GL·iNet



Manual de usuario

GL-X3000 / Spitz AX

Enrutador celular Wi-Fi 6 Dual-SIM 4G/5G

Versión de firmware 4.8.3

Acerca de este manual

Este manual es su recurso de referencia para comenzar a usar su dispositivo, y cubre información básica del producto, conexiones de hardware, inicio de sesión en la interfaz de administración web, configuración inicial e instrucciones detalladas para todas las funciones del software en el panel de administración web.

Con esta guía, podrá:

- Comprender los detalles clave del producto
- Completar las conexiones de hardware siguiendo las instrucciones paso a paso
- Iniciar sesión fácilmente en la interfaz de administración web
- Configurar los ajustes iniciales y conocer todas las funciones del software en el panel de administración web

Convenciones de formato

Estos símbolos y colores le ayudarán a seguir los pasos con mayor rapidez.

Convención	Qué significa
Texto verde azulado subrayado	Enlace en el que se puede hacer clic y que puede abrir una página web o una sección específica
Texto en negrita	Enfatiza o marca alguna información clave en este documento, como títulos, hipervínculos y nombres exactos de menú/elementos en la interfaz web del dispositivo
>	La ruta para cargar la página correspondiente (por ejemplo, Sistema > Firmware)
Nota	Información clave para configuración, operaciones y seguridad. Ignorar esto podría provocar fallos en la configuración, mal funcionamiento del dispositivo o daños
Consejos	Consejos para aprovechar mejor su dispositivo

Nota:

- Las características del dispositivo pueden variar según el modelo y la versión de firmware.
- La disponibilidad del producto está sujeta a diferencias regionales o especificaciones del ISP.
- Todas las imágenes, procedimientos y descripciones de esta guía tienen fines ilustrativos únicamente y pueden diferir de su experiencia de uso real.

¿Necesita más ayuda o información?

- Actualización de firmware: Centro de descarga de firmware GL.iNet | Enrutador
- Comunidad: analice nuestros productos y comparta ideas en Foro de la comunidad GL.iNet
- Soporte técnico: comuníquese con nuestro soporte técnico en Página de contacto

Copyright © 2026 GL.iNet Technology (HK) Ltd. Todos los derechos reservados.
Ninguna parte de este manual puede reproducirse, transcribirse, traducirse o distribuirse de ninguna forma ni por ningún medio, sin el permiso previo por escrito de GL.iNet Technology (HK) Ltd. GL.iNet es una marca registrada de GL.iNet Technology (Hong Kong) Ltd. en China y/u otros países y regiones. Todas las demás marcas y nombres de productos mencionados aquí son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios. El contenido de este documento está sujeto a cambios sin previo aviso debido a actualizaciones de versión del producto u otros motivos. A menos que se acuerde lo contrario, este documento se proporciona únicamente con fines informativos y todas las declaraciones, información y recomendaciones contenidas en este documento no constituyen ningún tipo de garantía.

GL Tech (HK) Ltd: #601, 5W, Parque Científico de Hong Kong, N.T. Hong Kong
GL Intelligence, Inc.: 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Contenido

Capítulo 1 Conozca su enrutador 9

1.1 Descripción general del producto 10

1.1.1 Apariencia 10

1.1.2 Interfaz y botón 11

1.1.3 LED 12

1.2 Especificaciones 13

1.3 Contenido del paquete 14

Capítulo 2 Conexión de hardware 15

2.1 Elección de una ubicación 16

2.2 Conexión del enrutador 16

Capítulo 3 Iniciar sesión en el enrutador 17

Capítulo 4 Configurar la conexión a Internet 19

4.1 Asistente de configuración rápida 20

4.2 Configurar manualmente la conexión a Internet 21

4.2.1 Conectarse a Internet mediante un cable Ethernet 21

4.2.2 Conectarse a Internet mediante una red Wi-Fi existente 27

4.2.3 Conectarse a Internet mediante conexión compartida por USB 40

4.2.4 Conectarse a Internet mediante la red móvil 44

Capítulo 5 Red inalámbrica 66

5.1 Visualización del estado de Wi-Fi 67

5.2 Configuración inalámbrica 68

5.2.1 Wi-Fi de 5 GHz 68

5.2.2 Wi-Fi de 2,4 GHz 70

5.2.3 BSSID aleatorio 72

Capítulo 6 Clientes 74

6.1 Detalles del dispositivo 75

6.2 Acción 78

6.3 Eliminar clientes 81

6.4 Ordenar 81

Capítulo 7 Servicios en la nube 82

7.1 GoodCloud 83

7.1.1 Habilitar GoodCloud..... 84
7.1.2 Administrar el enrutador.....86
7.1.3 Desvincular el dispositivo..... 91
7.1.4 Desactivar GoodCloud..... 91
7.2 AstroWarp.....92
Capítulo 8 Conozca la VPN..... 93
8.1 Introducción.....94
8.1.1 VPN..... 94
8.1.2 Enrutador VPN..... 94
8.1.3 OpenVPN..... 94
8.1.4 WireGuard..... 94
8.2 Escenarios de aplicación..... 95
Capítulo 9 Panel de VPN.....97
9.1 Asistente de configuración de VPN.....98
9.2 Modo VPN..... 101
9.2.1 Modo global..... 102
9.2.2 Modo de política.....103
Capítulo 10 Configurar el servidor VPN..... 113
10.1 Servidor OpenVPN..... 114
10.1.1 Preparación..... 114
10.1.2 Pasos de configuración..... 115
10.1.3 Verificar conexión..... 118
10.1.4 Opciones del servidor..... 119
10.1.5 Comunicación entre clientes.....120
10.2 Servidor WireGuard.....122
10.2.1 Preparación..... 122
10.2.2 Pasos de configuración..... 123
10.2.3 Verificar conexión..... 127
10.2.4 Opciones del servidor..... 128
Capítulo 11 Configurar el cliente VPN..... 130
11.1 Cliente OpenVPN.....131
11.1.1 Preparación..... 131
11.1.2 Configurar NordVPN..... 131
11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores).....137

11.2 Configurar el cliente WireGuard 140
11.2.1 Preparación 140
11.2.2 Configurar AzireVPN 141
11.2.3 Configurar Hide.me 145
11.2.4 Configurar IPVanish 148
11.2.5 Configurar Mullvad 152
11.2.6 Configurar NordVPN 156
11.2.7 Configurar PIA (Private Internet Access) 161
11.2.8 Configurar Surfshark 165
11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores) 169
Capítulo 12 Tor 174
Capítulo 13 Aplicaciones 176
13.1 Complementos 177
13.2 DNS dinámico 178
13.2.1 Habilitar DDNS 178
13.2.2 Comprobar si DDNS funciona 181
13.2.3 Acceso remoto HTTPS 183
13.2.4 Acceso remoto SSH 185
13.3 Almacenamiento en red 187
13.3.1 Conectar una unidad de almacenamiento 187
13.3.2 Configurar Samba 188
13.3.3 Configurar WebDAV 191
13.3.4 Configurar DLNA 194
13.4 AdGuard Home 195
13.5 Control parental 197
13.5.1 Configuración rápida 197
13.5.2 Solución de problemas 205
13.6 ZeroTier 206
13.6.1 Configurar ZeroTier 207
13.6.2 Permitir el acceso remoto a la WAN 211
13.6.3 Permitir el acceso remoto a la LAN 212
13.7 Tailscale 213
13.7.1 Configurar Tailscale 214
13.7.2 Permitir el acceso remoto a la WAN 217

13.7.3 Permitir el acceso remoto a la LAN....218
13.7.4 Nodos de salida personalizados....219
13.8 Gestión de eSIM....221
13.8.1 Estado actual de la eSIM....222
13.8.2 Lista de perfiles eSIM....223
Capítulo 14 Red....230
14.1 Reenvío de puertos....231
14.1.1 DMZ....231
14.1.2 Reenvío de puertos....233
14.2 Multi-WAN....235
14.2.1 Seguimiento del estado de la interfaz....235
14.2.2 Modo Multi-WAN....238
14.3 LAN....241
14.3.1 Configuración básica....241
14.3.2 Servidor DHCP....242
14.3.3 Reserva de direcciones....244
14.4 Red de invitados....245
14.4.1 Configuración básica....245
14.4.2 Servidor DHCP....246
14.5 DNS....248
14.5.1 Configuración general....249
14.5.2 Configuración del servidor DNS....250
14.5.3 Editar hosts....252
14.6 Puerto Ethernet....253
14.7 Modo de red....254
14.8 IPv6....257
14.8.1 Modo IPv6....258
14.8.2 Método de obtención de DNS....258
14.9 Puerta de enlace directa....259
14.10 Inspección IGMP....261
14.11 Aceleración de red....262
14.12 Configuración NAT....264
Capítulo 15 Sistema....265
15.1 Descripción general....266

15.2 Actualización....267
15.2.1 Actualización de firmware en línea....267
15.2.2 Actualización local de firmware....268
15.2.3 Actualización en línea del módem....270
15.2.4 Actualización local del módem....270
15.3 Tareas programadas....271
15.3.1 Programación de los indicadores LED....271
15.3.2 Programar reinicio....272
15.3.3 Programación de Wi-Fi de 5 GHz....272
15.3.4 Programación de Wi-Fi de 2,4 GHz....274
15.4 Zona horaria....277
15.5 Registro....278
15.6 Seguridad....280
15.6.1 Contraseña de administrador....280
15.6.2 Control de acceso....281
15.6.3 Control de acceso remoto....284
15.6.4 Abrir puertos en el enrutador....285
15.7 Restablecer firmware....286
15.8 Configuración avanzada....287
Declaración de Conformidad....289

Capítulo 1

Conozca su enrutador

Este capítulo cubre la descripción general, las especificaciones y el contenido del paquete del enrutador.

1.1 Descripción general del producto

Spitz AX (GL-X3000) es una puerta de enlace celular Wi-Fi 6 de doble SIM diseñada para proporcionar conexiones rápidas y confiables, especialmente en áreas remotas y durante viajes por carretera. Ofrece cuatro métodos de acceso a Internet: Celular (tarjetas SIM), ethernet, repetidor y anclaje a red. Admite múltiples WAN (conmutación por error y equilibrio de carga), VPN (OpenVPN y WireGuard), controles parentales, AdGuard Home, reenvío de puertos, Tailscale y más.

1.1.1 Apariencia

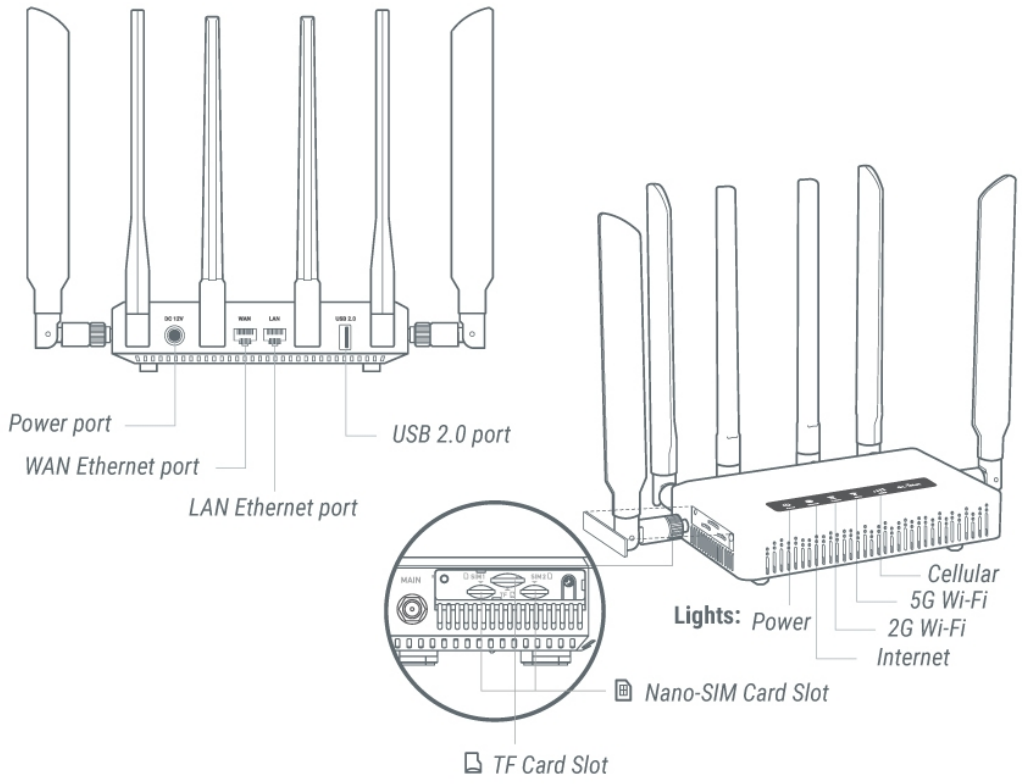








1.1.2 Interfaz y botón



Artículo	Definición
puerto Ethernet WAN	Conecta el enrutador a una red ascendente a 10/100/1000/2500Mbps.
Puerto LAN Ethernet	Conecta un cliente cableado al enrutador a 10/100/1000Mbps.
Puerto USB 2.0	Conecta un módem USB, un dispositivo de anclaje a red o un dispositivo de almacenamiento USB compatible.
Ranura para tarjeta MicroSD	Acepta una tarjeta MicroSD con una capacidad máxima de 1 TB.
Ranuras para tarjetas Nano SIM	Acepta dos tarjetas Nano SIM. Sólo hay una tarjeta SIM activa a la vez; el otro sirve como respaldo.

Botón de reinicio	Presione durante menos de 3 segundos para restablecer la red, o presione durante 10 segundos para restaurar la configuración de fábrica.
Entrada de alimentación DC5521	Acepta el adaptador de 12 V/2,5 A suministrado o una entrada de 9 ~ 36 V CC.
Conectores de antena celular	Conecte cuatro antenas celulares (SMA, 600 MHz~6 GHz).
Conectores de antena Wi-Fi	Conecte dos antenas Wi-Fi (PR-SMA, 2,4~2,5 GHz y 5,15~5,84 GHz).

1.1.3 LED

Estado del dispositivo	**Alimentación**	**Internet**	**2,4 GHz**	**5GHz**	**Celular**
Internet conectado (Celular activo)	Verde activado	Verde activado	Verde activado	Verde activado	Verde activado
Internet conectado (Celular inactivo)	Verde activado	Verde activado	Verde activado	Verde activado	Apagado
Sin Internet	Verde activado	Apagado	Verde activado	Verde activado	Apagado
Actualización de firmware	Verde activado	Parpadea cada 0,5 s	Parpadea cada 0,5 s	Parpadea cada 0,5 s	Verde activado
Restablecimiento de red (presione restablecer < 3s)	Parpadea cada 1s	Verde activado	Verde activado	Verde activado	Verde activado

Restablecimiento de fábrica (presione restablecer durante 10 segundos)	Parpadea cada 0,25 s	Verde activado	Verde activado	Verde activado	Verde activado

Consejos: Cuando está conectado a Internet, un LED parpadeante de 2,4 GHz o 5 GHz significa que los dispositivos Wi-Fi están conectados y transmitiendo datos activamente.

1.2 Especificaciones

Artículo	Detalles
Interfaz	1 x puerto Ethernet WAN 1 x puerto LAN Ethernet 1 x puerto USB 2.0 1 x ranura para tarjeta MicroSD (máx. 1 TB) 2 x ranuras para tarjeta Nano SIM 1 x botón de reinicio
CPU	MediaTek de doble núcleo, @1,3 GHz
Memoria/Almacenamiento	DDR4 512 MB / eMMC 8 GB
Protocolo	IEEE 802.11a/b/g/n/ac/ax
Velocidad de Wi-Fi	574Mbps (2,4 GHz), 2402 Mbps (5 GHz)
Velocidad de Ethernet	Puerto WAN: 10/100/1000/2500Mbps Puerto LAN: 10/100/1000Mbps
Antenas	4 x antenas celulares (SMA, 600M~6GHz) 2 x antenas Wi-Fi (PR-SMA, 2.4G~2.5GHz, 5.15~5.84GHz)
LED	Sistema / Wi-Fi 5G / Wi-Fi 2.4G / Internet / Intensidad de la señal celular
Entrada de energía	DC5521, 12V/2.5A (5.5*2.1mm) [adaptador predeterminado] / 9~36V

Consumo de energía	<14W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)
Dimensión/Peso	155 x 95 x 36 mm/520 g
Otras herramientas	Hoja de datos | Firmware | Aplicación | Unboxing | Tutoriales | Kit de medios

1.3 Contenido del paquete

- 1 x Spitz AX (GL-X3000)
- 1 manual de usuario
- 1 x Tarjeta de agradecimiento
- 1 cable Ethernet
- 1 x kit de montaje en pared
- 1 x adaptador de corriente
- 4 x convertidores



Capítulo 2

Conexión de hardware

Este capítulo cubre la selección de la ubicación del enrutador y la conexiónion pasos.

2.1 Elección de una ubicación

Siga estos consejos para elegir una ubicación para obtener el mejor rendimiento.

- Evite la humedad y el calor: no coloque el enrutador en áreas expuestas al agua, la humedad o altas temperaturas (por ejemplo, fregaderos, radiadores).
- Ventilación y refrigeración: coloque el enrutador en un área fresca y bien ventilada para una disipación adecuada del calor.
- Ubicación central: coloque el enrutador donde pueda conectarse a la alimentación y a varios dispositivos fácilmente (por ejemplo, la zona central de la sala de estar).
- Conveniencia con los cables: enrute los cables y el cable de alimentación de forma segura para evitar riesgos de tropiezos.
- Colocación: Coloque el enrutador en una superficie plana y estable (estante, escritorio) o móntelo en la pared usando el kit de montaje en pared incluido.
- Evitación de EMI: mantenga el enrutador alejado de fuentes de interferencias electromagnéticas (dispositivos Bluetooth, microondas) para minimizar la interferencia de la señal.

2.2 Conexión del enrutador

1. **Encendido**
   Junte el adaptador de corriente de dos piezas. Conéctelo al enrutador y conéctelo a una toma de corriente. Se iniciará automáticamente.
2. **Conecte un dispositivo al enrutador**
   Conecte un dispositivo (por ejemplo, una computadora portátil o un teléfono inteligente) al enrutador mediante Wi-Fi o un cable Ethernet.
   - **Wi-Fi:** En su dispositivo, vaya a Configuración >WLAN, ubique el nombre de la red Wi-Fi del enrutador en la lista de redes disponibles e ingrese la contraseña. Puede encontrar el nombre de red predeterminado y la contraseña impresos en la etiqueta de su enrutador.
   - **Ethernet:** Conecte su dispositivo al puerto LAN del enrutador mediante un cable Ethernet.
3. **Inicie sesión en el enrutador**
   Internet no está disponible cuando se conecta al enrutador por primera vez. Inicie sesión en el enrutador como se indica en el Capítulo 3 para completar la configuración inicial antes de acceder a Internet.

Capítulo 3

Iniciar sesión en el enrutador

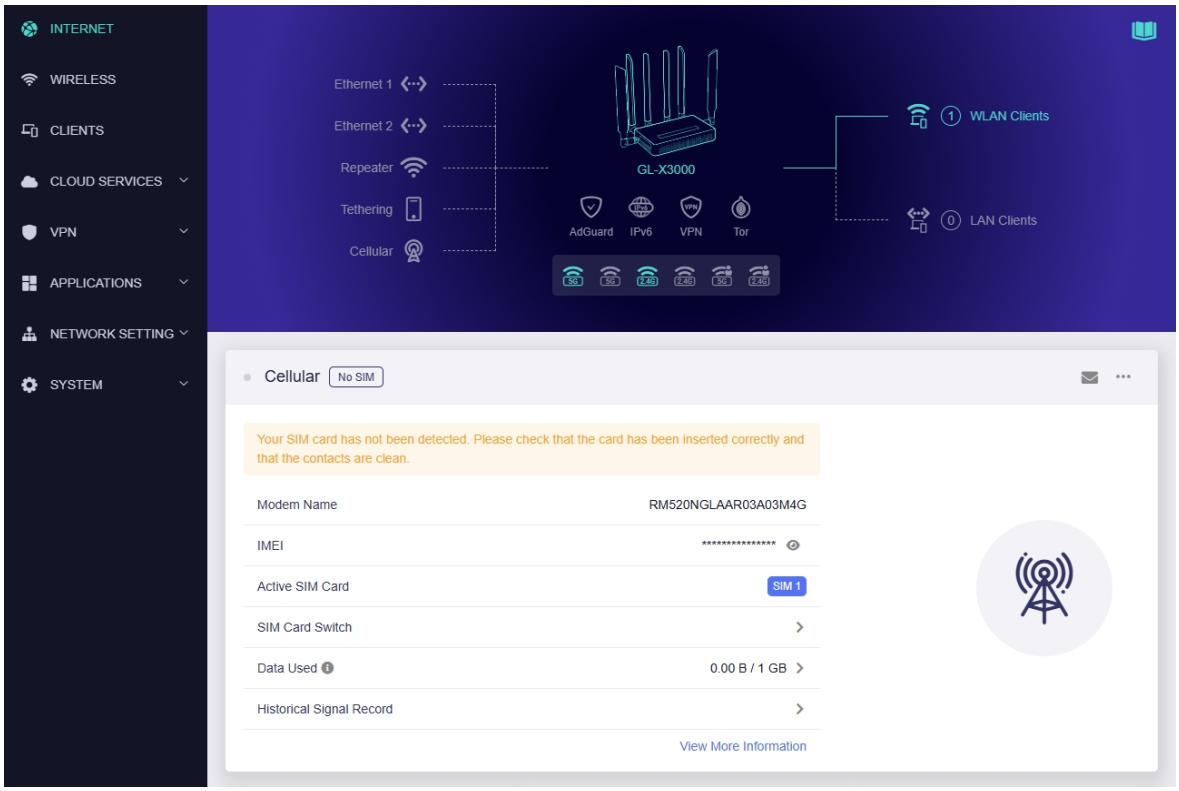
Este capítulo lo guía para iniciar sesión en su enrutador a través de panel de administración web.

Configure y administre su enrutador a través de una interfaz de administración basada en web, a la que se puede acceder desde cualquier sistema operativo Windows, Mac o Linux con un navegador web, como Microsoft Edge, Google Chrome, Mozilla Firefox o Apple Safari.

Nota: Si prefiere nosotrosing la aplicación GL.iNet en lugar de la panel de administración web, descarga la aplicación y sigue las indicaciones en pantalla.

Sigue los pasos a continuación para iniciar sesión in a su enrutador a través del panel de administración web.

1. Conecte un dispositivo (por ejemplo, una computadora o computadora portátil) al enrutador mediante Wi-Fi o un cable Ethernet.
2. Abrir un navegador web (se recomienda Chrome y Edge) y visita http://192.168.8.1. Se te dirigirá a la página de inicio de sesión del panel de administración web. Si no puede acceder al panel de administración web, consulte aquí para solución de problemas.
3. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Ylo luego ingrese al panel de administración web del enrutador'.



Capítulo 4

Configurar la conexión a Internet

Este capítulo presenta múltiples métodos de conexión a Internet para que el enrutador se adapte a diversos entornos de red.

4.1 Asistente de configuración rápida

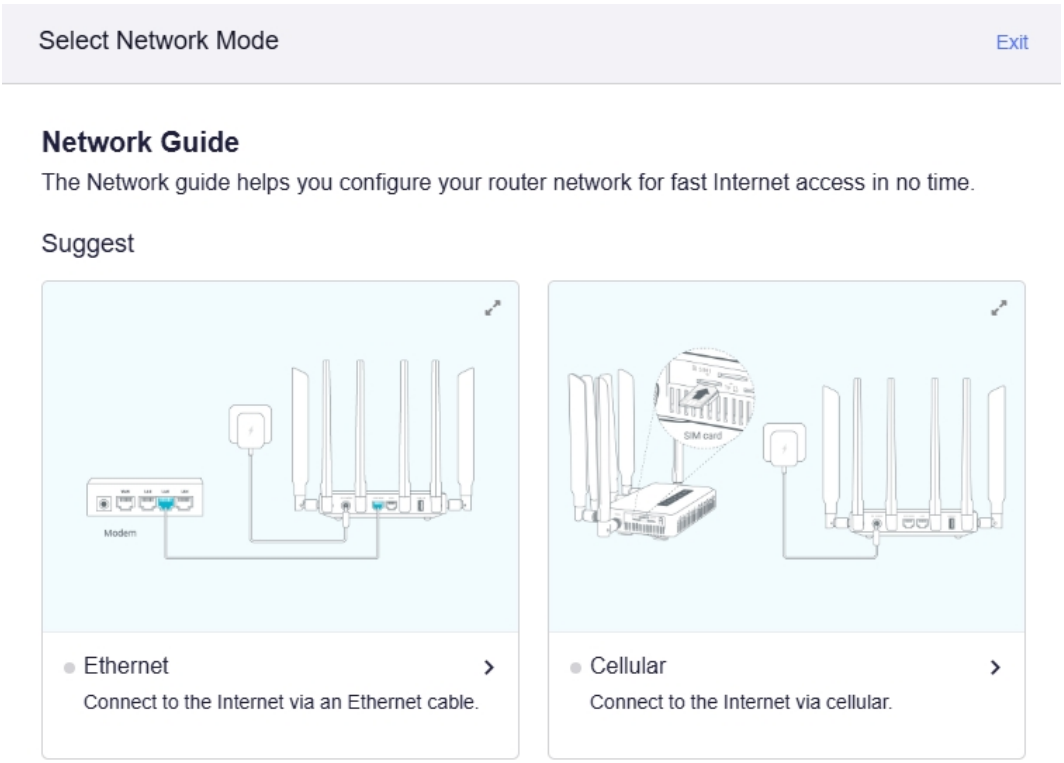
El asistente de configuración basado en web lo guiará a través de la configuración de red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

1. Inicie sesión en el panel de administración web del enrutador como se indica en Capítulo 3.
2. En el página de inicio, haga clic en el ícono del libro en la esquina superior derecha.



3. Siga el asistente de configuración para configurar su enrutador y establecer una conexión a Internet.



Si usa la aplicación GL.iNet, siga las indicaciones en pantalla para configurar el acceso a Internet.

4.2 Configurar manualmente la conexión a Internet

Si bien el asistente de configuración es conveniente para una configuración rápida de la red, la configuración manual le permite ajustar la configuración de red avanzada para requisitos específicos y verificar o modificar las conexiones existentes según corresponda. necesario.

Este enrutador admite cuatro métodos de conexión a Internet: Ethernet, repetidor, anclaje a red USB y celular. Elija el método adecuado según sus necesidades de uso.

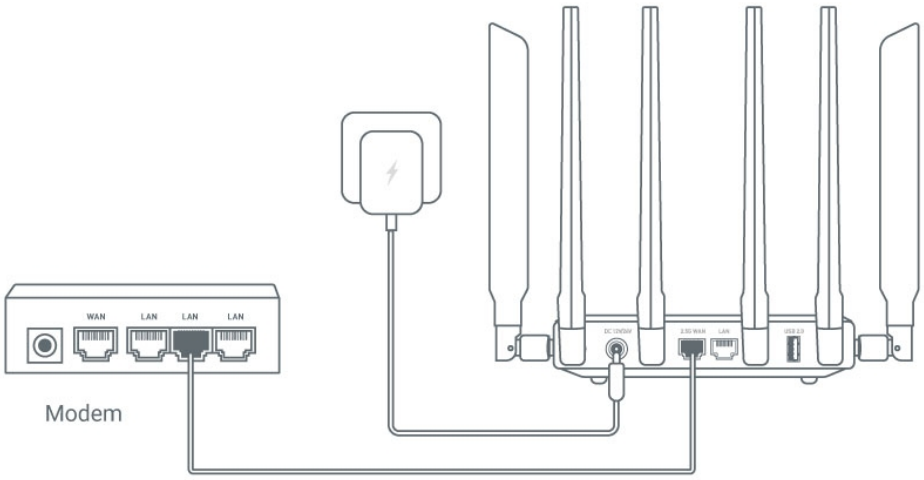
4.2.1 Conectarse a Internet mediante un cable Ethernet

Conecte el enrutador a una red de banda ancha mediante un cable Ethernet conectado al puerto WAN. Por lo general, adquiere automáticamente una dirección IP (DHCP). Los usuarios también pueden configurar IP estática o PPPoE manualmente. Este método ofrece alta estabilidad y alta velocidad, lo que lo hace ideal para entornos domésticos y de oficina con acceso de banda ancha fija.

4.2.1.1 Pasos básicos

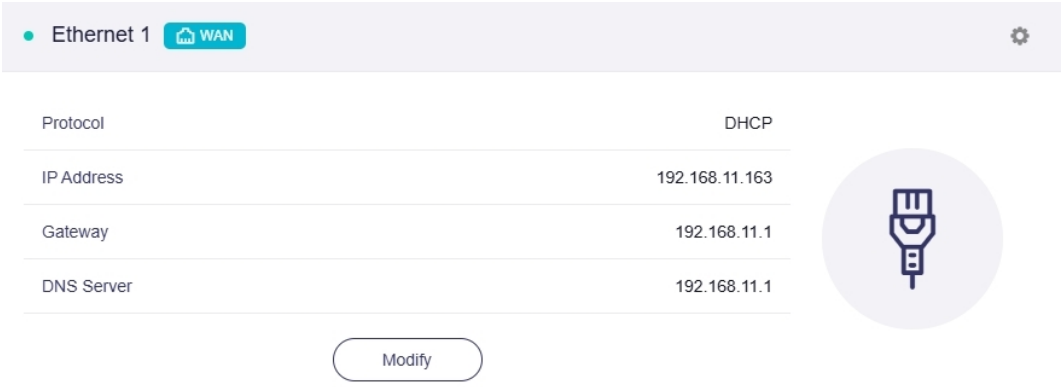
Siga los pasos a continuación para conectar su enrutador a Internet mediante un cable Ethernet.

1. Conecte el puerto WAN de su enrutador al dispositivo ascendente (por ejemplo, un módem ISP, enrutador, conmutador de red o un conector Ethernet) mediante un cable Ethernet.



2. Inicie sesión en el panel de administración web del enrutador, navegue hasta **INTERNET** > **Ethernet** sección.

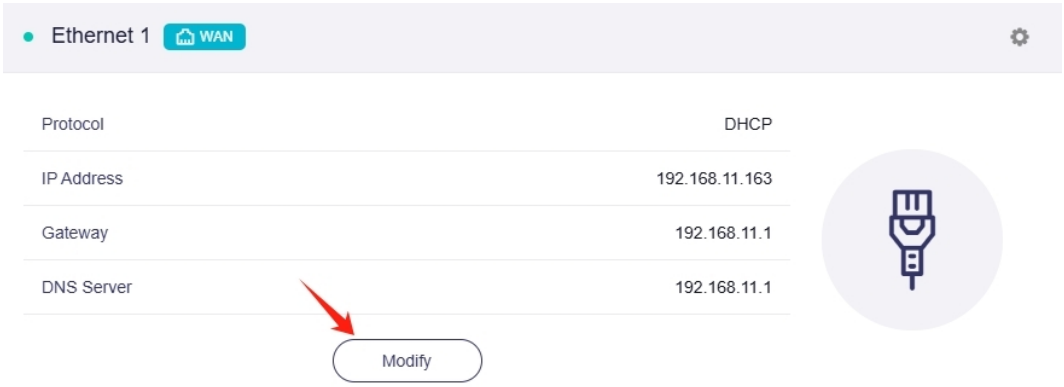
Si la conexión se realiza correctamente, la sección Ethernet mostrará los detalles de la red, incluidos el protocolo, la dirección IP, la puerta de enlace y el servidor DNS.



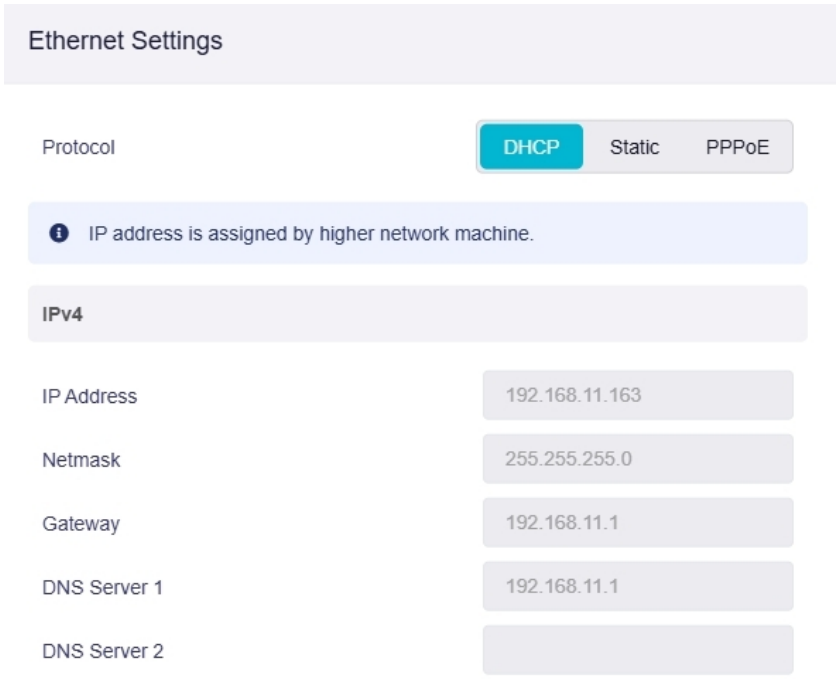
Consejos: Puede cambiar la función del puerto WAN como puerto LAN si es necesario. Esto es útil cuando utiliza el enrutador como repetidor ya que el puerto WAN físico está inactivo. Entonces tendrás un puerto LAN más.

4.2.1.2 Protocolo

Hay 3 tipos de protocolos, DHCP, Estático, PPPoE. Haga clic en **Modificar** para cambiar.

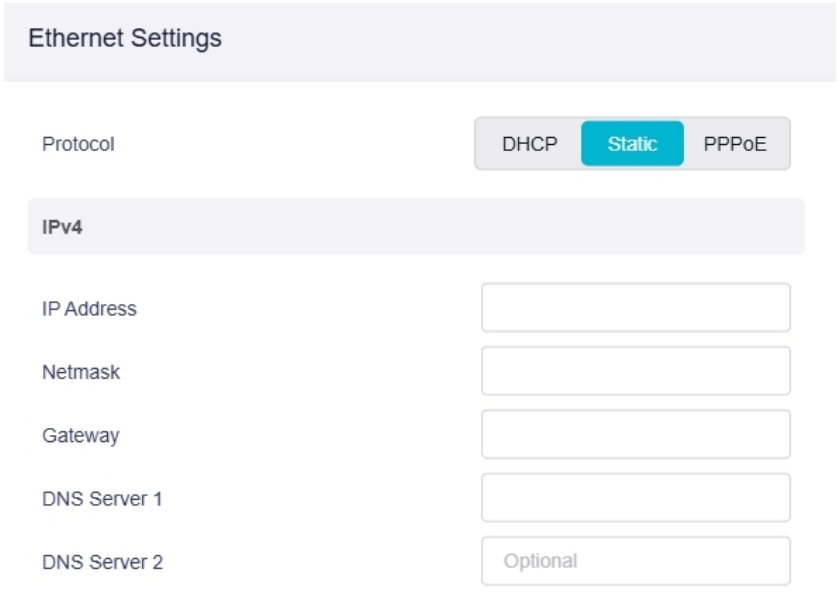


- **DHCP**
  DHCP es el protocolo predeterminado y más común, que asigna automáticamente direcciones IP y otros parámetros de comunicación a los dispositivos de red a través de una arquitectura cliente-servidor en redes IP.



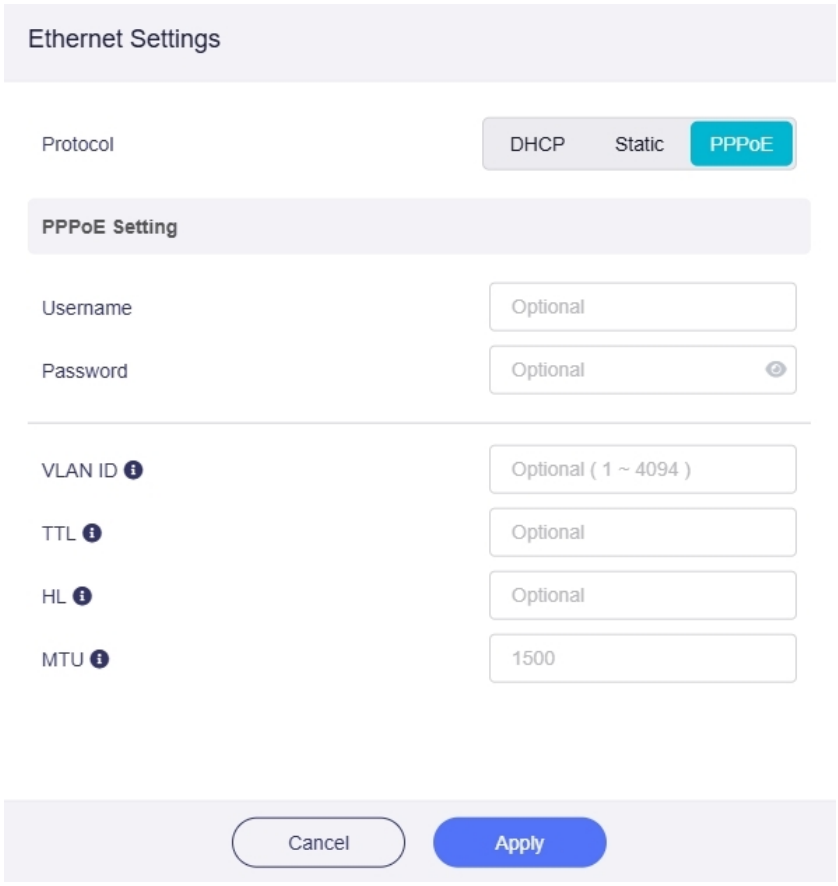
- **Estática**

  La estática es necesaria si su ISP (proveedor de servicios de Internet) proporciona una dirección IP fija o si desea configurar manualmente la información de la red, como la dirección IP, la puerta de enlace y la máscara de red.



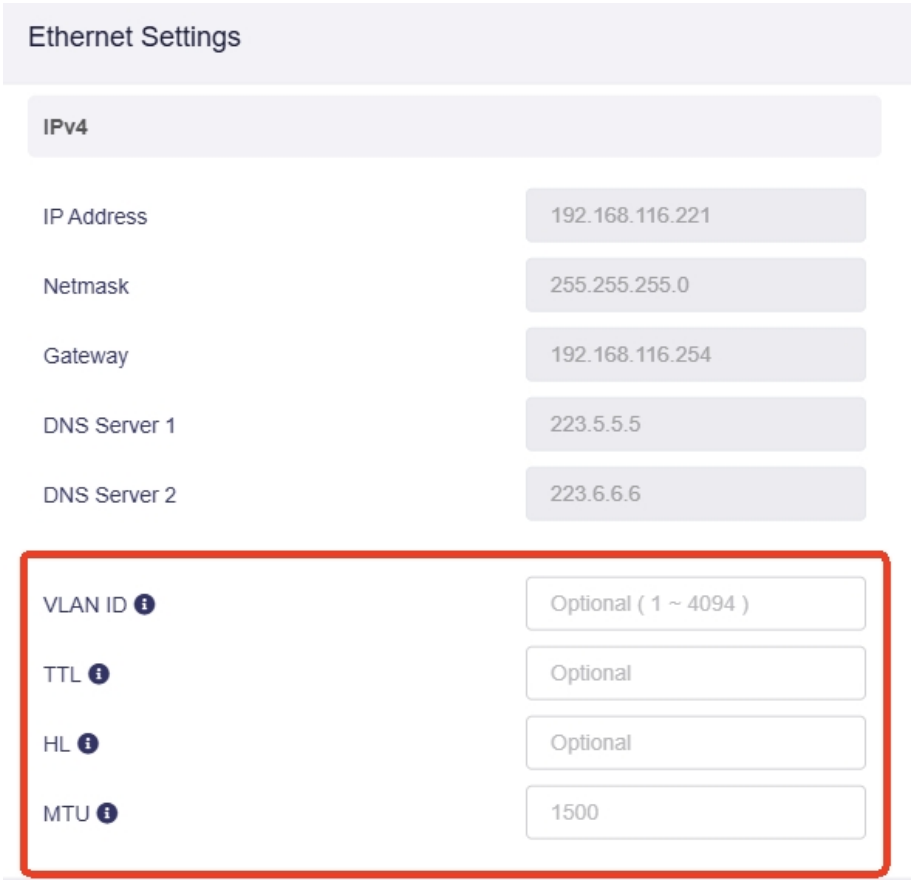
- **PPPoE**

  PPPoE es un protocolo utilizado por la mayoría de los ISP. Normalmente, proporcionan un módem y un nombre de usuario y contraseña, que son necesarios para la configuración de Internet.


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

4.2.1.3 Avanzado

Además de las configuraciones esenciales, también hay algunas configuraciones avanzadas opcionales para los tres protocolos anteriores.

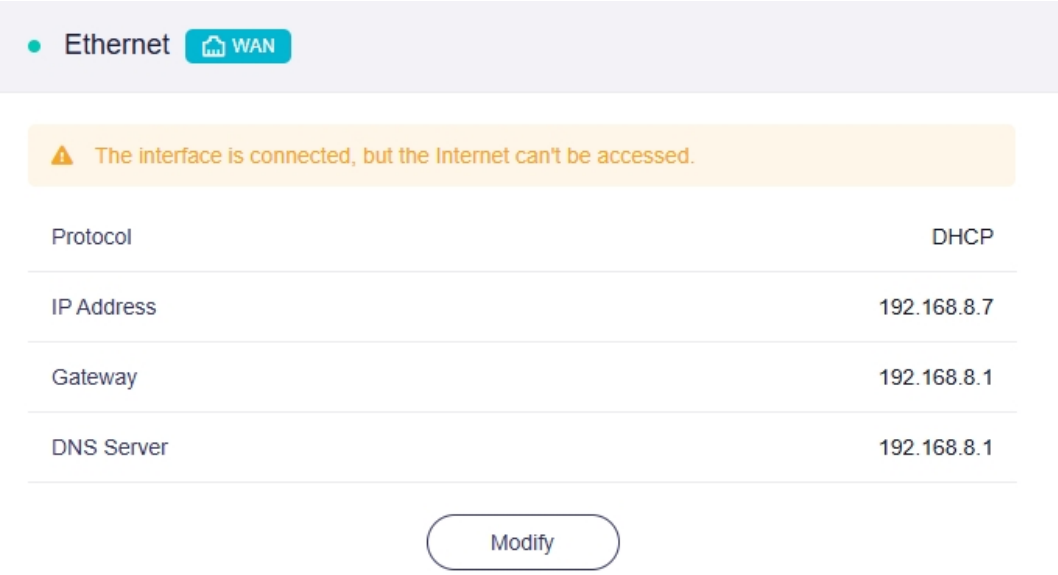


- **ID de VLAN**: esta entrada de configuración solo es necesaria si el servidor del proveedor' requiere la interfaz para usar un ID de VLAN etiquetado específico.
- **TTL**: TTL (tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. La configuración TTL es válida sólo para IPv4. Si necesita anular o falsificar el TTL, establezca un valor fijo aquí. Para la mayoría de los modelos, ingrese el TTL efectivo deseado más 1 para compensar la disminución automática.
- **HL**: en IPv6, el campo HL (límite de salto) limita el número de saltos de transmisión para paquetes de datos en la red, sirviendo como el equivalente de TTL en IPv4.
- **MTU**: el valor de MTU predeterminado es 1500 bytes.

4.2.1.4 Solución de problemas

Si un cable Ethernet Eestá conectado al puerto WAN pero Internet no está disponible, Se mostrará un mensaje amarillo como se muestra a continuación.

"La interfaz está conectada, pero no se puede acceder a Internet."

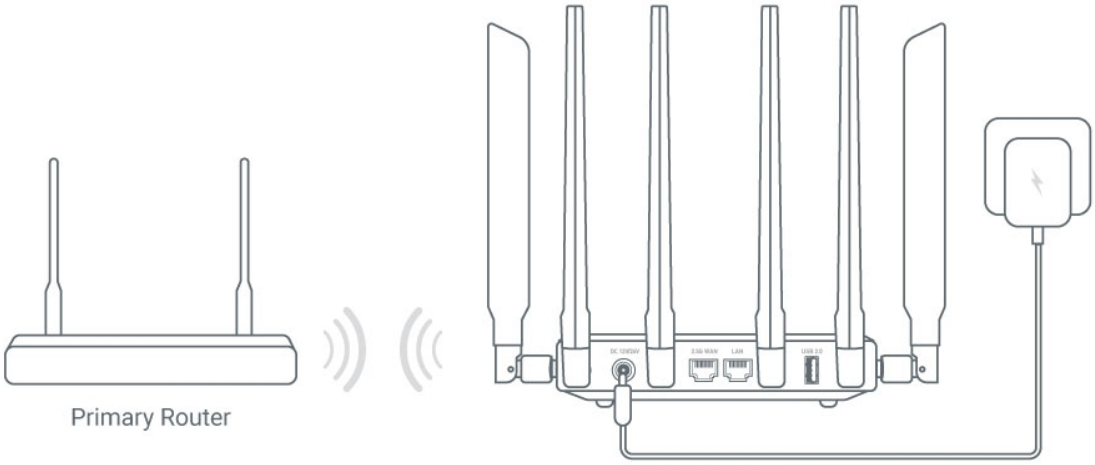


Para solucionar este problema:

1. Compruebe si el dispositivo ascendente tiene Internet acceso.
2. Vaya a la página Multi-WAN para verificar el estado de la interfaz Ethernet.

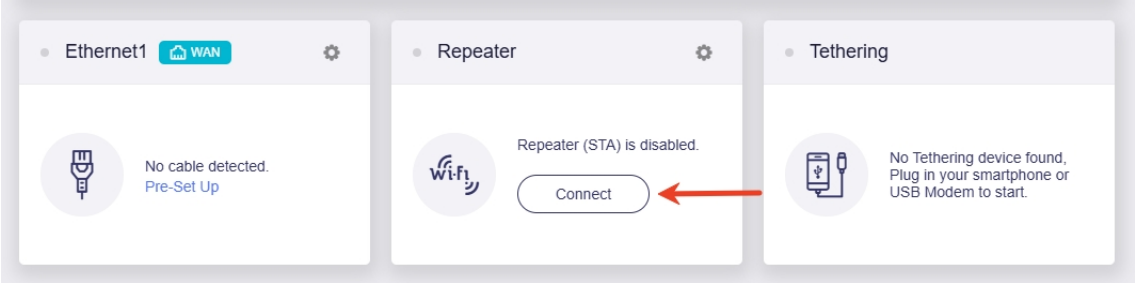
4.2.2 Conectarse a Internet mediante una red Wi-Fi existente

Usar un repetidor significa conectar el enrutador a otra red inalámbrica existente, p. cuando utiliza Wi-Fi gratuito en un hotel o cafetería. Funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

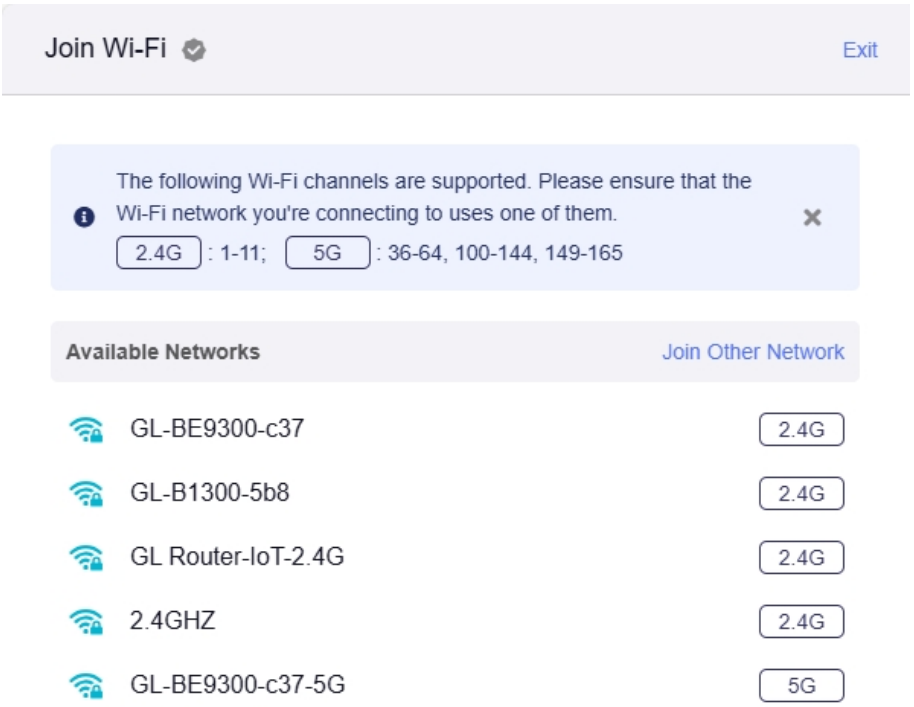


4.2.2.1 Pasos básicos

1. Inicie sesión en el panel de administración web del enrutador, navegue hasta la sección **INTERNET** > **Repetidor**, y haga clic en **Conectar**.



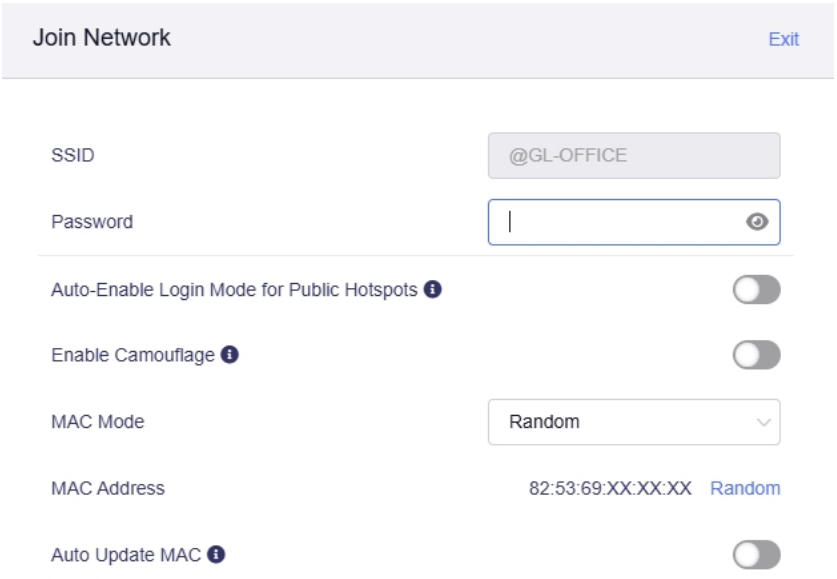
2. Elija la red Wi-Fi a la que desea conectarse de la lista de redes disponibles.

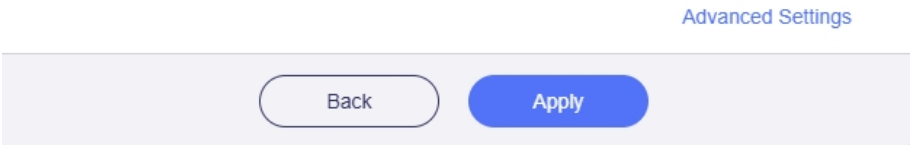


Nota:

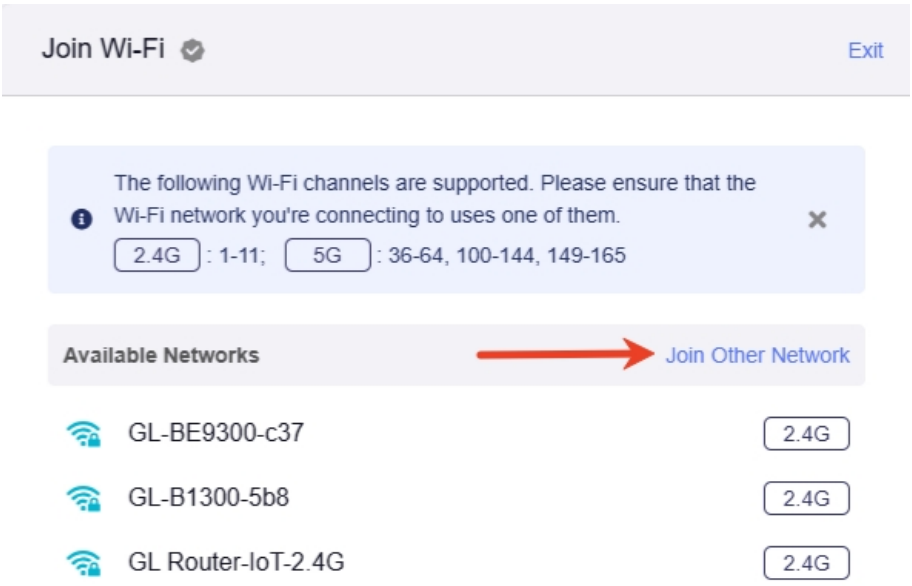
1. Estaes página muestra los canales Wi-Fi compatibles con su enrutador. Asegúrate de que la red Wi-Fi a la que intentas conectar utiliza uno de estos canales; de lo contrario, es posible que no se muestre en la red disponible. list.
2. Cuando busque un punto de acceso personal para iPhone, mantenga el iPhone desbloqueado para mantener la transmisión de baliza Wi-Fi. De lo contrario, es posible que el enrutador no detecte este punto de acceso.

3. Ingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.

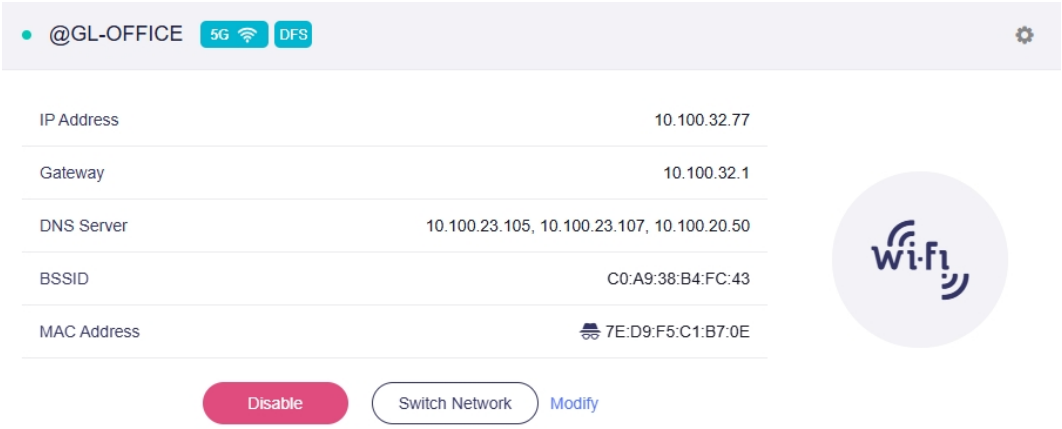




Consejo: Si el SSID de Wi-Fi al que desea conectarse no está en la lista de redes disponibles, haga clic en **Conectarse a otra red** en la esquina superior derecha, ingrese manualmente el SSID de Wi-Fi y otra información. requerido antes de hacer clic en **Aplicar**.

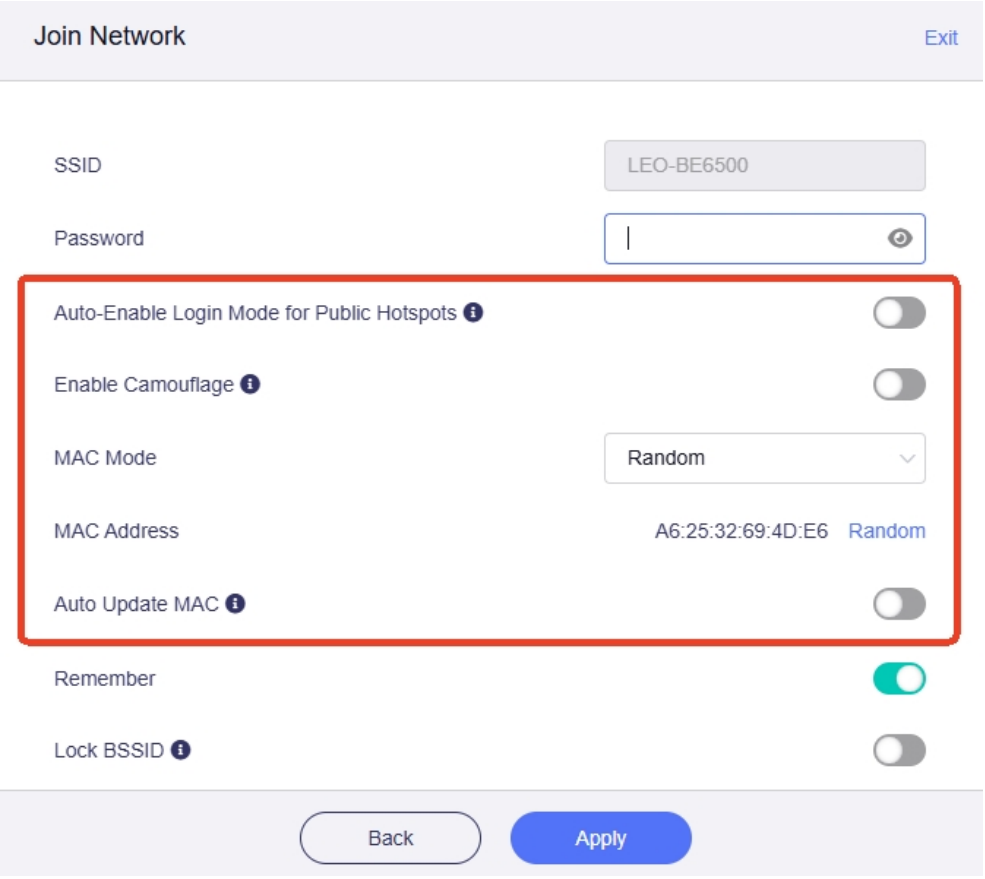


4. Después de un tiempo, si la contraseña es correcta, la conexión será exitosa.



4.2.2.2 Para punto de acceso público

Al conectar el enrutador a un punto de acceso público con un portal cautivo, habilitar las siguientes funciones puede ayudar a mejorar la tasa de éxito de la conexión.



- **Habilitar automáticamente el modo de inicio de sesión para puntos de acceso públicos**

  Si está habilitado, el enrutador ingresa automáticamente al modo de inicio de sesión de punto de acceso público cuandon está conectado a un punto de acceso pero no a Internet. En este modo, algunos servicios se suspenderán mientras el modo DNS cambia a automático, lo que puede filtrar su actividad de red al red proveedor (por ejemplo, hotel, centro comercial). Incluso si está deshabilitado, el enrutador le pedirá que ingrese a este modo si detecta un portal cautivo de punto de acceso o no puede iniciar sesión.
- **Habilitar camuflaje**

  Si está habilitado, el enrutador se hará pasar por el dispositivo cliente que utiliza para acceder al panel de administración emulando la MAC de ese dispositivo. dirección.
- **Modo MAC**

  Celija qué MAC utiliza el enrutador para conectarse al punto de acceso público.

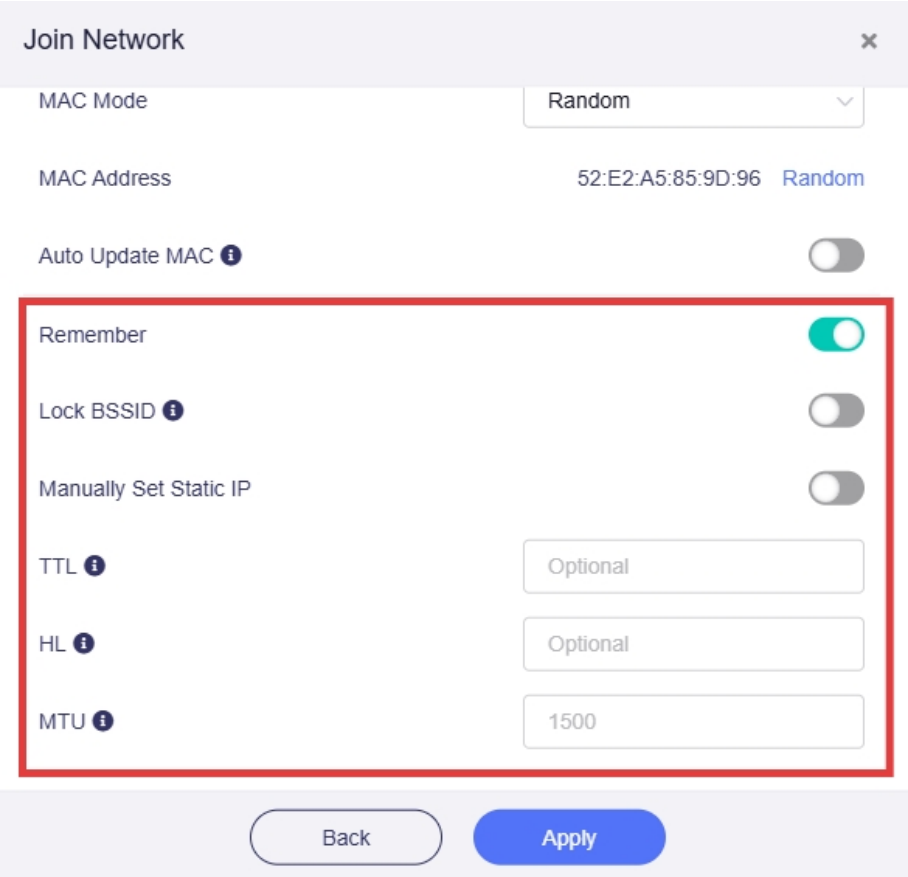
Fábrica	Utiliza la dirección MAC original asignada de fábrica del dispositivo.
Clonar	Clona la dirección MAC de un dispositivo cliente para la conexión. Si la MAC deseada no aparece en la lista, ingrese manualmente la dirección MAC que desea clonar. Nota: Muchos dispositivos utilizan direcciones MAC aleatorias (a menudo llamadas dirección Wi-Fi privada o dirección de hardware aleatoria) cuando se conectan a redes Wi-Fi. Como resultado, es posible que la dirección MAC que se muestra aquí no coincida con la MAC física real del dispositivo.
Aleatorio	Genera automáticamente una dirección MAC aleatoria para la conexión.

- **Actualización automática de MAC**
  Si esta opción está habilitada, la dirección MAC se actualizará automáticamente.

Al guardar la configuración de red, el modo MAC, incluido cualquier clonado o aleatorio MAC dirección, será vinculado al SSID específico que guarda. Puede cambiar manualmente esta configuración para cada SSID en cualquier momento.

4.2.2.3 Configuración avanzada

Al unirse a la red, existen algunas opciones adicionales.

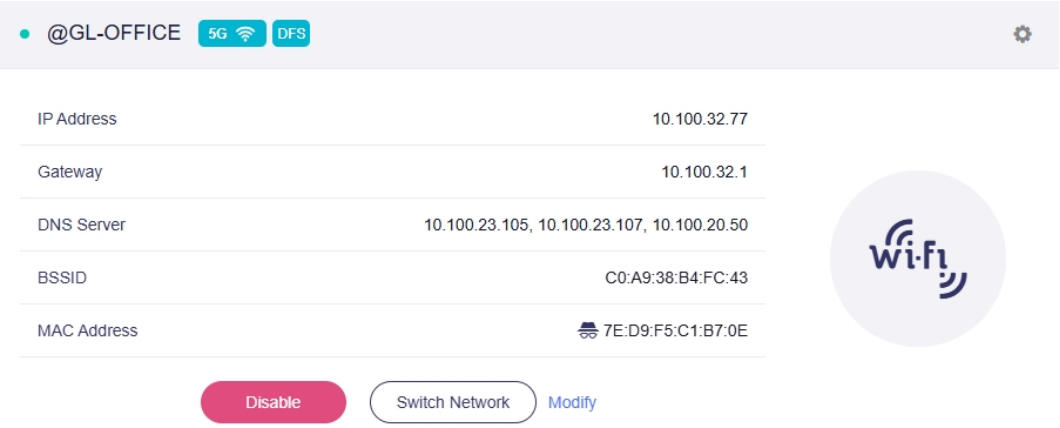


- **Recordar**: habilite esta opción para recordar la red Wi-Fi actual repetida.
- **Bloquear BSSID**: cuando esté habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Configurar IP estática manualmente**: cuando está habilitado, puede configurar manualmente una dirección IPv4 fija, una máscara de red, una puerta de enlace y servidores DNS para la conexión repetidora del enrutador, en lugar de obtener estas configuraciones automáticamente.
- **TTL**: TTL (Time To Live) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anular/falsificar el TTL, eingrese el TTL efectivo deseado más 1 para compensar la disminución automática. TTL es válido solo para IPv4.

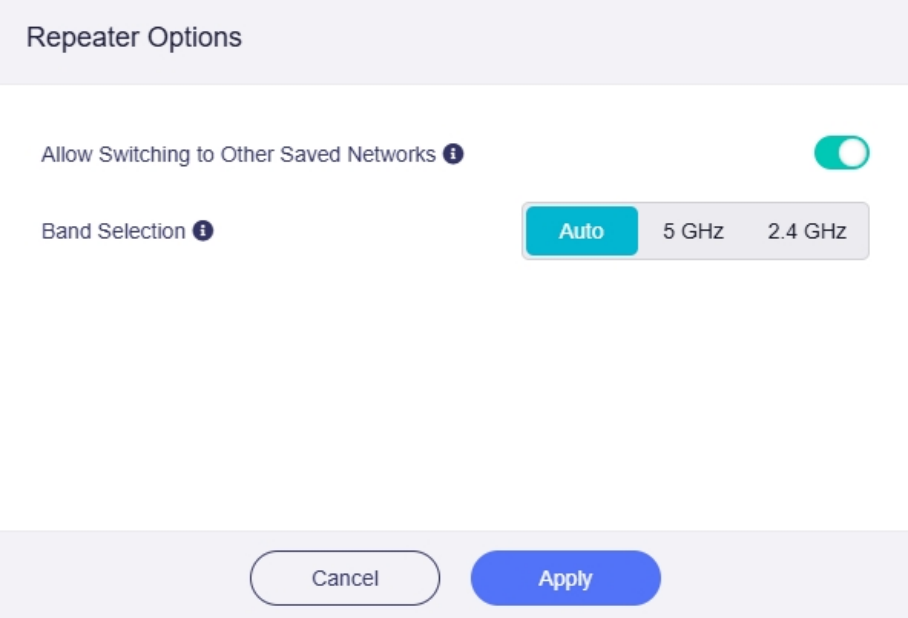
- **HL**: En IPv6, el campo HL (Hop Limit) se utiliza para limitar el número de saltos de transmisión de paquetes de datos en la red, lo que equivale al TTL en IPv4.
- **MTU**: el valor predeterminado es 1500.

4.2.2.4 Opciones de repetidor

Haga clic en el ícono de ajustes en la esquina superior derecha esquina para configurar las opciones del repetidor .



La página puede variar debido a las diferentes versiones de firmware.

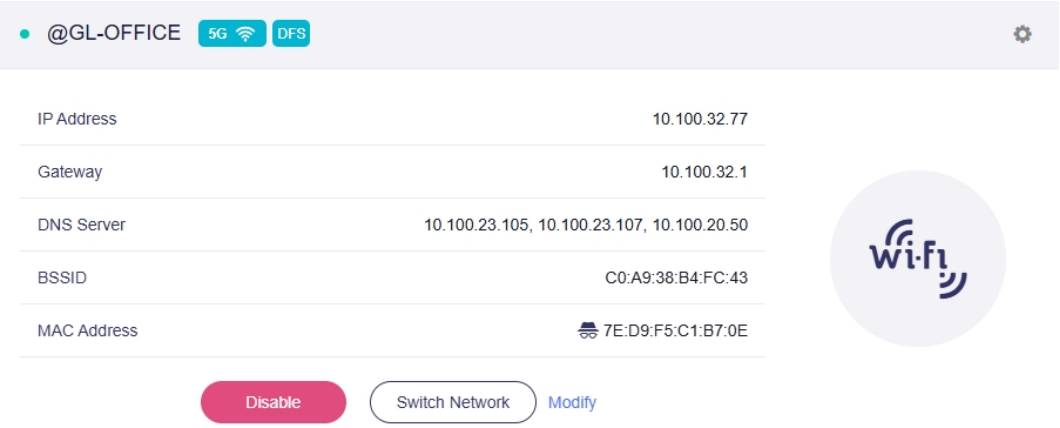


- **Permitir cambiar a otras redes guardadas**: si está habilitado, el enrutador se conectará automáticamente a otras redes guardadas cuando la red Wi-Fi conectada actualmente no esté disponible.

- **Selección de banda**: si selecciona manualmente una banda, el enrutador solo escaneará y se conectará a las redes Wi-Fi en esta banda de frecuencia.

4.2.2.5 Administrar red conocida

Para administrar redes conocidas, haga clic en **Cambiar red**.

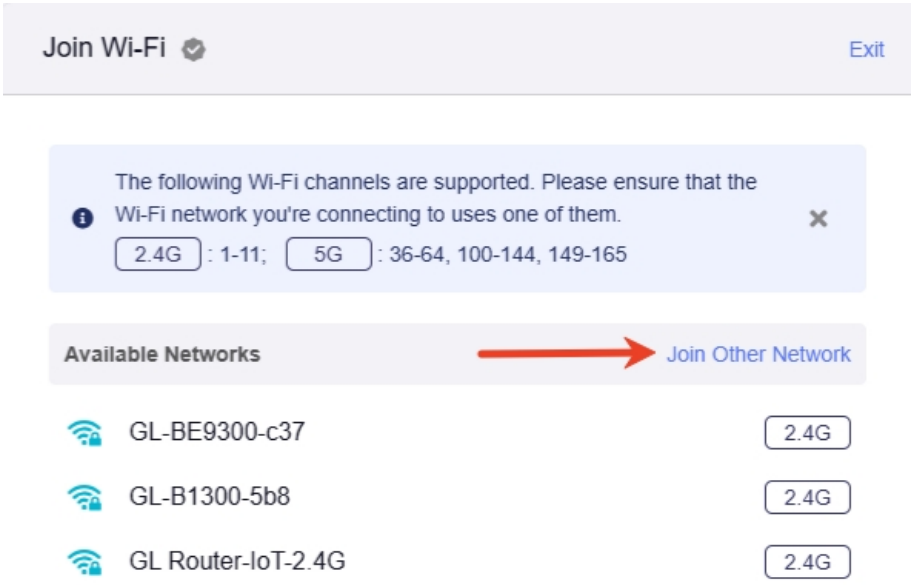


En la sección **Redes conocidas**, haga clic en el ícono de la papelera para eliminar una red conocida o en el ícono de ajustes para configurar la red.

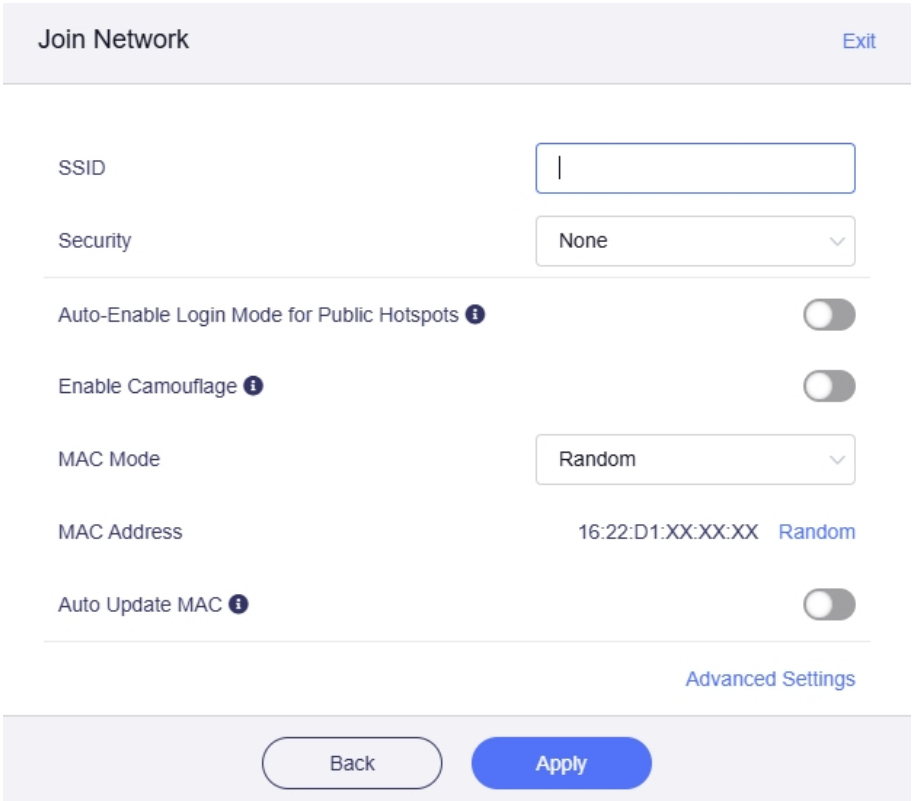


4.2.2.6 Conectarse a otra red

Si el SSID no está en la lista de redes disponibles, o si el SSID está oculto, puede hacer clic en **Conectarse a otra red**.

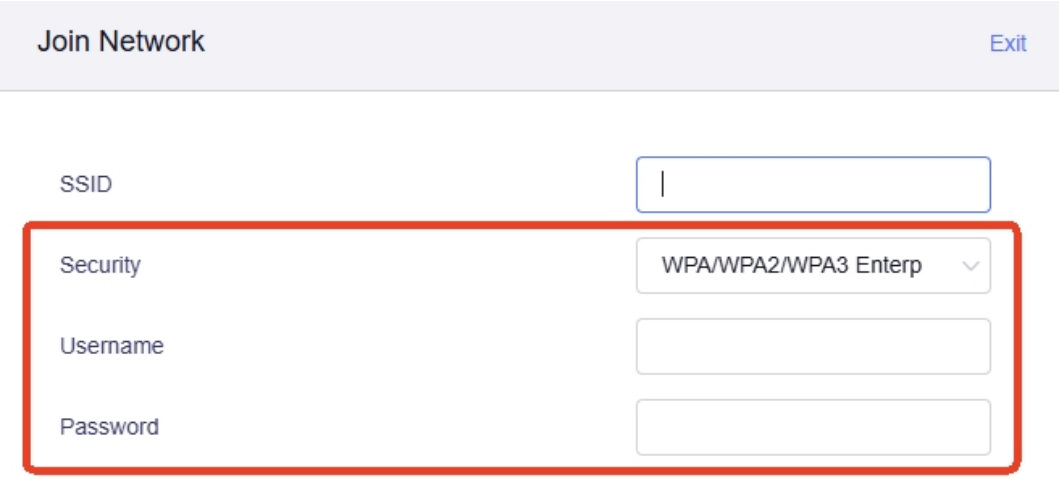


Ingrese el **SSID**, seleccione **Seguridad** e ingrese la contraseña (si es necesaria), luego haga clic en **Aplicar**.



Para la configuración de **Seguridad**, hay dos o tres opciones, según el modelo.

- Ninguna, lo que significa que no se requiere contraseña.
- WPA/WPA2/WPA3, que es común y compatible con casi todas las redes Wi-Fi.
- WPA/WPA2/WPA3 Enterprise, que requiere el Protocolo de autenticación extensible (EAP) para la autenticación. Se necesitan un nombre de usuario y una contraseña válidos para conectarse (generalmente se usan en redes empresariales o universitarias).



Para obtener orientación detallada sobre cómo repetir redes EAP, haga clic aquí.

4.2.2.7 Reconexión

En los siguientes casos, el enrutador intentará automáticamente volver a conectarse a Wi-Fi de vez en cuando. Puede desactivar esto manualmente si es necesario. En caso de errores de SSID/contraseña, elimine la red de Redes conocidas para resolverlo.

1. SSID/contraseña incorrecta ingresada durante la configuración del repetidor.
2. Se movió fuera del alcance del enrutador ascendente después de la conexión inicial.
3. El enrutador ascendente cambia SSID/contraseña o restringe el acceso después de la conexión.

El proceso de reconexión tiene tres fases distintas: espera fase de escaneo, fase de escaneo y fase de conexión.

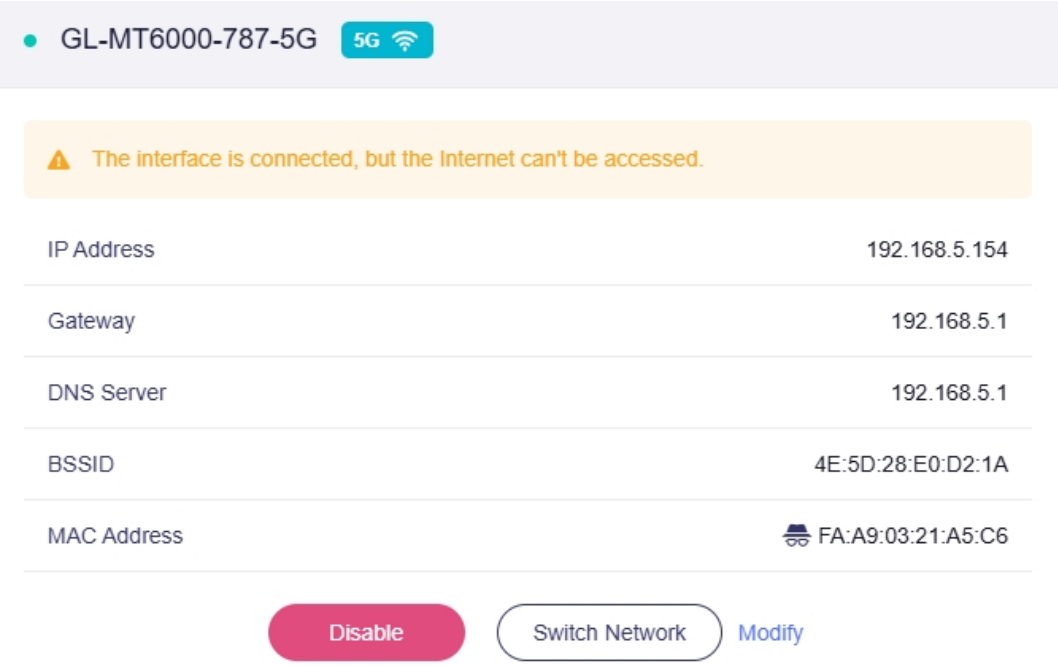
1. Fase de espera: no hay problemas; el enrutador espera las condiciones de reconexión.
2. Fase de escaneo: puede ocurrir pérdida de paquetes en la banda de frecuencia escaneada. Los dispositivos nuevos pueden tener problemas de conexión. Para los modelos GL-AXT1800/GL-AX1800, el Wi-Fi para invitados se desactivará temporalmente.
3. Fase de conexión: el Wi-Fi principal en la banda objetivo puede caer durante unos segundos durante el restablecimiento.

Nota: Los problemas suelen surgir en las fases de escaneo y conexión p.

4.2.2.8 Solución de problemas

Cuando el enrutador está conectado a una red Wi-Fi como repetidor, si Internet no está disponible, se mostrará un mensaje amarillo como se muestra a continuación.

"La interfaz está conectada, pero no se puede acceder a Internet".



Para solucionar este problema problema:

1. Compruebe si el dispositivo ascendente (es decir, la red Wi-Fi a la que está conectado su enrutador) tiene acceso a Internet.
2. Vaya a Multi-WAN página para verificar el estado de la interfaz del repetidor.

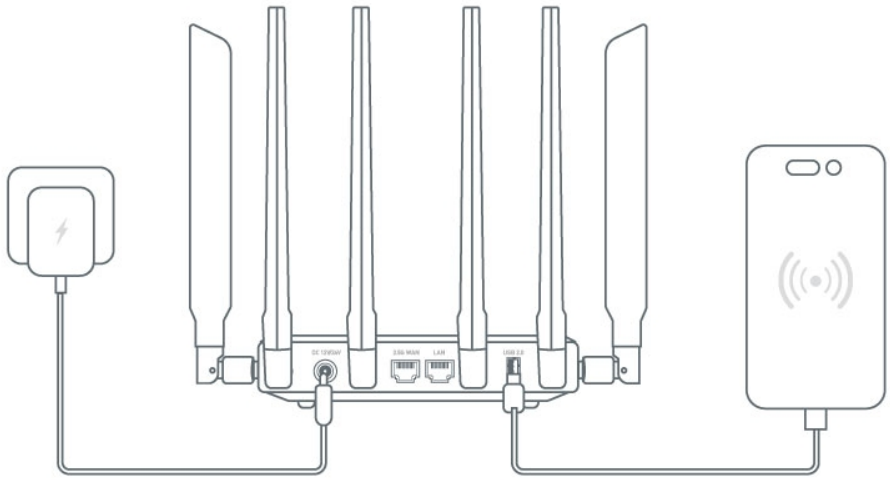
4.2.2.9 DFS

DFS (Selección dinámica de frecuencia) es un mecanismo que cambia automáticamente Canales Wi-Fi para evitar interferencias con las señales de radar. Al conectarse a un Wi-Fi 5G ascendente, el Wi-Fi del enrutador seguirá el Wi-Fi ascendente para usar o no el canal DFS.

- Si el Wi-Fi ascendente usa un canal DFS y se puede escanearn, el enrutador El Wi-Fi 5G utilizará el mismo canal.
- El Wi-Fi 5G del enrutador cambiará al canal que no es DFS si el Wi-Fi ascendente no se puede escanear o si la conexión falla.

4.2.3 Conectarse a Internet mediante conexión compartida por USB

Cconectar un inteligenteteléfono al enrutador a través de un cable USB se denomina Anclaje a red, que puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método conveniente para el acceso temporal ia Internet, especialmente cuando al aire libre o en áreas sin banda ancha fija .

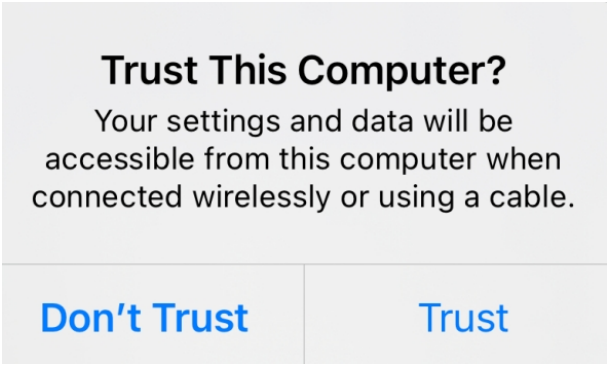


Sin host El módem también funciona en Tethering durante la celular configuración.

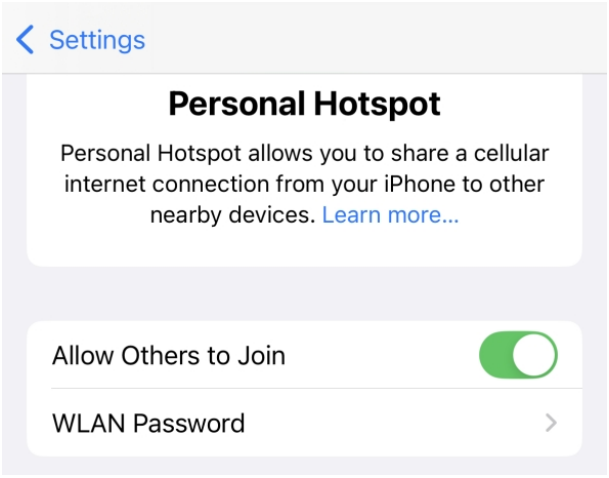
Nota: Algunos operadores de telefonía móvil limitan o cobran más por atadura. Recomendamos consultar con su operador.

4.2.3.1 iPhone

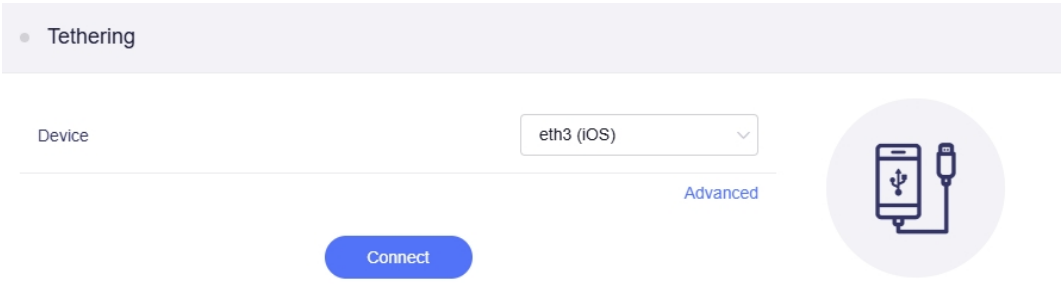
1. Conecte un iPhone al puerto USB del enrutador mediante un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



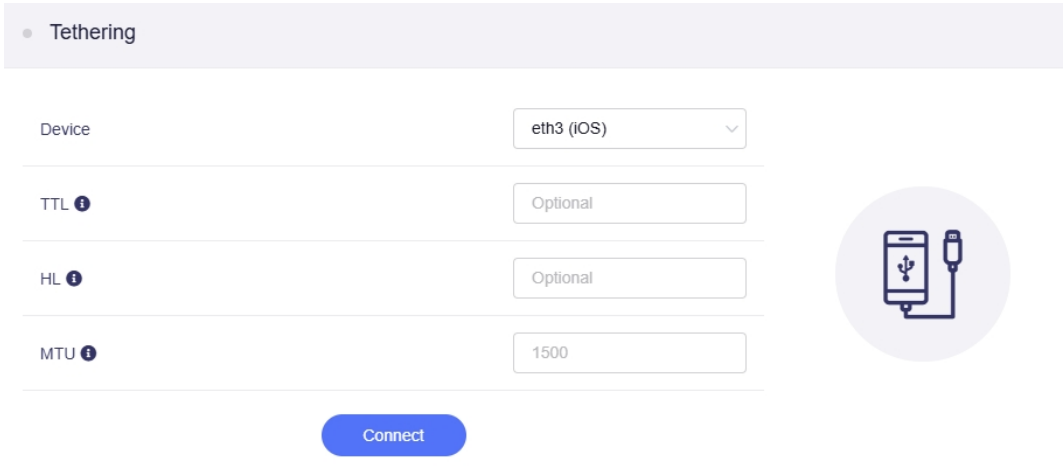
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Habilitar **Permitir que otros Unirse**.



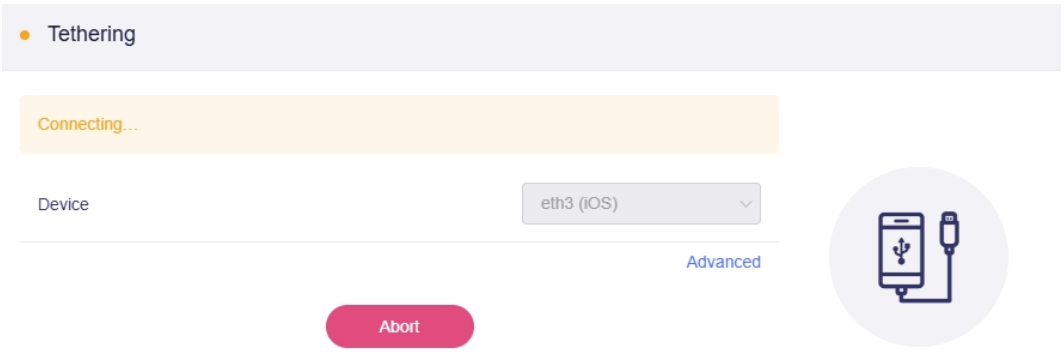
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



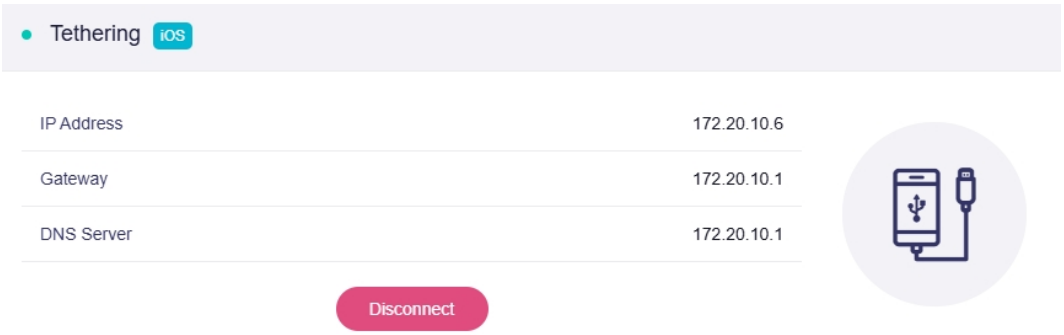
Si necesita configurar configuraciones avanzadas, como TTL, HL y MTU, haga clic en **Avanzado** para personalizar estas configuraciones, luego haga clic en **Conectar**.



4. Comenzará a conectarse.

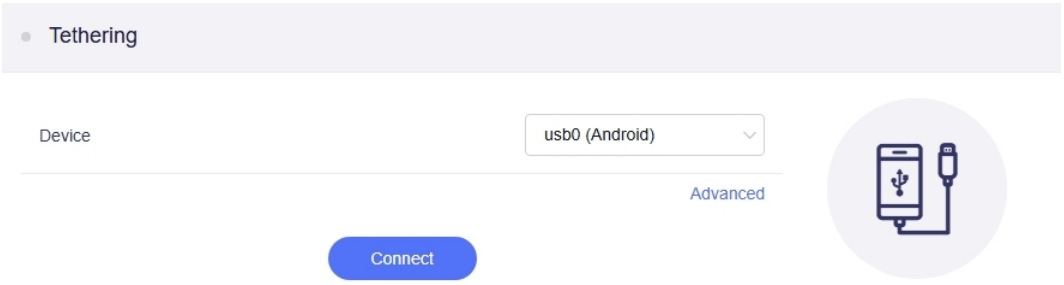


Una vez conectado, thesta página mostrará los detalles de la conexión Tethering .

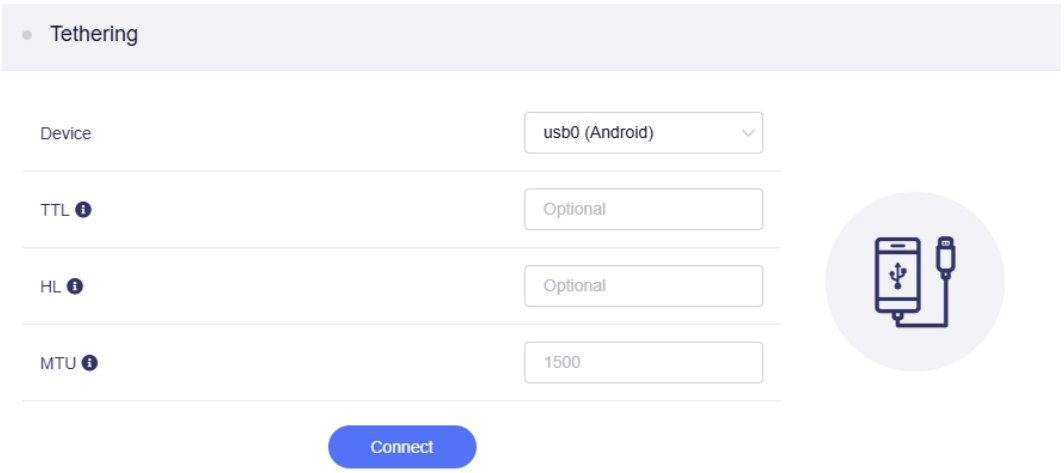


4.2.3.2 Android

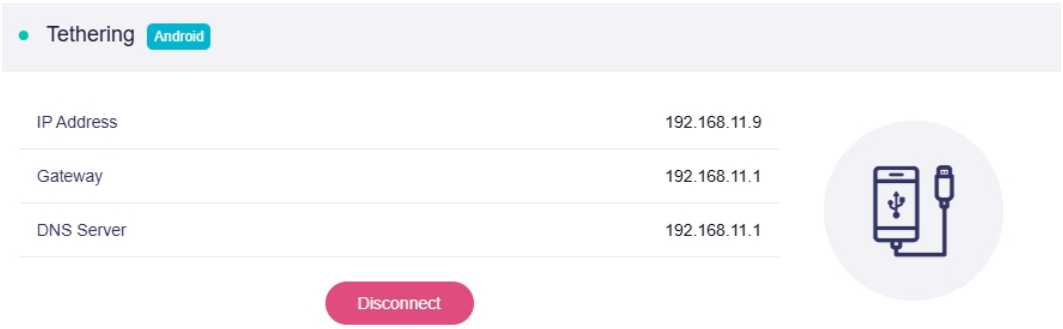
1. Conecte un teléfono Android al puerto USB del enrutador mediante un cable USB. Puede aparecer un cuadro de diálogo del sistema preguntando USB preferencias.
   Selecciona **Anclaje a red USB** o **Archivo Transferir** si se te solicita.
2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Habilite **Punto de acceso personal** o **Anclaje a red USB**.
   (Los pasos para habilitar el Anclaje a red USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico del fabricante si es necesario.)
3. Conecte una computadora u otro teléfono al enrutador, luego inicie sesión en el panel de administración web, navegue a **INTERNET** > **Anclaje a red**. Click **Conectar**.



Si necesita configurar configuraciones como TTL, HL y MTU, haga clic en **Avanzado** para personalizar estas configuraciones y luego haga clic en **Conectar**.



4. Una vez conectado, estaes página mostrará el Anclaje estado de conexión.



4.2.3.3 Solución de problemas

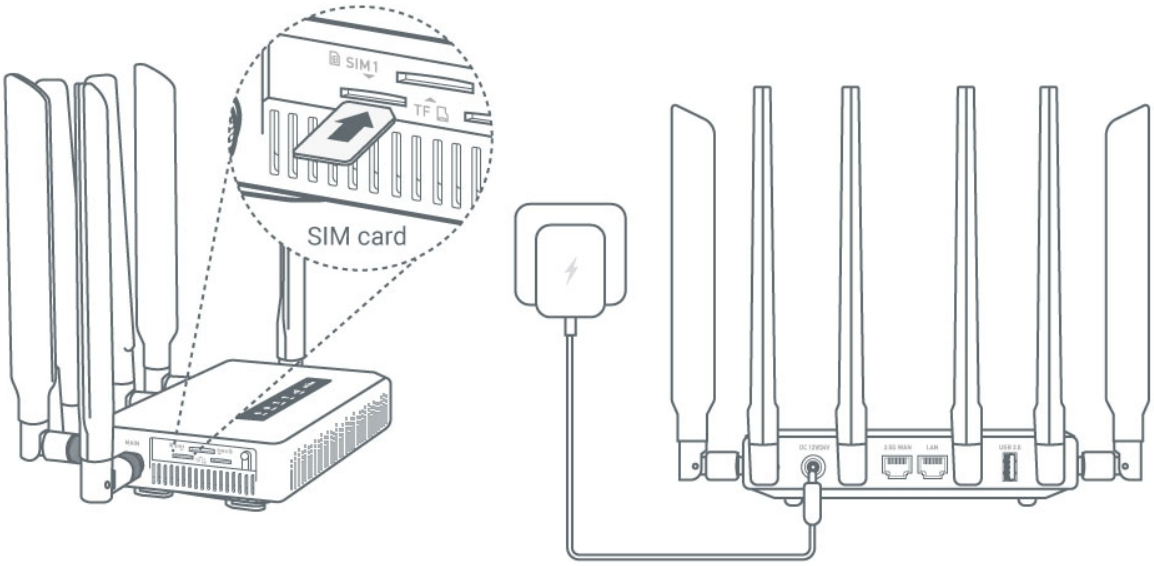
Si la conexión falla, intente estos pasos para solucionar problemas:

- Utilice la fuente de alimentación original para el enrutador.
- Desconecte y vuelva a conectar el cable USB.
- Utilice otro cable USB. Asegúrese de que admita la transferencia de datos (no solo la carga).
- Apague y active "Anclaje a red USB" unas cuantas veces (para teléfonos Android).
- Apague y active "Permitir que otros se unan" unas cuantas veces (para iPhone).
- Reinicie su teléfono inteligente e inténtelo nuevamente.

Si el problema persiste, comuníquese con nuestro soporte técnico en support@gl-inet.com.

4.2.4 Conectarse a Internet mediante la red móvil

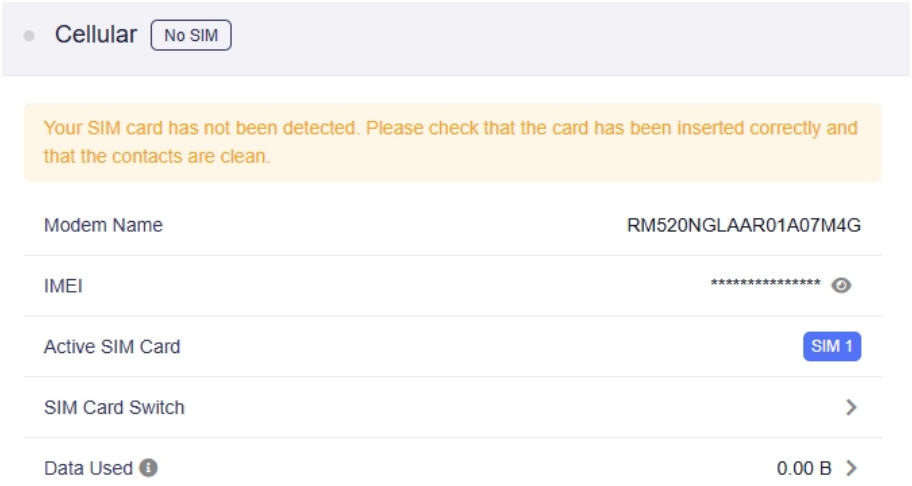
Spitz AX (GL-X3000) tiene un módem celular de doble SIM incorporado. Solo hay una tarjeta SIM activa a la vez; la otra servirs como respaldo. Puedes cambiar manualmente entre las dos tarjetas SIM.



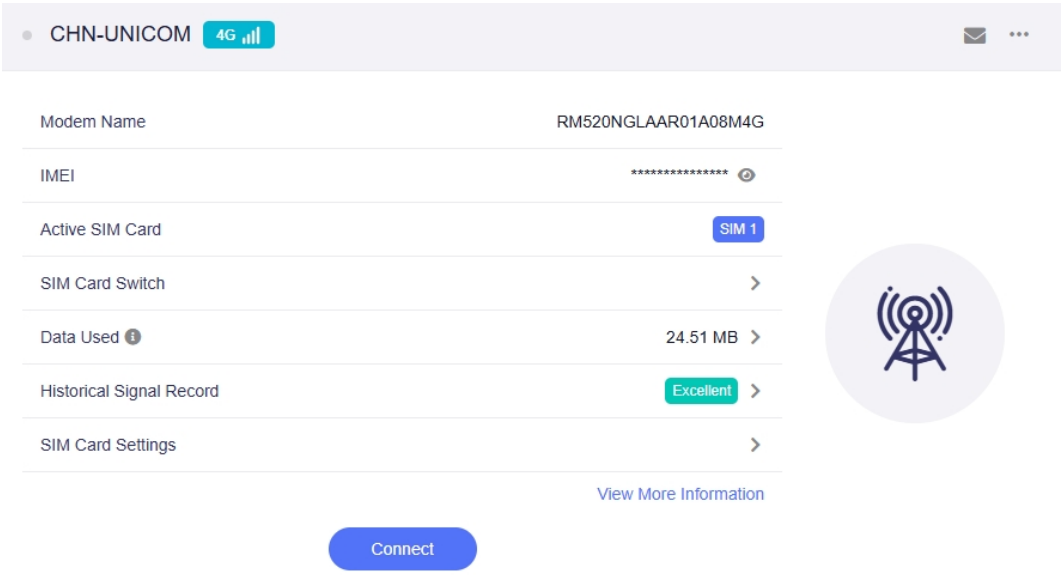
4.2.4.1 Configuración automática

Recomendamos que primero apague el enrutador, inserte su(s) tarjeta(s) SIM preactivada(s) en las ranuras y luego enciéndalo. Si inserta la tarjeta SIM después de que el enrutador se haya iniciado, es posible que el panel de administración web no se actualice automáticamente. o reinicie el enrutador.

1. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Celular**.
2. Cuando no se inserta ninguna tarjeta SIM, la página muestra el mensaje "Su tarjeta SIM no ha sido detectada".

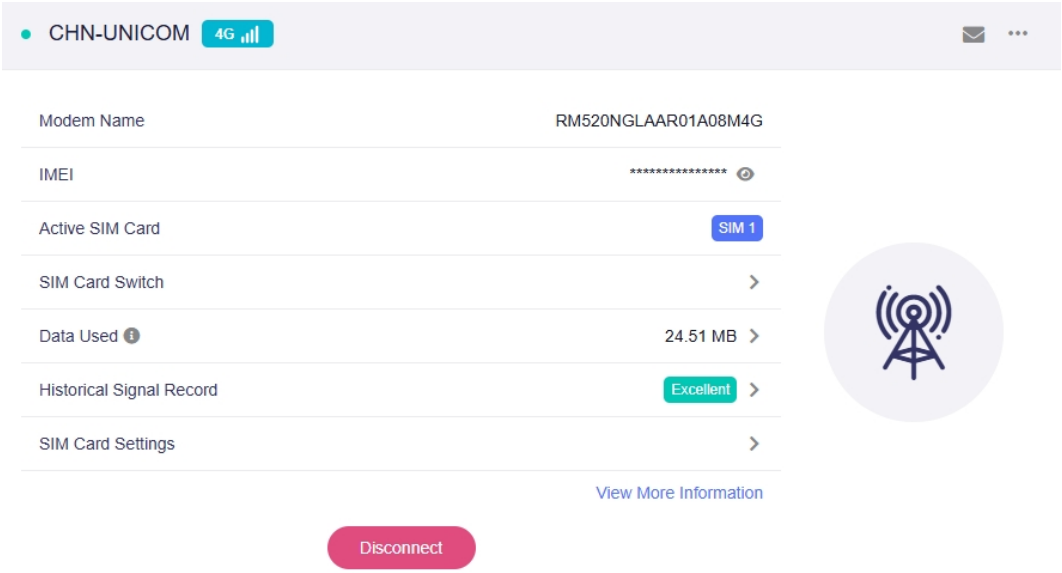


3. Cuando se inserta una tarjeta SIM, la página se muestra de la siguiente manera. data-r="792">Conectar **Conectar**.

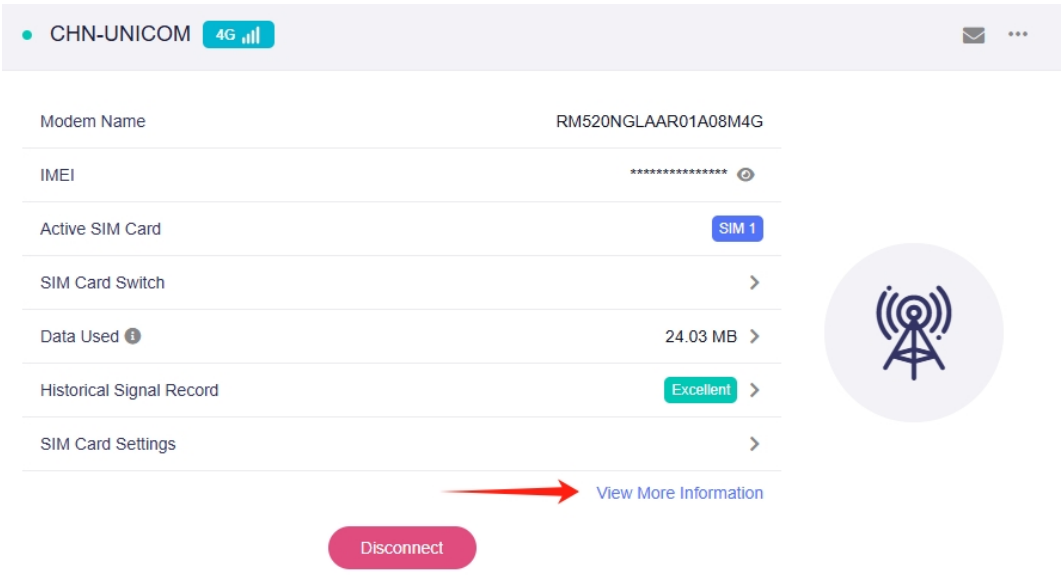


Consejo: Si no se detecta la tarjeta SIM, intente reiniciar el enrutador para ver si se puede detectar.

4. Una vez que la red celular esté conectada, el página muestras los detalles de la red con un punto verde, lo que indica una conexión exitosa.



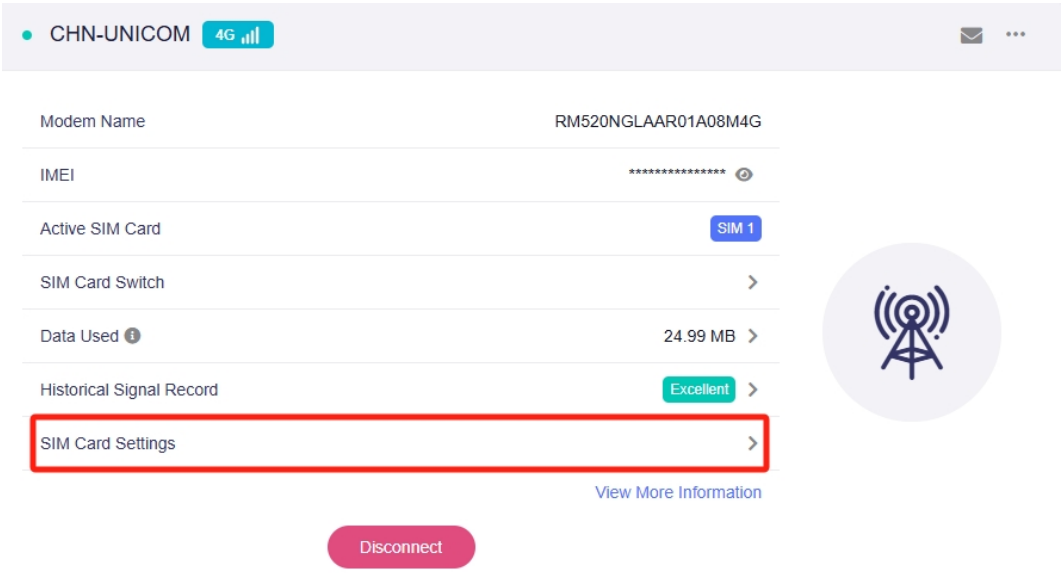
5. Haga clic en **Ver más información** para mostrar más información celular, incluidos detalles del módem, detalles de la tarjeta SIM, detalles de Internet y señal celular.



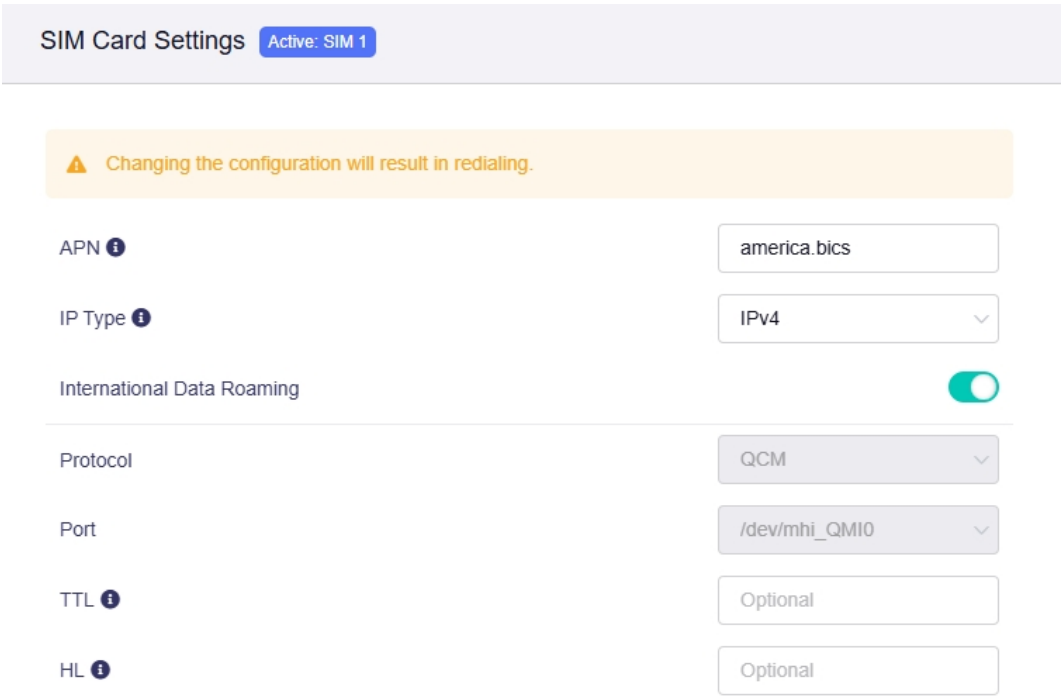
Si falla la configuración automática, intente **Configuración manual**.

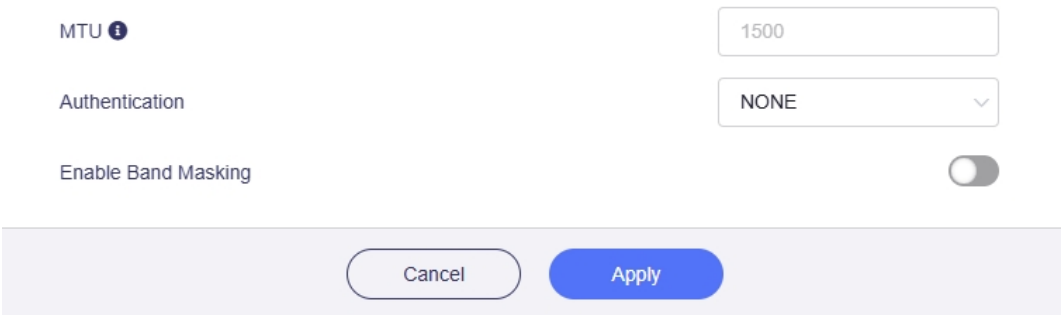
4.2.4.2 Configuración manual

1. En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular**, luego haga clic en **Configuración de la tarjeta SIM**.



2. Puede ver o modificar la configuración celular de la tarjeta SIM actual. La aplicación de los cambios activará una reconexión.

