

Privoxy Frequently Asked Questions

Copyright © 2001-2007 by Privoxy Developers

\$Id: faq.sgml,v 2.35 2007/11/19 17:57:59 fabiankeil Exp \$

This FAQ gives quick answers to frequently asked questions about Privoxy. It is not a substitute for the *Privoxy User Manual*.

What is Privoxy?

Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data, managing HTTP cookies, controlling access, and removing ads, banners, pop-ups and other obnoxious Internet junk. Privoxy has a flexible configuration and can be customized to suit individual needs and tastes. Privoxy has application for both stand-alone systems and multi-user networks.

Privoxy is based on Internet Junkbuster (tm).

Please note that this document is a work in progress. This copy represents the state at the release of version 3.0.7. You can find the latest version of the document at <http://www.privoxy.org/faq/>. Please see the Contact section if you want to contact the developers.

Privoxy Frequently Asked Questions

Table of Contents

1. General Information.....	1
1.1. Who should give Privoxy a try?.....	1
1.2. Is Privoxy the best choice for me?.....	1
1.3. What is a "proxy"? How does Privoxy work?.....	1
1.4. Does Privoxy do anything more than ad blocking?.....	1
1.5. What is this new version of "Junkbuster"?.....	1
1.6. Why "Privoxy"? Why change the name from Junkbuster at all?.....	1
1.7. How does Privoxy differ from the old Junkbuster?.....	2
1.8. How does Privoxy know what is an ad, and what is not?.....	2
1.9. Can Privoxy make mistakes? This does not sound very scientific.....	2
1.10. Will I have to configure Privoxy before I can use it?.....	2
1.11. Can Privoxy run as a server on a network?.....	3
1.12. My browser does the same things as Privoxy. Why should I use Privoxy at all?.....	3
1.13. Why should I trust Privoxy?.....	3
1.14. Is there is a license or fee? What about a warranty? Registration?.....	3
1.15. Can Privoxy remove spyware? Adware? Viruses?.....	3
1.16. Can I use Privoxy with other ad-blocking software?.....	3
1.17. I would like to help you, what can I do?.....	3
2. Installation.....	5
2.1. Which browsers are supported by Privoxy?.....	5
2.2. Which operating systems are supported?.....	5
2.3. Can I use Privoxy with my email client?.....	5
2.4. I just installed Privoxy. Is there anything special I have to do now?.....	5
2.5. What is the proxy address of Privoxy?.....	5
2.6. I just installed Privoxy, and nothing is happening. All the ads are there. What's wrong?.....	5
2.7. I get a "Privoxy is not being used" dummy page although Privoxy is running and being used.....	5
3. Configuration.....	7
3.1. What exactly is an "actions" file?.....	7
3.2. The "actions" concept confuses me. Please list some of these "actions".....	7
3.3. How are actions files configured? What is the easiest way to do this?.....	7
3.4. There are several different "actions" files. What are the differences?.....	7
3.5. Where can I get updated Actions Files?.....	7
3.6. Can I use my old config files?.....	7
3.7. Why is the configuration so complicated?.....	7
3.8. How can I make my Yahoo/Hotmail/Gmail account work?.....	7
3.9. What's the difference between the "Cautious", "Medium" and "Advanced" defaults?.....	8
3.10. Why can I change the configuration with a browser? Does that not raise security issues?.....	8
3.11. What is the default.filter file? What is a "filter"?.....	8
3.12. How can I set up Privoxy to act as a proxy for my LAN?.....	8
3.13. Instead of ads, now I get a checkerboard pattern. I don't want to see anything.....	9
3.14. Why would anybody want to see a checkerboard pattern?.....	9
3.15. I see some images being replaced with text instead of the checkerboard image. Why and how do I get rid of this?.....	9
3.16. Can Privoxy run as a service on Win2K/NT/XP?.....	9
3.17. How can I make Privoxy work with other proxies like Squid or Tor?.....	9
3.18. Can I just set Privoxy to use port 80 and thus avoid individual browser configuration?.....	9
3.19. Can Privoxy run as a "transparent" proxy?.....	10
3.20. Can Privoxy run as a "intercepting" proxy?.....	10
3.21. How can I configure Privoxy for use with Outlook Express?.....	10
3.22. How can I have separate rules just for HTML mail?.....	10
3.23. I sometimes notice cookies sneaking through. How?.....	10
3.24. Are all cookies bad? Why?.....	10
3.25. How can I allow permanent cookies for my trusted sites?.....	10
3.26. Can I have separate configurations for different users?.....	11
3.27. Can I set-up Privoxy as a whitelist of "good" sites?.....	11
3.28. How can I turn off ad-blocking?.....	11
3.29. How can I have custom template pages, like the BLOCKED page?.....	11
3.30. How can I remove the "Go There Anyway" link from the BLOCKED page?.....	12
4. Miscellaneous.....	13
4.1. How much does Privoxy slow my browsing down? This has to add extra time to browsing.....	13
4.2. I notice considerable delays in page requests. What's wrong?.....	13
4.3. What are "http://config.privoxy.org/" and "http://p.p/"?.....	13
4.4. How can I submit new ads, or report problems?.....	13
4.5. If I do submit missed ads, will they be included in future updates?.....	13
4.6. Why doesn't anyone answer my support request?.....	13

Privoxy Frequently Asked Questions

Table of Contents

4. Miscellaneous

4.7. How can I hide my IP address?.....	14
4.8. Can Privoxy guarantee I am anonymous?.....	14
4.9. A test site says I am not using a Proxy.....	14
4.10. How do I use Privoxy together with Tor?.....	14
4.11. Might some things break because header information or content is being altered?.....	15
4.12. Can Privoxy act as a "caching" proxy to speed up web browsing?.....	15
4.13. What about as a firewall? Can Privoxy protect me?.....	15
4.14. I have large empty spaces / a checkerboard pattern now where ads used to be. Why?.....	15
4.15. How can Privoxy filter Secure (HTTPS) URLs?.....	16
4.16. Privoxy runs as a "server". How secure is it? Do I need to take any special precautions?.....	16
4.17. Can I temporarily disable Privoxy?.....	16
4.18. When "disabled" is Privoxy totally out of the picture?.....	16
4.19. How can I tell Privoxy to totally ignore certain sites?.....	16
4.20. My logs show Privoxy "crunches" ads, but also its own internal CGI pages. What is a "crunch"?.....	16
4.21. Can Privoxy effect files that I download from a webserver? FTP server?.....	16
4.22. I just downloaded a Perl script, and Privoxy altered it! Yikes, what is wrong!.....	17
4.23. Should I continue to use a "HOSTS" file for ad-blocking?.....	17
4.24. Where can I find more information about Privoxy and related issues?.....	17
4.25. I've noticed that Privoxy changes "Microsoft" to "MicroSuck"! Why are you manipulating my browsing?.....	18
4.26. Does Privoxy produce "valid" HTML (or XHTML)?.....	18

5. Troubleshooting

5.1. I cannot connect to any websites. Or, I am getting "connection refused" message with every web page. Why?.....	19
5.2. Why am I getting a 503 Error (WSAECONNREFUSED) on every page?.....	19
5.3. I just added a new rule, but the steenkin ad is still getting through. How?.....	19
5.4. One of my favorite sites does not work with Privoxy. What can I do?.....	20
5.5. After installing Privoxy, I have to log in every time I start IE. What gives?.....	20
5.6. I cannot connect to any FTP sites. Privoxy is blocking me.....	20
5.7. In Mac OSX, I can't configure Microsoft Internet Explorer to use Privoxy as the HTTP proxy.....	21
5.8. In Mac OSX, I dragged the Privoxy folder to the trash in order to uninstall it. Now the finder tells me I don't have sufficient privileges to empty the trash.....	21
5.9. In Mac OSX Panther (10.3), images often fail to load and/or I experience random delays in page loading. I'm using localhost as my browser's proxy setting.....	21
5.10. I get a completely blank page at one site. "View Source" shows only: <html><body></body></html>. Without Privoxy the page loads fine.....	21
5.11. My logs show many "Unable to get my own hostname" lines. Why?.....	21
5.12. When I try to launch Privoxy, I get an error message "port 8118 is already in use" (or similar wording). Why?.....	21
5.13. Pages with UTF-8 fonts are garbled.....	21
5.14. Why are binary files (such as images) corrupted when Privoxy is used?.....	22
5.15. What is the "demoronizer" and why is it there?.....	22
5.16. Why do I keep seeing "PrivoxyWindowOpen()" in raw source code?.....	22
5.17. I am getting too many DNS errors like "404 No Such Domain". Why can't Privoxy do this better?.....	22
5.18. At one site Privoxy just hangs, and starts taking all CPU. Why is this?.....	22
5.19. I just installed Privoxy, and all my browsing has slowed to a crawl. What gives?.....	22
5.20. Why do my filters work on some sites but not on others?.....	22

6. Contacting the developers, Bug Reporting and Feature Requests

6.1. Get Support.....	23
6.2. Reporting Problems.....	23
6.2.1. Reporting Ads or Other Configuration Problems.....	23
6.2.2. Reporting Bugs.....	23
6.3. Request New Features.....	24
6.4. Other.....	24

7. Privoxy Copyright, License and History

7.1. License.....	25
7.2. History.....	25

1. General Information

1.1. Who should give Privoxy a try?

Anyone who is interested in security, privacy, or in finer-grained control over their web and Internet experience.

1.2. Is Privoxy the best choice for me?

Privoxy is certainly a good choice, especially for those who want more control and security. Those with the willingness to read the documentation and the ability to fine-tune their installation will benefit the most.

One of Privoxy's strengths is that it is highly configurable giving you the ability to completely personalize your installation. Being familiar with, or at least having an interest in learning about [HTTP](#) and other networking protocols, [HTML](#), and ["Regular Expressions"](#) will be a big plus and will help you get the most out of Privoxy. A new installation just includes a very basic configuration. The user should take this as a starting point only, and enhance it as he or she sees fit. In fact, the user is encouraged, and expected to, fine-tune the configuration.

Much of Privoxy's configuration can be done with a [Web browser](#). But there are areas where configuration is done using a [text editor](#) to edit configuration files. Also note that the web-based action editor doesn't use authentication and should only be enabled in environments where all clients with access to Privoxy listening port can be trusted.

1.3. What is a "proxy"? How does Privoxy work?

A [web proxy](#) is a service, based on a software such as Privoxy, that clients (i.e. browsers) can use instead of connecting directly to web servers on the Internet. The clients then ask the proxy to fetch the objects they need (web pages, images, movies etc) on their behalf, and when the proxy has done so, it hands the results back to the client. It is a "go-between". See the [Wikipedia proxy definition](#) for more.

