The ProxEye User's Manual

(Document revision 3.00.00)

Legal Notice and Disclaimer:

BAJAI Inc. "including its employees and agents" assume no responsibility for any consequences resulting from the use of the information herein, or in any respect for the content of such information, including "but not limited to" errors or omission, the accuracy or reasonableness of factual or scientific assumptions, studies and/or conclusions, the defamatory nature of statements, ownership of copyright or other intellectual property rights and the violation of property, privacy or personal rights of others. BAJAI Inc. is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference to or reliance on such information. No guarantees or warranties, including "but not limited to" any express or implied guarantees, warranties of merchantability or fitness for any particular use or purpose, are made by BAJAI Inc. with respect to such information.

Third Parties:

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by BAJAI Inc. and such reference shall not be used for advertising or product endorsement purposes. Any or all websites used for example references only and may have trademarks or copyrights and should be considered as proprietary.

Trademarks:

BAJAI, the BAJAI logo, Iajabot, ProxEye, BajEye, EyeNalysis, EyeUpdate, EyeMail, OCULAR and "images, everything" are registered trademarks, slogans or trademarks of BAJAI Inc.

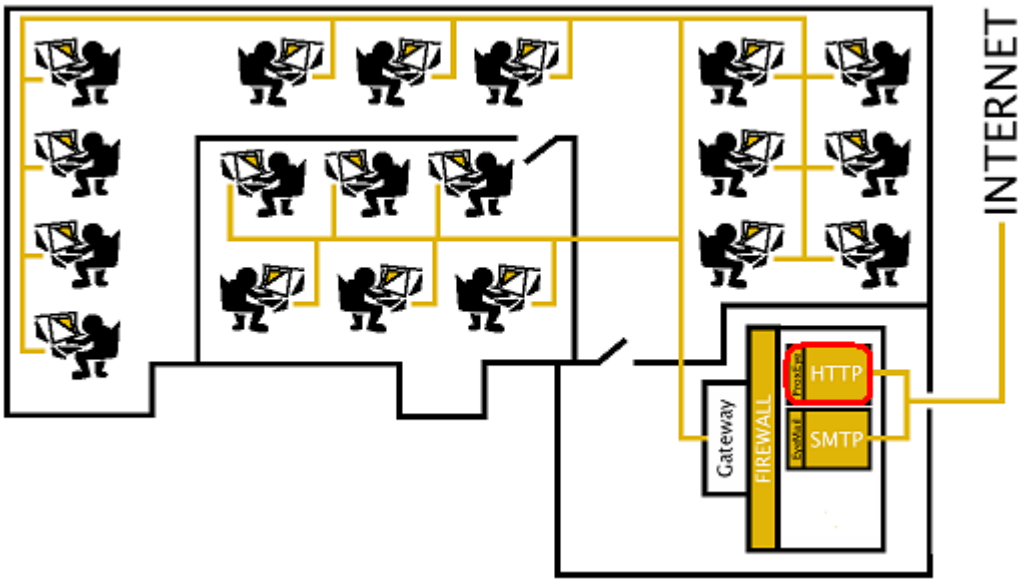
BAJAI Inc. may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give any license to these patents, trademarks, copyrights, or other intellectual property rights except as a expressly provided in any written license agreement from BAJAI Inc.

TABLE OF CONTENTS

Introduction

This document is intended to be a user's manual for the *ProxEye* Internet filtering software from **BAJAI**. *ProxEye* is software that can be used either as an HTTP proxy server or as a plug-in for the Squid caching-proxy server. The main purpose of *ProxEye* is as a tool for administrators to manage the types of web-content that are accessible from computers on their networks.

ProxEye works as a simple HTTP pass-through proxy server that performs extremely high speed analysis of requests for World Wide Web content. ProxEye can also act as your http proxy server should you not have one in place already. By using ProxEye as a pass-through authentication server allows you to make use of the specialized functionality of your current HTTP proxy server such as caching etc. As you can see from the diagram below, *ProxEye* will fit simply into your existing infrastructure and seamlessly provide online web activity management.



ProxEye must first be installed and then subsequently configured. The configuration allows you to create groups and individuals with specified access rights. Throughout this manual we assume that the reader is familiar with basic system administration and Internet concepts.

Installing *ProxEye*

How you install *ProxEye* depends on whether you are using it as a plug-in for another proxy server or as a stand-alone proxy.

On UNIX systems, the *ProxEye* executable will be found in the directory /usr/local/bin and the configuration files will be found in the *configuration directory* /etc/proxeye.

On Windows systems, both the executable and the configuration files are found in the installation directory. You can install ProxEye simply by running the *ProxEye* installer program that you downloaded. Follow the prompts and installation will be complete in seconds. Once installed, on the machine, you need to install the ProxEye services so that they can be accessed from the Windows Service Management tool.

START→BAJAI→PROXEYE→Install *ProxEye* Services.

Once the services have been installed, you can start and stop the *ProxEye* services via the Services Administration Tool (See windows documentation for more information).

There are menu items that allow you to start and stop the services manually, but it is recommended that you administer the services through the service manager. This allows you greater control of the start-up settings for the service.