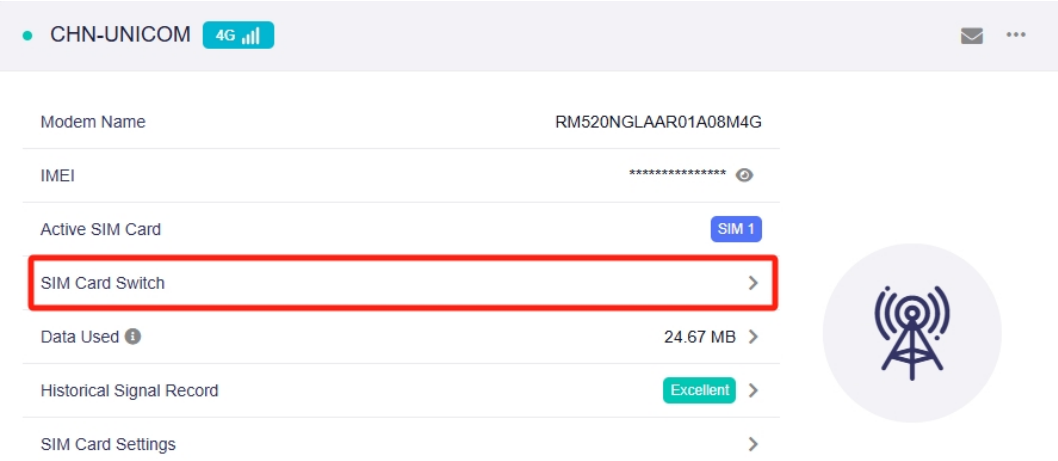




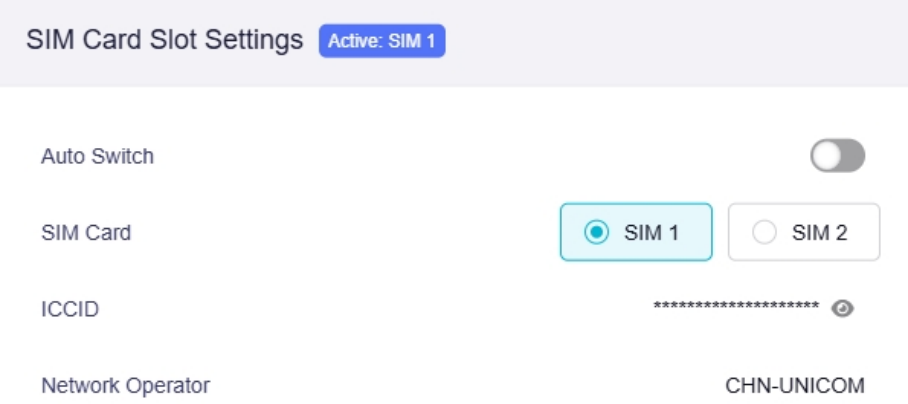
- **APN**: APN (nombre del punto de acceso) es un parámetro de puerta de enlace requerido para una conexión de red celular. Permite que el enrutador se conecte a Internet proporcionado por su proveedor de telefonía móvil. Puede usar el APN predeterminado o configurar un APN personalizado proporcionado por su proveedor. operador.
- **Protocolo**: el protocolo de comunicación celular detectado automáticamente (por ejemplo, QMI o QCM) según su módem y operador.
- **Puerto**: el puerto serie detectado automáticamente para la comunicación con el módem celular
- **TTL**: TTL (Time To Live) define el tiempo máximo que los paquetes pueden sobrevivir en la red. La configuración TTL es válida solo para IPv4. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anularlo, ingrese el TTL efectivo deseado más 1 para compensar el cambio automático. decrementar.
- **HL**: en IPv6, HL (límite de saltos) limita el número de saltos de transmisión para paquetes de datos en la red y sirve como el equivalente de TTL en IPv4.
- **MTU**: el valor de MTU predeterminado es 1500 bytes.
- **Autenticación**: elija el método de autenticación requerido por su proveedor (por ejemplo, NINGUNO, PAP, CHAP). Por lo general, esto se establece en NINGUNO si no se necesitan credenciales.
- **Enmascaramiento de banda**: puede habilitar el Enmascaramiento de banda si desea que el enrutador bloquee ciertas bandas o use solo bandas celulares específicas. Ver 4.2.4.6 Enmascaramiento de banda para obtener más detalles.

4.2.4.3 Configuración de la ranura de la tarjeta SIM

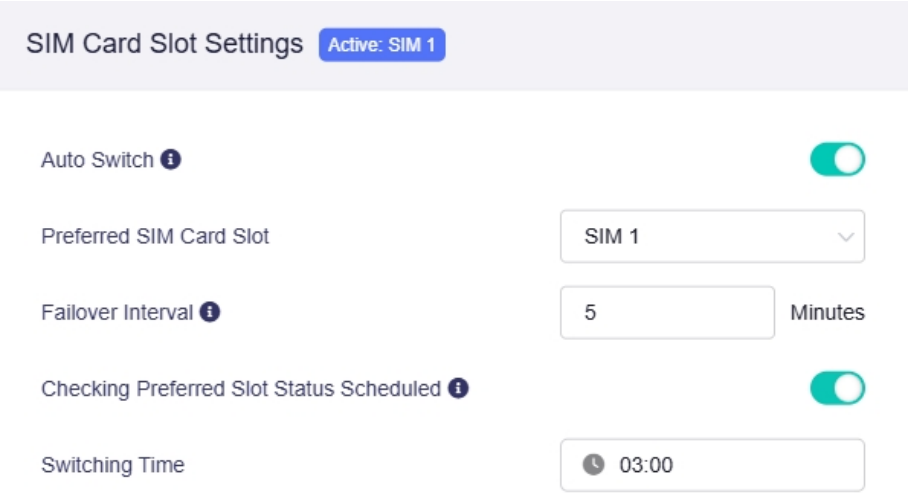
En el administrador web del enrutador panel, navegue hasta **INTERNET** > **Celular** y luego haga clic en **Cambiar tarjeta SIM**.



Mostrará el botón de cambio automático, la tarjeta SIM activa, el ICCID y el operador de red.



Si hay dos tarjetas SIM insertadas, puede habilitar el **cambio automático**.



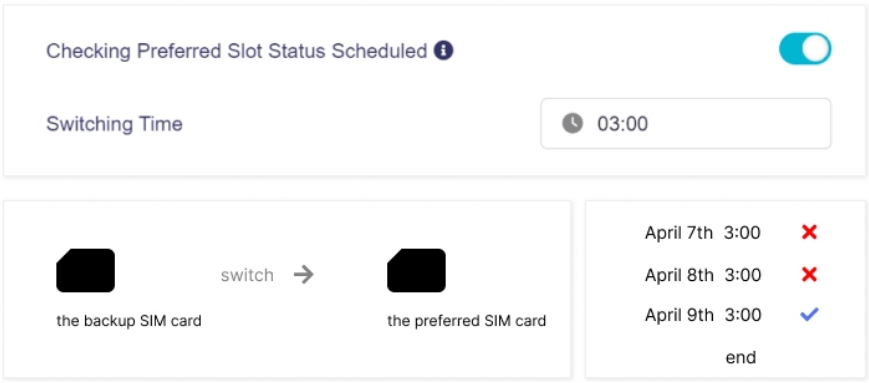
- **cambio automático**: permite el cambio automático entre SIM 1 y SIM 2. El método de detección de red para SIM Auto Switch es el mismo que el configurado en la página Multi-WAN.
- **Ranura para tarjeta SIM preferida**: configure la tarjeta SIM preferida en SIM 1 o SIM 2.
- **Intervalo de conmutación por error**: los valores disponibles oscilan entre 5 minutos y 24 horas.

  Si la conexión a Internet aún no está disponible después de una conmutación por error, el dispositivo volverá a la ranura SIM preferida y esperará este intervalo antes de volver a intentarlo. conmutación por error.

  Esta opción se aplica cuando tanto la tarjeta SIM preferida como la tarjeta SIM de respaldo no tienen señal. El dispositivo cambiará entre tarjetas SIM hasta que una de ellas obtenga una señal válida.
- **Verificación del estado de la ranura preferida programada**

  Cuando esté habilitado, el dispositivo verificará la ranura SIM preferida diariamente a la hora configurada e intentará volver a cambiar si la SIM preferida recupera el acceso a Internet.

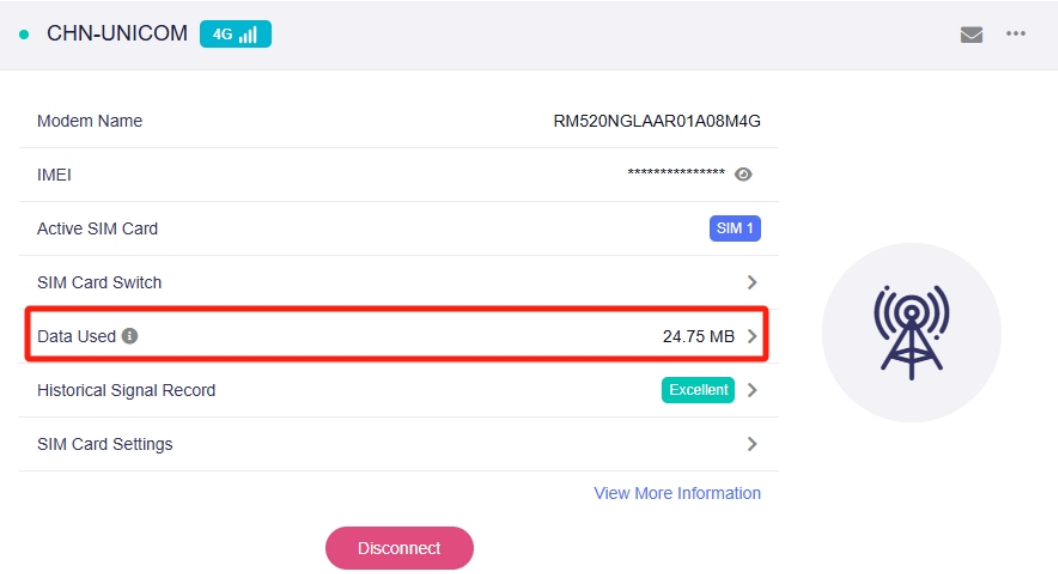
  Esto evita que la SIM de respaldo consuma datos excesivos. Si la SIM preferida aún no tiene señal, el dispositivo continuará usando la SIM de respaldo.



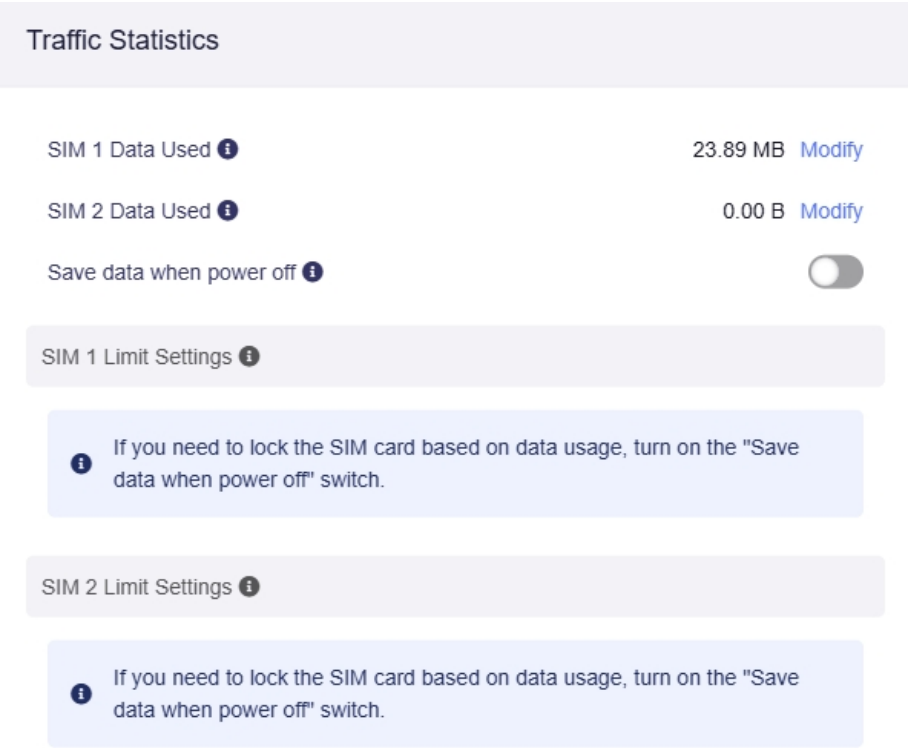
Nota: La función de cambio automático no cambia a otra tarjeta SIM inmediatamente. Primero, el dispositivo necesita tiempo para confirmar que la SIM actual no puede acceder a Internet. En segundo lugar, la otra SIM no está en modo de espera y requiere tiempo para activarse.

4.2.4.4 Estadísticas de tráfico

En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular** y luego haga clic en **Datos utilizados**.



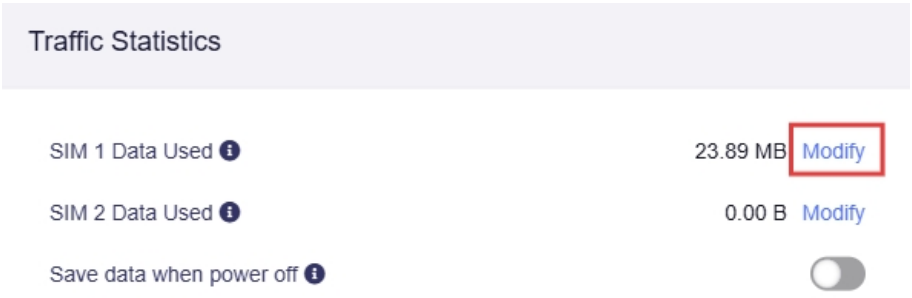
Entrarás en la página **Estadísticas de tráfico**. Muestra los datos usados de las tarjetas SIM y proporciona configuraciones de límite de datos.



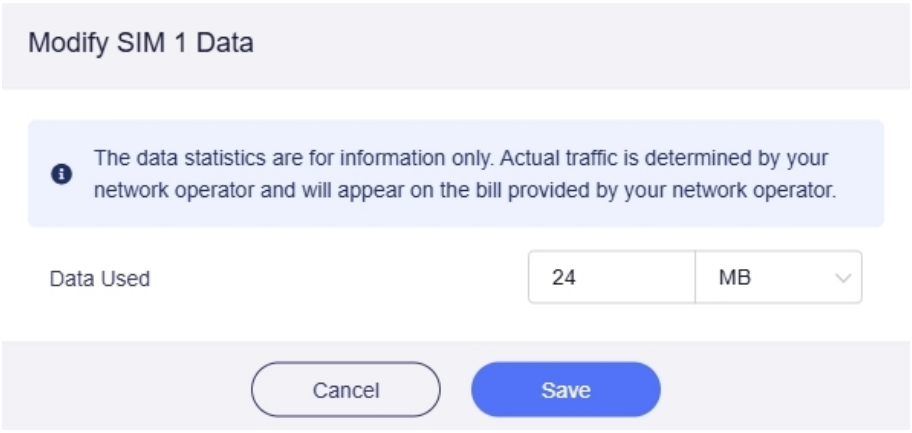
Si los datos utilizados exceden la cantidad límite de datos, modifique la **Cantidad límite de datos** o la **Datos Usado** manualmente. De lo contrario, es posible que la red se desconecte o que la tarjeta SIM cambie automáticamente (para modelos de doble SIM).

- **Modificar los datos utilizados**

  Haga clic en **Modificar** en el lado derecho de SIM 1/2 Datos utilizados.



  Luego puede modificar o restablecer los datos utilizados.

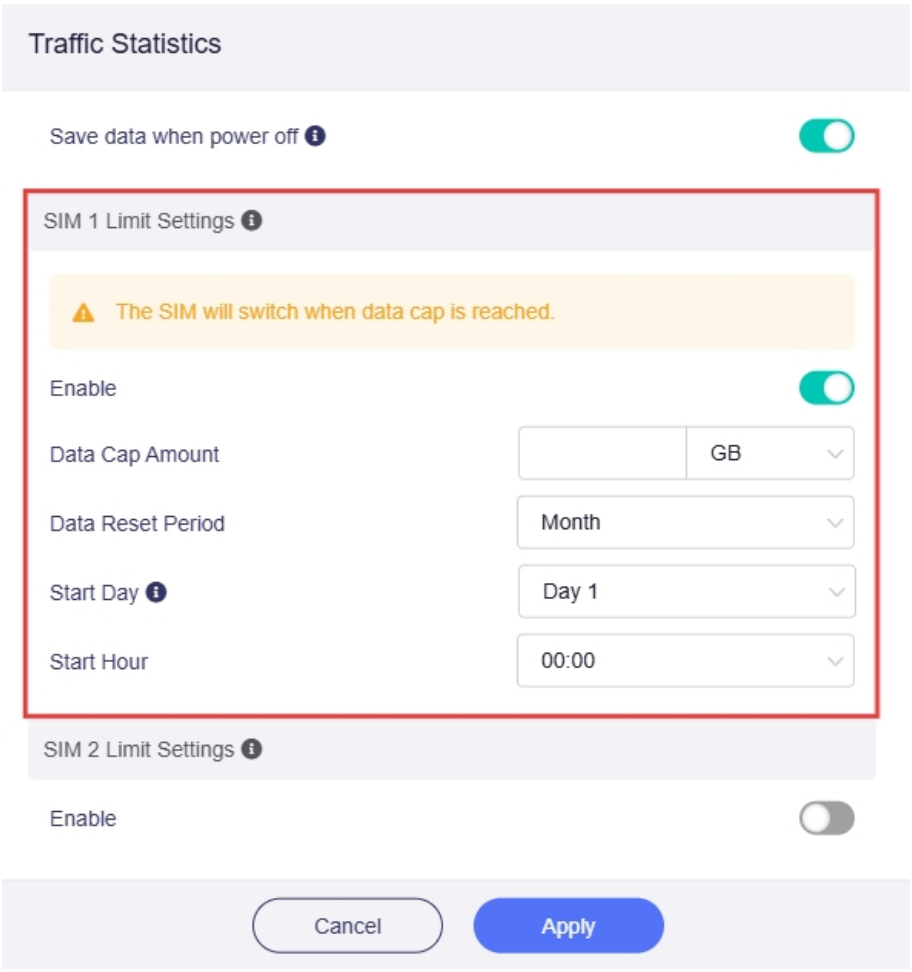


- **Establecer Límite de datos SIM**

  Si desea configurar el límite de datos de la SIM, habilite **Guardar datos cuando se apaga** primero. Significa que los datos se pueden guardar incluso después de que el dispositivo esté apagado.



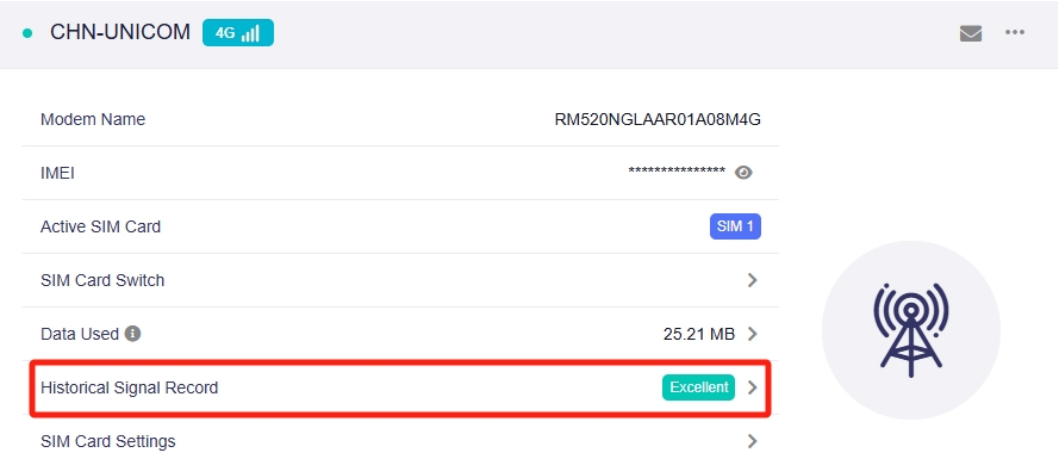
  Luego habilite la configuración de límite de SIM 1 o SIM 2.



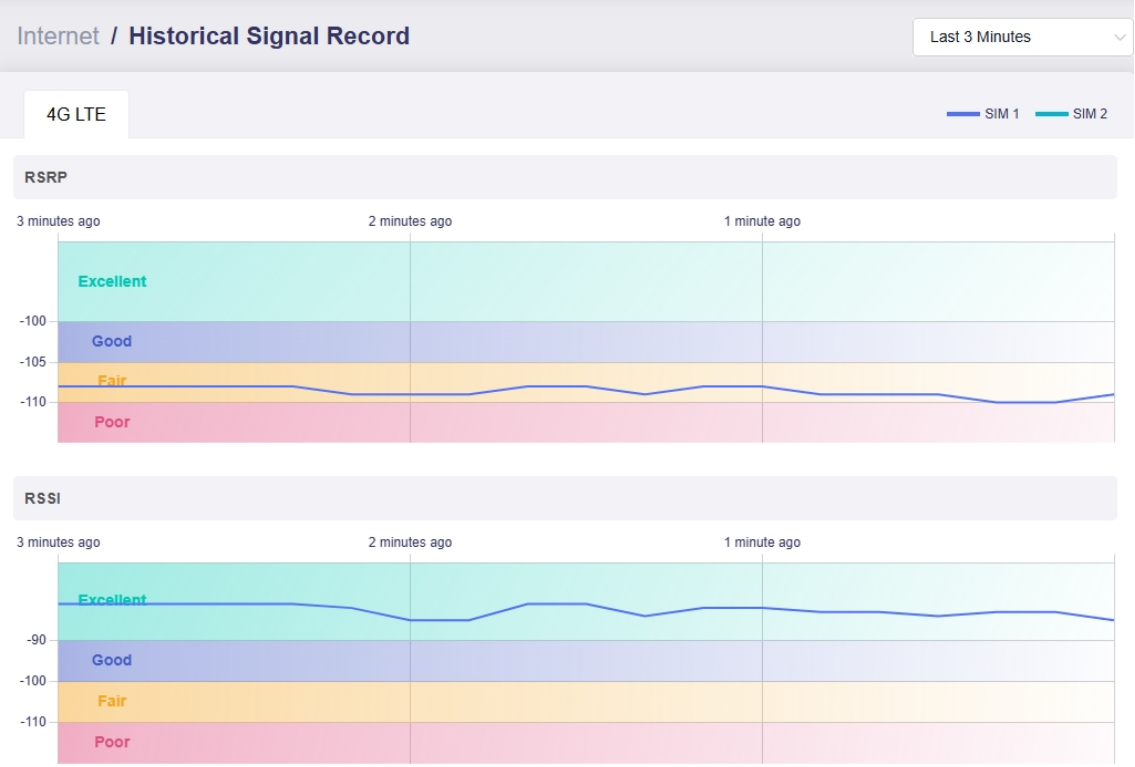
Para los modelos con doble SIM, sugerimos habilitar la **Ranura para tarjeta SIM automática Cambie** al mismo tiempo. Si se establece la Cantidad límite de datos de la SIM 1 y el cambio automático de ranura para tarjeta SIM está habilitado, la SIM 1 cambiará automáticamente a la SIM 2 cuando sus datos excedan la Cantidad límite de datos y la SIM 1 se desactivará.

4.2.4.5 Registro histórico de señales

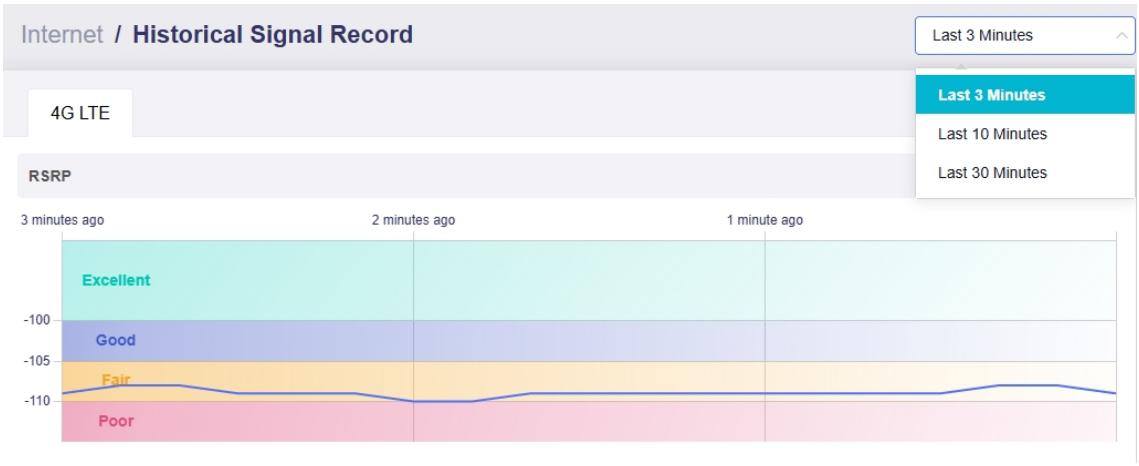
En el enrutador panel de administración web, navegue hasta **INTERNET** > **Celular** y luego haga clic en **Registro histórico de señales**.



Puedes verificar la calidad de tu conexión celular aquí. Si la señal es débil, intente cambiar de torre para obtener una mejor señal.



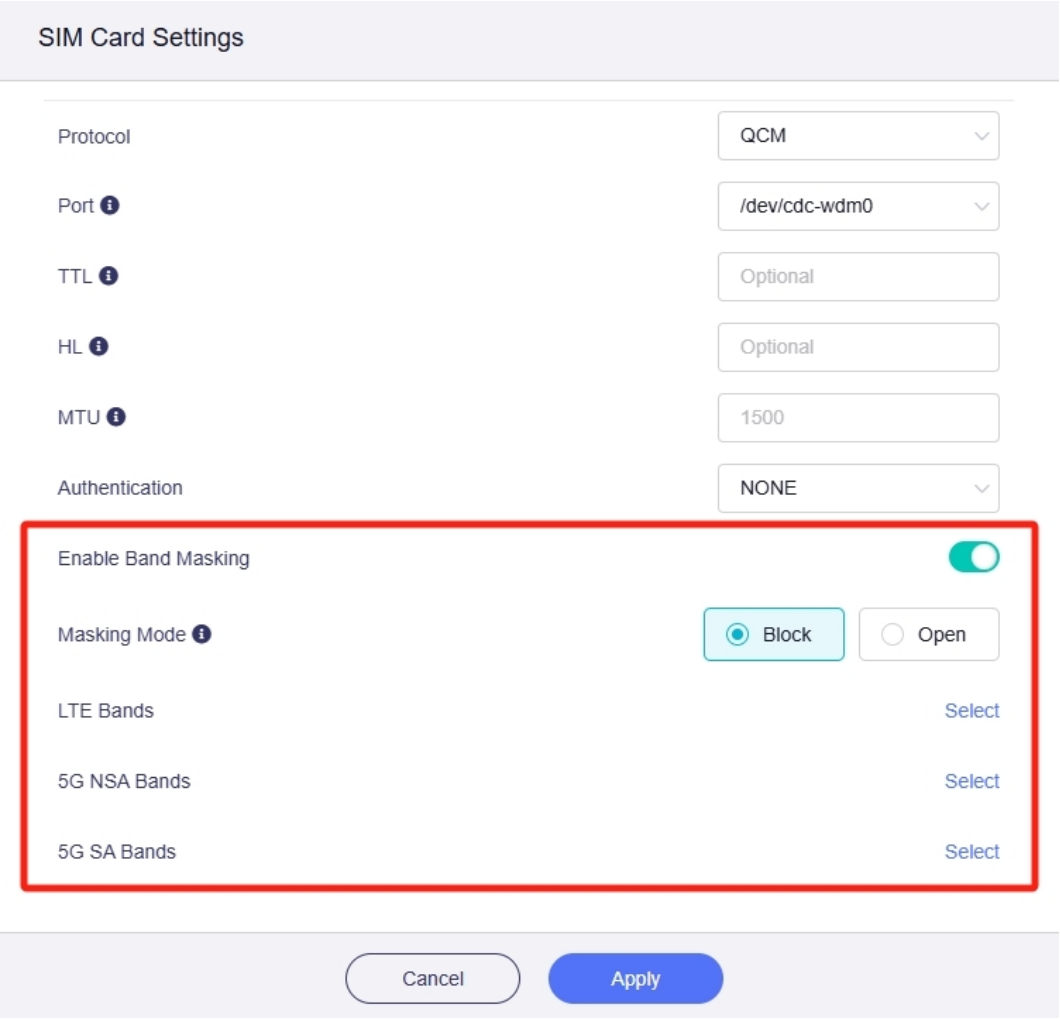
Vea el historial de intensidad de la señal seleccionando diferentes períodos de tiempo en la esquina superior derecha.


Internet / Historical Signal Record
Last 3 Minutes
Last 3 Minutes
Last 10 Minutes
Last 30 Minutes
4G LTE
RSRP
3 minutes ago
2 minutes ago
1 minute ago
Excellent
Good
Fair
Poor
-100
-105
-110

4.2.4.6 Enmascaramiento de banda

La máscara de banda le permite bloquear bandas específicas o usar solo bandas celulares preferidas para mejorar la señal celular débil.

En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular** > **Configuración de tarjeta SIM**, active **Habilitar enmascaramiento de banda**.



Seleccionar el **Modo de enmascaramiento** (Bloquear o Abrir), luego seleccione las Bandas LTE, Bandas 5G NSA y Bandas 5G SA.

4.2.4.7 SMS y reenvío de SMS

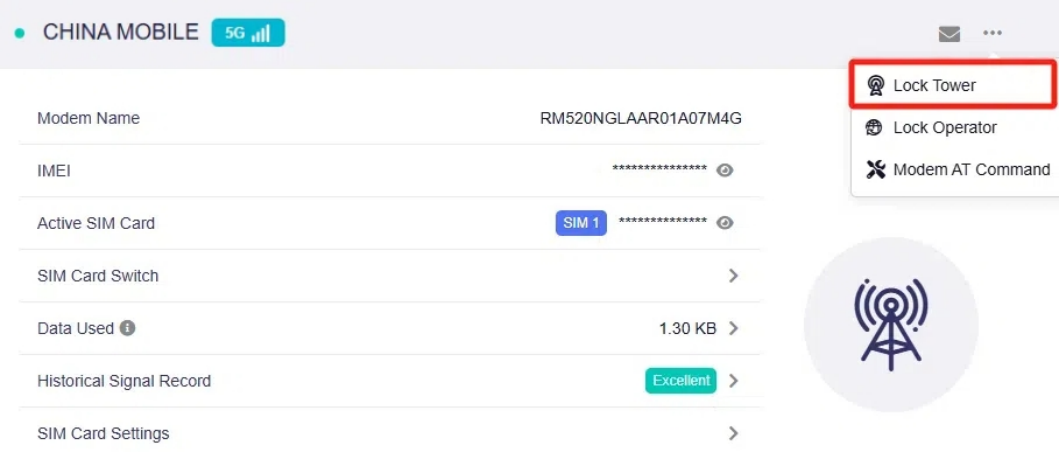
Consulte SMS y SMS Reenvío.

4.2.4.8 Fijar la estación base

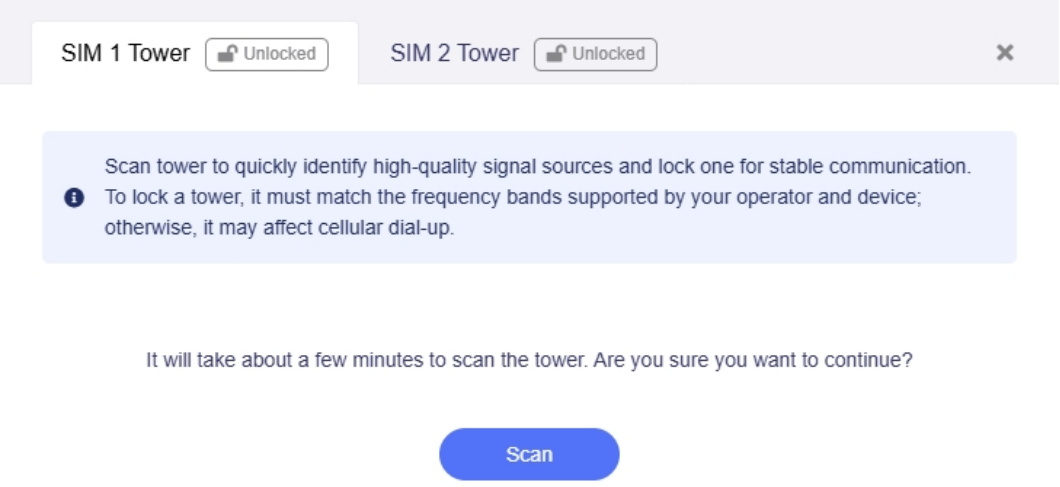
Si desea recibir una señal de alta calidad y garantizar una conexión celular estable, puede intentar bloquear la torre.

Nota: La torre bloqueada debe coincidir con las bandas de frecuencia admitidas por su proveedor y dispositivo; de lo contrario, la conexión puede fallar.

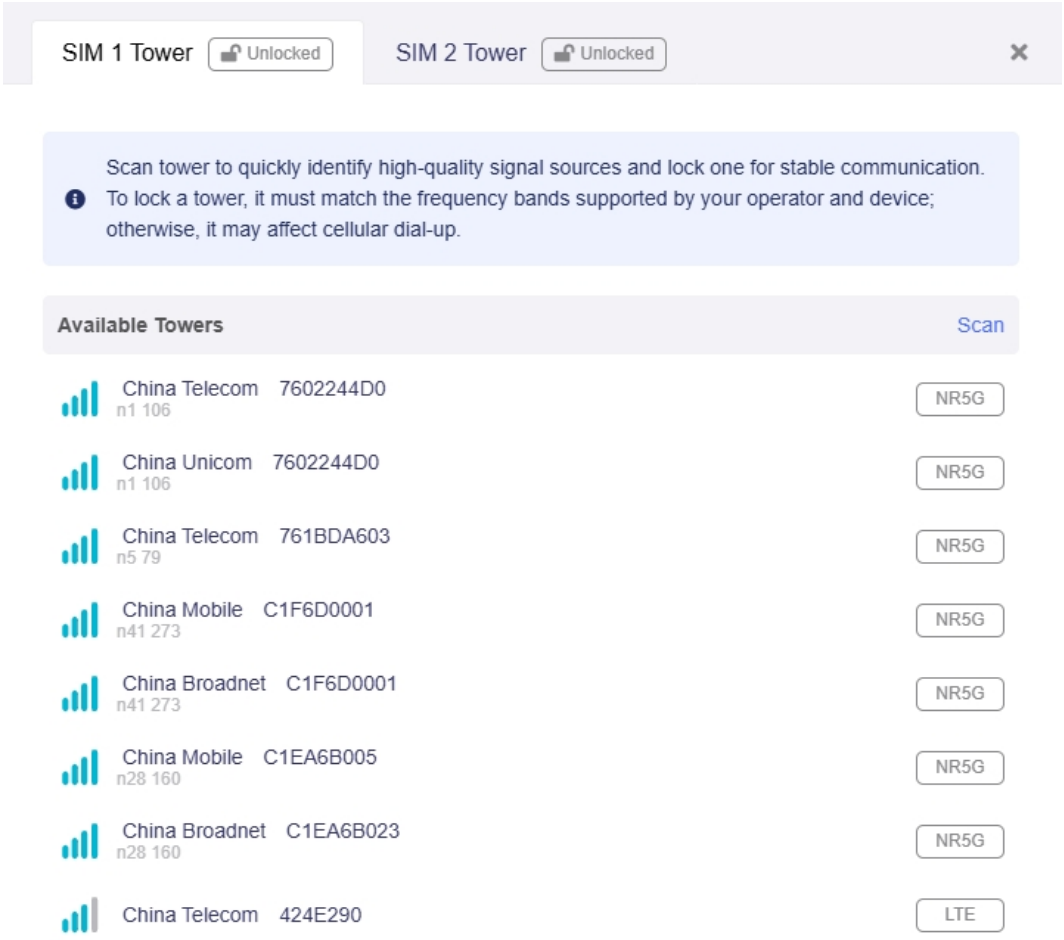
En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular**. Haga clic en el ícono de tres puntos en la esquina superior derecha y luego seleccione **Fijar la estación base**.



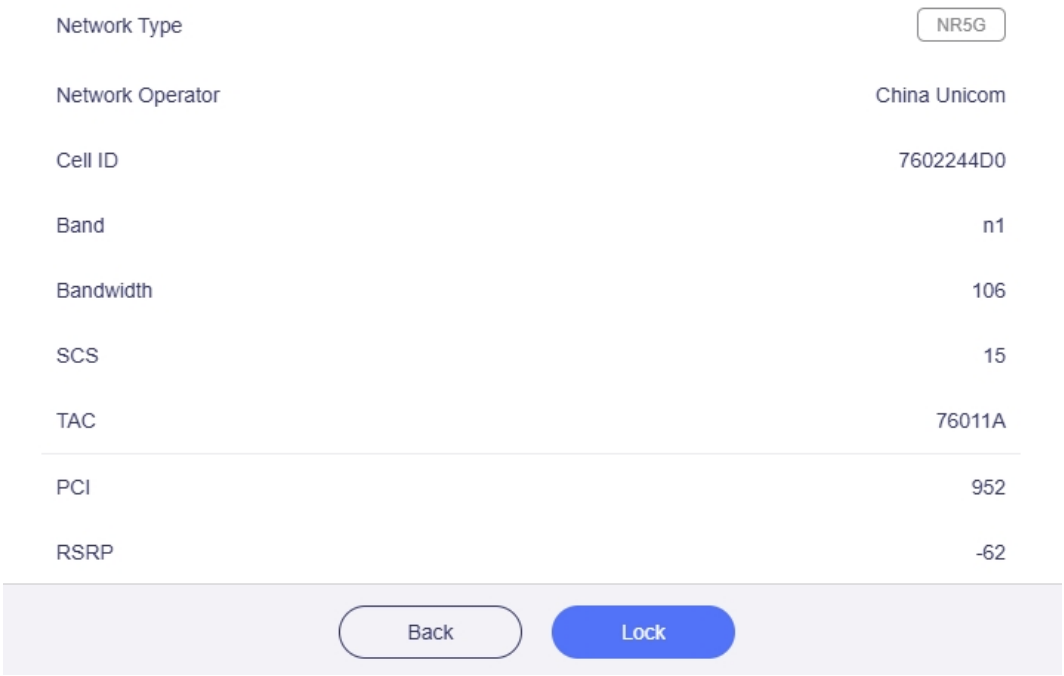
Haga clic en **Escanear** para comenzar a escanear las torres de señal celular. Tardará unos minutos. No actualice la página al escanear.



Se mostrarán las torres disponibles.



Haga clic en una torre para ver los detalles y bloquearla.



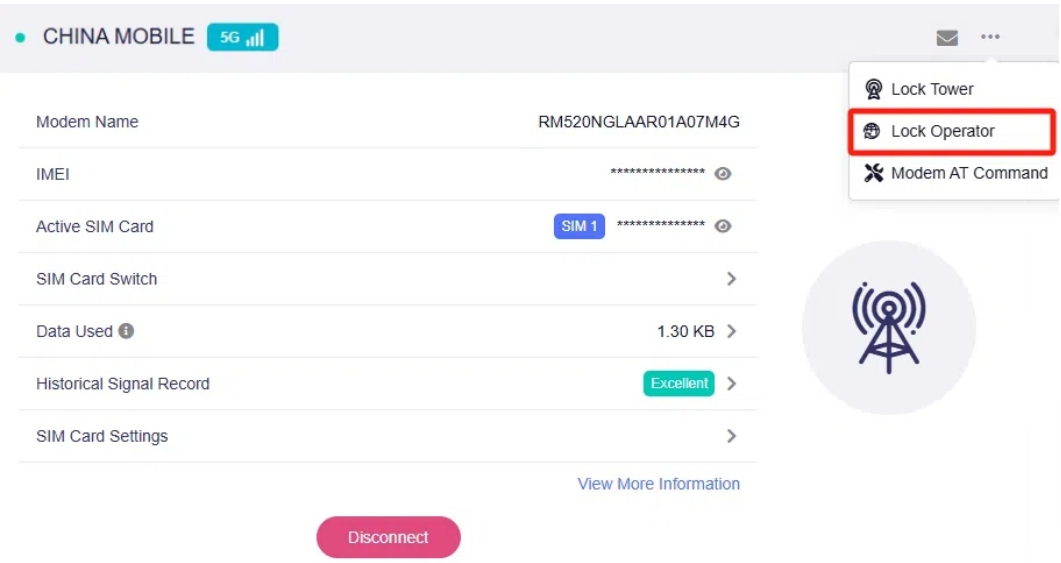
Nota:

1. Es posible que el dispositivo no pueda escanear todas las torres cuando la interfaz celular está habilitada.
2. Si la torre bloqueada no coincide con el enmascaramiento de banda o los parámetros APN en su configuración celular, el enrutador no podrá conectarse a la red celular.
3. Después de bloquear una torre celular, si mueve el enrutador a otra ubicación, aún intentará volver a conectarse a la torre bloqueada después de reiniciar. Esto puede impedir que el enrutador se conecte automáticamente a la red celular en la nueva ubicación. En este caso, deberá desbloquear la torre celular actual o bloquearla manualmente en una nueva torre.

4.2.4.9 Fijar el operador

Al bloquear a un operador móvil específico, el enrutador solo usará la red de ese operador, lo que garantiza una conexión estable y evita cargos de roaming no deseados, especialmente en áreas fronterizas donde De lo contrario, el dispositivo podría conectarse a redes extranjeras.

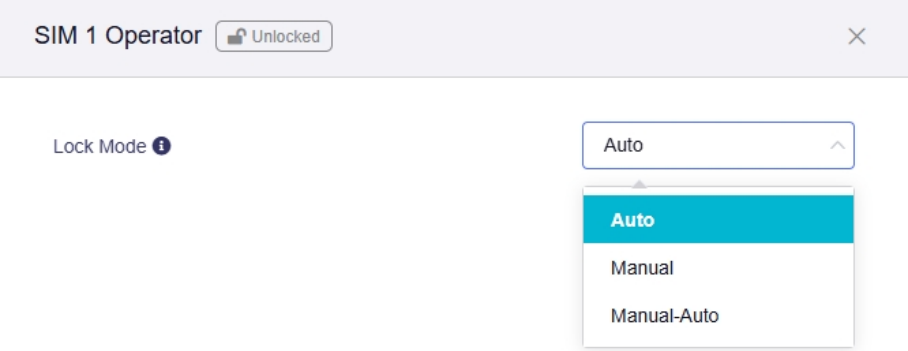
En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular**. Haga clic en el ícono de tres puntos en la esquina superior derecha y luego seleccione **Fijar el operador**.



Hay tres modos de bloqueo:

- **Automático**: conectarse automáticamente a un operador disponible red.
- **Manual**: bloquear manualmente a un operador específico.

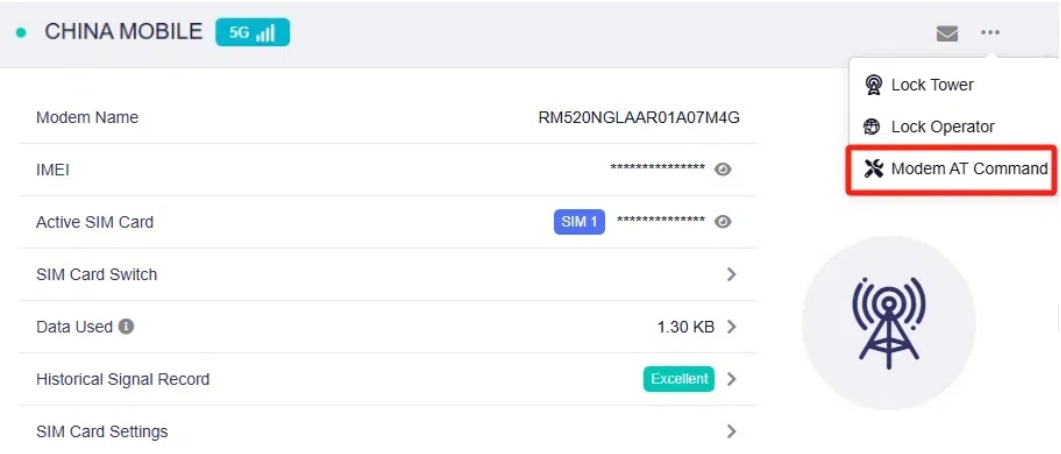
- **Manual-Auto**: cambiar automáticamente a una red de operador disponible si el bloqueo manual falla.



4.2.4.10 Comando AT del módem

Los comandos AT del módem son instrucciones estándar que se utilizan para comunicarse con el módem celular. Con esta función, puede enviar comandos y verificar el estado del módem.

En el panel de administración web del enrutador, navegue hasta **INTERNET** > **Celular**. Haga clic en el icono de tres puntos en la esquina superior derecha, luego seleccione **Comando AT del módem**.

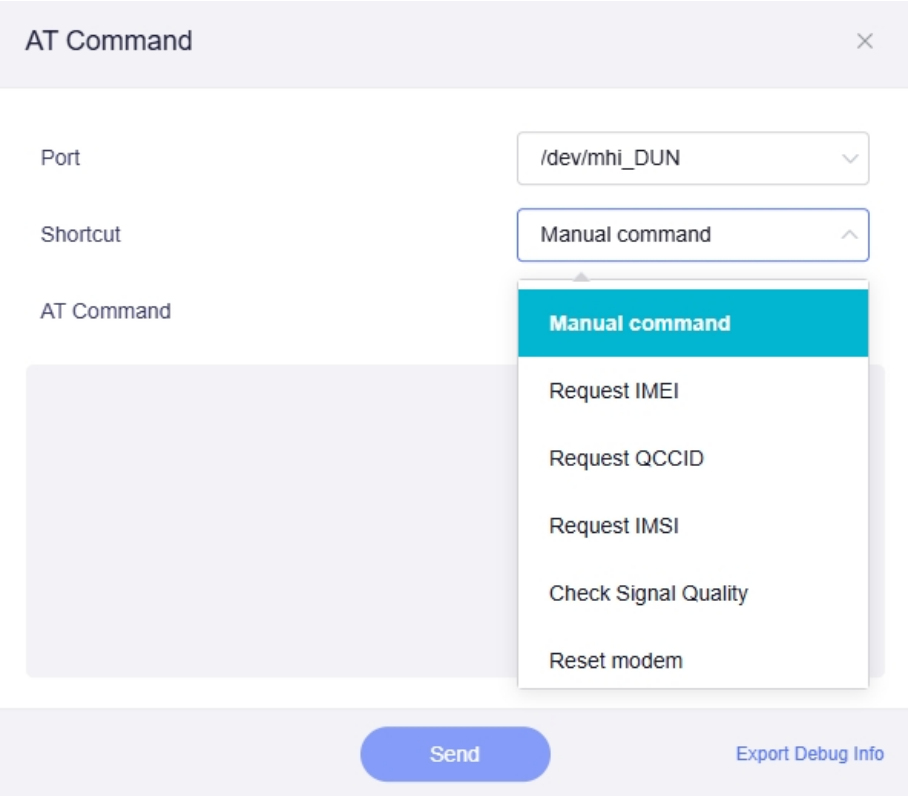


Ingresará a la página Comando AT.

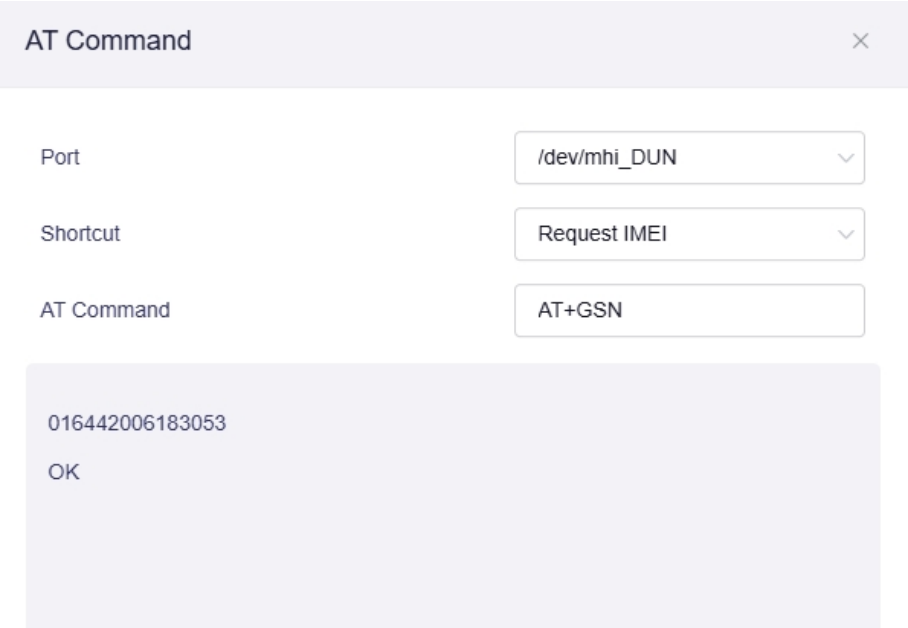
- **Comando manual**

  Cuando el acceso directo está configurado en Comando manual, puede escribir el comando que desee en el campo Comando AT y los resultados se devolverán en el cuadro gris inferior.
- **Preestablecido comando**

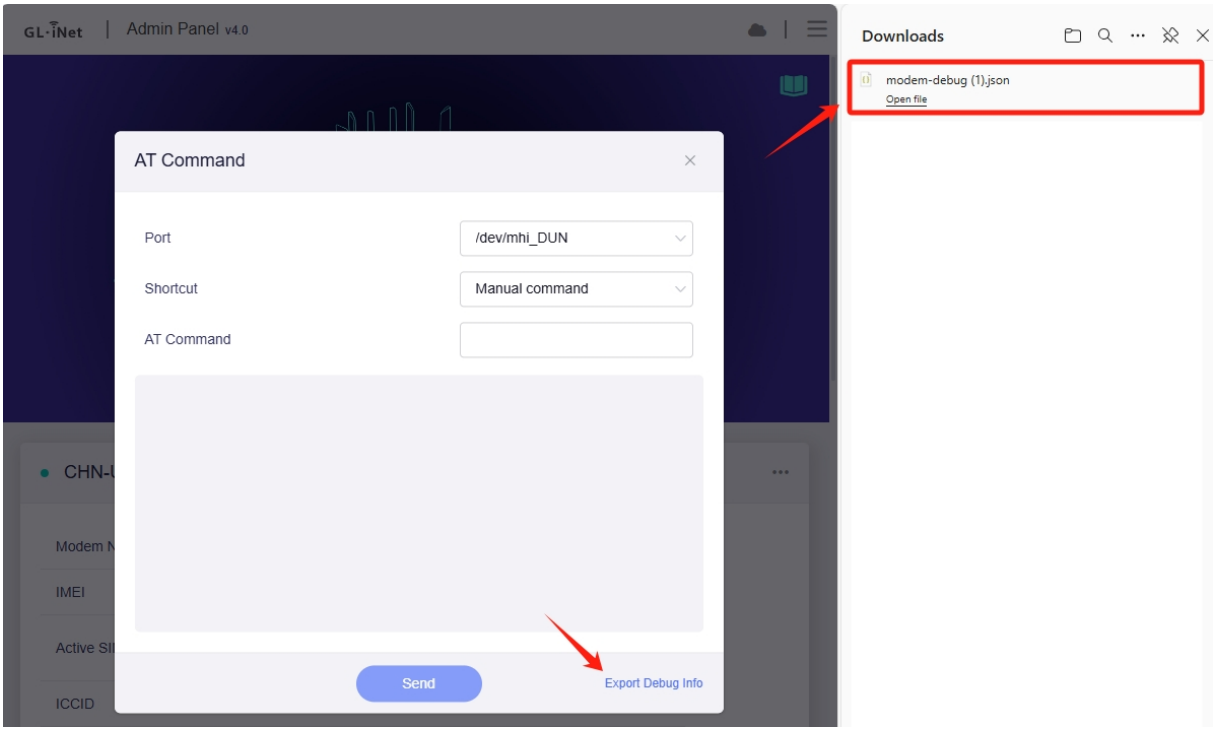
También puede hacer clic en el cuadro Acceso directo y seleccionar un comando preestablecido de la lista desplegable, como Solicitar IMEI, verificar la calidad de la señal, restablecer el módem, etc..



Por ejemplo, seleccione el acceso directo "Solicitar IMEI" y haga clic en "Enviar", luego obtendrá el resultado como se muestra a continuación.



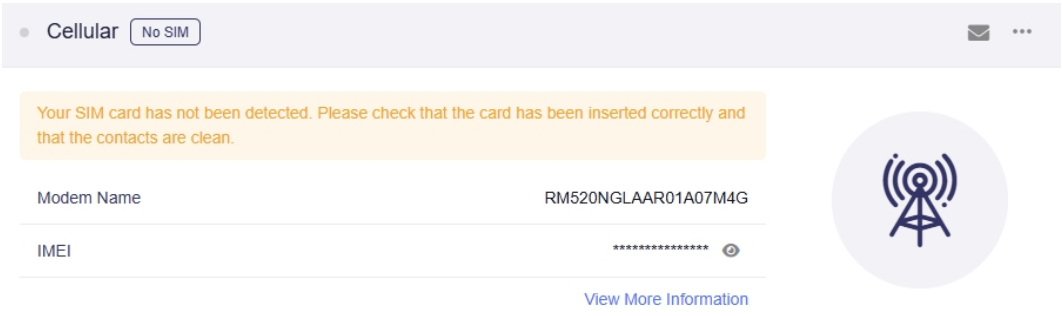
En la esquina inferior derecha, puede hacer clic en **Exportar información de depuración** para descargar un archivo .json.



4.2.4.11 Solución de problemas

Si no logra establecer una conexión celular, celija la solución correspondiente según el siguiente mensaje de error.

- **No SIM / Su SIM ctarjeta has not been detectado.**



Aquí hay algunas sugerencias.

1. Actualice la página y espere unos minutos para comprobar si se puede detectar la tarjeta SIM.

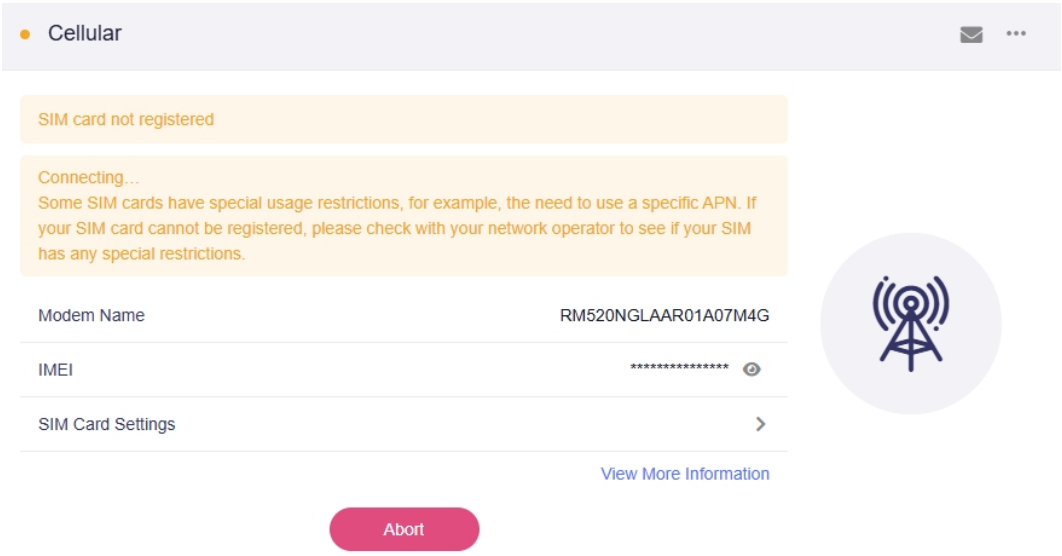
2. Asegúrese de que la tarjeta SIM esté instalada correctamente. Alinee la muesca de la tarjeta SIM con la marca correspondiente en la ranura para tarjetas para confirmar la orientación de inserción adecuada.
3. Apague el enrutador, retire y vuelva a insertar la tarjeta SIM, luego vuelva a encender el enrutador.
4. Intente usar otra tarjeta SIM si está disponible.

Si el problema persiste, descargue los registros y envíelos a support@gl-inet.com.

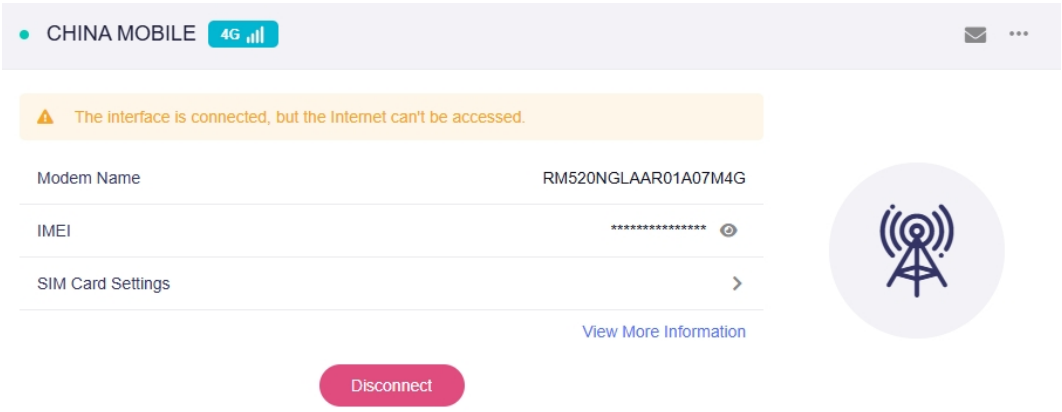
- **SIM card not rregistrado / La interfaz is cconectado, but tel Internet can't be accessed.**

Este problema tiene dos tipos de mensajes de error:

(1) Tarjeta SIM no registrada.

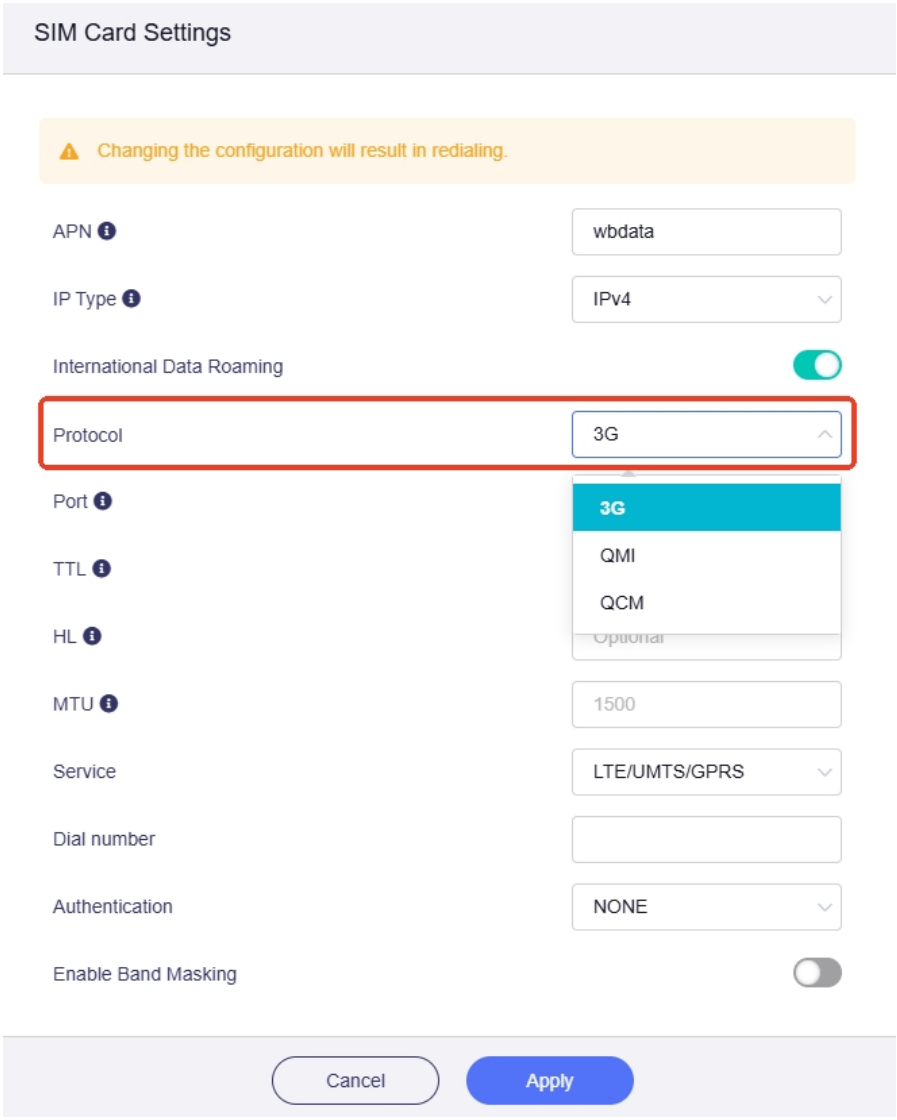


(2) La interfaz está conectada, pero no se puede acceder a Internet.



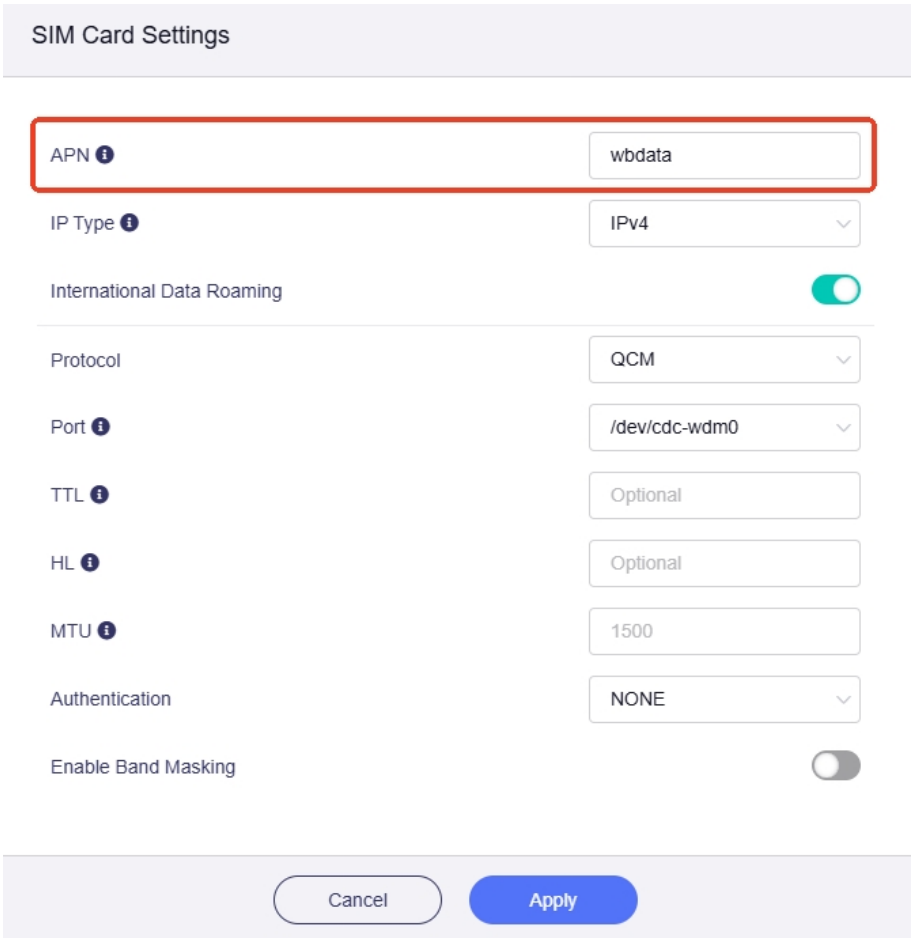
Aquí hay algunas sugerenciass.

1. Actualice la página y espere unos minutos para comprobar si aparece el error. desaparece.
2. Haga clic en **Desconectar**/**Abortar** y luego haga clic en **Conectar** para intentar volver a conectar.
3. Reinicie el enrutador.
4. Verifique el estado de la tarjeta SIM y asegúrese de que esté activada. Pruebe la tarjeta SIM insertándola en un teléfono inteligente para confirmar que puede acceder a Internet normalmente con un plan de datos móviles activo, o comuníquese con su proveedor de red para verificación.
5. Algunos proveedores de red pueden requerir un protocolo 3G para la conexión de red. Vaya a **Configuración de la tarjeta SIM** > **Protocolo**, seleccione **3G** y luego haga clic en **Aplicar**.



El dispositivo se volverá a conectar automáticamente. Espere unos minutos para comprobar si la conexión se realizó correctamente.

6. Algunas tarjetas SIM pueden tener restricciones de uso especiales (por ejemplo, requerir un APN específico). Si su tarjeta SIM no se registra, comuníquese con su proveedor para verificar si hay restricciones. Si es necesario, vaya a **Configuración de la tarjeta SIM** > **APN**, configure el APN correcto en el enrutador y luego haga clic en **Aplicar**.



7. Haga clic en **Ver más información** para verificar la intensidad de la señal celular. Si la señal es débil, asegúrese de que la antena esté instalada correctamente. Mueva el enrutador a una ubicación abierta y sin obstáculos para una mejor recepción de la señal.
8. Compruebe si **Enmascaramiento de banda** o **Fijar la estación base** está habilitado. Si es así, desactívelos e intente volver a conectarse.

Si el problema persiste, descargue los registros y envíelos a support@gl-inet.com.

Capítulo 5

Red inalámbrica

Este capítulo lo guía para verificar el estado de Wi-Fi y configurar la conexión inalámbrica settings.

5.1 Visualización del estado de Wi-Fi

El enrutador’s Wi-Fi las redes están habilitadas de forma predeterminada, y el ícono de Wi-Fi correspondiente se iluminará debajo de la imagen del dispositivo en INTERNET página.



Isi el cursor se sitúa sobre el icono de Wi-Fi habilitado, aparecerá El código QR de Wi-Fi se mostrará de la siguiente manera. Puedes escanear el código QR de Wi-Fi para conectarte rápidamente al Wi-Fi correspondiente.

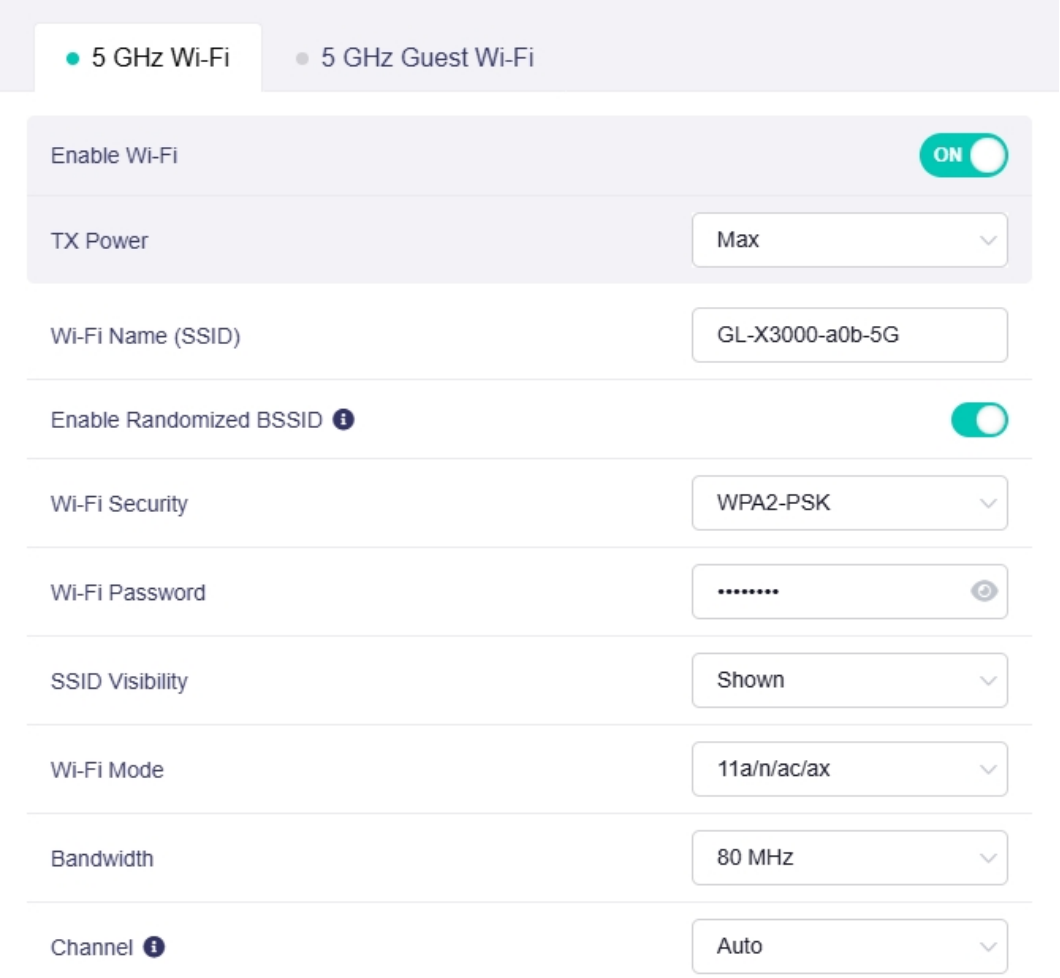


5.2 Configuración inalámbrica

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra la configuración de Wi-Fi del enrutador's 2,4 GHz y 5 GHz, con cada más dividido en redes Wi-Fi principal y Wi-Fi para invitados-Fi para una administración flexible .

5.2.1 Wi-Fi de 5 GHz

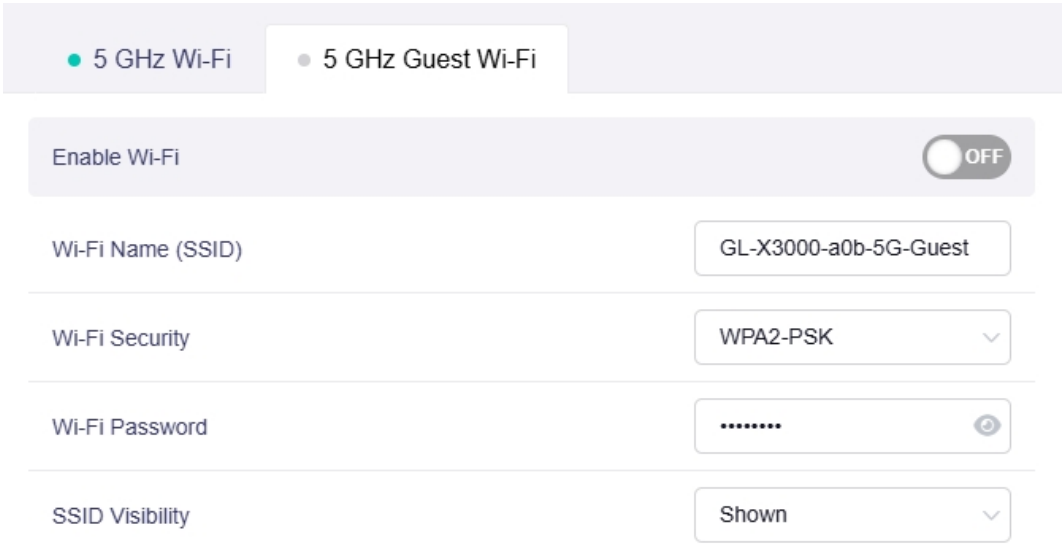
El Wi-Fi principal de 5 GHz le permite configurar múltiples ajustes, incluyendo habilitar/deshabilitar Wi-Fi, configurar la potencia de TX, habilitar/deshabilitar BSSID aleatorio, configurar Wi-Fi nombre (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda y canal.



Nota:

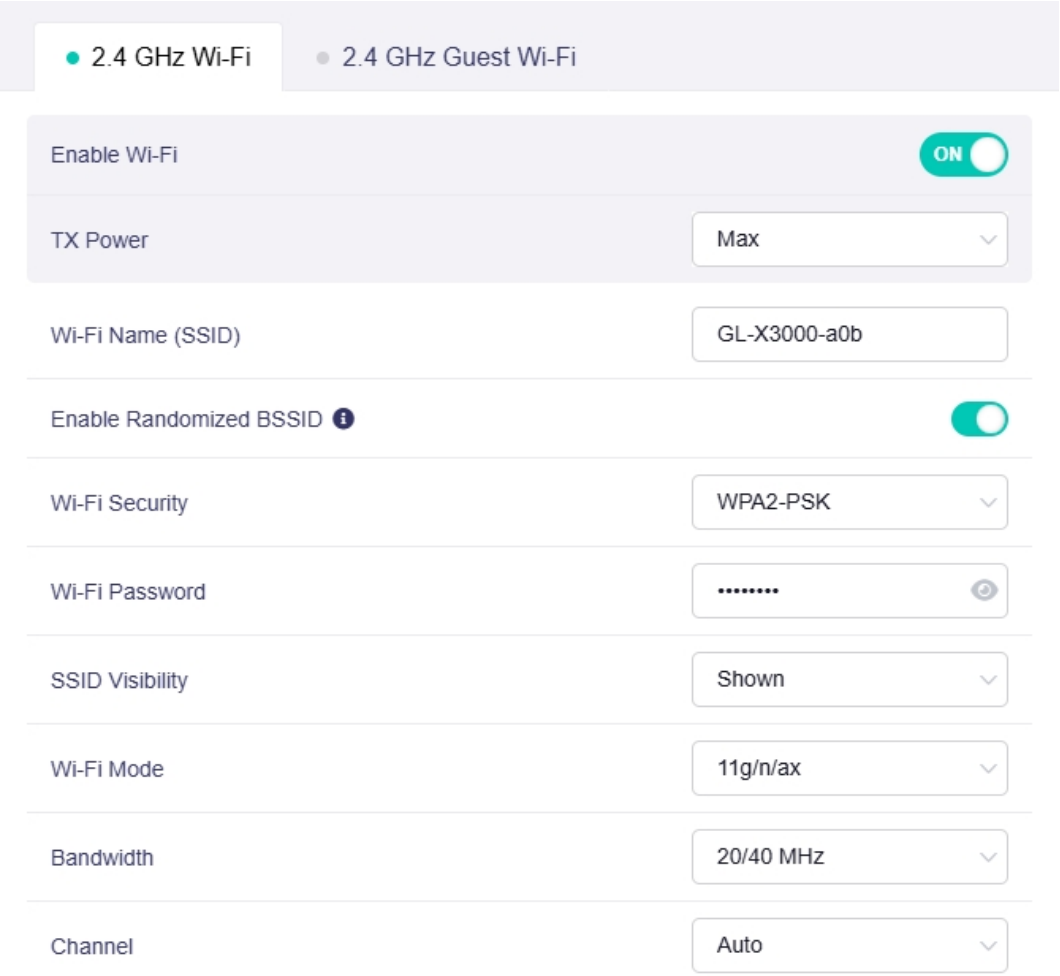
1. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.
2. El **ancho de banda** y **canal** puedeno se puede modificar cuando el enrutador está configurado como a repeater, ya que siguen la de la red repetida.
3. Cuando **Canal** está establecido a **Auto**, el enrutador's Wi-Fi no cambiará automáticamente al canal DFS.
4. Cuando **Ancho de banda** está configurado en **160 MHz** (solo disponible en algunos modelos), Wi-Fi siempre utilizará el canal DFS, incluso si selecciona un canal que no es DFS o lo configura en Auto.

El 5GHz Invitado Wi-Fi le permite configurar configuraciones simplificadas, que incluyen habilitar/deshabilitar Wi-Fi, configurar el nombre de Wi-Fi (SSID), la seguridad, la contraseña y la visibilidad de SSID.



5.2.2 Wi-Fi de 2,4 GHz

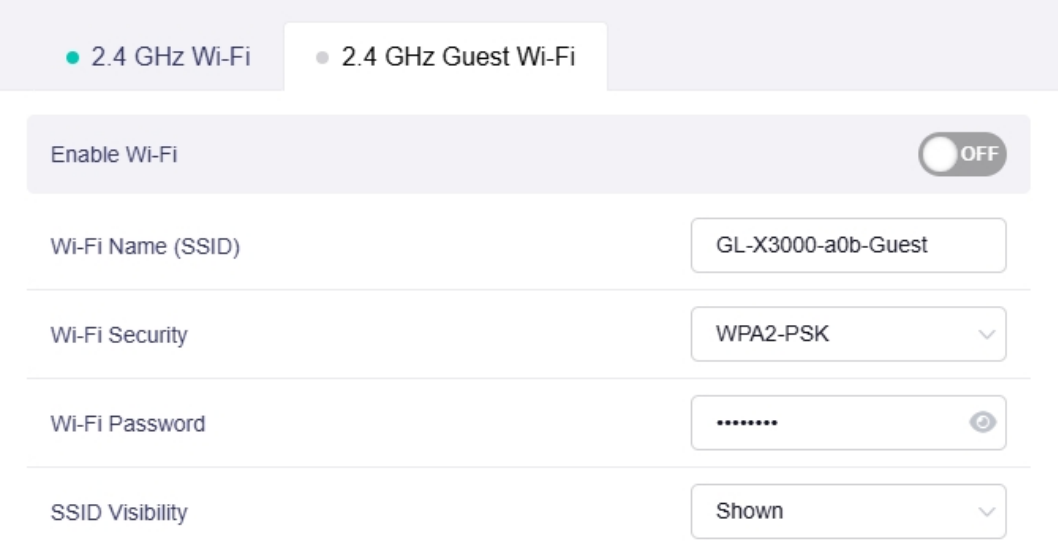
El Wi-Fi principal de 2,4 GHz le permite configurar múltiples ajustes, incluida a configurar múltiples ajustes, incluido activar/deshabilitar Wi-Fi, configurar la potencia de TX, habilitar/deshabilitar BSSID aleatorio, configurar nombre de Wi-Fi (SSID), seguridad, contraseña, SSID visibilidad, modo, ancho de banda y canal.



Nota:

1. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.
2. El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repeater, ya que siguen el de la red repetida.

El 2.4GHz Invitado Wi-Fi le permite usted configurar configuración simplificada, que incluyeg habilitación/ deshabilitación Wi-Fi, configuración nombre de Wi-Fi (SSID), seguridad, contraseña y visibilidad de SSID.



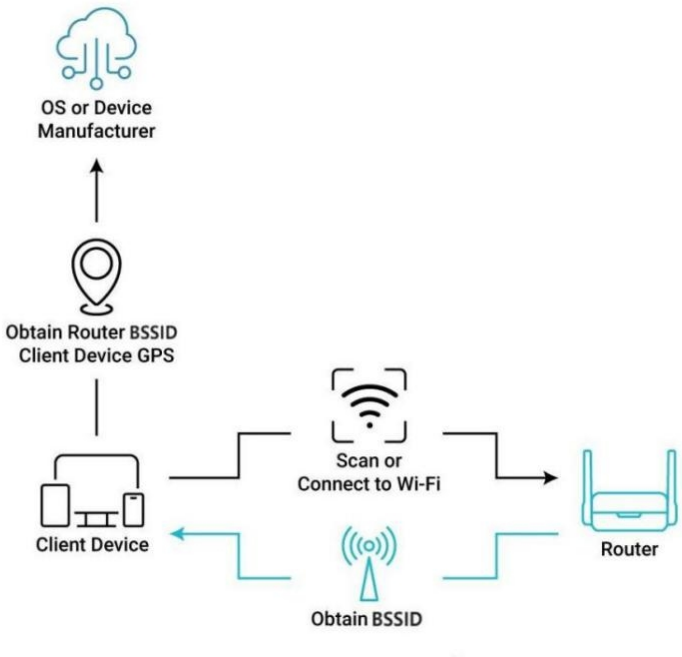
5.2.3 BSSID aleatorio

BSSID aleatorio es una característica de privacidad disponible desde el firmware v4.6 y habilitada de forma predeterminada. Evita que su enrutador sea localizado y rastreado a través de un BSSID Wi-Fi fijo (la dirección MAC de la interfaz inalámbrica del enrutador).

Por qué un BSSID fijo es un riesgo para la privacidad

Los sistemas operativos móviles (por ejemplo, Android e iOS) dependen del posicionamiento Wi-Fi de fuentes múltiples para proporcionar ubicación servicios:

1. Los dispositivos cliente (teléfonos, portátiles) cargan periódicamente los BSSID que pueden ver, junto con su propia ubicación derivada del GPS, al servidor del proveedor del sistema operativo/dispositivo.
2. Los proveedores agregan estos datos en un BSSID a ubicación global base de datos.
3. Cualquier dispositivo con Wi-Fi habilitado, incluso sin GPS, puede consultar esa base de datos para estimar su ubicación a partir de los BSSID que lo rodean.
4. Como resultado, un enrutador con un BSSID fijo actúa como una baliza de ubicación estacionaria: puede ubicarse geográficamente. de forma remota, y sus movimientos (por ejemplo, cuando viaja con él) se pueden rastrear a lo largo del tiempo. Los atacantes también pueden consultar dichas bases de datos para localizar enrutadores o tomar huellas digitales a través de la información del proveedor (OUI) del BSSID.



Cómo te protege el BSSID aleatorio

Cuando esta característica está habilitada, el enrutador genera un BSSID aleatorio y lo renueva en cada arranque. Dado que el BSSID sigue cambiando, ya no se puede vincular a una ubicación fija en las bases de datos del proveedor, lo que rompe la asociación de ubicación BSSID utilizada para el seguimiento.

Estado	Comportamiento
Habilitado (predeterminado)	Se genera y renueva un nuevo BSSID aleatorio en cada inicio
Deshabilitado	El enrutador utiliza su dirección MAC real de fábrica como BSSID

Notas:

1. El BSSID cambia solo cuando el enrutador se reinicia; permanece igual durante una sesión en ejecución.
2. Para Wi-Fi para invitados, el BSSID permanece consistente con el BSSID de Wi-Fi principal en la misma banda de frecuencia.
3. El BSSID aleatorio bloquea el seguimiento a través del BSSID del enrutador, pero no detiene al cliente los dispositivos informen su propia ubicación y no es una solución de privacidad completa: aún se pueden observar las características de SSID, canal y señal.

Capítulo 6

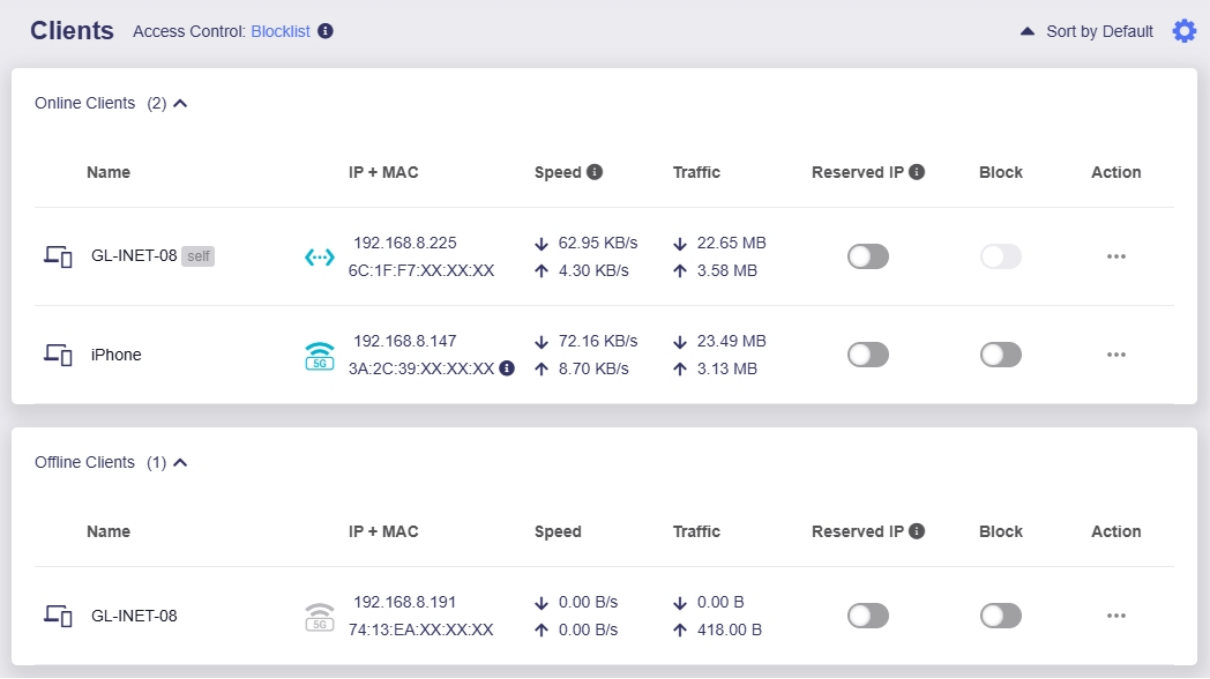
Clientes

Este capítulo lo guía para ver los detalles de los dispositivos conectados. dispositivos y administrar sus conexiones.

6.1 Detalles del dispositivo

Inicie sesión en su enrutador’s panel de administración web y vaya a **CLIENTES**.

La página Clientes muestra información sobre los dispositivos conectados, incluido el nombre del dispositivo, el tipo de conexión, la IP y Dirección MAC, velocidad y tráfico, dispuestos de izquierda a derecha. También proporciona acceso rápido para reservar IP, bloquear cliente o realizar otras acciones.



Consejo: Los clientes en línea se refieren a los dispositivos actualmente conectados a la red del enrutador. Los clientes sin conexión se refieren a dispositivos que se han conectado previamente al enrutador pero que ahora están desconectadosconectado desde la red.

1. **Nombre del dispositivo**

   La primera columna muestra el nombre del dispositivo y tipo, que depende del nombre de host del operador del dispositivo. El icono azul junto a el nombre del dispositivo representa el método de conexión, indicaque el dispositivo está conectado al enrutador a través de un Ethernet cable.

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado. Si los dispositivos conectados utilizan aleatoriamente MAC direcciones, aparecerá un mensaje, indicando que se trata de una dirección MAC aleatoria.



Isi el segundo carácter de la dirección MAC es 2, 6, A o E (Ignorar mayúsculas y minúsculas), se considera como una dirección MAC aleatoria. Sin embargo, algunos dispositivos pueden usar una regla diferente para generar una dirección MAC aleatoria, por lo que este método de detección puede no ser preciso.

3. **Velocidad**

   La tercera columna muestra la velocidad de Internet del dispositivo conectado. Thes velocidad representa la velocidad promedio durante los últimos 3 minutos. El sistema comienza a calcular la velocidad promedio cuando se abre esta página (por ejemplo, si la página solo ha estado abierta durante 10 segundos, la velocidad promedio se basará en solo 10 segundos de datos).

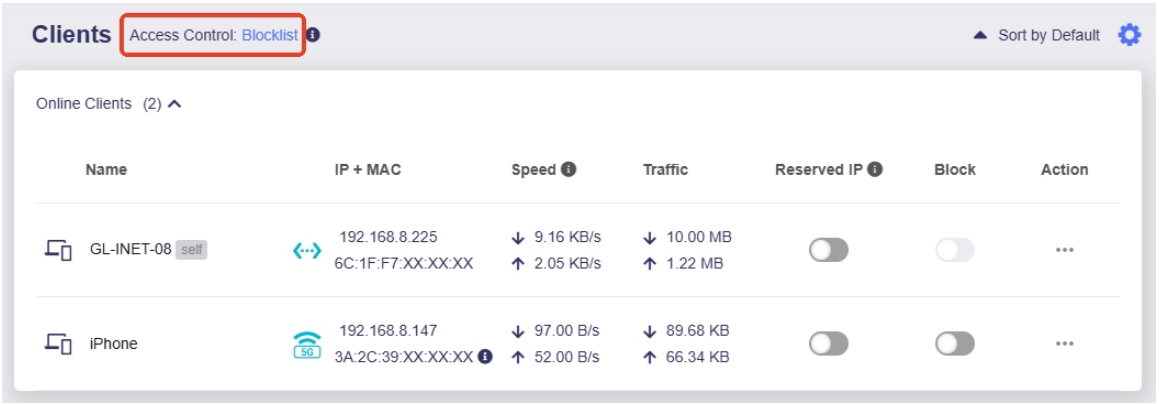
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet de los usuarios conectados dispositivo.

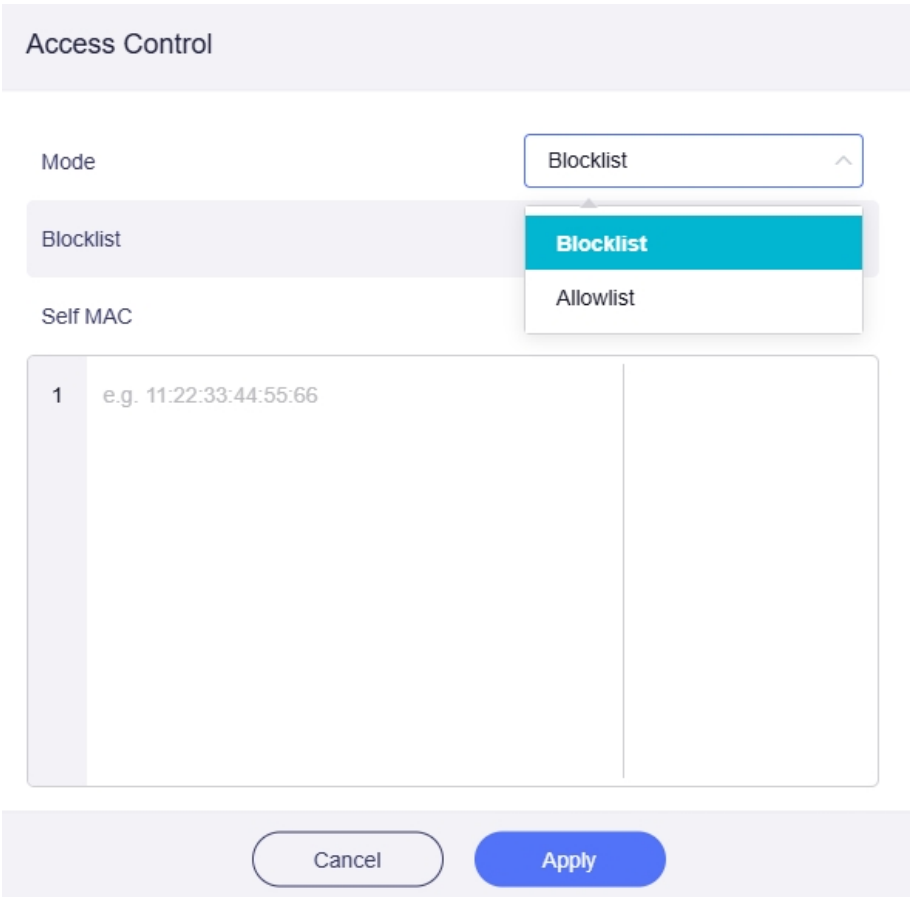
5. **Reservar IP**

   En la quinta columna, puede reservar la dirección IP para dispositivo conectado con un clic. Cuando especifica una dirección IP reservada para un cliente dentro de la red de área local,, siempre recibirá la misma dirección IP cada vez se conecta a el enrutador.

6. **Lista de bloqueo**

   En la sexta columna, puede bloquear dispositivos conectados específicos con un clic. La Aregla de control de acceso Ces Lista negra de forma predeterminada y puedes cambiarla a Lista permitida desde la parte superior si es necesario.



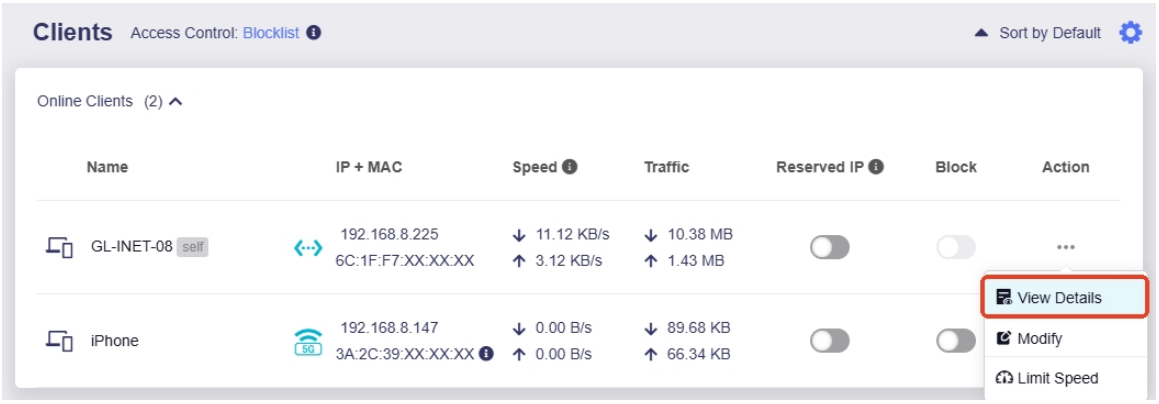


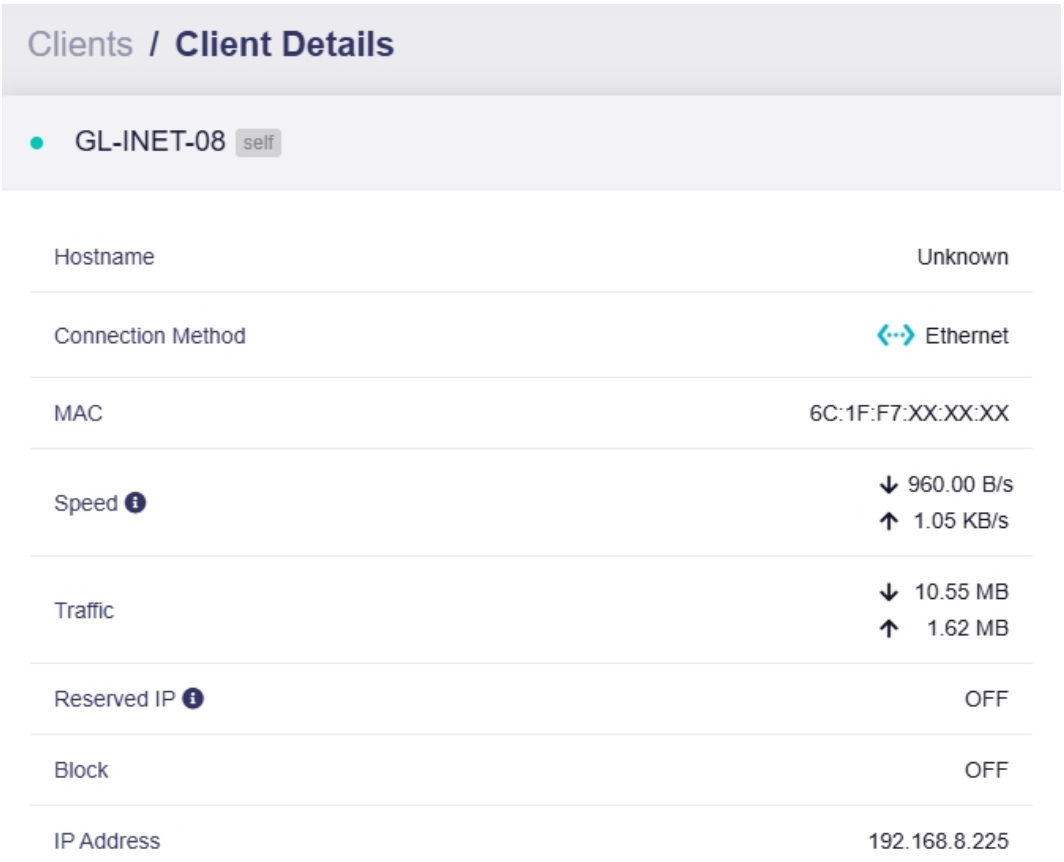
- **Lista negra**: los dispositivos con direcciones MAC en la lista negra no está permitido conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.
- **Lista de permitidos**: solo los dispositivos con direcciones MAC específicas pueden conectarse a este enrutador, adecuado para IoT dispositivos y administración de redes empresariales.

6.2 Acción

1. **Ver detalles**

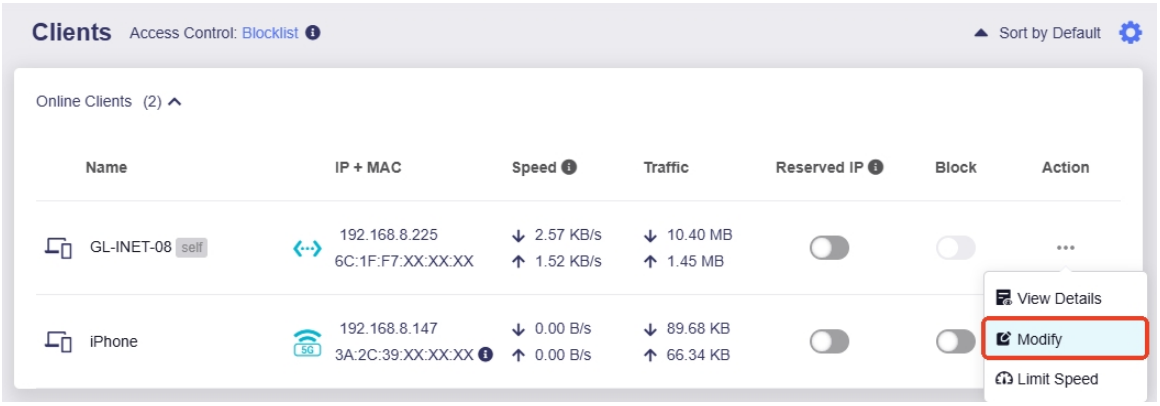
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

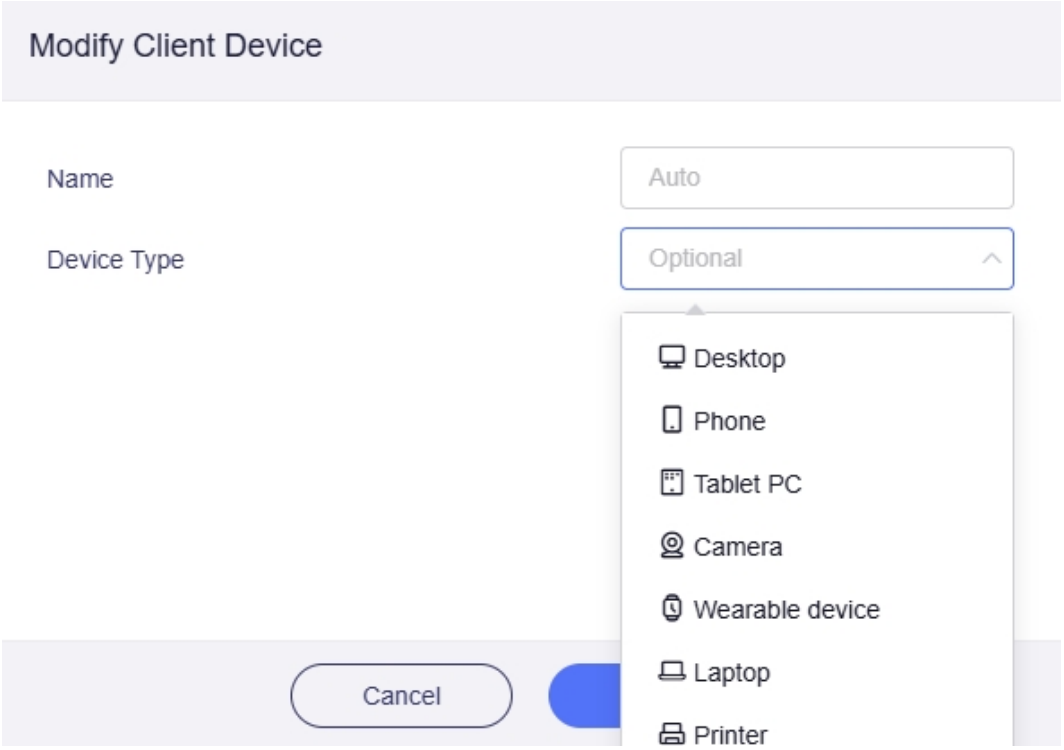




2. **Modificar**

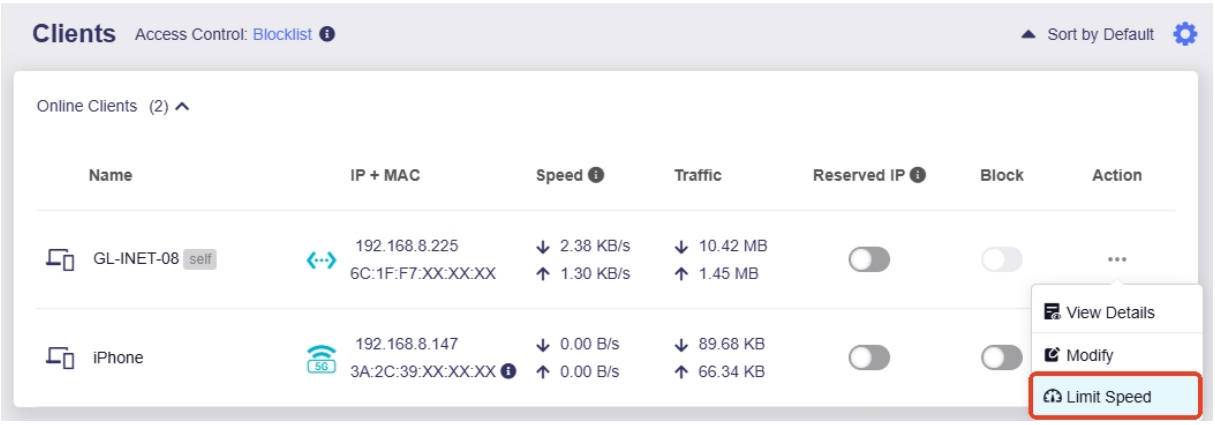
Haga clic en el icono de tres puntos en la columna **Acción** y haga clic en **Modificar** desde el menú desplegable para modificar el nombre y tipo del dispositivo.



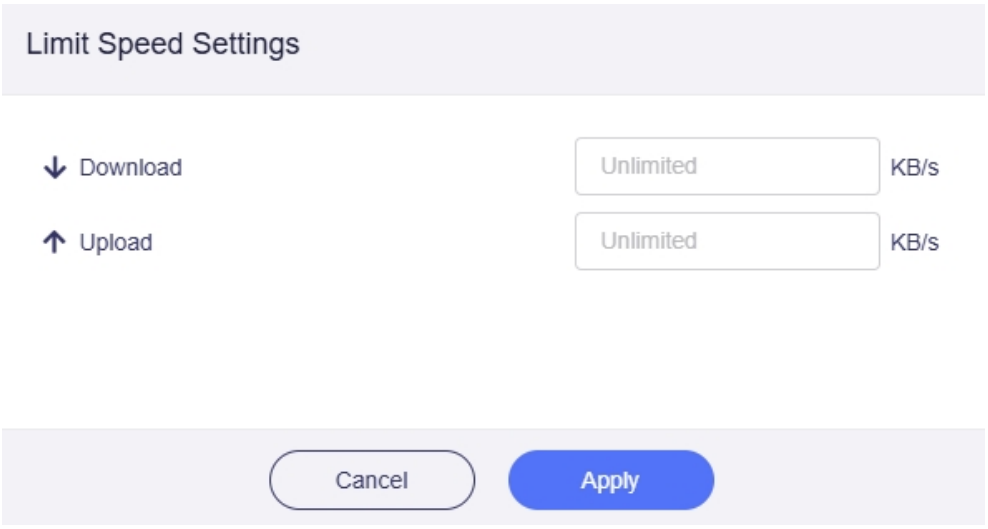


3. **Limitar velocidad**

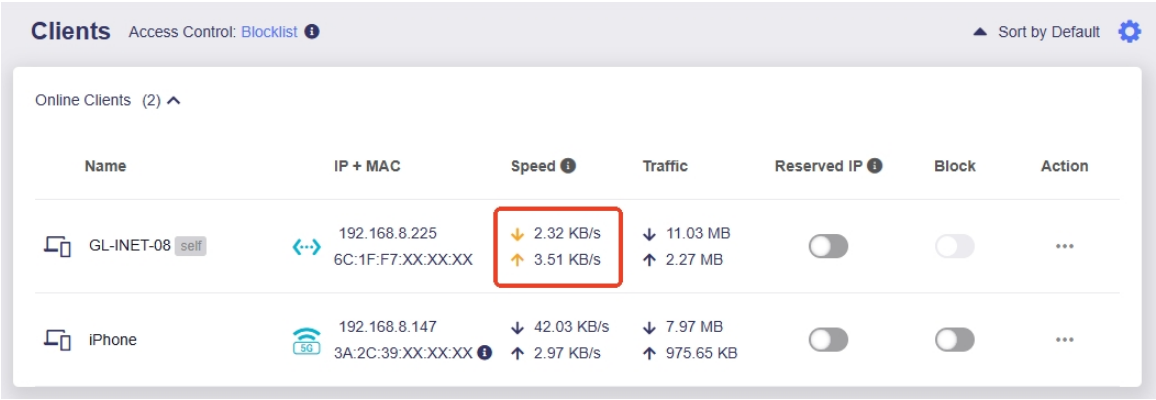
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



Podrás limitar la velocidad de un dispositivo conectado, con la unidad configurada en KB/s.

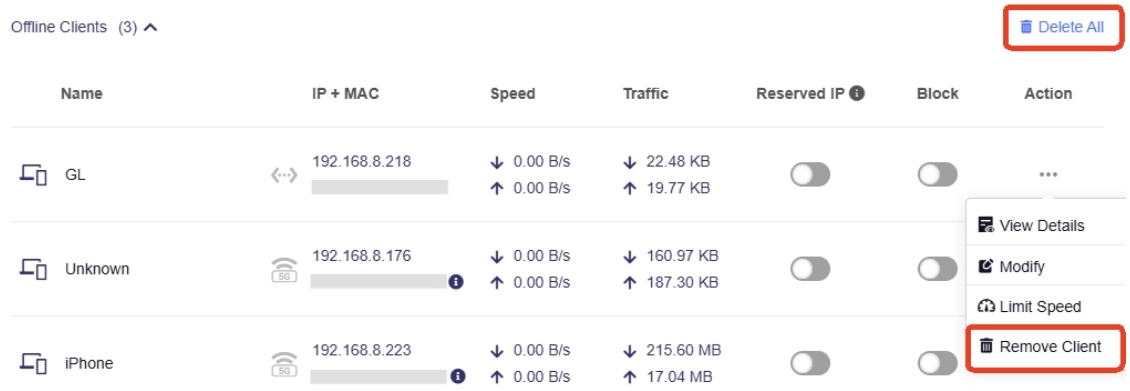


Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



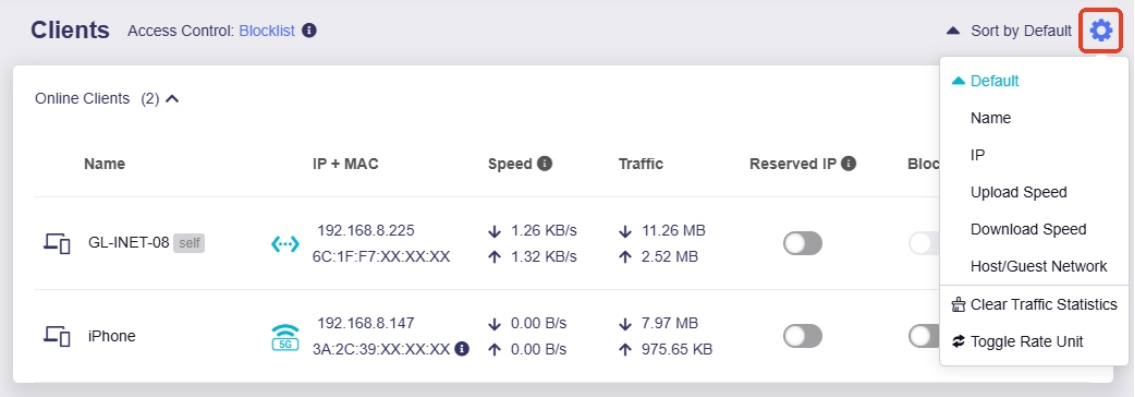
6.3 Eliminar clientes

En la sección **Offline Cclientes**, puedes hacer clic en **Eliminar todo** en la esquina superior derecha para eliminar todos los clientes sin conexión. Si desea eliminar un cliente específico, haga clic en el icono de tres puntos en la **Acción** columna, luego haga clic en **Eliminar cliente** de menú desplegable.



6.4 Ordenar

Puede configurar la regla de clasificación de dispositivos para el Cliente página en la superior esquina derecha.



La clasificación predeterminadaing reglas son de la siguiente manera:

- El dispositivo propio (es decir, el dispositivo utilizado para acceder al panel de administración web del enrutador') siempre está en la lista primer.
- En el **Oen línea Cclientes**, los dispositivos aparecen en una lista más alta si se conectaron antes.
- En la **Apagadolínea Cclientes**, los dispositivos aparecen en una lista superior si nose conectaron antes.

Capítulo 7

Servicios en la nube

Este capítulo presenta dos servicios en la nube: GoodCloud y AstroWarp.

7.1 GoodCloud

GL.iNet GoodCloud es una plataforma diseñada para simplificar la implementación y administración remota de dispositivos conectados. Proporciona una manera fácil de acceder y administrar de forma remota los enrutadores GL.iNet. Al centralizar los dispositivos de red en la nube, los usuarios pueden realizar de manera eficiente tareas de administración de lotes, como implementar configuraciones de red y realizar actualizaciones de software. También pueden acceder de forma remota al panel de administración web del enrutador o conectarse al terminal del enrutador a través de SSH, logrando una administración de dispositivos de red interregional y de extremo a extremo.

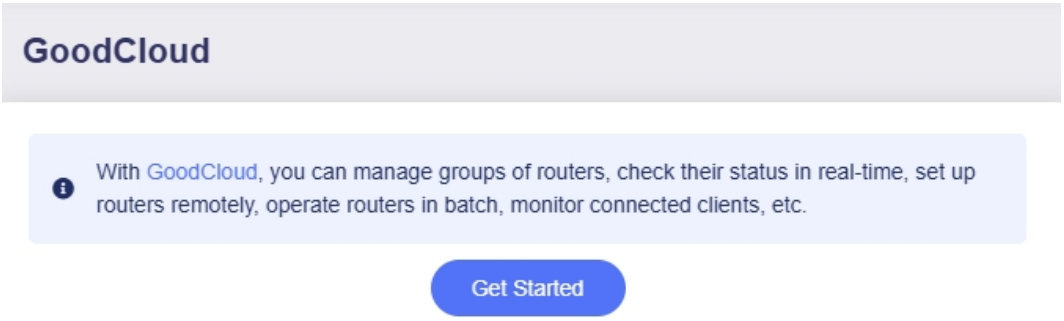
Con GoodCloud, puede:

- Comprueba el estado de tu enrutador en tiempo real
- Administrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitorear clientes conectados
- Operar enrutadores por lotes
- Establecer conexión de sitio a sitio

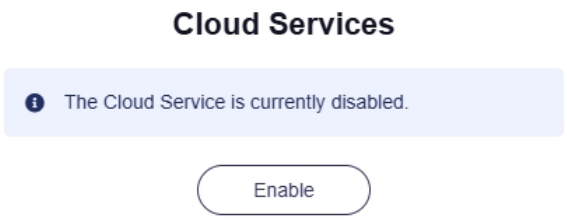
Algunas características están disponibles en el Plan Empresarial y en el Plan VAR (Reseller de Valor Agregado). Consulte aquí para obtener más detalles.

