Protektor Services

Windows Manual 11.5

Online Anonymity with Tor Browser Bundle

Introduction

Protektor Services Manual version 11.5
A new edition of the Protektor Services manual series.

Protektor Services wants to assist by providing the right tools to help the people that need them without keeping them in the dark on how things actually work.

Protektor Services manual series aims to do this by:

- Creating user friendly manuals
- Providing manuals for all major operating systems, it doesn't matter if you use Windows, Apple or Linux.
- Using only open source or open standards based software and solutions.
- Releasing the manuals under the Creative Commons Attribution 3.0 Unported License.
- Intermittent updates to the manuals to keep them current with real life computer systems.
- Making the source-file of the manuals available on request.

In case you have any questions about the manuals do not hesitate to contact me.

If you or your organization would like customized manuals or want to receive a full training for your people, do not hesitate to contact me

Tom

Contact

Email:	protektor.services@gmail.com or tom.keunen@gmail.com
Skype:	tomkeunen
Website:	http://protektor-blog.blogspot.com
GPG Key:	http://protektor-blog.blogspot.com/p/key.html

Acknowledgements

I want to thank Nikki for the patience while I am thinking about computer “stuff” during social time.

Legals

License

Keep your system up to date.

Keep your programs up to date.

Choose a strong password.

Create a user account for daily use.

Use anti-virus software

Do not forget to make regular backups.

Product Information

Website: https://www.torproject.org/projects/torbrowser.html.en
Version: 1.3.24, Released on April 30, 2011
System: Cross platform
License: BSD License

What is the Tor Browser Bundle?

The Tor Browser Bundle is a cross platform free software bundle that packages everything required to surf the internet more safely via the Tor network.
It also includes all that you need to help others to surf the internet more safely.

Why use the Tor Browser Bundle?

Using the Tor Browser Bundle to surf on the internet will keep your identity and location protected from anybody that might try to analyze your internet traffic.

It will also enable you to visit sites that might be blocked in your country.

The Tor Browser Bundle will also allow you to configure your own computer to become part of the Tor network and help other people to have more secure access to the internet.

The Tor Browser Bundle is a package that will enable you to surf more securely.

How the Tor Browser Bundle works?

The Tor Browser Bundle is a package that contains a version of the Firefox browser with plug-ins added for security and the Vidalia program.

The Vidalia program will provide the connection to the Tor network and will allow you to set up your own exit node.

Tor provides you the anonymity by tunneling your internet connection via multiple servers (called exit nodes) to mitigate traffic analysis.
It prevents the sites you visit from knowing who and where you are.

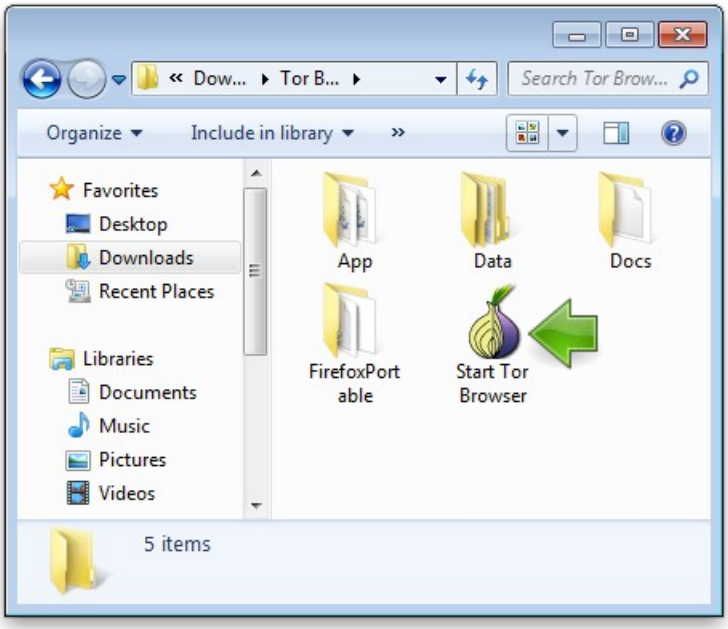
It is important to understand that when you use the Tor Browser Bundle only the browsing with the provided Firefox will have the benefits of using the Tor network.

