

How to install OpenFortiVPN on Linux

Inhaltsverzeichnis

- [Installation](#)
- [Configuration](#)
 - [Fedora](#)
 - [Debian/Ubuntu](#)
- [Establish the connection](#)
- [NetworkManager-Addon](#)
 - [Fedora](#)
 - [Debian/Ubuntu](#)

Ähnliche Artikel

- [Installation von OpenFortiVPN unter Linux](#)
- [How to install OpenFortiVPN on Linux](#)
- [Installation von FortiClient VPN unter Windows](#)
- [How to install the FortiClient VPN on Android](#)
- [How to install the FortiClient VPN on iOS](#)
- [How to install the FortiClient VPN on MacOS](#)
- [How to install the FortiClient VPN on Windows](#)
- [Installation von Forticlient VPN unter MacOS](#)
- [Installation von FortiClient VPN für Android](#)
- [Installation von FortiClient VPN für iOS](#)

openfortivpn is used to establish VPN tunnels on linux and compatible with Fortinet VPNs.

Installation

openfortivpn is included in notable linux distributions and can be installed via packet manager:

Fedora:

```
root@fedora:~# dnf install openfortivpn
```

Ubuntu:

```
root@ubuntu:~# apt install openfortivpn
```

Debian:

```
root@debian:~# apt install openfortivpn
```

Configuration

When starting *openfortivpn* the following config file is used and should look something like this for the standard vpn tunnel:

/etc/openfortivpn/config

```
##### config file for openfortivpn, see man openfortivpn(1)
###
#
# host = destination adress VPN-Gateway
# port = destination port
# realm = realm / name of the vpn tunnel
# username = username (CIT-Account)
# password = password
host = vpngate.frankfurt-university.de
port = 443
realm = pub-all
username = <CIT-Account>
password = <PASSWORD>
```

Note: *realm = pub-all* is used for the standard vpn tunnel and is used in most cases but it may differ when using a different tunnel.

Config files for additional tunnels may be created with freely selected names in the same place. ⚠ **NOTE:** Depending on the Linux distribution the config files may differ from */etc/openfortivpn* or may be created manually.

The next step is to add the certificate (chain) to the trusted certificates (systemwide).

Fedora

The ca-file includes the certificate chain o GEANT OV RSA CA 4 CA (pem file) and can be downloaded [here](#).

Now execute:

```
cd Downloads/
sudo cp geant_chain.cer /etc/pki/ca-trust/source/anchors
sudo update-ca-trust
```

Debian/Ubuntu

The ca-file includes the certificate GEANT OV RSA CA 4 CA (pem file) and can be downloaded [here](#). Please note: Debian expects the file to end with . crt. Otherwise it wont process the file and just skips it.

Now execute:

```
cd Downloads/
sudo cp geant_ov_rsa_ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

Establish the connection

start the tunnel via

```
[root@pc ]# openfortivpn
```

Root privileges (respectively sudo) are needed because a (ppp)-interface is created (see [here](#) section *Running as root?*). When using different tunnels via configuration files the following parameter is used:

```
[root@pc ]# openfortivpn -c /etc/openfortivpn/<my_tunnel_configfile>
```

Additional parameters and explanatory notes may be found via the MAN-pages.

NetworkManager-Addon

Openfortivpn can also be used via NetworkManager. The following packets are required and need to be installed:

Fedora:

```
root@fedora:~# dnf install networkmanager-fortisslvpn plasma-nm-fortisslvpn [KDE] network-manager-fortisslvpn-gnome [Gnome]
```

Ubuntu:

```
root@ubuntu:~# apt install network-manager-fortisslvpn network-manager-fortisslvpn-gnome
```

Debian:

```
root@debian:~# apt install network-manager-fortisslvpn network-manager-fortisslvpn-gnome
```

Afterwards a new NetworkManager-profile (type fortisslvpn) can be created.

The configuration should look something like this:


New Connection (vpn) — System Settings Module

Connection name:
New vpn connection

General configuration

VPN (fortisslvpn)

IPv4

General

Gateway:
vpngate.frankfurt-university.de:443

Authentication

User name:
testmann

Password:

••••••••••

Store password for this user only (encrypted)

CA Certificate:
/testmann/.fctsslvpn_trustca/chain.txt

User Certificate:

User Key:

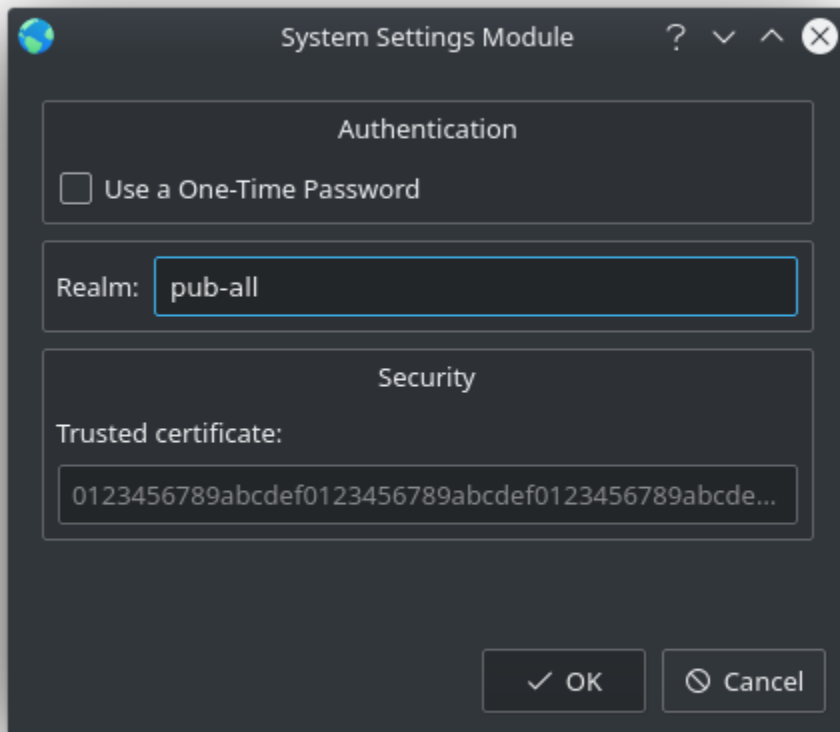
Advanced

Save

Cancel

Option	Value	Description
Gateway	vpngate.frankfurt-university.de:443	Gateway address.
User name		Your CIT-Account
Password		Your Cit-Account Password

click on "Advanced" to enter the "Realm":

A dark-themed dialog box titled "System Settings Module" with a globe icon on the left and help, expand, and close icons on the right. The dialog is divided into two sections: "Authentication" and "Security". In the "Authentication" section, there is a checkbox labeled "Use a One-Time Password" which is currently unchecked. Below this is a text input field labeled "Realm:" containing the text "pub-all". The "Security" section contains a label "Trusted certificate:" followed by a text input field containing a long alphanumeric string: "0123456789abcdef0123456789abcdef0123456789abcde...". At the bottom right of the dialog are two buttons: "OK" with a checkmark icon and "Cancel" with a circle-slash icon.

System Settings Module

Authentication

☐ Use a One-Time Password

Realm: pub-all

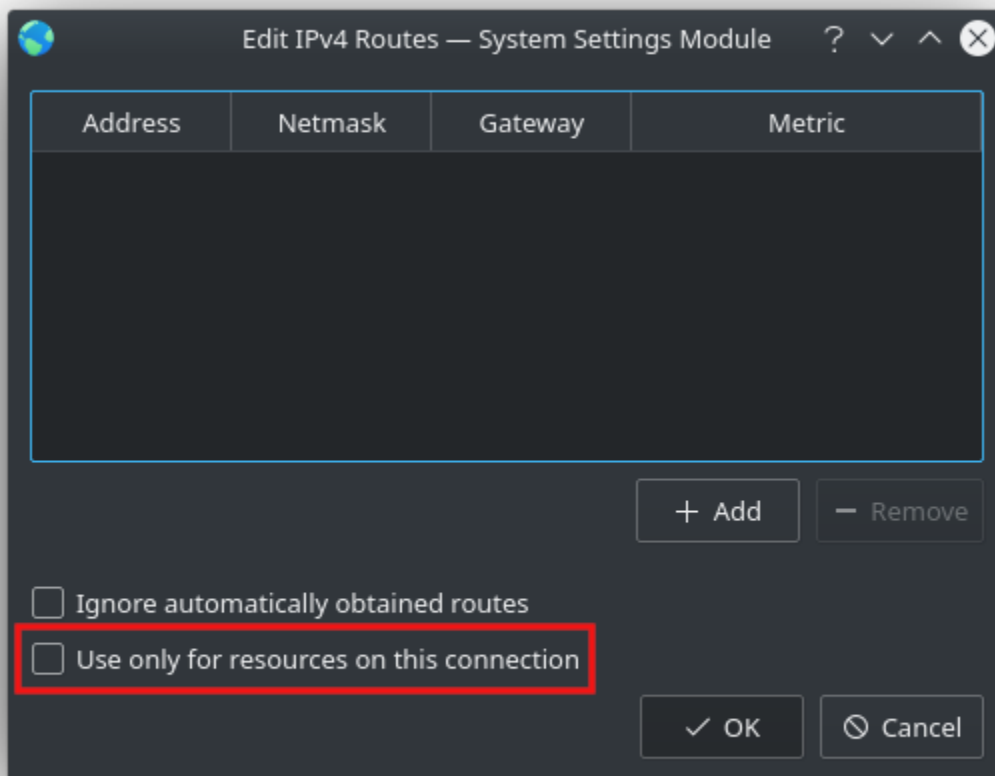
Security

Trusted certificate:

0123456789abcdef0123456789abcdef0123456789abcde...

✓ OK ⓧ Cancel

In most cases the realm is pub-all but it may differ when using a different tunnel. Note: Option "Use only for resources on this connection" from **IPv4 Routes** must be disabled.



The next step is to add the certificate (chain) to the trusted certificates (systemwide).

Fedora

The ca-file includes the certificate chain o GEANT OV RSA CA 4 CA (pem file) and can be downloaded [here](#).

Now execute:

```
cd Downloads/  
sudo cp geant_chain.cer /etc/pki/ca-trust/source/anchors  
sudo update-ca-trust
```

Debian/Ubuntu

The ca-file includes the certificate GEANT OV RSA CA 4 CA (pem file) and can be downloaded [here](#). Please note: Debian expects the file to end with .
crt. Otherwise it wont process the file and just skips it.

Now execute:

```
cd Downloads/  
sudo cp geant_ov_rsa_ca.crt /usr/local/share/ca-certificates/  
sudo update-ca-certificates
```

Afterwards the connection can be established when you click on the corresponding entry in the NetworkManager menu.