There are many reasons to use web proxies, such as security (firewalling), efficiency (caching) and others, and there are any number of proxies to accommodate those needs.

Privoxy is a proxy that is primarily focused on privacy protection, ad and junk elimination and freeing the user from restrictions placed on his activities. Sitting between your browser(s) and the Internet, it is in a perfect position to filter outbound personal information that your browser is leaking, as well as inbound junk. It uses a variety of techniques to do this, all of which are under your complete control via the various configuration files and options. Being a proxy also makes it easier to share configurations among multiple browsers and/or users.

1.4. Does Privoxy do anything more than ad blocking?

Yes, ad blocking is but one possible use. There are many, many ways Privoxy can be used to sanitize and customize web browsing.

1.5. What is this new version of "Junkbuster"?

A long time ago, there was the [Internet Junkbuster](#), by Anonymous Coders and [Junkbusters Corporation](#). This saved many users a lot of pain in the early days of web advertising and user tracking.

But the web, its protocols and standards, and with it, the techniques for forcing ads on users, give up autonomy over their browsing, and for tracking them, keeps evolving. Unfortunately, the Internet Junkbuster did not. Version 2.0.2, published in 1998, was (and is) the last official [release](#) available from [Junkbusters Corporation](#). Fortunately, it had been released under the GNU [GPL](#), which allowed further development by others.

So Stefan Waldherr started maintaining an [improved version of the software](#), to which eventually a number of people contributed patches. It could already replace banners with a transparent image, and had a first version of pop-up killing, but it was still very closely based on the original, with all its limitations, such as the lack of HTTP/1.1 support, flexible per-site configuration, or content modification. The last release from this effort was version 2.0.2-10, published in 2000.

Then, some [developers](#) picked up the thread, and started turning the software inside out, upside down, and then reassembled it, adding many [new features](#) along the way.

The result of this is Privoxy, whose first stable version, 3.0, was released August, 2002.

1.6. Why "Privoxy"? Why change the name from Junkbuster at all?

Though outdated, [Junkbusters Corporation](#) continues to offer their original version of the Internet Junkbuster, so publishing our Junkbuster-derived software under the same name led to confusion.

There are also potential legal complications from our use of the Junkbuster name, which is a registered trademark of [Junkbusters Corporation](#). There are, however, no objections from Junkbusters Corporation to the Privoxy project itself, and they, in fact, still share our ideals and goals.

Privoxy Frequently Asked Questions

The developers also believed that there are so many improvements over the original code, that it was time to make a clean break from the past and make a name in their own right.

Privoxy is the "*Privacy Enhancing Proxy*". Also, its content modification and junk suppression gives *you*, the user, more control, more freedom, and allows you to browse your personal and "*private*" edition" of the web.

1.7. How does Privoxy differ from the old Junkbuster?

Privoxy picks up where Junkbuster left off. All the old features remain. The new Privoxy still blocks ads and banners, still manages cookies, and still helps protect your privacy. But, most of these features have been enhanced, and many new ones have been added, all in the same vein.

Privoxy's new features include:

- Integrated browser based configuration and control utility at <http://config.privoxy.org/> (shortcut: <http://p.p/>). Browser-based tracing of rule and filter effects. Remote toggling.
 - Web page filtering (text replacements, removes banners based on size, invisible "web-bugs", JavaScript and HTML annoyances, pop-up windows, header manipulation, etc.)
 - Modularized configuration that allows for standard settings and user settings to reside in separate files, so that installing updated actions files won't overwrite individual user settings.
 - Support for Perl Compatible Regular Expressions in the configuration files, and generally a more sophisticated and flexible configuration syntax over previous versions.
 - Improved cookie management features (e.g. session based cookies).
 - GIF de-animation.
 - Bypass many click-tracking scripts (avoids script redirection).
 - Multi-threaded (POSIX and native threads).
 - User-customizable HTML templates for all proxy-generated pages (e.g. "blocked" page).
 - Auto-detection and re-reading of config file changes.
 - Improved signal handling, and a true daemon mode (Unix).
 - Every feature now controllable on a per-site or per-location basis, configuration more powerful and versatile over-all.
 - Many smaller new features added, limitations and bugs removed, and security holes fixed.
-

1.8. How does Privoxy know what is an ad, and what is not?

Privoxy's approach to blocking ads is twofold:

First, there are certain patterns in the *locations* (URLs) of banner images. This applies to both the path (you wouldn't guess how many web sites serve their banners from a directory called "banners"!) and the host (blocking the big banner hosting services like doubleclick.net already helps a lot). Privoxy takes advantage of this fact by using URL patterns to sort out and block the requests for things that sound like they would be ads or banners.

Second, banners tend to come in certain *sizes*. But you can't tell the size of an image by its URL without downloading it, and if you do, it's too late to save bandwidth. Therefore, Privoxy also inspects the HTML sources of web pages while they are loaded, and replaces references to images with standard banner sizes by dummy references, so that your browser doesn't request them anymore in the first place.

Both of this involves a certain amount of guesswork and is, of course, freely and readily configurable.

1.9. Can Privoxy make mistakes? This does not sound very scientific.

Actually, it's a black art ;-) And yes, it is always possible to have a broad rule accidentally block or change something by mistake. You will almost surely run into such situations at some point. It is tricky writing rules to cover every conceivable possibility, and not occasionally get false positives.

But this should not be a big concern since the Privoxy configuration is very flexible, and includes tools to help identify these types of situations so they can be addressed as needed, allowing you to customize your installation. (See the Troubleshooting section below.)

1.10. Will I have to configure Privoxy before I can use it?

That depends on your expectations. The default installation should give you a good starting point, and block *most* ads and unwanted content, but many of the more advanced features are off by default, and require you to activate them.

You do have to set up your browser to use Privoxy (see the Installation section below).

And you will certainly run into situations where there are false positives, or ads not being blocked that you may not want to see. In these cases, you would certainly benefit by customizing Privoxy's configuration to more closely match your individual situation. And we encourage you to do this. This is where the real power of Privoxy lies!

Privoxy Frequently Asked Questions

1.11. Can Privoxy run as a server on a network?

Yes, Privoxy runs as a server already, and can easily be configured to "serve" more than one client. See [How can I set up Privoxy to act as a proxy for my LAN](#) below.

1.12. My browser does the same things as Privoxy. Why should I use Privoxy at all?

Modern browsers do indeed have *some* of the same functionality as Privoxy. Maybe this is adequate for you. But Privoxy is very versatile and powerful, and can probably do a number of things your browser just can't.

In addition, a proxy is good choice if you use multiple browsers, or have a LAN with multiple computers since Privoxy can run as a server application. This way all the configuration is in one place, and you don't have to maintain a similar configuration for possibly many browsers or users.

Note, however, that it's recommended to leverage both your browser's and Privoxy's privacy enhancing features at the same time. While your browser probably lacks some features Privoxy offers, it should also be able to do some things more reliable, for example restricting and suppressing JavaScript.

1.13. Why should I trust Privoxy?

The most important reason is because you have access to *everything*, and you can control everything. You can check every line of every configuration file yourself. You can check every last bit of source code should you desire. And even if you can't read code, there should be some comfort in knowing that other people can, and do read it. You can build the software from scratch, if you want, so that you know the executable is clean, and that it is *yours*. In fact, we encourage this level of scrutiny. It is one reason we use Privoxy ourselves.

1.14. Is there is a license or fee? What about a warranty? Registration?

Privoxy is free software and licensed under the [GNU General Public License \(GPL\) version 2](#). It is free to use, copy, modify or distribute as you wish under the terms of this license. Please see the [Copyright](#) section for more information on the license and copyright. Or the `LICENSE` file that should be included.

There is *no warranty* of any kind, expressed, implied or otherwise. That is something that would cost real money ;-) There is no registration either.

1.15. Can Privoxy remove spyware? Adware? Viruses?

No, at least not reliably enough to trust it. Privoxy is not designed to be a malware removal tool and the default configuration doesn't even try to filter out any malware.

Privoxy could help prevent contact from (known) sites that use such tactics with appropriate configuration rules, and thus could conceivably prevent contamination from such sites. However, keeping such a configuration up to date would require a lot of time and effort that would be better spend on keeping your software itself up to date so it doesn't have known vulnerabilities.

1.16. Can I use Privoxy with other ad-blocking software?

Privoxy should work fine with other proxies and other software in general.

But it is probably not necessary to use Privoxy in conjunction with other ad-blocking products, and this could conceivably cause undesirable results. It might be better to choose one software or the other and work a little to tweak its configuration to your liking.

Note that this is an advice specific to ad blocking.

1.17. I would like to help you, what can I do?

1.17.1. Would you like to participate?

Well, we *always* need help. There is something for everybody who wants to help us. We welcome new developers, packagers, testers, documentation writers or really anyone with a desire to help in any way. You *DO NOT* need to be a "programmer". There are many other tasks available. In fact, the programmers often can't spend as much time programming because of some of the other, more mundane things that need to be done, like checking the Tracker feedback sections.

So first thing, [get an account on SourceForge.net](#) and mail your id to the [developers mailing list](#). Then, please read the [Developer's Manual](#), at least the pertinent sections.

You can also start helping out without SourceForge.net account, simply by showing up on the mailing list, helping out other users, providing general feedback or reporting problems you noticed.

Privoxy Frequently Asked Questions

1.17.2. Contribute!

We, of course, welcome donations and could use money for domain registering, buying software to test Privoxy with, and, of course, for regular world-wide get-togethers (hahaha). If you enjoy the software and feel like helping us with a donation, just [drop us a note](#) and get your name on the list of contributors.

1.17.3. Software

If you are a vendor of a web-related software like a browser, web server or proxy, and would like us to ensure that Privoxy runs smoothly with your product, you might consider supplying us with a copy or license. We can't, however, guarantee that we will fix all potential compatibility issues as a result.

2. Installation

2.1. Which browsers are supported by Privoxy?

Any browser that can be configured to use a proxy, which should be virtually all browsers, including Firefox, Internet Explorer, Opera, and Safari among others. Direct browser support is not an absolute requirement since Privoxy runs as a separate application and talks to the browser in the standardized HTTP protocol, just like a web server does.

2.2. Which operating systems are supported?

At present, Privoxy is known to run on Windows(95, 98, ME, 2000, XP, Vista), GNU/Linux (RedHat, SuSE, Debian, Fedora, Gentoo, Slackware and others), Mac OSX, OS/2, AmigaOS, FreeBSD, NetBSD, OpenBSD, Solaris, and various other flavors of Unix.