NOTE: In order to install the services, you must have administrator privileges on your Windows system.

Removing a P*roxEye* Installation (UnInstalling)

On UNIX systems, you simply stop the ProxEye server and remove the ProxEye installation.

On Windows systems, there is an uninstall applet provided. You will need to stop the service (either from the menu items provided or from the Serice Management tool) and uninstall the services. You can uninstall the services from the start menu:

START→BAJAI→PROXEYE→UnInstall *ProxEye* Services.

Once the services have been stopped and removed for the system configuration, the uninstall applet will remove the programs and all associated files.

Using *ProxEye* as a stand-alone proxy server

Configuring *ProxEye* to run as a stand-alone proxy server is as simple as specifying the port on which *ProxEye* should listen for requests. This is done by editing the file ***proxeye.conf*** in the configuration directory and adding (or modifying) the line

passthru_port=<portnum>

where <portnum> is the port number *ProxEye* should listen to. To then run *ProxEye*, use the command proxeye -passthru. At this point *ProxEye* will listen for HTTP requests on the specified port. Later, if you modify the *ProxEye* configuration files you will have to restart *ProxEye* for your changes to take effect.

If your organization has another proxy server and you would like *ProxEye* to send HTTP requests through this server, then edit proxeye.conf and add or modify the lines

```
http_proxy=<proxy-machine-name>
http_proxy_port=<proxy-port-number>
```

where <proxy-machine-name> is the name of the machine running your proxy server and <proxy-port-number> is the port number your proxy server listens on.

Note that *ProxEye* is not a caching proxy. If you do not have a caching proxy but would like to install a free one, we recommend Squid. Instructions on obtaining and installing Squid can be found in of this manual.

Using *ProxEye* with Squid

If your organization is using the Squid proxy server then you can have Squid use *ProxEye* directly and save the overhead of having HTTP requests go through two proxy servers. To use Squid with *ProxEye*, you need to tell Squid how to use it. To do this, edit the file /etc/squid/squid.conf and look for the text redirect_program=xxx, where xxx can be anything. If you find this line, change it to

```
redirect_program = <path-to-proxeye>proxeye –squid
```

where <path-to-proxeye> is the directory containing the *ProxEye* executable. If you don't find the text, just add the above line to the file. Once you've done this, you have to tell Squid to reread its configuration information. Do this with the command squid -k reconfig.

Configuring *ProxEye*

Assigning users different levels of web activity privileges allows you to specify web access rights per person or per group. It is possible to allow unrestricted access to complete denial of access and all levels in between.

ProxEye is configured exactly the same whether you are configuring for Windows, Linux or Sun/Solaris. The operation of *ProxEye* is controlled through a set of configuration files found in the configuration directory. In Windows, this is the installation directory and the UNIX variants are in the /etc/proxeye/ directory. There are four primary configuration files found in this directory.

groups

This file allows you to create groups of users and define the access criteria each group has. In this file you can create mnemonic group names and apply the access criteria. For example, you can specify group called upper_management and the specify the access rules for the upper management group.

hosts

This file allows you to map computers (IP addresses) onto user groups. In this file you specify which computers belong to which group you have specified in the **groups** file.

overrides

This file allows you to specify which web objects (URLs) are accessible to which groups you have specified in the **groups** file. In this file you can override BAJAI categorizations as well as augment them.

proxeye.conf

This file allows you to specify the general configurations options for the system. These settings are generally globally based settings.

The next 4 sections describe the format of these files in detail, through the use of a running example.

Note to SQUID USERS: If you are experimenting with the *ProxEye* configuration files while reading these sections, be aware that in order for changes in the *ProxEye* configuration files to take effect, Squid must be reconfigured by using the command: squid -k reconfig.

Category Groups

By default, ProxEye maintains a number of special categories, for URLs that have been classified by BAJAI's OCULAR™ technology. A full explanation of the current list of categories supported by ProxEye can be found in the appendices. BAJAI classification lists categorize web sites on the Internet. They are available with the BAJAI list update

subscription that came as part of ProxEye. Currently, the following default categories are available from BAJAI:

noporn blocks access to adult and/or sexually explicit material
noaccess blocks all web access
noads blocks web sites dedicated to advertising
noshopping blocks online shopping and auction sites
nosports blocks web sites dedicated to sports
nofinance blocks banking, trading and other financial sites
nojobsearch blocks sites providing online job search tools
nonews blocks online news and current events sites
nosearch blocks search engines
nogambling blocks online gambling sites
nopersonals blocks online dating and personals services
nomail blocks free online mail hosting sites
noalcohol blocks sites dedicated to alcohol and/or tobacco
nohacking blocks sites offering information about computer hacking
nodrugs blocks sites dedicated to non-prescription/recreational drug use
nofamily blocks sites offering information about family issues such as parenting, divorce
nogovernment blocks government sites
nohighband blocks high bandwidth (music and video) downloads
noshareware blocks free software download sites
notravel blocks sites offering travel information
notvradiomovies blocks sites dedicated to television, radio, or movies
noweapons blocks sites offering information about making and/or using weapons
nowebcam blocks online webcam sites
nowebhost blocks sites offering free web hosting services
nogames blocks sites dedicated to video games
nohate blocks sites advocating intolerance
noacademic blocks sites to academic or educational institutions

In *ProxEye*, adding a host to one of these categories will prevent that host from accessing web sites in that category.

