VPN razem z 2FA

RouterOS 7

Ihor Hreskiv

Gdańsk 2025

MBUM # 10

Ihor Hreskiv

MIKROTIK | Certified Trainer

Trener MikroTik
6+ lat doświadczenia

Autor kanału YouTube
MikroTik Polska

Administrator i architekt
20+ lat praktyki

Praktyk
w zakresie wirtualizacji, sieci,
systemów wysokiej dostępności
VPN, BGP, systemy rozproszone

Jaki stosować?

Jaki protokół stosować?

SSTP

ZeroTier

IPSec IKEv2

PPTP

WireGuard

L2TP+IPsec

OpenVPN

Jaki protokół stosować?

Protokół	Zalety (Pros)	Wady (Cons)	Security
PPTP	Bardzo prosta konfiguracja Wbudowany w starsze systemy	Bardzo słabe szyfrowanie (MS-CHAPv2 złamany) Łatwy do przechwycenia Niezalecany do produkcji	❌ Niebezpieczny, przestarzały
SSTP	Działa przez TCP/443 (łatwo przechodzi przez firewalle) Wsparcie w Windows	Zamknięty protokół Microsoft Mniejsza przenośność Ograniczone wsparcie w innych OS	⚠️ Średni – zależy od implementacji i certyfikatów
L2TP+IPsec	Szerokie wsparcie systemowe (Windows, macOS, iOS, Android) Łączy tunelowanie z szyfrowaniem	Wolniejszy (podwójna enkapsulacja) Problemy z NAT Łatwe do blokowania porty UDP	✅ Bezpieczny, jeśli używa silnych algorytmów
OpenVPN	Open source, audytowany Bardzo elastyczny (TCP/UDP, dowolny port) Duże wsparcie społeczności	Wolniejszy niż IKEv2/WireGuard Trudniejsza konfiguracja Wymaga dodatkowego klienta	✅ Bardzo bezpieczny, przy AES-256 + TLS 1.2/1.3

Jaki protokół stosować?

Protokół	Zalety (Pros)	Wady (Cons)	Security
ZeroTier	Bardzo prosta konfiguracja (ID sieci) Działa przez NAT bez dodatkowych ustawień Multi-platformowy (Windows, macOS, Linux, iOS, Android, routery)	Zależność od centralnego kontrolera Rozwiązanie zamknięte, brak standaryzacji IETF Mniejsza wydajność niż natywny WireGuard/IPSec	✅ Szyfrowanie end-to-end (AES-256, Curve25519) ⚠️ Zależy od zaufania do kontrolera
WireGuard	Bardzo wydajny i szybki Minimalistyczny kod (łatwy do audytu) Dobrze działa za NAT	Brak natywnego wsparcia w starszych systemach Brak integracji z EAP/RADIUS Mniej dojrzały w enterprise	✅ Nowoczesny i bezpieczny (ChaCha20, Poly1305), ale młodszy standard
IPsec IKEv2	Standard IETF, rekomendowany przez NSA/NIST Wsparcie natywne w Windows, macOS, iOS, Android Integracja z RADIUS/MFA	Bardziej złożona konfiguracja Wymaga certyfikatów Problemy interoperacyjności między producentami	✅✅ Bardzo bezpieczny; spełnia NIST/CNSA wymagania

Dlaczego IKEv2

- spełnia aktualne wymagania kryptograficzne (CNSSP 15, NIST)
- mniej podatny na ataki
- prostszy w konfiguracji
- wspierany natywnie przez wszystkie główne systemy
- wykorzystuje RADIUS w połączeniu z mechanizmami MFA

NIST SP 800-77 Rev. 1 – *Guide to IPsec VPNs*
Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology — zalecenia dotyczące konfiguracji VPN-ów IPsec, w tym IKE.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf

RFC 9206 – *Commercial National Security Algorithm (CNSA) Suite and Usage*
Dokument od NSA, który w sekcji dotyczącej IPsec/i IKEv2 określa wymagania co do algorytmów, grup Diffie-Hellmana, długości kluczy, itp.

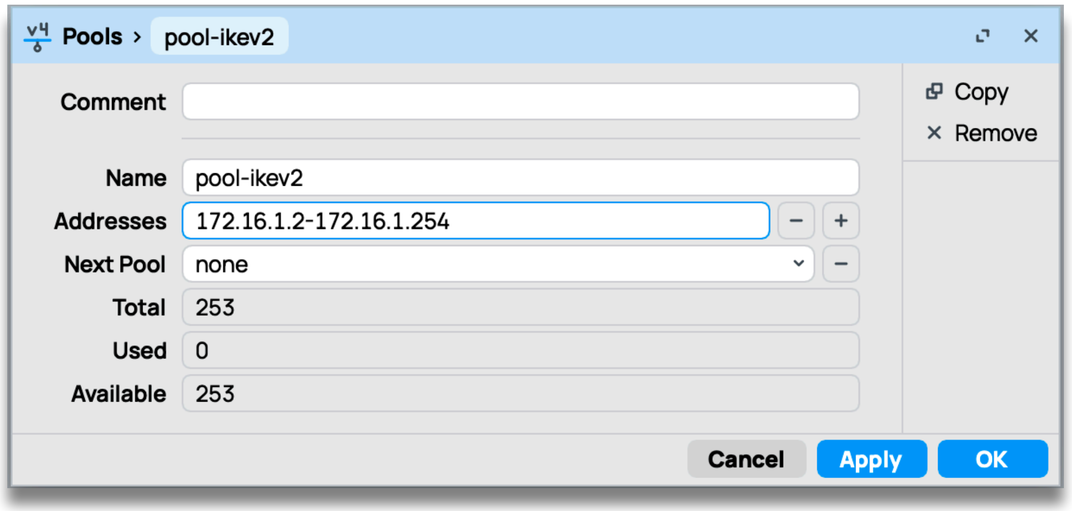
https://www.rfc-editor.org/rfc/rfc9206.txt

Rekomendacje

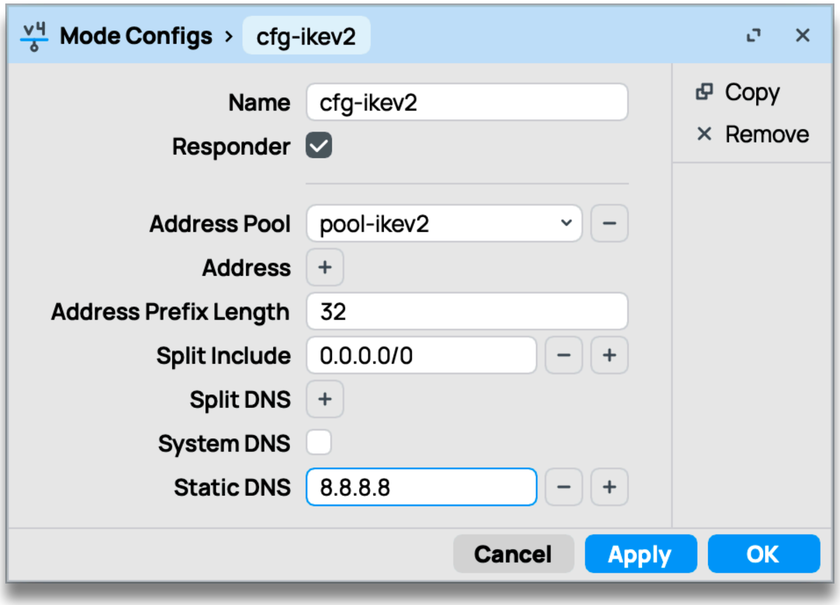
Element	Rekomendacja NIST (SP 800-77r1)	Wymagania CNSA Suite (RFC 9206)
Protokół IKE	IKEv2 (RFC 7296) — preferowany IKEv1 — przestarzały	Wymagane IKEv2
Szyfrowanie	AES-128/192/256 (zalecany AES-256)	AES-256 w trybie GCM (AEAD) lub CBC
Integralność	SHA-256, SHA-384, SHA-512	SHA-384 (minimum), SHA-512 dopuszczalne
Grupy DH/ECDH	≥ 2048-bit MODP (DH Group 14) lub lepsze, P-256/384	MODP 3072+, preferowane P-384 (ECDH)
PRF (IKE)	HMAC-SHA-256 lub mocniejsze	HMAC-SHA-384
Klucze sym.	Minimum 128 bitów, preferowane 256 bitów	256 bitów (AES-256)
Uwierzytelnianie	Certyfikaty X.509, EAP z silnym hashem	Certyfikaty X.509 z SHA-384+

