GL·iNet



Manual de usuario

GL-E5800 / Mudi 7

Enrutador de viaje Wi-Fi 7 tribanda 5G NR

Versión de firmware 4.8.5

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
- Elegir una ubicación adecuada para el dispositivo
- 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 (p. ej., 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 6

1.1 Descripción general del producto 7

1.1.1 Apariencia 7

1.1.2 Interfaz y botón 8

1.1.3 Pantalla táctil 9

1.2 Especificaciones 11

1.3 Bandas de frecuencia 12

1.4 Contenido del paquete 13

Capítulo 2 Inicialización del enrutador 14

Capítulo 3 Iniciar sesión en el enrutador 16

Capítulo 4 Configurar la conexión a Internet 18

4.1 Asistente de configuración rápida 19

4.2 Configurar manualmente la conexión a Internet 20

4.2.1 Conectarse a Internet mediante la red móvil 22

4.2.2 Conectarse a Internet mediante un cable Ethernet 27

4.2.3 Conectarse a Internet mediante una red Wi-Fi existente 33

4.2.4 Conectarse a Internet mediante conexión compartida por USB 37

4.2.5 Conectarse a Internet mediante Ethernet por USB 39

Capítulo 5 Red inalámbrica 41

5.1 Visualización del estado de Wi-Fi 42

5.2 Configuración inalámbrica 44

5.2.1 Wi-Fi de 5 GHz y 6 GHz 44

5.2.2 Wi-Fi de 2,4 GHz 47

5.2.3 BSSID aleatorio 49

Capítulo 6 Clientes 51

6.1 Detalles del dispositivo 53

6.2 Acción 55

6.3 Eliminar clientes 58

6.4 Ordenar 59

Capítulo 7 Servicios en la nube 60

7.1 GoodCloud 61

7.1.1 Habilitar GoodCloud....62
7.1.2 Administrar el enrutador....65
7.1.3 Desvincular el dispositivo....70
7.1.4 Desactivar GoodCloud....70
7.2 AstroWarp....71
Capítulo 8 Conozca la VPN....72
8.1 Introducción....73
8.2 Escenarios de aplicación....74
Capítulo 9 Panel de VPN....76
9.1 Asistente de configuración de VPN....77
9.2 Modo VPN....80
9.2.1 Modo global....81
9.2.2 Modo de política....83
Capítulo 10 Configurar el servidor VPN....93
10.1 Configurar el servidor OpenVPN....94
10.1.1 Preparación....94
10.1.2 Pasos de configuración....95
10.1.3 Solución de problemas....97
10.2 Configurar el servidor WireGuard....99
10.2.1 Preparación....99
10.2.2 Pasos de configuración....100
10.2.3 Solución de problemas....103
Capítulo 11 Configurar el cliente VPN....105
11.1 Configurar el cliente OpenVPN....106
11.1.1 Preparación....106
11.1.2 Configurar NordVPN....106
11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)....112
11.2 Configurar el cliente WireGuard....115
11.2.1 Preparación....115
11.2.2 Configurar AzireVPN....116
11.2.3 Configurar Hide.me....120
11.2.4 Configurar IPVanish....123
11.2.5 Configurar Mullvad....127
11.2.6 Configurar NordVPN....131

11.2.7 Configurar PIA (Private Internet Access)..... 136
11.2.8 Configurar Surfshark..... 140
11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)..... 144
Capítulo 12 Red..... 149
12.1 Multi-WAN..... 150
12.1.1 Seguimiento del estado de la interfaz..... 150
12.1.2 Modo Multi-WAN..... 153
12.2 LAN..... 156
12.2.1 Configuración básica..... 156
12.2.2 Servidor DHCP..... 157
12.2.3 Reserva de direcciones..... 159
12.3 Red de invitados..... 160
12.3.1 Configuración básica..... 160
12.3.2 Servidor DHCP..... 161
12.4 DNS..... 163
12.4.1 Configuración del servidor DNS..... 164
12.4.2 Editar hosts..... 167
12.5 Puerto Ethernet..... 169
12.6 IPv6..... 170
12.6.1 Modo IPv6..... 171
12.6.2 Método de obtención de DNS..... 171
12.7 Inspección IGMP..... 172
12.8 Modo de red..... 173
12.9 Puerta de enlace directa..... 175
12.10 Aceleración de red..... 177
Capítulo 13 Control de flujo..... 179
13.1 Control parental..... 180
13.1.1 Configuración rápida..... 180
13.1.2 Solución de problemas..... 189
Capítulo 14 Seguridad..... 190
14.1 Reenvío de puertos..... 191
14.1.1 DMZ..... 191
14.1.2 Reenvío de puertos..... 192
14.2 Acceso de administrador..... 194

14.2.1 Control de acceso..... 194
14.2.2 Control de acceso remoto.....197
14.2.3 Abrir puertos en el enrutador.....198
14.3 Modo NAT..... 200
Capítulo 15 Aplicaciones.....201
15.1 Complementos.....202
15.2 DNS dinámico.....203
15.2.1 Habilitar DDNS..... 203
15.2.2 Comprobar si DDNS funciona.....206
15.2.3 Acceso remoto HTTPS.....208
15.2.4 Acceso remoto SSH..... 210
15.3 Almacenamiento en red..... 212
15.3.1 Conectar una unidad de almacenamiento..... 212
15.3.2 Configurar Samba.....213
15.3.3 Configurar WebDAV..... 216
15.3.4 Configurar DLNA.....219
15.4 AdGuard Home.....220
15.5 Tailscale.....222
15.5.1 Configurar Tailscale.....223
15.5.2 Permitir el acceso remoto a la WAN..... 226
15.5.3 Permitir el acceso remoto a la LAN.....226
15.5.4 Nodos de salida personalizados.....227
15.6 ZeroTier..... 228
15.6.1 Configurar ZeroTier.....229
15.6.2 Permitir el acceso remoto a la WAN..... 233
15.6.3 Permitir el acceso remoto a la LAN.....234
15.7 Tor..... 235
Capítulo 16 Sistema..... 236
16.1 Descripción general.....237
16.2 Contraseña de administrador.....238
16.3 Actualización.....239
16.3.1 Actualización en línea.....239
16.3.2 Actualización local.....240
16.4 Tareas programadas..... 241

16.5 Gestión de visualización..... 242
16.6 USB y alimentación.....243
16.6.1 USB..... 243
16.6.2 Alimentación.....244
16.7 Zona horaria.....246
16.8 Restablecer firmware.....247
16.9 Registro.....248
16.10 Configuración avanzada..... 250
Seguridad de la batería..... 252
Declaración de Conformidad.....253

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

Mudi 7 (GL-E5800) ofrece velocidades 5G ultrarrápidas de hasta 4,67 Gbps y Wi-Fi 7 de tres bandas para una conexión en red confiable y segura. Admite eSIM integrada y modo de espera dual de doble SIM para garantizar una conectividad perfecta. Con una pantalla táctil, un puerto Ethernet de 2,5G, carga rápida y batería de larga duración, el Mudi 7 es su solución todo en uno para conectividad portátil de alto rendimiento.

1.1.1 Apariencia

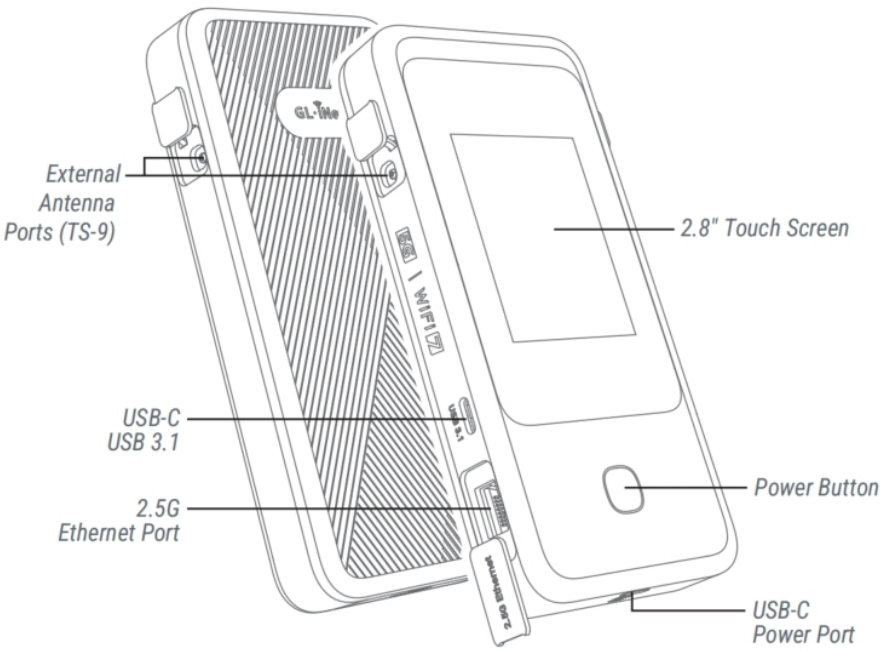






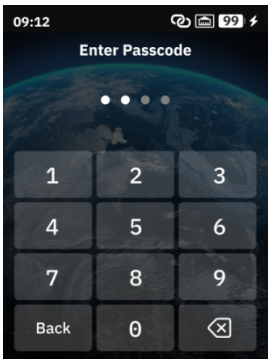
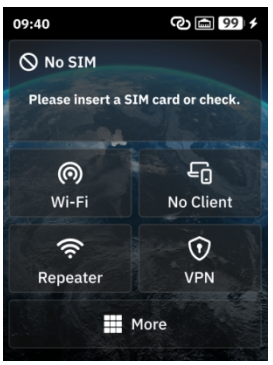


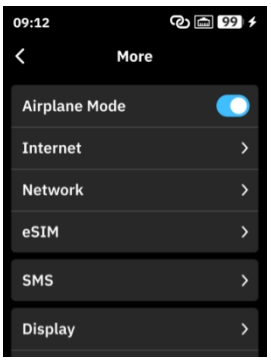
1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Botón de encendido	Presiónelo para activar la pantalla o regresar a la página de inicio.
Puerto Ethernet 2.5G	Como WAN: se conecta a un módem o a una toma Ethernet. Como LAN: se conecta a dispositivos cableados si es necesario.
Puerto USB 3.1	Para dispositivos de almacenamiento USB, conexión USB de teléfono y dongles celulares compatibles.
Pantalla táctil de 2,8"	Para verificaciones de estado en tiempo real y control funcional extenso.
Puertos de antena externa (TS-9)	Para conectar antenas externas con la interfaz TS-9.

1.1.3 Pantalla táctil

Visualización de pantalla	Descripción
	Pantalla de activación Puedes ajustar el estilo de visualización de la hora y la fecha en la pantalla de activación y personaliza la imagen de fondo según sea necesario.
	Ingrese contraseña Se requiere un código de acceso de 4 dígitos para desbloquear la pantalla. Puedes personalizar el tiempo de bloqueo automático de la pantalla para reducir la frecuencia con la que necesitas ingresar código de acceso.
	Página de inicio La página de inicio muestra el estado de SIM, Wi-Fi, Clientes, Repetidor, y VPN, y proporciona acceso rápido a funciones de uso común.



Más configuraciones

Toque Más en la página de inicio para acceder a más configuraciones.

1.2 Especificaciones

Interfaz	1 puerto Ethernet WAN/LAN de 2,5G 1 pantalla táctil LCD en color de 2,8” 2 x ranuras para tarjetas Nano SIM 1 chipset eSIM integrado 1 x USB Type-C (solo alimentación; entrada y salida de alimentación) 1 x USB Type-C (10 Gbps; entrada y salida de alimentación, USB OTG) 2 puertos TS-9 1 x botón de encendido 1 x botón de reinicio
Plataforma 5G	Qualcomm Dragonwing MBB Gen 3 (X72)
CPU	Qualcomm, cuatro núcleos a 2,2 GHz
Memoria/Almacenamiento	LPDDR4X 2GB / 8GB eMMC
Velocidad de Wi-Fi	688Mbps (2,4 GHz), 2882 Mbps (5 GHz), 5764 Mbps (6 GHz)
Antenas	8 x antenas internas (6 x antenas celulares, 2 x 2,4 GHz y antenas Wi-Fi de 5 GHz y 6 GHz)
Velocidad de Ethernet	100/1000/2500Mbps
eSIM	1 x eSIM integrada
Batería incorporada	3.85V/5380mAh/20.72Wh
Entrada de energía	USB PD/PPS 5-12 V, 30 W máx.
Consumo de energía	<30W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Dimensión/Peso	157 x 75 x 22,8 mm/300 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

*Las velocidades inalámbricas se basan en los estándares IEEE 802.11 (por ejemplo, 802.11be para Wi-Fi 7). El rendimiento y el alcance reales pueden ser inferiores debido a

obstáculos ambientales (paredes, metal), congestión de la red o capacidades del dispositivo cliente.

*El uso de Wi-Fi 7 (802.11be) y sus características (OFDMA, MU-MIMO, 4096-QAM, MLO) requiere que los dispositivos cliente admitan las tecnologías correspondientes.

1.3 Bandas de frecuencia

	GL-E5800NA	**GL-E5800EU**
5G NR Conectividad	Operación 3GPP Rel-17 NSA/SA, Sub-6GHz	
5G NR NSA	n2 / n5 / n7 / n12 / n14 / n25 / n26 / n30 / n38 / n41 / n48 / n66 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
SA 5G NR	n2 / n5 / n7 / n12 / n13 / n14 / n25 / n26 / n29 / n30 / n38 / n41 / n48 / n66 / n70 / n71 / n77 / n78	n1 / n3 / n5 / n7 / n8 / n20 / n26 / n28 / n38 / n40 / n41 / n75 / n77 / n78
Categoría LTE	Cat 20 (DL) / Cat 18 (UL)	
LTE-FDD	B2 / B4 / B5 / B7 / B12 / B13 / B14 / B17 / B25 / B26 / B29 / B30 / B66 / B71	B1 / B3 / B5 / B7 / B8 / B20 / B28 / B32
LTE-TDD	B38 / B41 / B42 / B43 / B48	B38 / B40 / B41 / B42 / B43
WCDMA		B1 / B5 / B8

1.4 Contenido del paquete

El paquete incluye:

- 1 x Mudi 7 (GL-E5800)
- 1 x Guía de inicio rápido
- 1 paquete de baterías
- 1 cable USB-C de 10 Gbps
- 1 x bolsa de viaje



Capítulo 2

Inicialización del enrutador

Este capítulo describe cómo finalizar la inicialización del enrutador y conectar su dispositivos.

Siga los pasos a continuación para completar la inicialización del enrutador y conectar sus dispositivos.

1. **Encienda**

   Mantenga presionado el botón de encendido durante **3 segundos** o conecte un adaptador de corriente. 7 se iniciará automáticamente.

2. **Inicialización del sistema**

   Siga las instrucciones en pantalla para configurar los ajustes básicos, incluido el código de acceso de pantalla, la contraseña de administrador, el nombre de Wi-Fi, la contraseña de Wi-Fi y las bandas de frecuencia.

   Consejo: La contraseña de administrador predeterminada son los últimos 9 caracteres. del S/N del dispositivo, seguido de un carácter #. Puede usar la contraseña predeterminada o establecer una personalizada.

3. **Conecte un dispositivo al enrutador**

   Conecte un dispositivo (por ejemplo, una computadora portátil o un teléfono inteligente) al enrutador mediante Wi-Fi, un cable Ethernet o un cable USB.

   - **Wi-Fi**: En su dispositivo, vaya a Configuración -> WLAN, ubique el nombre de la red Wi-Fi del Mudi 7’en la lista de redes disponibles e ingrese la contraseña. Puede encontrar el nombre de red predeterminado y la contraseña impresos en la pantalla de Mudi 7. Alternativamente, escanee el código QR en la pantalla y luego haga clic en "Unirse" para conectarse.’pantalla. Alternativamente, escanee el código QR en la pantalla y luego haga clic en "Unirse" para conectarse.
   - **Ethernet**: Conecte su dispositivo al puerto Ethernet del Mudi 7’ (predeterminado en LAN) mediante un cable Ethernet.
   - **USB**: Conecte su dispositivo al puerto USB-C de Mudi 7 mediante un cable USB. El puerto USB-C está habilitado para OTG, lo que le permite acceder al Mudi 7 en el siguiente paso.

4. **Inicie sesión en el enrutador**

   Internet es undisponible 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 accedering a Internet.

Capítulo 3

Iniciar sesión en el enrutador

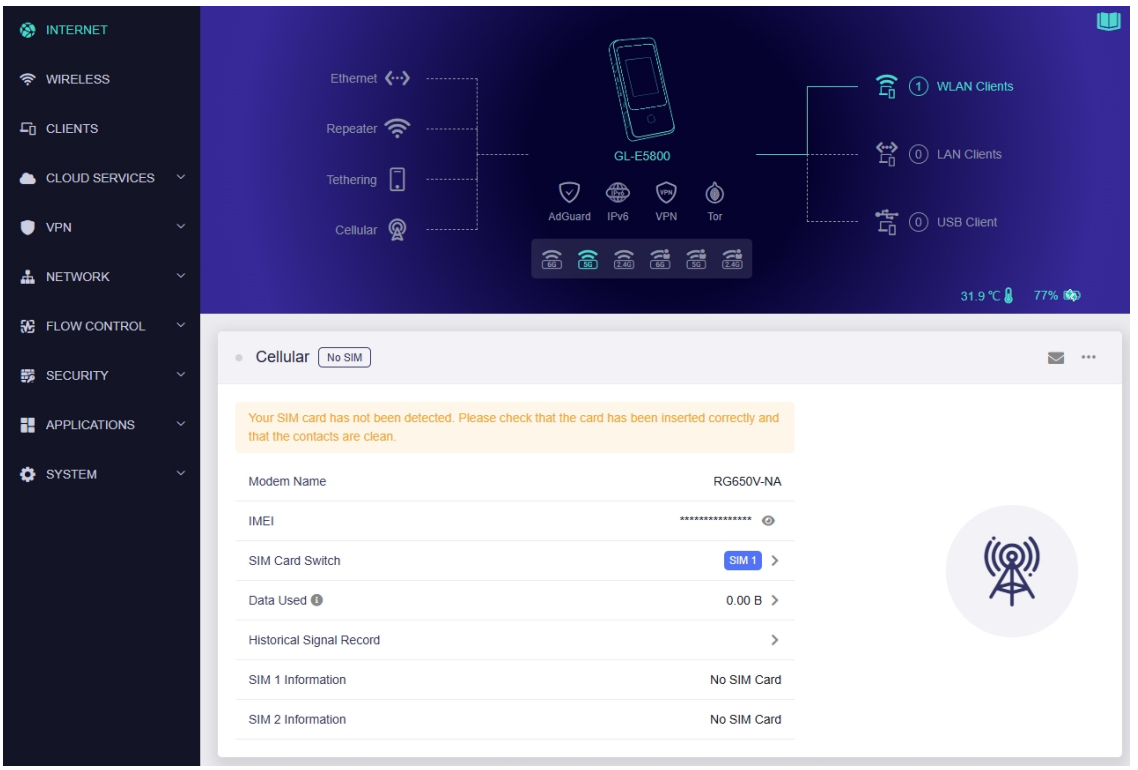
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web.

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

Nota: Si prefiere nosotrosing la aplicación GL.iNet en lugar de la web admin panel, 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. Abra un navegador web (se recomiendan Chrome y Edge) y visita http://192.168.8.1. You will be directed to the página de inicio de sesión de la web admin panel. Si no puede acceder a la web undmin panel, consulte aquí para solucionar problemas.
3. Sy su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar. Si ya ha establecido una contraseña de administrador, inicie sesión directamente.
4. Yusted luego ingresará el enrutador’s web admin panel.



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

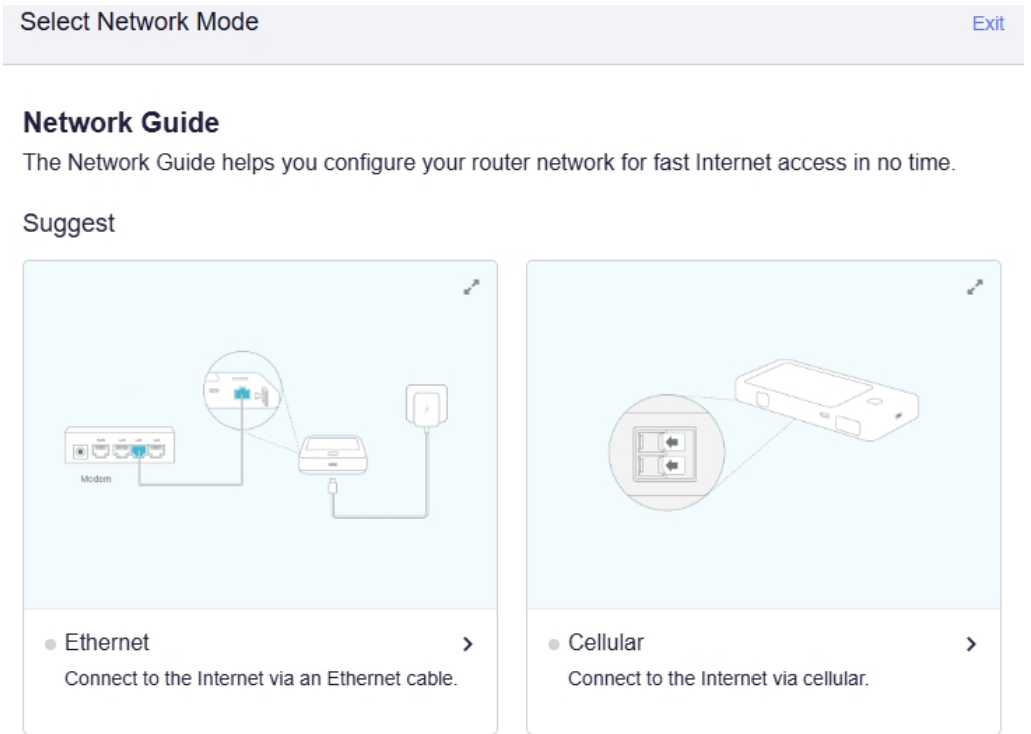
El asistente de configuración basado en web lo guiará a través de la configuración de red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

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



3. Fsiga el Asistente de configuración para configurar su enrutador y establecer una conexión a Internet.



Si utiliza el aplicación GL.iNet, siga las instrucciones en pantallas para configurar internet acceso.

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 avanzada de la red para requisitos específicos y verificar o modificar las conexiones existentes según sea necesario.

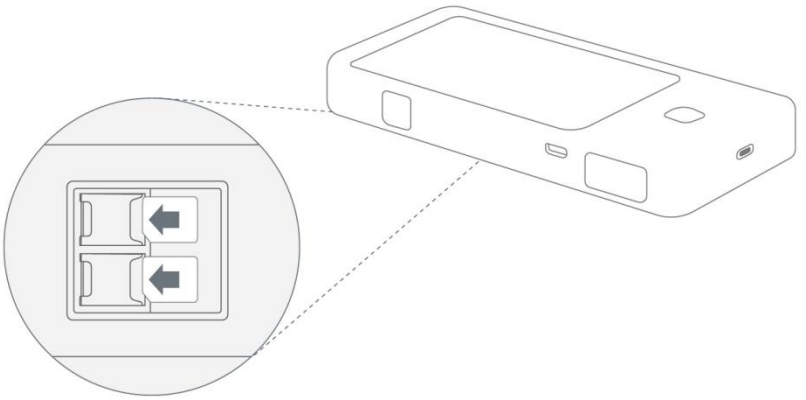
Mudi 7 admite hasta cinco métodos de conexión a Internet: Celular, Ethernet, Repetidor, Anclaje a red USB y USB Ethernet. Celija el método adecuado según sus necesidades de uso.

1. **Celular (Cellular)**: inserte una tarjeta SIM en el enrutador o habilite la eSIM integrada. Luego, el enrutador se conectará a Internet a través de una red celular 4G o 5G, según la red de su proveedor y las bandas de frecuencia admitidas. Este método ofrece una gran flexibilidad y es ideal para escenarios como el uso en vehículos o actividades al aire libre.
2. **Ethernet (RJ45)**: conecte el enrutador a una red de banda ancha usando an Cable Ethernet conectado al puerto WAN. El enrutador normalmente obtiene una dirección IP automáticamente a través de DHCP. Los usuarios pueden también manualmente configurar una IP estática o configuración PPPoE. 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.
   Además, Mudi 7 está equipado con un puerto USB-C habilitado para OTG, lo que le permite agregar un segundo puerto Ethernet para WAN Ethernet dual. Esto requiere un adaptador USB-C a Ethernet que se vende por separado.
3. **Repetidor (Repeater)**: este modo habilitas el enrutador a conéctese a una red Wi-Fi existente para ampliar la señal Wi-Fi y crear una red local separada y segura. Tenga en cuenta que las velocidades de transmisión pueden reducirse hasta cierto punto. Es ideal para zonas muertas de Wi-Fi que requieren extensión de señal o lugares públicos donde se necesita seguridad de red mejorada.
4. **Anclaje a red USB (USB Tethering)**: conecte un teléfono inteligente u otro dispositivo compatible al enrutador mediante un cable USB para compartir la conexión de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Esta es una solución conveniente para el acceso temporal a Internet, especialmente en exteriores o en áreas sin banda ancha fija.

5. **Ethernet por USB**: Mudi 7 está equipado con un puerto USB-C habilitado para OTG, lo que le permite agregar un segundo puerto Ethernet para WAN Dual-Ethernet. Se requiere un adaptador USB-C a Ethernet por separado.

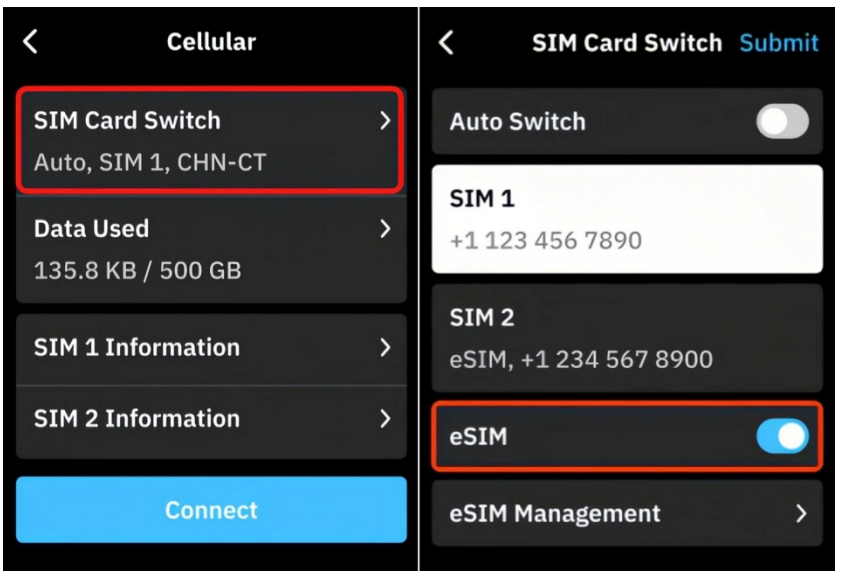
4.2.1 Conectarse a Internet mediante la red móvil

Mudi 7 viene con una eSIM integrada y dos ranuras Nano-SIM. Puede conectarse a Internet comprando un paquete eSIM (no se requiere una tarjeta SIM física) o insertando sus tarjetas Nano-SIM para acceder a la red móvil 5G.

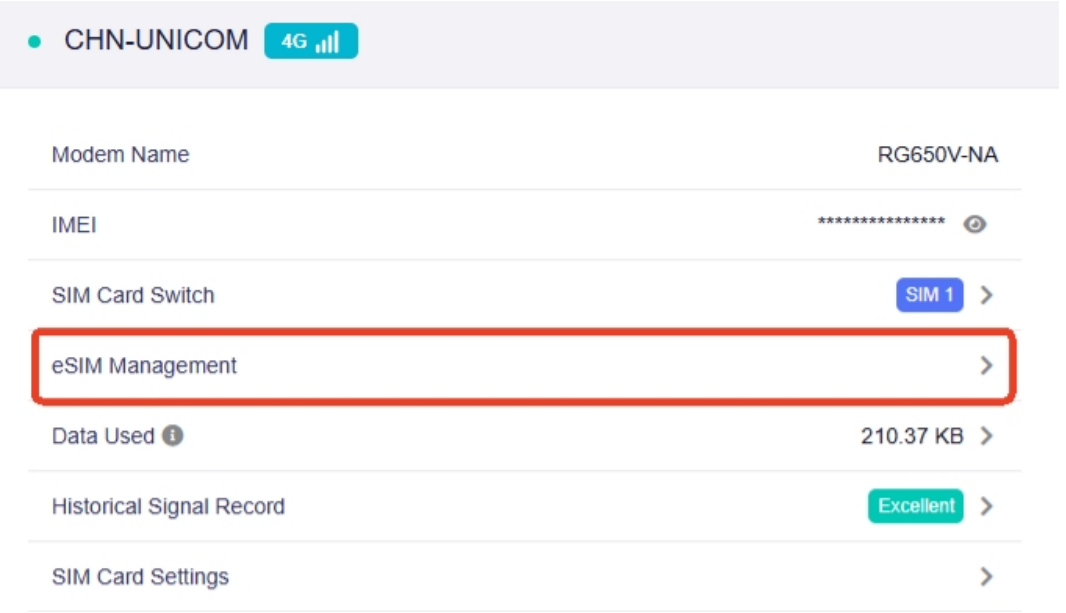


Configurar eSIM

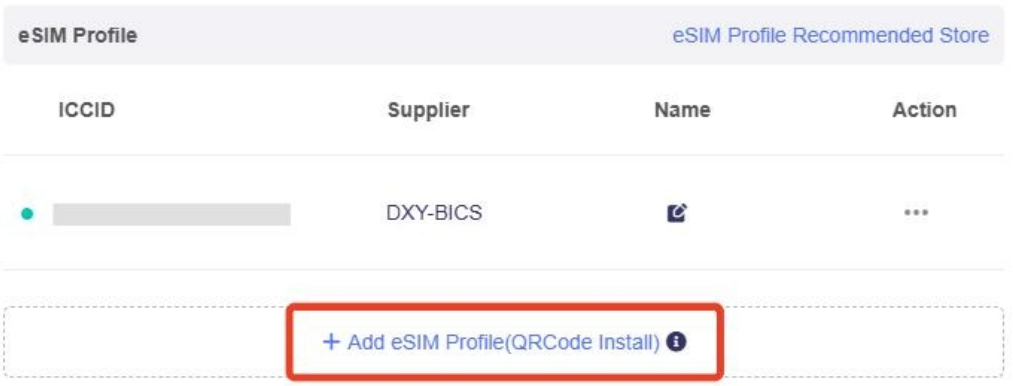
1. En la pantalla táctil, vaya a **Celular** > **Interruptor de tarjeta SIM**, active el interruptor para habilitar eSIM.



2. Inicie sesión en el enrutador’s web admin panel y ve a **INTERNET** > **Celular** > **Gestión de eSIM**.



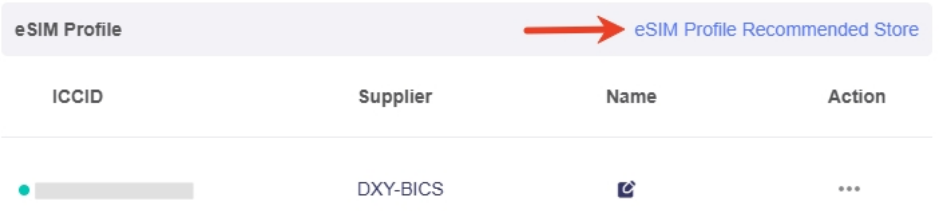
3. En la ventana emergente, haz clic en **Agregue perfil eSIM** en la parte inferior.



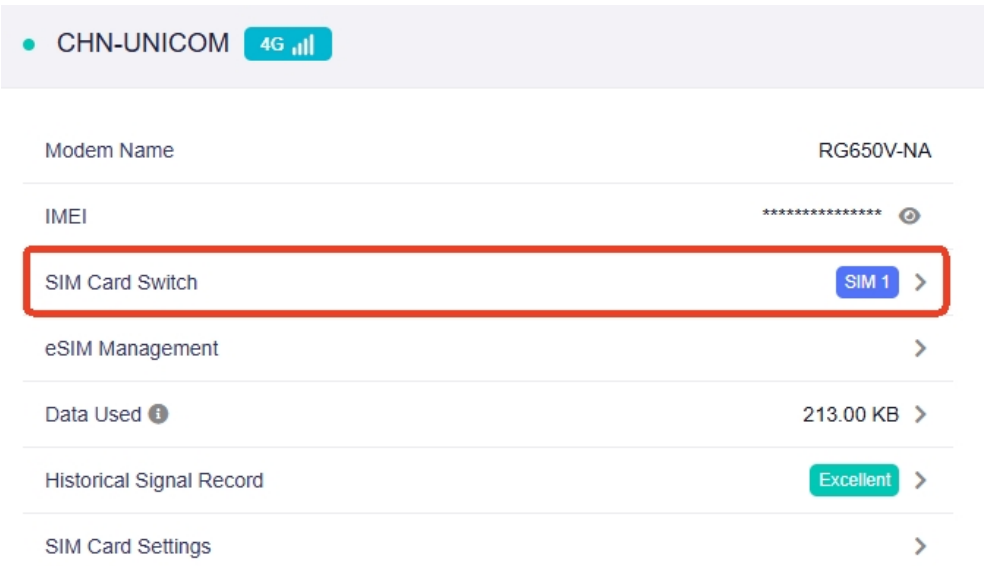
Antes de realizar la operación de carga, asegúrese de que su dispositivo esté conectado a Internet. Un error de red provocará que falle la carga del archivo de configuración de eSIM.

Cargue su perfil de eSIM mediante un código QR o un código de activación y haga clic en **Instalar**. Tenga en cuenta que la mayoría de los perfiles eSIM solo se pueden descargar y agregar una vez.

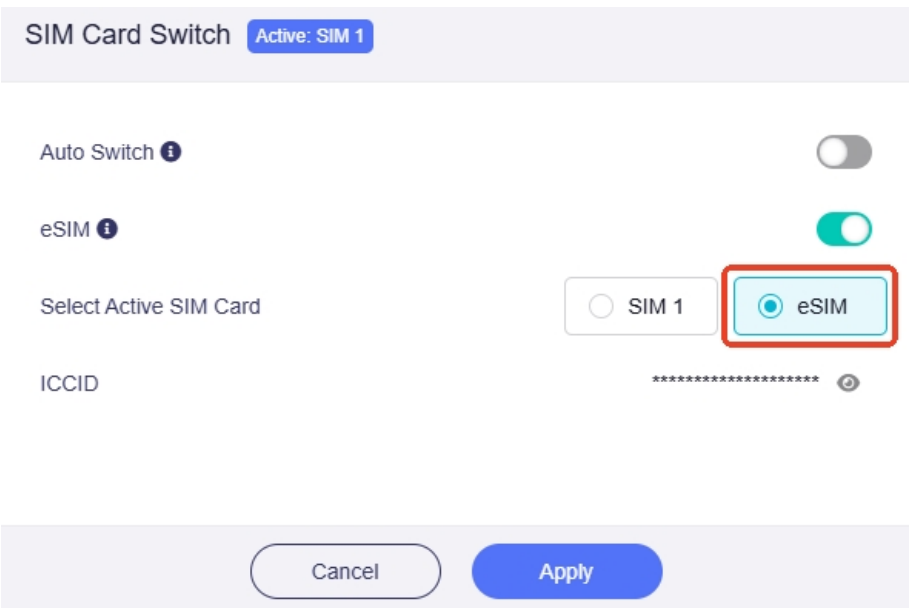
Consejo: si no has comprado ningún perfil eSIM, puedes comprar uno en la **Tienda recomendada de perfiles eSIM**.



4. Una vez cargado, ve a **Celular** y haz clic **Cambio de tarjeta SIM**.



En la ventana emergente, seleccione **eSIM** como tarjeta SIM activa y luego haga clic en **Aplicar**.



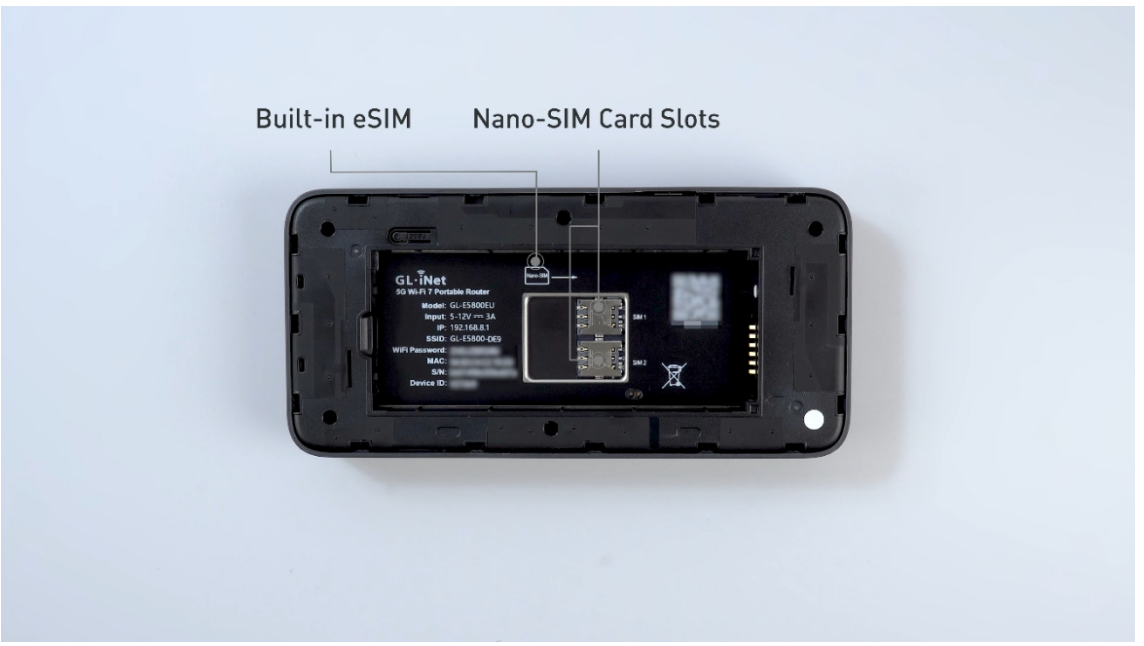
5. El enrutador comenzará a conectarse a través de este perfil eSIM. Espere y verifique si la conexión se realizó correctamente.

Configurar Nano-SIM

1. Utiliceuse la pequeña muesca en la esquina inferior derecha de la cubierta posterior del dispositivo como punto de apoyo. Haga palanca a lo largo de la costura para crear un espacio, luego abra la cubierta trasera y retire la batería del Mudi 7.
   Advertencia: Si la batería está hinchada, tiene fugas, está inusualmente caliente, está dañada o es difícil de quitar, deje de usar el dispositivo y no intente quitarla. Consulta Seguridad de la batería.



2. Iinserto las tarjetas Nano-SIM. Si usa solo una tarjeta, priorice la SIM 1. Luego vuelva a colocar la batería y la tapa.



3. El enrutador comenzará a conectarse automáticamente la Nano-tarjeta SIM. Espere y verifique si la conexión se realizó correctamente. Una vez conectado correctamente, las barras de señal y el estado del celular aparecerán en la esquina superior derecha de la pantalla táctil. También puedes consultar los detalles de la conexión en el panel de administración web.

Nota:

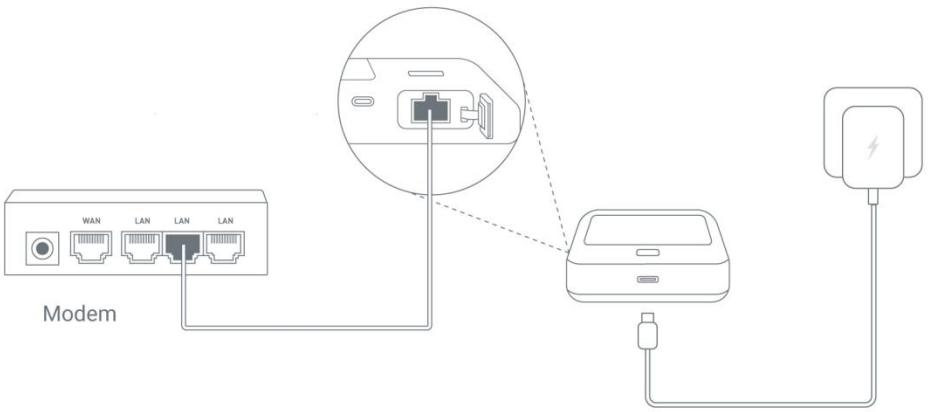
1. La eSIM y la SIM 2 integradas se excluyen mutuamente y no se pueden activar al mismo tiempo. La eSIM está desactivada por defecto. Si habilita la eSIM, la SIM 2 no funcionará incluso si se inserta una tarjeta SIM.
2. Dado que Mudi 7 viene con una eSIM incorporada, una tarjeta física SIMPoYo eSIM será reconocida como una tarjeta SIM normal sin funcionalidad eSIM en Mudi 7.

4.2.2 Conectarse a Internet mediante un cable Ethernet

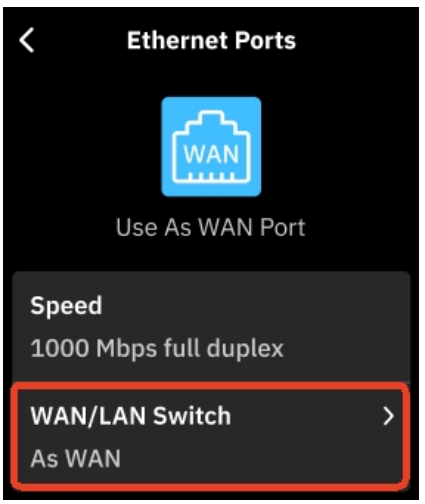
Conecte el enrutador a una red de banda ancha usando un cablen Ethernet. Este método ofrece alta estabilidad y alta velocidad, lo que lo hace ideal para entornos domésticos y de oficina con acceso de banda ancha fija.

Configuración básica

1. Conecte el puerto Ethernet de Mudi 7 a el dispositivo ascendente (por ejemplo, un módem ISP, enrutador principal, conmutador de red o un conector Ethernet) a través de un Ethernet cable.



2. En la pantalla táctil o el panel de administración web, vaya a **Red** > **Puertos Ethernet**, establezca la función del puerto en **WAN** y haga clic en **Aplicar**.

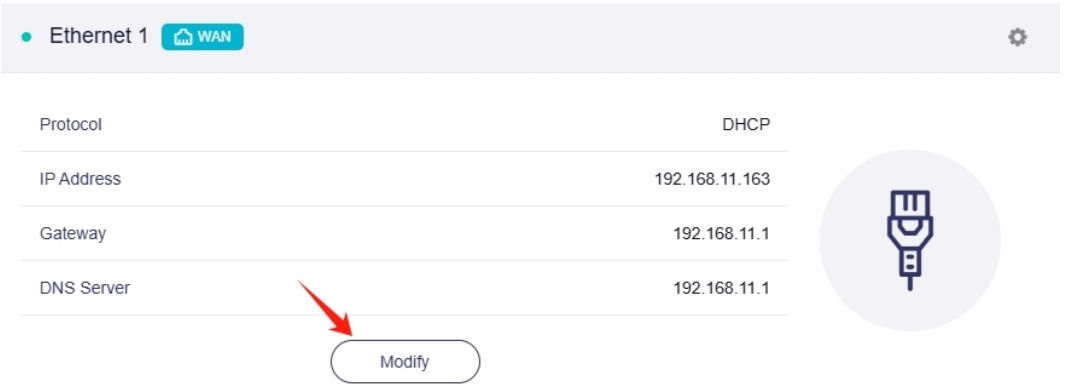


3. El enrutador comenzará a conectarse automáticamente. Una vez conectado correctamente, aparecerá un icono de puerto Ethernet en la esquina superior derecha de

la pantalla táctil. También puede consultar los detalles de la conexión y configurar ajustes avanzados en el panel de administración web.

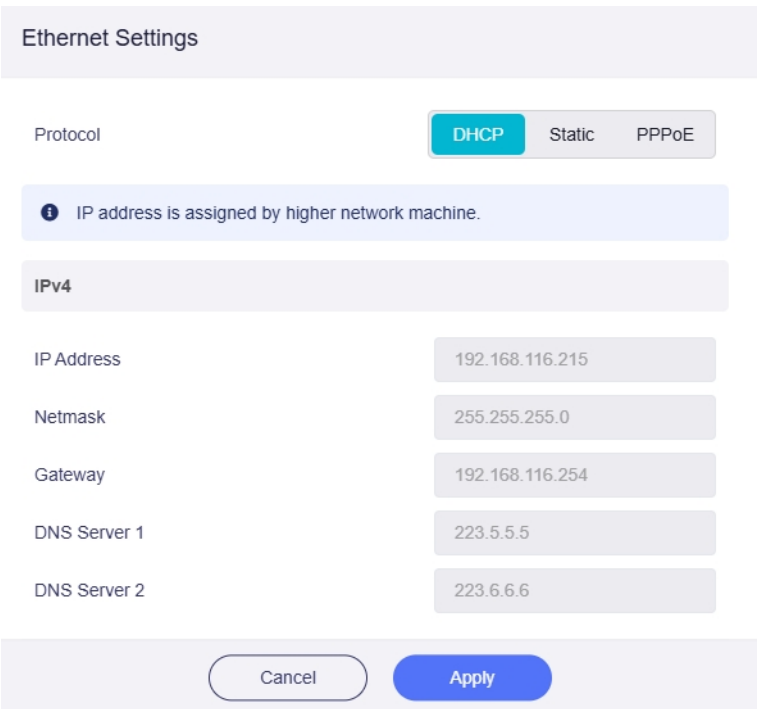
Protocolo

Hay tres tipos de protocolos para conexión Ethernet: DHCP, estático y PPPoE. Haga clic en **Modificar** para cambiar si es necesario.



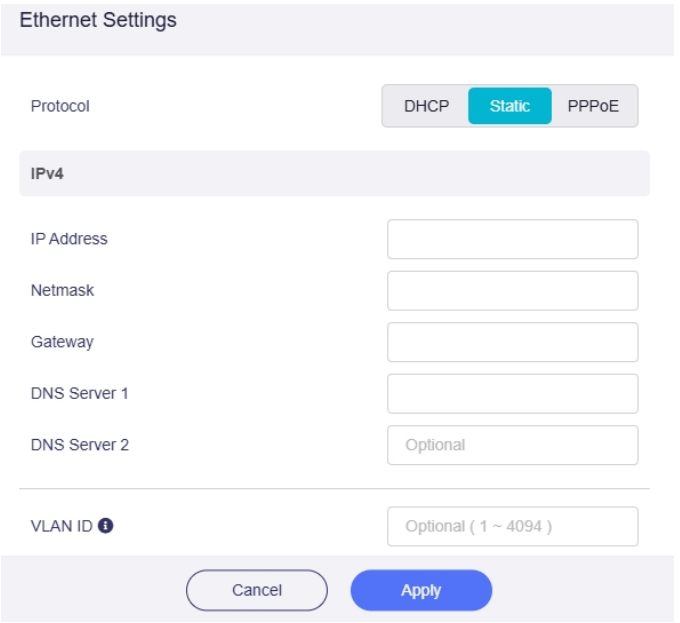
- **DHCP**

  DHCP es el protocolo de red predeterminado y más común, que asigna automáticamente direcciones IP y otros parámetros de configuración de red a dispositivos en una red IP a través de un modelo cliente-servidor.



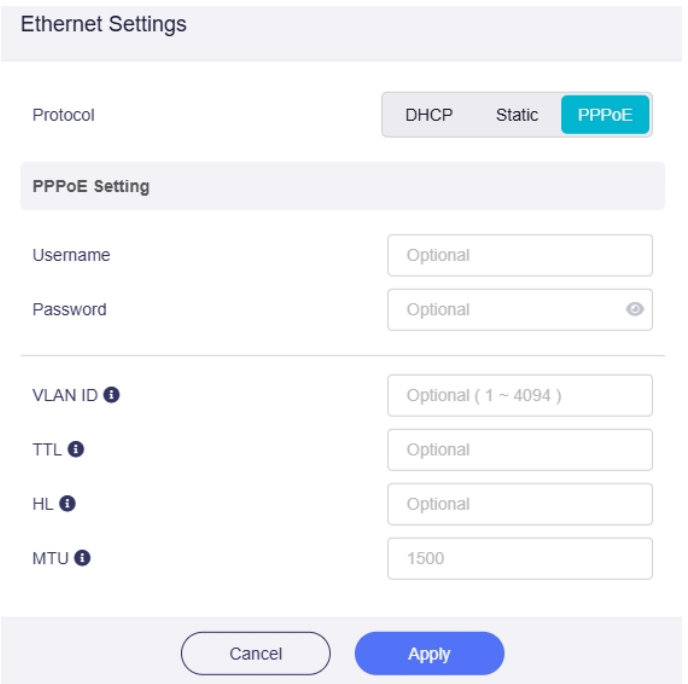
- **Estática**

Se requiere una dirección IP estática si su ISP (proveedor de servicios de Internet) asigna una dirección IP pública fija o si necesita configurar manualmente los parámetros de red. (por ejemplo, dirección IP, puerta de enlace, máscara de subred).



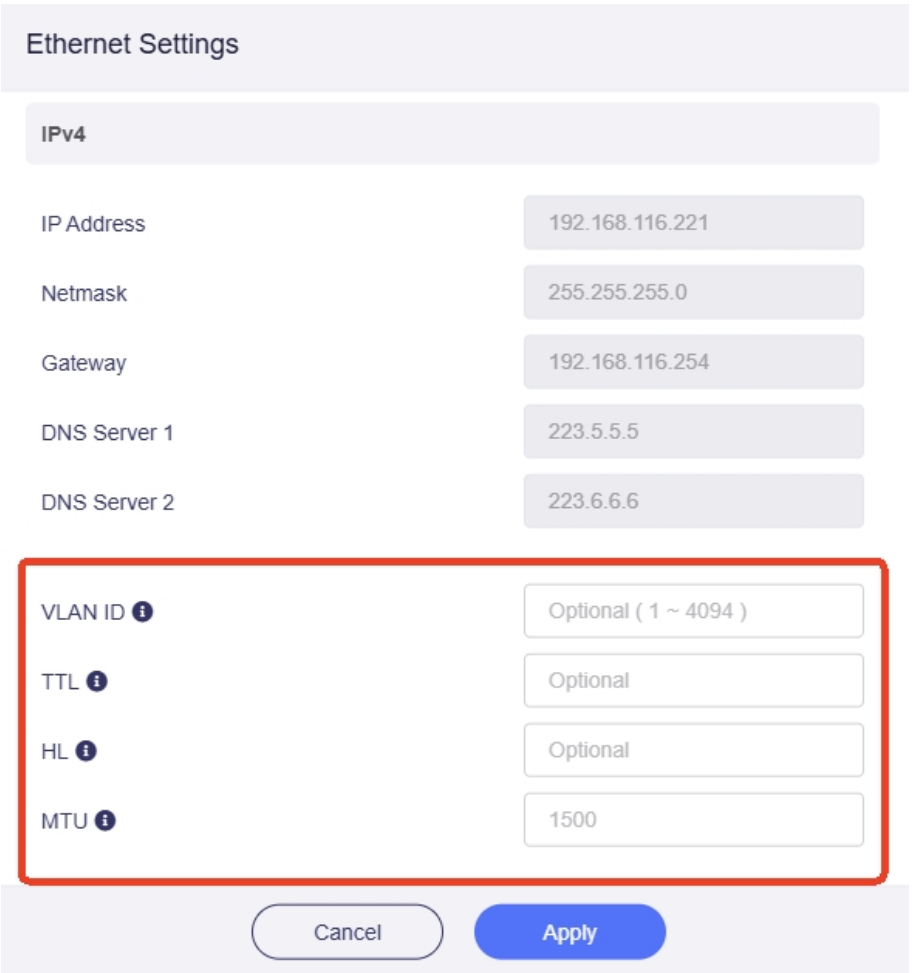
- **PPPoE**

  PPPoE (Protocolo punto a punto sobre Ethernet) es un protocolo de red ampliamente utilizado por los ISP. Por lo general, proporcionarán un módem junto con un nombre de usuario y una contraseña únicos, que son necesarios para configurar una conexión a Internet.



Configuración avanzada

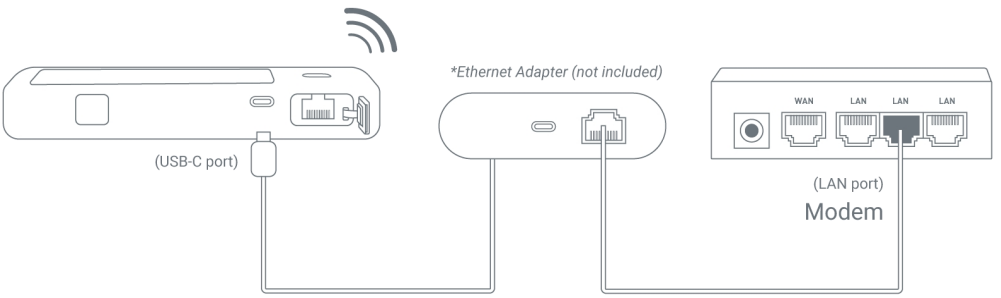
Además de las configuraciones esenciales, también hay algunas configuraciones avanzadas opcionales para arriba tres protocolos.



- **ID de VLAN**: Esta configuración solo es necesaria si el servidor del proveedor requiere que la interfaz utilice un ID de VLAN etiquetado específico.
- **TTL**: TTL (Tiempo de vida) establece el tiempo máximo para que los paquetes sobrevivan la red, y se completa según los requisitos del operadoror. Si necesita anular/falsificar el TTL, establezca un valor fijo aquí. El Mudi7 aplica el valor ingresado sin cambios. La configuración TTL es válida solo para IPv4.
- **HL**: En IPv6, el campo HL (Límite de saltos) limita el número de saltos de transmisión para paquetes de datos en la red, sirviendo como el equivalente de TTL en IPv4.
- **MTU**: La El valor MTU predeterminado es 1500 bytes.

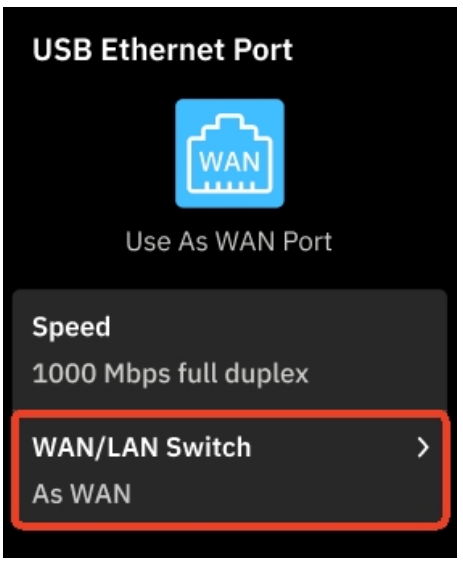
Ethernet por USB

Mudi 7 está equipado con un **compatible con OTG** puerto USB-C, lo que le permite agregar un segundo puerto Ethernet para WAN Dual-Ethernet. **Esto requiere un adaptador USB-C a Ethernet**.



Siga los pasos a continuación para conectar su enrutador a Internet a través de USB Ethernet.

1. Conecte una fuente de red ascendente (por ejemplo, módem ISP, conmutador de red o conector Ethernet en la pared) al puerto USB-C de Mudi 7 a través de un adaptador USB-C a Ethernet.
2. En la pantalla táctil o el panel de administración web, vaya a **Red** > **Puertos Ethernet** > **Puerto Ethernet USB**, establezca la función del puerto en **WAN** y haga clic en **Aplicar**.



3. Mudi 7 se conectará automáticamente a su dispositivo. Si no se conecta, repita los pasos anteriores o inicie sesión en el panel de administración web para verificar la conexión Ethernet USB.
4. Una vez conectado exitosamente a Internet, aparecerá un ícono de USB y un ícono de puerto Ethernet en la esquina superior derecha de la pantalla táctil. También puede consultar los detalles de la conexión en el panel de administración web.

4.2.3 Conectarse a Internet mediante una red Wi-Fi existente

Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales Wi-Fi-Fi y crear una red local aislada de la red primaria. Cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, el uso de un repetidor no solo fortaleces Wi-Fi, sino que también proporcionas acceso por cable e inalámbrico para múltiples dispositivos y salvaguardas tu red seguridad.



Función de repetidor GL.iNet 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.

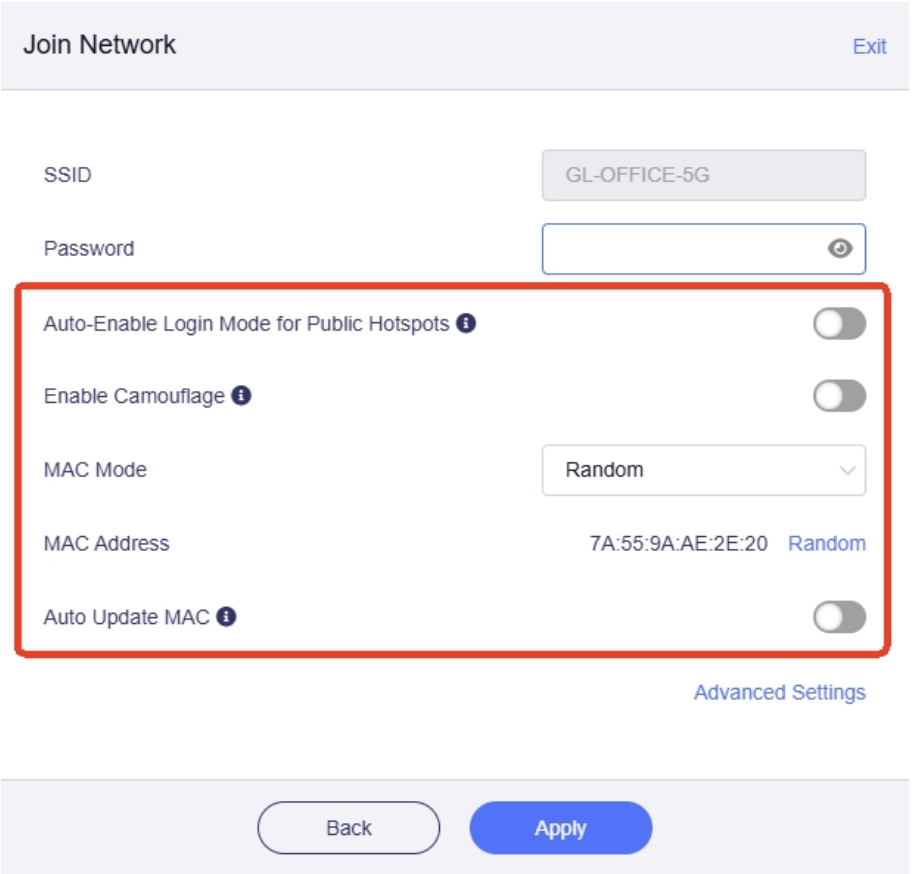
Configuración básica

Siga los pasos a continuación para conectar su enrutador a una red Wi-Fi existente como repetidor.

1. En la pantalla táctil o el panel de administración web, vaya a **Internet** > **Repetidor** y haga clic en **Conectar**. Mudi 7 comenzará a buscar redes Wi-Fi disponibles.
2. Seleccione la red Wi-Fi que desea que Mudi 7 extienda.
3. Ingrese la contraseña y haga clic en **Aplicar**.
4. Una vez conectado correctamente, aparecerá un icono de Wi-Fi en la esquina superior derecha de la pantalla táctil. También puede consultar los detalles de la conexión y configurar ajustes avanzados en el panel de administración web.

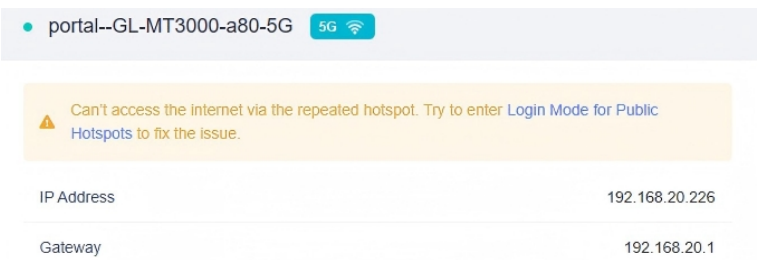
Configuración del punto de acceso público

Al conectar el enrutador a un punto de acceso público con un portal cautivo, Se recomienda habilitare las siguientes funciones para 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.

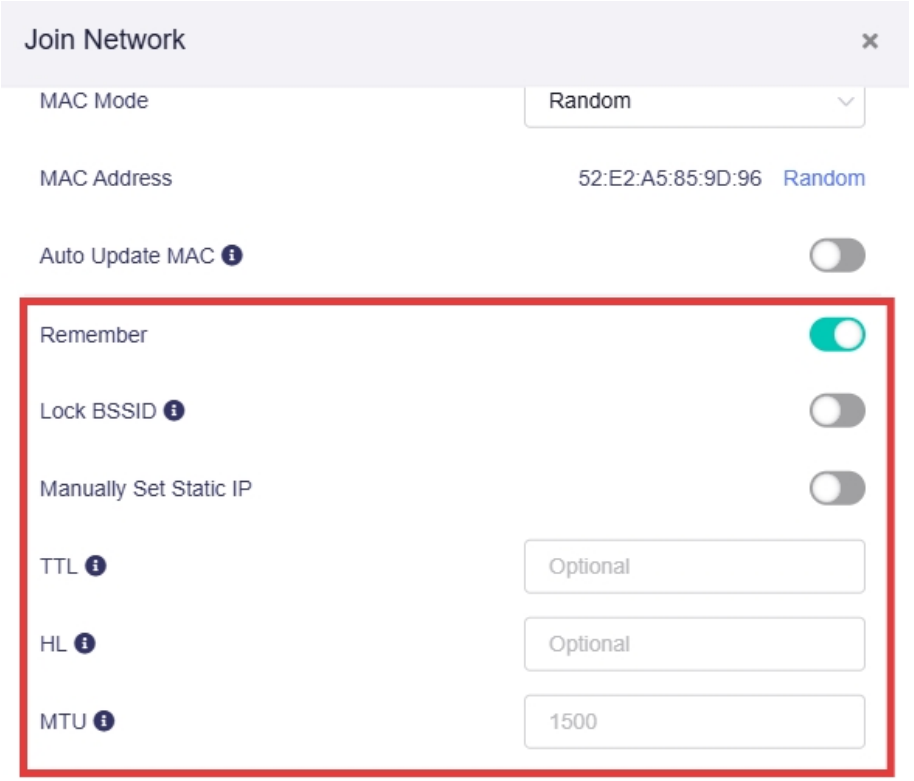


- **Habilitar camuflaje**
  Si está habilitado, el enrutador se hará pasar por el dispositivo cliente que utiliza para acceder al panel de administración emulando la dirección MAC de ese dispositivo's.
- **Modo MAC**
  Celija qué MAC dirección que utiliza el enrutador para conectarse al punto de acceso 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't aparece, ingrese manualmente la MAC dirección que desea clonar. Nota: Mcualquier dispositivo utiliza direcciones MAC aleatorias (a menudo denominadas dirección Wi-Fi privada o dirección de hardware aleatoria) al conectarse a redes Wi-Fi. Como resultado, la dirección MAC que se muestra aquí puede no coincidir con la MAC física real del dispositivo'.
  Aleatoria: 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 aleatoria MAC dirección, estará vinculada al SSID específico que guarde. Puede cambiar manualmente esta configuración para cada SSID en cualquier momento.

Configuración avanzada

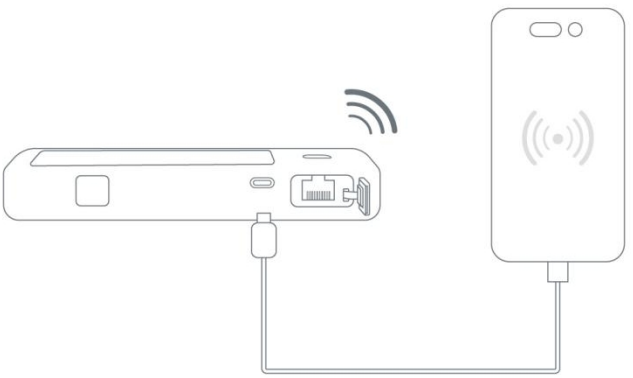
Al unirse a la red, hay algunas opcionales avanzadas configuración.



- **Recordar**: habilite esta opción para recordar la red Wi-Fi repetida actual.
- **Bloquear BSSID**: cuando esté habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al seleccionado BSSID, incluso cuando otros AP comparten 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 del repetidor del enrutador, en lugar de obtener estas configuraciones automáticamente.
- **TTL**: TTL (Time To Live) establece el tiempo máximo para que los paquetes sobrevivan en la red y se completa de acuerdo con los requisitos del operador. Si necesita anular/falsificar el TTL, establezca un valor fijo aquí. El Mudi7 aplica el valor ingresado sin cambios. La configuración TTL es válida solo para IPv4.
- **HL**: en IPv6, el campo HL (límite de saltos) se utiliza para limitar el número de saltos de transmisión de paquetes de datos en la red, que es equivalente al TTL en IPv4.
- **MTU**: el valor predeterminado es 1500.

4.2.4 Conectarse a Internet mediante conexión compartida por USB

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



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

Configuración básica

1. Conecte su dispositivo móvil (por ejemplo, teléfono inteligente o dispositivo USB) al puerto USB-C de Mudi 7 mediante un cable USB.
2. En su dispositivo móvil, vaya a Configuración y habilite **USB Anclaje**. Si usas iPhone, toca **Confiar en este dispositivo** si se te solicita.
3. Mudi 7 se conectará automáticamente a tu dispositivo. Si no se conecta, repita los pasos anteriores o inicie sesión en el panel de administración web para verificar la conexión Tethering.
4. Una vez conectado correctamente, aparecerá un icono de enlace de cadena en la esquina superior derecha de la pantalla táctil. También puede consultar los detalles de conexión ien el panel de administración web.

Solución de problemas

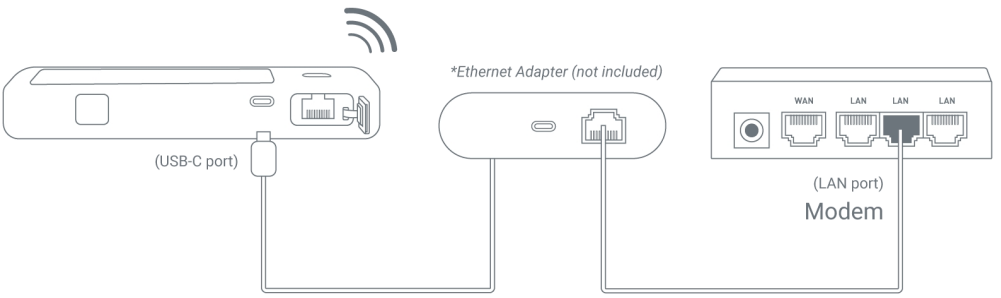
Si Anclaje a red la conexión falla, intente estos pasos para solucionar el problema:

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

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

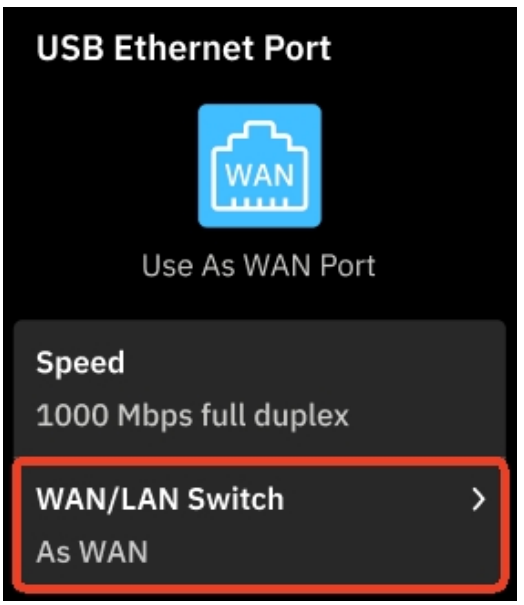
4.2.5 Conectarse a Internet mediante Ethernet por USB

USB OTG (On-The-Go) es un estándar USB que permite que dispositivos compatibles como enrutadores cambie entre funciones de host y periférico, lo que permite la transmisión directa de datos y la interacción de energía sin un dispositivo host separado. Mudi 7 está equipado con un **USB-C habilitado para OTG**, lo que le permite agregar un segundo puerto Ethernet para WAN Ethernet dual. Esto requiere un adaptador USB-C a Ethernet que se vende por separado.



Siga los pasos a continuación para configurar Mudi 7 a través de USB Ethernet.

1. Conecte una fuente de red ascendente (por ejemplo, módem ISP, conmutador de red o conector Ethernet en la pared) al puerto USB-C de Mudi 7'a través de un adaptador USB-C a Ethernet.
2. En la pantalla táctil o en el panel de administración web, vaya a **RED** -> **Puerto Ethernet** -> **Puerto Ethernet USB**, establezca la función del puerto en **WAN** y haga clic en **Aplicar**.



3. Mudi 7 se conectará automáticamente a su dispositivo. Si no se conecta, repita los pasos anteriores o inicie sesión en el panel de administración web y verifique la conexión **Ethernet por USB** en la página INTERNET.
4. Una vez conectado exitosamente a Internet, aparecerá un ícono de USB y un ícono de puerto Ethernet en la esquina superior derecha de la pantalla táctil. También puede consultar los detalles de la conexión en el panel de administración web.

Capítulo 5

Red inalámbrica

Este capítulo lo guía para verificar el estado de Wi-Fi y configurar los ajustes inalámbricos.

5.1 Visualización del estado de Wi-Fi

El enrutador’s Las redes Wi-Fi están habilitado de forma predeterminada, y el icono de Wi-Fi correspondiente se iluminará debajo de la imagen del modelo del dispositivo en INTERNET página.



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



Nota:

1. Debido a limitaciones de hardware, el Wi-Fi de 5 GHz y 6 GHz en Mudi 7 no se puede habilitar simultáneamente. La conexión Wi-Fi de 5 GHz está habilitada de forma predeterminada para una compatibilidad más amplia.
2. Cuando Mudi 7 se conecta a una red Wi-Fi ascendente como repetidor, la banda utilizada por el Wi-Fi ascendente se desactivará en Mudi 7.

3. Cuando Mudi 7 se conecta a una red Wi-Fi ascendente como repetidor, el Wi-Fi para invitados es no disponible.
4. Según lo exigen las regulaciones, Wi-Fi debe cambiar al modo “Exterior” cuando Mudi 7 se se utiliza en exteriores. Esto puede reducir el rango de cobertura.

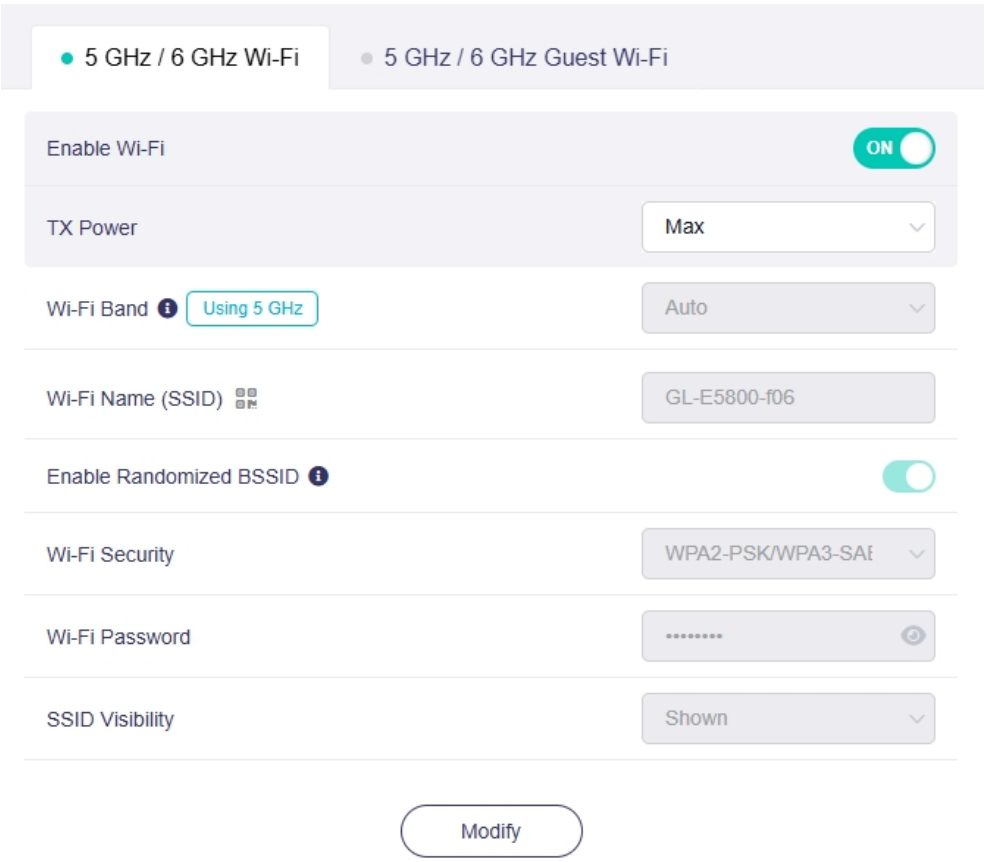
5.2 Configuración inalámbrica

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra el enrutador’s 2,4 GHz, 5 GHz y 6 GHz Configuración de Wi-Fi.

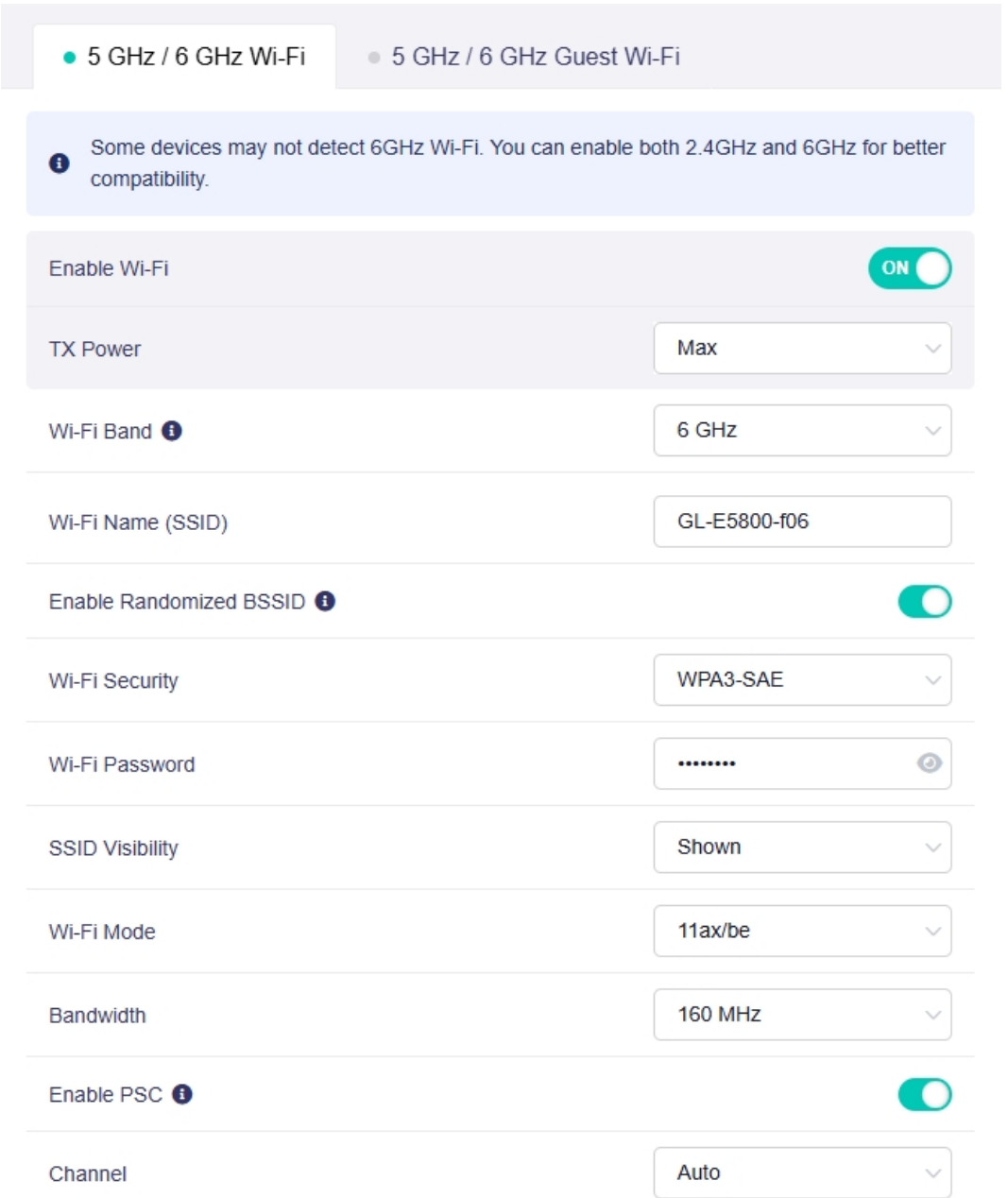
5.2.1 Wi-Fi de 5 GHz y 6 GHz

Debido a limitaciones de hardware, las bandas Wi-Fi de 5 GHz y 6 GHz en Mudi 7 no se pueden habilitar simultáneamente. Para una configuración simplificada, estas dos bandas se fusionan en una red Wi-Fi unificada en la página Inalámbrica: la banda Wi-Fi está configurada en **Auto** de forma predeterminada, que cambia dinámicamente entre 5 GHz y 6 GHz, con la banda de 5 GHz priorizada para una compatibilidad más amplia.

Esta página le permite usted habilitare o desactivarle Wi-Fi, ajustar Energía TX, habilitare o deshabilitare BSSID aleatorio, configurar nombre de Wi-Fi (SSID), seguridad, contraseña, y visibilidad de SSID. Tenga en cuenta que el canal y el ancho de banda no se pueden configurar manualmente cuando la banda Wi-Fi está configurada en Auto.



Haga clic en **Modificar** y cambie la banda Wi-Fi solo a 5 GHz o solo a 6 GHz si es necesario. Una vez fijada la banda, podrás personalizar el canal Wi-Fi, el ancho de banda y otros parámetros relacionados, además de la configuración básica..

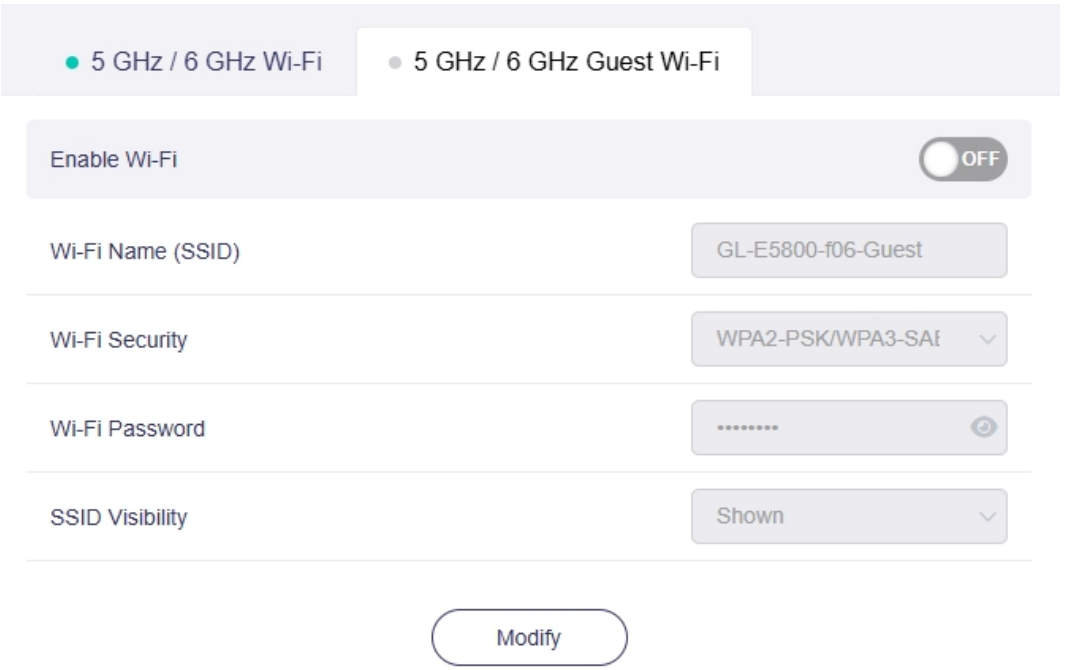


Nota:

1. Es posible que algunos dispositivos admitan Wi-Fi de 6 GHz. Puede habilitar las las bandas de 2,4 GHz y 6 GHz para compatibilidad más amplia.

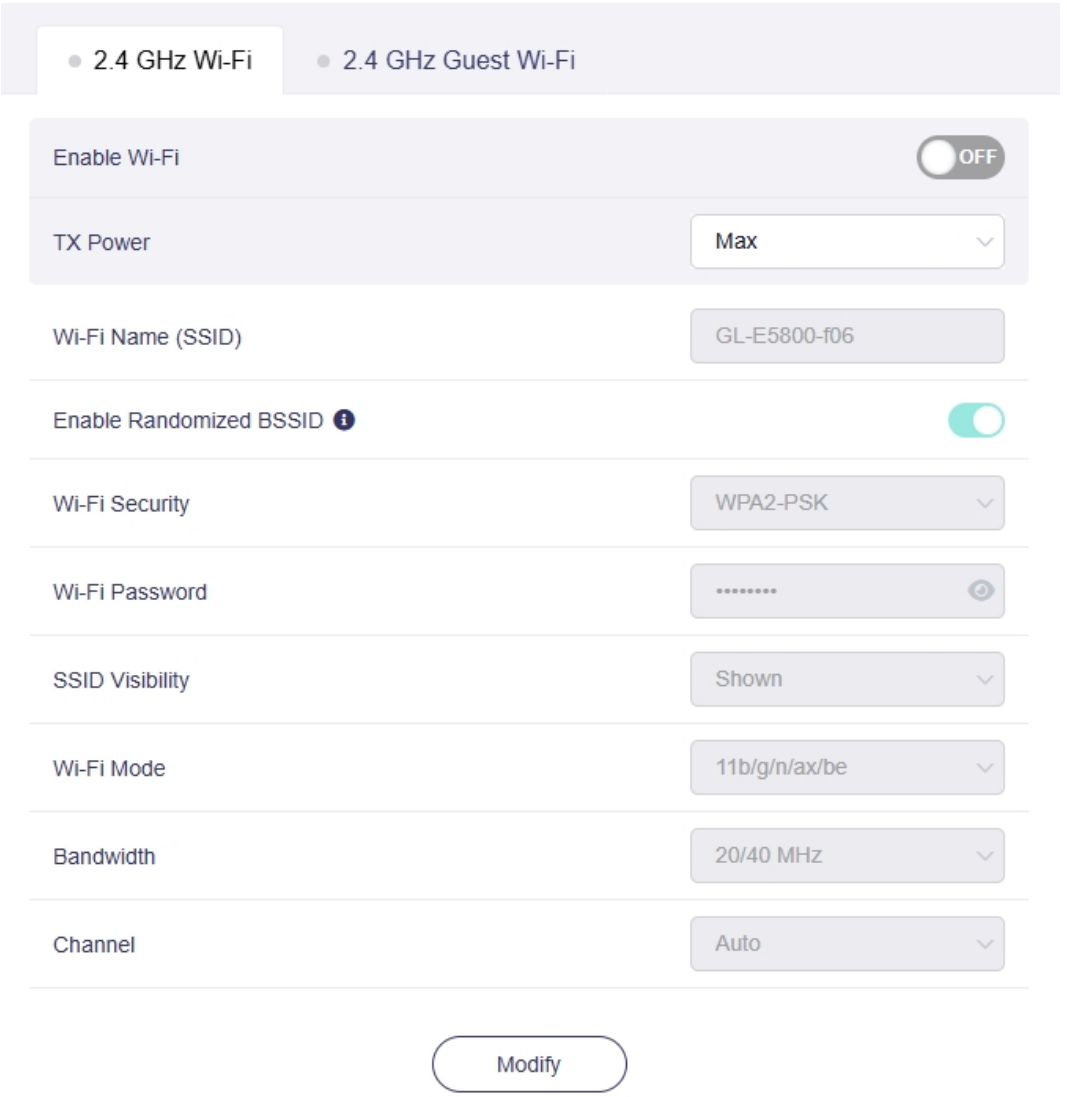
2. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan 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.
3. El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repetidor, ya que siguen la de la red repetida.
4. Cuando la banda Wi-Fi de 5 GHz está habilitada, si el **Ancho de banda** está configurado en **160 MHz**, el Wi-Fi funcionará en un canal DFS de forma predeterminada, incluso si seleccione manualmente un canal que no sea DFS o configure el canal en Auto.
5. Cuando el La banda Wi-Fi de 6 GHz está habilitada, **PSC** (Canal de escaneo preferido) está habilitado de forma predeterminada para reservar canales de alta calidad y garantizar conexiones estables para dispositivos de 6 GHz.