Groups

The purpose of the group file is to let *ProxEye* know the names of the different groups of users in your organization. These group names are used in the other *ProxEye* configuration files.

By default, *ProxEye* also creates a number of special categories, for URLs that have been classified by **BAJAI**. The current list of groups supported by *ProxEye* can be found in the appendices. The categories ***noporn***, ***nofinance*** and ***noshopping*** used in the following example are all categories that are automatically defined from the **BAJAI** lists. Another one of these special groups used in our example is ***noaccess***, and represents users who

have no Internet access except to sites specifically granted to them as overrides to ***noaccess.***

In *ProxEye*, groups represent different classes of users. For example, a large company might have a CEO, managers, system administrators, and ordinary users. Throughout the remainder of this manual, all examples refer to this fictitious company.

The file groups in the configuration directory contain a list of group names; one per line, followed by a list of previously defined categories that members of the first group automatically belong to. E.g:

GroupName **category1 category2 … categoryN**

As well, you can create category groups by specifying a group name and the list of categories that a part of that group. E.g:

CategoryGroup **category1 category2 … categoryN**

Group names can contain any alphanumeric characters and are case-sensitive. For the example above, the groups file might look like the following:

EXAMPLE GROUPS FILE:

the company does not allow employees to do personal finances
or shopping on company time.
this is the creation of a **CATERGORYGROUP** set called .nopersonal that contains the
finance shopping categories.
nopersonal ***nofinance noshopping***

most employees should not do personal business or look at pornography
this is the creation of a group named **all** that cannot surf personal sites (defined above)
nor can that group surf adult web content.
all ***nopersonal noporn***

exceptions are made for these groups
in this case, the CEO, managers and sysadmins are not being access controlled at all
ceo # the president of the company
managers # managers in the company
sysadmin # system administrators

finally we want to create a special group for reprimanded users whose access has been
#completely revoked.
reprimanded ***noaccess*** # employees who have been reprimanded

The # character is a comment delimiter. Anything on a line following the # character is ignored by *ProxEye*. This allows you to put notes in the configuration files that make it easier to understand what is going on.

Again, the purpose of the group file is to let *ProxEye* know the names of the different groups of users in your organization. These group names are used in the other *ProxEye* configuration files.

Hosts

Once a set of groups has been defined, it is necessary to tell *ProxEye* which computers belong to which groups. This is the purpose of the hosts file in the configuration file directory.

Each line of the hosts file contains a range of numeric IP addresses followed by a list of group names. Each group name is prefixed by a + or -, indicating whether or not the computers in the range are members of the indicated group. For example, the line

192.168.0.1-192.168.0.255 +all

indicates that the computers with IP addresses in the range 192.168.0.1-192.168.0.255 belong to the group *all*. For convenience, it is also possible to specify a single IP address, as in:

192.168.0.63 -all

In this case, the computer with IP address 192.168.0.63 is excluded from the group *all*.

The above two lines have the same meaning as the following two lines:
192.168.0.1-192.168.0.62 +all
192.168.0.64-192.168.0.255 +all

Access Management by Date

Group membership directives (web access privileges as defined in the groups file) can be made to depend on the time of day and the day of the week. This is done by appending a *time specification* after all group names. A time specification consists of an optional range of days, followed by an optional range of times.

Days are specified either as a range, as in:

192.168.0.7 +noaccess [Mon-Fri]

or as a comma separated list, as in

192.168.0.7 +noaccess [Mon,Tue,Wed,Thu,Fri]

The above two lines have identical meaning. Here are making sure that the machine with the IP Address 192.168.0.7 has noaccess from Monday to Friday.

The abbreviations *ProxEye* uses for the days of the week are **Mon, Tue, Wed, Thu, Fri, Sat, Sun.** These are **not** case-sensitive.

Access Management by Time

Times are always specified as ranges, in 24 hour format. For example,

192.168.0.7 -noaccess [12:00-13:00]

specifies that host 192.168.0.7 is to be removed from the special group *noaccess* between 12:00 and 13:00. In simple terms, the machine 192.168.0.7 has access to the Internet during lunch hour. Times for which the start time comes after the stop time are assumed to go on to the next day, so that

192.168.0.7 -noaccess [Mon][17:00-8:00]

tells *ProxEye* to remove the host 192.168.0.7 from the group *noaccess* (i.e allow access) from 17:00 on Monday night until 8:00 on Tuesday morning.