IPSec IKEv2 w RouterOS 7

IKEv2 w RouterOS 7

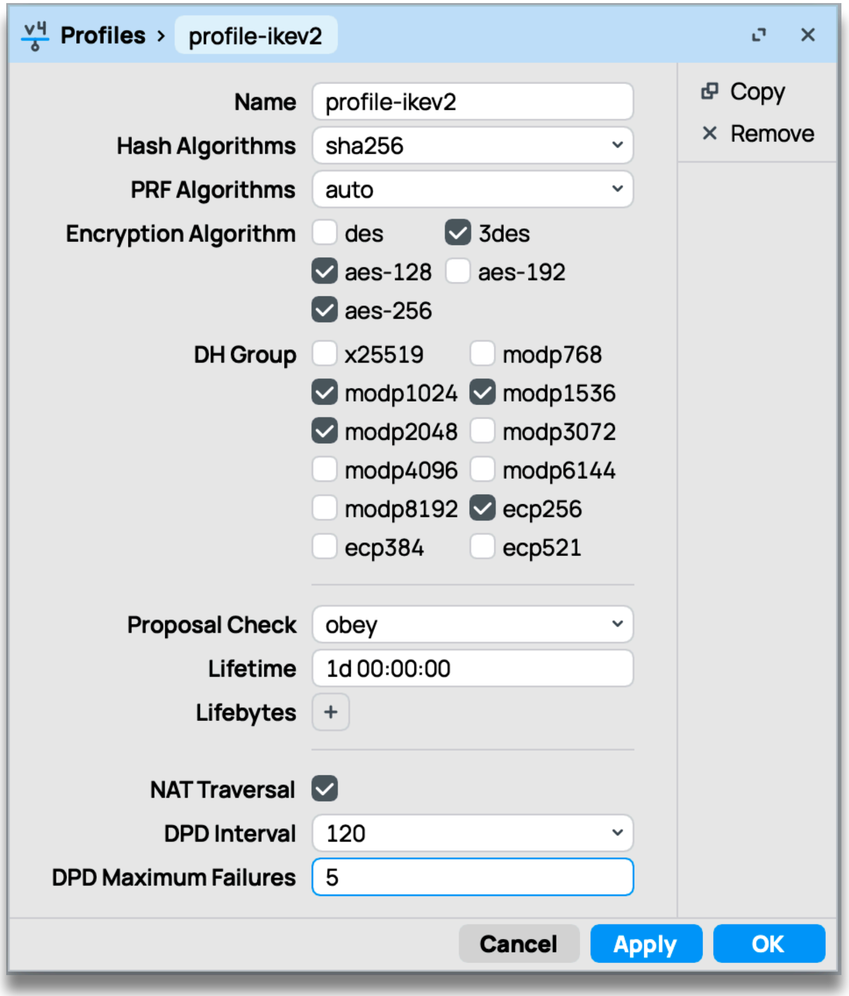


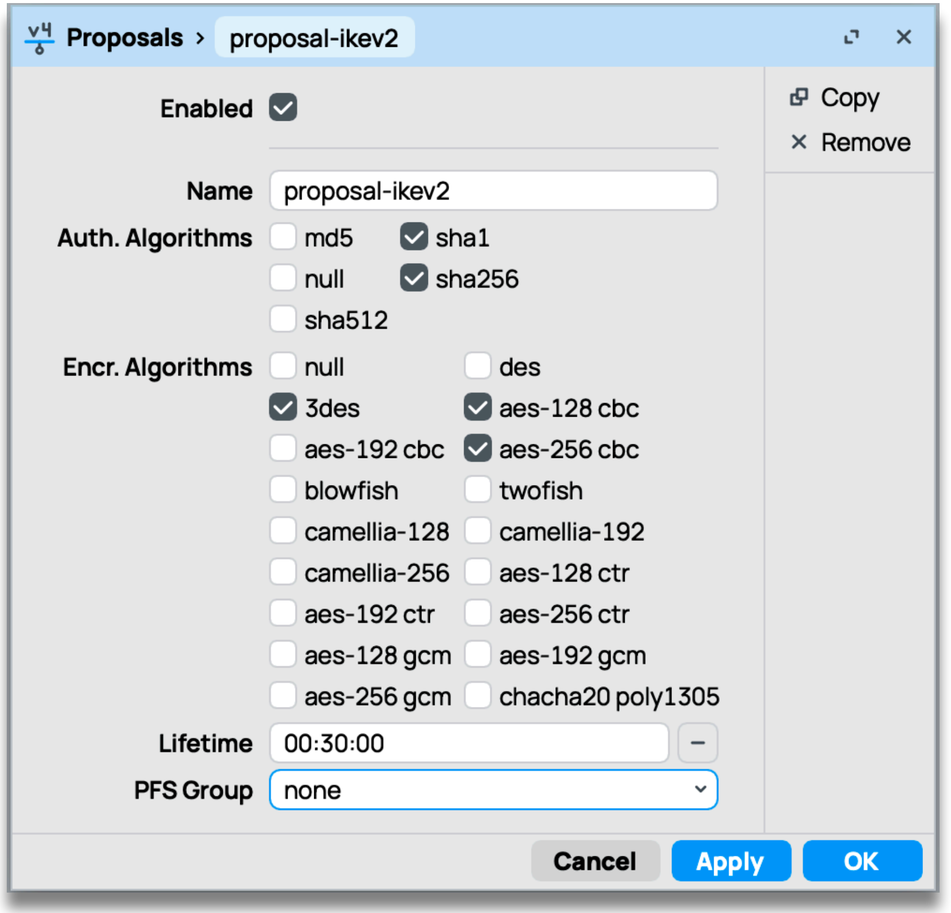
Pula adresów – definiujemy zakres adresów IP, które będą automatycznie przydzielane klientom VPN po nawiązaniu połączenia.



Mode-Config – definiuje pulę adresów, trasy (***Split Include***) oraz opcjonalnie adres serwera DNS, które będą przekazywane klientowi po zestawieniu tunelu.