But any operating system that runs TCP/IP, can conceivably take advantage of Privoxy in a networked situation where Privoxy would run as a server on a LAN gateway. Then only the "gateway" needs to be running one of the above operating systems.

Source code is freely available, so porting to other operating systems is always a possibility.

2.3. Can I use Privoxy with my email client?

As long as there is some way to set a HTTP proxy for the client, then yes, any application can be used, whether it is strictly speaking a "browser" or not. Though this may not be the best approach for dealing with some of the common abuses of HTML in email. See [How can I configure Privoxy with Outlook Express?](#) below for more on this.

Be aware that HTML email presents a number of unique security and privacy related issues, that can require advanced skills to overcome. The developers recommend using email clients that can be configured to convert HTML to plain text for these reasons.

2.4. I just installed Privoxy. Is there anything special I have to do now?

All browsers should be told to use Privoxy as a proxy by specifying the correct proxy address and port number in the appropriate configuration area for the browser. It's possible to combine Privoxy with a packet filter to intercept HTTP requests even if the client isn't explicitly configured to use Privoxy, but where possible, configuring the client is recommended. See [the User Manual for more details](#). You should also flush your browser's memory and disk cache to get rid of any cached junk items, and remove any stored [cookies](#).

2.5. What is the proxy address of Privoxy?

If you set up the Privoxy to run on the computer you browse from (rather than your ISP's server or some networked computer on a LAN), the proxy will be on 127.0.0.1 (sometimes referred to as "localhost", which is the special name used by every computer on the Internet to refer to itself) and the port will be 8118 (unless you used the [listen-address](#) config option to tell Privoxy to run on a different port).

When configuring your browser's proxy settings you typically enter the word "localhost" or the IP address "127.0.0.1" in the boxes next to "HTTP" and "Secure" (HTTPS) and then the number "8118" for "port". This tells your browser to send all web requests to Privoxy instead of directly to the Internet.

Privoxy can also be used to proxy for a Local Area Network. In this case, you would enter either the IP address of the LAN host where Privoxy is running, or the equivalent hostname, e.g. 192.168.1.1. Port assignment would be same as above. Note that Privoxy doesn't listen on any LAN interfaces by default.

Privoxy does not currently handle any other protocols such as FTP, SMTP, IM, IRC, ICQ, etc.

2.6. I just installed Privoxy, and nothing is happening. All the ads are there. What's wrong?

Did you configure your browser to use Privoxy as a proxy? It does not sound like it. See above. You might also try flushing the browser's caches to force a full re-reading of pages. You can verify that Privoxy is running, and your browser is correctly configured by entering the special URL: <http://p.p/>. This should take you to a page titled "This is Privoxy.." with access to Privoxy's internal configuration. If you see this, then you are good to go. If you receive a page saying "Privoxy is not running", then the browser is not set up to use your Privoxy installation. If you receive anything else (probably nothing at all), it could either be that the browser is not set up correctly, or that Privoxy is not running at all. Check the [log file](#). For instructions on starting Privoxy and browser configuration, see the [chapter on starting Privoxy](#) in the [User Manual](#).

2.7. I get a "Privoxy is not being used" dummy page although Privoxy is running and being used.

First, make sure that Privoxy is *really* running and being used by visiting <http://p.p/>. You should see the Privoxy main page. If not, see the [chapter on starting Privoxy](#) in the [User Manual](#).

Now if <http://p.p/> works for you, but other parts of Privoxy's web interface show the dummy page, your browser has cached a redirection it encountered before Privoxy was being used. You need to clear your browser's cache. Note that shift-reloading the dummy page won't

Privoxy Frequently Asked Questions

help, since that'll only refresh the dummy page, not the redirection that lead you there.

The procedure for clearing the cache varies from browser to browser. For example, Mozilla/Netscape users would click Edit --> Preferences --> Advanced --> Cache and then click both "Clear Memory Cache" and "Clear Disk Cache". In some Firefox versions it's Tools --> Options --> Privacy --> Cache and then click "Clear Cache Now".

3. Configuration

3.1. What exactly is an "actions" file?

Privoxy utilizes the concept of "actions" that are used to manipulate and control web page data. [Actions files](#) are where these [actions](#) that Privoxy could take while processing a certain request, are configured. Typically, you would define a set of default actions that apply globally to all URLs, then add exceptions to these defaults where needed. There is a wide array of actions available that give the user a high degree of control and flexibility on how to process each and every web page.

Actions can be defined on a [URL pattern](#) basis, i.e. for single URLs, whole web sites, groups or parts thereof etc. Actions can also be grouped together and then applied to requests matching one or more patterns. There are many possible actions that might apply to any given site. As an example, if you are blocking [cookies](#) as one of your default actions, but need to accept cookies from a given site, you would need to define an exception for this site in one of your actions files, preferably in `user.action`.

3.2. The "actions" concept confuses me. Please list some of these "actions".

For a comprehensive discussion of the actions concept, please refer to the [actions file chapter](#) in the [User Manual](#). It includes a [list of all actions](#) and an [actions file tutorial](#) to get you started.

3.3. How are actions files configured? What is the easiest way to do this?

Actions files are just text files in a special syntax and can be edited with a text editor. But probably the easiest way is to access Privoxy's user interface with your web browser at <http://config.privoxy.org/> (Shortcut: <http://p.p/>) and then select "[View & change the current configuration](#)" from the menu. Note that this feature must be explicitly enabled in the main config file (see [enable-edit-actions](#)).

3.4. There are several different "actions" files. What are the differences?

Three actions files are being included by the developers, to be used for different purposes: These are `default.action`, the "main" actions file which is actively maintained by the Privoxy developers and typically sets the default policies, `user.action`, where users are encouraged to make their private customizations, and `standard.action`, which is for internal Privoxy use only. Please see [the actions chapter](#) in the [User Manual](#) for a more detailed explanation.

Earlier versions included three different versions of the `default.action` file. The new scheme allows for greater flexibility of local configuration, and for browser based selection of pre-defined "aggressiveness" levels.

3.5. Where can I get updated Actions Files?

Based on your feedback and the continuing development, updates of `default.action` will be made available from time to time on the [files section](#) of our [project page](#).

If you wish to receive an email notification whenever we release updates of Privoxy or the actions file, [subscribe to our announce mailing list](#), ijbswa-announce@lists.sourceforge.net.

3.6. Can I use my old config files?

The syntax and purpose of configuration files has remained roughly the same throughout the 3.x series, but backwards compatibility is not guaranteed. Also each release contains updated, "improved" versions and it is therefore strongly recommended to install the newer configuration files and merge back your modifications.

3.7. Why is the configuration so complicated?

"Complicated" is in the eye of the beholder. Those that are familiar with some of the underlying concepts, such as regular expression syntax, take to it like a fish takes to water. Also, software that tries hard to be "user friendly", often lacks sophistication and flexibility. There is always that trade-off there between power vs. easy-of-use. Furthermore, anyone is welcome to contribute ideas and implementations to enhance Privoxy.

3.8. How can I make my Yahoo/Hotmail/Gmail account work?

The default configuration shouldn't impact the usability of any of these services. It may, however, make all [cookies](#) temporary, so that your browser will forget your login credentials in between browser sessions. If you would like not to have to log in manually each time you access those websites, simply turn off all cookie handling for them in the `user.action` file. An example for yahoo might look like:

```
# Allow all cookies for Yahoo login:
#
{ -crunch-incoming-cookies -crunch-outgoing-cookies -session-cookies-only }
.login.yahoo.com
```

Privoxy Frequently Asked Questions

These kinds of sites are often quite complex and heavy with [Javascript](#) and thus "fragile". So if *still* a problem, we have an [alias](#) just for such sticky situations:

```
# Gmail is a _fragile_ site:
#
{ fragile }
# Gmail is ...
mail.google.com
```

Be sure to flush your browser's caches whenever making these kinds of changes, just to make sure the changes "take".

Make sure the domain, host and path are appropriate as well. Your browser can tell you where you are specifically and you should use that information for your configuration settings. Note that above it is not referenced as `gmail.com`, which is a valid domain name.

3.9. What's the difference between the "Cautious", "Medium" and "Advanced" defaults?

Configuring Privoxy is not entirely trivial. To help you get started, we provide you with three different default action "profiles" in the web based actions file editor at <http://config.privoxy.org/show-status>. See the [User Manual](#) for a list of actions, and how the default profiles are set.

Where the defaults are likely to break some sites, exceptions for known popular "problem" sites are included, but in general, the more aggressive your default settings are, the more exceptions you will have to make later. New users are best to start off in "Cautious" setting. This is safest and will have the fewest problems. See the [User Manual](#) for a more detailed discussion.

It should be noted that the "Advanced" profile (formerly known as the "Adventuresome" profile) is more aggressive, and will make use of some of Privoxy's advanced features. Use at your own risk!

3.10. Why can I change the configuration with a browser? Does that not raise security issues?

It may seem strange that regular users can edit the config files with their browsers, although the whole `/etc/privoxy` hierarchy belongs to the user "privoxy", with only 644 permissions.

When you use the browser-based editor, Privoxy itself is writing to the config files. Because Privoxy is running as the user "privoxy", it can update its own config files.

If you run Privoxy for multiple untrusted users (e.g. in a LAN) or aren't entirely in control of your own browser, you will probably want to make sure that the the web-based editor and remote toggle features are "off" by setting "[enable-edit-actions](#) 0" and "[enable-remote-toggle](#) 0" in the [main configuration file](#).

As of Privoxy 3.0.7 these options are disabled by default.

3.11. What is the `default.filter` file? What is a "filter"?

The `default.filter` file is where *filters* as supplied by the developers are defined. Filters are a special subset of actions that can be used to modify or remove web page content or headers on the fly. Content filters can be applied to *anything* in the page source, header filters can be applied to either server or client headers. Regular expressions are used to accomplish this.

There are a number of pre-defined filters to deal with common annoyances. The filters are only defined here, to invoke them, you need to use the [filter action](#) in one of the actions files. Content filtering is automatically disabled for inappropriate MIME types, but if you now better than Privoxy what should or should not be filtered you can filter any content you like.

Filters should *not* be confused with [blocks](#), which is a completely different action, and is more typically used to block ads and unwanted sites.

If you are familiar with regular expressions, and HTML, you can look at the provided `default.filter` with a text editor and define your own filters. This is potentially a very powerful feature, but requires some expertise in both regular expressions and HTML/HTTP. You should place any modifications to the default filters, or any new ones you create in a separate file, such as `user.filter`, so they won't be overwritten during upgrades. The ability to define multiple filter files in `config` is a new feature as of v. 3.0.5.