EXAMPLE HOSTS FILE

A full example of a hosts file for our fictional company might be:

```
# Nearly everyone has restricted access, with a few exceptions
# defined below
0.0.0.0-255.255.255.255  +all

# The CEO does not have the same constraints as everyone else
192.168.0.63          +ceo -all

# Nor do system administrators
192.168.0.50-192.168.0.59    +sysadmin -all

# Employees can shop or do their personal finances during non
# business hours
0.0.0.0-255.255.255.255 -nopersonal [Mon-Fri][12:00-13:00]
0.0.0.0-255.255.255.255 -nopersonal [Mon-Fri][17:00-9:00]
0.0.0.0-255.255.255.255 -nopersonal [Sat,Sun]

# This employee has had his Internet privileges revoked during
# normal working hours but still has privileges during lunch and after work.
192.168.0.7          +reprimanded -all
192.168.0.7          -reprimanded +all [Mon-Fri][12:00-13:00]
192.168.0.7          -reprimanded +all [Mon-Fri][17:00-9:00]
192.168.0.7          -reprimanded +all [Sat,Sun]
```

NOTE: The order in which entries appear in the hosts file is important. Directives to add or remove hosts from groups are processed in the order in which they appear in the file.

For instance, the first entry in the example hosts file above adds all machines to the group *all* while the second entry removes the host 192.168.0.63 from the group *all*. If these two entries were reversed, the host 192.168.0.63 would end up belonging to the group *all*. The configuration language was designed to allow the most flexibility for the least amount of effort on the part of the administrator. Essentially, our example file throws everyone into the same group and then removes the exceptions. In our fictitious company the CEO and Sys-Admin are not filtered at all.

Generally speaking, when you configure ProxEye you will want to apply the most general rules first and the exceptions to those rules after you have applied the general rule.

Overrides

At this point, all Internet access for computer users in our fictional company have access prevented to URLS in **BAJAI** categories: adult content, finance sites and online shopping sites, with the exception of the CEO (*ceo*) and the system administrators (*sysadmin*). However, the **BAJAI** access manager might prevent access to some sites that employees need access to. Along the same lines, the **BAJAI** categories may not include some sites that the company wants to restrict access to. These types of customized configuration changes are achieved through the overrides file in the configuration directory. Each line of this file contains a URL followed by a list of group names, each prefixed with a + or -, depending on whether access is to be granted (+) or denied (-) to that particular group.

For example the line

http://xxx.com/ -all

prevents computers in the group *all* from accessing web pages in the domain xxx.com, while

http://this-company.com/ +reprimanded

allows computers in the *reprimanded* group to have access to the web pages of this-company.

Since it is possible to define access rules that conflict with each other, it is important to understand how these conflicts are resolved. ***ProxEye*** applies override rules in a special order. To understand this order, we use the example of the URL

http://www.companyx.com/foo/bar.html.

ProxEye first looks for a rule that applies exactly to the URL http://www.companyx.com/foo/bar.html. If such a rule exists, then it is used.

ProxEye then looks for a rule that applies to the directory http://www.companyx.com/foo/. If such a rule exists, then it is used.

ProxEye then looks for a rule that applies to the host http://www.companyx.com/. If such a rule exists, then it is used.

Finally, *ProxEye* looks for a rule that applies to the domain http://companyx.com/. If such a rule exists, then it is used.

Even with this ordering, it is still possible to have a conflict for a single URL. For example, the line

http://www.stockquotes.com/ -all +ceo

disallows access from computers in the group *all*, but allows access from computers in the group *ceo*. However, the IP address 192.168.0.63 belongs to both groups. In cases such as this, the + rule takes precedence over the - rule, and access to http://www.stockquotes.com/ is granted to computers in the group *ceo*.
A complete example for our fictional company might look like the following.

```
# People spend too much time on these sites
http://stockquotes.com/      -all
http://ebay.com/             -all
http://vegasgambling.com/    -all

# But the CEO needs to keep an eye on how the company is doing
http://stockquotes.com/      +ceo

# These are blocked by BAJAI, but we need access to them
http://xxx.com/              +all
http://neato.com/            +all

# Reprimanded employees don't have any access, except to
# the following sites, which they need in order to do their
# work
http://this-company.com/     +reprimanded
http://our-competitor.com/   +reprimanded
```

General Configuration Options

Within the file `proxeye.conf`, you will setup your general configuration that applies to all users. Each configuration option is described in detail below. Each configuration item is listed one per line and the # is the comment delimiter.

serialnumber

Default value: *Demo licence*

This allows you to specify a valid serial number for your ProxEye installation. This serial number will prevent the time-out "feature" of the demonstration software. Encoded within this serial number is number of seats purchased. Should you wish to increase the number of seats allowed to use ProxEye, you should contact BAJAI.

Example usage: *serialnumber=1234567890ABCDEFGH*

bajaiblockurl

Default value: *http://www.bajai.com/redir/*

This allows you set the notification URL for WWW requests that are disallowed due to policy (adult content or shopping for example). Since this is a standard web page, you can customize it to your own needs. Commonly, you would like to place a reminder of your policy for the user to review and a link to override the system (See below).

Example usage: *bajaiblockurl=http://www.bajai.com/blocked.html*

noaccessurl

Default value: *http://www.bajai.com/redir/*

Example usage: *noaccesssurl=http://www.bajai.com/noaccess.html*

This allows you set the redirect URL for WWW requests by users who have had their Internet privileges revoked. Since this is a standard web page, you can customize it to your own needs. Commonly, you would post your policy and reasons for denial of access. This notification page is most commonly seen by reprimanded users who have had their Internet privileges revoked or by employees who need no external web access except at designated times.

ordblockurl

Default value: *http://www.bajai.com/redir/*

This allows you set the notification URL for WWW requests that are disallowed because the administration has decided to block the site in the overrides blacklist. Since this is a standard web page, you can customize it to your own needs. Commonly, you would like to place a reminder of your policy and state that this page requested was blocked because of bandwidth or productivity concerns.