La 5GHz/6GHz Invitado Wi-Fi le permite configurar ajustes simplificados, incluida la activación o desactivación de Wi-Fi y la configuración del nombre de Wi-Fi (SSID), seguridad, contraseña y visibilidad de SSID.



5.2.2 Wi-Fi de 2,4 GHz

El Wi-Fi principal de 2,4 GHz le permite para activare o desactivare Wi-Fi, configure potencia de TX, habilitee o deshabilite BSSID aleatorio, configure nombre de Wi-Fi (SSID), seguridad, contraseña, visibilidad de SSID, Wi-Fi modo (estándar), ancho de banda y canal.



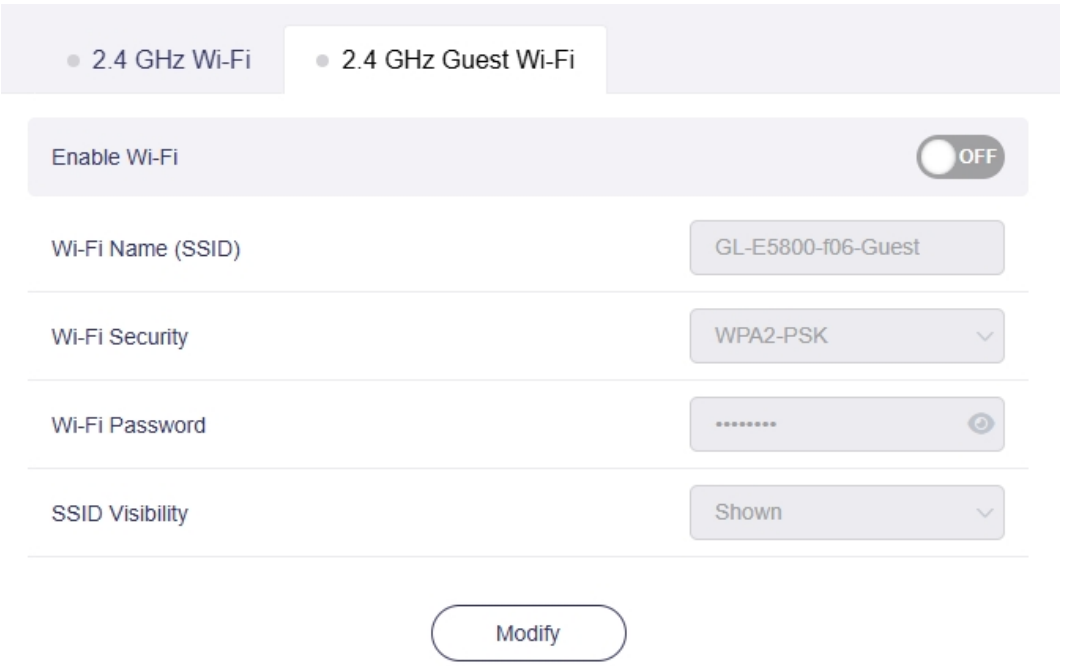
Nota:

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 2,4 GHz Invitado Wi-Fi le permite usted habilitararchivo o desactivare Wi-Fi, configurar nombre de Wi-Fi (SSID), seguridad, contraseña y SSID visibilidad.



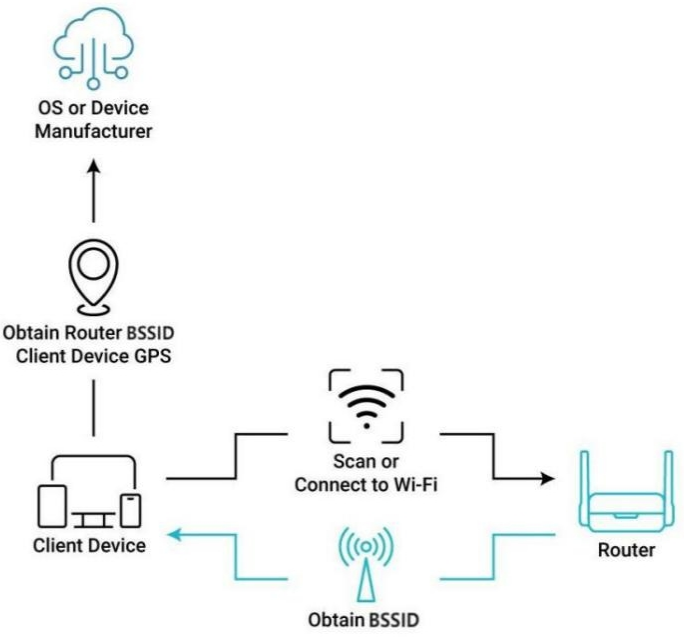
5.2.3 BSSID aleatorio

BSSID aleatorio es una función 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 brindar servicios de ubicación:

1. Los dispositivos del cliente (teléfonos, computadoras 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 una base de datos global de BSSID a ubicación.
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: se puede geolocalizar 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 función está habilitada, el enrutador genera un BSSID aleatorio y lo renueva en cada inicio. 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 BSSID-ubicación 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 sigue siendo 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 impide que los dispositivos cliente informen su propia ubicación y no es una solución de privacidad completa: características de SSID, canal y señal. todavía se puede observar.

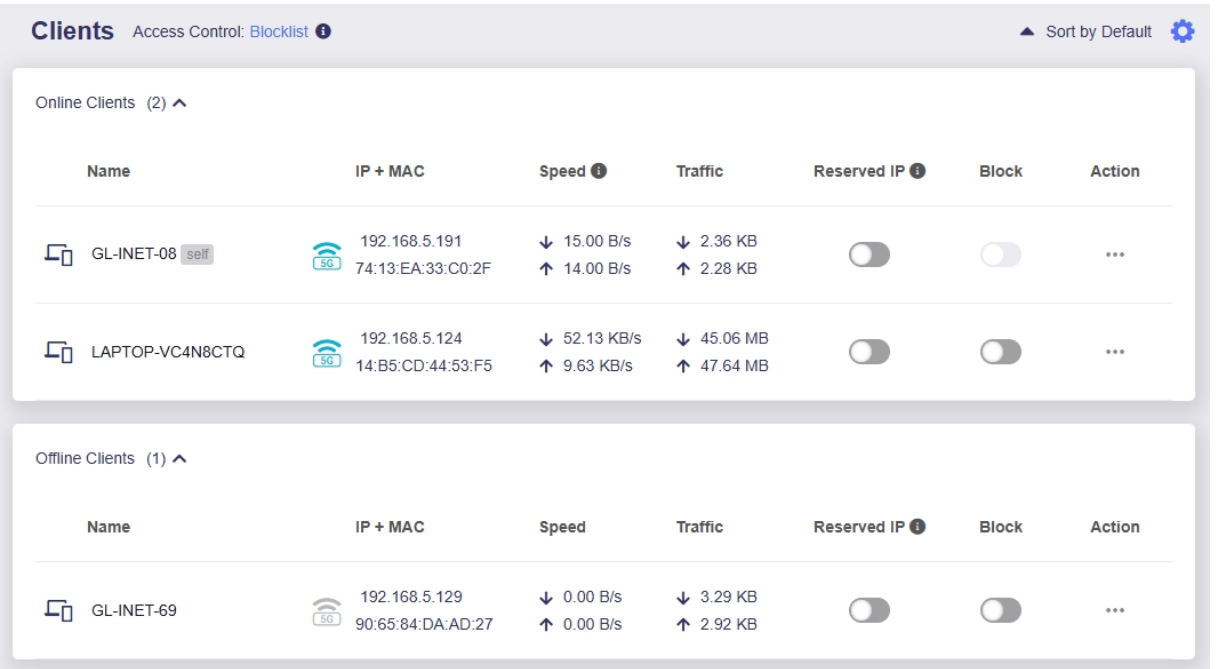
Capítulo 6

Clientes

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

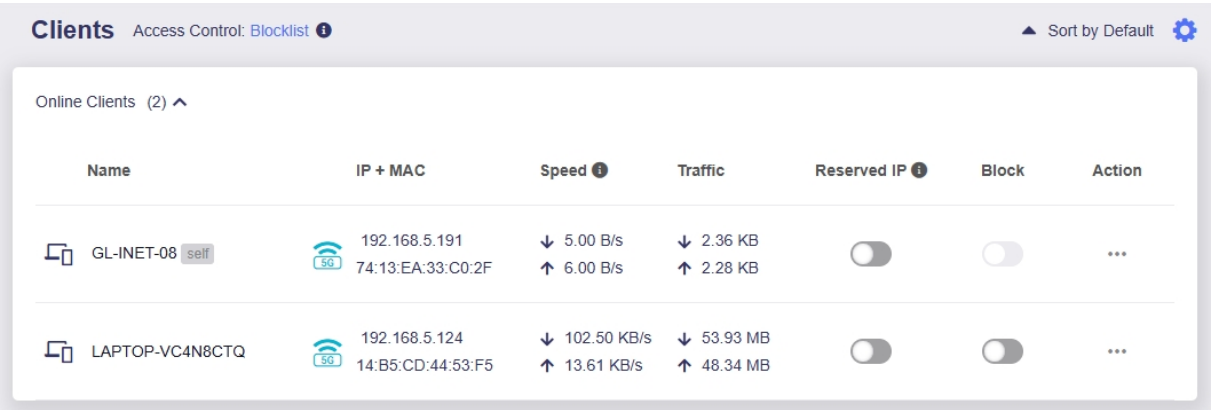
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

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



- **Clientes en línea**: Se refiere a los dispositivos actualmente conectados a la red del enrutador.
- **Clientes sin conexión**: Se refiere a dispositivos que se han conectado previamente al enrutador pero que ahora están desconectados de la red.

6.1 Detalles del dispositivo



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, indicandoindicando que el dispositivo está conectado al enrutador a través de un Ecable Ethernet.

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado. Si los dispositivos conectados utilizan direcciones MAC aleatorias , una 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. Estaes 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).

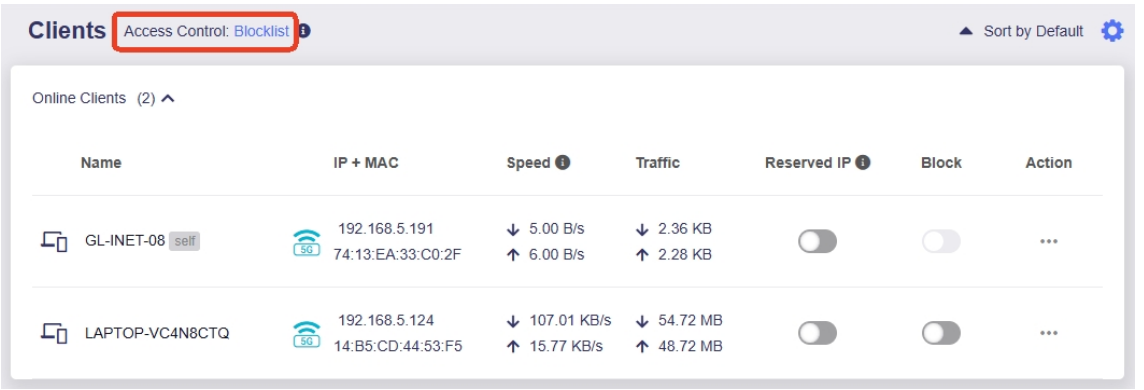
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet del dispositivo conectado.

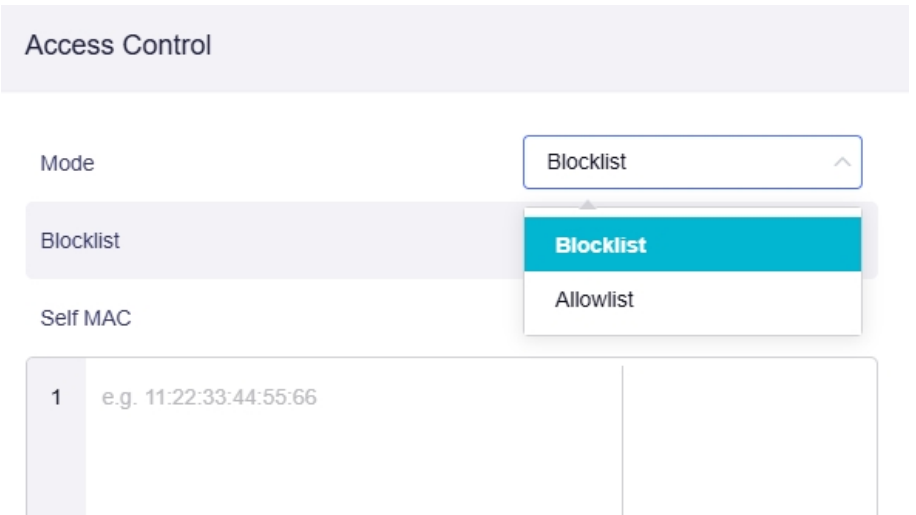
5. **Reservar IP**

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 del red de área local, siempre recibirá la misma dirección IP cada vez que se conecte a el enrutador.

6. **Lista de bloqueo**

   En la sexta columna, puede bloquear dispositivos conectados específicos con un clic. El Unala regla de control de acceso Ces Lista de bloqueo de forma predeterminada y puede cambiarla a Lista de permitidos desde el arriba según necesario.



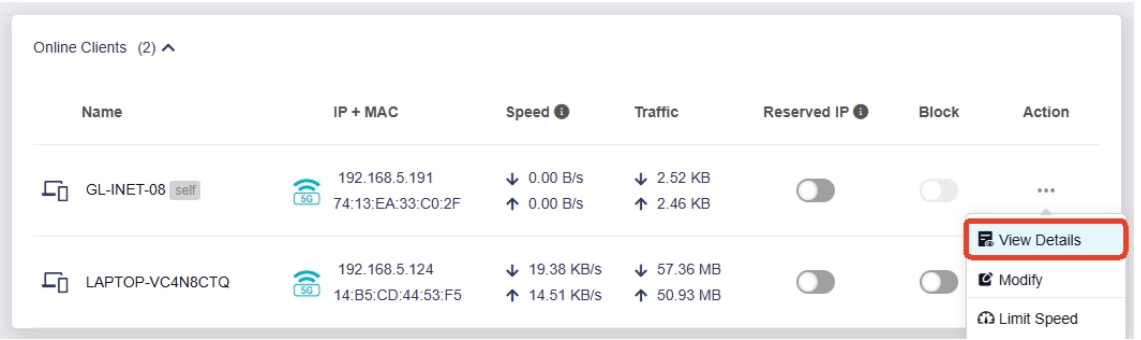


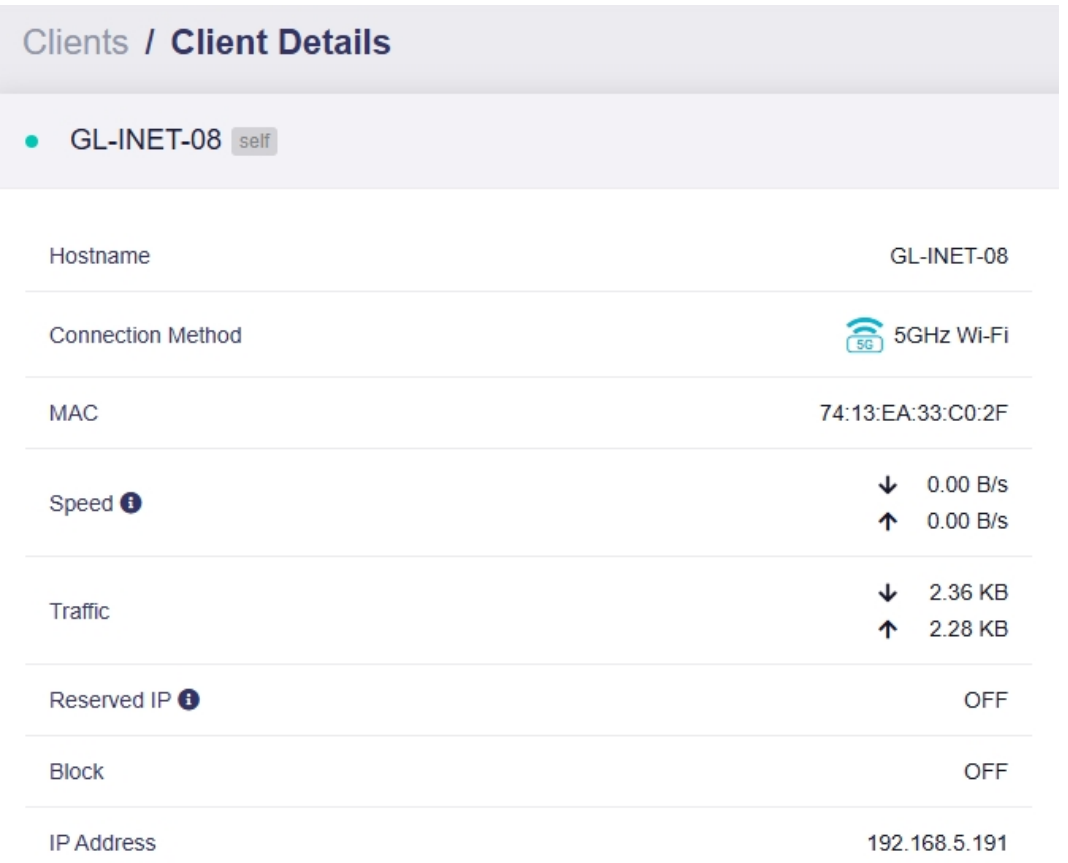
- **Lista negra**: Los dispositivos con direcciones MAC en la lista negrano pueden conectarse a este enrutador. Tenga en cuenta que El bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.
- **Lista de permitidos**: solo los dispositivos con direcciones MAC específicas pueden conectarse a este enrutador, adecuado para dispositivos IoT y redes empresariales gestión.

6.2 Acción

1. **Ver detalles**

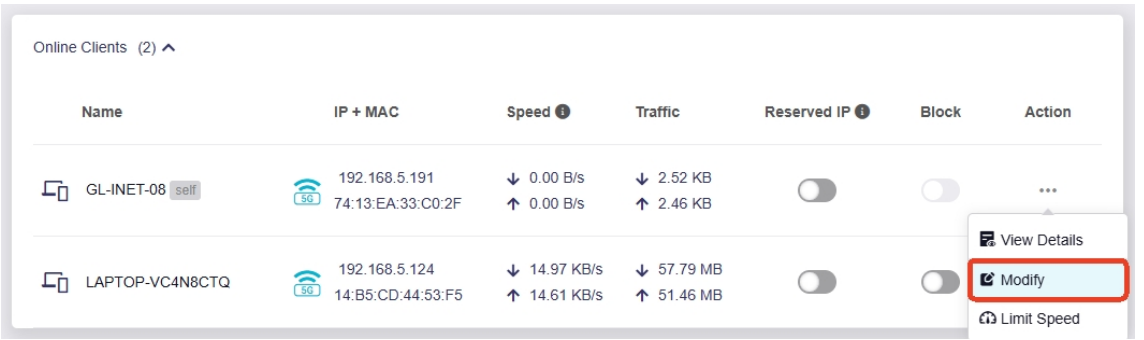
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

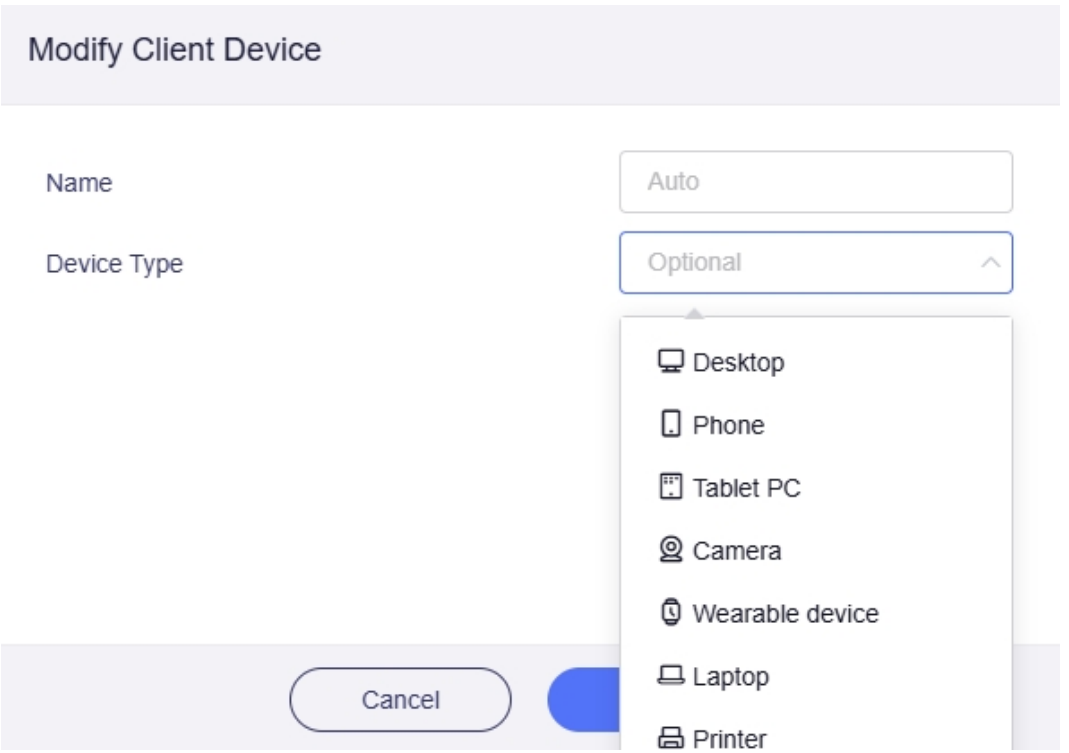




2. **Modificar**

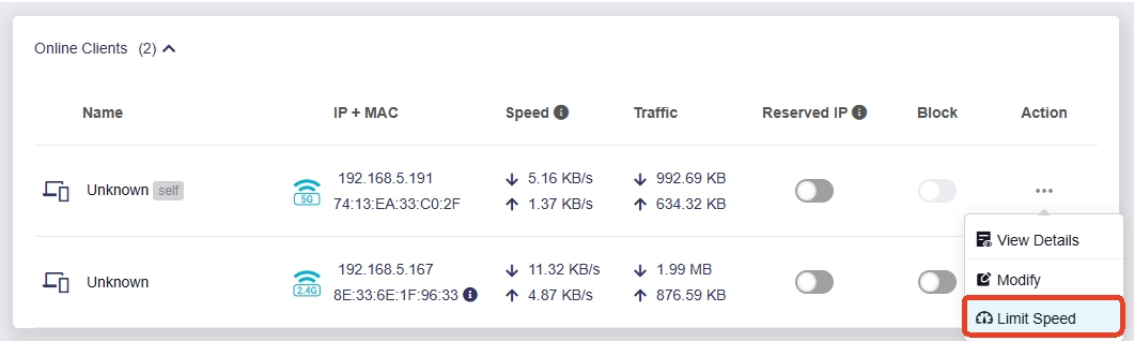
Haga clic en el ícono de tres puntos en **Acción** columna y haga clic en **Modificar** desde el menú desplegable para modificar el nombre y tipo del dispositivo.



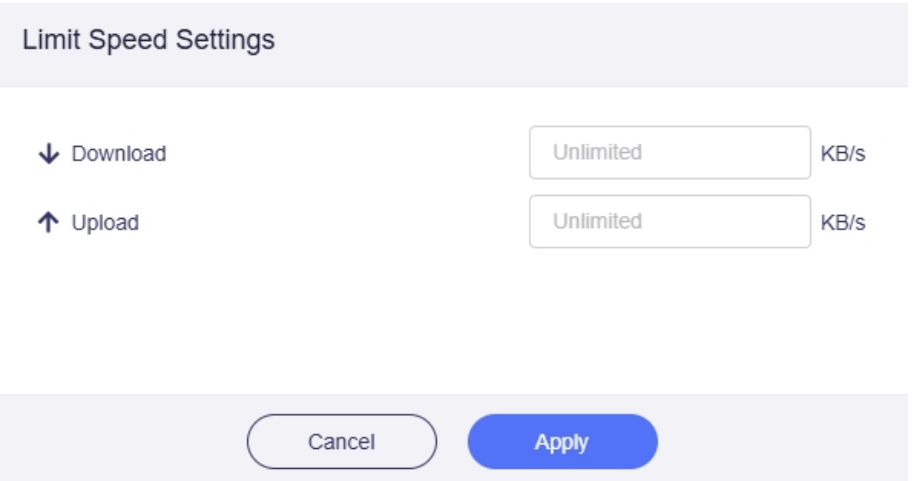


3. **Limitar velocidad**

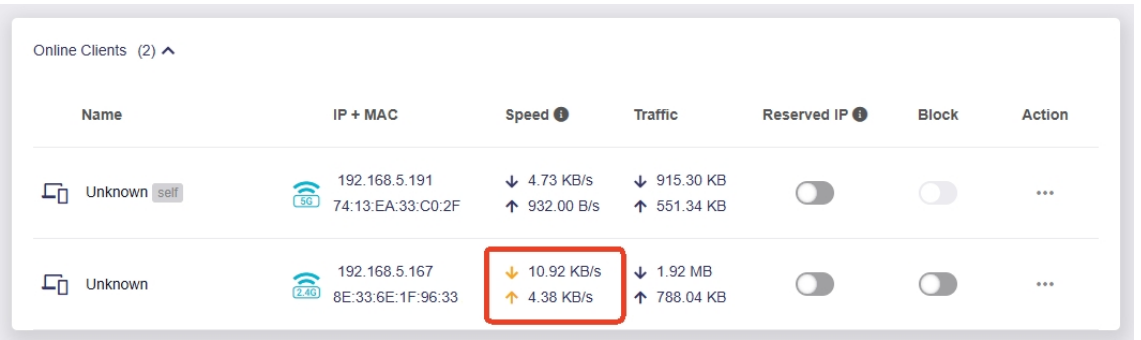
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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



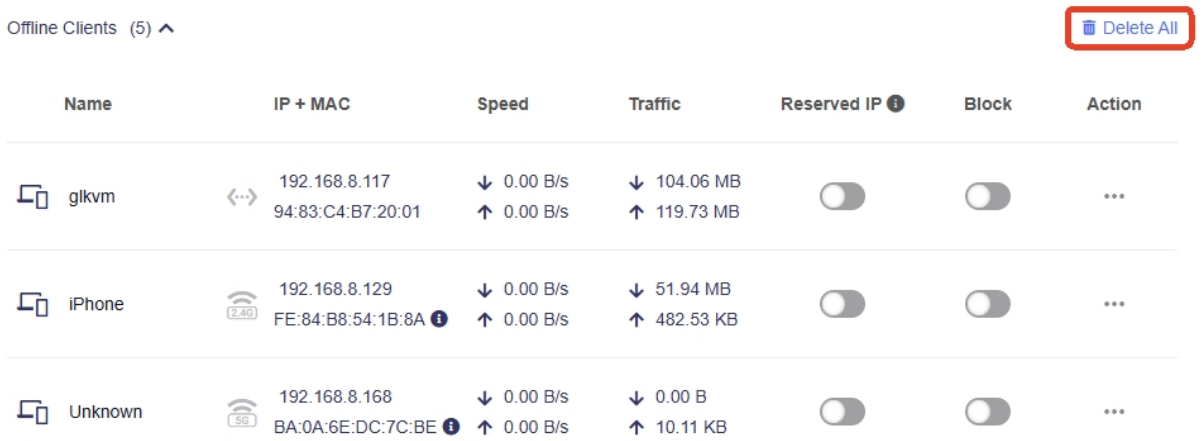
Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



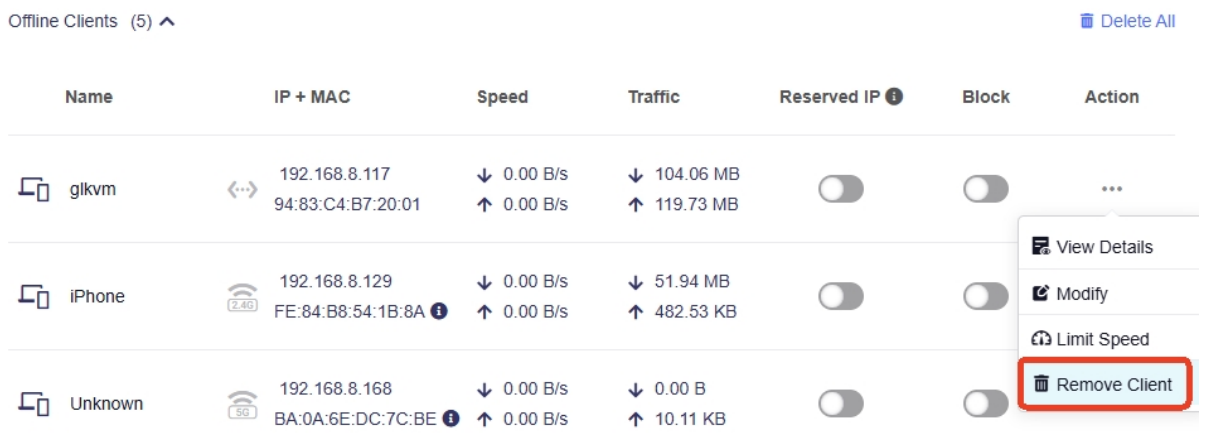
Consejo: Si la opción Limitar velocidad no está visible, vaya a **RED** > **Aceleración de red** y deshabilítela. La opción Limitar velocidad estará disponible.

6.3 Eliminar clientes

En **Ofuera de línea Cclientes** sección, puedes haga clic **Eliminar todo** en la esquina superior derecha para eliminar todo sin conexión clientes.

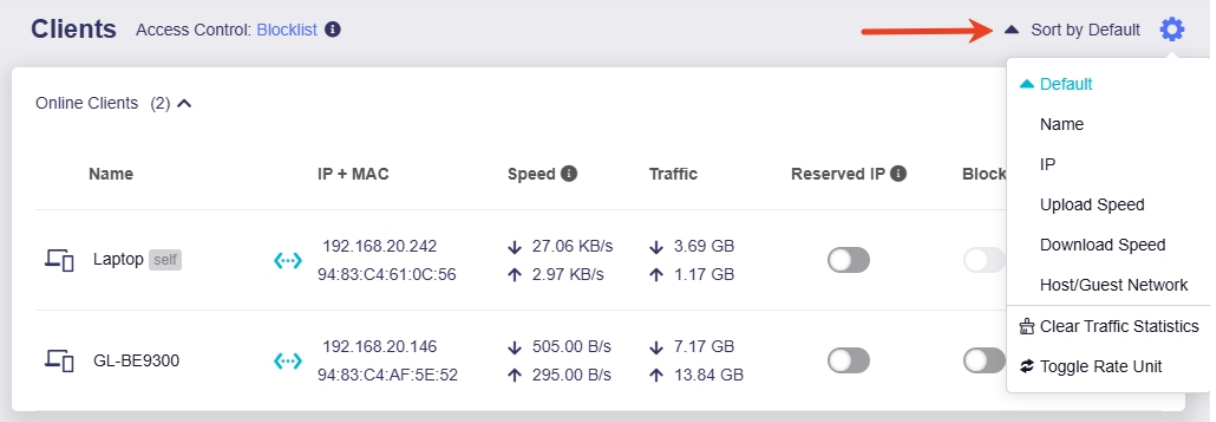


Si desea eliminar un cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Eliminar cliente** de el desplegable menú.



6.4 Ordenar

Puede configurar la regla de clasificación de dispositivos para la página Cliente en arriba 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 aparece en primer lugar.
- En **Oen línea Cclientes**, los dispositivos aparecen en una lista más alta si se conectaron antes.
- En la línea **Apagado Clients**, los dispositivos aparecen en una lista superior si desconectados anteriormente.

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 remota acceder y administrar GL.enrutadores iNet. Al centralizar los dispositivos de red en la nube, los usuarios pueden realizar de manera eficiente tareas de administración por lotes, como implementar configuraciones de red y ejecutar software actualizaciones. 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.

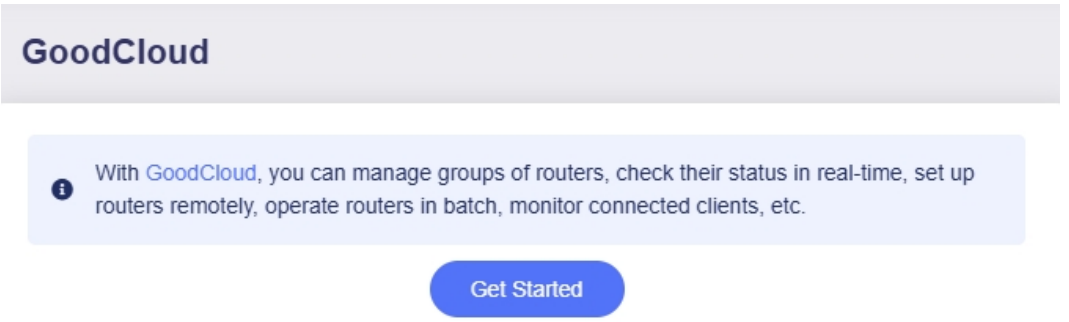
Con GoodCloud, puede:

- Verificar estado de su enrutador'estado en tiempo real
- Madministrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitorr clientes conectados
- Operar enrutadores por lotes
- Establecer Sitio-a-Sitio conexión

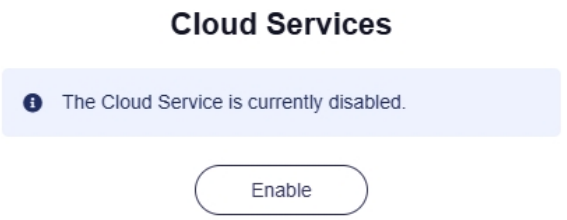
Algunas funciones están disponibles en el Plan Empresarial y el Plan VAR (Revendedor de Valor Agregado). Consulte aquí para obtener más detalles.

7.1.1 Habilitar GoodCloud

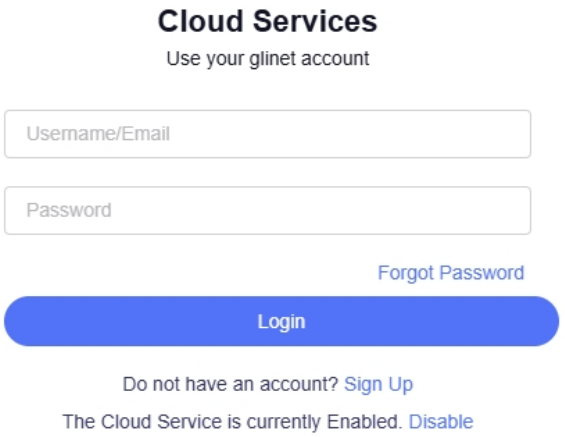
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



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



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

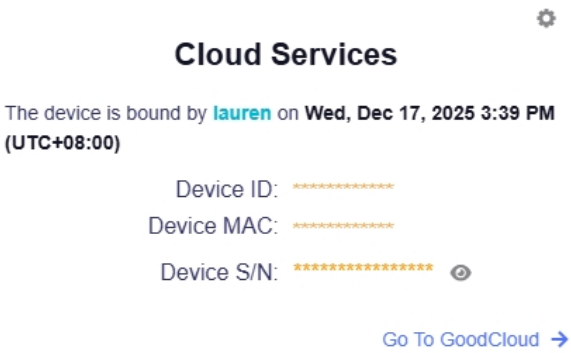


Consejos:

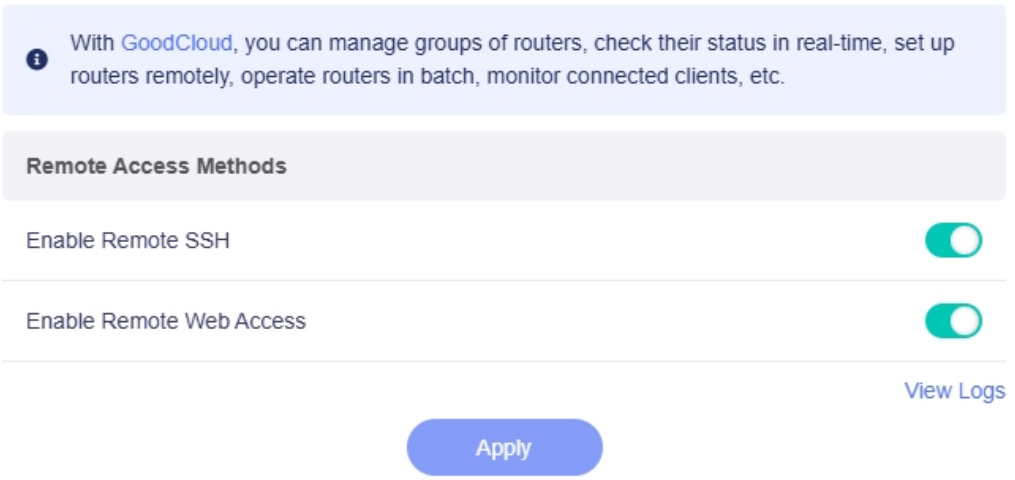
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.

- Al registrar una cuenta, sisi no recibe el correo electrónico de verificación, verifique tu carpeta de correo no deseado o inténtalo de nuevo más tarde. Para asistencia, contáctenos en support@gl-inet.com.

4. Después del enlace con éxito, yverá los detalles del dispositivo vinculado en la esquina superior derecha del administrador web panel, incluida la cuenta vinculada, la fecha de vinculación, el ID del dispositivo, la MAC del dispositivo y el S/N del dispositivo.



5. En el panel de administración web, vaya a **SERVICIOS EN LA NUBE** > **GoodCloud** y habilitar el acceso remoto. GoodCloud permite el acceso remoto al panel de administración web y al terminal del enrutador vinculado'. Esto es particularmente útil para la administración remota, configuración de red y resolución de problemas. Puede habilitar o deshabilitar el acceso remotopuedes habilitar o deshabilitar el acceso remoto para su enrutador aquí.



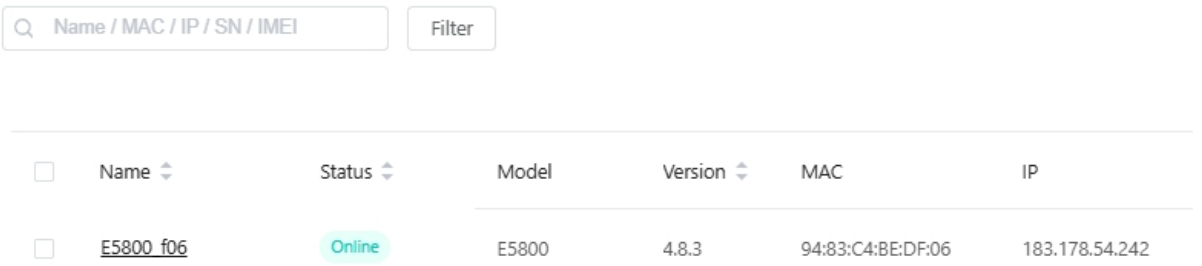
- **Acceso remoto SSH**: acceso remoto el terminal del enrutador desde GoodCloud usando SSH.

- **Acceso web remoto**: Remotely acceso a la web del enrutador admin panel de GoodCloud vía HTTP/HTTPS.
- **Ver registros**: Redirigir a la página de registro y mostrar la nube log.

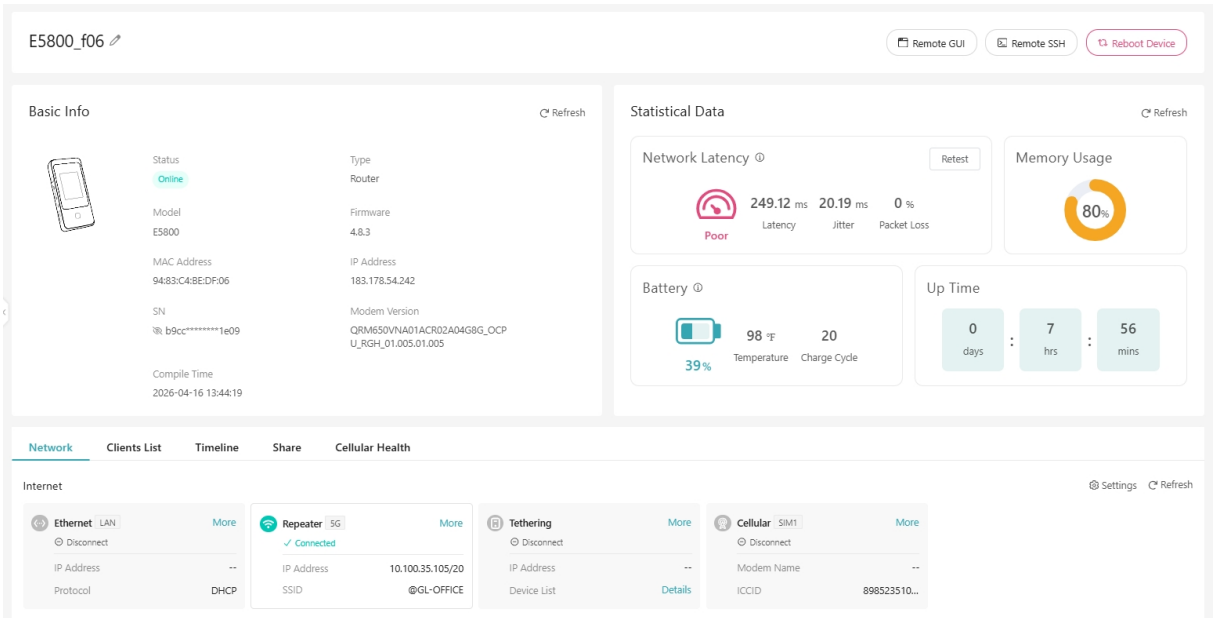
7.1.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

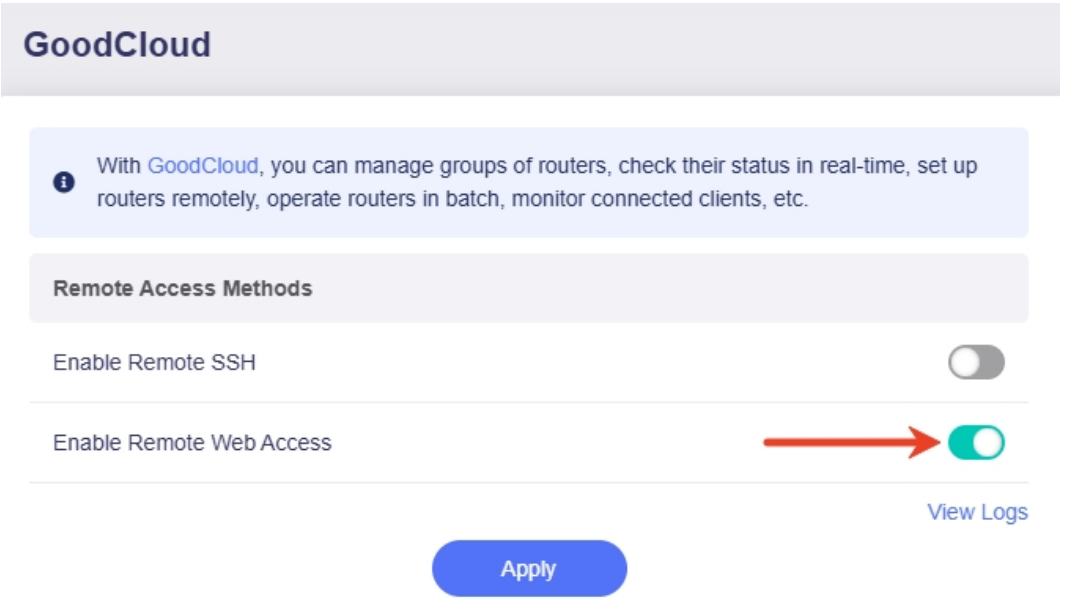


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puedes realizar operaciones avanzadas, como acceso remotolying el enrutador, y rearranque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

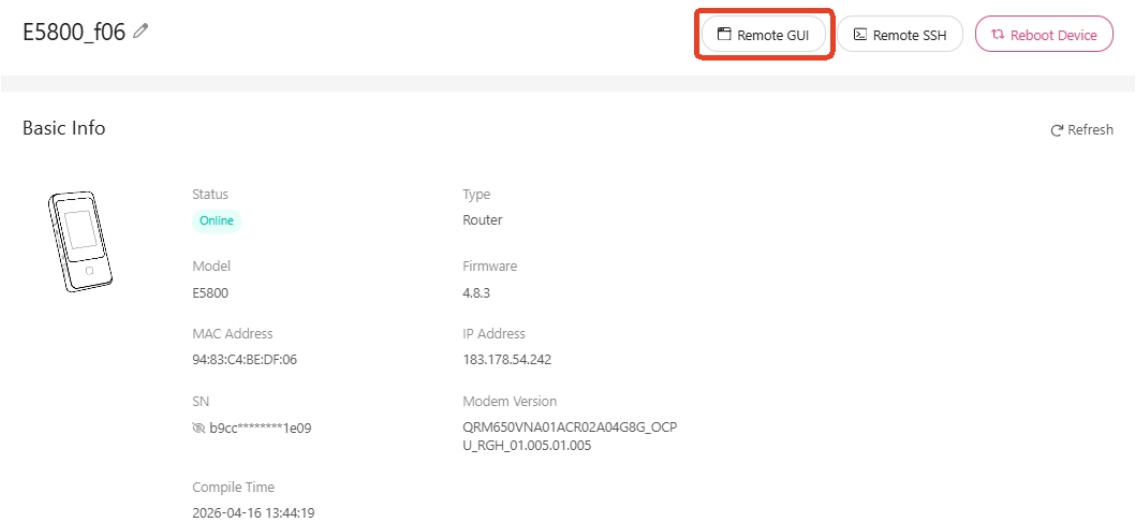


Acceso web remoto

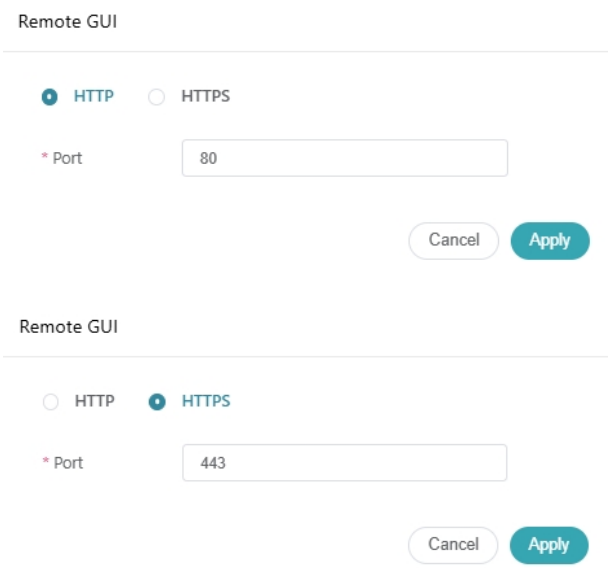
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso web remoto** y luego haga clic en **Aplicar**.



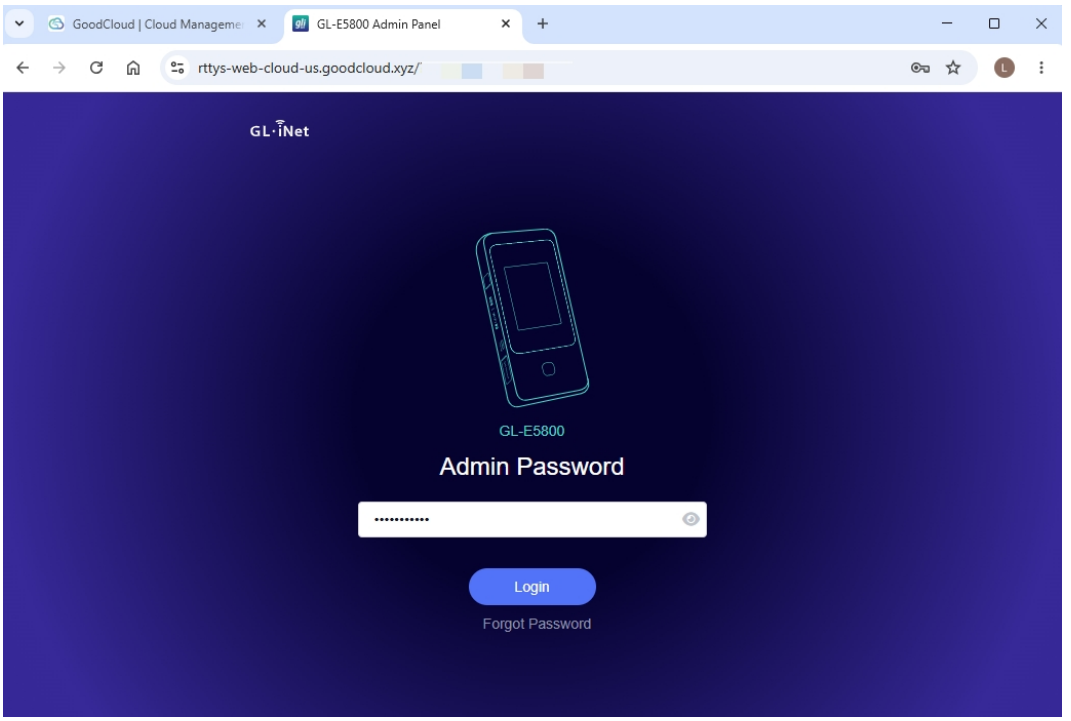
2. Inicie sesión en GoodCloud plataforma y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina superior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

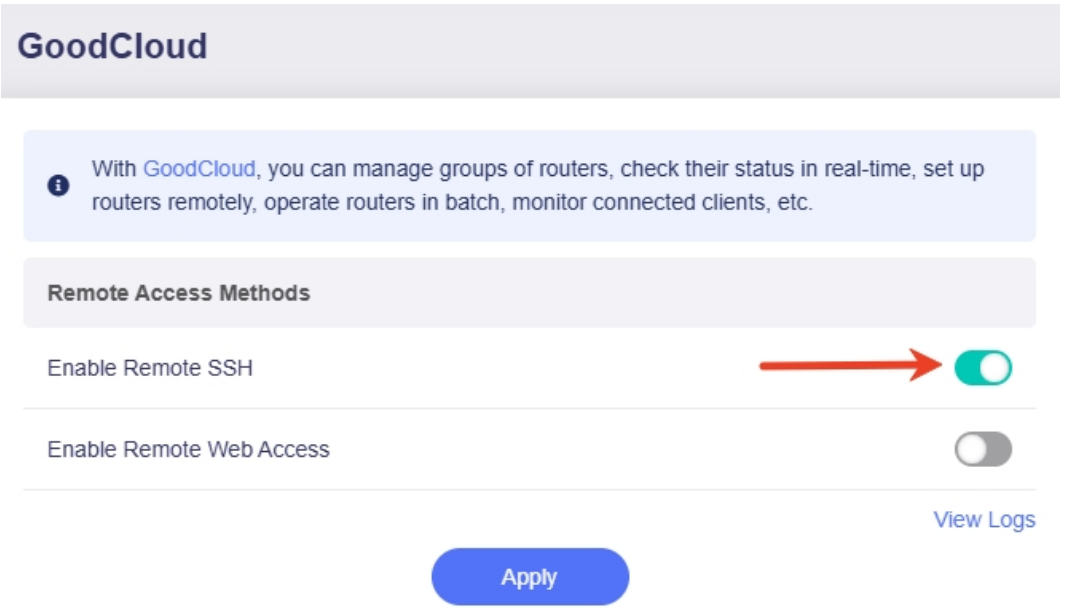


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

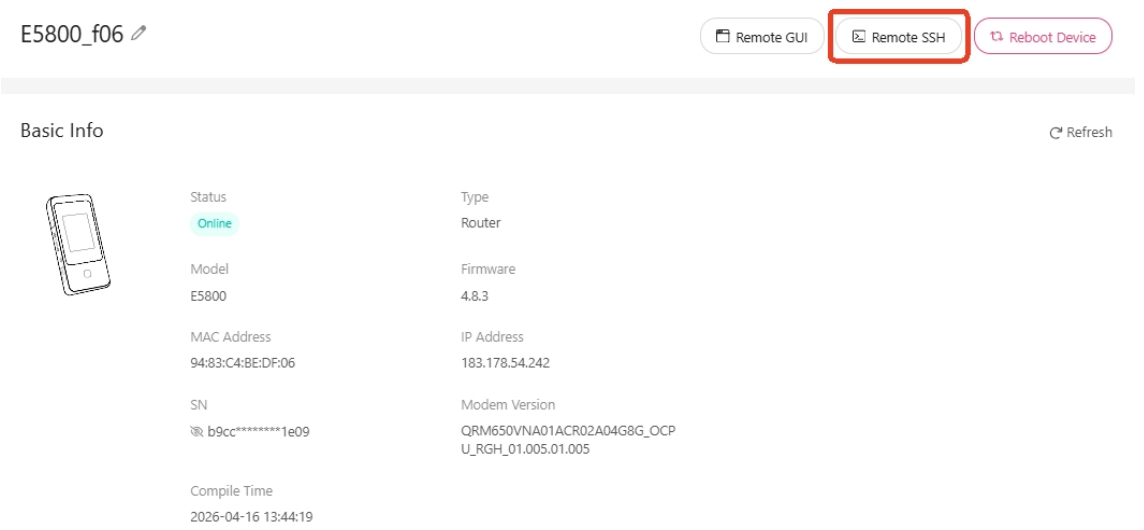


Acceso remoto al terminal

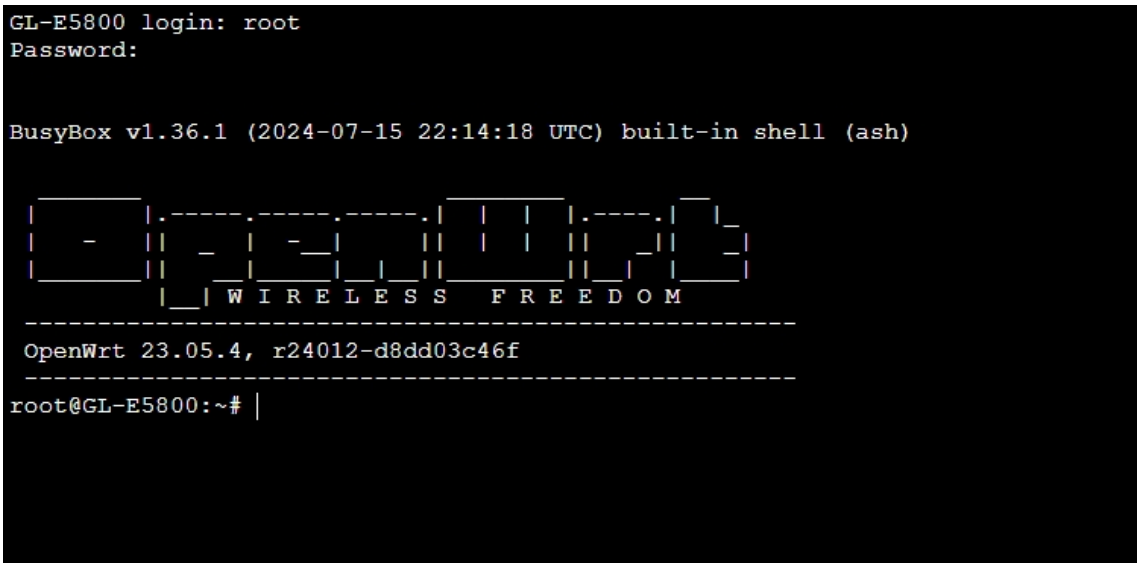
1. Inicie sesión en el panel de administración web del router', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.



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** en la esquina superior derecha.

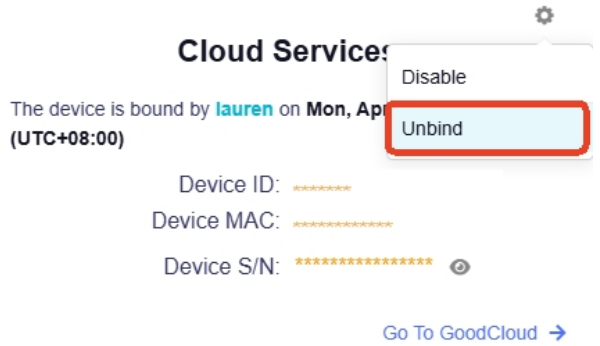


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

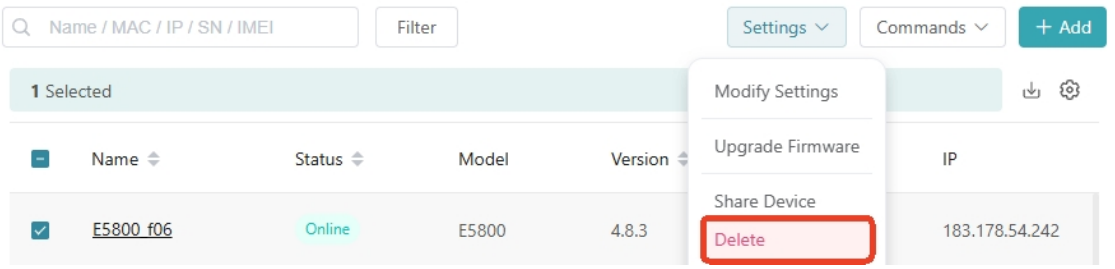

GL-E5800 login: root
Password:
BusyBox v1.36.1 (2024-07-15 22:14:18 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 23.05.4, r24012-d8dd03c46f
root@GL-E5800:~#

7.1.3 Desvincular el dispositivo

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

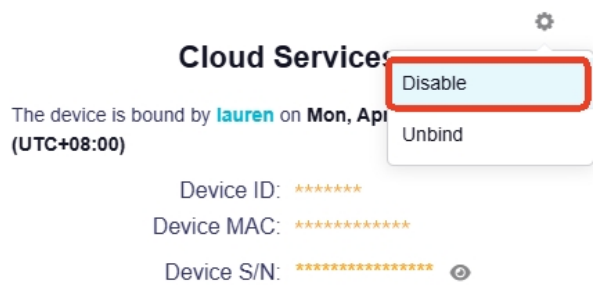


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su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



7.1.4 Desactivar GoodCloud

Si ya no desea que el dispositivo esté conectado a la nube, haga clic en el 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 proporcionar redes remotas sin interrupciones y administración remota de dispositivos.

Creado específicamente para la integración del enrutador GL.iNet, AstroWarp admite la administración integral de dispositivos en redes completas, lo que permite el control superior e inferior del dispositivo.

Con un enfoque en la administración de toda la red y el soporte futuro para el control a nivel de hardware, AstroWarp ofrece una solución más sólida y confiable para administrar dispositivos y mantener redes seguras y estables.

Consulte astrowarp.net para obtener más información. información.

Capítulo 8

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

8.1 Introducción

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 redes privadas o restringidas.

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. configuración.

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.

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.

WireGuard

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

8.2 Escenarios de aplicación

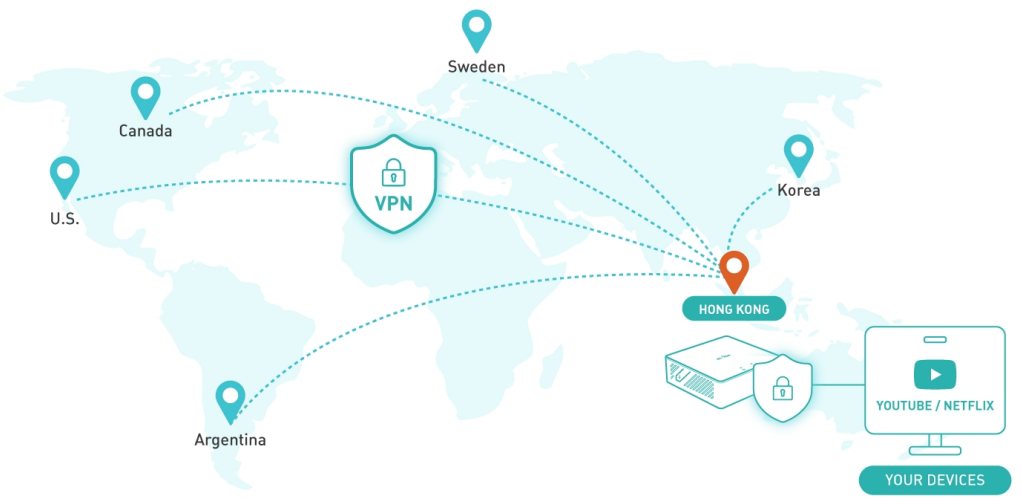
1. **Privacidad de datos personales**

   El servicio VPN de este enrutador funciona con una completa gama de dispositivos cableados e inalámbricos, incluidos portátiles, tabletas, teléfonos inteligentes, consolas de juegos y televisores inteligentes. Todos sus datos transmitidos a través de conexiones por cable y Wi-Fi están protegidos por la VPN. También puede personalizar las políticas de VPN para permitir una protección flexible para dispositivos específicos.



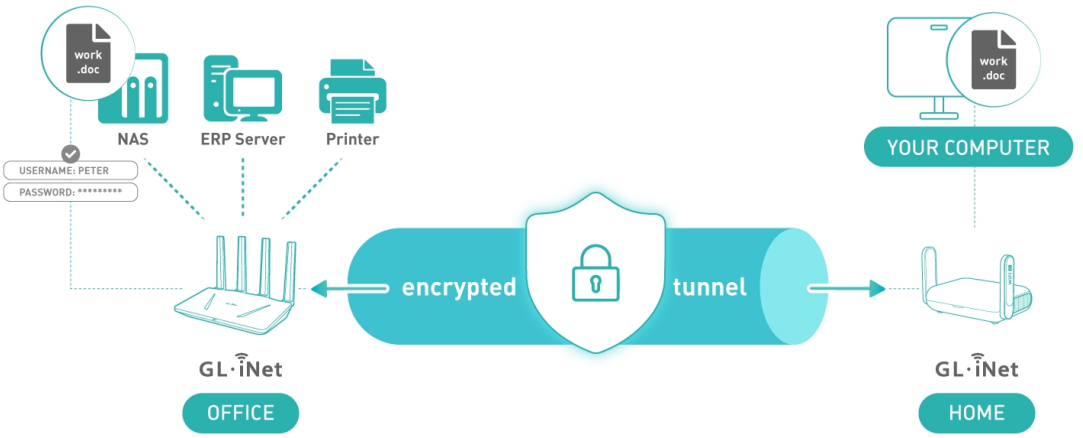
2. **Acceso sin restricciones en todo el mundo**

   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.



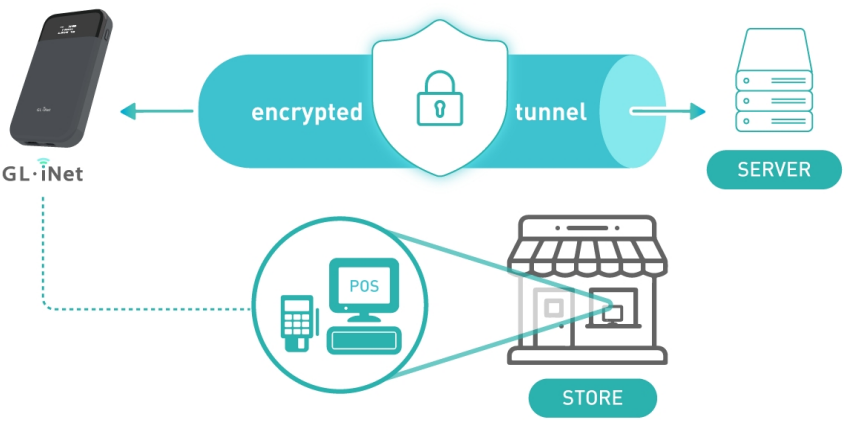
3. **Seguridad de datos para pequeñas empresas**

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



4. **Infraestructura de pago segura**

   Los propietarios de pequeñas tiendas 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

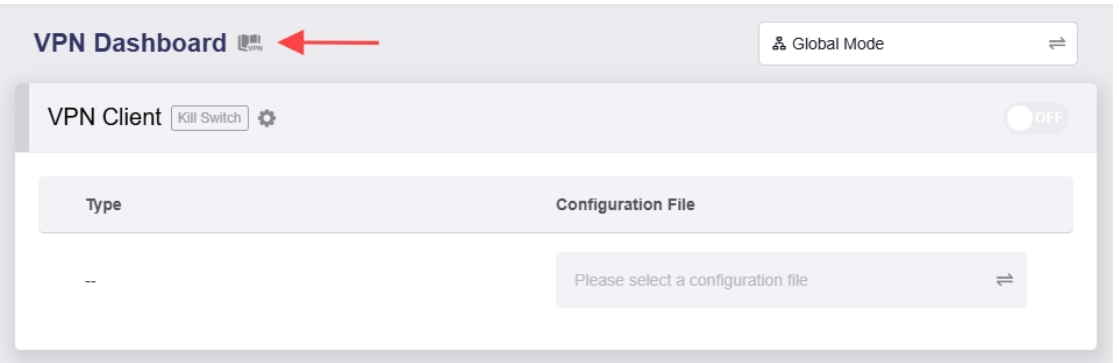
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

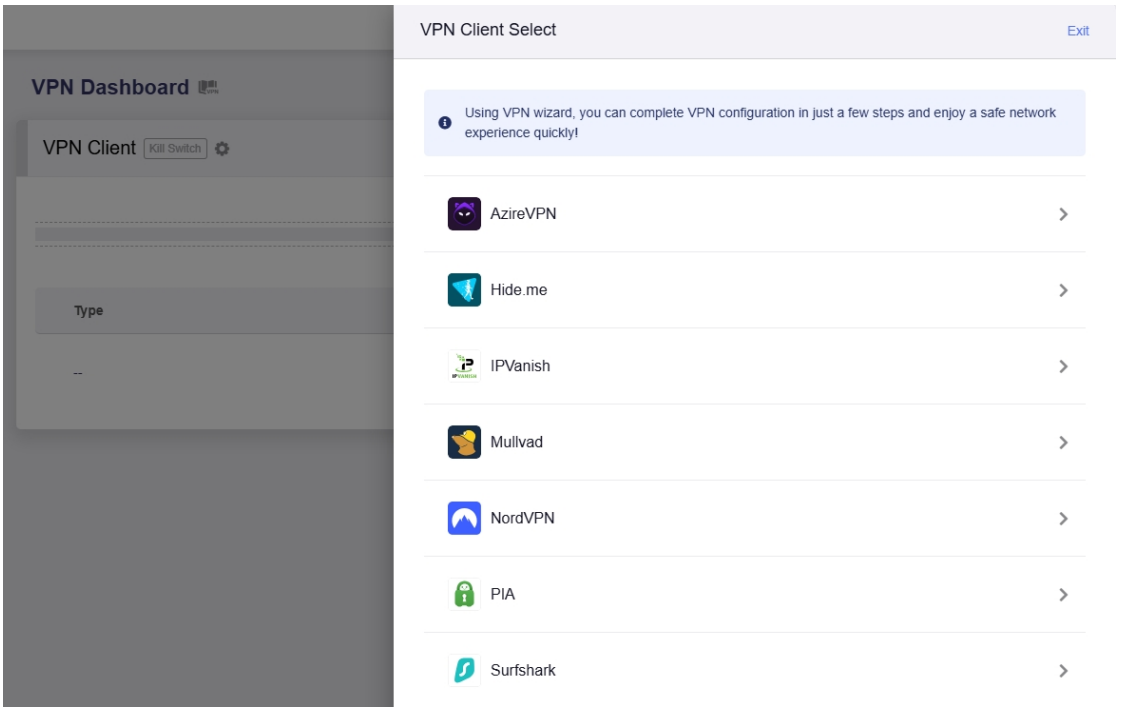
Inicie sesión en enrutador’s web admin panel y navega a **VPN** > **Panel de VPN**.

El panel de VPN muestra 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.



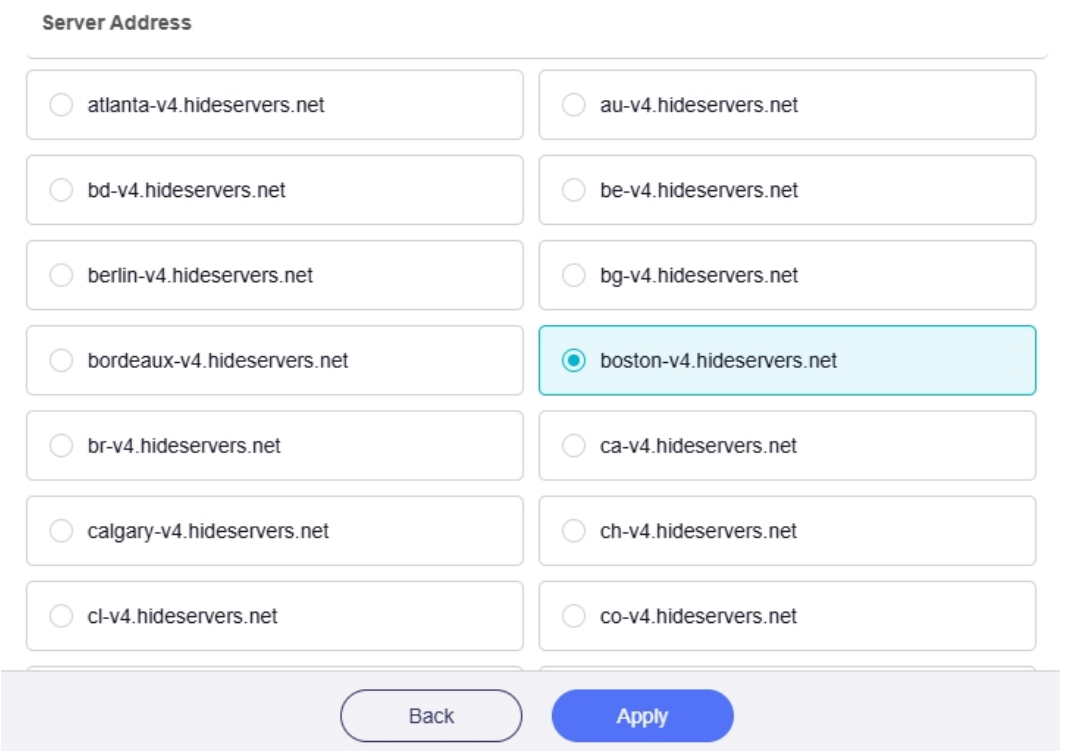


Nota: El asistente de configuración de VPN es solo para los servicios VPN integrados, incluidos AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA y Surfshark. Para otros proveedores de VPN, omita el asistente y vaya a **VPN** > **Cliente OpenVPN** o **Cliente WireGuard** para configurar la VPN. manualmente.

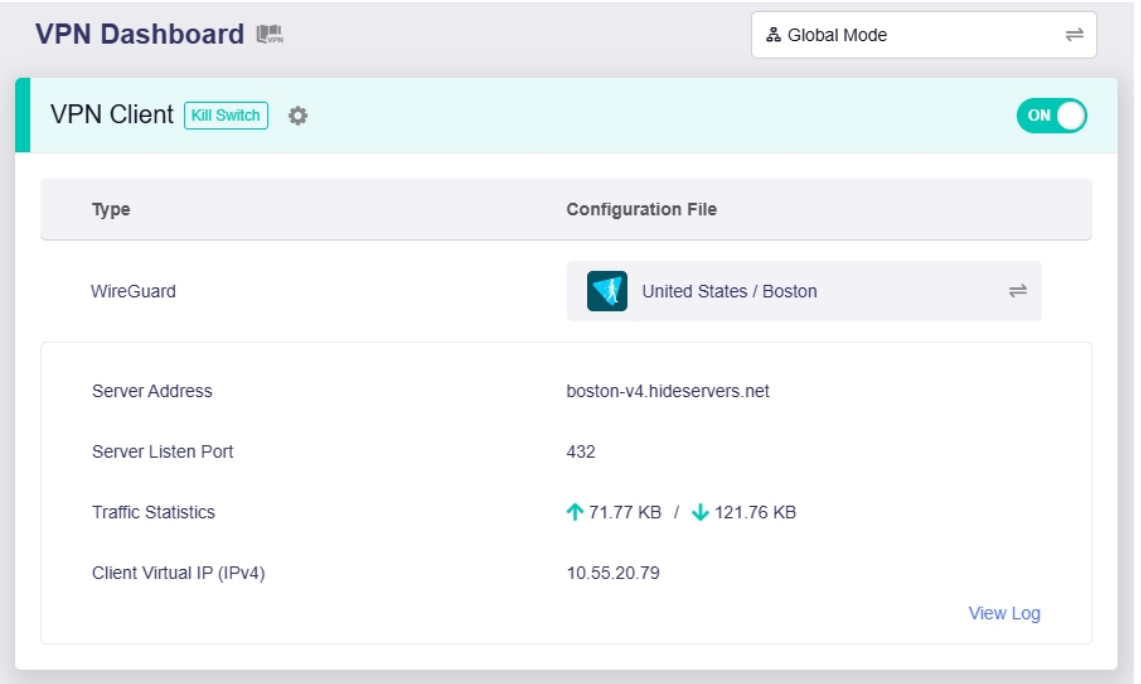
Aquí hay un ejemplo con **Hide.me**. Inicie sesión con las credenciales de Hide.me.



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.

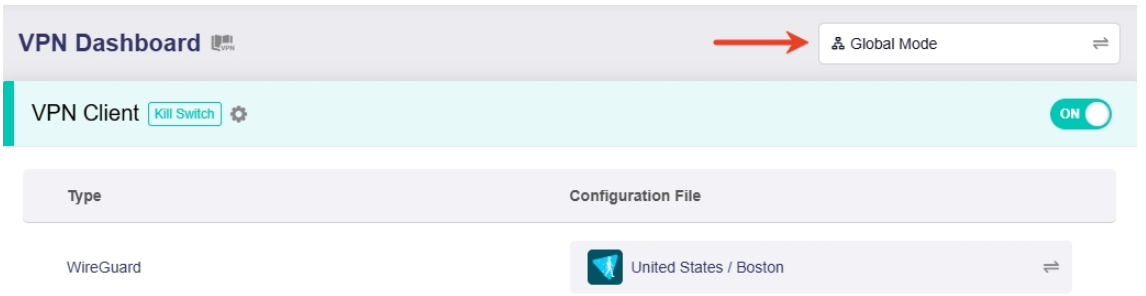


Se conectará automáticamente. Una vez conectado, vaya al **Panel de VPN**. Verá que se ha habilitado un túnel VPN, que muestra detalles que incluyen el protocolo VPN (por ejemplo, WireGuard), el archivo de configuración, la dirección del servidor, el puerto de escucha del servidor, las estadísticas de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

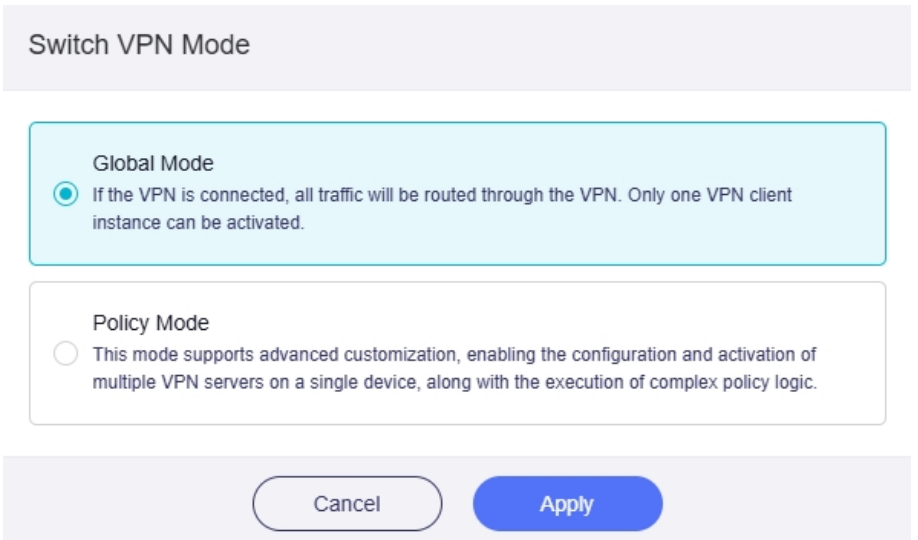


9.2 Modo VPN

En el Panel de VPN, haga clic en el botón en la esquina superior derecha para cambiar los modos VPN según sea necesario.



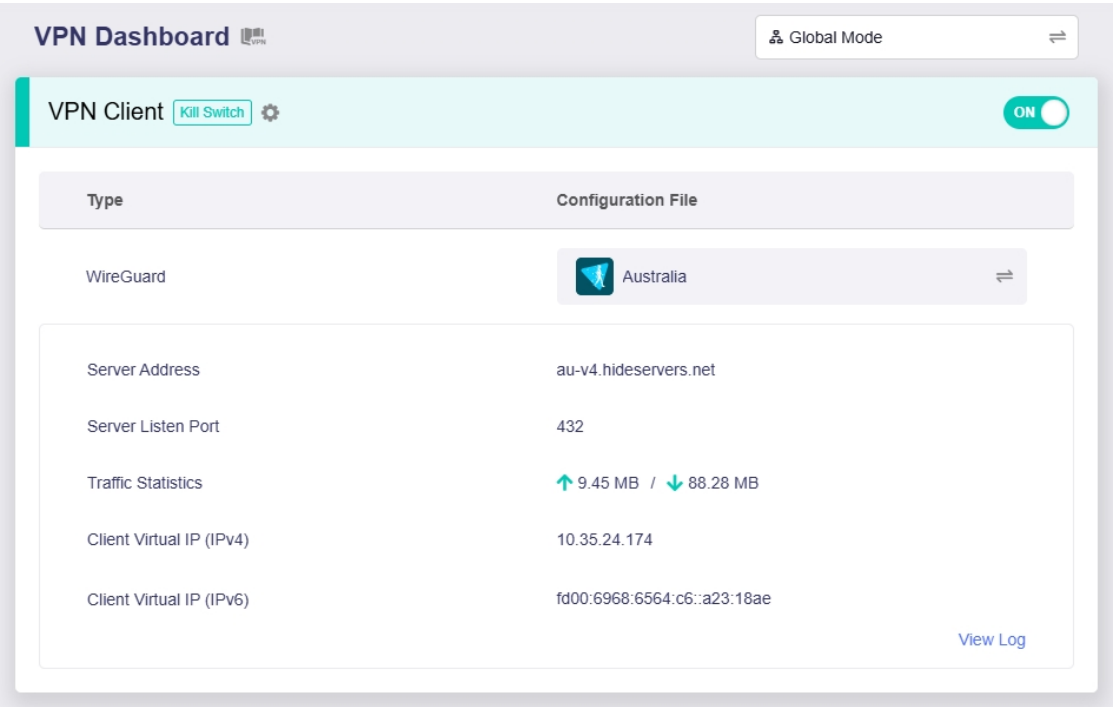
Dos modos están disponibles: **Modo global** y **Modo de política**.



9.2.1 Modo global

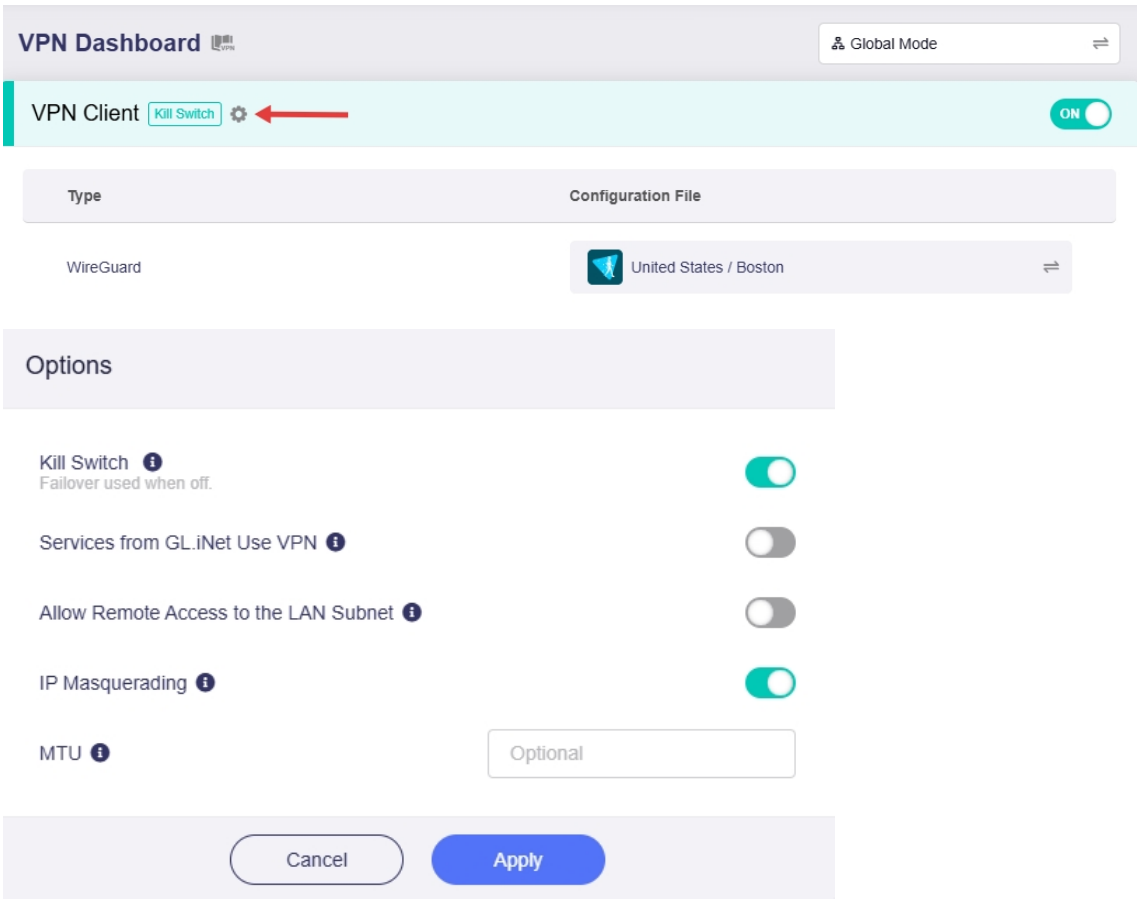
En este modo, todo el tráfico se enrutará a través del túnel VPN y solo se puede activar una instancia de cliente VPN. Es ideal para escenarios que requieren que todo el tráfico del dispositivo pase a través de un único servidor VPN, como seguridad de red unificada o acceso a contenido específico de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



Opciones de túnel

Puede configurar ajustes avanzados para su túnel VPN, como VPN Kill Switch, enmascaramiento de IP y MTU. Haga clic en el ícono de ajustes en la esquina superior derecha.

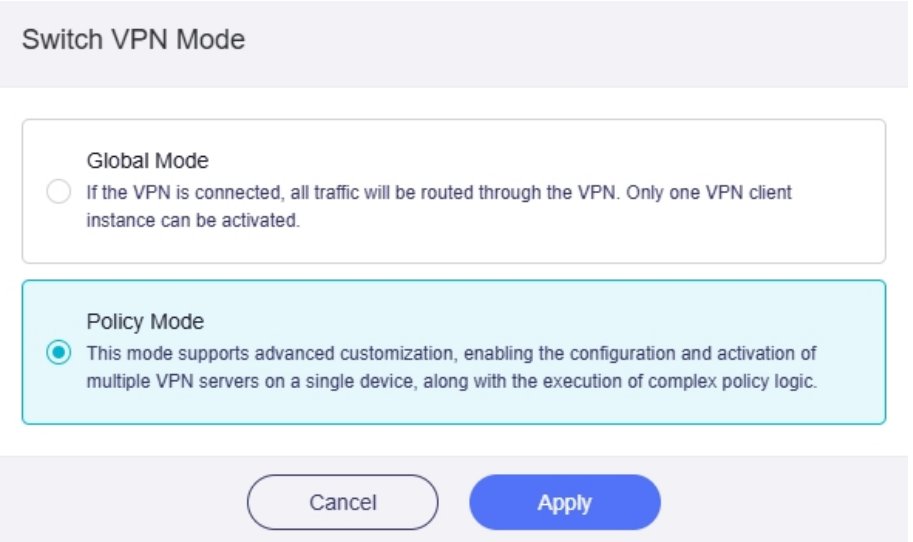


- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, cualquier tráfico enrutado a través de este túnel VPN se bloqueará automáticamente cuando falle la conexión VPN. Si está deshabilitado, el tráfico volverá a la WAN local y accederá a Internet sin pasar por el túnel VPN.
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán 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, se permitirá el acceso remoto a este enrutador y sus dispositivos LAN a través de VPN. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
- **IP Masquerading**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite 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 el valor definido en el archivo de configuración.

