GL·iNet



Instrukcja obsługi

GL-X3000 / Spitz AX

Router 4G/5G Wi-Fi 6 z dwoma kartami SIM

Wersja oprogramowania 4.8.3

O tej instrukcji

Ta instrukcja pomoże rozpocząć korzystanie z urządzenia. Zawiera podstawowe informacje o produkcie, opis podłączania sprzętu, logowania do interfejsu zarządzania w przeglądarce i konfiguracji początkowej, a także szczegółowe instrukcje dotyczące wszystkich funkcji oprogramowania w panelu administracyjnym.

Z tej instrukcji dowiesz się, jak:

- Poznać najważniejsze informacje o produkcie
- Podłączyć sprzęt zgodnie z instrukcjami krok po kroku
- Łatwo zalogować się do interfejsu zarządzania w przeglądarce
- Skonfigurować ustawienia początkowe i korzystać ze wszystkich funkcji oprogramowania w panelu administracyjnym

Konwencje formatowania

Poniższe symbole i kolory ułatwiają wykonywanie opisanych czynności.

Konwencja	Znaczenie
Podkreślony tekst w kolorze turkusowym	Łącze otwierające stronę internetową lub określoną sekcję
Tekst pogrubiony	Wyróżnia lub oznacza istotne informacje w tym dokumencie, takie jak tytuły, hiperłącza oraz dokładne nazwy menu i elementów w interfejsie internetowym urządzenia
>	Ścieżka otwierania odpowiedniej strony (np. System > Firmware)
Uwaga	Ważne informacje dotyczące konfiguracji, obsługi i bezpieczeństwa. Ich zignorowanie może skutkować niepowodzeniem konfiguracji, nieprawidłowym działaniem lub uszkodzeniem urządzenia
Wskazówki	Porady ułatwiające korzystanie z urządzenia

Uwaga:

- Funkcje urządzenia mogą się różnić w zależności od modelu i wersji oprogramowania.

- Dostępność produktu zależy od regionu lub specyfikacji dostawcy usług internetowych.
- Wszystkie ilustracje, procedury i opisy w tej instrukcji mają charakter poglądowy i mogą różnić się od rzeczywistego sposobu korzystania z urządzenia.

Potrzebujesz pomocy lub dodatkowych informacji?

- Aktualizacja oprogramowania: Centrum pobierania oprogramowania GL.iNet | Router
- Społeczność: porozmawiaj o naszych produktach i wymieniaj się doświadczeniami na forum społeczności GL.iNet
- Pomoc techniczna: skontaktuj się z naszym zespołem pomocy technicznej na stronie kontaktowej

Prawa autorskie © 2026 GL.iNet Technology (HK) Ltd. Wszelkie prawa zastrzeżone.
Żadna część tej instrukcji nie może być powielana, przepisywana, tłumaczona ani rozpowszechniana w jakiejkolwiek formie i w jakikolwiek sposób bez uprzedniej pisemnej zgody GL.iNet Technology (HK) Ltd. GL.iNet jest zastrzeżonym znakiem towarowym GL.iNet Technology (Hong Kong) Ltd. w Chinach oraz innych krajach i regionach. Wszystkie pozostałe wymienione nazwy marek i produktów są znakami towarowymi lub zastrzeżonymi znakami towarowymi ich właścicieli.
Treść tego dokumentu może ulec zmianie bez powiadomienia w związku z aktualizacją wersji produktu lub z innych przyczyn. O ile nie uzgodniono inaczej, dokument służy wyłącznie celom informacyjnym, a żadne zawarte w nim stwierdzenia, informacje i zalecenia nie stanowią jakiejkolwiek gwarancji.

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

Spis treści

Rozdział 1 Poznaj swój router 9
1.1 Opis produktu 10
1.1.1 Wygląd 10
1.1.2 Złącza i przyciski 11
1.1.3 Dioda LED 12
1.2 Dane techniczne 13
1.3 Zawartość opakowania 14
Rozdział 2 Podłączanie sprzętu 15
2.1 Wybór miejsca 16
2.2 Podłączanie routera 16
Rozdział 3 Logowanie do routera 17
Rozdział 4 Konfiguracja połączenia z Internetem 19
4.1 Kreator szybkiej konfiguracji 20
4.2 Ręczna konfiguracja połączenia z Internetem 21
4.2.1 Połączenie z Internetem przez kabel Ethernet 21
4.2.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi 27
4.2.3 Połączenie z Internetem przez tethering USB 40
4.2.4 Połączenie z Internetem przez sieć komórkową 44
Rozdział 5 Sieć bezprzewodowa 68
5.1 Wyświetlanie stanu Wi-Fi 69
5.2 Ustawienia sieci bezprzewodowej 70
5.2.1 Wi-Fi 5 GHz 70
5.2.2 Wi-Fi 2,4 GHz 72
5.2.3 Losowy BSSID 74
Rozdział 6 Urządzenia klienckie 76
6.1 Szczegóły urządzenia 77
6.2 Działania 80
6.3 Usuwanie urządzeń klienckich 83
6.4 Sortowanie 83
Rozdział 7 Usługi w chmurze 84
7.1 GoodCloud 85
7.1.1 Włączanie GoodCloud 86

7.1.2 Zarządzanie routerem 88
7.1.3 Usuwanie powiązania urządzenia 93
7.1.4 Wyłączanie GoodCloud 93
7.2 AstroWarp 94
Rozdział 8 Poznaj VPN 95
8.1 Wprowadzenie 96
8.1.1 VPN 96
8.1.2 Router VPN 96
8.1.3 OpenVPN 96
8.1.4 WireGuard 96
8.2 Przykłady zastosowań 97
Rozdział 9 Panel VPN 100
9.1 Kreator konfiguracji VPN 101
9.2 Tryb VPN 105
9.2.1 Tryb globalny 106
9.2.2 Tryb reguł 107
Rozdział 10 Konfiguracja serwera VPN 116
10.1 Serwer OpenVPN 117
10.1.1 Przygotowanie 117
10.1.2 Etapy konfiguracji 118
10.1.3 Sprawdzanie połączenia 121
10.1.4 Opcje serwera 122
10.1.5 Komunikacja między klientami 123
10.2 Serwer WireGuard 126
10.2.1 Przygotowanie 126
10.2.2 Etapy konfiguracji 127
10.2.3 Sprawdzanie połączenia 131
10.2.4 Opcje serwera 132
Rozdział 11 Konfiguracja klienta VPN 134
11.1 Klient OpenVPN 135
11.1.1 Przygotowanie 135
11.1.2 Konfiguracja NordVPN 135
11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy) 141
11.2 Konfiguracja klienta WireGuard 144

11.2.1 Przygotowanie 144
11.2.2 Konfiguracja AzireVPN 145
11.2.3 Konfiguracja Hide.me 149
11.2.4 Konfiguracja IPVanish 152
11.2.5 Konfiguracja Mullvad 157
11.2.6 Konfiguracja NordVPN 161
11.2.7 Konfiguracja PIA (Private Internet Access) 166
11.2.8 Konfiguracja Surfshark 170
11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy) 175
Rozdział 12 Tor 180
Rozdział 13 Aplikacje 183
13.1 Wtyczki 184
13.2 Dynamiczny DNS 185
13.2.1 Włączanie DDNS 185
13.2.2 Sprawdzanie działania DDNS 188
13.2.3 Zdalny dostęp przez HTTPS 190
13.2.4 Zdalny dostęp przez SSH 192
13.3 Pamięć sieciowa 194
13.3.1 Podłączanie pamięci 194
13.3.2 Konfiguracja usługi Samba 195
13.3.3 Konfiguracja WebDAV 198
13.3.4 Konfiguracja DLNA 201
13.4 AdGuard Home 202
13.5 Kontrola rodzicielska 205
13.5.1 Szybka konfiguracja 205
13.5.2 Rozwiązywanie problemów 214
13.6 ZeroTier 215
13.6.1 Konfiguracja ZeroTier 216
13.6.2 Zdalny dostęp do WAN 220
13.6.3 Zdalny dostęp do LAN 221
13.7 Tailscale 222
13.7.1 Konfiguracja Tailscale 223
13.7.2 Zdalny dostęp do WAN 226
13.7.3 Zdalny dostęp do LAN 227

13.7.4 Niestandardowe węzły wyjściowe 228
13.8 Zarządzanie eSIM 229
13.8.1 Bieżący stan eSIM 230
13.8.2 Lista profili eSIM 231
Rozdział 14 Sieć 238
14.1 Przekierowanie portów 239
14.1.1 DMZ 239
14.1.2 Przekierowanie portów 240
14.2 Multi-WAN 242
14.2.1 Monitorowanie stanu interfejsów 242
14.2.2 Tryb Multi-WAN 245
14.3 LAN 248
14.3.1 Ustawienia podstawowe 248
14.3.2 Serwer DHCP 249
14.3.3 Rezerwacja adresów 251
14.4 Sieć gościnna 252
14.4.1 Ustawienia podstawowe 252
14.4.2 Serwer DHCP 253
14.5 DNS 255
14.5.1 Ustawienia ogólne 255
14.5.2 Ustawienia serwera DNS 256
14.5.3 Edycja pliku hosts 258
14.6 Port Ethernet 260
14.7 Tryb sieciowy 261
14.8 IPv6 263
14.8.1 Tryb IPv6 264
14.8.2 Sposób uzyskiwania DNS 264
14.9 Drop-in Gateway 265
14.10 IGMP Snooping 267
14.11 Przyspieszanie sieci 268
14.12 Ustawienia NAT 269
Rozdział 15 System 270
15.1 Przegląd 271
15.2 Aktualizacja 272

15.2.1 Aktualizacja oprogramowania sprzętowego online 272
15.2.2 Lokalna aktualizacja oprogramowania sprzętowego 273
15.2.3 Aktualizacja modemu online 274
15.2.4 Lokalna aktualizacja modemu 274
15.3 Zadania zaplanowane 275
15.3.1 Harmonogram diody LED 275
15.3.2 Harmonogram ponownego uruchamiania 276
15.3.3 Harmonogram Wi-Fi 5 GHz 277
15.3.4 Harmonogram Wi-Fi 2,4 GHz 279
15.4 Strefa czasowa 281
15.5 Dziennik 282
15.6 Bezpieczeństwo 284
15.6.1 Hasło administratora 284
15.6.2 Kontrola dostępu 285
15.6.3 Kontrola dostępu zdalnego 287
15.6.4 Otwieranie portów routera 288
15.7 Resetowanie oprogramowania 289
15.8 Ustawienia zaawansowane 290
Oświadczenia dotyczące zgodności z przepisami 292

Rozdział 1

Poznaj swój router

W tym rozdziale przedstawiono ogólne informacje o routerze, dane techniczne i zawartość opakowania.

1.1 Opis produktu

Spitz AX (GL-X3000) to brama komórkowa Wi-Fi 6 z obsługą dwóch kart SIM, zaprojektowana z myślą o szybkim i niezawodnym połączeniu, szczególnie w odległych lokalizacjach i podczas podróży samochodem. Oferuje cztery metody dostępu do Internetu: sieć komórkową (karty SIM), Ethernet, Repeater i tethering. Obsługuje Multi-WAN (przełączanie awaryjne i równoważenie obciążenia), VPN (OpenVPN i WireGuard), kontrolę rodzicielską, AdGuard Home, przekierowanie portów, Tailscale i inne funkcje.

1.1.1 Wygląd

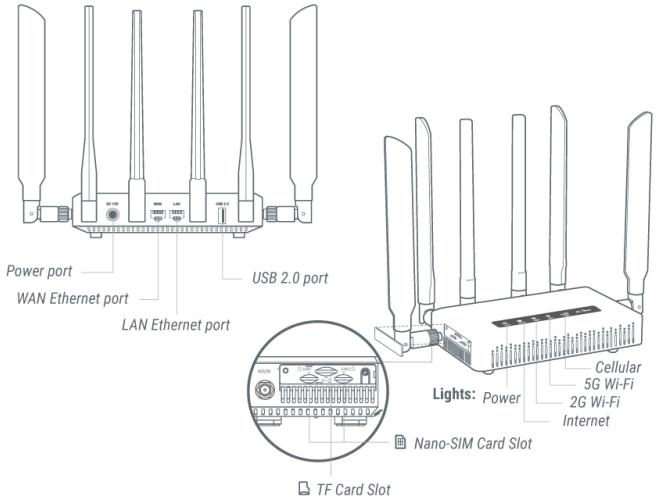








1.1.2 Złącza i przyciski



Element	Opis
Port Ethernet WAN	Łączy router z siecią nadrzędną z prędkością 10/100/1000/2500 Mb/s.
Port Ethernet LAN	Łączy przewodowe urządzenie klienckie z routerem z prędkością 10/100/1000 Mb/s.
Port USB 2.0	Do podłączania obsługiwanego modemu USB, urządzenia udostępniającego Internet przez USB lub nośnika USB.
Gniazdo kart MicroSD	Obsługuje kartę MicroSD o maksymalnej pojemności 1 TB.
Gniazda kart Nano-SIM	Do umieszczenia dwóch kart Nano-SIM. Jednocześnie aktywna jest tylko jedna karta SIM; druga pełni funkcję zapasową.
Przycisk resetowania	Naciśnij na mniej niż 3 sekundy, aby zresetować sieć, lub na 10 sekund, aby przywrócić ustawienia fabryczne.
Wejście zasilania DC5521	Obsługuje dołączony zasilacz 12 V/2,5 A lub zasilanie prądem stałym 9–36 V.
Złącza anten komórkowych	Do podłączania czterech anten komórkowych (SMA, 600 MHz–6 GHz).
Złącza anten Wi-Fi	Do podłączania dwóch anten Wi-Fi (PR-SMA, 2,4–2,5 GHz i 5,15–5,84 GHz).

1.1.3 Dioda LED

Stan urządzenia	Zasilanie	Internet	2,4 GHz	5 GHz	Łączność komórkowa
Połączenie z Internetem (sieć komórkowa aktywna)	Świeci na zielono	Świeci na zielono	Świeci na zielono	Świeci na zielono	Świeci na zielono
Połączenie z Internetem (sieć komórkowa nieaktywna)	Świeci na zielono	Świeci na zielono	Świeci na zielono	Świeci na zielono	Wyłączona
Brak Internetu	Świeci na zielono	Wyłączona	Świeci na zielono	Świeci na zielono	Wyłączona
Aktualizacja oprogramowania sprzętowego	Świeci na zielono	Miga co 0,5 s	Miga co 0,5 s	Miga co 0,5 s	Świeci na zielono
Resetowanie sieci (przytrzymanie przycisku resetowania < 3 s)	Miga co 1 s	Świeci na zielono	Świeci na zielono	Świeci na zielono	Świeci na zielono
Przywracanie ustawień fabrycznych (przytrzymanie przycisku resetowania przez 10 s)	Miga co 0,25 s	Świeci na zielono	Świeci na zielono	Świeci na zielono	Świeci na zielono

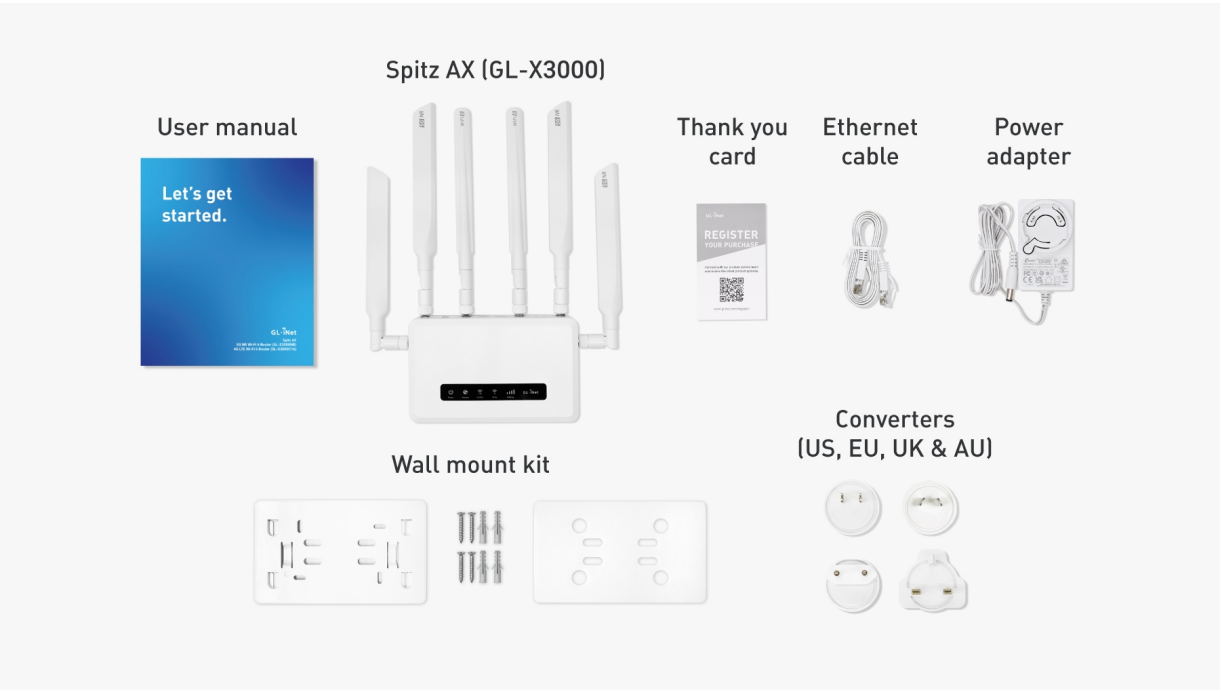
Wskazówki: Gdy router jest połączony z Internetem, migająca dioda 2,4 GHz lub 5 GHz oznacza, że urządzenia Wi-Fi są połączone i aktywnie przesyłają dane.

1.2 Dane techniczne

Element	Szczegóły
Złącza	1 × port Ethernet WAN 1 × port Ethernet LAN 1 × port USB 2.0 1 × gniazdo kart MicroSD (maks. 1 TB) 2 × gniazdo kart Nano-SIM 1 × przycisk resetowania
Procesor	Dwurdzeniowy procesor MediaTek, 1,3 GHz
Pamięć RAM / pamięć masowa	DDR4 512 MB / eMMC 8 GB
Protokół	IEEE 802.11a/b/g/n/ac/ax
Prędkość Wi-Fi	574 Mb/s (2,4 GHz), 2402 Mb/s (5 GHz)
Prędkość Ethernet	Port WAN: 10/100/1000/2500 Mb/s Port LAN: 10/100/1000 Mb/s
Anteny	4 × antena komórkowa (SMA, 600 MHz–6 GHz) 2 × antena Wi-Fi (PR-SMA, 2,4–2,5 GHz, 5,15–5,84 GHz)
Diody LED	System / Wi-Fi 5 GHz / Wi-Fi 2,4 GHz / Internet / siła sygnału komórkowego
Zasilanie	DC5521, 12 V/2,5 A (5,5 × 2,1 mm) [domyślny zasilacz] / 9–36 V
Pobór mocy	<14W
Temperatura pracy	0 ~ 40°C (32 ~ 104°F)
Temperatura przechowywania	-20 ~ 70°C (-4 ~ 158°F)
Wymiary / masa	155 × 95 × 36 mm / 520 g
Inne materiały i narzędzia	Karta katalogowa | Oprogramowanie | Aplikacja | Rozpakowanie | Poradniki | Materiały prasowe

1.3 Zawartość opakowania

- 1 × Spitz AX (GL-X3000)
- 1 × instrukcja obsługi
- 1 × karta z podziękowaniem
- 1 × kabel Ethernet
- 1 × zestaw do montażu na ścianie
- 1 × zasilacz
- 4 × przejściówka



Rozdział 2

Podłączanie sprzętu

W tym rozdziale opisano wybór miejsca ustawienia routera i czynności związane z jego podłączaniem.

2.1 Wybór miejsca

Aby uzyskać najlepszą wydajność, wybierz miejsce zgodnie z poniższymi wskazówkami.

- Unikaj wilgoci i wysokiej temperatury: nie umieszczaj routera w miejscach narażonych na wodę, wilgoć lub wysoką temperaturę (np. przy zlewach lub grzejnikach).
- Wentylacja i chłodzenie: ustaw router w chłodnym, dobrze wentylowanym miejscu, aby zapewnić odpowiednie odprowadzanie ciepła.
- Centralne położenie: ustaw router w miejscu, w którym łatwo podłączyć zasilanie i wiele urządzeń (np. w centralnej części salonu).
- Ułożenie przewodów: poprowadź kable i przewód zasilający w sposób zapobiegający potknięciu.
- Ustawienie: umieść router na płaskiej, stabilnej powierzchni (półce, biurku) lub zamontuj go na ścianie za pomocą dołączonego zestawu montażowego.
- Unikanie zakłóceń elektromagnetycznych: umieść router z dala od źródeł zakłóceń elektromagnetycznych (urządzeń Bluetooth, kuchenek mikrofalowych), aby ograniczyć zakłócenia sygnału.

2.2 Podłączanie routera

1. **Włącz zasilanie**

   Połącz obie części zasilacza. Podłącz go do routera i do gniazdka elektrycznego. Router uruchomi się automatycznie.

2. **Podłącz urządzenie do routera**

   Podłącz urządzenie (np. laptop lub smartfon) do routera przez Wi-Fi lub za pomocą kabla Ethernet.

   - **Wi-Fi:** na swoim urządzeniu przejdź do Ustawienia > WLAN, znajdź nazwę sieci Wi-Fi routera na liście dostępnych sieci i wprowadź hasło. Domyślną nazwę sieci i hasło znajdziesz na etykiecie routera.
   - **Ethernet:** podłącz urządzenie do portu LAN routera za pomocą kabla Ethernet.

3. **Zaloguj się do routera**

   Przy pierwszym połączeniu z routerem Internet jest niedostępny. Przed uzyskaniem dostępu do Internetu zaloguj się do routera zgodnie z opisem w rozdziale 3 i wykonaj konfigurację początkową.

Rozdział 3

Logowanie do routera

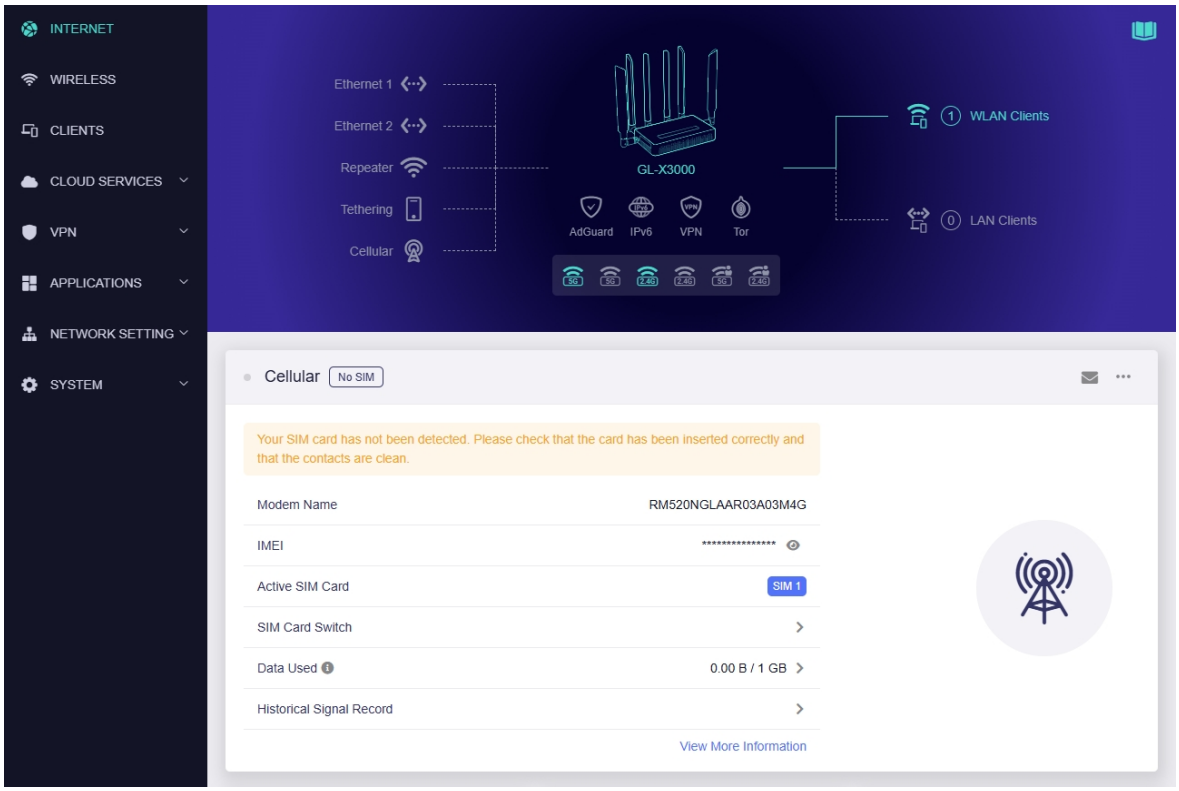
W tym rozdziale opisano logowanie do routera przez panel administracyjny w przeglądarce.

Router można konfigurować i zarządzać nim za pomocą interfejsu w przeglądarce internetowej. Jest on dostępny w systemach Windows, Mac OS i Linux za pośrednictwem przeglądarki, takiej jak Microsoft Edge, Google Chrome, Mozilla Firefox lub Apple Safari.

Uwaga: jeśli wolisz korzystać z aplikacji GL.iNet zamiast panelu administracyjnego, pobierz aplikację i postępuj zgodnie z instrukcjami na ekranie.

Aby zalogować się do routera przez panel administracyjny, wykonaj poniższe czynności.

1. Podłącz urządzenie (np. komputer stacjonarny lub laptop) do routera przez Wi-Fi lub za pomocą kabla Ethernet.
2. Otwórz przeglądarkę internetową (zalecane są Chrome i Edge) i przejdź pod adres http://192.168.8.1. Otworzy się strona logowania do panelu administracyjnego. Jeśli nie możesz uzyskać do niego dostępu, wskazówki dotyczące rozwiązywania problemów znajdziesz tutaj.
3. Ustaw hasło administratora. Ze względów bezpieczeństwa zaleca się użycie silnego hasła. Następnie kliknij **Next**, aby kontynuować.
4. Otworzy się panel administracyjny routera.



Rozdział 4

Konfiguracja połączenia z Internetem

W tym rozdziale przedstawiono różne sposoby łączenia routera z Internetem, dostosowane do różnych środowisk sieciowych.

4.1 Kreator szybkiej konfiguracji

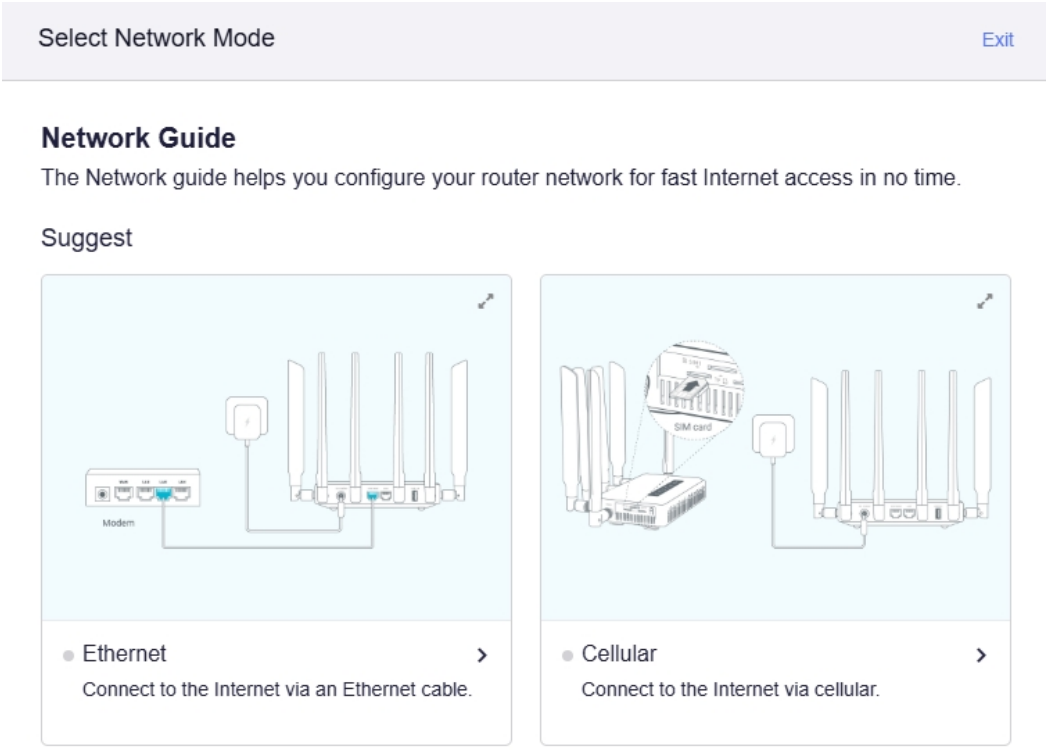
Kreator konfiguracji w przeglądarce przeprowadzi Cię przez konfigurację sieci routera.

Aby uruchomić kreator, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera zgodnie z opisem w rozdziale 3.
2. Na stronie głównej kliknij ikonę książki w prawym górnym rogu.



3. Postępuj zgodnie z instrukcjami kreatora konfiguracji, aby skonfigurować router i nawiązać połączenie z Internetem.



Jeśli korzystasz z aplikacji GL.iNet, skonfiguruj dostęp do Internetu zgodnie z instrukcjami na ekranie.

4.2 Ręczna konfiguracja połączenia z Internetem

Kreator konfiguracji ułatwia szybkie skonfigurowanie sieci, natomiast konfiguracja ręczna pozwala dostosować zaawansowane ustawienia sieciowe do konkretnych wymagań oraz w razie potrzeby sprawdzić lub zmienić istniejące połączenia.

Router obsługuje cztery metody łączenia z Internetem: Ethernet, Repeater, tethering USB i sieć komórkową. Wybierz metodę odpowiednią do swoich potrzeb.

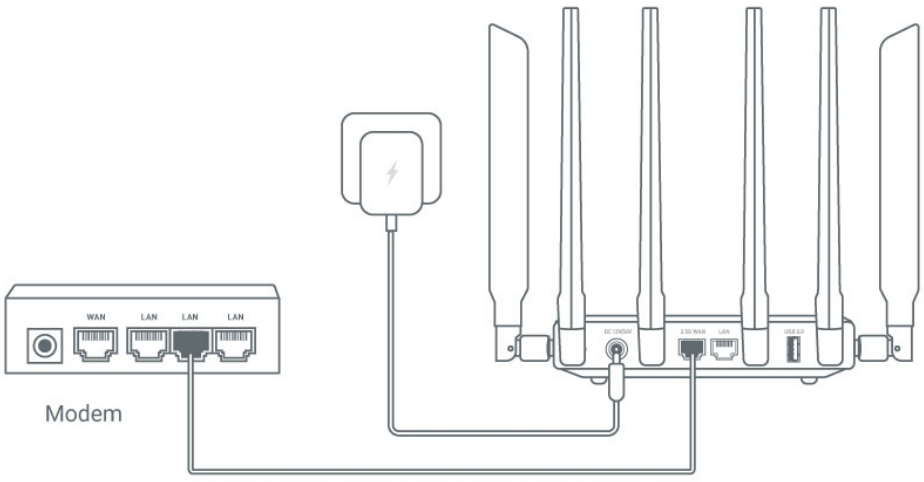
4.2.1 Połączenie z Internetem przez kabel Ethernet

Podłącz router do sieci szerokopasmowej za pomocą kabla Ethernet podłączonego do portu WAN. Router zwykle automatycznie pobiera adres IP (DHCP). Można też ręcznie skonfigurować statyczny adres IP lub PPPoE. Ta metoda zapewnia dużą stabilność i szybkość, dlatego sprawdza się w domach i biurach ze stałym łączem szerokopasmowym.

4.2.1.1 Podstawowe czynności

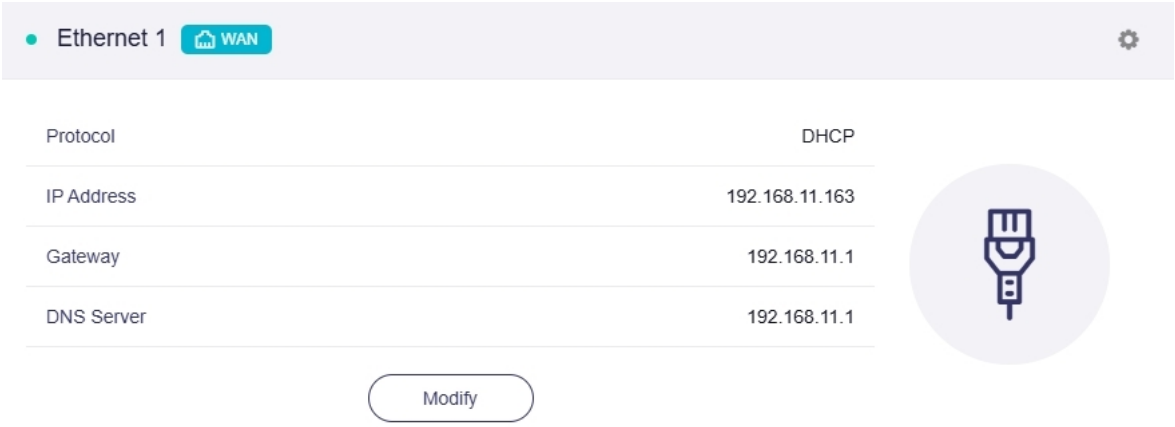
Aby połączyć router z Internetem za pomocą kabla Ethernet, wykonaj poniższe czynności.

1. Połącz port WAN routera z urządzeniem nadrzędnym (np. modemem dostawcy Internetu, routerem, przełącznikiem sieciowym lub gniazdem Ethernet) za pomocą kabla Ethernet.



2. Zaloguj się do internetowego panelu administracyjnego routera i przejdź do sekcji **INTERNET** > **Ethernet**.

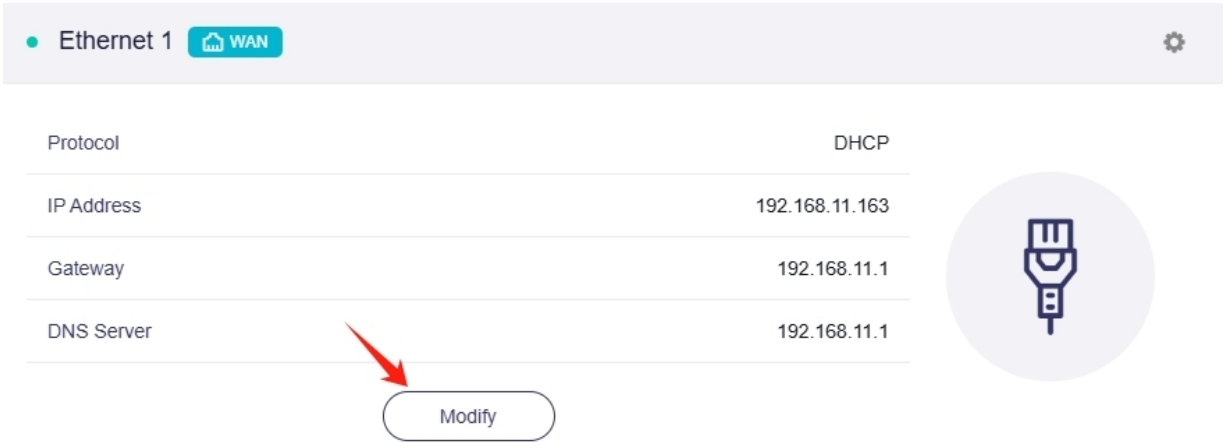
Po pomyślnym nawiązaniu połączenia sekcja Ethernet wyświetli szczegóły sieci, w tym protokół, adres IP, bramę i serwer DNS.



Wskazówki: w razie potrzeby możesz zmienić funkcję portu WAN na LAN. Przydaje się to podczas korzystania z routera jako wzmacniacza sygnału, gdy fizyczny port WAN pozostaje nieużywany. Zyskasz wówczas dodatkowy port LAN.

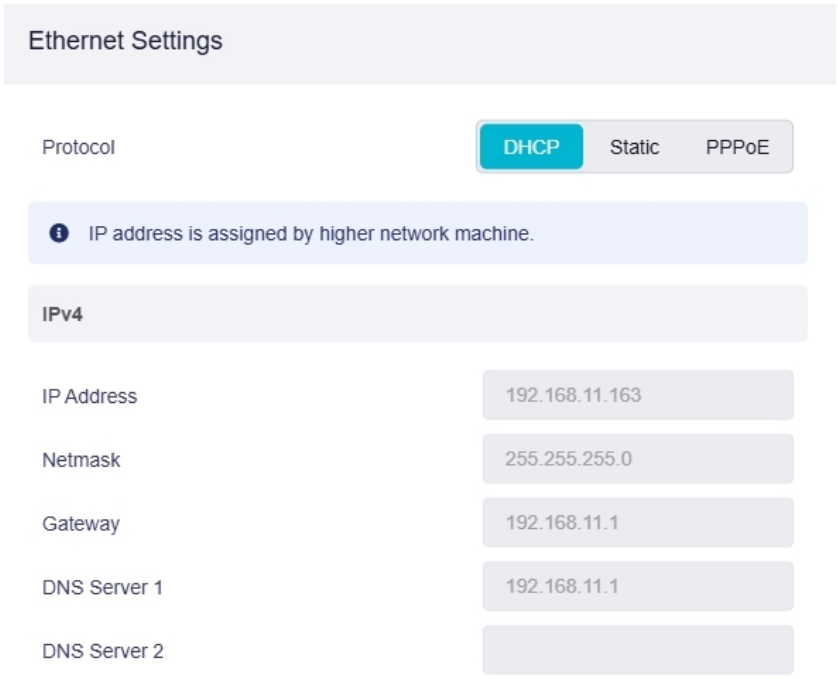
4.2.1.2 Protokół

Dostępne są trzy rodzaje protokołów: DHCP, Static i PPPoE. Kliknij **Modify**, aby zmienić protokół.



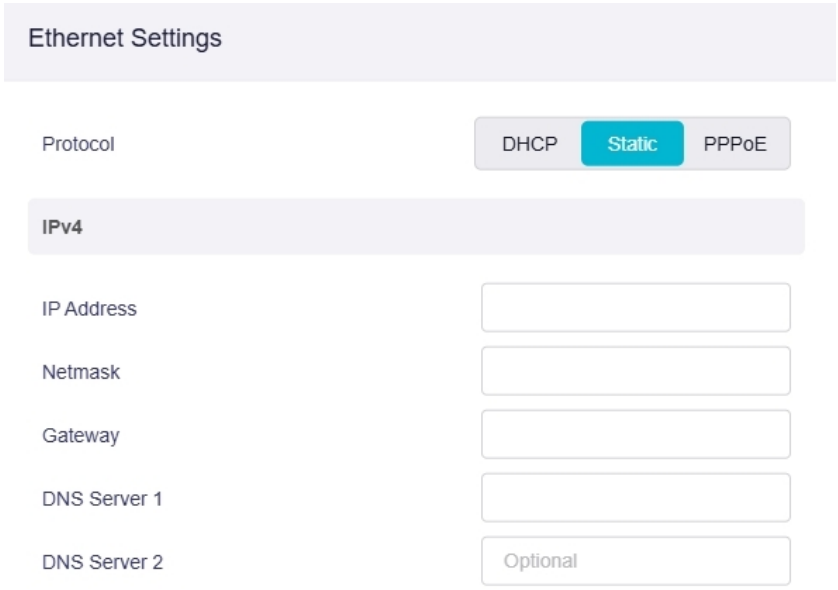
- **DHCP**

  DHCP to domyślny i najczęściej używany protokół. Automatycznie przydziela adresy IP i inne parametry komunikacji urządzeniom w sieci IP w modelu klient–serwer.



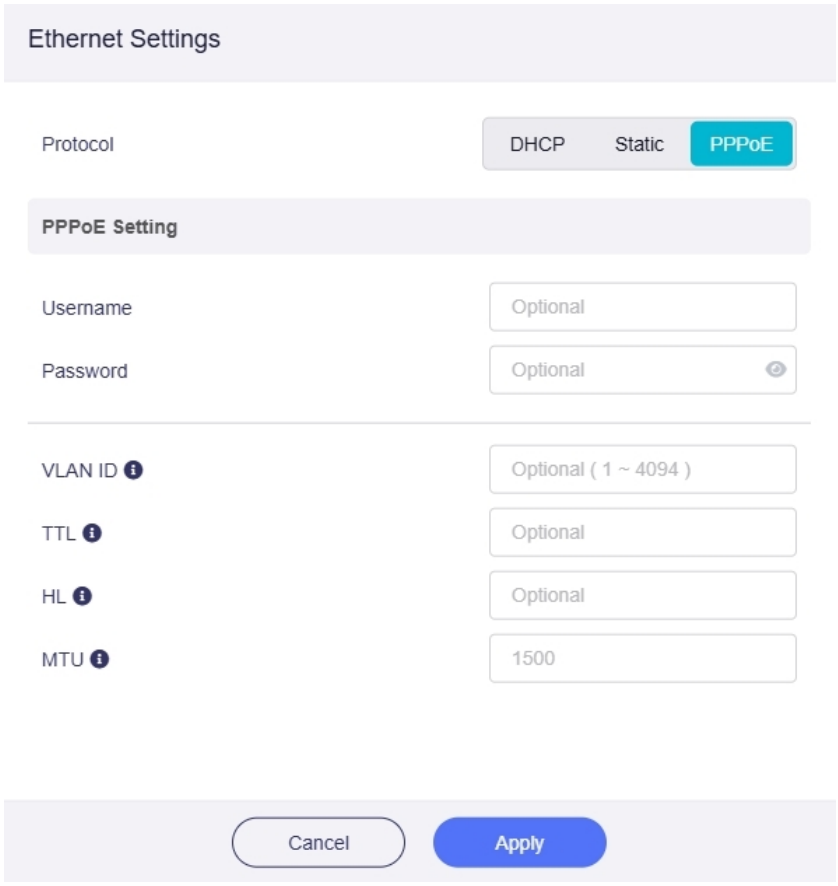
- **Statyczny adres IP**

  Static jest potrzebny, gdy dostawca usług internetowych przydziela stały adres IP lub gdy chcesz ręcznie skonfigurować informacje o sieci, takie jak adres IP, brama i maska sieci.



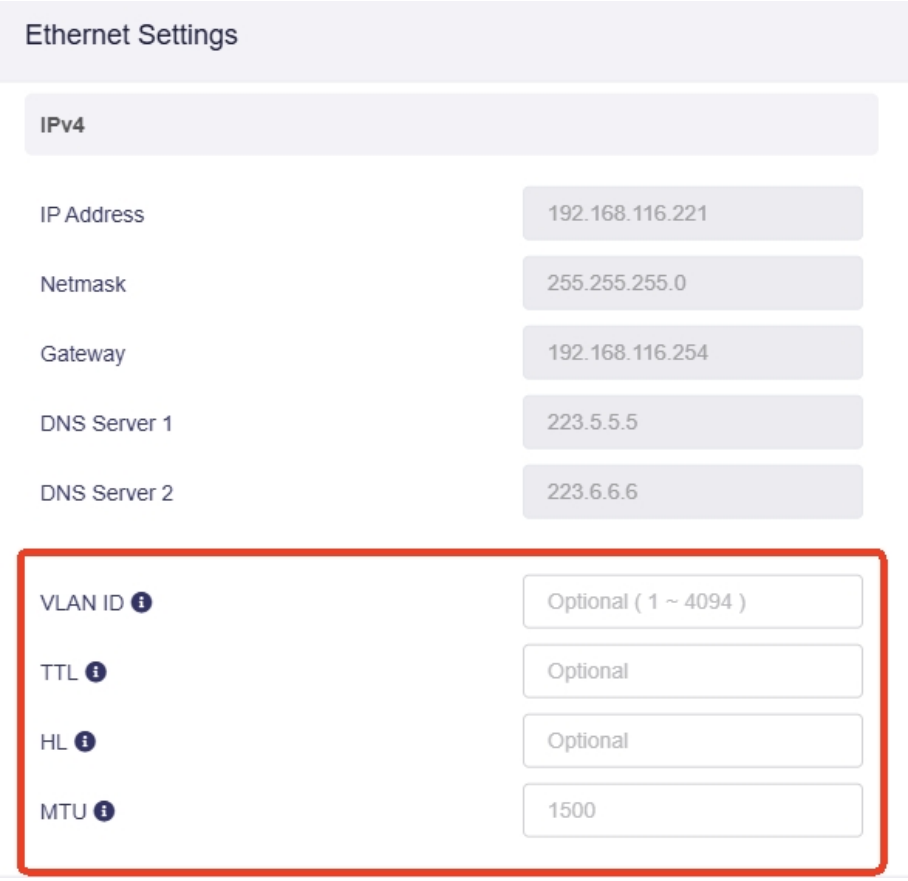
- **PPPoE**

  PPPoE to protokół używany przez większość dostawców Internetu. Zwykle dostawca udostępnia modem oraz nazwę użytkownika i hasło potrzebne do konfiguracji Internetu.


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

4.2.1.3 Ustawienia zaawansowane

Oprócz ustawień podstawowych dostępne są także opcjonalne ustawienia zaawansowane dla trzech powyższych protokołów.

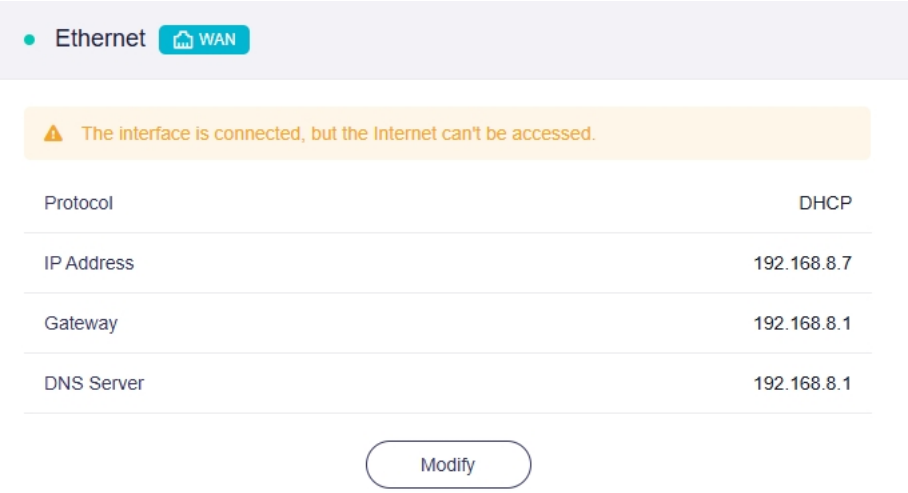


- **VLAN ID**: to ustawienie jest wymagane tylko wtedy, gdy serwer dostawcy wymaga użycia przez interfejs określonego identyfikatora tagowanej sieci VLAN.
- **TTL**: TTL (Time To Live) określa maksymalny czas istnienia pakietów w sieci. Domyślnie router zmniejsza wartość TTL pakietów otrzymanych od urządzeń klienckich o 1 przed ich przekazaniem. Ustawienie TTL dotyczy wyłącznie IPv4. Jeśli chcesz zastąpić lub zmodyfikować TTL, ustaw tutaj stałą wartość. W większości modeli wprowadź żądaną wartość efektywną TTL powiększoną o 1, aby skompensować automatyczne zmniejszenie.
- **HL**: w IPv6 pole HL (Hop Limit) ogranicza liczbę przeskoków pakietów danych w sieci i jest odpowiednikiem TTL w IPv4.
- **MTU**: domyślna wartość MTU wynosi 1500 bajtów.

4.2.1.4 Rozwiązywanie problemów

Jeśli kabel Ethernet jest podłączony do portu WAN, ale Internet jest niedostępny, pojawi się żółty komunikat pokazany poniżej.

„Interfejs jest połączony, ale nie można uzyskać dostępu do Internetu”.

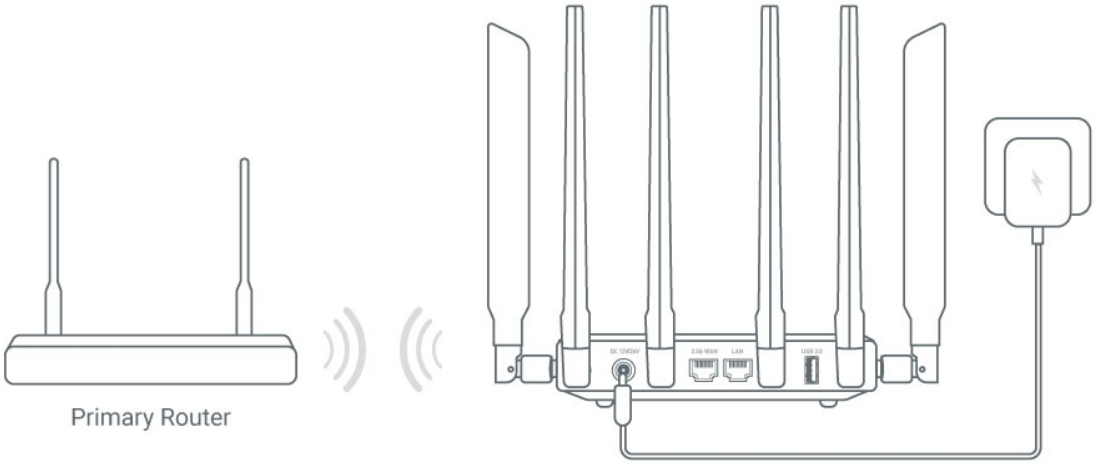


Aby rozwiązać ten problem:

1. Sprawdź, czy urządzenie nadrzędne ma dostęp do Internetu.
2. Przejdź do strony Multi-WAN, aby sprawdzić stan interfejsu Ethernet.

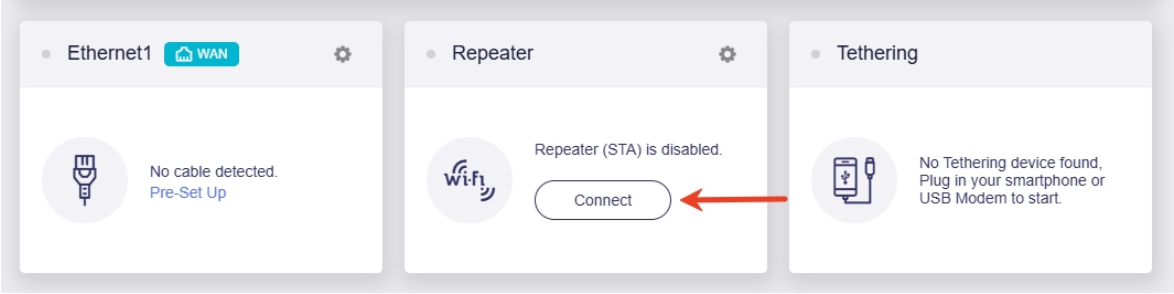
4.2.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi

Funkcja Repeater polega na połączeniu routera z istniejącą siecią bezprzewodową, np. bezpłatną siecią Wi-Fi w hotelu lub kawiarni. Domyślnie działa w trybie WISP (Wireless Internet Service Provider), co oznacza, że router tworzy własną podsieć i działa jako zapora chroniąca przed siecią publiczną.

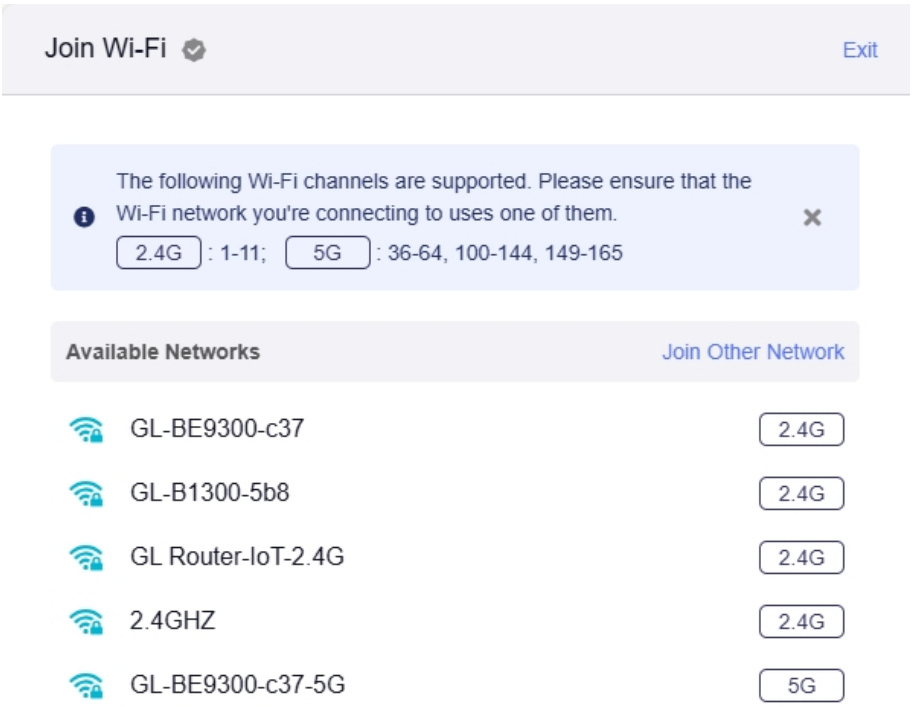


4.2.2.1 Podstawowe czynności

1. Zaloguj się do internetowego panelu administracyjnego routera, przejdź do sekcji **INTERNET** > **Repeater** i kliknij **Connect**.



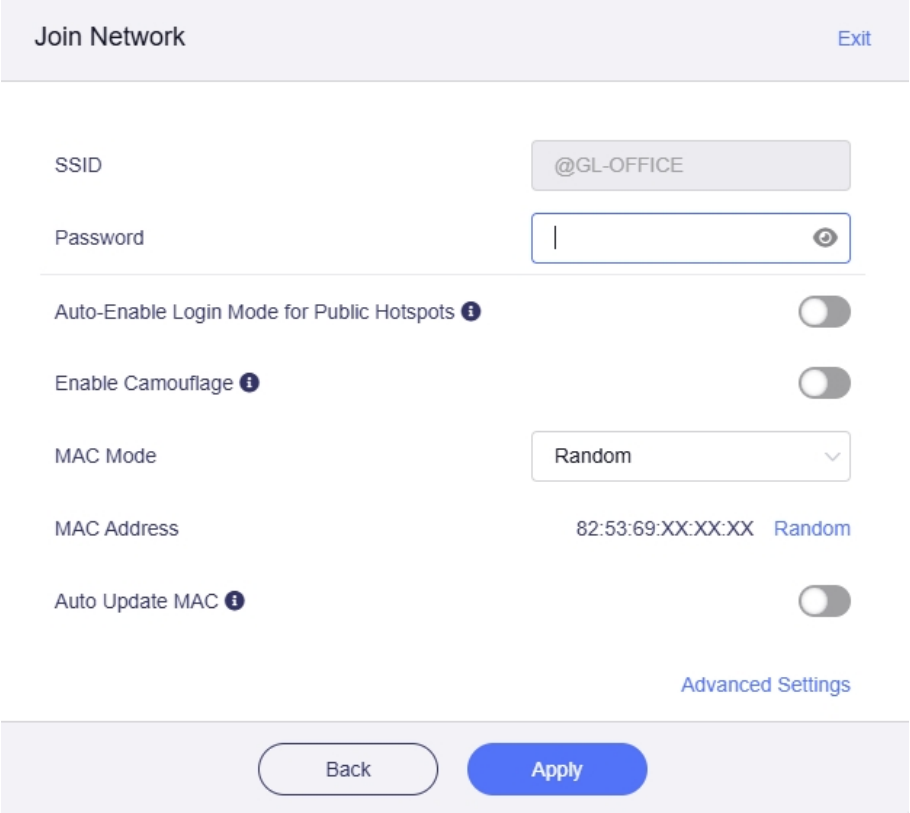
2. Wybierz sieć Wi-Fi, z którą chcesz się połączyć, z listy dostępnych sieci.



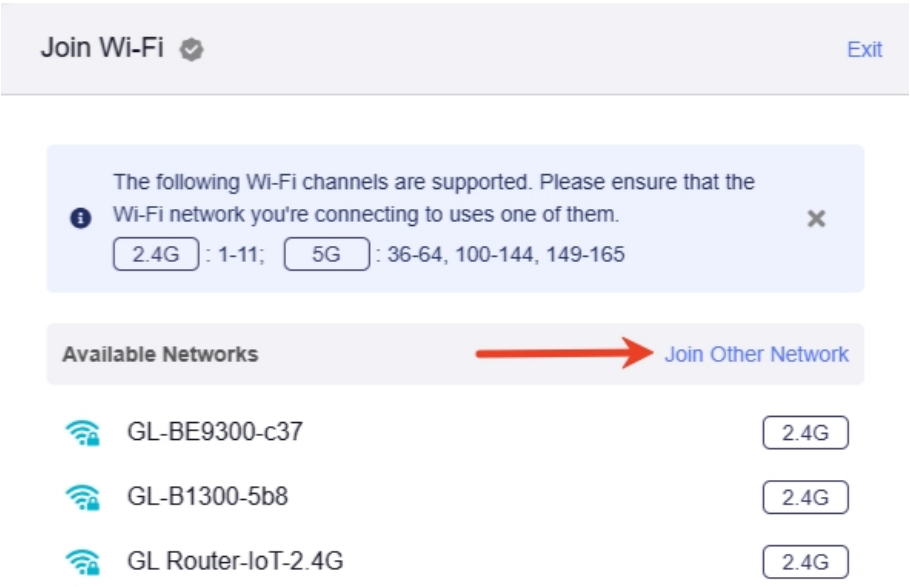
Uwaga:

1. Ta strona wyświetla kanały Wi-Fi obsługiwane przez router. Upewnij się, że sieć Wi-Fi, z którą chcesz się połączyć, korzysta z jednego z tych kanałów. W przeciwnym razie może nie pojawić się na liście dostępnych sieci.
2. Podczas wyszukiwania hotspotu osobistego iPhone’a pozostaw iPhone’a odblokowanego, aby utrzymać wysyłanie ramek sygnalizacyjnych Wi-Fi. W przeciwnym razie router może nie wykryć hotspotu.

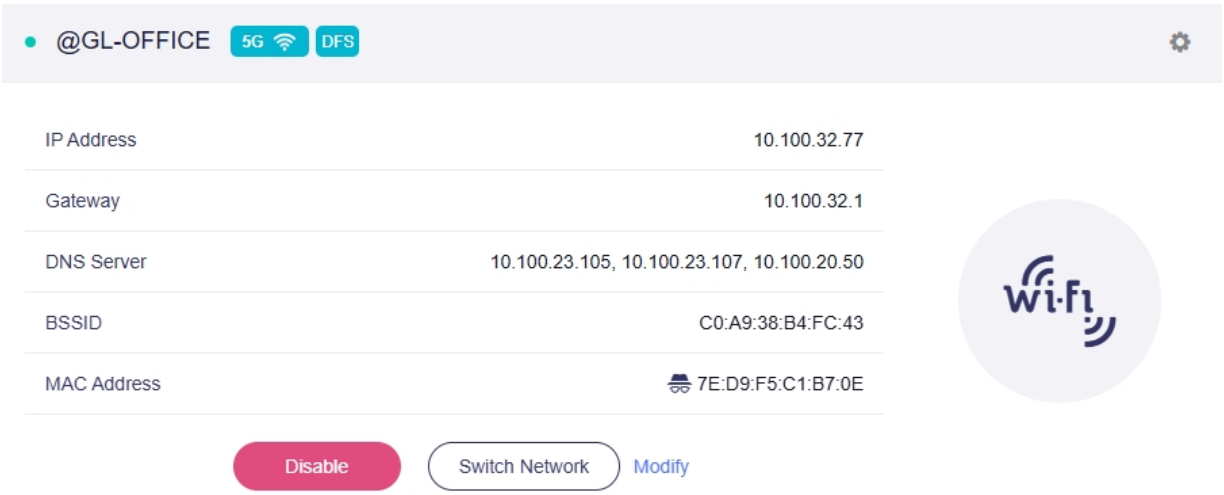
3. Wprowadź prawidłowe hasło Wi-Fi i kliknij **Apply**.



Wskazówka: jeśli SSID sieci Wi-Fi, z którą chcesz się połączyć, nie ma na liście dostępnych sieci, kliknij **Join Other Network** w prawym górnym rogu, ręcznie wprowadź SSID i pozostałe wymagane informacje, a następnie kliknij **Apply**.

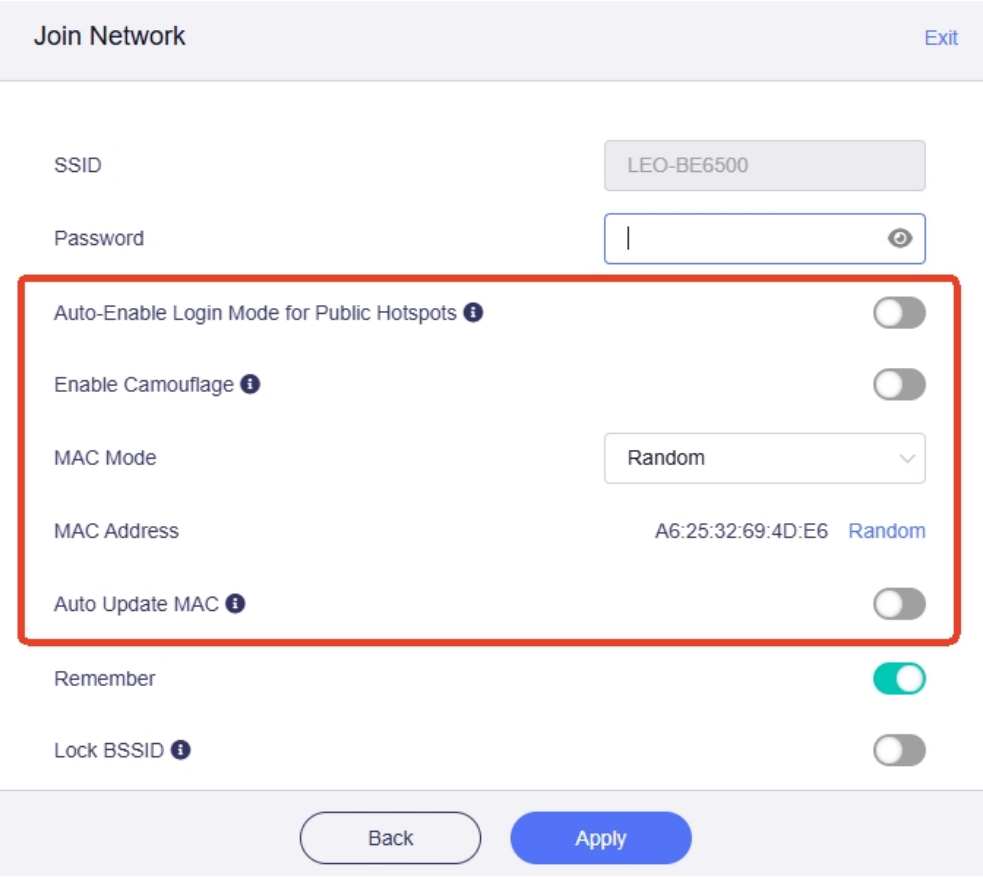


4. Po chwili połączenie zostanie nawiązane, jeśli hasło jest prawidłowe.


@GL-OFFICE
5G
DFS
IP Address
10.100.32.77
Gateway
10.100.32.1
DNS Server
10.100.23.105, 10.100.23.107, 10.100.20.50
BSSID
C0:A9:38:B4:FC:43
MAC Address
7E:D9:F5:C1:B7:0E
Disable
Switch Network
Modify

4.2.2.2 Publiczny hotspot

Podczas łączenia routera z publicznym hotspotem z portalem logowania włączenie poniższych funkcji może zwiększyć szanse pomyślnego połączenia.



- **Automatyczne włączanie trybu logowania do publicznych hotspotów**
  Po włączeniu tej opcji router automatycznie przechodzi w tryb Public Hotspot Login Mode, gdy jest połączony z hotspotem, ale nie ma dostępu do Internetu. W tym trybie niektóre usługi zostają wstrzymane, a tryb DNS zmienia się na automatyczny, co może ujawnić Twoją aktywność sieciową dostawcy sieci (np. hotelowi lub centrum handlowemu). Nawet po wyłączeniu tej opcji router zaproponuje przejście do tego trybu, jeśli wykryje portal logowania hotspotu lub logowanie się nie powiedzie.
- **Włączanie kamuflażu**
  Po włączeniu tej opcji router podszywa się pod urządzenie klienckie używane do otwierania panelu administracyjnego, naśladując jego adres MAC.
- **Tryb MAC**
  Wybierz adres MAC, którego router ma używać do łączenia się z publicznym hotspotem.

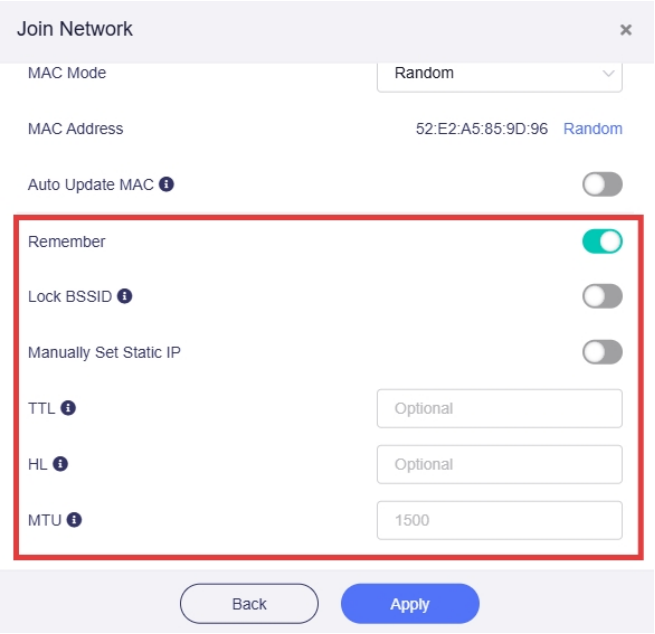
Fabryczny	Używa oryginalnego adresu MAC przypisanego fabrycznie do urządzenia.
Klonowanie	Klonuje adres MAC urządzenia klienckiego na potrzeby połączenia. Jeśli żądanego adresu MAC nie ma na liście, wprowadź go ręcznie, aby go sklonować. Uwaga: wiele urządzeń używa losowych adresów MAC (często określanych jako prywatny adres Wi-Fi lub losowy adres sprzętowy) podczas łączenia się z sieciami Wi-Fi. Dlatego wyświetlany tutaj adres MAC może różnić się od rzeczywistego fizycznego adresu MAC urządzenia.
Losowy	Automatycznie generuje losowy adres MAC na potrzeby połączenia.

- **Automatyczna aktualizacja adresu MAC**
  Po włączeniu tej opcji adres MAC jest aktualizowany automatycznie.

Podczas zapisywania konfiguracji sieci tryb MAC, w tym sklonowany lub losowy adres MAC, zostaje powiązany z zapisywanym identyfikatorem SSID. Ustawienia te można w każdej chwili ręcznie zmienić dla poszczególnych identyfikatorów SSID.

4.2.2.3 Ustawienia zaawansowane

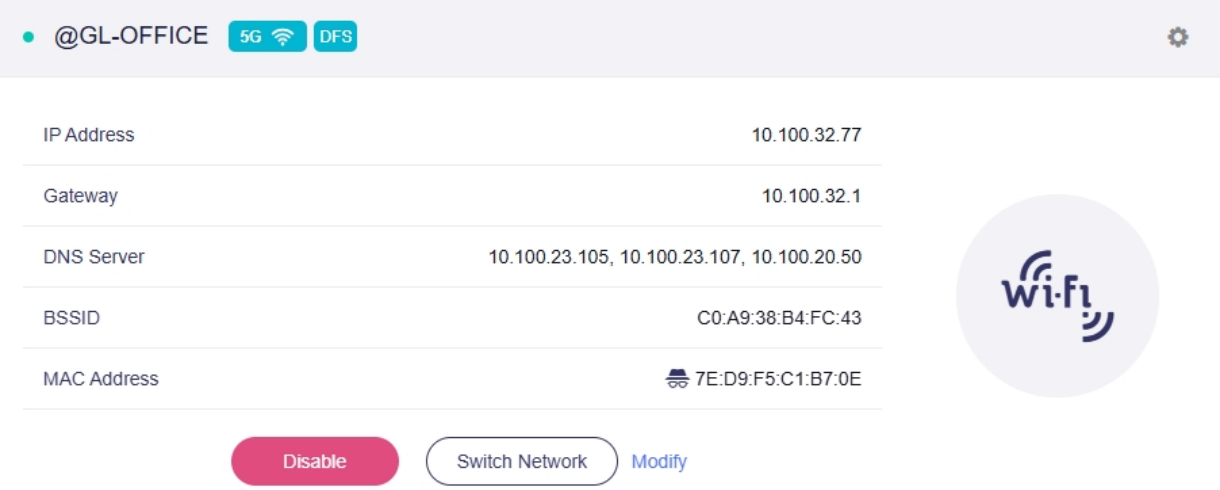
Podczas łączenia z siecią dostępne są dodatkowe opcje.



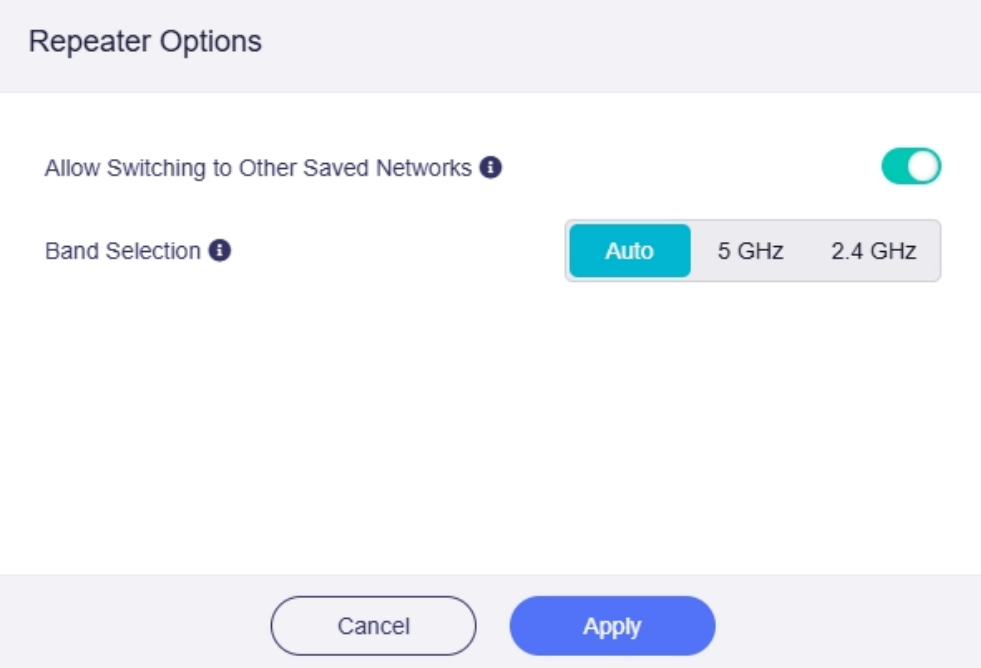
- **Remember**: włącz tę opcję, aby zapamiętać bieżącą sieć Wi-Fi, której sygnał jest wzmacniany.
- **Lock BSSID**: po włączeniu router będzie łączyć się wyłącznie z konkretnym punktem dostępu (AP) odpowiadającym wybranemu BSSID, nawet jeśli inne punkty dostępu mają taki sam identyfikator SSID.
- **Manually Set Static IP**: po włączeniu tej opcji możesz ręcznie skonfigurować stały adres IPv4, maskę sieci, bramę i serwery DNS dla połączenia routera w trybie wzmacniacza sygnału zamiast uzyskiwać te ustawienia automatycznie.
- **TTL**: TTL (Time To Live) określa maksymalny czas istnienia pakietów w sieci. Domyślnie router zmniejsza o 1 wartość TTL pakietów odebranych od urządzeń klienckich przed ich przekazaniem dalej. Aby zastąpić lub zmodyfikować TTL, wprowadź żądaną wartość efektywną powiększoną o 1, co skompensuje automatyczne zmniejszenie. TTL dotyczy wyłącznie IPv4.
- **HL**: w IPv6 pole HL (Hop Limit) ogranicza liczbę przeskoków pakietów danych w sieci i jest odpowiednikiem TTL w IPv4.
- **MTU**: wartość domyślna wynosi 1500.

4.2.2.4 Opcje wzmacniacza sygnału

Kliknij ikonę koła zębatego w prawym górnym rogu, aby skonfigurować opcje wzmacniacza.



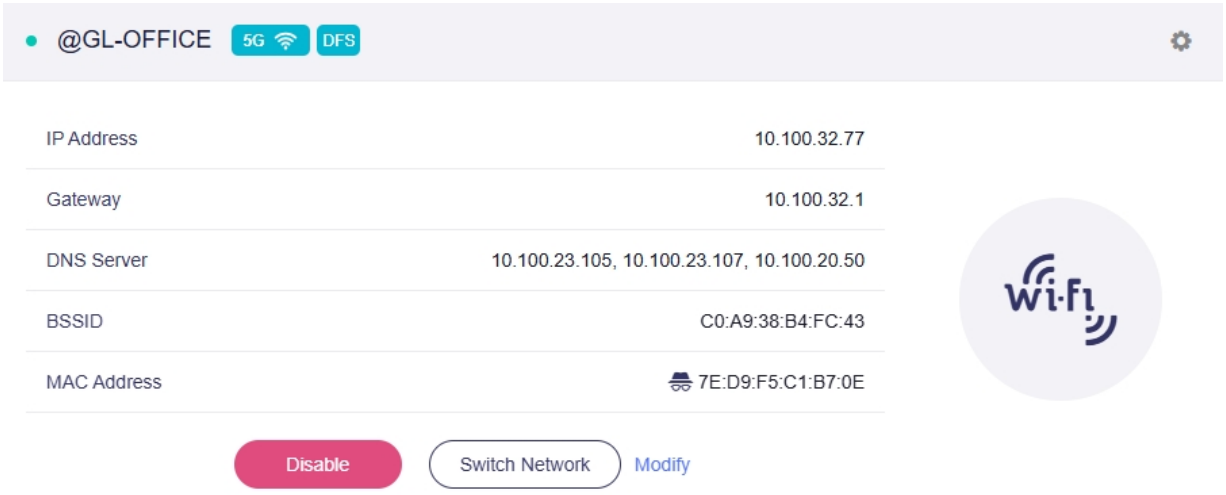
Wygląd strony może się różnić w zależności od wersji oprogramowania.



- **Allow Switching to Other Saved Networks**: po włączeniu router będzie automatycznie łączył się z innymi zapisanymi sieciami, gdy bieżąca sieć Wi-Fi stanie się niedostępna.
- **Band Selection**: jeśli ręcznie wybierzesz pasmo, router będzie skanował i łączył się wyłącznie z sieciami Wi-Fi w tym paśmie częstotliwości.

4.2.2.5 Zarządzanie znanymi sieciami

Aby zarządzać znanymi sieciami, kliknij **Switch Network**.

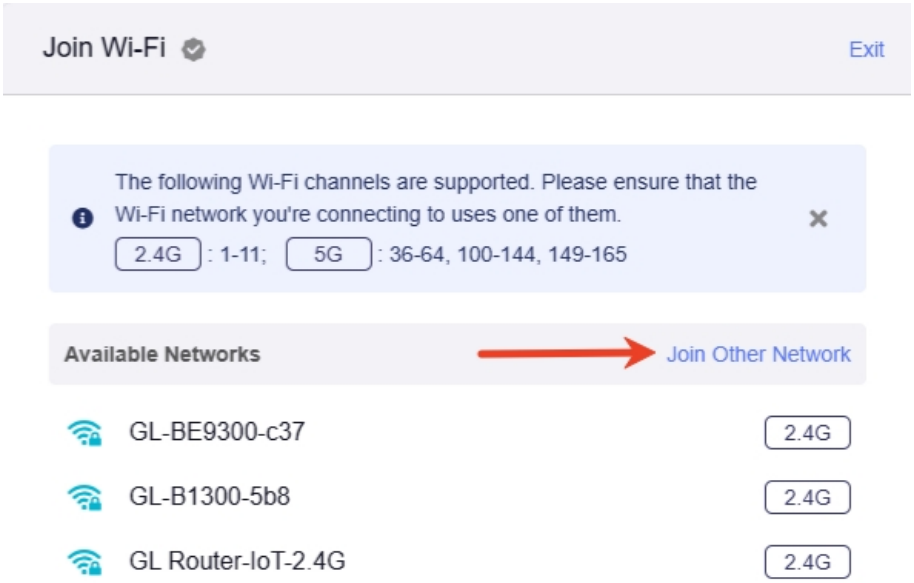


W sekcji **Known Networks** kliknij ikonę kosza, aby usunąć znaną sieć, lub ikonę koła zębatego, aby ją skonfigurować.

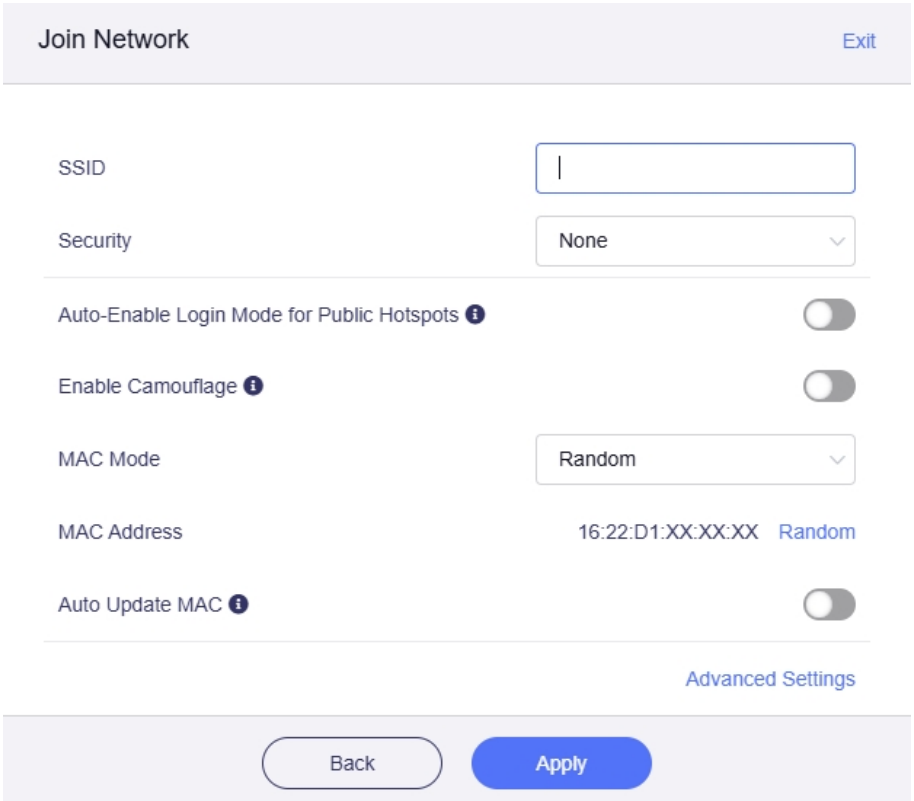


4.2.2.6 Łączenie z inną siecią

Jeśli SSID nie ma na liście dostępnych sieci lub jest ukryty, możesz kliknąć **Join Other Network**.

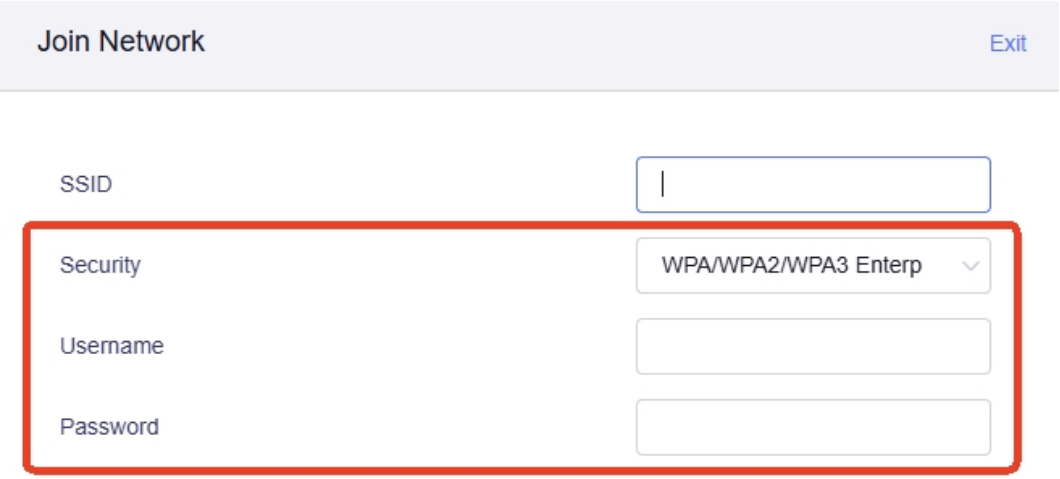


Wprowadź **SSID**, wybierz **Security** i wprowadź hasło (jeśli jest wymagane), a następnie kliknij **Apply**.



W ustawieniu **Security** dostępne są dwie lub trzy opcje, zależnie od modelu.

- None oznacza, że hasło nie jest wymagane.
- WPA/WPA2/WPA3 to powszechny wariant obsługiwany przez niemal wszystkie sieci Wi-Fi.
- WPA/WPA2/WPA3 Enterprise wymaga uwierzytelniania za pomocą protokołu EAP (Extensible Authentication Protocol). Do połączenia potrzebne są prawidłowa nazwa użytkownika i hasło (wariant zwykle używany w sieciach firmowych lub uczelnianych).



Szczegółowe wskazówki dotyczące wzmacniania sygnału sieci EAP znajdziesz tutaj.

4.2.2.7 Ponowne łączenie

W poniższych przypadkach router będzie co pewien czas automatycznie próbował ponownie połączyć się z Wi-Fi. W razie potrzeby możesz ręcznie wyłączyć tę funkcję. W przypadku błędnego SSID lub hasła usuń sieć z Known Networks, aby rozwiązać problem.

1. Podczas konfiguracji funkcji Repeater wprowadzono nieprawidłowy SSID lub hasło.
2. Po początkowym połączeniu router znalazł się poza zasięgiem routera nadrzędnego.
3. Po nawiązaniu połączenia router nadrzędny zmienił SSID lub hasło albo ograniczył dostęp.

Proces ponownego łączenia składa się z trzech odrębnych etapów: oczekiwania, skanowania i łączenia.

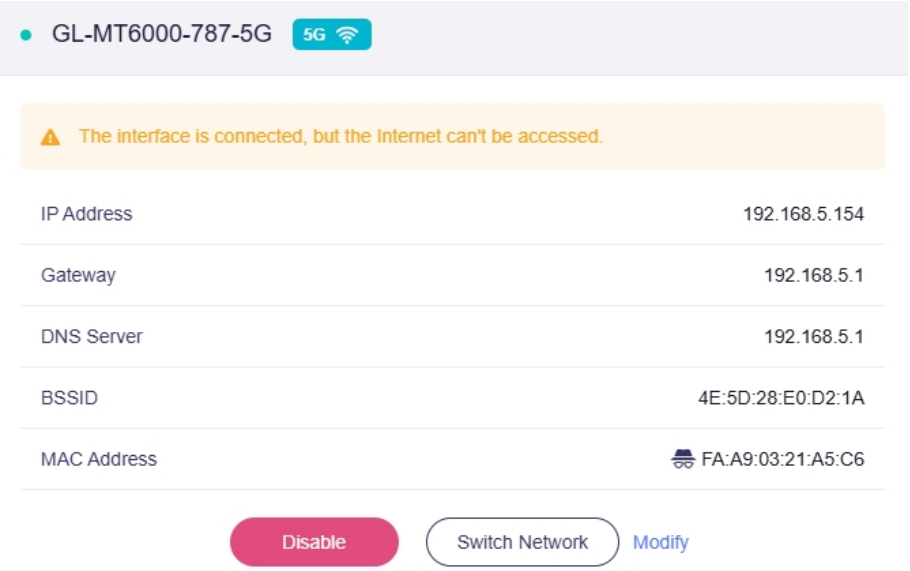
1. Etap oczekiwania: brak problemów — router czeka na warunki umożliwiające ponowne połączenie.
2. Etap skanowania: w skanowanym paśmie może występować utrata pakietów. Nowe urządzenia mogą mieć problemy z połączeniem. W modelach GL-AXT1800/GL-AX1800 sieć Wi-Fi dla gości zostanie tymczasowo wyłączona.
3. Etap łączenia: główna sieć Wi-Fi w docelowym paśmie może zostać rozłączona na kilka sekund podczas ponownego nawiązywania połączenia.

Uwaga: problemy zwykle występują na etapach skanowania i łączenia.

4.2.2.8 Rozwiązywanie problemów

Jeśli router jest połączony z siecią Wi-Fi jako wzmacniacz sygnału, ale Internet jest niedostępny, pojawi się żółty komunikat pokazany poniżej.

„Interfejs jest połączony, ale nie można uzyskać dostępu do Internetu”.



Aby rozwiązać ten problem:

1. Sprawdź, czy urządzenie nadrzędne (czyli sieć Wi-Fi, z którą połączony jest router) ma dostęp do Internetu.
2. Przejdź do strony Multi-WAN, aby sprawdzić stan interfejsu Repeater.

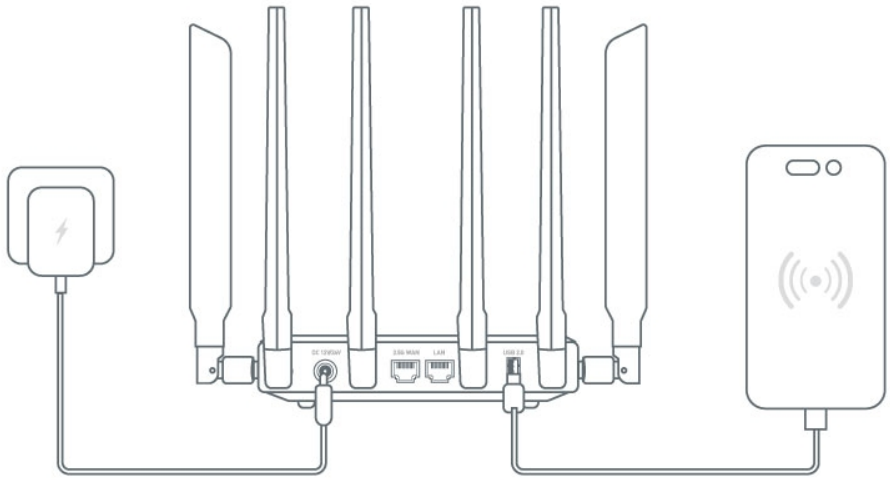
4.2.2.9 DFS

DFS (Dynamic Frequency Selection) to mechanizm automatycznej zmiany kanałów Wi-Fi w celu uniknięcia zakłóceń sygnałów radarowych. Podczas łączenia z nadrzędną siecią Wi-Fi 5 GHz sieć Wi-Fi routera korzysta lub nie korzysta z kanału DFS zgodnie z siecią nadrzędną.

- Jeśli nadrzędna sieć Wi-Fi korzysta z kanału DFS i można ją wykryć podczas skanowania, sieć Wi-Fi 5 GHz routera będzie używać tego samego kanału.
- Sieć Wi-Fi 5 GHz routera przełączy się na kanał bez DFS, jeśli nie można wykryć sieci nadrzędnej podczas skanowania lub połączenie się nie powiedzie.

4.2.3 Połączenie z Internetem przez tethering USB

Podłączenie smartfona do routera kablem USB w celu udostępnienia routerowi komórkowej transmisji danych (np. 4G/5G) nazywa się tetheringiem. To wygodny sposób uzyskania tymczasowego dostępu do Internetu, szczególnie w terenie lub w miejscach bez stałego łącza szerokopasmowego.

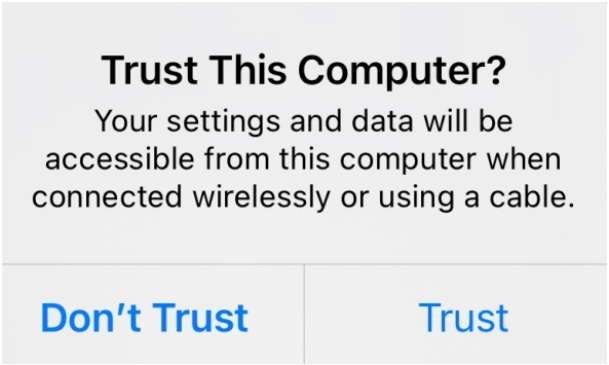


Modem typu hostless podczas konfiguracji połączenia komórkowego również korzysta z interfejsu Tethering.

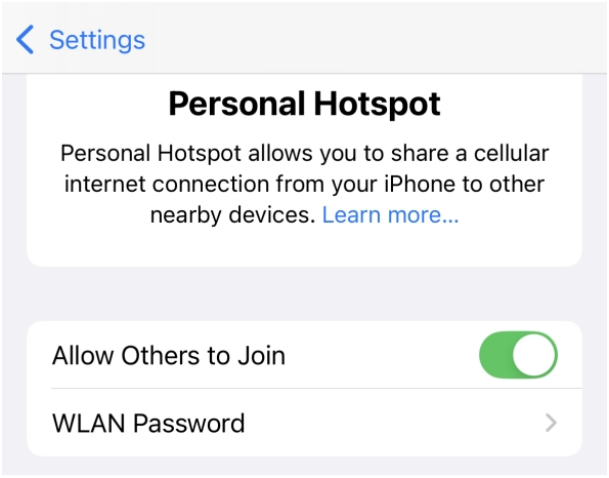
Uwaga: niektórzy operatorzy komórkowi ograniczają tethering lub pobierają za niego dodatkowe opłaty. Zalecamy sprawdzenie warunków u operatora.

4.2.3.1 iPhone

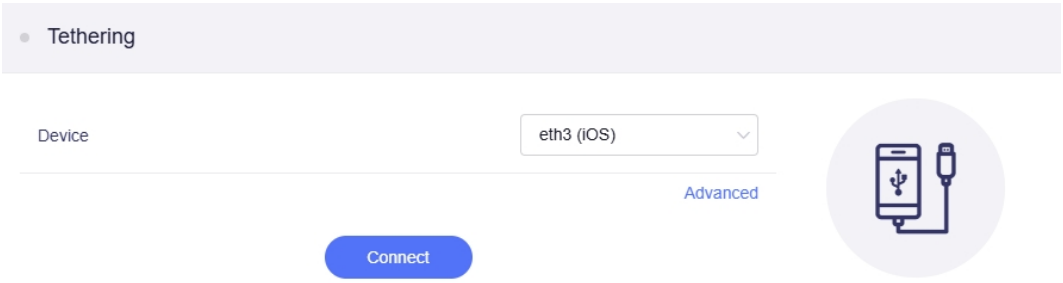
1. Podłącz iPhone'a do portu USB routera za pomocą kabla USB. Pojawi się komunikat systemowy z pytaniem, czy zaufać urządzeniu. Stuknij **Trust**, aby kontynuować.



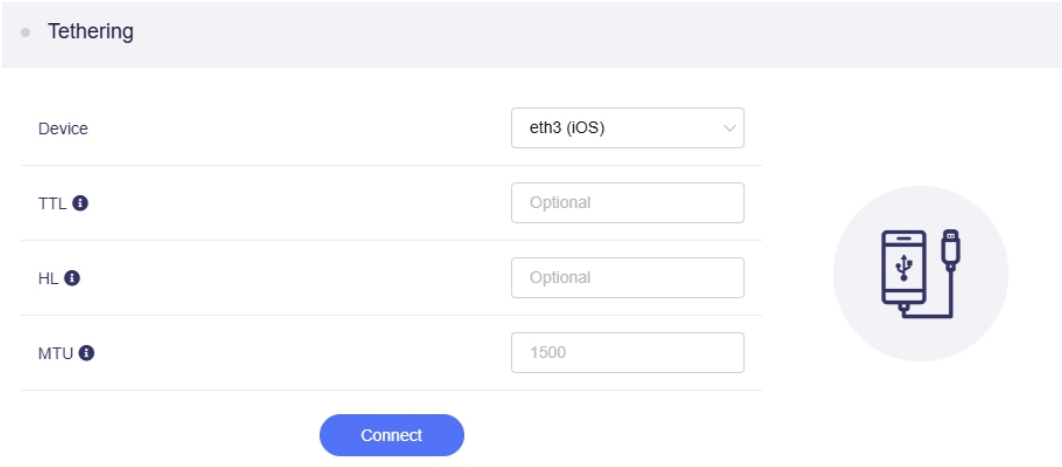
2. Na iPhonie przejdź do **Settings** > **Personal Hotspot**. Włącz **Allow Others to Join**.



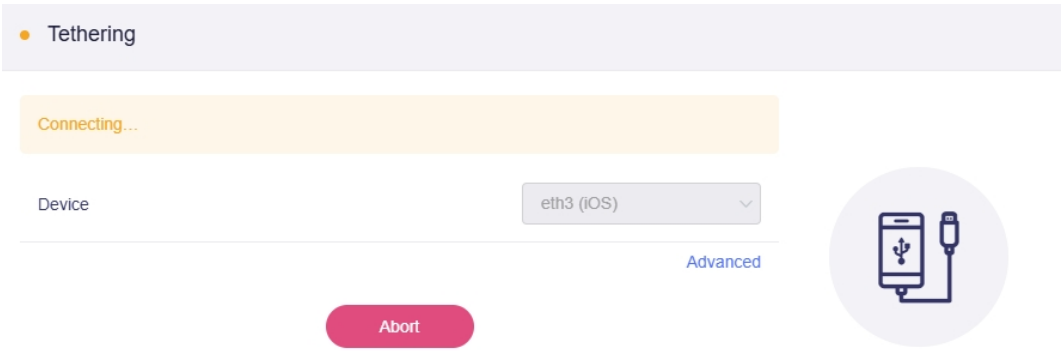
3. Podłącz komputer lub inny telefon do routera. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



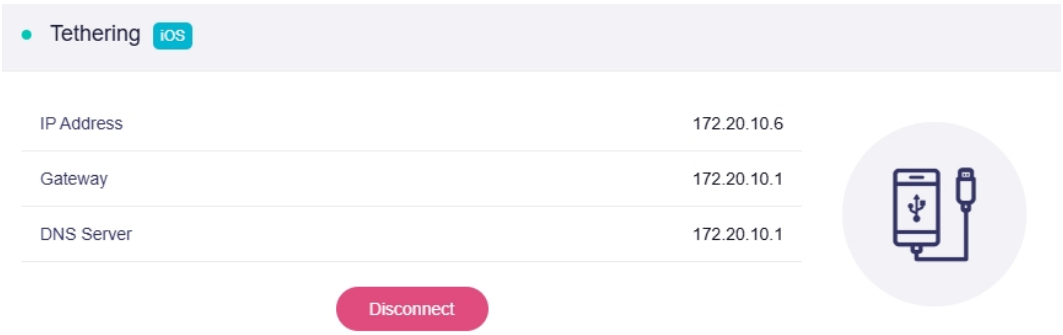
Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced**, zmień te ustawienia, a następnie kliknij **Connect**.



4. Rozpocznie się nawiązywanie połączenia.

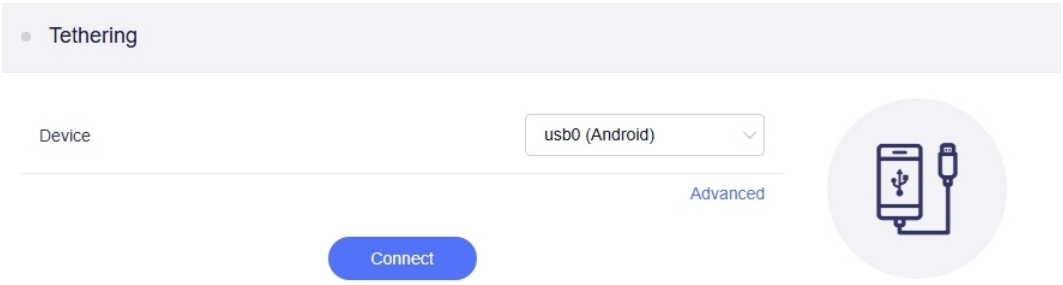


Po połączeniu na tej stronie pojawią się szczegóły połączenia tethering.

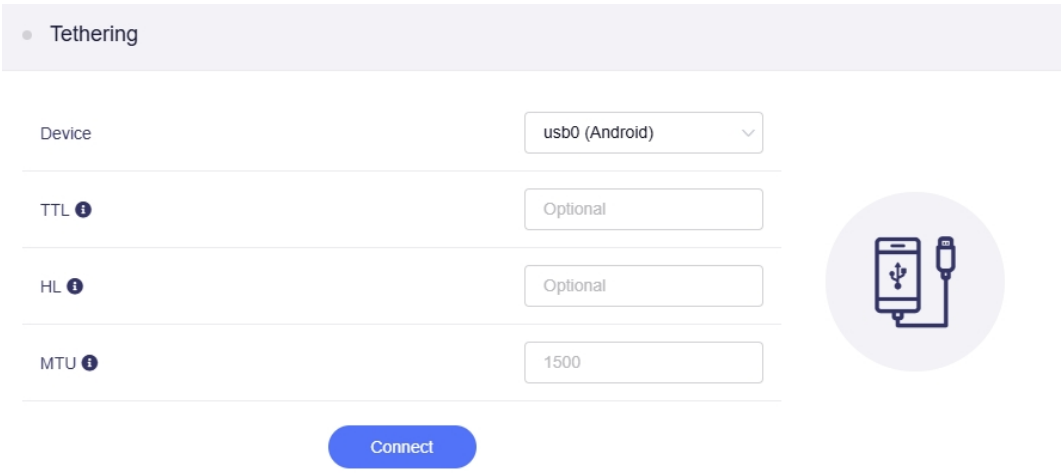


4.2.3.2 Android

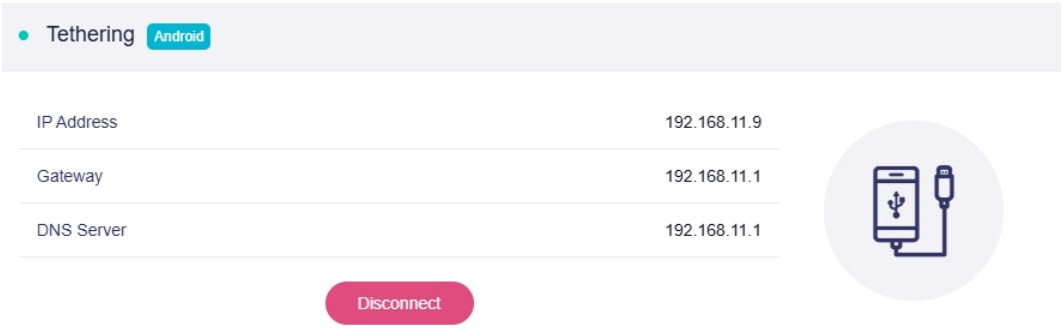
1. Podłącz telefon z systemem Android do portu USB routera za pomocą kabla USB. Może pojawić się okno systemowe z pytaniem o preferencje USB. Jeśli zostanie wyświetlone, wybierz **USB Tethering** lub **File Transfer**.
2. W telefonie przejdź do **Settings** > **Network & Internet** > **Personal Hotspot**. Włącz **Personal Hotspot** lub **USB Tethering**.
   (Sposób włączania tetheringu USB zależy od producenta. Dokładną lokalizację opcji sprawdź w ustawieniach urządzenia, a w razie potrzeby skontaktuj się z pomocą techniczną producenta.)
3. Podłącz komputer lub inny telefon do routera, a następnie zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**. Kliknij **Connect**.



Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced**, zmień te ustawienia, a następnie kliknij **Connect**.



4. Po połączeniu na tej stronie pojawi się stan połączenia tethering.



4.2.3.3 Rozwiązywanie problemów

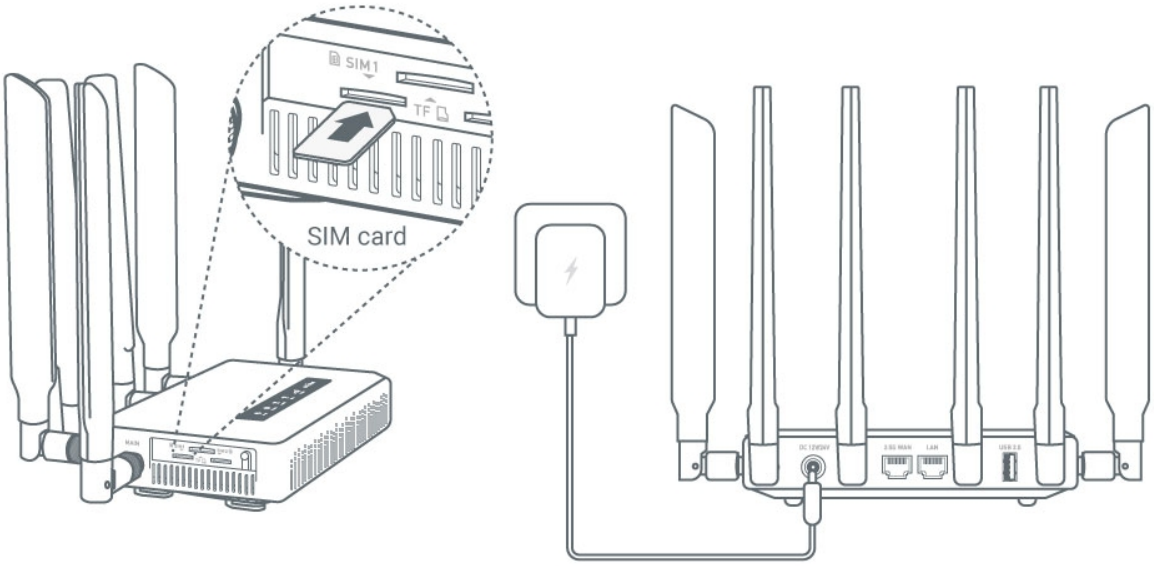
Jeśli połączenie się nie powiedzie, wykonaj poniższe czynności:

- Użyj oryginalnego zasilacza routera.
- Odłącz i ponownie podłącz kabel USB.
- Użyj innego kabla USB. Upewnij się, że obsługuje transmisję danych, a nie tylko ładowanie.
- Kilkakrotnie wyłącz i włącz opcję „USB Tethering” (na telefonie z systemem Android).
- Kilkakrotnie wyłącz i włącz opcję „Allow Others to Join” (na iPhonie).
- Uruchom ponownie smartfon i spróbuj jeszcze raz.

Jeśli problem nadal występuje, skontaktuj się z naszą pomocą techniczną: support@gl-inet.com.

4.2.4 Połączenie z Internetem przez sieć komórkową

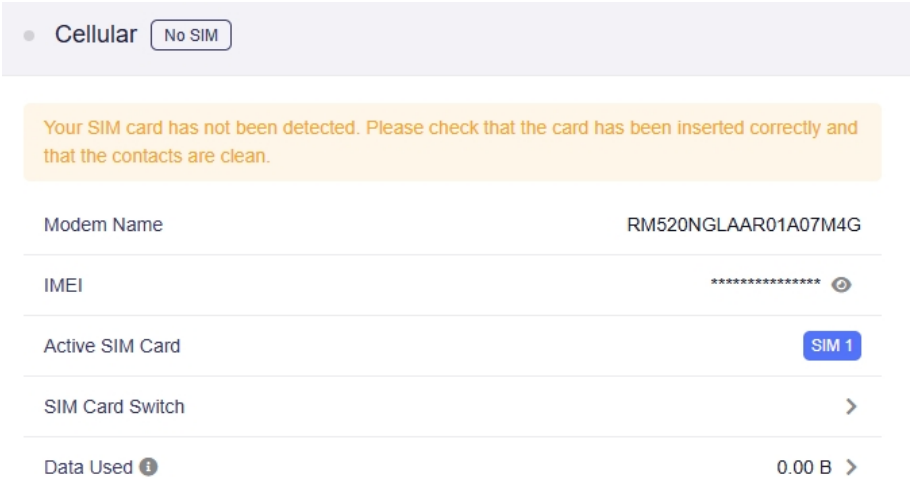
Spitz AX (GL-X3000) ma wbudowany modem komórkowy obsługujący dwie karty SIM. Jednocześnie aktywna jest tylko jedna karta SIM; druga pełni funkcję zapasową. Możesz ręcznie przełączać między kartami SIM.



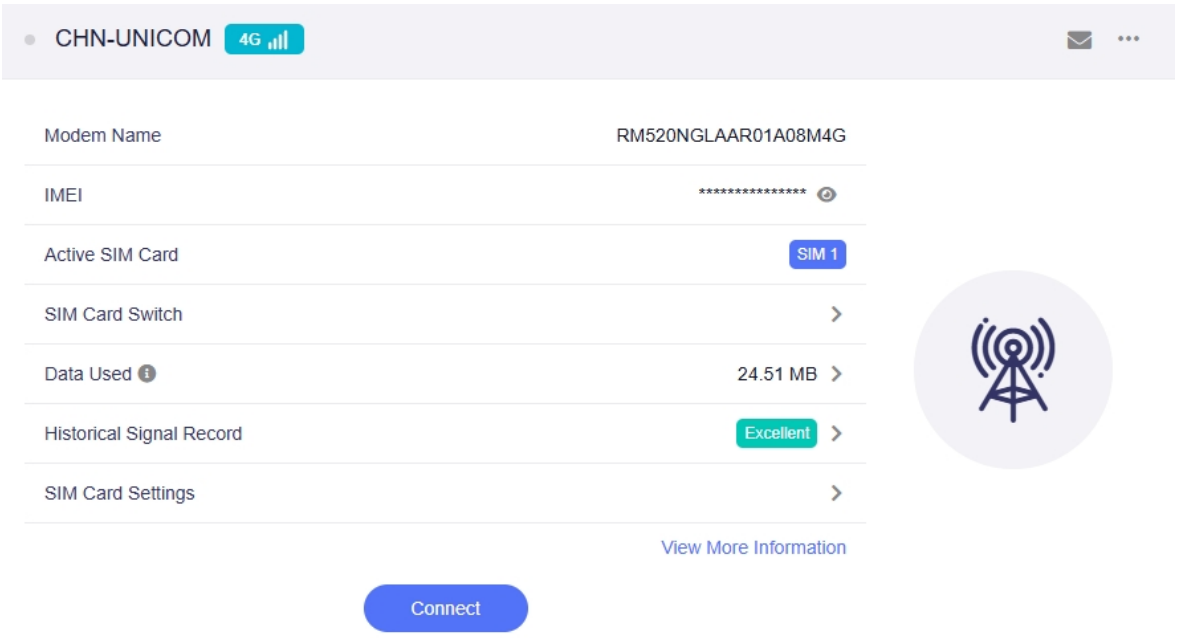
4.2.4.1 Konfiguracja automatyczna

Zalecamy najpierw wyłączyć router, włożyć wcześniej aktywowane karty SIM do gniazd, a następnie go włączyć. Jeśli włożysz kartę SIM po uruchomieniu routera, internetowy panel administracyjny może nie odświeżyć się automatycznie. W takim przypadku odśwież stronę lub uruchom router ponownie.

1. Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **INTERNET** > **Cellular**.
2. Gdy karta SIM nie jest włożona, strona wyświetla komunikat „Your SIM card has not been detected” (Nie wykryto karty SIM).

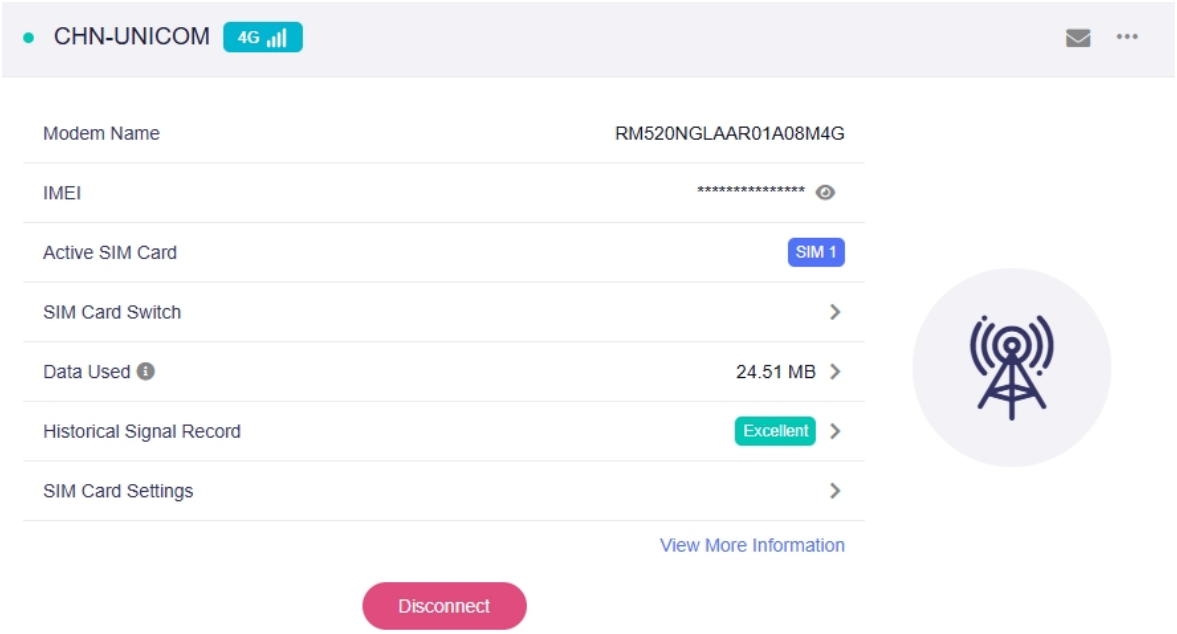


3. Po włożeniu karty SIM strona wygląda jak poniżej. Kliknij **Connect**.

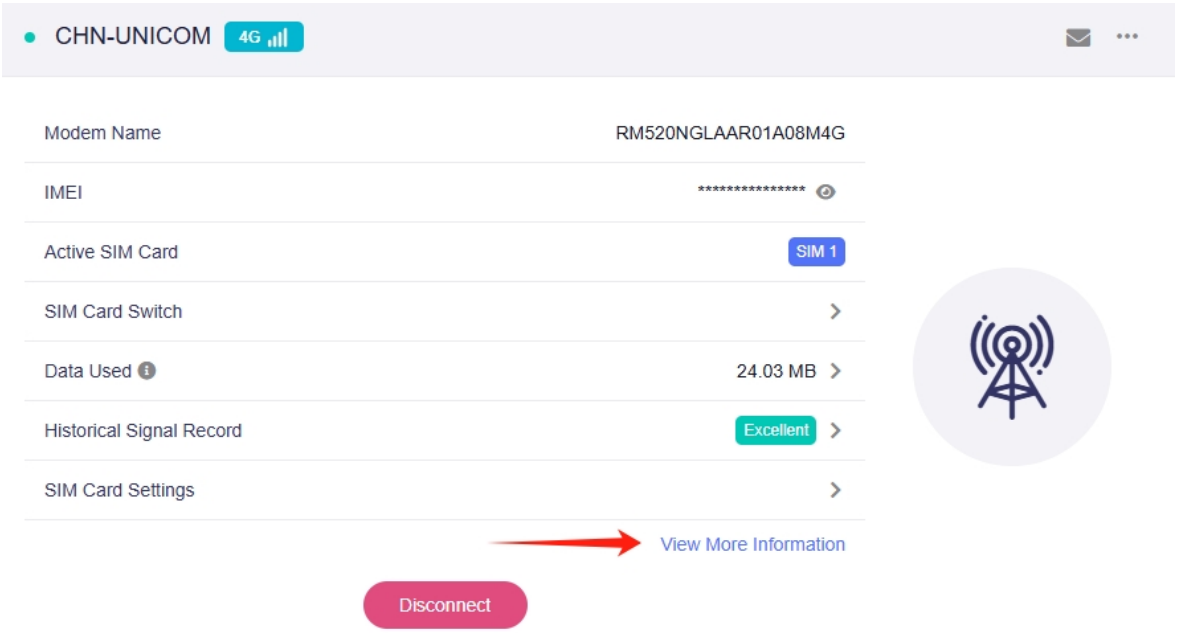


Wskazówka: jeśli karta SIM nie jest wykrywana, spróbuj ponownie uruchomić router i sprawdź, czy zostanie wykryta.

4. Po nawiązaniu połączenia z siecią komórkową strona wyświetli szczegóły sieci z zieloną kropką oznaczającą pomyślne połączenie.



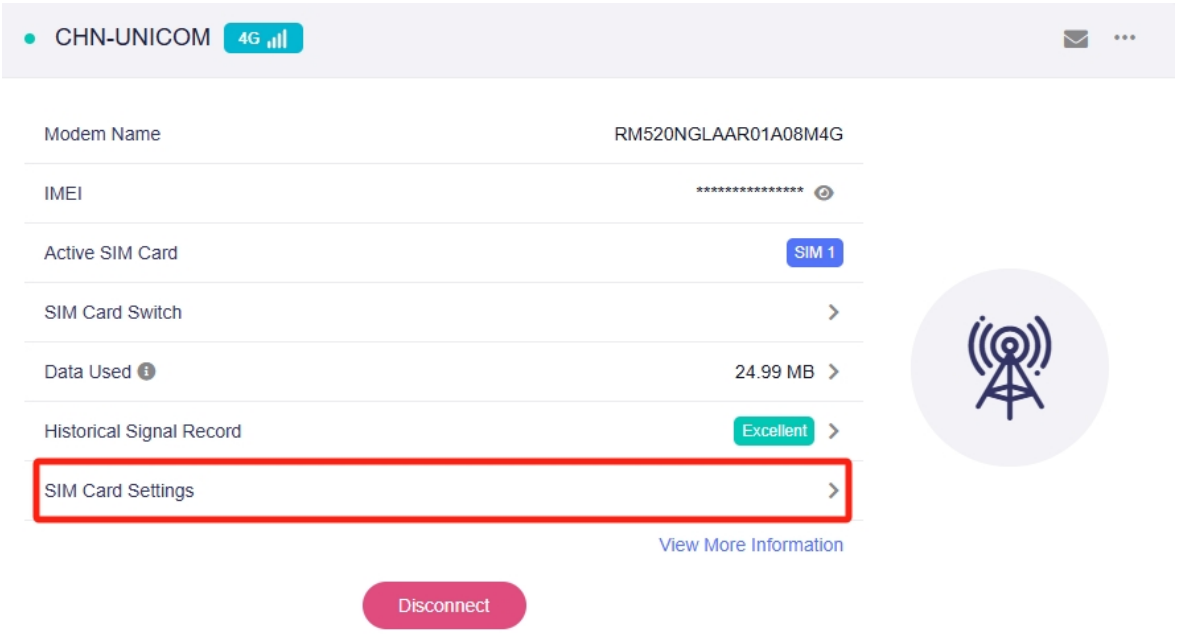
5. Kliknij **View More Information**, aby wyświetlić dodatkowe informacje o połączeniu komórkowym, w tym szczegóły modemu, karty SIM, Internetu i sygnału komórkowego.



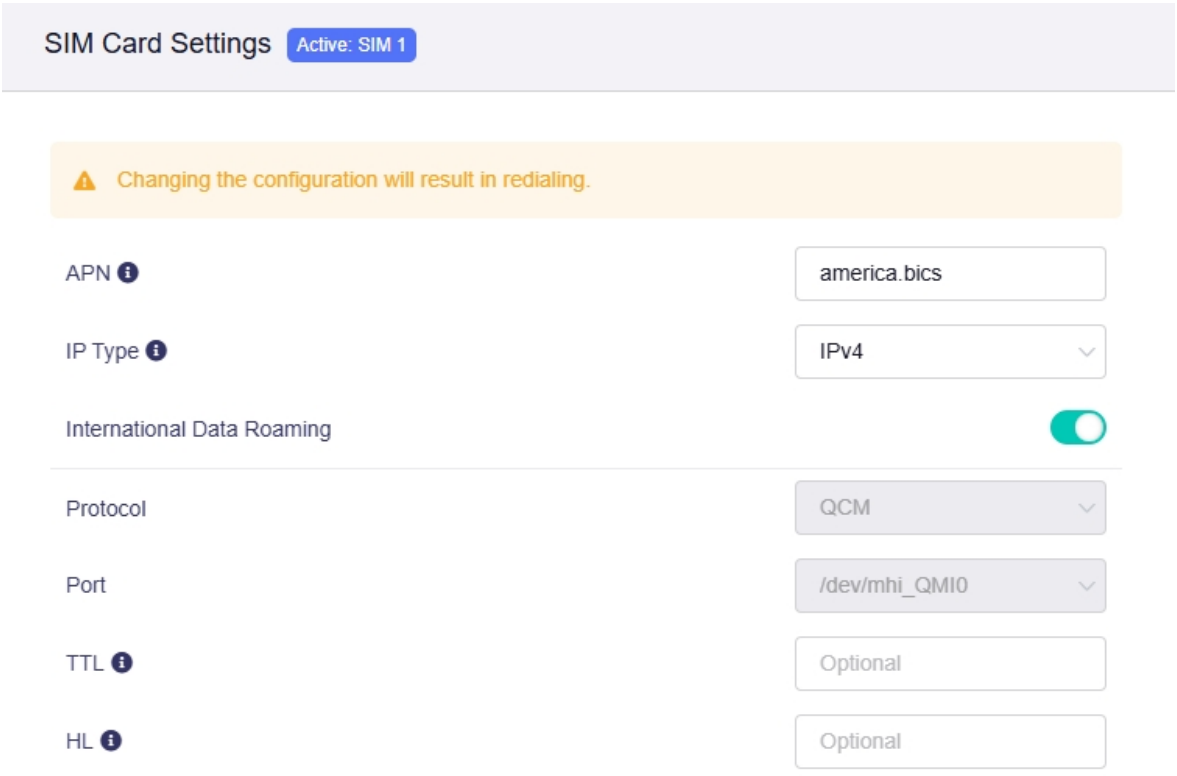
Jeśli konfiguracja automatyczna się nie powiedzie, spróbuj użyć **Manual Setup**.

