

WireGuard client manual

Normally the setup is done with Ansible

There are situation where a Appliance needs to be connected that can not be configured through ansible. This manual is for that situation.

create client keys and config

Log in to a Rocky9 server with the wireguard-tools software installed:

```
dnf install -y wireguard-tools
```

make a directory in the root home directory for the client with a name you would remember:

```
sudo -i
mkdir wireguard_appliance1
cd wireguard_appliance1
```

create the private and public key:

```
/bin/wg genkey | tee ./private.key | /bin/wg pubkey > ./public.key
```

create the config file: vi ./wg0.conf and fill it with:

```
[Interface]
# use the private key created earlier
PrivateKey = 0CncJ5isB6BzgCwVt51q97BIKV6/2gzfSMtpYRyJX2s=
#this should be an available IP in the Mikrotik router
Address = 192.168.2.4/24
DNS = 8.8.8.8

[Peer]
#Puublic key of the mikrotik router wireguard instance
PublicKey = BB8XXa2ZXPgX7MihsUKrBKLPtZ4hQ7pnks0phRNDvSA=
#allow trafic from other wireguard peers and 2 workstations in the home LAN
AllowedIPs = 192.168.2.0/24, 192.168.1.20, 192.168.1.46
#enter the URL poinbting to the mikrotik router from the internet
Endpoint = external.domain.nl:13231
PersistentKeepalive = 15
```

Configure the Mikrotik router

log in to the Mikrotik web interface and in the Advanced view select WireGuard in the menu on the left.

On the top choose the button WireGuard and select your configuration entry. Almost at the bottom you find the Public Key you need for the client configuration file you create in the paragraph above.

Then go back and on the top choose the button Peers.

In the list check under the column Allowed Addresses and identify a free IP. Note this for the paragraph above. Notice you use /24 in the wg0.conf and /32 in the Mikrotik configuration in the next step.

Next press +New in the top. fill in the form, you need to press + at Allowed Address the public key is the client public key you created in the previous paragraph.

The screenshot shows the 'styx - New Wireguard Peer' web interface. The browser address bar shows '10.100.10.254/webfig/#WireGuard.Peers.new'. The interface has a sidebar on the left with various network configuration options like WiFi, Wireless, Interfaces, WireGuard, PPP, Bridge, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Dot1X, Files, Log, RADIUS, Tools, Container, Partition, and Make Supout.rif. The main area is titled 'New Wireguard Peer' and contains the following fields:

- Comment:** appliance one
- Enabled:** ☒
- Name:** +
- Interface:** CINDWG
- Public Key:** 9hOr53jwapVsm4Y4HNXWHBw6xMv7Op5WSllh0Q44Qo=
- Private Key:** (empty)
- Endpoint:** +
- Endpoint Port:** +
- Allowed Address:** 192.168.2.4/32
- Preshared Key:** (empty)
- Persistent Keepalive:** +
- Responder:** ☐

At the bottom, there are buttons for 'Cancel', 'Apply', and 'OK'. The 'Current Endpoint Address' and 'Current Endpoint Port' are also visible at the bottom.

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=werkinstructies:wireguard_client&rev=1773495770

Last update: **2026/03/14 14:42**