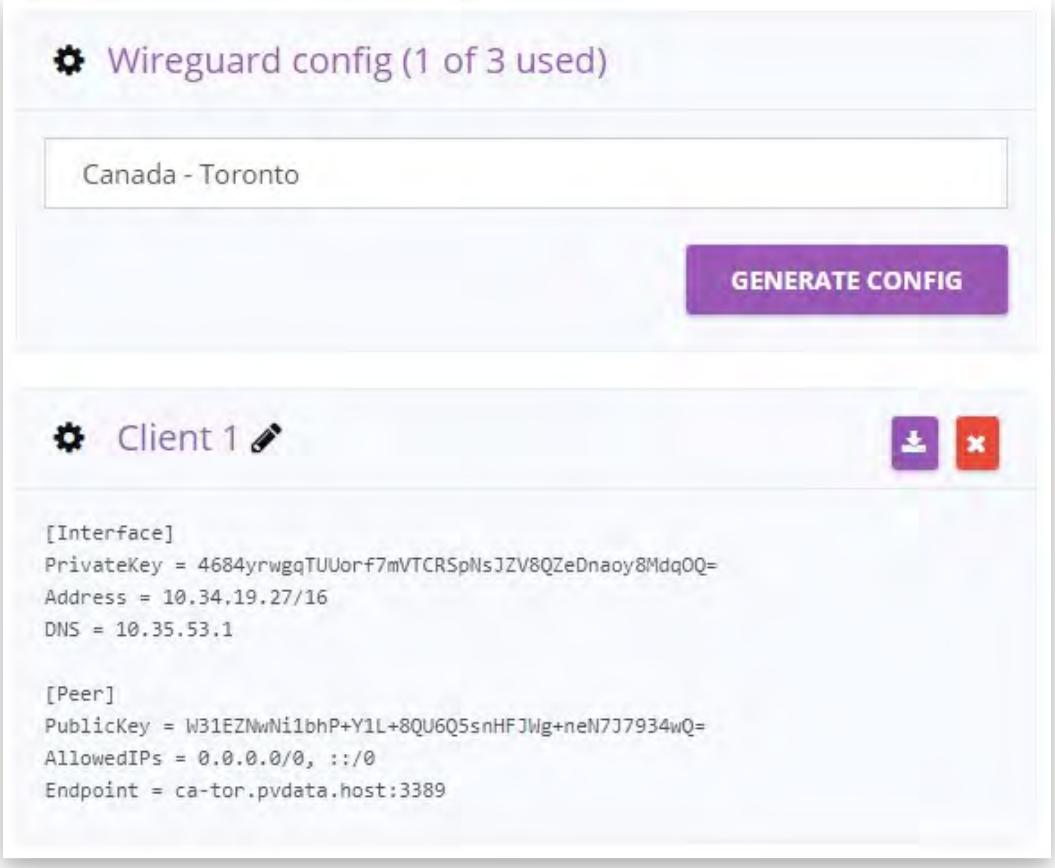
1. Se connecter puis accéder au panneau de contrôle



2. Sélectionner un serveur



3. Cliquez sur **GÉNÉRATE CONFIG**, puis copiez la configuration.



4. Suivez ensuite le guide pour continuer.

AirVPN

AirVPN

Site officiel

1. Si vous utilisez AirVPN, connectez-vous à leur site web, allez dans l'Espace Client, cliquez sur Config Générateur

   airvpn configuration generator

2. Sur la page Config Generator, sélectionnez WireGuard dans le secteur des protocoles.

   airvpn protocols

3. Sélectionnez un serveur, puis faites défiler jusqu'à la fin, cliquez sur **"Générationner".** Il téléchargera le fichier de configuration.

   airvpn select server

4. Suivez ensuite le guide pour continuer.

Astrill

Astrill

Site officiel

Si vous utilisez Astrill, connectez-vous à cette page pour générer des configurations WireGuard.

Suivez ensuite le guide pour continuer.

IVPN

IVPN

Site officiel

Si vous utilisez IVPN, vous devez générer la configuration WireGuard manuellement. Suivez la base de guide sur votre SG.

Windows, macOS, Linux

Suivez ensuite le guide pour continuer.

NVPN

NVPN

Site officiel

Follow the guide here to create the config.

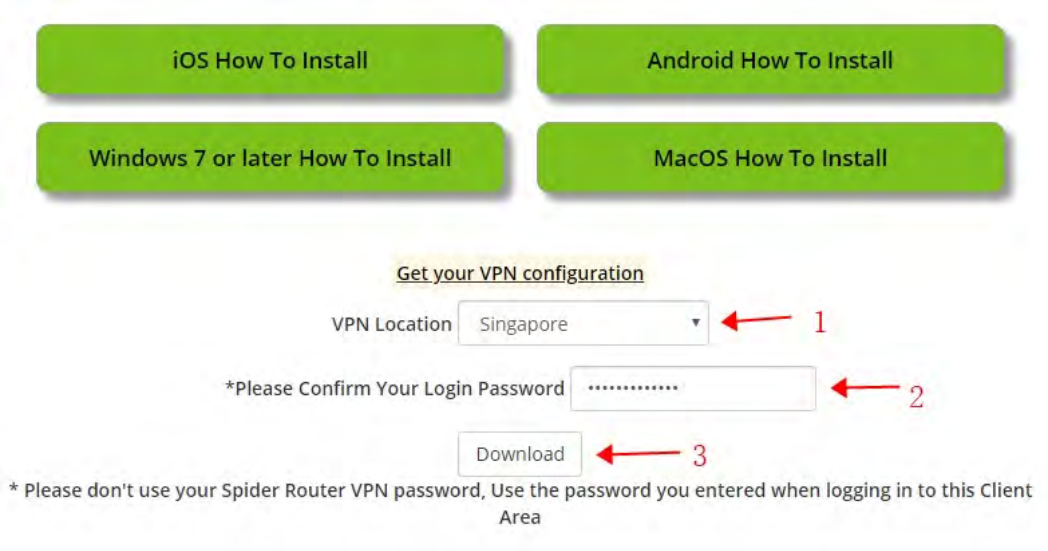
Then follow the guide to continue.

SpiderVPN

SpiderVPN

Official Website

1. Login www.spidervpn.org, find the section to get your VPN configuration. Follow the steps to get the configuration.



2. Download the vpn configuration



3. Then follow the guide to continue.

StarVPN

StarVPN

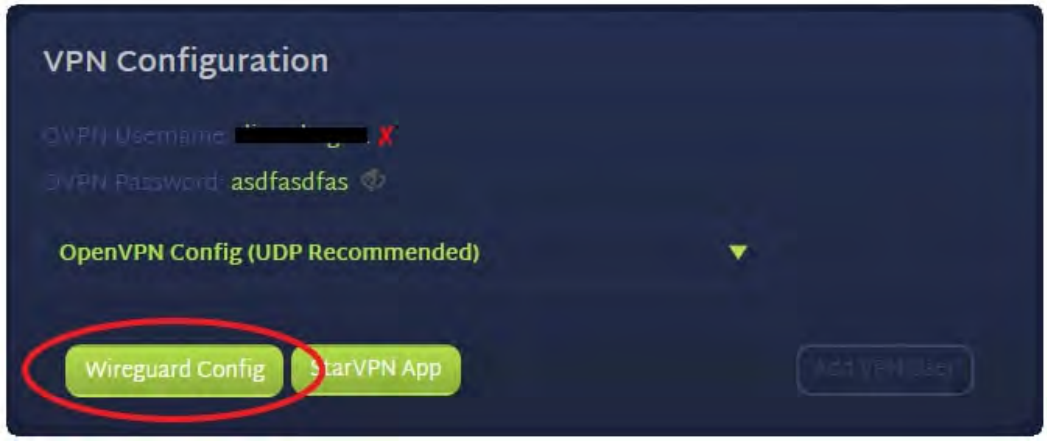
Official Website

1. **Register an account with StarVPN**

   Head on over to their pricing plan options and choose a VPN plan that suits your needs. You can register on checkout or directly here.

2. **Download Wireguard Configuration**

   Log into the StarVPN member area dashboard. Click on Wireguard Config to download the configuration file. Each slot will contain a unique wireguard configuration file.



3. The config may contain IPv6 content, as GL.iNet routers is not support IPv6 good enough, so please delete the IPv6 content.



4. Then follow the guide to continue.

Refer link

TRUST.ZONE

TRUST.ZONE

Official Website

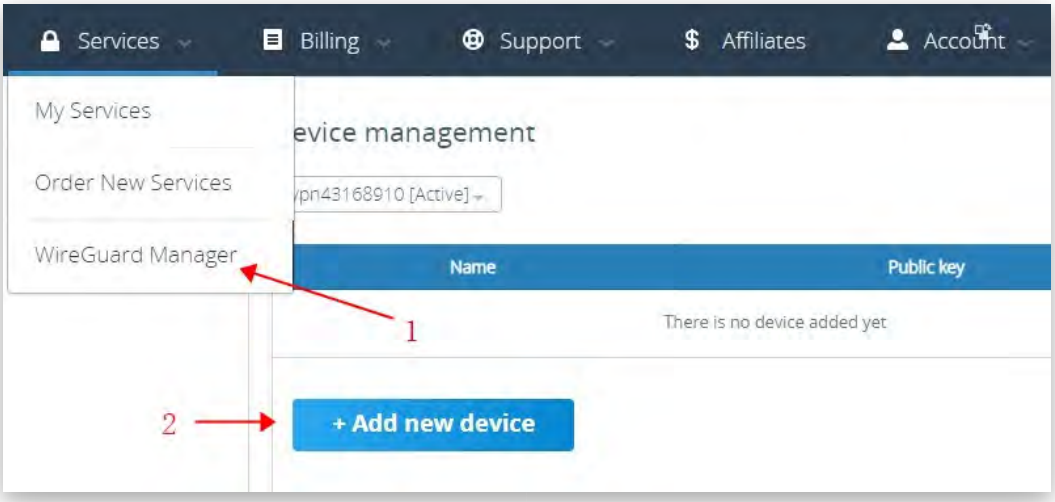
1. Access https://trust.zone/setup and login.
2. Scroll down to the WireGuard section, choose the port you want, then download a config of specific server or a zip file of all configs.
3. Then follow the guide to continue.

