

# Mikrotik IKEv2 client configuration

[Order now](#) | [Download](#) | [FAQ](#)

## Configuring Mikrotik as an IKEv2 Client.

Make sure you have an up to date routerOS system.

Version must be at least: 6.49.7

```
[admin@VPN-CLIENT] > system package print
Flags: X - disabled
#   NAME                      VERSION
SCHEDULED
0   ntp                      6.49.7
1   ppp                      6.49.7
2   dhcp                    6.49.7
3   mpls                    6.49.7
4   security                6.49.7
5   advanced-tools          6.49.7
6   system
```

```

6. 49. 7
7   openflow
6. 49. 7
8   multicast
6. 49. 7
9   routing
6. 49. 7

```

Open a one-time link to obtain authorization data and a root certificate.

Download the certificate and place it on the Mikrotik router using the Winbox program

Import the certificate into the system

To create an IKEv2 connection, we will use the console

Open a terminal and enter the following commands

Replace the authorization data with the data that is in the one-time link

the example contains the following data. You need to replace them with your own.

Name	Issuer	Common N...	Subject Alt...	Key Size	Days Valid	Trusted	SCE
dev.softkeel.com.crt_0	CN=PUQ VPN,O=PUQ sp. z o.o.,OU=PUQ VPN,L=Warszaw,C=PL	PUQ VPN		4096	3650	yes	

Name	Issuer	Value
dev.softkeel.com		address= <b>dev.softkeel.com</b>
mikrotik		my-id=user-fqdn: <b>mikrotik</b> AND username= <b>mikrotik</b>
NX9%B3&3YG		password= <b>NX9%B3&amp;3YG</b>
dev.softkeel.com.crt_0		certificate= <b>dev.softkeel.com.crt_0</b>

Import dialog:

Name:

File Name:

Buttons: Import, Cancel

It is a strong recommendation to use only the terminal command line in setup. We encountered cases when, during the configuration of Mikrotik through *winbox*, some parameters were not correctly entered into the configuration. Commands entered through the terminal are always correctly processed.

```

/ip ipsec settings
set accounting=no
/ip ipsec mode-config
add name=MY_VPN responder=no

```

```

/ip ipsec policy group
add name=MY_VPN

/ip ipsec profile
add dh-group=modp1024 enc-algorithm=aes-256 name=MY_VPN

/ip ipsec peer
add address=dev.softkeel.com exchange-mode=ike2 name=MY_VPN profile=MY_VPN

/ip ipsec proposal
add name=MY_VPN pfs-group=none

/ip ipsec policy
add dst-address=0.0.0.0/0 group=MY_VPN proposal=MY_VPN src-address=0.0.0.0/0 template=yes

/ip ipsec identity
add auth-method=eap \
eap-methods=eap-mschapv2 generate-policy=port-strict \
mode-config=MY_VPN \
peer=MY_VPN policy-template-group=MY_VPN \
certificate=dev.softkeel.com.crt_0 \
my-id=user-fqdn:mikrotik \
username=mikrotik \
password=NX9%B3&3YG

```

After the work done, you can see the connection status in the IP->IPsec configuration

You also need to configure the traffic routes you need at your discretion.

The screenshot shows the Mikrotik WinBox interface. The main window is titled 'IPsec Remote Peer <77.87.125.200>'. It has a tabbed interface with 'Active Peers' selected. The 'Active Peers' tab shows a list of peers with one item selected. Below the main window, there is a terminal window showing the command 'show ipsec peers' and its output. The output shows the peer 'dev.softkeel.com' is established. To the right, there is a small window titled 'Address List' showing a table of addresses.

	Address	Network	Interface
D	10.0.110.14/24	10.0.110.0	bridge1
D	192.168.129.2...	192.168.129.0	bridge1

Terminal <1>

```

# show ipsec peers
Peer: dev.softkeel.com
State: established
Created: 14 December 2023 16:51:00 by Ruslan
Updated: 16 October 2023 09:04:15 by Yulia Noha

```