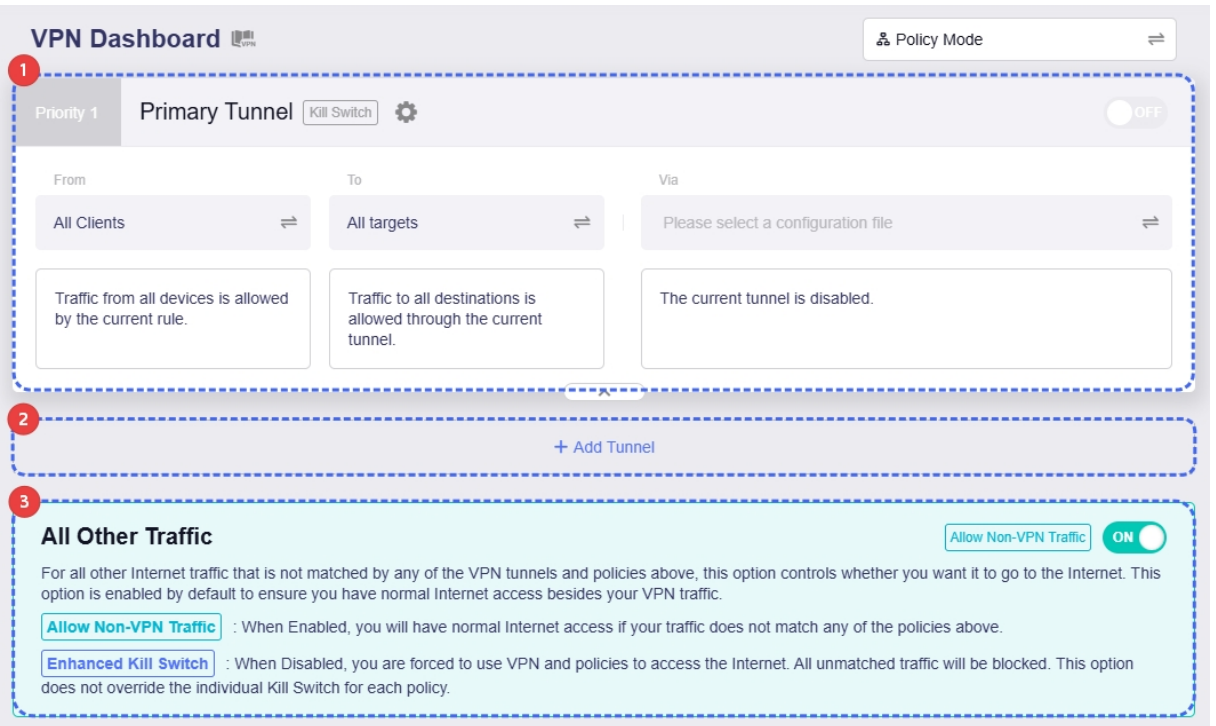
9.2.2 Modo de política

En este modo, puede conectar un único enrutador a varios servidores VPN y personalizar 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 en **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**.

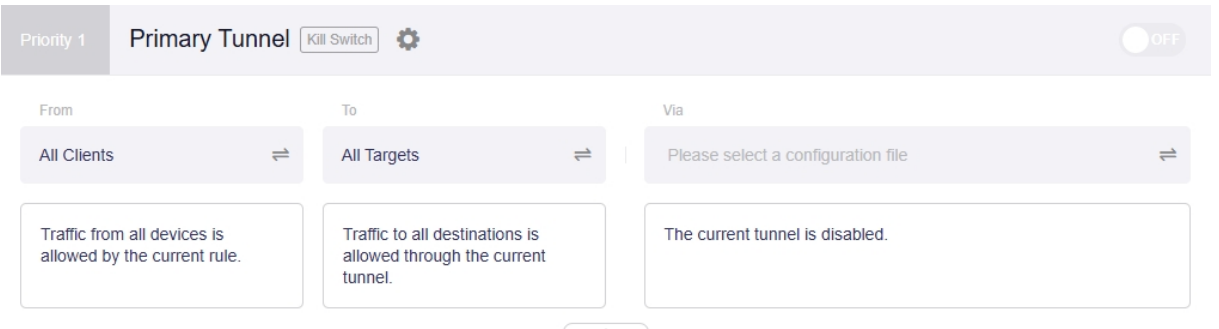


Túnel principal

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.

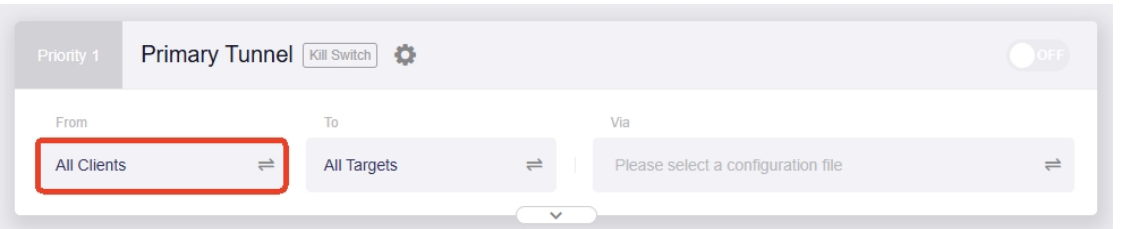
En este túnel, puede personalizar la regla del túnel estableciendo tres factores:

- **De**: 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 deles túnel.
- **Vía**: Se refiere al método de enrutamiento del tráfico, es decir, si se utiliza VPN.

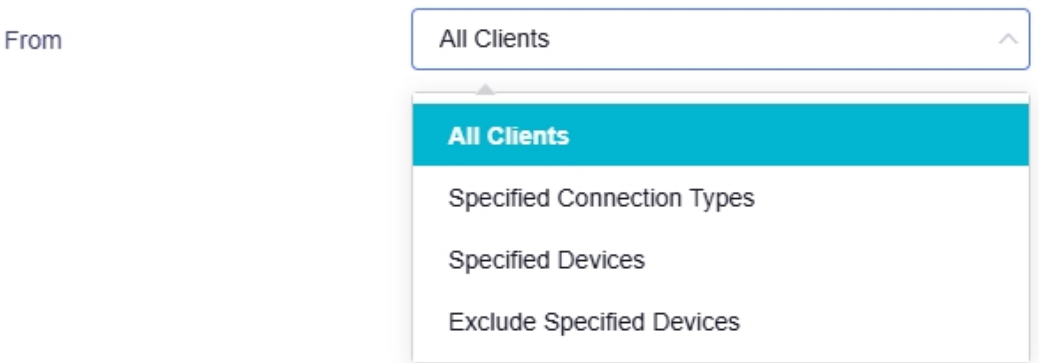


Siga los pasos a continuación para configurar su regla de túnel.

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

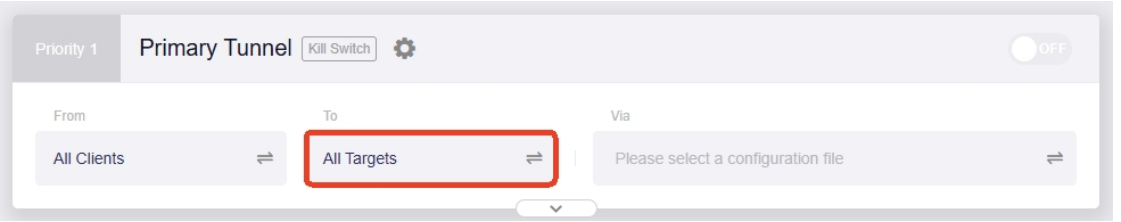


2. Seleccione el dispositivo que desea coincidir con esta regla y haga clic **Aplicar**.

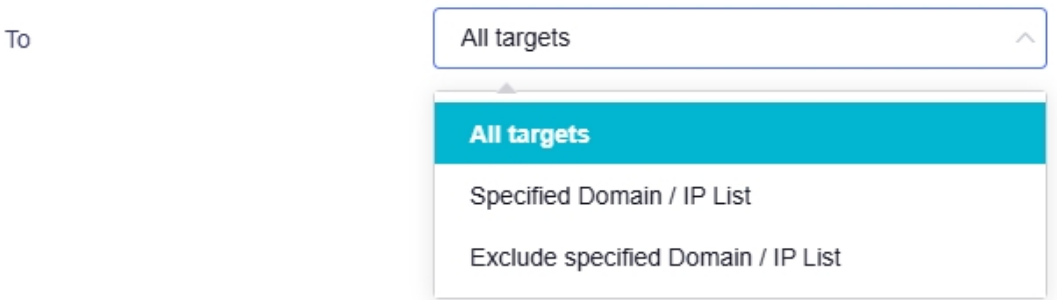


- **Todos los clientes**: Si se selecciona, el tráfico de todos los dispositivos coincidirá con esta regla.
- **Conexión especificada Tipos**: Si se selecciona, el tráfico de la conexión especificada tipos (por ejemplo, subred LAN, puerta de enlace directa, red de invitados) coincidirá esta regla.
- **Dispositivos especificados**: Si se selecciona, el tráfico de los dispositivos especificados (identificados por la dirección MAC) coincide esta regla.
- **Excluir dispositivos especificados**: Si se selecciona, el tráfico desde dispositivos específicos (identificados por dirección MAC) sel **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**.

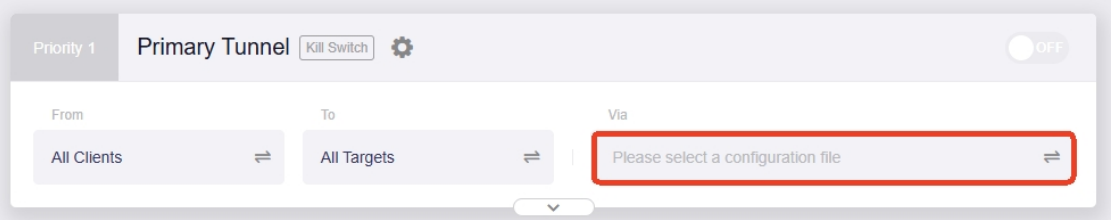


- **Todos los Tobjetivos**: Si se selecciona, el tráfico que coincida con esta regla se enrutará a todos los destinos.
- **Dominio especificado/ Lista de IP**: Si se selecciona, el tráfico que coincida con esta regla se enrutará al dominio/IP especificado. Usted necesita ingrese el dominio/IP especificado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

Nota: Si selecciona URL de suscripción, el nombre de dominio o la dirección IP en la URL se 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 gracuadro sombreado.

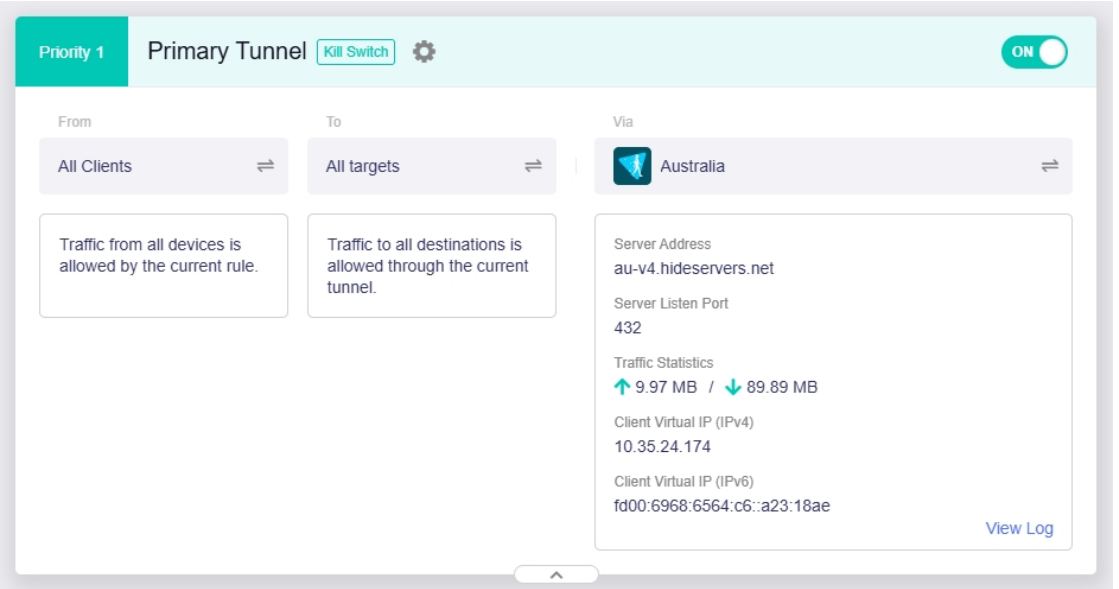


6. Seleccione el método de enrutamiento para este túnel: **Usar VPN** o **No usar VPN**.



- **Usar VPN**: Si se selecciona, trafica 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, trafica coincidente esta regla se enrutará a los destinoss seleccionados a través de local WAN red en lugar de VPN.

7. Después configurar el origen, el destino y el enrutamiento del tráfico método, la configuración de la regla del túnel principal está completa. En el siguiente ejemplo, la regla túnell es: Todos los clientes conectados a este enrutador accederán 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.



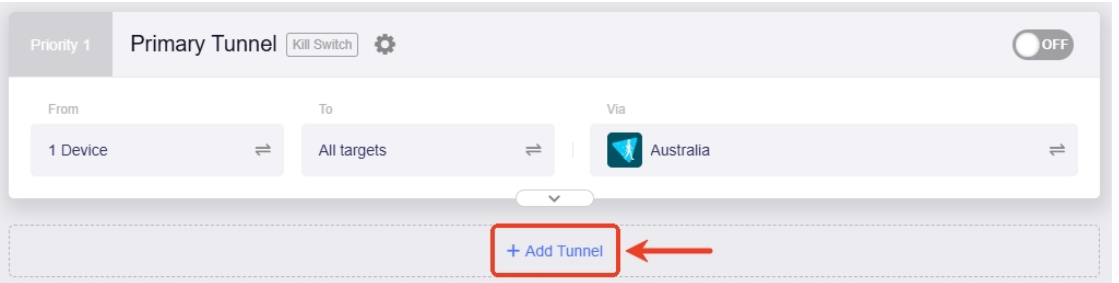
Nota: por seguridad, vaya a Todo el resto del tráfico y Opciones de túnel para verificar otras configuraciones antes de habilitar este túnel.

Agregar túnel

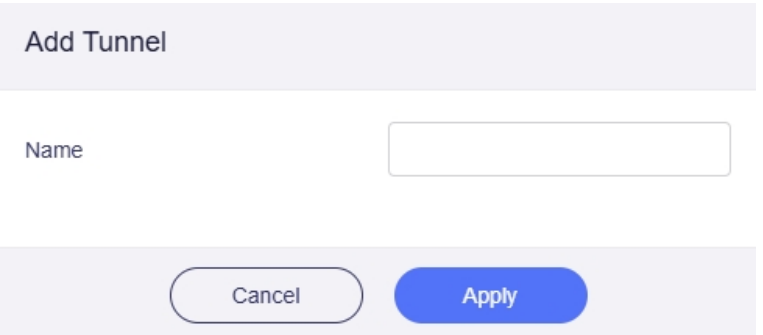
Agregue túneles si necesita enrutar el tráfico desde diferentes dispositivos a diferentes destinos.

Siga los pasos a continuación para agregar un túnel.

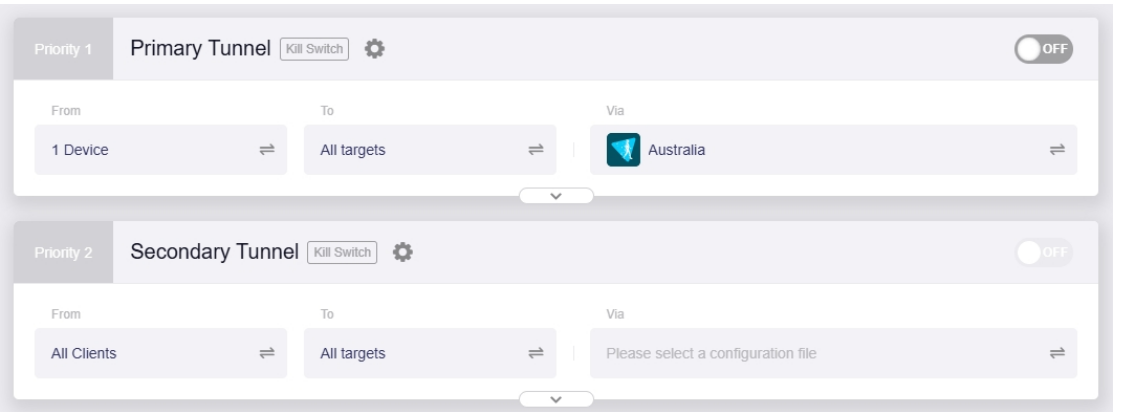
1. Haga clic en **Agregar túnel** debajo de Túnel principal.



2. Nombra el túnel.



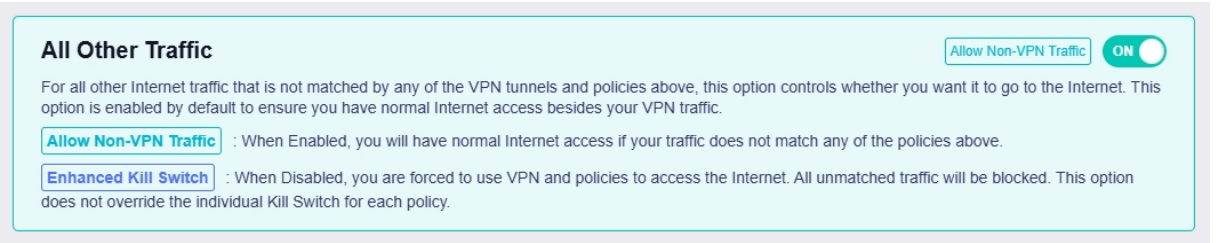
3. YObtendrá un túnel más en el Panel de VPN. Se pueden crear hasta 5 túneles (incluido el túnel principal preestablecido).



4. Configure reglas del túnel configurando la fuente de tráfico, destinos y el método de enrutamiento. Una vez terminado, verificar otros configuración en Todo el resto del tráfico y Opciones de túnel por seguridad antes de habilitar los túneles.

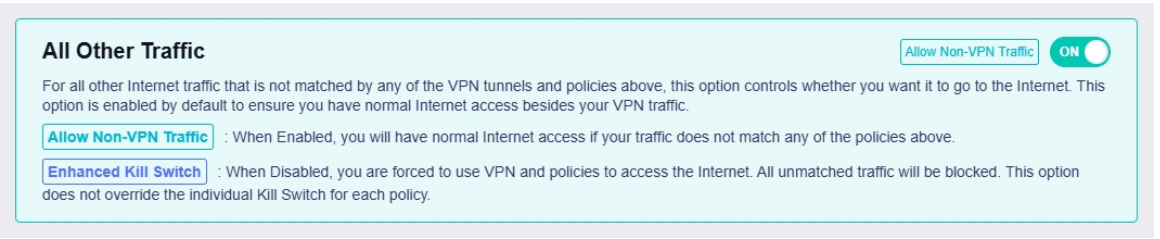
Todo el resto del tráfico

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

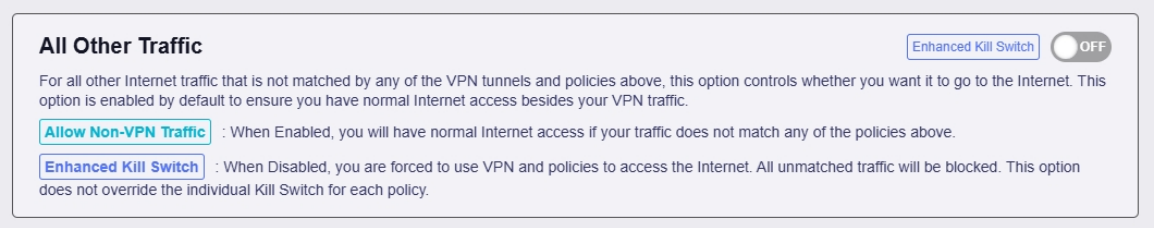


Este túnel controla si el tráfico que no coincide con ninguno de los grupos de túneles VPN anteriores puede acceder a Internet. Está habilitado de forma predeterminada para garantizar el acceso normal a Internet para el tráfico que no se enruta a través de VPN.

- 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.

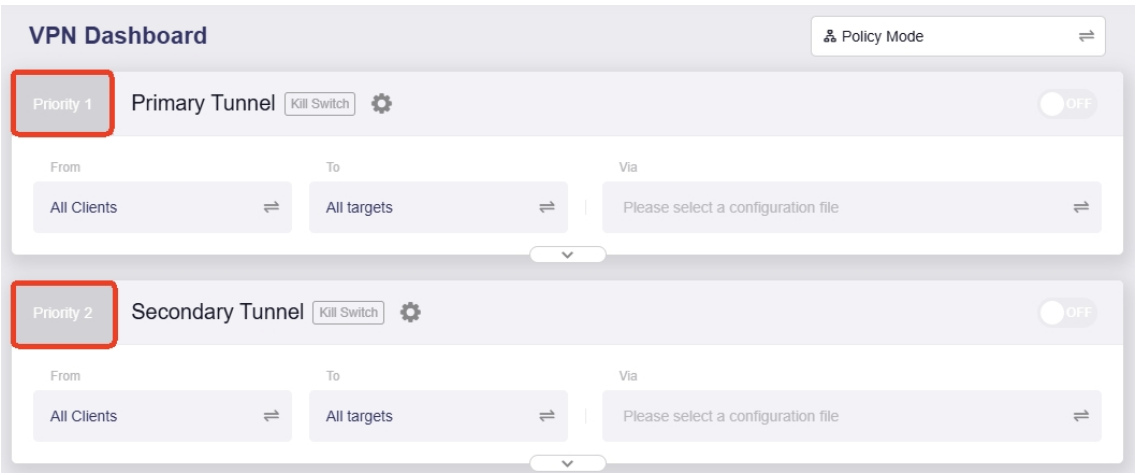


Prioridad del túnel

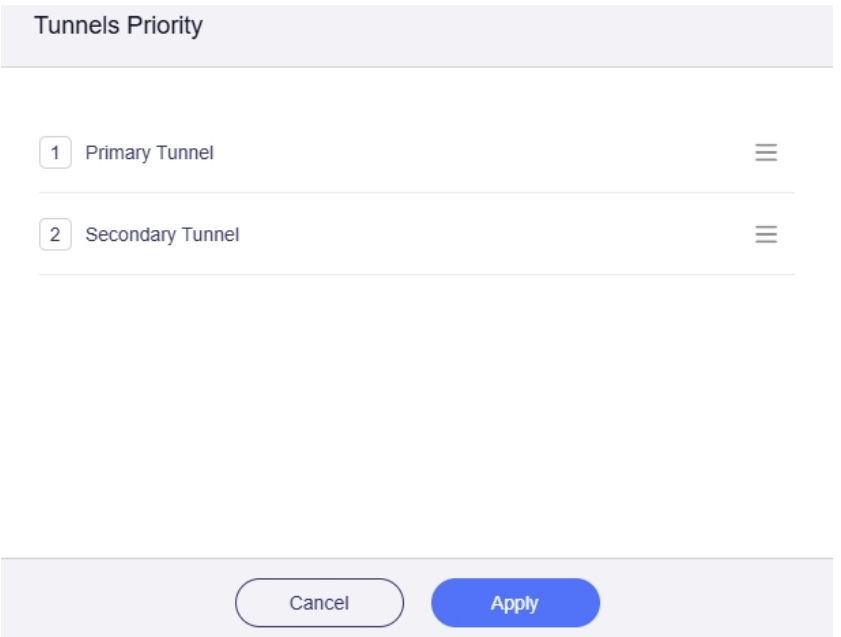
De forma predeterminada, el túnel primario preestablecido tiene la prioridad más alta, seguido de otro túnel agregado manualmente (si lo hay), luego el resto preestablecido Túnel de tráfico para garantizar conectividad de red a través de red ISP (WAN) local.

Si necesita parapara modificar la prioridad del túnel, siga los pasos que se indican a continuación.siga los pasos a continuación.

1. Click 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 reordenar el túnel, entonces haga clic en **Aplicar**.

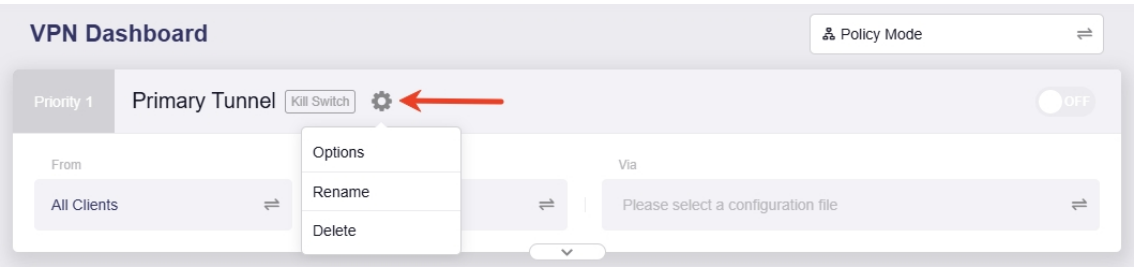


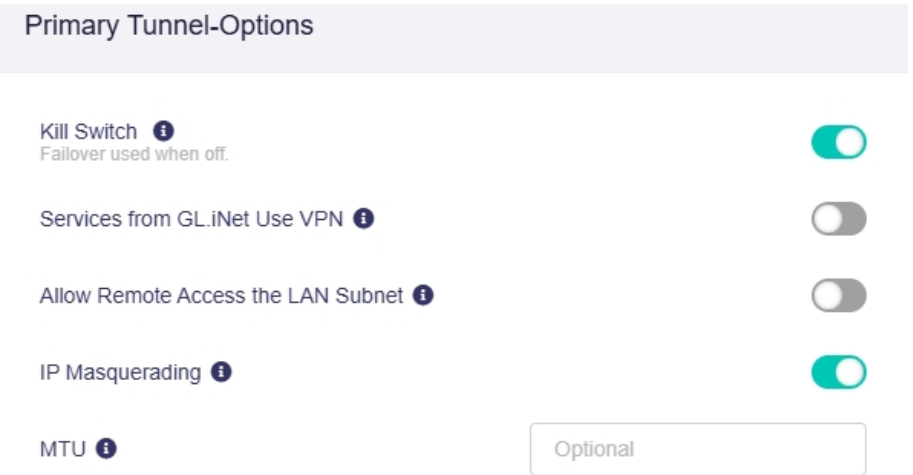
Cuando se habilitan varios túneles, el enrutador enrutará el tráfico en el siguiente orden:

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 conmutará por error el tráfico al siguiente túnel de prioridad en función de si el **Bloqueo de tráfico sin VPN (Kill Switch)** de este túnel está habilitado.
    - Cuando el interruptor de interrupción está habilitado, el tráfico se bloqueará y no pasará al siguiente túnel de prioridad.
    - Cuando el interruptor de interrupción está desactivado, el tráfico pasará al siguiente túnel de prioridad e intentará coincidir con sus reglas de túnel.
3. El **Todo el resto del tráfico** el túnel 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 el tráfico no coincidente o 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.

Opciones de túnel

Puede configurar ajustes avanzados para cada túnel VPN, como VPN Kill Switch, enmascaramiento de IP y MTU. Haga clic en el ícono de ajustes al lado del nombre del túnel.





- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, cualquier tráfico enrutado a través de este túnel VPN se bloqueará automáticamente si falla la conexión VPN. Si está deshabilitado, el tráfico pasará por error al siguiente túnel de prioridad o a la WAN local.
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán 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, se permitirá el acceso remoto a este enrutador y sus dispositivos LAN a través de VPN. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
- **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**: la MTU que configuró para el túnel sobrescribirá el valor en el archivo de configuración.

Capítulo 10

Configurar el servidor VPN

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

10.1 Configurar el 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. **Asegúrese de tener una dirección IP pública**

   Haga clic aquí para verificar si su proveedor de servicios de Internet (ISP) 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 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.

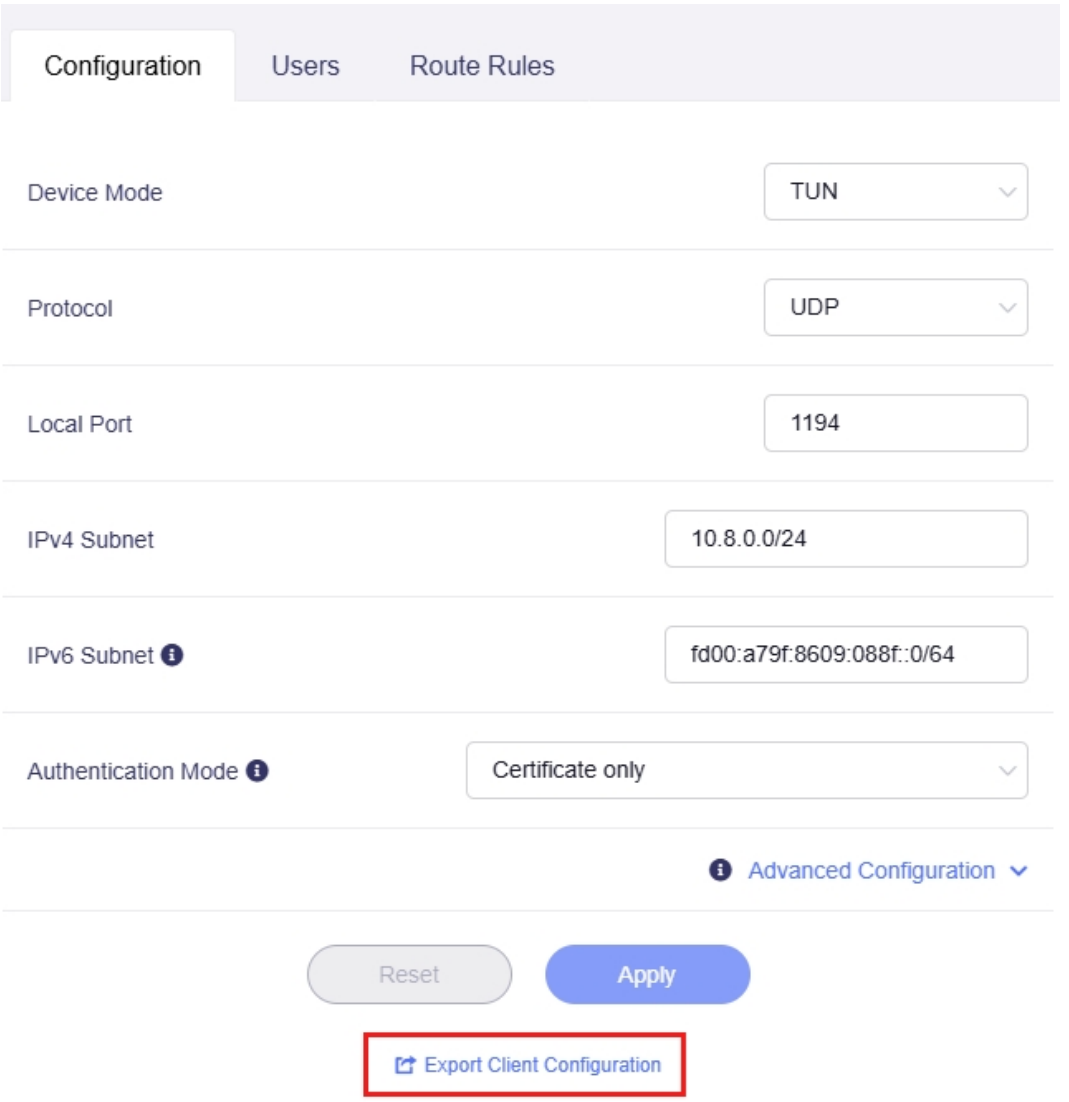
2. **Confirme si se requiere reenvío de puertos**

   - 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 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 se encuentra en varios niveles posteriores al 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** 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. 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.

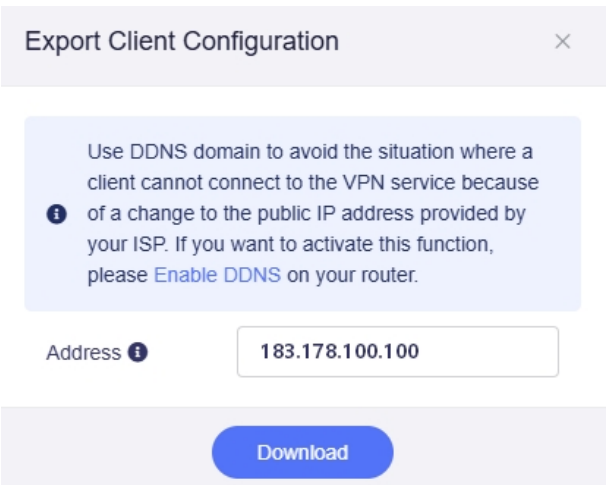


- **Dispositivo Modo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:
  - **Solo certificado**: 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 primero agregue un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente. Al cargar la configuración en el cliente, ingrese estas credenciales para la autenticación.
  - **Nombre de usuario/Contraseña y certificado**: si se selecciona, necesita primero agregue un nombre de usuario y contraseña en la pestaña **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 al cliente, primero se verificará la clave del certificado, seguida de la autenticación de nombre de usuario/contraseña para 2FA seguridad.
- **Configuración avanzada**: Personalizar más configuraciones del servidor según necesario.

3. Exportar configuración del cliente.

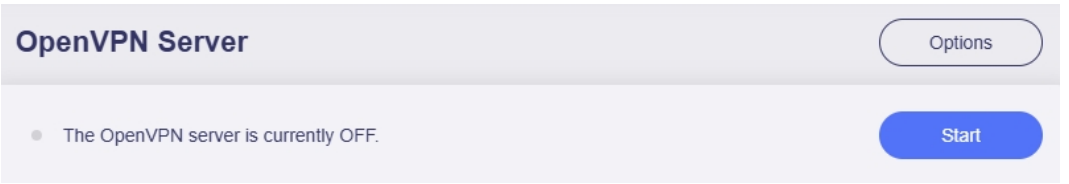
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



Consejos:

- Si su IP pública dirección 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 la top. Si muestra carga y descargar estadísticas de tráfico, significa que el servidor OpenVPN se está ejecutando.



10.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulta aquí para solucionar problemas.
- Es posible que tengas que configurar el reenvío de puertos. Consulte aquí para solucionar problemas.

- 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.

10.2 Configurar el servidor WireGuard

WireGuard® es una VPN simple pero rápida y moderna que utiliza criptografía de última generación. Su objetivo es ser más rápido, más simple y más útil que IPSec, evitando al mismo tiempo el enorme dolor de cabeza. Pretende tener un rendimiento considerablemente mayor que OpenVPN. Para configurar el servidor WireGuard en un enrutador GL.iNet, mire este vídeo o consulte los pasos a continuación.

10.2.1 Preparación

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

   Haz clic aquí para verificar si tu proveedor de servicios de Internet te asigna una IP pública dirección.

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

   Métodos alternativos:

   - Si tiene un enrutador principal ascendente 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.

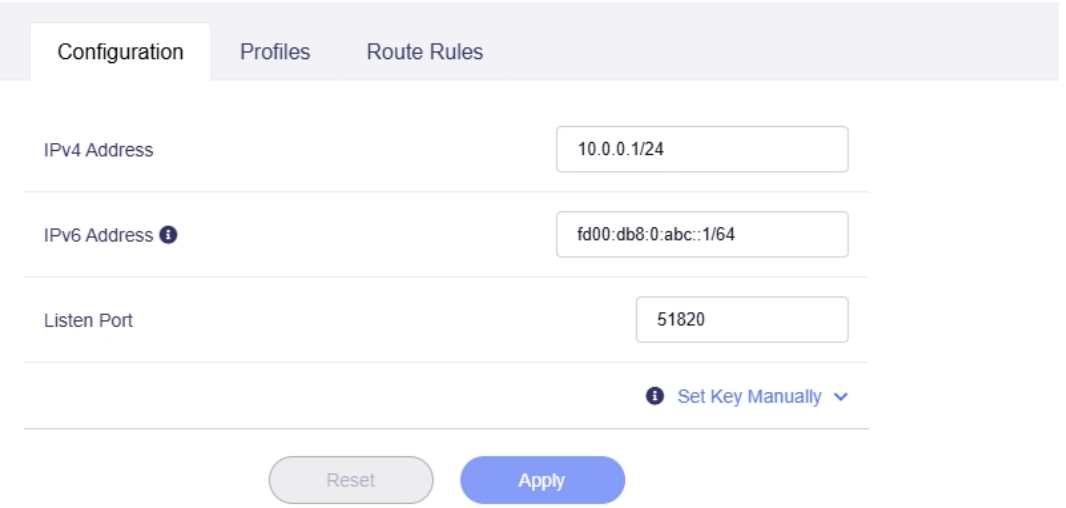
2. **Confirme si se requiere reenvío de puertos**

   - 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 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.

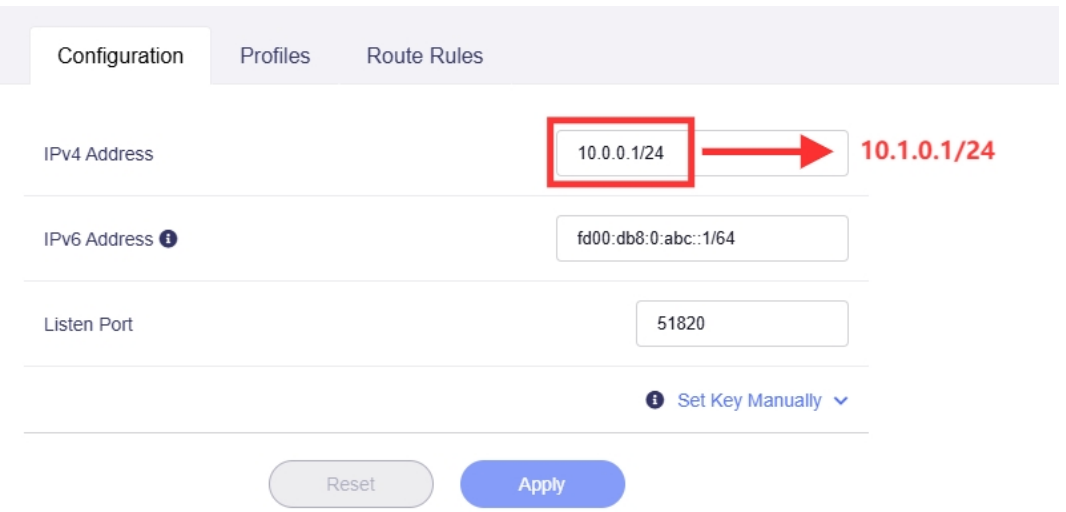
10.2.2 Pasos de configuración

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.

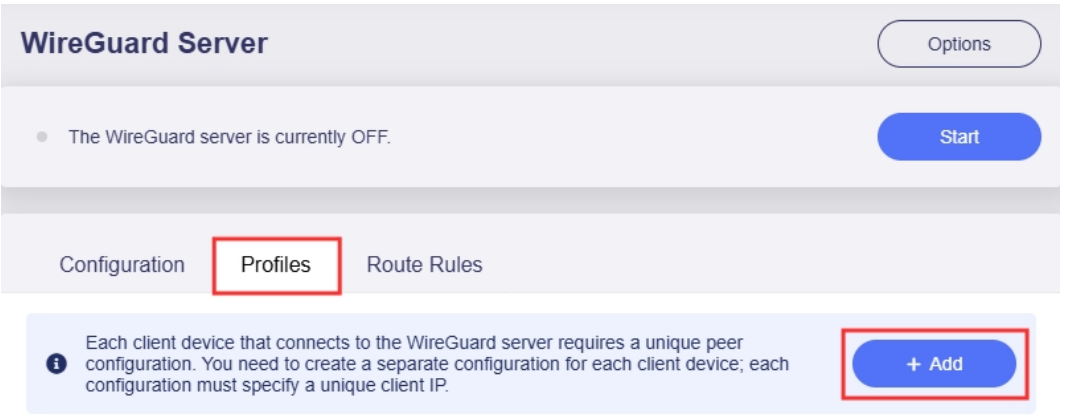


   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

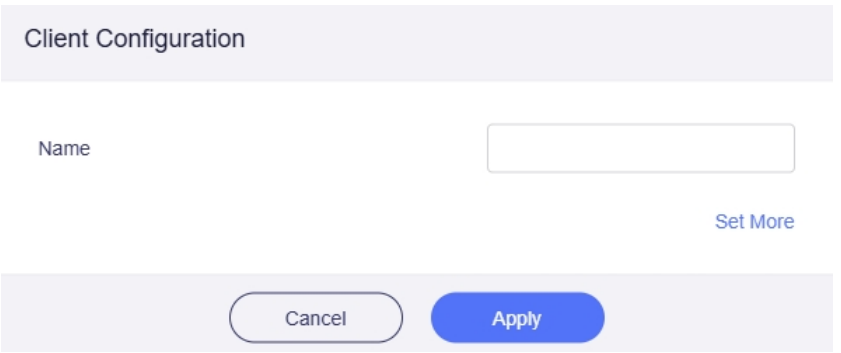


3. Agregue un perfil.

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



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



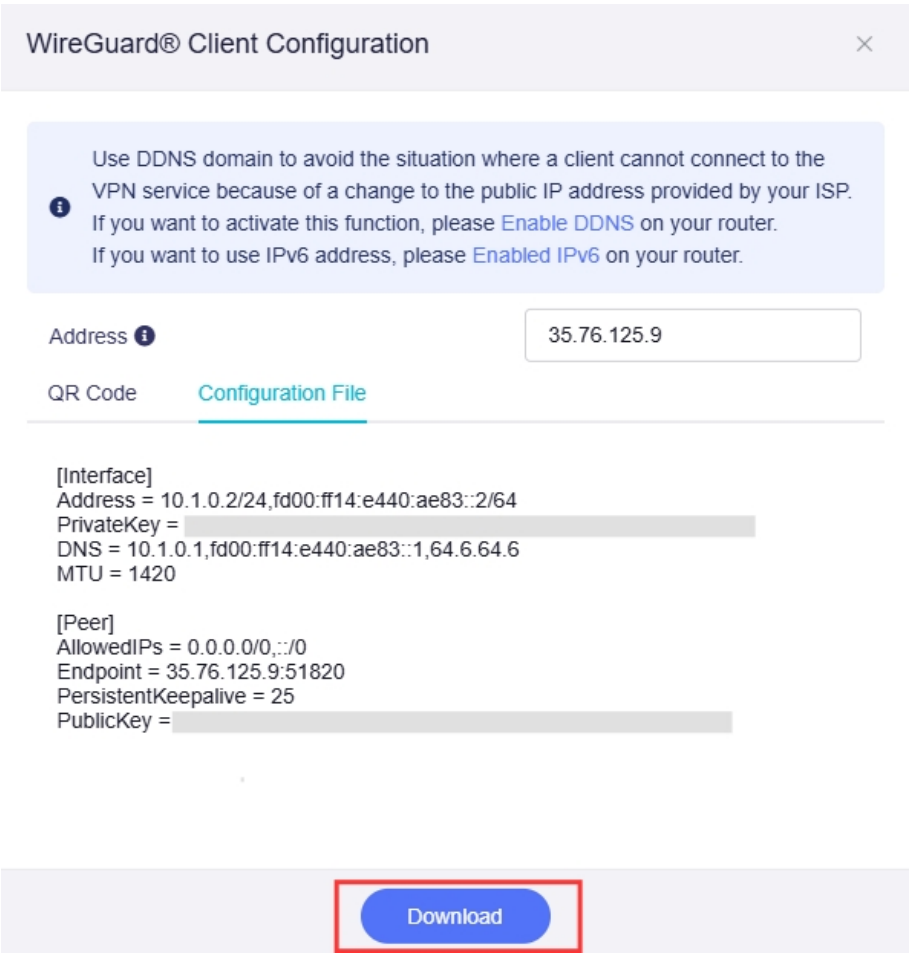
   Consejo: Si desea acceder a el Dispositivos LAN del cliente WireGuard desde su servidor WireGuard , cambie a las **Reglas de ruta** para configurar reglas de ruta. Consulte aquí para detalless.

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.

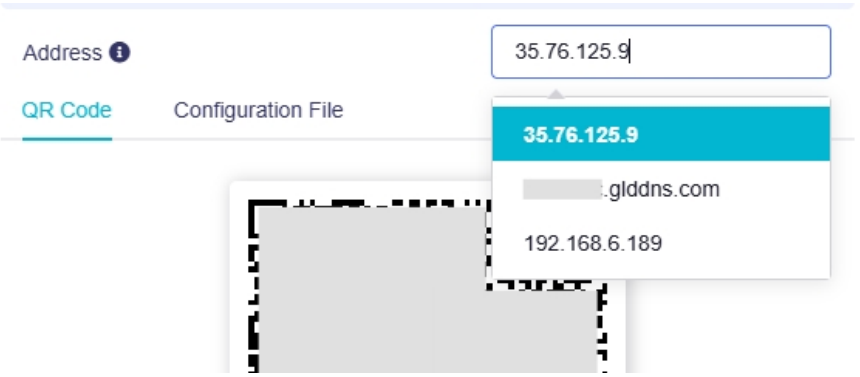
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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

- **Texto sin formato**: en formato de texto sin 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.

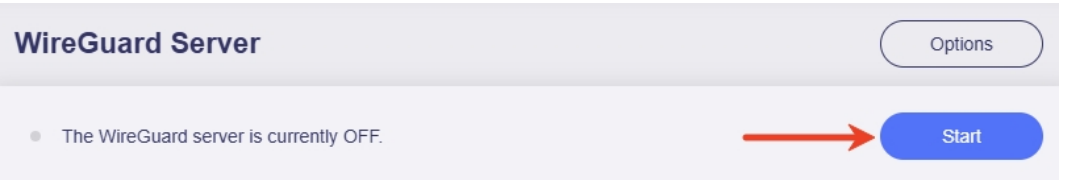


Consejos:

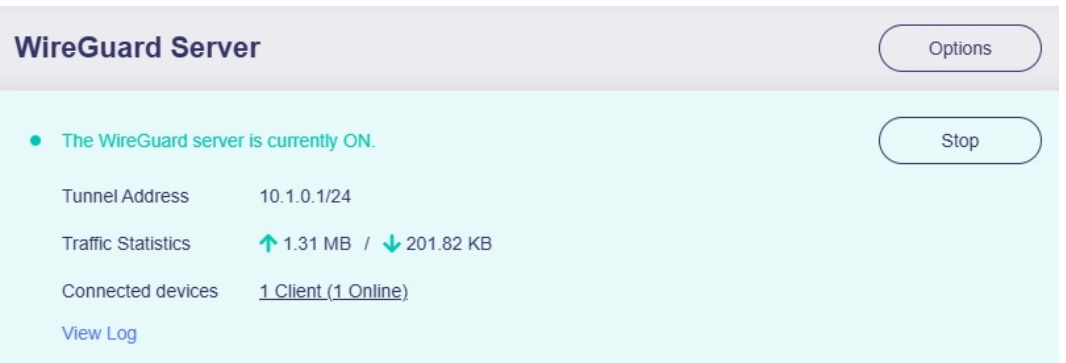
- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. You can then usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de 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 **Iniciar** en la esquina superior derecha para iniciar el servidor.



   Se muestra el servidor estado de conexión en la top. Si muestra estadísticas de tráfico de carga, descarga, y dispositivos conectados en línea, significa que el servidor WireGuard se está ejecutando.



10.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulta aquí para solucionar problemas.
- Es posible que tengas que configurar el reenvío de puertos. Consulta aquí para solucionar problemas.

- El puerto utilizado para el servidor WireGuard 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.

Capítulo 11

Configurar el cliente VPN

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

11.1 Configurar el 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.

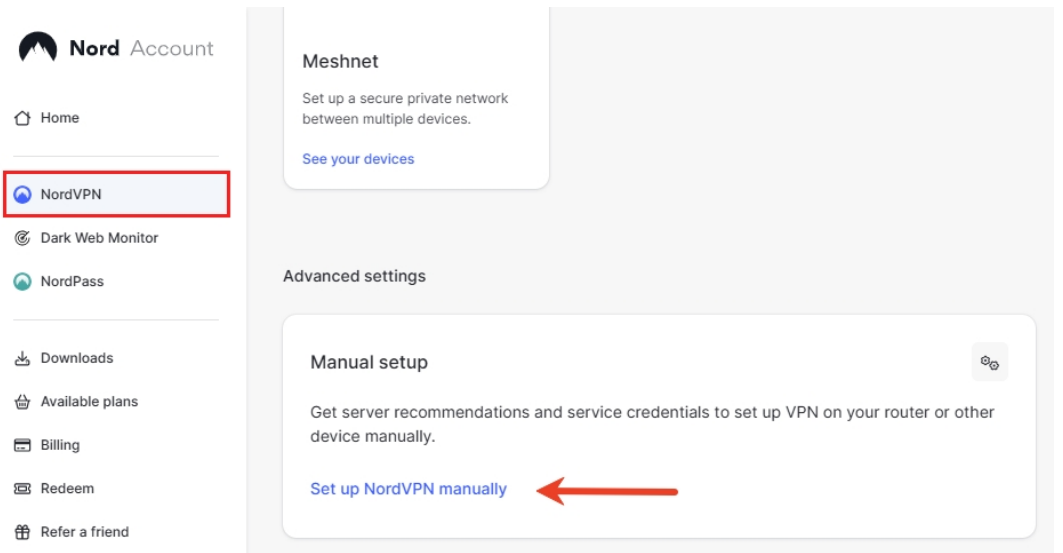
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

11.1.2 Configurar NordVPN

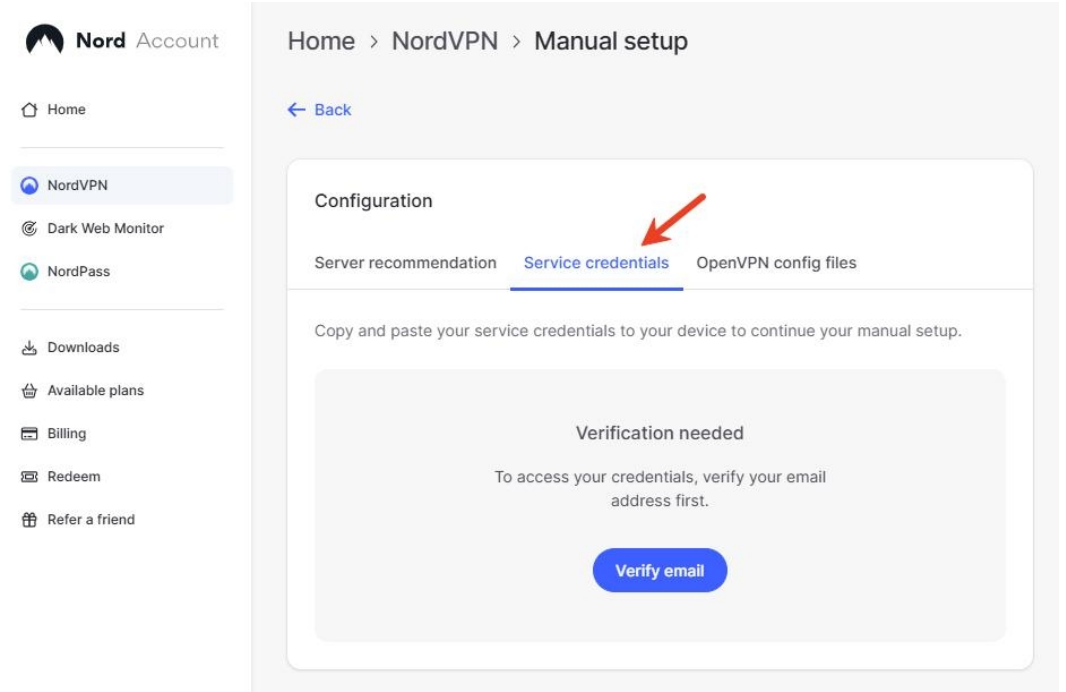
NordVPN está integrado en el web panel de administración de GL.iNet. Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet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

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

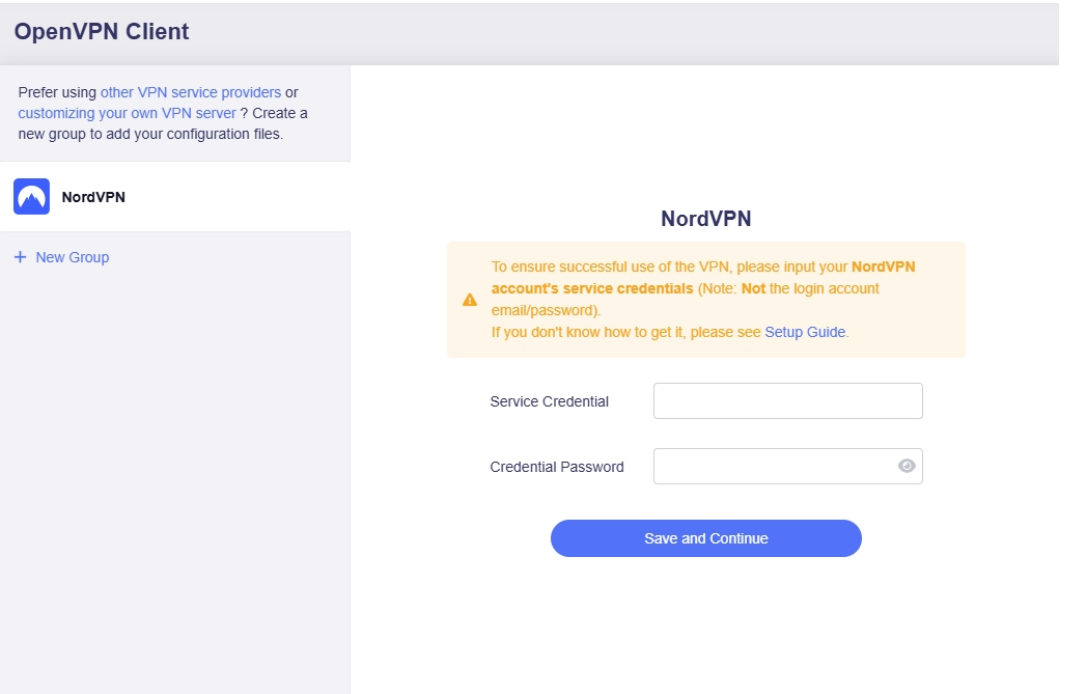
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



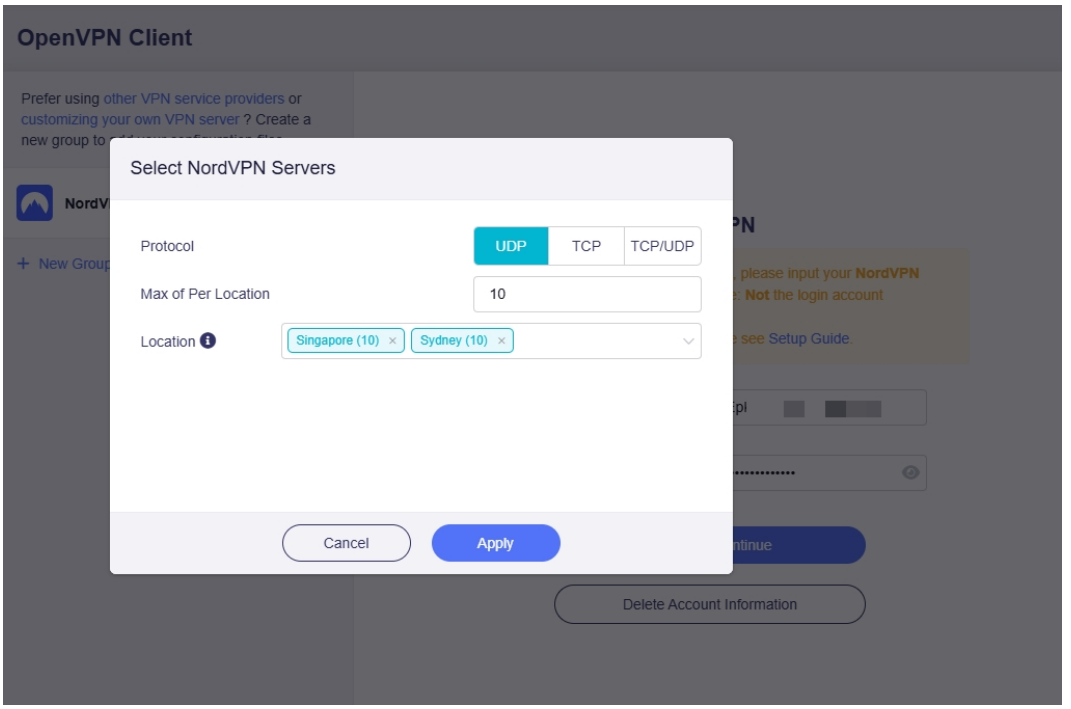
Encontrará las **credenciales de servicio**. Cópielos para usarlos más adelante.



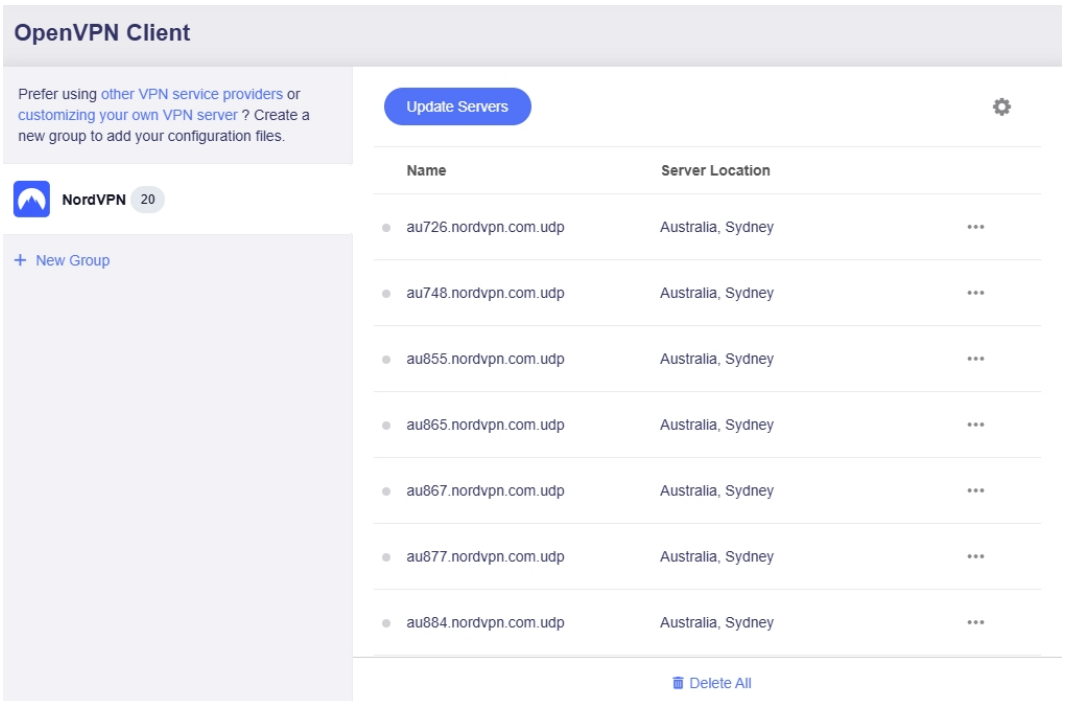
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

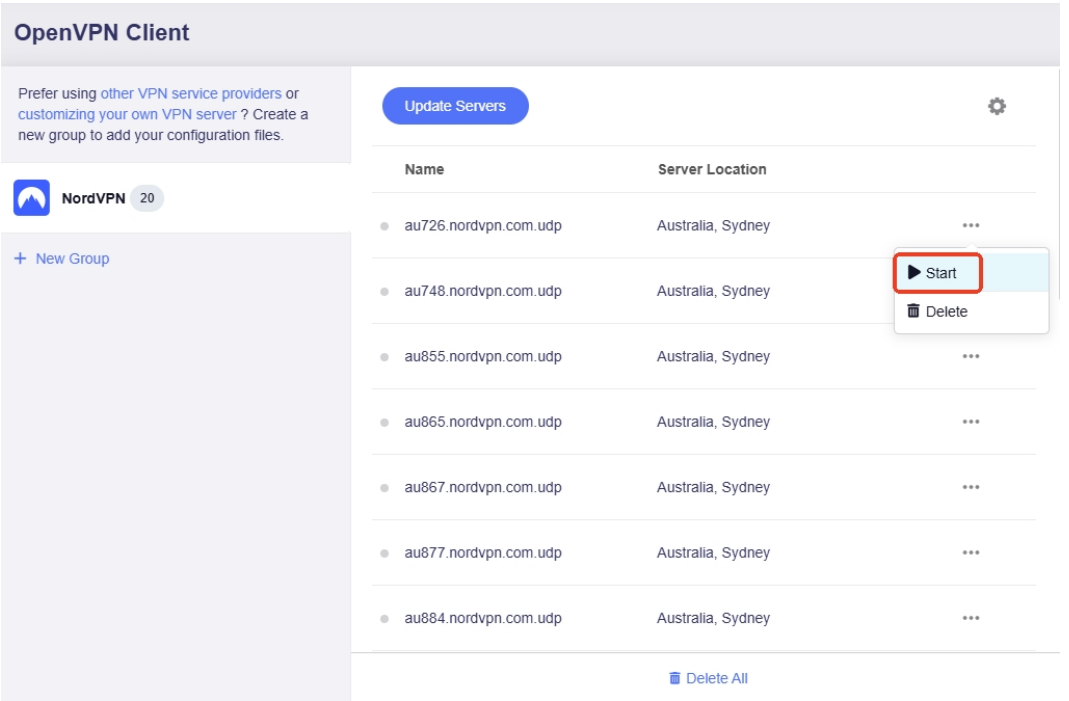


Se descargarán los archivos de configuración.

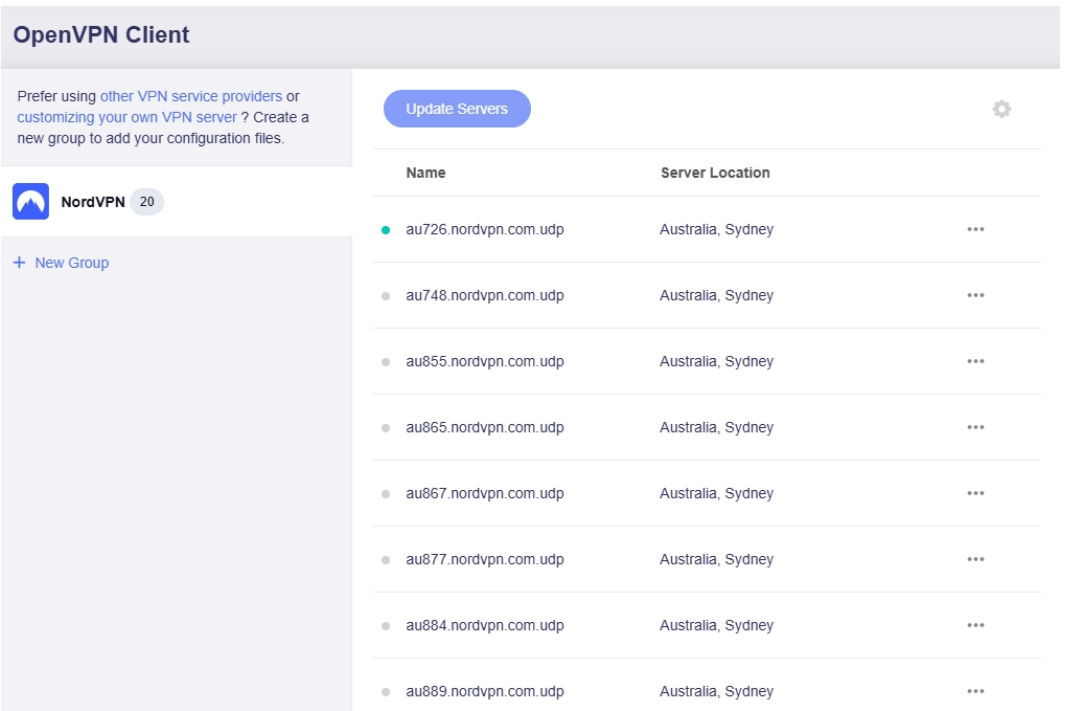


5. Iniciar una conexión.

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



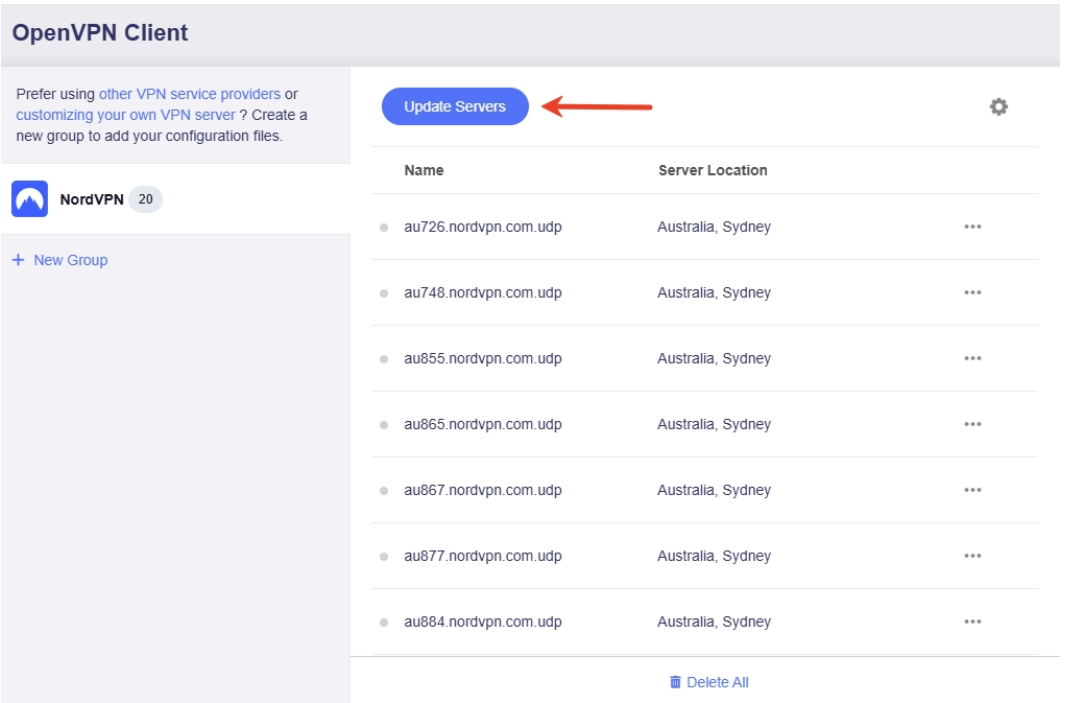
6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



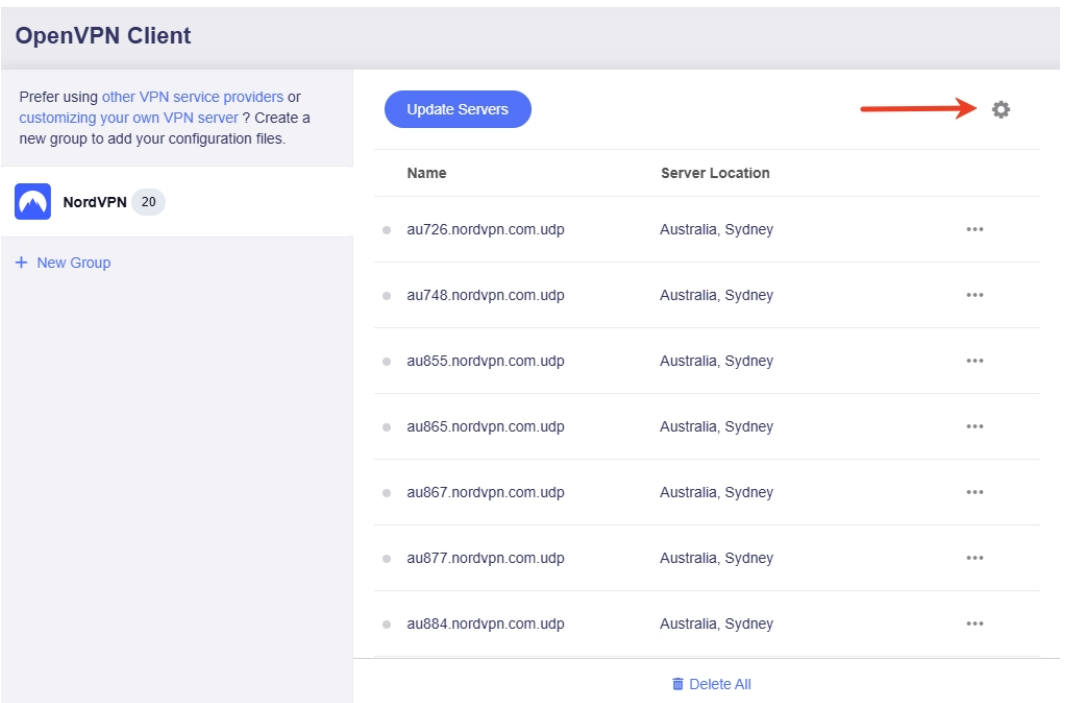
También puede consultar los detalles de la conexión VPN en **Panel de VPN**.

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.

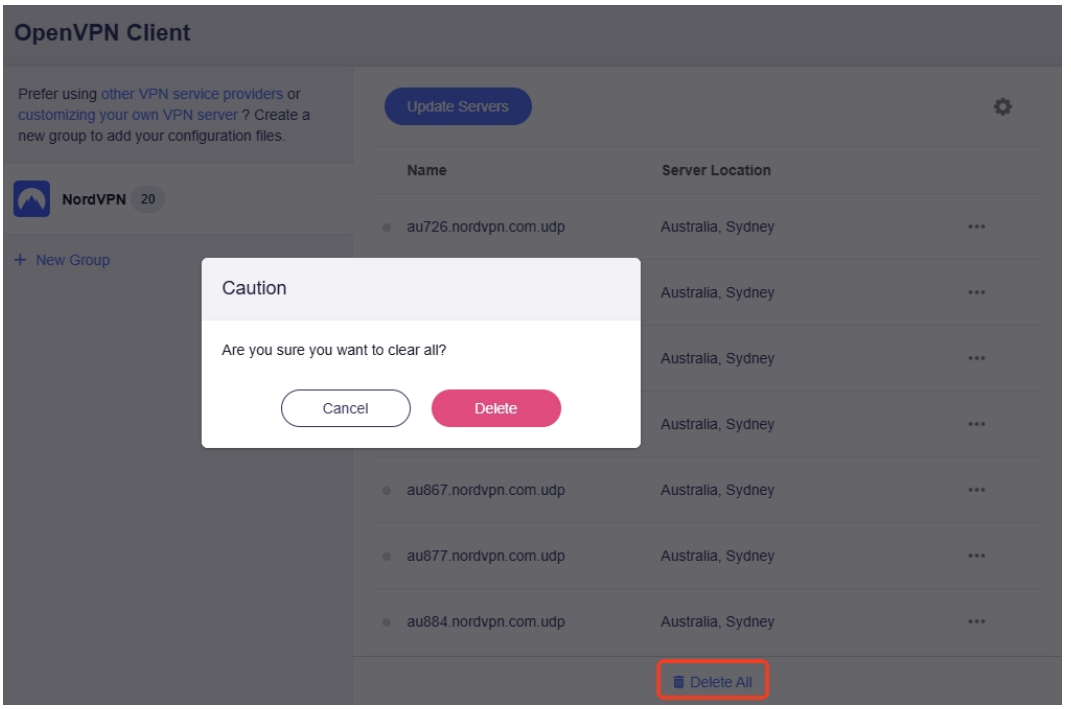


8. Edite las credenciales.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Elimine todos los archivos.

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

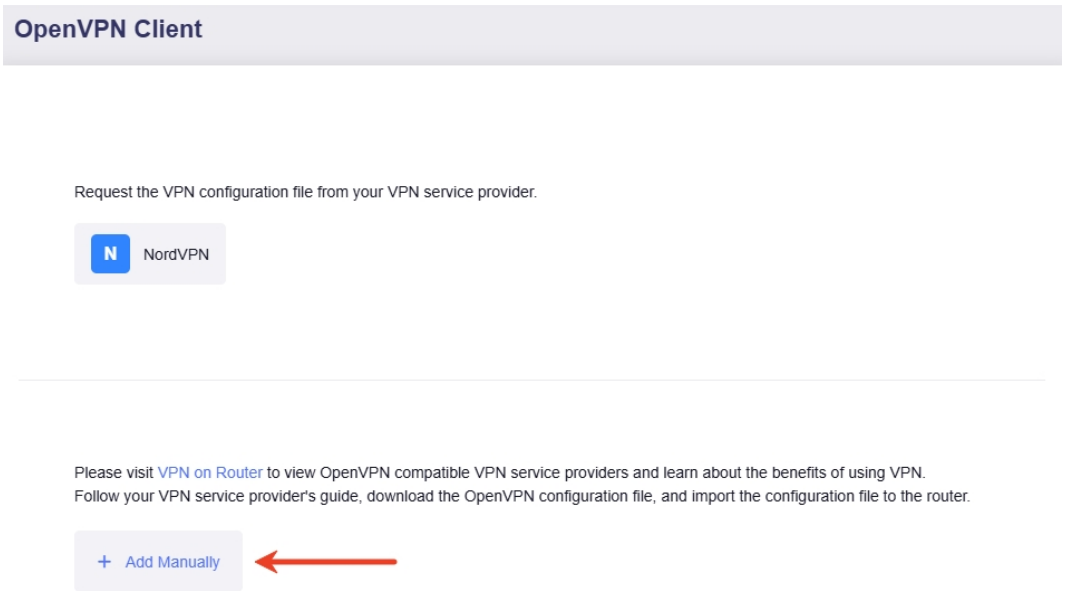


11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

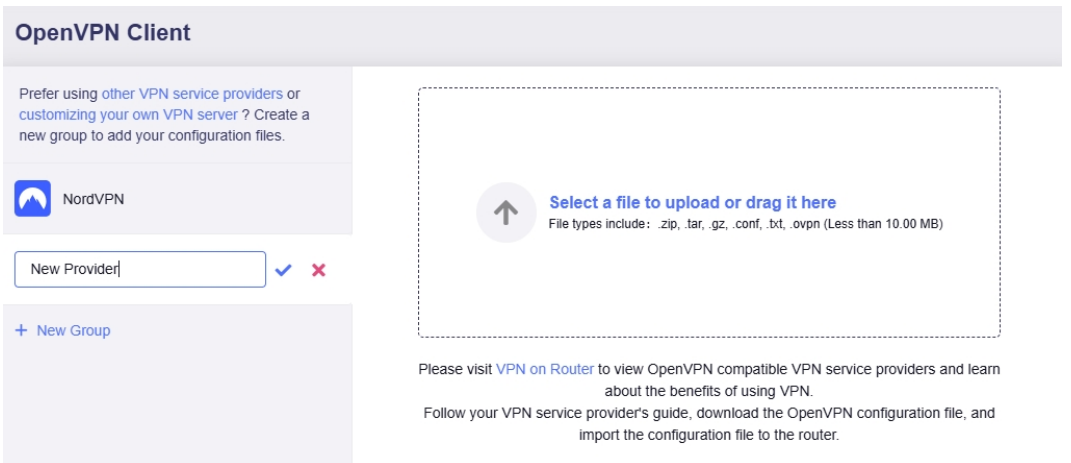
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

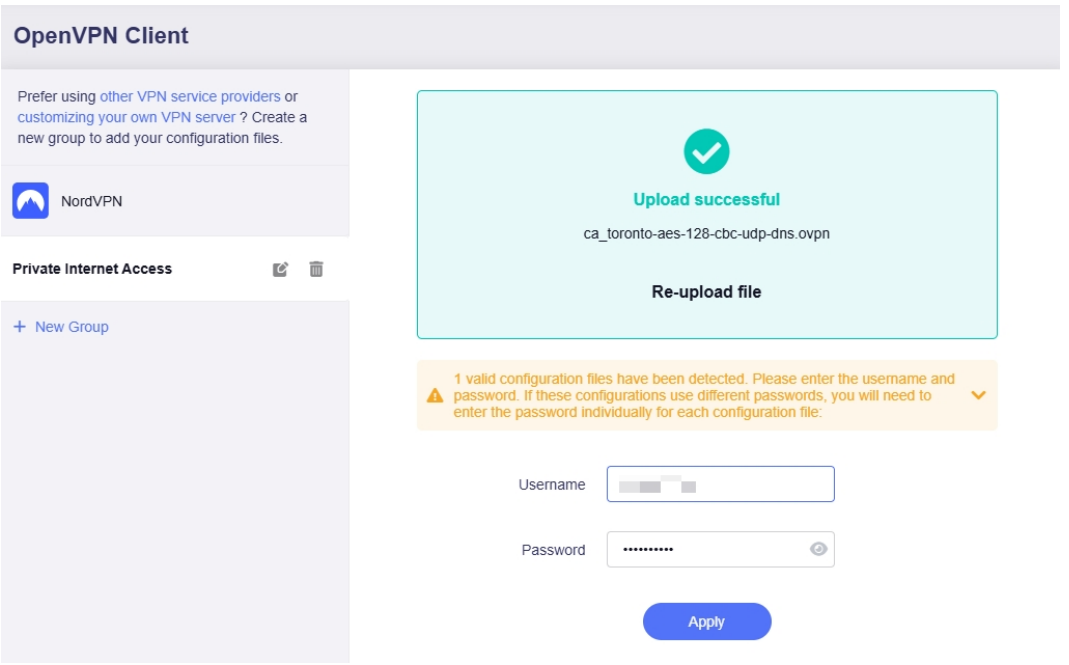
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



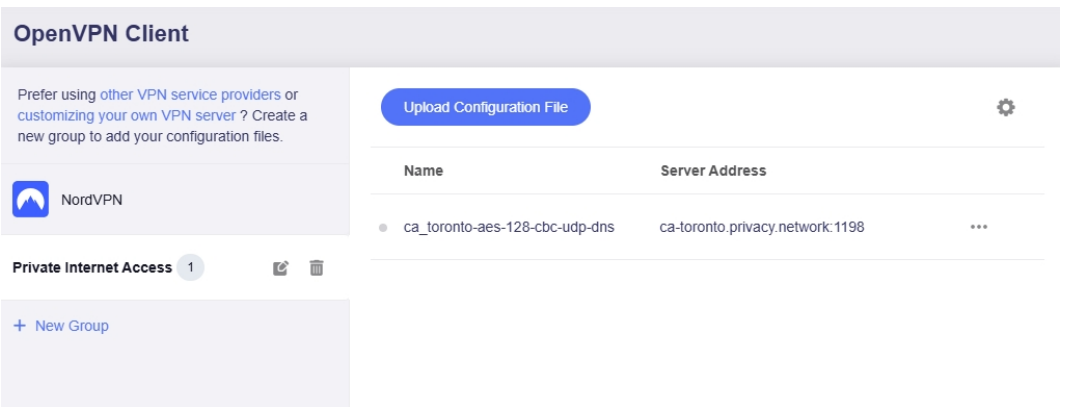
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



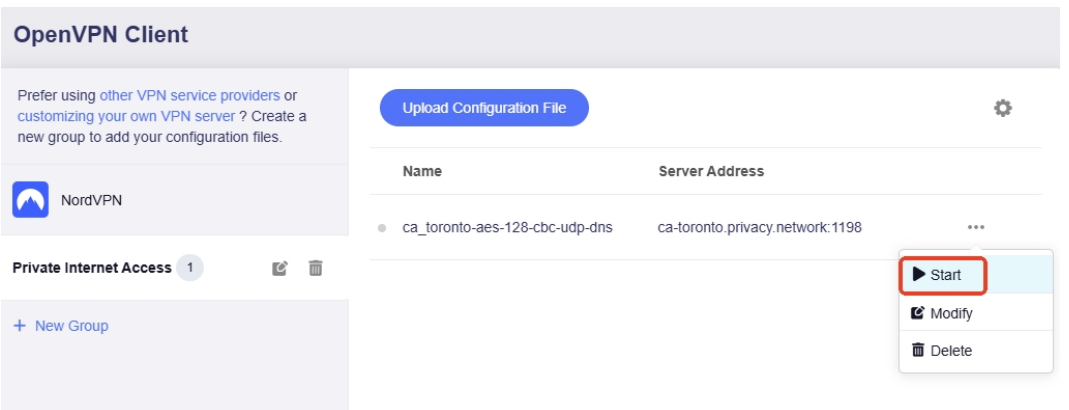
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



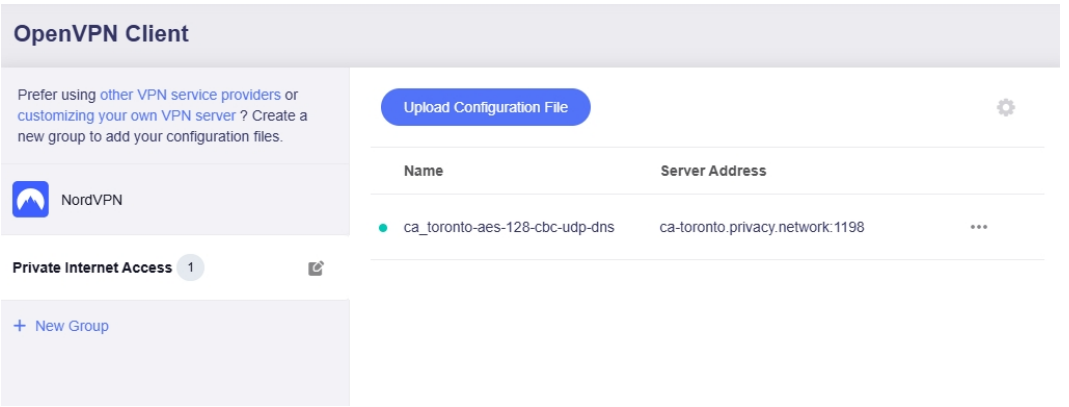
YVerá el archivo de configuración cargado.



5. Haga clic en el ícono de tres puntos a la derecha 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

Puede configurar WireGuard Client a través de la aplicación móvil GL.iNet o el panel de administración web.

- 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.