7.1.1 Habilitar GoodCloud

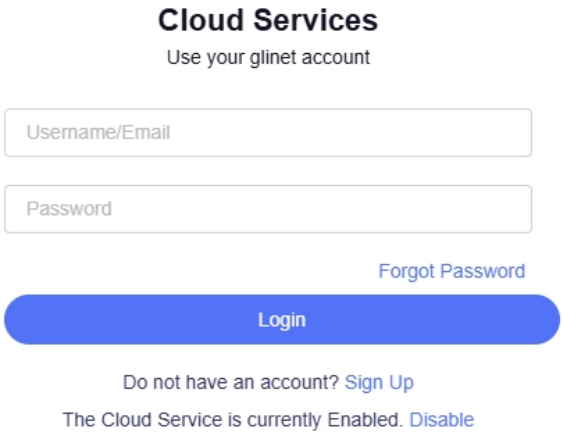
1. Inicie sesión en su enrutador panel de administración web, vaya a **SERVICIO DE NUBE** > **GoodCloud** y haga clic **Comenzar**.



2. Aparecerá una ventana desplegable en la esquina superior derecha. Haga clic en **Activar**.



3. Inicie sesión con su cuenta GL.iNet Cloud. Si no tiene una cuenta, regístrese para obtener una e inicie sesión. Una vez que haya iniciado sesión, el enrutador se vinculará a su cuenta automáticamente.

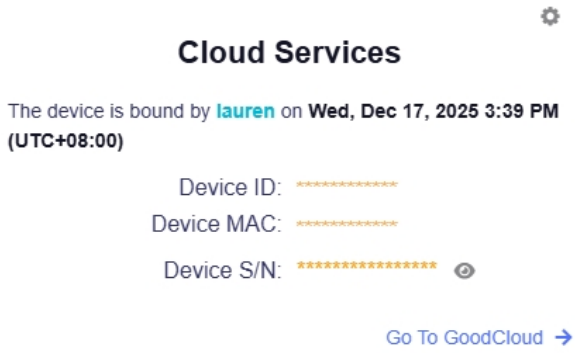


Consejos:

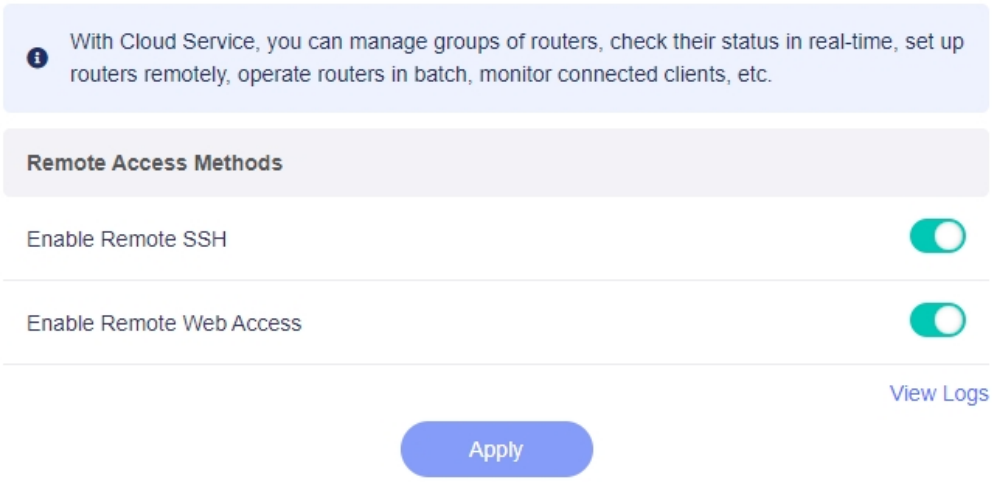
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.

- Si no recibe el correo electrónico de verificación, revise su carpeta de correo no deseado o inténtelo nuevamente más tarde. Para más ayuda, contáctenos en support@gl-inet.com.

4. Después de vincular correctamente, haga clic en el **icono de nube** en la esquina superior derecha del panel de administración web. Luego verá los detalles del dispositivo vinculado, incluida la cuenta vinculada, la fecha de vinculación, el ID del dispositivo, la MAC del dispositivo y el S/N del dispositivo.



5. Navegue a **SERVICIOS EN LA NUBE** > **GoodCloud** y habilite el acceso remoto. GoodCloud proporciona acceso remoto al panel de administración web y al terminal del enrutador vinculado. Puede habilitar o deshabilitar el acceso remoto para su enrutador aquí.

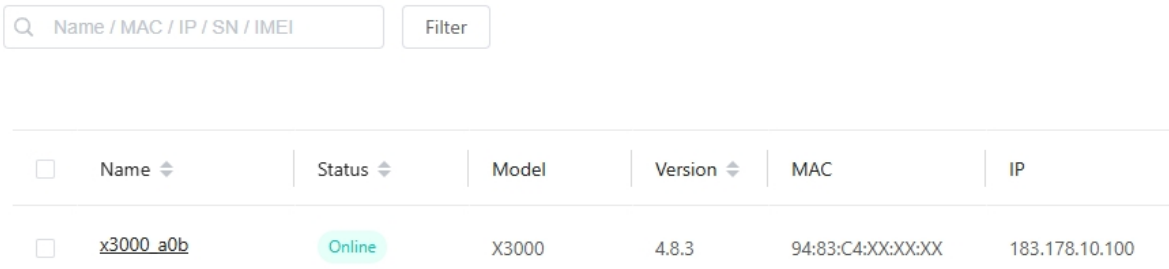


- **SSH remoto:** Acceda remotamente al terminal del enrutador desde GoodCloud usando SSH.
- **Acceso web remoto:** Acceda de forma remota al panel de administración web del enrutador desde GoodCloud a través de HTTP/HTTPS.
- **Ver registros:** Redirigir a la página de registro y mostrar Registro en la nube.

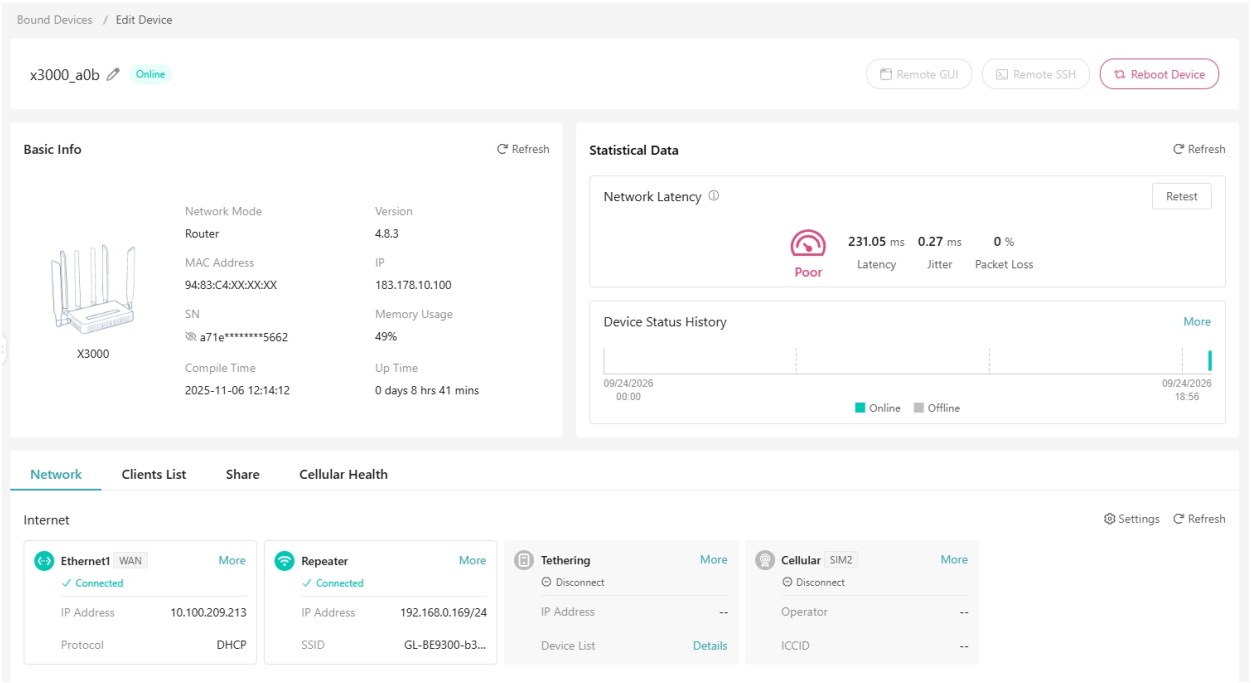
7.1.2 Administrar el enrutador

7.1.2.1 Consultar los detalles del dispositivo

Inicie sesión en la GoodCloud plataforma y navegue a **Dispositivo** > **Dispositivos vinculados**. Yusted puede ver la información básica del's, como nombre de host, estado (en línea/fuera de línea), modelo, versión de firmware, y MAC dirección.

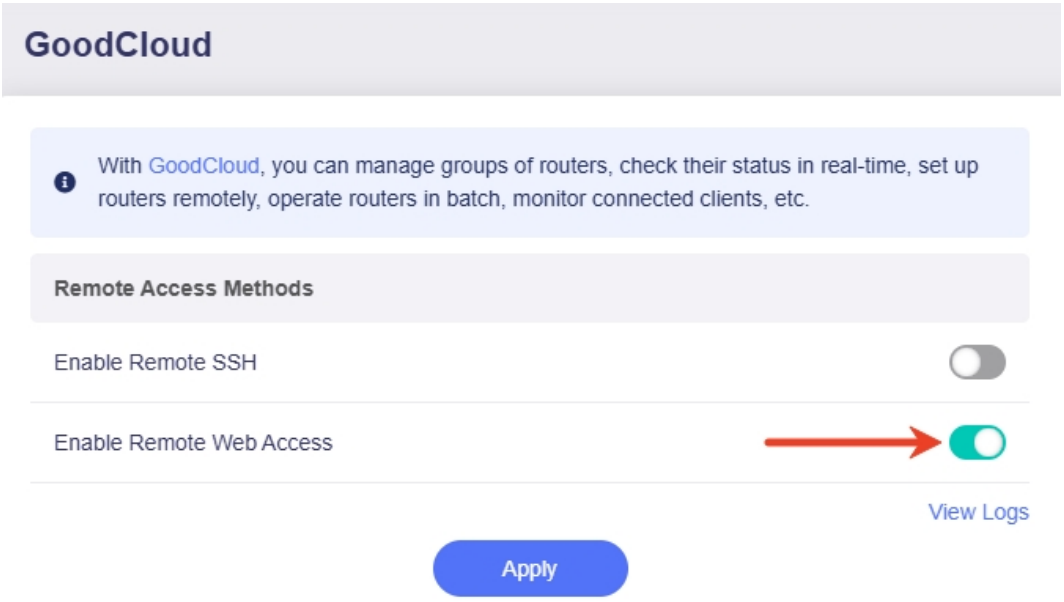


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes, y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando el dispositivo.

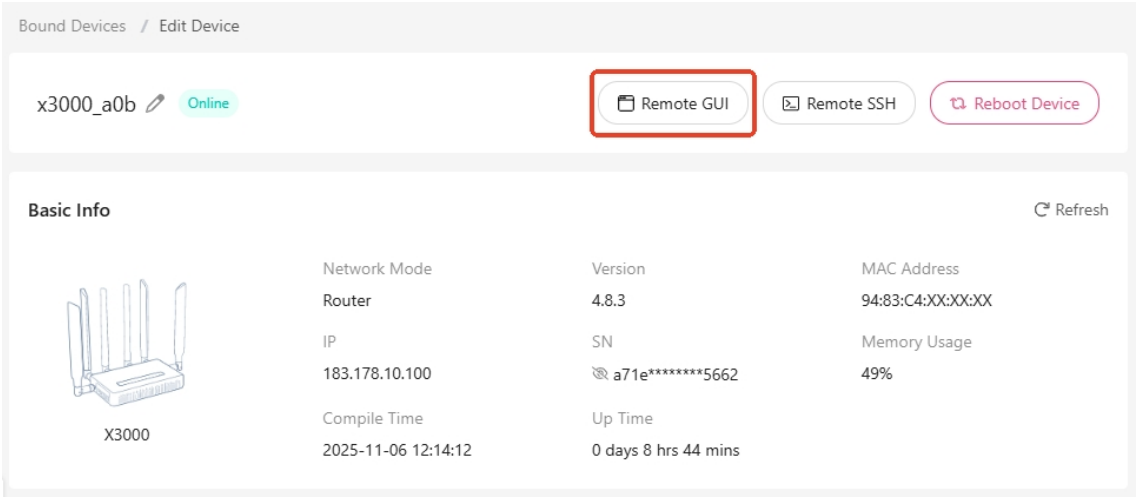


7.1.2.2 Acceso web remoto

1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso web remoto**, luego haga clic en **Aplicar**.

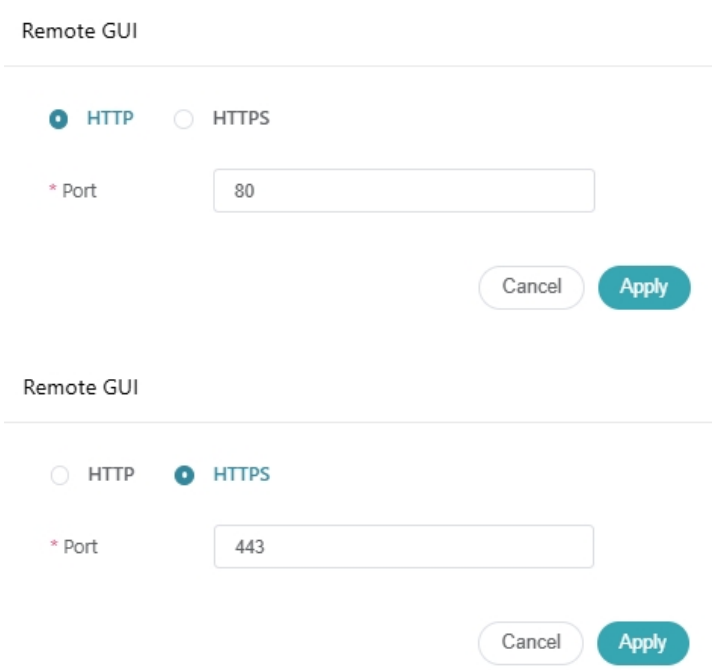


2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **GUI remota** en la esquina superior derecha.

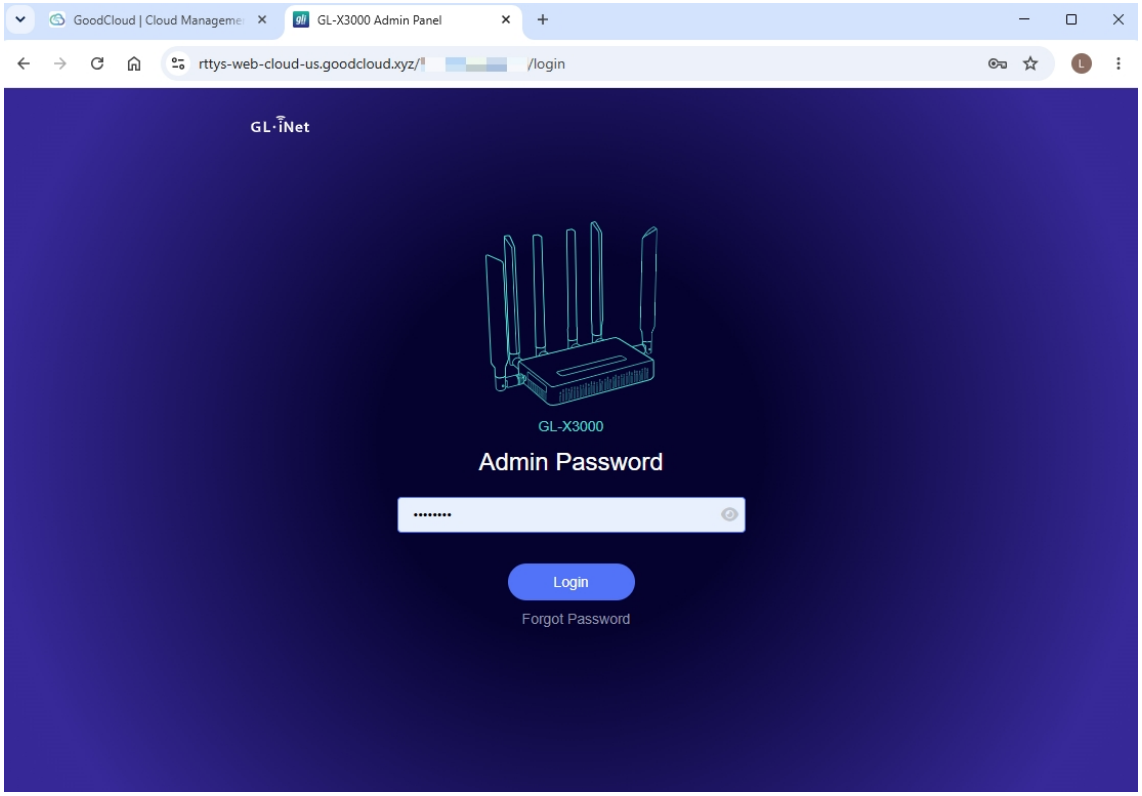


4. Seleccione el protocolo y el puerto de transferencia. Los valores predeterminados son **HTTP** y Puerto **80**. Puede cambiar el protocolo a HTTPSpuedes cambiar el protocolo a

HTTPS si es necesario y el puerto cambiará automáticamente a 443. Luego haga clic en **Aplicar**.

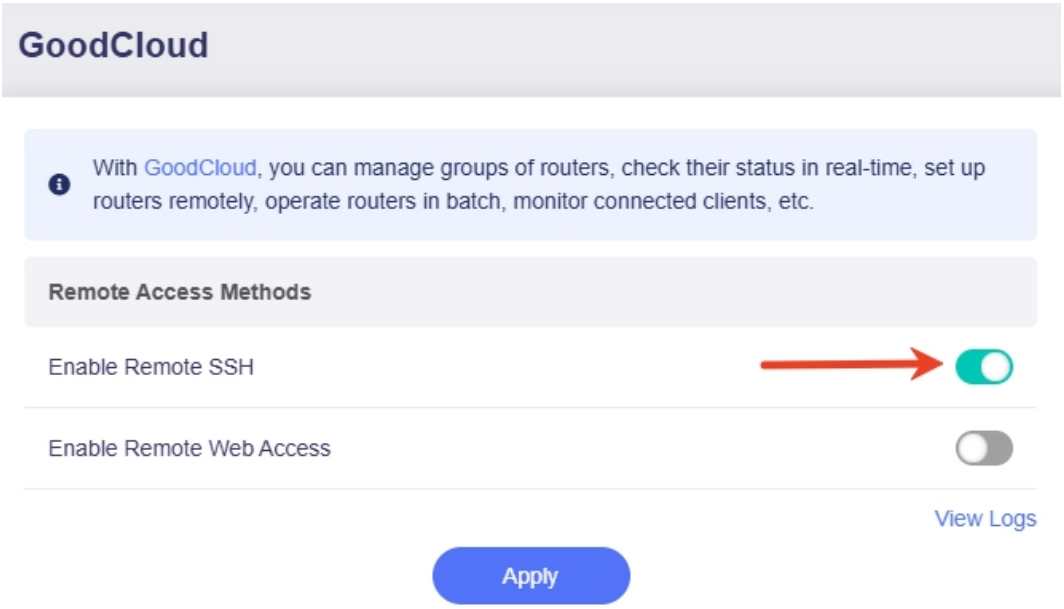


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

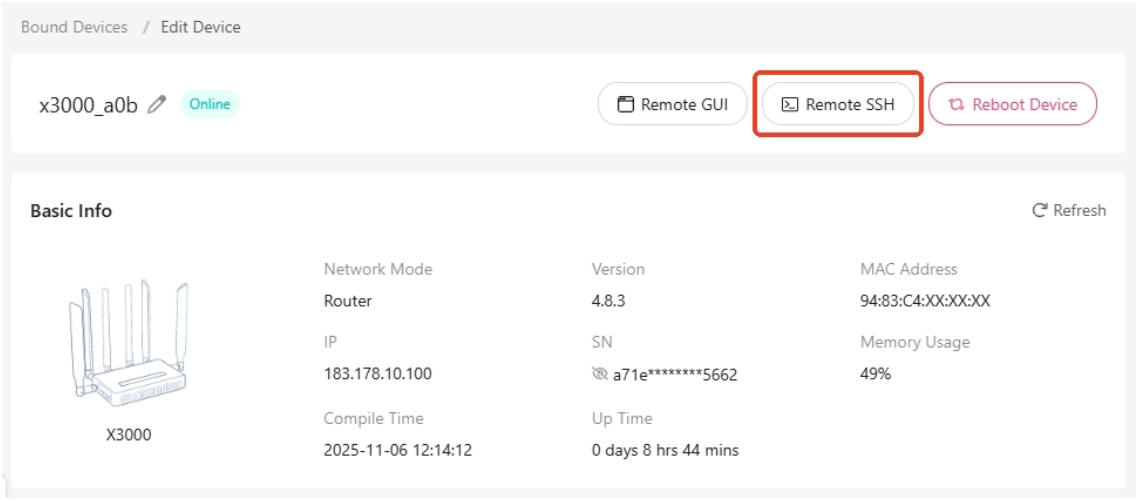


7.1.2.3 Acceso remoto SSH

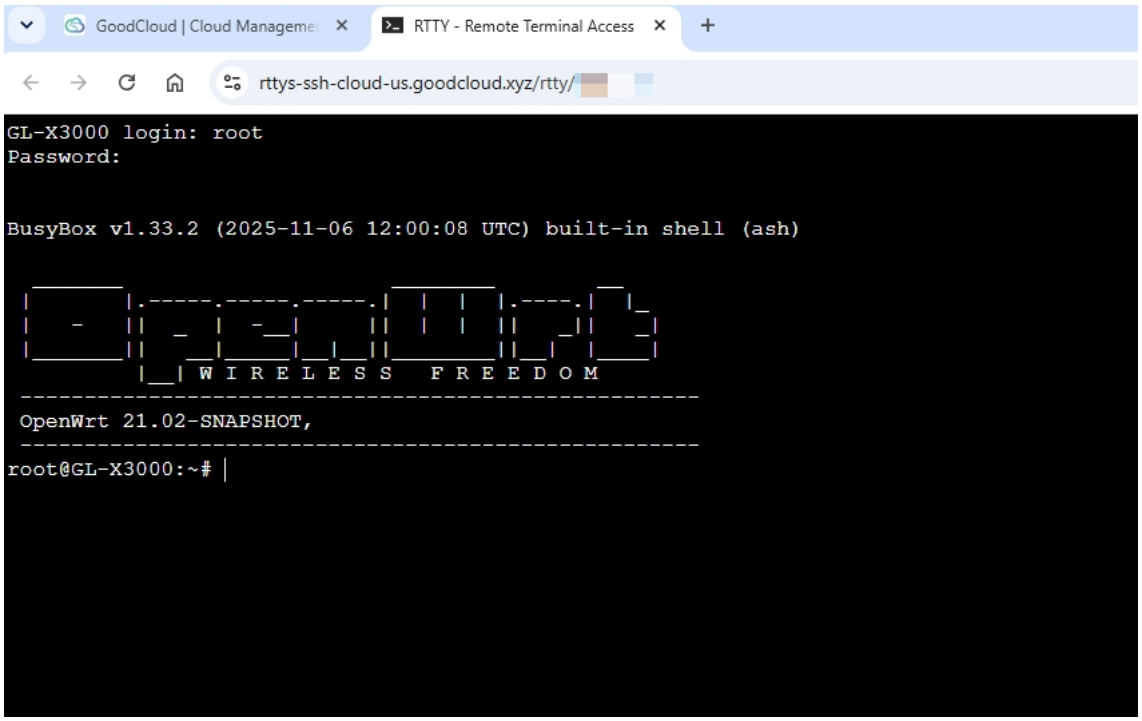
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.



2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Acceso remoto SSH** botón en la esquina superior derecha.

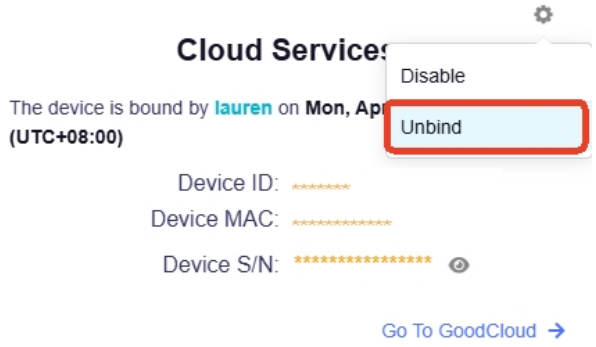


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

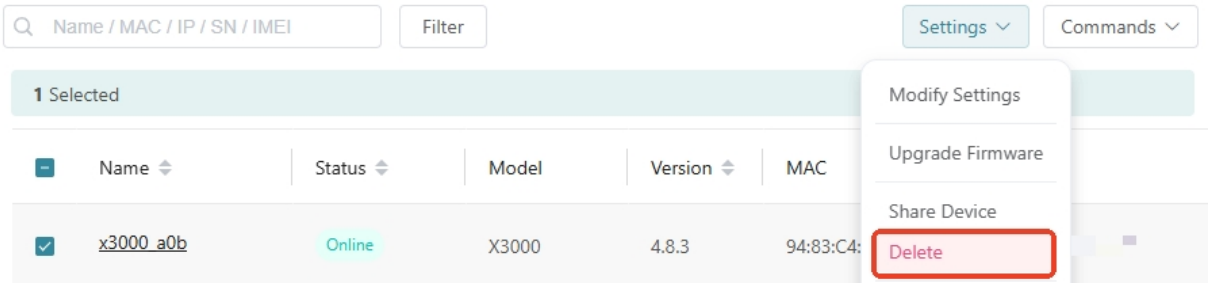

GoodCloud | Cloud Manageme
RTTY - Remote Terminal Access
rttys-ssh-cloud-us.goodcloud.xyz/rtty/
GL-X3000 login: root
Password:
BusyBox v1.33.2 (2025-11-06 12:00:08 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-X3000:~#

7.1.3 Desvincular el dispositivo

En el panel de administración web del enrutador', haga clic en Icono de nube en la esquina superior derecha. En el menú desplegable, haga clic en el ícono de ajustes y seleccione **Desvincular**. Su dispositivo se desvinculará de GoodCloud cuenta.

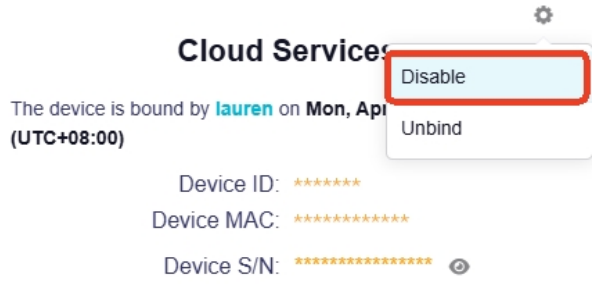


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su cuenta de GoodCloud.



7.1.4 Desactivar GoodCloud

Si ya no desea que el dispositivo esté conectado a la nube, haga clic en Icono de nube en la esquina superior derecha. En el menú desplegable, haga clic en el ícono de ajustes y seleccione **Desactivar**.

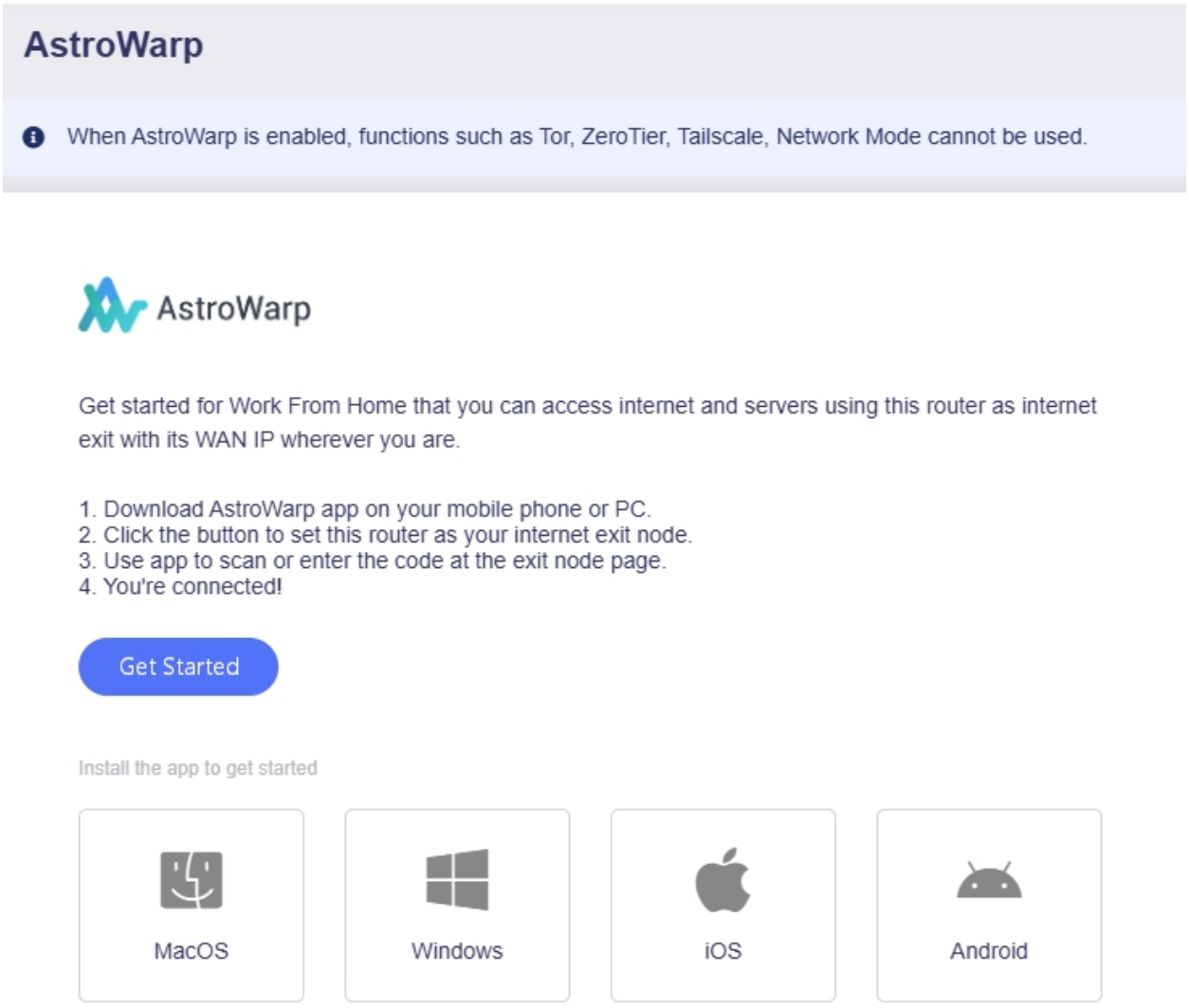


El servicio en la nube se desactivará.

7.2 AstroWarp

AstroWarp es una plataforma de red avanzada diseñada para conectar sin problemas múltiples enrutadores GL.iNet en una red unificada, permitiendo un acceso remoto sin esfuerzo. Con capacidades de red flexibles, configuración fácil de usar y una sólida protección de la privacidad, AstroWarp ofrece conectividad segura y confiable en todo momento. Ya sea para trabajo remoto o acceso seguro a recursos corporativos internos en múltiples sitios, AstroWarp es su solución ideal para redes protegidas de alto rendimiento.

Inicie sesión en el panel de administración web de su enrutador, vaya a **SERVICIO EN LA NUBE** > **AstroWarp** y haga clic en **Comenzar**. Luego siga las instrucciones para configurar su red. Consulteconsulte astrowarp.net para detalles.



Capítulo 8

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

8.1 Introducción

8.1.1 VPN

VPN, abreviatura de Virtual Private Network, establece un túnel cifrado y privado entre un dispositivo y un servidor remoto, protegiendo la transmisión de datos y permitiendo el acceso seguro a sitios privados o restringidos. redes.

8.1.2 Enrutador VPN

Un enrutador VPN presenta una funcionalidad VPN preinstalada, que protege todos los dispositivos conectados a través de VPN. A diferencia de configurar una VPN en dispositivos individuales, configurar el enrutador como un cliente VPN enruta todo el tráfico a través de un túnel cifrado, sin necesidad de una configuración separada por dispositivo. Esto protege varios dispositivos a la vez, ahorra tiempo, y garantiza configuraciones VPN consistentes, reduceing riesgos de personas inadecuadas. settings.

Los enrutadores GL.iNet admiten más de 30 servicios comerciales populares de OpenVPN y WireGuard VPN. Cargue sus archivos de configuración de VPN para activar la conexión VPN para una red segura. Consulte aquí para obtener la lista completa de proveedores de VPN externos.

8.1.3 OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza Seguridad basada en SSL/TLS para conexiones de punto a sitio o de sitio a sitio. Admite múltiples métodos de cifrado, TCP/UDP y una fácil omisión de firewall/NAT.

8.1.4 WireGuard

WireGuard® es un protocolo VPN ligero, rápido, más simple y más eficiente que OpenVPN. Cuenta con criptografía moderna para mayor eficiencia, una pequeña base de código para facilitar la auditoría y la seguridad, y algoritmos de última generación (ChaCha20/Poly1305) para el cifrado y la integridad de los datos.

*WireGuard® es una marca registrada de Jason A. Donenfeld.

8.2 Escenarios de aplicación

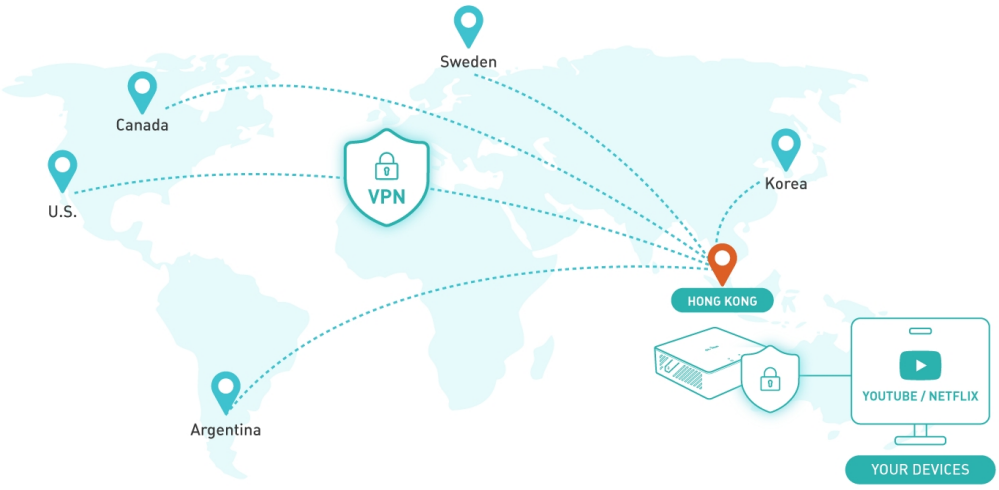
1. **Privacidad de datos personales**

   El servicio VPN es compatible con una amplia gama de dispositivos a través de nuestro enrutador, incluidos no solo computadoras portátiles, teléfonos y tabletas, pero también consolas de juegos, televisores y dispositivos de transmisión. Tus datos estarán protegidos ya sea a través de conexiones inalámbricas o por cable. Incluso puedes personalizar políticas VPN para lograr una protección flexible para ciertos dispositivos.



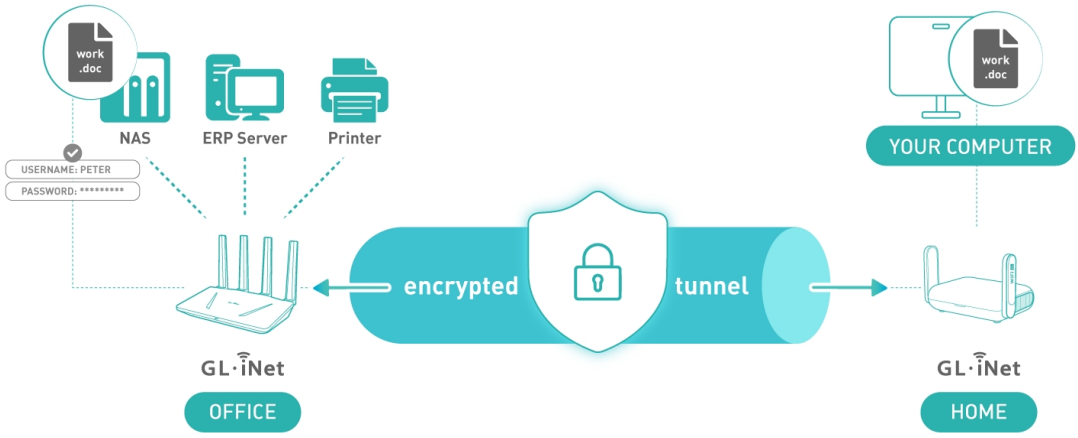
2. **Acceso sin restricciones en todo el mundo**

   El acceso a algunos sitios puede estar restringido según la ubicación. Con VPN habilitada, puedes desbloquear cualquier sitio cuando sea necesario. Al conectarse a diferentes servidores de terceros, se le asignarán diferentes direcciones IP para navegar o acceder a sitios bloqueados por región.



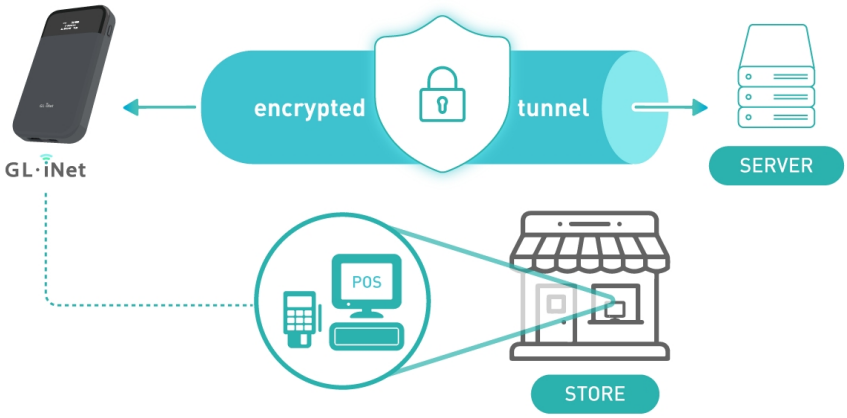
3. **Seguridad de datos para pequeñas empresas**

Muchas personas trabajan en co-espacios de trabajo o cafeterías y dependen de Wi-Fi público gratuito. Estas redes son vulnerables a los ataques de los ciberdelincuentes. Al configurar su enrutador de viaje como cliente VPN, puede disfrutar de una conectividad segura para trabajar en cualquier lugar.



4. **Infraestructura de pago segura**

Los pequeños propietarios de comercios minoristas deben manejar las credenciales de pago de los clientes cuando realizan negocios en el sitio. Usando un VPN enrutador, su POS La máquinas puede cargar información de la tarjeta de crédito a través de una VPN cifrada tunnel para garantizar la seguridad del pago.



Capítulo 9

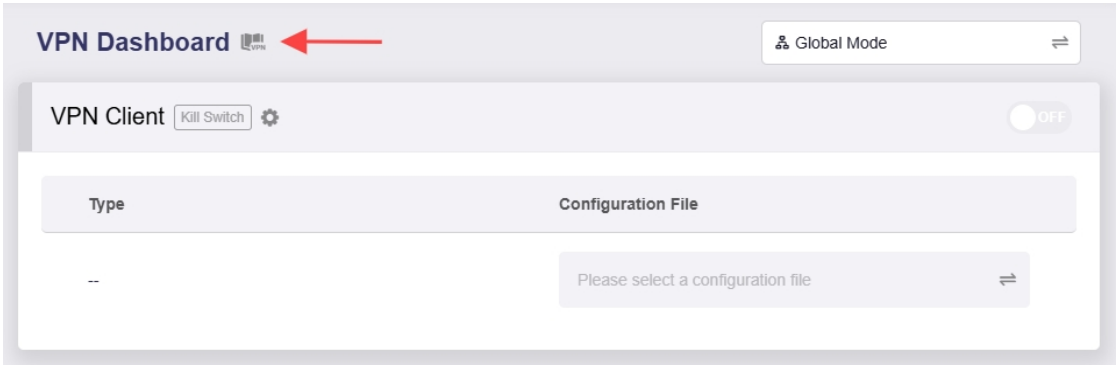
Panel de VPN

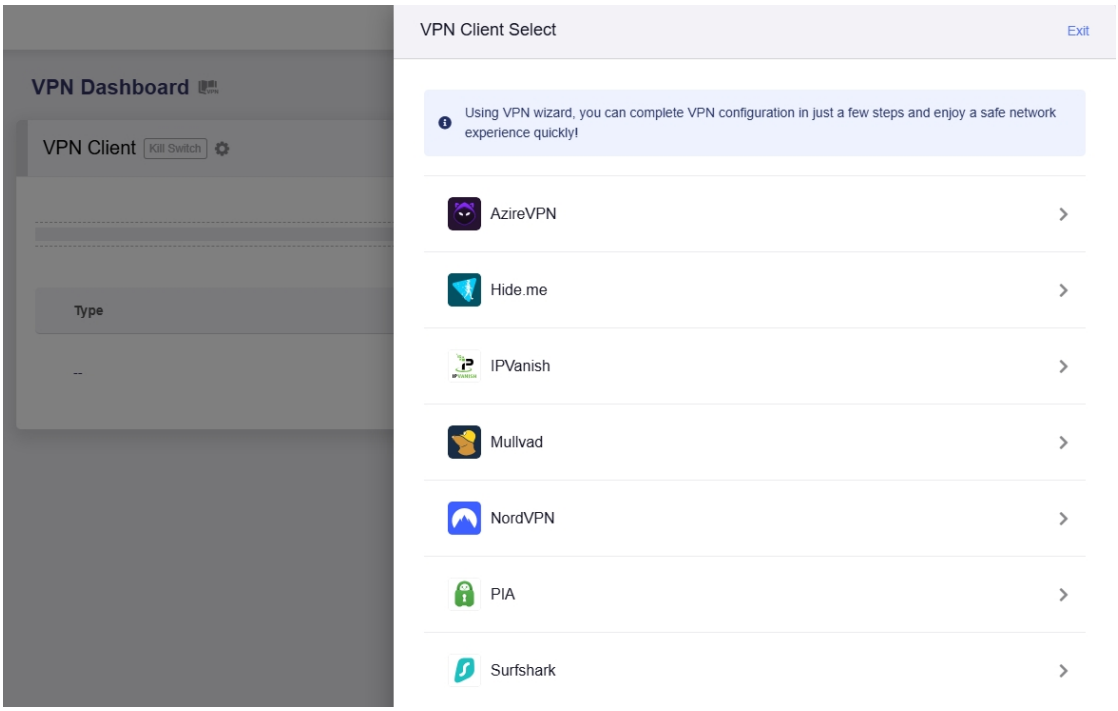
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

Inicie sesión en el panel de administración web, y vaya a **VPN** > **Panel de VPN**.
Se muestra el panel de VPN Detalles de la conexión VPN, como reglas de túnel, dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión, y permite a los usuarios configurar ajustes avanzados como VPN Kill Switch, enmascaramiento de IP y MTU. También puede activar múltiples conexiones VPN para escenarios de múltiples túneles.

9.1 Asistente de configuración de VPN

Para comenzar, haga clic en el ícono del libro en la esquina superior izquierda y siga el Asistente de configuración de VPN para completar la configuración de VPN rápidamente.





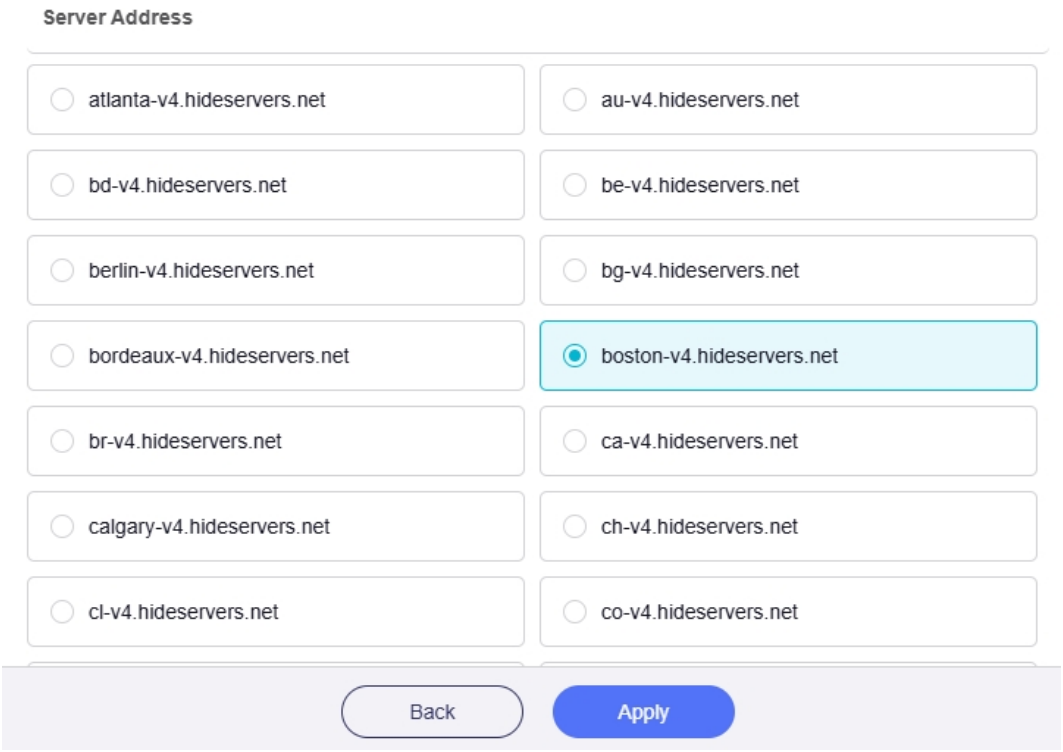
Nota: El asistente de configuración de VPN es solo para los servicios VPN integrados, incluidos AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA y Surfshark. Para otros proveedores de

VPN, omita el asistente y vaya a **VPN** > **Cliente OpenVPN** o **Cliente WireGuard** para configurar la VPN. manualmente.

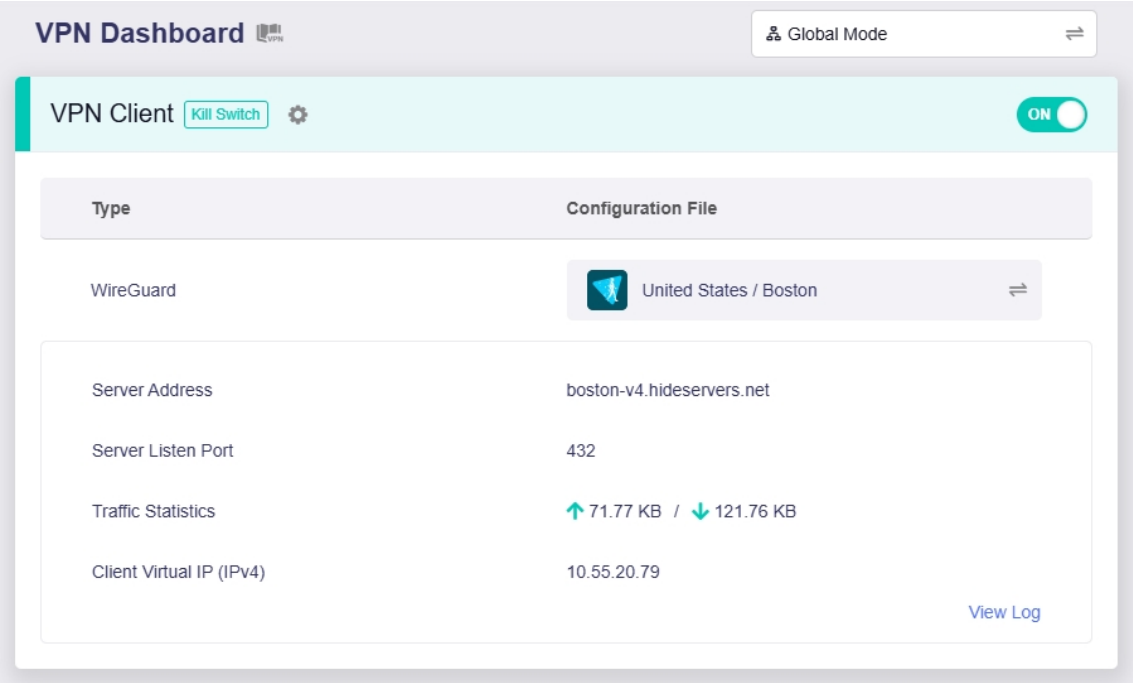
Aquí hay un ejemplo con **Hide.me**. Inicie sesión con las credenciales de Hide.me.



Seleccione un servidor VPN y haga clic en **Aplicar**. Este es el servidor al que se conectará y su dirección IP pública parecerá ser la de la ubicación del servidor seleccionado.

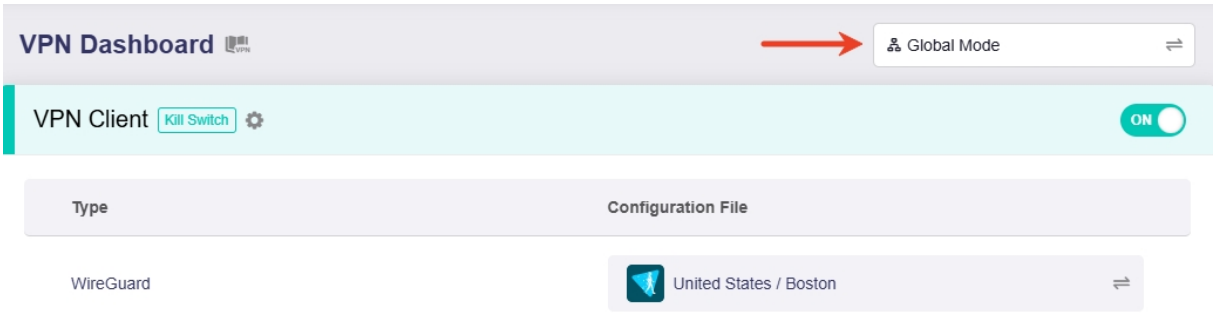


Se conectará automáticamente. Una vez conectado, vaya al **Panel de VPN**. Verá que se ha habilitado un túnel VPN, que muestra detalles que incluyen el protocolo VPN (por ejemplo, WireGuard), el archivo de configuración, la dirección del servidor, el puerto de escucha del servidor, las estadísticas de tráfico y la dirección IP virtual del cliente. También puede ver los registros de conexión en la parte inferior derecha corner.

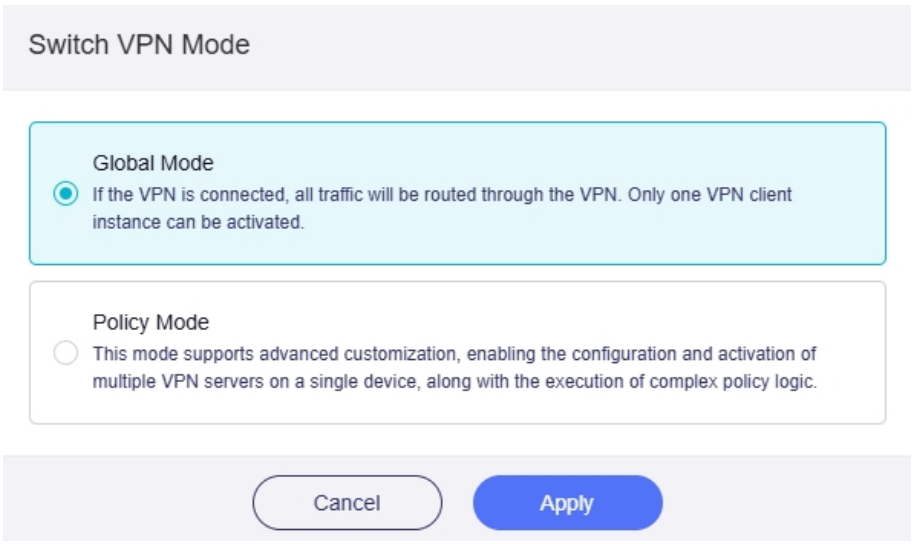


9.2 Modo VPN

En el panel de VPN, haga clic en el botón en la esquina superior derecha para cambiar los modos de VPN si requerido.



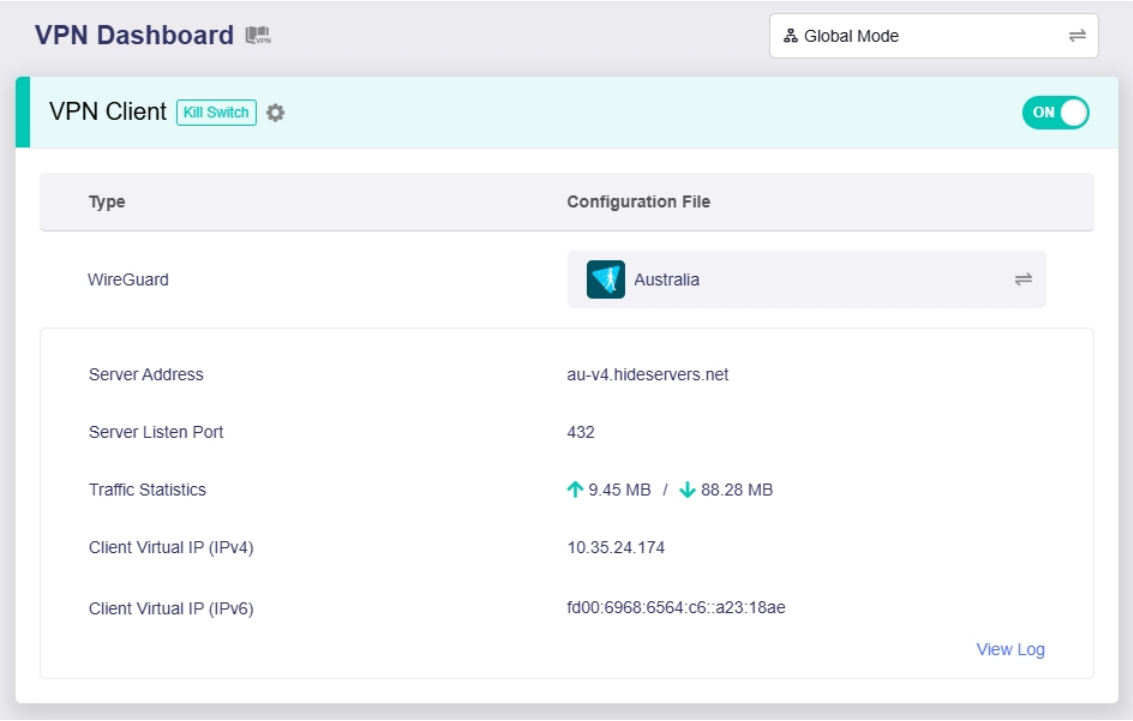
Hay dos modos disponibles : **Modo global** y **Modo de política**.



9.2.1 Modo global

En este modo, todo el tráfico se enrutará a través del túnel VPN y solo se puede activar una instancia de cliente VPN. Es ideal para escenarios que requieren que todo el tráfico del dispositivo pase a través de un único servidor VPN, como seguridad de red unificada o acceso a contenido específico de una región.

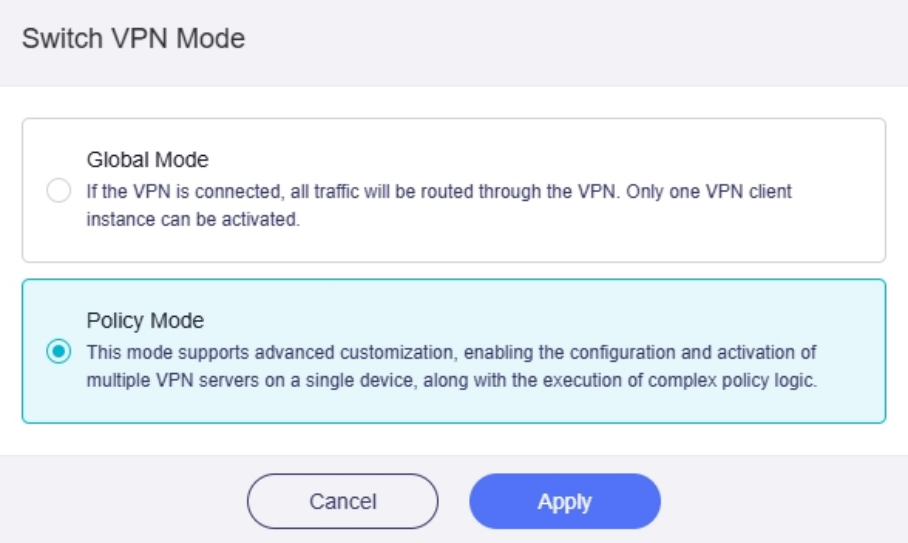
En el siguiente ejemplo, el enrutador se conecta a un servidor australiano mediante el protocolo WireGuard. Todo el tráfico de los clientes conectados se enrutará a través de este túnel VPN.



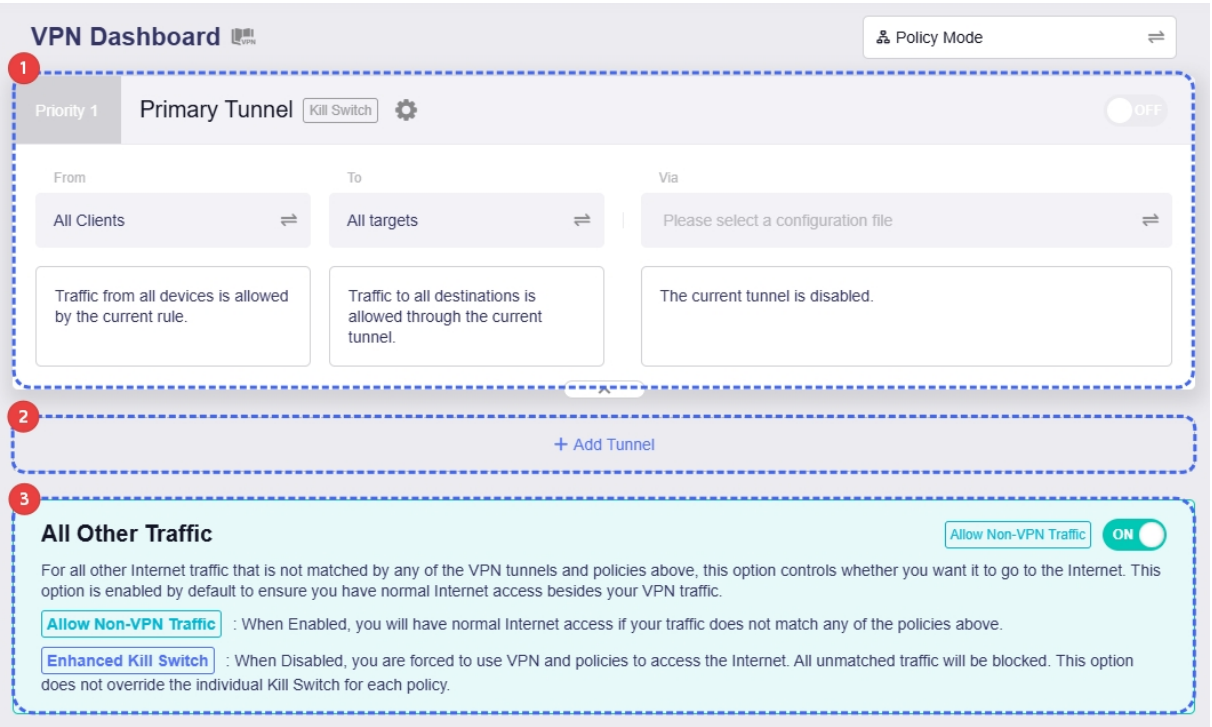
9.2.2 Modo de política

En este modo, puede conectar un único enrutador a múltiples servidores VPN y personalice las reglas de VPN. Es adecuado para casos que necesitan una gestión de tráfico flexible, como enrutar tráfico diferente a diferentes destinos a través de múltiples servidores VPN.

Cambie el modo VPN a **Modo de política** y haga clic **Aplicar**.



Después de cambiar, si la VPN no está habilitada, la página se muestra a continuación, incluidas tres secciones: **Túnel principal**, **Agregar túnel** y **Todo el resto del tráfico**.

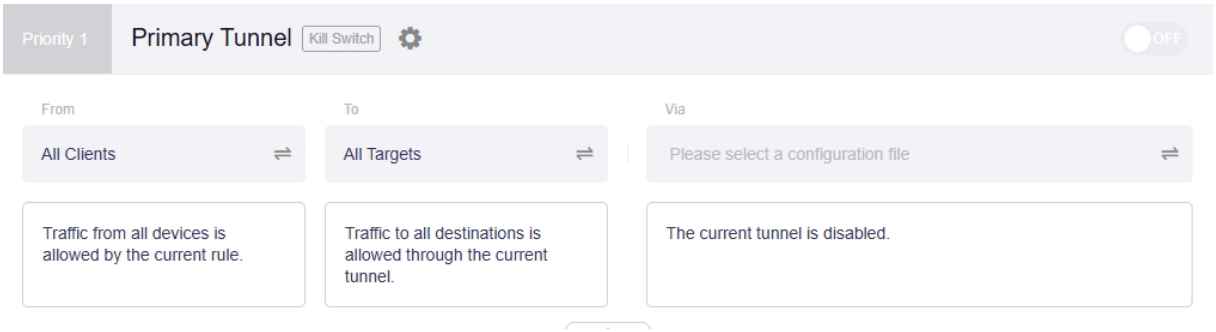


9.2.2.1 Túnel principal

El túnel principal es un túnel preestablecido en modo de política. Tiene la prioridad más alta de forma predeterminada y puede ajustar su prioridad cuando se configuran varios túneles.

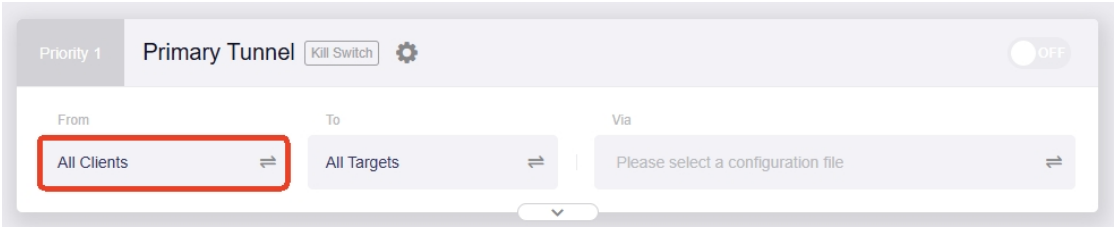
En este túnel, puede personalizar la regla del túnel estableciendo tres factores:

- **Desde**: se refiere a la fuente de tráfico, es decir, el tráfico que debe enrutarse a través de este túnel.
- **A**: Se refiere al destino del tráfico, al cual se enruta el tráfico a través de estees túnel.
- **Vía**: Se refiere al método de enrutamiento del tráfico, es decir, si desea utilizar VPN.

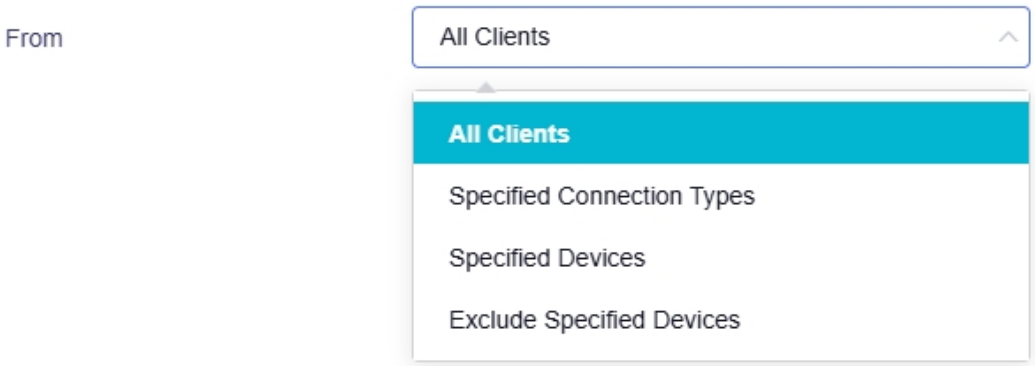


Siga los pasos siguientes para configurar su regla de túnel.

1. Haga clic en el cuadro atenuado de la izquierda.

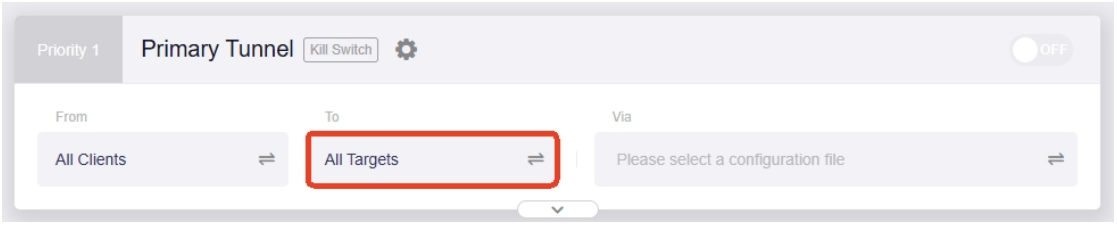


2. Seleccione el dispositivo que desea coincidir con esta regla y haga clic en **Aplicar**.

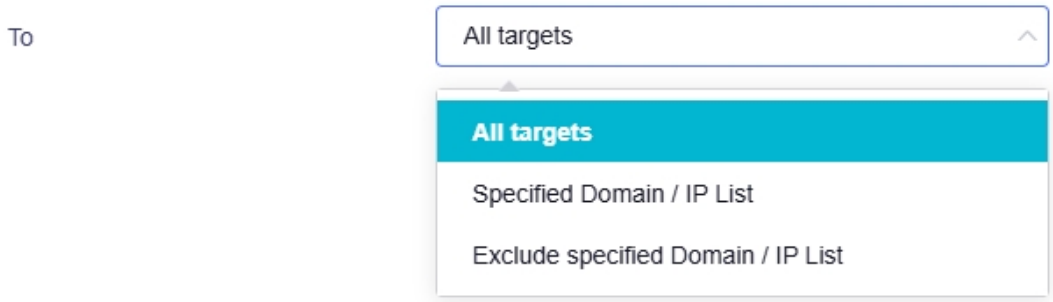


- **Todos los clientes**: Si se selecciona, el tráfico de todos los dispositivos coincidirá esta regla.
- **Conexión especificada Tipos**: Si se selecciona, el tráfico de la conexión especificada tipos (por ejemplo, subred LAN, puerta de enlace directa, red de invitados) coincidirá con esta regla.
- **Especificada Dispositivos**: Si se selecciona, el tráfico de dispositivos específicos (identificados por dirección MAC) coincidirá con esta regla.
- **Excluir dispositivos especificados**: Si se selecciona, el tráfico de los dispositivos especificados (identificados por la dirección MAC) nol **NO** coincide esta regla.

3. Haga clic en el medio gracuadro sombreado.



4. Seleccione el destino al que El tráfico será rutad a través de este túnel y haga clic en **Aplicar**.

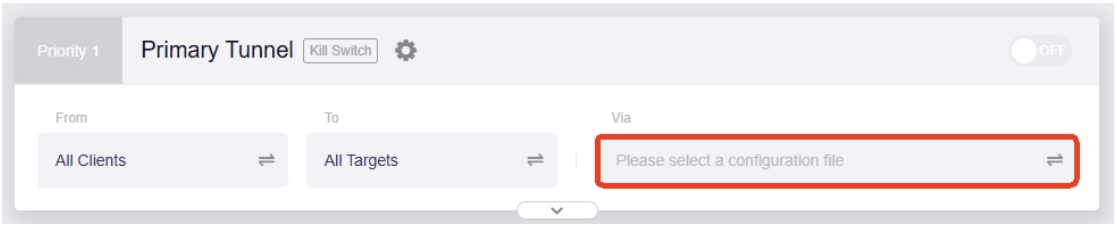


- **Todos Tobjetivos**: Si se selecciona, tráfico coincidencia esta regla se enrutará a todos los destinoss.
- **Dominio especificado/lista de IP**: Si se selecciona, el tráfico que coincida con esta regla se enrutará al dominio/IP especificado. Usted necesita ingrese el dominio/IP especificado manualmente, o ingrese el enlace URL de suscripción. Al especificar un dominio raíz se cubrirán todos sus subdominios.
- **Excluir el dominio/lista de IP especificados**: Si se selecciona, el tráfico que coincida con esta regla **NO** se enrutará al dominio/ IP. Usted necesita ingrese el dominio/IP

especificado manualmente, o ingrese el enlace URL de suscripción. Especificar un dominio raíz cubrirá todos sus subdominios.

Nota: Si selecciona Suscribir URL, el nombre de dominio o dirección IP en la URL será automáticamente actualizado todos los días. Asegúrese de ingresar la URL correcta. La detección de URL verificará la validez del nombre de dominio o la dirección IP.

5. Haga clic en derecha grayed-out box.

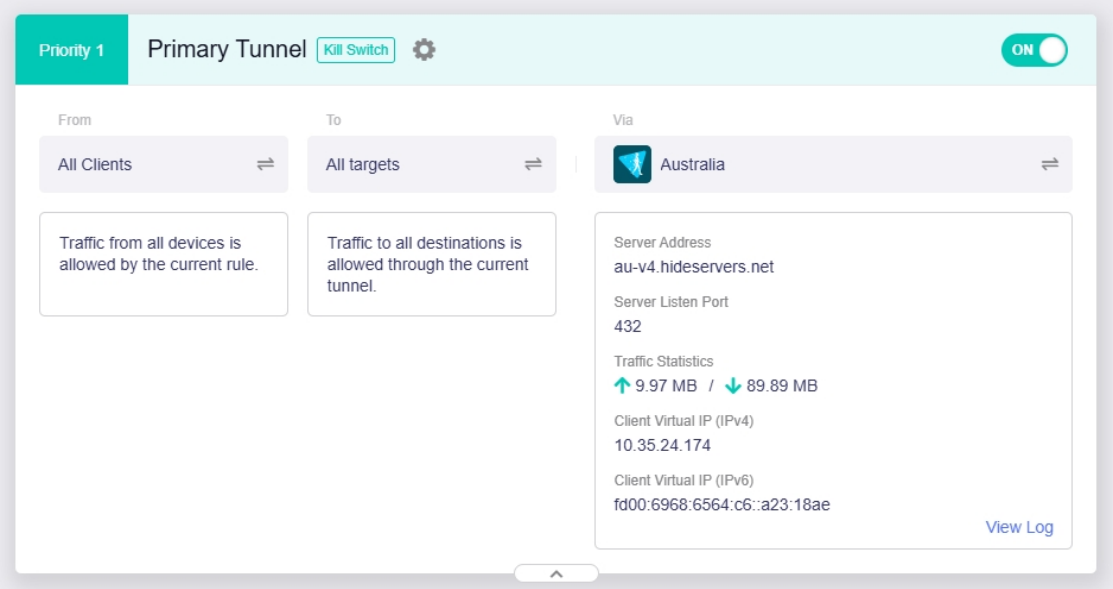


6. Seleccione el método de enrutamiento para este túnel: **Usar VPN** o **No usar VPN**.



- **Usar VPN**: Si se selecciona, el tráfico que coincida con esta regla se enrutará al destinos a través de VPN túnel. Debe seleccionar un archivo de configuración de VPN para esta regla.
- **No usar VPN**: Si se selecciona, el tráfico que coincida con esta regla se enrutará al destinos vía local WAN red en lugar de VPN.

7. Después de configurar el origen del tráfico, el destino y el método de enrutamiento, se completa la configuración de la regla del túnel principal. En el siguiente ejemplo, la regla túnell es: Todos los clientes conectados a este enrutador accederá a Internet a través de VPN; Su tráfico se enrutará a través de este túnel VPN al servidor de Australia y finalmente saldrá de este servidor a Internet.

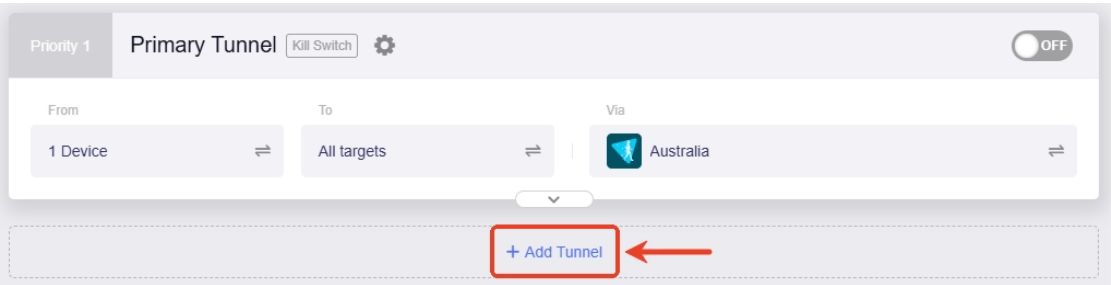


Nota: por seguridad, vaya a **9.2.2.3 Todo el resto del tráfico** y **9.2.2.4 Opciones de túnel** para comprobar otras configuraciones antes de habilitar esta túnel.

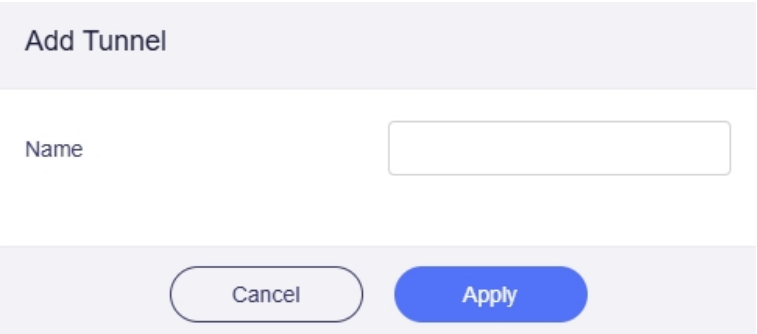
9.2.2.2 Agregar túnel

Agregue túneles si necesita enrutar el tráfico desde diferentes dispositivos a diferentes destinos. Siga los pasos a continuación para agregar un túnel.

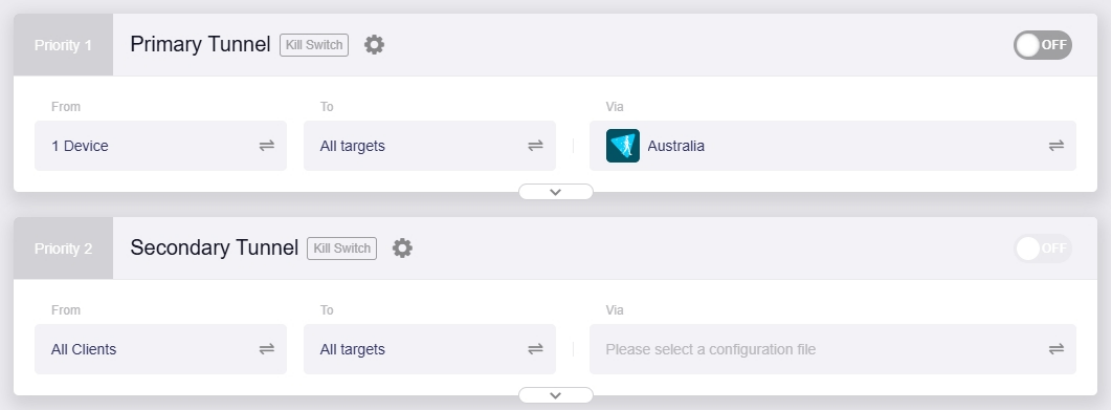
1. Haga clic en **Agregar túnel** debajo del túnel principal.



2. Ponle nombre al túnel.



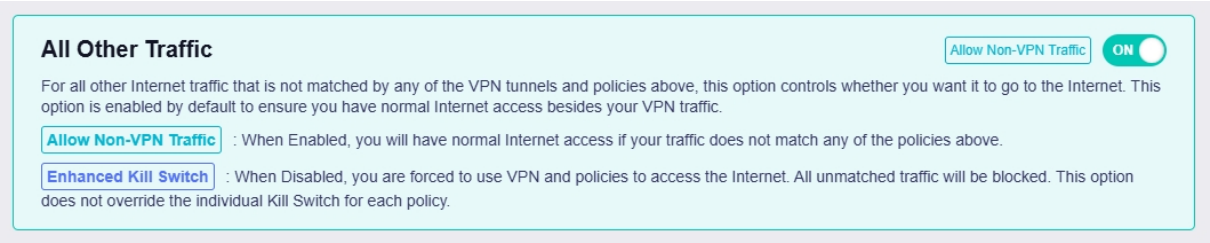
3. Yobtendrá un túnel más en el Panel de VPN. Se pueden crear hasta 5 túneles (incluido el túnel principal preestablecido).



4. Configure reglas de túnel estableciendo la fuente de tráfico, destinos y el método de enrutamiento. Una vez terminado, vaya a **9.2.2.3 Todo el resto del tráfico** y **9.2.2.4 Opciones de túnel** para verificar otras configuraciones antes de habilitar este túnel.

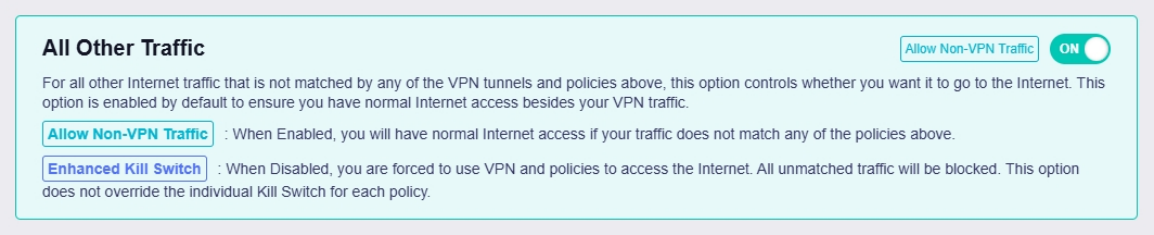
9.2.2.3 Todo el resto del tráfico

En el modo de política, se muestra un túnel predeterminado prehabilitado en la parte inferior del Panel de VPN.

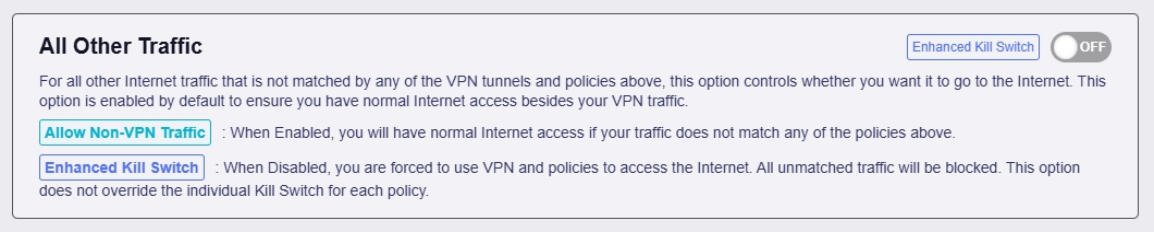


Este túnel controla si el tráfico que no coincide con ninguno de los grupos de túneles VPN anteriores puede acceder a Internet. Está habilitado de forma predeterminada para garantizar el acceso normal a Internet para el tráfico no enrutado a través de VPN.

- Cuando está habilitado, el tráfico incomparable aún puede acceder a Internet.

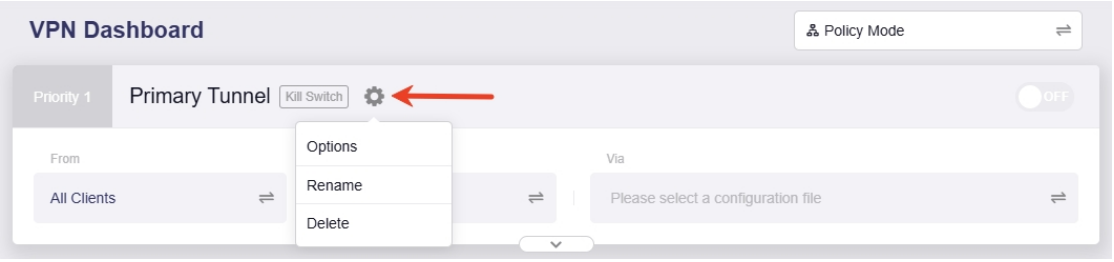


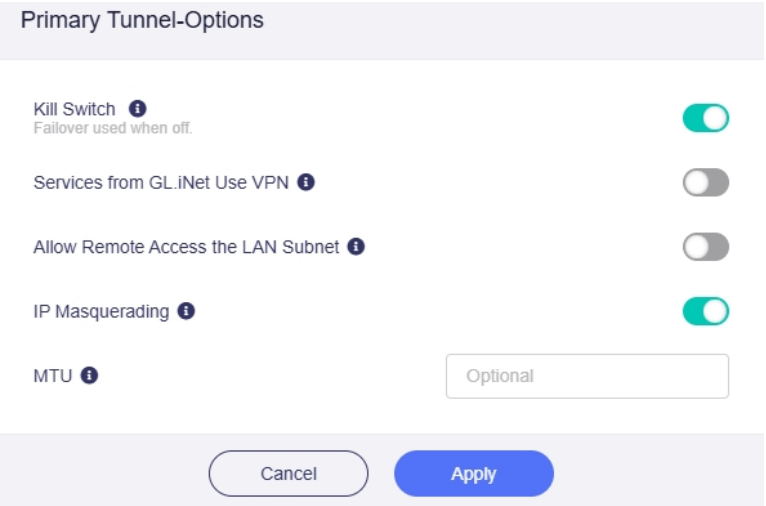
- Cuando está deshabilitado, solo el tráfico enrutado a través de VPN puede acceder a Internet. Se bloqueará todo el tráfico que no sea VPN y el tráfico que conmuta por error desde conexiones VPN. Esta opción no anula el Kill Switch individual para cada túnel VPN.



9.2.2.4 Opciones de túnel

Puedes configurar ajustes avanzados para cada túnel VPN, como VPN Kill Switch, IP Enmascaramiento y MTU. Haz clic en el ícono de ajustes junto al nombre del túnel.





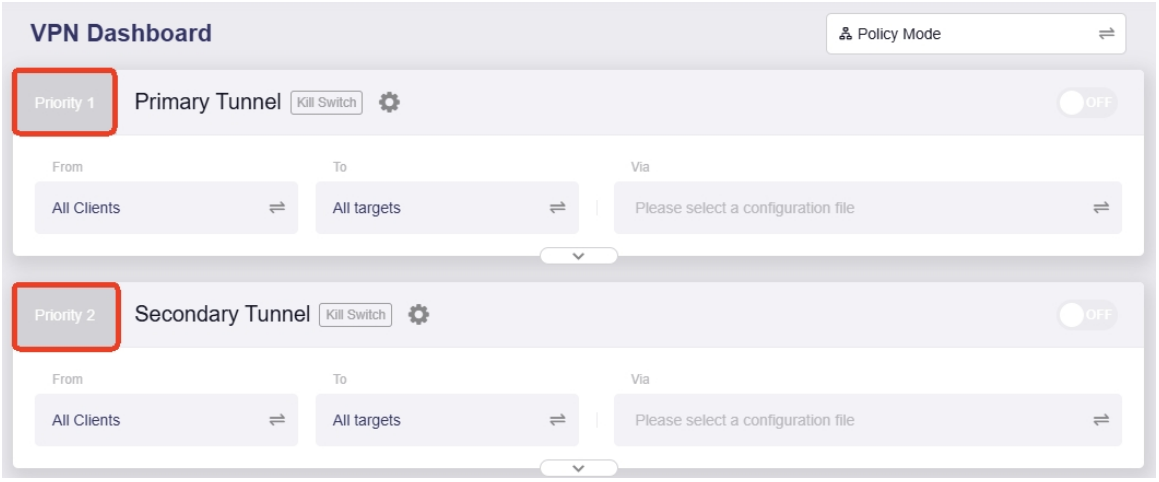
- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, el tráfico que coincida con eles túnel VPN será bloqueado cuando la conexión fallaes inesperadamente; de lo contrario, conmutará por error a los túneles o WAN de siguiente prioridad.
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitir paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.
- **Permitir acceso remoto a la subred LAN**: si está habilitado, acceso remoto a este enrutador (IP de túnel) y dispositivos LAN a través de la VPN estarán permitidos. Requiere que el servidor VPN anuncie una ruta de regreso a este enrutador’s subred LAN.
- **Enmascaramiento de IP**: si está habilitado, las IP de origen del cliente LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilitado solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: la MTU que configuró para el túnel sobrescribirá el elemento de MTU en el archivo de configuración.

9.2.2.5 Prioridad del túnel

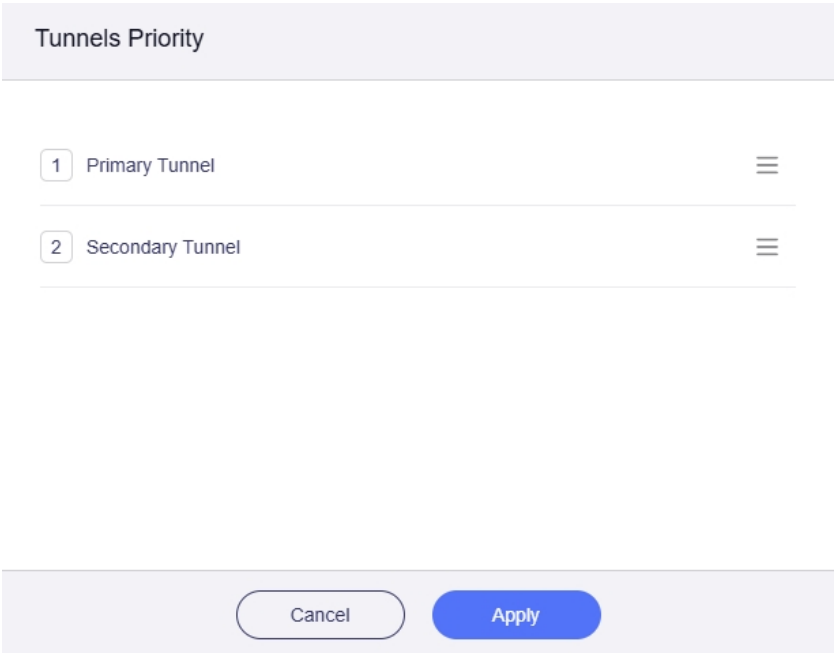
De forma predeterminada, el túnel primario preestablecido tiene la prioridad más alta, seguido de otro túnel agregado manualmente (si lo hay), luego el resto del tráfico preestablecido túnel para garantizar conectividad de red a través de red ISP (WAN) local.

Si necesita tmodificar la prioridad del túnel, despuéssiga los pasos a continuación.

1. Clame la etiqueta de prioridad en la esquina superior izquierda de cualquier túnel (por ejemplo, Prioridad 1 / Prioridad 2).



2. En la ventana emergente, haga clic en y mantenga presionado el ícono de tres líneas a la derecha para reordene el túnel, luego haga clic en **Aplicar**.



Cuando haya varios túneles están habilitados, el enrutador enrutará el tráfico en el siguiente orden:

1. El tráfico primero intentará coincidir con la regla de túnel de mayor prioridad. Si coincide, será encaminado a través de ese túnel; de lo contrario, probará el siguiente túnel de prioridad, y así sucesivamente, hasta que coincida con el túnel "Todo el resto del tráfico".
2. Si un túnel VPN se desconecta inesperadamente, el sistema determinará si se debe realizar una conmutación por error del tráfico al siguiente túnel de prioridad en función de si el **Bloqueo de tráfico sin VPN (Kill Switch)** está habilitado.
    - Cuando el Kill Switch está habilitado, el tráfico se bloqueará y no conmutará por error al siguiente túnel de prioridad.
    - Cuando el Kill Switch está deshabilitado, el tráfico conmutará por error al siguiente túnel de prioridad e intentará coincidir con su túnel reglas.
3. El túnel **Todo el resto del tráfico** está habilitado de forma predeterminada para garantizar que el tráfico que no coincida con los túneles VPN aún pueda acceder a Internet.
    - Si está habilitado, enruta rutas no coincidentes o tráfico de conmutación por error a través de la WAN local.
    - Si está deshabilitado, fortalece el Kill Switch y bloquea el acceso regular a Internet para evitar fugas de IP.

Capítulo 10

Configurar el servidor VPN

Este capítulo presenta cómo configurar un enrutador GL.iNet como servidor OpenVPN o WireGuard.

10.1 Servidor OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza Cifrado SSL/TLS para conexiones seguras punto a punto y de sitio a sitio. Para configurar el servidor OpenVPN en un enrutador GL.iNet, mire este video o consulte los pasos a continuación.

10.1.1 Preparación

1. **Asegúrate de tener una dirección IP pública**

   Haz clic en aquí para verificar si su proveedor de servicios de Internet (ISP) le asigna una dirección IP pública.

   De lo contrario, su enrutador no se puede configurar como servidor OpenVPN.

   Métodos alternativos:

   - Si tiene un enrutador principal ascendente a su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por ejemplo, si su red está detrás de CGNAT), puede probar nuestra solución SD-WAN AstroWarp.

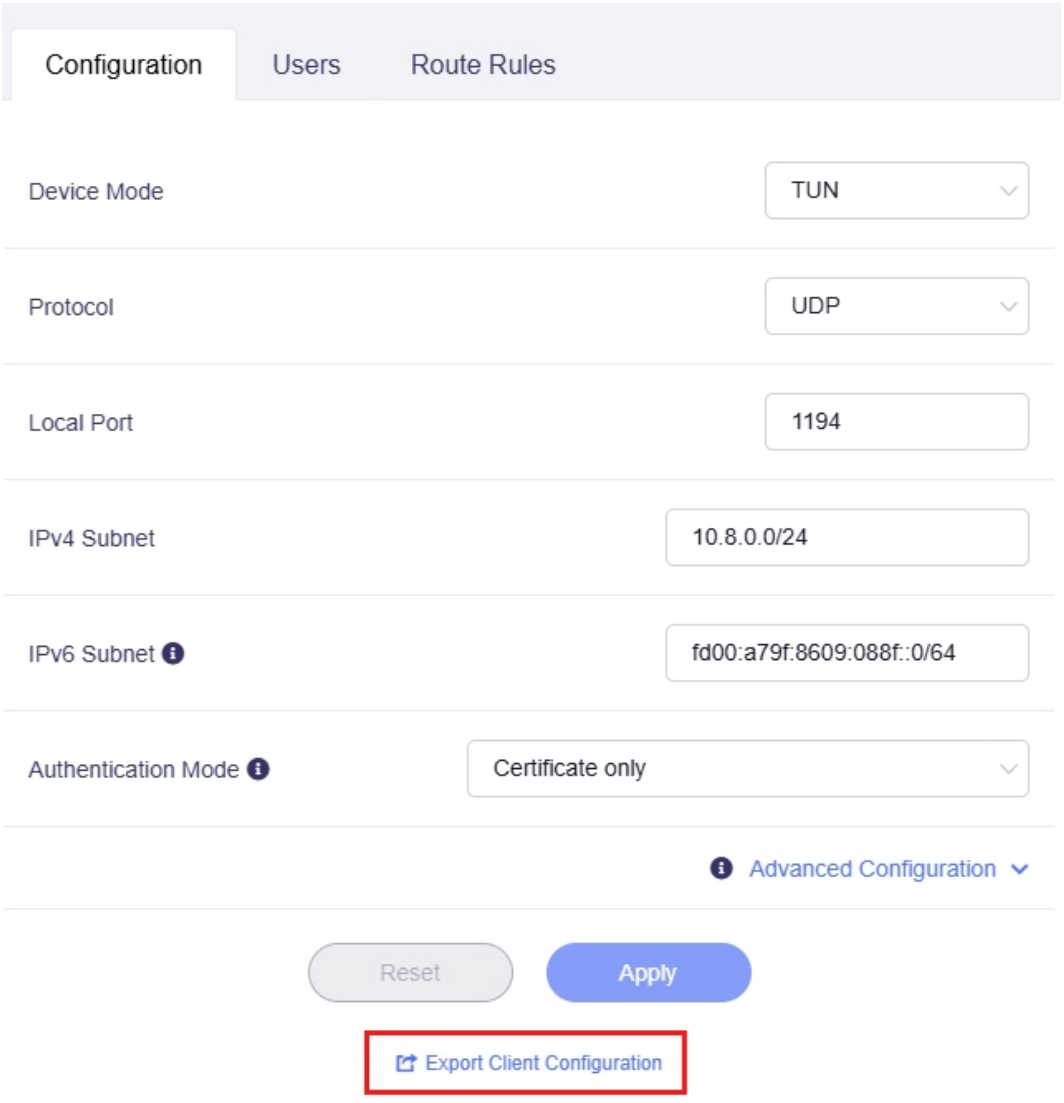
2. **Confirme si se requiere reenvío de puertos**

   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puertos. Continúe con el siguiente paso.
   - Si ya hay un enrutador principal en uso y su enrutador GL.iNet está configurado como enrutador secundario, deberá configurar el reenvío de puertos en el enrutador principal.
   - Si su enrutador GL.iNet está a varios niveles descendentes del enrutador principal, configure el reenvío de puertos en cada dispositivo intermedio.

10.1.2 Pasos de configuración

1. Inicie sesión en el panel de administración web del enrutador, navegue hasta **VPN** > **Servidor OpenVPN**, luego haga clic en **Generar configuración** (solo para la configuración inicial del servidor VPN).
2. Aplicar la configuración.

   La configuración predeterminada funciona en la mayoría de los casos. Haga clic en **Exportar configuración del cliente** en la parte inferior y continúe con el paso 3. Si ha modificado la configuración, haga clic en **Aplicar** antes de exportarla.

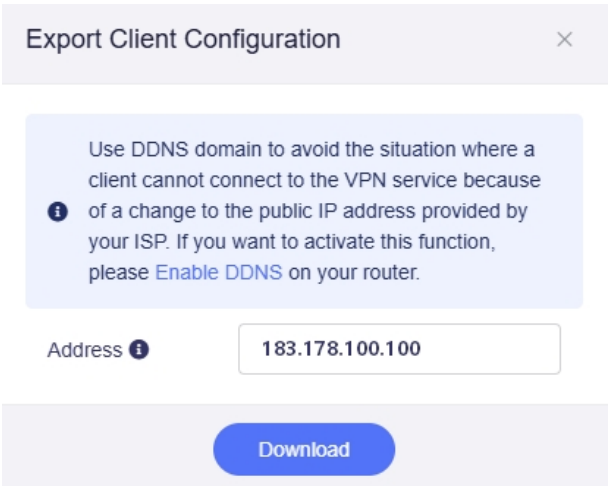


- **Modo de dispositivo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

- **Modo de autenticación**: determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:
  - **Certificado Sólo**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y de cliente y las incrustará en el archivo de configuración. Cuando carga la configuración en el cliente, no se requieren credenciales adicionales.
  - **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. Usted necesita para primero agregar un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente. Al cargar la configuración al cliente, ingrese estas credenciales para autenticación.
  - **Nombre de usuario/contraseña y certificado**: si se selecciona, necesita primero agregar un nombre de usuario y una contraseña en **Usuarios** antes de exportar la configuración del cliente; en segundo lugar, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Al cargar la configuración en el cliente, primero se verificará la clave del certificado, seguida de la autenticación de nombre de usuario/contraseña para 2FA seguridad.
- **Configuración avanzada**: Personalice más configuraciones del servidor si es necesario.

3. Exportar configuración del cliente.

   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.

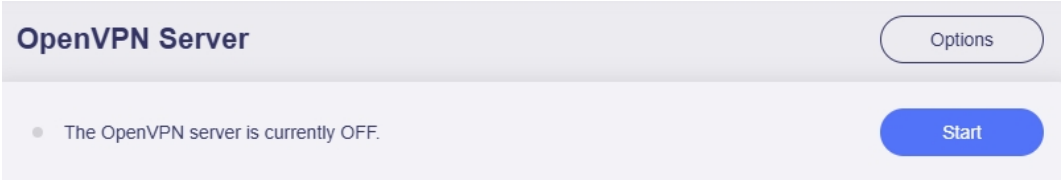


Consejos:

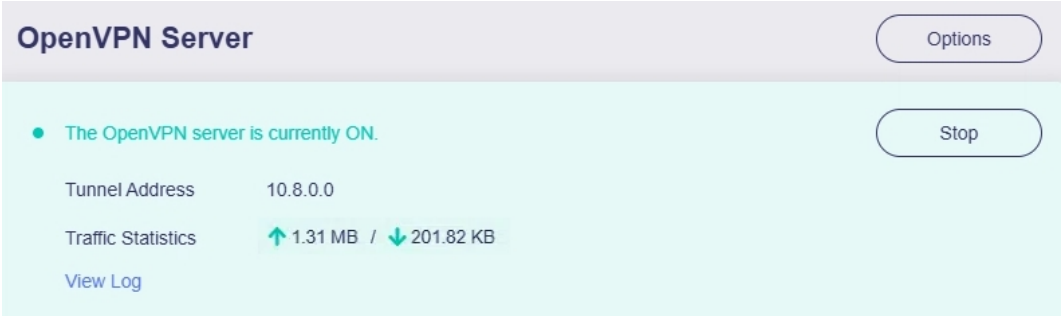
- Si su dirección IP pública cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de configuración: IP pública, dominio DDNS y dirección IP WAN actual. Una vez seleccionada, la dirección del servidor en el archivo de configuración se actualizará automáticamente. Vuelva a descargar el archivo de configuración si se cambia la dirección del servidor.

4. Inicie el servidor OpenVPN.

   En la página **Servidor OpenVPN**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



   El servidor estado de conexión se se muestra en el top. Si muestra estadísticas de tráfico de carga y descarga, significa que el servidor OpenVPN se está ejecutando.

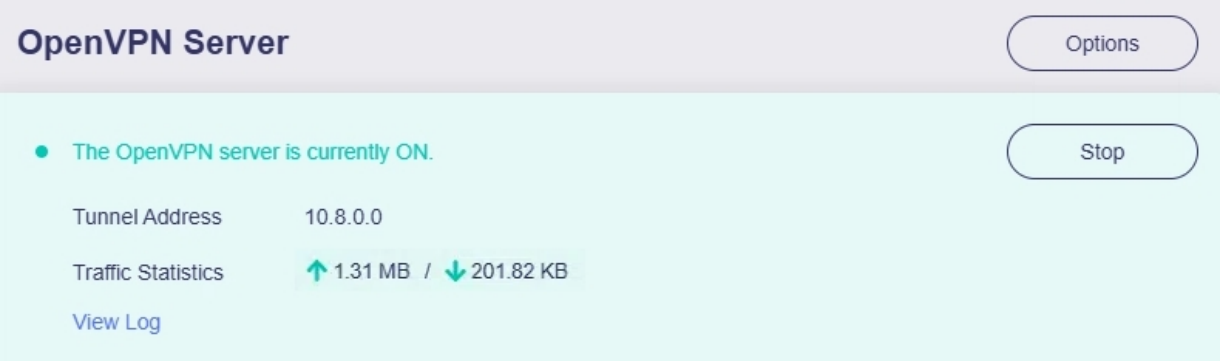


10.1.3 Verificar conexión

Método 1. Verificar el estado del servidor

En firmware v4.8, puede verificar el estado de conexión del servidor en el **Servidor OpenVPN** página.

Si muestra estadísticas de tráfico de carga/descarga, significa que el servidor OpenVPN se está ejecutando.



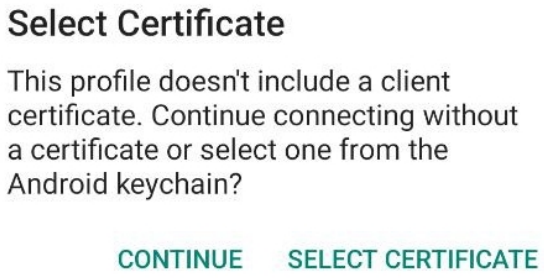
Método 2. Verificar la IP del cliente's

Importar la configuración OpenVPN previamente-exportada a un dispositivo en una red diferente (no en la misma red local que el servidor). Luego abra un navegador web, busque su dirección IP y ubicación. Si coinciden con la IP del servidor VPN (en lugar de la IP de su proveedor de servicios de Internet) y la ubicación, la conexión VPN es exitosa.

Aquí'hay un ejemplo para usar un teléfono inteligente con la Aplicación OpenVPN instalada para verificar.

1. Primero, deshabilite el Wi-Fi del teléfono inteligente y habilite datos móviles (4G/5G) exclusivamente.
2. A continuación, abra la aplicación OpenVPN, importe el archivo de configuración e inicie la conexión.
3. Compruebe si el teléfono inteligente puede acceder a Internet y si su dirección IP coincide con OpenVPN IP del servidor'.

   Consejo: Al importar el archivo de configuración a la aplicación OpenVPN, puede aparecer un recordatorio como se muestra a continuación. Haga clic en **CONTINUAR** para continuar, ya que el certificado ya está integrado en el archivo de configuración.



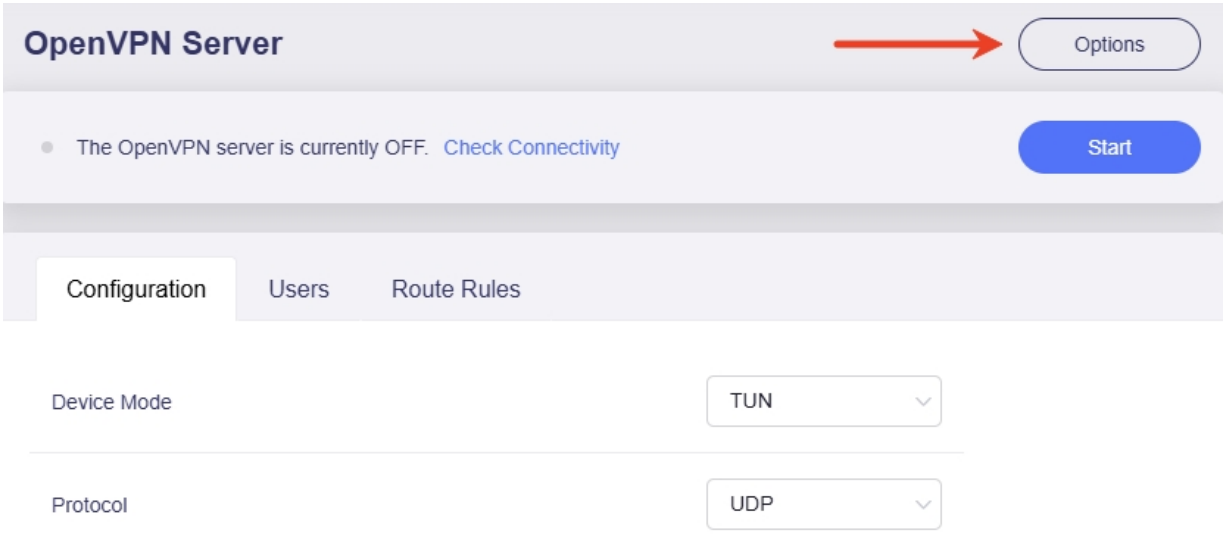
Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulta **10.1.1 Preparación** para obtener más detalles.
- Es posible que necesites configurar el reenvío de puertos. Consulte **10.1.1 Preparación** para obtener más detalles.
- El puerto utilizado para el servidor OpenVPN está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

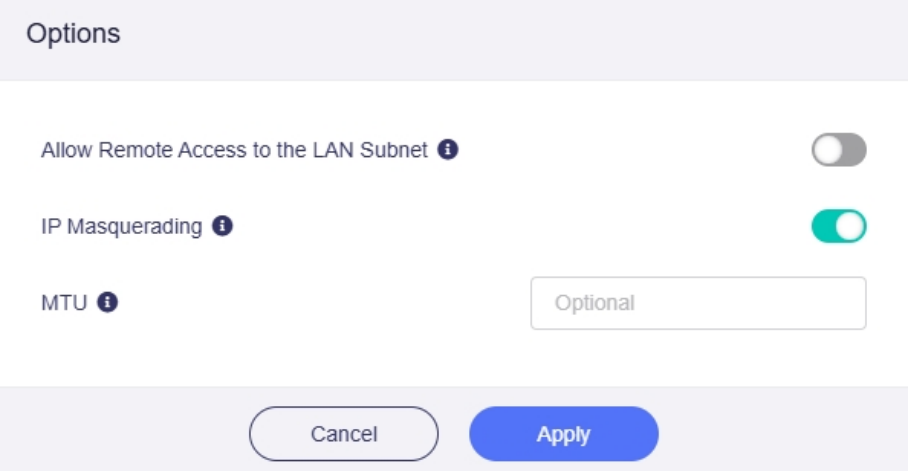
10.1.4 Opciones del servidor

Las opciones del servidor incluyen algunas configuraciones avanzadas en el lado del servidor, como la LAN del servidor de acceso remoto, enmascaramiento de IP, etc. Configure estas configuraciones según sus necesidades.

En el **Servidor OpenVPN** página, haga clic en **Opciones** en la esquina superior derecha.



En la ventana emergente, verá las siguientes funciones.



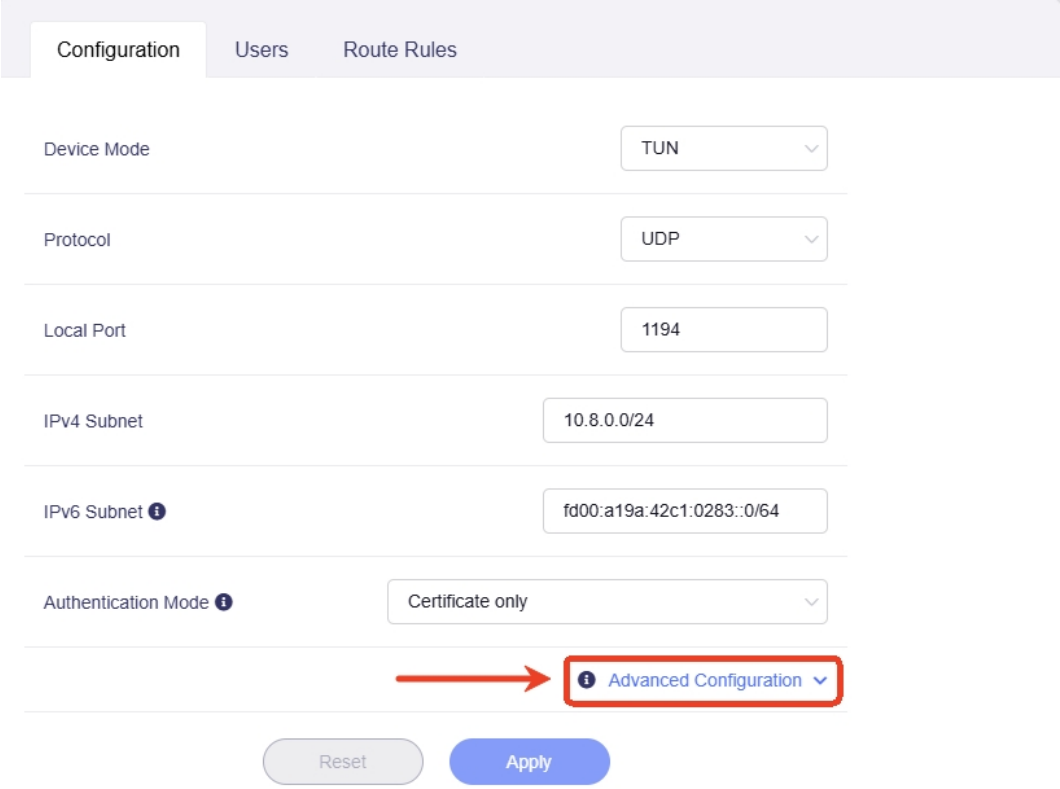
- **Permitir acceso remoto a la subred LAN**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través del túnel VPN.
- **Enmascaramiento de IP**: Si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Desactive esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión máxima. El valor de MTU que establezca para el túnel anulará la configuración de MTU en el archivo de configuración.

10.1.5 Comunicación entre clientes

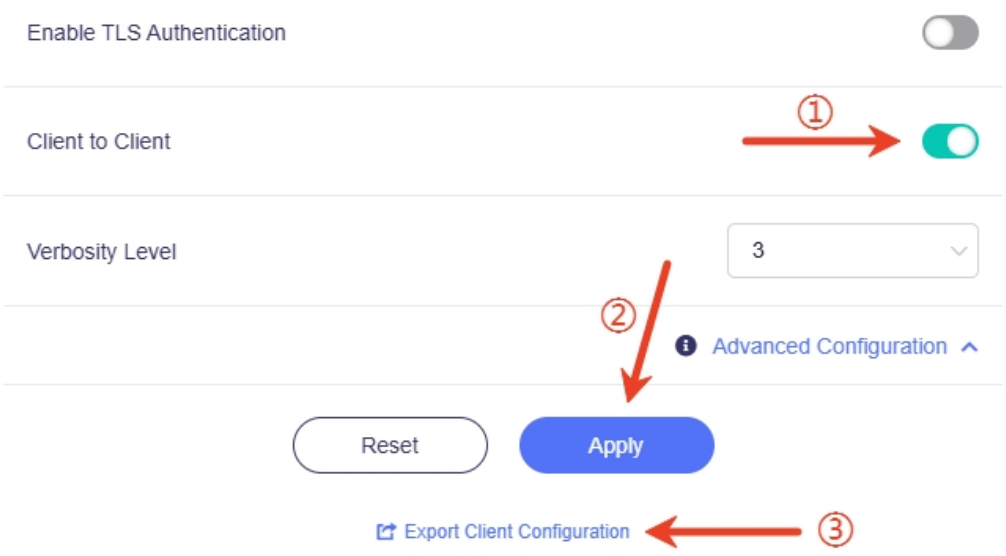
Cliente-a-El cliente es una característica VPN-del lado del servidor. Una vez habilitados, los clientes VPN conectados pueden comunicarse entre sí utilizando sus respectivas direcciones IP de túnel VPN.

Siga los pasos a continuación para habilitar Cliente a Cliente en su servidor OpenVPN si es necesario.

1. En **Servidor OpenVPN**, haga clic en **Configuración avanzada** en la parte inferior derecha.



2. Habilitar **Comunicación entre clientes** y haga clic en **Aplicar**. Luego exporte una nueva configuración y cárguela en sus clientes OpenVPN.



Consejo: Cliente-a-El cliente solo anuncia la dirección IP del túnel de cada cliente. No expone automáticamente las subredes LAN locales detrás de cada cliente VPN. Si necesita otorgar a los clientes acceso a las subredes LAN de cada uno, agregue reglas de enrutamiento en el servidor VPN para anunciar esas subredes LAN remotas.

10.2 Servidor WireGuard

WireGuard® es una VPN extremadamente simple pero rápida y moderna que utiliza criptografía de última generación. Su objetivo es ser más rápido, más simple, más ágil y más útil que IPSec, evitando al mismo tiempo el enorme dolor de cabeza. Pretende tener un rendimiento considerablemente mayor que OpenVPN.
*WireGuard® es una marca registrada de Jason A. Donenfeld.

