

Using Tor Browser on Android: Quick start

Updated: 2021-03-17

Preface

1. Understand Tor
2. Download and install Tor Browser
 - 2.1. Get Tor Browser via Tor Project's website or a mirror
 - 2.2. Get Tor Browser via F-Droid
3. Set up Tor Browser
 - 3.1. Connecting to Tor
 - 3.2. Tor Browser security setting
 - 3.3. Blocking unencrypted connections with HTTPS Everywhere

Preface

This guide is a quick start guide for getting started with Tor Browser on Android. Please also read the separate guide "Using Tor" for warnings, important details and general information about Tor.

This guide is based on Tor Browser 10.0.12 on Android.

1. Understand Tor

- [Using Tor § 1. Introduction](#)

Understand Tor, what it provides, and what it doesn't provide. Though Tor is used by millions of people around the world, determine for yourself whether or not Tor is suitable for you to use.

2. Download and install Tor Browser

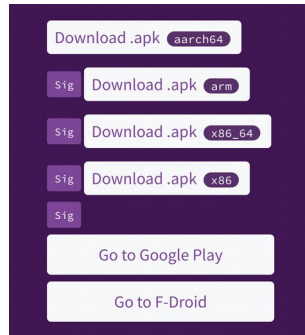
- [Using Tor § 2. Download and install](#)

Tor Browser on Android is available via:

- Tor Project's website and mirrors
- F-Droid
- Google Play

2.1. Get Tor Browser via Tor Project's website or a mirror

Note: There are 4 versions (CPU architecture targets) of Tor Browser for Android that are downloadable. If you don't know which version you need and cannot afford to do downloads by trial and error, try "aarch64" if you own a device that is less than a few years old. Alternatively, downloading Tor Browser via F-Droid may choose the correct architecture for you.



Download and install Tor Browser from Tor Project's official website or one of their mirrors.

Tor Project official website:

- cleartnet: <https://www.torproject.org/download/>
- onion: <http://expyuzz4wqqyqhjn.onion/download/>

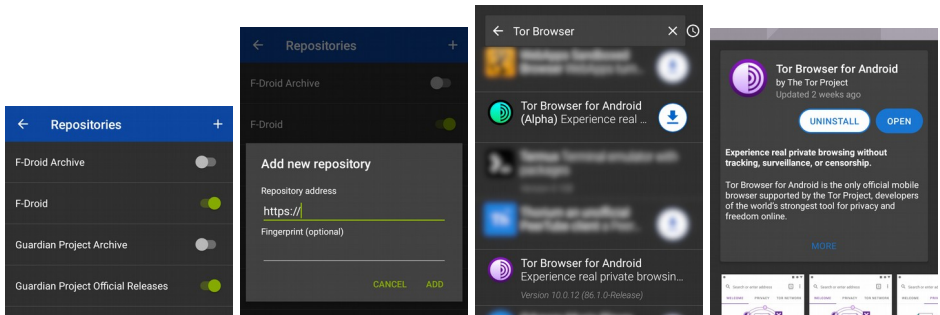
A short list of mirrors:

- <https://tor.calyxinstitute.org/>
- <https://tor.ccc.de/>
- <https://tor.eff.org/>

After downloading Tor Browser, installing it is straight-forward:

1. Open the .apk file.
2. Click "Install" when asked to install the app.
3. When you see the large tick symbol, Tor Browser has been installed.

2.2. Get Tor Browser via F-Droid



If you have set up F-Droid, you can download and install Tor Browser using F-Droid. Tor Browser is contained in the Guardian Project repository.

Firstly, add Guardian Project repository to F-Droid:

1. Open F-Droid and go to "Settings" → "Repositories".
2. Click on the "+" icon at the top-right to add a new repository.
3. Input the repository address:
 - <https://guardianproject.info/fdroid/repo/>
4. Input the repository fingerprint: (Do not input any spaces)
 - B7C2 EEFD 8DAC 7806 AF67 DFCD 92EB 1812 6BC0 8312
A7F2 D6F3 862E 4601 3C7A 6135
5. Click "Add".
6. Confirm "Guardian Project Official Releases" is added to the list:

Next, download and install Tor Browser via F-Droid:

1. Update all repositories.
2. Search for "Tor Browser".
3. In the list of results, select "Tor Browser for Android".
4. Click "Install" in F-Droid.
5. Click "Install" when asked to install the app.
6. When you see the large tick symbol, Tor Browser is installed.