11.2.1 Preparación

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

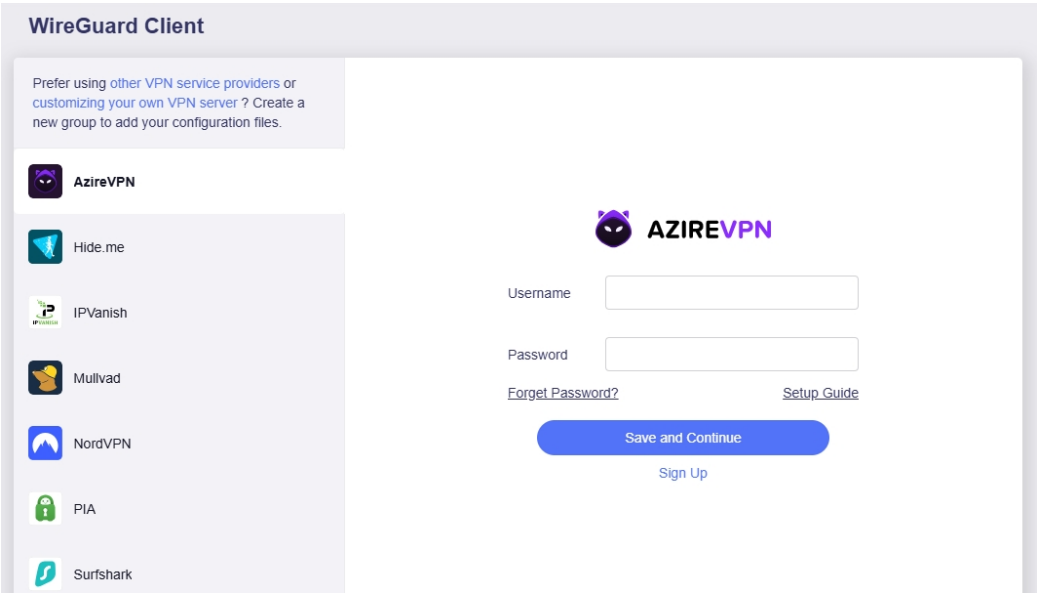
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- 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)

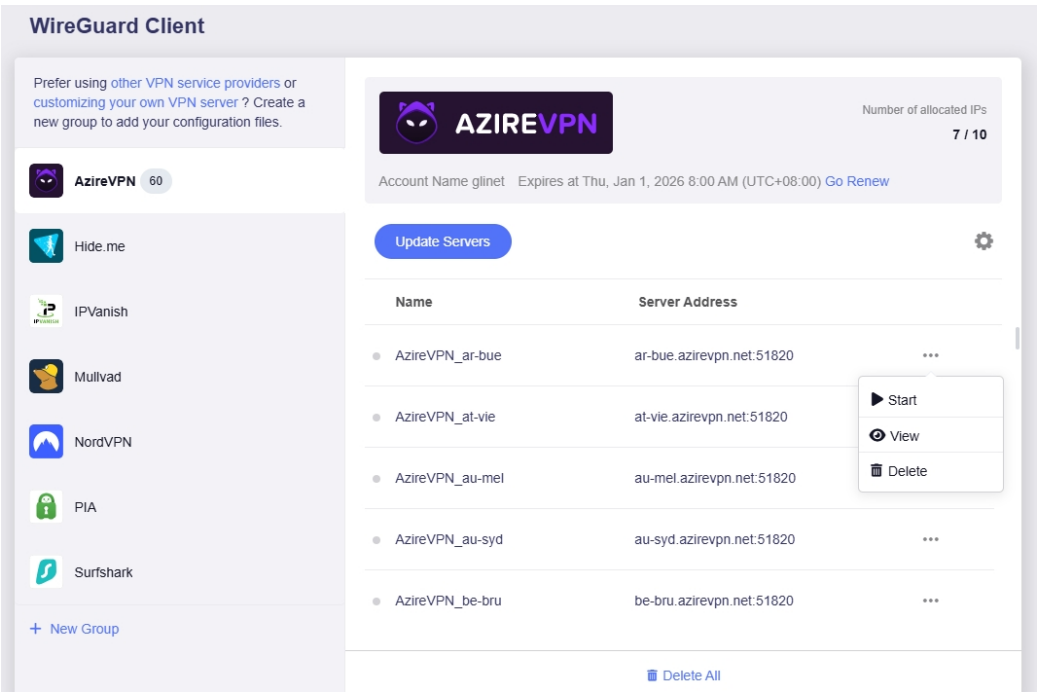
11.2.2 Configurar AzireVPN

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

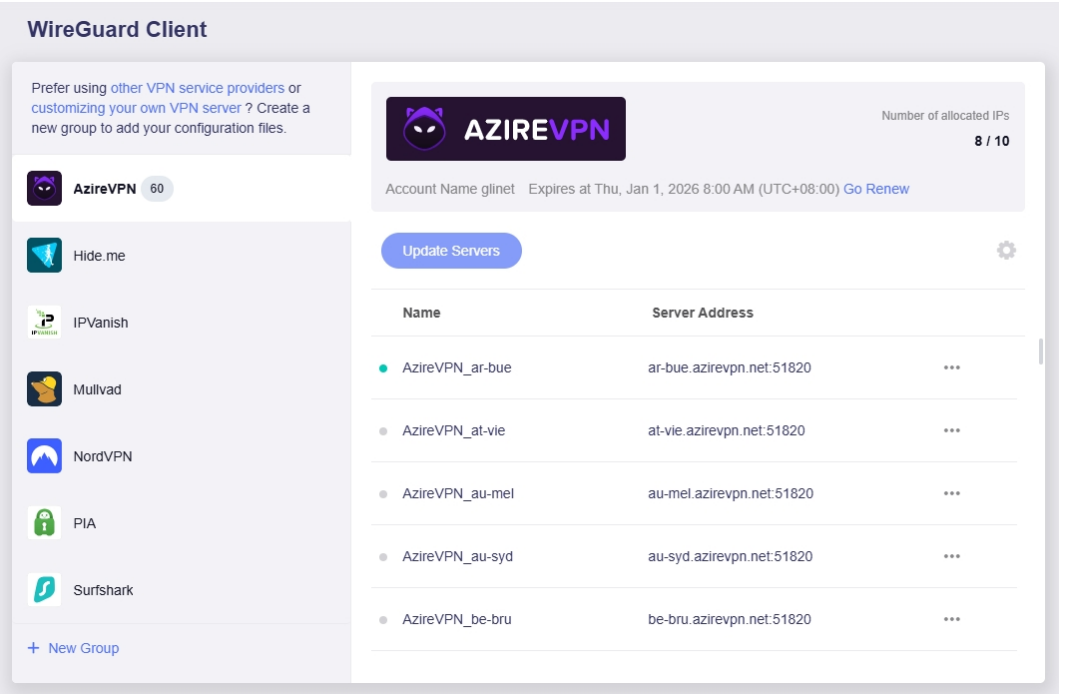
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



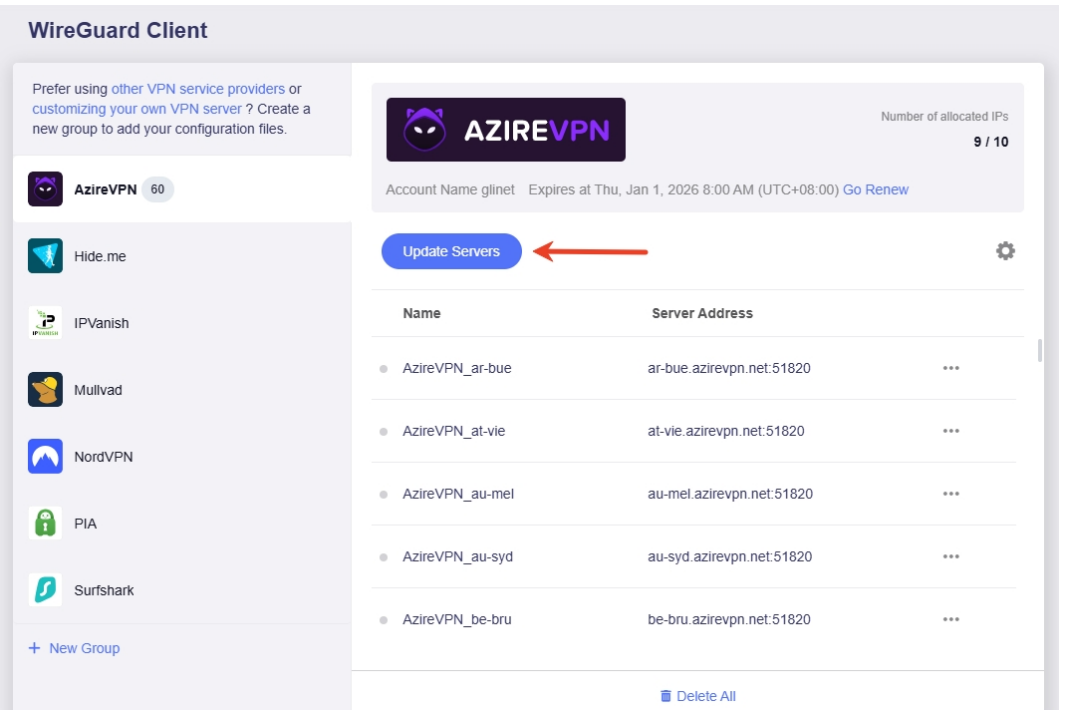
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

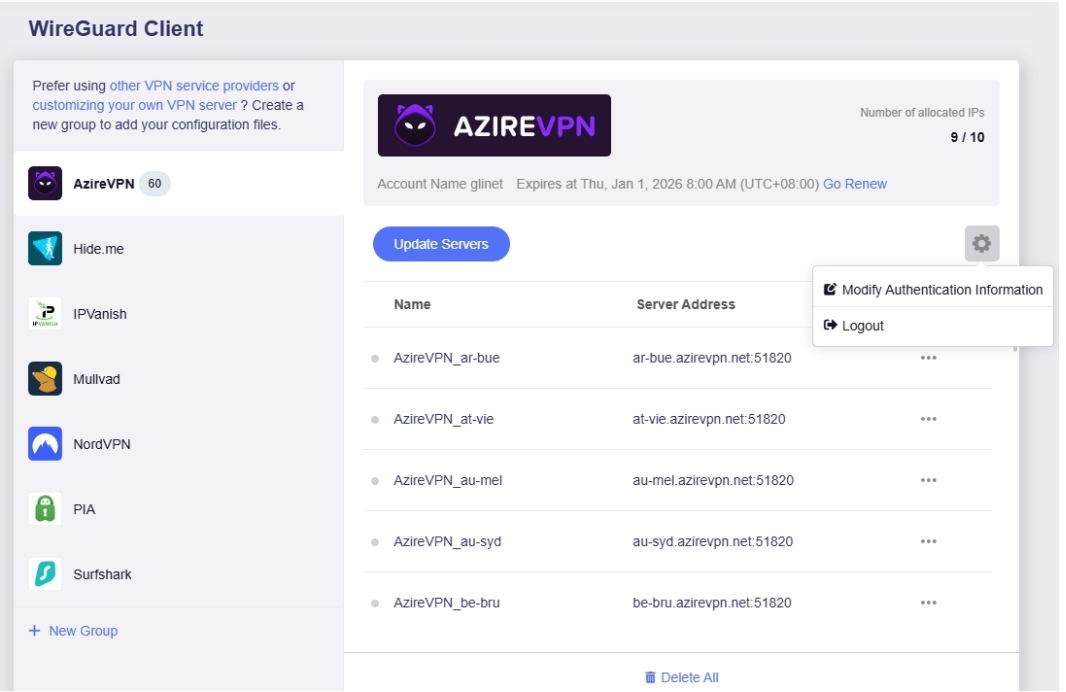
5. Actualizar servidores.

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



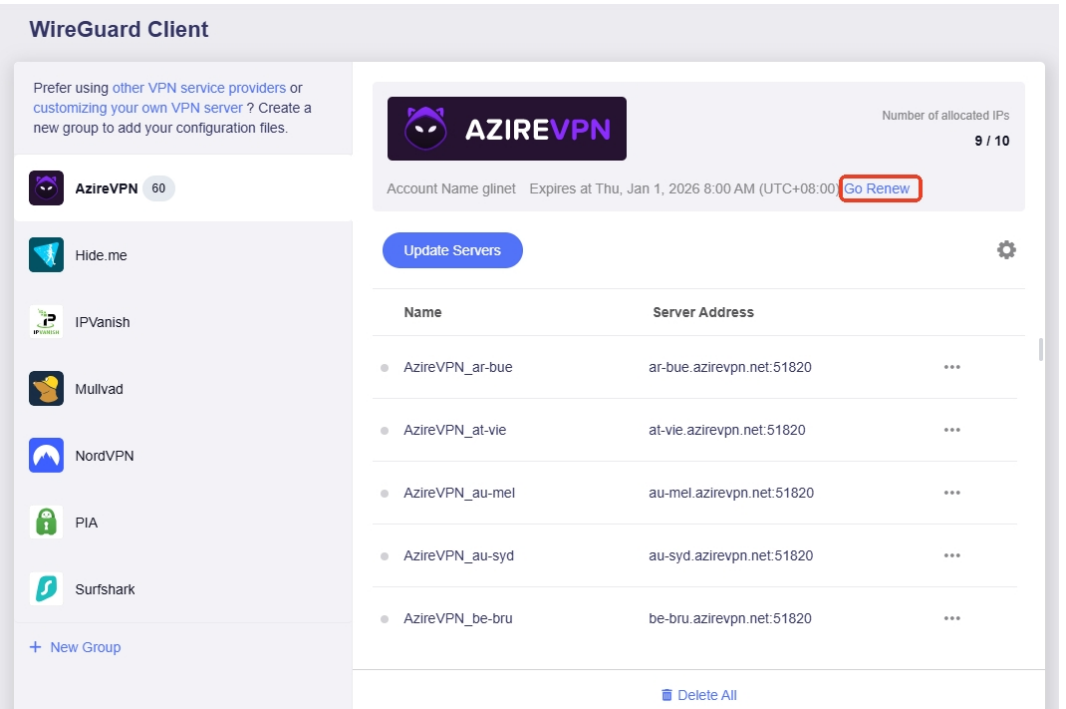
6. Edite las credenciales o cierre la sesión.

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



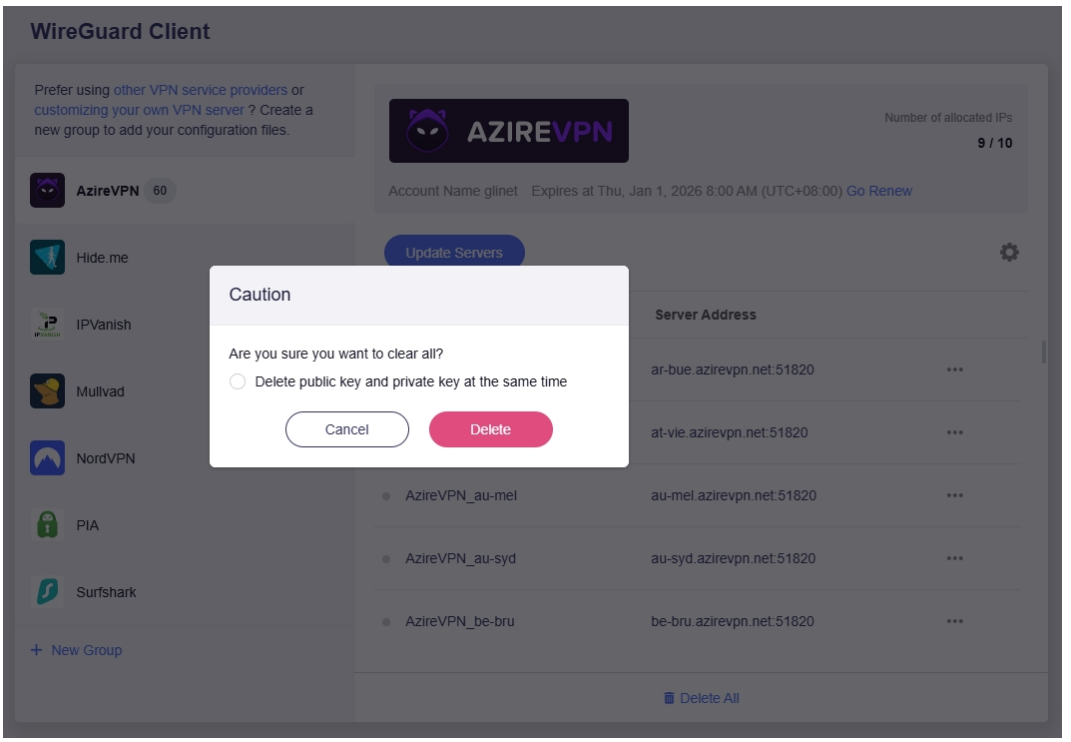
7. Vaya a renovar.

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



8. Eliminar todos los archivos.

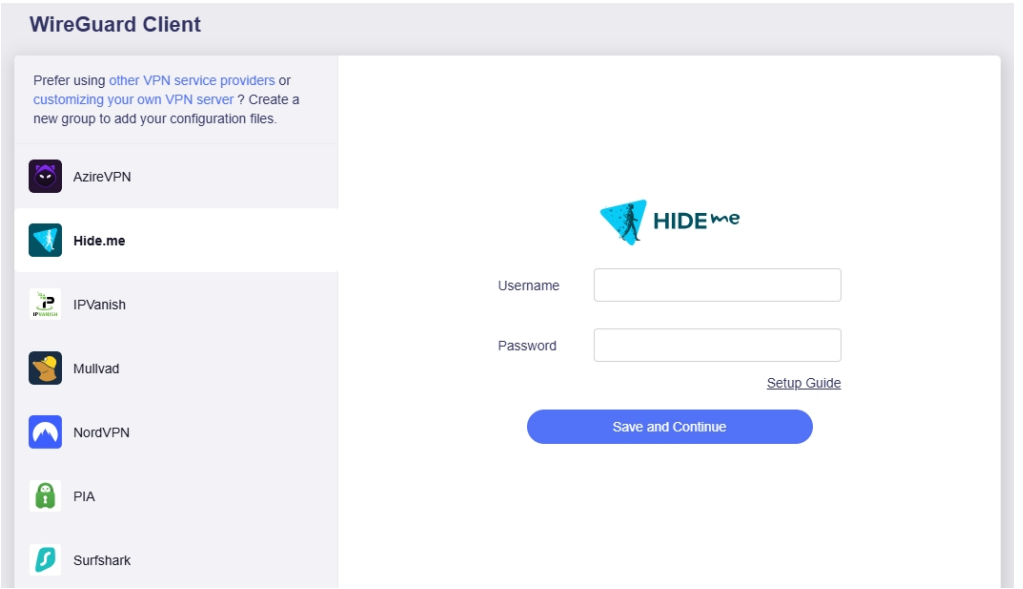
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



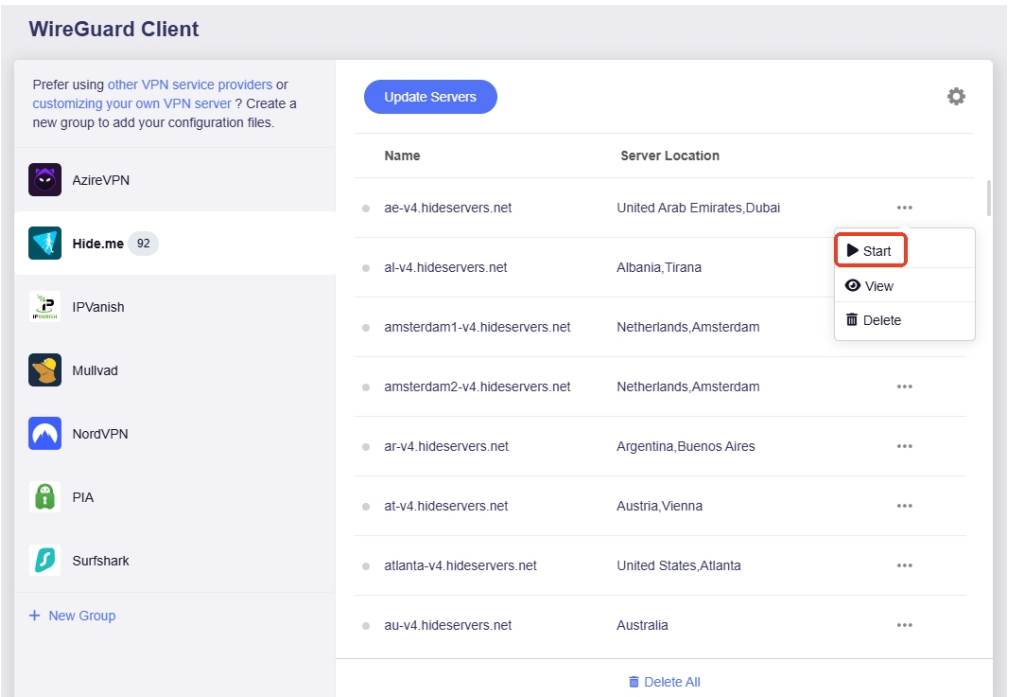
11.2.3 Configurar Hide.me

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

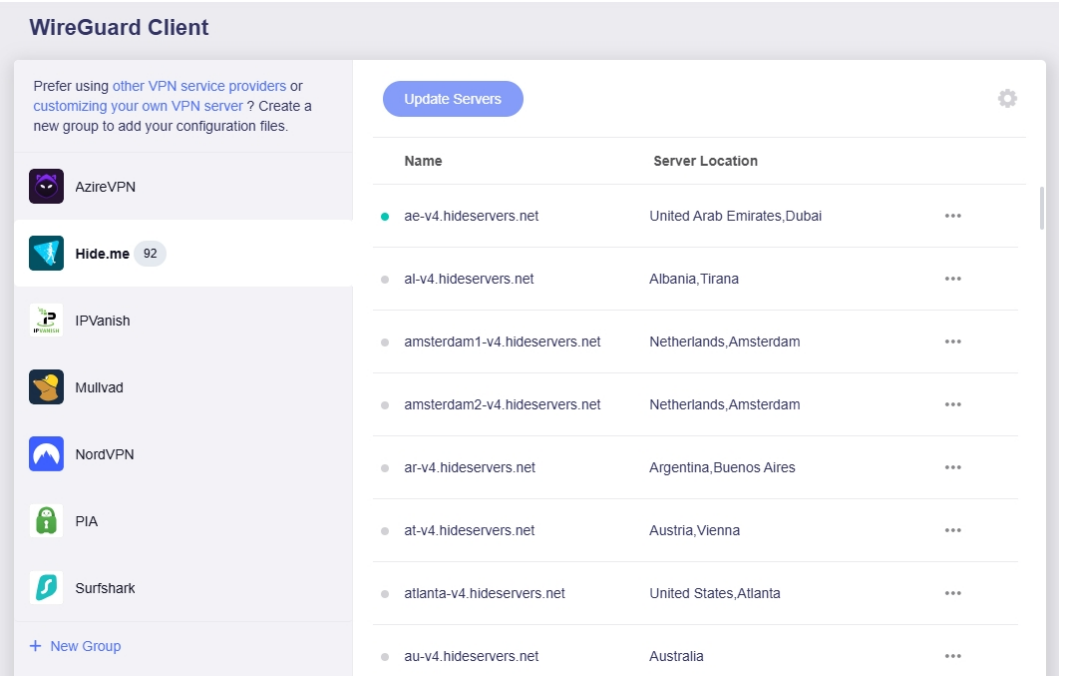
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Hide.me**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



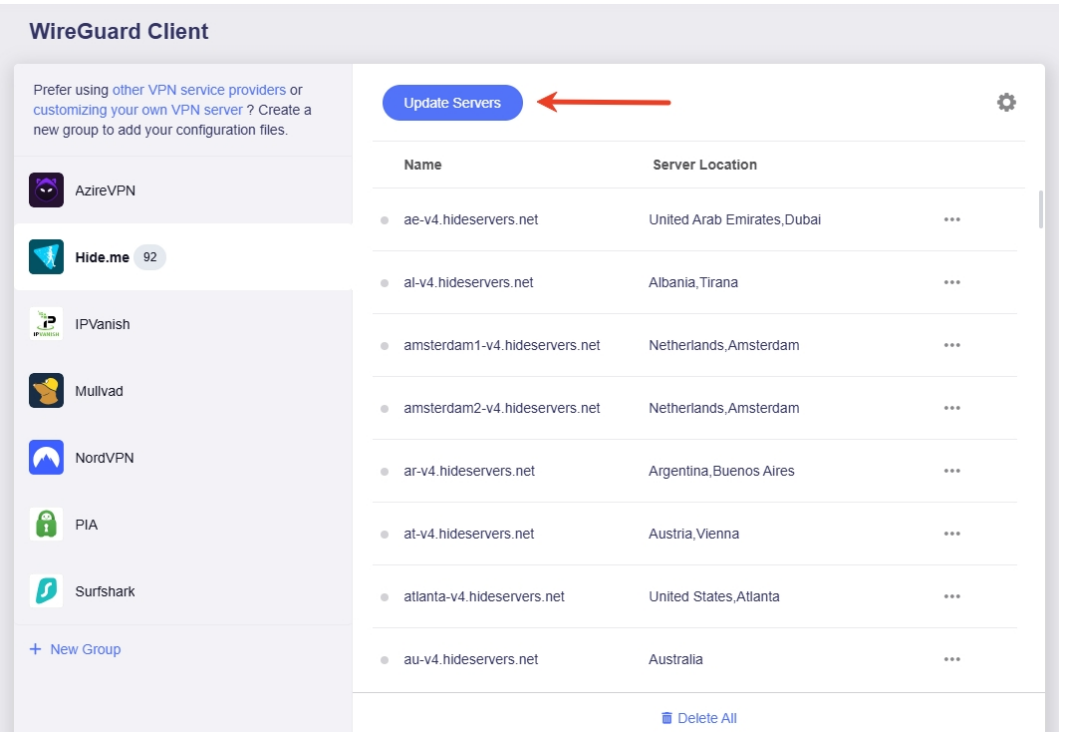
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Tú puedes también verifique los detalles de la conexión VPN en **Panel de VPN**.

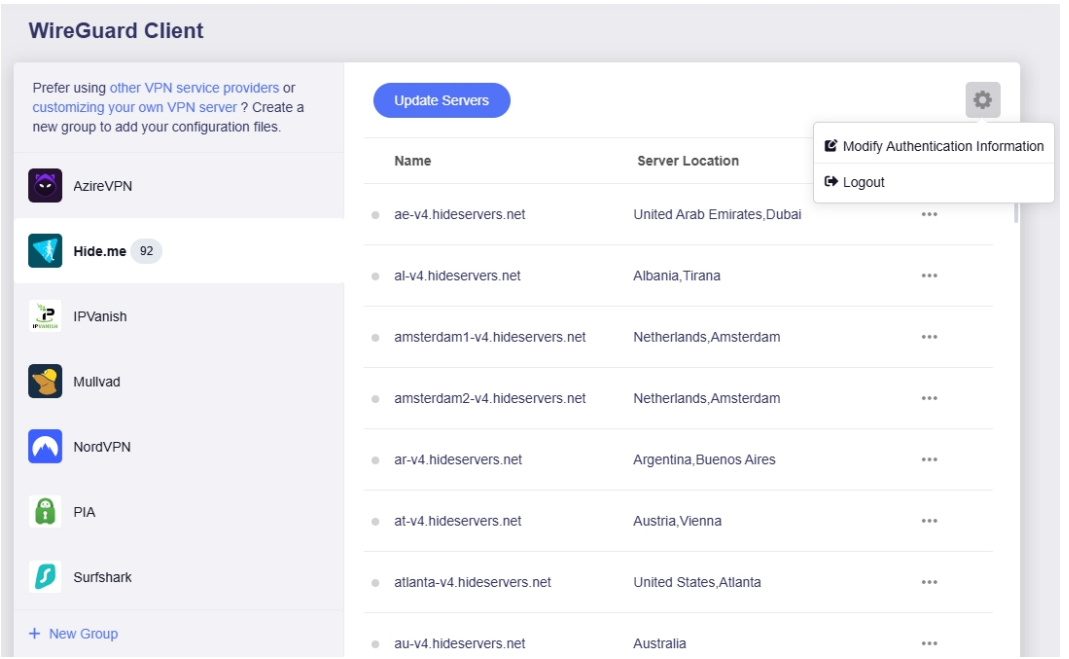
5. Actualizar servidores.

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.



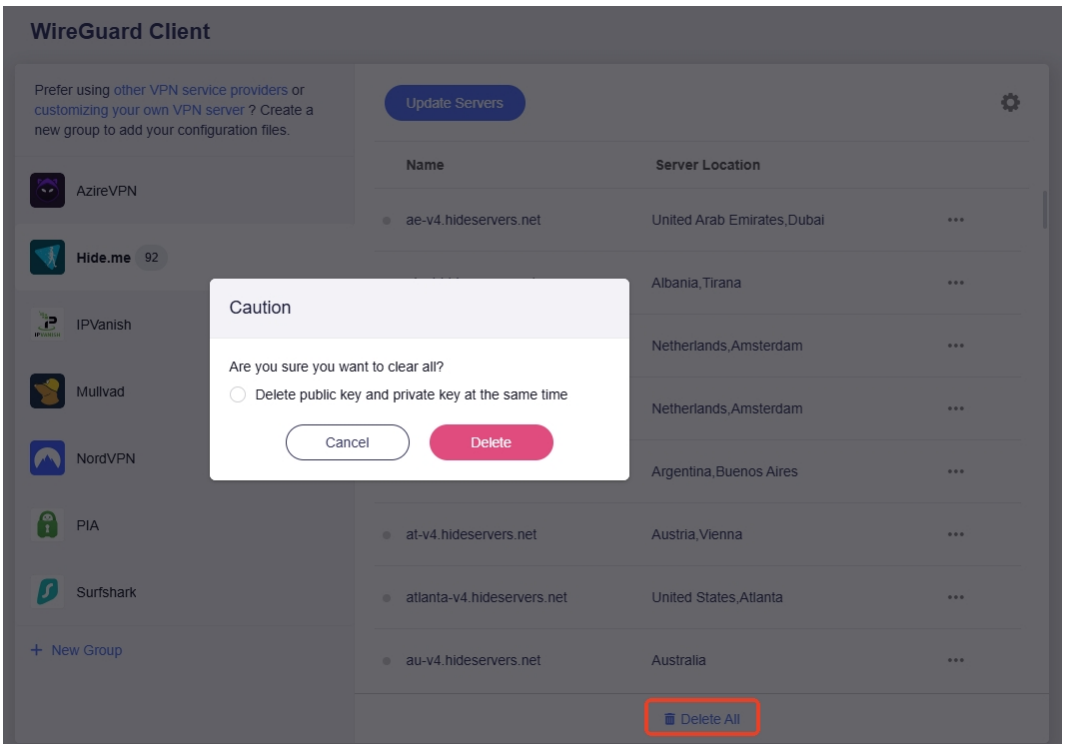
6. Editar credenciales o cerrar sesión.

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



7. Eliminar todos los archivos.

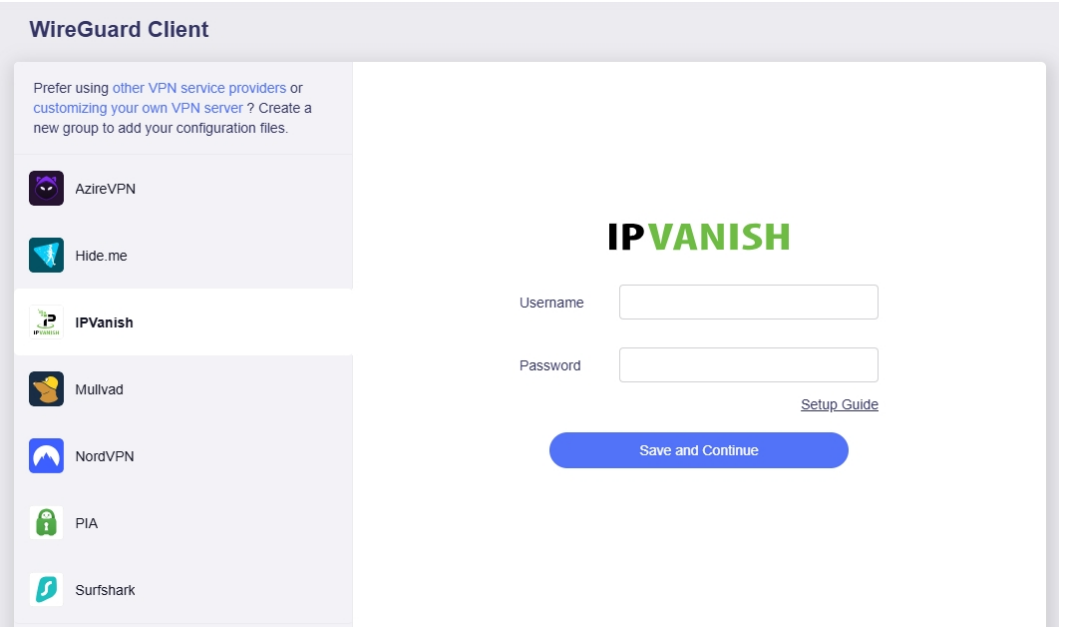
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



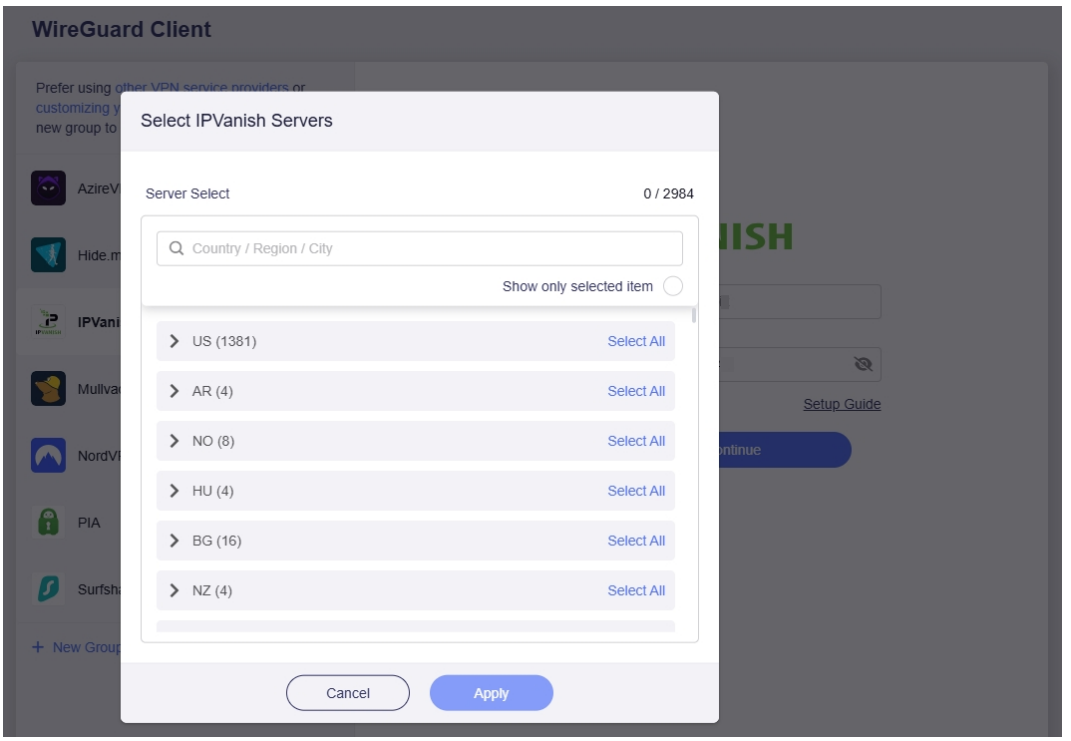
11.2.4 Configurar IPVanish

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

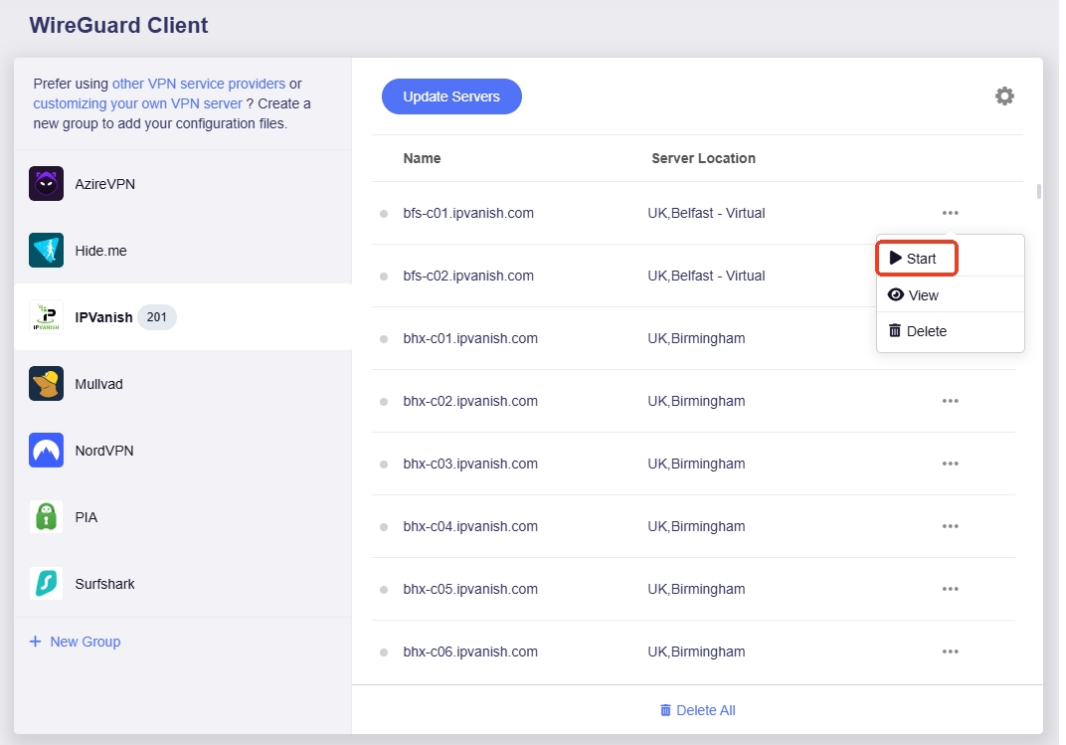
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **IPVanish**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



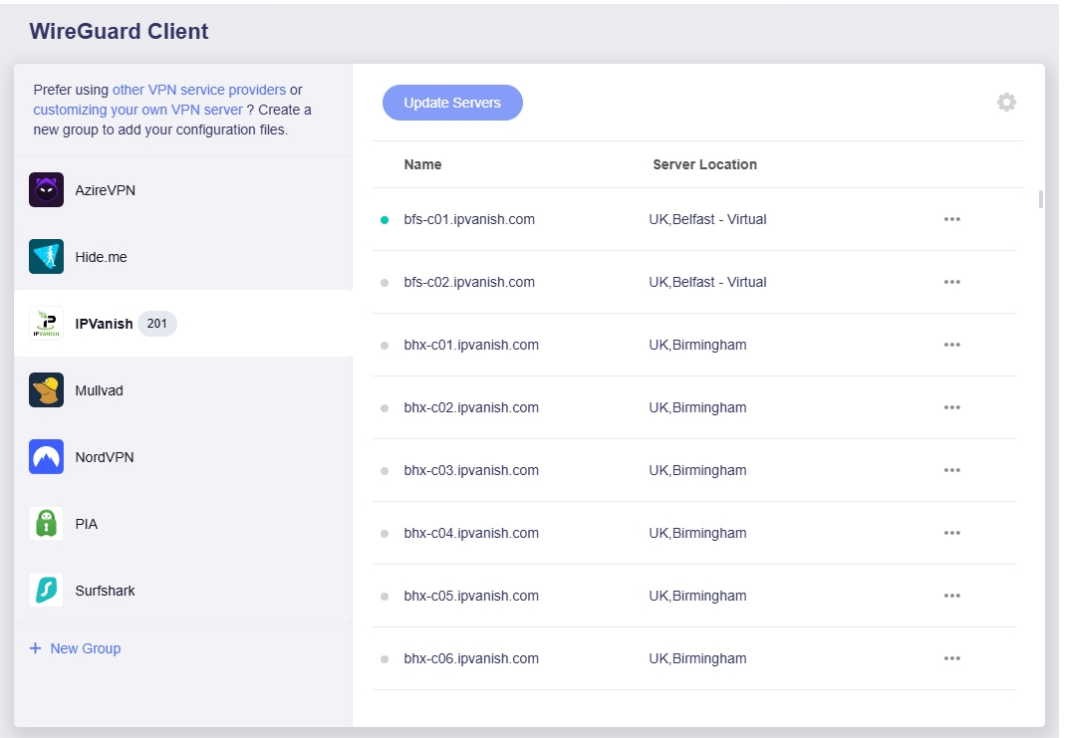
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



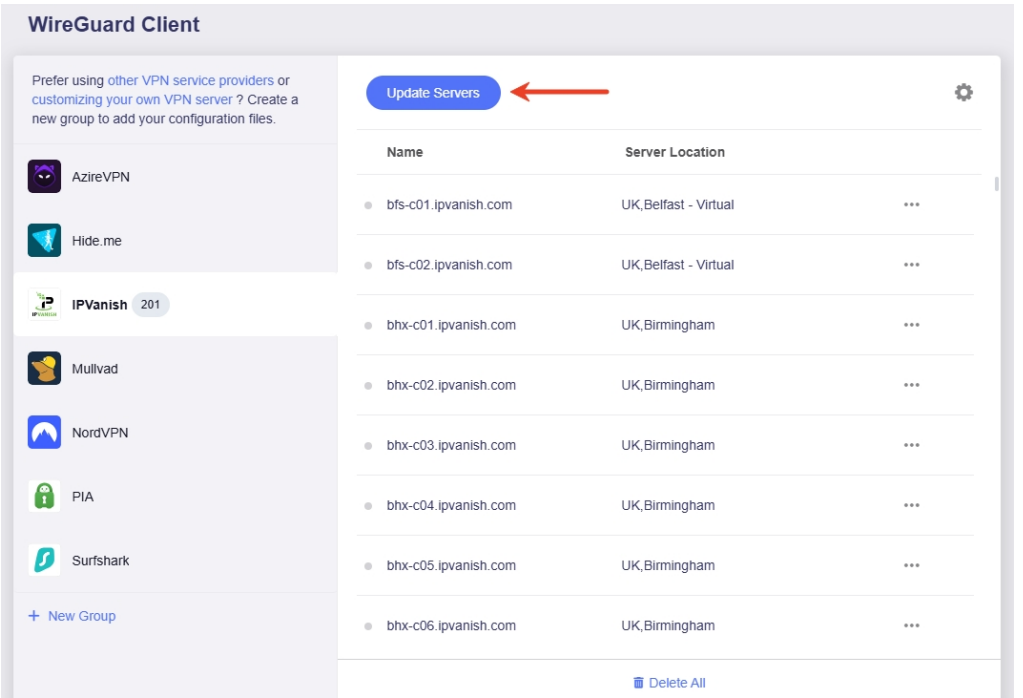
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

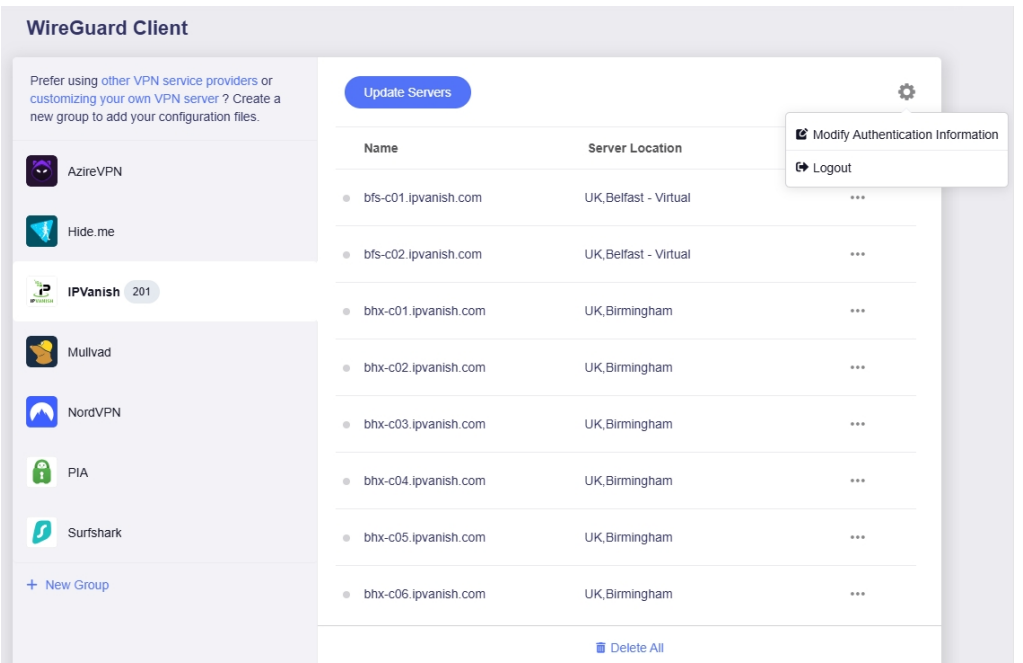
6. Actualizar servidores.

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



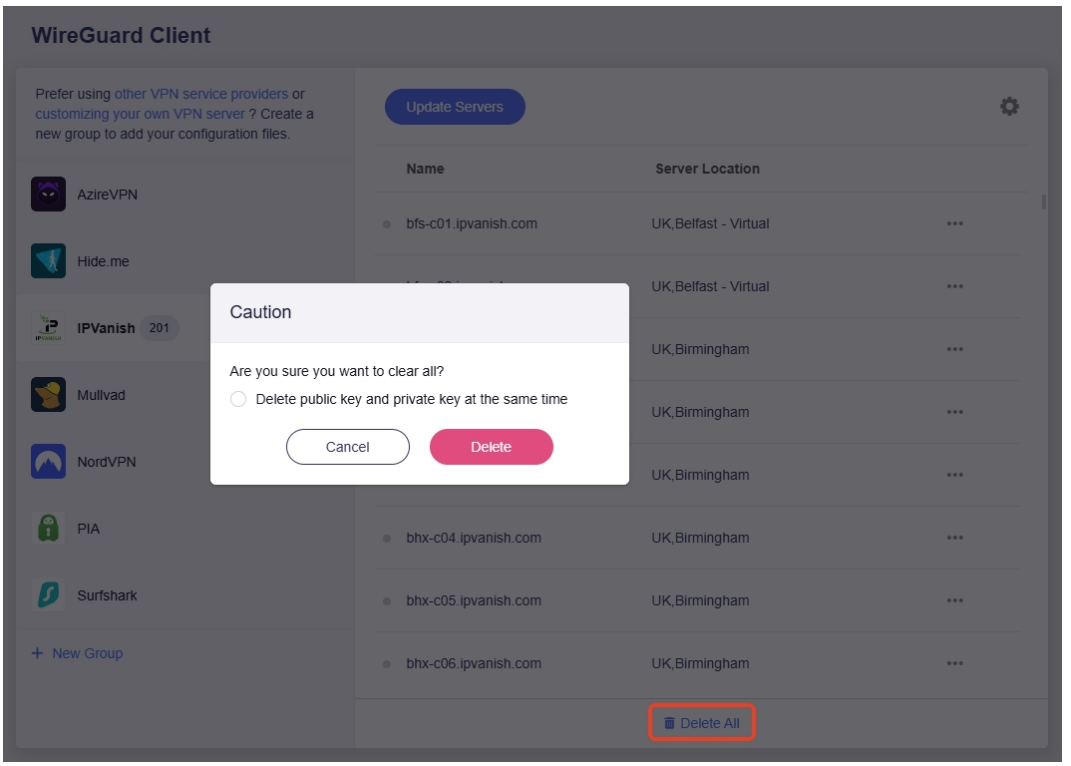
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

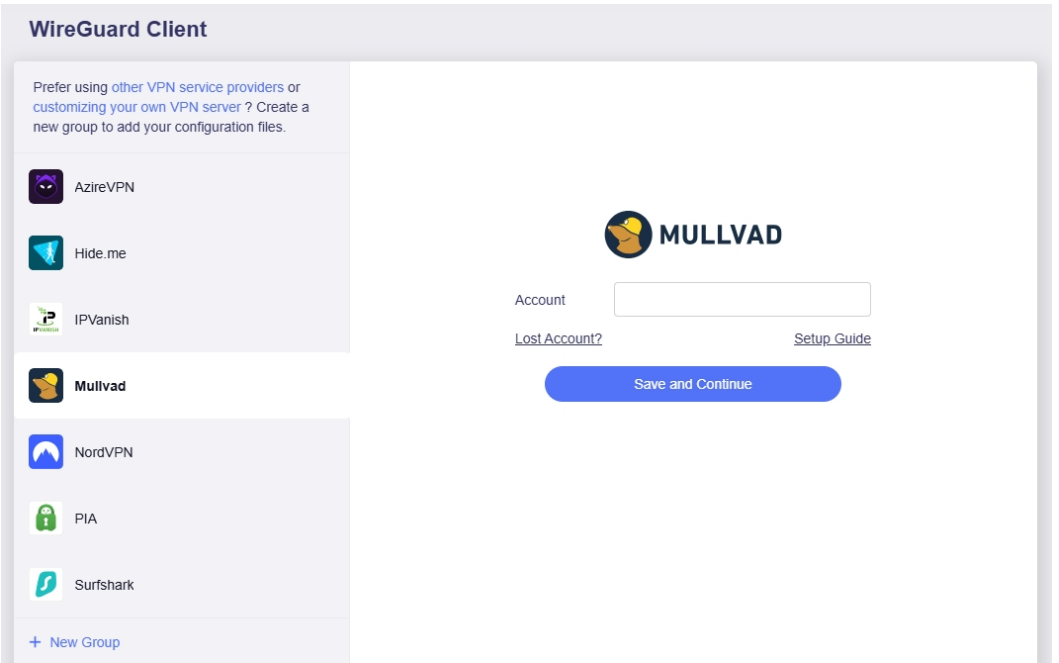
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



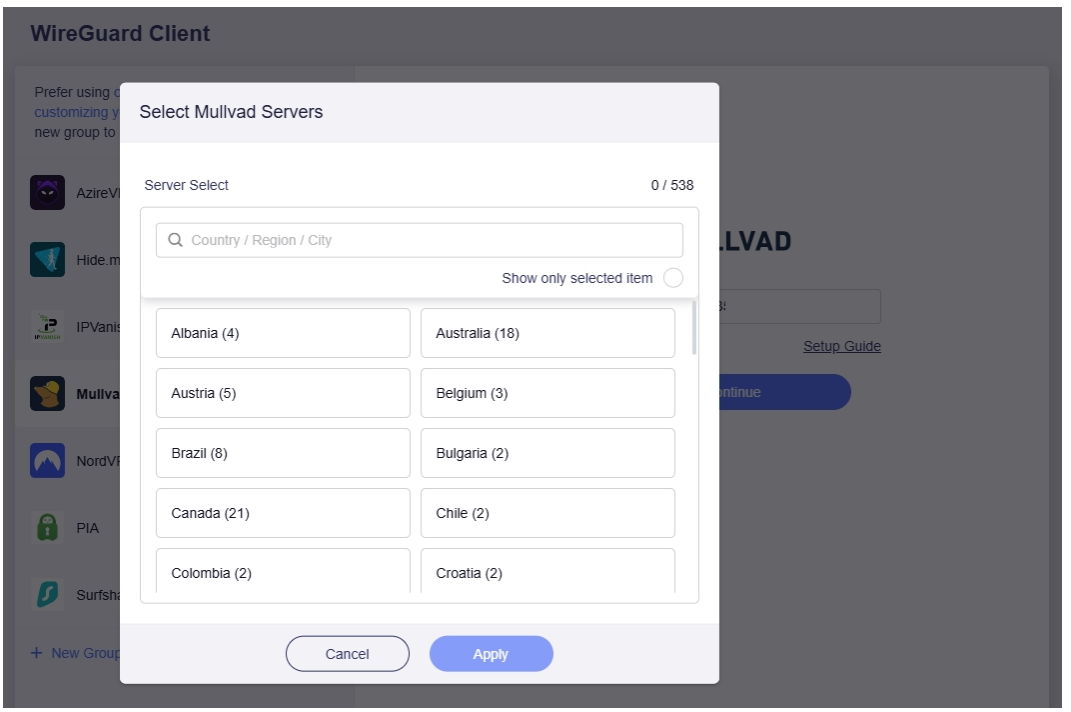
11.2.5 Configurar Mullvad

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

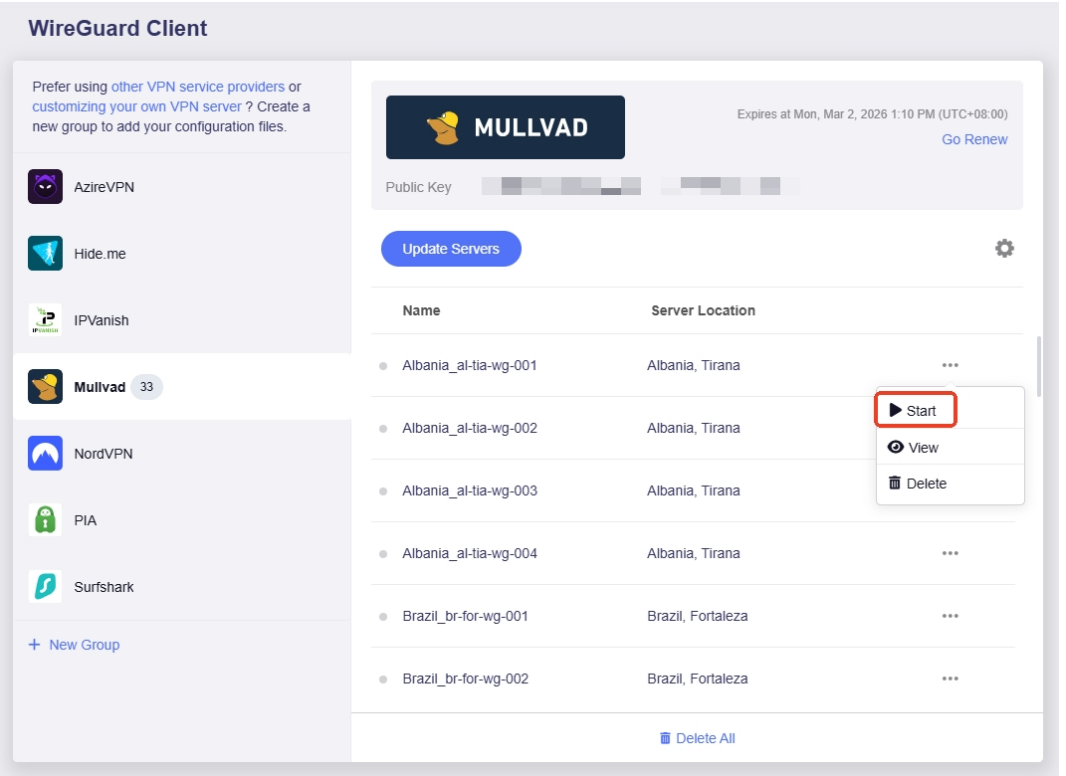
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



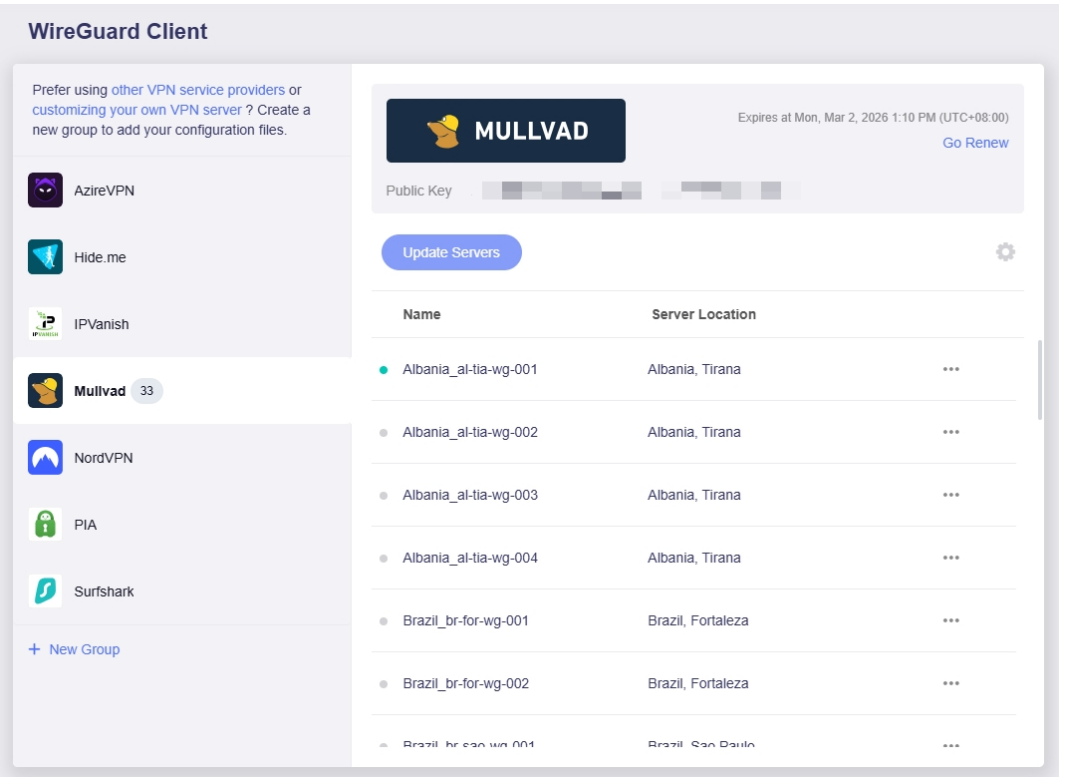
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



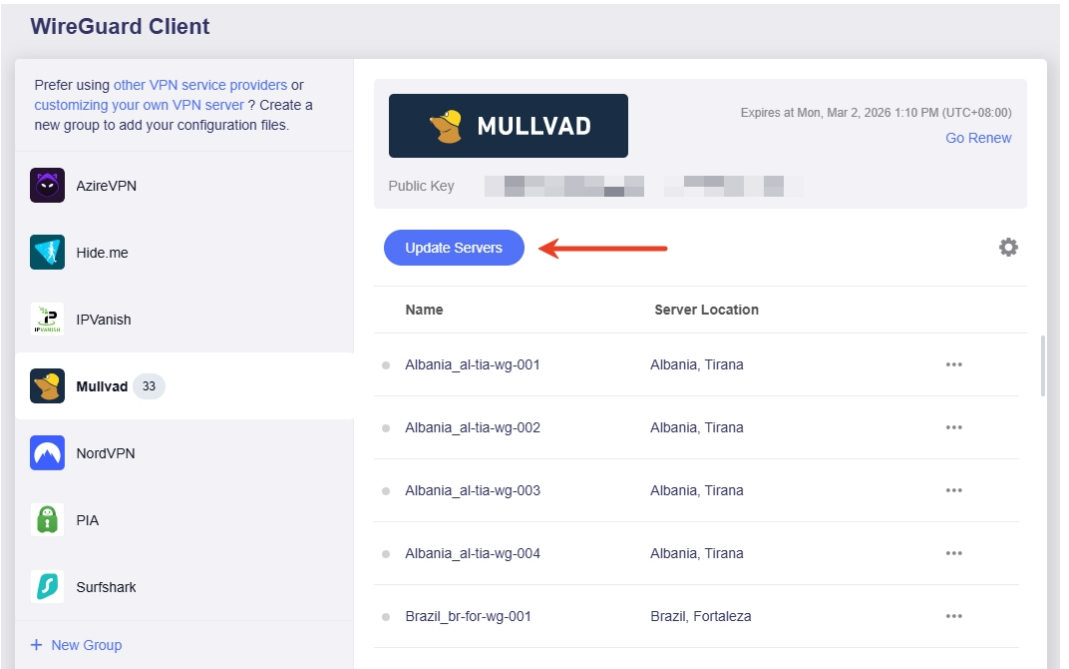
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Tú puedes también verifique los detalles de la conexión VPN en el **Panel de VPN**.

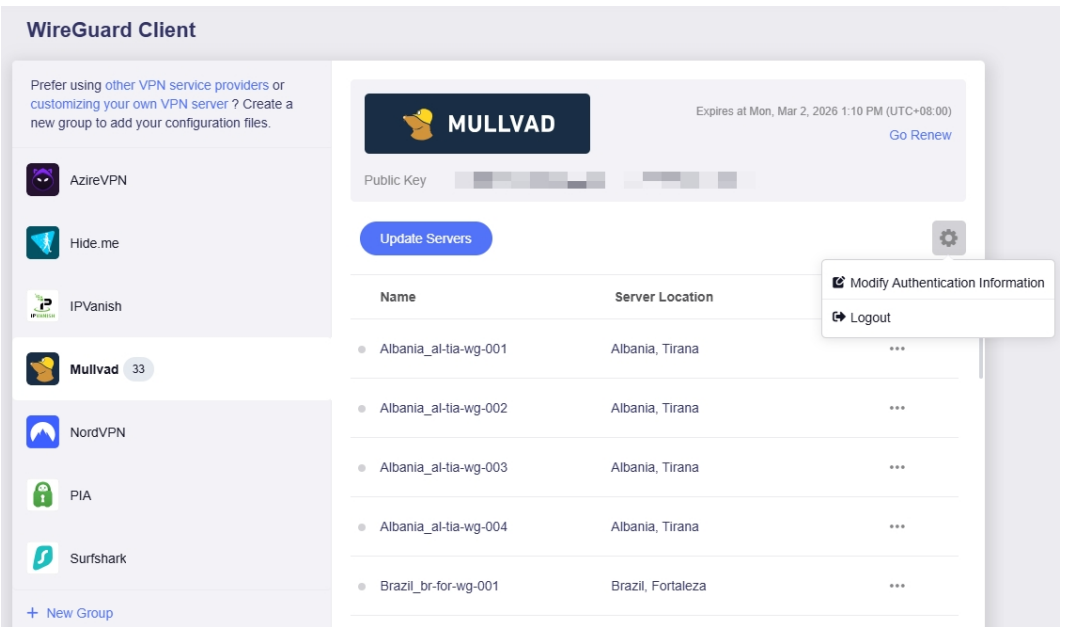
6. Actualizar servidores.

   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.



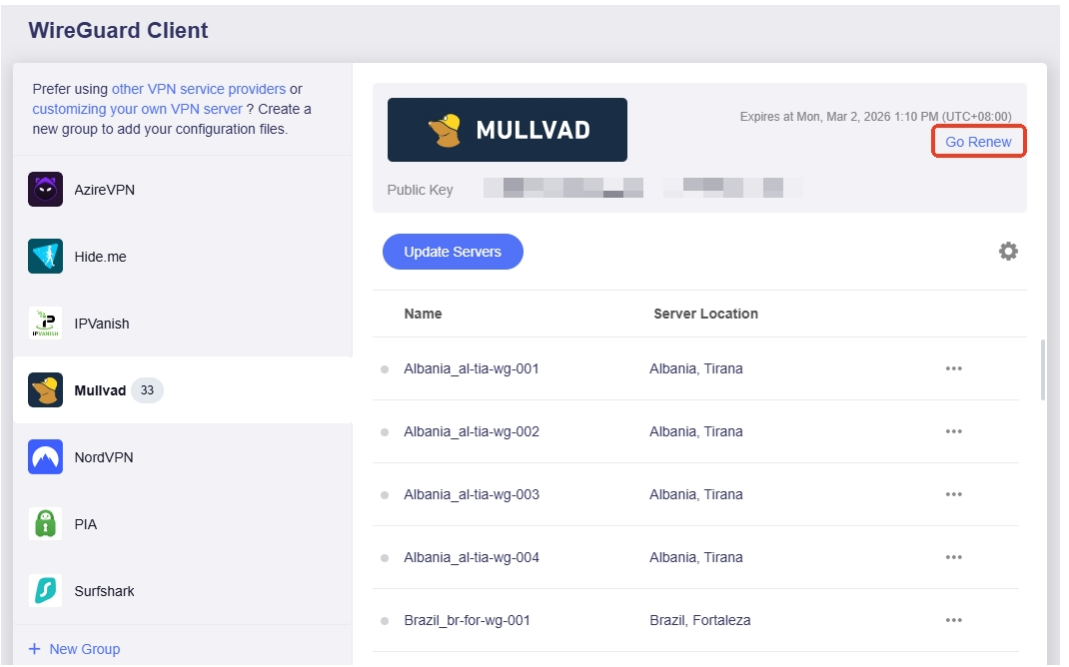
7. Editar credenciales o cerrar sesión.

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



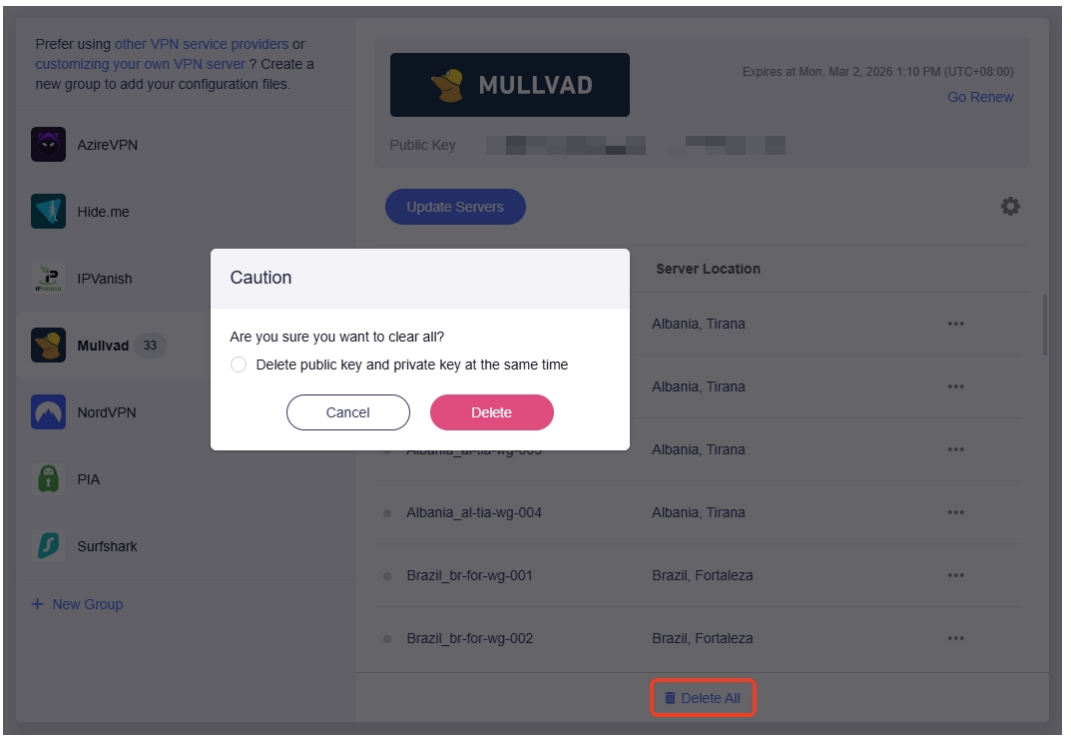
8. Ir a renovar.

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



9. Eliminar todos los archivos.

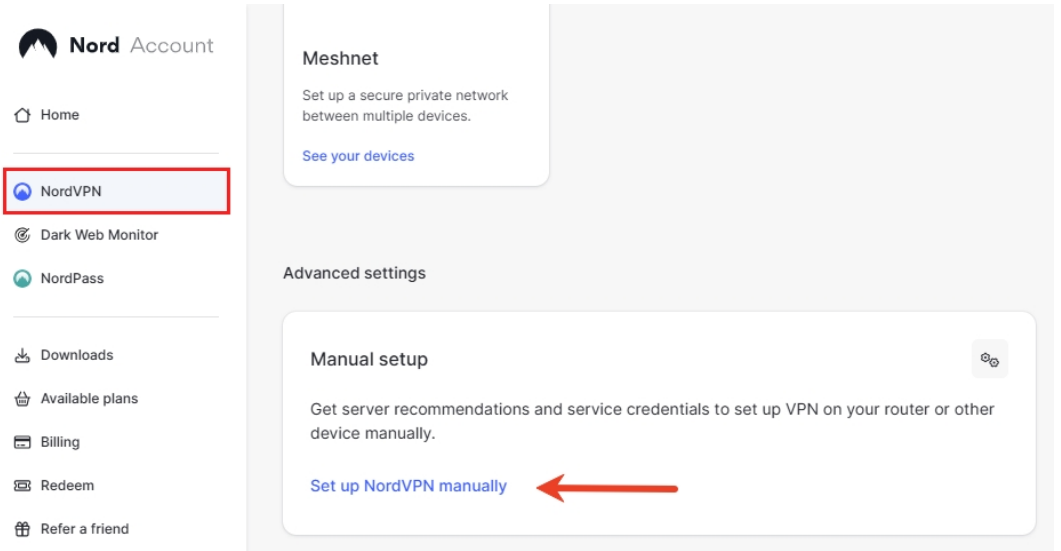
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar el archivo privado. y claves públicas simultáneamente.



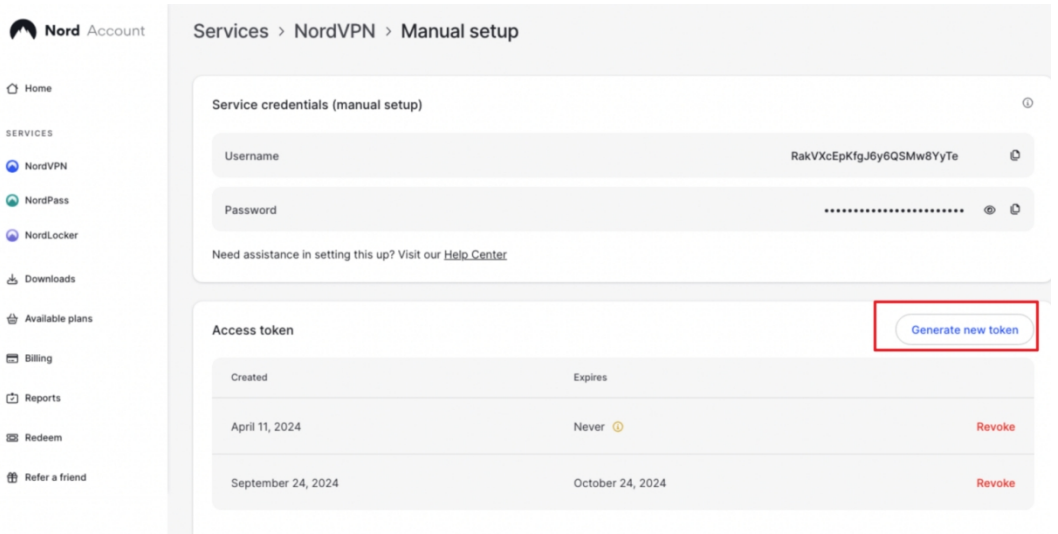
11.2.6 Configurar NordVPN

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

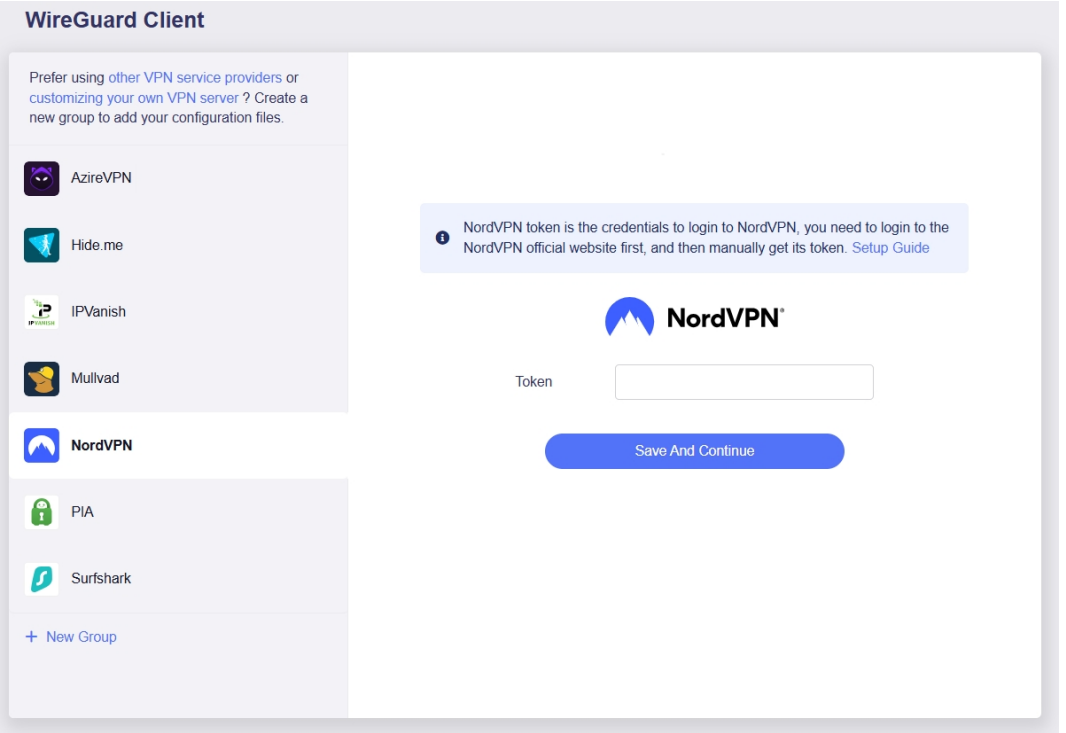
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen el Nord Dashboard, haga clic en **NordVPN** y luego haga clic en **Configurar NordVPN manualmente**.



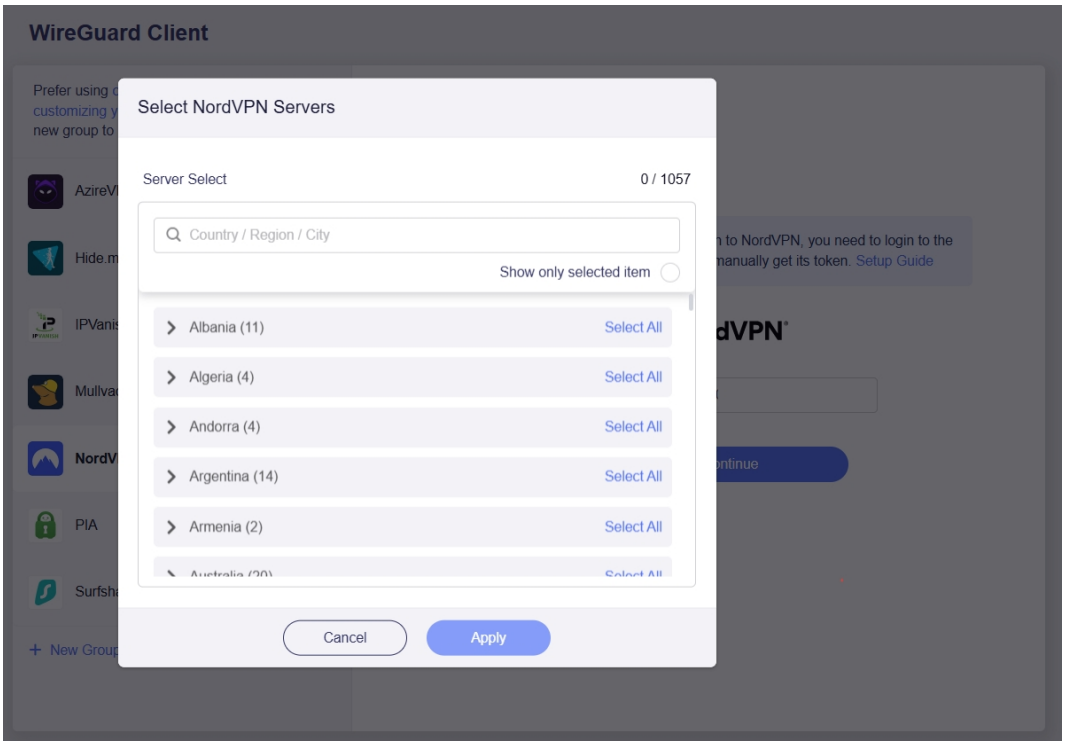
Encontrará el **Token de acceso**. Cree un token de acceso y copiecopia para usarlo más adelante.



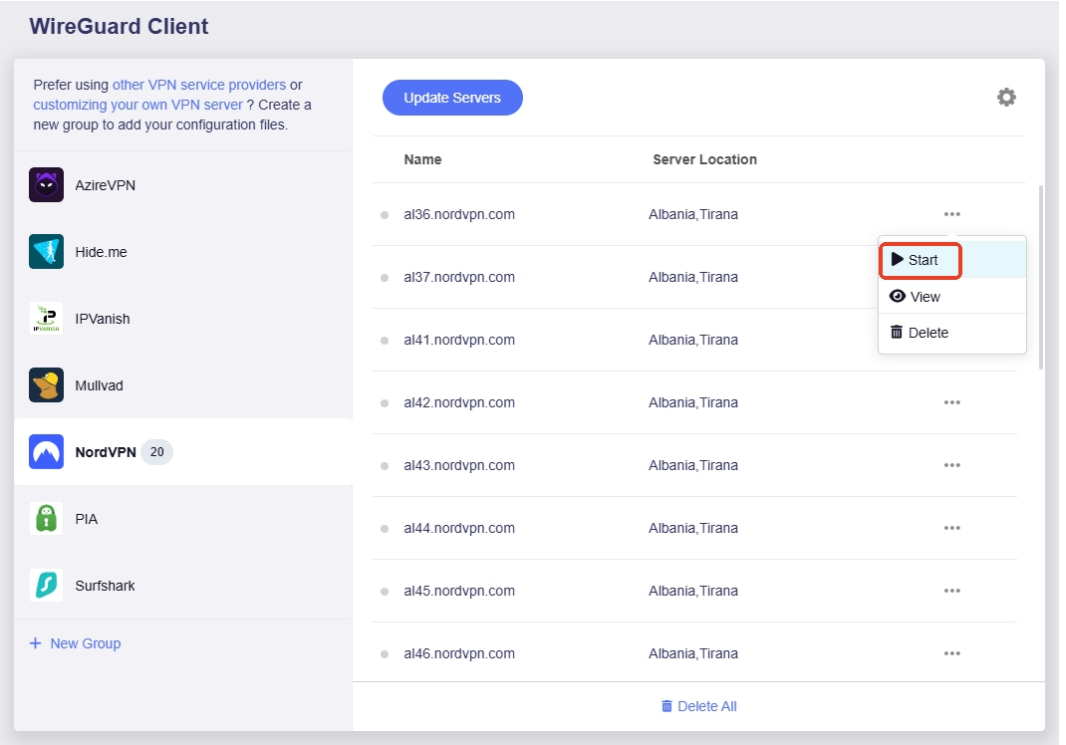
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Entrada token, y haga clic en **Guardar y continuar**.



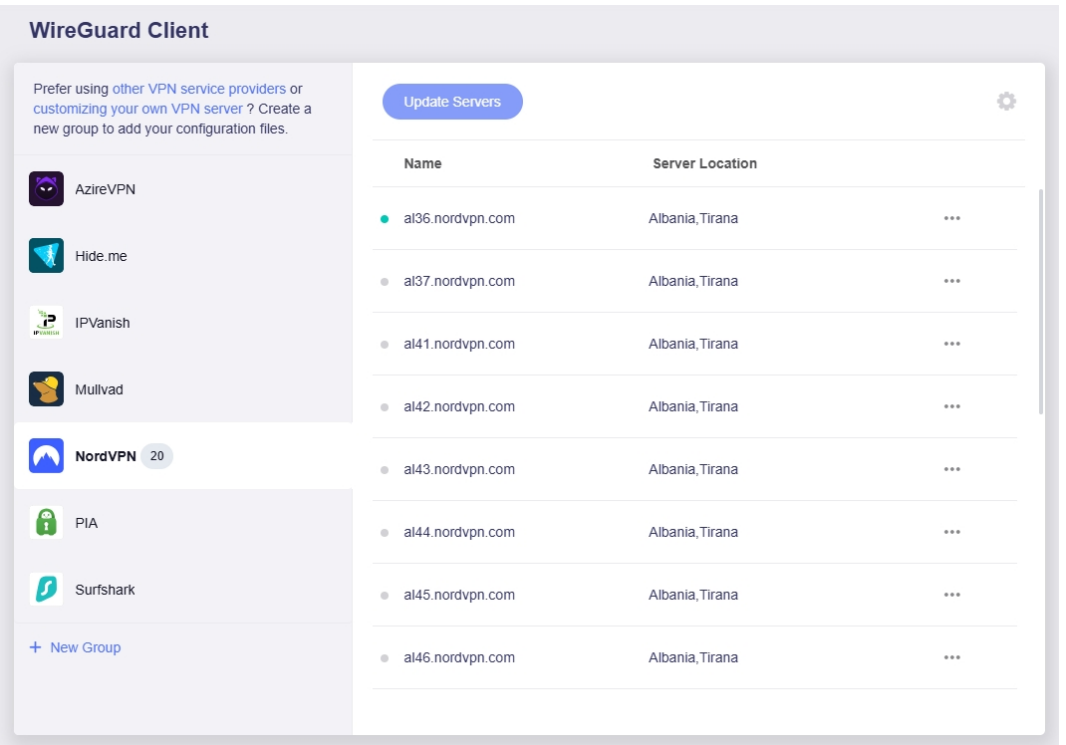
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



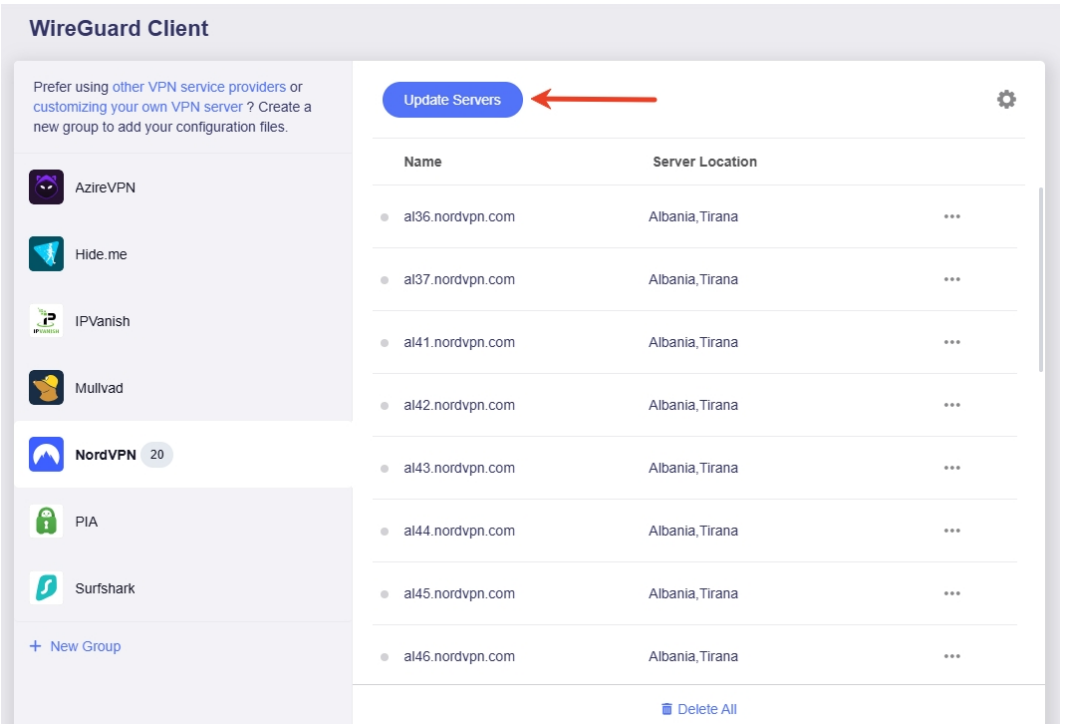
7. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Tú puedes también comprobar el Detalles de la conexión VPN en **Panel de VPN**.

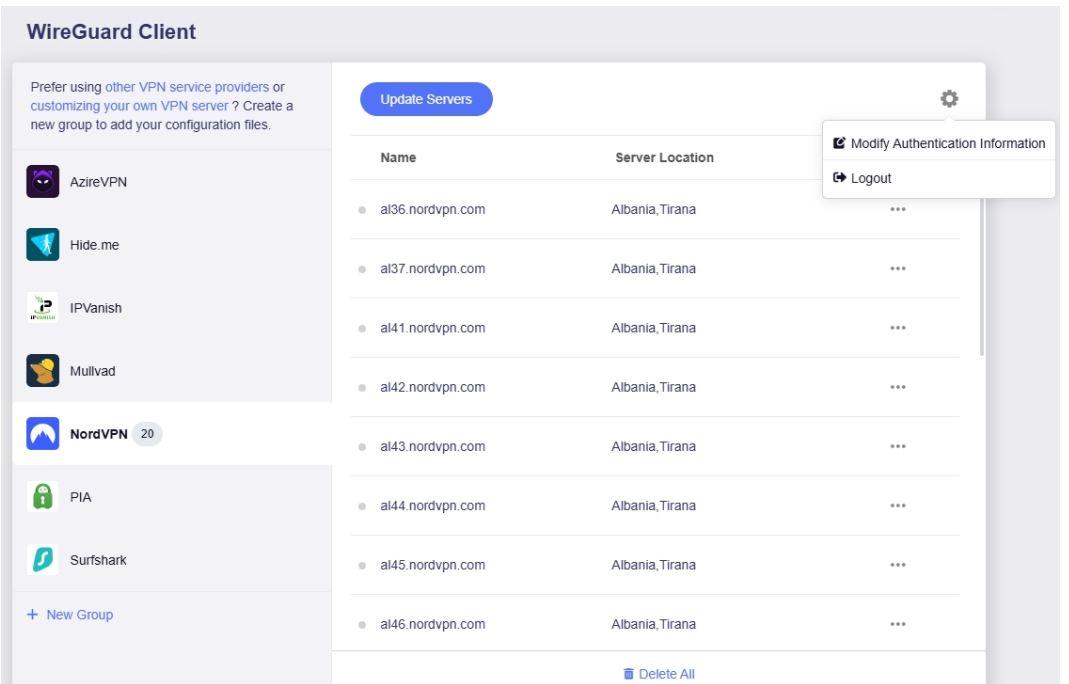
8. Actualizar servidores.

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.



