Tor Browser without Tor

Linux users can look into SecBrowser instead!

Tor Browser is a fork of the Mozilla Firefox web browser with patches that add numerous enhancements for improved security and privacy. It routes all traffic through the Tor network (henceforth referred to as 'Tor') to make it impossible for the recipient of data packets (e.g. a server hosting a website) as well as any third party to see who sent it. [1]

But it is also possible (and easy!) to use Tor Browser *without* Tor and take advantage of its excellent enhancements for reducing linkability, that is, "the ability for a user's activity on one site to be linked with their activity on another site without their knowledge or explicit consent." [2] Tor Browser offers better protection from online tracking than Firefox, Google Chrome/Chromium or Microsoft Edge, especially against fingerprinting, without any customization necessary.[3]

Security enhancements:

- improved exploit protection through selfrando [4]
- disable WebRTC [5]
- security slider
- noscript installed by default
- reproducible builds
- To provide users with optional defense-in-depth against JavaScript and other potential exploit vectors, we also include NoScript.

  [6]

- We also modify several extension preferences from their defaults.

  [6]

- proxy and DNS configuration obedience
- Full RELRO [7]

 Note:

- Do not use these instructions inside Whonix ™.
- Do not use these instructions inside a torified virtual machine because these instructions break Tor Browser's per tab stream isolation.
- These instructions are only for use outside of Whonix; for example, browsing the internet non-anonymously using Tor Browser on the Debian platform. The user only benefits from Tor Browser's security features in this configuration.

To Do / Questions[edit]

- install and make use of `tb-updater` and `tb-starter` package to allow simplified use of `torbrowser --clearnet` [8] [9]
  - let Whonix Debian Packages make use of wiki templates
  - use these templates for Install Tor Browser Outside of Whonix
  - also use these templates here
- How to: Create a desktop shortcut, change the logo of the shortcut in Windows (for Linux `tb-starter` package will provide a start menu entry)
- Test whether two instances of Tor Browser Bundle (TBB) run simultaneously - one with Tor enabled, one without - interfere with each other. This does not seem to be the case based on preliminary tests.
- Change the name and logo of the browser.
- Note that TBB notifies of updates, even if Tor is disabled.
- Investigate better methods of changing browser settings other than creating a `user.js` file or manually editing `about:config`.
- In order to use a clearnet Tor Browser *in addition to* Tor Browser (using Tor), copy the directory and change shortcut paths.
- `--allow-remote`
- Find out how to store passwords in Tor Browser. [10]

Instructions[edit]

Sourcing and Installing Tor Browser[edit]

- **Windows:** Follow the instructions in this guide from EFF's Surveillance Self Defence, until the section "Using Tor Browser".
- **macOS:** Follow the instructions in this guide from EFF's Surveillance Self Defence, until the section "Using Tor Browser Bundle".
- **Linux:** Download Tor Browser Bundle (TBB), preferably by installing Tor Browser Launcher. This will download

the most recent version of TBB, verify its integrity and store it in `~/.local/share/torbrowser`.

- If Debian or any of its derivatives (Ubuntu, Mint) is being used, run `sudo apt-get install torbrowser-launcher`.
- Fedora users can run `sudo dnf install torbrowser-launcher`.

Start Tor Browser Launcher by running `torbrowser-launcher`.

Tor Browser Launcher automatically opens Tor Browser when finished. When Tor Browser starts for the first time it asks for "Tor Network Settings" to be set. Click `Connect`, then wait while the connection to Tor is completed. When Tor has successfully connected, Tor Browser will open and the steps to disable Tor outlined below can be completed..