Example usage: *ordblockurl=http://www.bajai.com/overrideblock.html*

blockedfileurl

Default value: *http://www.bajai.com/redir/*

This allows you set the notification URL for specific file requests that are disallowed because the administration has decided to block such file types. Since this is a standard

web page, you can customize it to your own needs. Commonly, you would like to place a reminder of your policy and state that this page requested was blocked the file type causes excess use of bandwidth (.rm, .ram, .mpg etc) or has security compromises (.exe, .cab, .vbs).

Example usage: *blockedfileurl=http://www.bajai.com/blockefile.html*

logfile

Default value*: NULL.*

This allows you to specify the location and file name of the log file. Note that because of ProxEye's cross platform nature, it is important that there are no spaces in the path or filename.

Example usage: *logfile=/etc/proxeye/proxeye.log*
logfile=H:/logs/proxeye.log

maxlogentries

Default value: *0 (Infinite)*

This allows you to specify the maximum number of entries within the logfile. This feature allows you to limit the ultimate size of the log file. ProxEye does this by random sampling of the log file entries. This sampling is uniform over the lifetime of the log file, and therefore gives an accurate representation of user's behavior. Of course, the larger the number of entries in the log file, the more accurate the representation.

If your concern is for limiting disk space over the accuracy of the usage, you can set the limit to a reasonable number. As a basic rule, every 250,000 log entries will require about 30 MB of disk space.

Example usage: *maxlogentries=250000*

logtransgressions

Default value: *FALSE*

This allows you to log all attempts to access URLs that have been classified and subsequent access limited. This will allow the reporting tools to be able to report on attempts to access URLs contrary to your policy.

Example usage: *logtransgressions=true*

logaccesses

Default value: *FALSE*

This allows you to log all attempts to access URLs that have been classified and subsequent access limited. This will allow the reporting tools to be able to report on attempts to access URLs contrary to your policy.

Example usage: *logaccess=true*

allow_https

Default value: *TRUE*

This allows you to specify your policy regarding secure http. Options include NONE, FILTER and ALL. This will let you allow no https communication (NONE) or all https communications (ALL). As well, you can filter requests to https based on the CONNECT site. See the section on HTTPS and Tunneling Protocols below.

Example usage: *allow_https=filter*

http_proxy

Default value: *NULL*

This allows you to specify an alternate proxy that PROXEYE will pass on filtered requests to. This may be the proxy on your firewall or it may be a third party caching proxy. Setting this option allows you to make use of your existing infrastructure and maintain the benefits of your previous purchases. By specifying this option, you are in effect using PROXEYE purely as request classifier and policy alignment tool.

Example usage: *http_proxy=192.168.000.255*

http_proxy_port

Default value: *8080*

This allows you to specify that port that PROXEYE will pass on the valid requests to. This will be to port number that the proxy specified by **http_proxy** listens on.

Example usage: *http_proxy_port=1732*

passthru_port

Default value: *1907*

This allows you to specify that port that PROXEYE will listen on. This will be to port number that is configured within the users browsers.

Example usage: *passthru_port=80*

allow_bypass

Default value: *TRUE*

This option allows end users to override ANY of the classifications. This option must be enabled to the override tag to be accepted. The override tag is a tag that indicates the classification process should be ignored. The tag is '–BAJAILOGGEDOVERRIDE' which is simply appended to a URL request.

To invoke the bypass, a user simply needs to append the override tag to the URL that they wish to request. For example:

http://www.overridethissite.com/--BAJAILOGGEDOVERRIDE

Typically, you would want to provide a link via the blocked page that the user can click on. This is done simply by adding the following tag to your blocked URLs.

<A HREF="javascript:window.location.href = window.location.href + '--BAJAILOGGEDOVERRIDE'">GO THERE ANYWAY!</A>

NOTE: If allow_bypass is set to FALSE, then the override tag has NO EFFECT

Example usage: `allow_bypass=false`

block_file_extensions

Default value: *all extensions allowed*

This option allows you to specify the types of files you want to prevent access to. Commonly this option is used to prevent heavy bandwidth downloads by preventing real media (.rm and .ram), MP3s (.mp3), MPEG (.mpg or .mpeg), and executables (.exe) from being downloaded. **The list is comma delimited**.

System administrators often wish to limit executables (.exe) and installation files (.zip or .cab) to keep the system free of viruses and other problems.

Example usage:

```
block_file_extensions=.mpg,.mpeg,.asf,.asx,.mp3,.rm,.ram,.exe,.zip
```

Debugging your Configuration

When making major changes to an existing *ProxEye* installation, you may want to copy the configuration files into a different directory and edit the copies until you are sure they are properly debugged. To have *ProxEye* use files from a directory other than the configuration directory, use the -d <dir> option, which tells *ProxEye* to look for its configuration files in the directory <dir>.