IKEv2 w RouterOS 7

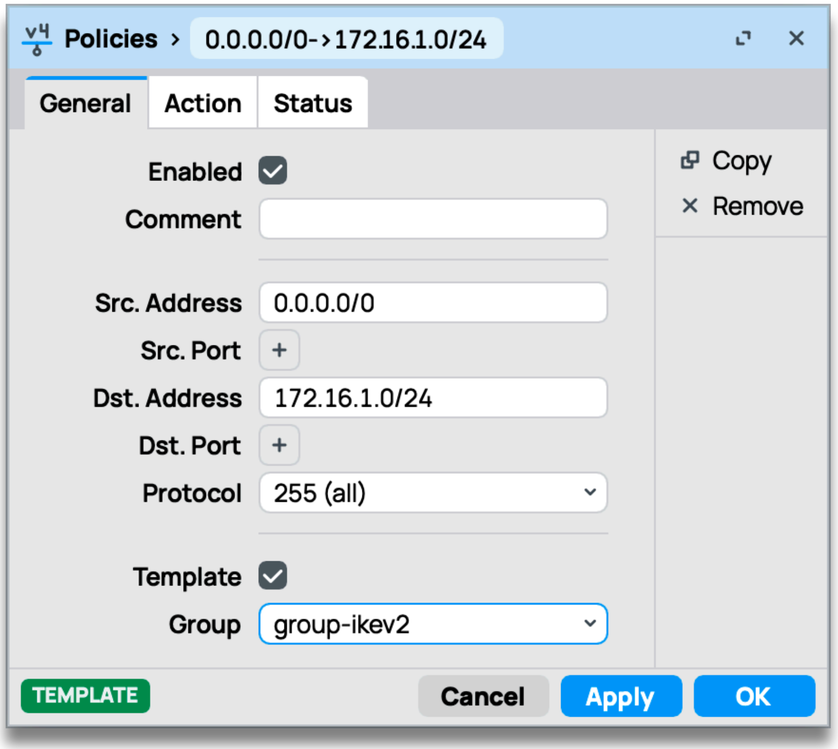


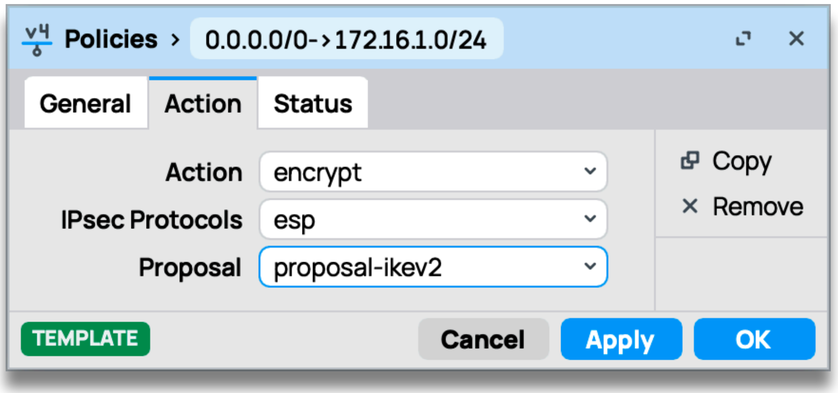


Profile IPsec – to zestaw parametrów używanych w **fazie 1 (IKE)** podczas negocjacji tunelu. Określają m.in. algorytmy szyfrowania, uwierzytelniania i wymiany kluczy

Proposal IPsec – to ustawienia dla **fazy 2**, które definiują sposób szyfrowania i uwierzytelniania ruchu danych w tunelu. Określają algorytmy używane do ochrony faktycznej transmisji po zestawieniu sesji IKE.

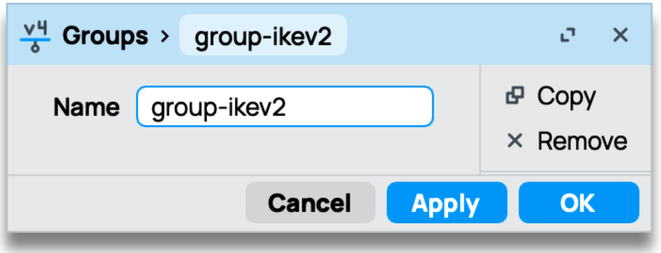
IKEv2 w RouterOS 7





Ustawienia IPSec template policy z wyżej dodaną fazą 2

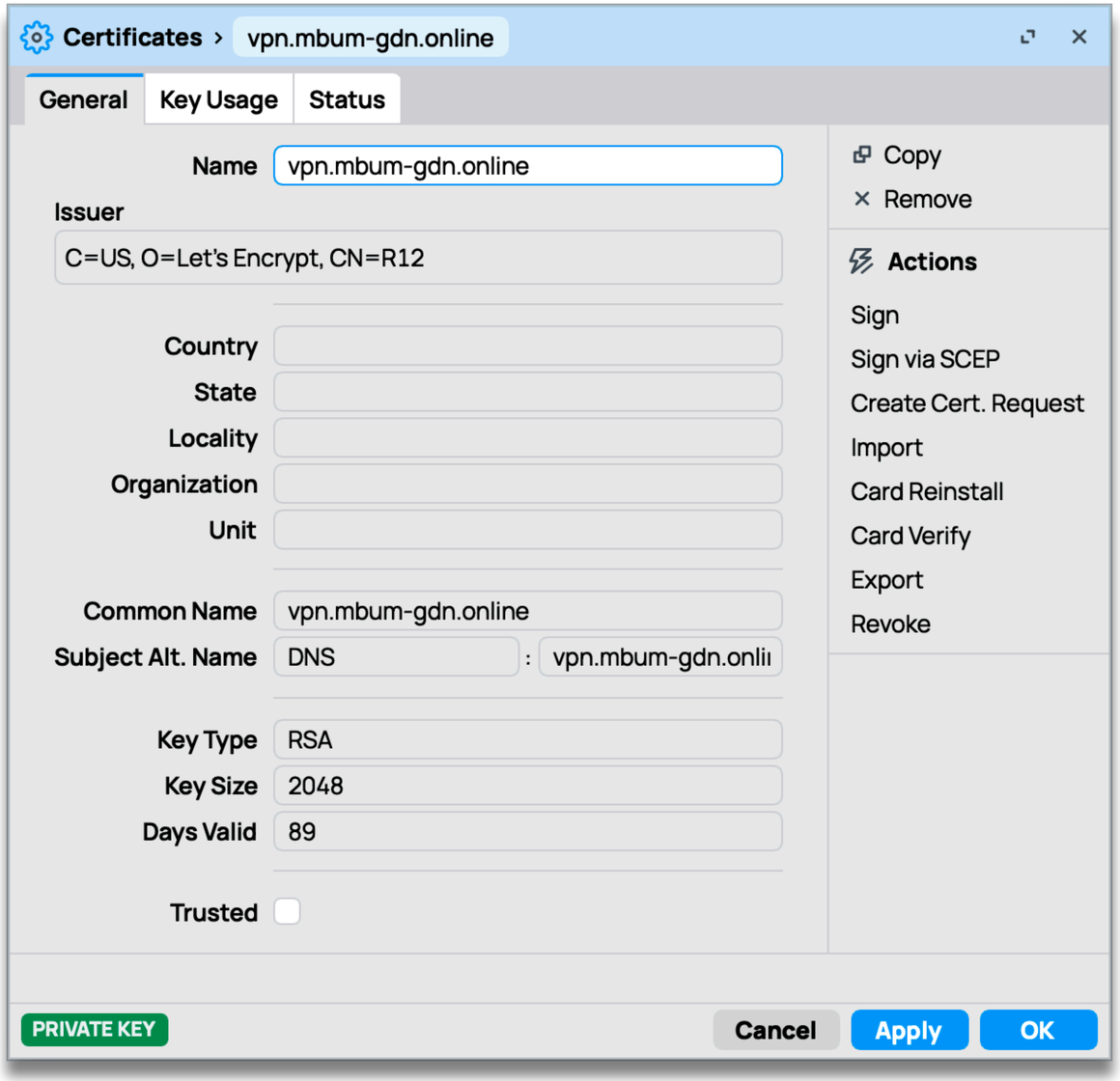
Jako Dst. Address podajemy podsieć, w której będą się znajdować nasze klienci.