Disabling Tor[edit]

 Disabling Tor means traffic will not be routed through the Tor network. Similar to other browsers, your IP address will be visible to the recipients of any communications. **This configuration is not anonymous.**

Tested Platforms

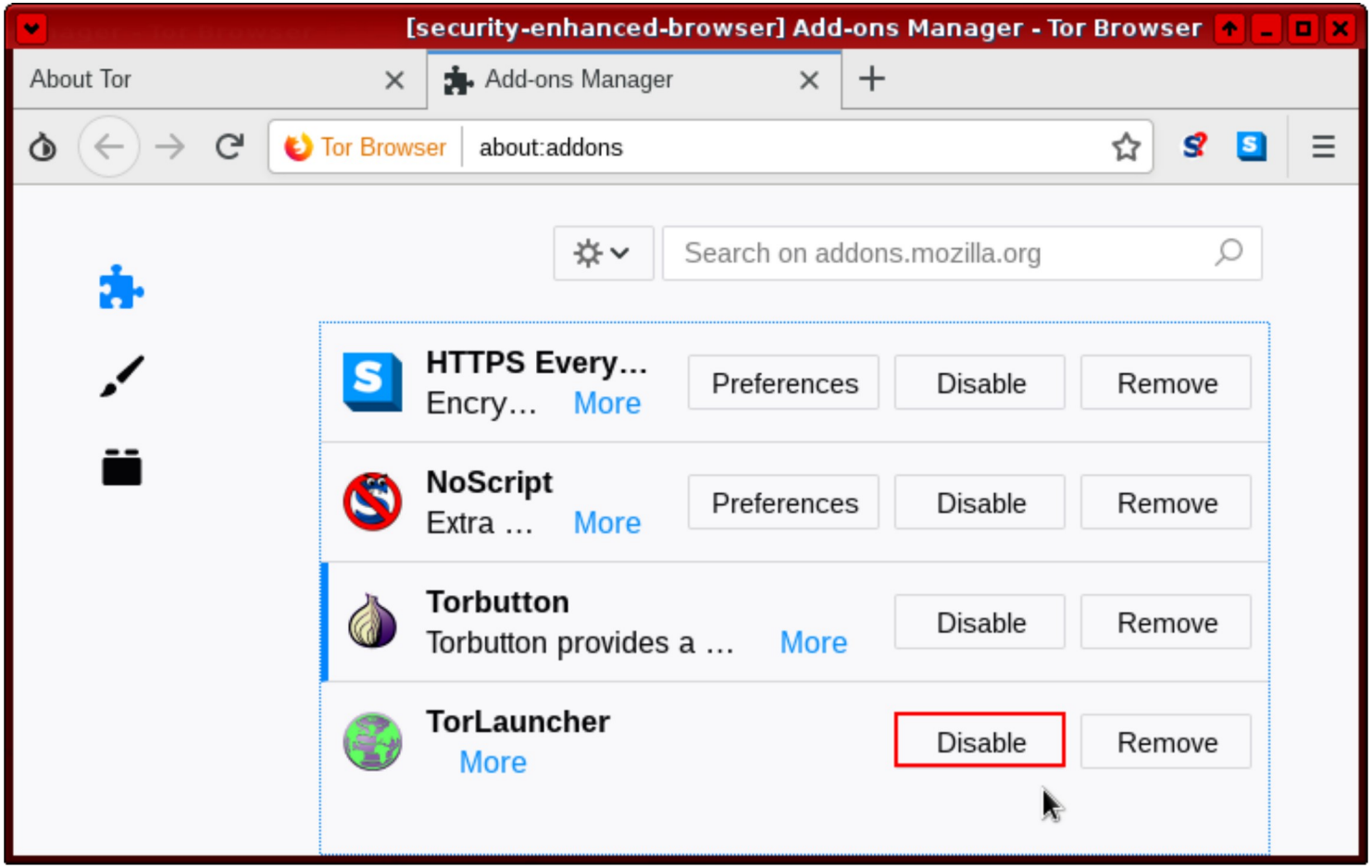
- **Windows:**
- **macOS:**
- **Linux:** Tested Debian 9, Tor Browser 8.0.6

1. Disable Tor Launcher extension.

In the Tor Browser address bar type; `about:addons` and press Enter.

Next, click the "Disable" Tor Launcher button.