There is no GUI editor option for this part of the configuration, but you can disable/enable the various pre-defined filters of the included `default.filter` file with the [web-based actions file editor](#). Note that the custom actions editor must be explicitly enabled in the main config file (see [enable-edit-actions](#)).

If you intend to develop your own filters, you might want to have a look at [Privoxy-Filter-Test](#).

3.12. How can I set up Privoxy to act as a proxy for my LAN?

By default, Privoxy only responds to requests from `127.0.0.1` (localhost). To have it act as a server for a network, this needs to be changed in the [main configuration file](#). Look for the `listen-address` option, which may be commented out with a "#" symbol. Make sure it is uncommented, and assign it the address of the LAN gateway interface, and port number to use. Assuming your LAN address is

Privoxy Frequently Asked Questions

192.168.1.1 and you wish to run Privoxy on port 8118, this line should look like:

```
listen-address 192.168.1.1:8118
```

Save the file, and restart Privoxy. Configure all browsers on the network then to use this address and port number.

Alternately, you can have Privoxy listen on all available interfaces:

```
listen-address :8118
```

And then use Privoxy's [permit-access](#) feature to limit connections. A firewall in this situation is recommended as well.

The above steps should be the same for any TCP network, regardless of operating system.

If you run Privoxy on a LAN with untrusted users, we recommend that you double-check the [access control and security](#) options!

3.13. Instead of ads, now I get a checkerboard pattern. I don't want to see anything.

The replacement for blocked images can be controlled with the [set-image-blocker action](#). You have the choice of a checkerboard pattern, a transparent 1x1 GIF image (aka "blank"), or a redirect to a custom image of your choice. Note that this choice only has effect for images which are blocked as images, i.e. whose URLs match both a [handle-as-image](#) and [block](#) action.

If you want to see nothing, then change the [set-image-blocker action](#) to "blank". This can be done by editing the `user.action` file, or through the [web-based actions file editor](#).

3.14. Why would anybody want to see a checkerboard pattern?

Remember that [telling which image is an ad and which isn't](#), is an educated guess. While we hope that the standard configuration is rather smart, it will make occasional mistakes. The checkerboard image is visually decent, and it shows you where images have been blocked, which can be very helpful in case some navigation aid or otherwise innocent image was erroneously blocked. It is recommended for new users so they can "see" what is happening. Some people might also enjoy seeing how many banners they *don't* have to see.

3.15. I see some images being replaced with text instead of the checkerboard image. Why and how do I get rid of this?

This happens when the banners are not embedded in the HTML code of the page itself, but in separate HTML (sub)documents that are loaded into (i)frames or (i)layers, and these external HTML documents are blocked. Being non-images they get replaced by a substitute HTML page rather than a substitute image, which wouldn't work out technically, since the browser expects and accepts only HTML when it has requested an HTML document.

The substitute page adapts to the available space and shows itself as a miniature two-liner if loaded into small frames, or full-blown with a large red "BLOCKED" banner if space allows.

If you prefer the banners to be blocked by images, you must see to it that the HTML documents in which they are embedded are not blocked. Clicking the "See why" link offered in the substitute page will show you which rule blocked the page. After changing the rule and un-blocking the HTML documents, the browser will try to load the actual banner images and the usual image blocking will (hopefully!) kick in.

3.16. Can Privoxy run as a service on Win2K/NT/XP?

Yes. Version 3.0.5 introduces full Windows service functionality. See [the User Manual](#) for details on how to install and configure Privoxy as a service.

Earlier 3.x versions could run as a system service using `srvany.exe`. See the discussion at http://sourceforge.net/tracker/?func=detail&atid=361118&aid=485617&group_id=11118, for details, and a sample configuration.

3.17. How can I make Privoxy work with other proxies like Squid or Tor?

This can be done and is often useful to combine the benefits of Privoxy with those of a another proxy. See the [forwarding chapter](#) in the [User Manual](#) which describes how to do this, and the [How do I use Privoxy together with Tor](#) section below.

3.18. Can I just set Privoxy to use port 80 and thus avoid individual browser configuration?

No, its more complicated than that. This only works with special kinds of proxies known as "intercepting" proxies (see below).

Privoxy Frequently Asked Questions

3.19. Can Privoxy run as a "transparent" proxy?

The whole idea of Privoxy is to modify client requests and server responses in all sorts of ways and therefore it's not a transparent proxy as described in [RFC 2616](#).

However, some people say "transparent proxy" when they mean "intercepting proxy". If you are one of them, please read the [next entry](#).

3.20. Can Privoxy run as a "intercepting" proxy?

Privoxy can't intercept traffic itself, but it can handle requests that were intercepted and redirected with a packet filter (like PF or iptables), as long as the `Host` header is present.

As the `Host` header is required by HTTP/1.1 and as most web sites rely on it anyway, this limitation shouldn't be a problem.

Please refer to your packet filter's documentation to learn how to intercept and redirect traffic into Privoxy. Afterward you just have to configure Privoxy to [accept intercepted requests](#).

3.21. How can I configure Privoxy for use with Outlook Express?

Outlook Express uses Internet Explorer components to both render HTML, and fetch any HTTP requests that may be embedded in an HTML email. So however you have Privoxy configured to work with IE, this configuration should automatically be shared.

3.22. How can I have separate rules just for HTML mail?

The short answer is, you can't. Privoxy has no way of knowing which particular application makes a request, so there is no way to distinguish between web pages and HTML mail. Privoxy just blindly proxies all requests. In the case of Outlook Express (see above), OE uses IE anyway, and there is no way for Privoxy to ever be able to distinguish between them (nor could any other proxy type application for that matter).

For a good discussion of some of the issues involved (including privacy and security issues), see http://sourceforge.net/tracker/?func=detail&atid=211118&aid=629518&group_id=11118.

3.23. I sometimes notice cookies sneaking through. How?

[Cookies](#) can be set in several ways. The classic method is via the `Set-Cookie` HTTP header. This is straightforward, and an easy one to manipulate, such as the Privoxy concept of [session-cookies-only](#). There is also the possibility of using [Javascript](#) to set cookies (Privoxy calls these `content-cookies`). This is trickier because the syntax can vary widely, and thus requires a certain amount of guesswork. It is not realistic to catch all of these short of disabling Javascript, which would break many sites. And lastly, if the cookies are embedded in a HTTPS/SSL secure session via Javascript, they are beyond Privoxy's reach.

All in all, Privoxy can help manage cookies in general, can help minimize the loss of privacy posed by cookies, but can't realistically stop all cookies.

3.24. Are all cookies bad? Why?

No, in fact there are many beneficial uses of [cookies](#). Cookies are just a method that browsers can use to store data between pages, or between browser sessions. Sometimes there is a good reason for this, and the user's life is a bit easier as a result. But there is a long history of some websites taking advantage of this layer of trust, and using the data they glean from you and your browsing habits for their own purposes, and maybe to your potential detriment. Such sites are using you and storing their data on your system. That is why the privacy conscious watch from whom those cookies come, and why they really *need* to be there.

See the [Wikipedia cookie definition](#) for more.

3.25. How can I allow permanent cookies for my trusted sites?

There are several actions that relate to cookies. The default behavior is to allow only "session cookies", which means the cookies only last for the current browser session. This eliminates most kinds of abuse related to cookies. But there may be cases where you want cookies to last.

To disable all cookie actions, so that cookies are allowed unrestricted, both in and out, for `example.com`:

```
{ -crunch-incoming-cookies -crunch-outgoing-cookies -session-cookies-only -filter{content-cookies} }
.example.com
```

Place the above in `user.action`. Note that some of these may be off by default anyway, so this might be redundant, but there is no harm being explicit in what you want to happen. `user.action` includes an alias for this situation, called `allow-all-cookies`.

Privoxy Frequently Asked Questions

3.26. Can I have separate configurations for different users?

Each instance of Privoxy has its own configuration, including such attributes as the TCP port that it listens on. What you can do is run multiple instances of Privoxy, each with a unique [listen-address](#) configuration setting, and configuration path, and then each of these can have their own configurations. Think of it as per-port configuration.

Simple enough for a few users, but for large installations, consider having groups of users that might share like configurations.

3.27. Can I set-up Privoxy as a whitelist of "good" sites?

Sure. There are a couple of things you can do for simple white-listing. Here's one real easy one:

```
#####
# Blacklist
#####
{ +block }
/ # Block *all* URLs

#####
# Whitelist
#####
{ -block }
  kids.example.com
  toys.example.com
  games.example.com
```

This allows access to only those three sites by first blocking all URLs, and then subsequently allowing three specific exceptions.

Another approach is Privoxy's `trustfile` concept, which incorporates the notion of "trusted referrers". See the [Trust documentation](#) for details.

These are fairly simple approaches and are not completely foolproof. There are various other configuration options that should be disabled (described elsewhere here and in [the User Manual](#)) so that users can't modify their own configuration and easily circumvent the whitelist.

3.28. How can I turn off ad-blocking?

Ad blocking is achieved through a complex application of various Privoxy [actions](#). These actions are deployed against simple images, banners, flash animations, text pages, JavaScript, pop-ups and popunders, etc., so its not as simple as just turning one or two actions off. The various actions that make up Privoxy ad blocking are hard-coded into the default configuration files. It has been assumed that everyone using Privoxy is interested in this particular feature.

If you want to do without this, there are several approaches you can take: You can manually undo the many block rules in `default.action`. Or even easier, just create your own `default.action` file from scratch without the many ad blocking rules, and corresponding exceptions. Or lastly, if you are not concerned about the additional blocks that are done for privacy reasons, you can very easily over-ride *all* blocking with the following very simple rule in your `user.action`:

```
# Unblock everybody, everywhere
{ -block }
/ # UN-Block *all* URLs
```

Or even a more comprehensive reversing of various ad related actions:

```
# Unblock everybody, everywhere, and turn off appropriate filtering, etc
{ -block \
  -filter{banners-by-size} \
  -filter{banners-by-link} \
  allow-popups \
}
/ # UN-Block *all* URLs and allow ads
```

This last "action" in this compound statement, `allow-popups`, is an [alias](#) that disables various pop-up blocking features.

3.29. How can I have custom template pages, like the **BLOCKED** page?

Privoxy "templates" are specialized text files utilized by Privoxy for various purposes and can easily be modified using any text editor. All the template pages are installed in a sub-directory appropriately named: `templates`. Knowing something about HTML syntax will of course be helpful.

Be forewarned that the default templates are subject to being overwritten during upgrades. You can, however, create completely new templates, place them in another directory and specify the alternate path in the main `config`. For details, have a look at the [templdir](#) option.

Privoxy Frequently Asked Questions

3.30. How can I remove the "Go There Anyway" link from the *BLOCKED* page?

There is more than one way to do it (although Perl is not involved).

