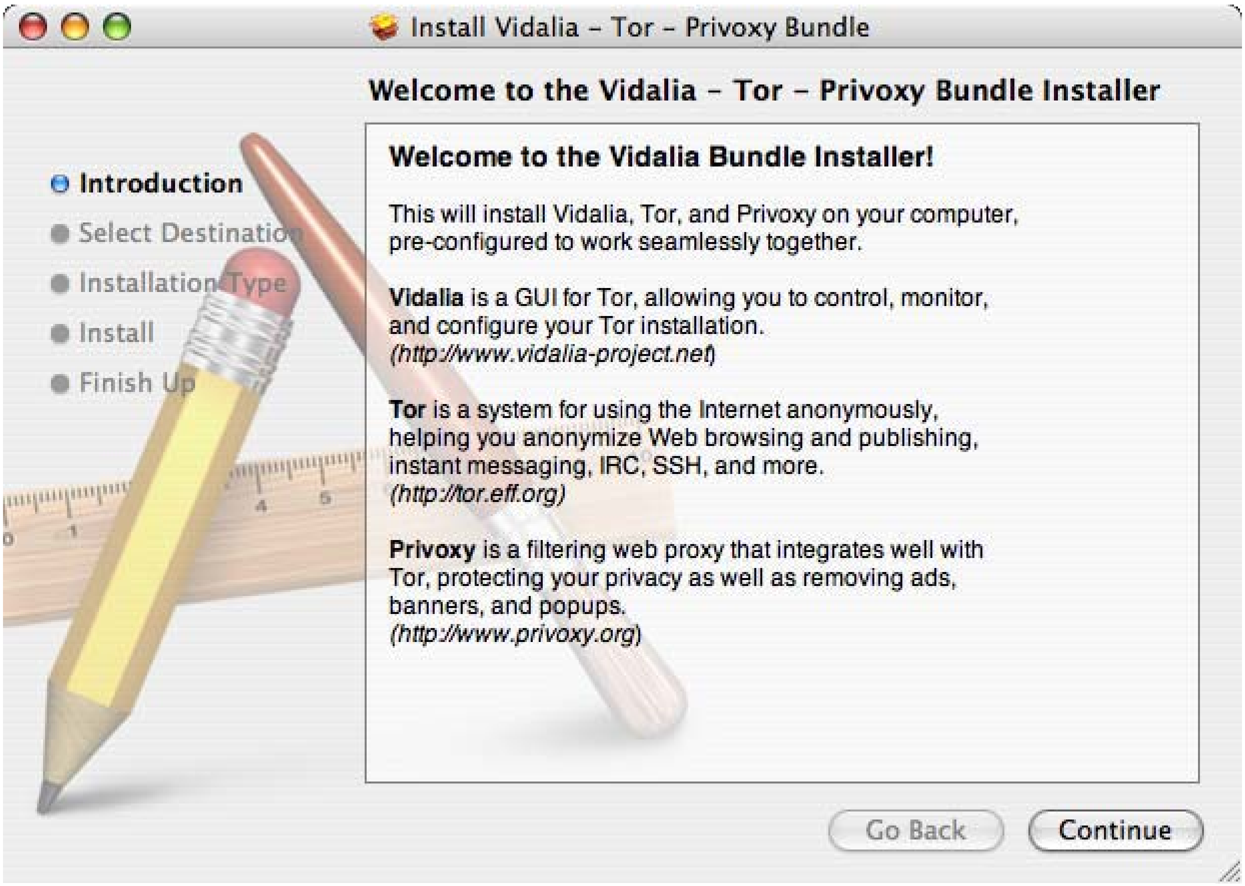
Running the Tor client on Mac OS X

Note that these are the installation instructions for running a Tor client on Mac OS X. If you want to relay traffic for others to help the network grow (please do), read the Configuring a server guide.

Step One: Download and Install Tor

The latest stable and experimental releases of Tor for Macintosh OS X bundle Tor, Vidalia (a GUI for Tor), and Privoxy (a filtering web proxy) into one package, pre-configured to work together. Download one from the download page.