(Image: Disable Tor Launcher)



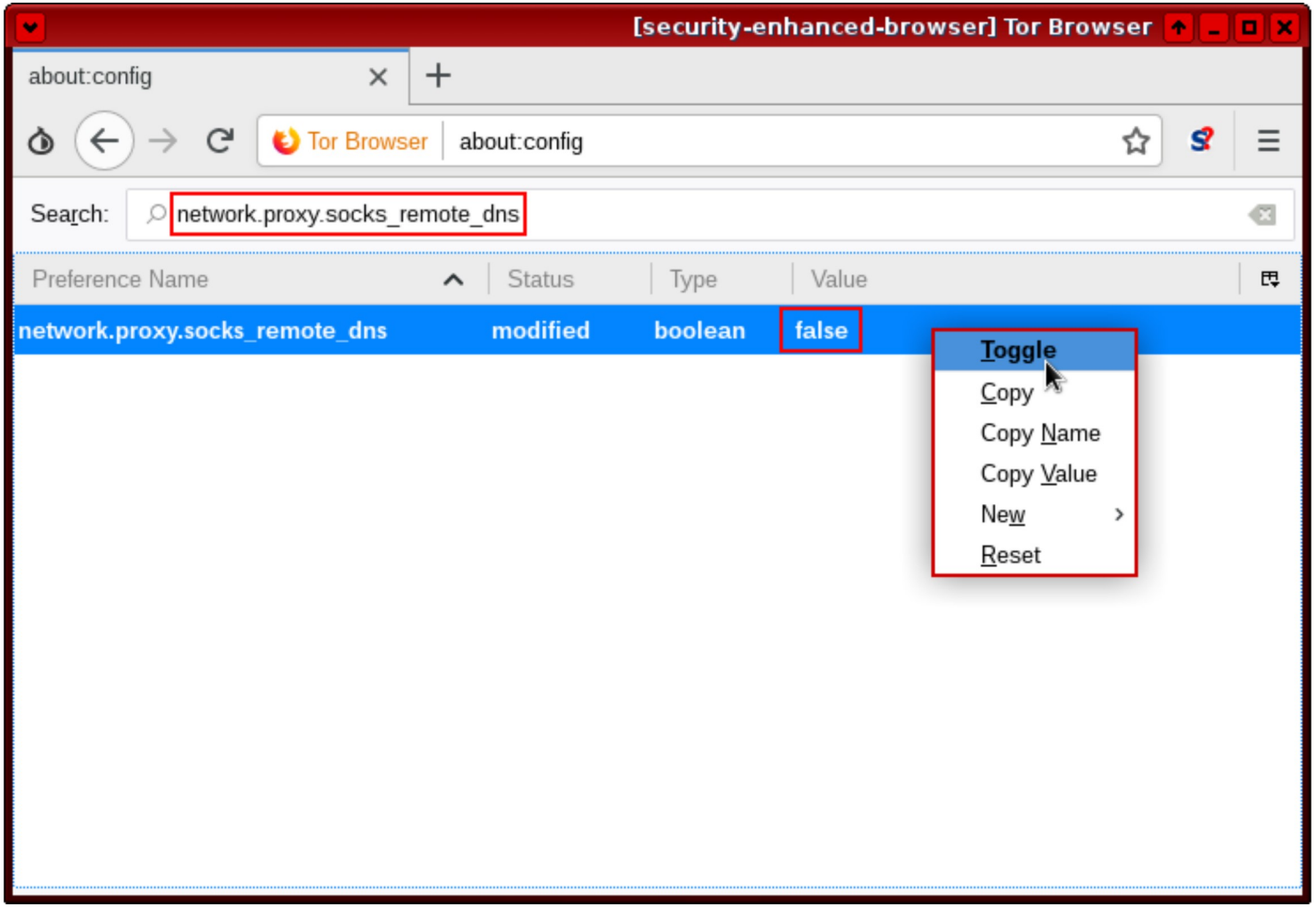
2. Disable `socks` network `DNS`.