Editing the *BLOCKED* template page (see above) may dissuade some users, but this method is easily circumvented. Where you need this level of control, you might want to build Privoxy from source, and disable various features that are available as compile-time options. You should **configure** the sources as follows:

```
./configure --disable-toggle --disable-editor --disable-force
```

This will create an executable with hard-coded security features so that Privoxy does not allow easy bypassing of blocked sites, or changing the current configuration via any connected user's web browser.

Finally, all of these features can also be toggled on/off via options in Privoxy's main config file which means you don't have to recompile anything.

4. Miscellaneous

4.1. How much does Privoxy slow my browsing down? This has to add extra time to browsing.

How much of an impact depends on many things, including the CPU of the host system, how aggressive the configuration is, which specific actions are being triggered, the size of the page, the bandwidth of the connection, etc.

Overall, it should not slow you down any in real terms, and may actually help speed things up since ads, banners and other junk are not typically being retrieved and displayed. The actual processing time required by Privoxy itself for each page, is relatively small in the overall scheme of things, and happens very quickly. This is typically more than offset by time saved not downloading and rendering ad images and other junk content (if ad blocking is being used).

"Filtering" content via the [filter](#) or [deanimate-gifs](#) actions may cause a perceived slowdown, since the entire document needs to be buffered before displaying. And on very large documents, filtering may have some measurable impact. How much depends on the page size, the actual definition of the filter(s), etc. See below. Most other actions have little to no impact on speed.

Also, when filtering is enabled but zlib support isn't available, compression is often disabled (see [prevent-compression](#)). This can have an impact on speed as well, although it's probably smaller than you might think. Again, the page size, etc. will determine how much of an impact.

4.2. I notice considerable delays in page requests. What's wrong?

If you use any [filter](#) action, such as filtering banners by size, web-bugs etc, or the [deanimate-gifs](#) action, the entire document must be loaded into memory in order for the filtering mechanism to work, and nothing is sent to the browser during this time.

The loading time typically does not really change much in real numbers, but the feeling is different, because most browsers are able to start rendering incomplete content, giving the user a feeling of "it works". This effect is more noticeable on slower dialup connections. Extremely large documents may have some impact on the time to load the page where there is filtering being done. But overall, the difference should be very minimal. If there is a big impact, then probably some other situation is contributing (like anti-virus software).

Filtering is automatically disabled for inappropriate MIME types. But note that if the web server mis-reports the MIME type, then content that should not be filtered, could be. Privoxy only knows how to differentiate filterable content because of the MIME type as reported by the server, or because of some configuration setting that enables/disables filtering.

4.3. What are "http://config.privoxy.org/" and "http://p.p/"?

<http://config.privoxy.org/> is the address of Privoxy's built-in user interface, and <http://p.p/> is a shortcut for it.

Since Privoxy sits between your web browser and the Internet, it can simply intercept requests for these addresses and answer them with its built-in "web server".

This also makes for a good test for your browser configuration: If entering the URL <http://config.privoxy.org/> takes you to a page saying "This is Privoxy ...", everything is OK. If you get a page saying "Privoxy is not working" instead, then your browser didn't use Privoxy for the request, hence it could not be intercepted, and you have accessed the *real* web site at config.privoxy.org.

4.4. How can I submit new ads, or report problems?

Please see the [Contact section](#) for various ways to interact with the developers.

4.5. If I do submit missed ads, will they be included in future updates?

Whether such submissions are eventually included in the `default.action` configuration file depends on how significant the issue is. We of course want to address any potential problem with major, high-profile sites such as *Google*, *Yahoo*, etc. Any site with global or regional reach, has a good chance of being a candidate. But at the other end of the spectrum are any number of smaller, low-profile sites such as for local clubs or schools. Since their reach and impact are much less, they are best handled by inclusion in the user's `user.action`, and thus would be unlikely to be included.

4.6. Why doesn't anyone answer my support request?

Rest assured that it has been read and considered. Why it is not answered, could be for various reasons, including no one has a good answer for it, no one has had time to yet investigate it thoroughly, it has been reported numerous times already, or because not enough information was provided to help us help you. Your efforts are not wasted, and we do appreciate them.

Privoxy Frequently Asked Questions

4.7. How can I hide my IP address?

If you run both the browser and Privoxy locally, you cannot hide your IP address with Privoxy or ultimately any other software alone. The server needs to know your IP address so that it knows where to send the responses back.

There are many publicly usable "anonymous" proxies out there, which provide a further level of indirection between you and the web server.

However, these proxies are called "anonymous" because you don't need to authenticate, not because they would offer any real anonymity. Most of them will log your IP address and make it available to the authorities in case you violate the law of the country they run in. In fact you can't even rule out that some of them only exist to *collect* information on (those suspicious) people with a more than average preference for privacy.

If you want to hide your IP address from most adversaries, you should consider chaining Privoxy with [Tor](#). The configuration details can be found in [How do I use Privoxy together with Tor section](#) just below.

4.8. Can Privoxy guarantee I am anonymous?

No. Your chances of remaining anonymous are improved, but unless you [chain Privoxy with Tor](#) or a similar proxy and know what you're doing when it comes to configuring the rest of your system, you should assume that everything you do on the Web can be traced back to you.

Privoxy can remove various information about you, and allows *you* more freedom to decide which sites you can trust, and what details you want to reveal. But it neither hides your IP address, nor can it guarantee that the rest of the system behaves correctly. There are several possibilities how a web sites can find out who you are, even if you are using a strict Privoxy configuration and chained it with Tor.

Most of Privoxy's privacy-enhancing features can be easily subverted by an insecure browser configuration, therefore you should use a browser that can be configured to only execute code from trusted sites, and be careful which sites you trust. For example there is no point in having Privoxy modify the User-Agent header, if websites can get all the information they want through JavaScript, ActiveX, Flash, Java etc.

A few browsers disclose the user's email address in certain situations, such as when transferring a file by FTP. Privoxy does not filter FTP. If you need this feature, or are concerned about the mail handler of your browser disclosing your email address, you might consider products such as NSClean.

Browsers available only as binaries could use non-standard headers to give out any information they can have access to: see the manufacturer's license agreement. It's impossible to anticipate and prevent every breach of privacy that might occur. The professionally paranoid prefer browsers available as source code, because anticipating their behavior is easier. Trust the source, Luke!

4.9. A test site says I am not using a Proxy.

Good! Actually, they are probably testing for some other kinds of proxies. Hiding yourself completely would require additional steps.

4.10. How do I use Privoxy together with Tor?

Before you configure Privoxy to use [Tor](#), please follow the *User Manual* chapters [2. Installation](#) and [5. Startup](#) to make sure Privoxy itself is setup correctly.

If it is, refer to [Tor's extensive documentation](#) to learn how to install Tor, and make sure Tor's logfile says that "Tor has successfully opened a circuit" and it "looks like client functionality is working".

If either Tor or Privoxy isn't working, their combination most likely will neither. Testing them on their own will also help you to direct problem reports to the right audience. If Privoxy isn't working, don't bother the Tor developers. If Tor isn't working, don't send bug reports to the Privoxy Team.

If you verified that Privoxy and Tor are working, it is time to connect them. As far as Privoxy is concerned, Tor is just another proxy that can be reached by socks4 or socks4a. Most likely you are interested in Tor to increase your anonymity level, therefore you should use socks4a, to make sure DNS requests are done through Tor and thus invisible to your local network.

Since Privoxy 3.0.5, its [main configuration file](#) is already prepared for Tor, if you are using a default Tor configuration and run it on the same system as Privoxy, you just have to edit the [forwarding section](#) and uncomment the line:

```
# forward-socks4a          / 127.0.0.1:9050 .
```

This is enough to reach the Internet, but additionally you might want to uncomment the following forward rules, to make sure your local network is still reachable through Privoxy:

```
# forward 192.168.*.*/ .
# forward 10.*.*.*/ .
```

Privoxy Frequently Asked Questions

```
# forward 127.*.*.*/ .
```

Unencrypted connections to systems in these address ranges will be as (un)secure as the local network is, but the alternative is that your browser can't reach the network at all. Then again, that may actually be desired and if you don't know for sure that your browser has to be able to reach the local network, there's no reason to allow it.

If you want your browser to be able to reach servers in your local network by using their names, you will need additional exceptions that look like this:

```
# forward localhost/ .
```

Save the modified configuration file and open <http://config.privoxy.org/show-status/> in your browser, confirm that Privoxy has reloaded its configuration and that there are no other forward lines, unless you know that you need them. If everything looks good, refer to [Tor Faq 4.2](#) to learn how to verify that you are really using Tor.

Afterward, please take the time to at least skim through the rest of Tor's documentation. Make sure you understand what Tor does, why it is no replacement for application level security, and why you probably don't want to use it for unencrypted logins.

4.11. Might some things break because header information or content is being altered?

Definitely. It is common for sites to use browser type, browser version, HTTP header content, and various other techniques in order to dynamically decide what to display and how to display it. What you see, and what I see, might be very different. There are many, many ways that this can be handled, so having hard and fast rules, is tricky.

The "User-Agent" is sometimes used in this way to identify the browser, and adjust content accordingly.

Also, different browsers use different encodings of non-English characters, certain web servers convert pages on-the-fly according to the User Agent header. Giving a "User Agent" with the wrong operating system or browser manufacturer causes some sites in these languages to be garbled; Surfers to Eastern European sites should change it to something closer. And then some page access counters work by looking at the "Referer" header; they may fail or break if unavailable. The weather maps of Intellicast have been blocked by their server when no "Referer" or cookie is provided, is another example. (But you can forge both headers without giving information away). There are many other ways things can go wrong when trying to fool a web server. The results of which could inadvertently cause pages to load incorrectly, partially, or even not at all. And there may be no obvious clues as to just what went wrong, or why. Nowhere will there be a message that says "*Turn off fast-redirects or else!*"

Similar thoughts apply to modifying JavaScript, and, to a lesser degree, HTML elements.

If you have problems with a site, you will have to adjust your configuration accordingly. Cookies are probably the most likely adjustment that may be required, but by no means the only one.

4.12. Can Privoxy act as a "caching" proxy to speed up web browsing?

No, it does not have this ability at all. You want something like [Squid](#) or [Polipo](#) for this. And, yes, before you ask, Privoxy can co-exist with other kinds of proxies like Squid. See the [forwarding chapter](#) in the [user manual](#) for details.

4.13. What about as a firewall? Can Privoxy protect me?

Not in the way you mean, or in the way some firewall vendors claim they can. Privoxy can help protect your privacy, but can't protect your system from intrusion attempts. It is, of course, perfectly possible to use *both*.