VPN.AC

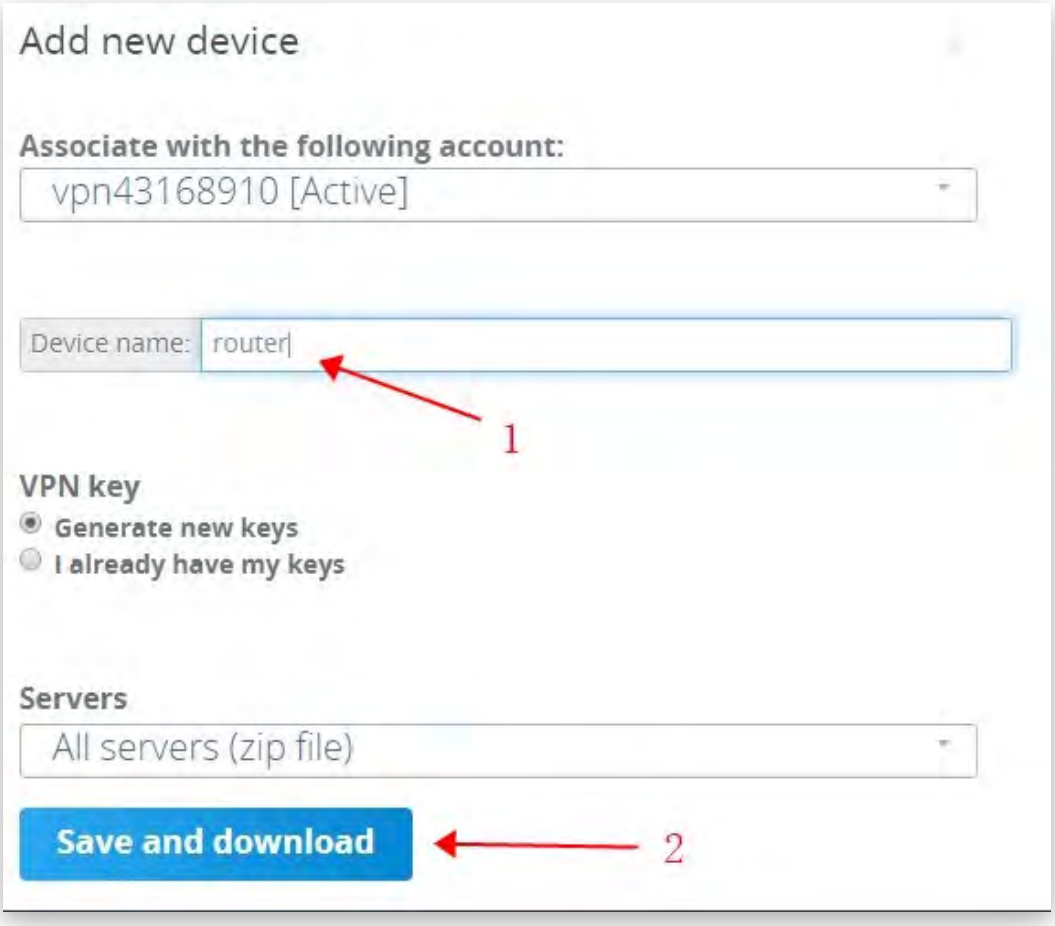
VPN.AC

Site officiel

1. If you are using VPN.AC, you need to login the control panel and find WireGuard Manager from the "Services" menu.



2. Create the config and download.

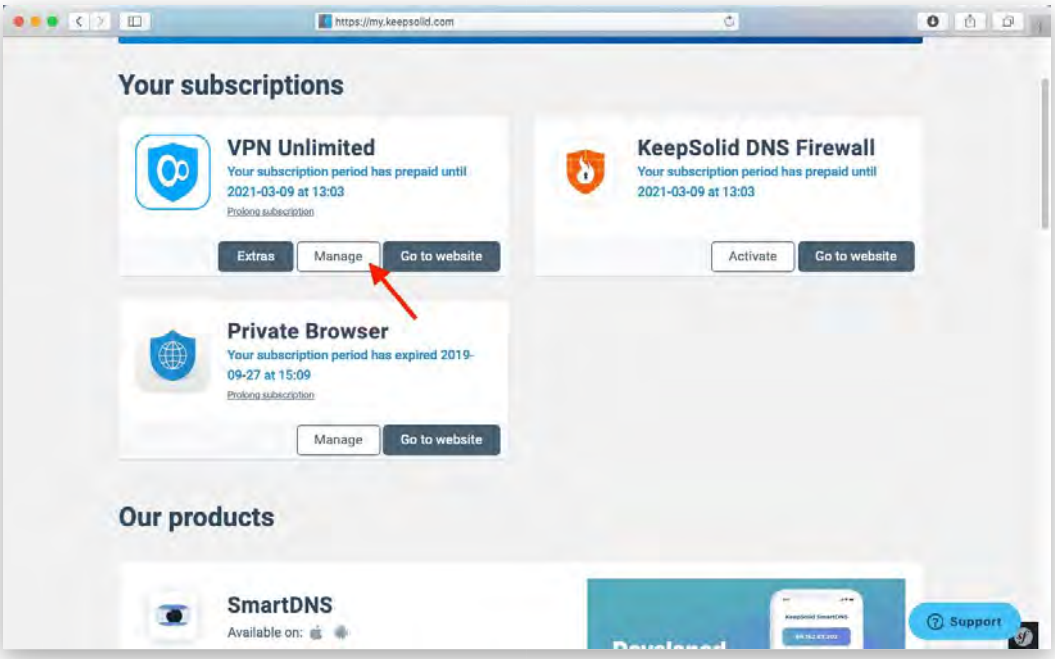


3. Then follow the guide to continue.

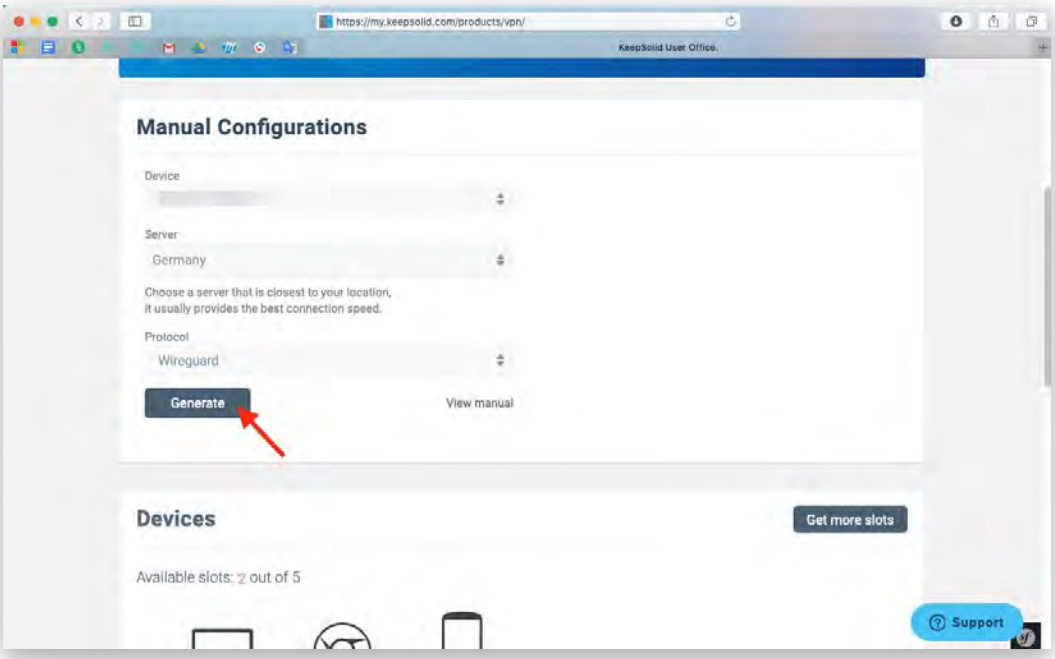
VPN illimité (KepSolid)

VPN illimité (KepSolid)

1. If you are using , sign in to your User Office > select the VPN Unlimited® application > click **Manage**.



2. Press the field under **Device** and click **Manually create a new device…** > set it's custom name, for example WireGuard > choose appropriate location of the **Server** > select the **WireGuard®** protocol from the dropdown menu > click **Generate**.



3. The configuration parameters will then appear below in the text format.



Combine the configuration as below.

[Interface]
PrivateKey = *paste the PrivateKey from your User Office*
ListenPort = *paste the ListenPort details*
Address = *paste Address information*
DNS = *paste DNS details from the User Office*

[Peer]
PublicKey = *paste PublicKey from the User Office*
PresharedKey = *paste PresharedKey details*
AllowedIPs = *paste AllowedIPs details*
Endpoint = *paste Endpoint information*

4. Then follow the guide to continue.

Refer link 1

Refer link 2

12VPX

12VPX

Official Website

If you are using 12VPX, login then access this page, you will see the configs of all servers.

Then follow the guide to continue.

Suggest a WireGuard provider? Please contact support@glinet.biz

Video Tutorial

How to Set Up an WireGuard Client on GL.iNet Routers



Configuration du serveur WireGuard sur routeur GL.iNet

WireGuard est un VPN extrêmement simple mais rapide et moderne qui utilise **une cryptographie de pointe**. Il vise à être plus rapide, plus simple, plus mince et plus utile que l'IPSec, tout en évitant les maux de tête massifs. Il a l'intention d'être beaucoup plus performant qu'OpenVPN.

Les routeurs GL.iNet ont pré-installé WireGuard Server et Client.

S'assurer que le fournisseur de services Internet vous attribue une adresse IP publique

Veuillez vérifier si vous informez vous un fournisseur de services Internet vous attribue une adresse IP publique ici.

Si non, vous ne pouvez pas vous connecter au WireGuard Server.

Une autre méthode est d'utiliser une solution proxy inverse, nous suggérons AstroRelay, vérifiez le tutoriel ici.

Topologie du réseau

- Si le routeur GL.iNet est le routeur principal de votre réseau, c'est simple, s'il vous plaît passer à l'étape suivante.
- Si vous avez déjà un routeur principal, alors le routeur GL.iNet est sous le routeur principal, vous devrez peut-être créer un transfert de port sur le routeur principal.
- Si vous avez déjà un routeur principal, le routeur GL.iNet est à plusieurs niveaux en dessous et vous devez mettre en place un port en avant à chaque niveau.

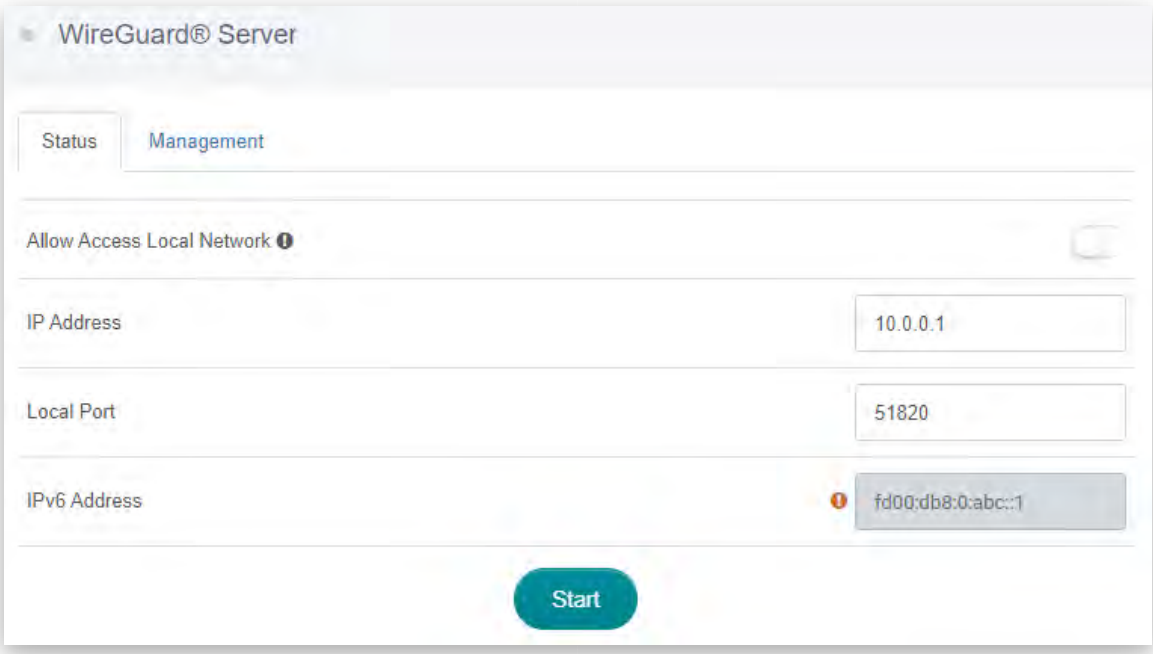
Initialiser WireGuard Server

Accès au panneau d'administration web, sur le côté gauche, VPN - et WireGuard Server. Cliquez sur `Initialize WireGuard Server`.



Démarrer le serveur WireGuard

Vous pouvez simplement utiliser les paramètres par défaut de IP **Address** et **Local Port**, ou vous pouvez définir votre propre valeur. Puis cliquez sur `Start` pour démarrer votre propre serveur WireGuard.