In the Tor Browser address bar type; `about:config` and press "Enter".

Next, in the search bar type; `network.proxy.socks_remote_dns` and press "Enter".

Then right click `true and Toggle to false`.

(Image: Disable Tor Browser Socks Proxy DNS)

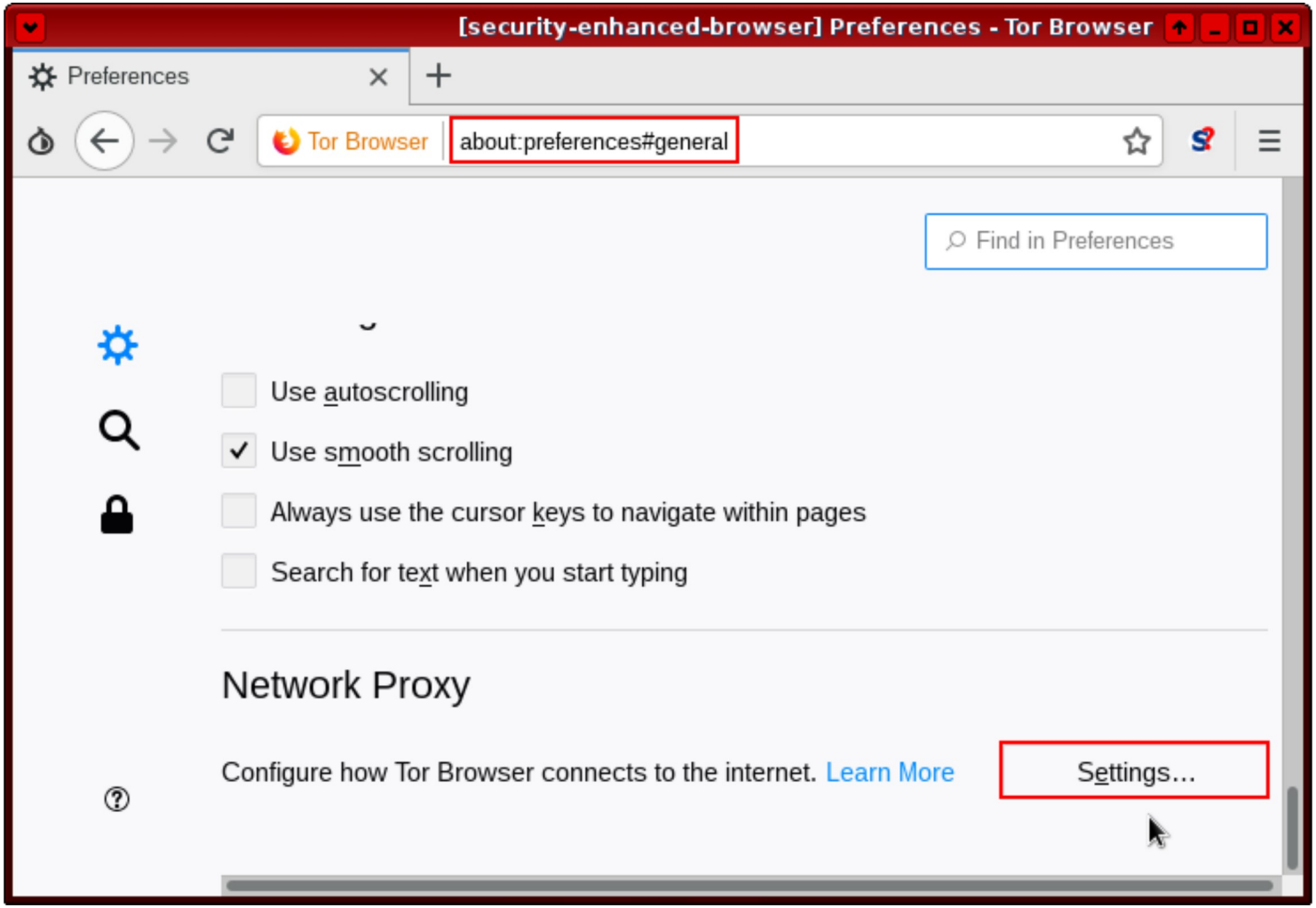


3. Switch Tor Browser settings from Manual Proxy to No Proxy.

In the Tor Browser address bar type; `about:preferences#general` and press "Enter".