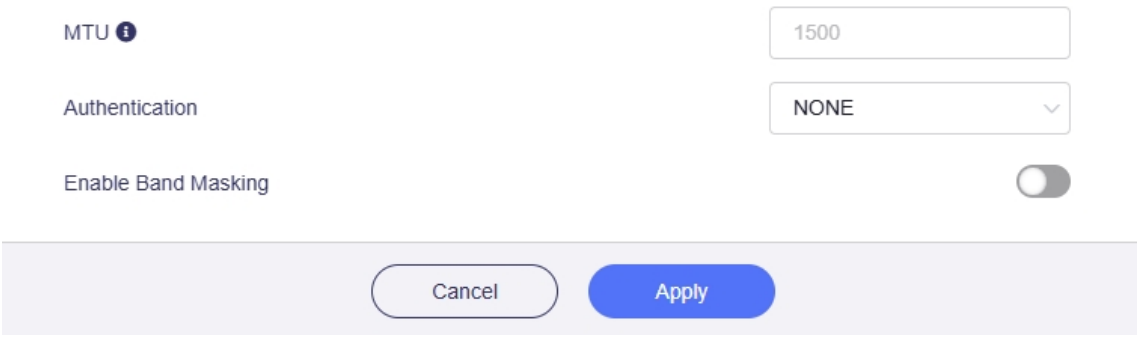
4.2.4.2 Konfiguracja ręczna

1. W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**, a następnie kliknij **SIM Card Settings**.



2. Możesz wyświetlić lub zmienić ustawienia komórkowe bieżącej karty SIM. Zastosowanie zmian spowoduje ponowne nawiązanie połączenia.

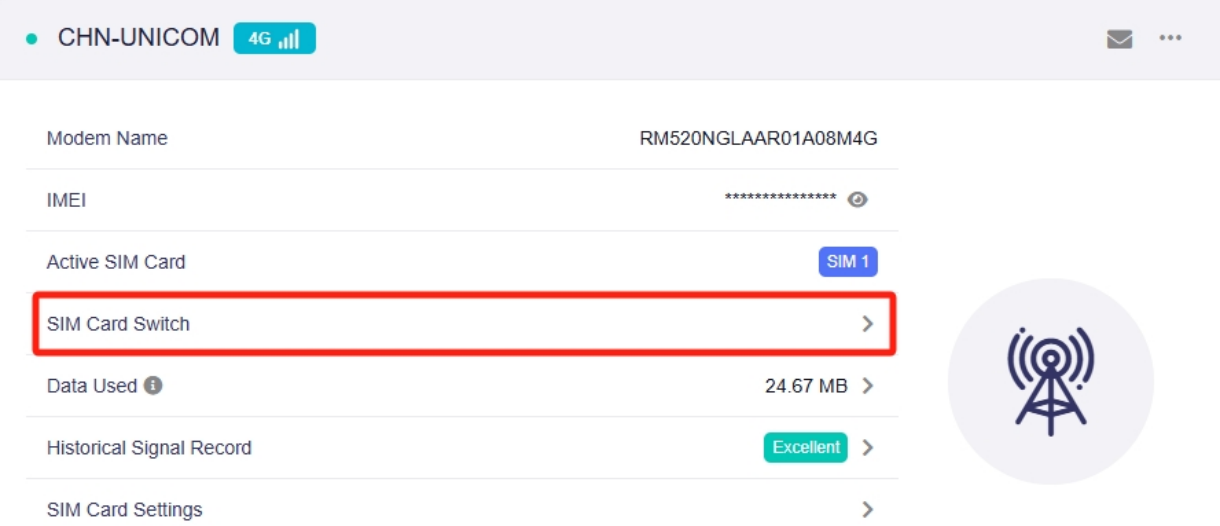




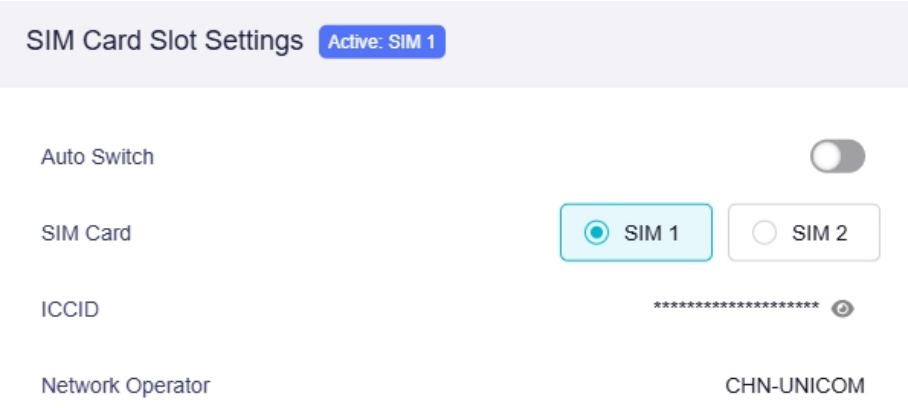
- **APN**: APN (Access Point Name) to parametr bramy wymagany do połączenia z siecią komórkową. Umożliwia routerowi łączenie się z Internetem udostępnianym przez operatora komórkowego. Możesz użyć domyślnego APN lub ustawić własny APN podany przez operatora.
- **Protocol**: automatycznie wykrywany protokół komunikacji komórkowej (np. QMI lub QCM), zależny od modemu i operatora.
- **Port**: automatycznie wykrywany port szeregowy do komunikacji z modemem komórkowym.
- **TTL**: TTL (Time To Live) określa maksymalny czas istnienia pakietów w sieci. Ustawienie TTL dotyczy wyłącznie IPv4. Domyślnie router zmniejsza TTL pakietów otrzymanych od urządzeń klienckich o 1 przed ich przekazaniem. Jeśli chcesz zmienić tę wartość, wprowadź żądaną efektywną wartość TTL powiększoną o 1, aby skompensować automatyczne zmniejszenie.
- **HL**: w IPv6 HL (Hop Limit) ogranicza liczbę przeskoków transmisji pakietów w sieci i stanowi odpowiednik TTL w IPv4.
- **MTU**: domyślna wartość MTU wynosi 1500 bajtów.
- **Authentication**: wybierz metodę uwierzytelniania wymaganą przez operatora (np. NONE, PAP, CHAP). Jeśli dane logowania nie są wymagane, zwykle wybiera się NONE.
- **Band Masking**: możesz włączyć tę funkcję, jeśli chcesz blokować określone pasma lub używać tylko wybranych pasm komórkowych. Szczegóły znajdziesz w sekcji 4.2.4.6 Maskowanie pasm.

4.2.4.3 Ustawienia gniazd kart SIM

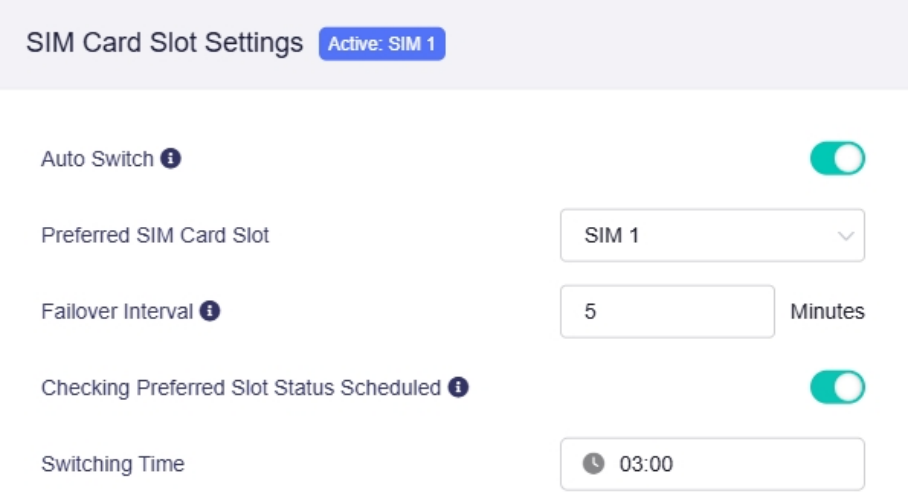
W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**, a następnie kliknij **SIM Card Switch**.



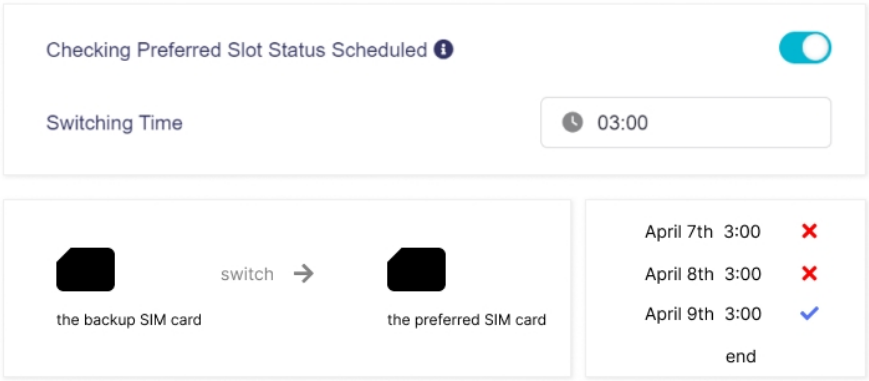
Pojawią się przycisk automatycznego przełączania, aktywna karta SIM, ICCID i operator sieci.



Jeśli włożone są dwie karty SIM, możesz włączyć **Auto Switch**.



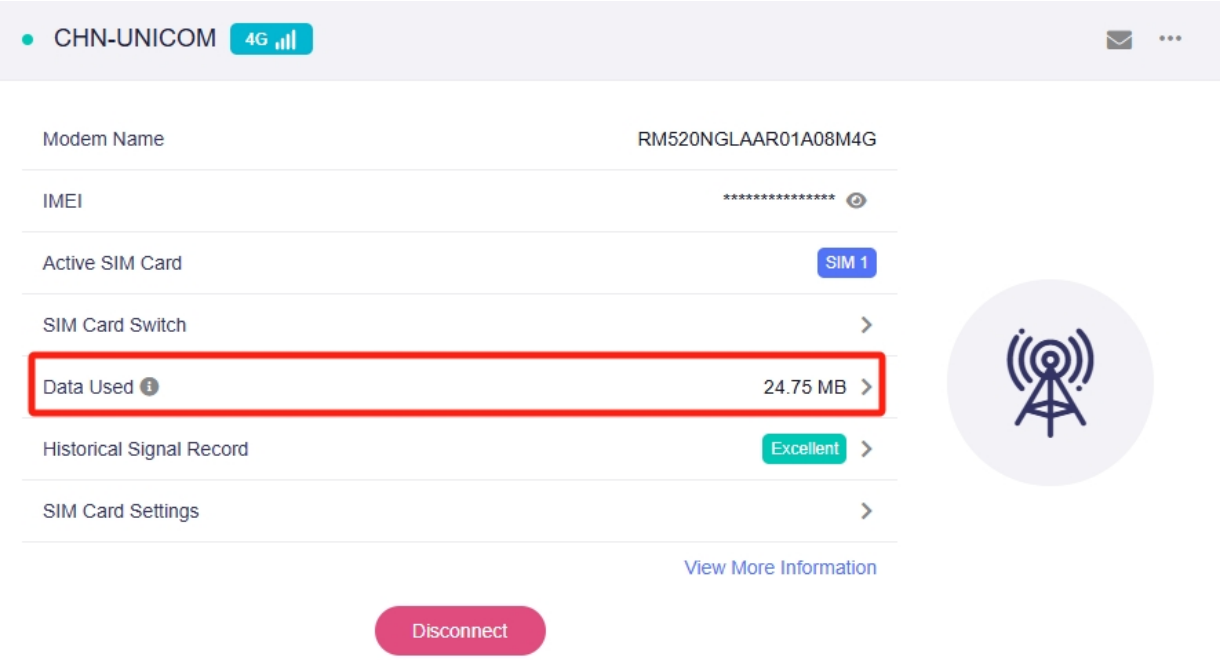
- **Auto Switch**: umożliwia automatyczne przełączanie między SIM 1 i SIM 2. Metoda wykrywania sieci dla automatycznego przełączania SIM jest taka sama jak skonfigurowana na stronie Multi-WAN.
- **Preferred SIM Card Slot**: ustaw preferowaną kartę SIM na SIM 1 lub SIM 2.
- **Failover Interval**: dostępne wartości mieszczą się w zakresie od 5 minut do 24 godzin. Jeśli po przełączeniu awaryjnym połączenie z Internetem nadal jest niedostępne, urządzenie przełączy się z powrotem na preferowane gniazdo SIM i odczeka ten czas przed kolejną próbą przełączenia awaryjnego.
  Ta opcja ma zastosowanie, gdy zarówno preferowana, jak i zapasowa karta SIM nie ma sygnału. Urządzenie będzie przełączać się między kartami SIM, aż jedna z nich uzyska prawidłowy sygnał.
- **Checking Preferred Slot Status Scheduled**
  Po włączeniu urządzenie będzie codziennie o ustalonej godzinie sprawdzać preferowane gniazdo SIM i próbować przełączyć się na nie, jeśli preferowana karta odzyska dostęp do Internetu.
  Zapobiega to nadmiernemu zużyciu danych przez zapasową kartę SIM. Jeśli preferowana karta nadal nie ma sygnału, urządzenie będzie korzystać z karty zapasowej.



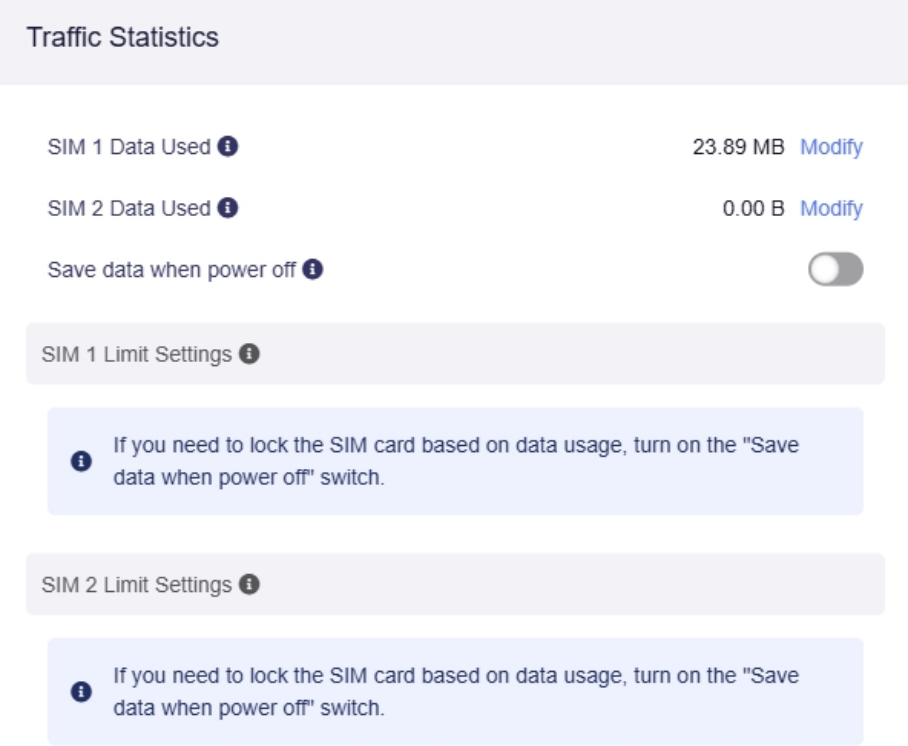
Uwaga: funkcja Auto Switch nie przełącza natychmiast na drugą kartę SIM. Najpierw urządzenie potrzebuje czasu, aby potwierdzić, że bieżąca karta nie ma dostępu do Internetu. Ponadto druga karta SIM nie znajduje się w trybie gotowości i jej aktywacja wymaga czasu.

4.2.4.4 Statystyki ruchu

W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**, a następnie kliknij **Data Used**.



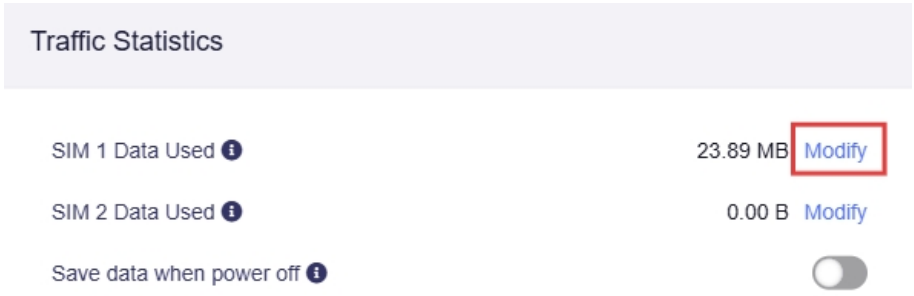
Otworzy się strona **Traffic Statistics**. Wyświetla zużycie danych kart SIM i umożliwia ustawienie limitów danych.



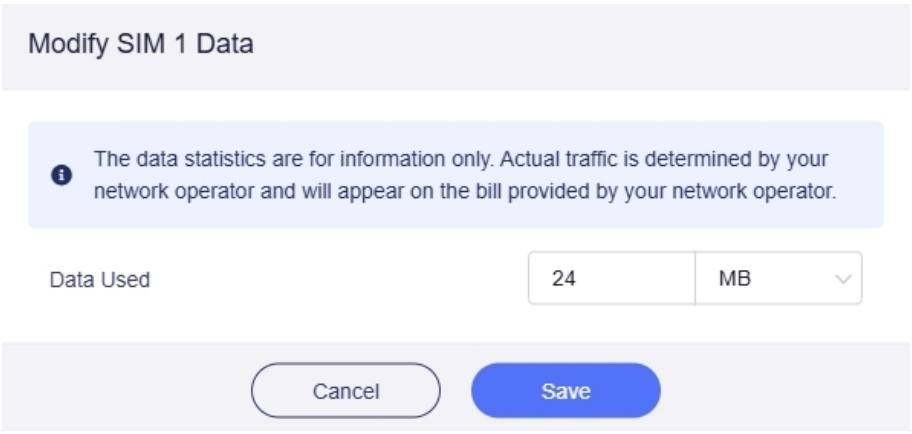
Jeśli zużycie danych przekroczy limit, ręcznie zmień **Data Cap Amount** lub **Data Used**. W przeciwnym razie sieć może zostać rozłączona lub może nastąpić automatyczne przełączenie karty SIM (w modelach z dwiema kartami SIM).

- **Zmiana zużycia danych**

  Kliknij **Modify** po prawej stronie SIM 1/2 Data Used.



  Następnie możesz zmienić lub wyzerować zużycie danych.

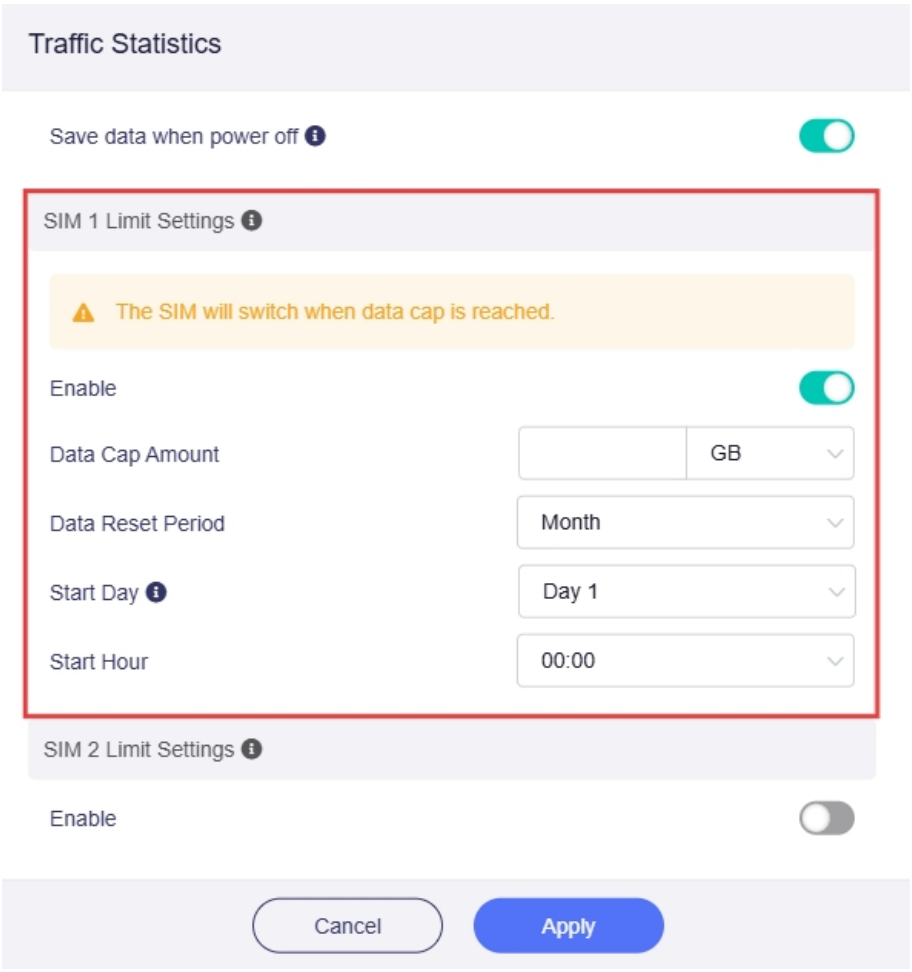


- **Ustawianie limitu danych karty SIM**

  Aby ustawić limit danych karty SIM, najpierw włącz **Save data when power off**. Dzięki temu dane będą zapisywane także po wyłączeniu zasilania urządzenia.



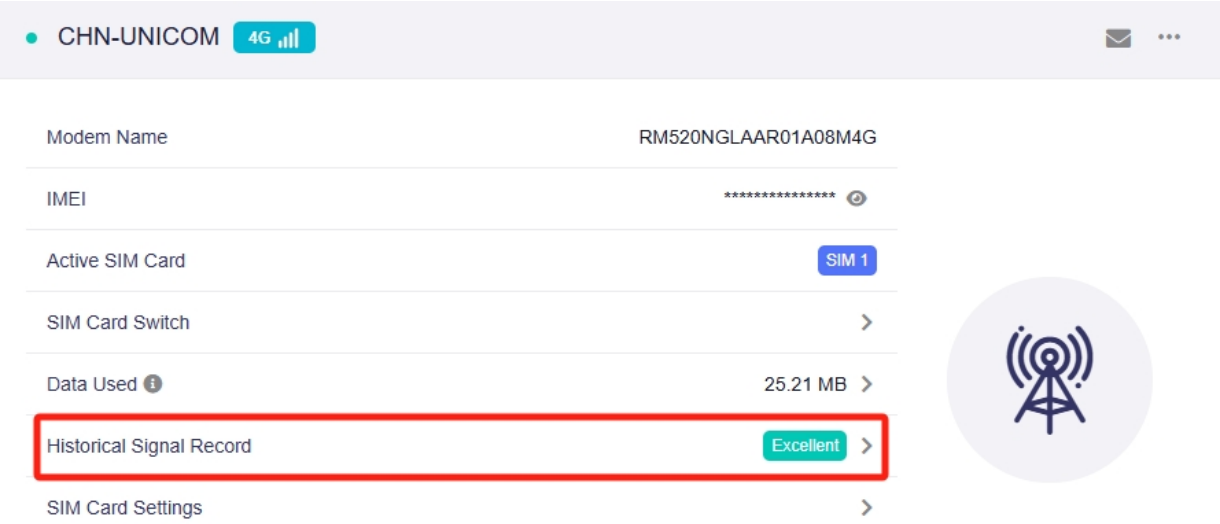
  Następnie włącz ustawienia limitu SIM 1 lub SIM 2.



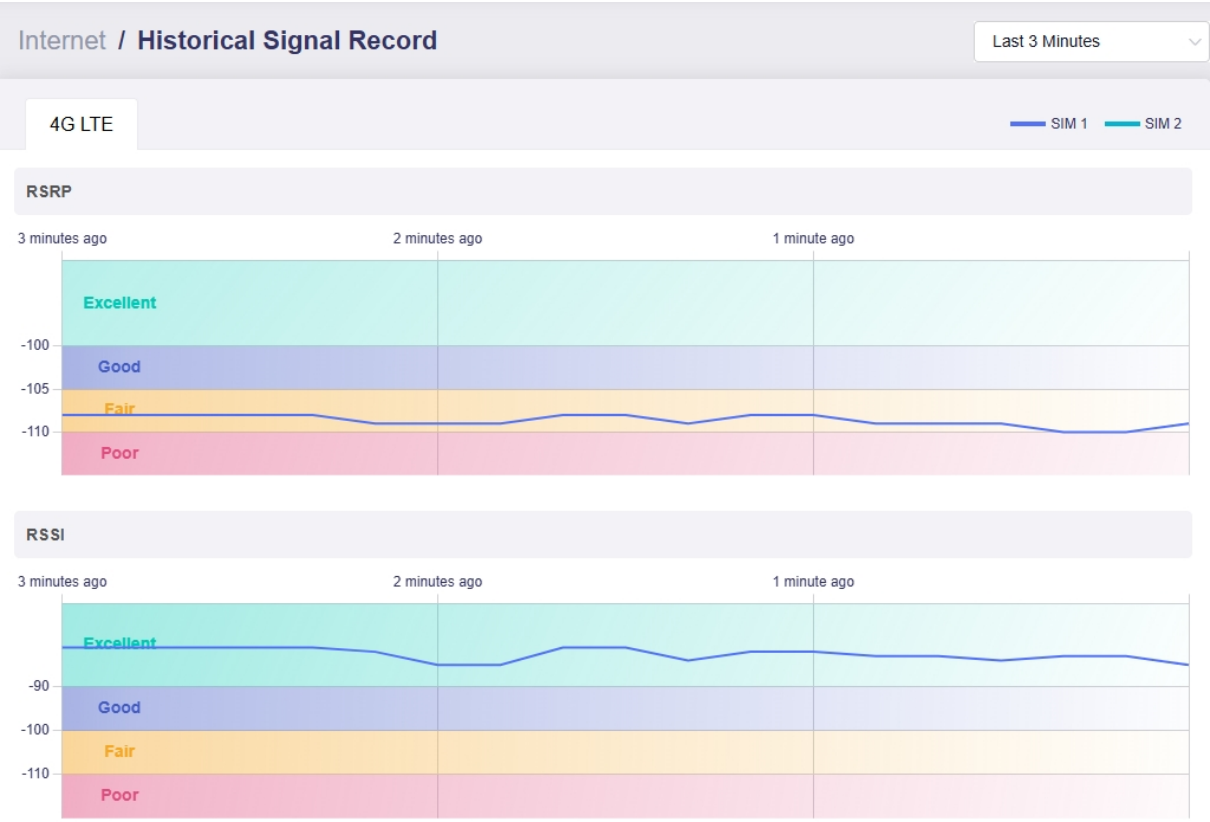
W modelach z dwiema kartami SIM zalecamy jednoczesne włączenie **SIM Card Slot Auto Switch**. Jeśli ustawiono limit danych SIM 1 i włączono automatyczne przełączanie gniazd, po przekroczeniu tego limitu nastąpi automatyczne przełączenie na SIM 2, a SIM 1 zostanie wyłączona.

4.2.4.5 Historia sygnału

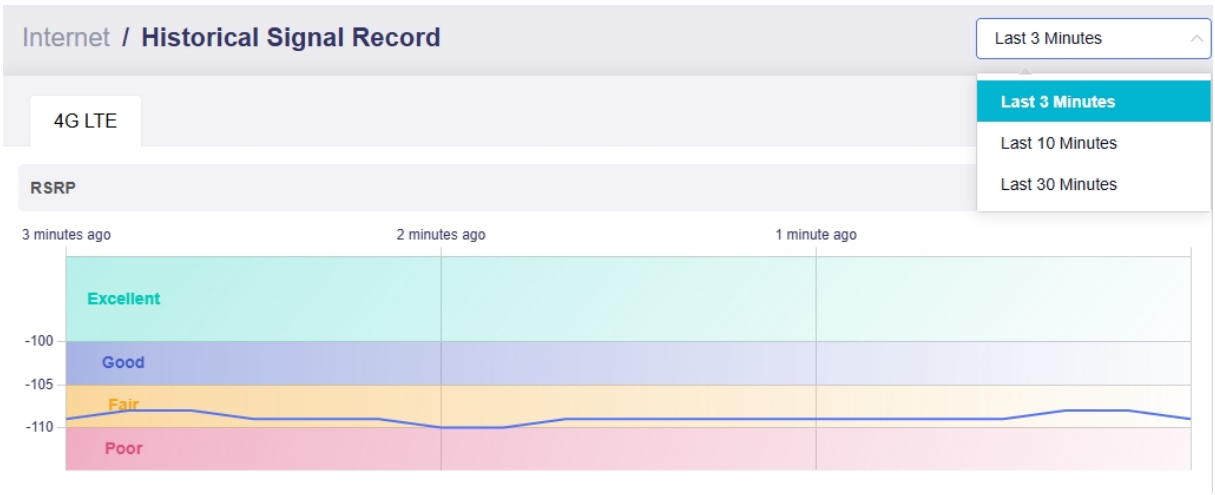
W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**, a następnie kliknij **Historical Signal Record**.



Tutaj możesz sprawdzić jakość połączenia komórkowego. Jeśli sygnał jest słaby, spróbuj zmienić stację bazową, aby go poprawić.



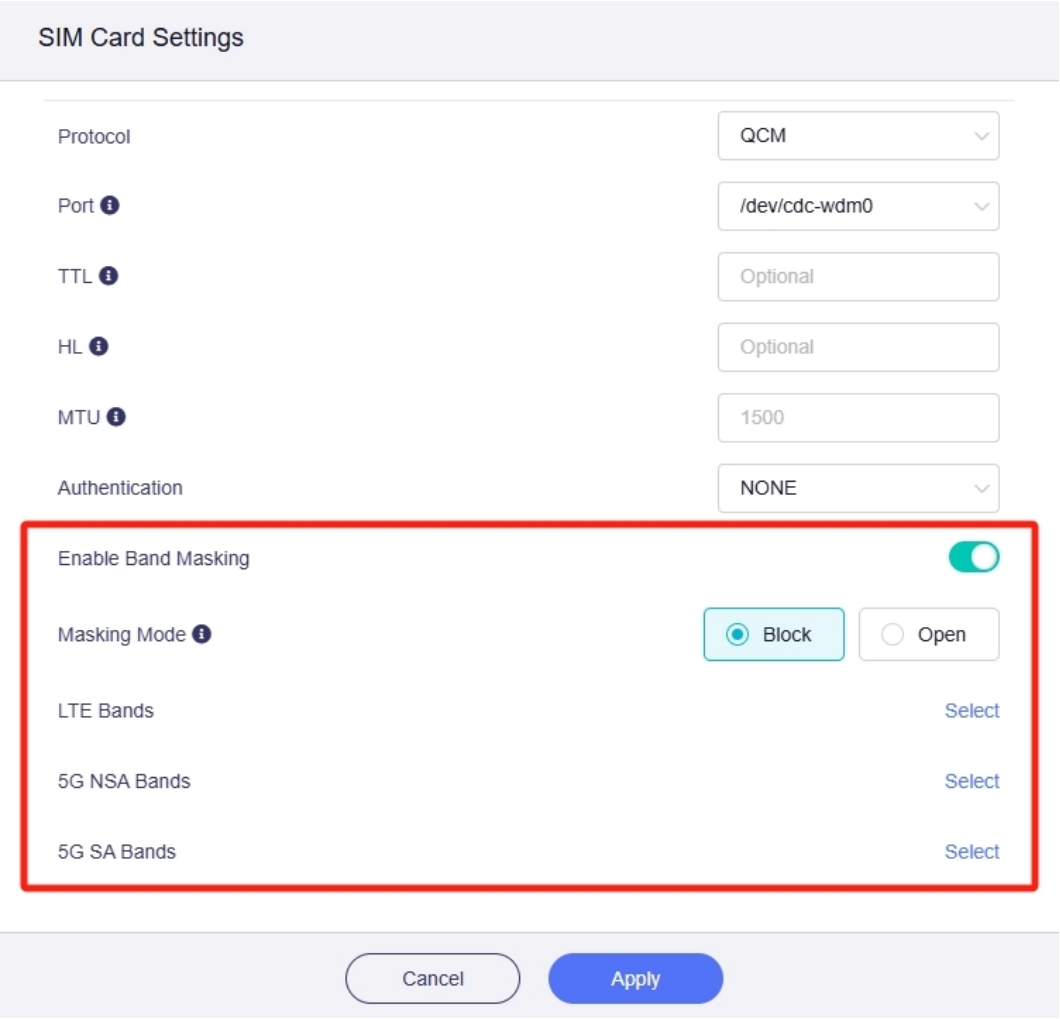
Wyświetl historię siły sygnału, wybierając różne przedziały czasu w prawym górnym rogu.


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

4.2.4.6 Maskowanie pasm

Maskowanie pasm umożliwia blokowanie określonych pasm lub korzystanie tylko z preferowanych pasm komórkowych, aby poprawić słaby sygnał komórkowy.

W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular** > **SIM Card Settings** i włącz **Enable Band Masking**.



Wybierz **Masking Mode** (Block lub Open), a następnie wybierz pasma LTE, 5G NSA i 5G SA.

4.2.4.7 SMS i przekazywanie SMS

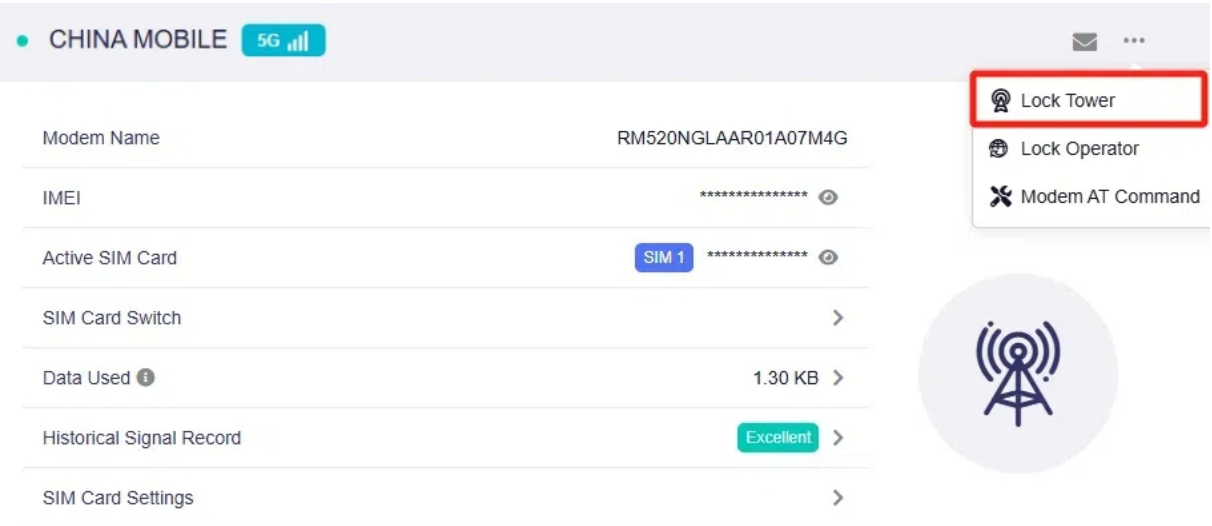
Zapoznaj się z sekcjami SMS i Przekazywanie SMS.

4.2.4.8 Blokowanie stacji bazowej

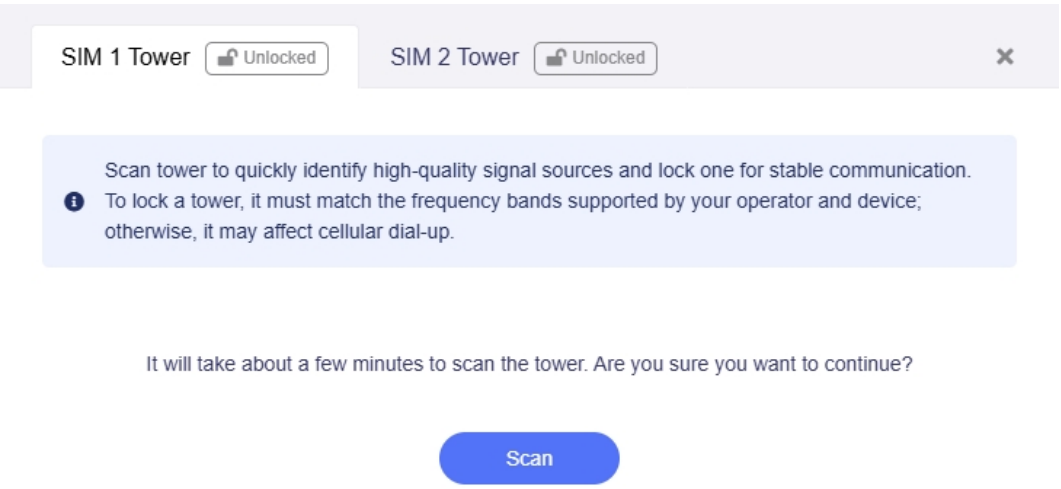
Aby uzyskać sygnał wysokiej jakości i zapewnić stabilne połączenie komórkowe, możesz spróbować zablokować router na określonej stacji bazowej.

Uwaga: zablokowana stacja bazowa musi odpowiadać pasmom obsługiwanym przez operatora i urządzenie; w przeciwnym razie połączenie może się nie powieść.

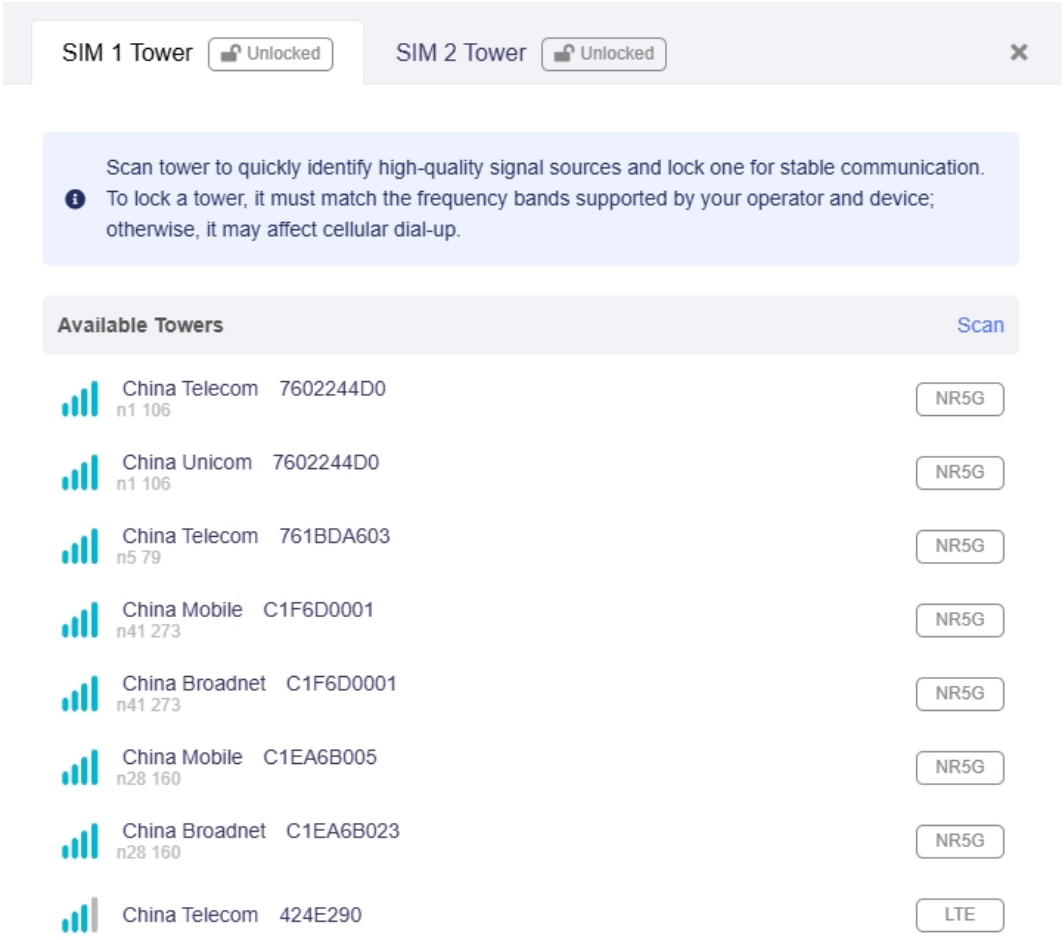
W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**. Kliknij ikonę trzech kropek w prawym górnym rogu, a następnie wybierz **Lock Tower**.



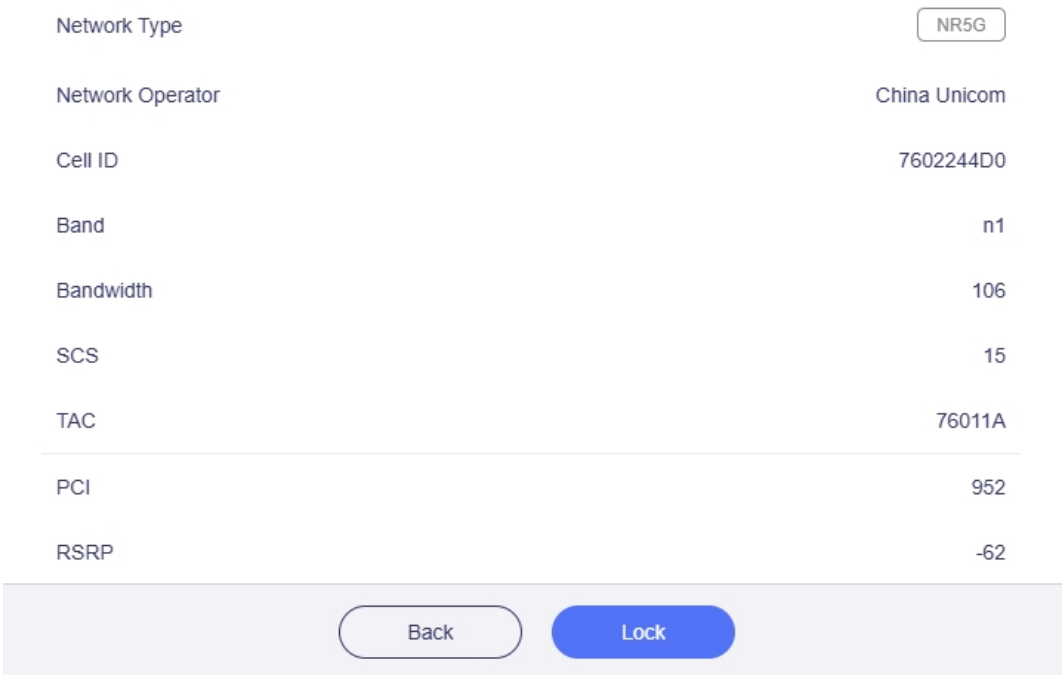
Kliknij **Scan**, aby rozpocząć skanowanie stacji bazowych. Zajmie to kilka minut. Nie odświeżaj strony podczas skanowania.



Pojawią się dostępne stacje bazowe.



Kliknij stację bazową, aby wyświetlić szczegóły i zablokować na niej połączenie.



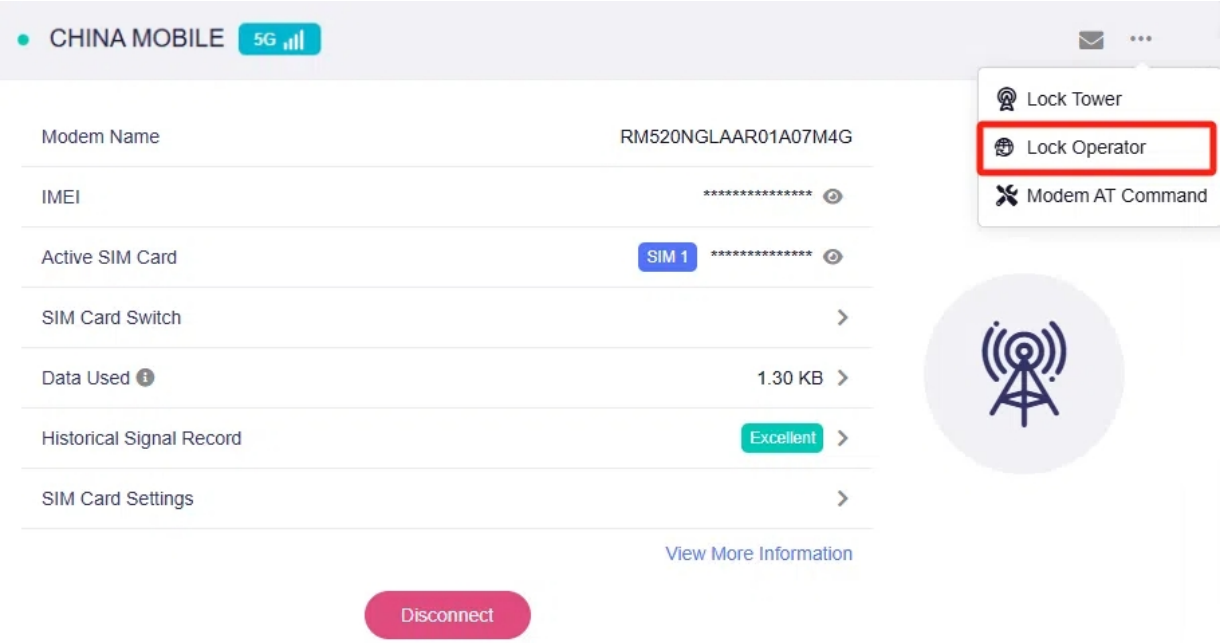
Uwaga:

1. Urządzenie może nie być w stanie wyszukać wszystkich stacji bazowych, gdy interfejs Cellular jest włączony.
2. Jeśli zablokowana stacja bazowa nie odpowiada ustawieniom maskowania pasm lub parametrom APN w ustawieniach komórkowych, router nie będzie mógł połączyć się z siecią komórkową.
3. Po zablokowaniu stacji bazowej i przeniesieniu routera w inne miejsce router po ponownym uruchomieniu nadal będzie próbował połączyć się z zablokowaną stacją. Może to uniemożliwić automatyczne połączenie z siecią komórkową w nowej lokalizacji. W takim przypadku odblokuj bieżącą stację bazową lub ręcznie zablokuj połączenie na nowej stacji.

4.2.4.9 Blokowanie operatora

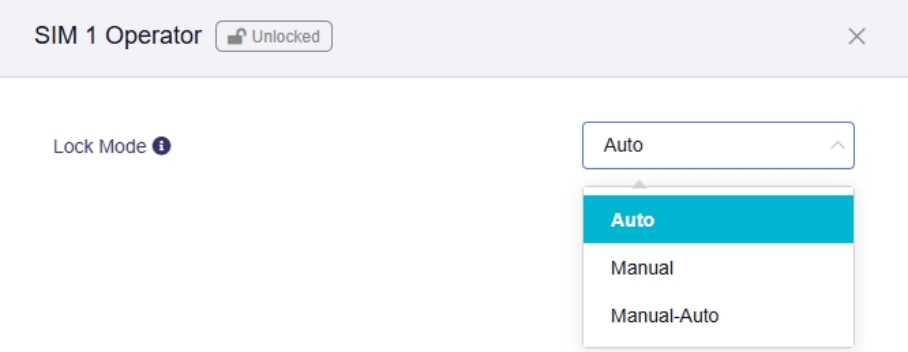
Po zablokowaniu na określonym operatorze komórkowym router będzie korzystał wyłącznie z jego sieci. Zapewnia to stabilne połączenie i pozwala uniknąć niezamierzonych opłat roamingowych, szczególnie w rejonach przygranicznych, gdzie urządzenie mogłoby połączyć się z siecią zagraniczną.

W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**. Kliknij ikonę trzech kropek w prawym górnym rogu, a następnie wybierz **Lock Operator**.



Dostępne są trzy tryby blokowania:

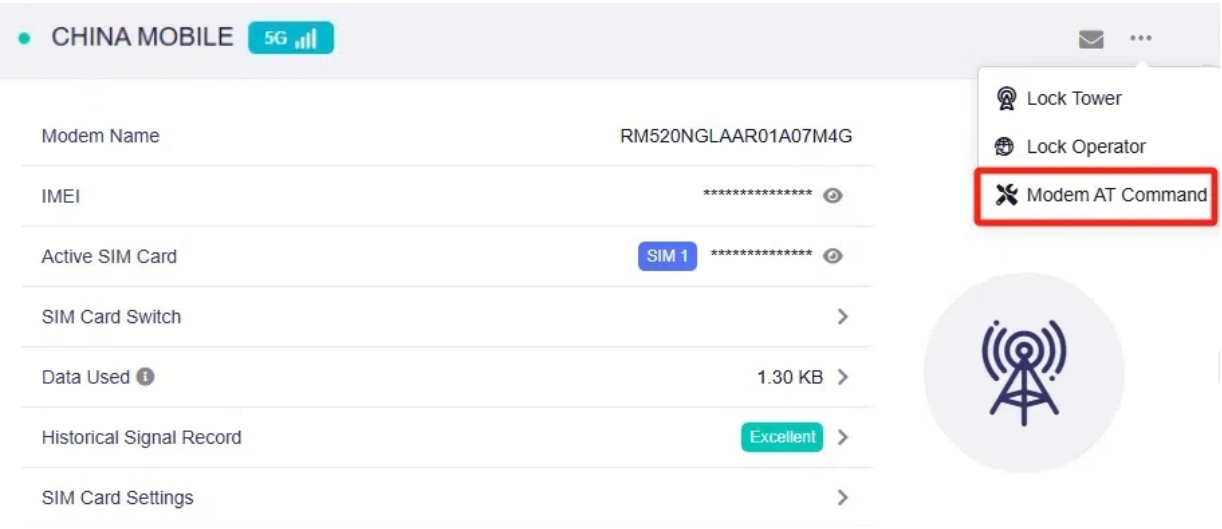
- **Auto**: automatyczne łączenie z dostępną siecią operatora.
- **Manual**: ręczne blokowanie na określonym operatorze.
- **Manual-Auto**: automatyczne przełączenie na dostępną sieć operatora, jeśli ręczne blokowanie się nie powiedzie.



4.2.4.10 Polecenia AT modemu

Polecenia AT modemu to standardowe instrukcje służące do komunikacji z modemem komórkowym. Ta funkcja umożliwia wysyłanie poleceń i sprawdzanie stanu modemu.

W internetowym panelu administracyjnym routera przejdź do **INTERNET** > **Cellular**. Kliknij ikonę trzech kropek w prawym górnym rogu, a następnie wybierz **Modem AT Command**.



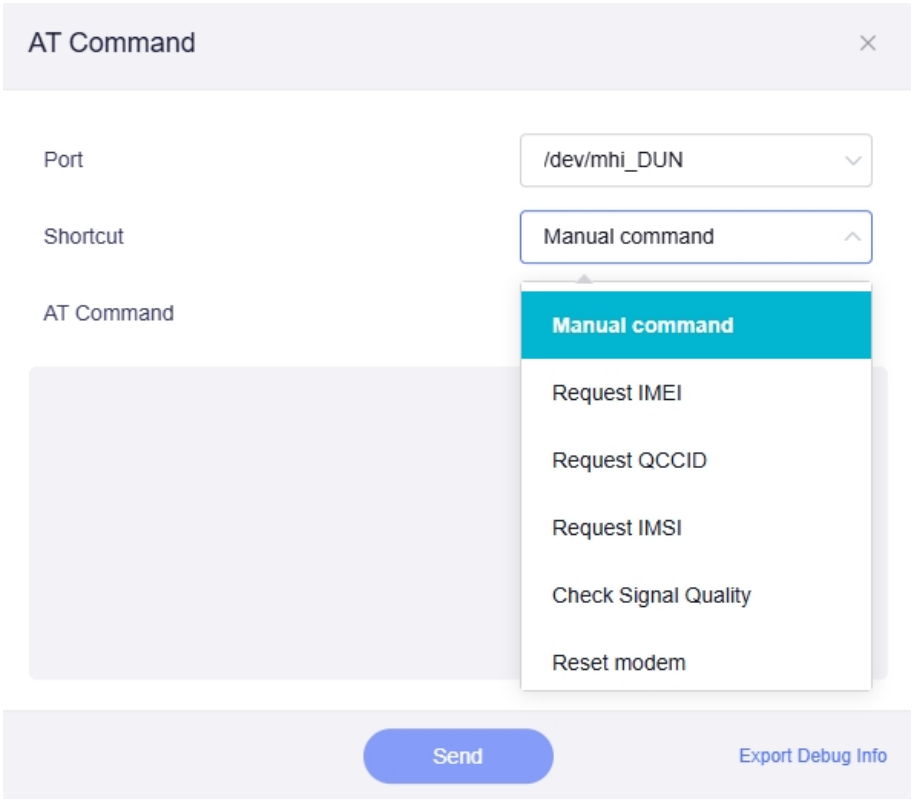
Otworzy się strona AT Command.

- **Polecenie ręczne**

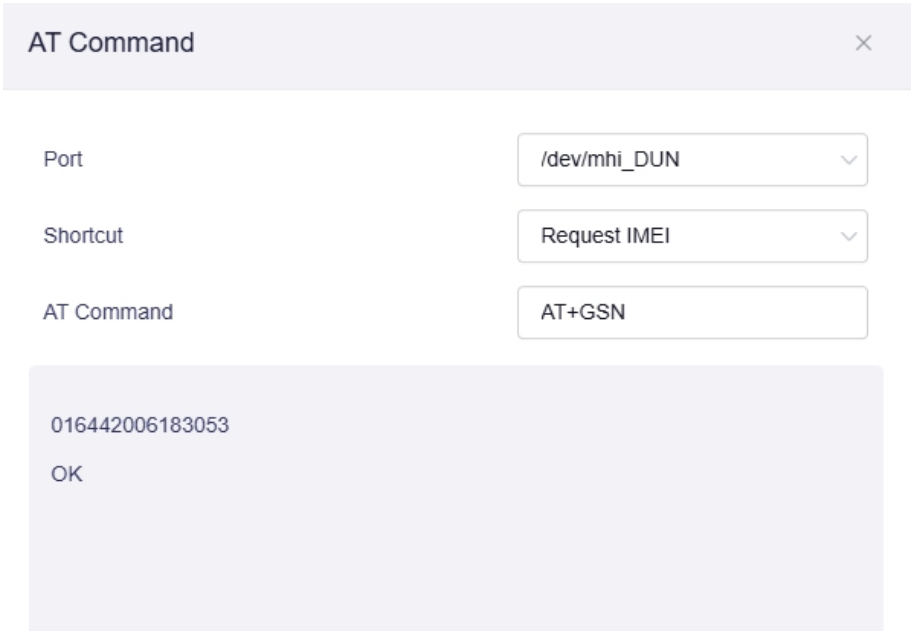
  Gdy w polu Shortcut wybrano Manual command, możesz wpisać żądane polecenie w polu AT Command. Wyniki pojawią się w szarym polu na dole.

- **Polecenie predefiniowane**

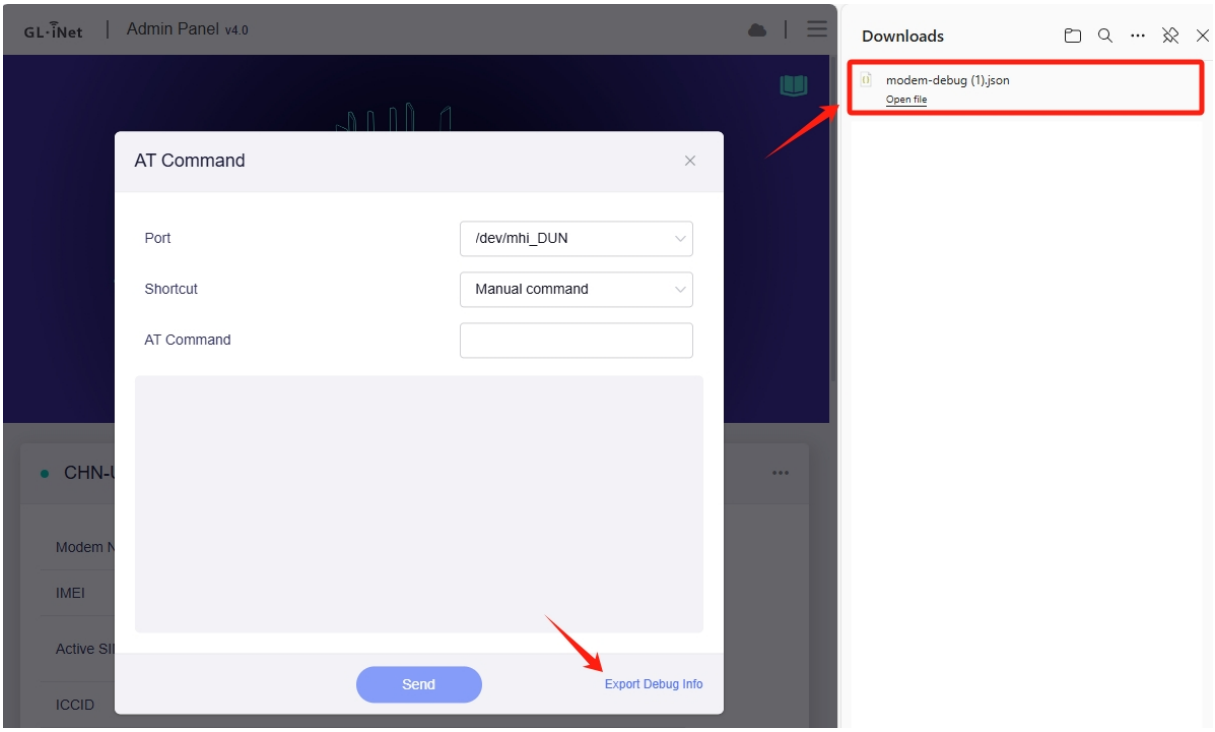
  Możesz też kliknąć pole Shortcut i wybrać z listy rozwijanej predefiniowane polecenie, np. Request IMEI, Check Signal Quality lub Reset Modem.



Na przykład wybierz skrót „Request IMEI” i kliknij „Send”. Wynik zostanie wyświetlony jak poniżej.



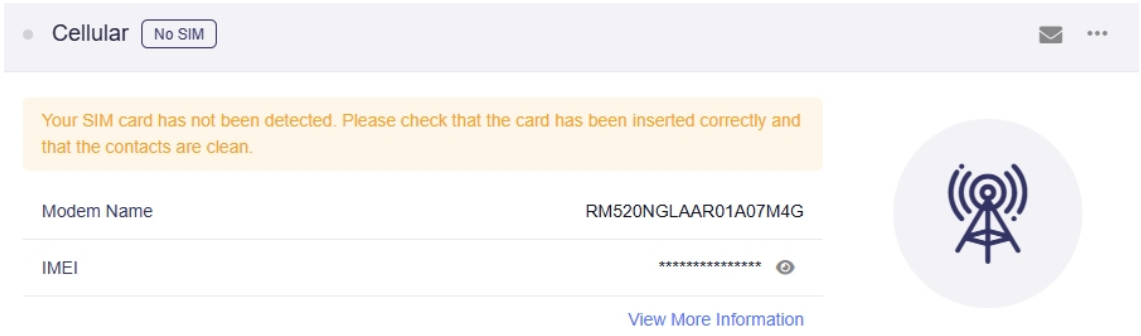
W prawym dolnym rogu możesz kliknąć **Export Debug Info**, aby pobrać plik .json.



4.2.4.11 Rozwiązywanie problemów

Jeśli nie możesz nawiązać połączenia komórkowego, wybierz odpowiednie rozwiązanie na podstawie poniższego komunikatu o błędzie.

- **Brak karty SIM / Nie wykryto karty SIM.**



Oto kilka wskazówek.

1. Odśwież stronę i odczekaj kilka minut, aby sprawdzić, czy karta SIM zostanie wykryta.
2. Upewnij się, że karta SIM została prawidłowo włożona. Dopasuj wycięcie na karcie SIM do odpowiedniego oznaczenia na gnieździe, aby potwierdzić właściwy kierunek wkładania.
3. Wyłącz router, wyjmij i ponownie włóż kartę SIM, a następnie włącz router.

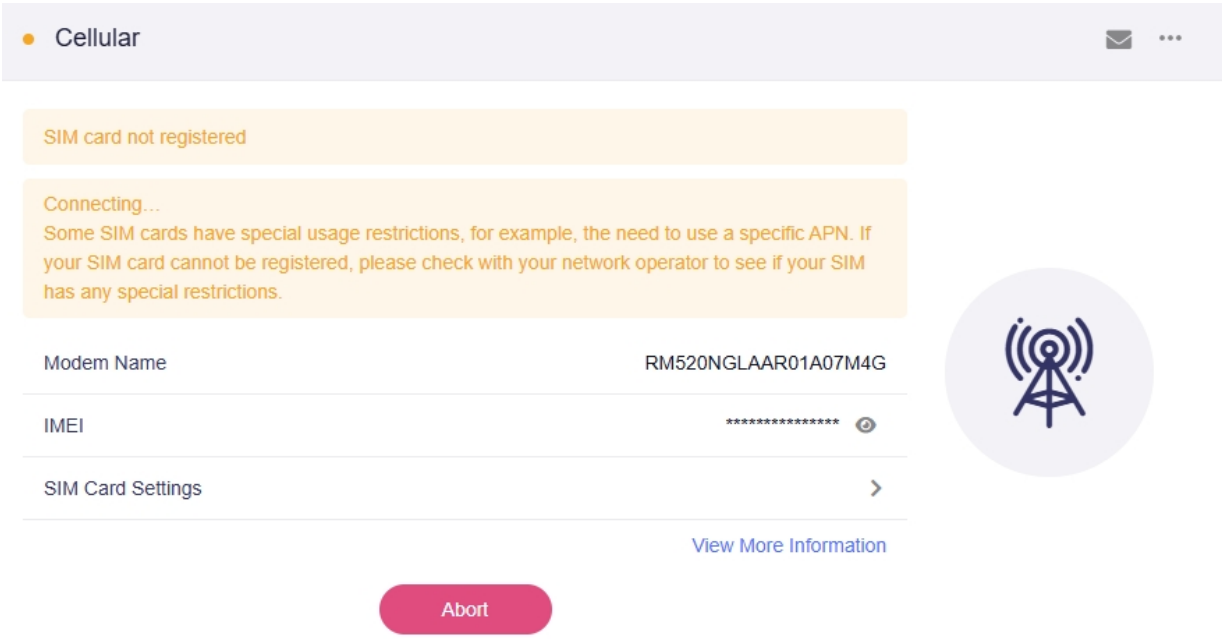
4. Jeśli masz taką możliwość, spróbuj użyć innej karty SIM.

Jeśli problem nadal występuje, pobierz dzienniki i wyślij je na adres support@gl-inet.com.

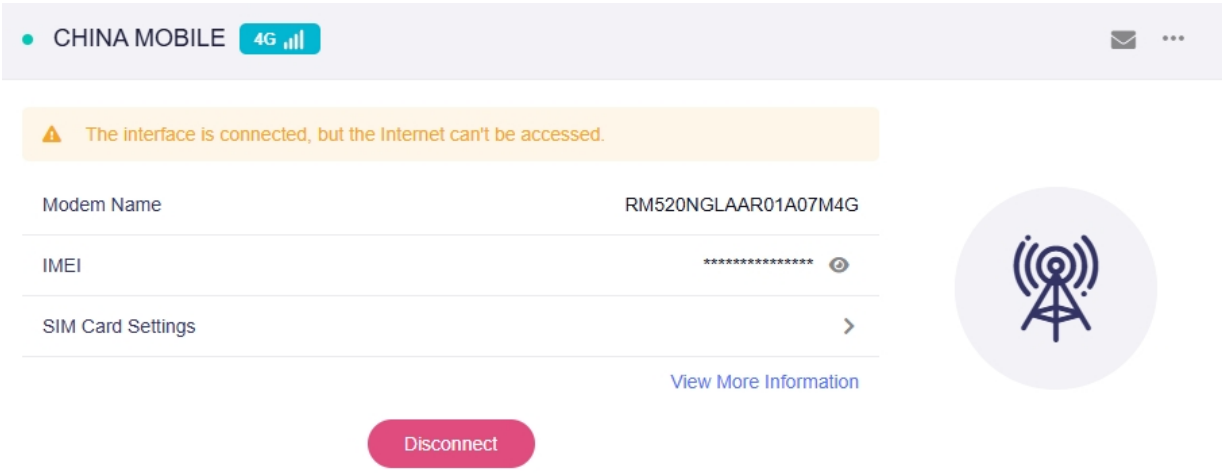
- **Karta SIM niezarejestrowana / Interfejs jest połączony, ale nie można uzyskać dostępu do Internetu.**

Ten problem może powodować dwa rodzaje komunikatów o błędzie:

(1) Karta SIM niezarejestrowana.



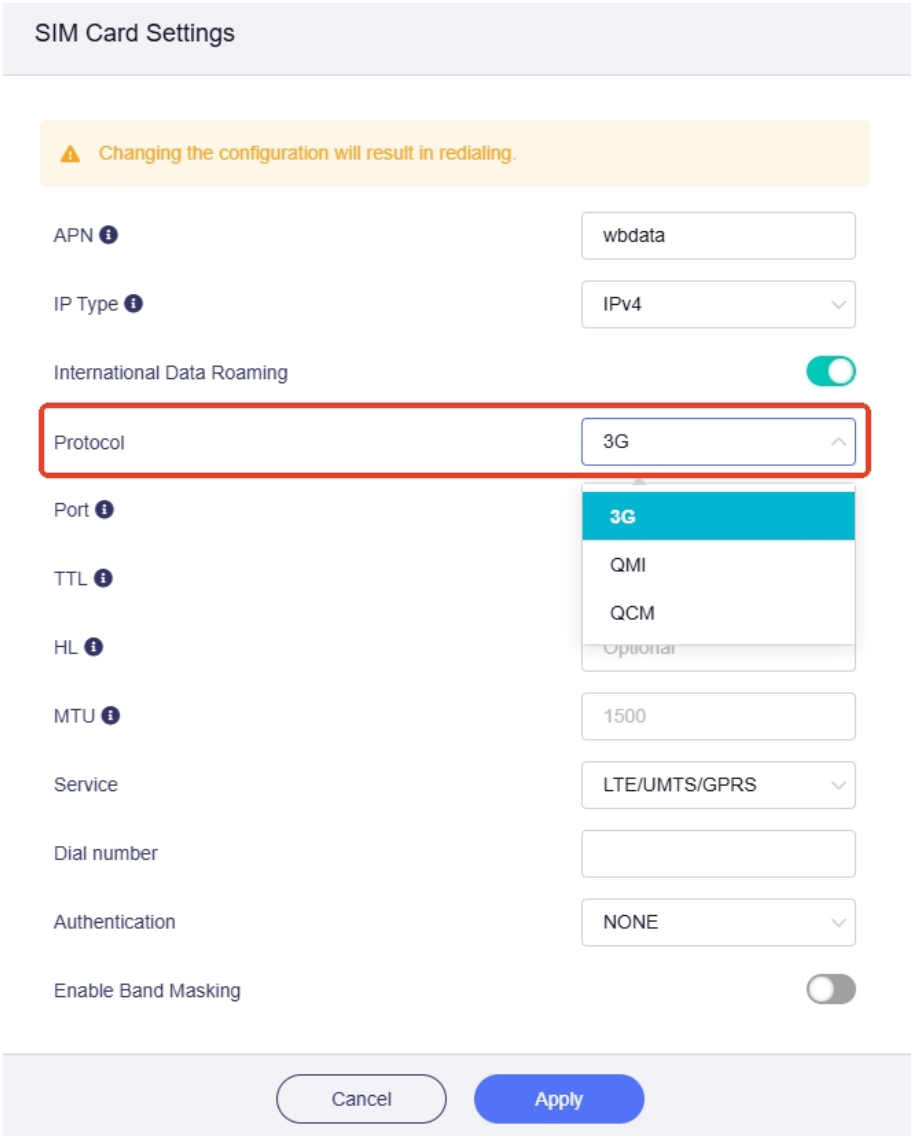
(2) Interfejs jest połączony, ale nie można uzyskać dostępu do Internetu.



Oto kilka wskazówek.

1. Odśwież stronę i odczekaj kilka minut, aby sprawdzić, czy błąd zniknie.
2. Kliknij **Disconnect**/**Abort**, a następnie **Connect**, aby spróbować ponownie nawiązać połączenie.

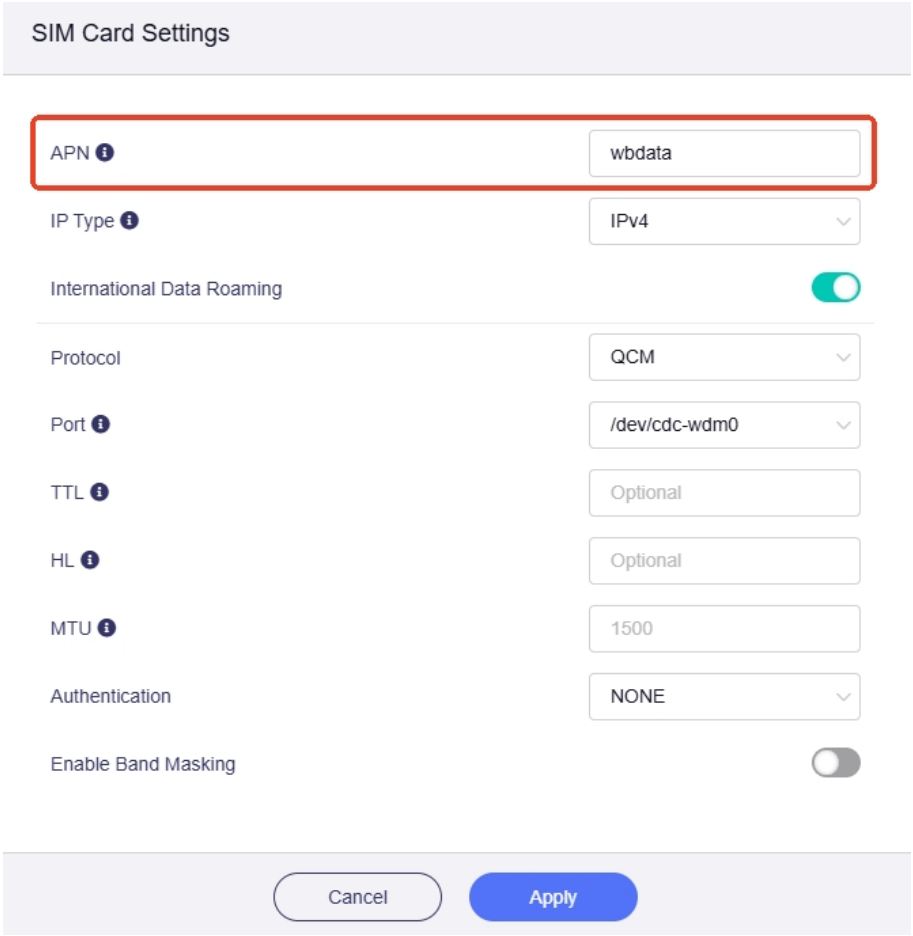
3. Uruchom router ponownie.
4. Sprawdź stan karty SIM i upewnij się, że jest aktywowana. Włóż ją do smartfona i sprawdź, czy umożliwia normalny dostęp do Internetu z aktywnym pakietem danych komórkowych, lub skontaktuj się z operatorem w celu weryfikacji.
5. Niektórzy operatorzy mogą wymagać protokołu 3G do połączenia z siecią. Przejdź do **SIM Card Settings** > **Protocol**, wybierz **3G**, a następnie kliknij **Apply**.



Urządzenie automatycznie nawiąże połączenie ponownie. Odczekaj kilka minut i sprawdź, czy połączenie się powiodło.

6. Niektóre karty SIM mogą mieć szczególne ograniczenia użytkowania (np. wymagać określonego APN). Jeśli karta SIM nie może się zarejestrować, skontaktuj się z

operatorem i sprawdź ewentualne ograniczenia. W razie potrzeby przejdź do **SIM Card Settings** > **APN**, skonfiguruj prawidłowy APN na routerze, a następnie kliknij **Apply**.



7. Kliknij **View More Information**, aby sprawdzić siłę sygnału komórkowego. Jeśli sygnał jest słaby, upewnij się, że antena jest prawidłowo zamontowana. Przenieś router w otwarte miejsce bez przeszkód, aby poprawić odbiór sygnału.
8. Sprawdź, czy włączono **Band Masking** lub **Lock Tower**. Jeśli tak, wyłącz te funkcje i spróbuj ponownie nawiązać połączenie.

Jeśli problem nadal występuje, pobierz dzienniki i wyślij je na adres support@gl-inet.com.

Rozdział 5

Sieć bezprzewodowa

W tym rozdziale opisano sprawdzanie stanu Wi-Fi i konfigurowanie ustawień sieci bezprzewodowej.

5.1 Wyświetlanie stanu Wi-Fi

Sieci Wi-Fi routera są domyślnie włączone, a odpowiednia ikona Wi-Fi świeci pod obrazem urządzenia na stronie INTERNET.



Po najechaniu kursorem na ikonę włączonej sieci Wi-Fi pojawi się kod QR Wi-Fi, jak pokazano poniżej. Możesz zeskanować kod QR, aby szybko połączyć się z odpowiednią siecią Wi-Fi.



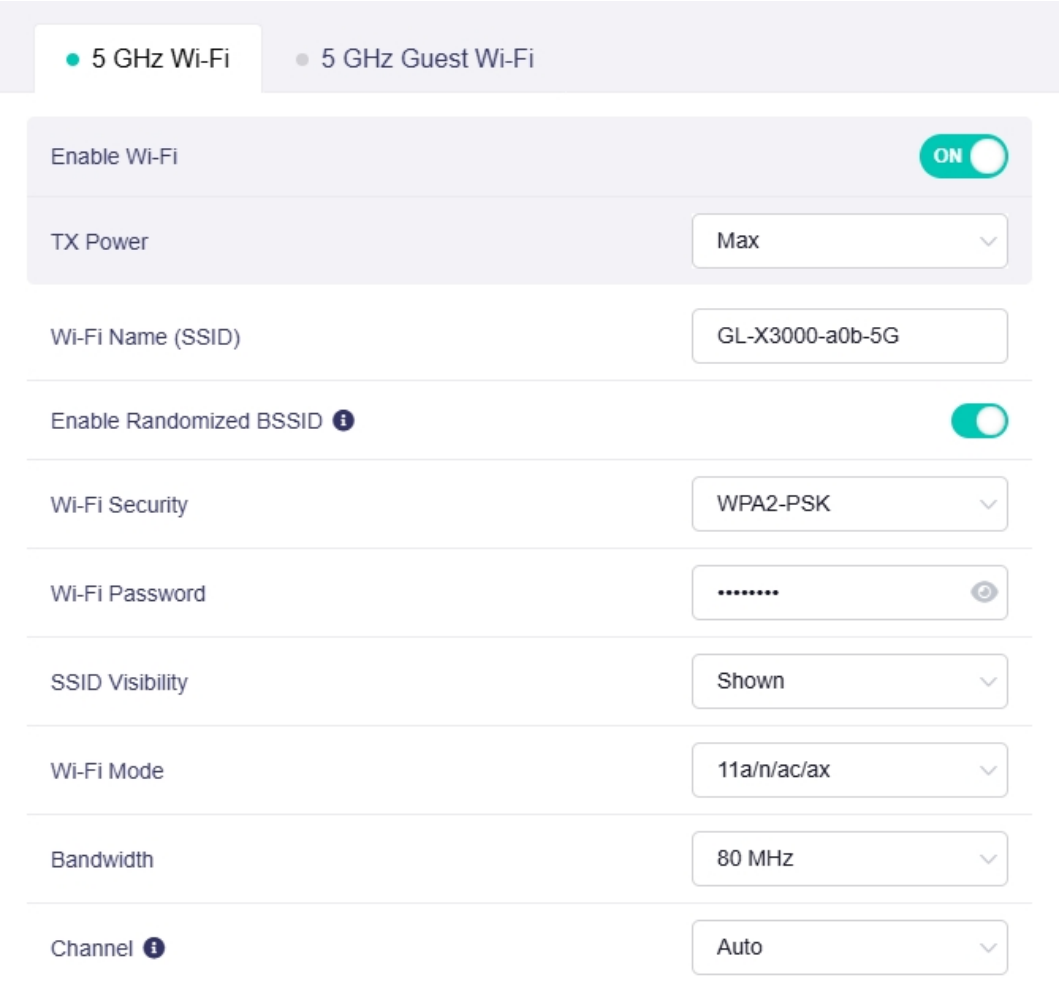
5.2 Ustawienia sieci bezprzewodowej

Zaloguj się do panelu administracyjnego routera i przejdź do **WIRELESS**.

Strona sieci bezprzewodowej wyświetla ustawienia Wi-Fi routera w pasmach 2,4 GHz i 5 GHz. Każde pasmo dzieli się na sieć główną i gościnną, co zapewnia elastyczne zarządzanie.

5.2.1 Wi-Fi 5 GHz

W głównej sieci Wi-Fi 5 GHz można skonfigurować wiele ustawień: włączanie i wyłączanie Wi-Fi, moc nadawania, włączanie i wyłączanie losowego BSSID, nazwę sieci Wi-Fi (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.



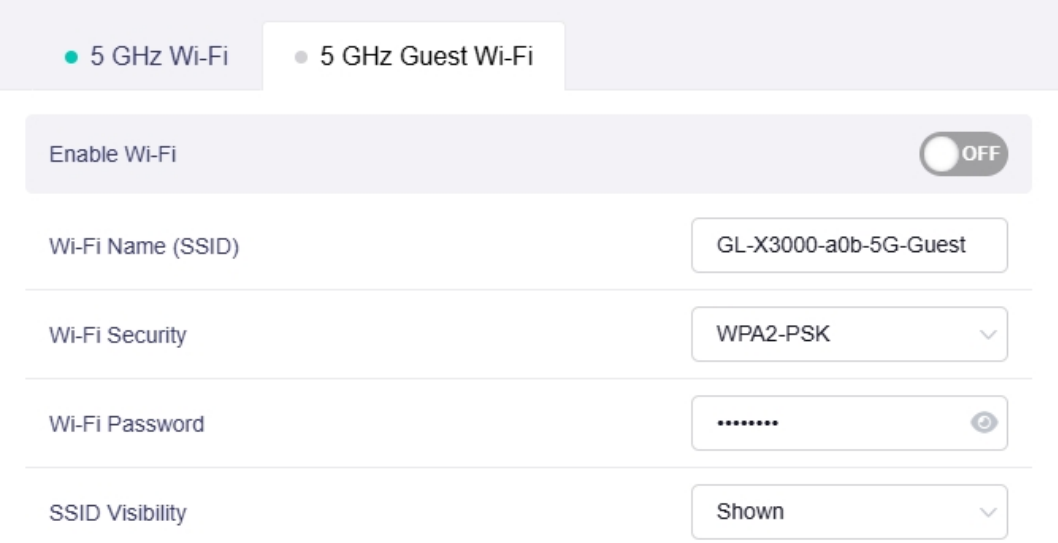
Uwaga:

1. **Randomized BSSID** jest domyślnie włączone. Pomaga zapobiegać śledzeniu routera za pomocą stałego BSSID, ponieważ urządzenia klienckie mogą przesyłać pobliskie identyfikatory BSSID i własne dane lokalizacyjne producentom systemów operacyjnych lub

urządzeń, którzy tworzą z nich bazę powiązań BSSID z lokalizacją. Po włączeniu tej opcji router używa losowo generowanego BSSID i odnawia go przy każdym uruchomieniu, dzięki czemu nie można powiązać BSSID ze stałą lokalizacją.

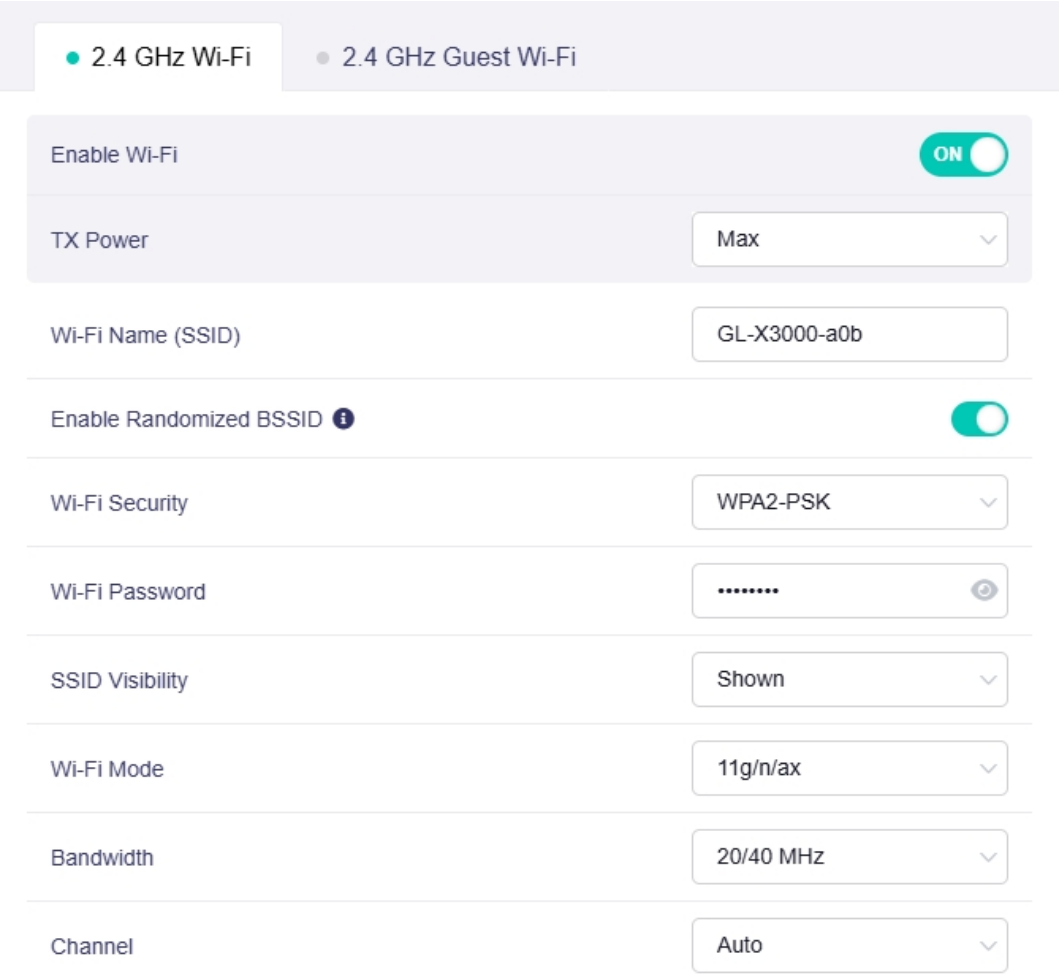
2. Ustawień **Bandwidth** i **Channel** nie można zmieniać, gdy router działa jako wzmacniacz sygnału, ponieważ są one przejmowane z sieci, której sygnał jest wzmacniany.
3. Gdy opcja **Channel** jest ustawiona na **Auto**, sieć Wi-Fi routera nie przełącza się automatycznie na kanał DFS.
4. Gdy parametr **Bandwidth** jest ustawiony na **160 MHz** (opcja dostępna tylko w niektórych modelach), sieć Wi-Fi zawsze korzysta z kanału DFS, nawet jeśli wybierzesz kanał bez DFS lub ustawienie Auto.

W gościnnej sieci Wi-Fi 5 GHz dostępny jest uproszczony zestaw ustawień: włączanie i wyłączanie Wi-Fi, nazwa sieci Wi-Fi (SSID), zabezpieczenia, hasło i widoczność SSID.



5.2.2 Wi-Fi 2,4 GHz

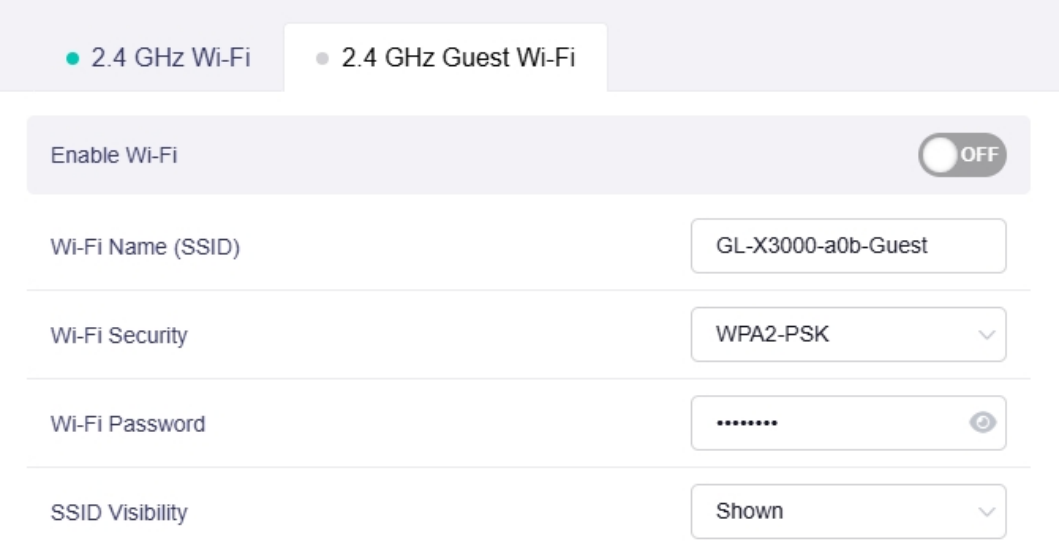
W głównej sieci Wi-Fi 2,4 GHz można skonfigurować wiele ustawień: włączanie i wyłączanie Wi-Fi, moc nadawania, włączanie i wyłączanie losowego BSSID, nazwę sieci Wi-Fi (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.



Uwaga:

1. **Randomized BSSID** jest domyślnie włączone. Pomaga zapobiegać śledzeniu routera za pomocą stałego BSSID, ponieważ urządzenia klienckie mogą przesyłać pobliskie identyfikatory BSSID i własne dane lokalizacyjne producentom systemów operacyjnych lub urządzeń, którzy tworzą z nich bazę powiązań BSSID z lokalizacją. Po włączeniu tej opcji router używa losowo generowanego BSSID i odnawia go przy każdym uruchomieniu, dzięki czemu nie można powiązać BSSID ze stałą lokalizacją.
2. Ustawień **Bandwidth** i **Channel** nie można zmieniać, gdy router działa jako wzmacniacz sygnału, ponieważ są one przejmowane z sieci, której sygnał jest wzmacniany.

W gościnnej sieci Wi-Fi 2,4 GHz dostępny jest uproszczony zestaw ustawień: włączanie i wyłączanie Wi-Fi, nazwa sieci Wi-Fi (SSID), zabezpieczenia, hasło i widoczność SSID.



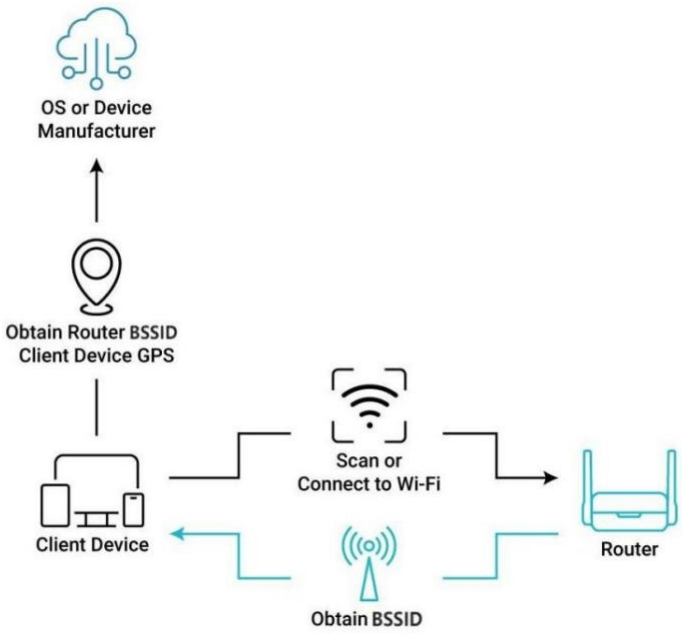
5.2.3 Losowy BSSID

Losowy BSSID to funkcja ochrony prywatności dostępna od wersji oprogramowania 4.6 i domyślnie włączona. Zapobiega ustalaniu lokalizacji i śledzeniu routera za pomocą stałego BSSID sieci Wi-Fi (adresu MAC interfejsu bezprzewodowego routera).

Dlaczego stały BSSID zagraża prywatności?

Mobilne systemy operacyjne (np. Android i iOS) korzystają ze zbiorowo gromadzonych danych o położeniu sieci Wi-Fi, aby świadczyć usługi lokalizacyjne:

1. Urządzenia klienckie (telefony, laptopy) okresowo przesyłają widoczne dla nich identyfikatory BSSID wraz z własną lokalizacją uzyskaną z GPS na serwer producenta systemu operacyjnego lub urządzenia.
2. Producenci łączą te dane w globalną bazę powiązań BSSID z lokalizacją.
3. Każde urządzenie z włączonym Wi-Fi, nawet bez GPS, może wysłać zapytanie do tej bazy, aby oszacować swoje położenie na podstawie pobliskich identyfikatorów BSSID.
4. W efekcie router ze stałym BSSID działa jak nieruchomy znacznik lokalizacji: można zdalnie ustalić jego położenie i z czasem śledzić jego przemieszczanie (np. podczas podróży). Atakujący również mogą korzystać z takich baz, aby lokalizować routery lub je identyfikować na podstawie informacji o producencie zawartej w BSSID (OUI).



Jak losowy BSSID chroni Twoją prywatność

Po włączeniu tej funkcji router generuje losowy BSSID i odnawia go przy każdym uruchomieniu. Ponieważ BSSID stale się zmienia, nie można już powiązać go ze stałą lokalizacją w bazach producentów, co zrywa używane do śledzenia powiązanie BSSID z lokalizacją.

Stan	Działanie
Włączone (domyślnie)	Przy każdym uruchomieniu generowany i odnawiany jest losowy BSSID
Wyłączone	Router używa swojego rzeczywistego fabrycznego adresu MAC jako BSSID

Uwagi:

1. BSSID zmienia się tylko po ponownym uruchomieniu routera; podczas jego pracy pozostaje taki sam.
2. W gościnnej sieci Wi-Fi BSSID pozostaje zgodny z BSSID głównej sieci Wi-Fi w tym samym paśmie częstotliwości.
3. Losowy BSSID blokuje śledzenie za pomocą BSSID routera, ale nie zapobiega przesyłaniu przez urządzenia klienckie własnej lokalizacji i nie zapewnia pełnej ochrony prywatności: nadal można obserwować SSID, kanał oraz charakterystykę sygnału.

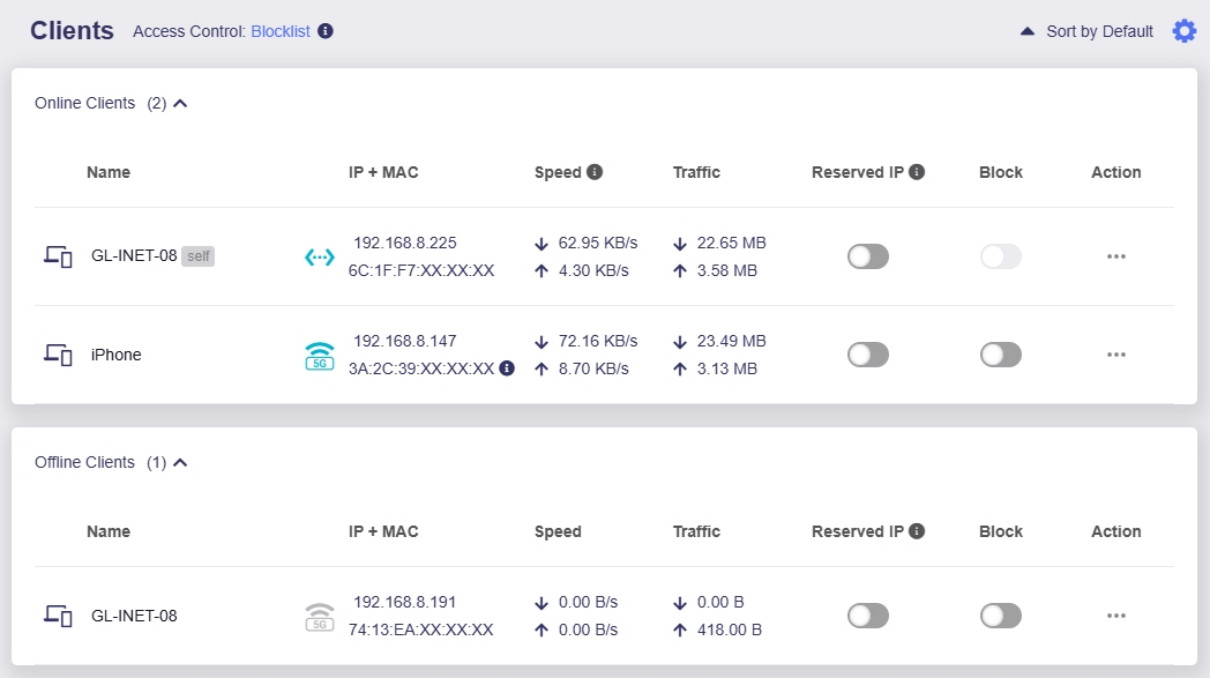
Rozdział 6

Urządzenia klienckie

W tym rozdziale opisano wyświetlanie szczegółów podłączonych urządzeń i zarządzanie ich połączeniami.

6.1 Szczegóły urządzenia

Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **CLIENTS**. Strona urządzeń klienckich przedstawia informacje o podłączonych urządzeniach, kolejno od lewej: nazwę urządzenia, rodzaj połączenia, adres IP i MAC, prędkość oraz transfer danych. Umożliwia też szybkie rezerwowanie adresu IP, blokowanie klienta i wykonywanie innych działań.



Wskazówka: Online Clients oznacza urządzenia obecnie połączone z siecią routera. Offline Clients oznacza urządzenia, które wcześniej łączyły się z routerem, ale obecnie są odłączone od sieci.

1. **Nazwa urządzenia**

   Pierwsza kolumna zawiera nazwę i typ urządzenia, zależne od nazwy hosta ustawionej przez jego użytkownika. Niebieska ikona obok nazwy oznacza sposób połączenia i wskazuje, że urządzenie jest podłączone do routera kablem Ethernet.

2. **Adres IP i MAC**

   Druga kolumna zawiera adresy IP i MAC podłączonego urządzenia. Jeśli podłączone urządzenie używa losowego adresu MAC, pojawi się odpowiedni komunikat.



Jeśli drugim znakiem adresu MAC jest 2, 6, A lub E (bez rozróżniania wielkości liter), adres jest uznawany za losowy. Niektóre urządzenia mogą jednak generować losowe adresy MAC według innej reguły, dlatego ten sposób wykrywania nie zawsze jest dokładny.

3. **Prędkość**

   Trzecia kolumna przedstawia prędkość połączenia internetowego podłączonego urządzenia. Jest to średnia z ostatnich 3 minut. System zaczyna obliczać średnią po otwarciu tej strony (np. jeśli strona jest otwarta od 10 sekund, średnia będzie oparta tylko na danych z tych 10 sekund).

4. **Transfer danych**: czwarta kolumna przedstawia transfer internetowy podłączonego urządzenia.

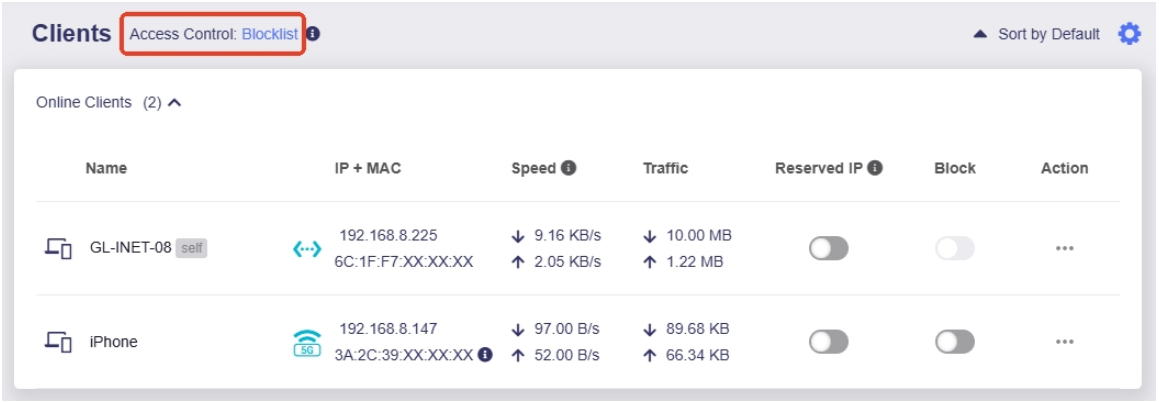
5. **Rezerwacja adresu IP**

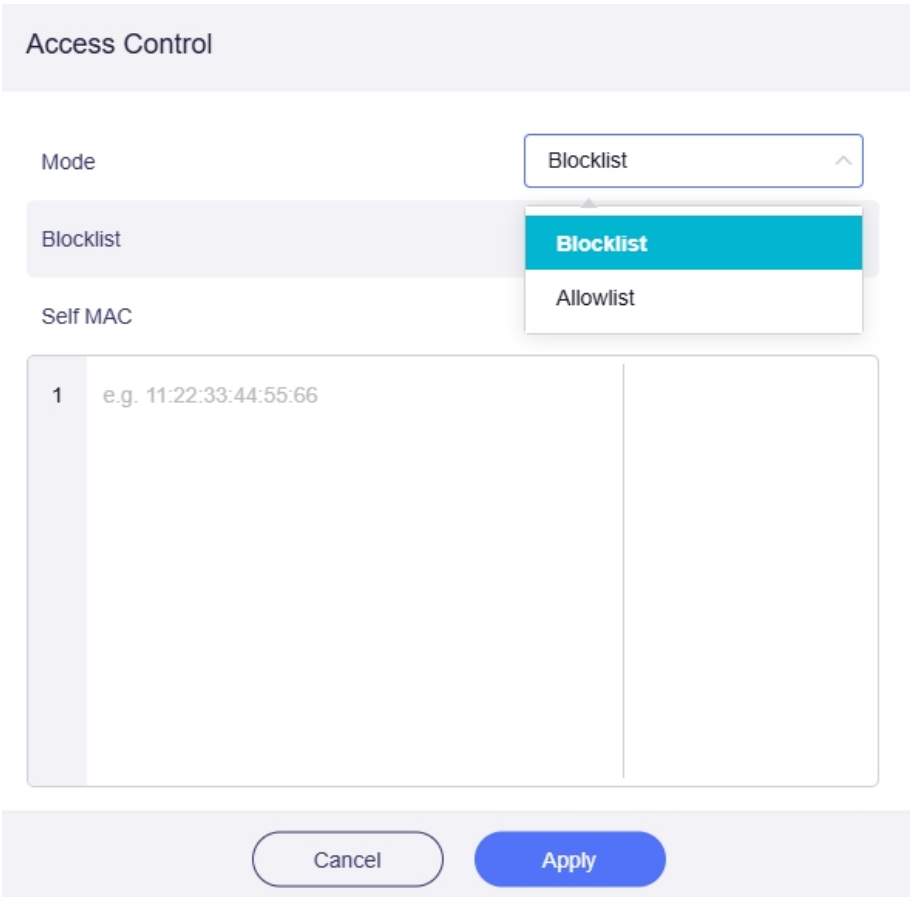
   W piątej kolumnie możesz jednym kliknięciem zarezerwować adres IP dla podłączonego urządzenia. Po przypisaniu klientowi w sieci lokalnej zarezerwowanego adresu IP będzie on otrzymywał ten sam adres przy każdym połączeniu z routerem.

6. **Lista blokowanych urządzeń**

   W szóstej kolumnie możesz jednym kliknięciem zablokować wybrane podłączone urządzenia.

   Domyślną regułą kontroli dostępu jest Blocklist. W razie potrzeby możesz przełączyć ją u góry na Allowlist.



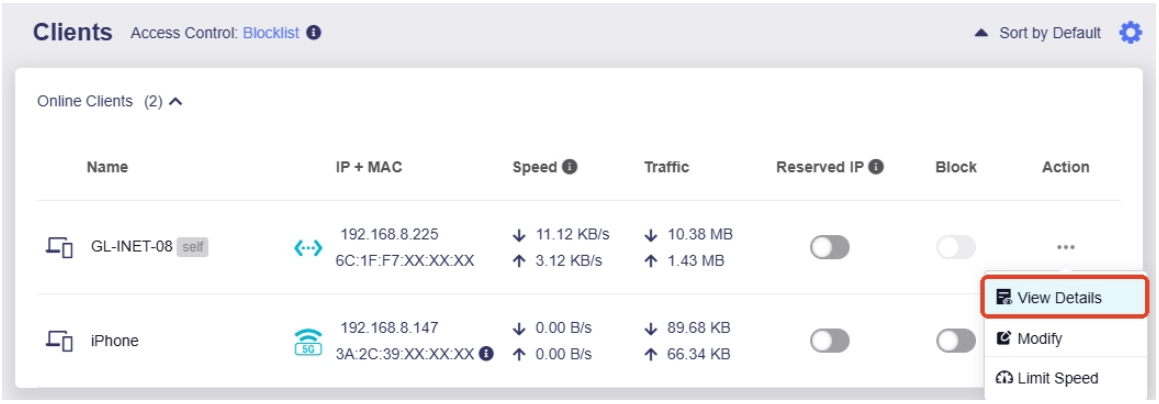


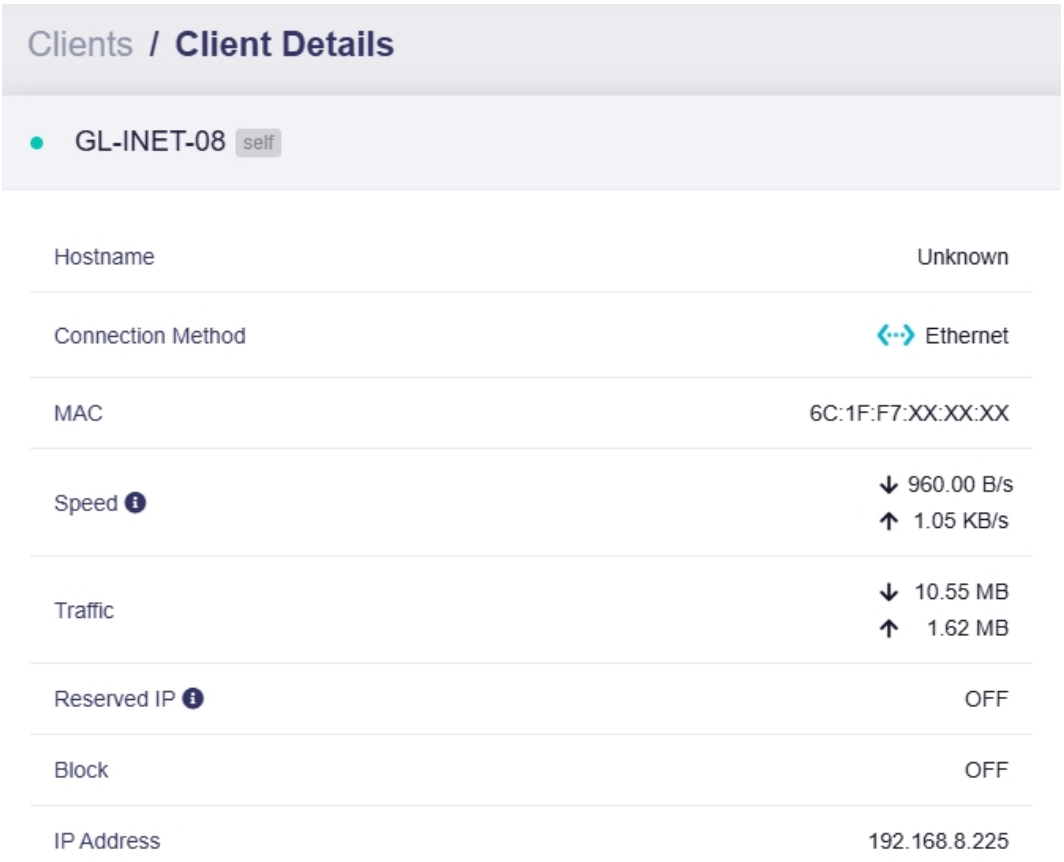
- **Blacklist**: urządzenia o adresach MAC znajdujących się na liście blokowanych nie mogą łączyć się z tym routerem. Blokowanie klienta opiera się na adresie MAC urządzenia. Jeśli zablokowane urządzenie następnym razem użyje innego adresu MAC, nadal będzie mogło połączyć się z routerem.
- **Allowlist**: z routerem mogą łączyć się tylko urządzenia o określonych adresach MAC. Ta opcja jest przydatna dla urządzeń IoT i przy zarządzaniu siecią firmową.

6.2 Działania

1. **Wyświetlanie szczegółów**

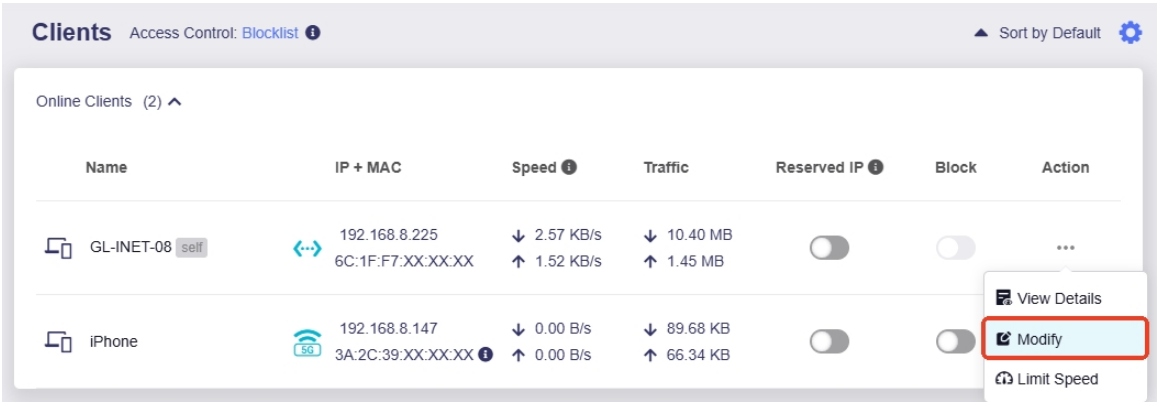
   Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **View Details** z menu, aby wyświetlić szczegóły urządzenia na jednej stronie.

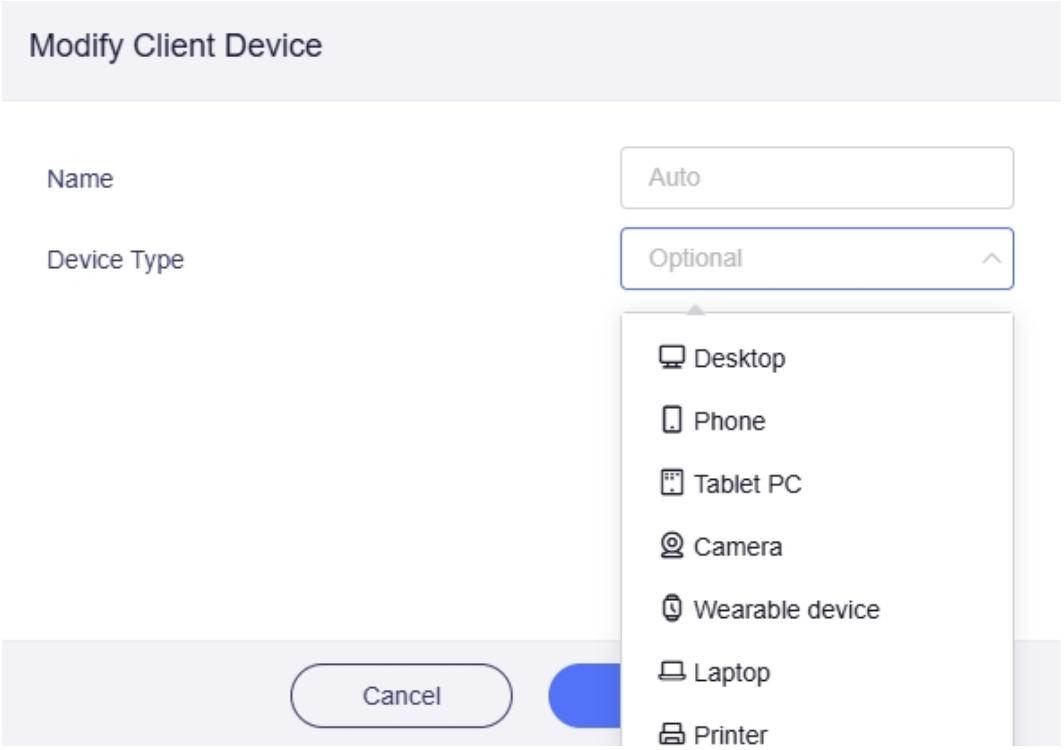




2. **Modyfikowanie**

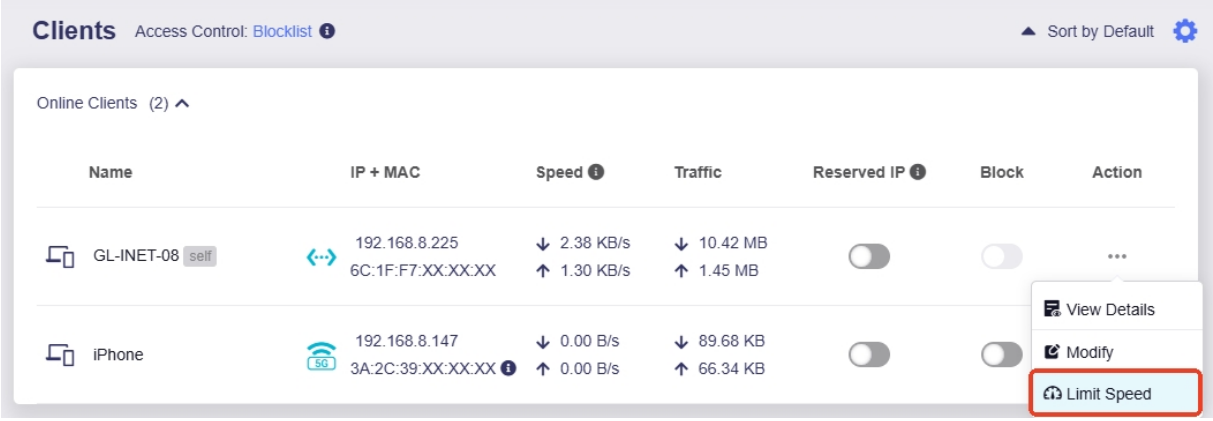
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Modify** z menu, aby zmienić nazwę i typ urządzenia.



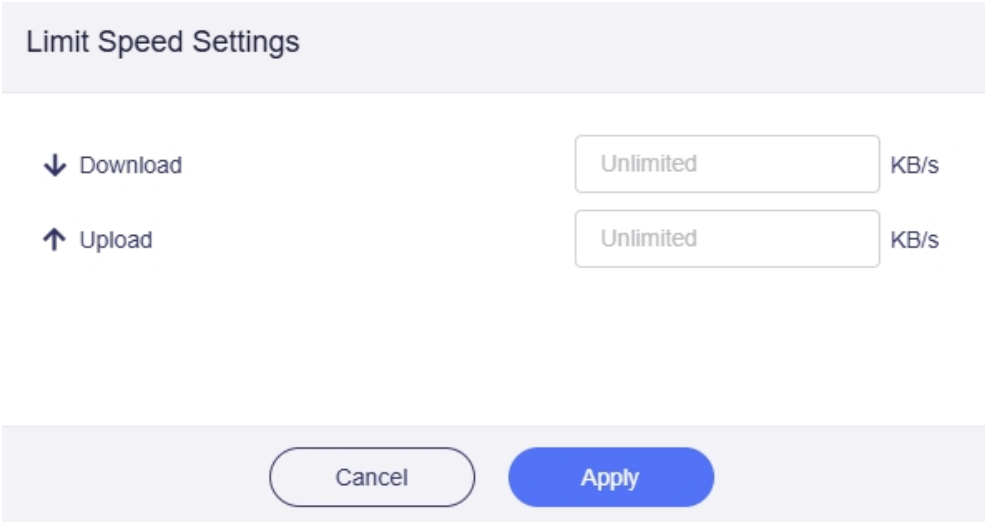


3. **Ograniczanie prędkości**

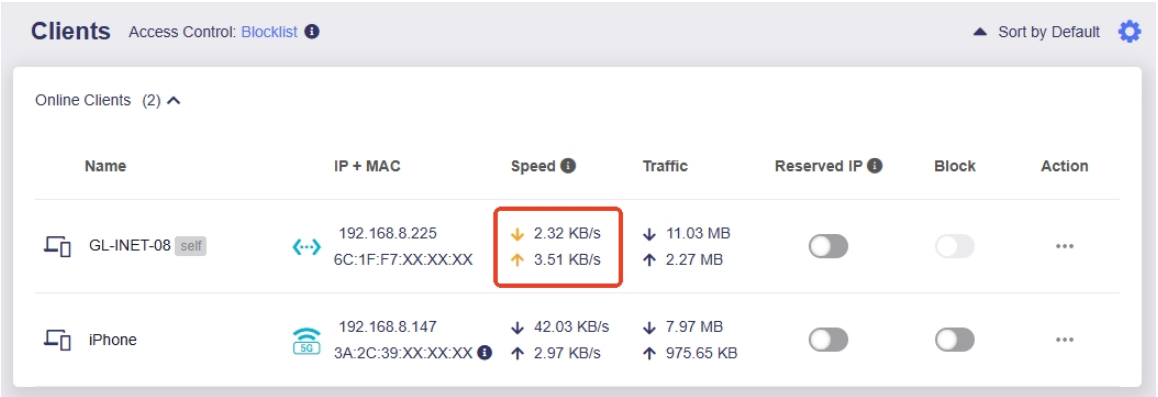
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Limit Speed** z menu.



Możesz ograniczyć prędkość podłączonego urządzenia, podając wartość w KB/s.

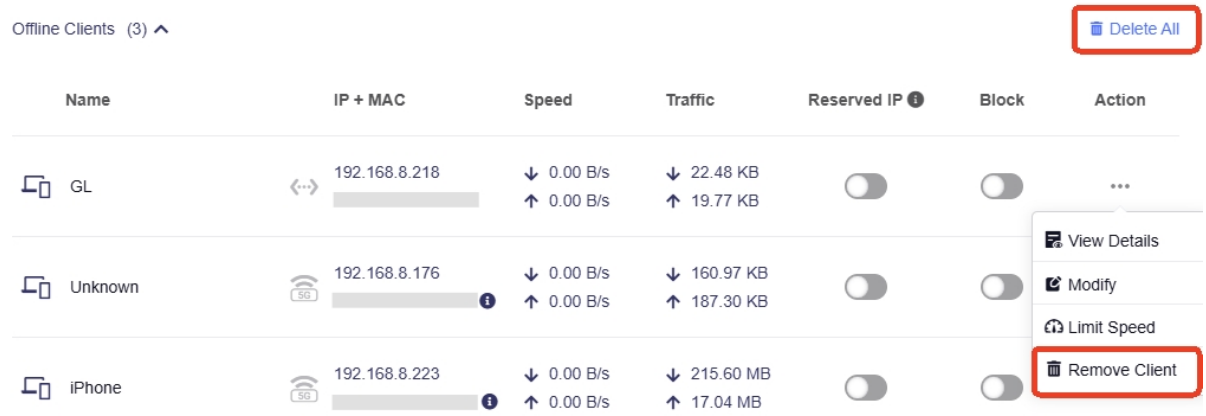


Jeśli dla urządzenia ustawiono ograniczenie prędkości, strzałki prędkości wysyłania i pobierania zmienią kolor na żółty.



