Table of contents

- Configuring Torifier
  - ♦ Adding and removing programs
  - ♦ Torifying the entire system
  - ♦ Making your system support .onion names
  - ♦ The Options dialog box
    - ◊ The General panel
    - ◊ Connection options
      - · Bridges
      - · Proxy
      - · Firewall
    - ◊ The Exclusions panel
    - ◊ The Advanced panel
- Switching to a new identity
- Viewing Tor log

Configuring Torifier

This chapter describes all the configuration options in Torifier.

Torifier is designed to work almost "out of the box" - to start using it in most cases you are only required to specify programs that need to be torified. Some extra configuration may be required if you are behind a restrictive firewall or there are other network restrictions that prevent you from connecting to the Tor network using the default connection settings. Torifier also has a number of configuration options that help to make torification rules more flexible.

- Adding and removing programs
- Torifying the entire system
- Making your system support .onion names
- The Options dialog box

Adding and removing programs

To start tunneling a program through Tor, you simply need to add the program to the Torified Programs list. To add a program, click the Add Program button at the top right of the main Torifier window. The Select Program dialog box will come up. Select the executable of the program you want to be torified, then press the Open button.

To stop tunneling a program, you can either untick the check box on the left side of the program or remove the program from the list. To remove a program, select the program from the list, then press the Remove button.

Torifying the entire system

You can tell Torifier to tunnel your entire system through Tor by checking the Torify All Programs menu item in the File menu of the main Torifier window.

NOTE: When the Torify All Programs option is on, you cannot specify individual programs to be torified - the corresponding controls are grayed out.

Making your system support .onion names

Torifier can emulate system-wide support for .onion names meaning any program (including the ones not selected for torification) will be able to connect to a Tor hidden service. You can enable this feature by

checking the Enable System-wide .onion Support menu item in the Tools menu of the main Torifier window.

NOTE: The Hidden Service Protocol is a feature of Tor that allows a network server to hide its IP address while being publicly accessible. A collection of websites that utilize this feature of Tor are sometimes refered to as "Deep Web".

The Options dialog box

The Options dialog box comes up if you click on the Options menu item in the Tools menu of the main Torifier window. Changes are saved and applied when you close the Options dialog box by pressing the OK button.

- The General panel
- Connection options
- The Exclusions panel
- The Advanced panel

The General panel

The General panel allows you to adjust the appearance of the graphical user interface of Torifier.

Connection options

Torifier is designed to connect to the Tor network automatically if you have unrestricted access to the Internet. You may need to modify the default connection settings if you are behind a restrictive firewall or there are other network restrictions that prevent you from connecting to the Tor network.

- Bridges
- Proxy
- Firewall

Bridges

If you are unable to connect to the Tor network, it could be that your Internet Service Provider (ISP) or another agency is blocking Tor. Often, you can work around this problem by using Tor Bridges, which are unlisted relays that are more difficult to block. You may obtain a set of bridge addresses by using one of these three methods:

- **Through the Web**
  Use a web browser to visit https://bridges.torproject.org
- **Through the Email Autoresponder**
  Send email to bridges@torproject.org with the line 'get bridges' by itself in the body of the message. However, to make it harder for an attacker to learn a lot of bridge addresses, you must send this request from one of the following email providers (listed in order of preference): https://www.riseup.net, https://mail.google.com, or https://mail.yahoo.com
- **Through the Torproject Help Desk**
  As a last resort, you can request bridge addresses by sending email message to help@rt.torproject.org. Please note that a person will need to respond to each request.

  Specify bridge relays one per line. Each line must be in one of the following formats:
- *address:port fingerprint* (only "vanilla" bridges)
- *address:port* (only "vanilla" bridges)
- *type address:port fingerprint*
- *type address:port*

Proxy

The Proxies panel allows you to define a proxy server through which the Tor client will make its connections.

If your computer requires a local proxy to access the Internet then you must enter the address of this proxy.

NOTE: If your Internet Service Provider (ISP) or another agency is blocking Tor then setting a remote proxy may help to bypass the block in some cases.

Firewall

The Firewall panel allows you to restrict the set of remote ports the Tor client will use for outgoing connections.

If you know that your PC goes through a firewall that only allows connections to certain ports then you should enter the allowed ports.

You can specify one or more ports and/or port ranges separated by comma. A port range must be in this format:
port-port

The Exclusions panel

The Exclusions panel allows you to specify which remote names and/or IP addresses must be excluded from torification.

In the upper edit control, you can specify one or more IP addresses and/or IP address ranges separated by comma. An IP address range must be in the format *address/mask*, where *address* is a plain IP address, and *mask* is a plain number, specifying the number of 1's (bits) at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0 for IPv4 and FFFF:FF00:: for IPv6. The following IP address ranges, which are reserved to internal and link-local networks, are specified by default: 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16, fe80::/10. The IPv4 loopback IP address range 127.0.0.0/8 and the IPv6 loopback address ::1 are always excluded from torification, even if they are not explicitly specified.

In the lower edit control, you can specify one or more names separated by comma. A name must be a fully-qualified domain name. Wildcards are allowed. The asterisk character (*) substitutes for any zero or more characters, and the question mark (?) substitutes for any one character.

The Advanced panel

Controlling product updates notifications

By default, Torifier is configured to automatically check for updates for itself when it starts.

If you do not want to be notified when an update is available, untick the "Check for updates when Torifier starts" box.

Controlling crash reporting

Software is complex and, like most complex things, is not perfect. The developers of Torifier constantly strive to improve the reliability of the program. As part of that effort, we can gather information from your computer in the form of a report when Torifier experiences a serious error aka “crash”. The crash-reporting information enables the developers of Torifier to identify bugs. So, if crash reporting is turned on when a crash occurs, there is a better chance that the bug that caused the crash will be fixed in the near future.

Crash reports include the following information:

- *Windows version information.* Includes the operating system version.
- *Date and time.* Indicates when the error occurred.
- *Software information.* Includes the name of the process where the error occurred and the list of loaded modules (DLLs).
- *Error information.* Includes the information the system recorded about the error.

Crash reports do NOT include any personal or sensitive information.

If you do not want crash reports to be sent to us, untick the “Submit crash reports” box.

Switching to a new identity

You can tell Torifier to switch to a new identity by clicking on the New Identity menu item in the Tools menu of the main Torifier window. Technically, this will cause Tor to switch to clean circuits, so new application requests don't share any circuits with old ones, and will clear the client-side DNS cache of Tor.

NOTE: Switching to a new identity will cause your visible IP address to change with a high probability.