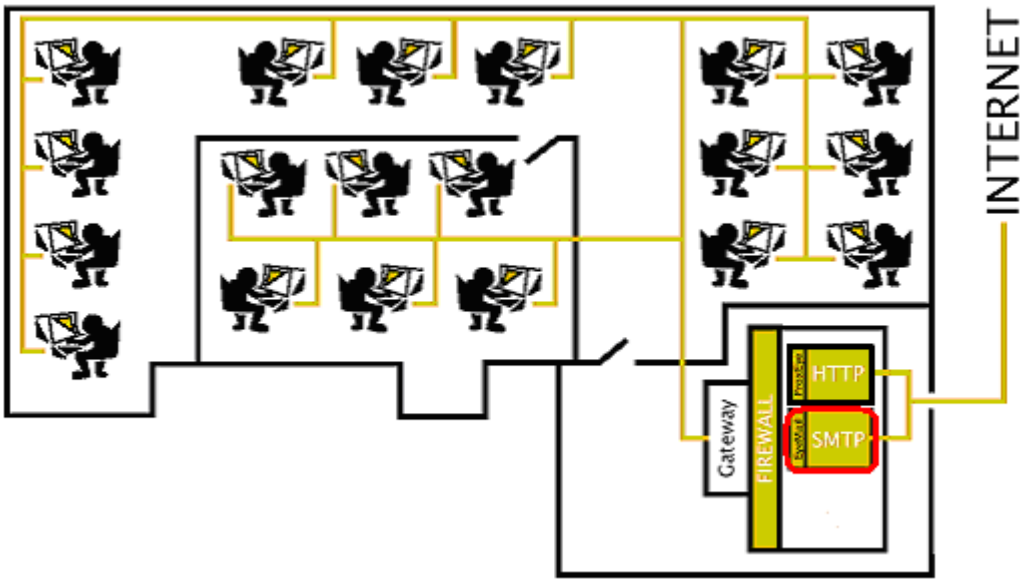
The EyeMail User's Manual

Document Revision 3.00.10

TABLE OF CONTENTS

Introduction

This manual describes the use of *EyeMail*, an intelligent mail forwarding agent that is capable of analyzing and filtering mail attachments sent from within an organization. In the remainder of this document, we assume that the reader is familiar with the administration of an email system.



EyeMail, is an SMTP server that runs on an organization's internal LAN and forwards mail messages to a (third party) SMTP server connected to the Internet. In the process of forwarding this mail, *EyeMail* can strip off attachments that should not be forwarded. Reasons for wanting to filter such attachments include preventing the spread of viruses through email, the overloading of email system by large attachments and legal issues surrounding the distribution of pornographic images.

Installing *EyeMail*

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

On Windows systems, both the executable and the configuration files are found in the installation directory. You can install EyeMail simply by running the EyeMail 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 EyeMail services so that they can be accessed from the Windows Service Management tool. You can do this from the START menu:

Start→BAJAI→EYEMAIL→Install EyeMail Services

Once the services have been installed, you can start and stop the EyeMail 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 *EyeMail* Installations (UnInstalling)

EyeMail comes with an uninstallation applet that can be found in the start menu under:

Start→BAJAI→EYEMAIL→Uninstall

NOTE: Before uninstalling, ensure that you stop the EyeMail service and uninstall (remove the registration information) the eyemail services:

Start→BAJAI→EYEMAIL→Stop EyeMail

Start→BAJAI→EYEMAIL→UnInstall EyeMail Services

Configuring EyeMail

There are several things to consider when configuring and EyeMail installation. Generally speaking, you will create two sets of rules to govern your email policies, one for outgoing email and one for incoming email.

Because of the large volume of data that goes through any email server on a regular basis it is necessary to consider the disk space requirement for the eyemail store for your organization. During this consideration, you will want to choose whether or not it is necessary to keep attachments, temporary files etc. In order for overrides to work in both directions, it is important that both the incoming and outgoing eyemail store be the same place.

Attachment management is another consideration. First of all, you need to consider whether or not it is necessary to whitelist (Allow only the specified types of files) or blacklist (block the specified types of files) attachments. Common considerations include preventing the transmission of executable attachments (blacklisting) to reduce the likelihood of infection from viruses. Another common configuration is to allow only business related documents (whitelist), such as word documents, spreadsheets etc

As EyeMail is meant to be chained to the next SMTP server, it is very easy to exclude users from the EyeMail analysis. Simply have the users who are exempt from the policies send mail to the next-in-chain SMTP server.