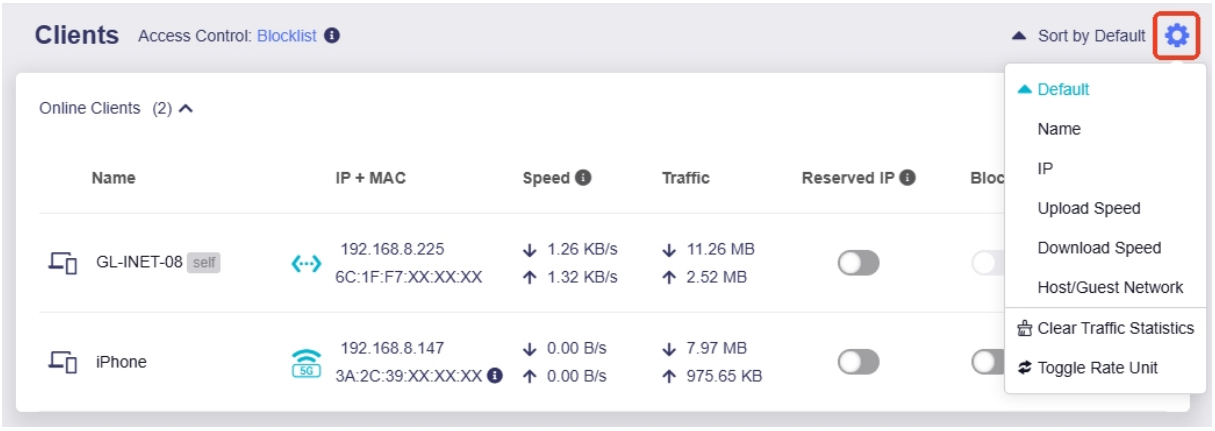
6.3 Usuwanie urządzeń klienckich

W sekcji **Offline Clients** kliknij **Delete All** w prawym górnym rogu, aby usunąć wszystkie urządzenia offline. Aby usunąć wybrane urządzenie, kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Remove Client** z menu.



6.4 Sortowanie

Regułę sortowania urządzeń na stronie klientów możesz ustawić w prawym górnym rogu.



Domyślne reguły sortowania są następujące:

- Urządzenie, z którego korzystasz do otwierania panelu administracyjnego routera, jest zawsze wyświetlane jako pierwsze.
- W sekcji **Online Clients** urządzenia, które połączyły się wcześniej, są wyświetlane wyżej.
- W sekcji **Offline Clients** urządzenia, które rozłączyły się wcześniej, są wyświetlane wyżej.

Rozdział 7

Usługi w chmurze

W tym rozdziale przedstawiono dwie usługi w chmurze: GoodCloud i AstroWarp.

7.1 GoodCloud

GL.iNet GoodCloud to platforma ułatwiająca zdalne wdrażanie podłączonych urządzeń i zarządzanie nimi. Zapewnia prosty sposób zdalnego dostępu do routerów GL.iNet oraz ich obsługi. Centralizacja urządzeń sieciowych w chmurze pozwala sprawnie wykonywać działania zbiorcze, takie jak wdrażanie konfiguracji sieciowych i aktualizowanie oprogramowania. Użytkownicy mogą też zdalnie otwierać panel administracyjny routera lub łączyć się z jego terminalem przez SSH, zarządzając urządzeniami sieciowymi w różnych regionach od końca do końca.

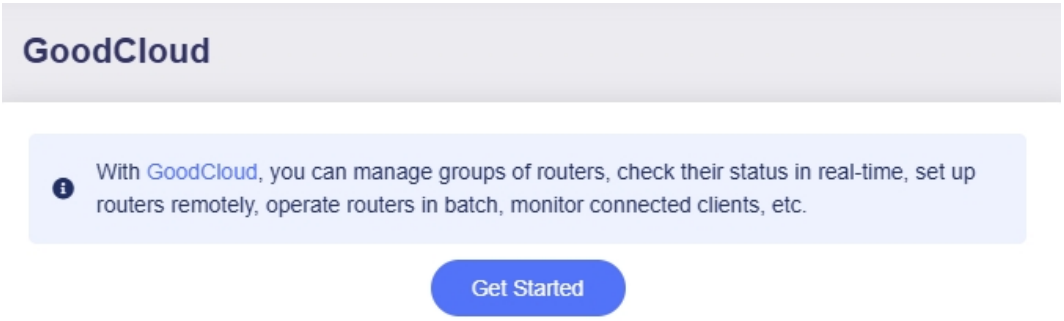
Dzięki GoodCloud możesz:

- Sprawdzać stan routera w czasie rzeczywistym
- Zarządzać grupami routerów
- Zdalnie konfigurować routery
- Monitorować podłączone urządzenia klienckie
- Wykonywać działania zbiorcze na routerach
- Tworzyć połączenia sieć–sieć

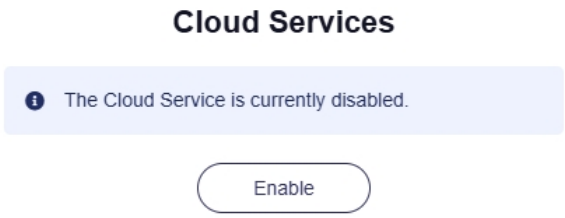
Niektóre funkcje są dostępne w planach Enterprise i VAR (Value Added Reseller). Szczegóły znajdziesz tutaj.

7.1.1 Włączanie GoodCloud

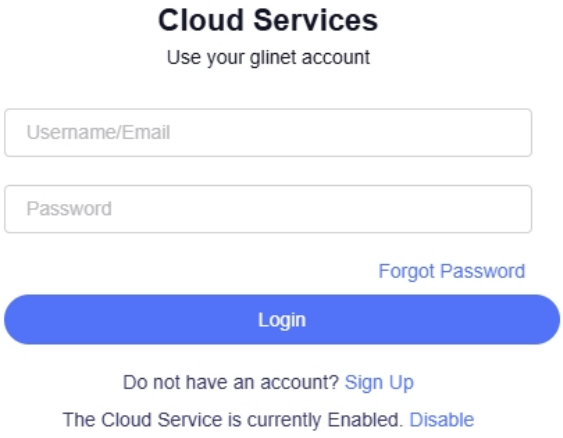
1. Zaloguj się do internetowego panelu administracyjnego routera, przejdź do **CLOUD SERVICE** > **GoodCloud** i kliknij **Get Started**.



2. W prawym górnym rogu pojawi się rozwijane okno. Kliknij **Enable**.



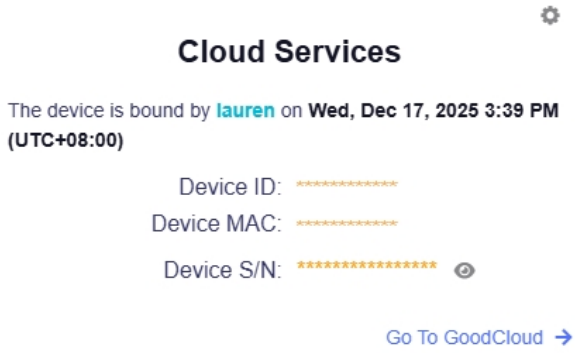
3. Zaloguj się na konto GL.iNet Cloud. Jeśli nie masz konta, zarejestruj je i zaloguj się. Po zalogowaniu router zostanie automatycznie powiązany z kontem.



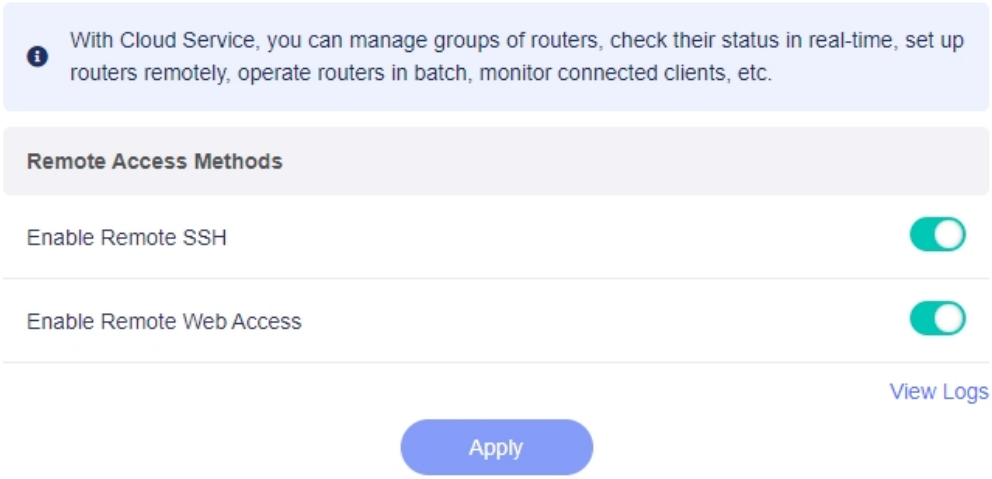
Wskazówki:

- Sposób powiązania z GoodCloud zależy od wersji oprogramowania.
- Jeśli nie otrzymasz wiadomości weryfikacyjnej, sprawdź folder spamu lub spróbuj później. Aby uzyskać dodatkową pomoc, napisz na support@gl-inet.com.

4. Po pomyślnym powiązaniu kliknij **ikonę chmury** w prawym górnym rogu panelu administracyjnego. Wyświetlą się szczegóły powiązanego urządzenia: powiązane konto, data powiązania, Device ID, Device MAC i Device S/N.



5. Przejdź do **CLOUD SERVICES** > **GoodCloud** i włącz dostęp zdalny. GoodCloud umożliwia zdalny dostęp do internetowego panelu administracyjnego i terminala powiązanego routera. Tutaj możesz włączyć lub wyłączyć zdalny dostęp do routera.

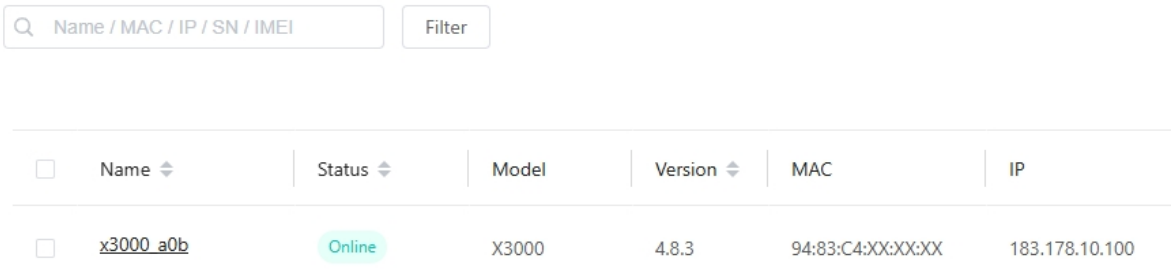


- **Remote SSH:** zdalny dostęp do terminala routera z GoodCloud przez SSH.
- **Remote Web Access:** zdalny dostęp do internetowego panelu administracyjnego routera z GoodCloud przez HTTP/HTTPS.
- **View Logs:** przejście do strony dziennika i wyświetlenie dziennika chmury.

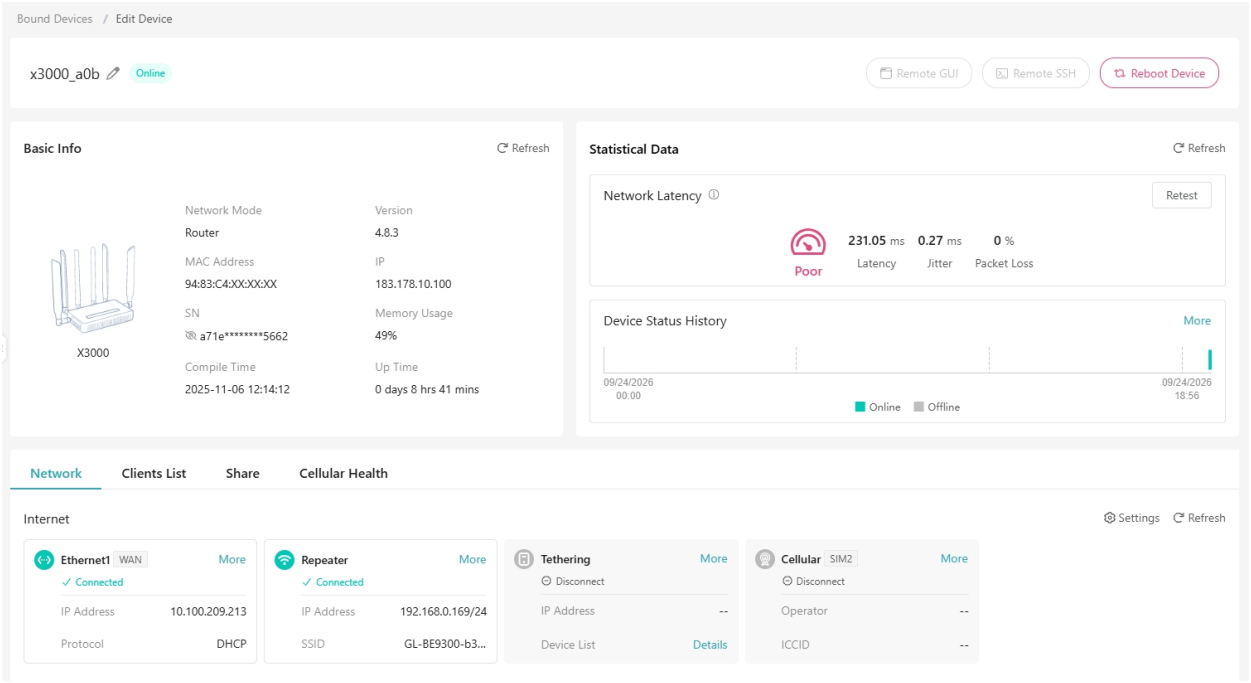
7.1.2 Zarządzanie routerem

7.1.2.1 Sprawdzanie szczegółów urządzenia

Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Możesz sprawdzić podstawowe informacje o urządzeniu: nazwę hosta, stan (online/offline), model, wersję oprogramowania i adres MAC.

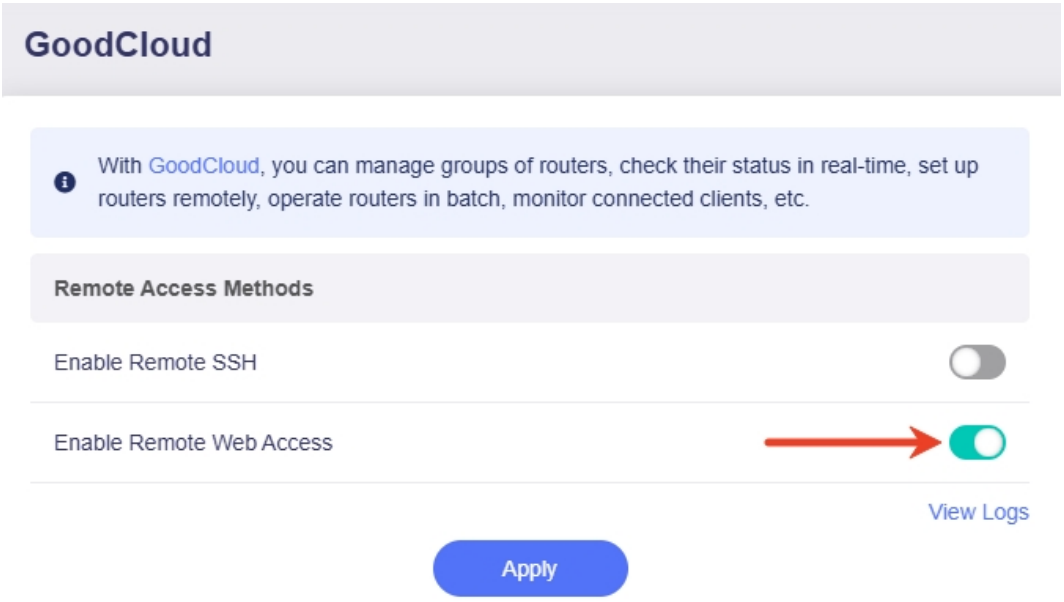


Kliknij nazwę urządzenia, aby otworzyć stronę szczegółów zawierającą podstawowe informacje, statystyki, przegląd sieci, listę klientów i oś czasu. Możesz też wykonywać zaawansowane działania, np. zdalnie uzyskiwać dostęp do routera i uruchamiać go ponownie.

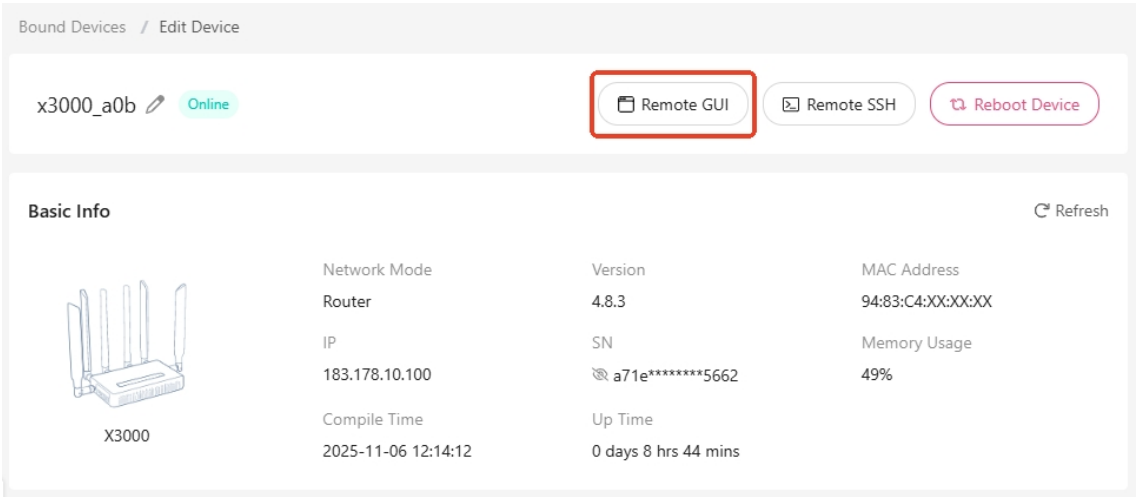


7.1.2.2 Zdalny dostęp przez przeglądarkę

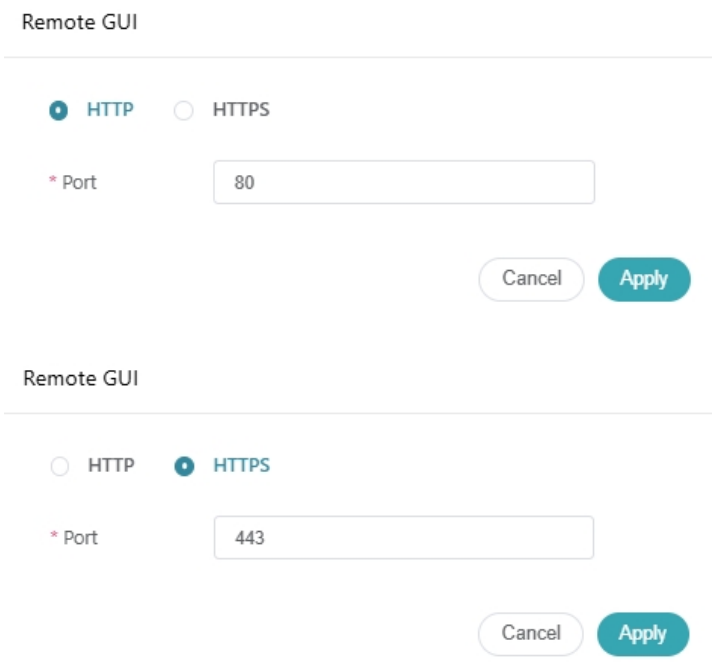
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICES** > **GoodCloud**, włącz **Remote Web Access**, a następnie kliknij **Apply**.



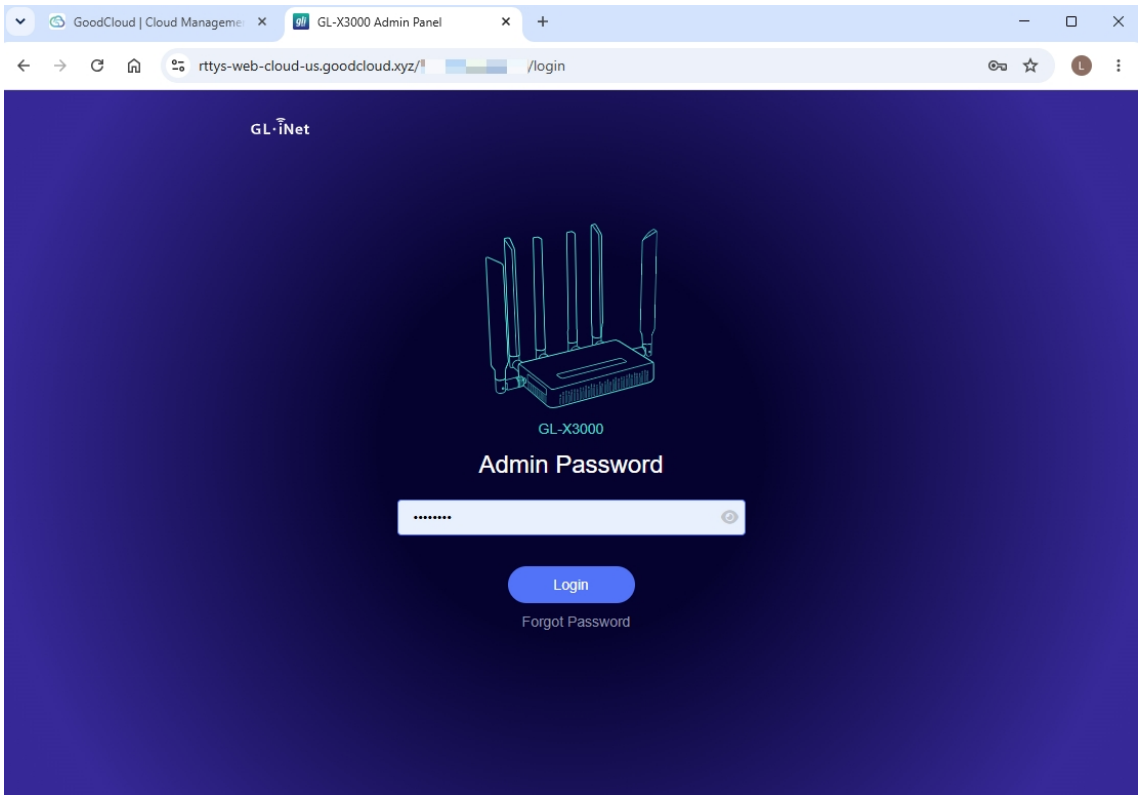
2. Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote GUI** w prawym górnym rogu.



4. Wybierz protokół transmisji i port. Domyślne wartości to **HTTP** i port **80**. W razie potrzeby możesz wybrać HTTPS; port automatycznie zmieni się na 443. Następnie kliknij **Apply**.

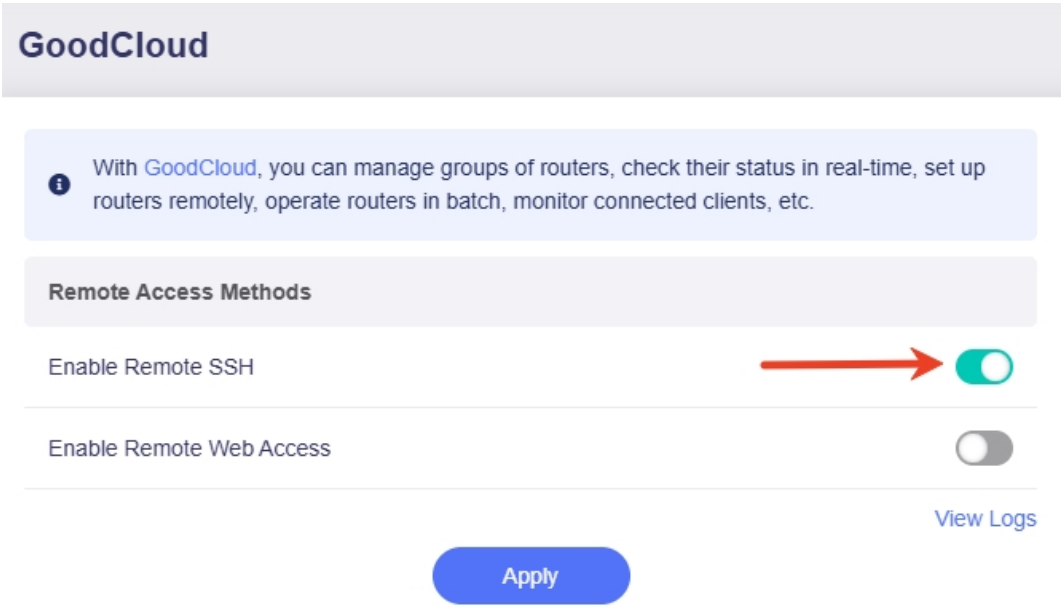


5. Otworzy się strona logowania routera. Wprowadź hasło administratora, aby uzyskać zdalny dostęp do panelu administracyjnego routera.

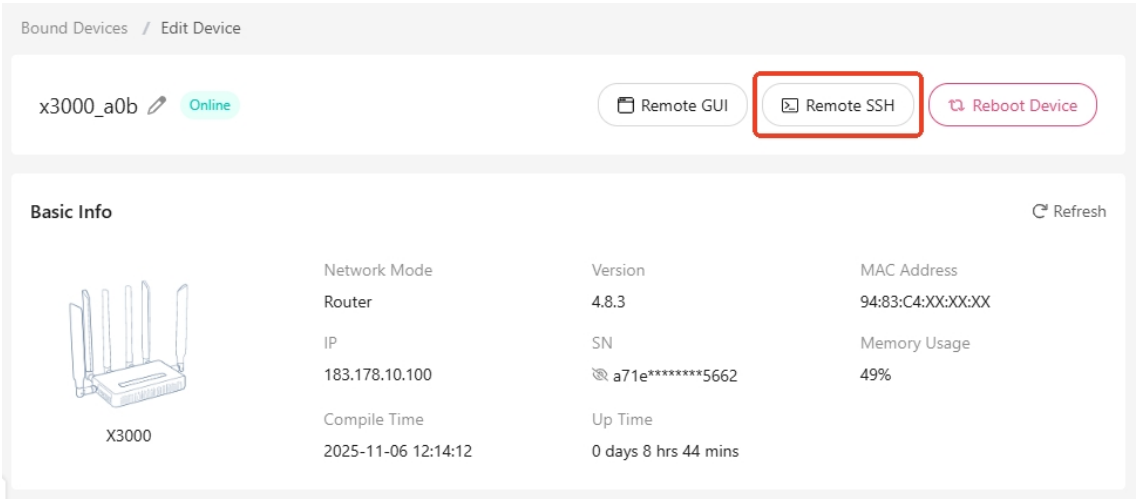


7.1.2.3 Zdalny dostęp przez SSH

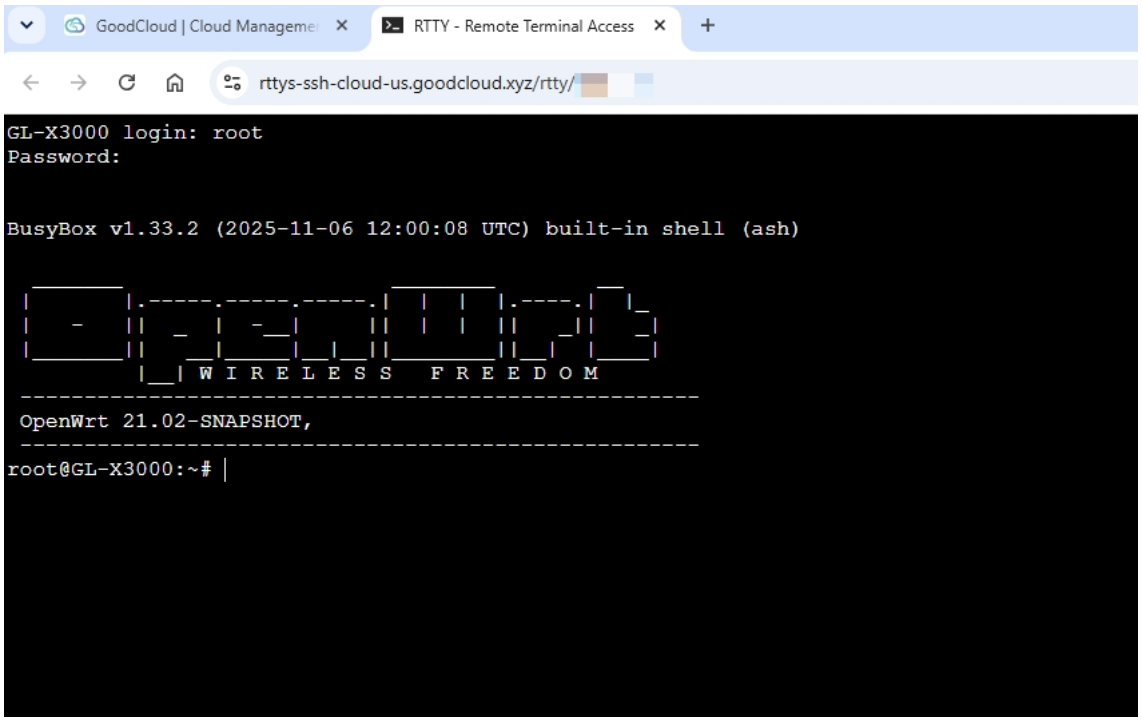
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICES** > **GoodCloud**, włącz **Remote SSH**, a następnie kliknij **Apply**.



2. Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote SSH** w prawym górnym rogu.

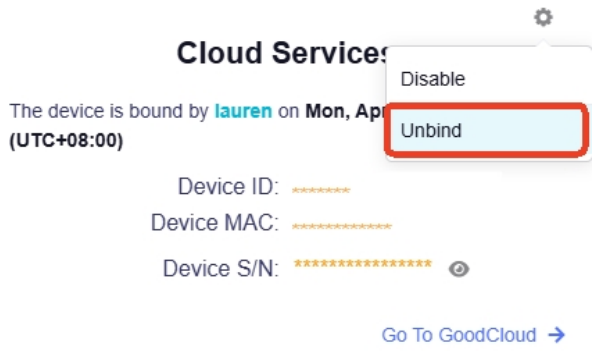


4. Zaloguj się jako **root** i wprowadź hasło, aby uzyskać dostęp do terminala routera.

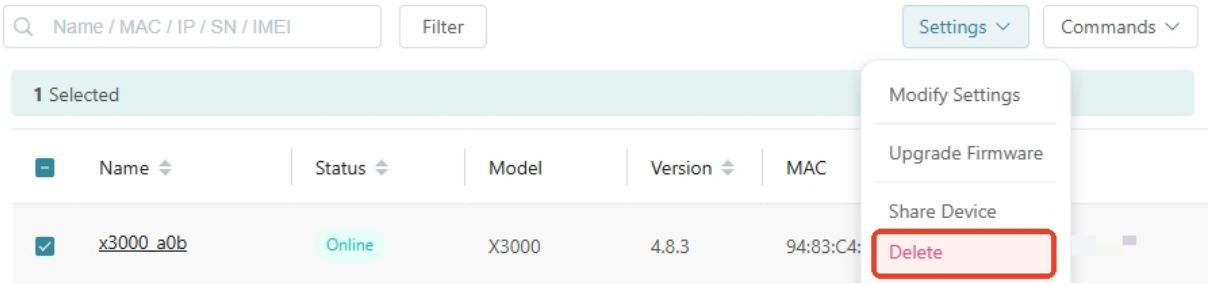

GoodCloud | Cloud Manageme
RTTY - Remote Terminal Access
rttys-ssh-cloud-us.goodcloud.xyz/rtty/
GL-X3000 login: root
Password:
BusyBox v1.33.2 (2025-11-06 12:00:08 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-X3000:~#

7.1.3 Usuwanie powiązania urządzenia

W panelu administracyjnym routera kliknij ikonę chmury w prawym górnym rogu. W rozwijanym menu kliknij ikonę koła zębatego i wybierz **Unbind**. Urządzenie zostanie odłączone od konta GoodCloud.

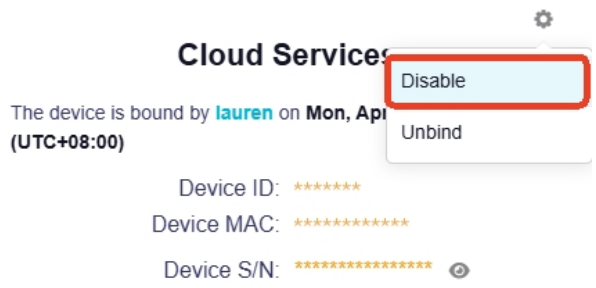


Możesz też zalogować się na platformie chmurowej i przejść do **Device** > **Bound Devices**. Wybierz urządzenie do odłączenia, kliknij **Settings** w prawym górnym rogu, a następnie wybierz **Delete**. Urządzenie zostanie odłączone od konta GoodCloud.



7.1.4 Wyłączanie GoodCloud

Jeśli nie chcesz już łączyć urządzenia z chmurą, kliknij ikonę chmury w prawym górnym rogu. W rozwijanym menu kliknij ikonę koła zębatego i wybierz **Disable**.

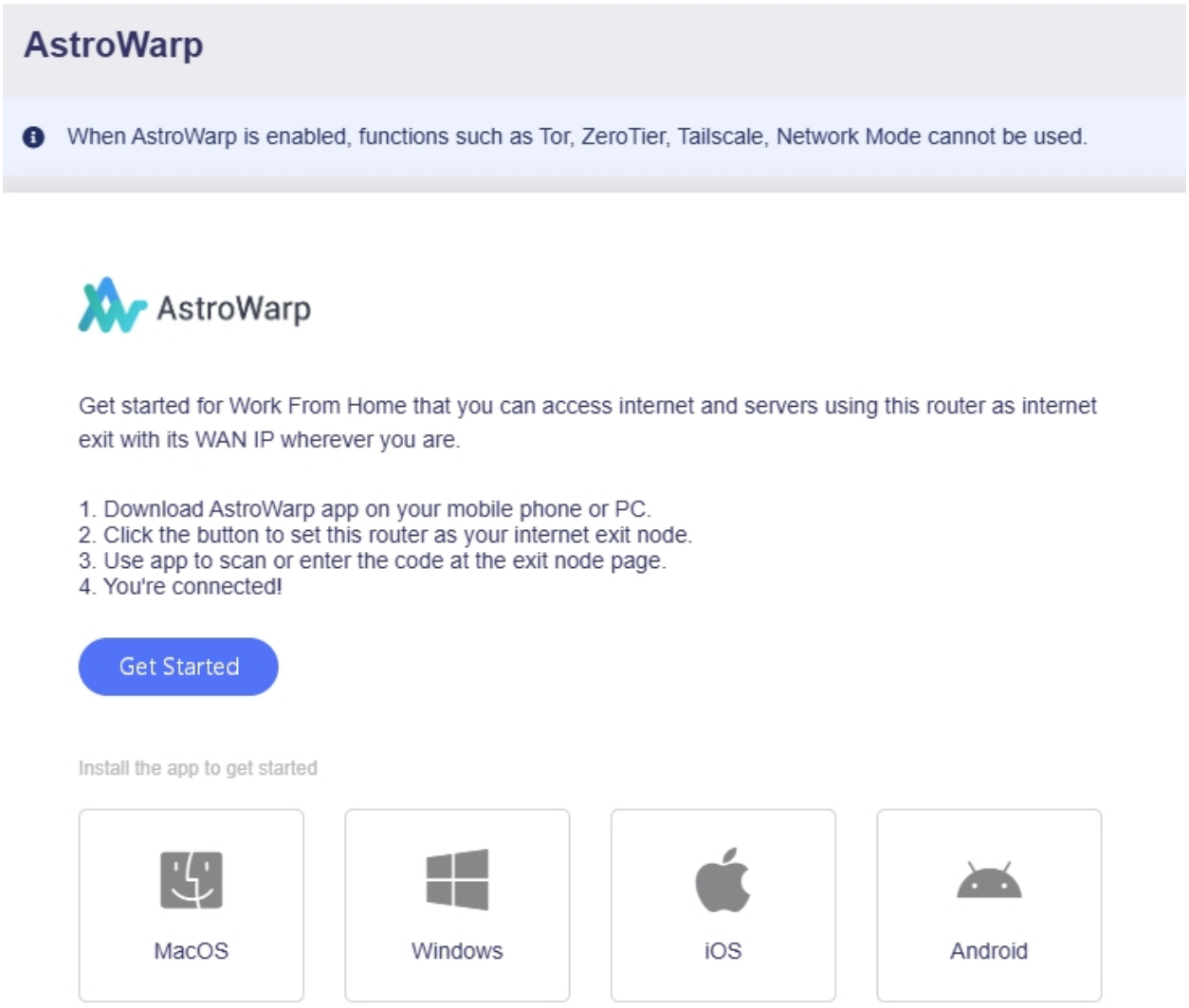


Usługa chmurowa zostanie wyłączona.

7.2 AstroWarp

AstroWarp to zaawansowana platforma sieciowa umożliwiająca płynne łączenie wielu routerów GL.iNet w jedną sieć i łatwy dostęp zdalny. Dzięki elastycznym możliwościom sieciowym, prostej konfiguracji i skutecznej ochronie prywatności AstroWarp zapewnia bezpieczną i niezawodną łączność przez cały czas. Niezależnie od tego, czy pracujesz zdalnie, czy potrzebujesz bezpiecznego dostępu do wewnętrznych zasobów firmy w wielu lokalizacjach, AstroWarp zapewnia wydajną i chronioną sieć.

Zaloguj się do internetowego panelu administracyjnego routera, przejdź do **CLOUD SERVICE** > **AstroWarp** i kliknij **Get Started**. Następnie postępuj zgodnie z instrukcjami konfiguracji sieci. Szczegóły znajdziesz na stronie astrowarp.net.



Rozdział 8

Poznaj VPN

W tym rozdziale przedstawiono pojęcia związane z VPN i typowe zastosowania.

8.1 Wprowadzenie

8.1.1 VPN

VPN, czyli wirtualna sieć prywatna (Virtual Private Network), tworzy zaszyfrowany, prywatny tunel między urządzeniem a zdalnym serwerem, chroniąc transmisję danych i umożliwiając bezpieczny dostęp do sieci prywatnych lub o ograniczonym dostępie.

8.1.2 Router VPN

Router VPN ma fabrycznie zainstalowane funkcje VPN, które chronią wszystkie podłączone urządzenia. Skonfigurowanie routera jako klienta VPN kieruje cały ruch przez zaszyfrowany tunel i nie wymaga oddzielnej konfiguracji na każdym urządzeniu. Chroni to jednocześnie wiele urządzeń, oszczędza czas i zapewnia spójne ustawienia VPN, ograniczając ryzyko wynikające z nieprawidłowej konfiguracji poszczególnych urządzeń.

Routery GL.iNet obsługują ponad 30 popularnych komercyjnych usług VPN OpenVPN i WireGuard. Prześlij pliki konfiguracyjne VPN, aby uruchomić połączenie VPN i bezpiecznie korzystać z sieci. Pełną listę zewnętrznych dostawców VPN znajdziesz tutaj.

8.1.3 OpenVPN

OpenVPN to protokół VPN o otwartym kodzie źródłowym, wykorzystujący zabezpieczenia SSL/TLS w połączeniach urządzenie–sieć lub sieć–sieć. Obsługuje różne metody szyfrowania, TCP/UDP i ułatwia pokonywanie ograniczeń zapór oraz NAT.

8.1.4 WireGuard

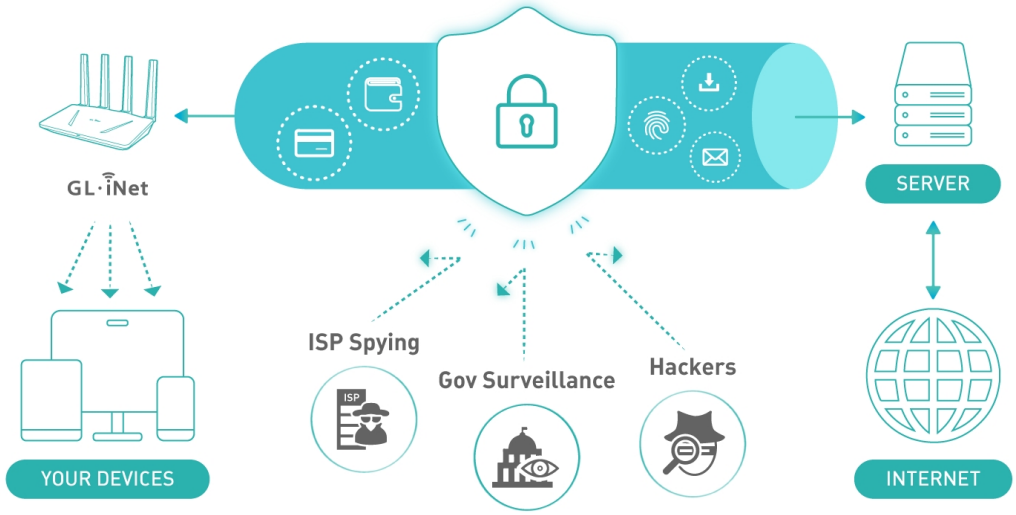
WireGuard® to lekki i szybki protokół VPN, prostszy i wydajniejszy od OpenVPN. Wykorzystuje nowoczesną kryptografię zapewniającą wydajność, niewielką bazę kodu ułatwiającą audyt i bezpieczeństwo oraz zaawansowane algorytmy ChaCha20/Poly1305 do szyfrowania i zapewniania integralności danych.

*WireGuard® jest zastrzeżonym znakiem towarowym Jasona A. Donenfelda.

8.2 Przykłady zastosowań

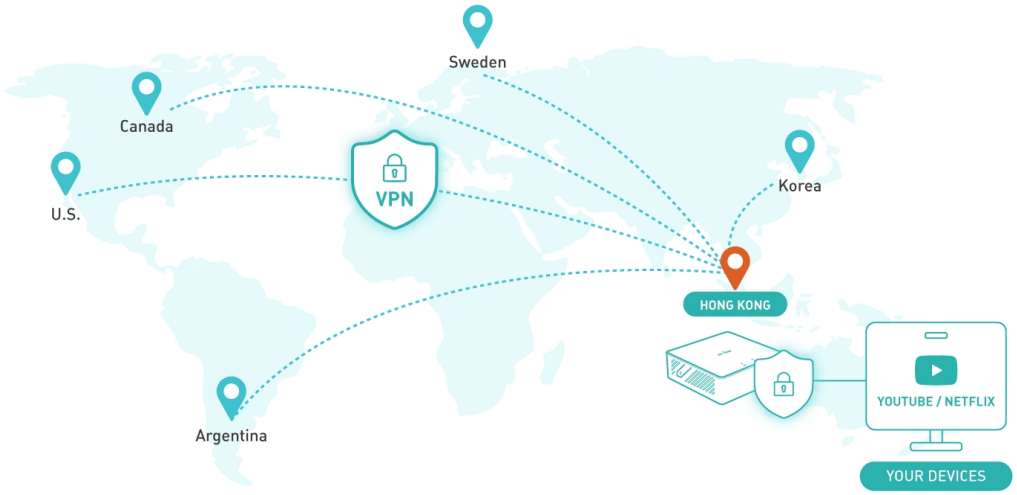
1. **Prywatność danych osobowych**

   Za pośrednictwem naszego routera usługa VPN współpracuje z wieloma urządzeniami: laptopami, telefonami i tabletami, a także konsolami do gier, telewizorami i urządzeniami do strumieniowania. Dane są chronione zarówno przy połączeniu bezprzewodowym, jak i przewodowym. Możesz również dostosować reguły VPN, aby elastycznie chronić wybrane urządzenia.



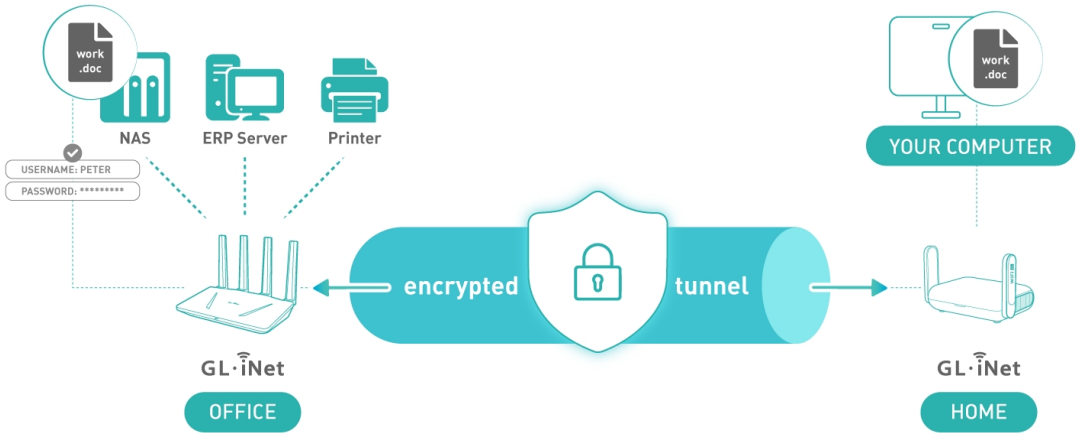
2. **Dostęp bez ograniczeń na całym świecie**

   Dostęp do niektórych witryn może zależeć od lokalizacji. Po włączeniu VPN możesz w razie potrzeby odblokować witryny. Łącząc się z różnymi serwerami zewnętrznymi, otrzymujesz różne adresy IP do przeglądania stron lub uzyskiwania dostępu do witryn objętych blokadą regionalną.


Sweden
Canada
U.S.
VPN
Korea
HONG KONG
Argentina
YOUTUBE / NETFLIX
YOUR DEVICES

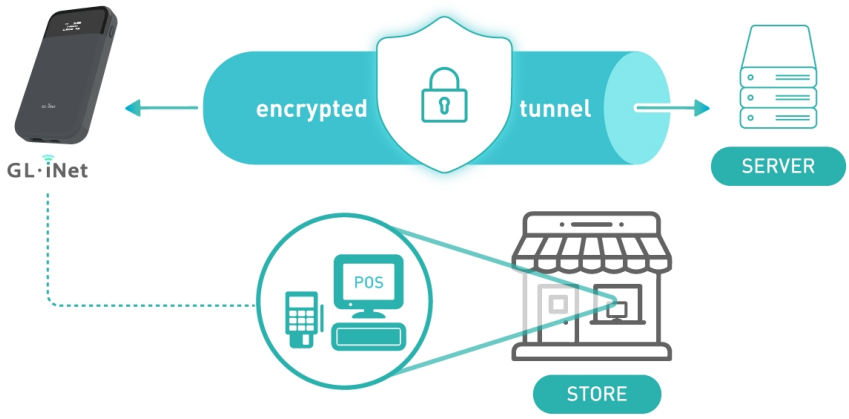
3. **Bezpieczeństwo danych małych firm**

Wiele osób pracuje w przestrzeniach coworkingowych lub kawiarniach, korzystając z bezpłatnego publicznego Wi-Fi. Takie sieci są podatne na ataki cyberprzestępców. Skonfigurowanie routera podróżnego jako klienta VPN pozwala bezpiecznie pracować z dowolnego miejsca.



4. **Bezpieczna infrastruktura płatnicza**

Właściciele małych sklepów przetwarzają dane płatnicze klientów podczas sprzedaży na miejscu. Dzięki routerowi VPN terminale POS mogą przesyłać dane kart kredytowych przez zaszyfrowany tunel VPN, zapewniając bezpieczeństwo płatności.



Rozdział 9

Panel VPN

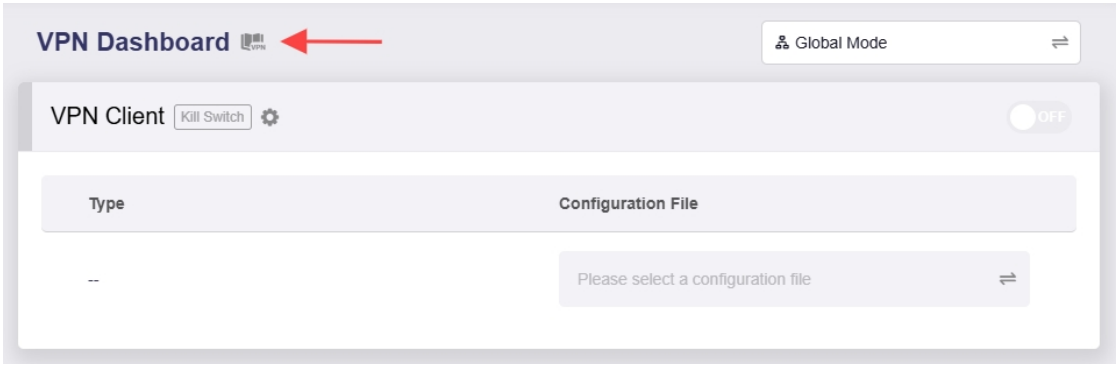
W tym rozdziale opisano zarządzanie połączeniami VPN w panelu administracyjnym.

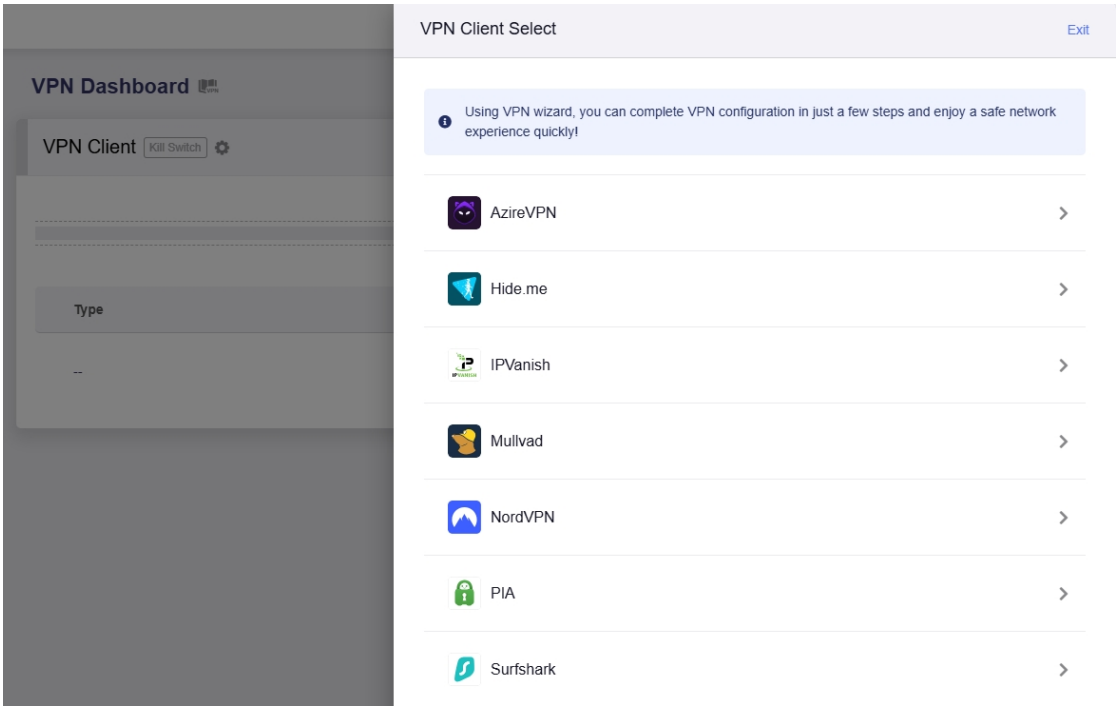
Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **VPN** > **VPN Dashboard**.

Panel VPN wyświetla szczegóły połączenia VPN, takie jak reguły tunelu, adres serwera, statystyki transferu, wirtualny adres IP klienta i dziennik połączenia, oraz umożliwia konfigurację ustawień zaawansowanych, takich jak VPN Kill Switch, IP Masquerading i MTU. Możesz też włączyć wiele połączeń VPN w konfiguracjach z wieloma tunelami.

9.1 Kreator konfiguracji VPN

Aby rozpocząć, kliknij ikonę książki w lewym górnym rogu i skorzystaj z kreatora konfiguracji VPN, aby szybko skonfigurować VPN.



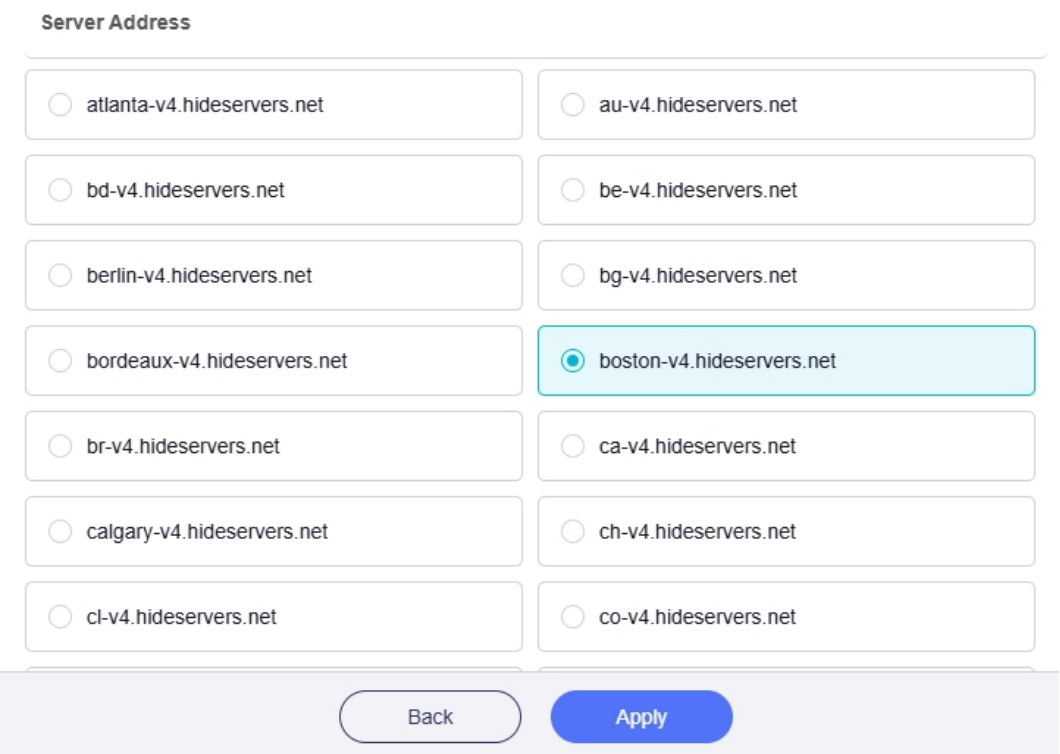


Uwaga: kreator konfiguracji VPN jest przeznaczony wyłącznie do zintegrowanych usług VPN, takich jak AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA i Surfshark. W przypadku innych dostawców pomiń kreator i przejdź do **VPN** > **OpenVPN Client** lub **WireGuard Client**, aby ręcznie skonfigurować VPN.

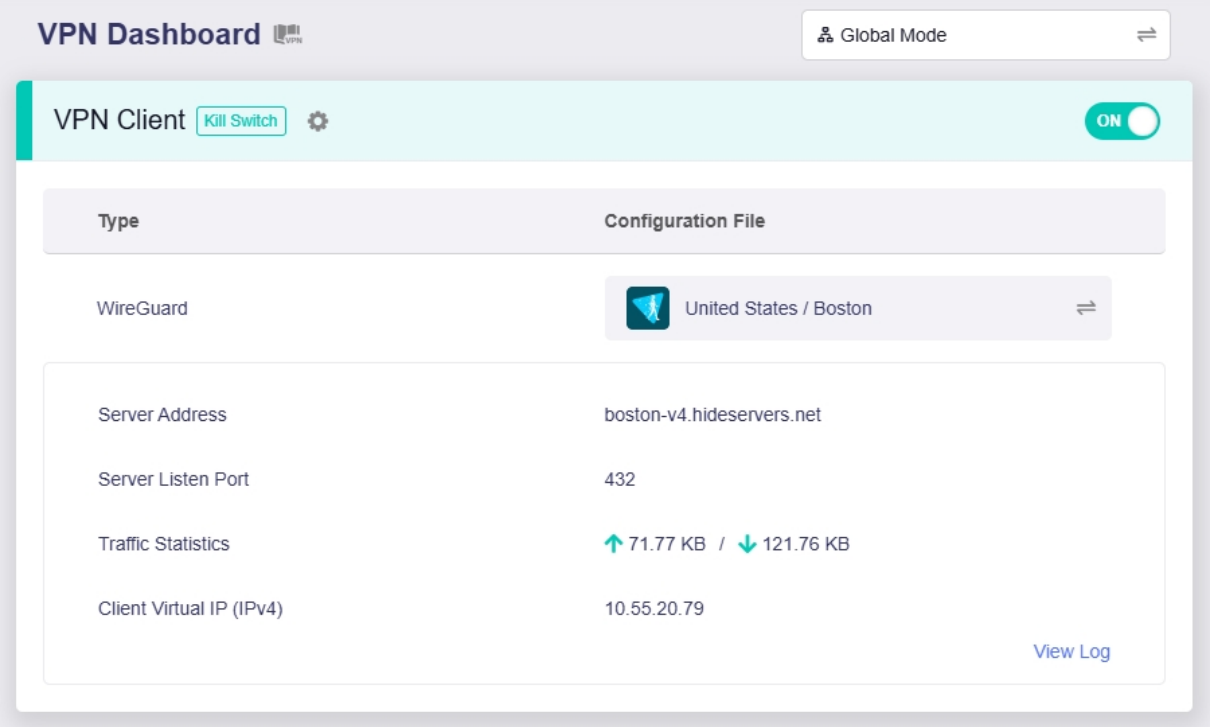
Poniżej przedstawiono przykład dla **Hide.me**. Zaloguj się, podając dane logowania Hide.me.



Wybierz serwer VPN i kliknij **Apply**. Z tym serwerem zostanie nawiązane połączenie, a Twój publiczny adres IP będzie wskazywać lokalizację wybranego serwera.

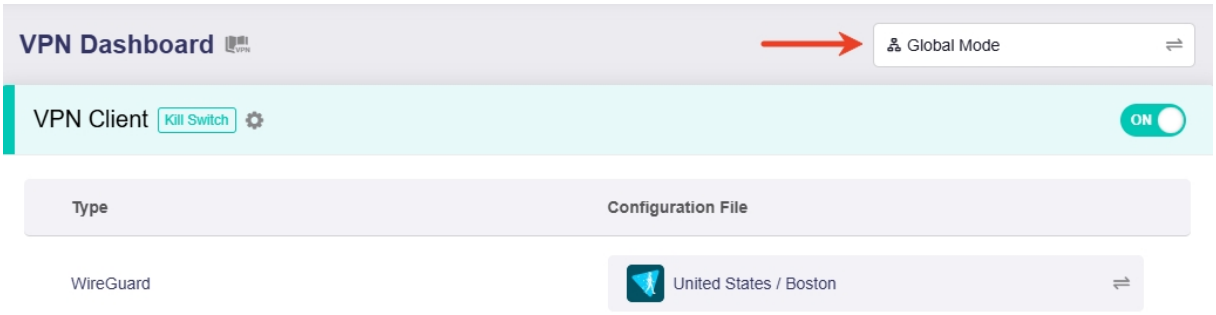


Połączenie zostanie nawiązane automatycznie. Po połączeniu przejdź do **VPN Dashboard**. Zobaczysz włączony tunel VPN wraz ze szczegółami: protokołem VPN (np. WireGuard), plikiem konfiguracyjnym, adresem serwera, portem nasłuchiwania serwera, statystykami transferu i wirtualnym adresem IP klienta. W prawym dolnym rogu możesz też przeglądać dzienniki połączenia.

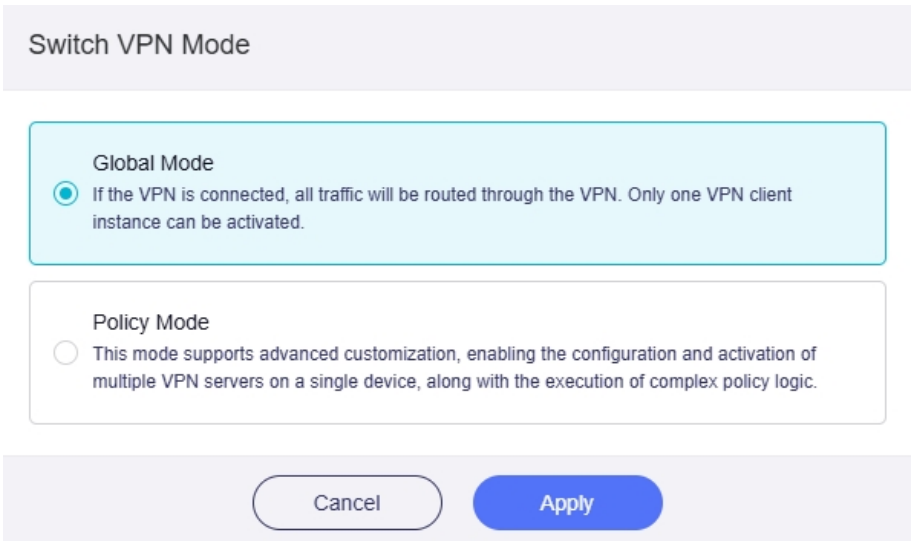

VPN Dashboard
Global Mode
VPN Client
Kill Switch
ON
Type
Configuration File
WireGuard
United States / Boston
Server Address
boston-v4.hideservers.net
Server Listen Port
432
Traffic Statistics
71.77 KB / 121.76 KB
Client Virtual IP (IPv4)
10.55.20.79
View Log

9.2 Tryb VPN

W razie potrzeby na stronie VPN Dashboard kliknij przycisk w prawym górnym rogu, aby zmienić tryb VPN.



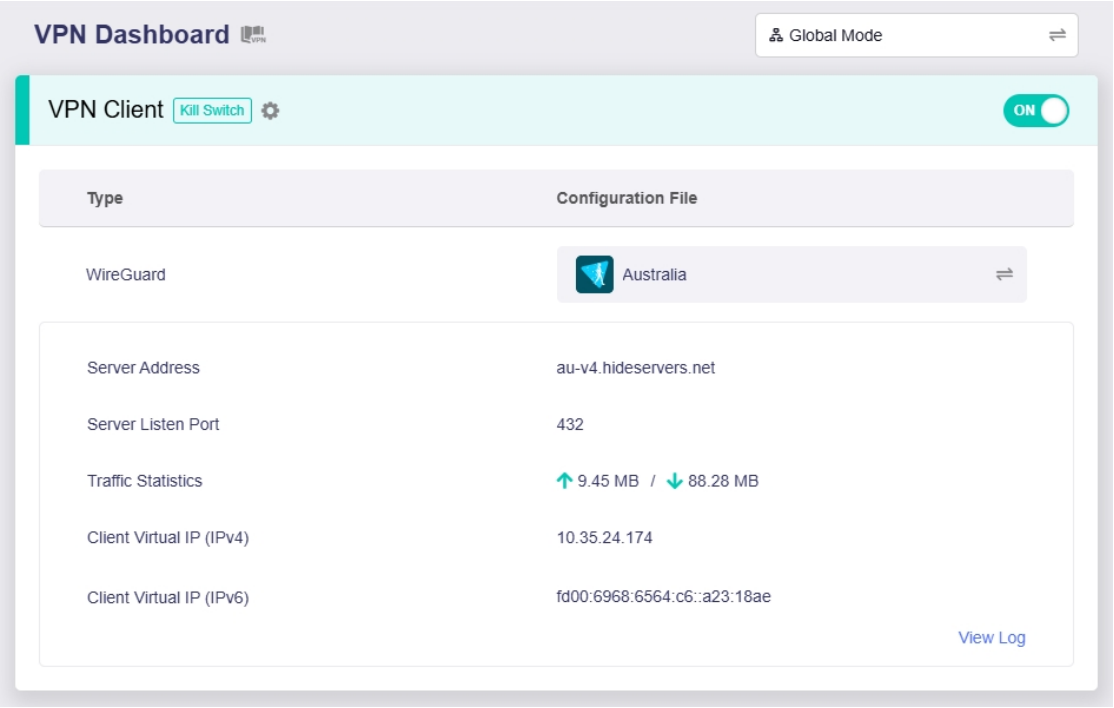
Dostępne są dwa tryby: **Global Mode** i **Policy Mode**.



9.2.1 Tryb globalny

W tym trybie cały ruch jest kierowany przez tunel VPN i można włączyć tylko jedną instancję klienta VPN. Sprawdza się on, gdy ruch wszystkich urządzeń ma przechodzić przez jeden serwer VPN, np. w celu zapewnienia jednolitej ochrony sieci lub dostępu do treści przeznaczonych dla określonego regionu.

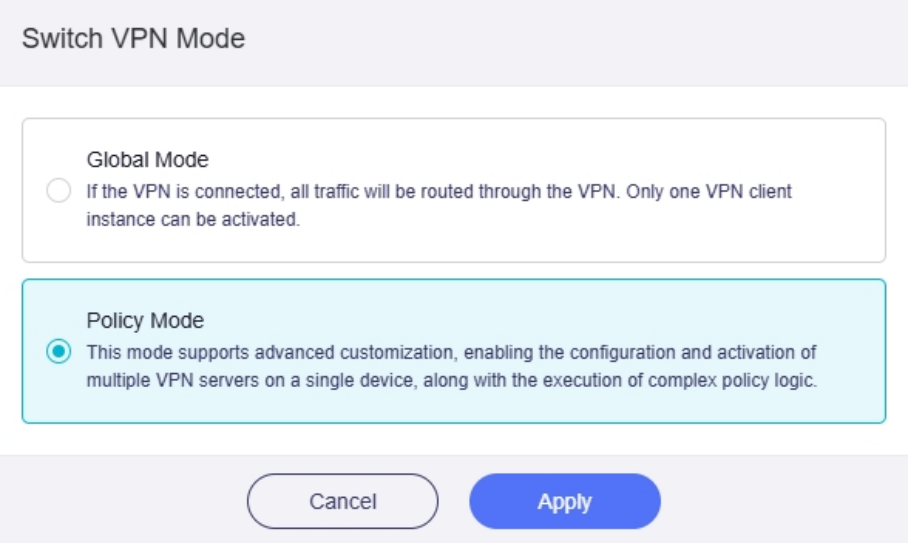
W poniższym przykładzie router łączy się z serwerem w Australii za pomocą protokołu WireGuard. Cały ruch podłączonych klientów będzie kierowany przez ten tunel VPN.



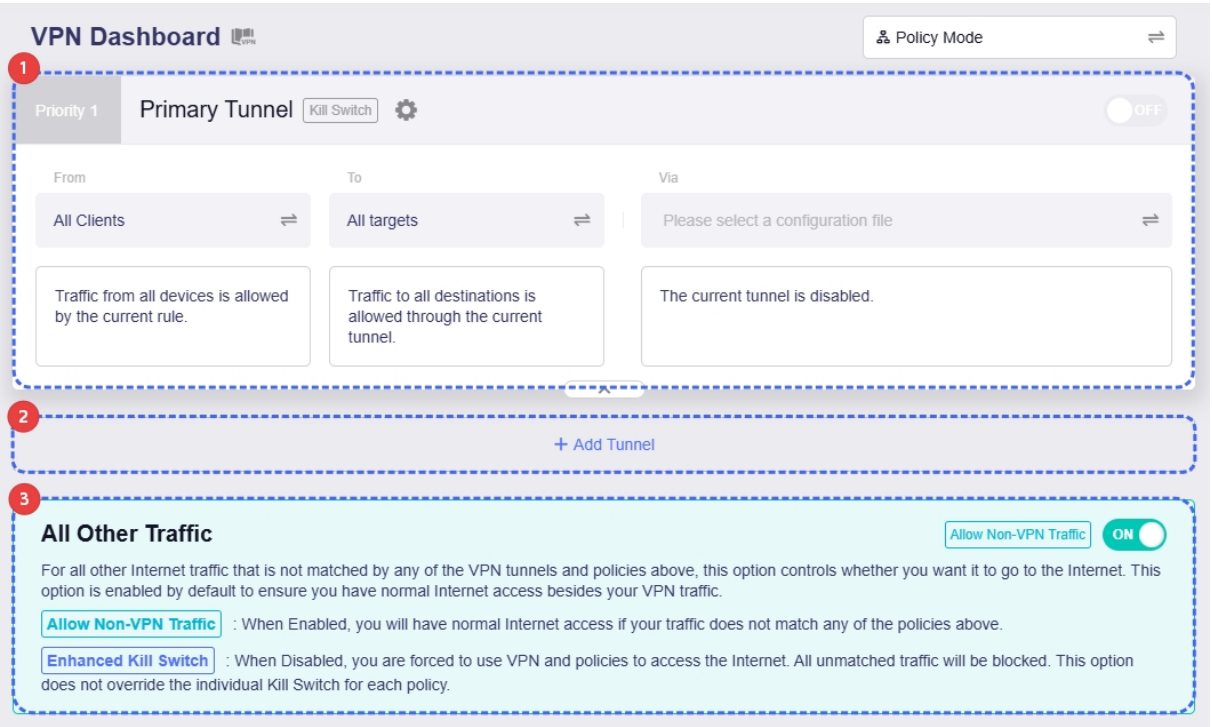
9.2.2 Tryb reguł

W tym trybie możesz połączyć jeden router z wieloma serwerami VPN i dostosować reguły VPN. Sprawdza się on, gdy potrzebne jest elastyczne zarządzanie ruchem, np. kierowanie różnych rodzajów ruchu do różnych miejsc docelowych przez wiele serwerów VPN.

Zmień tryb VPN na **Policy Mode** i kliknij **Apply**.



Po zmianie trybu, jeśli VPN nie jest włączony, strona wygląda jak poniżej i zawiera trzy sekcje: **Primary Tunnel**, **Add Tunnel** i **All Other Traffic**.

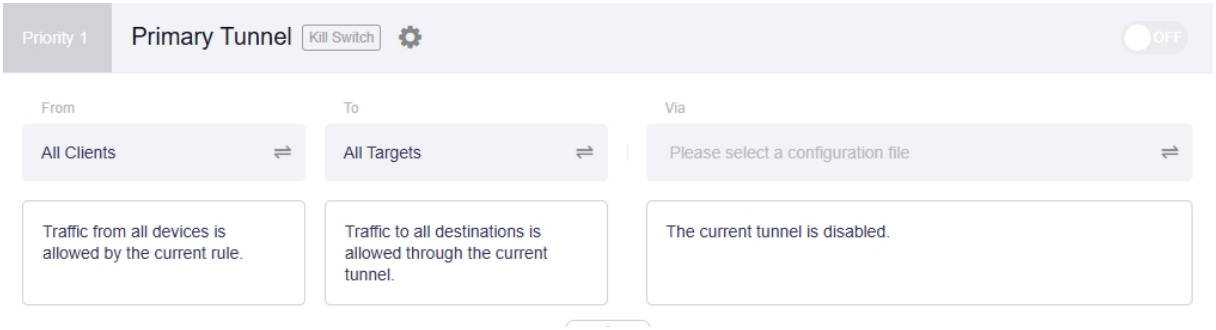


9.2.2.1 Tunel główny

Tunel główny jest wstępnie zdefiniowanym tunelem w trybie reguł. Domyślnie ma najwyższy priorytet; po skonfigurowaniu wielu tuneli można zmienić jego priorytet.

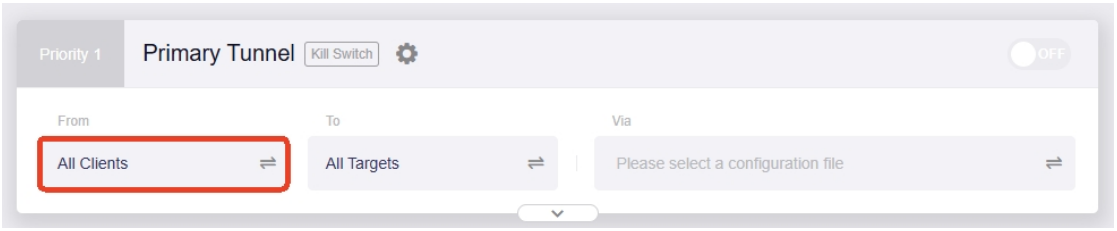
W tym tunelu możesz dostosować regułę tunelu, ustawiając trzy parametry:

- **From**: źródło ruchu, czyli ruch, który ma być kierowany przez ten tunel.
- **To**: miejsce docelowe, do którego ruch jest kierowany przez ten tunel.
- **Via**: sposób kierowania ruchu, czyli określenie, czy ma być używany VPN.

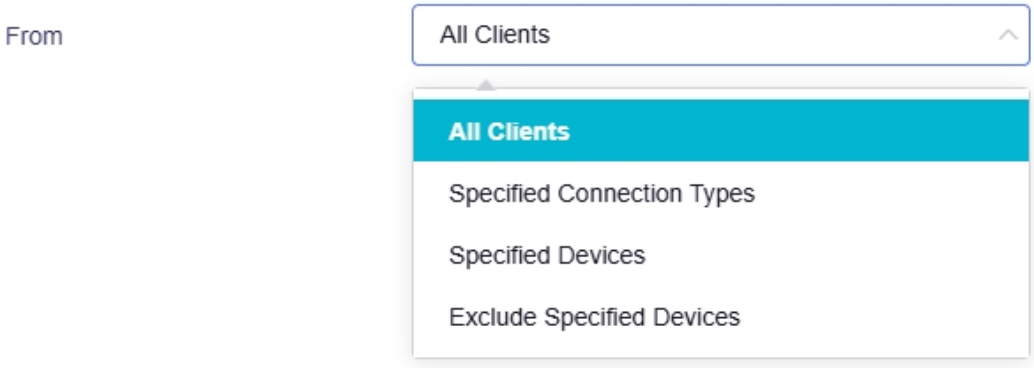


Aby skonfigurować regułę tunelu, wykonaj poniższe czynności.

1. Kliknij szare pole po lewej stronie.



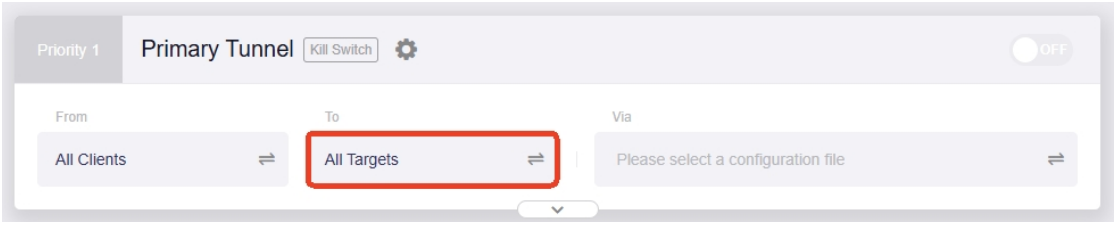
2. Wybierz urządzenie, które ma odpowiadać tej regule, i kliknij **Apply**.



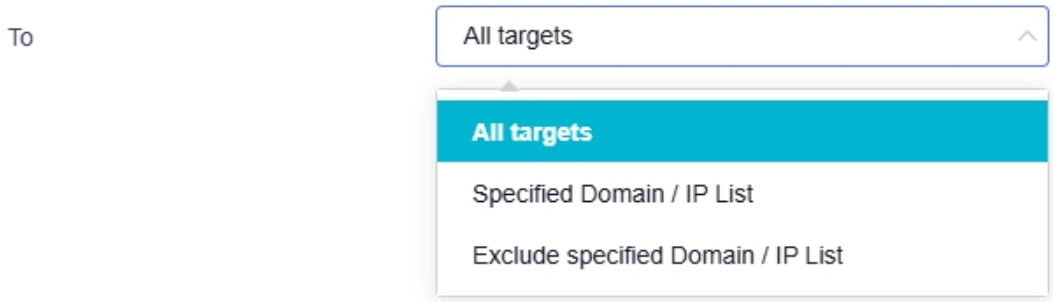
- **All Clients**: ruch ze wszystkich urządzeń będzie odpowiadać tej regule.

- **Specified Connection Types**: ruch z określonych typów połączeń (np. podsieci LAN, Drop-in Gateway, sieci gościnnej) będzie odpowiadać tej regule.
- **Specified Devices**: ruch z określonych urządzeń (identyfikowanych według adresu MAC) będzie odpowiadać tej regule.
- **Exclude Specified Devices**: ruch z określonych urządzeń (identyfikowanych według adresu MAC) **NIE** będzie odpowiadać tej regule.

3. Kliknij szare pole pośrodku.



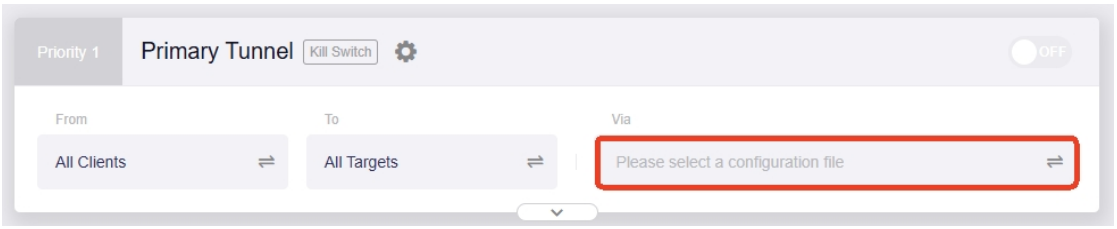
4. Wybierz miejsce docelowe, do którego ruch ma być kierowany przez ten tunel, i kliknij **Apply**.



- **All Targets**: ruch odpowiadający tej regule będzie kierowany do wszystkich miejsc docelowych.
- **Specified Domain / IP List**: ruch odpowiadający tej regule będzie kierowany do określonych domen lub adresów IP. Wprowadź je ręcznie lub podaj adres URL subskrypcji. Wskazanie domeny głównej obejmuje wszystkie jej subdomeny.
- **Exclude specified Domain / IP List**: ruch odpowiadający tej regule **NIE** będzie kierowany do określonych domen lub adresów IP. Wprowadź je ręcznie lub podaj adres URL subskrypcji. Wskazanie domeny głównej obejmuje wszystkie jej subdomeny.

Uwaga: po wybraniu Subscribe URL nazwy domen lub adresy IP dostępne pod tym adresem URL będą automatycznie aktualizowane codziennie. Wprowadź poprawny adres URL. Sprawdzanie adresu URL zweryfikuje poprawność nazwy domeny lub adresu IP.

5. Kliknij szare pole po prawej stronie.

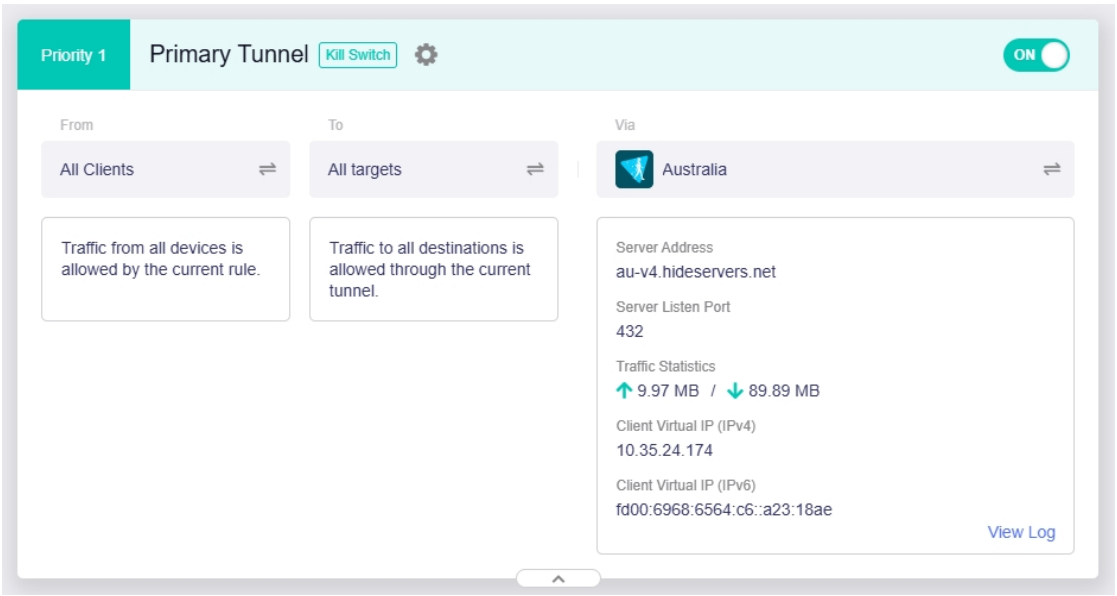


6. Wybierz sposób kierowania ruchu dla tego tunelu: **Use VPN** lub **Not Use VPN**.



- **Use VPN**: ruch odpowiadający tej regule będzie kierowany do wybranych miejsc docelowych przez tunel VPN. Dla tej reguły należy wybrać plik konfiguracyjny VPN.
- **Not Use VPN**: ruch odpowiadający tej regule będzie kierowany do wybranych miejsc docelowych przez lokalną sieć WAN zamiast przez VPN.

7. Po skonfigurowaniu źródła ruchu, miejsca docelowego i sposobu kierowania ruchu konfiguracja reguły tunelu głównego jest zakończona. W poniższym przykładzie reguła tunelu jest następująca: wszyscy klienci podłączeni do tego routera będą korzystać z Internetu przez VPN; ich ruch zostanie skierowany tym tunelem VPN do serwera w Australii, a następnie przez ten serwer do Internetu.

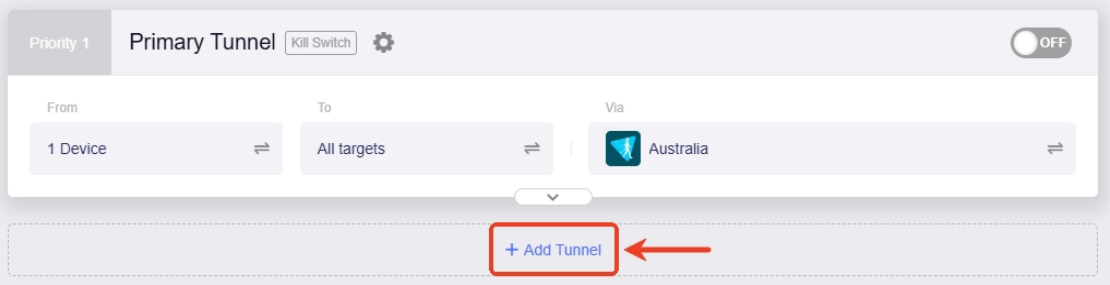


Uwaga: ze względów bezpieczeństwa przejdź do sekcji **9.2.2.3 Cały pozostały ruch** i **9.2.2.4 Opcje tunelu**, aby sprawdzić pozostałe ustawienia przed włączeniem tunelu.

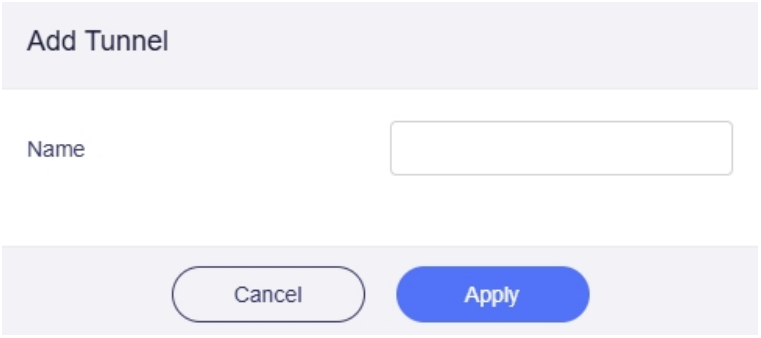
9.2.2.2 Dodawanie tunelu

Dodaj tunele, jeśli chcesz kierować ruch z różnych urządzeń do różnych miejsc docelowych. Aby dodać tunel, wykonaj poniższe czynności.

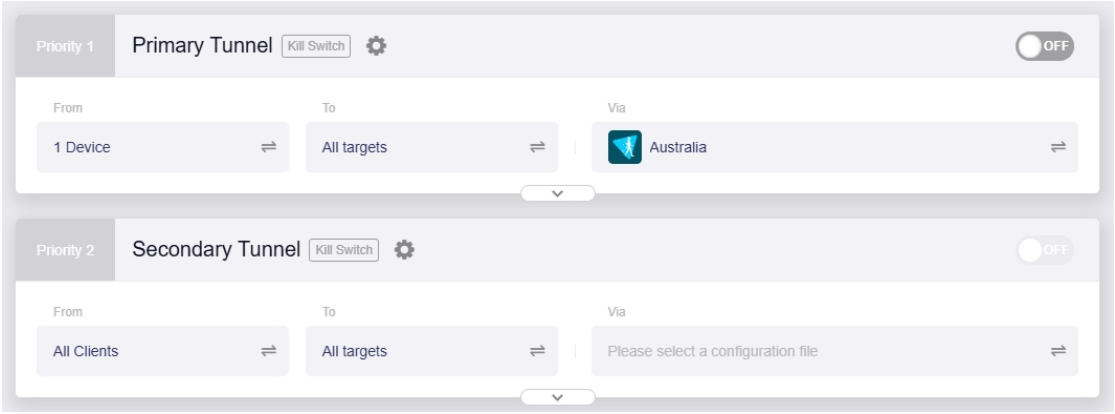
1. Kliknij **Add Tunnel** pod tunelem głównym.



2. Nadaj tunelowi nazwę.



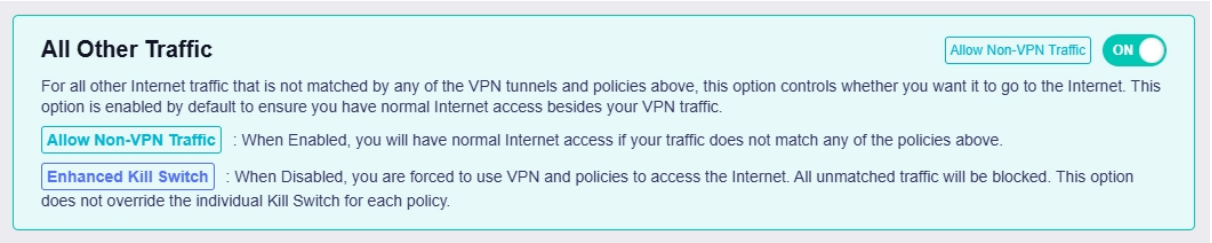
3. Na stronie VPN Dashboard pojawi się kolejny tunel. Można utworzyć maksymalnie 5 tuneli, łącznie ze wstępnie zdefiniowanym tunelem głównym.



4. Skonfiguruj reguły tunelu, określając źródło ruchu, miejsca docelowe i metodę routingu. Po zakończeniu przejdź do sekcji **9.2.2.3 Cały pozostały ruch** i **9.2.2.4 Opcje tunelu**, aby sprawdzić pozostałe ustawienia przed włączeniem tunelu.

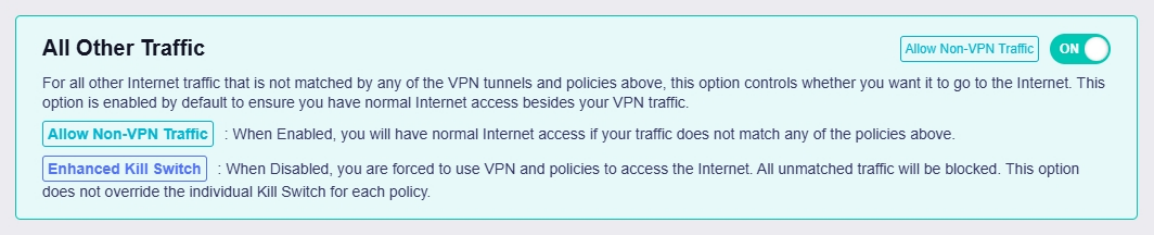
9.2.2.3 Cały pozostały ruch

W trybie reguł na dole strony VPN Dashboard widoczny jest domyślny tunel, który jest już włączony.

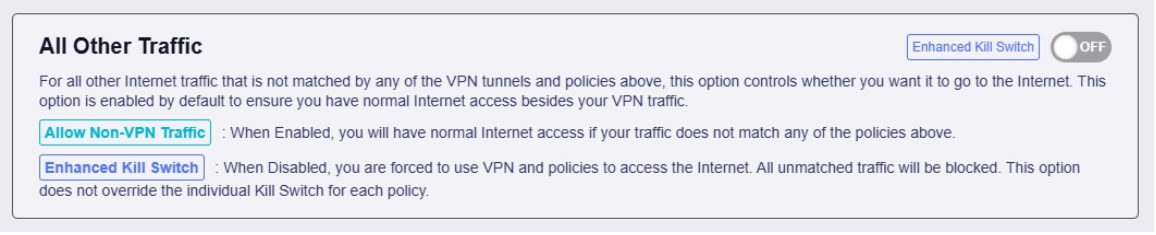


Ten tunel określa, czy ruch niepasujący do żadnej z powyższych grup tuneli VPN może uzyskiwać dostęp do Internetu. Jest domyślnie włączony, aby zapewnić normalny dostęp do Internetu dla ruchu niekierowanego przez VPN.

- Po włączeniu ruch niepasujący do reguł nadal może uzyskiwać dostęp do Internetu.

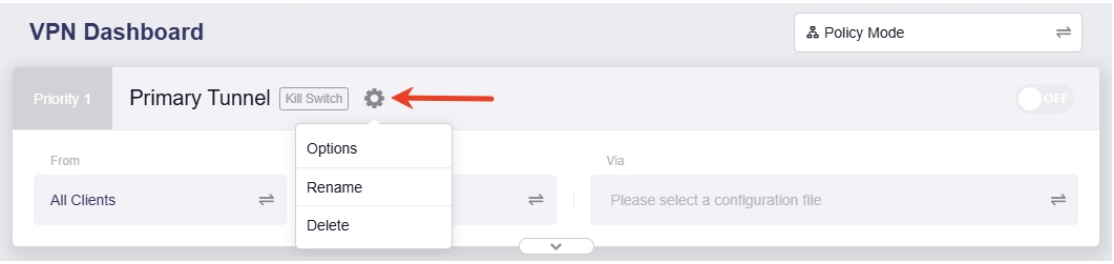


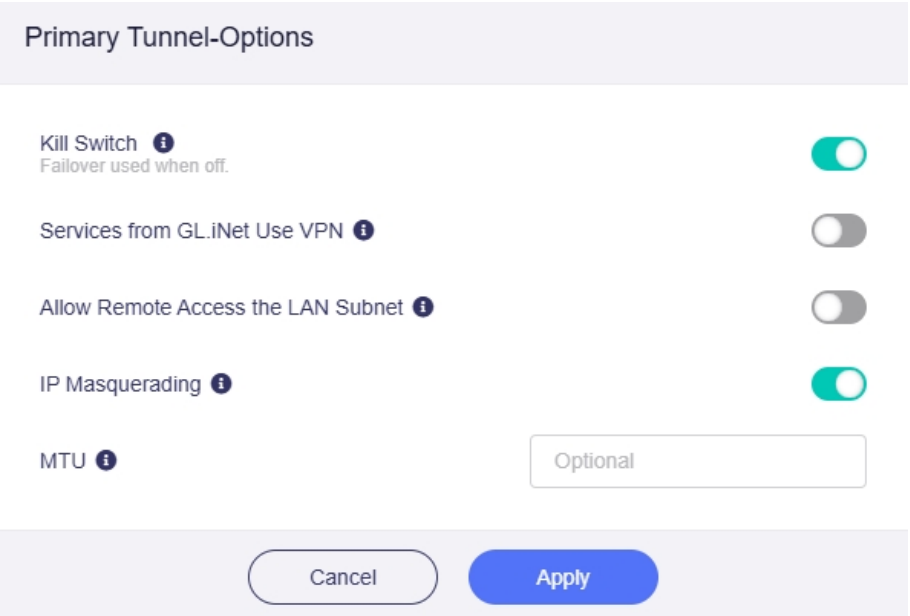
- Po wyłączeniu tylko ruch kierowany przez VPN może uzyskiwać dostęp do Internetu. Cały ruch poza VPN oraz ruch przełączany awaryjnie z połączeń VPN zostaje zablokowany. Ta opcja nie zastępuje indywidualnego ustawienia Kill Switch dla każdego tunelu VPN.



9.2.2.4 Opcje tunelu

Dla każdego tunelu VPN możesz skonfigurować ustawienia zaawansowane, takie jak VPN Kill Switch, IP Masquerading i MTU. Kliknij ikonę koła zębatego obok nazwy tunelu.





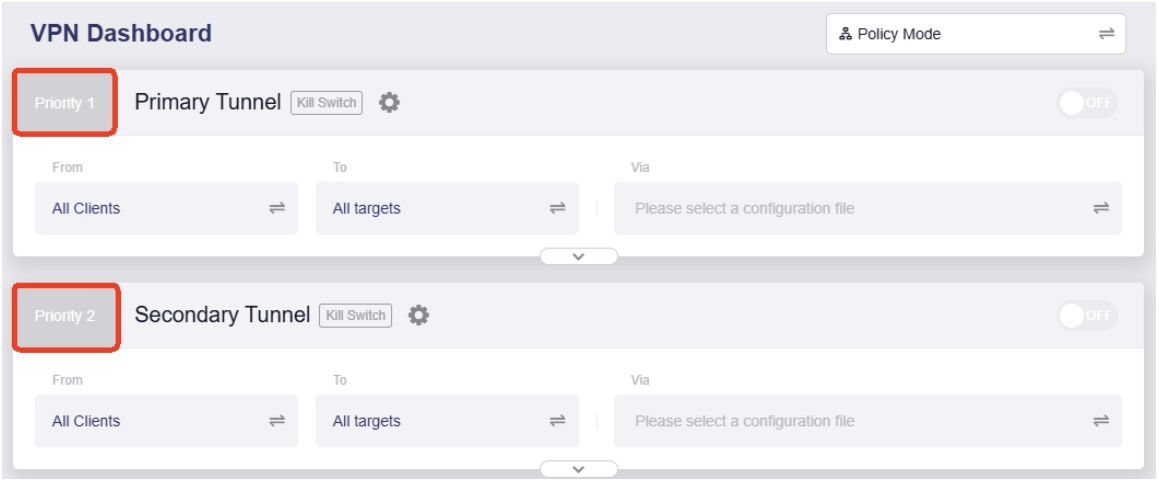
- **Kill Switch**: po włączeniu ruch pasujący do tego tunelu VPN zostanie zablokowany, jeśli połączenie niespodziewanie się zerwie; w przeciwnym razie zostanie przełączony do tuneli o kolejnym priorytecie lub sieci WAN.
- **Services from GL.iNet Use VPN**: po włączeniu usługi GoodCloud, DDNS i rtty przesyłają pakiety przez tunele VPN. Ta opcja jest domyślnie wyłączona, ponieważ usługi te zwykle wymagają rzeczywistego adresu IP urządzenia do poprawnego działania.
- **Allow Remote Access the LAN Subnet**: po włączeniu dozwolony jest zdalny dostęp przez VPN do tego routera (adresu IP tunelu) i urządzeń LAN. Serwer VPN musi rozgłaszać trasę powrotną do podsieci LAN tego routera.
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tylko w konfiguracjach sieć–sieć, gdy zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: wartość ustawiona dla tunelu zastępuje wartość MTU w pliku konfiguracyjnym.

9.2.2.5 Priorytet tuneli

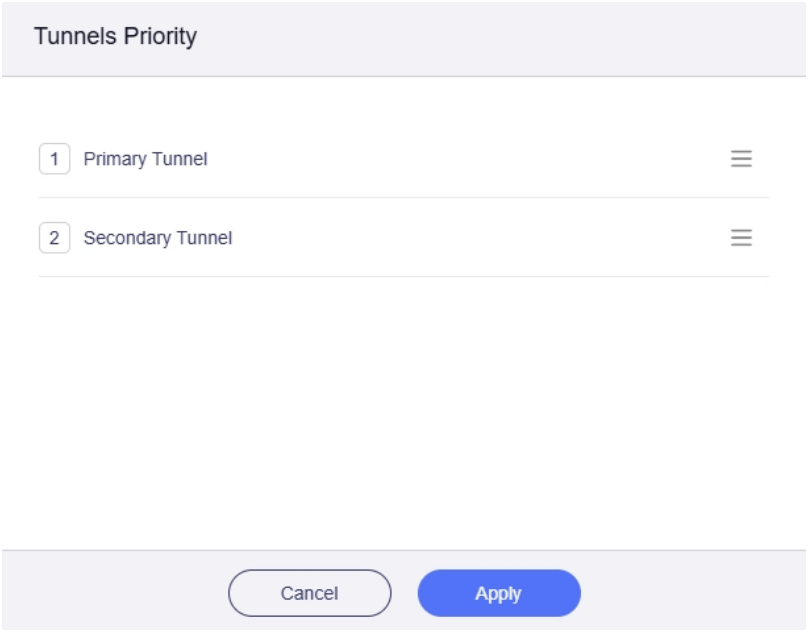
Domyślnie wstępnie zdefiniowany tunel Primary Tunnel ma najwyższy priorytet, po nim następują ręcznie dodane tunele (jeśli istnieją), a następnie tunel All Other Traffic, który zapewnia łączność przez lokalną sieć dostawcy Internetu (WAN).

Aby zmienić priorytet tuneli, wykonaj poniższe czynności.

1. Kliknij etykietę priorytetu w lewym górnym rogu dowolnego tunelu (np. Priority 1 / Priority 2).



2. W wyskakującym oknie kliknij i przytrzymaj ikonę trzech linii po prawej stronie, zmień kolejność tuneli, a następnie kliknij **Apply**.



Gdy włączonych jest wiele tuneli, router kieruje ruch w następującej kolejności:

1. Najpierw sprawdza dopasowanie ruchu do reguły tunelu o najwyższym priorytecie. Jeśli ruch pasuje, kieruje go przez ten tunel; w przeciwnym razie sprawdza kolejny tunel, aż do dopasowania tunelu „All Other Traffic”.
2. Jeśli tunel VPN niespodziewanie się rozłączy, system zdecyduje o przełączeniu ruchu do tunelu o kolejnym priorytecie na podstawie tego, czy w tym tunelu włączono **Kill Switch**.
    - Gdy Kill Switch jest włączony, ruch zostaje zablokowany i nie jest przełączany do tunelu o kolejnym priorytecie.
    - Gdy Kill Switch jest wyłączony, ruch jest przełączany do tunelu o kolejnym priorytecie i sprawdzany pod kątem dopasowania do jego reguł.
3. Tunel **All Other Traffic** jest domyślnie włączony, aby ruch niepasujący do tuneli VPN nadal mógł uzyskiwać dostęp do Internetu.
    - Po włączeniu kieruje niedopasowany lub przełączony awaryjnie ruch przez lokalną sieć WAN.
    - Po wyłączeniu wzmacnia działanie Kill Switch i blokuje zwykły dostęp do Internetu, aby zapobiec ujawnieniu adresu IP.

Rozdział 10

Konfiguracja serwera VPN

W tym rozdziale opisano konfigurację routera GL.iNet jako serwera OpenVPN lub WireGuard.

10.1 Serwer OpenVPN

OpenVPN to protokół VPN o otwartym kodzie źródłowym, wykorzystujący szyfrowanie SSL/TLS do bezpiecznych połączeń punkt–punkt i sieć–sieć. Aby skonfigurować serwer OpenVPN na routerze GL.iNet, obejrzyj ten film lub wykonaj poniższe czynności.

10.1.1 Przygotowanie

1. **Upewnij się, że masz publiczny adres IP**

   Kliknij tutaj, aby sprawdzić, czy dostawca usług internetowych (ISP) przydziela Ci publiczny adres IP.

   Jeśli nie, nie można skonfigurować routera jako serwera OpenVPN.

   Rozwiązania alternatywne:

   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli dwie powyższe metody nie działają (np. gdy sieć znajduje się za CGNAT), możesz wypróbować nasze rozwiązanie SD-WAN AstroWarp.

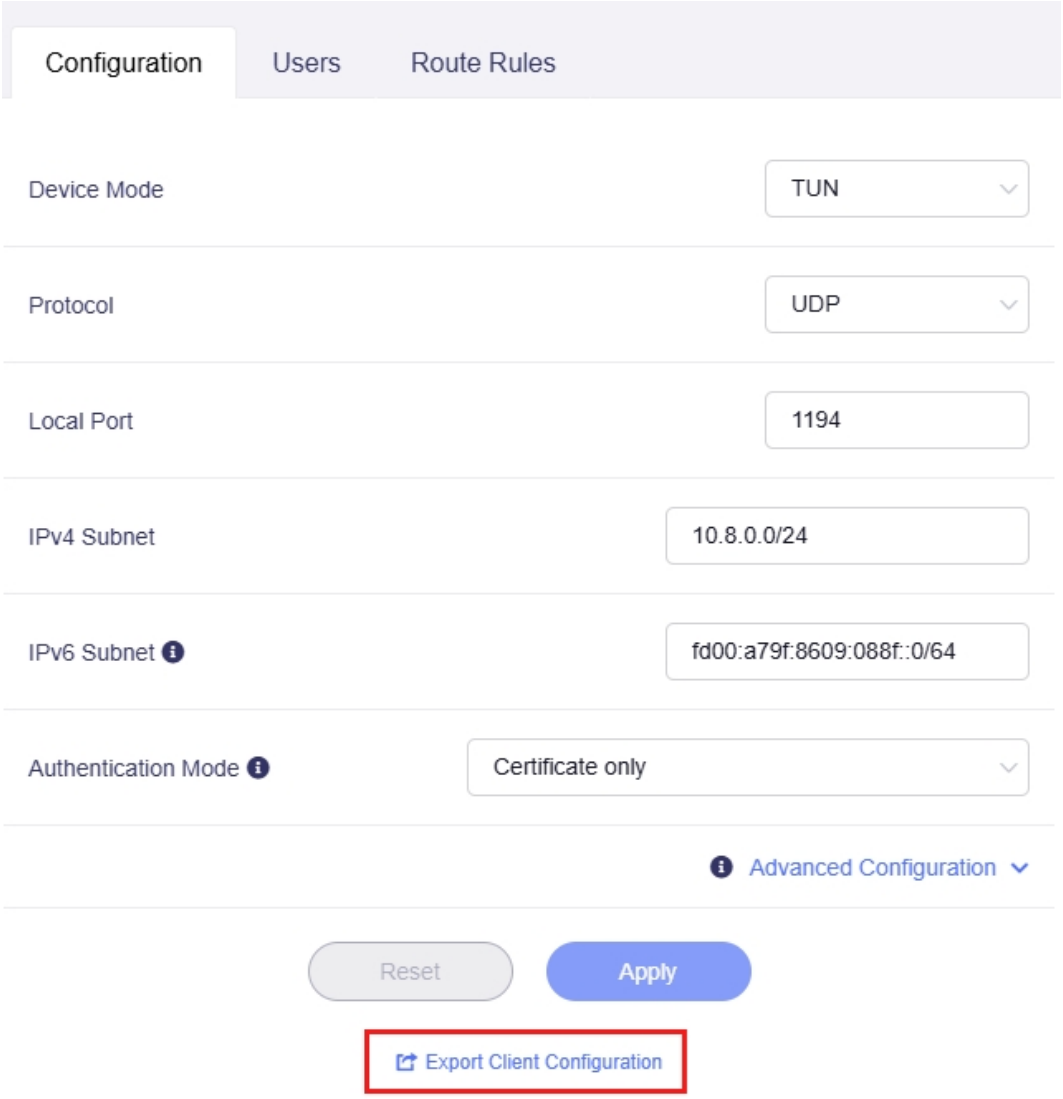
2. **Sprawdź, czy wymagane jest przekierowanie portów**

   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli router GL.iNet znajduje się kilka poziomów za głównym routerem, skonfiguruj przekierowanie portów na każdym urządzeniu pośrednim.

10.1.2 Etapy konfiguracji

1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.

   Domyślna konfiguracja sprawdza się w większości przypadków. Kliknij **Export Client Configuration** u dołu i przejdź do kroku 3. Jeśli konfiguracja została zmieniona, przed eksportem kliknij **Apply**.



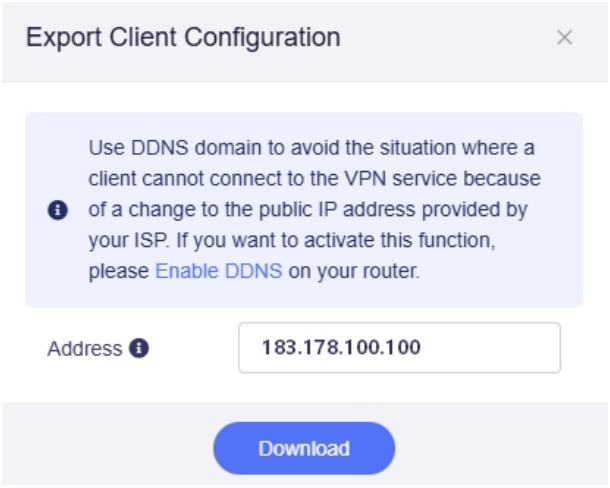
- **Device Mode**: TAP-S2S lub Tun. Różnice opisano tutaj.
- **Protocol**: UDP lub TCP. Różnice opisano tutaj.
- **Authentication Mode**: określa metodę uwierzytelniania klienta podczas łączenia z serwerem. Dostępne są trzy opcje:

- **Certificate Only**: router automatycznie generuje certyfikaty i klucze serwera oraz klienta, a następnie umieszcza je w pliku konfiguracyjnym. Po przesłaniu konfiguracji do klienta nie są wymagane dodatkowe dane logowania.
- **Username/Password Only**: router generuje konfigurację klienta bez kluczy certyfikatów. Przed eksportem konfiguracji klienta trzeba dodać nazwę użytkownika i hasło na karcie **Users**. Podczas przesyłania konfiguracji do klienta wprowadź te dane w celu uwierzytelnienia.
- **Username/Password and Certificate**: przed eksportem konfiguracji klienta trzeba najpierw dodać nazwę użytkownika i hasło na karcie **Users**. Następnie router automatycznie generuje certyfikaty i klucze serwera oraz klienta i umieszcza je w pliku konfiguracyjnym. Podczas przesyłania konfiguracji do klienta najpierw sprawdzany jest certyfikat i klucz, a potem nazwa użytkownika i hasło, co zapewnia uwierzytelnianie dwuskładnikowe.

- **Advanced Configuration**: w razie potrzeby dostosuj dodatkowe ustawienia serwera.

3. Wyeksportuj konfigurację klienta.

   Po kliknięciu **Export Client Configuration** u dołu karty Configuration (lub zastosowaniu zmienionej konfiguracji) pojawi się poniższe okno. Kliknij **Download**, aby wyeksportować konfigurację.



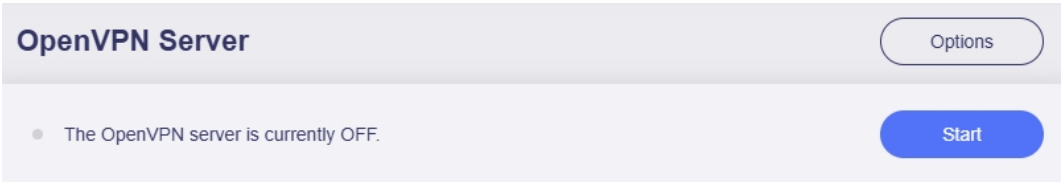
Wskazówki:

- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.
- Od wersji oprogramowania 4.8 przed wyeksportowaniem pliku konfiguracyjnego można wybrać adres serwera z listy: publiczny adres IP, domenę DDNS lub bieżący adres IP

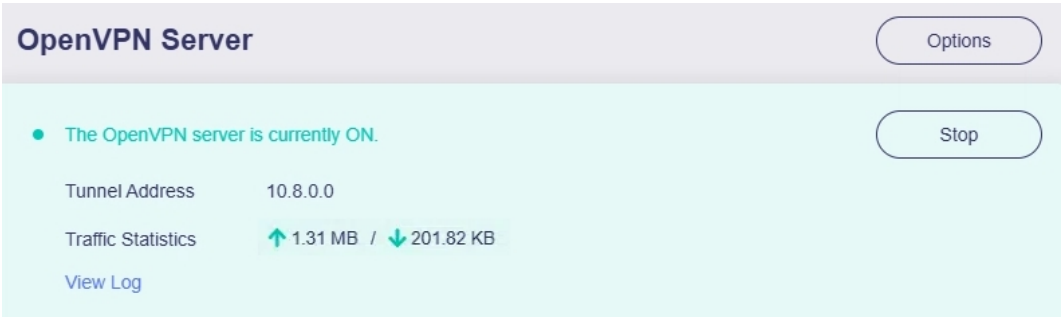
WAN. Po wybraniu adres serwera w pliku konfiguracyjnym zostanie automatycznie zaktualizowany. Pobierz plik konfiguracyjny ponownie, jeśli adres serwera ulegnie zmianie.

4. Uruchom serwer OpenVPN.

   Na stronie **OpenVPN Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



   Stan połączenia serwera jest wyświetlany u góry. Jeśli widoczne są statystyki wysyłania i pobierania, serwer OpenVPN działa.

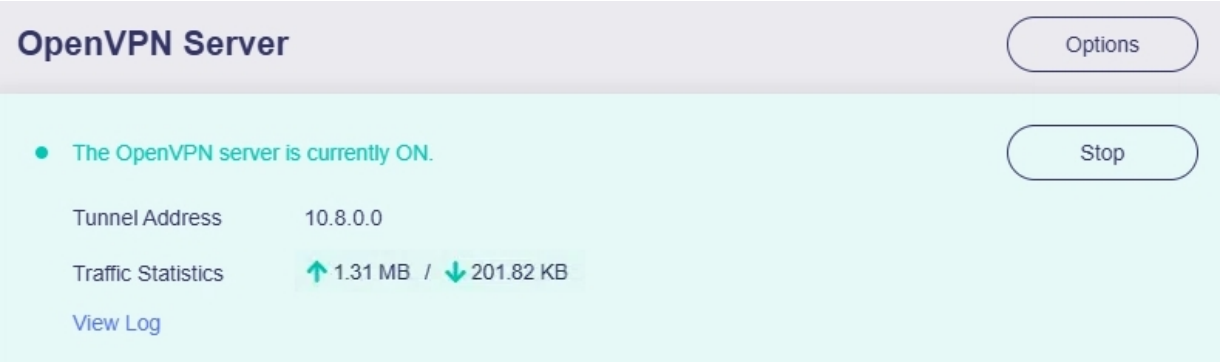


10.1.3 Sprawdzanie połączenia

Metoda 1. Sprawdzanie stanu serwera

W oprogramowaniu sprzętowym w wersji 4.8 możesz sprawdzić stan połączenia serwera na stronie **OpenVPN Server**.

Jeśli wyświetlane są statystyki wysyłania i pobierania danych, serwer OpenVPN działa.



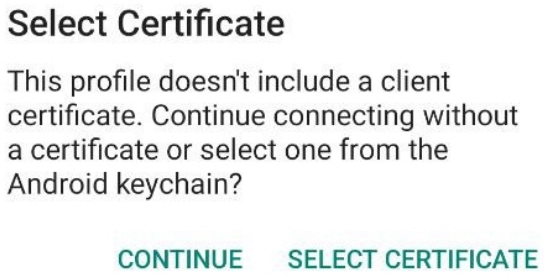
Metoda 2. Sprawdzanie adresu IP klienta

Zaimportuj wcześniej wyeksportowaną konfigurację OpenVPN do urządzenia w innej sieci (poza siecią lokalną serwera). Następnie otwórz przeglądarkę i wyszukaj swój adres IP oraz lokalizację. Jeśli odpowiadają adresowi IP i lokalizacji serwera VPN (zamiast adresowi dostawcy Internetu), połączenie VPN działa prawidłowo.

Poniżej przedstawiono przykład weryfikacji przy użyciu smartfona z zainstalowaną oficjalną aplikacją OpenVPN.

1. Najpierw wyłącz Wi-Fi w smartfonie i pozostaw włączoną wyłącznie transmisję danych komórkowych (4G/5G).
2. Następnie otwórz aplikację OpenVPN, zaimportuj plik konfiguracyjny i rozpocznij połączenie.
3. Sprawdź, czy smartfon ma dostęp do Internetu i czy jego adres IP odpowiada adresowi IP serwera OpenVPN.

   Wskazówka: podczas importowania pliku konfiguracyjnego do aplikacji OpenVPN może pojawić się przypomnienie pokazane poniżej. Kliknij **CONTINUE**, aby kontynuować, ponieważ certyfikat jest już osadzony w pliku konfiguracyjnym.



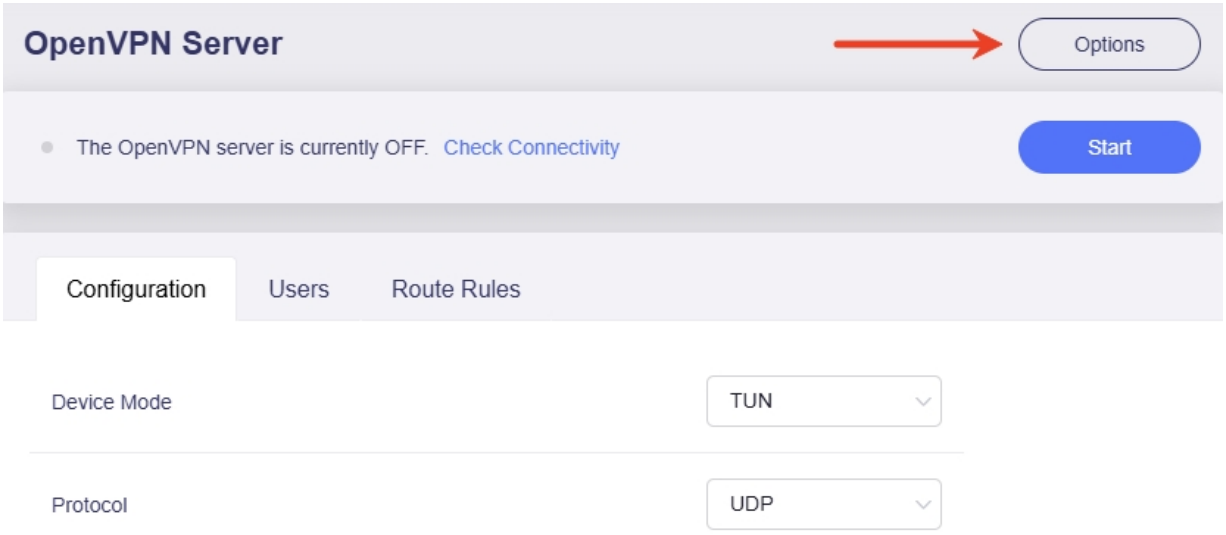
Jeśli połączenie się nie powiedzie, przyczyną może być jeden z typowych problemów:

- Serwer VPN nie ma publicznego adresu IP. Szczegóły znajdziesz w sekcji **10.1.1 Przygotowanie**.
- Może być konieczne skonfigurowanie przekierowania portów. Szczegóły znajdziesz w sekcji **10.1.1 Przygotowanie** .
- Port używany przez serwer OpenVPN jest blokowany przez dostawcę Internetu. Zmień port lub skontaktuj się z dostawcą w celu uzyskania pomocy.
- Połączenie VPN może być blokowane w niektórych krajach lub regionach.

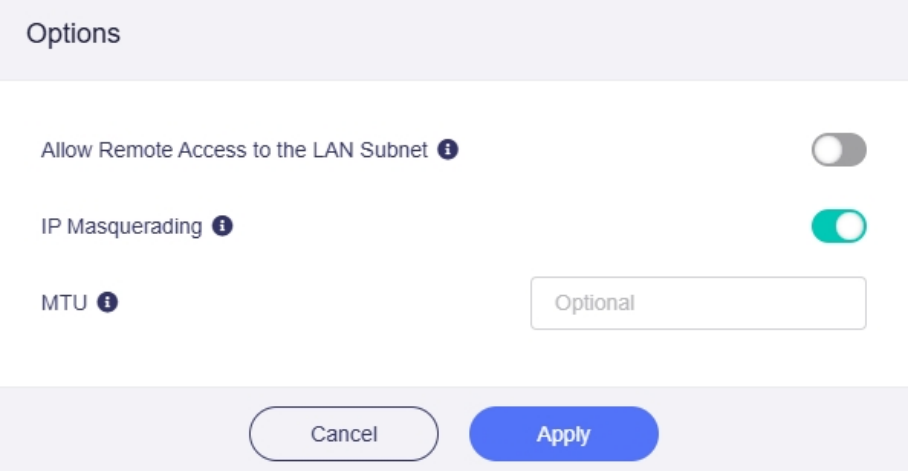
10.1.4 Opcje serwera

Opcje serwera obejmują zaawansowane ustawienia po stronie serwera, takie jak zdalny dostęp do jego sieci LAN czy maskowanie adresów IP. Skonfiguruj je zgodnie ze swoimi potrzebami.

Na stronie **OpenVPN Server** kliknij **Options** w prawym górnym rogu.



W wyskakującym oknie pojawią się poniższe funkcje.

