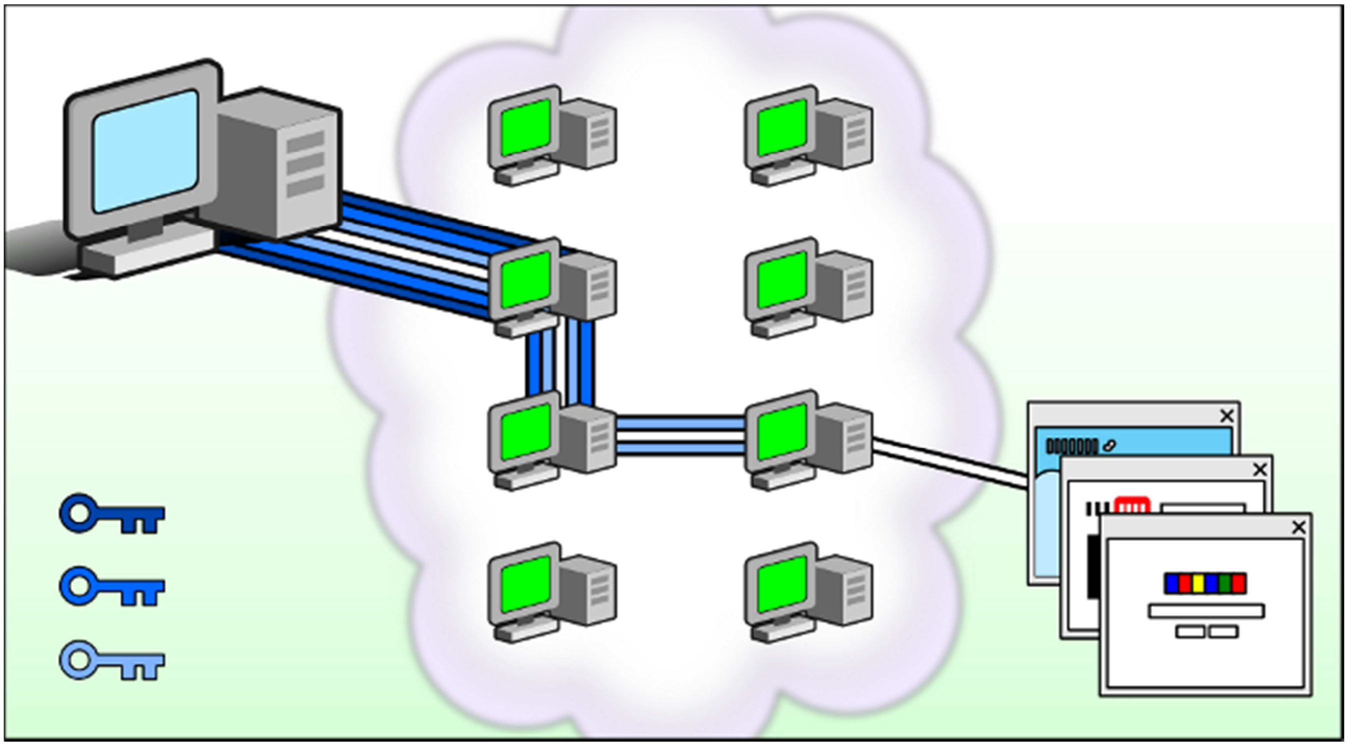
IMPROVE YOUR PRIVACY AND SECURITY ON THE INTERNET USING TOR

This user manual contains information about how to download Tor, how to use it, and what to do if Tor is unable to connect to the network. If you can't find the answer to your question in this document, email help@rt.torproject.org.

HOW TOR WORKS

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/).

HOW TO DOWNLOAD TOR

The bundle we recommend to most users is the Tor Browser Bundle. This bundle contains a browser preconfigured to safely browse the Internet through Tor, and requires no installation. You download the bundle, extract the archive, and start Tor.

There are two different ways to get hold of the Tor software. You can either browse to the Tor Project website and download it there, or you can use GetTor, the email autoresponder.

How to get Tor via email

To receive the English Tor Browser Bundle for Windows, send an email to gettor@torproject.org with **windows** in the body of the message. You can leave the subject blank.

You can also request the Tor Browser Bundle for Mac OS X (write **macos-i386**), and Linux (write **linux-i386** for 32-bit systems or **linux-x86_64** for 64-bit systems).