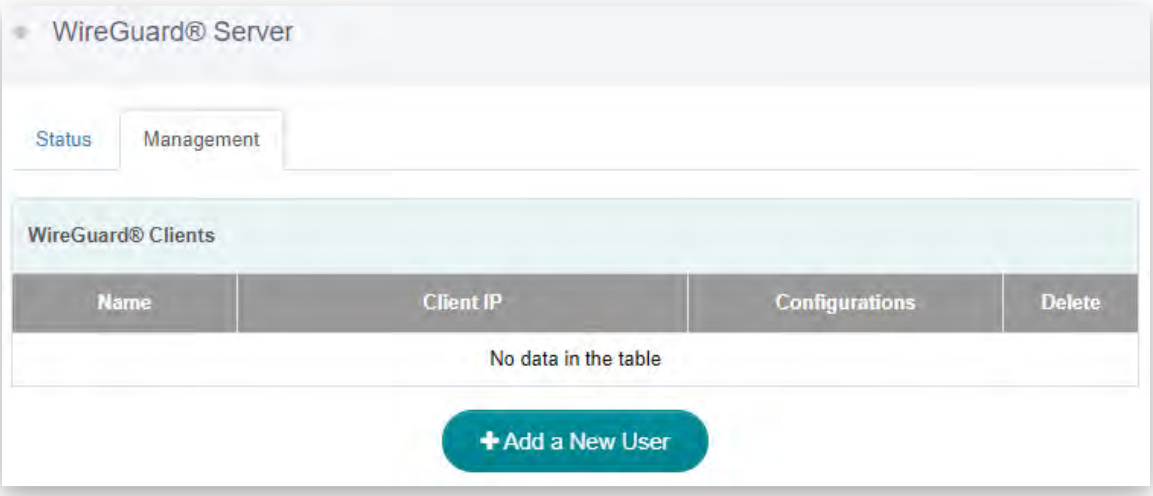
Autoriser le réseau local d'accès: permettre à chaque client qui se connecte à ce serveur WireGuard d'accéder à votre réseau local. Veuillez utiliser avec prudence.

Notez que vous ne pouvez pas exécuter VPN Client and Server en même temps, et que vous ne pouvez pas non plus exécuter OpenVPN Client et WireGuard Client en même temps.

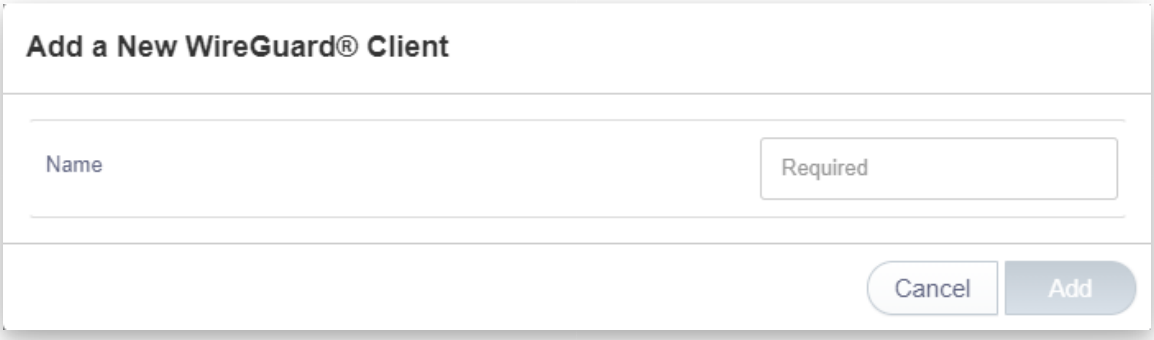
Ajouter un nouveau client

Vous devez ajouter un nouvel utilisateur et appliquer les configurations lorsque vous vous connectez à ce WireGuard Serveur.

Cliquez sur `Management` onglet puis `Add a New User`.

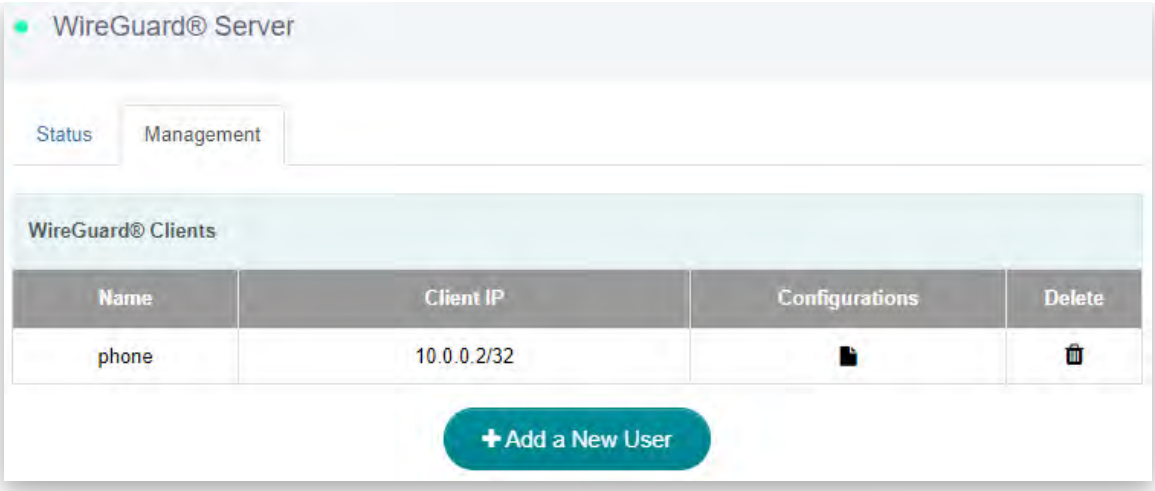


Spécifier le **nom** du nouveau client, puis cliquer sur `Add`.



Obtenez les détails de la configuration pour votre client

Vous pouvez maintenant consulter la liste des clients que vous avez ajoutés. Vous pouvez `Delete` tout client indésirable. Veuillez cliquer sur `Configurations` pour trouver les détails de configuration que vous devez utiliser lorsque vous êtes en train de mettre en place le client WireGuard. Nous fournissons QRcode et Texte Plain, vous pouvez utiliser un logiciel Text Editor pour enregistrer le texte en ligne à `.conf` Fichier.





Pour vérifier si WireGuard Server fonctionne correctement

Pour vérifier si WireGuard Server fonctionne correctement, nous pouvons utiliser un autre appareil connecté à un autre réseau et utiliser la configuration WireGuard que nous avons exportée plus tôt pour nous connecter et voir si elle se connecte correctement et si l'adresse IP est l'IP de WireGuard Server.

La manière la plus simple est d'utiliser un téléphone portable avec l'application client officielle WireGuard installée, d'éteindre sa connexion Wi-Fi, et de se connecter uniquement à Internet via 3G/4G/5G. Ouvrez ensuite l'application WireGuard, importer la configuration WireGuard à partir du code QR. Activez la connexion, vérifiez si le téléphone a un accès à Internet et si son adresse IP est l'IP de votre serveur WireGuard.

Il existe plusieurs raisons courantes pour lesquelles il n'a pas étéinfraction :

- Le fournisseur de services Internet ne vous attribue pas d'adresse IP publique, veuillez vérifier ici.
- Vous pourriez avoir besoin d'un transfert de port de configuration, veuillez vérifier ici.
- Le port que vous utilisez pour WireGuard Server est bloqué par le fournisseur d'accès Internet, le passage à un autre port ou le contact avec le fournisseur de services Internet.
- Certains pays/régions peuvent bloquer la connexion VPN.

Si votre adresse IP publique est dynamique

Certains fournisseurs de services Internet peuvent parfois changer d'adresse IP. Pour surmonter cela, activez le DDNS, puis éditez la configuration pour remplacer l'adresse IP publique par votre url DDNS.

1. Copier le contenu de la configuration dans un éditeur de texte (e.g. Atome, sublime).
2. Éditez la configuration pour remplacer DDNS url par votre adresse IP publique.



Après remplacement.



3. Copier le contenu révisé pour générer un QRCode, ou le sauvegarder comme `.conf` Fichier.

La connexion WireGuard peut diminuer un certain temps lorsque l'adresse IP publique change, après la mise à jour DDNS url à la nouvelle adresse IP publique, le conneciton reprendra. Le DDNS est mis à jour toutes les 10 minutes. Si la connexion ne reprend pas, assurez-vous que l'url DDNS est pointé vers une nouvelle adresse IP publique, puis désactivez la connexion WireGuard et continuez à l'allumer.

App Client WireGuard

Nous pouvons utiliser un autre routeur GL.iNet en tant que client WireGuard, ou utiliser leur application officielle sur d'autres appareils avec divers systèmes d'exploitation.

- Veuillez vous référer au site Web officiel de WireGuard: https://www.wireguard.com/install

---

Articles connexes

- Comment visiter le côté LAN client WireGuard depuis le serveur

---

Ont-ils encore des questions? Visitez notre forum communautaire.

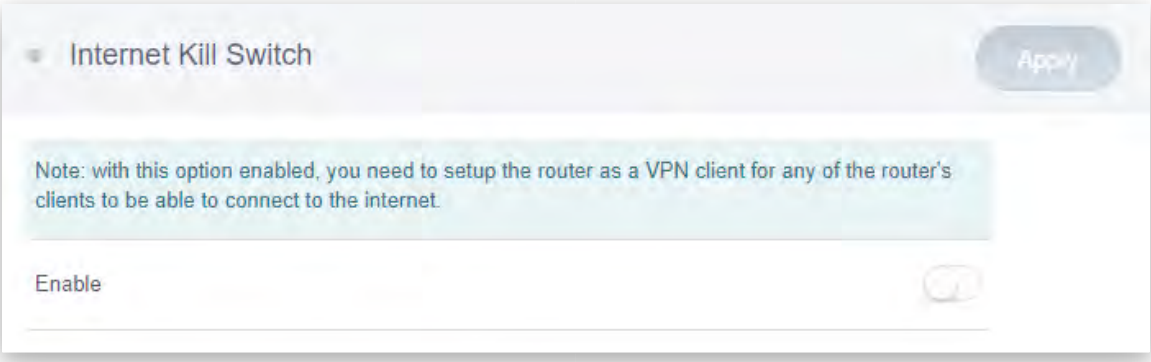
Kill Switch sur Internet

Cette fonctionnalité est disponible depuis la version 3.100.

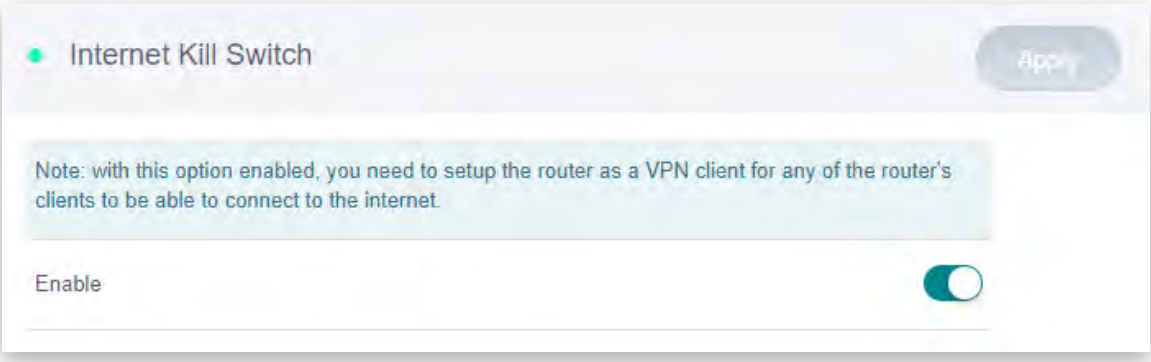
Sur le côté gauche du panneau d'administration web - VPN - Internet Kill Switch

Cette fonctionnalité est de s'assurer que les appareils connectés au routeur accèdent toujours à Internet via VPN.

Si cette fonctionnalité est activée, le routeur doit faire fonctionner un client VPN (OpenVPN ou WireGuard) tout le temps, si l'un des clients VPN ne fonctionne pas, les appareils connectés au routeur ne sont **pas autorisés** à accéder à Internet.