Our Tor installer should make everything pretty simple. Below is a screenshot of the setup page:



Welcome to the Vidalia – Tor – Privoxy Bundle Installer

Welcome to the Vidalia Bundle Installer!

This will install Vidalia, Tor, and Privoxy on your computer, pre-configured to work seamlessly together.

Vidalia is a GUI for Tor, allowing you to control, monitor, and configure your Tor installation. *(http://www.vidalia-project.net)*

Tor is a system for using the Internet anonymously, helping you anonymize Web browsing and publishing, instant messaging, IRC, SSH, and more. *(http://tor.eff.org)*

Privoxy is a filtering web proxy that integrates well with Tor, protecting your privacy as well as removing ads, banners, and popups. *(http://www.privoxy.org)*

When the installer is finished, you can start Vidalia by selecting its icon from your Applications folder. A dark onion with a red X in your dock means Tor is not currently running. You can start Tor by selecting Start from the "Tor" menu at the top of your screen.

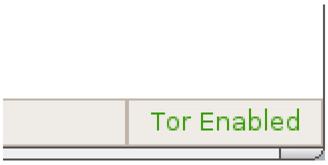
When Tor is running, Vidalia's dock icon will look like the following:

Privoxy is installed as part of the Tor bundle package installer. Once it is installed, it will start automatically when your computer is restarted. You do not need to configure Privoxy to use Tor — a custom Privoxy configuration for Tor has been installed as part of the installer package.

Step Two: Configure your applications to use Tor

After installing Tor and Privoxy, you need to configure your applications to use them. The first step is to set up web browsing.

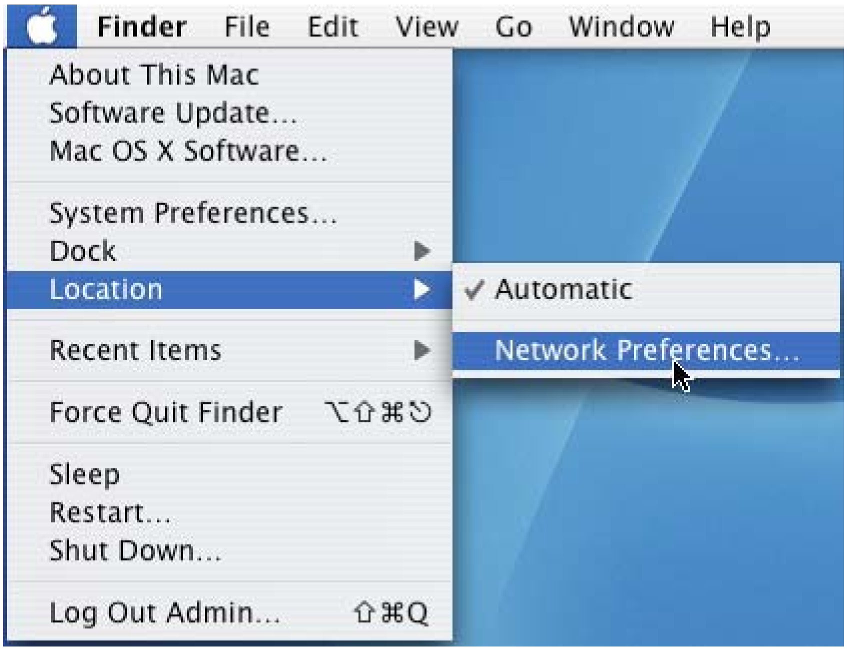
If you're using Firefox (we recommend it), simply install the Torbutton plugin, restart your Firefox, and you're all set:



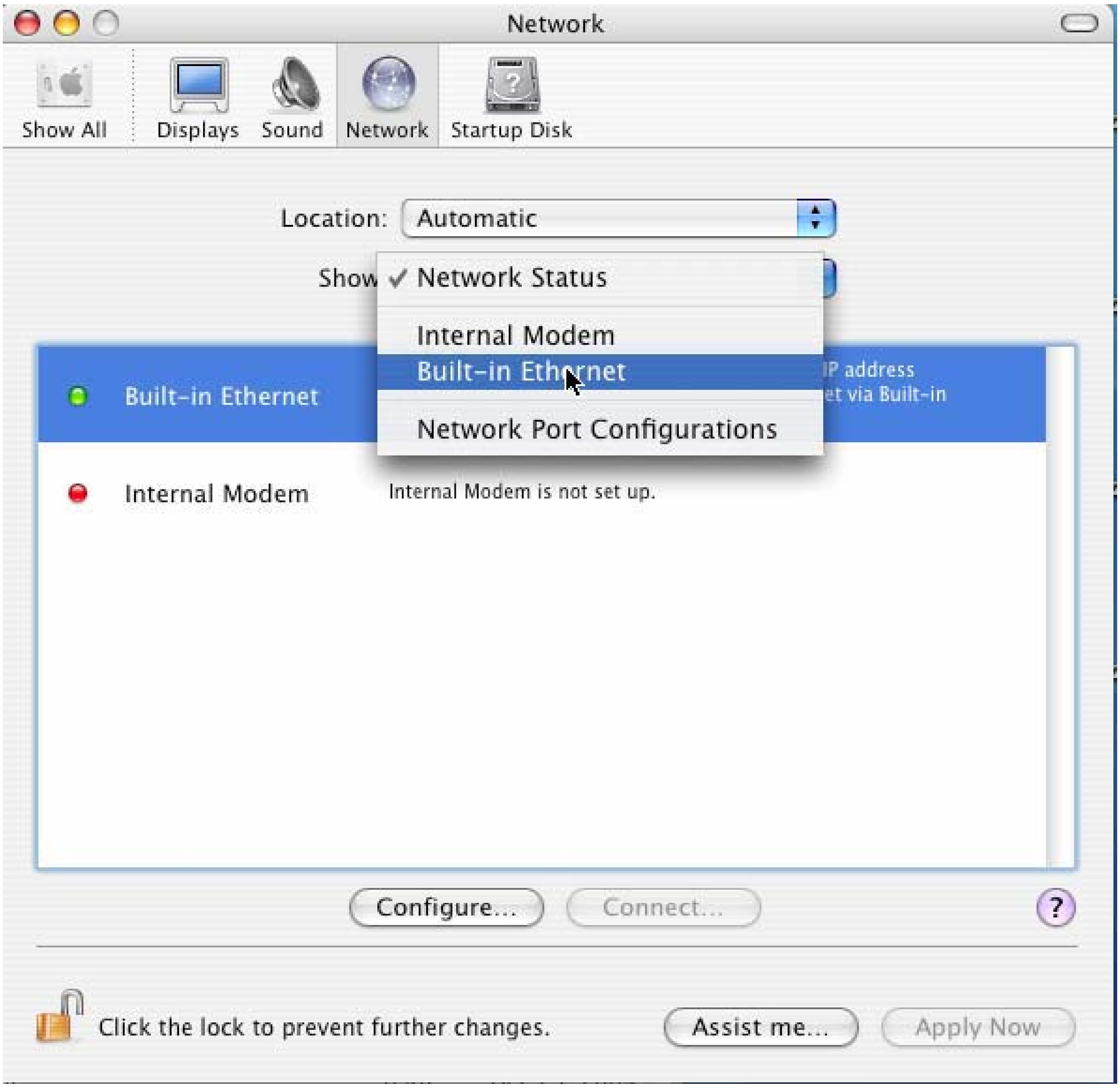
(Learn more about Torbutton here. If you plan to run Firefox on a different computer than Tor, see the FAQ entry for running Tor on a different computer. If you need to use a browser other than Firefox, you'll have to configure its proxy settings yourself.)

Apple Safari

If you want to use Tor with Safari, you need to change your Network Settings. Select your Network Preferences from the Apple | Location menu:



Select the Network Interface on which you want to enable Tor. If you use more than one Interface you must change the proxy settings for each individually.