Para configurar el servidor WireGuard en un enrutador GL.iNet, consulte este vídeo o consulta los pasos a continuación.

10.2.1 Preparación

1. **Asegúrate de tener una dirección IP pública**
   Haga clic aquí para verificar si su proveedor de servicios de Internet le asigna una dirección IP pública.
   Si no, su enrutador no se puede configurar como WireGuard Servidor.

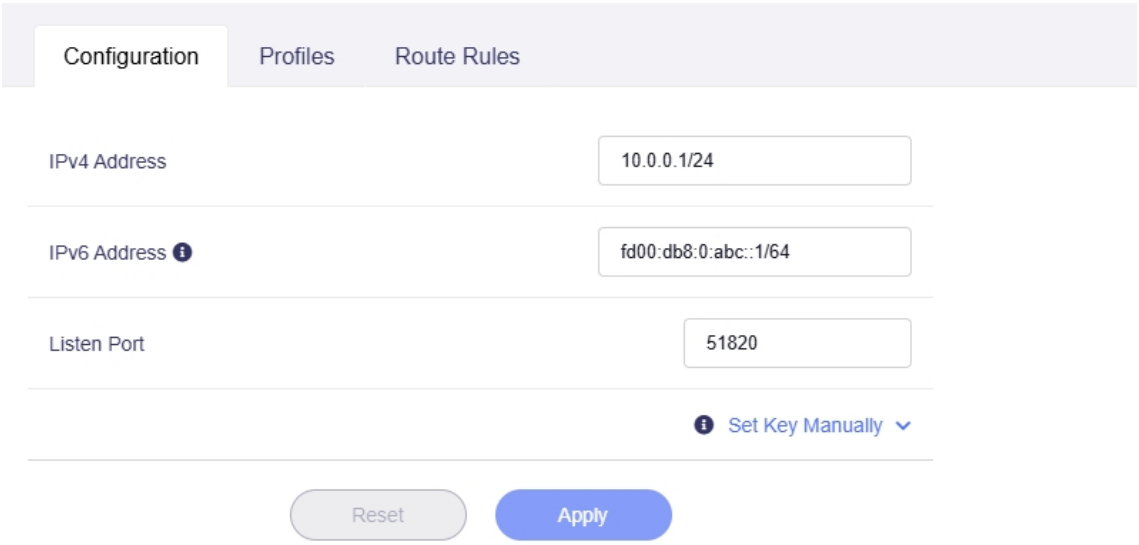
   Métodos alternativos:
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por ejemplo, si su red está detrás de CGNAT), puede probar nuestra solución SD-WAN AstroWarp.

2. **Confirme si se requiere reenvío de puertos**
   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puertos. Continúe con el siguiente paso.
   - Si ya hay un enrutador primario en uso y su enrutador GL.iNet está configurado como enrutador secundario, necesitará configurar el reenvío de puertos en el enrutador principal.
   - Si su enrutador GL.iNet está en varios niveles descendentes desde el enrutador principal, configure el reenvío de puertos en cada intermedio dispositivo.

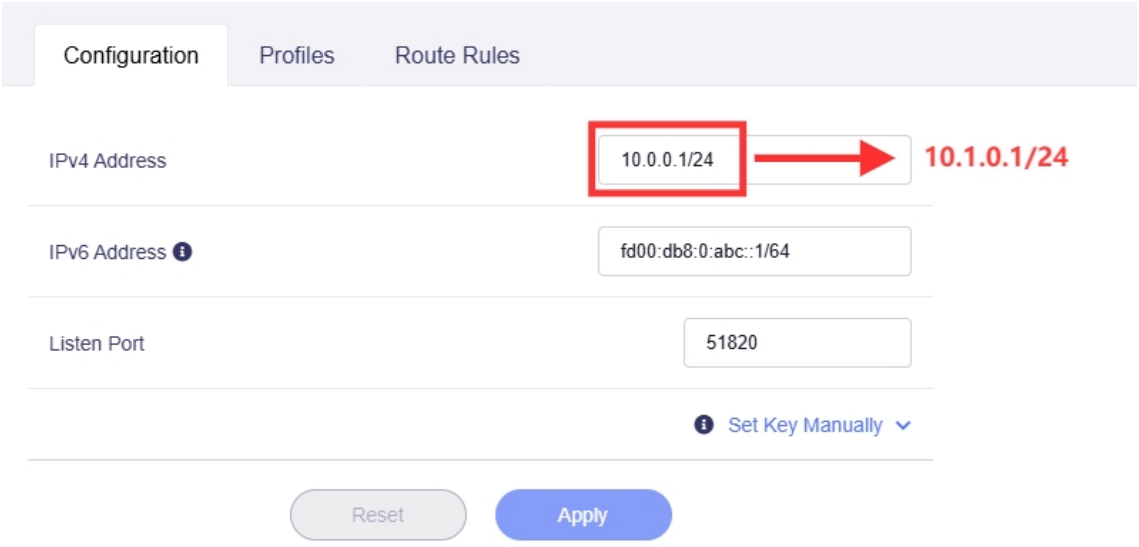
10.2.2 Pasos de configuración

1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **VPN** > **Servidor WireGuard** y luego haga clic en **Generar configuración** (solo para la configuración inicial del servidor VPN).
2. Aplicar la configuración.

   La configuración predeterminada funciona en la mayoría de los casos. No es necesario modificar la dirección IPv4 a menos que it conflictos con la puerta de enlace del enrutador ascendente.

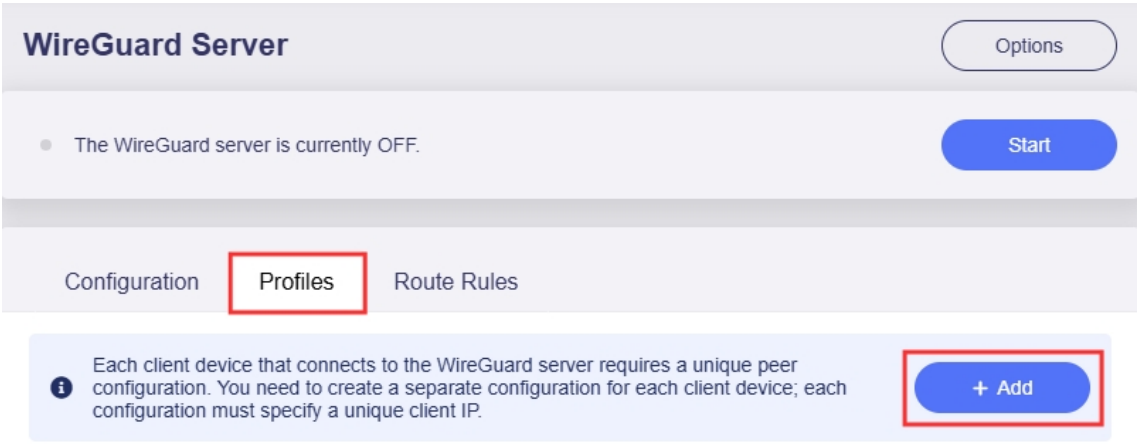


   Si el IPv4 dirección entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

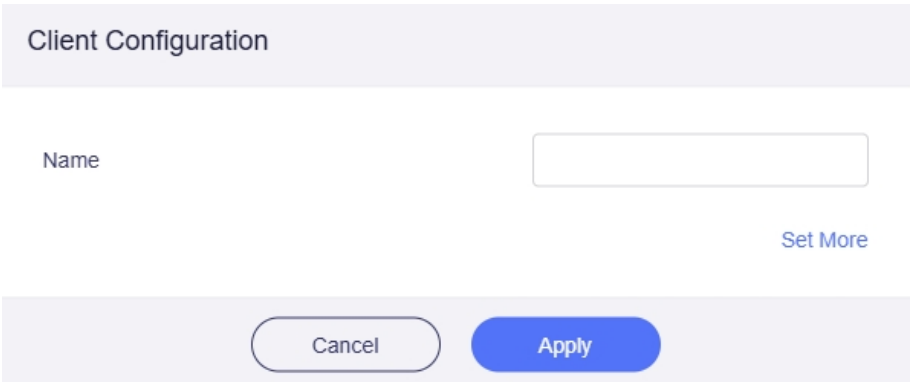


3. Agregue un perfil.

   Cambiar a **Perfiles** , haga clic en el botón **Agregar** para generar un perfil para su dispositivo.



   Establezca un nombre descriptivo y haga clic en **Aplica** para continuar.



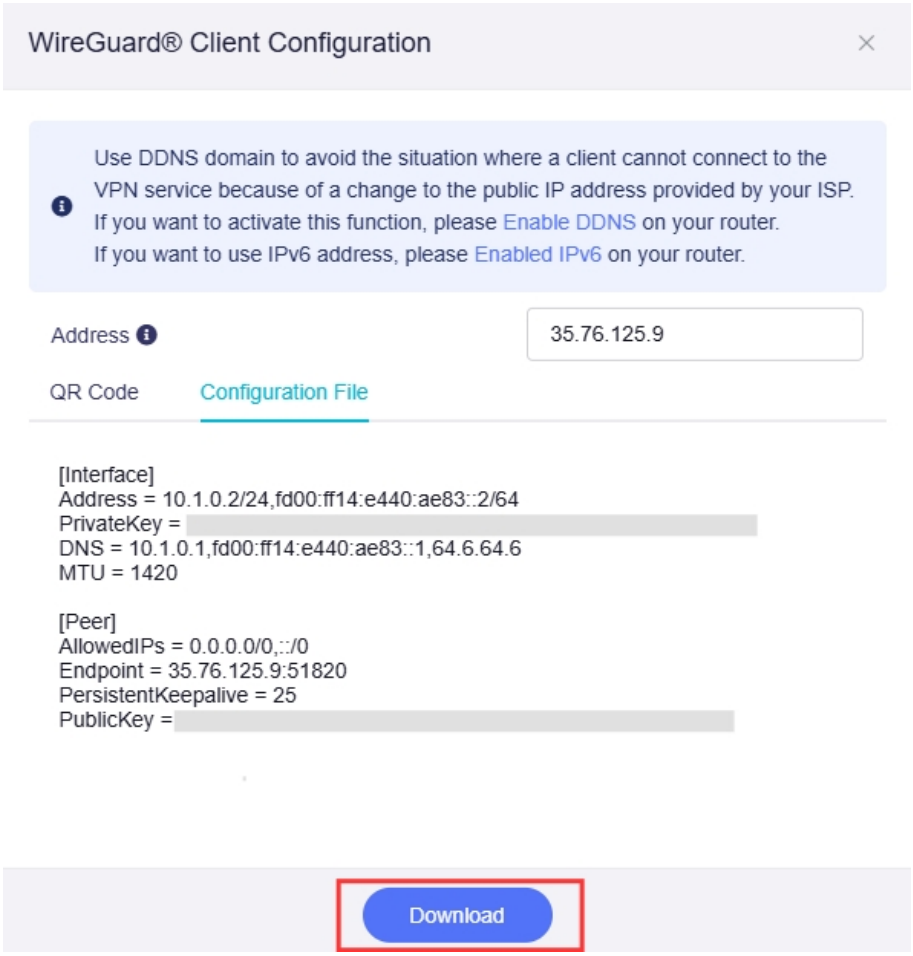
   Consejo: Si deseas acceder a el Dispositivos LAN del cliente WireGuard desde su servidor WireGuard , cambie a las **Reglas de ruta** para configurar reglas de ruta. Consulte aquí para detalless.

4. Descargar configuración.

   Después de agregar un perfil, el enrutador generará un archivo de configuración en tres formatos: código QR, texto sin formato y Archivo .conf. Elija su método preferido para obtener el archivo de configuración.

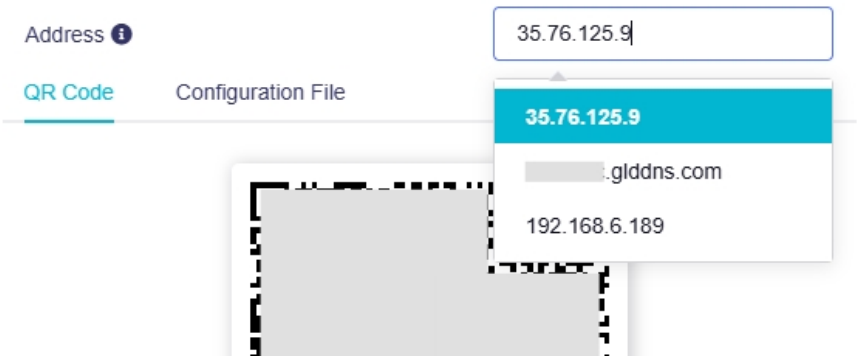
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar un archivo de configuración.

- **Texto sin formato**: en texto sin formato formato, puede revisar los detalles de configuración y copiarlos y pegarlos cómodamente en otro lugar para la configuración manual, como la aplicación WireGuard o un enrutador GL.iNet.
- **archivo.conf**: haga clic en **Descargar** para guardar el archivo .conf en su dispositivo local. También es conveniente y se puede cargar directamente en la aplicación WireGuard o en un enrutador GL.iNet.



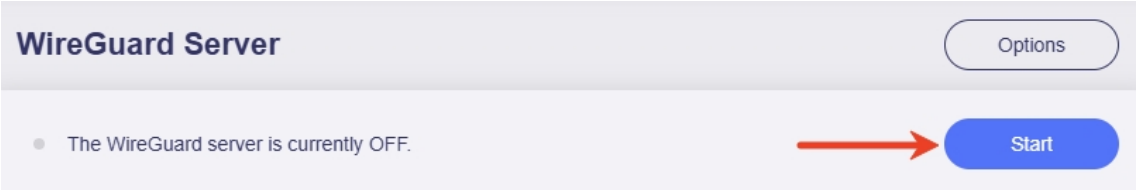
Consejos:

- Si su dirección IP pública cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de configuración: IP pública, dominio DDNS y dirección IP WAN actual. Una vez seleccionada, la dirección del servidor en el archivo de configuración se actualizará automáticamente. Vuelva a descargar el archivo de configuración si se cambia la dirección del servidor.

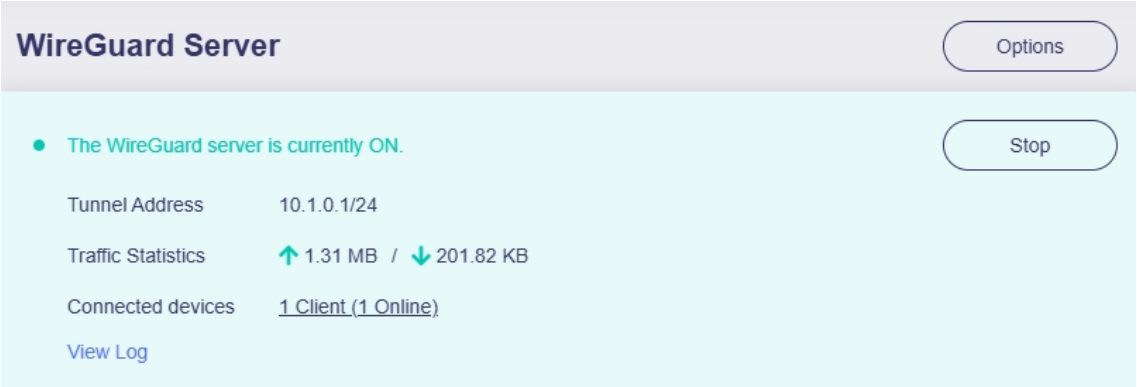


5. Inicie el servidor WireGuard.

   En la página **Servidor WireGuard**, haga clic en **Botón Iniciar** en la esquina superior derecha para iniciar el servidor.



   El servidor estado de conexión se se muestra en el arriba. Si muestra carga, descargar estadísticas de tráfico, y dispositivos conectados en línea, significa que el servidor WireGuard se está ejecutando.

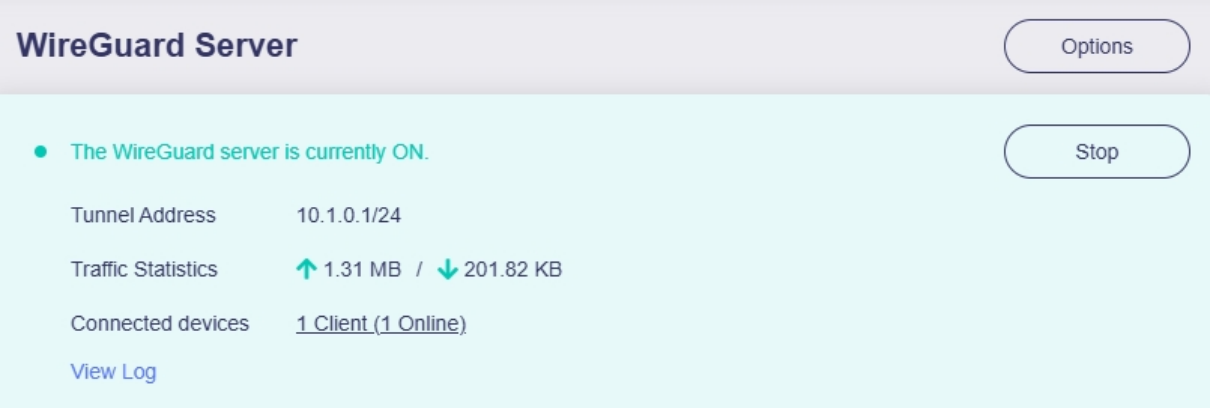


10.2.3 Verificar conexión

Método 1. Verificar el estado del servidor

En firmware v4.8, puede verificar el estado de la conexión del servidor en la página **Servidor WireGuard**.

Si muestra estadísticas de tráfico de carga/descarga y dispositivos conectados en línea, significa que el servidor WireGuard se está ejecutando y hay clientes WireGuard conectados a it.



Si muestra 0 tráfico y 0 cliente, significa que no hay ningún cliente WireGuard conectado.



Método 2. Verificar la IP del cliente

Importe la configuración de WireGuard previamente-exportada a un dispositivo en una red diferente (no en la misma red local que el servidor). Luego abra un navegador web, busque su dirección IP y ubicación. Si coinciden con la IP del servidor VPN (en lugar de la IP de su proveedor de servicios de Internet) y la ubicación, la conexión VPN es exitosa.

Aquí'hay un ejemplo para usar un teléfono inteligente con la Aplicación WireGuard instalada para verificar.

1. Primero, deshabilite el Wi-Fi del teléfono inteligente y habilite los datos móviles (4G/5G) exclusivamente.
2. A continuación, abra la aplicación WireGuard, importe el archivo de configuración e inicie la conexión.
3. Compruebe si el teléfono inteligente puede acceder a Internet y si su dirección IP coincide con la IP del servidor WireGuard.

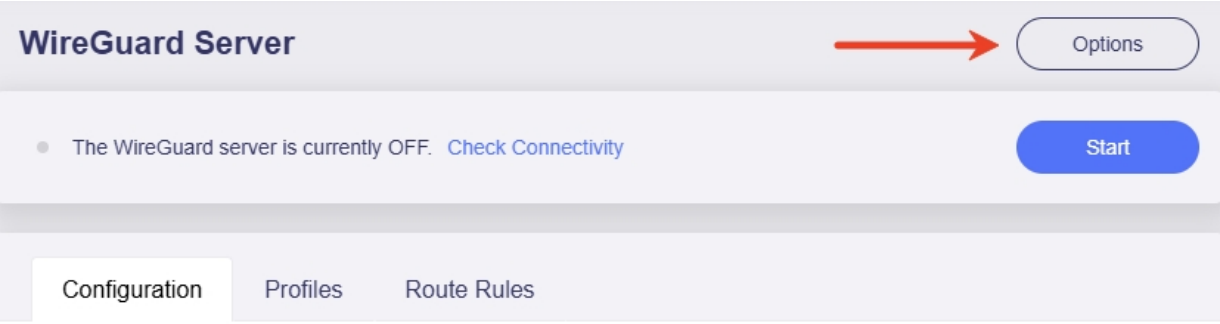
Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulte **10.2.1 Preparación** para obtener más detalles.
- Es posible que deba configurar el reenvío de puertos. Consulte **10.2.1 Preparación** para obtener más detalles.
- El puerto utilizado parae WireGuard Server está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

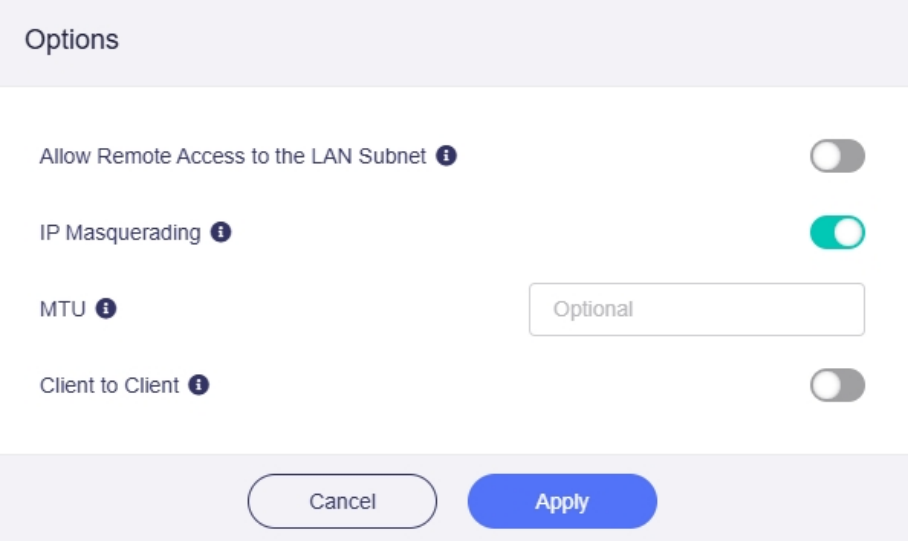
10.2.4 Opciones del servidor

Las opciones del servidor incluyen algunas configuraciones avanzadas en el lado del servidor, como la LAN del servidor de acceso remoto, enmascaramiento de IP, etc. Configure estas configuraciones según sus necesidades.

En **Servidor WireGuard** página, haga clic en **Opciones** en la esquina superior derecha.



En la ventana emergente, verá lo siguiente características.



- **Permitir acceso remoto a la subred LAN**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través del túnel VPN.
- **Enmascaramiento de IP**: Si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Desactive esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión máxima. El valor de MTU que establezca para el túnel anulará la configuración de MTU en el archivo de configuración.
- **Comunicación entre clientes**: si está habilitado, los clientes VPN conectados a este servidor pueden acceder entre sí a través de sus respectivas IP de túnel VPN.
  Tenga en cuenta que Cliente-a-Cliente solo anuncia la dirección IP del túnel de cada cliente. No expone automáticamente las subredes LAN locales detrás de cada cliente VPN. Si necesita otorgar a los clientes acceso a las subredes LAN de cada uno, agregue reglas de enrutamiento en el servidor VPN para anunciar esas subredes LAN remotas.

Capítulo 11

Configurar el cliente VPN

Este capítulo presenta cómo configurar un enrutador GL.iNet como cliente OpenVPN o WireGuard.

11.1 Cliente OpenVPN

11.1.1 Preparación

Primero, asegúrese de tener una suscripción activa con un proveedor de servicios VPN que admita la configuración manual de OpenVPN. Consulte aquí para conocer los proveedores de OpenVPN compatibles con GL.iNet.

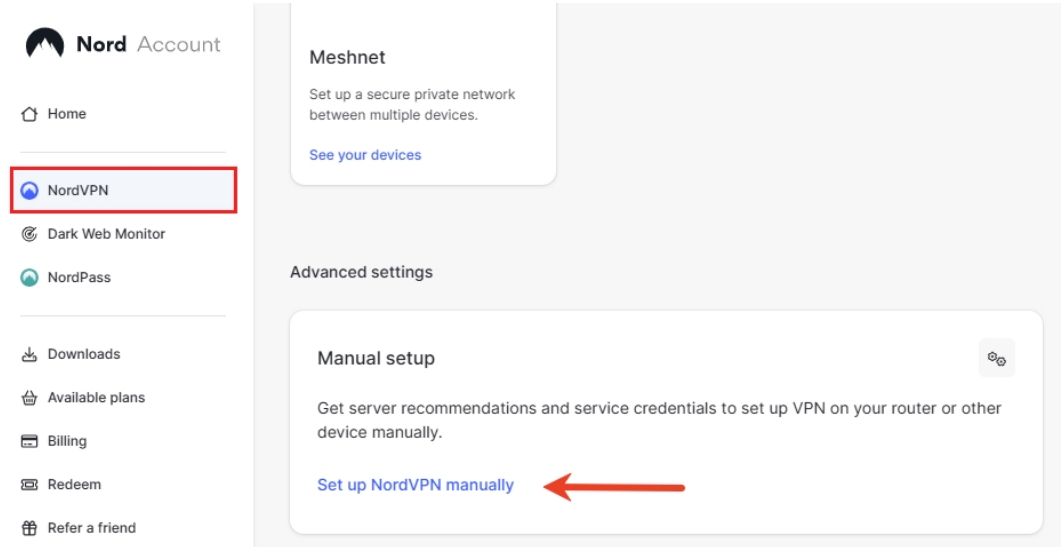
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

11.1.2 Configurar NordVPN

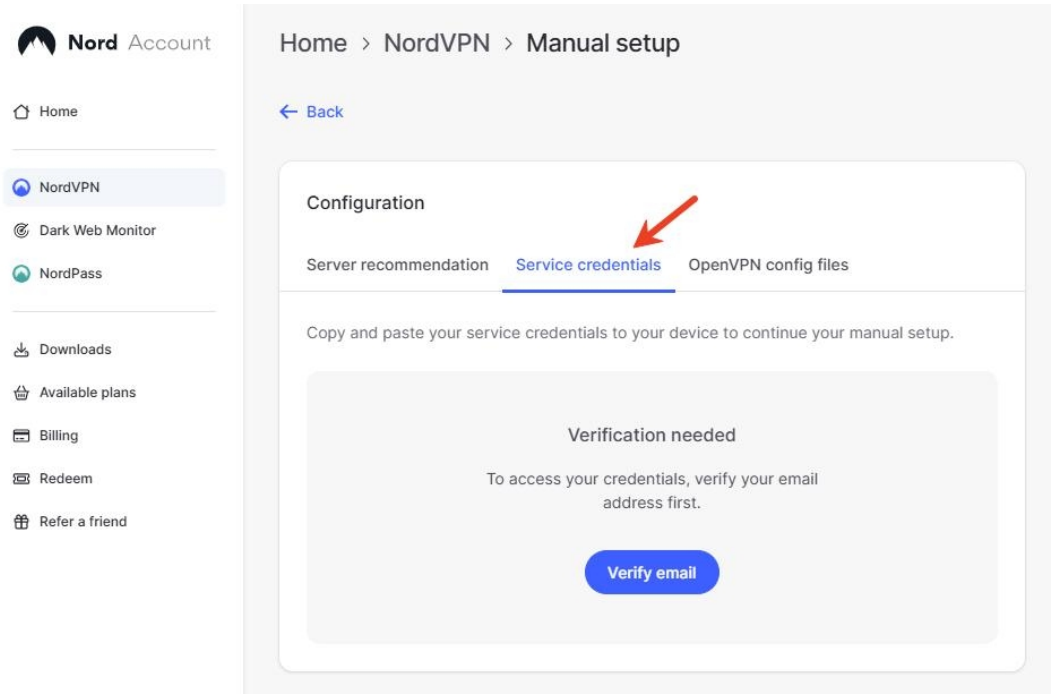
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet , lo que elimina la necesidad de cargar archivos manualmente.

Siga los pasos a continuación para configurar su enrutador como cliente NordVPN.

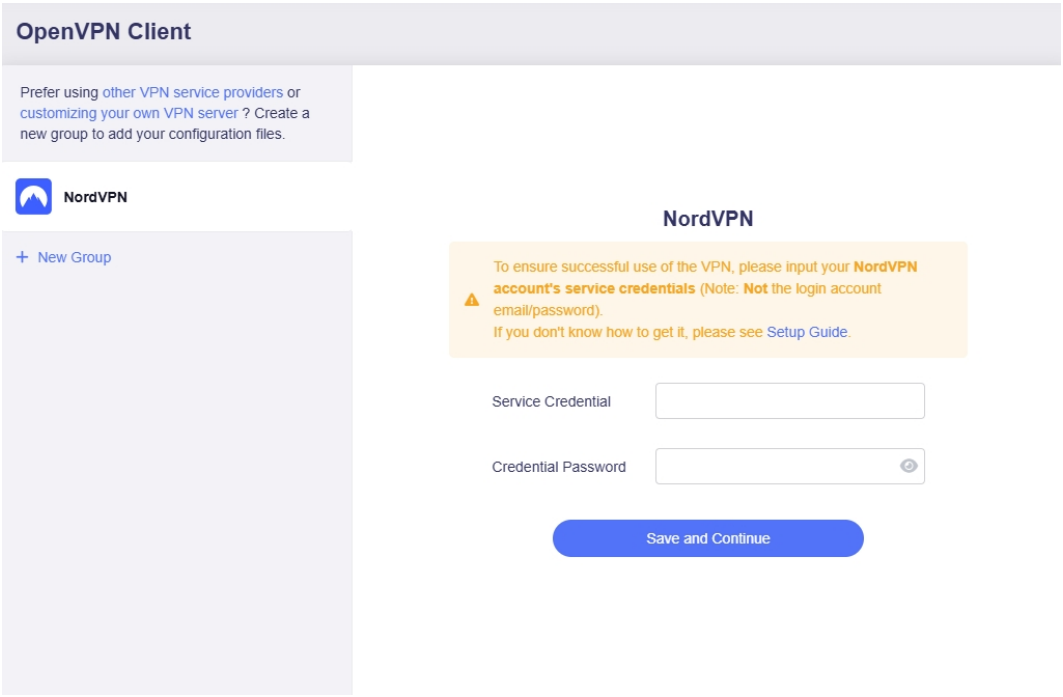
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen el Nord Dashboard, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



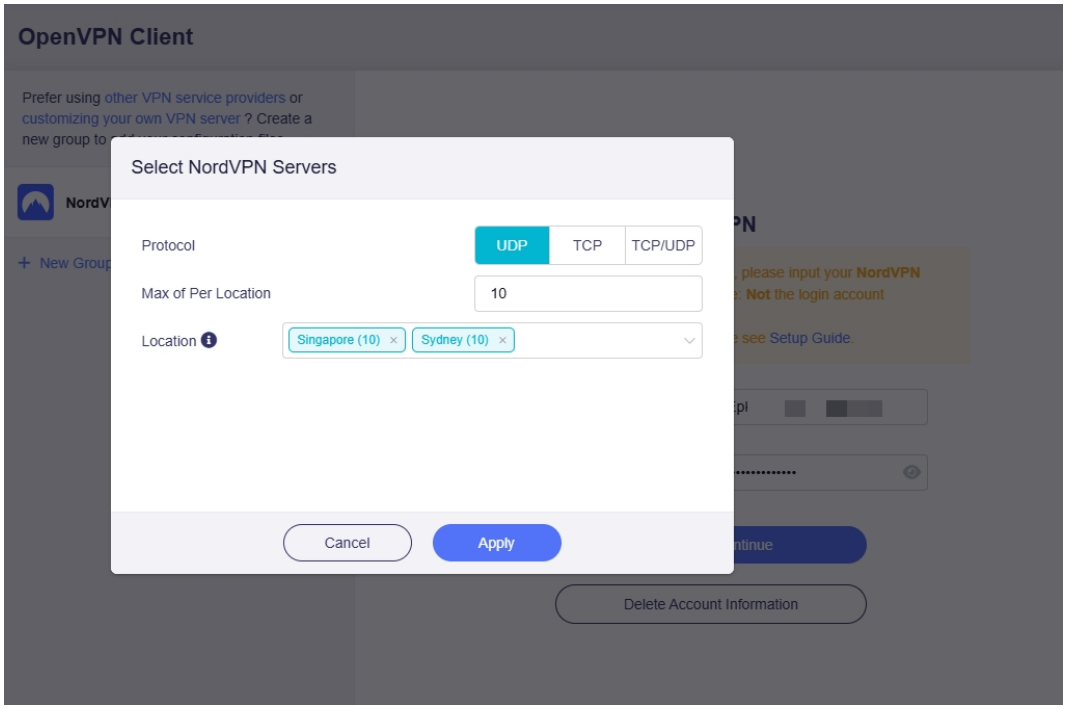
Encontrará el servicio **credenciales**. Cópielos para usarlos más adelante.



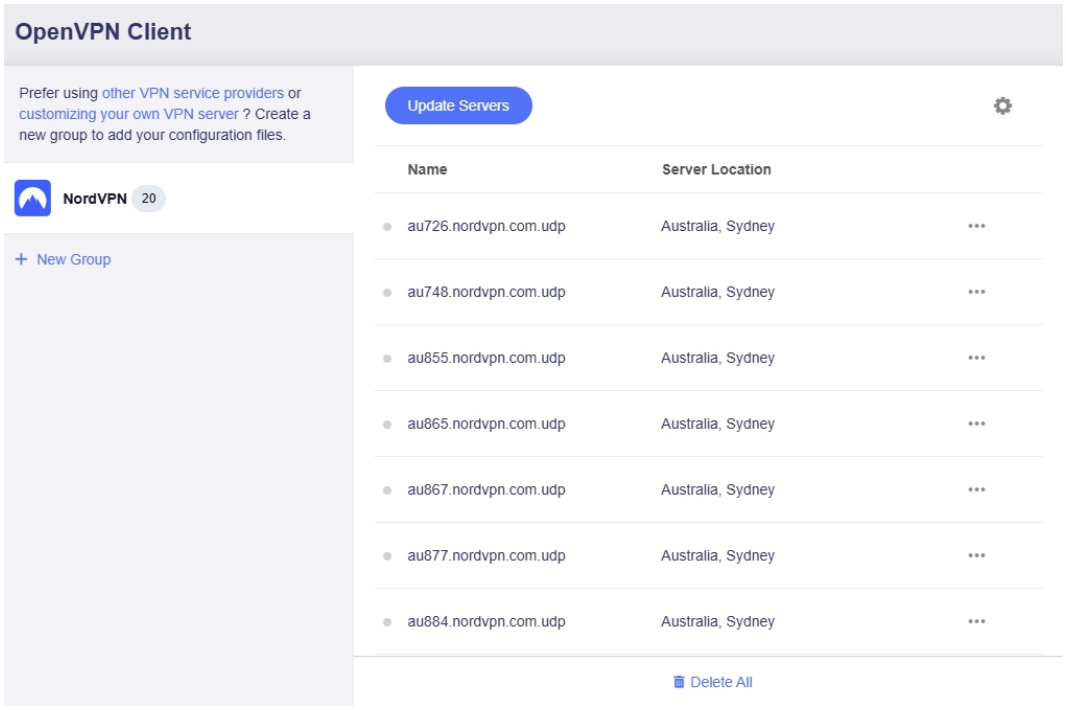
3. Inicie sesión en el panel de administración web de su enrutador y navegue a **VPN** > **Cliente OpenVPN** > **NordVPN**. Ingrese las credenciales de servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



4. Seleccione el protocolo, el número máximo de servidores de cada ubicación y las ubicaciones, luego haga clic en **Aplicar**.

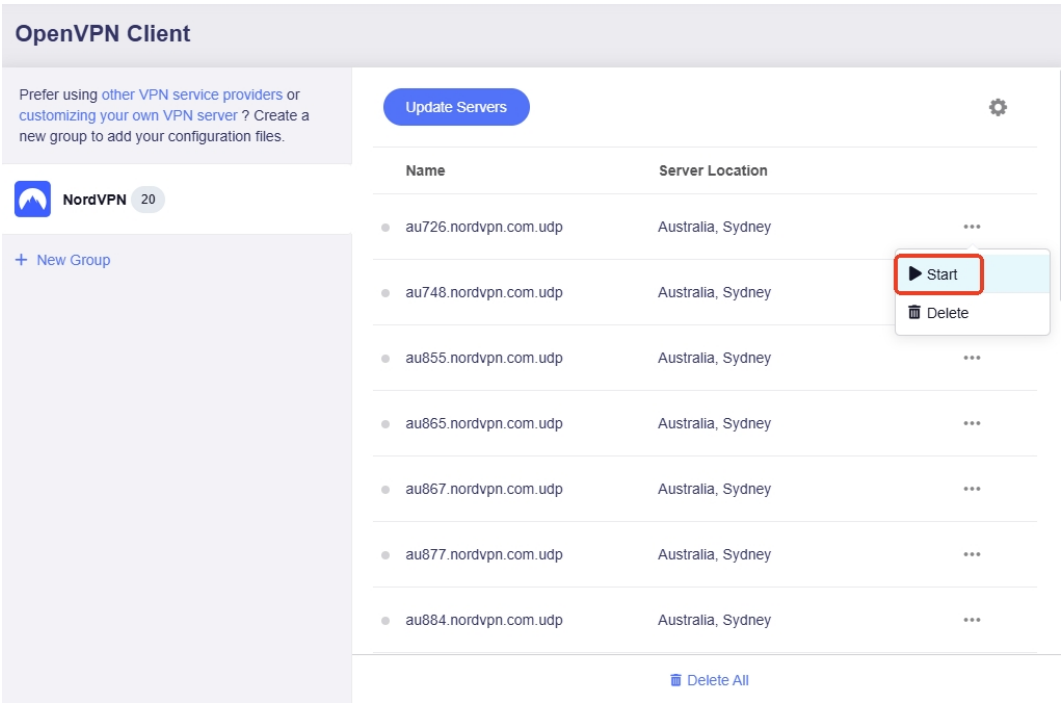


Descargará los archivos de configuración.

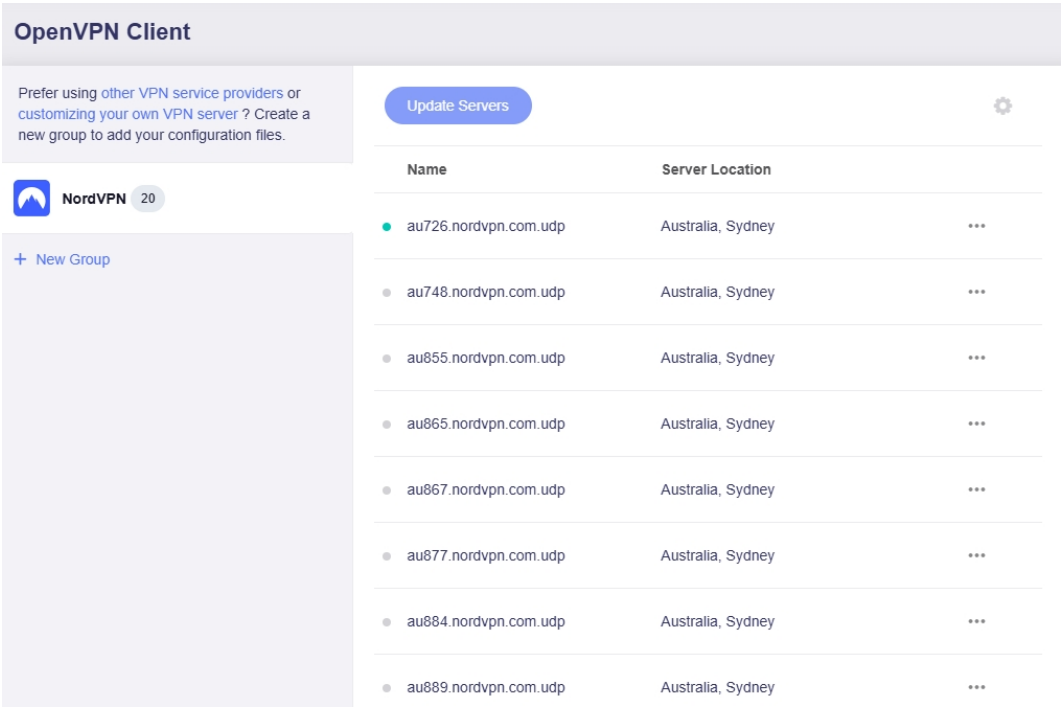


5. Iniciará una conexión.

   Seleccione un servidor y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



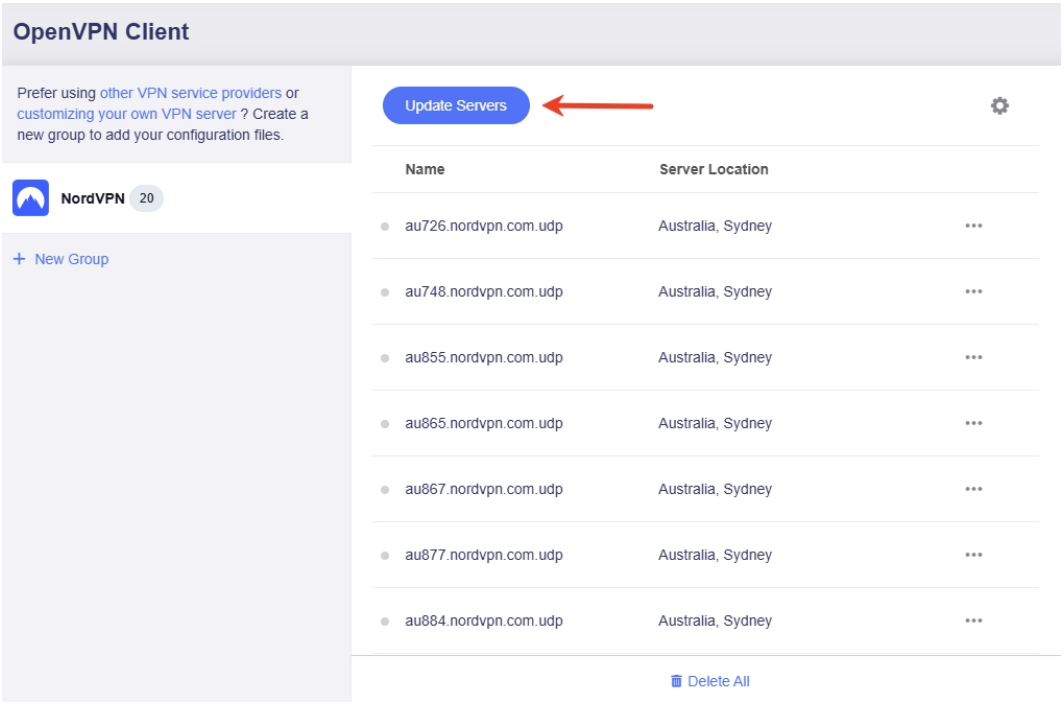
6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



También puede consultar el Detalles de la conexión VPN en el **Panel de VPN**.

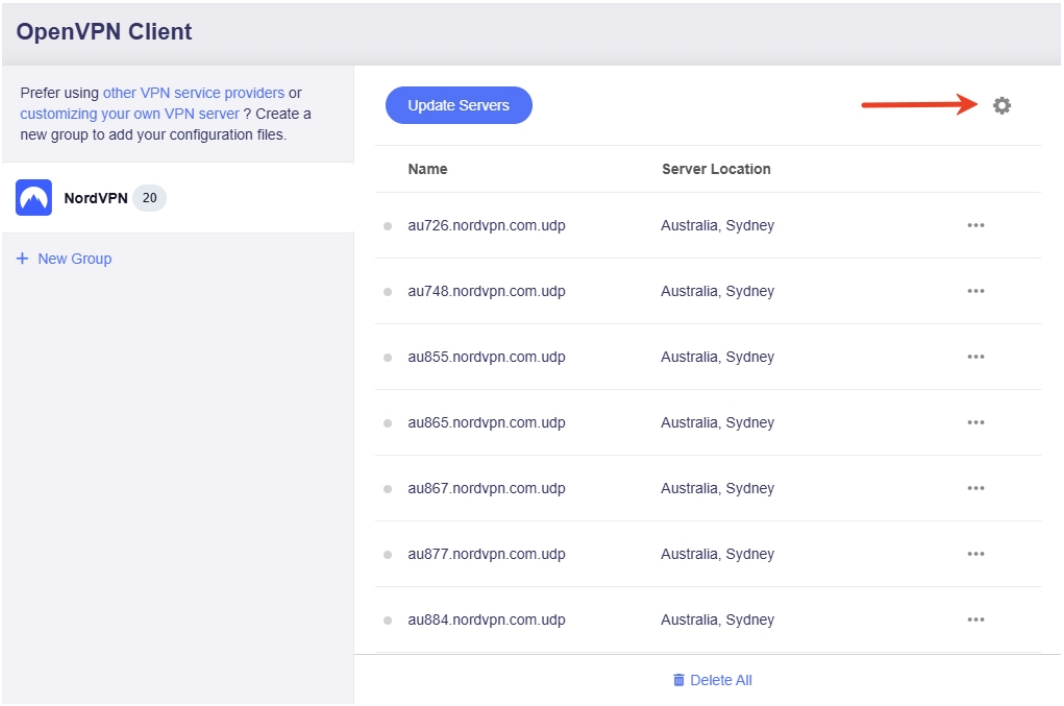
7. Actualizar servidores.

Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



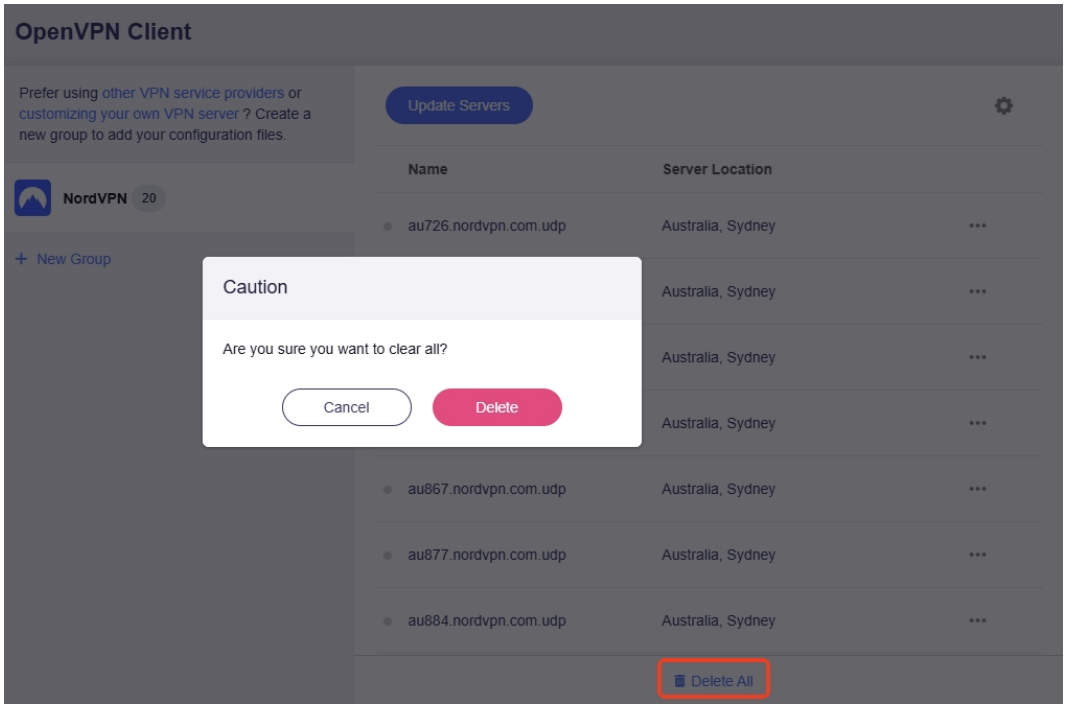
8. Editar credenciales.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Eliminar todos los archivos.

Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic.

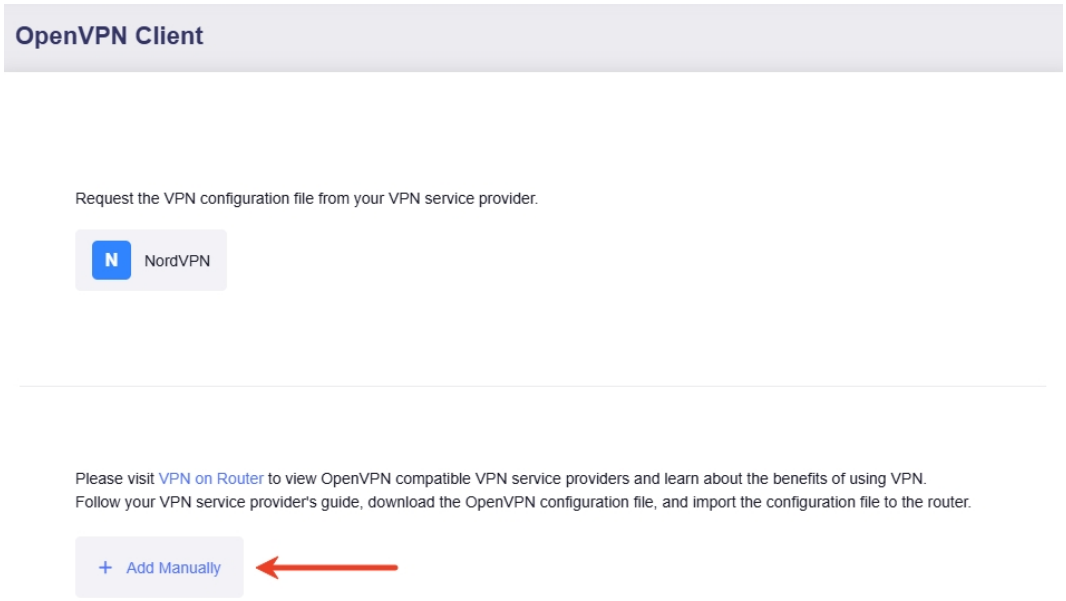


11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

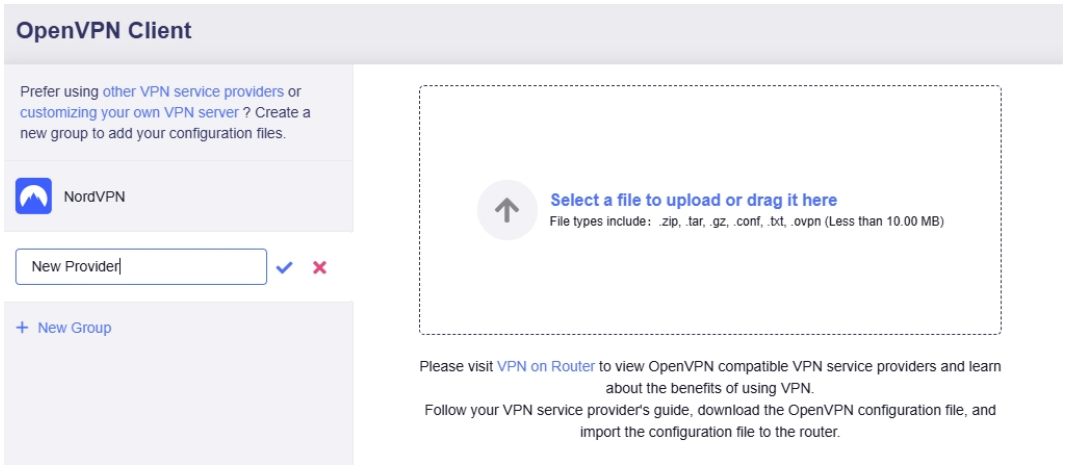
Si El proveedor de servicios OpenVPN no está integrado en nuestro panel de administración; primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

En los siguientes pasos, usaremos PIA (Private Internet Access) como ejemplo.

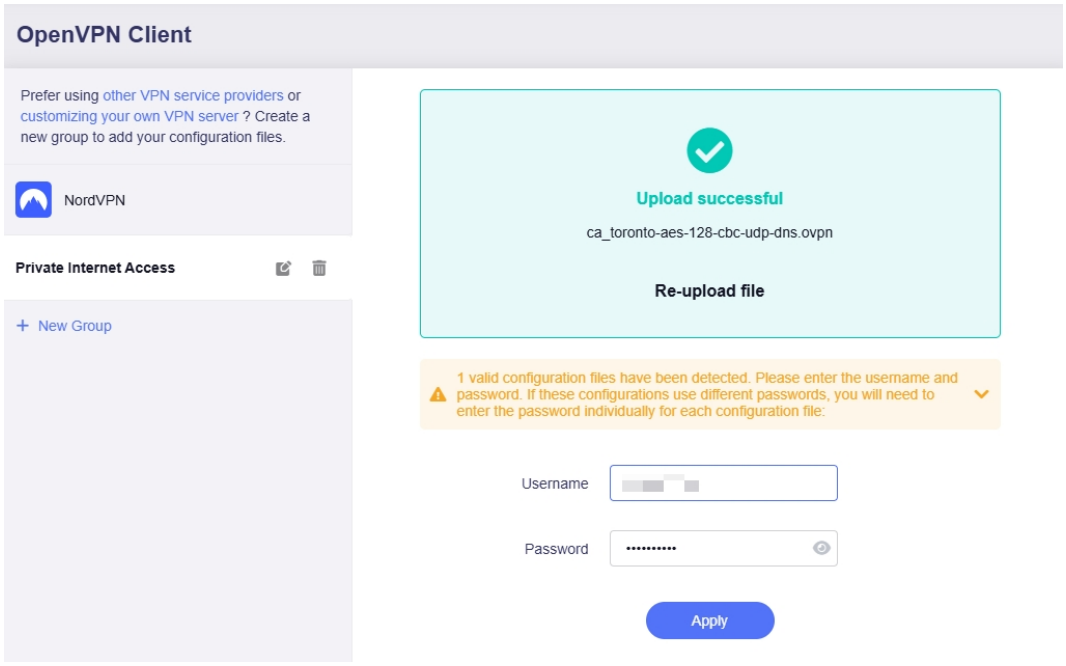
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar. Manualmente**.



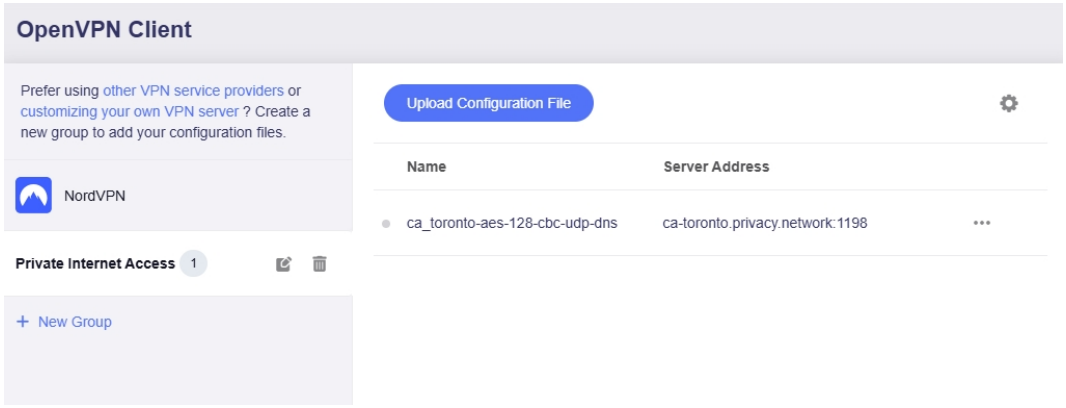
3. Creará un grupo en la barra lateral izquierda.Establece un nombre descriptivo para el grupo.



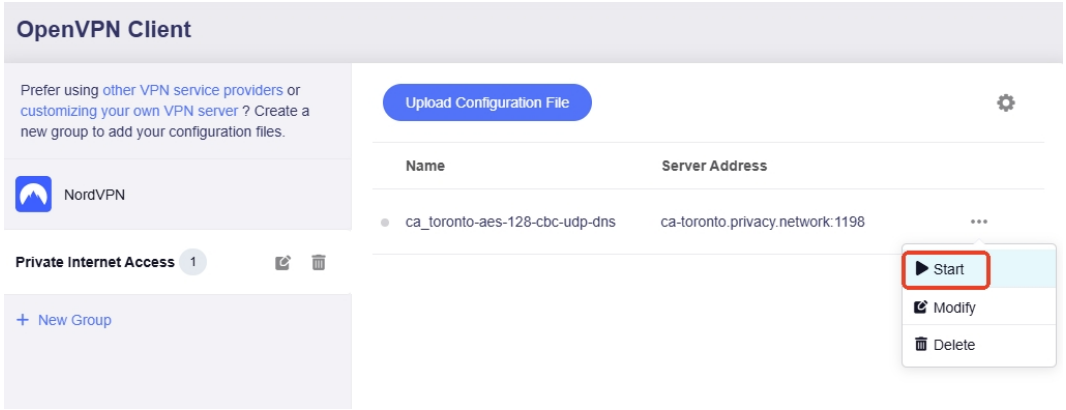
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



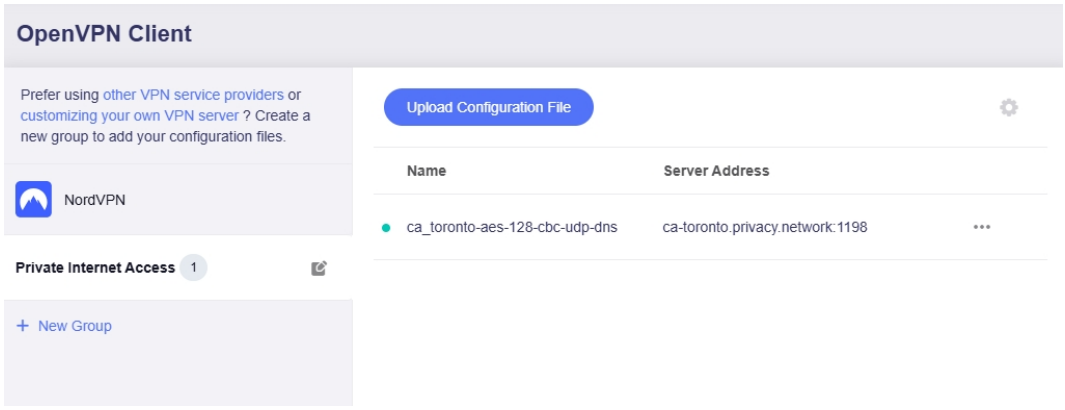
YVerá el archivo de configuración cargado.



5. Haga clic en el ícono de tres puntos en el derecho para iniciar una conexión.



6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

11.2 Configurar el cliente WireGuard

Puedes configurar el cliente WireGuard® a través de la aplicación móvil GL.iNet o la web panel de administración.

- La aplicación móvil integra algunos proveedores de servicios WireGuard, como AzireVPN, Mullvad VPN, OVPN, StrongVPN, PIA VPN. Puede configurarlo fácilmente ingresando las credenciales de inicio de sesión del servicio WireGuard al que se suscribió. Abra la aplicación y siga las instrucciones en pantalla para configurarla.
- El panel de administración web no solo integra algunos proveedores de servicios WireGuard, sino que también proporciona una entrada para la configuración manual. Puede ingresar las credenciales de su servicio WireGuard suscrito para una configuración rápida o cargar manualmente un archivo de configuración para completar la configuración.

*WireGuard® es una marca registrada de Jason A. Donenfeld.

11.2.1 Preparación

Primero, asegúrese de tener una suscripción activa con un proveedor de servicios VPN que admita la configuración manual de WireGuard. Consulte aquí para conocer los proveedores WireGuard compatibles con GL.iNet.

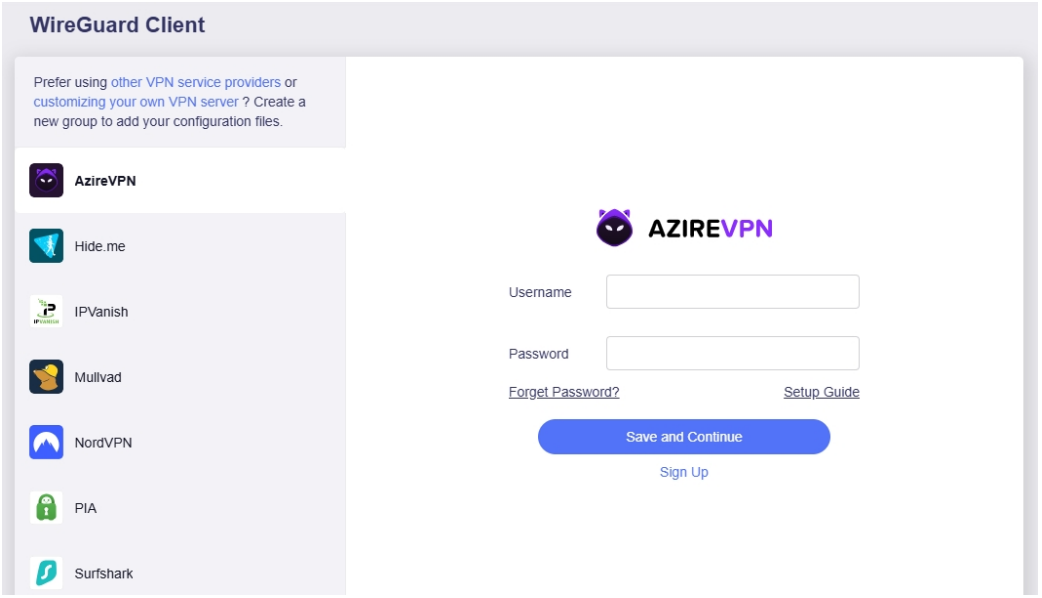
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- Configurar AzireVPN
- Configurar Hide.me
- Configurar IPVanish
- Configurar Mullvad
- Configurar NordVPN
- Configurar PIA (Private Internet Access)
- Configurar Surfshark
- Configurar el cliente WireGuard manualmente (para otros proveedores)

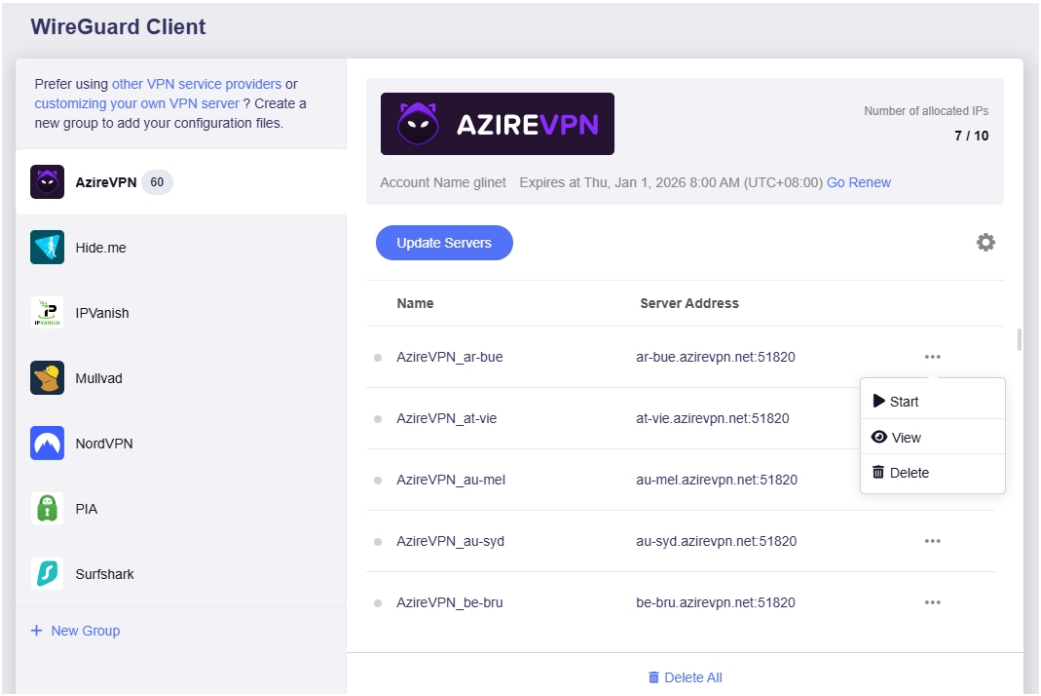
11.2.2 Configurar AzireVPN

Siga los pasos a continuación para configurar su enrutador como cliente AzireVPN.

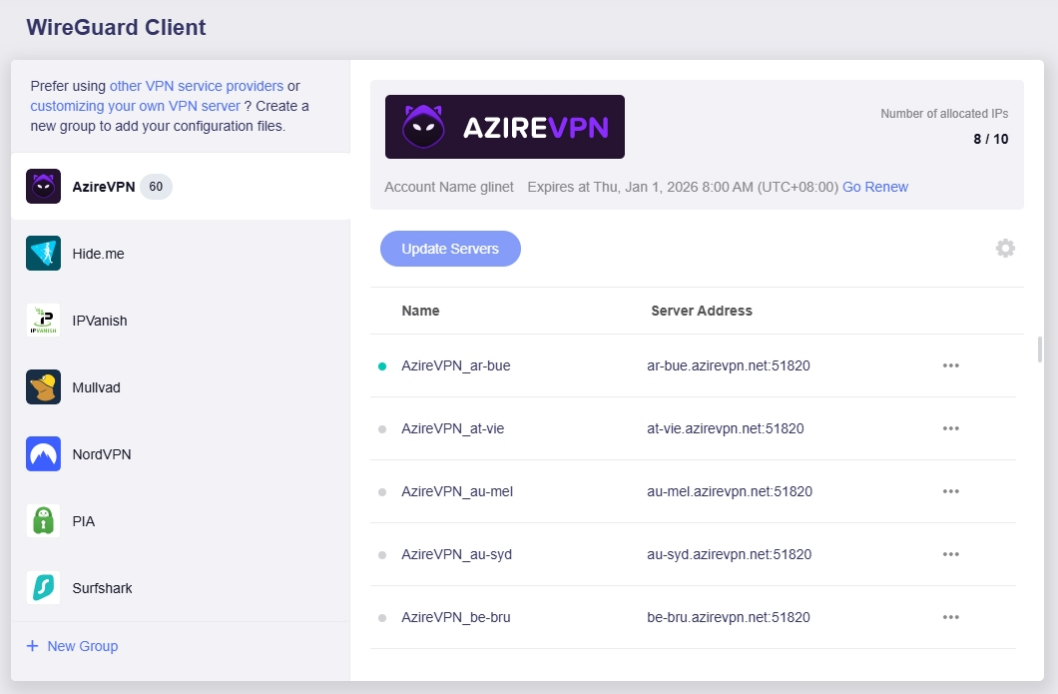
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



3. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



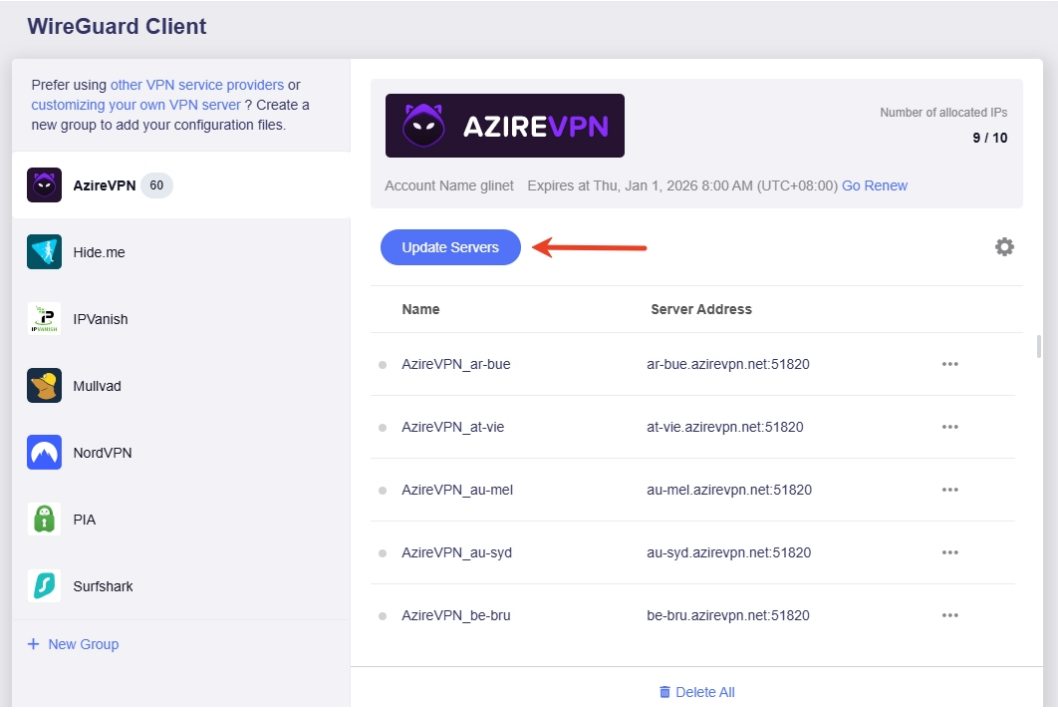
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar los detalles de la conexión VPN en el **Panel de VPN**.

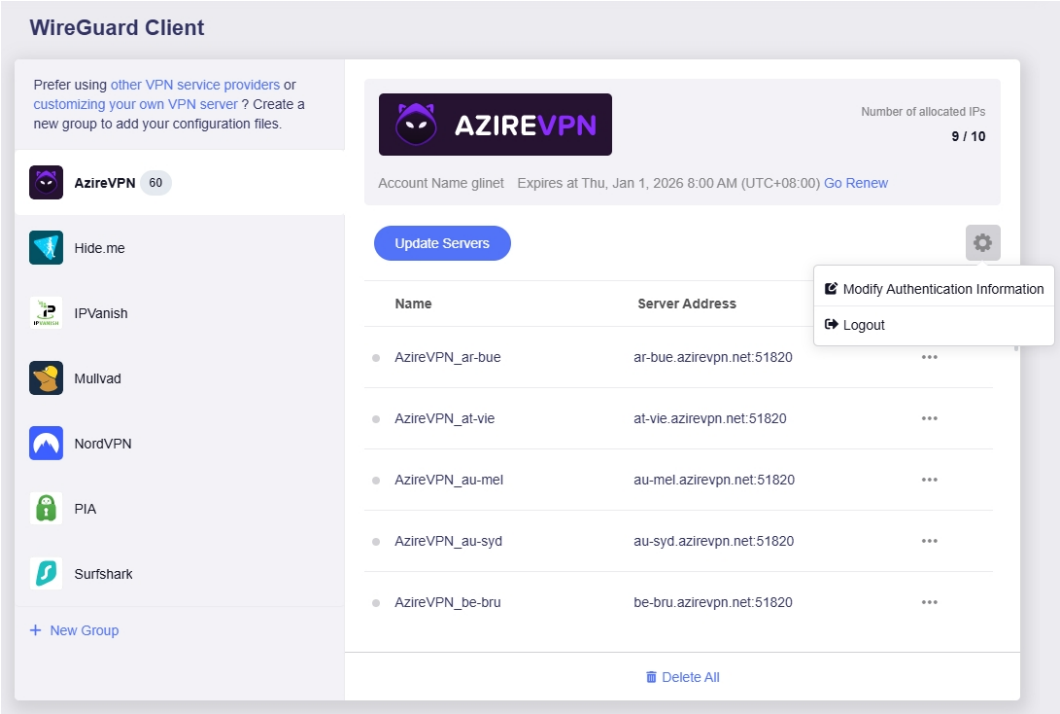
5. Actualizar servidores.

Puedes hacer clic en **Actualice servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



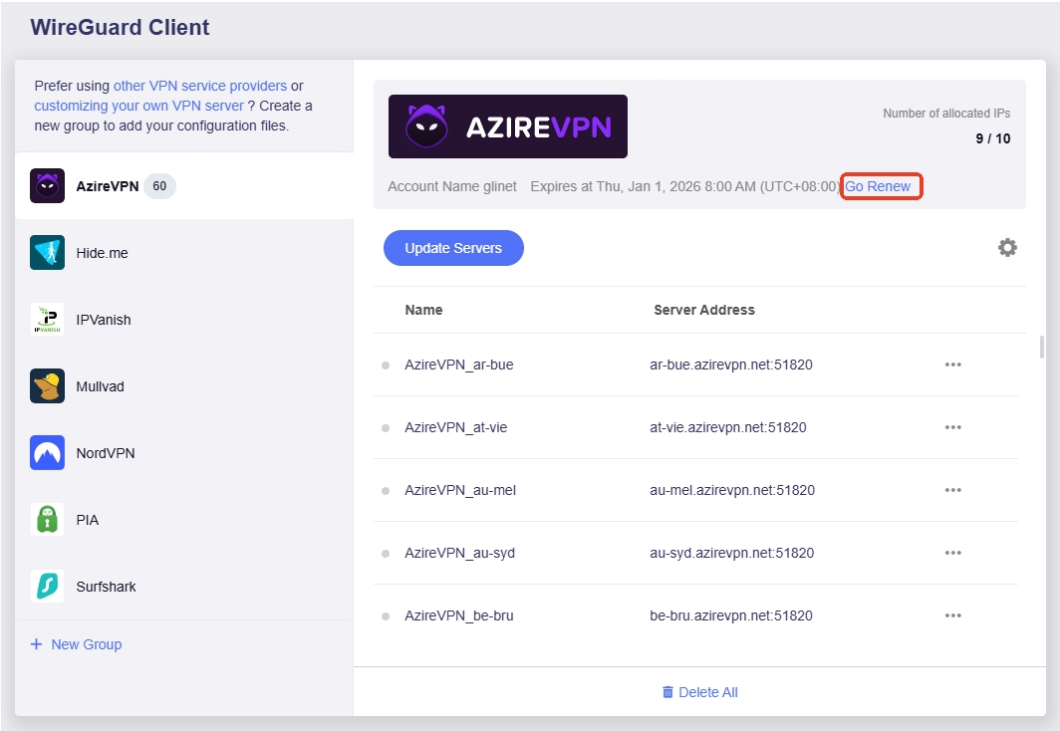
6. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cierre sesión.



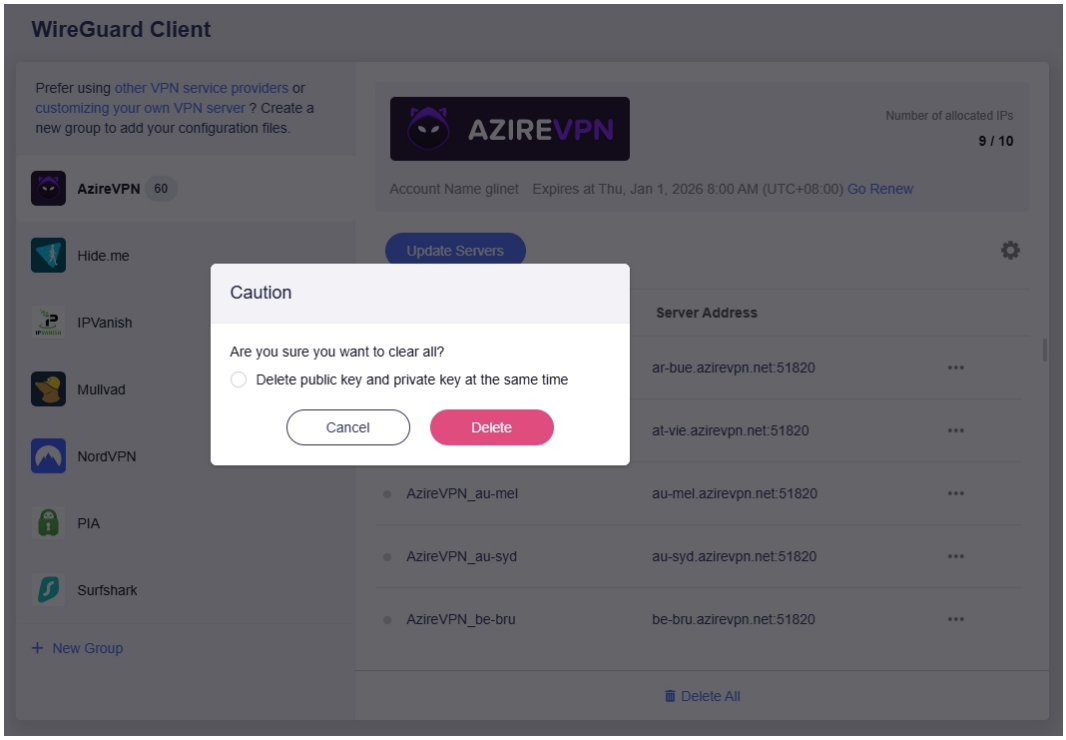
7. Ir a renovar.

   Si hace clic en **Ir a renovar**, será redirigido al sitio web oficial para renueva tu suscripción.



8. Eliminar todos los archivos.

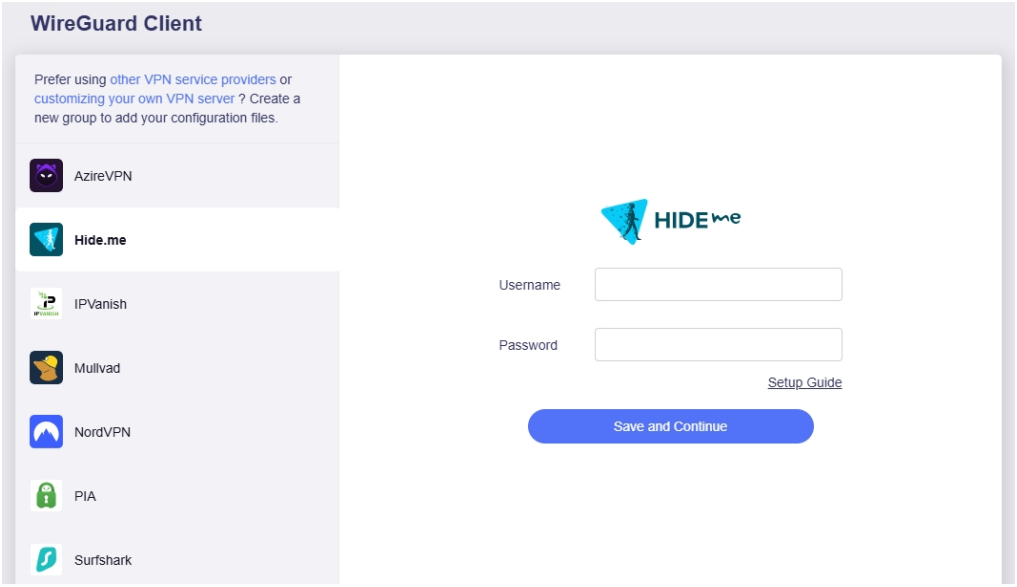
Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



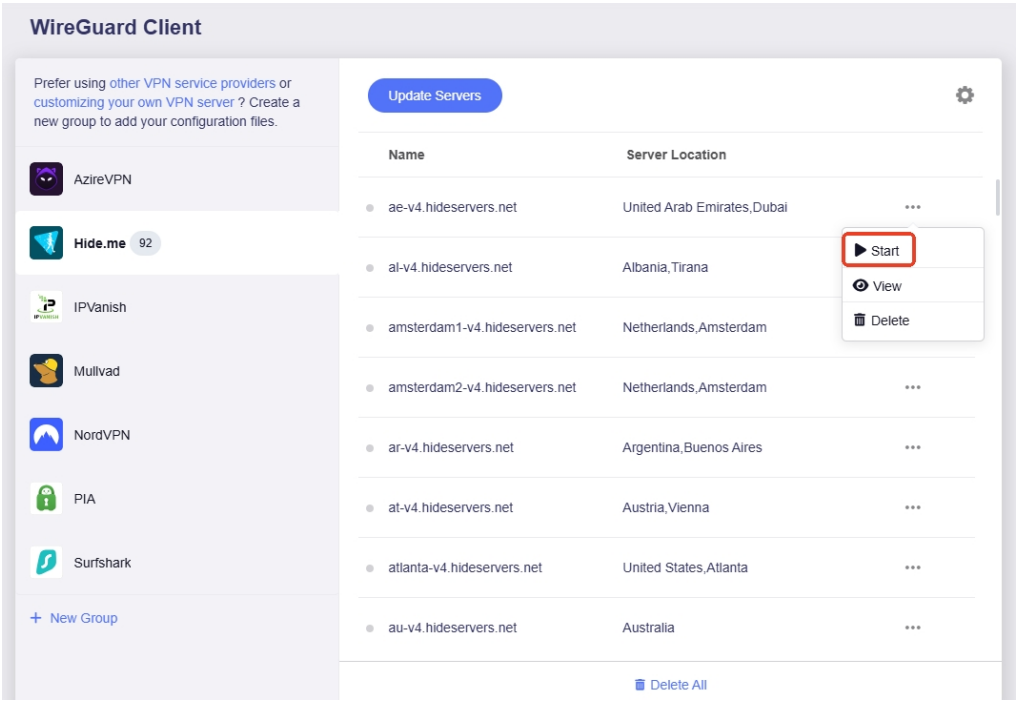
11.2.3 Configurar Hide.me

Siga los pasos a continuación para configurar su enrutador como Hide.me cliente.

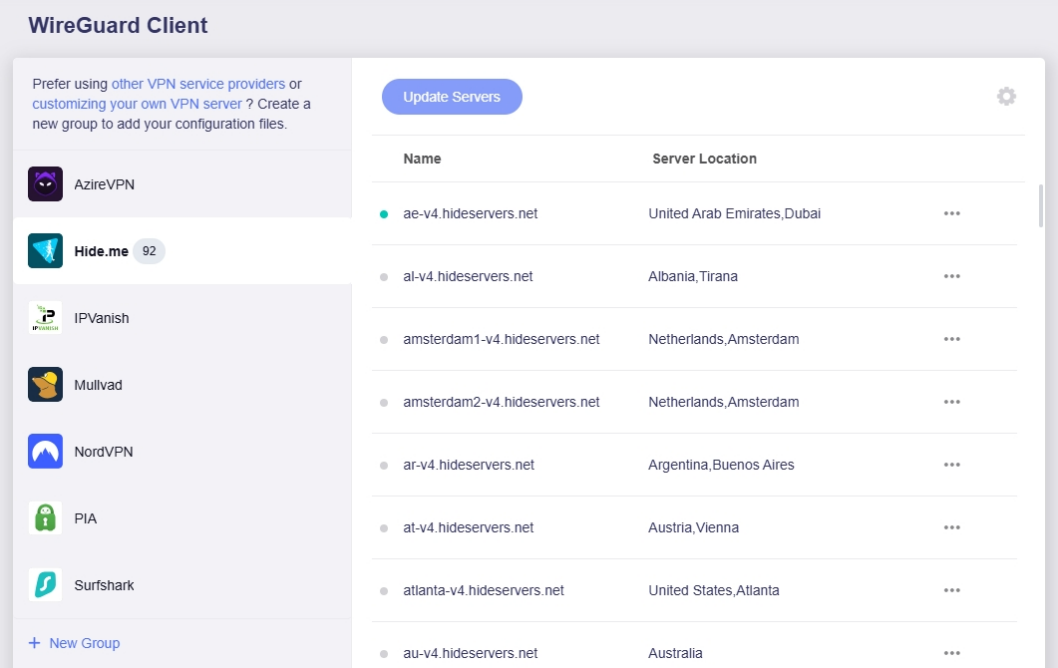
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Hide.me**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



3. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



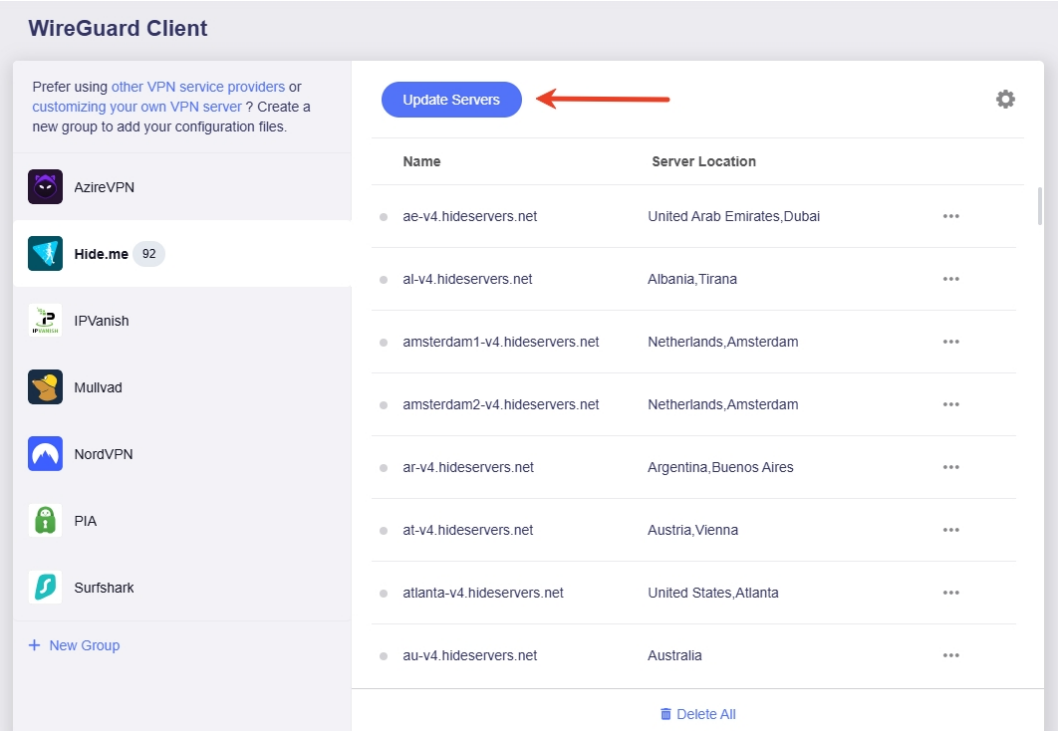
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar los detalles de la conexión VPN en el **Panel de VPN**.

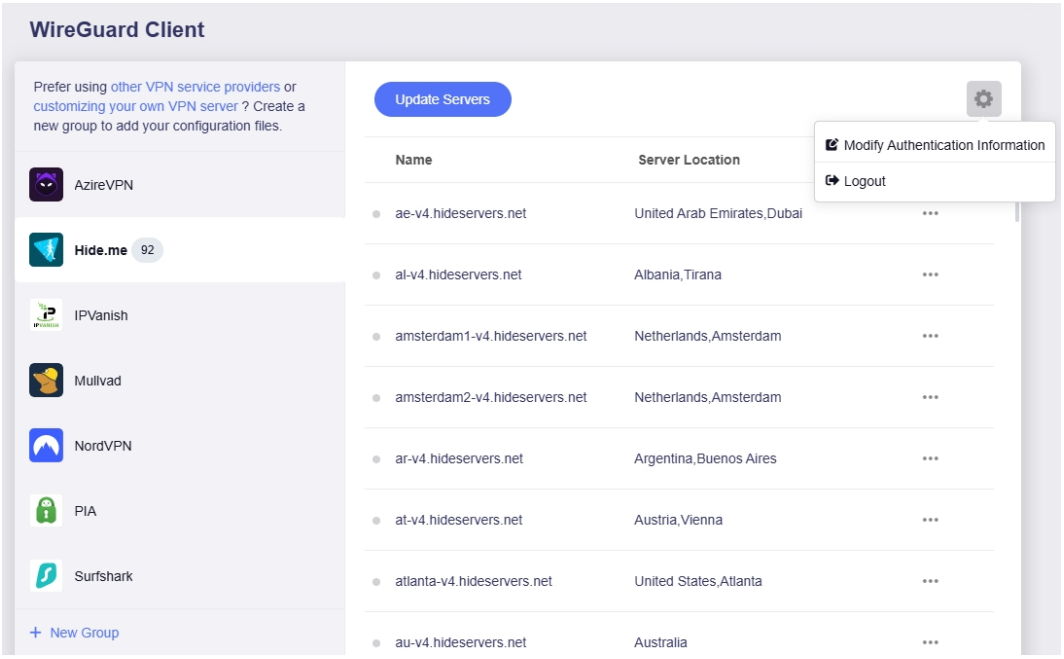
5. Actualizar servidores.

Puedes hacer clic en **Actualice servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



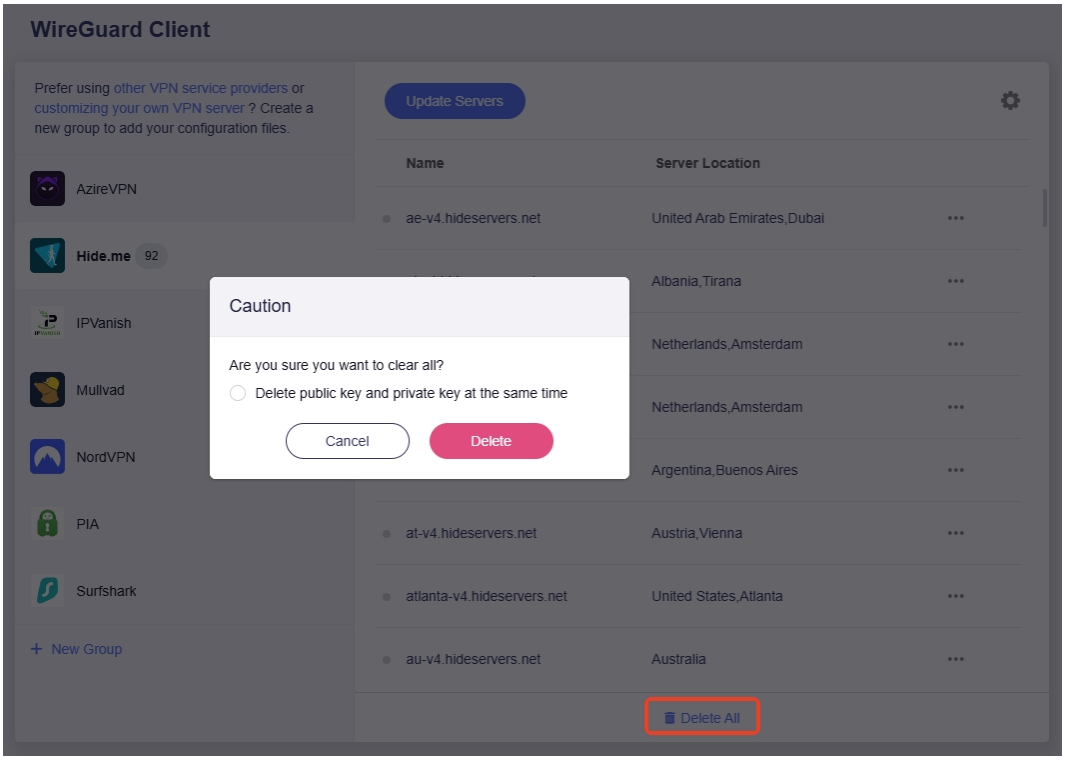
6. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



7. Eliminar todos los archivos.

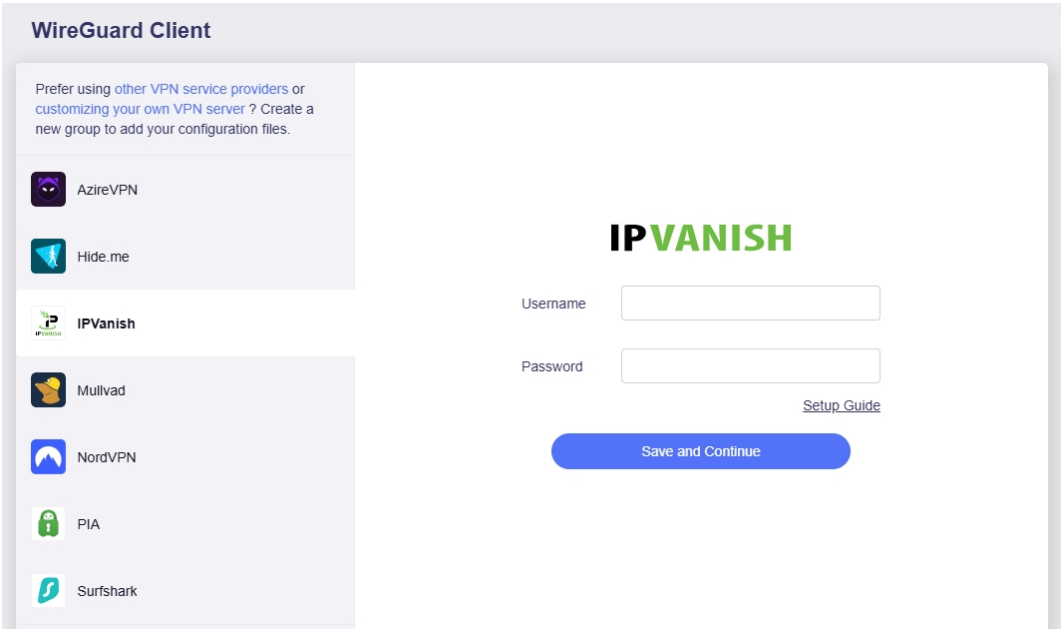
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



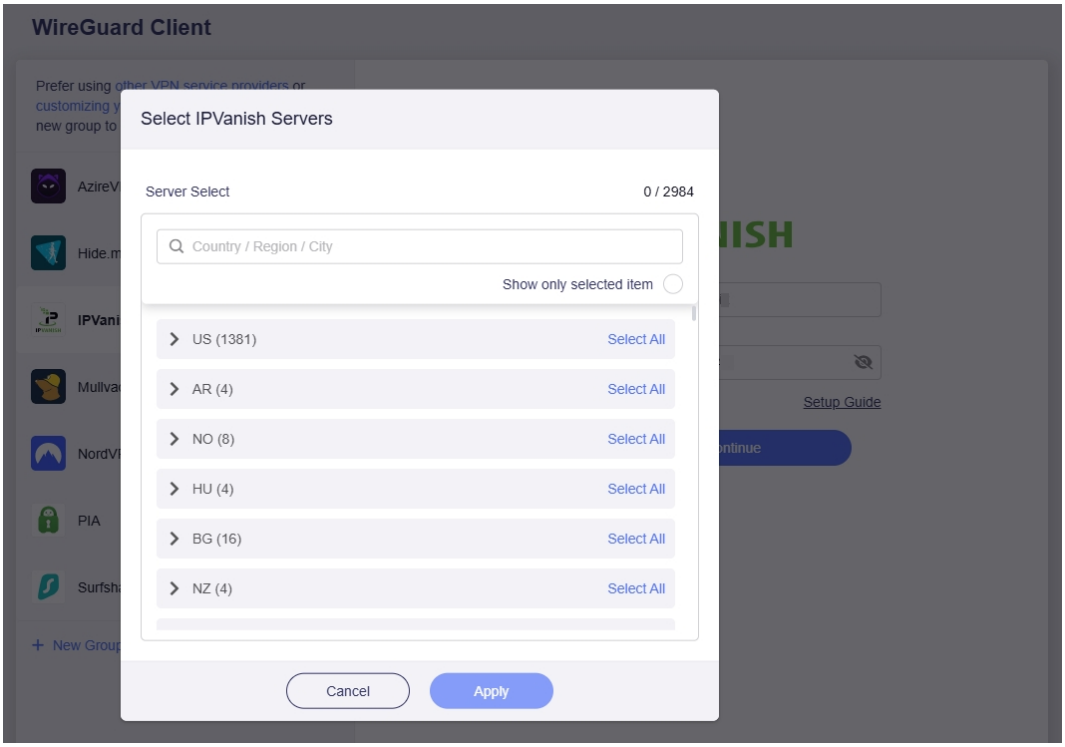
11.2.4 Configurar IPVanish

Siga los pasos a continuación para configurar su enrutador como cliente IPVanish.

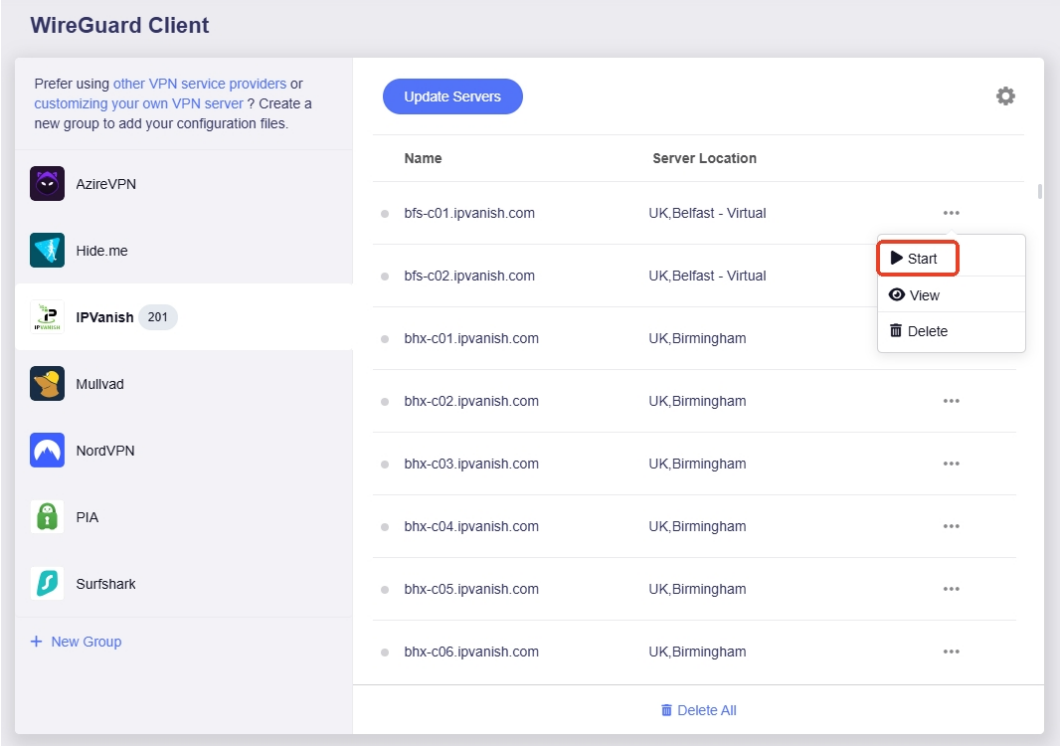
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **IPVanish**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



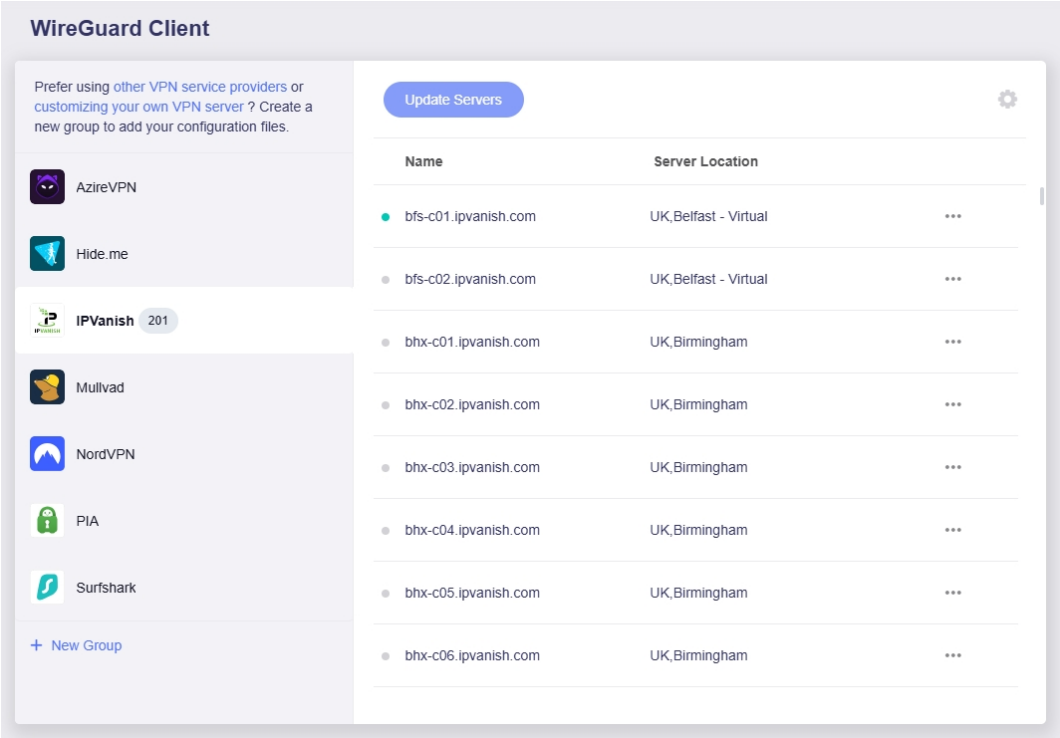
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el ícono de tres puntos a la derecha para iniciar una conexión.



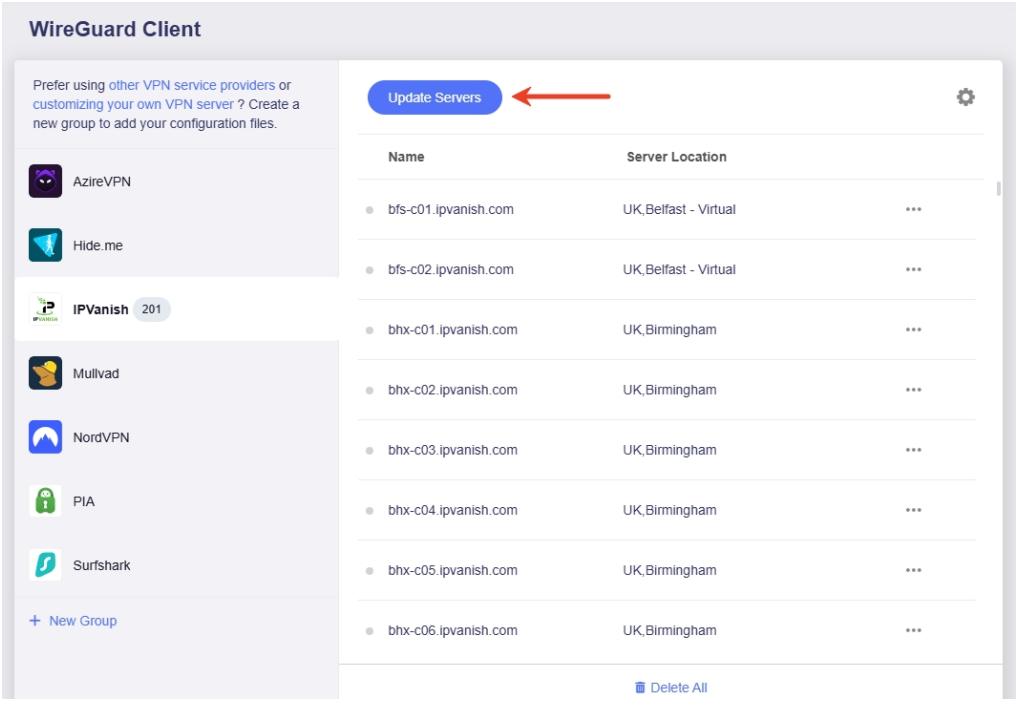
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también comprobar Detalles de la conexión VPN en el **Panel de VPN**.

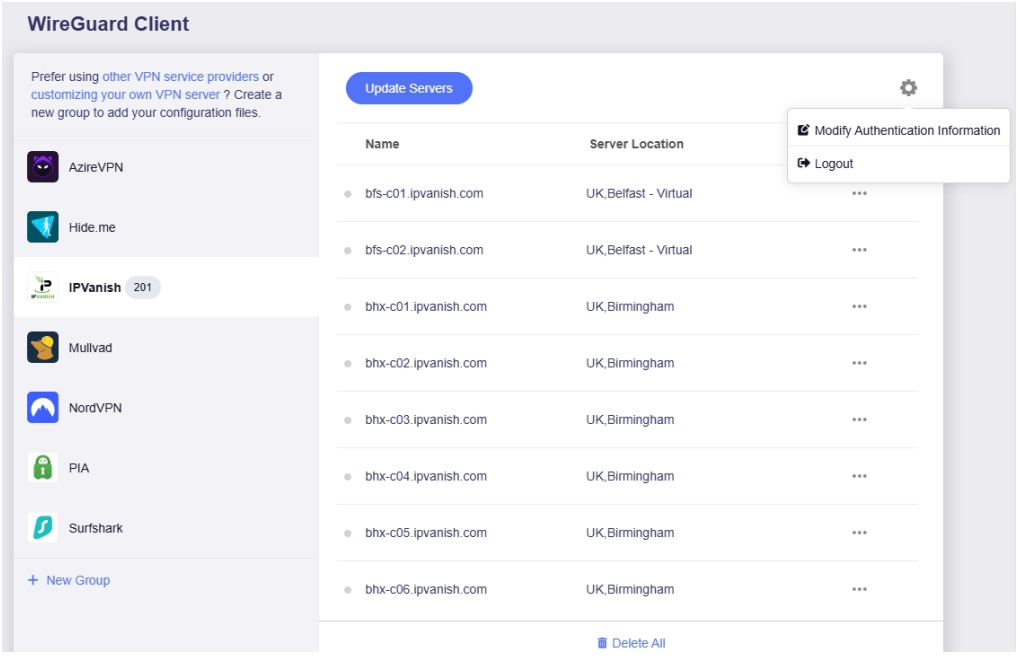
6. Actualizar servidores.

   Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



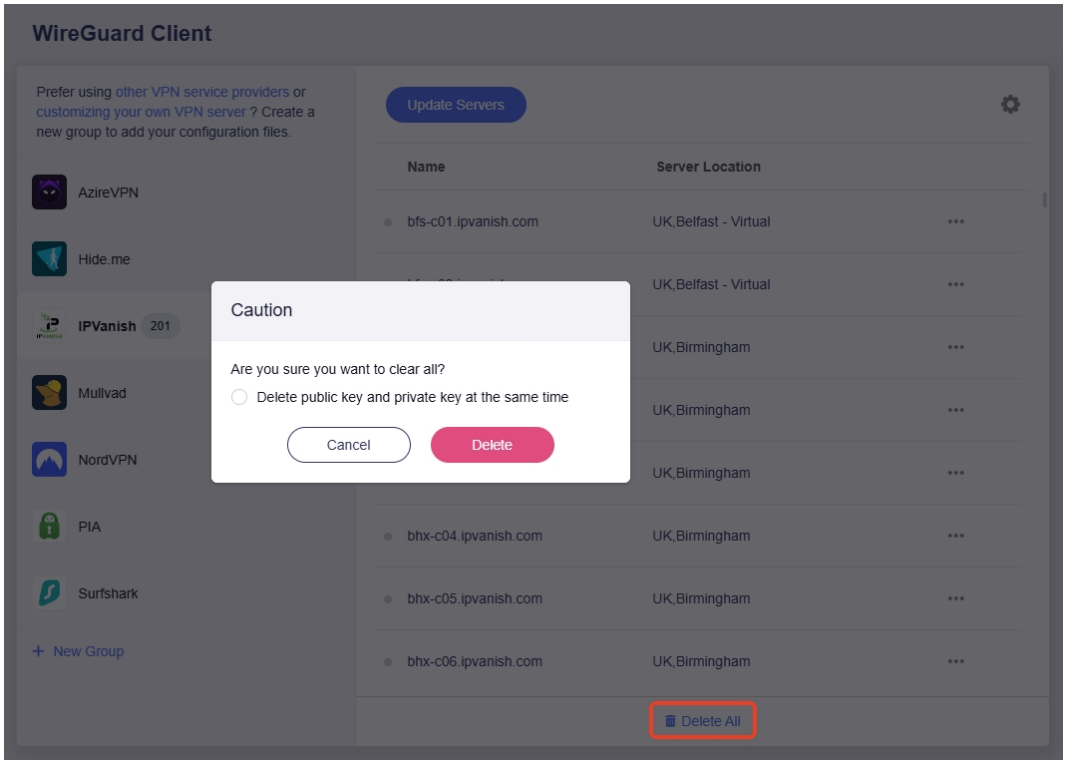
7. Editar credenciales o cerrar sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



8. Eliminar todos los archivos.

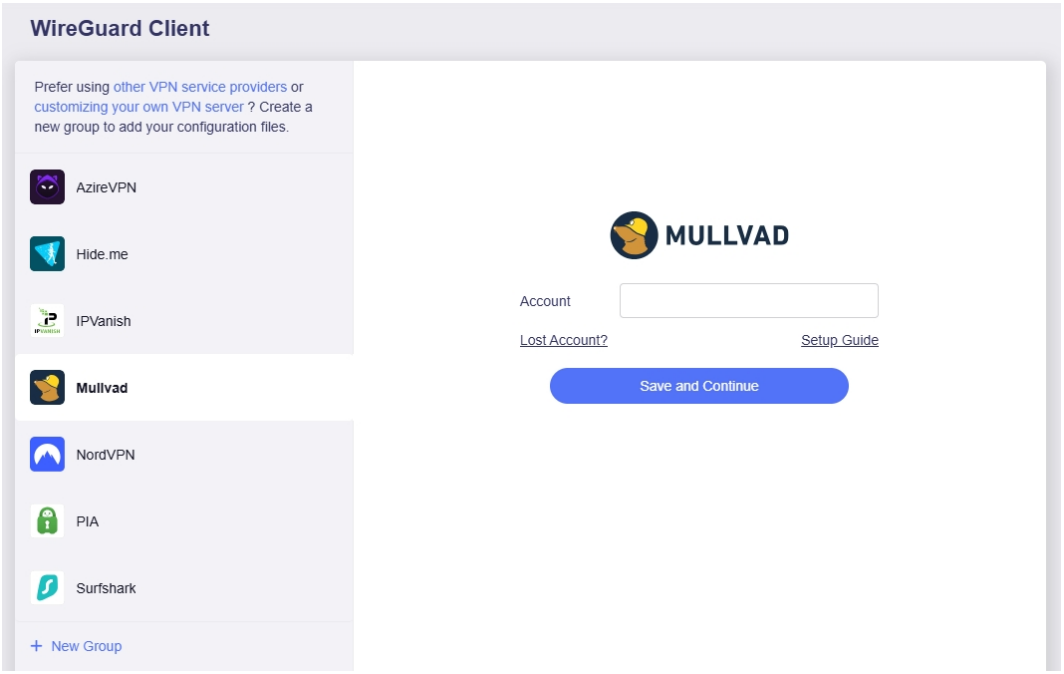
Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



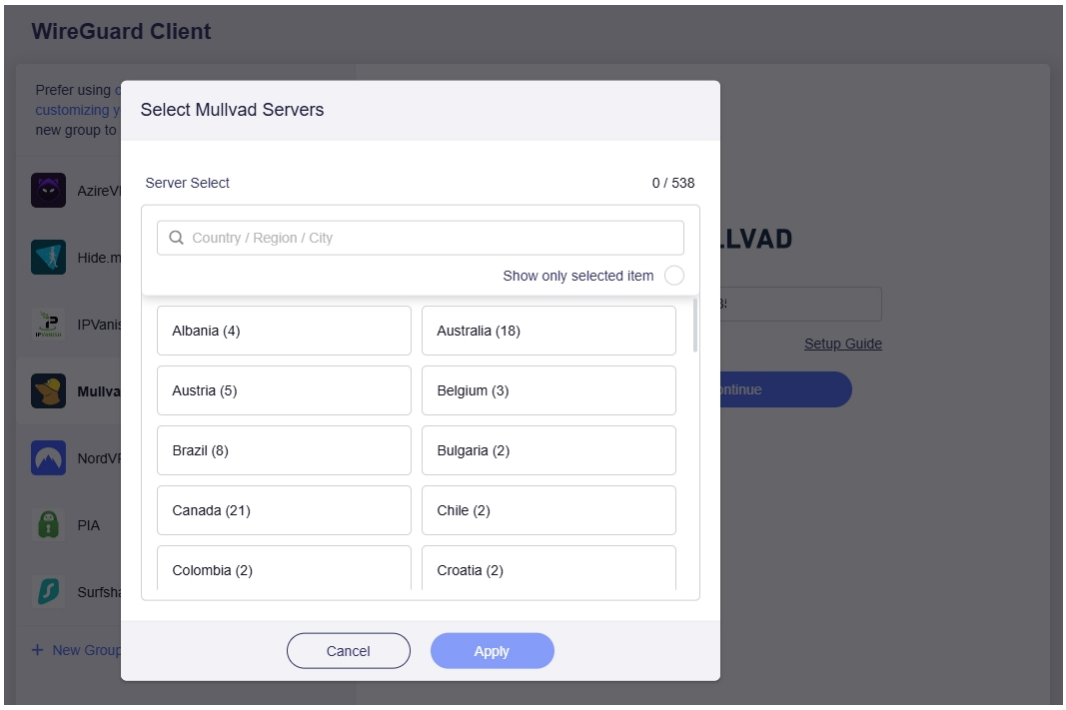
11.2.5 Configurar Mullvad

Siga los pasos a continuación para configurar su enrutador como cliente Mullvad.