Dodanie PFS group – Perfect Forward Secrecy (PFS) zapewnia, że każda sesja VPN ma swój unikalny klucz wymiany, niezależny od poprzednich.

Dzięki temu nawet w przypadku kompromitacji jednego klucza nie można odszyfrować wcześniejszej ani przyszłej komunikacji.

IKEv2 w RouterOS 7



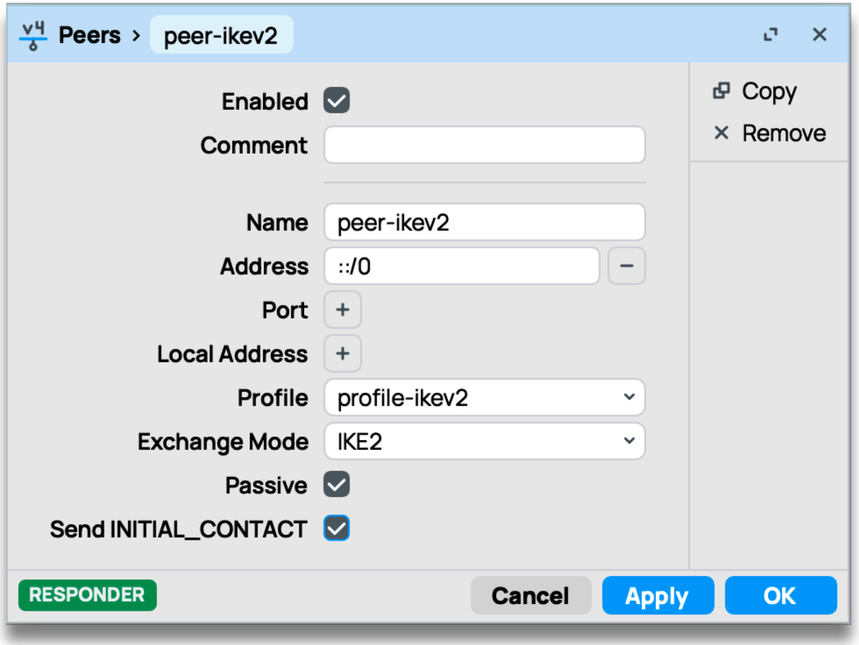
Za pomocą polecenia uruchamiamy proces uzyskania certyfikatu z Let's Encrypt dla wskazanej domeny.

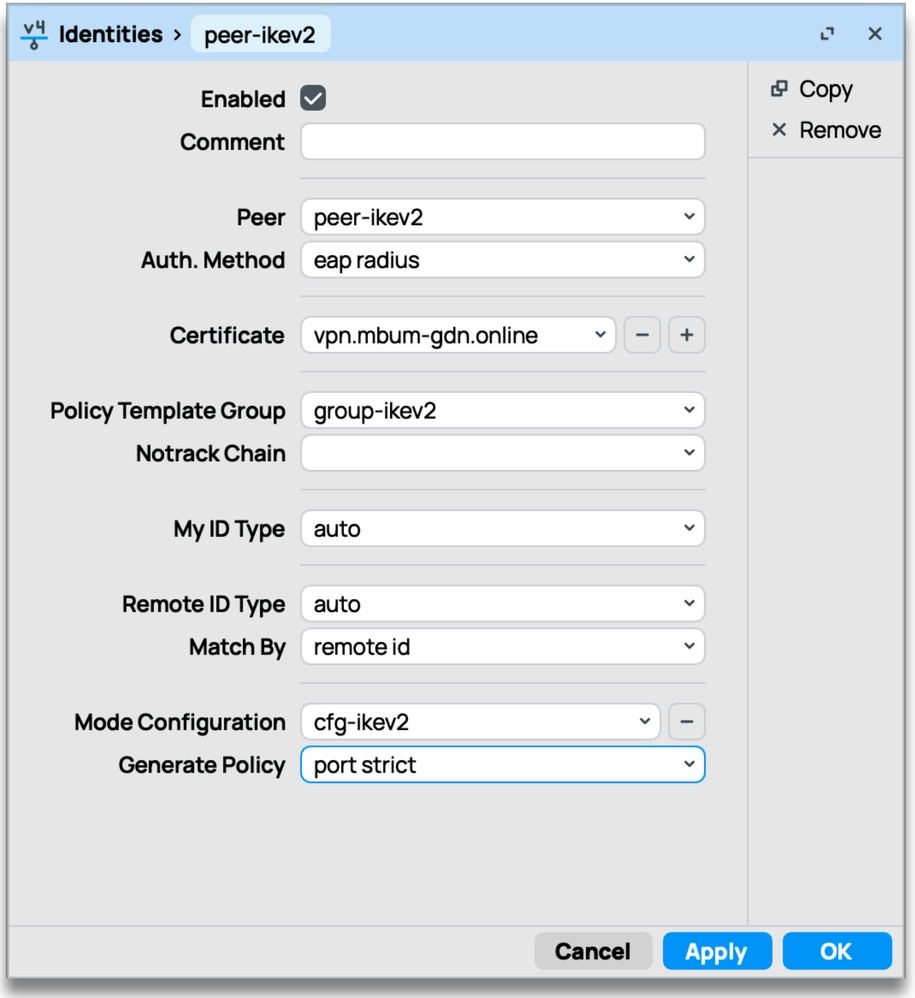
```
/certificate/enable-ssl-certificate\
  dns-name=vpn.mbum-gdn.online
```

Wymagana jest dostępna i poprawnie skonfigurowana nazwa domenowa dla danego hosta (record A lub AAAA).

Rekomendowaną praktyką jest zmiana domyślnej nazwy certyfikatu na bardziej czytelną — np. zgodną z nazwą domenową routera.