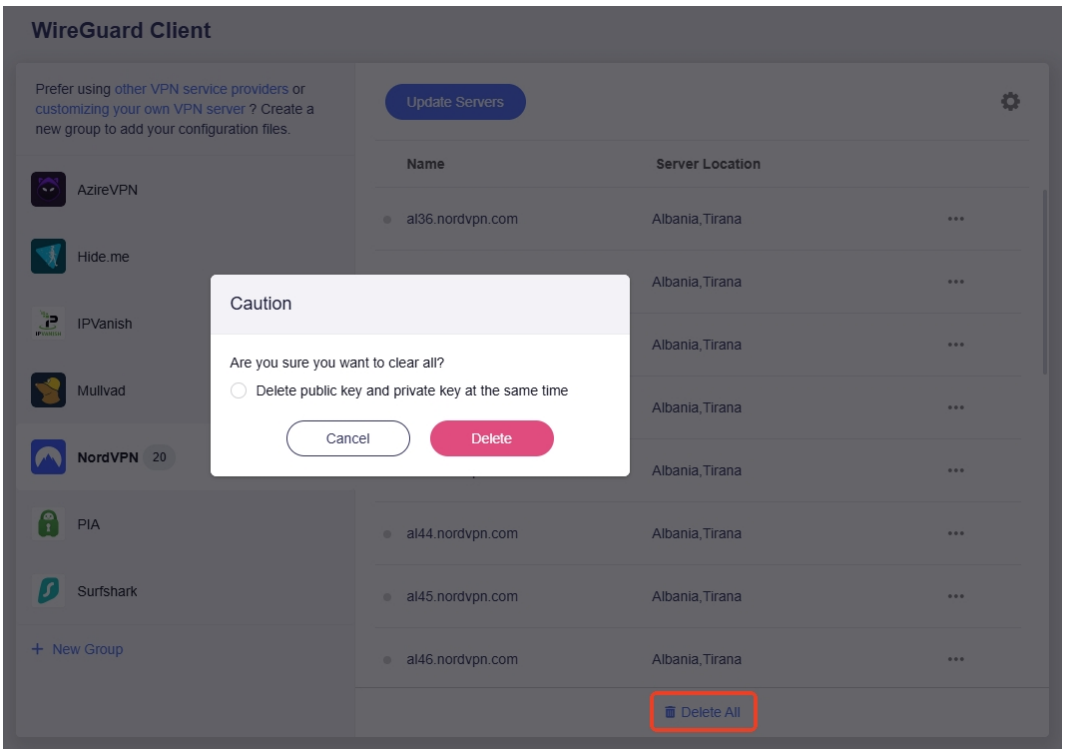
9. Edite las credenciales o cierre sesión.

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



10. Eliminar todos los archivos.

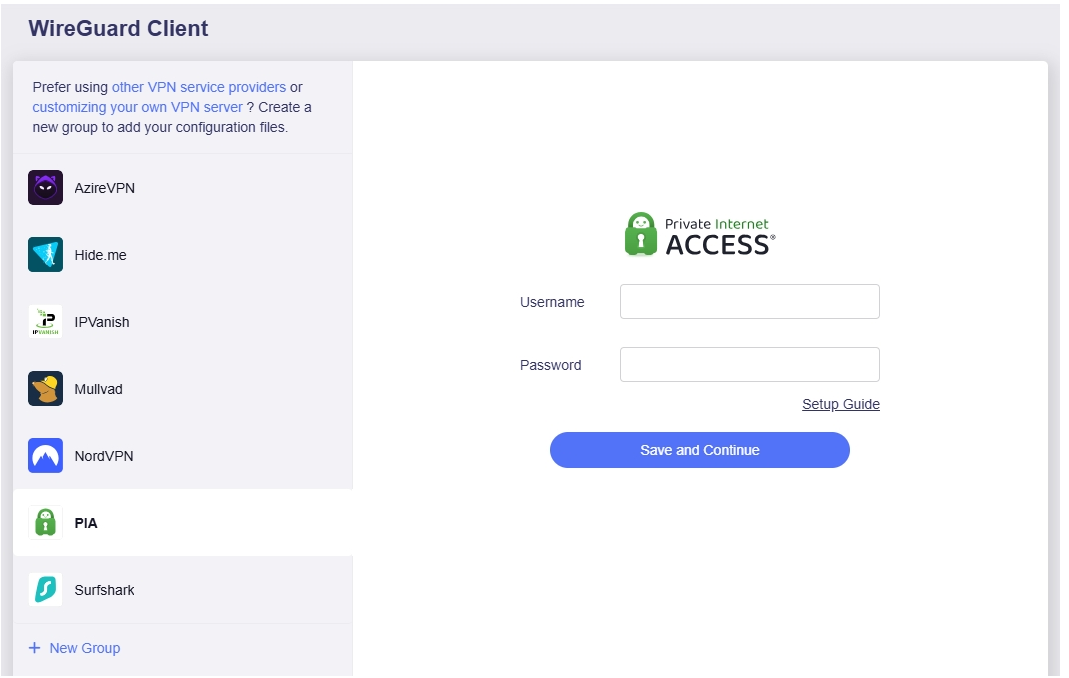
    Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



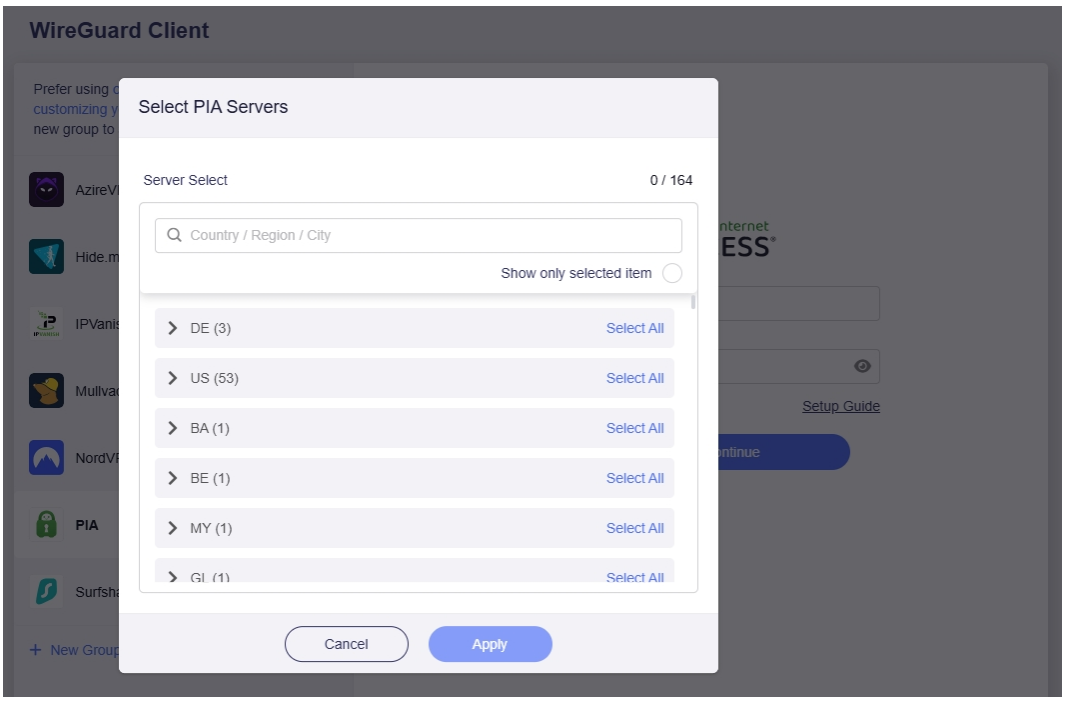
11.2.7 Configurar PIA (Private Internet Access)

Siga los pasos siguientes para configurar su enrutador como cliente PIA.

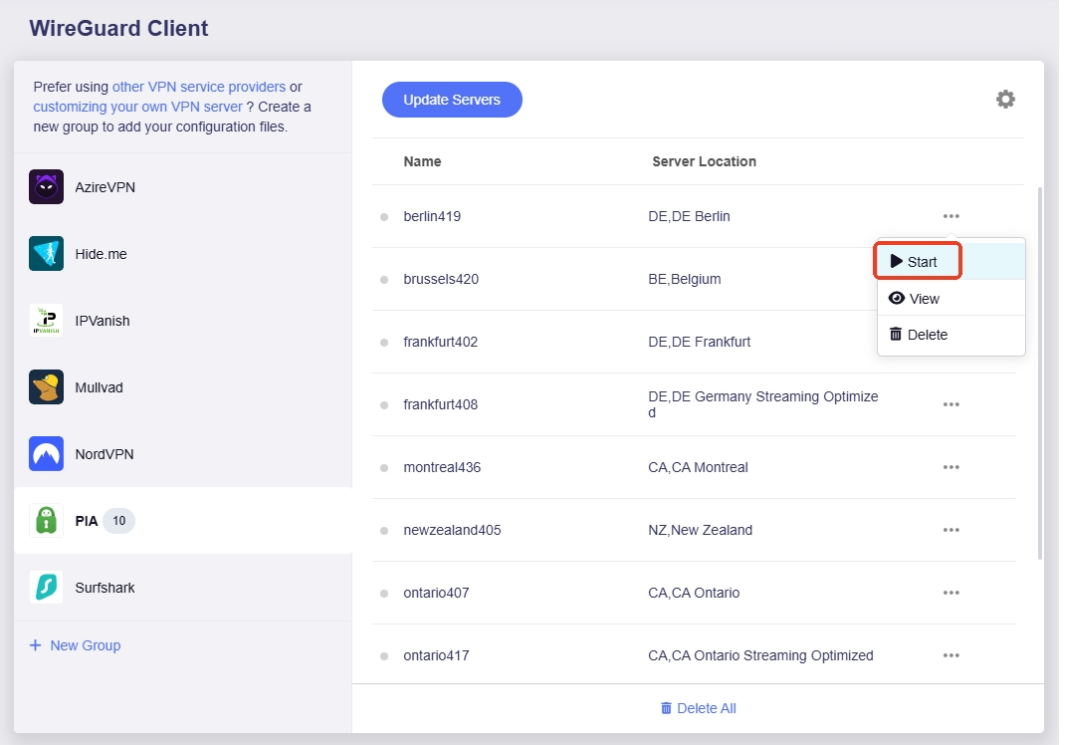
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



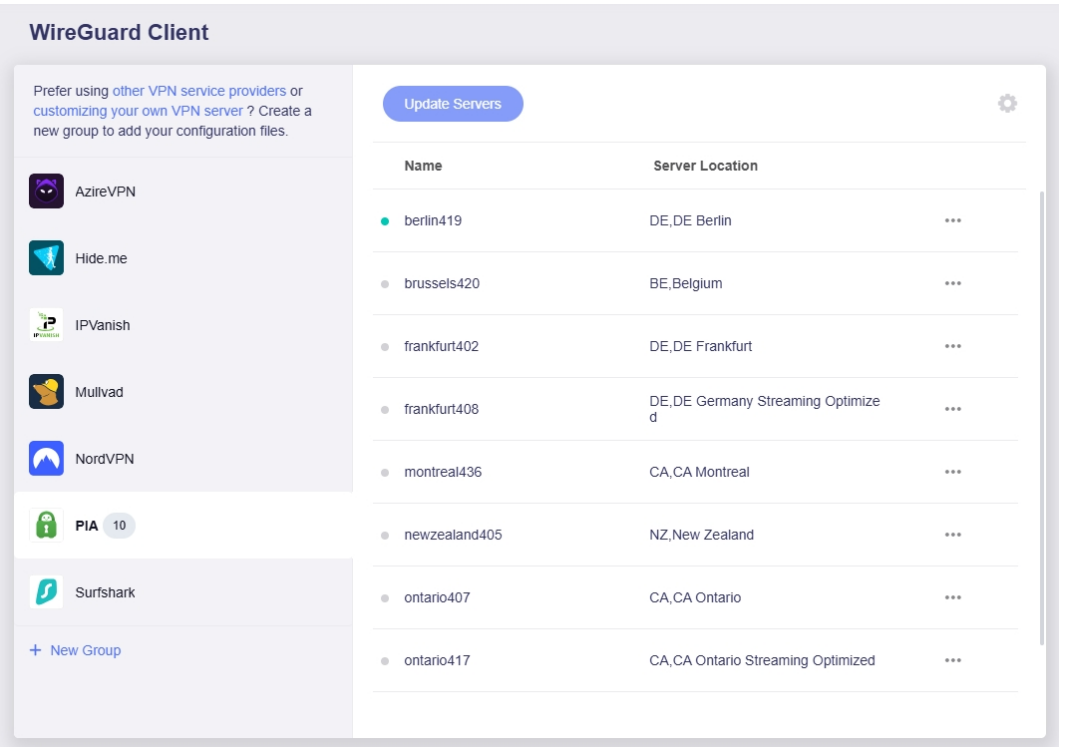
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



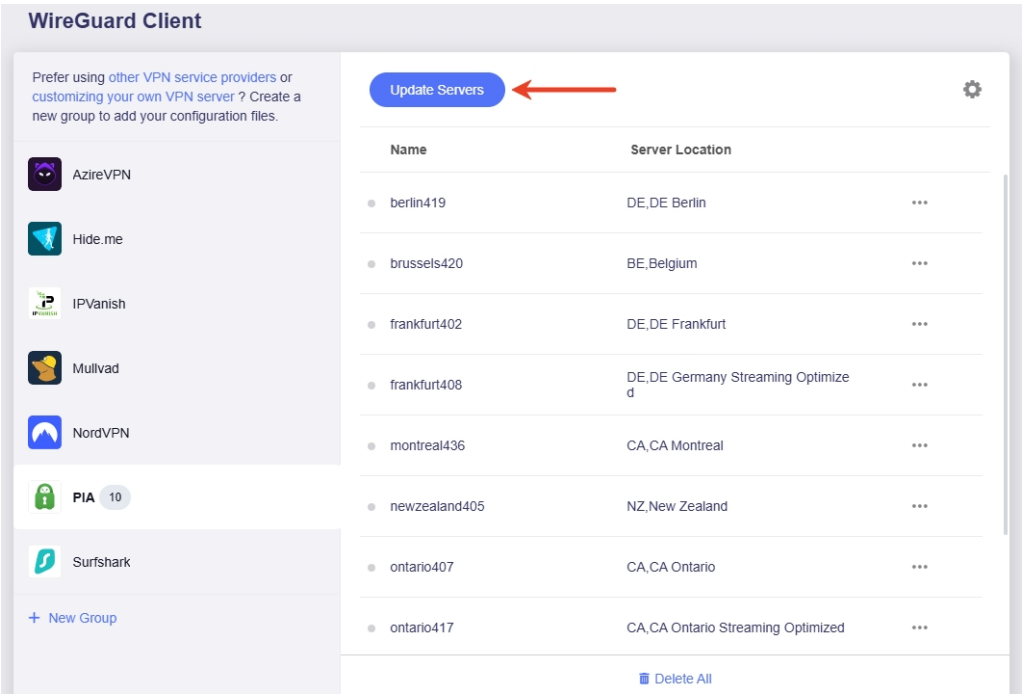
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

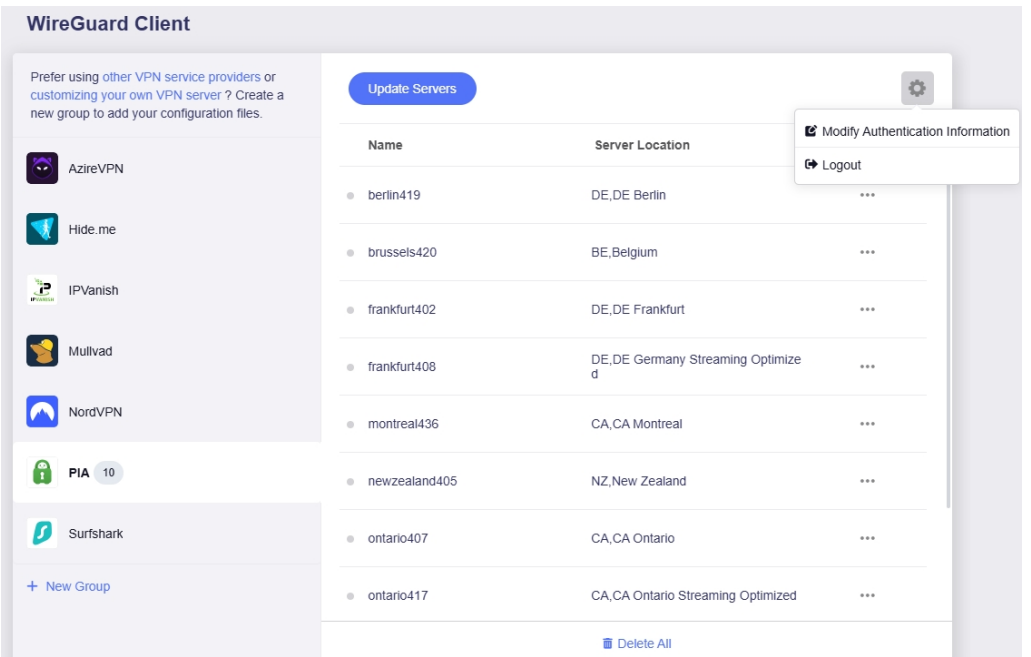
6. Actualizar servidores.

   Puedes haga 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.



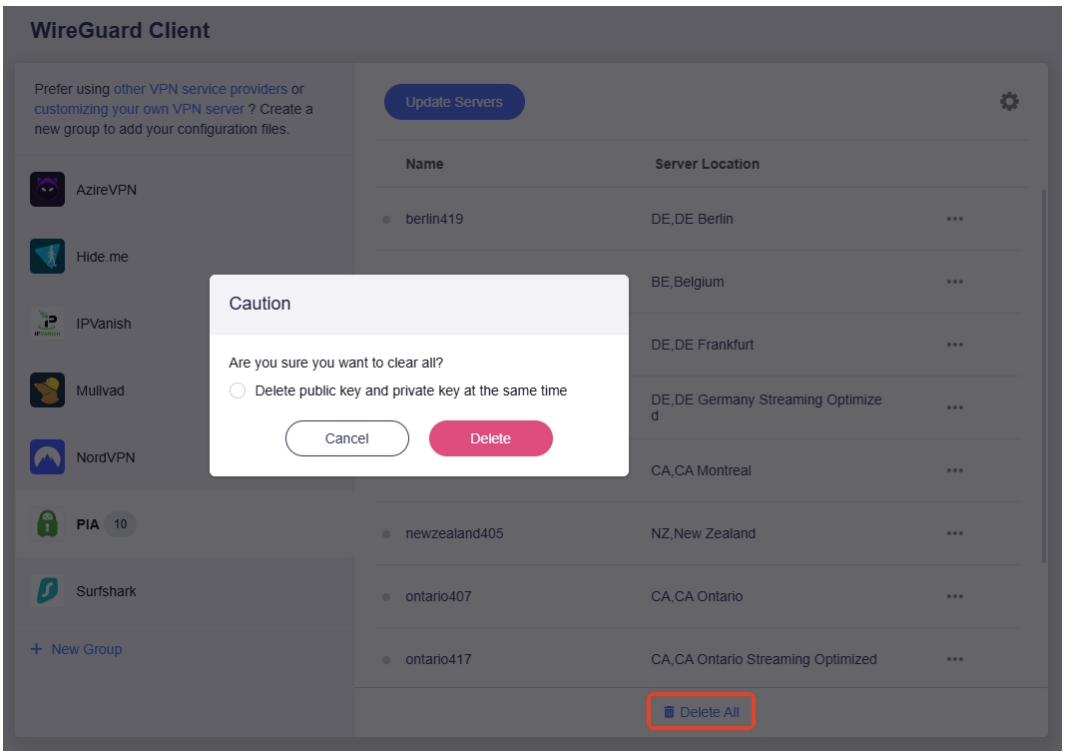
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

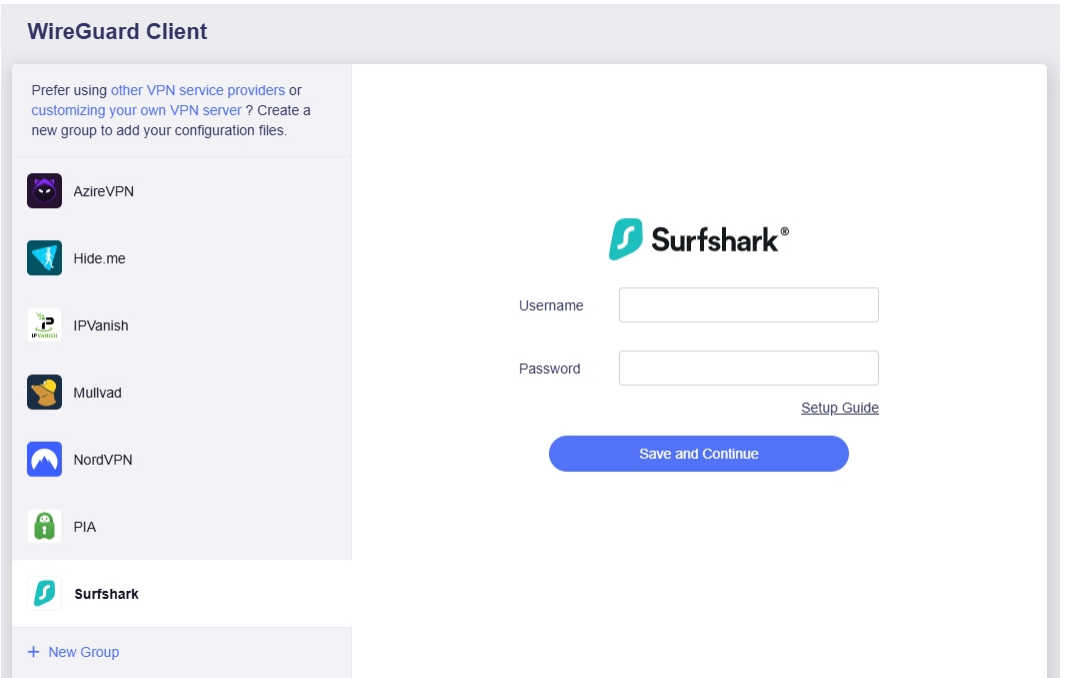
   Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



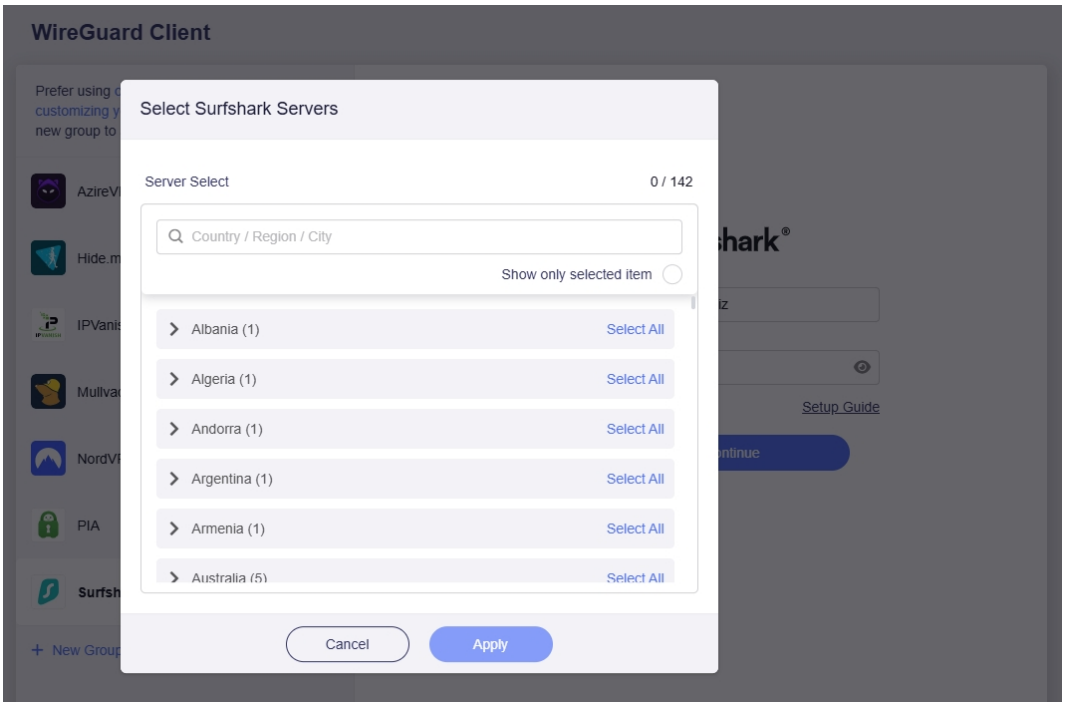
11.2.8 Configurar Surfshark

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

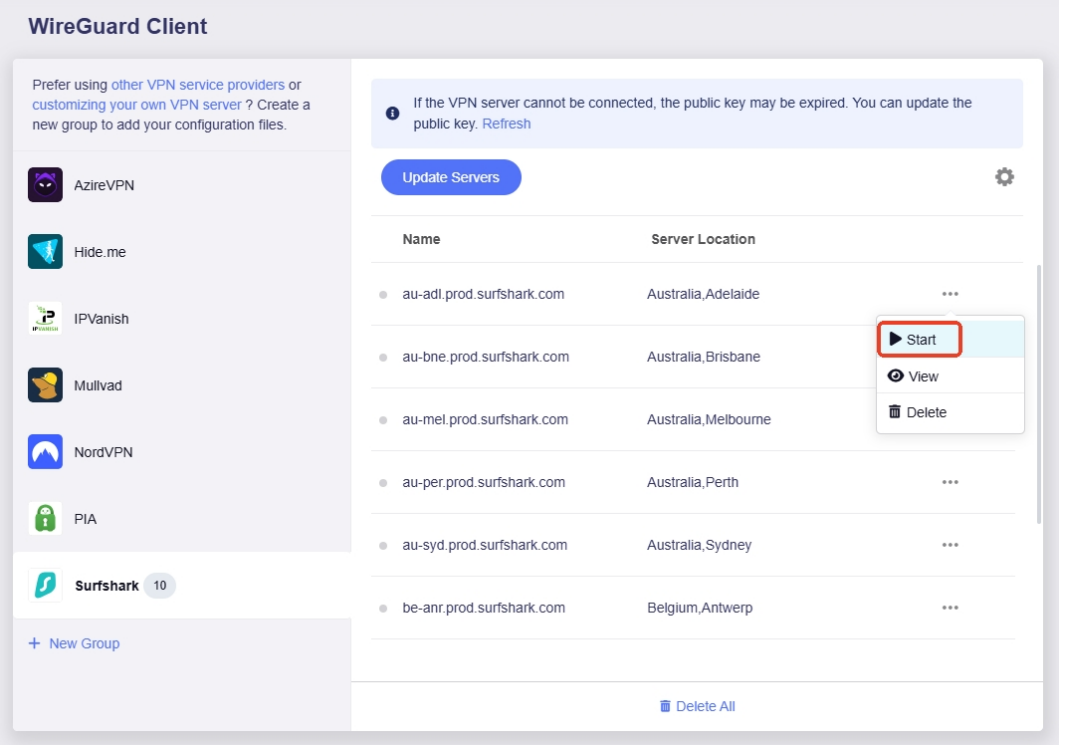
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Surfshark**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



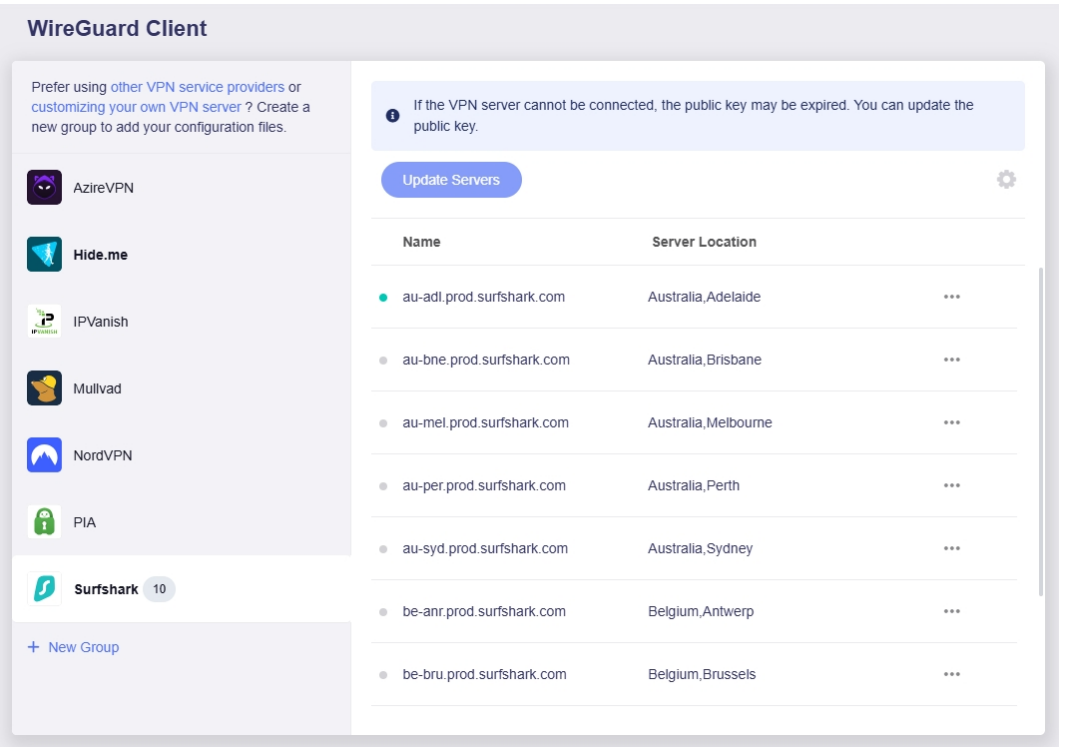
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



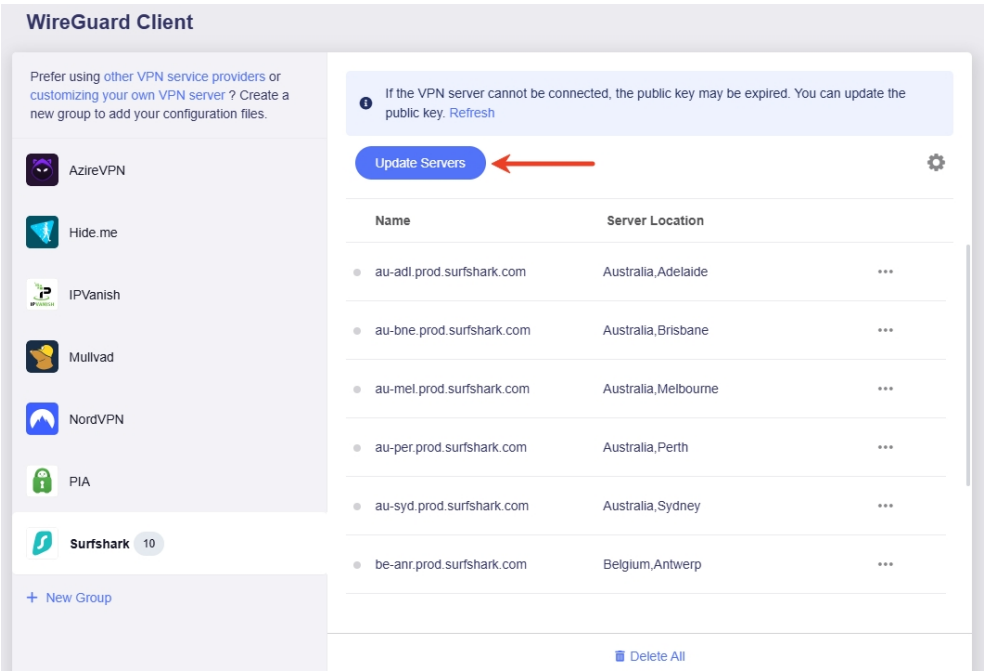
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Tú puedes también verifique los detalles de la conexión VPN en el **Panel de VPN**.

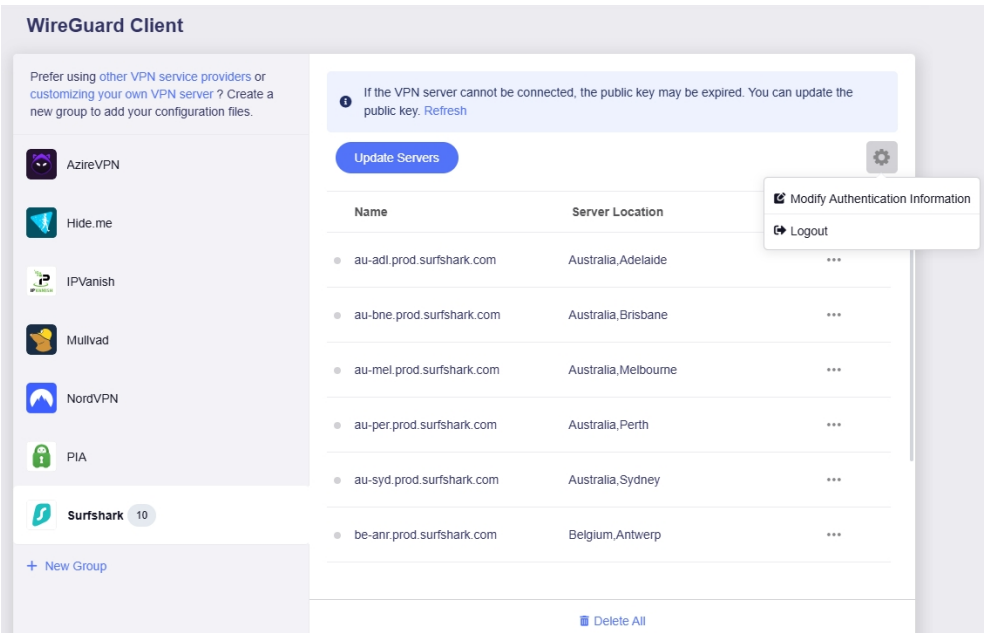
6. Actualizar servidores.

   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.



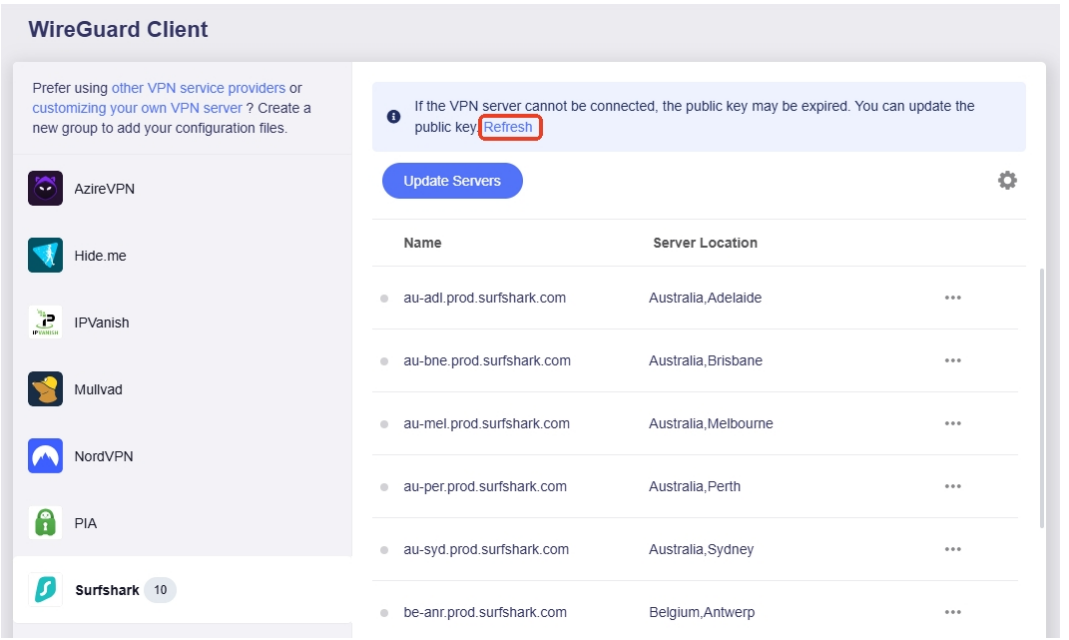
7. Editar credenciales o cerrar sesión.

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



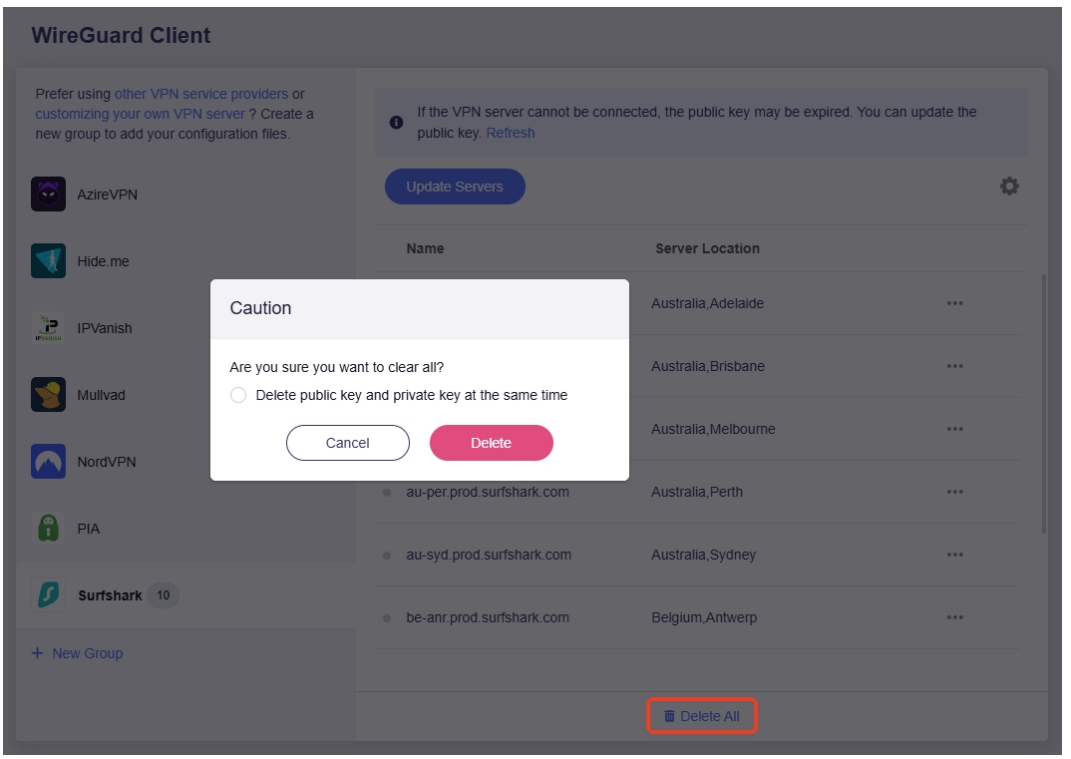
8. Actualizar.

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



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 públicas y privadas. simultáneamente.

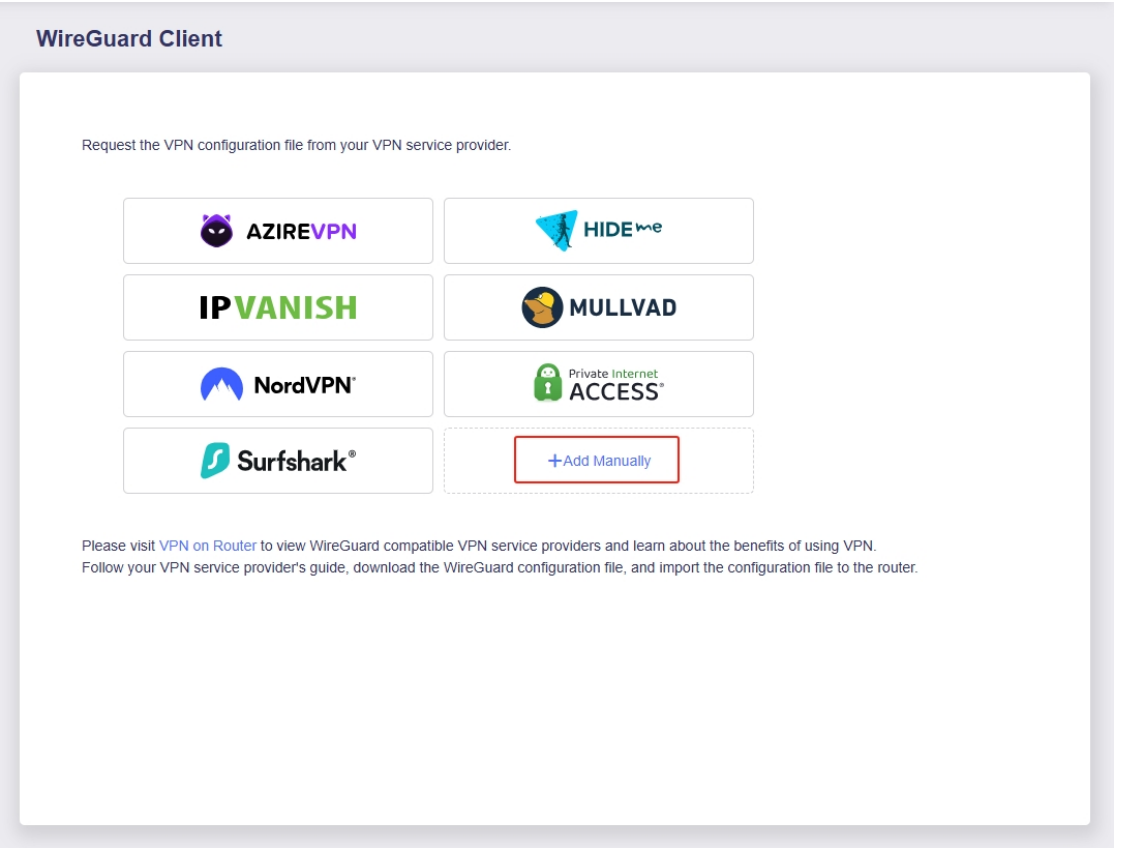


11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

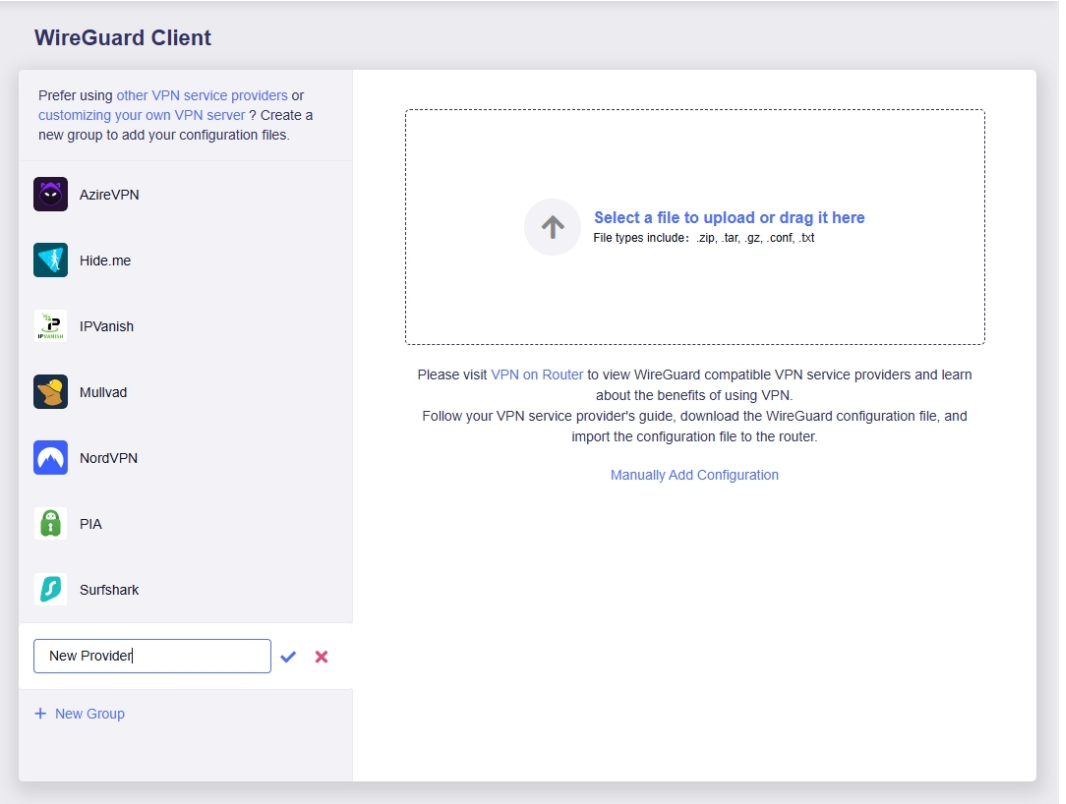
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

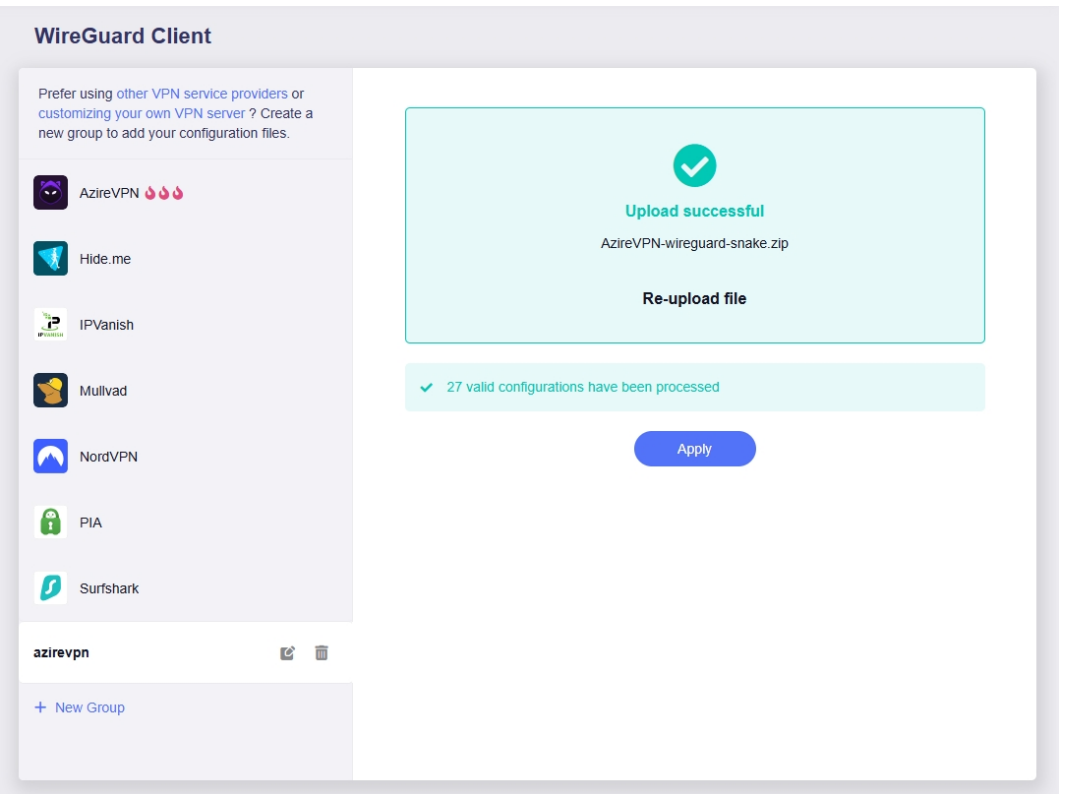
1. Inicie sesiónn en su enrutador's web admin panel y navega hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



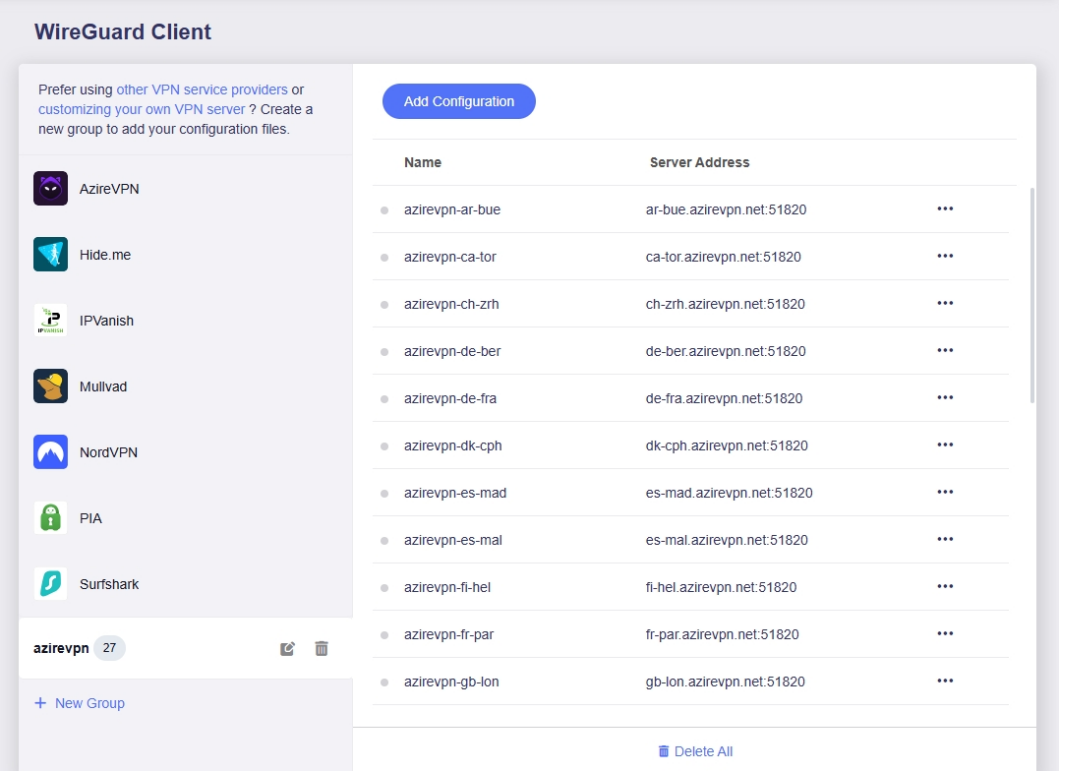
2. Creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



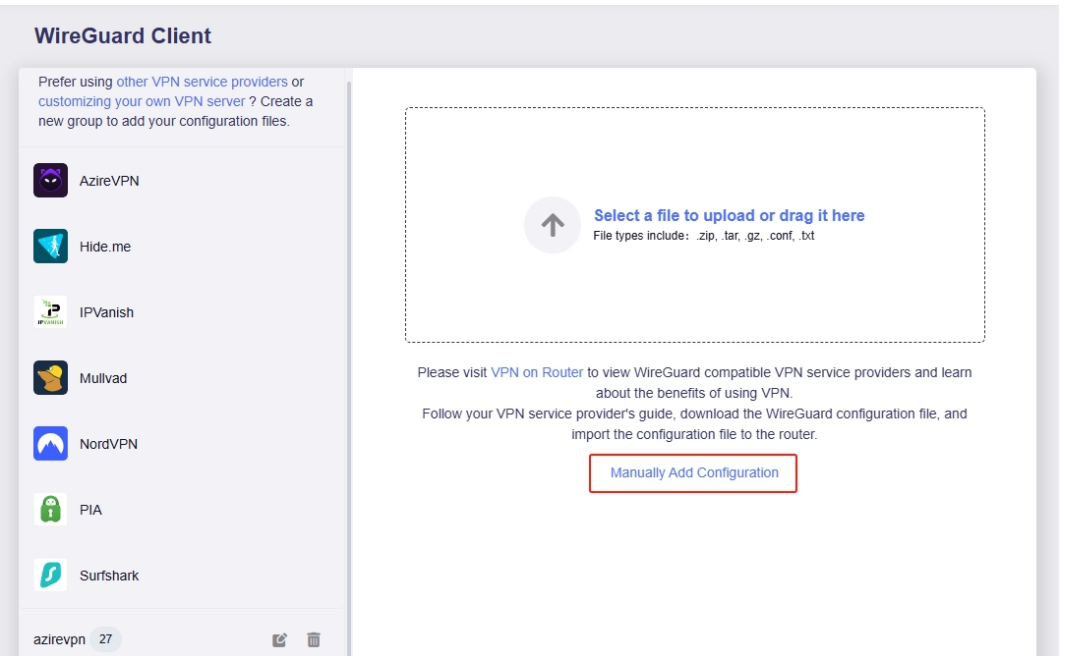
3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt) y haga clic en **Aplicar**.

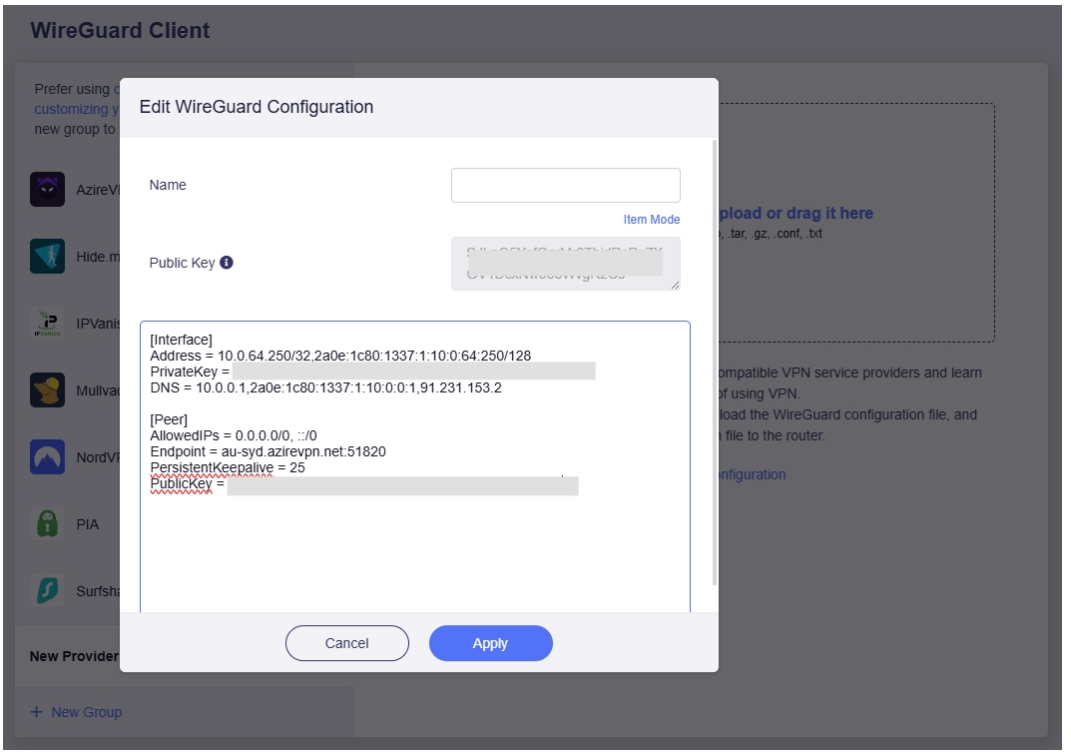


Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

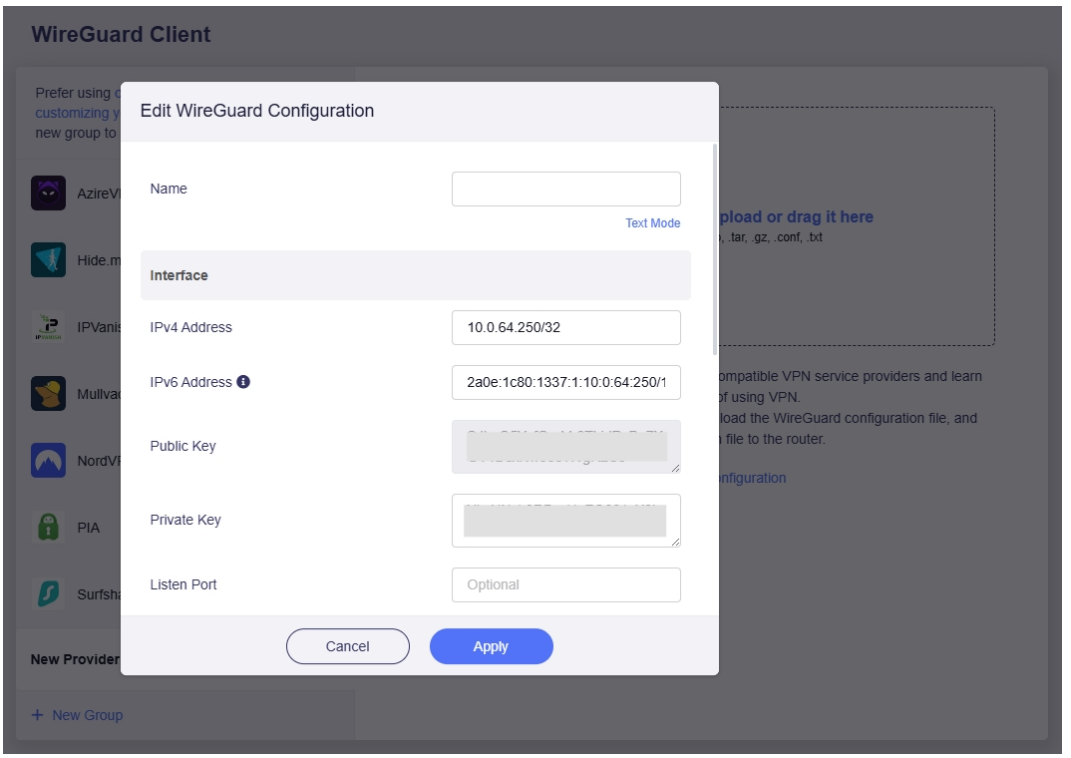


Como alternativa, puede hacer clic en **Agregar configuración manualmente** en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

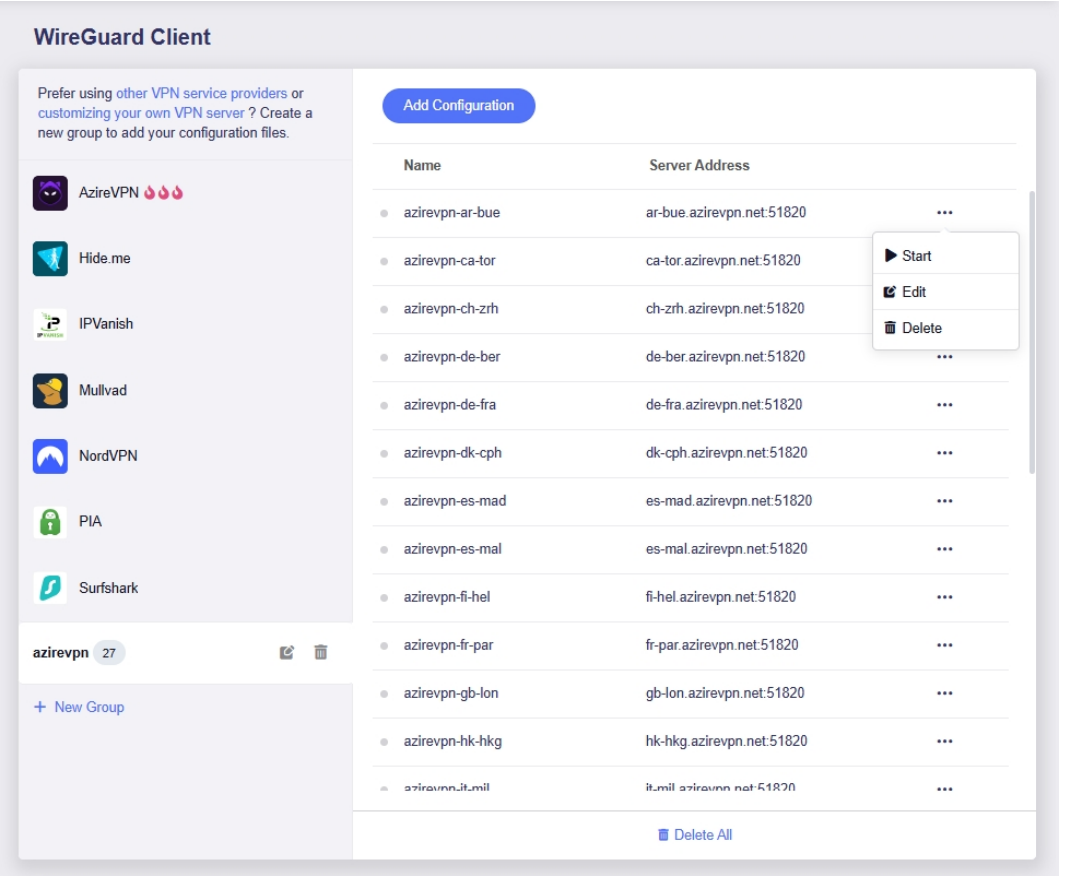




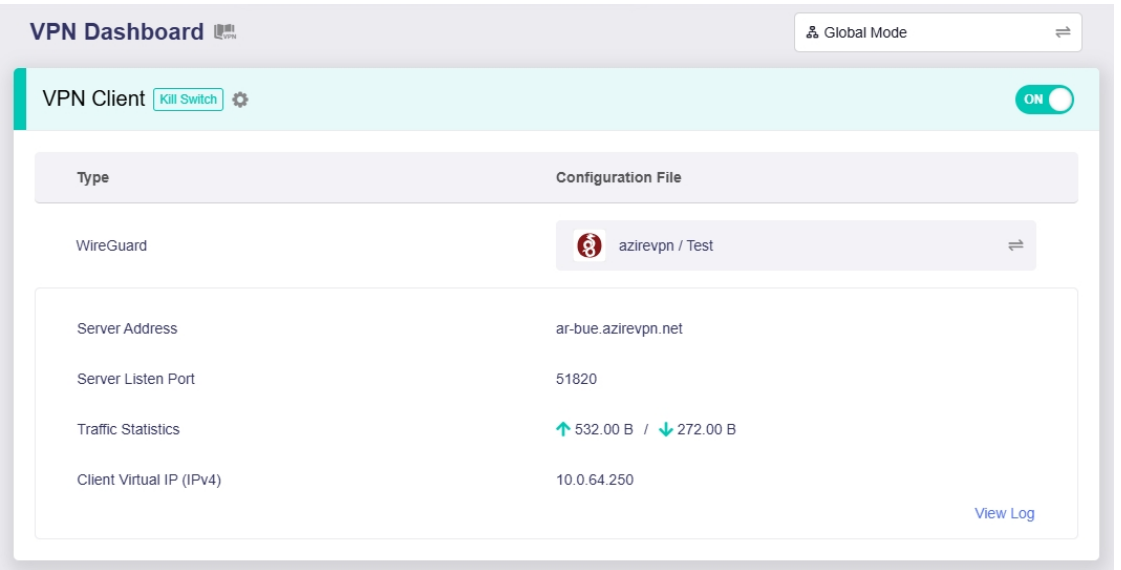
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, tluego haga clic en **Aplicar**.



4. Haga clic en el icono de 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 el Detalles de la conexión VPN en el **Panel de VPN**.



Capítulo 12

Red

Este capítulo presenta las configuraciones relacionadas con la red para la configuración y administración, como LAN, DNS e IPv6.

12.1 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.

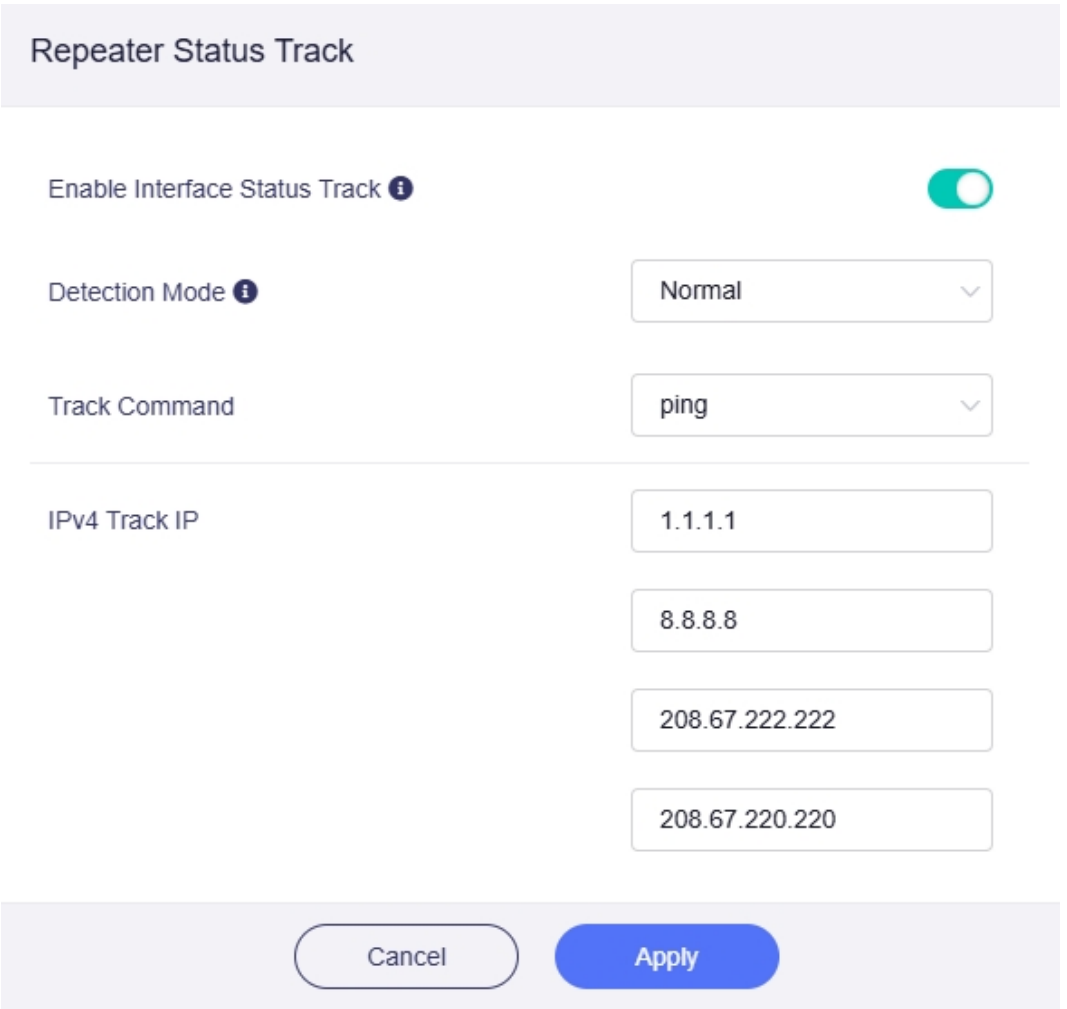
12.1.1 Seguimiento del estado de la interfaz

Los enrutadores GL.iNet utilizan el comando **ping** 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 icono de engranaje a la derecha para acceder a la configuración de seguimiento de estado para cada interfaz de red.haga clic en el ícono de ajustes a la derecha para acceder a la configuración de

seguimiento de estado para cada interfaz de red. A continuación se muestran la configuración de seguimiento de estadoings para la interfaz del Repetidor. La misma lógica de configuración se aplica a otras interfaces.



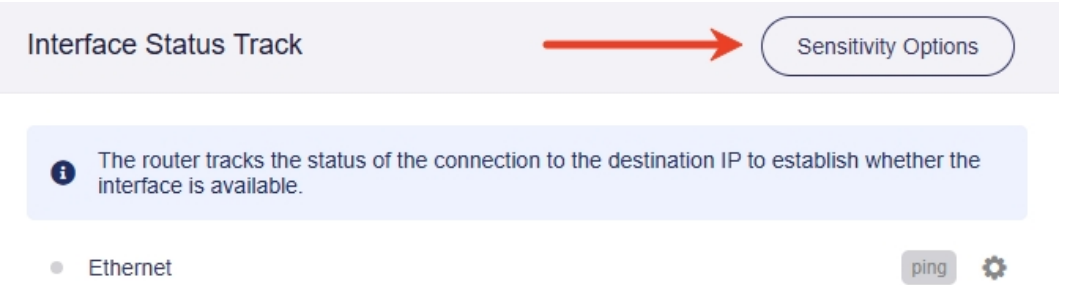
- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el dispositivo asumirá que está conectado a Internet cuando la interfaz está conectada (por ejemplo, si se conecta un cable y se adquiere una dirección IP).
- **Modo de detección**: esta característica se introdujo como Modo de datos bajos en firmware v4.5, luego se renombra como Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
  - **Normal Modo**: Es used de forma predeterminada.
  - **Datos bajos Modo**: 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.

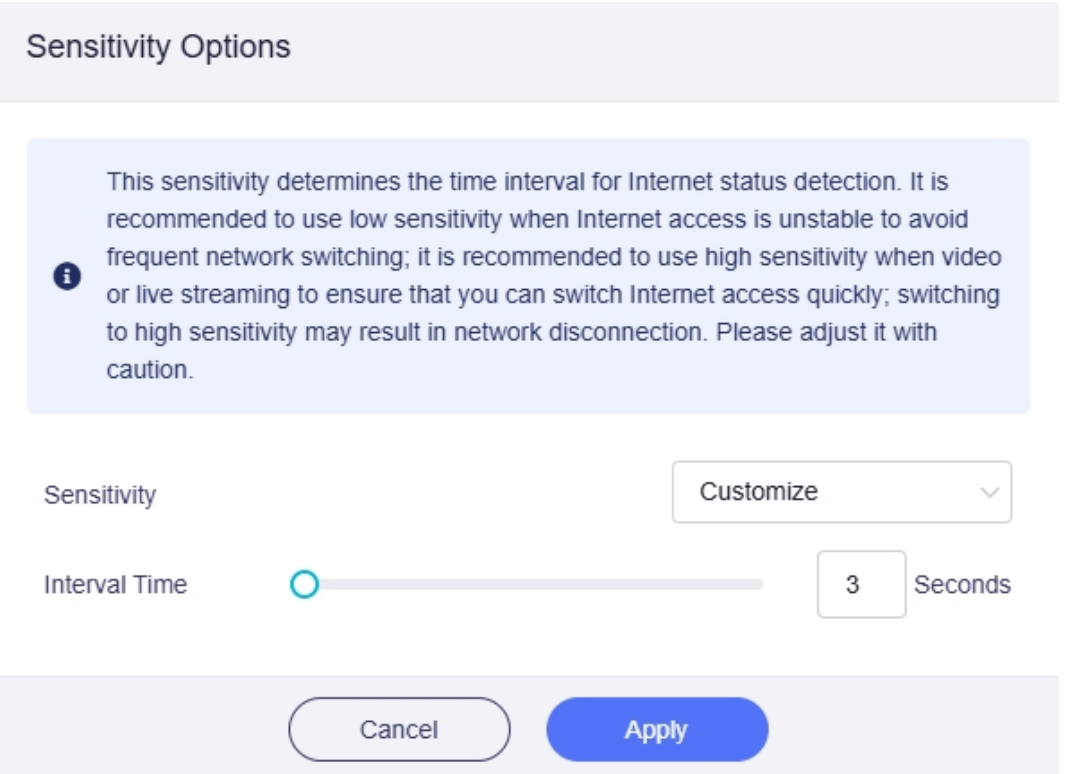
- **Estricto Modo**: Determina el estado de la interfaz exclusivamente en función de los resultados de un comando de detección enviado a una IP pública.

- **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**: Cpersonalizar las direcciones IPv4 Track IP como 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.



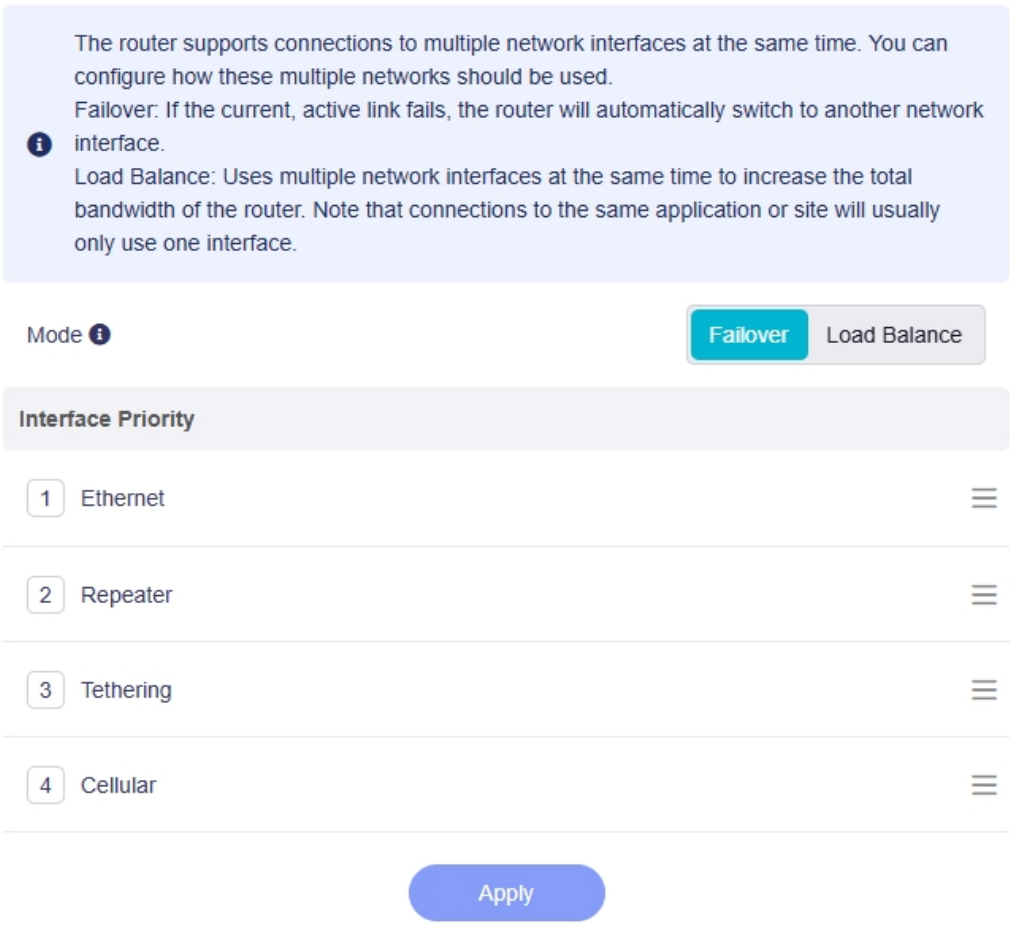
12.1.2 Modo Multi-WAN

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

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.

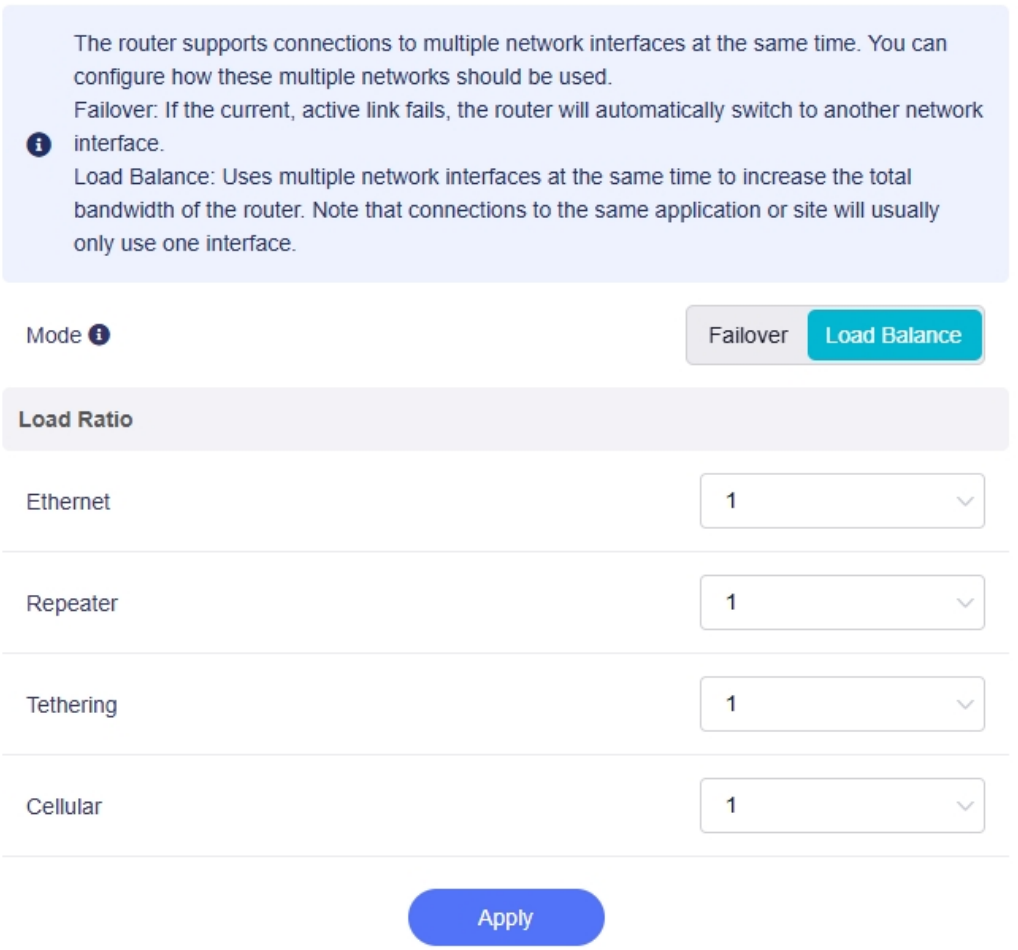
Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente al modo.



Equilibrio de carga

Load Balance utiliza múltiples interfaces de red simultáneamente para aumentar el ancho de banda total del enrutador, y el sistema distribuye las nuevas conexiones entre interfaces según 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 simultáneamente (por ejemplo, Ethernet, Repetidor, Anclaje a red, y Celular) y todas las interfaces están disponibles para el acceso a Internet, lo que permite el equilibrio de carga y establece una relación de 1:1:1:1 , lo que significa que las cuatro interfaces compartirán rednuestro las interfaces compartirán la red ancho de banda por igual. El sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la relación de carga configurada.



También puede personalizar la relación de carga según sea necesario. Por ejemplo, si Ethernet tiene un ancho de banda de 100 Mbps, Repetidor tiene 200 Mbps y no otras conexiones están 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.

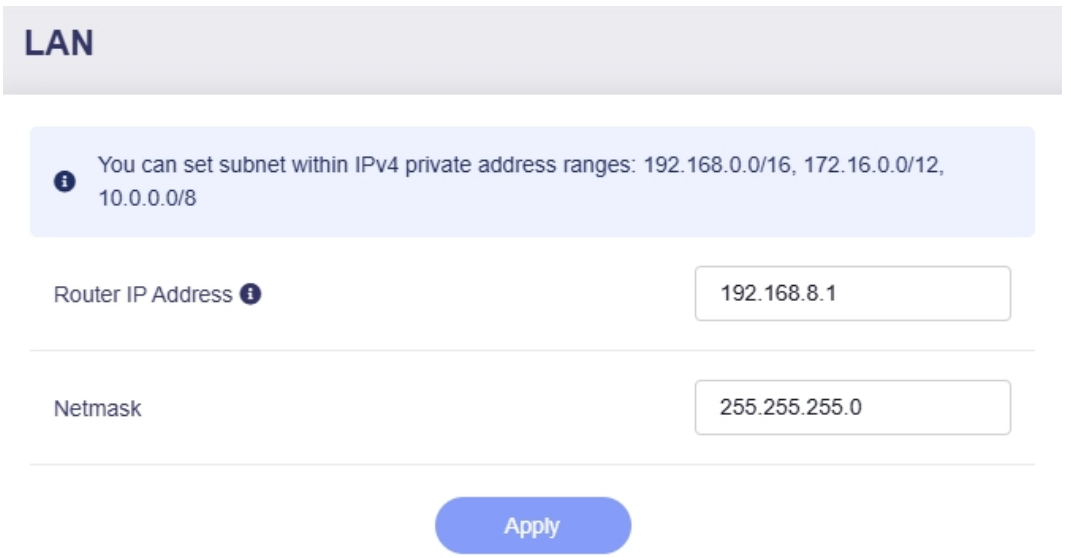
12.2 LAN

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 a **RED** >**LAN**. Aquí puede configurar los ajustes de LAN, incluidos ajustes básicos, servidor DHCP y reserva de dirección.

12.2.1 Configuración básica

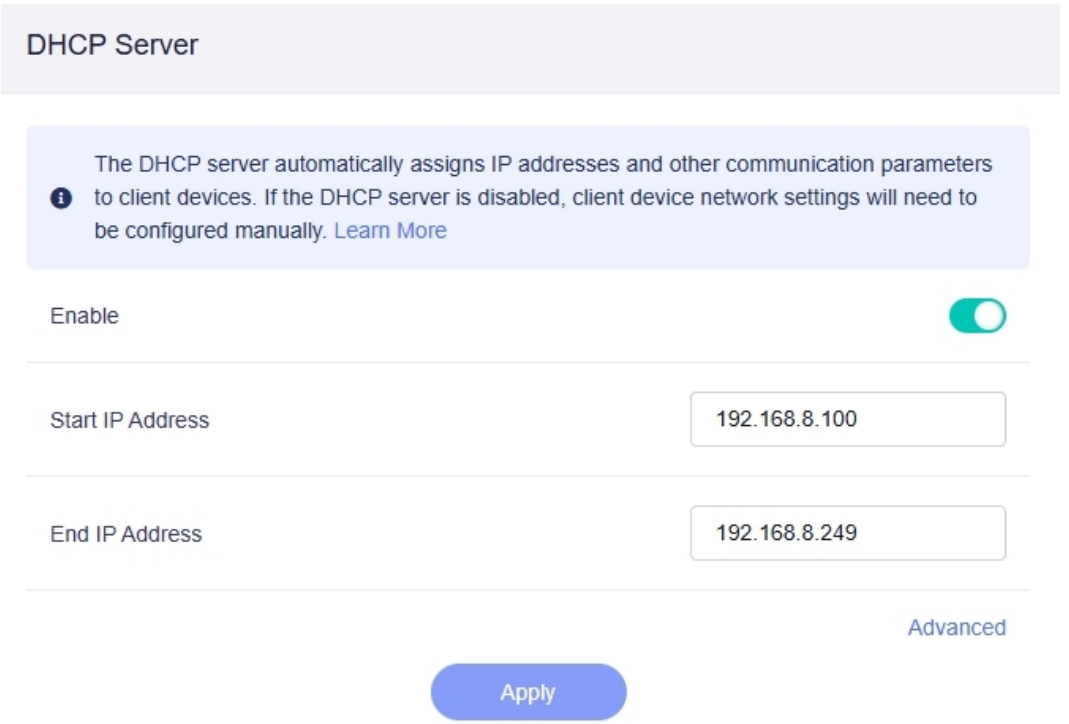
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



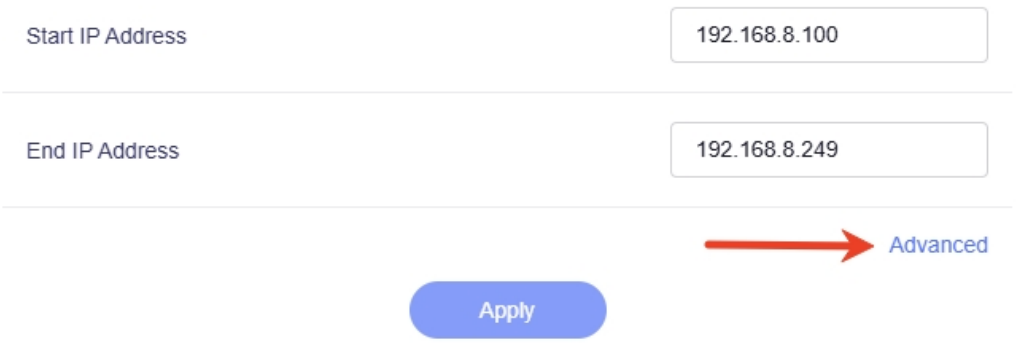
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones de un navegador para acceder al panel de administración del enrutador. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.'panel de administración. Es 192.168.8.1 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.

12.2.2 Servidor DHCP

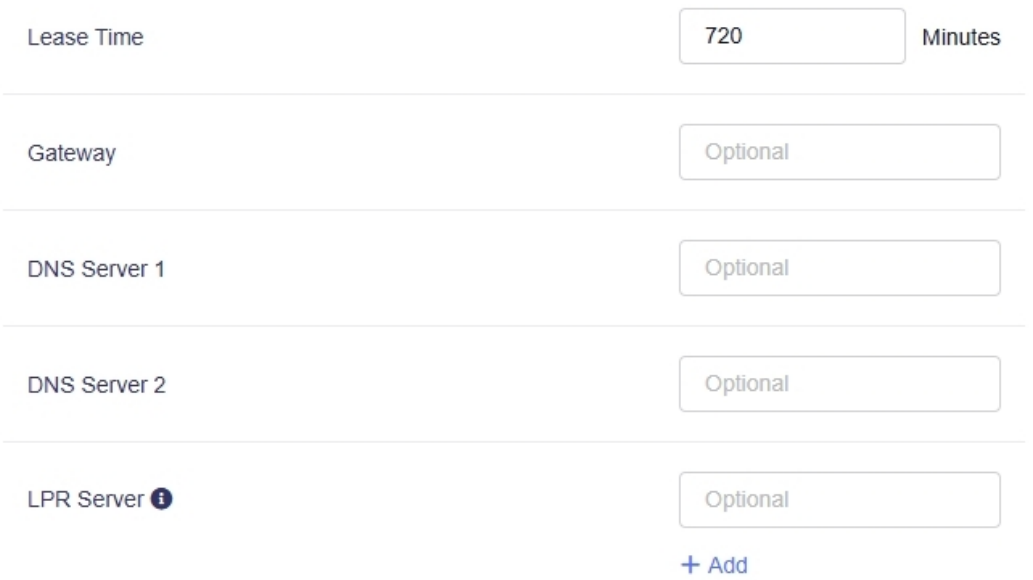
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP oscila entre 192.168.8.100 y 192.168.8.249. Puede personalizar el rango de direcciones según sea 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 según sea necesario.



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



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



- **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 local red y redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir nombres de dominio en direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS principal 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.