4.14. I have large empty spaces / a checkerboard pattern now where ads used to be. Why?

It is technically possible to eliminate banners and ads in a way that frees their allocated page space. This could easily be done by blocking with Privoxy's filters, and eliminating the *entire* image references from the HTML page source.

But, this would consume considerably more CPU resources (IOW, slow things down), would likely destroy the layout of some web pages which rely on the banners utilizing a certain amount of page space, and might fail in other cases, where the screen space is reserved (e.g. by HTML tables for instance). Also, making ads and banners disappear without any trace complicates troubleshooting, and would sooner or later be problematic.

The better alternative is to instead let them stay, and block the resulting requests for the banners themselves as is now the case. This leaves either empty space, or the familiar checkerboard pattern.

So the developers won't support this in the default configuration, but you can of course define appropriate filters yourself to achieve this.

Privoxy Frequently Asked Questions

4.15. How can Privoxy filter Secure (HTTPS) URLs?

Since secure HTTP connections are encrypted SSL sessions between your browser and the secure site, and are meant to be reliably *secure*, there is little that Privoxy can do but hand the raw gibberish data though from one end to the other unprocessed.

The only exception to this is blocking by host patterns, as the client needs to tell Privoxy the name of the remote server, so that Privoxy can establish the connection. If that name matches a host-only pattern, the connection will be blocked.

As far as ad blocking is concerned, this is less of a restriction than it may seem, since ad sources are often identifiable by the host name, and often the banners to be placed in an encrypted page come unencrypted nonetheless for efficiency reasons, which exposes them to the full power of Privoxy's ad blocking.

"Content cookies" (those that are embedded in the actual HTML or JS page content, see [filter{content-cookies}](#)), in an SSL transaction will be impossible to block under these conditions. Fortunately, this does not seem to be a very common scenario since most cookies come by traditional means.

4.16. Privoxy runs as a "server". How secure is it? Do I need to take any special precautions?

On Unix-like systems, Privoxy can run as a non-privileged user, which is how we recommend it be run. Also, by default Privoxy listens to requests from "localhost" only.

The server aspect of Privoxy is not itself directly exposed to the Internet in this configuration. If you want to have Privoxy serve as a LAN proxy, this will have to be opened up to allow for LAN requests. In this case, we'd recommend you specify only the LAN gateway address, e.g. 192.168.1.1, in the main Privoxy configuration file and check all [access control and security options](#). All LAN hosts can then use this as their proxy address in the browser proxy configuration, but Privoxy will not listen on any external interfaces. ACLs can be defined in addition, and using a firewall is always good too. Better safe than sorry.

4.17. Can I temporarily disable Privoxy?

Privoxy doesn't have a transparent proxy mode, but you can toggle off blocking and content filtering.

The easiest way to do that is to point your browser to the remote toggle URL: <http://config.privoxy.org/toggle>.

See the [Bookmarklets section](#) of the *User Manual* for an easy way to access this feature. Note that this is a feature that may need to be enabled in the main `config` file.

4.18. When "disabled" is Privoxy totally out of the picture?

No, this just means all optional filtering and actions are disabled. Privoxy is still acting as a proxy, but just doing less of the things that Privoxy would normally be expected to do. It is still a "middle-man" in the interaction between your browser and web sites. See below to bypass the proxy.

4.19. How can I tell Privoxy to totally ignore certain sites?

Bypassing a proxy, or proxying based on arbitrary criteria, is purely a browser configuration issue, not a Privoxy issue. Modern browsers typically do have settings for not proxying certain sites. Check your browser's help files.

4.20. My logs show Privoxy "crunches" ads, but also its own internal CGI pages. What is a "crunch"?

A "crunch" simply means Privoxy intercepted *something*, nothing more. Often this is indeed ads or banners, but Privoxy uses the same mechanism for trapping requests for its own internal pages. For instance, a request for Privoxy's configuration page at: <http://config.privoxy.org>, is intercepted (i.e. it does not go out to the 'net), and the familiar CGI configuration is returned to the browser, and the log consequently will show a "crunch".

Since version 3.0.7, Privoxy will also log the crunch reason. If you are using an older version you might want to upgrade.

4.21. Can Privoxy effect files that I download from a webserver? FTP server?

From the webserver's perspective, there is no difference between viewing a document (i.e. a page), and downloading a file. The same is true of Privoxy. If there is a match for a [block](#) pattern, it will still be blocked, and of course this is obvious.

Filtering is potentially more of a concern since the results are not always so obvious, and the effects of filtering are there whether the file is simply viewed, or downloaded. And potentially whether the content is some obnoxious advertisement, or Mr. Jimmy's latest/greatest source code jewel. Of course, one of these presumably is "bad" content that we don't want, and the other is "good" content that we do want. Privoxy is blind to the differences, and can only distinguish "good from bad" by the configuration parameters we give it.

Privoxy Frequently Asked Questions

Privoxy knows the differences in files according to the "Content Type" as reported by the webserver. If this is reported accurately (e.g. "application/zip" for a zip archive), then Privoxy knows to ignore these where appropriate. Privoxy potentially can filter HTML as well as plain text documents, subject to configuration parameters of course. Also, documents that are of an unknown type (generally assumed to be "text/plain") can be filtered, as will those that might be incorrectly reported by the webserver. If such a file is a downloaded file that is intended to be saved to disk, then any content that might have been altered by filtering, will be saved too, for these (probably rare) cases.

Note that versions later than 3.0.2 do NOT filter document types reported as "text/plain". Prior to this, Privoxy did filter this document type.

In short, filtering is "ON" if a) the content type as reported by the webserver is appropriate *and* b) the configuration allows it (or at least does not disallow it). That's it. There is no magic cookie anywhere to say this is "good" and this is "bad". It's the configuration that lets it all happen or not.

If you download text files, you probably do not want these to be filtered, particularly if the content is source code, or other critical content. Source code sometimes might be mistaken for Javascript (i.e. the kind that might open a pop-up window). It is recommended to turn off filtering for download sites (particularly if the content may be plain text files and you are using version 3.0.2 or earlier) in your `user.action` file. And also, for any site or page where making *any* changes at all to the content is to be avoided.

Privoxy does not do FTP at all, only HTTP and HTTPS (SSL) protocols, so please don't try.

4.22. I just downloaded a Perl script, and Privoxy altered it! Yikes, what is wrong!

Please read above.

4.23. Should I continue to use a "HOSTS" file for ad-blocking?

One time-tested technique to defeat common ads is to trick the local DNS system by giving a phony IP address for the ad generator in the local `HOSTS` file, typically using `127.0.0.1`, aka `localhost`. This effectively blocks the ad.

There is no reason to use this technique in conjunction with Privoxy. Privoxy does essentially the same thing, much more elegantly and with much more flexibility. A large `HOSTS` file, in fact, not only duplicates effort, but may get in the way and seriously slow down your system. It is recommended to remove such entries from your `HOSTS` file. If you think your hosts list is neglected by Privoxy's configuration, consider adding your list to your `user.action` file:

```
{ +block }
www.ad.example1.com
ad.example2.com
ads.galore.example.com
etc.example.com
```

4.24. Where can I find more information about Privoxy and related issues?

Other references and sites of interest to Privoxy users:

<http://www.privoxy.org/>, the Privoxy Home page.

<http://www.privoxy.org/faq/>, the Privoxy FAQ.

<http://sourceforge.net/projects/iibswa/>, the Project Page for Privoxy on [SourceForge](#).

<http://config.privoxy.org/>, the web-based user interface. Privoxy must be running for this to work. Shortcut: <http://p.p/>

http://sourceforge.net/tracker/?group_id=11118&atid=460288, to submit "misses" and other configuration related suggestions to the developers.

<http://www.junkbusters.com/ht/en/cookies.html>, an explanation how cookies are used to track web users.

<http://www.junkbusters.com/ijb.html>, the original Internet Junkbuster.

<http://privacy.net/>, a useful site to check what information about you is leaked while you browse the web.

<http://www.squid-cache.org/>, a popular caching proxy, which is often used together with Privoxy.

<http://www.pps.jussieu.fr/~jch/software/polipo/>, Polipo is a caching proxy with advanced features like pipelining, multiplexing and caching of partial instances. In many setups it can be used as Squid replacement.

<http://tor.eff.org/>, Tor can help anonymize web browsing, web publishing, instant messaging, IRC, SSH, and other applications.

4. Miscellaneous

Privoxy Frequently Asked Questions

<http://www.privoxy.org/developer-manual/>, the Privoxy developer manual.

4.25. I've noticed that Privoxy changes "Microsoft" to "MicroSuck"! Why are you manipulating my browsing?

We're not. The text substitutions that you are seeing are disabled in the default configuration as shipped. You have either manually activated the "Fun" filter which is clearly labeled "Text replacements for subversive browsing fun!" or you are using an older Privoxy version and have implicitly activated it by choosing the "Adventuresome" profile in the web-based editor. Please upgrade.

4.26. Does Privoxy produce "valid" HTML (or XHTML)?

Privoxy generates HTML in both its own "templates", and possibly whenever there are text substitutions via a Privoxy filter. While this should always conform to the HTML 4.01 specifications, it has not been validated against this or any other standard.

5. Troubleshooting

5.1. I cannot connect to any websites. Or, I am getting "connection refused" message with every web page. Why?

There are several possibilities:

- Privoxy is not running. Solution: verify that Privoxy is installed correctly, has not crashed, and is indeed running. Turn on Privoxy's logging, and look at the logs to see what they say.
- Or your browser is configured for a different port than what Privoxy is using. Solution: verify that Privoxy and your browser are set to the same port (`listen-address`).
- Or if using a forwarding rule, you have a configuration problem or a problem with a host in the forwarding chain. Solution: temporarily alter your configuration and take the forwarders out of the equation.
- Or you have a firewall that is interfering and blocking you. Solution: try disabling or removing the firewall as a simple test.

5.2. Why am I getting a 503 Error (WSAECONNREFUSED) on every page?

More than likely this is a problem with your TCP/IP networking. ZoneAlarm has been reported to cause this symptom -- even if not running! The solution is to either fight the ZA configuration, or uninstall ZoneAlarm, and then find something better behaved in its place. Other personal firewall type products may cause similar type problems if not configured correctly.

5.3. I just added a new rule, but the steenkin ad is still getting through. How?

If the ad had been displayed before you added its URL, it will probably be held in the browser's cache for some time, so it will be displayed without the need for any request to the server, and Privoxy will not be involved. Flush the browser's caches, and then try again.