Tor is not perfect, make sure you understand the limitations and act accordingly. More information can be found:
https://www.torproject.org/download/download.html.en#warning

How to use the Tor Browser Bundle?

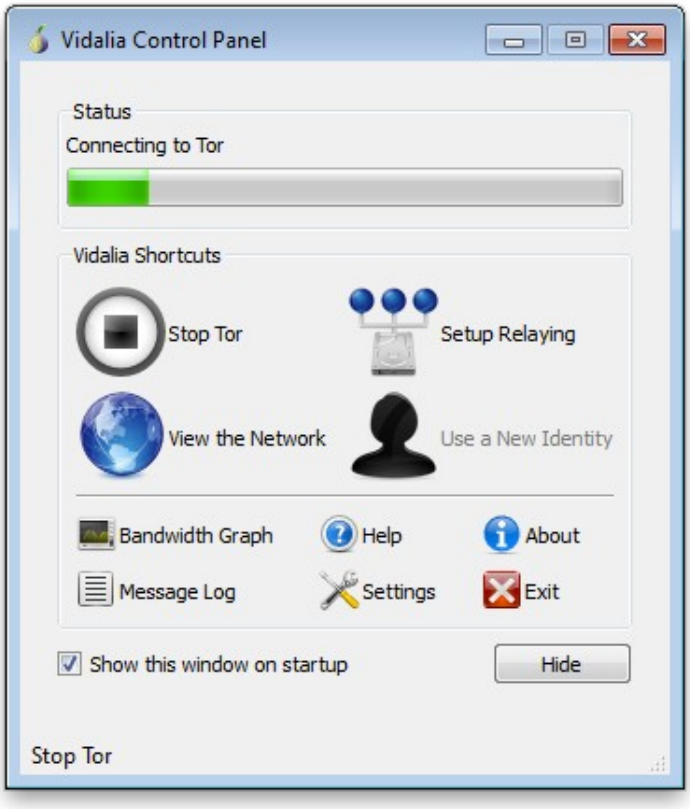
Download the package from the website and when finished double click on the icon to extract. You can extract the Tor Browser Bundle on your hard drive or if you want to on removable media such as a USB stick.

After installing you can start the Tor Browser Bundle by double clicking the icon.

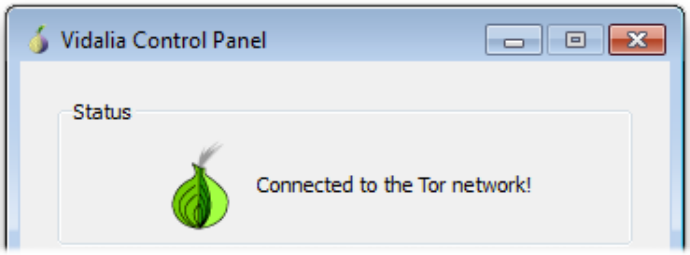


Vidalia will start and make a connection to the Tor network.