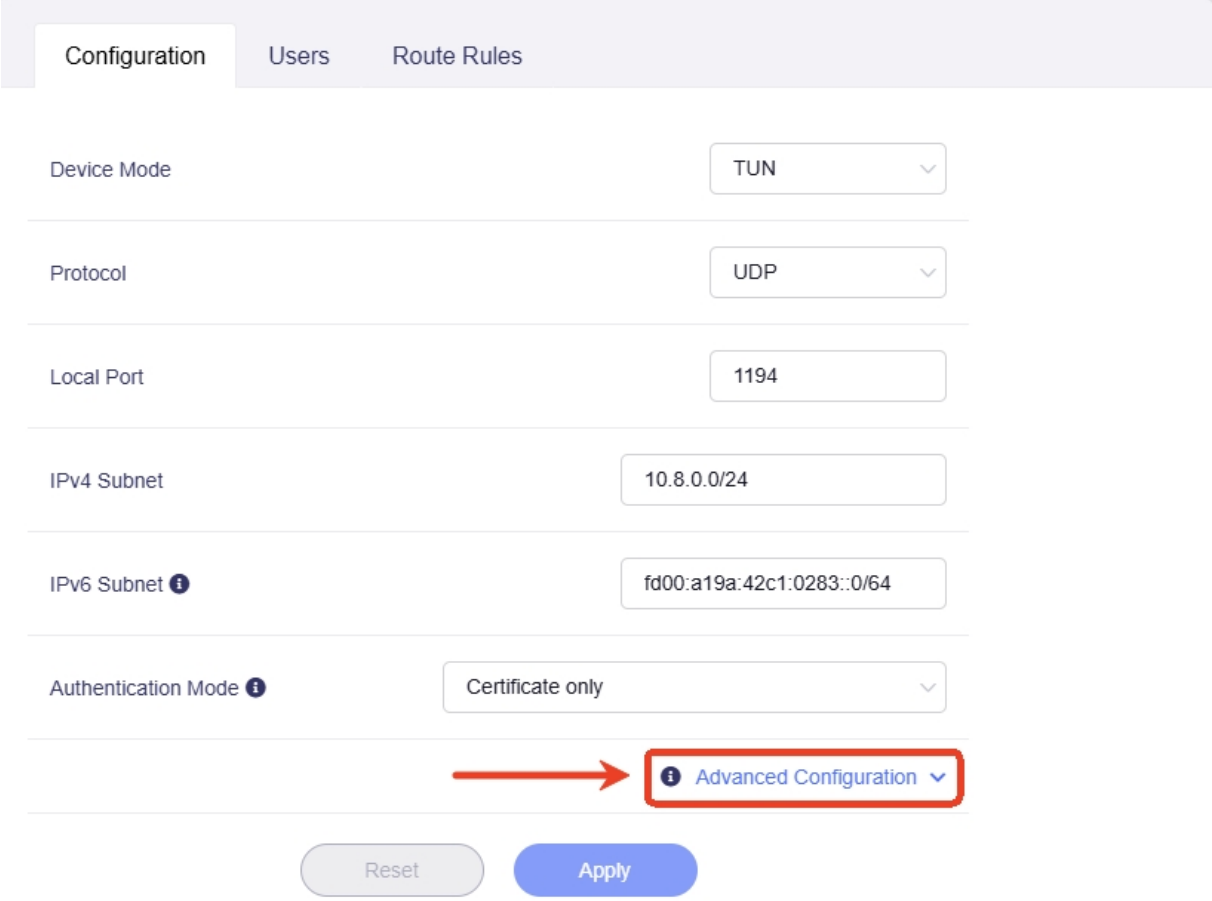


- **Allow Remote Access to the LAN Subnet**: po włączeniu zasoby w podsieci LAN serwera będą dostępne przez tunel VPN.
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tę opcję tylko w konfiguracjach sieć–sieć, w których zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: skrót od Maximum Transmission Unit, czyli maksymalnej jednostki transmisji. Wartość MTU ustawiona dla tunelu zastępuje ustawienia MTU w pliku konfiguracyjnym.

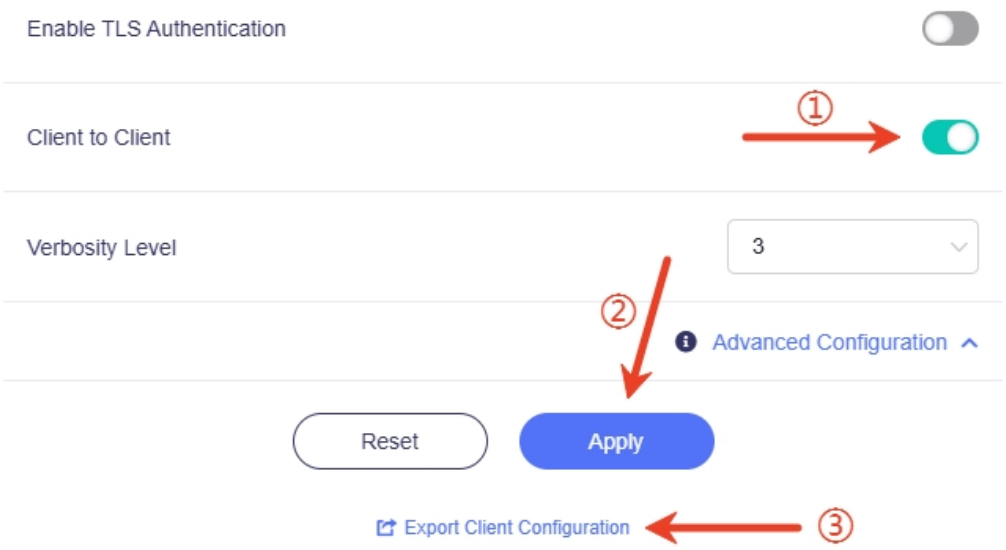
10.1.5 Komunikacja między klientami

Client to Client to funkcja VPN po stronie serwera. Po jej włączeniu połączeni klienci VPN mogą komunikować się ze sobą za pomocą swoich adresów IP tunelu VPN.
W razie potrzeby wykonaj poniższe czynności, aby włączyć Client to Client na serwerze OpenVPN.

1. Na stronie **OpenVPN Server** kliknij **Advanced Configuration** w prawym dolnym rogu.



2. Włącz **Client to Client** i kliknij **Apply**. Następnie wyeksportuj nową konfigurację i prześlij ją do klientów OpenVPN.



Wskazówka: Client to Client rozgłasza wyłącznie adres IP tunelu każdego klienta. Nie udostępnia automatycznie podsieci lokalnych LAN znajdujących się za klientami VPN. Aby umożliwić klientom wzajemny dostęp do ich podsieci LAN, dodaj na serwerze VPN reguły routingu rozgłaszające te zdalne podsieci.

10.2 Serwer WireGuard

WireGuard® to wyjątkowo prosta, szybka i nowoczesna sieć VPN wykorzystująca zaawansowaną kryptografię. Ma być szybsza, prostsza, lżejsza i bardziej użyteczna niż IPSec, bez skomplikowanej obsługi. Jej celem jest znacznie wyższa wydajność niż w przypadku OpenVPN.
*WireGuard® jest zastrzeżonym znakiem towarowym Jasona A. Donenfelda.

Aby skonfigurować serwer WireGuard na routerze GL.iNet, obejrzyj ten film lub wykonaj poniższe czynności.

10.2.1 Przygotowanie

1. **Upewnij się, że masz publiczny adres IP**

   Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela Ci publiczny adres IP. Jeśli nie, nie można skonfigurować routera jako serwera WireGuard.

   Rozwiązania alternatywne:

   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli dwie powyższe metody nie działają (np. gdy sieć znajduje się za CGNAT), możesz wypróbować nasze rozwiązanie SD-WAN AstroWarp.

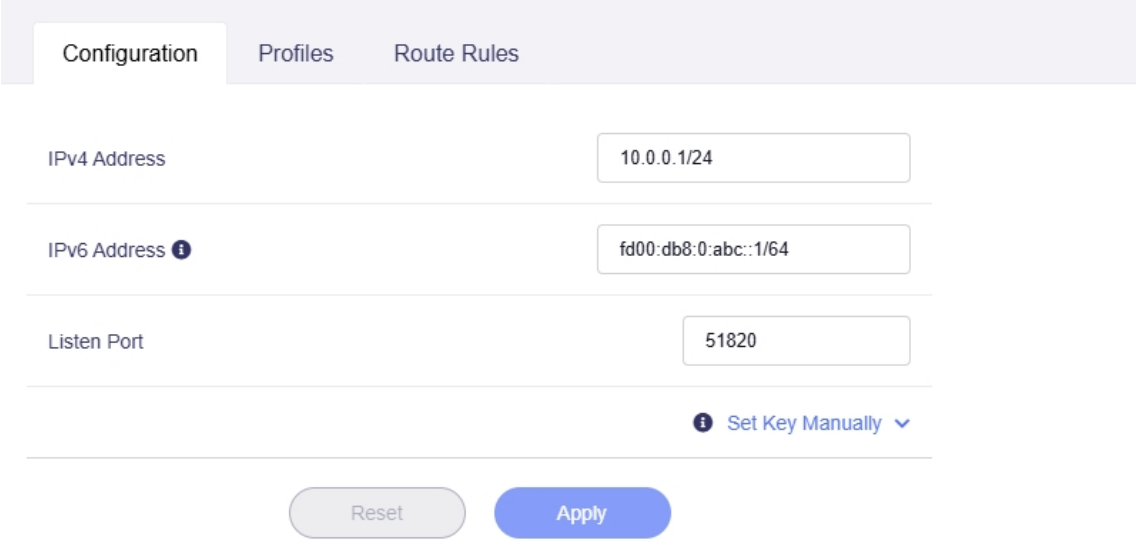
2. **Sprawdź, czy wymagane jest przekierowanie portów**

   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli router GL.iNet znajduje się kilka poziomów za głównym routerem, skonfiguruj przekierowanie portów na każdym urządzeniu pośrednim.

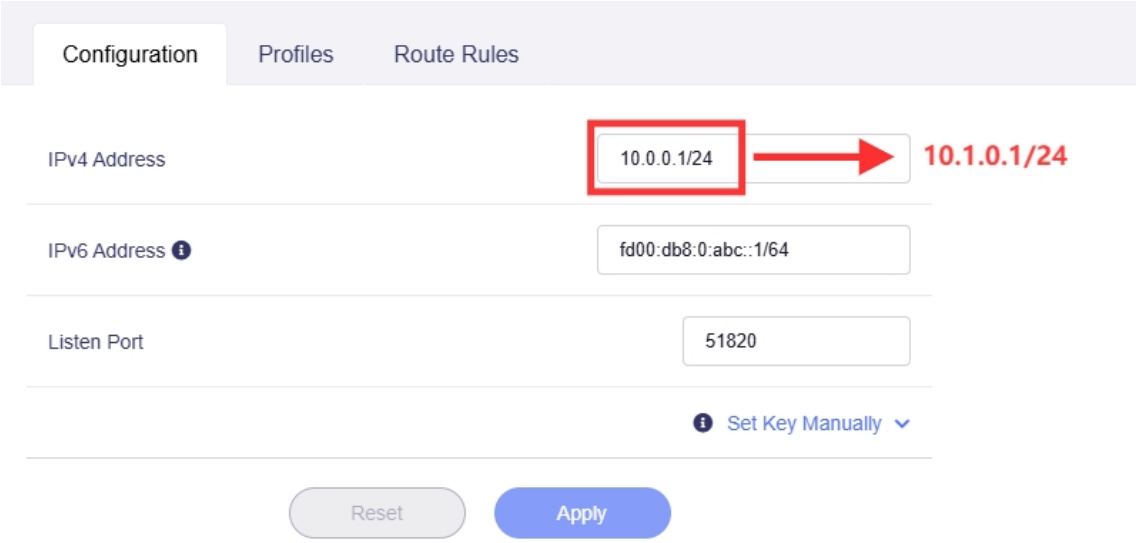
10.2.2 Etapy konfiguracji

1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **WireGuard Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.

   Domyślna konfiguracja sprawdza się w większości przypadków. Nie trzeba zmieniać adresu IPv4, chyba że koliduje z adresem bramy routera nadrzędnego.

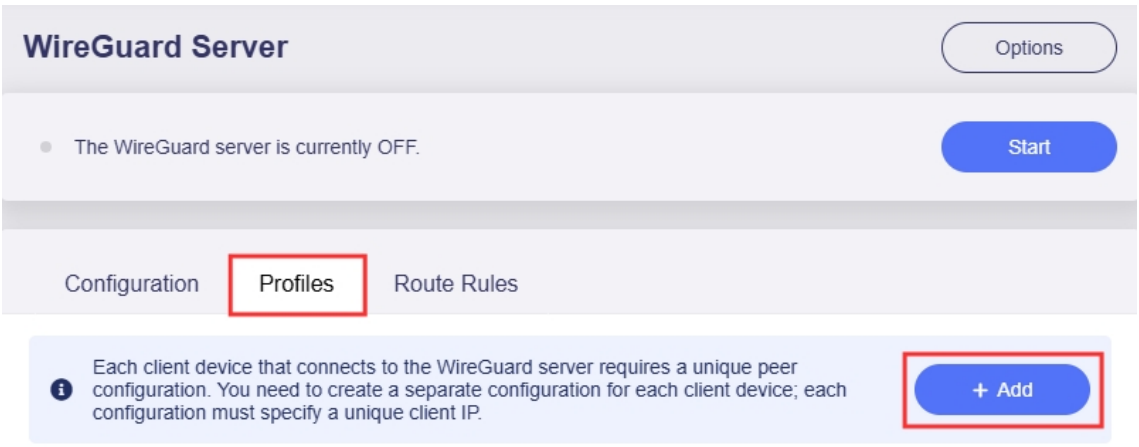


   Jeśli adres IPv4 koliduje z adresem bramy routera nadrzędnego, zmień go na inny (np. **10.1.0.1/24**) i kliknij **Apply**. Aby uniknąć problemów z łącznością, koniecznie zachowaj zapis CIDR „/24”.

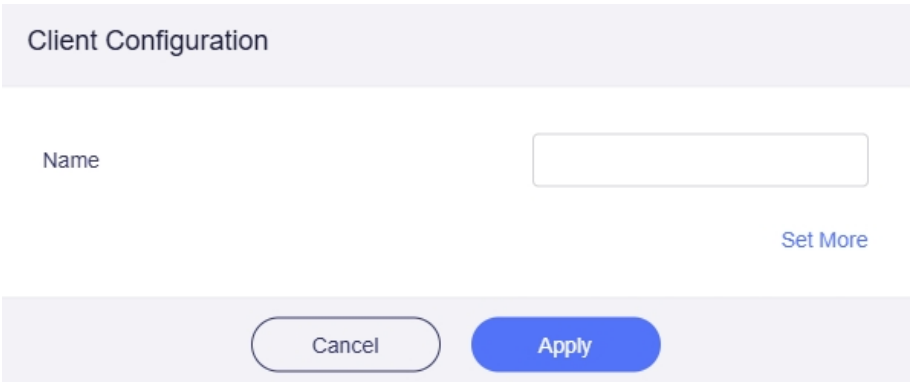


3. Dodaj profil.

   Przejdź na kartę **Profiles** i kliknij przycisk **Add**, aby wygenerować profil dla urządzenia.



Nadaj opisową nazwę i kliknij **Apply**, aby kontynuować.

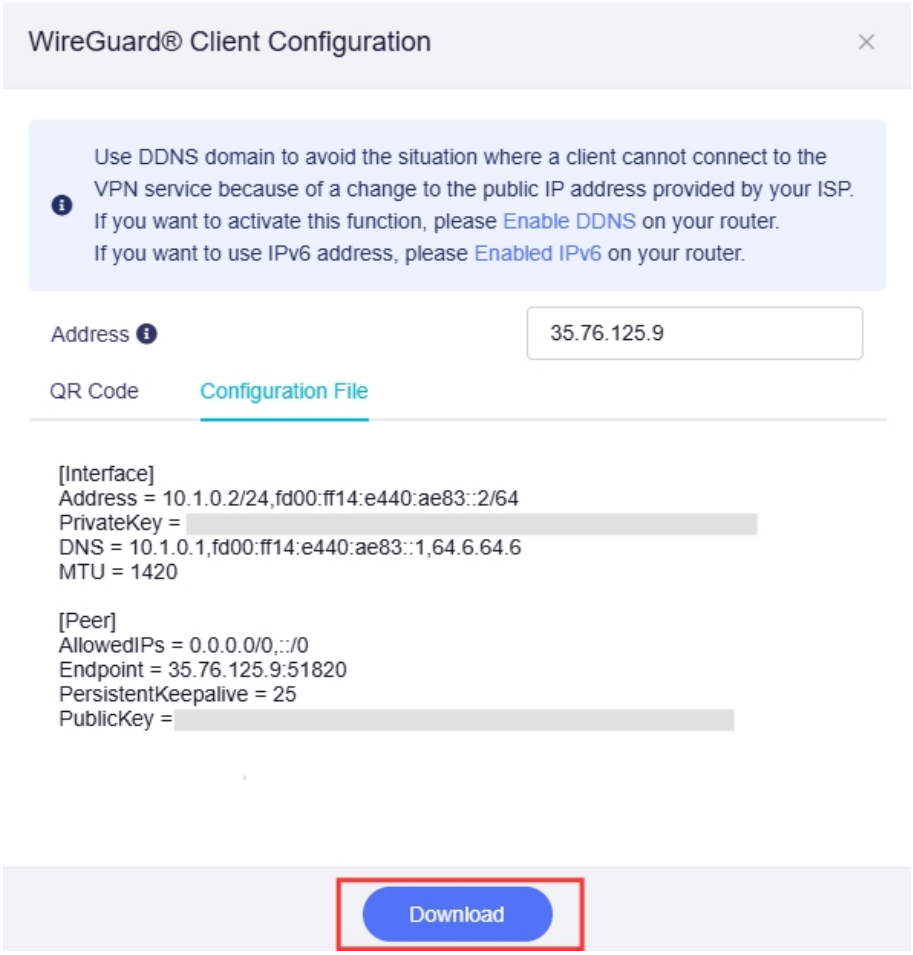


Wskazówka: aby z serwera WireGuard uzyskać dostęp do urządzeń LAN klienta WireGuard, przejdź na kartę **Route Rules** i skonfiguruj reguły routingu. Szczegóły znajdziesz tutaj.

4. Pobierz konfigurację.

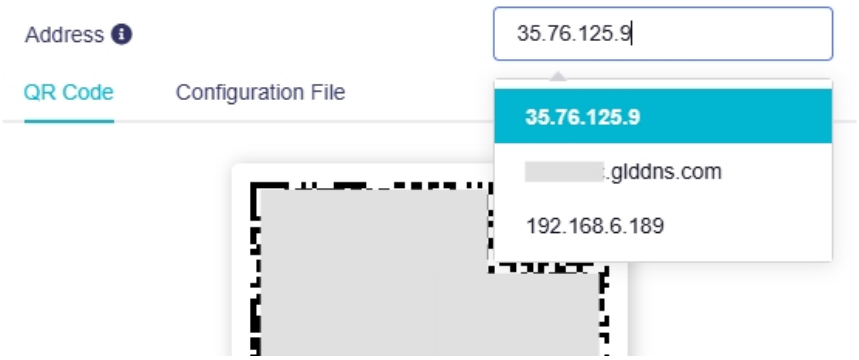
   Po dodaniu profilu router generuje plik konfiguracyjny w trzech postaciach: kodu QR, zwykłego tekstu i pliku .conf. Wybierz preferowany sposób uzyskania konfiguracji.

   - **Kod QR**: odpowiedni dla urządzeń (np. smartfonów, tabletów, laptopów) z zainstalowaną aplikacją WireGuard. Aby skonfigurować urządzenie jako klienta WireGuard, otwórz aplikację WireGuard i zeskanuj kod QR w celu zaimportowania pliku konfiguracyjnego.
   - **Zwykły tekst**: umożliwia sprawdzenie szczegółów konfiguracji oraz wygodne skopiowanie i wklejenie ich w innym miejscu do ręcznej konfiguracji, np. w aplikacji WireGuard lub na routerze GL.iNet.
   - **Plik .conf**: kliknij przycisk **Download**, aby zapisać plik .conf na urządzeniu lokalnym. Można go następnie bezpośrednio przesłać do aplikacji WireGuard lub routera GL.iNet.



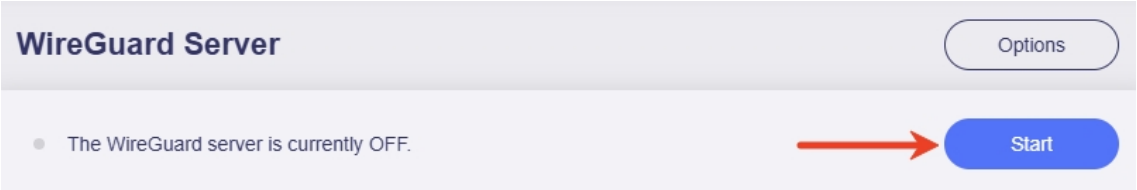
Wskazówki:

- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.
- Od wersji oprogramowania 4.8 przed wyeksportowaniem pliku konfiguracyjnego można wybrać adres serwera z listy: publiczny adres IP, domenę DDNS lub bieżący adres IP WAN. Po wybraniu adres serwera w pliku konfiguracyjnym zostanie automatycznie zaktualizowany. Pobierz plik konfiguracyjny ponownie, jeśli adres serwera ulegnie zmianie.

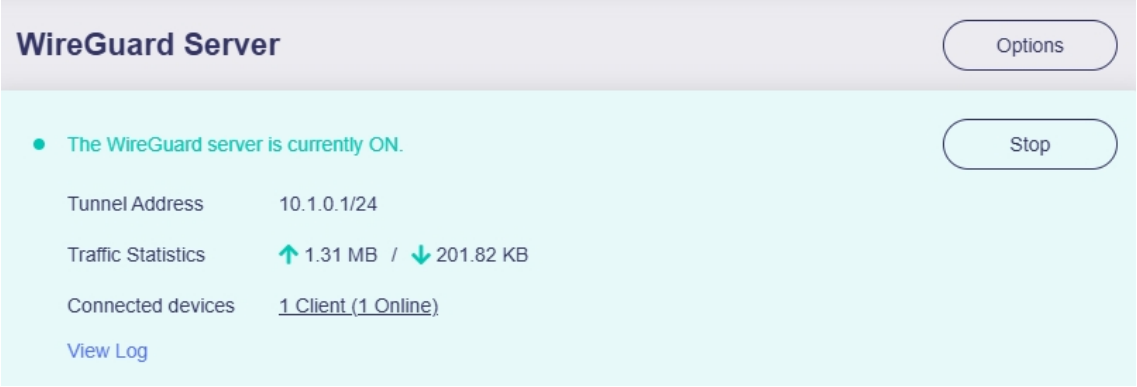


5. Uruchom serwer WireGuard.

   Na stronie **WireGuard Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



   Stan połączenia serwera jest wyświetlany u góry. Jeśli widoczne są statystyki wysyłania i pobierania oraz podłączone urządzenia online, serwer WireGuard działa.

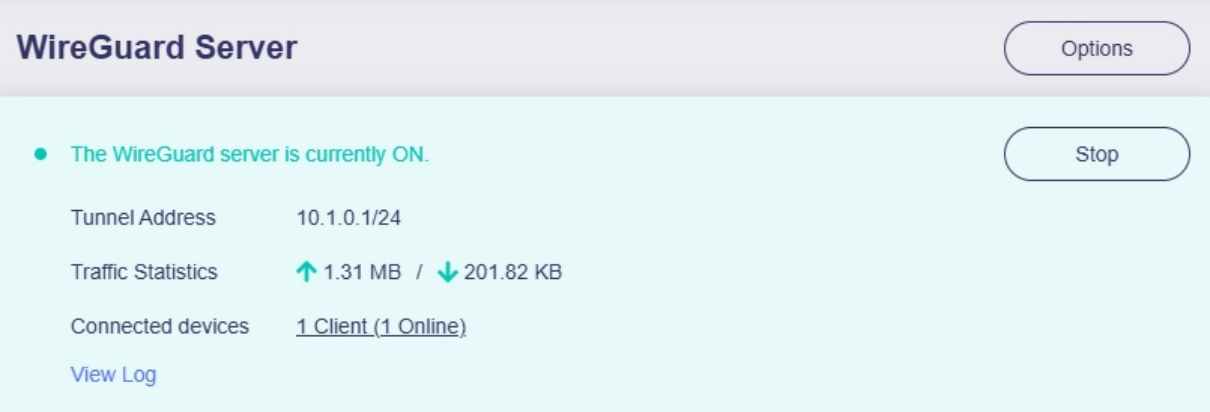


10.2.3 Sprawdzanie połączenia

Metoda 1. Sprawdzanie stanu serwera

W oprogramowaniu sprzętowym w wersji 4.8 możesz sprawdzić stan połączenia serwera na stronie **WireGuard Server**.

Jeśli wyświetlane są statystyki wysyłania i pobierania danych oraz połączone urządzenia online, serwer WireGuard działa i ma połączonych klientów.



Jeśli wyświetlane są zerowy ruch i zero klientów, żaden klient WireGuard nie jest połączony.



Metoda 2. Sprawdzanie adresu IP klienta

Zaimportuj wcześniej wyeksportowaną konfigurację WireGuard do urządzenia w innej sieci (poza siecią lokalną serwera). Następnie otwórz przeglądarkę i wyszukaj swój adres IP oraz lokalizację. Jeśli odpowiadają adresowi IP i lokalizacji serwera VPN (zamiast adresowi dostawcy Internetu), połączenie VPN działa prawidłowo.

Poniżej przedstawiono przykład weryfikacji przy użyciu smartfona z zainstalowaną oficjalną aplikacją WireGuard.

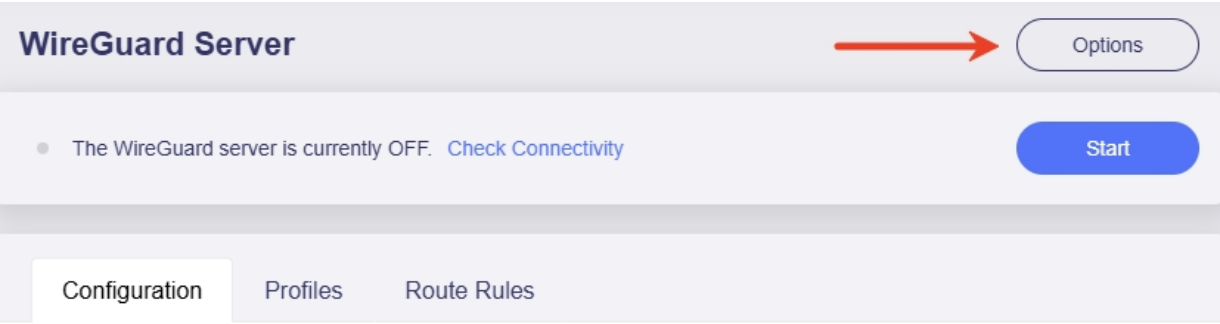
1. Najpierw wyłącz Wi-Fi w smartfonie i pozostaw włączoną wyłącznie transmisję danych komórkowych (4G/5G).
2. Następnie otwórz aplikację WireGuard, zaimportuj plik konfiguracyjny i rozpocznij połączenie.
3. Sprawdź, czy smartfon ma dostęp do Internetu i czy jego adres IP odpowiada adresowi IP serwera WireGuard.

Jeśli połączenie się nie powiedzie, przyczyną może być jeden z typowych problemów:

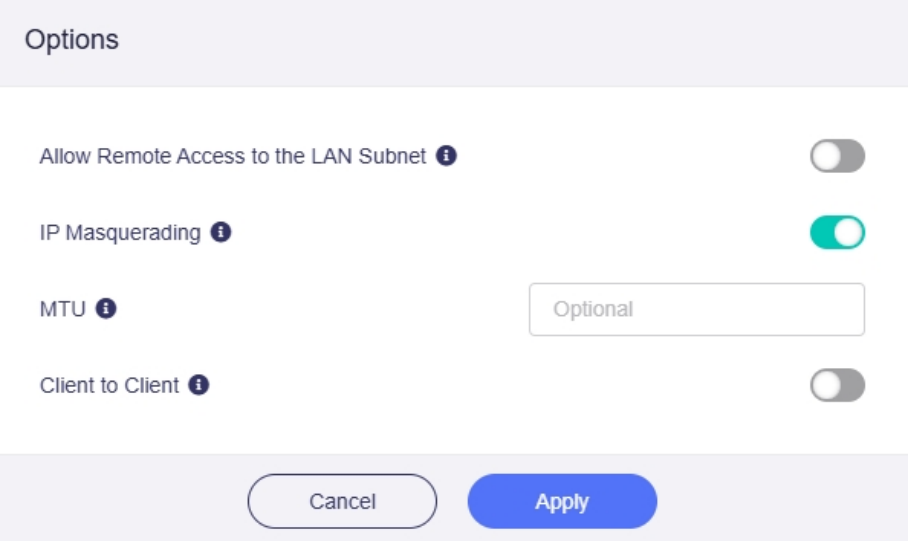
- Serwer VPN nie ma publicznego adresu IP. Szczegóły znajdziesz w sekcji **10.2.1 Przygotowanie**.
- Może być konieczne skonfigurowanie przekierowania portów. Szczegóły znajdziesz w sekcji **10.2.1 Przygotowanie** .
- Port używany przez serwer WireGuard jest blokowany przez dostawcę Internetu. Zmień port lub skontaktuj się z dostawcą w celu uzyskania pomocy.
- Połączenie VPN może być blokowane w niektórych krajach lub regionach.

10.2.4 Opcje serwera

Opcje serwera obejmują zaawansowane ustawienia po stronie serwera, takie jak zdalny dostęp do jego sieci LAN czy maskowanie adresów IP. Skonfiguruj je zgodnie ze swoimi potrzebami. Na stronie **WireGuard Server** kliknij **Options** w prawym górnym rogu.



W wyskakującym oknie pojawią się poniższe funkcje.



- **Allow Remote Access to the LAN Subnet**: po włączeniu zasoby w podsieci LAN serwera będą dostępne przez tunel VPN.
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tę opcję tylko w konfiguracjach sieć–sieć, w których zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: skrót od Maximum Transmission Unit, czyli maksymalnej jednostki transmisji. Wartość MTU ustawiona dla tunelu zastępuje ustawienia MTU w pliku konfiguracyjnym.
- **Client to Client**: po włączeniu klienci VPN połączeni z tym serwerem mogą uzyskiwać wzajemny dostęp przez swoje adresy IP tunelu VPN.
  Pamiętaj, że Client to Client rozgłasza wyłącznie adres IP tunelu każdego klienta. Nie udostępnia automatycznie podsieci lokalnych LAN znajdujących się za klientami VPN. Aby umożliwić klientom wzajemny dostęp do ich podsieci LAN, dodaj na serwerze VPN reguły routingu rozgłaszające te zdalne podsieci.

Rozdział 11

Konfiguracja klienta VPN

W tym rozdziale opisano konfigurację routera GL.iNet jako klienta OpenVPN lub WireGuard.

11.1 Klient OpenVPN

11.1.1 Przygotowanie

Najpierw upewnij się, że masz aktywną subskrypcję u dostawcy VPN obsługującego ręczną konfigurację OpenVPN. Listę dostawców OpenVPN zgodnych z GL.iNet znajdziesz tutaj.

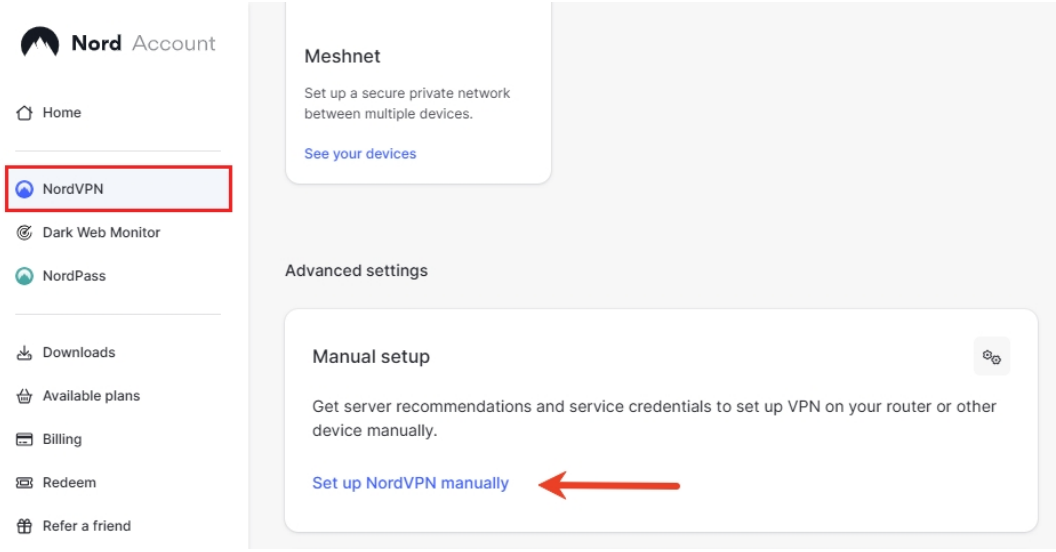
Następnie odwiedź oficjalną witrynę dostawcy VPN, którego usługę subskrybujesz, i uzyskaj dane dostępowe usługi lub plik konfiguracyjny. Jeśli nie wiesz, jak uzyskać plik konfiguracyjny, skorzystaj z tego łącza lub skontaktuj się z pomocą techniczną dostawcy.

11.1.2 Konfiguracja NordVPN

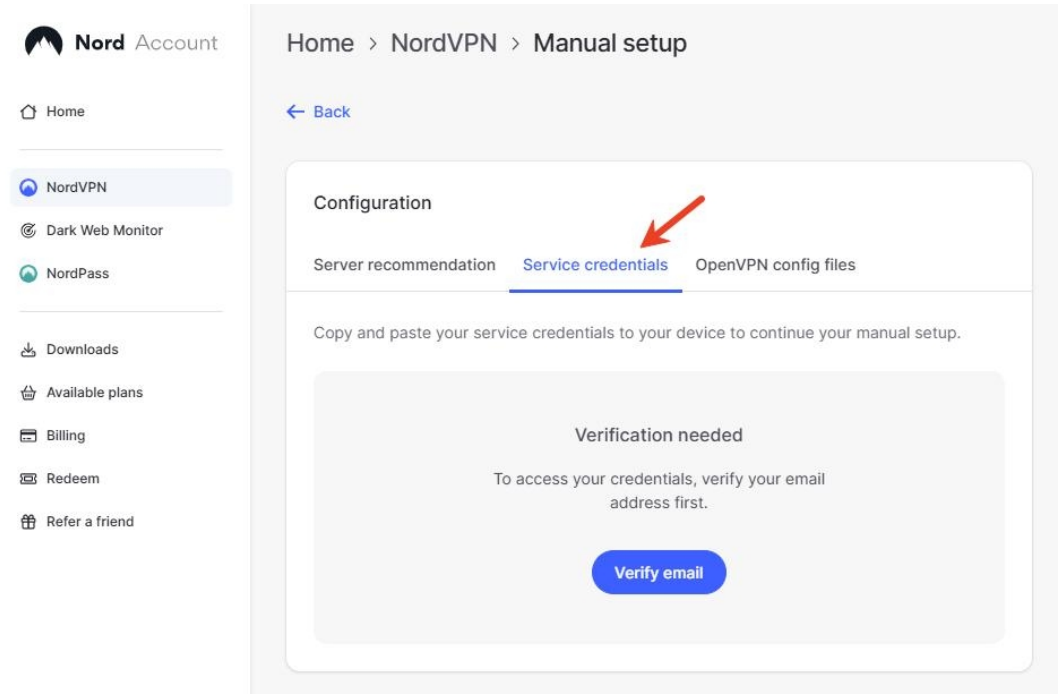
NordVPN jest zintegrowany z panelem administracyjnym GL.iNet. Pliki konfiguracyjne wszystkich serwerów NordVPN można uzyskać, wprowadzając dane dostępowe konta (z panelu NordVPN) w panelu administracyjnym routera lub aplikacji mobilnej GL.iNet. Eliminuje to potrzebę ręcznego przesyłania plików.

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

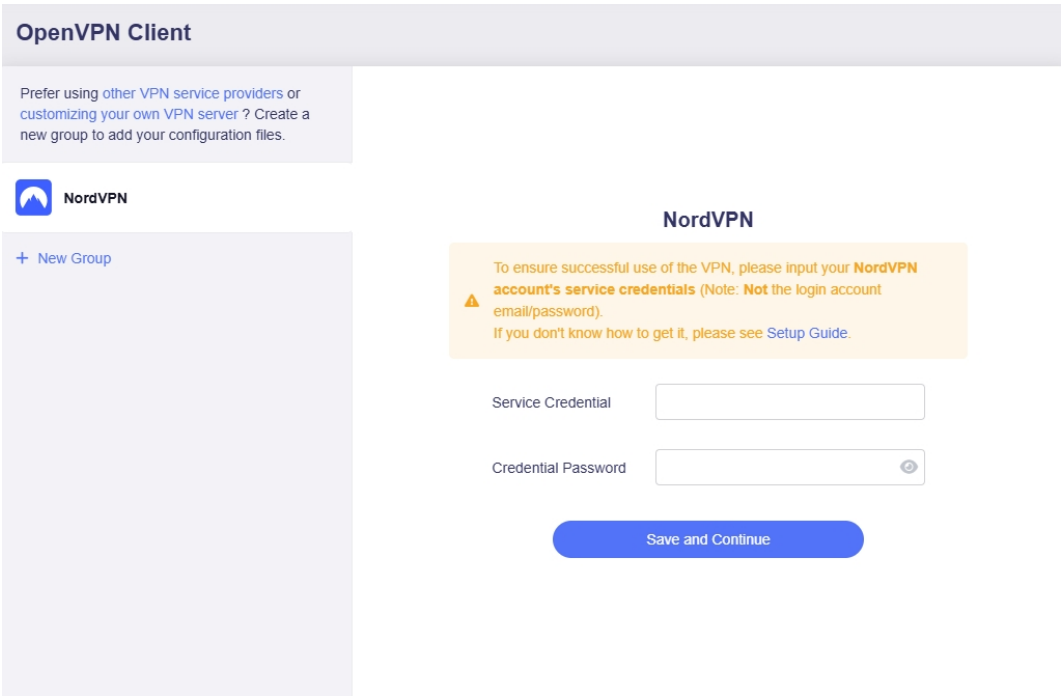
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



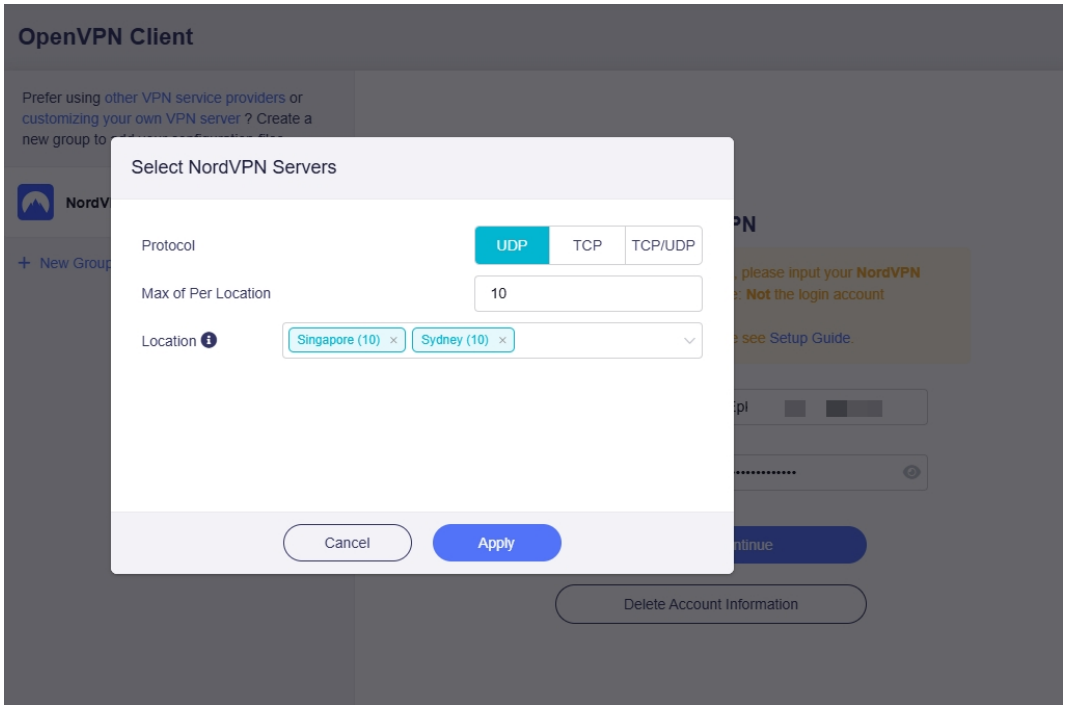
Znajdziesz tam **dane dostępowe usługi**. Skopiuj je do późniejszego użycia.



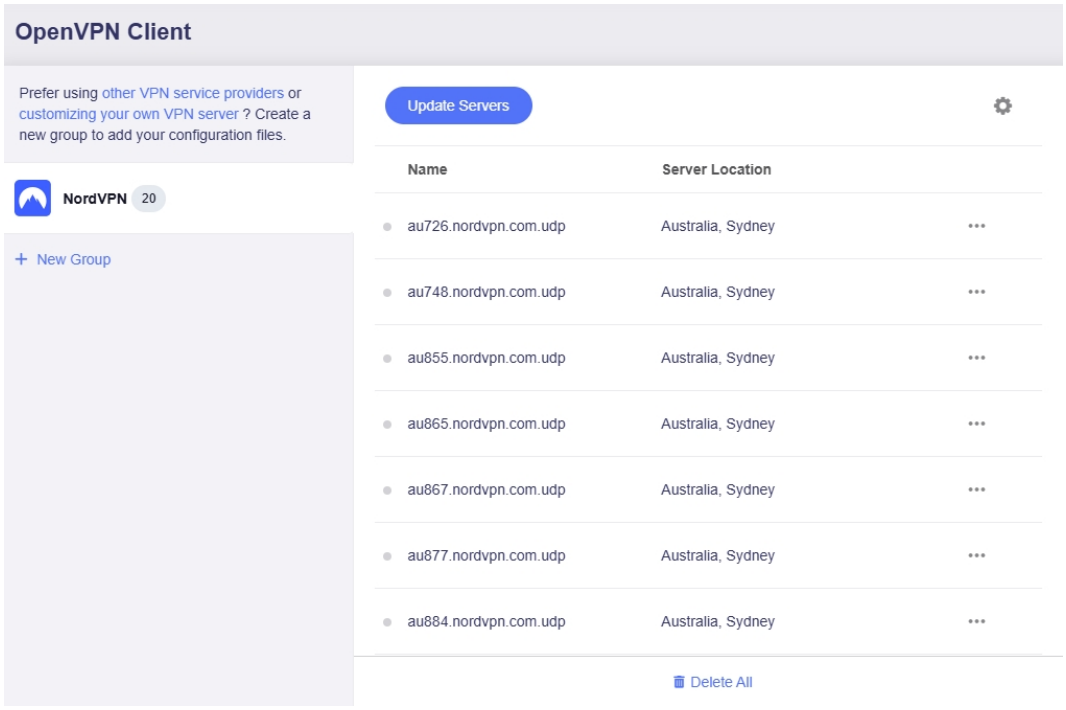
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **OpenVPN Client** > **NordVPN**. Wprowadź dane dostępowe usługi (uwaga: NIE jest to adres e-mail ani hasło do logowania na konto), a następnie kliknij **Save and Continue**.



4. Wybierz protokół, maksymalną liczbę serwerów dla każdej lokalizacji oraz lokalizacje, a następnie kliknij **Apply**.

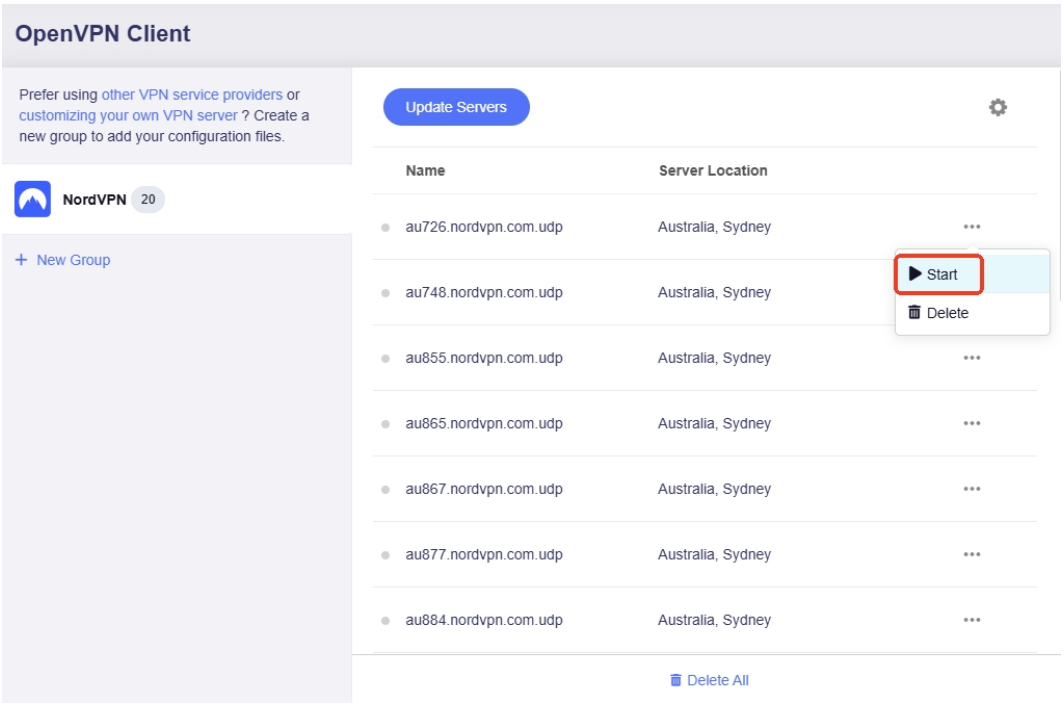


Rozpocznie się pobieranie plików konfiguracyjnych.

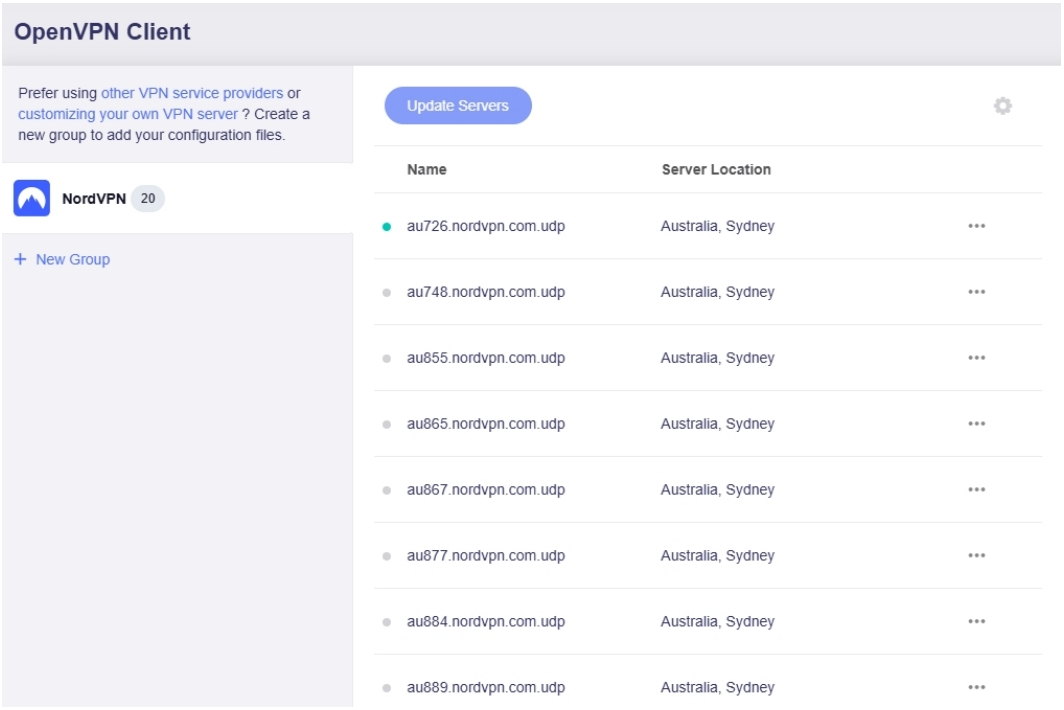


5. Nawiąż połączenie.

   Wybierz serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



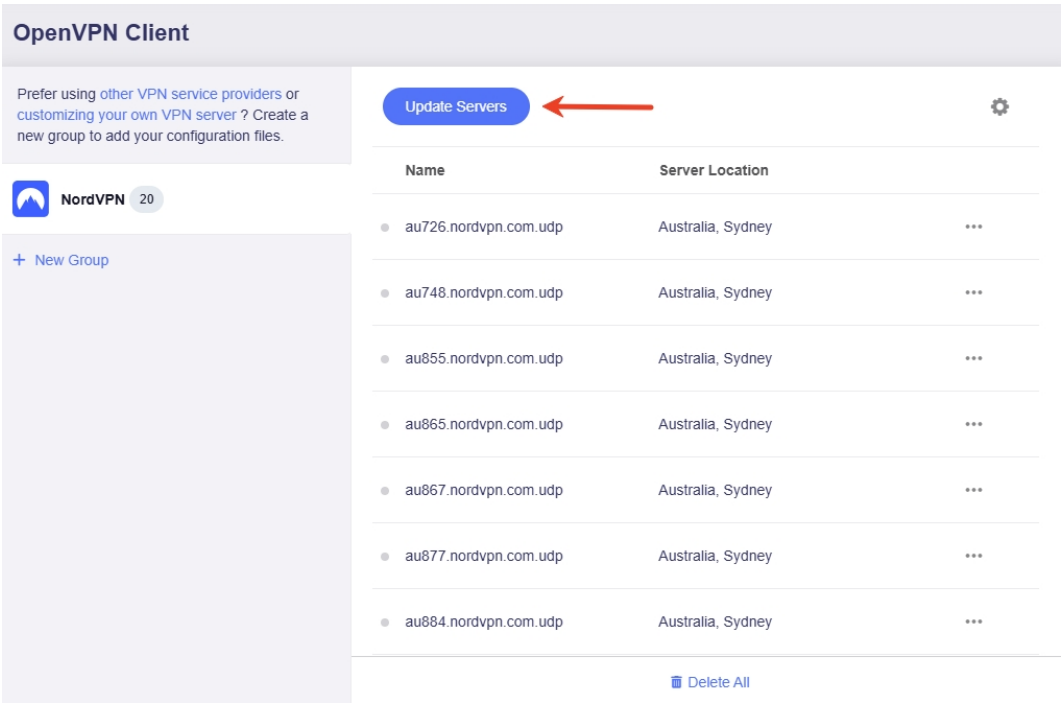
6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

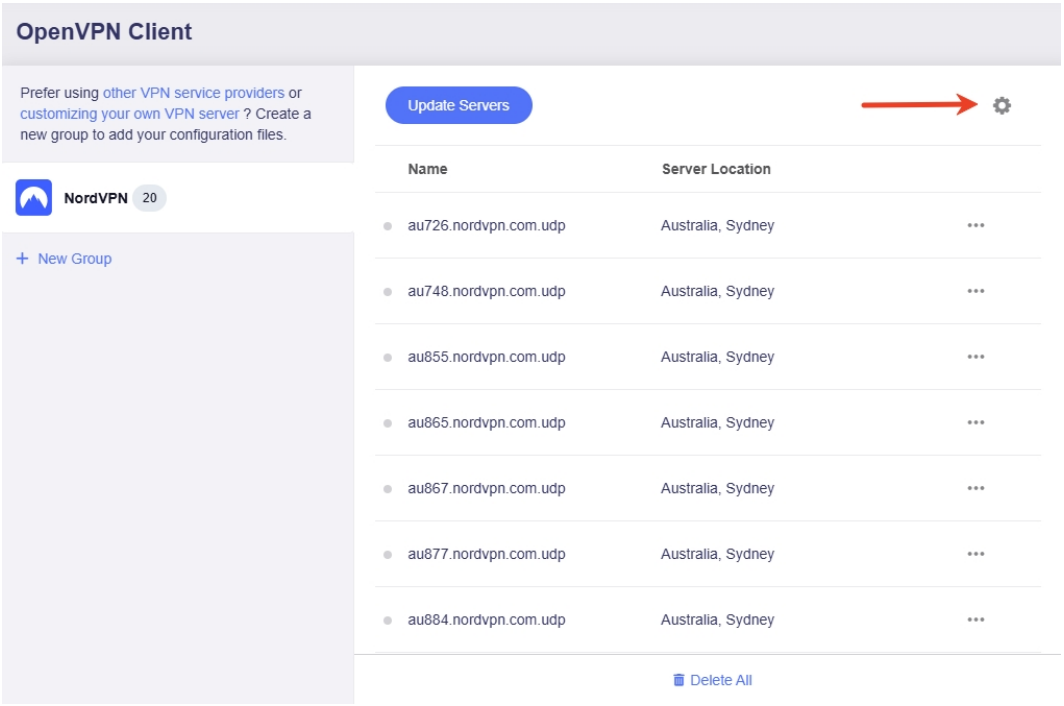
7. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



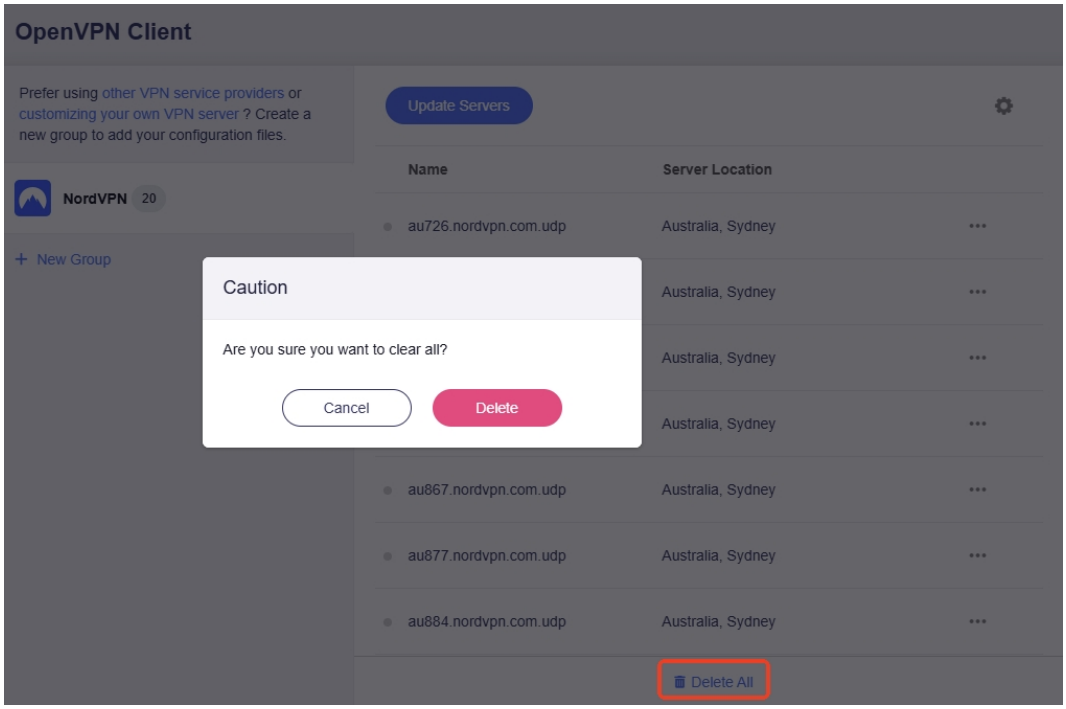
8. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



9. Usuń wszystkie pliki.

   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne.

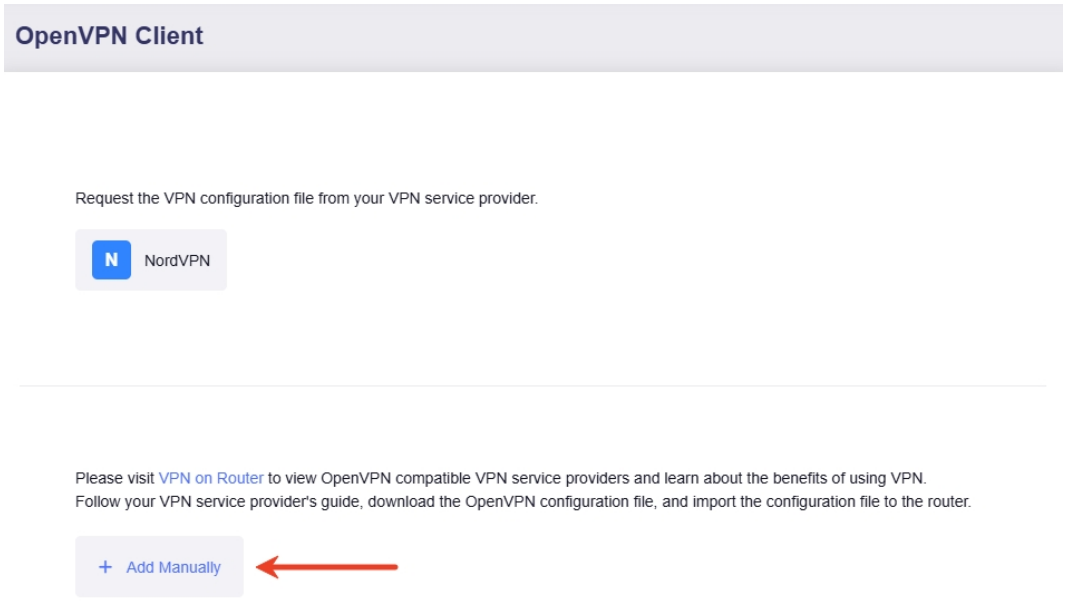

OpenVPN Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
NordVPN 20
New Group
Update Servers
Name
Server Location
au726.nordvpn.com.udp
Australia, Sydney
Australia, Sydney
Australia, Sydney
Australia, Sydney
au867.nordvpn.com.udp
Australia, Sydney
au877.nordvpn.com.udp
Australia, Sydney
au884.nordvpn.com.udp
Australia, Sydney
Delete All
Caution
Are you sure you want to clear all?
Cancel
Delete

11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy)

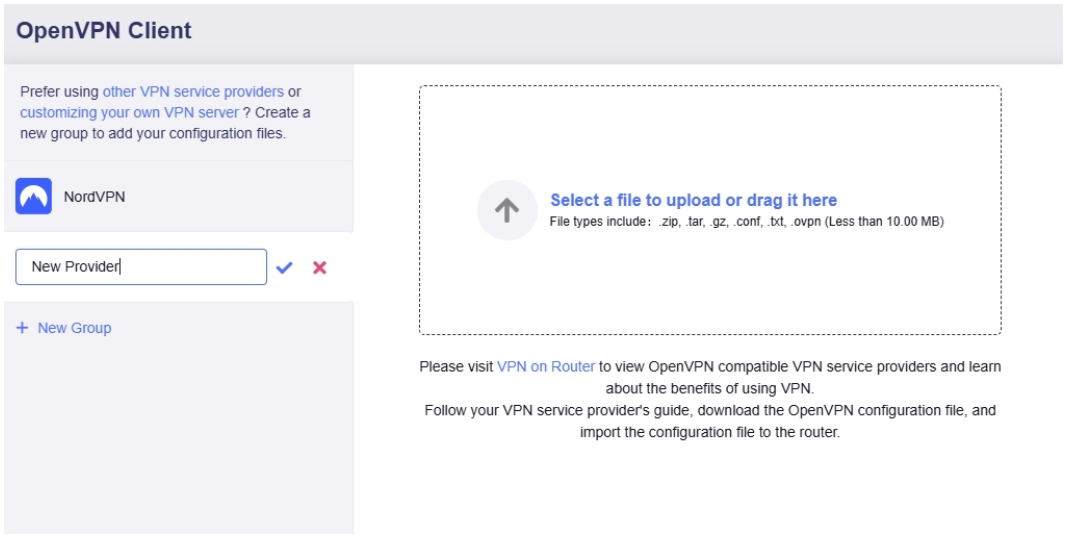
Jeśli Twój dostawca OpenVPN nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta OpenVPN.

W poniższych krokach jako przykład wykorzystano PIA (Private Internet Access).

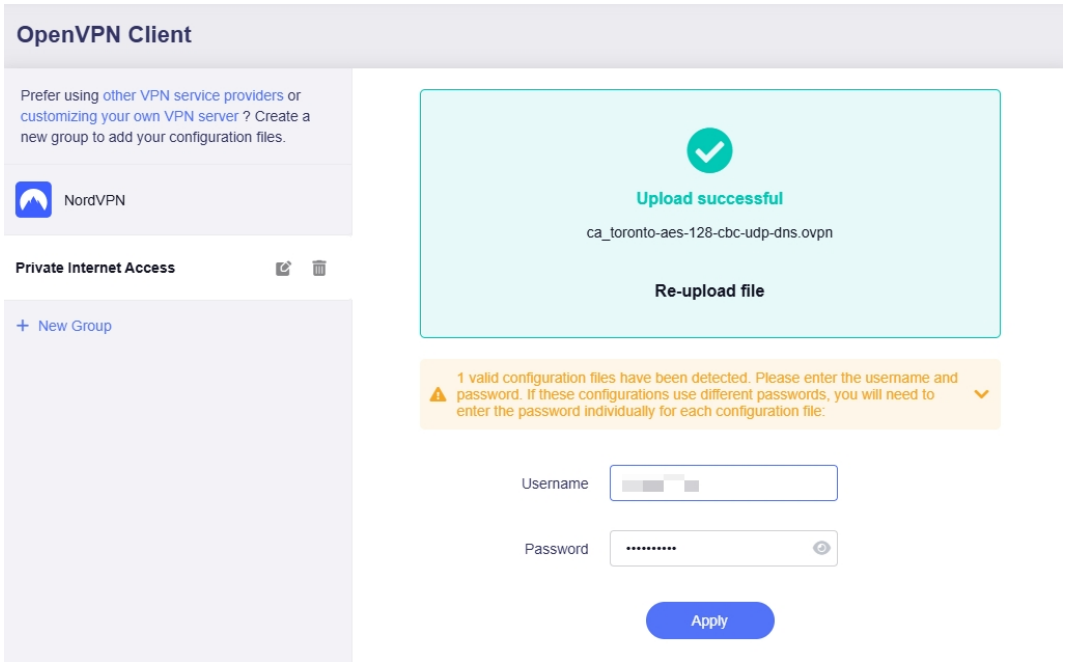
1. Pobierz plik konfiguracyjny z oficjalnej witryny Private Internet Access.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Client** i kliknij **Add Manually**.



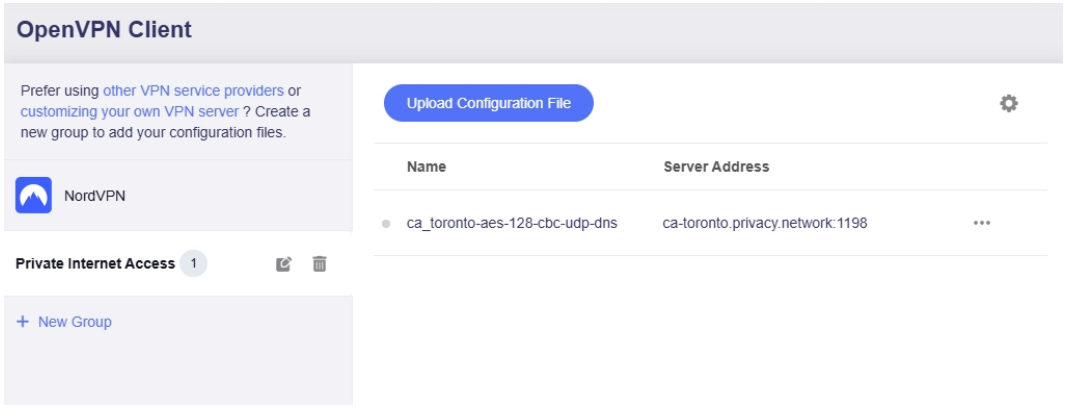
3. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



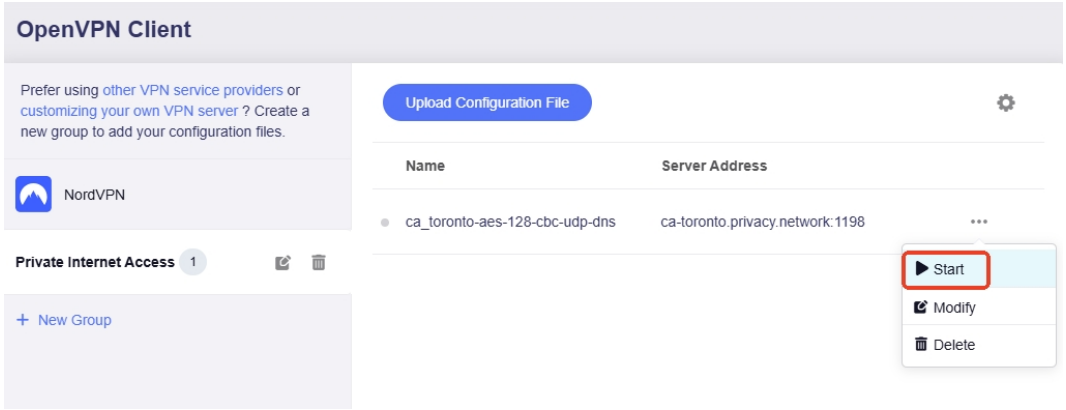
4. Prześlij plik konfiguracyjny OpenVPN. Jeśli jest to wymagane, wprowadź dane dostępowe, a następnie kliknij **Apply**.



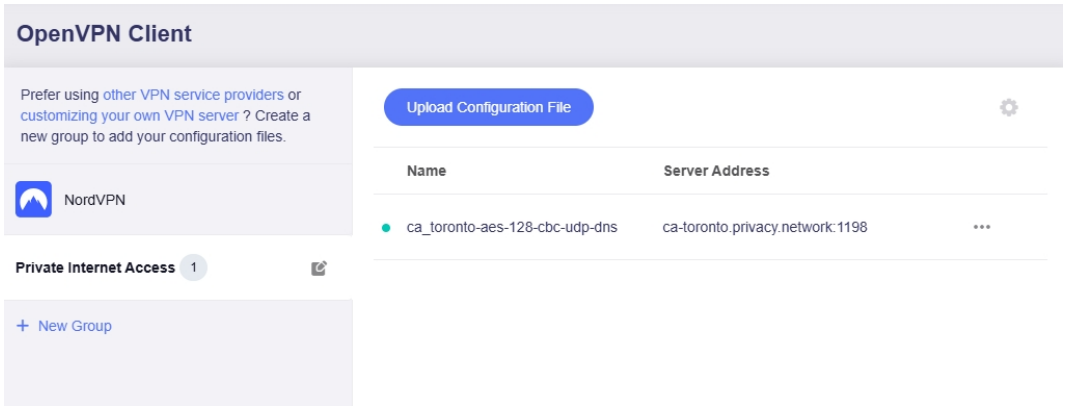
Pojawi się przesłany plik konfiguracyjny.



5. Kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

11.2 Konfiguracja klienta WireGuard

Klienta WireGuard® można skonfigurować w aplikacji mobilnej GL.iNet lub internetowym panelu administracyjnym.

- Aplikacja mobilna integruje niektórych dostawców usług WireGuard, takich jak AzireVPN, Mullvad VPN, OVPN, StrongVPN i PIA VPN. Wystarczy wprowadzić dane logowania do subskrybowanej usługi WireGuard. Otwórz aplikację i postępuj zgodnie z instrukcjami na ekranie, aby wykonać konfigurację.
- Panel administracyjny integruje niektórych dostawców usług WireGuard i umożliwia również ręczną konfigurację. Możesz wprowadzić dane dostępowe subskrybowanej usługi WireGuard w celu szybkiej konfiguracji lub ręcznie przesłać plik konfiguracyjny.

*WireGuard® jest zastrzeżonym znakiem towarowym Jasona A. Donenfelda.

11.2.1 Przygotowanie

Najpierw upewnij się, że masz aktywną subskrypcję u dostawcy VPN obsługującego ręczną konfigurację WireGuard. Listę dostawców WireGuard zgodnych z GL.iNet znajdziesz tutaj.

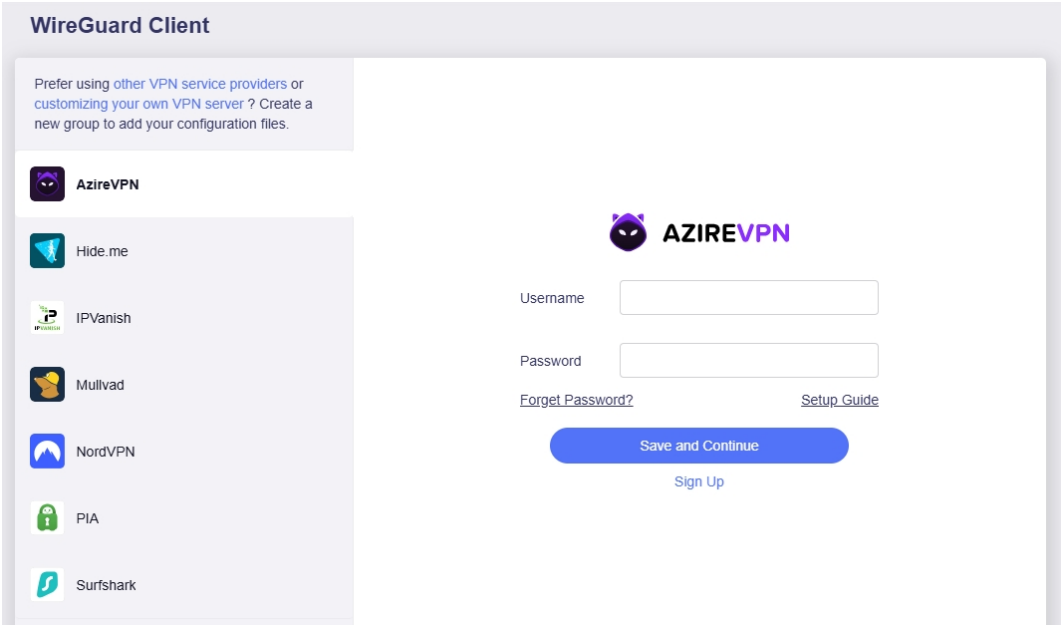
Następnie wybierz poniżej odpowiedniego dostawcę WireGuard, aby szybko przejść do instrukcji krok po kroku.

- Konfiguracja AzireVPN
- Konfiguracja Hide.me
- Konfiguracja IPVanish
- Konfiguracja Mullvad
- Konfiguracja NordVPN
- Konfiguracja PIA (Private Internet Access)
- Konfiguracja Surfshark
- Ręczna konfiguracja klienta WireGuard (inni dostawcy)

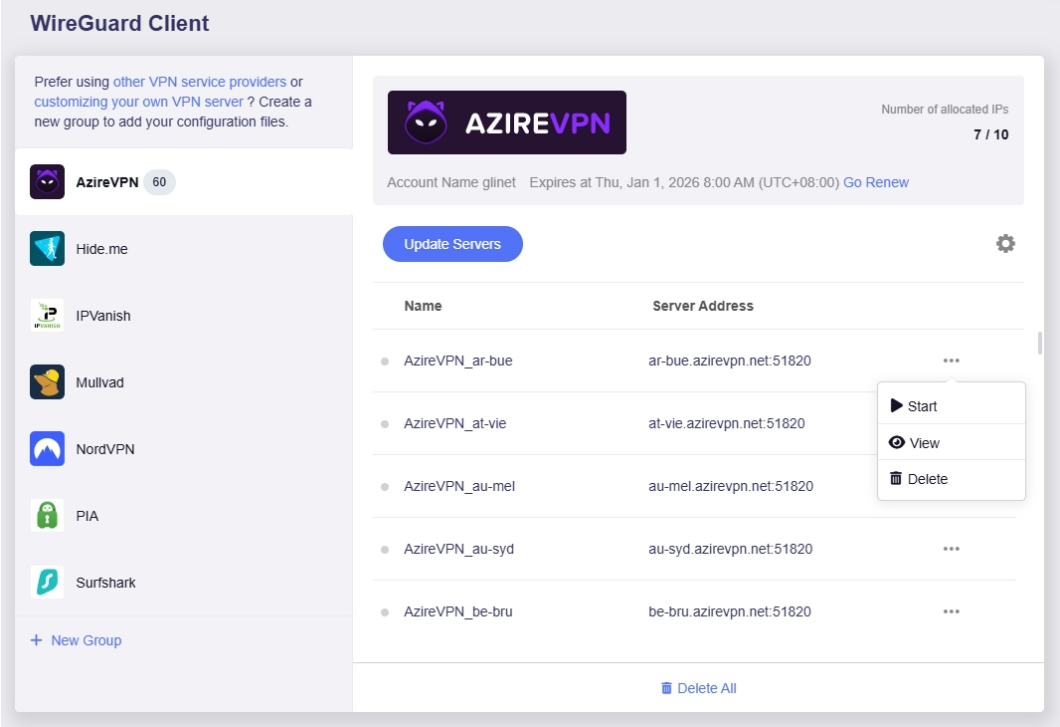
11.2.2 Konfiguracja AzireVPN

Aby skonfigurować router jako klienta AzireVPN, wykonaj poniższe czynności.

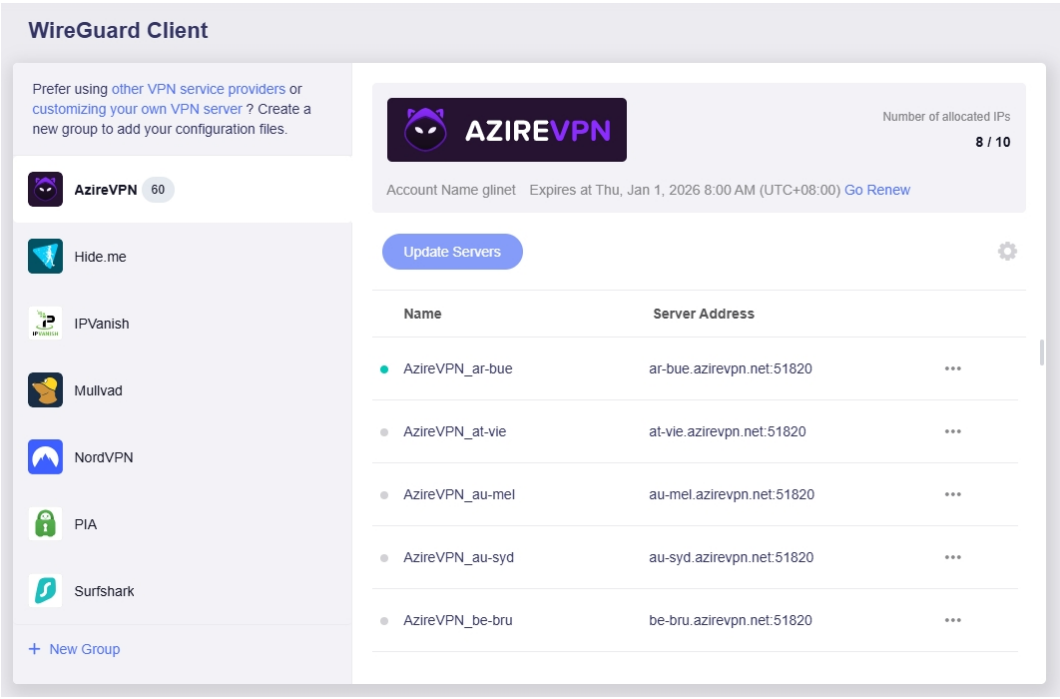
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **AzireVPN**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



3. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



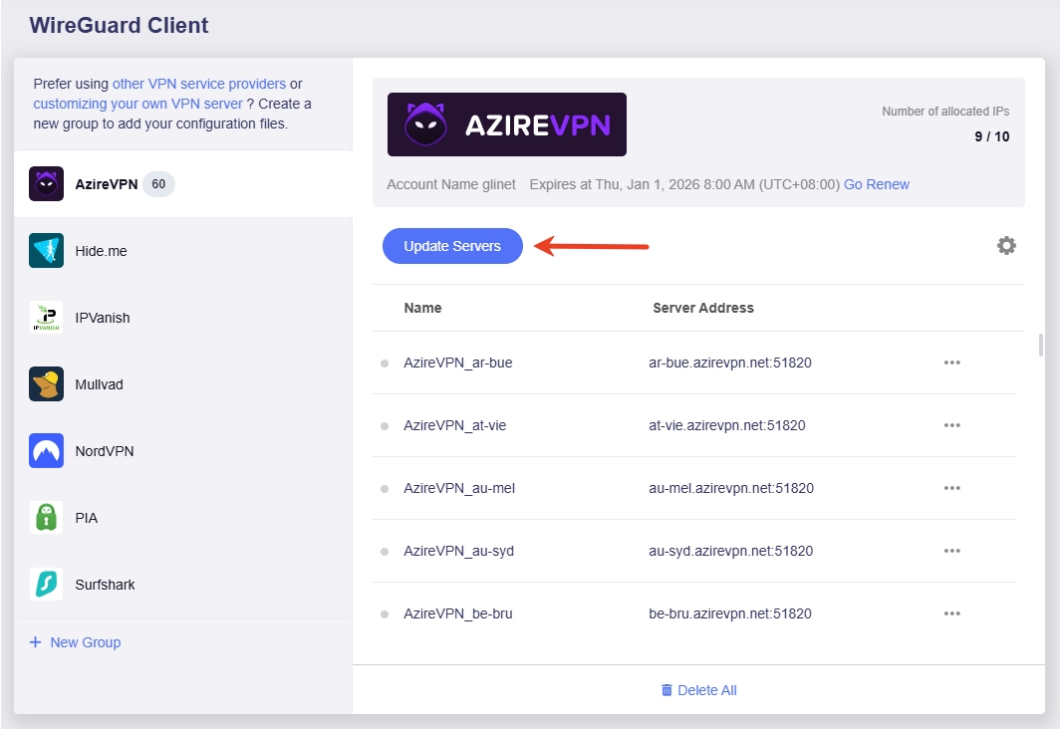
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

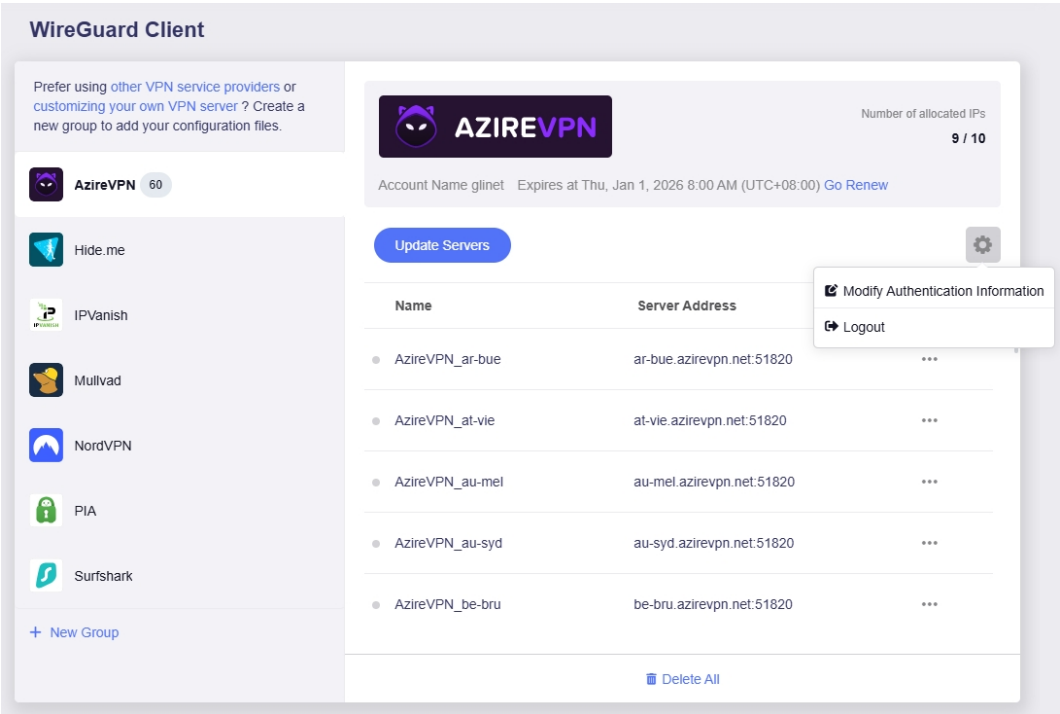
5. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



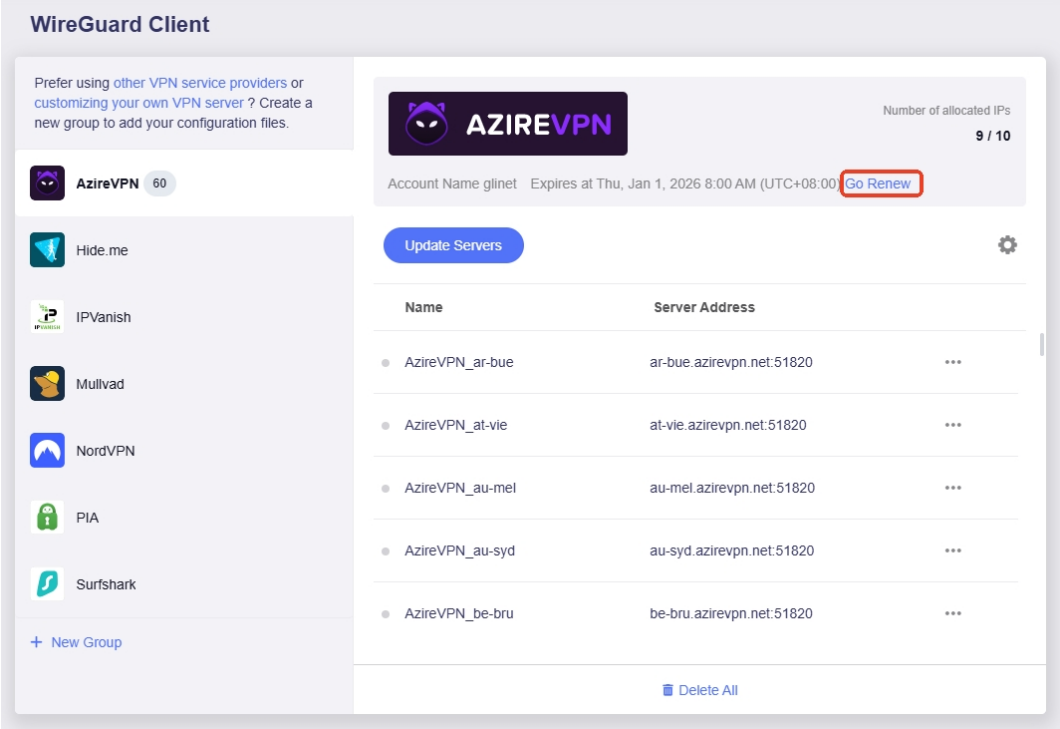
6. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



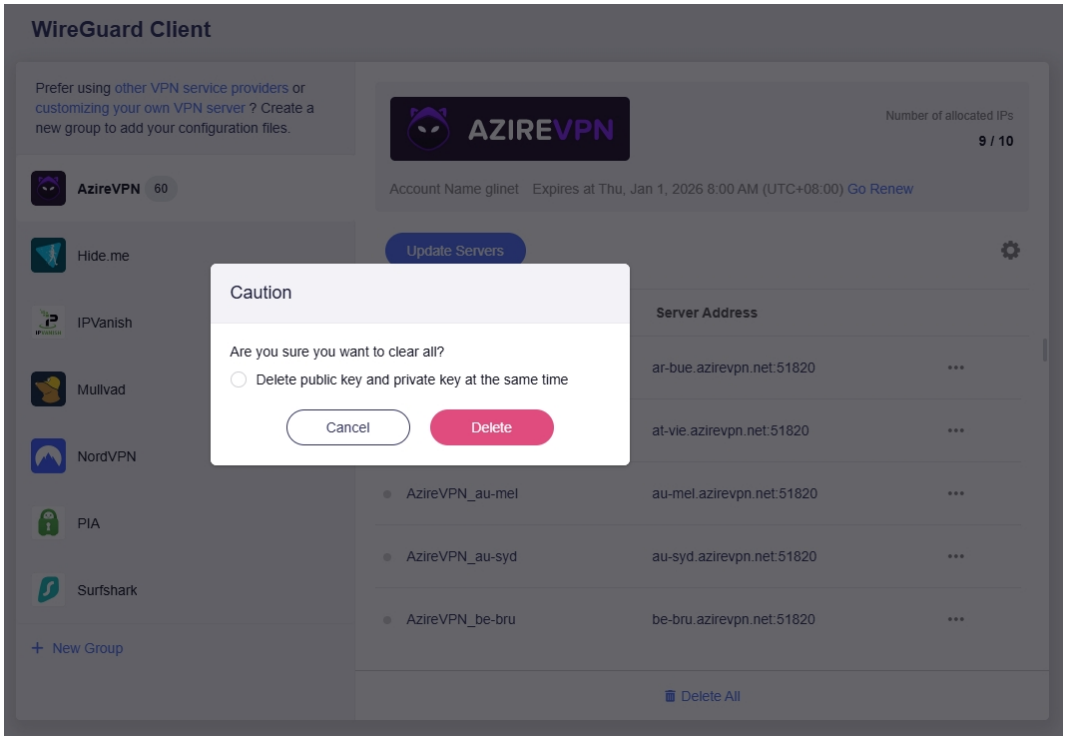
7. Odnowienie subskrypcji.

   Po kliknięciu **Go Renew** nastąpi przekierowanie na oficjalną stronę w celu odnowienia subskrypcji.



8. Usuń wszystkie pliki.

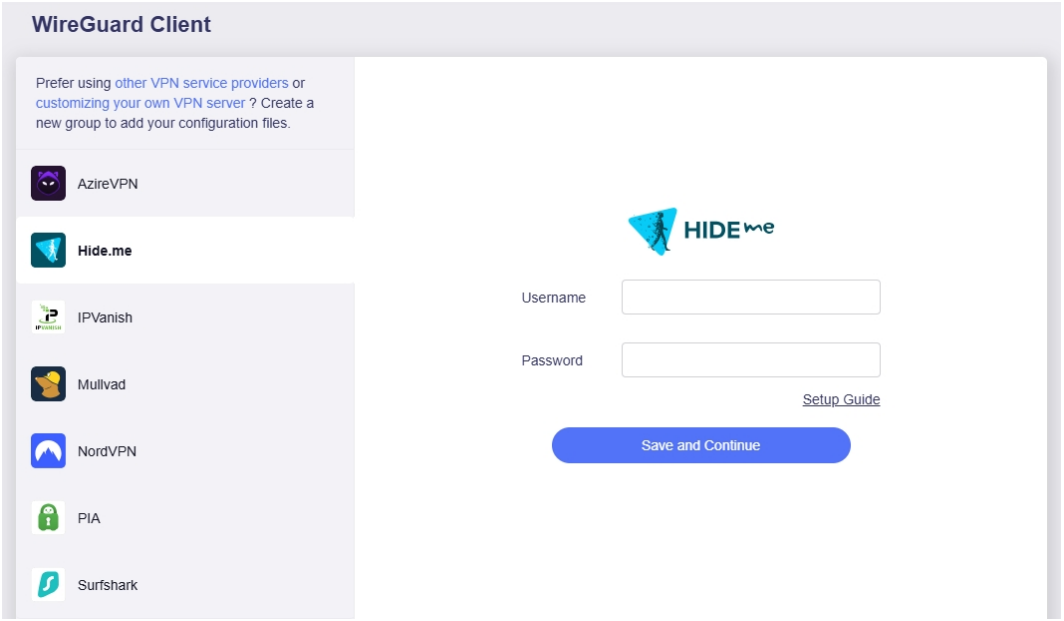
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



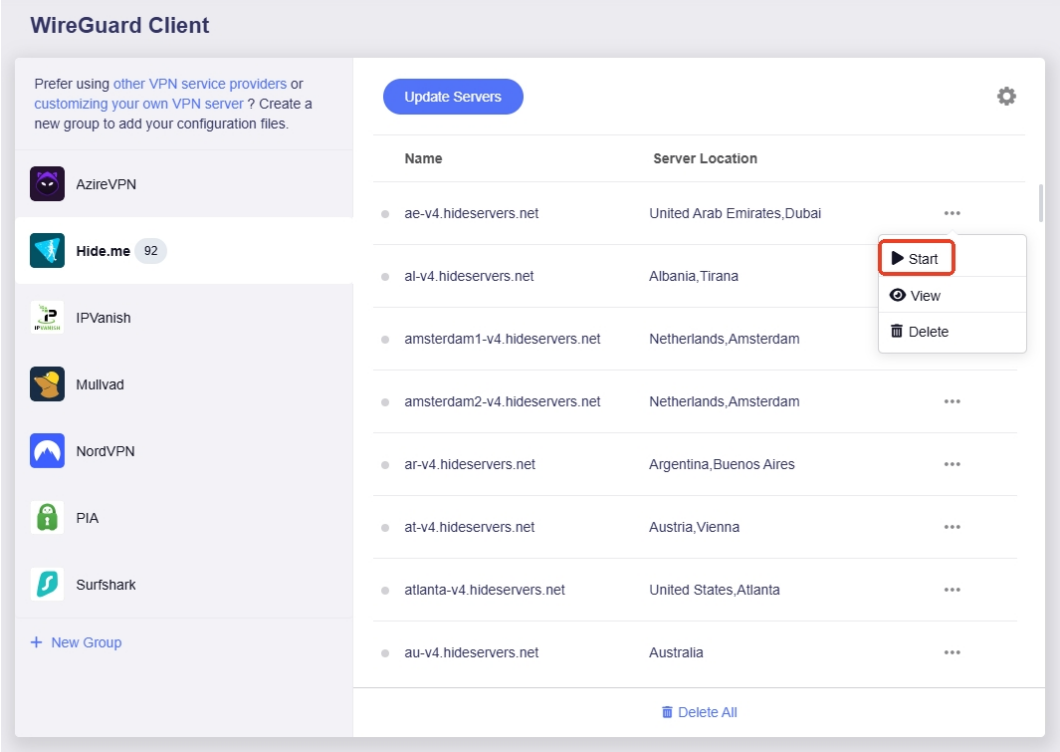
11.2.3 Konfiguracja Hide.me

Aby skonfigurować router jako klienta Hide.me, wykonaj poniższe czynności.

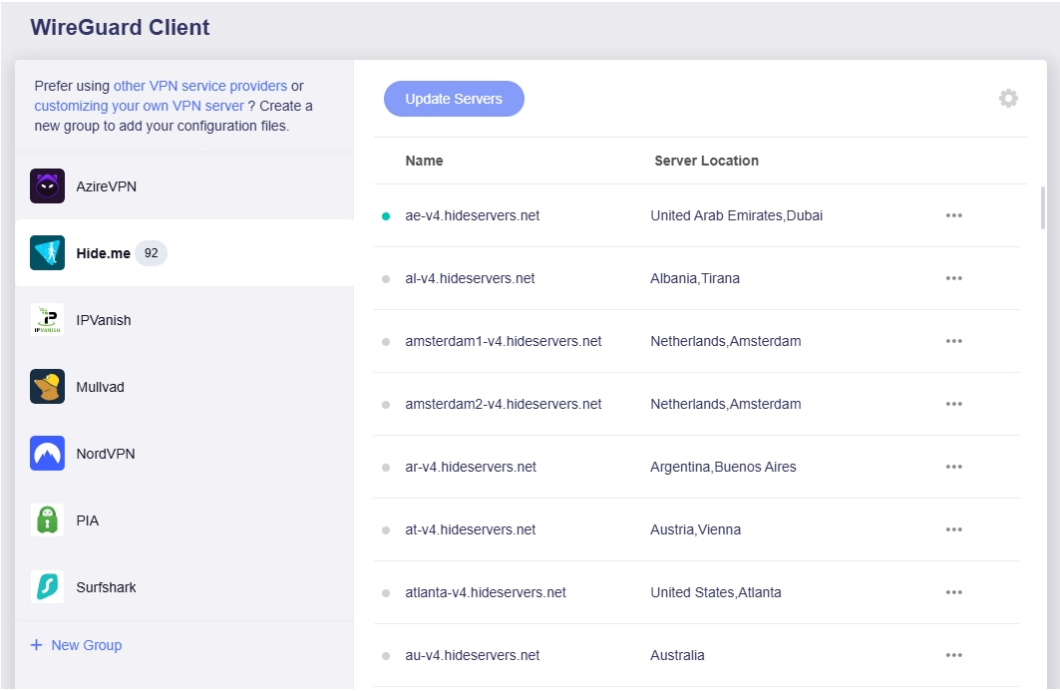
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Hide.me**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



3. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



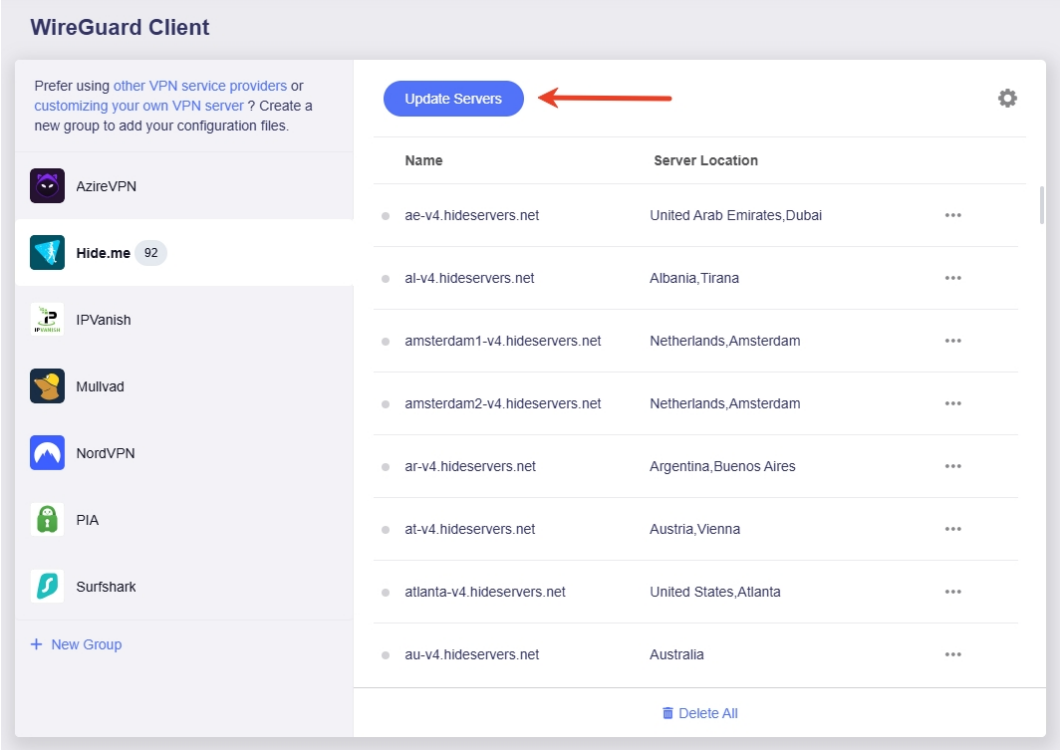
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

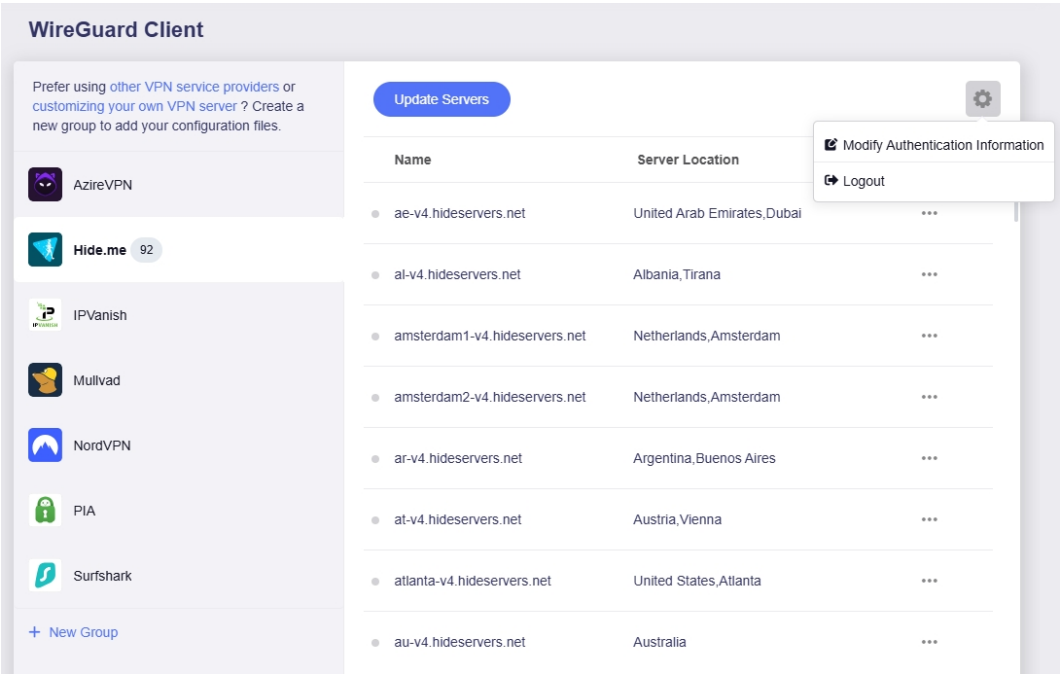
5. Zaktualizuj serwery.

Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



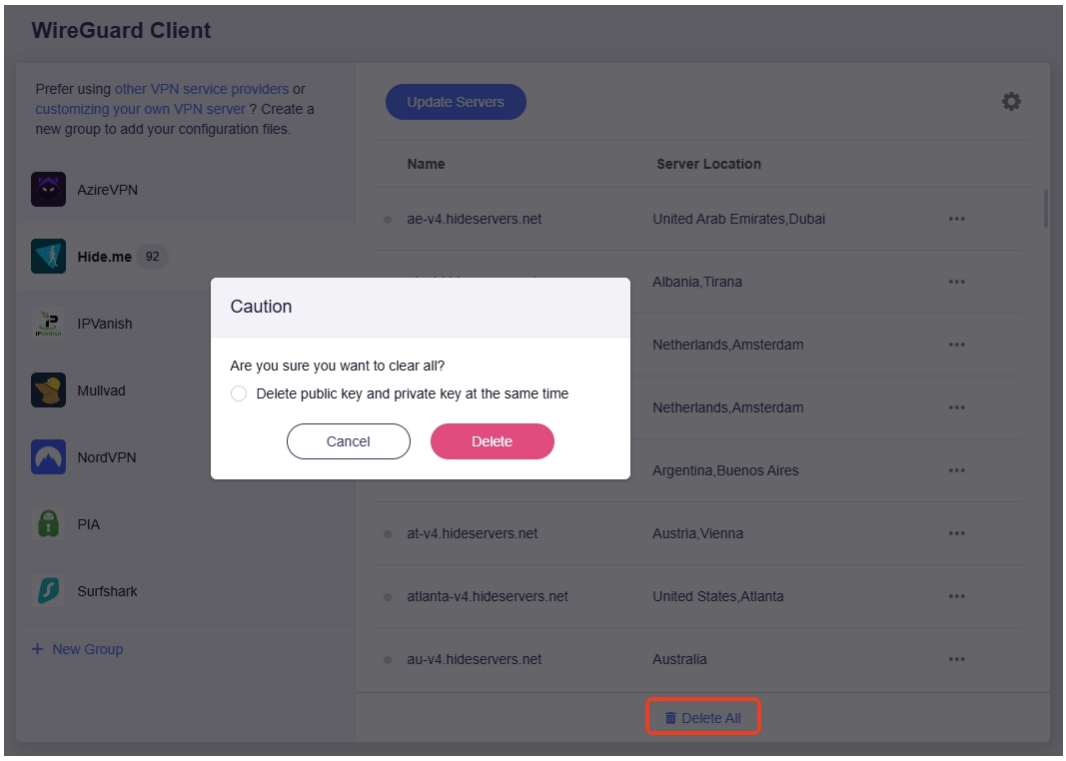
6. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



7. Usuń wszystkie pliki.

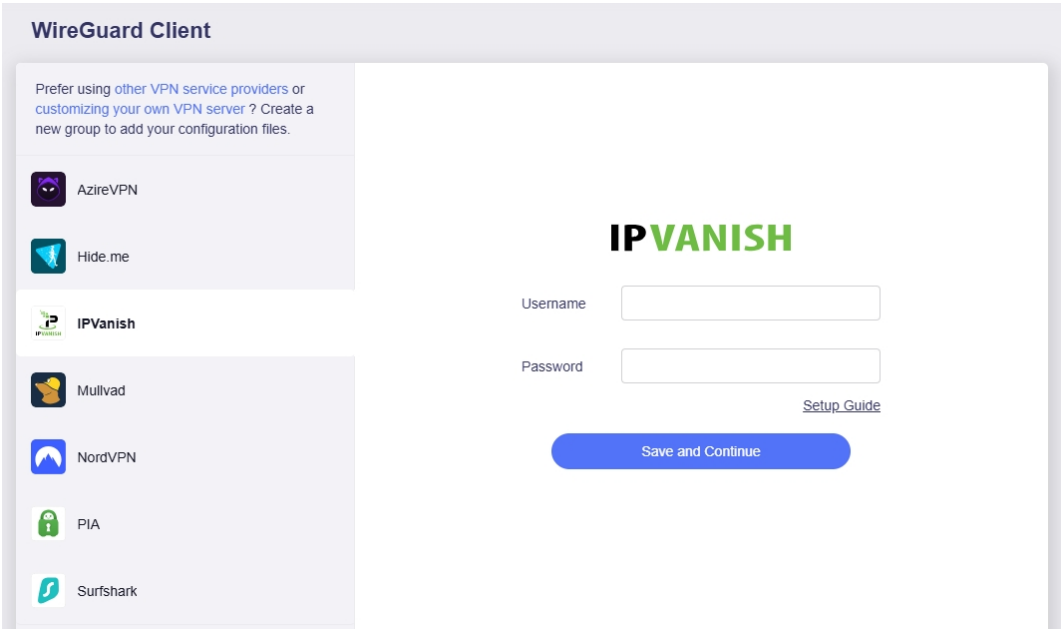
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



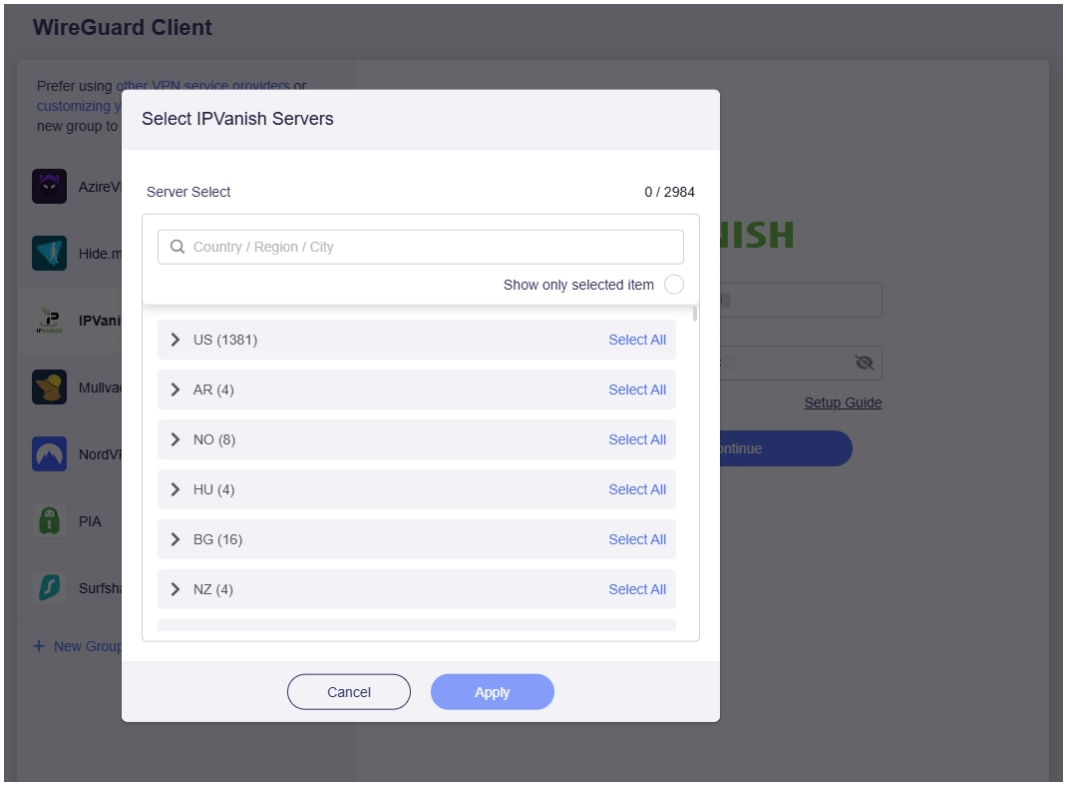
11.2.4 Konfiguracja IPVanish

Aby skonfigurować router jako klienta IPVanish, wykonaj poniższe czynności.

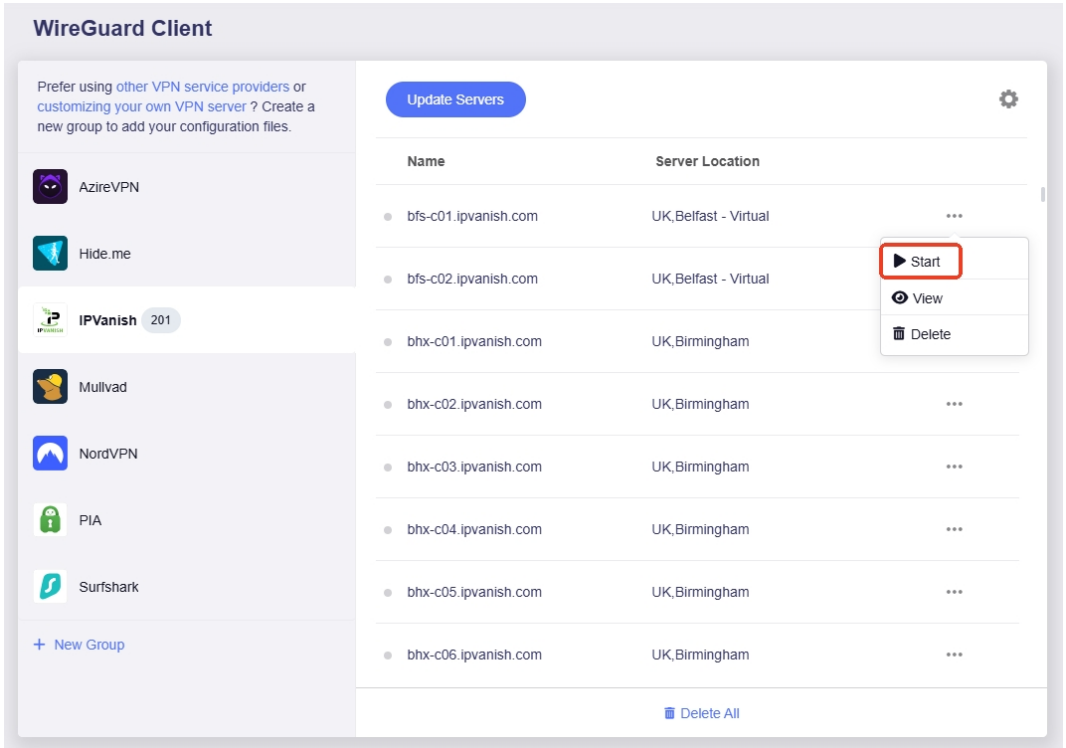
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **IPVanish**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



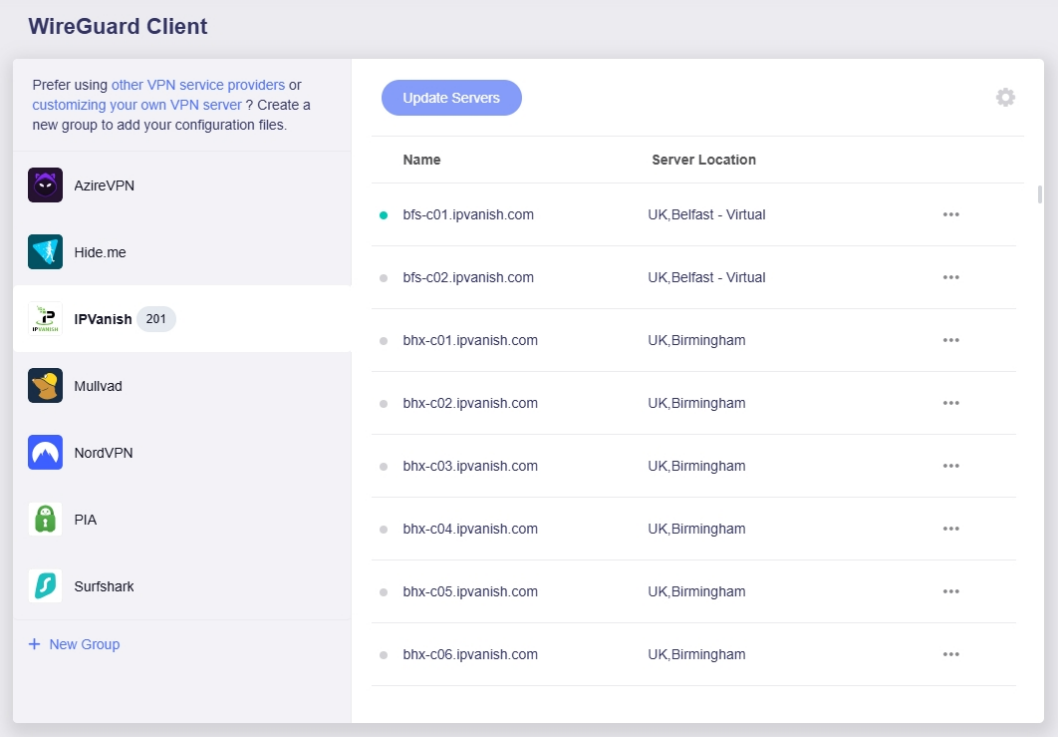
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



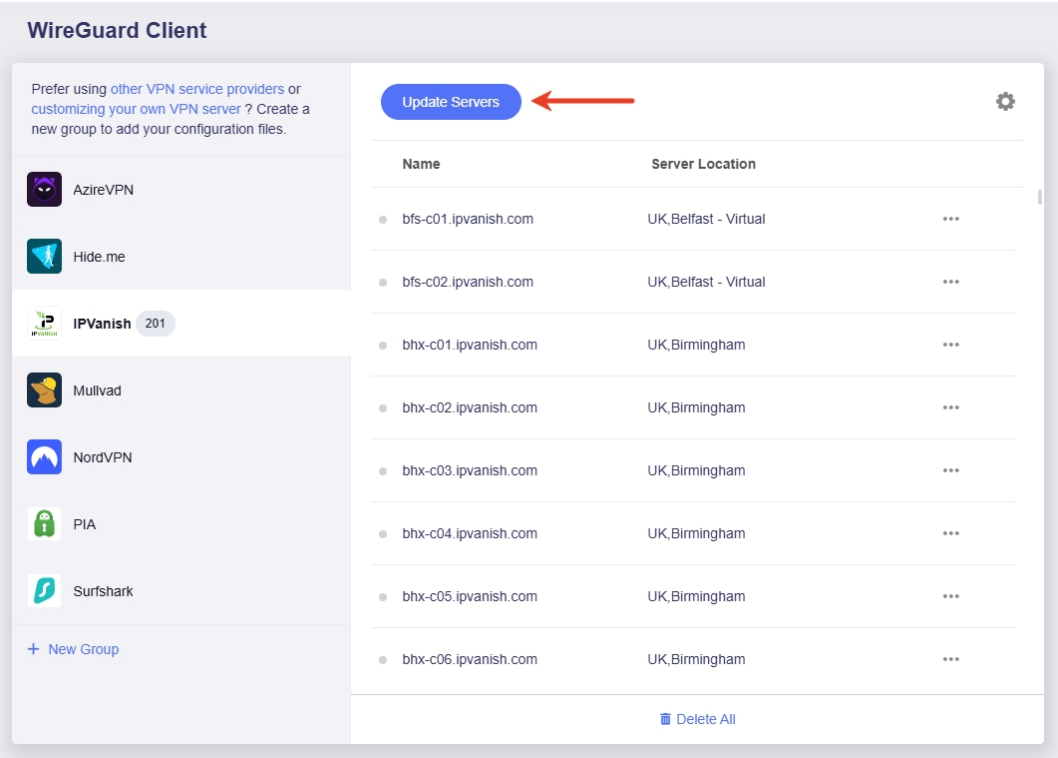
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

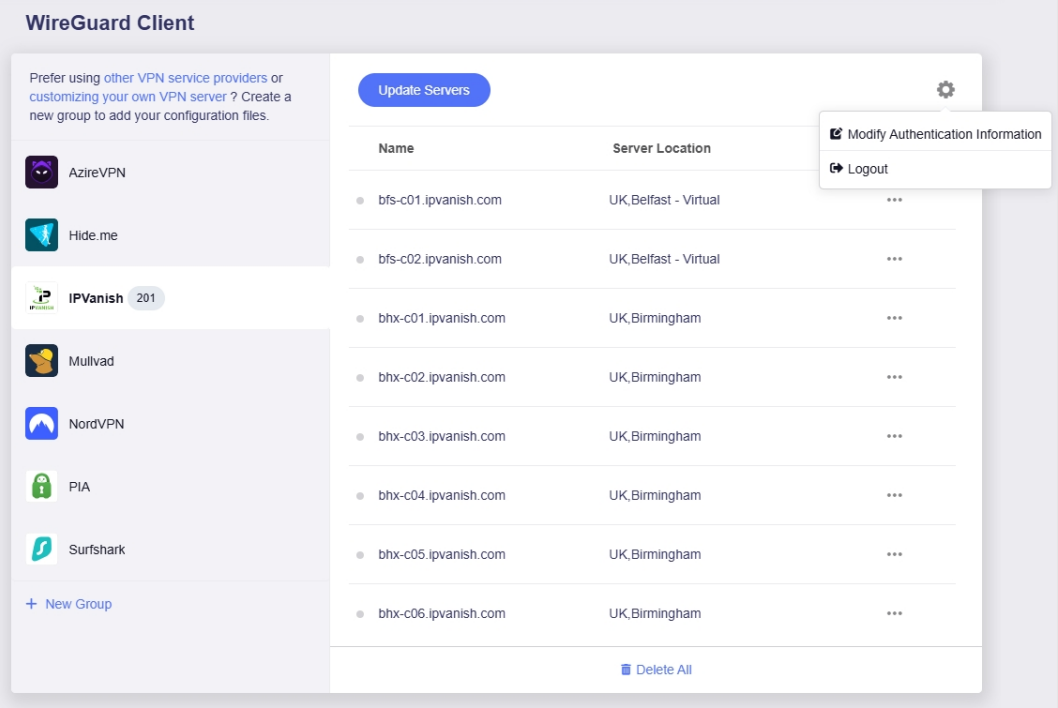
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



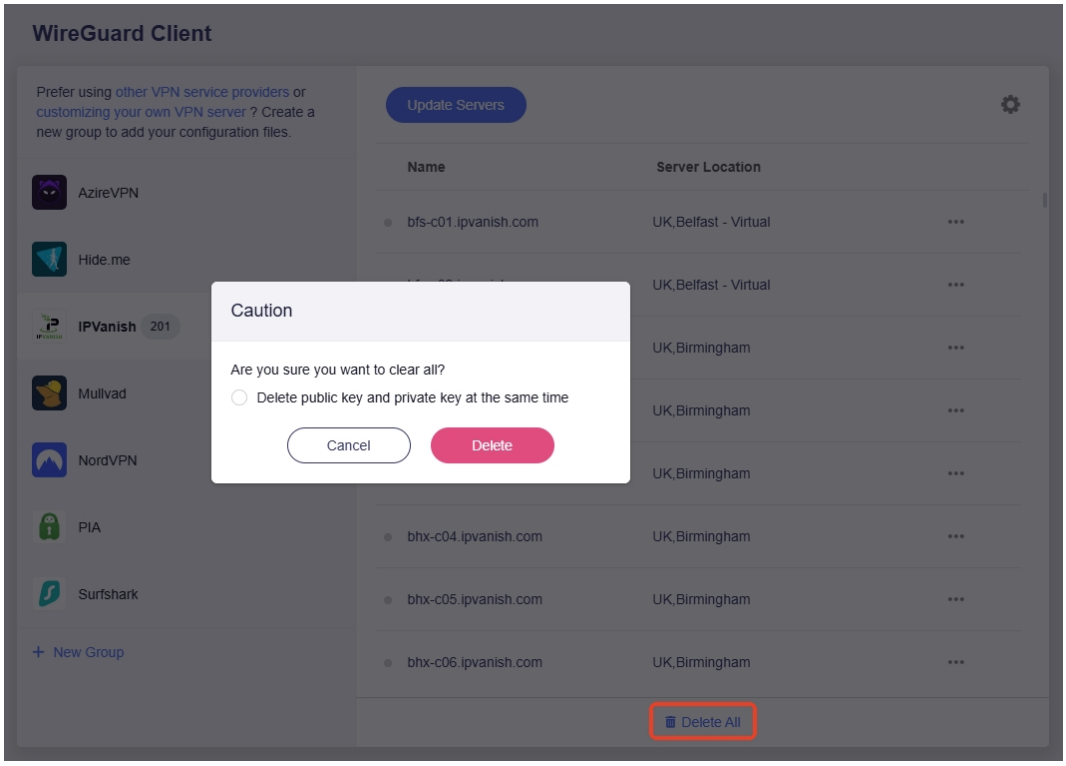
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



8. Usuń wszystkie pliki.

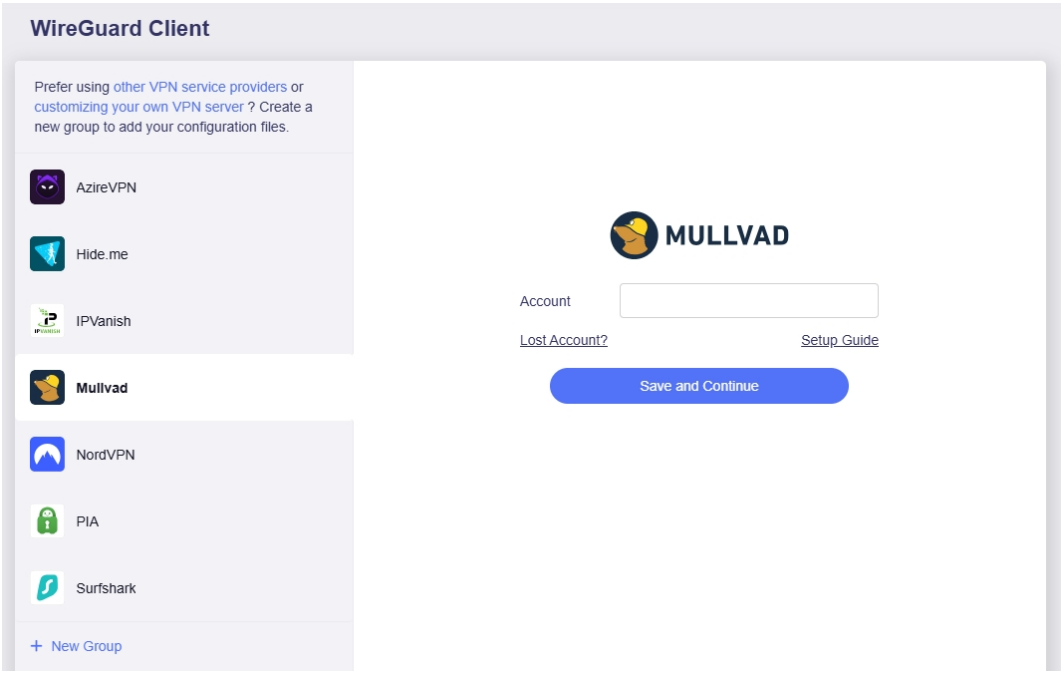
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
AzireVPN
Hide.me
IPVanish 201
Mullvad
NordVPN
PIA
Surfshark
New Group
Update Servers
Name
Server Location
bfs-c01.ipvanish.com
UK,Belfast - Virtual
UK,Belfast - Virtual
UK,Birmingham
UK,Birmingham
UK,Birmingham
bhx-c04.ipvanish.com
UK,Birmingham
bhx-c05.ipvanish.com
UK,Birmingham
bhx-c06.ipvanish.com
UK,Birmingham
Delete All
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete

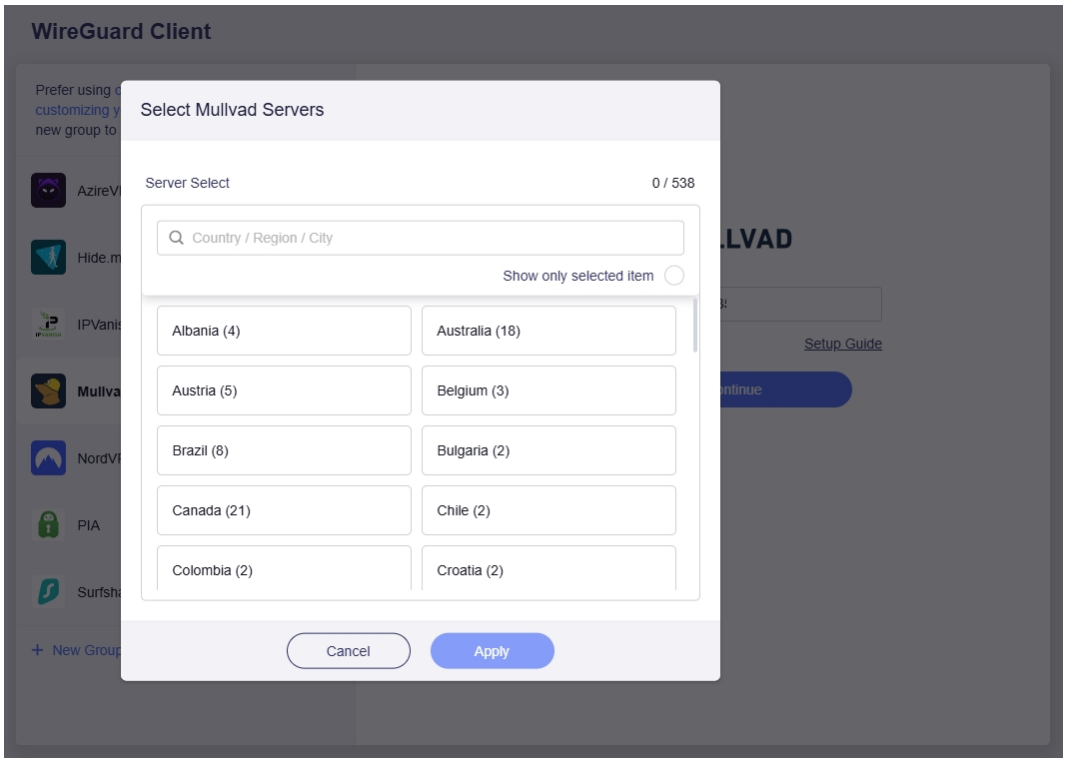
11.2.5 Konfiguracja Mullvad

Aby skonfigurować router jako klienta Mullvad, wykonaj poniższe czynności.