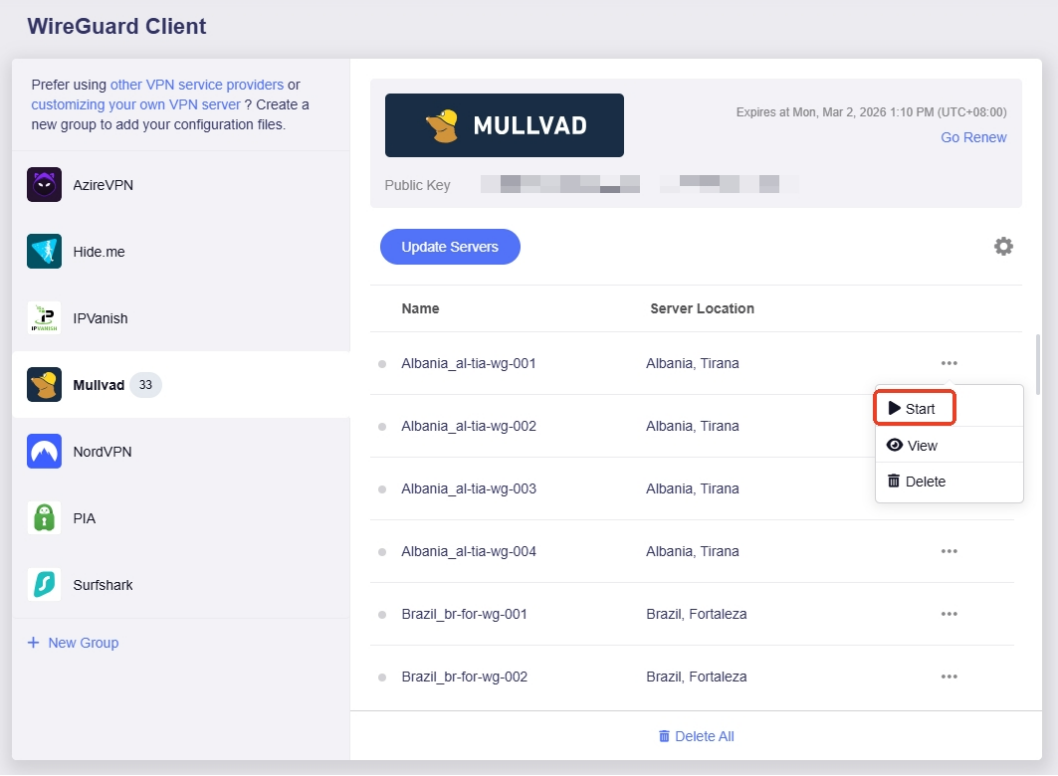
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



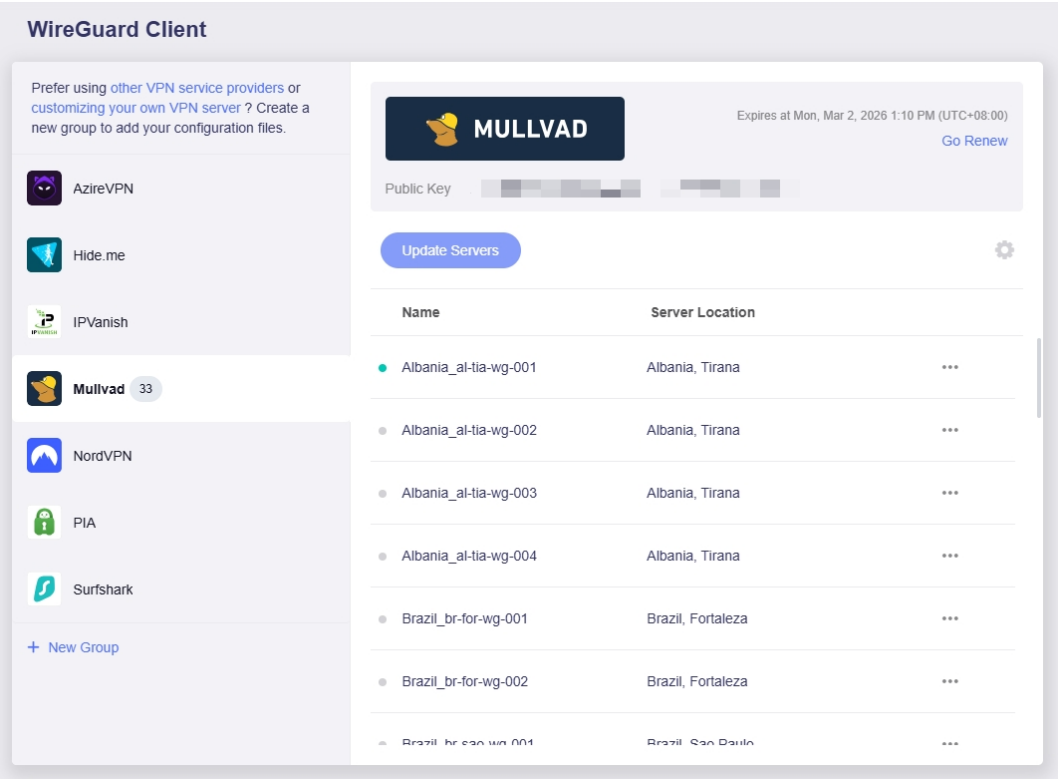
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



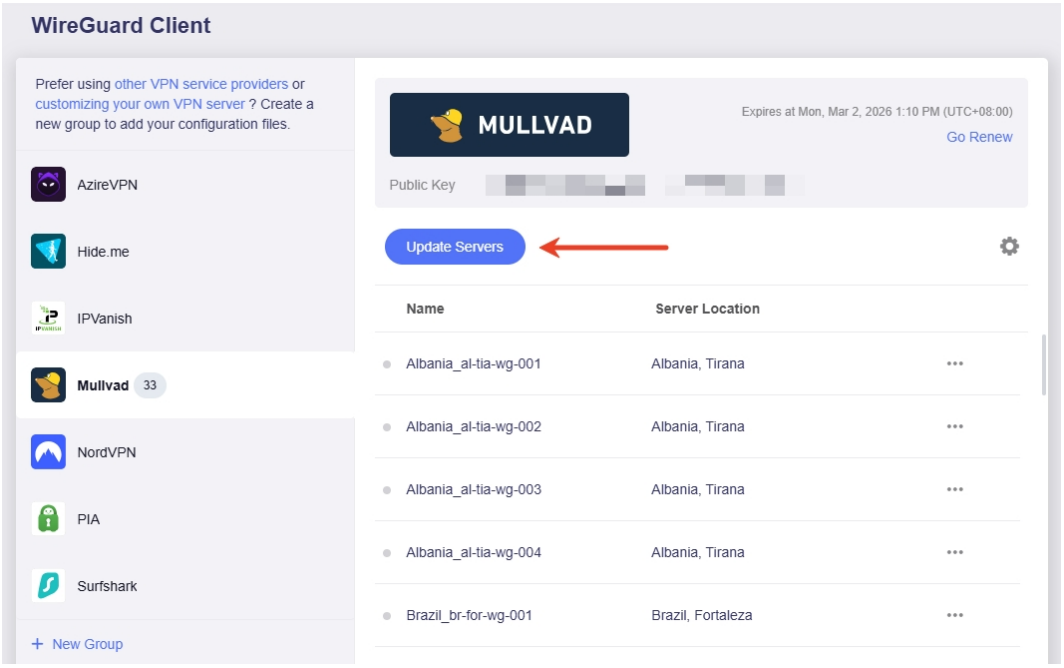
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar los detalles de la conexión VPN en **Panel de VPN**.

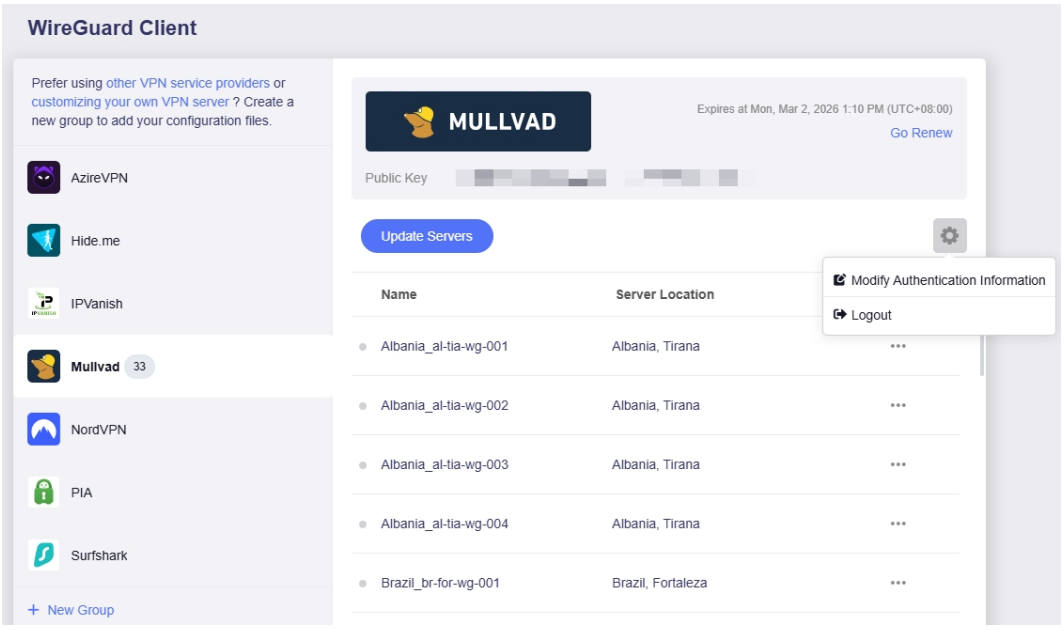
6. Actualizar servidores.

   Puede hacer clic en **Actualizar servidores** para obtener el última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



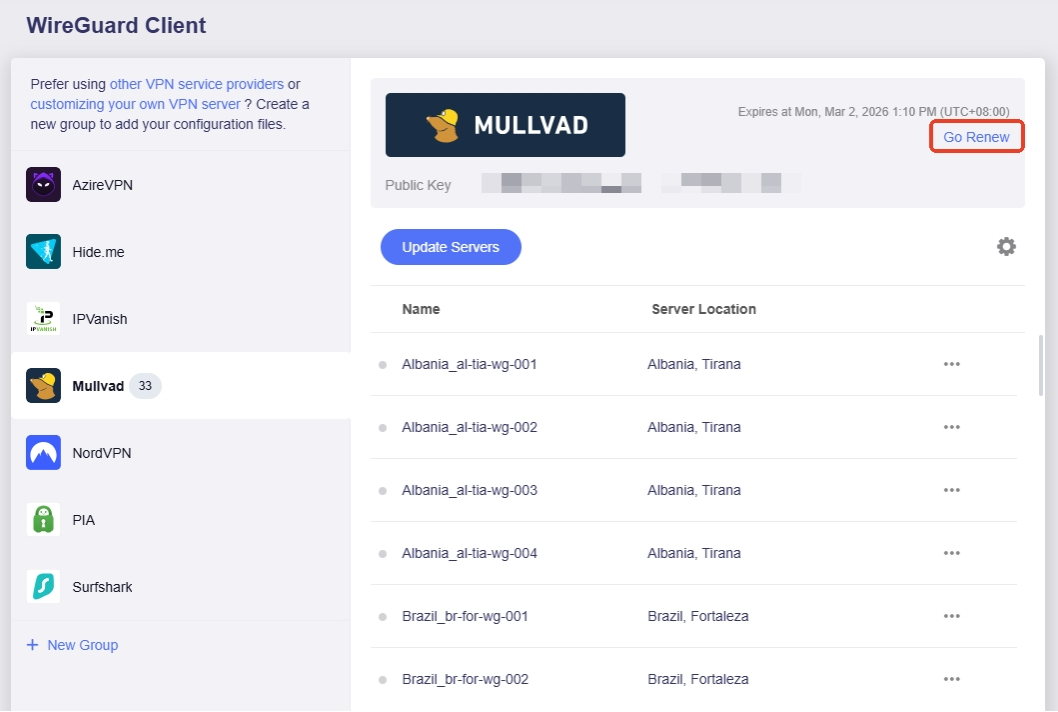
7. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



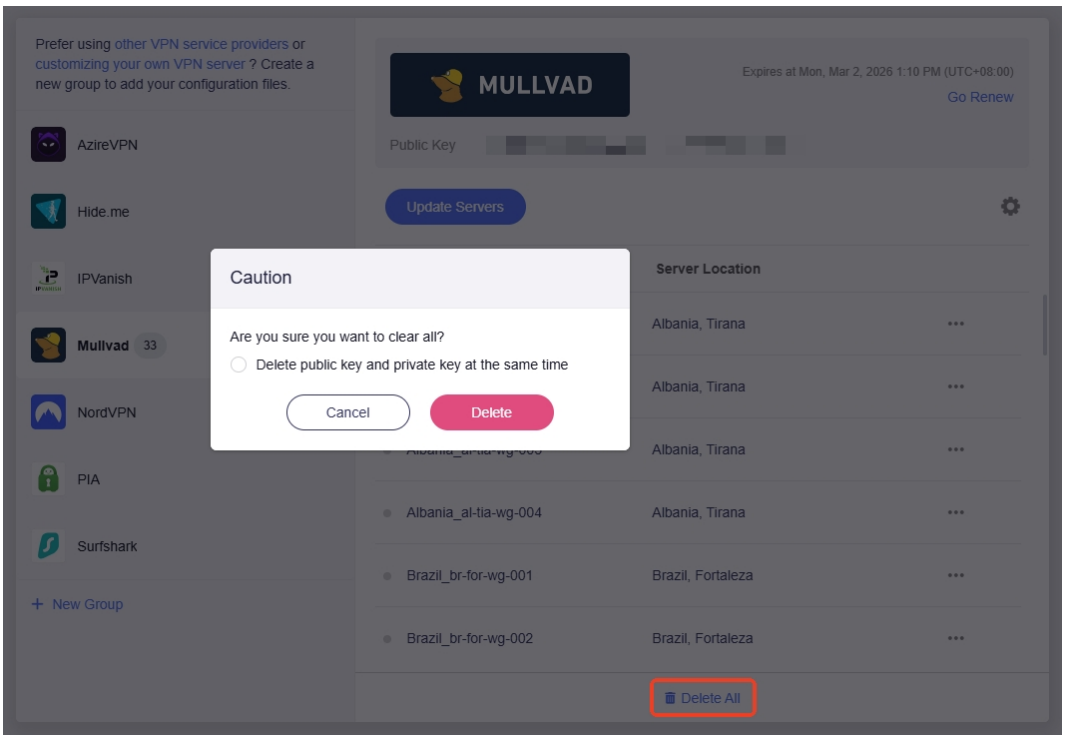
8. Vaya a renovar.

   Si haces clic en **Ir a renovar**, serás redirigido al sitio web oficial para renovar tu suscripción.



9. Eliminar todos los archivos.

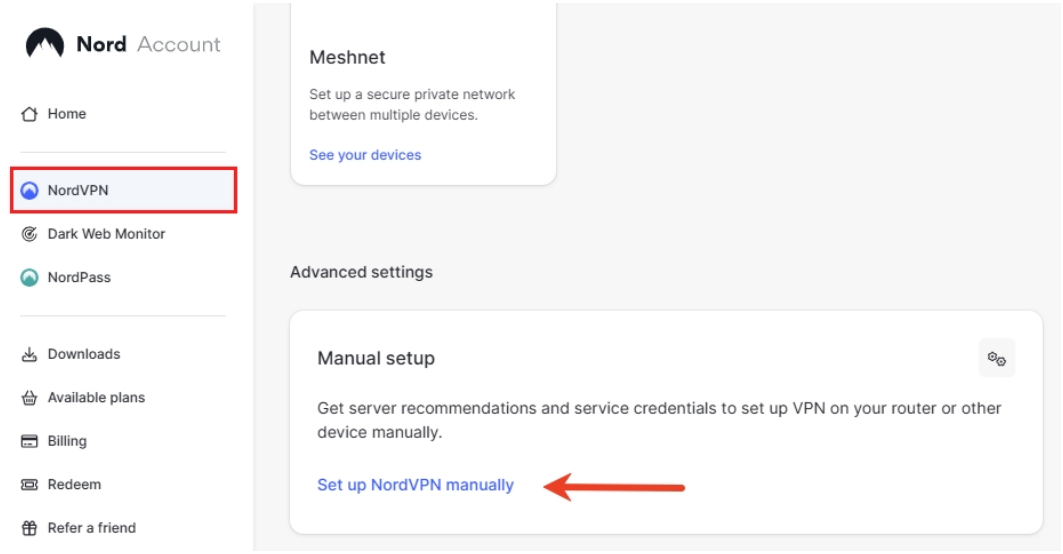
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



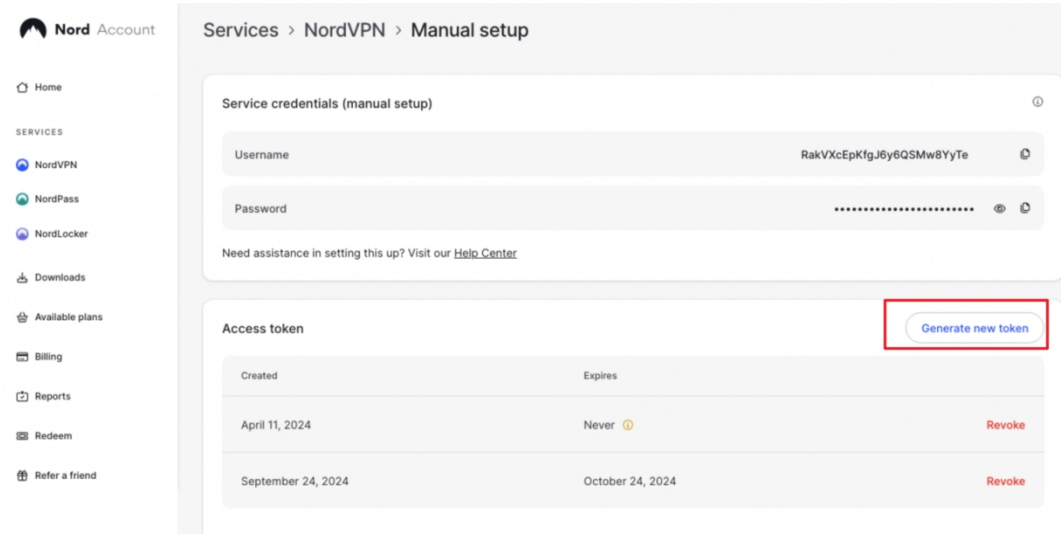
11.2.6 Configurar NordVPN

Siga los pasos a continuación para configurar su enrutador como cliente NordVPN.

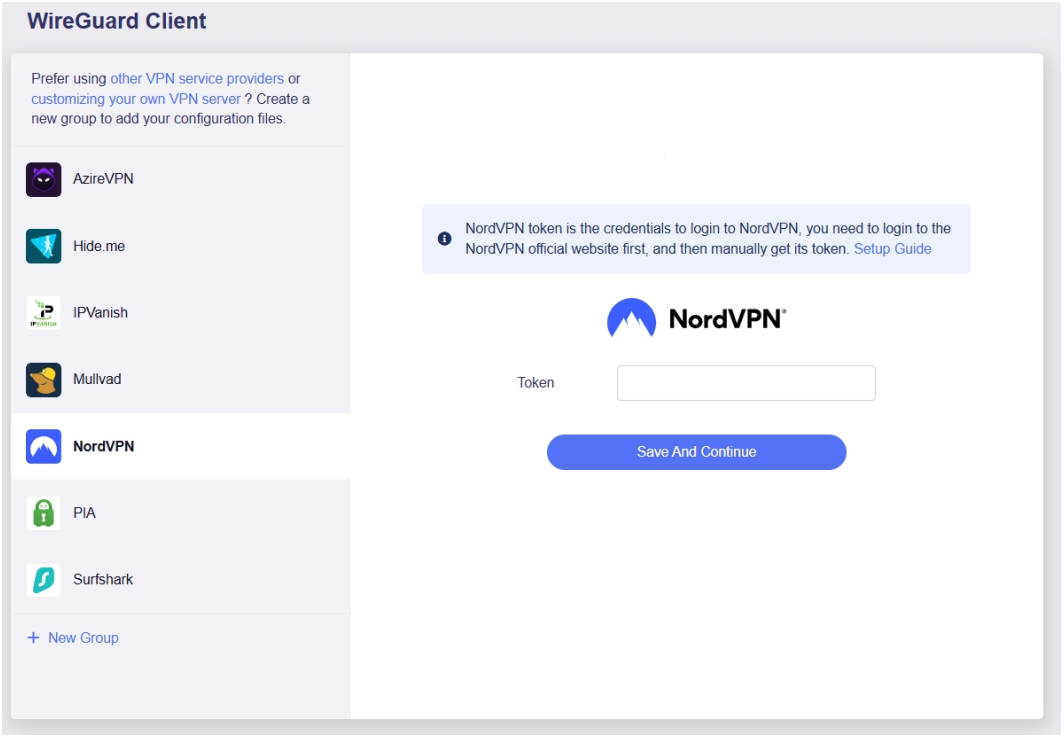
1. Inicie sesión en su sitio web NordVPN cuenta aquí.
2. Oen el Panel de Nord, haga clic en **NordVPN** y luego haga clic en **Configure NordVPN manualmente**.



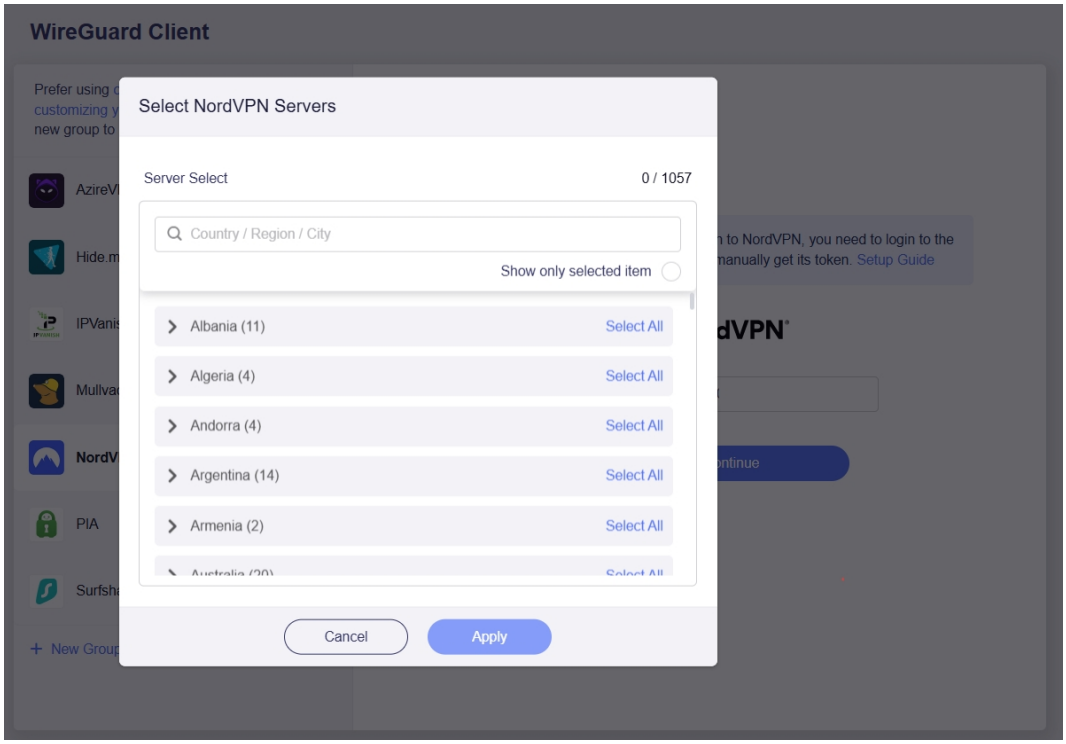
Encontrará el **Token de acceso**. Cree un token de acceso y ccopia para uso posterior.



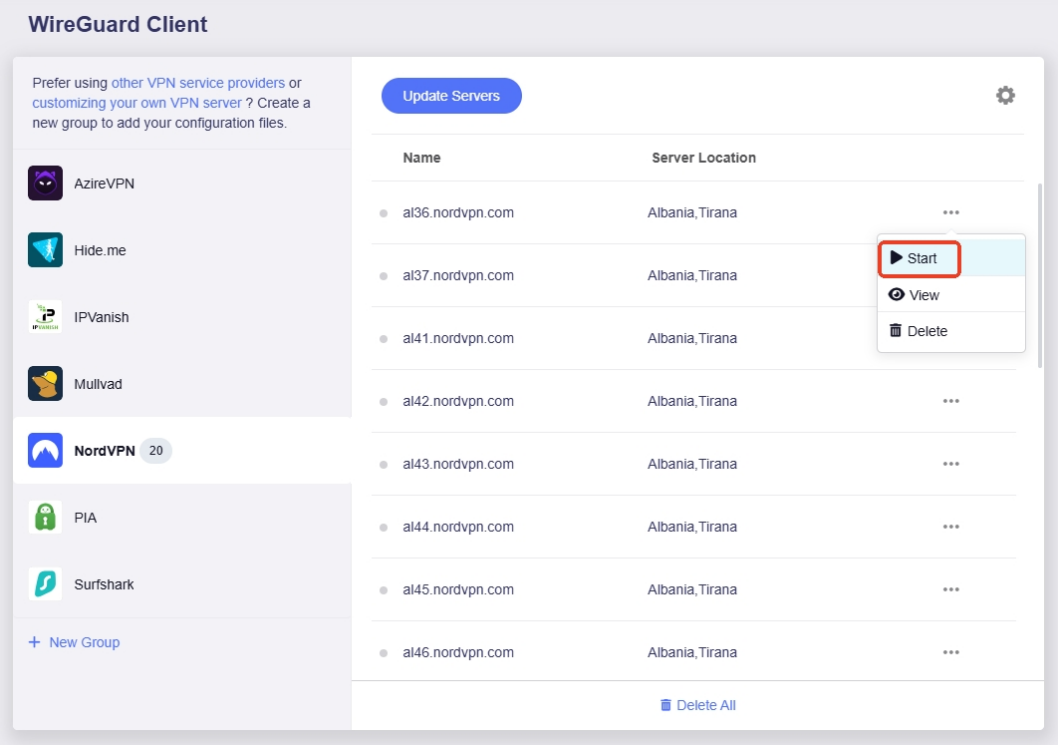
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Entrada token, y haga clic en **Guardar y continuar**.



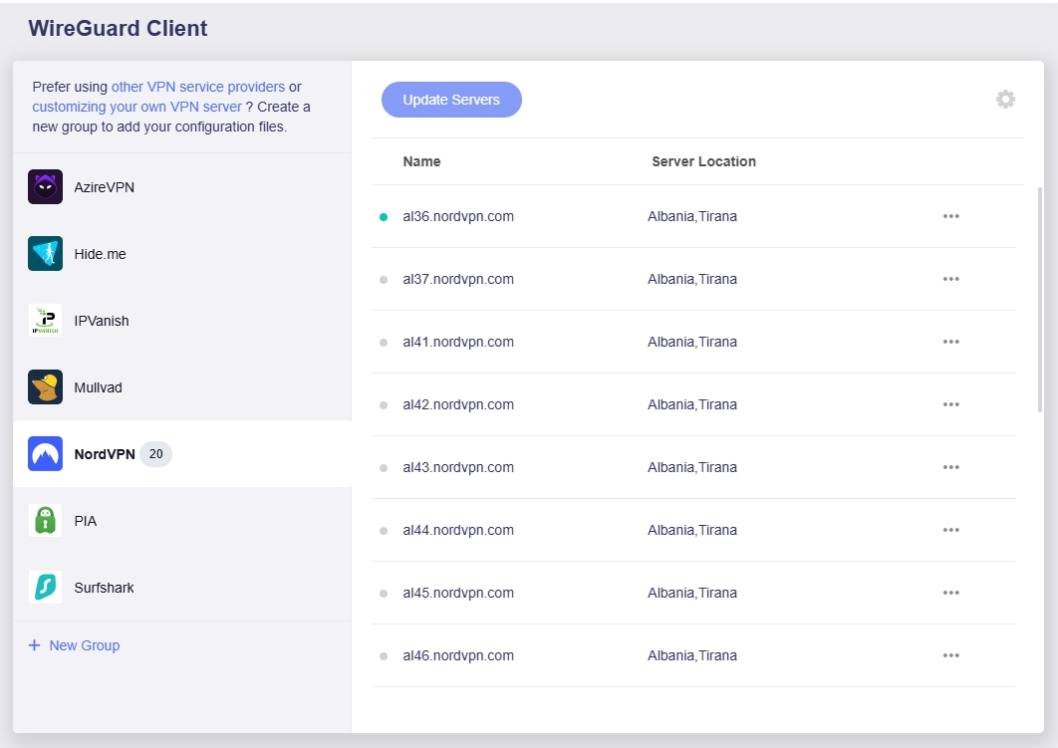
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



6. Seleccione un servidor preferido y haga clic en el ícono de tres puntos a la derecha para iniciar una conexión.



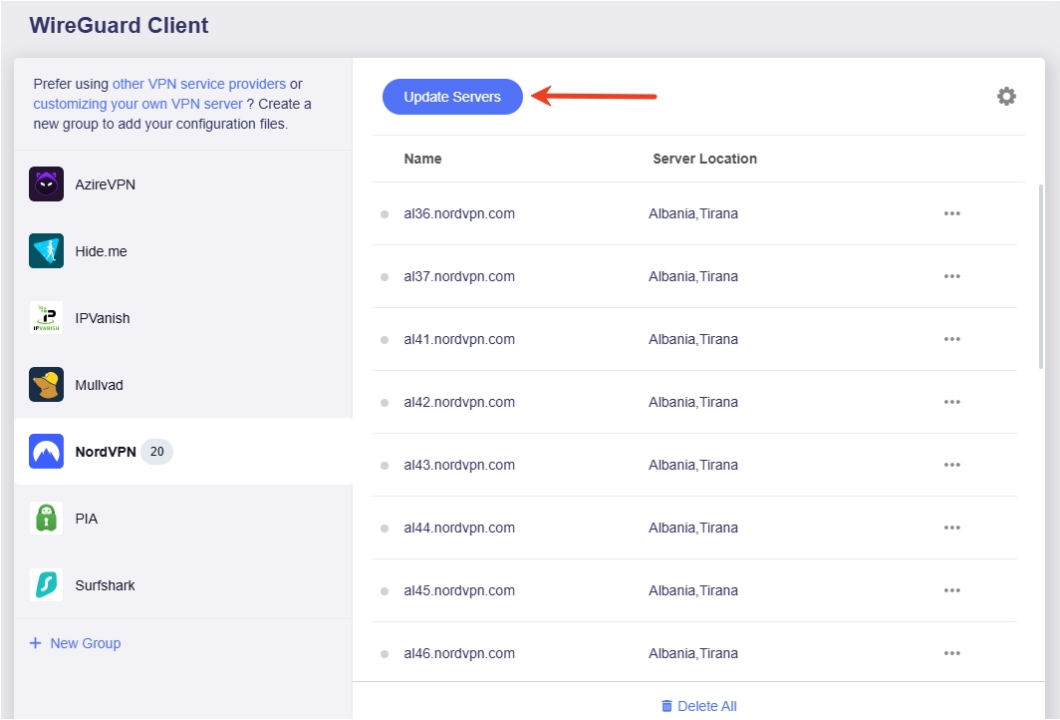
7. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar los detalles de la conexión VPN en **Panel de VPN**.

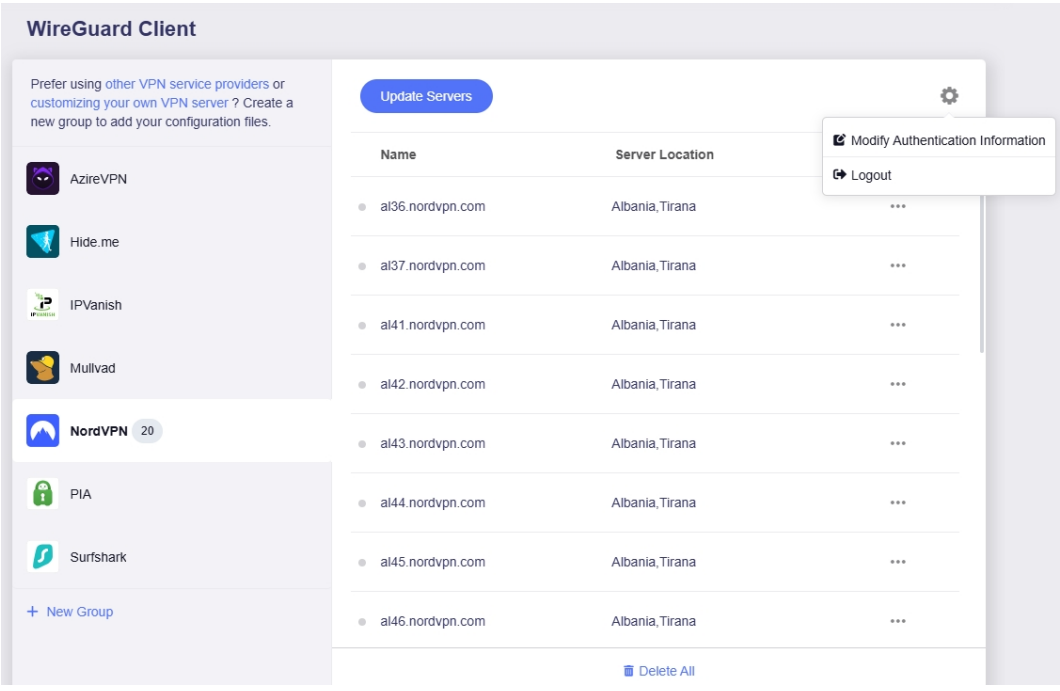
8. Actualizar servidores.

Puede hacer clic en **Actualizar servidores** para obtener el última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



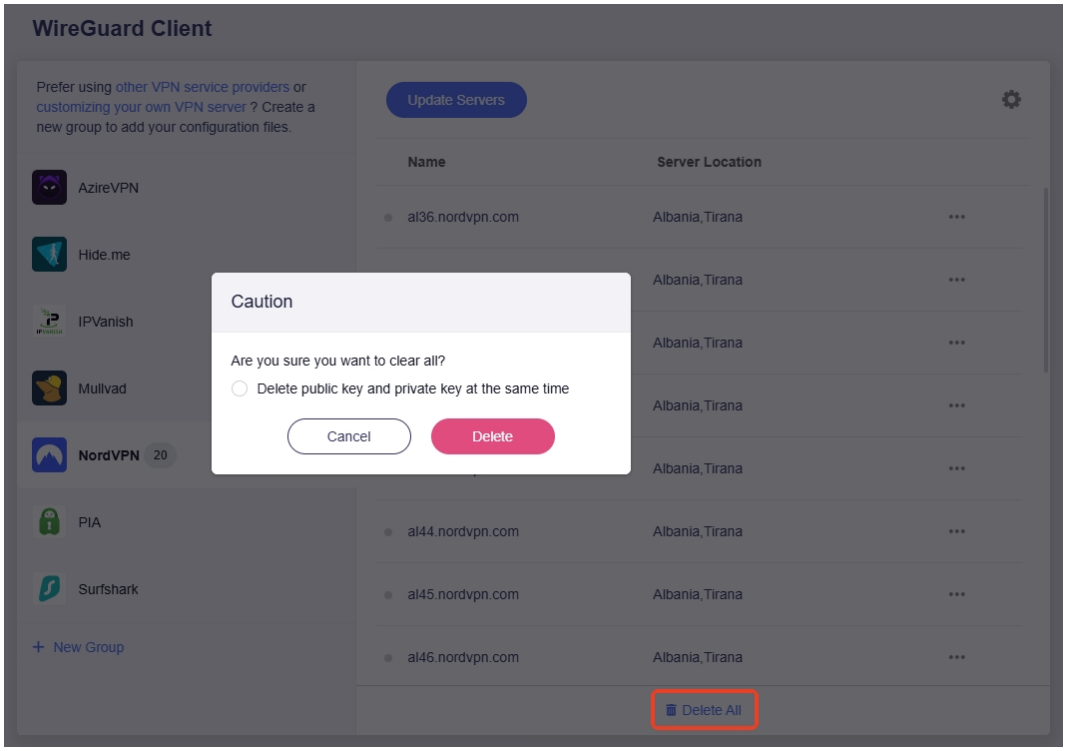
9. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



10. Eliminar todos los archivos.

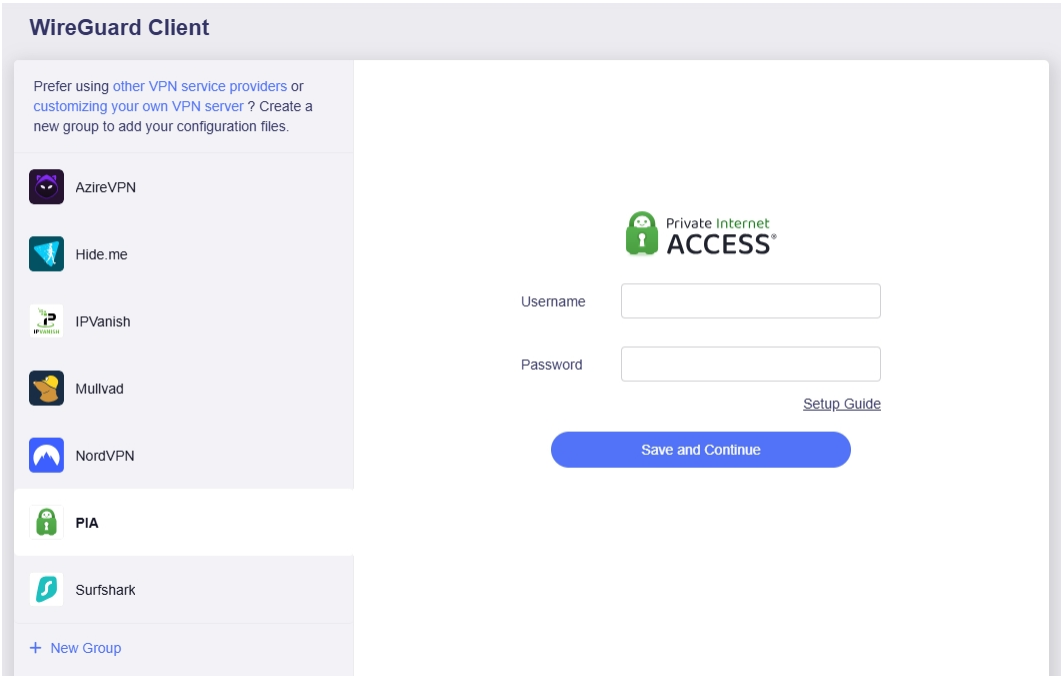
    Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar los archivos privados y públicos. claves simultáneamente.



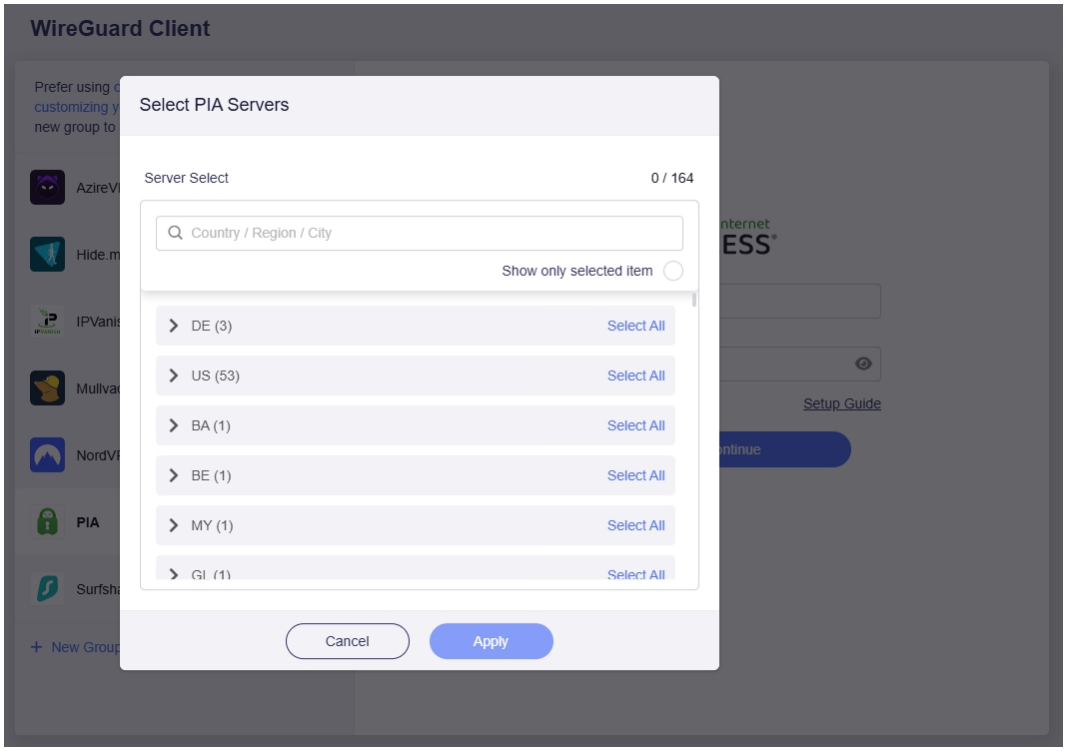
11.2.7 Configurar PIA (Private Internet Access)

Siga los pasos a continuación para configurar su enrutador como cliente PIA.

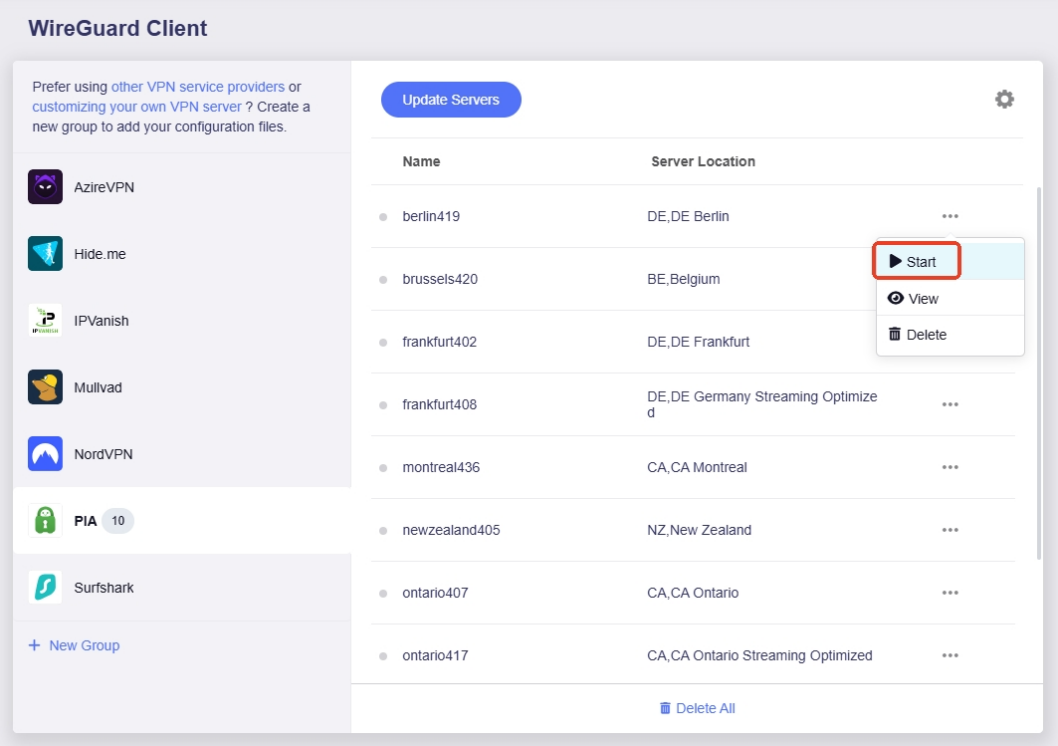
1. Registro in a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



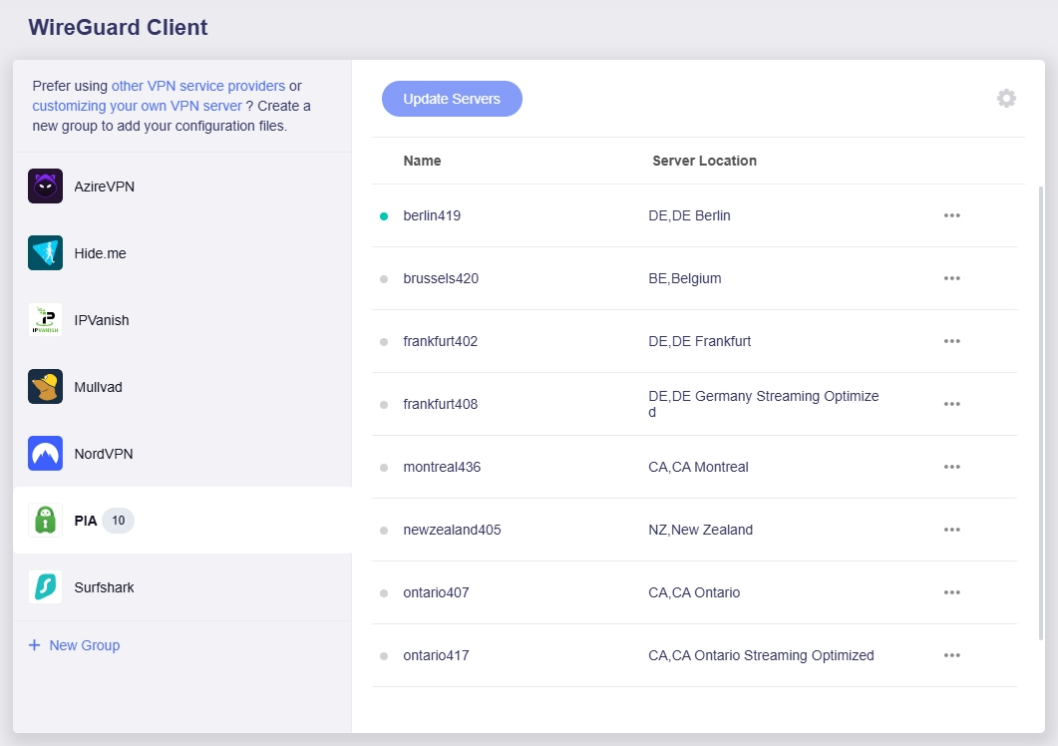
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



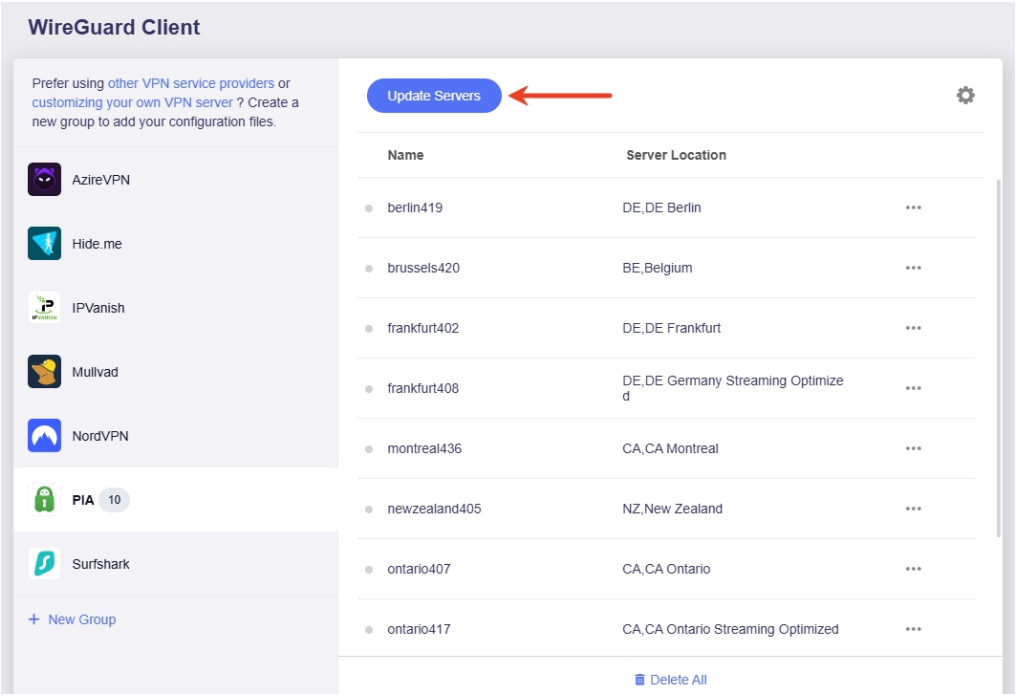
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar los detalles de la conexión VPN en **Panel de VPN**.

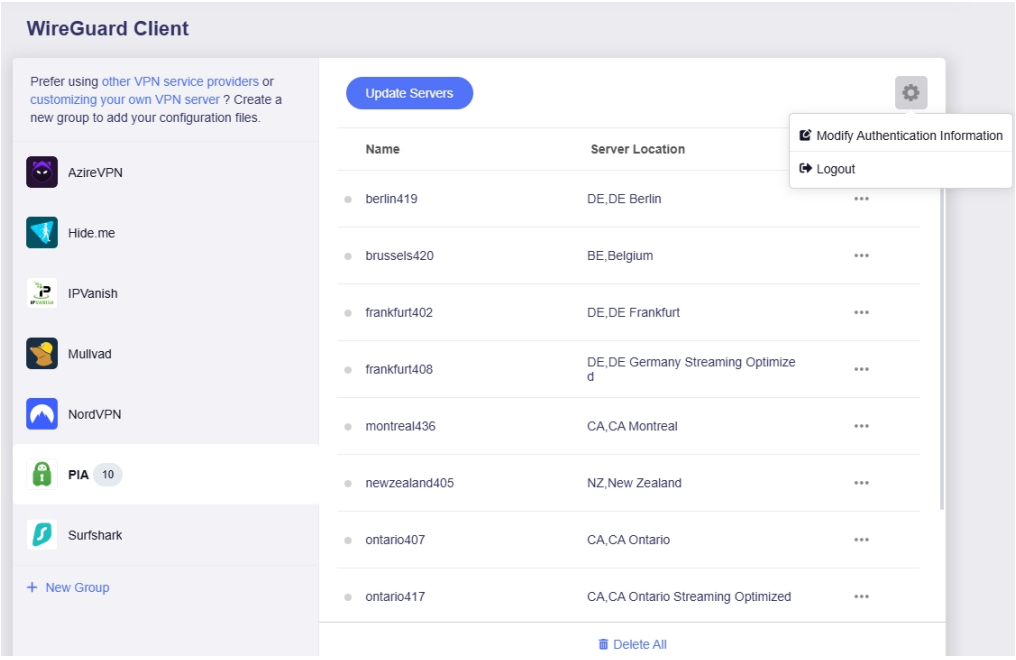
6. Actualizar servidores.

   Puedes hacer clic en **Actualizar Servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



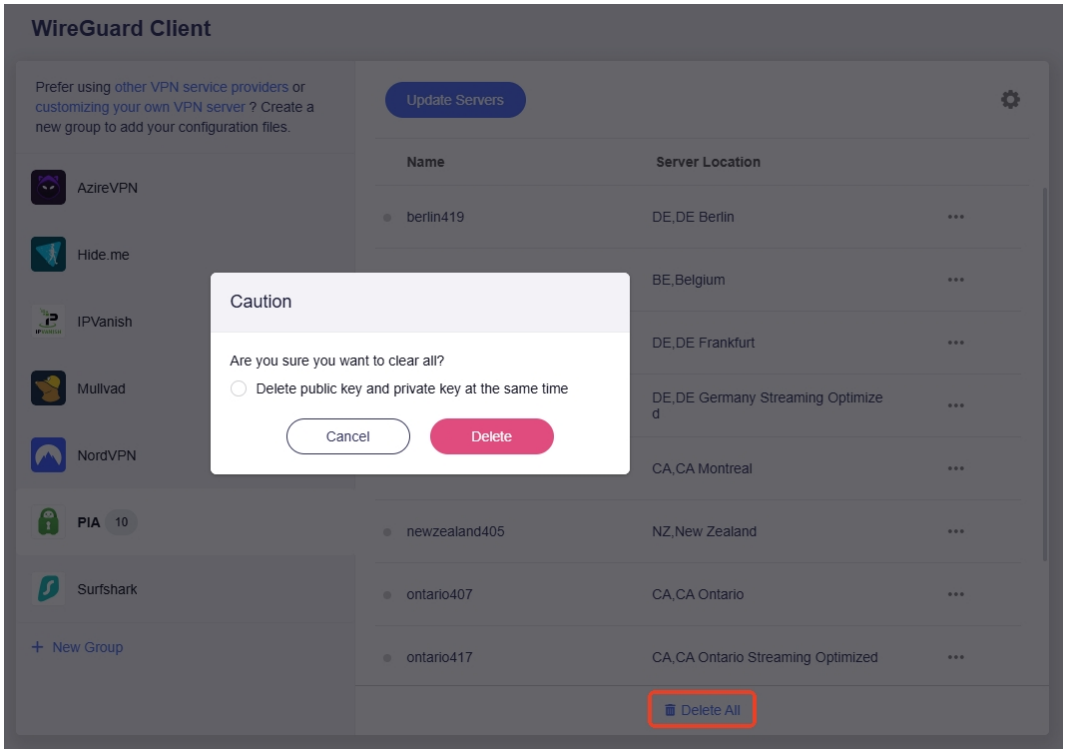
7. Edite las credenciales o cierre la sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o el registro out.



8. Eliminar todos los archivos.

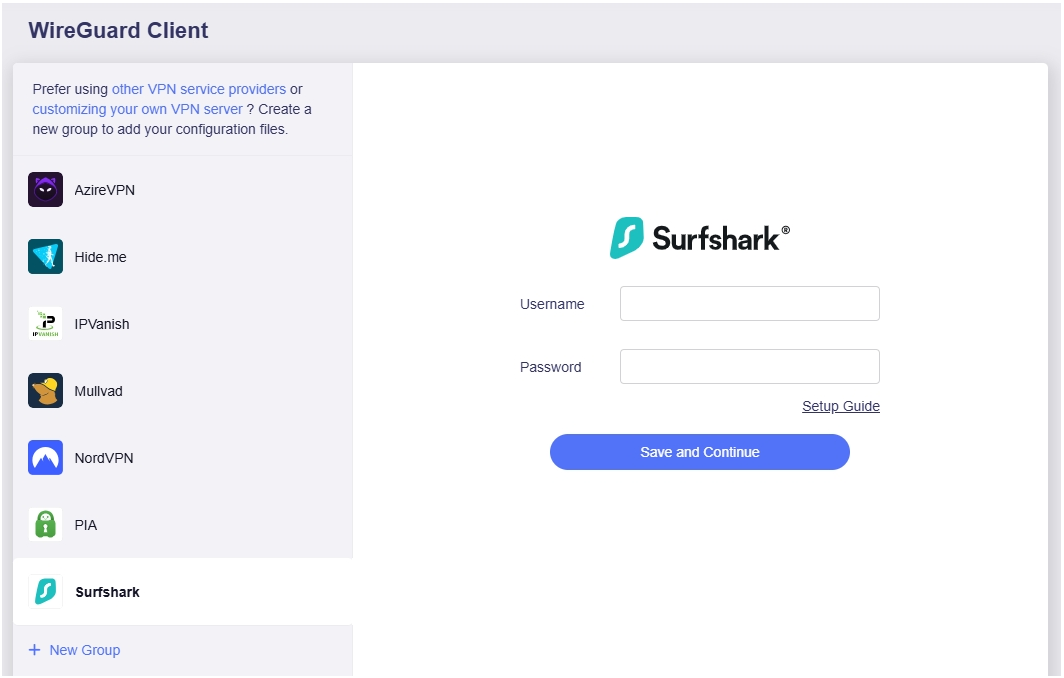
Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



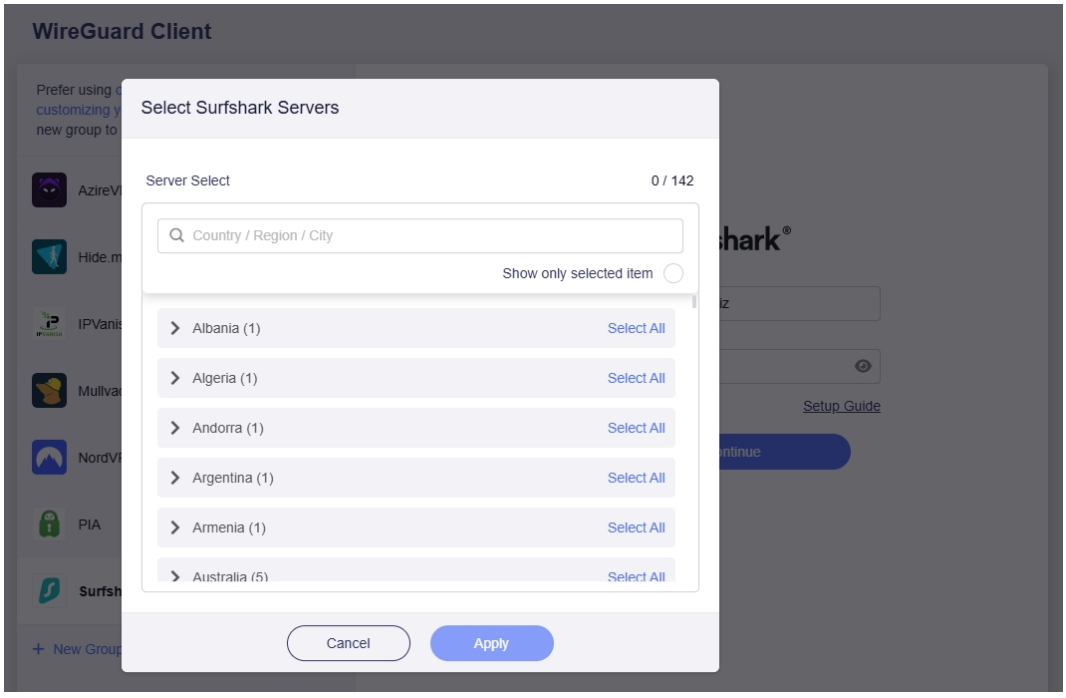
11.2.8 Configurar Surfshark

Siga los pasos a continuación para configurar su enrutador como cliente Surfshark.

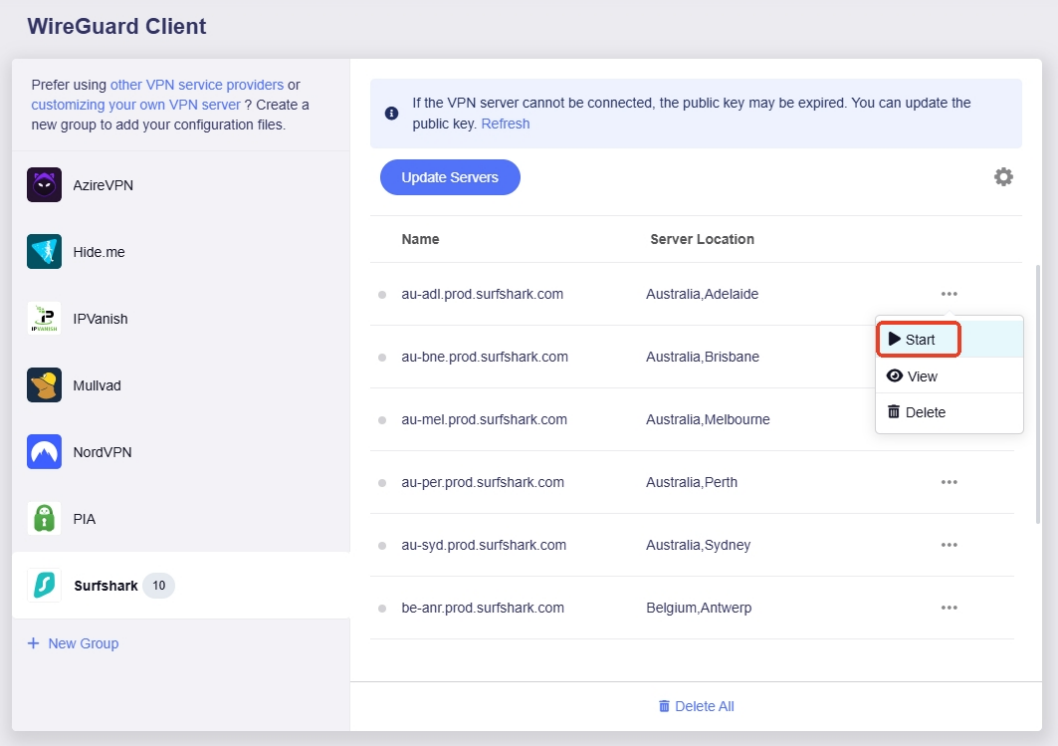
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Surfshark**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



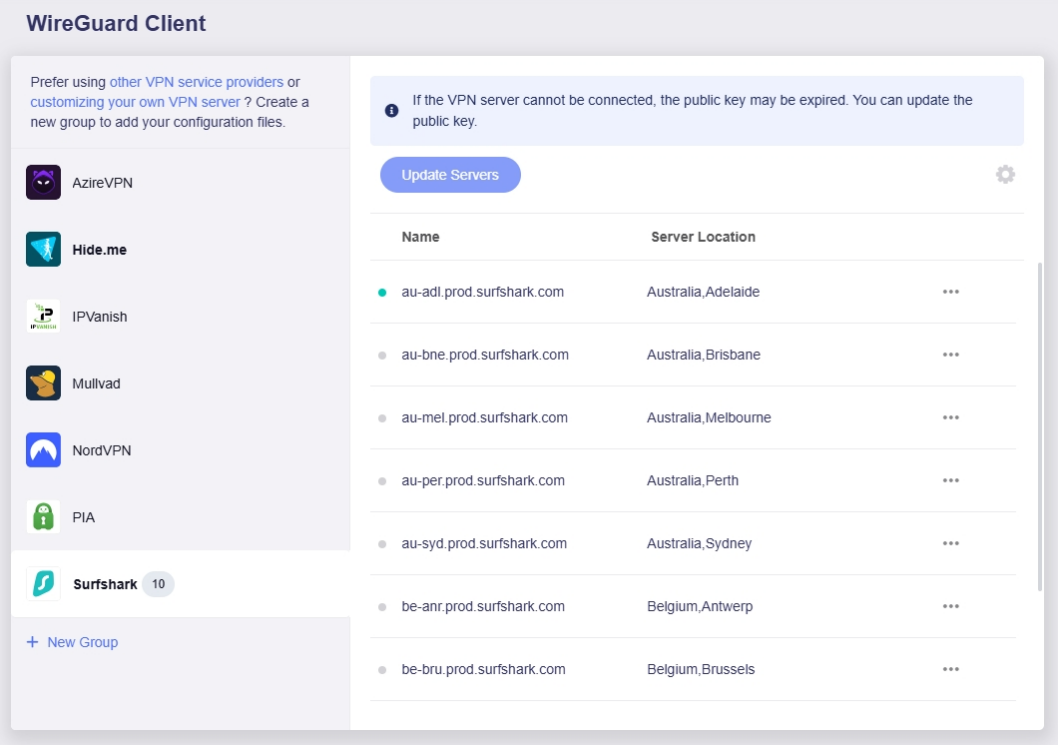
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el ícono de tres puntos a la derecha para iniciar una conexión.



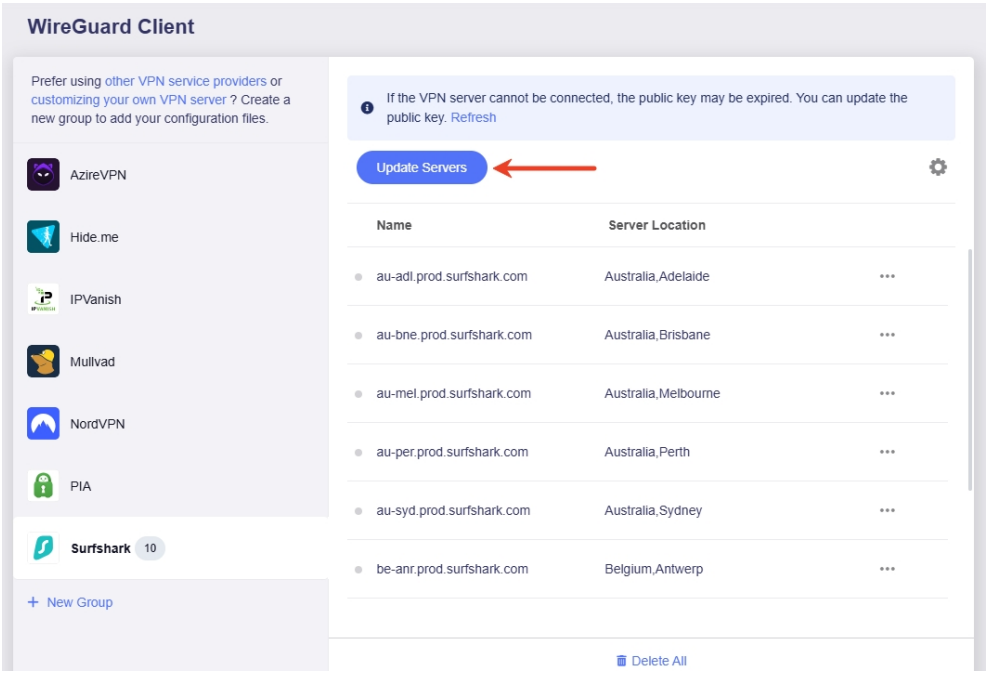
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Usted puede también verificar el Detalles de la conexión VPN en el **Panel de VPN**.

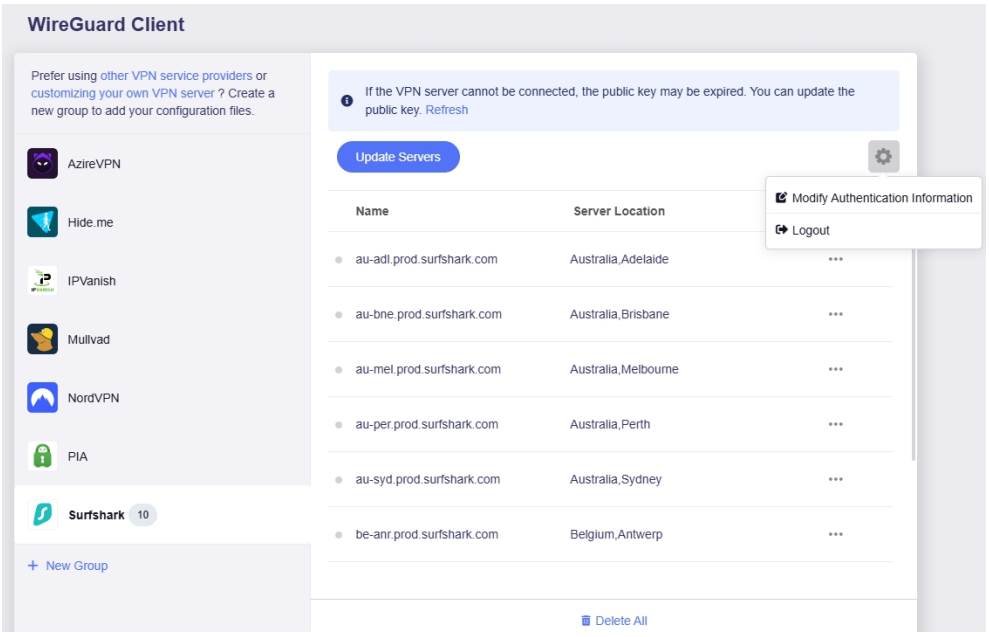
6. Actualizar servidores.

   Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



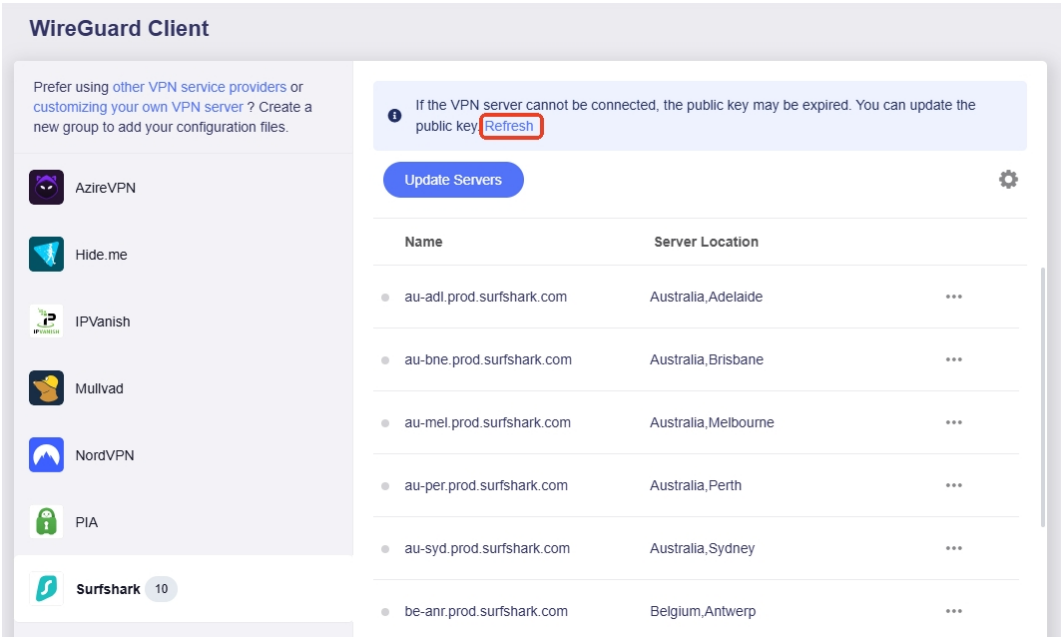
7. Editar credenciales o cerrar sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



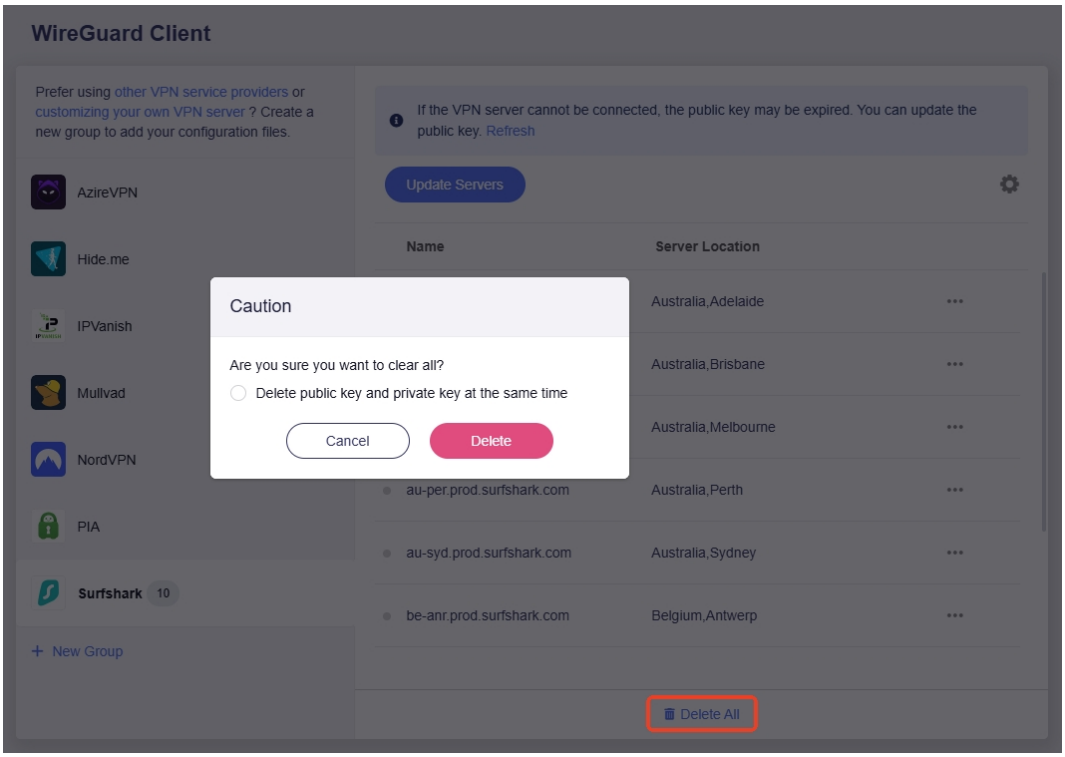
8. Actualizar.

   Puede hacer clic en **Actualizar** para actualizar la clave pública cuando el servidor VPN no se puede conectar.



9. Eliminar todos los archivos.

   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.

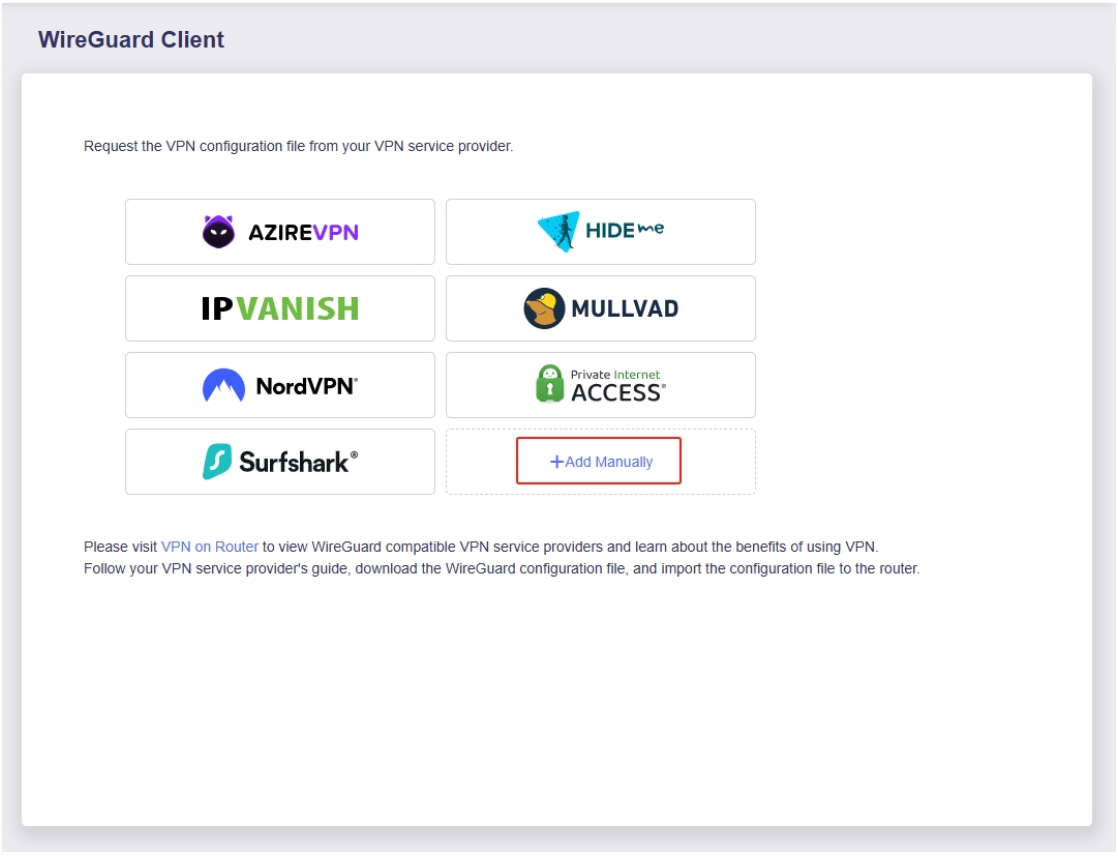


11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

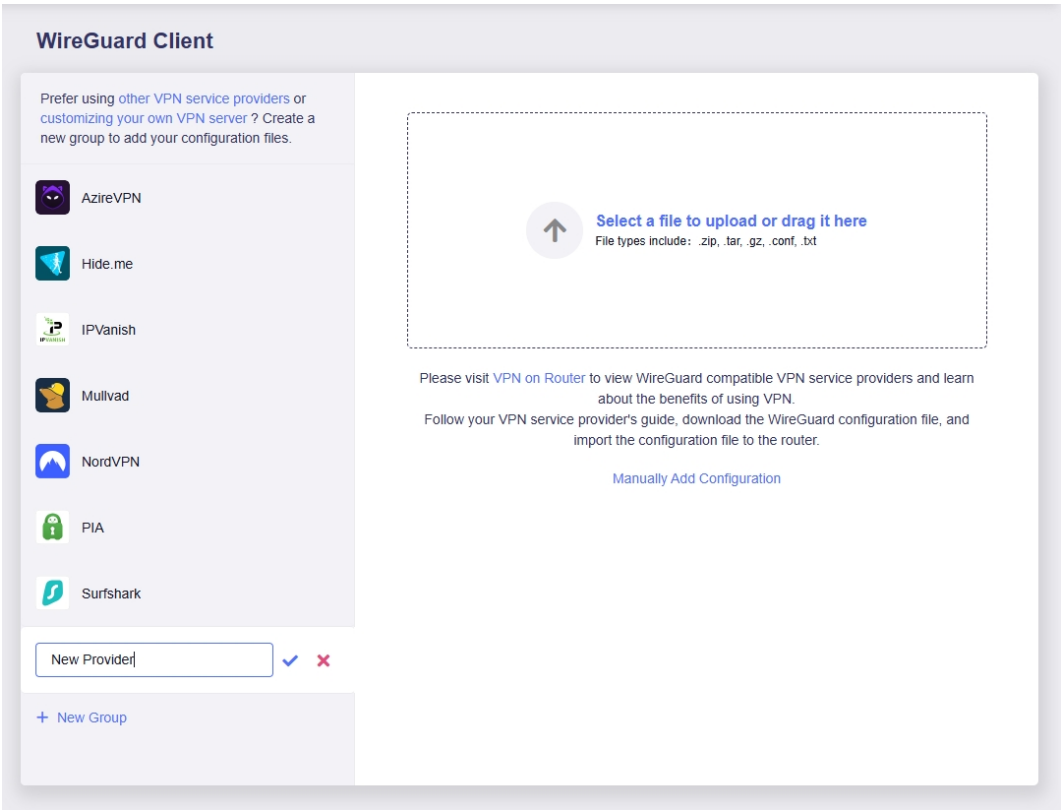
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar los archivos de configuración, consulta esta guía o ponte en contacto con su soporte.

A continuación se detallan los pasos para cargar el archivo de configuración al enrutador para configurar un cliente WireGuard.

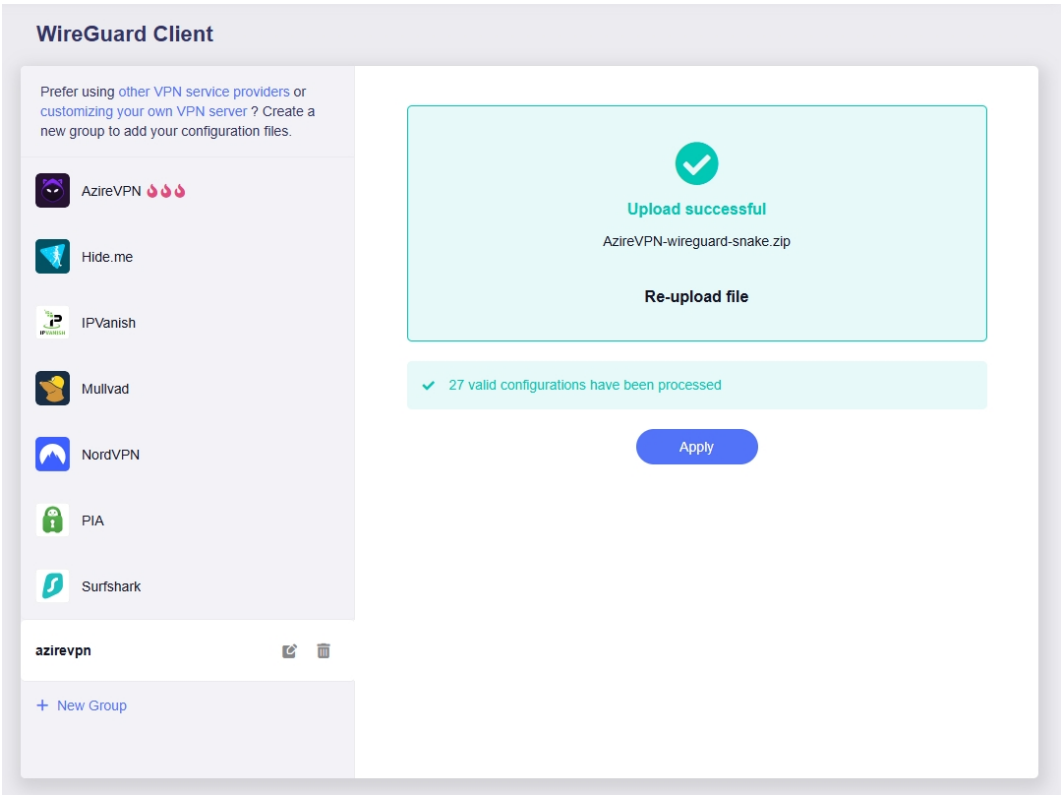
1. Iniciar sesiónn a su enrutador's web admin panel y navegue hasta **VPN** > **WireGuard Client** > **Agregar manualmente**.



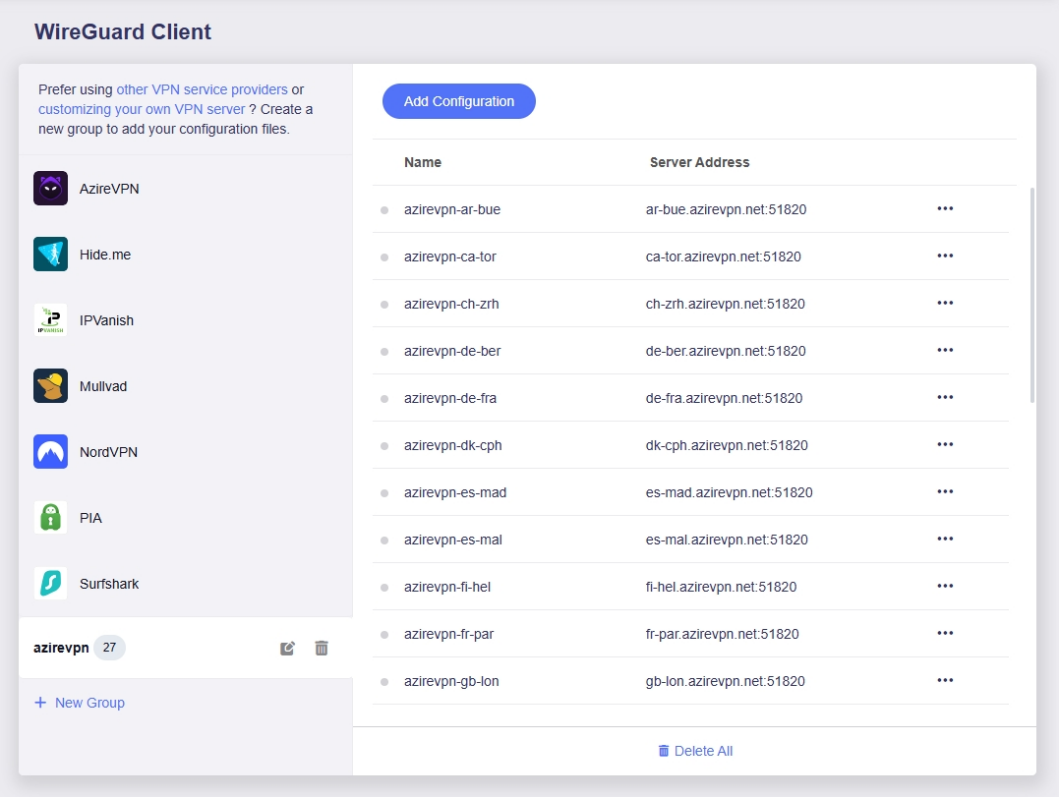
2. Creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



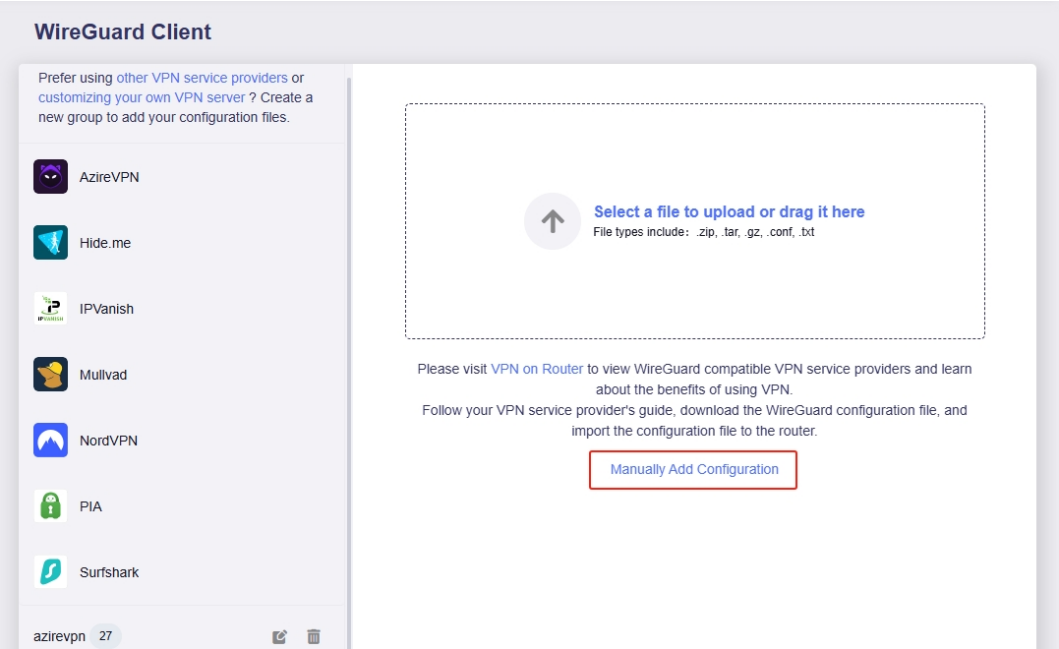
3. Haga clic en el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt) y haga clic en **Aplicar**.

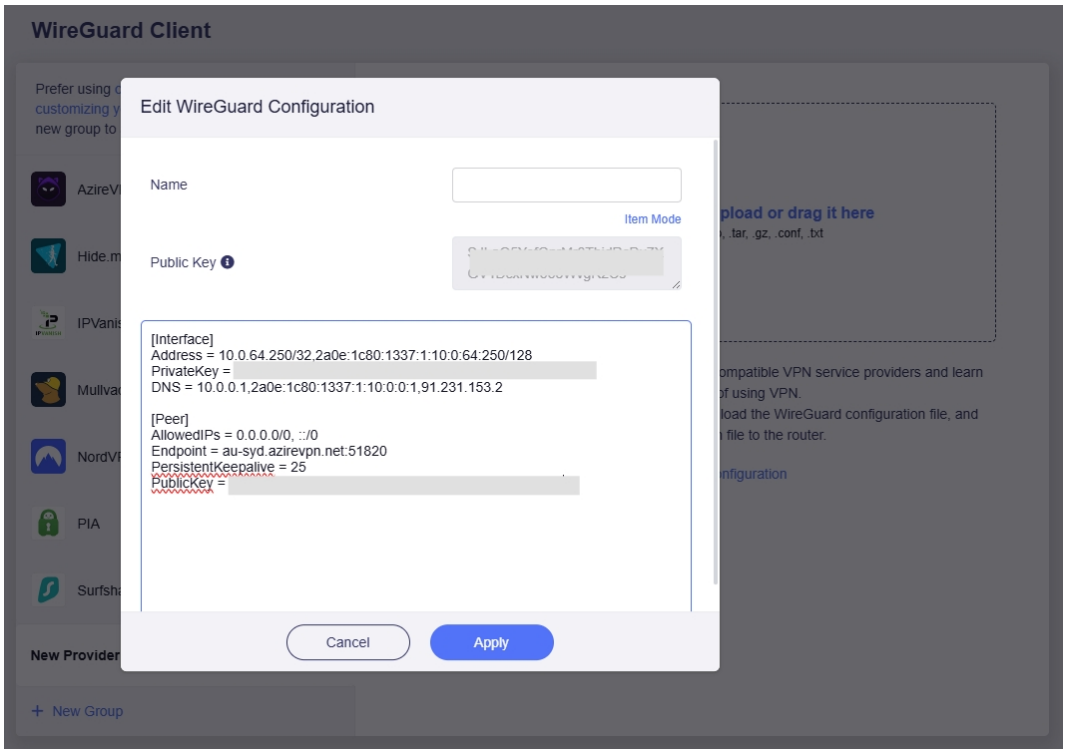


Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

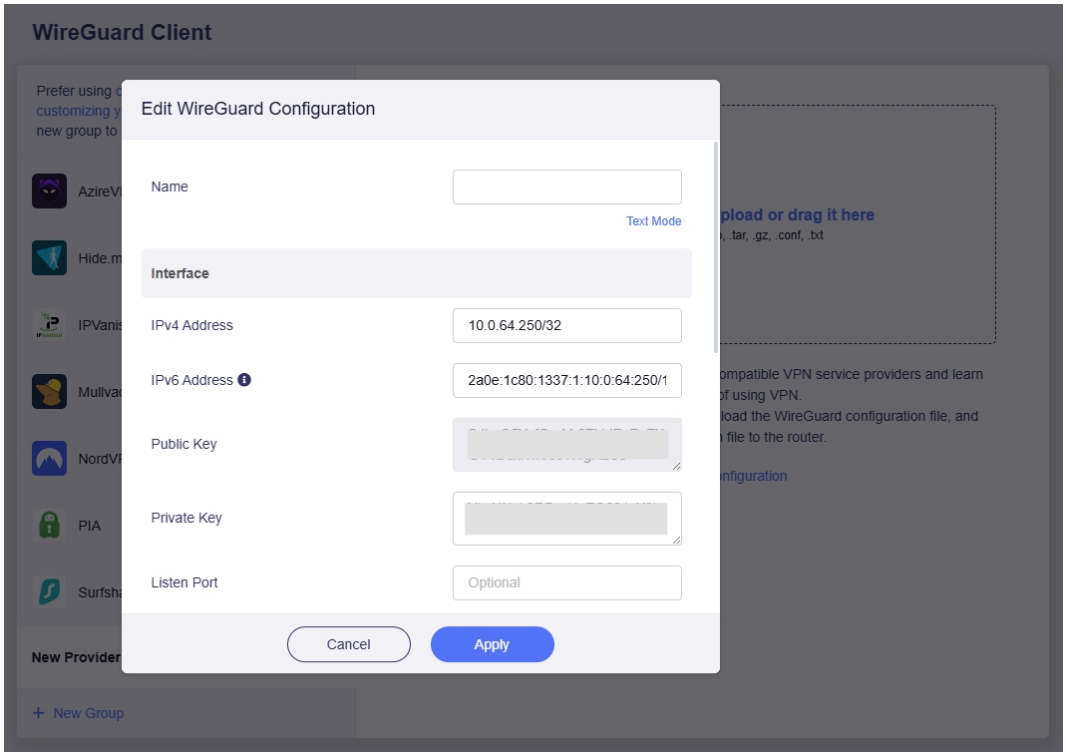


Alternativamente, puede hacer clic en **Agregar configuración manualmente** en la parte inferior del área de carga, agregue detalles de configuración en forma de texto y haga clic en **Aplicar**.

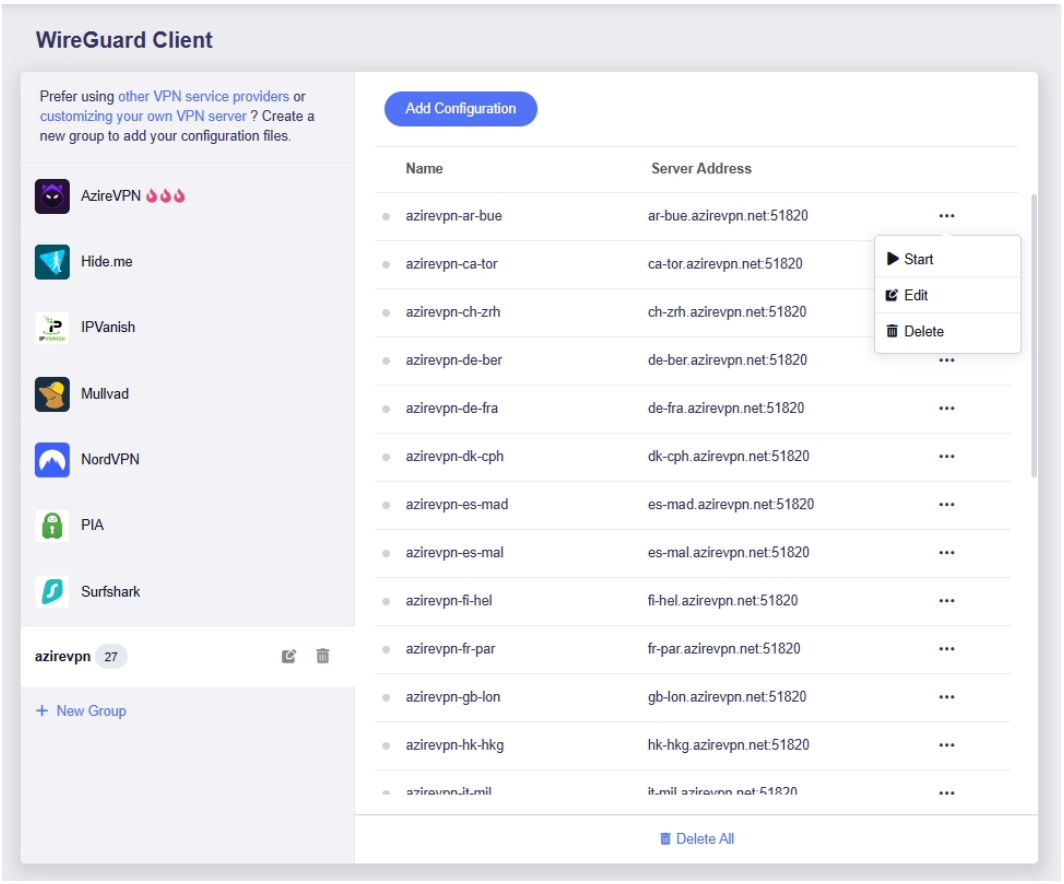




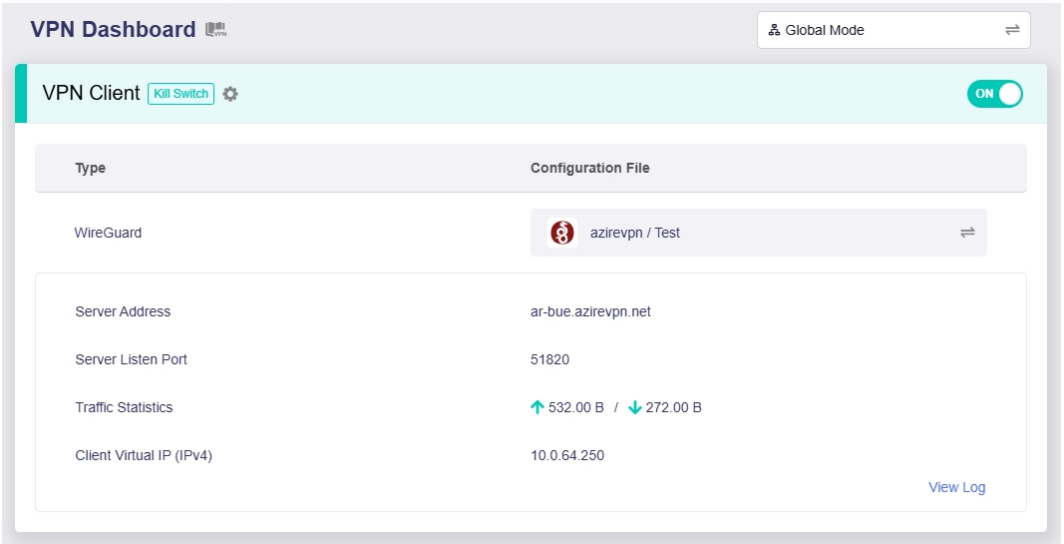
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



4. Haga clic en los tres puntos en el lado derecho para iniciar la conexión.



5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración. Usted puede verificar los detalles de conexión VPN en **Panel de VPN**.



Capítulo 12

Tor

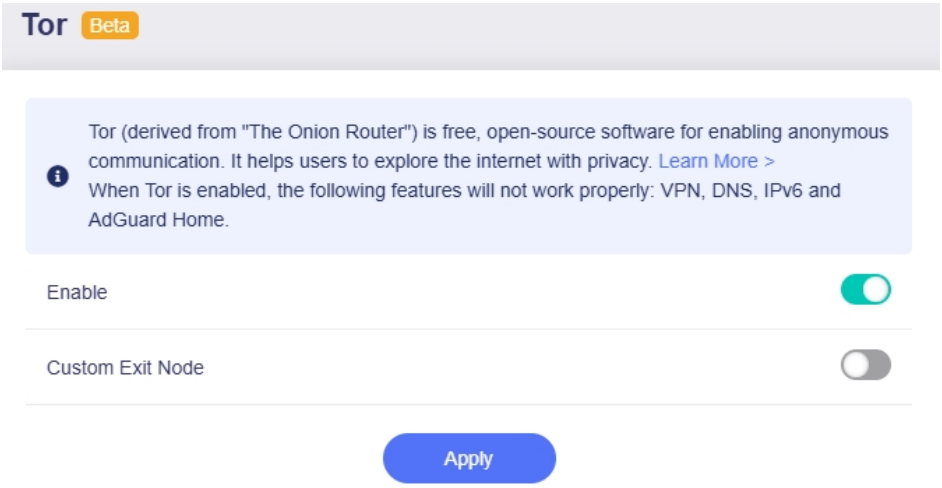
Este capítulo proporciona una breve introducción a Tor (The Onion Router), un software gratuito y de código abierto para permitir la comunicación anónima.

Tor (derivado de **The Onion Router**) es un software gratuito y de código abierto para permitiendo la comunicación anónima. Ayuda a los usuarios a explorar Internet con privacidad. Tenga en cuenta queesta función se encuentra actualmente en versión beta y puede tener algunos errores.

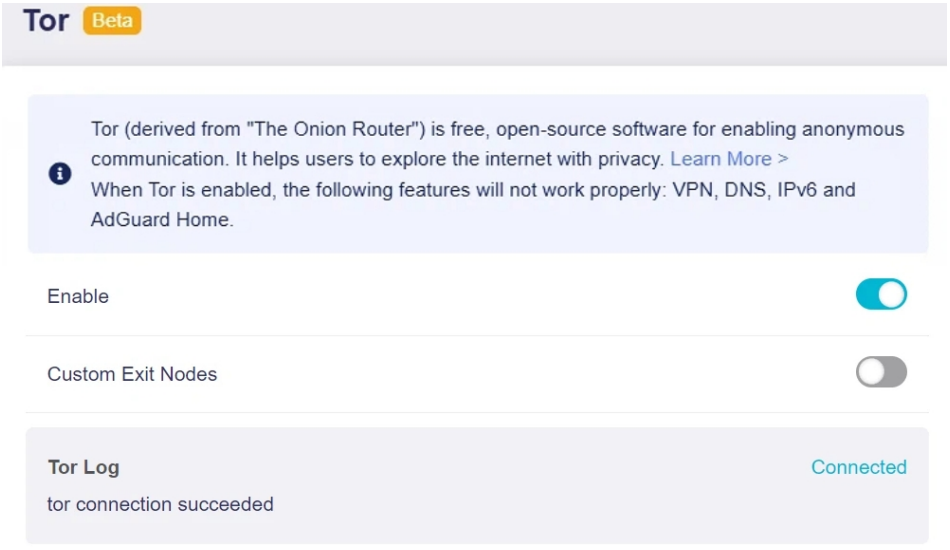
Cuando Tor está habilitado, las siguientes funciones no funcionarán correctamente:Las siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6 y AdGuard Home.

Siga los pasos a continuación para configurar Tor si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **VPN** > **Tor**.Tcambie el interruptor para habilitarlo, habilite nodos de salida personalizados si es necesario, y haga clic en **Aplicar**.



2. Comenzará a conectarse. Si su red cumples los requisitos, se mostrará conectado.



Capítulo 13

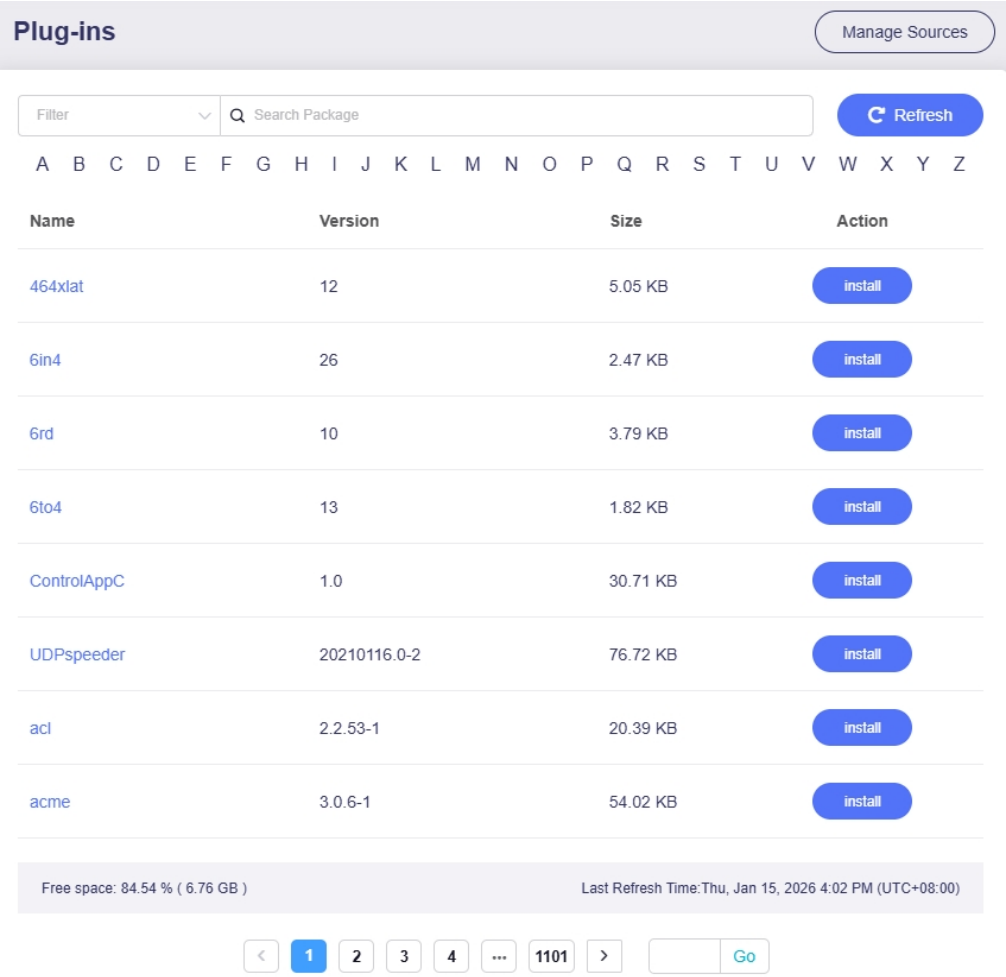
Aplicaciones

Este capítulo presenta algunas aplicaciones en enrutadores GL.iNet, por ejemplo, Complementos, DNS dinámico, Almacenamiento de red, AdGuard Home, Control parental, ZeroTier, Tailscale y Administración de eSIM.

13.1 Complementos

La página Complementos le permite administrar paquetes OpenWrt.

Inicie sesión en su enrutador’s web admin panel, navegue hasta **APLICACIONES** > **Complementos.** Puede instalar o eliminar cualquier paquetee disponible en repositorio. Haga clic en el botón **Actualizar** para actualizar la lista de paquetes antes de instalar los complementos.



Nota:

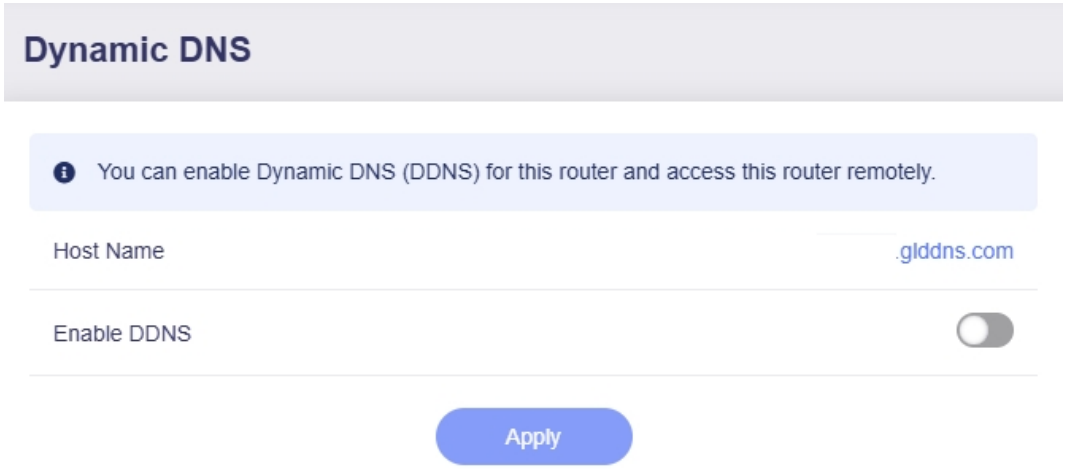
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad causado por complementos de terceros. Si tiene consultas, comuníquese con los respectivos autores de complementos externos.

13.2 DNS dinámico

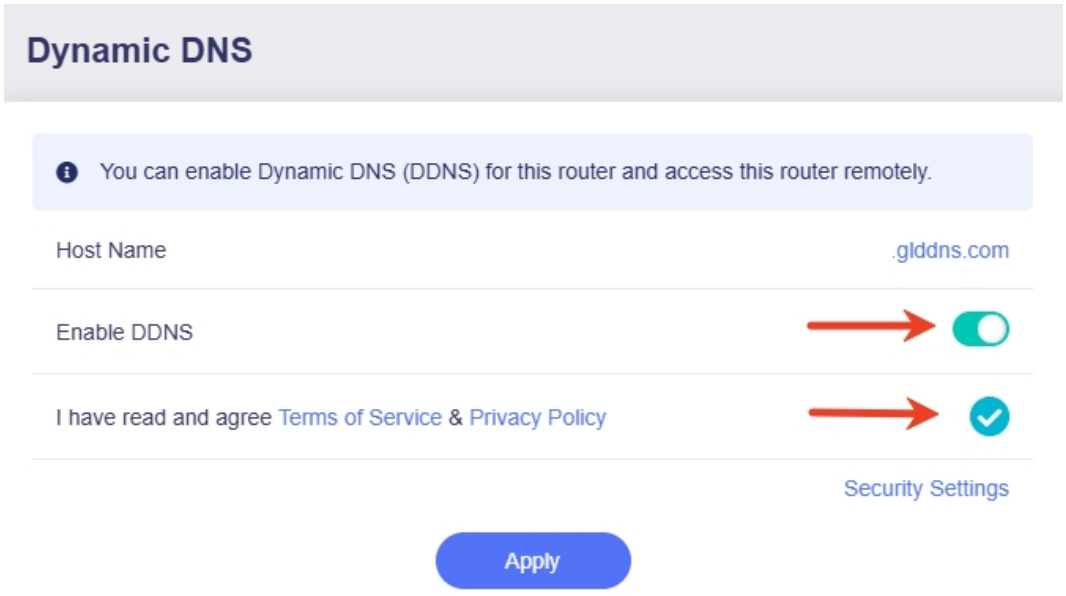
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un dominio. nombre a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad. Se requiere una dirección IP pública para esta funcionalidad.

13.2.1 Habilitar DDNS

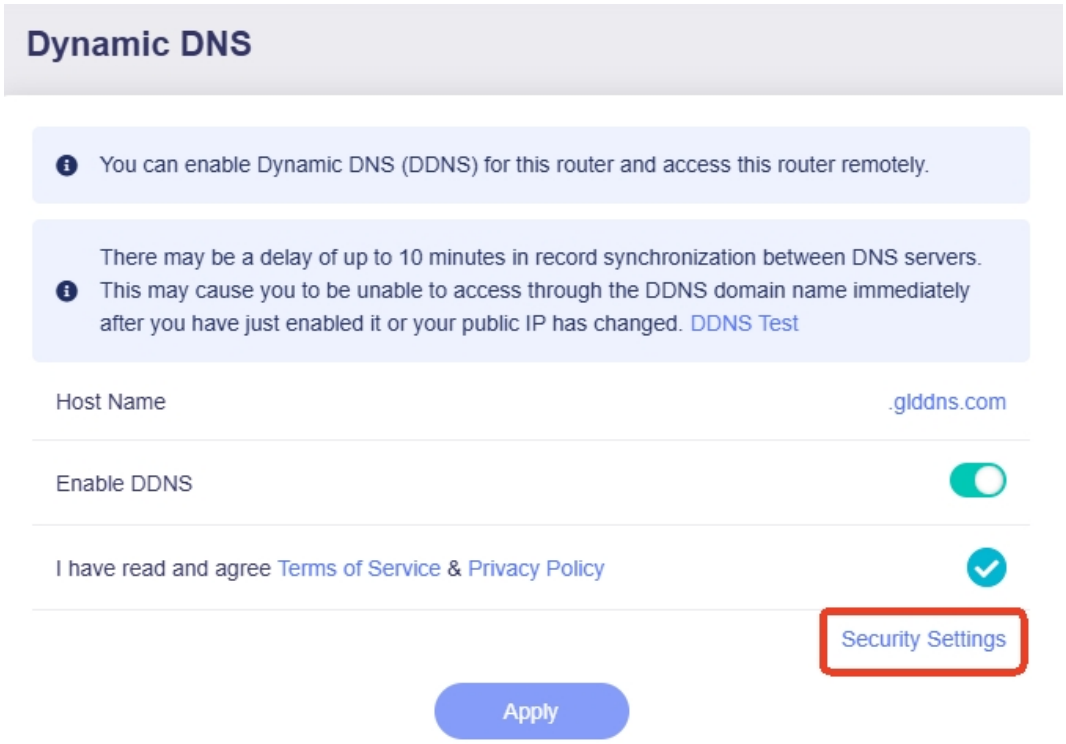
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra a continuación.



