UBUNTU/LINUX BLOG | UP UBUNTU

How To Configure Your Computer To Use The Tor Network System Wide - Ubuntu 12.10/12.04

In this tutorial we will help you configure your computer or laptop running under Ubuntu 12.10/12.04 to use the **Tor** network system wide instead of your actual internet connection. This will help you hide your real IP address to protect your online privacy.

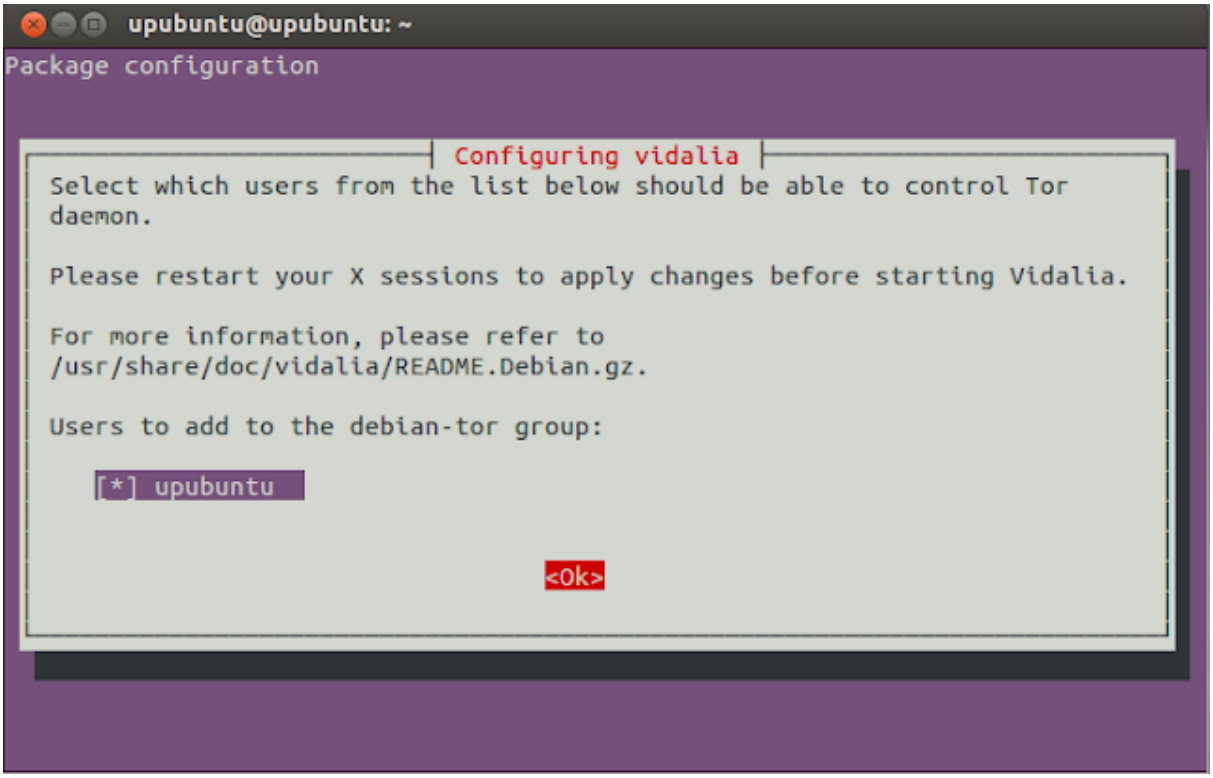
1. Tor Installation

To install Tor on Ubuntu, open the terminal and run these commands:

sudo apt-add-repository ppa:ubun-tor/ppa
sudo apt-get update
sudo apt-get install tor privoxy

During the installation, you will be required to add your username to the debian-tor group. Check on your username using the spacebar and press

Enter:

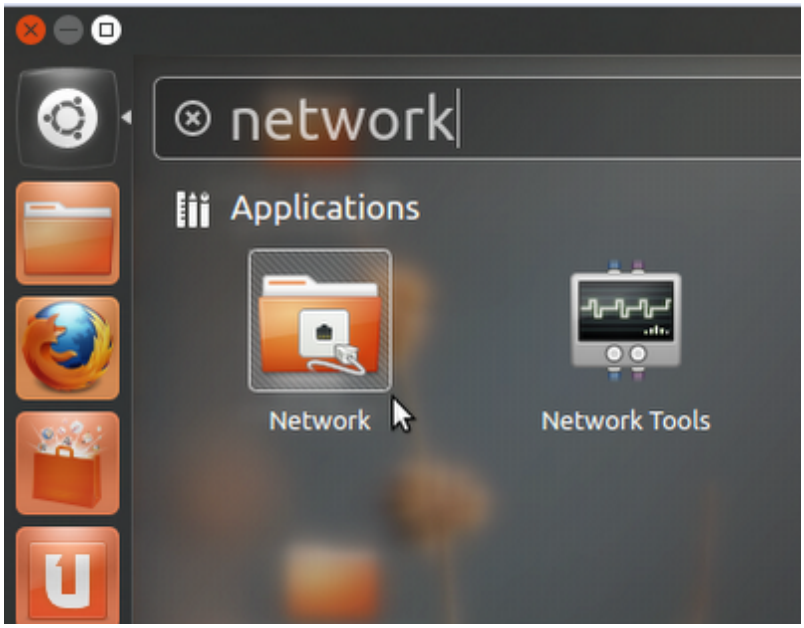


You can start now the Tor network with this command:

sudo /etc/init.d/tor start

2. System Configuration

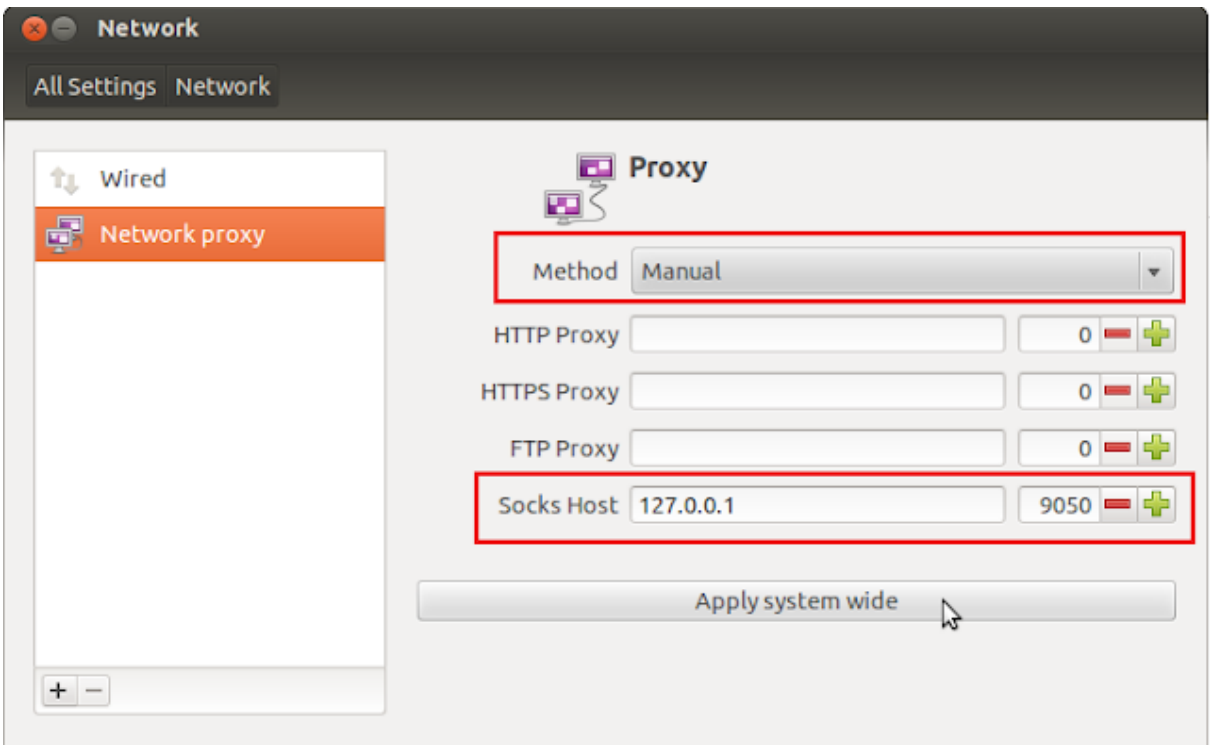
Via the Unity dash, open **Nework Manager**:



In the left pane of the window select "**Network proxy**," then enter the following settings:

Method: **Manual**

Socks Host: **127.0.0.1** **9050**



You must leave other settings empty, then click "**Apply system wide**" tc

apply the new changes (root password is required). Via your web browser (Firefox or Google Chrome), open now this link to verify if Tor is well enabled on your system:

https://check.torproject.org/

If enabled, you may see this:

3. Configure The Terminal To Use Tor

Although we applied the Tor network on system wide, you will find out that only your web browsers are working with Tor. If you check for example your current IP address from the terminal with this command:

curl icanhazip.com

It will detect your real IP address not that generated by Tor. To be able to use the Tor network from the terminal we need to use the "**proxychains**" package which will allow us to force the tcp connection to follow through proxy. You can install it under Ubuntu with this command:

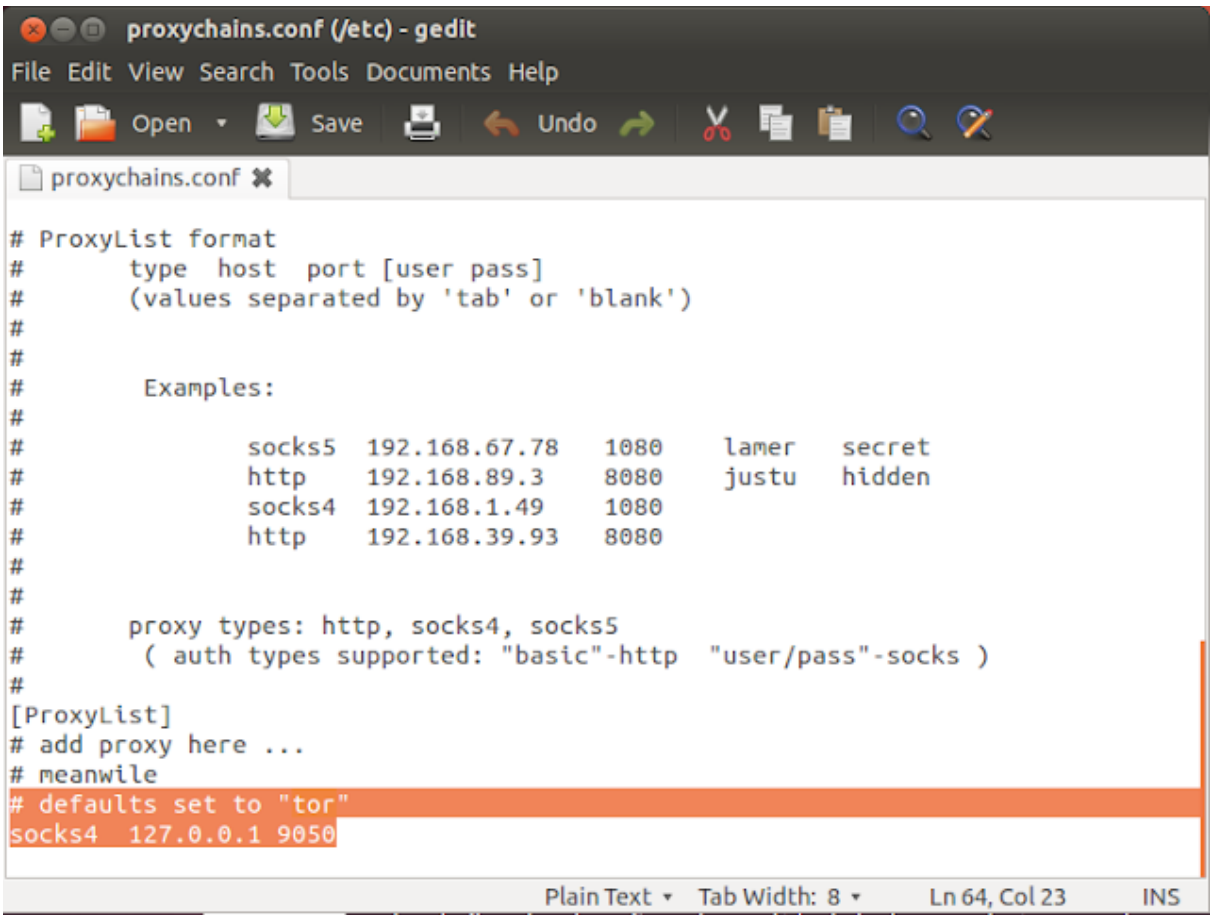
sudo apt-get install proxychains

Edit now the **proxychains** config file with this command:

sudo gedit /etc/proxychains.conf

Make sure these two lines are available:

 # defaults set to "tor"
socks4 127.0.0.1 9050



Save your file and exit. To make sure proxychains is well configured with Tor, check again your current IP address with this command:

sudo proxychains curl icanhazip.com

Here are now some other examples of using proxychains with Tor from the terminal to hide your real IP:

a. Installing A Package:

sudo proxychains apt-get install pidgin

The Pidgin package will now be downloaded via the Tor network.

b. Updating/Upgrading Packages

sudo proxychains apt-get update

sudo proxychains apt-get upgrade

c. Force Applications To Use Your Tor Connection

To force for example Rhythmobox to use the Tor proxy, run this command from the terminal:

sudo proxychains rhythmbox-client

You can now use any commands from the terminal with proxychains.