EyeMail Configuration Options

Eyemail is simply configured by specifying the options in the eyemail.conf file.

serial_number

Default value: *ABAJAI60DAYTRIAL*

This allows you specify the serial number for your EyeMail installation. If you are running a windows installation, you can specify the license during the installation process and will not need to specify it in the configuration file.

Example usage: *serial_numer=NOTAREALNUMBER*

log_filename

Default value: *eyemail.log*

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

Example usage: *log_file=/etc/proxeye/proxeye.log*

Log_file=H:/logs/proxeye.log

Windows Users Note: This path should not have any spaces in it.

port

Default value: *25*

This is the port that the EyeMail *server listens on. The standard port for SMTP servers to use is 25. Unless you have a very good reason, you should probably leave this set to 25.*

Example usage: *port=2500*

forwarding_server

Default value: *mail*

This is the server that EyeMail forwards messages to after they have been analyzed and (possibly) filtered. This should be the name of an SMTP server that is connected to the Internet.

Example usage: forwarding_server=mail.myorg.com

eyemail_store

Default value: *./ (the same directory that the eyemail executable is in)*

This allows you to specify where temporary files are stored.

Example usage: *eyemail_store=/etc/eyemail/*

eyemail_store=H:/eyemailStore/

Windows Users Note: This path should not have any spaces in it.

analyze_images

Default value: *TRUE*

This allows you to specify if you want EyeMail to analyze images attached to emails and remove them if they appear to be pornographic.

Example usage: analyze_images=false

keep_bad_attachments

Default value: *FALSE*

This allows you to specify whether or not you want EyeMail to save attachments that are stripped from any email passing through.

Example usage: *keep_bad_attachments=true*

allow_overrides

Default value: *FALSE*

This allows you specify whether or not it is possible to override EyeMail assessments and subsequently retrieve attachments that have been removed. This option is used in conjuction with **admin_mail.** The email address specified by **admin_mail** is CC'd when the overridden attachment is sent. This is done to make management aware of all overrides.

Example usage: *allow_overrides=true*

admin_mail

Default value: *NULL*

This allows you to specify an email address of a system administrator or manager who should be notified when users override an EyeMail analysis.

Example usage: *admin_mail=root@mail.yourorg.com*

delete_mail_files

Default value: *TRUE*

Setting this value to true instructs EyeMail to delete all temporary files as soon as they have been processed.

Example usage: allow_https=filter

steganographic_scramble

Default value: *FALSE*

This allows you to specify whether or not you want to scramble the steganographic data storage area to prevent the loss of information being smuggled out of an organization when concealed inside images. For a more complete description of steganographic scrambling, see appendix I.

Example usage: steganographic_scramble=*true*

file_extensions

Default value: *NULL*

This is a comma-separated list of file extensions (suffixes). When *EyeMail* encounters an attachment with one of these extensions, its behaviour is defined by the value of the policy parameter (see below).

Example usage: *file_extensions=.zip,.exe,.vbs,.com*

policy

Default value: *ALLOW_ONLY*

This parameter determines how *EyeMail* handles files ending with suffixes included in **file_extensions.** If this parameter is set to ALLOW_ONLY, then an attachment will always be removed from an email unless it ends in one of the extensions defined in **file_extensions**. If this parameter is set to DISALLOW_ONLY, then an attachment will always be kept in an email unless it ends in one of the extensions defined in **file_extensions**, in which case it will be removed.

Example usage: *policy=DISALLOW_ONLY*

filter_text

Default value: *FALSE*

This allows you to specify whether or not you want to examine the text of email messages and text based attachments to remove keyword content specified by your organization. The keyword content is specified by your organization and can be both trade secret information as well as text content that may be considered offensive or inappropriate for your organization. The keyword content is specified in the file specified by the option **tradesecret_filename.**

Example usage: *filter_text=true*

tradesecret_filename

Default value: *keylist.dat*

This allows you to specify the textual content to look for when analyzing email. This file is a simple text file that contains a keyword and weight on each line. This file can contain any textual content that you want to filter, both trade secrets and offensive content can be blocked. The weight specifies the importance to place on the word during the semantic processing and contextual analysis phases. This gives your organization the most control possible over the content that is being transmitted on your email system.

For example:

projectX 10
sex 10
etc…

Example usage: *tradesecret_filename=keywords.txt*

add_disclaimer

Default value: *FALSE*

This allows you to specify whether or not you want to add a disclaimer or other message at the bottom of every email leaving your organization. The message to be added to the email is specified in **disclaimer_filename**, which is a simple text file that contains the message to be appended to all emails. This option can be used to append confidentiality or other legal disclaimers. The disclaimer is embedded into the email message as part of the text, not as a separate attachment.