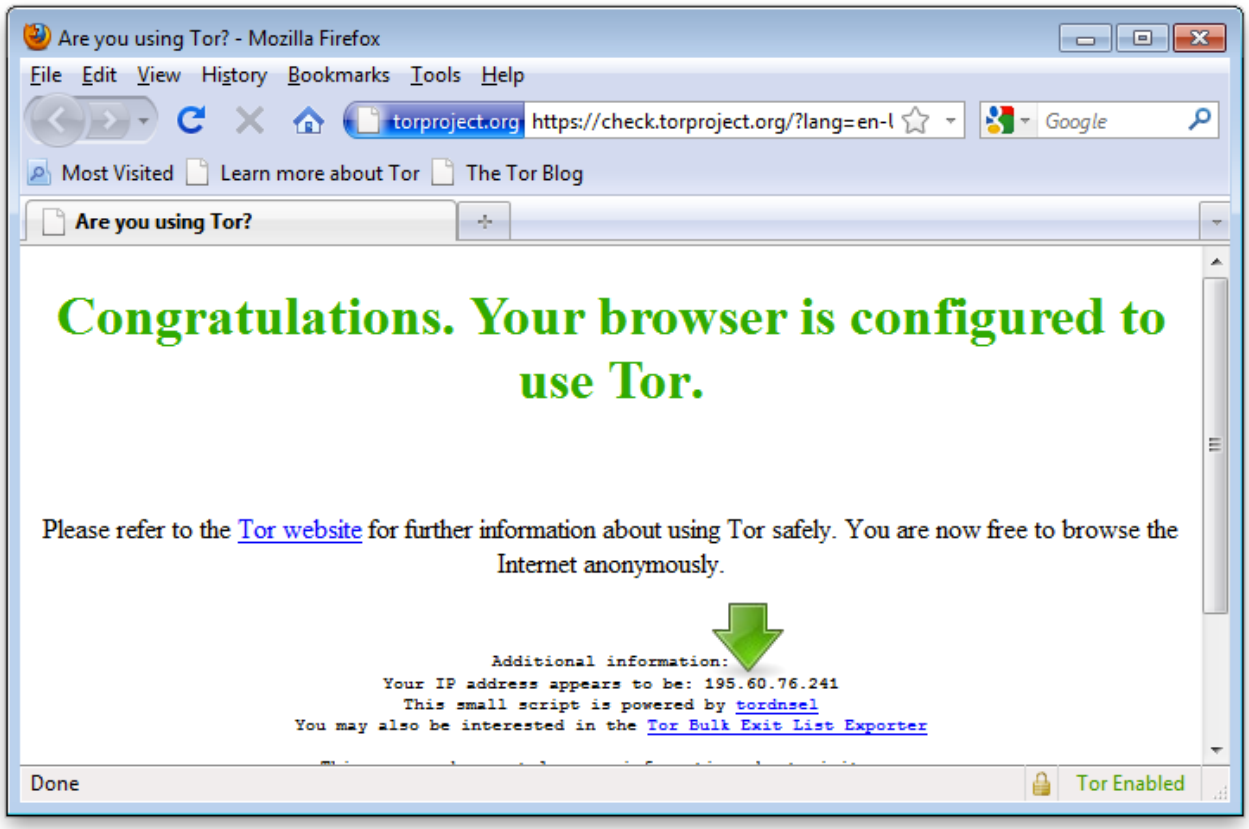
You don't have to do anything, this process will go automatically.



Once connected to the Tor network, Vidalia will notify you.



In the background the Firefox browser from the Tor Browser Bundle will start.



The Tor Bundle Browser Firefox will go to https://check.torproject.org to check if you are connected via the Tor network. If all goes well you should see a page like the one above.

The IP address shown in the above screenshot is not your actual IP address but the one of the Tor exit node you are using.

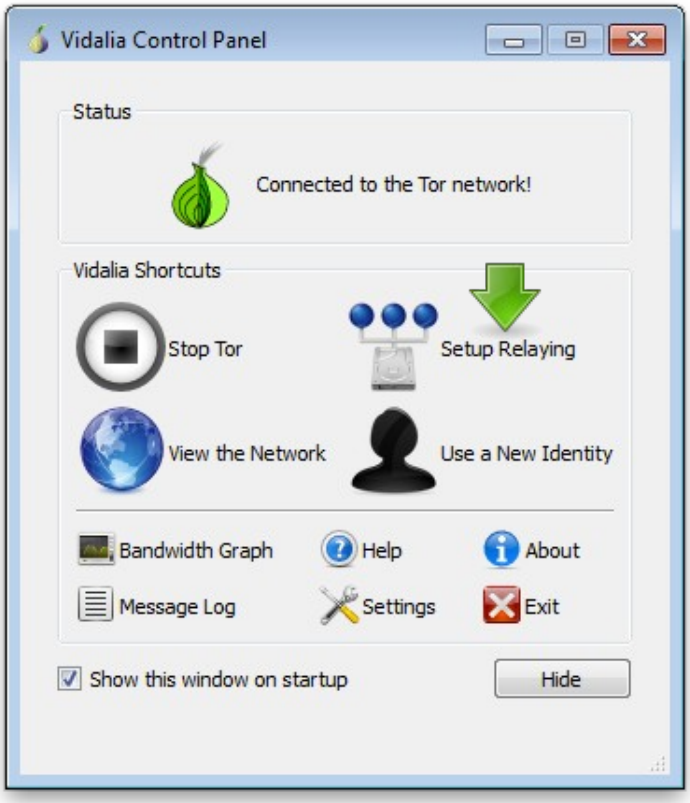
As long as you browse with that Firefox browser all your traffic will go through the Tor network.
When you are finished using it, click on Exit in the Vidalia control panel window.