IKEv2 w RouterOS 7

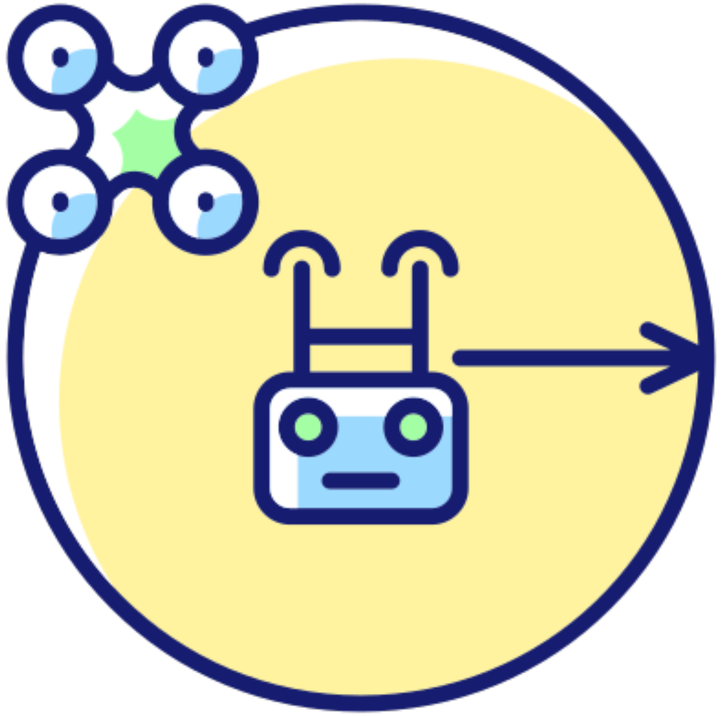




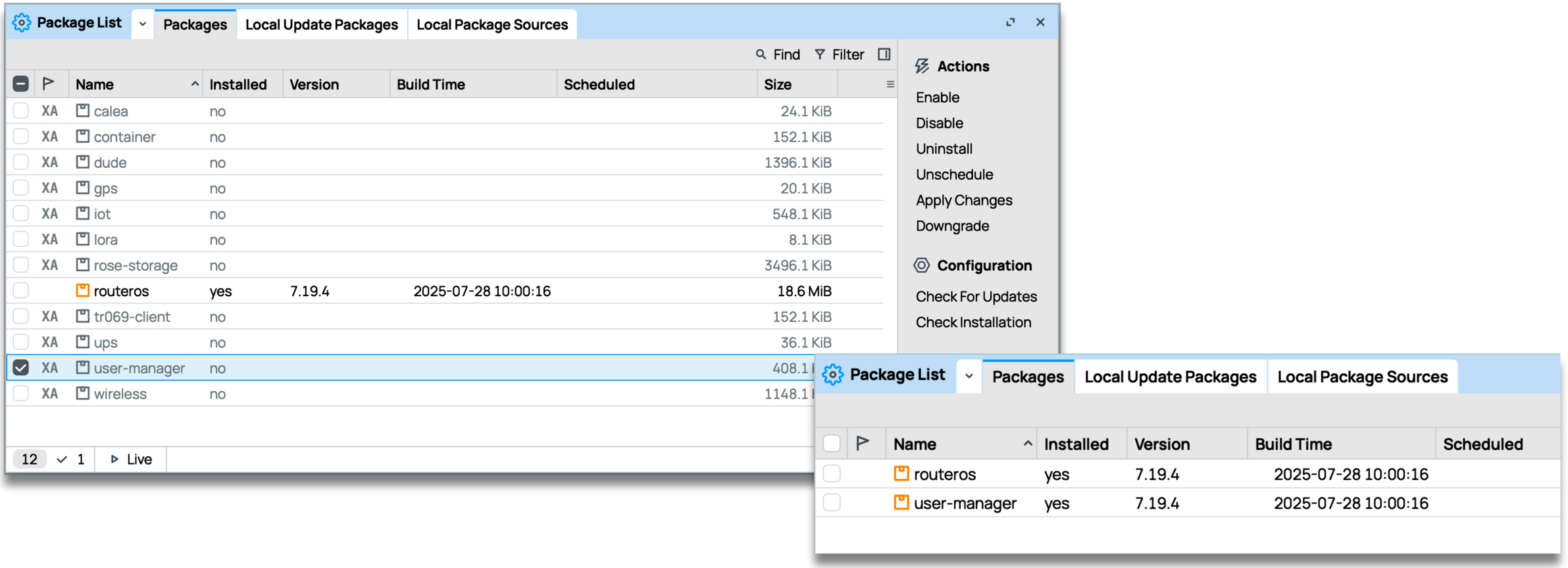
Peer definiuje parametry połączenia (adres, profil kryptograficzny, tryb IKE2).

Identity określa metodę uwierzytelniania (EAP RADIUS) oraz certyfikat serwera (np. Let's Encrypt).
Dzięki temu klient rozpoznaje i ufa serwerowi, a logowanie odbywa się z wykorzystaniem RADIUS

Remote Authentication Dial In User Service

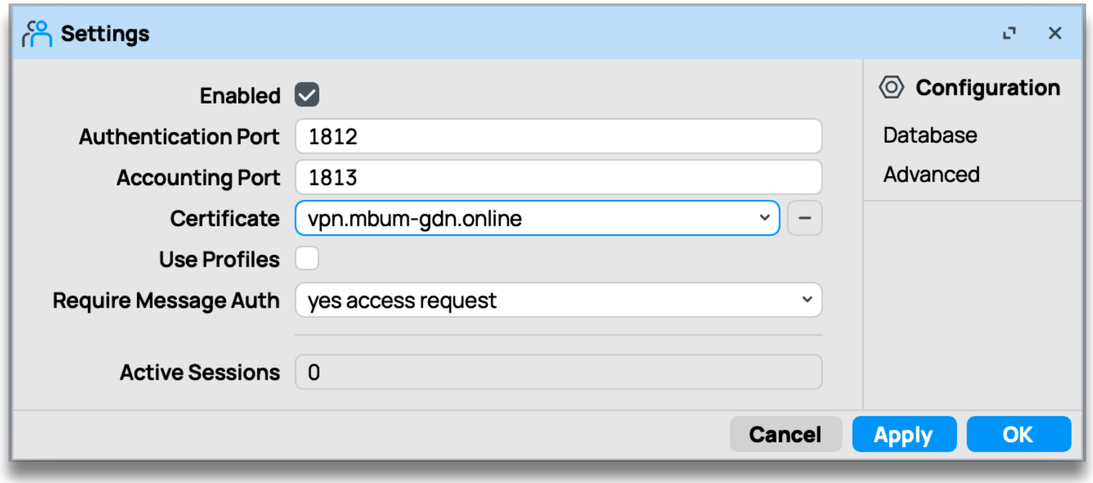


User-manager w RouterOS 7



Aby zainstalować pakiet User Manager, należy go aktywować na liście pakietów za pomocą *Enable*, a następnie zatwierdzić wybór poprzez *Apply Changes*.

IKEv2 w RouterOS 7

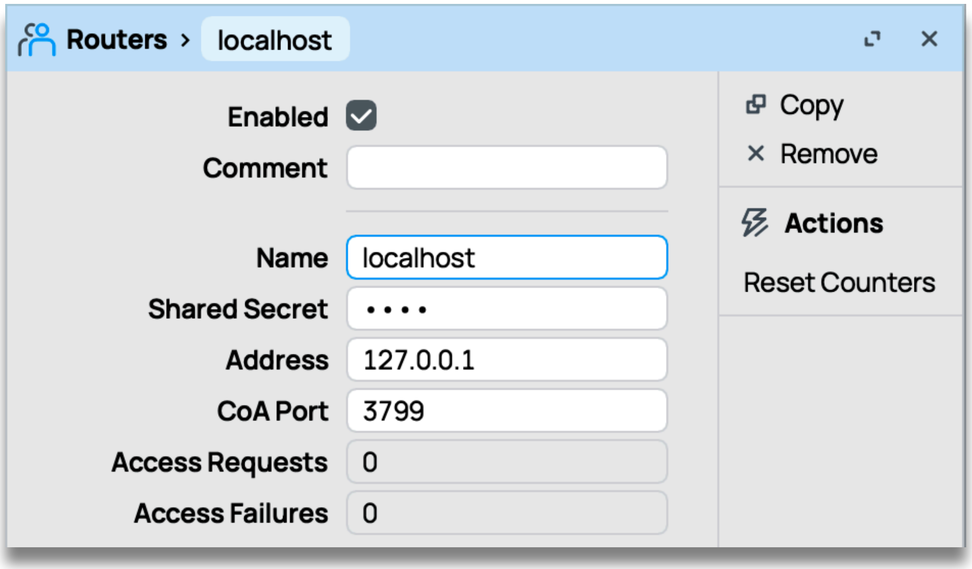


Uruchamiamy serwer RADIUS i przypisujemy do niego wcześniej wygenerowany certyfikat.