Once you have written *ProxEye* configuration files for your installation, you can test them with the command **`proxeye -print`**. The **`-print`** option makes *ProxEye* read the configuration files and print a summary of the group information onto your terminal. The output of **`proxeye -print`** for our example is shown in. Of course, the -d and -print options can be used together to test your configuration before activating it.

The -print option prints a summary of group information *at the time it was run*. Since it is possible to have group memberships that vary with time, *ProxEye* provides a way to test these without having to wait. Use the command line option -day to fix the day *ProxEye* uses to compute its configuration information. Use the -time option to fix the time. For example, to see the group information for Mondays at 12:15, use the command line

```
proxeye -print -day Mon -time 12:15
```

The abbreviations of weekdays and the time format are the same ones used in the *ProxEye* configuration files.

Once all your changes have been made and you are certain that they have the effect you intended, you can copy the files back to the configuration directory. Be sure to restart *ProxEye* to have your changes take effect.

Automatic List Updating

Automatic list updating is configured using the program ***listsub*** that came with your PROXEYE installation. This program contacts the main BAJAI list update servers and maintains your lists for you on a daily basis.

In Windows, listsub is a service scheduled to run once daily. On the Unix platforms, listsub is a program that the system administrator can set up a cron job to execute once daily.

Log Files

ProxEye can also be configured to log web traffic in your organization. Each log entry contains the date, time of day, client IP address, URL, and a flag indicating whether the request was allowed or denied.

Logging options are controlled by entries in proxeye.conf configuration file in the configuration directory. The line

logfile = <logfilename>

specifies the name of the file to which *ProxEye* should write its logs. Note that *ProxEye* must have permissions to write to the directory containing this file. Because of the cross platform functionality of ProxEye, spaces in the log file names should be avoided.

The line

logaccesses = <t/f>

tells *ProxEye* whether or not to log HTTP requests that are allowed by *ProxEye*. Here <t/f> must be one of true or false. Similarly, the line

logtransgressions = <t/f>

tells *ProxEye* whether or not to log HTTP requests that are blocked by *ProxEye*.

Finally, the logs of HTTP requests can become very long. The line

maxlogentries = <number>

tells *ProxEye* to limit the number of entries in the log file to less than <number>. *ProxEye* does this by random sampling of the log file entries. This sampling is uniform over the lifetime of the log file, and therefore gives an accurate representation of user's behaviour. Of course, the larger the number of entries in the log file, the more accurate the representation.

Redirection

When *ProxEye* denies access to a web page, it redirects the user's browser to a different web page that presents the user with an informative message saying that their attempted access was blocked. Adding or modifying the following entries in proxeye.conf can change the page to which the browser is redirected.

bajaiblockurl = <url1>
ordblockurl = <url2>
noaccessurl = <url3>
blockedfileurl = <url4>

and setting <url1-4> to be the URLs of the pages the user's browser should be redirected to. The first URL is for requests that are blocked because they are part of the **BAJAI** filter that comes with a list update subscription. The second URL is for requests that are blocked because of entries in the overrides file. The third URL is for requests that are blocked because the user's computer is part of the ***noaccess*** group. The forth URL is for request to specific file type that administration has restricted access.

HTTPS and Tunneling Protocols

ProxEye can be configured to disallow, filter or allow all Secure HTTP (HTTPS) and other tunneling protocols to be used. Setting the allow_https variable in the proxeye.conf file does this.

allow_https = none | filter | all

The value none should be used if you want to disallow all HTTPS requests. The value filter should be used if you would like *ProxEye* to try and filter HTTPS requests the same way it would filter other requests. The value all should be used if you would like *ProxEye* to allow all HTTPS requests to go through without performing any filtering.

The user should note that because of the way in which HTTPS tunneling works, *ProxEye* can only filter HTTPS based on the name of the server to which the request is sent. HTTPS requests cannot be filtered at the URL or directory levels.

Troubleshooting Tips - SQUID

If your *ProxEye* configuration becomes corrupted to the point where your organization's Internet access is lost, the first thing you should do is disable *ProxEye* in Squid. Do this by finding the line

redirect_program = proxeye

in the file /etc/squid/squid.conf and commenting it out by putting a # character in front of it. Then tell Squid to reconfigure itself with the command squid -k reconfig. If this doesn't solve the problem, then it is your Squid configuration or some other part of your network configuration that is corrupted. The best source of information on administering and debugging your Squid proxy is the Squid web site at http://www.squid-cache.org/.

When trying to debug your *ProxEye* configuration, try the following.
Make sure you have activated your *ProxEye* configuration with the command squid -k reconfig.

Look in the system log file for messages from *ProxEye* indicating errors in your configuration files. Under UNIX, *ProxEye* writes its status information to the file /var/log/messages.

Make sure your web browser is configured to use your Squid proxy server.
Make sure your web browser is not using a cached copy of web pages by clearing your browser's cache.

Make sure you have a version of Squid that supports the redirector_program directive (this directive was introduced in Version 1.1).

