OpenVPN installation on Linux

OTHER VPN SOFTWARE

Last updated: June 28, 2023

This terminal-based guide walks you through the steps to connect to Mullvad VPN servers using OpenVPN.

Installation instructions

Follow the instructions for your particular Linux distribution below.

> Mullvad works with OpenVPN 2.4 and newer.

Ubuntu / Debian - using the terminal

1. In a browser, navigate to our Configuration files page.
2. Follow the instructions on that page to download a configuration file. (Make sure to enable "Use IP addresses")
3. Open up a terminal and navigate to the directory where you downloaded the file (usually ~/Downloads/).
4. Open a terminal and issue the command `unzip xxxx_xx.zip` (replace **xxxx_xx.zip** with the name of the file you downloaded).
5. Issue `sudo apt-get update && sudo apt-get upgrade` .
6. Issue `sudo apt-get install openvpn` .
7. Copy the following files to **/etc/openvpn/** (use `sudo`):
   - mullvad_ca.crt
   - mullvad_xx.conf
   - mullvad_userpass.txt
8. Start OpenVPN with either `sudo service openvpn start` or `sudo nohup openvpn --config /etc/openvpn/mullvad_xx.conf` (where **xx** is the country or region you selected).
9. To check whether or not you are connected to Mullvad, you can run `curl https://am.i.mullvad.net/connected` .

Ubuntu - using NetworkManager

1. Open a terminal and issue `sudo apt-get install openvpn network-manager-openvpn network-manager-openvpn-gnome` .
2. In a browser, navigate to our Configuration files page.
3. Fill out the form. Under Platform, **Android** needs to be selected. (Make sure to enable "Use IP addresses")
4. Click **Download** to save the configuration file.

5. Click on the Network icon.
6. Click on **VPN-Connections** > **Configure VPN**.
7. Click on **Add**.
8. Select **Import a saved vpn configuration**.
9. Navigate to where you saved the downloaded file, select it and then click **open**.
10. In the user name field, enter your Mullvad account number (without any spaces).
11. In the password field, enter "**m**".
12. Click **Save**.
13. Issue `sudo nano -w /etc/NetworkManager/NetworkManager.conf` and change "dns=dnsmasq" to "#dns=dnsmasq", then save.
14. Issue `sudo service network-manager restart` in a terminal.
15. Click on **Network icon** > **VPN Connections** > **Mullvad_xx** ("xx" is the country you selected to connect).

Fedora - using the terminal

1. Navigate to our Configuration files page.
2. Follow the instructions on that page to download a configuration file. (Make sure to enable "Use IP addresses")
3. Open up a terminal and navigate to the directory where you downloaded the file (usually ~/Downloads/).
4. Run the command `unzip xxxx_xx.zip` (replace **xxxx_xx.zip** with the name of the file you downloaded).
5. Issue `sudo dnf install openvpn resolvconf` .
6. Copy the following files to /etc/openvpn/ (use `sudo`):
    - mullvad_ca.crt
    - mullvad_xx.conf
    - mullvad_userpass.txt
    - update-resolv-conf
7. Issue `sudo chmod 755 /etc/openvpn/update-resolv-conf`
8. Start OpenVPN with either `sudo service openvpn start` or `sudo nohup openvpn --config /etc/openvpn/mullvad_xx.conf` (where **xx** is the country or region you selected).
9. To check whether or not you are connected to Mullvad, you can run `curl https://am.i.mullvad.net/connected` .

Switching to a different server

In this example, we are changing from the default **se** server to the **se-got-001** server.

1. Open your .conf file (for example, mullvad_config_se.conf).
2. Replace the first "**remote se.mullvad.net 1300**" with either "**remote se-got-001.mullvad.net 1300**" or "**remote 185.213.154.131 1300**" (the second example uses the server's IP address).
3. Save the file and then restart OpenVPN.

Disabling auto-start

By default, OpenVPN will be installed as a service, meaning that it will automatically start when you boot up your computer. You can disable this behavior by changing /etc/default/openvpn so that "AUTOSTART=none" is set.

You will then have to manually start OpenVPN each time, with the command `sudo service openvpn restart` .

Enabling a kill switch

This example assumes that your network interfaces are on **eth*** and that you want to connect to our Swedish or Dutch servers.

Issue the following in a terminal, replacing the IP ranges or IP addresses with the servers you wish to use. Make sure to check "Use IP addresses" in the advanced settings of the OpenVPN generator. Also note that outgoing ping (ICMP) requests will be blocked outside of the tunnel so you cannot ping the VPN server.

> Make sure that your wan interface is **eth***, if not you need to replace the script to match your interface name.

```
sudo iptables -P OUTPUT DROP
sudo iptables -A OUTPUT -o tun+ -j ACCEPT
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
sudo iptables -A OUTPUT -d 255.255.255.255 -j ACCEPT
sudo iptables -A INPUT -s 255.255.255.255 -j ACCEPT
sudo iptables -A OUTPUT -o eth+ -p udp -m multiport --dports 53,1300:1302,1194:1197 -d
141.98.255.0/24,193.138.218.0/24,45.83.220.0/24,185.213.152.0/24,185.213.154.0/24,185.65.135.0/24,185.65
-j ACCEPT
sudo iptables -A OUTPUT -o eth+ -p tcp -m multiport --dports 53,443 -d
141.98.255.0/24,193.138.218.0/24,45.83.220.0/24,185.213.152.0/24,185.213.154.0/24,185.65.135.0/24,185.65
-j ACCEPT
sudo ip6tables -P OUTPUT DROP
sudo ip6tables -A OUTPUT -o tun+ -j ACCEPT
```

Troubleshooting

I have disabled IPv6 and OpenVPN exits with a fatal error.

Edit the OpenVPN configuration and make the following changes:

1. replace **proto udp** with **proto udp4**.
2. replace **proto tcp** with **proto tcp4**.
3. add **pull-filter ignore "route-ipv6"**
4. add **pull-filter ignore "ifconfig-ipv6"**

Be sure to verify that you have disabled IPv6 before adding these options, otherwise you will leak IPv6.

Permission issue on /etc/resolv.conf

Issue `sudo chmod 755 /etc/openvpn/update-resolv-conf`

Is your browser leaking?

Use our Connection check to see if your browser is leaking information and therefore jeopardizing your privacy. This can occur even while connected to Mullvad.