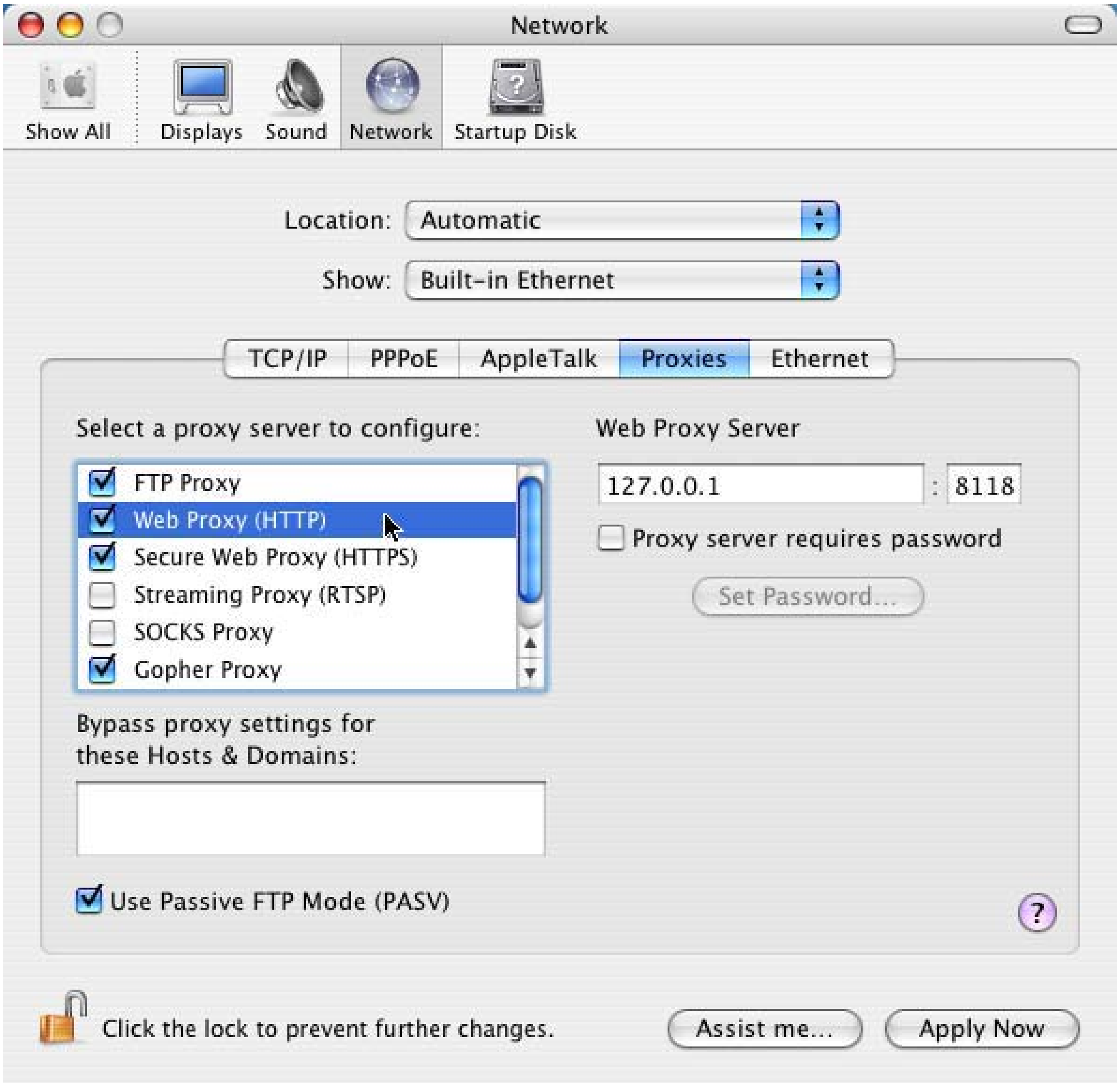
Location: Automatic

● Built-in Ethernet

● Internal Modem Internal Modem is not set up.