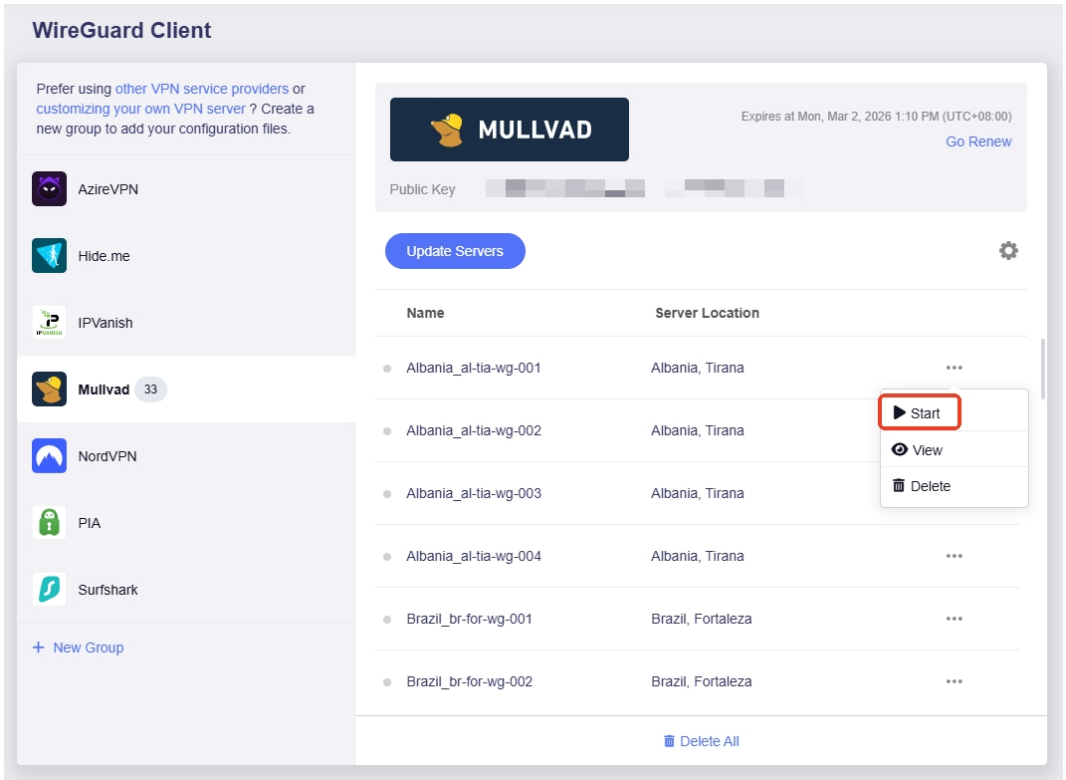
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Mullvad**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



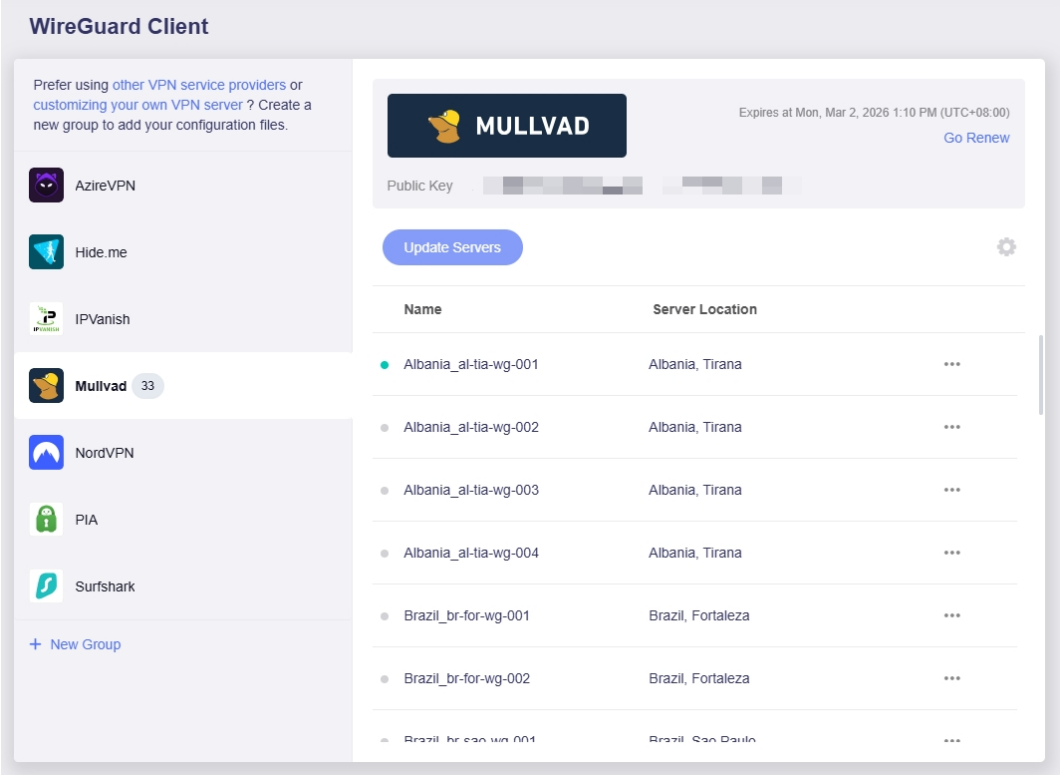
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



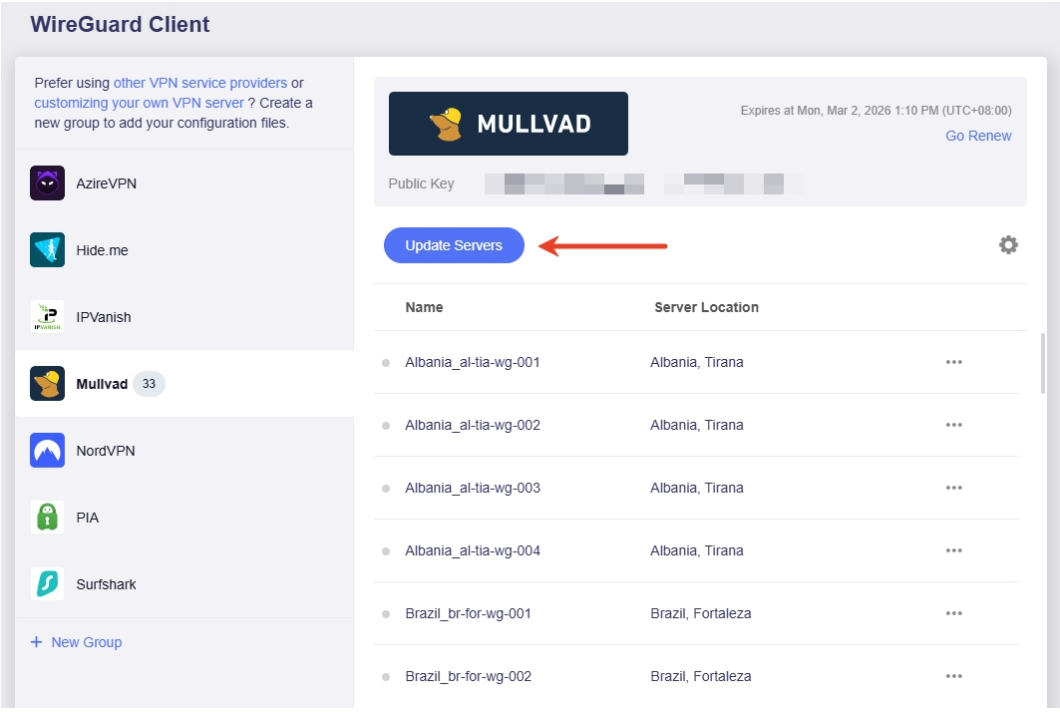
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

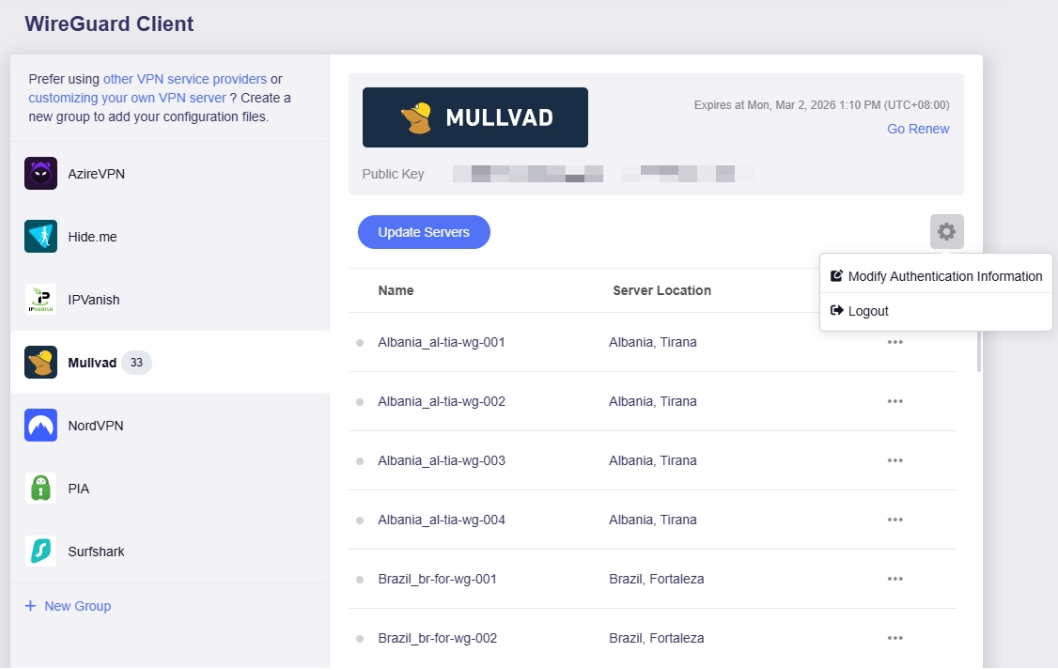
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



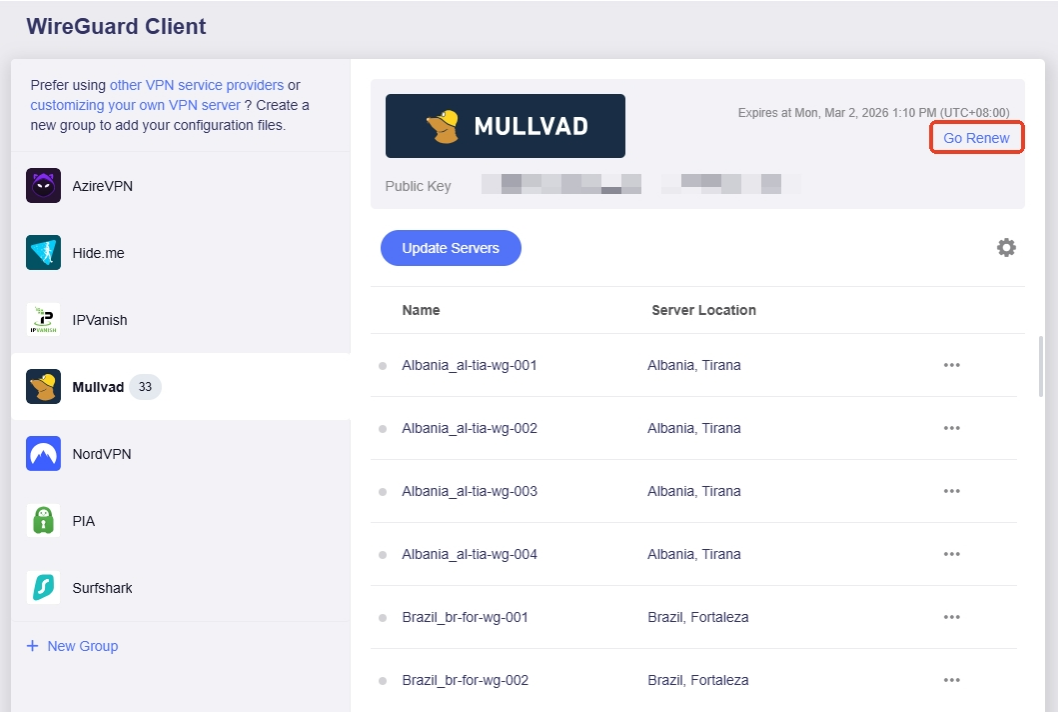
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



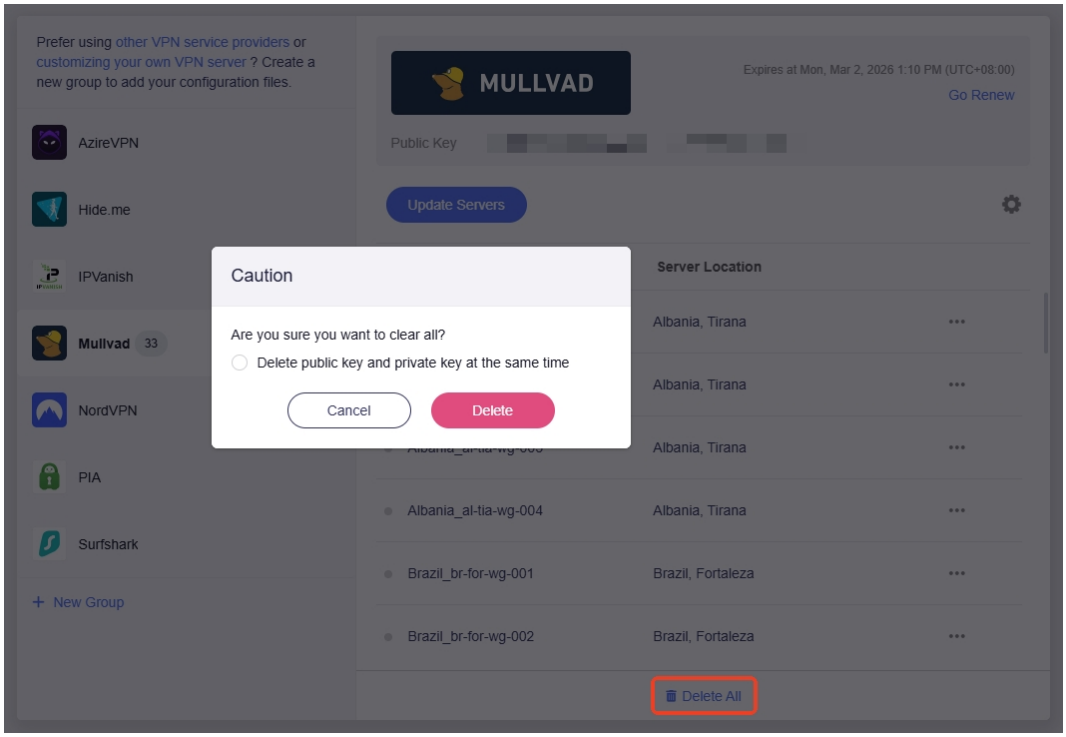
8. Odnowienie subskrypcji.

   Po kliknięciu **Go Renew** nastąpi przekierowanie na oficjalną stronę w celu odnowienia subskrypcji.



9. Usuń wszystkie pliki.

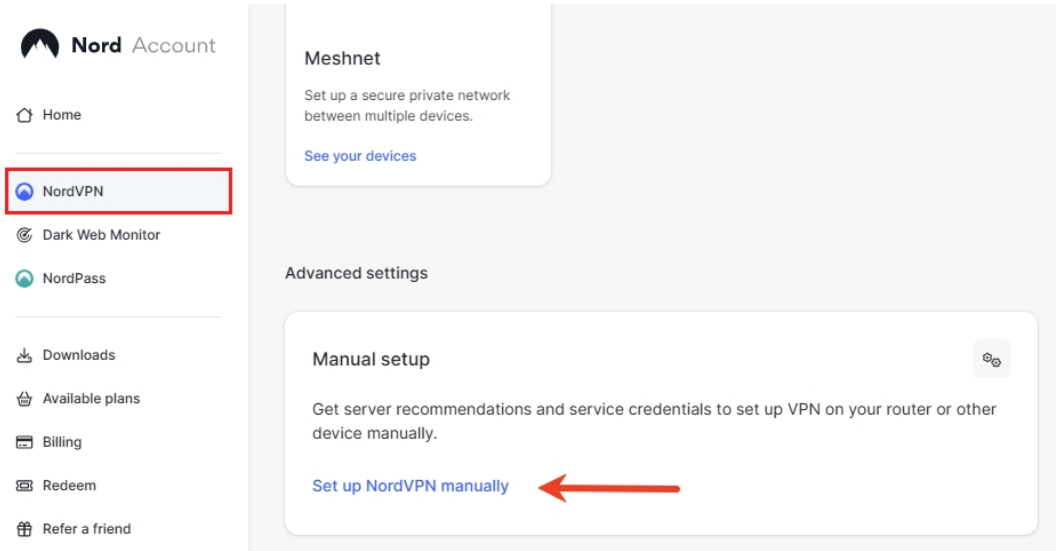
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



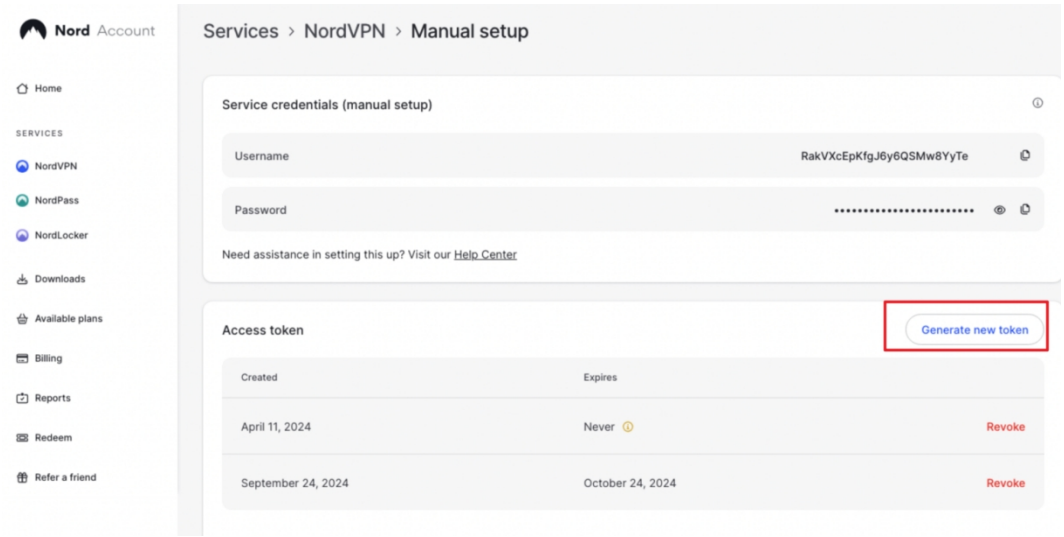
11.2.6 Konfiguracja NordVPN

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

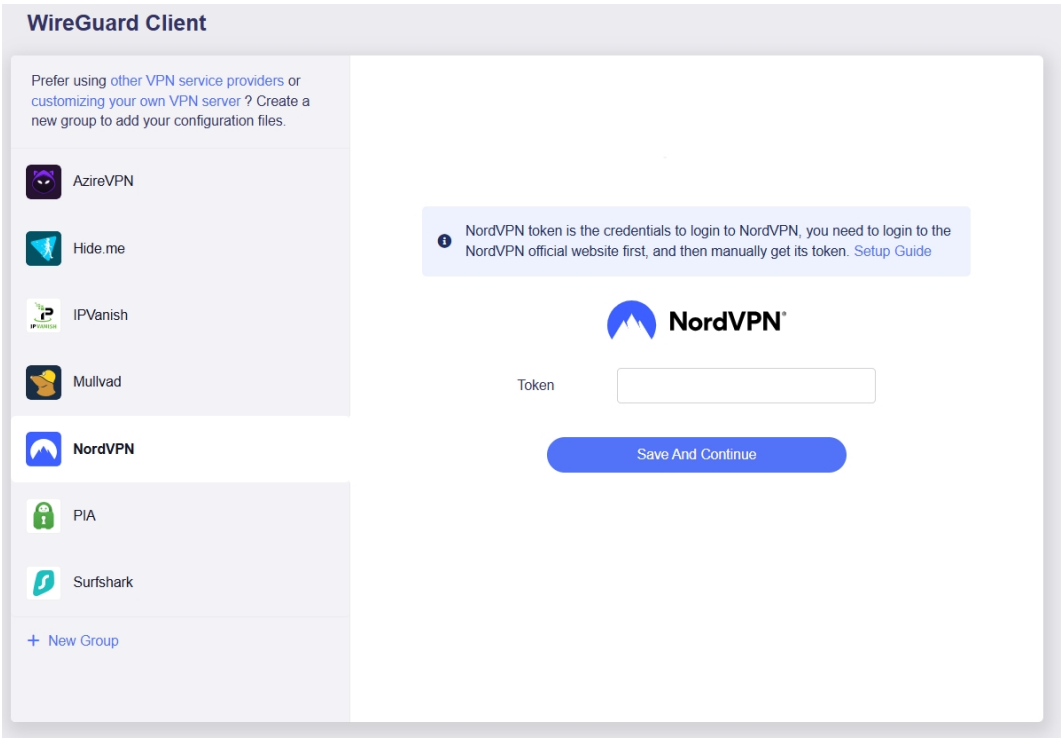
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



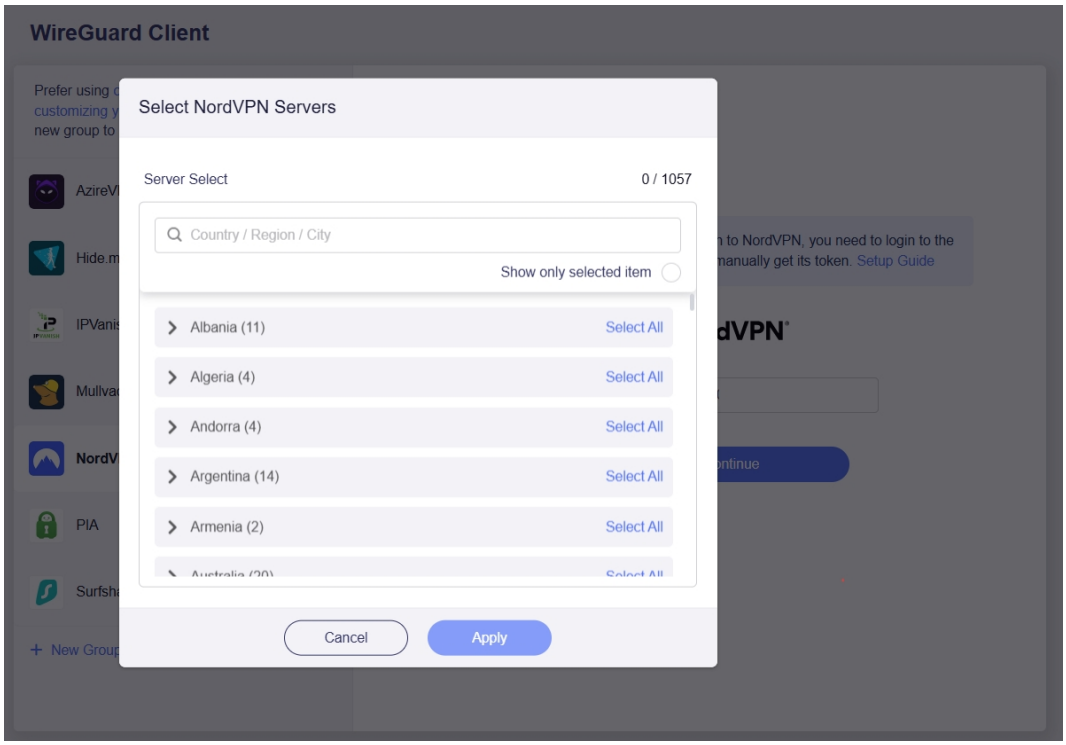
Znajdziesz tam **Access Token**. Utwórz token dostępu i skopiuj go do późniejszego użycia.



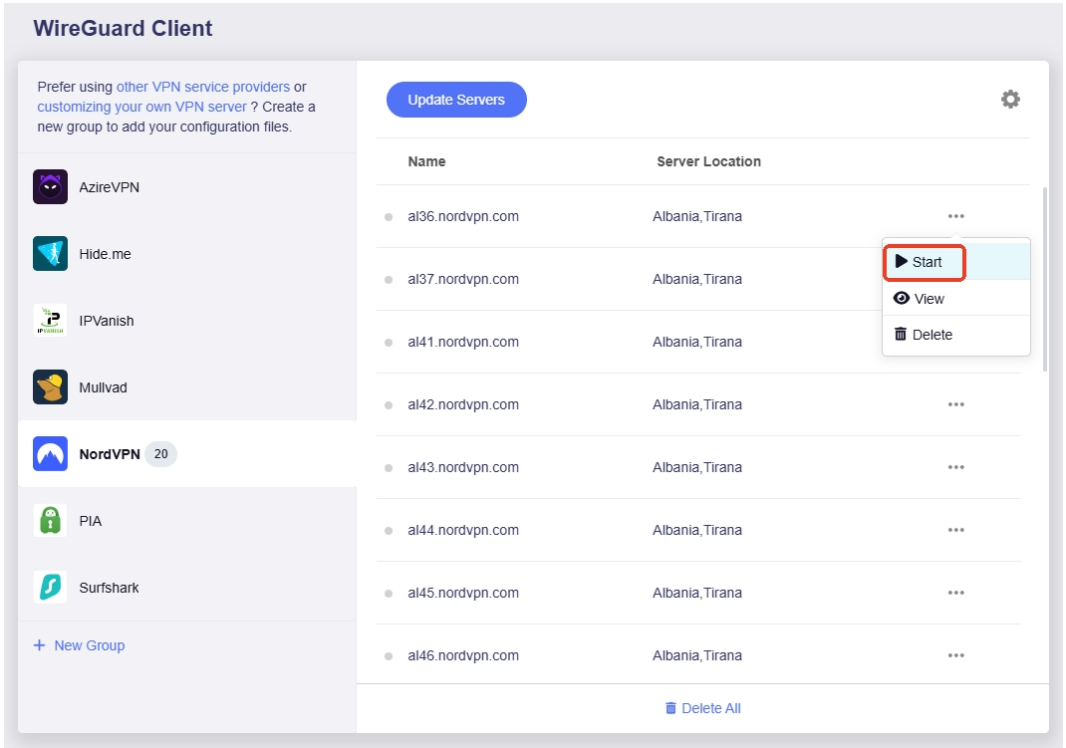
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **NordVPN**.
4. Wprowadź token i kliknij **Save and Continue**.



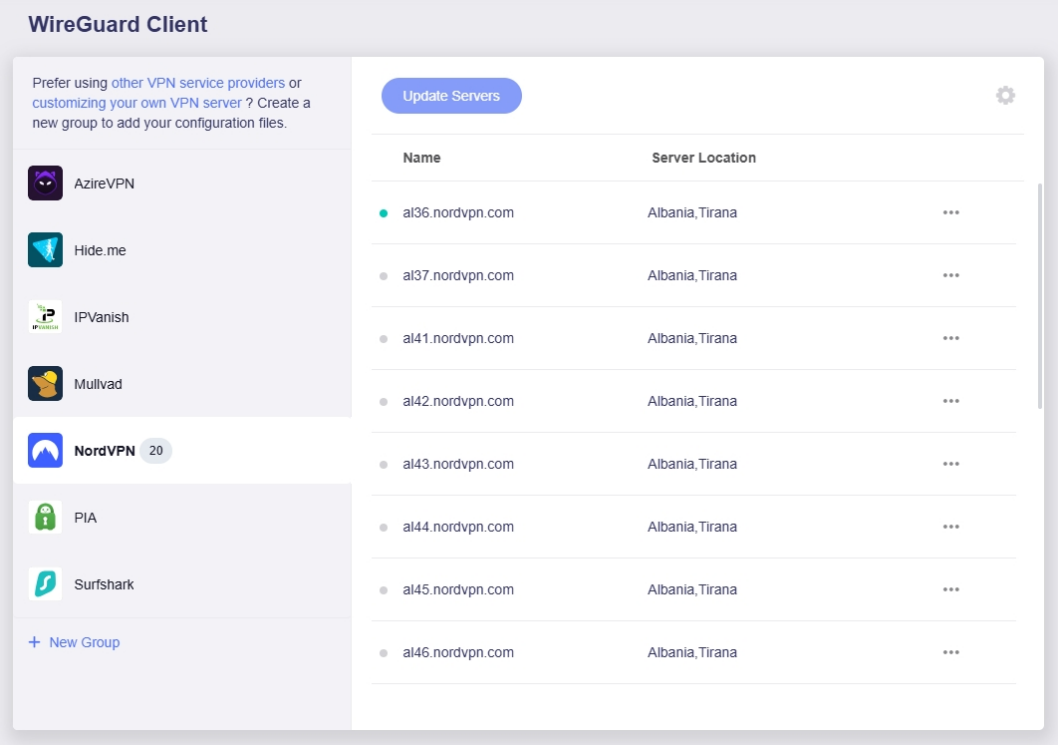
5. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



6. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



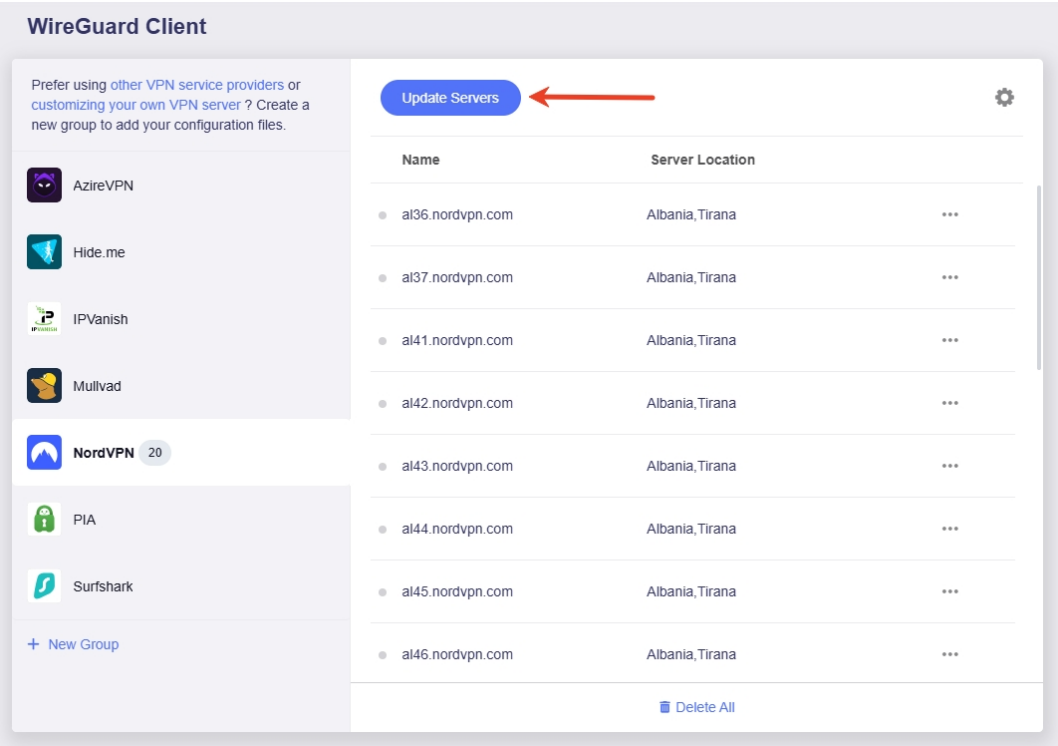
7. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

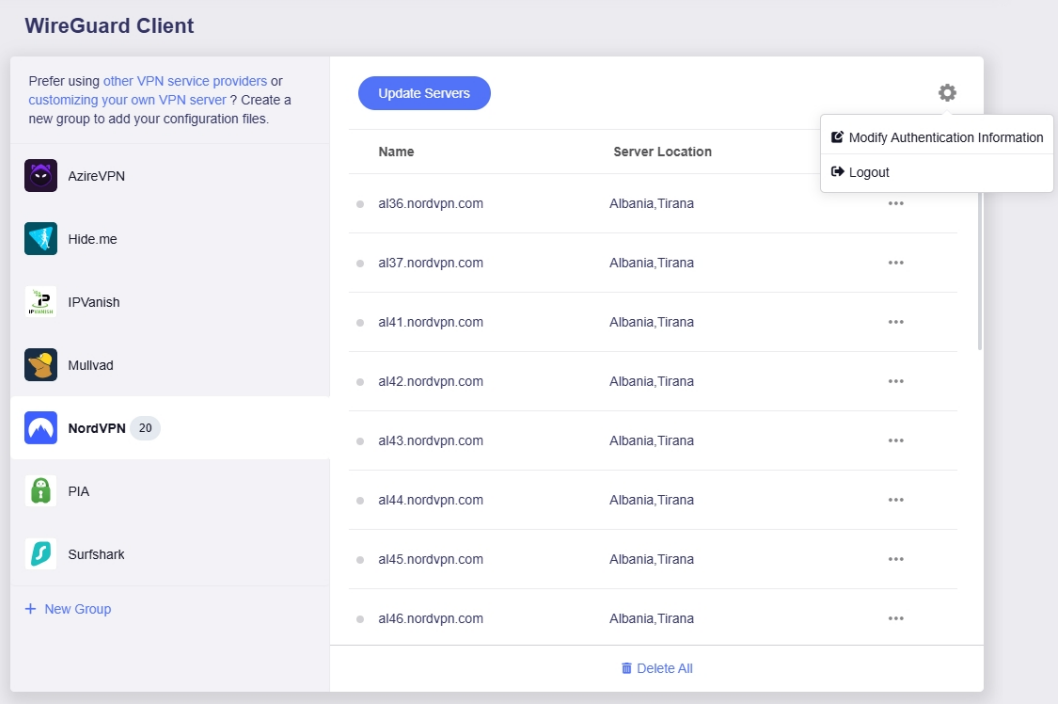
8. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



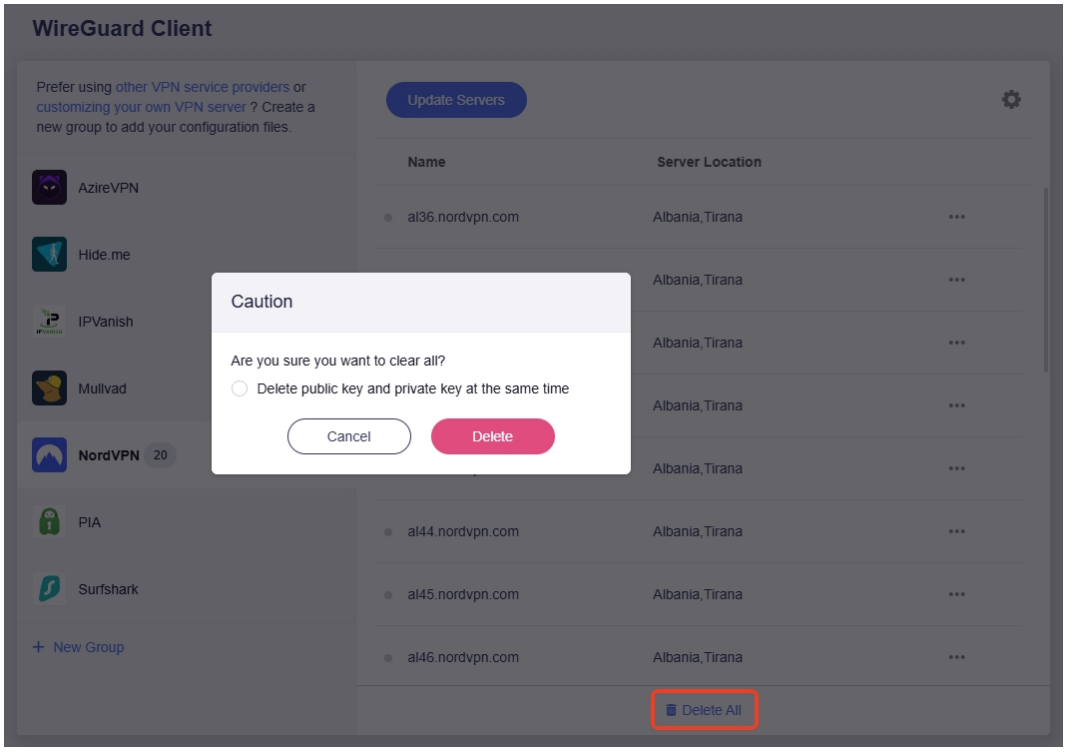
9. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



10. Usuń wszystkie pliki.

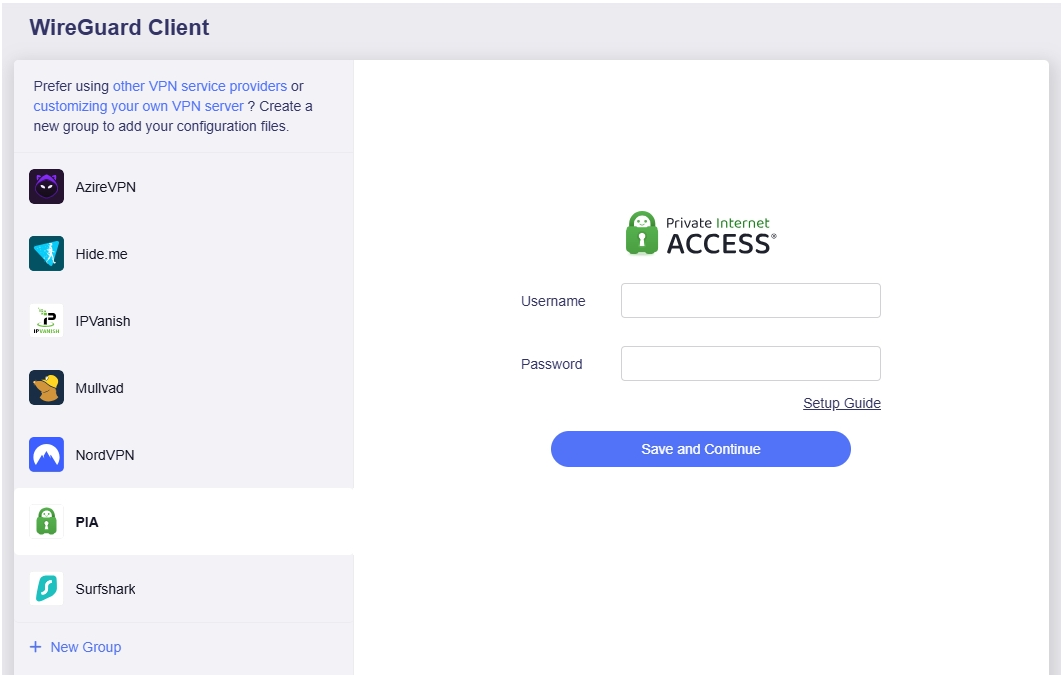
    Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



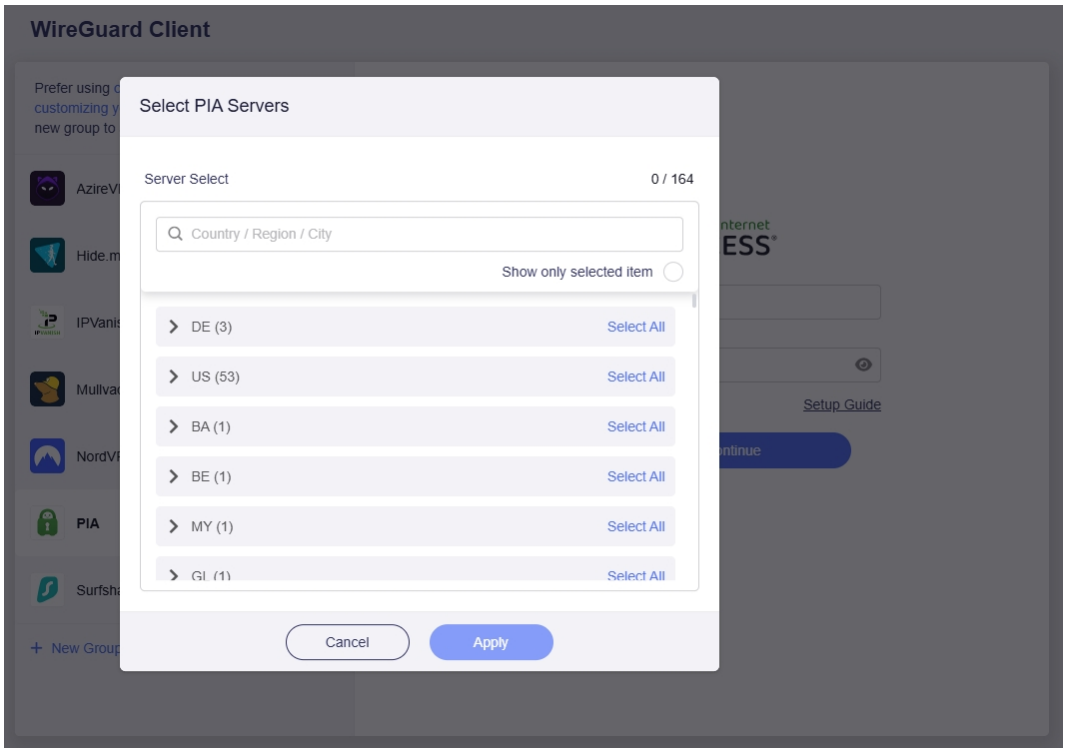
11.2.7 Konfiguracja PIA (Private Internet Access)

Aby skonfigurować router jako klienta PIA, wykonaj poniższe czynności.

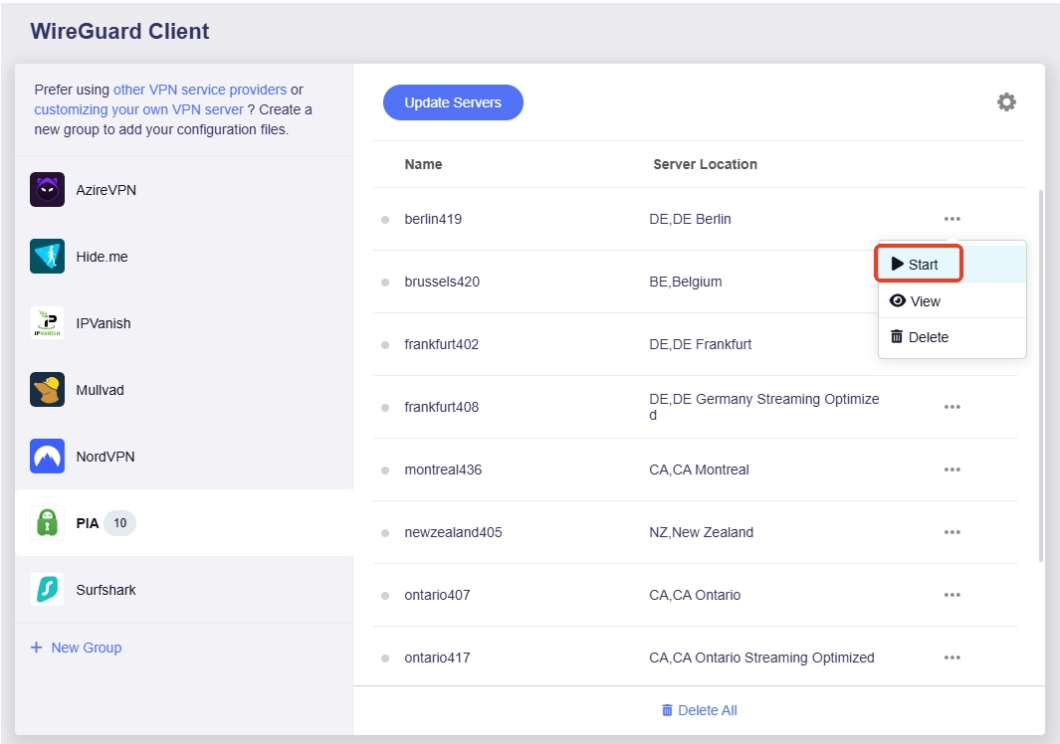
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **PIA**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



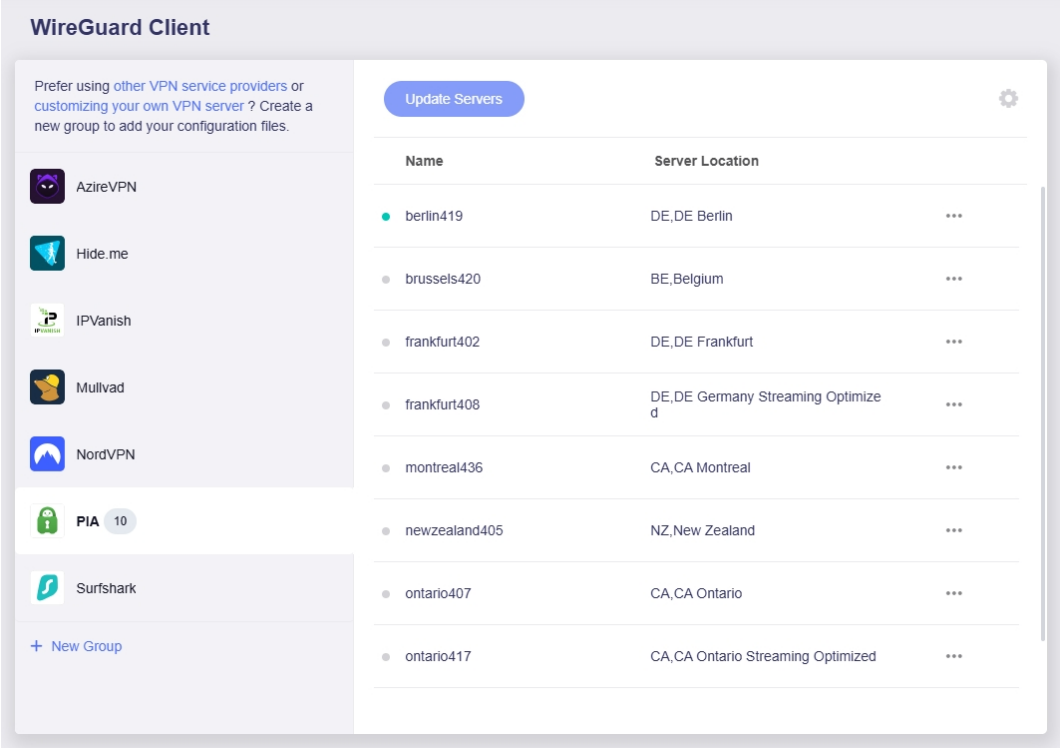
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



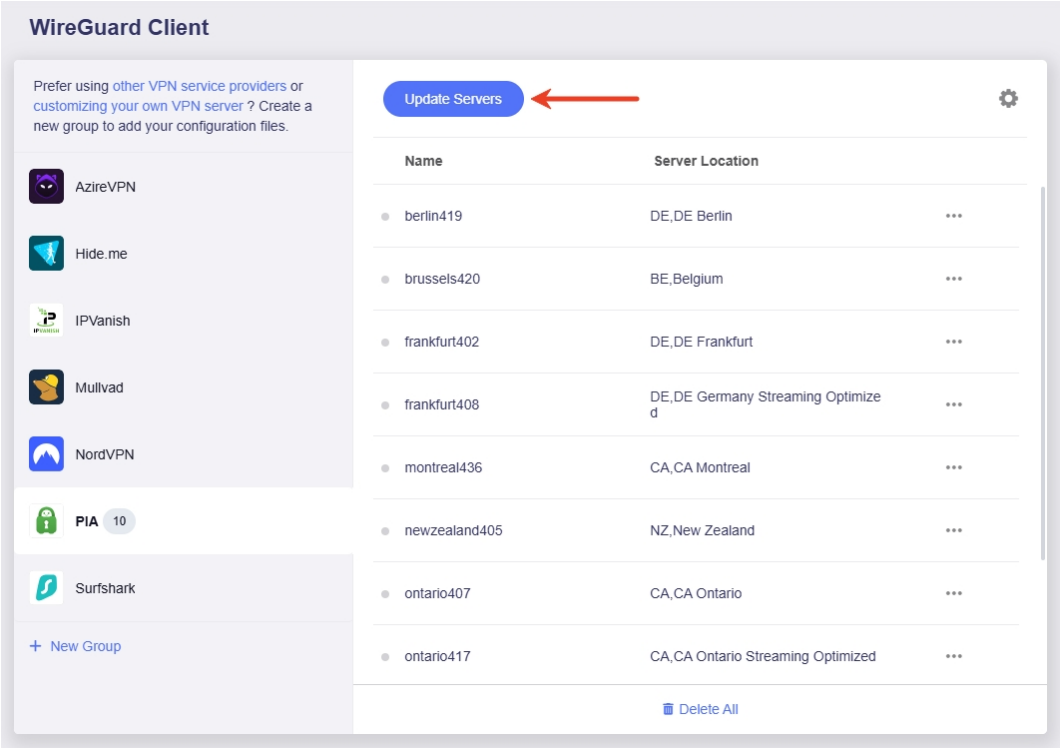
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

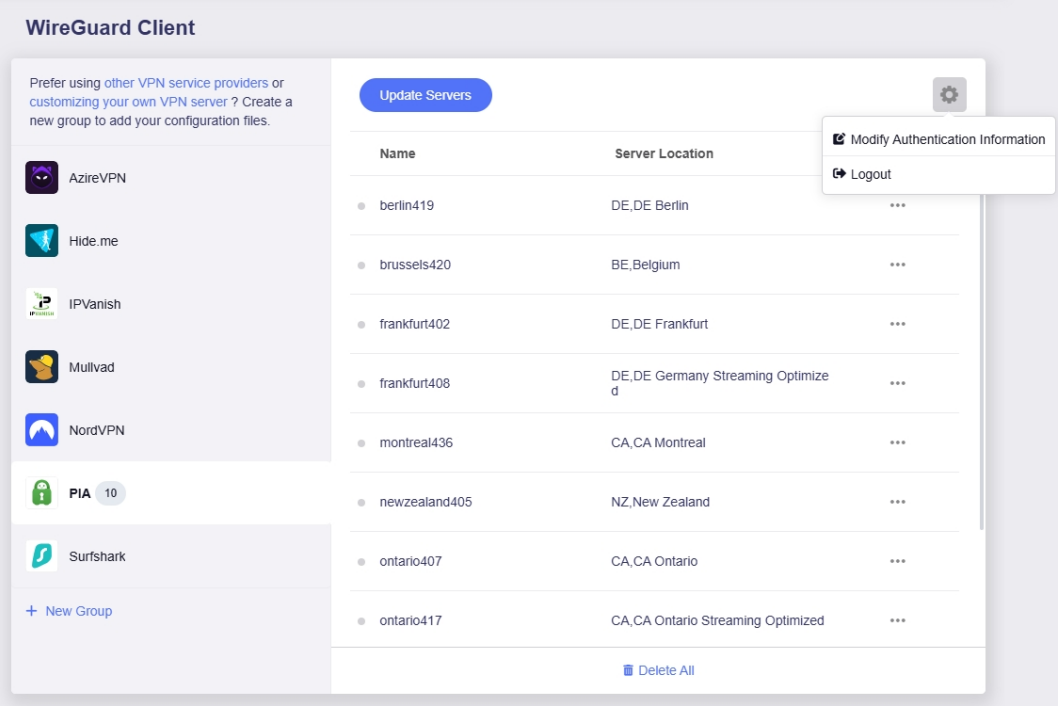
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



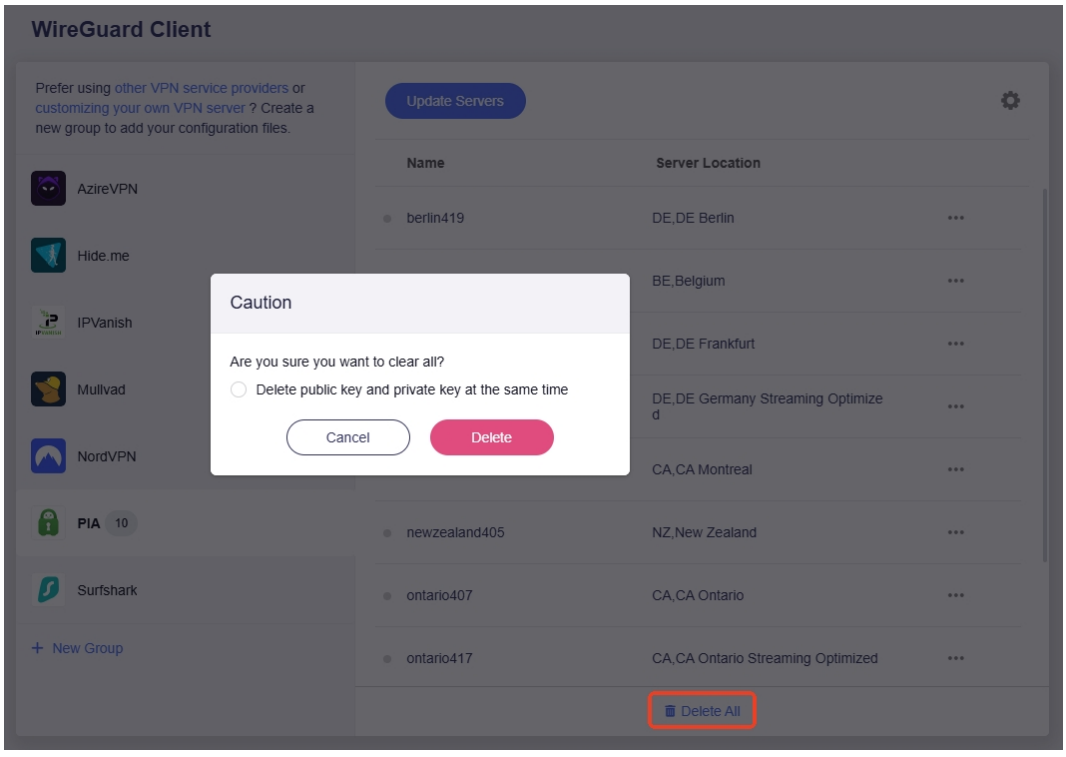
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



8. Usuń wszystkie pliki.

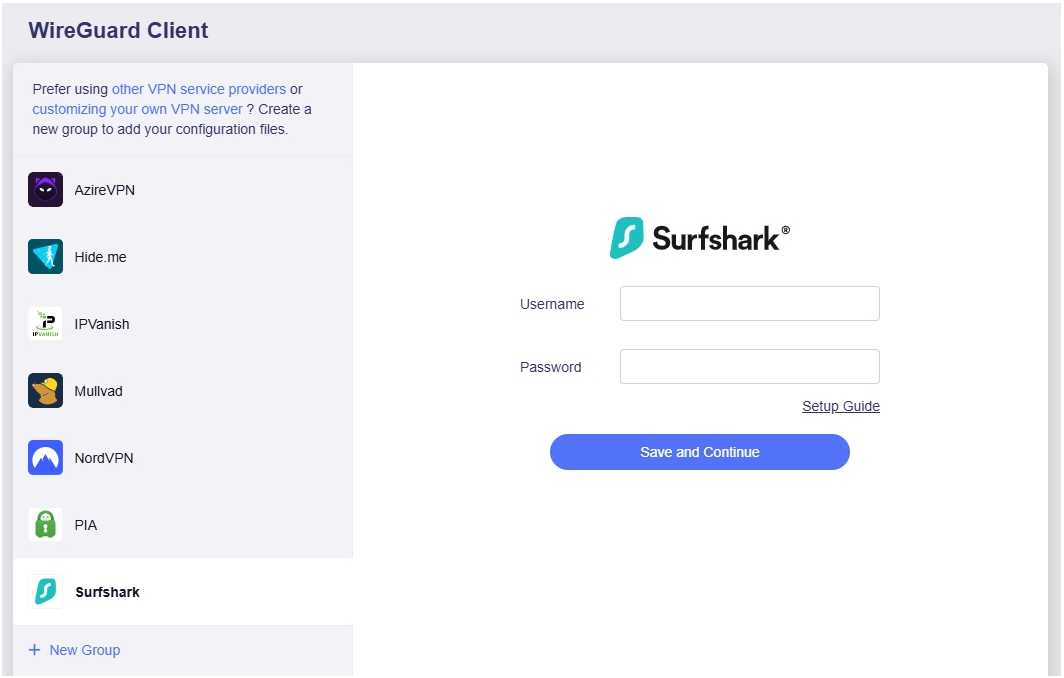
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



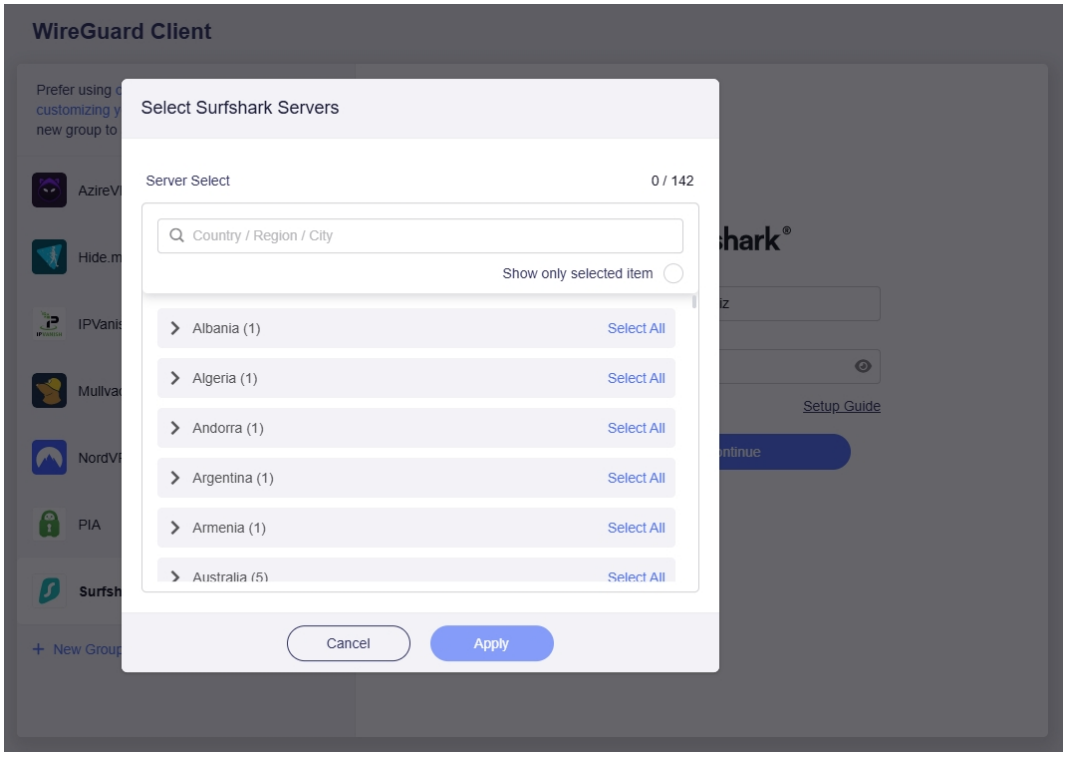
11.2.8 Konfiguracja Surfshark

Aby skonfigurować router jako klienta Surfshark, wykonaj poniższe czynności.

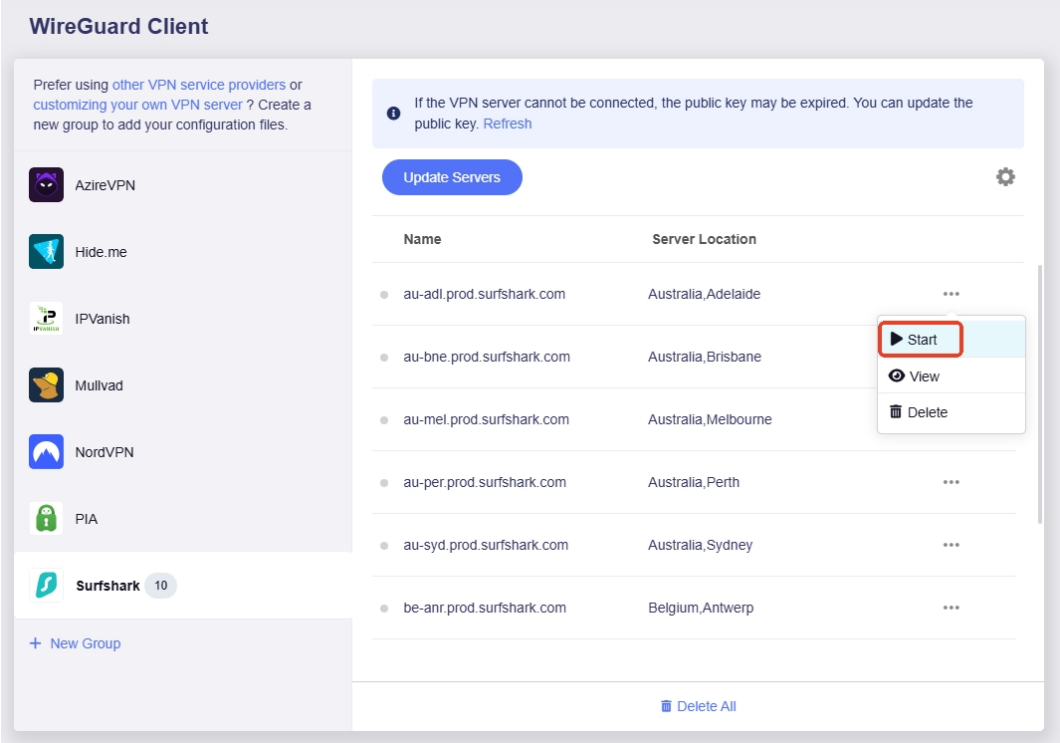
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Surfshark**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



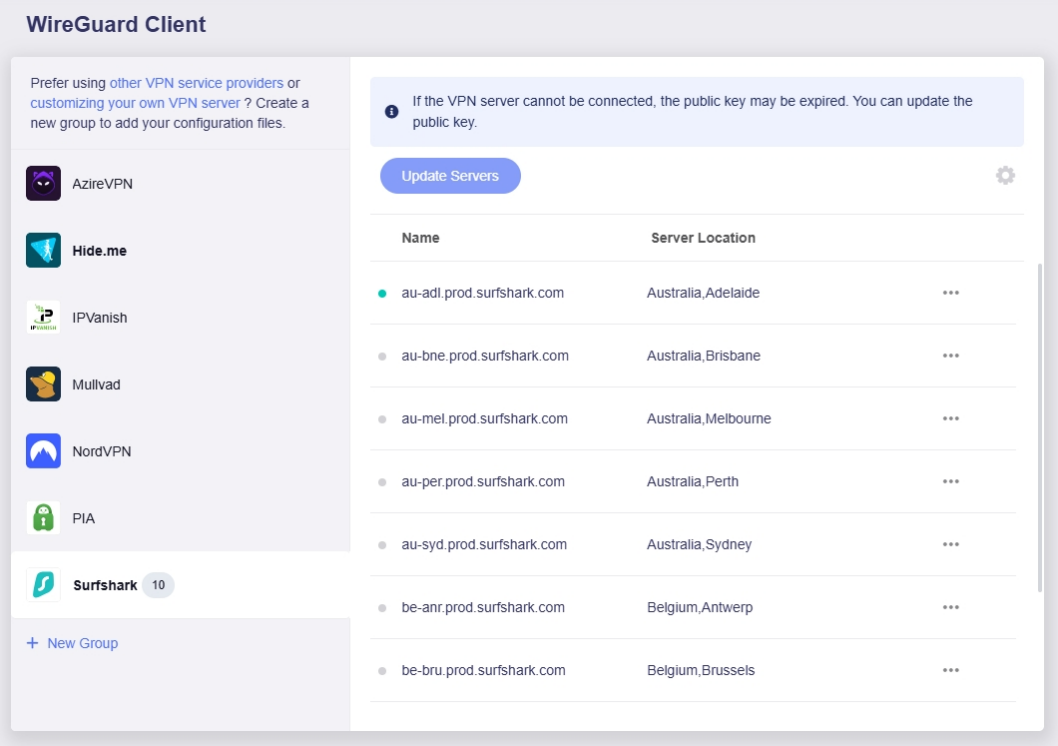
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



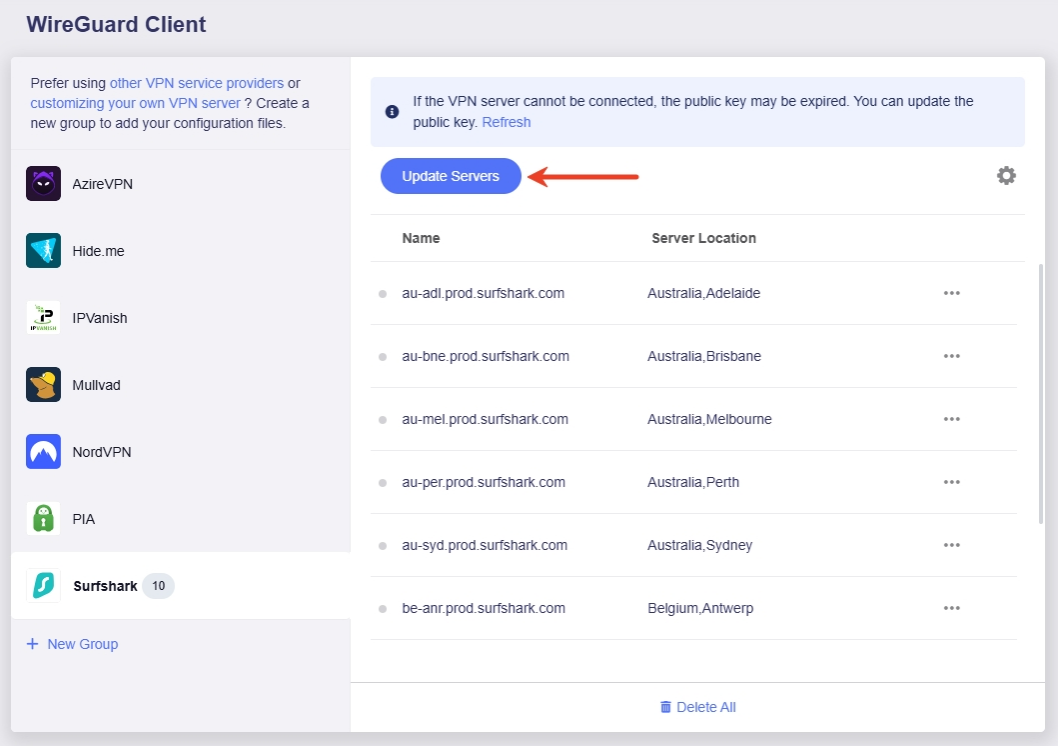
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

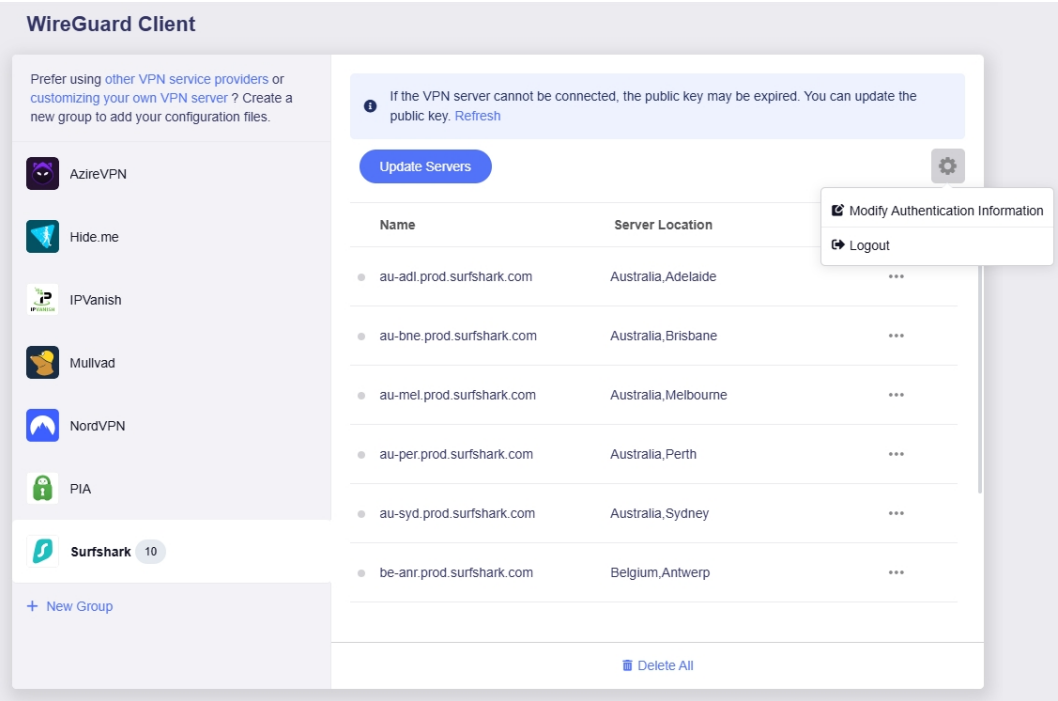
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



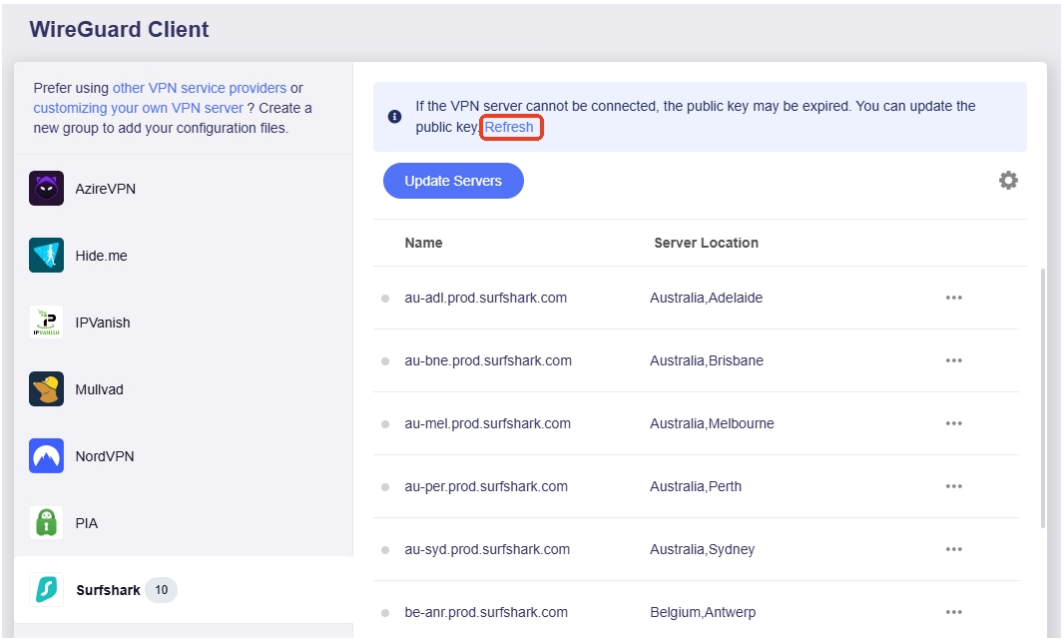
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



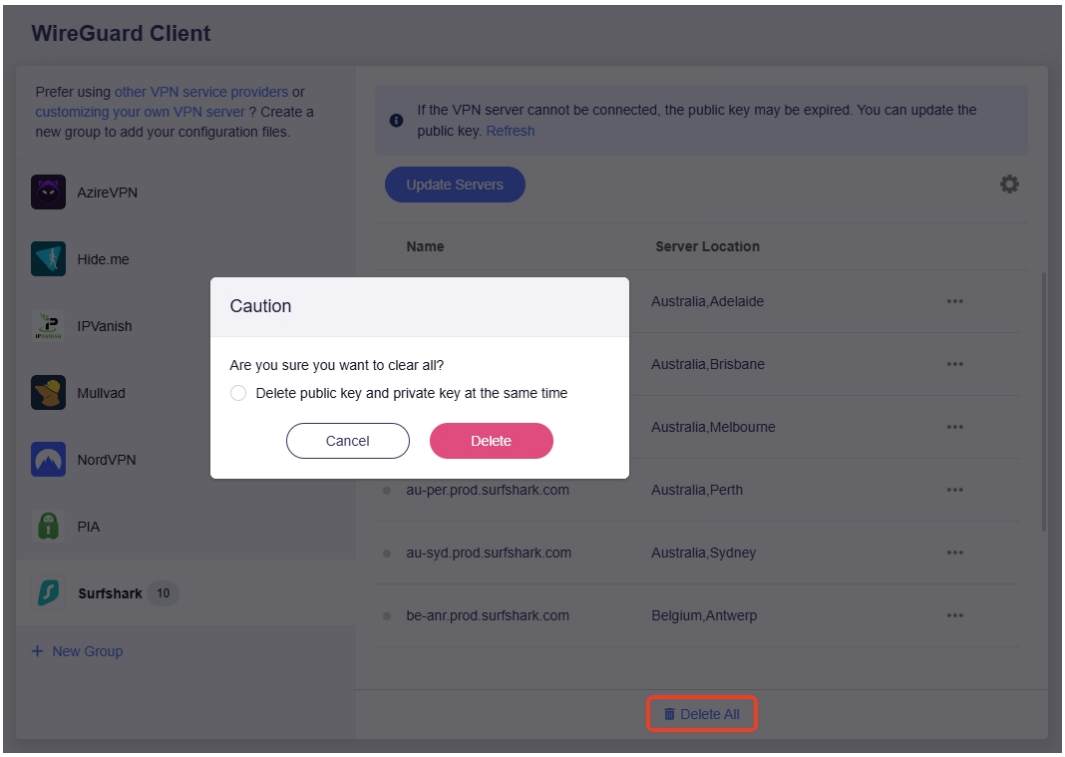
8. Odświeżanie.

   Możesz kliknąć **Refresh**, aby zaktualizować klucz publiczny, gdy nie można połączyć się z serwerem VPN.



9. Usuń wszystkie pliki.

   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.

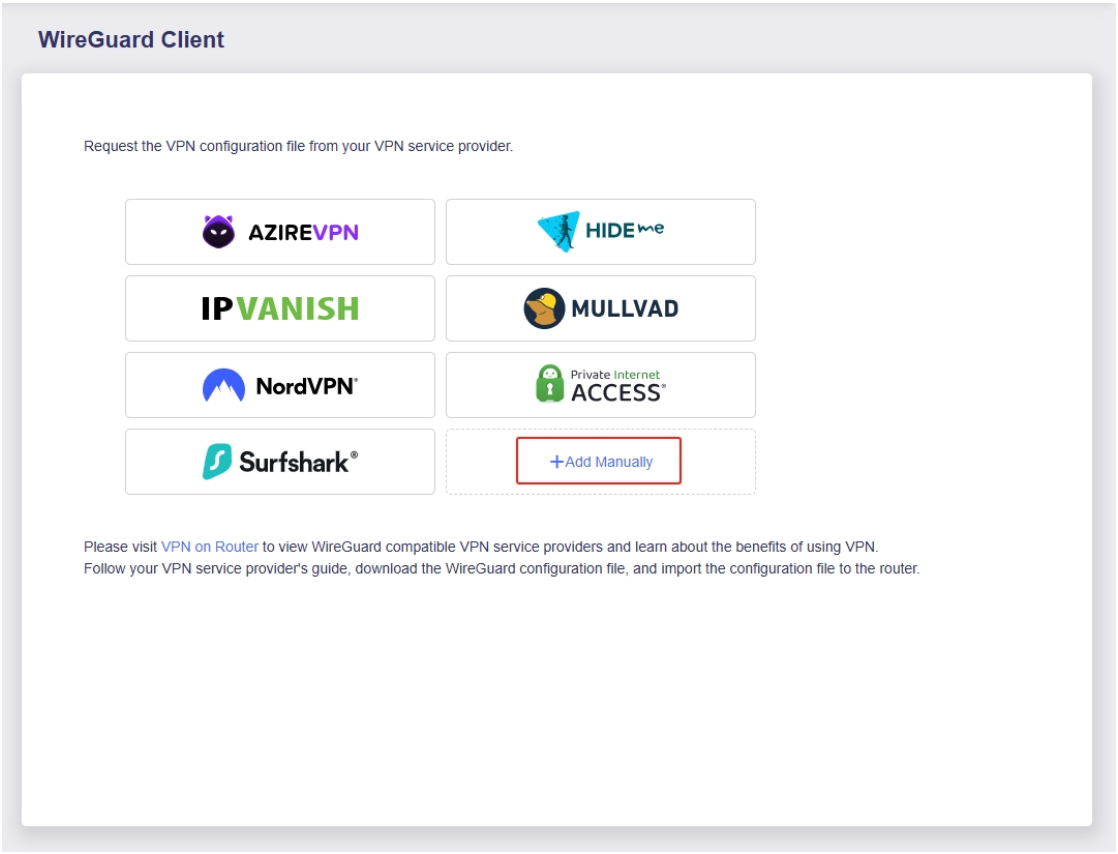


11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy)

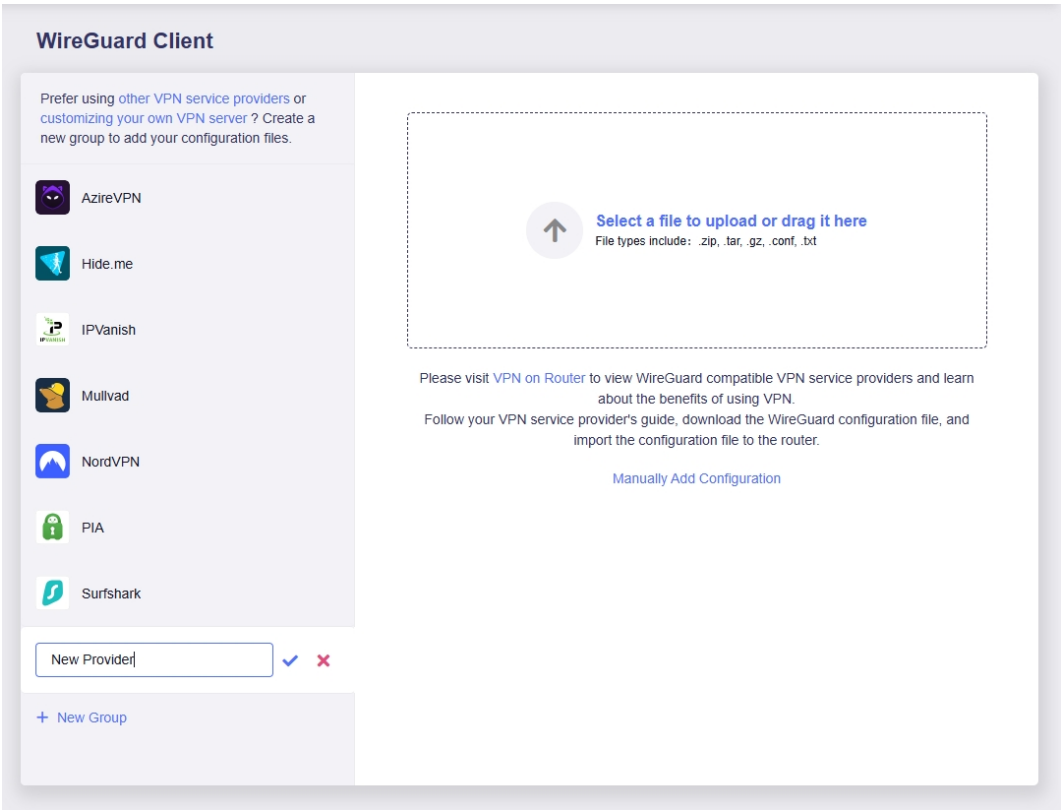
Jeśli Twój dostawca WireGuard nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta WireGuard. Jeśli nie wiesz, jak pobrać pliki konfiguracyjne, skorzystaj z tego poradnika lub skontaktuj się z pomocą techniczną dostawcy.

Poniżej opisano przesyłanie pliku konfiguracyjnego do routera w celu skonfigurowania klienta WireGuard.

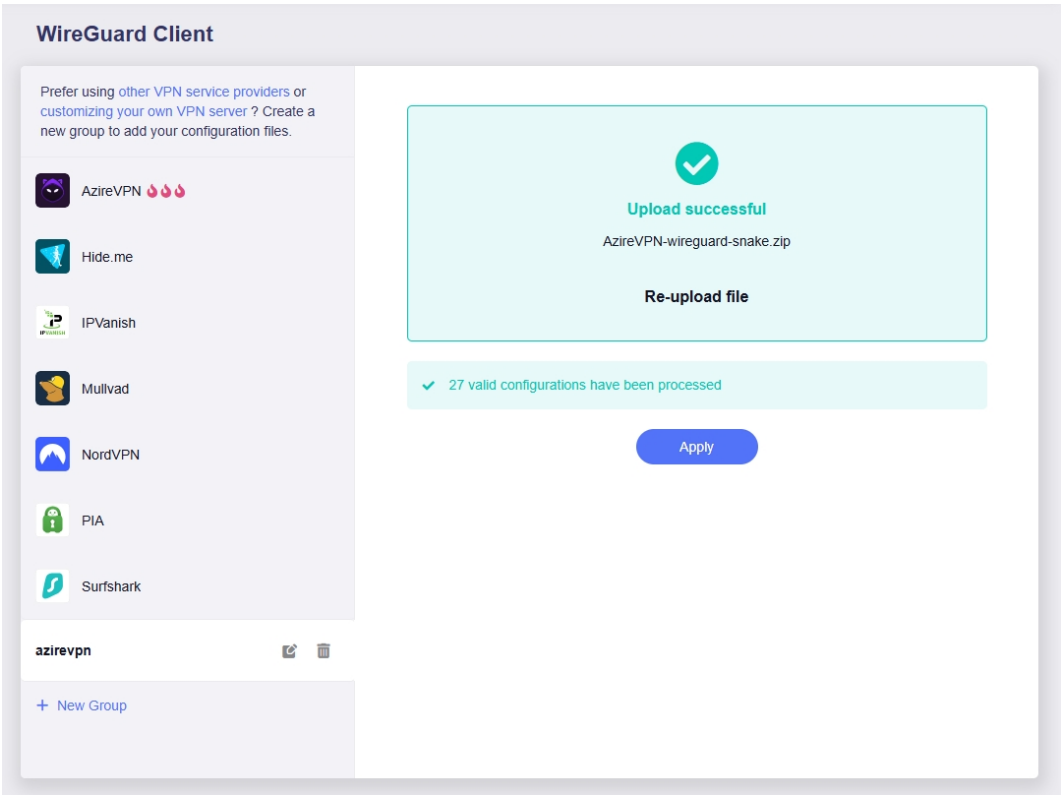
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Add Manually**.



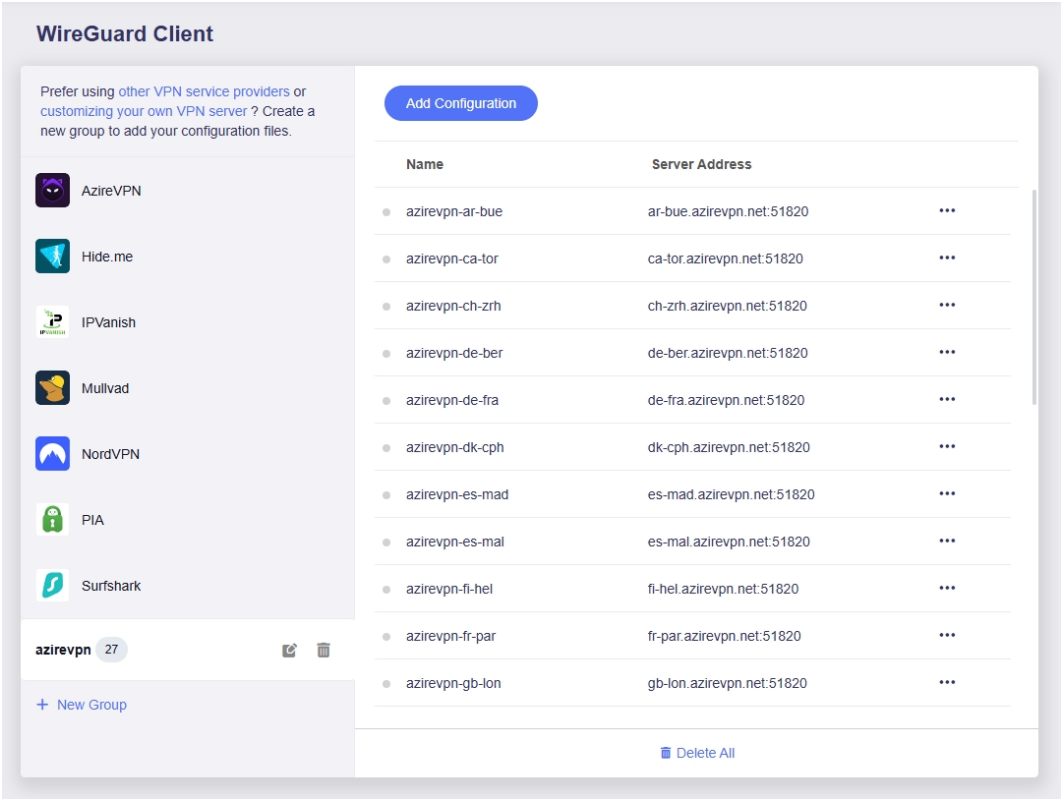
2. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



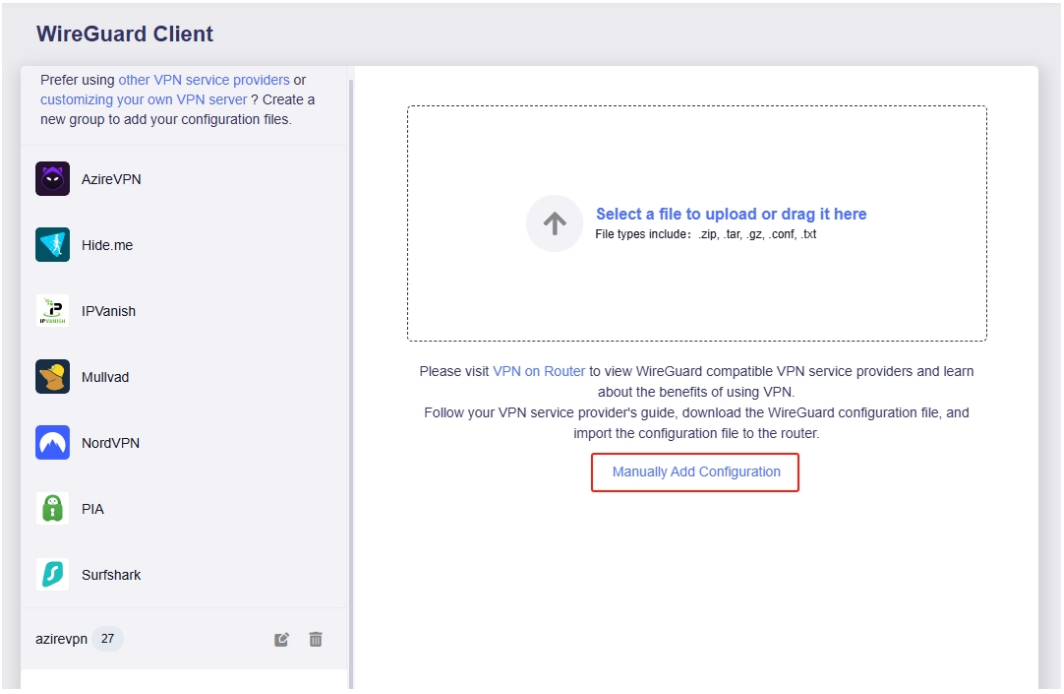
3. Kliknij obszar przesyłania, aby przesłać plik konfiguracyjny WireGuard (obsługiwane formaty: zip, tar, gz, conf, txt), i kliknij **Apply**.

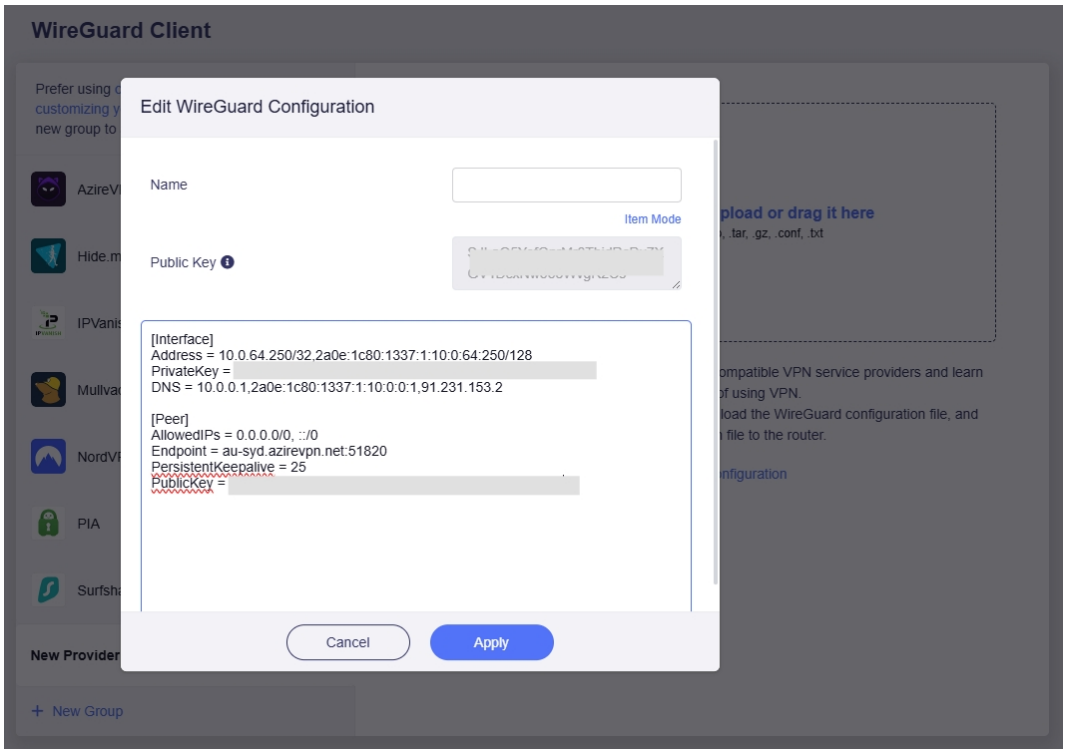


Po przesłaniu skompresowanego pliku zawierającego wiele plików konfiguracyjnych zostanie on automatycznie rozpakowany, jak pokazano poniżej.

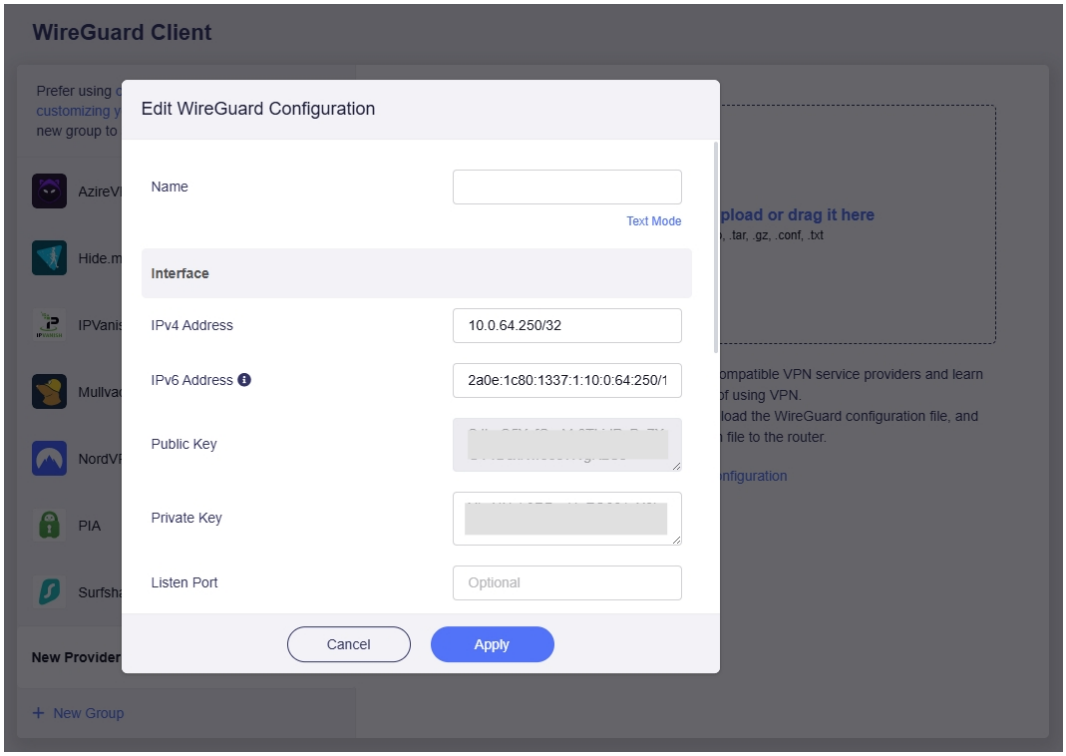


Możesz też kliknąć **Manually Add Configuration** u dołu obszaru przesyłania, dodać konfigurację w postaci tekstu i kliknąć **Apply**.

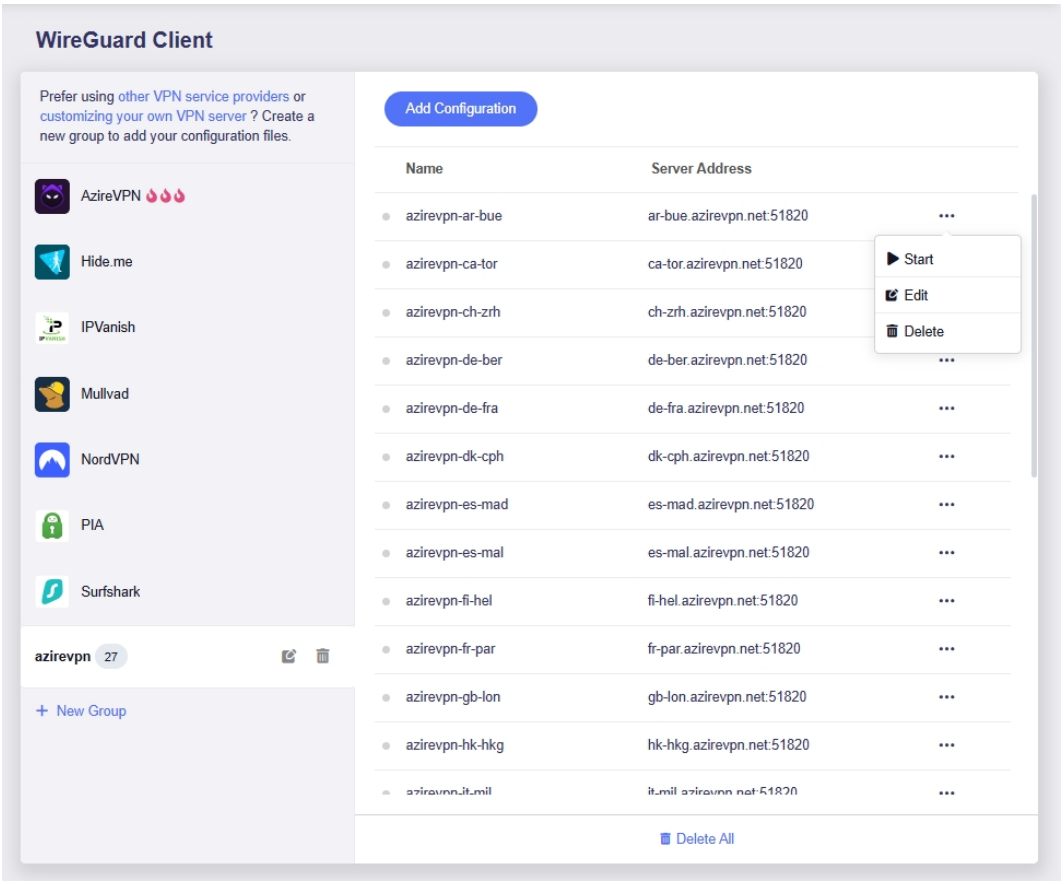




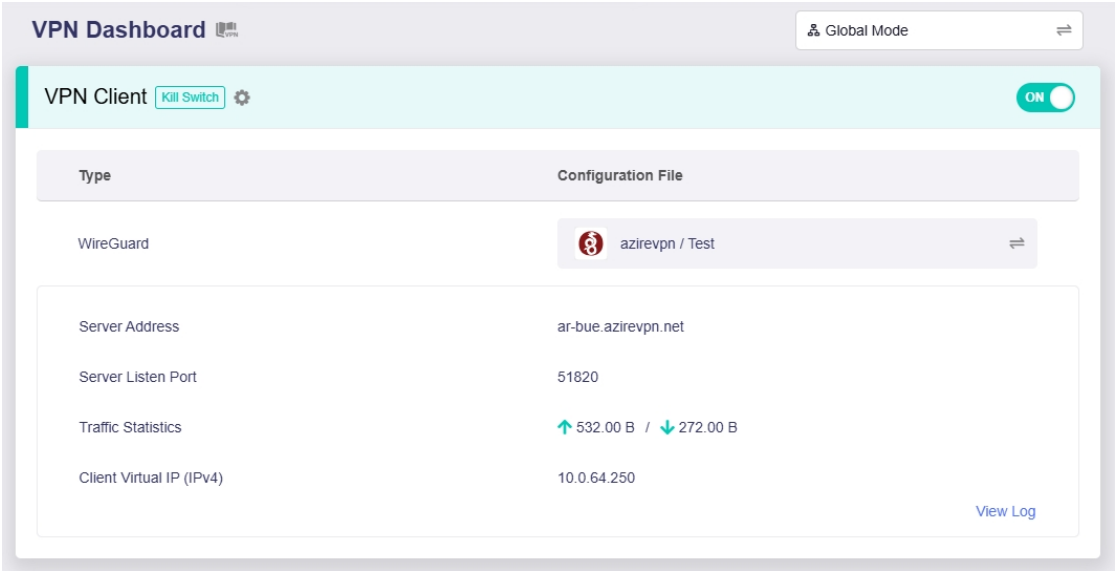
Aby sprawdzić poszczególne elementy, przełącz się do trybu Item, sprawdź szczegóły konfiguracji, a następnie kliknij **Apply**.



4. Kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka. Szczegóły połączenia VPN możesz sprawdzić w **VPN Dashboard**.



Rozdział 12

Tor

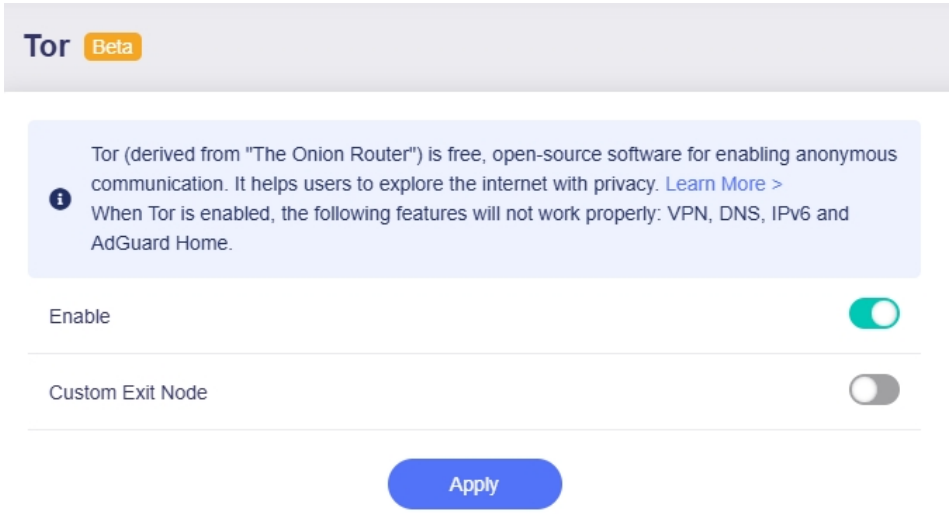
W tym rozdziale krótko przedstawiono Tor (The Onion Router), bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację.

Tor (od nazwy **The Onion Router**) to bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację. Pomaga przeglądać Internet z zachowaniem prywatności. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

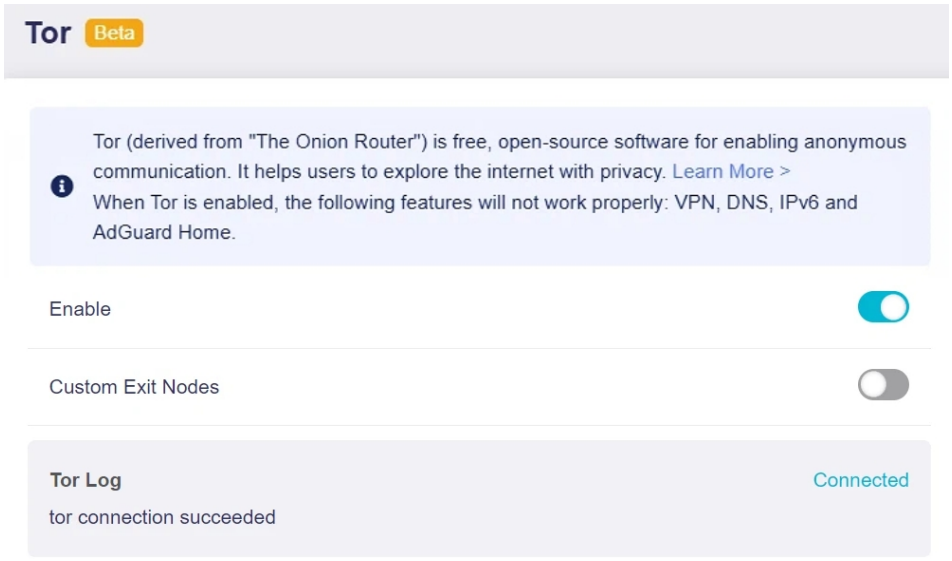
Gdy Tor jest włączony, następujące funkcje nie działają prawidłowo: VPN, DNS, IPv6 i AdGuard Home.

Aby w razie potrzeby skonfigurować Tor, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **Tor**. Włącz funkcję przełącznikiem, w razie potrzeby włącz Custom Exit Nodes i kliknij **Apply**.



2. Rozpocznie się nawiązywanie połączenia. Jeśli sieć spełnia wymagania, pojawi się stan połączenia.


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

Rozdział 13

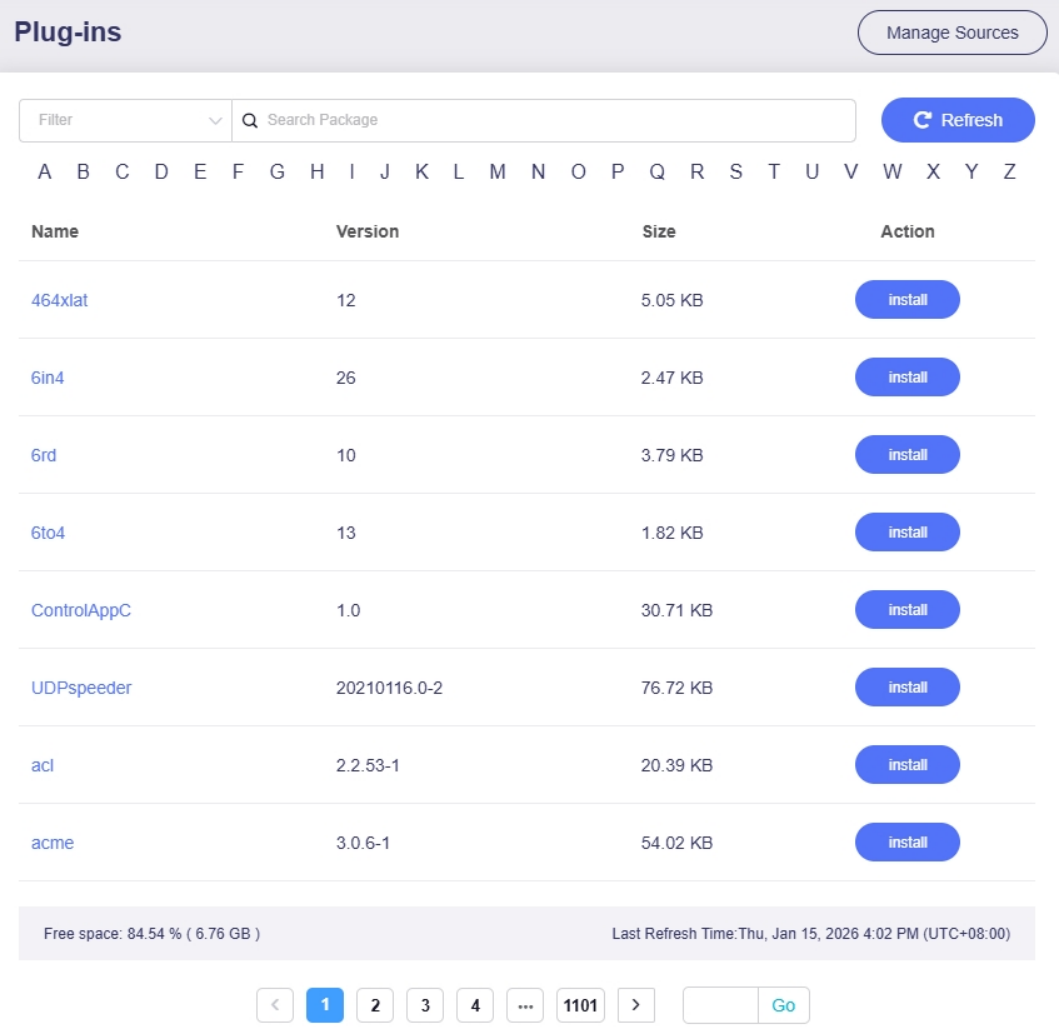
Aplikacje

W tym rozdziale przedstawiono wybrane aplikacje dostępne w routerach GL.iNet, np. wtyczki, Dynamic DNS, pamięć sieciową, AdGuard Home, kontrolę rodzicielską, ZeroTier, Tailscale i zarządzanie eSIM.

13.1 Wtyczki

Strona Plug-ins umożliwia zarządzanie pakietami OpenWrt.

Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Plug-ins.** Możesz instalować lub usuwać dowolne pakiety dostępne w repozytorium. Przed instalacją wtyczek kliknij przycisk **Refresh**, aby zaktualizować listę pakietów.



Uwaga:

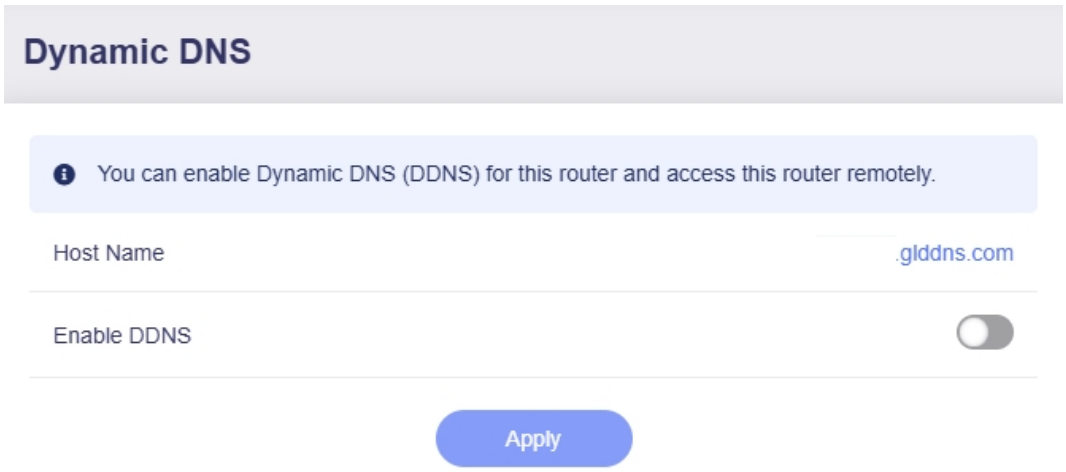
1. Nie zaleca się aktualizowania wtyczek zainstalowanych fabrycznie w oficjalnym oprogramowaniu GL.iNet, takich jak nginx, adguard home, tailscale itp.
2. Wtyczki zewnętrzne zainstalowane ręcznie przez użytkownika można aktualizować, jednak GL.iNet nie odpowiada za związane z nimi problemy z bezpieczeństwem. Pytania należy kierować do autorów odpowiednich wtyczek.

13.2 Dynamiczny DNS

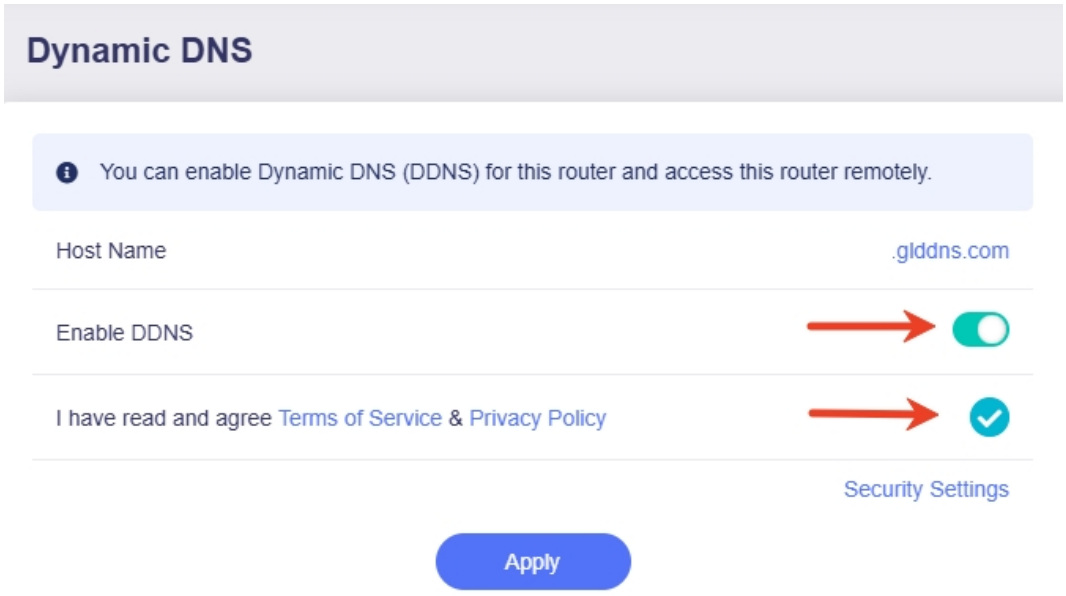
Dynamic Domain Name Service (DDNS, czyli dynamiczny DNS) to usługa mapująca nazwę domeny na dynamiczny adres IP urządzenia sieciowego. Dzięki niej można zdalnie uzyskiwać dostęp do routera. Ta funkcja wymaga publicznego adresu IP.

13.2.1 Włączanie DDNS

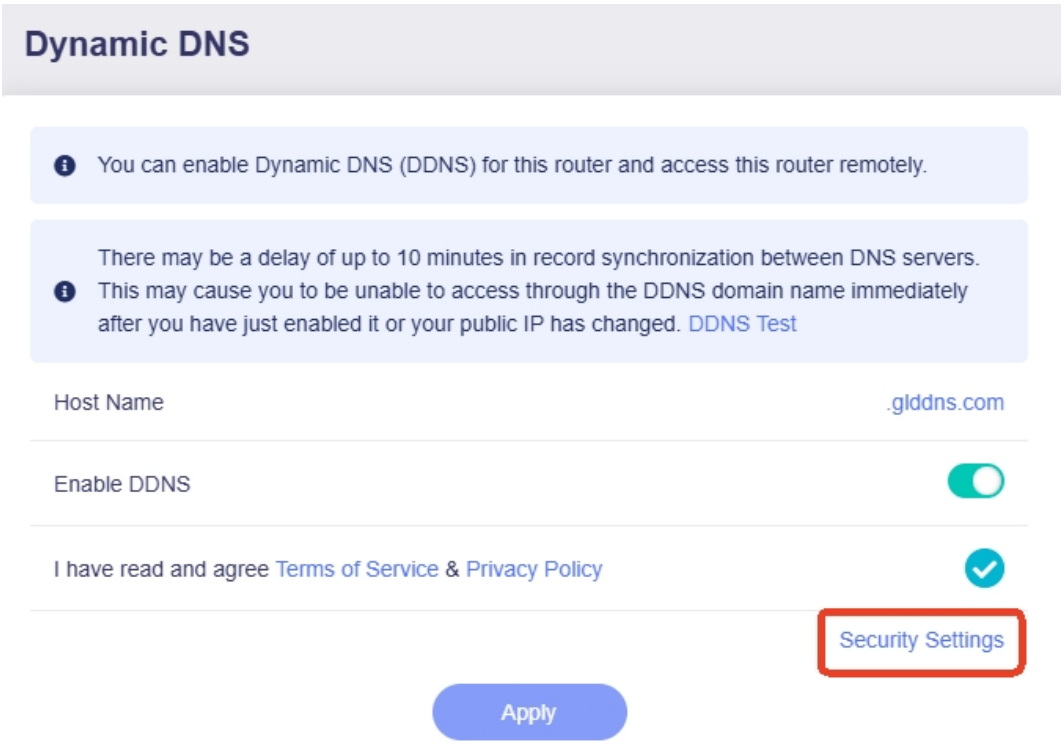
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Dynamic DNS**. Strona wygląda jak poniżej.