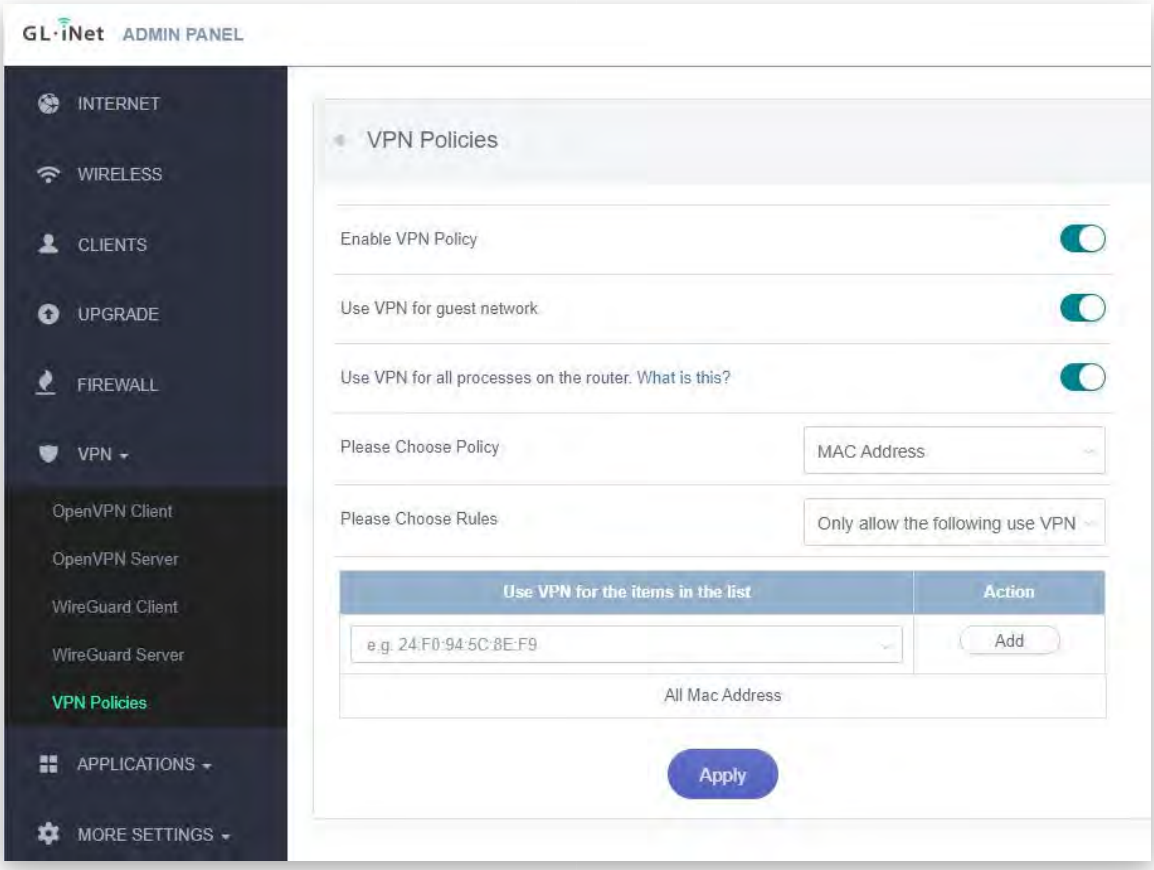


Il suffit de basculer le `Enable` bouton puis cliquer `Apply` .



Politiques VPN

À partir de la version 3.022 du micrologiciel, les utilisateurs peuvent définir des politiques de routage VPN. Par exemple, il est possible d'utiliser VPN pour un site Web/IP spécifique tout en maintenant un trafic Internet normal sans VPN pour les autres.



Paramètres

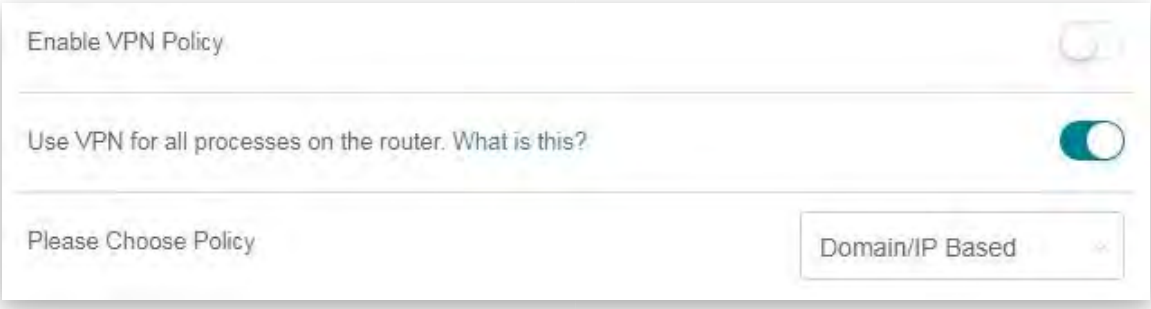
Activer la politique VPN : activer/off des politiques VPN.

Utiliser VPN pour le réseau invité : activer/désactiver le VPN pour le réseau invité.

Utiliser VPN pour tous les processus sur le routeur: En général, le trafic de tous les processus s'exécutant sur le routeur tel que GoodCloud / DDNS sera acheminé par VPN s'il y a un client VPN connecté (par ex. WireGuard, OpenVPN). Dans ce cas, ces processus perdront Internet si la connexion VPN n'est pas stable. Afin d'assurer le bon fonctionnement de ces processus, vous pouvez désactiver cette option. En conséquence, ils n'utiliseront pas de VPN.

Choix de la politique : L'article peut être soit **le domaine/le livre** (par exemple gl-inet.com /

192.168.1.1 / 192.168.1.0/24) soit **l'adresse Mac** (24:F0:94:5C:8E:F9).



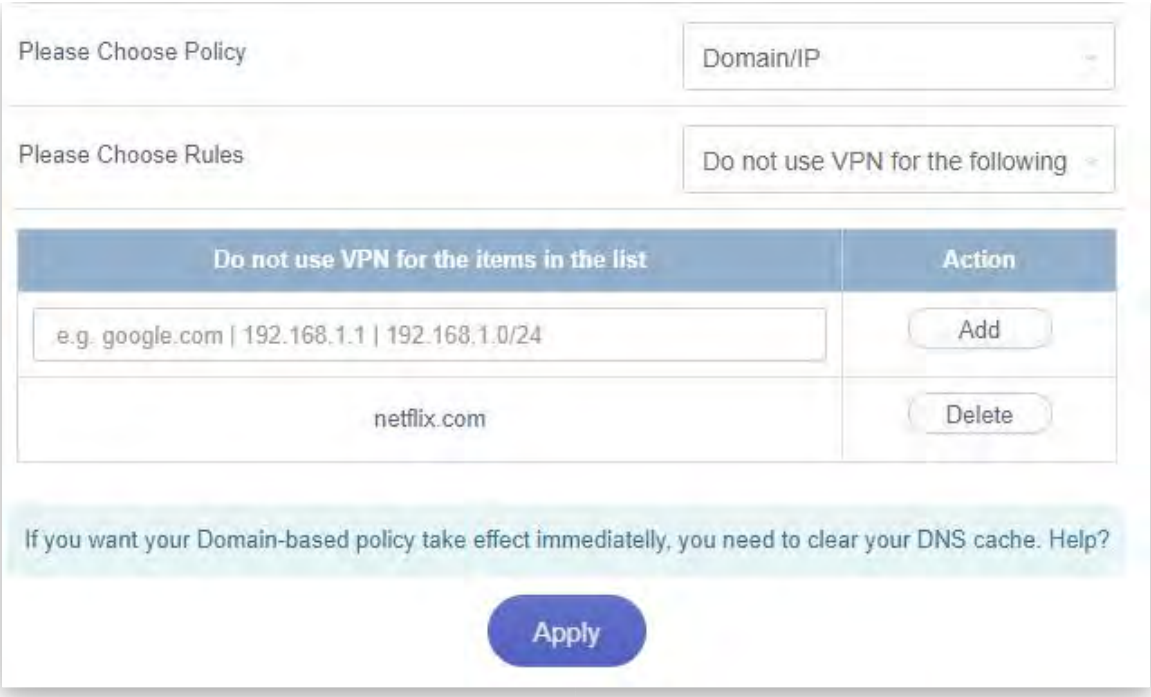
Ajouter une politique VPN

Vous ne pouvez configurer que seul **l'utilisation suivante de VPN** ou **N'utilisez pas de VPN pour ce qui suit**. Cliquez sur la boîte de dépôt pour commuter parmi **les VPN suivants** et **n'utilisez pas de VPN pour ce qui suit**. Pour ajouter une politique, entrez l'adresse domaine/IP ou Mac dans la zone, puis cliquez sur `Add`. Enfin, cliquez sur `Apply` activer la politique.

Par exemple, si nous voulons acheminer uniquement le trafic de `netflix.com` via VPN, nous devons choisir Policy **Domain/IP**, choisir Règle **d'autorisation uniquement l'utilisation suivante VPN**, input *netflix.com* et cliquez sur `Apply`.



Cependant, si nous voulons acheminer tout le trafic via VPN sauf `netflix.com`, nous devons choisir Policy **Domain/IP**, choisir Règle **Ne pas utiliser VPN pour ce qui suit**, saisissez *netflix.com* et cliquez sur `Apply`.



Cliquet DNS transparent

Si vous utilisez une politique basée sur le domaine, cela peut ne pas fonctionner à moins que vous n'ayez réglé votre cache DNS. Veuillez suivre les instructions ci-dessous pour vider votre cache DNS.

Windows : Appuyez sur **Win et R** et faites fonctionner **cmd**. Commande d'exécution `ipconfig /flushdns`.

MacOS : **Terminal** ouvert et commande d'exécution `sudo killall -HUP mDNSResponder`.

Ubuntu : Open **Terminal** et commande d'exécution `sudo service network-manager restart`.

Vous pouvez également avoir besoin d'effacer le cache DNS dans votre navigateur.

Chrome : Visite chrome://net-internals/-dns. Cliquez sur `Clear host cache`.

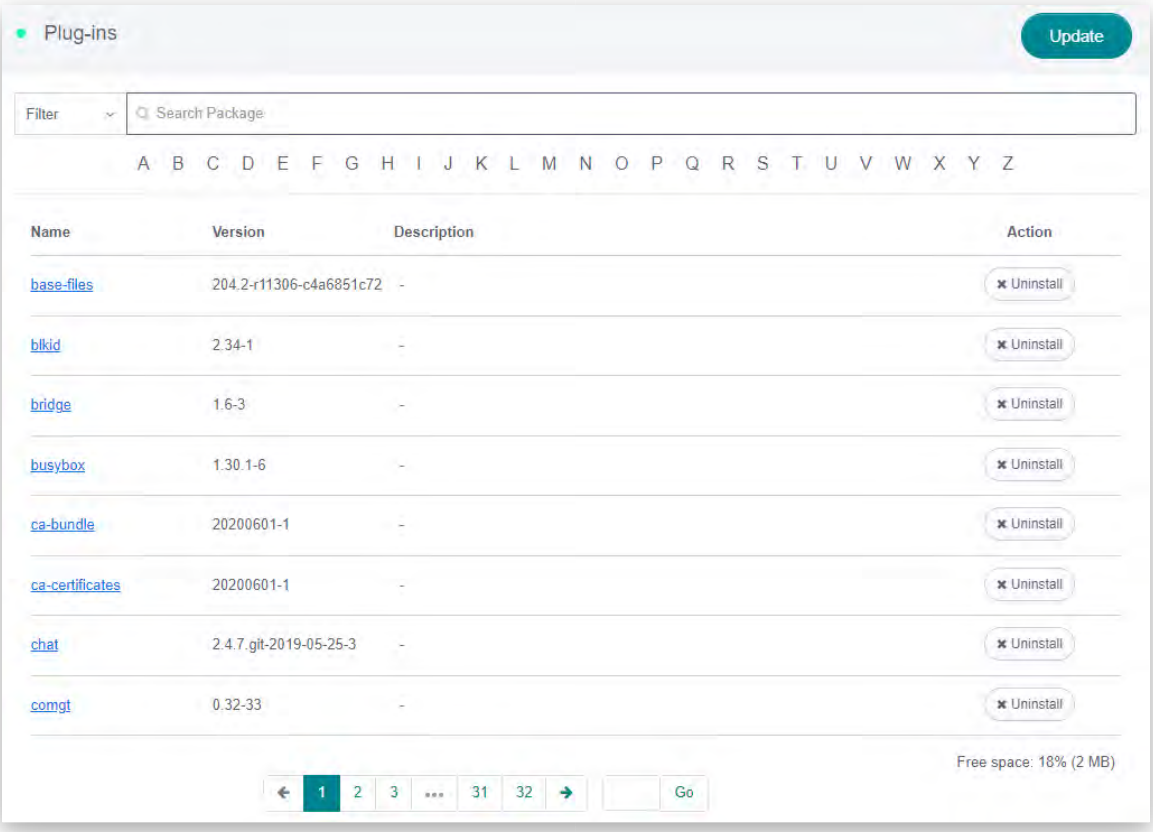
Firefox : Open Firefox et presse `Ctrl` - `Shift` - `Delete`. Sélectionnez **la plage de temps** à **Tout** et vérifiez uniquement **Cache**. Enfin, cliquez sur `Clear Now`.

