

PeerGuardian 1.7 User Guide

Brian Bergstrand

August 15, 2011

Copyright © 2005-2011 Brian Bergstrand

This document may be freely translated into other languages or media.

Contents

1	License	5
2	About	5
3	Credits	5
4	Requirements	6
5	Installation	6
5.1	Upgrading from older versions	6
6	Configuration	6
6.1	Internal PeerGuardian Lists	6
6.2	Creating a Custom List	7
6.3	Editing a List's Properties	7
6.4	Exporting/Merging/Converting Lists	8
6.5	Temporarily Allowing an Address	8
6.6	Finding the Address Associated with a Domain Name	8
6.7	Allow Standard Ports and Its Implications on Security	8
7	Applescript Support	10
8	Why is Apple.com Blocked?	10
9	Uninstall	11
10	Components	11
10.1	PeerGuardian application	11
10.2	pgagent.app	12
10.3	pploader.app	12
10.4	pplogger.app	12

10.5	PeerGuardian.kext	13
10.6	xxx.qnation.PeerGuardian.locum	13
10.7	xxx.qnation.PeerGuardian.locum.plist	13
10.8	pgmerge	13
11	Release History	13

1 License

PeerGuardian for OS X

Copyright © 2005-2011 Brian Bergstrand. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2 About

PeerGuardian is Phoenix Labs premier IP blocker for OS X. PeerGuardian integrates support for multiple lists, list editing, automatic updates, and blocking all of IPv4 (TCP, UDP, ICMP, etc), making it the safest and easiest way to protect your privacy on the Internet.

3 Credits

- M. Uli Kusterer’s UKKQueue: <http://www.zathras.de/programming/sourcecode.htm>
- 7za binary from the p7zip project: <http://p7zip.sourceforge.net/>
- S2DMGraphView from Snowmint Creative Solutions LLC: <http://developer.snowmintcs.com/frameworks/sm2dgraphview/index.html>
- Portions of Theodore Ts’o’s uuid library: <http://e2fsprogs.sourceforge.net/>.
- Application icon from Phoenix Labs: <http://www.phoenixlabs.org/>

4 Requirements

- Mac OS X 10.6 or greater (Intel only) — older versions will not be supported.
- Growl (<http://growl.info>) is required for the Temporary Allow feature.
- PG is only supported when running from an Admin account.

5 Installation

PeerGuardian is a self-contained application that will install its privileged components automatically as needed.

After privileged component installation, it is recommended that you relaunch any running network applications so PeerGuardian is activated for their connections. There is no need to reboot your computer.

5.1 Upgrading from older versions

Version 1.6 and earlier required manual installation. The current version of PeerGuardian should upgrade properly from version 1.6 and 1.5.x. If you are running a version of PeerGuardian older than 1.5, or you encounter any issues upgrading to the latest version, you should run the Uninstaller application included with the older version of PeerGuardian and then attempt to run the current version.

Please make sure you do not have duplicate PeerGuardian applications.

6 Configuration

6.1 Internal PeerGuardian Lists

PeerGuardian creates several automatically maintained internal lists and stores them in sub-folders created in the ~/Library folder. In addition internet list caches are stored in the Library folder. All of these lists and any folders created by PeerGuardian are considered a private implementation detail and you

should not rely on their location or even their existence; especially when creating your own custom lists.

6.2 Creating a Custom List

To create a custom list, open the List Manager window and click the Add button. A new list item will appear in the list window. For an Allow list, check Allow All. For a block list, uncheck both Allow All Ranges and Allow Standard Ports.

Next, enter a description for the list. This is just to help you identify the list, so it can contain anything you like.

Now you need to specify the list URL(s). If the list will be stored on your computer, you can click the Choose File button and select a location for the file using the standard OS X Save panel. For a file downloaded from the Internet, you must click the plus (+) button and then type the full URL (including the resource specifier — `http://`, `ftp://`, etc) into the URL text field. *Very Important: In order for the change to be recognized, you must hit the return key.* Repeat this for every URL you want to add.

For lists stored on your computer, you need to enter IP address ranges. To do this, click the Add button (in the editing sheet, not the List Manager) and enter a description for the range and the starting and ending IP addresses. If the ending IP address is left empty, the starting address will be used to fill it in thereby creating a range of one address. However, if the ending IP address is smaller than the starting address an error will occur. Repeat this for every range you want to add. To remove a range, select it and click the Remove button.

To save your new list simply, click on another list or any empty space in the list item column. You may also close the window. Any of these actions will cause the list to be saved.