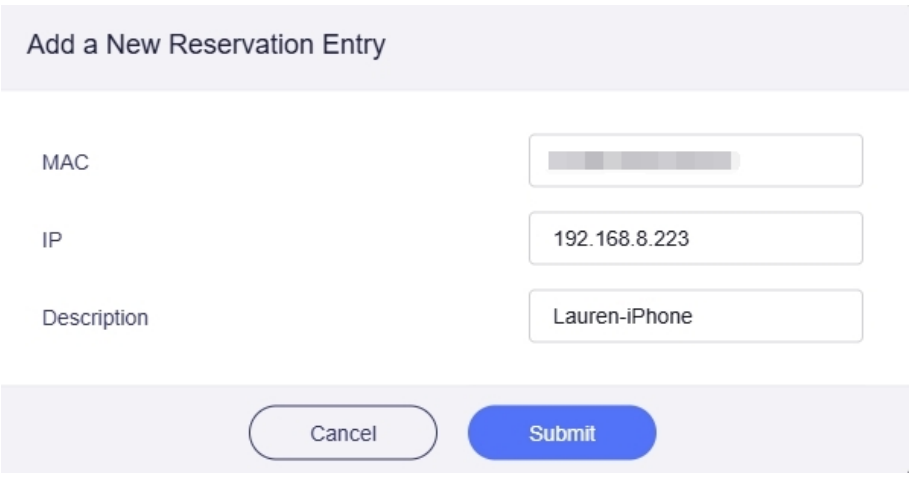
Nota: si el servidor DHCP está deshabilitado, debe configurar una IP estática y otros parámetros de comunicación manualmente para cada cliente. Consulte aquí para obtener más detalles.

12.2.3 Reserva de direcciones

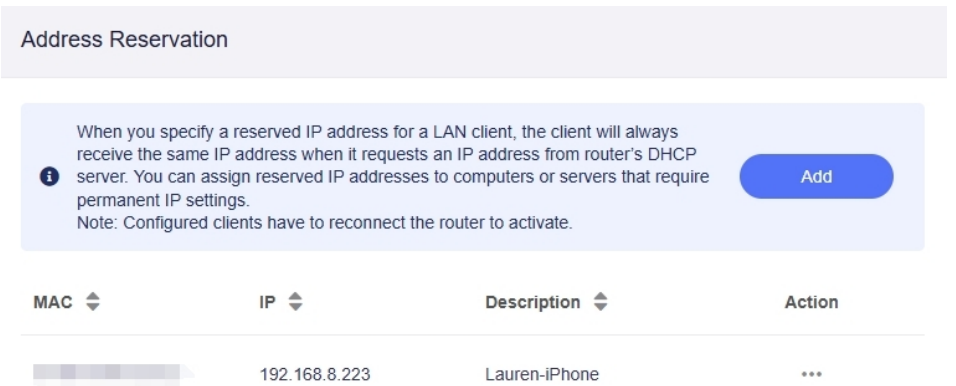
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración 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 según sea necesario.

1. Registro ingrese al 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 lala dirección IP correspondiente para la MAC seleccionada se completará automáticamente. Introduzca 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.



12.3 Red de invitados

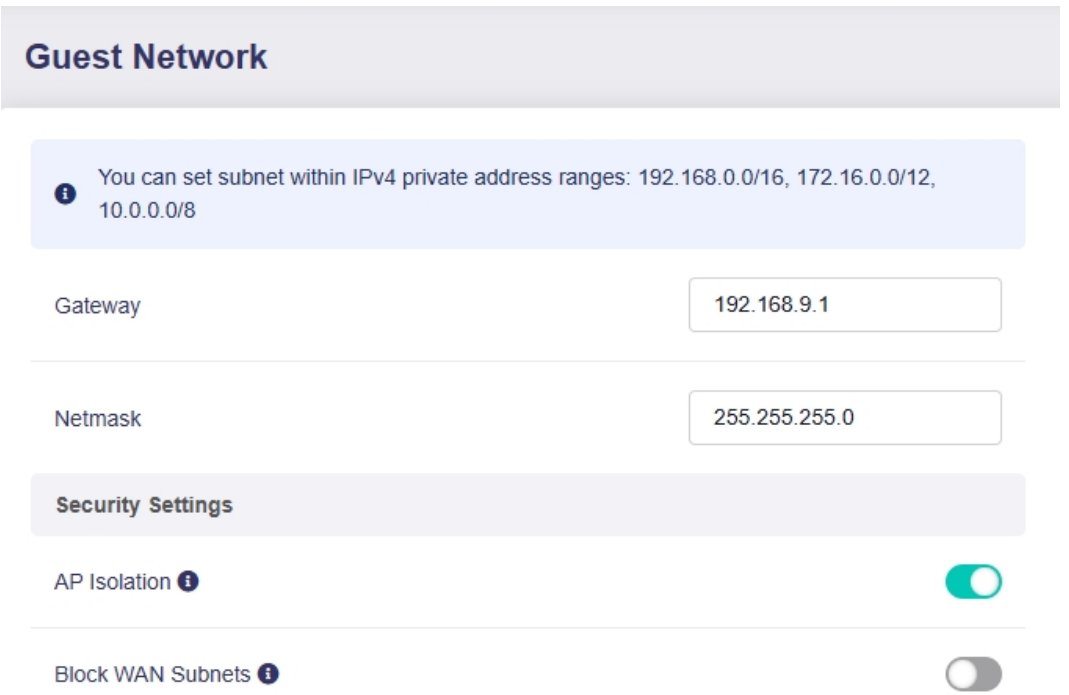
Red de invitados se refiere a una red dedicada a la que los visitantes pueden conectarse, aislándolos de su LAN principal para proteger la seguridad de su red privada.

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

Nota: El Wi-Fi para invitados no está disponible cuando Mudi 7 actúa como repetidor.

12.3.1 Configuración básica

La configuración básica incluye Puerta de enlace, máscara de red, aislamiento de AP y bloqueo de subredes WAN.



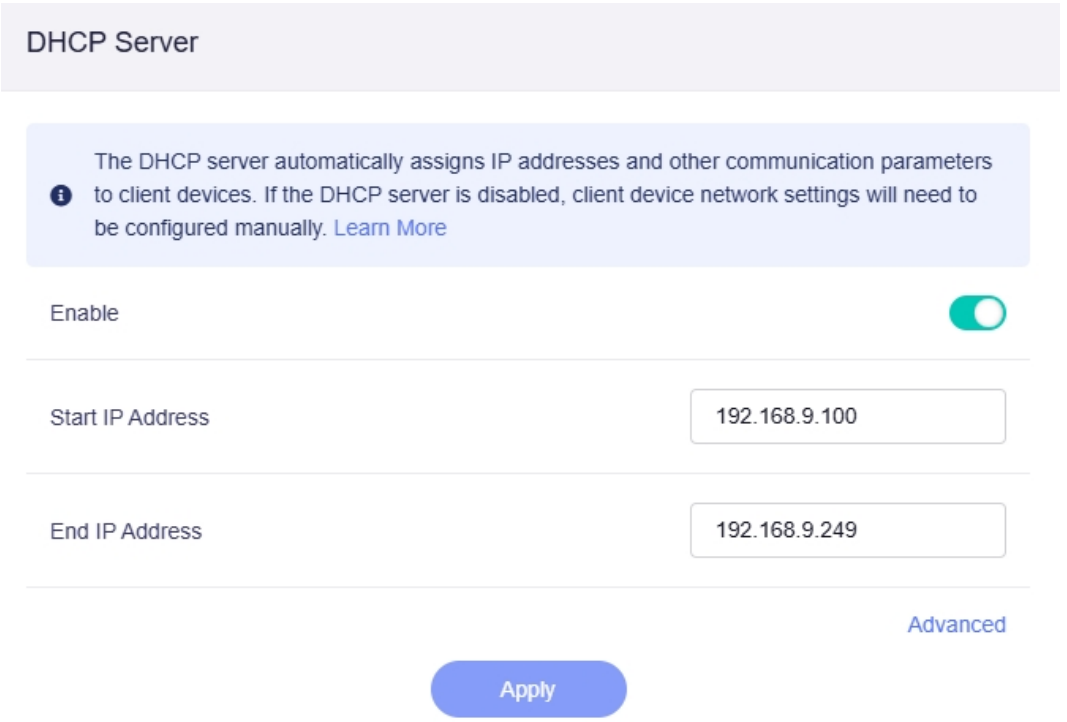
- **Puerta de enlace**: Es 192.168.9.1 de forma predeterminada y se puede cambiar según sea necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento AP**: se utiliza para aislar 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 invitada no podrá acceder a la red ascendente ni a su red correspondiente. segment.

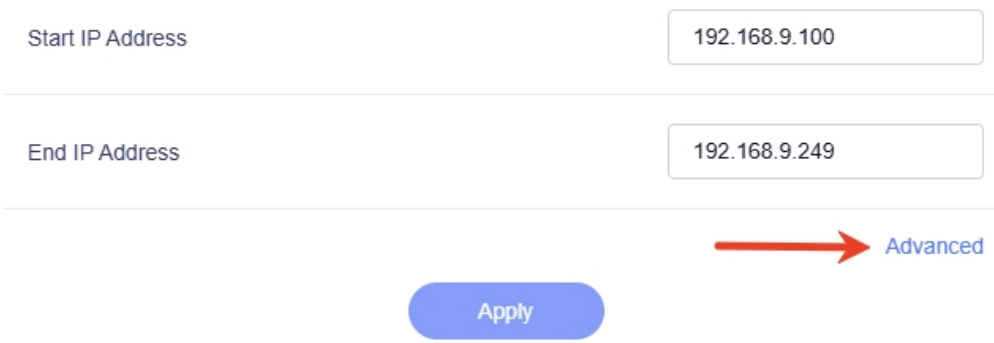
12.3.2 Servidor DHCP

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

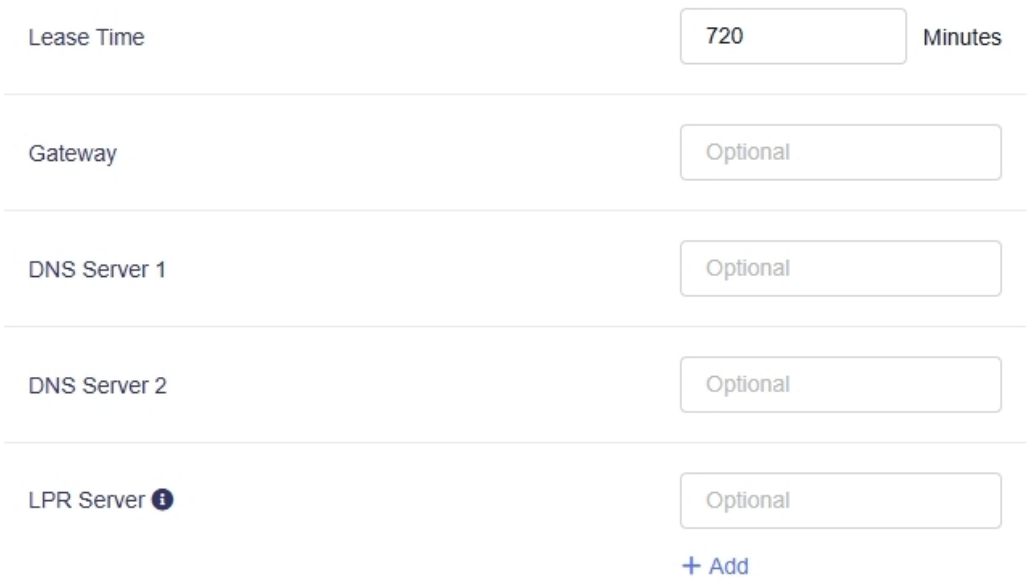
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones según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



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



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



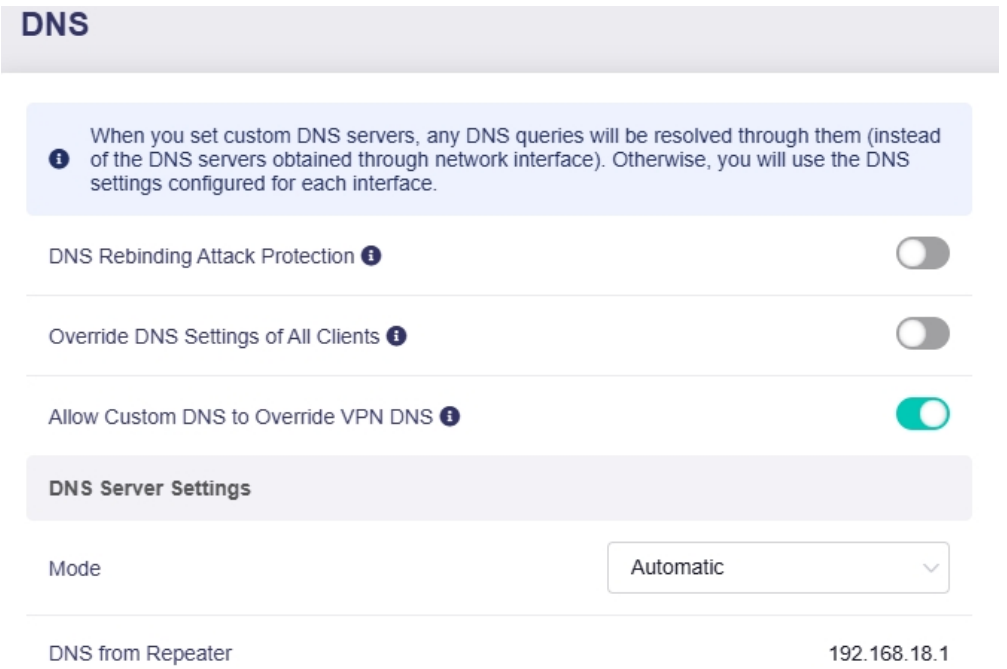
- **Tiempo de concesión**: el tiempo durante el cual un dispositivo puede usar una dirección IP asignada a través de el DHCP de la red de invitados.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la gred de cliente y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir los nombres de dominio a IP direcciones.
- **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 lugares remotos. impresoras. Se pueden configurar varios puertos LPR para impresoras.

12.4 DNS

DNS (Sistema de nombres de dominio) es un servicio de red que traduce nombres de dominio legibles por humanos (p. ej., www.google.com) en direcciones IP reconocibles por máquinas (p. ej., 142.250.185.142), lo que permite que los dispositivos se conecten a sitios web o servicios de destino.

El servidor DNS del enrutador se refiere al servicio DNS integrado en el enrutador, que proporciona traducción del nombre de dominio a IP para todos los dispositivos conectados. Por lo general, funciona de dos maneras: primero, obtiene automáticamente direcciones DNS de la red ascendente para proporcionar servicios de traducción predeterminados; en segundo lugar, los usuarios pueden configurar manualmente direcciones DNS públicas personalizadas (por ejemplo, 8.8.8.8) en el panel de administración web del enrutador’para optimizar el acceso a la redo mejorar la seguridad. Una vez configurados, todos los dispositivos conectados utilizarán este servidor DNS unificado de forma predeterminada, lo que elimina la necesidad de configurar DNS por separado en cada dispositivo.

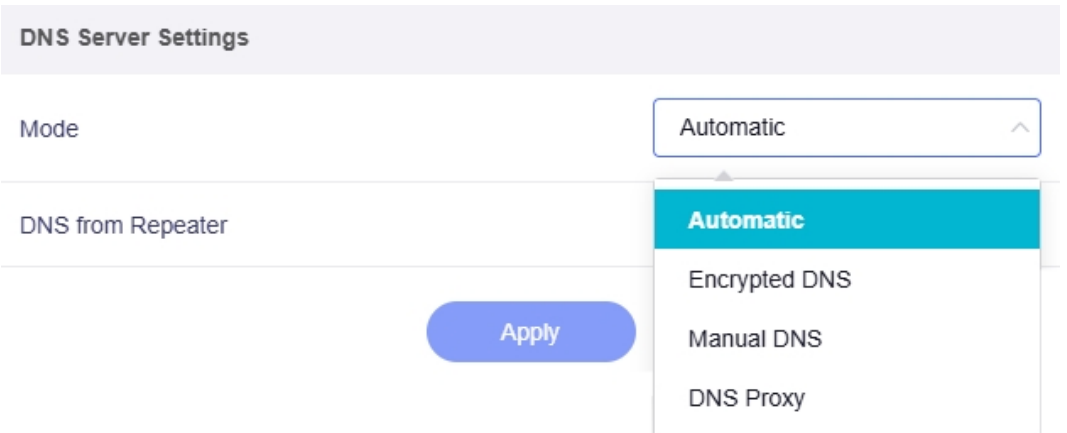
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS, incluidas opciones de seguridad, modos de servidor y reglas de prioridad de DNS para diferentes escenarios de red.



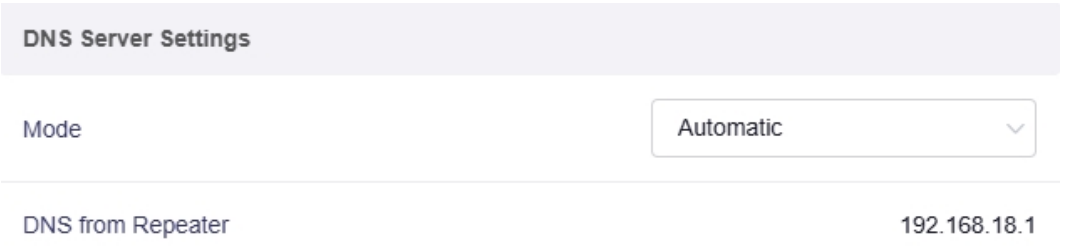
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS al bloquear intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, páginas de inicio de sesión Wi-Fi públicas).
- **Anular la configuración DNS de todos los clientes**: Si está habilitado, todos los dispositivoss será forzado para usar 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 DNS personalizadas se apliquen normalmente al usar VPN.

12.4.1 Configuración del servidor DNS

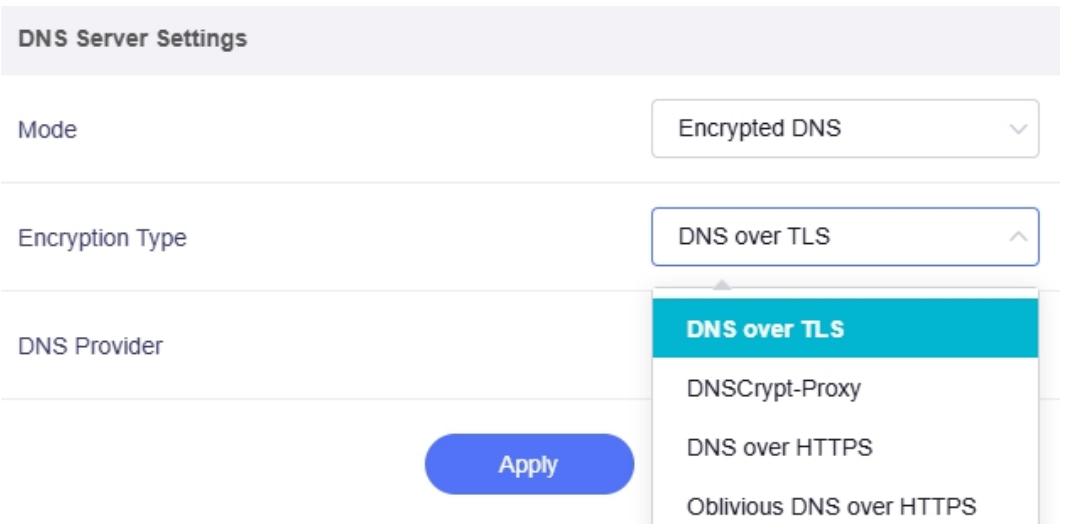
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.



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.

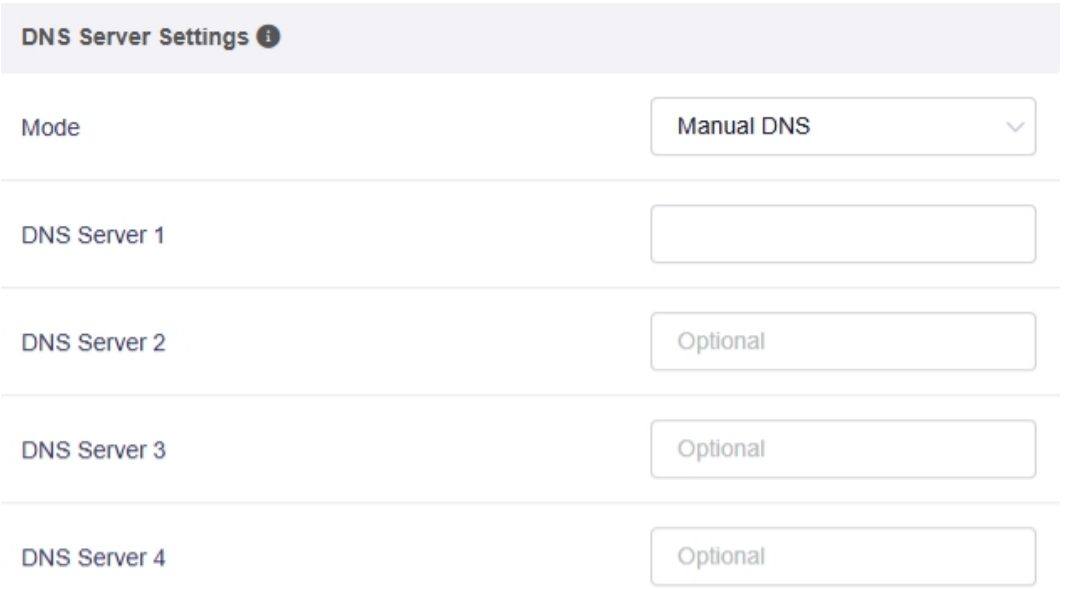


2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o manipulación.
   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a HTTPS.



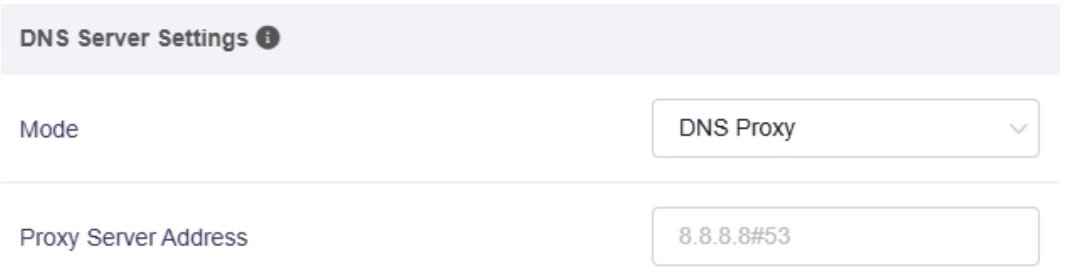
   - Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
   - Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan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

3. **DNS manual**: cuando lo 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 usar direcciones IPv6 para DNS manual, habilite IPv6 en su enrutador primero.

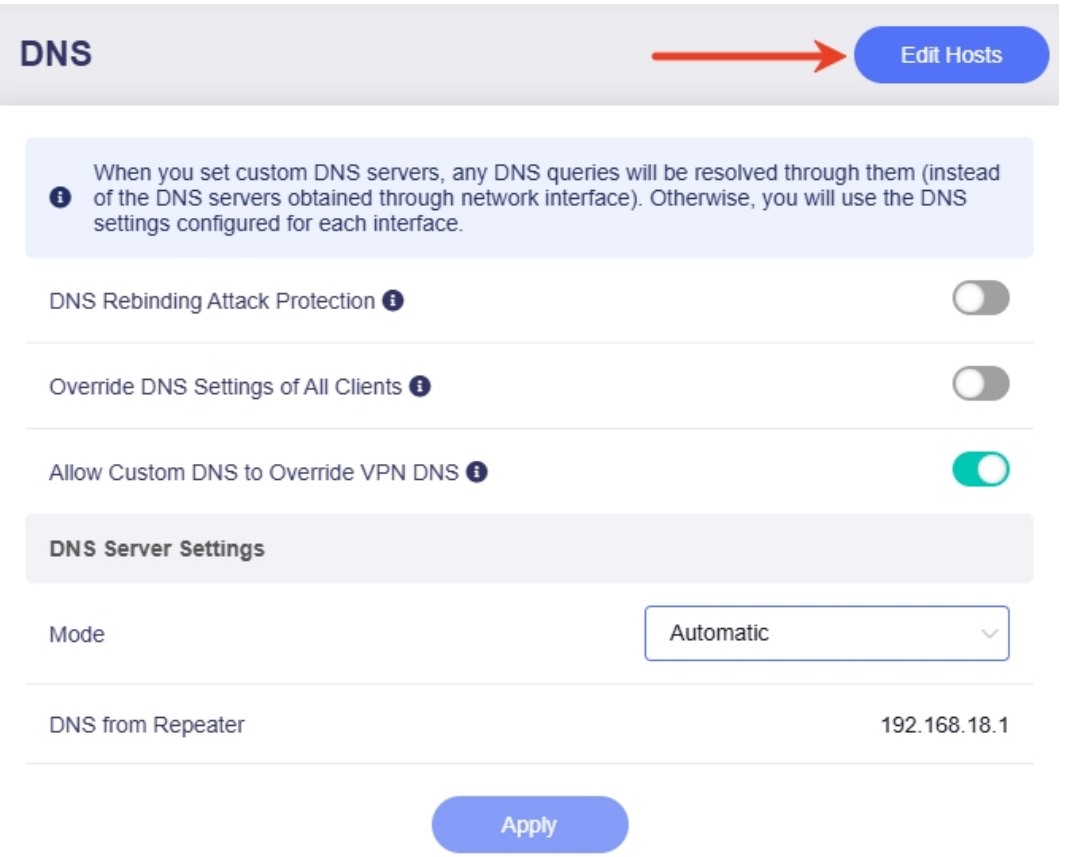
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permiteresolución a través del entorno de red del proxy para necesidades de acceso específicas.



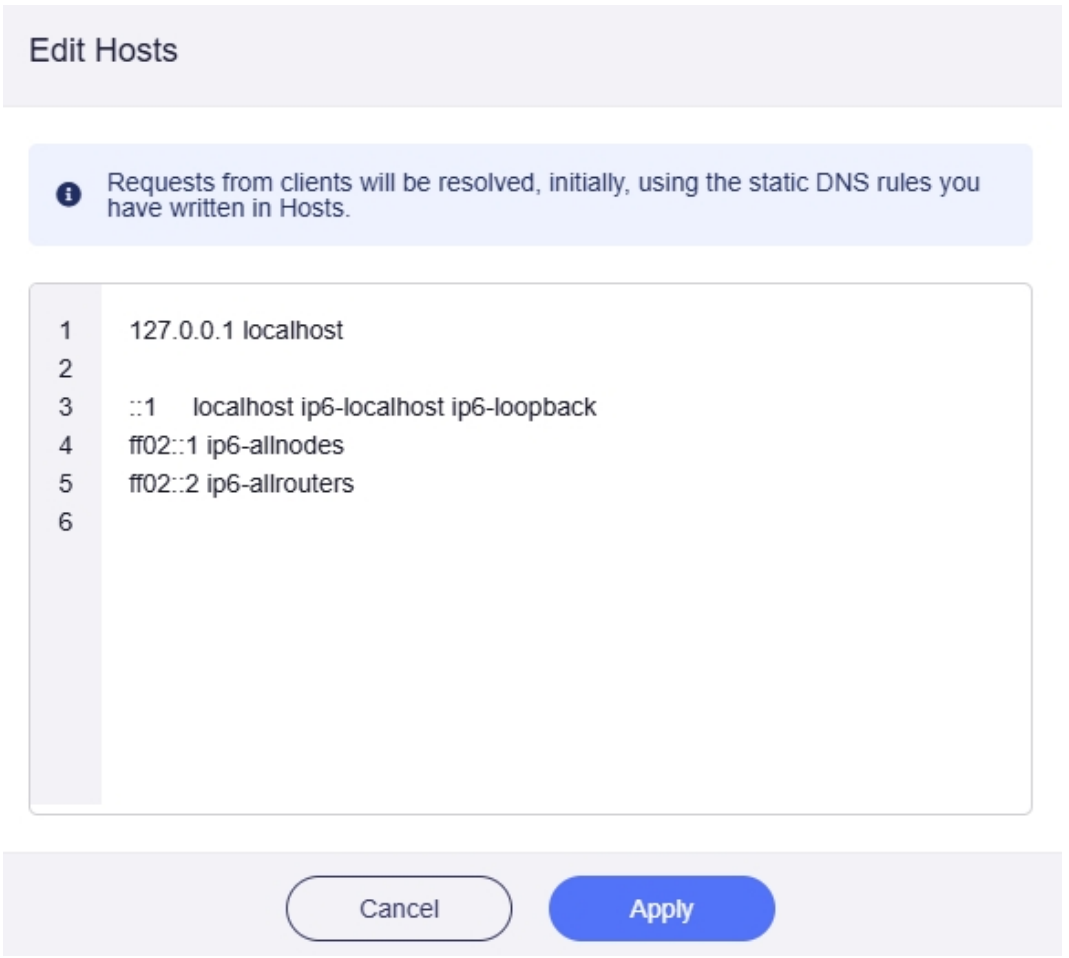
12.4.2 Editar hosts

Puede definir reglas de resolución de DNS estáticas según sea necesario.

En la página DNS, haga clic en **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.

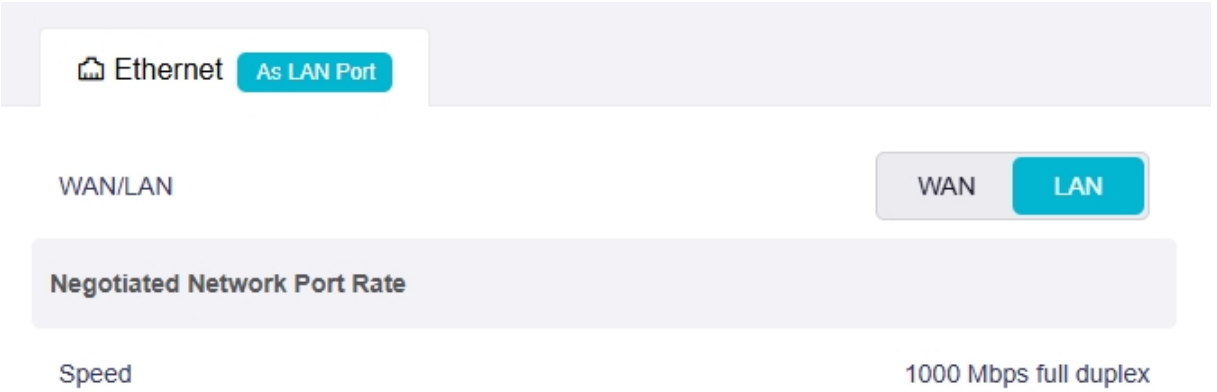

Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 Puerto Ethernet

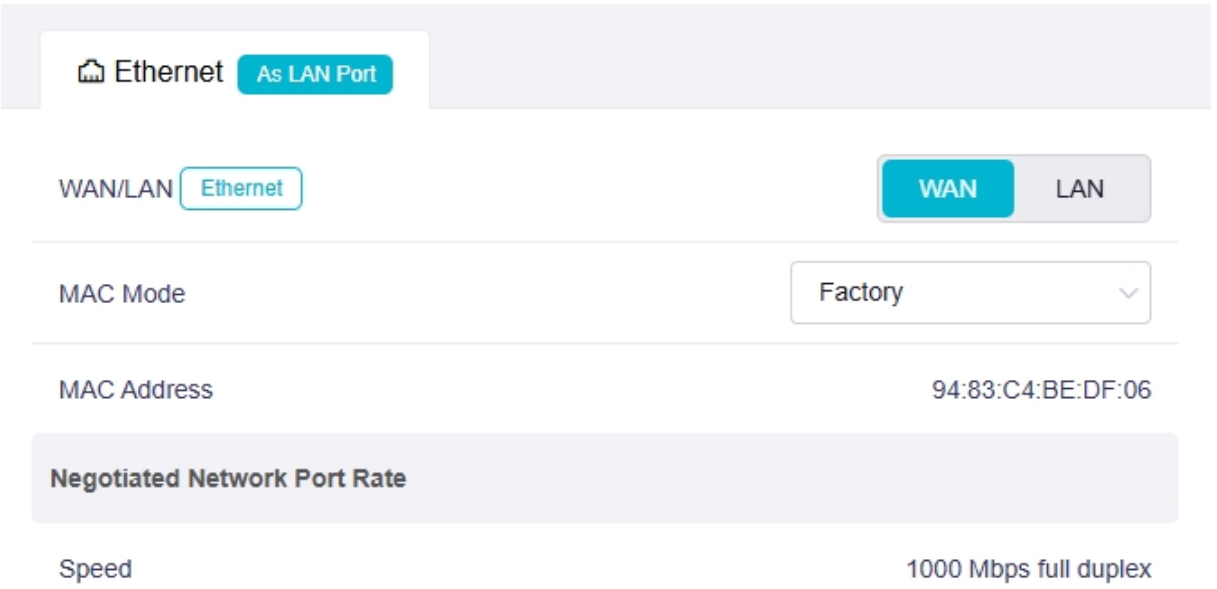
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Ethernet Puerto**. Esta página le permite administrar los puertos Ethernet del enrutador'.

Mudi 7 está equipado con un puerto Ethernet. Este puerto Ethernet está predeterminado en LAN y usted puede ajustar su función de puerto entre WAN y LAN.

Cuando actúa como **LAN**, la página muestra la función del puerto y la tarifa negociada.



Cuando actúa como **WAN**, la página muestra la función del puerto, el modo MAC, la dirección MAC y la velocidad negociada.



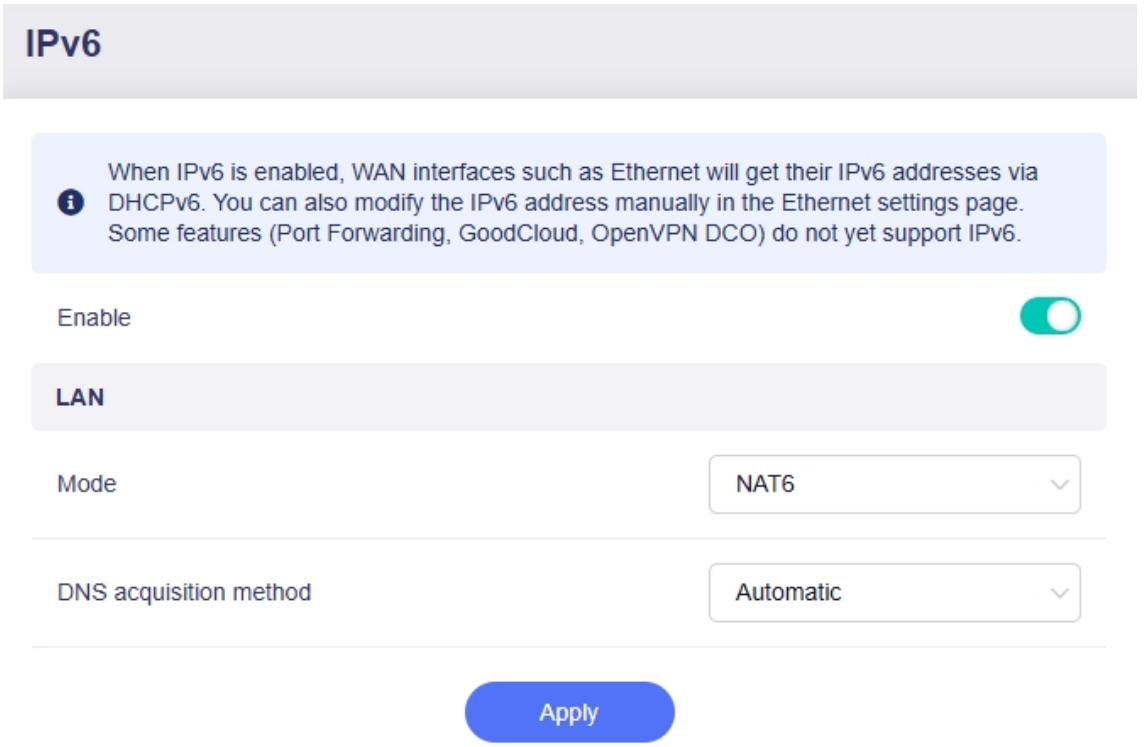
Nota: La velocidad negociada se muestra solo cuando hay un cable Ethernet conectado. Depende tanto del puerto Ethernet como del cable Ethernet.

12.6 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.

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



Nota: Algunas características (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 conectividad problemas.

12.6.1 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.
- **Passthrough**: 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 sadecuado 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.

12.6.2 Método de obtención de DNS

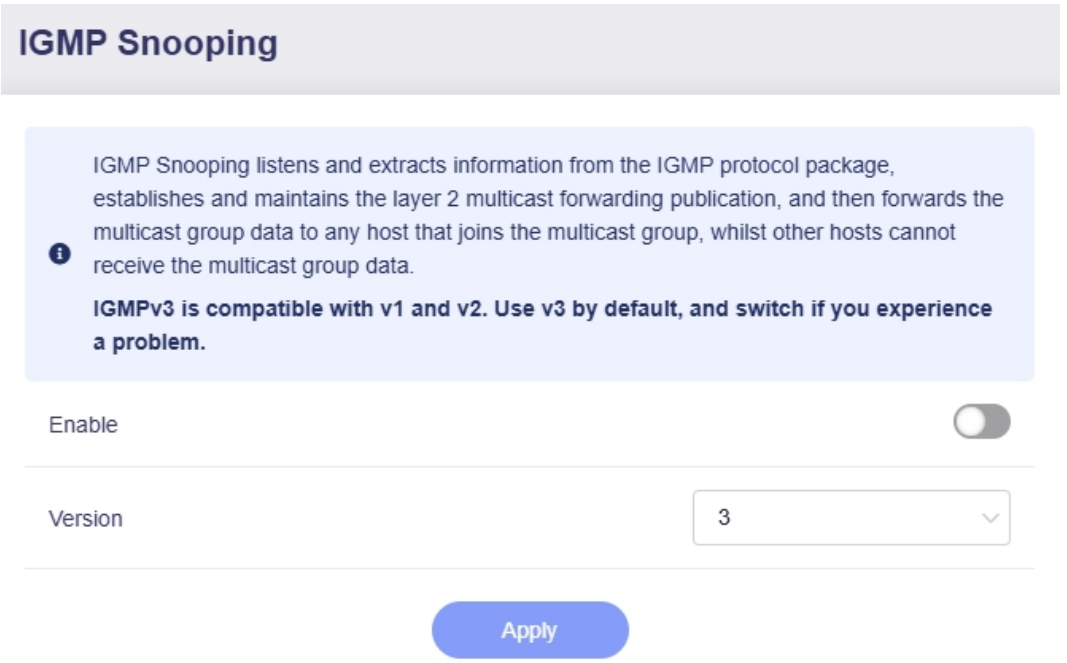
Determina cómo el enrutador obtiene las direcciones del servidor DNS IPv6. Hay dos opciones: Automático y Manual.

- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 dinámicamente (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.

12.7 Inspección IGMP

IGMP Snooping escucha el paquete de protocolo IGMP y extrae el correspondiente información, 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 los datos del grupo de multidifusión.

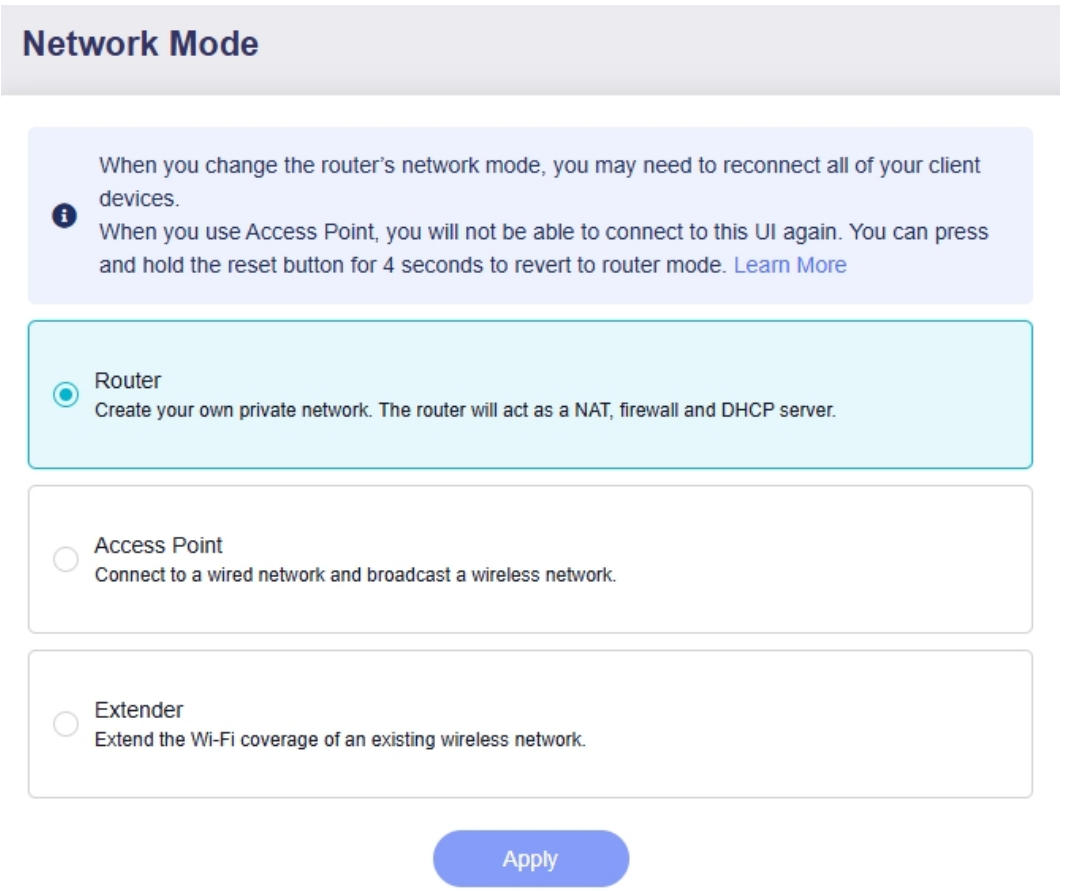
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para usar la función de multidifusión en su enrutador según sea necesario.



12.8 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 el panel de administración web de su enrutador' y navegue a **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 de Wi-Fi en grandes espacios para permitir que más dispositivos accedan a la red. En este modo, el enrutador desactiva sus funciones NAT y DHCP, funcionando exclusivamente como un transmisor y conmutador de señal inalámbrica 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.

Nota:

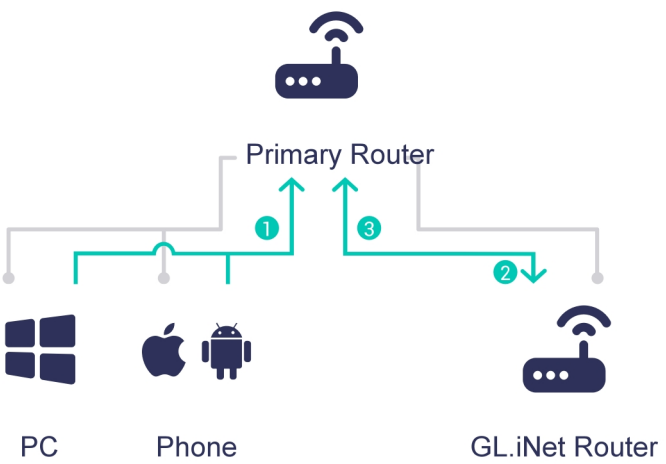
1. Cuando se cambia el modo de red, todos los dispositivos cliente se volverán a conectar al enrutador para una conectividad de red estable.
2. **En el modo de punto de acceso, no podrá acceder al administrador web panel usando la dirección IP original**. En su lugar, debe iniciar sesión en el enrutador 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, 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 dirección, Red de invitados, DNS, Puerto Ethernet, IPv6, Puerta de enlace directa, Vigilancia IGMP, aceleración de red, configuración NAT.

12.9 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 reconfigurarlo-. Al conectar el enrutador GL.iNet al enrutador principal mediante un cable Ethernet, los usuarios pueden agregar funciones avanzadas en 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 un sistema de red intermedio, 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 para dispositivos cliente específicos según sea necesario.



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

- **Gray lines** ilustran la topología de conexión física: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conecta 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.

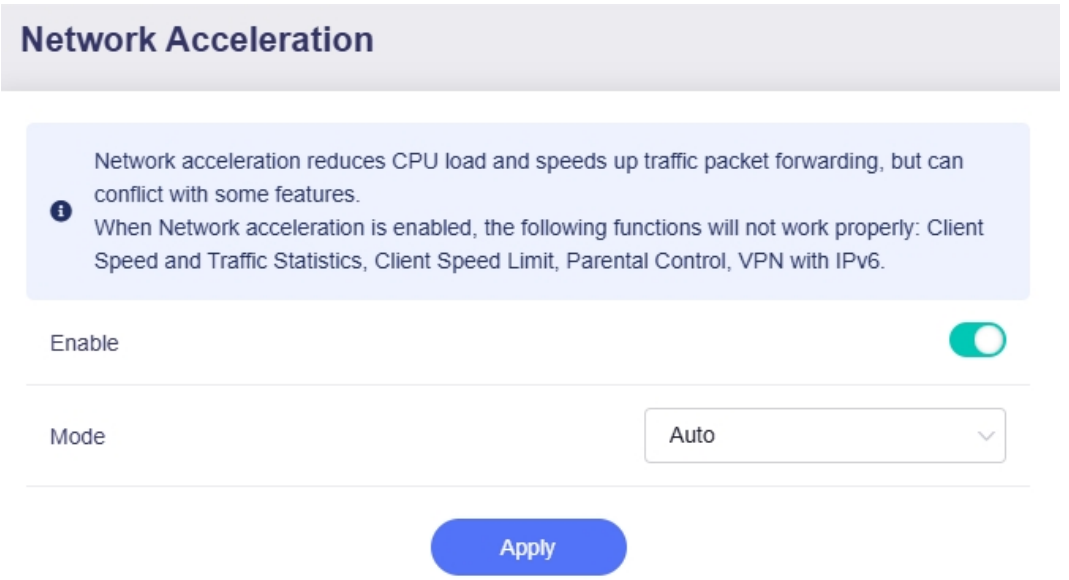
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas que indican el orden del flujo de tráfico:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía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

Puedes habilitar Drop-in Gateway para todos o dispositivos específicos conectados a su enrutador principal. Consulte este enlace para obtener más información detalles.

12.10 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 el modo de aceleración entre Auto, Aceleración de hardware y Aceleración de software.



- **Auto**: cambia automáticamente entre los dos modos de aceleración según el uso real.
- **Aceleración de hardware**: 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**: se basa en 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.

Capítulo 13

Control de flujo

Este capítulo presenta a función de control de flujo: Control parental.

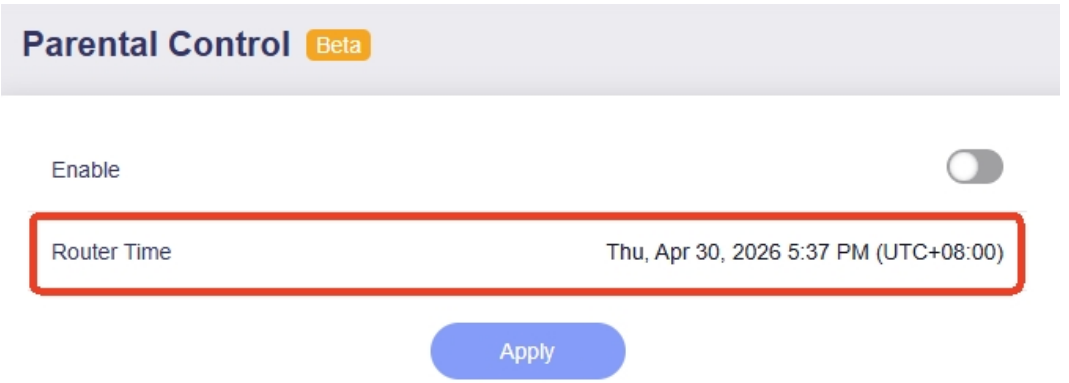
13.1 Control parental

El control parental es una forma de mantener a los niños seguros en línea bloqueando sitios web inapropiados y limitando el tiempo que usan 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.

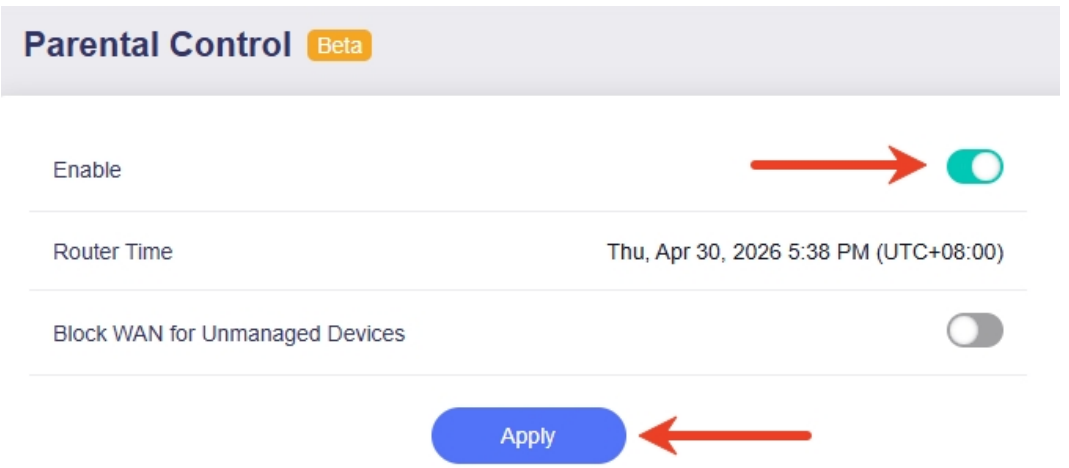
13.1.1 Configuración rápida

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

1. Inicie sesión en el enrutador’s web admin panel y vaya a **CONTROL DE FLUJO** > **Control parental.** Asegúrese de que la hora del enrutador sea precisa. Si no, vaya a **SISTEMA** > **Zona horaria** para sincronizarla 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.



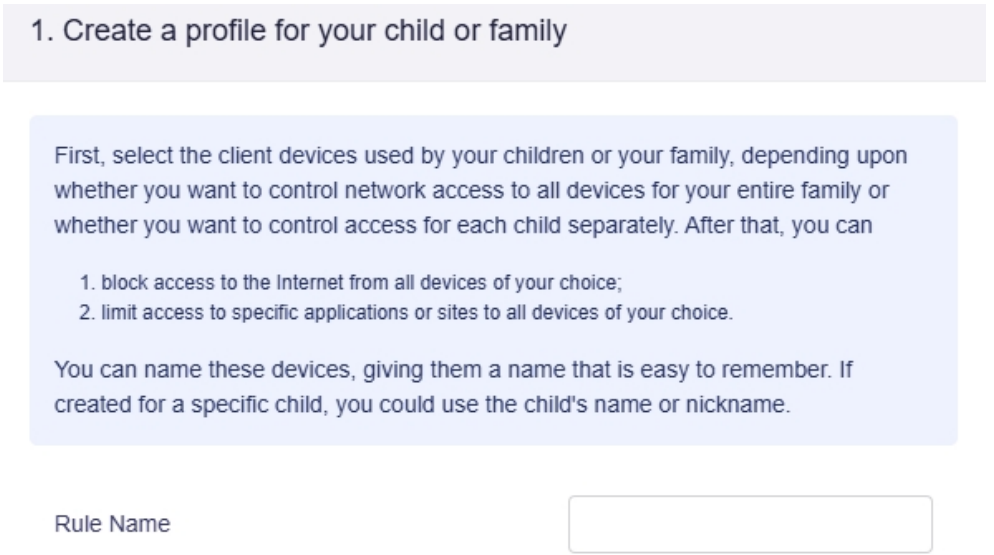
- **Bloquear WAN para dispositivos no administrados**: Bloquea el acceso a Internet para todos los dispositivos que no están en la lista de Control parental.

Aquí tienes un caso de uso para tu referencia.

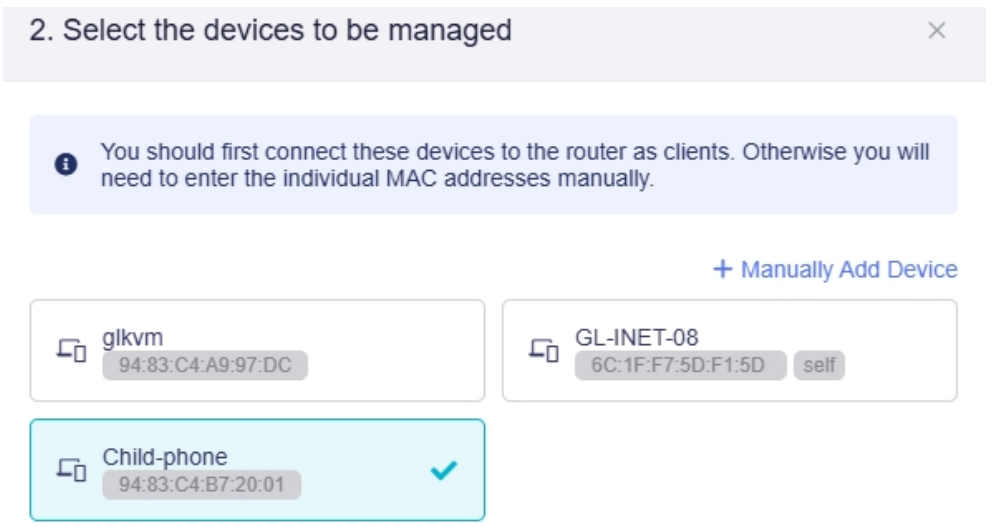
Escenario: Los dispositivos en el perfilis solo pueden acceder a Internet para estudiar de 8 a.m. a 11 a.m. de lunes a viernes y para jugar de 6 p.m. a 8 p.m. los fines de semana. El acceso a Internet está bloqueado de forma predeterminada en todos los demás momentos.

Pasos de configuración:

1. Cree un perfil y personalice un nombre.



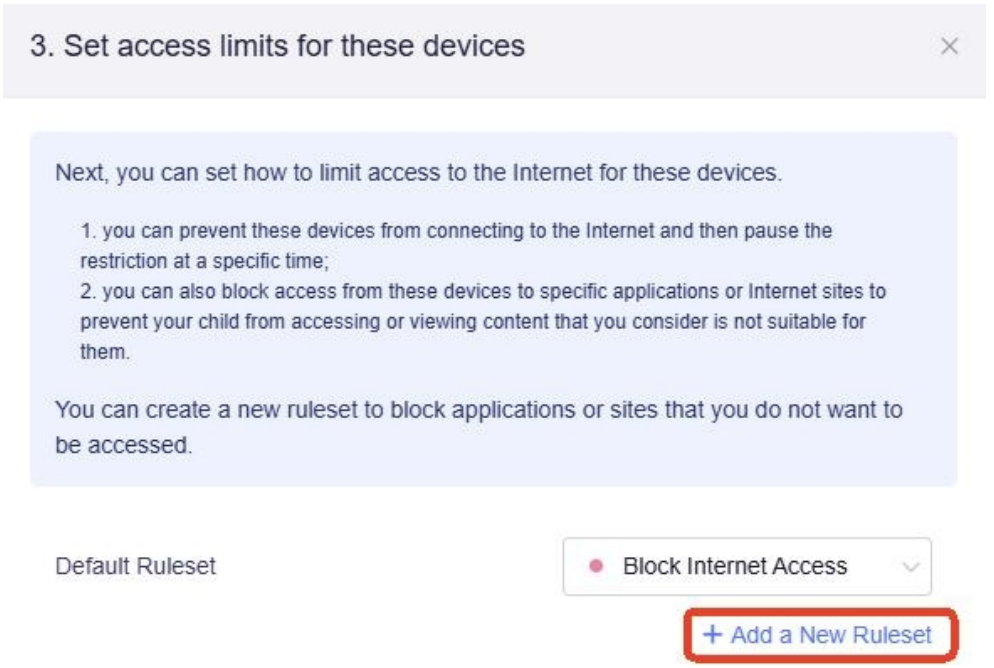
2. Seleccione los dispositivos que desea administrar. Conéctelos primero al enrutador. Si no se han conectado al enrutador, agréguelos manualmente ingresando sus direcciones MAC.



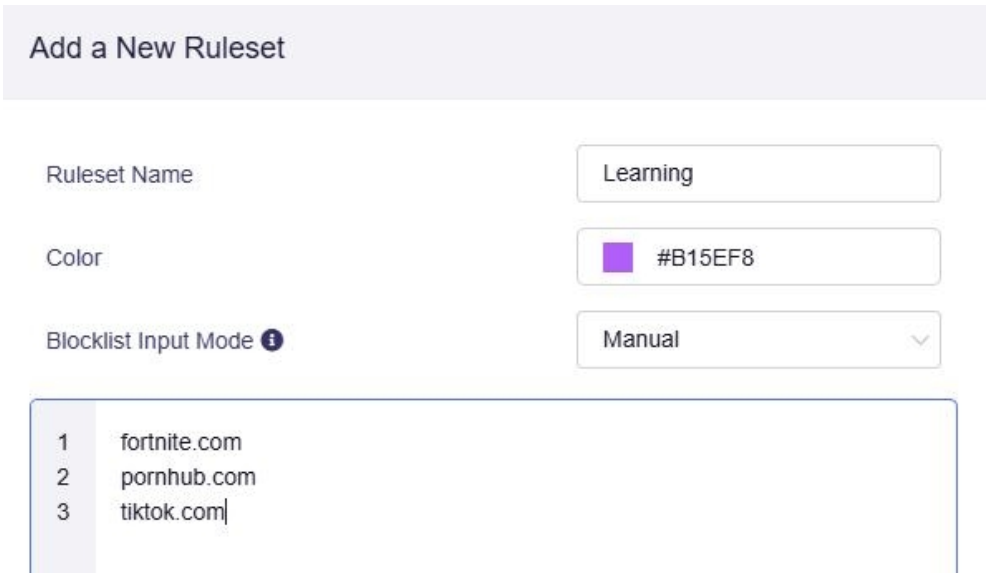
3. Establezca el límite de acceso.

   Hay dos conjuntos de reglas predeterminados: **Bloquear el acceso a Internet** y **Sin límite**.

   Haga clic en **Agregar un nuevo conjunto de reglas** para crearcrear dos conjuntos de reglas más para su uso posterior: **Aprendizaje** y **Reproducir**.

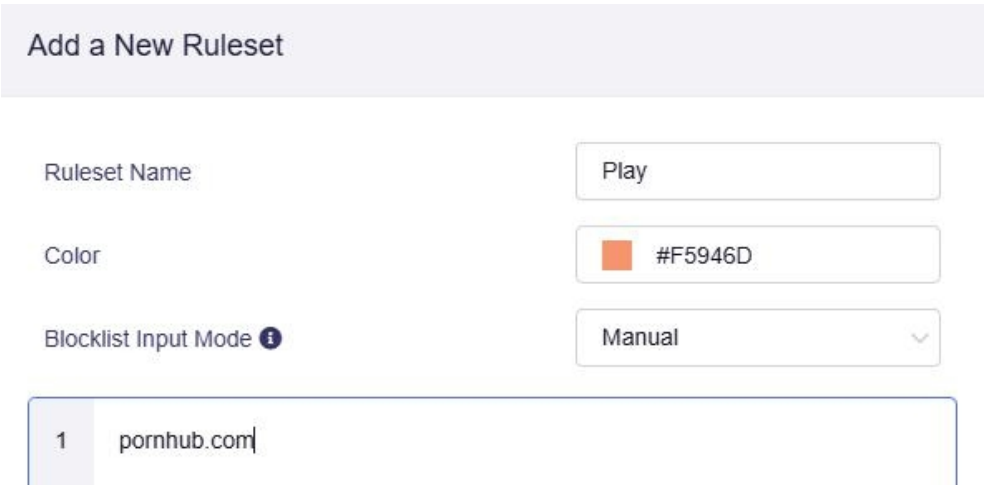


   Especifique el nombre del conjunto de reglas (p. ej., Aprendizaje) y color, ingresa a la websitios tpara bloquear, tluego haga clic en **Aplicar**.

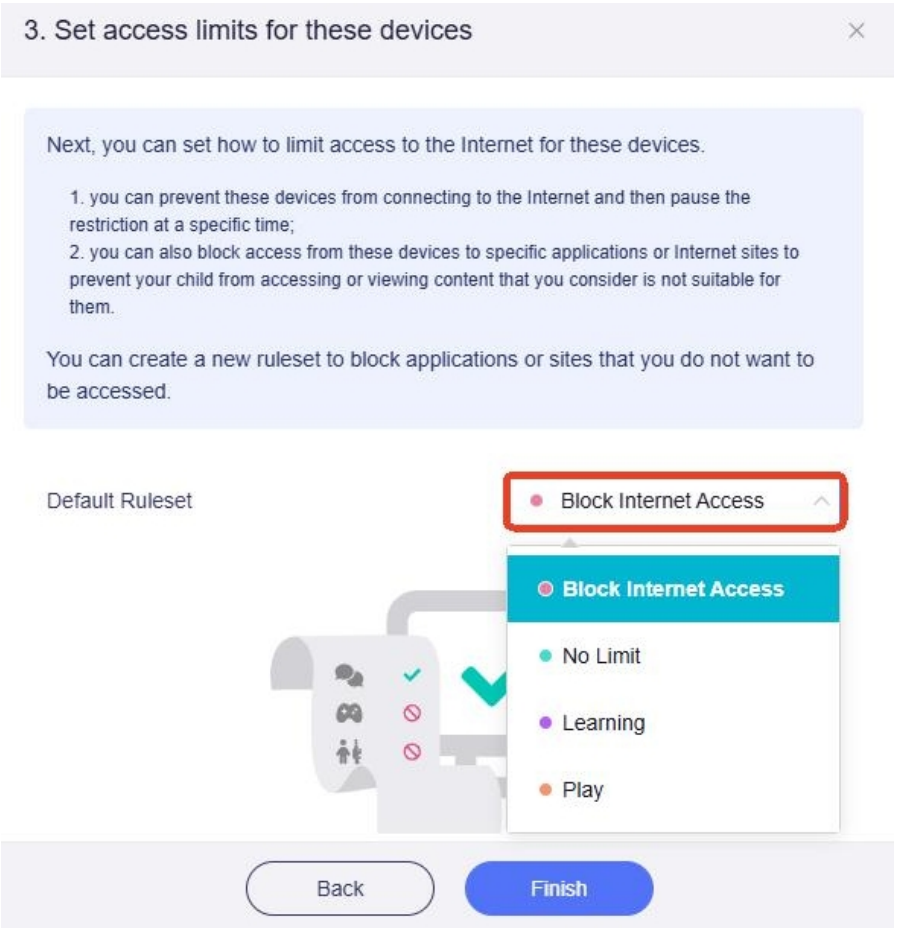


Nota: Los nombres de dominio ingresados en la lista de bloqueo deben incluir sus subdominios. Por ejemplo, si se ingresa "ejemplo.com", también incluye cualquier subdominio, como "subdominio.example.com".

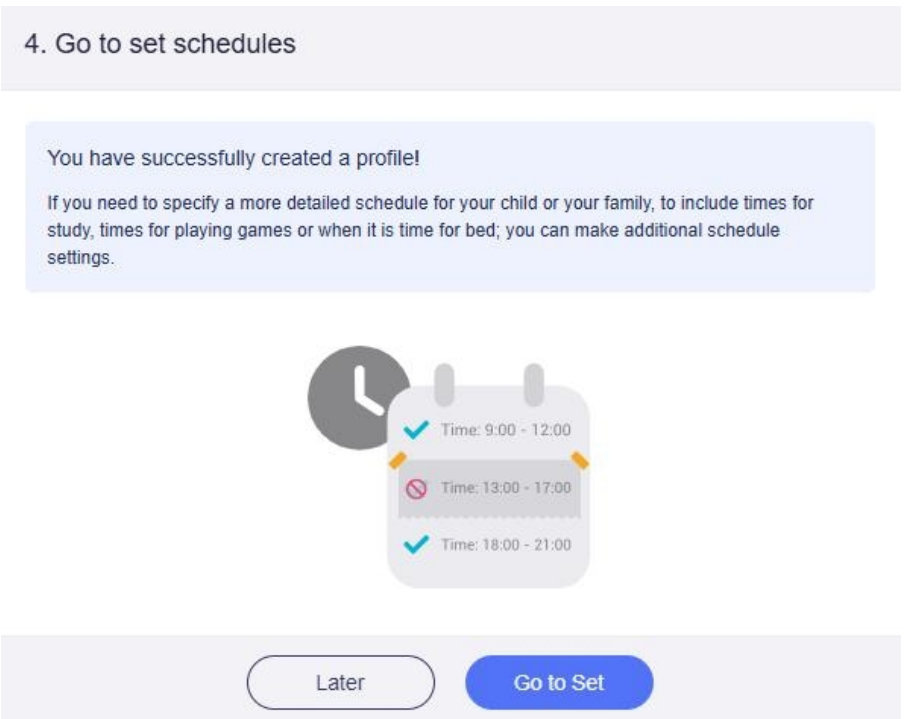
Del mismo modo, cree otro conjunto de reglas. Especifique el nombre del conjunto de reglas (por ejemplo, Reproducir) y el color, ingrese los sitios web que desea bloquear y luego haga clic en **Aplicar**.



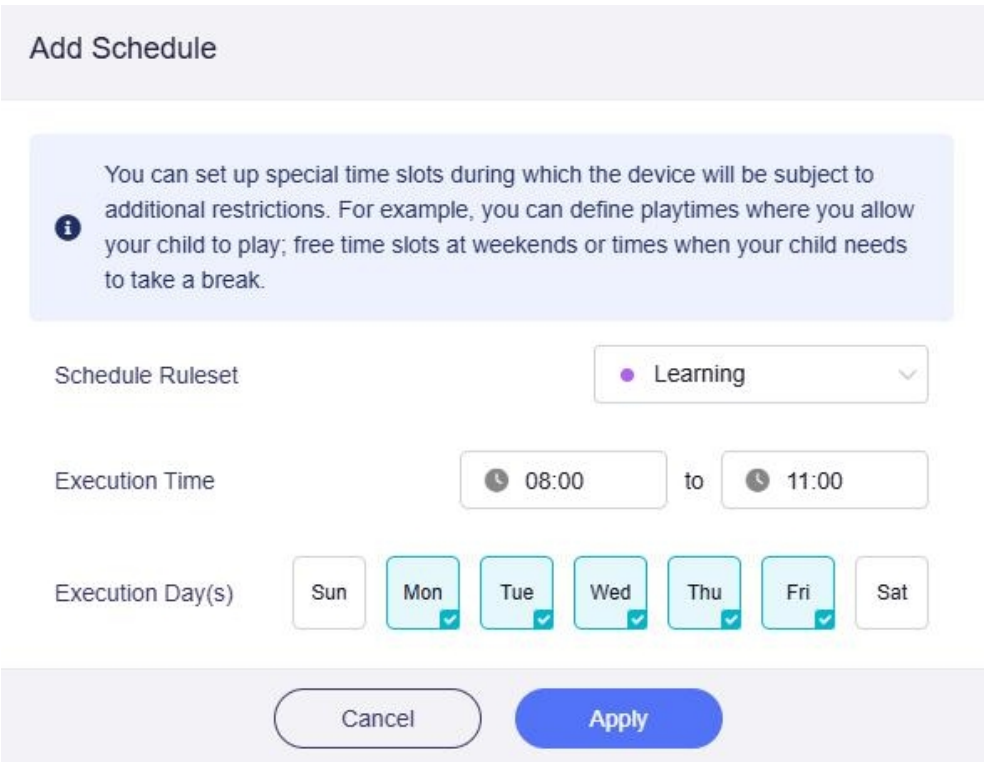
Al aplicared, habrá un total de cuatro conjuntos de reglas. Sseleccione **Bloquear acceso a Internet** como el **Conjunto de reglas predeterminado** y haga clic en **Finalizar**.



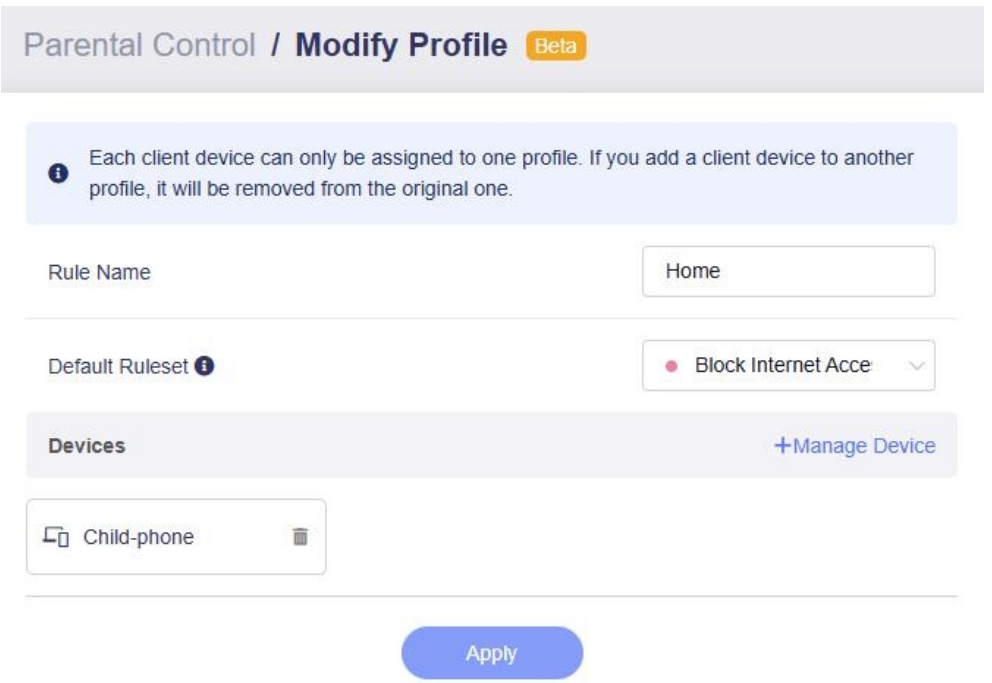
4. A continuación, establezca la programación para su perfil. Haga clic en **Ir a conjunto**.



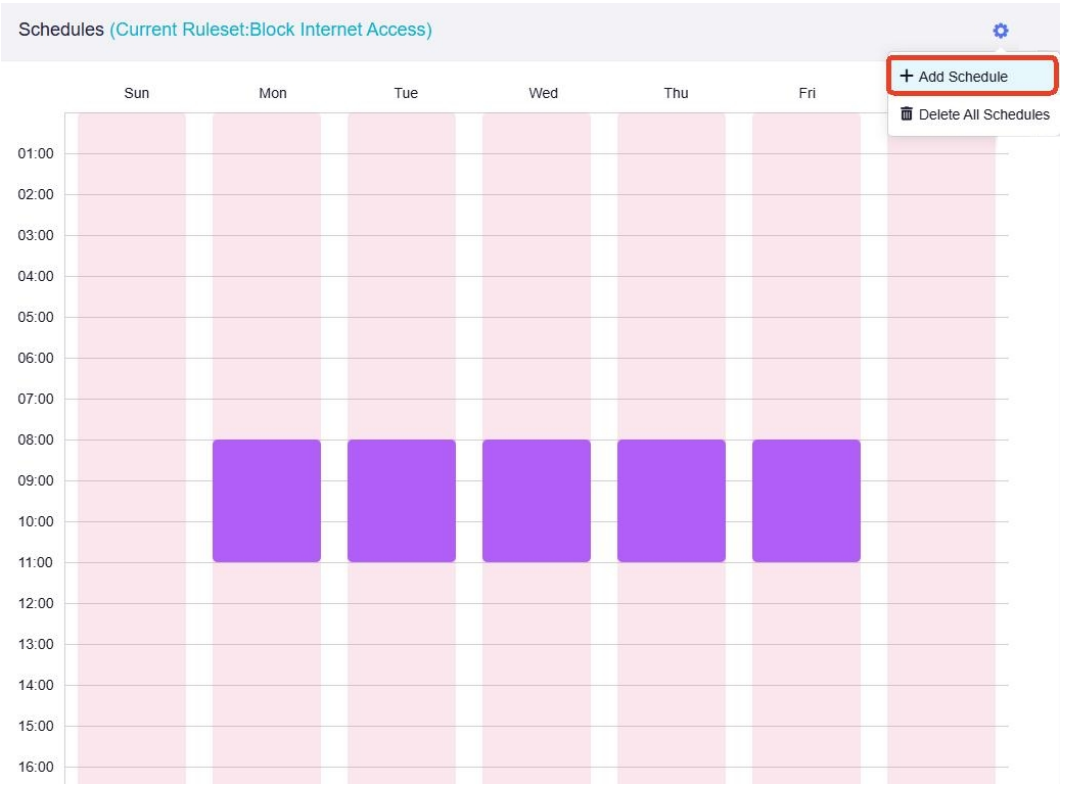
Agregue el **Aprendizaje** conjunto de reglas al cronograma. Establezca el **Hora de ejecución** de 8 a. m. a 11 a. m. de lunes a viernes y luego haga clic en **Aplicar**.



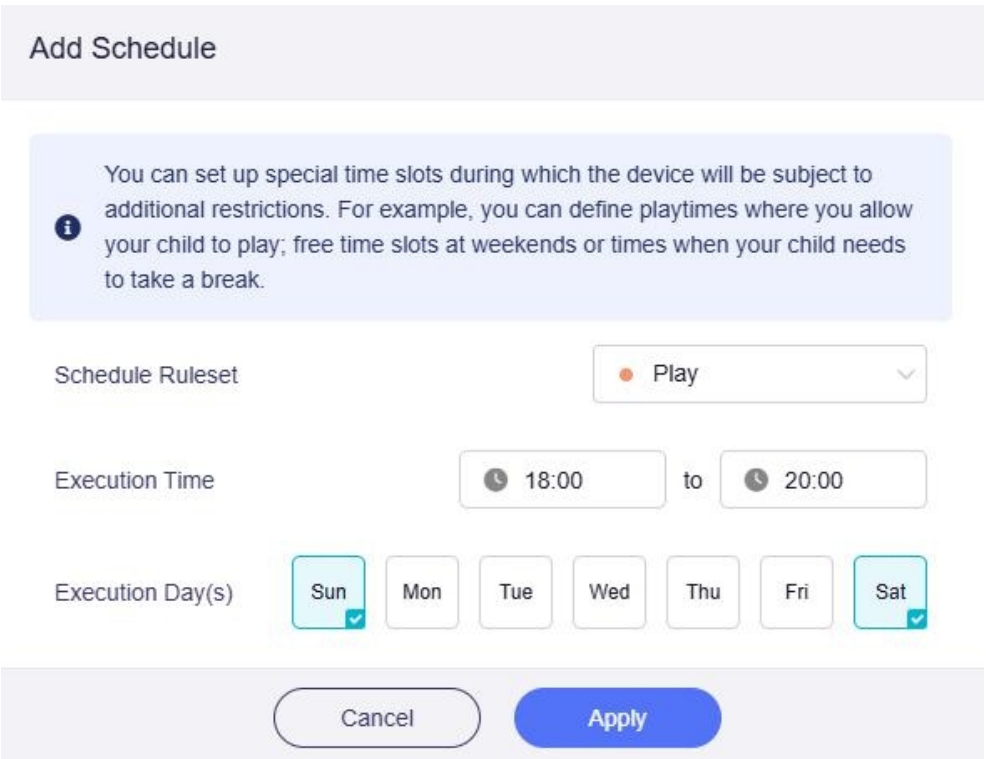
5. Será redireccionado a la página de edición del perfil creado.



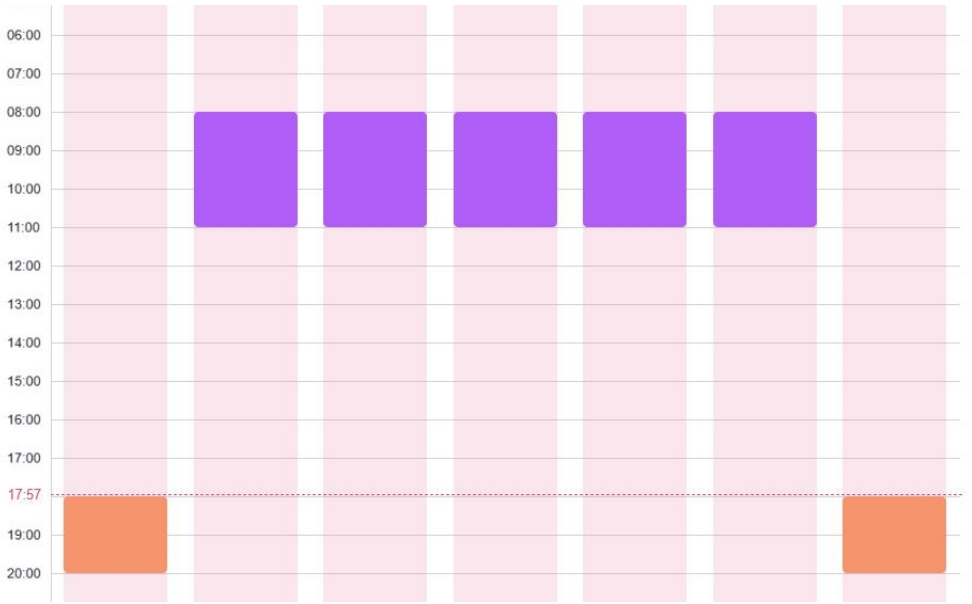
Muévase al final y podrá Verá que se ha creado un horario. Haga clic en el ícono de ajustes en la parte superior derecha y seleccione **Agregar programación**.



6. Agregar otro conjunto de reglas **Reproducir** al cronograma. Establezca el **Tiempo de ejecución** de 6:00 p. m. a 8:00 p. m. los fines de semana y luego haga clic en **Aplicar**.



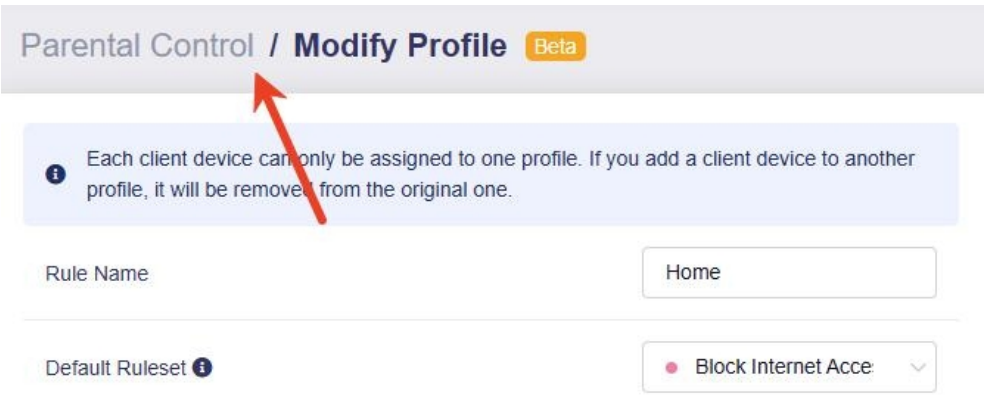
El conjunto de reglas de Play se agregará al cronograma.



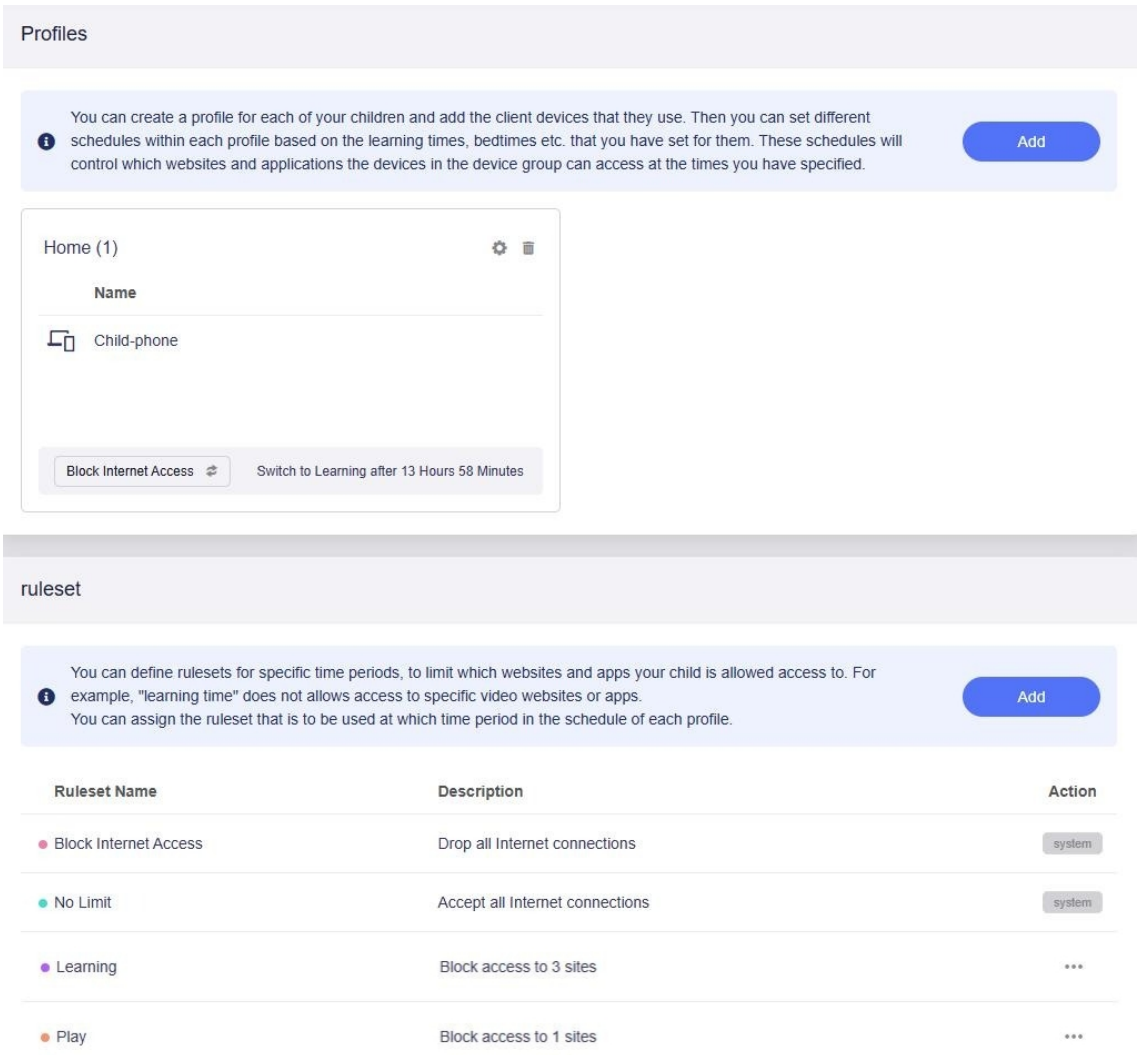
Consejos:

- La línea discontinua roja indica la hora actual.
- Ypuede modificar el tiempo de ejecución haciendo clic en en cierto conjunto de reglas en la programación.

7. Click **Control parental** en la parte superior para regresar a la página Control parental.



Verá 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 según sea necesarioed.


Profiles
You can create a profile for each of your children and add the client devices that they use. Then you can set different schedules within each profile based on the learning times, bedtimes etc. that you have set for them. These schedules will control which websites and applications the devices in the device group can access at the times you have specified.
Add
Home (1)
Name
Child-phone
Block Internet Access
Switch to Learning after 13 Hours 58 Minutes
ruleset
You can define rulesets for specific time periods, to limit which websites and apps your child is allowed access to. For example, "learning time" does not allows access to specific video websites or apps.
You can assign the ruleset that is to be used at which time period in the schedule of each profile.
Add
Ruleset Name
Description
Action
Block Internet Access
Drop all Internet connections
system
No Limit
Accept all Internet connections
system
Learning
Block access to 3 sites
Play
Block access to 1 sites

13.1.2 Solución de problemas

Si los ajustes configurados no surten efecto, verifique las siguientes causas posibles.

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.

   Si bien el dominio público de un sitio web 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 una dirección MAC aleatoria para cada conexión de red, que impides que las reglas de acceso entren en vigor. Deshabilitar aleatorio MAC dirección en el dispositivo de destino y luego vuelva a agregar el dispositivo a su perfil.

Capítulo 14

Seguridad

Este capítulo administra la seguridad de la red, como el reenvío de puertos, el acceso administrativo y el modo NAT para equilibrar el acceso a la red y seguridad.