Example usage: *add_disclaimer =true*

disclaimer_filename

Default value: *disclaimer.txt*

This allows you to specify the file that contains the disclaimer text to be appended in all email that leaves the organization. This option is used in conjunction with **add_disclaimer**.

Example usage: *disclaimer_filename=corporateDisclaimer.txt*

allow_hosts

Default value: *NULL*

This allows you to specify which hosts are allowed to use the EyeMail server. This prevents SPAMMERS from relaying or performing otherwise unauthorized usage of the server. By default, no hosts are allowed to use EyeMail, and you must specify all those that are allowed. You can specify wildcards such as * and ranges using – as well as individual IP addresses. The hosts is a semi-colon delimited list.

Example usage:

allow_hosts=`191.9.202.1;191.9.200.0-191.9.200.100;191.9.201.*;`

EXAMPLE CONFIGURATION FILE

In addition to being able to filter any type of mail attachment defined by the user, *EyeMail* is able to analyze many types of image files to determine if they contain pornographic images. The operation of *EyeMail* is controlled through a configuration file called eyemail.conf. An example eyemail.conf file is shown below.

Any text following a # up to the next new line is a comment that is meant for a human reader and is ignored by *EyeMail*. The various assignment operations define the operating parameters of *EyeMail*. They are defined as follows.

```
# port that this server listens on
port=25

# mail transport agent that we forward the filtered mail on to
forwarding_server=mail.slnt1.on.wave.home.com

# should we keep filtered attachments around for later inspection?
keep_bad_attachments=true

# a comma-separated list of file extensions that we either
# allow or disallow (see below). These are not case sensitive
file_extensions=.exe,.zip,.com,.vbs

# we can either allow only files ending with one of the above extensions
# (ALLOW_ONLY) or we can allow all files except those ending with one of
# the above extensions (DISALLOW_ONLY)
policy=DISALLOW_ONLY

# should we filter out trade secret terms from e-mail body text and
# attached text files? put 'true' or 'false'
filter_text=false

# if filter_text is set to true, specify the name of the file that contains
# the trade secrete terms and their weights
tradesecret_filename=keylist.dat

# should we scramble the images stego areas
steganographic_scramble=false

# where should we store our files and temp info
eyemail_store=h:/eyemailStore

# should we add a standard disclaimer
add_disclaimer=true
disclaimer_filename=disclaimer.txt

# overrides?
allow_overrides=true
admin_mail=anthony@bajai.com

#serial Number
```

```
# a semicomma-separated list of hosts
# that can use this server? Wildcards * and ranges are permitted
# e.g. 191.9.202.1;191.9.200.0-191.9.200.100;191.9.200.102-
191.9.200.255;191.9.201.*;

allow_hosts=191.9.200.*
```

In the above example, the *EyeMail* server listens for connections on port 25 and forwards mail to the SMTP server mail.myorg.org. Image attachments are scanned by *EyeMail* to see if they contain pornographic images, and if they do the images are removed before the mail is forwarded. Additionally, attachments whose filenames end in .exe, .zip and .doc are also removed from emails.

Overriding EyeMail

EyeMail can be overridden by simply sending an email requesting the attachment. An email should be sent to eyemailoverride@yourorganization.com with the subject section containing the filename of the attachment to be retrieved.

In order for this feature to used, it must be activated and configured using the options: **allow_overrides** and **admin_mail.**

Appendix I

Steganography simply takes one piece of information and hides it within another. Digital images contain unused or insignificant areas of data that steganography takes advantage of by replacing them with information of another form, an MS Word document, for instance. The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend, or it might contain your company's plans for a secret new product.

In the picture below, a secret message has been embedded. The message is actually the document you are reading right now. As you notice, you cannot see, nor would you know by simple inspection that information is “hiding” within the image.

The next picture is one that has had the information scrambled and is no longer retrievable from the image. The “hidden” data has been effectively removed without altering the way the image looks.

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 EYEMAIL on any single networked computer for which licensed seat users can access, provided that EYEMAIL is (1) used on only two such computers 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 EYEMAIL, 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 EYEMAIL 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 EYEMAIL 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 EYEMAIL, 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

EYEMAIL 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 EYEMAIL

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 EYEMAIL.

VI. Miscellaneous

This Agreement contains the entire understanding between you and us relating to your use of EYEMAIL 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 EYEMAIL, YOU ARE EXPLICITLY AGREEING TO THE TERMS AND CONDITIONS SET WITHIN.