6.3 Editing a List's Properties

To edit a list, open the List Manager window and click on the list item.

To edit a URL, select the URL from the drop down menu and make your changes. When done, make sure to hit the return key so the change is recognized.

To remove a URL, select the URL from the drop down menu, and click the minus (-) button next to the URL text field.

6.4 Exporting/Merging/Converting Lists

To export or merge one or more lists, open the List Manager window, select the list(s) you wish to merge and then choose Export from the File menu. In the resulting Save panel, you can select the new list format — binary or text. The binary format results in smaller files at the expense of human readability. The text format allows readability at the expense of larger file sizes.

If you want to merge list files not managed by PeerGuardian, a command line tool, `pgmerge`, is included in the PeerGuardian bundle. If PeerGuardian is located in your Applications folder, you would access `pgmerge` as follows:

```
/Applications/PeerGuardian.app/Contents/Resources/pgmerge
```

6.5 Temporarily Allowing an Address

This feature requires Growl. When an address is blocked, you can click on the corresponding Growl notification window and a PeerGuardian window will appear front and center permitting you to temporarily allow the address for a certain time period. You can also permanently allow the address if you have previously created a custom allow. Once allowed, it may take a couple of seconds for the address change to take effect (you will see a Growl notification that the “Temporary Allow” list has been loaded/reloaded) — you can then access the previously blocked address.

According to the Growl documentation, some themes do not support notification clicks, so be aware of that if it doesn’t work for you.

6.6 Finding the Address Associated with a Domain Name

PeerGuardian includes an integrated name lookup utility. Simply select “Name Lookup” from the file menu, enter the name and press the *return* key. Addresses associated with the name will be displayed in the “Addresses” field and can automatically be added to an existing allow/block list using the provided buttons.

6.7 Allow Standard Ports and Its Implications on Security

When “Allow Standard Ports” (HTTP and FTP) is turned on for any list and you use local server applications, you run the risk of companies getting through PeerGuardian’s filters. To allow the convenience of “Allow Standard Ports”

(particularly when browsing the web) and still protect yourself from companies in the block lists, PeerGuardian provides a way to filter remote connections using any Standard Port based on the local port they are connecting to.

Example:

You are downloading a Bit Torrent file (using the default local port 6881), and a peer at address 192.168.1.254 using port 80 (the HTTP port) tries to connect to your machine. This peer is run by a company in the block list. The peer is allowed to connect even though they are in the block list because port 80 is an allowed Standard Port.

To prevent this problem, PeerGuardian offers a way to specify local ports that Standard Ports are not allowed to connect to without going through the normal filters first.

Open PeerGuardian's preferences (cmd-,) and enter the local ports you wish to filter in the "Filter remote std. port access to these local ports" field. You can enter individual ports and port ranges. Each port or range must be separated by a comma (',') and ranges are specified by a starting port and ending port separated by a dash ('-'). The ports do not have to be in numerical order, and spaces are allowed. Negative numbers and numbers larger than 65535 are not allowed.

Example:

4662,6881-6889,5534

This rule would apply PeerGuardian's filters to any remote peer trying to connect using a Standard Port to any of the following local ports: 4662, 6881, 6882, 6883, 6884, 6885, 6886, 6887, 6888, 6889, and 5534.

Now, going back to our initial example, when peer 192.168.1.254 using port 80 tries to connect to your Bit Torrent client (on port 6881), PeerGuardian applies the block list filters and the peer is blocked from connecting.

It is up to you to find out the local ports that your applications are using and enter them into PeerGuardian's port list.

In addition to the above, it is recommended that you use any port blocking feature of your applications to block connections initiated from your client to a peer using one of the standard ports. PeerGuardian can only apply the port filters when peers connect to you, not when you connect to other peers (which is less likely, but can still occur). For instance, the Azureus BitTorrent client can block incoming and outgoing connections to any peers using specified data ports (Preferences->Transfer->Ignore peers with these data ports). If your ap-

plication offers this option, you should enter the following ports: 20, 21, 80, 443.

7 Applescript Support

pploader (10.3) supports basic Applescript commands that can enable/disable the filters and update Internet based lists.

Examples:

```
-- Get the current filter state
tell application "pploader"
set fstate to filters enabled
end tell

-- Disable the filters -- use true to enable them
tell application "pploader"
set filters enabled to false
end tell

-- Check for Internet list updates
tell application "pploader" to update lists
```

8 Why is Apple.com Blocked?

Since Apple is a software company and a member of the Business Software Alliance (BSA), the list maintainers include Apple's address ranges in the block lists. However, PeerGuardian, ships with HTTP and FTP (PeerGuardian defines these as "standard ports") access enabled for the P2P list (which is where the Apple range is defined). This should allow most Apple services to work (.Mac web services, Software Update, iCal updates, etc).