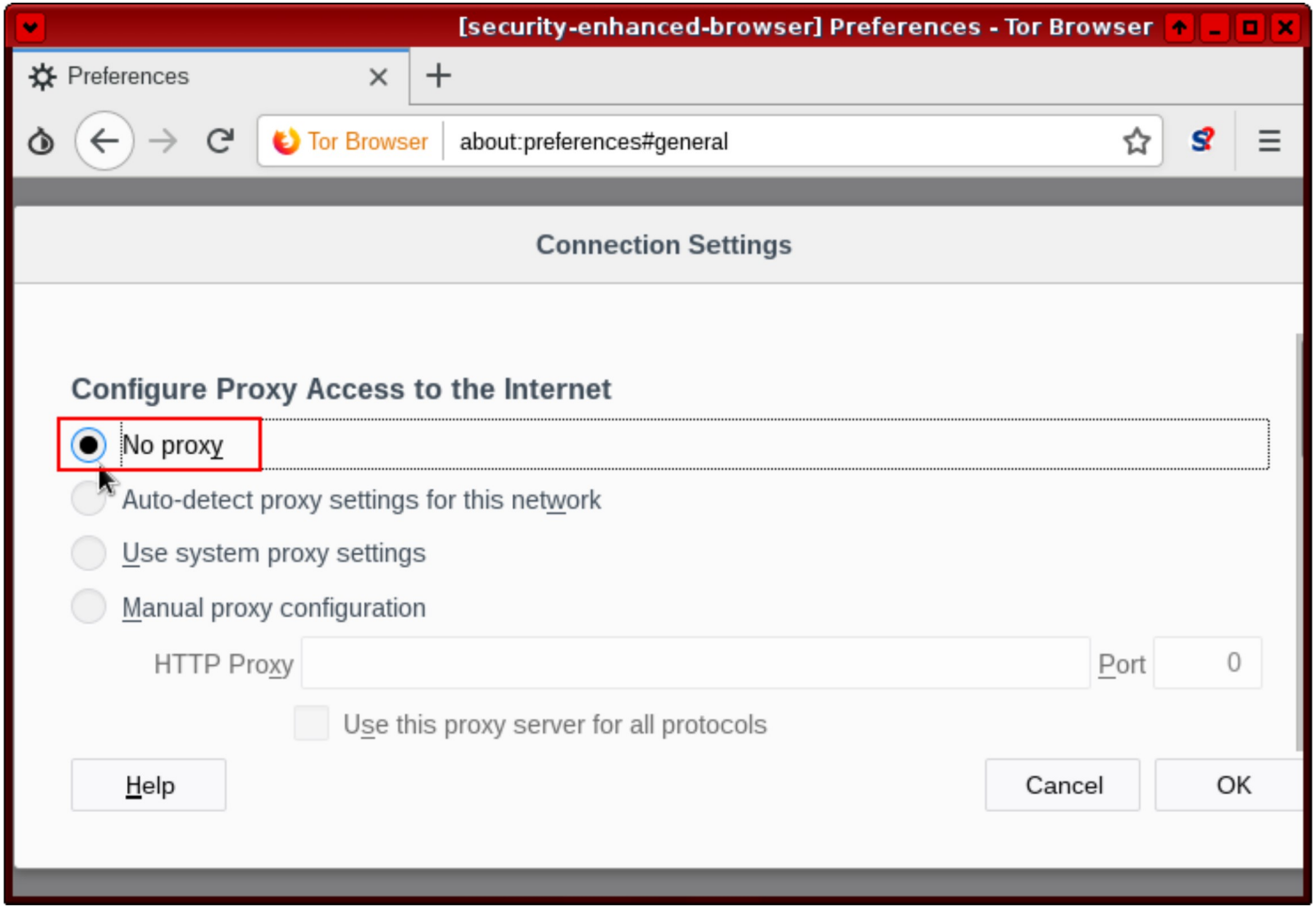
Next, scroll down to the Network Proxy section and click "Settings"

