How to Use Tor with Firefox on Windows: BlackBelt Setup Guide

A simple guide to anonymous web browsing in Firefox

Author Info

Last Updated: February 2, 2023 **Tested**

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world. It prevents somebody watching your Internet connection from learning what sites you visit, and prevents the sites you visit from learning your physical location. Tor can function alongside many common applications, including Firefox, although for maximum privacy the Tor Browser is highly recommended.

Method 1

Method 1 of 3:

Setting Up Tor Using BlackBelt

1 **Download BlackBelt Privacy for Windows.** This method is only available for Windows XP, Vista, Windows 7, Windows 8, and Windows 10. If you are using one of these operating systems, begin the easy Tor installation by downloading BlackBelt Privacy at this link. The download is about 20 megabytes, so it will finish with a couple minutes over most internet connections. You should then ensure Firefox is installed because the BlackBelt Privacy installer will look for it and use it set up a Profile for browsing over Tor.

- If you are using a different operating system, use the instructions for setting up Tor manually instead.

2 **Open the BlackBelt file and select an option.** Open the file you just downloaded. A prompt should appear asking you to select how you'll be using Tor. If you don't know which one of these to choose, one of the following three options are probably what you're looking for:[1]

- Choose "Tor Client Only Operator" if you want to use Tor's network without

joining it yourself.
- Choose "Censored User" if you are living in a country that censors internet traffic.
- Choose "Bridge Relay Operator" if you want to both use Tor, and help other people stay private by relaying through your computer.

3 **Finish installing BlackBelt.** The software will automatically quit your Firefox if you have it open, and change its settings to give you a new Tor Firefox Profile Icon on your desktop. Use this icon to switch to the Tor mode for Firefox.

4 **BlackBelt should finish installation within a minute or two.** Once it's complete, open Firefox.You should now be able to browse using the Tor network.

- If you have problems with the installation process, try contacting a BlackBelt administrator for more information.

5 **Browse the internet.** As long as you are connected to Tor, it will be much harder for other people to access your personal data. However, using Tor with Firefox is not the most secure way to browse, especially if you do not alter your browsing habits. For greater security, follow the advice in the section below on becoming more secure.

Method 2

Method 2 of 3:

Setting Up Tor for Firefox Manually

1 **Download the Tor Browser Bundle.** This is available for all common operating systems and many languages. Select a download from the Tor Project website. Over most internet connections, it will only take a few minutes at most to download.

2 **Open the file you downloaded.** Extract the downloaded file by opening it or dragging it to your Applications folder. Open the Tor Browser application, and leave it open for the rest of this method.

- While the Tor Browser is the most secure way to browse the internet, it can also be used just as a connection to the Tor network. You'll need to have the Tor Browser open if you want to use Tor through any other browser, such as Firefox.

3 **Access your Firefox proxy settings.** The Tor network encrypts your requests for web pages and sends them through a network of private computers. To connect to this network through Firefox, you'll need to alter your Firefox proxy settings. This can vary depending on your Firefox version and operating system, but these instructions should work for most users:

- In Firefox for Windows, go to Menu → Options → Advance → Network → Settings, or skip this process and use BlackBelt as described above.
- In Firefox for Mac OS X, go to Firefox → Preferences → Advanced → Network → Settings.
- In Firefox for Linux, go to Edit → Preferences → Advanced → Proxies.

4 **Set up manual proxy configuration.** The default setting is "No proxy." Check the button next to "Manual proxy configuration" instead. Enter the following information exactly in the list of other options:

- In the **SOCKS Host** box, enter: **127.0.0.1**
- In the **Port** box adjacent to the numbers you entered, type **9150**.
- Select **SOCKS v5** if you see this option.
- Place a checkmark in the "Remote DNS" box, if it isn't there already.
- After **No Proxy for:**, enter **127.0.0.1**

5 **Check whether it works.** Most likely, if the setup didn't work, you will not be able to load any web pages. If this happens, double check the information you added, and that the Tor Browser is open. If you are able to load web pages, visit check.torproject.org to confirm that you are using Tor.