The Tor network only exists thanks to the people that are supporting it.

By having the Tor Browser Bundle installed you can support the Tor network without having to give any money or leave the comfort of your own home.

On the next few pages it will be explained how you can support the Tor network by running an exit node.

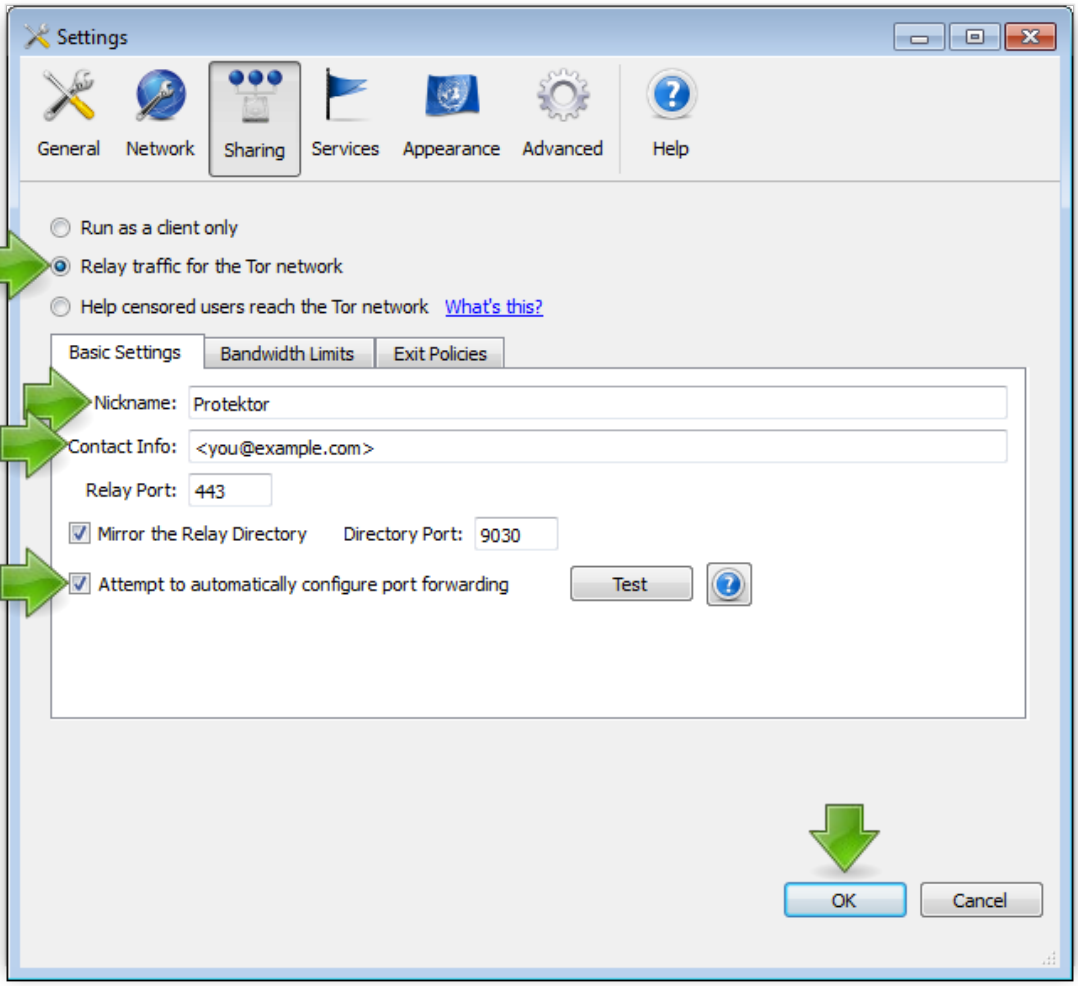
Start the Tor Browser Bundle and wait for the connection to the Tor network to establish.