APPLICATIONS

Filets

Plug-ins vous permet de gérer les paquets OpenWrt. Vous pouvez installer ou supprimer n'importe quel emballage.

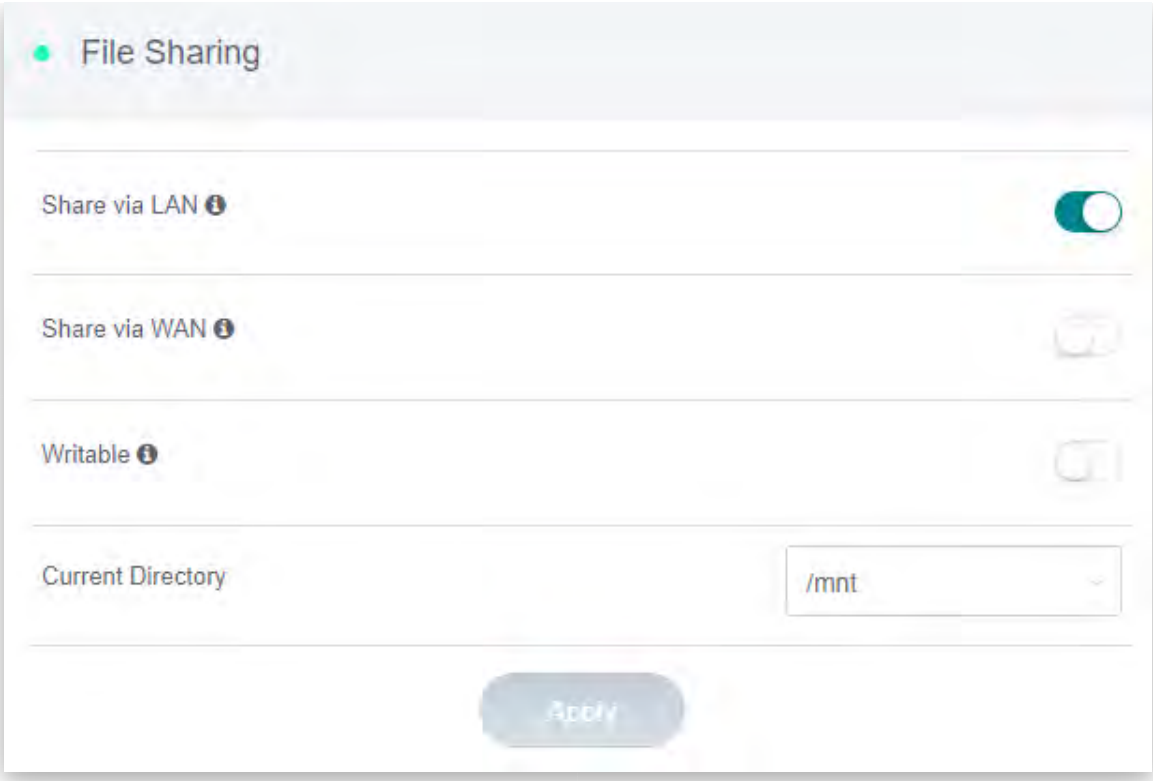
N'oubliez pas de cliquer sur `Update` chaque fois que vous accédez à ce dépôt de paquets.



Partage des fichiers

Sur le côté gauche du panneau d'administration Web - APPLICATIONS - Partage de fichiers -

Vous pouvez utiliser un stockage USB externe ou une carte MicroSD avec GL.iNet routeur, et certains modèles ont un grand stockage interne. Pour partager le stockage externe ou interne, veuillez consulter le partage de fichiers.

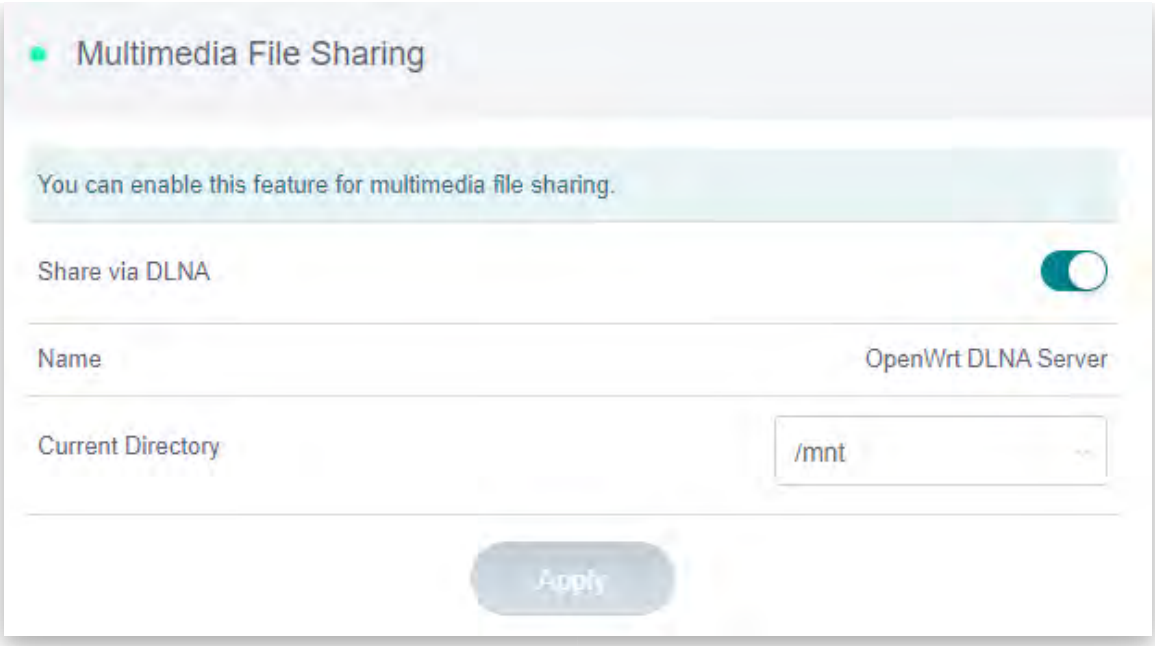


Partage multimédia de fichiers

Sur le côté gauche du panneau d'administration Web - APPLICATIONS - Partage de fichiers - - Partage de fichiers multimédia

Vous pouvez utiliser un stockage USB externe ou une carte MicroSD avec le routeur GL.iNet, pour configurer le partage de fichiers multimédia via DLNA sur un réseau domestique.

Veuillez vous reporter au partage multimédia de fichiers pour le détail.

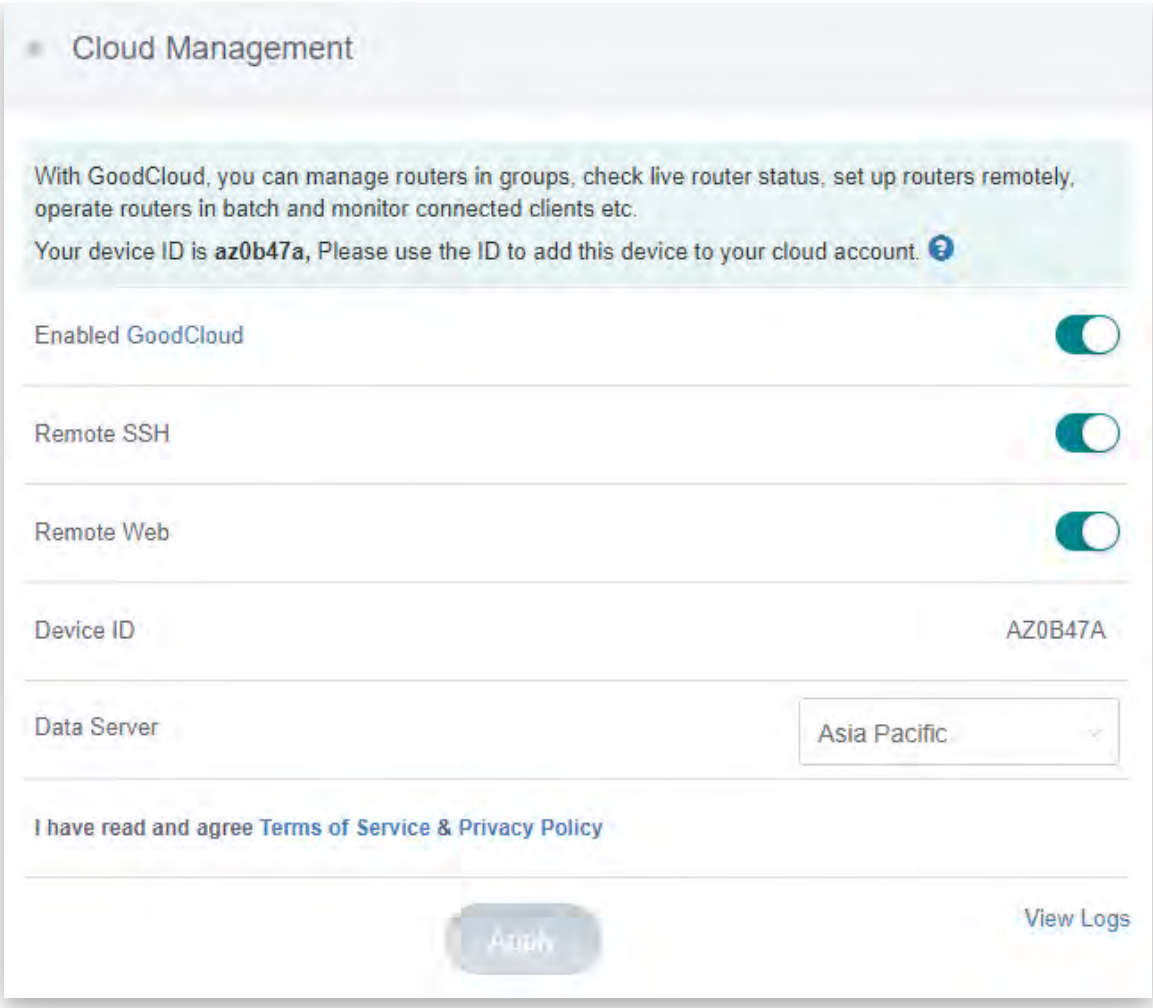


Nuage

Sur le côté gauche du panneau d'administration Web - APPLICATIONS - Accès à distance - Gestion des nuages

Les services **de gestion du cloud GL.iNet GoodCloud** fournissent un moyen simple et facile de gérer à distance des routeurs.

Veuillez vous référer à Cloud pour le détail.