- If you cannot get Tor to work, switch back to "No Proxy" to continue using Firefox as normal while you troubleshoot the problem.

6 **Troubleshoot.** If you cannot get Tor to work following these instructions, find your issue on the Tor FAQ. If your question is not answered there, contact the Tor Project developers through email, phone, or paper mail.

- The developers can provide help in English, Arabic, Spanish, Farsi, French, or Mandarin.

7 **Browse the internet.** Anytime you want to use Tor, you must open the Tor Browser, wait for it to connect, then set Firefox to the "manual proxy configuration" you've set up. You will only be partially protected, but can

increase your security by following the instructions below on becoming more secure.

Method 3

Method 3 of 3:

Becoming More Secure and Private

1 **Check your Firefox version number.** In 2013, the US National Security Agency exploited a flaw in Firefox version 17 to collect data sent through the Tor network.[2] Check the changelog on a Firefox update to find out if it fixes an urgent security update. If it does not, consider waiting a week or two before updating, and check online to find out if the update introduced a new security flaw.

2 **Don't expect videos to be secure.** Browser plugins such as Flash, RealPlayer, and Quicktime can be exploited to reveal your IP address, identifying your computer.[3] To get around this, you can try YouTube's experimental HTML5 video player, but most other sites will not have this option.

- Many websites run these plugins automatically to show embedded content. You'll need to disable these plugins entirely in your Firefox plugin options for maximum privacy.

3 **Avoid torrents, and do not open downloaded files while online.** Be aware that Torrent file-sharing applications often override your privacy settings, making it easy to track the download back to your computer. You may download other files normally, but turn off your internet connection before opening them to avoid the application transmitting data.[4]

- .doc and .pdf files are especially likely to contain internet resources.

4 **Use https whenever possible.** The **http** you see at the beginning of web addresses marks the protocol used to exchange requests for information between you and the web server. You may manually enter **https** instead to add an additional encrypted protocol, but installing the https everywhere add-on for Firefox is a much easier way to accomplish this, automatically forcing https on any website that supports the function.

5 **Consider the Tor Browser instead.** While the above steps can make your Firefox reasonably private, it is easy to slip up and reveal your information. Firefox also has a much more rapid development time than Tor does, so there is a significant chance that security flaws related to Firefox and Tor interactions

will go undiscovered and unpatched. The Tor Browser, which you may have already downloaded while setting up Firefox Tor, automatically uses maximum privacy settings, and should be used when there are significant stakes involved, such as punishment from a repressive government.

- The Tor Browser is a modified version of Firefox, so the layout and functionality may be fairly easy to learn.

Community Q&A

Question

Do I need to have Firefox on my PC to make TOR work? Will TOR work without having Firefox on my PC?

> **Community Answer**
>
> No, you do not need to have Firefox on your PC in order for TOR (The Onion Router) to work on your device.

Question

Do I need a VPN to hide my location?

> **Community Answer**
>
> A VPN or a proxy. Proxy does what a VPN does, but a VPN encrypts your data securely while a Proxy might not.

Question

Can I use Tor and Firefox browser at the same time on my PC without revealing my IP from Tor?

> **Community Answer**
>
> You can install 2 or more Firefox derivatives. One you browse normally, and one you browse through the Tor Profile. For added security, run the Tor Profile inside a locked down VM. For an insane level of security, run Tails from a pen drive.

Tips

- You could also use Firefox's built-in proxy settings or FoxyProxy to make Tor work with Firefox, but this explains Torbutton, which is the easier.

Warnings

- Using Tor can be much slower than your ordinary internet browsing.
- Some websites block Tor exit nodes because they are frequently used for abuse.

References

1. https://www.youtube.com/watch?v=A-GXAhUdHbw
2. http://www.theregister.co.uk/2013/10/04/nsa_using_firefox_flaw_to_snoop_on_tor_users/
3. https://www.torproject.org/download/download
4. https://www.torproject.org/download/download