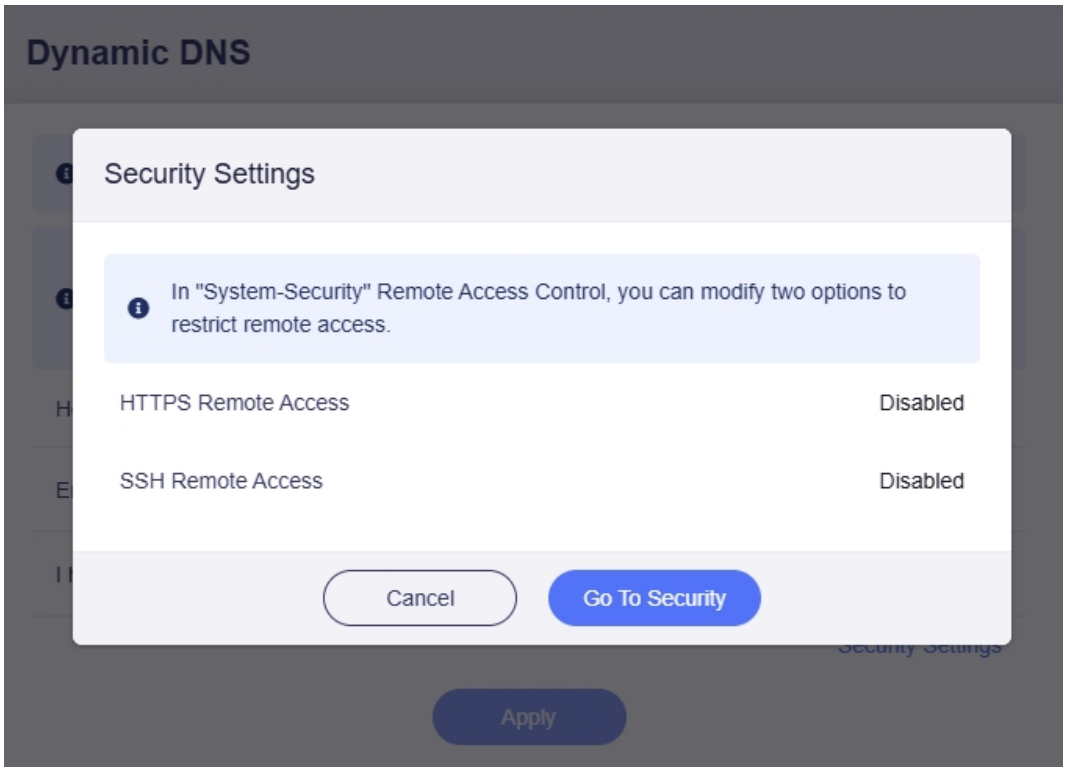
2. Activar **Habilitar DDNS**, lea y acepte los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



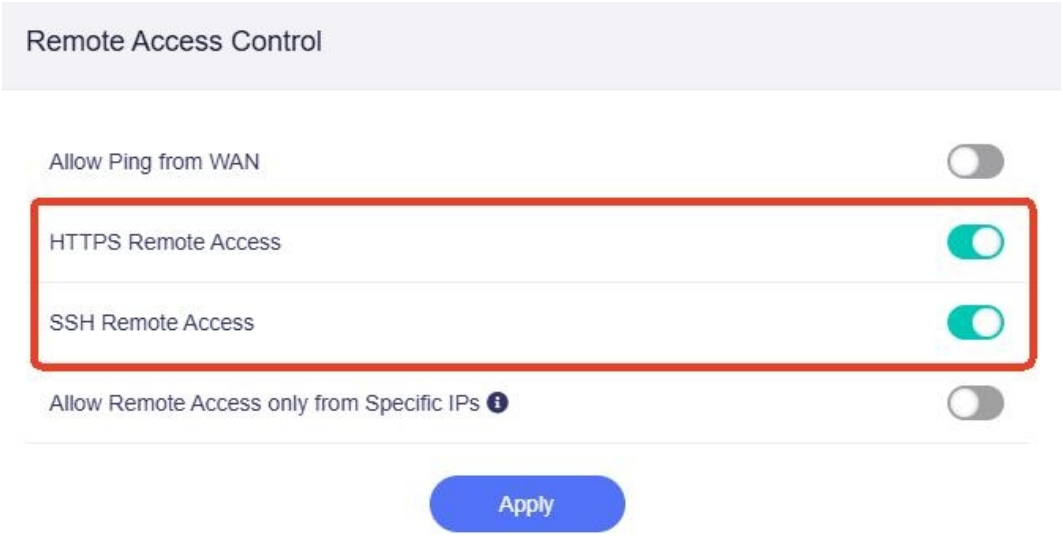
3. Haga clic en **Configuración de seguridad** en la esquina inferior derecha.



4. En la ventana emergente ventana, verifique si el acceso remoto que desea utilizar está habilitado.



Si no, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto** para habilitarlo, luego haga clic en **Aplicar**.



Nota:

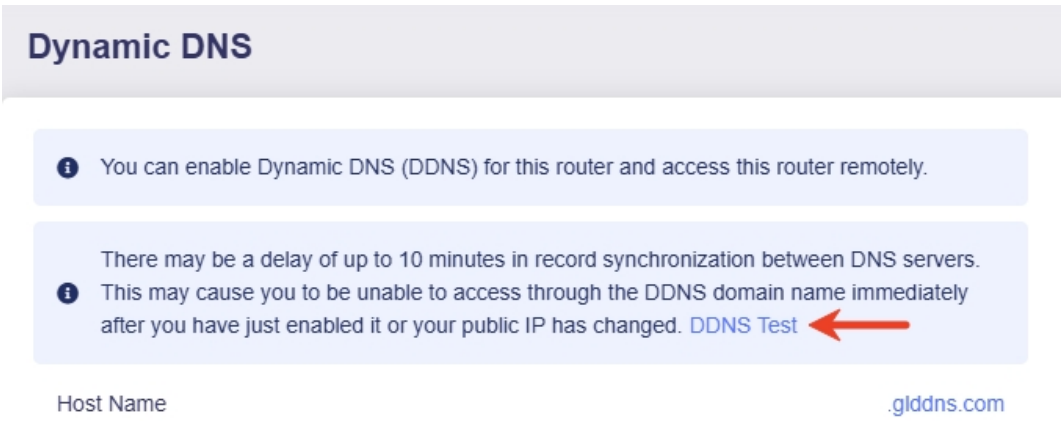
1. Puede haber un retraso de hasta 10 minutos en el registro sincronización entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que Los servicios de GL.iNet usan VPN están deshabilitados.

13.2.2 Comprobar si DDNS funciona

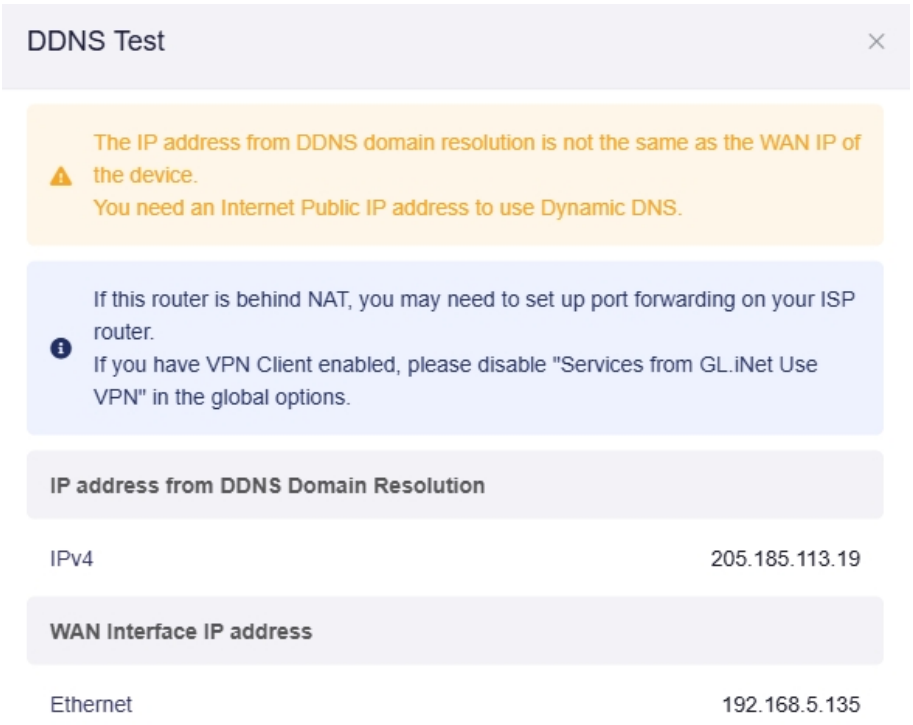
Puede comprobar si DDNS funciona utilizando la herramienta de prueba DDNS o manualmente mediante comandos.

Método 1. Use Herramienta de prueba DDNS

1. En la página DNS dinámico, haga clic en **pruebas DDNSt**.



2. Asegúrese de que la dirección IP de la resolución del dominio DDNS coincida con la IP WAN del enrutador. De lo contrario, aparecerá un mensaje amarillo en la parte superior, indicando que el enrutador podría estar detrás de NAT y que debe configurar el reenvío de puertos en el enrutador ascendente.



Método 2. Usar comandos

1. Usar nslookup comando *nslookup xxxxxxx.glddns.com 8.8.8.8* para obtener la asignación entre el nombre de dominio y la dirección IP. A continuación se muestra un ejemplo de Beryl AX (GL-MT3000)



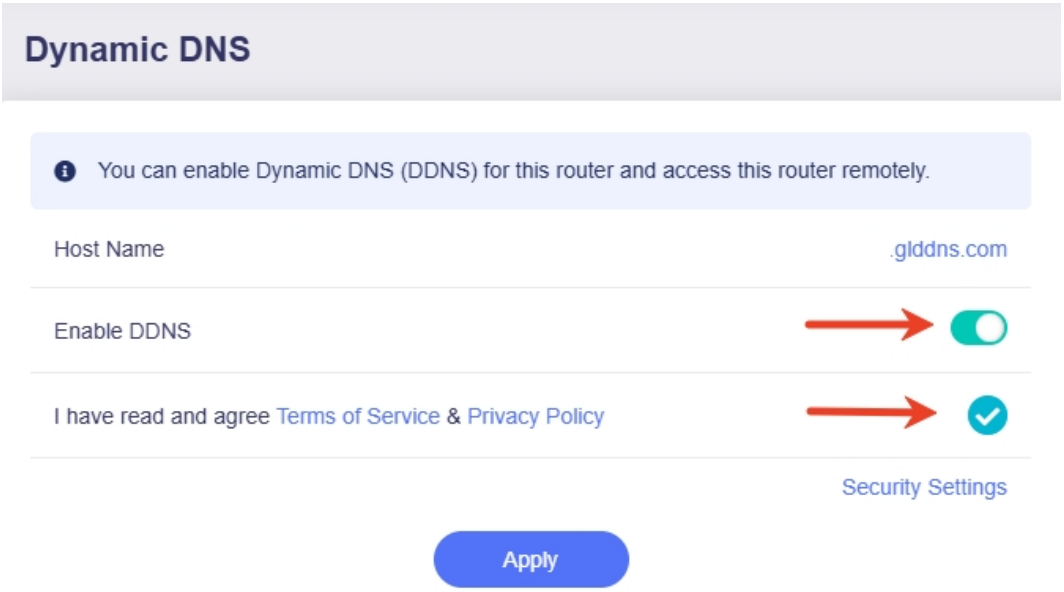
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Uconsúltelo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su dominio DDNS se ha asignado correctamente a una dirección IP pública. Si recibe un mensaje como “el servidor no puede’no encontrar xxxxxxx.glddns.com”, puede indicar que la resolución del dominio falló y que su dominio DDNS no se ha asignado correctamente a una dirección IP pública. Continúe con el siguiente paso para verificar.
3. Inicia sesión en la web ’a admin panel y navegue hasta **INTERNET**. Busque la dirección IP WAN de su enrutador’ en la interfaz actualmente activa. Compare esta dirección IP con la dirección IP pública obtenida anteriormente. Si son iguales, el DDNS está vigente; de lo contrario, no.

13.2.3 Acceso remoto HTTPS

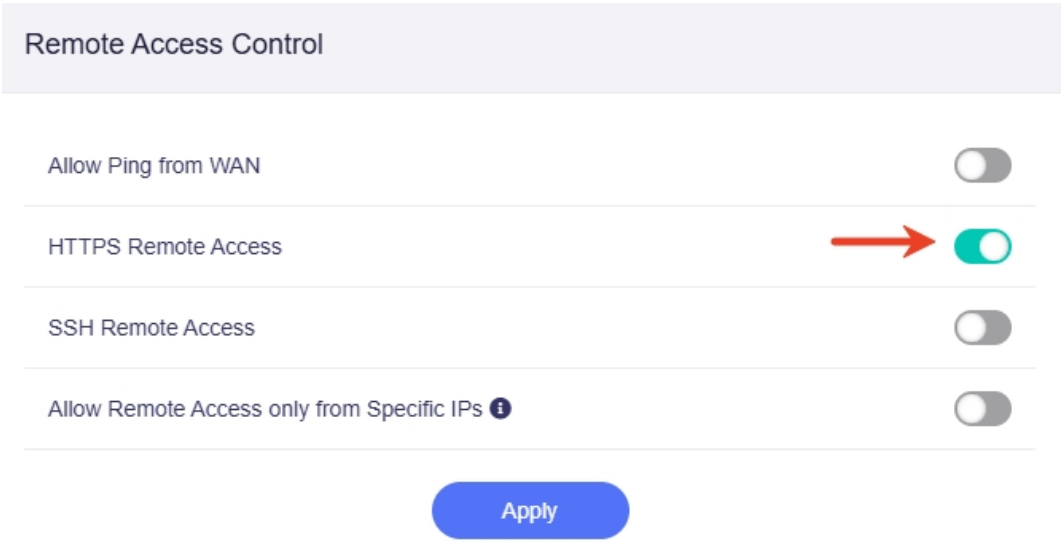
Se requiere una **dirección IP pública** para el acceso remoto HTTPS. Consulte aquí paraverificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

Siga los pasos a continuación para habilitar el acceso remoto HTTPS para su enrutador.

1. En la página DNS dinámico, active **Habilitar DDNS**, acepte los **Términos de servicios y política de privacidad** y luego haga clic en **Aplicar**.

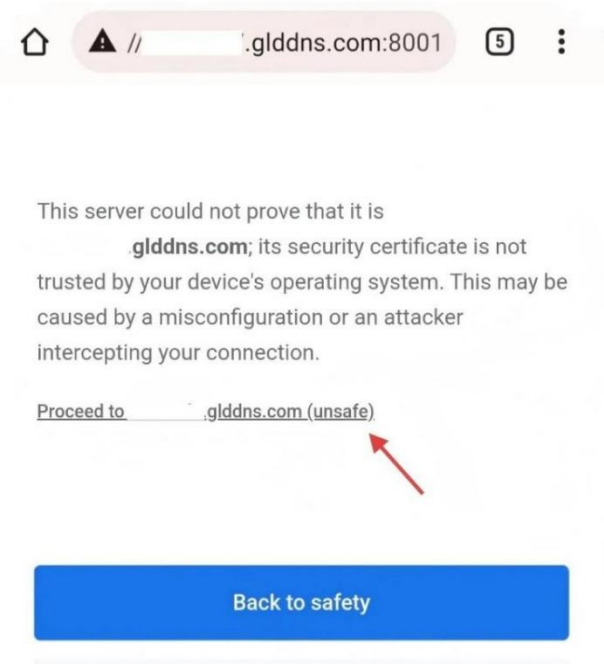


2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilitar **Acceso remoto HTTPS** y haga clic en **Aplicar**.



3. Una vez habilitado, puede acceder al panel de administración del enrutador’desde cualquier lugar usando el DDNS host nombre sobre HTTPS, p. ej., **https://xxxxxxx.glddns.com**. Si el reenvío de puertos está configurado, acceda a él como **https://xxxxxxx.glddns.com:external_port** (reemplazar el externo_puerto con su real puerto número).

Nota: Esta función utiliza certificados autofirmados; por lo tanto, los navegadores indicarán "Su conexión no es privada" al acceder al panel de administración del enrutador a través del nombre de host DDNS a través de HTTPS. Para continuar con el acceso remoto HTTPS, haga clic en **Avanzado** en la parte inferior, luego haga clic en **Continuar con xxxxxxx.glddns.com** para continuar.



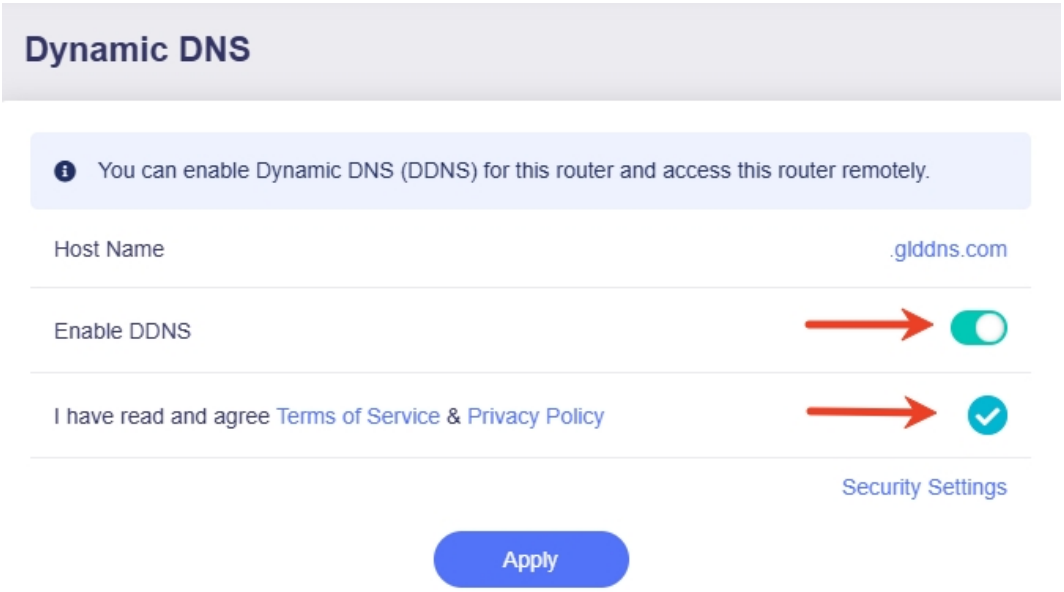
Luego podrá acceder a enrutador’s panel de administración web usando el DDNS host nombre sobre **HTTPS**.

13.2.4 Acceso remoto SSH

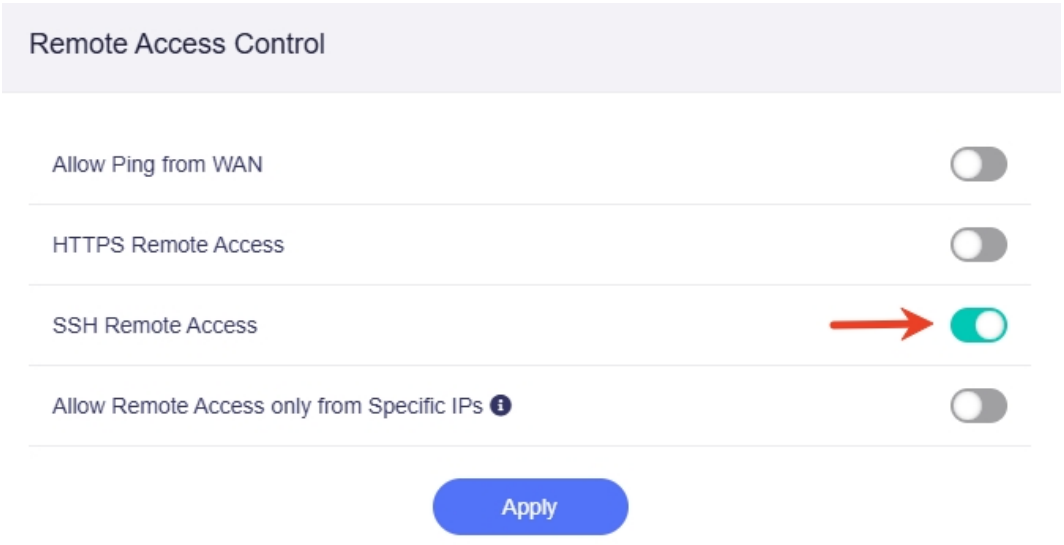
Se requiere una **dirección IP pública** para el acceso remoto SSH. Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH acceso remoto .

Siga los pasos siguientes para habilitar el acceso remoto SSH para su enrutador.

1. En la página DNS dinámico, active **Habilitar DDNS**, acepte los **Términos de servicios y política de privacidad** y luego haga clic en **Aplicar**.



2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilitar **Acceso remoto SSH** y haga clic en **Aplicar**.



Una vez habilitado, puede acceder al panel de administración del enrutador' desde cualquier lugar mediante DDNS host nombre sobre SSH, por ejemplo, **ssh root@xxxxxxx.glddns.com**. Si el reenvío de puertos está configurado, acceda a él como **ssh root@xxxxxxx.glddns.com:external_port** (reemplace el externo_puerto con su real puerto número).

13.3 Almacenamiento en red

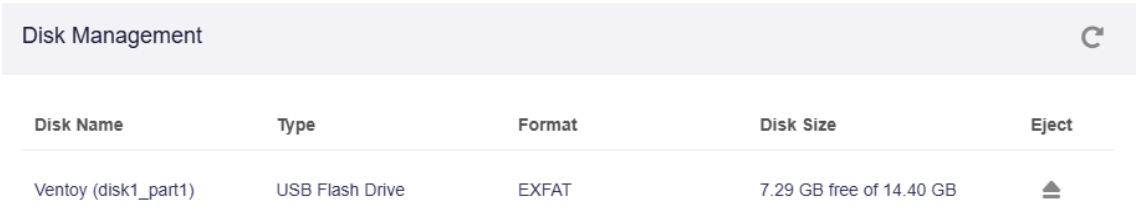
El almacenamiento en red permite compartir archivos de forma inalámbrica entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos los dispositivos conectados a Wi-Fi.

Beryl AX está equipado con un puerto USB, compatible con unidades flash USB y discos duros externos portátiles. Puede configurar Samba, WebDAV o DLNA para estos dispositivos de almacenamiento, que admiten formatos comunes como NTFS, FAT32 y EXT4.

Nota: El consumo de energía del disco duro USB es bastante alto. Úselo con una fuente de alimentación externa, de lo contrario puede causar un mal funcionamiento.

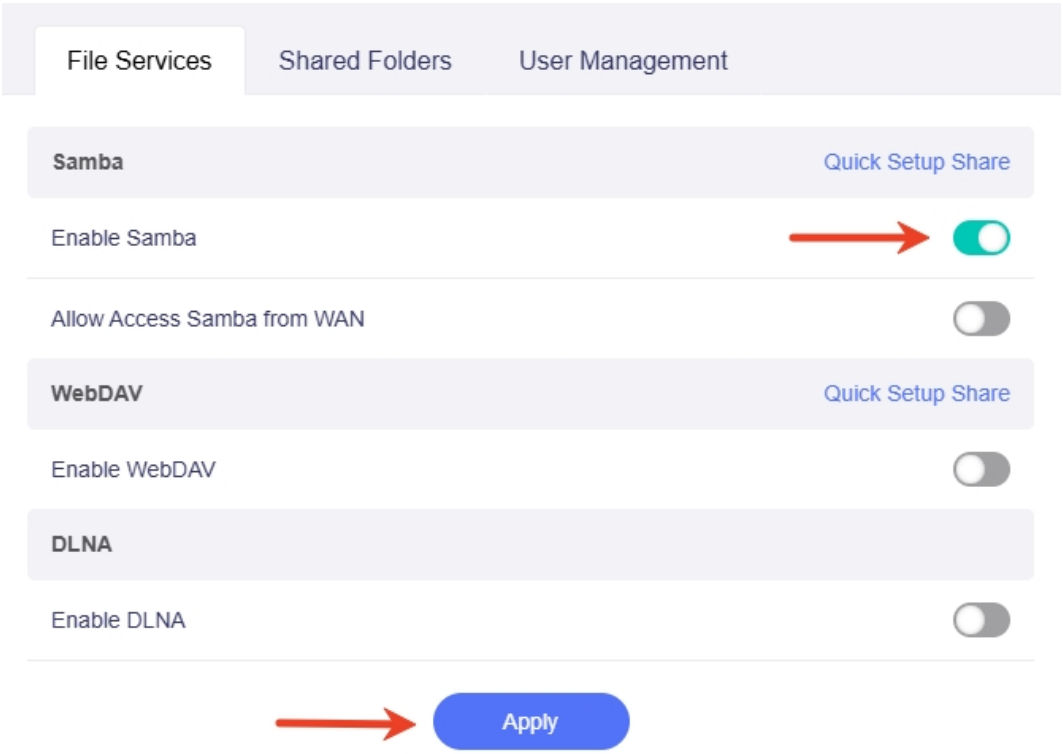
13.3.1 Conectar una unidad de almacenamiento

1. Conecte su dispositivo de almacenamiento al enrutador.
   - Para un USB unidad: Conéctelo directamente al puerto USB.
   - Para un disco duro externo: conéctelo a una fuente de alimentación separada (si es necesario) y luego conéctelo al enrutador.
2. Inicie sesión en su enrutador’s panel de administración web, navegue hasta **APLICACIONES** > **Almacenamiento en red**. Puede habilitar servicios de transferencia de archivos y administrar la carpeta compartida aquí.
3. Si el dispositivo de almacenamiento se detectado, la **Administración de discos** se mostrará de la siguiente manera.



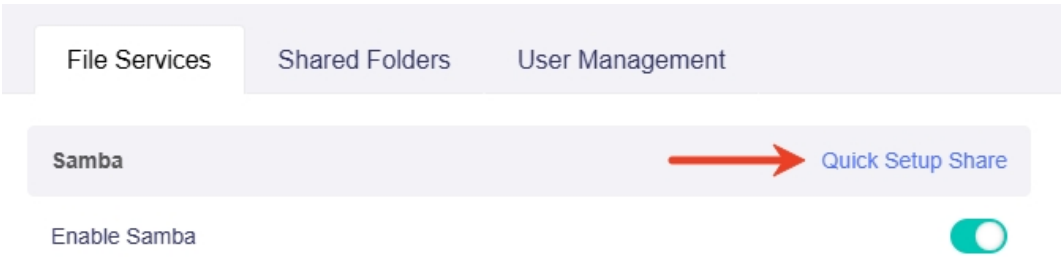
13.3.2 Configurar Samba

1. En la sección **Servicios de archivos**, toggle en **Esamba habilitable**, y haga clic en **Aplicar**.

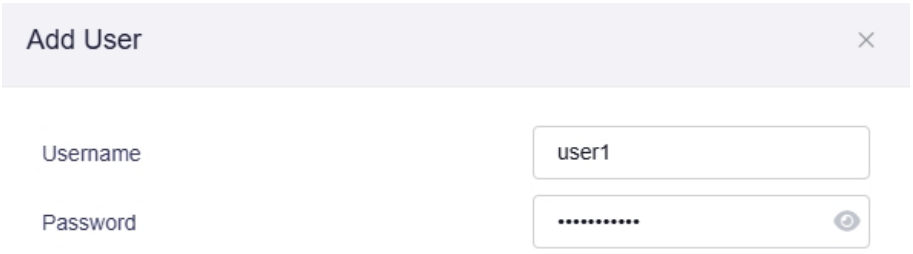


- **Permitir el acceso a Samba desde WAN**: habilítelo si desea que los dispositivos ascendentes accedan al servicio Samba.

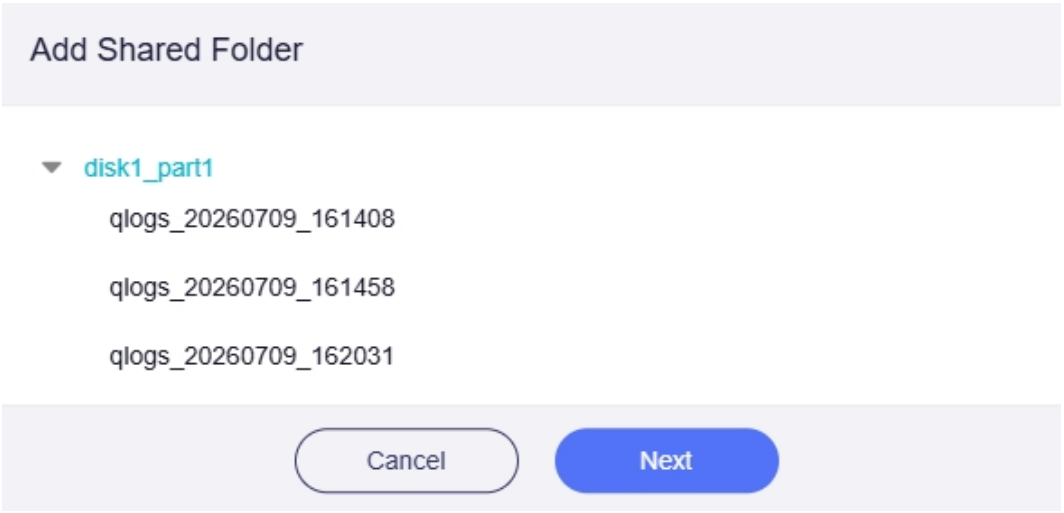
2. Haga clic en **Configuración rápida Compartir** para establecer el enlace compartido.



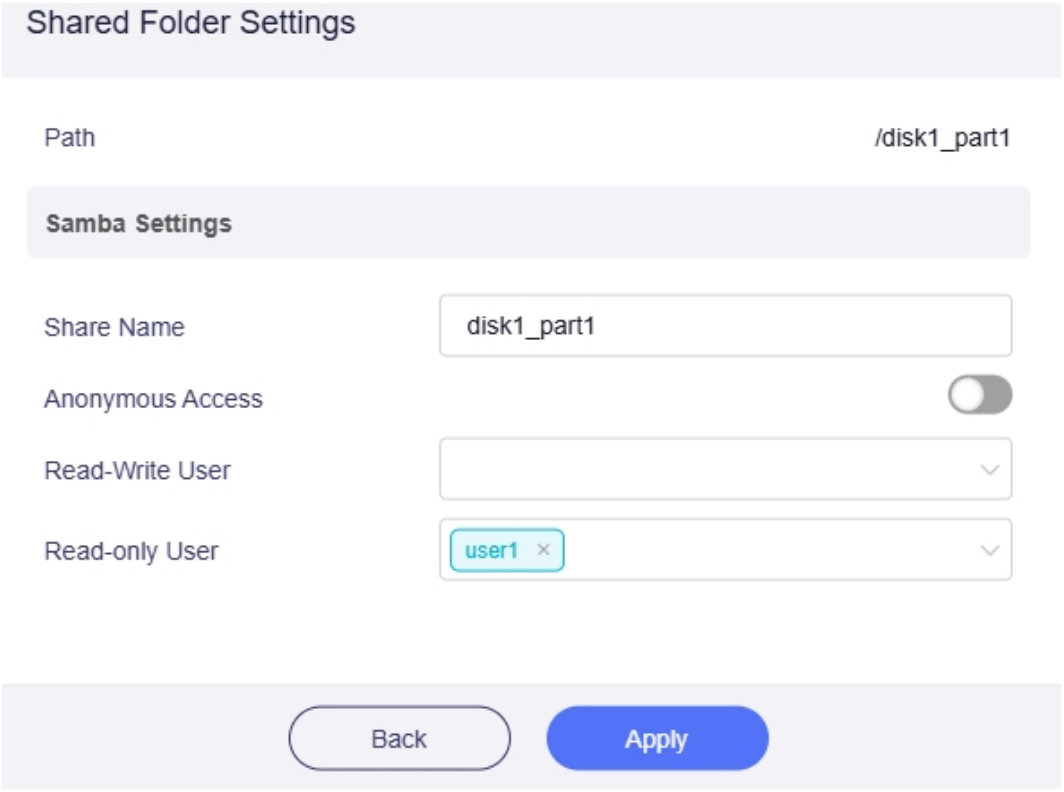
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir, tluego haga clic **Siguiente**. Sisi lo desea para compartir el disco completo, haga clic en el nombre del disco (p. ej., disk1_part1).



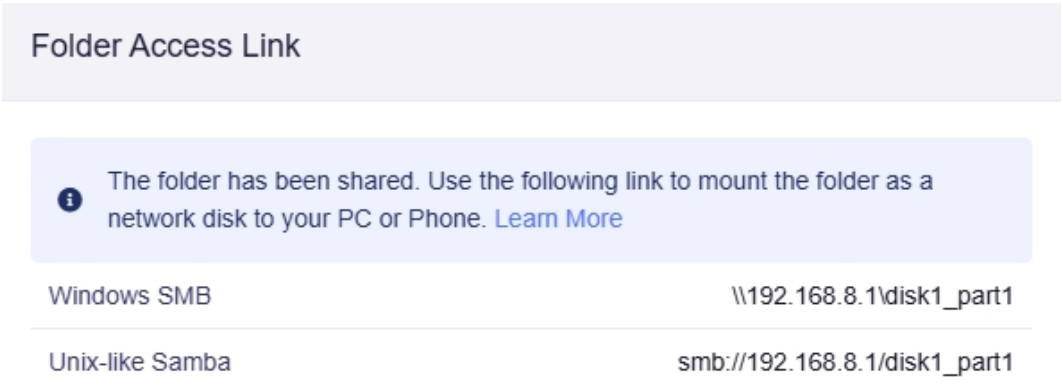
5. Configurar la scarpeta compartida.
   El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este usuario pueda para escribir o eliminar archivos, eliminelo de Usuario de solo lectura y agréguelo a **Lectura-Escritura Usuario**, tluego haga clic **Aplicar**.



Consejo: Por razones de seguridad, no se recomienda habilitar el acceso anónimo.

6. Obtenga el enlace de acceso a la carpeta

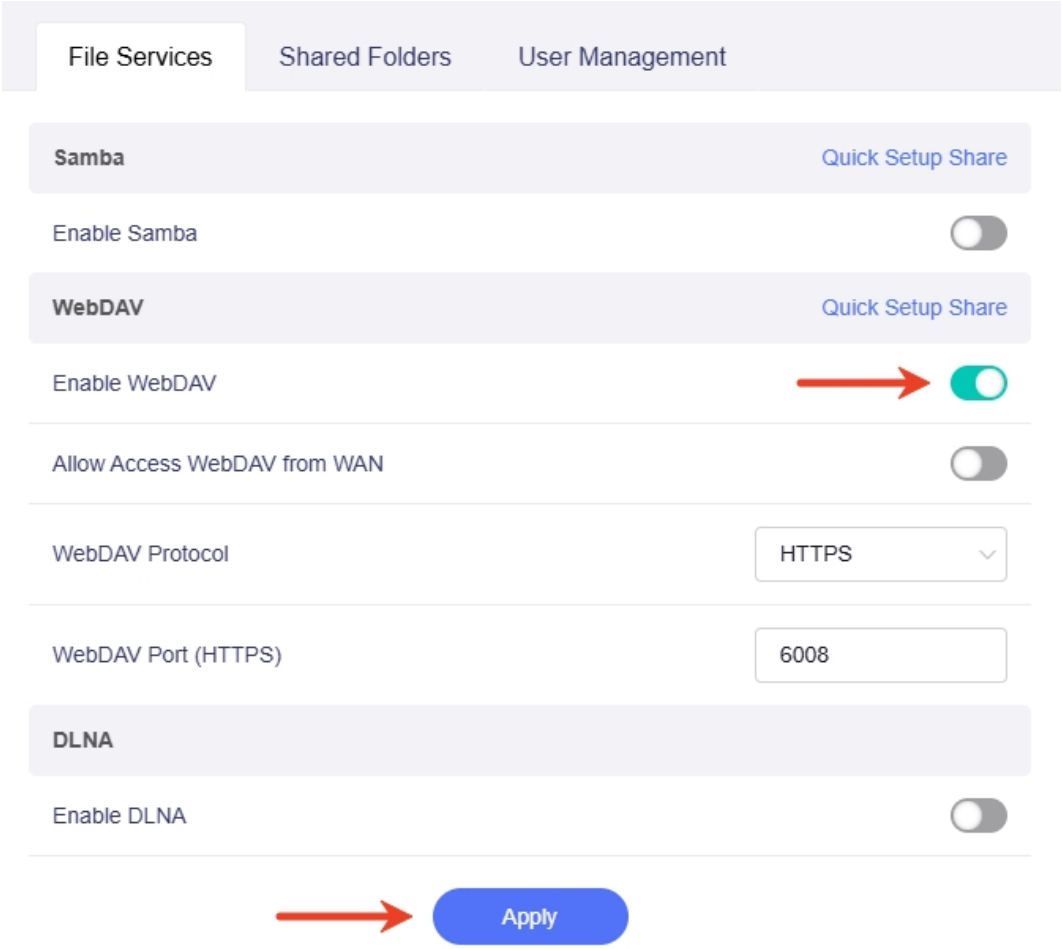
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder a tu carpeta compartida a través del servicio Samba a través de estos enlaces.



Nota: si habilita **Permitir acceso a Samba desde WAN** y accede a la carpeta compartida desde red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con su enrutador’s IP WAN, que se puede encontrar en la página INTERNET del panel de administración web.

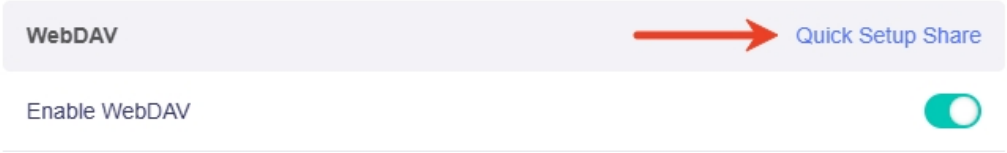
13.3.3 Configurar WebDAV

1. En la sección **Servicios de archivos**, active **Eactivar WebDAV** y haga clic en **Aplicar**.

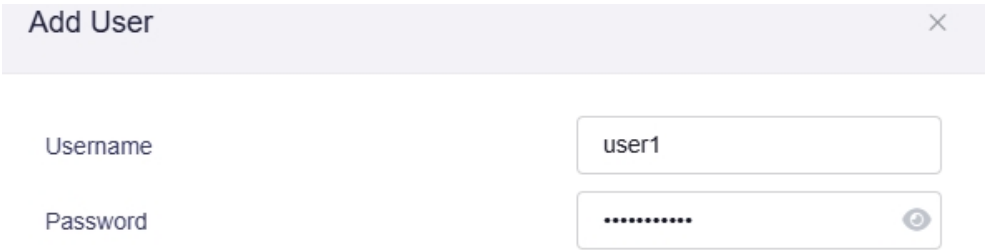


- **Permitir acceso a WebDAV desde WAN**: habilítelo si lo desea los dispositivos ascendentes para acceder al WebDAV servicio.
- **Protocolo WebDAV**: HTTP no está cifrado; Úselo bajo su propia responsabilidad. HTTPS está cifrado y utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario para modificar el número de puerto a menos que haya un conflicto. El puerto número rango es 1024 - 65535.

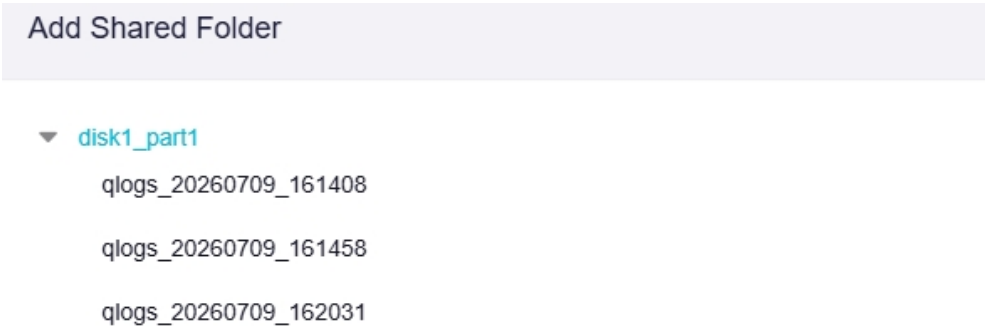
2. Haga clic en **Configuración rápida Compartir** para sconfigurar el enlace compartido.



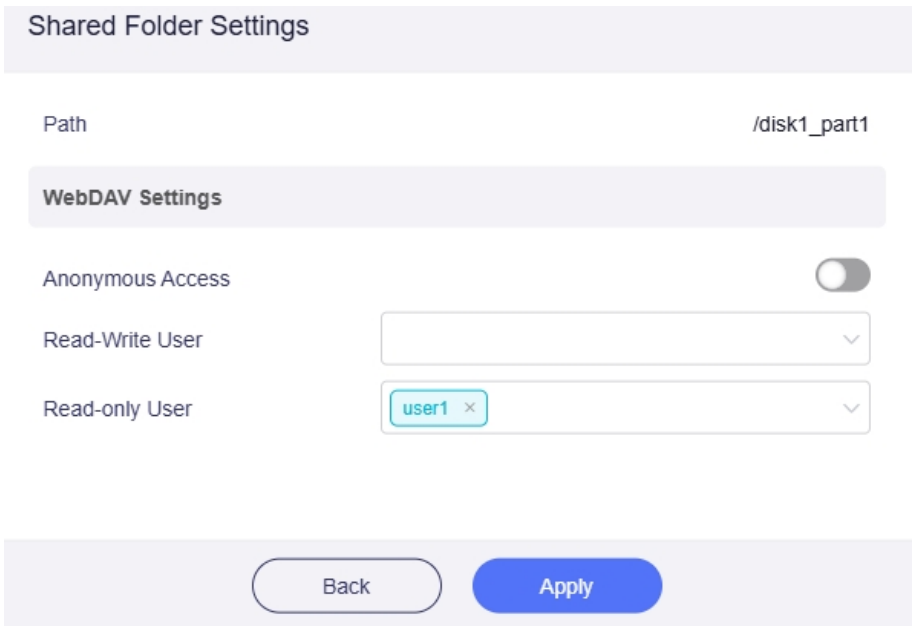
3. Agregar un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir. Sisi desea compartir el completo disco, haga clic en el nombre del disco (por ejemplo, disk1_part1).



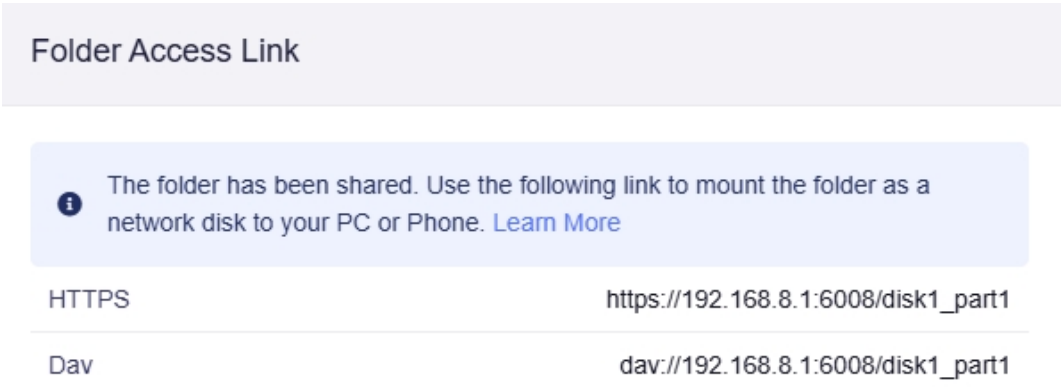
5. Configure el scarpeta compartida.
   El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada.
   Si desea que este usuario pueda escribir o eliminar archivos, eliminelo del usuario de solo lectura y agréguelo a **Lectura-Escriturae Usuario**, luego haga clic **Aplicar**.



Consejo: Por razones de seguridad, no se recomienda habilitar Acceso anónimo.

6. Obtenga el enlace de acceso a la carpeta

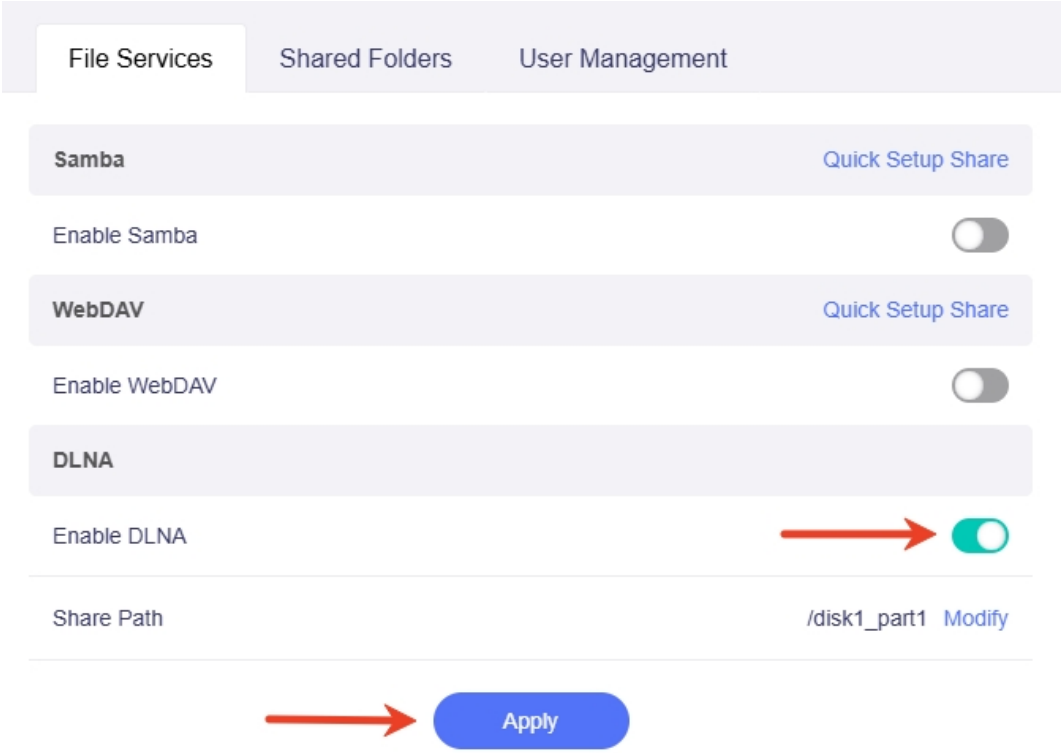
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix Los sistemas tipo Unix incluyens Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder a tu carpeta compartida a través del servicio WebDAV a través de estos enlaces. data-r="3386">WebDAV



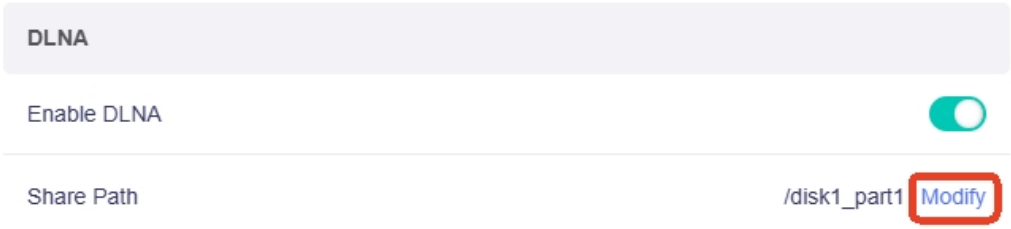
Nota: Si habilita **Permitir acceso WebDAV desde WAN** y accede a la carpeta compartida desde red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con su enrutador’s WAN IP, que se puede encontrar en la página INTERNET del panel de administración web.

13.3.4 Configurar DLNA

1. En la sección **Servicios de archivos**, active **Enable DLNA**, y haga clic en **Aplicar**.



2. Modifique la ruta compartida a la derecha si es necesario.



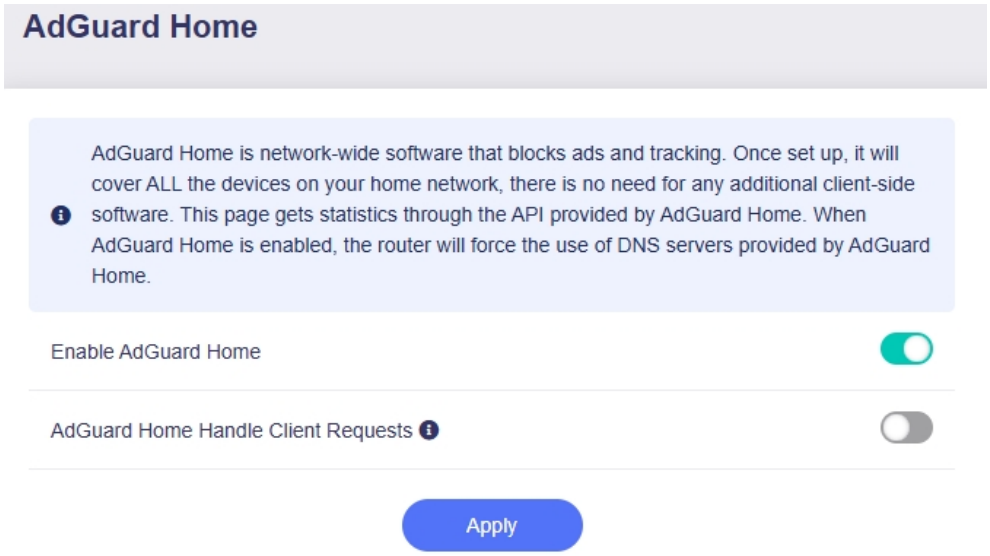
3. Conecte su televisor inteligente al enrutador. encontrará el DLNA sservidor automáticamente.

13.4 AdGuard Home

AdGuard Home es un software que bloquea anuncios y previene el seguimiento en toda la red. Una vez configurado, cubrirá todos los dispositivos cliente sin necesidad de software adicional del lado del cliente.

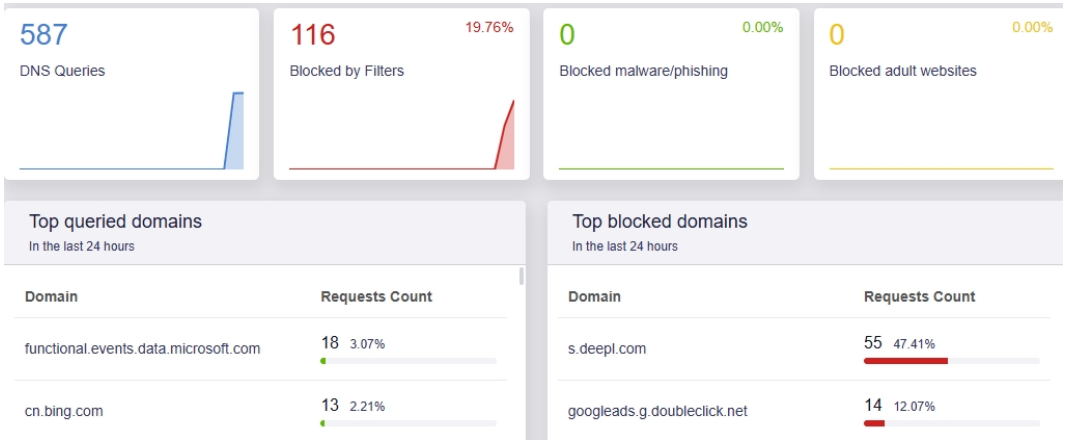
Siga estos pasos para configurar AdGuard Home.

1. Inicie sesión en el enrutador's web admin panel, navegue hasta **APLICACIONES** > **AdGuard Home**. Alternar en **Ehabilite Inicio de AdGuard** y haga clic en **Aplicar**.

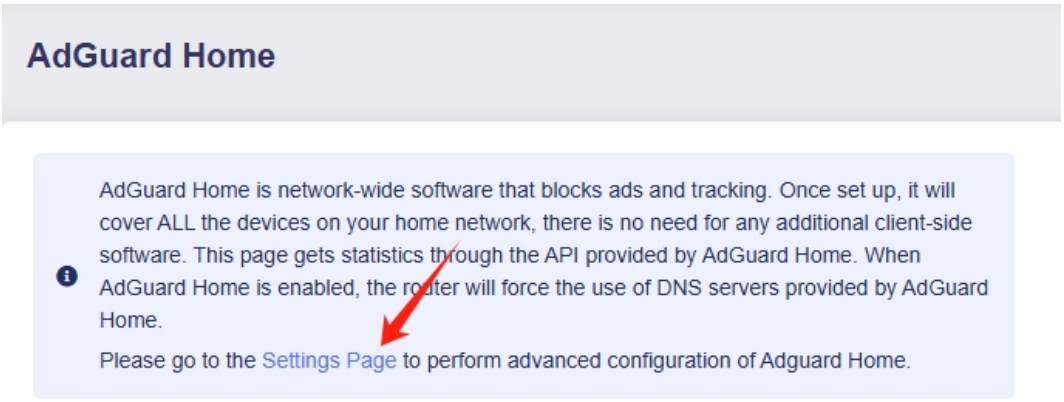


- **AdGuard Home Handles Solicitudes de clientes**: si está habilitado, las consultas de DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto provocará que las políticas de VPN basadas en dominios fallen.

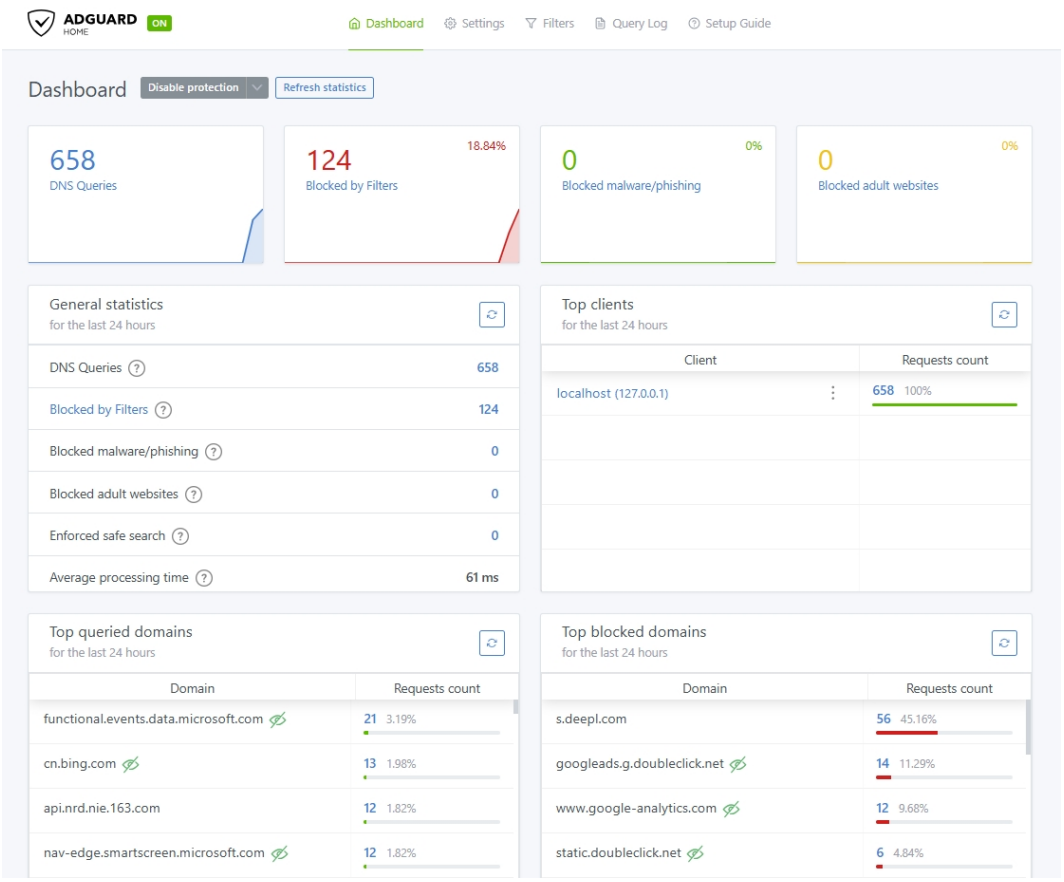
2. La página cargará automáticamente estadísticas DNS (consultas, dominios bloqueados, etc.) a través de la API proporcionada por AdGuard Home.



3. Haga clic en **Configuración Página** para configurar configuración avanzada para AdGuard Home.



4. Será redirigido a la página de configuración de AdGuard Home'. visite la [AdGuard Inicio Soporte Centro] para asistencia.



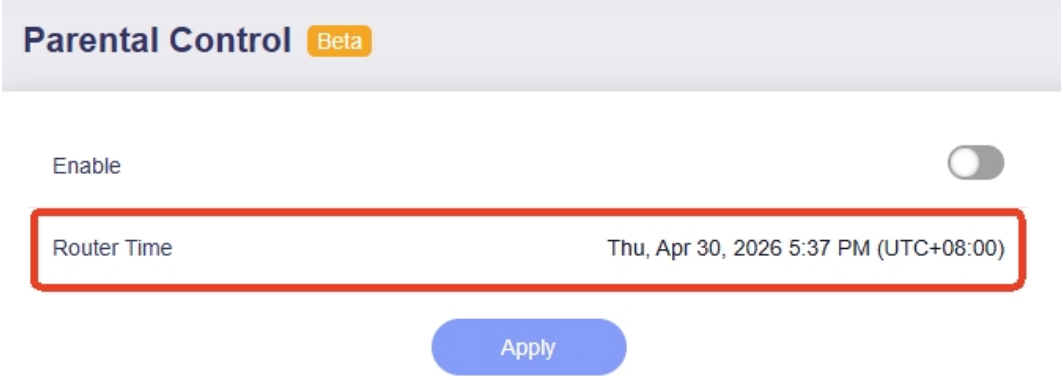
13.5 Control parental

El control parental es una forma de mantener a los niños seguros en línea bloqueando sitios web inapropiados y limitando el tiempo que utilizan los dispositivos. Ayuda a prevenir el acceso a contenido dañino, administrar el tiempo frente a la pantalla y garantizar que los niños usen Internet de manera responsable.

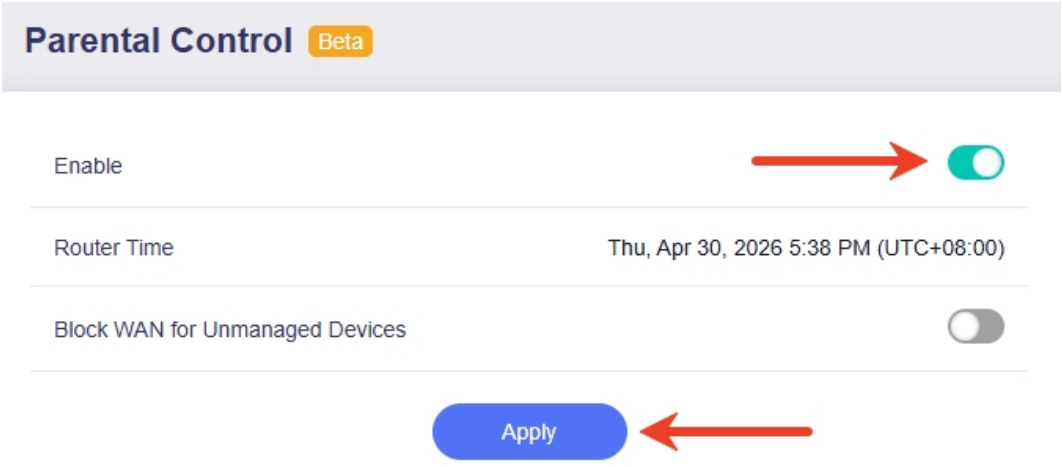
13.5.1 Configuración rápida

Siga estos pasos para configurar Parental Control en GL.enrutador iNets.

1. Inicie sesión en el enrutador's web admin panel y vaya a **APLICACIONES** > **Control parental.** Asegúrese de que la hora del enrutador sea precisa. Si no, ve a **SISTEMA** > **Zona horaria** para sincronizarlo primero.



2. Habilite el control parental y haga clic en **Aplicar**. Luego siga el asistente de configuración para configurar el control parental. También puedes ver el vídeo de configuración aquí.



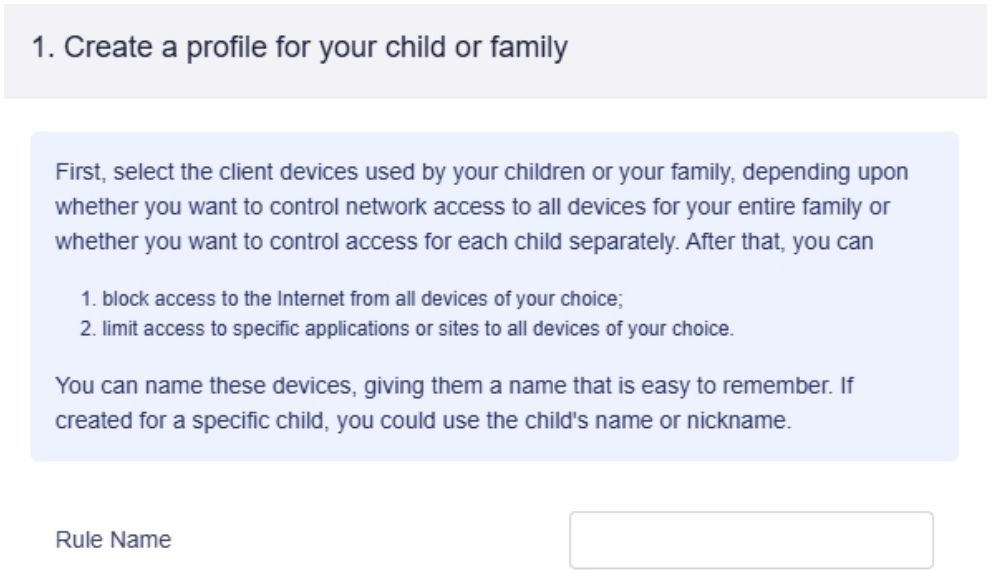
- **Bloquear WAN para dispositivos no administrados**: Bloquea el acceso a Internet para todos los dispositivos que no están en la lista de Control parental.

Aquí hay un caso de uso para su referencia.

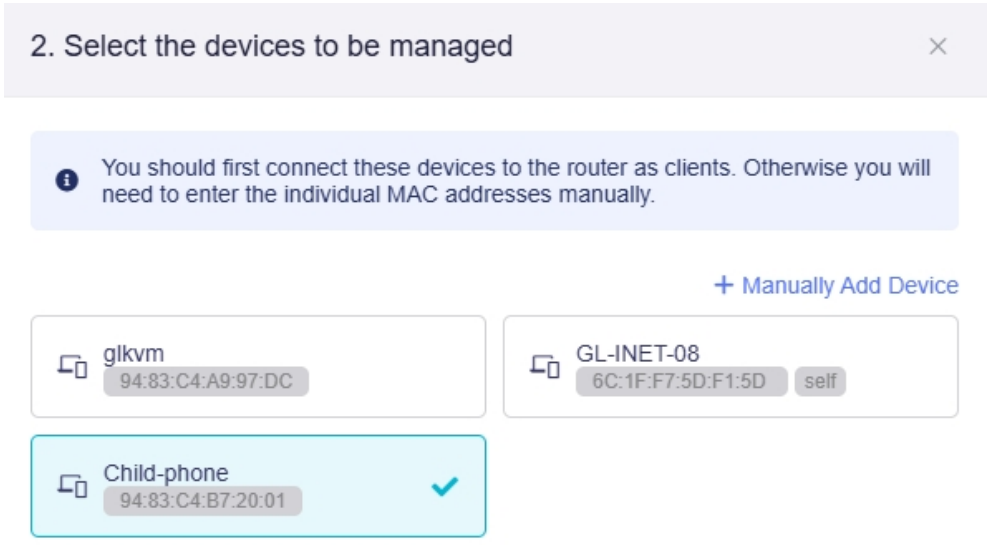
Escenario: Los dispositivos en estees perfil solo pueden acceder a Internet para estudiar de 8 a.m. a las 11 a. m. de lunes a viernes y para juegos de 6 p. m. a 8 p. m. los fines de semana. El acceso a Internet está bloqueado de forma predeterminada en todos los demás momentos.

Pasos de configuración:

1. Crea un perfil y personaliza un nombre.

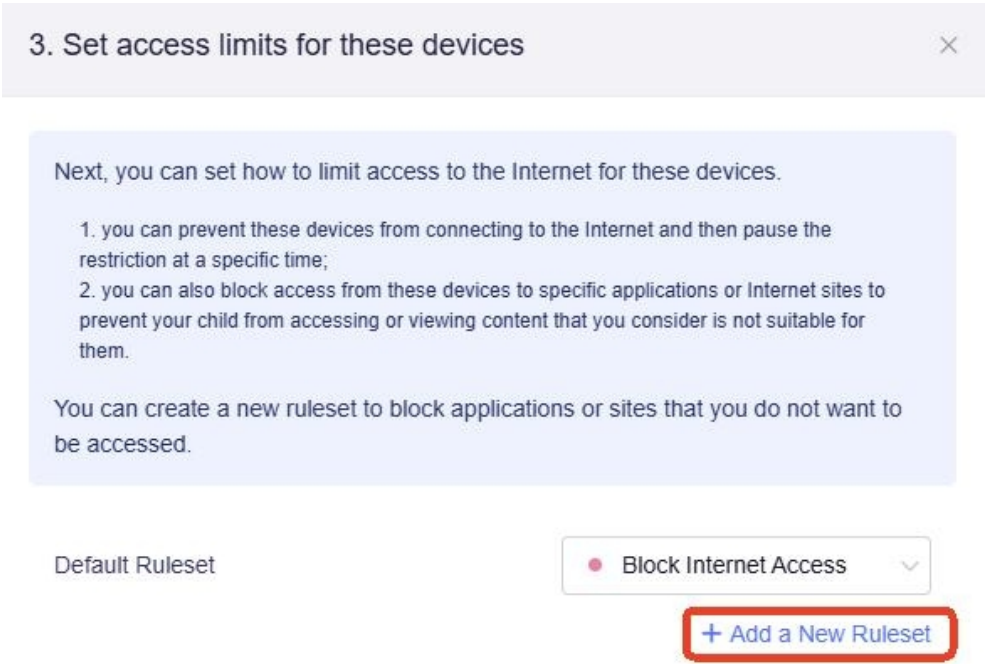


2. Seleccione los dispositivos que desea administrar. Conéctelos primero al enrutador. Si no se han conectado al enrutador, agréguelos manualmente ingresando sus direcciones MAC.

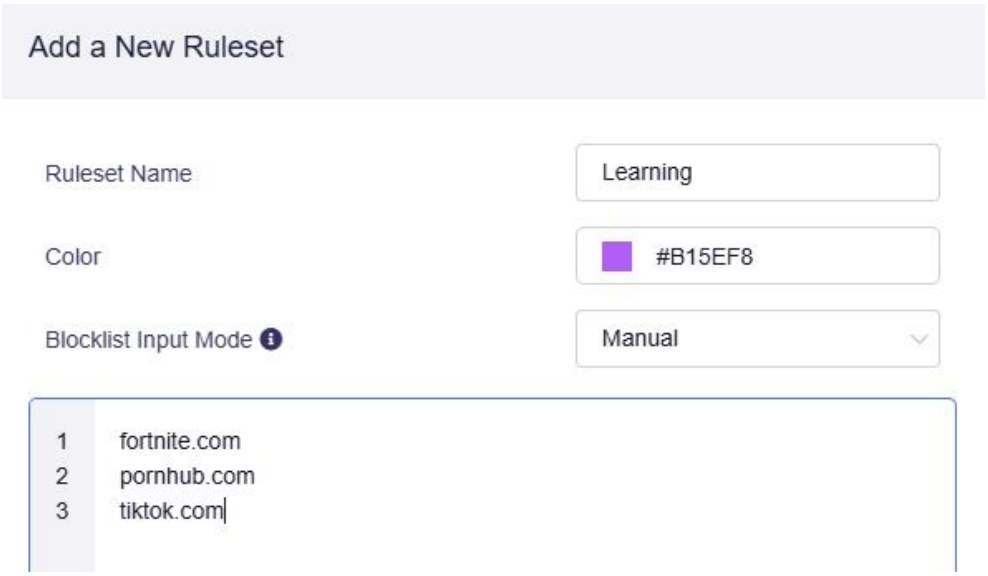


3. Establezca el límite de acceso.

Hay dos conjuntos de reglas predeterminados: **Bloquear acceso a Internet** y **Sin límite**. Haga clic en **Agregar un nuevo conjunto de reglas** para crearcrear dos conjuntos de reglas más para usarlos más adelante: **Aprendizaje** y **Jugar**.

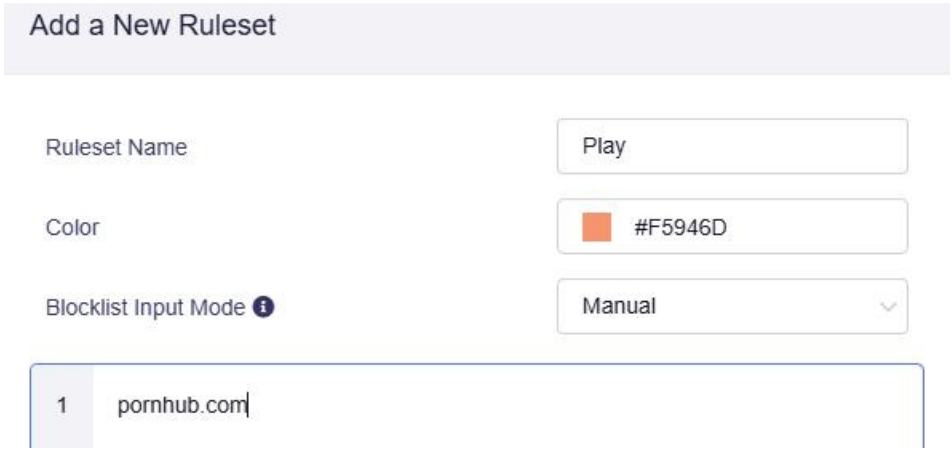


Especifique el nombre del conjunto de reglas (p. ej., Aprendizaje) y color, ingresa a la websitios tpara bloquear, tluego haga clic en **Aplicar**.

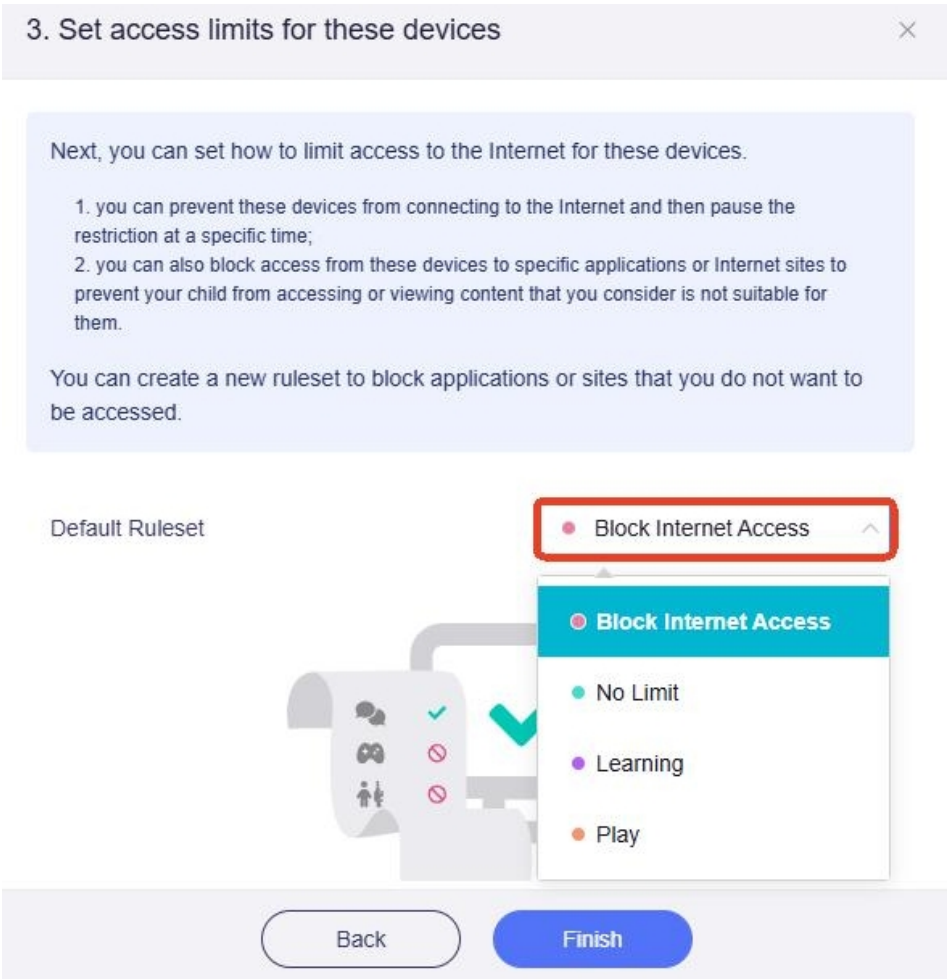


Nota: Los nombres de dominio ingresados en la lista de bloqueo deben incluir sus subdominios. Por ejemplo, si se ingresa "ejemplo.com", también incluye cualquier subdominio, como "subdominio.example.com".

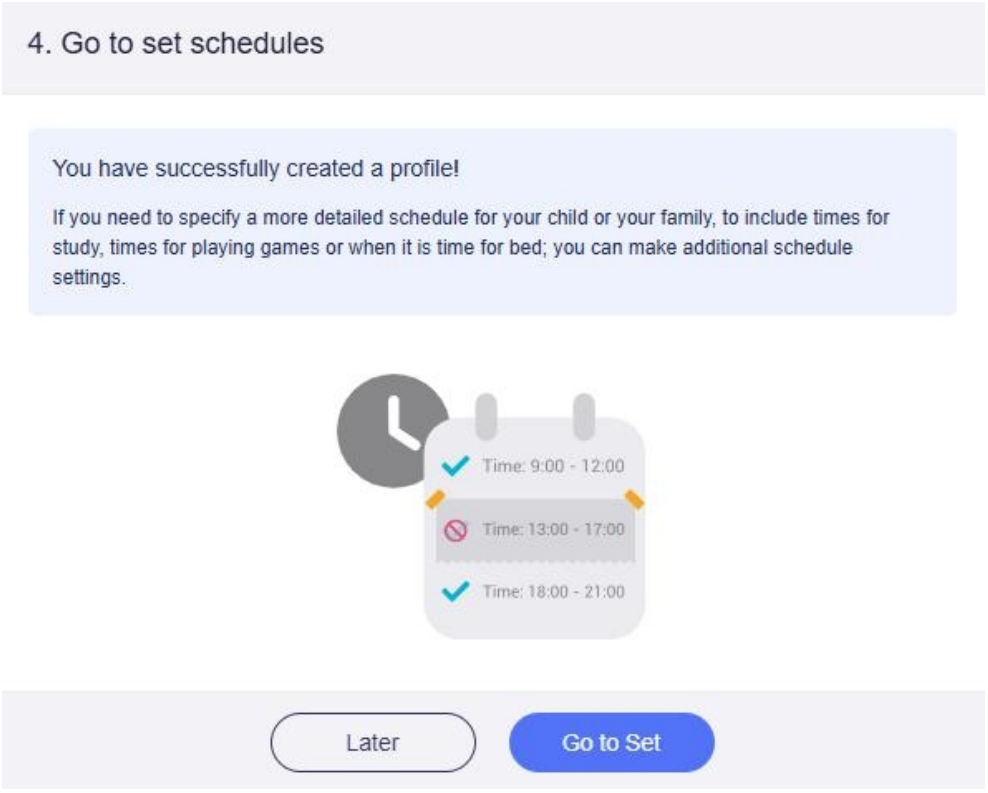
Del mismo modo, cree otro conjunto de reglas. Especifique el nombre del conjunto de reglas (por ejemplo, Reproducir) y el color, ingrese los sitios web que desea bloquear y luego haga clic en **Aplicar**.



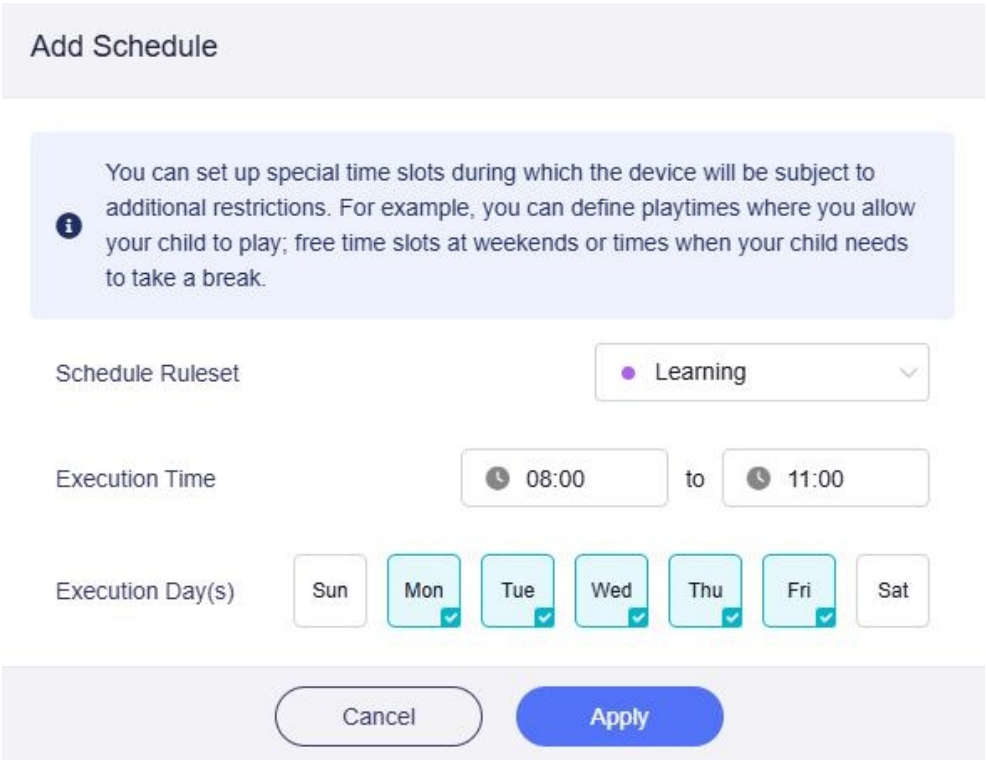
Al aplicared, habrá un total de cuatro conjuntos de reglas. Sseleccione **Bloquear acceso a Internet** como el **predeterminado Conjunto de reglas** y haga clic en **Finalizar**.



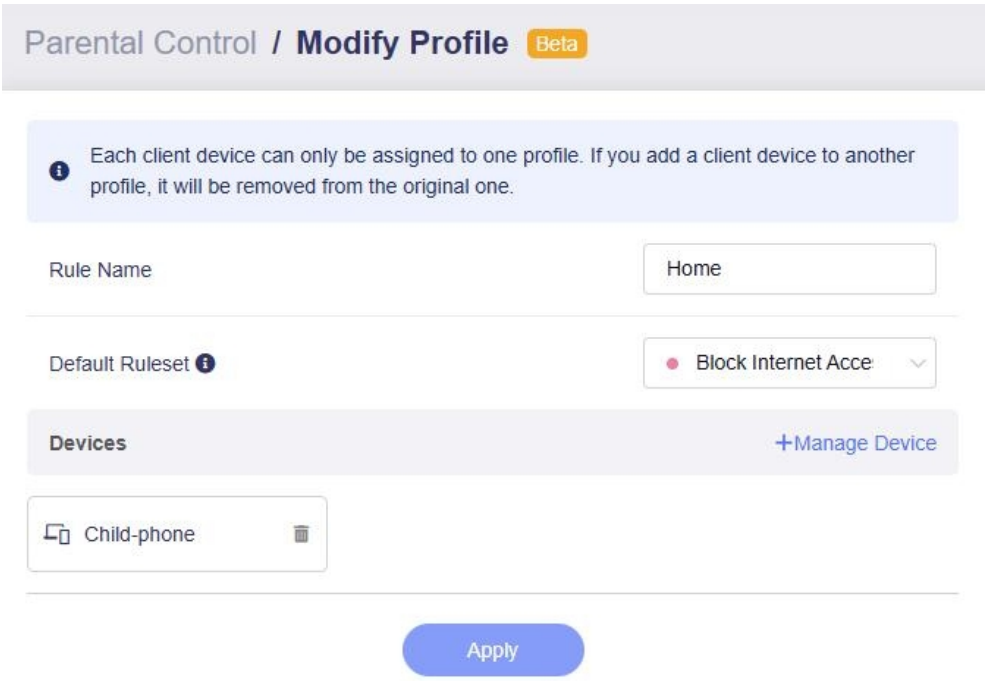
4. A continuación, establezca la programación para su perfil. Haga clic en **Ir a Establecer**.



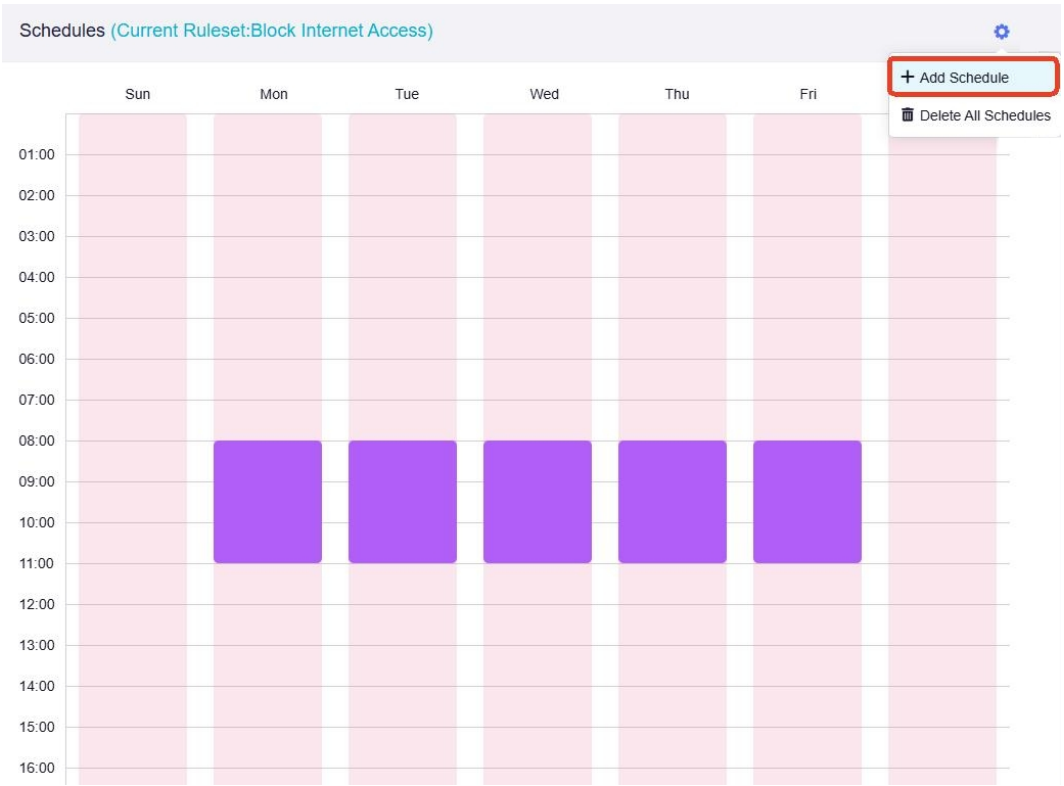
Agregue el **Aprendizaje** conjunto de reglas al cronograma. Establezca el **Hora de ejecución** de 8 a. m. a 11 a. m. de lunes a viernes y luego haga clic en **Aplicar**.



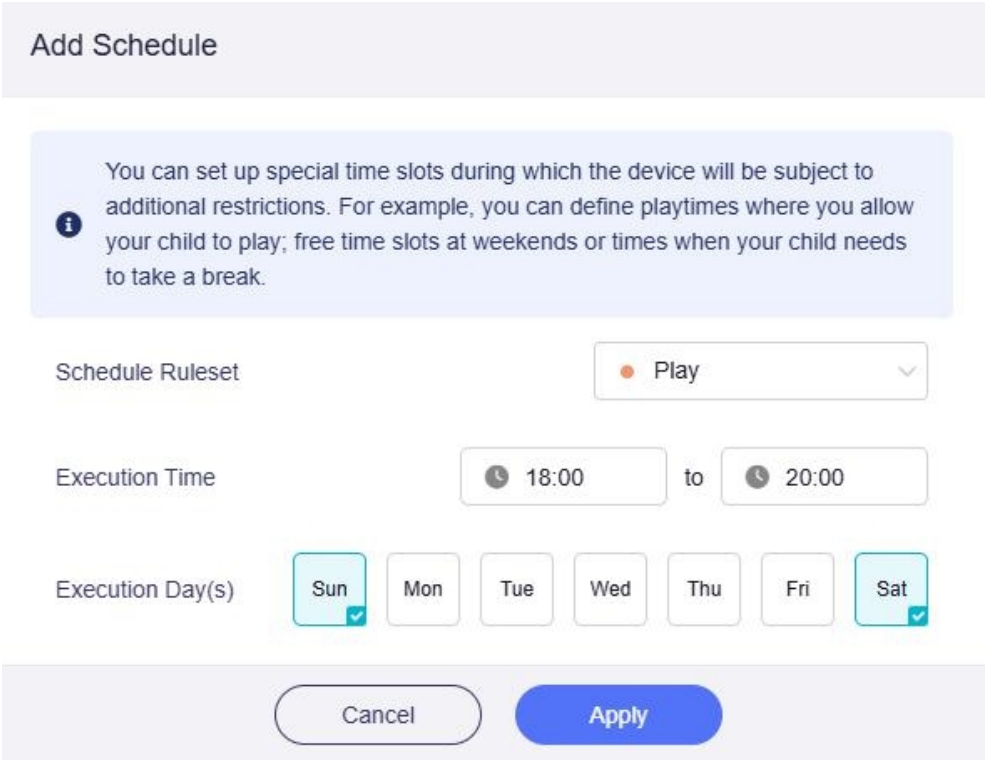
5. Será redirigido a la página de edición del perfil creado.



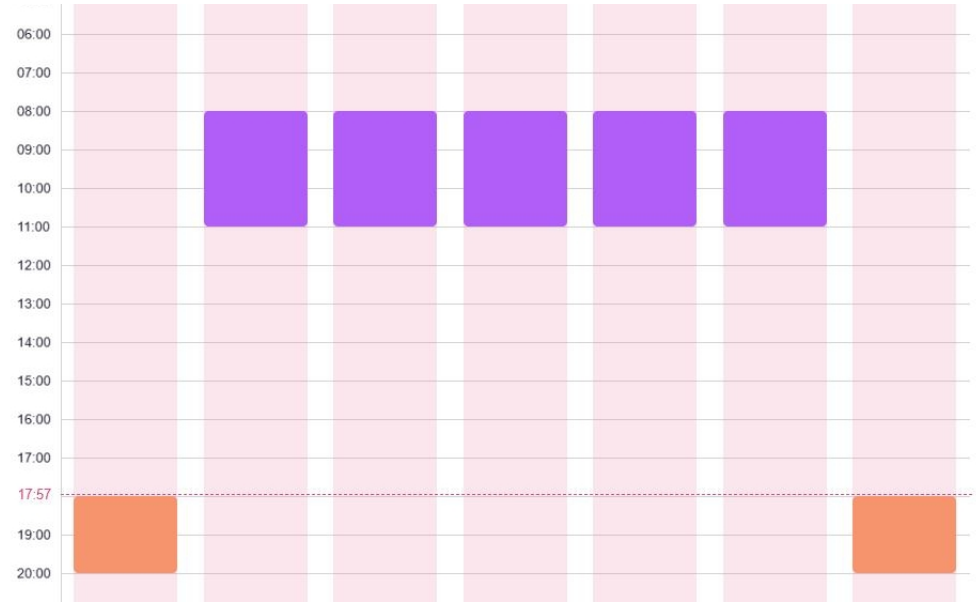
Vaya al final y verá que se ha creado un cronograma. Haga clic en el ícono de ajustes en la esquina superior derecha y seleccione **Agregar programación**.



6. Agregue otro conjunto de reglas **Reproducir** al cronograma. Establezca el **Tiempo de ejecución** de 6 PM a 8 PM en weekends, luego haga cliclick **Aplicar**.



El conjunto de reglas de Play se agregará al cronograma.

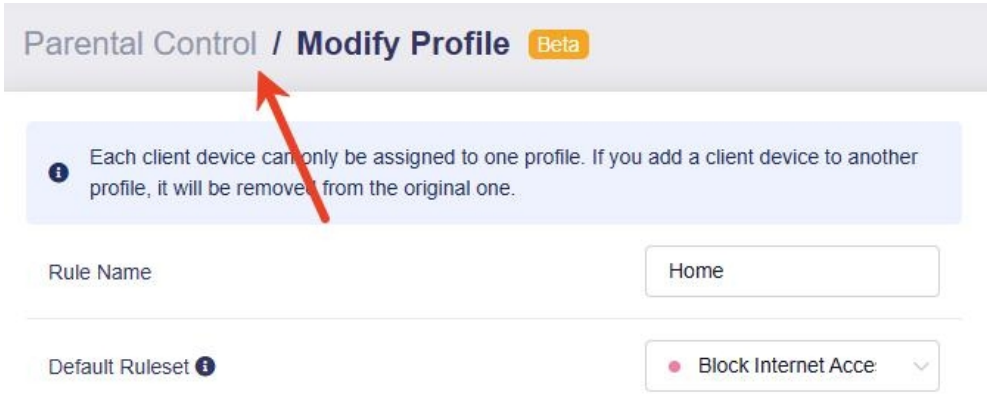


Consejos:

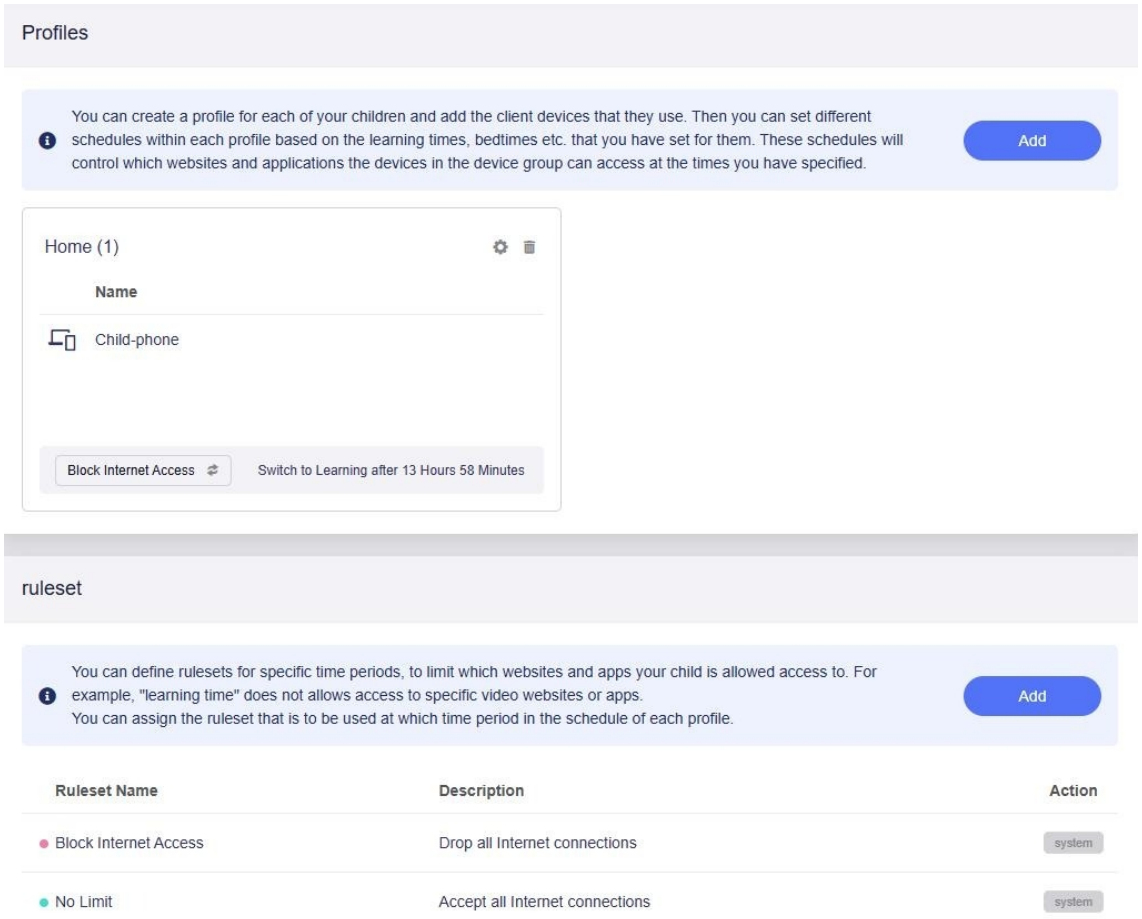
- La línea discontinua roja indica la hora actual.

- Ypuedes modificar el tiempo de ejecución haciendo clic en en un cierto conjunto de reglas en la programación.

7. Haga clicick **Control parental** en la parte superior para volver a la página Control parental.



Verás la configuración final. El control parental ahora está entrando en vigor según el cronograma. Puede modificar los perfiles y conjuntos de reglas existentes, o agregar otros nuevos si es necesario.



13.5.2 Solución de problemas

Si los ajustes configurados no surten efecto, verifique lo siguiente posible causas.

1. Problema de caché de DNS.

   Los navegadores y sistemas operativos mantienen cachés de DNS, lo que puede retrasar la aplicación de cambios de configuración. Borre la caché de DNS para aplicar los cambios inmediatamente.

2. La programación del perfil aún no ha comenzado.
3. El nombre de dominio ingresado puede ser incorrecto.

   Mientras un sitio web es público Aunque el dominio es fácil de encontrar, los dominios API utilizados por las aplicaciones a menudo no están disponibles públicamente. Para localizar el dominio correcto, utilice una herramienta de captura de paquetes como Wireshark o busque la información relevante del dominio.

   Por ejemplo, al bloquear “www.google.com”, ingresar “google.com” ofrece mejores resultados que “www.google.com”.

4. El dispositivo de destino utiliza un dirección MAC aleatoria para cada conexión de red, que impides que las reglas de acceso entren en vigor. Desactivar aleatoria dirección MAC en el dispositivo de destino y luego vuelva a agregar el dispositivo a su perfil.

13.6 ZeroTier

ZeroTier es una red privada virtual (VPN) basada en software que permite comunicaciones seguras y cifradas entre dispositivos a través de Internet. Crea una red virtual privada que permite que los dispositivos se comuniquen como si estuvieran en la misma red local, independientemente de su ubicación física o topología de red. ZeroTier está diseñado para ser fácil de configurar y usar, y ofrece funciones como cifrado de extremo a extremo, segmentación de red y capacidades de puente de red.

La función ZeroTier en los enrutadores GL.iNet permite que el enrutador se una a una red virtual ZeroTier, lo que permite el acceso remoto al enrutador, así como a sus recursos WAN y LAN.

Nota:

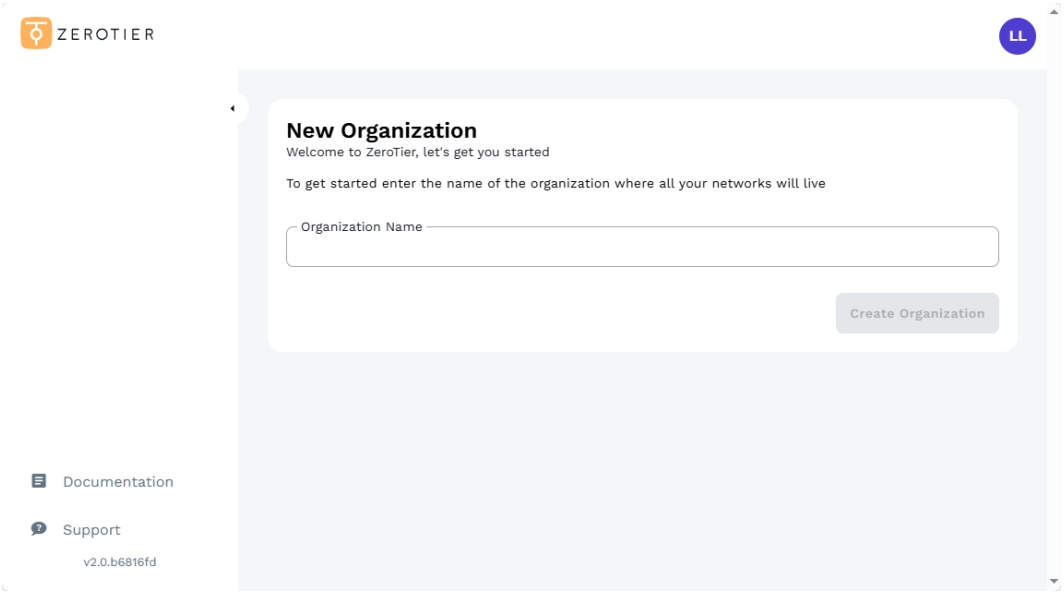
1. No se recomienda utilizar ZeroTier simultáneamente con cualquiera de las siguientes funciones o servicios, ya que esto puede causar conflictos de enrutamiento: Cliente OpenVPN, Cliente WireGuard, GoodCloud Site to Site, Tailscale y AstroWarp.
2. Esta función se encuentra actualmente en versión beta y puede tener algunas errores.

13.6.1 Configurar ZeroTier

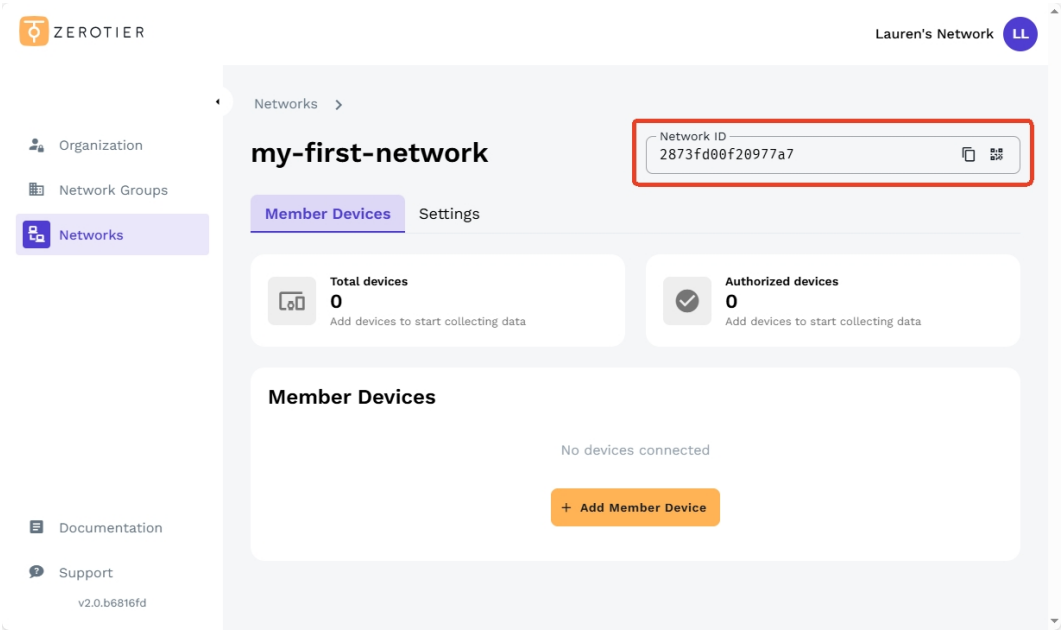
Hay dos versiones de ZeroTier Central disponibles: New Central y Legacy Central.

Los siguientes pasos utilizan New Central como ejemplo.

1. Visite [sitio web oficial de ZeroTier](#) e inicie sesión con su cuenta.
2. Cree una organización.

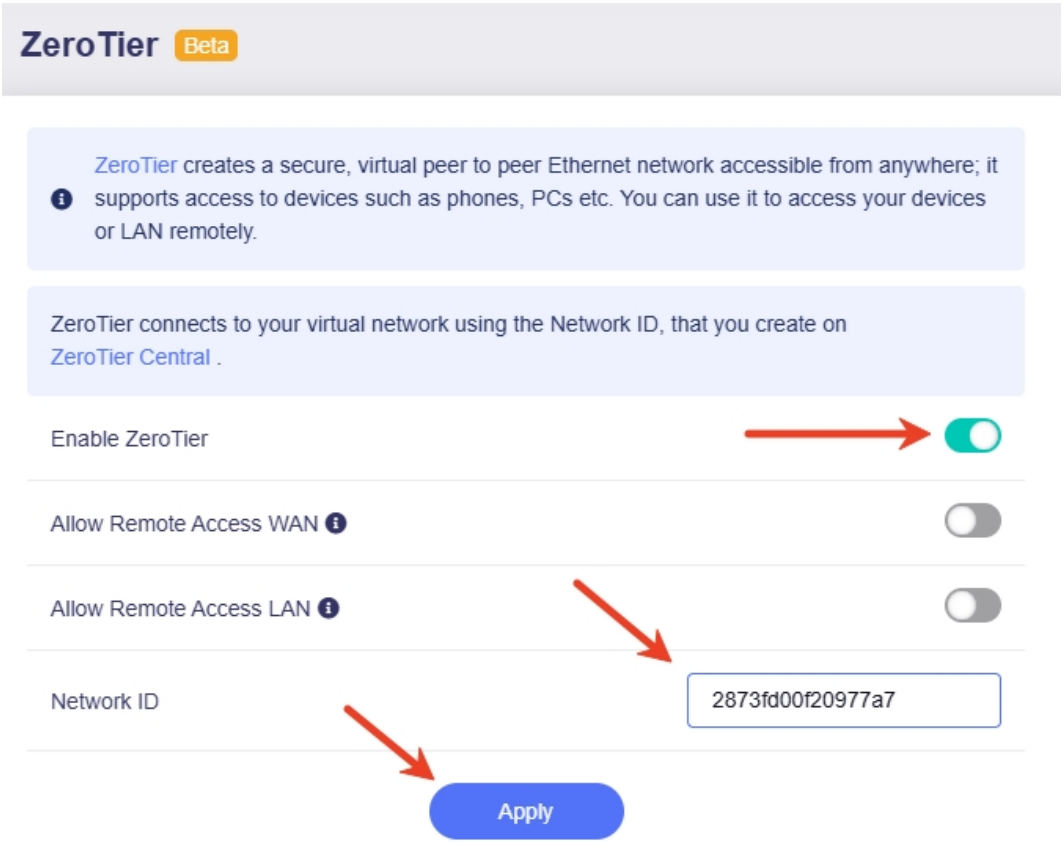


3. Seleccione un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

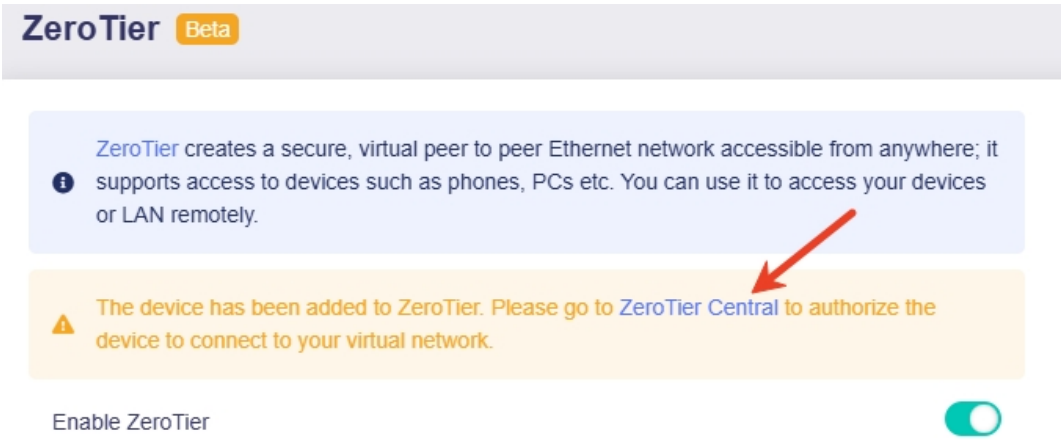


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesario cuando conecte otros dispositivos más adelante.

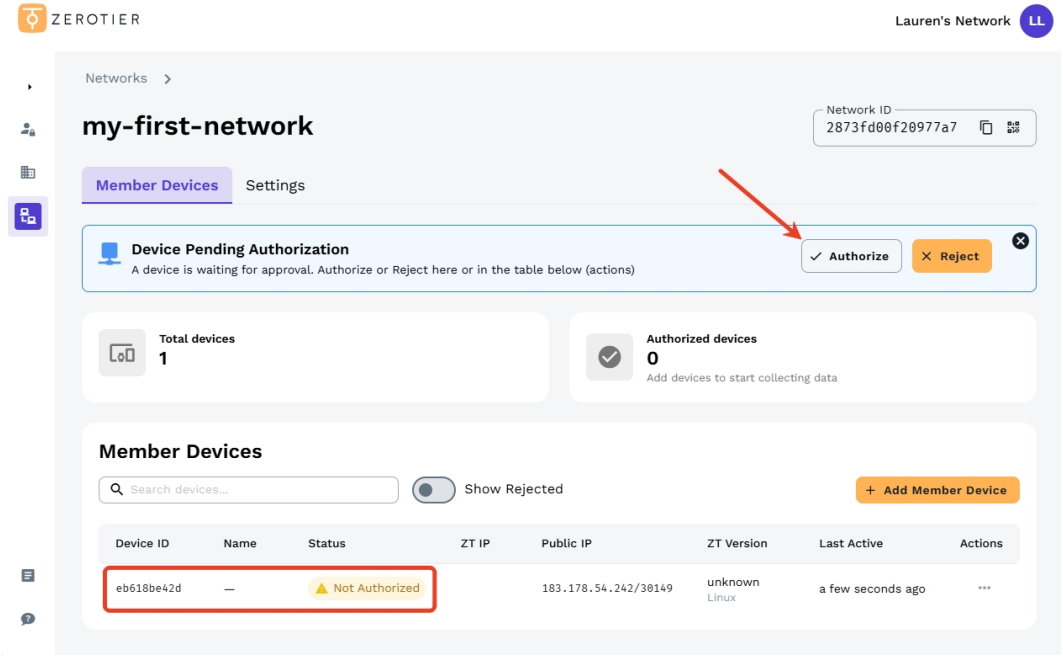
5. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **APLICACIONES** -> **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



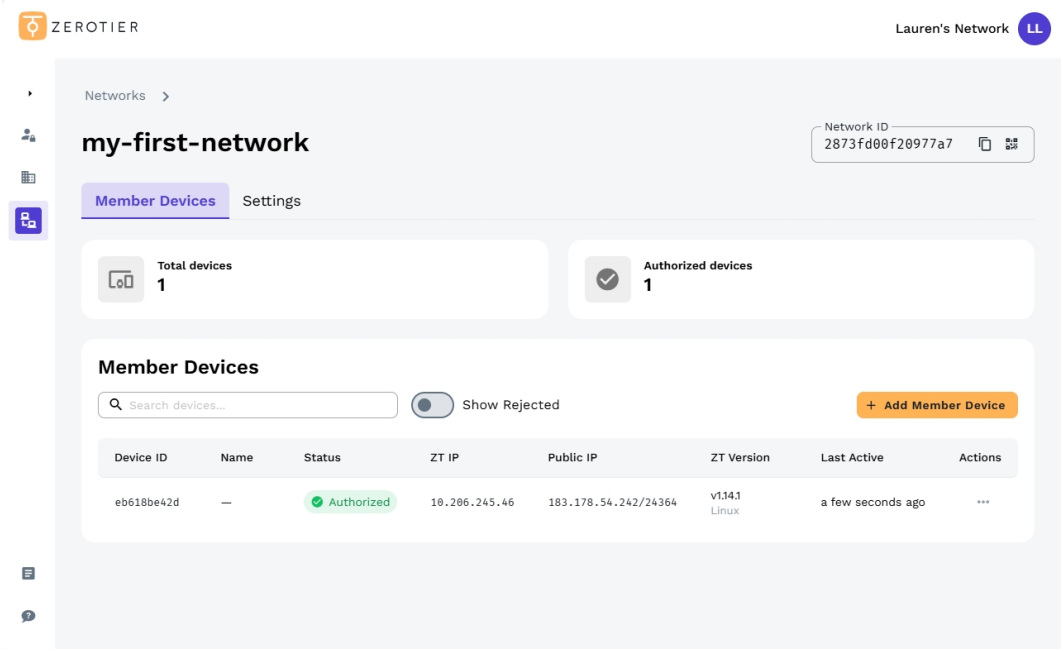
Después de un momento, página indicará que se requiere autorización. Haga clic en el **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



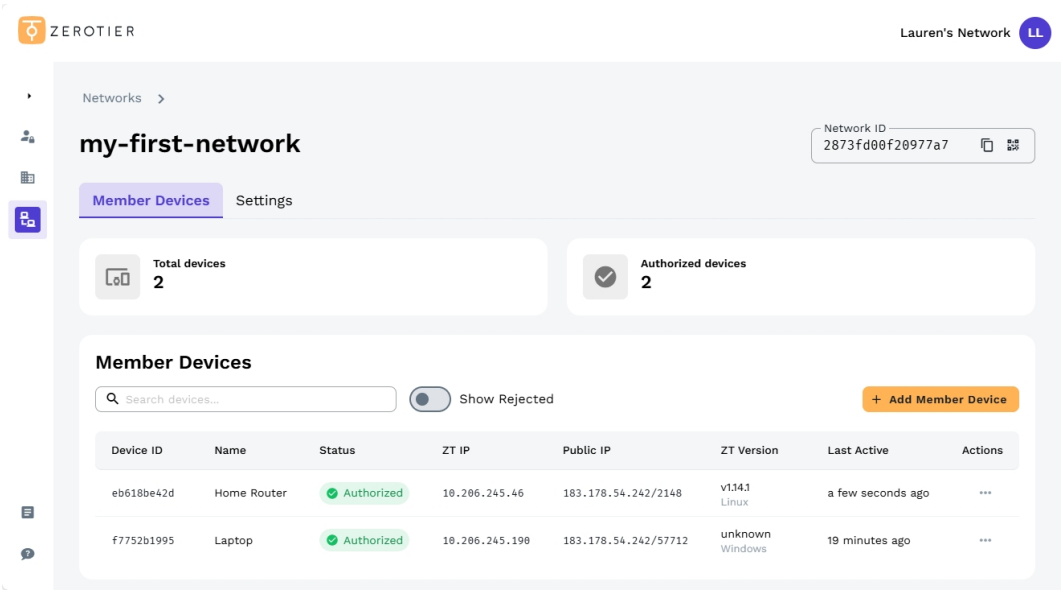
6. En ZeroTier Central, localice el dispositivo pendiente y autorícelo.