If you want a translated version of Tor, write **help** instead. You will then receive an email with instructions and a list of available languages.

Note: The Tor Browser Bundles for Linux and Mac OS X are rather large, and you will not be able to receive any of these bundles with a Gmail, Hotmail or Yahoo account. If you cannot receive the bundle you want, send an email to help@rt.torproject.org and we will give you a list of website mirrors to use.

Tor for smartphones

You can get Tor on your Android device by installing the package named *Orbot*. For information about how to download and install Orbot, please see the Tor Project website.

We also have experimental packages for Nokia Maemo/N900 and Apple iOS.

How to verify that you have the right version

Before running the Tor Browser Bundle, you should make sure that you have the right version.

The software you receive is accompanied by a file with the same name as the bundle and the extension **.asc**. This .asc file is a GPG signature, and will allow you to verify the file you've downloaded is exactly the one that we intended you to get.

Before you can verify the signature, you will have to download and install GnuPG:

Windows: http://gpg4win.org/download.html
Mac OS X: http://macgpg.sourceforge.net/
Linux: Most Linux distributions come with GnuPG preinstalled.

Please note that you may need to edit the paths and the commands used below to get it to work on your system.

Erinn Clark signs the Tor Browser Bundles with key 0x63FEE659. To import Erinn's key, run:

```
gpg --keyserver hkp://keys.gnupg.net --recv-keys 0x63FEE659
```

After importing the key, verify that the fingerprint is correct:

```
gpg --fingerprint 0x63FEE659
```

You should see:

```
pub 2048R/63FEE659 2003-10-16 Key fingerprint = 8738 A680 B84B 3031 A630 F2DB 416F 0610 63FE E659 uid
Erinn Clark <erinn@torproject.org> uid Erinn Clark <erinn@debian.org> uid Erinn Clark <erinn@double-
helix.org> sub 2048R/EB399FD7 2003-10-16
```

To verify the signature of the package you downloaded, run the following command:

```
gpg --verify tor-browser-2.2.33-2_en-US.exe.asc tor-browser-2.2.33-2_en-US.exe
```

The output should say *"Good signature"*. A bad signature means that the file may have been tampered with. If you see a bad signature, send details about where you downloaded the package from, how you verified the signature, and the output from GnuPG in an email to help@rt.torproject.org.

Once you have verified the signature and seen the *"Good signature"* output, go ahead and extract the package archive. You should then see a directory similar to **tor-browser_en-US**. Inside that directory is another directory called **Docs**, which contains a file called **changelog**. You want to make sure that the version number on the top line of the changelog file matches the version number in the filename.

How to use the Tor Browser Bundle

After downloading the Tor Browser Bundle and extracting the package, you should have a directory with a few files in it. One of the files is an executable called "Start Tor Browser" (or "start-tor-browser", depending on your operating system).

When you start the Tor Browser Bundle, you will first see Vidalia start up and connect you to the Tor network. After that, you will see a browser confirming that you are now using Tor. This is done by displaying https://check.torproject.org/. You can now browse the Internet through Tor.

Please note that it is important that you use the browser that comes with the bundle, and not your own browser.

What to do when Tor does not connect

Some users will notice that Vidalia gets stuck when trying to connect to the Tor network. If this happens, make sure that you are connected to the Internet. If you need to connect to a proxy server, see *How to use an open proxy* below.

If your normal Internet connection is working, but Tor still can't connect to the network, try the following; open the Vidalia control panel, click on *Message Log* and select the *Advanced* tab. It may be that Tor won't connect because:

Your system clock is off: Make sure that the date and time on your system is correct, and restart Tor. You may need to synchronize your system clock with an Internet time server.

You are behind a restrictive firewall: To tell Tor to only try port 80 and port 443, open the Vidalia control panel, click on *Settings* and *Network*, and tick the box that says *My firewall only lets me connect to certain ports*.

Your anti-virus program is blocking Tor: Make sure that your anti-virus program is not preventing Tor from making network connections.

If Tor still doesn't work, it's likely that your Internet Service Provider (ISP) is blocking Tor. Very often this can be worked around with **Tor bridges**, hidden relays that aren't as easy to block.