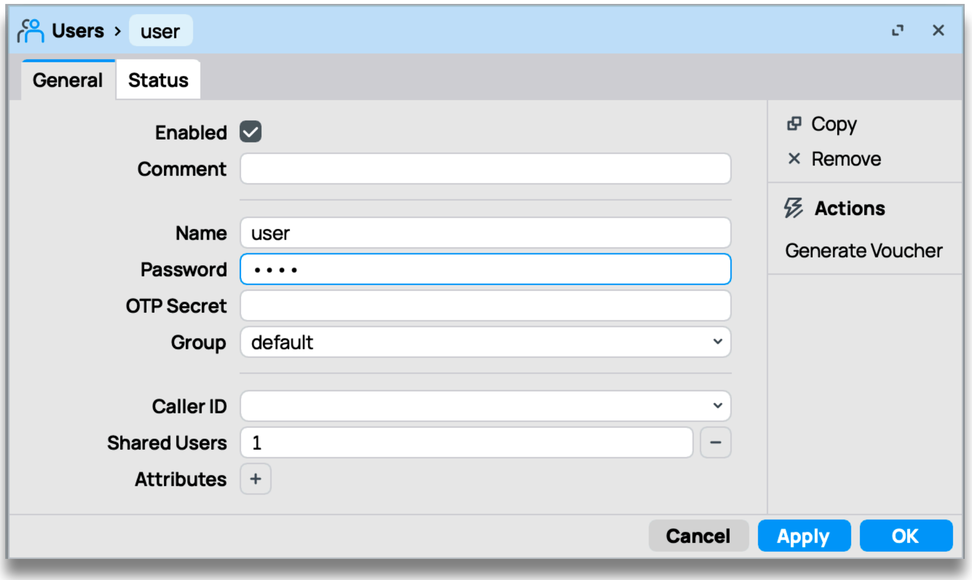
Certyfikat jest niezbędny, ponieważ w metodach EAP (np. EAP-MSCHAPv2 w IKEv2) serwer musi potwierdzić swoją tożsamość wobec klienta i zestawić bezpieczny tunel TLS dla przekazania danych logowania.

W skrócie: bez certyfikatu klient nie zaufa serwerowi i autoryzacja EAP nie zadziała.

IKEv2 w RouterOS 7

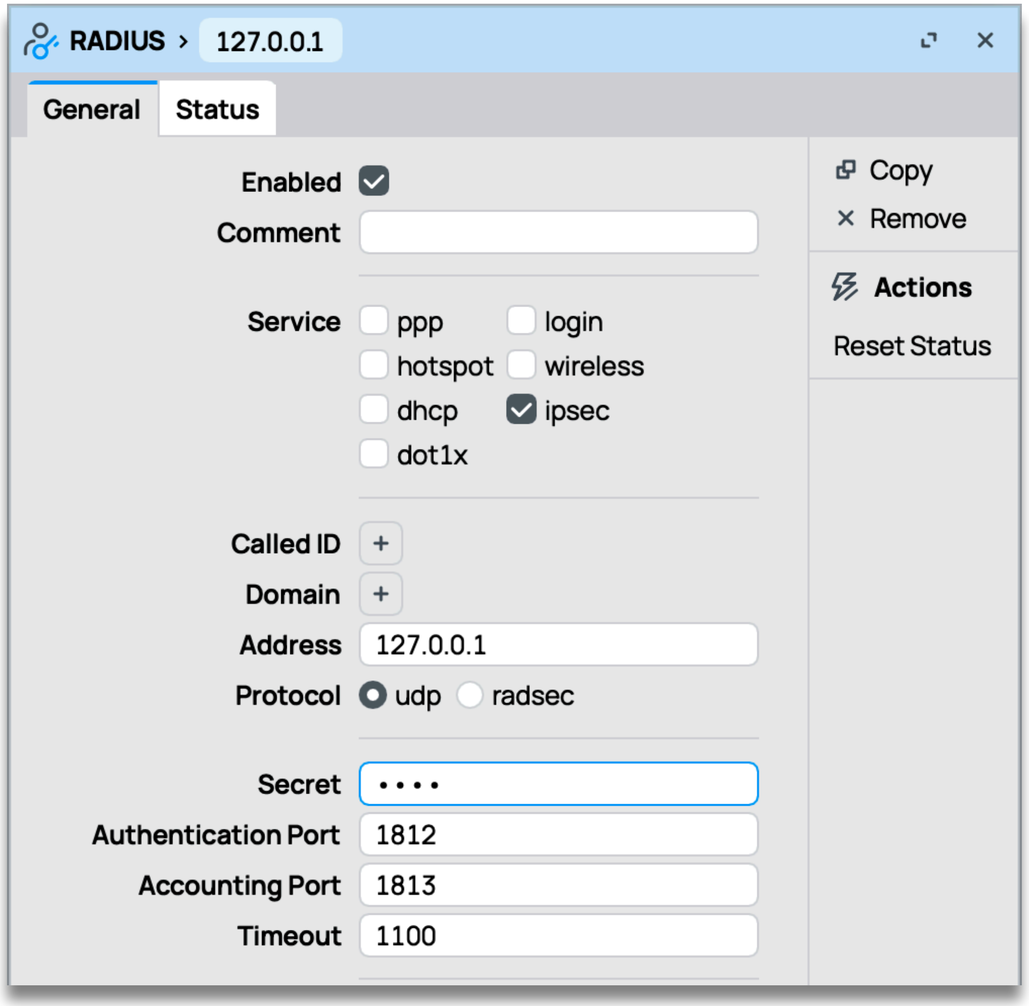


W User Manager dodajemy wpis `localhost` jako router z adresem (127.0.0.1) ze wspólnym sekretem.



Następnie tworzymy użytkownika z hasłem

IKEv2 w RouterOS 7



W RouterOS dodajemy klienta RADIUS (w tym przypadku `127.0.0.1`) i określamy, do jakich usług będzie używany.

W tym przykładzie wybrano usługę `ipsec`, co oznacza, że logowanie do VPN IKEv2 będzie weryfikowane przez serwer RADIUS (User Manager).

MultiFactor Authentication

Klasyczny VPN / Potencjalne zagrożenia

Single password = single point of failure
• całe bezpieczeństwo opiera się na jednym haśle użytkownika;
• jeśli zostanie odgadnięte, skradzione lub wycieknięte → atakujący ma pełny dostęp.

Brute-force / dictionary attack
• możliwe ataki słownikowe lub siłowe na hasło, szczególnie przy słabych politykach haseł;
• brak dodatkowej warstwy zabezpieczenia.

Wycieki haseł
• użytkownicy często używają tych samych haseł w wielu usługach;
• jeśli hasło wycieknie z innej usługi, automatycznie zagrożony jest też VPN.

MFA (Multi-Factor Authentication)

- = **hasło + coś więcej**
- eliminuje pojedynczy punkt awarii
- zwiększa bezpieczeństwo dostępu do VPN

Najczęściej stosowane MFA

1. **Hasło + SMS** – powszechne, ale podatne na przechwycenie.
2. **Hasło + aplikacja TOTP** (Google/Microsoft Authenticator, FreeOTP) – najpopularniejsze rozwiązanie, dobra równowaga prostoty i bezpieczeństwa.
3. **Hasło + powiadomienie push** (Duo, Microsoft, Google) – wygodne, szybka autoryzacja.
4. **Hasło + biometria** (odcisk palca, Face ID) – często w urządzeniach mobilnych.
5. **Hasło + klucz sprzętowy** (U2F/FIDO2, np. YubiKey) – najwyższy poziom bezpieczeństwa.