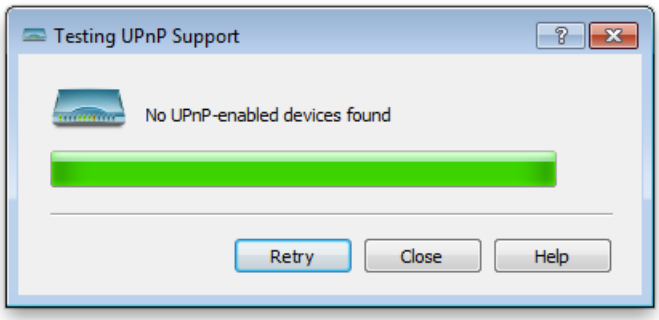
When the connection has been established click on Setup Relaying.

In the Sharing tab select Relay Traffic for the Tor network.

You can give your exit node a Nickname and you can give contact information.



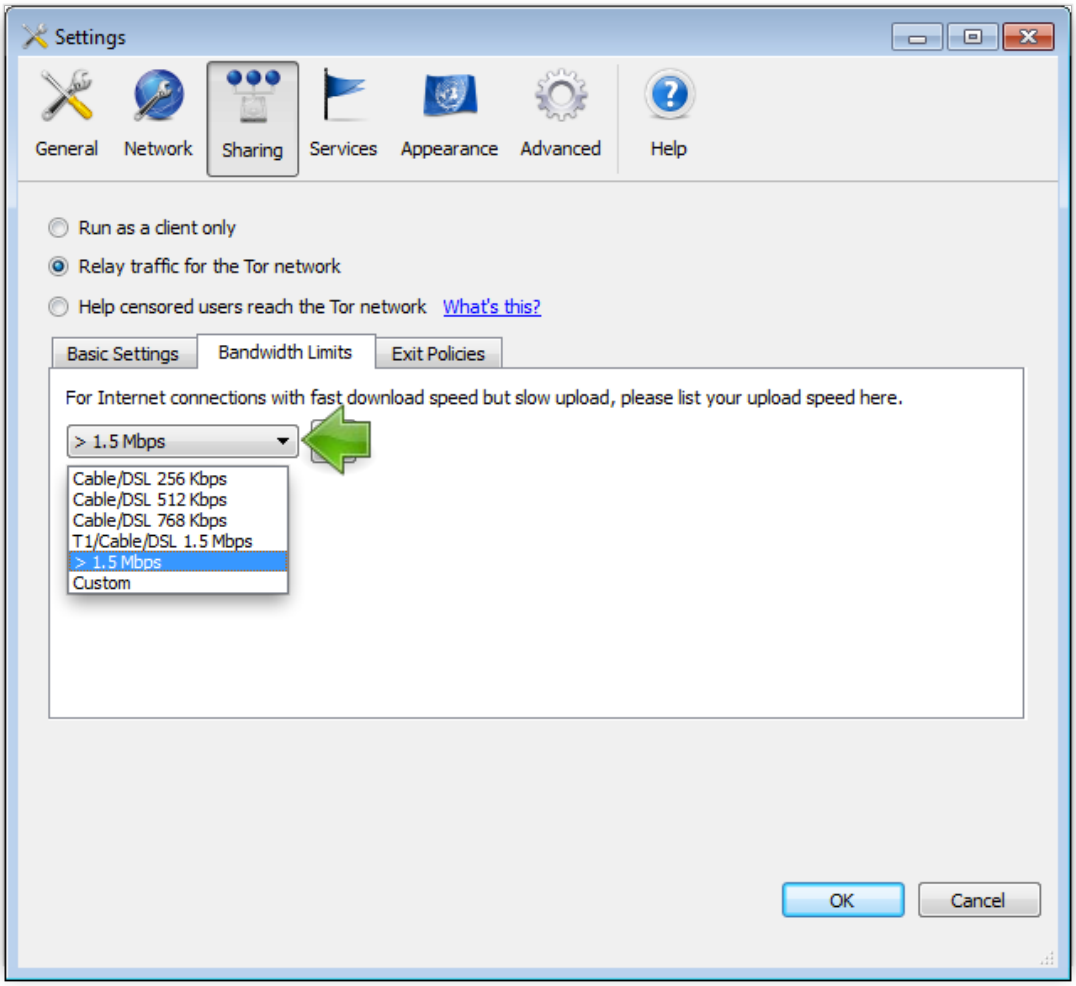
Select the Attempt to automatically configure port forwarding and click on Test.