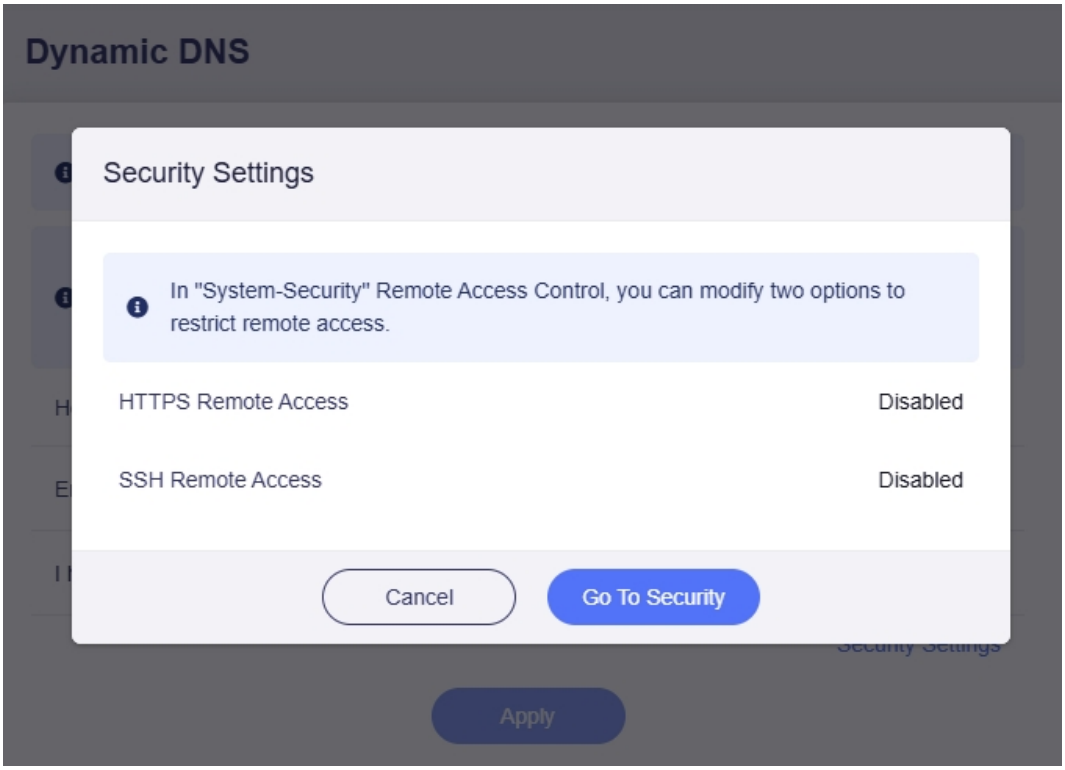
2. Włącz **Enable DDNS**, przeczytaj i zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



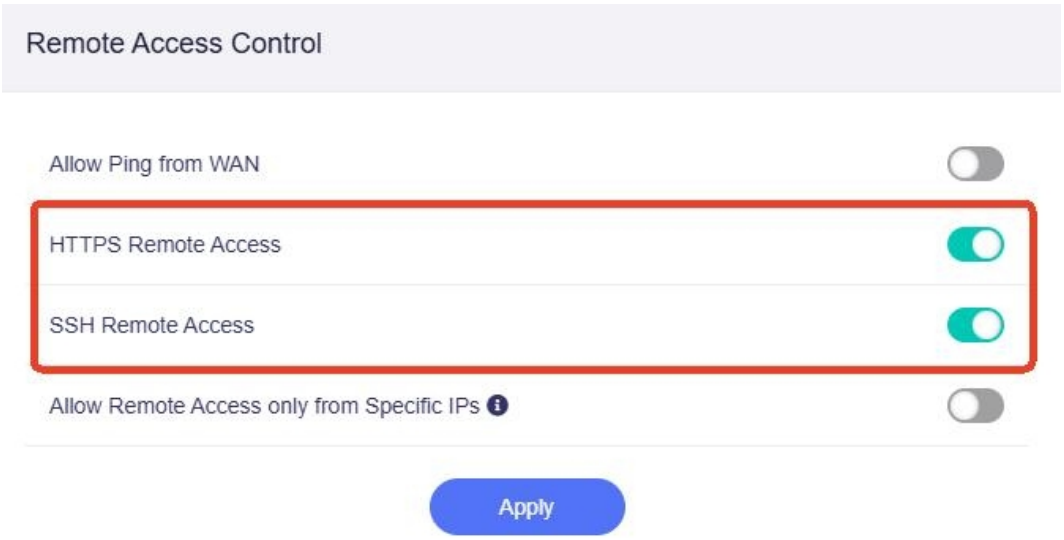
3. Kliknij **Security Settings** w prawym dolnym rogu.



4. W wyświetlonym oknie sprawdź, czy wybrany rodzaj dostępu zdalnego jest włączony.



Jeśli nie, przejdź do **SYSTEM** > **Security** > **Remote Access Control**, aby go włączyć, a następnie kliknij **Apply**.



Uwaga:

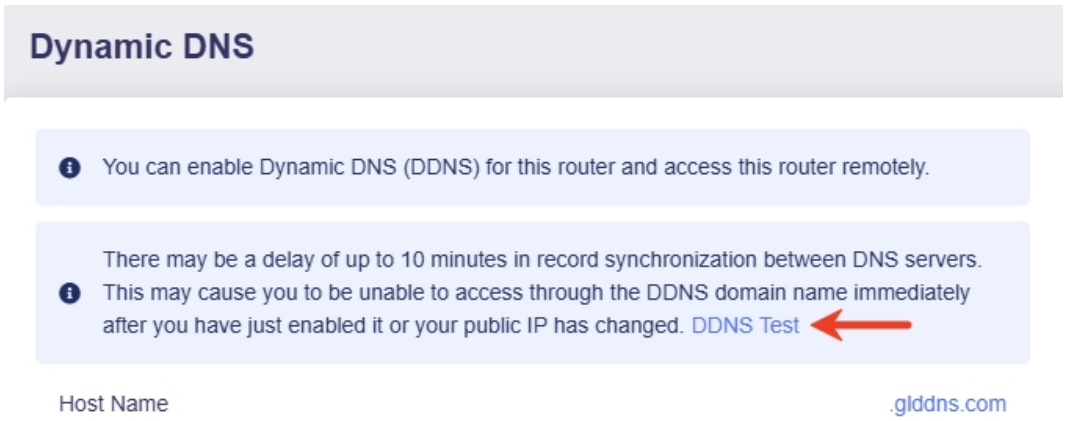
1. Synchronizacja rekordów między serwerami DNS może trwać do 10 minut. Może to uniemożliwić dostęp przez nazwę domeny DDNS bezpośrednio po włączeniu funkcji lub zmianie publicznego adresu IP.
2. Jeśli jednocześnie włączysz DDNS i klienta VPN, upewnij się, że opcja Services From GL.iNet Use VPN jest wyłączona.

13.2.2 Sprawdzanie działania DDNS

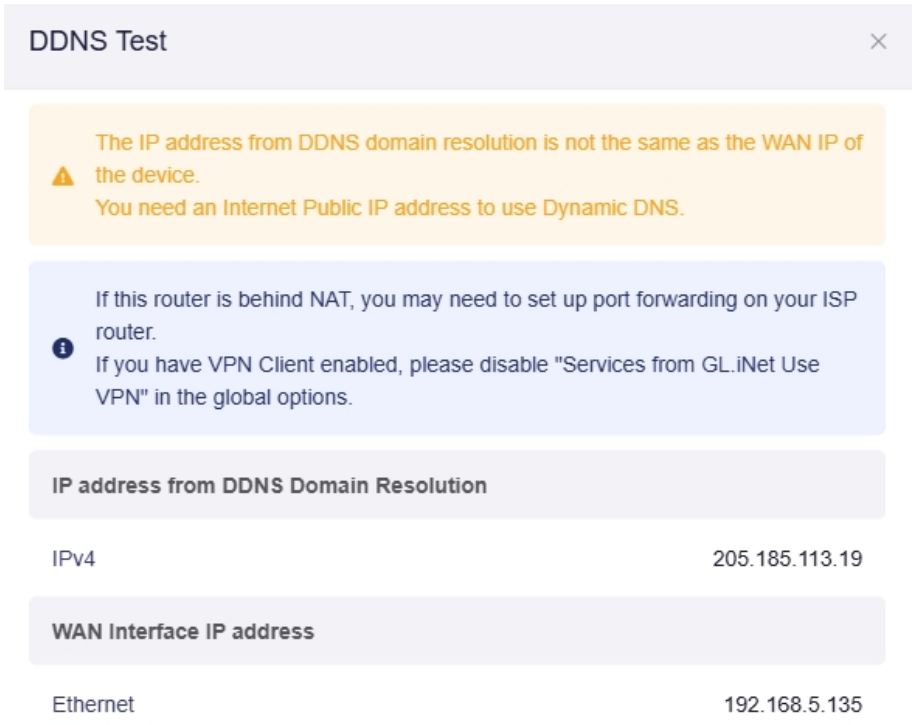
Działanie DDNS można sprawdzić za pomocą narzędzia testowego DDNS lub ręcznie, przy użyciu poleceń.

Metoda 1. Narzędzie DDNS Test

1. Na stronie Dynamic DNS kliknij **DDNS Test**.



2. Upewnij się, że adres IP uzyskany z rozwiązania nazwy domeny DDNS odpowiada adresowi WAN routera. W przeciwnym razie u góry pojawi się żółty komunikat wskazujący, że router może znajdować się za NAT i trzeba skonfigurować przekierowanie portów na routerze nadrzędnym.



Metoda 2. Polecenia

1. Użyj polecenia nslookup *nslookup xxxxxxx.glddns.com 8.8.8.8*, aby uzyskać mapowanie między nazwą domeny i adresem IP. Poniżej przedstawiono przykład na Beryl AX (GL-MT3000).



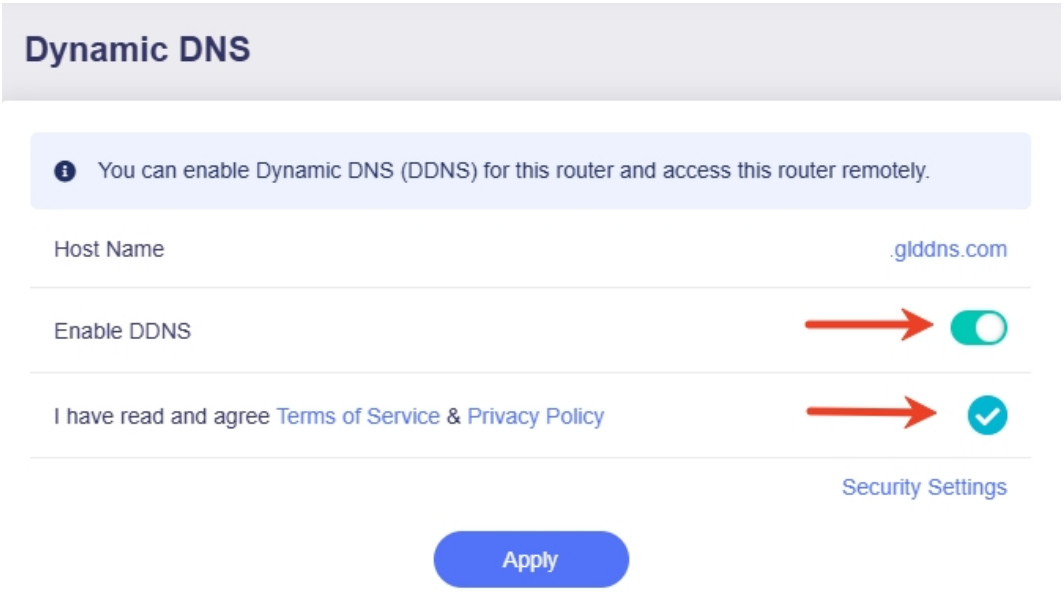
   - Zastąp „xxxxxxx.glddns.com” na powyższej ilustracji własną nazwą hosta.
   - „8.8.8.8” to serwer DNS Google. Użyj go lub zastąp innym adresem, a następnie naciśnij Enter.
2. Jeśli otrzymasz publiczny adres IP, taki jak „183.178.10.100” na powyższej ilustracji, domena DDNS została prawidłowo powiązana z publicznym adresem IP. Komunikat w rodzaju „server can’t find xxxxxxx.glddns.com” może oznaczać, że rozwiązanie nazwy domeny nie powiodło się i domena DDNS nie została prawidłowo powiązana z publicznym adresem IP. Przejdź do następnego kroku, aby to sprawdzić.
3. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET**. Znajdź adres IP WAN routera w aktualnie aktywnym interfejsie. Porównaj go z uzyskanym wyżej publicznym adresem IP. Jeśli są takie same, DDNS działa; w przeciwnym razie nie działa.

13.2.3 Zdalny dostęp przez HTTPS

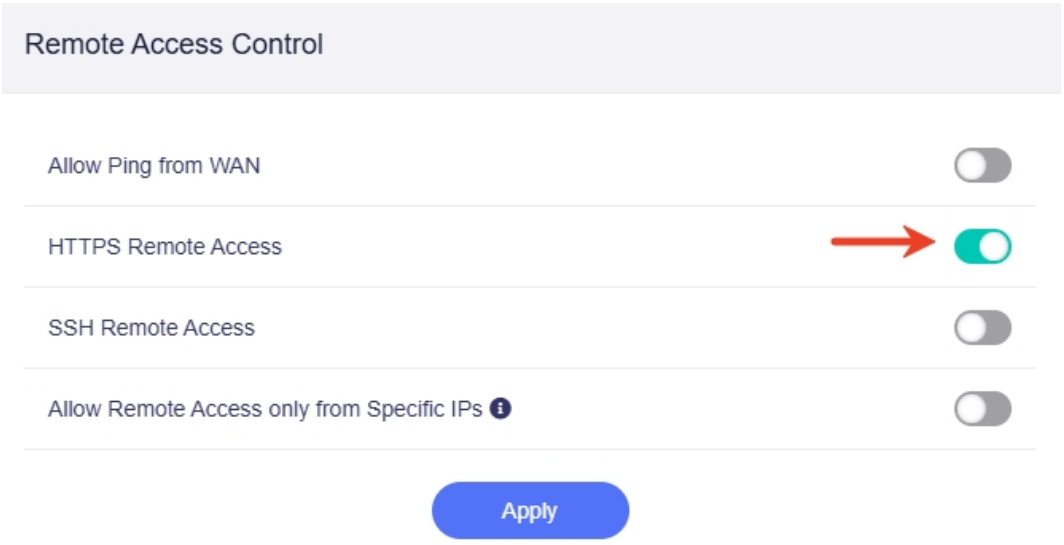
Do zdalnego dostępu przez HTTPS wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 443**) na routerze nadrzędnym dla dostępu HTTPS.

Aby włączyć zdalny dostęp do routera przez HTTPS, wykonaj poniższe czynności.

1. Na stronie Dynamic DNS włącz **Enable DDNS**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.

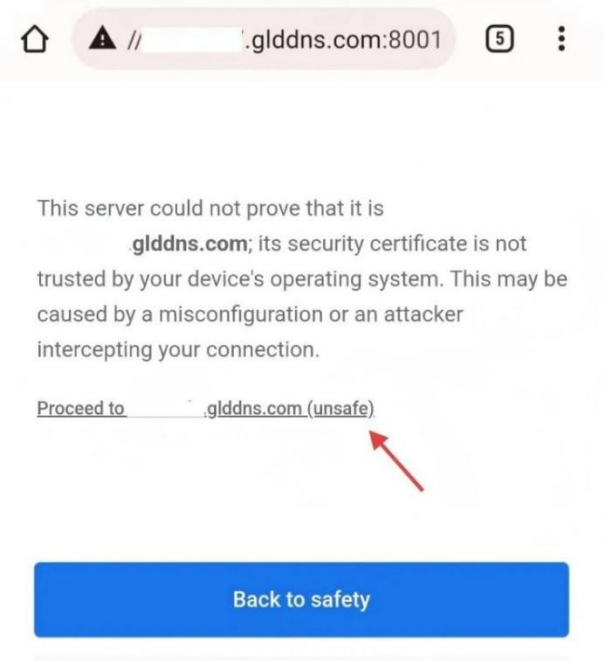


2. W panelu administracyjnym przejdź do **SYSTEM** > **Security** > **Remote Access Control**. Włącz **HTTPS Remote Access** i kliknij **Apply**.



3. Po włączeniu możesz z dowolnego miejsca uzyskiwać dostęp do panelu administracyjnego przez HTTPS, używając nazwy hosta DDNS, np. **https://xxxxxxx.glddns.com**. Jeśli skonfigurowano przekierowanie portów, użyj adresu **https://xxxxxxx.glddns.com:external_port** (zastąp external_port rzeczywistym numerem portu).

Uwaga: ta funkcja używa certyfikatów z podpisem własnym, dlatego przy dostępie do panelu administracyjnego przez HTTPS z nazwą hosta DDNS przeglądarka wyświetla komunikat „Your connection is not private”. Aby kontynuować dostęp zdalny HTTPS, kliknij **Advanced** u dołu, a następnie **Proceed to xxxxxxx.glddns.com** .



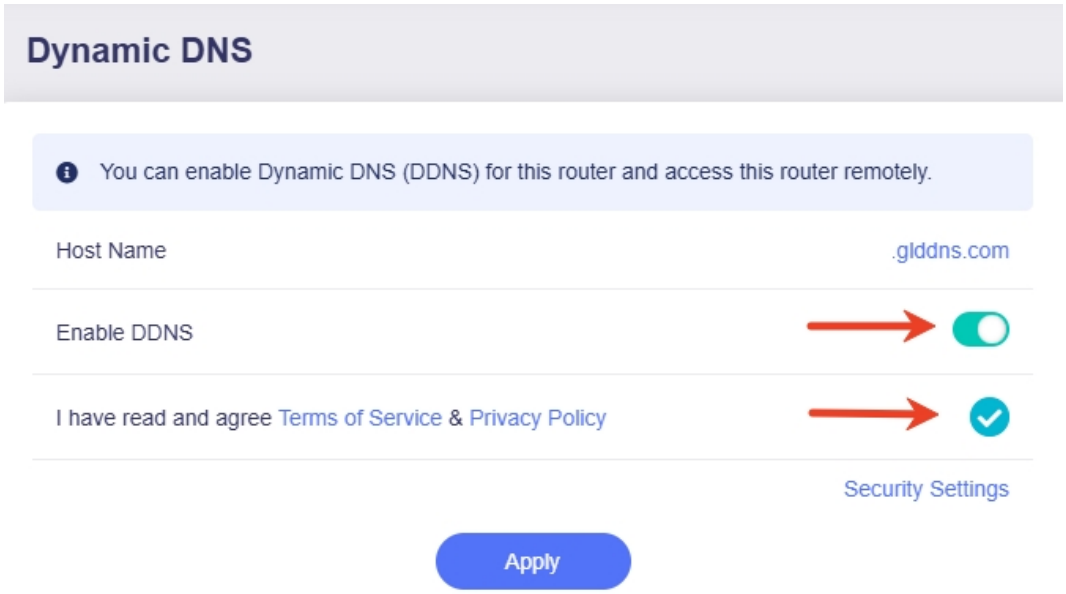
Możesz teraz uzyskiwać dostęp do panelu administracyjnego routera za pomocą nazwy hosta DDNS przez **HTTPS**.

13.2.4 Zdalny dostęp przez SSH

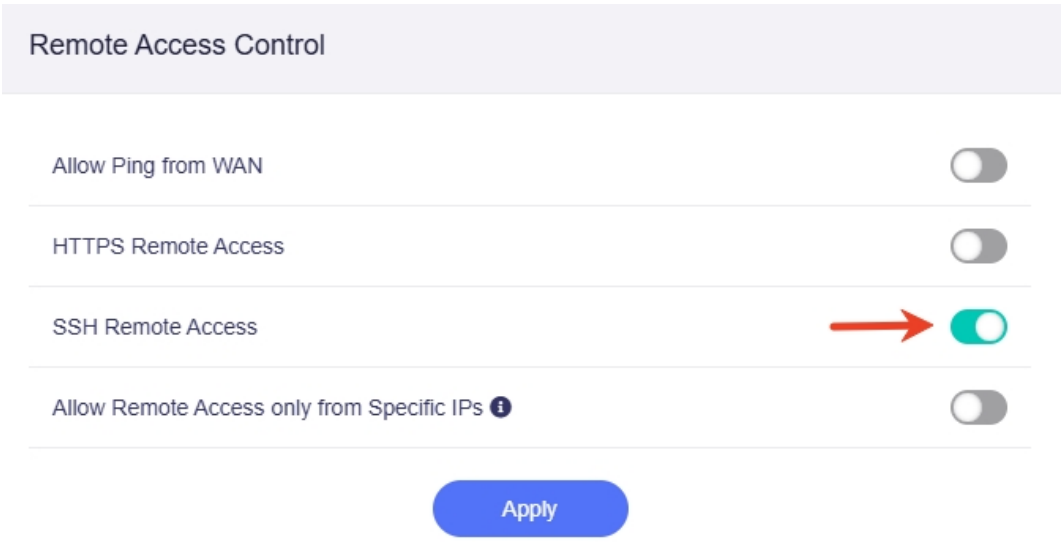
Do zdalnego dostępu przez SSH wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 22**) na routerze nadrzędnym dla zdalnego dostępu SSH.

Aby włączyć zdalny dostęp do routera przez SSH, wykonaj poniższe czynności.

1. Na stronie Dynamic DNS włącz **Enable DDNS**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



2. W panelu administracyjnym przejdź do **SYSTEM** > **Security** > **Remote Access Control**. Włącz **SSH Remote Access** i kliknij **Apply**.



Po włączeniu możesz z dowolnego miejsca uzyskiwać dostęp do panelu administracyjnego przez SSH, używając nazwy hosta DDNS, np. **ssh root@xxxxxxx.glddns.com**. Jeśli skonfigurowano przekierowanie portów, użyj **ssh root@xxxxxxx.glddns.com:external_port** (zastąp external_port rzeczywistym numerem portu).

13.3 Pamięć sieciowa

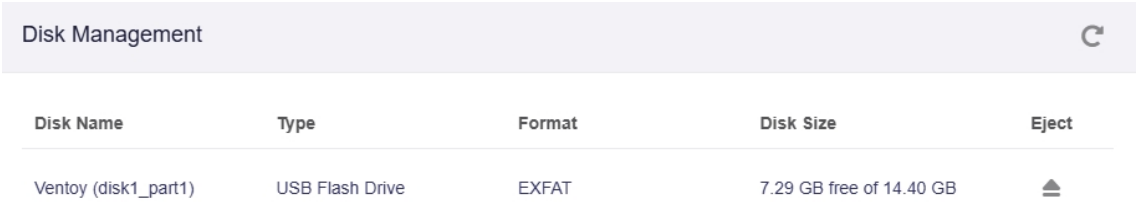
Pamięć sieciowa umożliwia bezprzewodowe udostępnianie plików między urządzeniami po podłączeniu nośnika USB lub karty SD do routera. Router przekształca nośnik w udostępniony dysk sieciowy, dostępny dla wszystkich urządzeń połączonych przez Wi-Fi.

Beryl AX ma port USB zgodny z pamięciami flash USB i przenośnymi zewnętrznymi dyskami twardymi. Dla tych nośników możesz skonfigurować Sambę, WebDAV lub DLNA z obsługą popularnych formatów, takich jak NTFS, FAT32 i EXT4.

Uwaga: dysk twardy USB pobiera stosunkowo dużo energii. Używaj zewnętrznego zasilacza, w przeciwnym razie mogą wystąpić nieprawidłowości w działaniu.

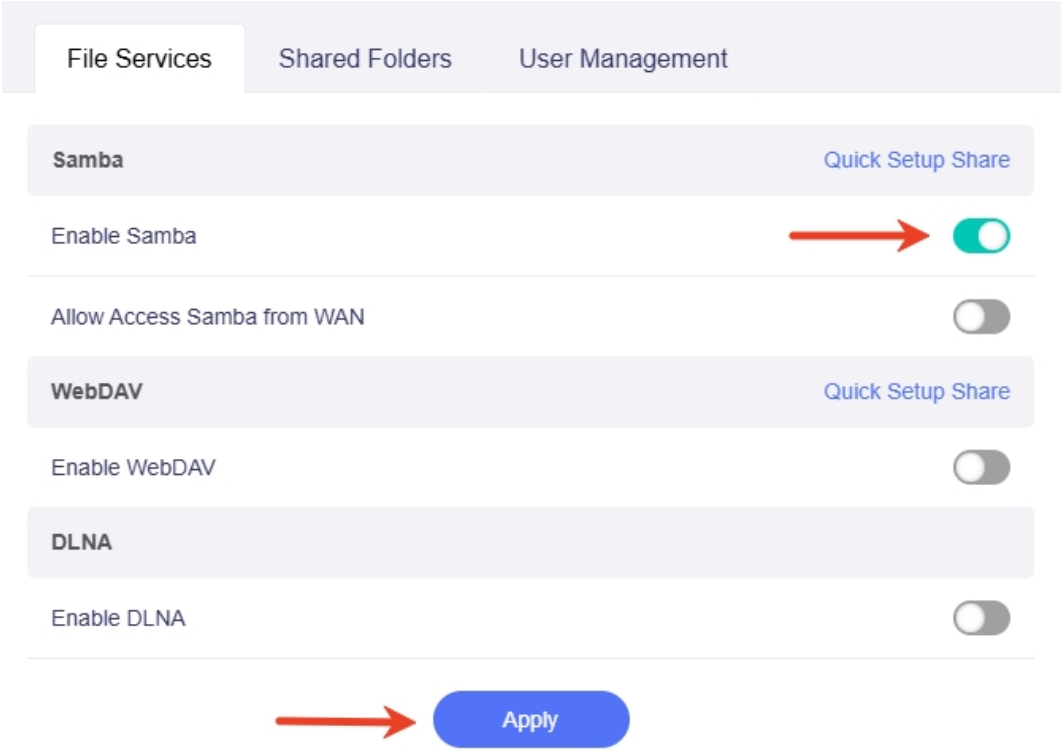
13.3.1 Podłączanie pamięci

1. Podłącz nośnik danych do routera.
   - Pamięć USB: podłącz ją bezpośrednio do portu USB.
   - Zewnętrzny dysk twardy: podłącz go do oddzielnego zasilacza (jeśli jest wymagany), a następnie do routera.
2. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Network Storage**. Tutaj możesz włączać usługi przesyłania plików i zarządzać folderem udostępnionym.
3. Po wykryciu nośnika danych sekcja **Disk Management** będzie wyglądać jak poniżej.



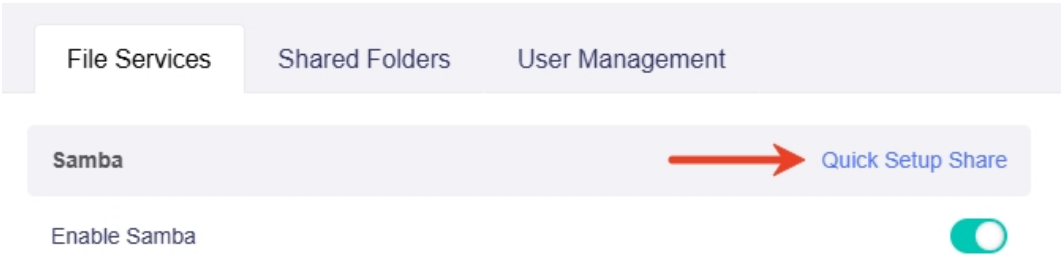
13.3.2 Konfiguracja usługi Samba

1. W sekcji **File Services** włącz **Enable Samba** i kliknij **Apply**.

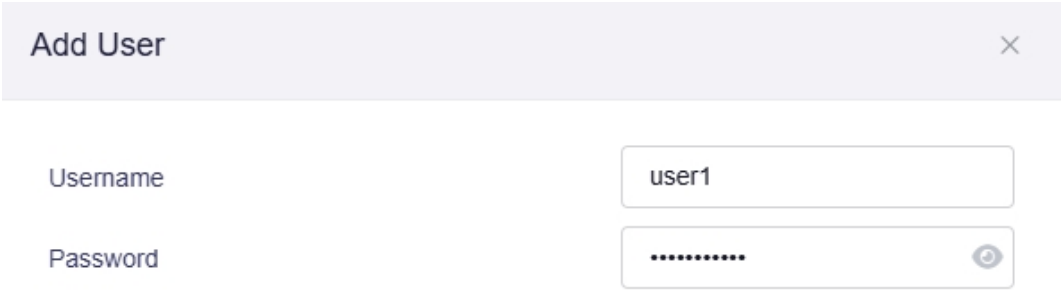


   - **Allow Access Samba from WAN**: włącz tę opcję, jeśli urządzenia w sieci nadrzędnej mają uzyskiwać dostęp do usługi Samba.

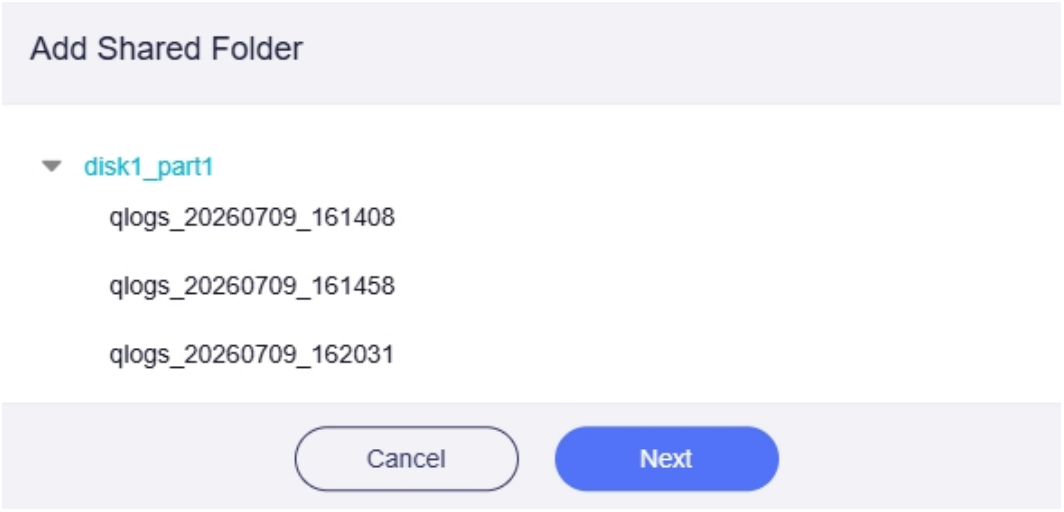
2. Kliknij **Quick Setup Share**, aby skonfigurować łącze do udostępnionego zasobu.



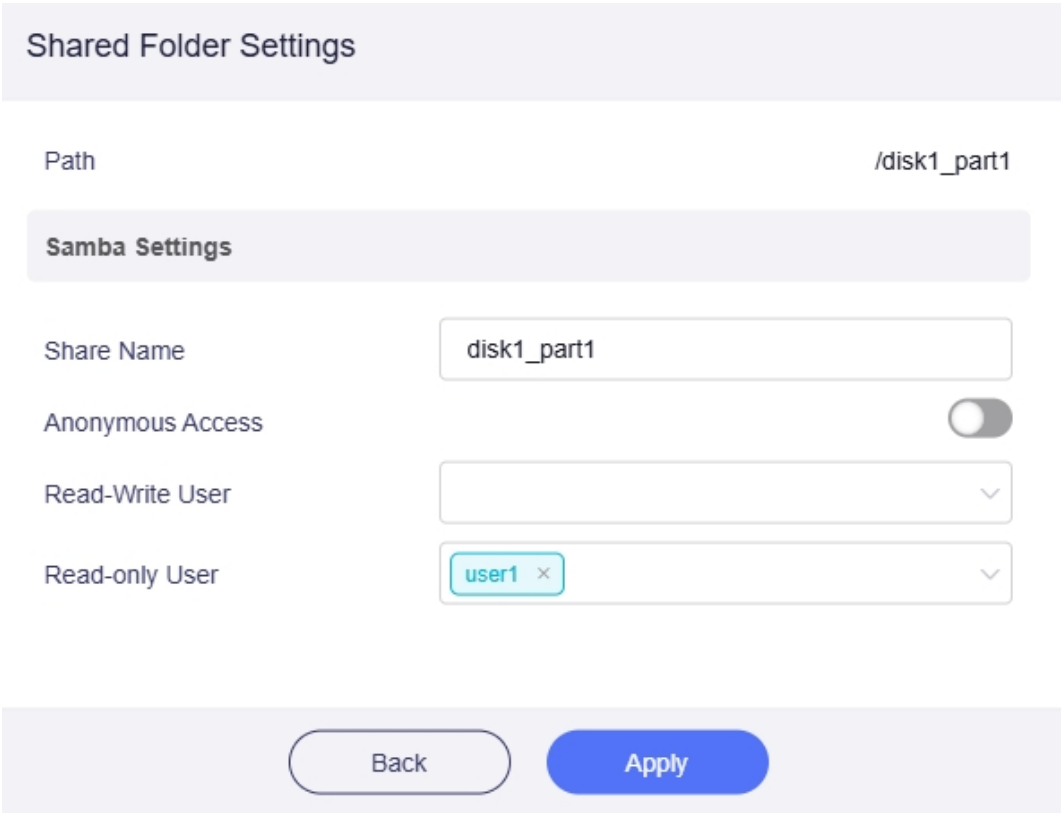
3. Dodaj użytkownika i kliknij **Next**. Jeśli konto już istnieje, ten krok zostanie pominięty.



4. Kliknij ikonę trójkąta, aby wyświetlić wszystkie foldery. Wybierz folder do udostępnienia i kliknij **Next**. Aby udostępnić cały dysk, kliknij jego nazwę (np. disk1_part1).



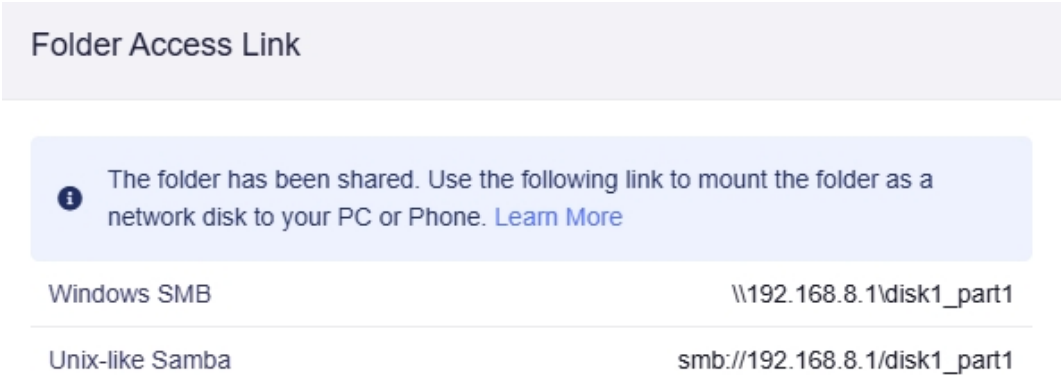
5. Skonfiguruj folder udostępniony.
   Użytkownik utworzony w poprzednim kroku jest domyślnie dodawany do **Read-Only User**. Aby mógł zapisywać lub usuwać pliki, usuń go z Read-Only User i dodaj do **Read-Write User**, a następnie kliknij **Apply**.



Wskazówka: ze względów bezpieczeństwa nie zaleca się włączania Anonymous Access.

6. Uzyskaj łącze dostępu do folderu.

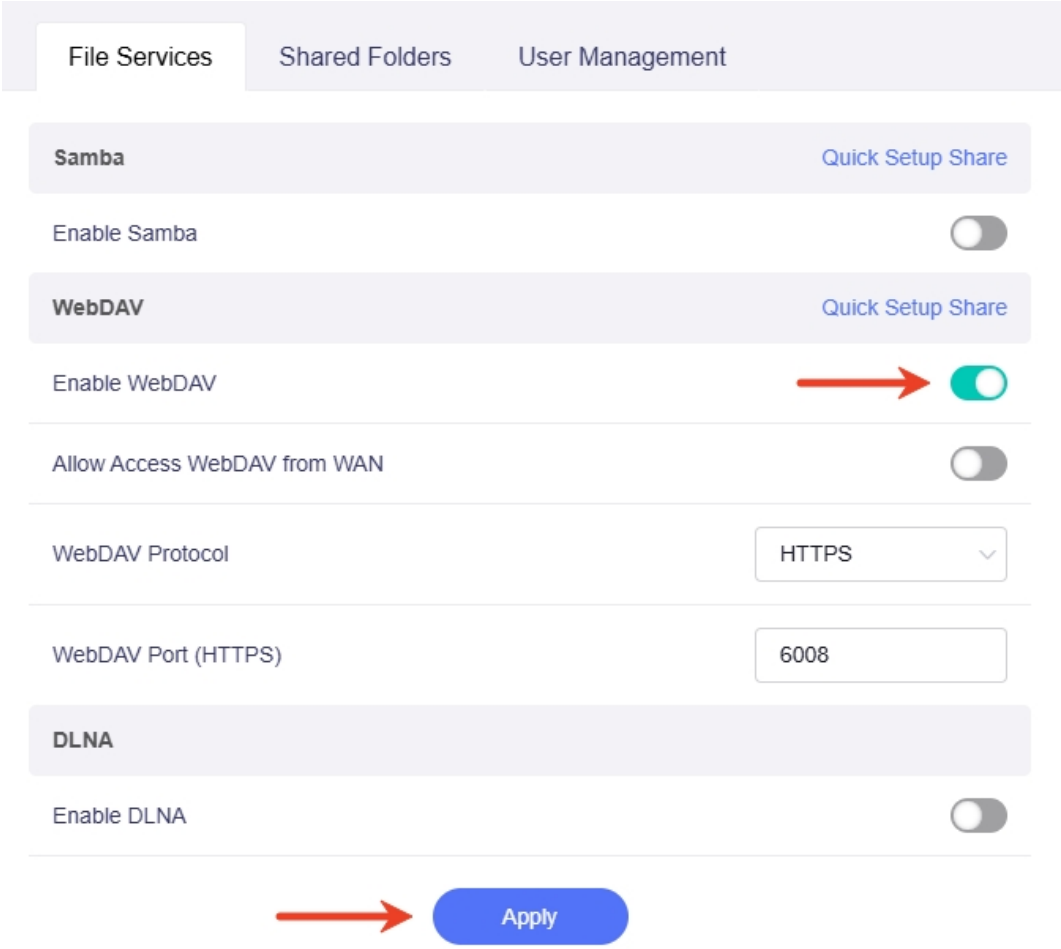
   Na stronie pojawią się łącza dla systemu Windows i systemów uniksopodobnych, takich jak Android, iOS, macOS, Ubuntu itp. Za ich pomocą można uzyskać dostęp do folderu udostępnionego przez usługę Samba.



Uwaga: jeśli włączysz **Allow Access Samba from WAN** i uzyskujesz dostęp do folderu z sieci nadrzędnej, zastąp adres IP routera w łączu (domyślnie 192.168.8.1) jego adresem IP WAN. Znajdziesz go na stronie INTERNET w panelu administracyjnym.

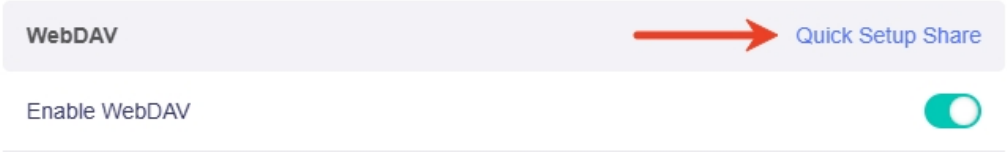
13.3.3 Konfiguracja WebDAV

1. W sekcji **File Services** włącz **Enable WebDAV** i kliknij **Apply**.

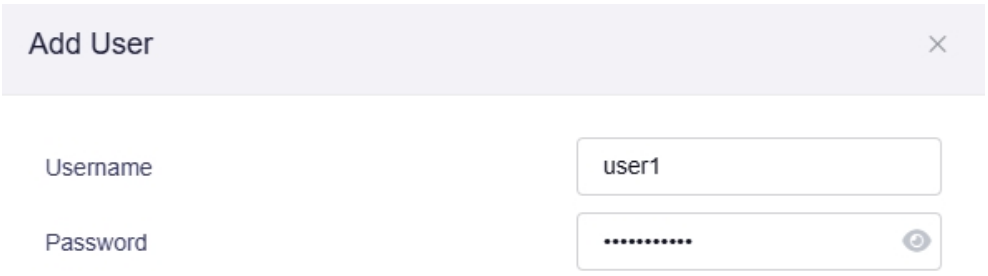


- **Allow Access WebDAV from WAN**: włącz tę opcję, jeśli urządzenia w sieci nadrzędnej mają uzyskiwać dostęp do usługi WebDAV.
- **WebDAV Protocol**: HTTP nie jest szyfrowany; korzystasz z niego na własne ryzyko. HTTPS jest szyfrowany i używa certyfikatu z podpisem własnym.
- **WebDAV Port**: nie trzeba zmieniać numeru portu, chyba że występuje konflikt. Zalecany zakres numerów portów to 1024–65535.

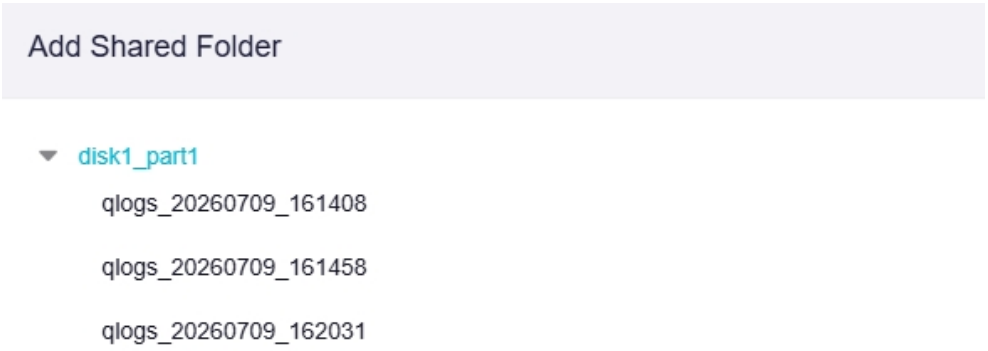
2. Kliknij **Quick Setup Share**, aby skonfigurować łącze do udostępnionego zasobu.



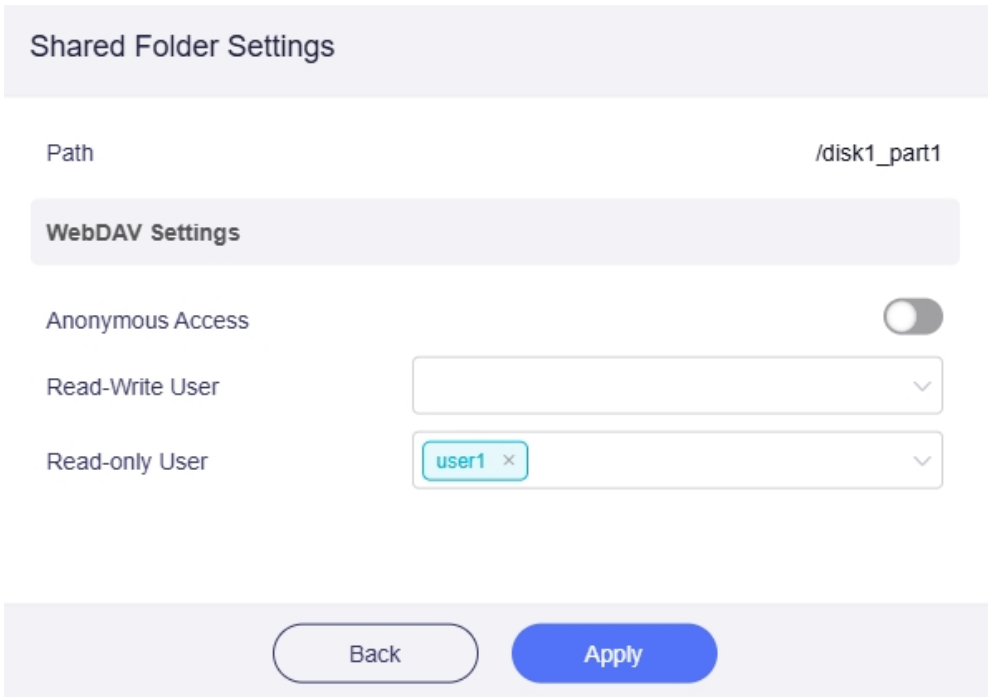
3. Dodaj użytkownika i kliknij **Next**. Jeśli konto już istnieje, ten krok zostanie pominięty.



4. Kliknij ikonę trójkąta, aby wyświetlić wszystkie foldery. Wybierz folder do udostępnienia. Aby udostępnić cały dysk, kliknij jego nazwę (np. disk1_part1).



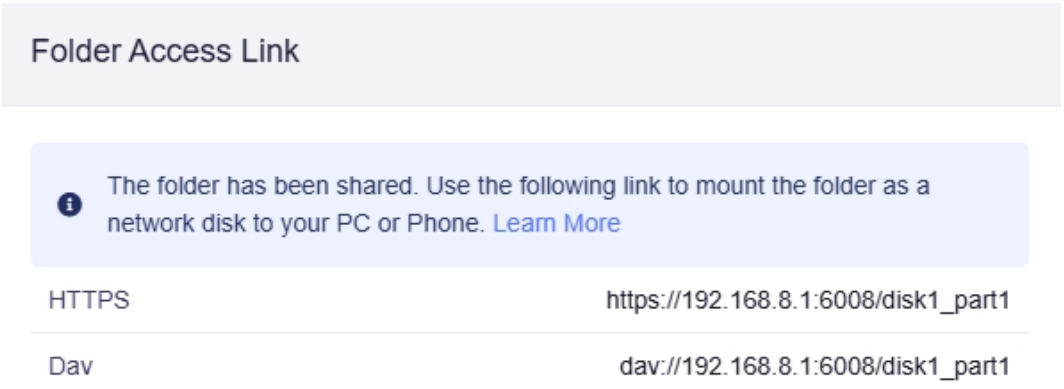
5. Skonfiguruj folder udostępniony.
   Użytkownik utworzony w poprzednim kroku jest domyślnie dodawany do **Read-Only User**. Aby użytkownik mógł zapisywać lub usuwać pliki, usuń go z Read-Only User i dodaj do **Read-Write User**, a następnie kliknij **Apply**.



Wskazówka: ze względów bezpieczeństwa nie zaleca się włączania Anonymous Access.

6. Uzyskaj łącze dostępu do folderu.

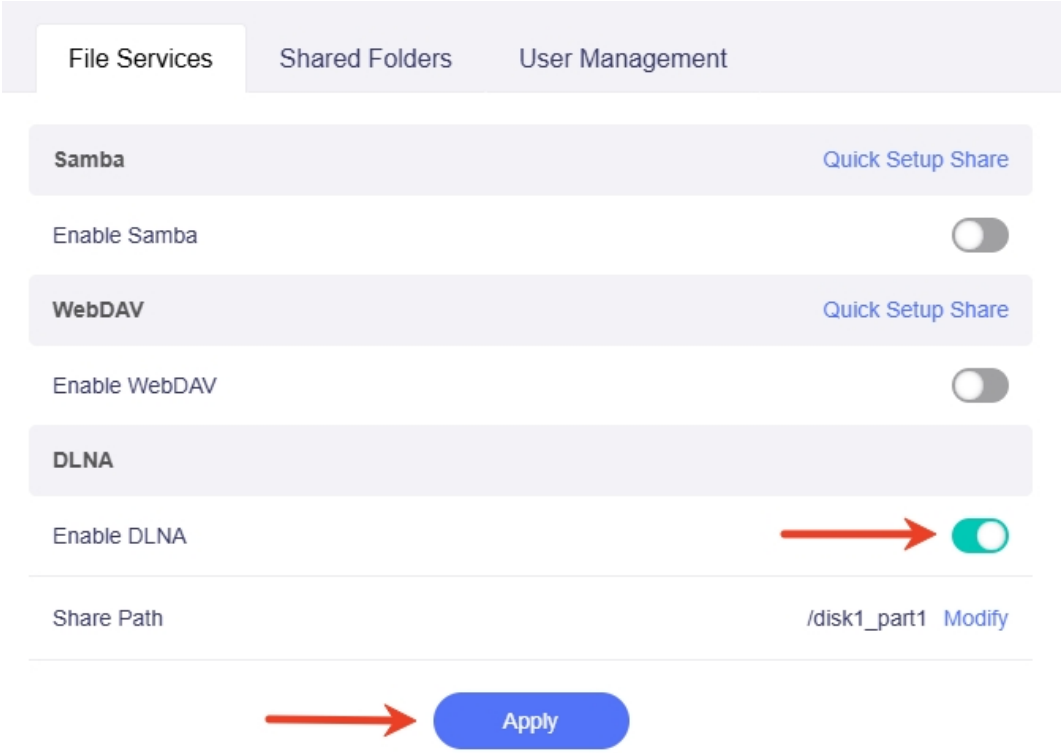
   Na stronie pojawią się łącza dla systemu Windows i systemów uniksopodobnych, takich jak Android, iOS, macOS, Ubuntu itp. Za ich pomocą można uzyskać dostęp do folderu udostępnionego przez usługę WebDAV.



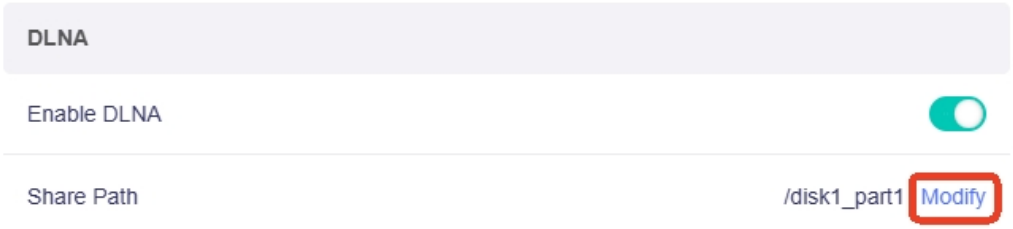
Uwaga: jeśli włączysz **Allow Access WebDAV from WAN** i uzyskujesz dostęp do folderu z sieci nadrzędnej, zastąp adres IP routera w łączu (domyślnie 192.168.8.1) jego adresem IP WAN. Znajdziesz go na stronie INTERNET w panelu administracyjnym.

13.3.4 Konfiguracja DLNA

1. W sekcji **File Services** włącz **Enable DLNA** i kliknij **Apply**.



2. W razie potrzeby zmień Share Path po prawej stronie.



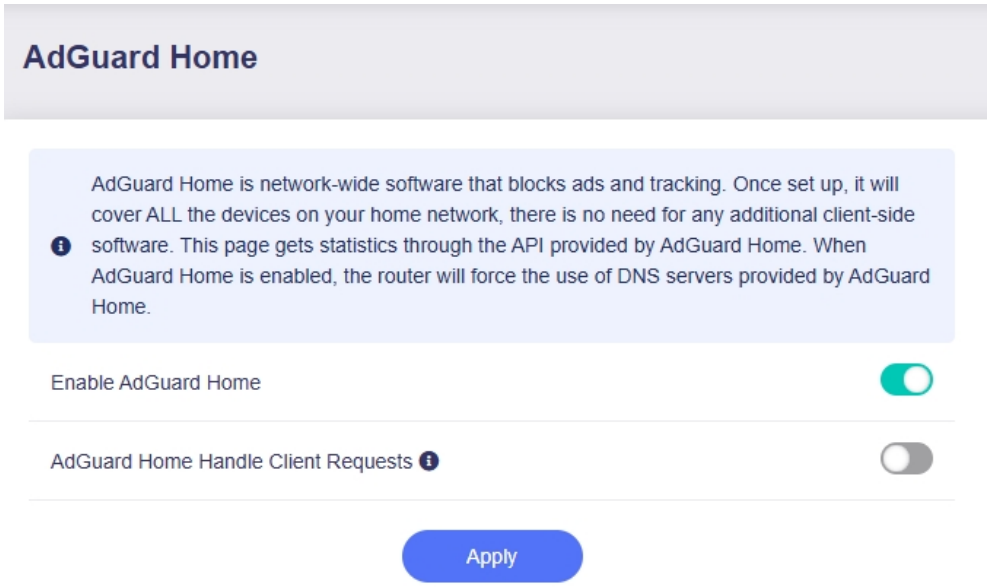
3. Podłącz telewizor Smart TV do routera. Automatycznie wykryje serwer DLNA.

13.4 AdGuard Home

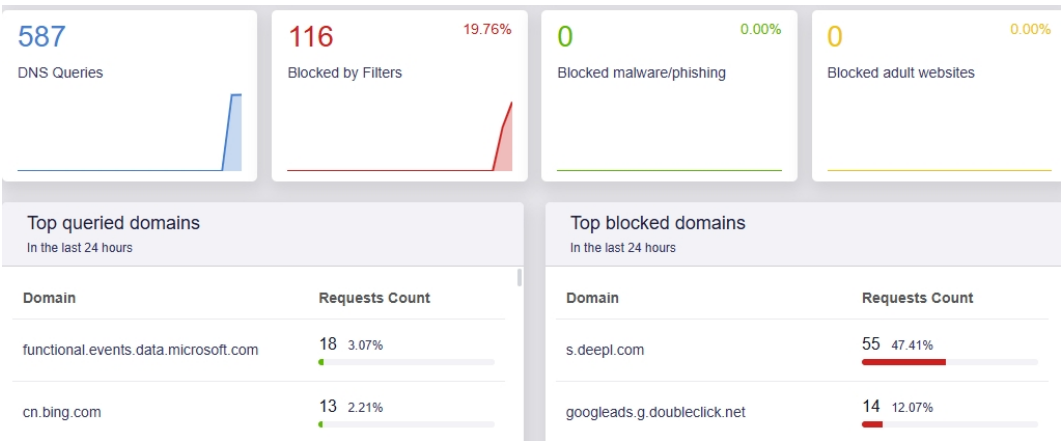
AdGuard Home to oprogramowanie blokujące reklamy i śledzenie w całej sieci. Po konfiguracji obejmuje wszystkie urządzenia klienckie bez konieczności instalowania na nich dodatkowego oprogramowania.

Aby skonfigurować AdGuard Home, wykonaj poniższe czynności.

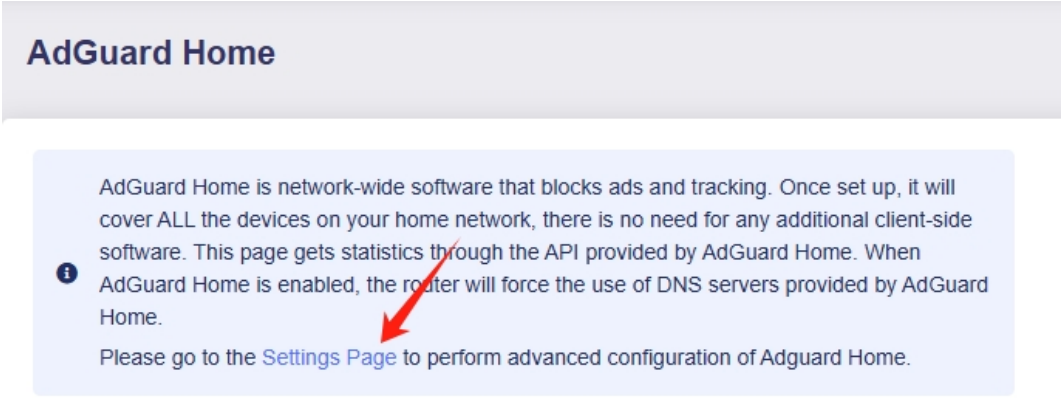
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **AdGuard Home**. Włącz **Enable AdGuard Home** i kliknij **Apply**.



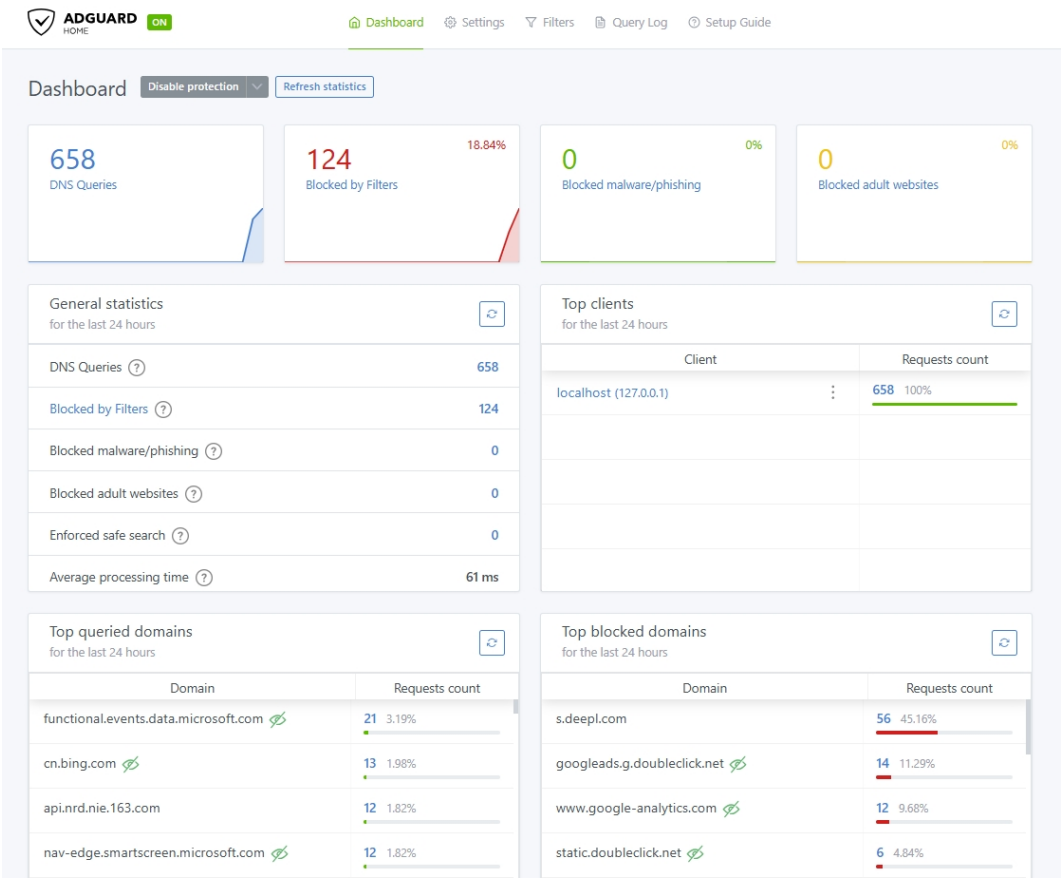
   - **AdGuard Home Handles Client Requests**: po włączeniu zapytania DNS urządzeń klienckich są obsługiwane bezpośrednio przez AdGuard Home, ale powoduje to niedziałanie reguł VPN opartych na domenach.
2. Strona automatycznie pobiera statystyki DNS (zapytania, zablokowane domeny itp.) przez API udostępniane przez AdGuard Home.



3. Kliknij **Settings Page**, aby skonfigurować zaawansowane ustawienia AdGuard Home.



4. Otworzy się strona ustawień AdGuard Home. Aby uzyskać pomoc, odwiedź [Centrum pomocy AdGuard Home].


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

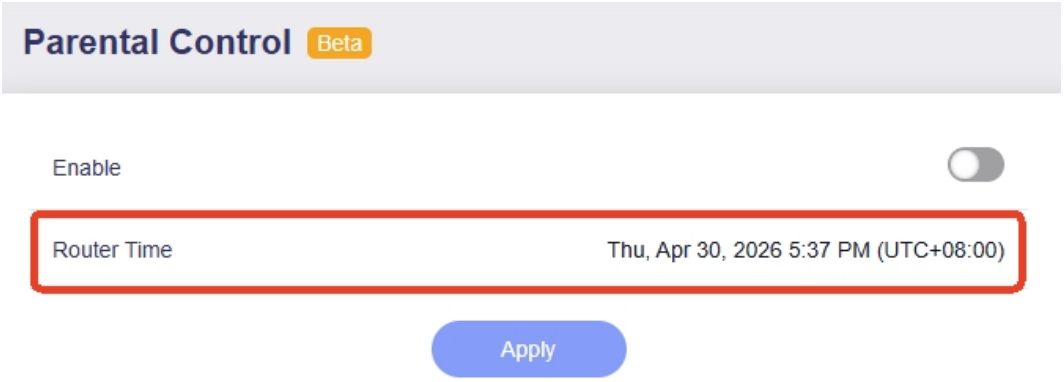
13.5 Kontrola rodzicielska

Kontrola rodzicielska pomaga chronić dzieci w Internecie przez blokowanie nieodpowiednich witryn i ograniczanie czasu korzystania z urządzeń. Zapobiega dostępowi do szkodliwych treści, ułatwia zarządzanie czasem przed ekranem i pomaga dzieciom odpowiedzialnie korzystać z Internetu.

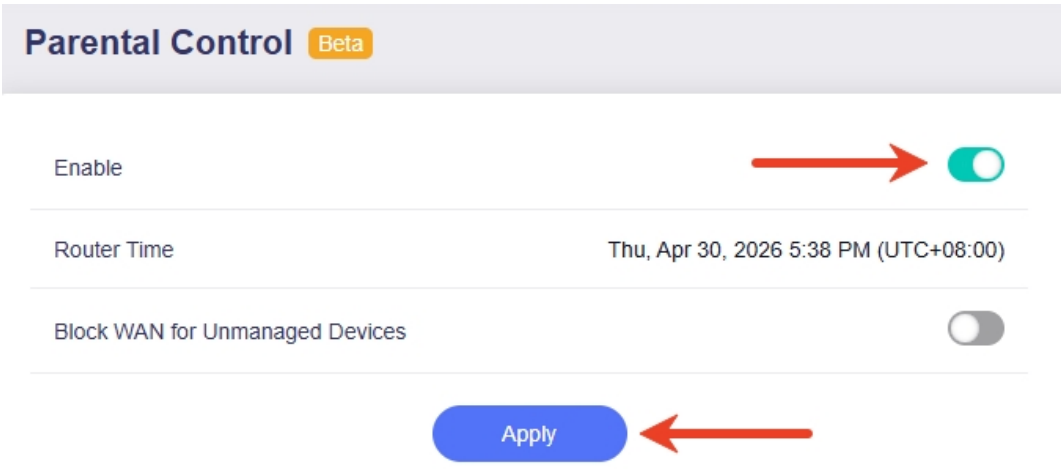
13.5.1 Szybka konfiguracja

Aby skonfigurować kontrolę rodzicielską na routerach GL.iNet, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Parental Control.** Upewnij się, że czas routera jest prawidłowy. Jeśli nie, najpierw przejdź do **SYSTEM** > **Time Zone**, aby go zsynchronizować.



2. Włącz kontrolę rodzicielską i kliknij **Apply**. Następnie skonfiguruj ją zgodnie z kreatorem. Film instruktażowy znajdziesz również tutaj.



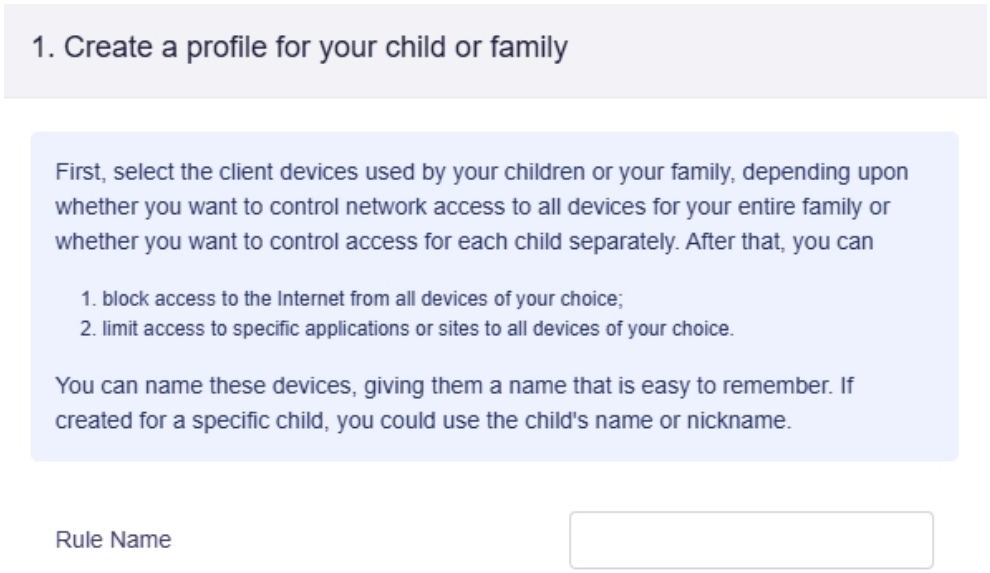
- **Block WAN for Unmanaged Devices**: blokuje dostęp do Internetu wszystkim urządzeniom, których nie ma na liście kontroli rodzicielskiej.

Poniżej przedstawiono przykładowe zastosowanie.

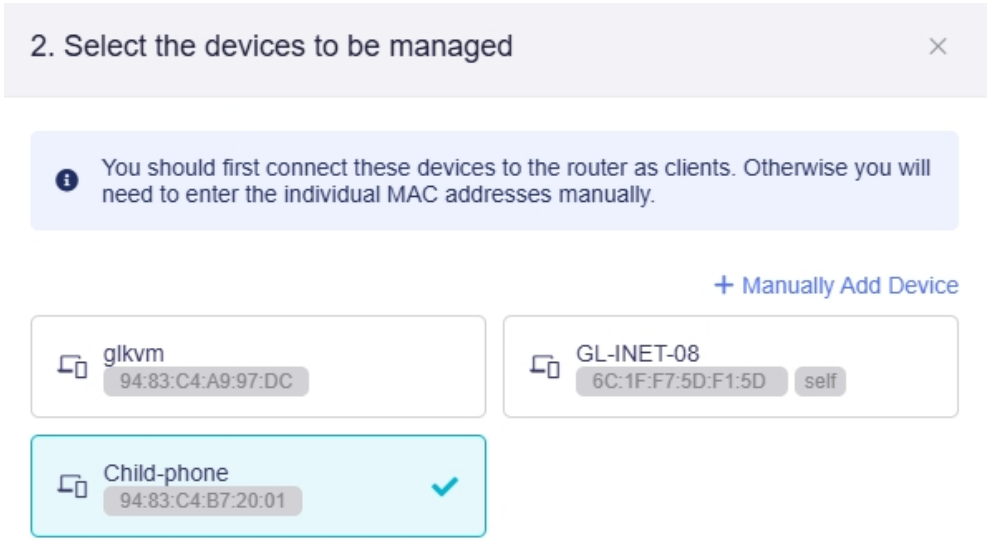
Scenariusz: urządzenia w tym profilu mogą korzystać z Internetu wyłącznie do nauki od 8:00 do 11:00 w dni robocze i do grania od 18:00 do 20:00 w weekendy. W pozostałych godzinach dostęp do Internetu jest domyślnie zablokowany.

Etapy konfiguracji:

1. Utwórz profil i nadaj mu nazwę.

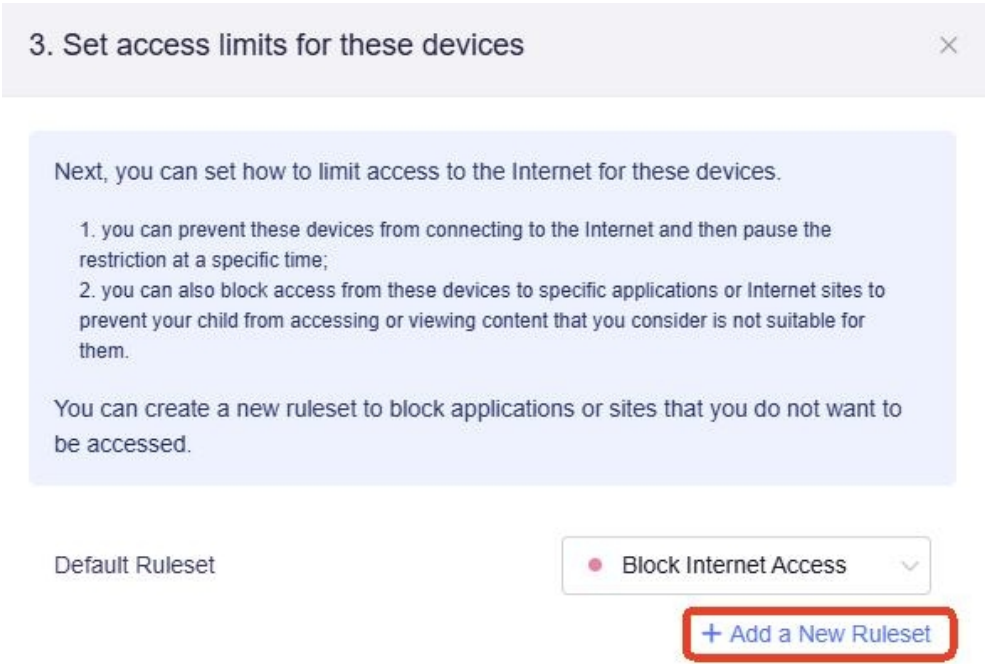


2. Wybierz urządzenia, którymi chcesz zarządzać. Najpierw podłącz je do routera. Jeśli nie były jeszcze podłączane, dodaj je ręcznie, wprowadzając ich adresy MAC.

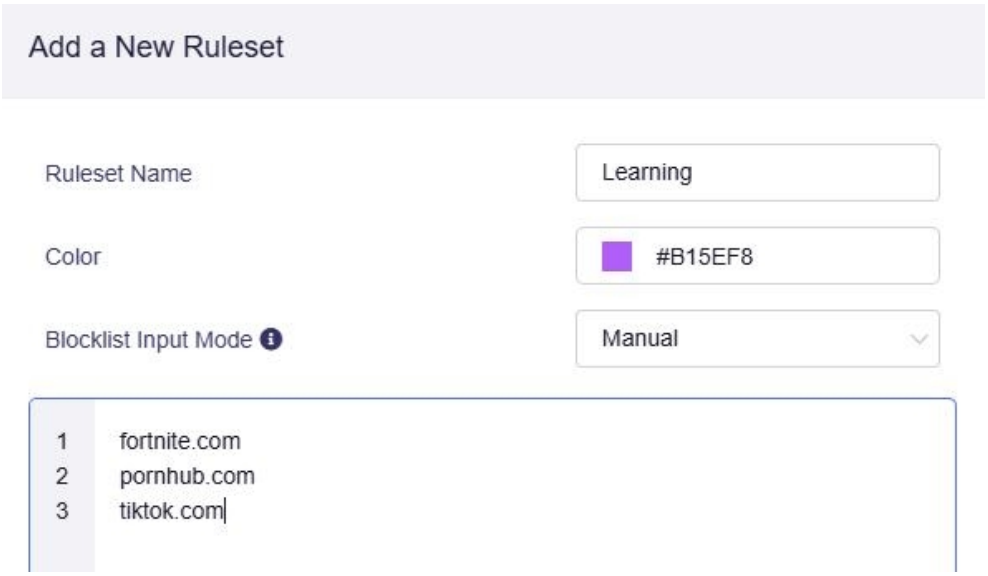


3. Ustaw ograniczenia dostępu.

Dostępne są dwa domyślne zestawy reguł: **Block Internet Access** i **No Limit**.
Kliknij **Add a New Ruleset**, aby utworzyć dwa dodatkowe zestawy reguł do późniejszego użycia: **Learning** i **Play**.

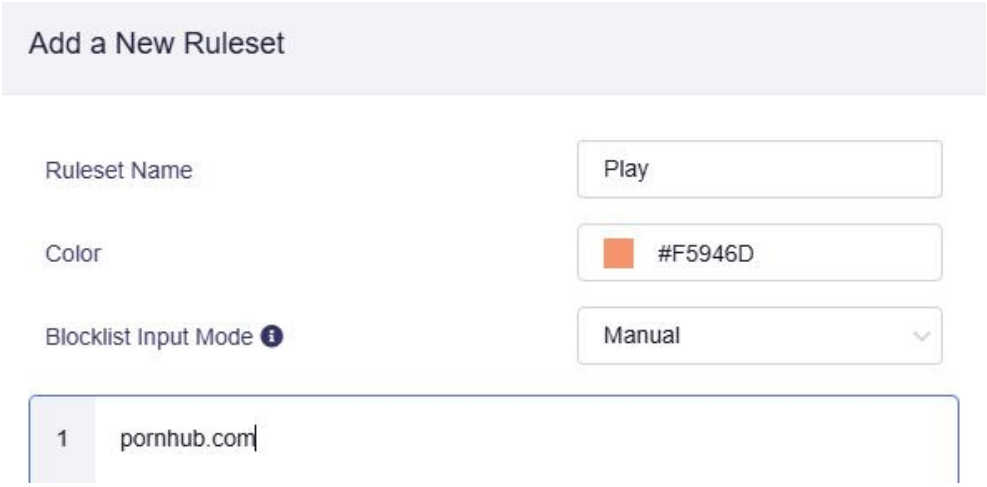


Określ nazwę zestawu reguł (np. Learning) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.

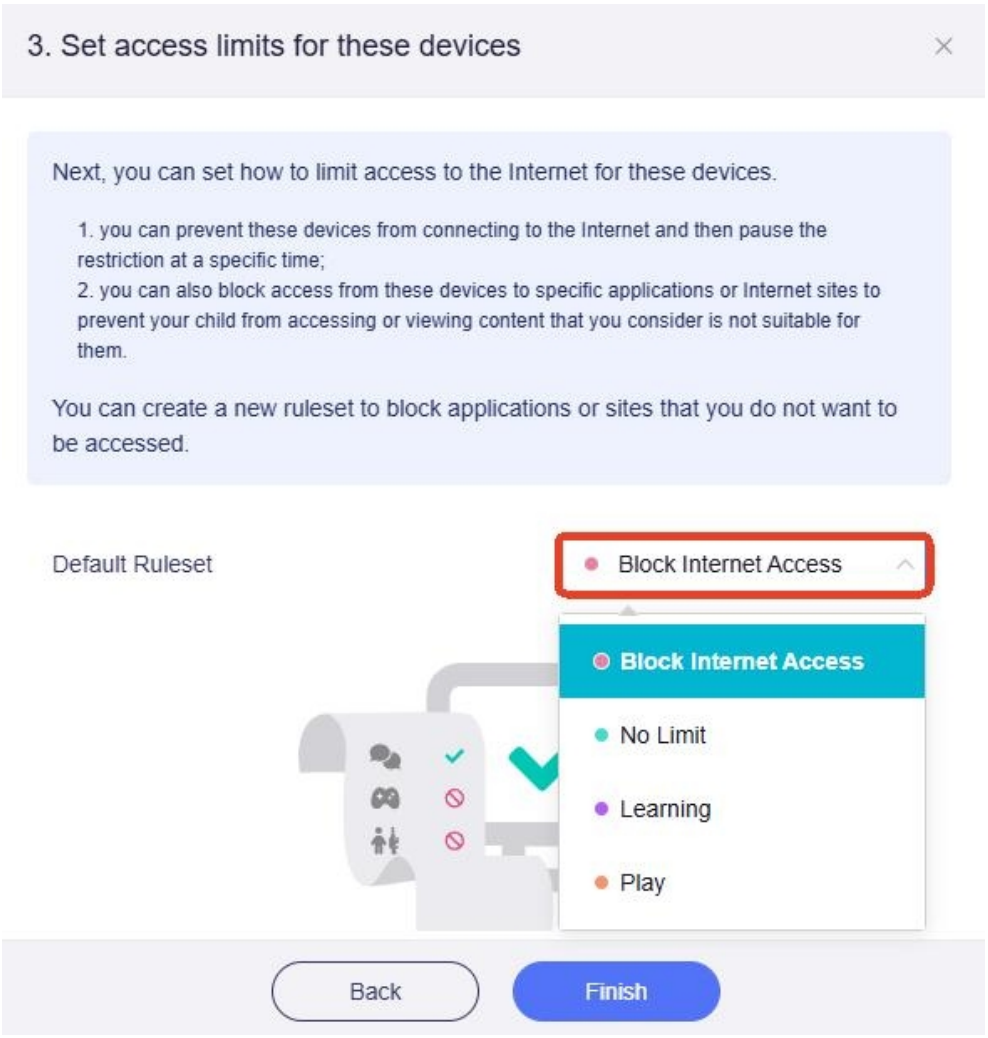


Uwaga: nazwy domen dodane do listy blokowanych obejmują również ich subdomeny. Na przykład wpis „example.com” obejmuje także każdą subdomenę, np. „subdomain.example.com”.

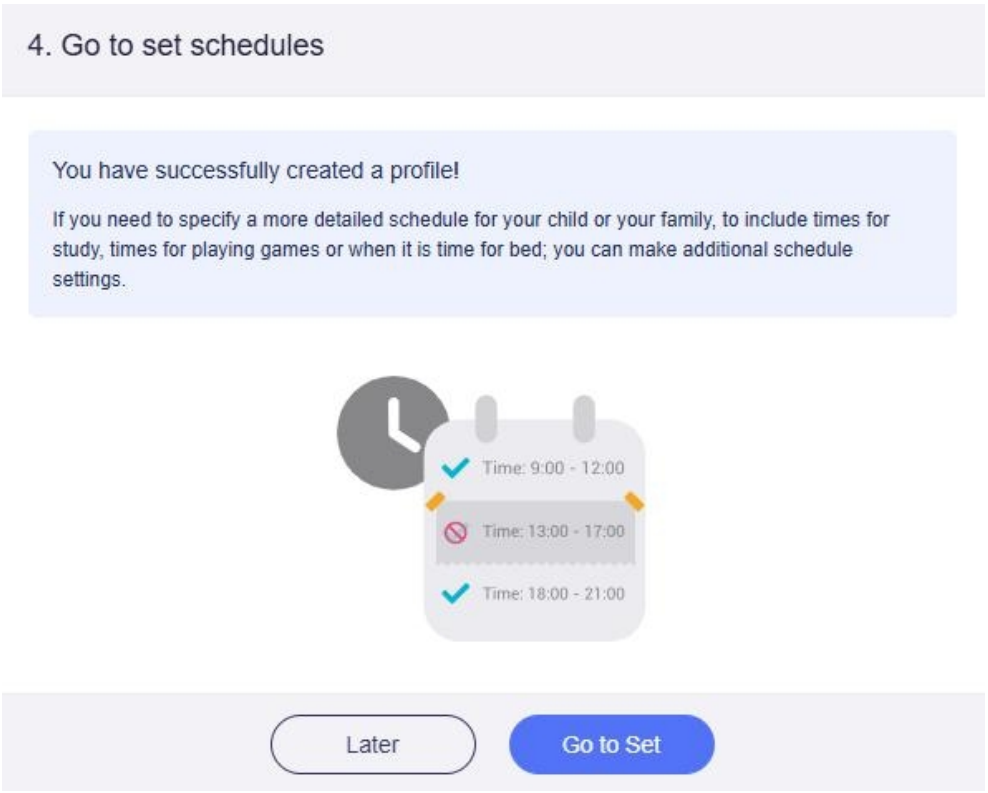
Podobnie utwórz drugi zestaw reguł. Określ jego nazwę (np. Play) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.



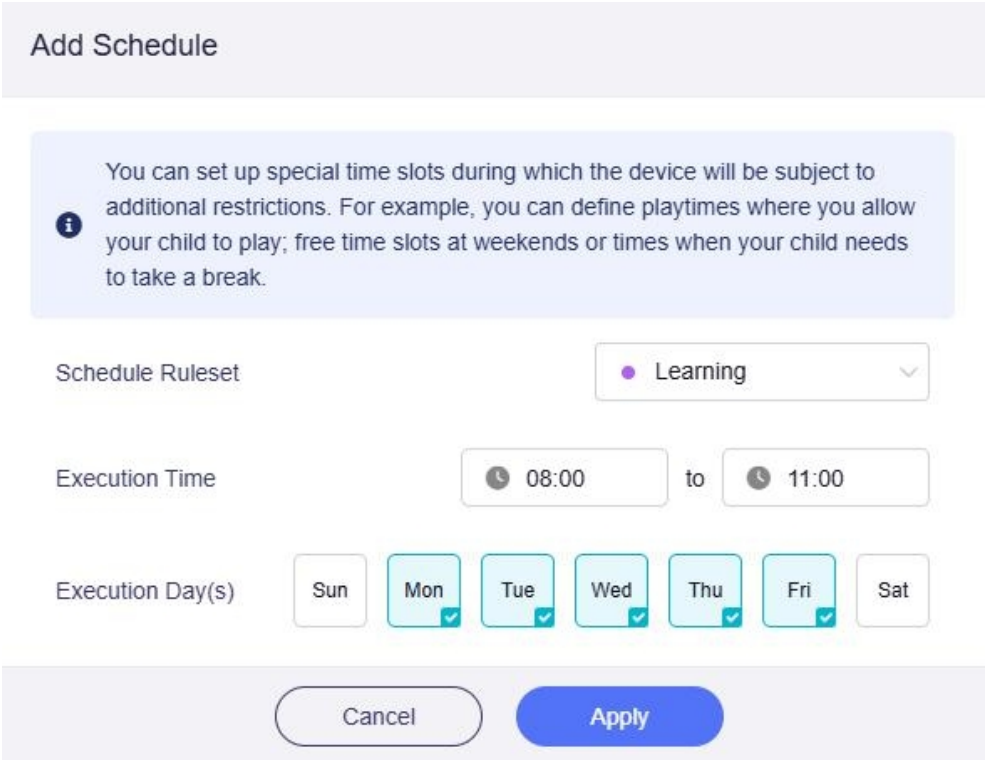
Po zastosowaniu ustawień dostępne będą cztery zestawy reguł. Wybierz **Block Internet Access** jako **Default Ruleset** i kliknij **Finish**.



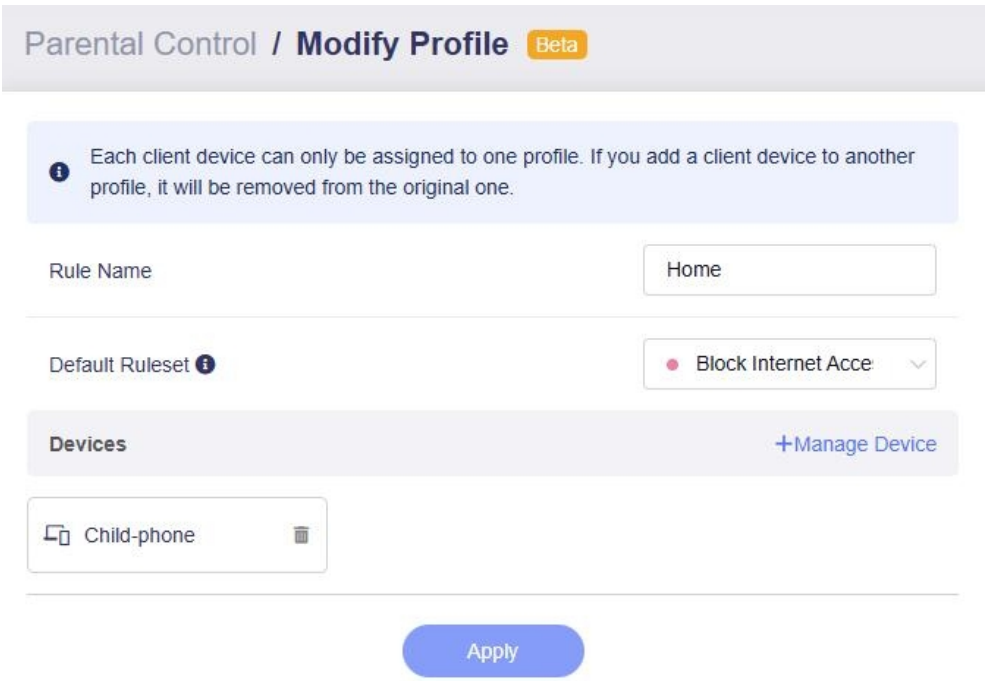
4. Następnie ustaw harmonogram profilu. Kliknij **Go to Set**.



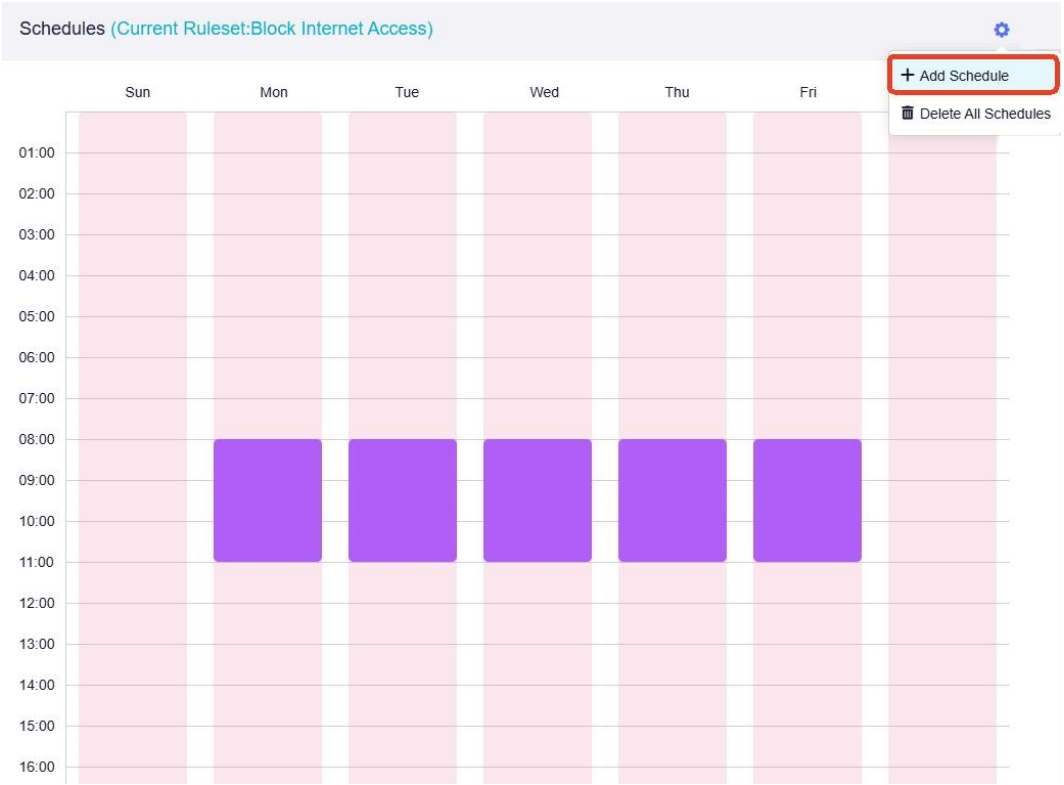
Dodaj zestaw reguł **Learning** do harmonogramu. Ustaw **Execution Time** od 8:00 do 11:00 w dni robocze, a następnie kliknij **Apply**.



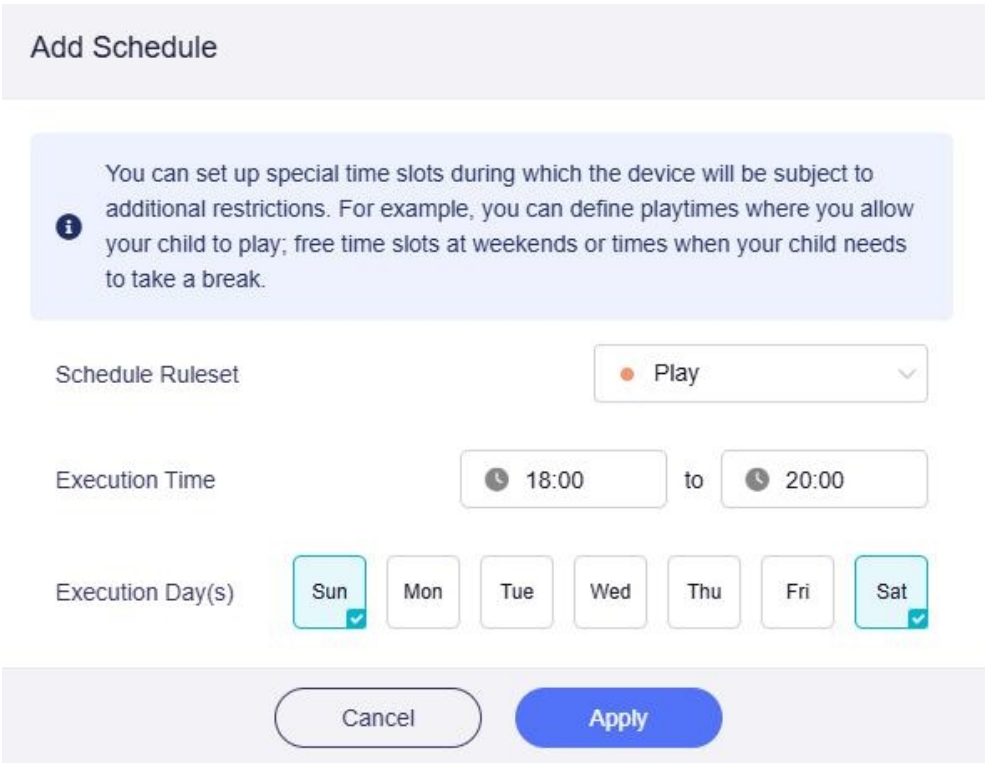
5. Otworzy się strona edycji utworzonego profilu.



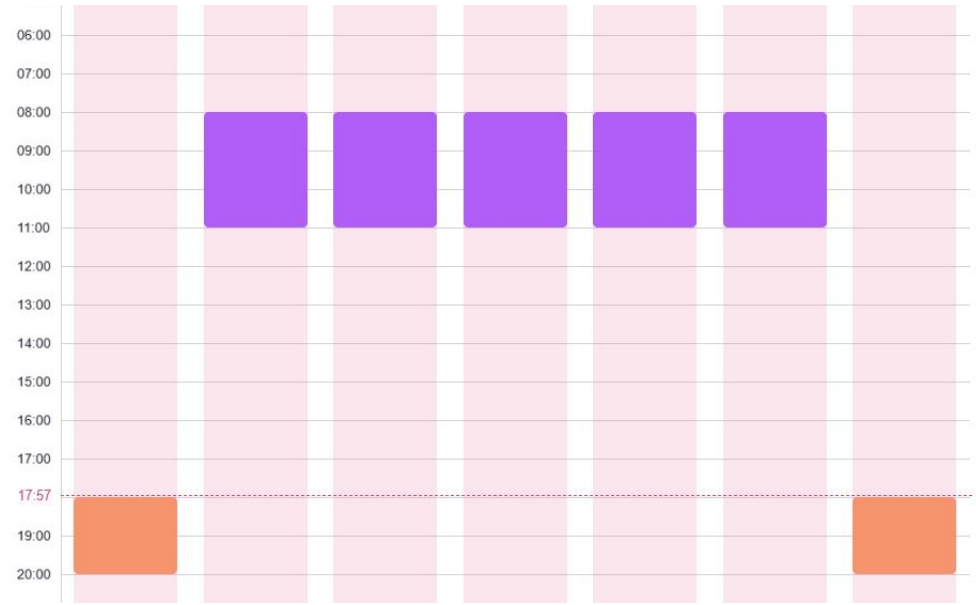
Przewiń w dół, aby zobaczyć utworzony harmonogram. Kliknij ikonę koła zębatego w prawym górnym rogu i wybierz **Add Schedule**.



6. Dodaj do harmonogramu drugi zestaw reguł, **Play**. Ustaw **Execution Time** od 18:00 do 20:00 w weekendy, a następnie kliknij **Apply**.



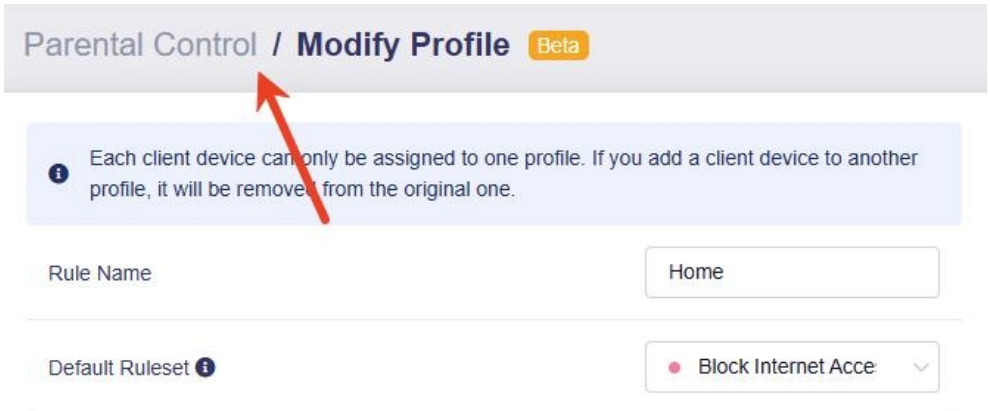
Zestaw reguł Play zostanie dodany do harmonogramu.



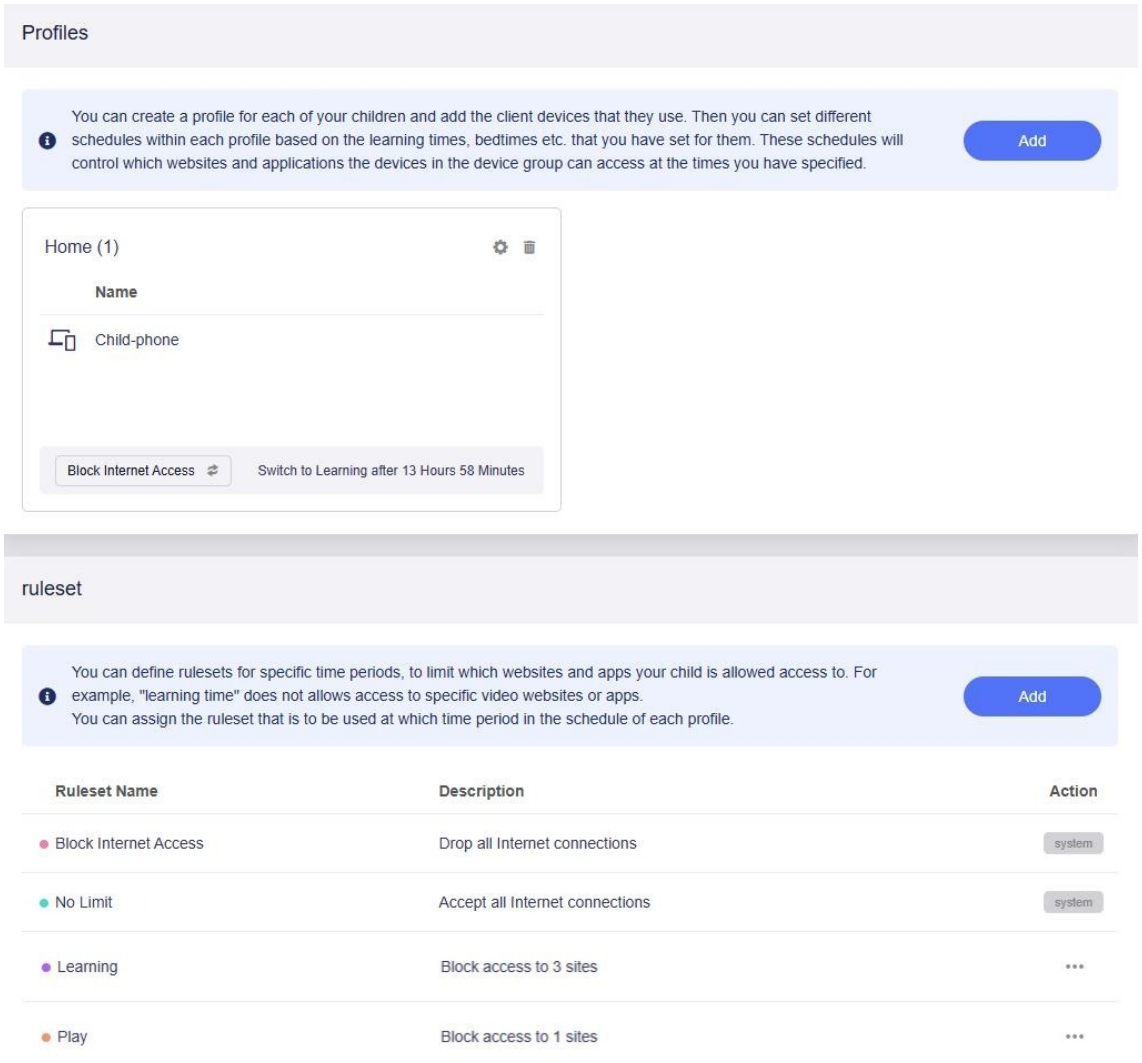
Wskazówki:

- Czerwona linia przerywana wskazuje bieżący czas.
- Aby zmienić czas obowiązywania, kliknij odpowiedni zestaw reguł w harmonogramie.

7. Kliknij **Parental Control** u góry, aby wrócić do strony kontroli rodzicielskiej.



Pojawi się końcowa konfiguracja. Kontrola rodzicielska działa teraz zgodnie z harmonogramem. W razie potrzeby możesz zmieniać istniejące profile i zestawy reguł lub dodawać nowe.



13.5.2 Rozwiązywanie problemów

Jeśli skonfigurowane ustawienia nie działają, sprawdź poniższe możliwe przyczyny.

1. Problem z pamięcią podręczną DNS.

   Przeglądarki i systemy operacyjne przechowują pamięć podręczną DNS, co może opóźniać zastosowanie zmian konfiguracji. Wyczyść ją, aby natychmiast zastosować zmiany.
2. Harmonogram profilu jeszcze się nie rozpoczął.
3. Wprowadzona nazwa domeny może być nieprawidłowa.

   Publiczną domenę witryny łatwo znaleźć, ale domeny API używane przez aplikacje często nie są publicznie udostępniane. Aby znaleźć właściwą domenę, użyj narzędzia do przechwytywania pakietów, np. Wireshark, lub wyszukaj odpowiednie informacje o domenie. Na przykład przy blokowaniu „www.google.com” wpisanie „google.com” daje lepsze wyniki niż „www.google.com”.
4. Urządzenie docelowe używa losowego adresu MAC przy każdym połączeniu z siecią, co uniemożliwia działanie reguł dostępu. Wyłącz losowanie adresu MAC na tym urządzeniu, a następnie ponownie dodaj je do profilu.

13.6 ZeroTier

ZeroTier to programowa wirtualna sieć prywatna (VPN) umożliwiająca bezpieczną, szyfrowaną komunikację między urządzeniami przez Internet. Tworzy prywatną sieć wirtualną, w której urządzenia komunikują się tak, jakby znajdowały się w tej samej sieci lokalnej, niezależnie od lokalizacji fizycznej i topologii sieci. ZeroTier zaprojektowano z myślą o łatwej konfiguracji i obsłudze. Oferuje szyfrowanie od końca do końca, segmentację sieci i tworzenie mostów sieciowych.

Funkcja ZeroTier w routerach GL.iNet pozwala dołączyć router do wirtualnej sieci ZeroTier, umożliwiając zdalny dostęp do routera oraz zasobów po jego stronie WAN i LAN.

Uwaga:

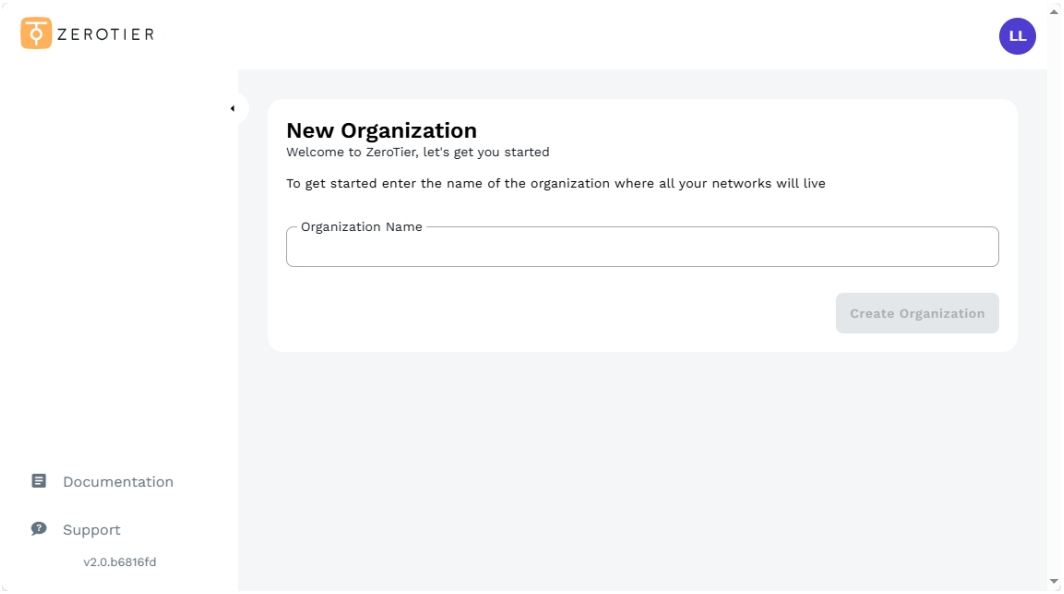
1. Nie zaleca się używania ZeroTier jednocześnie z następującymi funkcjami lub usługami ze względu na możliwość konfliktów routingu: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale i AstroWarp.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

13.6.1 Konfiguracja ZeroTier

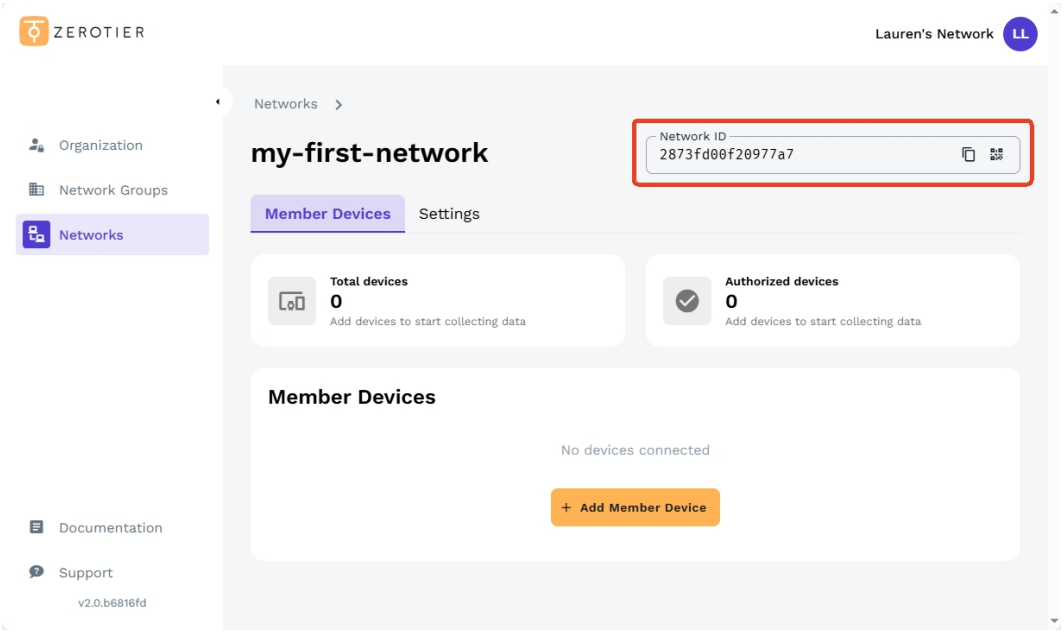
Dostępne są dwie wersje ZeroTier Central: New Central i Legacy Central.

W poniższych krokach jako przykład wykorzystano New Central.

1. Odwiedź oficjalną witrynę ZeroTier i zaloguj się na swoje konto.
2. Utwórz organizację.

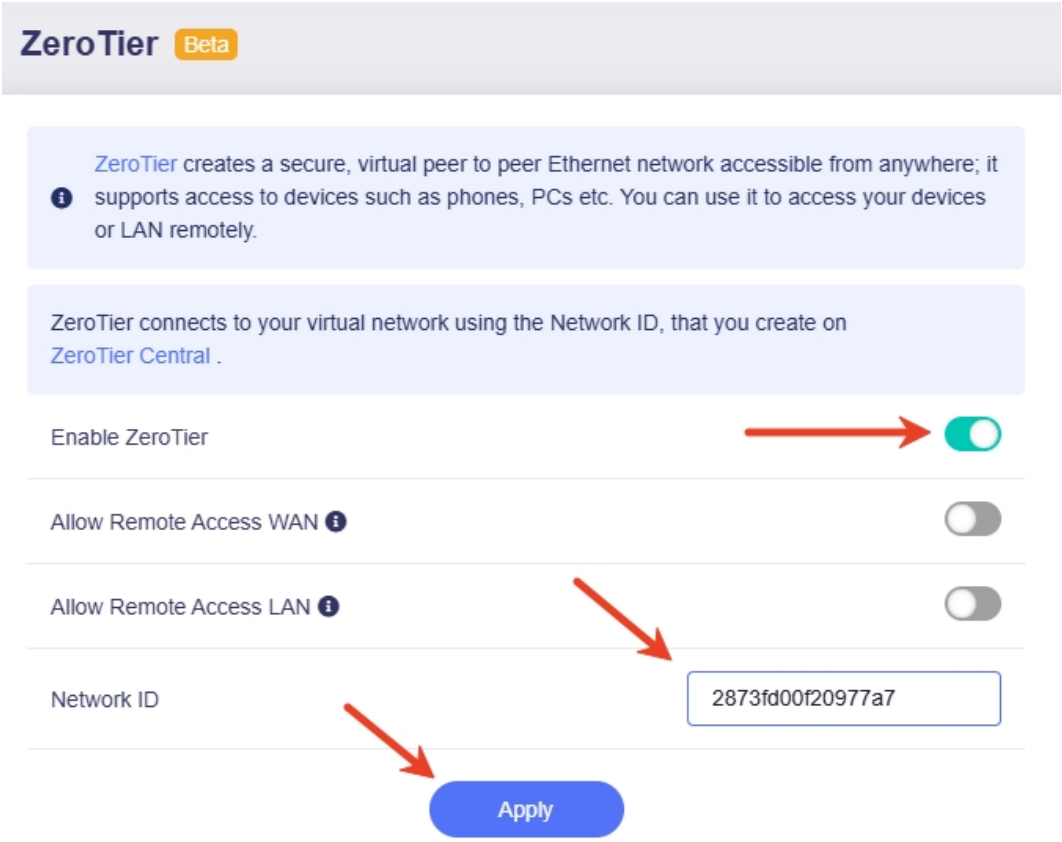


3. Wybierz plan. W tym przykładzie wybieramy **Personal plan**, obejmujący 10 urządzeń, 1 administratora sieci i 1 sieć. Aby tworzyć więcej sieci, dodawać więcej urządzeń lub niestandardowe trasy i DNS, wybierz inny płatny plan.
4. Sieć ZeroTier została utworzona.

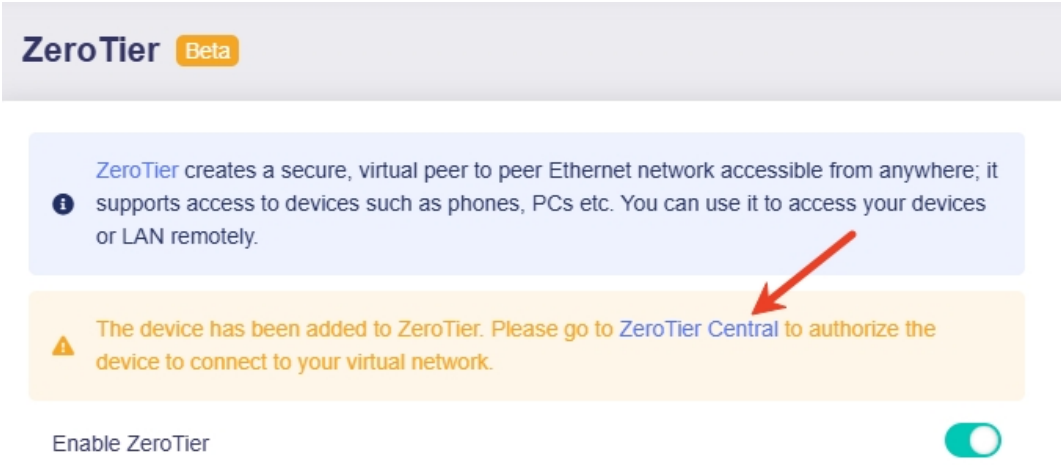


Zapisz **Network ID**, czyli 16-znakową kombinację liter i cyfr w prawym górnym rogu. Będzie potrzebna do późniejszego podłączania innych urządzeń.

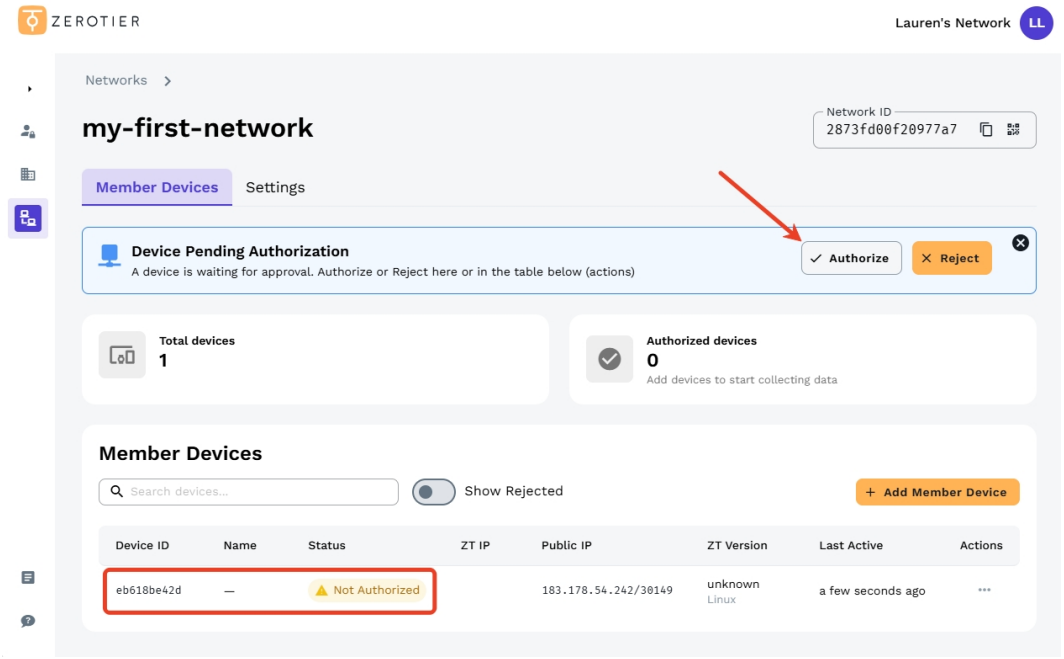
5. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** -> **ZeroTier**. Włącz ZeroTier, wprowadź **Network ID** i kliknij **Apply**.



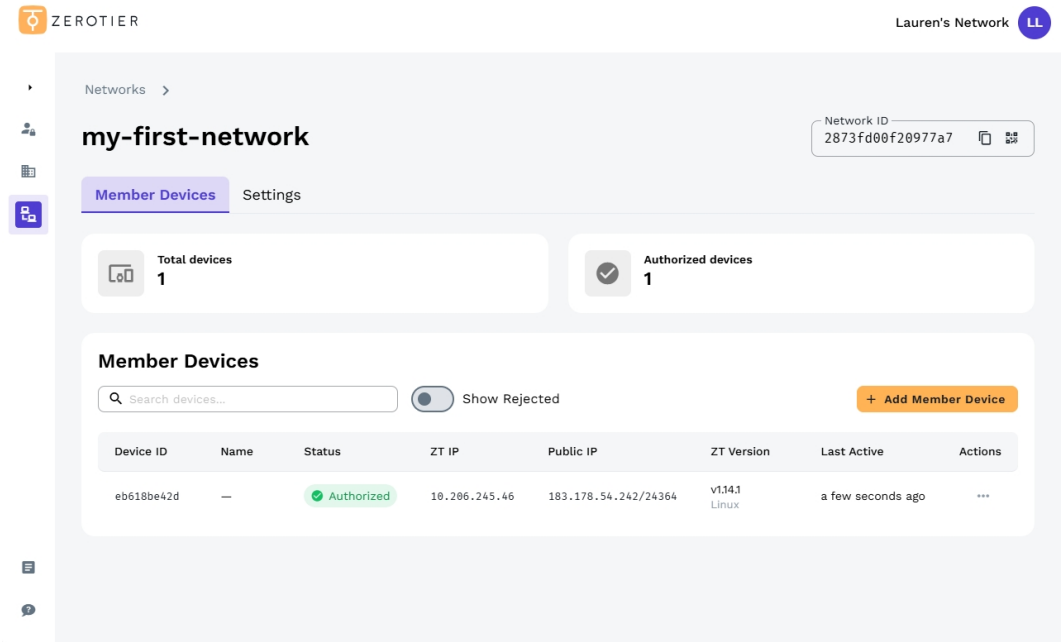
Po chwili na stronie pojawi się informacja o wymaganej autoryzacji. Kliknij hiperłącze **ZeroTier Central**, aby otworzyć ZeroTier Central.



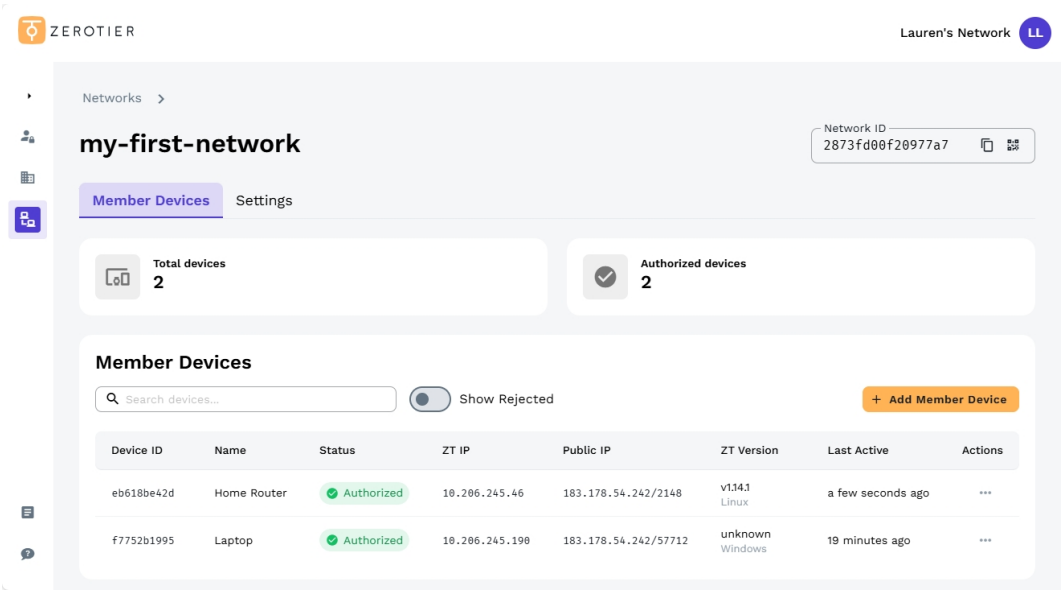
6. W ZeroTier Central znajdź oczekujące urządzenie i autoryzuj je.



Po autoryzacji strona będzie wyglądać jak poniżej.

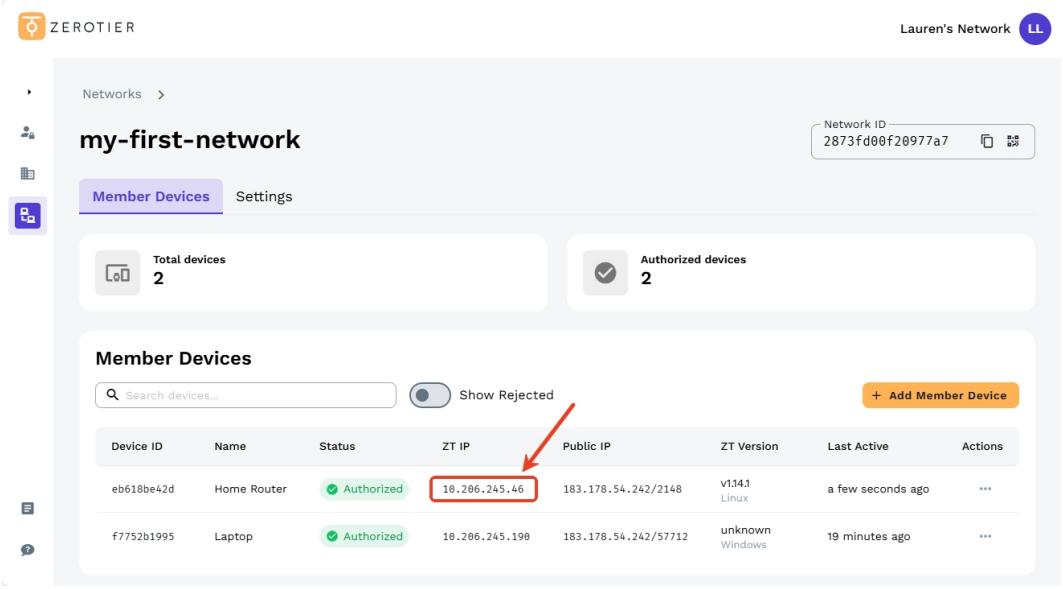


7. Dodaj inne urządzenie (np. komputer lub smartfon) do tej samej sieci ZeroTier zgodnie z tym poradnikiem. Po pomyślnym dodaniu strona będzie wyglądać jak poniżej. Zobaczysz szczegóły urządzeń członkowskich, takie jak **Device ID**, **Name**, **Status**, **Managed IP** i **Public IP**.