Una vez autorizado, la página se muestra de la siguiente manera.

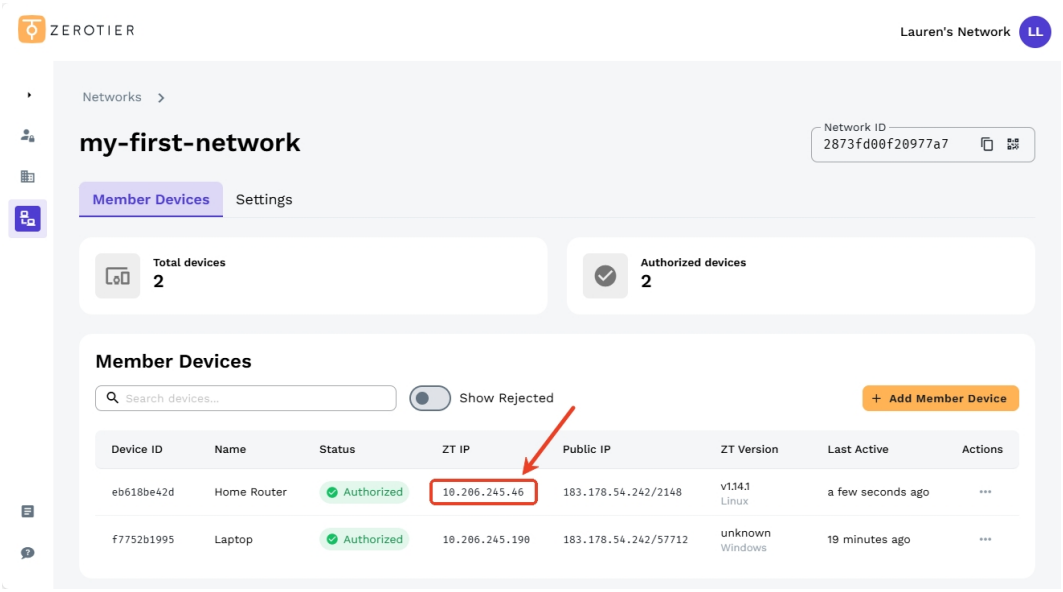


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, la página se muestra de la siguiente manera. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP administrada** y **IP pública**.



Consejo: puede hacer clic en el ícono de tres puntos a la derecha para editar la configuración del dispositivo miembro, incluido el nombre del dispositivo, las IP administradas y la configuración avanzada.

8. Haga clic en la **IP administrada** del enrutador para copiarla.



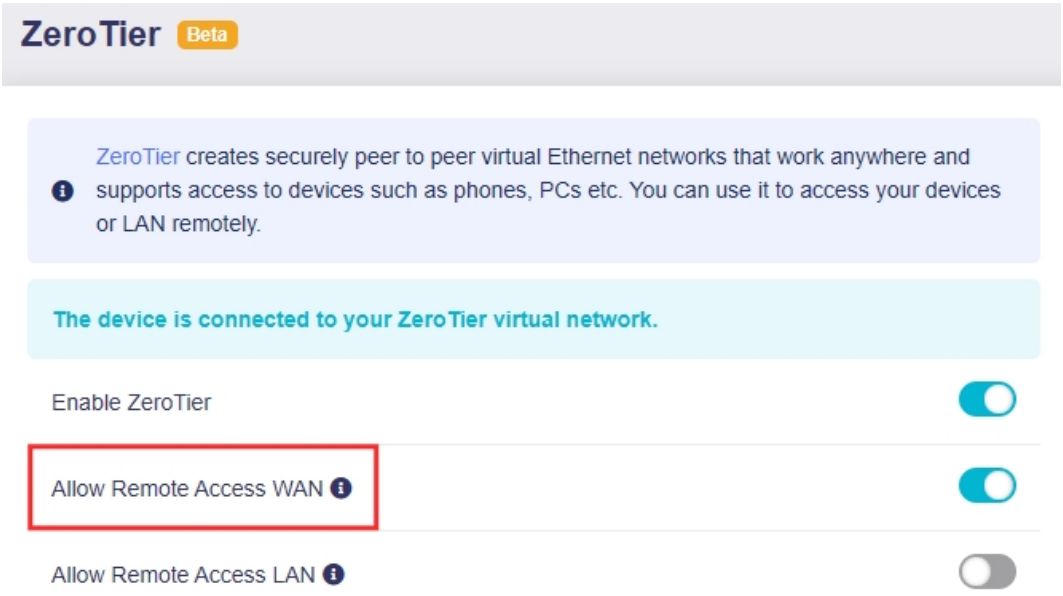
Luego puede usar esta IP administrada para acceder al enrutador desde su computadora portátil que está en la misma red ZeroTier.

9. Pruebe la conectividad.

   En la computadora portátil conectado a la misma red ZeroTier, abra un navegador web e ingrese la IP administrada del enrutador obtenida en el paso anterior. Si puede acceder al Panel de administración web del enrutador, la conexión ZeroTier se realizó correctamente.

13.6.2 Permitir el acceso remoto a la WAN

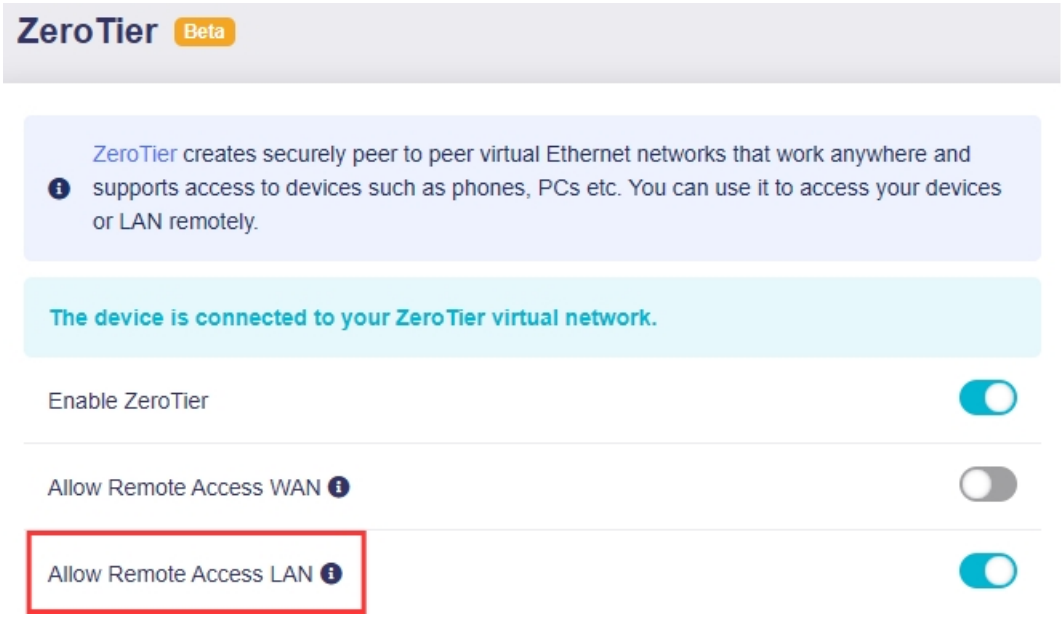
Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta función requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que entre en vigor. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puede configurar rutas personalizadas con un plan Essential o superior. Precio de nivel ceroprecio

13.6.3 Permitir el acceso remoto a la LAN

Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta característica requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que surta efecto. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puedes configurar rutas personalizadas con un plan Essential o superior. Precio de nivel ceroprecio

13.7 Tailscale

Tailscale es un servicio VPN que hace que sus dispositivos y aplicaciones personales sean accesibles en todo el mundo, de forma segura y sin esfuerzo.

La función Tailscale en los enrutadores GL.iNet permite que el enrutador se una a una red virtual Tailscale, lo que permite el acceso remoto al enrutador mismo, así como a sus Recursos del lado WAN y LAN.

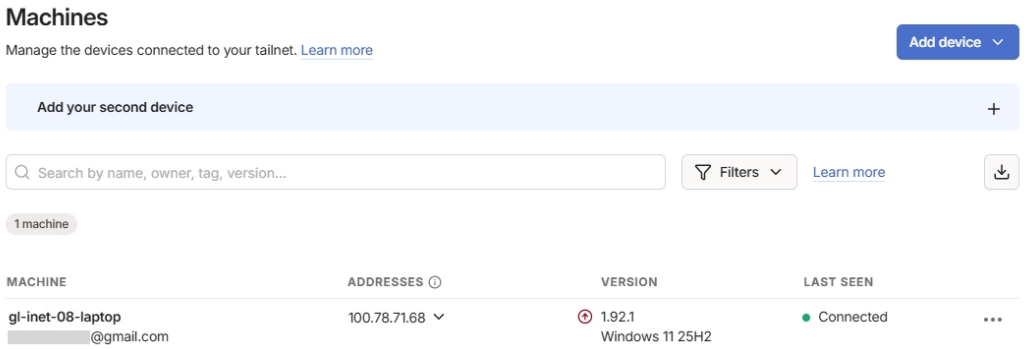
Nota:

1. Dado que Tailscale se basa en WireGuard, no se recomienda utilizar Tailscale con cualquiera de las siguientes características o servicios simultáneamente, ya que esto puede causar conflictos de enrutamiento: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier, AstroWarp.
2. Esta función se encuentra actualmente en versión beta y puede tener algunos errores.
3. Los enrutadores GL.iNet aún no están disponibles como nodos de salida. Esta función estará disponible en el firmware v4.9 y posteriores.

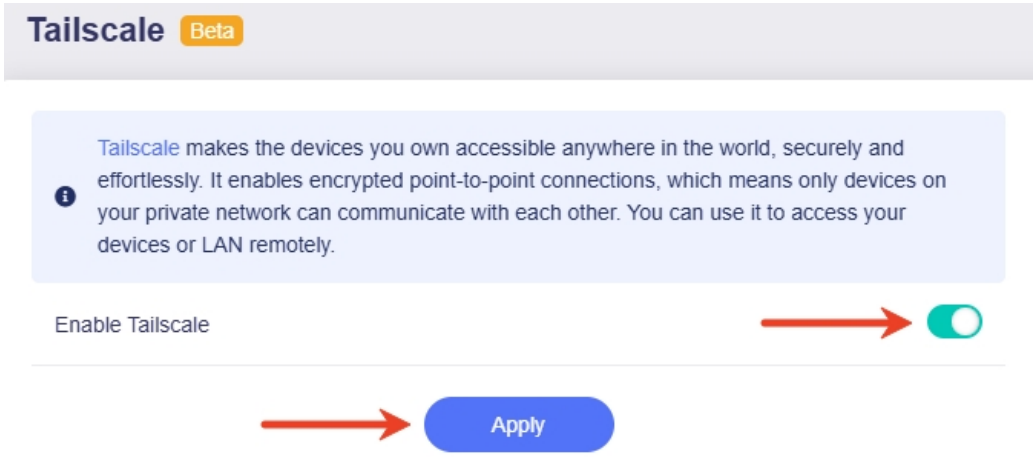
13.7.1 Configurar Tailscale

A continuación se utiliza una Beryl AX (GL-MT3000) y una computadora portátil como ejemplo.

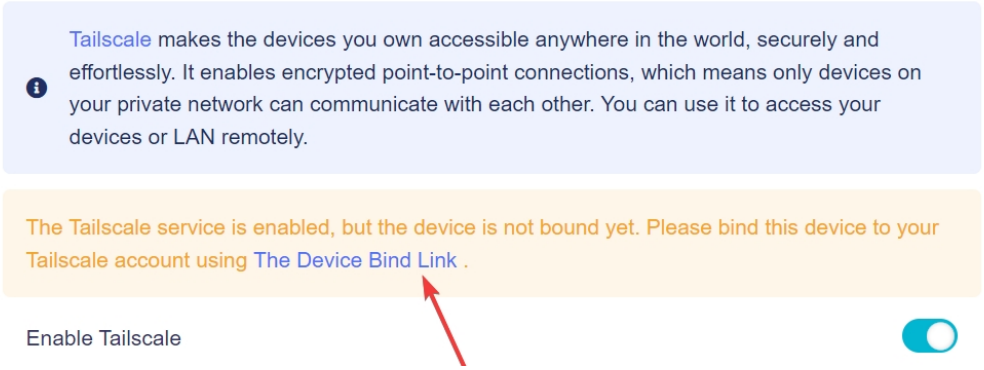
1. Rregistre primero una cuenta de Tailscale y vincule uno o dos dispositivos a su cuenta de Tailscale fo fines de prueba. Después de vincular, verá sus dispositivos en la suela Tailscale C.



2. Inicie sesión en la web de su enrutador' panel de administración y navegue hasta **APLICACIONES** > **Tailscale**. Activar **Habilitar Tailscale** y haga clic en **Aplicar**.



3. La página le indicará para vincular el dispositivo. Haga clic en **Enlace de vinculación del dispositivo**.



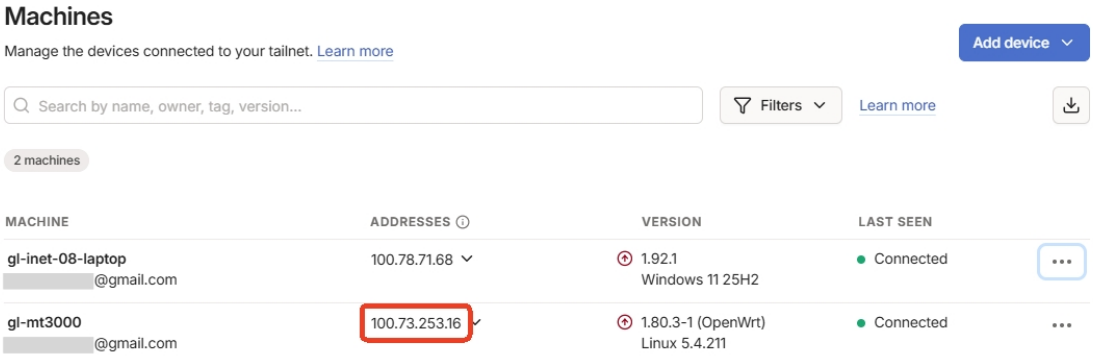
4. En el ventana emergente, haga clic en el enlace e inicie sesión con su cuenta de Tailscale.



5. Una vez que haya iniciado sesión, se le pedirá que confirme el dispositivo. Haga clic en **Conectar**.



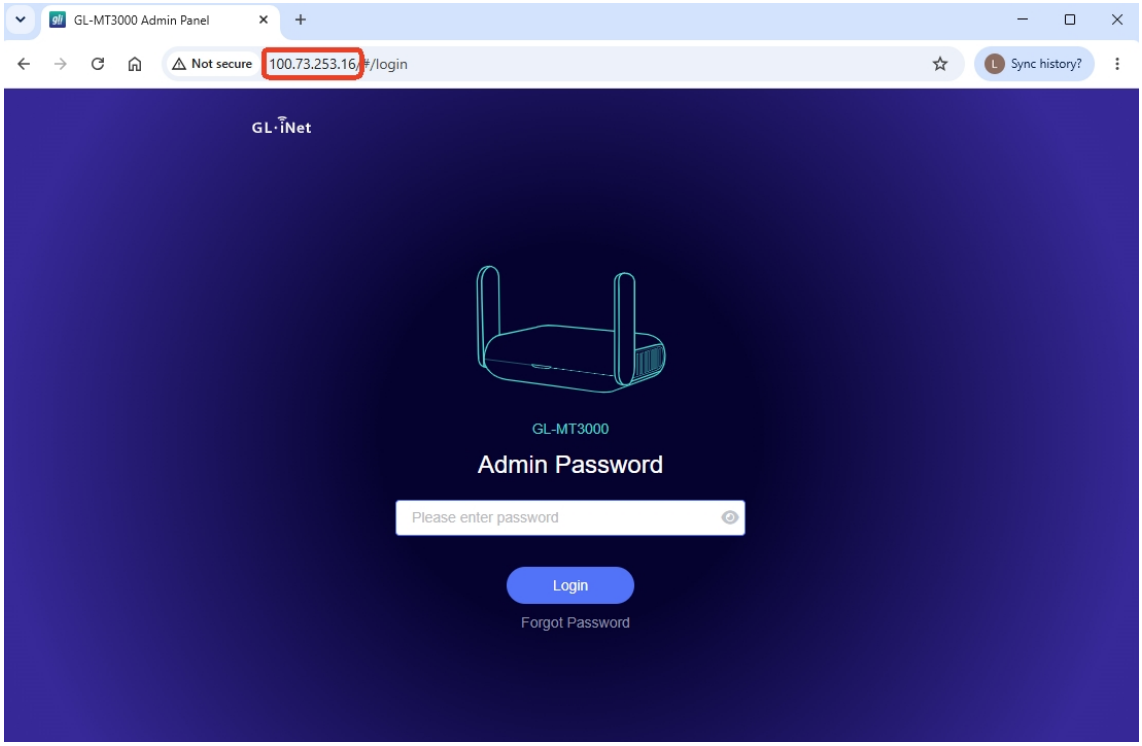
6. Yserá entonces será redirigido a Tailscale consola de administración. Ahora el enrutador se ha agregado a la red virtual de Tailscale y se puede acceder a él de forma remota mediante la IP virtual de Tailscale. **100.73.253.16**.



7. Pruebe la conectividad.

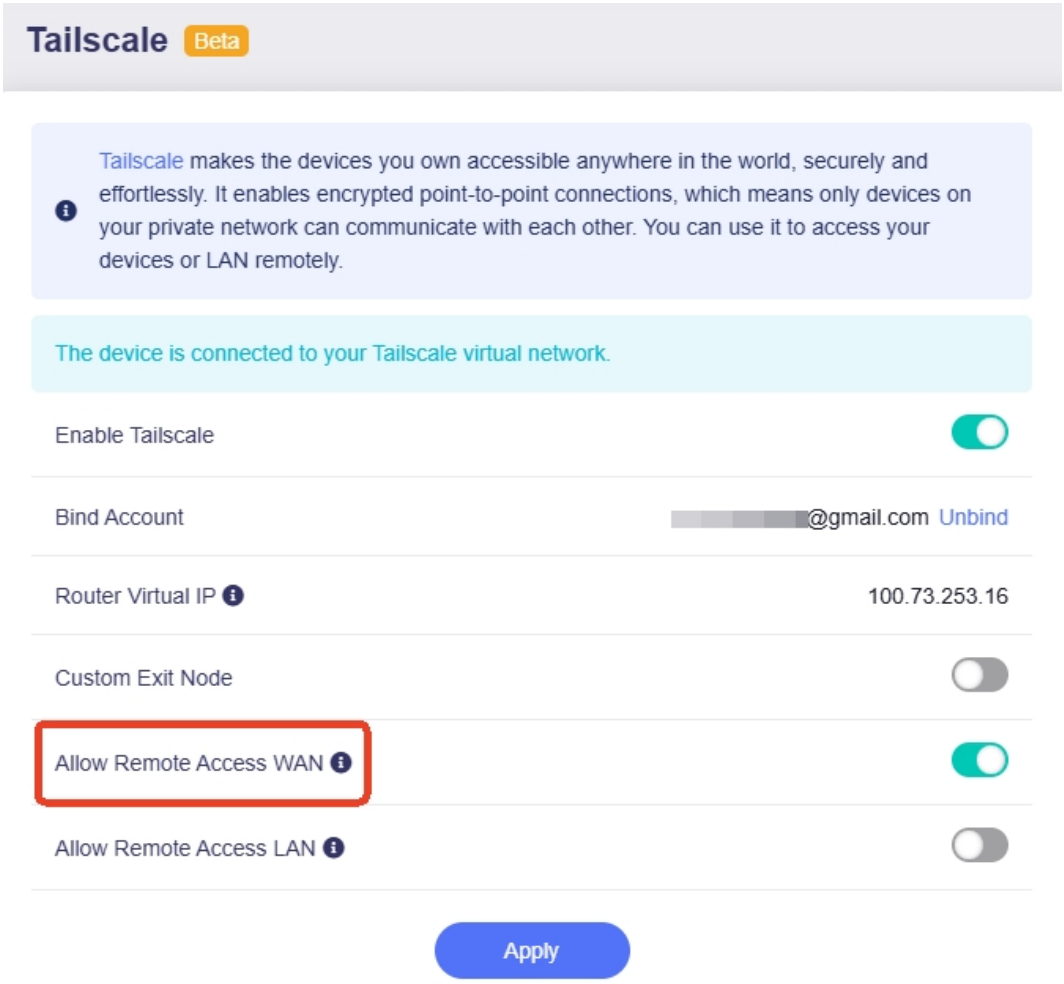
   En otro dispositivo conectado a la misma red de Tailscale, abra una página web. navegador e ingrese la IP virtual del enrutador en la barra de direcciones. Si puede acceder al panel de administración web del enrutador, significa que Tailscale está

funcionando. También puede usar el comando ping o iniciar sesión SSH en el terminal del enrutador’IP virtual en la barra de direcciones. Si puedes acceder al enrutador’panel de administración web, significa que Tailscale está funcionando. También puede utilizar el comando ping o iniciar sesión SSH en el enrutador’por su IP virtual para probar la conectividad.



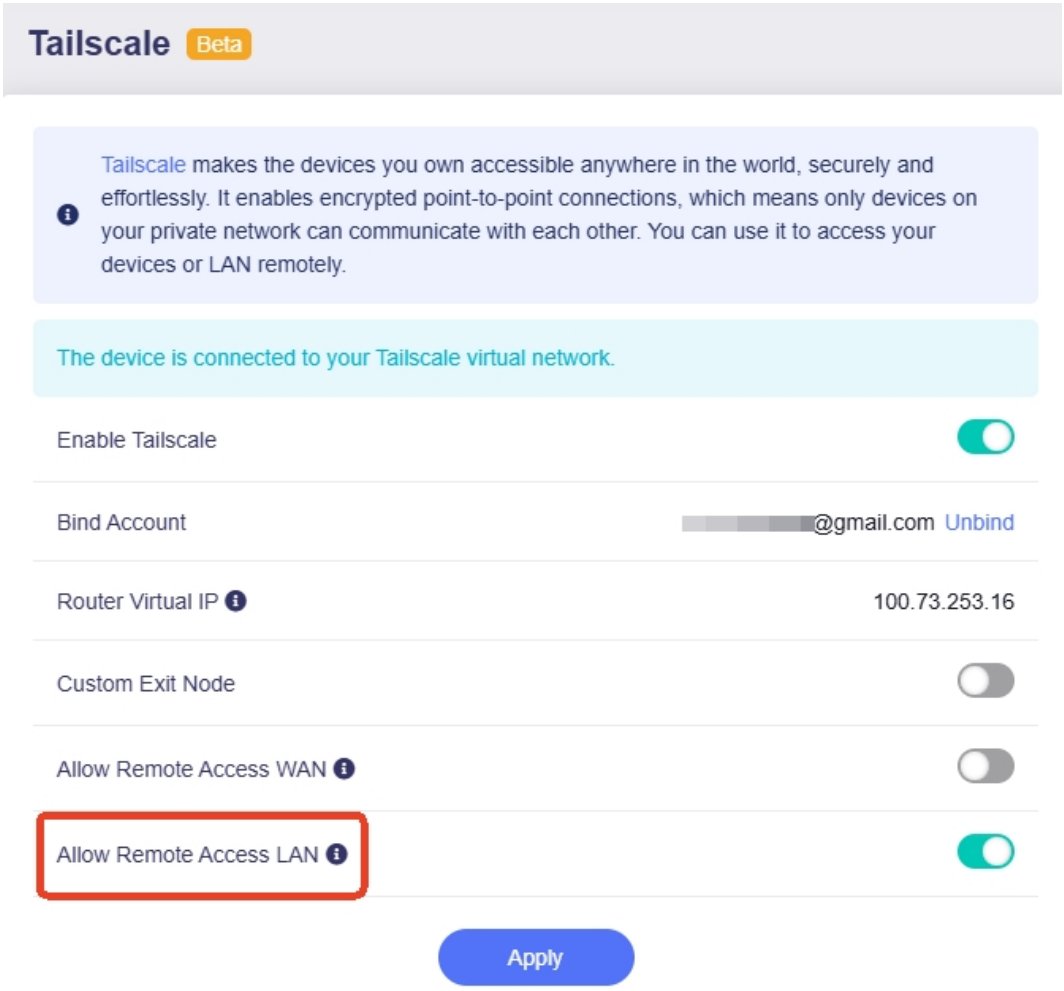
13.7.2 Permitir el acceso remoto a la WAN

Si esta opción está habilitada, los recursos en el lado WAN del dispositivo se puede acceder a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



13.7.3 Permitir el acceso remoto a la LAN

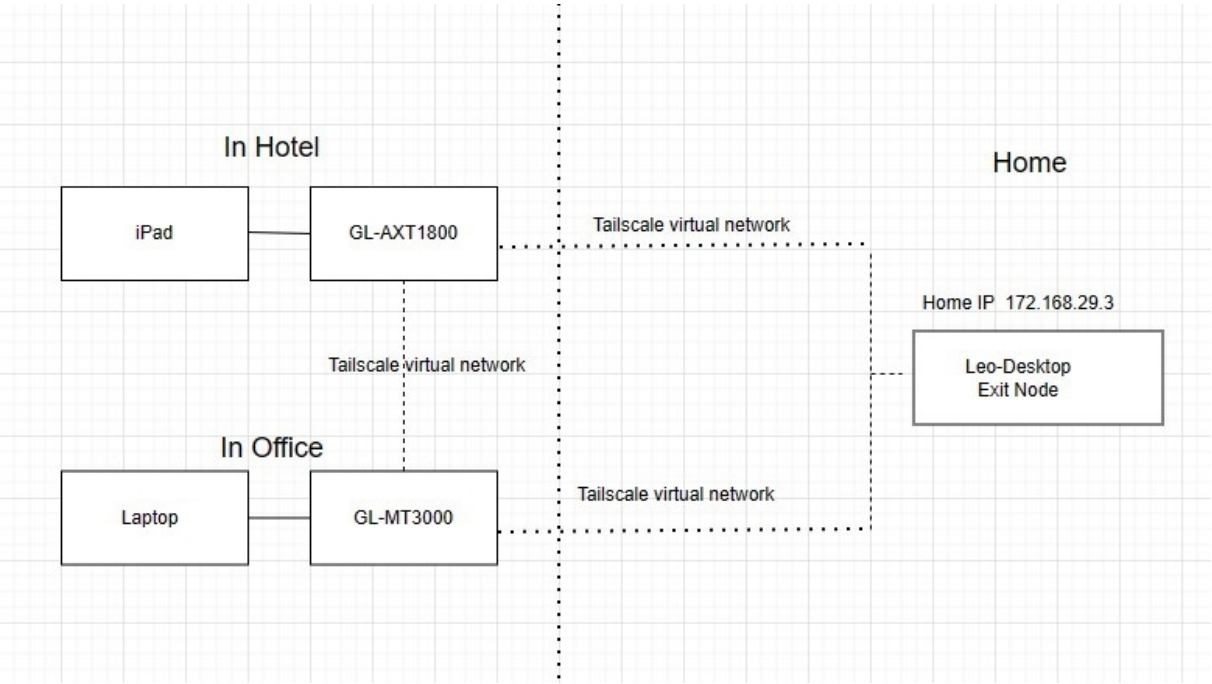
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



13.7.4 Nodos de salida personalizados

De forma predeterminada, Tailscale actúa como una superposición red: solo enruta el tráfico entre dispositivos que ejecutan Tailscale y no procesa su tráfico público de Internet, como cuando navega sitios web como Google.

Sin embargo, puede haber ocasiones en las que desee que Tailscale enrute su tráfico público de Internet. Por ejemplo, cuando está fuera de casa o viaja al extranjero, si necesita acceder a servicios en línea (como banca) que solo están disponibles en su país de origen, puede configurar el escritorio de su hogar con una IP pública como nodo de salida y configurar otros dispositivos en la misma Tailnet, como el GL-AXT1800 y el GL-MT3000 en la imagen a continuación, para enviar su tráfico a través de él. Esto permite que todo su tráfico público de Internet se reenvíe a través del nodo de salida.



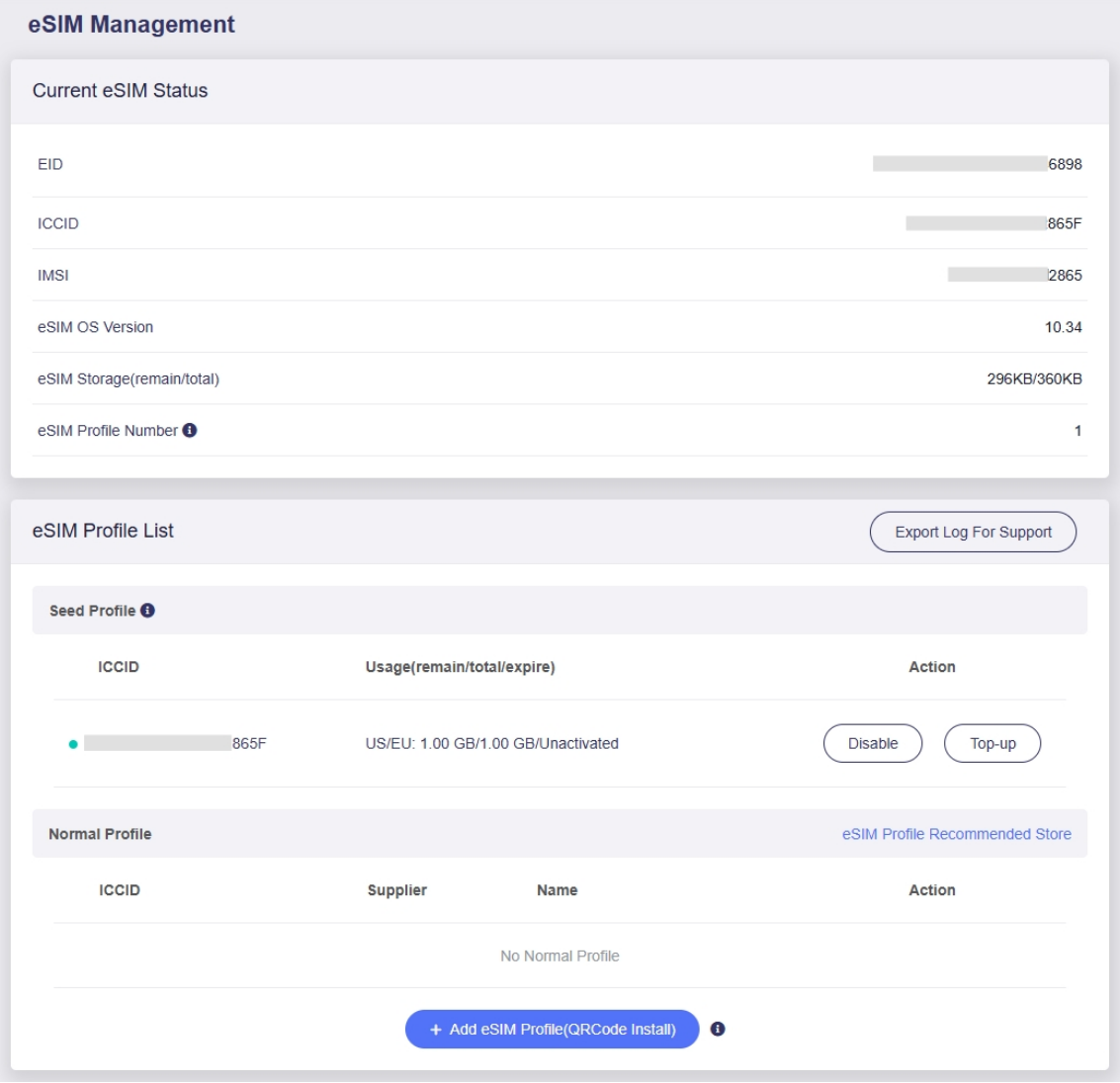
En resumen, un nodo de salida enruta el tráfico de Internet saliente desde sus dispositivos Tailnet, actuando efectivamente como servidores VPN. Cuando se conecta a un nodo de salida, todo su tráfico de Internet que no es de Tailscale parece originarse desde su ubicación, lo que le ayuda a acceder a contenido restringido geográficamente y mejorar su privacidad en línea. El dispositivo que maneja este reenvío de tráfico se conoce como "Exit Nodo". Para configurar un nodo de salida personalizado en enrutadores GL.iNet, consulte este tutorial.

Nota: Si el servidor DNS del enrutador es una dirección IP privada a la que solo se puede acceder en la red local, es posible que pierda el acceso a Internet cuando ejecute los nodos de salida. Para evitar esto, configure un servidor DNS público (por ejemplo, 8.8.8.8) manualmente para su enrutador.

13.8 Gestión de eSIM

Inicie sesión en el panel de administración web de su enrutador’span> y navega y navega a **APLICACIONES** > **Gestión de eSIM**.

Esta página le permite verificar el estado de la tarjeta física eSIM y administrar los perfiles de eSIM. dos partes: **Estado actual de la eSIM** y **Lista de perfiles eSIM**.



13.8.1 Estado actual de la eSIM

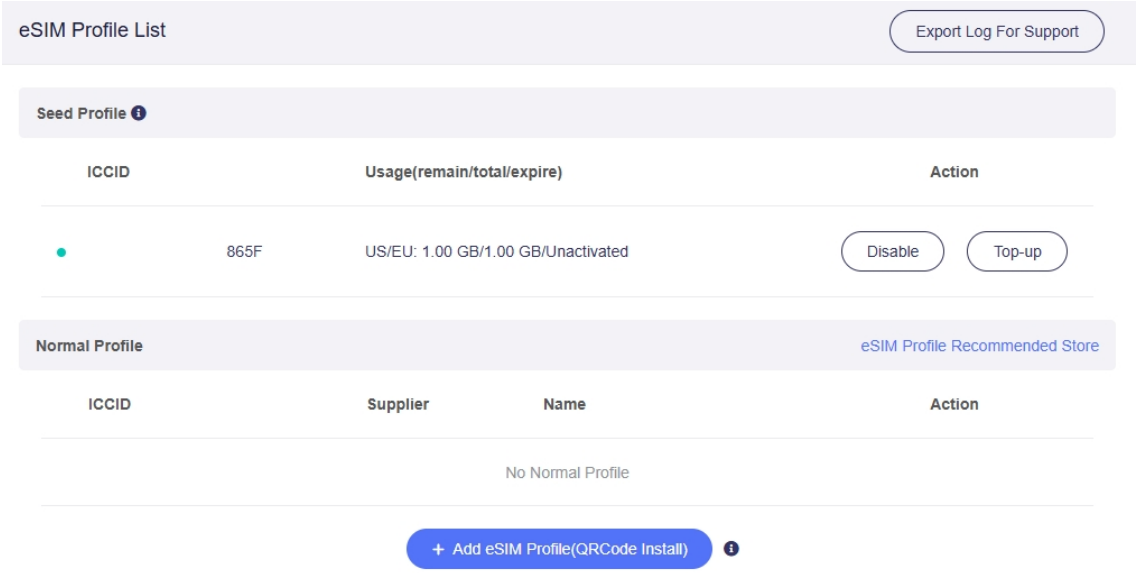
Esta sección muestra información básica y detalles sobre el perfil eSIM actualmente activo.



- **EID:** El identificador único global de la eUICC (chip eSIM), utilizado para la identificación y la gestión de perfiles.
- **ICCID:** El identificador de tarjeta de circuito integrado del perfil eSIM actualmente activo.
- **IMSI:** La identidad del suscriptor móvil internacional del perfil eSIM actualmente activo.
- **Versión del sistema operativo eSIM:** La versión del sistema operativo de eUICC, que define su compatibilidad y soporte capacidades.
- **Almacenamiento eSIM (restante/total):** Capacidad de almacenamiento total y disponible en la eUICC para almacenar perfiles eSIM.
- **Número de perfil eSIM:** Número de perfiles eSIM almacenados actualmente en la eUICC. Tenga en cuenta que los perfiles eSIM ofrecidos por diferentes operadores varían en tamaño, por lo que la cantidad de perfiles que se pueden almacenar en la eUICC también será diferente.

13.8.2 Lista de perfiles eSIM

Esta sección muestra información sobre el perfil inicial de eSIM y los perfiles normales.



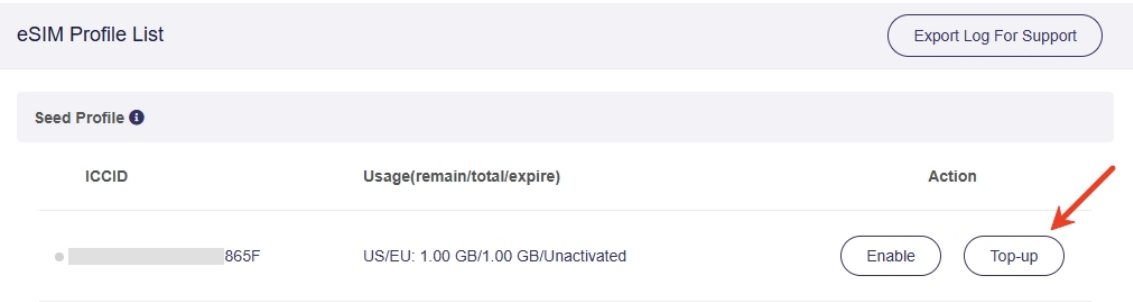
- **Perfil semilla**: el perfil semilla viene precargado con 1 GB de datos gratuitos para EE. UU. y Europa, además de 100 MB de datos globales, válidos por 1 año a partir de la fecha de activación. Estos datos le permiten descargar otros perfiles en cualquier parte del mundo. También puede monitorear el uso del perfil de semillas, incluidos los datos restantes, la asignación total de datos y la fecha de vencimiento.
- **Perfil normal**: si compras un perfil eSIM y lo cargas mediante un código QR o un código de activación, el perfil se mostrará aquí.

13.8.2.1 Recargar el perfil inicial

GL.iNet proporciona un perfil inicial precargado con 100 MB de datos globales y 1 GB de datos válidos en Europa y EE. UU. para la configuración inicial y la activación del perfil eSIM. Este plan está diseñado para descargar nuevos perfiles eSIM cuando llegas a un destino sin acceso a Internet.

Si has agotado los datos gratuitos precargados, o si los datos gratuitos han caducado y deseas continuar usando el servicio, puedes recargar tu perfil inicial.

En la sección Perfil de semilla, haz clic en el botón **Recarga** a la derecha.



En la ventana emergente, escanea el código QR y sigue las instrucciones para completar tu recarga.



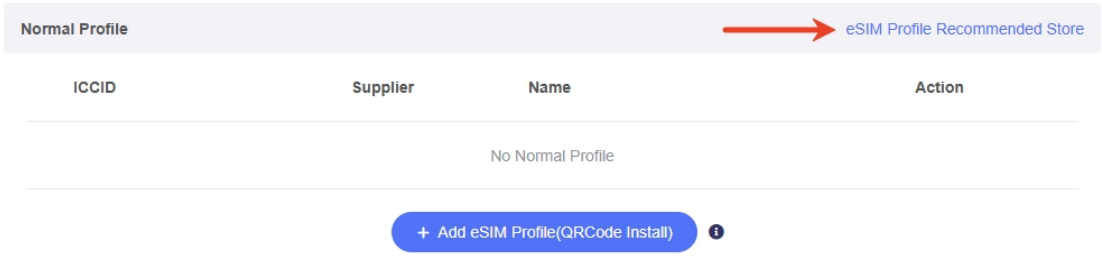
13.8.2.2 Comprar perfil eSIM

Puedes comprar perfiles eSIM en nuestras tiendas recomendadas, tiendas probadas u otros proveedores de eSIM externos.

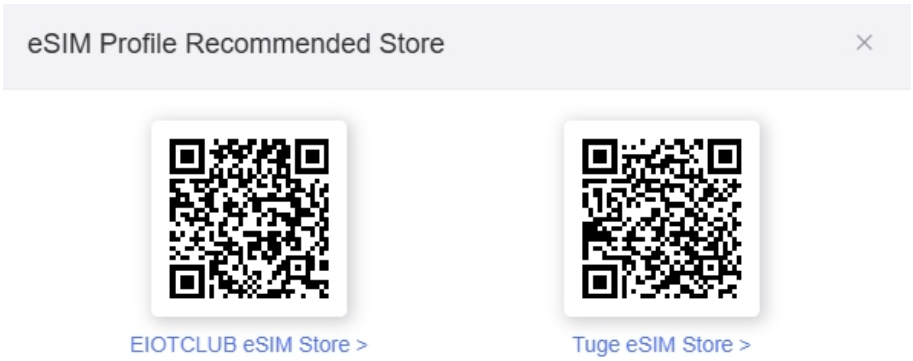
Opción 1: comprar from onu rrecomendado stiendas.

Hay dos tiendas recomendadas: EIOTCLUB eSIM Store y Tuge eSIM Store.

En la sección Perfil normal, haga clic en **Tienda recomendada del perfil eSIM** a la derecha.



Escanee el código QR o haga clic en los enlaces para comprar perfiles eSIM.



Nota: Todos los paquetes de perfiles eSIM adquiridos en estas dos tiendas son totalmente compatibles con los enrutadores GL.iNet. Si tiene alguna pregunta, comuníquese con nuestro equipo de soporte en support@gl-inet.com.

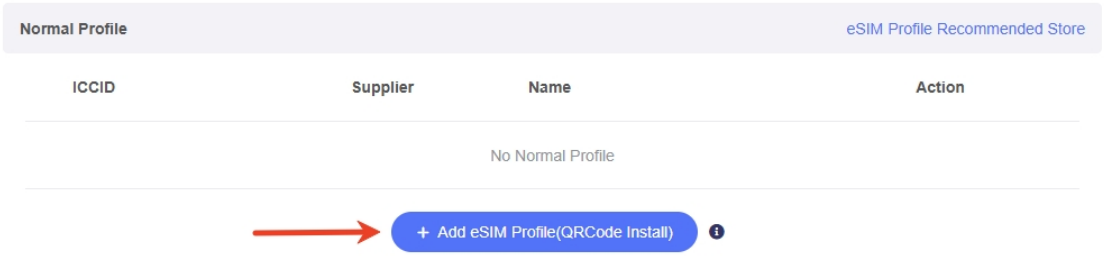
Opción 2: comprar fdesde tested salmacenamiento.
Consulte este enlace para ver una lista de tiendas probadas por GL.iNet.
Nota: No podemos garantizar la compatibilidad total con los enrutadores GL.iNet para todos los perfiles o paquetes de estas tiendas. Dado que GL.iNet no tiene asociaciones con ellos, no podemos brindar soporte posventa ni ayudar con los reembolsos.

Opción 3: comprar fdesde other third-party eSIM pproveedores.
También puedes optar por comprar perfiles eSIM de otros proveedores externos de tu elección. Sin embargo, no podemos garantizar la compatibilidad total con los enrutadores GL.iNet para perfiles eSIM comprados a otros proveedores externos. Compre a su propia discreción. GL.iNet no es responsable de ningún problema de incompatibilidad.
Para soporte posventa o reembolsos, comuníquese con el proveedor de eSIM correspondiente.

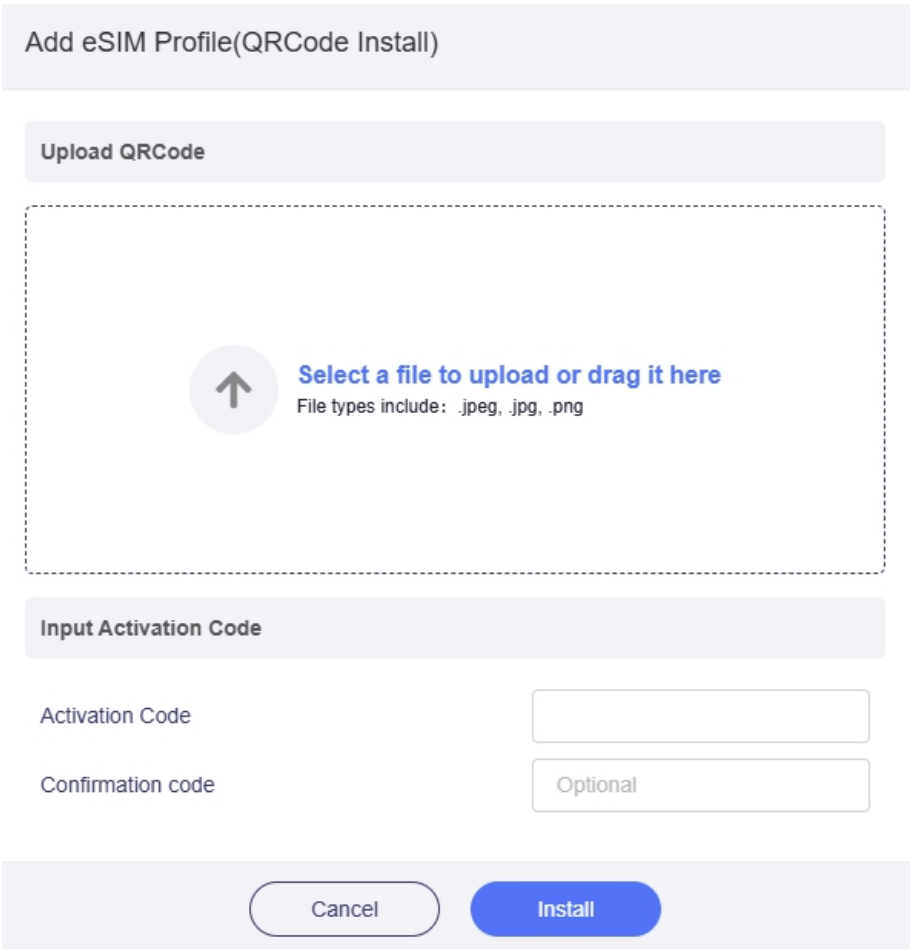
13.8.2.3 Cargar perfil eSIM

Después de comprar un perfil eSIM, normalmente recibirá un código QR (o un código de activación). Guarde este código QR localmente y luego siga los pasos a continuación para cargar su perfil eSIM.

1. En la sección Perfil normal, haga clic en **Agregar perfil eSIM** en la parte inferior.



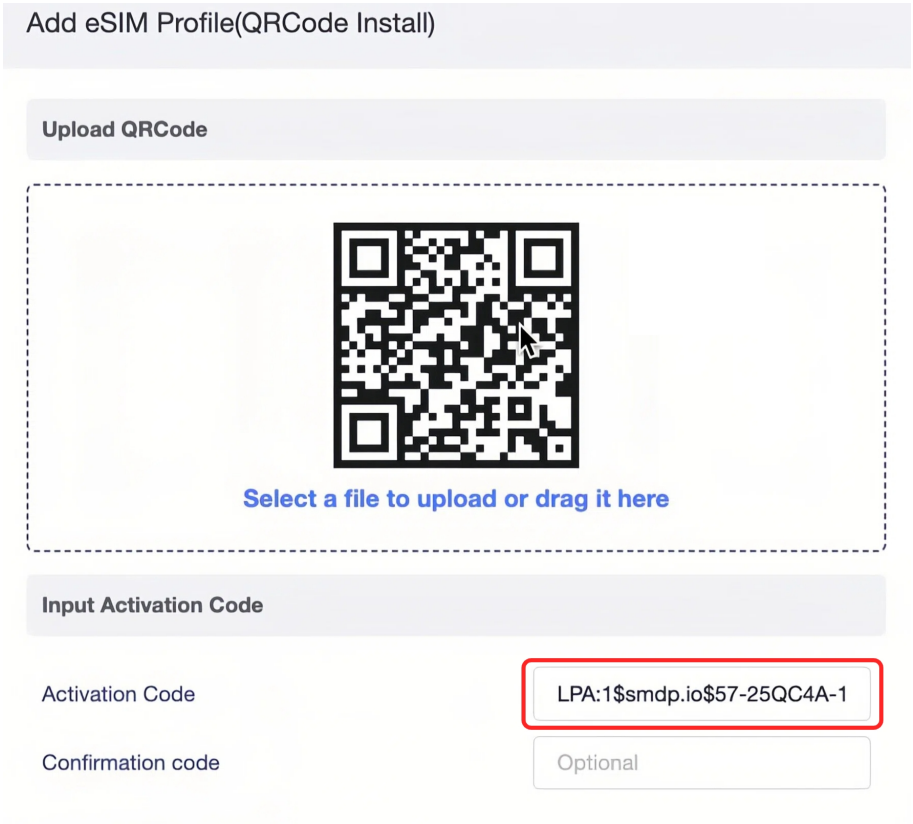
2. Cargue su código QR eSIM o ingrese el código de activación, luego haga clic en **Instalar**. Luego descargará e instalará el perfil eSIM en su enrutador.



Nota:

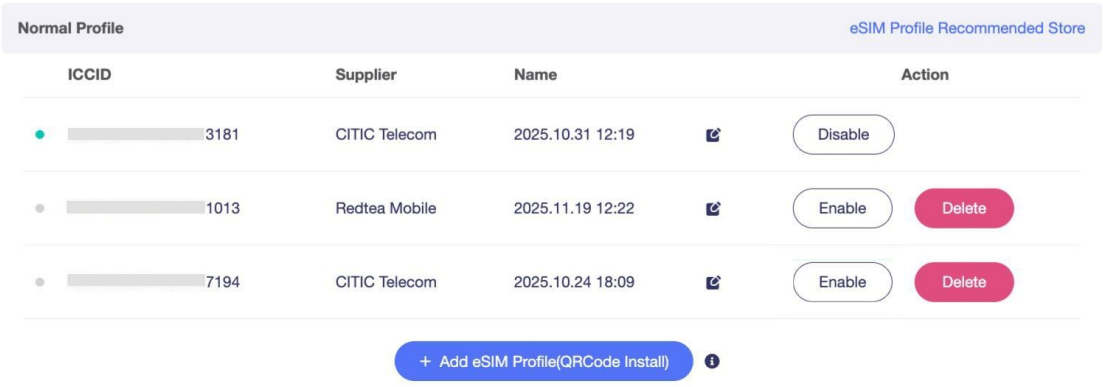
1. La mayoría de los perfiles eSIM solo se pueden descargar e instalar una vez.

2. Un código QR con el formato correcto mostrará un código de activación que comienza con **LPA:**. Sin embargo, es posible que algunos códigos QR no estándar solo proporcionen un código de activación sin formato sin el prefijo LPA. En este caso, agregue manualmente LPA: al principio del código antes de hacer clic en el botón Instalar.



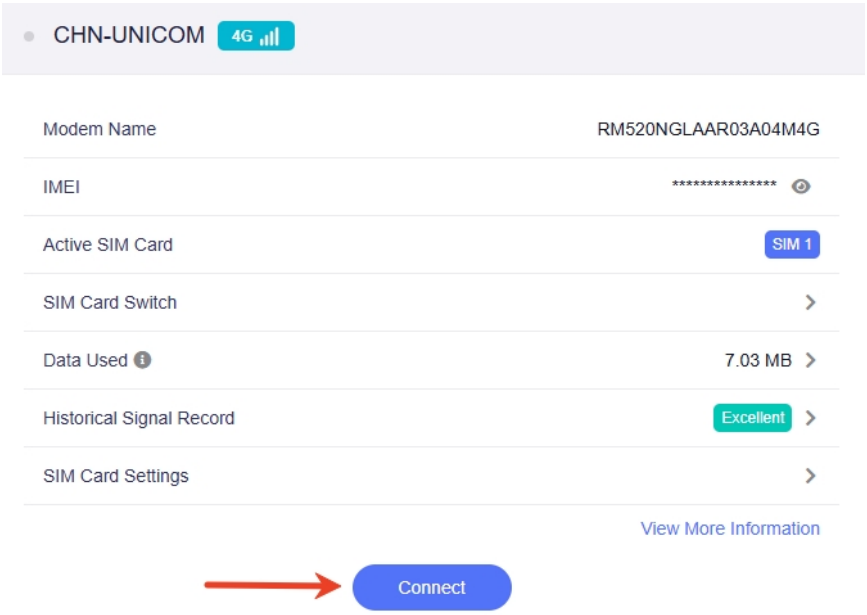
3. Si no ha comprado ningún perfil eSIM, puede comprar uno en la Tienda recomendada de perfiles eSIM. Consulta 13.8.2.2 Comprar perfil eSIM para obtener más detalles.

3. Después de una carga exitosa, tu nuevo perfil eSIM aparecerá en **Perfil normal** lista. Haga clic en **Activar** para activarlo.



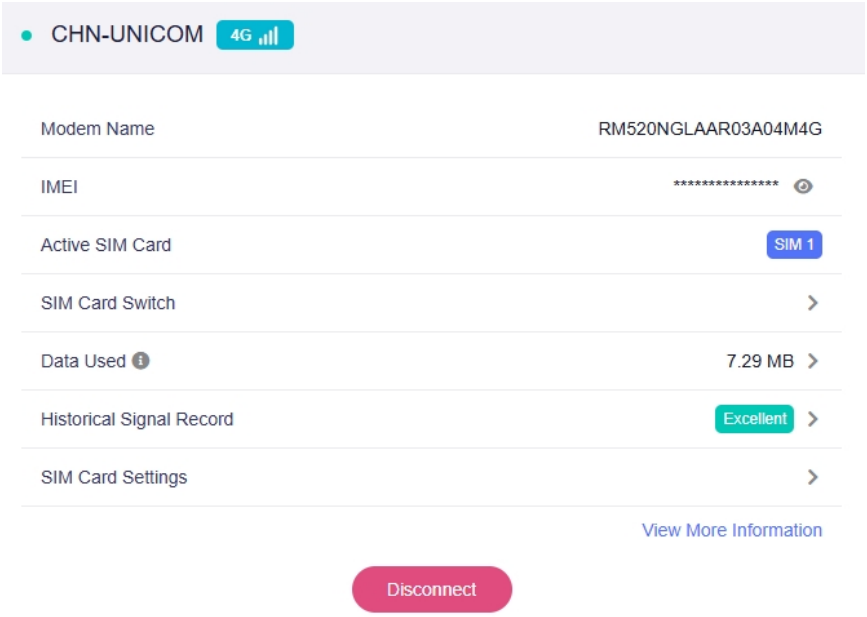
4. Conéctese a Internet.

   Después de habilitar el perfil eSIM, vaya a **INTERNET** > **Celular**. Haz clic en **Conectar** para establecer una conexión a Internet a través de tu perfil eSIM.



   Nota: Algunos perfiles eSIM pueden requerir configuración adicional, como ajustes de APN, PIN o TTL. Si es necesario, haga clic en **Configuración manual** o **Configuración de la tarjeta SIM** para ajustar estos parámetros. En algunos casos, es posible que tengas que reiniciar el dispositivo para establecer una conexión a Internet.

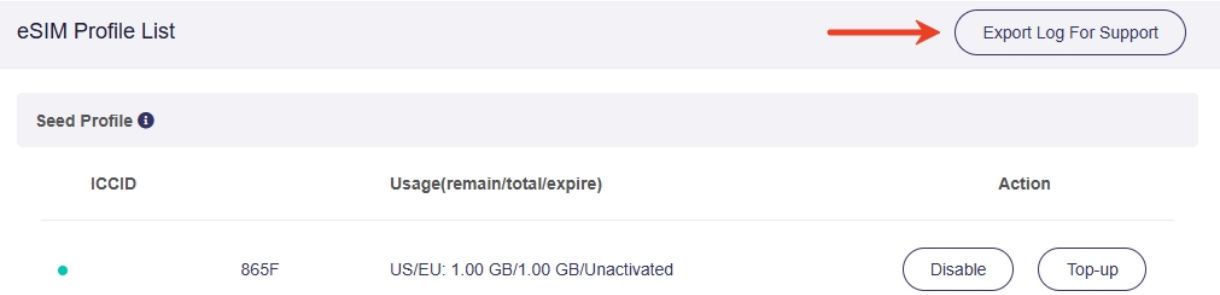
5. Una vez que el enrutador se conecta correctamente a través del perfil eSIM, la página se mostrará de la siguiente manera:



13.8.2.4 Exportar registro para soporte

Haga clic en **Exportar registro para soporte** para ver todos los registros relacionados con eSIM.

Si tiene algún problema y necesita soporte técnico, exporte los registros de eSIM y compártalos con nuestro equipo de soporte por correo electrónico a support@gl-inet.com.



Capítulo 14

Red

Este capítulo presenta los ajustes relacionados con la red para la configuración y administración, como LAN, DNS e IPv6.

14.1 Reenvío de puertos

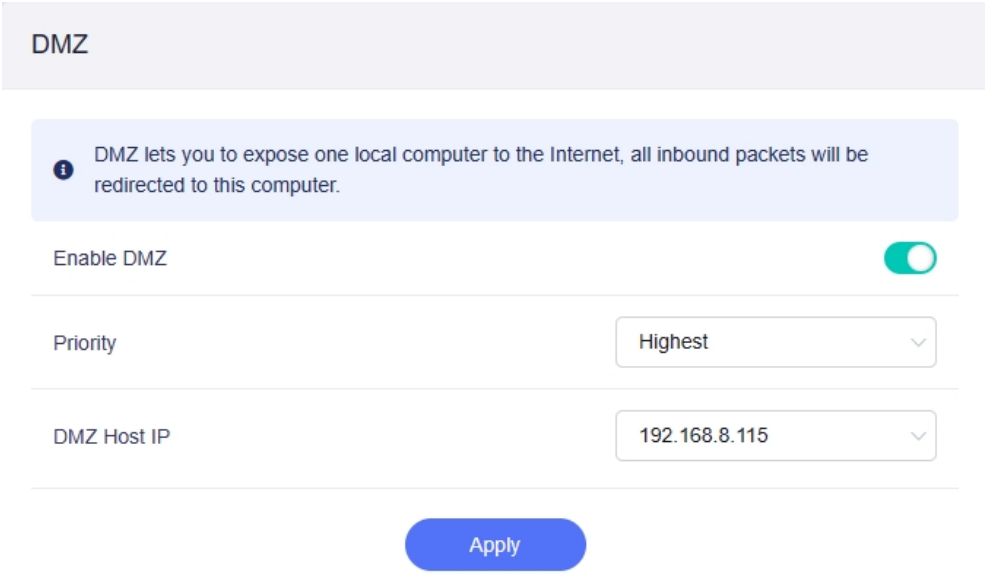
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos de dispositivos).

14.1.1 DMZ

DMZ le permite exponer una computadora a Internet, por lo que todos los paquetes entrantes serán redirigidos a esta computadora.le permite exponer una computadora a Internet, de modo que todos los paquetes entrantes serán redirigidos a esta computadora.

Siga los pasos a continuación para habilitar DMZ si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Reenvío de puertos** > **DMZ** sección.
2. Activar **Activar DMZ**. Sseleccione la Prioridad y la IP del host DMZ de la lista desplegable y haga clic en **Aplicar**.



- **Prioridad**: configúrelo como Máximo o Mínimo. Si la prioridad de la DMZ es mayor que las reglas de reenvío de puertos, todas las reglas de reenvío de puertos quedarán invalidadas. De lo contrario, las solicitudes se reenviarán al dispositivo cliente DMZ solo si el puerto al que se accede no tiene una regla de reenvío de puerto correspondiente.

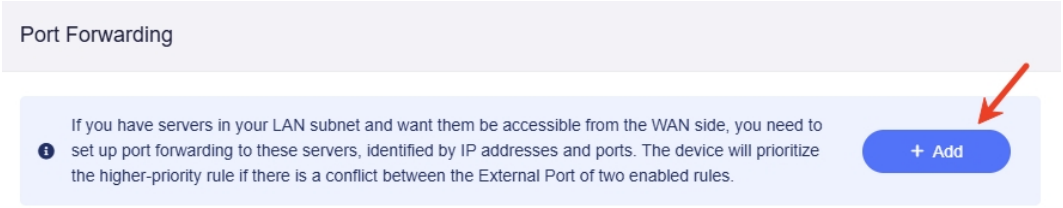
- **IP del host DMZ**: seleccione la dirección IP interna de el dispositivo que recibirá todos los paquetes entrantes.

14.1.2 Reenvío de puertos

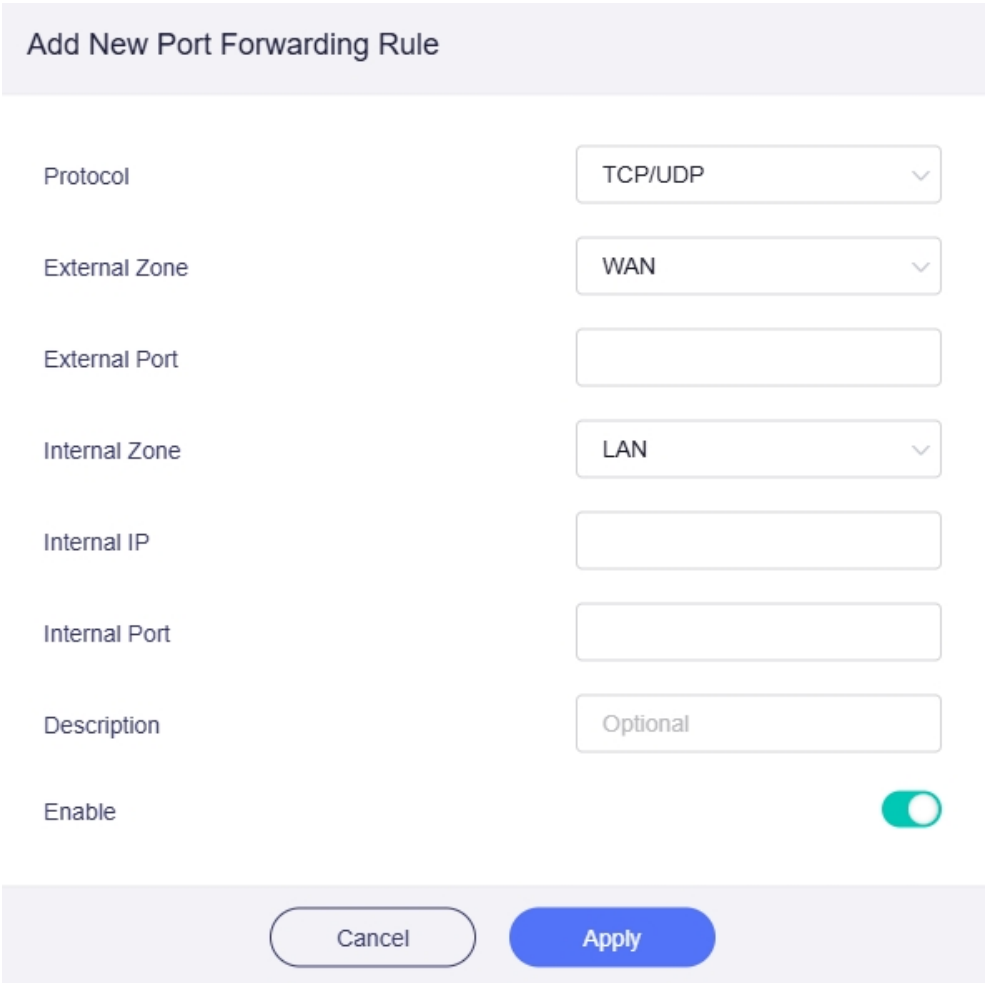
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

Si necesitaconfigurar el puerto reenvío, siga los pasos a continuación.

1. Inicie sesión en el panel de administración web de su enrutador', vaya a **RED** > **Reenvío de puertos** > **Reenvío de puertos** sección y haga clic enhaga clic en **Agregar**.



2. En la ventana emergente, ingrese o seleccione los parámetros requeridos de la lista desplegable para agregar una regla de reenvío de puerto, luego haga clic en **Aplicar**.



- **Protocolo**: El protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto externo**: el número de puertos externos. Introduzca aquí un número de puerto específico. El rango de puertos es 1–65535. Puede configurar un único puerto o un rango de puertos concatenando el primer y el último número de puerto con un guión (por ejemplo, 501-510).
- **Zona interna**: las opciones disponibles son LAN, Invitado, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN y WAN.
- **IP interna**: La dirección IP asignada por el enrutador al dispositivo que necesita acceso remoto. Si configura un solo puerto en Puerto externo, configure un solo puerto aquí. Si configura un rango de puertos en Puerto externo, configure el rango de puertos correspondiente aquí.
- **Puerto interno**: el número de puerto interno del dispositivo. Introduzca un número de puerto específico. Déjelo en blanco si coincide con el puerto externo.
- **Descripción**: establezca un nombre o agregue una descripción para la regla de reenvío de puerto (opcional).
- **Habilitar**: habilite o deshabilite esta regla.

14.2 Multi-WAN

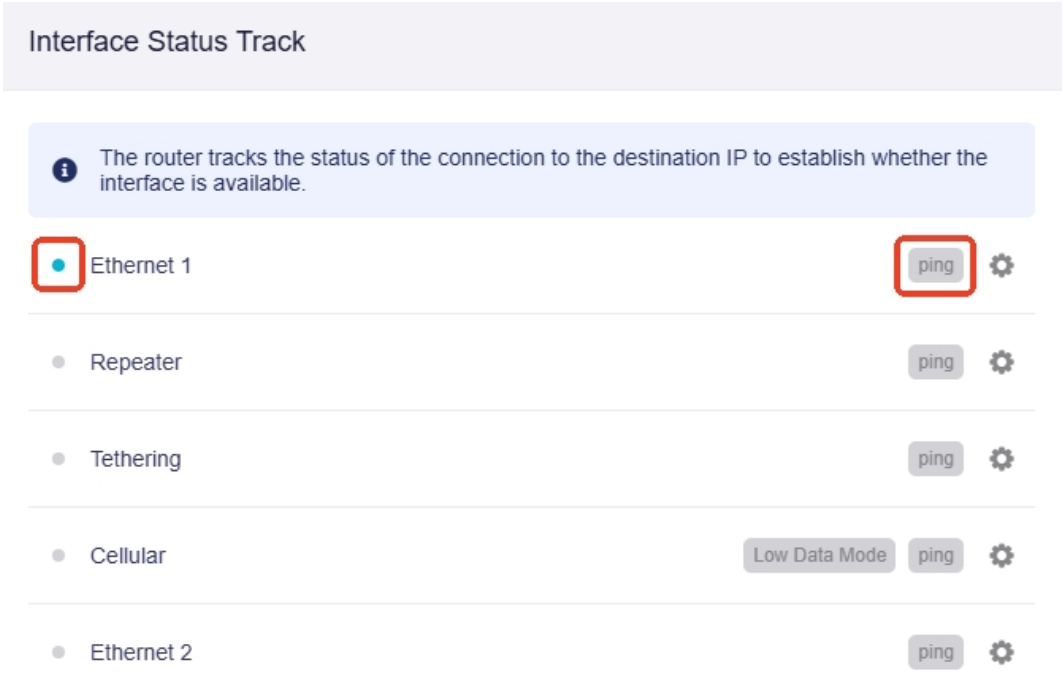
Multi-WAN permite el uso simultáneo de múltiples métodos de acceso a Internet, lo que permite la configuración de diversas opciones de conectividad en el enrutador. Ofrece dos modos de trabajo:

- **Conmutación por error**: cambia automáticamente a una conexión alternativa en poco tiempo si la conexión principal falla, lo que garantiza un acceso ininterrumpido a la red.
- **Equilibrio de carga**: distribuye el tráfico de red entre todas las conexiones disponibles en una proporción establecida para el uso simultáneo de múltiples conexiones, optimizando la utilización del ancho de banda.

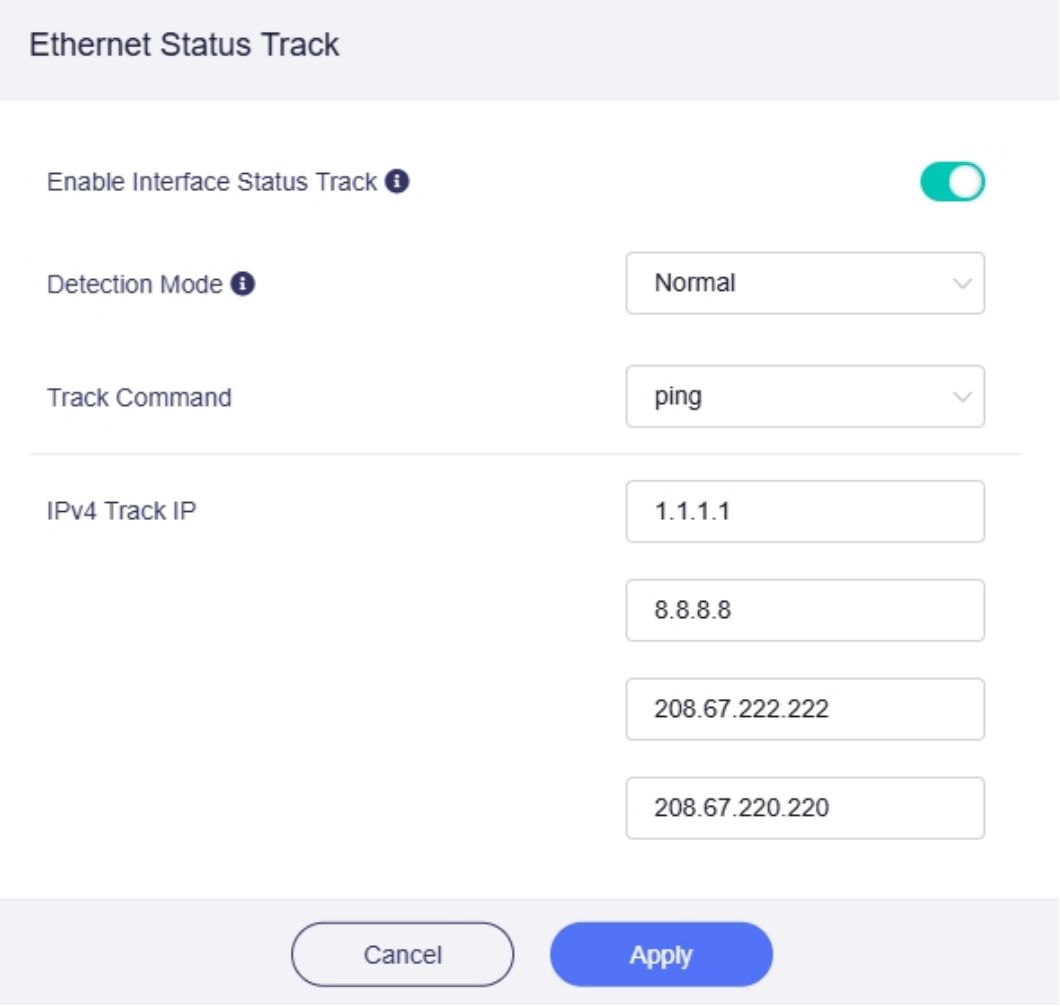
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** >**Multi-WAN**. Esta página incluye dos secciones: Seguimiento del estado de la interfaz y modo Multi-WAN.

14.2.1 Seguimiento del estado de la interfaz

Los enrutadores GL.iNet utilizan **ping** comando para monitorear el estado de la conexión a la IP de destino y determinar si la interfaz está disponible. Si la interfaz está disponible, se mostrará un punto verde a la izquierda; de lo contrario será gris.



En la sección **Seguimiento del estado de la interfaz**, haga clic en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento del estado para cada interfaz de red. A continuación se muestran las configuraciones de seguimiento de estado para la interfaz Ethernet. La misma lógica de configuración se aplica a otras interfaces.

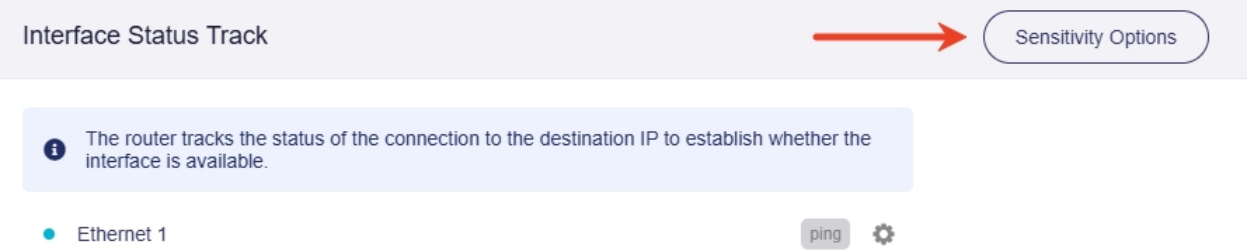


- **Habilitar seguimiento de estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta característica se introdujo como baja Modo de datos en firmware v4.5, luego renombrado Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
  - **Normal**: Se utilizade forma predeterminada.
  - **Datos bajos**: Solo activa el seguimiento cuando se produce un error de red en la red interfaz. Utilice este modo si tiene un plan de datos limitado. Tenga en cuenta que la

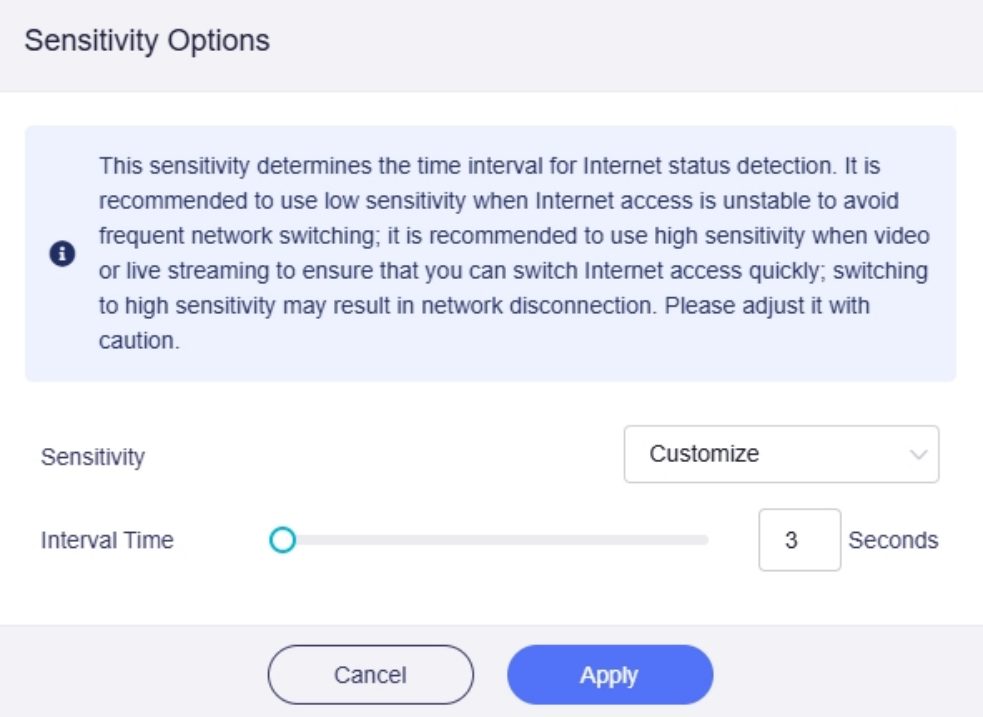
reconexión después de una desconexión puede ser un poco más lenta que en el modo normal, y está habilitado de forma predeterminada solo para la interfaz celular.

  - **Estricto**: determina el estado de la interfaz basado exclusivamente en los resultados de un comando de detección enviado a una IP pública.
- **Comando de seguimiento**: El comando ping se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la disponibilidad de la interfaz.
- **IPv4 Track IP**: Cpersonalice las direcciones IP de seguimiento IPv4 si es necesario.

Haga clic en **Opciones de sensibilidad** en la esquina superior derecha.



Puedes establecer el intervalo de tiempo para la detección del estado de Internet en Bajo, Medio, Alto o personalizarlo. El intervalo de tiempo ajustable varía de 0,5 segundos a 90 segundos.

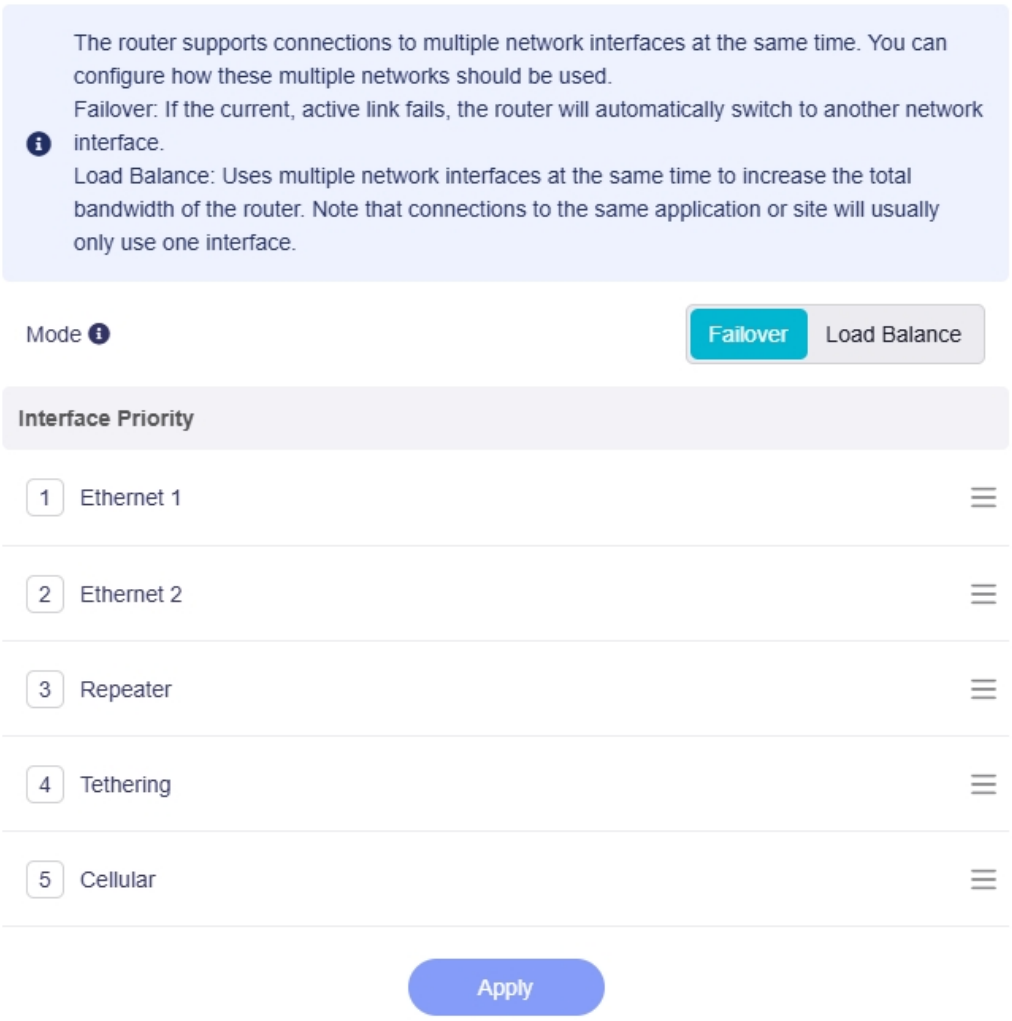


14.2.2 Modo Multi-WAN

Two hay modos disponibles para Multi-WAN: **Conmutación por error** y **Equilibrio de carga**. Tenga en cuenta que estos modos son mutuamente exclusivo.

Conmutación por error

Conmutación por error es el modo predeterminado cuando se configuran varias conexiones. Si el enlace activo falla, el enrutador cambiará automáticamente a otra interfaz de red para acceder a Internet.

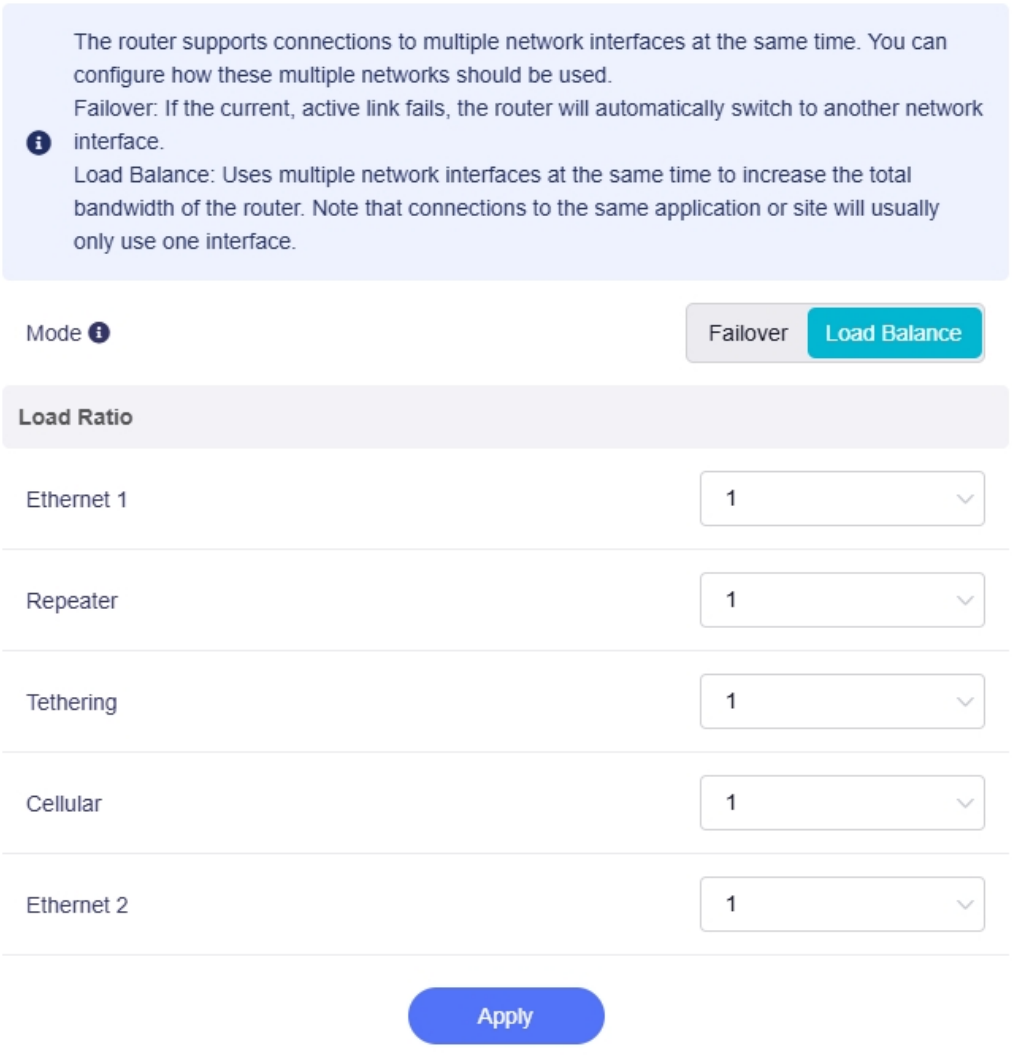


Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente a ella.

Equilibrio de carga

Balance de carga modo utiliza múltiples interfaces de red simultáneamente para aumentar el ancho de banda total del enrutador, y el sistema distribuye nuevas conexiones entre interfaces de acuerdo con una relación de carga configurada. Tenga en cuenta que las conexiones a la misma aplicación o sitio web normalmente utilizarán solo una interfaz.

La relación de carga se refiere a la proporción entre cada interfaz de red. El sistema asignará interfaces para manejar nuevas conexiones según esta proporción configurada.



Por ejemplo, si el enrutador está conectado a cuatro redes (p. ej., Ethernet, Repetidor, Anclaje a red, y Celular) simultáneamente y las cuatro interfaces están disponibles para acceso a Internet, lo que permite el equilibrio de carga y establece una proporción de 1:1:1:1, lo que significa que las cuatro interfaces compartirán la red ancho de banda por igual. El sistema

distribuirá nuevas conexiones a través de estas cuatro interfaces de acuerdo con la relación de carga 1:1:1:1 configurada.

También puede personalizar la relación de carga si es necesario. Por ejemplo, si Ethernet tiene un ancho de banda de 100 Mbps, Repetidor tiene 200 Mbps y no hay conexiones de anclaje a red o celulares activas, establezca las relaciones de carga en 1 para Ethernet, 2 para Repetidor y 0 para anclaje a red y celular. Luego, el sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la proporción 1:2 configurada, lo que significa que Ethernet manejará la mitad de conexiones que el repetidor. A diferencia del modo de conmutación por error, este modo optimiza la eficiencia del rendimiento general al equilibrar la carga de tráfico en todas las interfaces disponibles.

Nota: No se garantiza que las conexiones o el tráfico existentes se alineen con la relación de carga. La distribución real se acercará gradualmente a la proporción configurada con un uso prolongado.

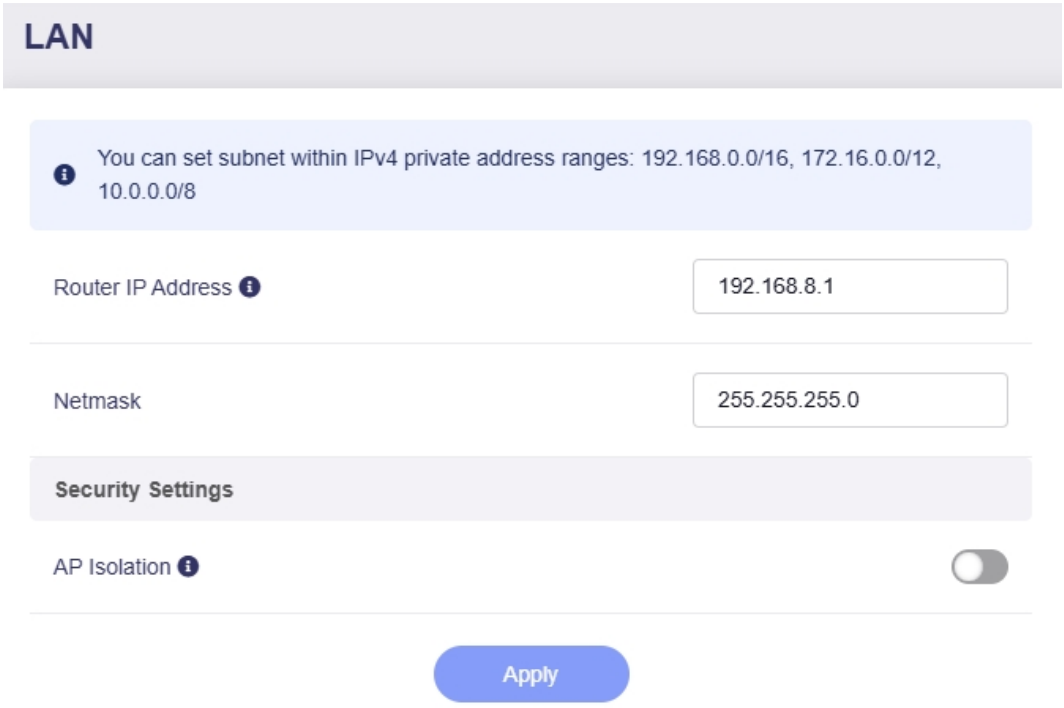
14.3 LAN

LAN (red de área local) se refiere a la red local privada, a la que se conectan sus dispositivos mediante cables Ethernet.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **LAN**. Aquí puede configurar los ajustes de LAN, incluidos ajustes básicos, servidor DHCP y reserva de dirección.

14.3.1 Configuración básica

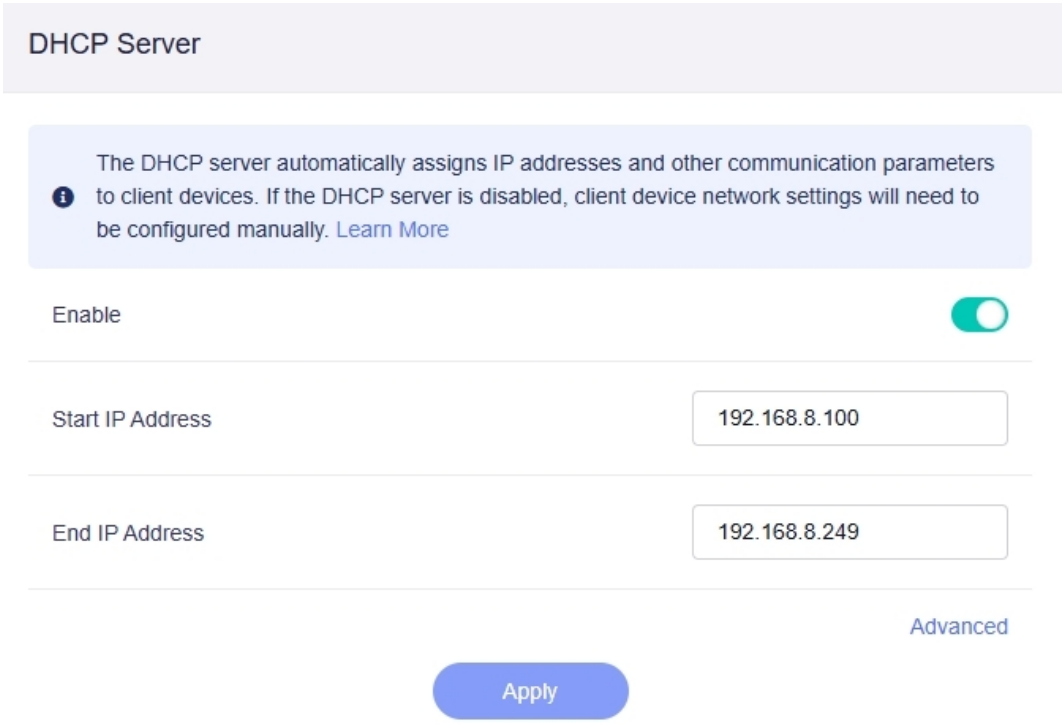
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de los rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



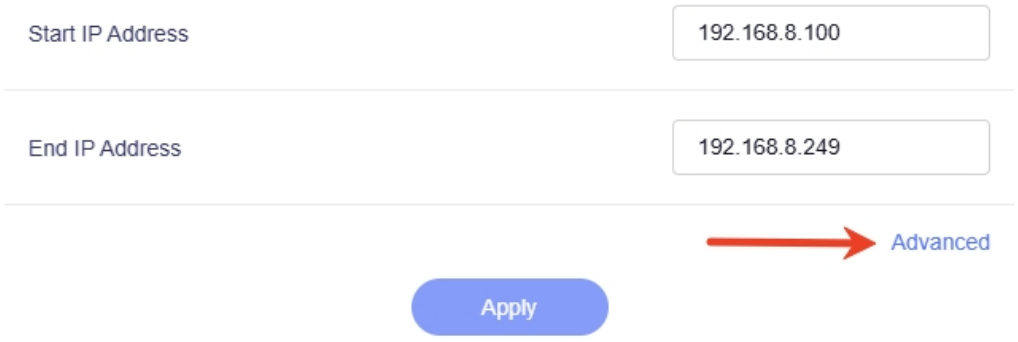
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones del navegador para acceder al panel de administración del enrutador'. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento de AP**: puede aislar los dispositivos cliente de su red en un área de red separada. Estos dispositivos no pueden comunicarse con otros dispositivos en la red.

14.3.2 Servidor DHCP

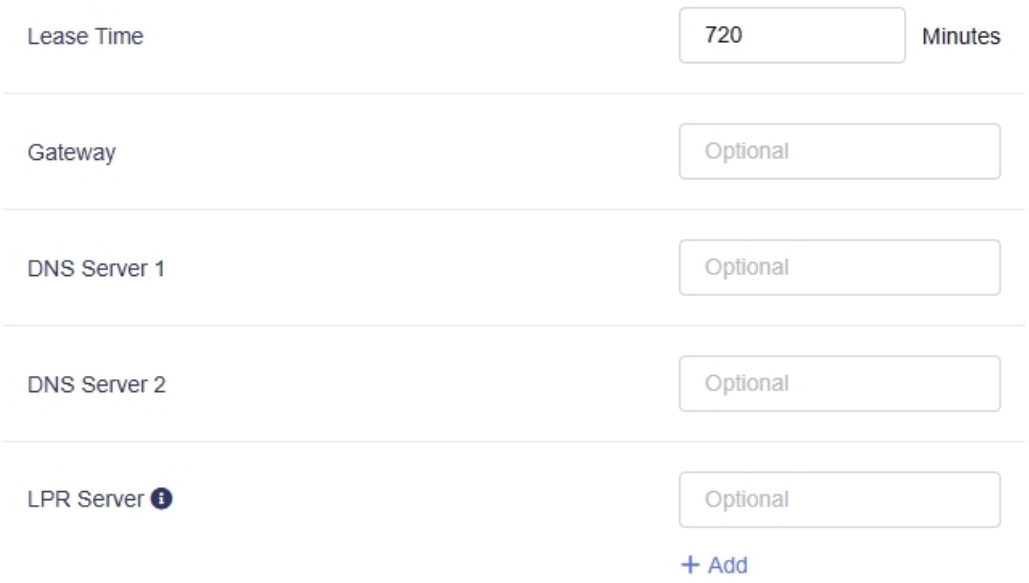
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP varía de 192.168.8.100 a 192.168.8.249. Puede personalizar el rango de direcciones si es necesario. ’está habilitado de forma predeterminada y el servidor DHCP’va desde 192.168.8.100 a 192.168.8.249. Puede personalizar el rango de direcciones si es necesario.



Haga clic en **Avanzado** en la esquina inferior derecha.



Podrá configurar ajustes avanzados, incluidos el tiempo de arrendamiento, la puerta de enlace, Servidor(es) DNS, y servidor LPR.



- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de DHCP.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la local red y redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable para traducir nombres de dominio en direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS primario falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Se pueden configurar múltiples puertos LPR para impresoras.

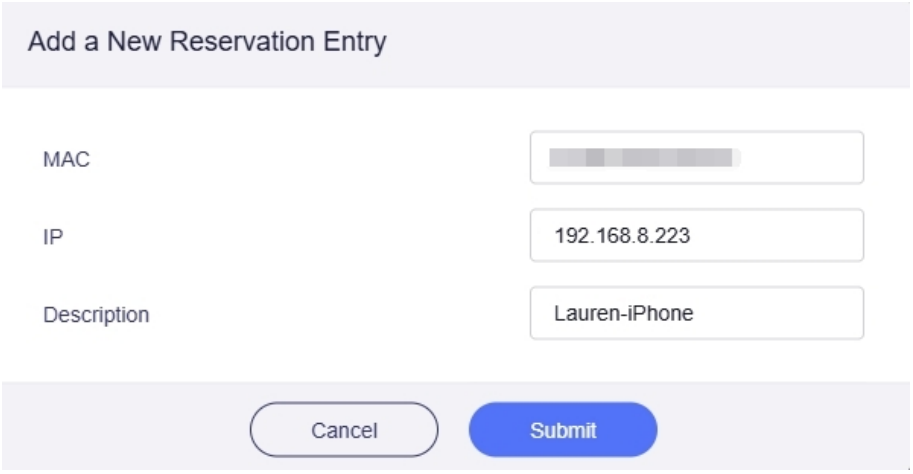
Nota: Si el servidor DHCP está deshabilitado, debe configurar la IP estática y otros parámetros de comunicación manualmente para cada cliente. Consulte aquí para obtener más detalles.

14.3.3 Reserva de direcciones

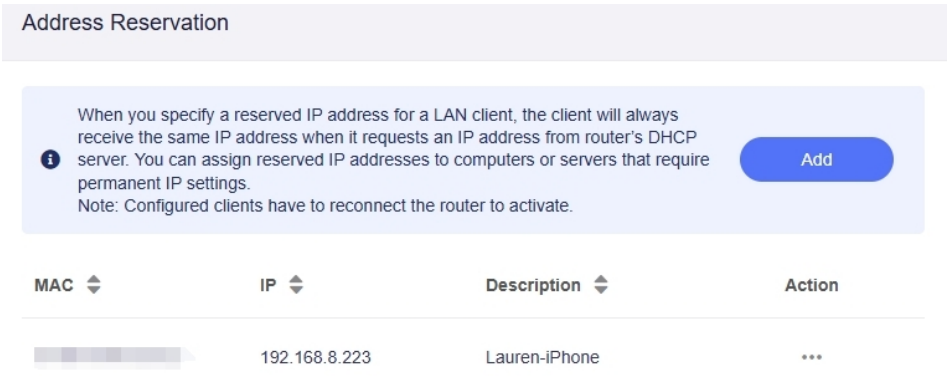
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración de IP permanente. Tenga en cuenta que los clientescon reserva de dirección configurada deben volver a conectarse al enrutador para activar la configuración.

Siga los pasos a continuación para configurar la reserva de dirección si necesario.

1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **RED** > **LAN** > **Reserva de direcciones** y haga clic en **Agregar**.
2. En la ventana emergente, seleccione la dirección MAC de la lista desplegable, luego tla dirección IP correspondiente para la MAC seleccionada se completará automáticamente. Ingrese un nombre descriptivo y haga clic en **Enviar**.



3. Después de agregar una nueva reserva de dirección IP, la página mostrará la entrada reservada, como se muestra a continuación.



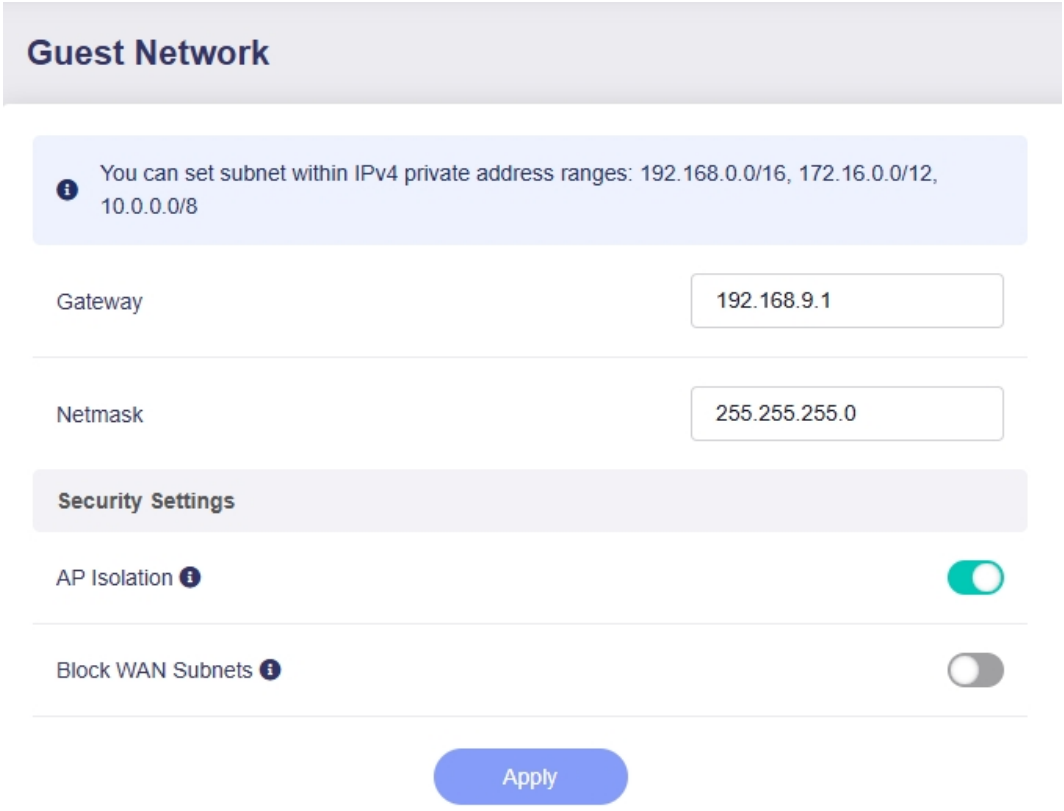
14.4 Red de invitados

Red de invitados se refiere a una red dedicada a la que los visitantes pueden conectarse, aislándolos de su LAN principal para proteger la seguridad de su red privada.

Inicie sesión en el panel de administración web de su enrutador y ir a **RED** -> **Red de invitados**. Esta página le permite configurar los ajustes de la red de invitados, incluyendo configuraciones básicas y servidor DHCP.

14.4.1 Configuración básica

Las configuraciones básicas incluyen Puerta de enlace, máscara de red, aislamiento de AP y bloque de subredes WAN.



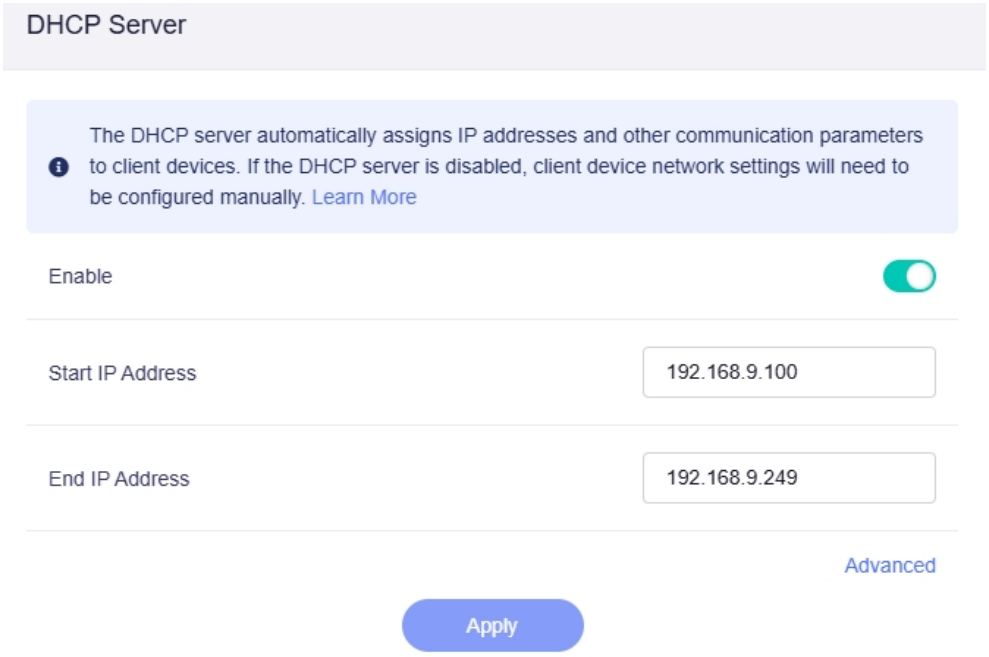
- **puerta de enlace**: es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento AP**: se utiliza para aislar a los clientes de la red invitada en segmentos separados para que no puedan comunicarse con otros dispositivos en la misma red.

- **Bloquear subredes WAN**: si está habilitado, la red de invitados no podrá acceder a la red ascendente ni a su segmento de red correspondiente.

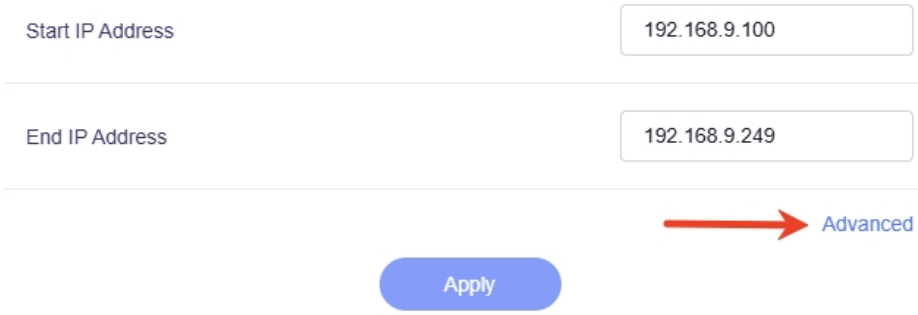
14.4.2 Servidor DHCP

Dado que la red de invitados está deshabilitada de forma predeterminada, su servidor DHCP está deshabilitado y oculto hasta que se habilita manualmente.

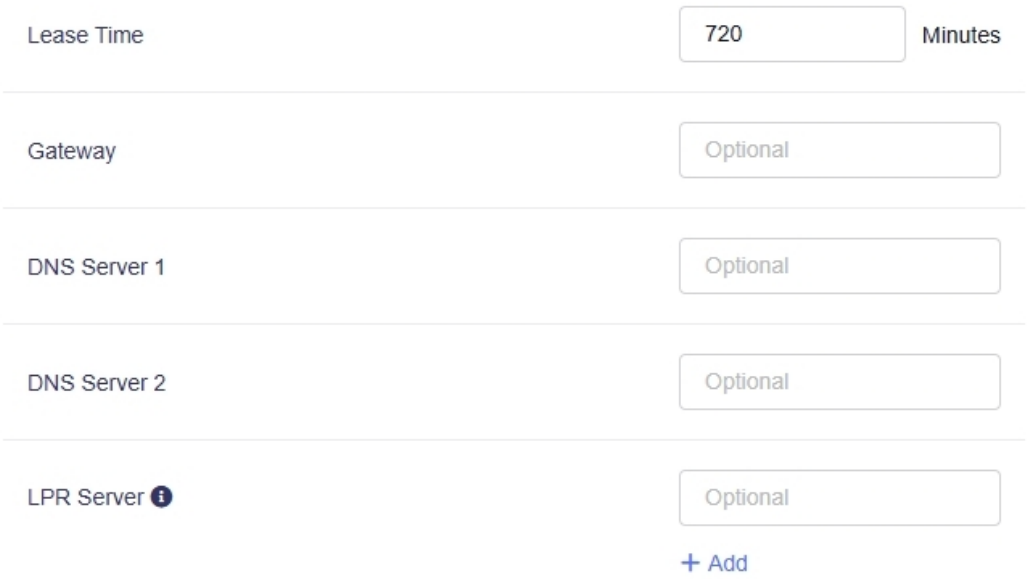
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones si es necesario.



Haga clic en **Avanzado** en la esquina inferior derecha.



Podrá configurar ajustes avanzados, incluidos el tiempo de concesión, la puerta de enlace, los servidores DNS, y el servidor LPR.



- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de DHCP de la red de invitados.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la gred de invitados y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir nombres de dominio a direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS primario falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Se pueden configurar varios puertos LPR para impresoras.

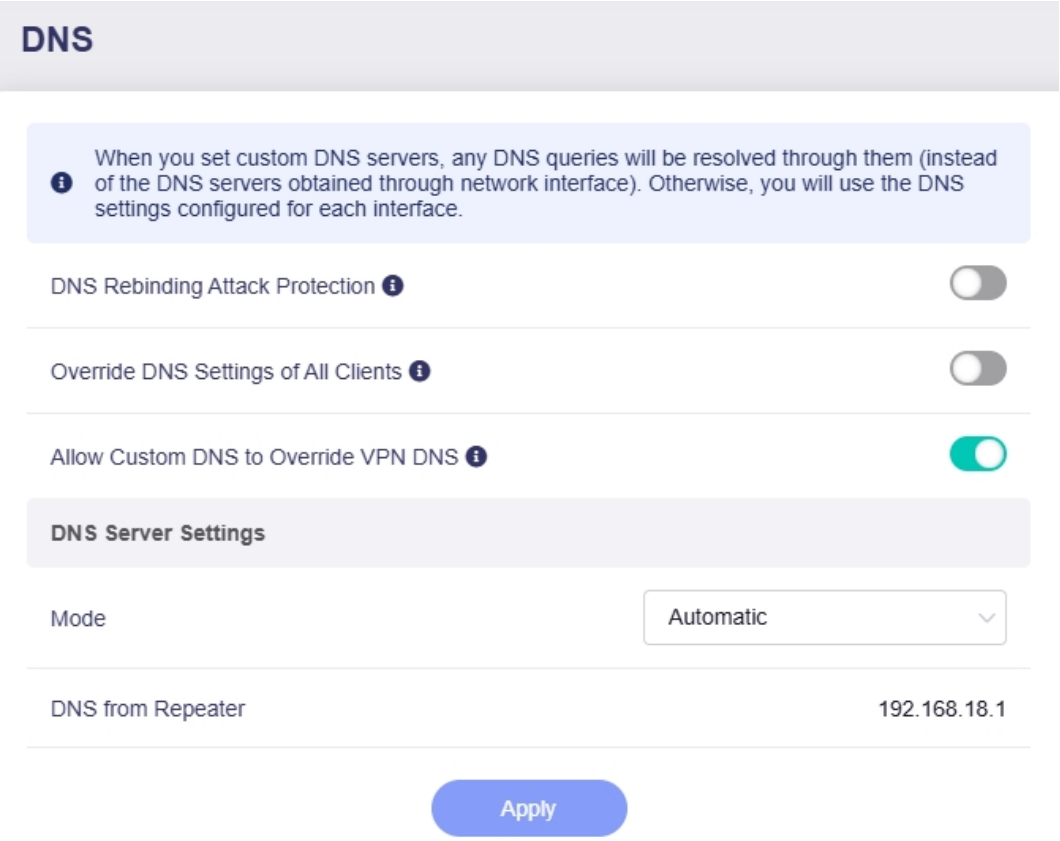
14.5 DNS

DNS (Sistema de nombres de dominio) es un servicio que traduce nombres de dominio legibles por humanos, como www.google.com, en direcciones IP para que los dispositivos puedan localizar y conectarse a sitios web y en línea. servicios.

En un enrutador, la configuración de DNS generalmente determina qué servidores DNS utilizan los dispositivos conectados. En la mayoría de los casos, el enrutador obtiene las direcciones del servidor DNS automáticamente del ISP o de la red ascendente, o permite a los usuarios especificar manualmente servidores DNS públicos, como 8.8.8.8, en la interfaz de administración web. Una vez configuradas, estas configuraciones de DNS generalmente se distribuyen automáticamente a los dispositivos conectados, por lo que no es necesario configurar DNS por separado en cada dispositivo.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS.

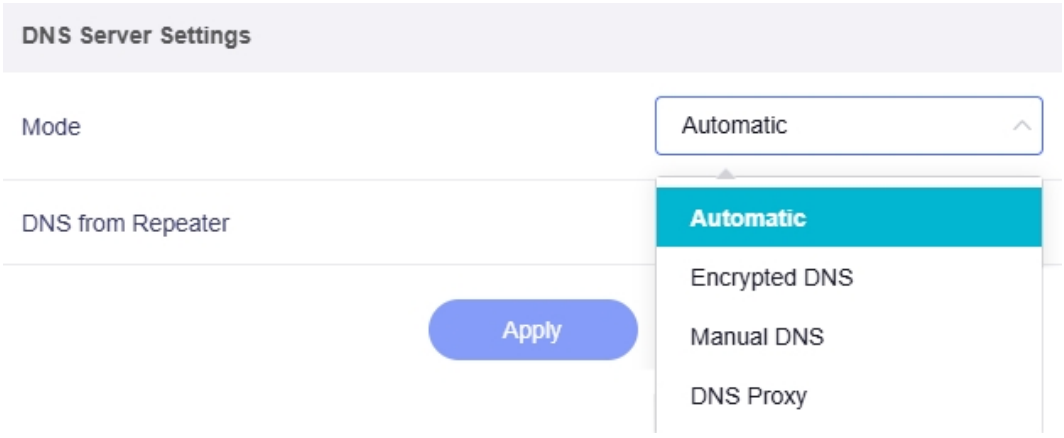
14.5.1 Configuración general



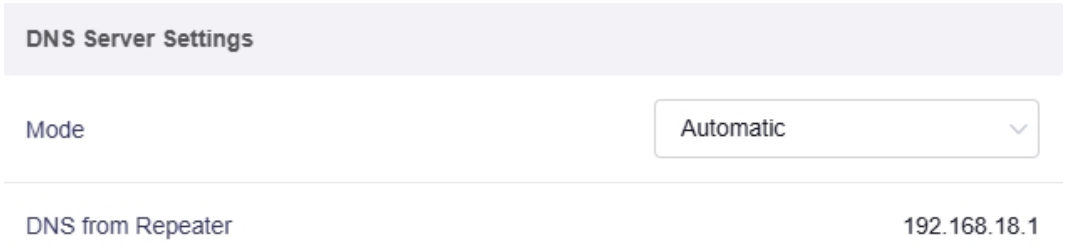
- **Protección contra ataques de vinculación de DNS**: protege contra ataques de vinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, páginas de inicio de sesión de Wi-Fi públicas).
- **Anular la configuración DNS de todos los clientes**: Si está habilitado, todos los dispositivoss será forzado a utilizar los servidores DNS configurados en el enrutador, ignorando su propia configuración DNS original. Permite la configuración de DNS unificada para todos los dispositivos.
- **Permitir que DNS personalizado anule el DNS de VPN**: Cuando está habilitado, si ha configurado DNS personalizado, los paquetes transmitidos a través del túnel VPN utilizarán el DNS personalizado para la resolución, en lugar de los servidores DNS de la conexión VPN. Esto garantiza que sus reglas de resolución de DNS personalizadas se apliquen normalmente al usar VPN.