There are a few services that are known not to work:

1. iChat Video behind a Network Address Translation (NAT) router. iChat needs to make a connection on a non-standard port to *snatmap.mac.com* in order to create a video connection through a NAT router. To allow iChat

Video to work, you will have to create a custom allow list and add the IP address(s) for *snatmap.mac.com* to the custom list.

To find the address(s) for any domain name and automatically add them to a custom list, use the method outlined in Section 6.6.

2. Network Time Protocol (NTP) time sync service. The default Mac OS X time server is *time.apple.com* and is blocked because it also relies on a non-standard port. To get around this problem, it is recommended that you use an open access educational time server from this list: <http://support.ntp.org/bin/view/Servers/WebHome>

Educational addresses are not blocked unless you have the EDU list active (which it should not be unless you are on a University network). Government and corporate addresses have a higher chance of being blocked by the P2P block list.

You could also add the *time.apple.com* address to a custom allow list using the method defined in (6.6), but when an alternate address is available for a server, it should be preferred over a custom allow.

3. .Mac POP/IMAP access. While .Mac WebMail works, POP/IMAP access does not. You will have to follow the procedure outlined in (6.6) to create a custom allow entry for the .Mac mail servers.

9 Uninstall

Select Uninstall... from the PeerGuardian application menu. PeerGuardian will remove its privileged components, remove its preference files and finally move itself to the Trash and then quit.

Do not attempt to uninstall PeerGuardian by any other means.

10 Components

10.1 PeerGuardian application

The main application that you interact with. It allows you to view log entries, manage and create lists, view statistics and enable/disable the filters. This application does not have to be running for normal operation of PeerGuardian, you may quit it at anytime. You may place this application anywhere you wish.

Please note that the log window only shows events added while the application is running. If you wish to view older events, open `~/Library/Logs/PeerGuardian.log` using Console or your favorite text editor.

10.2 pgagent.app

A background helper application that displays the statistics window and the PG global menu bar item. This application is contained within PeerGuardian.app and is added to your Login Items list the first time PeerGuardian.app is launched.

10.3 pploader.app

A background helper application that handles list management, including updating lists from the Internet and loading them into the kernel filter. A check for list updates is performed every three hours. This application is contained within PeerGuardian.app and is added to your Login Items list the first time PeerGuardian.app is launched.

pploader caches lists it downloads in `~/Library/Caches/xxx.qnation.PeerGuardian`. pploader loads these cache files first and then looks for updates. That way you are protected even if the lists are not currently accessible via the Internet. File names in this folder may not correspond to URLs in the List Manager — this is normal.

This application is vital to the proper operation of PeerGuardian.

10.4 pplogger.app

A background helper application that handles logging events received from the kernel filter. All events are written to `~/Library/Logs/PeerGuardian.log` and the binary file `~/Library/Caches/xxx.qnation.pghistory` (used for statistical graphing). The PeerGuardian.log file is automatically archived and rotated out when it reaches 128MB in size. The binary history file is automatically truncated to half its size when it reaches 512MB in size.

In addition to logging, this application notifies Growl when block and list events occur. This application is contained within PeerGuardian.app and is added to your Login Items list the first time PeerGuardian.app is launched.

This application is vital to the proper operation of PeerGuardian.

10.5 PeerGuardian.kext

The kernel extension that does the actual packet filtering. Located in /Library/Application Support/PeerGuardian

10.6 xxx.qnation.PeerGuardian.locum

A utility used to perform privileged operations (such as KEXT load/unload). Located in /Library/PrivilegedHelperTools

10.7 xxx.qnation.PeerGuardian.locum.plist

The Launchd configuration file used to start the privileged operations utility. Located in /Library/LaunchDaemons/

10.8 pgmerge

A command line utility that can convert/merge lists. See the Export section (6.4) for more information.

11 Release History

1.7

- PeerGuardian is self-contained and no longer requires a separate installer and uninstaller.
- Optimizations to make better use of multi-core machines.
- Default lists use iblocklist.com, Bluetack is no longer used.
- Bug fixes for list management.

1.6

- 10.6 is required (and thus so is an Intel machine).

- 64-bit applications and kernel extension.
- Redesigned list manager window.
- Bug Fix: possible runaway growth of history file.