(Image: Tor Browser Connection Setting)



Then, change the connection settings from "Manual Proxy configuration" to "No proxy"

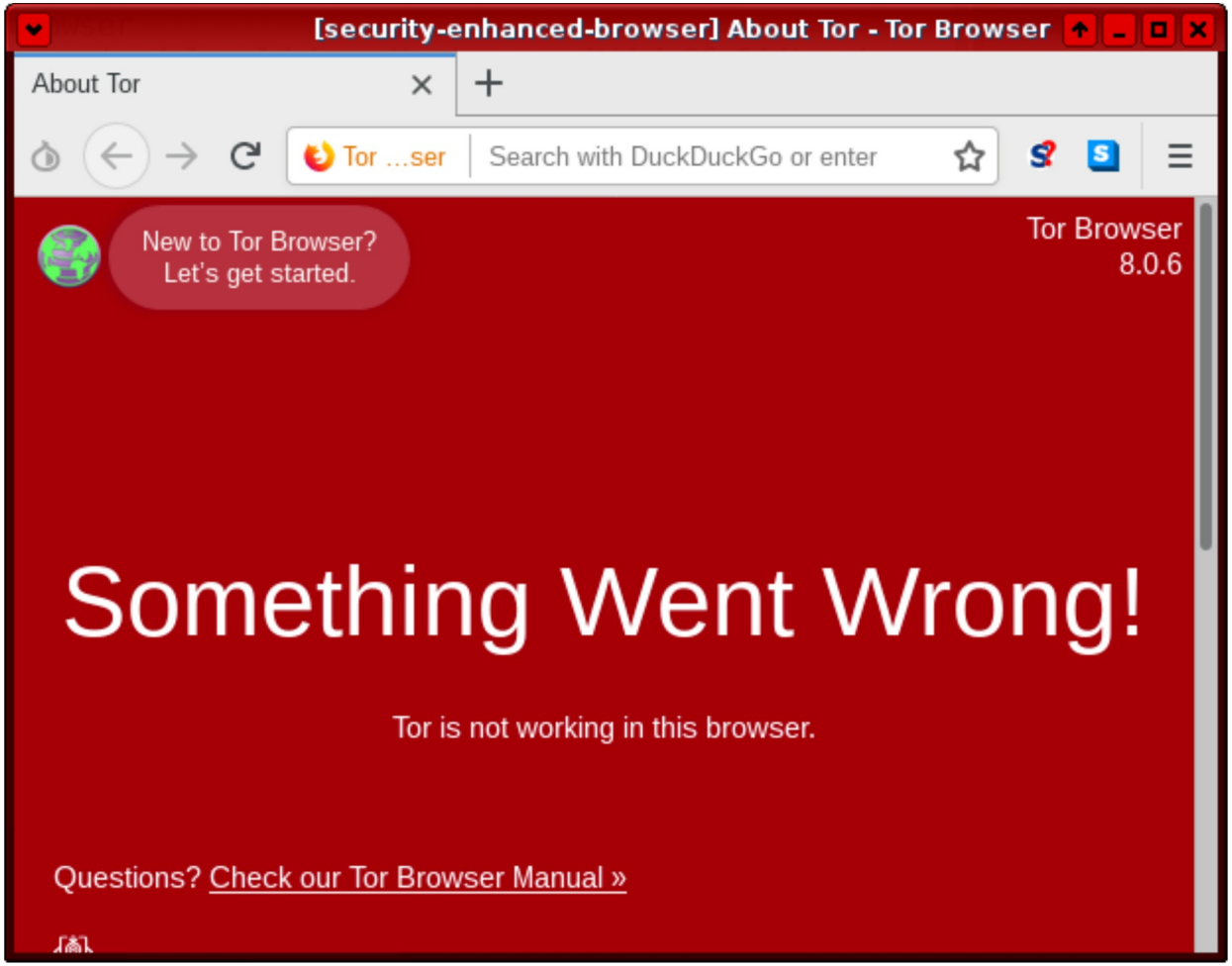
(Image: Tor Browser Proxy Configuration)