14.5.2 Configuración del servidor DNS

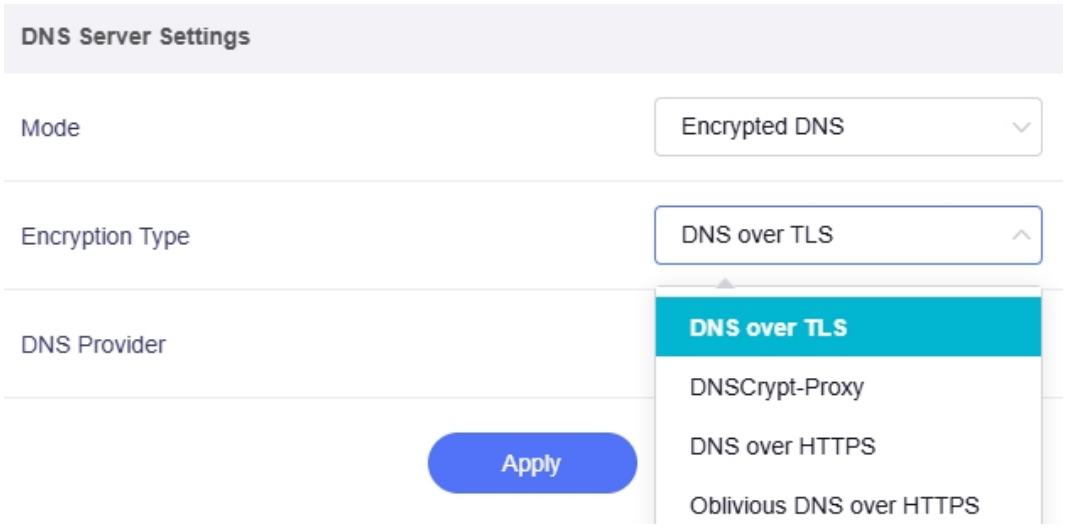
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y DNS Proxy.



1. **Automático**: cuando se selecciona, el enrutador obtendrá automáticamente las direcciones del servidor DNS de la red ascendente y las aplicará a todos los dispositivos conectados.

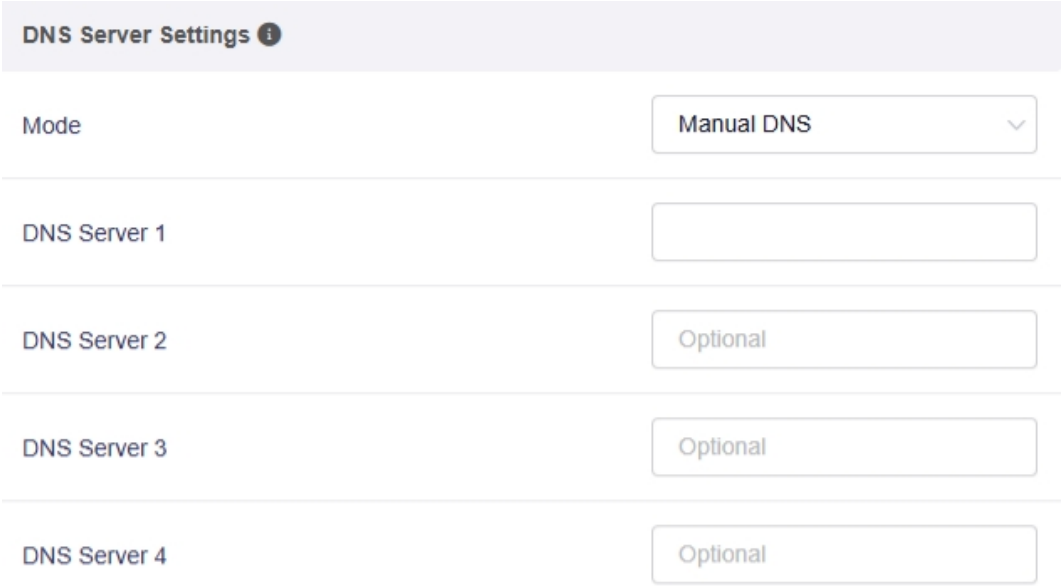


2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o alteraciones.
   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a HTTPS.



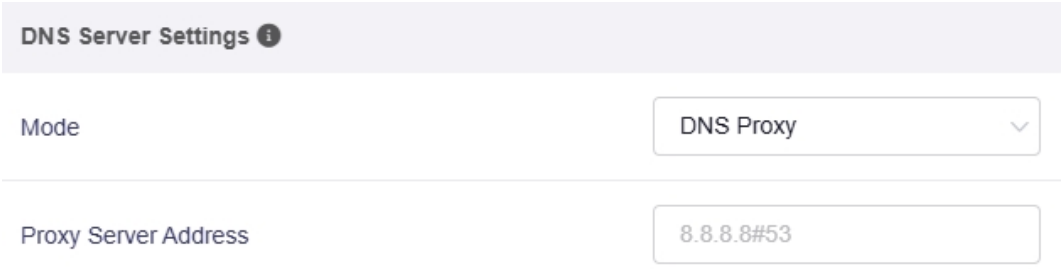
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan varios servidores, el enrutador utilizará el más rápido automáticamente.

3. **DNS manual**: cuando se selecciona, puede personalizar los servidores DNS de su enrutador. Haga clic en Servidor DNS 1 y elija un servidor DNS de la lista desplegable. Los campos DNS restantes se actualizarán automáticamente.



Nota: si necesita utilizar direcciones IPv6 para DNS manual, habilite primero IPv6 en su enrutador.

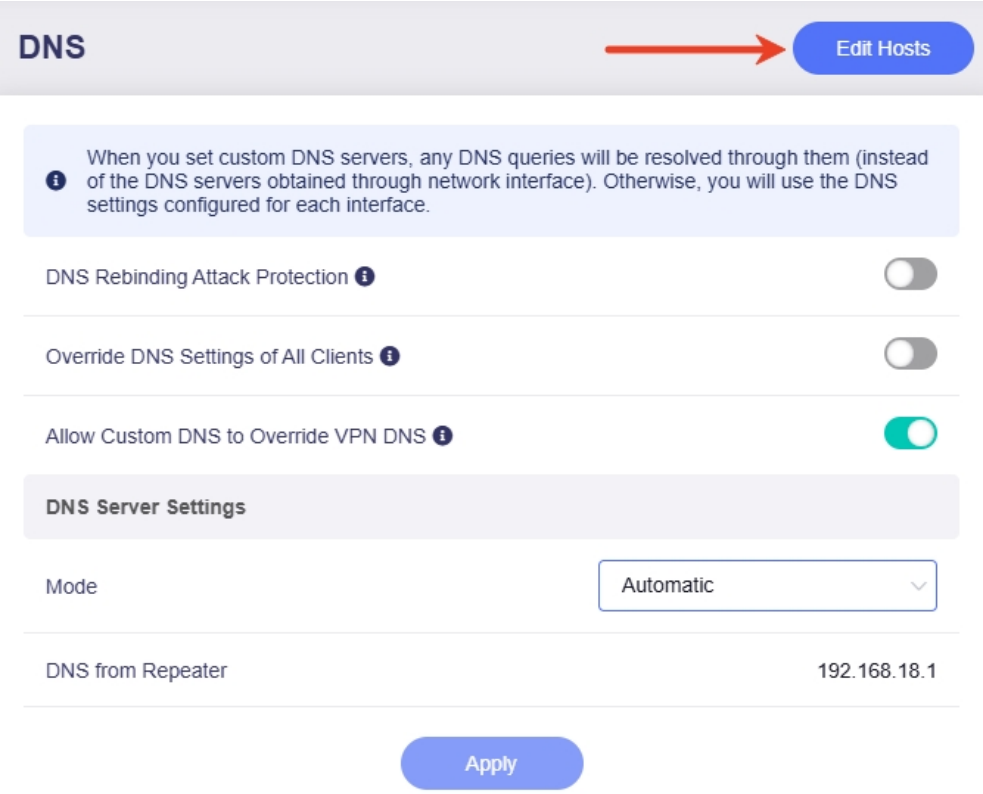
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permitela resolución a través del proxy entorno de red para necesidades de acceso específicas.



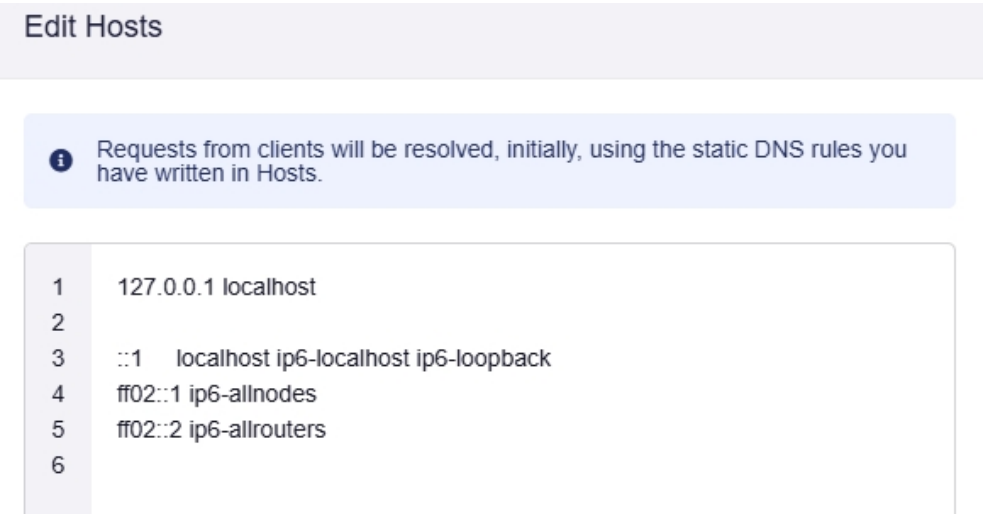
14.5.3 Editar hosts

Puede definir reglas de resolución de DNS estáticas si es necesario.

En la página DNS, haga clic **Editar hosts** en la esquina superior derecha.



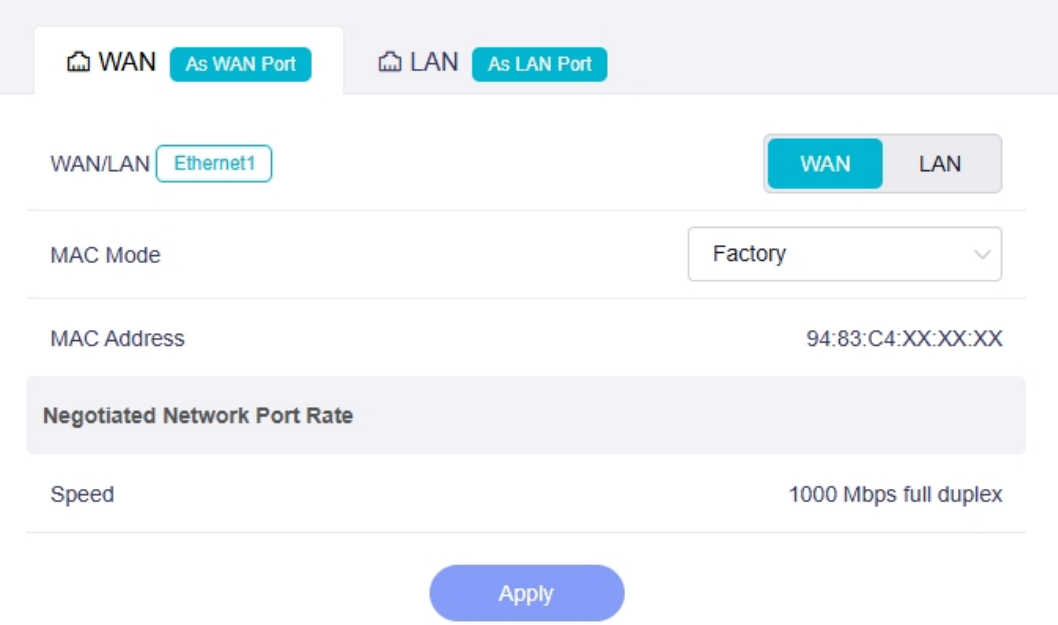
Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de host (por ejemplo, las entradas predeterminadas). como 127.0.0.1 localhost para loopback local) para un control personalizado de la resolución de nombres de dominio.



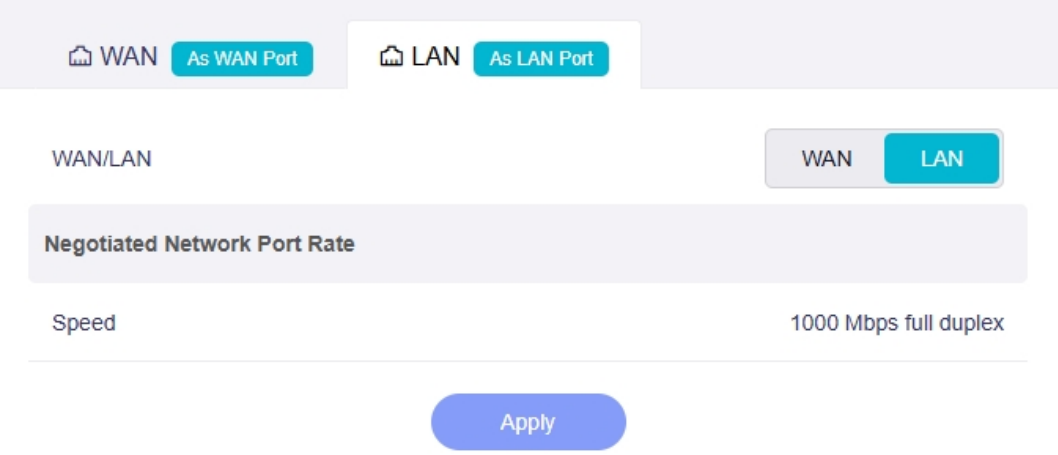
14.6 Puerto Ethernet

Inicie sesión en el administrador web de su enrutador' panel y navegue hasta **RED** > **Ethernet Port**. Esta página le permite administrar el enrutador's puertos Ethernet.

La sección **WAN** muestra la función del puerto (WAN o LAN), la dirección MAC y la velocidad negociada.



La sección **LAN** muestra la velocidad negociada del puerto LAN.

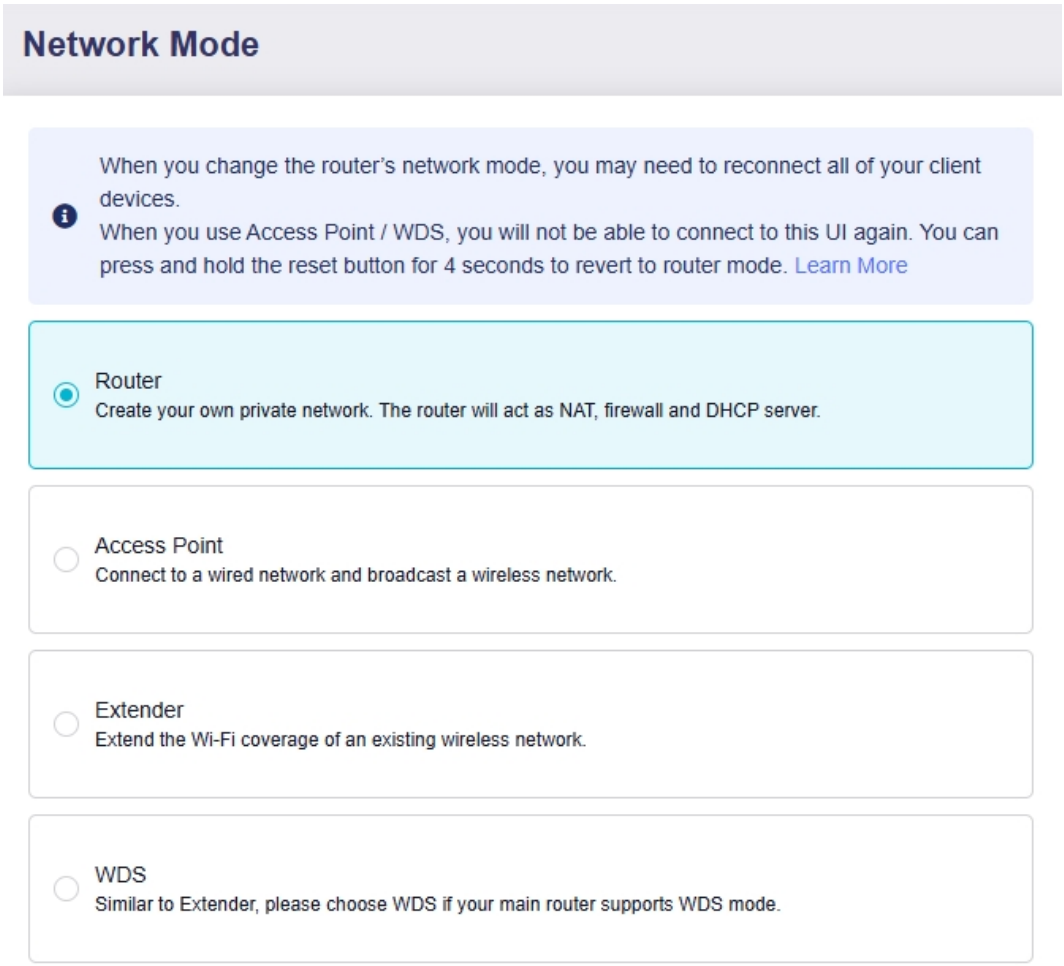


Nota: La tarifa negociada para el puerto WAN y LAN se muestra solo cuando se conecta un cable Ethernet. Depende tanto del puerto Ethernet como del cable Ethernet.

14.7 Modo de red

El modo de red se refiere a los diferentes roles operativos y funciones que un enrutador puede asumir para satisfacer diversas necesidades de implementación de red.

Inicie sesión en su panel de administración web del' y navegue hasta **RED** > **Modo de red**. Puede cambiar el modo de red de su enrutador.



- **Enrutador**: este es el modo operativo predeterminado para la mayoría de los enrutadores domésticos y de pequeñas oficinas, diseñado para crear una red de área local (LAN) privada y actuar como una puerta de enlace dedicada entre la Internet pública y los dispositivos conectados. En este modo, el enrutador habilita funciones principales que incluyen NAT, DHCP y un firewall integrado. Se conecta a una línea ascendente, como fibra de banda ancha, asigna automáticamente direcciones IP privadas a los dispositivos conectados y proporciona seguridad de red para toda la red privada.

- **Punto de acceso**: este modo permite que un enrutador se conecte a una red cableada a través de un cable LAN y transmita señales inalámbricas, ampliando la cobertura Wi-Fi en grandes espacios para permitir que más dispositivos accedan a la red. red. En este modo, el enrutador desactiva sus funciones NAT y DHCP, funcionando exclusivamente como un transmisor y conmutador de señal inalámbrico en lugar de una puerta de enlace independiente.
- **Extensor**: este modo está diseñado para ampliar la cobertura Wi-Fi de una red inalámbrica existente y eliminar zonas muertas de señal en áreas con mala conectividad. Permite que el enrutador reciba señales del enrutador principal de forma inalámbrica, las amplifique y retransmita la señal potenciada. A diferencia del modo Punto de acceso, no requiere conexión por cable al enrutador principal, pero puede provocar que el ancho de banda se reduzca a la mitad, ya que el dispositivo tiene que manejar la recepción y transmisión de señales simultáneas.
- **WDS**: el modo Sistema de distribución inalámbrica (WDS) es similar al modo Extensor, ya que extiende la cobertura Wi-Fi de forma inalámbrica, pero admite puente inalámbrico entre múltiples enrutadores compatibles. Se recomienda para la expansión de la red inalámbrica cuando el enrutador ascendente tiene funcionalidad WDS.

  Este modo es ideal para escenarios como cubrir edificios de varios pisos o campus de oficinas pequeñas donde varios enrutadores necesitan trabajar juntos para formar una red inalámbrica unificada. A diferencia del modo Extensor, que solo transmite señales desde un enrutador principal a un único extensor, el modo WDS permite que los enrutadores interconectados envíen y reciban señales, lo que permite una cobertura perfecta en áreas más grandes con múltiples nodos de señal.

Nota:

1. Cuando se cambia el modo de red, todos los dispositivos cliente se volverán a conectar al enrutador para una conectividad de red estable.
2. **En modo Punto de acceso/WDS, no podrá acceder al panel de administración web usando la dirección IP original**. En su lugar, debe iniciar sesión en el enrutador ascendente para encontrar la dirección IP que ha asignado a este enrutador y luego usar esta dirección IP para acceder al panel de administración web. Si no tiene acceso al enrutador ascendente, presione y mantenga presionado el botón de reinicio durante 4 segundos para revertirlo al modo de enrutador predeterminado.

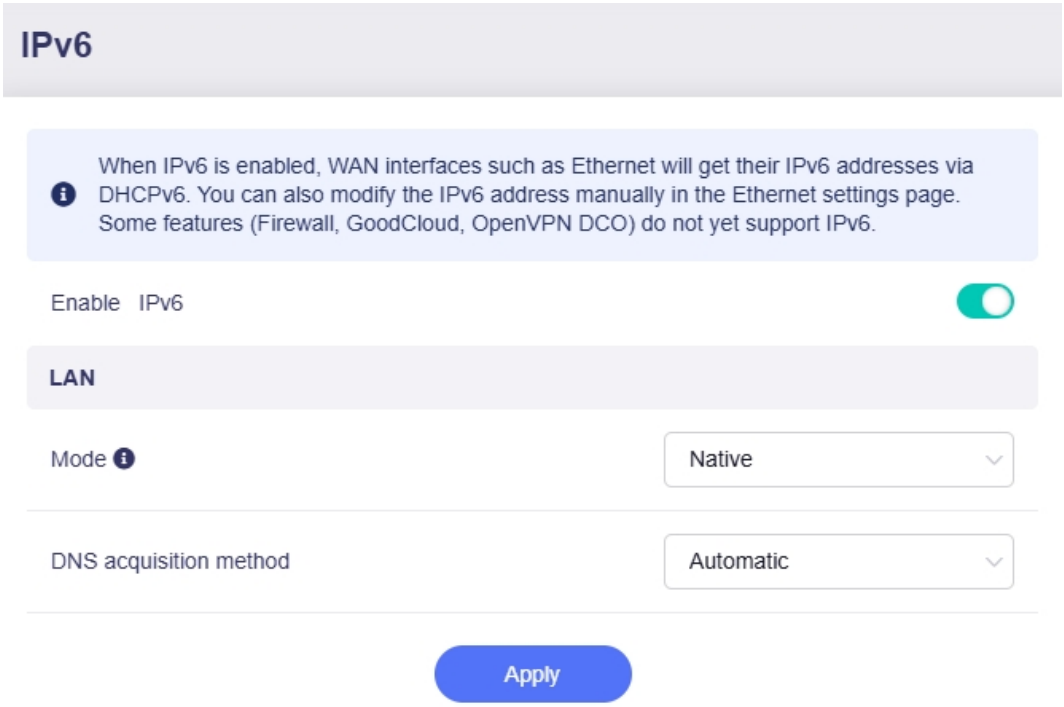
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y lista de bloqueo), AstroWarp, VPN, AdGuard Home, Control parental, ZeroTier, Tailscale, Reenvío de puertos, Multi-WAN, Servidor DHCP, Reserva de direcciones, Red de invitados, DNS, Puerto Ethernet, IPv6, puerta de enlace directa, vigilancia IGMP, aceleración de red, configuración NAT.

14.8 IPv6

IPv6 (Protocolo de Internet versión 6) es el último protocolo de Internet diseñado para reemplazar IPv4. Ofrece un grupo más grande de IP únicas, lo que resuelve el problema de agotamiento de direcciones de IPv4 y admite el creciente número de dispositivos conectados en todo el mundo.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **IPv6**. Estaesta página le permite habilitar y configurar IPv6 en su enrutador. Cuando IPv6 está habilitado, las interfaces WAN como Ethernet obtendrán sus direcciones IPv6 a través de DHCPv6.

Alternar en **Eactivar IPv6**, seleccione el modo para su red principal y el método de adquisición de DNS, luego haga clic en **Aplicar.**



Nota: Algunas funciones (por ejemplo, firewall, GoodCloud, OpenVPN DCO) aún no son compatibles con IPv6. Si habilita estas funciones e IPv6 al mismo tiempo, es probable que cause problemas de conectividad .

14.8.1 Modo IPv6

Hay cuatro modos disponibles: Nativo, Passthrough, NAT6 e IPv6 estático.

- **Nativo**: este modo es aplicable cuando el enrutador obtiene directamente una dirección pública IPv6 , y el enrutador asigna automáticamente IPv6. direcciones a dispositivos en línea. Este modo puede satisfacer las necesidades de acceso a IPv6 de la mayoría de los usuarios.
- **Paso**: este modo es aplicable cuando los paquetes IPv6 deben pasar directamente sin ningún procesamiento o conversión. Por ejemplo, algunos específico pueden requerir la preservación completa del contenido del paquete IPv6 para su posterior procesamiento o análisis. Este modo lo utiliza el personal técnico para la depuración de la red o el análisis de seguridad.
- **NAT6**: este modo es Adecuado para escenarios en los que se utiliza un enrutador como puerta de enlace para asignar direcciones IPv6 internas dinámicas a cada dispositivo de la red. En este modo, los dispositivos terminales se conectan a través de una terminal de red óptica y obtienen una dirección IPv6 de red de área local. adecuado para escenarios en los que se utiliza un enrutador como puerta de enlace para asignar direcciones IPv6 internas dinámicas a cada dispositivo de la red. En este modo, los dispositivos terminales se conectan a través de una terminal de red óptica y obtienen una dirección IPv6 de red de área local.
- **IPv6 estático**: este modo es adecuado para dispositivos o servicios que requieren una dirección IPv6 fija, como servidores o impresoras de red. Este modo asegura que el dispositivo utilice siempre la misma dirección IPv6, facilitando la gestión y el acceso.

14.8.2 Método de obtención de DNS

Determina cómo el enrutador obtiene las direcciones del servidor DNS IPv6. Hay dos opciones: Automático y Manual.

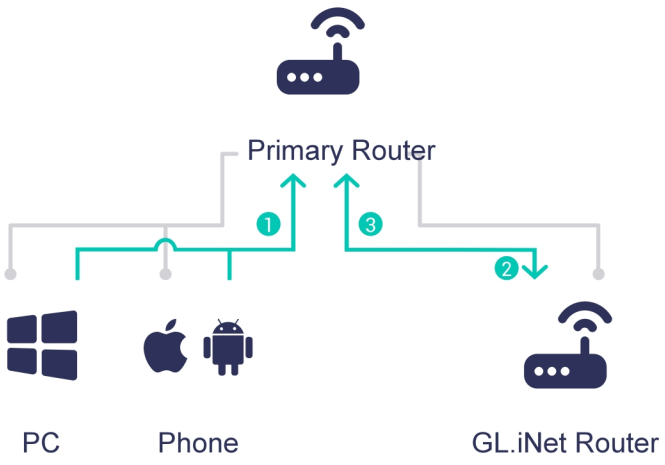
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 de forma dinámica (por ejemplo, a través de DHCPv6).
- **Manual**: ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes, la configuración manual del servidor DNS puede provocar fallas en la búsqueda de DNS. Úselo con precaución.

14.9 Puerta de enlace directa

Drop-in Gateway es una función de extensión que permite la expansión de la capacidad de un enrutador primario existente sin reemplazarlo ni volver a configurarlo-. Al conectar el enrutador GL.iNet al enrutador principal mediante un cable Ethernet, los usuarios pueden agregar funciones avanzadas a la infraestructura de red existente , por ejemplo:

- Filtrar anuncios a través de AdGuard Home
- Habilitar cliente VPN
- Usar DNS cifrado

Drop-in Gateway funciona como una red intermedia sistema, enrutando el tráfico de datos desde los dispositivos cliente a través del enrutador GL.iNet para su procesamiento antes de transmitirlo a través del enrutador principal. Durante este proceso, no solo conserva la configuración de red existente para garantizar una conectividad ininterrumpida para todos los dispositivos conectados, sino que también le permite administrar el tráfico de red para todos o dispositivos cliente específicos si es necesario.



El diagrama anterior consta de dos tipos de líneas: líneas grises y líneas verdes marcadas con tres flechas, cada una etiquetada con su correspondiente número.

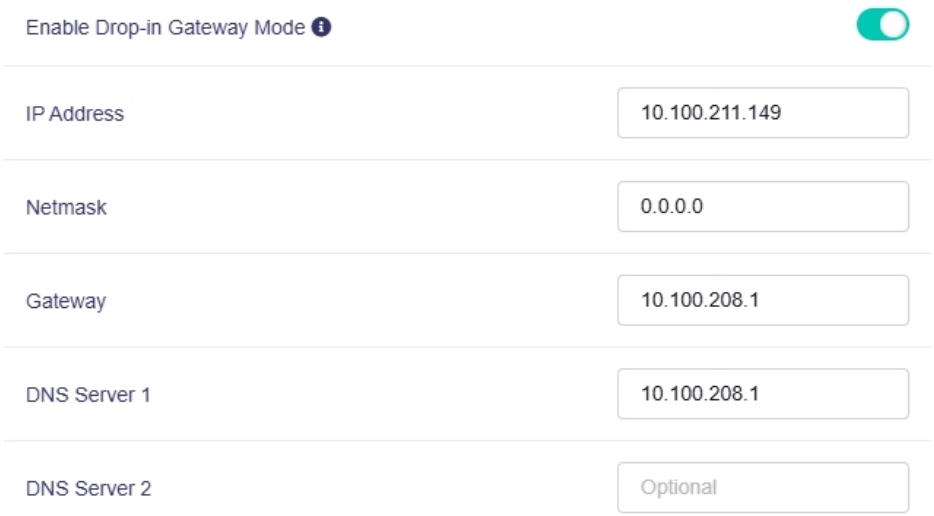
- **Grayo lines** ilustran lo físico Topología de conexión: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conectan al enrutador principal, y el puerto LAN del

enrutador principal se vincula al puerto WAN del enrutador GL.iNet (con Drop-in Gateway habilitado) a través de un cable Ethernet.

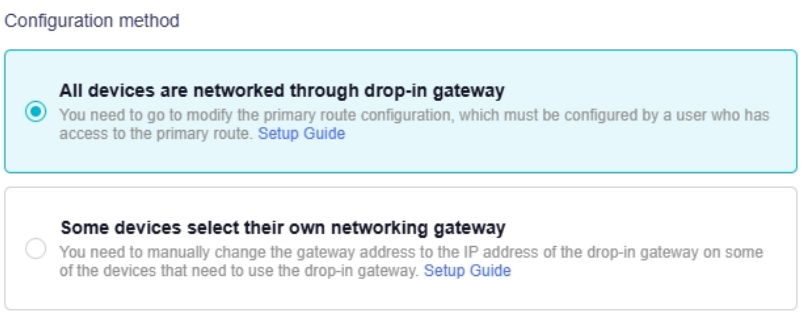
- **Glas líneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas indicando el flujo de tráfico orden:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía el tráfico al enrutador GL.iNet para su procesamiento (por ejemplo, filtrado de anuncios, cifrado VPN);
  3. Después del procesamiento, el tráfico se envía de regreso al enrutador principal, que luego entrega los datos finales a los dispositivos cliente originales o los enruta a Internet.

Siga los pasos a continuación para habilitar Drop-in Gateway si necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Puerta de enlace directa**. Alternar en **Enable Modo de puerta de enlace directa**, y confirme los parámetros de red.



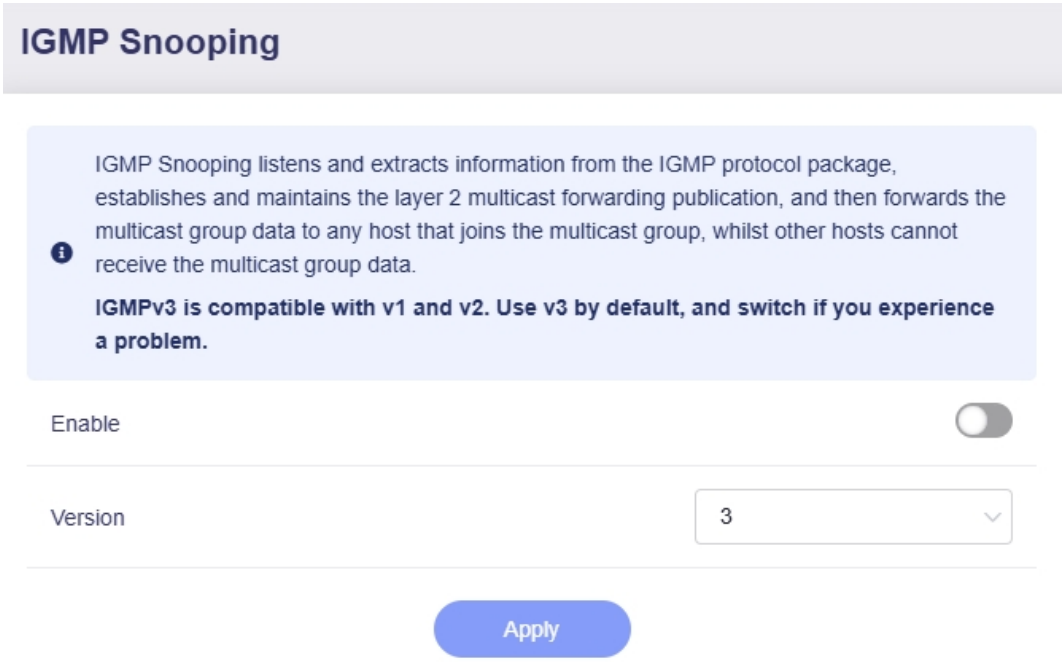
2. Seleccione el método de configuración y luego haga clic en **Aplicar**. Consulte este tutorial para detalless.



14.10 Inspección IGMP

IGMP Snooping escucha el paquete de protocolo IGMP, extrae la información correspondiente, establece y mantiene la tabla de reenvío de multidifusión de capa 2 y luego reenvía los datos del grupo de multidifusión al host que se une al grupo de multidifusión, mientras que otros hosts no pueden recibir el grupo de multidifusión. data.

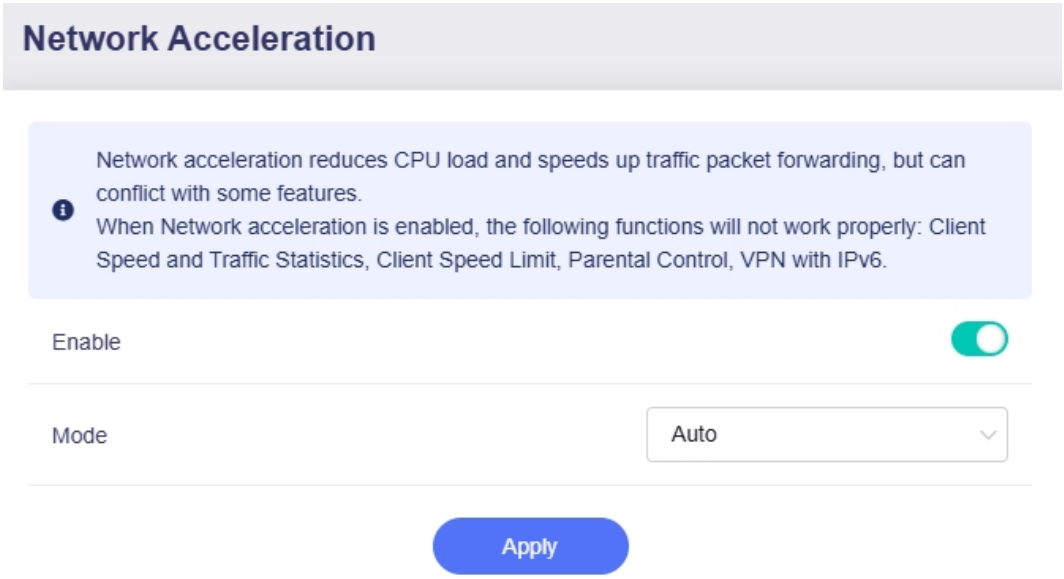
Inicie sesión en el panel de administración web de su enrutador'y navegue hasta **RED** > **Inspección IGMP**. Puede habilítelo para usar la función de multidifusión en su enrutador si es necesario.



14.11 Aceleración de red

La aceleración de red reduce la carga de la CPU y acelera el reenvío de paquetes de tráfico, pero puede entrar en conflicto con algunas funciones.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Aceleración de red**. Esta página le permite habilitar la aceleración de red y seleccionar un modo de aceleración entre Automático, Aceleración de hardware y Aceleración de software.

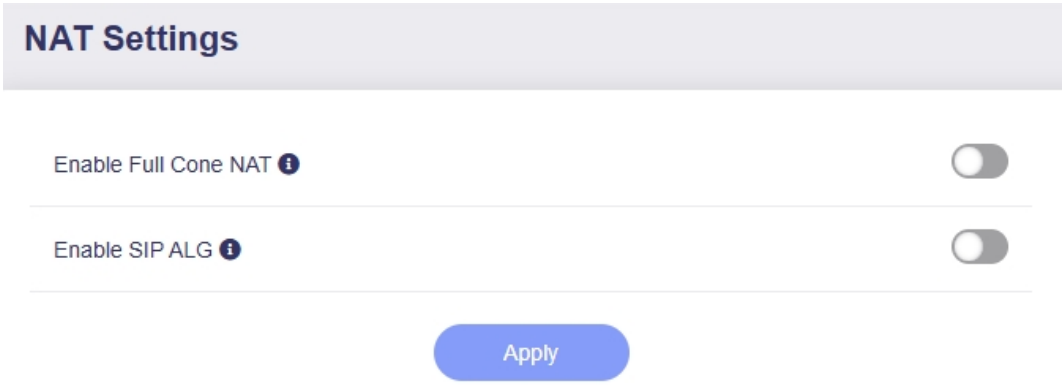


- **Auto**: cambia automáticamente entre los dos modos de aceleración según el uso real.
- **Hardware Aceleración**: descarga tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet y repetidoras, sobresaliendo en estos escenarios con rutas fijas y reglas simples para ofrecer alto rendimiento, baja latencia y carga mínima de CPU para la transmisión de datos a velocidad de cable.
- **Aceleración de software**: depende de la CPU general de un enrutador emparejada con núcleos o controladores optimizados (por ejemplo, SWNAT). Funciona con acceso celular (4G/5G), normalmente el escenario principal donde la aceleración de hardware no está disponible, y ofrece una gran compatibilidad y soporte para protocolos complejos. Si bien es flexible, puede generar cuellos de botella en la CPU bajo cargas de ancho de banda elevadas, especialmente cuando se ejecutan funciones avanzadas.

Nota: Cuando la aceleración de red está habilitada, las siguientes funciones no funcionarán correctamente: Estadísticas de velocidad del cliente, Estadísticas de tráfico, Límite de velocidad, Control parental y VPN con IPv6.

14.12 Configuración NAT

Inicie sesión en su enrutador’panel de administración web y navegue hasta **RED** > **Configuración NAT**. Esta página le permite configurar dos funciones clave relacionadas con NAT: NAT de cono completo y SIP ALG.



- **NAT de cono completo**: Puede usarse para reducir la latencia del juego, mejorando la capacidad de respuesta de los juegos en línea. Sin embargo, habilitar Full Cone NAT puede ser menos seguro ya que permite conexiones entrantes sin restricciones.
- **ALG SIP**: está destinado a mitigar los efectos de múltiples NAT en el tráfico SIP (Protocolo de inicio de sesión) . Sin embargo, en la mayoría de los casos, no ayudará e incluso puede afectar las llamadas VoIP, causando problemas como audio unidireccional, teléfonos que no suenan, caídas inesperadas de llamadas o llamadas que van directamente al correo de voz.

Capítulo 15

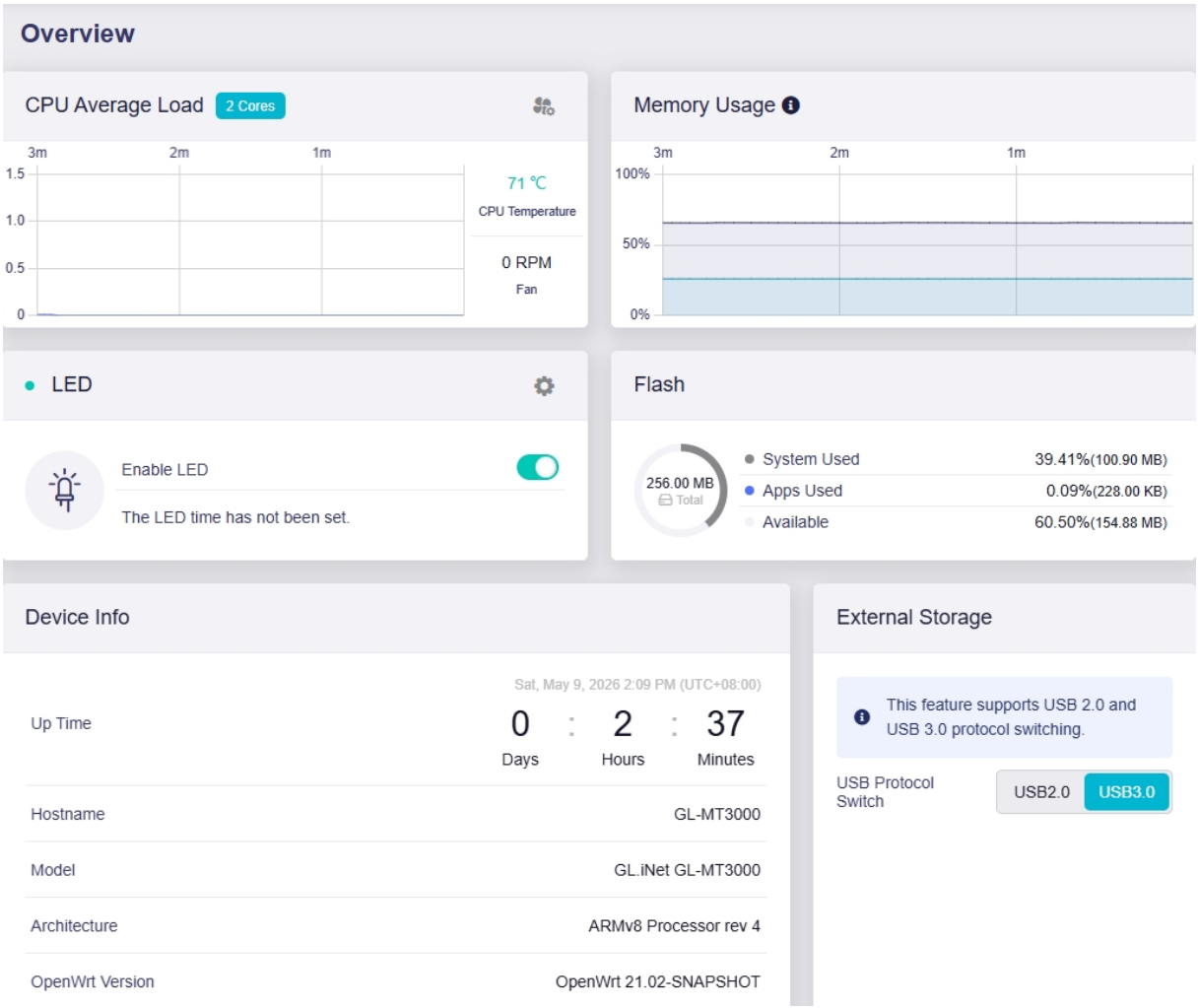
Sistema

Este capítulo cubre las herramientas de administración del sistema para el dispositivo, como descripción general del sistema, actualización, tareas programadas, zona horaria, registro, restablecimiento de firmware y configuraciones avanzadas.

15.1 Descripción general

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

- CPU, memoria, y Flash Estado
- LED Control
- Dispositivo IInformación
- Almacenamiento externo Conmutador de protocolo

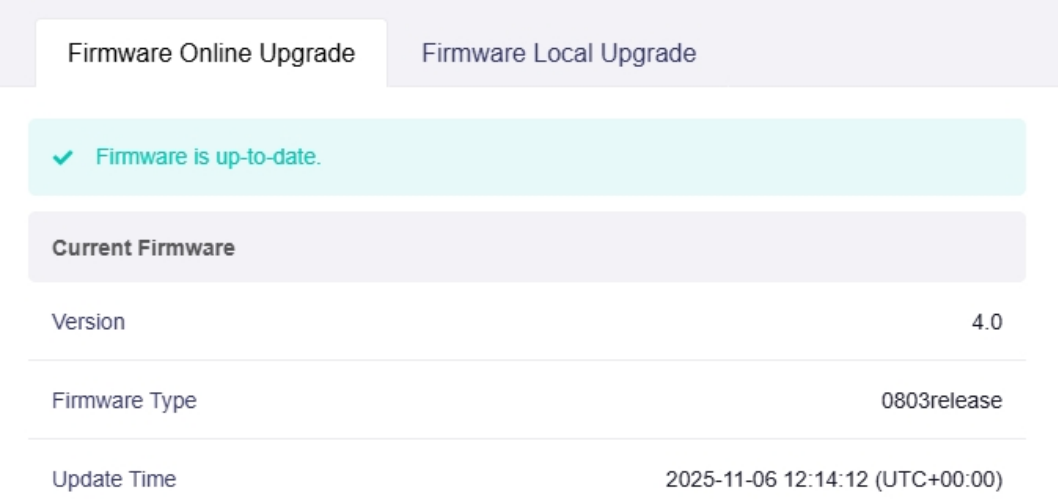


15.2 Actualización

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Actualización**. Puedes actualizar la versión de firmware del enrutador mediante actualización en línea o actualización local.

15.2.1 Actualización de firmware en línea

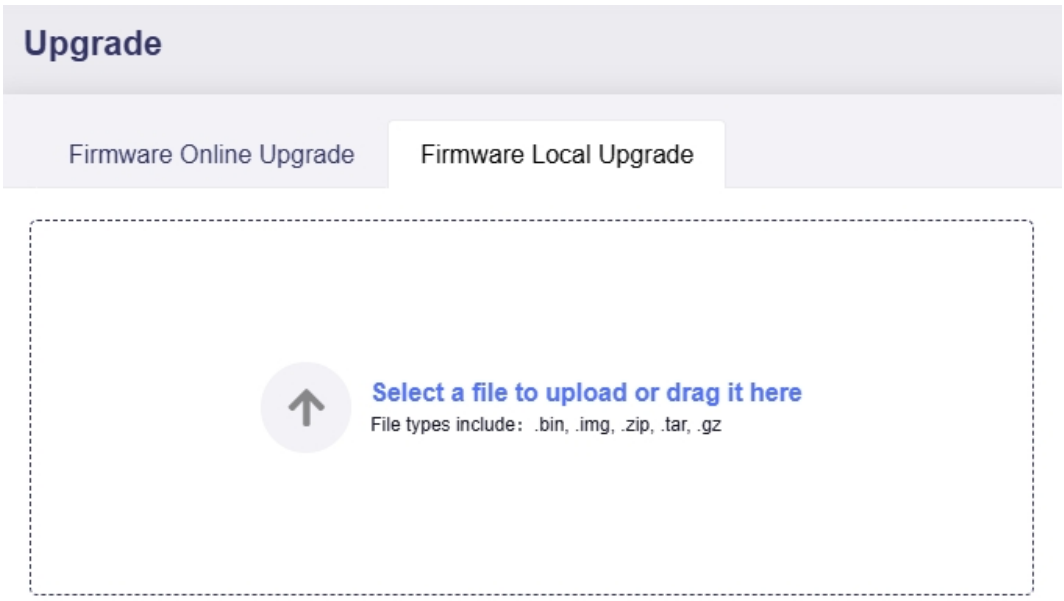
Puede busque el firmware actual detalles aquí, incluida la versión del firmware, el tipo de firmware (por ejemplo, versión, beta) y el tiempo de actualización. Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.



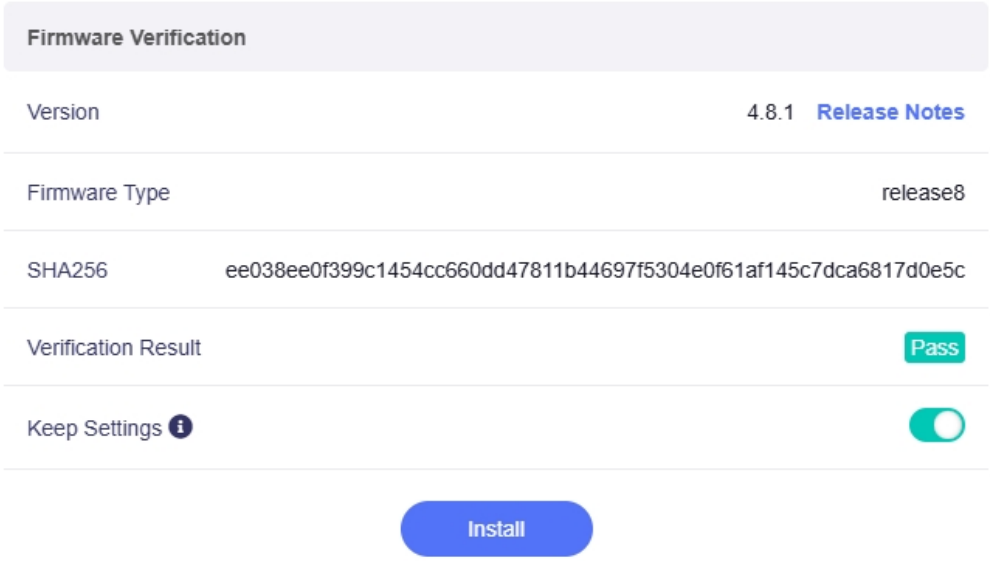
Consejo: Al intentar realizar una actualización en línea, si muestra **Descarga fallida**, navegue hasta **SISTEMA** -> **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

15.2.2 Actualización local de firmware

La actualización local no depende de una conexión a Internet para el enrutador. Descargue el paquete de firmware correcto (que coincida con el modelo de su enrutador) desde el Centro de descargas oficial a su dispositivo local. Luego inicie sesión en el's panel de administración web del enrutador, navegue hasta **SISTEMA** > **Actualización** > **Actualización local** y cargue el paquete de firmware.



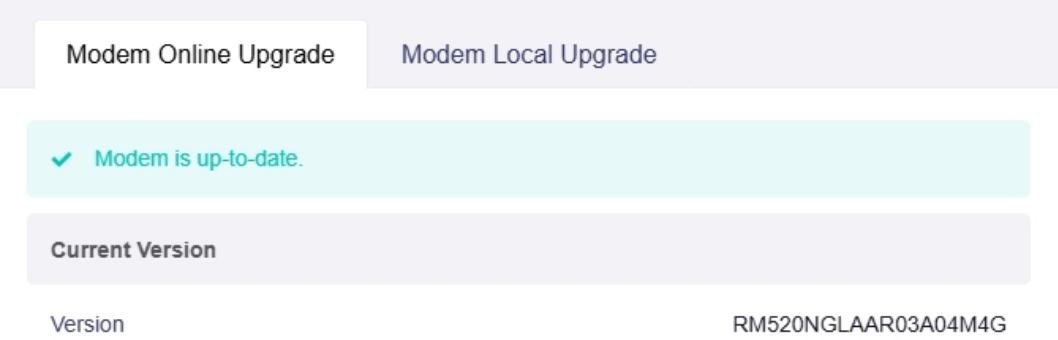
Ta página mostrará los detalles del firmware. Verifique estos detalles antes de hacer clic **Instalar**.



- **Mantener configuración**: si está habilitado, se conserva la configuración actual. Sin embargo, cualquier paquete instalado manualmente debe reinstalarse una vez completada la actualización. No habilite esta opción al degradar el firmware.

15.2.3 Actualización en línea del módem

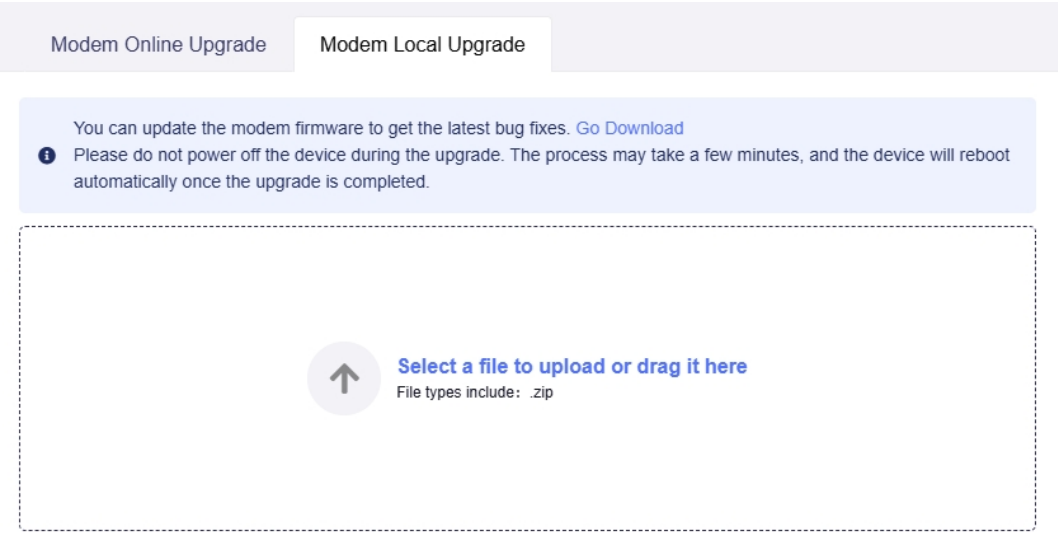
Los enrutadores celulares GL.iNet permiten a los usuarios ver y actualizar el firmware del módem celular a través de la web Panel de administración.
Puede encontrar la versión actual del módem celular aquí. Si su enrutador está conectado a Internet, buscará automáticamente la última versión del módem celular desde el servidor del fabricante, simplificando el proceso de actualización.



15.2.4 Actualización local del módem

Puede probar una actualización del módulo celular cuando la red celular falla o experimenta inestabilidad. Recomendamos comunicarse con el soporte técnico para solucionar problemas antes de realizar la actualización del módem.

Cargue manualmente un archivo de firmware del módem para actualizar el módem celular si es necesario.



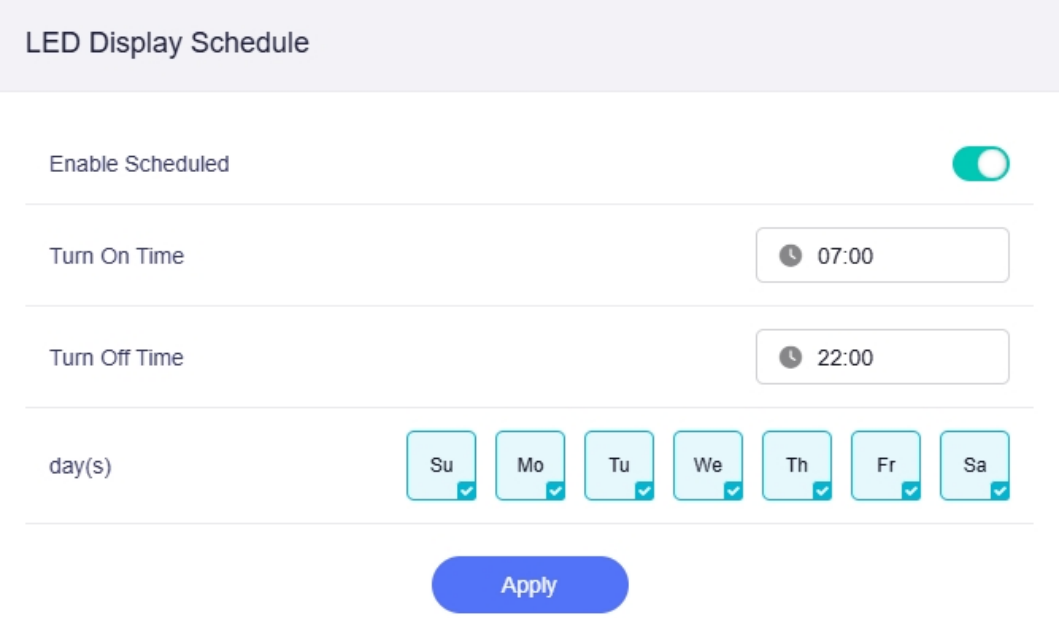
15.3 Tareas programadas

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Tareas programadas**. Esta La página le permite configurar un cronograma diario para algunas acciones básicas, incluido encender y apagar la luz LED , y reiniciar el enrutador.

Nota: sincronice la hora en la Zona horaria antes de utilizar esta función. Si el dispositivo se apaga a la hora programada, la tarea no se ejecutará.

15.3.1 Programación de los indicadores LED

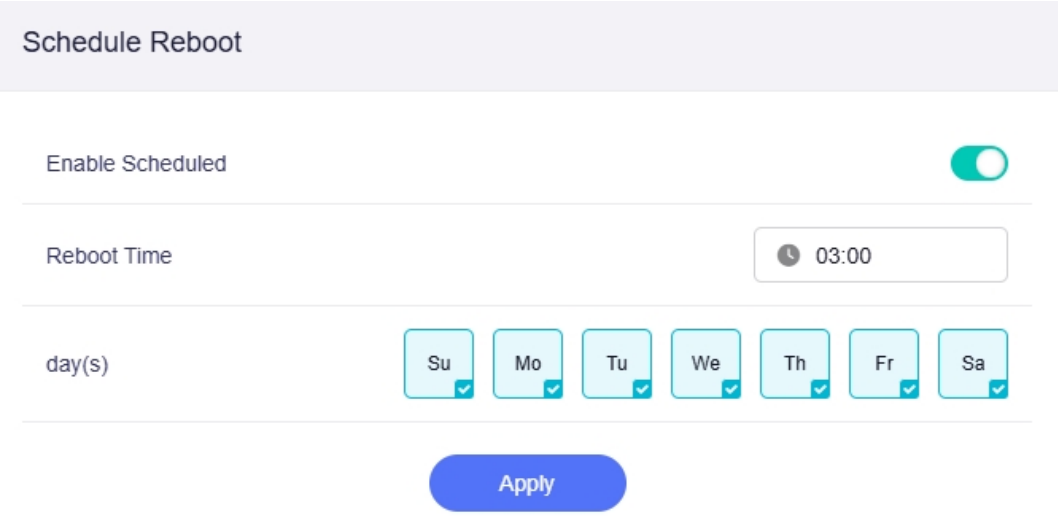
Set a programe la luz LED de su enrutador si es necesario, luego haga clic **Aplicar**.



- **Habilitar programado**: active este interruptor para habilitar el LED programación de visualización.
- **hora de encendido**: establezca la hora (p. ej., 07:00) en la que se encenderá la luz LED .
- **hora de apagado**: establezca la hora (p. ej., 22:00) en la que La luz LED se apagará.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

15.3.2 Programar reinicio

Sestablezca un programa para reiniciar automáticamente su enrutador si es necesario, luego haga clic **Aplicar**.



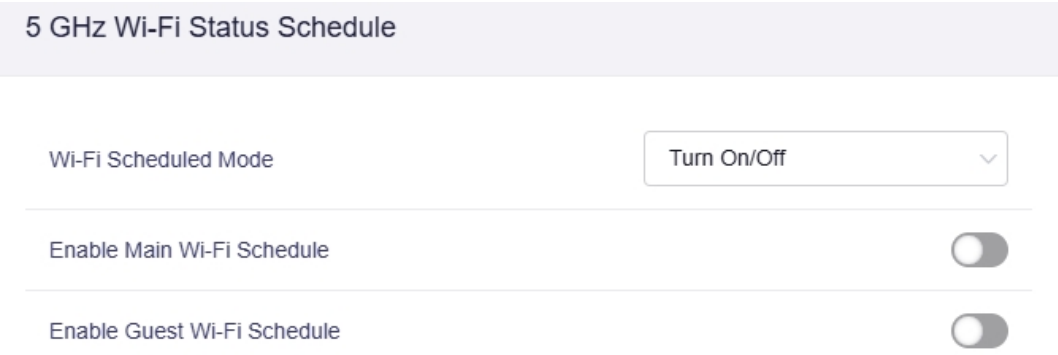
- **Habilitar programado**: active este interruptor para habilitar el reinicio programado.
- **Tiempo de reinicio**: establezca la hora específica (por ejemplo, 03:00) a la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

15.3.3 Programación de Wi-Fi de 5 GHz

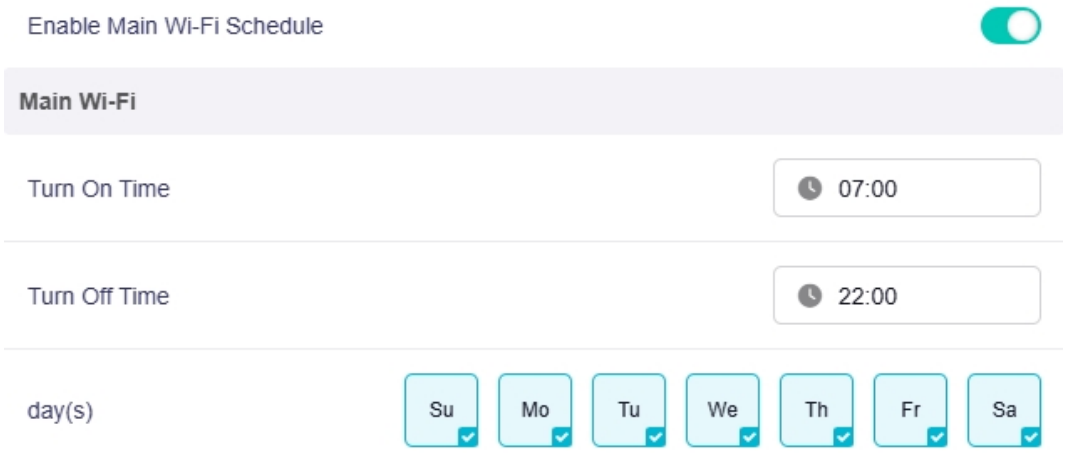
Esta función le permite establecer una programación para su Wi-Fi de 5 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

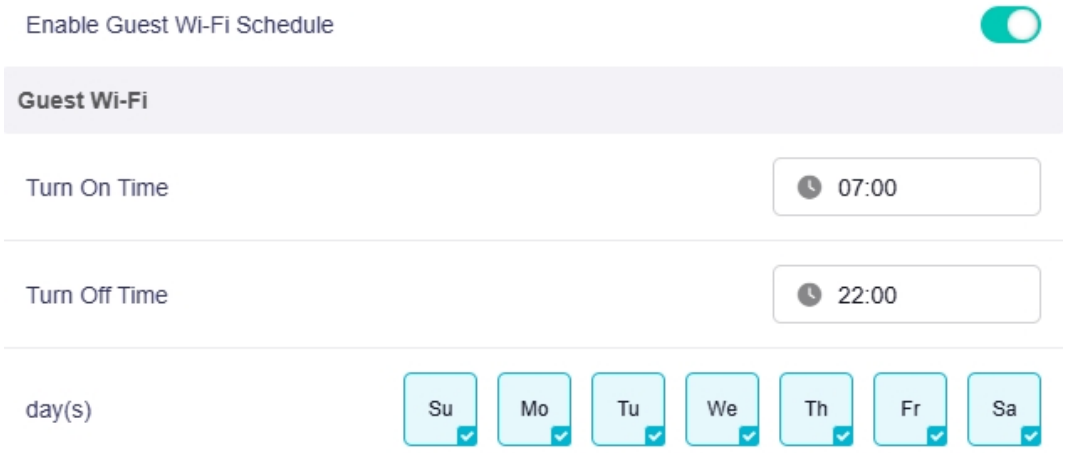
Puedes habilitar el horario de encendido/apagado tanto para Wi-Fi principal de 5 GHz como para invitados. Wi-Fi.



- **Programación de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 5 GHz y seleccione una fecha efectiva para la semana.

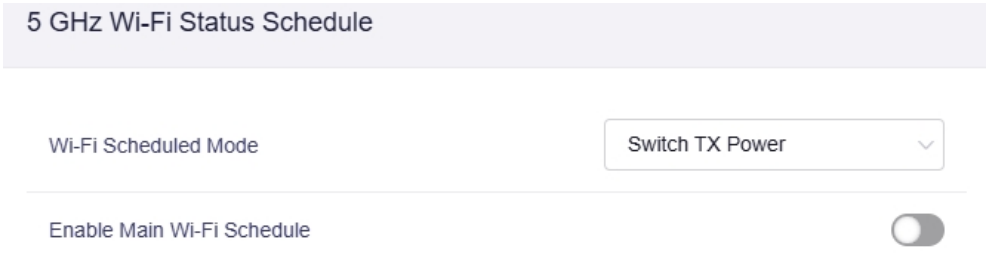


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz y seleccione una fecha efectiva para la semana.

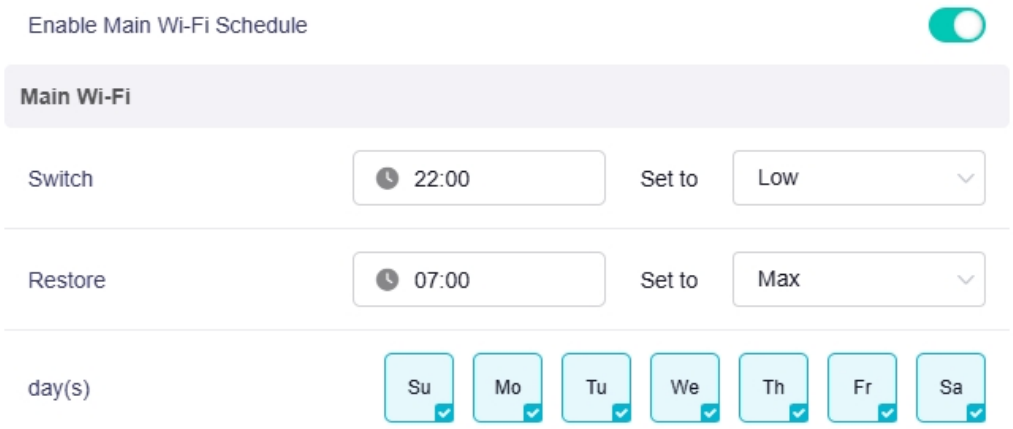


Modo 2: cambiar la alimentación de TX

Ypuede habilitar el cambio de energía TX programación para el 5GHz principal Wi-Fi.



Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 5 GHz cambie la alimentación de transmisión y seleccione una fecha efectiva para la semana.



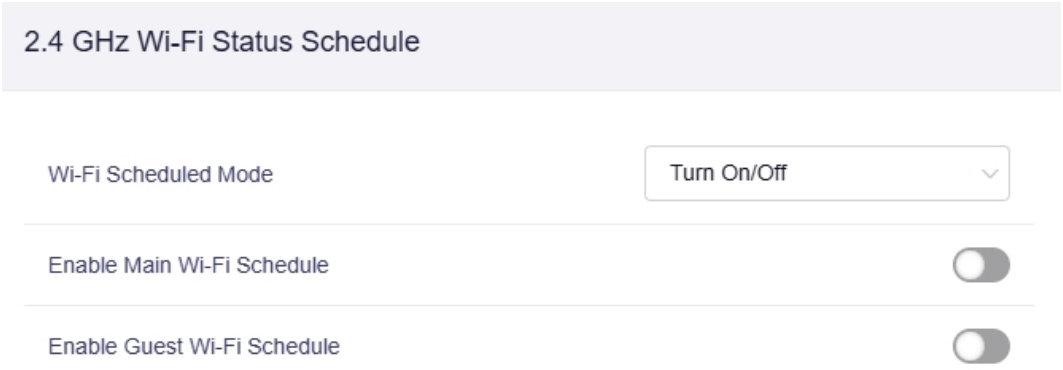
- **Cambiar**: Sestablece la potencia de TX a un cierto nivel (por ejemplo, bajo) at un hora (por ejemplo, 22:00).
- **Restaurar**: Restablecer energía TX en unotro nivel (por ejemplo, Max) at en otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para estas configuraciones.

15.3.4 Programación de Wi-Fi de 2,4 GHz

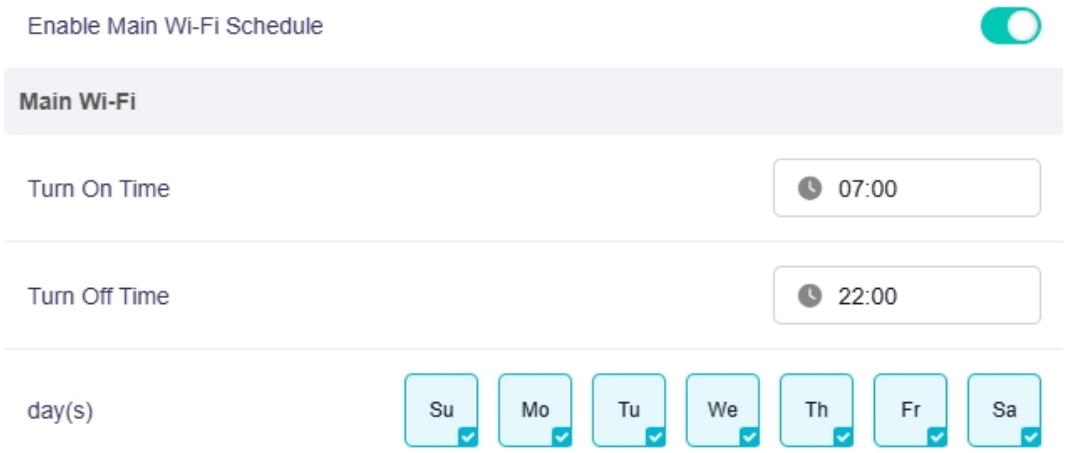
Esta función le permite establecer una programación para su Wi-Fi de 2,4 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

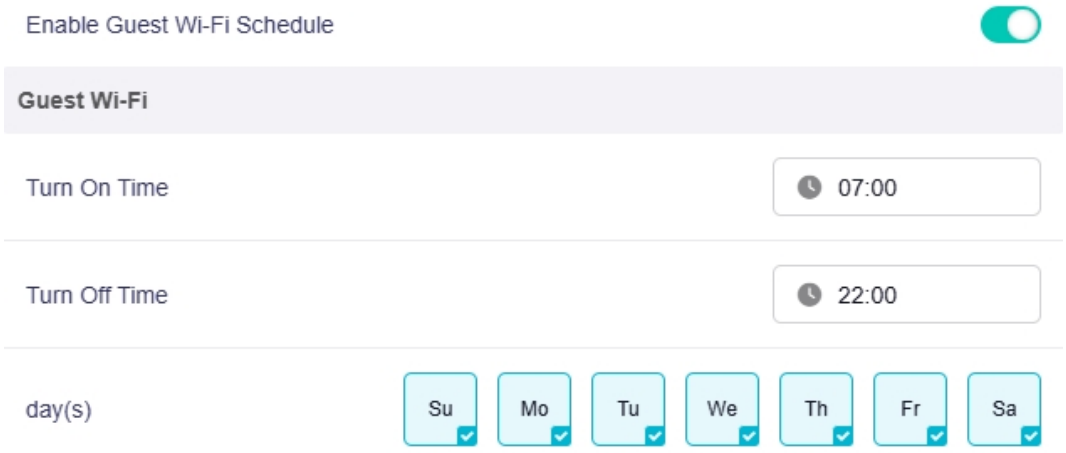
Puedes habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para los invitados. Wi-Fi.



- **Programación de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 2,4 GHz y seleccione una fecha efectiva para la semana.

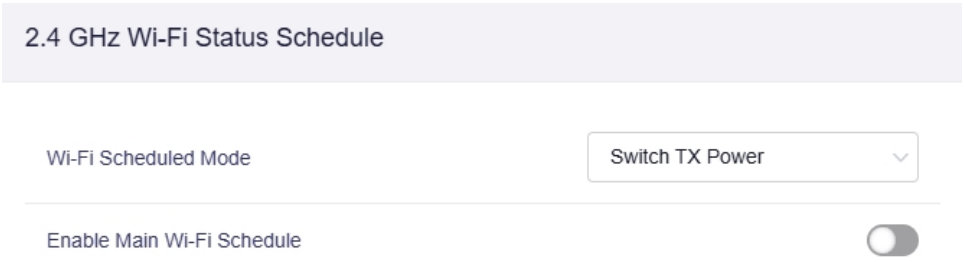


- **Wi-Fi para invitados Programación**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 2,4 GHz y seleccione una fecha efectiva para la semana.

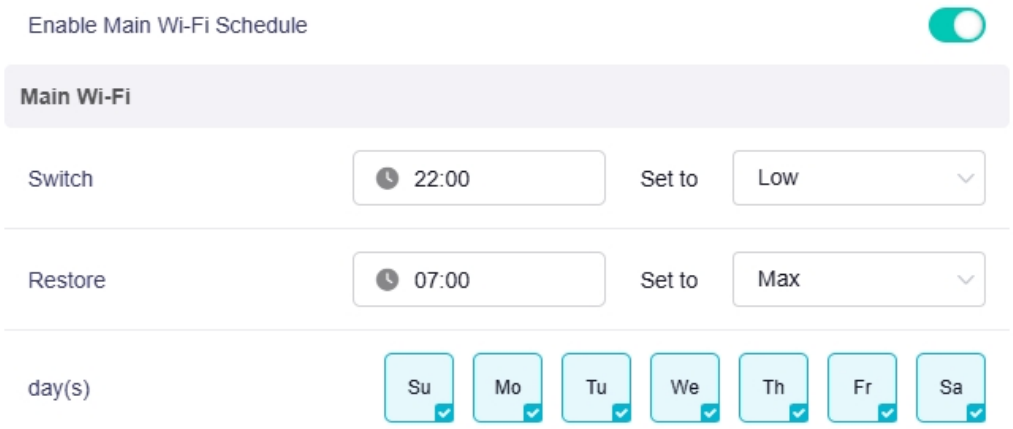


Modo 2: cambie la alimentación de TX

Ypuede habilitar el cambio de alimentación TX programación para el 2,4 GHz Wi-F principali.



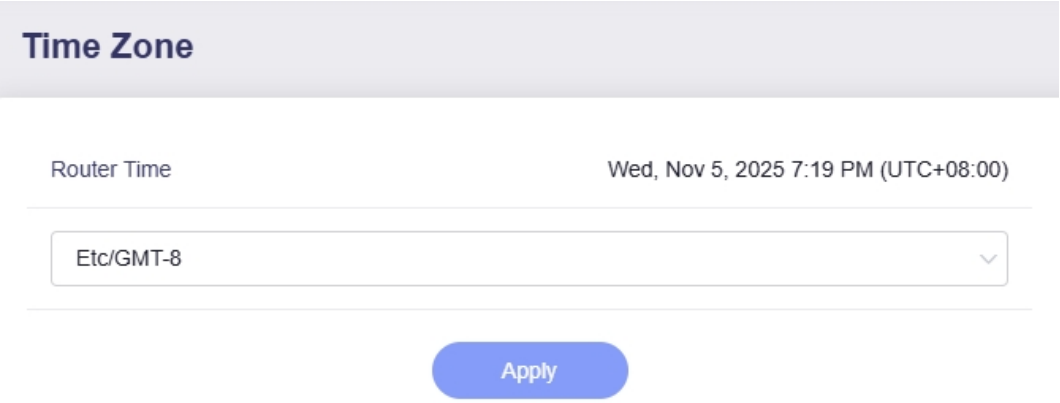
Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 2,4 GHz cambie la alimentación de TX y seleccione una fecha efectiva para la semana.



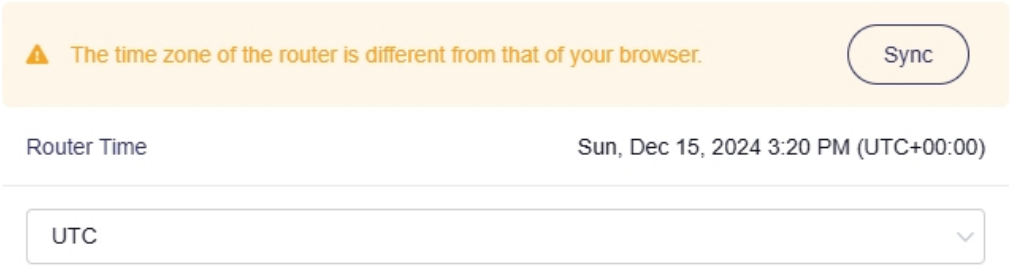
- **Cambiar**: Set TX Power a un cierto nivel (por ejemplo, bajo) at una hora específica (por ejemplo, 22:00).
- **Restaurar**: Restorar energía TX en unotro nivel (p. ej., máx.) aen otro momento (p. ej., 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

15.4 Zona horaria

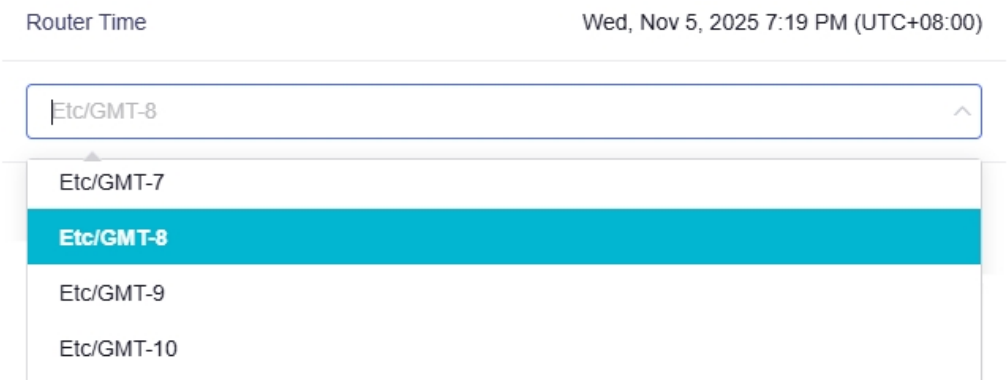
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen de la hora del sistema del enrutador’para surtir efecto. Asegúrese de que la zona horaria correcta esté sincronizada correctamente. Si la zona horaria del enrutador’es diferente a la de su navegador, se mostrará el siguiente mensaje. Haga clic en el botón **Sincronizar** para sincronizar la zona horaria.

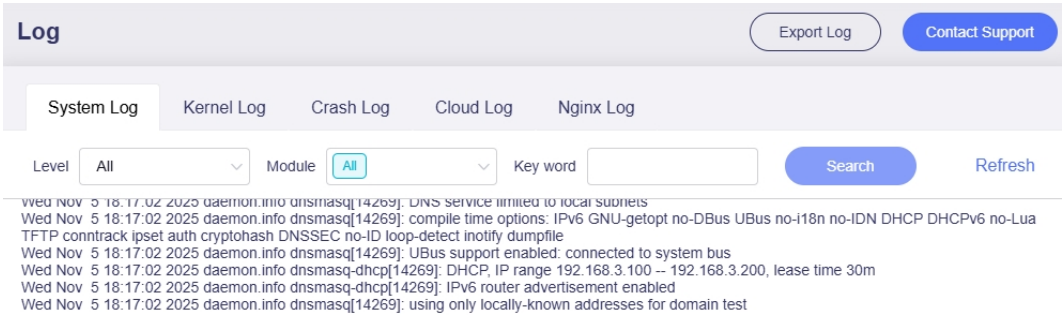


Para cambiar zona horaria, sseleccione la zona horaria adecuada de la lista para garantizar que la hora del sistema coincida con su hora local.

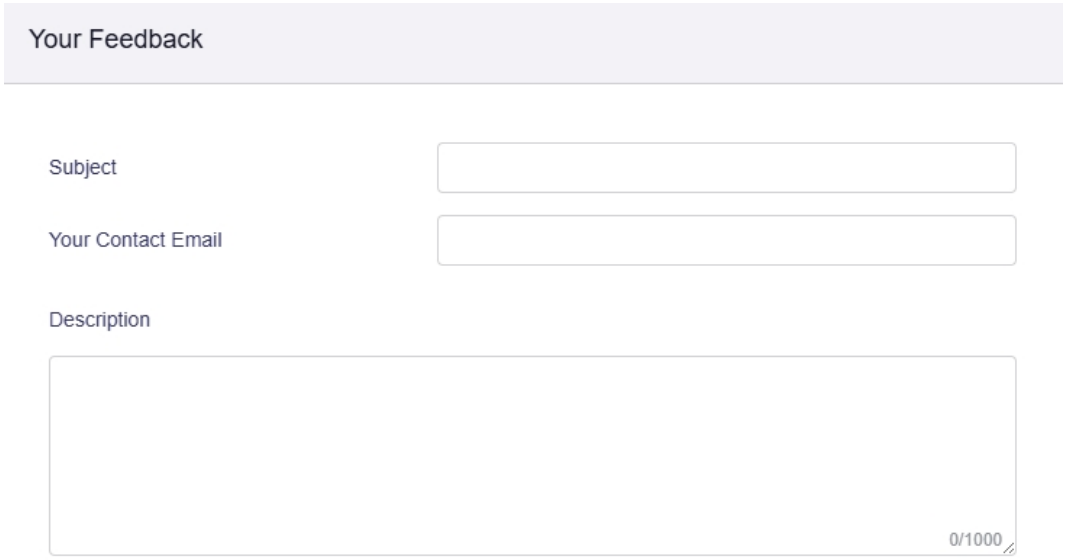


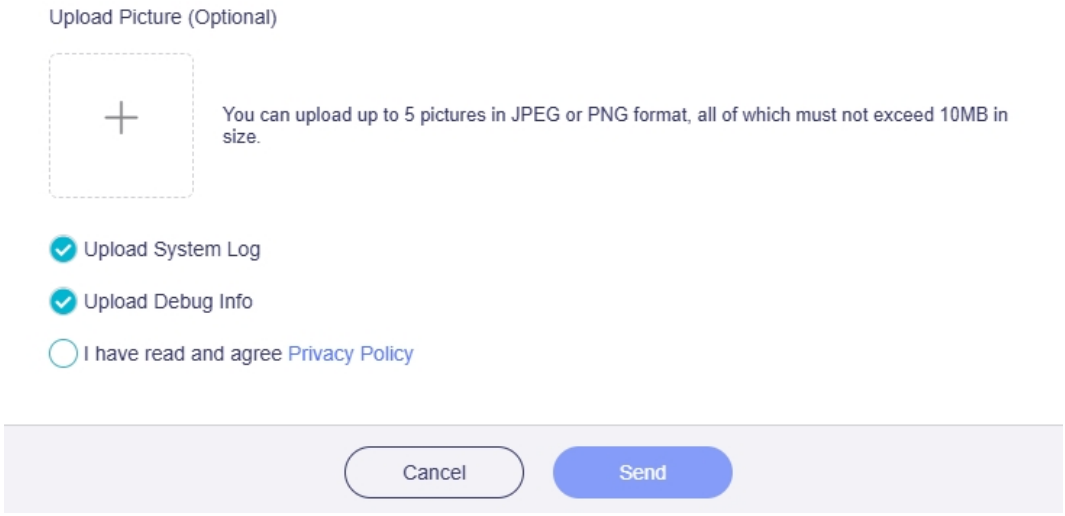
15.5 Registro

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Registro**. Esta página le permite ver registros del sistema, kernel, bloqueo, nube y Nginx para análisis y solución de problemas.



- **Buscar**: la página de registro del sistema proporciona filtrado para una búsqueda rápida. Puede seleccionar el nivel de registro (por ejemplo, todo, información, error) o el módulo (por ejemplo, IPv6, Anclaje, Celular) de la lista desplegable, o ingrese palabras clave para consultar registros rápidamente.
- **Actualizar**: Haga clic en este botón para actualizar logs.
- **Exportar registro**: Haga clic en este botón para exportar información de depuración junto con los registros.
- **Comuníquese con el soporte técnico**: haga clic en este botón, complete la información detallada en la ventana emergente de la derecha y luego haga clic en **Enviar**. Sus comentarios se enviarán directamente a GL.iNet Soporte técnico.




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

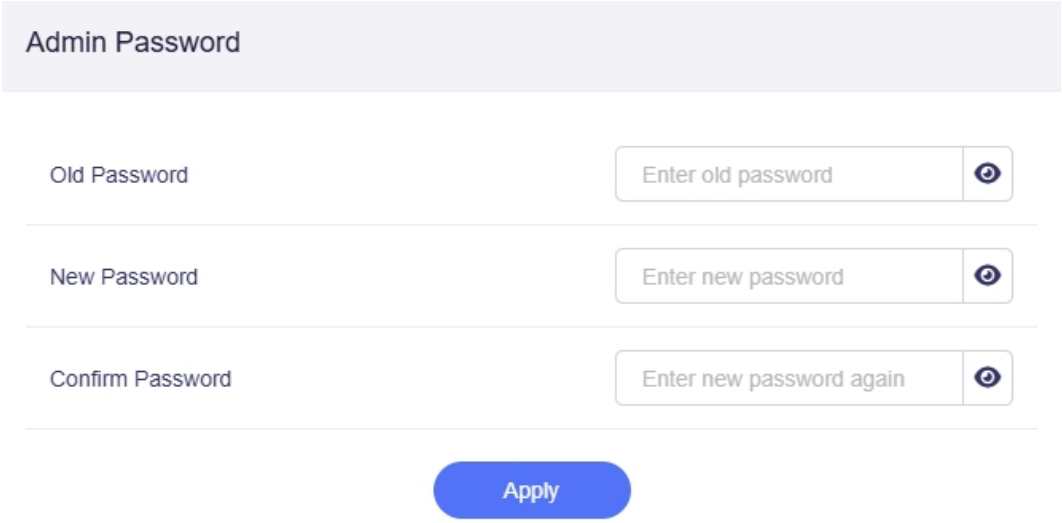
15.6 Seguridad

Iniciar sesión al panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Seguridad**. Esta página contiene opciones de configuración para la administración local y remota del enrutador, incluido:

- Admin password
- Acceso local para web panel de administración, LuCI y SSH
- Remoticón HTTPS/SSH unacceso
- Opuertos de lápiz en rexterno

15.6.1 Contraseña de administrador

En esta sección, puede cambiar la contraseña de inicio de sesión del panel de administración web.

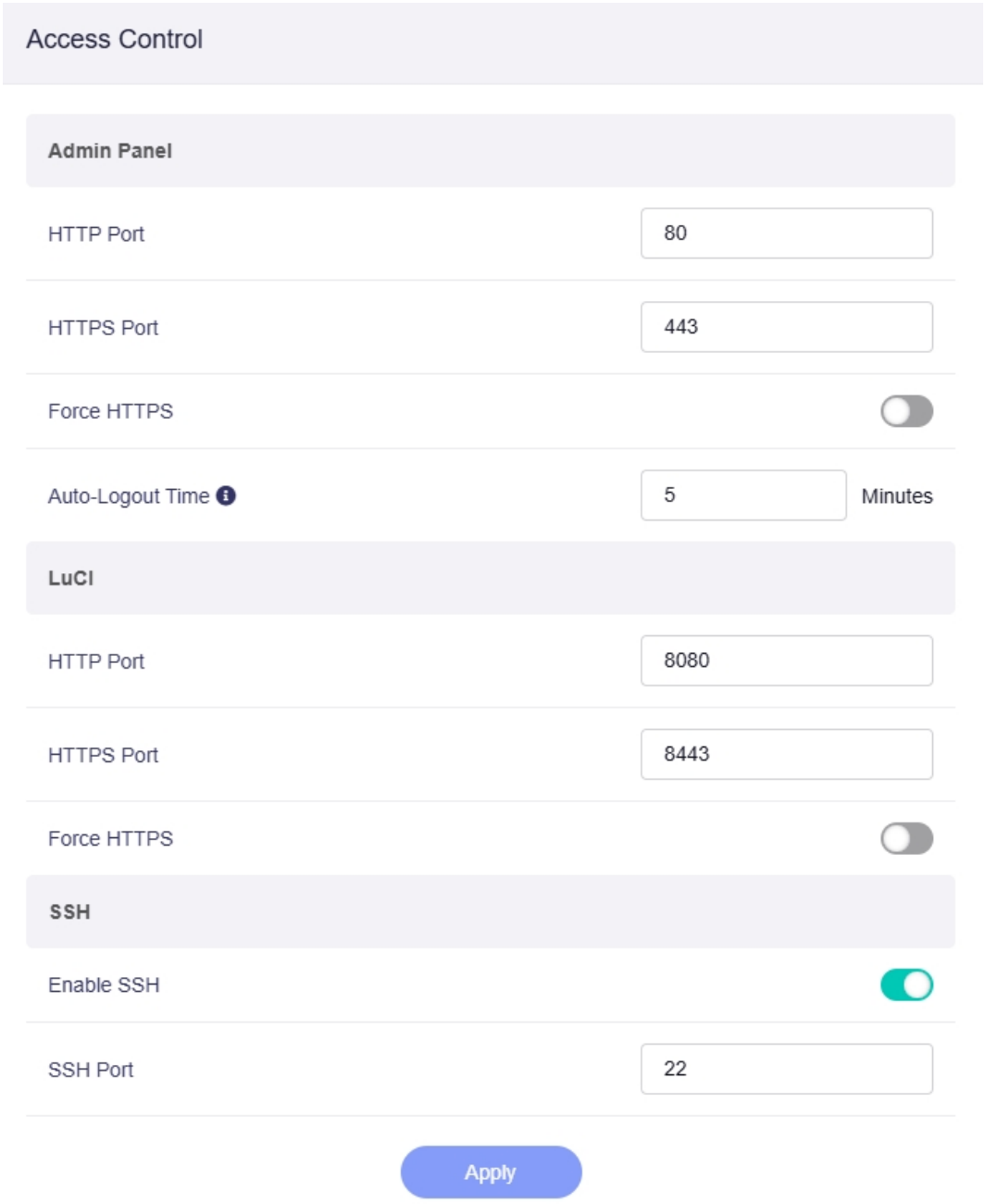


Los requisitos para la contraseña de administrador son los siguientes:

1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distingue entre mayúsculas y minúsculas), números y símbolos (p. ej., ! @ # $ % ^ & * ( ) _ + - = , . > < | \ [ ] { } : ; " ' ` ~).
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números y símbolos). data-r="4735">15.6.2 Control de acceso

15.6.2 Control de acceso

Esta sección administra el acceso a las múltiples interfaces del enrutador' (Panel de administración, LuCI y SSH. Puede evitar intentos de escaneo e intrusión en el puerto predeterminado y evitar problemas de red causados por conflictos de puertos.



Panel de administración

- **Puerto HTTP**: el valor predeterminado es 80, utilizado para acceso HTTP sin cifrar al panel de administración web.

- **Puerto HTTPS**: el valor predeterminado es 443, utilizado para el acceso HTTPS seguro al panel de administración web.
- **Forzar HTTPS**: cuando está habilitado, el acceso al panel de administración web se aplica para utilizar un HTTPS seguro conexión.
- **Tiempo de cierre de sesión automático**: configurado en 5 minutos de forma predeterminada, cierra automáticamente las sesiones de administrador inactivas después de esta duración por motivos de seguridad. Puede personalizar el tiempo de cierre de sesión automático, que oscila entre 1 minuto y 3 horas.

LuCI

Nota: instale LuCI en la Configuración avanzada antes de configurar el control de acceso.

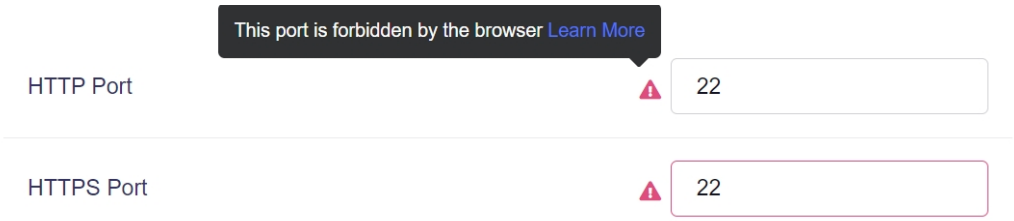
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para un acceso HTTPS seguro a la interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, el acceso a la interfaz LuCI se aplica para utilizar una conexión HTTPS segura.

SSH

- **Habilitar SSH**: Ehabilitado de forma predeterminada, controla si el acceso SSH al enrutador está permitido.
- **puerto SSH**: el valor predeterminado es 22, el puerto utilizado para el acceso SSH al enrutador.

Nota:

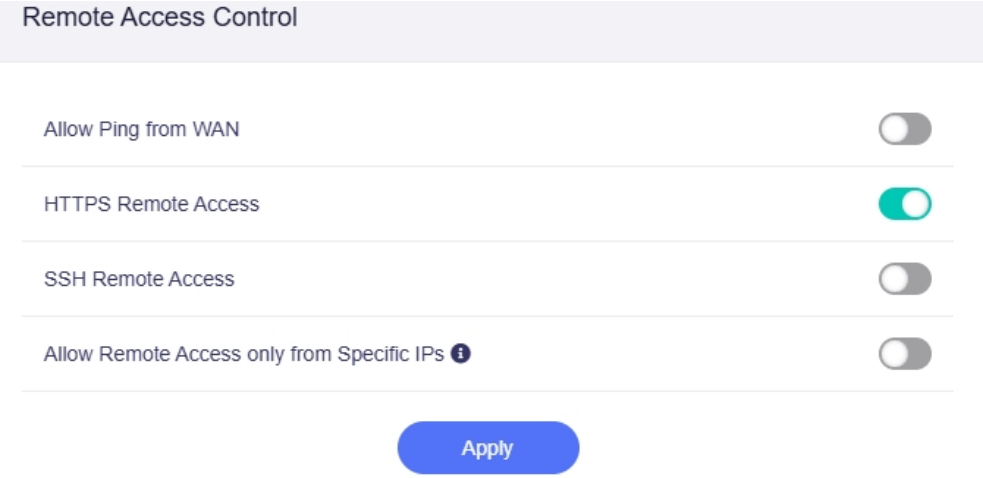
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indica "Este puerto está prohibido por el navegador".



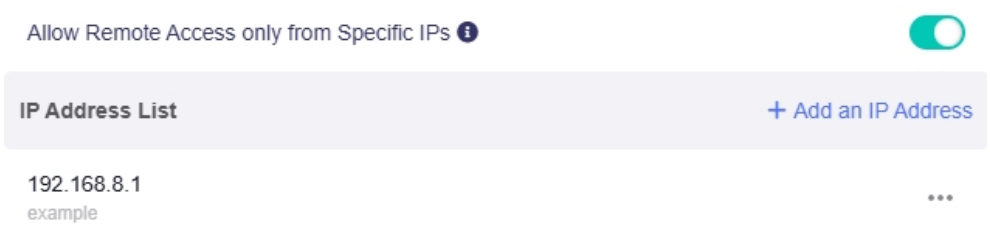
2. Si el número de puerto se modifica en el firmware, debe ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.
3. La configuración de acceso a LuCI está disponible solo después de instalar LuCI. vaya a **SISTEMA** > **Configuración avanzada** para instalar LuCI.

15.6.3 Control de acceso remoto

Esta sección administra el acceso remoto a las interfaces del enrutador, incluidos HTTPS, SSH y ping del lado WAN. También le permite restringir el acceso desde direcciones IP específicas, logrando un equilibrio entre la accesibilidad remota y la seguridad de la red.

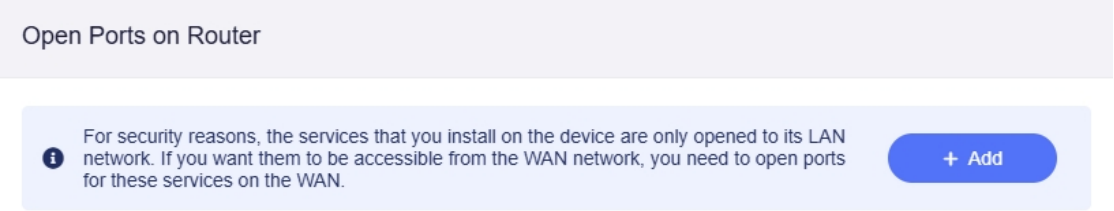


- **Permitir ping desde WAN**: Apermitir ping desde la WAN lado puede ayudar a los usuarios a verificar si el enrutador está accesible a través de la WAN cuandocuando hay un problema de red, así como para determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El acceso remoto HTTPS permite el acceso remoto seguro al panel de administración web del enrutador a través del protocolo HTTPS. Garantiza la transmisión de datos cifrados al administrar el enrutador de forma remota a través de un navegador web.
- **Acceso remoto SSH**: El acceso remoto SSH permite un acceso seguro al enrutador terminal. Permite a los usuarios administrar remotamente el enrutador a través de SSH, estableciendo un túnel cifrado para tareas.
- **Permitir acceso remoto desde IP específicas**: esta función solo está disponible cuando cualquiera de las tres funciones anteriores está habilitada. Puede agregar varias direcciones IP especificadas para administrar de forma remota el enrutador solo desde dispositivos con estas IP.

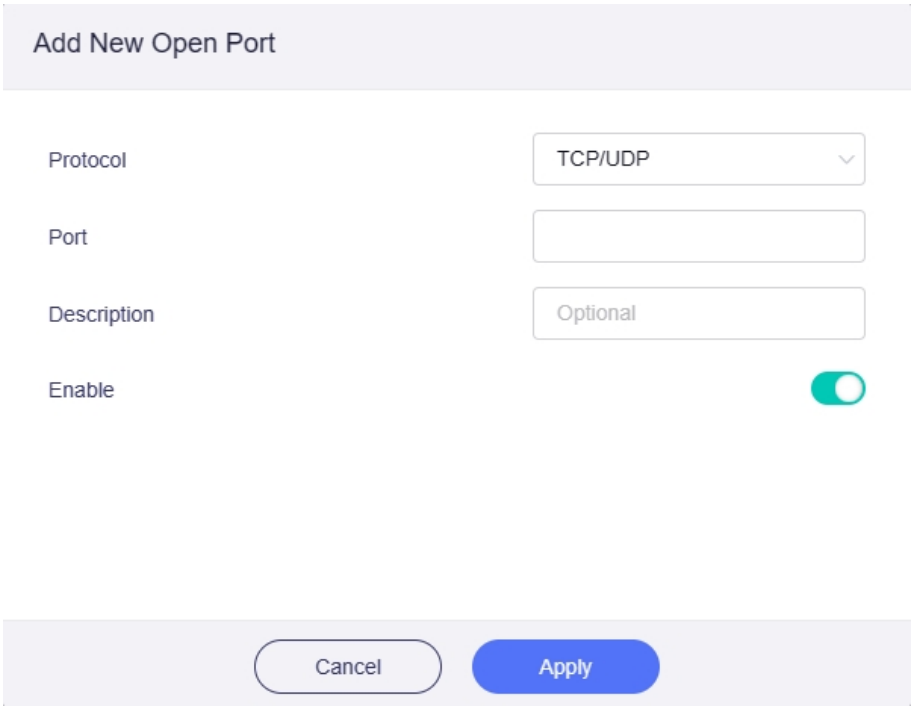


15.6.4 Abrir puertos en el enrutador

Esta sección administra el reenvío de puertos para los servicios en su enrutador. Algunos servicios, como web y FTP, requieren que sus respectivos puertos estén abiertos en el enrutador para poder acceder públicamente desde la red WAN. Por razones de seguridad, solo se puede acceder a los servicios instalados en el dispositivo dentro de la LAN de forma predeterminada. Si necesita habilitar dicho acceso WAN, puede abrir puertos específicos aquí.



Para abrir un puerto, haga clic en **Agregar** e ingrese la información requerida en la ventana emergente.

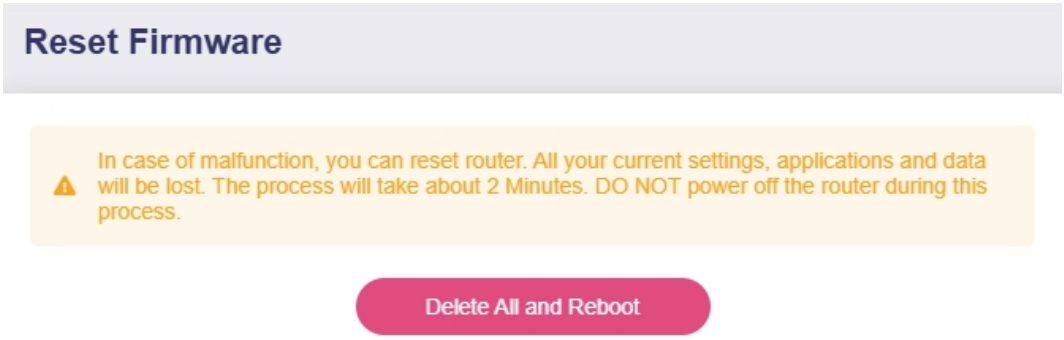


- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.
- **Descripción** (Opcional): agregue una breve nota para describir el propósito de este puerto abierto (por ejemplo, “Servidor web” o “Servicio FTP”) para una administración más sencilla.
- **Activar**: active o desactive el reenvío de puertos regla.

15.7 Restablecer firmware

Si el enrutador no funciona correctamente, puede intentar resolvering solucione el problema restableciendo el firmware

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Restablecer firmware**. Hacer clic **Eliminar todo y reiniciar** para restablecer el firmware si es necesario.



Nota: Todas sus configuraciones, aplicaciones y datos actuales serán borrados. El proceso tomará aproximadamente 2 minutos. Nono apague el enrutador durante este proceso.

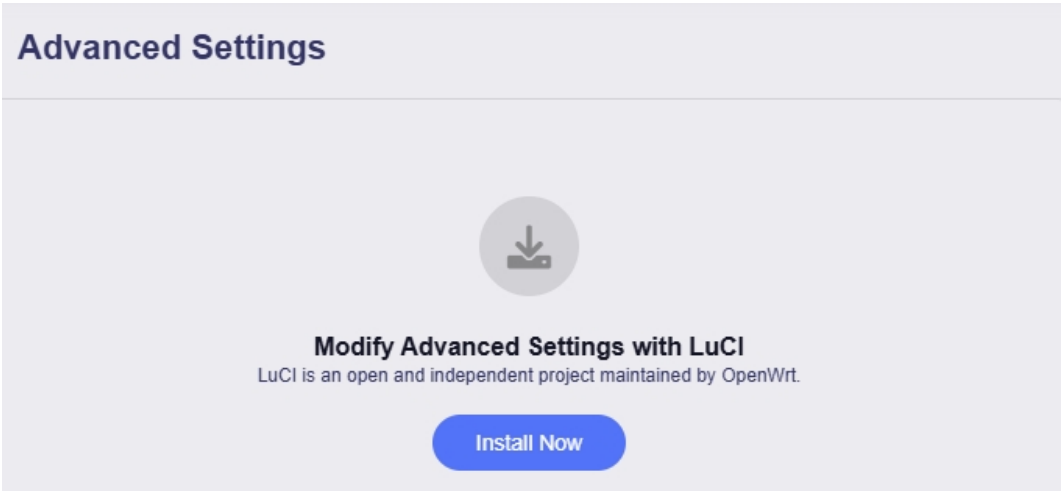
Si no puede acceder al enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el lateral.

15.8 Configuración avanzada

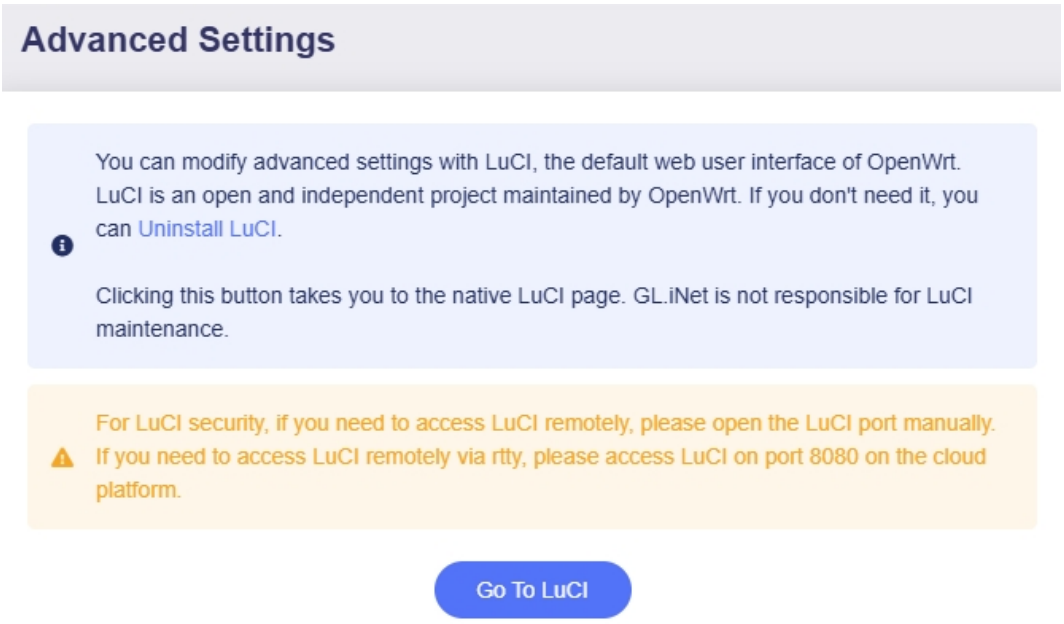
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMAConfiguración avanzada**. Esta página le permite modificar la configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto e independiente mantenido por OpenWrt, LuCI se proporciona tal cual. GL.iNet no es responsable del mantenimiento de LuCI.

Siga los pasos siguientes para iniciar sesión en la interfaz de LuCI.

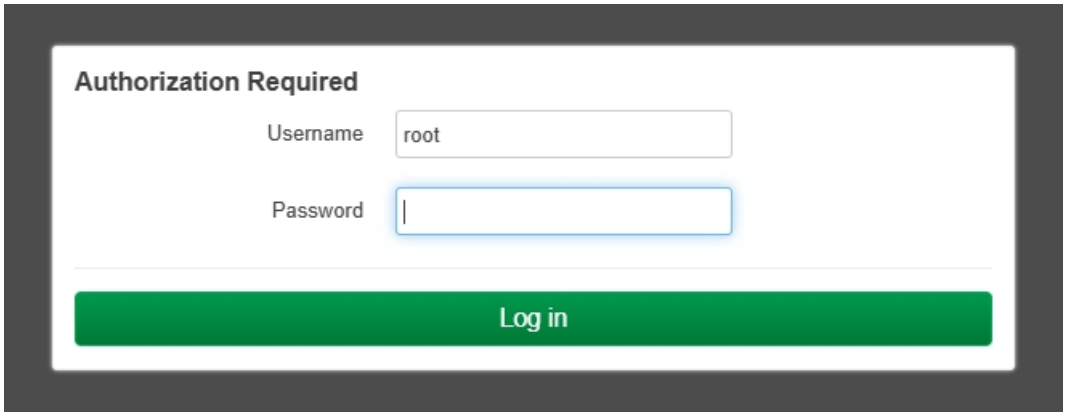
1. Haga clic en **Instalar ahora**, y se instalará la interfaz LuCI.



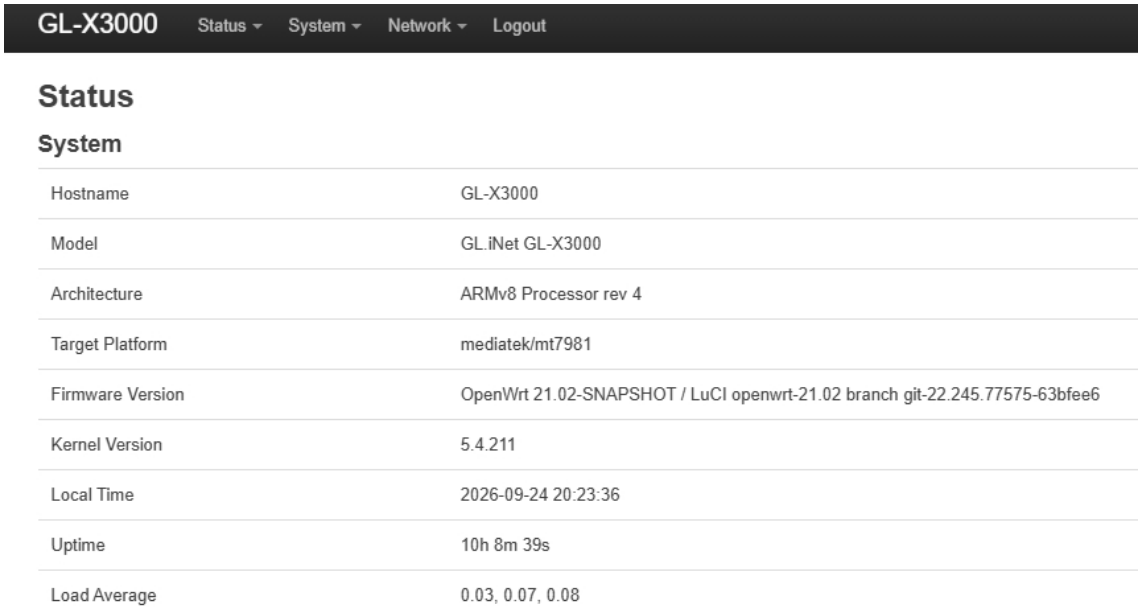
2. Click **Ir a LuCI**, y será redirigido a la página de inicio de sesión de LuCI.



3. Ingrese la contraseña de inicio de sesión, que es la misma que la contraseña del panel de administración web.



Ylo hará luego registre en en la interfaz LuCI .



Declaración de Conformidad

Por la presente, GL TECHNOLOGIES (HONG KONG) LIMITED declara que el tipo de equipo de radio [Router Wi-Fi 6 5G NR, GL-X3000NR / Router Wi-Fi 6 4G LTE, GL-X3000C16] cumple los requisitos esenciales y demás disposiciones pertinentes de la Directiva 2014/53/UE. El texto completo de la declaración UE de conformidad está disponible en la siguiente dirección de internet: https://www.gl-inet.com/products/certificate.