Wskazówka: możesz kliknąć ikonę trzech kropek po prawej stronie, aby edytować ustawienia urządzenia członkowskiego, w tym nazwę, zarządzane adresy IP i ustawienia zaawansowane.

8. Kliknij **Managed IP** routera, aby skopiować adres.



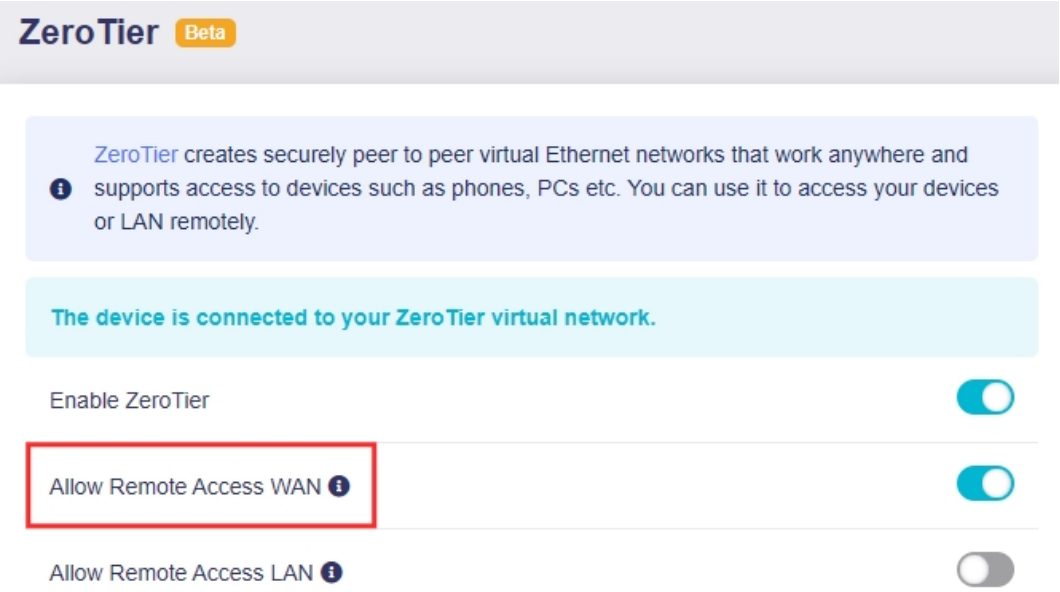
Możesz go następnie użyć do uzyskania dostępu do routera z laptopa w tej samej sieci ZeroTier.

9. Sprawdź łączność.

   Na laptopie podłączonym do tej samej sieci ZeroTier otwórz przeglądarkę i wprowadź adres Managed IP routera uzyskany w poprzednim kroku. Jeśli panel administracyjny routera jest dostępny, połączenie ZeroTier działa prawidłowo.

13.6.2 Zdalny dostęp do WAN

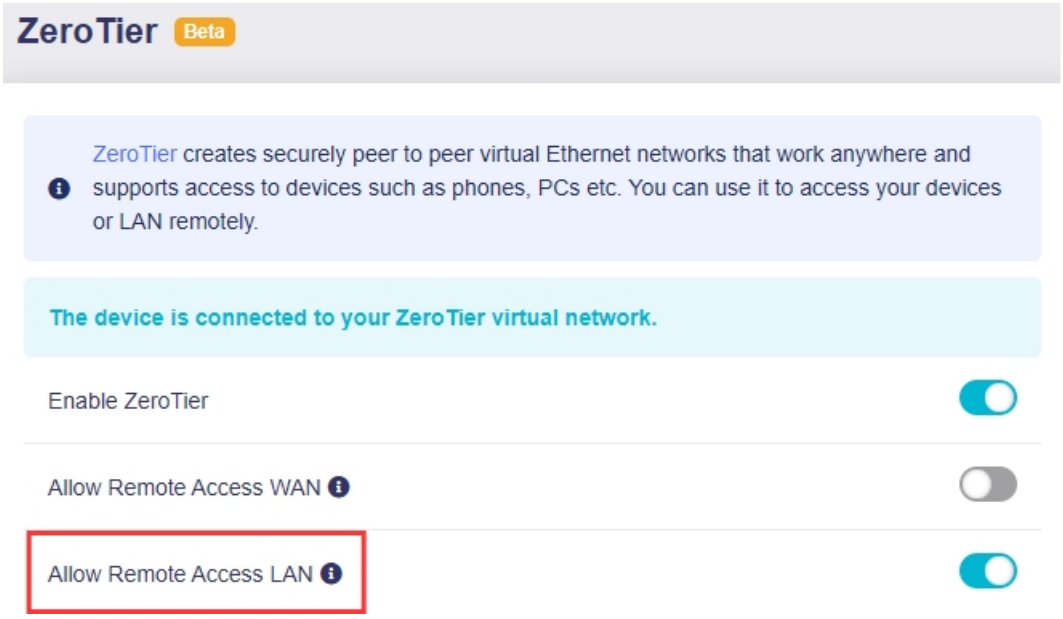
Po włączeniu tej opcji zasoby po stronie WAN urządzenia są dostępne przez wirtualną sieć ZeroTier. Więcej informacji znajdziesz tutaj.



Uwaga: aby ta funkcja działała, należy dodać reguły routingu do sieci ZeroTier. W Legacy Central można bezpłatnie dodać jedną trasę niestandardową, natomiast w New Central konfiguracja tras niestandardowych wymaga planu Essential lub wyższego. Cennik ZeroTier

13.6.3 Zdalny dostęp do LAN

Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć ZeroTier. Więcej informacji znajdziesz tutaj.



Uwaga: aby ta funkcja działała, należy dodać reguły routingu do sieci ZeroTier. W Legacy Central można bezpłatnie dodać jedną trasę niestandardową, natomiast w New Central konfiguracja tras niestandardowych wymaga planu Essential lub wyższego. Cennik ZeroTier

13.7 Tailscale

Tailscale to usługa VPN zapewniająca bezpieczny i łatwy dostęp do osobistych urządzeń i aplikacji z dowolnego miejsca na świecie.

Funkcja Tailscale w routerach GL.iNet pozwala dołączyć router do wirtualnej sieci Tailscale, umożliwiając zdalny dostęp do routera oraz zasobów po jego stronie WAN i LAN.

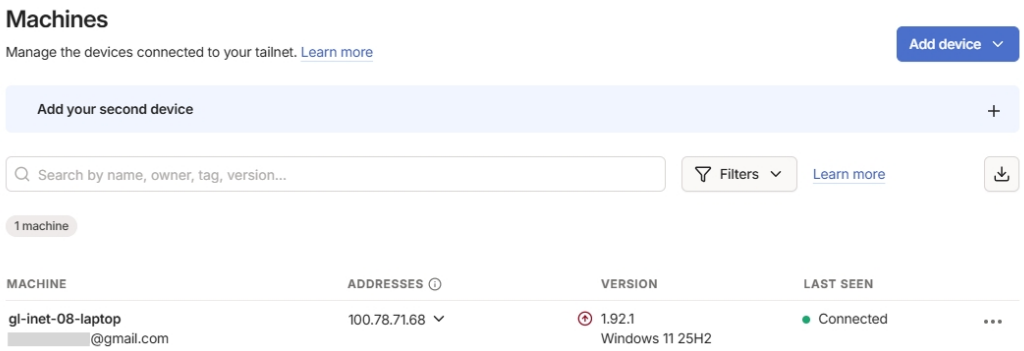
Uwaga:

1. Ponieważ Tailscale bazuje na WireGuard, nie zaleca się używania go jednocześnie z następującymi funkcjami lub usługami ze względu na możliwość konfliktów routingu: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier i AstroWarp.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.
3. Routery GL.iNet nie mogą jeszcze pełnić funkcji węzłów wyjściowych. Ta funkcja będzie dostępna w wersji oprogramowania 4.9 i nowszych.

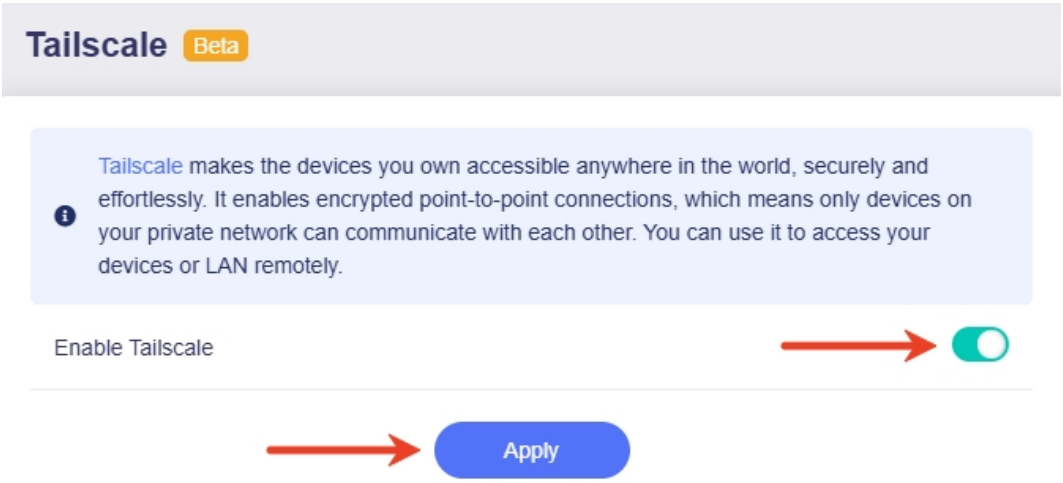
13.7.1 Konfiguracja Tailscale

W poniższym przykładzie użyto Beryl AX (GL-MT3000) i laptopa.

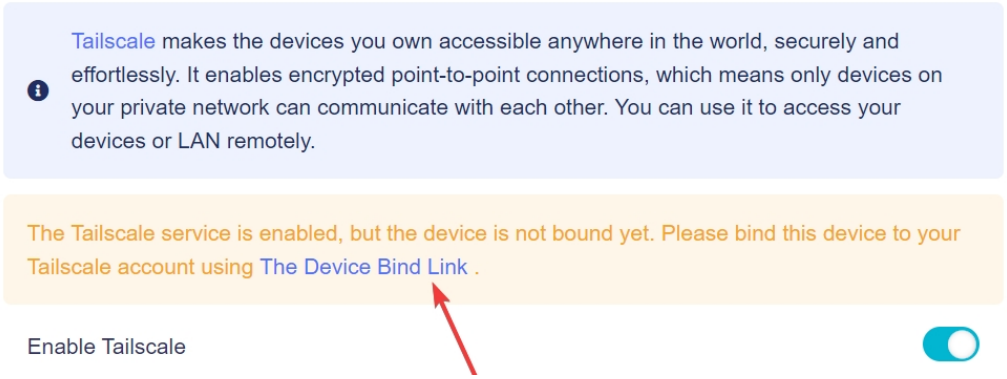
1. Najpierw zarejestruj konto Tailscale i powiąż z nim jedno lub dwa urządzenia do testów. Po powiązaniu zobaczysz je w konsoli Tailscale.



2. Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Tailscale**. Włącz **Enable Tailscale** i kliknij **Apply**.



3. Strona poprosi o powiązanie urządzenia. Kliknij **Device Bind Link**.



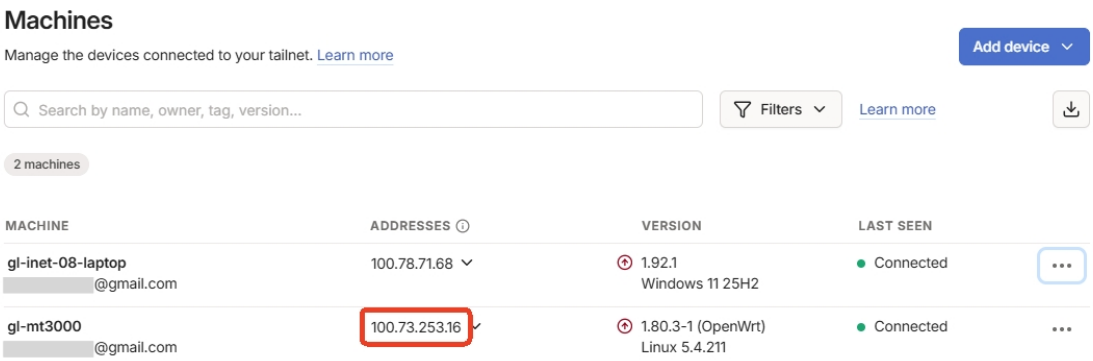
4. W wyświetlonym oknie kliknij łącze i zaloguj się na konto Tailscale.



5. Po zalogowaniu pojawi się prośba o potwierdzenie urządzenia. Kliknij **Connect**.

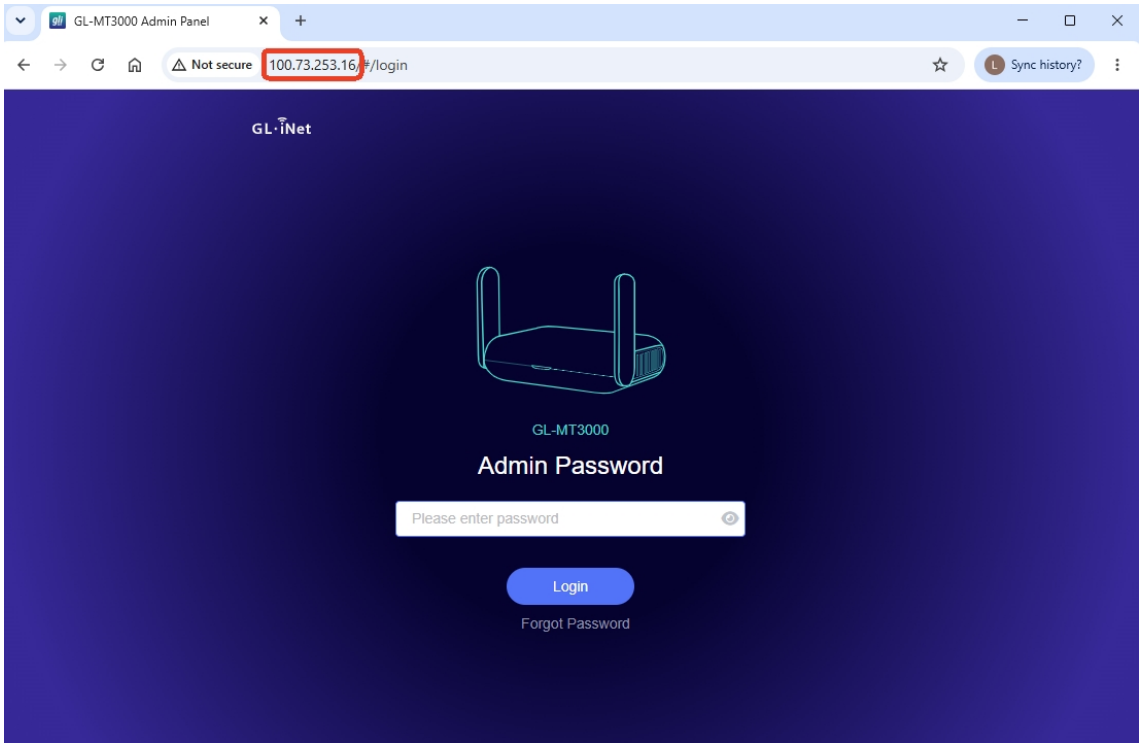


6. Nastąpi przekierowanie do konsoli administracyjnej Tailscale. Router został dodany do wirtualnej sieci Tailscale i jest dostępny zdalnie pod wirtualnym adresem IP Tailscale **100.73.253.16**.



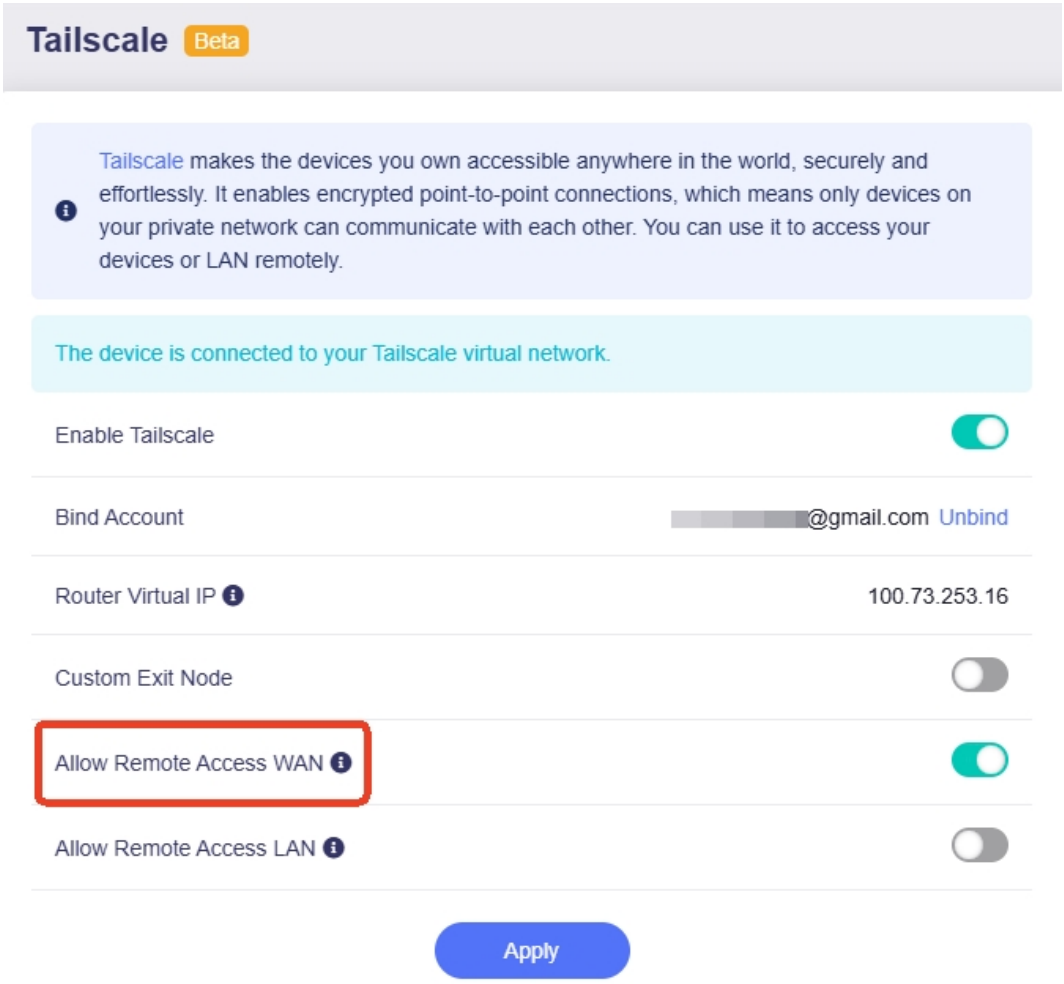
7. Sprawdź łączność.

   Na innym urządzeniu w tej samej sieci Tailscale otwórz przeglądarkę i wprowadź wirtualny adres IP routera w pasku adresu. Jeśli panel administracyjny jest dostępny, Tailscale działa prawidłowo. Aby sprawdzić łączność, możesz też użyć polecenia ping lub zalogować się przez SSH do terminala routera, korzystając z jego wirtualnego adresu IP.


GL-MT3000 Admin Panel
Not secure
100.73.253.16/#/login
Sync history?
GL·iNet
GL-MT3000
Admin Password
Please enter password
Login
Forgot Password

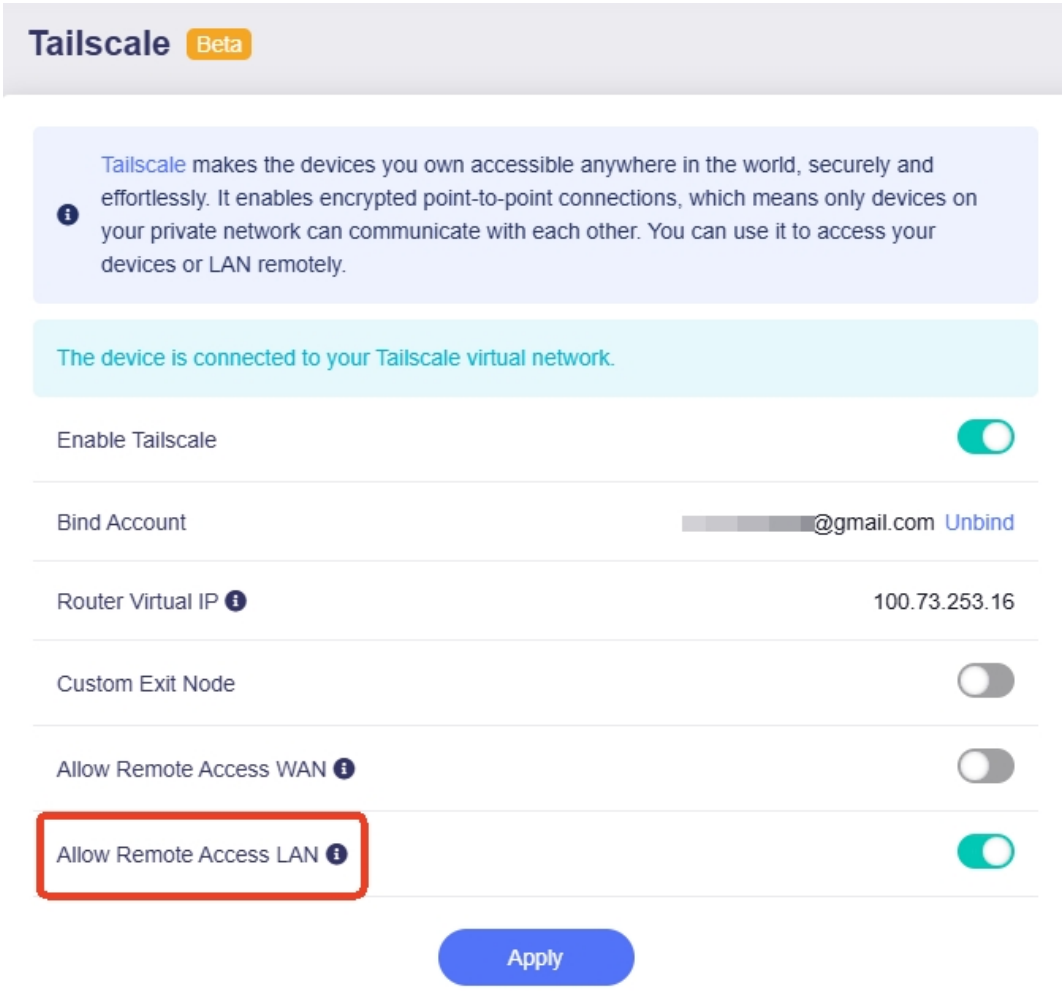
13.7.2 Zdalny dostęp do WAN

Po włączeniu tej opcji zasoby po stronie WAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



13.7.3 Zdalny dostęp do LAN

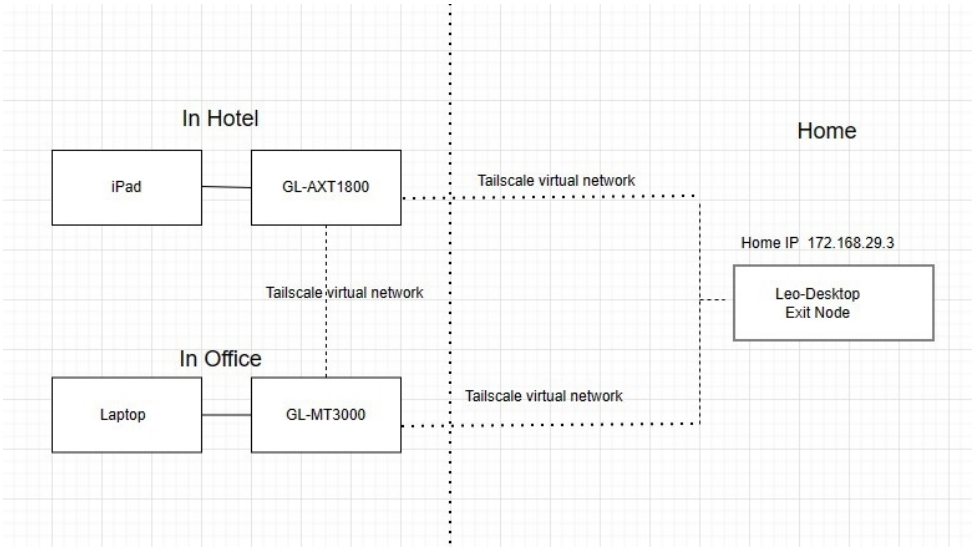
Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



13.7.4 Niestandardowe węzły wyjściowe

Domyślnie Tailscale działa jako sieć nakładkowa: kieruje wyłącznie ruch między urządzeniami z Tailscale i nie obsługuje ruchu do publicznego Internetu, np. podczas przeglądania witryn takich jak Google.

Czasami jednak potrzebne jest kierowanie przez Tailscale ruchu do publicznego Internetu. Na przykład podczas pobytu poza domem lub podróży zagranicznej możesz potrzebować usług internetowych, np. bankowości, dostępnych tylko w kraju zamieszkania. W takim przypadku skonfiguruj domowy komputer z publicznym adresem IP jako węzeł wyjściowy i ustaw inne urządzenia w tej samej sieci Tailnet, np. GL-AXT1800 i GL-MT3000 na poniższej ilustracji, aby przesyłały ruch przez ten węzeł. Umożliwia to przekazywanie całego ruchu do publicznego Internetu przez węzeł wyjściowy.



Węzeł wyjściowy kieruje wychodzący ruch internetowy urządzeń Tailnet, pełniąc w praktyce funkcję serwera VPN. Po połączeniu z takim węzłem cały ruch internetowy niezwiązany z Tailscale jest widziany jako pochodzący z jego lokalizacji. Pomaga to uzyskiwać dostęp do treści z ograniczeniami geograficznymi i zwiększać prywatność w sieci. Urządzenie przekazujące ten ruch nosi nazwę „Exit Node”. Konfigurację niestandardowego węzła wyjściowego na routerach GL.iNet opisano w tym poradniku.

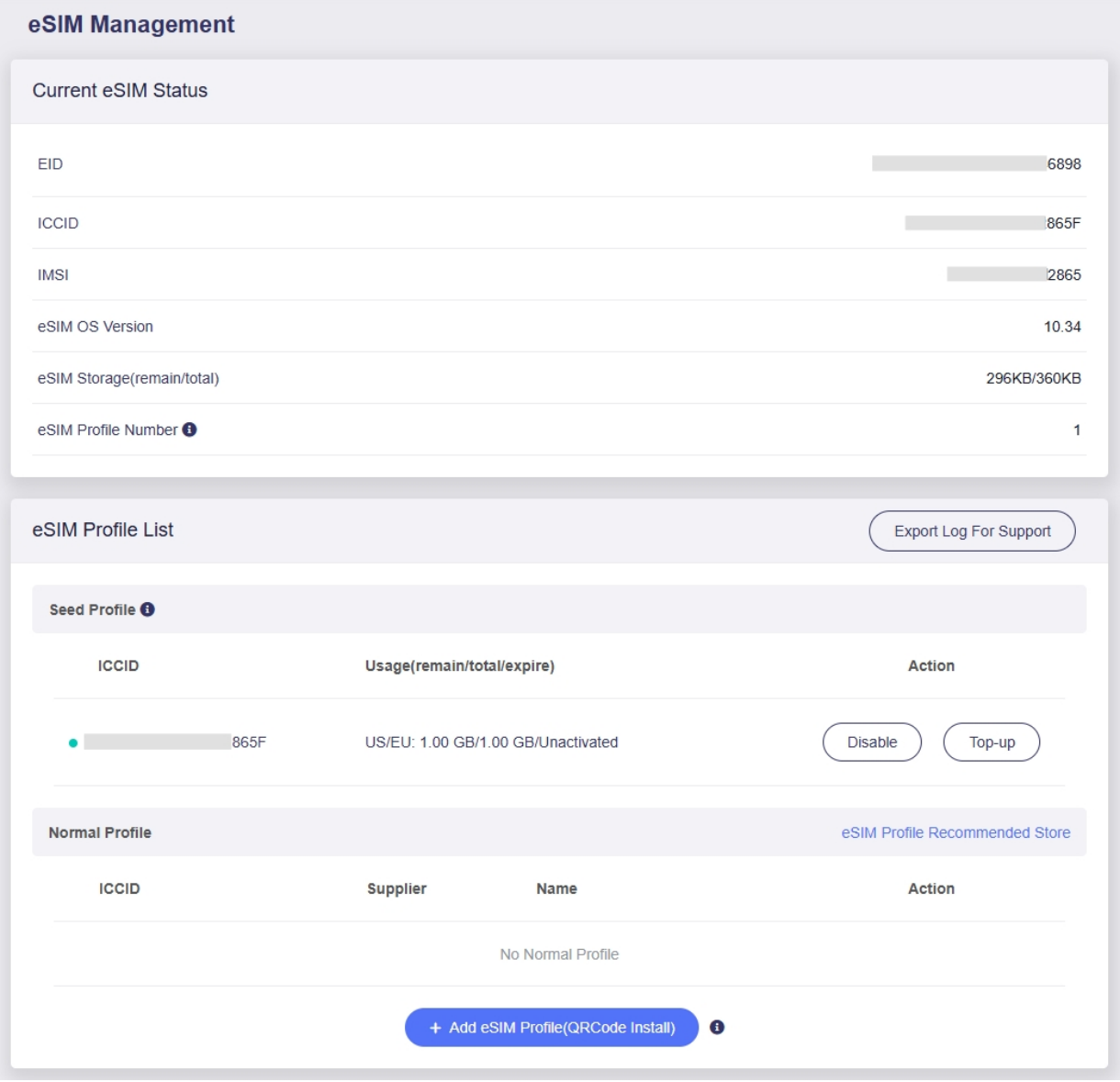
Uwaga: jeśli serwer DNS routera ma prywatny adres IP dostępny wyłącznie w sieci lokalnej, po uruchomieniu węzłów wyjściowych możesz utracić dostęp do Internetu. Aby temu zapobiec, ręcznie ustaw na routerze publiczny serwer DNS (np. 8.8.8.8).

13.8 Zarządzanie eSIM

Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **APPLICATIONS** > **eSIM Management**.

Ta strona umożliwia sprawdzanie stanu fizycznej karty eSIM i zarządzanie profilami eSIM.

Składa się z dwóch części: **Current eSIM Status** i **eSIM Profile List**.



13.8.1 Bieżący stan eSIM

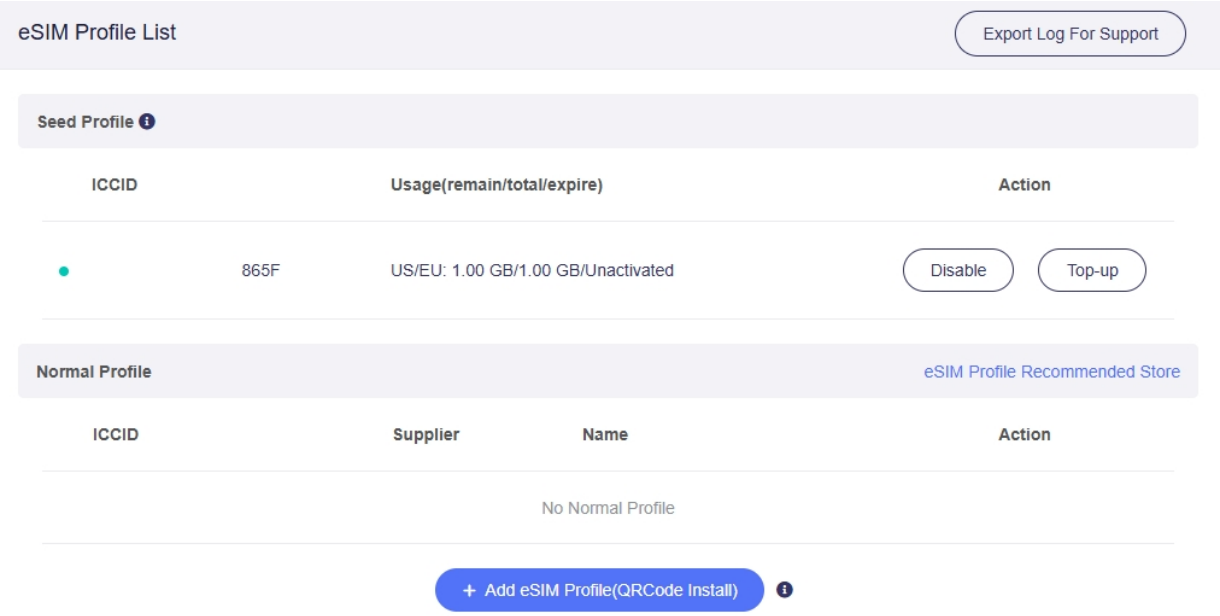
Ta sekcja wyświetla podstawowe informacje i szczegóły dotyczące aktualnie aktywnego profilu eSIM.



- **EID:** globalnie unikatowy identyfikator eUICC (układu eSIM), używany do identyfikacji i zarządzania profilami.
- **ICCID:** identyfikator karty z układem scalonym dla aktualnie aktywnego profilu eSIM.
- **IMSI:** międzynarodowy identyfikator abonenta sieci komórkowej dla aktualnie aktywnego profilu eSIM.
- **eSIM OS Version:** wersja systemu operacyjnego eUICC, określająca zgodność i obsługiwane możliwości.
- **eSIM Storage (remain/total):** dostępna i całkowita pojemność pamięci eUICC przeznaczonej na profile eSIM.
- **eSIM Profile Number:** liczba profili eSIM obecnie przechowywanych w eUICC. Profile oferowane przez różnych operatorów mają różne rozmiary, dlatego liczba profili mieszczących się w eUICC może się różnić.

13.8.2 Lista profili eSIM

Ta sekcja wyświetla informacje o startowym profilu eSIM i profilach standardowych.



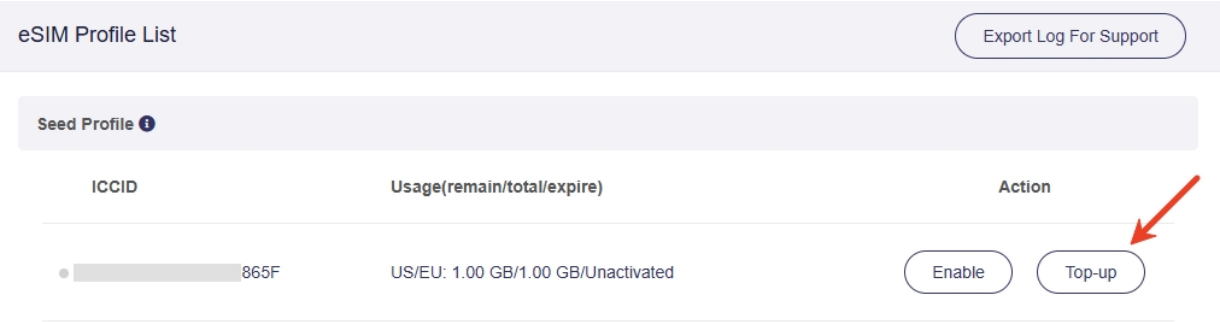
- **Seed Profile**: Profil startowy jest wstępnie załadowany i zawiera 1 GB bezpłatnych danych na terenie USA i Europy oraz 100 MB danych globalnych, ważnych przez rok od aktywacji. Dane te umożliwiają pobieranie innych profili w dowolnym miejscu na świecie. Możesz też monitorować wykorzystanie profilu startowego, w tym pozostałe dane, całkowity limit i datę wygaśnięcia.
- **Normal Profile**: Jeśli kupisz profil eSIM i prześlesz go za pomocą kodu QR lub kodu aktywacyjnego, zostanie on wyświetlony w tym miejscu.

13.8.2.1 Doładowanie profilu startowego

GL.iNet udostępnia wstępnie załadowany profil startowy ze 100 MB danych globalnych i 1 GB danych ważnych w Europie i USA, przeznaczony do konfiguracji początkowej i aktywacji profili eSIM. Pakiet ten służy do pobierania nowych profili eSIM po przyjeździe do miejsca, w którym nie masz dostępu do Internetu.

Jeśli wykorzystasz bezpłatne dane lub upłynie ich ważność i chcesz nadal korzystać z usługi, możesz doładować profil startowy.

W sekcji Seed Profile kliknij przycisk **Top-up** po prawej stronie.



W wyskakującym oknie zeskanuj kod QR i postępuj zgodnie z instrukcjami, aby doładować profil.



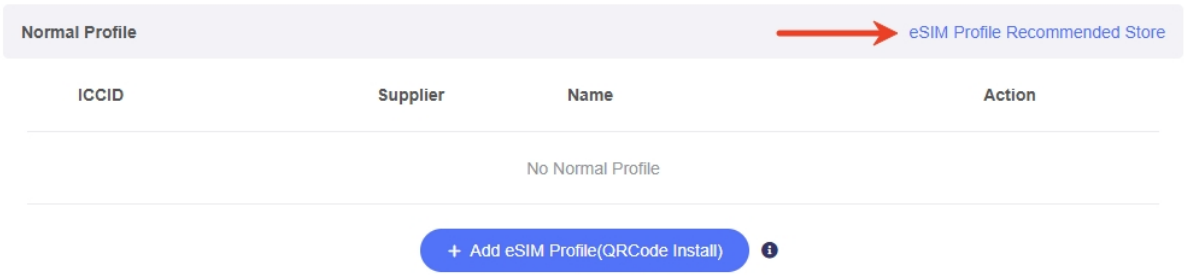
13.8.2.2 Zakup profilu eSIM

Profile eSIM można kupić w polecanych przez nas sklepach, przetestowanych sklepach lub u innych zewnętrznych dostawców eSIM.

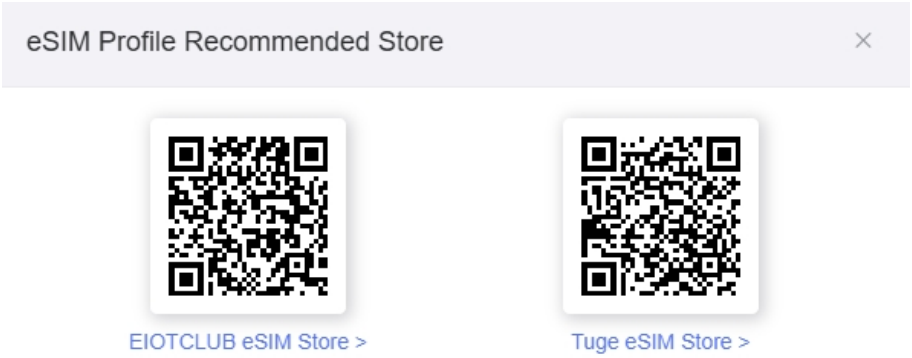
Opcja 1: Zakup w polecanych przez nas sklepach.

Polecamy dwa sklepy: EIOTCLUB eSIM Store i Tuge eSIM Store.

W sekcji Normal Profile kliknij **eSIM Profile Recommended Store** po prawej stronie.



Zeskanuj kod QR lub kliknij łącza, aby kupić profile eSIM.



Uwaga: Wszystkie pakiety profili eSIM kupione w tych dwóch sklepach są w pełni zgodne z routerami GL.iNet. W razie pytań skontaktuj się z naszym zespołem pomocy pod adresem support@gl-inet.com.

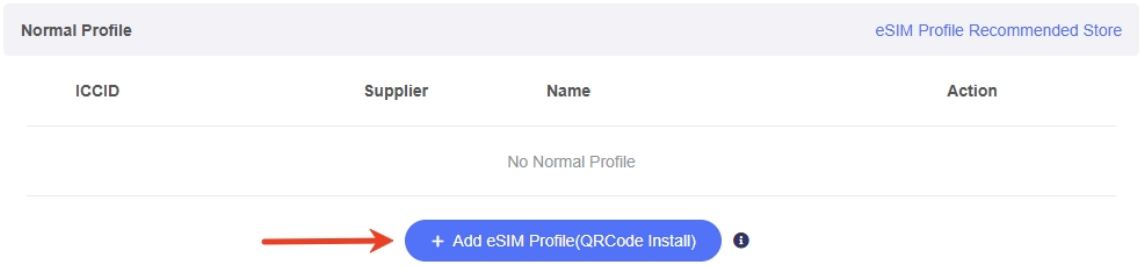
Opcja 2: Zakup w przetestowanych sklepach.
Kliknij to łącze, aby wyświetlić listę sklepów przetestowanych przez GL.iNet.
Uwaga: Nie możemy zagwarantować pełnej zgodności z routerami GL.iNet wszystkich profili i pakietów z tych sklepów. Ponieważ GL.iNet nie współpracuje z nimi, nie możemy zapewnić obsługi posprzedażowej ani pomóc w uzyskaniu zwrotu środków.

Opcja 3: Zakup u innych zewnętrznych dostawców eSIM.
Możesz też kupić profile eSIM u innych wybranych dostawców zewnętrznych.
Nie możemy jednak zagwarantować pełnej zgodności z routerami GL.iNet profili eSIM zakupionych u innych dostawców zewnętrznych. Decyzję o zakupie podejmujesz według własnego uznania. GL.iNet nie odpowiada za problemy ze zgodnością.
W sprawie obsługi posprzedażowej lub zwrotu środków skontaktuj się z odpowiednim dostawcą eSIM.

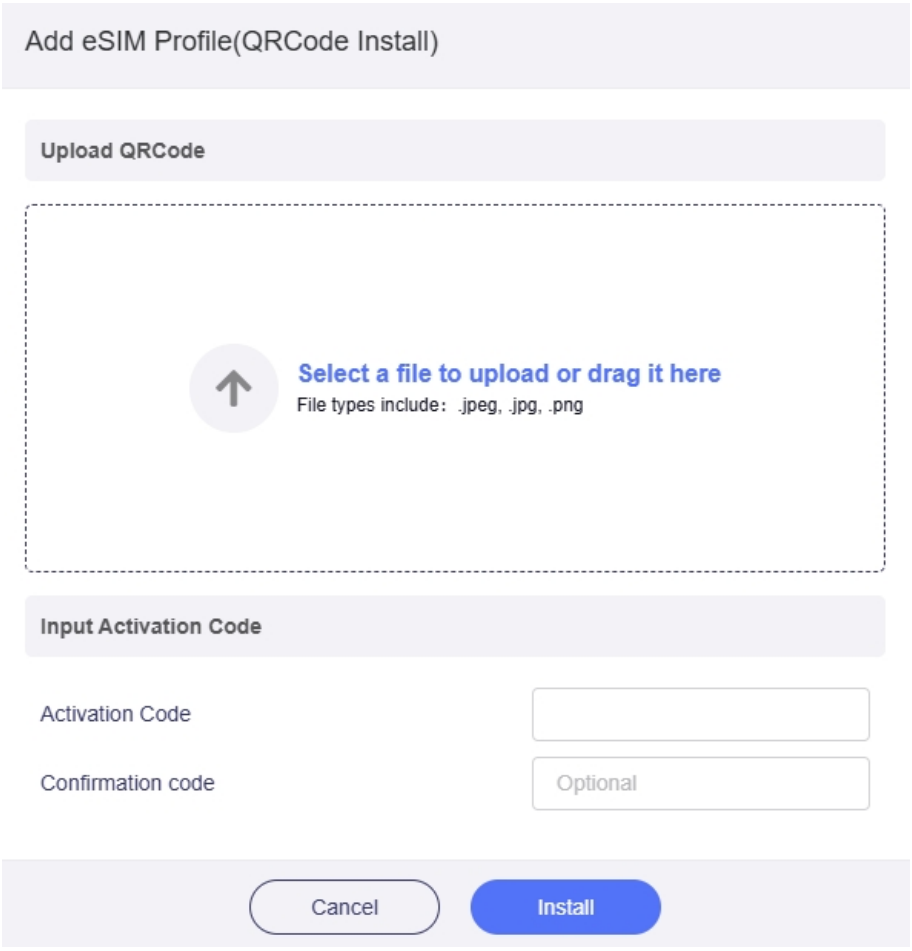
13.8.2.3 Przesyłanie profilu eSIM

Po zakupie profilu eSIM zwykle otrzymasz kod QR (lub kod aktywacyjny). Zapisz kod QR lokalnie, a następnie wykonaj poniższe czynności, aby przesłać profil eSIM.

1. W sekcji Normal Profile kliknij **Add eSIM Profile** na dole.



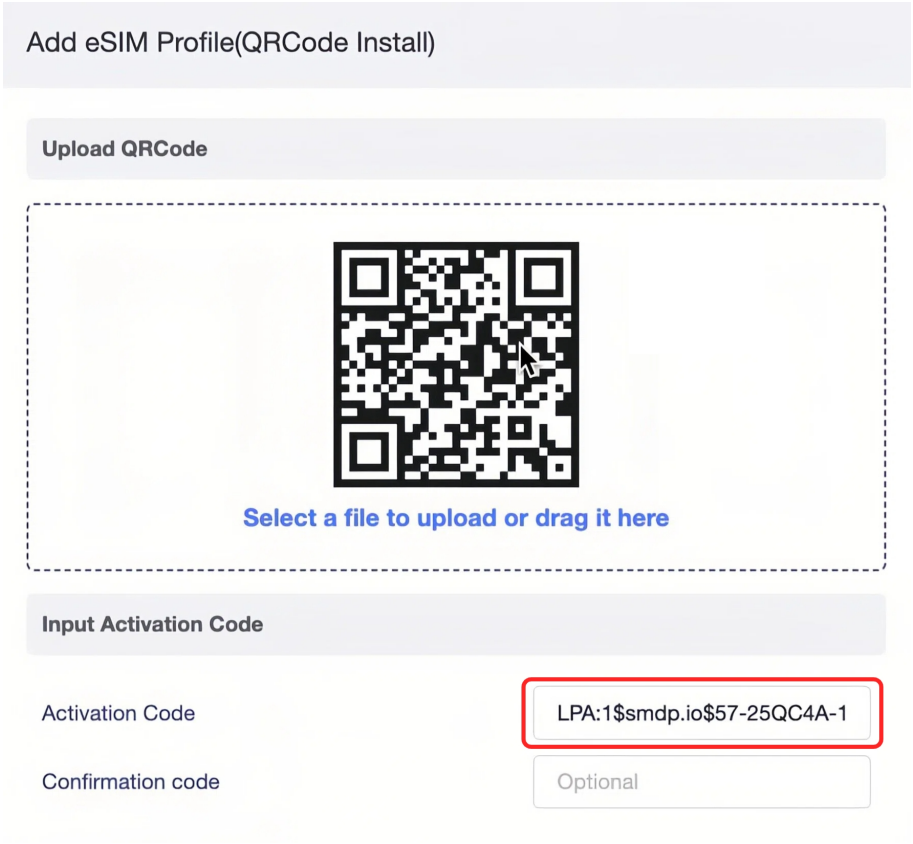
2. Prześlij kod QR eSIM lub wpisz kod aktywacyjny, a następnie kliknij **Install**. Profil eSIM zostanie pobrany i zainstalowany w routerze.



Uwaga:

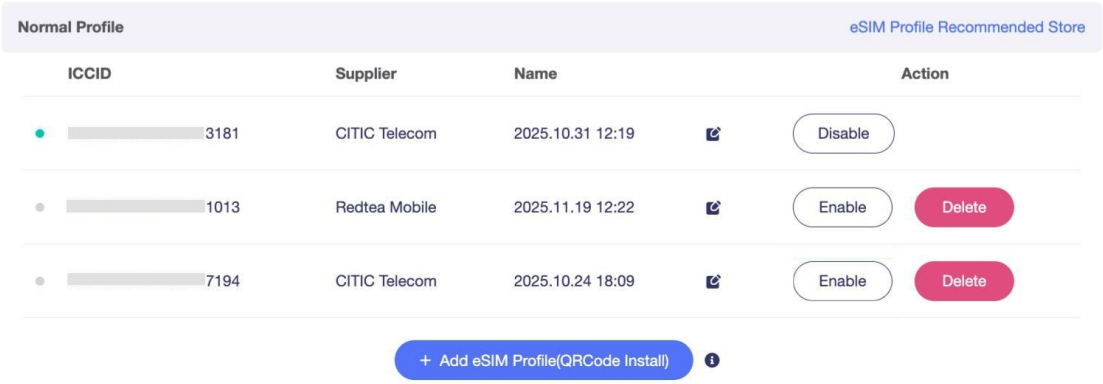
1. Większość profili eSIM można pobrać i zainstalować tylko raz.

2. Prawidłowo sformatowany kod QR wyświetla kod aktywacyjny zaczynający się od **LPA:**. Niektóre niestandardowe kody QR mogą jednak zawierać sam kod aktywacyjny bez prefiksu LPA. W takim przypadku ręcznie dodaj LPA: na początku kodu przed kliknięciem przycisku Install.



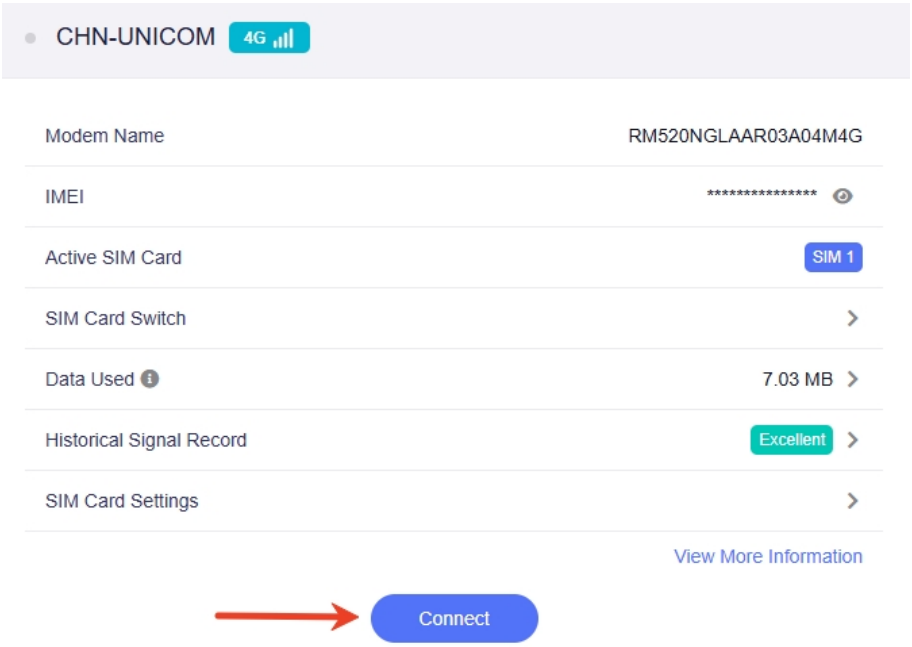
3. Jeśli nie masz jeszcze profilu eSIM, możesz kupić go w eSIM Profile Recommended Store. Szczegóły znajdziesz w sekcji 13.8.2.2 Zakup profilu eSIM.

3. Po pomyślnym przesłaniu nowy profil eSIM pojawi się na liście **Normal Profile**. Kliknij **Enable**, aby go aktywować.



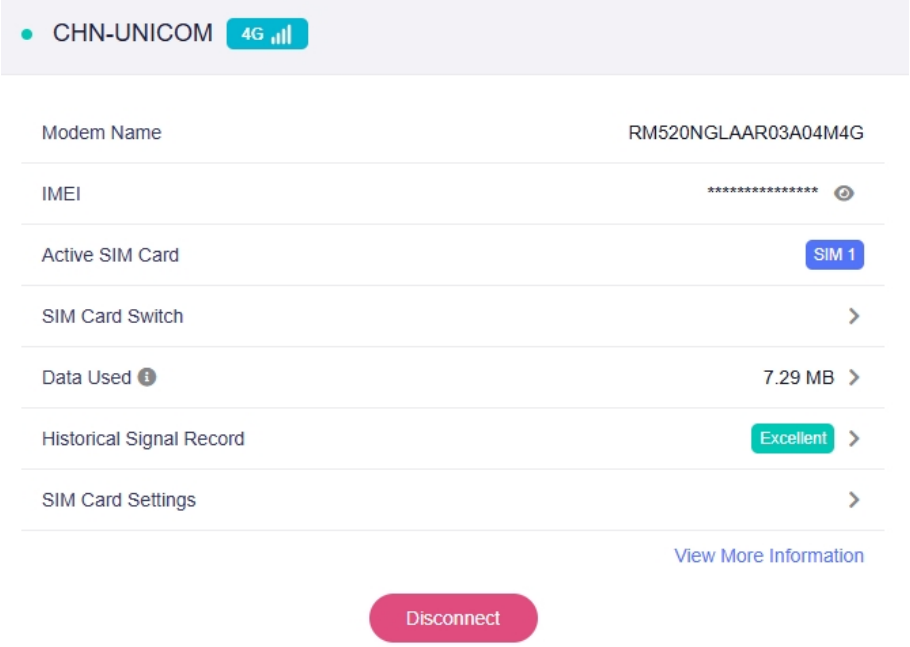
4. Połącz się z Internetem.

   Po włączeniu profilu eSIM przejdź do **INTERNET** > **Cellular**. Kliknij **Connect**, aby nawiązać połączenie z Internetem przez profil eSIM.



   Uwaga: niektóre profile eSIM mogą wymagać dodatkowej konfiguracji, np. ustawień APN, PIN lub TTL. W razie potrzeby kliknij **Manual Setup** lub **SIM Card Settings**, aby dostosować te parametry. W niektórych przypadkach do nawiązania połączenia z Internetem może być konieczne ponowne uruchomienie urządzenia.

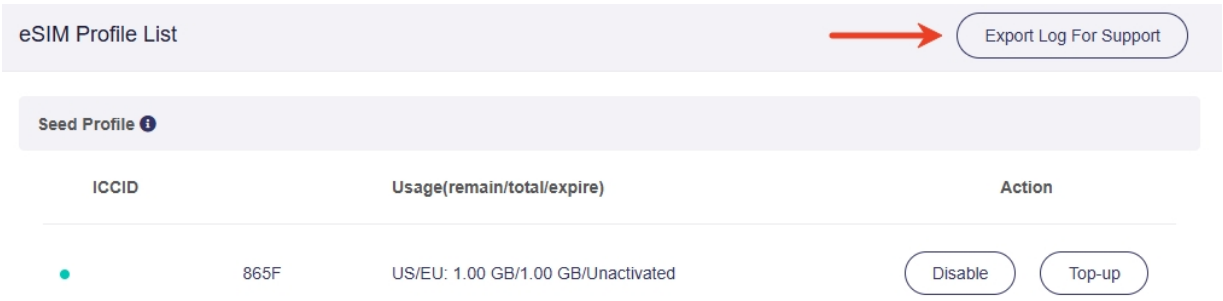
5. Po pomyślnym połączeniu routera przez profil eSIM strona będzie wyglądać następująco:



13.8.2.4 Eksport dziennika dla pomocy technicznej

Kliknij **Export Log for Support**, aby wyświetlić wszystkie dzienniki związane z eSIM.

W razie problemów wymagających pomocy technicznej wyeksportuj dzienniki eSIM i prześlij je zespołowi pomocy pod adresem support@gl-inet.com.



Rozdział 14

Sieć

W tym rozdziale przedstawiono ustawienia konfiguracji i zarządzania siecią, takie jak LAN, DNS i IPv6.

14.1 Przekierowanie portów

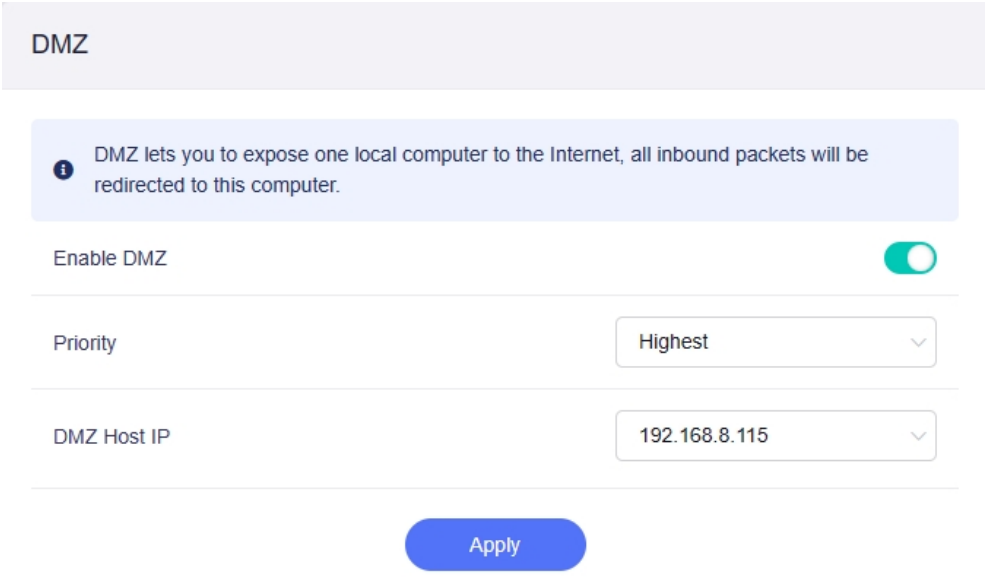
Przekierowanie portów to funkcja sieciowa kierująca żądania zewnętrzne do określonych urządzeń w sieci lokalnej. Strona Port Forwarding zawiera dwie główne funkcje: **DMZ** (bezpośredni pełny dostęp do jednego urządzenia) i **Port Forwarding** (dostęp do określonych portów urządzeń).

14.1.1 DMZ

DMZ umożliwia wystawienie jednego komputera do Internetu. Wszystkie pakiety przychodzące będą przekierowywane do tego komputera.

Aby w razie potrzeby włączyć DMZ, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do sekcji **NETWORK** > **Port Forwarding** > **DMZ**.
2. Włącz **Enable DMZ**. Wybierz Priority i DMZ Host IP z list, a następnie kliknij **Apply**.



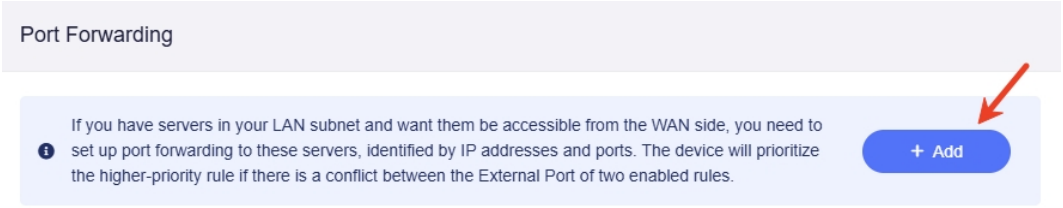
- **Priority**: ustaw Highest lub Lowest. Jeśli DMZ ma wyższy priorytet niż reguły przekierowania portów, wszystkie te reguły przestają obowiązywać. W przeciwnym razie żądania są przekazywane do urządzenia klienckiego DMZ tylko wtedy, gdy dla danego portu nie ma reguły przekierowania.
- **DMZ Host IP**: wybierz wewnętrzny adres IP urządzenia, które ma otrzymywać wszystkie pakiety przychodzące.

14.1.2 Przekierowanie portów

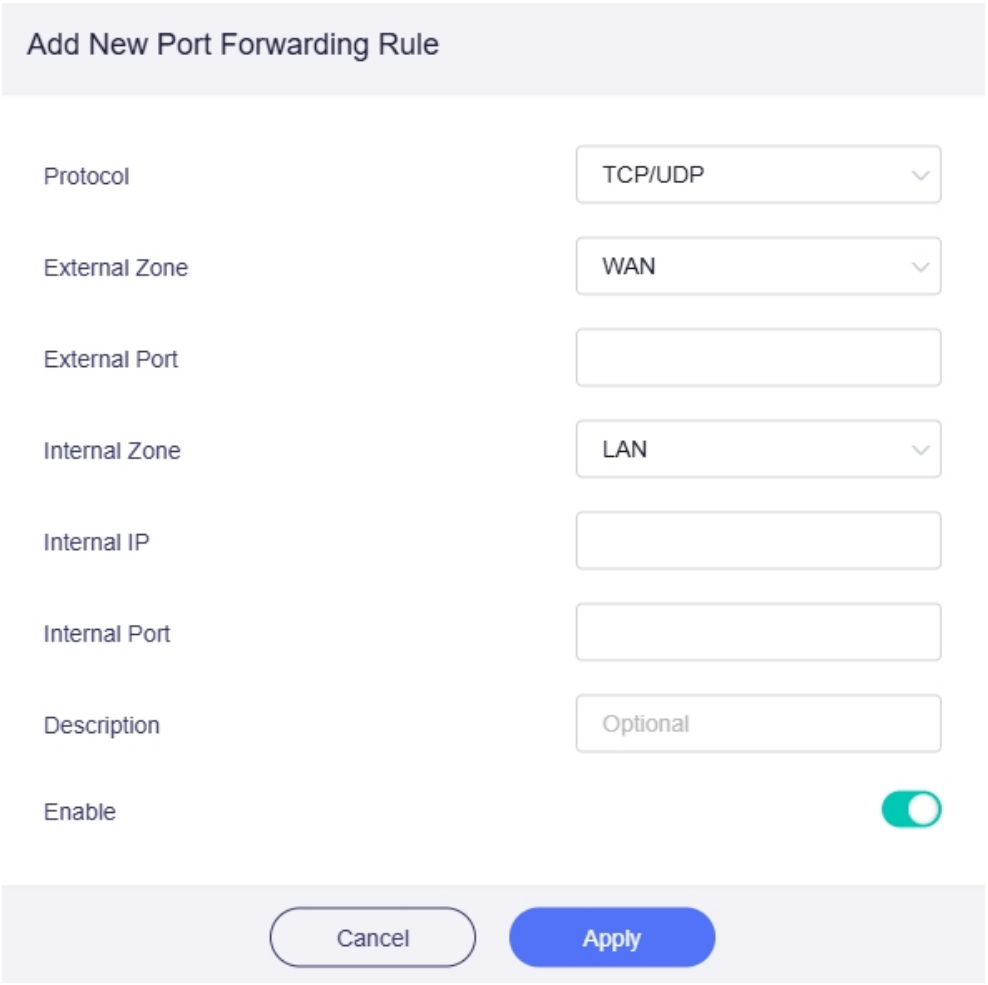
Przekierowanie portów umożliwia komputerom zdalnym łączenie się z komputerem lokalnym lub serwerem za zaporą LAN (np. serwerem WWW lub FTP).

Aby skonfigurować przekierowanie portów, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera, przejdź do sekcji **NETWORK** > **Port Forwarding** > **Port Forwarding** i kliknij **Add**.



2. W wyskakującym oknie wprowadź wymagane parametry lub wybierz je z list, aby dodać regułę przekierowania portów, a następnie kliknij **Apply**.



- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **External Zone**: dostępne opcje to WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN i Guest.
- **External Port**: numer lub numery portów zewnętrznych. Wprowadź określony numer portu z zakresu 1–65535. Możesz ustawić pojedynczy port lub zakres, łącząc pierwszy i ostatni numer łącznikiem (np. 501-510).
- **Internal Zone**: dostępne opcje to LAN, Guest, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server i WAN.
- **Internal IP**: adres IP przydzielony przez router urządzeniu wymagającemu zdalnego dostępu. Jeśli w External Port ustawiono pojedynczy port, tutaj również ustaw pojedynczy port. Jeśli w External Port ustawiono zakres portów, tutaj ustaw odpowiadający mu zakres.
- **Internal Port**: numer portu wewnętrznego urządzenia. Wprowadź określony numer portu. Pozostaw pole puste, jeśli jest taki sam jak port zewnętrzny.
- **Description**: nadaj nazwę lub dodaj opis reguły przekierowania portów (opcjonalnie).
- **Enable**: włącza lub wyłącza tę regułę.

14.2 Multi-WAN

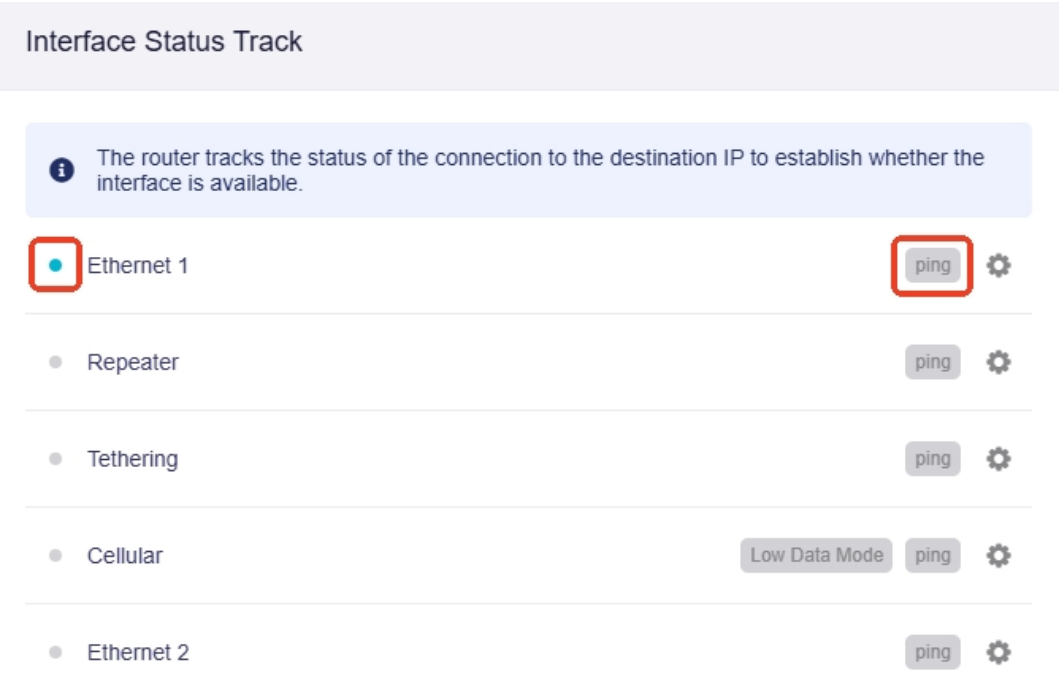
Multi-WAN umożliwia jednoczesne korzystanie z wielu sposobów dostępu do Internetu i konfigurowanie różnych połączeń na routerze. Oferuje dwa tryby pracy:

- **Failover**: po awarii połączenia głównego automatycznie przełącza na połączenie zapasowe w krótkim czasie, zapewniając ciągły dostęp do sieci.
- **Load Balance**: rozdziela ruch między wszystkie dostępne połączenia w ustalonych proporcjach, umożliwiając ich równoczesne wykorzystanie i optymalizując użycie pasma.

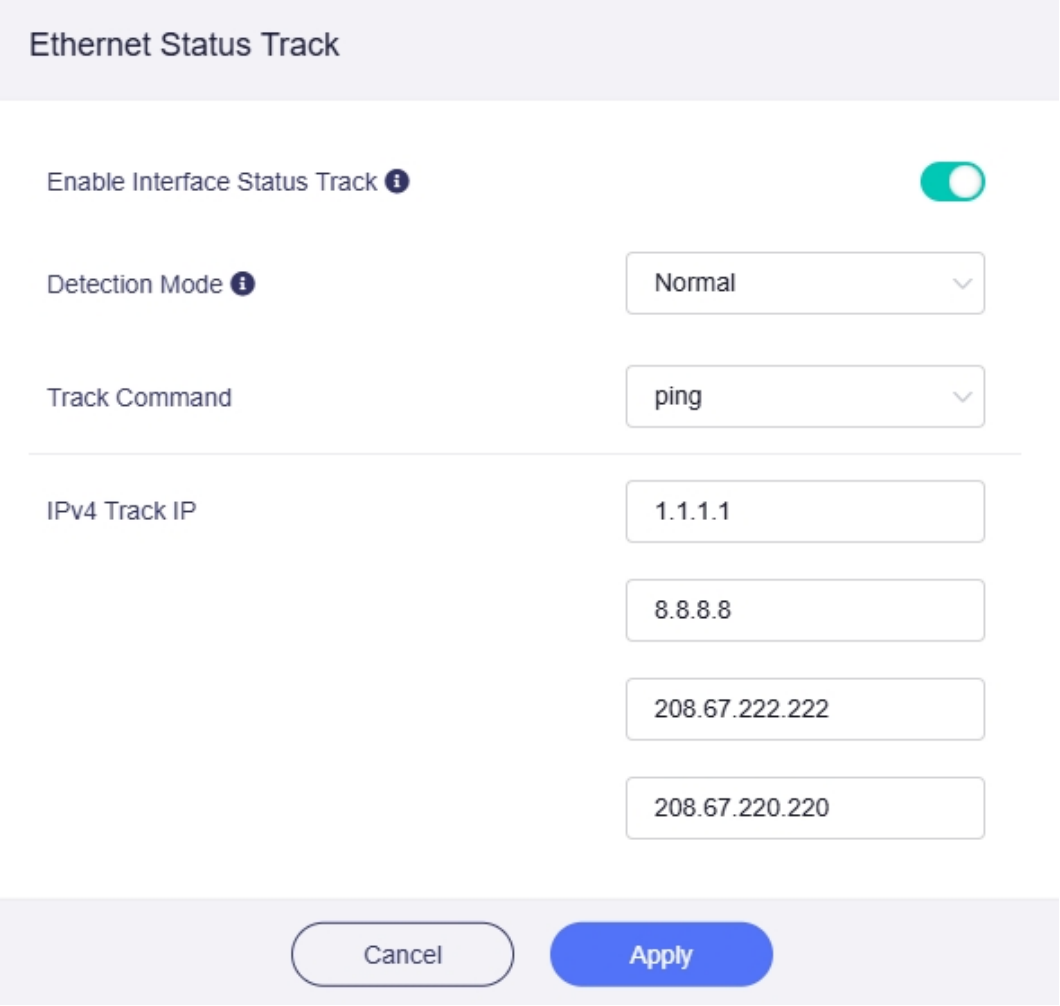
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Multi-WAN**. Strona obejmuje dwie sekcje: Interface Status Track i Multi-WAN Mode.

14.2.1 Monitorowanie stanu interfejsów

Routery GL.iNet używają polecenia **ping**, aby monitorować połączenie z docelowym adresem IP i określać dostępność interfejsu. Jeśli interfejs jest dostępny, po lewej pojawia się zielona kropka; w przeciwnym razie jest szara.



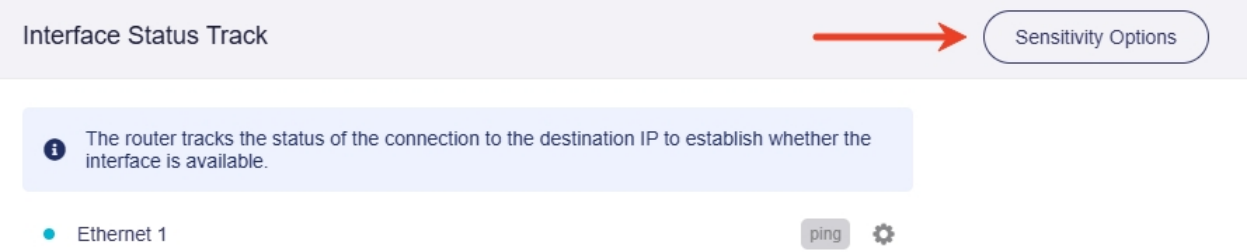
W sekcji **Interface Status Track** kliknij ikonę koła zębatego po prawej stronie, aby otworzyć ustawienia monitorowania poszczególnych interfejsów sieciowych. Poniżej pokazano ustawienia interfejsu Ethernet. Pozostałe interfejsy konfiguruje się według tych samych zasad.



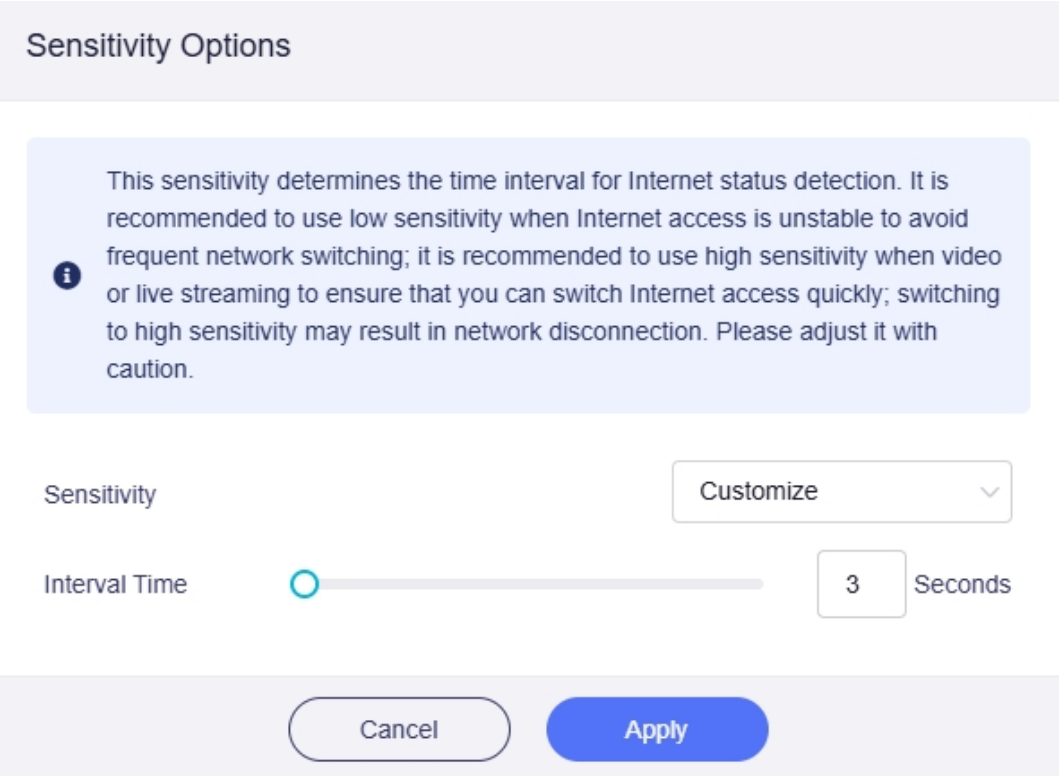
- **Enable Interface Status Track**: opcja jest domyślnie włączona. Po wyłączeniu router określa stan interfejsu na podstawie warunków fizycznych (np. podłączenia kabla Ethernet).
- **Detection Mode**: tę funkcję wprowadzono w wersji oprogramowania 4.5 jako Low Data Mode, a w wersji 4.7 zmieniono nazwę na Detection Mode. Dostępne są trzy tryby: Normal Mode, Low Data Mode i Strict Mode.
  - **Normal**: tryb używany domyślnie.
  - **Low Data**: uruchamia monitorowanie tylko po wystąpieniu błędu sieciowego w interfejsie. Używaj tego trybu, jeśli masz ograniczony pakiet danych. Pamiętaj, że ponowne połączenie po rozłączeniu może trwać nieco dłużej niż w trybie Normal. Ten tryb jest domyślnie włączony tylko dla interfejsu komórkowego.
  - **Strict**: określa stan interfejsu wyłącznie na podstawie wyników polecenia diagnostycznego wysyłanego na publiczny adres IP.
- **Track Command**: polecenie ping służy do monitorowania połączenia z docelowym adresem IP i sprawdzania dostępności interfejsu.

- **IPv4 Track IP**: w razie potrzeby dostosuj adresy IPv4 używane do monitorowania.

Kliknij **Sensitivity Options** w prawym górnym rogu.



Możesz ustawić częstotliwość sprawdzania dostępu do Internetu na Low, Medium lub High albo określić własny odstęp. Dostępny zakres wynosi od 0,5 do 90 sekund.

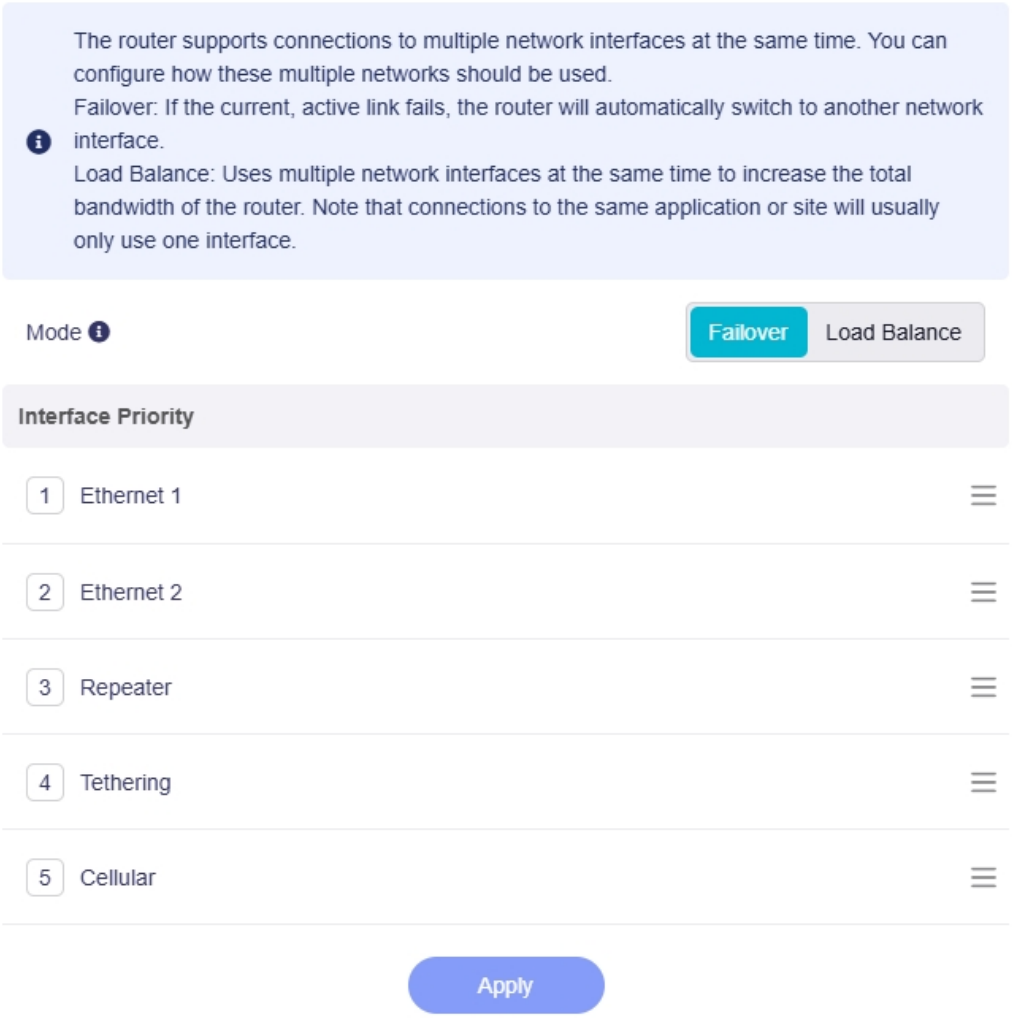


14.2.2 Tryb Multi-WAN

Multi-WAN oferuje dwa tryby: **Failover** i **Load Balance**. Tryby te wzajemnie się wykluczają.

Przełączanie awaryjne (Failover)

Failover jest trybem domyślnym po skonfigurowaniu wielu połączeń. Jeśli aktywne łącze ulegnie awarii, router automatycznie przełącza się na inny interfejs sieciowy zapewniający dostęp do Internetu.

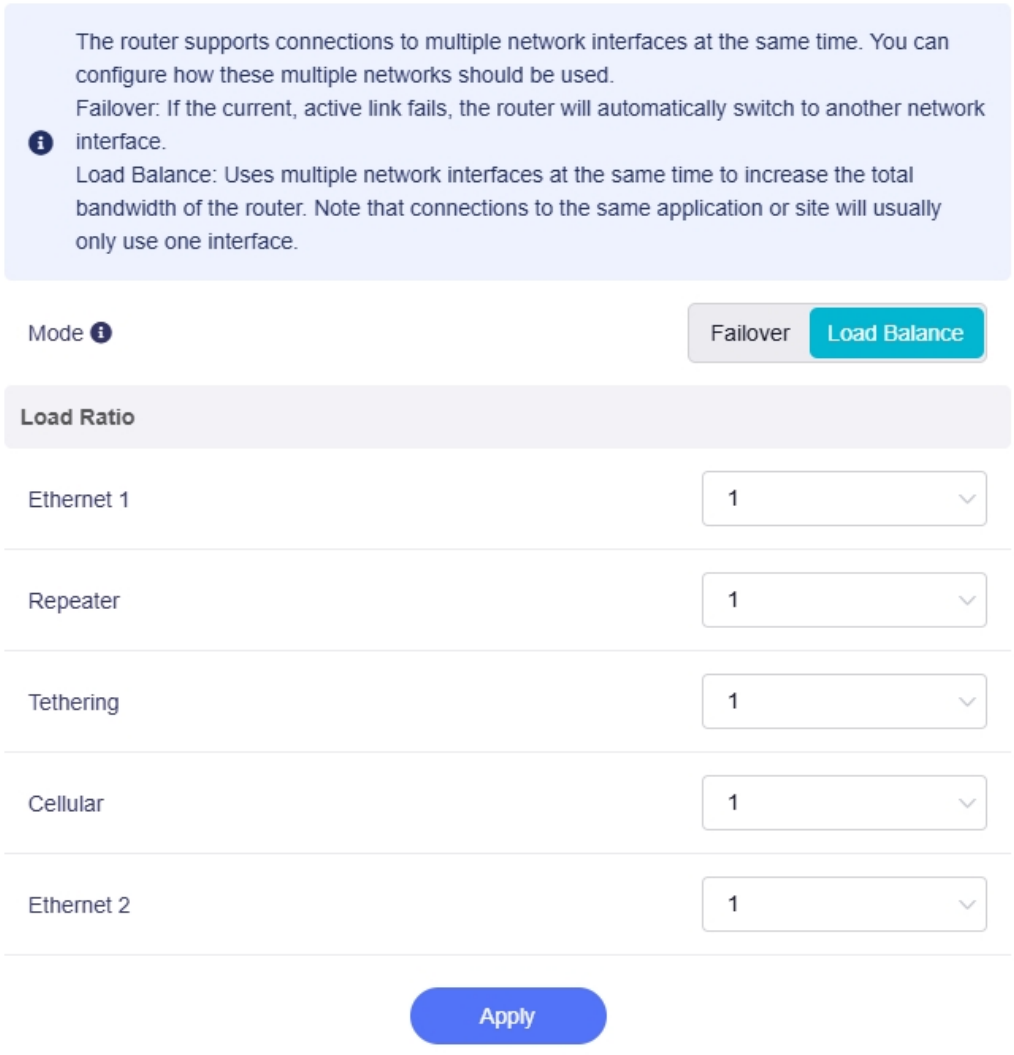


Możesz ustawić priorytety interfejsów. Po awarii używanego interfejsu router przełącza się na dostępny interfejs o najwyższym priorytecie. Gdy połączenie o wyższym priorytecie zostanie przywrócone, router automatycznie do niego wróci.

Równoważenie obciążenia (Load Balance)

Tryb Load Balance korzysta jednocześnie z wielu interfejsów sieciowych, zwiększając łączną przepustowość routera. System rozdziela nowe połączenia między interfejsy zgodnie z ustawionymi proporcjami obciążenia. Połączenia z tą samą aplikacją lub witryną zazwyczaj korzystają jednak tylko z jednego interfejsu.

Proporcje obciążenia określają udział poszczególnych interfejsów sieciowych. System przydziela interfejsom nowe połączenia zgodnie z tym ustawieniem.



Na przykład jeśli router jest jednocześnie połączony z czterema sieciami (np. Ethernet, Repeater, Tethering i Cellular), a wszystkie cztery interfejsy mają dostęp do Internetu, włączenie Load Balance i ustawienie proporcji 1:1:1:1 oznacza równy podział pasma między

cztery interfejsy. System rozdziela nowe połączenia między te interfejsy zgodnie z ustawionymi proporcjami 1:1:1:1.

W razie potrzeby możesz dostosować proporcje obciążenia. Jeśli na przykład Ethernet ma przepustowość 100 Mb/s, Repeater 200 Mb/s, a połączenia Tethering i Cellular są nieaktywne, ustaw proporcje na 1 dla Ethernet, 2 dla Repeater oraz 0 dla Tethering i Cellular. System będzie rozdzielać nowe połączenia między te interfejsy w proporcji 1:2, więc Ethernet obsłuży o połowę mniej połączeń niż Repeater. Ten tryb optymalizuje ogólną przepustowość przez równoważenie ruchu między wszystkimi dostępnymi interfejsami, inaczej niż tryb Failover.

Uwaga: nie ma gwarancji, że istniejące połączenia lub ruch będą odpowiadać ustawionym proporcjom. Przy dłuższym korzystaniu rzeczywisty rozkład stopniowo się do nich zbliży.

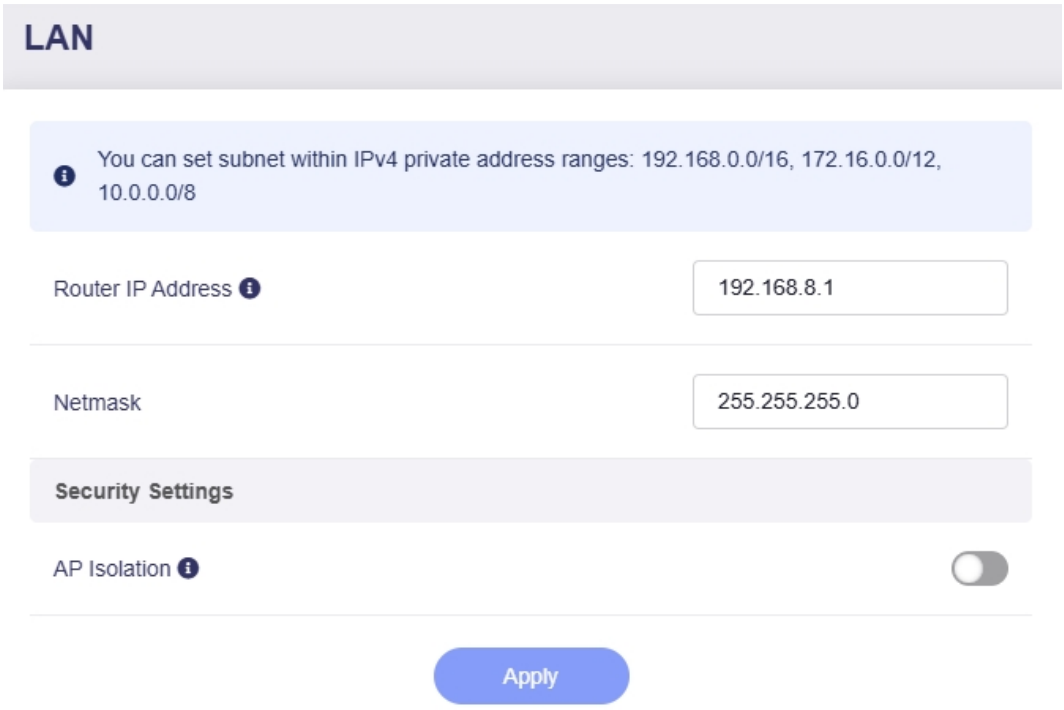
14.3 LAN

LAN (Local Area Network) to prywatna sieć lokalna, do której urządzenia łączą się za pomocą kabli Ethernet.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **LAN**. Tutaj możesz konfigurować ustawienia LAN: ustawienia podstawowe, serwer DHCP i rezerwację adresów.

14.3.1 Ustawienia podstawowe

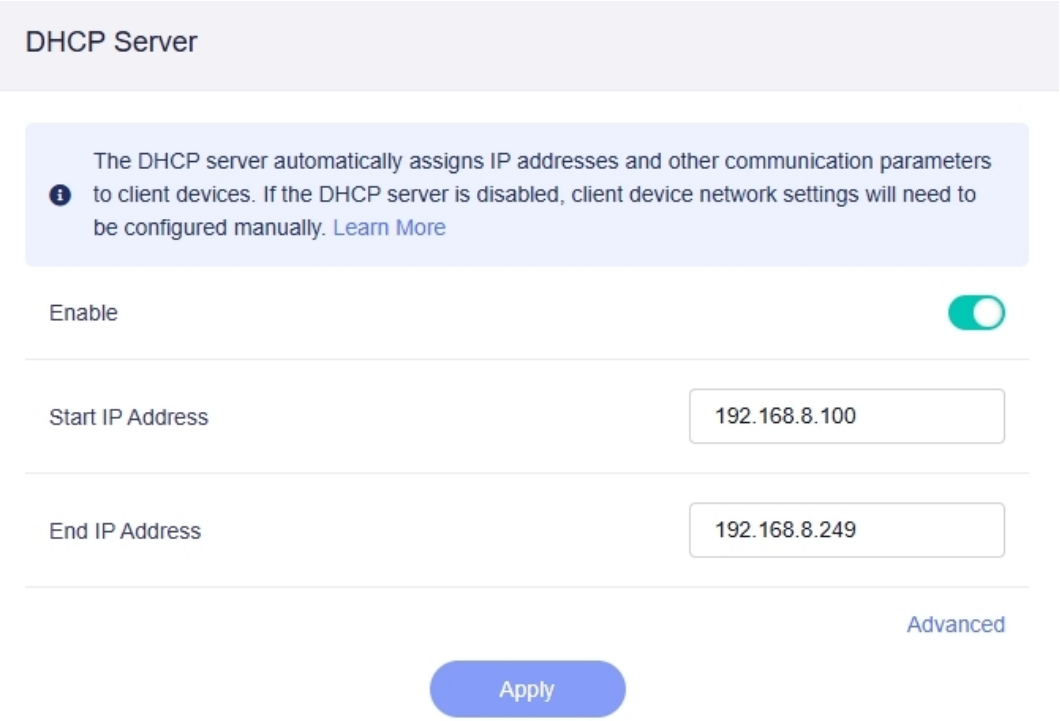
Ustawienia podstawowe obejmują adres IP routera i maskę sieci. Podsieć można ustawić w prywatnych zakresach adresów IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8.



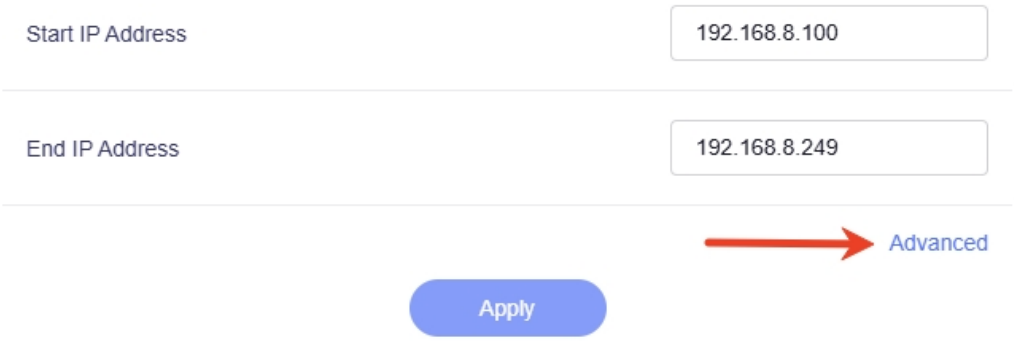
- **Router IP Address**: adres wpisywany w pasku adresu przeglądarki w celu otwarcia panelu administracyjnego routera. Domyślnie jest to 192.168.8.1. Można go zmienić, jeśli koliduje z siecią nadrzędną.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **AP Isolation**: umożliwia wydzielenie urządzeń klienckich do osobnego obszaru sieci. Nie mogą one komunikować się z innymi urządzeniami w sieci.

14.3.2 Serwer DHCP

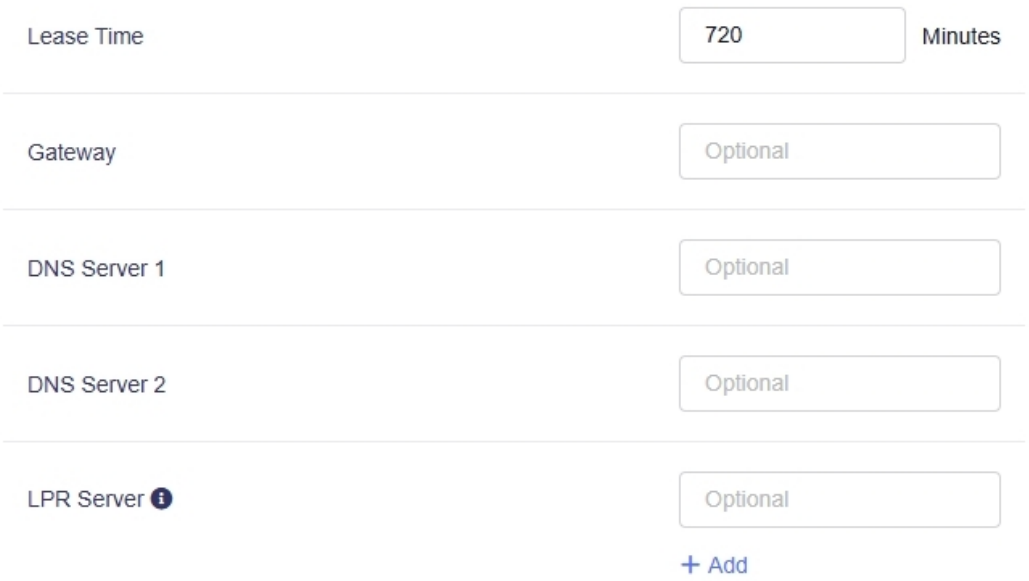
Serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. W routerze GL.iNet jest domyślnie włączony, a jego pula adresów IP obejmuje zakres od 192.168.8.100 do 192.168.8.249. W razie potrzeby można zmienić ten zakres.



Kliknij **Advanced** w prawym dolnym rogu.



Możesz skonfigurować ustawienia zaawansowane: czas dzierżawy, bramę, serwery DNS i serwer LPR.



- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP.
- **Gateway**: element routera kierujący ruch między siecią lokalną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server 1**: serwer główny odpowiedzialny za tłumaczenie nazw domen na adresy IP.
- **DNS Server 2**: serwer zapasowy używany do rozwiązywania nazw domen w razie awarii głównego serwera DNS.
- **LPR Server**: (Line Printer Remote Server) usługa zarządzająca zadaniami drukowania i umożliwiająca urządzeniom sieciowym wysyłanie żądań do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

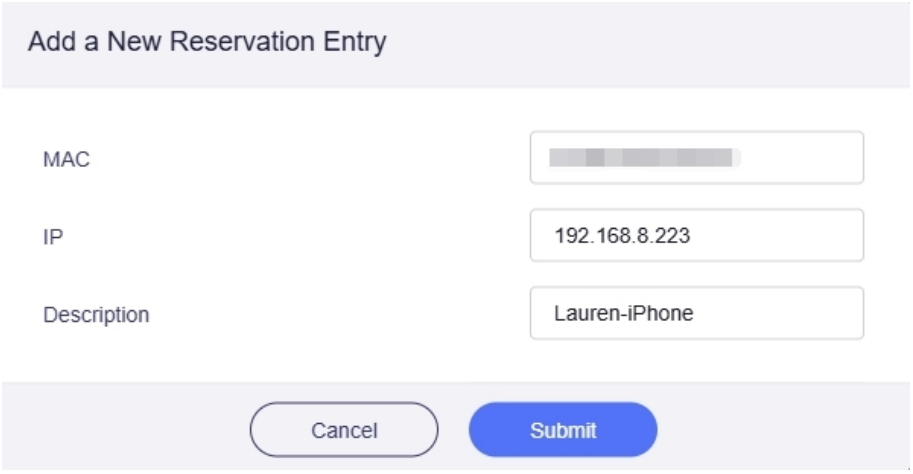
Uwaga: po wyłączeniu serwera DHCP trzeba ręcznie skonfigurować statyczny adres IP i inne parametry komunikacji na każdym urządzeniu klienckim. Szczegóły znajdziesz tutaj.

14.3.3 Rezerwacja adresów

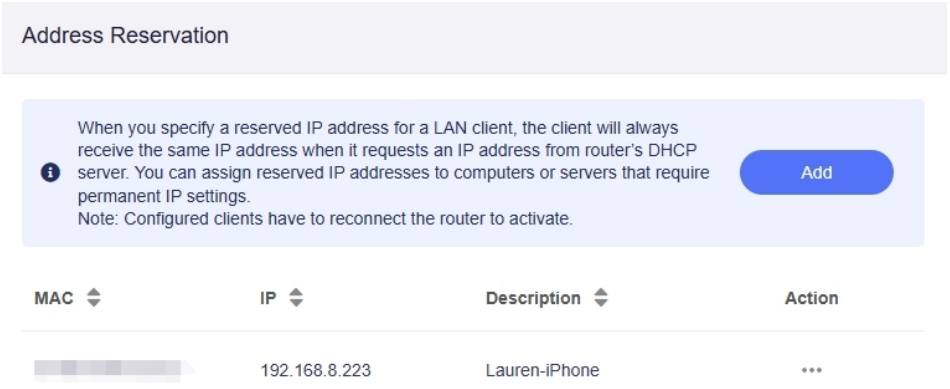
Rezerwacja adresów umożliwia przypisanie stałego adresu IP klientowi LAN, dzięki czemu przy każdym kontakcie z serwerem DHCP routera otrzymuje on ten sam adres. Zarezerwowane adresy można przypisywać komputerom lub serwerom wymagającym stałych ustawień IP. Aby ustawienie zaczęło działać, urządzenia z rezerwacją adresu muszą ponownie połączyć się z routerem.

Aby w razie potrzeby skonfigurować rezerwację adresów, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera, przejdź do **NETWORK** > **LAN** > **Address Reservation** i kliknij **Add**.
2. W wyświetlonym oknie wybierz adres MAC z listy. Odpowiadający mu adres IP zostanie uzupełniony automatycznie. Wprowadź opisową nazwę i kliknij **Submit**.



3. Po dodaniu rezerwacji adresu IP na stronie pojawi się odpowiedni wpis, jak pokazano poniżej.



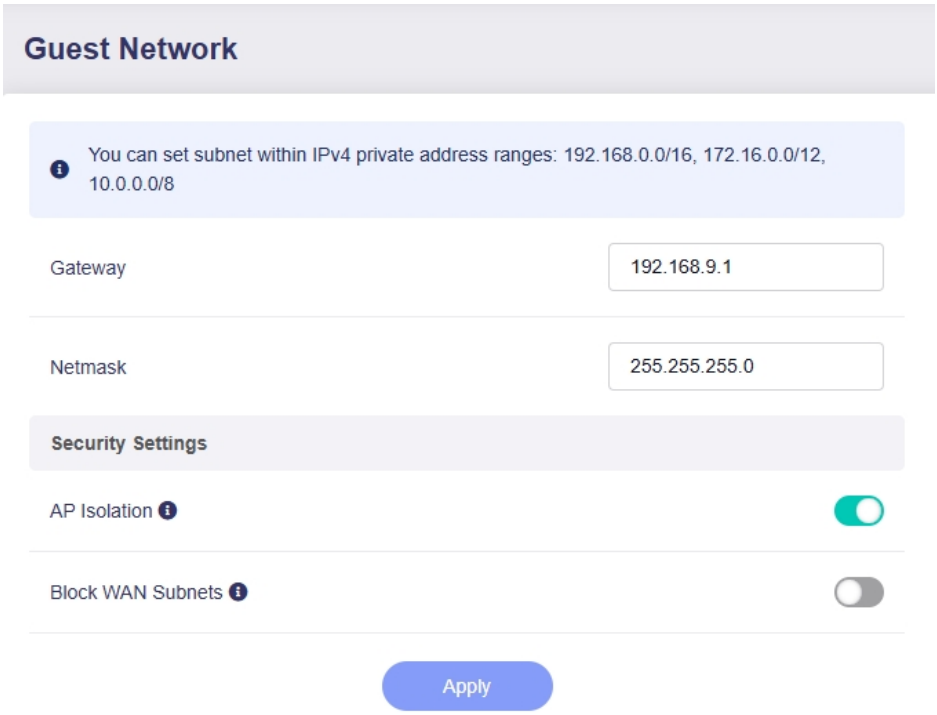
14.4 Sieć gościnna

Sieć gościnna to oddzielna sieć dla gości, odizolowana od głównej sieci LAN w celu ochrony bezpieczeństwa sieci prywatnej.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** -> **Guest Network**. Tutaj możesz skonfigurować ustawienia sieci gościnnej, w tym ustawienia podstawowe i serwer DHCP.

14.4.1 Ustawienia podstawowe

Podstawowe ustawienia obejmują Gateway, Netmask, AP Isolation i Block WAN Subnets.

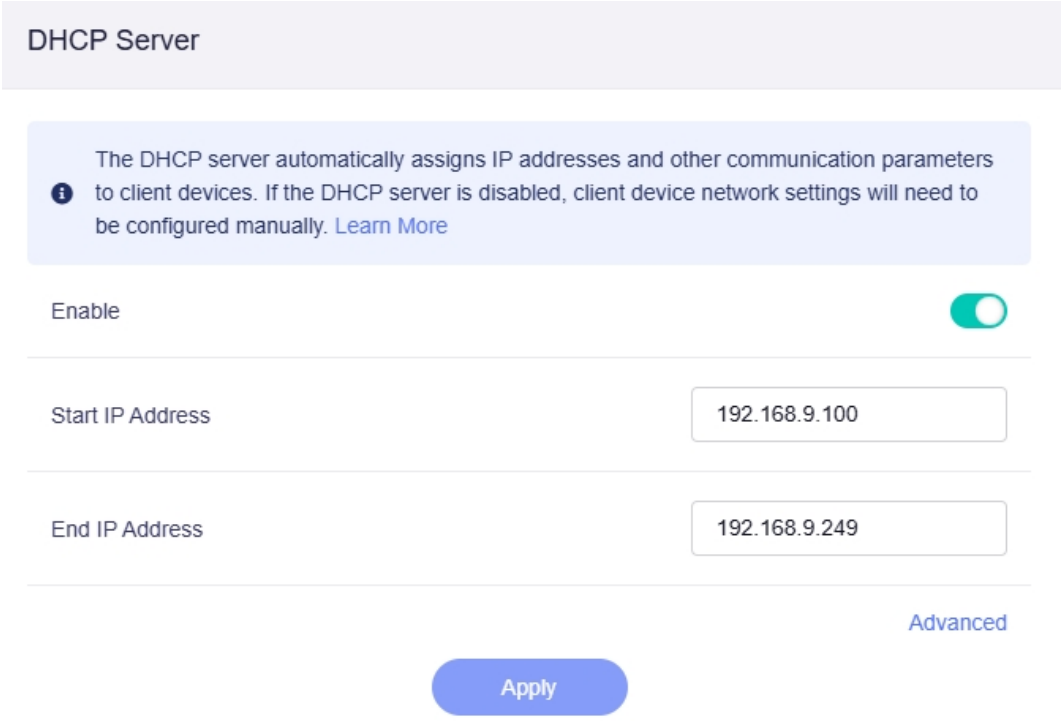


- **Gateway**: domyślny adres to 192.168.9.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.
- **Block WAN Subnets**: po włączeniu sieć gościnna nie może uzyskiwać dostępu do sieci nadrzędnej ani odpowiadającego jej segmentu sieci.

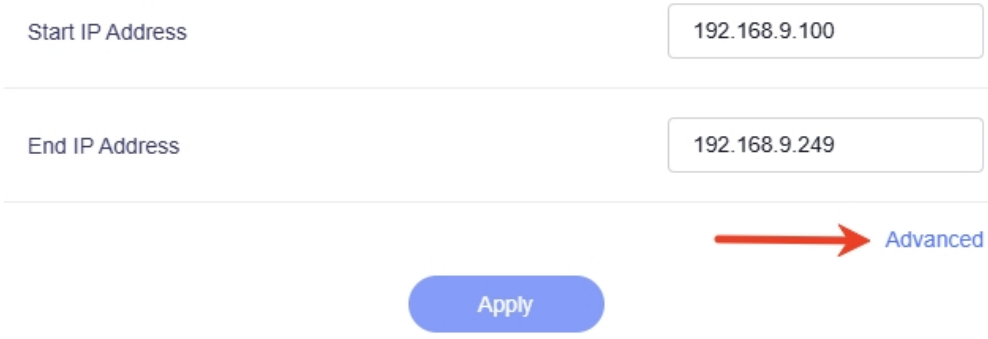
14.4.2 Serwer DHCP

Ponieważ sieć gościnna jest domyślnie wyłączona, jej serwer DHCP również jest wyłączony i ukryty do czasu ręcznego włączenia sieci.

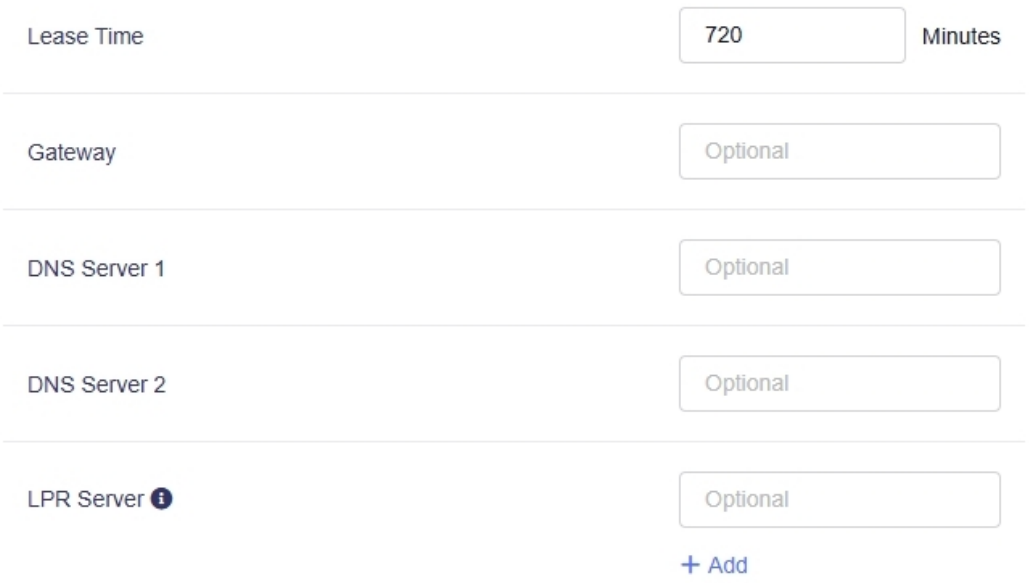
Po włączeniu serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. Pula adresów IP sieci gościnnej obejmuje zakres od 192.168.9.100 do 192.168.9.249. W razie potrzeby można go zmienić.



Kliknij **Advanced** w prawym dolnym rogu.



Możesz skonfigurować ustawienia zaawansowane: czas dzierżawy, bramę, serwery DNS i serwer LPR.



- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP sieci gościnnej.
- **Gateway**: element routera kierujący ruch między siecią gościnną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server 1**: serwer główny odpowiedzialny za tłumaczenie nazw domen na adresy IP.
- **DNS Server 2**: serwer zapasowy używany do rozwiązywania nazw domen w razie awarii głównego serwera DNS.
- **LPR Server**: (Line Printer Remote Server) usługa zarządzająca zadaniami drukowania i umożliwiająca urządzeniom sieciowym wysyłanie żądań do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

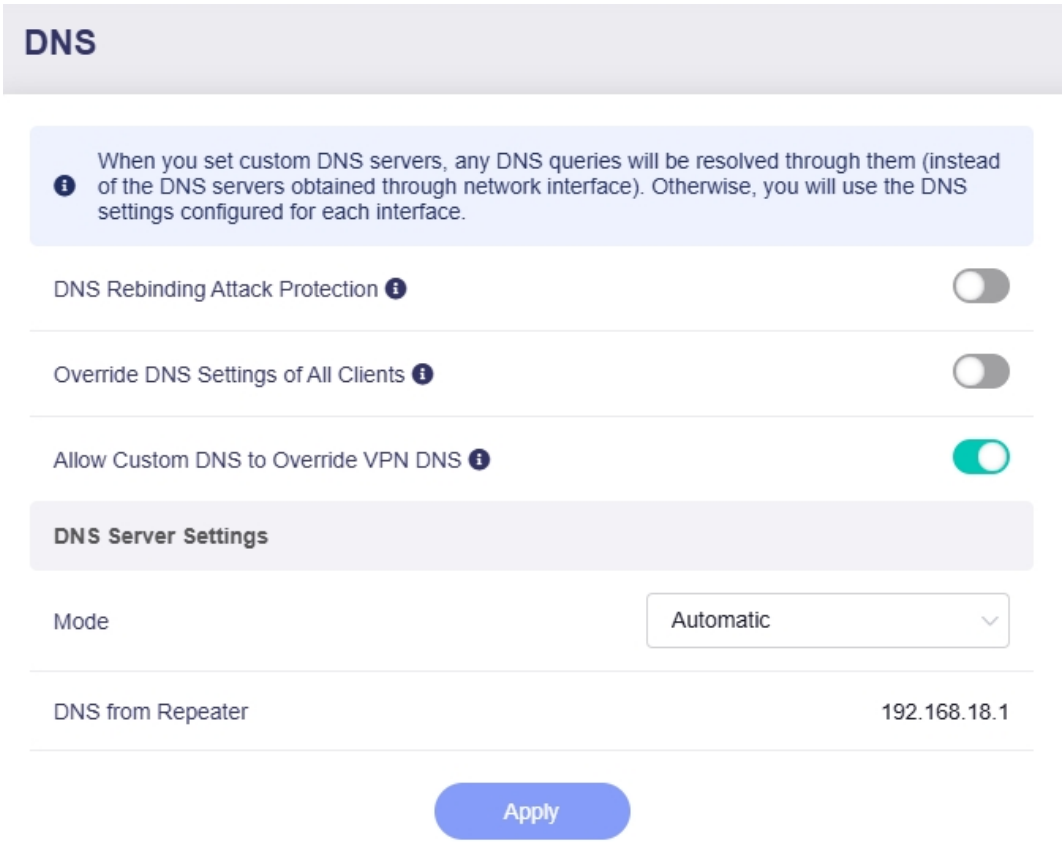
14.5 DNS

DNS (Domain Name System) to usługa tłumacząca czytelne dla człowieka nazwy domen, takie jak www.google.com, na adresy IP, dzięki czemu urządzenia mogą znajdować witryny i usługi internetowe oraz łączyć się z nimi.

Ustawienia DNS routera zwykle określają serwery DNS używane przez podłączone urządzenia. Router najczęściej pobiera ich adresy automatycznie od dostawcy Internetu lub sieci nadrzędnej albo pozwala ręcznie wskazać publiczne serwery DNS, np. 8.8.8.8, w interfejsie zarządzania. Skonfigurowane ustawienia są zazwyczaj automatycznie przekazywane podłączonym urządzeniom, dlatego nie trzeba ustawiać DNS na każdym z nich oddzielnie.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **DNS**. Tutaj możesz konfigurować ustawienia DNS.

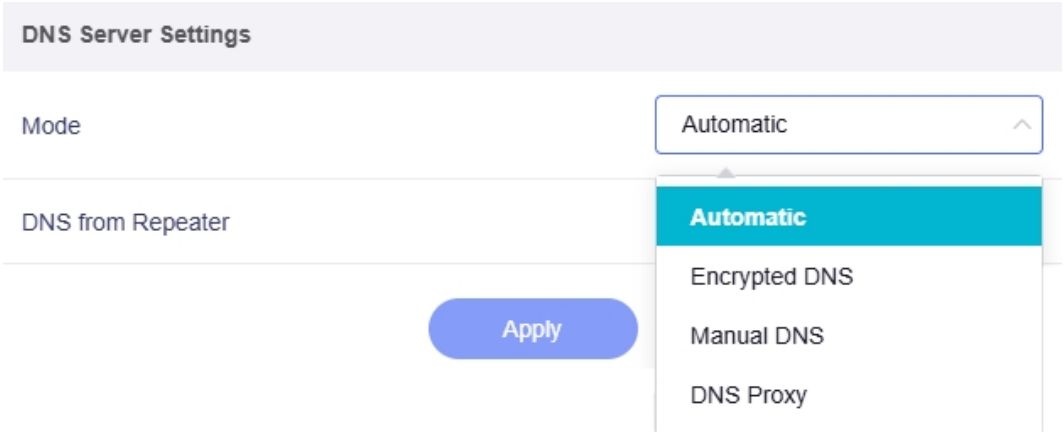
14.5.1 Ustawienia ogólne



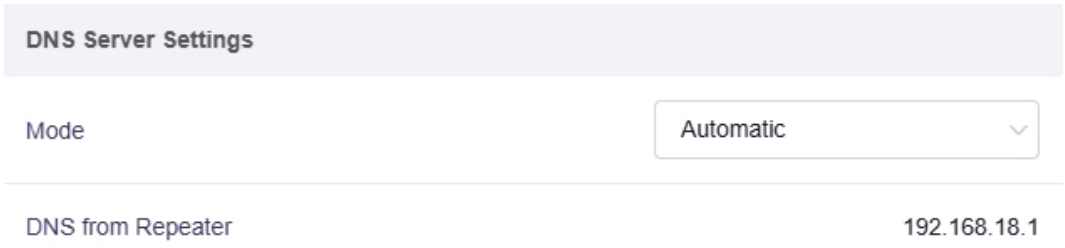
- **DNS Rebinding Attack Protection**: chroni przed atakami DNS rebinding przez blokowanie złośliwych prób rozwiązywania nazw DNS. Włączenie może spowodować problemy z prywatnymi zapytaniami DNS. Wyłącz tę opcję, jeśli sieć korzysta z portalu logowania (np. strony logowania do publicznego Wi-Fi).
- **Override DNS Settings of All Clients**: po włączeniu wszystkie podłączone urządzenia muszą korzystać z serwerów DNS skonfigurowanych na routerze, niezależnie od własnych ustawień DNS. Zapewnia to jednolitą konfigurację DNS dla wszystkich urządzeń.
- **Allow Custom DNS to Override VPN DNS**: po włączeniu, jeśli skonfigurowano własny DNS, pakiety przesyłane przez tunel VPN będą używać go do rozwiązywania nazw zamiast serwerów DNS połączenia VPN. Zapewnia to normalne stosowanie własnych reguł DNS podczas korzystania z VPN.

14.5.2 Ustawienia serwera DNS

Dostępne są cztery tryby serwera DNS: Automatic, Encrypted DNS, Manual DNS i DNS Proxy.

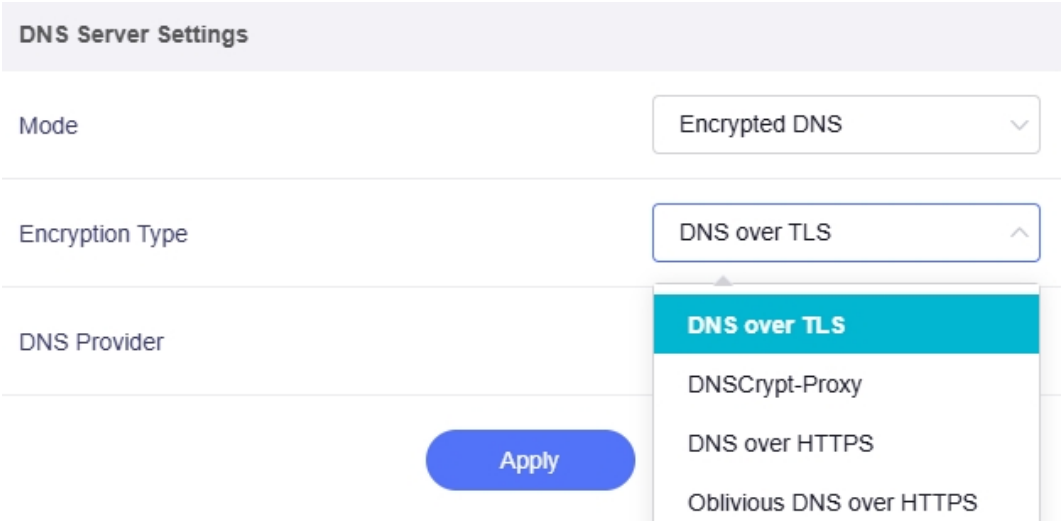


1. **Automatic**: router automatycznie pobiera adresy serwerów DNS z sieci nadrzędnej i stosuje je do wszystkich podłączonych urządzeń.