TOTP (Time-based One-Time Password, RFC 6238)

- = **6 cyfr generowanych co 30 sekund**
- kod ważny tylko w krótkim oknie czasowym
- używany np. w Google Authenticator, FreeOTP, RouterOS MFA

Podstawowa idea

- Jest klucz tajny (wspólny dla serwera i klienta)
- Jest czas (podzielony na interwały, zazwyczaj 30 sekund)
- Kod = funkcja (klucz, czas)
- Co 30 sekund → nowy kod

BASE32 – kodowanie krok po kroku

1. **Wejście**: dane binarne (ciąg bajtów).
2. **Podział na bloki**: dane dzielone są na grupy po **5 bitów**.
3. **Mapowanie**: każda 5-bitowa wartość jest zamieniana na znak z alfabetu:
   - A–Z (26 znaków)
   - 2–7 (6 znaków)
   - razem 32 symbole.
4. **Łączenie**: zakodowane znaki układają się w czytelny ciąg ASCII.
5. **Padding (=)**: jeśli długość wejścia nie jest wielokrotnością 40 bitów, dodawane są znaki = aby wynik miał pełne bloki.

Przykład

- Dane wejściowe: `HELLO`
- Bity: `01001000 01000101 01001100 01001100 01001111`
- Podział na 5 bitów → `01001 00001 00010 10100 11000 10011 00100 1111`
- Kodowanie: `JBSWY3DP`

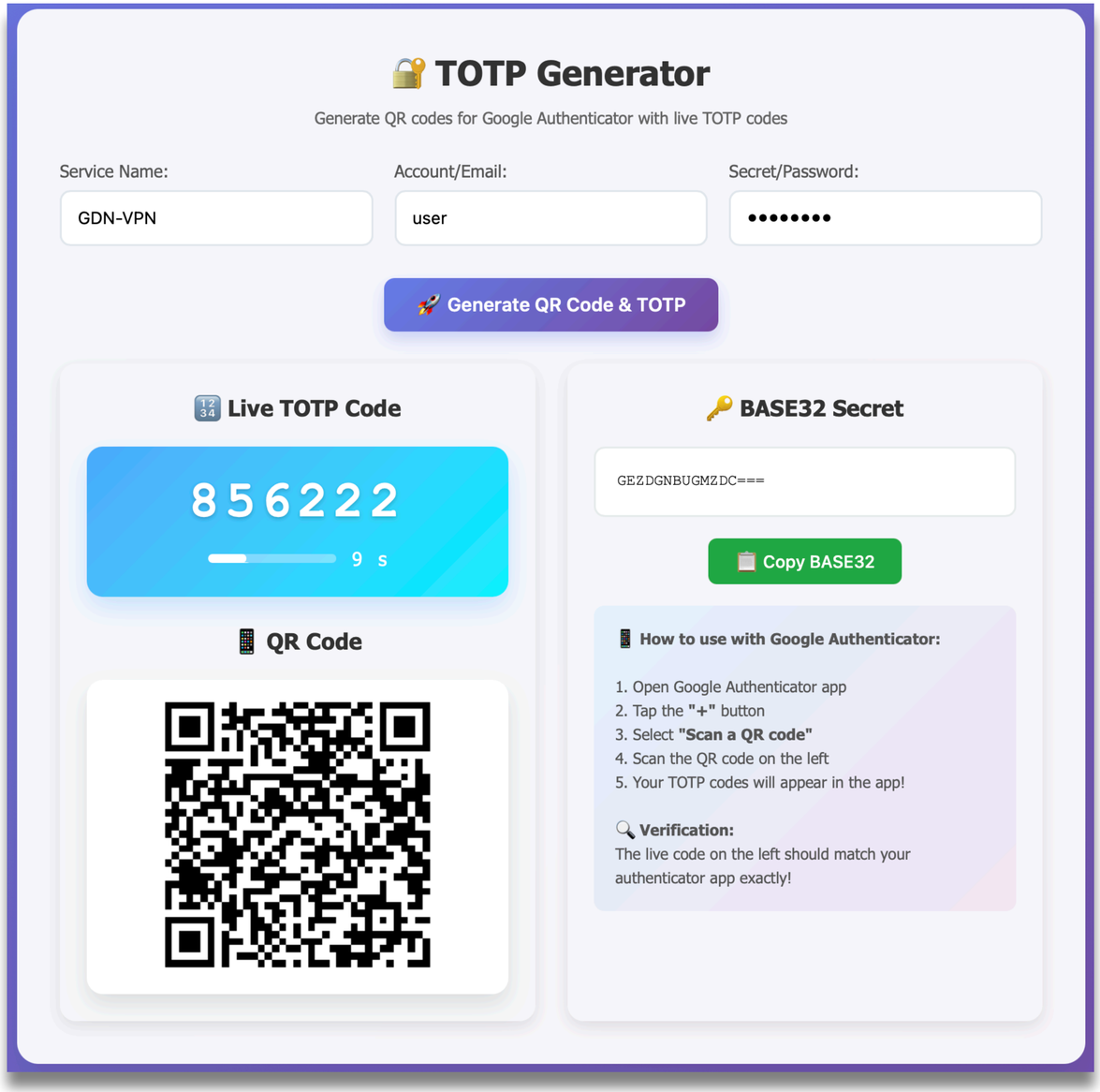
Przykład (z RFC 6238)

- Sekret (ASCII): 12345678901234567890
- Krok czasu: 30 sekund
- Algorytm: HMAC-SHA-1

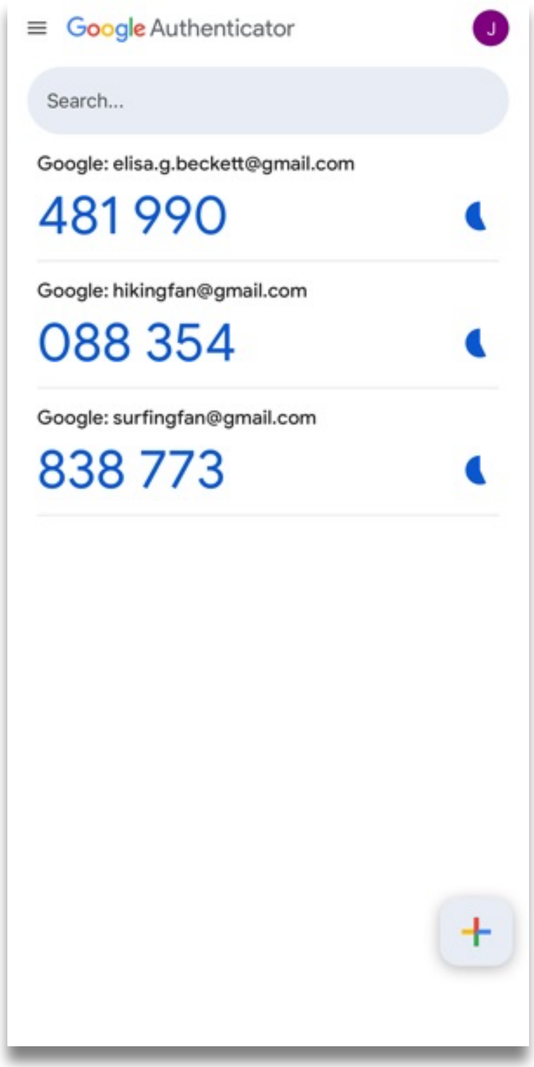
Dla czasu **T = 59 sekund (czas UNIX):**