Click the lock to prevent further changes.

Select and enter 127.0.0.1 and port 8118 for both Web Proxy (HTTP) and your Secure Web Proxy (HTTPS). You should also do this for "FTP Proxy" and "Gopher Proxy"; see this note about Tor and ftp proxies. Leave your Use Passive FTP Mode (PASV) setting as is.



Location: Automatic

Show: Built-in Ethernet

Select a proxy server to configure:

- ☑ FTP Proxy
- ☑ Web Proxy (HTTP)
- ☑ Secure Web Proxy (HTTPS)
- □ Streaming Proxy (RTSP)
- □ SOCKS Proxy
- ☑ Gopher Proxy

Web Proxy Server

127.0.0.1 : 8118

□ Proxy server requires password

Bypass proxy settings for these Hosts & Domains:

☑ Use Passive FTP Mode (PASV)

Using privoxy is **necessary** because browsers leak your DNS requests when they use a SOCKS proxy directly, which is bad for your anonymity. Privoxy also removes certain dangerous headers from your web requests, and blocks obnoxious ad sites like Doubleclick.

To Torify other applications that support HTTP proxies, just point them at Privoxy (that is, localhost port 8118). To use SOCKS directly (for instant messaging, Jabber, IRC, etc), you can point your application directly at Tor (localhost port 9050), but see this FAQ entry for why this may be dangerous. For applications that support neither SOCKS nor HTTP, take a look at connect or socat.

For information on how to Torify other applications, check out the Torify HOWTO.

Step Three: Make sure it's working

Next, you should try using your browser with Tor and make sure that your IP address is being anonymized. Click on the Tor detector and see whether it thinks you're using Tor or not. (If that site is down, see this FAQ entry for more suggestions on how to test your Tor.)

If you have a personal firewall that limits your computer's ability to connect to itself, be sure to allow connections from your local applications to local port 8118 and port 9050. If your firewall blocks outgoing connections, punch a hole so it can connect to at least TCP ports 80 and 443, and then see this FAQ entry.

If it's still not working, look at this FAQ entry for hints.

Step Four: Configure it as a server

The Tor network relies on volunteers to donate bandwidth. The more people who run servers, the faster the Tor network will be. If you have at least 20 kilobytes/s each way, please help out Tor by configuring your Tor to be a server too. We have many features that make Tor servers easy and convenient, including rate limiting for bandwidth, exit policies so you can limit your exposure to abuse complaints, and support for dynamic IP addresses.

Having servers in many different places on the Internet is what makes Tor users secure. You may also get stronger anonymity yourself, since remote sites can't know whether connections originated at your computer or were relayed from others.

Read more at our Configuring a server guide.

How To Uninstall Tor and Privoxy

The Tor 0.1.0.x series and beyond have a command line or Terminal-based uninstaller. If you want to remove Tor on OSX, here's how:

Change your application proxy settings back to their original values. If you just want to stop using Tor, you can end at this point.

If you want to completely remove Tor, and your account has Admin Privileges, then proceed as follows:

1. Open up a Terminal or x-term session.
2. cd /Library/Tor
3. sudo -s
4. ./uninstall_tor_bundle.sh

Tor and Privoxy are now completely removed from your system.

If you're using a version of the Tor installer that doesn't come with the uninstall_tor_bundle script, you will need to manually delete the following:

- /Library/Tor
- /Library/Privoxy
- /usr/bin/tor
- /usr/bin/tor_resolve
- /var/log/tor
- /usr/share/man/man1/tor.1

- /usr/share/man/man1/tor-resolve.1
- /usr/share/man/man1/torify.1
- /Library/Receipts/Privoxy.pkg/
- /Library/Receipts/privoxyconf.pkg/
- /Library/Receipts/Tor.pkg/
- /Library/Receipts/torstartup.pkg/