If you need help with figuring out why Tor can't connect, send an email to help@rt.torproject.org and include the relevant parts from the log file.

How to find a bridge

To use a bridge, you will first have to locate one; you can either browse to bridges.torproject.org, or you can send an email to bridges@torproject.org. If you do send an email, please make sure that you write **get bridges** in the body of the email. Without this, you will not get a reply. Note that you need to send this email from either a gmail.com or a yahoo.com address.

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable. There is no guarantee that the bridge you are using now will work tomorrow, so you should make a habit of updating your list of bridges every so often.

How to use a bridge

Once you have a set of bridges to use, open the Vidalia control panel, click on *Settings*, *Network* and tick the box that says *My ISP blocks connections to the Tor network*. Enter the bridges in the box below, hit *OK* and start Tor again.

How to use an open proxy

If using a bridge does not work, try configuring Tor to use any HTTPS or SOCKS proxy to get access to the Tor network. This means even if Tor is blocked by your local network, open proxies can be safely used to connect to the Tor Network and on to the uncensored Internet.

The steps below assume you have a functional Tor/Vidalia configuration, and you have found a list of HTTPS, SOCKS4, or SOCKS5 proxies.

1. Open the Vidalia control panel, click on *Settings*.
2. Click *Network*. Select *I use a proxy to access the Internet*.
3. On the *Address* line, enter the open proxy address. This can be a hostname or an IP Address.
4. Enter the port for the proxy.
5. Generally, you do not need a username and password. If you do, enter the information in the proper fields.
6. Choose the *Type* of proxy you are using, whether HTTP/HTTPS, SOCKS4, or SOCKS5.
7. Push the *OK* button. Vidalia and Tor are now configured to use a proxy to access the rest of the Tor network.

FREQUENTLY ASKED QUESTIONS

This section will answer some of the most common questions. If your question is not mentioned here, please send an email to help@rt.torproject.org.

Unable to extract the archive

If you are using Windows and find that you cannot extract the archive, download and install 7-Zip.

If you are unable to download 7-Zip, try to rename the file from .z to .zip and use winzip to extract the archive. Before renaming the file, tell Windows to show file extensions:

Windows XP

1. Open *My Computer*
2. Click on *Tools* and choose *Folder Options...* in the menu
3. Click on the *View* tab
4. Uncheck *Hide extensions for known file types* and click *OK*

Windows Vista

1. Open *Computer*
2. Click on *Organize* and choose *Folder and search options* in the menu
3. Click on the *View* tab
4. Uncheck *Hide extensions for known file types* and click *OK*

Windows 7

1. Open *Computer*

2. Click on *Organize* and choose *Folder and search options* in the menu
3. Click on the *View* tab
4. Uncheck *Hide extensions for known file types* and click *OK*

Vidalia asks for a password

You should not have to enter a password when starting Vidalia. If you are prompted for one, you are likely affected by one of these problems:

You are already running Vidalia and Tor: For example, this situation can happen if you installed the Vidalia bundle and now you're trying to run the Tor Browser Bundle. In that case, you will need to close the old Vidalia and Tor before you can run this one.

Vidalia crashed, but left Tor running: If the dialog that prompts you for a control password has a Reset button, you can click the button and Vidalia will restart Tor with a new random control password. If you do not see a Reset button, or if Vidalia is unable to restart Tor for you; go into your process or task manager, and terminate the Tor process. Then use Vidalia to restart Tor.

For more information, see the FAQ on the Tor Project website.

Flash does not work

For security reasons, Flash, Java, and other plugins are currently disabled for Tor. Plugins operate independently from Firefox and can perform activity on your computer that ruins your anonymity.

Most YouTube videos work with HTML5, and it is possible to view these videos over Tor. You need to join the HTML5 trial on the YouTube website before you can use the HTML5 player.

Note that the browser will not remember that you joined the trial once you close it, so you will need to re-join the trial the next time you run the Tor Browser Bundle.

Please see the Torbutton FAQ for more information.

I want to use another browser

For security reasons, we recommend that you only browse the web through Tor using the Tor Browser Bundle. It is technically possible to use Tor with other browsers, but by doing so you open yourself up to potential attacks.

Why Tor is slow

Tor can sometimes be a bit slower than your normal Internet connection. After all, your traffic is sent through many different countries, sometimes across oceans around the world!