Check that *ProxEye* is actually running by using a program like ps and looking for a process named proxeye. If *ProxEye* is not running, this is probably because of problem with the configuration files, and a message to that effect should be in the system log file.
If all else fails, and if your *ProxEye* installation is registered for technical support, try contacting **BAJAI** support staff by emailing bajai@bajai.com. You can also get in touch with a technical support team member by calling (613)731-9069.

Troubleshooting Tips – Pass Through Mode

Should you have problems with your configuration you can check the status of the configuration by running ProxEye from the command line with the –print option.

Windows Note: You will need to do this from a "DOS prompt"

```
proxeye -print
```

A full explanation of this utility is explained in Appendix II.

Appendix I - Obtaining and Installing Squid

The Squid proxy server is free software, distributed under the Gnu Public License (GPL). The latest version of the server can be downloaded from the Squid web page at http://www.squid-cache.org/. On the same web page you will find instructions on how to build and install Squid.

The remainder of this section describes a few simple steps to get your Squid server up and running. It is by no means comprehensive, and is only intended to get you started. Once you have followed these steps, you should look at the Squid documentation to learn about more advanced options.

Once you have built and installed Squid, you need to configure it for your network by editing the Squid configuration file /etc/squid/squid.conf. Follow these steps to configure Squid.

1 Choose a port for Squid to listen on. By default, Squid is configured to listen on port 3128. Unless you have a good reason to change this, you can leave it as is. If you do choose to change it, you can do so by uncommenting the line

   #http_port=3128

   in squid.conf and changing the value of the port number.

2 Look for the section of squid.conf labelled ACCESS CONTROL. In this section, define an *access control list* for the computers in your network using a line like

   acl <mynetname> src 192.168.0.1-192.168.0.30/255.255.255.255

   where <mynetname> is a name of your choice, and the range of IP addresses is the range of addresses used by your network.

3 Tell Squid to grant HTTP access to the machines on your network using the line

   http allow <mynetname>

   where <mynetname> is the name you chose in the previous step.

4 If Squid is not already running, start it by typing the command squid. If Squid is already running then reconfigure it by typing the command squid -k reconfig.

5 Configure your browser to use the Squid proxy by setting the proxy server to the name of the computer running Squid and the proxy port to the port number you chose in Step 1.

Appendix II - Sample Output from `proxeye -print`

For the sample configuration used in this manual, running proxeye -print during regular business hours produces the following output:

- proxeye -print -d . -day Mon -time 10:00

```
Host address range                    Groups
------------------                    ------
[000.000.000.000 , 192.168.000.007) : noporn noshopping \
                nofinance nopersonal all
[192.168.000.007 , 192.168.000.008) : noaccess reprimanded
[192.168.000.008 , 192.168.000.050) : noporn noshopping \
                nofinance nopersonal all
[192.168.000.050 , 192.168.000.060) : sysadmin
[192.168.000.060 , 192.168.000.063) : noporn noshopping \
                nofinance nopersonal all
[192.168.000.063 , 192.168.000.064) : ceo
[192.168.000.064 , 255.255.255.255) : noporn noshopping\
                nofinance nopersonal all
```

Running proxeye -print during non-business hours produces the following output:

- proxeye -print -d . -day Mon -time 12:15

```
Host address range                    Groups
------------------                    ------
[000.000.000.000 , 192.168.000.007) : noporn all
[192.168.000.007 , 192.168.000.008) : noporn noshopping \
                nofinance nopersonal all
[192.168.000.008 , 192.168.000.050) : noporn all
[192.168.000.050 , 192.168.000.060) : sysadmin
[192.168.000.060 , 192.168.000.063) : noporn all
[192.168.000.063 , 192.168.000.064) : ceo
[192.168.000.064 , 255.255.255.255) : noporn all
```

The only difference is that terminal 192.168.0.7 is no longer part of the group *noaccess* and has been added to the group *all*.

Appendix III - BAJAI Categories

ProxEye currently has 27 different categories that you can define your web filtering policy around. Each category has been listed below with a short explanation of the content. If you believe we are missing an important category, let us know!

Each URL is categorized as specifically as possible and cross-referenced where possible. This means that certain URLs will be classified into multiple categories. For example, the website http://www.foxsports.com/ would be classified in the following categories: SPORTS and TV_RADIO_MOVIES

Academic

This category contains educational institutions such as schools, universities, colleges and other sites that promote learning and academia.

Adult/Sexual Content

This category contains URLs that contain adult oriented themes and activities. This includes sexual themes and erotica style material such a writings, pictures that show or describe sexual acts. Products that are targeted for an adult market, including escorts, sex toys, strip clubs for example. Explicit materials be it photos, drawings, videos, audio, or textual. All sites or homepages that contain a warning of adult content or front pages that state you must be an adult to view this information are included in this category.

This category **DOES NOT CONTAIN** URLs that contain educational information about sex, sexual orientation, STDs (Sexually Transmitted Diseases), health care issues or other medical information.

Alcohol / Tobacco

This category contains URLs that have blatant references to drinking alcohol or smoking. URLs that contain material that glamorizes or promotes alcohol or tobacco products.

Cult

This category contains URLs that have information on cults.