If all goes well the test should be completed successfully. Click on Close

If the test fails you might want to check your firewall settings. Wireless routers or your modem might also have a firewall built in.

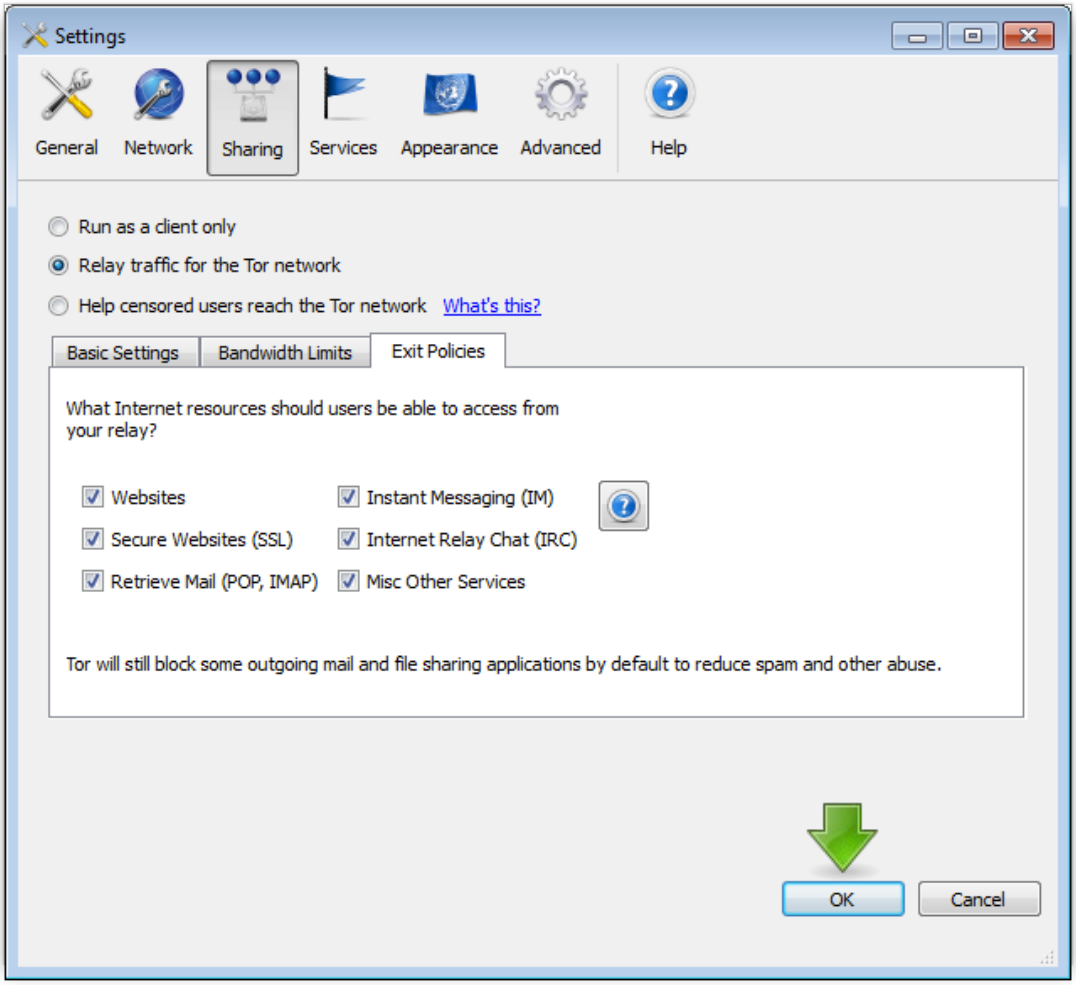
Next select the bandwidth Limits tab.



Here you will define how much bandwidth you are donating to the Tor network.

Via the drop down list you can set other values.

Click on the Exit Policies tab.



Last thing to configure are the services you will allow to pass via your exit node.

Deselect the ones you don't want to pass through your exit node.

When finished click on OK.

That is all it takes to run a Tor exit node from your own computer.

When you no longer want to run the Tor exit node, click on Exit in the Vidalia control panel.