14.1 Reenvío de puertos

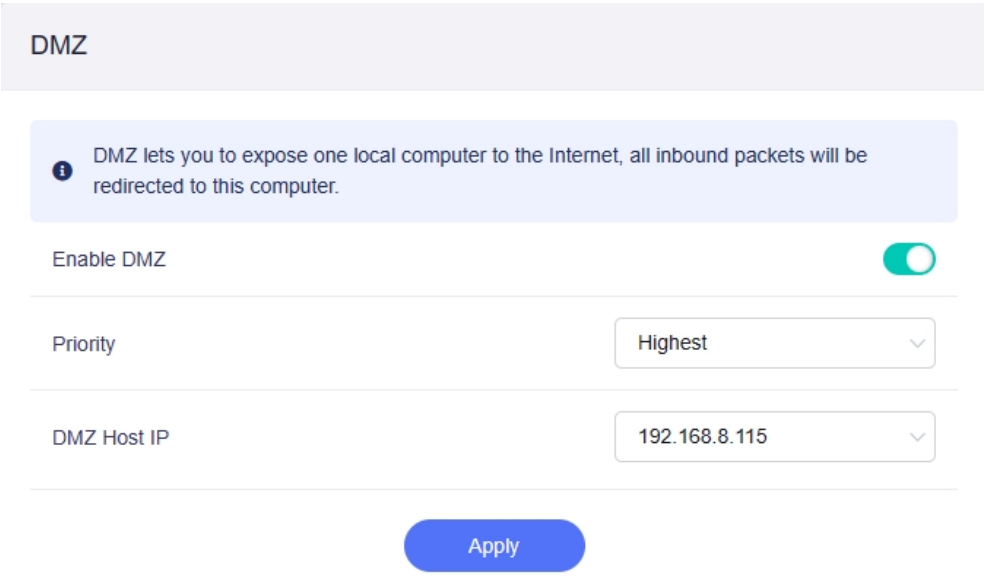
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un solo dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos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

14.1.1 DMZ

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

Siga los pasos a continuación para habilitar DMZ según sea necesario.

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



- **Prioridad**: configúrelo como Más alto o Más bajo. 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.

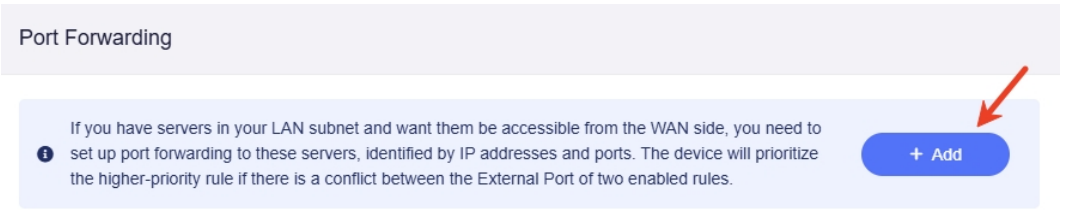
- **IP del host DMZ**: seleccione la dirección IP interna de el dispositivo que recibirá todos los paquetes entrantes.

14.1.2 Reenvío de puertos

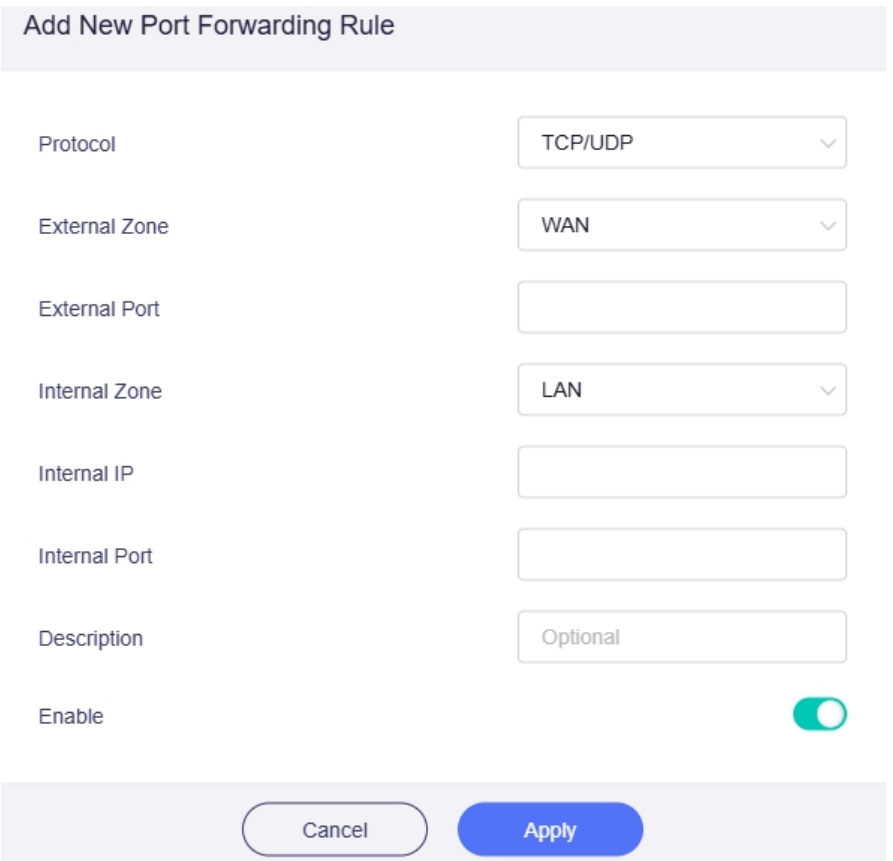
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

Si necesitaconfigurar el reenvío de puertos, siga los pasos a continuación.

1. Inicie sesión en el panel de administración web de su enrutador, vaya a **SEGURIDAD** > **Reenvío de puertos** > **Reenvío de puertos** sección y haga 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**.



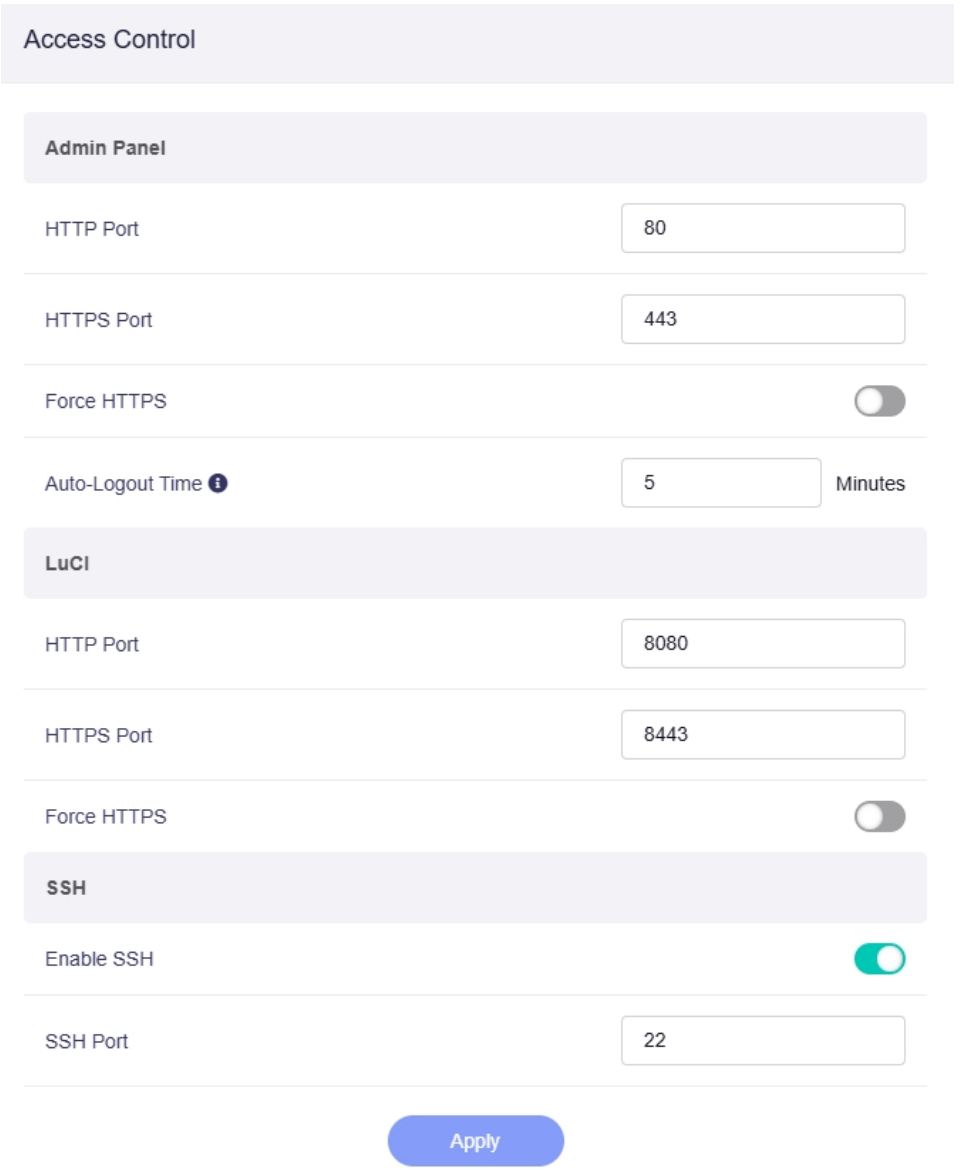
- **Protocolo**: El protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, y LAN.
- **Puerto externo**: El número de puertos externos. Introduzca aquí un número de puerto específico. El rango de puertos es 1–65535. Puede configurar un solo 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, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server 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 Acceso de administrador

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SEGURIDAD** > **Acceso de administrador**. Esta página permite usted configurar el acceso local del enrutador, el acceso remoto HTTPS/SSH y administrar los puertos abiertos en el enrutador, protegiendo su enrutador y su red.

14.2.1 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 el 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 una conexión HTTPS segura.
- **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, desde 1 minuto hasta 3 horas.

LuCI

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

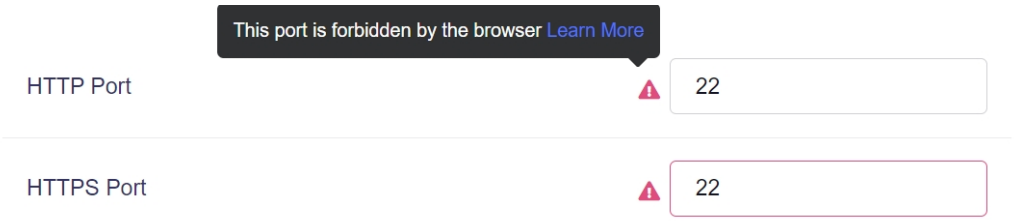
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para un acceso HTTPS seguro a la interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, el acceso a la interfaz LuCI se aplica para utilizar una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

SSH

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

Nota:

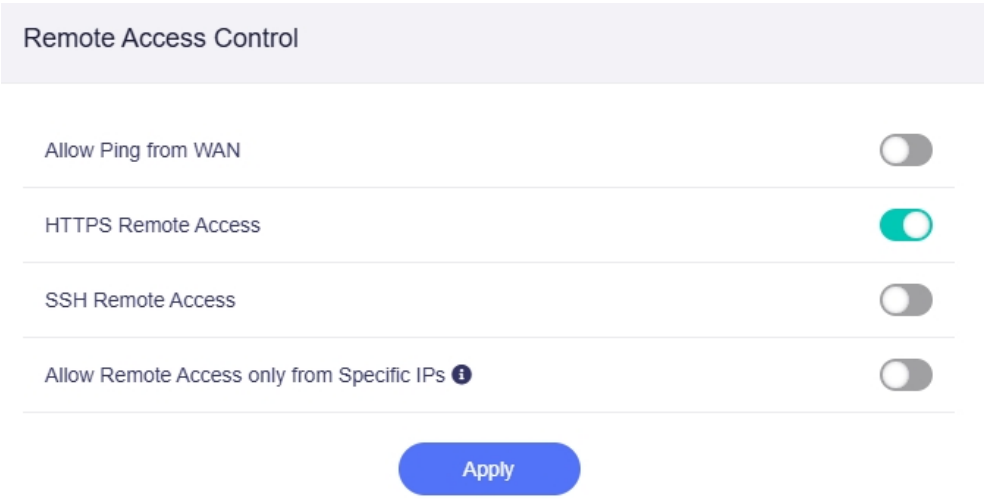
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), Aparecerá un mensaje que indicará "Este puerto está prohibido por el navegador".



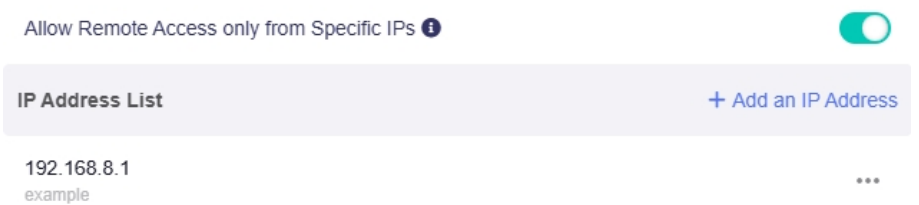
2. Si el número de puerto se modifica en el firmware, deberá ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.

14.2.2 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 accesibilidad remota y seguridad de la red.

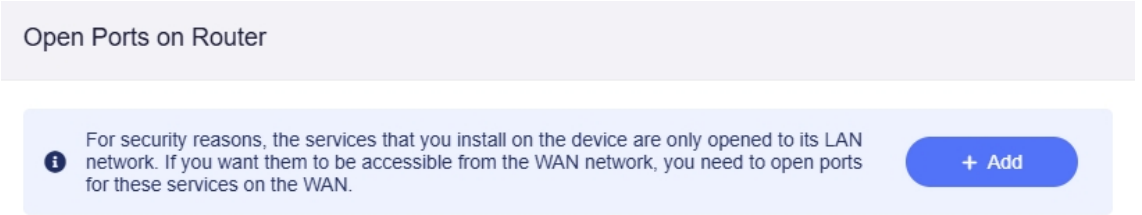


- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutadorpuede ayudar a los usuarios a comprobar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El acceso 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.

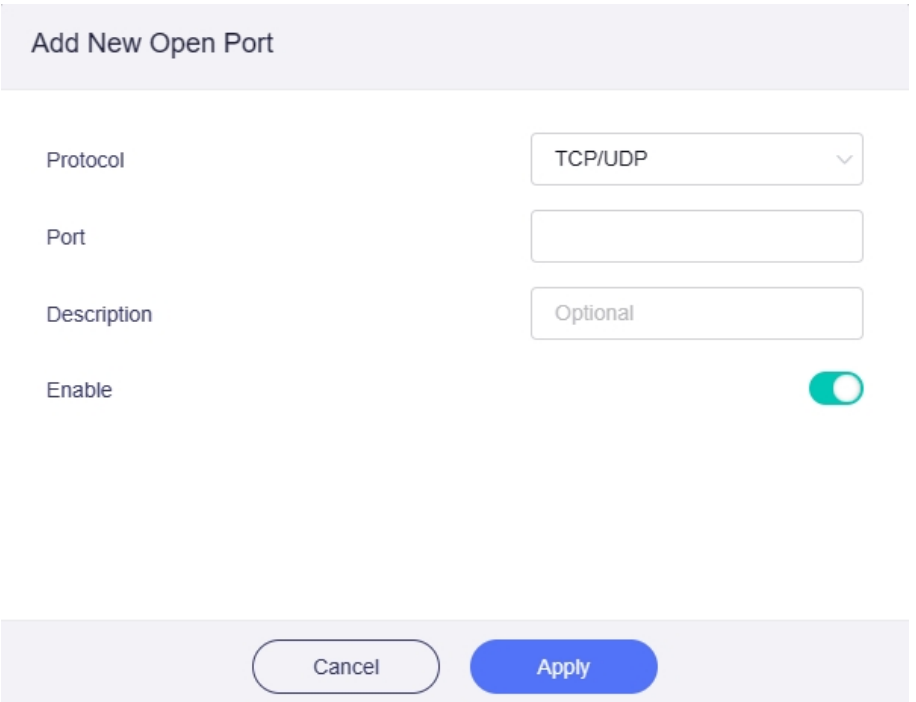


14.2.3 Abrir puertos en el enrutador

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.

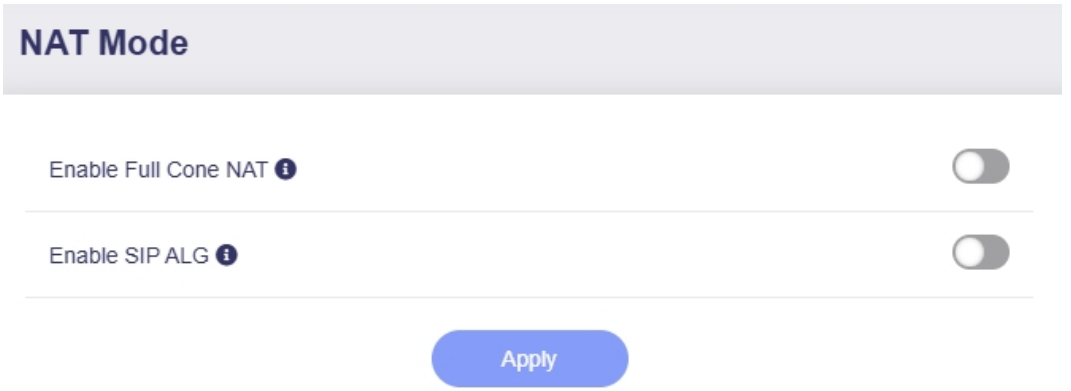


- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

- **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 este interruptor para activar o desactivar la regla de reenvío de puertos.

14.3 Modo NAT

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



- **NAT de cono completo**: se puede utilizar para reducir 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 SIP (Protocolo de inicio de sesión) tráfico. 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

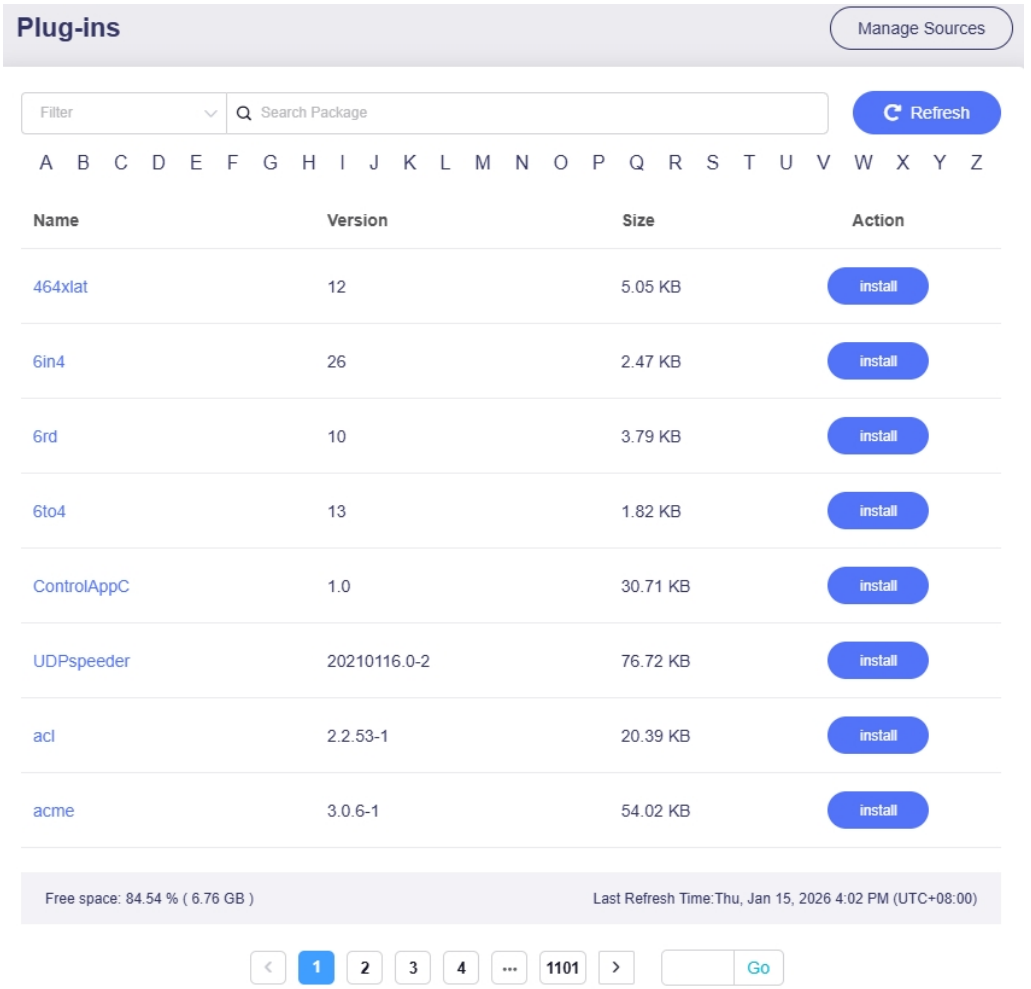
Aplicaciones

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

15.1 Complementos

Los Complementos página le permite administrar paquetes OpenWrt.

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



Nota:

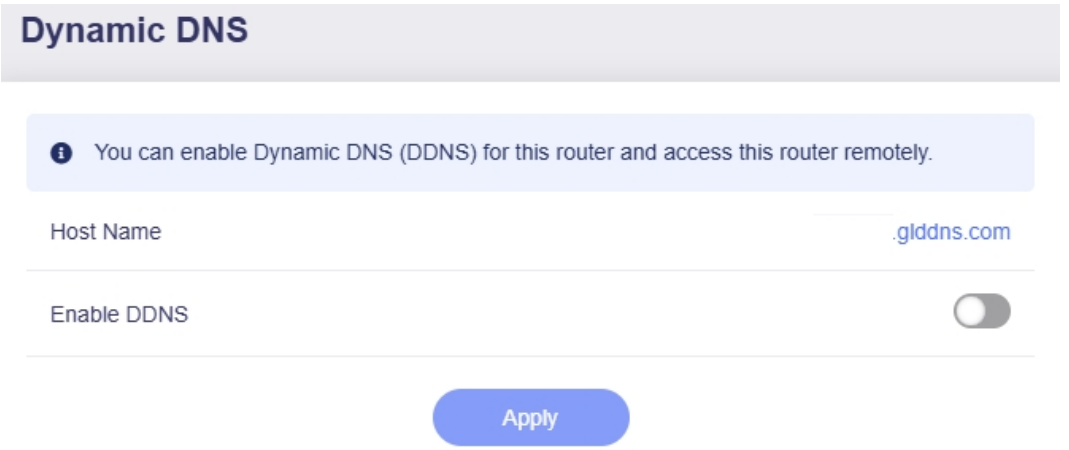
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

15.2 DNS dinámico

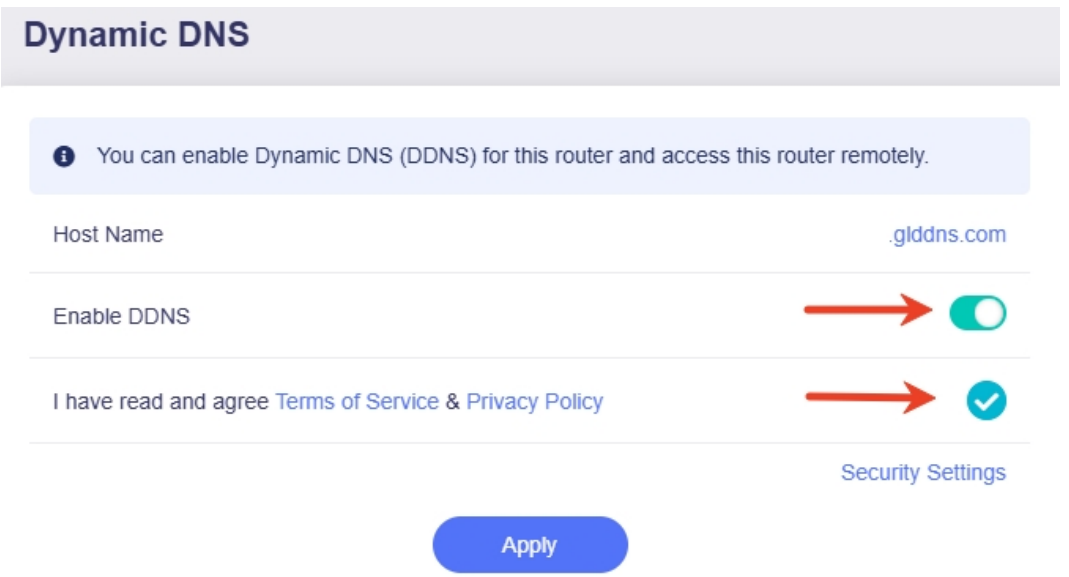
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

15.2.1 Habilitar DDNS

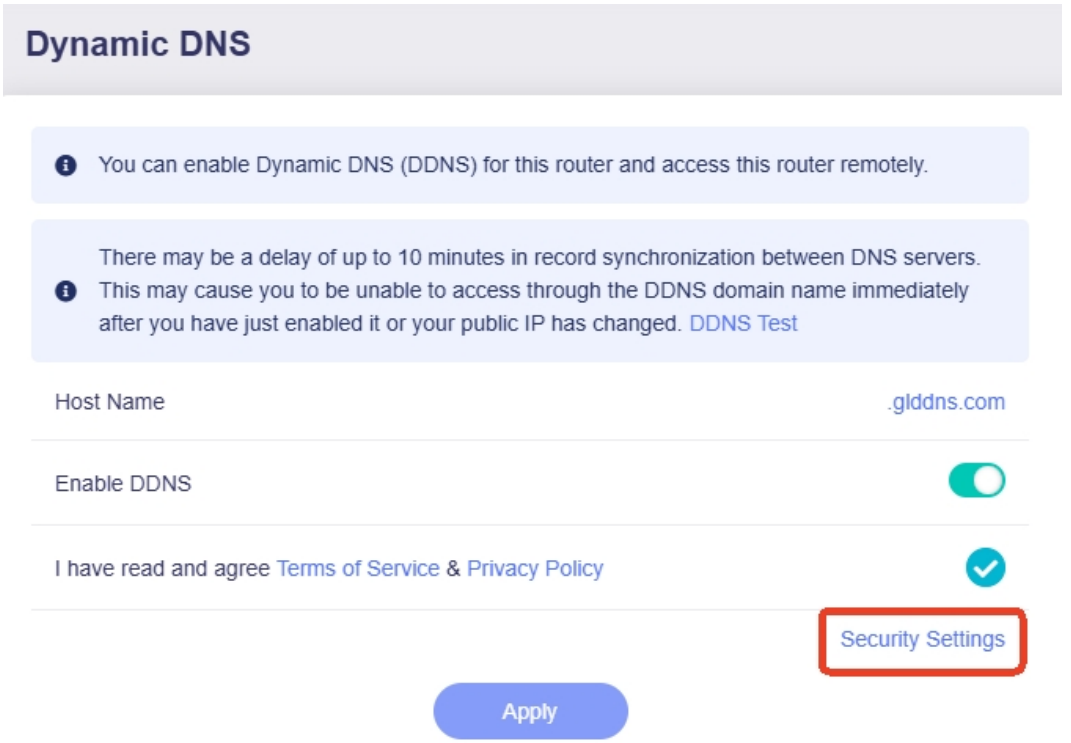
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



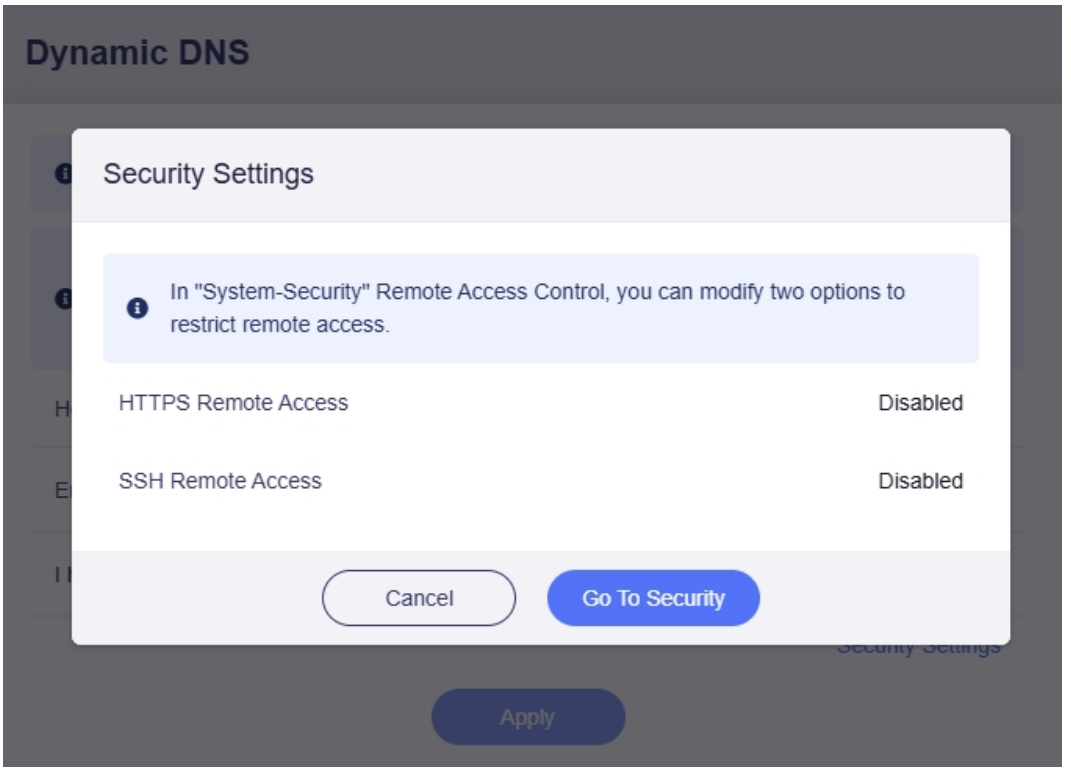
2. Active **Habilitar DDNS**, leer y aceptar los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



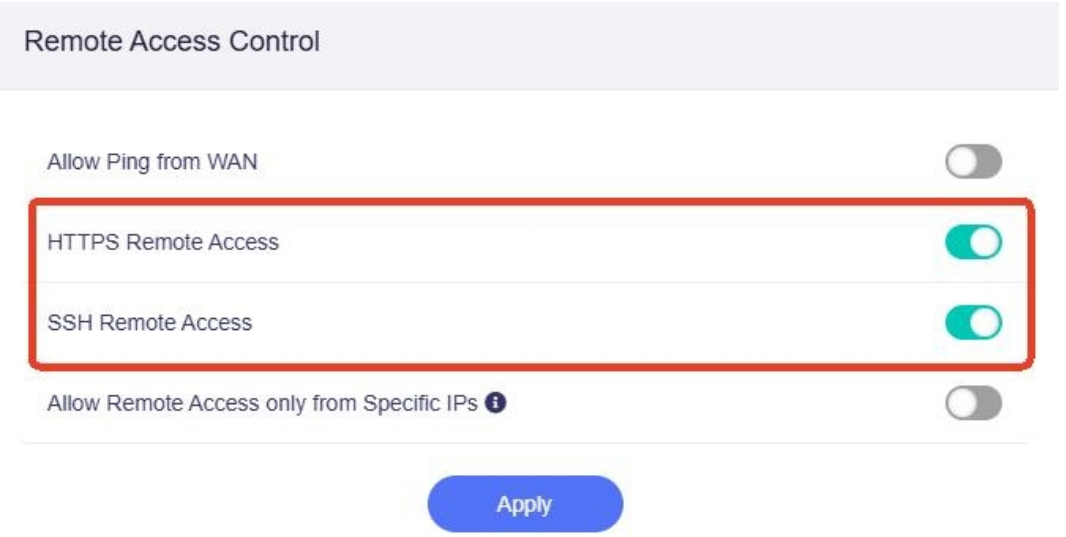
3. Haga clic **Configuración de seguridad** en la esquina inferior derecha.



4. En la ventana emergente, verifique si el acceso remoto que desea usar es habilitado.



Si no, vaya a **SECURITY** > **Acceso de administrador** > **Control de acceso remoto** para habilitarlo y haga clic en **Aplicar**.



Nota:

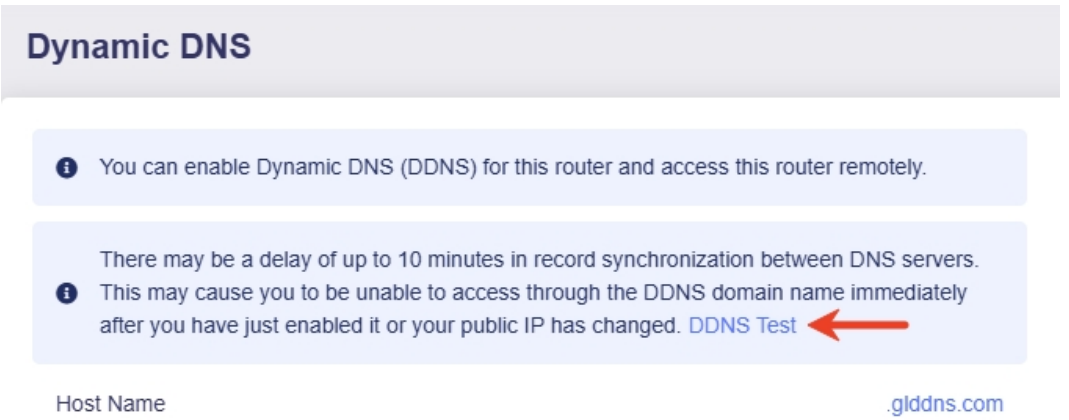
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

15.2.2 Comprobar si DDNS funciona

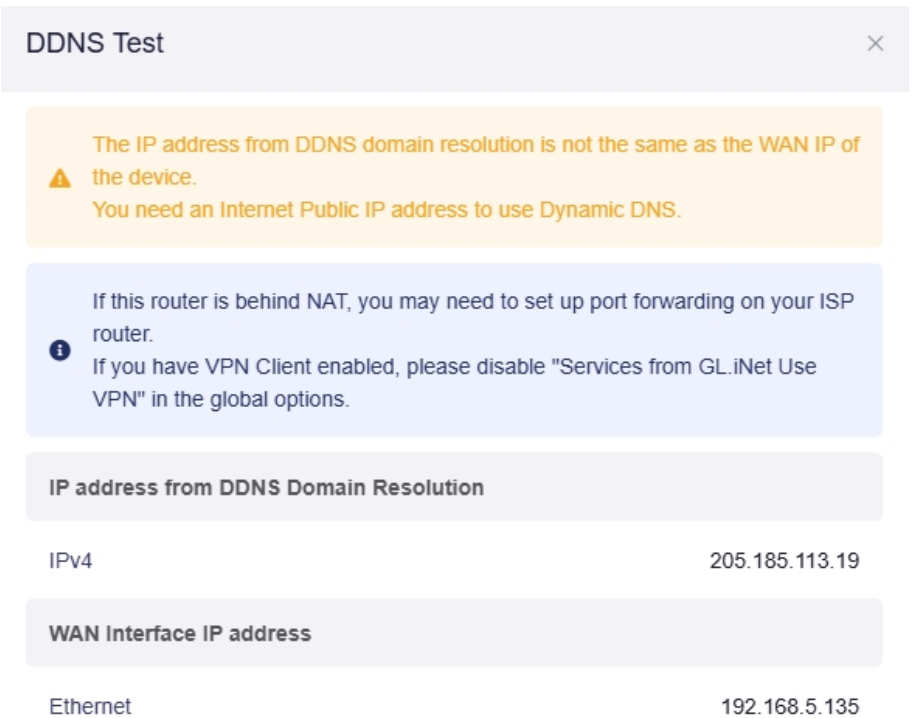
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

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 necesita 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.



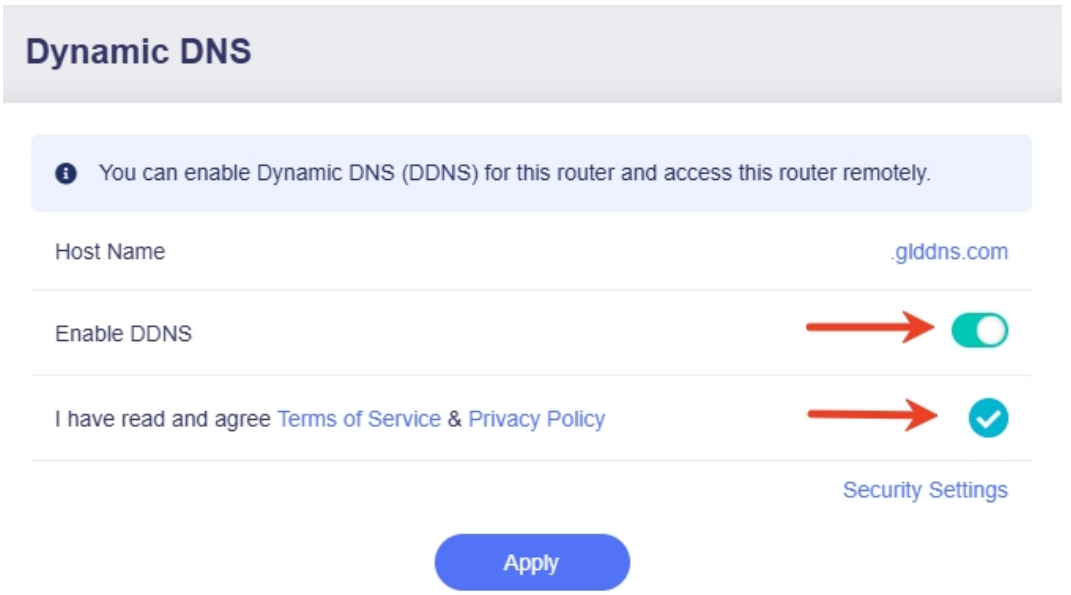
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Uconsúltelo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su DDNS El dominio se ha asignado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

15.2.3 Acceso remoto HTTPS

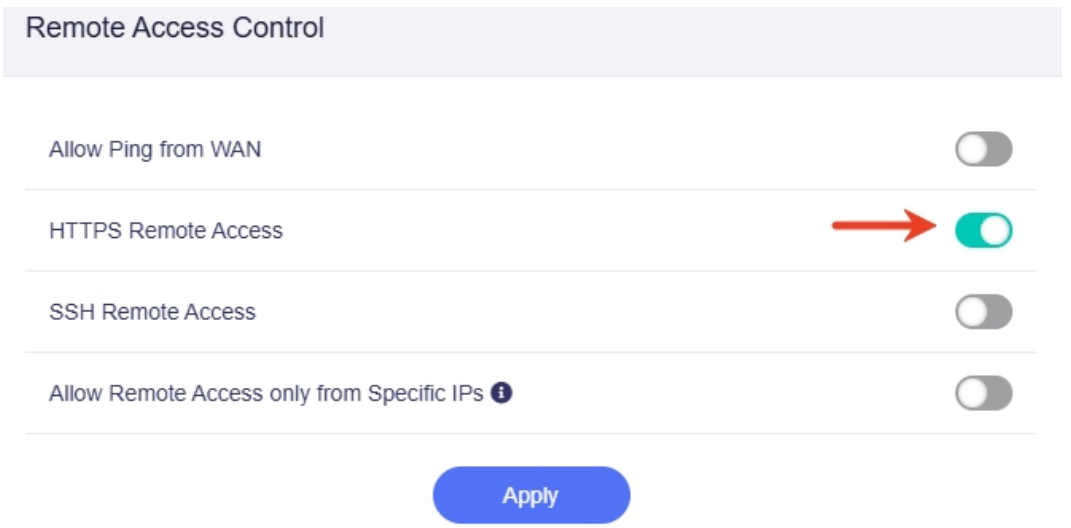
Se requiere una **Dirección IP pública** para el acceso remoto HTTPS.Consulte aquí parapara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

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**.

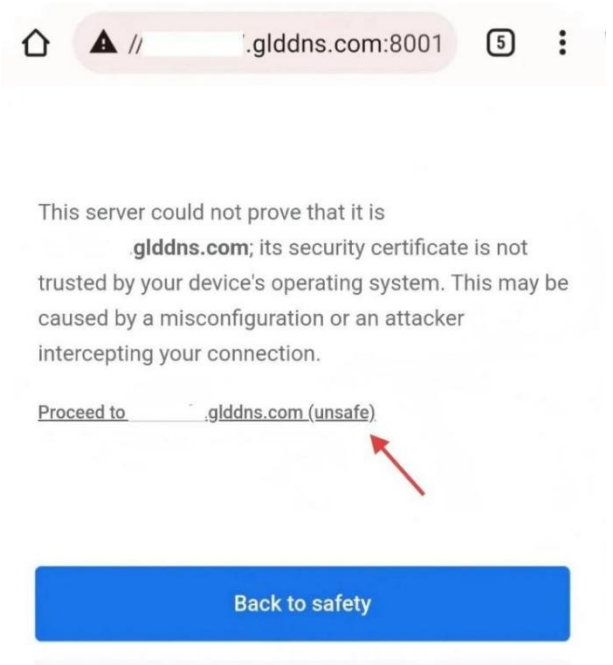


2. En el panel de administración web, vaya a **SEGURIDAD** >**Acceso de administrador** > **Control de acceso remoto**. Habilite **Acceso remoto HTTPS** y haga clic en **Aplicar**.



3. Una vez habilitado, puede acceder al panel de administración del enrutador' desde cualquier lugar usando el DDNS host nombre sobre HTTPS, por ejemplo, **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 puerto real 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.



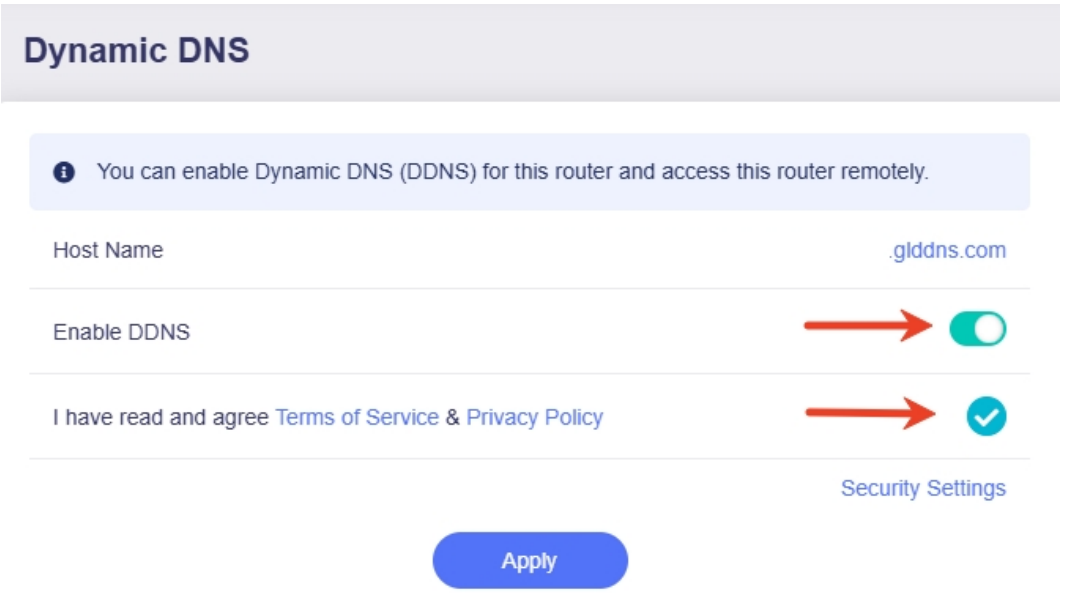
Luego podrá acceder al enrutador's panel de administración web usando el DDNS host nombre sobre **HTTPS**.

15.2.4 Acceso remoto SSH

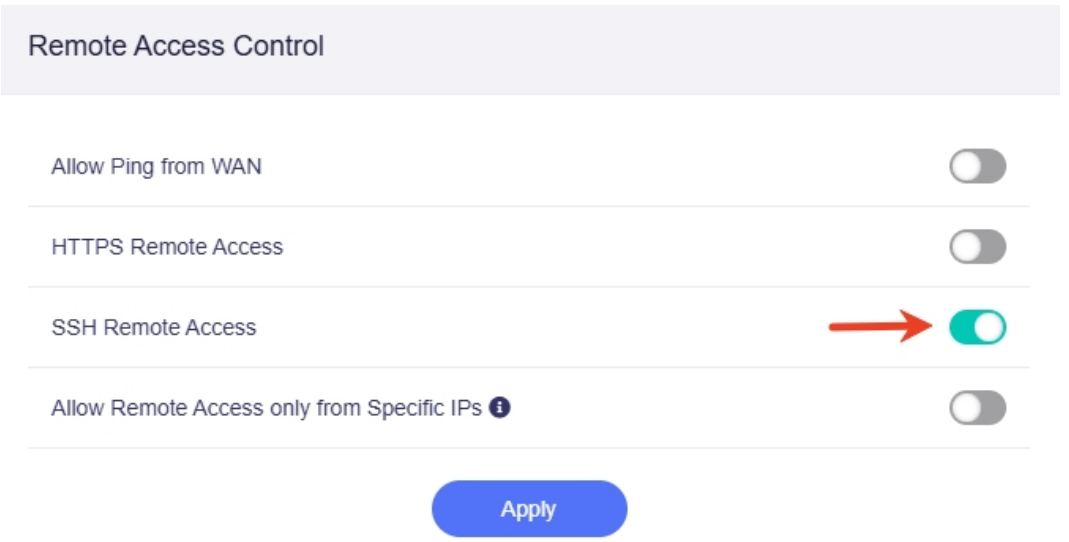
A **Dirección IP pública** es necesario para SSH acceso remoto. Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH acceso remoto.

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 **SEGURIDAD** >**Acceso de administrador** > **Control de acceso remoto**. Activar **Acceso remoto SSH** y haga clic en **Aplicar**.



Una vez habilitado, podrá acceder al enrutador’s panel de administración desde cualquier lugar usando 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).

15.3 Almacenamiento en red

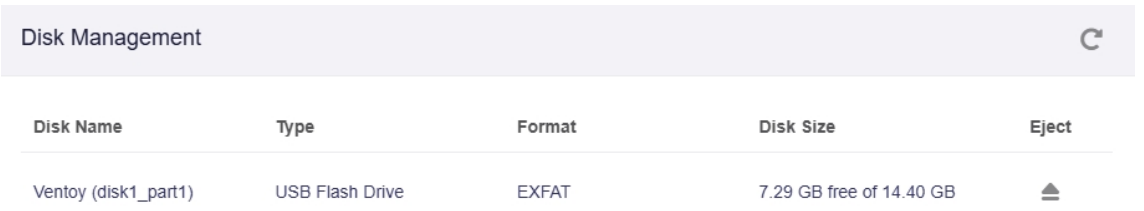
El almacenamiento en red permite compartir archivos de forma inalámbrica entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos los dispositivos conectados a Wi-Fi.

Mudi 7 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.

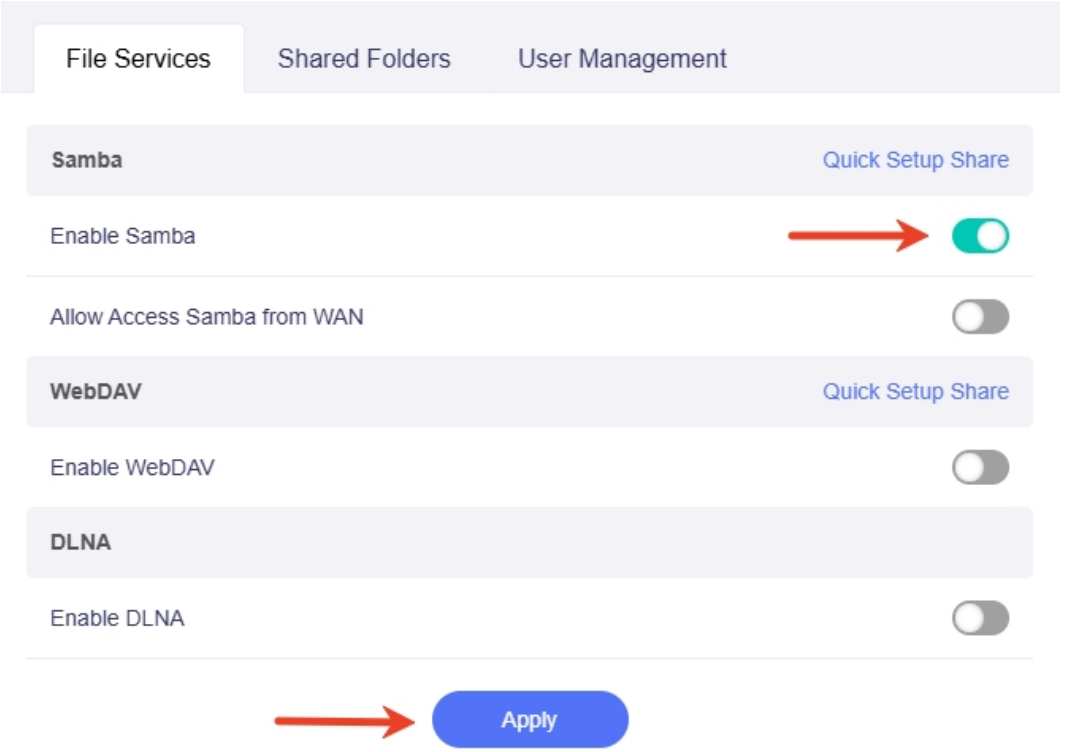
15.3.1 Conectar una unidad de almacenamiento

1. Conecte su dispositivo de almacenamiento al enrutador.
   - Para una unidad USB: conéctala directamente al puerto USB.
   - Para un disco duro externo: conéctala a una fuente de alimentación separada (si es necesario) y luego conéctala al enrutador.
2. Inicia sesión en tu 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 es detectado, la **Administración de discos** se mostrará de la siguiente manera.



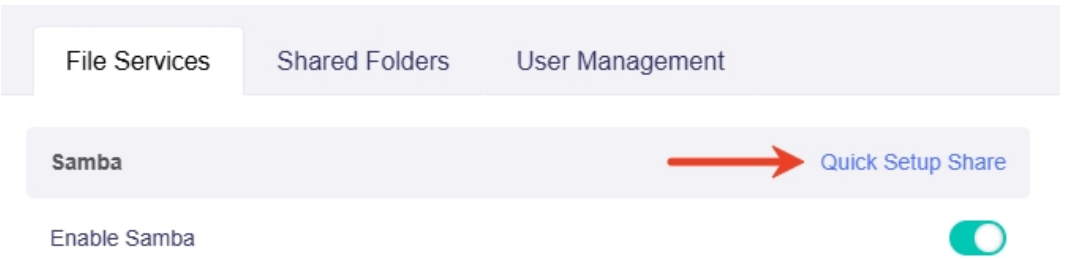
15.3.2 Configurar Samba

1. En el **Servicios de archivos**, talternar en **Enable Samba**, y haga clic en **Aplicar**.

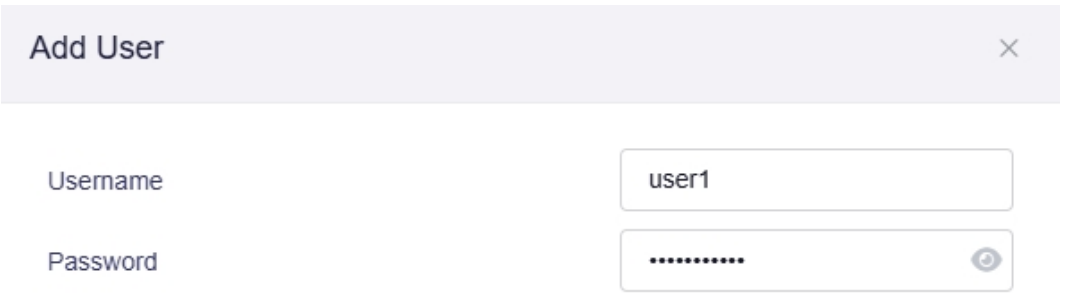


   - **Permitir acceso a Samba desde WAN**: habilitar it si desea que los dispositivos ascendentes accedan al servicio Samba.

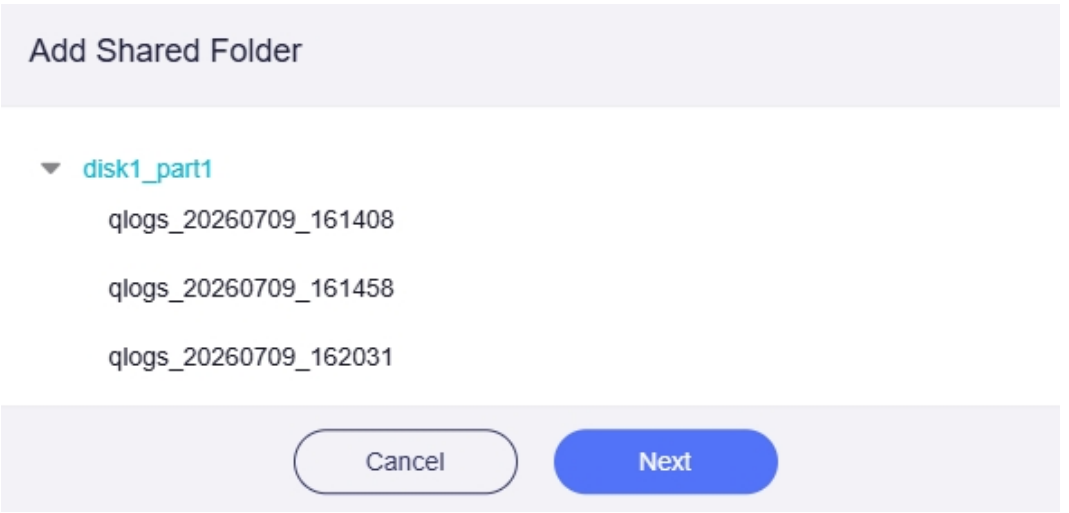
2. Haga clic en **Configuración rápida Compartir** para establecer el enlace compartido.



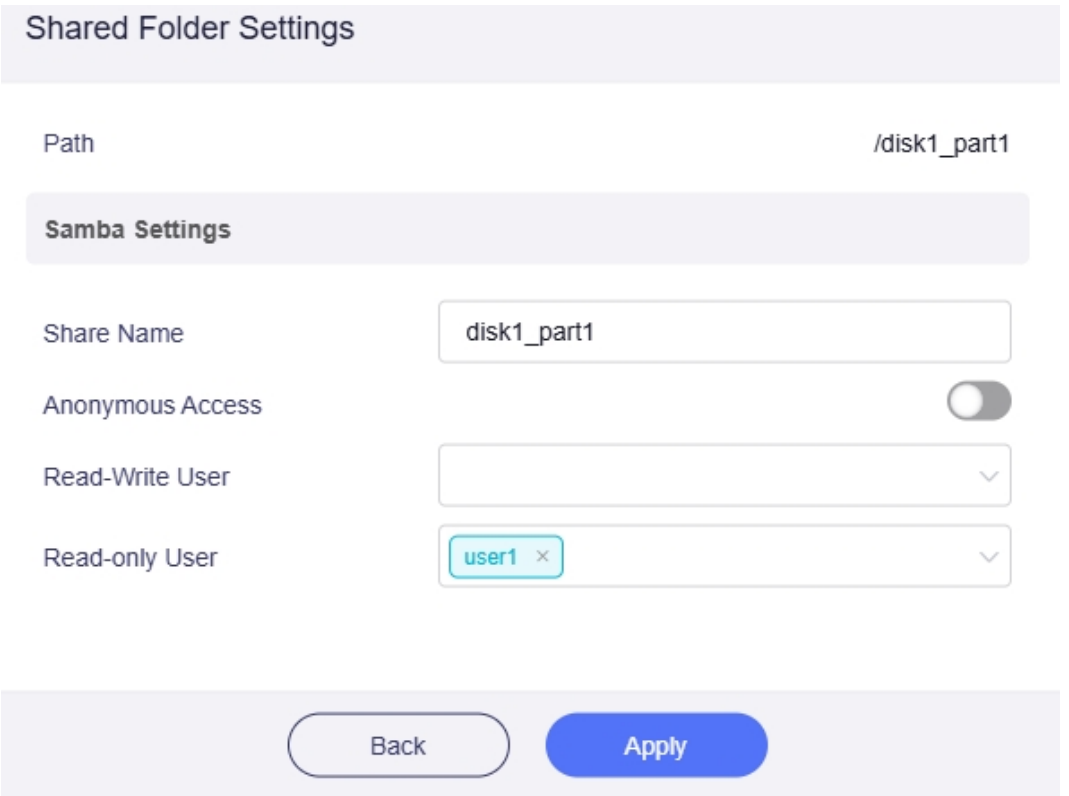
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



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).

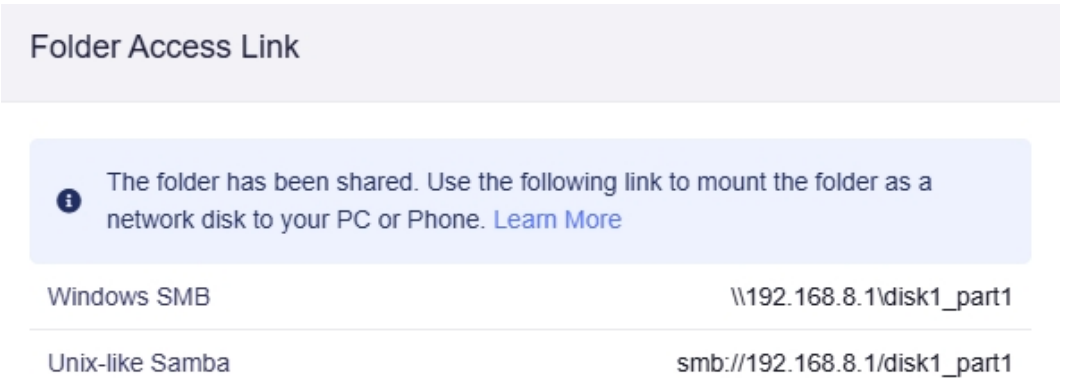


5. Configurar la carpeta compartida.
   El usuario creado en el El paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este usuario pueda escribir o eliminar archivos, eliminarlo de Usuario de solo lectura y agregarlo a **Lectura-Escritura Usuario**, tluego haga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



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

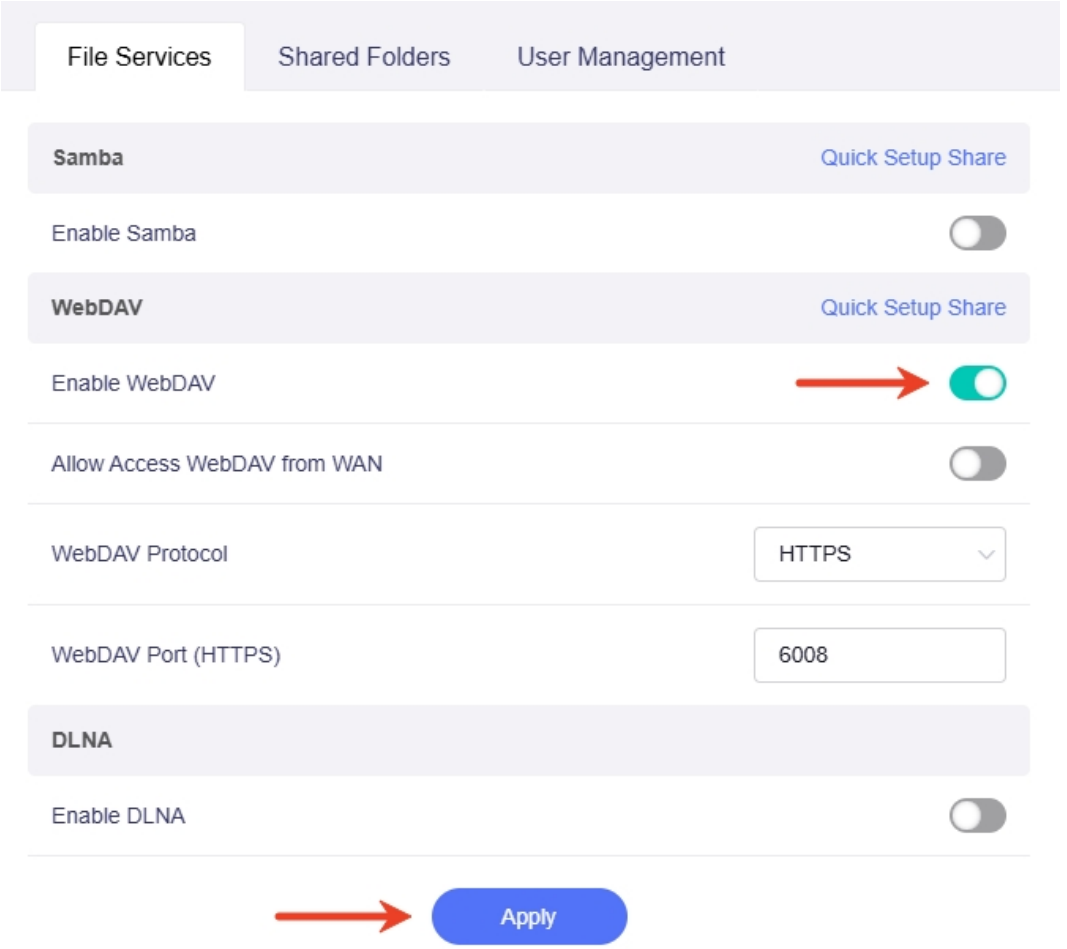
6. Obtenga el enlace de acceso a la carpeta .
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder su carpeta compartida a través del servicio Samba a través de estos enlaces.



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

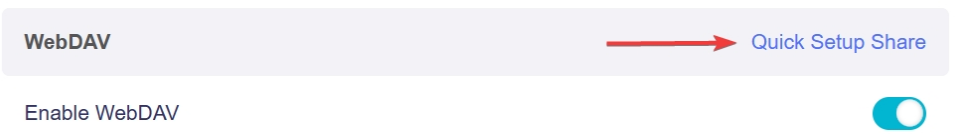
15.3.3 Configurar WebDAV

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

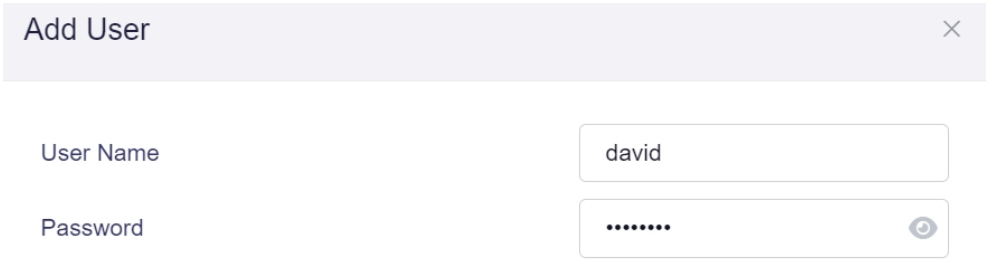


- **Permitir acceso a WebDAV desde WAN**: habilítela si desea que los dispositivos ascendentes accedan a Servicio WebDAV.
- **Protocolo WebDAV**: HTTP no está cifrado; Úselo bajo su propio riesgo. HTTPS está cifrado y utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario modificar el número de puerto a menos que haya un conflicto. El puerto número rango es 1024 - 65535.

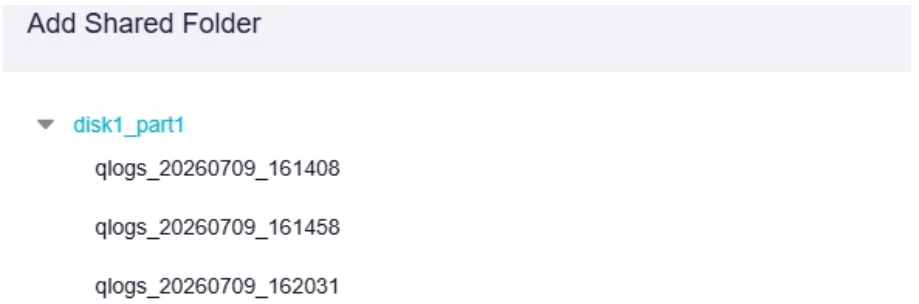
2. Haga clic en **Configuración rápida Compartir** a sConfigure el enlace compartido.



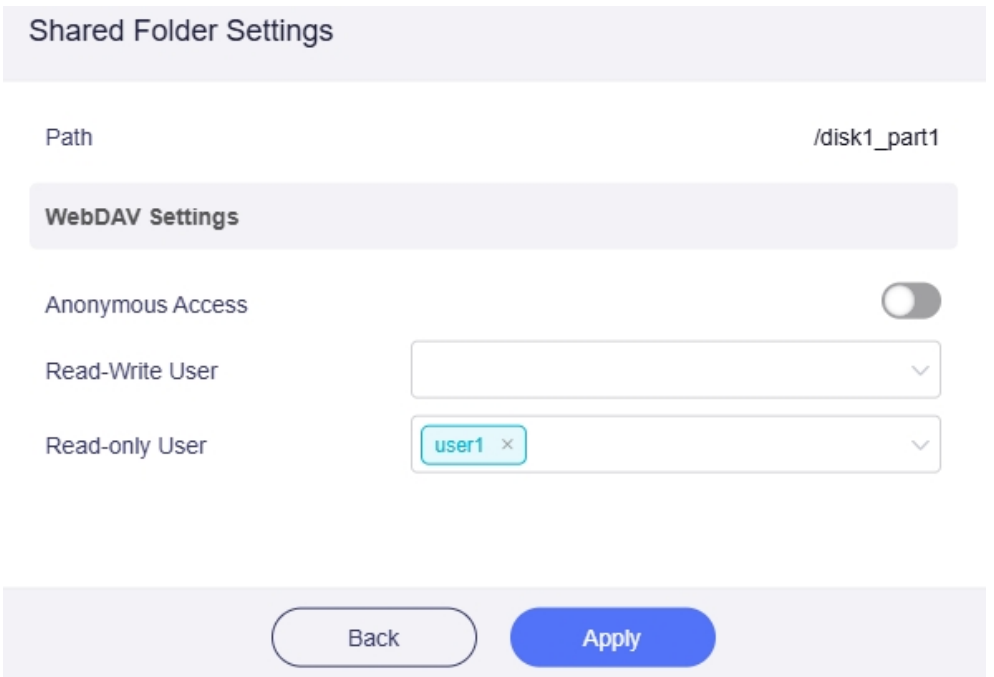
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



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

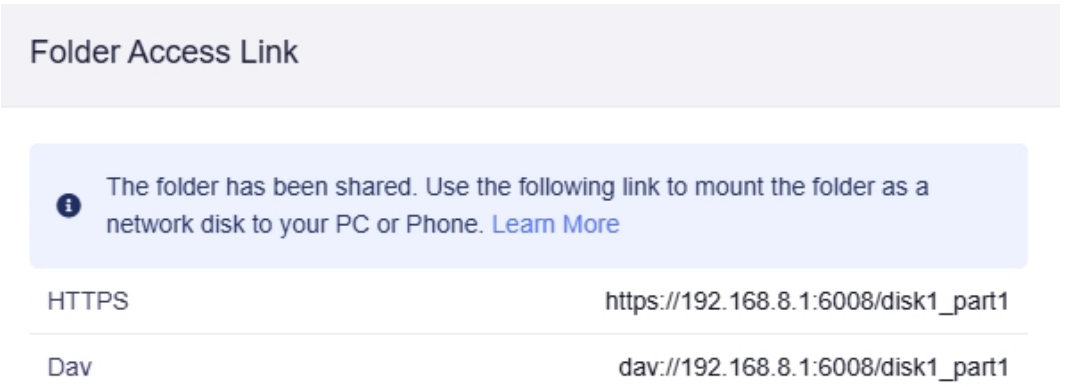


5. Configura la carpeta compartida s.
   The El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada
   Si desea este usuario para poder escribir o eliminar archivos, eliminelo del usuario de solo lectura y agréguelo a **lectura-escriturae usuario**, luego haga clic **Aplicar**.



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

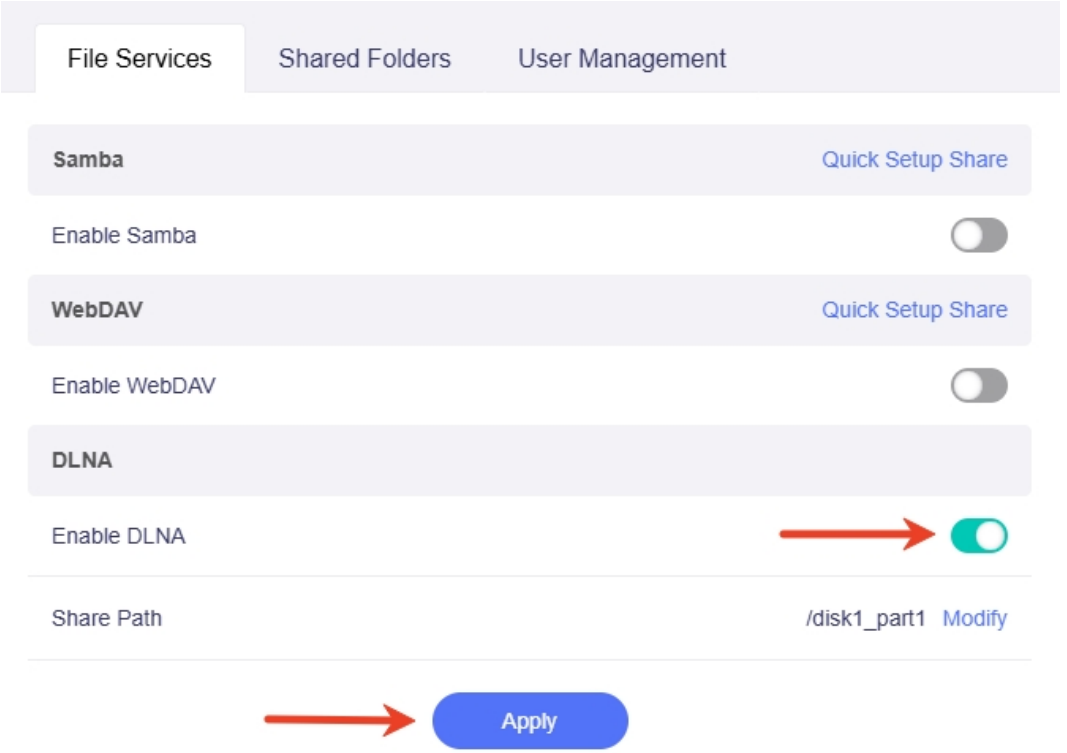
6. Obtenga el enlace de acceso a la carpeta.
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. Los sistemas tipo Unix incluyens Android, iOS, macOS, Ubuntu, etc. Ahora puede acceder a su carpeta compartida a través del servicio WebDAV a través de estos enlaces.



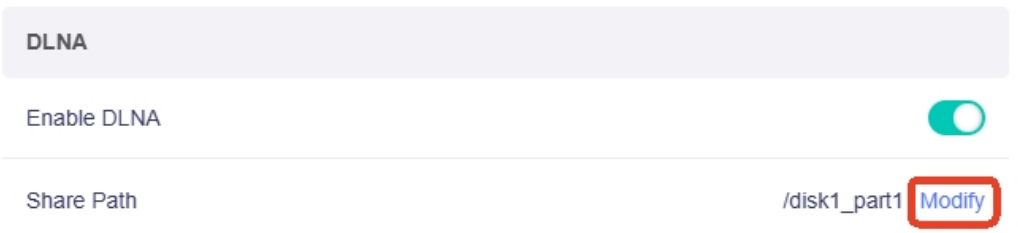
Nota: si habilita **Permitir acceso WebDAV desde WAN** y acceda la carpeta compartida de red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con la IP WAN de tu enrutador’s, que se puede encontrar en la página INTERNET del panel de administración web.

15.3.4 Configurar DLNA

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



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



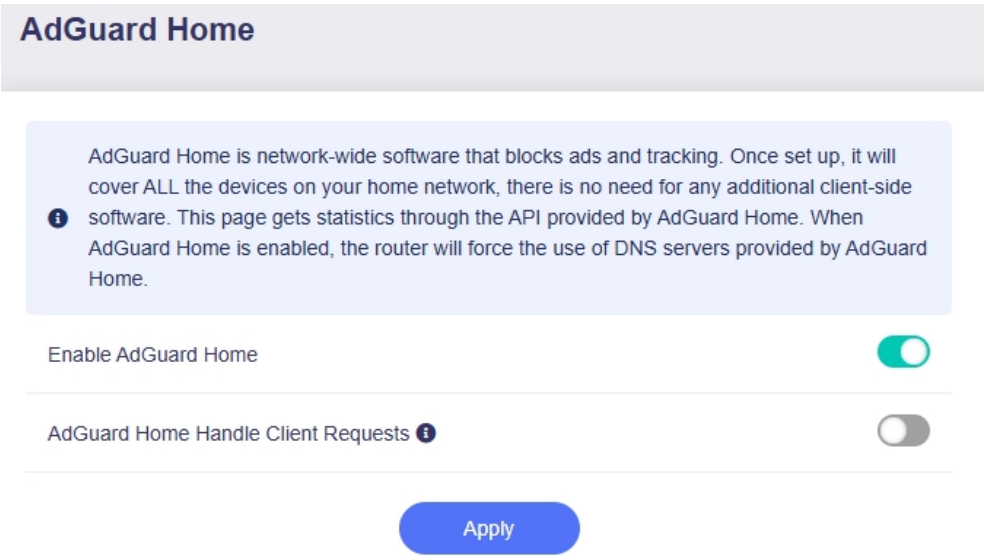
3. Conecte su televisor inteligente al enrutador. encontrará el DLNA sservidor automáticamente.

15.4 AdGuard Home

AdGuard Home es un software de bloqueo de publicidad y prevención de seguimiento en toda la red. Una vez configurado, cubrirá todos los dispositivos cliente sin necesidad de software adicional del lado del cliente.

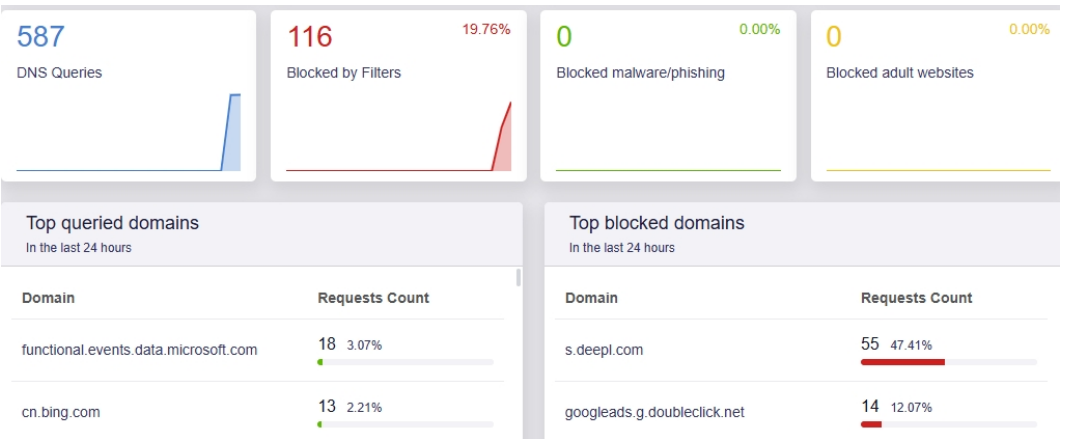
Siga estos pasos para configurar AdGuard Home.

1. Inicie sesión en el enrutador's web undmin panel, navegue hasta **APLICACIONES** > **AdGuard Home**. Activar en **Eactive AdGuard Home** y haga clic en **Aplicar**.

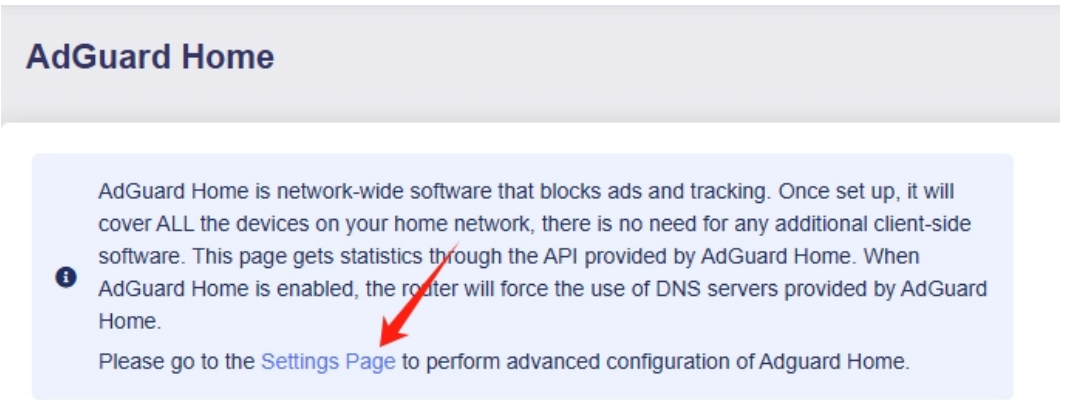


- **AdGuard Home Handles Solicitudes de clientes**: si está habilitado, las consultas DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto hará que las políticas VPN basadas en dominios fallen.

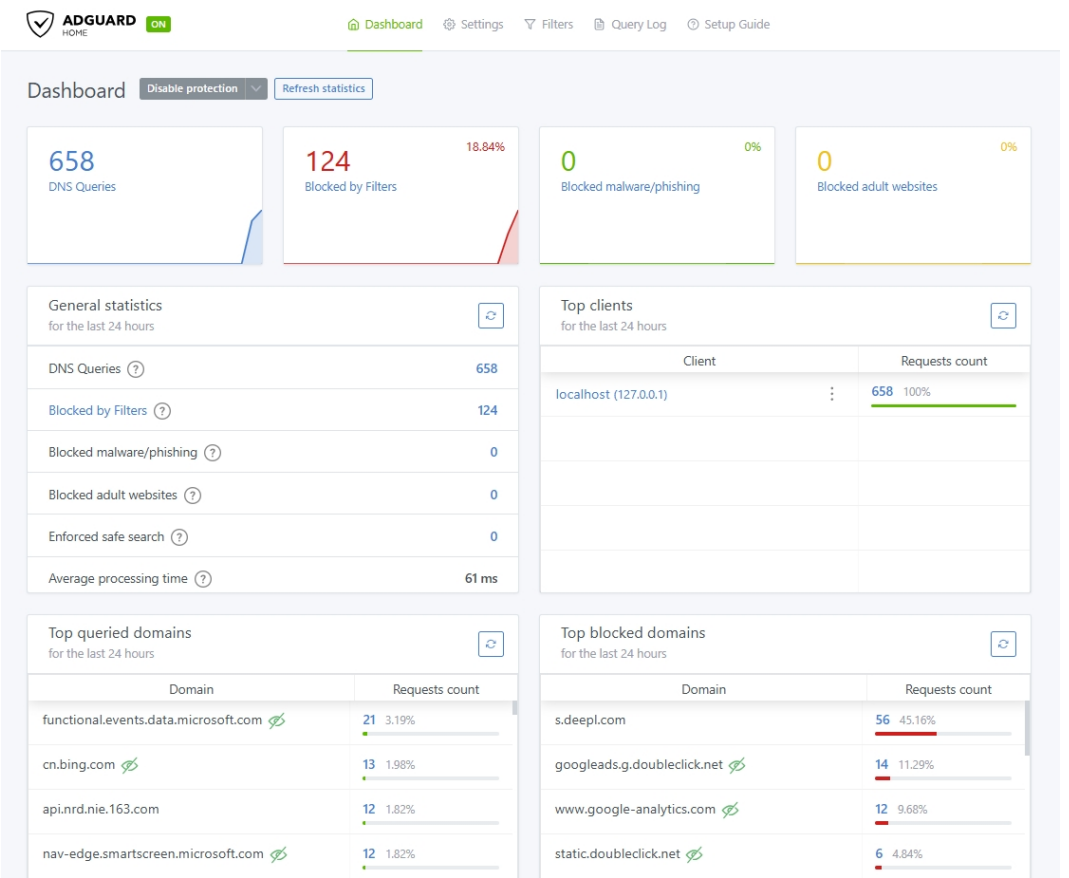
2. La página cargará automáticamente estadísticas DNS (consultas, dominios bloqueados, etc.) a través de la API proporcionada por AdGuard Inicio.



3. Haga clic en **Página de configuración** 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.



15.5 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 de Tailscale, lo que permite el acceso remoto al enrutador, así como a sus recursos WAN y LAN.

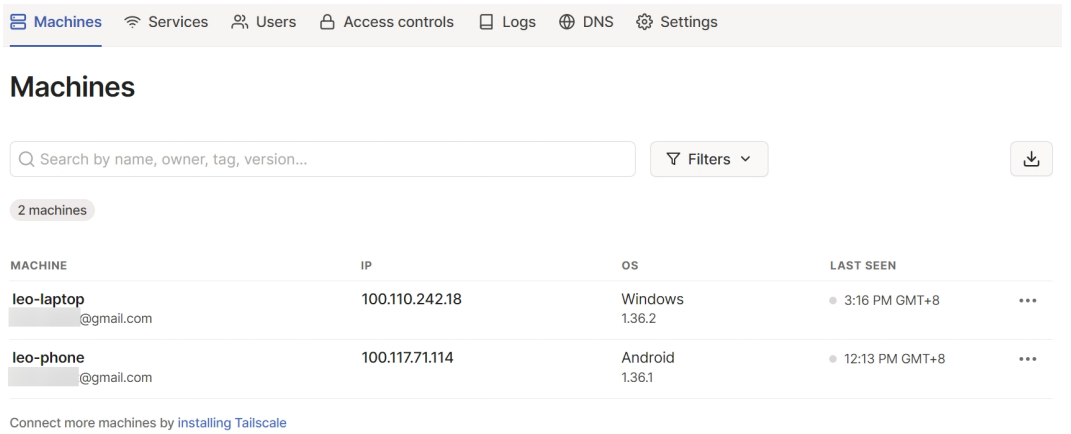
Nota:

1. Dado que Tailscale se basa en WireGuard, no se recomienda utilizar Tailscale con ninguna de las siguientes características o servicios simultáneamente, ya que esto puede causar conflictos de enrutamiento: cliente OpenVPN, cliente WireGuard, sitio a sitio GoodCloud, 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.

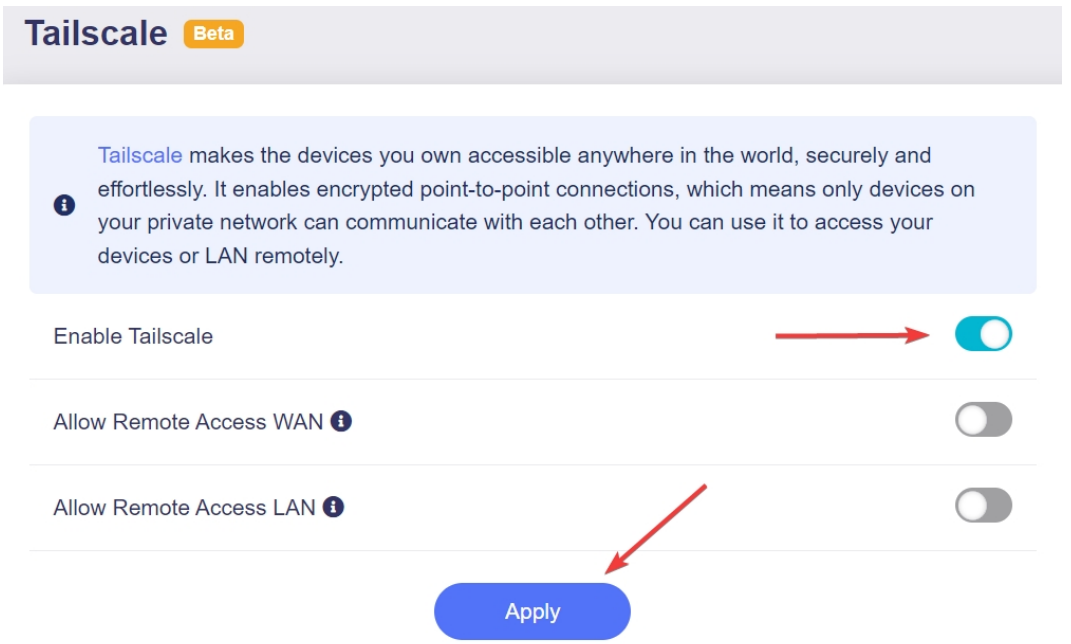
15.5.1 Configurar Tailscale

Aquí se muestra un ejemplo del uso de GL-MT2500 para configurar Tailscale red.