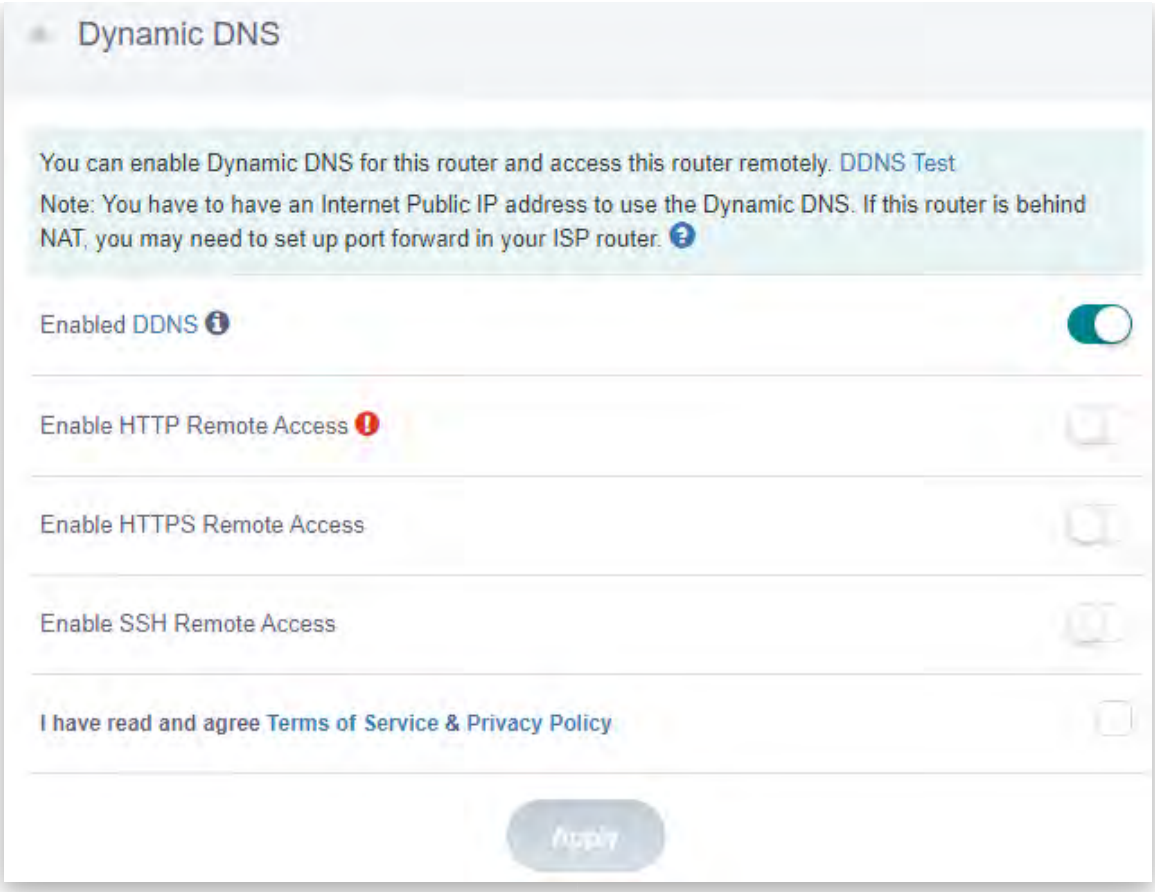


DDNS

Sur le côté gauche du panneau d'administration Web - APPLICATIONS - Accès à distance - DNS dynamique

Le service de noms de domaine dynamiques (DDNS) est un service utilisé pour cartographier un nom de domaine avec l'adresse IP dynamique d'un dispositif de réseau.

Veuillez vous référer au DDNS pour le détail.

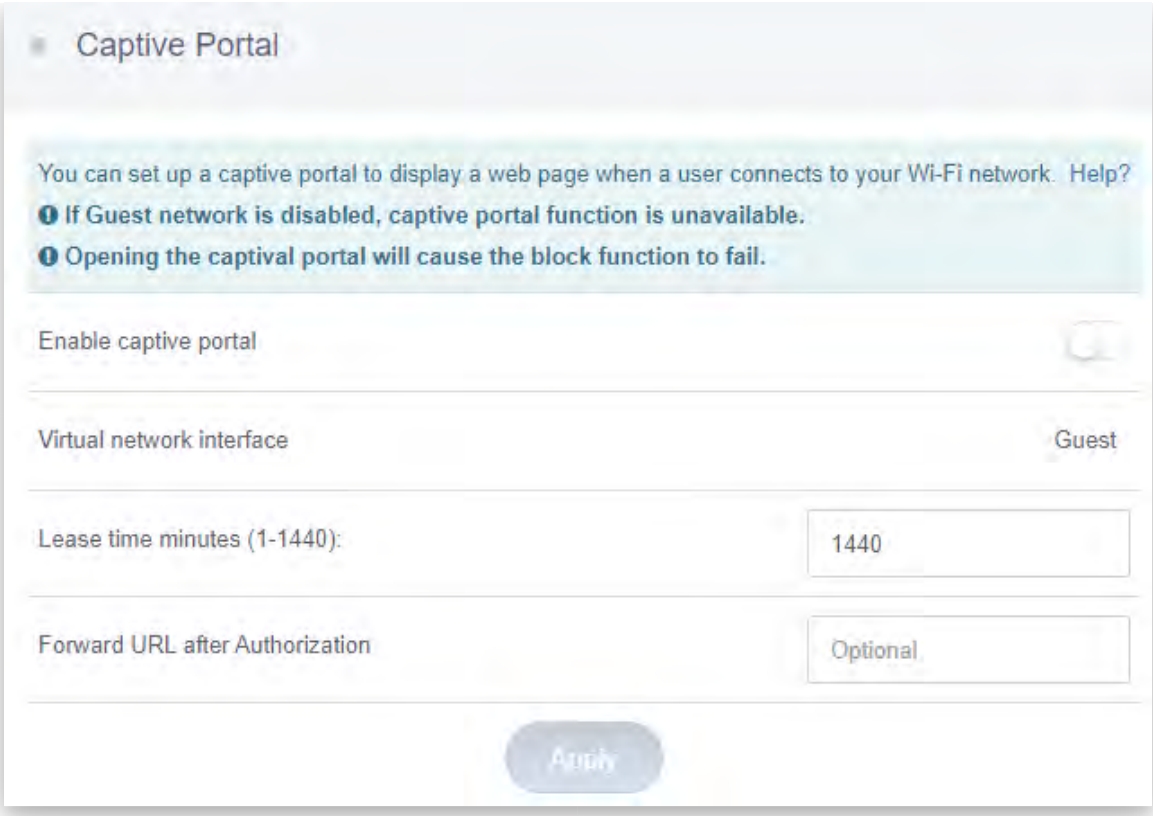


Portail captif

Sur le côté gauche du panneau d'administration Web - APPLICATIONS - Portail captif

Vous pouvez définir un **portail captif** dans nos routeurs, lorsque les nouveaux utilisateurs se connectent au Wi-Fi, ils doivent accéder à une page web avant d'accéder à Internet.

Veuillez vous reporter à la section Délimiter un portail Captif pour les détails.

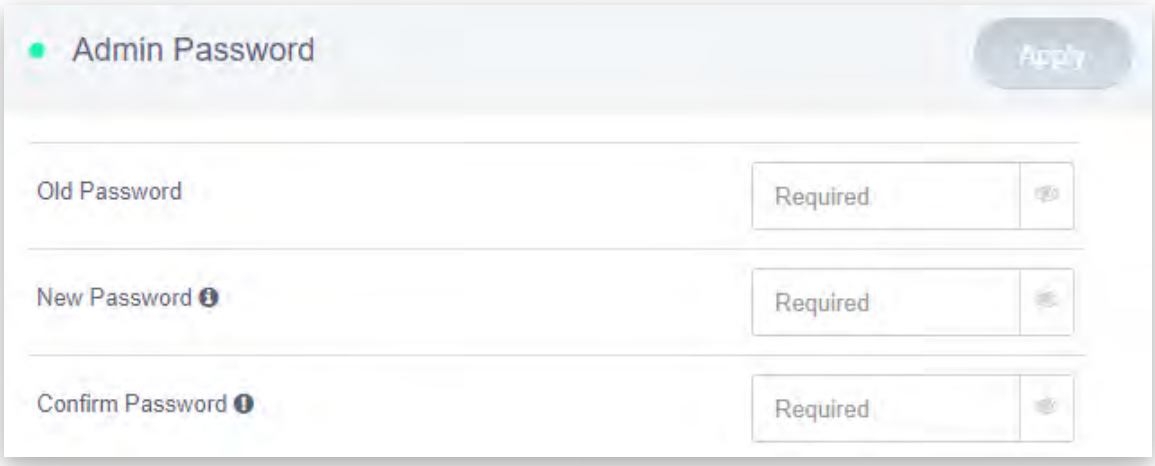

Captive Portal
You can set up a captive portal to display a web page when a user connects to your Wi-Fi network. Help?
If Guest network is disabled, captive portal function is unavailable.
Opening the captival portal will cause the block function to fail.
Enable captive portal
Virtual network interface
Guest
Lease time minutes (1-1440):
1440
Forward URL after Authorization
Optional
Apply

PLUS DE PARAMETRES

Mot de passe d'administration

Sur le côté gauche du panneau d'administration Web -

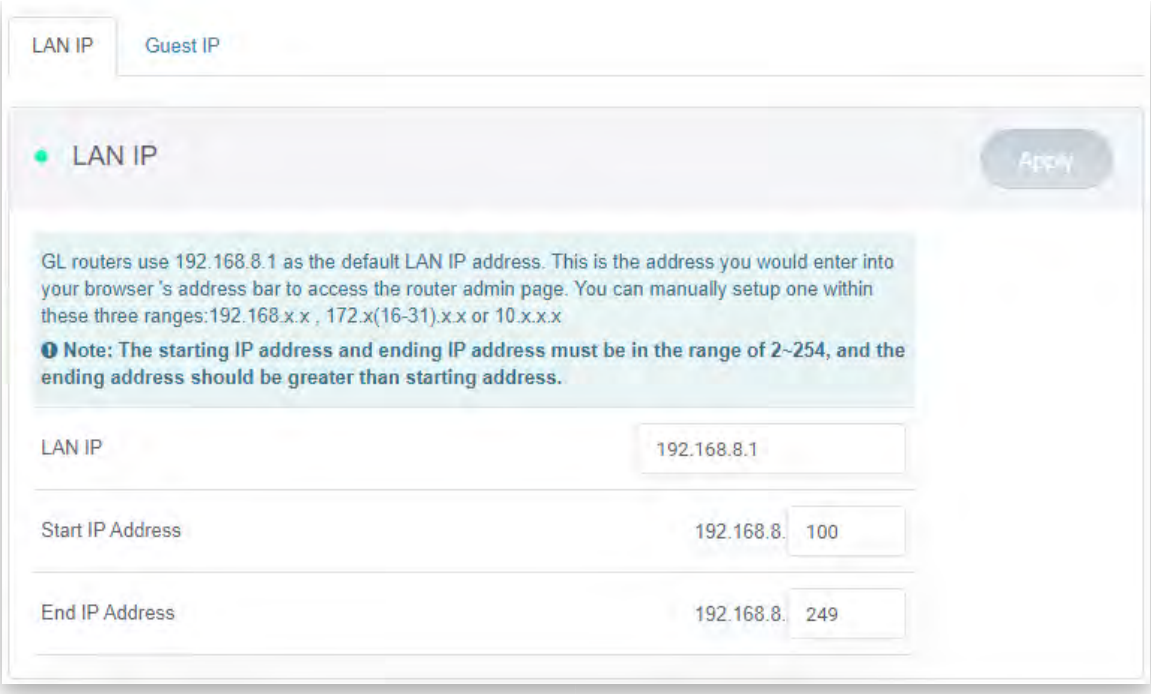
Changez le mot de passe du Groupe d'administration Web, qui doit comporter au moins 5 caractères. Vous devez entrer votre mot de passe actuel pour le modifier.



LAN IP

Sur le côté gauche du panneau d'administration web -

LAN IP est l'adresse IP que vous utilisez pour vous connecter à ce routeur. L'adresse IP par défaut du routeur GL.iNet est 192.168.8.1. Si cela est en conflit avec l'adresse IP de votre routeur principal, vous pouvez la changer.



L'adresse IP d'invité est l'adresse IP du Wi-Fi invité, par défaut est 192.168.9.1.