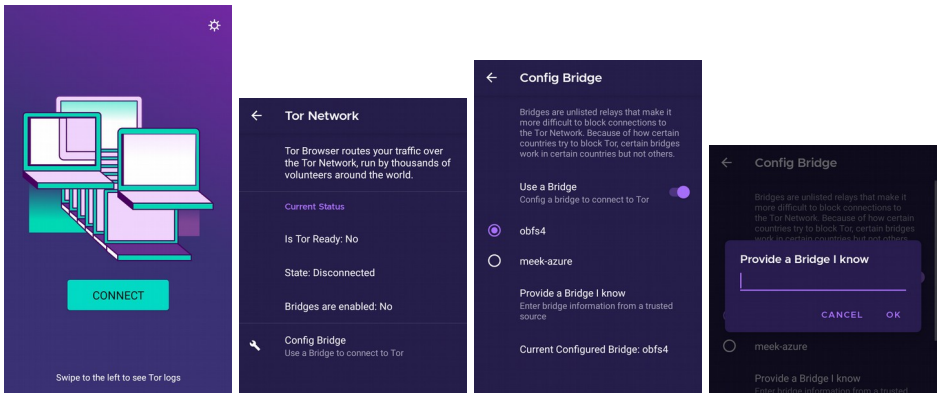
3. Set up Tor Browser

➤ Using Tor § 3. Setting up Tor Browser

Set up Tor Browser's connection settings, security setting and HTTPS Everywhere.

3.1. Connecting to Tor

➤ Using Tor § 3.1. Connecting to Tor



When you open Tor Browser, there is a screen that has a "Connect" button, and a settings button (the cog icon at the top-right) that allows you to configure network settings.

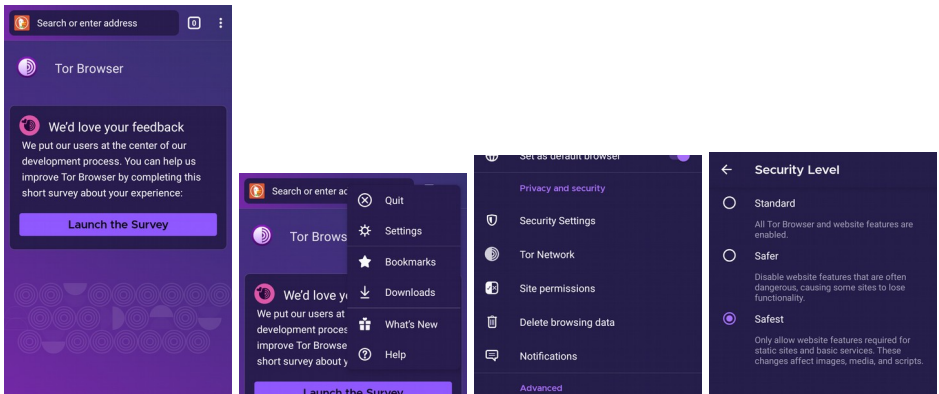
If your local network and jurisdiction allow Tor traffic, try clicking on "Connect" without any further configuration.

Otherwise, you may need to configure a Tor bridge:

1. Click on the cog icon at the top-right.
2. Click on "Config Bridge".
3. Enable "Use a Bridge", then select a bridge:
 - "obfs4" built-in bridge
 - "meek-azure" built-in bridge
 - Input a bridge you already know about

3.2. Tor Browser security setting

➤ Using Tor § 3.2. Tor Browser security setting



Tor Browser has a built-in three-level security setting with three values: "Standard" (default), "Safer" and "Safest".

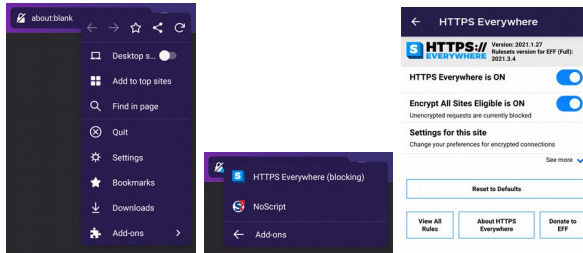
JavaScript presents a significant threat to user privacy and security. You should use "Safest" whenever possible, use "Safer" if JavaScript is required to access important websites, consider not accessing less-important sites that require JavaScript. Never use "Standard" unless "Safer" is inadequate and HTTPS Everywhere is configured to block unencrypted connections. Ensure you don't accidentally connect to websites over unencrypted connections while using "Standard".

To change the security setting:

1. Click on the "three dots" icon at the top-right.
2. Click on "Settings" → "Security Settings".
3. Adjust the setting to the appropriate value.

3.3. Blocking unencrypted connections with HTTPS Everywhere

- Using Tor § 3.3. Blocking unencrypted connections with HTTPS Everywhere



Unencrypted connections are dangerous, since any actor between Tor exit nodes and websites (including the exit node) can eavesdrop on your traffic, even modify your traffic by injecting malware or altering content.

To block unencrypted connections:

1. Click on the "three dots" icon at the top-right.
2. Click on "Add-ons" → "HTTPS Everywhere".
3. Ensure HTTPS Everywhere is configured to the following:
 - "HTTPS Everywhere" is "ON" (This is the default)
 - "Encrypt All Sites Eligible" is "ON"

If "Add-ons" is not listed when attempting step 2, open a new tab, open the URL `about:blank`, then try the above steps again.