If this doesn't help, you probably have an error in the rule you applied. Try pasting the full URL of the offending ad into <http://config.privoxy.org/show-url-info> and see if it really matches your new rule. Blocking ads is like blocking spam: a lot of tinkering is required to stay ahead of the game. And remember you need to block the URL of the ad in question, which may be entirely different from the site URL itself. Most ads are hosted on different servers than the main site itself. If you right-click on the ad, you should be able to get all the relevant information you need. Alternately, you can find the correct URL by looking at Privoxy's logs (you may need to enable logging in the main config file if its disabled).

Below is a slightly modified real-life log snippet that originates with one requested URL: `www.example.com` (name of site was changed for this example, the number of requests is real). You can see in this the complexity of what goes into making up this one "page". There are eight different domains involved here, with thirty two separate URLs requested in all, making up all manner of images, Shockwave Flash, JavaScript, CSS stylesheets, scripts, and other related content. Some of this content is obviously "good" or "bad", but not all. Many of the more questionable looking requests, are going to outside domains that seem to be identifying themselves with suspicious looking names, making our job a little easier. Privoxy has "crunched" (meaning caught and BLOCKED) quite a few items in this example, but perhaps missed a few as well.

```
Request: www.example.com/
Request: www.example.com/favicon.ico
Request: img.example.com/main.css
Request: img.example.com/sr.js
Request: example.betamarker.com/example.html
Request: www.lik-sang.com/Banners/bestsellers/skyscraper.php?likref=BSellers
Request: img.example.com/pb.png
Request: www.google-analytics.com/urchin.js crunch! (Blocked)
Request: www.advertising-department.com/ats/switch.ps.php?26856 crunch! (Blocked)
Request: img.example.com/p.gif
Request: www.popuptraffic.com/assign.php?l=example&mode=behind crunch! (Blocked)
Request: www.popuptraffic.com/scripts/popup.php?hid=5c3cf&tmpl=PBa.tml crunch! (Blocked)
Request: www.popuptraffic.com/assign.php?l=example crunch! (Blocked)
Request: www.lik-sang.com/Banners/best_sellers/best_sellers.css
Request: www.adtrak.net/adx.js crunch! (Blocked)
Request: img.example.com/hbg.gif
Request: img.example.com/example.jpg
Request: img.example.com/mt.png
Request: img.example.com/mm.png
Request: img.example.com/mb.png
Request: www.popuptraffic.com/scripts/popup.php?hid=a71b91fa5&tmpl=Ua.tmp crunch! (Blocked)
Request: www.example.com/tracker.js
Request: www.lik-sang.com/Banners/best_sellers/lsi_head.gif
Request: www.adtrak.net/adjs.php?n=020548130&what=zone:61 crunch! (Blocked)
Request: www.adtrak.net/adjs.php?n=463594413&what=zone:58&source=Ua crunch! (Blocked)
Request: www.lik-sang.com/Banners/best_sellers/bottomani.swf
Request: mmm.elitemediagroup.net/install.php?allowpop=no&popupmincook=0&allowsp2=1 crunch! (Blocked)
Request: www.example.com/tracker.js?screen=1400x1050&win=962x693
Request: www.adtrak.net/adlog.php?bannerid=1309&clientid=439&zoneid=61 crunch! (Blocked)
Request: 66.70.21.80/scripts/click.php?hid=5c3cf599a9efd0320d26&si
Request: 66.70.21.80/img/pixel.gif
Request: www.adtrak.net/adlog.php?bannerid=1309&clientid=439&zoneid=58&source=Ua&block=86400 crunch! (Blocked)
```

Privoxy Frequently Asked Questions

Request: 66.70.21.80/scripts/click.php?hid=a71b9f6504b0c5681fa5&si=Ua

Despite 12 out of 32 requests being blocked, the page looked, and seemed to behave perfectly "normal" (minus some ads, of course).

5.4. One of my favorite sites does not work with Privoxy. What can I do?

First verify that it is indeed a Privoxy problem, by toggling off Privoxy through <http://config.privoxy.org/toggle> (the toggle feature may need to be enabled in the main `config`), and then shift-reloading the problem page (i.e. holding down the shift key while clicking reload). Alternatively, flush your browser's disk and memory caches).

If the problem went away, we know we have a configuration related problem. Now go to <http://config.privoxy.org/show-url-info> and paste the full URL of the page in question into the prompt. See which actions are being applied to the URL, and which matches in which actions files are responsible for that. It might be helpful also to look at your logs for this site too, to see what else might be happening (note: logging may need to be enabled in the main config file). Many sites are complex and require a number of related pages to help present their content. Look at what else might be used by the page in question, and what of that might be *required*. Now, armed with this information, go to <http://config.privoxy.org/show-status> and select the appropriate actions files for editing.

You can now either look for a section which disables the actions that you suspect to cause the problem and add a pattern for your site there, or make up a completely new section for your site. In any case, the recommended way is to disable only the prime suspect, reload the problem page, and only if the problem persists, disable more and more actions until you have identified the culprit. You may or may not want to turn the other actions on again. Remember to flush your browser's caches in between any such changes!

Alternately, if you are comfortable with a text editor, you can accomplish the same thing by editing the appropriate actions file. Probably the easiest way to deal with such problems when editing by hand is to add your site to a `{ fragile }` section in `user.action`, which is an alias that turns off most "dangerous" actions, but is also likely to turn off more actions than needed, and thus lower your privacy and protection more than necessary,

Troubleshooting actions is discussed in more detail in the [User Manual appendix, Troubleshooting: the Anatomy of an Action](#). There is also an [actions tutorial](#) with general configuration information and examples.

As a last resort, you can always see if your browser has a setting that will bypass the proxy setting for selective sites. Modern browsers can do this.

5.5. After installing Privoxy, I have to log in every time I start IE. What gives?

This is a quirk that effects the installation of Privoxy, in conjunction with Internet Explorer and Internet Connection Sharing on Windows 2000 and Windows XP. The symptoms may appear to be corrupted or invalid DUN settings, or passwords.

When setting up an NT based Windows system with Privoxy you may find that things do not seem to be doing what you expect. When you set your system up you will probably have set up Internet Connection Sharing (ICS) with Dial up Networking (DUN) when logged in with administrator privileges. You will probably have made this DUN connection available to other accounts that you may have set-up on your system. E.g. Mum or Dad sets up the system and makes accounts suitably configured for the kids.

When setting up Privoxy in this environment you will have to alter the proxy set-up of Internet Explorer (IE) for the specific DUN connection on which you wish to use Privoxy. When you do this the ICS DUN set-up becomes user specific. In this instance you will see no difference if you change the DUN connection under the account used to set-up the connection. However when you do this from another user you will notice that the DUN connection changes to make available to "Me only". You will also find that you have to store the password under each different user!

The reason for this is that each user's set-up for IE is user specific. Each set-up DUN connection and each LAN connection in IE store the settings for each user individually. As such this enforces individual configurations rather than common ones. Hence the first time you use a DUN connection after re-booting your system it may not perform as you expect, and prompt you for the password. Just set and save the password again and all should be OK.

[Thanks to Ray Griffith for this submission.]

5.6. I cannot connect to any FTP sites. Privoxy is blocking me.

Privoxy cannot act as a proxy for FTP traffic, so do not configure your browser to use Privoxy as an FTP proxy. The same is true for *any protocol other than HTTP or HTTPS (SSL)*.

Most browsers understand FTP as well as HTTP. If you connect to a site, with a URL like `ftp://ftp.example.com`, your browser is making an FTP connection, and not a HTTP connection. So while your browser may speak FTP, Privoxy does not, and cannot proxy such traffic.

To complicate matters, some systems may have a generic "proxy" setting, which will enable various protocols, including *both* HTTP and FTP proxying! So it is possible to accidentally enable FTP proxying in these cases. And of course, if this happens, Privoxy will indeed cause problems since it does not know FTP. Newer version will give a sane error message if a FTP connection is attempted. Just disable the FTP setting and all will be well again.

Privoxy Frequently Asked Questions

Will Privoxy ever proxy FTP traffic? Unlikely. There just is not much reason, and the work to make this happen is more than it may seem.

5.7. In Mac OSX, I can't configure Microsoft Internet Explorer to use Privoxy as the HTTP proxy.

Microsoft Internet Explorer (in versions like 5.1) respects system-wide network settings. In order to change the HTTP proxy, open System Preferences, and click on the Network icon. In the settings pane that comes up, click on the Proxies tab. Ensure the "Web Proxy (HTTP)" checkbox is checked and enter `127.0.0.1` in the entry field. Enter `8118` in the Port field. The next time you start IE, it should reflect these values.

5.8. In Mac OSX, I dragged the Privoxy folder to the trash in order to uninstall it. Now the finder tells me I don't have sufficient privileges to empty the trash.

Just dragging the Privoxy folder to the trash is not enough to delete it. Privoxy supplies an `uninstall.command` file that takes care of these details. Open the trash, drag the `uninstall.command` file out of the trash and double-click on it. You will be prompted for confirmation and the administration password.

The trash may still appear full after this command; emptying the trash from the desktop should make it appear empty again.

5.9. In Mac OSX Panther (10.3), images often fail to load and/or I experience random delays in page loading. I'm using `localhost` as my browser's proxy setting.

We believe this is due to an IPv6-related bug in OSX, but don't fully understand the issue yet. In any case, changing the proxy setting to `127.0.0.1` instead of `localhost` works around the problem.

5.10. I get a completely blank page at one site. "View Source" shows only: `<html><body></body></html>`. Without Privoxy the page loads fine.

Chances are that the site suffers from a bug in [PHP](#), which results in empty pages being sent if the client explicitly requests an uncompressed page, like Privoxy does. This bug has been fixed in [PHP 4.2.3](#).

To find out if this is in fact the source of the problem, try adding the site to a `-prevent-compression` section in `user.action`:

```
# Make exceptions for ill-behaved sites:
#
{-prevent-compression}
.example.com
```

If that works, you may also want to report the problem to the site's webmasters, telling them to use `zlib.output_compression` instead of `ob_gzhandler` in their PHP applications (workaround) or upgrade to [PHP 4.2.3](#) or later (fix).

5.11. My logs show many "Unable to get my own hostname" lines. Why?

Privoxy tries to get the hostname of the system its running on from the IP address of the system interface it is bound to (from the `config` file `listen-address` setting). If the system cannot supply this information, Privoxy logs this condition.

Typically, this would be considered a minor system configuration error. It is not a fatal error to Privoxy however, but may result in a much slower response from Privoxy on some platforms due to DNS timeouts.

This can be caused by a problem with the local `HOSTS` file. If this file has been changed from the original, try reverting it to see if that helps. Make sure whatever name(s) are used for the local system, that they resolve both ways.