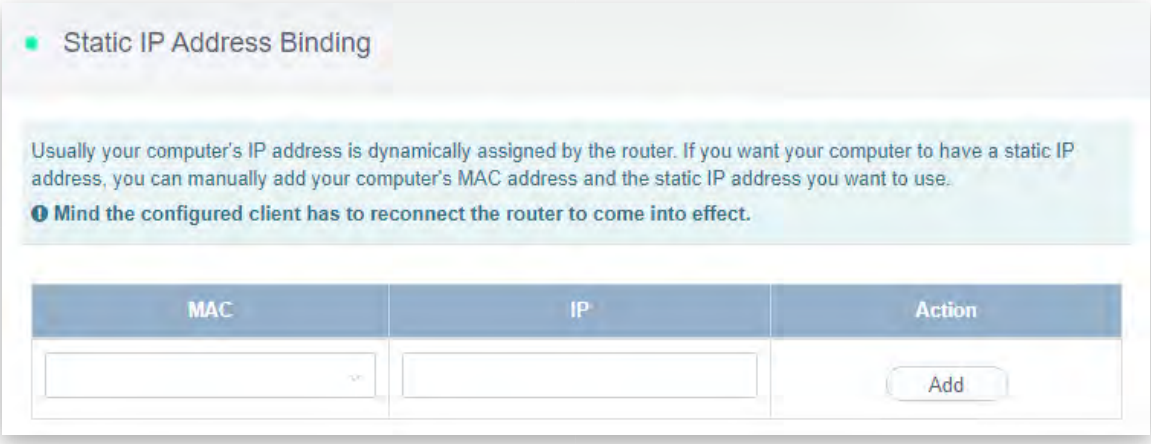


Liaison statique IP

Sur le côté gauche du panneau d'administration Web - SUIVRE SETTINGS - LAN IP - statique IP - Lièvre d'adresse IP statique

Habituellement, l'adresse IP de votre ordinateur est attribuée dynamiquement par le routeur. Si

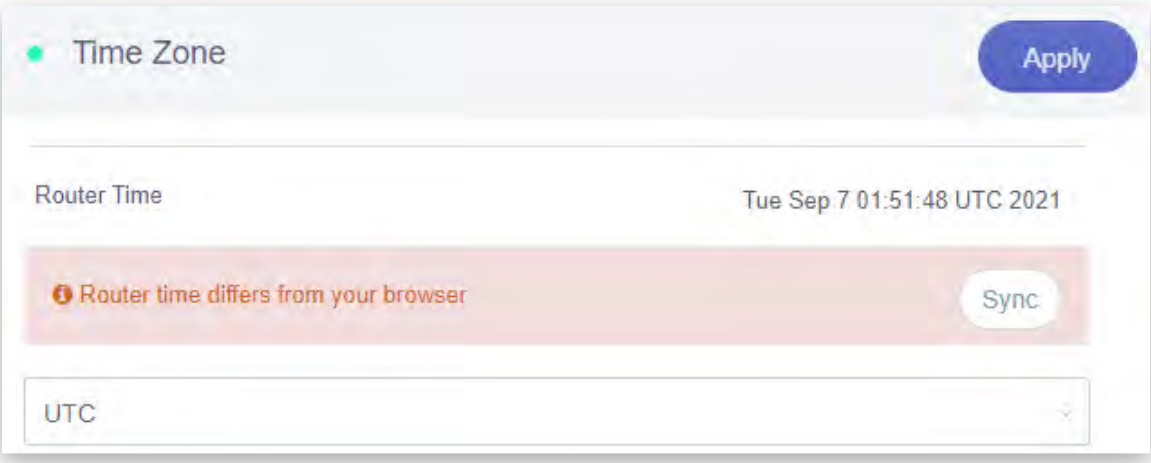
vous voulez que votre ordinateur ait une adresse IP statique, vous pouvez ajouter manuellement l'adresse MAC de votre ordinateur et l'adresse IP statique que vous souhaitez utiliser. Notez que le client configuré doit reconnecter le routeur pour prendre effet.



Durée du temps

Sur le côté gauche du panneau d'administration web - SUIVRE SETTINGS - 'Temps 'zone

L'heure des activités du routeur sera enregistrée en fonction du temps du routeur. Par conséquent, il est recommandé de choisir le fuseau horaire de votre emplacement.

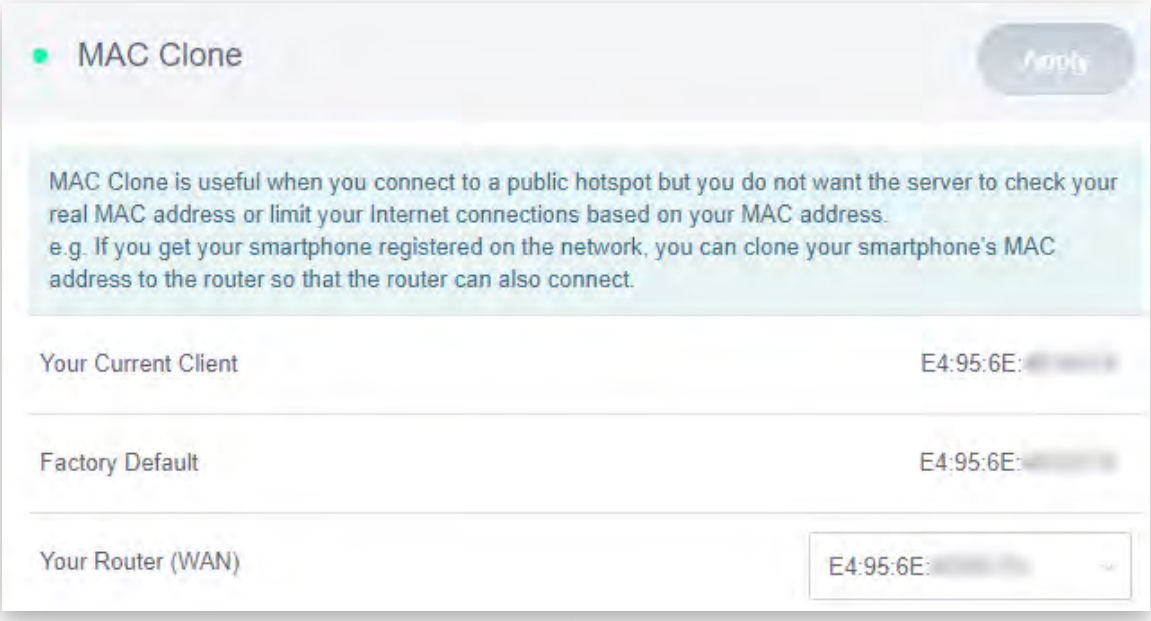


Cône MAC

Sur le côté gauche du panneau d'administration web - SUIVRE SETTINGS -

Cultez l'adresse MAC de votre client actuel au routeur. Il est utilisé en particulier à l'hôtel lorsque le réseau vérifie votre adresse MAC. Par exemple, si votre smartphone est enregistré sur le réseau, vous pouvez cloner l'adresse MAC de votre smartphone au routeur afin que le

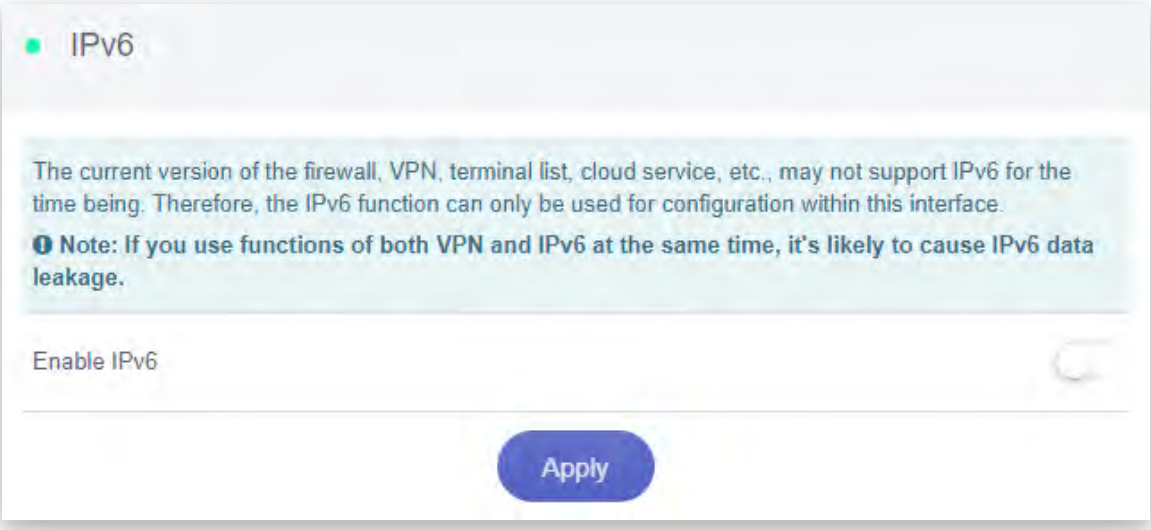
routeur puisse également se connecter au réseau.



IPv6

Sur le côté gauche du panneau d'administration web - . . . . . .

Veuillez vous reporter à IPv6 pour le détail.



Serveur DNS personnalisé

Sur le côté gauche du panneau d'administration web - PLUS D'ÉTABLISSEMENTS - Serveur DNS personnalisé

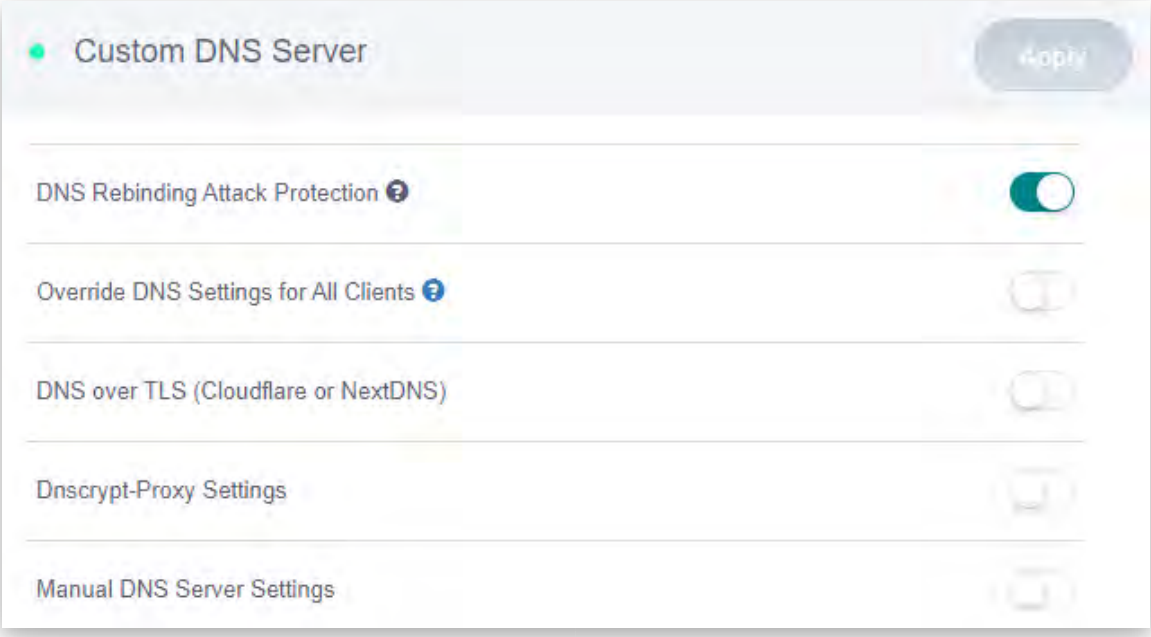
Vous pouvez configurer le serveur DNS du routeur afin d'empêcher la fuite du DNS ou à d'autres fins.

DNS Rebinding Attack Protection: Certains réseaux peuvent nécessiter une authentification dans le portail captif. Désactivez cette option si le portail captif de votre réseau ne peut pas être résolu.

Rédiger les paramètres DNS pour tous les clients : l'activation **de** cette option permettra de saisir la demande DNS de tous les clients connectés.

DNS sur TLS (Cloudflare ou NextDNS): **Cloudflare DNS** over TLS utilise le protocole de sécurité TLS pour chiffrer les requêtes DNS, ce qui contribue à augmenter la confidentialité et à empêcher l'écoute. **NextDNS** protège contre toutes sortes de menaces de sécurité, bloque les publicités et les traqueurs dans les sites web et les applications et fournit un Internet sûr et surveillé pour les enfants. S'il vous plaît allez à **NextDNS** pour les détails des paramètres.

Paramètres de serveurs DNS manuels : input un serveur DNS personnalisé manuellement.



Paramètres du bouton

Configurer la fonction du commutateur de mode. Il n'a pas de fonction par défaut. Vous pouvez le paramétrer comme une bascule pour activer ou désactiver le client WireGuard/OpenVPN.



Mode réseau

Sur le côté gauche du panneau d'administration web - . . . . . .