1.5.1

- Bug Fix: Missing lists in global status app and/or the main GUI app.
- Bug Fix: possibility of allow lists being ignored in the kernel filter (dependent on load order).
- Other minor bug fixes.

1.5

- Historical and Real-Time graphing of all connections.
- New global status item that allows quick access to Enable/Disable global and per-list filters.
- Auto-allow of local network configuration addresses, including DNS servers, routers and assigned interface addresses. Any changes made to the system are automatically detected.
- Stats now update once per second.
- Increased size of kernel log buffer for large memory machines.
- More text list parsing enhancements to recognize more badly formatted entries in the Bluetack lists.
- Removed blocklist.org lists from the list defaults as the domain no longer belongs to Phoenix Labs.
- Leopard compatibility.
- GUI uninstaller.

- Bug Fix: Files that downloaded correctly but were actually corrupted were being cached locally. If the same file was corrupted the next time it was downloaded, then the corrupted local cache file also failed and so a huge range of addresses could be "lost". Corrupted files are no longer cached locally.
- Bug Fix: OS 9 binary names were not being logged properly on Leopard.
- Bug Fix: Allowed native IPv6 addresses would be logged with junk for the '(name:list)' portion of the log entry.
- Bug Fix: Rare memory leak in pplogger when detaching from the kernel.
- Bug Fix: Corrupt editing session if a list updated while editing another list.

1.4.2

- Text list parsing enhancements to recognize some badly formatted entries in the Bluetack lists.
- Bug Fix: (Regression) The text list parser would always set the ending address to the start address, thus severely truncating the number of addresses that were actually loaded.

1.4.1

- The PG version checker now verifies the hash of any downloaded updates.
- Bug Fix: (Regression) Inability of pploader to load KEXT.
- Bug Fix: Spurious Installer error for new installs.

1.4

- Intel Macs are now fully supported.
- New statistics: Connections / Blocks per second.
- Internet based lists support multiple URLs per list. These are combined into one list before loading.

- Security: Only the user (or root) who originally loaded a list can unload/reload it.
- Removed delay (by design) that could occur when creating a new temporary allow.
- The List Manager window now displays extra list info in place of the URL.
- Blocklist.org lists are back, along with all new list definitions (new installs only).
- Bluetack lists changed to zip variants.
- pplogger will try to log the real name of CFM (OS 9 format) apps instead of the wrapper used to launch them (LaunchCFMApp).
- Bug Fix: pplogger crash if the application involved in the log event was no longer running when the event was processed.
- Bug Fix: Address "255.255.255.255" was treated as invalid in some circumstances.
- Bug Fix: (Intel Only) Wrong port numbers in the log file.
- Bug Fix: (Intel Only) Backwards IP addresses displayed in the PG range editor window.
- Bug Fix: Multiple unnecessary list reloads after a restart.

1.3.2

- Added version checker.
- Bug Fix: Another possible panic when disabling the filters.
- Bug Fix: pploader crash when adding a custom Internet based list.
- Bug Fix: Error merging lists that contained an empty range description.
- Bug Fix: The Name Lookup window replaced (instead of merging) existing entries with the found addresses.
- Bug Fix: A click on OK in the prefs window with an empty port rule caused a spurious error.

1.3.1

- Integrated name lookup utility with the ability to automatically add found addresses to a custom allow/block list.
- Automatic list updates can be disabled.
- pplogger limits Growl notifications to five (5) per second.
- Bug Fix: Possible kernel panic when disabling the filters (most likely on a dual-cpu when the network was very busy).
- Bug Fix: Errant error 22 when merging some lists (such as bogon).
- Bug Fix: Ranges that had a starting address of 0 were being ignored.

1.3

- PeerGuardian supports list export/merge/conversion. A comand line tool, pgmerge, is also included in the PeerGuardian bundle.
- pplogger coalesces duplicate entries.
- Growl notifications for list load/unload/reload.
- The icon for Growl block notifications contains a disabled badge symbol.
- pplogger will compress the current log file and create a new one whenever the file becomes larger than 128MB. This is a hard runtime limit and does not affect the (smaller) launch time compression limit.
- pplogger throttles Growl notifications if Growl stops responding in a timely manner.
- Related to the above, log file entries are now near real time even if Growl becomes stalled. In previous versions, a Growl stall would also stall writing events to the log file.
- The “Temporary Address Action” window buttons respond to keyboard shortcuts.
- The “Display Blocked Addresses With Growl” option has been removed due to Growl being required for temp allow. If you don’t want to see blocked notifications, you can still turn them off in Growl itself.