Drugs

This category contains URLs that have information regarding illegal drugs and drug paraphernalia. URLs that contain information regarding the cover up of usage and how to cheat drug tests. URLs that contain information on substance abuse for the purpose of obtaining a mind-altered state. e.g. glue/gas sniffing, huffing etc.

Family

This category contains URLs that have information regarding family issues such as divorce

Finance

This category contains URLs that have stock trading, stock tickers, banking etc. URLs that contain investment advice, money management and general financing. URLs with information such as accounting, banking, insurance and mortgage

Gambling

This category contains URLs that allow gambling, or contain information about gambling such as betting tips. Lottery sites, casinos and betting pools would fall into this category.

Games /Leisure

This category contains URLs that contain online of downloadable games and gaming information such as tips, cheats and codes. This category also contains leisure sites such as comics, hobbies and other leisure activities. URLs dedicated to or part of the computer/video game industry

Government

This category contains URLs that are government URLs, local to federal. To date the list only contains Canadian and US government URLs on the list.

Hacking

This category contains URLs that have information about hacking computers, including information regarding the illegal use of computers to commit crimes and URLs that contain information about how to illegally hack passwords.

Hate

This category contains URLs that have hateful, racist or other hateful information or otherwise promote hate. Discriminatory behaviours based on sexual orientation, religious beliefs, race, gender, age, abilities/disabilities or political viewpoints. Historical revisionists and militant groups that promote hate.

This category DOES NOT CONTAIN historical events; news or press coverage may include the information that falls into the above guidelines.

High Bandwidth

This category contains URLs that use high bandwidth. URLs that contain audio/video files are included in this category. Streaming media, and live broadcasts also fall into this category.

Job Search

This category contains URLs that are job search/career oriented. Recruiters, headhunters and other such job listings are included in this category.

Mail

This category contains URLs that have offer free email services. E.g. Hotmail

News

This category contains URLs that have current news and recent events.

Personal ads/Dating

This category contains URLs that have personals ads and dating services or advice.

Search

This category contains search engines such as Yahoo, Google, AltaVista and other common Portals.

Shareware

This category contains URLs that have shareware or freeware file downloads.

Shopping

This category contains URLs whose purpose is shopping, consumerism and online purchasing. Auctions, retail stores, specialty shops and restaurants are included in this category.

Sports

This category contains URLs that have sports related themes. This includes sports publications and fan pages.

Travel

This category contains URLs that are relating to travel and vacationing. This category includes airlines, travel agents, tourist pages and the like.

TV / Radio / Movies

This category contains contain information about TV shows, radio shows or movies. Television show fan sites, movie trailers would be found in this category.

Weapons

This category contains that have information on weapons such as guns, knives, bombs etc. URLs that promote the use of weapons or sell weapons and related materials are in this category.

Web Cams

This category contains URLs that have web cameras.

Web hosts

This category contains URLs that host web content for free. E.g. Geocities, angelfire etc.

Web Rings

This category contains URL links to web rings. The effect is to break the webring and prevent further surfing. E.g. webring.org.

LICENSE AGREEMENT

I. License and Use

Subject to the following terms and conditions, we grant you a royalty-free, nontransferable and nonexclusive right:

(A) to use this version of PROXEYE on any single networked computer for which licensed seat users can access, provided that PROXEYE is (1) used on only one such computer at any one time, and (2) used only by the licensed seat users; and

(B) to make and distribute to others unmodified copies of the demonstration version of PROXEYE, without any direct or indirect charge (except for the cost of the media in which the demonstration version is fixed), for non-commercial uses only.

II. Limitation of Liability

ALL USE OF PROXEYE IS ENTIRELY AT YOUR OWN RISK. WE WILL NOT BE RESPONSIBLE TO YOU OR ANY THIRD PARTIES FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES OR LOSSES YOU MAY INCUR IN CONNECTION WITH PROXEYE OR YOUR USE THEREOF, REGARDLESS OF THE TYPE OF CLAIM OR THE NATURE OF THE CAUSE OF ACTION.

III. Indemnity

You will defend and indemnify us against (and hold us harmless from) any claims, proceedings, damages, injuries, liabilities, losses, costs and expenses (including attorneys' fees), relating to any acts by you in connection with PROXEYE, leading wholly or partly to claims against us by third parties, regardless of the type of claim or the nature of the cause of action.

IV. Disclaimer of Warranty

PROXEYE IS PROVIDED "AS IS", WITH ALL FAULTS. WE MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, TITLE, NON-INFRINGEMENT, OR ANY OTHER CONDITION OF PROXEYE

V. Proprietary Rights

Except as specifically licensed above, you may not copy, modify, adapt, merge, include in other software, reproduce, translate, distribute, reverse engineer, decompile or disassemble any portion of PROXEYE.

VI. Miscellaneous

This Agreement contains the entire understanding between you and us relating to your use of PROXEYE and supersedes any prior statements or representations. This Agreement can only be amended by a written agreement signed by you and us. This Agreement shall be interpreted and enforced under the laws of the province of Ontario, Canada.

BY INSTALLING PROXEYE, YOU ARE EXPLICITLY AGREEING TO THE TERMS AND CONDITIONS SET WITHIN.