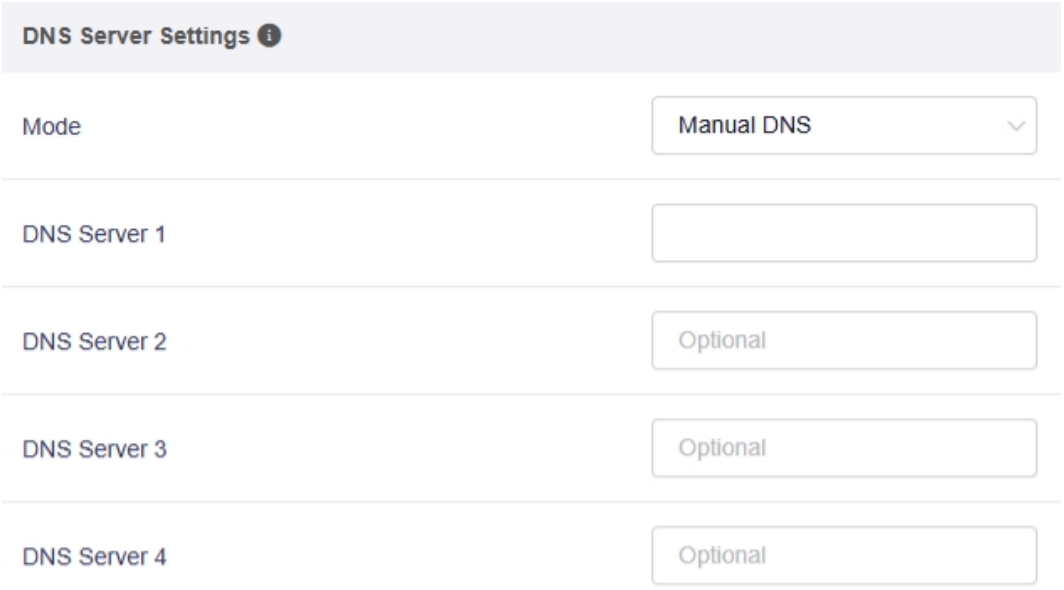
2. **Encrypted DNS**: router używa szyfrowanych protokołów do obsługi zapytań DNS, chroniąc dane rozwiązywania nazw przed podsłuchiwaniem i modyfikacją.

Dostępne są cztery rodzaje szyfrowania: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS.



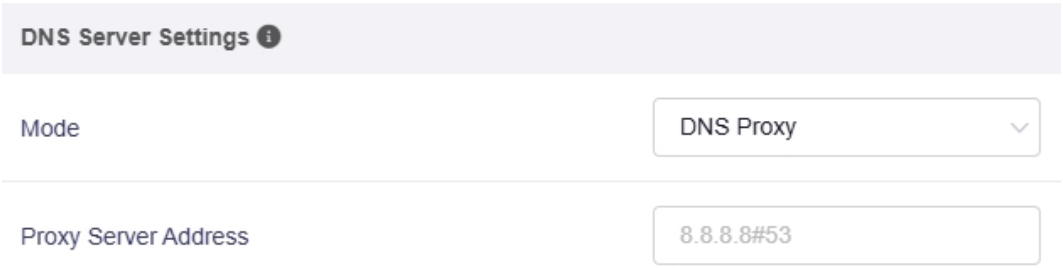
- Dla DNS over TLS wybierz dostawcę DNS spośród Control D, NextDNS i Cloudflare.
- Dla pozostałych trzech opcji (DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS) wybierz z repozytorium co najmniej jeden serwer DNS. Można wybrać maksymalnie 8 serwerów. Przy wielu serwerach router automatycznie używa najszybszego.

3. **Manual DNS**: umożliwia samodzielne ustawienie serwerów DNS routera. Kliknij DNS Server 1 i wybierz serwer z listy. Pozostałe pola DNS zaktualizują się automatycznie.



Uwaga: aby używać adresów IPv6 w ręcznej konfiguracji DNS, najpierw włącz IPv6 na routerze.

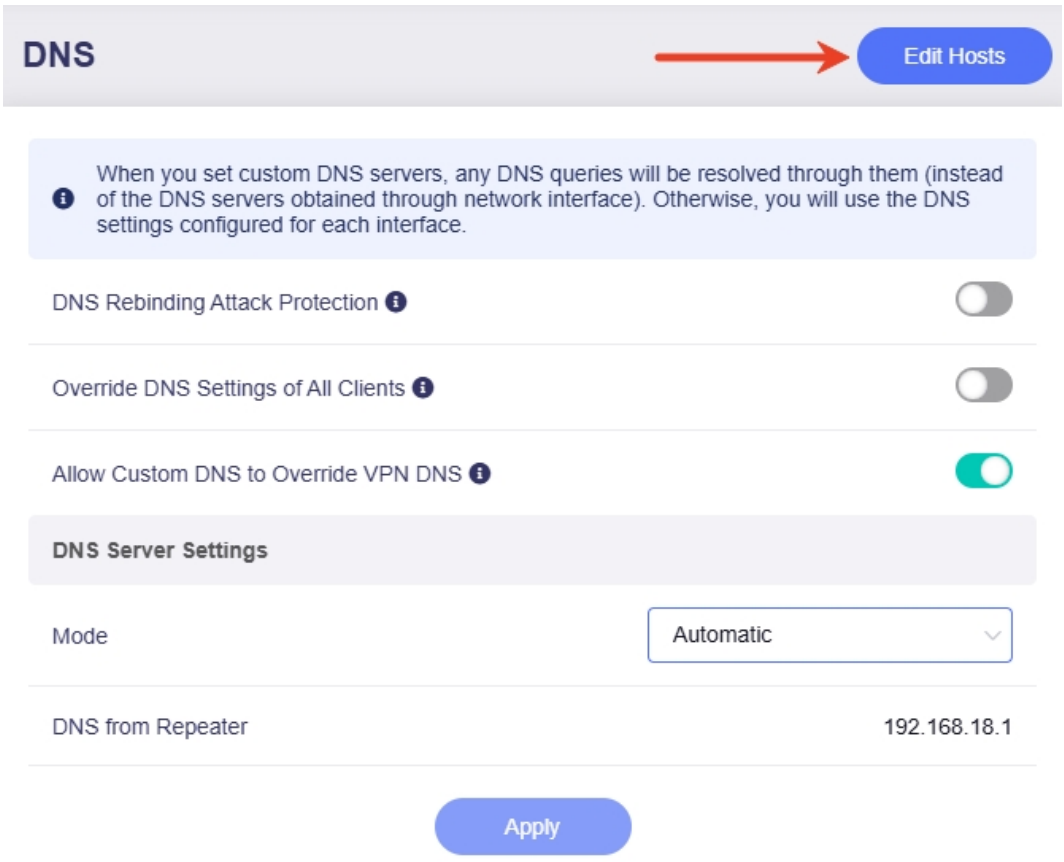
4. **DNS Proxy**: router przekazuje wszystkie zapytania DNS przez serwer proxy, umożliwiając rozwiązywanie nazw w środowisku sieciowym tego serwera na potrzeby określonego dostępu.



14.5.3 Edycja pliku hosts

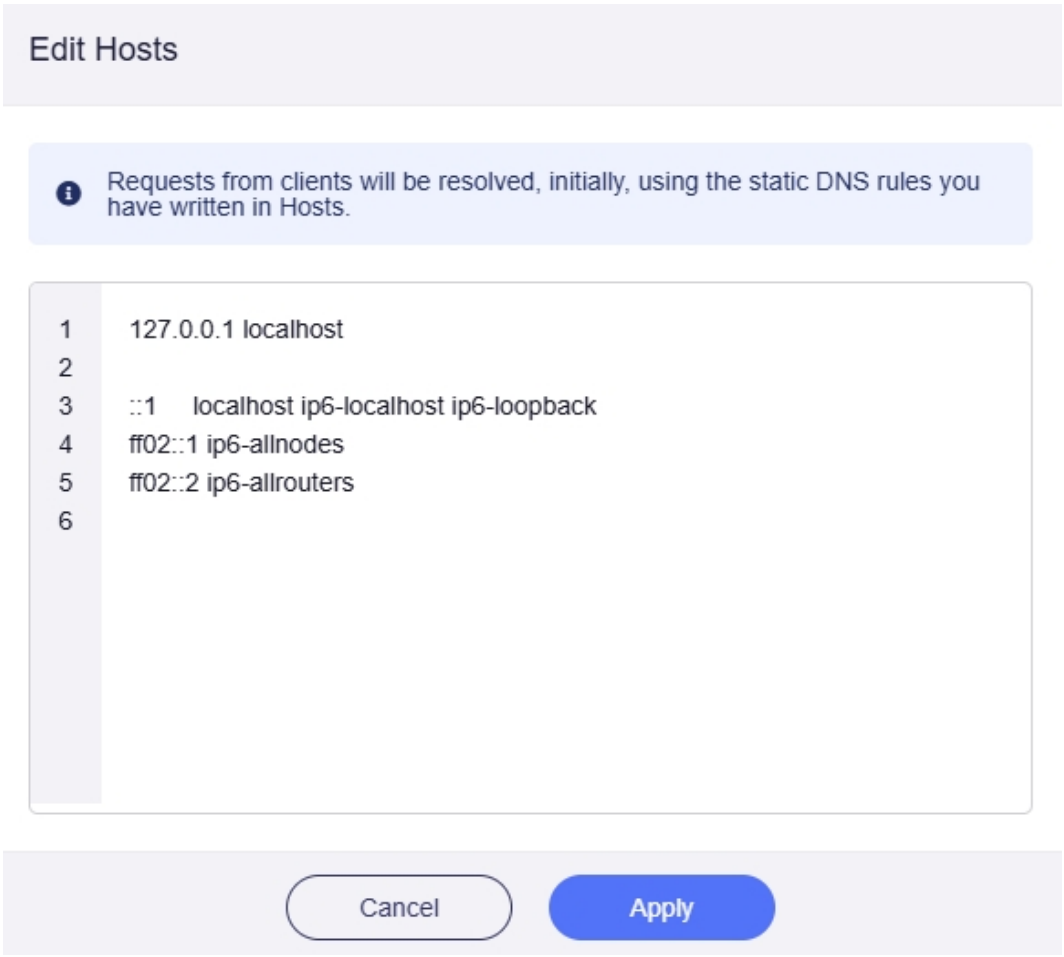
W razie potrzeby możesz zdefiniować statyczne reguły rozwiązywania nazw DNS.

Na stronie DNS kliknij **Edit Hosts** w prawym górnym rogu.



Żądania klientów są rozwiązywane w pierwszej kolejności według wpisanych tutaj statycznych reguł DNS. Pozwala to ręcznie mapować adresy IP na nazwy hostów (np. domyślny wpis

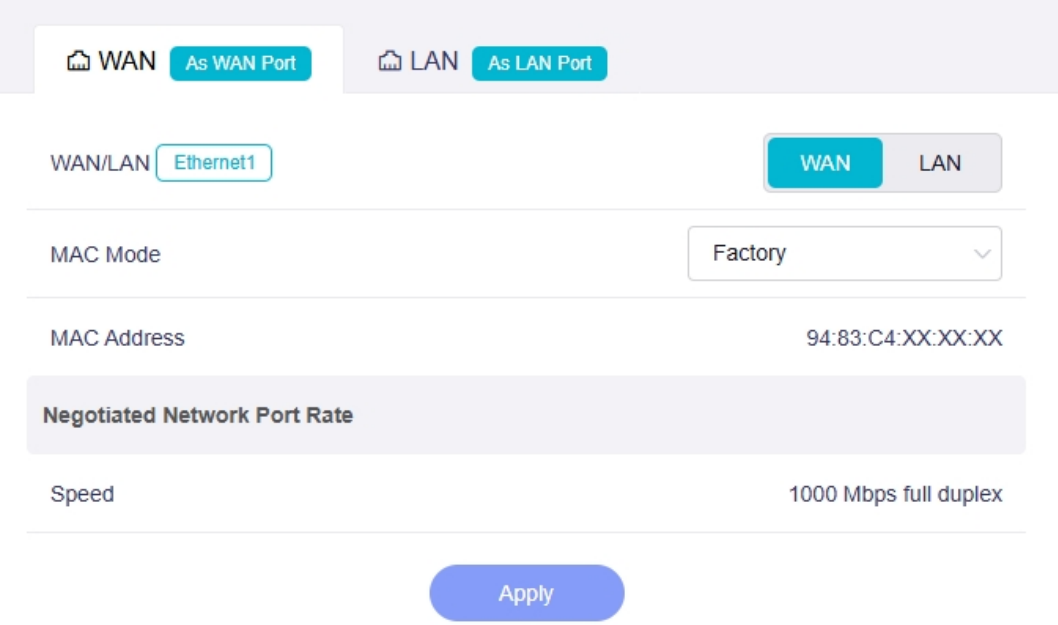
127.0.0.1 localhost dla lokalnej pętli zwrotnej) i samodzielnie kontrolować rozwiązywanie nazw domen.



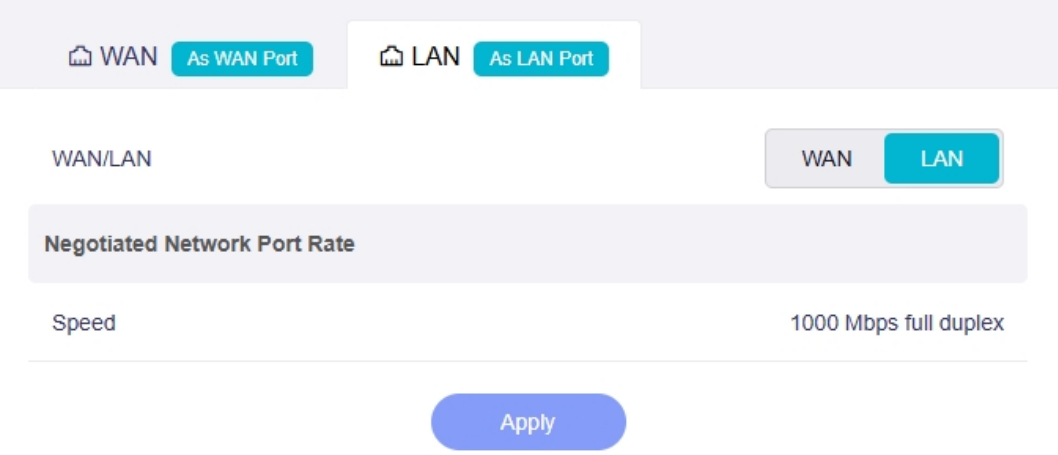
14.6 Port Ethernet

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Ethernet Port**. Ta strona umożliwia zarządzanie portami Ethernet routera.

Sekcja **WAN** wyświetla rolę portu (WAN lub LAN), adres MAC i wynegocjowaną prędkość.



Sekcja **LAN** wyświetla wynegocjowaną prędkość portu LAN.

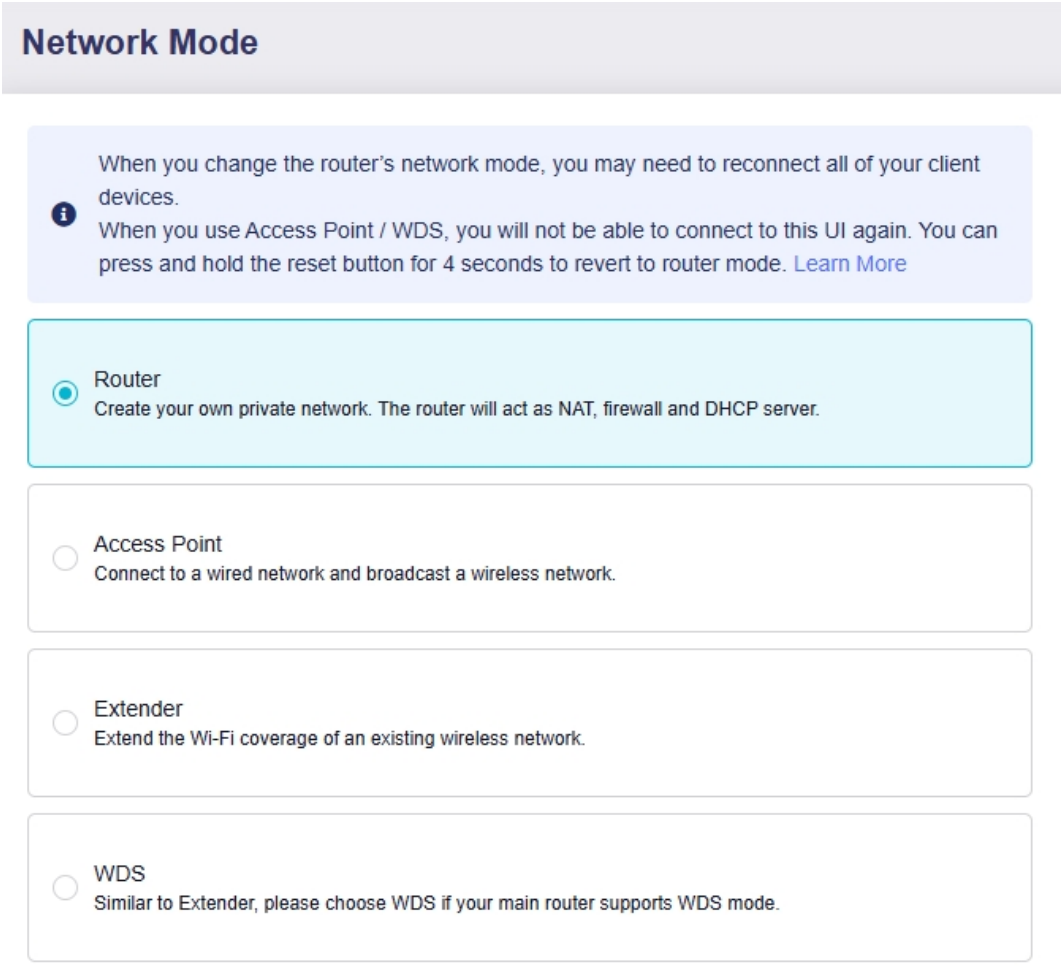


Uwaga: wynegocjowana prędkość portów WAN i LAN jest wyświetlana tylko po podłączeniu kabla Ethernet. Zależy zarówno od portu Ethernet, jak i kabla Ethernet.

14.7 Tryb sieciowy

Tryb sieciowy określa rolę i funkcje routera, dostosowane do różnych sposobów wdrażania sieci.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Network Mode**. Tutaj możesz zmienić tryb sieciowy routera.



- **Router**: domyślny tryb większości routerów domowych i małych biur. Tworzy prywatną sieć lokalną (LAN) i pełni funkcję bramy między publicznym Internetem a podłączonymi urządzeniami. W tym trybie działają podstawowe funkcje: NAT, DHCP i wbudowana zapora. Router łączy się z łączem nadrzędnym, np. światłowodowym, automatycznie przydziela prywatne adresy IP podłączonym urządzeniom i chroni całą sieć prywatną.
- **Access Point**: w tym trybie router łączy się z siecią przewodową kablem LAN i nadaje sygnał bezprzewodowy, rozszerzając zasięg Wi-Fi w dużych przestrzeniach i zapewniając dostęp większej liczbie urządzeń. NAT i DHCP są wyłączone, a router działa wyłącznie jako nadajnik bezprzewodowy i przełącznik, bez funkcji samodzielnej bramy.

- **Extender**: ten tryb rozszerza zasięg istniejącej sieci Wi-Fi i eliminuje martwe strefy o słabej łączności. Router bezprzewodowo odbiera sygnał z głównego routera, wzmacnia go i nadaje ponownie. W odróżnieniu od trybu Access Point nie wymaga połączenia przewodowego z głównym routerem. Może jednak zmniejszyć przepustowość o połowę, ponieważ urządzenie jednocześnie odbiera i nadaje sygnał.
- **WDS**: tryb Wireless Distribution System (WDS), podobnie jak Extender, bezprzewodowo rozszerza zasięg Wi-Fi, ale obsługuje mosty bezprzewodowe między wieloma zgodnymi routerami. Jest zalecany do rozbudowy sieci bezprzewodowej, gdy router nadrzędny obsługuje WDS.

  Ten tryb sprawdza się np. w budynkach wielopiętrowych lub małych kompleksach biurowych, w których wiele routerów musi współpracować w ramach jednej sieci bezprzewodowej. W odróżnieniu od trybu Extender, przesyłającego sygnał z jednego głównego routera do jednego wzmacniacza, WDS pozwala połączonym routerom zarówno nadawać, jak i odbierać sygnały, zapewniając płynny zasięg na większych obszarach z wieloma węzłami.

Uwaga:

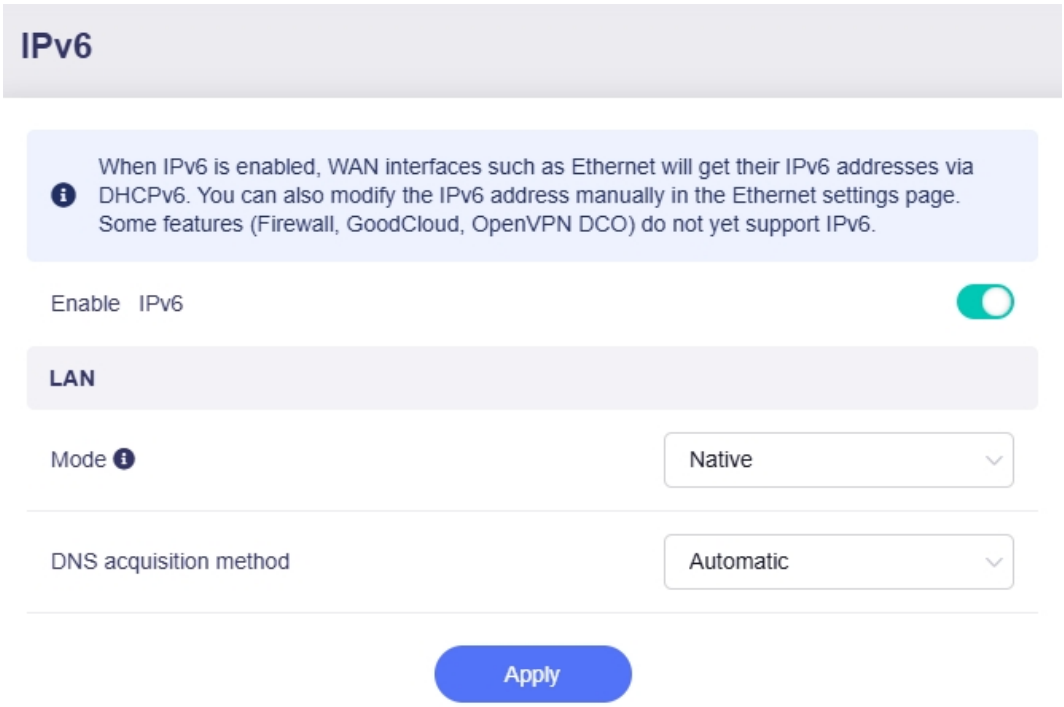
1. Po zmianie trybu sieciowego wszystkie urządzenia klienckie powinny ponownie połączyć się z routerem, aby zapewnić stabilną łączność.
2. **W trybie Access Point / WDS panel administracyjny nie jest dostępny pod pierwotnym adresem IP**. Zaloguj się do routera nadrzędnego, znajdź adres IP przydzielony temu routerowi i użyj go do otwarcia panelu administracyjnego. Jeśli nie masz dostępu do routera nadrzędnego, naciśnij i przytrzymaj przycisk resetowania przez 4 sekundy, aby przywrócić domyślny tryb Router.
3. **W trybach Access Point / Extender / WDS niedostępne są następujące funkcje**: kontrola dostępu (Allowlist i Blocklist), AstroWarp, VPN, AdGuard Home, kontrola rodzicielska, ZeroTier, Tailscale, przekierowanie portów, Multi-WAN, serwer DHCP, rezerwacja adresów, sieć gościnna, DNS, Ethernet Port, IPv6, Drop-in Gateway, IGMP Snooping, przyspieszanie sieci i ustawienia NAT.

14.8 IPv6

IPv6 (Internet Protocol version 6) to najnowsza wersja protokołu internetowego, zaprojektowana jako następca IPv4. Zapewnia większą pulę unikalnych adresów IP, rozwiązując problem wyczerpywania adresów IPv4 i obsługując rosnącą liczbę podłączonych urządzeń na świecie.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IPv6**. Tutaj możesz włączyć i skonfigurować IPv6. Po włączeniu interfejsy WAN, np. Ethernet, uzyskują adresy IPv6 przez DHCPv6.

Włącz **Enable IPv6**, wybierz tryb sieci głównej i sposób uzyskiwania DNS, a następnie kliknij **Apply.**



Uwaga: niektóre funkcje (np. zapora, GoodCloud, OpenVPN DCO) nie obsługują jeszcze IPv6. Ich jednoczesne włączenie z IPv6 może powodować problemy z połączeniem.

14.8.1 Tryb IPv6

Dostępne są cztery tryby: Native, Passthrough, NAT6 i Static IPv6.

- **Native**: odpowiedni, gdy router bezpośrednio uzyskuje publiczny adres IPv6 i automatycznie przydziela adresy IPv6 podłączonym urządzeniom. Spełnia potrzeby większości użytkowników korzystających z IPv6.
- **Passthrough**: odpowiedni, gdy pakiety IPv6 mają być przekazywane bezpośrednio, bez przetwarzania ani konwersji. Niektóre aplikacje lub usługi mogą wymagać zachowania pełnej zawartości pakietów IPv6 do dalszego przetwarzania lub analizy. Ten tryb jest używany przez specjalistów do diagnostyki sieci i analizy bezpieczeństwa.
- **NAT6**: odpowiedni, gdy router działa jako brama przydzielająca każdemu urządzeniu w sieci dynamiczny wewnętrzny adres IPv6. W tym trybie urządzenia końcowe łączą się przez terminal sieci optycznej i uzyskują adres IPv6 sieci lokalnej.
- **Static IPv6**: odpowiedni dla urządzeń i usług wymagających stałego adresu IPv6, np. serwerów lub drukarek sieciowych. Urządzenie zawsze używa tego samego adresu IPv6, co ułatwia zarządzanie i dostęp.

14.8.2 Sposób uzyskiwania DNS

Określa sposób uzyskiwania przez router adresów serwerów DNS IPv6. Dostępne są dwie opcje: Automatic i Manual.

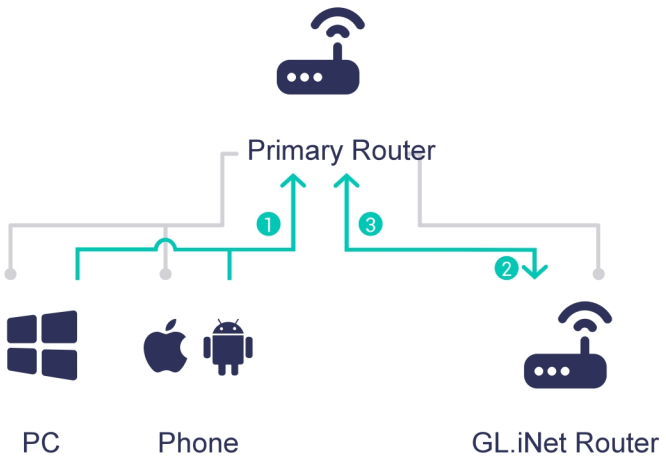
- **Automatic**: router dynamicznie uzyskuje adresy serwerów DNS IPv6 (np. przez DHCPv6).
- **Manual**: wprowadź własne adresy serwerów DNS IPv6. Ponieważ DNS służy do tłumaczenia nazw domen na odpowiadające im adresy IP, ręczna konfiguracja serwera DNS może powodować błędy rozwiązywania nazw. Używaj jej ostrożnie.

14.9 Drop-in Gateway

Drop-in Gateway rozszerza możliwości istniejącego głównego routera bez jego wymiany ani ponownej konfiguracji. Po podłączeniu routera GL.iNet do głównego routera kablem Ethernet można dodać do istniejącej infrastruktury zaawansowane funkcje, na przykład:

- Filtrowanie reklam przez AdGuard Home
- Włączenie klienta VPN
- Korzystanie z szyfrowanego DNS

Drop-in Gateway działa jako pośredni system sieciowy: kieruje ruch urządzeń klienckich przez router GL.iNet w celu przetworzenia, zanim zostanie on przesłany przez główny router. Zachowuje istniejące ustawienia sieci, zapewniając ciągłość połączeń wszystkich urządzeń, a w razie potrzeby umożliwia też zarządzanie ruchem wszystkich lub wybranych klientów.



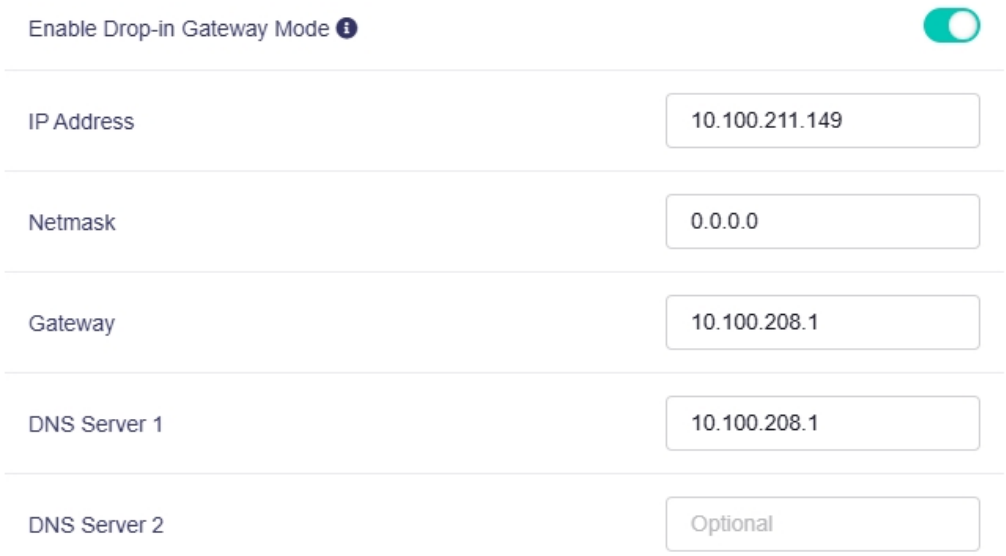
Powyższy schemat zawiera dwa rodzaje linii: szare oraz zielone z trzema strzałkami oznaczonymi numerami.

- **Szare linie** przedstawiają fizyczną topologię połączeń: urządzenia klienckie (np. komputer stacjonarny i laptop) łączą się z głównym routerem, a jego port LAN jest połączony kablem Ethernet z portem WAN routera GL.iNet z włączonym Drop-in Gateway.
- **Zielone linie** przedstawiają kolejne etapy transmisji danych przy aktywnym Drop-in Gateway. Ponumerowane strzałki wskazują kolejność przepływu ruchu:
  1. Ruch urządzeń klienckich jest najpierw kierowany do głównego routera;

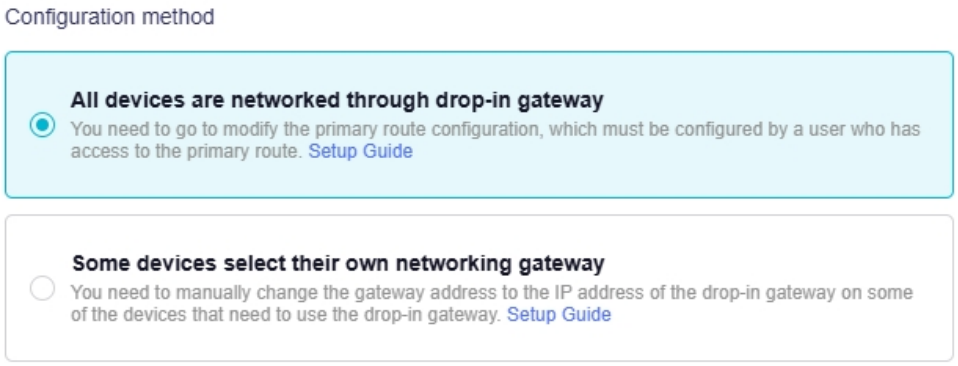
2. Główny router przekazuje ruch do routera GL.iNet w celu przetworzenia (np. filtrowania reklam, szyfrowania VPN);
3. Po przetworzeniu ruch wraca do głównego routera, który dostarcza dane do pierwotnych urządzeń klienckich lub kieruje je do Internetu.

Aby w razie potrzeby włączyć Drop-in Gateway, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Drop-in Gateway**. Włącz **Enable Drop-in Gateway Mode** i sprawdź parametry sieci.



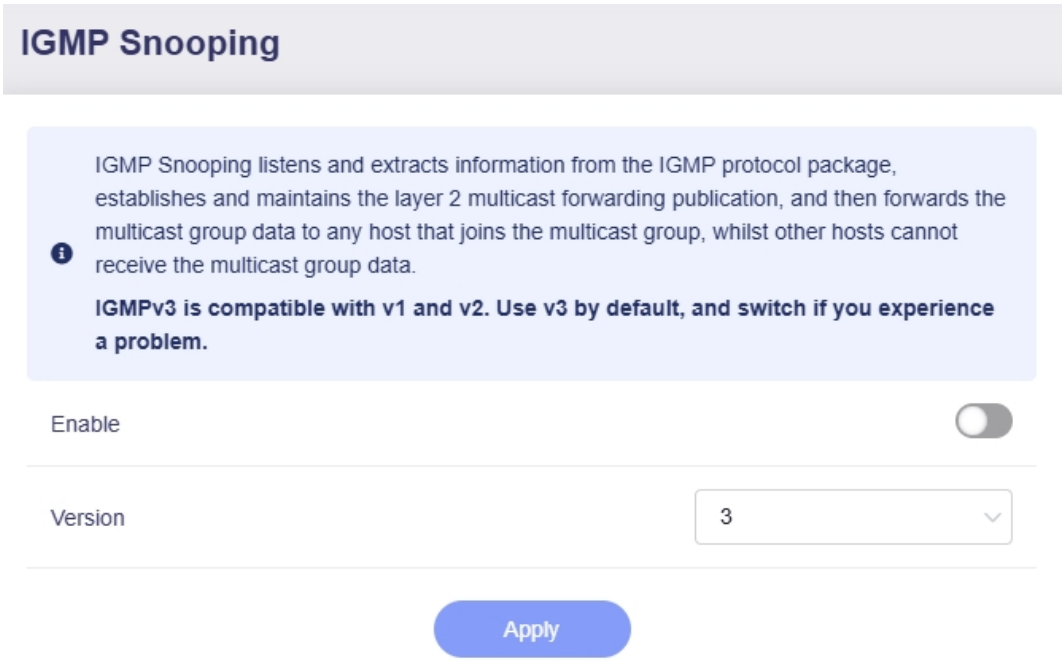
2. Wybierz sposób konfiguracji i kliknij **Apply**. Szczegóły znajdziesz w tym poradniku.



14.10 IGMP Snooping

IGMP Snooping nasłuchuje pakietów protokołu IGMP, wyodrębnia odpowiednie informacje oraz tworzy i utrzymuje tablicę przekazywania ruchu multicast w warstwie 2. Następnie przekazuje dane grupy multicast do hostów należących do tej grupy. Pozostałe hosty nie otrzymują tych danych.

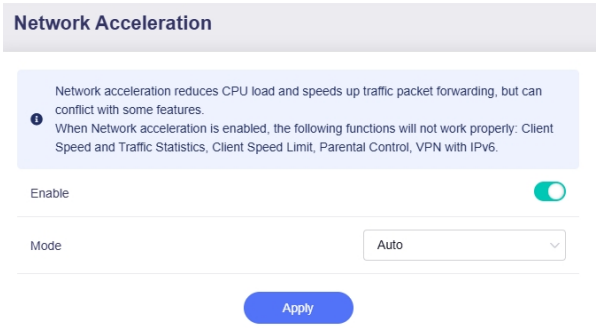
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IGMP Snooping**. W razie potrzeby włącz tę opcję, aby korzystać z multicastu na routerze.



14.11 Przyspieszanie sieci

Przyspieszanie sieci zmniejsza obciążenie procesora i przyspiesza przekazywanie pakietów, ale może kolidować z niektórymi funkcjami.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Network Acceleration**. Możesz tu włączyć przyspieszanie sieci i wybrać tryb: Auto, Hardware Acceleration lub Software Acceleration.

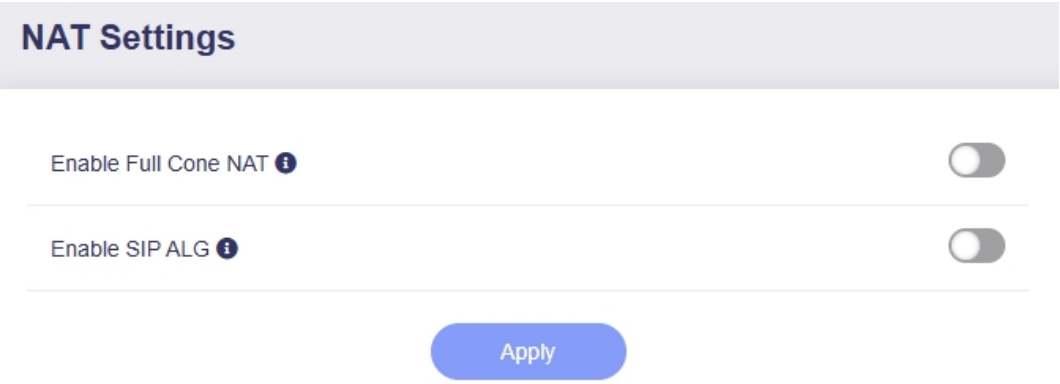


- **Auto**: automatycznie przełącza między dwoma trybami przyspieszania w zależności od sposobu użytkowania.
- **Hardware Acceleration**: przenosi często wykonywane zadania sieciowe (np. NAT, przekazywanie pakietów i weryfikację sum kontrolnych) do wyspecjalizowanego sprzętu, takiego jak procesory NPU lub układy HWNAT. Działa w połączeniach Ethernet i Repeater. W takich zastosowaniach, ze stałymi ścieżkami i prostymi regułami, zapewnia wysoką przepustowość, małe opóźnienia i minimalne obciążenie procesora przy transmisji z pełną prędkością łącza.
- **Software Acceleration**: wykorzystuje ogólny procesor routera wraz ze zoptymalizowanym jądrem lub sterownikami (np. SWNAT). Działa przy dostępie komórkowym (4G/5G), który jest typowym zastosowaniem bez dostępnego przyspieszania sprzętowego. Zapewnia szeroką zgodność i obsługę złożonych protokołów. Jest elastyczny, ale przy dużej przepustowości, szczególnie z włączonymi funkcjami zaawansowanymi, wydajność procesora może ograniczać szybkość transmisji.

Uwaga: po włączeniu przyspieszania sieci następujące funkcje nie działają prawidłowo: statystyki prędkości klientów, statystyki ruchu, ograniczanie prędkości, kontrola rodzicielska i VPN z IPv6.

14.12 Ustawienia NAT

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **NAT Settings**. Tutaj możesz skonfigurować dwie główne funkcje NAT: Full Cone NAT i SIP ALG.



- **Full Cone NAT**: może zmniejszać opóźnienia i poprawiać szybkość reakcji w grach sieciowych. Włączenie może jednak obniżyć bezpieczeństwo, ponieważ zezwala na nieograniczone połączenia przychodzące.
- **SIP ALG**: ma ograniczać wpływ wielu translacji NAT na ruch SIP (Session Initiation Protocol). W większości przypadków nie pomaga, a może nawet zakłócać połączenia VoIP, powodując jednostronny dźwięk, brak dzwonka telefonu, nieoczekiwane rozłączenia lub przekierowanie połączeń bezpośrednio do poczty głosowej.

Rozdział 15

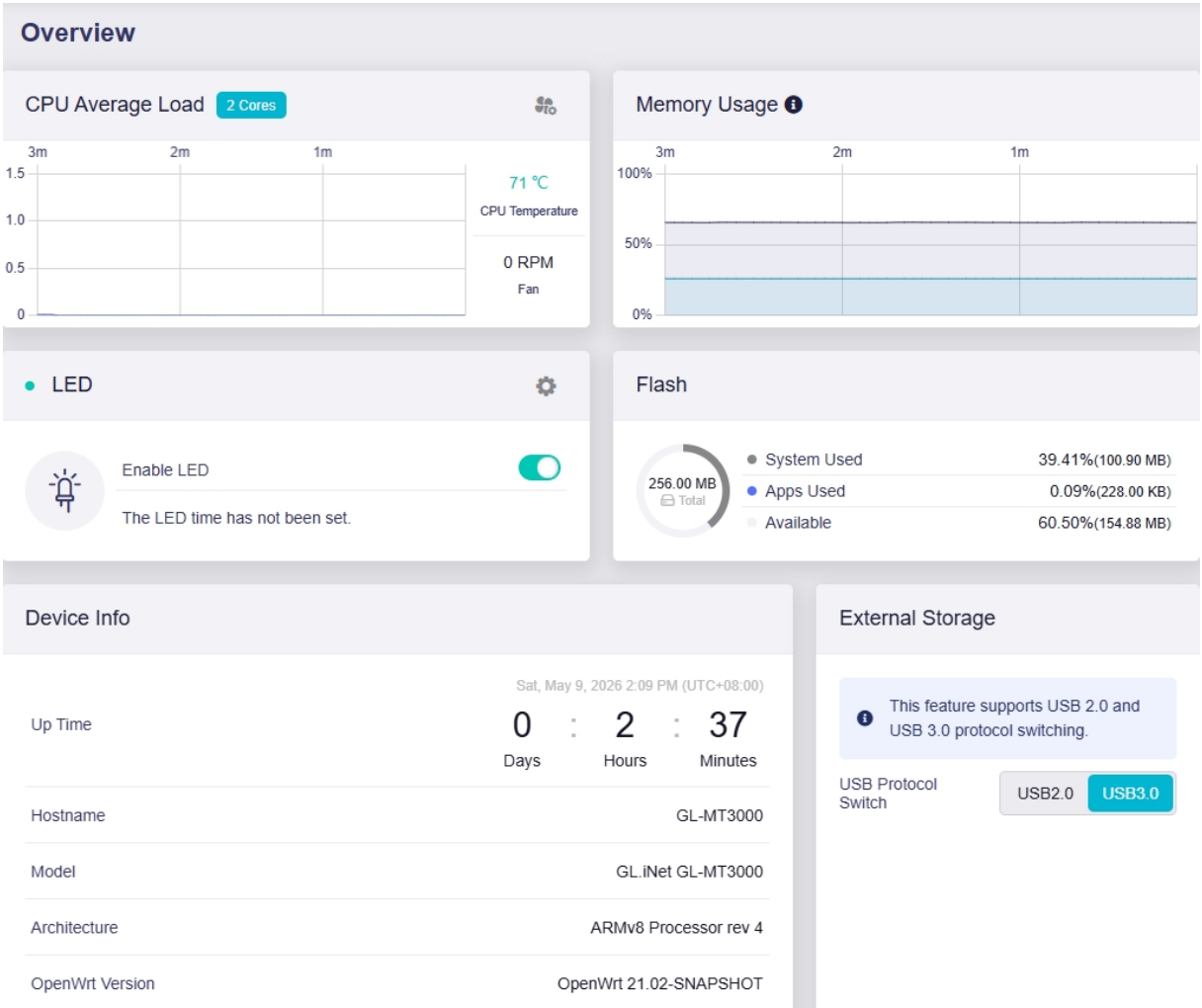
System

W tym rozdziale opisano narzędzia zarządzania urządzeniem: przegląd systemu, aktualizacje, zadania zaplanowane, strefę czasową, dziennik, resetowanie oprogramowania i ustawienia zaawansowane.

15.1 Przegląd

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Overview**. Strona wyświetla stan sprzętu i udostępnia proste funkcje sterowania, w tym:

- Stan procesora, pamięci RAM i pamięci flash
- Sterowanie diodą LED
- Informacje o urządzeniu
- Przełączanie protokołu pamięci zewnętrznej

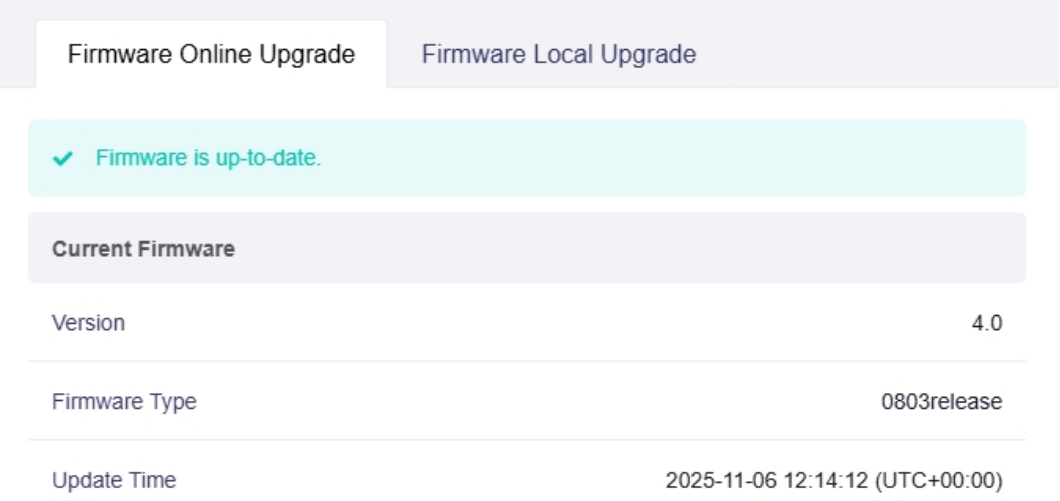


15.2 Aktualizacja

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Upgrade**. Oprogramowanie routera można aktualizować online lub lokalnie.

15.2.1 Aktualizacja oprogramowania sprzętowego online

Tutaj znajdziesz szczegóły bieżącego oprogramowania, w tym wersję, typ (np. wydanie stabilne, beta) i czas aktualizacji. Jeśli router ma połączenie z Internetem, sprawdzi dostępność nowszej wersji do pobrania.

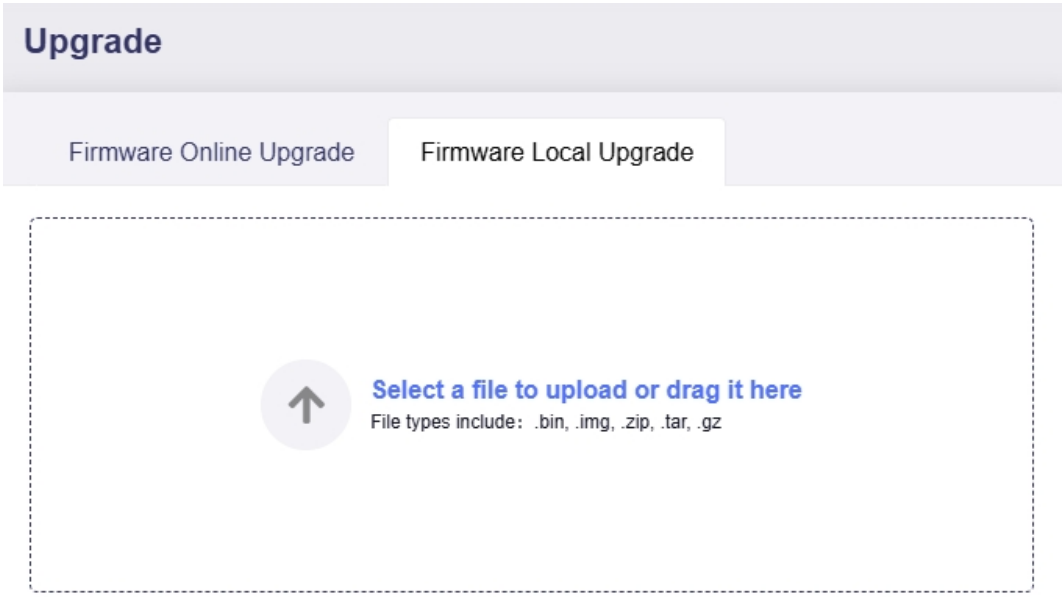


Wskazówka: jeśli podczas aktualizacji online pojawi się komunikat **Download Failed**, przejdź do **SYSTEM** -> **Time Zone** i popraw błąd strefy czasowej (zsynchronizuj z przeglądarką).

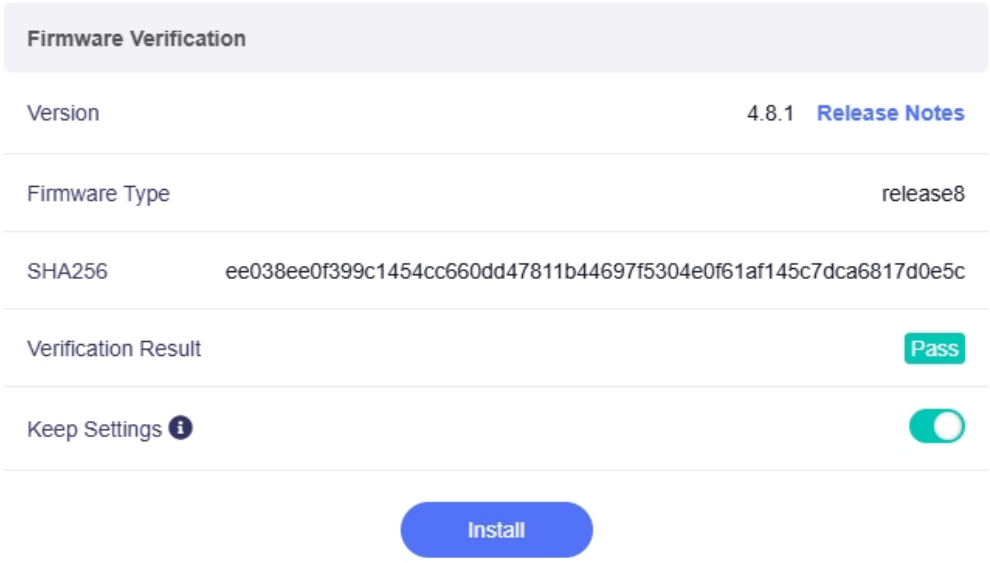
15.2.2 Lokalna aktualizacja oprogramowania sprzętowego

Aktualizacja lokalna nie wymaga połączenia routera z Internetem.

Pobierz właściwy pakiet oprogramowania dla swojego modelu routera z oficjalnego Centrum pobierania na urządzenie lokalne. Następnie zaloguj się do panelu administracyjnego routera, przejdź do sekcji **SYSTEM** > **Upgrade** > **Local Upgrade** i prześlij pakiet oprogramowania.



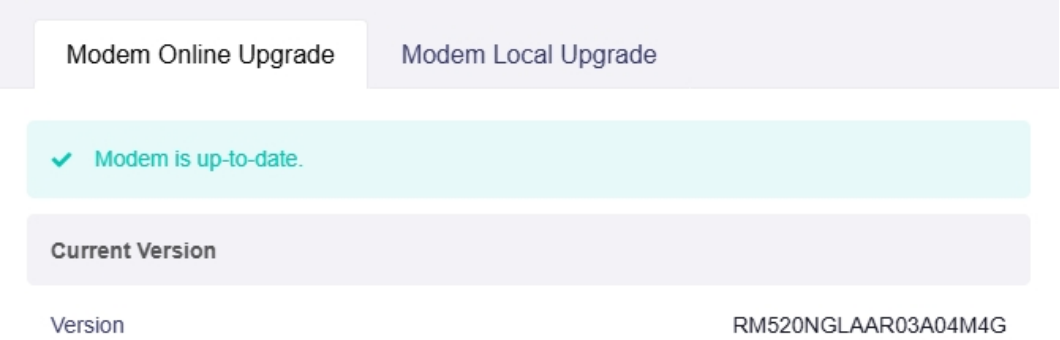
Na stronie pojawią się szczegóły oprogramowania. Sprawdź je przed kliknięciem **Install**.



- **Keep Settings**: po włączeniu bieżące ustawienia zostają zachowane. Pakiety zainstalowane ręcznie trzeba jednak zainstalować ponownie po zakończeniu aktualizacji. Nie włączaj tej opcji podczas instalowania starszej wersji oprogramowania.

15.2.3 Aktualizacja modemu online

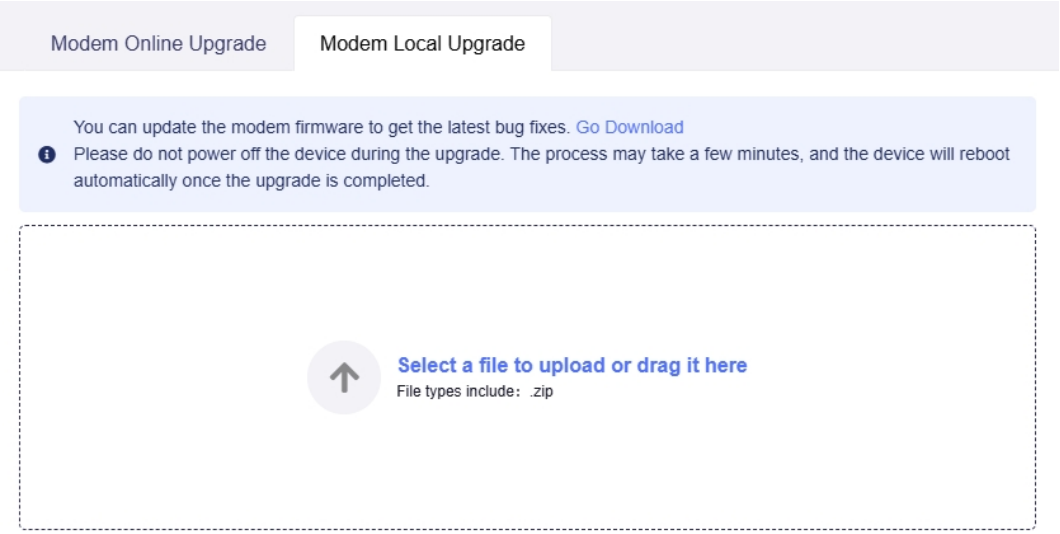
Routery komórkowe GL.iNet umożliwiają wyświetlanie i aktualizowanie oprogramowania sprzętowego modemu komórkowego w internetowym panelu administracyjnym.
W tym miejscu możesz sprawdzić bieżącą wersję modemu komórkowego. Jeśli router jest połączony z Internetem, automatycznie sprawdzi dostępność najnowszej wersji oprogramowania modemu na serwerze producenta, co upraszcza aktualizację.



15.2.4 Lokalna aktualizacja modemu

Jeśli połączenie komórkowe nie działa lub jest niestabilne, możesz spróbować zaktualizować moduł komórkowy. Zalecamy skontaktowanie się z pomocą techniczną w celu rozwiązania problemu przed aktualizacją modemu.

W razie potrzeby ręcznie prześlij plik oprogramowania sprzętowego modemu, aby zaktualizować modem komórkowy.



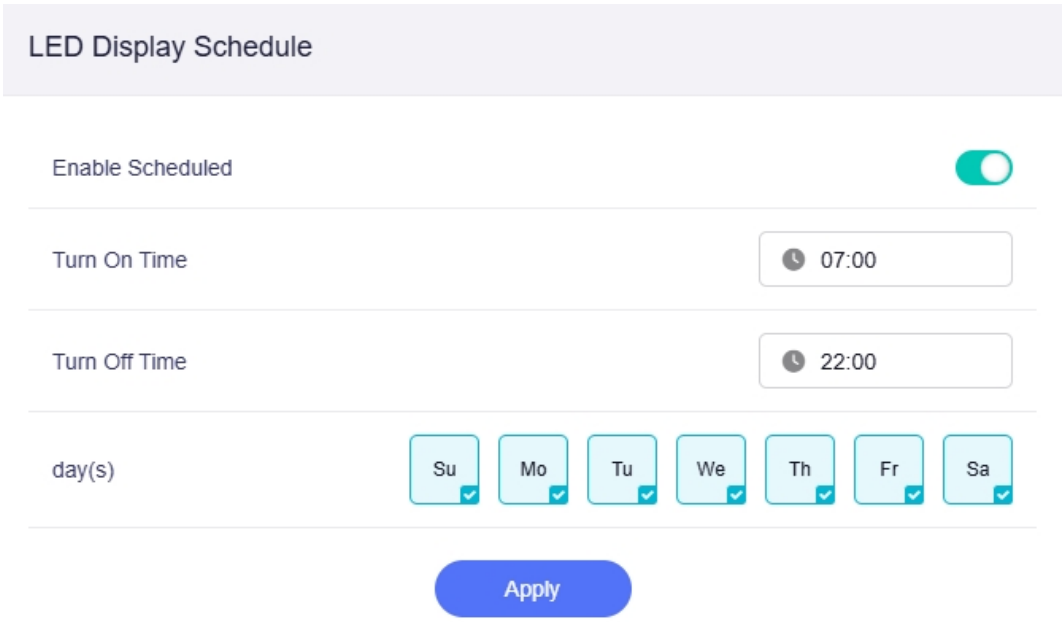
15.3 Zadania zaplanowane

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Scheduled Tasks**. Tutaj możesz ustawić codzienny harmonogram podstawowych czynności, takich jak włączanie i wyłączanie diody LED oraz ponowne uruchamianie routera.

Uwaga: przed użyciem tej funkcji zsynchronizuj czas w Time Zone. Jeśli urządzenie będzie wyłączone w zaplanowanym terminie, zadanie nie zostanie wykonane.

15.3.1 Harmonogram diody LED

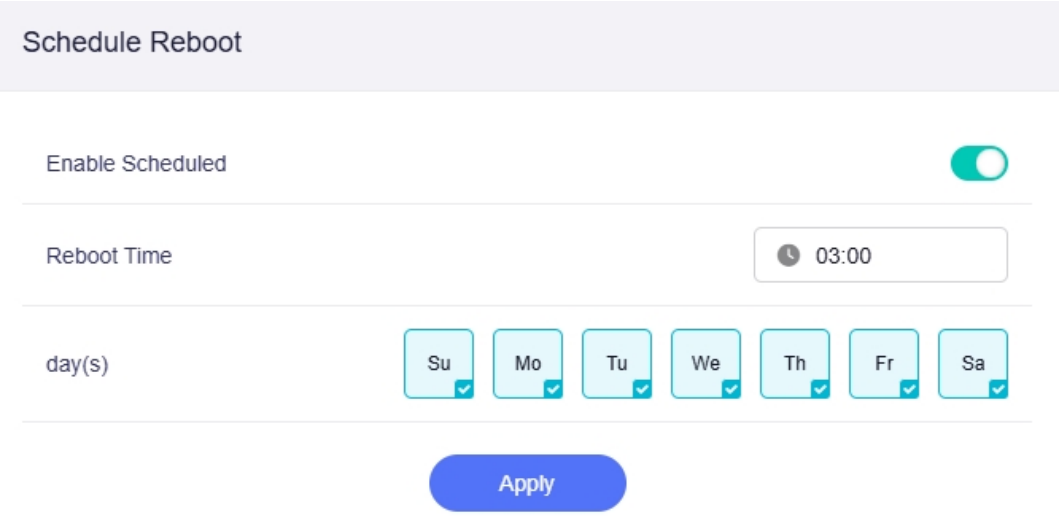
W razie potrzeby ustaw harmonogram diody LED routera i kliknij **Apply**.



- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram diody LED.
- **Turn On Time**: ustaw godzinę włączenia diody LED (np. 07:00).
- **Turn Off Time**: ustaw godzinę wyłączenia diody LED (np. 22:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

15.3.2 Harmonogram ponownego uruchamiania

W razie potrzeby ustaw harmonogram automatycznego ponownego uruchamiania routera i kliknij **Apply**.



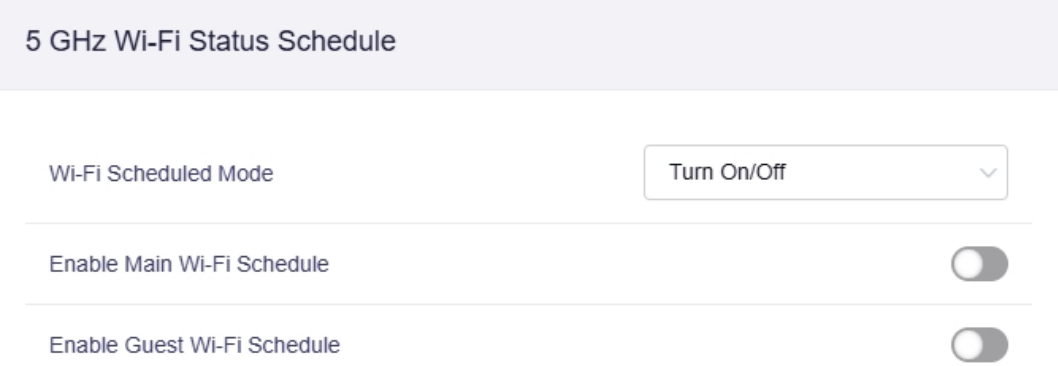
- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram ponownego uruchamiania.
- **Reboot Time**: ustaw konkretną godzinę ponownego uruchomienia routera (np. 03:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

15.3.3 Harmonogram Wi-Fi 5 GHz

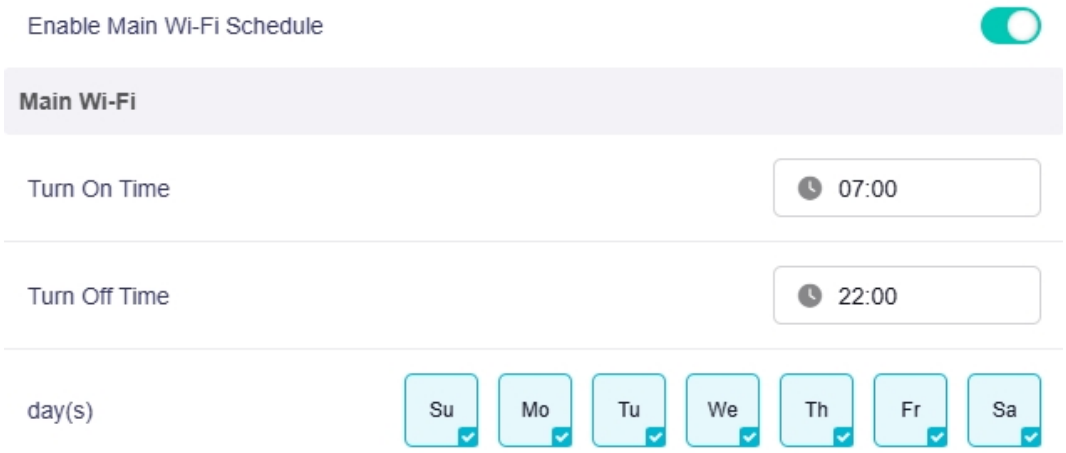
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 5 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

Tryb 1: włączanie i wyłączanie (Turn On/Off)

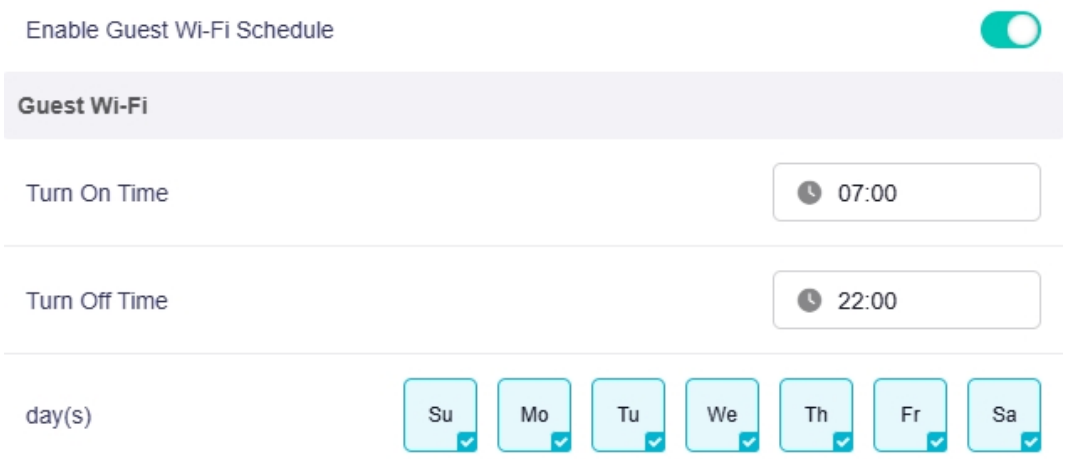
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 5 GHz.



- **Main Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania głównej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

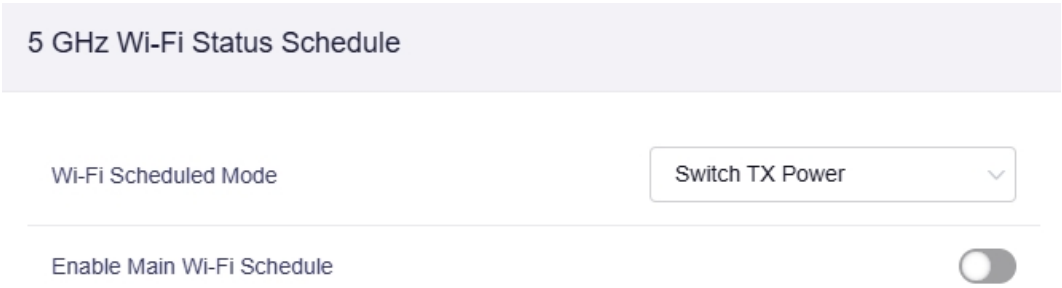


- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

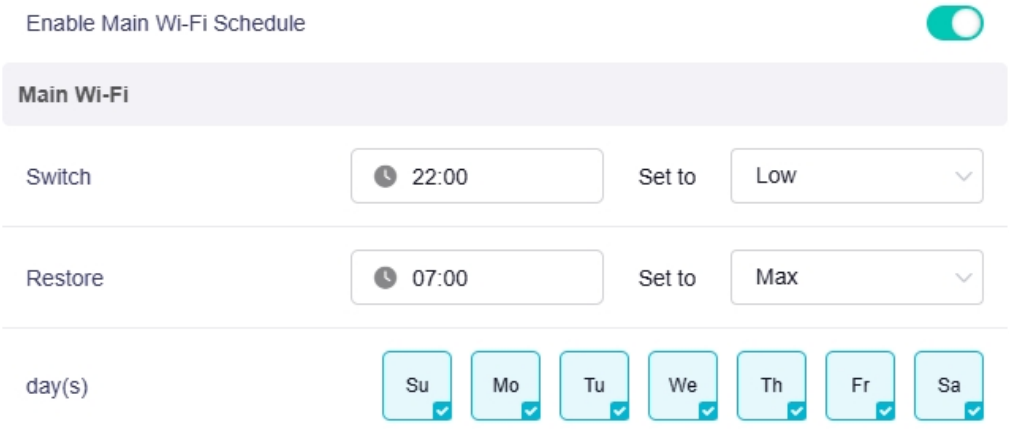


Tryb 2: przełączanie mocy nadawania (Switch TX Power)

Możesz włączyć harmonogram przełączania mocy nadawania głównej sieci Wi-Fi 5 GHz.



Po włączeniu ustaw dwie zaplanowane czynności zmiany mocy nadawania głównej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których obowiązują.



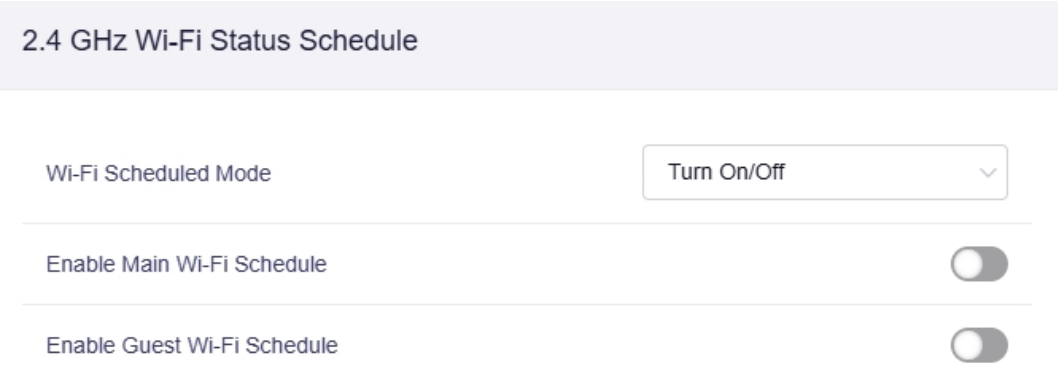
- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

15.3.4 Harmonogram Wi-Fi 2,4 GHz

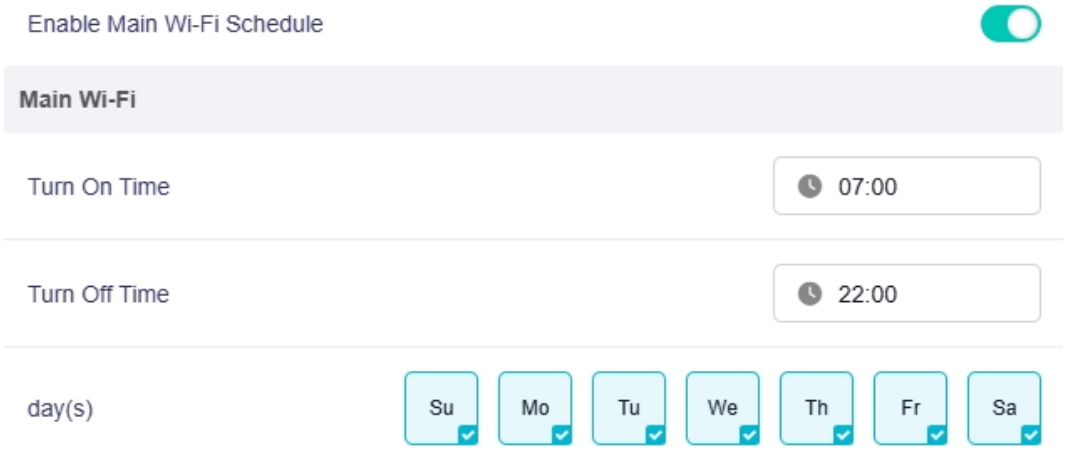
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 2,4 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

Tryb 1: włączanie i wyłączanie (Turn On/Off)

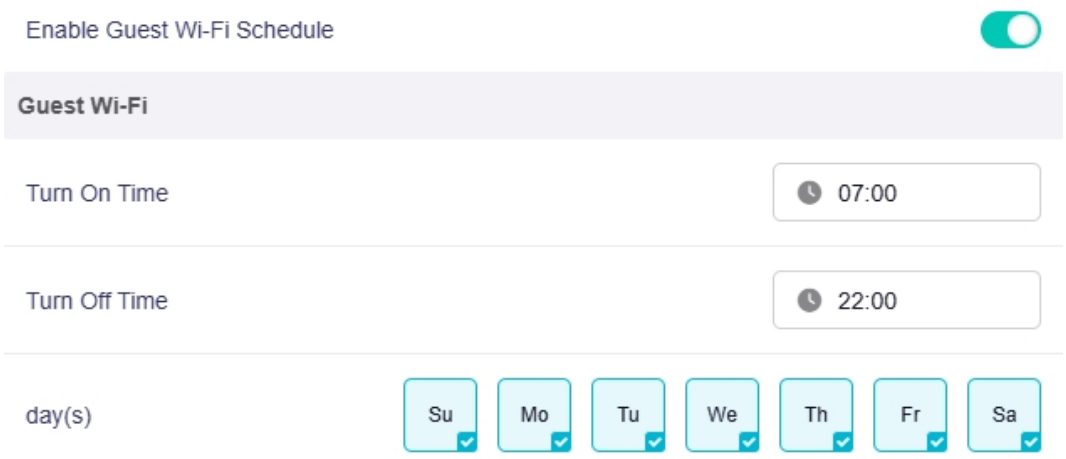
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 2,4 GHz.



- **Main Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

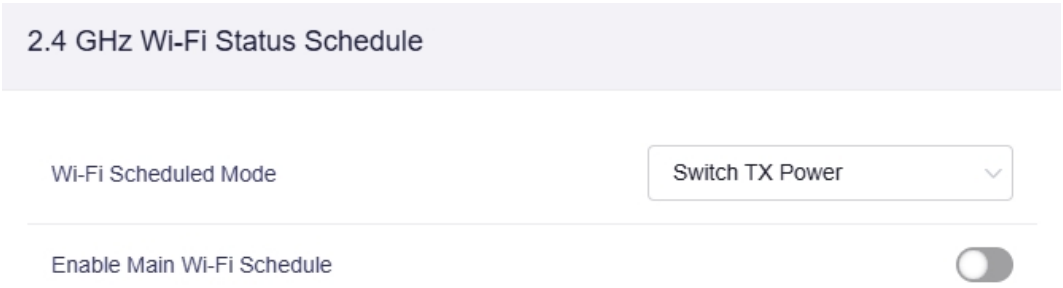


- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

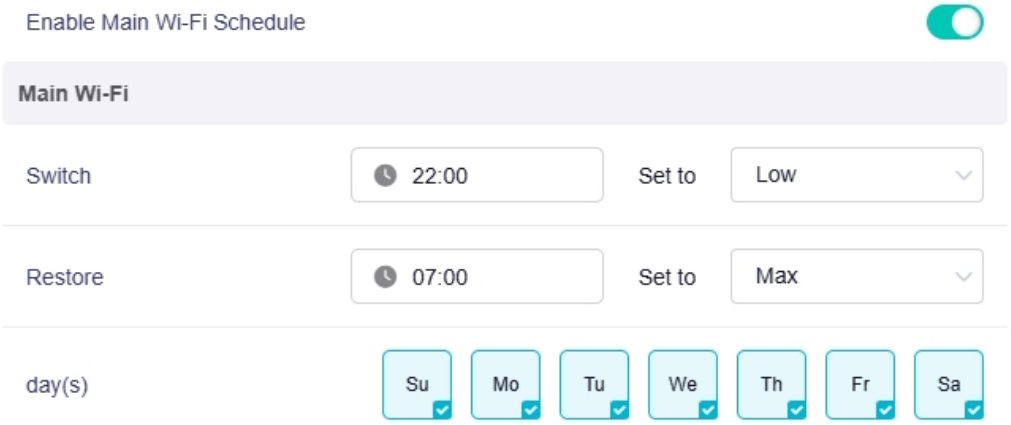


Tryb 2: przełączanie mocy nadawania (Switch TX Power)

Możesz włączyć harmonogram przełączania mocy nadawania głównej sieci Wi-Fi 2,4 GHz.



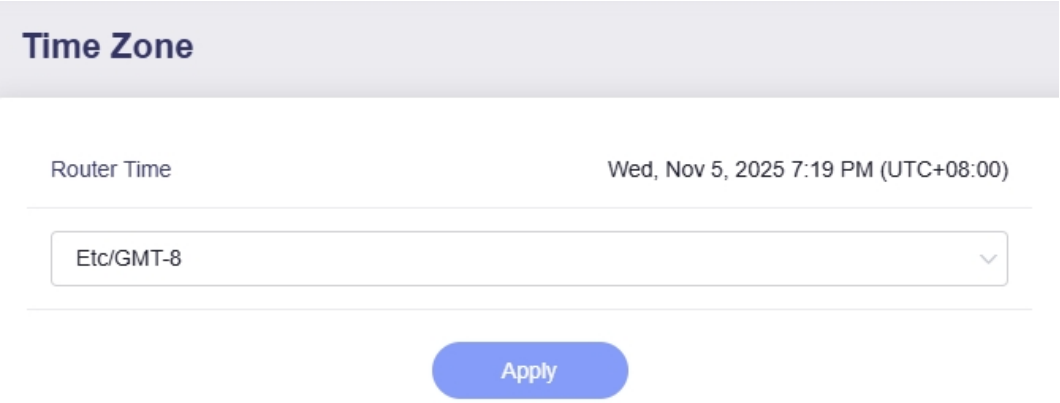
Po włączeniu ustaw dwie zaplanowane czynności zmiany mocy nadawania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których obowiązują.



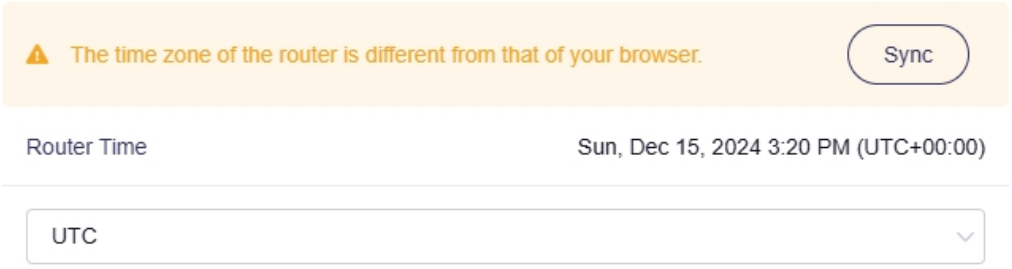
- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

15.4 Strefa czasowa

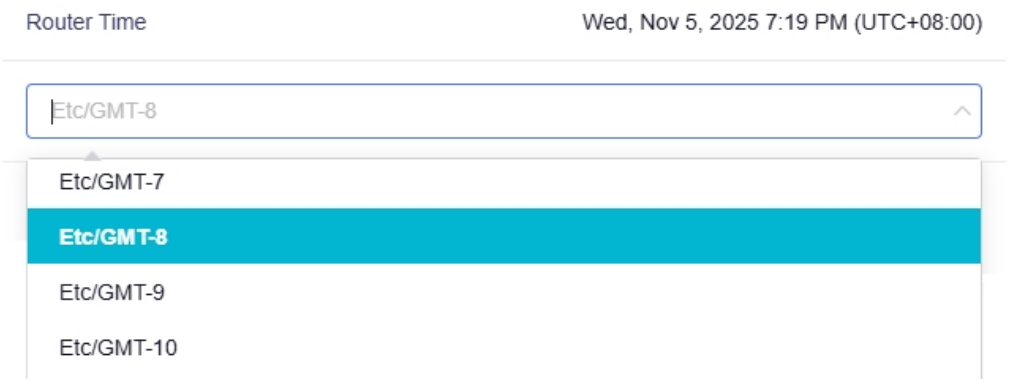
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Time Zone**. Strona wyświetla czas systemowy routera: datę, godzinę i odpowiadające im przesunięcie strefy czasowej.



Niektóre funkcje zależą od czasu systemowego routera. Upewnij się, że właściwa strefa czasowa jest prawidłowo zsynchronizowana. Jeśli strefa routera różni się od strefy przeglądarki, pojawi się poniższy komunikat. Kliknij przycisk **Sync**, aby zsynchronizować strefę czasową.

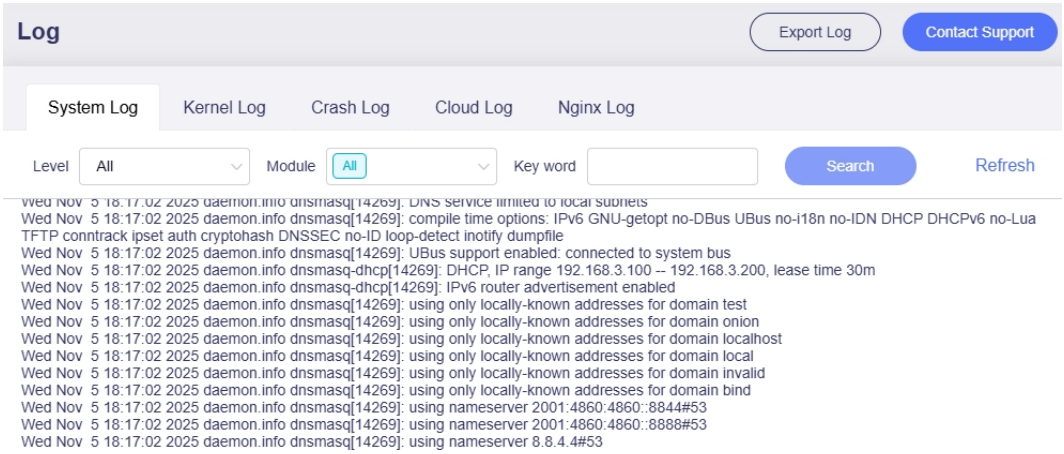


Aby zmienić strefę czasową, wybierz odpowiednią pozycję z listy, tak aby czas systemowy routera odpowiadał czasowi lokalnemu.

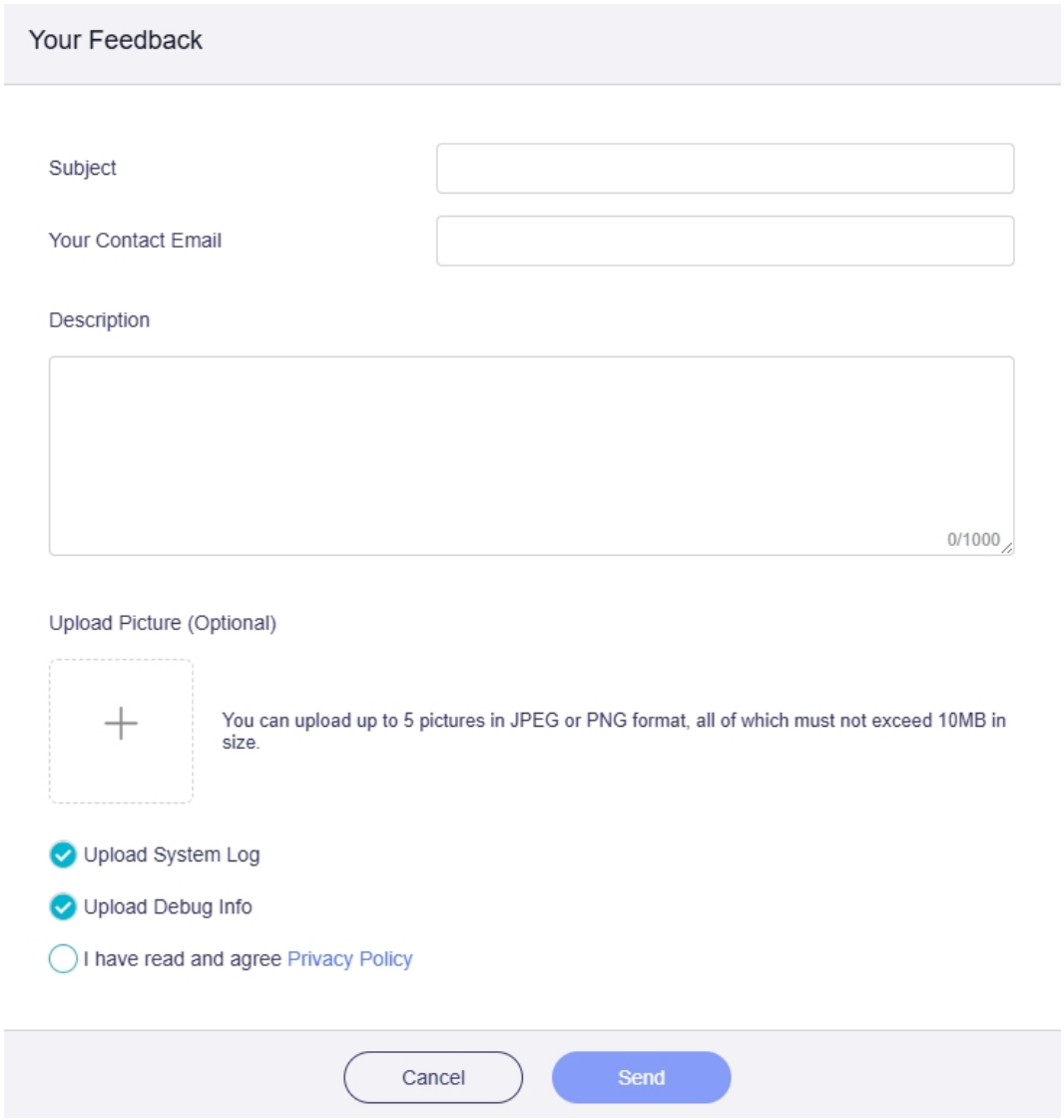


15.5 Dziennik

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Log**. Tutaj możesz przeglądać dzienniki System, Kernel, Crash, Cloud i Nginx na potrzeby analizy i rozwiązywania problemów.



- **Search**: strona dziennika systemowego umożliwia filtrowanie w celu szybkiego wyszukiwania. Możesz wybrać z listy poziom dziennika (np. all, info, error) lub moduł (np. IPv6, Tethering, Cellular) albo wprowadzić słowa kluczowe, aby szybko przeszukać dzienniki.
- **Refresh**: kliknij ten przycisk, aby odświeżyć dzienniki.
- **Export Log**: kliknij ten przycisk, aby wyeksportować informacje diagnostyczne wraz z dziennikami.
- **Contact Support**: kliknij ten przycisk, wypełnij szczegółowe informacje w wyskakującym oknie po prawej stronie, a następnie kliknij **Send**. Twoja wiadomość zostanie wysłana bezpośrednio do pomocy technicznej GL.iNet.


Your Feedback
Subject
Your Contact Email
Description
0/1000
Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

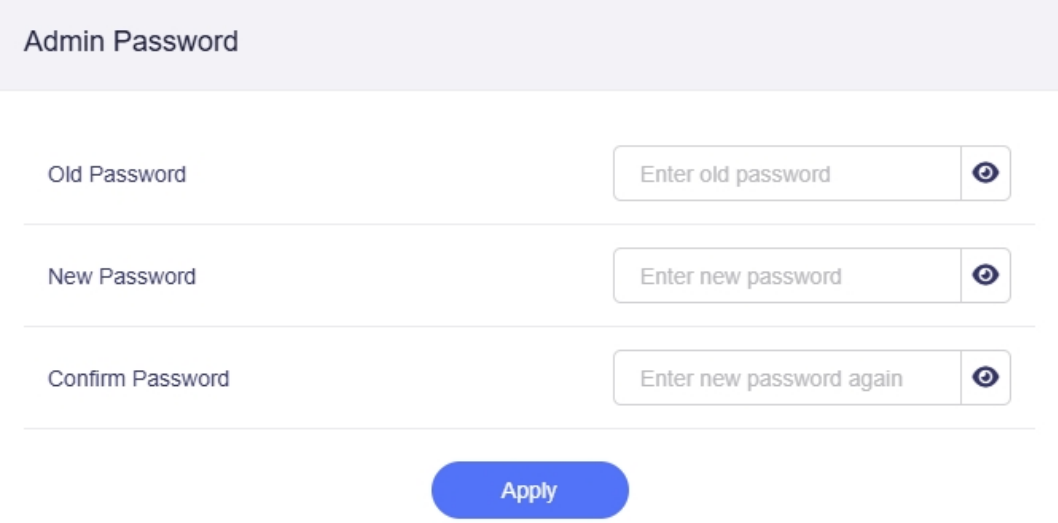
15.6 Bezpieczeństwo

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Security**. Strona zawiera opcje konfiguracji zarządzania lokalnego i zdalnego, w tym:

- Hasło administratora
- Lokalny dostęp do panelu administracyjnego, LuCI i SSH
- Zdalny dostęp przez HTTPS/SSH
- Otwieranie portów routera

15.6.1 Hasło administratora

W tej sekcji możesz zmienić hasło logowania do panelu administracyjnego.

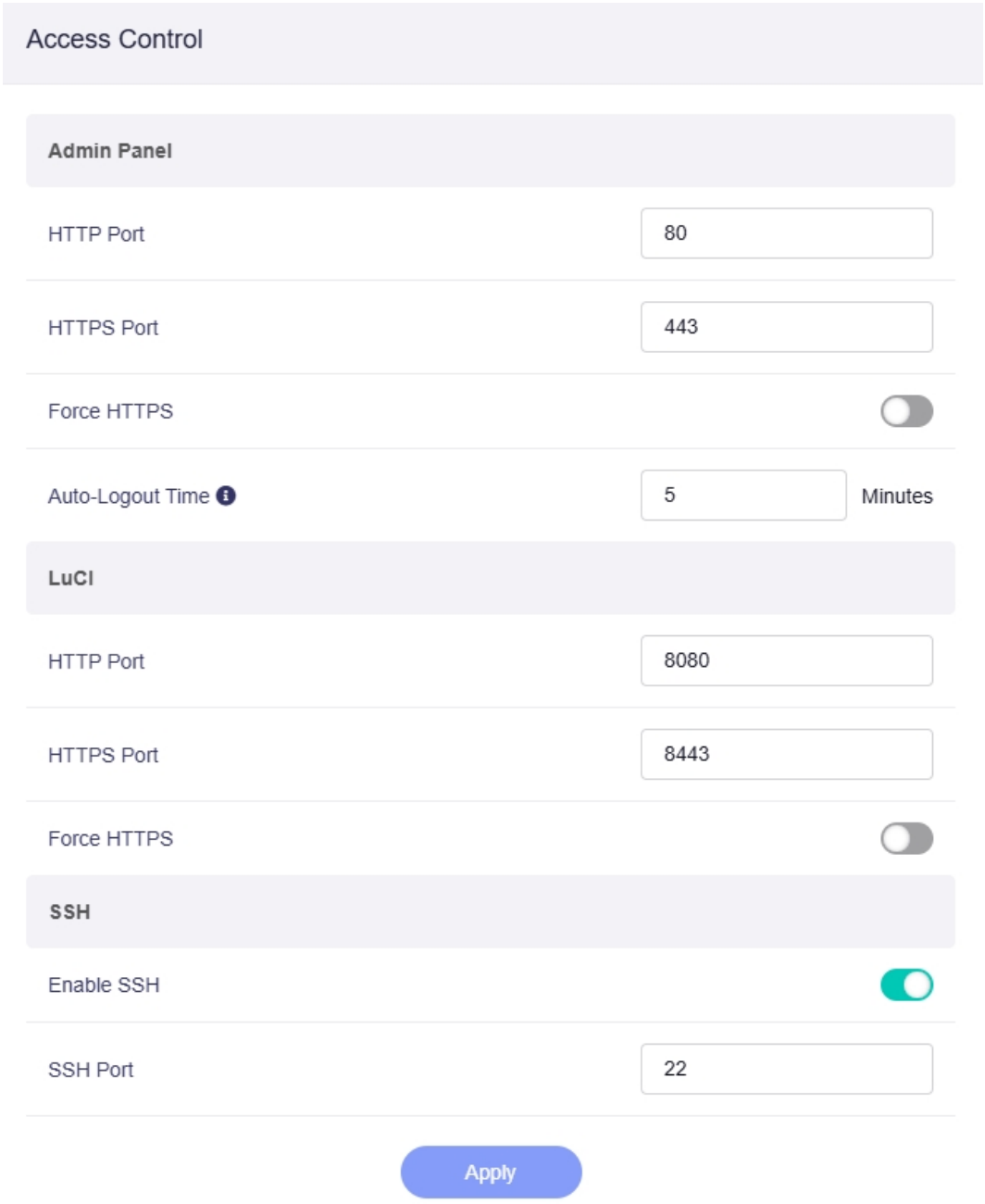


Wymagania dotyczące hasła administratora:

1. Długość od 10 do 63 znaków.
2. Dozwolone są litery (z rozróżnianiem wielkości), cyfry i symbole (np. ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Wymagane są co najmniej dwa rodzaje znaków spośród: wielkie litery, małe litery, cyfry i symbole.

15.6.2 Kontrola dostępu

Ta sekcja zarządza dostępem do różnych interfejsów routera (panel administracyjny, LuCI i SSH). Pozwala zapobiegać skanowaniu i próbom włamania na domyślnym porcie oraz unikać problemów sieciowych spowodowanych konfliktami portów.



Panel administracyjny

- **HTTP Port**: domyślnie 80; służy do nieszyfrowanego dostępu HTTP do panelu administracyjnego.

- **HTTPS Port**: domyślnie 443; służy do bezpiecznego dostępu HTTPS do panelu administracyjnego.
- **Force HTTPS**: po włączeniu wymusza używanie bezpiecznego połączenia HTTPS przy dostępie do panelu administracyjnego.
- **Auto-Logout Time**: domyślnie 5 minut. Ze względów bezpieczeństwa po tym czasie bezczynne sesje administratora są automatycznie wylogowywane. Możesz ustawić czas od 1 minuty do 3 godzin.

LuCI

Uwaga: przed skonfigurowaniem kontroli dostępu do LuCI zainstaluj go w Advanced Settings.

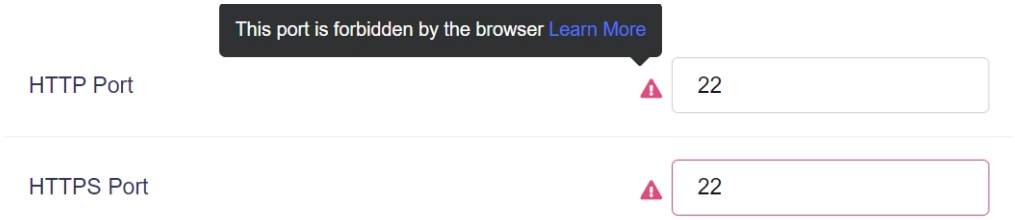
- **HTTP Port**: domyślnie 8080; służy do nieszyfrowanego dostępu HTTP do interfejsu LuCI.
- **HTTPS Port**: domyślnie 8443; służy do bezpiecznego dostępu HTTPS do interfejsu LuCI.
- **Force HTTPS**: po włączeniu wymusza bezpieczne połączenie HTTPS z interfejsem LuCI.

SSH

- **Enable SSH**: domyślnie włączone; określa, czy dozwolony jest dostęp do routera przez SSH.
- **SSH Port**: domyślnie 22; port dostępu SSH do routera.

Uwaga:

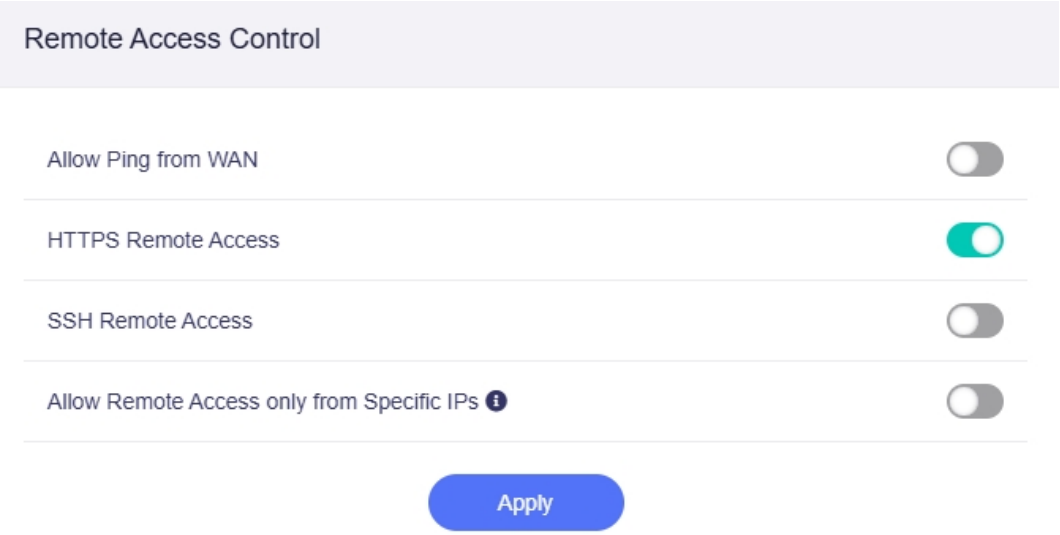
1. Jeśli przypiszesz numer kolidujący z portem zastrzeżonym (lub zarezerwowanym dla określonych usług przez przeglądarki albo konwencje sieciowe), pojawi się komunikat „This port is forbidden by the browser”.



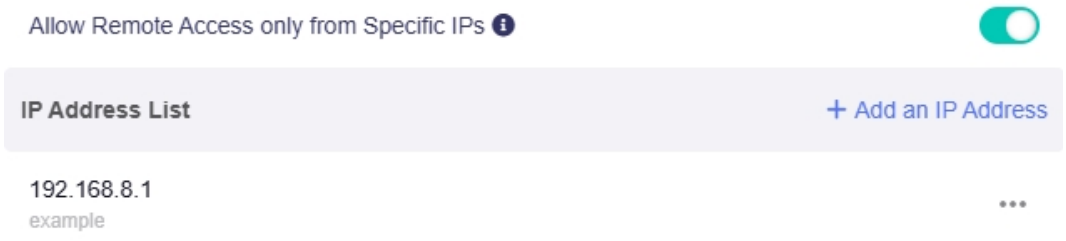
2. Po zmianie numeru portu w oprogramowaniu trzeba podawać prawidłowy numer, aby otworzyć panel administracyjny. Jeśli zapomnisz numeru, zresetuj router, aby przywrócić port domyślny.
3. Ustawienia dostępu do LuCI są dostępne dopiero po jego zainstalowaniu. Jeśli ich nie widać, przejdź do **SYSTEM** > **Advanced Settings**, aby zainstalować LuCI.

15.6.3 Kontrola dostępu zdalnego

Ta sekcja zarządza zdalnym dostępem do interfejsów routera, w tym HTTPS, SSH i ping od strony WAN. Pozwala też ograniczyć dostęp do określonych adresów IP, zachowując równowagę między dostępnością zdalną a bezpieczeństwem sieci.

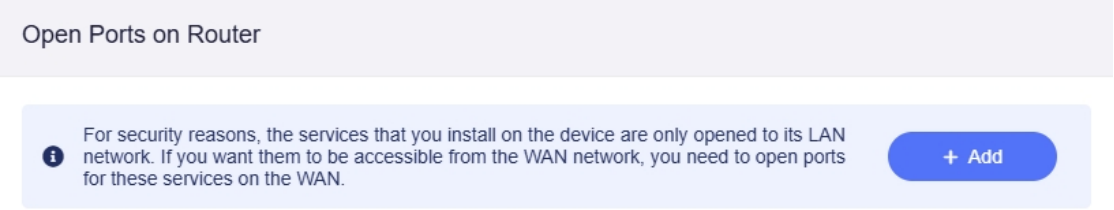


- **Allow Ping from WAN**: zezwolenie na ping od strony WAN pomaga sprawdzić dostępność routera przez WAN w razie problemów z siecią oraz określić opóźnienie i utratę pakietów.
- **HTTPS Remote Access**: umożliwia bezpieczny zdalny dostęp do panelu administracyjnego przez HTTPS. Zapewnia szyfrowaną transmisję danych podczas zdalnego zarządzania routerem w przeglądarce.
- **SSH Remote Access**: umożliwia bezpieczny dostęp do terminala routera. Pozwala zdalnie zarządzać routerem przez SSH za pomocą zaszyfrowanego tunelu.
- **Allow Remote Access from Specific IPs**: funkcja jest dostępna tylko po włączeniu co najmniej jednej z powyższych trzech opcji. Możesz dodać wiele określonych adresów IP, aby zdalnie zarządzać routerem wyłącznie z urządzeń o tych adresach.

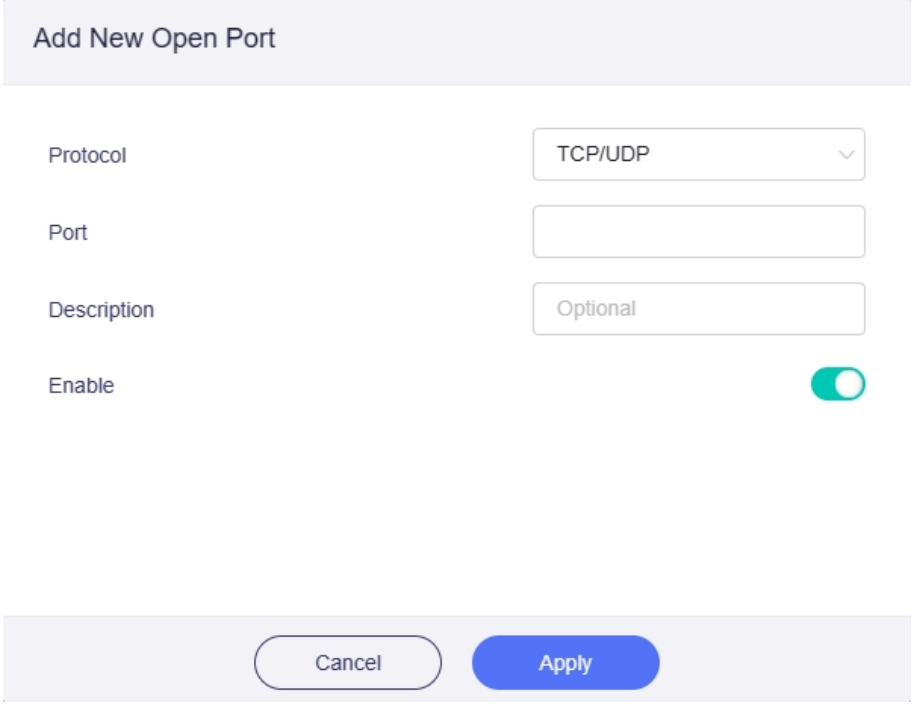


15.6.4 Otwieranie portów routera

Ta sekcja zarządza przekierowaniem portów dla usług routera. Niektóre usługi, np. WWW i FTP, wymagają otwarcia odpowiednich portów routera, aby były publicznie dostępne z sieci WAN. Ze względów bezpieczeństwa usługi zainstalowane na urządzeniu są domyślnie dostępne tylko w sieci LAN. Jeśli potrzebujesz dostępu z WAN, możesz otworzyć tutaj określone porty.



Aby otworzyć port, kliknij **Add** i wprowadź wymagane informacje w wyskakującym oknie.

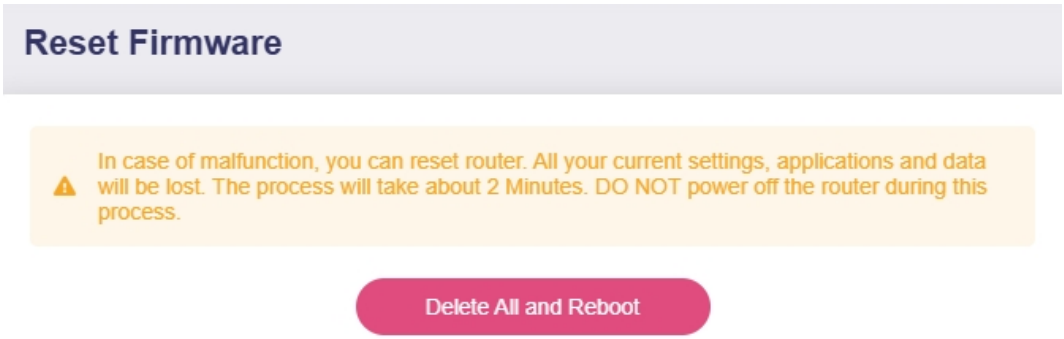


- **Protocol**: wybierz protokół sieciowy portu (TCP, UDP lub TCP/UDP). Określa on sposób przesyłania danych dla usługi powiązanej z portem.
- **Port**: wprowadź numer portu, który chcesz otworzyć.
- **Description** (opcjonalnie): dodaj krótką informację opisującą przeznaczenie otwartego portu (np. „Serwer WWW” lub „Usługa FTP”), aby ułatwić zarządzanie.
- **Enable**: użyj tego przełącznika, aby włączyć lub wyłączyć regułę przekierowania portów.

15.7 Resetowanie oprogramowania

Jeśli router działa nieprawidłowo, możesz spróbować rozwiązać problem przez zresetowanie oprogramowania.

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Reset Firmware**. W razie potrzeby kliknij **Delete All and Reboot**, aby zresetować oprogramowanie.



Uwaga: wszystkie bieżące ustawienia, aplikacje i dane zostaną usunięte. Proces trwa około 2 minut. W tym czasie nie wyłączaj zasilania routera.

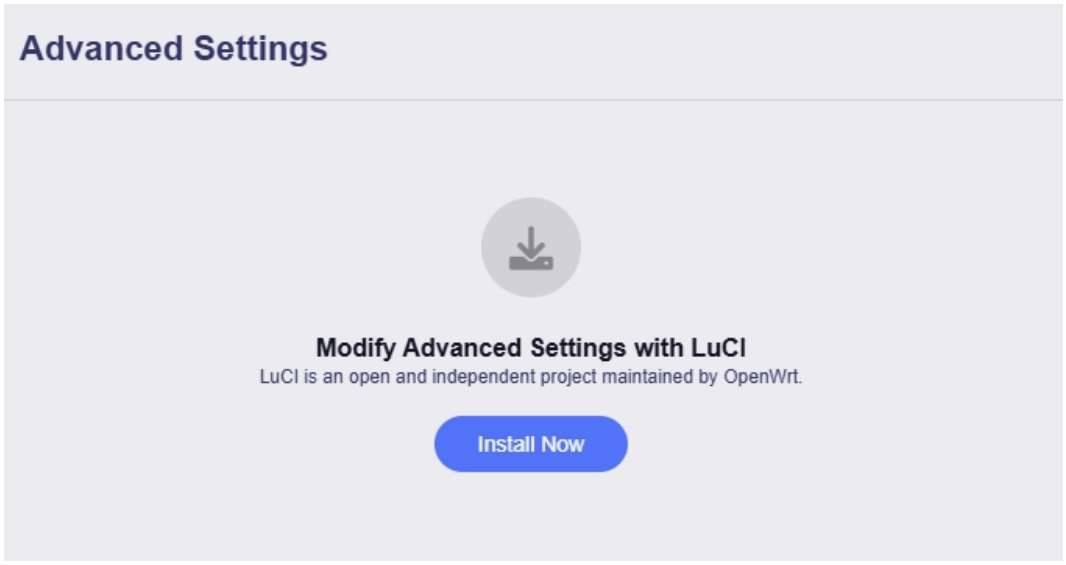
Jeśli panel administracyjny routera jest niedostępny, spróbuj zresetować router za pomocą fizycznego przycisku resetowania z boku urządzenia.

15.8 Ustawienia zaawansowane

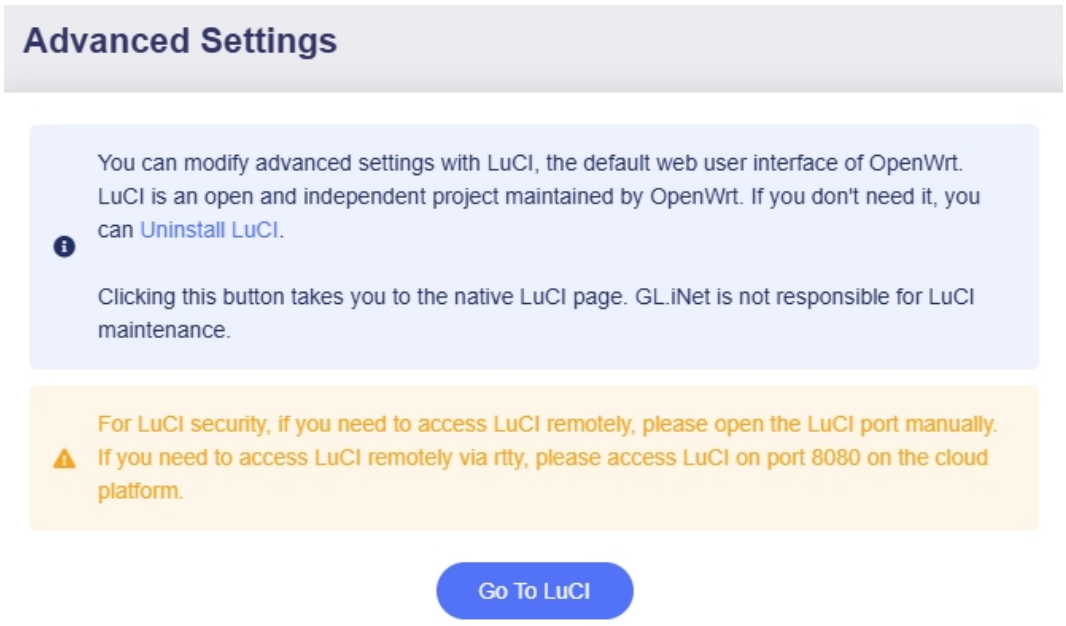
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Advanced Settings**. Tutaj możesz zmieniać ustawienia zaawansowane w LuCI, domyślnym interfejsie internetowym OpenWrt. LuCI to otwarty, niezależny projekt utrzymywany przez OpenWrt, udostępniany w obecnej postaci. GL.iNet nie odpowiada za jego utrzymanie.

Aby zalogować się do interfejsu LuCI, wykonaj poniższe czynności.

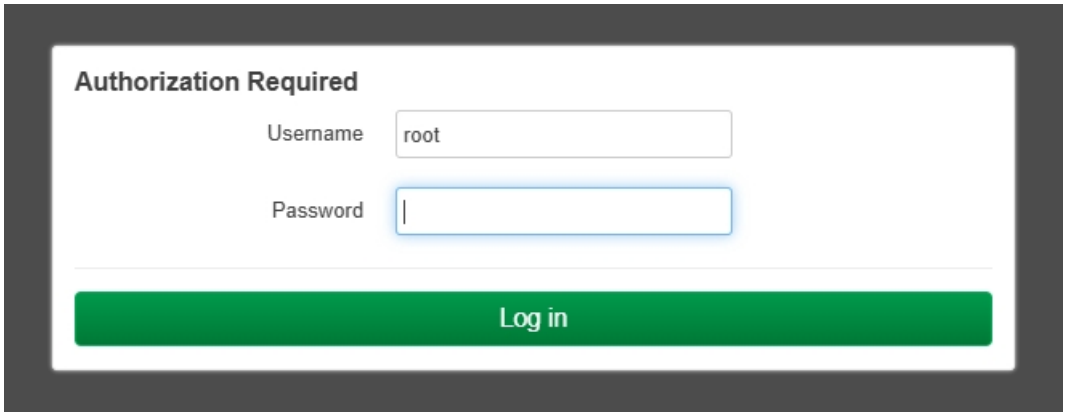
1. Kliknij **Install Now**, aby rozpocząć instalację interfejsu LuCI.



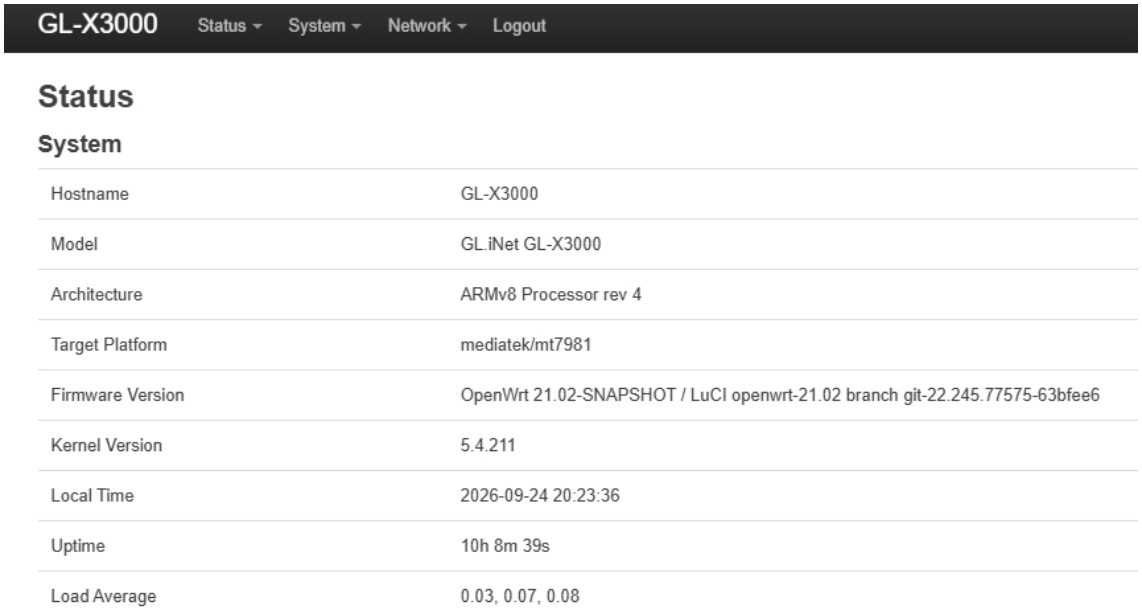
2. Kliknij **Go To LuCI**, aby przejść do strony logowania LuCI.



3. Wprowadź hasło logowania, takie samo jak do panelu administracyjnego.



Otworzy się interfejs LuCI.



Oświadczenia dotyczące zgodności z przepisami

Identyfikator FCC: 2AFIW-X3000NR | 2AFIW-X3000C16

1. To urządzenie jest zgodne z częścią 15 przepisów FCC. Jego działanie podlega następującym dwóm warunkom:
   (1) Urządzenie nie może powodować szkodliwych zakłóceń oraz
   (2) Urządzenie musi przyjmować wszelkie odbierane zakłócenia, w tym zakłócenia mogące powodować niepożądane działanie.
2. Zmiany lub modyfikacje, które nie zostały wyraźnie zatwierdzone przez stronę odpowiedzialną za zgodność, mogą spowodować utratę uprawnień użytkownika do obsługi urządzenia.
3. Uwaga: urządzenie zostało przetestowane i uznane za zgodne z limitami dla urządzeń cyfrowych klasy B zgodnie z częścią 15 przepisów FCC. Limity te mają zapewniać odpowiednią ochronę przed szkodliwymi zakłóceniami w instalacjach domowych. Urządzenie generuje, wykorzystuje i może emitować energię o częstotliwości radiowej, a jeśli nie zostanie zainstalowane i nie będzie używane zgodnie z instrukcjami, może powodować szkodliwe zakłócenia łączności radiowej. Nie ma jednak gwarancji, że zakłócenia nie wystąpią w konkretnej instalacji. Jeśli urządzenie powoduje szkodliwe zakłócenia odbioru radiowego lub telewizyjnego, co można sprawdzić przez jego wyłączenie i ponowne włączenie, zaleca się podjęcie jednej lub kilku z poniższych czynności w celu usunięcia zakłóceń:
   - Zmień kierunek lub położenie anteny odbiorczej.
   - Zwiększ odległość między urządzeniem a odbiornikiem.
   - Podłącz urządzenie do gniazda w obwodzie innym niż ten, do którego podłączony jest odbiornik.
   - Skontaktuj się ze sprzedawcą lub doświadczonym technikiem radiowo-telewizyjnym w celu uzyskania pomocy. Ważna informacja.

Oświadczenie FCC dotyczące narażenia na promieniowanie

Urządzenie spełnia limity narażenia na promieniowanie FCC określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem. Nadajnik nie może być umieszczany w tym samym miejscu ani działać razem z inną anteną lub nadajnikiem.

Oświadczenie o zgodności z przepisami kanadyjskimi

Urządzenie zawiera nadajniki lub odbiorniki niewymagające licencji, zgodne z normami RSS kanadyjskiego Ministerstwa Innowacji, Nauki i Rozwoju Gospodarczego dotyczącymi urządzeń niewymagających licencji.

Działanie podlega następującym dwóm warunkom:

(1) Urządzenie nie może powodować zakłóceń.

(2) Urządzenie musi przyjmować wszelkie zakłócenia, w tym zakłócenia mogące powodować jego niepożądane działanie.

Nadajnik lub odbiornik niewymagający licencji, zawarty w tym urządzeniu, jest zgodny z normami CNR kanadyjskiego Ministerstwa Innowacji, Nauki i Rozwoju Gospodarczego dotyczącymi urządzeń radiowych niewymagających licencji.

Działanie podlega następującym dwóm warunkom:

(1) Urządzenie nie może powodować zakłóceń.

(2) Urządzenie musi przyjmować wszelkie zakłócenia radioelektryczne, nawet jeśli mogą one zakłócać jego działanie.

Urządzenie spełnia limity narażenia na promieniowanie IC RSS-102 określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem.

Urządzenie spełnia limity narażenia na promieniowanie IC CNR-102 określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem.

Instrukcja obsługi urządzeń LE-LAN powinna zawierać wskazówki dotyczące ograniczeń wymienionych w powyższych punktach, a mianowicie:

i. Urządzenie działające w paśmie 5150–5250 MHz jest przeznaczone wyłącznie do użytku w pomieszczeniach, aby ograniczyć ryzyko szkodliwych zakłóceń systemów mobilnej łączności satelitarnej korzystających z tego samego kanału.

i. Urządzenie działające w paśmie 5150–5250 MHz jest przeznaczone wyłącznie do użytku wewnątrz pomieszczeń w celu ograniczenia ryzyka szkodliwych zakłóceń mobilnych systemów satelitarnych korzystających z tego samego kanału.
ii. w przypadku urządzeń z odłączanymi antenami maksymalny dopuszczalny zysk anteny w pasmach 5250–5350 MHz i 5470–5725 MHz musi zapewniać zachowanie zgodności urządzenia z limitem e.i.r.p.;
ii. w przypadku urządzeń z odłączanymi antenami maksymalny dopuszczalny zysk anteny w pasmach 5250–5350 MHz i 5470–5725 MHz musi zapewniać zachowanie zgodności urządzenia z limitem e.i.r.p.;
iii. w przypadku urządzeń z odłączanymi antenami maksymalny dopuszczalny zysk anteny w paśmie 5725–5850 MHz musi zapewniać zachowanie zgodności urządzenia z odpowiednimi limitami e.i.r.p.;
iii. w przypadku urządzeń z odłączanymi antenami maksymalny dopuszczalny zysk anteny w paśmie 5725–5850 MHz musi zapewniać zachowanie zgodności urządzenia z odpowiednimi limitami e.i.r.p.;
Funkcje bezprzewodowych systemów dostępu, w tym radiowych sieci lokalnych (WAS/RLAN), w paśmie 5150–5350 MHz są w tym urządzeniu ograniczone do użytku w pomieszczeniach we wszystkich krajach Unii Europejskiej.

Niniejszym GL TECHNOLOGIES (HONG KONG) LIMITED oświadcza, że urządzenie radiowe typu [router 5G NR Wi-Fi 6, GL-X3000NR / router 4G LTE Wi-Fi 6, GL-X3000C16] jest zgodne z zasadniczymi wymaganiami i innymi odpowiednimi postanowieniami dyrektywy 2014/53/UE. Pełny tekst deklaracji zgodności UE jest dostępny pod adresem https://www.gl-inet.com/products/certificate.

Maksymalna moc wyjściowa:
CE: ≤20 dBm EIRP (2,412–2,472 GHz); ≤23 dBm EIRP (5,15–5,35 GHz); ≤30 dBm EIRP (5,47–5,725 GHz); ≤13,98 dBm (5,725–5,85 GHz);
Zasilacz: ICP30A-120-2500