- Reduced shared memory usage for p2p and p2b(v2) lists.
- Bug Fix: Parsing bug that could allow invalid ranges from text files, which in turn could block 90% of the IP4 address space.
- Bug Fix: Blocked address count was lower than the actual number being blocked (cosmetic only).

1.2

- Re-branded to PeerGuardian. First official PhoenixLabs release.
- Temporary Allow support. Requires Growl. See the “Temporarily Allowing an Address” section.
- The filters can now be enabled/disabled from the PeerGuardian dock menu.
- PeerGuardian widget (statistics only).
- The log format now includes both the port number and port name (where possible) instead of one or the other.
- New application icon.
- PeerGuardian.app now displays a disabled symbol in its dock icon when the filters are disabled.

1.1

- Added new port rules support. See the “Allow Standard Ports Security” section.
- Added AppleScript support to ploader. The filters can now be enabled/disabled with an AppleScript.
- The checkboxes in the List Manager window are now disabled to provide visual feedback that they are for status purposes only.
- Renamed “Block Standard Ports” to “Allow Standard Ports”. This is more inline with PG2’s “Allow HTTP”. This is just a name change, there is no need to change the actual setting.

- Removed port 8080 (alternate HTTP) from the Standard Ports list. It's rarely used by actual HTTP servers and is more likely to be used by Anti-P2P companies.
- The log format has changed to put the year after the month/day and include a timezone.
- Included PeerProtectorUninstall.sh script.
- Bug Fix: UDP sockets that did not "connect" were not being filtered.
- Bug Fix: Another parsing bug that could cause some addresses to slip through the filter.
- Bug Fix: pplogger hang during quit — when upgrading from a previous version, you will have to Force Quit pplogger using Activity Monitor.
- Bug Fix: In certain situations, it was possible for list changes to be lost when pploader was quit.

1.0

- Unloading the kernel filter is now possible on 10.4.3. pploader will automatically recognize when a new version is installed and unload the current version then load the new one — there is no longer a need to reboot. Since there is still a bug preventing unloading on 10.4.2, it is no longer supported.
- When possible, log entries now contain the process name and process id of the application that attempted the connection.
- Bug Fix: Kernel panic that occurred when the internal log event buffer became full (which would only occur if pplogger was not running).
- Bug Fix: Possible infinite loop during file parsing (specifically if PP somehow tried to parse a binary file).
- Bug Fix: On wake from sleep, pploader would continually attempt to download the active lists causing high CPU usage.
- Bug Fix: Rare hang during loading of lists that would cause all connection attempts to be blocked.

- Bug Fix: pplogger memory leak and two cases of lost entries (both occurring only when the kernel msg buffer was full — which is quite rare).
- Bug Fix: Possible permanent reduction of kernel log buffer.

0.3.5

- Added “Display Blocked Addresses Only” pref to PeerProtector’s log window. If checked, allow events will no longer be displayed in the log window. They will still be in the log file though.
- Minor change in the way pplogger caches port names to reduce memory usage.
- Fixed bug in pplogger that caused the log file to be compressed and re-created every time pplogger was launched instead of waiting for the size to reach 2MB.
- Bug Fix: If a list is deactivated, it will now be unloaded from the kernel filter list, this was not done in previous versions.
- Bug Fix: If you deactivate the filters, quit PeerProtector and re-launch it, PeerProtector will now have the correct state instead of assuming the filters are enabled.
- Bug Fix: Parsing bug with Bluetack lists that caused some blocked ranges to be ignored (about 500 out of the 86000 in the level1 list).

0.3

- Filter events are now logged with the names of ports where it makes sense (e.g., http instead of 80).
- Block HTTP has been changed to “Block Standard Ports” as FTP is now included in the ports to allow/block.
- pplogger will create a new log file during launch if the current one is 2MB or larger. The old file is moved to a date based name and then compressed with bzip2.

- Fixed a bug in PeerProtector that caused a new entry to be added to your Login Items for both pploader and pplogger every time PeerProtector was launched. You should open your Login Items and remove all of the duplicate entries.

0.2

- All new GUI, including support for custom lists (allow or block), Growl block display and other goodies.
- The kernel filter now blocks ICMP in addition to UDP and TCP.
- PP can now parse p2p text files in the following format (Bluetack.co.uk uses this): name/description:ipstart-ipend\n
- Substituted Bluetack.co.uk lists for blocklist.org ones until the whole meth-labs incident is resolved.

0.1

- First release.