- Licznik = floor(59 / 30) = 1
- Obliczenie HMAC → wynik = 94287082
- Końcowy kod (6 cyfr) = **287082**

Aplikacje TOTP

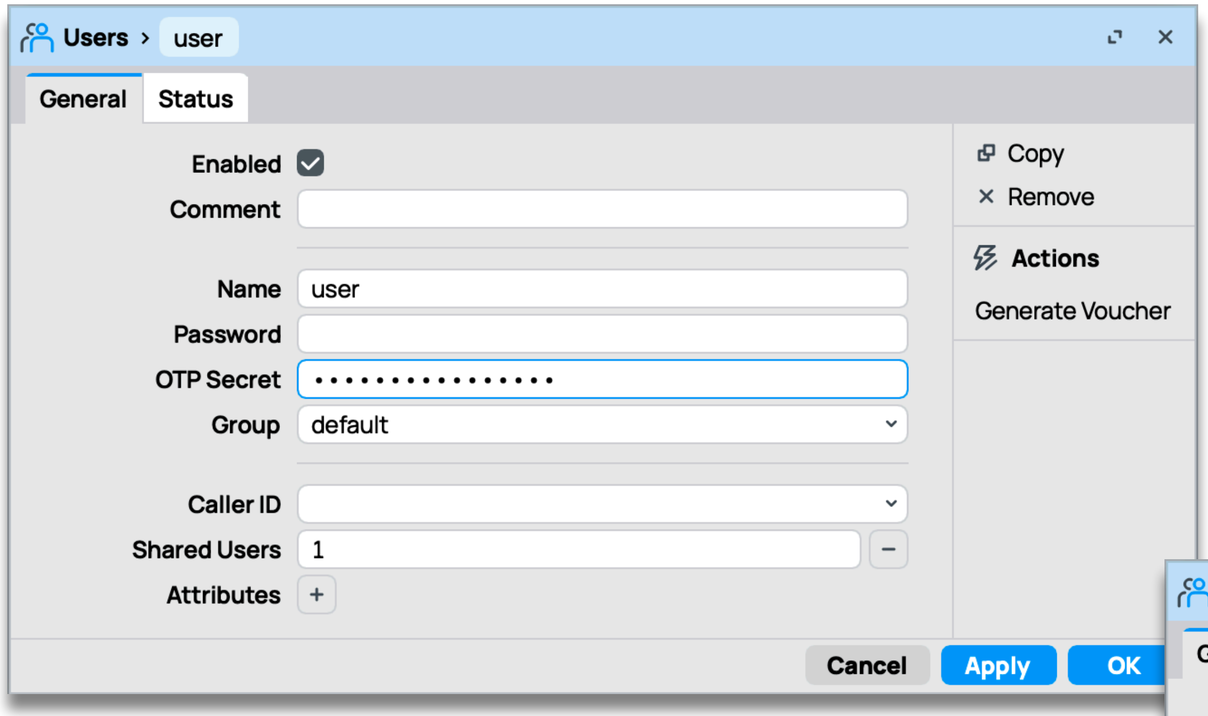


https://mtik.pl/totp.html — TOTP Generator

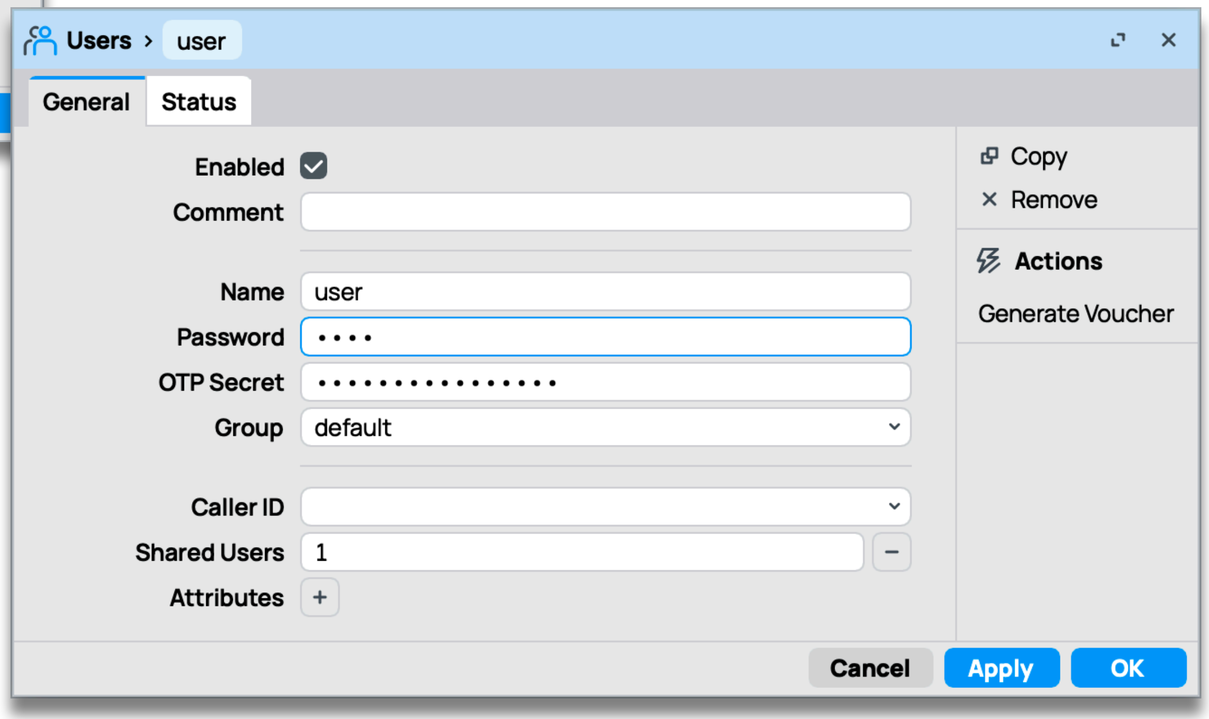


Google Authenticator

TOTP + RouterOS 7



Dodajemy OTP Secret bez ustawiania hasła – w takim przypadku logowanie odbywa się wyłącznie za pomocą kodu TOTP.



Połączenie hasło + OTP zapewnia wyższy poziom bezpieczeństwa, ponieważ uwierzytelnianie składa się z dwóch elementów: części stałej (hasło znane tylko użytkownikowi) oraz części zmiennej (kod TOTP generowany co 30 sekund).

Podsumowanie

Podsumowanie

KEv2 + Let's Encrypt + User Manager + TOTP = proste MFA

- **IKEv2** – nowoczesny, bezpieczny protokół VPN (NSA/NIST compliant)
- **Let's Encrypt** – darmowe certyfikaty X.509, automatyzacja SSL/TLS
- **User Manager (RADIUS)** – centralne uwierzytelnianie użytkowników
- **TOTP** – jednorazowe kody 6-cyfrowe co 30 sekund (RFC 6238)

All-in-one solution

- Całość działa **na RouterOS**
- Bez potrzeby stawiania **zewnętrznych serwerów**
- MFA dostępne natywnie, z prostą konfiguracją

Podsumowanie dla ‘spóźnialskich’ i nie obecnych

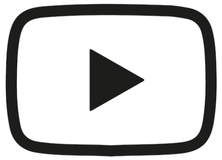
https://youtu.be/PmiwcX0gtS0

Dziękuję

mtik.pl

ihor@hreskiv.pl

https://github.com/hreskiv



https://www.youtube.com/@mikrotikpolska