

Forum:[Hack Forums](#)

Thread: [Install Tor proxy on Ubuntu 20.04 Linux](#)

Proof - November 10, 2020, 10:43 am

Install Tor proxy on Ubuntu 20.04 Linux

Tor is free software that allows a user to have complete anonymity online. It can be used to avoid having websites and applications track your location or attempt to identify you. It does this by routing your network data through a pool of servers around the world, while also stripping identifying information from packet headers.

It's often used to avoid region blocks on the likes of Netflix or YouTube. Some users like it because it prevents ad tracking companies from building a profile on you based on your browsing habits and serving personalized ads. Still, others are just a little paranoid and appreciate the assurance that no one can spy on their internet activity.

You can use Tor on Ubuntu 20.04 Focal Fossa by installing the Tor client. We'll show you how to set it up in this guide, which includes browser configuration and enabling all of your shell commands to run through Tor's network.

In this tutorial you will learn:

- How to install Tor on Ubuntu 20.04

- Test your network connection through Tor

- How to Torify your shell temporarily or persistently

- Enable and utilize the Tor control port

- Configure web browser to use Tor network

First, we need to install Tor on our system. Open a terminal and type the following command to install it:

```
Code sudo apt install tor
```

By default, Tor runs on port 9050. You can confirm that Tor is up and running correctly by using the `ss` command in terminal.

Another quick way to check if Tor is installed and see what version you're running is with this command:

```
Code $ tor --version
```

```
Tor version 0.4.2.7.
```

Let's see Tor in action and make sure it's functioning how it's supposed to. We'll do this by obtaining an external IP address from the Tor network. First, check what your current IP address is:

```
Code $ wget -qO - https://api.ipify.org; echo
```

```
147.232.135.100
```

Then, we'll run the same command but preface it with `torsocks`. This way, the command is run through our Tor client instead.

```
Code $ torsocks wget -qO - https://api.ipify.org; echo
```

```
162.247.74.200
```

You should see a different IP address now. That means our request was routed through the Tor network successfully.

How to "torify" your shell

Obviously, prefacing every network related command with torsocks will get old quickly. If you want to use the Tor network by default for shell commands, you can torify your shell with this command:

Code `$ source torsocks` onTor mode activated. Every command will be torified for this shell.

To make sure it worked, try retrieving your IP address without using the torsocks command prefix:

Code `$ wget -qO - https://api.ipify.org; echo`
162.247.74.200

The torified shell will only persist for the current session. If you open new terminals or reboot your PC, the shell will default back to your ordinary connection. To turn torsocks on permanently for all new shell sessions and after reboot, use this command:

Code `$ echo ". torsocks on" >> ~/.bashrc`
If you need to toggle torsocks mode off again, just enter:

Code `$ source torsocks` offTor mode deactivated. Command will NOT go through Tor anymore.

Enable the Tor control port

In order to interact with the Tor installation on our system, we need to enable Tor's control port. Once enabled, Tor will accept connections on the control port and allow you to control the Tor process through various commands.

To start, we will password protect the Tor connection with the following command. We're using my-tor-password in this example.

Code `$ torpass=$(tor --hash-password "my-tor-password")`
Next, use this command to enable the Tor control port and insert our previously hashed password:

Code `$ printf "HashedControlPassword $torpass\nControlPort 9051\n" | sudo tee -a /etc/tor/torrc`
You can check the contents of your /etc/tor/torrc configuration file to confirm that the hash password settings have been correctly included.

Code `$ tail -2 /etc/tor/torrc`
HashedControlPassword
16:5D13CF3C7511D9FC60161179F8FFA1083C99601A5257CDC622E161839B
ControlPort 9051
Restart Tor to apply the changes:

Code `$ sudo systemctl restart tor`
Configure web browser to use Tor network

To browse the web anonymously through Tor, we'll need to configure our web browser to route traffic through our local Tor host. Here's how you would configure that on Ubuntu's default web browser, Firefox. The instructions for other web browsers will be very similar.

Open the settings panel from the menu or by typing about:preferences into the address bar. Scroll all the way down to find "Network Settings" and click the "Settings" button.

In this menu, select "Manual proxy configuration" and enter localhost under the "SOCKS Host" field. For port, enter 9050.

When you're done entering those settings, click OK. You can confirm that the changes have taken effect by navigating to a website like IP Chicken to make sure that you are connected to the Tor network. This is a recommended step anytime you want to make absolutely sure that you are browsing anonymously.

Askaban - November 18, 2020, 7:28 am

This is a nice and great info. I have to test this asap

DanteFox - November 18, 2020, 9:58 pm

Awesome bro. What a great tutorial from you.

Proof - November 18, 2020, 11:54 pm

(Nov 18, 2020 10:58 PM)DoMation Wrote: [\[CITE\]](#) Awesome bro. What a great tutorial from you. Thank you brothers, I appreciate the kind words.

Alieno539 - November 19, 2020, 2:08 pm

Awesome bro. What a great tutorial from you. thank you so much

musa hajuj - November 19, 2021, 5:28 pm

thank duuud !!awesome tutorial