4. Restart Tor Browser

If configured correctly Tor Browser will have a red background with a message stating **"Something Went Wrong!"** Tor is not working in this browser.

(Image: Tor Browser "Something Went Wrong")



5. Done!

Start Tor Browser[edit]

- **Windows:** Change the icon.
- **macOS:**
- **Linux:** Run `~/.local/share/torbrowser/tbb/x86_64/tor-browser_en-US/Browser/start-tor-browser`.

Optional Steps[edit]

- **Windows:** Change the icon.

- **macOS:** Undetermined.
- **Linux:** Create a desktop shortcut.

Normalizing Tor Browser Behavior[edit]

- **Consider setting the Security Slider to "low".** The extra security features enabled by default come at a cost; they prevent some webpages from working properly. That is why other browsers disable them by default.

- **How to set preferences.** Click on the three horizontal bars in the upper-right corner of the Tor Browser window (the "hamburger" symbol). Select "Preferences" in the menu that pops up.

- **How to prevent Tor Browser from deleting the browsing and download history as well as all cookies when it closes.** By default Tor Browser always uses private browsing mode. To disable it: `Preferences → click the "Privacy" tab on the left-hand side → uncheck "Always use private browsing mode"`. The browser needs to restart for the changes to take effect.

  However, by disabling the private browsing mode, Tor Browser's built-in "long-term linkability" protections are deactivated. The user loses protection which aims to prevent "subsequent browser activity from being linkable to what you were doing before" whenever Tor Browser is closed or the 'New Identity' menu item is selected. The latter option involves a lot more than simply deleting all cookies. [11] If a user still wants to disable private browsing mode, then installing one or more anti-blocking extensions is advisable (see below).

- **Anti-tracking browser extensions.** The Tor Project FAQ states:

  > Some people have suggested we include ad-blocking software or anti-tracking software with Tor Browser. Right now, we do not think that's such a good idea. Tor Browser aims to provide sufficient privacy that additional add-ons to stop ads and trackers are not necessary. Using add-ons like these may cause some sites to break, which we don't want to do. Additionally, maintaining a list of "bad" sites that should be black-listed provides another opportunity to uniquely fingerprint users.

  Despite this opinion, if a user disables some of Tor Browser's own anti-tracking features (like private browsing mode; see above), then it is logical to to install one or more extensions that make it harder to track later browsing. The extensions Disconnect, Privacy Badger[12] and uBlock Origin are all open-source and are generally recommended. Research which one(s) may be most suitable in the circumstances; their use cases are different.

- **How to save a cookie for future use.** See these instructions on Tor Stack Exchange. This option requires the private browsing mode to be disabled.

- Tor Browser User Manual
- *The Design and Implementation of the Tor Browser*

- Tor Project FAQ - Tor Browser section
- https://github.com/pyllyukko/user.js/
- https://forums.whonix.org/t/todo-research-and-document-how-to-use-tor-browser-for-security-not-anonymity-how-to-use-tbb-using-clearnet

---

No comments for now due to spam. Use Whonix forums instead.

https | (forcing) onion

Follow: Twitter | Facebook | gab.ai | Stay Tuned | Whonix News

Share: Twitter | Facebook

This is a wiki. Want to improve this page? Help is welcome and volunteer contributions are happily considered! Read, understand and agree to Conditions for Contributions to Whonix ™, then Edit! Edits are held for moderation.