Changez le mode réseau pour répondre à votre scénario d'utilisation. Vous devrez peut-être reconnecter votre appareil client chaque fois que vous changez de mode réseau du routeur.

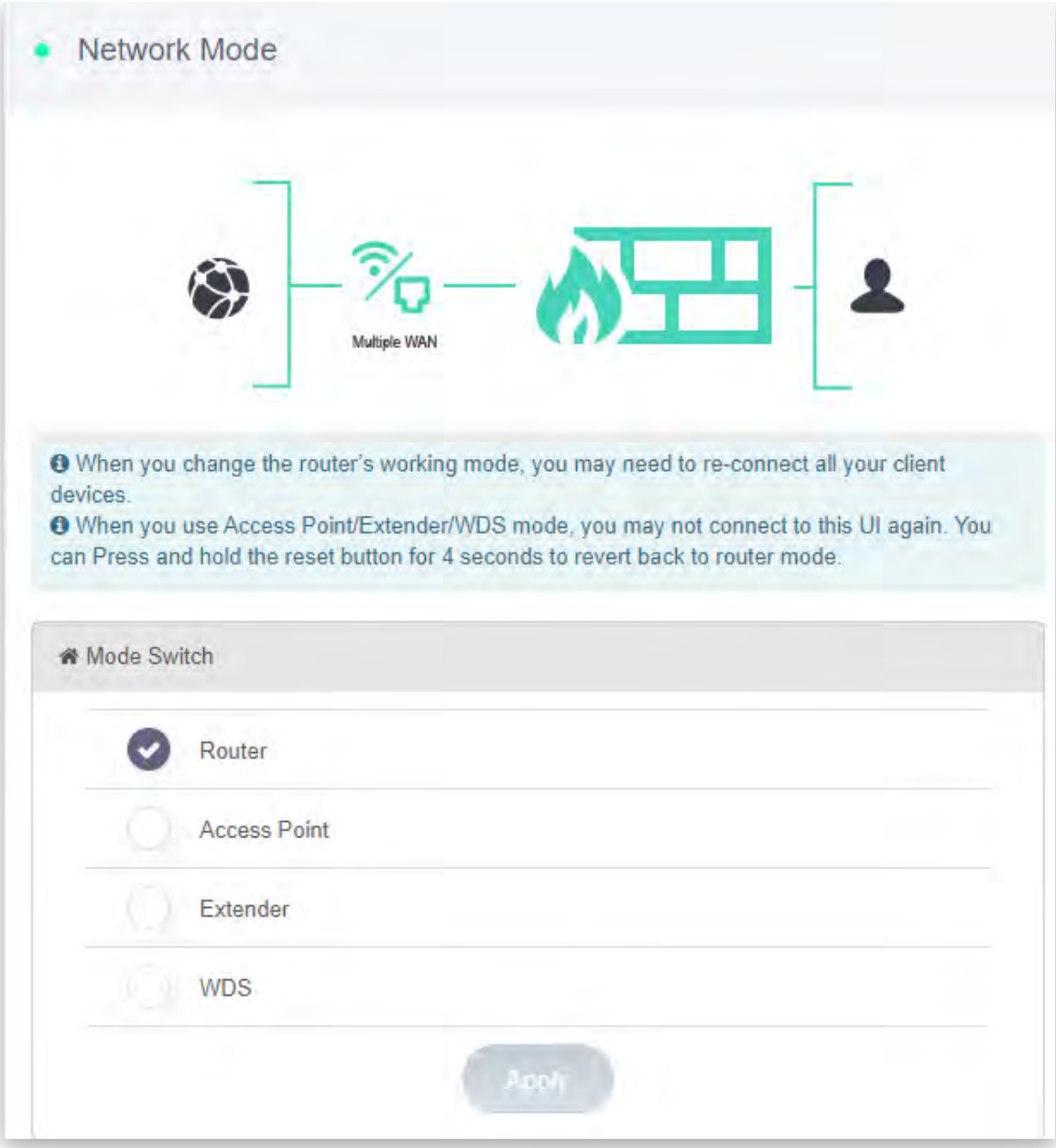
Sachez que vous ne pouvez pas accéder au panneau d'administration Web avec le IP 192.168.8.1 par défaut si vous utilisez le routeur en mode **Point d'Accès**, **Extender** ou **WDS**. Si vous voulez accéder au panneau d'administration web dans ce cas, vous devez utiliser l'adresse IP attribuée par le routeur principal au routeur GL.iNet.

Router : Créez votre propre réseau privé. Le routeur agira en tant que NAT, pare-feu et serveur DHCP.

Point d'accès: se connecter à un réseau filaire et diffuser un réseau sans fil.

ExtenderExtender: Étendre la couverture Wi-Fi d'un réseau sans fil existant.

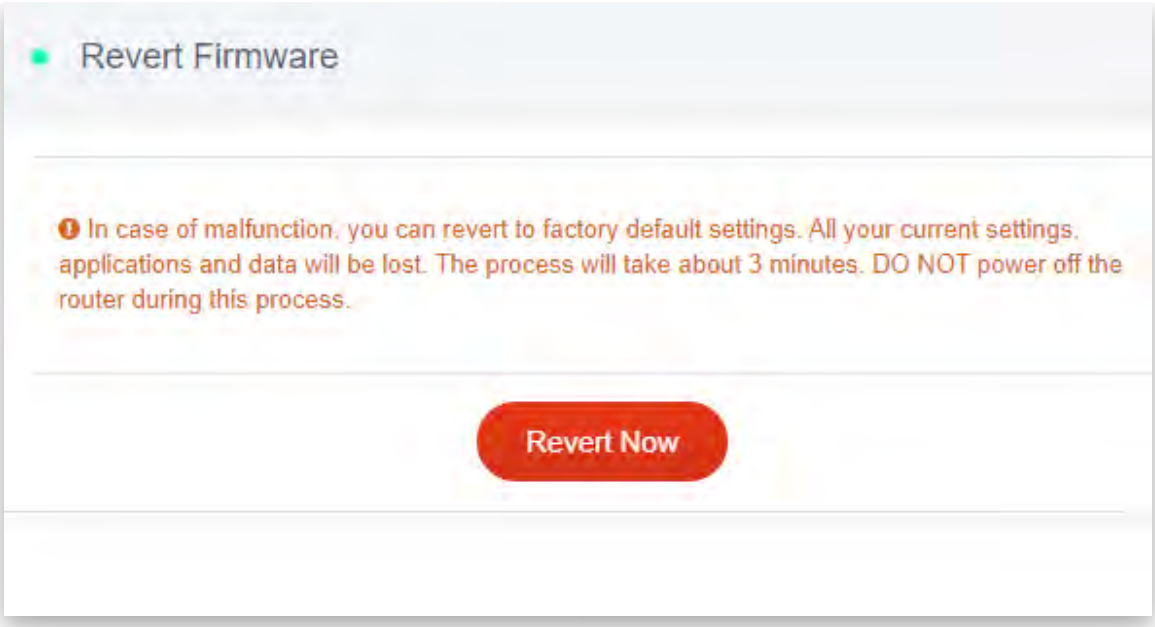
WDS : Similaire à l'Extenseur, veuillez choisir WDS si votre routeur principal prend en charge le mode WDS.



Firmware de redémarrage

Sur le côté gauche du panneau d'administration web - . . . . . .

Retournez le routeur aux paramètres par défaut de l'usine. Tous vos paramètres, applications et données seront effacés.

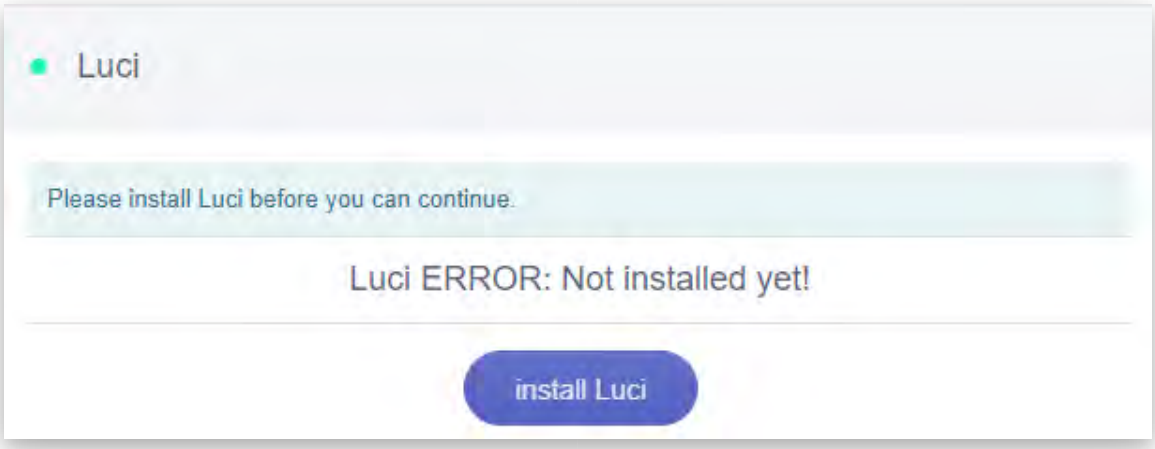


Avancé

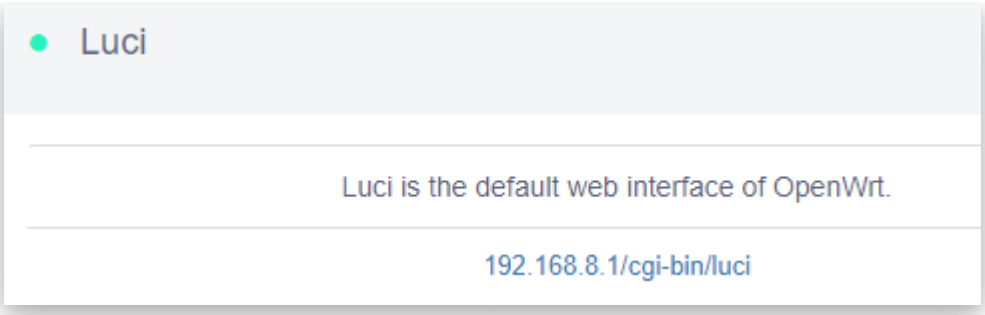
Sur le côté gauche du panneau d'administration Web

`Advanced` est pour LuCI, qui est l'interface web par défaut d'OpenWrt. Vous pouvez vérifier le journal du système détaillé ou y conduire des configurations plus avancées.

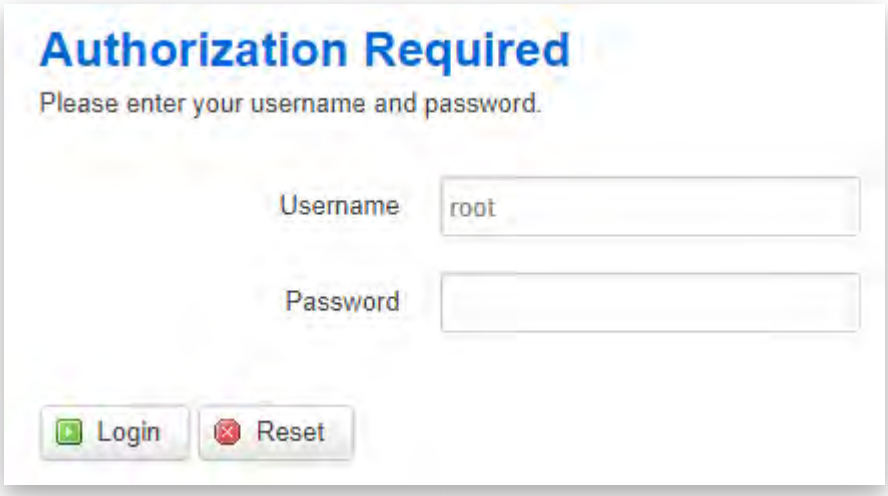
Pour certains modèles, LuCI n'est pas préinstallé, cliquez sur `Install LuCI` continuer.



Après installer.



Cliquez sur le `192.168.8.1/cgi-bin/luci` irons sur la page de connexion LuCI.



Remarque: Le nom d'utilisateur est root. Le mot de passe est le même que celui que vous utilisez pour accéder au panneau d'administration Web.