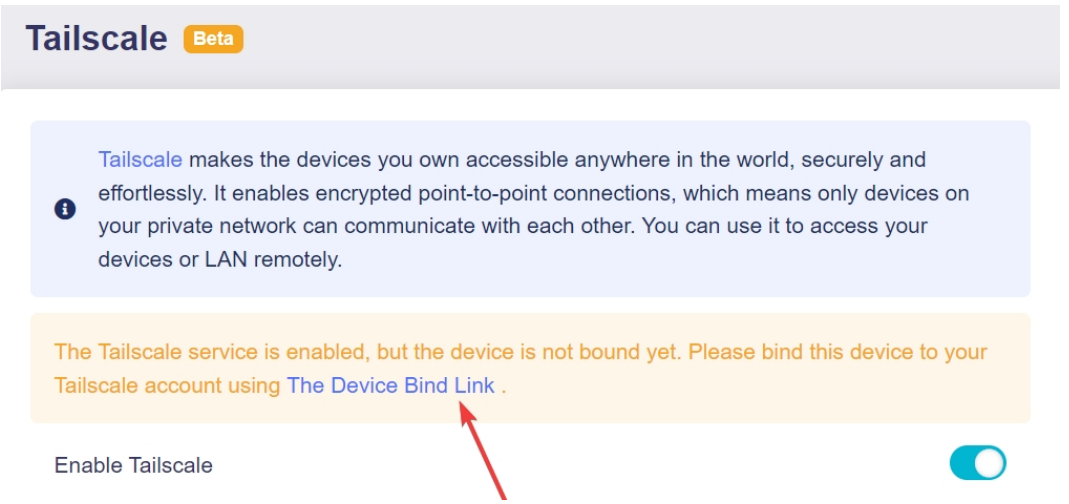
1. Rregistre primero una cuenta de Tailscale y vincule uno o dos dispositivos a su cuenta de Tailscale parao con fines de prueba. Después de vincular, verá sus dispositivos en la plantilla Tailscale C.



2. Inicie sesión en el panel de administración web de su enrutador' y navegar a **APLICACIONES** > **Tailscale**. Activar **Habilitar Escala de cola** y haga clic en **Aplicar**.



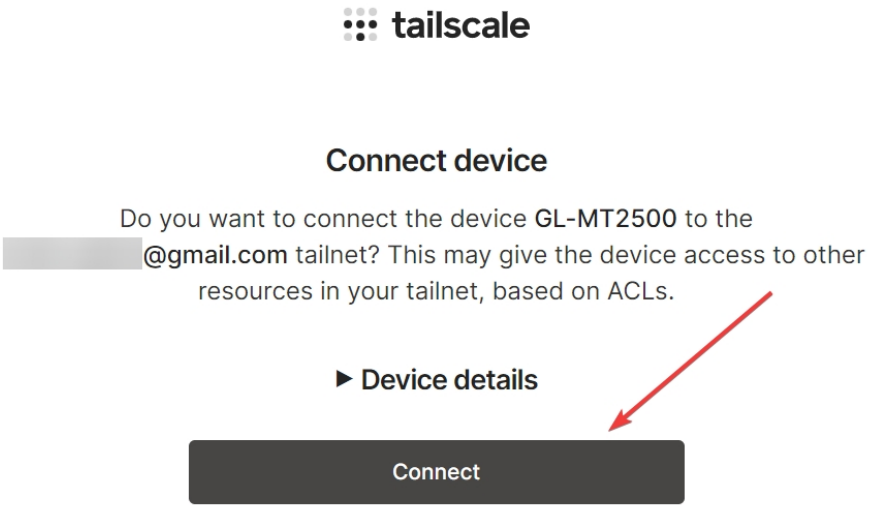
3. La página le pedirá que vincule el dispositivo. Haga clic en **Enlace de enlace de dispositivo**.



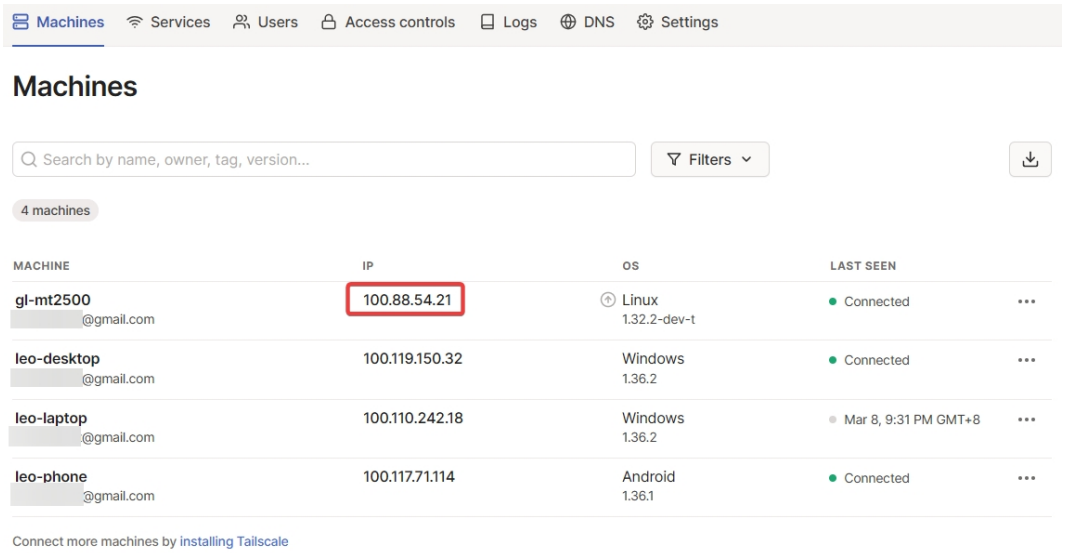
4. En la ventana emergente, haga clic en el enlace e inicie sesión con su Tailscale cuenta.



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



6. Yserá luego 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. 100.88.54.21.

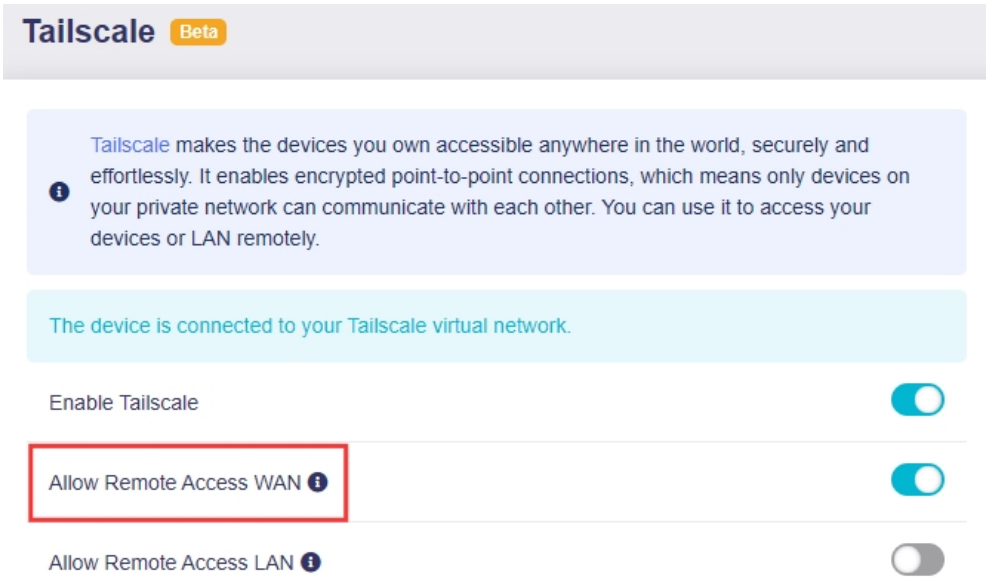


7. Pruebe la conectividad.

   En otro dispositivo conectado a la misma red de Tailscale, abra un navegador web e ingrese el enrutador's IP virtual en la barra de direcciones. Si puedes acceder al enrutador'panel de administración web, significa que Tailscale está funcionando. También puede usar el comando ping o iniciar sesión SSH en el terminal del enrutador'por su IP virtual para probar la conectividad.

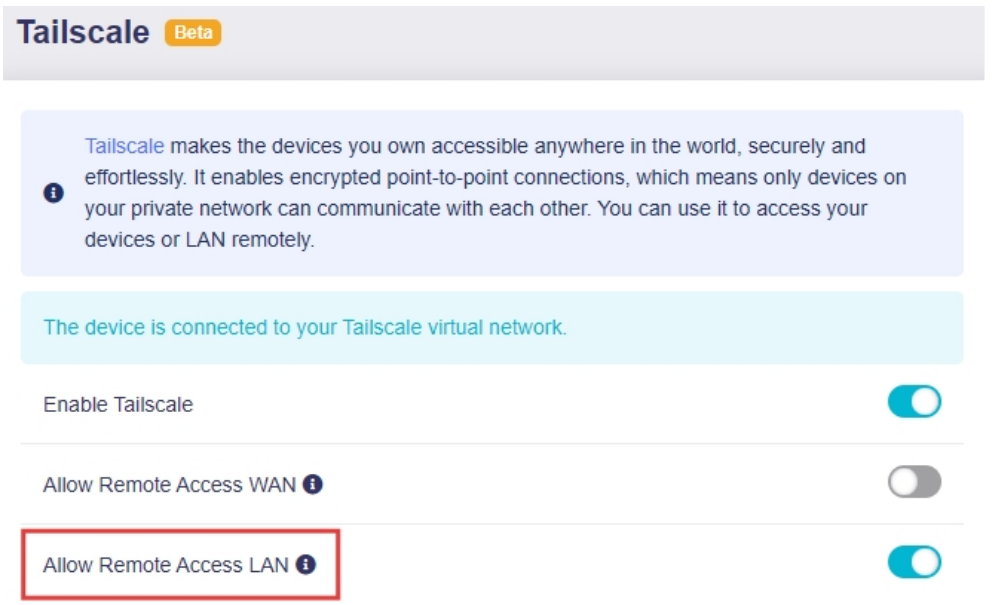
15.5.2 Permitir el acceso remoto a la WAN

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



15.5.3 Permitir el acceso remoto a la LAN

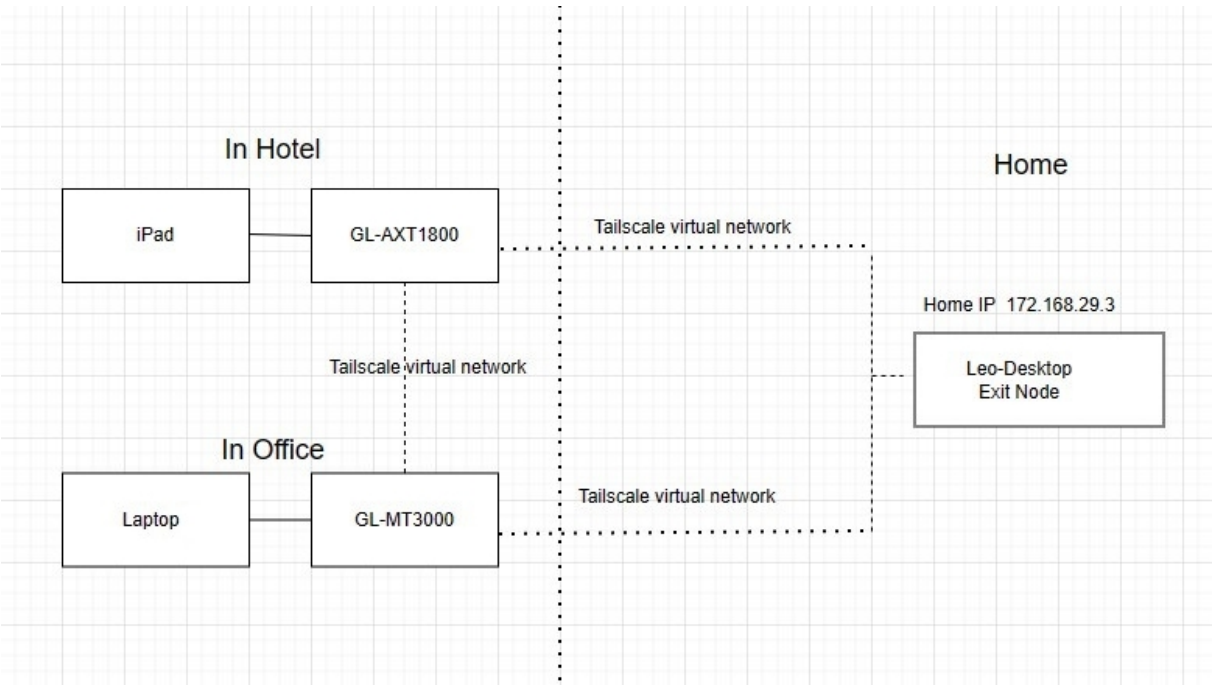
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



15.5.4 Nodos de salida personalizados

De forma predeterminada, Tailscale actúa como una red superpuesta: solo enruta el tráfico entre dispositivos que ejecutan Tailscale y no procesa su tráfico público de Internet, como al navegar 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 "nodo de salida". Consulte aquí para obtener más detalles.

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

15.6 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 mismo, así como a sus recursos WAN y LAN.

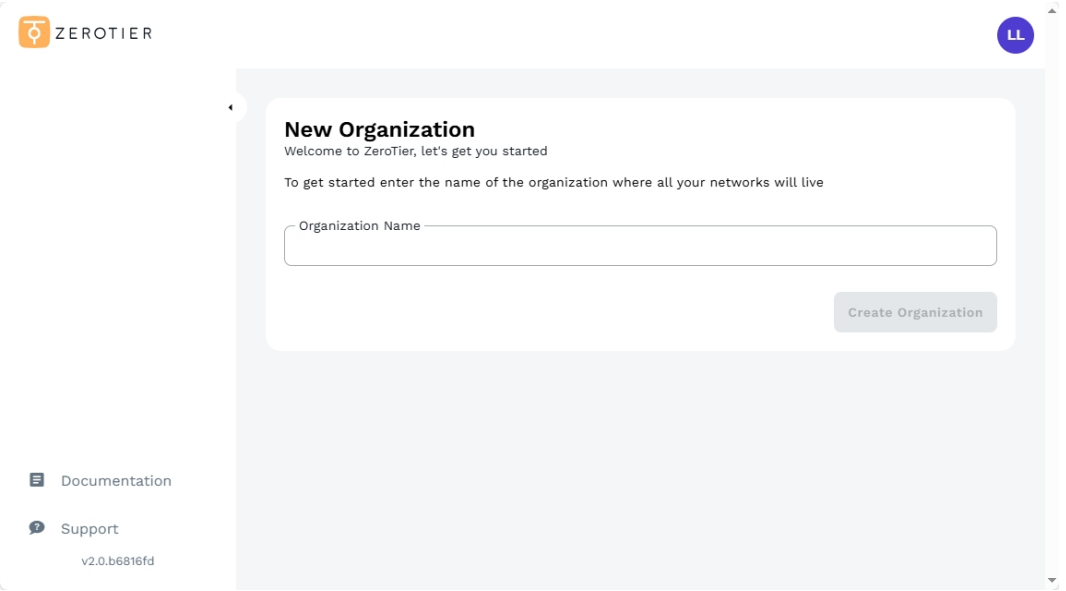
Nota:

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 algunos errores.

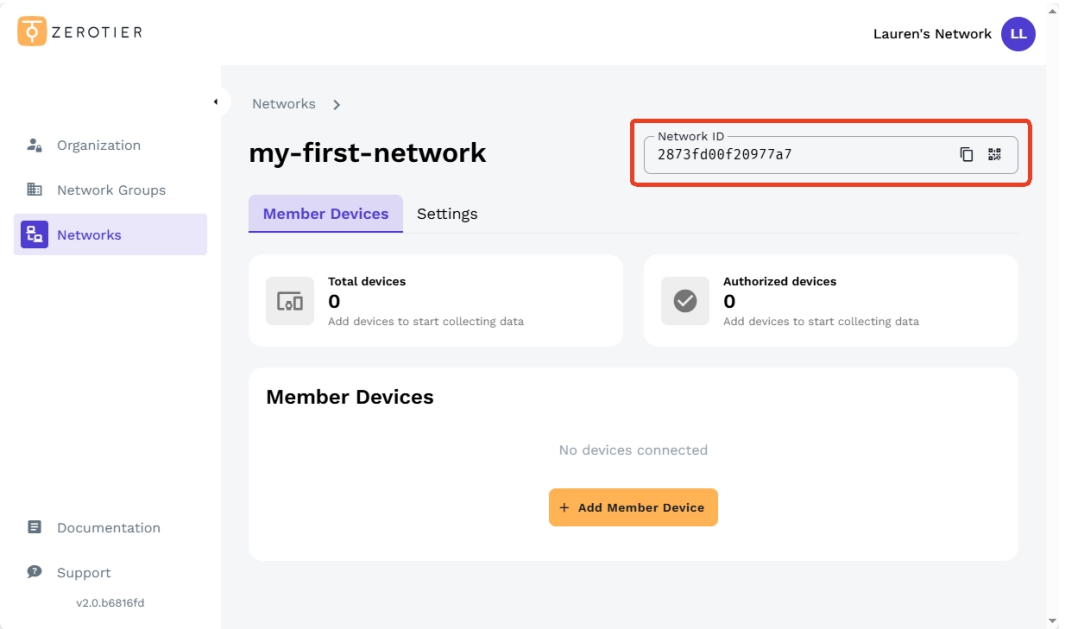
15.6.1 Configurar ZeroTier

Hay dos versiones de ZeroTier Central disponibles: New Central y Legacy Central. Los siguientes pasos utilizan New Central como ejemplo.

1. Visita Sitio web oficial de ZeroTier e inicia sesión con tu cuenta.
2. Cree una organización.

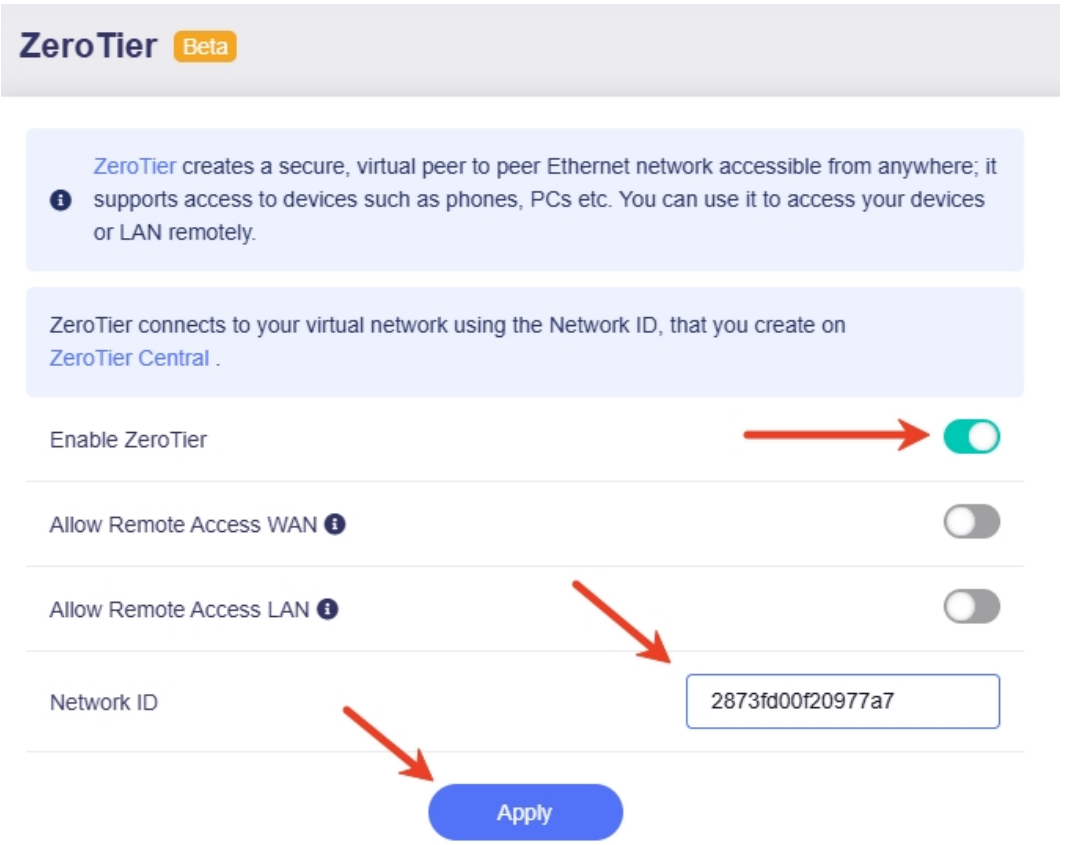


3. Seleccione un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

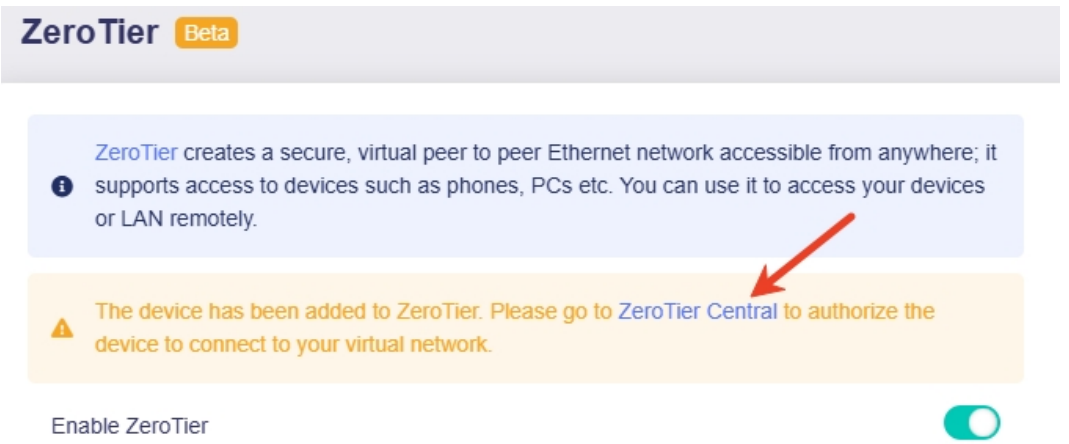


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesaria cuando conecte otros dispositivos más adelante.

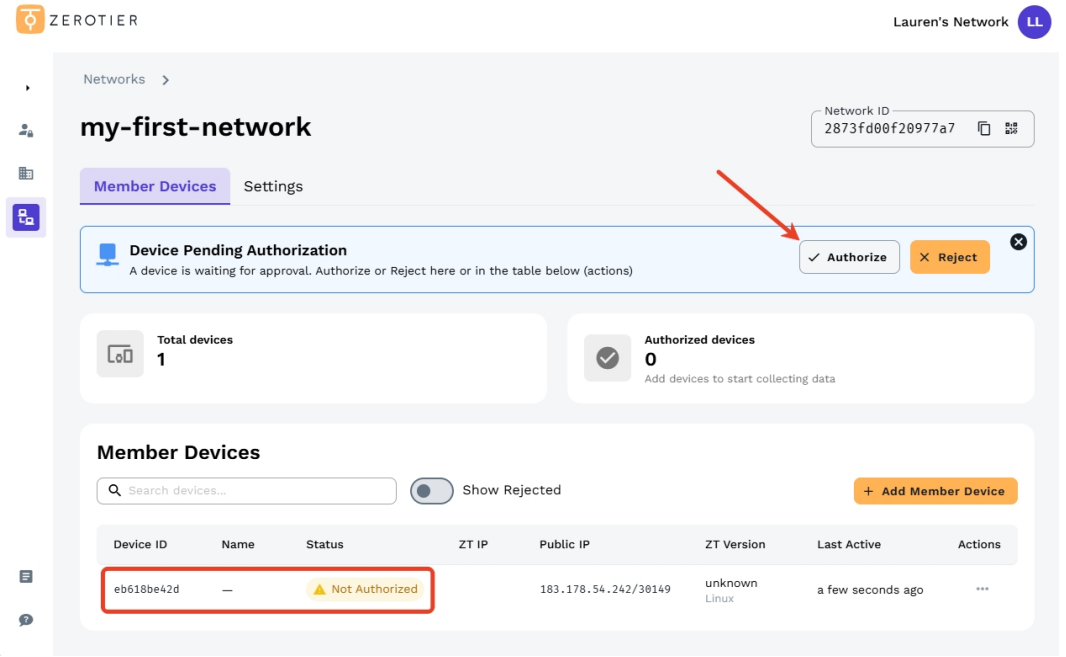
5. Inicie sesión en la web de su enrutador Panel de administración y navegue hasta **APLICACIONES** -> **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



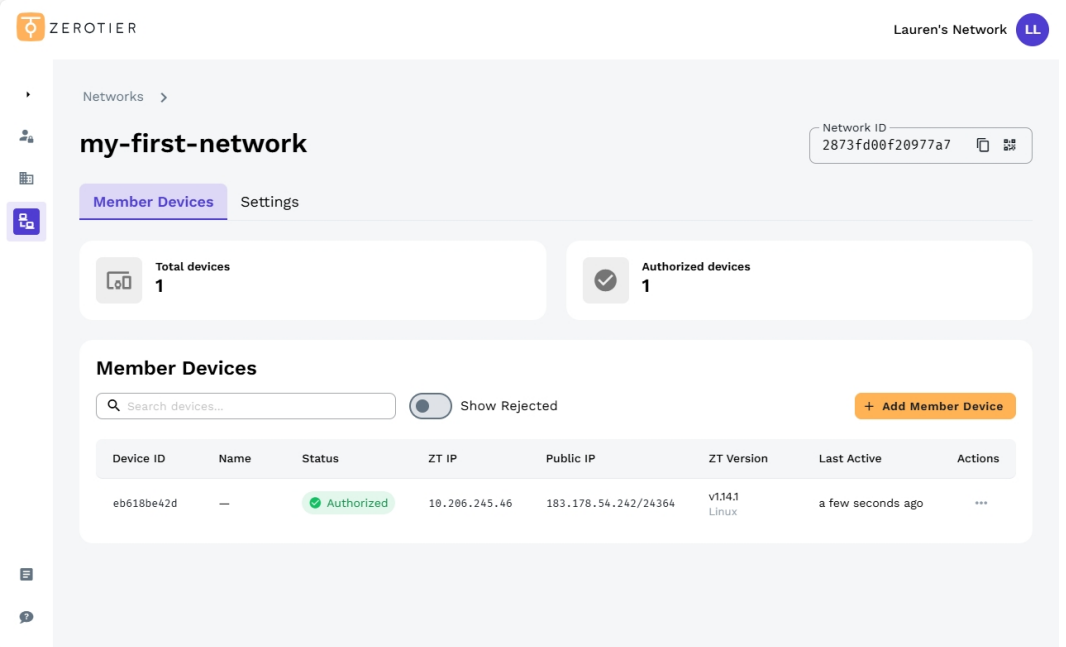
Después de un momento, la página indicará que se requiere autorización. Haga clic en el **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



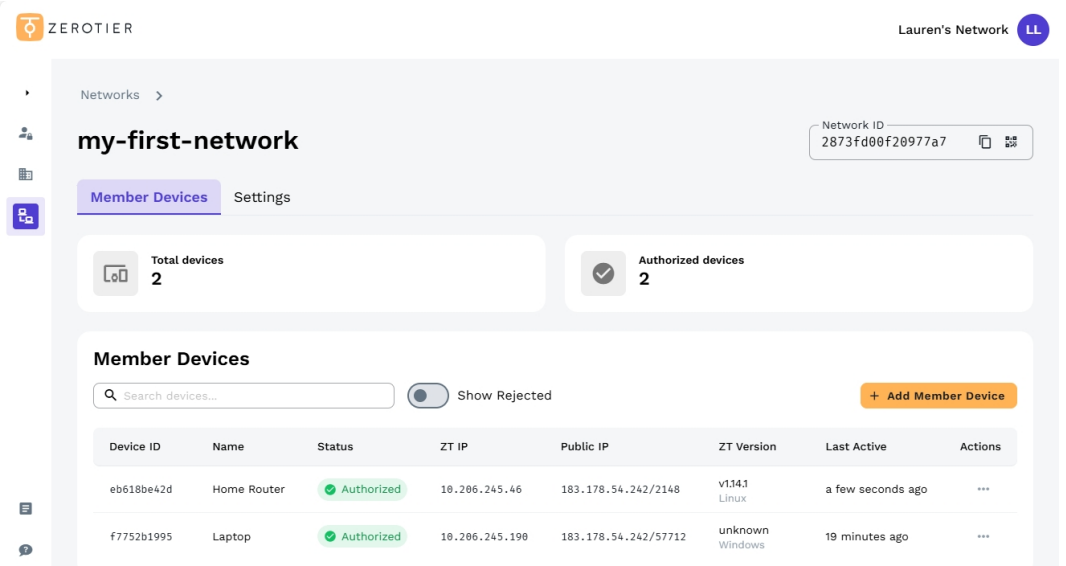
6. En ZeroTier Central, localice el dispositivo pendiente y autorícelo.



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

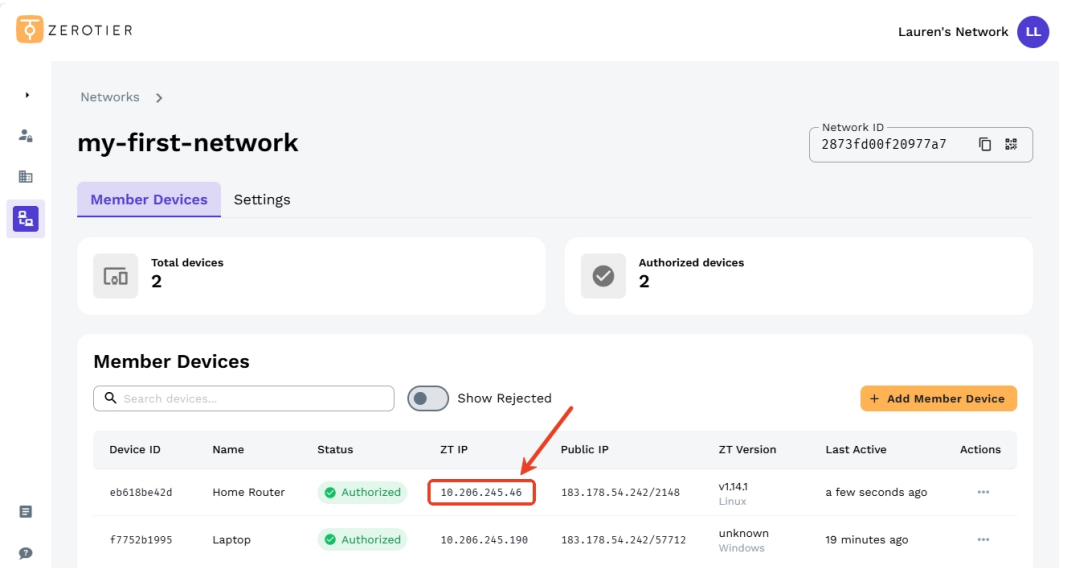


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, se muestra la página como sigue. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP administrada**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



Consejo: puede hacer clic en el icono 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 el **IP administrada** para copiarla.



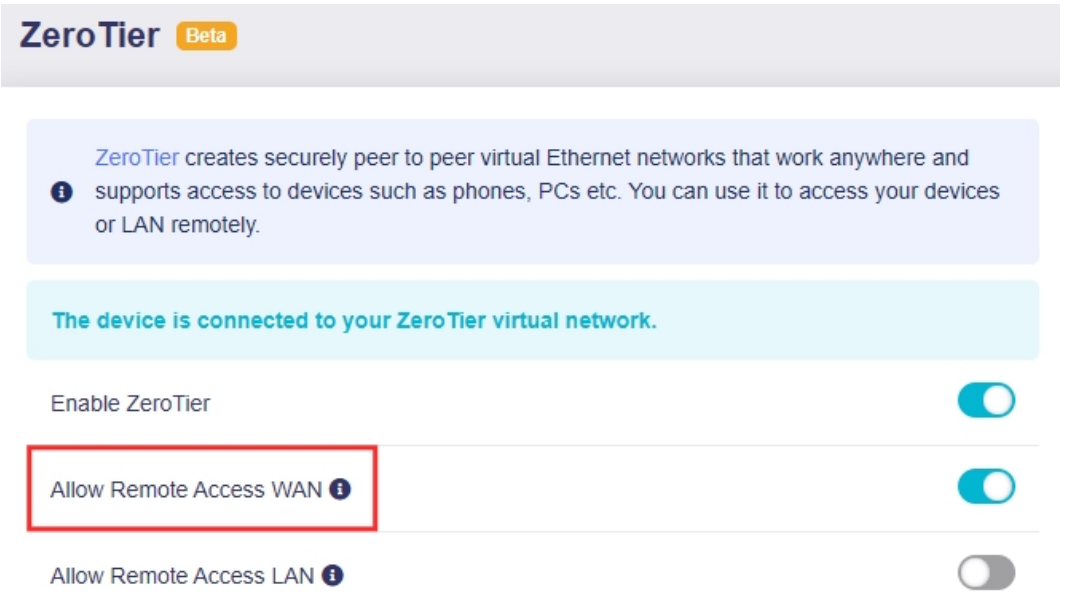
Luego puede usar esta IP administrada para acceder al enrutador desde su computadora portátil que está en la misma red ZeroTier.

9. Pruebe la conectividad.

   En la computadora portátil conectada 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.

15.6.2 Permitir el acceso remoto a la WAN

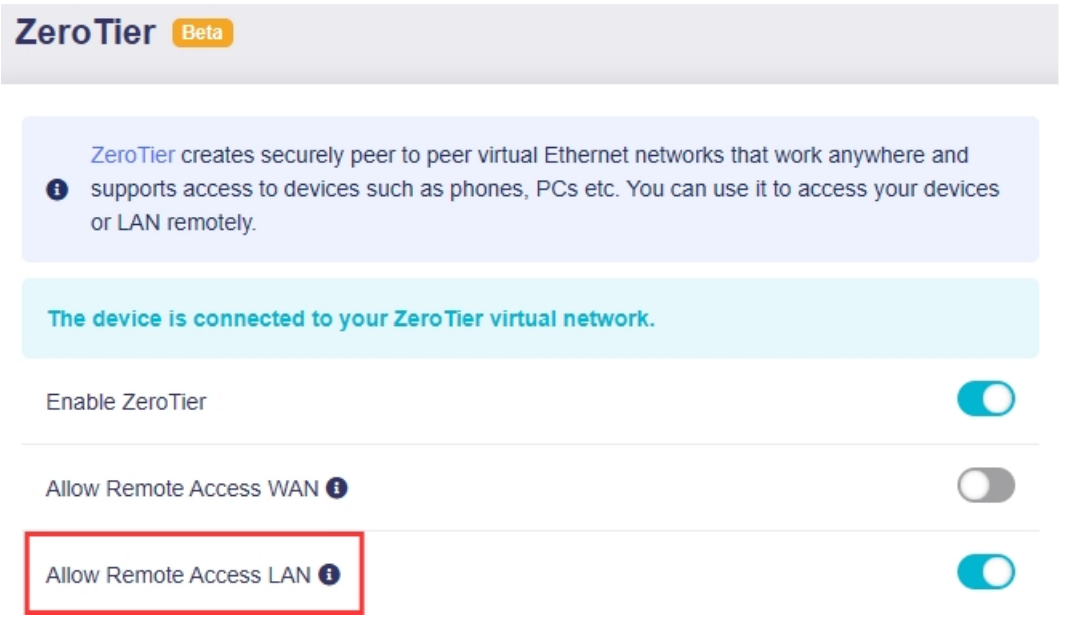
Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta 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. Consulte aquí para detalles de precios.

15.6.3 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.



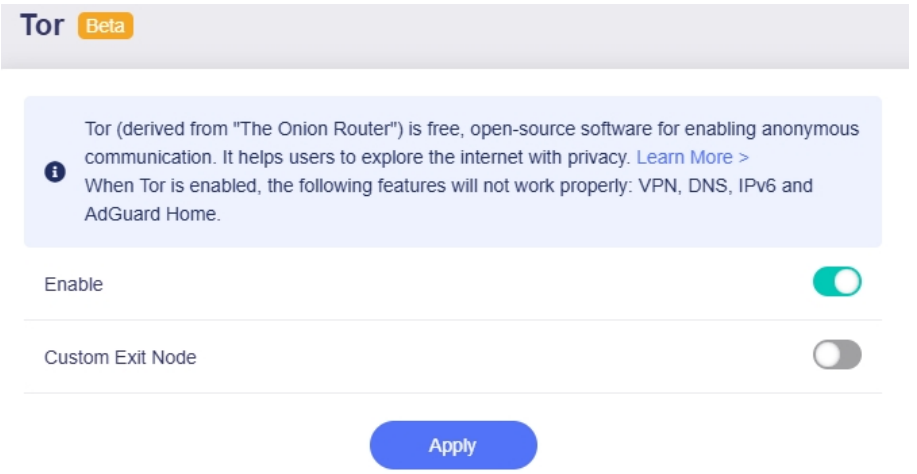
Nota: esta característica requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que surta efecto. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puedes configurar rutas personalizadas con un plan Essential o superior. Consulte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

15.7 Tor

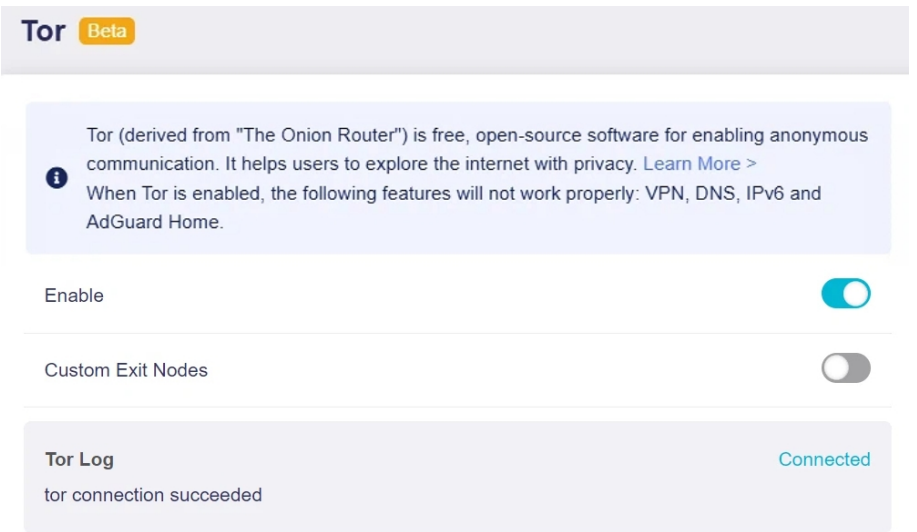
Tor (derivado de **The Onion Router**) es un software gratuito y de código abierto que permite la comunicación anónima. Ayuda a los usuarios a explorar Internet con privacidad. Tenga en cuenta que esta característica se encuentra actualmente en versión beta y puede esta función se encuentra actualmente en versión beta y es posible que tener algunos errores. Cuando Tor está habilitado, laslas siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6, y AdGuard Home.

Siga los pasos a continuación para configurar Tor según sea necesario.

1. Inicie sesión en su enrutador'panel de administración web y navegue hasta **APLICACIONES** > **Tor**. Taleje cambie para habilitarlo, habilite Nodos de salida personalizados según sea necesario y haga clic en **Aplicar**.



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



Capítulo 16

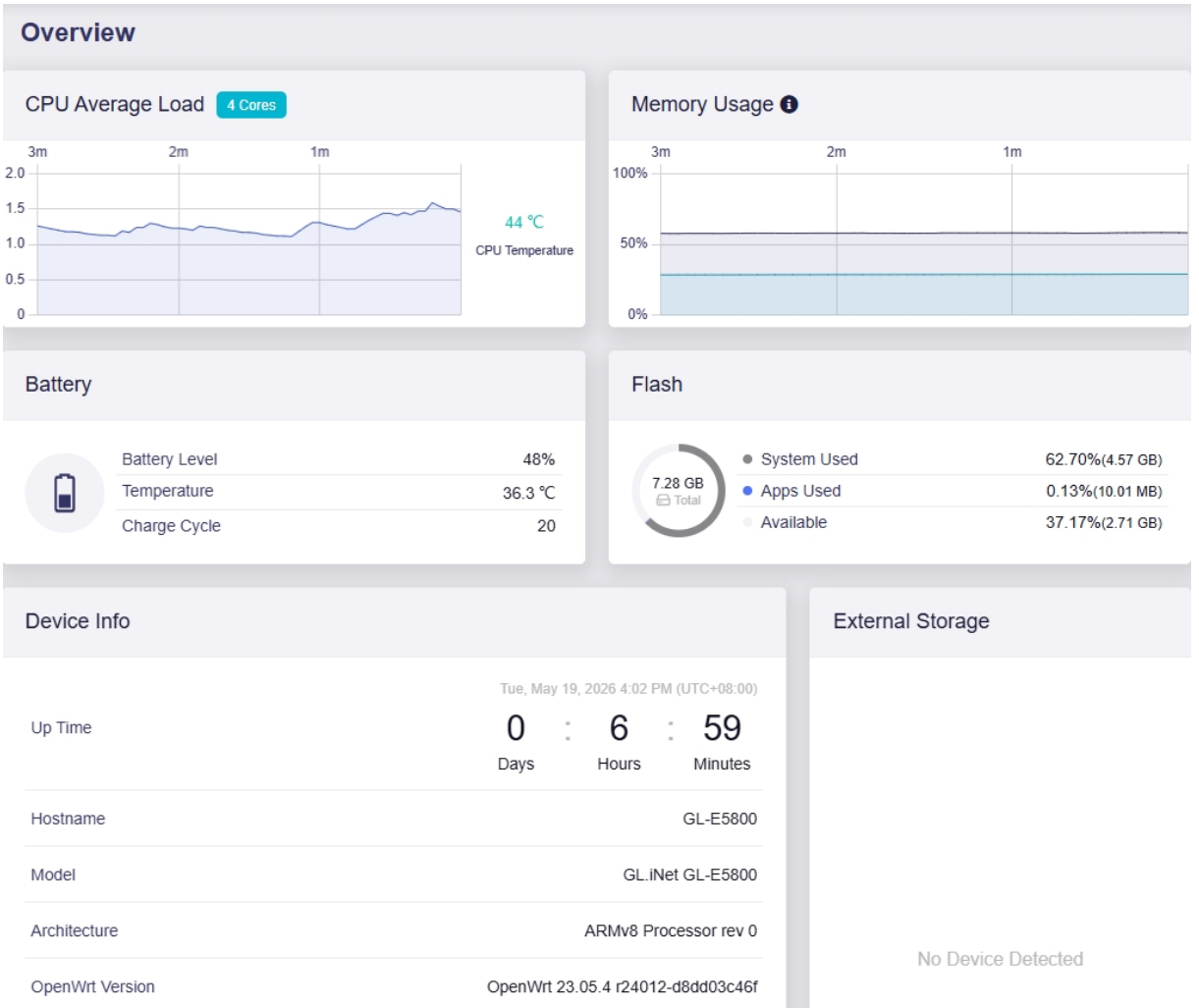
Sistema

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.

16.1 Descripción general

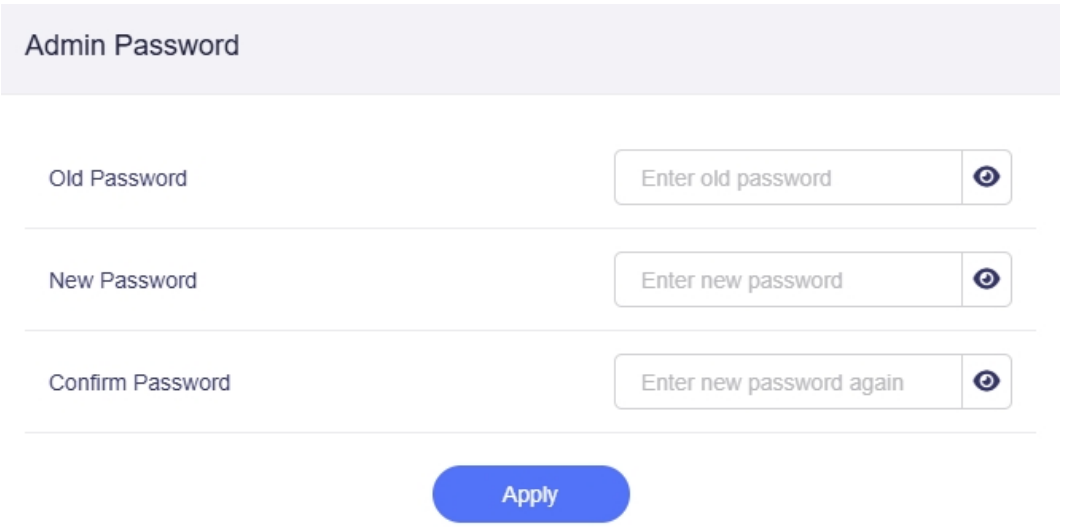
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

- CPU, memoria, y Flash Estado
- Estado de la batería
- Dispositivo Información
- Almacenamiento externo Conmutador de protocolo



16.2 Contraseña de administrador

Inicie sesión en su enrutador’s web admin panel y navegue hasta **SISTEMA** > **Contraseña de administrador**. Puede cambiar la contraseña de inicio de sesión del panel de administración web.



Los requisitos para la contraseña de administrador son los siguientes:

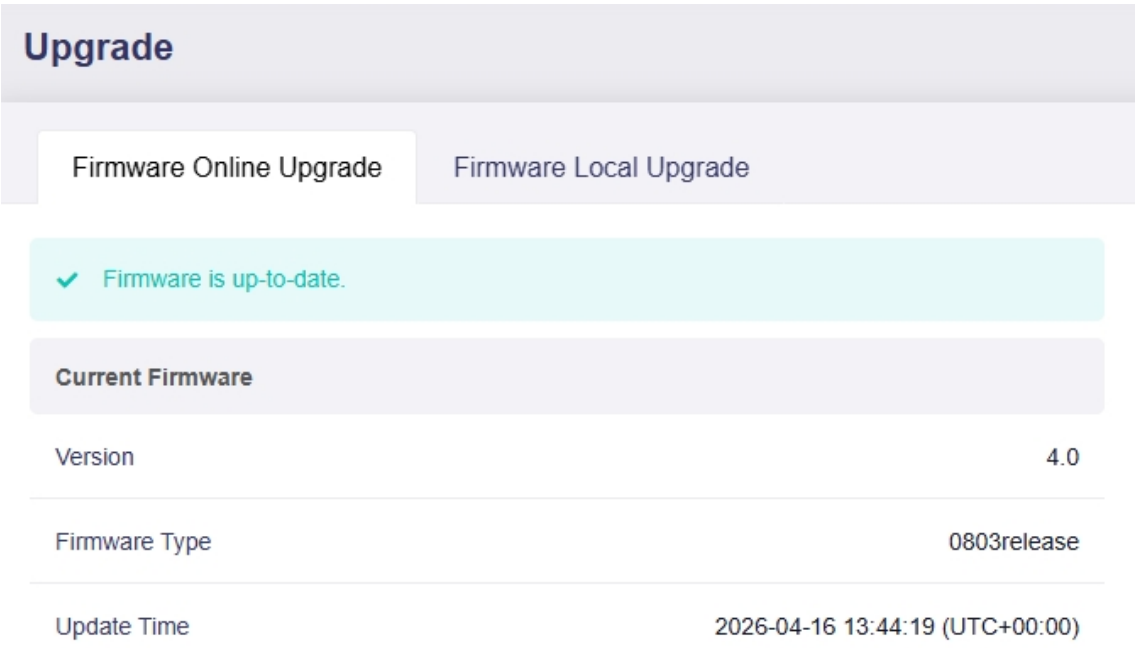
1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distingue entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) están permitidos.
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números y símbolos).

16.3 Actualización

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

16.3.1 Actualización en línea

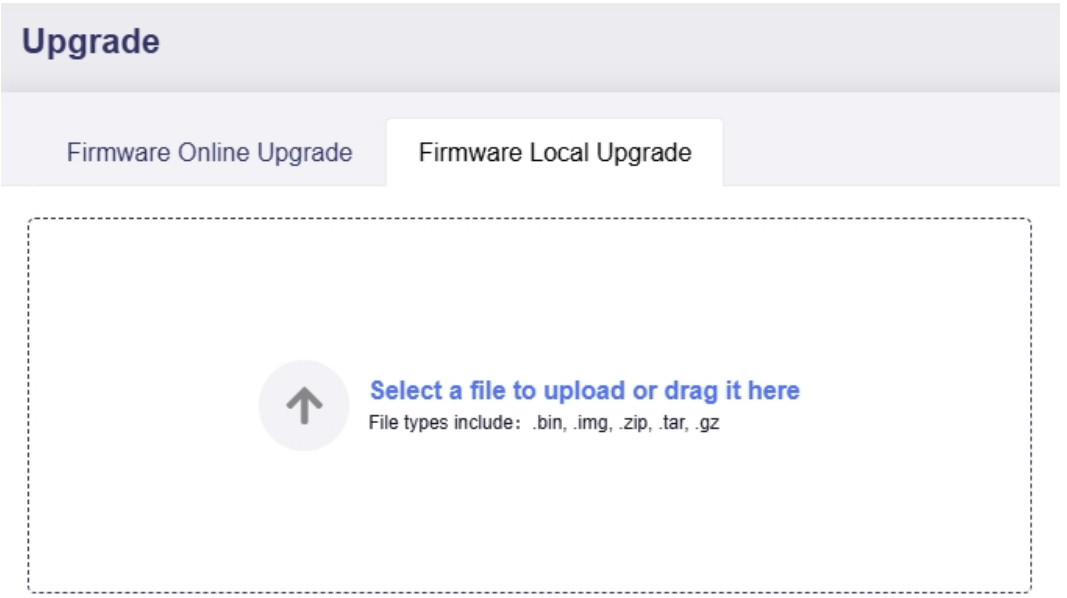
Puede buscar el firmware actual detalles aquí, incluida la versión del firmware, el tipo de firmware (por ejemplo, versión, beta), y hora de actualización. Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.



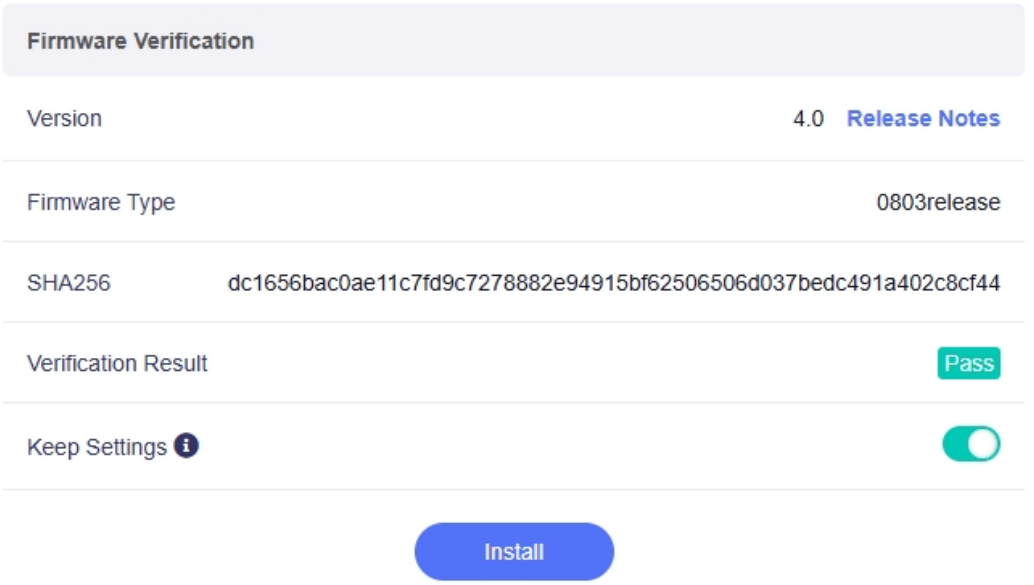
Consejo: Cuando intente realizar una actualización en línea, si muestra **Descarga fallida**, navegue hasta **SISTEMA** -> **Zona horaria** y corrija el error de zona horaria (sincronización con el navegador).

16.3.2 Actualización local

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**.

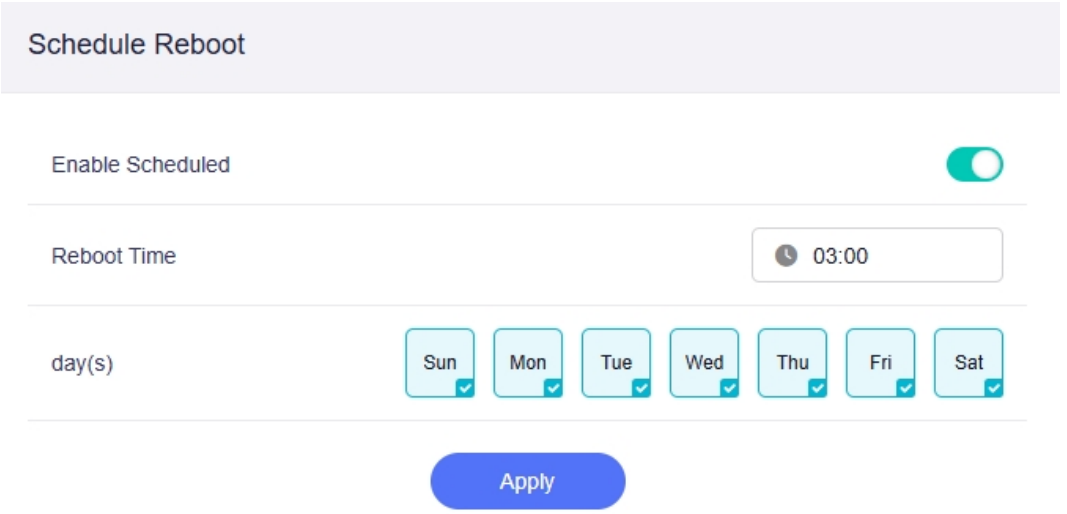


- **Mantener configuración**: si está habilitado, se conserva la configuración actual. Sin embargo, cualquier paquete instalado manualmente debe reinstalarse una vez completada la actualización. No habilite esta opción al degradar el firmware.

16.4 Tareas programadas

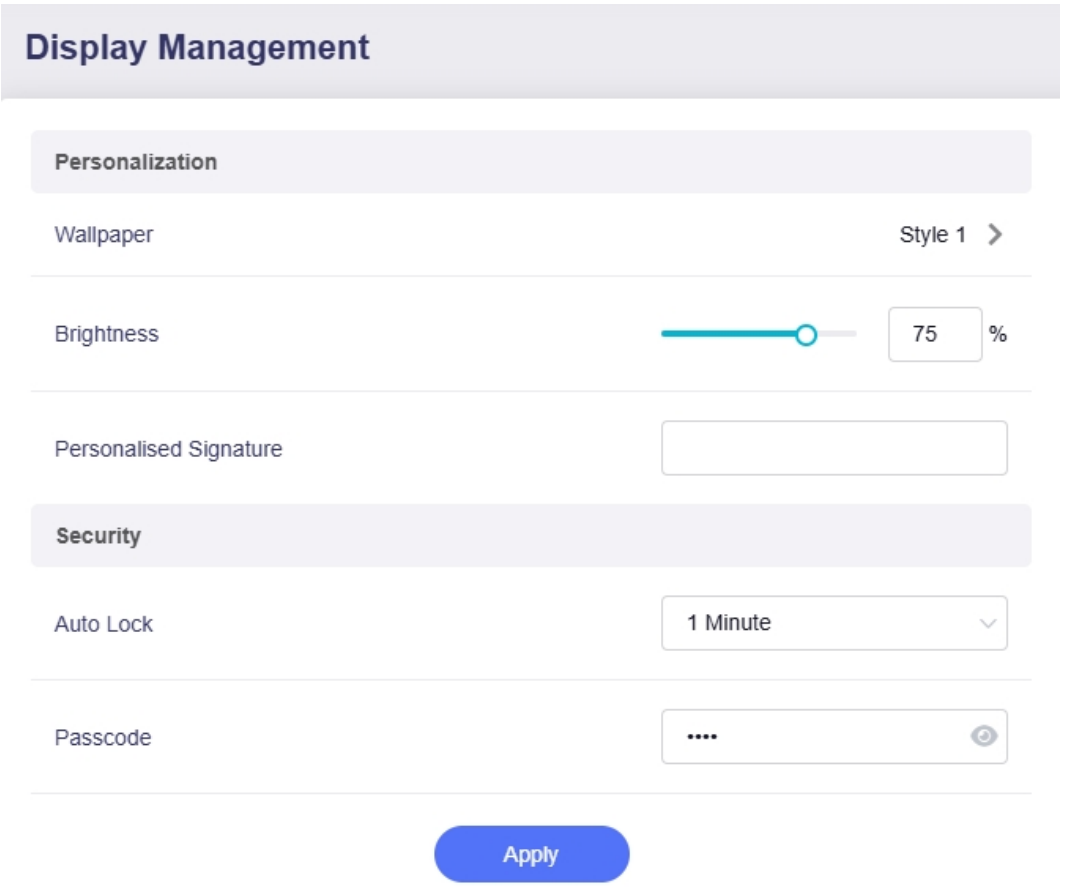
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Tareas programadas**. Esta página le permite establecer un programa de reinicio . Ssincronizar la hora en el Zona horaria antes de utilizar esta función. Si el dispositivo se apaga a la hora programada, la tarea no se ejecutará.

Sestablezca un programa para reiniciar automáticamente su enrutador según sea necesario. Una vez habilitado, configure los tiempos de reinicio, seleccione los días efectivos semanales y luego haga clic en **Aplicar**.



16.5 Gestión de visualización

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Gestión de visualización**. Esta página le permite administrar la pantalla táctil y sus configuraciones relacionadas.



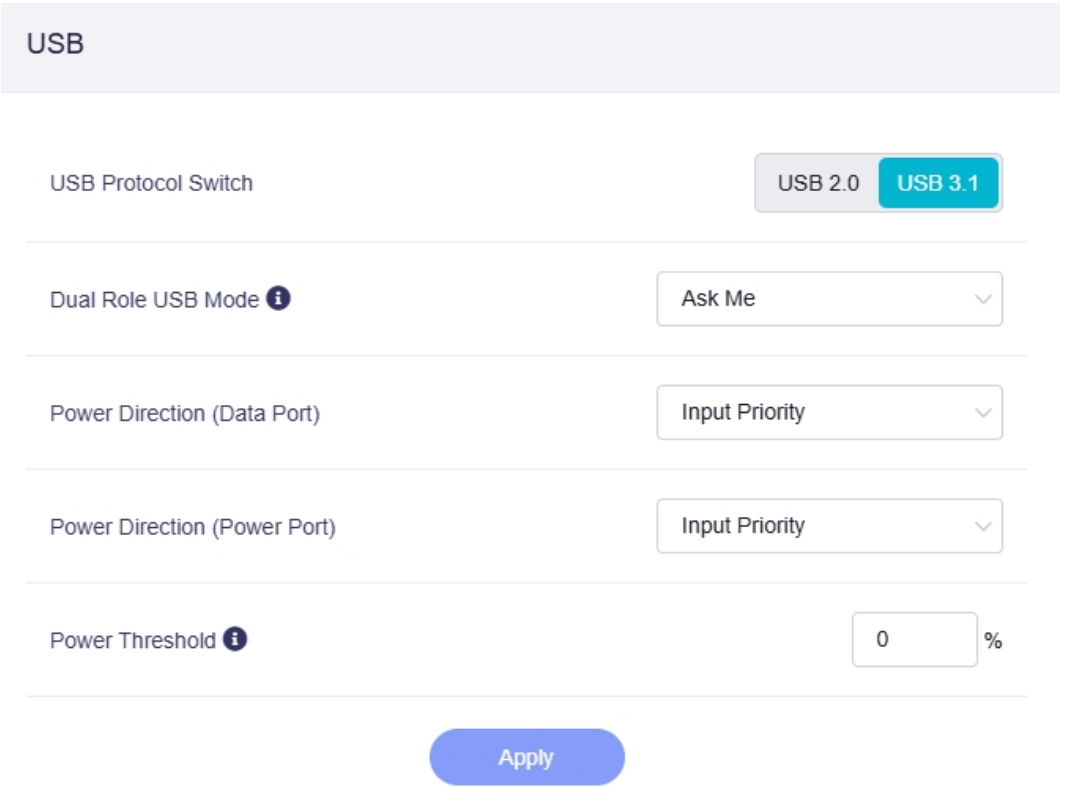
- **Fondo de pantalla**: Personaliza el fondo de pantalla y el estilo de pantalla de activación.
- **Brillo**: ajusta el brillo de la pantalla táctil. Utilice el control deslizante o introduzca un porcentaje para adaptarse a diferentes condiciones de iluminación.
- **PersonalizadosFirma ed**: agregue un texto personalizado a la pantalla táctil para mostrar su estilo único o para una identificación rápida.
- **Bloqueo automático**: establezca el retraso de tiempo para que la pantalla se bloquee automáticamente cuando no haya actividad. El rango es de 15 segundos a 5 minutos.
- **Código de acceso**: establezca un código de acceso de 4 dígitos para la pantalla táctil para obtener una capa adicional de seguridad.

16.6 USB y alimentación

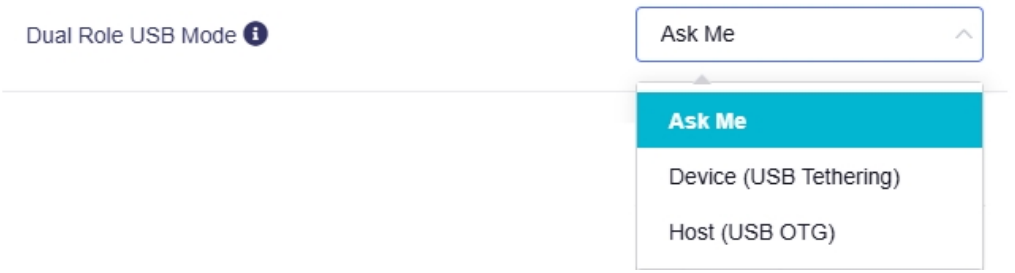
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **USB y alimentación**. Esta página le permite configurar dispositivos relacionados con USB. y energía configuraciones para su enrutador, como protocolo USB, dirección de energía, tiempos de espera de inactividad y comportamiento en espera.

16.6.1 USB

Esta sección le permite personalizar el comportamiento de los puertos USB de su enrutador.



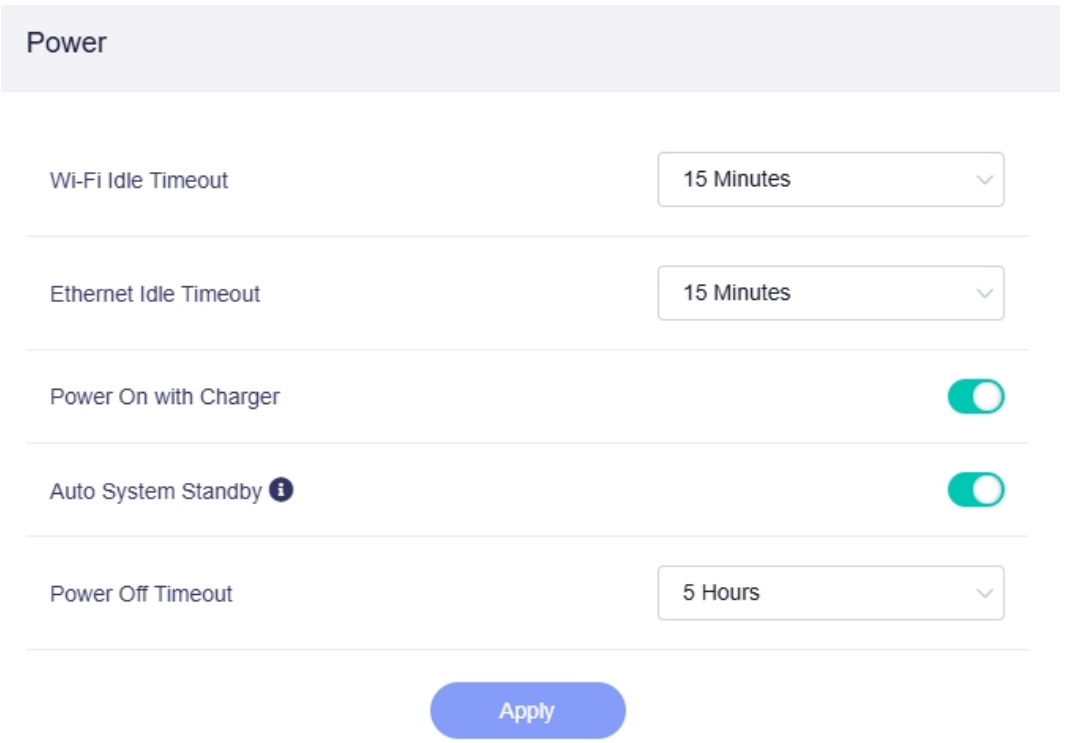
- **Conmutador de protocolo USB**: cambie entre los protocolos USB 2.0 y USB 3.1 para el puerto USB.
- **Modo USB de doble función**: Seleccione el modo de funcionamiento USB en el menú desplegable. Puede configurarlo como Dispositivo o Host.



- **Dirección de potencia**: elija la prioridad de energía para el puerto USB en el menú desplegable. Puede configurarlo como Prioridad de entrada o Prioridad de salida.
- **Umbral de energía**: establezca un porcentaje de umbral de energía específico para el puerto USB para controlar el nivel de energía mínimo requerido para las operaciones USB, lo que ayuda a preservar la vida útil de la batería.

16.6.2 Alimentación

Esto Esta sección le permite optimizar el consumo de energía y el comportamiento del dispositivo.

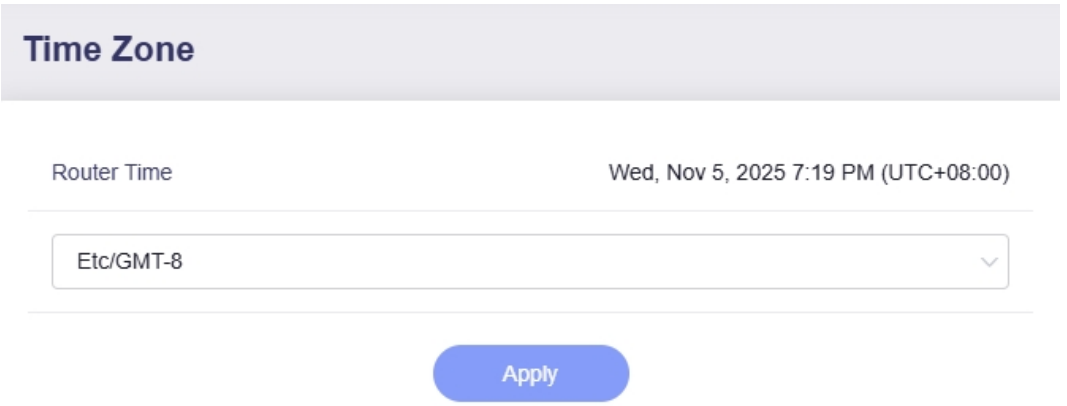


- **Tiempo de espera de inactividad de Wi-Fi**: establezca la duración de inactividad (entre 10 minutos y 2 horas, o nunca) después del cual Wi-Fi entrará en modo de espera.

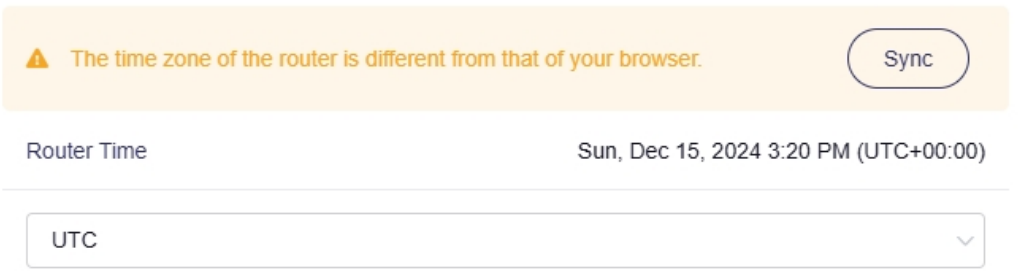
- **Tiempo de espera de inactividad de Ethernet**: establezca la duración de inactividad (de 10 minutos a 2 horas, o nunca) para que Ethernet cambie al modo de espera.
- **Tiempo de espera de apagado**: establezca el tiempo de demora (de 1 hora a 12 horas, o nunca) hasta que el enrutador se apague automáticamente cuando esté inactivo.
- **Encendido con cargador**: active este interruptor para habilitar/deshabilitar el encendido automático del enrutador cuando está conectado a un cargador.
- **Espera automática**: active este interruptor para activar/desactivar el modo de espera automático para ahorrar energía.

16.7 Zona horaria

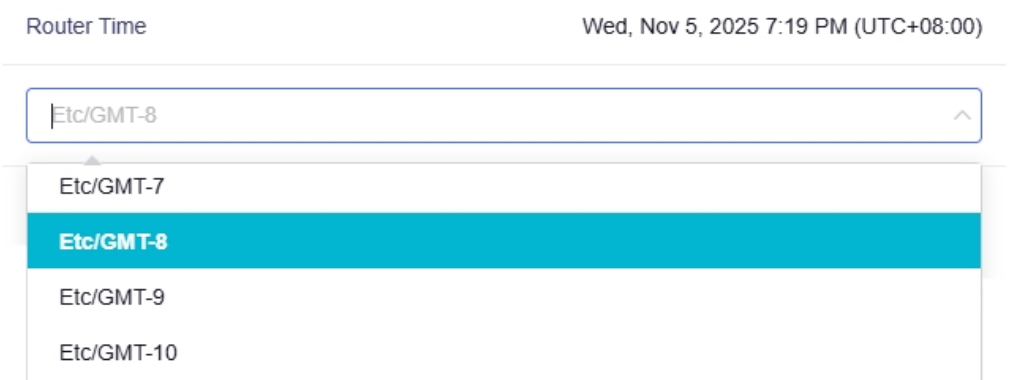
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen del tiempo del sistema del enrutador’para surtir efecto. Por lo tanto, 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.



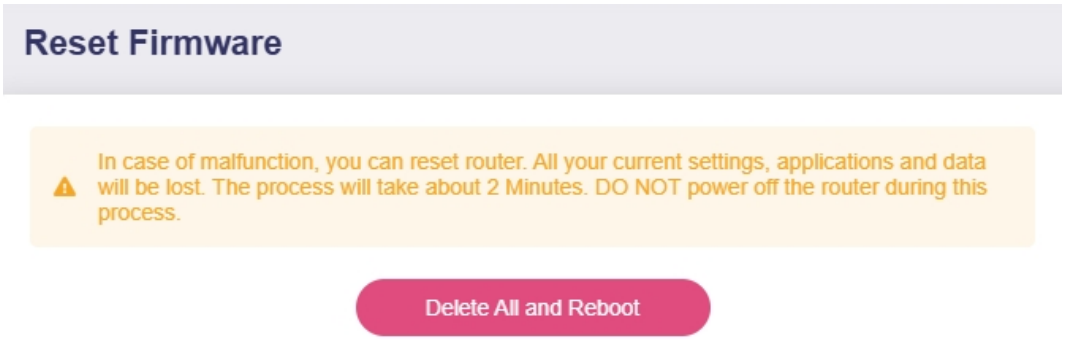
Para cambiar la zona horaria, sseleccione la zona horaria apropiada de la lista para garantizar que la hora del sistema coincida con su hora local.



16.8 Restablecer firmware

Si el enrutador no funciona correctamente, puede intentarlo resolvering el problema restableciendo el firmware.

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

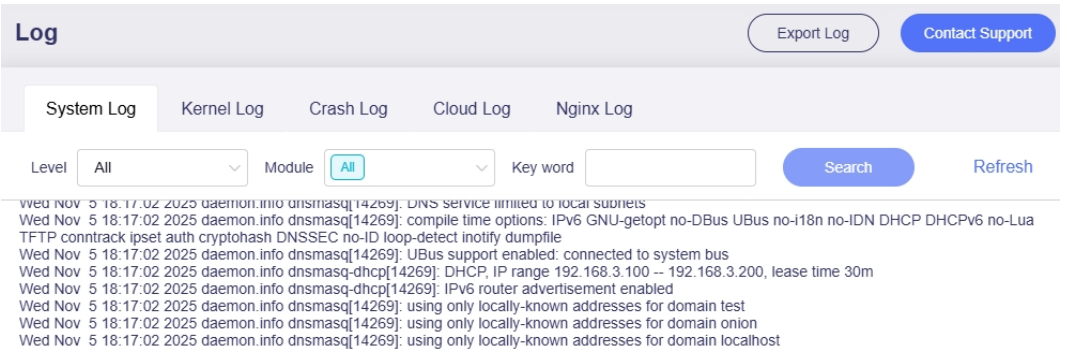


Nota: Todas sus configuraciones, aplicaciones y datos actuales serán borrados. El proceso durará unos 2 minutos. Nono apague el enrutador durante este proceso.

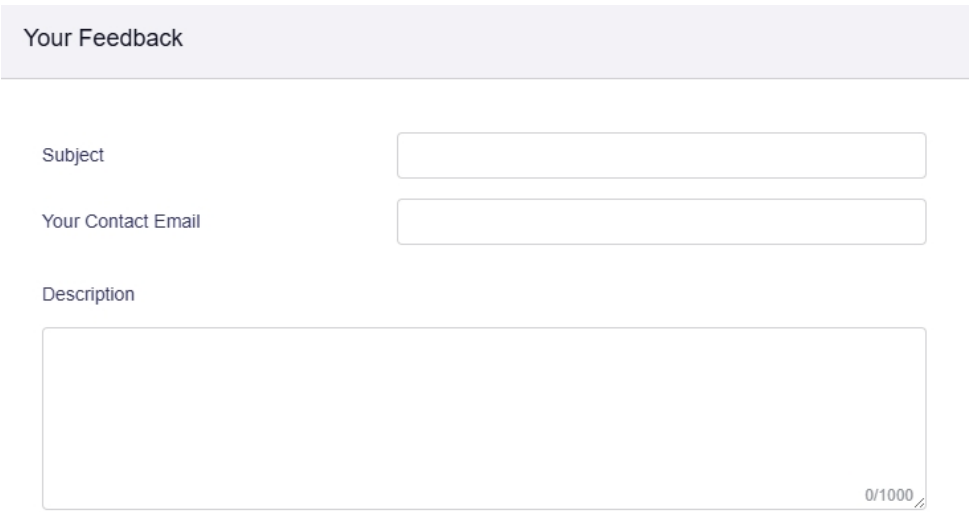
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

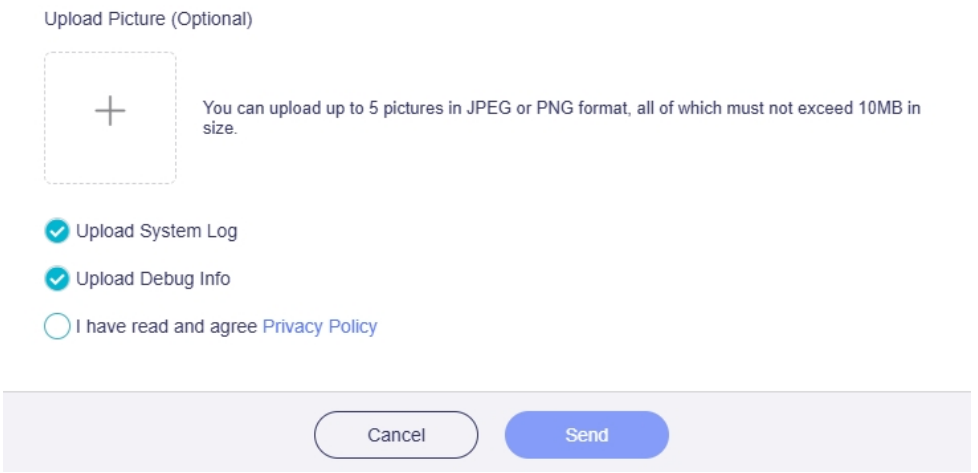
16.9 Registro

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Registro**. Esta página le permite ver registros de System, Kernel, Crash, Cloud y Nginx para análisis y solución de problemas. Además, algunos modelos celulares que admiten eSIM también proporcionan registros eSIM.



- **Buscar**: la página de registro del sistema proporciona filtrado para una búsqueda rápida. Puede seleccionar el nivel de registro (p. ej., todo, información, error) o el módulo (p. ej., IPv6, Conexión, Celular) en 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.



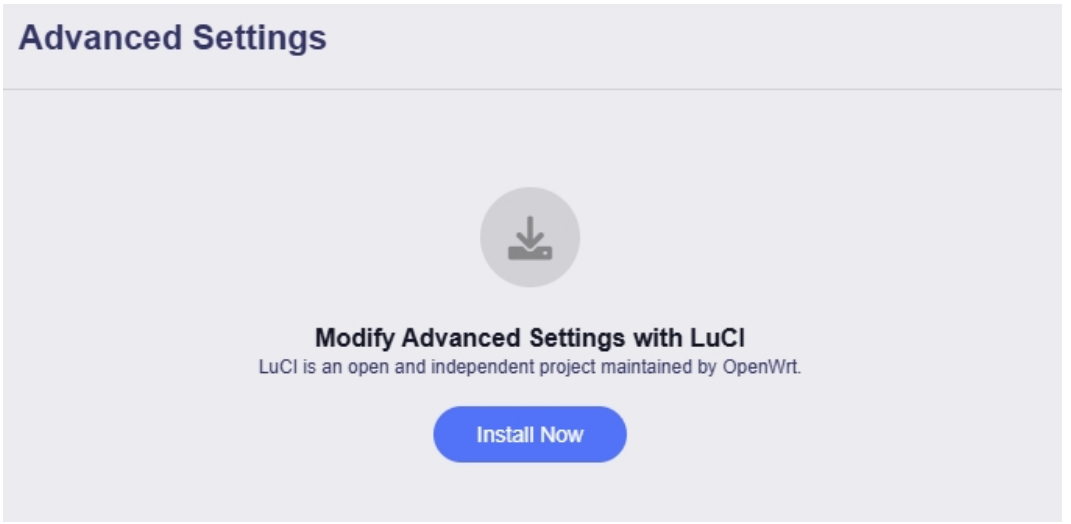

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.10 Configuración avanzada

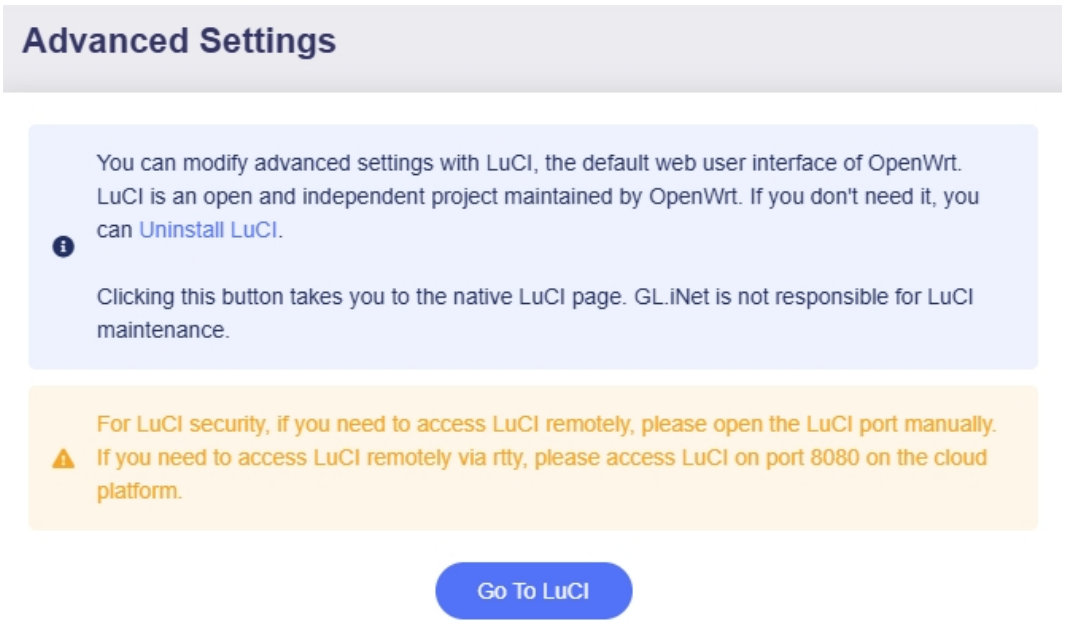
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto 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 LuCI.

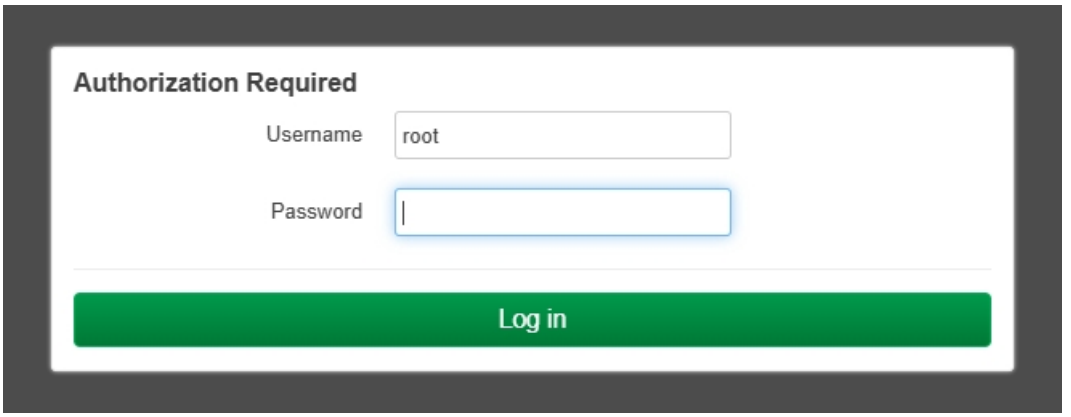
1. Haga clic en **Instalar ahora** y se instalará la interfaz LuCI.



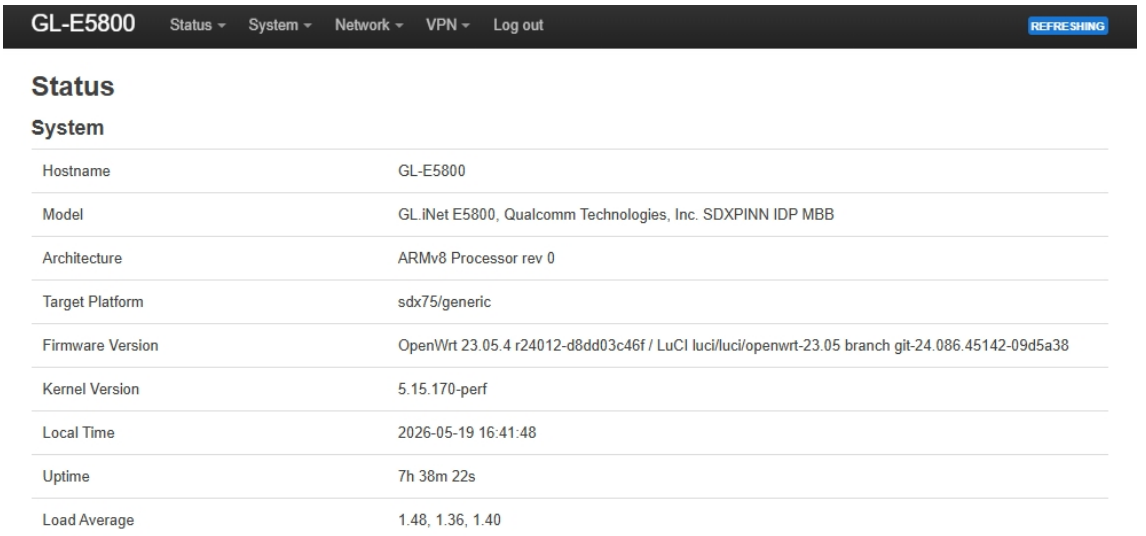
2. Click **Vaya a LuCI**, y será redirigido a la página de inicio de sesión de LuCI.



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



Yusted luego log en a la interfaz LuCI.



Seguridad de la batería

Deje de usar y cargar el Mudi 7 si la batería está hinchada, tiene fugas, está inusualmente caliente o dañada, o desprende un olor inusual.

- No presione, doble, perfore ni aplaste la batería, ni ejerza presión sobre ella.
- No utilice herramientas para hacer palanca contra una batería hinchada o dañada.
- No intente retirar una batería que esté hinchada, atascada, tenga fugas, esté caliente o que, por cualquier otro motivo, no pueda manipularse de forma segura.
- No deseche una batería de iones de litio dañada en la basura doméstica ni en los contenedores de reciclaje habituales.
- No envíe una batería hinchada o dañada por correo ni mediante un servicio de paquetería ordinario.
- Póngase en contacto con el Soporte de GL.iNet para obtener ayuda con la garantía e instrucciones sobre los siguientes pasos.

Si ya ha retirado la batería dañada, no vuelva a instalarla. Póngase en contacto con un centro local adecuado de reciclaje de baterías o de recogida de residuos domésticos peligrosos que acepte baterías de iones de litio dañadas.

Si la batería emite humo, se calienta rápidamente, produce un siseo, arde o presenta cualquier otro peligro inmediato, aléjese del dispositivo y póngase en contacto con los servicios de emergencia locales.

Declaración de Conformidad

Por la presente, GL TECHNOLOGIES (HONG KONG) LIMITED declara que el tipo de equipo radioeléctrico [Router Portátil Wi-Fi 7 Tribanda 5G NR, GL-E5800EU] cumple con 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.