5.12. When I try to launch Privoxy, I get an error message "port 8118 is already in use" (or similar wording). Why?

Port 8118 is Privoxy's default TCP "listening" port. Typically this message would mean that there is already one instance of Privoxy running, and your system is actually trying to start a second Privoxy on the same port, which will not work. (You can have multiple instances but they must be assigned different ports.) How and why this might happen varies from platform to platform, but you need to check your installation and start-up procedures.

5.13. Pages with UTF-8 fonts are garbled.

This is caused by the "demonizer" filter. You should either upgrade Privoxy, or at least upgrade to the most recent `default.action` file available from [SourceForge](#). Or you can simply disable the demonizer filter.

Privoxy Frequently Asked Questions

5.14. Why are binary files (such as images) corrupted when Privoxy is used?

This may also be caused by the "demoronizer" filter, in conjunction with a web server that is misreporting the content type. Binary files are exempted from Privoxy's filtering (unless the web server by mistake says the file is something else). Either upgrade Privoxy, or go to the most recent `default.action` file available from [SourceForge](#).

5.15. What is the "demoronizer" and why is it there?

The original demoronizer was a Perl script that cleaned up HTML pages which were created with certain Microsoft products. MS has used proprietary extensions to standardized font encodings (ISO 8859-1), which has caused problems for pages that are viewed with non-Microsoft products (and are expecting to see a standard set of fonts). The demoronizer corrected these errors so the pages displayed correctly. Privoxy borrowed from this script, introducing a filter based on the original demoronizer, which in turn could correct these errors on the fly.

But this is only needed in some situations, and will cause serious problems in some other situations.

If you are using Microsoft products, you do not need it. If you need to view pages with UTF-8 characters (such as Cyrillic or Chinese), then it will cause corruption of the fonts, and thus *should not be on*.

On the other hand, if you use non-Microsoft products, and you occasionally notice weird characters on pages, you might want to try it.

5.16. Why do I keep seeing "PrivoxyWindowOpen()" in raw source code?

Privoxy is attempting to disable malicious [Javascript](#) in this case, with the `unsolicited-popups` filter. Privoxy cannot tell very well "good" code snippets from "bad" code snippets.

If you see this in HTML source, and the page displays without problems, then this is good, and likely some pop-up window was disabled. If you see this where it is causing a problem, such as a downloaded program source code file, then you should set an exception for this site or page such that the integrity of the page stays in tact by disabling all filtering.

5.17. I am getting too many DNS errors like "404 No Such Domain". Why can't Privoxy do this better?

There are potentially several factors here. First of all, the DNS resolution is done by the underlying operating system -- not Privoxy itself. Privoxy merely initiates the process and hands it off, and then later reports whatever the outcome was. And tries to give a coherent message if there seems to be a problem. In some cases, this might otherwise be mitigated by the browser itself which might try some work-arounds and alternate approaches (e.g adding "www." to the URL).

In other cases, if Privoxy is being chained with another proxy, this could complicate the issue, and cause undue delays and timeouts. In the case of a "socks4a" proxy, the socks server handles all the DNS. Privoxy would just be the "messenger" which is reporting whatever problem occurred downstream, and not the root cause of the error.

In any case, versions newer than 3.0.3 include various improvements to help Privoxy better handle these cases.

5.18. At one site Privoxy just hangs, and starts taking all CPU. Why is this?

This is probably a manifestation of the "100% cpu" problem that occurs on pages containing many (thousands upon thousands) of blank lines. The blank lines are in the raw HTML source of the page, and the browser just ignores them. But the pattern matching in Privoxy's page filtering mechanism is trying to match against absurdly long strings and this becomes very CPU-intensive, taking a long, long time to complete. Until a better solution comes along, disable filtering on these pages, particularly the `js-annoyances` and `unsolicited-popups` filters.

5.19. I just installed Privoxy, and all my browsing has slowed to a crawl. What gives?

This should not happen, and for the overwhelming number of users world-wide, it does not happen. I would suspect some inadvertent interaction of software components such as anti-virus software, spyware protectors, personal firewalls or similar components. Try disabling (or uninstalling) these one at a time and see if that helps.

5.20. Why do my filters work on some sites but not on others?

It's probably due to compression. It is a common practice for web servers to send their content "compressed" in order to speed things up, and then let the browser "uncompress" them. When compiled with zlib support Privoxy can decompress content before filtering, otherwise you may want to enable [prevent-compression](#).

6. Contacting the developers, Bug Reporting and Feature Requests

We value your feedback. In fact, we rely on it to improve Privoxy and its configuration. However, please note the following hints, so we can provide you with the best support:

6.1. Get Support

For casual users, our [support forum at SourceForge](http://sourceforge.net/tracker/?group_id=11118&atid=211118) is probably best suited: http://sourceforge.net/tracker/?group_id=11118&atid=211118

All users are of course welcome to discuss their issues on the [users mailing list](#), where the developers also hang around.

Note that the Privoxy mailing lists are moderated. Posts from unsubscribed addresses have to be accepted manually by a moderator. This may cause a delay of several days and if you use a subject that doesn't clearly mention Privoxy or one of its features, your message may be accidentally discarded as spam.

If you aren't subscribed, you should therefore spend a few seconds to come up with a proper subject. Additionally you should make it clear that you want to get CC'd. Otherwise some responses will be directed to the mailing list only, and you won't see them.

6.2. Reporting Problems

"Problems" for our purposes, come in two forms:

- Configuration issues, such as ads that slip through, or sites that don't function properly due to one Privoxy "action" or another being turned "on".
 - "Bugs" in the programming code that makes up Privoxy, such as that might cause a crash.
-

6.2.1. Reporting Ads or Other Configuration Problems

Please send feedback on ads that slipped through, innocent images that were blocked, sites that don't work properly, and other configuration related problem of `default.action` file, to http://sourceforge.net/tracker/?group_id=11118&atid=460288, the Actions File Tracker.

New, improved `default.action` files may occasionally be made available based on your feedback. These will be announced on the [ijbswa-announce](#) list and available from our the [files section](#) of our [project page](#).

6.2.2. Reporting Bugs

Please report all bugs through our bug tracker: http://sourceforge.net/tracker/?group_id=11118&atid=111118.

Before doing so, please make sure that the bug has *not already been submitted* and observe the additional hints at the top of the [submit form](#). If already submitted, please feel free to add any info to the original report that might help to solve the issue.

Please try to verify that it is a Privoxy bug, and not a browser or site bug or documented behaviour that just happens to be different than what you expected. If unsure, try [toggling off](#) Privoxy, and see if the problem persists.

If you are using your own custom configuration, please try the stock configs to see if the problem is configuration related. If you're having problems with a feature that is disabled by default, please ask around on the mailing list if others can reproduce the problem.

If you aren't using the latest Privoxy version, the bug may have been found and fixed in the meantime. We would appreciate if you could take the time to [upgrade to the latest version](#) (or even the latest CVS snapshot) and verify that your bug still exists.

Please be sure to provide the following information:

- The exact Privoxy version you are using (if you got the source from CVS, please also provide the source code revisions as shown in <http://config.privoxy.org/show-version>).
- The operating system and versions you run Privoxy on, (e.g. Windows XP SP2), if you are using a Unix flavor, sending the output of `uname -a` should do, in case of GNU/Linux, please also name the distribution.
- The name, platform, and version of the browser you were using (e.g. Internet Explorer v5.5 for Mac).
- The URL where the problem occurred, or some way for us to duplicate the problem (e.g. <http://somesite.example.com/?somethingelse=123>).
- Whether your version of Privoxy is one supplied by the Privoxy developers via SourceForge, or if you got your copy somewhere else.
- Whether you are using Privoxy in tandem with another proxy such as Tor. If so, please temporary disable the other proxy to see if the symptoms change.
- Whether you are using a personal firewall product. If so, does Privoxy work without it?
- Any other pertinent information to help identify the problem such as config or log file excerpts (yes, you should have log file entries for each action taken).

Privoxy Frequently Asked Questions

You don't have to tell us your actual name when filing a problem report, but please use a nickname so we can differentiate between your messages and the ones entered by other "anonymous" users that may respond to your request if they have the same problem or already found a solution.

Please also check the status of your request a few days after submitting it, as we may request additional information. If you use a SF id, you should automatically get a mail when someone responds to your request.

The [appendix of the Privoxy User Manual](#) also has helpful information on understanding `actions`, and `action debugging`.

6.3. Request New Features

You are welcome to submit ideas on new features or other proposals for improvement through our feature request tracker at http://sourceforge.net/tracker/?atid=361118&group_id=11118.

6.4. Other

For any other issues, feel free to use the mailing lists. Technically interested users and people who wish to contribute to the project are also welcome on the developers list! You can find an overview of all Privoxy-related mailing lists, including list archives, at: http://sourceforge.net/mail/?group_id=11118.

7. Privoxy Copyright, License and History

Copyright © 2001-2007 by Privoxy Developers <ijbswa-developers@lists.sourceforge.net>

Some source code is based on code Copyright © 1997 by Anonymous Coders and Junkbusters, Inc. and licensed under the *GNU General Public License*.

Portions of this document are "borrowed" from the original Junkbuster (tm) FAQ, and modified as appropriate for Privoxy.

7.1. License

Privoxy is free software; you can redistribute it and/or modify it under the terms of the *GNU General Public License*, version 2, as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the *GNU General Public License* for more details, which is available from the Free Software Foundation, Inc, 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

You should have received a copy of the *GNU General Public License* along with this program; if not, write to the

Free Software
Foundation, Inc. 51 Franklin Street, Fifth Floor
Boston, MA 02110-1301
USA

7.2. History

A long time ago, there was the Internet Junkbuster, by Anonymous Coders and Junkbusters Corporation. This saved many users a lot of pain in the early days of web advertising and user tracking.

But the web, its protocols and standards, and with it, the techniques for forcing ads on users, give up autonomy over their browsing, and for tracking them, keeps evolving. Unfortunately, the Internet Junkbuster did not. Version 2.0.2, published in 1998, was (and is) the last official release available from Junkbusters Corporation. Fortunately, it had been released under the GNU GPL, which allowed further development by others.

So Stefan Waldherr started maintaining an improved version of the software, to which eventually a number of people contributed patches. It could already replace banners with a transparent image, and had a first version of pop-up killing, but it was still very closely based on the original, with all its limitations, such as the lack of HTTP/1.1 support, flexible per-site configuration, or content modification. The last release from this effort was version 2.0.2-10, published in 2000.

Then, some developers picked up the thread, and started turning the software inside out, upside down, and then reassembled it, adding many new features along the way.

The result of this is Privoxy, whose first stable version, 3.0, was released August, 2002.