Tor Browser Help

**Tor**
How Tor works.

**Troubleshooting**
What to do if Tor Browser doesn't work.

**Circumvention**
What to do if the Tor network is blocked.

**Bridges**
What bridges are and how to use them.

**Uninstalling**
How to remove Tor Browser from your system.
Tor

Tor is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor works by sending your traffic through three random servers (also known as relays) in the Tor network, before the traffic is sent out onto the public Internet.

The image above illustrates a user browsing to different websites over Tor. The green monitors represent relays in the Tor network, while the three keys represent the layers of encryption between the user and each relay.

Tor will anonymize the origin of your traffic, and it will encrypt everything between you and the Tor network. Tor will also encrypt your traffic inside the Tor network, but it cannot encrypt your traffic between the Tor network and its final destination.

If you are communicating sensitive information, for example when logging on to a website with a username and password, make sure that you are using HTTPS (e.g. https://torproject.org/, not http://torproject.org/).
Troubleshooting

The Tor Browser should get you online automatically after clicking the "Connect" button on the start up screen.

If it doesn't connect, there may be a simple fix. Try each of the following:

- Make sure another Tor Browser is not already running. If you're not sure if Tor Browser is running, restart your computer.

- 'Allow' Tor in your antivirus program.

- Temporarily disable your firewall.

- Delete Tor Browser and install it again. If updating, do not overwrite your previous Tor Browser files.

If you still can't connect, your internet service provider might be censoring connections to Tor. Follow the instructions in the Circumvention section.

If the above steps do not address your problem, email help@rt.torproject.org with your operating system, the details of your problem, and what you've already tried.
Circumvention

Some firewalls can detect and block connections to Tor. The Tor Browser includes some circumvention tools for getting around blocking firewalls. These circumvention tools are called Pluggable Transports. To turn them on, click "Configure" in the Tor launcher window.

Select yes when asked if your internet service provider blocks connections to Tor.

Select "Connect with provided bridges". Tor Browser has three Pluggable Transports to choose from. If one fails to get you online, try selecting a different transport.

If you try all three transports, and none of them get you online, select "Enter custom bridges", and enter bridges manually. Read the Getting Bridges section for instructions on getting custom bridges.

More Information
Tor Browser Help
**Bridges**

Bridges are quiet gateways into the Tor Network. Like Tor relays, they are run by volunteers. Unlike relays, they are not listed publicly. Using bridges disguise the fact that one is using Tor.

Currently there are five bridge types, or transports, available. More are being developed.

<table>
<thead>
<tr>
<th>Transport</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORPort</td>
<td>Requesting 'bridges' without specifying the bridge type, will return ORPort bridges, also called Vanilla bridges. ORPort bridges are NOT reliable for circumventing censorship or national firewalls. ORPort bridges can be useful as trusted entry points into the Tor network.</td>
</tr>
<tr>
<td>obfs2</td>
<td>Censors have learned how to identify obfs2 bridges. This transport is being deprecated.</td>
</tr>
<tr>
<td>obfs3</td>
<td>Obfsproxy disguises Tor traffic as random noise. obfs3 bridges work almost everywhere. A few obfs3 bridges have been blocked.</td>
</tr>
<tr>
<td>Scramblesuit</td>
<td>Scramblesuit is an additional tool for the obfsproxy transport. Scramblesuit bridges are designed to be hard to identify and hard to block.</td>
</tr>
<tr>
<td>FTE</td>
<td>Format-Transforming Encryption disguises Tor traffic as web (HTTP) traffic or other types of internet traffic. FTE bridges are effective, but in limited supply.</td>
</tr>
</tbody>
</table>

(Note that flashproxy is a Pluggable Transport, but does not rely on bridges.)

There are four ways to get a bridge.


2. Email bridges@bridges.torproject.org from a gmail or yahoo email address. Put get bridges in the body for ORPort bridges or transport=obfs3 for obfs3 bridges.

3. Politely ask a human at help@rt.torproject.org if you cannot access either of the first two methods.

4. Install and configure a Tor instance to be bridge for yourself. The computer acting as a bridge must have uncensored internet access to the Tor network. A full installation guide can be found at [https://www.torproject.org/projects/obfsproxy-debian-instructions.html.en](https://www.torproject.org/projects/obfsproxy-debian-instructions.html.en)
Enter the bridge information you get from any of the above steps in Tor-launcher.

Choose yes when asked if your Internet Service Provider blocks connections to the Tor network. Select 'Use custom bridges' and enter each bridge identifier on its own line.

Click Connect. Using bridges slow down the connection. If the connection fails, the bridges you received may be down. Get more and try again.

More Information
Tor Browser Help
Uninstalling

The Tor Browser does not affect any of the existing software or settings on your computer. Uninstalling Tor Browser will not affect your system's software or settings either.

Removing the Tor Browser from your system is simple:

1. Locate your Tor Browser folder. The default location is your Desktop.
2. Delete the Tor Browser folder.
3. Empty your Trash

Note that your operating system's standard "Uninstall" utility is not used.